

# THE 8 LAYERS OF THE OSI CAKE

# A FORENSIC TASTE OF EACH LAYER

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "HOW TO HACK FACEBOOK?" ARE NOT ALLOWED FACEBOOK.COM/GROUPS/CYBERSECRETS

# The 8 Layers of the OSI Cake A Forensic Taste of Each Layer

By Information Warfare Center And Cyber Secrets The 8 Layers of the OSI Cake: A Forensic Taste of Each Layer Cyber Secrets: 203 Copyright © 2020 by Information Warfare Center

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems without permission in writing from the publisher

First Edition First Published: July 1, 2020

Authors: Jeremy Martin, Richard Medlin, Nitin Sharma, LaShanda Edwards, Mossaraf Zaman Khan, Ambadi MP Editors: Jeremy Martin, Daniel Traci, Brady Genz

The information in this book is distributed on an "As IS" basis, without warranty. The author and publisher have taken great care in preparation of this book but assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Rather than use a trademark symbol with every occurrence of a trademarked name, this book uses the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark. All trademarks presented in the magazine were used only for informative purposes. All rights to trademarks presented in the magazine are reserved by the companies which own them.

The writer and publisher of this article do not condone the misuse of Tor for illegal activity. This is purely instructional for the purposes of anonymous surfing on the internet for legal usage and for testing Tor traffic monitoring in a subsequent article. To access .onion sites, you must have access to the Tor network. To access i2p sites, you must have access to the I2P network. To access any Surface Web site, you must have access to the Internet.

Cataloging-in-Publication Data: ISBN: 9798652368944

Disclaimer: Do NOT break the law!

## Table of Contents

About the Authors	A
What is inside?	1
Evidence	1
IOT Cyber Investigation Challenges	3
Dark Web Corner	4
Dark Markets	5
Dark Market Busts	6
Tech Giants help Law Enforcement:	7
Exploit Those That Exploit Children	7
#BlueLeak	9
Article Title Hacker Groups	10
Something cools about hacker groups	10
CSI Linux	13
CSI Linux Forensic Challenge 204	15
CSI Linux Forensic Challenge 201	17
Winner: Apostolos Gkletos	17
The Challenge	17
CTF 201 Chain of Custody	
Case Challenge - Apostolos Gkletos	21
Lessons Learned	
Finding the Evidence - Keith Swagler	
Layers of the OSI Model:	
Where the hardware and data fits	50
OSI Model Layers	51
Application layer	51
Presentation Layer	
Session Layer	53
Transport Layer	54
Network Layer	56
Data Link Layer	57
Physical layer	

Forensic Data Recovery	61
Capturing Evidence in a Forensically sound manner	61
What is Recoverable?	63
Chain of Custody	65
Write Blocking Labs	66
Data Destruction / Wiping	69
Forensic Imaging Labs	71
Data Carving Labs	78
EVIDENCE CHAIN OF CUSTODY TRACKING FORM	84
Introduction to Network Forensics	86
Prepping Wireshark	95
Wireshark Basics	97
Wireshark Data Taster for ARP Poisoning	107
Detection of ARP Poisoning	108
Detection of ARP Poisoning through Wireshark:	110
The Delicious Network Layer	114
Layer 3 – The Network Layer Explained	115
Taking a Bigger Bite With Wireshark	131
Windows Analysis	133
Analyzing Conversations	143
Analyzing traffic graphs	144
Analysing the Application Layer	151
Analyzing malware traffic through Wireshark	152
Analyzing a MODBUS DoS attack on SCADA	168
Analyzing the Trickbot Malware	175
Trickbot: The Beginning	177
Trickbot: Capabilities	177
Trickbot: Infection Vectors	178
Trickbot: Symptoms of Infection	179
How Trickbot works	179
Trickbot Targeting	
Walkthrough: Trickbot PCAP Analysis	
Trickbot PCAP Analysis – Scenario	
References	200

	Email Forensic Analysis	.202
	Email: OSI Perspective	.203
	Email Headers	204
	MIME Encoding	206
	Advantages of MIME	. 207
	Email Authentication	207
	Walkthrough: Email Header Analysis	.211
	Best Practices for Email Security	.218
	References	.219
	Kibana, ElasticSearch, and Logstash	. 220
	Visualizing your Data	. 220
	Creating Visualizations for the SIEM Dashboard	. 222
	Saving Visualizations	227
	View the Newly Created Visualization	228
	GeoIP Unique Count	229
	Top Network Traffic Generation	. 233
	Top Network Traffic Destination	. 237
	Sum of Bytes	242
	Building the Dashboard	. 247
	Saving the Dashboard	248
A١	NS Phishing - Layer 8	. 249
	The Individual	250
	Introduction	250
	Extended OSI Model	251
	Layer 8: Perspective and Use Cases	.252
	Layer 8: The OSINT Connection	.253
	Analysis: AWS Phishing Campaign	254
	CIR Contributors	257
	Information Warfare Center Publications	.258

# About the Authors



Jeremy Martin, CISSP-ISSAP/ISSMP LinkedIn.com/in/infosecwriter

A Security Researcher that has focused his work on Red Team penetration testing, Computer Forensics, and Cyber Warfare. Starting his career in 1995 Mr. Martin has worked with fortune 200 companies and Federal Government agencies, receiving a number of awards for service. He is also a qualified expert witness with cyber/digital forensics. He has been teaching classes such as the Advanced Ethical Hacking, Computer Forensics, Data Recovery, SCADA/ICS security, and Security Management since 2003. Most of his certification bootcamps follow DoD 8570.1m/8140 mandates.

As a security evangelist, his current research projects include OSINT, threat profiling, exploitation automation, anti-forensics, digital surveillance, and reverse engineering. This included the CSI Linux project, an investigation system originally built for Law Enforcement online /social media/dark web investigations.



#### **Richard Medlin**

LinkedIn.com/in/richard-medlin1

An Information Security researcher with 20 years of information security experience. I have written several articles and walkthroughs in the Cyber Intelligence Report and other publications. I enjoy teaching industry experts from many regions around the world how to investigate and minimize risks on their networks using Risk Management Framework. I am currently focused on writing about bug hunting, vulnerability research, exploitation, and digital forensic investigations. I am an author and one of the original developers on the first all-inclusive digital forensic investigations operating systems, CSI Linux. I primarily focus on red and blue team operations, and digital forensics.

I enjoy playing GUItar, bowling, working out, shooting pool, and spending time with my family. My dogs are like people to me, and I enjoy having them both nearby! I have had an extraordinarily strong interest in computing since I was 5 years old and taught myself how to use computers using MS-DOS and messing around with an original Macintosh machine. Computing has always been a part of my life, and I highly enjoy working with technology. Info Sec is the perfect field for me because it is what I genuinely love.



#### Nitin Sharma

LinkedIn.com/in/nitinsharma87

A cyber and cloud enthusiast who can help you in starting your Infosec journey and automating your manual security burden with his tech skillset and articles related to IT world. He found his first love, Linux while working on Embedded Systems during college projects. And met his second love, Python while programming for web automation tools and security.

As a Security Analyst, he has completed a couple of projects related to vulnerability remediation and management. Fascinated by emerging cloud providers like AWS, he has started his cloud journey and became a core member of AWS User Group Delhi NCR. He is still working around the AWS buzz and currently holding 4 AWS certifications including DevOps Professional and Security Specialty.

He has been writing articles and blogs since 2014. He specializes in writing content related to AWS Cloud, Linux, Python, Databases, Ansible, Cybersecurity, etc. He is also managing a GOOGLE-Adsense approved blog titled as "4hathacker.in". Apart from being a tech freak, Nitin enjoys staying fit and going to gym daily. He is a veg foodie and sing-a-lot crooner. Having an ice-calm persona and love for nature, he is looking for new challenges to uncover.



Justin Casey LinkedIn.com/in/justin-casey-80517415b

young but dedicated security professional who has spent the past number of years seizing each and every opportunity that has crossed his path in order to learn and progress within the industry, including extensive training in Physical, Cyber and Intelligence sectors. As an instructor & official representative of the European Security Academy (ESA) over the years Justin has been involved in the delivery of specialist training solutions for various international Law Enforcement, Military, and government units. He has led both covert surveillance and close protection operations as well as previously putting in the groundwork here in Ireland as a security operative for Celtic Security Solutions and working in Dublin as a trainer for the International Center for Security Excellence (ICSE).



#### LaShanda Edwards CECS-A, MSN, BS

LinkedIn.com/in/lashanda-edwards-cecs-a-msn-bs-221282140 facebook.com/AbstractionsPrintingandDesigns

As a Cyber Defense Infrastructure Support Specialist and a Freelance Graphic Artist, her background is not traditional but extensive. Capable of facing challenges head on, offering diverse experiences, and I am an agile learner. 11+ years of military service, as well as, healthcare experience. Also, freelance graphic artist for over 20 years. Recently graduated with a master's of Cybersecurity Technology degree, 3.8 GPA, offering a strong academic background in Cybersecurity. Swiftly to study and master new technologies; equally successful in both teams and self-directed setting; and skillful in a variety of computer systems, tools, and testing methodologies. Seeking to leverage my experience and passion towards cybersecurity. My goal is to obtain a challenging career within the cybersecurity career field with a leading company, healthcare facility, or the federal government as a Security Architect Cybersecurity and Technology Architecture, Information Systems Security Developer, Cybersecurity Analysis and Engineering, Board Advising, Security Control Assessor, Cybersecurity Consultant or Threat/Warning Analyst.



#### Mossaraf Zaman Khan

LinkedIn.com/in/mossaraf

Mossaraf is a Cyber Forensic Enthusiast. His areas of interest are Digital Forensics, Malware Analysis & Cyber Security. He is passionate and works hard to put his knowledge practically into the field of Cyber.

#### Ambadi MP





A Cyber Security Researcher and a non-IT Graduate primarily focused on Red Teaming and Penetration Testing. Experience within web application and network penetration testing and Vulnerability Assessment. Passion towards IT Industry led to choose career in IT Sector. Within one year of experience in Cyber Security got several achievements and Acknowledged by Top Reputed Companies and Governmental Organizations for reporting vulnerabilities.

# What is inside?

The Cyber Intelligence Report (CIR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threats, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

The CIR rotates between odd issues focusing on Blue Team / Defense and the even issues on Red Team / Offense.



InformationWarfareCenter.com/CIR



# **Evidence Everywhere**

Post 2000, almost everyone has some sort of digital footprint. If you have a cellphone and use Social Media, your footprint is a unique signature that identifies you as a person in many different databases. Most of the services you use are probably running analytics on your data for marketing, troubleshooting, or maybe even more nefarious reasons. The government is watching you because they can. If you are using smart devices, you are probably bleeding far more data than you realize. Your data (your digital self) is now a

commodity that is now considered the new gold. Data is everywhere... This means trace evidence is also everywhere.

What does this mean for you personally?

Big companies and governments are getting hacked daily. Facebook data gets leaked. Insert name here gets leaked... It is interesting to see how much sensitive data is being leaked. For about \$8 USD, you can download billions of username/email password combinations at Raidforums.com. Here is a link to their archived data: raidforums.com/Announcement-Database-Index-CLICK-ME. Please look at those databases. There is an exceptionally good chance YOU are in there. Not just your passwords, it also contains voter registration databases and more.

These are big organizations that spend a lot of money on IT and Security solutions to protect their data and they are still leaking data. Many of the hacking groups, especially state sponsored Advanced Persistent Threats, will go over the top and seem paranoid when communicating or accessing their data. However, it just takes one mistake to take down the entire security house of cards. There is a saying that goes: "the bad guy has to be lucky every single time and the investigator only has to be lucky once". Most people do not put forth the same due care and diligence into protecting their own systems and data at home. Some bad guys do not either and that is a very good thing for an investigation.

Now... To turn the tables, a lot of the tools and tactics the attackers employ are ESPECIALLY useful during cyber investigations. Think of it as two sides of the same coin. This goes without saying, DO NOT break the law... However, using the same methods the bad actors do can drastically increase your capability during the "anti-hack". As for using leaked data, it can help your investigation if you have access to it.

Open Source Intelligence (OSINT) can sometimes give you a ton of good information. Your network is a goldmine of transactional evidence and if you can get access to a device, there is more data than most people realize. Just remember to always make sure you are within your jurisdictional limitations and you have legal access to the data you are seeking.

Using tools like packet sniffers and protocol analyzers have always been a staple in network forensics. It is amazing how much data your systems are hemorrhaging. When investigating either a hacking incident or inappropriate use, there is trace evidence in many different areas that can help you "*break the case*".

Network traffic analysis can also help you identify devices that were previously unknown or accounted for. It is amazing how many times an organization just adds "things" to the environment without proper documentation. This makes managing security a daunting task and preventing risk near impossible at times.

# IOT Cyber Investigation Challenges

Cyber forensic investigations in the IoT space have come across a few speedbumps or challenges that have made the process more difficult than your average cases. These include but are not limited to:

- The increasing number of objects with evidence on them.
- Relevance of the devices for the investigation.
- Network boundaries that cross jurisdictions and ownership.
- Edgeless networks.
- Lack of properly documented devices.
- Small OS or Storage capability with limited access.
- Lack of firmware validation.

Now you must plan on what kind of evidence you can get from the suspect devices. Can you get a physical (bitstream) copy of the storage on the device? Can you only get a logical copy of the data? Do you have the tools and access to even get the data? Do you know where the devices are physically located? Do you even know of all the devices on the network? Who owns them? If the firmware is what you need to analyze, now you are going into the realm of Reverse Engineering.

Here are some smaller scoped IoT devices that are easier to identify, but also have their own challenges. Especially if they have an Internet connection.

- Smart car navigation systems (Hacked for full control)
- Drone or antonymous vehicles (Hacked video feeds and hijack control)
- RFID access control systems (Easy to Duplicate)
- CCTV Cameras (Hacked using IR and over networks)

Sometimes these hacks are only identified when they trip security sensors like the traditional IDS/IPS or when the organization does full traffic analysis through a SIEM.

With so many different devices and implementations of the devices, there is not a canned or off the shelf solution to cover every situation. Even mobile device forensics has this challenge, but not nearly at this scale. Sometimes you will need to contact the vendor to get the right tools or access for the job. The first step though is being able to identify all the devices that are relevant to the investigation. Only then can you move to the next step, acquisition.

This publication will describe cyber forensics and investigation methods that cross through the multiple layers of the OSI model ("OSI Cake").

# Dark Web Corner

### Dark Web Search Engines

**Ahmia:** searches hidden services on the Tor network. To access these hidden services, you need the Tor browser bundle. Abuse material is not allowed on Ahmia. See our service blacklist and report abuse material if you find it in the index. It will be removed as soon as possible.

Be careful with the RAW link!

Link: msydqstlz2kzerdg.onion Raw: msydqstlz2kzerdg.onion/address

**Candle:** Tor Search is a "Google" like search engine that crawls Tor sites.

Link: gjobqjj7wyczbqie.onion

**TORCH:** "Tor Search is a very efficient crawler and search engine which is 24 hour indexing new contents from the TOR network. It serves over 80,000 search requests every day from TOR users looking for content in TOR network and it is referred by hundreds of sites within TOR and on the clear web."

Link: xmh57jrzrnw6insl.onion

Below is a list of secure communications methods using Tor Onion network. Just remember, you can only access these if you are going through the Tor network



ProtonMail is a Swiss encrypted email service. They use end-to-end encryption and don't keep any logs. Moreover, you do not need personal information to create an account.

#### protonirockerxow.onion



"SecureDrop is an open

source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources. It was originally created by the late Aaron Swartz and is now managed by Freedom of the Press Foundation. SecureDrop is available in 20 languages."

Notable SecureDrop links

2600: lxa4rh3xy2s7cvfy.onion Reuters: smb7p276iht3i2fj.onion



### secrdrop5wyphb5x.onion

SecMail has become one of the most used dark web email providers. "We won't ask you for your name, address or any personal data. We are using the safest security protocols, so you don't have to worry about nothing."

secmailw453j7piv.onion



# Dark Markets

A Dark Market or "cryptomarket is a commercial website on the web that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the sale of legal products." - wikipedia.org





White House Market is a market with a high level of security and anonymity while maintaining a simple user interface.

### I2P Address: eeej5nynwa5pe4slg6ny66l2rck37m2rtaglair53cff56xmssaq.b32.i2p Tor Address: auzbdiguv5qtp37xoma3n4xfch62duxtdiu4cfrrwbxgckipd4aktxid.onion



**Monopoly Market**: a direct deal, walletless, userless, XMR exclusive, drug-focused, marketplace aimed to provide a portfolio of well-vetted vendors for reliable, safe trading. Over the course of the past few months, we have built Monopoly from the ground up while taking keynotes from comments made on Dread, especially within /d/DarkNetMarkets.

### Tor Address:

- monopolyberbucxu.onion
- 2lbcyr5kftntuvfbd22h3ayxtrvzymk5vzcc54oj3qc62xuvcefqtlid.onion



**Recon** is the largest Dark Net Market vendor archive service and multi marketplace search engine, providing up to date content from the majority of established markets all in one place. We strive to serve a fast and easy

to use platform allowing you to cross reference vendor details, listings, statistics and marketplace addresses.

Tor Address: reconponydonugup.onion

Fun Facts	
-----------	--

65%

"Bitcoin Activity on the Dark Web Grew by 65% first Quarter" -Crvstal Blockchain Analytics

# Dark Market Busts

This section showcases recent busts made on the Dark Web within the Dark Market Communities. This ranges from buyers to sellers to admins of these websites.

The information is taken from several online resources including, but not limited to



### reddit.com/r/DNMBusts

Law enforcement got access to all customer info of anyone who dealt with:

"'Xanax King' arrested again for alleged dark web drug manufacturing scheme based out of Concord warehouse

Jeremy Donagal had previously been charged with selling pills designed to look like Xanax" - mercurynews.com

"Pharmacist Arrested in Plot to Firebomb a Rival to Sell More Drugs on the Dark Web. Hyrum T. Wilson of Auburn, Neb., conspired with a drug dealer to rob, then destroy a competitor's pharmacy, according to federal prosecutors." - nytimes.com "Empire Vendor NeverPressedRX Arrested by the FBI

A Maryland man accused of running the "NeverPressedRX" vendor account on Empire market was arrested for unlawful distribution of medications and money laundering. NeverPressedRX sold a variety of prescription medications on marketplaces as well as through Wickr." - darknetlive.com

"An 18-year-old man from Lindisfarne has been arrested and charged with trafficking in a controlled drug following an operation focused on the mail corridor into Tasmania.

The work of dedicated detectives resulted in the seizure of approximately \$100,000 worth of controlled drugs" - police.tas.gov.au

# Tech Giants help Law Enforcement: Exploit Those That Exploit Children

Facebook recently hit the news when they paid a security research firm to exploit the popular Tor live bootable workstation called The Amnesic Incognito Live System or Tails (htttails.boum.org). "The FBI and Facebook used a so-called zero-day exploit in the privacy-focused operating system Tails, which automatically routes all of a user's internet traffic through the Tor anonymity network, to unmask Hernandez's real IP address, which ultimately led to his arrest." -vice.com

"Tails is a complete operating system designed to be used from a DVD, USB stick, or SD card independently of the computer's original operating system. It is free software and based on Debian GNU/Linux. Tails comes with several built-in applications pre-configured with security in mind: a web browser, an instant messaging client, an email client, an office suite, an image and sound editor, etc." - torproject.org

This is not the first time that big tech has helped Law Enforcement track down pedophiles and it will not be the last. Companies like Google, Microsoft, and others use algorithms to monitor uploads and downloads of material that contain possible child pornography. When detected, they review the data and contact The National Center for Missing and Exploited Children, known as NCMEC and send the sample image along with information about the digital fingerprints of the traffic source and destination.

This is also not the first time that exploits have been used to deanonymize people on Dark Web networks. On August 4, 2013: "all the sites hosted by Freedom Hosting – some with no connection to child porn – began serving an error message with hidden code embedded in the page. Security researchers dissected the code and found it exploited a security hole in Firefox to identify users of the Tor Browser Bundle, reporting back to a mysterious server in Northern Virginia." – wired.com

The FBI also used a project codenamed called Torpedo that targeted Pedophiles on the Tor network. "Operation Torpedo was a 2011 operation in which the FBI compromised three different hidden services hosting child pornography, which would then target anyone who happened to access them using a network investigative technique (NIT)." -wikipedia The use of the project was said by a judge to be "crossing the line". However, in the case of Gabriel Werdene, 53, of Bucks County, Philadelphia serving two years in a federal prison for rummaging through the Playpen dark-web filth souk for images and footage of child sexual abuse, the judge said that the line was crossed in "good faith".

Not all people that use Tor, I2P, Freenet, and all the other Dark Web networks are criminals, terrorists, and evil people. With that said, there are a lot of bad guys that do. Always be careful where you go and what you do. So, who use it for legitimate purposes? Well, let's list a few:

- Activists
- Businesses
- Intelligence Officers
- Journalists and News Agencies
- Law Enforcement
- Political Dissidents
- Security Researchers

"Keep in mind that only activities you do inside of Tor Browser itself will be anonymized. Having Tor Browser installed on your computer does not make things you do on the same computer using other software (such as your regular web browser) anonymous." – ssd.eff.org

This comes down to a level of effort issue. How anonymous do you want? If you are investigating a small-time drug dealer on a dark market, your name is probably going to be added to the public court records. If you are a political dissident and are afraid your family may be executed for your crimes, you need to take a few more steps.

Keep this in mind when investigating a suspect or target websites. This is all about Operational Security or OPSEC. The running joke with Law Enforcement is that the bad guy must be lucky EVERY SINGLE TIME and you only must be lucky once. Now, from the darkest of places, I do know of officers investigating some wretched guys (Cartels and Terrorists) getting murdered because they did not follow basic OPSEC procedures. Know the risk and protect yourself accordingly.

You also need to be on the same network as the suspect if you plan to access their open resources. This is where the technical knowledge kicks in. You need to understand the mechanics of how network traffic works.

### **Tor Resources:**

#### Tor must be installed...

"Just like Tor users, the developers, researchers, and founders who've made Tor possible are a diverse group of people. But all of the people who have been involved in Tor are united by a common belief: internet users should have private access to an uncensored web."

• Tor Project

### Local proxies

- <u>Corridor</u>
- Privoxy
- Proxychains
- Torsocks

### Tor Network Gateway

These are systems that you can run to send traffic through.

- CSI Linux
- Whonix Gateway

### **Tor Workstations**

- CSI Linux
- Tails
- Whonix Workstation \*

### Multi-layer Environment

- CSI Linux
- Qubes OS

# #BlueLeak

In June 19, 2020, the user @DDoSecrets posted on Twitter that they released a 269



Gb leak of 10 years' worth of Law Enforcement data. When you follow their link, it does take some time to load the page. After a few minutes, it comes up with what you see in the graphic below. Further investigation shows that a large bulk of this data is already public information. This seems to be more of a political statement for a news clip than an actual leak of sensitive investigation and other sensitive data. However, when everything is on one easy to search database, useful data may still be parsed from it. Intelligence is all about seeing patterns and trying to predict future behavior.

With this said, here is another tweet from @DDoSecrets: "#BlueLeaks provides unique insights into law enforcement and a wide array of government activities, including thousands of documents mentioning #COVID19". This was taken down by both Twitter and Archive.org, but can be found on BitTorrent sites.

÷ → C	hunter.ddosecrets.com/datasets/102					ବ 🕁 🛃 🔸	۵ 🕷
🔹 📑 Blue	Leaks 🔹 🔍 Search in BlueLeaks	0				🛢 Datasets	→] Sign in
🗮 Leaks 🗇 📲	BlueLeaks						
		hi Overview 🗈 Documents	i 1m (8) People 29	2 💥 Cross-reference			
Leaks							
BlueLeak	S	10		25	4	1	
en years of dat	a from over 200 police departments, fusion	15		234	+	Im	
enters, and oth	er law enforcement training and support	≣≣ Тур	25	() Count	ries	🖽 Names	
esources, court	esy of Anonymous.						
		🖂 Images	564,701	United States	70,481	Netsential.com Inc	58,714
		Documents	291,672	Seychelles	4,265	All Rights Reserved	45,591
		III Tables	167,319	Mexico	3,372	AGENCY / CASE	14,015
ublisher	Distributed Denial of Secrets	🗒 Web pages	102,445	Honduras	1,785	D.L. State Male Female DriverPass	enger 13,690
CALCULATION .		Text files	28,594	Canada	1,520	First DOB:(mm/dd	13,420
rata UKL	e data.ddosecrets.com	E Folders	15,751	Guatemala	976	Cross Streets	12,197
4anager	O Mxyzptik	🗊 Files	4,936	Ireland	971	Permission to Disseminate Basic In	form 11.771
Jountry	United States	Packages	4,665	France	948	St. Louis Intelligence Project Incid	ent In., 11,348
	06/10/2020	Workbooks	1,468	Syria	857	Car Clouting	10.524
an apadrea	00/15/2020	Videos	1,468	China	844	MIAC Intel	10,140
oreign ID	06cfa50d113b412a8f3e514fe53ace60	(8) People	292	Jamaica	822	Badge Number	10,089
		E-Mails	167	Jordan	776	Law Enforcement Partners	9,248
econclustion	https://hunter.ddosecrets.com/api/2/c 📋	<ul> <li>Audio files</li> </ul>	101	Colombia	775	Tab View List	9,078
	Match your own data against the entities in this			El Salvador	772	Session("nonce")="nonce=" & no	inceval 8,136
	collection using the free OpenRefine tool by adding			Iraq	685	XING CASE AGENT / POINT OF CO	ONTAC., 7,669
is://hunter.ddc	secrets.com/search?filter.collection_id=102&filters	countri		Show more		Show more	

Here is the original link:hunter.ddosecrets.com/datasets/102

The user Emma Best/@the\_mike\_best also uploaded the leak to Archive.org: archive.org/details/BlueLeaks The torrent file has a lot of individual files and doesn't work with all BitTorrent programs like uTorrent. It does however work with Transmission on Linux.

		* 6
Public Domain Mark 1 D 🛞 🌀 pulice nationalsecuttyarchive; adoitional_collections	0 Views	
Englise	DOWNLOAD OPTIONS	
	TORRENT	1 /1
2520-08-20 00.22.28 BlueLesks	SHOW ALL	0 File 5 Origini
	Public Domain Mark 1.0 @ puice nationalecultyarchive, additional, collections English ng modifiedrypated by the tasic detive 2020-68-20.00.22.28 State tasis State tasis	Public Domain Mark 1 D @ puice puice nationalecultyarchive, additional_collections English rg modifiedspated by the task: derive 2020-06-20 00 22-28 BULIE entis BULIE entis

# CSI Linux The Evolving Forensic Investigation Environment



This project started about a year ago when several of the environments we commonly used were either going in different directions than we were wanting, or support stopped when the project hit its end of life. The original purpose was to have a Linux environment that could be used for Online, Social Media, and Dark Web investigations. We took a lot of the base inspiration from the amazing work from Michael Bazzell's Buscador at Intel Techniques. We switched out some tools, added some more, and thought, why not make this an all in one environment? Then, the project exploded.

The first revisions of the environment became 3 separate operating systems that would work together or work separately. It was designed this way to make it as simple as possible to run right out of the box with little Linux and networking experience. We used the same idea some had with using Buscador with Whonix and by version 2020.2, created our own Tor gateway to replace Whonix. Our SIEM was a stand-alone system that was set to replace the Security Onion. Everything was built for virtual machines to run on top of a secured system to give layers of protection. Some people wanted to be able to run the Analyst on a single system as their main OS. This was not an option if you wanted to use the Tor gateway unless you built a physical network infrastructure.

Things are evolving. In this latest version, we have combined all three into one bootable distribution. This means that you can run it from an internal/external hard drive or push it into any Virtual Environment you want. The Tor gateway no longer runs similarly to Whonix but uses similar methods to tunnel as the Tails Tor based distribution. Like the previous versions, this allows you to turn on a level of security and anonymity if needed but can be turned off if that is not your primary goal. The Tor is still running when in Surface Web mode, but ALL traffic is not protected, just what you want. If you decide to run in in a virtual environment, you can add Whonix to the mix and force your traffic through up to three layers of Tor, akin to how some use Qubes-OS. It is now up to you how far you want to go.

whonix.org tails.boum.org qubes-os.org The SIEM is now in a Docker, still stand alone, and can be integrated into the Analyst. This allows us to rename the Analyst to just CSI Linux, as was originally indented. The SIEM has been given some steroids... Amazon ics protocols, ClamAV, Cyber chef, Elastalert, geolite2, Mitre cyber analytics, Moloch, Nginx for https

reverse proxying, and more... With the extra power, it means that it will need more resources. A minimum of 6 GB Ram is needed for CSI Linux or 12 GB Ram for CSI Linux to run the SEIM on top to run comfortably.

With the Gateway being merged with Analyst, the "sub" distros will be SIEM and Acquisition. Acquisition will be a bootable distro built for imaging and evidence capture. Acquisition is planned for release in the next month.

So, what does all of this mean?

Well, CSI Linux can be booted off an internal/external drive or within a Virtual MAchine since it no longer requires the use of an external Tor gateway. If you would like to run it the traditional way, you absolutely can run CSI Linux through Whonix. You can Even Tor gateway through the Whonix Tor Gateway for an added layer of security. You can decide not to install the SIEM on CSI Linux, run it on a completely different system, or not at all. There are many configuration options now available. You can make it as simple or as complicate as you want.

We have also added a Bug Tracker website http://tracker.csilinux.com to help for future development. We are also in the process of creating a training site as well.

Now to highlight some of the additions to the base CSI Linux system.

- \* CSI Linux updater
- \* Tools updated
- \* More GUI options for the CSI Tools
- \* Updated CSI Tools
- \* SIGINT Tools added
- \* More OSINT resources
- \* More computer forensics tools added

This is update is a major update with many of the mechanics fundamentally changed. Thank you to all of those that have helped build the distribution with the countless hours spent and all of the suggestions from the users. This has been a great project and the ever evolving product of the labor is amazing to watch.

If you have any suggestions on making CSI Linux better, whether it be tools, methods, resources, or engineering ideas, pleas let us know.

# CSI Linux Forensic Challenge 204

This Capture the Flag (CTF) can be done anywhere since it is a downloadable image. We are using one of the prebuilt cases from CFREDS.NIST.GOV.

**Download:** cfreds.nist.gov/dfrws/Rhino\_Hunt.html

The Challenge... Using whatever tool of your choice. Identify the flags, write a report, and write a walk through on how you found each item. The findings and final report will then be graded, with the best combo being the winner. Make sure that the report and the walkthrough are two separate documents.

Winner will have their report and walkthrough showcased in a future issue of the Cyber Intelligence Report (CIR) and win a commemorative Bitcoin challenge coin (Not a real Bitcoin). Submit reports to CTF@informationwarfarecenter.com.

### Scenario:

The city of New Orleans passed a law in 2004 making possession of nine or more unique rhino images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal Evidence in the case includes a rhino traffic. computer and USB key seized from one of the University's labs. Unfortunately, the computer had no hard drive. The USB key was imaged and a copy of the dd image is on the CD-ROM you have been given. In addition to the USB key drive image, three network traces are also available—these were provided by the network administrator and involve the machine with the missing hard drive. The suspect is the primary user of this machine, who has been pursuing his Ph.D. at the University since 1972.



### CTF TARGET DETAILS

rhino.log

c0d0093eb1664cd7b73f3a5225 ae3f30 rhino2.log cd21eaf4acfb50f71ffff857d7968 341 rhino3.log 7e29f9d67346df25faaf18efcd95f c30 RHINOUSB.dd 80348c58eec4c328ef1f7709adc 56a54

### CSI Linux:

• <u>CSILinux.com</u>

### Additional Resources:

- Wireshark
- Autopsy

The Rhino Hunt data set requires examination of a small image file and three network traces.

Deadline: December 15th

### The task:

Recover at least nine rhino pictures from the available evidence and include them in a brief report. In your report, provide answers to as many of the following questions as possible:

- Who gave the accused a telnet/ftp account?
- What is the username/password for the account?
- What relevant file transfers appear in the network traces?
- What happened to the hard drive in the computer? Where is it now?
- What happened to the USB key?
- What is recoverable from the dd image of the USB key?
- Is there any evidence that connects the USB key and the network traces? If so, what?

*Remember: Score is based off the quality of the report and walkthrough.* 

To receive full credit, use CSI Linux as your base investigation system. You can add more tools on top, but make sure to document what you have added in your walkthrough and step by step actions for gathering the evidence.



# CSI Linux Forensic Challenge 201

# \* Winner: Apostolos Gkletos

### \* Honorable Mention Keith Swagler

# The Challenge

Using CSI Linux and the tools included, go through this forensic project, and identify all the flags you can. Use Autopsy as your main application. Write a walk through on how you found each item within Autopsy and any other tools within your final report. The findings and final report will then be graded, with the best combo being the winner.

### You can try the challenge yourself: www.cfreds.nist.gov/Hacking\_Case.html

#### CYBER INTELLIGENCE REPORT | Issue 2020.1 JANUARY

#### CSI Linux Forensic Challenge

Using CSI Linux and the tools included, go through this forensic project and identify all the flags you can. Use Autopsy as your main application. Write a walk through on how you found each item within Autopsy and any other tools within your final report. The findings and final report will then be graded, with the best combo being the winner.

Winner will have their report and walkthrough showcased in a future issue of the Cyber Intelligence Report (CIR) and win a commemorative Bitcoin challenge coin (Not a real Bitcoin). Submit reports to <u>csilinux@informationwarfarecenter.com</u>. **Deadline is June 15<sup>th</sup>, 2020!** 

Here is the Autopsy user manual: <a href="https://sleuthkit.org/autopsy/docs/user-docs/4.0/">https://sleuthkit.org/autopsy/docs/user-docs/4.0/</a> Sign up here: <a href="https://comms.informationwarfarecenter.com/?p=subscribe&id=4">https://sleuthkit.org/autopsy/docs/user-docs/4.0/</a> Sign up here: <a href="https://sleuthkit.org/autopsy/docs/user-docs/4.0/">https://sleuthkit.org/autopsy/docs/user-docs/4.0/</a> Sign up here: <a href="https://sleuthkit.org/autopsy/docs/user-docs/4.0/">https://sleuthkit.org/autopsy/docs/user-docs/4.0/</a>

#### Hacking Case (https://www.cfreds.nist.gov/Hacking Case.html)

This test image requires a variety of skills to answer the given questions.

#### Scenario

On 09/20/04, a Dell CPi notebook computer, serial #VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. Was used to instanting purposes, antrodge real and be end of anaking suspect, ended a set of a real signs are just to prevent web crawlers from indexing this name; there are no equal signs in the image files.) Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to the to the suspect, G=r=e=g S=c=h=a=r=d=t.

### A DD image (in seven parts: 1, 2, 3, 4, 5, 6, 7, 8, and notes) and a EnCase image (second part) of the abandoned computer have already been made.

- What is the image hash? Does the acquisition and verification hash match?
- What operating system was used on the computer? When was the install date?
- What is the timezone settings? Δ 5 Who is the registered owner?
- What is the computer account name?
- What is the primary domain name?
- When was the last recorded computer shutdown date/time?
- How many accounts are recorded (total number)?
- 10. What is the account name of the user who mostly uses the computer?

#### CYBER INTELLIGENCE REPORT | Issue 2020.1 JANUARY

- 11.Who was the last user to logon to the computer?
- 12.A search for the name of "G=r=e=g S=c=h=a=r=d=t" reveals multiple hits. One of these proves that G=r=e=g S=c=h=a=r=d=t is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?
- 13. List the network cards used by this computer
- This same file reports the IP address and MAC address of the computer. What are they
- 15.An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and setup for LOOK@LAN?
- 16. Find 6 installed programs that may be used for hacking. 17. What is the SMTP email address for Mr. Evil? 18. What is the NNTP (news server) settings for Mr. Evil?

- 19. What two installed programs show this information? 20. List 5 newsgroups that Mr. Evil has subscribed to.
- 21.A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?
- 22. This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.
- 23 Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?
- 24. Viewing the file in a text format reveals much information about who and what was intercepted What type of wireless computer was the victim (person who had his internet surfing recorded) using?
- 25. What websites was the victim accessing?
- 26. Search for the main user's web-based email address. What is it? 27. Yahoo mail, a popular web-based email service, saves copies of the email under what file name?
- 28. How many executable files are in the recycle bin?
- 29. Are these files really deleted?
- 30. How many files are reported to be deleted by the file system?
- 31.Perform an Anti-Virus check. Are there any viruses on the computer?

- · Download the DD/Raw images
- Start a case within Autops Use other tools within CSI Linux as needed.
- Document everything.
- · Walk through with screenshots including the third-party modules you've added
- Complete a Chain of Custody (Use the attached form below).
- Complete a final report Profit!

17

# CTF 201 Chain of Custody

# **SUBMITTER:** PLEASE COMPLETE SECTIONS 1 AND 2 AND SIGN/DATE ON SUBMITTER LINE OF SECTION 4. DOCUMENT ALL SUBSEQUENT EVIDENCE TRANSFERS IN SECTION 4.

#### **SECTION 1**

INVESTIGATOR NAME: Apostolos Gkletos		DATE SU	BMITTED: 01/01/2020
AGENCY: INFORMATION WARFARE CENTER		AGENCY CASE NO.: 01072020-SHARDT	
ADDRESS:			
Athens Greece	STATE: At	tiki	ZIP CODE: ******
PHONE NO.:	E-MAIL: g	klapost	olos@gmail.com
EMERGENCY CONTACT:	PHONE NO	D.:	

#### **SECTION 2**

Sampling Site: CSI Linux Forensics Challen	ge	Site Address: csilinux.com
Collected By: NIST	Date Collected: 01/01/2020	Agency: Information warfare center
SUBMITTER DESCRIPTION: INCLUDE THE DESCRIPTION OF EACH SAMPLE SUBMITTE	NUMBER OF CONTA	AINERS, IDENTIFICATION NUMBER(S) AND A PHYSICAL
The image of a laptop was taken by NIST.	gov.	
They have submitted via the website <u>www.</u> original hardware. There are two different images contain a forensic copy of the same	<u>cfreds.nist.gov/Hac</u> image formats inclu e drive.	cking Case html for review. We do not have access to the uding a split DD image and an EnCase .E01 format. Both
SUBMITTER COMMENTS:		
When trying to download	the images	initially I have the option to save
them as txt which is solve	d by cance	lling the action and resuming the
downloading action which	saves ther	n to their original type.

Laboratory Description of Sample: Include the num description of each item submitted for testing.	ber of containers, identification number(s) and a physical
	and the
SIGNATURE:	DATE:

#### **SECTION 4**

**Chain of Custody:** Persons relinquishing and receiving evidence must provide their signature, organization and date/time to document evidence transfers.

Submitter Signature: IWC Signature			Ager	cy: INF	ORMATION WARFARE	Date: 01/01/2	Date: 01/01/2020	
	1	CENTER		TER	ž.			
Received by	Organization	Date/	Time		Relinguished by	Organization	Date/Time	
<sup>1.</sup> Apostolos Gkletos	IWC	14/06/	2020	2.		ι.		
Received by	Organization	Date/	Time		Relinquished by	Organization	Date/Time	
3.				4.		÷		
Received by	Organization	Date/	Time		Relinquished by	Organization	Date/Time	
5.				6.				
Received by	Organization	Date/	Time		Relinquished by	Organization	Date/Time	
7.				8.		<b>.</b>		
Received by	Organization	Date/	Time		Relinquished by	Organization	Date/Time	
9.				10.				

#### SECTION 5 – EVIDENCE DISPOSAL (TO BE COMPLETED BY LABORATORY EVIDENCE CUSTODIAN)

Disposition Site:	Destruction No.:	Method of Destruction/Date:
e Almanies		
Performed by:		Date:
Witnessed by:		Date:

#### **SECTION 6**

Supplemental Information (i.e. sample description comments other)	

# Case Challenge - Apostolos Gkletos

On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

### Solution

For investigation purposes a DD image and an EnCase image were acquired from the laptop found and CSI Linux tools were used to analyze these images. The procedure that was followed is described below supported by screenshots where needed.

### **Requirements Section**

Section #1

- Requirement 1
  - $\circ$  A laptop with at least 8 Gb of Ram, 16Gb recommended
- Requirement 2
  - Latest edition of Virtual Box installed along with its additions
- Requirement 3
  - $\circ$  Hard disk with at least 80 Gb of free space, recommended 100 Gb at least
- Requirement 4
  - CSI Linux .ova file

Section #2:

- Requirement 1
  - Autopsy NSRL hash sets
- Requirement 2
  - Case DD, EnCase images

### CSI Linux Challenge Answers

**1.** What is the image hash? Does the acquisition and verification hash match? The image hash is:



Device ID:	e81a7a7b-f207-45cf-9adb-a1a005c35338
Usage:	OS Drive (Microsoft Windows XP)
OS:	Microsoft Windows XP
Time Zone:	Etc/GMT-5
Acquisition Details:	Description: Dell Latitude CPI
	Case Number: Greg Schardt
	Evidence Number: 1 of 1
	Examiner Name: Shane Robinson
	Notes: sn # VLQLW hdsn # RQQF7429
	Acquired Date: Wed Sep 22 19:06:04 2004
	System Date: Wed Sep 22 19:06:04 2004
	Acquiry Operating System: Windows XP
	Acquiry Software Version: 4.19a
Image Type:	E01
Size:	4 87 GB (4871301120 bytes)
Unallocated Space:	4.92 GB (4924159519 bytes)
Sector Size:	512 hytes
MD5:	aee4fcd9301c03b3b054623ca261959a
File Paths:	C:\Users\gkl_a\OneDrive\Desktop\CSI case\4Dell Latitude CPi.E01
	C:\Users\gkl_a\OneDrive\Desktop\CSI case\4Dell Latitude CPi.E02

aee4fcd9301c03b3b054623ca261959a. Yes, they are the same.

Picture 1:Acquisition and verification hash match

Picture 2:Image MD5

2. What operating system was used on the computer? On the system the software that was used is **Microsoft Windows XP**.

Add Data Source 🛅 Images Alideos 💹 Communications 🧿 Geolo	cation 🗮 Timeline 🗍 Ele D	isroverv	Ger	nerate Report	te Cate						0
		iscovely	00		/se case				() · )	eyword Lists	Ce Keyword Search
< ⇒	C Listing										+ > •
4Del Latitude CPi.E01	Operating System I	nformation									2 Re
🕀 🖶 Data Source Files	Table Thumbhail										
Uiews											Save Table as CS
🕀 🖧 File Types	Source File	s	c 0	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Path
Zeleted Files		-		N LACODAY TRY & O	C G I I G G I I	Illadaus MT		Of Cushen De abor LTCAD	anali abarda chi nor		
MB File Size	system	×		W-THAODINOTOKALÓ		WINDOWS_N1	200	%SystemR00t%(TEMP	4Dell Lautobe CPI.201		
🖨 🌆 Results	Software .								4Dell Latitude CPI.ED1	Microsoft Windows >	P C:\WINDOWS
Extracted Content											
📄 Extension Mismatch Detected (773)											
- 🚝 Operating System Information (2)											
Recent Documents (8)											
🥂 Shel Bags (51)											
USB Device Attached (1)											
- 🖉 Web Bookmarks (6)											
Web Cookies (24)	<										
Web History (887)	Land Land Land				Dec des 1						
Web Search (4)	Hex Text Appli	cation Me	ssage   F	File Metadata Context	Results A	nnotations Othe	er Occurrences Video Tria	ge			
E Keyword Hits	Result: 1 of	275	Re	sult 🗧 🏓						Operat	ing System Informat
Single Literal Keyword Search (0)	-										
Single Regular Expression Search (0)	Type	Value								S	ource(s)
E G Empl Addresses (22542)	Program Name	Micro	oft Wind	lows XP						Re	cent Activity
Email Addresses (22642)	Path	C:\W	NDOWS							Re	cent Activity
B G Dhama Numbers (1504)	Product ID	5527	F-640-014	47306-23684						Re	cent Activity
(1) Phone Numbers (1594)	Owner	Greg	Schardt							Re	cent Activity
Hadvast Lite	Organization	N/A								Re	cent Activity
E Mai Marcanar	Source File Path	/img_	4Dell Lati	tude CPi.E01/vol_vol2/V	VINDOWS/sy	stem32/config/so	ftware				
Default (Default)	Artifact ID	-9223	3720368	54766395							
Toteresting Tems											
Describe Zin Bowh (1)											
Previously Seen Devices (Central Repository) (1)											
Previously Tagged As Notable (Central Repository) (1)											
Accounts											
Email											
🕀 💭 Credit Card											
Credit Card     Tags											
Credit Card     Tags     SCHARDT.001											

Picture 3:Software used

- **3.** When was the install date? 0x41252e3b (1092955707)
  - a. GMT: Thursday, August 19, 2004 10:48:27 PM

- 4. What is the timezone settings? Etc/GMT-5 as it is shown in picture 1
- 5. Who is the registered owner? The registered owner is **Greg Schardt**.

Data Source 📠 Images/Videos 🔣 Com	munications 💡 Geolocati	an 🧮 Tim	sine 🌡	File Discovery	Generate Re	port 💊 Close	Case			<b>E</b>	•••	Keyword Lists	Qr Keyword Search
	O Listing												< ) <b>-</b>
	Operating Syste	n Information											4 Res
a sources	Table Thumb	vail											
SCHARDT.001													Save Table as CS
NS	Source File	s	c 0	Name	Domain	Version	Processor Architecture	Temporary Elec Directory	Data Source	Program Nam		Path	Product ID
File Types	and the states	-		H LADODAN TAKE O	Company	Mindeme MT	-necessor Architecture	N Further Dealth (TEMP)	SCHADDT 001	riogramman	~	1001	riodoce to
Deleted Files	e system	v		N-1WAODU057/K4EG		WINDOWS_NT	X00	765950ettik00c76(1Ehte	SCHARD1.001				
File Size	a software								SCHARDT.001	Microsoft Win	idows XP	C:/WINDOWS	55274-640-0147306-23
ults	E system	V		N-1A9ODN6ZXK4LQ		Windows_NT	×86	%5ystemRoot%\TEMP	4Dell Latitude CPI.E01				
Extracted Content	🗔 software								4Dell Latitude CPi.E01	Microsoft Win		C:\WINDOWS	55274-640-0147306-23
Web Search (8) Web Search (8)	<	of 275	ssage   Re	File Metadata Context	Results A	Annotations Oth	er Occurrences Video Tria	ge				0	perating System Informat
Web Bookmarks (12) Web Cookies (48) Web History (1774) Web Search (8) Keyword Hiss Single Literal Keyword Search (0)	<	of 275	nsage Re Valu	File Metadata Context sult 🍝 🌛	Results A	Annotations Oth	er Occurrences Video Tria	0e.				O	perating System Informati re(s)
Web Bookmarks (12) Web Cookers (12) Web Cookers (48) Web Search (8) Web Search (8) Keyword His Single Regular Expression Search (0) Single Regular Expression Search (0)	K Hex Text A Result: 1 Type Program Name	of 275	ssage Re Valu Micro	File Metadata Context suit 🔄 🌛 e soft Windows XP	Results A	Annotations Oth	er Occurrences   Video Tria	ge				O Sourc Recen	perating System Informati re(s) It Activity
Web Bolkmarks (12) Web Bolkmarks (12) Web Coolsec (46) Web History (1774) Web Search (6) Keyword Hits Single Literal Keyword Search (0) Single Regular Expression Search (0) CSI Challenge (868)	K Hex Text A Result: 1 Type Program Name Path	of 275	NSAGE Re Valu Micro C:\W	File Metadata Context sult ( )	Results A	Annotations Oth	er Occurrences   Video Tria	0F				O Source Recen	iperating System Informati te(s) it Activity it Activity
Doab Derive Filadole (c)           Web Bookmiss (12)           Web Dookmiss (12)           Web Dookmiss (12)           Web Holsmiss (12)           Single Littlera Keyword Search (0)           Single Littlera Keyword Search (0)           CSL Ohlenge (68)           Backforeact (10123)	K Text A Result: 1 Type Program Name Path Product ID	of 275	Nisage Re Valu Micro C:\W 5527	File Metadata Context sult A and A a	Results A	Annotations Oth	er Occurrences   Video Tria	oe.				O Sourc Recen Recen	perating System Informati re(s) It Activity It Activity It Activity
Web Sokmins (12)           Web Sokmins (12)           Web Sokmins (12)           Web Sokmins (12)           Web Search (1774)           Web Search (1774)           Web Search (1774)           Single Litteral Keyword Search (10)           Single Regular Expression Search (10)           CSI Challenge (868)           Email Addresses (22642)           P. Addresses (10674)           Ehoon Number (1784)	K Text A Result: 1 Type Program Name Path Product ID Owner	of 275	Value Micro C:\W S527 Greg	File Metadata Context sult  sult  soft Windows XP TMOOWS 4-640-0147306-23684 Schardt	Results A	Annotations Oth	er Occurrences   Video Tria	je				O Sourc Recen Recen Recen Recen	perating System Informati re(s) it Activity it Activity it Activity it Activity
Usa Userka Fikadular (J)           Web Solmins (IZ)           Web Solmins (IZ)           Web Solmins (IZ)           Web History (IZ74)           Single Regular Expression Search (ID)           Single Regular Expression Search (ID)           CSI Challenge (685)           Email Addresse (IZ542)           JP Addresse (ID574)           VIDEs (1994)           VIDEs (946)	K Hex Text A Result 1 Type Program Name Path Product ID Owner Crganization	of 275	Value Micro C:\W 5527 Greg N/A	File Metadata Context sult  sult  soft Windows XP INDOWS 4640-0147306-23684 Schardt	Results A	Annotations Oth	er Occurrences   Video Tria	96				O Sourc Recen Recen Recen Recen Recen	perating System Informati re(s) it Activity it Activity it Activity it Activity it Activity
Doal Derive Fillad Del (J)           Web Bookmins (12)           Web Dookmins (12)           Web Dookmins (12)           Web Holsmins (12)           Single Littlera Keyword Search (0)           Single Littlera Keyword Search (0)           CSL Ohlenge (68)           Email Addresses (12544)           IP Addresses (12674)           UBL (39946)           Hadnet His	Kesult: 1           Hex:         Text:         A           Result:         1           Type         Program Name           Path         Product ID           Owner         Organization           Source File Path         Source File Path	of 275	Value Nalue Micro C:\W 5527 Greg N/A /img_	File Metadata Context sult ( ) ( ) soft Windows XP INDOWS 4-640-0147306-23684 Schardt 4Del Latitude CPi.E01/A	Results A	Innotations Other	er Occurrences   Video Tria	oe				O Sourc Recen Recen Recen Recen	perating System Informat :e(s) it Activity it Activity it Activity it Activity it Activity
Web Solkmins (12)           Single Literal Keyword Search (0)           Cst Challenge (868)           Email Addresses (22642)           Phone Numbers (1794)           Phone Numbers (1794)           Hills (38946)           Heald Messages	Kesuff 1 Hex Text A Result: 1 Type Program Name Path Product ID Owner Organization Source File Path Artifact ID	of 275	Re Value Micro C:\W 5527 Greg N/A <i>jmg_</i> -922	File Metadata Context sult  Sult  Soft Windows XP INDOWS 4640-0147306-23684 Schardt 40el Latitude CPI.E01/1 3372036854766395	Results A	Innotations Other	er Occurrences   Video Tria	0e				O Source Recen Recen Recen	perating System Informa- ice(s) It Activity It Activity It Activity It Activity It Activity
Use berne multiple (c)           Web bookmins (12)           Web bookmins (12)           Web bookmins (12)           Web basens (17)           Web basens (17)           Web basens (17)           Web basens (17)           Single Exerch (10)           Single Exerch (10)           Single Exerch (10)           Cit Challenge (68)           Email Addresses (12544)           PAdresses (10574)           UBLS (13944)           UBLS (15944)           UBLS (15944)           UBLS (15944)           Default (15)	<ul> <li>Hex Text A Result: 1</li> <li>Type Program Name Path</li> <li>Product ID</li> <li>Owner</li> <li>Organization</li> <li>Source File Path</li> <li>Artifact ID</li> </ul>	of 275	Re Valu Micro C:\W 5527 Greg N/A /img_ -922	File Metadata Context suit ( ) soft Windows XP INDOWS 4640-0147306-23684 Schardt 4Del Latitude CPI.ED1/4 3372036854766395	Results A	Annotations Oth	er Occurrences   Video Tris	pe				O Sourc Recen Recen Recen Recen	perating System Informa ice(s) it Activity it Activity it Activity it Activity it Activity it Activity
Up before Rubble (2)           Web Bookmiss (12)           Web Bookmiss (12)           Web Bookmiss (12)           Web Biokmiss (12)           Web Biokmiss (12)           Web Biokmiss (12)           Web Biokmiss (174)           Web Biokmiss (174)           Web Biokmiss (174)           Web Biokmiss (174)           CSt Oblege (68)           Enal Addresses (2544)           PAdresses (10579)           UB L3 (3946)           Heatrest His           E-Mail Messages           Default (Default))           Interesting Temm	Hex Text A Result: 1 Type Program Name Path Product ID Owner Organization Source File Path Artifact ID	of 275	Re Valu Micro C:\W 5527 Greg N/A /img_ -922	File Metadata Context sult $$ $$ e soft Windows XP INCOWS 4-640-0147206-22884 Schardt 4-0147206-22884 Schardt	Results A	Annotations Other	er Occurrences <sup>–</sup> Video Tria configitoftware	pe				O Sourc Recen Recen Recen	perating System Informa ce(s) It Activity It Activity It Activity It Activity It Activity It Activity
Web Solimins (12)     Single Regular Expression Search (0)     Cit Colleange (688)     Enail Addresses (26542)     P Addresses (26542)     P Addresses (26542)     Ubs (3949)     Harbaret His     E-Mail Messages     Default (Default)     Interesting Items     Possible 220 Bomb (1)     Possible 220 Bomb (1)	<ul> <li>Hex Text A Result: 1</li> <li>Type Program Name Path Product ID</li> <li>Owner</li> <li>Organization</li> <li>Source File Path Artifact ID</li> </ul>	of 275	Re Value Micro C:\W 5527 Greg N/A Amg_ -922	File Metadata Context suit $(\cdot, \cdot)$ c c SOUTWINDOWS 4640-0147306-23684 50ardt 400E Latitude CPI.E01/ 3372036854765395	Results A	Annotations Other	r Occurrences Video Tra configitoftware	pe				O Sourc Recen Recen Recen	perating System Informat re(s) Et Activity Et Activity Et Activity Et Activity Et Activity
Doal betwee Handbell (2)           Web Bookmins (12)           Web Bookmins (12)           Web Bookmins (12)           Web Hostmy (1774)           Web Hostmy (1774)           Web Bookmins (8)           Keyword His           Single Literal Keyword Search (0)           Single Literal Keyword Search (0)           CS Challenge (688)           Enal Addresses (25542)           PhAdresses (10574)           URLs (3946)           Hadraset His           Erfall (Default)           Interesting Titems           Provide Y Board As Intable (Central Reposit)           Provide Y Board As Intable (Central Reposit)	<ul> <li>Hex Text A Result: 1</li> <li>Type</li> <li>Program Name</li> <li>Path</li> <li>Product ID</li> <li>Owner</li> <li>Organization</li> <li>Source File Path</li> <li>Artifact ID</li> </ul>	of 275	Value Micro C:\W 5527 Greg N/A /img_ -922	File Metadata Context suit C 2015 e soft Windows XP INDOWS 4640 0147306-23684 54hardt 24hardt 2015 25hardt 40bel Latitude CPI,E01(A	Results a	Annotations Other	er Occurrences Video Tris config/lioftware	pe				O Sourc Recen Recen Recen	perating System Informat 2c(6) Xt Activity A Activity A Activity A Activity A Activity A Activity A Activity
Dob Derive Rubble (J)           Web Bookmiss (12)           Web Dookmiss (12)           Web Dookmiss (12)           Web Holmstry (174)           Web Holmstry (1774)           Web Bookmiss (1774)           Web Holmstry (1774)           Web Bookmiss (178)           Single Literal Keyword Search (0)           Single Regular Expression Search (0)           CSC trailinger (688)           Enal Addresses (25542)           J. PAddresses (10574)           Website Site (0074)           Harlsnet Hits           EMail Messages           Default (Default)           Interesting Titems           Previously Seen Devices (Central Reposit           Previously Seen Devices (Central Reposit           Previously Tagged As Notable (Central Reposit	Hex Text A Result: 1 Type Program Name Product ID Owner Organization Source File Path Artifact ID	of 275	Kenge Valu Micro C:\W 5527 Greg N/A /img_ -922	File Metadata Context sult () () () () () () () () () () () () ()	Results a	knotations Oth	er Occurrences Video Tris	pe				O Sourc Recer Recer Recer Recer	perating System Informat e(s) 14 Activity 14 Activity 14 Activity 14 Activity 14 Activity
Use Jorna Ruduleu (J)           Web Solmmiss (12)           Web Solmmiss (12)           Web Solms (174)           Web History (1774)           Web History (1774)           Web Solms (18)           Web History (1774)           Web Solms (18)           Single Eulard Represents Search (0)           CSI Challenge (868)           Braid Addresses (2542)           Photone Numbers (1794)           Ullus (3994)           Hadraset His           E-Mail (Default))           Interesting Items           Prosolit 20 Both (1)           Prevoluty Seen Devices (Central Repost)           Prevoluts (200 All Notable (Central Repost)           Credit Card	<ul> <li>Hex Text A Result: 1</li> <li>Type Program Name Path Product ID</li> <li>Owner Organization Source File Path Artifact ID</li> </ul>	of 275	Ree Ree Micro C:\W S527 Greg N/A /mg_ -922	File Metadata Context aut Context e of Windows XP INDOVS 4640-0147306-23684 4640-014700-014700-014700 4700-014700-014700-014700-014700-0140000000000	Results A	unotations Oth	r Occurrences Video Tria	pe				O Recer Recer Recer	perating System Informat ec(s) t Activity t Activity t Activity t Activity t Activity
Usb Deriver Rubble (∠)           Web Doolmins (12)           Web Doolmins (12)           Web Doolmins (12)           Web Starbins (12)           Single Literal Keyword Starbins (12)           Single Regular Expression Search (0)           Single Literal Keyword Starbins (12)           End Addresses (2542)           Phodresses (1054)           Phodresses (1054)           Erfail (Usf-full)           Interesting Tems           Previously Tagged As Notable (Central Reposite           Previously Tagged As Notable (Central Reposite           Previously Tagged As Notable (Central Reposite           © End Card           © End Card	Hex Text A Result: 1 Type Program Name Product ID Owner Organization Source File Path Artifact ID	of 275	Re Valui Micro C:W S527 Greg N/A Amg_ -922	File Metadata Context suit ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	Results A	Unnotations Other	er Occurrences Video Tria config/software	pe				O Sourr Recen Recen Recen	peraling System Informat re(s) 4 Activity 4 Activity 4 Activity 4 Activity 4 Activity
Use Jorne Rudole (c) Web Solmriss (12) Default Literal Keyword Search (0) CSI Contempe (68) Enail Addresses (25:44) Photon Numbers (12) Default (Default) Hadract His E-Mail Messages Default (Default) Interesting Items Providually Search (2) Previoually Tagged As Notable (Central Reposit Previoualle Previoualle Pr	Hex Text A Result 1 Type Program Name Path Product ID Owner Organization Source The Path Artifact ID	of 275	Re Valui Micro C:W S527 Greg N/A Amg_ -922	File Metadata Context suit Context soft Windows XP INDOWS 4-640-0147206-22864 Schardt 4-Del Lattude CPI.E01/ 1372036854766395	Results A	knotations Oth	r Ocarrences Video Tra	pe				O Sour Recer Recer Recer	perating System Informa ec(s) t Activity t Activity t Activity t Activity t Activity

Picture 4:Registered owner

6. What is the computer account name? The computer name is N-1A9ODN6ZXK4LQ

€ → C				Ocherone ree	port S close	Case			· ()	Keyword Lists	Keyword Search	
and blast the	Listing										( ) <del>-</del>	1
E Data Courses	Operating System Information	tion									4 Results	- 16
del Sources     del Latitude CPI.E01     SCHAPDT 001	Table Thumbnail										Save Table as CSV	
- Wews	Course Ela		Name	Demain	Varaina	Descences Audultures and	Termeney Eiler Directory	Data Causas	Deserves Name	Dath	Dead and ID	
🕀 👶 File Types	Source File	5 0 0	Name	Domain	version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Paul	Product ID	
🕀 😠 Deleted Files	system	v	W-THAODARCYK4EG		windows_N1	×86	765ystemikooc16(TEMP	SCHARD1.001				
MB File Size	e software	_			Net of the	1.55	Managine and a state of the state of the	SCHARD1.001	Microsoft Windows XP	CIWINDOWS	552/4-640-014/306-23684	
Results	C system		N-1A90DN6ZXK4LQ		Windows_NT	x86	%5ystemRoot%\TEMP	4Dell Latitude CPI.E01				4
Extracted Content	software							4Dell Latitude CPi.E01	Microsoft Windows XP	C:\WINDOWS	55274-640-0147306-23684	
Web History (1774) Web Search (8)	Hex Text Application Result: 2 of 44	Message Re	File Metadata Context	Results	Annotations Othe	er Occurrences Video Tria	ge			c	Operating System Information	1
Single Literal Keyword Search (0)     Single Dec Arc Extremelion Search (0)	Туре	Value	2							Sour	ce(s)	
Gildenge (868)	Name	N-1A	90DN6ZXK4LQ							Rece	nt Activity ^	
Email Addresses (22642)	Vertion	Wind	NT.							Rece	nt Activity	
⊕ IP Addresses (10674)	Processor Architecture	x86	0415_141							Rece	nt Activity	
Phone Numbers (1794)	Temporary Files Directory	%Sys	stemRoot%\TEMP							Rece	nt Activity	1
	Source File Path	/img_	4Dell Latitude CPi.E01/	vol_vol2/WIN	DOWS/system32/	config/system						
E Mai Messager	Artifact ID	-9223	3372036854766448									1
Default ((Default))     Finterstrong tems     forstrong tems     Freviously Seen Devices (Central Repository) (2     Freviously Tagged As Notable (Central Repositor)     Accounts     Grad Card     Grad Lag												
Tags	*										~	

*Picture 5:Computer name* 

7. What is the primary domain name? The Domain Name is N-1A9ODN6ZXK4LQ

SCHARDT_01072020 -	Autopsy 4.15.0									2	- 0	×
Add Data Source	ow Help Images/Videos 🔣 Communication	ns 💡 Geolocation 🗮 Tim	eline 🔏	File	Discovery 📗 Generate Report	Close Case			⊙ • Keyword	Lists (	Q- Keyword Sea	arch
4	A	Listing									( )	-
	~	/mg_4Dell Latitude CPi.E01/v	ol_vol2/W	INDOV	/S/system32/config						23	Results
₽- <b>₩</b>	system32 (1794)	Table Thumbnail										
	1025 (2)										Save Table as	s CSV
	1031 (2)				N. 10.17	d		Contract Toronto	<b>5</b> -1	Fl (D: .)		
	1033 (3)	Name	5 0	. 0	Modified (ime	Change Time	Access time	Created lime	size	Hags(Dir)	Hags(Meta)	) <b>FR</b>
	1037 (2)	default.sav		3	2004-08-19 21:56:20 GMT+05:0	0 2004-08-19 22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:	:00 90112	Allocated	Allocated	- u ^
	1041 (2)	SAM		3	2004-08-27 20:46:33 GMT+05:0	0 2004-08-20 03:35:21 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:	:00 262144	Allocated	Allocated	u
	1042 (2)	SAM.LOG		3	2004-08-27 20:08:23 GMT+05:0	0 2004-08-27 20:08:23 GMT+05:00	2004-08-27 20:08:23 GMT+05:00	2004-08-19 21:58:55 GMT+05:	:00 1024	Allocated	Allocated	u
	1054 (2)	SecEvent.Evt		3	2004-08-19 21:59:15 GMT+05:0	0 2004-08-19 22:02:15 GMT+05:00	2004-08-19 21:59:15 GMT+05:00	2004-08-19 21:59:15 GMT+05:	:00 65536	Allocated	Allocated	U
	2052 (2)	SECURITY		3	2004-08-27 20:46:33 GMT+05:0	0 2004-08-20 04:04:03 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:	:00 262144	Allocated	Allocated	u.
	30/6 (2) 3com dmi (2)	SECURITY.LOG		3	2004-08-27 20:32:56 GMT+05:0	0 2004-08-27 20:32:56 GMT+05:00	2004-08-27 20:32:56 GMT+05:00	2004-08-19 21:58:55 GMT+05:	:00 1024	Allocated	Allocated	ú
	CatRoot (4)	software		3	2004-08-27 20:46:33 GMT+05:0	0 2004-08-27 20:29:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:	:00 8650752	Allocated	Allocated	U
	CatRoot2 (9)	software.LOG		3	2004-08-27 20:46:32 GMT+05:0	0 2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-19 21:56:08 GMT+05:	:00 1024	Allocated	Allocated	
1 I I I.	📙 Com (9)	<										>
9	Lonfig (23)											
	🕀 🐊 systemprofile (14)	Hex Text Application M	issage	File Me	adata Context Results Annot	ations Other Occurrences Video Triag	e					
	📙 dhap (2)	Type 1 In	staller		A Metz	idata					-	
	DirectX (3)	Userinsta	lable.driv	ers	* Name	: DefaultDomainName						
	dicache (2352)	⊕- Windows			Type	REG_SZ						
	drivers (1/6)	Winlogon			Valu	e						
	iae (d)	III Notif	(		N-1A	90DN62XK4LQ						
	ids (4)	() Sped	alAccount	s								
(A)	IME (5)	- Auto	RestartSh	el								
	inetsry (2)	-• Defa	ultDomain	Name								
	Macromed (3)	-      Defa	ItUserNa	me								
(F)	Microsoft (3)	- Clegal	NoticeCap	not								
	MsDtc (4)	- Cegai	rdownAft	erShut	town							
	mui (4)	- e Repo	tBootOk	er on los								
	npp (4)	Shell										
	oobe (45)	-  Shute	lownWith	outLog	on							
L L	nas (8)	Syste	m									
	Restore (6)	Useri	nit									
	Setup (18)	VmAp	piet									
	ShellExt (2)	- Steel	tacdrome									
æ	spool (5)	- @ aloca	tedasd									
	📙 usmt (23) 🗸	- e alloca	tefloppies		~							

Picture 6:Primary Domain name

8. When was the last recorded computer shutdown date/time? The last recorded shutdown time at 27-08-2004 10:46:27.

Add Data Sou	urce 🌆 Images/Videos 📷 Comm	inications V Geolocation		denerone report	S CON CON						Ge Neyword Search	
€ ⇒		C Listing									+ + + 1	-
	- svstem 32 (1794)	/img_4Dell Latitude CF	h.E01/vol_vol2/WINDOWS/system32/co	nfig							23 Resul	ts
	1025 (2)	Table Thumbnail										
	1028 (2)										Save Table as CSV	
	1033 (3)	he	Access Time	Created Time		Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	s
	- 📜 1037 (2)	20:29:44 GMT+05:0	0 2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:	56:08 GMT+05:00	8650752	Allocated	Allocated	unknown	/img_4Dell Latitude CPI.E01/vol_vol2/WINDOWS/system32.	. 85af9ce354890337cel /	^
	- 📜 1041 (2)	20:46:32 GMT+05:0	0 2004-08-27 20:46:32 GMT+05:00	2004-08-19 21:	56:08 GMT+05:00	1024	Allocated	Allocated	unknown	/img_4Dell Latitude CPI.E01/vol_vol2/WINDOWS/system32.	. 41ae974e38e845822t	
		22:02:15 GMT+05:0	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:	56:18 GMT+05:00	630784	Allocated	Allocated	unknown	/img_4Dell Latitude CPI.E01/vol_vol2/WINDOW5/system32.	. 7240000a70df45789d	
	1054 (2)	20:46:29 GMT+05:0	2004-08-27 20:46:29 GMT+05:00	2004-08-19 21:	59:15 GMT+05:00	65536	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOW5/system32.	, 06e1549454814d1d5f	
	2052 (2)	20:31:44 GMT+05:0	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:	56:06 GMT+05:00	2621440	Allocated	Allocated	unknown	/img_4Dell Latitude CPI.E01/vol_vol2/WINDOW5/system32.	. 3e4f17d1e4d84e2766	
	3com dmi (2)	20:46:33 GMT+05:0	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:	56:08 GMT+05:00	1024	Allocated	Allocated	unknown	/img_4Dell Latitude CPI.E01/vol_vol2/WINDOW5/system32.	698b64ed72db5eb91c	
	E CatRoot (4)	22:02:15 GMT+05:0	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:	56:18 GMT+05:00	389120	Allocated	Allocated	unknown	/img_4Dell Latitude CPI.ED1/vol_vol2/WINDOW5/system32.	. 061b9a703b1fbb591a	
	🕀 📜 CatRoot2 (9)										>	1
												Ц
		Hex Text Applica	tion Message File Metadata Contex	Results Annot	tations Other Occur	rences Vide	so Triage					
	DirectV (3)		CI	^ Meta	ədata							٦
	dicache (2352)		CI Extensions	Name	e: ExitTime							
			Idimap	Valu	-							-
	export (2)		loduleCompatibility	2004	/08/27-10:46:27							1
	📕 ias (4)	9 N	etwork									1
	icsxml (7)		etworkCards InenGLDrivers									1
	IME (5)		erfib									1
	Macromed (3)	🛞 - 🚺 P	erHwIdStorage									1
	CE PRODUCTION CON		orts									1
	Microsoft (3)											
	Microsoft (3)     MsDtc (4)	e- <mark>.</mark> P	refetcher									ч
	<ul> <li>⊕- ↓ Microsoft (3)</li> <li>⊕- ↓ MsDtc (4)</li> <li>⊕- ↓ mui (4)</li> </ul>	e- P	refetcher Version StartTime									
	Microsoft (3)     MsDtc (4)     mui (4)     npp (4)	₽- <mark>-</mark> ₽	efetcher Version StartTime TracesProcessed									
	Microsoft (3)     Microsoft (3)     MsDtc (4)     mui (4)     npp (4)     oobe (45)	P	e Fetcher • Version • StartTime • TracesProcessed • TracesSuccessful									
	⊕-     B. Microsoft (3)     ⊕-     B. MsDtc (4)     ⊕-     B. mai (4)     ⊕-     pp (4)     ⊕-     obce (45)     −     B. ras (8)		refetcher Version StartTime TracesProcessed TracesSuccessful LastTraceFalure									
	(3)     MsDtc (4)     MsDtc (4)     MsDtc (4)     Mp (4)     Obs (45)     Obs (45)     Obs (45)     Restore (6)		refetcher Version StartTime TracesProcessed TracesSuccessful LastTraceFalure ExitCode									
	B -      B. Microsoft (3)     Herbort (4)     MsDitc (4)     mai (4)     -      nop (4)     e -      obse (45)     ras (8)     Restore (6)     Restore (18)		efetcher 9 Version 9 StartTime 1 TraceBrocessed 9 TraceBrocessed 9 TraceBrocessed 9 TraceBrocessed 9 TraceBrocessed 9 TraceBrocessed 9 TraceBrocessed 9 TraceBrocessed 9 TraceBrocessed 9 String 9 BottleeCommand 9 BottleeCommand									
	<ul> <li>B - 20 Microsoft (3)</li> <li>B - 20 Microsoft (3)</li></ul>		refetcher > Version > TraceByCocssed > TraceSyLocssful > LaStTraceFakure > ExtCode ExtCode > BootFileSOptmized > LaStDiskLayoutTime									
	B → Microsoft (3)     Walch (4)     Walch (4)     Mobit (4)     monometry (4)     monometry (4)     monometry (4)     monometry (5)     monometry (5)     monometry (5)     monometry (5)     monometry (5)     monometry (5)		refetcher > Version > StartTime TraceByCocssed TraceByCocssed > LaSTLaceFalure > ExitCode > BooTriesOphmzed > LaSTLacyDimeztmegt > LaSTDalayouTimestring									
	Horosoft (3)     Horosoft (3)     Horosoft (3)     Horosoft (4)     StelExt (2)     Horosoft (5)     Horosoft (2)     Horosoft (2)		refetter Version StartTime TracesProcessed TracesProcessful b InstTraceSurgers Biotocole Biotoco									

Picture 7:Last recorded Shutdown Time

9. How many accounts are recorded (total number)? There are 5 accounts: Administrator, Guest, Help Assistant, Mr.Evil, Support 388945a0.

source an subgest	Ideos 🔯 Communication	is V Geolocation 🚬 Time	ine 🤞	File	Discovery biscovery	eport 🕜 Close Case		•	<ul> <li>Keyword Lis</li> </ul>	its Q	Keyword Searc	ch .
	0	Listing Keyword search	1 - He	lpAssis	tant ×							• 🗆
- system32 (	794)	/img_4Dell Latitude CPi.E01/vol	_vol2/V	VINDO	WS/system32/config						23 R	Results
1025 (2		Table Thumbnail										
1028 (2											Save Table as C	CSV
1031 (2		Name	s	c o	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	K
1037 (2		default		3	2004-08-27 20:46:33 GMT+	+05:00 2004-08-20 03:53:22 GMT+05:0	00 2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	262144	Allocated	Allocated	u ^
1041 (2		default.LOG		3	2004-08-27 20:32:56 GMT+	+05:00 2004-08-27 20:32:56 GMT+05:0	00 2004-08-27 20:32:56 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	1024	Allocated	Allocated	u
1042 (2		default.sav		3	2004-08-19 21:56:20 GMT+	+05:00 2004-08-19 22:02:15 GMT+05:0	00 2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:00	90112	Allocated	Allocated	u
1054 (2		SAM		3	2004-08-27 20:46:33 GMT+	+05:00 2004-08-20 03:35:21 GMT+05:0	00 2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	262144	Allocated	Allocated	u
2052 (2		SAM.LOG		3	2004-08-27 20:08:23 GMT+	+05:00 2004-08-27 20:08:23 GMT+05:0	00 2004-08-27 20:08:23 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	1024	Allocated	Allocated	u
3com d	mi (2)	SecEvent.Evt		з	2004-08-19 21:59:15 GMT+	+05:00 2004-08-19 22:02:15 GMT+05:0	00 2004-08-19 21:59:15 GMT+05:00	2004-08-19 21:59:15 GMT+05:00	65536	Allocated	Allocated	u
CatRoo	: (4)	SECURITY		3	2004-08-27 20:46:33 GMT+	+05:00 2004-08-20 04:04:03 GMT+05:0	00 2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	262144	Allocated	Allocated	u.,
Roo	2 (9)											>
📙 Com (9)												<u> </u>
config (	23)	Hex Text Application Me	sage	File Me	tadata Context Results	Annotations Other Occurrences Video Tr	riage					
H Sys	emprofile (14)	- • V			^ !	Metadata						
DirectX	(3)		IF5		1	Name: V						
dicache	(2352)	- F			-	0x1c0 43 00 4E 00 3D 00 4D	00 69 00 63 00 72 00 68 00	le n -	Micro			
ivers	176)	00000	3E8			0x1d0 73 00 6F 00 66 00 74	00 20 00 43 00 6F 00 72 00	s.o.1	.tC.o.r			
export	2)	-0 F				0x1e0 70 00 6F 00 72 00 61	00 74 00 69 00 6F 00 6E 00	p.o.r	.a.t.i.o.n			
ias (4)		- • V	EΛ			0x1f0 2C 00 4C 00 3D 00 52	00 65 00 64 00 6D 00 6F 00	,.L.=	.R.e.d.m.o			
icsxmi (	2	- F	~			0x200 6E 00 64 00 2C 00 53	00 3D 00 57 00 61 00 73 00	n.d.,	.S.=.W.a.s	•		
inatery	2)	- • 🗹				0x220 43 00 30 00 55 00 53	00 74 00 65 00 65 00 20 00	n.1.n C = 1	SThie	•		
Macrom	ed (3)	00000	EB			0x230 20 00 69 00 73 00 20	00 61 00 20 00 76 00 65 00	.1.5	av.e			
Microso	t (3)	E Names	ministra	ator		0x240 6E 00 64 00 6F 00 72	00 27 00 73 00 20 00 61 00	n.d.o	.r.'.sa			
otc (	Ð		est	100		0x250 63 00 63 00 6F 00 75	00 6E 00 74 00 20 00 66 00	c.c.0	.u.n.tf			
mui (4)		D He	pAssist	tant		0x260 6F 00 72 00 20 00 74	00 68 00 65 00 20 00 48 00	0.r.	.t.h.eH			
inci (4)			Evil	-		0x270 65 00 60 00 70 00 20	00 61 00 62 00 64 00 20 00	e.1.p	a.n.d.	5 C		
npp (4)	5]	10 SU	PPORT	_38894	5a0	0x290 53 00 65 00 72 00 76	00 69 00 63 00 65 00 00 00	S.e.r	.v.i.c.e	53		
npp (4) oobe (4	->					0#250 01 02 00 02 02 00 02	00 01 00 01 00 01 00 01 00			827		
npp (4) oobe (4 ras (8)	(6)	• (Defau	lt)			04240 101 02 00 00 07 00 00						
npp (4) oobe (4) ras (8) Restore	(6)	• (Defau • F	lt)			0x2b0 3C DB B9 0E CC 23 11	5F 57 96 11 C9 60 42 91 B8	<	♦₩`B.			
npp (4) oobe (4) ras (8) Restore Setup (	(6) (8) (2)	- • (Defau - • F - • V	it)			0x2b0 3C DB B9 0E CC 23 11 0x2c0 01 00 01 00 01 00 01	5F 57 96 11 C9 60 42 91 B8 00	<	♦₩`B. 			
npp (4) oobe (4 ras (8) Restore Setup ( ShellExt	(6) (8) (2)	(Defau     (Defau     (Pefau      (Pefau     (Pefa	lt)			0x2b0 01 02 00 00 07 00 00 0x2b0 3C DB B9 0E CC 23 11 0x2c0 01 00 01 00 01 00 01	5F 57 96 11 C9 60 42 91 B8 00	<	∳W`B. 	•		

*Picture 8:Existing accounts* 

**10.** What is the account name of the user who mostly uses the computer? The user that mostly uses the computer is **Mr.Evil**.

Add Data source and Images/videos 🔯 Communica	Geo		one di	rite L	Jocovery enerate Report	Ubse case			•	<ul> <li>Keyword List</li> </ul>	s C	Keyword Sea	rch
÷ (	Listing	Keyword seard	h 1 - 1074	ŧ ×	Keyword search 2 - Event ID: 1074	× Keyword search 3 - Event Vie	wer × Keyword search 4 - event	vwr.msc ×	Keyword search 5 - S	hutdown Time	×	( )	• 🗆
4Dell Latitude CPi.E01	/img_4Del	Latitude CPi.E01/vo	x_vol2/Do	cumen	its and Settings/Mr. Evil							19	Results
Data Source Files	iable 1	numonali											
🗇 🔜 4Dell Latitude CPI.E01												Save Table as	CSV
vol1 (Unallocated: 0-62) vol2 (NTES / exEAT (0x07): 63-9510479)	Name		S (	0	Modified Time	Change Time	Access Time	Created Tir	me	Size	Flags(Dir)	Flags(Meta)	Kr
\$OrphanFiles (0)	🔍 Star	t Menu			2004-08-19 22:00:09 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-27 20:08:06 GMT+05:00	2004-08-20	04:04:05 GMT+05:00	256	Allocated	Allocated	un ^
\$CarvedFiles (995)	Temp	plates			2004-08-20 03:24:35 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-20 20:17:59 GMT+05:00	2004-08-20	04:04:05 GMT+05:00	56	Allocated	Allocated	un
	gtk-	-bookmarks		0	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27	20:40:43 GMT+05:00	0	Allocated	Allocated	kn
SUnaloc (4)	inter	rception		4	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27	20:41:00 GMT+05:00	173372	Allocated	Allocated	un
All Users (9)	NTU:	SER.DAT		4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:13 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20	04:04:05 GMT+05:00	786432	Allocated	Allocated	un
🕞 📙 Default User (98)	ntus	er.dat.LOG		4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20	04:04:06 GMT+05:00	1024	Allocated	Allocated	un
Description (8)	🐻 ntus	ier.ini		0	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20	04:04:08 GMT+05:00	180	Allocated	Allocated	kn 🗸
🕀 📕 Mr. Evil (19)	<												>
RECYCLER (3)     System Volume Information (3)	Matches	s on page: Displays	s extracte	d text	from files and keyword-search res	ults. Requires Keyword Search ing	est to be run on a file to activate thi	s viewer.		Text Source	e: File Text		~
Interp (2)     I	regf nd Set +gDIRT	tings\Mr. Evil	\ntuse:	r.dat									
USB Device Attached (1)													



#### 11. Who was the last user to logon to the computer? Last user was Mr.Evil

	unications 🦞 Geolocation 🗮 Tim	ene d	f rie i	Discovery b Generate Re	port 😸 close case			<ul> <li>Keyword L</li> </ul>	ists C	Keyword Searc	h
	C Listing Keyword sear	dh 1 - Hei	pAssist	ant X						4	• •
- 1031 (2)	/img_4Dell Latitude CPi.E01/v	ol_vol2/V	VINDOV	/S/system32/config						23 R	esults
	Table Thumbnail									Caus Table as C	~
1037 (2)	News			MadfadTas	Channel Trave	town Tex	Contractions	5	Finan (Din)	Save rable as c	SV
- 1042 (2)	Name	2	0	Modified Time	Change Time	Access Time	Created lime	Size	Hags(Uir)	Flags(Meta)	N ED
1054 (2)	SECURITY		3	2004-08-27 20:46:33 GMT+	-05:00 2004-08-20 04:04:03 GMT+05:00	2004-08-27 20:46:33 GM1+05:00	2004-08-19 21:58:55 GMT+05	262144	Allocated	Allocated	"^
- 📜 2052 (2)	SECURITY.LOG		3	2004-08-27 20:32:56 GMT-	-05:00 2004-08-27 20:32:56 GMT+05:00	2004-08-27 20:32:56 GMT+05:00	2004-08-19 21:58:55 GMT+05	00 1024	Allocated	Allocated	U
3076 (2)	software		3	2004-08-27 20:46:33 GMT-	-05:00 2004-08-27 20:29:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05	00 8650752	Allocated	Allocated	u
3com_dmi (2)	software.LOG		3	2004-08-27 20:46:32 GMT-	-05:00 2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-19 21:56:08 GMT+05	00 1024	Allocated	Allocated	u
CatRoot (4)	software.sav		3	2004-08-19 21:56:20 GMT-	-05:00 2004-08-19 22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05	00 630784	Allocated	Allocated	u
	SysEvent.Evt		3	2004-08-27 20:46:29 GMT-	-05:00 2004-08-27 20:46:29 GMT+05:00	2004-08-27 20:46:29 GMT+05:00	2004-08-19 21:59:15 GMT+05	00 65536	Allocated	Allocated	u.
config (23)	system		3	2004-08-27 20:46:33 GMT-	-05:00 2004-08-27 20:31:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:06 GMT+05	00 2621440	Allocated	Allocated	
Illcache (2352) dilcache (2352) drivers (176) export (2) ias (4) icsml (7) JME (5) inetsrv (2) Macromed (3)	Hex Text Application Writiogo GPE-GPE-GPE- G	tensions y alAccoun RestartSI ultDomair ultUserNa NoticeTe erdownAf	File Me ts hell Name ption xt terShut	adata Context Results .	Innotations Other Occurrences Video Tria Metadata Name: De <b>fault/Scritame</b> Type: REG_52 Yalue Mr. Evil	pe					
Microsoft (3)     Microsoft (4)     Microsoft (4)     mui (4)     npp (4)     oobe (45)     fraction (6)	Rep.     Shell     Shut     System	rtBootOk downWit <del>l</del> m nit	outLog	on							

Picture 10:Last user

12. A search for the name of "G=r=e=g S=c=h=a=r=d=t" reveals multiple hits. One of these proves that G=r=e=g S=c=h=a=r=d=t is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to? The file is the irunin.ini and is related to Look@LAN



*Picture 11:Mr.Evil is the Administrator* 

#### **13.** List the network cards used by this computer. There are two cards.



Picture 12:Wireless card



Picture 13:Ethernet interface card

14. This same file reports the IP address and MAC address of the computer. What are they? The information can be found in picture 11 and is the following: IP Address:192.168.1.1

MAC Address:**0010a4933e09** (The first three digits refer to the company that produce this card)

- **15.** An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN? **Xircom**
- **16.**Find 6 installed programs that may be used for hacking. There are 6 programs related to hacking.
  - a. 123Wasp

Add Da	ta Source	e 📠 Images/Videos 🔣 Com	munication	: 💡 Geolocation 🗮 Tim	neline 🔏	File	Discovery 📗 Generate Report	B Close Case		🖂 o	• Keyword I	ists
>		\$CarvedFiles (995) \$Extend (5)	•	Listing Keyword sear /mg_4Dell Latitude CPi.E01/v Table Thumbnail	rch 1 - Help vol_vol2/Pr	Assis ogran	tant × Keyword search 2 - Greg : n Files/123WASP	Schardt ×				
	B-	SUnalloc (4)     Documents and Settings (7)     My Documents (11)     Program Files (36)	- 11	Name	s c	: 0	Modified Time	Change Time	Access Time	Created Time	Size	
	B- 0			(current folder)			2004-08-20 20:13:12 GMT+05:00	2004-08-20 20:13:12 GMT+05:00	2004-08-27 20:14:44 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	56	
		123WASP (9)		Darent folder]			2004-08-27 20:28:49 GMT+05:00	2004-08-27 20:28:49 GMT+05:00	2004-08-27 20:29:18 GMT+05:00	2004-08-18 21:31:52 GMT+05:00	152	
		Accessories (3)		123wasp.exe		4	2001-06-15 01:55:06 GMT+05:00	2004-08-27 20:14:44 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	73728	
		Agent (20)		G HELP.htm		4	2001-06-15 05:29:54 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	17985	
	1	Anonymizer (6)		HISTORY.txt		4	2001-06-14 00:34:28 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	634	
	1	Can (39)		INSTALL.LOG		4	2004-08-20 20:13:14 GMT+05:00	2004-08-20 20:13:12 GMT+05:00	2004-08-20 20:13:12 GMT+05:00	2004-08-20 20:13:12 GMT+05:00	1714	
		Common Files (8)		LICENSE.txt		4	2001-06-15 03:01:00 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2477	
	1-	ComPlus Applications (2)		README.txt		4	2001-06-14 00:33:28 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	1963	

b. Cain

dd Da	ita Souro	e 📠 Images/Videos 🔣 Con	munications	s 💡 Geolocation 🧮 Tim	elne 🚚 I	File Disc	overy 📗 Generate Report 🍙	Close Case		💌 💿 • Ke	eyword Lists
>	×	\$CarvedFiles (995) \$Extend (5)	•	Listing Keyword search /mg_4Dell Latitude CPi.E01/vo Table Thumbnail	th 1 - HelpAr ol_vol2/Prog	sistant ram File	X Keyword search 2 - Greg Scha s/Cain	rdt ×			
	·	Documents and Settings (7)	- 11	Name	s	со	Modified Time	Change Time	Access Time	Created Time	Size
	<b>•</b> -	My Documents (11)		Cain.exe		4	2003-12-13 08:32:04 GMT+05:00	2004-08-27 20:33:01 GMT+05:00	2004-08-27 20:33:07 GMT+05:00	2004-08-20 20:05:58 GMT+05:00	2064384
		Program Hies (36)		Cain.exe.sig		4	2003-12-13 08:32:44 GMT+05:00	2004-08-20 20:05:59 GMT+05:00	2004-08-20 20:05:59 GMT+05:00	2004-08-20 20:05:59 GMT+05:00	66
		Accessories (3)		CCD.LST		0	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	0
		Agent (20)		CERT.LST		0	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-25 21:18:34 GMT+05:00	2004-08-25 21:18:34 GMT+05:00	0
		Anonymizer (6)		Credits.txt		4	2003-10-28 06:07:08 GMT+05:00	2004-08-20 20:05:58 GMT+05:00	2004-08-20 20:05:58 GMT+05:00	2004-08-20 20:05:58 GMT+05:00	627
	100	CHAT (2)		DRR.LST		0	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-25 21:20:19 GMT+05:00	0
		Common Files (8)		FTP.LST		0	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	0
		ComPlus Applications (2)		HOSTS.LST		0	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-25 21:20:19 GMT+05:00	0
		DirectX (3)		HTTPJST		0	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21-18-37 (MT±05-00	0

c. Network Stumbler

Case View	Tools Window Help			_								_
🛖 Add Da	ata Source 📠 Images/Videos 📓 Co	mmunication	s 💡 Geolocation 🧮 Tim	elne 🌡	File	Disc	covery 📗 Generate Report 🧃	Close Case		🛛 🖉	- Keyword Li	ists
€ >	Documents and Settings (7)     My Documents (11)     Program Elec (26)	•	Listing Keyword searcy /mg_4Dell Latitude CPi.E01/vo Table Thumbnail	th 1 - He ol_vol2/F	lpAssis Program	tant n File	t × Keyword search 2 - Greg So es/Network Stumbler	hardt X				
	- 123WASP (9)		Name	s	C (	0	Modified Time	Change Time	Access Time	Created Time	Size	Fk
	Accessories (3)		退 [current folder]				2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-27 20:12:15 GMT+05:00	56	Alle
	B- Anonymizer (6)		Darent folder]				2004-08-27 20:28:49 GMT+05:00	2004-08-27 20:28:49 GMT+05:00	2004-08-27 20:29:18 GMT+05:00	2004-08-18 21:31:52 GMT+05:00	152	Alk
	🕀 📕 Cain (39)		netstumbler.chm		4	ŧ	2004-04-21 11:42:58 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:27 GMT+05:00	2004-04-21 11:42:58 GMT+05:00	149914	Alk
	- 🔛 CHAT (2)		NetStumbler.exe		4	•	2004-04-21 12:16:58 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-27 20:12:37 GMT+05:00	2004-04-21 12:16:58 GMT+05:00	561152	Alic
	Common Files (8)		Fins-aos-new.wav		4		2002-04-12 04:43:25 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2002-04-12 04:43:25 GMT+05:00	15668	Allo
	Complus Applications (2)     DirectX (3)		J ns-gps-err.wav		4		2002-04-12 05:26:41 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2002-04-12 05:26:41 GMT+05:00	10704	Alio
	Ethereal (45)		🖋 ns-los.wav		4		2002-04-12 05:26:41 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2002-04-12 05:26:41 GMT+05:00	10704	Allo
	B-      Faber Toys (10)     B-      GlobalSCAPE (3)		ørs-signal-0.wav <		4	•	2002-04-12 04:13:33 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2002-04-12 04:13:33 GMT+05:00	11160	Allo

Picture 16:Network Stumbler

#### d. Look@LAN

SCHARDT_010720 ase View Tools W	20 - Autopsy 4.15.0 indow Help									
🛖 Add Data Source	Images/Videos 🐹 Communic	ations 💡 Geolocation 🧮 Timeline 縜	File Diso	overy		Generate Report 🛛 👩 Close Case			🐼 💿 • Keyword Lis	sts
< >	Documents and Settings (7) My Documents (11) Program Files (36)	Listing Keyword search 1 - HelpA /img_HDell Latitude CPI.E01/vol_vol2/Prov Table Thumbnail	lssistant gram File	× s/Looi	Key GLAN	word search 2 - Greg Schardt X				
T	📜 123WASP (9)	Name	s	с	0	Modified Time	Change Time	Access Time	Created Time	
	Accessories (3)	🐨 irunin.bmp			4	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	
	Agent (20)	irunin.dat			4	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	
	Cain (39)	(a) in min. ini	0	-	4	2004-08-25 20-56:10 GMT+05:00	2004-08-25 20:56:10 GMT+05:00	2004-08-25 20:56:10 GMT+05:00	2004-08-25 20:56-09 GMT+05-00	
	CHAT (2)	in pin log		-	4	2004-08-25 20-55-27 GMT+05-00	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:56-09 GMT+05-00	2004-08-25 20-56-09 GMT+05-00	
	Common Files (8)	lalarror dat			4	2003-04-27 18-31-26 GMT±05-00	2004-08-25 20-56-05 CMT±05-00	2004-08-25 20:06:15 GMT±05:00	2004-02-16 15-51-14 CMT±05-00	
	ComPlus Applications (2)	lalemáres dat			4	2004-02-19-14-24-22 CMT+05-00	2004-08-25-20-56-05-CMT+05-00	2004-08-26-20-06-19 GMT+05-00	2004-02-16 15:51:14 GMT+05:00	
	DirectX (3)	laise vices.cat	-		1	2004/02/10 14:24:32 04/14/05:00	2004-09-25 20:56:05 GHT+05:00	2004-00-20 20:00:10 0/11405:00	2004-02-10 15:51:14 GMT+05:00	
	Ethereal (45)	License.txt			4	2004-02-17 15:48:00 GM1+05:00	2004-08-25 20:55:11 GMT+05:00	2004-02-18 15:00:03 GMT+05:00	2004-02-17 15:40:55 GM1+05:00	-
	Clobals CARE (2)	Look@LAN on the WEB.ur	e.txt		4	2004-02-17 15:31:21 GMT+05:00	2004-08-25 20:56:11 GMT+05:00	2004-02-18 14:19:04 GMT+05:00	2004-02-17 15:31:39 GMT+05:00	
(B)-	Internet Explorer (10)	<								
	Look@LAN (18)	Hey Text Amiration Message El	ia Matada	a la		1 Results Annotations Other Occ	Video Triace			
	Messenger (14)	Hex Tedand Test	emetaua	1.0		A Resource Animotations Other Occ	unences maco mage			
	microsoft frontpage (3)	Strings Indexed Text Translation			_					_
	MIRC (16)	Matches on page: - of - Ma	atch 🧲	$\rightarrow$		Page: 1 of 1 Page 🗲 🔿	100% 🗩 🕀 Reset		Text Sour	ce:
	Movie Maker (8)									
	📕 MSN (4)	1. Non-commercial								
₽-	MSN Gaming Zone (3)									
1 1 1 1	NetMeeting (23)	This software is considered	as FR	EEWAI	RE I	or any individual/home/per	sonal use.			

Picture 17:Look@LAN

#### e. mIRC



f. Ethereal



Picture 19:Ethereal

#### 17. What is the SMTP email address for Mr. Evil? The SMTP email address for Mr.Evil is: iswhoknowsme@sbcglobal.net

ata Source	📠 Images/Videos 🔣 Commu	nications 💡 Geolocation 🧮	Timeline 🍃	File D	iscovery 📗 Generate Report	B Close Case			•	- Keyword Li	ists C	- Keyword Sear	ch		
		C Listing Keyword s	sarch 1 - SM	P email	add ×							< >	Ŧ		
\$CarvedFiles (995)		/mg_4Dell Latitude CPI.E0	ng_@beitatube_ChR:DJ/up/upi2/program Fies/Agent/Data 36 Results Table Thumbhad												
	Extend (5)	Table Thumbhail									1	Save Table as	csv		
@- 📕 D	ocuments and Settings (7)	Name	s		Modified Time	Chappe Time		Access Time	Created Time	Size	Flags(Dir)	Flacs(Meta)	d		
@- 📜 M	ly Documents (11)	AGENT INI		4	2004-08-25 21-18-07 CMT±05-00	2004-08-25 21-18-	17 CMT±05-00	2004-08-25 21-18-07 CMT±05-00	2004-08-21 00/28/37 CMT±05-00	11309	Allocated	Allocated			
0- 0 P	rogram Files (36)	- Address het		4	2004-09-21-00-47-20 CMT+05-00	2004-09-21-00-47	20 CMT LOELOD	2004-00-23-21120-07-07-1405-00	2004-00-21-00-45-44 CMT+05-00	21000	Allocated	Allocated			
	123WASP (9)	Elionog.okt		-	2004-08-21 00:47:30 GMT+05:00	2004-00-21 00:47:	30 GHT+05:00	2004-00-21 00:47:30 GHT+05:00	2004-00-21 00:45:44 041405:00	000	Allocated	Allocated			
	Accessories (3)	FILTERS.DAT		0	2004-06-21 02:15:06 GM1+05:00	2004-06-21 02:13:	06 GP11+05:00	2004-06-21 02:13:06 GMT+05:00	2004-00-21 02:13:00 GM1+05:00	0	Allocated	Allocated	K		
T	- All COD (40)	FILTERS.IDX		0	2004-08-21 02:13:06 GM1+05:00	2004-08-21 02:13:	05 GM1+05:00	2004-08-21 02:13:06 GMT+05:00	2004-08-21 02:13:05 GMT+05:00	U	Allocated	Allocated	10		
E	Data (36)	GROUPS.DAT		4	2004-08-25 20:57:34 GMT+05:00	2004-08-25 20:57:	34 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	835657	Allocated	Allocated	U		
	- 🐊 temp (2)	GROUPS.IDX		4	2004-08-25 21:18:07 GMT+05:00	2004-08-25 21:18:	07 GMT+05:00	2004-08-25 21:18:07 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	568944	Allocated	Allocated	u		
æ- 🕽	Anonymizer (6)	GRPDAT.BAK		4	2004-08-21 02:13:07 GMT+05:00	2004-08-25 20:57:	34 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	835578	Allocated	Allocated	U		
œ- ,	Cain (39)	GRPIDX.BAK		4	2004-08-21 02:13:07 GMT+05:00	2004-08-25 20:57:	34 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	568880	Allocated	Allocated	ш.		
	CHAT (2)	<											>		
(±)- (#	Common Files (8)														
-	DirectX (3)	Hex Text Application	Message	File Met	adata Context Results Annotat	ions Other Occurren	ces Video Triage								
	Ethereal (45)	Strings Indexed Text	Translation												
œ- 🖡	Faber Toys (10)	Matches on page: -	of - 1	fatch	Page: 1 of 1 P	age ( ->	100% 9	D Reset		Text Sour	rce: File Text		~		
œ- 🕽	GlobalSCAPE (3)	Proprieta de la companya de la compa				S. Demonstrational									
œ- 🔒	Internet Explorer (10)	FullName="Hr Evil Whaillddrease"who	in catema la	bealo	al ner"								1		
<b>P</b>	Look@LAN (18)	EMailAddressForma	=0	begro	J#1.1180										
	Messenger (14)	ReplyTo=""	-												
	microsoft frontpage (3)	Organization="N/A													
0.0	Mauja Makar (9)	DoAuthorisation=1													
	MSN (4)	UserName="whoknow	smellsbegl	obal .	net"										
-	MSN Gamino Zone (3)	Password="84106D9	1696F"												
L	NetMeeting (23)	SMTPLoginProtocol	-2												
	Network Stumbler (15)	SHTPUsePOPLogin=0	·												
- D	Online Services (5)	SMTPUserName="who	knowsme@s	beglo	bal.net"										
L	Outlook Express (14)	SHIPSavePassword=	L												
·	PLUSI (4)	IsRegistered=0													
	Uninstall Information (20)	IsRegistered19=0													
-	Whois (8)	IsLicensed=3													
æ- 🖡	Windows Media Player (15)	Key=""													
		Enable Support Manu	- 10												

Picture 20:SMTP email address

**18.** What are the NNTP (news server) settings for Mr. Evil? The NNTP settings for Mr.Evil are:



Picture 21:NNTP news server settings

# **19.** What two installed programs show this information? MS Outlook Express and Forte Agent

SCHARDT_010	72020 - Autopsy 4.15.0									- 🗆 ×					
Add Data So	urce 📠 Images/Videos 🔣 Co	mmunications	s 💡 Geolocation 🗮 Timeline 縜 File Discove	ry 📗 Generate Report	g Close Case				✓ • Keyword Lists	Q Keyword Search					
4 5		A	TP Keyword search 3 - NNTP X Keyword	search 4 - news.dallas.sb	X Keyword searc	h 5 - forte agent X Kr	word search 6 - MS Outloo	ok Exp X Keyword search	7 - Outlook Expres X	<					
		¥	Keyword search							118 Results					
	vol1 (Unallocated: 0-62)	^	Table Thumbnail												
B-10	vol2 (NTFS / exFAT (0x07): 63-951	0479)								Save Table ac CSV					
	\$OrphanFiles (0)									Save Table as C34					
	CarvedFiles (995)		△ Name	Keyword	Preview		Location			1×					
	sextend (5)		SMFT SMFT	current v	version of the «Outlo	ok Express< Read Me inform	a /img_SCHARDT.001/v	vol_vol2/\$MFT	2/\$MFT						
	Sunaloc (4)		MFT SMFT	current v	rersion of the «Outlo	k Express< Read Me inform	a /mg 4Dell Latitude CP	Pi.E01/vol_vol2/\$MFT	11/vol_vol2/\$MFT						
	My Documents (11)		<b>D</b> 0	cofbuara	For Outlook «Outloo	Everance AOL Europea	in line 40ell Latitude CE	S E01 and unltimester and Settings/Mr. Englines of Settings/Temporary Internet Elec-							
9	Program Files (36)			Jurtinuro			him ping_nour control of	- Interprotection of the second	the second second second	pyromporus y sincernour no.					
	123WASP (9)		0	software	For Outlook, «Outloo	k Express≪, AOL, Eudora,	n /mg_SCHARDT.UU1/v	ol_vol2/Documents and Settings/	Mr. Evil/Local Settings/Temp	orary Internet Hies/Conte					
	Accessories (3)		00000152.DAT	X-Newsre	eader: Microsoft «Ou	tlook Express« 6.00.2800.1	4 /img_SCHARDT.001/v	/ol_vol2/Program Files/Agent/Dat	a/00000152.DAT						
	- Agent (20)		00000152.DAT	X-Newsre	X-Newsreader: Microsoft «Outlook Express» 6.00.2800.14 /mg_4Dell Latitude CPI.E01/vol_vol2/Program Files/Agent/Data/00000152.DAT										
	Anonymizer (6)		00000157.DAT	X-Newsre	X-Newsreader: Microsoft «Outlook Express» 6.00.2800.14 /mg_SCHARDT.001/vol_vol2/Program Files/Agent/Data/00000157.DAT										
	🕀 🚺 Cain (39)	Cain (39)				X-Newsreader: Microsoft «Outlook Express« 6.00.2800.14 /img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000157.DAT									
	- 📜 CHAT (2)		00000158.DAT	B.DAT Schewerzeider: Microsoft «Childock Entresses 6.00.2800.14 (mm. SCHARDT.001.(vol. vol2/Dimoram Electanent/Data/00000158.DAT											
	🕀 📕 Common Files (8)		monosts par												
	<ul> <li>— Description Complus Applications (2)</li> </ul>		00000158.DA1	UUUUU125.DAT X-hewsreader: microsoft «Outbook Express» 6.00.2200.14 jmg_dbell Latitude Ch.201/vol_vol2/hogram https/Agent/Data/UUUU155.DAT v											
	🕀 🛃 DirectX (3)		<							>					
	🕀 🍌 Ethereal (45)														
	🐵 📕 Faber Toys (10)		Hex Text Application Message File Metadata	Hex Text Application Message File Metadata Context Results Annotations Other Occurrences Video Triage											
	GlobalSCAPE (3)		Strings Indexed Text Translation												
	Internet Explorer (10)		Matches on page: 1 of 1 Match -	Page: 1 of 6 P	age ( ->	100% 🗩 🗩 F	leset		Text Source: Sea	rch Results 🗸 🗸					
	Look@LAN (18)														
	Messenger (14)		X-Newsreader: Microsoft Outlook Exp	ess 6.00.2800.1437						^					
	microsoft montpage (3)		X-MIMEOLE: Produced By Microsoft Min	#OLE V6.00.2800.1441											
	miRC (10)		Xref: newsmst0la.news.prodigy.com al	t.2600.hackerz:26550	57										
	MCN (4)		in UPPER CASE or lower case?												
	MSN Gamine Zona (3)		"Rhaevn" <rhaevn@hotmail.com> wrote</rhaevn@hotmail.com>	in message											
	NetWeeting (23)		news:1DGMc.46677\$Gf7.1692139@news20.	bellglobal.com											
	Network Stumbler (15)		> well holy 8#\$!8%^ !												
	Online Services (5)		> why didnt i think of that to begin	with?											
	Outlook Express (14)		> shit, 1 must be in the forest F'n	oump newsgroup if s	someone thought	1									
	- PLUSI (4)		> guess a little genie sent this em	il for me huh?											
	- Uninstall Information (20)		> can you say "a, b, c "?												
	- 😺 Whois (8)		> "kyralea" <kyra@cotse.com> wrote :</kyra@cotse.com>	n message											
	🕀 🚺 Windows Media Player (15)		<pre>&gt; news:chFMc.24772\$eM2.10701@attbi_s</pre>	51											
	🕢 〕 Windows NT (7)	~	> > Rhaevn wrote:							*					

Picture 22:MS Outlook Express

SCHARDT_010720	020 - Autopsy 4.15.0 Vindow Help				- 0 ×
🐈 Add Data Sourc	ce 📠 Images/Videos 🔣 Commu	nications 💡 Geolocation 🗮 Timeline 縜 File Discov	ery 📓 Generate Report 🧕 Close Case	•	Keyword Lists     Qr Keyword Search
€ ⇒		C TP Keyword search 3 - NNTP × Keyword	search 4 - news.dallas.sb × Keyword search 5 - forte agent ×	Keyword search 6 - MS Outlook Exp × Keyword search 7 - Out	took Expres X 4 ) 🔻
- 100 VO	ol1 (Unallocated: 0-62)	Table Thumboail			35 Resu
₽-10 VO	2 (NTFS / exFAT (0x07): 63-9510479				Save Table ac CSV
V	SOrphannies (0)				Sore rook of Cor
	Section (5)	△ Name	Keyword Preview	Location	Modified Time C
	Sunaloc (4)	b0019813.ppt	d04>X-Newsreader: «Forte Agent« 2.0/32.640MIME-	-Versi /img_4Dell Latitude CPI.E01/vol_vol2//\$CarvedFiles/b0019813	3.ppt 0000-00-00 00:00:00 00
i i i i i i i i i i i i i i i i i i i	Documents and Settings (7)	b0081777.doc	oʻlpa4`Ina ta@[%«Forte Agent« 1.9 Release.A	Agent 1 /img_4Dell Latitude CPi.E01/vol_vol2//\$CarvedFiles/b0081777	7.doc 0000-00-00 00:00:00 00
1 I I I	My Documents (11)	b0346561.lnk	net>X-Newsreader: «Forte Agent« 1.91/32.564X-No	-Archi /mg_4Dell Latitude CPi.E01/vol_vol2//\$CarvedFiles/b0346561	1.lnk 0000-00-00 00:00:00 00
e- 🚺	Program Files (36)	emailferret.exe	"AcentName"=string:"«Forte Acent«""AcentLocTyce"	"=nu /img_4Dell Latitude CPI.E01/vol_vol2/Mv Documents/ENLIMER	ATI 2000-10-19 23:18:02 GMT+05:00 20
	123WASP (9)	m m332503 reg	DriverceDrivercEOPTEx/23/Enrie Agent/(0)/Driverce	ADrivers / Imm. 4Dell Latitude CDI ED1/vol. vol2//#CarvadElac/E0332503	steg 0000-00-00 00-00-00 00
۲	- 🕌 Accessories (3)	- Instanting	La resta de	ADTITOTS / Mig_tool backade criteor/toi_toic/jpca real tostcoccos	
۲	- 📙 Agent (20)	readme.txt	readme.txt «Porte Agent« 1.9 Release.Agent 1.9 is t	.ne /mg_SCHARD1.uu1/vol_vol2/Program Piles/Agenc/readme.txt	1 2002-01-25 01:04:54 GMT+05:00 20
	Anonymizer (6)	readme.txt	readme.txt «Forte Agent« 1.9 Release.Agent 1.9 is t	.he /img_4Dell Latitude CPI.E01/vol_vol2/Program Files/Agent/rea	rdm 2002-01-25 01:04:54 GMT+05:00 20
(D)	Cain (39)	i smdata.dat	comCommNet Program«Forte Agent«ftp.forteinc.com	<pre>./pub/ /img_SCHARDT.001/vol_vol2/Program Files/GlobalSCAPE/Cute</pre>	eFT 1999-06-10 20:54:14 GMT+05:00 20
	CHAT (2)	📑 smdata.dat	comCommNet Program«Forte Agent«ftp.forteinc.com	/pub/ /img_4Dell Latitude CPI.E01/vol_vol2/Program Files/GlobalSCA	4PE/ 1999-06-10 20:54:14 GMT+05:00 20
۲	Common Files (8)	📑 software	383-00C04FBD7C09). «Forte Agent« & Forte Free Ag	entrFl /img_4Dell Latitude CPi.E01/vol_vol2/WINDOW5/repair/softw-	vare 2004-08-20 03:49:11 GMT+05:00 20
	Directly (2)	<			>
	Ethereal (45)				
	Ether Toys (10)	Hex Text Application Message File Metadata	Context Results Annotations Other Occurrences Video Triage		
(e)	GlobalSCAPE (3)	Stringer Indexed Text Translation			
	Internet Explorer (10)	Sungs indexed feat intribution			
	Look@LAN (18)	Matches on page: 1 of 1 Match	Page: 1 of 1 Page - 100% 9 9	Reset	Text Source: Search Results ~
	Messenger (14)	readme tyt Forte Scent 1 9 Delease			
	microsoft frontpage (3)	reduction and reduce ingene and herease.			i i i i i i i i i i i i i i i i i i i
	J mIRC (16)	Agent 1.9 is the official release w	ersion of Forte's commercial		
	Movie Maker (8)	newsreader. This version fixes a n	umber of problems reported		1
۲	- 📕 MSN (4)	by Agent users.			
۲	MSN Gaming Zone (3)	For full details on what's contained	d in this new version plasse		
	NetMeeting (23)	consult the Release Notes in Agent'	s online help. (Simply select		
	Network Stumbler (15)	Menu option Help   Release Notes.)			
۲	Online Services (5)				
	Uutlook Express (14)	Agent 1.9 is available as "trialwar	e." If you are not sure you want		
	- DUS! (4)	to purchase Agent, you can use Agen	t for 30 days at no cost. After		
	Uninstall Information (20)	your trialware 30 days have expired	you can still read your retrieved		
	whois (8)	messages, but agent will no longer	support any online operations.		
	windows Media Player (15)	You can purchase Agent at any time	during or after the trialware		
1 1 1 1	weidows N1 (7)	×			

Picture 23:Forte Agent
20. List 5 newsgroups that Mr. Evil has subscribed to. News Groups found:

- a. alt.2600.phreakz
- b. alt.2600
- c. alt.2600.cardz
- d. alt.2600codez
- e. alt.2600.crackz
- f. alt.2600.moderated
- g. alt.binaries.hacking.utilities
- h. alt.stupidity.hackers.malicious
- i. free.binaries.hackers.malicious
- j. free.binaries.hacking.talentless.troll\_haven
- k. free.binaries.hacking.talentless.troll-haven
- l. alt.nl.binaries.hack
- m. free.binaries.hacking.beginner
- n. free.binaries.hacking.computers
- o. free.binaries.hacking.utilities
- p. free.binaries.hacking.websites
- q. alt.binaries.hacking.computers
- r. alt.binaries.hacking.websites
- s. alt.dss.hack
- t. alt.binaries.hacking.beginner
- u. alt.hacking
- v. alt.2600.programz
- w. alt.2600.hackerz

🕨 Add Data Source 📠 Images/Videos 🐹 Communications	💡 Geolocation 🗮 Timeline 📕 File Discovery 📗	Generat	e Repo	rt 🍙 Close Case			👁 • Keyword Lists 🛛 🔍	Keyword Search
6.3 0	Listing Keyword search 1 - newsgroups X							( ) + c
titude CRI E01	/mg_4Dell Latitude CPi.E01/vol_vol2/Documents and Setting	ps/Mr. Evil/L	ocal Se	ttings/Application Data/Identities/{EF	086998-1115-4ECD-9813-9ADC06784	929}/Microsoft/Outlook Express		31 Result
a Source Files	Table Thumbnail							
4Del Latitude CPI.E01							5	ave Table as CSV
vol1 (Unallocated: 0-62)	Name	s	0	Modified Time	Change Time	Access Time	Created Time	Size 😽
vol2 (NTFS / exFAT (0x07): 63-9510479)	alt.2600.codez.dbx		4	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:18:44 GMT+05:00	142036
ScarvedEles (995)	alt.2600.crackz.dbx		4	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:18:46 GMT+05:00	469716
SExtend (5)	alt.2600.dbx		4	2004-08-21 02:27:23 GMT+05:00	2004-08-21 02:27:23 GMT+05:00	2004-08-21 02:27:23 GMT+05:00	2004-08-21 02:18:32 GMT+05:00	600788
SUnalloc (4)	alt.2600.hackerz.dbx		4	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:25:57 GMT+05:00	469716
Documents and Settings (7)	alt.2600.moderated.dbx		4	2004-08-21 02:19:20 GMT+05:00	2004-08-21 02:19:20 GMT+05:00	2004-08-21 02:19:20 GMT+05:00	2004-08-21 02:19:15 GMT+05:00	76500
All Users (9)     Default Lizer (99)	alt.2600.phreakz.dbx		4	2004-08-21 02:27:10 GMT+05:00	2004-08-21 02:27:10 GMT+05:00	2004-08-21 02:27:10 GMT+05:00	2004-08-21 02:25:09 GMT+05:00	273108
LocalService (8)	alt.2600.programz.dbx		4	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:24:25 GMT+05:00	207572
🗐 📜 Mr. Evil (19)	alt.binaries.hacking.beginner.dbx		4	2004-08-21 02:23:41 GMT+05:00	2004-08-21 02:23:41 GMT+05:00	2004-08-21 02:23:41 GMT+05:00	2004-08-21 02:22:54 GMT+05:00	600788
Application Data (6)	alt.binaries.hacking.computers.dbx		4	2004-08-21 02:20:55 GMT+05:00	2004-08-21 02:20:55 GMT+05:00	2004-08-21 02:20:55 GMT+05:00	2004-08-21 02:20:36 GMT+05:00	76500
Cookies (27)	alt.binaries.hacking.utilities.dbx		4	2004-08-21 02:19:24 GMT+05:00	2004-08-21 02:19:24 GMT+05:00	2004-08-21 02:19:24 GMT+05:00	2004-08-21 02:19:22 GMT+05:00	76500
Eavorites (6)	alt.binaries.hacking.websites.dbx		4	2004-08-21 02:20:50 GMT+05:00	2004-08-21 02:20:50 GMT+05:00	2004-08-21 02:20:50 GMT+05:00	2004-08-21 02:20:42 GMT+05:00	76500
E- Local Settings (7)	alt.dss.hack.dbx		4	2004-08-21 02:22:54 GMT+05:00	2004-08-21 02:22:54 GMT+05:00	2004-08-21 02:22:54 GMT+05:00	2004-08-21 02:20:55 GMT+05:00	600788
- DApplication Data (5)	alt.hacking.dbx		4	2004-08-21 02:27:07 GMT+05:00	2004-08-21 02:27:07 GMT+05:00	2004-08-21 02:27:07 GMT+05:00	2004-08-21 02:23:41 GMT+05:00	535252
😑 🔑 Identities (3)	alt.nl.binaries.hack.dbx		4	2004-08-21 02:20:34 GMT+05:00	2004-08-21 02:20:34 GMT+05:00	2004-08-21 02:20:34 GMT+05:00	2004-08-21 02:19:52 GMT+05:00	76500
E- (EF086998-1115-4ECD-9B13-9AL	alt.stupidity.hackers.malicious.dbx		4	2004-08-21 02:19:27 GMT+05:00	2004-08-21 02:19:27 GMT+05:00	2004-08-21 02:19:27 GMT+05:00	2004-08-21 02:19:25 GMT+05:00	76500
Outlook Express (31)	deanup.log		4	2004-08-21 02:13:58 GMT+05:00	2004-08-21 02:13:58 GMT+05:00	2004-08-21 02:13:58 GMT+05:00	2004-08-21 02:13:55 GMT+05:00	962
	Deleted Items.dbx		4	2004-08-21 02:18:30 GMT+05:00	2004-08-21 02:18:30 GMT+05:00	2004-08-21 02:18:30 GMT+05:00	2004-08-21 02:18:30 GMT+05:00	142036
⊕- 😼 History (4)	Folders.dbx		4	2004-08-21 02:25:59 GMT+05:00	2004-08-21 02:25:59 GMT+05:00	2004-08-21 02:13:57 GMT+05:00	2004-08-21 02:13:25 GMT+05:00	4072416
⊕- 🔑 Temp (6)	free, binaries, hackers, malicious, dbx		4	2004-08-21 02:19:31 GMT+05:00	2004-08-21 02:19:31 GMT+05:00	2004-08-21 02:19:31 GMT+05:00	2004-08-21 02:19:29 GMT+05:00	76500
Temporary Internet Piles (4)	free, binaries, hacking, beginner, dbx		4	2004-08-21 02:20:14 GMT+05:00	2004-08-21 02:20:14 GMT+05:00	2004-08-21 02:20:14 GMT+05:00	2004-08-21 02:20:09 GMT+05:00	76500
B NetHood (9)	free.binaries.hacking.computers.dbx		4	2004-08-21 02:20:21 GMT+05:00	2004-08-21 02:20:21 GMT+05:00	2004-08-21 02:20:21 GMT+05:00	2004-08-21 02:20:14 GMT+05:00	76500
	free.binaries.hacking.talentless.troll-haven.dbx		4	2004-08-21 02:19:38 GMT+05:00	2004-08-21 02:19:38 GMT+05:00	2004-08-21 02:19:38 GMT+05:00	2004-08-21 02:19:37 GMT+05:00	76500
	free binaries hacking talentless troll haven dbx		4	2004-08-21 02:19:35 GMT+05:00	2004-08-21 02:19:35 GMT+05:00	2004-08-21 02:19:35 GMT+05:00	2004-08-21 02:19:33 GMT+05:00	76500
SendTo (7)	free.binaries.hadking.utilities.dbx		4	2004-08-21 02:20:26 GMT+05:00	2004-08-21 02:20:26 GMT+05:00	2004-08-21 02:20:26 GMT+05:00	2004-08-21 02:20:21 GMT+05:00	76500
Emplates (14)	free.binaries.hacking.websites.dbx		4	2004-08-21 02:20:31 GMT+05:00	2004-08-21 02:20:31 GMT+05:00	2004-08-21 02:20:31 GMT+05:00	2004-08-21 02:20:26 GMT+05:00	76500
NetworkService (8)	Tahay day			2004 00 21 02:10:22 CMT LODIOD	2004 00 21 02:10:22 CMT : 0E:00	2004 00 21 02:10:22 CMT ( 05:00	2004 00 21 02:12:25 CMT LOS:00	1 100076 V

Picture 24:Newsgroups

- **21.** A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?
  - a. user=**Mini Me**
  - b. email=**none@of.ya**
  - c. nick=**Mr**
  - d. anick=mrevilrulez

	4	Listing Keyword se	arch 5 - mIRC	c >	Keyword search 6 - user=Mini M	e X			
	\$CarvedFiles (995) \$Extend (5)	/img_4Dell Latitude CPi.E0: Table Thumbnail	L/vol_vol2/Pro	ogram	Files/mIRC				
•	\$Unalloc (4) Documents and Settings (7)	Name	s c	0	Modified Time	Change Time	Access Time	Created Time	Size
	My Documents (11) Program Files (35)	ircintro.hlp		4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	69423
TT	123WASP (9)	mirc.exe		4	2004-08-20 20:09:55 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-25 21:20:27 GMT+05:00	2004-08-20 20:09:55 GMT+05:00	1867776
	Accessories (3)	mirc.hlp		4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	224213
	Agent (20)	mirc.ini		4	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	5483
	Anonymizer (6)	🖲 popups.ini		4	2004-08-20 20:09:56 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2568
197	CHAT (2)	readme.txt		4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	1104
	Common Files (8)	i servers.ini		4	2004-08-21 00:16:33 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	31500
	ComPlus Applications (2)	🐻 urls.ini		4	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	355
	DirectX (3) Ethereal (45)	<							
	GlobalSCAPE (3)	Hex Text Application	Message Fi	ile Met	tadata Context Results Annot	ations Other Occurrences Video Triag	6		
	Internet Explorer (10)	Strings Indexed Text	Translation						
۲	Look@LAN (18)	Matches on page: -	of - M	atch	← → Page: 1 of 1	Page - 100% (9)	① Reset		Text Sou
•	Messenger (14)     microsoft frontpage (3)     miRC (15)     download (2)     logs (14)     logs (14)	private=1,1,1,1 other=1,1,1,1,1,1, pos=20,20 [mirc] user=Mini Me email=none@of_ya nick=Mr	1						



- **22.** This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed. IRC Channels found are:
  - a. Chataholics.undernet.log
  - b. Chataholics.undernet.log
  - c. Cybercafé.undernet.log
  - d. Elite.hackers.undernet.log
  - e. evilfork.efnet.log
  - f. funny.undernet.log
  - g. houston.undernet.log
  - h. Iso-warez.efnet.log
  - i. Luxshell.undernet.log
  - j. mp3xserv.undernet.log
  - k. thedarktower.afternet.log
  - l. ushells.undernet.log
  - m. m5tar.undernet.log

ase View Tool	072020 - Autopsy 4.15.0 Is Window Help								
🛖 Add Data S	Source 📠 Images/Videos 🔣 Comm	nunications 💡 Geolocation 🗮 Timeline 🚚 Fil	le Discove	ery	Generate Report 👩 Close Cas	e		🐼 💿 🕶 Keyword I	Lists
€ ⇒	f an ad Elar (00E)	Listing Keyword search 5 - mIRC /mg_4Dell Latitude CPi.E01/vol_vol2/Progra	× Key am Files/n	/word s nIRC/lo	earch 6 - user =Mini Me X gs				
	Scarvednies (555) \$Extend (5) \$Unalloc (4)	Table Thumbnail							
Œ	Documents and Settings (7)	Name	s d	с о	Modified Time	Change Time	Access Time	Created Time	Size
	My Documents (11)	(current folder)			2004-08-20 20:24:48 GMT+05:00	2004-08-20 20:24:48 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-20 20:24:48 GMT+05:00	56
	123WASP (9)	Darent folder]			2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-20 20:09:53 GMT+05:00	56
	- Accessories (3)	#Chataholics.UnderNet.log		4	2004-08-20 20:54:11 GMT+05:00	2004-08-20 20:54:11 GMT+05:00	2004-08-20 20:54:11 GMT+05:00	2004-08-20 20:52:09 GMT+05:00	688
	🕀 🕌 Agent (20)	#CyberCafe.UnderNet.log		4	2004-08-21 00:02:55 GMT+05:00	2004-08-21 00:02:55 GMT+05:00	2004-08-21 00:02:55 GMT+05:00	2004-08-20 20:54:21 GMT+05:00	9373
	Anonymizer (6)	#Elite.Hackers.UnderNet.log		4	2004-08-20 20:49:05 GMT+05:00	2004-08-20 20:49:05 GMT+05:00	2004-08-20 20:49:05 GMT+05:00	2004-08-20 20:45:34 GMT+05:00	464
	① Cain (39)	#evilfork.EFnet.log		4	2004-08-20 20:31:07 GMT+05:00	2004-08-20 20:31:07 GMT+05:00	2004-08-20 20:31:07 GMT+05:00	2004-08-20 20:30:18 GMT+05:00	335
	Common Files (8)	#funny.UnderNet.log		4	2004-08-21 00:28:14 GMT+05:00	2004-08-21 00:28:14 GMT+05:00	2004-08-21 00:28:14 GMT+05:00	2004-08-21 00:26:18 GMT+05:00	263
	- D ComPlus Applications (2)	#houston.UnderNet.log		4	2004-08-20 20:52:01 GMT+05:00	2004-08-20 20:52:01 GMT+05:00	2004-08-20 20:52:01 GMT+05:00	2004-08-20 20:48:59 GMT+05:00	265
	🐵 📙 DirectX (3)	#ISO-WAREZ.EFnet.log		4	2004-08-20 20:29:42 GMT+05:00	2004-08-20 20:29:42 GMT+05:00	2004-08-20 20:29:42 GMT+05:00	2004-08-20 20:29:01 GMT+05:00	148
	Ethereal (45)     Ethereal (45)	#LuxShell.UnderNet.log		4	2004-08-20 20:43:21 GMT+05:00	2004-08-20 20:43:21 GMT+05:00	2004-08-20 20:43:21 GMT+05:00	2004-08-20 20:42:03 GMT+05:00	589
	Faber Toys (10)	#mp3xserv.UnderNet.log		4	2004-08-20 20:44:32 GMT+05:00	2004-08-20 20:44:32 GMT+05:00	2004-08-20 20:44:32 GMT+05:00	2004-08-20 20:43:16 GMT+05:00	1283
	Internet Explorer (10)	#thedarktower.AfterNET.log		4	2004-08-21 00:16:23 GMT+05:00	2004-08-21 00:16:23 GMT+05:00	2004-08-21 00:16:23 GMT+05:00	2004-08-21 00:14:45 GMT+05:00	578
	B- 1 Look@LAN (18)	#ushells.UnderNet.log		4	2004-08-20 20:45:07 GMT+05:00	2004-08-20 20:45:07 GMT+05:00	2004-08-20 20:45:07 GMT+05:00	2004-08-20 20:44:49 GMT+05:00	284
	- 📜 Messenger (14)	mStar LinderNet log		4	2004-08-20 21:00:08 GMT+05:00	2004-08-20 21-00-08 GMT+05-00	2004-08-20 21:00:08 GMT+05:00	2004-08-20 20:54:55 GMT+05:00	285
	microsoft frontpage (3)	<			2001-00-20-21:00:00-0111-00:00	2001-00-20 21:00100 0111100100	200700-20 21:00:00 01:1100:00	2001-00-20 20/01/00 00/11/00/00	200
						(			_
	download (2)	Hex Text Application Message File M	Metadata	Cont	ext Results Annotations Other O	courrences Video Triage			
	sounds (2)	Strings Indexed Text Translation		21.1					100
	- 🖟 Movie Maker (8)	Matches on page: - of - Match	h < 🦻	2	Page: 1 of 1 Page 🗧 🤿	100% (🗩 )🕀 Rese	et .	Text Sou	urce: Fi
	B         MSN (4)           MSN (4)         MIN (4)           MSN (4)         MIN (4)           MIN (4)         MIN (4)           MIN (4)         MIN (4)           MIN (4)         MIN (4)	<pre>[10:52] * Topic is 'thigheave [10:52] * So by X on Med Aug [10:52] * So by X on Med Aug [10:52] * Joins: 'Sonehead (- 10:53] * Joins: Wgsa30 (wolf [10:53] * Joins: Wgsa30 (wolf [10:53] * Parts: presed (-coo [10:53] * Parts: presed (-coo [10:53] * Carts: DjMenica () [10:53] * Quits: DjMenica () Session Close: Fri Aug 20 10:</pre>	m) Lif 18 02 over@2 30@ads 30@ads 1 user 10 nouil@ 54:11	e is :49:0 02.13 203.1 1015. 1007. @203. 82.20 2004	what happens when you plan 6 1.116.123) 35.35.220) r28-dbg2.vie.at.eu.net^) ( r24-bbg2.vie.AT.KDMQuest.n 10.156.161) 8.166.157^) (Quit^)	a to do other things^' Ping timecut^) (et)			

**23.** Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and reassembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data? The file is **Interception** 

4 3	A Listing	Keyword search	5 - mIR	c ×	Keyword search 6 - user -Mini Me	×				
\$CarvedFiles (995)     \$Extend (5)     \$Unaloc (4)	/img_4Dell L Table Th	atitude CPi.E01/vol_ umbnail	vol2/De	cumen	ts and Settings/Mr. Evil					
Documents and Settings (7)     All Users (9)	Name		s	c o	Modified Time	Change Time	Access Time	Created Time	Size	Flag
Default User (98)	Start	Menu			2004-08-19 22:00:09 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-27 20:08:06 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	256	Allo
E LocalService (8)	📜 Temp	ates			2004-08-20 03:24:35 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-20 20:17:59 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	56	Alloc
Amicaton Data (6)	gtk-2	ookmarks		0	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	0	Aloc
Coolies (27)	intero	eption		4	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	173372	Alloc
B- Desktop (3)	NTUS	R.DAT		4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:13 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	786432	Alloc
Favorites (6)	ntuse	.dat.LOG		4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	1024	Alloc
E Local Settings (7)	(iii) ntuse	ini		0	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20.04:04:08 GMT+05:00	180	Alloc
My Music (4)	۲.									
Wy Pictures (4)	Hex Text	Application Mesi	age F	ie Met	adata Context Results Annotatio	ns Other Occurrences Video Triage	5			
PrintHood (2)	Strings I	idexed Text Trans	ation							
- 🔛 Recent (11)	Matches	n page: - of	• N	latch	Page: 1 of 5 Page: 1 of 5 Page	pe ← → 100% Ø Ø	Reset		Text Source	e: File

Picture 27:Re-assembled packets file

24. Viewing the file in a text format reveals much information about who and what was intercepted. What type of wireless computer was the victim (person who had his internet surfing recorded) using? Windows CE (Pocket PC)



Picture 28: Victim's wireless computer

#### 25. What websites was the victim accessing?

- a. Mobile.msn.com
- b. msn(hotmail) email

		~ 01								· NEYHOLD LIS		e neyword dea	
÷ 0	Listing Keyword search	5 - mIR	c ×	Keyword search 6 - user=Mini Me	e ×							( )	• •
4Dell Latitude CPi.E01	/mg_4Dell Latitude CPi.E01/vol	_vol2/Do	cumen	ts and Settings/Mr. Evil								19	Results
Data Source Files	Table Inditional											C	001
ADell Latitude CPI.E01												Save Table as	CSV
vol1 (Unallocated: 0-62)	Name	S (	0	Modified Time	Change Time		Access Time		Created Time	Size	Flags(Dir)	Flags(Meta)	Kr
SOrphanFiles (0)	Start Mercu			2004-08-19 22:00:09 GMT+05:00	2004-08-20 04-	04-06 GMT+05-00	2004-08-27 20	-08-06 GMT+05-00	2004-08-20-04-04-05 (MT+05-00	256	Allocated	Allocated	-
\$CarvedFiles (995)	Tamplatae			2004-08-20 03-24-35 CMT+05-00	2004-08-20 04	04:06 CMT+05:00	2004-08-20 20	17:50 CMT+05:00	2004-08-20 04-04-05 GMT+05-00	EG	Allocated	Allocated	
	atk baskmarks		0	2004-08-27 20:40:42 CMT+05:00	2004-09-27 20	40.42 CMT+05.00	2004-00-20-20	40-42 CMT+05-00	2004-08-27 20:40:43 GMT+05:00	0	Allocated	Allocated	ka
SUnalloc (4)	got-bookmarks			2004-05-27 20.40.45 GHT 405.00	2004-00-27 20.	40.45 001 +05.00	2004-00-27 20		2001-00-27 20:40:43 GHT+05:00		Miocated	MICCALED	NU
Documents and Settings (7)	interception		4	2004-08-27 20:41:00 GM1+05:00	1 2004-08-27 20:	41:00 GM1+05:00	2004-08-27 20	:41:00 GM1+05:00	2004-08-27 20:41:00 GM1+05:00	1/33/2	Allocated	Allocated	un
All Users (9)	NTUSER.DAT		4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:	46:13 GMT+05:00	2004-08-27 20	:46:23 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	786432	Allocated	Allocated	un
B- LocalService (8)	ntuser.dat.LOG		4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:	46:23 GMT+05:00	2004-08-27 20	:46:23 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	1024	Allocated	Allocated	un
- Mr. Evil (19)	ntuser.ini		0	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:	46:23 GMT+05:00	2004-08-27 20	:46:23 GMT+05:00	2004-08-20 04:04:08 GMT+05:00	180	Allocated	Allocated	kn 🖌
Cookies (27)	Hex Text Application Mes	sage F	ie Met	adata Context Results Annota	tions Other Occurr	ences Video Triago	e						
Desktop (3)     Eavorites (6)	Strings Indexed Text Tran	slation	110.1110.1				- 1.						
E- Local Settings (7)	Matches on page: - of	- M	atch	← → Page: 1 of 5 1	Page 🗧 🔶	100% Ø\$	① Reset	]		Text Sour	e: File Text		~
	Referer: http://mobil UA-Language: JavaScri Accept-Encoding: grig User-Agent: Mosilla/ Host: mobile.msn.com Connection: Keep-Alin Cookie: lc=en-US; crr MSPProf=5ynN;922m513	le.msn lpt b, def: 1.0 (co re =1; MSI (QzUnhi	com/	hm/folder.aspx?ts=109360. ible; MSIE 4.01; Windows =5vuMneQNFDh0sFVrAbKrt*q mrXHUam6W2H3bXqJqZESuF27( qr1EV0.0MMs	CE; PPC; 240x ce; PPC; 240x edOGfSSmKz131 DFVIdTd0zwZL2f	664556folder⇒} 320) flClh6FdbNqQyJ LhhQB8q*Sto505	ACTIVE&msg=0 PyqubrB97DYRu 8d!UJp8ulXjB8	10T⊮oA5kpliId3¢ ;g4RJME!*WBUVqv	aIZ3TUiZ45LQ≎3; r#UvAhSUu£lyJHTMQt*6C4vjOy	vqgDT6F1XA	1jAg01		^

Picture 29:mobile.msn.com

Coll Latitude CPI.ED1     Voll (Unalocated: 0-62)     Voll (	ting Keyword search Oell Latitude CPi.E01/vol ble Thumbnail me Start Menu	s 5 - mli _vol2/D	C X	Keyword search 6 - user =Mini Me ts and Settings/Mr. Evil	×					<	-
40el Latitude CPI.E01	Latitude CPI.E0 1/vol ble Thumbnail me Start Menu	_vol2/D	ocumen	ts and Settings/Mr. Evil							
→         Data Source Files           →         →	me	s								19	Results
	me Start Menu	s								Cause Table as	CC14
	Start Menu	S								Save rable as	CSV
SOrphanFiles (0)     SCarvedFiles (995)     SExtend (5)     Sunaloc (4)	Start Menu		C O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kr
				2004-08-19 22:00:09 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-27 20:08:06 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	256	Allocated	Allocated	un ^
SExtend (5)	Templates			2004-08-20 03:24:35 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-20 20:17:59 GMT+05:00	2004-08-20.04:04:05 GMT+05:00	56	Allocated	Allocated	10
SUnalloc (4)	atk-bookmarks		0	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	0	Allocated	Allocated	kn
	interception		4	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 CMT+05:00	2004-08-27 20:41:00 CMT+05:00	2004-08-27 20:41:00 CMT+05:00	173372	Allocated	Allocated	100
Documents and Settings (7)	MTUSED DAT		4	2004-08-27 20:46:22 CMT+05:00	2004-09-27 20:46:13 CMT±05:00	2004-09-27 20:46+22 GMT±05:00	2004-09-20 04-04-05 CMT+05-00	706422	Allocated	Allocated	10
Default User (98)	at an dat LOC		4	2001-00-27 20:40:23 GHT+05:00	2001-00-27 20:40:13 GHT+05:00	2004-00-27 20:40:23 GMT+05:00	2001-08-20 04:04:05 GMT+05:00	100402	Allegated	Allegated	Carl
⊕- 📜 LocalService (8)	huser lat.cog		4	2001-00-27 20:40:23 0111-05:00	2004-00-27 20:40:23 GHT+05:00	2004-00-27 20:40:20 GMT+00:00	2001-00-20 04:04:00 GHT+05:00	1004	Allecated	Allerated	- La
😑 🔒 Mr. Evil (19)	ý nuser in		U	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-00-27 20:46:23 GM1+05:00	2004-08-20 04:04:08 GP11+05:00	100	MEDCACED	Asocaceu	NI Y
Application Data (6)											<i>.</i>
Cookies (27)	Text Application Mes	isage:	File Met	adata Context Results Annotatio	ns Other Occurrences Video Triage						
Eavorites (6)	rings Indexed Text Tran	slation									_
⊕ B Local Settings (7)	latches on pages		Match	A A Dama 1 of 5 Da	- 4 A 1008 Q (	Paret		Taxt Cours	Ele Text		
- D My Documents (6)	atches on page. • or	0.0	Hatun	rage: 1 01 5 Fa	100 % D 1	U Reset		TEXT SOULC	rie lext		~
- 🥦 My Music (4) X-	Powered-By: ASP.NET	r									^
My Pictures (4) P3	P: CP="BUS CUR CON che-Control: privat	o FIN	IVDo	ONL OUR PHY SAMo TELO"							
Printiland (2)	ntent-Type: text/ht	aml; o	harse	t=utf-8							
Recent (1)	ntent-Length: 7983 pires: -1										
	tml>										
🕀 🔒 Start Menu (4)	ead>	125000									
- D Templates (14)	head>	1016-	•								
NetworkService (8) <s< td=""><td>tyle&gt;.text (font-fa</td><td>amily</td><td>Tahom</td><td>a;font-size:llpx;color:#00</td><td>0080;}A {color:#0000FF;}A:</td><td>Hover {text-decoration:non</td><td>e;}A.header {color:#000080</td><td>;}A.header</td><td>::Hover {t</td><td>ext-</td><td></td></s<>	tyle>.text (font-fa	amily	Tahom	a;font-size:llpx;color:#00	0080;}A {color:#0000FF;}A:	Hover {text-decoration:non	e;}A.header {color:#000080	;}A.header	::Hover {t	ext-	
⊕- 📜 My Documents (11) de	coration:underline;	}.hea	der (	font-family:Tahoma; font-si	ze:11px;color:#000080;font	-weight:bold; }.columnheade	r {font-family:Tahoma; font	-size:11ps	; font-wei	.ght:bold;	
Program Files (36)     fa	mily:Tahoma; font-s:	ze:11	px; fo	nt-weight:bold;color:#0000	80]A.toolbar (text-decorat	ion:none; }A.toolbar:Hover	{color:#0000FF;text-decora	tion:under	cline; }.bu	itton (font-	
B B RECYCLER (3) fa	mily:Tahoma, sans-	serif;	font-	size:llpx;background: #D6E	7EF;border-bottom: 1px sol	id #104A7B;border-right: 1	px solid \$104A7B;border-le	ft: 1px so	olid #AFC4	D5;border-	
System Volume Information (3)	p:1px solid #AFC4D	5; colo	r:#00	0000; height: 19px; text-decc	ration:none;cursor:hand;fo	nt-weight:noraml).input (f	ont-family:Tahoma, sans-se	rif;font-s	size:llpx;	border-	2
	coom. Ipr solid #1		Dorde	i iigne, ipa soitu şiotan	, boulder lett. Ipa solid ##	action of the solution of the solution	**************************************	due : r shut e	EXC GECON	acton.none,	A.
wIN98 (103) nt	-weight:noraml}.ch	ckboz	{fon	t-family:Tahoma, sans-seri	f;font-size:llpx;color:#00	0000;text-decoration:none;	font-weight:noraml}.texta:	ea (font-f	family:Tab	oma, sans-	
E- WINDOWS (109) se	rif;font-size:llpx;	borde	r-bot	tom: 1px solid #104A7B;bor	der-right: lpx solid #104A	7B;border-left: lpx solid	#AFC4D5;border-top:lpx sol	1d #AFC4D8	;color:#0	.000000;text-	
- 🛃 addins (2)	rightmargin="0" to	opmarc	in="0	ani / TRODE . HEADIE ID (DOLUE	1-Dobcom. Bolid #55DEE2 ips	, jimple.neable ik.n	(BRONGROOND-CODOR: #C.	Derel-/sel	Are-pond	Teromergrue	

Picture 30:MSN Hotmail

#### 26. Search for the main users web-based email address. What is it? mrevilrulez@yahoo.com



Picture 31:Main user's web-based email address

**27.** Yahoo mail, a popular web based email service, saves copies of the email under what file name? **Showletter[1].htm** 



Picture 32:Showletter[1].htm

28. How many executable files are in the recycle bin? 4 executables

Add Data Source III Images/Videos 📓 Communicatio	ns V Geolocation 🔁 Tim	eline	File	Discovery hereite Report	😸 Close Case		•	<ul> <li>Keyword Lis</li> </ul>	its (	🗧 Keyword Se	arch
- > <b>O</b>	Listing Keyword sear	dh 5 - m	IRC >	Keyword search 6 - user =Mini Me	× Keyword search 7 - @yahoo.c	om ×				4	•
vol1 (Unallocated: 0-62)	Table Thumbnail	ol_vol2	RECTOL	:R/S-1-5-21-2000478354-688789844	-1/08537768-1003						s Result
vol2 (NTFS / exFAT (0x07): 63-9510479) \$OrphanFiles (0)										Save Table a	s CSV
\$CarvedFiles (995)	Name	s	с о	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
SExtend (5)	[current folder]			2004-08-27 20:29:58 GMT+05:00	2004-08-27 20:29:58 GMT+05:00	2004-08-27 20:29:58 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	56	Allocated	Allocated	unkno
SUnalloc (4)     Documents and Settings (7)	Digarent folder]			2004-08-25 21:18:25 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	2004-08-27 20:12:30 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	328	Allocated	Allocated	unkno
H Wy Documents (11)	Dc1.exe		4	2004-08-25 20:51:23 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	2004-08-25 20:56:08 GMT+05:00	2004-08-25 20:51:24 GMT+05:00	2160043	Allocated	Allocated	unkno
Program Files (36)	Dc2.exe		0	2004-08-27 20:11:07 GMT+05:00	2004-08-27 20:12:30 GMT+05:00	2004-08-27 20:12:18 GMT+05:00	2004-08-27 20:11:07 GMT+05:00	1324940	Allocated	Allocated	known
ECYCLER (3)	Dc3.exe		4	2004-08-27 20:14:20 GMT+05:00	2004-08-27 20:15:26 GMT+05:00	2004-08-27 20:15:16 GMT+05:00	2004-08-27 20:14:20 GMT+05:00	442417	Allocated	Allocated	unkno
System Volume Information (3)	Dc4.exe		4	2004-08-27 20:24:24 GMT+05:00	2004-08-27 20:29:58 GMT+05:00	2004-08-27 20:29:47 GMT+05:00	2004-08-27 20:24:24 GMT+05:00	8460502	Allocated	Allocated	unkno
Temp (2)	🗟 desktop.ini		0	2004-08-25 21:18:25 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	2004-08-27 20:12:30 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	65	Allocated	Allocated	known
	INFO2		4	2004-06-27 20:46:17 GMT+05:00	2004-08-27 20:46:17 GMT+05:00	2004-08-27 20:46:17 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	3220	Allocated	Allocated	unknow
由→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→											
vol3 (Unallocated: 9510480-9514259)	<										>
Wews											
Deleted Files	Hex Text Application M	essage	File Me	tadata Context Results Annotati	ons Other Occurrences Video Triag	e					
MB File Size	Strings Indexed Text	nslation	R.								
E Results	Matches on page: - o	f -	Match	Page: 1 of 1 Page:	age (	① Reset		Text Source	ce: File Text		~
DeviaceU Control     Section Manualth Detected (773)     Section Manualth Detected (773)     Section Manualth Detected (773)     Section Manualth Detected (773)     Section Manualth Detected (19)     Section Manualth Detected (19)     USB Device Attached (1)     Section Manualth Detected (19)     Web Cookes (24)	C:\Documents and Se C:\Documents and S C:\Documents and Se C:\Documents and Se C:\Documents and Se C:\Documents and Se C:\Documents and Se	tings ttings ttings ttings ttings ttings ttings	(\Mr. ] s\Mr. ] (\Mr. ] (\Mr. ] (\Mr. ] (\Mr. ]	<pre>Vil\Desktop\lalsetup260.et Zvil\Desktop\lalsetup250. Vil\Desktop\netstumblerin Vil\Desktop\metstumblerin Vil\Desktop\WinPcap_3_01_ Vil\Desktop\WinPcap_3_01_ Vil\Desktop\ethereal-setu Vil\Desktop\ethereal-setu</pre>	re exe staller_0_4_0.exe a.exe a.exe p-0.10.6.exe p-0.10.6.exe						

Picture 33:Executable files in the Recycle Bin

- 29. Are these files really deleted? No
- 30. How many files are actually reported to be deleted by the file system? 3
- **31.** Perform a Anti-Virus check. Are there any viruses on the computer? Yes, there is one interesting file, possible malware.



Picture 34:Possible malware

### Lessons Learned

During the investigation I had the chance to search and learn for the location of many windows files, registry entries location and build a guide for myself on how to investigate without wasting time. I hope that in the next challenge will do it better.

# Finding the Evidence - Keith Swagler

### CSI Linux Forensic Challenge Installation and setup:

Due to CSI Linux being a virtual appliance, it was relatively easy to install. Being a KVM/QEMU user and not a VirtualBox or VMWare user it was a little bit more difficult but doable. I wrote on my blog on how to do this and even wrote a script for this situation. Unfortunately, the script only works with one disk image, not multiple per file, so I had to do it the manual way. It was not more than to be expected from being a KVM user, but still I usually prefer ISO images to already built appliances.

Especially considering that many DFIR distros do double duty to run live and serve as evidence collection distros. Overall, just again a minor inconvenience.

### Extra tools installed:

- Sleuthkit
- RegRipper Fred

Sleuthkit is in the default repos, so installation is as easy as running:

### \$ sudo apt install sleuthkit

I do find it odd that Autopsy is installed and even recommended when sleuthkit was not installed. Due to its small size but huge impact, and since they are from the same author as Autopsy.

RegRipper is a Registry parser and something I find hugely

In CSI Linux 2020.3 Sleuthkit and FRED have been added and the been has RegRipper

resolved

valuable when performing Windows Forensics. I was disappointed to find that it was installed but not working

correctly for me. I ended up redownloading and following the instructions on DFIR blog to get it working again. I ended up writing a set of scripts to automate it in the future. Apparently I am behind the times and Version 3 is out, so maybe it will work easier in that version.

FRED is a Linux compatible Windows Registry viewer similar to the one found on Windows computers. When RegRipper does not have a plugin for a certain registry key, Fred is incredibly valuable.

Installation is as simple as adding the authors repo to your machine as per the instructions, and running apt install. Full commands are

\$ sudo wget -P /etc/apt/sources.list.d/ deb.pinGUIn.lu/pinGUIn.lu.list \$ wget -q deb.pinGUIn.lu/debsign\_public.key -O- | sudo apt-key add -\$ sudo apt-get update \$ sudo apt installfred

After the second boot of my CSI Linux VM Autopsy would not run for me. It was mildly frustrating as I am sure there were many answers, I missed because of it, but by the time I noticed it was too late to do much troubleshooting and meet the deadline.

There are some answers in which the files are mentioned. I mounted the image to examine the filesystem directly using the following steps.

Create directories "/mnt/schardt/" "/mnt/schardtraw"

\$ mkdir "/mnt/schardt" "/mnt/schardtraw"

When adding the image to Autopsy I disabled Plaso parser.

Find the offset of the main partition by running: mmls on SCHARDT.001

\$ mmls "/home/csi/Documents/Cases/SCHARDT.001"

csi@c DOS P	si-analys artition	t:~/Documents, Table	/Cases/CSIlin	ux\$ mmls SCHA	RDT.001
Offse	t Sector:	0			
Units	are in 5	12-byte secto	rs		
	Slot	Start	End	Length	Description
000:	Meta	00000000000	0000000000	0000000001	Primary Table (#0)
001:		00000000000	0000000062	0000000063	Unallocated
002:	000:000	0000000063	0009510479	0009510417	NTFS / exFAT (0x07)
003:		0009510480	0009514259	0000003780	Unallocated
csi@c	si-analys	t:~/Documents,	/Cases/CSIlin	ux\$	

Mount the image using affuse, which groups all of the disk images together into one "device" for other commands like mount to more easily understand.

\$ sudo affuse SCHARDT.001 "/mnt/schardt"

Using the offset we found in mmls 32256 = (the offset \* the sector size (512))

\$ sudo mount -o loop,ro,offset=32256 "/mnt/schardt/SCHARDT.001.raw" "/mnt/schardtraw" A quick note, could also be written in bash as \$((63 \* 512 )) ie

\$ sudo mount -o loop,ro,offset=\$(( 63 \* 512 ))"/mnt/schardt/SCHARDT.001.raw" "/mnt/schardtraw"

### What is the image hash? Does the acquisition and verification hash match?

The images hashes were only available for the SCHARDT images. The hash files from the acquisition log (SCHARDT.LOG) and the computed hashes do match. Also, of note images 006 and 007 are the same, leading us to believe that those images are in fact completely empty.

28a9b613d6eefe8a0515ef0a675bdebd	SCHARDT.001
c7227e7eea82d218663257397679a7c4	SCHARDT.002
ebba35acd7b8aa85a5a7c13f3dd733d2	SCHARDT.003
669b6636dcb4783fd5509c4710856c59	SCHARDT.004
c46e5760e3821522ee81e675422025bb	SCHARDT.005
99511901da2dea772005b5d0d764e750	SCHARDT.006
99511901da2dea772005b5d0d764e750	SCHARDT.007
8194a79a5356df79883ae2dc7415929f	SCHARDT.008

#### What operating system was used on the computer?

Running mmls from Sleuthkit to see the partitions on the raw disk.

csi@c DOS P Offse	si-analys artition t Sector:	t:~/Documents/ Table 0	/Cases/CSIlin	IX\$ mmls SCHA	RDT.001
Units	are in 5	12-byte secto	rs		
	Slot	Start	End	Length	Description
000:	Meta	00000000000	00000000000	0000000001	Primary Table (#0)
001:		00000000000	0000000062	0000000063	Unallocated
002:	000:000	0000000063	0009510479	0009510417	NTFS / exFAT (0x07)
003:		0009510480	0009514259	0000003780	Unallocated
csi@c	si-analys	t:~/Documents,	/Cases/CSIlin	IX\$	

As we can see the File system format is either NTFS or exFAT so it is likely a Windows OS, but we don't know what version.

Using the fsstat command using the offset that was determined by the mmls output we can see the version is reported as Windows XP.

	😺 CSIL_Forensic_Cha 🍪 Mozilla Firefox 🛛 📓 [Writeup.odt - Libr 📄 CSIlinux - File Man 🖭 Terminal - csi@csi	🖻 Terminal - csi@csi 🕅 🥥 💶 📘	07 Jun, 14:57 夰 🏭 🗐 🕘
6		CSIlinux - File Manager	×
en c	Terminal - csi@csi-analyst: ~/Documents/Cases/CSIlinux	×	Ċ
0000 000 0	File Edit View Terminal Tabs Help -f fstype: File system type (use '-f list' for supported types) -o imgoffset: The offset of the file system in the image (in sec -v: verbose output to stderr -V: Print version csi@csi-analyst:-/Occuments/Cases/CSILinux\$ fsstat -o 63 SCHARDT.001 FILE SYSTEM INFORMATION	ctors)	01 SCHARDT.002 SCHARDT.003
* * * **** **** ****	File System Type: NTFS Volume Serial Number: B26CB1CE6CB18D9B OEM Name: NTFS Version: Windows XP METADATA INFORMATION	200_ 107100	37 SCHARDT.008 SCHARDT.LOG
* [	First Cluster of MFT: 2097152 First Cluster of MFT Mirror: 4755208 Size of MFT Entries: 1024 bytes Size of Index Records: 4096 bytes Range: 0 - 12305 Root Directory: 5		
* 50 * * 50 * * 50 * * 50 *	CONTENT INFORMATION Sector Size: 512 Cluster Size: 512 Total Cluster Range: 0 - 9510415 Total Sector Range: 0 - 9510415		
* 50 * 50 * 50 * 50	SAttrDef Attribute Values: \$STANDARD INFORMATION (16) Size: 48-72 Flags: Resident \$ATTRBUTE LIST (32) Size: No Limit Flags: Non-resident \$FILE NAME (48) Size: 68-578 Flags: Resident,Index \$OBJECT_ID (64) Size: 0-256 Flags: Resident \$USWAY&SOUTP 400ACUC 7419207		
1/2 (	S) 💶 🗉 📄 💊 🌍 😳 🕄 💉 🗄 💵 🕐 🛔	🕥 🗞 🥑 🐇 💻	U.

### When was the install date?

Reference: forensics-matters.com/2018/09/15/find-out-windows-installation-date/

The install date should be under Windows NT. I instead accidentally clicked Windows and explored around a bit and found the key

SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\User Data\S-1-5-18\Products\ 0B79C053C7D38EE4AB9A00CB3B5D2472\InstallProperties

The value of key **InstallDate** is 20040819, which would indicate **August 19th, 2004**.



#### What is the timezone settings?

Central Time, currently in Daylight savings.



#### Who is the registered owner?

Using the same parent key as the install date the registered owner is Greg Schardt

WAB WEEM Windows CurrentVersion CurrentVersion App Panagement App Paths Applets Control Panel Controls Folder CSCSettings DateTime DateTime Dynamic Directory Extensions	Language LocalPackage NoModify NoRemove NoRepair ProductID Publisher Readme RegCompany ReagOwner	REG_DWORD REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_SZ REG_SZ	0x00000409 C:WINDOWS\Installer\d2a9f. 0x00000001 0x00000001 12345-111-111111-15636 Microsoft Corporation	f.msi	
WBEM Windows CurrentVersion App Paths App Paths Applets Control Folder CSCSettings DateTime Dynamic Directory Explorer Extensions	LocalPackage NoModify NoRemove NoRepair ProductID Publisher Readme RegCompany RegOwner	REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_SZ REG_SZ	C:WINDOWS\Installer\d2a9f. 0x00000001 0x00000001 0x00000001 12245-111-111111-15636 Microsoft Corporation	f.msi	
Windows	NoModify NoRemove NoRepair ProductID Publisher Readme RegCompany RegOwner	REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_SZ REG_SZ	0x00000001 0x00000001 0x00000001 12345-111-111111-15636 Microsoft Corporation		
CurrentVersion     App Management     App Paths     Applets     Control Panel     Controls Folder     CSCSettings     DateTime     Dynamic Directory     Explorer     Extensions	NoRemove NoRepair ProductID Publisher Readme RegCompany RegOwner	REG_DWORD REG_DWORD REG_SZ REG_SZ REG_SZ	0x00000001 0x00000001 12345-111-1111111-15636 Microsoft Corporation		
<ul> <li>App Paths</li> <li>Applets</li> <li>Control Panel</li> <li>Controls Folder</li> <li>CSCSettings</li> <li>DateTime</li> <li>Dynamic Directory</li> <li>Explorer</li> <li>Extensions</li> </ul>	NoRepair ProductID Publisher Readme RegCompany RegOwner	REG_DWORD REG_SZ REG_SZ REG_SZ	0x00000001 12345-111-1111111-15636 Microsoft Corporation		
<ul> <li>Applets</li> <li>Control Panel</li> <li>Controls Folder</li> <li>CSCSettings</li> <li>DateTime</li> <li>Dynamic Directory</li> <li>Explorer</li> <li>Explorer</li> <li>Extensions</li> </ul>	ProductID Publisher Readme RegCompany RegOwner	REG_SZ REG_SZ REG_SZ	12345-111-1111111-15636 Microsoft Corporation		
Control Panel     Controls Folder     CSCSettings     DateTime     Dynamic Directory     Explorer     Extensions	Publisher Readme RegCompany RegOwner	REG_SZ REG_SZ	Microsoft Corporation		
Controls Folder CSCSettings DateTime Dynamic Directory Explorer Extensions	Readme RegCompany RegOwner	REG_SZ	Microsoft Corporation		
CSCSettings DateTime Dynamic Directory Explorer Extensions	RegCompany RegOwner	NEG_32			
Date Infle     Dynamic Directory     Explorer     Extensions	RegOwner	DEC CZ	NZA		
Explorer     Extensions	Regowner	REG_3Z	Crog Schordt		
Extensions	Cine	REG_52	dreg scharut		
	Size	REG_52	0.0000001		
Group Policy	SystemComponent	REG_DWORD	0x0000001		
H32315P	URLINIOADOUL	REG_SZ			
* Installer	URLUpdateInfo	REG_SZ	0.000044.6		
Folders	Version	REG_DWORD	0x093214c6		
Secure	VersionMajor	REG_DWORD	0x0000009		
UpgradeCodes	VersionMinor	REG_DWORD	0x0000032		
<ul> <li>UserData</li> </ul>	WindowsInstaller	REG_DWORD	0x0000001		
<ul> <li>S-1-5-18</li> <li>Components</li> </ul>	Hex viewer				
<ul> <li>Products</li> </ul>	0000 00 00				int8: 0
<ul> <li>0B79C053C7D38EE4AB9A00CB3B5D24</li> </ul>					uint8: 0
Teatures InstallProperties					int16: 0
Usage					uint16: 0
111E13C6BB69CDA4C9186E3DEEDD8					
<ul> <li>Internet Settings</li> </ul>					
IPConfTSP					

#### What is the computer account name?

Using compname plugin for RegRipper we can see it is N-1A9ODN6ZXK4LQ



#### What is the primary domain name?

In the SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key we can find the DefaultDomainName is "**N-1A9ODN6ZXK4LQ**" the same as the computer name, which is common in individual installations.

Node **	Kev	Type	Value					
related.desc	AllowMultipleTSSessions	REG DWORD	0x00000001					
▹ SeCEdit	AltDefaultDomainName	REG SZ	N-1A9ODN6Z	KK4LQ				
<ul> <li>Setup</li> </ul>	AltDefaultUserName	REG SZ	Mr. Evil	•				
<ul> <li>Storage</li> <li>SycHoct</li> </ul>	AutoRestartShell	REG DWORD	0x00000001					
SystemRestore	Background	REG SZ	000					
<ul> <li>Terminal Server</li> </ul>	DebugServerCommand	REG SZ	00					
Time Zones	DefaultDomainName	REG SZ	N-1A9ODN67XK4LO					
Tracing	DefaultUserName	REG SZ	Mr. Evil					
Iserinstallable drivers	HibernationPreviouslyEnabled	REG DWORD	0x00000001					
Windows	LegalNoticeCaption	REG S7	0.00000001					
<ul> <li>Winlogon</li> </ul>	LegalNoticeText	REG SZ						
✓ GPExtensions	LogonType	REG DWORD	0x0000001					
{2553/BA6-7/A8-11D2-9B6C-0000F8080861} (2610eda5 77ef 11d2 8dc5 00c04fa21a66)	PowerdownAfterShutdown	REG S7	0					
{3610e0a5-77e1-1102-80C5-00C041a31a66} {426031c0-0b47-4852-b0ca-ac3d37bfcb39}	PenortBootOk	REG_SZ	1					
{42B5FAAE-6536-11d2-AE5A-0000F87571E3}	SEED' LL	REG_32	0.00000000					
{827D319E-6EAC-11D2-A4EA-00C04F79F83A}	Hex viewer							
{A2E30F80-D7DE-1102-BBDE-00C04F86AE3B} {B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}	0000 01 00 00 00				int8	1	1	1
{c6dc5466-785a-11d2-84d0-00c04fb169f7}					uint	:8: 1	1	
{e437bc1c-aa7d-11d2-a382-00c04f991e27}						6: 1	1	
<ul> <li>Notify</li> <li>chunt22chain</li> </ul>						16: 1	1	
cryptozonam					int3	2: 1	1	
cscdll					uint	32: 1	1	
ScCertProp					unio	ctime: 1	1970/01/01 00:00:01	1
Schedule								
Sonsi ogn								
termsrv								
wilhalloon								

### When was the last recorded computer shutdown date/time?

According to the registry the last shutdown time was. Fri Aug 27 15:46:33 2004 (UTC)



#### How many accounts are recorded (total number)?

By counting the number of accounts in samparse (see screenshot below) the computer has **5** accounts.

#### What is the account name of the user who mostly uses the computer?

RegRipper samparse plugin we can see that **Mr. Evil** has logged into the computer 15 times, while the other users have login counts of zero.



Who was the last user to logon to the computer?

According to **samparse** in the answer above **Mr. Evil** is the only user to have logged in.

A search for the name of Greg Schardt reveals multiple hits. One of these proves that Greg is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?

While I'm not certain what the first part of the questions relates to, we can see that Greg Schardt is the registered owner of the laptop and has the local account named "Mr. Evil". Given that there is only one user account on the computer as seen previously we can say that Greg Schardt is the administrator and Mr. Evil.

le <u>E</u> dit <u>R</u> eports <u>H</u> elp						
Node	•	Key	Туре	Value		
▶ WAB		Language	REG_DWORD	0x00000409		
WBEM		LocalPackage	REG_SZ	C:\WINDOWS\Installer\d	l2a9f.m	
<ul> <li>Windows</li> <li>CurrentVersion</li> </ul>		NoModify	REG_DWORD	0x0000001		
App Management	NoRemove		REG_DWORD	0x0000001		
▶ App Paths		NoRepair	REG_DWORD	0x0000001 12345-111-1111111-15636		
<ul> <li>Applets</li> </ul>		ProductID	REG_SZ			
Control Panel	Publisher Readme		REG_SZ	Microsoft Corporation	10	
Controls Folder     CSCSettings			REG SZ			
► DateTime		RegCompany REG SZ		N/A		
<ul> <li>Dynamic Directory</li> <li>Explorer</li> </ul>		RegOwner	REG SZ	Greg Schardt		
		Size	REG SZ			
Extensions		SystemComponent	REG DWORD	0x00000001		
H323TSP		URLInfoAbout	REG SZ			
Hints		URI UndateInfo	REG SZ			
<ul> <li>Installer</li> <li>Folders</li> <li>Secure</li> <li>UpgradeCodes</li> <li>UserData</li> </ul>		Version	REG DWORD	0x093214c6 0x00000009 0x00000032		
		VersionMaior	REG DWORD			
		VersionMinor	REG DWORD			
		WindowsInstaller	REG_DWORD	0x00000001		
▼ S-1-5-18		Windowstristdiler	hed_bhonb	0x0000001		
<ul> <li>Components</li> </ul>		Hex viewer				
<ul> <li>Products</li> <li>0B79C053C7D38EE4AB9A00CB3B5D2- Features</li> </ul>		0000 00 00				
Usage + 111E13C6BB69CDA4C9186E3DEEDD8 + Internet Settings IPConfTSP + MediaContentIndex + MediaContentIndex						

#### List the network cards

- Xircom CardBus Ethernet 100 + modem 56
- Compaq WL110 Wireless LAN

\$					
File Edit View Terminal Tabs Help					
csi@csi-analyst: /mnt/schardtraw/WINDOWS/system32/c ×	csi@csi-analyst: ~/Progams/RegRipper2.8 ×	csi@csi-analyst: ~/Progams/RegRipper2.8			
csi@csi-analyst:/mnt/schardtraw/WINDOWS Launching networkcards v.20080325 networkcards v.20080325 (Software) Get NetworkCards NetworkCards Microsoft\Windows NT\CurrentVersion\Net	/system32/config\$ rip.pl -r software workCards	-p networkcards			
Xircom CardBus Ethernet 100 + Modem 56 Compaq WL110 Wireless LAN PC Card [Thu csi@csi-analyst:/mnt/schardtraw/WINDOWS	(Ethernet Interface) [Thu Jan 1 00 Jan 1 00:00:00 1970] /system32/config\$	:00:00 1970]			0

### Find 6 installed programs that may be used for hacking.

Thought they are not "installed" as such there are a number of programs located under the "My Documents" folder. For a small sample this is a screenshot under the "EXPLOITATION" and "NT" folder

- Brutus
- Get Admin
- l0pht301
- lsadump2
- SMBGrind Crack
- John

There are a number of "hacking" applications installed that can be found under the Program Files directory, including 123WASP, Cain, and Anonymizer.

A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?

From the logs directory under "C:\Program Files\mIRC" the enter and exit times are

This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.

From the logs directory under "**C:\Program Files\mIRC**" there are a number of channels including #LuxShell, #CyberCafe, #Chatacholics, #Elite.Hackers, and #houston. It appears that mrevilrulez only appears to have posted in #Chataholics, #CyberCafe, and #LuxShell



Terminal - csi@csi-analyst: /mnt/schardt/Program Files/mIRC	-		×
<pre>File Edit View Terminal Tabs Help csi@csi-analyst:/mnt/schardt/Program Files/mIRC\$ grep mrevilrulez/logs/#Chataholics.UnderNet.log:[10:53] <mrevilrulez> glib marm ./logs/#CyberCafe.UnderNet.log:[10:55] <mrevilrulez> glib marm cuyk ./logs/#CyberCafe.UnderNet.log:[10:57] <mrevilrulez> hi ./logs/#CyberCafe.UnderNet.log:[11:00] <mrevilrulez>/logs/#LuxShell.UnderNet.log:[10:42] <mrevilrulez> glib smarm cuyk csi@csi-analyst:/mnt/schardt/Program Files/mIRC\$</mrevilrulez></mrevilrulez></mrevilrulez></mrevilrulez></mrevilrulez></pre>	/logs	/*	0

Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and reassembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?

The file is as stated in the question in the My Documents directory, the file is named interception.

Viewing the file in a text format reveals much information about who and what was intercepted.

# What type of wireless computer was the victim (person who had his internet surfing recorded) using?

User agent in the packet capture says that the intercepted machine is a Windows CE (Pocket PC) - Version 4.20



### What websites was the victim accessing?

After doing a grep of the file it appears most of the sites visited were mobile.msn.com and login.passport.net

### Search for the main user's web-based email address. What is it?

From the *Local Settings/History/History.IE5/index.dat* file we can see a few visits to Yahoo mail with the email address of **mrevilrulez@yahoo.com** 



How many executables are in the recycle bin?

4 (named Dc1.exe, Dc2.exe, Dc3.exe, and Dc4.exe)

### Are these files really deleted?

**No**, they are fully functional in the Recycle Bin.

### Perform an Anti-Virus check. Are there any viruses on the computer?

Running clamscan with the database versions in footnotes returned 25 infected files. The majority of which are located under directories titled ENUMERATION, EXPLOITATION, COMMANDS, and FOOTPRINTING, in the My Documents directory. Given the suspects purported level of technical skills and the file location, it is unlikely that these files were used to infect this machine. There are a number of other infected files under the System32 directory that could actually be viruses that the user of the machine installed or another malicious user.

- daily.cld: 25836
- main.cvd: 59
- bytecode.cLinux 3 vd: 331

### Appendix

#### Anti-Virus scan

csi@csi-analyst:/mnt/schardtraw\$ clamscan -ri./ ./My Documents/COMMANDS/enum.exe: Win.Tool.EnumPlus-1 FOUND ./My Documents/COMMANDS/SAMDUMP.EXE: Win.Trojan.Pwdump-2 FOUND ./My Documents/COMMANDS/snitch.exe: Win.Trojan.Snitch-1 FOUND ./My Documents/ENUMERATION/NT/enum/enum.tar.gz: Win.Tool.EnumPlus-1 FOUND ./My Documents/ENUMERATION/NT/enum/files/enum.exe: Win.Tool.EnumPlus-1 FOUND ./My Documents/ENUMERATION/NT/Legion/Chrono.dl\_: Win.Trojan.Bruteforce-3 FOUND ./My Documents/ENUMERATION/NT/Legion/NetTools.ex\_: Win.Trojan.Spion-4 FOUND ./My Documents/ENUMERATION/NT/ntreskit.zip: Win.Trojan.Nemo-1 FOUND ./My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe: Win.Tool.Brutus-3 FOUND ./My Documents/EXPLOITATION/NT/brutus.zip: Win.Tool.Brutus-3 FOUND ./My Documents/EXPLOITATION/NT/Get Admin/GetAdmin.exe: Win.Exploit.WinNT-3 FOUND ./MyDocuments/EXPLOITATION/NT/lsadump2/lsadump2.exe:Win.Trojan.Lsadump-1FOUND ./MyDocuments/EXPLOITATION/NT/lsadump2/lsadump2.zip:Win.Trojan.Lsadump-1FOUND ./My Documents/EXPLOITATION/NT/netbus/NetBus170.zip: Win.Trojan.Netbus-2 FOUND ./My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE: Win.Trojan.Sehole-1 FOUND ./My Documents/EXPLOITATION/NT/sechole/sechole3.zip: Win.Trojan.Sehole-1 FOUND Documents/EXPLOITATION/NT/WinVNC/Windows/vnc-3.3.3r7\_x86\_win32.zip: ./My Win.Tool.Winvnc-10 FOUND ./My Documents/FOOTPRINTING/NT/superscan/superscan.exe: Win.Trojan.Agent-6240252-0 FOUND ./Program Files/Cain/Abel.dll: Win.Trojan.Cain-9 FOUND ./Program Files/Online Services/MSN50/MSN50.CAB: Txt.Malware.CMSTPEvasion-6664831-0 FOUND ./WIN98/WIN98\_OL.CAB: Txt.Malware.CMSTPEvasion-6664831-0 FOUND ./WINDOWS/system32/ahui.exe: Win.Virus.Virut-6804272-0 FOUND ./WINDOWS/system32/dllcache/ahui.exe: Win.Virus.Virut-6804272-0 FOUND ./WINDOWS/system32/dllcache/mmc.exe: Win.Virus.Virut-6804520-0 FOUND ./WINDOWS/system32/mmc.exe: Win.Virus.Virut-6804520-0 FOUND

., which wo, systems 2, mine.exe. whi. whus. white oboty 20-01001

------ SCAN SUMMARY ------Known viruses: 7162840 Engine version: 0.102.1 Scanned directories: 766 Scanned files: 11305 Infected files: 25 Data scanned: 1806.71 MB Data read: 1768.03 MB (ratio 1.02:1) Time: 2432.815 sec (40 m 32 s)

### Layers of the OSI Model: Where the hardware and data fits LaShanda Edwards

The use of networks is everywhere. Examples of network use include the following: using social media, browsing the web, as well as accessing your email. When the "SEND" button is hit after writing an email, the email then goes only to the specified destination. The OSI model contains a lot of information that could be overwhelming to understand and remember; although, understanding the model will help you in everyday networking activities and will make troubleshooting problems within the network much faster and easier. The OSI model is comprised of 7 layers that help information technology professionals figure out what is going on in a networking system. The OSI model was birthed in the 70s by the International Organization of Standards (ISO) as Open System Interconnection (OSI) to make this form of communication standard over different systems and unique across the world.

In accordance with Shaw, during the time when computer networking was expanding, two separate models were merged in 1983 and published in 1984 to create the OSI model that most people are familiar with today (2018). This seven-layer model is greatly used by all organizations to continuously improve the network today. The model consists of the following layers as shown in figure 1 from top to bottom: Layer 7 – Application, Layer 6 – Presentation, Layer 5 – Session, Layer 4 – Transport, Layer 3 – Network, Layer 2 – Datalink, and Layer 1 – Physical.

The OSI model is simply a theory or structured way to ensure the performance, security, and integrity of data delivery. The model essentially divides the responsibility of communication in each independent layer.

**Editor's Note**: According to the Industry, there is an unofficial 8<sup>th</sup> layer. The Layer 8 is referred to as the human factor. From an attack perspective, social engineering fits here. From the investigation side, this is where Open Source Intelligence OSINT resides.

"Open-source intelligence is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources. It is not related to open-source software or collective intelligence." - Wikipedia

### **OSI Model Layers**

The International Organization Standardization (ISO) for conceived the OSI model which is a hypothetical model created to aid various communication systems to communicate to interchange data using standard protocols. According Cloudflare, the to modern Internet doesn't strictly follow the OSI model, although the model is still very useful for troubleshooting network problems. Whether it's a person



Figure 2: OSI Model credit - static.javatpoint.com

who is unable to get their laptop on the Internet, the OSI model can help to break down the problem and separate the source of the trouble. If the problem can be attached to one specific layer of the model, a lot of useless work can be avoided. Each layer of the OSI model is responsible for certain roles and responsibilities as shown in figure 2.

# Application layer

Layer 7 is called the Application Layer. The responsibility of this layer is to integrate the services on the network with the operating system in order for users to gain access to the network (Codecamp, 2019). This layer would probably be the most familiar to consumers due to it being the closest to the end-user. The end-user interacts with this layer of the OSI model generally every day by simply



using applications such as web browsers (Microsoft Edge, Firefox, Internet Explorer, Chrome, Safari) and Social Media Platforms (Instagram, Facebook, Twitter, Hangouts).

As shown in figure 3, the Application Layer's basic job is to provide an interface between the user and the network. This layer does not refer to the application itself, but it provides all the needed services to support applications to run properly. Some protocols contained within in the Application Layer include the following: File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Hypertext Transfer Protocol (HTTP), Post Office Protocol (POP), Trivial File Transfer Protocol (TFTP), Simple Network Management Protocol (SNMP), and Network News Transfer Protocol (NNTP) (Codecamp, 2019). Most protocols will extend down to the Session Layer, although protocols flow down multiple layers.

### **Application Layer Roles and Responsibility**

The Application Layer is the request sender or File transfer, access, and management (FTAM). It uses multiple applications to allow the user the ability to perform or access different operations such as uploading pictures, sending emails, blogging, etc. The Application Layer also represents the response. It acts as a mail service; it can view the response or destination of the user's data seen by another user from an alternate system. Lastly, it involves directory services, which is when the application provides the distributed database source.

### **Presentation Layer**

Layer 6 is called the Presentation Layer. The responsibility of this layer is to provide a format. This layer is consumed by encryption, compression, and syntax in which the communication will occur. Since it is attached with the Application Layer, the layer is also responsible for configuring the message into the Application Layer usable format. In other words, the Presentation Layer makes information presentable for the application or network as shown in figure 4.

An example of this is when a website is using the HTTP protocol. If the data is encrypted then the HTTP protocol would not do this: as an alternative, the SSL would encrypt the data in the Presentation Layer. The following are main the function of the Presentation Layer: Translation, Encryption, and Compression.



Figure 4: Layer 7 credit -static.javatpoint.com

### Presentation Layer Roles and Responsibility

Javatpoint states, translation is the process of duel systems exchanging information in character string form, numbers, etc. The data received from the sender's device is not consumable by any given application directly. Because different encoding methods are used for different computers, interoperability is handled by the Presentation Layer between various encoding methods (Javatpoint, 2018). It transforms the data from sender- dependent format to a common format and transforms the common format into a receiver-dependent format at the receiving end. To maintain privacy encryption is a necessity. The encryption method is a process of transforming the sender-transmitted information in a different form and transmits the resulting message over the network (Javatpoint, 2018).

The last function of the Presentation Layer is compression. Compression is the process of compressing the data. It is responsible for compressing the date received from the Application Layer. The number of bits is reduced to be transmitted. Compression is important in multimedia such as the following: video, text messaging, and audio. The protocols used in the Presentation Layer of the OSI model are SSL and TLS (Codecamp, 2019).

### Session Layer

Layer 5 is called the Session Layer. The responsibility of this layer is to create sessions between device communication by opening and closing a session between the two devices that are communicating as shown in figure 5.

The functions of this layer involves

maintaining,

From presentation layer To presentation layer L6 data L6 data Session Session H5 Layer H5 Layer syn syn syn L5 data L5 data To transport layer From transport layer

Figure 5: Layer 6 credit -static.javatpoint.com

synchronization between the applications at each end of the sessions (Javatpoint, 2018).

and

### Protocols at this layer

establishing,

ADSP, ASP, H.245, ISO-SP, OSI session-layer protocol (X.225, ISO 8327), iSNS, L2F, L2TP, NetBIOS, PAP, PPTP, RPC, RTCP, SMPP, SCP, SOCKS, ZIP, and SDP

### Session Layer Roles and Responsibility

Dialog control and synchronization are important in the Session Layer. Within the dialog control the Session Layer is the dialog controller that develops dialog between duel processes. It determines whose turn to speak in a session, very useful for video conferencing (Codecamp, 2019). Synchronization occurs when the Session Layer adds barriers to be met when transmitting data in sequential order. If an error occurs during the data transmission process, then the transmission will restart again from the barrier set. The protocols used in the Session Layer is NetBIOS (Codecamp, 2019).

### Transport Layer

Layer 4 is called the Transport Layer. The responsibility of this layer is to deliver data on the network as shown in figure 6. In accordance with Javatpoint, the Transport Layer ensures that the transmission of messages in the order in which they are sent without duplicating the data (2018).



The Transport layer generates a circuit that is used by the Session Layer to communicate with session. This layer can be thought of as the end-to- end layer because it offers a point-to-point connection amongst the source and destination to reliably deliver data.

### **Protocols Used**

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are two protocols used in this layer. Shaw states, the best-known example of the Transport Layer is the TCP, this protocol is built at the top of the Internet Protocol (IP). The IP is known as TCP/IP (2018). TCP is the standard protocol that allows systems to communicate over the internet. It maintains and establishes host connections.

Segments are formed when data is transported over the TCP connection and the TCP protocol distributes the data into smaller units. UDP is an original protocol in the Transport Layer. Due to the internet being unsecured the TCP/IP provides no security. The UDP protocol is considered unreliable due to the receiver not receiving an acknowledgment when the packet is received and the sender not waiting for an acknowledgment. Netscape created the Secure Socket Layer (SSL) protocol that was later adopted as a standard for Transport Layer Security (TLS) and it is now known as SSL/TLS (Holl, 2003). Countless financial institutions use these protocols to encrypt data crossing the Internet. SSL/TLS is not TCP/IP reliant and can layer on top of any transport protocol. They can even run under application protocols such as HTTP, FTP, and TELNET. SSL/TLS offers all three of the critical "CIA" security components: Confidentiality, Authentication, and Integrity. These protocols give protection against message tampering, eavesdropping, and spoofing. SSL counteracts eavesdropping of communication between a client and a server by encrypting passwords. TLS is very much like SSL except there is an interface between the handshaking portion and the record layer (Holl, 2003). In all Security efforts, there are going to be weaknesses and that's when hackers program to attack the vulnerabilities. TLS seems to have fewer security breaches than SSL, but the SSL/TLS combination improves them both.

#### Transport Layer Roles and Responsibility

Data transfer, dividing and reassembling, flow control, and error handling are the essential role and responsibility of the Transport Layer. Data transfer is simply transferring data between the sender and receiver accumulated from the Session Layer. To make communication quicker the data received from the Session Layer gets packaged into smaller segments on the sender device by dividing and reassembling.

Once the receiver receives the segments it collects, all segments reassembles back to the original data to be presented to the Session Layer. Flow control is the responsibility of the Transport Layer, although it is performed end-to-end rather than across a single link. Lastly, error handling is also the responsibility of this Layer. The error control is useful to ensure full data delivery, as the data are divided into segments.

### Network Layer

Layer 3 is called the Network Layer. The responsibility of this layer is moving data between systems throughout the network as shown in figure 7.

Routers are strongly used in the Network Layer; its job is very crucial within this layer to help determine the route for the fastest data delivery. Furthermore, the Network layer is responsible for determining the



effective path for the data. The routing protocols specify how the router identifies destination networks and the path data should travel to the destination network. Routers are the third layer devices and their main job is to provide the routing services within an internetwork. The Network Layer is also responsible for further breaking down the segments into small units called packets. The receiver side renovates packets back to segment. The Data Link Layer is responsible for routing and forwarding packets. Assignment of internet protocol (IP) addresses is another important thing that happens on the Network Layer. The IP address is often referred to as the Network Layer address or third level address.

### Network Layer Roles and Responsibility

The primary functions of the Network Layer are Routing, Internetworking, Addressing, and Packetizing. Internetworking is the main responsibility of the Network Layer. It delivers a logical connection between multiple devices (Javatpoint, 2018). Routing is intelligently designed to find the shortest and fastest route available from the multiple routes using a routing table, which is used by the Network Layer to perform routing. Addressing identifies each network distinctively in the network-connection and determines what device is on the internet, the Network Layer uses the IP address. A Network Layer collects the packets from the upper layer and converts them into packets, this process is known as packetizing achieved by IP. The protocols used in the Network Layer are the following: IP, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), Internet Protocol Security (IPSec), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP) (Codecamp, 2019).

# Data Link Layer

Layer 2 is called the Data Link Layer. The responsibility of this layer is interfacing between the physical communication of media, physical devices, and the Network Layer as shown in figure 8.

The Data link layer mainly consists of switches and hubs to connect the actual network for data exchange. The layer is split into two sub layers called Logical



Figure 8: Data Link Layer – Layer 2 static.javatpoint.com

Link Control (LLC) and Media Access Control (MAC). The LLC is the top sublayer and provides the interfacing between the lower layers and upper layers. It's liable for transporting the packets to the Network Layer of the receiver collecting, identifies the Network Layer protocol address from the header, and provides flow control.

The bottom layer is the MAC sublayer and it is responsible for identifying how devices can access the physical medium and it is used for transferring the packets over the network (Javatpoint, 2018). The Data Link layer is responsible for data exchange between two interconnected switches or hubs via the Network Layer. In other words, this OSI layer ensures the data moves node to node. Once the packets are received in the Data Link Layer from the Network Layer it further distributes packets into frames to transmit data using MAC address.

### Data Link Layer Roles and Responsibility:

Framing, Acknowledgement, Retransmission, Error Control, Flow Control, Physical Addressing, and Access Control all play a major role in the Data Link Layer. The Data Link Layer transforms physical raw bit stream into packets that are called frames. Framing enable a way of transmitting a set of frames in bits that are useable by the receiver. When notice is sent by the accepting end to inform the source that the frame was received without any mistakes is the Acknowledgment (Codecamp, 2019). If the source fails to receive an acknowledgement, then the packet goes through a process called Retransmission and will be retransmitted. Error and Flow Control provides error control by identifying an error in the Physical Layer and rectifying it. Flow control can also be achieved by regulating the data rate on both sides to prevent data corruption. This layer adds header and trailer to the frame. The header added to the frame contains the hardware destination and source addresses. Physical Addressing of the Data Link Layer adds headers to the frames that includes the destination address. Access Control is when more than one device is connected to the same communication channel. The protocols used within the Data Link Layer are PPP, ATM, Ethernet (Codecamp, 2019).

# Physical layer

Layer 1 of the OSI model is called the Physical Layer as it provides the actual connection between two devices using cables as shown in figure 9. It consists of the information in the form of bits. This is also the layer where the data gets converted into a bit stream from the Data Link layer (Layer 2) into electrical signals. Codecamp, refers to the Physical Layer as a way to help transmit data between duel machines communicating in a physical manner, which can be optical fibers, copper wire, wireless, etc. (2019).



Figure 9: Layer 1 static.javatpoint.com

#### **Physical Layer Roles and Responsibility**

The following are the roles and responsibility of the Physical Layer: Line Configuration, Signals, Physical Topology, and Data Transmission Mode. The Line configuration defines the way multiple devices physically connects. Signals used within the Physical Layer determines the type of signal used for the transmission of information (Javatpoint, 2018). When using cables and switches within the Physical Layer, the layer is enabled to connect multiple devices into a Physical Topology. This can also be done with mesh topology, bus topology, star topology, and hybrid topology ideas. The Physical Layer also defines the way the transmission will be done between two devices by a process called Transmission Mode. Transmission Modes in the Physical Layer can be categorized into three modes: simplex, half-duplex, or full duplex. Protocols used by this layer are USB, Bluetooth, etc. (Codecamp, 2019). The OSI model describes how devices communicate with each other. The model divides network communication between two hosts. The OSI model is divided into seven different layers, and has data being transformed at each layer to prepare it to be sent through the network. It is important to memorize the 7 Layers of the OSI model: Application Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, and Physical Layer. Added to the data at the upper layers are encrypted, formatting, and session numbers. Data is broken down into bit segments with accordance to a port number, then given an IP address at the middle layers. At the lower levels, packets are changed into frames that include the source and destination MAC address; frames are changed into bits for communication through the network.

The bottom layers of the OSI model are heavily related to the hardware. The top layers of the OSI model are related to the protocols. The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol has 4 layers. This is the main protocol used in all Internet operations. The Open System Interconnection (OSI) model divides network communication between 2 hosts into layers. The network access layer is equivalent to OSI layers 1 and 2, the Internet Protocol layer is comparable to layer 3 in the OSI model, the host-to-host layer is equivalent to OSI layer 4, and finally, the application layer is similar to OSI layers 5, 6, and 7 combined (Frenzel, 2013). TCP/IP is the older of the two methods of data communications and is well recognized throughout the world. The OSI model, however, is a proven concept that is used in all other data communications protocols. It will continue to be used as a GUIdeline for all other communications applications.

Let us walk through an example that will explain how the process takes place to convey the data. If I wanted to send an email to my mom, I will compose the email on yahoo and click send. Yahoo will pass my email message to the Application Layer, which will select a protocol and pass the data to the presentation layer. The Presentation Layer will encrypt depending upon the security level and condense the data. It will move to the Session Layer next, which will initialize the communication session by opening the session to ensure the quality delivery of the data. The data then goes to the sender's Transportation Layer. Here is where the data will be divided into small segments. Those segments will then hit the network layer and will be broken up into packets. These packets will break down into frames at the Data Link Layer. The Data Link Layer will then send those frames to the Physical Layer. Here, the data will be converted into a bit stream of 1s and 0s and sent through the network. On the other end, on my mom's computer, it will first capture the bit stream at the Physical Layer and wait until every bit stream transforms into frames to go to the Data Link Layer. If there are any errors in the Physical Layer, they will be trapped in the Data Link Layer, which is now liable to take all frames and reunite them into packets. From the Data Link Layer, it will go to the Network Layer, to generate segments from the given packets. It will then flow into the Transport Layer where the original data will be formed from segments through the reassembly function. After the initial data are formed, it will move to the Session Layer. Here in this layer, the session will terminate once the data is received completely and move into the next layer called the Presentation Layer. The Presentation Layer will now decrypt the data that is consumed for the application. Finally comes the Application Layer from where the application will be able to function and display the email sent to my mom's computer screen using the Application Layer's services.

### Citation

- Codecamp. (2019, October 29). 7 layer of OSI Model | 7 Layer OSI model in Computer Network. Retrieved February 12, 2020, from
- mycodecamp.blogspot.com/2019/10/7-layer-of-osi-model.html
- Cloudflare. (n.d.). Retrieved January 19, 2020, from
- cloudflare.com/learning/ddos/glossary/open-systems- interconnection-model-osi/
- Frenzel, L. (2013, October 02). What's The Difference Between The OSI Seven-Layer Network Model And TCP/IP? Retrieved February 21, 2010.
- electronicdesign.com/what-s-difference-between/what-s-difference-between-osiseven-layer-network-model-and-tcpip
- Holl, K. (2003). OSI Defense in Depth to Increase Application Security. Retrieved March 8, 2020. giac.org/paper/gsec/2868/osi-defense-in-depth-increase- applicationsecurity/104841
- Javatpoint. (2018). Retrieved February 20, 2020, from

### javatpoint.com/osi-model

Shaw, K. (2018, October 22). The OSI model explained: How to understand (and remember) the 7-layer network model. Retrieved February 8, 2020, from networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html

# Forensic Data Recovery Capturing Evidence in a Forensically sound manner Layer 1

By Jeremy Martin



### Data Destruction

We will cover the different levels of data destruction from full files to completely obliterated hardware. Some stages are recoverable while some others are not. There are several labs ready for you to follow along with. We will cover the potential of data recovery of five of those phases, and only a handful of methods and software at each phase. To follow along, create your own "evidence disk" by copying known graphics, documents, and other files to create a known base line. Once you are comfortable with basic recovery, move on to more advanced content.

An easy way to think about data recovery is that if data is written to a data container (RAM, file, database, partition, drive, etc.), it is always there until it is overwritten or in the case of RAM, released. You can format a drive a thousand times, and it does not overwrite the entire drive. This is why there have been many cases over the years that digital evidence was still found even after the suspect took great lengths to hide or destroy it.



### Un-deleting vs. Data carving

Un-deleting is recovering data from a file system after it has been deleted. This means that the record in the file system's index (FAT, MFT, Catalog, etc...) still points to the location of the data on the drive. With the FAT file systems, the first character of the file name is overwritten with the hex characters "E5". When you recover the data, you may have the original file name with the file. This method of recovery is a far faster than data carving.

Data carving does not look for a file system index. Instead, this method starts at the beginning of the data set and searches for the header (first few bytes) and/or footer (last few bytes) of a file. For example, a common header of a .JPG file is the hex combination "*FF D8 FF E0*" with a footer of "*FF D9*". When a data carving utility finds the header, it copies the data until it finds the footer and that becomes a recovered data set or file. Some of the programs will even allow you to ignore the footer to recover "partially recoverable files". The challenge with not looking for the footer of a file type means that you will get a lot more "false positives".

### What is Recoverable?

What can you carve? Well, any data container that may contain files. What I mean by that is you can carve an entire disk, a partition, a raw copy of a drive, a swap file (pagefile.sys in windows), and even memory. You can even recover data from a drive that had an operating system reinstalled over a previous system. During this section of training, we will make a forensically sound bit-stream image of a "suspect" USB thumb drive. After



the raw image is complete, we will use several tools to recover "evidence" including mounting the raw DD image to data carving both deleted and undeleted files. Some of the open source Linux tools we will look at are RecoverJPEG, Foremost, and Scalpel.

### The Different Phases of Data Destruction

**Full files**: Files have not been deleted. The index (FAT, MFT, Catalog, etc.) for the file system is 100% intact. Data can easily be recovered.

**Deleted files**: Files have been deleted. The index for the file system is 100% intact. These files can be "Undeleted" or recovered as long as the data on the disk has not been overwritten.

**Formatted**: The Operating System index (FAT, MFT, Catalog, etc.) has been rebuilt or the records in that index have been overwritten. If the data on the disk has not been overwritten, they can be recovered with data carving. Names cannot be recovered unless located in the MATA information of the file & file signatures/headers need to be known.

**Partially overwritten**: Some data is recoverable, but usually in bits and pieces. This is where forensic tools become handy.

**Physical Failure**: The data is still there in most cases and the devices need to be repaired before an attempt to recover it can be made.

**Wiped**: All data has been overwritten or "nuked" and is unrecoverable within reasonable means.

**Physical Annihilation**: Drive or media is destroyed and unrecoverable.

**Volatile Data:** This is the data that you will lose when the system is turned off. This includes RAM, System Processes, and Network connections. Capturing this data can be extremely important in many cases.

**Semi-Volatile Data:** Swap space (pagefile.sys for Windows for example), temp files, slack space, and free space on the drive are examples of data that can still be recovered if the acquisition of the evidence is done properly. Simply turning on the system or computer can overwrite and make data unrecoverable.

# Chain of Custody

Now you understand that data can be recovered, even from a formatted drive, what next? Before you touch anything, you need to start a Chain of Custody. Even though you may not be dealing with forensic investigations, getting in the habit of documenting everything. This helps with logistics to make sure you know what you received and what needs to go back. If you do find illegal content and it goes to court, if you treat it like a "forensic" recovery, you will not have tampered with or destroyed the evidence. *An example of a Chain of Custody will be added to the end of this section*.



#### Scope

Before you do anything, you need to determine the intent and scope of the investigation or recovery. You need to know what to find BEFORE you can find it. This only helps you. If they want to recover family pictures, this will be your first target to recover. If the client wants everything, you can hand the drive back and request payment for services rendered. If you are recovering data for a forensic investigation, if there is no scope, there is no case. In the United States, the 4th Amendment is clear "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". It is always better to err on the side of caution.* 

### **Capturing Volatile Memory**

If you need to pull the volatile memory, there are many tools that you can accomplish this with. In the spirit of being free, I will mention two that are currently free. You can use FTK Imager from Access Data. This is a phenomenal forensic imaging tool and is currently free. DumpiIt is another good free tool out there that will capture memory and works great with the memory analysis tool Volatility. We will not cover these in this section.

There are many tools out there you can use, just remember, minimize interaction with the system to minimize the destruction of evidence, know what your tool is/is not doing, and document EVERYTHING. If you did not document it, it did not happen. This can bite you in the butt if it ever gets to court.

Now you need to image the drive. We are specifically covering physical acquisition of evidence, so the system needs to be off so you can pull the drive and move forward.

### Write Blocking Labs

First, print off a copy of the Chain of Custody included in this lab manual. Fill in everything related to the "case". Now you have your Scope and Chain of Custody, you can start to acquire the physical evidence.

For a lab-based environment, download a group of files to create a known baseline. When you know what files you have copied, you know what content should be recoverable. For example:

- (20) .JPG images,
- (10) .PDF documents
- (10) .DOCX documents
- (5) .TXT files

Now you can test the differences between the different tools and see the levels of recoverability with each tool and method. You can also use the recovery.001 image that is used in the IWC Cyber Secrets episodes dealing with data recovery. If you use that downloaded image, skip to "File Recovery Labs".

Now, imagine you have a suspect drive and a hardware write blocker (aka: forensic bridge). Make sure you read the different ports that the drive connects into, versus the output that plugs into the computer.
#### Lab: Hardware

- 1. Buy a hardware write blocker & connect it to the drive to be protected.
  - a. Skip if you don't have a hardware forensic bridge/write blocker.
  - b. Follow the instructions provided by the vendor.
  - c. Forensic Bridges or Write Blockers from vendors like: Firefly, Tableau, etc...

Imagine that you need to write block and do NOT have a hardware write blocker. Your workstation is a Linux system and you still want to make sure you connect the evidence drive in a forensically sound manner. The first thing you are going to have to do is log in and make sure you have root privileges in Linux. You will also need access to a terminal or a Command Line Interface "CLI" prompt.

### Lab: Windows Registry Hack for External USB Devices

- 1. Open Windows Run dialog by pressing Win + R keys together.
- 2. Type in **regedit**
- 3. Press **Enter** to open Windows Registry Editor.

🗾 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	regedit	~
	OK Cancel Browse	

- 4. Navigate to: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies.
- 5. If StorageDevicePolicies key does not exist, you will have to create.
  - a. Right click on '**Control**' key.
  - b. Click **New**.
  - c. Click **Key**.
  - d. Name the new key StorageDevicePolicies
- 6. Select StorageDevicePolicies.
- 7. Right-click in the right window.
  - a. Select New
  - b. Dword (32-bit) Value.
- 8. Name the new entry **WriteProtect**.
- 9. Double-click on **WriteProtect**
- 10. Change the value from 0 to 1. (1 tuns on write blocking and 0 turns it off).

ile <u>E</u> dit <u>V</u> iew	F <u>a</u> vorites <u>H</u> elp				
	SrpExtensionConfig	*	Name	Туре	Data
▶ 	🎍 StillImage 🝶 Storage		(Default)	REG_SZ	(value not set)
	StorageDevicePolicies	1	vinteprotect	KEG_DWORD	00000001 (1)
	SystemInformation				
∆. 	SystemResources TabletPC				
Þ-	Terminal Server TimeZoneInformation				

11. Insert the USB

The USB should now be write protected.

### Lab: Linux Mount as Read-Only

- 12. Insert the USB (below are multiple options in Linux to identify the right drive).
  - a. Verify your USB device by typing "lsblk" and look for the sd(?) drive
  - b. Verify your USB device by typing "df" and look for the sd(?) drive
  - c. Verify your USB device by typing "dmesg | grep sd" and look for the sd(?) drive
  - d. Verify your USB device by typing "ls /dev/sd\*" and look for the sd(?) drive

Assume the drive is sdb for the rest of the lab.

- 1. sudo mkdir /media/usbdrive
- 2. sudo mount /dev/sdb1 /media/usbdrive -o ro

This will mount the drive or make the drive usable as read-only to the folder "/media/usbdrive"

If the drive is already mounted, type:

#### sudo mount -o remount,ro /media/usbdrive

## Data Destruction / Wiping

Why are we talking about wiping or overwriting data before we even get to the imaging portion? Logistically, you should always wipe your destination drive, especially if you are copying from a disk to another disk. The reasoning behind this is to eliminate the possibility of residual evidence or contamination residing on the destination drive that could get misidentified in your current investigation. MAKE SURE YOU WIPE THE RIGHT DRIVE!!! The wrong one could be your Operating System! Always verify!

### Lab: Eraser (Windows)

- 1. Instal Eraser from sourceforge.net/projects/eraser/files/latest/download
- 2. Use the default settings.
- 3. Once installed, run Eraser



4. Click on the down arrow between Erase Schedule and Settings



- 5. Click **New Task** or use the keys **ctrl+N**.
- 6. Name the task

We are using "Wipe" for our name.

- 7. Chose Run immediately.
- 8. Click Add Data.

IGOK	Schedule			
Task r	name (optional):	Wipe		
Task T	Гуре:	O Run manu	ially	
		Run imme	diately	
		O Run on re:	start	
		○ Recurring		
Data f	o erase:			

9.	Click on the <b>Ta</b>	rget type: dropdo	wn box	Select Data to Erase	×
10	and choose <b>Driv</b>	e/Partition. sure method: dra	ondown	Target type:	Drive/Partition $\checkmark$
10.	box and choose <b>U</b>	JS DoD 5220.22-M	<b>I</b> .	Erasure method:	US DoD 5220.22-M (8-306./E) (3 $ \sim$
11.	Click on the Set choose the drive	tings dropdown ł to wipe	oox and	Settings	
This will to use in 12.	be the external US your lab Click <b>OK</b> .	B drive that you as	re going	Hard disk 1 (3.74	GB) ~
		– Data to erase:	-		
		Data Set		Erasure Method	
		Hard disk I		US DoD 5220.2	OK Cancel
13. 14.	Click <b>OK</b> . Now wait	Add Data			
	🍺 Erase Scł	neaule		OK Cancel	
	Task Name		Next Run		Status
	Tasks executed manua Wipe	ally	Running		

### Lab: dcfldd/dd (CLI) (Linux)

- 1. Once the OS is loaded, open a terminal window with root access.
- 2. Verify your drive letter
  - a. Type **lsblk**
  - b. Type fdisk -l
- 3. Assuming the drive is sdb
- 4. Type dcfldd if=/dev/zero of=/dev/sdb

## Forensic Imaging Labs

You have already filled out the Chain of Custody and connected the drive in a forensically sound manner. Now what? Well, Copy the data... Never analyze the original disk. Always make at least two copies of the original evidence before you start to work with it. Working on the original runs the risk of damaging the evidence and making it inadmissible in court. The second copy is what you work with. The first copy, you put in storage, so you do not have to touch the original again unless there is an emergency. It is also suggested to make an MD5 hash along with a SHA hash of the original evidence and each copy. A hash is a digital fingerprint that ads a level of trust that the data has not changed during the usage.

There are two types of copies. There is a "Physical copy" (aka: bit stream, clone, image, etc...) that duplicates allocated and un-allocated space. This means all data. You can recover deleted content and even partially over written data. The other copy is called a "Logical copy" (aka: backup, archive, file copy, dos copy, copy & paste, etc...). The most forensically sound copy is of course a physical copy.



Image credit: Atola TaskForce atola.com

Most physical forensic imagers have write blockers built into them and it takes some of the risk out of the equation. Just make sure to put the evidence drive as the source and if you are imaging to another disk, that will be your destination. Too many people destroy the evidence by attaching the wrong drive to the destination...

What we want to do in these labs: create a known baseline. As mentioned previously, copy files in groups so we have a consistent set to play with. Since computer forensics IS a science, everything you do needs to be done is a consistent and reproducible manner. Once you are comfortable with the tools and methods, you can use what you have learned with real evidence and have confidence in your scientific results or analysis.

If you want to do your Imaging from a Windows computer, use FTK Imager. FTK Imager has software write blocking built in, so you will not destroy the evidence, but your next issue is the Operating System. Microsoft has had a history of trying to "help" the user when a new drive is added by adding data to the drive. If this happens, the evidence is destroyed due to contamination. To prevent this, use a physical write blocker. With that said, FTK Imager can be downloaded from accessdata.com. You may have to register to download the tool here: accessdata.com/product-download

1. 2.	Do Write Blockin Run FTK Imager	ng Lab first	DO NOT pick your boot drive and copy to your
3.	K Imager Left click the <b>Fil</b>	<b>e</b> menu	boot drive. You will run out of space and no fun will be had.
	<mark>E AccessData FTK Im.</mark> File <u>V</u> iew <u>M</u> ode <u>H</u> e A A A & A A A A A A A A A A A A A A A A	ager 4.3.1.1 p   # @ ⇒ ■ <b>© ९   े े े े </b> <mark>™</mark> 證   ×   File List	Select Source
4. 5.	Select Create a D Choose the sour a. Select_Sourc b. Select_Device In my cas	Name isk Image ce e ( <b>Physical Drive</b> ) e (your USB) se, a 4GB SD card	Please Select the Source Evidence Type   Physical Drive  Logical Drive  Image File  Contents of a Folder
	Source Drive S Please select	election t from the following available drives: LDRIVE1 - SDHC Card [4GB]	(logical file-level analysis only; excludes deleted, unallocat co Device (multiple CD/DVD)

### FTK Imager Walkthrough

#### Click **Finish**: 6.

< <u>B</u>ack <u>F</u>inish Click Add 7. Add... Select Image Type Choose RAW (DD) 8. Please Select the Destination Image Type 9. Left click **Next**  Raw (dd) Fill in your information 10. Left click **Next** 11. <u>○E</u>01  $\times$ Evidence Item Information Case Number: USB1 Evidence Number: 001 001 Unique Description: Examiner: Your Name Notes: Level 1 Image for data recovery lab < <u>B</u>ack <u>N</u>ext > <u>C</u>ancel Help

Select the	destination folder for the image	
~ 5	OS (C:)	^
>	📕 \$Recycle.Bin	
>	🦲 Cases	-
	🧵 USB1	
>	📃 CSI Linux Investigator	
>	🔝 Documents and Settings	
>	🣜 Drivers	~
Folder:	USB1	

<u>N</u>ext >

< <u>B</u>ack

Cancel

- Image Destination Folder is where you 12. want to store the image
  - a. Left click Browse and choose the folder for your image

- 13. Name the image
- 14.
- Image segment size a. Type in "**0**" or zero Click **Finish**

#### 15.

C:\Cases\USB1				Browse
<u>m</u> age Filename (	Excluding Ext	ension)		
usb1.dd				
For Raw, E	01, and AFF fi	Image Fragment ormats: 0 = do not	: <u>S</u> ize (MB) 0 t fragment	
Compre	ssion (0=Non	e, 1=Fastest,, 9=	=Smallest) 0	-
		l Ise AD	Encryption	1

#### Check "Verify images after they are created" 16.

#### Left click **Start**... 17.

\\.\PHYSICALDRIVE1		
	Starting Evidence Number:	1
nage Destination(s)		
:\Cases\USB1\usb1.dd	[raw/dd]	
<u>A</u> dd	<u>E</u> dit	Remove
<u>A</u> dd	Edit Add Overflow Location	<u>R</u> emove
Add	Edit Add Overflow Location	<u>R</u> emove.
<u>A</u> dd Verify images after they Create <u>d</u> irectory listings	Edit Add Overflow Location are created Precalculate of all files in the image after the	Remove

18. Now wait...

Creating Image	e —		
Image Source:	\\.\PHYSICALDRIVE1		
Destination:	C:\Cases\USB1\usb1.dd		
Status:	Creating image	Image Summary	×
Progress Ela Es	apsed time: 0:00:17	Created By AccessData® FTK® Imager 4.3.1.1 Case Information: Acquired using: ADI4.3.1.1 Case Number: USB1 Evidence Number: 001 Unique description: 001 Examiner: Your Name Notes: Level 1 Image for data recovery lab	^
19. V 20. C 21. C 22. N	Cancel When done, click <b>Summary</b> Click <b>OK</b> Click <b>Done</b> Now you are done!	Information for C:\Cases\USB1\usb1.dd: Physical Evidentiary Item (Source) Information: [Device Info] Source Type: Physical [Drive Geometry] Cylinders: 488 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 7,843,840 [Physical Drive Information] Drive Model: SDHC Card Removable drive: True	>

You have successfully created a forensic image using FTK Imager. Now to create your different images for the data carving labs.

- 1. Delete all the files on the USB.
- 2. Repeat the FTK Imager steps.
- 3. Quick Format the USB.
- 4. Repeat the FTK Imager steps.
- 5. Wipe the drive using Eraser
- 6. Repeat the FTK Imager steps.



Now, if you are using a Linux or Unix computer, dcfldd is a command line imager that creates a physical copy. DCFLDD is based off dd with some upgrades. It gives a progress of the data copied and it allows you to create a hash. Best of all is it is free. If you do not have dcfldd installed, you can substitute "dcfldd" with "dd" in the commands.

Note: Unless you are logged in as root (NOT suggested for security reasons), you must use the "sudo" command any time you touch hardware or run a system level utility.

"sudo is a program for Unix-like computer operating systems that allows users to run programs with the security privileges of another user, by default the superuser. It originally stood for "superuser do" as the older versions of sudo were designed to run commands only as the superuser." - wikipedia.org

### Lab: dcfldd (Linux)

- 1. Do Write Blocking Lab first
- 2. Burn a live Linux .iso to a bootable CD, DVD, or USB.
- 3. Boot off the CD, DVD. or bootable USB.

We use CSI Linux Acquisition for imaging, but any Linux distribution will do.

- 4. Once the OS is loaded, open a terminal window with root access.
- 5. Type "mkdir /recovery"
- 6. Type "cd /recovery"
- 7. Type "mkdir usb1"
- 8. Repeat for usb2-4
- 9. Wipe the drive by typing "sudo dcfldd if=/dev/zero of=/dev/sdb"
- 10. Format the USB with FAT by typing "sudo mkfs.vfat /dev/sdb1"
- 11. Download a theme of files (.jpg, .pdf, .txt). This will create a controlled environment.
- 12. Copy the files onto the USB.
- 13. Image the drive typing "sudo dcfldd if=/dev/sdb of=/recovery/usb1.dd".
- 14. Delete all the files on the USB.
- 15. Image the drive typing "sudo dcfldd if=/dev/sdb of=/recovery/usb2.dd".
- 16. Format the USB with FAT by typing "sudo mkfs.vfat /dev/sdb1"
- 17. Image the drive typing "sudo dcfldd if=/dev/sdb of=/recovery/usb3.dd".
- 18. Wipe the drive by typing "sudo dcfldd if=/dev/zero of=/dev/sdb"
- 19. Image the drive typing "sudo dcfldd if=/dev/sdb of=/recovery/usb4.dd".

To benefit of DCFLDD, is that it can create a hash instead of being forced to use a thirdparty tool. This makes scripting things or automation that much easier.

Example:

# sudo dcfldd if=/dev/sdb1 of=usb(?).dd hashwindow=0 hashlog=hash.txt cat hash.txt

If you have the hardware, use it. Doing this will minimize the risk of destroying evidence...

#### Lab: Hardware Imaging

1. Skip if you do not have a hardware imager or buy one & connect it to the drive to be duplicated.

Make sure you connect it to the right port. You do not want to wipe or overwrite the evidence drive. Then follow the instructions provided by the forensic imager vendor

Here is a list of vendors for forensic Imagers

a. Forensics: SuperChief, Tableau, Forensic Duplicator...

Here is a list of vendors for Data Recovery Imagers

b. Data Recovery: DeepSpar, Atola, Data Copy King, etc...

If you image the logical drive/volume/partition, you can mount the volume directly.

### Lab: Volume Image Mount in Linux

mkdir /mnt/evidence sudo mount usb(?).dd /mnt/evidence cd /mnt/evidence ls

If you image the physical drive, all partitions, you can use **losetup** (losetup is used to associate loop devices with regular files or block devices).

### Lab: Drive Image Mount for All Partitions in Linux

### sudo losetup --show -f -P usb(?).dd

## Data Carving Labs

Now for recovering the data from the images. During your investigation, you are given an image (the ones created in the imaging lab) and it is your job to recover any data that you can. In this lab, we will cover several possible tools to use.

### Lab: Using Autopsy

"Autopsy<sup>®</sup> is a digital forensics platform and graphical interface to The Sleuth Kit<sup>®</sup> and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card." - sleuthkit.org/autopsy

- 1. Download and install Autopsy GUI
  - a. You can also use CSI Linux. Autopsy is already installed
- 2. Run Autopsy



- 3. Click on **New Case**.
- 4. Enter your **Case Name**.
- 5. Click on **Browse** to pick the folder you want your case content.



- 6. Keep the Case Type: as **Single-user**.
- 7. You will see the case folder at the bottom of the window.

ase Informatio	n	
Case Name:	USB1	
Base Directory:	C:\Cases\USB1	Browse
Case Type:	Single-user     Multi-user	
Case data will be	stored in the following directory:	
C:\Cases\USB1\	JSB1	

8. Under Case **Number:**, enter your case number.

This would be assigned by your organization, but in this lab, use 001.

- 9. Under Examiner **Name:** enter your name.
- 10. Under Examiner **Phone:** enter your phone number.
- 11. Under Examiner **Email:** enter your email.



- 12. Under Examiner **Notes**, enter the description or notes for the case.
- 13. Click on **Finish**.

Number:	001
Examiner	
Name:	Investigator Name
Phone:	(555) 555-5555
Email:	test@csilinux.com
Notes:	This is the first Data Recovery Lab for the image usb1
Organizatior	1
Organiza	tion analysis is being done for: Not Specified $$

- 14. Select the Disk Image or VM File option.
- 15. Click Next.

#### Steps

#### Select Type of Data Source To Add

Disk Image or VM File

- 1. Select Type of Data Source To Add
- 2. Select Data Source
- 3. Configure Ingest Modules
- 4. Add Data Source
  - 16. Click on Browse and chose the image (DD) file you created.
  - 17. Click on **Next**.

Path:		
C:\Cases\US	B1\usb1.dd.001	Browse
Ignore o	rphan files in FAT file systems	
Time zone:	(GMT-7:00) America/Denver	~
Sector size:	Auto Detect	

#### 18. Click on Select All.

This is a small lab and should not be an issue. For larger cases, pick only the options you want to use

#### 19. Click on **Next**.

Steps	Configure Ingest Modules	
<ol> <li>Select Type of Data Source To Add</li> <li>Select Data Source</li> <li>Configure Ingest Modules</li> <li>Add Data Source</li> </ol>	Run ingest modules on:         All Files, Directories, and Unallocated Space         Y         Extension Mismatch Detector         Y         Exit Parser         Y         Keyword Search         Y         Email Parser         Y         Encryption Detection         Y         Interesting Files Identifier         Y         Correlation Engine         Y         PhotoRec Carver         Y         Virtual Machine Extractor         Y         Data Source Integrity         Y         Select All         Deselect All	PhotoRec Settings
		< Back Next > Einish

#### 20. Click on **Finish**.

500	eps	Add Data Source
1. 2. 3. <b>4.</b>	Select Type of Data Source To Add Select Data Source Configure Ingest Modules Add Data Source	Data source has been added to the local database. Files are being analyzed.

#### 21. Now Wait...

You should see a progress bar on the bottom right of the Autopsy window.

0%	📓 (1 more)
----	------------

Once Autopsy has completed the Ingest Modules, you should see data on the left-hand side, assuming that data was recoverable. Autopsy is more than just a recovery tool like some of the other tools we are going to cover, it is a very powerful forensics tool, especially for it being free.

Notice in the screenshot below that Autopsy also parsed out deleted files and even EXIF data from the JPG files it recovered. This means even location data if GPS or location services were enabled when the picture was taken.

🕂 Add Data Source 📠 Images/Videos 📓 Com	munications 💡 Geolocation	🧮 Time	eline 🍃	File Discovery 📗 Gener	ate Report 🛛 😹 Clos	≥ <sup>m</sup> ∢	⊙ • Keyword L	ists	🔍 Keyword Search
< > C	Listing								$( + \mathbf{v})$
Data Sources	EXIF Metadata								613 Resu
- Wiews	Table Thumbnail								
🖨 🖏 File Types									Save Table as CSV
🖨 🍰 By Extension	Source File	s	c o	Date Created	△ Device Model	Device Make	Data Source	Size	Path
Images (644)	IMG_8413.JPG			2020-05-08 03:07:15 MDT	Canon EOS REBEL T5i	Canon	usb1.dd.001	4589801	/img_usb1.dd.001/ .
Videos (0)	IMG_8414.JPG			2020-05-08 04:06:21 MDT	Canon EOS REBEL TSi	Canon	usb1.dd.001	9628282	/img_usb1.dd.001/
Archives (0)	IMG_8424.JPG			2020-05-08 04:15:45 MDT	Canon EOS REBEL TSi	Canon	usb1.dd.001	5441000	/img_usb1.dd.001/
Databases (0)	IMG 8426.JPG			2020-05-08 04:17:52 MDT	Canon EOS REBEL TSi	Canon	usb1.dd.001	7868454	/img_usb1.dd.001/
Documents	IMG 8427.JPG			2020-05-08 04:20:00 MDT	Canon EOS REBEL TSi	Canon	usb1.dd.001	9974849	/ima_usb1.dd.001/
🗄 🗒 Executable	IMG 8432, 1PG			2020-05-08 04:34:54 MDT	Capon EOS REBEL TSI	Capon	ush1.dd.001	5634916	(img_ush1.dd.001)
🗈 🐇 By MIME Type	<								>
Elected Files									
All (136)	Hex Text Application	Message	File Me	tadata Context Results A	Innotations Other Occur	rences			
ND st. s	0° 0 0	6% O	⊕   R	eset					Tags Menu
		~		MA.391					rago rioria
Results	100 Mar								
		*							
Merry File Size     Results     Extracted Content     Single Iteral Keyword 5earch (0)     Single Regular Expression Search (0)     Email Addresses (3)     URLS (1277)									

NOTE: The Autopsy application works in Windows, MAC, and Linux. Some of the third party ingest modules however may only work in Windows since they tie into .EXE files.

### Lab: Using RecoverJPEG

"A tool to recover lost files on damaged memory cards or USB drives. recoverjpeg tries to recover JFIF (JPEG) pictures and MOV movies (using recovermov) from a peripheral." - rfc1149.net/devel/recoverjpeg.html

- 1. Do Imaging Lab 1 first
- 2. recoverjpeg usb(?).dd

### Lab: Using Foremost

"Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types. These built-in types look at the data structures of a given file format allowing for a more reliable and faster recovery.

Originally developed by the United States Air Force Office of Special Investigations and The Center for Information Systems Security Studies and Research, foremost has been opened to the general public. We welcome any comments, suggestions, patches, or feedback you have on this program. Please direct all correspondence to namikus@users.sf.net." foremost.sourceforge.net

- 23. Do Imaging Lab 1 first
- 24. Type "foremost –i usb1.dd –o usb1 -v". Wait until complete.
- 25. Repeat step 2 for each other usb?.dd image
- 26. Use a file explorer or manager to view results
- 27. View and compare the results.

Optional: Only generate an audit file and print to the screen (verbose mode).

#### foremost -av usb(?).dd

Search all defined types

foremost -t all -i usb(?).dd Search for gif and pdf foremost -t jpg,pdf -i usb(?).dd Run the default case foremost usb(?).dd

### Lab: Scalpel (Linux)

"Scalpel is a file carving and indexing application that runs on Linux and Windows. The first version of Scalpel, released in 2005, was based on Foremost 0.69". - github.com/machn1k/Scalpel-2.0

Scalpel takes a little more configuring out of the box. We are going to look at the configuration file that will allow us to data carve. This is what the /etc/scalpel/conf/scalpel.conf file will look like:

# Ex	rtensio	n Case	size head	er footer #	
#					
#	GIF a	and JPG	files (very c	ommon)	
#	gif	У	5000000	x47x49x46x38x37x61	\x00\x3b
#	gif	У	5000000	$x47\x49\x46\x38\x39\x61$	\x00\x00\x3b
#	jpg	У	20000000	$xff\xd8\xff\xe0\x00\x10$	\xff\xd9
#	jpg	У	20000000	\xff\xd8\xff\xe1	\xff\xd9

Once we edit the scalpel.conf file to look for what we want to find, save it and now we can use Scalpel to start carving data.

#### **Using Scalpel**

- 1. Do Imaging Lab 1 first
- 2. Type "scalpel /dev/sdb –o usb1 -v". Wait until complete.
- 3. Type "cat /usb1/audit.txt"
- 4. Repeat steps 2-3 for each other usb?.dd images we created earlier
- 5. Use a file explorer or manager to view results
- 6. View and compare the results.

#### Optional: scalpel usb(?).dd -o Directory-you-want-the-output-to

Note: The trick is to use all the tools in your disposal and compare. The easiest way to do this is to create the "evidence" drive yourself and documenting every file on the drive. Then delete several of the files or folders. At this point, you have a known baseline to start from. Create the dd raw image to analyze with the various methods.

### EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Event Number: Reason: Submitting Individual: (Name/ID#) Client: Date/Time Seized: Locatio

Location of Acquisition:

Description of Evidence				
Item #	Quantity	<b>Description of</b> <b>Item</b> (Model, Serial #, Condition, Marks,		
		Scratches)		

Chain of Custody						
Item #	Date/Time	<b>Released by</b> (Signature & ID#)	<b>Received by</b> (Signature & ID#)			

APD\_Form\_#PE003\_v.1 (12/2012) Technical Working Group on Biological Evidence Preservation. The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

### (Continued)

	Final Disposal Authority					
	Authorization for Disposal					
Item(s) #:	on this document pertaining to (suspect): is(are) no longer needed as evidence and					
is/are authorized for disposal by (check appropriate disposal method)						
$\Box$ Return to Owner $\Box$ Auction/Destroy/Divert Name & ID# of Authorizing						
Officer:						
Signature:	Date:					
	Witness to Destruction of					
	Evidence					
Item(s) #:	on this document were destroyed by Evidence					
Custodian						
Name & ID# of Wit	ID#: In my presence on (date) .					
Signature:	Date:					
	Release to Lawful Owner					
Item(s) #: ID#: Address:	on this document was/were released by Evidence Custodian					
City:	State: Zip Code:					
Telephone Number	r:( )					
Under penalty of la above item(s).	aw, I certify that I am the lawful owner of the					
Signature:	Date:					
Copy of Governme	ent-issued photo identification is attached. $\Box$ Yes $\Box$ No					
This Evidence Ch	nain-of-Custody form is to be retained as a permanent record by all parties involved.					

APD\_Form\_#PE003\_v.1(12/2012)

Page 2 of 2 pages (See front)

Technical Working Group on Biological Evidence Preservation. The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers. U.S. Department of Commerce, National Institute of Standards and Technology.

## Introduction to Network Forensics

By Nitin Sharma Cyber-crime and digital forensics have evolved a lot in last few decades. The History of Computing Project<sup>[1]</sup> defines 1947 as the beginning of the Industrial Era of Computing and we are still in the midst of this era. So much has happened in the computing since 1947 that it is helpful to break it down into manageable chunks. Digital forensics - or forensic computing as some like to call it – has a shorter history. Mark has emphasized upon some critical elements that combined to create the discipline – people, targets, tools, organizations, and the community as a whole<sup>[2]</sup>.



University of Washington, Seattle, United States <sup>[3]</sup>

With advancement of interconnecting devices in every field whether it be educational universities, large manufacturing industries, information technology companies or legal firms, the traditional computing has evolved into computing networks. This has forced the digital forensics to unfold even more specialized cross-disciplinary domains like Network Forensics.

### Network Forensics

"Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data." <sup>[4]</sup>

Network Forensics can be generally defined as science of discovering and retrieving evidential information in a networked environment about a crime in such a way as to make it admissible in court.

Network forensics follow the same basic principle of digital forensics which include data integrity, audit trail, specialist support, appropriate training, and legality. Most of the Network forensics analysis tasks are based on a rigid framework. One such popular framework for performing Network forensics analysis is OSCAR methodology<sup>[5]</sup>.



- 1. Obtain Information: The gathering of general information about the incident itself and the environment where it took place in, such as the date and time when an incident was discovered, persons and systems involved, what has initially happened, what actions have been taken since then, who is in charge, etc. The goals of investigation should be defined, written down and prioritized, as there will always be resource constraints on the investigation.
- 2. Strategize: This deals with the planning of the investigation. Acquisition should be prioritized according to the volatility of the sources, their potential value to the investigation and the effort needed to get them. This priority list should be starting point for allocating resources and personnel to conduct the present tasks such as acquiring information and evidence.
- 3. Collect evidence: Based on the plan from the previous phase, evidence is collected from each identified source. Three points must be considered,
  - Documentation
  - Capture of evidence
  - Store/Transport maintaining Chain of Custody, i.e., "showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic."
- 4. Analyze: During the analysis, an investigator recovers evidence material using a number of different methodologies and tools. The method depends on the case and what leads are already present.
- 5. Report: This will deal with conveying the results of the investigations to the client(s). It must be understandable by non-technical persons like managers, jury, etc. It must be factual and defensible in detail.

From the perspective of law enforcement officers, investigations will be conducted in response to cyber-crime incidents with appropriate incident timing <sup>[6]</sup>. This is important to understand as forensic laws differ with investigation timing.



Network Forensics with Laws

#### 1. **Pro-Active Investigations**: Occurs before cyber-crime incidents.

a. People's Reasonable Expected Privacy (The Fourth Amendment) referred to as the "right to be left alone". The Fourth Amendment protects people's reasonable privacy by limiting government agent's authority to search and seize without a warrant. Govt. Investigators cannot gather digital evidence and identify a suspect based on hunch; they must have probable cause <sup>[7]</sup>.

#### 2. **Real-Time Investigations**: Occurs during cyber-crime incidents.

- a. Title III or Wiretap Act <sup>[8]</sup> is an important statutory privacy law which prohibits unauthorized government access to private electronic communications in real time.
- b. Pen Register Act <sup>[8]</sup> also known as the Pen Registers and Trap and Trace Devices statute (Pen/Trap statute) regulates the collection of addressing and other non-content information such as packet size for wire and electronic communications.
- 3. Retro-Active Investigation: Occurs during cyber-crime incidents.
  - a. Stored Communications Act (SCA) <sup>[9]</sup> is a part of Electronic Communications Privacy Act (ECPA) which protects the privacy rights of customers and subscribers of ISPs and regulates the government access to stored content and non-content records held by ISPs.

The single most significant piece of legislation relating to privacy protection in the EU is the **General Data Protection Regulation (GDPR) (EU) 2016/679**. It supersedes the older Data Protection Directive 95/46/EC and affects all organizations that collect or process PII data if they are based in the EU or if the data belongs to a person based in the EU and limited to professional or commercial activity. This hugely impacts commercial investigation processes.

### Different Types of Network Based Evidences

There are different types of network-based evidence, all of which have pros and cons w.r.t. network forensics analysis.



- 1. **Full Content Data**: This consists of every possible single piece of information that passes across a network (or networks). This is known as "packet capture" (PCAP).
- 2. **Session Data**: This consists of aggregated metadata and usually refers to the conversation between two network entities, grouped together into "flows" and/or groups of network packets related to one another.
- 3. **Alert Data**: Whenever network traffic triggers a pre-defined item of interest (such as a particular pattern of bytes, or counts of activity, or other characteristics), the analyst will be dealing with alert data. Typically generated by Network Intrusion Detection Systems (NIDS) such as Suricata or Snort.
- 4. **Statistical Data**: This consists of different types of metadata which provide the analyst with network related aspects such as the number of bytes contained in a packet trace, start and end times of network conversations, number of services and protocols being used, average packet size, etc.

All of the above information can be used to do a definite network baselining and the deviation from such baseline will provide the definition for an incident, which further lead to network forensics. Here, we can say that incident response analyst/security analyst need to incorporate forensics while mitigating the incident. This is true from corporate perspective. However, there is quite significant thing one can notice,

Security Analyst and Incident Responders have responsibilities such as identifying affected assets, returning those assets to normal operations, preventing similar incident and so on. Network Forensics Analysts, have similar mindset while also taking care of collection of court admissible evidence for a possible legal proceeding. Maintaining proper chain-of-custody is not the only concern here to satisfy all the applicable laws and regulations.

To ascertain the legal value of evidence, some considerations are mentioned as "Guidelines for Evidence Collection and Archiving" <sup>[10]</sup> which includes,

- Admissible: It must conform to certain legal rules before it can be put before a court.
- Authentic: It must be possible to positively tie evidentiary material to the incident.
- **Complete**: It must tell the whole story and not just a particular perspective.
- **Reliable**: There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.
- Believable: It must be readily believable and understandable by a court.

### Network Forensics Analysis and Tools

Systems used to collect network data for forensics in two forms <sup>[11]</sup>:

- 1. **Catch-it-as-you-can systems**: All the packets passing through a particular traffic point are captured and written to storage. Analysis is subsequently done in batch mode. This approach requires large amount of storage. Example of such system is tcpdump.
- 2. **Stop-look and listen systems**: Each packet is analyzed in a rudimentary way in memory and only certain information is saved for future analysis. This requires a faster processor to match the pace of incoming traffic. Example of such system is NetFlow.

Before moving towards different tools, let us look at packet capture and network flow analysis <sup>[12]</sup>.

- 1. **Network Flow Analysis**: A flow is a traffic stream with a common set of identifiers. It can be defined by a traffic that has the same source IP, destination IP, protocol, source port and destination port. If any of these variables change, then a new flow is defined. For example, when a client is connecting to a server, several flows might be created because the client might establish several connections to the server, involving new source ports. Each one of these connections would be a separate flow. NetFlow, sFlow, IPFIX are all ways to collect information about traffic that is traversing a network. Most NetFlow collection applications use NetFlow v5, which tracks,
  - a. Source Interface
  - b. Source and Destination IP address
  - c. Layer 4 Protocol (for example ICMP, TCP, UDP, OSPF, etc.)
  - d. Source and Destination port number (if protocol is TCP/UDP)
  - e. Type of service value
- 2. **Packet Analysis:** Packet analysis is normally associated with SPAN or mirror ports, which are available on most managed network switches. Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or on an entire VLAN) to a network monitoring connection on another switch port. Port mirroring on a Cisco System switch is generally referred to as Switched Port Analyzer (SPAN); some other vendors have other names for it, such as Roving Analysis Port (RAP) on 3Com switches. Deep Packet Inspection is possible here to extract metadata such as application/website names. This is ideal for monitoring important applications, servers or internet connections where low-level information is critical.

Some popular general-purpose network forensics analysis tools include,

- 1. Packet Sniffers dumpcap, pcapdump and netsniff-ng
- 2. Protocol Analyzer tcpdump, wireshark/tshark and tstat.
- 3. Network Forensic Analysis Tools Xplico and Network Miner

Specific Task Tools include,

- 1. Intrusion Detection Snort, Suricata, Bro.
- 2. Match regular expressions ngrep
- 3. Extract files or pictures infex and driftnet
- 4. Sniff passwords or HTTP sessions dsniff, firesheep, Ettercap, creds
- 5. Extract emails mailsnarf, smtpcat
- 6. Print network/packet statistics ntop, tcpstat.
- 7. Extract SSL information ssldump
- 8. Reconstruct TCP flows tcpflow, tcpick
- 9. Fingerprinting p0f, prads

### Importance of Network Forensics

Network forensics is an important component of a successful security operations program. It is a significant capability that provides a data of record for the incident responders and security analysts which plays a key role in in their daily workflow. However, network forensics is not limited to security professionals and cyber-crime investigators. Their lies a definite business value in it.

- 1. Breach Response Most of the questions that organizations will have during a breach like the rapid identification of extent of damage, containment timelines, affected assets, etc., will only be answered with the help of network forensics analysis results.
- 2. Threat Hunting Detecting unusual or suspect activities like APT compromise of endpoints, etc. are very challenging scenarios that could only be handled by skilled threat hunters and network forensic analysts.
- 3. Intelligence Alerting In today's modern era, attackers are highly intelligent and sophisticated. The alerting mechanism requires the fundamental of network activity gathering as well as mature, scalable, powerful network forensics solution with a robust query language. Such an implementation can help in alerting the business execs to identify suspicious and malicious activity under the radar.

#### References

[1] The History of Computing Project, Timeline: Chronology of the history of computing, The History of Computing Foundation, Maurik, The Netherlands, 2010. Last Accessed on June 18, 2020. - thocp.net/timeline/timeline.htm

[2] Mark Pollitt. A History of Digital Forensics. 6th IFIP WG 11.9 International Conference on Digital Forensics (DF), Jan 2010, Hong Kong, China. pp.3-15, ff10.1007/978-3-642-15506-2\_1ff. ffhal-01060606f. Last Accessed on June 18, 2020. - hal.inria.fr/hal-01060606/document

[3] University of Washington [Photo], Seattle, United States, Taylor Vick, Unsplash. Last Accessed on June 18, 2020. - unsplash.com/photos/M5tzZtFCOfs

[4] Guide to Integrating Forensic Techniques into Incident Response, Timothy Grance, Suzanne Chevalier, Karen Kent Scarfone, Hung Dang, Special Publication (NIST SP) – 800-86, Published on September 1, 2006. Last Accessed on June 18, 2020. - <u>nist.gov/publications/guide-integrating-forensic-techniques-incident-response</u>

[5] Introduction to Network Forensics Handbook Final V1.1, Cybersecurity ENISA Training, Published August 2019. Last Accessed on June 18, 2020. - enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf

[6] A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation, Junwei Huang, Yinjie Chen, Zhen Ling, Kyungseok Choo, Xinwen Fu University of Massachusetts Lowell, USA + Southeast University, China. Last Accessed on June 18, 2020. pdfs.semanticscholar.org/10b8/8debc818ca1da825fb9848cfaf8dccf2aa9f.pdf

[7] Privacy and Search, Expectation of Privacy, Wikipedia. Last Accessed on June 18, 2020. Link: en.wikipedia.org/wiki/Expectation\_of\_privacy#Privacy\_and\_search

[8] H. Marshall Jarrett and Michael W. Bailie, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Washington, DC: Office of Legal Education Executive Office, 2009). Last Accessed on June 18, 2020. - justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[9] Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 2701-2712), Wikipedia. Last Accessed on June 18, 2020. - en.wikipedia.org/wiki/Stored\_Communications\_Act

[10] Legal Considerations, Guidelines for Evidence Collection and Archiving, RFC3227. Last Accessed on June 18, 2020. - tools.ietf.org/html/rfc3227

[11] Network Forensics, Wikipedia. Last accessed on June 19, 2020. – en.wikipedia.org/wiki/Network\_forensics#Overview

[12] Flow Analysis Versus Packet Analysis, What should you Choose, Netfort.com. Last Accessed on June 19, 2020. - netfort-prod.k8s.corpwebsite.gcp.rapid7.com/content/uploads/PDF/WhitePapers/NetFlow-Vs-Packet-Analysis-What-Should-You-Choose.pdf



# NETWORK FORENSICS WITH WIRESHARK

## **Prepping Wireshark**

<sup>By</sup> Ambadi MP / Mossaraf Zaman Khan

### What is Network Forensic?

Network forensics is concerned with capturing, tracking, and evaluating network activities to detect the source of threats, malware, intrusions, or breaches of security that occur on a network or in network transit. Network forensic research is also considered to be under the umbrella of digital forensics, alongside smartphone forensics or digital image forensics. It includes a detailed knowledge of specific programs and network protocols to identify attack trends. The investigator needs to consider the usual type and actions of certain protocols to distinguish the irregularities associated with an attack.

Web protocols including:

- HTTP
- HTTPS
- FTP
- SMB
- NFS

Network Protocols including:

- Ethernet protocol
- WLAN Protocol
- TCP/IP Protocol

There are two primary sources network forensics experts focused on they are :

- Packet Full capture
- Logging of files

### Packet Full Capture

Packet Full capture's main advantage is that it is possible to determine the content and therefore the meaning and value of the transmitted data. Packet capture is normally not implemented in full-time networks due to the large amount of storage required for even one hour of data on a typical business network. While most companies today allow all workers to sign an agreement that they do not have the right to privacy on business-owned systems and networks, privacy issues may exist.

Usually, data collection is applied when suspicious behavior has been observed and may still be in progress. The tap point for the packet-capture-network must be carefully selected so that it can capture traffic flowing between all affected devices, or multiple taps must be implemented.

#### Logging of files

NetFlow (or equivalent) data can be stored in full-time log files by most modern network devices, such as routers. Web, Proxy servers, firewalls, DS, DNS, DHCP, and server log files from Active Directory also provides valuable information. These log files can be analyzed to detect suspicious source and destination pairs and suspicious client behavior. One main advantage of using log files is that the size of the file is much smaller than the capture of a full packet. Another advantage is that collection points are already in place at key places, so collecting and storing data from various devices into one master log is not difficult to analyze.

Enhance the skills

A lot of free tools are available for the forensic network software. Although some have a GUI, most free tools only have a command-line GUI, and others only run on Linux. Particularly for full packet captures, data needs to be reduced before a thorough filtering analysis is carried out.

Wireshark is an open-source application which captures and displays data on and off a network. It is widely used to troubleshoot network problems and check applications as it has the ability to drill and read each packet's, and is a multi-platform, open source network analyzer running Linux, OS X, BSD, MAC, and Windows. It is particularly useful to know what is happening within your network, which accounts for its widespread use in government, business, and education. It works like TCPDump, but Wireshark adds a great graphical interface that allows you to filter, organize and order the captured data so it takes less time to analyze it. A text-based version, called Tshark, features similar.

Wireshark uses ".pcap and .pcapng" files to store the captured packets.

The ability to view data in log and capture files and identify malicious activity in the data is a special skill requiring deep knowledge of network and application protocols. This article provides a brief introduction to networked forensic investigations of suspected illegal activity linked to IT. Criminals are hacking computer networks for a variety of purposes but primarily for economic advantage. Banking and other personal information stored on PCs and servers are among the most common targets that will help to complete fraudulent financial transactions. A specific skill requiring in-depth knowledge of network and application protocols is the ability to translate data into log and capture files and detect malicious activity in the data. This article includes a brief introduction to network based forensic investigations of alleged information technology-related criminal activity.

For additional information, please refer the Wireshark User Guide -Wireshark.org/download/docs/user-GUIde.pdf

## Wireshark Basics

### Installation:

**Windows OS:** Download the latest edition of the Wireshark from Wireshark's Official Website (Wireshark.org/#download). After downloading, executing it with administrative privilege. After that install wizard appeared then install it by clicking the "Next". For that time also install the "WinPcap" with it.

**Linux OS:** Some of the Linux distributions like CSI Linux, Kali Linux, Parrot Security OS comes with Wireshark already installed. But for rest of the Linux system you can use the following steps to install in your system.

- a. Open Terminal
- b. Add the Wireshark Package [sudo add-apt-repository ppa:Wireshark-dev/stable]
- c. Update the Repository [**sudo apt-get update**]
- d. Install the Wireshark [sudo apt-get install Wireshark]

### How to Download and Install Wireshark

Wireshark can be downloaded for most Operating Systems. You will see the most recent stable release and the current release of the development. Unless you are an advanced user, get the stable version downloaded.

Download: wireshark.org/download.html

If prompted, during the Windows setup process, choose to install WinPcap or Npcap as these include the libraries required to capture live data.





Wireshark is available through the Ubuntu Universe repository. You can enable repository in the universe and then install it like this:

Installation on Ubuntu

sudo add-apt-repository universe sudo apt install wireshark

Installation on CentOS

yum install gcc gcc-c++ bison flex libpcap-devel qt-devel gtk3-devel rpm-build libtool c-ares-devel qt5-qtbase-devel qt5-qtmultimedia-devel qt5-linGUIst desktop-file-utils

sudo yum install wireshark wireshark-qt

### User Interface:

#### **Opening Wireshark**

By Double clicking on the Wireshark shortcut (Windows) or type "**Wireshark**" on terminal (Linux) to execute the Wireshark.



Fig 1: Internet Configuration details (ifconfig)

Before capturing, open your terminal and type '**ifconfig**' to know about your interface. For me, the interface is '**eth0**' and IP address is '**192.168.27.131**'.

After determining the Network Interface. Now open the Wireshark and choose the specific interface and double-click to start capture the traffic. In Figure 2, I choose **eth0** as network interface. You can also use Capture filter to capture only specific types of network packets (e.g. ARP). I will discuss in later section.

9	The Wireshark Network Analyzer	
<u>File E</u> dit <u>V</u> iew	<u>Go</u> <u>Capture</u> <u>Analyze</u> <u>Statistics</u> Telephony <u>Wireless</u> <u>Tools</u> <u>H</u> elp	
	9 🖿 🖹 🛛 🤇 🗢 🗢 🖭 看 坐 🔜 🗨 Q, Q, X	
Apply a display	filter <ctrl-></ctrl->	
	Welcome to Wireshark Captureusing this filter:	*
	otho A	Ē
	Loopback: lo	

Fig 2: Basic Interface of Wireshark

The Graphical User Interface of Wireshark is shown in the following screenshot:

	test.pcapng	0 _	_ = ×
<u>File Edit View Go Capture Analyze</u>	Statistics Telephony Wireless Tools	Help 2	
	۹ ♦ ♦ 😤 🖣 👤 📃 🛛	ି କ୍ ବ୍ ବ୍ 🎹 🛛 😗	
Apply a display filter <ctrl-></ctrl->			• ► • •
No.         Time         Source           2 0.003455492         8.8.8.8           3 1.00209742         192.168.27.131           4 1.006173827         8.8.8.8           - 5 2.003493578         192.168.27.131           - 6 2.006799934         8.8.8.3           7 3.005878844         192.168.27.131           8 3.009301015         8.8.8.8           9 4.008702434         192.168.27.131           10 4.012165977         8.8.8.8	Destination         Protocol         I           192.168.27.131         ICMP           8.8.8         ICMP           92.168.27.131         ICMP           8.8.8.8         ICMP           192.168.27.131         ICMP           8.8.8.8         ICMP           192.168.27.131         ICMP           8.8.8.8         ICMP           192.168.27.131         ICMP           8.8.8.8         ICMP           192.168.27.131         ICMP           9.8.8.8         ICMP           192.168.27.131         ICMP           9.8.8.8         ICMP           192.168.27.131         ICMP	sength Info         id=0x05c7, seq=7           98 Echo (ping) reply         id=0x05c7, seq=8           98 Echo (ping) reply         id=0x05c7, seq=9           98 Echo (ping) reply         id=0x05c7, seq=1           98 Echo (ping) reply         id=0x05c7, seq=1	/1792, ttl=128 (re //2048, ttl=64 (rep //2048, ttl=128 (re //2304, ttl=128 (re 0/2360, ttl=128 (re 0/2560, ttl=128 (r 11/2816, ttl=128 (r 11/2816, ttl=128 (re 5
11 5.009956990 192.168.27.131 12 5.01302365 8.8.8.8 Frame 6: 98 bytes on wire (784 bits) Ethernet II, Src: VMware_f5:32:6a (0 Internet Protocol Version 4, Src: 8. Internet Control Message Protocol	8.8.8.8 ICMP 192.168.27.131 ICMP ), 98 bytes captured (784 bits) on 1 90:50:56:f5:32:6a), Dst: VMware_7f:a .8.8.8, Dst: 192.168.27.131	98 Echo (ping) request id=0x05c7, seq=1 98 Echo (ping) reply id=0x05c7, seq=1 interface eth0, id 0 ie:3d (00:0c:29:7f:ae:3d)	2/3072, ttl=64 (re 2/3072, ttl=128 (r
Type: 0 (Echo (ping) reply) Code: 0 Checksum: 0xd76c [correct] [Checksum Status: Good] Identifier (BE): 1479 (0x05c7) Identifier (LE): 50949 (0xc705) Sequence number (BE): 9 (0x0009)			8
0000         00         0c         29         7f         ae         3d         00         56         f5         32           0010         00         54         55         56         00         00         80         01         f9         17         06           0020         1b         83         00         00         07         6c         05         c7         00         09         06         01         f9         17         05           0030         00         02         20         8b         07         00 <t< td=""><td>2       6a       08       00       45       00         3       08       01       0       0       1       0       1       0       1       0       1       0       1       1       0       1       1       1       1       1       1       1       1       1       1       1       1       1</td><td>Ð</td><td>0</td></t<>	2       6a       08       00       45       00         3       08       01       0       0       1       0       1       0       1       0       1       0       1       1       0       1       1       1       1       1       1       1       1       1       1       1       1       1	Ð	0
<ul> <li>Ready to load or capture</li> </ul>		Packets: 32 · Displayed: 32 (100.0%) · Dropped:	: 0 (0.0%) Profile: Default

Fig 3: Main user interface of Wireshark

- 2. Title Bar: Display the packet title or Captured file name (test.pcapng)
- 3. Menu Bar: All the tools, settings and customization options are available here.
- 4. Main Tool Bar: Shortcut of essential tools (capture, stop, save) are located
- 5. **Display Filter Bar:** You can use the custom filters here to narrow down the results. It will help to analyze the specific types of packets.
- 6. Packet List Pane: This section is reserved for the captured packet. This section displays all the packets captured in a list view along with some useful information like Source and Destination IP and Port, Time, Protocol type etc. You can customize this information from Edit > Preferences...> Appearance > Columns > Add a New Column > Give a Column Title and Select the 'Type'.
- 7. **Packet Details Pane:** This section displays information about the selected packet. This section contains almost all the information about the packet including IP Address, Port Number & Details, MAC address
- 8. Packet Bytes Pane: This section displays selected packet details in Hexadecimal view.
- 9. **Expert Information Button:** By clicking this button is shown the error and information related data etc.
- 10. **Status Bar:** It displays the status of the Wireshark and PCAP information. This section provides details about the total number of capture packets and related information.
- 11. **Profile Bar:** This section shown the current and active profile. You can change the profile by clicking on it. Right-clicking on the Profile Bar allows to **Create a New Profile** or **Manage an Existing Profile**.

Wireshark - Conf	iguration Profiles X
Search for profile	All profiles 👻
Profile	Туре
Default Bluetooth Classic No Boarcomblu	Default Global Global
MarkOnSecurity	Personal
1	
+ - 9	Created from default settings
	Cancel 🔀 Help

### Filters:

Fig 4: Profile Customization

When we start to capture the packets. It will capture everything that happens on the system's network. In those packets some are extremely useful and rest of them are useless. Filters helps us to capture a specific type of packet (like ARP) or narrow down the results of the capture packet. Wireshark mainly supports two kind of filters those are **Capture Filters** and **Display Filters**.

### Capture Filters:

Capture filter helps to capture a specific type of the packet. Except that others packet will ignored. It works before the capturing the traffic. In this situation, first you must set the capture filter then you can start the capture.

For Setting the capture filter, you will find the **Capture Filter Box** when choosing the Network Interfaces (Fig - 2, Mark-1). Or, Go to the **Capture > Capture Filters** > List of the Capture Filters. Here you can Add or Delete a custom capture filter also. **Resource:** wiki.Wireshark.org/CaptureFilters

### Display Filters:

Display filters helps to narrow down the results from captured packets. It can also be used in running process of capturing. It locates above the packet list pane (Fig - 3, Mark - 4). When you type the filter in the box it will suggest some filter. If the box shown as red then the filter is incorrect, if it shown in green then the filter is correct.

It supports the Boolean expressions, that uses for specifying the data or combine two commands. These expressions are commonly used in display filters -

or or || : OR and or && : AND gt or > : Greater than lt or < : Less than eq or == : Equals

#### Example of Display Filters:

ARP Protocol Size - **arp.proto.size** TCP URG Flag - **tcp.flags.urg** Filter through IP Source and Destination address using Boolean operator **ip.src == 192.168.27.31 or ip.dst == 10.42.30.67** 

#### **Resources:**

packetlife.net/media/library/13/Wireshark\_Display\_Filters.pdf wiki.Wireshark.org/DisplayFilters Wireshark.org/docs/dfref

### Other Useful Options:

#### **Coloring Rules:**

In Wireshark, colorizing a specific packet type is a effective method to identify and spot the packet of interest from the Packet List Pane.

Wireshark has its own predefined coloring rules. But you can add and delete the coloring rules as per your requirements. To add a new coloring rule go to **View** > **Coloring Rules...** to Add a new coloring rule click on '+' button to add a new rules and enter the Name of the rules and Filter. You can change the Foreground and the Background color is per your requirement.
Wireshark · Coloring Rules Mark	OnSecurity
Name	Filter
ARP Protocol Size	arp.proto.size 2
A Bad TCP	tcp.analysis.flags && ltcp.analysis.window_update
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	ge stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type eq 3    icmp.type eq 4    icmp.type eq 5    icmp.type eq 11    icmpv6.type eq 1    icmpv6.type eq 2    icmpv6.type eq 3    icmpv6.type eq 4
ARP	arp
	icmp    icmpv6
TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq ABORT
TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && lpim && lospf)    (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && l(vrrp    carp))
Checksum Errors	eth.fcs.status== "Bad"    ip.checksum.status== "Bad"    tcp.checksum.status== "Bad"    udp.checksum.status== "Bad"    sctp.checksum.status== "Bad"    mstp.ch
	smb    nbss    nbms    netbios
Мник	http    tcp.port == 80    http2
M DCERPC	dcerpc
Kouting	hsrp    eigrp    ospr    bgp    cdp    vrrp    carp    gvrp    igmp    ismp
M TCP SYN/FIN	tcp.flags & 0x02    tcp.flags.fin == 1
	tcp
	uap aktory e. +
	entiti or i
System Event	systemd_journal    sysdig
<	
OSDE State Channel	
+ - b Foreground	Background Apply as filter 5
0	3 OK Copy from ▼ Cancel Import Export Help

Fig 5: Coloring Rules

### **Network Statistics:**

Wireshark provide us a huge range of network statistics features. It helps to gather the general knowledge about the captured or loaded packet file. It can be accessible from Menu Bar of the Wireshark named 'Statistics'.

From the Statistics menu you can do the following things -

- 1. **Capture File Properties:** It provides general information about the captured packet. Including Name, Length, Hash value, Hardware information, Interface details, Packet data statistics etc.
- 2. **Resolved Addresses:** Mapping all the IP addresses with the Domain Name.
- 3. **Protocol Hierarchy:** All the protocol that has been captured & percentage of the packets.
- 4. **Conversations:** All the conversations between Client A to Client B of the packets. Click on **Name Resolution** on Ethernet section it allows to reveal the domain names.
- 5. **Endpoints:** Like Conversations but only display the endpoint addresses.
- 6. **Packet Lengths:** Certain amount of packet length to the destination. Including packet count and percentages from total packet.
- 7. IO graph: Graphical representation of communication between two endpoints.
- 8. **DNS:** Reveals all the DNS services
- 9. Flow Graph: Reveals all the TCP packets in a Graphical manner.

10.**HTTP > Load Distribution:** Reveals what the servers and IP addresses served for this computer system.



Fig 6: Network Statistics of Packets

### Follow Stream:

Protocol stream following is one of the powerful features. It helps you to looking for crucial data from a stream. You can follow TCP, UDP, TLS, HTTP packets from packet list pane. It also allows you to identify the login credential from HTTP Packet.

You can follow the stream by two ways:

- Select a packet which you want to follow then Right-click > Follow > TCP / UDP/ TLS Stream
- Or go to Analyze > Follow > TCP / UDP/ TLS Stream



Fig 7: Following a HTTP Stream



Fig 8: Login credentials found from HTTP Stream

## Expert Information:

Expert Information provides the deeper information in a quick way. When it tracks down any abnormalities and area of interest it raises a flag for it. You can access expert information from **Analyze** > **Expert Information** or from the left corner of the buttom (Fig 3, Mark 8)

**Red:** Indicates for Malformed packets (Error) **Yellow:** Indicates for any Warnings **Blue:** Indicates for Information (Chat) **Cyan:** Indicates for any events (Note)

Pa	cket	Summary	Group	Protocol
~	Error	New fragment overlaps old data (retransmission?)	Malformed	TCP
	839	[TCP Out-Of-Order] 443 → 8266 [PSH, ACK] Seq=49882 Ac	Malformed	TCP
×	Warning	DNS query retransmission. Original request in frame 287	Protocol	DNS
>	Warning	Connection reset (RST)	Sequence	TCP
>	Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP
5	Warning	Previous segment(s) not captured (common at capture sta	Sequence	TCP
>	Warning	Ignored Unknown Record	Protocol	TLS
-	Note	This session reuses previously negotiated keys (Session res	Sequence	TLS
×	Note	This frame is a (suspected) spurious retransmission	Sequence	TCP
>	Note	This frame is a (suspected) retransmission	Sequence	TCP
×	Note	ACK to a TCP keep-alive segment	Sequence	TCP
>	Note	TCP keep-alive segment	Sequence	TCP
>	Note	Duplicate ACK (#1)	Sequence	TCP
>	Chat	GET /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRDC9IOTx	Sequence	HTTP
×	Chat	Connection finish (FIN)	Sequence	TCP
>	Chat	Connection establish acknowledge (SYN+ACK): server por	Sequence	TCP
>	Chat	Connection establish request (SYN): server port 443	Sequence	TCP
>	Chat	NOTIFY * HTTP/1.1\r\n	Sequence	SSDP

Fig 9: Expert Information Window

# Saving a Captured Packets:

After capturing the network packets, you can also save those packets for further analysis. To save those packets go to the **File** > **Save (Ctrl+S)** > **Choose the Location** > **Give a 'Filename'** > **Choose the file type** (Default: .pcapng)



Fig 10: Saving a Network packets

This process helps you to save all the packet the captured. But sometimes the packet sizes are too huge, and you do not need all of those packets. In that scenario you choose your packet as per your needs and mark them by Right-click > Mark/ Unmark Packet or by pressing shortcut key [Ctrl+ M]. After the marking go to the **File > Export Specified Packets...** > Enter the **Name** & Choose the **File types** > **Save**.

# Wireshark Data Taster for ARP Poisoning Layer 2/3

<sup>ву</sup> Mossaraf Zaman Khan

# **Detection of ARP Poisoning**

# Introduction to ARP:

ARP stands for Address Resolution Protocol. It helps to mapping an Internet Protocol (IP) address to a Media Access Control (MAC) address i.e. machine address. IPv4 is 32bits long and the MAC address is 48bits long. So, it helps to translate 32bit address to 48bit addresses and vice versa. ARP works on layer 2 (Data link Layer) and layer 3 (Network Layer) of the OSI model.

How ARP works:

When User-A wants to establish the connection with User-B but User-A doesn't know about the User-B MAC address. The User-A sends an **ARP-Request** packet to the destination IP address (User-B's IP address). Because the destination IP address is indicating to User-B, so User-B will reply with the **ARP-Reply** packet, listening its MAC address. Now User-A has the required information to exchange the traffic with the User-B.

Ro view the ARP table:

- a. Open a command prompt
- b. type '**arp -a**'



Fig 11: How ARP Works

# ARP Poisoning:

ARP Poisoning is a type of attack, where attacker sends falsified ARP messages over the local host so attacker can link their MAC address with the victim's IP address. Once attacker's MAC is successfully authenticated with the victim's computer network, then the attacker can intercept, modify any communications to the legitimate MAC address. It is also known as Man-in-the-Middle (MITM) attack.

In Man-in-the-Middle attack attackers creates a connection between two users and intercept their communication by controlling the connection.



#### How ARP Poisoning Attack Works:

Fig 12: ARP Poisoning Attack

In ARP Poisoning attack, attacker creates a huge number of forged ARP-Request and ARP-Reply packets to overload the switch. Then ARP table is flooded with the spoofed ARP packets, and then the attacker sniff all of the packets. This time malicious attacker redirect traffic so they can obtain the sensitive information or prepare for more advanced attack.

## **ARP** Poisoning Tools:

Ettercap arpspoof Bettercap [github.com/bettercap/bettercap] Xerosploit [github.com/LionSec/xerosploit]

# Detection of ARP Poisoning through Wireshark:

Lab Configuration:

**Tool:** Ettercap - GUI [for ARP Poisoning], Wireshark [Sniffing] **Victim Machine:** Windows 7 **Attacker Machine:** Kali Linux

# Configure the Wireshark:

Wireshark should be placed in Attacker's Machine i.e. Kali Linux

When there is a large number of falsified ARP request, this is an indication of an ARP storm. It could be detected easily through Wireshark. To detect this storm, go to **Edit** > **Preferences** > **Protocols** > **ARP/RARP** > [ x ] **Detect ARP request storms**.

Wireshark · Preferenc	25	×
AODV AOL APRS AR Drone Armagetrona ARP/RARP	Address Resolution Protocol Detect ARP request storms Number of requests to detect during period 30 Detection period (in ms) 100	
Artemis ARTNET ARUBA_ERM	<ul> <li>Detect duplicate IP address configuration</li> <li>Register network address mappings</li> </ul>	

Fig 13: Detection of ARP request storms

# Getting the Victim Machine IP:

Command Prompt > Type "ipconfig" to get the IP address of Victim Machine

dows IP Configurat	inn					
aono in contragarao.						
. <u></u>	1.2					
hernet adapter Loca.	L Hre	a Co	nne	CT:	LON	
Nesi 1000 (1005-10						
Connection-specific	DNS	Suf	fix		. :	localdomain
Connection-specific Link-local IPv6 Add	c DNS	Suf	fi×			localdomain fe80::a4b1:eb74:4df3:95faz11
Connection-specific Link-local IPv6 Add	: DNS tress	Suf	fi×			localdomain fe80::a4b1:eb74:4df3:95fa×11 192 168 27 128
Connection-specific Link-local IPv6 Add IPv4 Address.	: DNS tress	Suf	fi×			localdomain fe80::a4b1:eb74:4df3:95fax11 192.168.27.128
Connection-specific Link-local IPv6 Add IPv4 Address. Subnet Mask	c DNS lress	Suf	fi×			localdomain fe80::a4b1:eb74:4df3:95fa×11 192.168.27.128 255.255.255.0

Fig 14: Windows 7 IP configuration (ipconfig)

So, Victim Machine (Windows 7): Target IP address is 192.168.27.128

# EtterCap Configuration & Launching Attack:

Step 1: Set System Configuration (sysctl) for forwarding IPv4 packet. This is allows to
movement the packets through attacker's system.
# sysctl -w net.ipv4.ip\_forward=1



#### Fig 15: sysctl Configuration

**Step 2**: Search on Kali linux for Ettercap-graphical and execute it with root access.



Fig 16: Ettercap Graphical

**Step 3:** Click on **Search** button. It will automatically search for the available host on the network. From Fig-14 we know our target IP is **192.168.25.128**. So set the IP for ARP Poisoning Attack.

1 9 🛢	6 and	Ettercap 0.8.3 (EB)	٩	۲	:	•	×
Targets ×	Host List ×						
IP Address	MAC Address	Description					
fe80::a4b1:eb74:4	4df3:95fa 00:0C:29:E0:4F:76						
192.168.27.2	00:50:56:F5:32:6A						
192.168.27.128	00:0C:29:E0:4F:76	2					
192.168.27.254	00:50:56:E0:D1:F6						

Fig 17: Gathering the Live Host

**Step 4:** Now choose the "**ARP Poisoning**" Attack from the drop-down menu and checkmark for the **Sniff Remote Connection**. Click OK to Continue

	1	Ettercap 0.8.3 (EB)	0	0	•	•	×
Targets × Host List	:						
IP Address M	Cancel	MITM Attack: ARP Poisonin 3	OK				
fe80::a4b1:eb74:4df3:95fa 00	C	Optional parameters					
192.168.27.2 00	2 C	Sniff remote connections					
192.168.27.128 00			<u>`</u>				
192.168.27.254 00		- Only poison one-way.					

Fig 18: Selecting the Attack Type

**Step 5:** Start the Wireshark and choose the interface (eth0) and start capturing. The go back to Ettercap and click on red circle to start the attack.

Ettercap 0.8.3 (EB)	3	۲	:	-	•	×
Description						
4F:76						
32:6A						
4F:76						
D1:F6						
	Description 4F:76 32:6A 4F:76 D1:F6	Ettercap 0.8.3 (EB) Description 4F:76 32:6A 4F:76 D1:F6	Ettercap 0.8.3 (EB) ③ Description 4F:76 32:6A 4F:76 D1:F6	Ettercap 0.8.3 (EB)	Ettercap 0.8.3 (EB)	Ettercap 0.8.3 (EB) ● ● : - □ 5 Description 4F:76 32:6A 4F:76 D1:F6

Fig 19: Launching the ARP Poisoning attack

**Step 6:** Now in Victim Machine (Win 7). Victim access the **testphp.vulnweb.com** site and enter the login credential. That also captured via the Ettercap. Username: **test** & Password: **test** 

192.168.27.128	00:0C:29:E0:4F:76	
192.168.27.254	00:50:56:E0:D1:F6	
Delete Host	Add to Target 1	Add to Target 2
DHCP: [192.168.27.254] OF DHCP: [00:50:56:C0:00:08 DHCP: [192.168.27.254] OF HTTP : 176.28.50.165:80 -> CONTENT: uname=test&pa	FER : 192.168.27.1 255.255.255.0 GW invalid DISCOVER FER : 192.168.27.1 255.255.255.0 GW invalid USER: test PASS: test INFO: http://testphp.vulnweb.c ss=test	com/login.php

### Fig 20: Gathering Credential by ARP Poisoning

# Packet Analysis using Wireshark:

**Step 1:** After attacking, stop the packet capture in Wireshark and save into a pcap file for further investigation.

**Step 2**: Analyze the captured Packets using Wireshark. You will notice a flood of ARP packets are captured. And some packets also tells that "**duplicate use of 192.168.27.128 detected**". That's our victim's IP address. And it also tells us "**duplicate use of 192.168.27.2 detected**" that is our default gateway (shown in Fig 14). In Packet Details Pane tells us about the position where duplicate IP address is detected.

File Edit View Go C	apture Analyze Statistics Telephony Wireless Tools Help				
	( C 4 * * * * * * = = e e e e				
Apply a display filter <ctr< td=""><td>H/&gt;</td><td></td><td></td><td></td><td></td></ctr<>	H/>				
No. Time	Source	Destination	Protocol	Length Info	^
• 1 0.00000000	VMware_7f:ae:3d	VMware_e0:d1:f6	ARP	42 192.168.27.128 is at 00:0c:29:7f:ae:3d	
2 0.000241390	VMware_7f:ae:3d	VMware_e0:4f:76	ARP	42 192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	
3 0.010561388	VMware_7f:ae:3d	VMware_e0:d1:f6	ARP	42 192.168.27.2 is at 00:0c:29:7f:ae:3d	
4 0.010594194	VMware 7f:ae:3d	VMware f5:32:6a	ARP	42 192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)	
5 0.021258537	VMware_7f:ae:3d	VMware_e0:4f:76	ARP	42 192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	
6 0.021928303	VMware_7f:ae:3d	VMware_e0:d1:f6	ARP	42 192.168.27.128 is at 00:0c:29:7f:ae:3d	
7 0.032548356	VMware_7f:ae:3d	VMware_e0:4f:76	ARP	42 192.168.27.2 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	_
8 0.032698988	VMware_7f:ae:3d	VMware_f5:32:6a	ARP	42 192.168.27.128 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)	
9 0.043555827	VMware_7f:ae:3d	VMware_f5:32:6a	ARP	42 192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)	_
10 0.043687929	VMware_7f:ae:3d	VMware_e0:d1:f6	ARP	42 192.168.27.2 is at 00:0c:29:7f:ae:3d	
11 0.054061127	VMware_7f:ae:3d	VMware_f5:32:6a	ARP	42 192.168.27.128 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)	
12 0.054291765	VMware_7f:ae:3d	VMware_e0:4f:76	ARP	42 192.168.27.2 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	
13 9.331658609	192.168.27.128	192.168.27.2	DNS	97 Standard query 0xe80b A firefox.settings.services.mozilla.com	
<pre>&gt; Ethernet II, Srci V ) Address Resolution &gt; Idoress Rowing e &gt; [Expert Info [Seconds since e &gt; [Doplicate IP addre [Seconds since e &gt; [Doplicate IP addre &gt; [Expert Info &gt; [Expert Info &gt; [Severity] [Group: Set</pre>	<pre>Wware_frime:3d (00:06:129:7f:ae:3d), Dst: VWware_06:4f?? Protocol (reply) ss detected for 192.168.27.254 (00:06:229:7f:ae:3d) - als arlier use of PL address: 1 (Warning/Sequence): Duplicate IP address configured (192 IP address configured (192.168.27.254)] uence] arlier frame seen: 0] ss detected for 192.168.27.128 (00:06:229:e0:4f:76) - als arlier use of IP address: 1 (Warning/Sequence): Duplicate IP address configured (192 IP address configured (192.168.27.128)] uencel IP address configured (192.168.27.128)] uencel</pre>	<pre>(00:0::29:e0:47:76) to in use by 00:50:56 .168.27.254)] to in use by 00:00:29 .168.27.128)]</pre>	:e0:d1:f6 :7f:ae:3d	(frame 1)] (frame 1)]	
0000 00 0c 29 e0 4f	ariler frame seen: 0j 76 00 0c 29 7f ae 3d 08 06 00 01 ··)·Ov·· )··=··· 32 00 0c 29 7f ae 3d c0 a8 1b fe ······)·=···				
0020 00 0c 29 e0 4f	76 c0 a8 1b 80				

Fig 21: Packet Analysis using Wireshark

Step 3: If we are analyze the Expert Information Section. It also raises a warning for "**Duplicate IP address Configured**" for 79 times. By expanding this area, we can easily navigate to those packets where duplicate IP address was used. That is also a clear indication of ARP Poisoning.

<b>4</b> w	ireshark • <mark>E</mark>	xpert Information • arp_posioning.pcapng			_25		×
Pack	et	Summary	Group	Protocol	Count		^
> E	rror	New fragment overlaps old data (retransmission?)	Malformed	TCP		19	98
> V	Varning	Connection reset (RST)	Sequence	TCP			4
> V	Varning	This frame is a (suspected) out-of-order segment	Sequence	TCP		54	47
> V	Varning	DNS response retransmission. Original response in frame 17	Protocol	DNS		2	28
> V	Varning	DNS query retransmission. Original request in frame 13	Protocol	DNS		2	22
~V	Varning	Duplicate IP address configured (192.168.27.254)	Sequence	ARP/RARP		7	79
	2	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	Sequence	ARP/RARP			_
	2	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	Sequence	ARP/RARP			
	4	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)	Sequence	ARP/RARP			
	4	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)	Sequence	ARP/RARP			
	5	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	Sequence	ARP/RARP			

Fig 22: ARP Poisoning detection by Expert Information

# The Delicious Network Layer Layer 3

<sup>By</sup> Nitin Sharma

# Layer 3 – The Network Layer Explained

A quick review: In the seven-layer OSI model, Layer 3 is known as Network Layer. This layer is the part of Internet communication process where network-to-network connections occur, by sending packets of data back and forth between different networks. The network layer uses 4 basic processes <sup>[1]</sup>:

**Addressing end devices** – In the same way, that a phone has a unique telephone number, end devices must be configured with a unique IP address for identification on the network. An end device with a configured IP address is referred to as a host.

**Encapsulation** - The network layer receives a protocol data unit (PDU) from the transport layer. In a process called encapsulation, the network layer adds IP header information, such as the IP address of the source (sending) and destination (receiving) hosts. After header information is added to the PDU, the PDU is called a packet.

**Routing** - The network layer provides services to direct packets to a destination host on another network. To travel to other networks, the packet must be processed by a router. The role of the router is to select paths for and direct packets toward the destination host in a process known as routing. A packet may cross many intermediary devices before reaching the destination host. Each route the packet takes to reach the destination host is called a hop.

**De-encapsulation** - When the packet arrives at the network layer of the destination host, the host checks the IP header of the packet. If the destination IP address within the header matches its own IP address, the IP header is removed from the packet. This process of removing headers from lower layers is known as de-encapsulation. After the packet is de-encapsulated by the network layer, the resulting Layer 4 PDU is passed up to the appropriate service at the transport layer.



Data Encapsulation at OSI Layers<sup>[2]</sup>

### Network Layer Protocols

There are several protocols operating at the Network Layer protocol suite which includes CLNS, DDP, EGP, EIGRP, etc. However, some commonly implemented protocols that are utilized more often include:

- 1. Internet Protocol (IPv4 and IPv6)
- 2. Internet Message Control Protocol (ICMP)

# IP Protocol

Host-to-Host network-layer delivery protocol for the internet with the following properties:

- Connectionless No connection with the destination is established before sending data packets.
- Best Effort (unreliable) Does its best to deliver packet but packet delivery is not guaranteed. Limited error controls and corrupted packets are discarded.
- No flow-control.
- Must be paired with a reliable transport TCP and/or application layer protocol to ensure reliability.
- Encapsulate the Transport Layer "Segment" by adding an IP header.

Offsets	Octet				(	0							1	1								2								3			
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	7 18	19	20	21	22	23	24	2	25 26	27	28	3 29	30	31
0	0		Vers	sion			⊪	L				DS	CP			EC	CN							٦	otal	Leng	gth	l					
4	32							lo	dentif	icati	on							Flags Fragment Offset															
8	64			Ti	Time To Live Protocol									Header Checksum																			
12	96								Source IP Address																								
16	128														D	estir	atio	n IP	Add	dress													
20	160																																
24	192															Onti	one	/if I∟	JI ~	5)													
28	224															Opti	0115	(n n	122	> 0)													
32	256																																

#### 32-bit IPv4 Header <sup>[3]</sup>

### Internet Protocol Version 4 (IPv4)

An IP packet consists of a header section and a data section. An IP packet has no data checksum or any other footer after the data section. Typically, the Data Link Layer encapsulates IP packets in "Frames" with a CRC footer that detects most errors, and typically the end-to-end TCP layer checksum detects most other errors.

Significant fields in IPv4 header include:

**1. Version** - Contains a 4-bit binary value identifying the IP packet version. For IPv4 packets, this field is always set to 0100.

**2. Differentiated Services** - Formerly called the *Type of Service (ToS)* field, the DS field is an 8-bit field used to determine the priority of each packet. The first 6 bits identify the Differentiated Services Code Point (DSCP) value that is used by a quality of service (QoS) mechanism. The last 2 bits identify the explicit congestion notification (ECN) value that can be used to prevent dropped packets during times of network congestion.

**3. Time-to-Live (TTL)** - Contains an 8-bit binary value that is used to limit the lifetime of a packet. It is specified in seconds but is commonly referred to as hop count. The packet sender sets the initial time-to-live (TTL) value and is decreased by one each time the packet is processed by a router or hop. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. The traceroute command uses this field to identify the routers used between the source and destination.

**4. Protocol** - This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. Common values include ICMP (1), TCP (6), and UDP (17)

**5. Source IP Address** - Contains a 32-bit binary value that represents the source IP address of the packet (Identifies where the packet is from)

**6. Destination IP Address** - Contains a 32-bit binary value that represents the destination IP address of the packet. (Identifies where the packet is going)

The remaining fields are used to identify and validate the packet, or to reorder a fragmented packet. These include:

**1. Internet Header Length (IHL)** - Contains a 4-bit binary value identifying the number of 32-bit words in the header. The IHL value varies due to the Options and Padding fields. The minimum value for this field is 5 (i.e.,  $5 \times 32 = 160$  bits = 20 bytes) and the maximum value is 15 (i.e.,  $15 \times 32 = 480$  bits = 60 bytes).

**2. Total Length** - Sometimes referred to as the Packet Length, this 16-bit field defines the entire packet (fragment) size, including header and data, in bytes. The

minimum length packet is 20 bytes (20-byte header + 0 bytes data) and the maximum is 65,535 bytes.

**3.** Header Checksum - The 16-bit field is used for error checking of the IP header.

The checksum of the header is recalculated and compared to the value in the checksum field. If the values do not match, the packet is discarded.

A router may have to fragment a packet when forwarding it from one medium to another medium. When this happens, fragmentation occurs and the IPv4 packet uses the following fields to keep track of the fragments:

**1. Identification** – This 16-bit field uniquely identifies the fragment of an original IP packet.

**2. Flags** – The 3-bit field identifies how the packet is fragmented. It is used with Fragment Offset and Identification fields to help reconstruct the fragment into the original packet.

**3. Fragment Offset** – This 13-bit field identifies the order in which to place the packet fragment in the reconstruction of the original unfragmented packet.

# Types of IPv4 Addresses

**1. Public Addresses** – Designated for use in networks that are accessible on the Internet.

**2. Private Addresses** – Blocks of Addresses that are used in networks that require limited or no Internet Access. [per RFC 1918]

- **a.** 10.0.0.0 to 10.255.255.255 (10.0.0/8)
- **b.** 172.16.0.0 to 172.31.255.255.255(172.16.0.0/12)
- **c.** 192.168.0.0 to 192.168.255.255(192.168.0.0/16)

Note: Per RFC 6598, IANA reserved another group of addresses know as shared address space intended for use in service provider networks with address block 100.64.0.0/10

## Special Use IPv4 Addresses

### 1. Network and Broadcast Addresses –

- a. First address of Network  $\rightarrow$  Network Address
- b. Last address of Network  $\rightarrow$  Broadcast Address

**2.** Loopback Address – For testing purposes, this is a special address to direct traffic to itself. [127.0.0.1]

**3. Link Local Addresses** – Address block 169.254.0.0 to 169.254.255.255 [169.254.0.0/16] are designated as link-local addresses. These addresses can be

automatically assigned to the local to the local host by the operating system in environments where no IP configuration is available.

**4. TEST-NET Addresses** – Address block 192.0.2.0 to 192.0.2.255 (192.0.2.0/24) is set aside for teaching and learning purposes. Can be used in documentation and network examples with domain names example.com or example.net in RFCs, vendor docs, etc.

**5. Experimental Addresses** – The addresses in the block 240.0.0.0 to 255.255.255.254 are listed as reserved for future use (per RFC 3330)

## Legacy Classful Addressing

Per RFC 1700 Assigned Numbers, the unicast ranges are grouped into specific sizes called Class A, Class B, and Class C addresses. Use of single such address space for complete network is referred to as classful addressing.

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network ()) and Host ()) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
В	128-191	1000000040111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
с	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,152 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

IP Address Classes [4]

# Limitations of IPv4

1. IP Address Depletion (Limited IPv4 availability while internet connected devices still increasing)

2. Internet Routing Table Expansion (IPv4 routes consume a great deal of memory and processor resources on the Internet routers)

**3.** Lack of end-to-end connectivity (Public IPv4 is shared while internal NAT IPs remain hidden which is problematic for technologies that require end-to-end connectivity)

# Internet Protocol Version 6 (IPv6)

Improvements over IPv4 includes increase in address space, improved packet handling, NAT elimination and integrated security.



128-bit IPv6 Header <sup>[5]</sup>

**1. Version** - This field contains a 4-bit binary value identifying the IP packet version. For IPv6 packets, this field is always set to 0110.

**2. Traffic Class** - This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field. It also contains a 6-bit Differentiated Services Code Point (DSCP) value used to classify packets and a 2-bit Explicit Congestion Notification (ECN) used for traffic congestion control.

**3.** Flow Label - This 20-bit field provides a special service for real-time applications. It can be used to inform routers and switches to maintain the same path for the packet flow so that packets are not reordered.

**4. Payload Length** - This 16-bit field is equivalent to the Total Length field in the IPv4 header. It defines the entire packet (fragment) size, including header and optional extensions.

**5. Next Header** - This 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol. This field is also used if there are optional extension headers added to the IPv6 packet.

**6.** Hop Limit - This 8-bit field replaces the IPv4 TTL field. This value is decremented by one by each router that forwards the packet. When the counter reaches 0 the packet is discarded and an ICMPv6 message is forwarded to the sending host, indicating that the packet did not reach its destination.

7. Source Address - This 128-bit field identifies the IPv6 address of the sending host.

**8. Destination Address** - This 128-bit field identifies the IPv6 address of the receiving host

**9. Extension Headers** – Optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, etc.

## IPv6 Address and Prefix Notation

The IPv6 convention is different from dotted decimal address notation of IPv4. The 128 bits in the IPv6 address <sup>[6]</sup>:

**1.** Are written as eight 16-bit hexadecimal blocks separated by colons ( not case sensitive)

**2.** Use abbreviations to simplify the notation

**3.** Omit (optionally) leading zeroes.

**4.** Use double colons (::) to replace consecutive zeros (or leading or trailing zero strings), but never more than once per address.

So, an address like: **2eba:0000:0000:0241:cbfa:8bc5:0000** can be written as: **2eba:0:0:0:241:cbfa:8bc5:0** or **2eba::0241:cbfa:8bc5:0** 

#### but not as: 2eba::0241:cbfa:8bc5::

Routers seldom have to worry about complete ("host") addresses because their routing tables (and the forwarding tables they are based on) usually employ a prefix and examine only the number of bits that match the longest entry in the table. This is the "longest match" rule, and ensures that a 64-bit prefix (if present) is preferred over a 32-bit prefix; when the first 32 bits of a packet's destination address are the same in both table entries (longest match wins). Prefixes used for routing are defined in IPv6 by RFC 4291. So, the IPv6 address:

2eba:0000:0000:0241:cbfa:8bc5:5c85/64 has as a 64-bit prefix of 2bfc:0000:0000:0000:

## ICMP (Internet Control Message Protocol)

The Internet Control Message Protocol is a layer 3 protocol used by network devices to diagnose network communication issues. The ICMP packet is encapsulated in an IPv4 packet. The ICMP packet consists of header and data sections <sup>[7]</sup>.

												IC	MP H	lead	er F	orm	at																
Offsets	Octet		0							1							2							3									
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Тур	be							Co	de					1.1		Ch	ecks	um			-										
4	32	Re	st of	Hea	der																												

The ICMP header starts after the IPv4 header and is identified by IP protocol number '1'. All ICMP packets have an 8-byte header a variable-sized data section.

- **a**. TYPE ICMP type
- **b**. CODE ICMP subtype

**c**. Checksum – Internet checksum for error checking, calculated from the ICMP header and data with value 0 substituted for this field.

**d**. Rest off Header – Four bytes field, contents based on the ICMP type and code.

**Primary Use Case**: Error Reporting. To determine whether or not data is reaching its intended destination in a timely manner.

#### Supporting use cases include:

- 1. Source Quench Message: ICMP will take source IP from the discarded packet and informs to source by sending this message. (to reduce speed of transmission)
- **2. Parameter Problem**: ICMP will take source IP from the discarded packet and informs to source by sending parameter problem message. (Calculated Header Checksum mismatched to Received Header Checksum)
- **3. Time Exceeded Message** ICMP will take source IP from discarded packet and informs to the source, of discarded datagram due to time to live field reaches to zero, by sending time exceeded message
- **4. Destination Unreachable**: This is generated by host or its inbound gateway to inform the client that the destination is unreachable for some reason
- **5. Redirection Mess**age: Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route)

# **Routing Basics**

A host can send a packet to:

1. **Itself** – Pinging itself by sending a packet to special IPv4 address of 127.0.0.1 which is referred to as the loopback interface. [Direct Connection]

2. **Local Host** – This is a host on the same network as the sending host. The hosts share the same network address. [Local Network Route]

3. **Remote Host** – This is a host on a remote network which do not share the same network address. [Local Default Route]

#### **Default Gateway**

The default gateway is the device that routes traffic from the local network to devices on remote networks. In a home or small business network, the default gateway is often used to connect the local network to the Internet.

Note: A host device does not maintain routing information beyond the local network, to reach remote destinations. This is done by default gateway by maintaining a route table.

#### **IPv4 Routing Table**

Running the "**netstat -r**" or "**route -n**" command over a Linux host displays the host route table.

<pre># netstat -r</pre>						
Kernel IP rout	ing table					
Destination	Gateway	Genmask	Flags	MSS	Window	irtt Iface
192.168.0.0	*	255.255.255.0	U	0	0	0 eth0
link-local	*	255.255.0.0	U	0	0	0 eth0
default	192.168.0.1	0.0.0.0	UG	0	0	0 eth0

Routing Table: Linux

1. **Destination** – Lists the reachable networks.

**2. Gateway** – Lists the address used by the local computer to get to a remote network destination.

**3. Genmask/Netmask** – Lists a subnet mask that informs the host how to determine the network and the host portions of the IP address.

**4.** Flags – U $\rightarrow$ Route is Up, G $\rightarrow$ Route is to Gateway, H $\rightarrow$ Route is to Host, D $\rightarrow$ Route is created by Redirect, M $\rightarrow$ Route is modified by Redirect.

**5. MSS** – Max. Segment Size field for TCP header specify the largest amount of data in bytes that a computer can receive in a single TCP segment.

6. Window – TCP Window Size in bytes.

7. irtt – Initial Round Trip Time for TCP connections over this route.

**8.** Iface – Outbound NIC name.

## **Router: Introduction**

A router is a computer, L3 device. There are many types of infrastructure routers available. Cisco routers are designed to address the needs of:

 Branch – Teleworkers, small business, and medium-size branch sites, Includes Cisco 800, 1900, 2900, and 3900 Integrated Series Routers (ISR) G2 (2nd generation)
 WAN – Large businesses, organizations, and enterprises. Includes the Cisco Catalyst 6500 Series Switches and the Cisco Aggregation Service Router (ASR) 1000.
 Service Provider – Large service providers. Includes Cisco ASR 1000, Cisco ASR 9000, Cisco XR 12000, Cisco CRS-3 Carrier Routing System, and 7600 Series routers.

The focus of CCNA certification is on the Branch family of routers. Regardless of their function, size or complexity, all router models are essentially computers. Routers also require:

- Operating System (OS) Required to provide routing and switching functions. The Cisco Internetwork Operating System (IOS) is the system software used for most Cisco devices regardless of the size and type of the device.
- Central Processing Unit (CPU) To execute OS instructions such as System Initialization, routing functions, and switching functions.
- Random Access Memory (RAM) To store various applications and processing including: Cisco IOS, Running configuration files, IP routing table, ARP cache, Packet Buffer, etc.

• Read Only Memory (ROM) – To store bootup instructions, basic diagnostic software and Limited backup version of the OS.

Memory	Volatile / Nonvolatile	Stores
RAM	Volatile	Running IOS Running Configuration IP Routing and ARP tables Packet Buffer
ROM	Nonvolatile	Bootup instruction Basic diagnostic software Limited IOS
NVRAM	Nonvolatile	Startup configuration file
Flash	Nonvolatile	IOS Other system files

Router Memory

### IPv4 vs IPv6

Basis	IPv4	IPv6
Size of IP Address	IPv4 has 32-bit address length.	IPv6 has 128-bit address length.
\ddressing Method	IPv4 utilizes dotted decimal notation.	IPv6 utilizes hexadecimal convention with colon separation.
Number of Header Fields	14	8
Length of Header Fields	20	40
Checksum	Yes	No
Type of Addresses	Unicast, Broadcast and Multicast	Unicast, Multicast and Anycast
Example	192.168.34.21	2839:0dfc:0000:0000:ff53:0043:5aea:00ed
No. of Classes	5 [A <b>→</b> E]	IPv6 allows storing an unlimited no. of IP Address.
Configuration	Required for newly installed system.	Optional
VLSM Support	Yes	No
Fragmentation	Done by sending and forwarding routes.	Done by sender.
Routing Information Protocol	Yes	No. Only Static routes.
NAT	Yes	No. Only Direct addressing.
Address Mask	Yes	No
SNMP Support	Yes	No
Security	Dependent on applications.	IPSec built in. Needs to be enabled.
Authentication	No	Yes
Encryption	No	Yes
QoS Handling Packet Header	No	Yes

IP to MAC resolution	Broadcast ARP	Multicast Neighbor Solicitation
Local Subnet Group Mgmt.	IGMP	MLD
Mapping	ARP	NDP

## Network Layer: Attacks and Security Measures

There are several attacks that could be performed to compromise/disrupt the Network Layer. As we know, the main responsibility of the network layer is to transmit the packets from the source to the destination by finding the best route, which is the route that has the lowest cost and shortest path between source and destination, the major goal is to disrupt this path. Some of the attacks related to network layer are discussed below <sup>[8]</sup>.

**1. IP Spoofing Attack:** Used to gain unauthorized access to the servers when attacker spoofed its own IP address with a "trusted" IP address such that victim will not understand the source of traffic is malicious. The main root cause of DDoS attacks is IP spoofing.



#### Security Measures to mitigate IP Spoofing:

**a.** Use AUTH(N) based on Key Exchange between the machines on your network; IPv6 has IPSec built-in that can significantly cut down the risk of IP Spoofing.

- **b.** Use of an ACL to deny private IP addresses on the downstream interfaces.
- c. Implementing filters on both Inbound and Outbound traffic.

**d.** Configure Routers and Switches to reject packets originating from outside of local network that claim to originate from within.

**e.** Enable encryption sessions on the routers so that trusted hosts outside the network can securely communicate with the local hosts.

2. Hijacking Attack: The basic idea for this attack is to disrupt a session between client and server and take over the IP address of the trusted client. In the next step, the attacker will discontinue the communication between the server and the trusted client and create a new session with server pretending to be the trusted client. This might require additional capture efforts for information like authentication cookie, session IDs, BGP etc. along with trusted IP.



Security Measures to mitigate Hijacking Attack:

- a. Utilizing advanced encryption methods,
- **b.** Different AUTH(N) mechanisms.
- c. IP Prefix Filtering
- **d.** BGP Hijacking Detection.

**3. The Smurf Attack**: The attacker will send a high number of packets from a spoofed IP address to the server in order to disable the service provided by the network. An example of this attack will be similar to ICMP request flooding or ping

flood by using an IP broadcast address. The slight difference is due to an amplification attack vector that boosts its damage potential by exploiting characteristics of broadcast network.



Security Measures to mitigate Smurf Attacks and Ping Floods:

- **a.** Blanket Block pings from outside networks.
- **b.** Deploy DDoS protection solution

**4.** Wormhole Attacks: Wormhole nodes fake a route that is shorter than the original one within the network to confuse routing mechanisms which rely on distance between the nodes. The attackers will record the packets at one point of the network and retransmits them to another point of the network using private highspeed network, and then replays them into the network from that point. Such kind of attacks are a serious threat against network routing protocols. Mostly seen in wireless sensor networks.



Security Measures to mitigate Wormhole Attack:

**a.** A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Use Geographical and Temporal Leashes.

#### **b.** Digital Signature Based Approach

- c. Protocol Specific Solutions
- d. SAM (Statistical Analysis of Multipath)

**5.** Blackhole Attack: The attacker will capture all the packets and discard them instead of forwarding them to the destination. The effectiveness of the network will be decreased during this attack, while important packets will not reach the destination. Network parameters such as delay and throughput will be changed during the blackhole attack. The delay will be increased because the packets will not be delivered to the destination. The throughput will become very less, while it will be used from the blackhole attacker. It's a kind of DoS Attack. It is also known as Packet Drop Attack.



Security Measures to mitigate Blackhole Attack:

- a. IDS (Intrusion Detection System)
- **b.** Cross Checking Data Routing Information (DRIs)
- c. Using Destination Sequence No. Parameter of Reply Packet with threshold.

#### References

[1] Network Layer, Data Communication, TeachWeb Milinis Reference. Accessed on 14th June 2020.

Link: teachweb.milin.cc/datacommunicatie/tcp\_osi\_model/network\_layer.htm

[2] Data Encapsulation and De-encapsulation Explained [Image] Accessed on 16th June, 2020.

Link: computernetworkingnotes.com/ccna-study-GUIde/data-encapsulation-and-de-encapsulation-explained.html

[3] IPv4 [Image], Wikipedia. Accessed on 14th June 2020. Link: en.wikipedia.org/wiki/IPv4

[4] Legacy Classful Addressing [Image], IPv4, Network Layer, TCP OSI Model, TeachWeb Millinis Reference. Accessed on 14th June 2020 Link:

teachweb.milin.cc/images/datacommunicatie/introduction\_to\_networks/8.1.4.4\_leg acy\_classful\_addressing\_small.jpg

[5] IPv6 Packet Format, Network Layer and Routing, Computer Networking [Image]. Accessed on 14th June 2020.

Link: expertsmind.com/CMSImages/426\_IPv6%20packet%20Format.png

[6] Differences in Addressing Between IPv4 and IPv6, Juniper Networks. Accessed on 15th June 2020.

Link: juniper.net/documentation/en\_US/learn-about/ipv4-ipv6-differences.pdf

[7] Datagram Structure, ICMP, Wiki. Accessed on 16<sup>th</sup> June 2020. Link: en.wikipedia.org/wiki/Internet\_Control\_Message\_Protocol

[8] A review of Network Layer and Transport Layer Attacks on Wireless Networks, Edvald Sula, International Journal of Modern Engineering Research (IJMER), 9th Feb, 2019. Accessed on 16th June 2020. Link: ijmer.com/papers/Vol8\_issue12/D0812012327.pdf

# Taking a Bigger Bite With Wireshark Layer 3/4

By Ambadi MP

# Packet Capturing With WireShark

Click on the Wireshark icon after downloading and installing Wireshark and start Wireshark.

Apply a display filter <c< th=""><th>H-[&gt;.</th></c<>	H-[>.
	Welcome to Wireshark         Capture        seng the filter         Whware Network Adapter VMnet8         Vithemet (Default Switch)         Vithaure Network Adapter VMnet8         Local Area Connection* 7         Vithaure Network Adapter VMnet8         Vithaure Network Adapter VMnet8         Local Area Connection* 8         Local Area Connection* 6         Vithaure (SwitchName)         Local Area Connection* 6         VitualBox Host-Only Network         Adapter for loopback traffic capture         Adapter for loopback traffic capture         Adapter for loopback traffic capture         Local Area Connection         Local Area Connection
	Learn
	Base's Colds - 1906 - Constitute and Annuals - Mailing Lints

This screen allows you to select the network interface you wish to capture the packets from. As you can see, Wireshark has detected all interfaces.

- Ethernet,
- Local Area Connection 2
- Bluetooth Network Connection
- Wi-Fi

Depending on the network interfaces of your system yours may appear differently.

# Windows Analysis

di, I	<b>.</b> 🥹 💿 🔚 🗄					
A	oply a display filter	<ctrl-></ctrl->				
о.	Time	Source	Destination	Protocol	Length Info	
	422 35.231122	192.168.1.33	224.0.0.22	IGMPv3	70 Membership	Report / Join
	423 38.000575	192.168.1.36	1.1.1.1	DNS	77 Standard qu	ery 0x3433 A c
	424 38.149007	192.168.1.36	192.168.1.33	AJP13	164 AJP13 Error	? [TCP segment
	425 38.153491	192.168.1.33	192.168.1.36	AJP13	164 AJP13 Error	? [TCP segment
	426 38.153549	192.168.1.36	192.168.1.33	TCP	54 18778 → 800	9 [ACK] Seq=88
	427 39.930164	192.168.1.36	52.157.234.37	TCP	1494 1862 → 443	[ACK] Seq=5228
F	rame 1: 60 byte thernet II, Src ata (46 bytes)	s on wire (480 bits), :: currento_0e:be:c8 (	, 60 bytes captured (48 (14:a7:2b:0e:be:c8), Ds	0 bits) on t: Broadca	interface \Device st (ff:ff:ff:ff:ff	> \NPF_{438B604I :ff)
Fi Di	rame 1: 60 byte thernet II, Src ata (46 bytes)	s on wire (480 bits), : currento_0e:be:c8 (	, 60 bytes captured (48 (14:a7:2b:0e:be:c8), Ds	00 bits) on t: Broadca:	interface \Device st (ff:ff:ff:ff:ff	> \NPF_{438B604L :ff)
F	rame 1: 60 byte thernet II, Src ata (46 bytes)	s on wire (480 bits), :: currento_0e:be:c8 (	, 60 bytes captured (48 (14:a7:2b:0e:be:c8), Ds	00 bits) on t: Broadca:	interface \Device st (ff:ff:ff:ff	> \NPF_{438B604L :ff)
F D	rame 1: 60 byte thernet II, Src ata (46 bytes) 0 <b>ff ff ff ff</b>	s on wire (480 bits); :: currento_0e:be:c8 ( ff ff 14 a7 2b 0e be	, 60 bytes captured (48 (14:a7:2b:0e:be:c8), Ds : c8 ff fa de ad	00 bits) on t: Broadca: +	interface \Device st (ff:ff:ff:ff:ff	> \NPF_{438B604D :ff)
F D D	rame 1: 60 byte thernet II, Sro ata (46 bytes) 0 <b>ff ff ff</b> ff 0 be ef 01 72	ff ff 14 a7 2b 0e be 56 61 6c 74 65 6b 5f	, 60 bytes captured (48 (14:a7:2b:0e:be:c8), Ds e c8 ff fa de ad f 6c 6f 6f 70 62r	00 bits) on t: Broadca: + ealt ek_loc	interface \Device st (ff:ff:ff:ff:ff ppb	> \NPF_{438B604D :ff)
Fi D: 0000 010 024	rame 1: 60 byte thernet II, Sro ata (46 bytes) 0 ff ff ff ff 0 be ef 01 72 3 61 63 6b 5f 74 00 00 00	ff ff 14 a7 2b 0e be 65 61 6c 74 65 63 74 5f 64 65 74 65 63 74 5f	, 60 bytes captured (48 (14:a7:2b:0e:be:c8), Ds c8 ff fa de ad 6c 6f 6f 70 62 70 61 63 6b 65 ack	00 bits) on t: Broadca: + ealt ek_loc dete ct_pac	interface \Device st (ff:ff:ff:ff: ppb :ke	> \NPF_{438B604[ :ff)

Wireshark will start capturing and packaging packets in.pcap format from your network interface. This is the standard packet capture file format (you'll find it's used in products like Snort, aircrack-ng and many more across our industry).

You will see three different windows for review in Wireshark. The top window in the following screenshot is known as the Packet List Pane, labeled # 1. Color coded packets should be seen moving through that window in real time.

The middle window is called the Packet Details Panel, labeled as # 2. This pane gives us header details from a selected packet in Window # 1.

Finally, Packet Bytes Pane, Window # 3 provides you with information about payload in both left hexadecimal format and right ASCII format.

## **Create Filter**

Overall, there will be much too much information to carry out a realistic study. Packs fly by hundreds or tens of thousands per minute. To make effective use of Wireshark, we need to filter the traffic to see only those packets we want. Wireshark has a simple filtering language to use effectively and effectively, which you should understand in a forensics investigation. There are many different protocols to the packets which fly through our interface. Perhaps the first filter we want to add is a protocol filter. Know, TCP / IP is a suite of protocols and we would like to concentrate on only a few of them in our study.

Type "tcp" in the filter window. Note that it turns green showing that your syntax is correct (if your syntax is wrong, it remains pink). Now, to add the filter, press the arrow button at the far right of the filter window.

																			X		1.
).	1	Time			S	ource	2				De	stinatio	n		Protocol	Length	Info				
18	884	157.29	9192	31	1	92.3	168.3	1.30	58		10	4.17.	207.1	.02	TCP	54	1876 ÷ 44	43 [F	IN, A	CK] S	ec
18	885	157.38	3412	0	1	04.1	17.20	07.1	102		19	2.168	3.1.30	;	TCP	60	443 → 187	76 [F	IN, A	K] S	ec
18	886	157.38	3420	3	1	92.3	168.3	1.30	5	_	10	4.17.	207.1	.02	TCP	54	1876 ÷ 44	43 [A	CK] S	eq=32	85
18	888	158.28	3810	6	1	92.3	168.	1.30	5		19	2.168	3.1.33	1	TCP	164	18778 → 8	8009	[PSH,	ACK]	-
18	889	158.29	9192	8	1	92.	168.	1.33	3		19	2.168	3.1.30	ī	TCP	164	8009 + 18	8778	[PSH,	ACK]	-
18	890	158.29	9199	9	1	92.1	168.3	1.30	5		19	2.168	3.1.33	1	TCP	54	18778 → 8	8009	[ACK]	Seg=	3
Fra Eth Int Tra	ime : ierni ierni insm:	3: 66 et II, et Pro	byt Sr toc	es ( c:   ol \ ntro	on v Kiyo Vers	wire on_9 sior Prot	e (52 96:9a 1 4, tocol	28 b a:ee Src 1, S	oits e (0 e: 1 Grc	), 6 0:17 92.1 Port	6 by :6b: 68.1 : 18	tes c 96:9a .36, 57, D	aptur :ee), Dst: St Pc	ed (528 Dst: cu 74.208.2 rt: 443,	oits) o rrento_ 36.69 Seq: 0	n interf Øe:be:c8 , Len: @	ace \Devi   (14:a7:2	lce\N 2b:0e	PF_{43 :be:c8	88604 )	> 4C
Fra Eth Int Tra	ame i terno terno	3: 66 et II, et Pro	byt Sr toc	es ( c:   ol \ ntro	on v Kiyo Vers	wire on_9 sior Prot	e (52 96:9a 1 4, tocol	28 b a:ee Src	oits 2 (0 2: 1 5rc	), 6 0:17 92.1 Port	6 by :6b: 68.1 : 18	tes c 96:9a .36, 57, D	aptur :ee), Dst: st Pc	ed (528 Dst: cu 74.208.2 rt: 443,	oits) o rrento_ 36.69 Seq: 0	n interf Øe:be:c8 , Len: 0	ace \Devi (14:a7:2	Lce\Ni 2b:0e	PF_{43 :be:c8	(88604 ()	>
Fra Eth Int Tra	ime : ierni insm	3: 66 et II, et Pro ission	byt Sr toc	es ( c:   ntro	on v Kiyo Ver: ol P	vire on_9 sior Prot	2 (52 96:9a 1 4, tocol	28 b src	oits e (0 e: 1 Grc	), 6 0:17 92.1 Port	6 by :6b: 68.1 : 18	tes c 96:9a .36, 57, D	aptur :ee), Dst: st Po	ed (528   Dst: cu 74.208.2 rt: 443,	oits) o rrento_ 36.69 Seq: 0	n interf Øe:be:c8 , Len: @	ace \Devi : (14:a7:2	lce\N 2b:0e	PF_{43	(88604 ()	>
Fra Eth Int Tra	ime i ierni insmi 14	3: 66 et II, et Pro Lission	byt Sr Co	es o c:   ntro	on v Vers ol F	wire on_9 sior Prot	2 (52 96:9a 1 4, cocol	28 b a:ee Src L, S	96	), 6 0:17 92.1 Port	6 by :6b: 68.1 : 18	tes c 96:9a .36, 57, D	aptur :ee), Dst: st Po	ed (528   Dst: cu 74.208.2 rt: 443,	pits) o rrento_ 36.69 Seq: 0 Seq: 0	n interf Øe:be:c8 , Len: @	ace \Devi	Lce\N	PF_{43	(88604 ()	>
Fra Eth Int Tra 00	ime ierni insm 14 00	3: 66 et II, et Pro Lssion a7 2b 34 8c	byt Sr toc Co Øe 3b	es o c:   ol v ntro be 40	on v Kiyo Vers ol F c8 00	wire on_9 sior Prot 00 40	2 (52 96:9a 1 4, cocol 17 06	28 b src 1, 5	96 9	), 6 0:17 92.1 Port 9a e c0 a	6 by :6b: 68.1 : 18 e 08 8 01	tes c 96:9a .36, 57, D 00 4! 24 4;	aptur :ee), Dst: st Po 5 00 a d0	ed (528   Dst: cu 74.208.2 rt: 443, 	bits) o crento_ 36.69 Seq: 0 Seq: 0	n interf Øe:be:c8 , Len: @	ace \Devi	Lce\N	PF_{43	(88604 ))	> 4[
Fra Eth Int Tra 00 10 20	ime : erno insm: 14 00 ec	3: 66 et II, et Pro ission a7 2b 34 8c 45 07	byt Sr toc Co 0e 3b 41	es 0 c:   ol ' ntro be 40 01	on v Kiyo Vers ol F c8 00 bb	vire on_9 sior Prot 00 40 54	2 (52 06:9a 1 4, cocol 17 06 cb	28 b s:ee Src 1, S 6b 00 d6	96 9 2f (	), 6 0:17 92.1 Port 9a e 00 a	6 by :6b: 68.1 : 18 e 08 8 01 0 00	tes c 96:9a .36, 57, D 00 4 24 4 00 8	aptur :ee), Dst: st Po 5 00 a d0 0 02	ed (528 Dst: cu 74.208.2 rt: 443, 	bits) o crento_ 36.69 Seq: 0 	n interf Øe:be:c8 , Len: @ *E* \$J	ace \Devi (14:a7:2	lce\Ni b:0e	PF_{43	(88604 ()	>
Fra Eth Int Tra 00 10 20 30	ame : cerno nnsm 14 00 ec fa	3: 66 et II, et Pro ission a7 2b 34 8c 45 07 f0 f9	byt Sr toc Co 0e 3b 41 08	es ( c:   ntro be 40 01 00	on v Kiyo ol F ol F 00 bb 00	vire on_9 sior Prot 00 40 54 02	2 (52 06:9a 1 4, cocol 17 06 cb 04	28 b 3:ee Src 1, 5 6b 00 d6 05	96 9 96 9 96 9 96 9 96 9 96 9	), 6 0:17 92.1 Port 9a e c0 a 00 0 01 0	6 by :6b: 68.1 : 18 : 18 e 08 8 01 0 00 3 03	tes c 96:9a .36, 57, D 00 4 24 4 00 8 08 0	aptur :ee), Dst: st Pc 5 00 a d0 0 02 1 01	ed (528 Dst: cu 74.208.2 rt: 443, 	bits) o rrento_ 36.69 Seq: 0	n interf Øe:be:c8 , Len: @ 	ace \Devi	Lce\N	PF_{43	88604	>

When you do that, Wireshark will filter out all traffic but the tcp traffic will. You can do just about the same for any protocol like "http," "smtp," "udp," "dns," etc. Try some and see what kind of traffic is going through your interface.

If we only want to see traffic from a particular IP address, we can create a filter that only displays traffic from or from that address. We can do this by logging into the filter window.

#### ip.addr==<IP address>

Notice double equal sign (==) in Wireshark filter syntax. A single = will not function in that syntax.

Want to see traffic coming in or going to the IP address 192.168.1.36, make a filter like this.

ip.addr == 192.168.1.36

ip.addr == 192.168	.1.36						$\times$
. Time	Source	Destination	Pr	otocol Lend	ith Info		
3 2.422990	192.168.1.3	36 74.208.23	36.69 TI	CP	66 1857 →	443 [SYN	Seq=0
5 2.684063	192.168.1.3	36 74.208.2	36.69 T	CP	54 1857 →	443 [ACK	<] Seq=1
6 2.684826	i92.168.1.3	36 74.208.2	36.69 TI	LSv1.2 5	06 Client	Hello	
9 2,956473	192.168.1.3	36 74.208.2	36.69 T	CP	54 1857 →	443 [ACH	(] Seq=4
12 2.95658	192.168.1.3	36 74.208.23	36.69 TI	CP	54 1857 →	443 [ACK	(] Seq=4
13 2.958018	192.168.1.3	36 74.208.2	36.69 TI	LSv1.2 1	29 Client	Key Exch	nange
1							
14 a7 2b 0 00 14 a7 2b 0 010 00 34 8c 3 020 ec 45 07 4 036 fa f0 f9 0	e be c8 00 17 6b b 40 00 40 06 00 1 01 bb 54 cb d6 8 00 00 02 04 05	96 9a ee 08 00 45 00 c0 a8 01 24 4a 2f 00 00 00 08 01 4 01 03 03 08 01	00 ++ d0 ++;@.@ 02 -E-A - T 01	kE. \$3. ./			*****
040 04 02	thernet_2020061210172	15_a91916.pcapng	Packet	s: 2289 · Displ	ayed: 2139 (9	3.4%)    P	rofile: Defi
<ul> <li>Wireshark_E</li> <li>Wireshark_E</li> <li>Ethernet</li> <li>Edit View Go</li> <li>Mitted 00</li> </ul>	thernet_2020061210172 Gapture Analyze Stati 전 이 약 송 송 영	15_a91916.pcapng istics Telephony Wireless *	Iools Help	s: 2289 · Displ	ayed: 2139 (9	3.4%)    P _	rofile: Def
<ul> <li>Wireshark_E</li> <li>Wireshark_E</li> <li>Ethernet</li> <li>Edit Yiew Go</li> <li>Edit Yiew Go</li> <li>Ep.dstport==80</li> <li>Time</li> </ul>	thernet_2020061210172 Capture Analyze Stati R G Q = = S	15_a91916.pcapng istics Telephony Wireless	Iools ∐elp Q II Protool Length	s: 2289 · Displ	ayed: 2139 (9	3.4%)    P 	rofile: Defi
	thernet_2020061210172 Capture Analyze Stati	15_a91916.pcapng istics Telephony Wireless Telephony @ Q Destination 203.205.219.54	Iools ∐elp Q Ⅲ Protocol Length HTTP 277	s: 2289 · Displ	ayed: 2139 (9	3.4%)    P 	rofile: Defi
Kernet     Kerne	thermet_2020061210172 Capture Analyze Stati	15_a91916.pcapng istics Telephony Wireless	Iools Help Protocol Length HTTP 265 HTTP 265	s: 2289 · Displ	ayed: 2139 (9 /1.1 (appli 2.crl HTTP/1	3.4%)    P 	rofile: Defa
840         64         62           Wireshark_E         *Ethernet           *Ethernet         £dit         View         Go           Image:	thernet_2020061210172 Capture Analyze Stati	15_a91916.pcapng istics Telephony Wireless	Iools         Help           @         Ⅲ           Protocol         Length           HTTP         277           HTTP         265           HTTP         241           TCP         341           TCP         341	s: 2289 · Displ Info POST / HTTP, GET /root-r/ GET /root-r/ GET /root-r/	ayed: 2139 (9 /1.1 (appli 2.crl HTTP/1 load/update/ inscen_scenus	3.4%)    P 	rofile: Defa
840         84         82           Wireshark_E         "Ethernet           *Ethernet         Edit View Go           Ime         Ime           455         40.349501           1668         113.556449           2432         271.289543           403.559224         447           447         40.249130	thernet_2020061210172 Capture Analyze Stati Capture Analyze Stati Source 192.168.1.36 192.168.1.36 192.168.1.36	15_a91916.pcapng istics Telephony Wireless	Iools Help Protocol Length HTTP 265 HTTP 241 TCP 54 TCP 54	Info POST / HTTP, GET /root-r- GET /root-r-	/1.1 (appli 2.crl HTTP/1 Load/update/ indcame.cguc	3.4%)    P 	rofile: Def
e40 04 02     wireshark_E     Edit View Go     Edit View Go     @ @ @ @     @     @ @ @ @     @     @ @ @ @     @     @     @ @ @ @     @     @     @ @ @ @     @     @     @     @ @ @ @     @	Capture Analyze Stati Capture Analyze Stati Capture Analyze Stati Capture Analyze Stati Capture 192.168.1.36	15_a91916.pcapng istics Telephony Wireless	Раскет Icols <u>H</u> elp Ротосо Length НТТР 265 НТТР 246 ТСР 54 ТСР 54 ТСР 66 ТСР 66	Info POST / HTTP, GET /root-r) GET /root-r) GET /root-r) IEGT /restore IEGT /restore I	41.1 (appli c.crl HTTP/1 c.crl HTTP/1 inscen_segme VII Seq=0 W VII Seq=0 W	cation/x1 v3/static n1_12626 in=64240	vww-form vww-form /trusted = 80 (AL Len=0 MSS Len=0 MSS

We can filter traffic also through port. I can create the filter below if I only want to see TCP traffic destined for port 80;

tcp.dstport==80

When creating filters, we will most often use = = as the operator in our filter (see others below). This works fine if we are looking for one of the many fields of protocol. If we are looking for payload strings, we must use the "contains" operator. So, if I were looking for packets with the Facebook word in them, I could create filters like this below.

#### tcp contains youtube

	Fair	Viev	v <u>G</u>	<u>ه</u>	aptur	e <u>A</u> r	alyze	Stat	stics	Tele	phony	Wir	eless <u>I</u>	ools <u>H</u>	elp							
di, 📕	2	۲			0	٩	۰ چې	⇒ 🕾	Ŷ	₽		Đ,	ର୍ଷ୍	11								
tcp	conta	ins you	utube																		X	
io.		Time			Sour	ce			0	Destin	ation			Protocol	Length	Info						
4	1795	345.8	32554	2	192	.168.	1.36		1	72.1	217.16	6.110	i i	TLSv1.3	752	Client	Hello					
	5068	348.1	15794	13	192	.168.	1.36		1	72.2	217.16	6.110	е в	TLSv1.3	752	Client	Hello					
3	5141	356.1	26767	0	192	.168.	1.36		3	72.2	217.16	6.110	6 B	TLSv1.3	752	Client	Hello					
	5145	357.0	8293	16	192	.168.	1.36	ł	į,	172.3	217.16	6.110	p	тср	752	[TCP R	etrans	mission	] 2017 -	+ 443	PSH, A	ICK] S
-	5479	386.3	28371	9	192	.168.	1.36		1	72.1	217.16	6.110	l, i	TLSv1.3	752	Client	Hello					
1	5522	388.3	21156	0	192	.168.	1.36		1	72.3	217.16	56.110	i, ii	TLSv1.3	752	Client	Hello					
-																			_			
		✓ Ex	tens: Type Leng Cert	Lon: 2: s 3th: 2:ifi	stat atus 5 ate	us_re _requ Statu	eques lest ls Ty	t (le (5) pe: 0	n=5) CSP	(1)												
		✓ Ex	tens: Type Leng Cert Resp Requ	ion: sth: ifi ond uest ion:	stat status 5 ate r ID Exte supp	us_requ _requ Statu list nsior	eques lest is Ty : Len is Le	t (le (5) pe: O gth: ngth: ups (	n=5) CSP 0 0 len=	(1)												
		✓ Ex	tens: Type Leng Cert Resp Requ tens:	ion: sth: ifi oond lest ion:	stat status 5 ate r ID Exte supp	us_requ _requ Statu list nsior orteo	iest is Ty Len s Le	t (le (5) pe: O gth: ngth: ups (	n=5) CSP 0 len=:	(1) 22)												>
0000	с0 С	<ul> <li>Ex</li> <li>Ex</li> <li>05 c</li> </ul>	tens: Type Leng Cert Resp Requ tens:	ion: sth: sth: ifi oond uest ion: c0	stat status 5 cate er ID Exte subb	us_re _requ Statu list nsior ortec	eques lest s Ty Len s Le l gro	t (le (5) pe: O gth: ngth: ups ( d 00	n=5) CSP 0 len=: 9c 0	(1) 22) 0 3d	00 3	c ••			=-<							>
10d0 10e0	c0 00	<ul> <li>Ex</li> <li>Ex</li> <li>05 c</li> <li>35 0</li> </ul>	tens: Type Leng Cert Resp Requ tens: 0 0f 0 2f	ion: sth: ifi ond uest ion: c0 c0	stat status 5 sate Exte supp 04 c0 08 c0	us_requ Statu list nsior ortec 0 0e 0 12	equest is Ty Len is Len l gro 00 1	t (le (5) pe: 0 gth: ngth: ups ( d 00 6 00	n=5) CSP ( 0 len=: 9c 0 13 c	(1) 22) 0 3d 0 03	00 3 c0 0	c ··	5./		=-<							>
0d0 0e0 0f0	c0 00 00	<ul> <li>Ex</li> <li>Ex</li> <li>05 c</li> <li>35 0</li> <li>0a 0</li> </ul>	tens: Type Leng Cert Resp Requ tens: 0 0f 0 2f 0 ff	ion: sth: ifi oond uest ion: c0 c0 01	stat status sate r ID Exte subb 04 c0 08 c0	us_re _requ Statu list nsior orteo 0 0e 0 12 ed	eques lest : Len s Le l erc 00 9 00 1 00 0	t (le (5) pe: O gth: ngth: ups ( 0 00 6 00	n=5) CSP 0 len=: 9c 0 13 c 14 0	(1) 22) 0 3d 0 03 0 12	00 3 c0 0	c ·· d ··	5./		= • <							>
0000 0000 00100 0100	c0 00 00 0f	<ul> <li>Ex</li> <li>Ex</li> <li>05 c</li> <li>35 0</li> <li>0a 0</li> <li>77 7</li> <li>95 0</li> </ul>	tens: Type Leng Cert Resp Requ tens: 0 0f 0 2f 0 ff 7 77 0 05	ion: sth: ifi oond uest ion: c0 c0 01 2e 01	stat status sate er ID Exte supp 04 c0 08 c0 00 00 79 6f	us_re _requ Statu list nsior orted 0 0e 0 12 0 ed 75	eques lest : Len is Le l gro 00 9 00 1 00 0 74 7	t (le (5) pe: 0 gth: ngth: ups ( d 00 6 00 5 62 8 03	n=5) CSP 0 len=: 9c 0 13 c 14 0 65 2 00 1	(1) 22) 0 3d 0 03 0 12 0 12	00 3 c0 0 00 0 6f 6	c • •	5•/•••	·····	=•<  con					*********		>
0000 0000 0000 0000 0100 01100 01100	c0 00 00 0f 00 1d	<ul> <li>Ex</li> <li>Ex</li> <li>05 c</li> <li>35 0</li> <li>0a 0</li> <li>77 7</li> <li>05 0</li> <li>00 1</li> </ul>	tens: Type Leng Cert Resp Requ tens: 0 0f 0 2f 0 0f 7 77 0 05 7 00	ion: :: s ::fi ::fi ::ond ::est ::on: :c0 :c0 :c0 :c0 :c0 :01 :2e :01 :18	stat status 5 sate r ID Exte subb 04 c0 08 c0 00 00 79 6f 00 00	us_requ Statu list nsior orted 0 0e 12 ed 75 0 00	eques lest is Ty : Len is Le l gro 00 9 00 1 00 0 1 00 0 1 00 0 1 00 0	t (1e (5) pe: 0 gth: ngth: ups ( 0 6 00 5 62 0 0a 1 00	n=5) CSP 0 0 len= 13 c 14 0 65 2 00 1 01 0	(1) 22) 0 3d 0 03 0 12 0 63 6 00 1 01	00 3 c0 0 00 0 6f 5 14 0 02 0	c •	5-/	tube.	= - < 							>
00d0 00e0 00f8 0100 0110 0120	C0 00 0f 00 1d 03	Ex Ex 05 c 35 0 0a 0 77 7 05 0 00 1 01 0	tens: Type Leng Cert Resp Requ tens: 0 0f 0 2f 7 77 0 05 7 00 4 00	ion: :: s' :: fi :: ifi :: ifi :: ifi :: oond uest :: oo : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0	stat status 5 cate er ID Exte subb 04 c0 08 c0 00 00 79 6f 00 00 19 00 02	US_requ Statu list nsior orteo 0 0e 0 12 0 ed 75 0 00 0 00 0 01	eques lest is Ty is Len of ero 00 1 00 0 00 1 00 0 1e 0 00 0	t (1e (5) pe: 0 gth: ngth: ups ( 0 0 00 5 62 0 0a 1 00 0 0d	n=5) CSP 0 len=: 9c 0 13 c 14 0 65 2 00 1 01 0 00 2	(1) 22) 0 3d 0 03 0 12 6 00 1 01 a 00	00 3 c0 0 00 00 6f 6 14 0 02 0 28 0	c •• 0 •• 0 •• 1 •• 4 ••	5-/	tube.	= - < 							>
0000 0000 0000 0000 0000 0000 0000 0000 0000	c0 00 0f 00 1d 03 03	Ex Ex 05 c 35 0 08 0 07 7 05 0 00 1 01 0 05 0	tens: Type Leng Cert Resp Requ tens: 0 0f 0 2f 0 0f 7 77 0 05 7 00 4 00 3 06	ion: strifi conducest ion: c0 c0 01 2e 01 18 0b 03	stat status 5 sate subp 84 c0 88 c0 80 00 79 61 80 00 90 02 80 04 80 000 80 000 80 000 80 000 80 00000000	us_requ Statu list nsior orted 0 0e 0 12 0 ed 0 20 0 00 0 01 0 08	eques est s Ty s Len s Le d gro 00 1 00 0 74 7 00 0 1e 0 00 0 00 0	t (1e (5) pe: 0 gth: ngth: ups ( 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n=5) 0 0 len=: 14 0 65 2 00 1 01 0 00 2 08 0	(1) 22) 0 3d 0 03 0 12 6 00 1 01 a 00 9 08	00 3 c0 0 6f 6 14 0 28 0 0a 0	c ··· d ·· d ·· d ·· 1 ··· 4 ··· 8 ··	5-/	tube.	< 							>

As you can see above, with the word Facebook it has found just two packets in the payload and we can see the word Facebook in the # 3 pane of the ASCII window.

Finally, we can find filter expressions on

#### $View \rightarrow Internals \rightarrow Supported \ Protocols$

it will open the window for Wireshark Filter Expressions as below.

This window lists all filters. These are hundreds of protocols, and they include fields. You can extend a protocol and select all its fields of interest.

# **Operator Description**

Na	ime	Filter	Туре	Description
	ADDGRPC	dsrc.addgrpc		DSRC Addition Gro C (EU)
v	ADP	adp		Aruba Discovery Protocol
	MAC address	adp.mac	Ethernet or other MAC ad	•
	Switch IP	adp.switch	IPv4 address	Switch IP address
	Transaction ID	adp.id	Unsigned integer, 2 bytes	ADP transaction ID
	Type	adp.type	Unsigned integer, 2 bytes	ADP type
	Version	adp.version	Unsigned integer, 2 bytes	ADP version
~	ADwin	adwin		ADwin communication protocol
	3+1 Instruction	adwin.i3plus1	Unsigned integer, 4 bytes	
	Blocksize	adwin.blocksize	Unsigned integer, 4 bytes	Maximum number of unacknowledged packet
	Complete packets	adwin.complete_pac	Unsigned integer, 4 bytes	Highest sequential package number
	Count	adwin.count	Unsigned integer, 4 bytes	Number of longs
	DLL Version	adwin.dll_version	Character string	
	Data	adwin.data	Label	
	Data No. (16bit)	adwin.data_no16	Unsigned integer, 2 bytes	
	Data No. (32bit)	adwin.data_no32	Unsigned integer, 4 bytes	
	Data element float	adwin.data_float	Floating point (single-prec	
	Data element hex	adwin.data_hex	Unsigned integer, 4 bytes	
	Data element int	adwin.data_int	Signed integer, 4 bytes	
	Data packet index	adwin.data_packet_in	Unsigned integer, 4 bytes	
	Data type	adwin.data_type	Unsigned integer, 4 bytes	
	End packet	adwin.packet_end	Unsigned integer, 4 bytes	GDSH: End Packet
	FiFo No. (16bit)	adwin.fifo_no	Unsigned integer, 4 bytes	
	File size	adwin.binfilesize	Unsigned integer, 4 bytes	Size of binary file
	GDSH status	adwin.gdsh_status	Unsigned integer, 4 bytes	
_	Cash ADA4 Vansian	a divis a seatle si a	I loainmad inkense. A hoken	

== Equal to	2,570 protocols, 187,320 fields.
!= Not equal	to
> Greater th	an
< Less than	
>= Greater th	an or equal to
<= Less than d	or Equal to
contains Protocol or	r Field contains a value
matches Protocol or	r text field matches a regular expression

Try building filters using some of these other operators and fields to get a feel for what Wireshark can do for you.

### Following a Stream

You will want to follow a communication stream instead of examining all the packets of a particular protocol, or in some cases traveling to a particular port or IP. Wireshark lets you do that just with little effort. This can be helpful if you try to follow a conversation between, for example, a rogue, disgruntled employee who is trying to damage your network

Simply select a packet by clicking on it and right-clicking to follow a stream.

File Edit	View Go	Capture Analyze Stati	stics Telephony Wireless	Tools Help					10000		~
1 .	OND	X 🖸 9 👄 🕾 🕾	T 1 3 3 0 0 0	Q. 11							
Apply a d	lisplay filter <c< th=""><th>br(-/&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>-</th><th>- +</th></c<>	br(-/>								-	- +
lo.	Time	Source	Destination	Protocol Length Info	<b>2</b>						
8067 8077	-19.820185 -19.767250	192.168.1.36 74.125.130.188	74.125.130.188 192.168.1.36	TCP 66 172 TCP 66 522	210 → 5228 [SYN] 9 28 → 17210 [SYN, 4	Seq=0 Win=64240 Len ACK] Seq=0 Ack=1 Wi	=0 MSS=1460 WS=2 n=62920 Len=0 MS	56 SACK_PERM=1 S=1430 SACK_PERM=	=1 WS=256		
8078	-19.767145	192.168.1.36	74.125.130.188	TCP 54 172	210 → 5228 [ACK] S	Seq=1 Ack=1 Win=131	328 Len=0				
8082 -19.716087 74.125.136 8083 -19.716062 192.168.1. 8085 -19.716030 192.168.1. 8085 -19.716030 192.168.1.		74.125.130.188 192.168.1.36 192.168.1.36 74.135.130.188	5.130.188 192.168.1.36 .68.1.36 74.125.130.188 168.1.36 74.125.130.188 168.1.36 74.125.130.188	Mark/Unmark Packet Ctrl+M Ignore/Unignore Packet Ctrl+D Set/Unset Time Reference Ctrl+T		-1431 Ack=518 Win=65792 Len=1430 [TCP segment of a reassembled PDU] -518 Ack=2861 Win=131328 Len=0 -518 Ack=3784 Win=130556 Len=0 -1 Ack=3784 Win=702 Len=0					
> Frame 8081: 54 bytes on wire (432 bits), 54 bytes captured > Ethernet II, Src: Kiyon_96:9a:ee (00:17:6b:96:9a:ee), Dst: > Internet Protocol Version 4, Src: 192.168.1.36, Dst: 74.12 > Transmission Control Protocol, Src Port: 17210, Dst Port: 1			Time Shift     Ctrl+Shift+T       Packet Comment     Ctrl+Alt+C       Edit Resolved Name     Apply as Filter       Prepare as Filter     Image: Comment of the second secon		38604D-08D8-4283-970D-CAFA21A6FBC8}, id 0						
		•									
0000 14 a7 2b 0e be c8 00 17 6b 96 9a ee 08 00 45 00 ···+			Conversation Filter Colorize Conversatio SCTP	in I	* *						
0020 82 bc 43 3a 14 6c ca 37 19 4c cc 9d 61 f6 50 10 ···C:		Follow	(	TCP Stream	Ctrl+Alt+Shift+T	1					
0030 02	01 8f 20 00 00			Сору		UDP Stream	Ctrl+Alt+Shift+U Ctrl+Alt+Shift+S				
		Protocol Preferences Decode As		HTTP Stream	Ctrl+Alt+Shift+H						
wireshark Ethernet 20200612135439 a00104.ocaono			Show Packet in New <u>W</u> indow		QUIC Stream		24 (0, 2%)	III	Profile: De	fault	

This will open a window as above pull down. Click "Follow" then click "TCP Stream."

	istream eq (2) · ethen	net	_		^
K∼G;.407V +./.,0	/OYP#N.X /.5JJ	n.J@E}.M.'Q mtalk.google.com.	зн		1
·····#·····					
	+.)	.m;b.ĸ!b			
.4					
·····ZI·····			•••••		•
	••••••		•••••	• • • • • • • •	•
.vT.O.WJ\$/.*4.?hK					•
.~.Wb n.J@E}.M.'Q	H	3.\$ I~7.	.Te	.Bw.	
/.k.+PT8 <h< td=""><td>łIA3\$h</td><td>.py.\1nq.}.</td><td></td><td></td><td></td></h<>	łIA3\$h	.py.\1nq.}.			
+hDhD%	BC^.@L.	}Td^JLT	>	35.W.,.	
3i.G3bm/el.:]	.~rTAusM.T	?r}C	:nV5	۷	
V4.Pm.&.HWy5n.	.G:.4.~y	(i.fBU,bL];.	QtBW	• • • • • • •	
5A*P+* 'C`ww.	u(4	td\.Q.5. v	v(3*.,P	.6XP	
u = 8ta oD	V IVIII	Ta			
	- D D D				
9.8TXTLK.:		.n.\$>bJ.HN	1. v		
9.8IXT K.;	>.;.TI	.n.\$>bJ.HM d 7\$ a.(	1.v ∖ f		
(cDK+N.		.n.\$>bJ.HM dZ\$a.(.	1.v \f.		
			1.v .\f.		
		.n.\$>.bJ.H№ dZ\$a.(. .n~w 0}Pr^y.~9	1.v \\f. 9[2	l	
2	Vp)*0	,	l.v ∖f. 9[2		
	Vp)*.0 Vp)*.0 Vv.I Lwo)H G%!I.T[*	, \$, bJ.HN d	1.v ∖f. 9[2]		
J.B.       I.I.XT K.,		,,,,,,,	1.v \\f. 9[2] .p" .j.zt	fт.	
		, \$	1.v ∖f. ∂[2  p" ;.zi	Fт.	
	Vp)*.0	,\$	1.v .\f. 9[2] .p	FT.	
			N.v Af. 9[2] 9 9	Fт.	
			1.v .∖f. 9[2  .p	Fт.	
			1.v \f. 9[2] p	fт.	
			A.v \f. 0[2] 	fT.	12
			A.v \f. 9[2] 	fT. Stream [ Find N	12 (
<pre></pre>			I.v .∖f. D[2] pj.z1 tP @ ASCII ↓	FT. Stream [ Find <u>N</u>	12 diext

This opens a window that includes all the packets and their contents in this stream. Note the statistics at the bottom of the window to the far left (5221 bytes) and the method for displaying content (ASCII).

## Statistics

Finally, we would want to gather statistics about our packet capture. This may be particularly useful when creating a standard baseline for traffic. Just click the Statistics tab at the top of Wireshark and a pulldown menu will appear. In our case, let's browse down to IPv4 Statistics, and then to all addresses.

As we click, there is a window that displays statistics for every and every IP address in our packet capture

<b>∡ ■ </b>	Capture File Properties Ctrl+Alt+Shift+C Resolved Addresses	
Time         Source           11544         389.704770         35.170.0.145           11544         389.704770         35.170.0.145           11544         389.704770         35.170.0.145           11601         406.572547         192.168.1.36           11605         407.573319         104.17.188.10           11605         407.574320         192.168.1.36           8080         77.869124         74.125.130.18           9880         77.869124         74.125.130.18           9880         77.869124         74.125.130.18           9880         77.869124         74.125.130.18           9880         77.869124         74.125.130.18           9880         77.869124         74.125.130.18           9165         115         115           917         7.869124         74.125.130.18           92.681.136         0869.77.869124         74.125.130.19           918         74.125.130.18         115           919         Frame 80801: 1484 bytes on wire (11         115           911         149.75         150.75           912         168.13         150.75           913         173.75         174.55           914	Protocol Hierarchy Conversations Endpoints Packet Lengths J/O Graph Service <u>Response Time</u> DHCP (BOOTP) Statistics ONC-RPC Programs 29West ANCP BACnet Collectd DNS	<pre>info 9 Application Data 2 [[[CP_SpuiPous Keranscission] , 2 Client Hello 9 Server Hello, Change Cipher Spee, 2 Change Cipher Spee, Encrypted Hi 1 Client Hello 1 Server Hello, Change Cipher Spee, 5) on interface \Device\NPF_[4386 e (00:17:6b:96:9a:ee) :: 518, Len: 1430</pre>
0006         000         17         6b         96         9a         ee         14         a7         2b         6e           0015         05         be         35         66         000         00         75         06         7b         d           0012         01         24         14         6c         43         3a         cc         66         000         00         15         03         06         000         03         06	Flow Graph HART-IP HPFEEDS HTTP + HTTP2 Sametime TCP Stream Graphs + UDP Multicart Streams	
Transmission Control Protocol: Protocol	F5 •	
	IPv4 Statistics	All Addresses
cle VM Cisco Packet HTTrack Pl JalBox Tracer Websi	IPv6 Statistics	Destinations and Ports

<ul> <li>All Addresses</li> </ul>		ivini vui	Iviax vai	Rate (ms)	Percent	Burst rate	Burst start		^
	43397			51.2347	100%	0.1000	1645.064		
95.218.79.44	2			0.0024	0.00%	0.0100	44.691		
94.202.245.130	3			0.0035	0.01%	0.0100	6.813		
92.99.231.8	2			0.0024	0.00%	0.0100	76.080		
92.98.60.232	1			0.0012	0.00%	0.0100	1536.588		
92.97.46.158	1			0.0012	0.00%	0.0100	1391.117		
86.99.200.216	1			0.0012	0.00%	0.0100	934.286		
85.154.183.146	4			0.0047	0.01%	0.0100	29.462		
84.255.165.65	4			0.0047	0.01%	0.0100	388.696		
82.1,242.128	2			0.0024	0.00%	0.0100	1222.284		
8.8.8	8			0.0094	0.02%	0.0200	714.390		
74.208.40.131	1			0.0012	0.00%	0.0100	1433.071		
74.125.24.188	7			0.0083	0.02%	0.0200	30.314		
74.125.130.188	117			0.1381	0.27%	0.1700	77.869		
61.6.243.105	5			0.0059	0.01%	0.0100	25.277		
60.243.93.128	4			0.0047	0.01%	0.0100	212.143		
59.99.49.233	2			0.0024	0.00%	0.0100	783.595		
59.98.50.24	6			0.0071	0.01%	0.0100	1033.037		
59.96.192.58	6			0.0071	0.01%	0.0100	1161.976		
59.93.236.195	5			0.0059	0.01%	0.0200	1225.099		
59.92.189.28	3			0.0035	0.01%	0.0100	340.645		Y
splay filter:								Annia	

We 're going to try to advance your knowledge and understanding of Wireshark to the level where you can use many features in an actual forensic investigation network.
## Name Resolution

The data that you are analyzing on any network often have indecipherable names. IPv4 addresses are 4 bytes of decimal data such as 192.168.1.101 and 6 hexadecimal addresses such as "00.AA.CD.11.EF.23." Sometimes this data becomes easier to decode and interpret if it is translated to a human-readable name rather than a number, just as DNS does to us when we browse the Internet.

There are three types of naming resolution at Wireshark.

- MAC Addresses
- Network Name
- **Transport** Name •

Go to Capture  $\rightarrow$  Options to enable name resolution (the capture must stop first).

In the Capture Interfaces window, click on the 3rd tab, Options. It will show "Name Resolution" box, and the three options. **\***Ethernet

tcp

No.

Time

11601 406 572547

11603 407.573319

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Ctrl+F

Ctrl+E

Ctrl+R

F5

Ctrl+K | = 🕀 Q Q 👭

8.1.36

8.1.36

8.1.36

188, 107

Protocol Lengt

TLSv1.2 16

37

42

TLSv1.2 37

TLSv1.2

TI Sv1.2

🖌 🔳 🙍 💿 📙 🔚 💿 <u>O</u>ptions...

11544 389.704770 🙇 <u>R</u>estart

<u>Start</u>

11548 390.299603 Capture Eilters...

Stop

**Refresh Interfaces** 

Click all three boxes to see nomenclature resolution on all three levels. This definitely should make your analysis a bit easier.

		11002	407.373313		p.1.50	ILJVI.	E 11
		11605	407.574320	192.168.1.36	104.17.188.1	107 TLSv1.	2 4
		8079	77.818437	192.168.1.36	74.125.130.1	188 TLSv1.	3 5
Wireshark · Capture Interfaces			× .869124	74.125.130.188	192.168.1.36	5 TLSv1.	3 14
			960391	74 105 120 100	103 160 1 26	T1 51/1	2 N
Logical Copacity Solutions     Copacity Copacity     Copacity Copacity     Copacity Copacity     Copacity Social Curring live capture     Show capture information during live capture     Stop capture automatically after     T     T     Social Copacity	Name Resolution		80: 1484 b II, Src: Protocol ;ion Contr : Layer Se	ytes on wire (11872 currento_0e:be:c8 (: Version 4, Src: 74.; ol Protocol, Src Por curity	bits), 1484 byt 14:a7:2b:0e:be:c 125.130.188, Dst -t: 5228, Dst Po	es captured (118 8), Dst: Kiyon_9 192.168.1.36 ort: 17210, Seq:	372 bi 96:9a: 1, Ac
□         □         ○         fifes           □         □         ○         Holoytes         ∨           □         □         ○         seconds         ∨			6b 96 9a 35 60 00 14 6c 43 65 dc 00 d8 4f b8 17 4b ea 09 6e 88 fe e3 a3	ee         14         a7         2b         0e         be           00         75         06         7b         d4         4a           3a         cc         9d         5c         60         ca           00         16         03         03         00         7a           57         4a         b7         10         24         2f           dc         eb         82         0a         f9         7e           4a         40         45         13         e4         7d           dc         c5         33         fe         e5         a2	c8 08 00 45 00 7d 82 bc c0 a8 37 19 4c 50 10 02 00 00 76 03 d8 2a 34 02 3f 7f 57 ba 2d 8e a0 4d c9 27 51 9b c9 1c e3 48	· k · · + -5` · u { · J} -\$ · 1C · · \` 7 - e · Z - T · O · WJ · \$/ ·* h · K · · · · · h b · n J@E · } M	•E• •V• •4•? /• 1• 'Q

## Protocol Dissection

Analysis of network traffic will require a certain dissection of the protocol to illuminate what really happened on the network. We may want to see for example which IP packets are broken, or which TCP packets a has the RST flag collection. We can do this by creating the appropriate filter and dissecting those packets using the middle window in Wireshark.

For example, if we want to see which IP packets have been fragmented, we want to create a field filter in the IP header that is also called flags or more fragments (MF). When setting this flag, it means the packet has been broken and the target network needs to be reassembled (attackers also break packets in an effort to bypass firewalls and IDS's).

Name		Filter	Туре	Description	^
1	Fragment overlap	ip.fragment.overlap	Boolean	Fragment overlaps with other fragments	
	Fragment too long	ip.fragment.toolongf	Boolean	Fragment contained data past end of packet	
1	Function	ip.opt.qs_func	Unsigned integer, 1 byte		
	GENSER	ip.opt.sec_prot_auth	Boolean		
1	Handling Restrictions	ip.opt.sec_rfc791_hr	Character string		
1	Header Length	ip.hdr_len	Unsigned integer, 1 byte		
1	Header checksum	ip.checksum	Unsigned integer, 2 bytes		
1	Header checksum status	ip.checksum.status	Unsigned integer, 1 byte		
i	ID Number	ip.opt.id_number	Unsigned integer, 2 bytes		
	IP Address	ip.opt.addr	IPv4 address		
1	IPv4 Fragment	ip.fragment	Frame number		
1	IPv4 Fragments	ip.fragments	Sequence of bytes		
1	Identification	ip.id	Unsigned integer, 2 bytes		
1	Invalid length for option	ip.opt.len.invalid	Label		
1	Length	ip.opt.len	Unsigned integer, 1 byte		
1	MTU	ip.opt.mtu	Unsigned integer, 2 bytes		
1	Malformed CIPSO tag	ip.cipso.malformed	Label		
1	More fragments	ip.flags.mf	Boolean		
1	Multiple tail fragments fo	ip.fragment.multiplet	Boolean	Several tails were found when defragmenting the packet	
1	NSA	ip.opt.sec_prot_auth	Boolean		
1	Not Used	ip.opt.qs_unused	Unsigned integer, 1 byte		
1	Number	ip.opt.type.number	Unsigned integer, 1 byte		
1	Originator IP Address	ip.opt.originator	IPv4 address		
1	Outbound Hop Count	ip.opt.ohc	Unsigned integer, 2 bytes		
	Overflow	ip.opt.overflow	Unsigned integer, 1 byte		
	Dealist leas and interes	in a line and	امطما		•
earch:					
2.570 pro	tocols, 187,320 fields.				
0.0					
					Close

On the Filter Expression we can find fragmented packets as below.

## ip.flags.mf==1

Here the IP protocol can be selected and expanded until we find the ip.flags.mf, then select = = and set the value to 1. Now Wireshark can only show packets which have the IP flag set for MF or fragmented packets. The shown packets are broken packets. This may occur during the usual transmission process or could be an indicator that an attacker is attempting to bypass IDS or firewall detection.

Unlike IP flag TCP has its own flags. These flags signal the intent of the TCP packet sender, for example initiating a connection (SYN) or breakdown of a session (FIN). If we want to see all the packets starting a TCP session, we can set the Wireshark filter to;

## tcp.flags.syn == 1

This filters packets out except those initiating a TCP session. When we pick one of those packets, we can dissect it in the middle window and see it has the SYN flag set.

						1000 DOI 10
10.5	aga.ayri == 1					- C3
B.	Tine	Source	Destination	Protocol	Length Info	
00	67 27.765146	192.168.1.26	74.125.138.188	TCP	66 [17210 + 5228 [519] Seg-8 Min+64348 Len+8 755+1468 M5+256 SACK_PTRT+3	
88	77 77.018801	74,125,130,158	192.168.1.36	TCP	66 5228 + 17210 [SVN, ACK] Sequel Ackr1 Min=82928 Lenne MSI=1438 SACK_PERMA1 MS+256	
61	11 78.333794	192,168.1.26	192.368.1.53	TCP	06 17211 + 0000 [SYN] Seq+0 Win+64240 Len+0 MSS+1460 WS+256 SACK_PORM+1	-
BT:	32.78.338882	192.168.1.33	192.168.1.36	TCP	06 0000 + 17211 [SYN, ACX] Seq+0 Ack+1 Win+05535 Len+0 MS5+1460 SACK_FERM+1 W5+64	
1.5	64 89,278028	292.168.1.26	192.168.1.33	TCP	06.17212 - 0000 [511] Seq+0 101+64240 Len+0 755+1460 16+256 SACK_PERP+1	
13	55 89.279630	102.108.1.11	192,168.1.36	TCP	00 0000 + 17212 [SYN, ACK] Seq+0 Ack+1 W10+05535 Len+0 M55+1460 SACK_PERM+1 M5+64	
- 87	91.29,572966	192.168.1.36	74.125,139,188	TOP	68 17213 + 5228 [SYN] Seq+8 kEx+64248 Len+8 255+1468 k5+256 SACK_PERH+1	1.0
	0.	<pre> = Acknowledgeent:  = Push: Not set  = Reset: Not set</pre>	Not set			
	TCP Plags:	<pre> = Acknowledgeent:  = Push: Not set  = Reset: Not set I = Syni Set .0 = Fin: Not set </pre>	Not set	-		-
100	TCP Flags: Indow size val	= Acknowledgment; = Push: Not set = Reset: Not set I. = Syni Set 	Not set		E	
100	TCP Flags: Indow size val 14 a7 2b 0e be 80 34 22 a1 40 20 2b c 43 23 34	= Acknowledgement; = Push: Not set = Reset: Not set E. = Synl Set 	Not set	0.0 × 5	£ 3)	
100 158 128 130	TCP Plags: Indow size val 14 a7 2b 0e be 80 34 22 a1 46 82 bc 43 3a 14 fa f0 8f 2c 08	= Acknowledgement; = Push: Not set = Reset: Not set I. = 5ynl Set I. = 5ynl Set .0 = Fin: Not set 	Not set ee 00 00 45 00 + a0 01 24 4e 7d 4" 00 00 00 80 02 - C 05 00 00 10 1	€ € 5 : 1 7 . F	€ 5]	
100 58 50 100	[TCP Flags: [Infow size val 4 47 2b 0e be 80 34 22 al 40 82 bc 43 3a 14 fa f0 8f 2c 00 04 02	= Acknowledgewri = Push: Not set = Reset: Not set I = Syni Set 0 = Fin: Not set 	Not set	0 0 5 1 1 7 7	¥ 	

The same is true for either of the six TCP flags (SYN, ACK, FIN, PSH, URG, RST). TCP uses the RST flag to signal a "strong" link termination, or a packet has entered the wrong port or IP. The following filter can be used to find certain packets.

## tcp.flags.reset==1



# Statistics Window

Using each protocol such as TCP, UDP, DNS, ICMP etc., statistics are often useful when we analyze large amounts of data. This can be a useful technique for creating a reference snapshot of what your usual traffic looks like to promote the detection of anomalous traffic when a question occurs.

Click on the Statistics tab at the top menus to view the protocol statistics, and then select Protocol Hierarchy.

Capturing from Ethernet	Statistics Telephony Wireless Tools Help	– 🗆 x
	Capture File Properties Ctrl+Alt+Shift+C	
Apply a display filter <ctrl-></ctrl->	Resolved Addresses	
No. Time Source	Protocol Hierarchy	1 Info
51 22.372909 192.168.1.33 52 23.309636 192.168.1.33 53 24.491677 192.168.1.36 54 24.502486 192.168.1.36 55 24.502553 192.168.1.36 56 24.909332 currento 6:b	<u>Conversations</u> Endpoints Packet Lengths J/O Graph Service Researce Time	5 Standard query response boddeD PTR NITV-X5000_rrc_tcp.local SW, cache Fluid 0 0 6091 mill. DeMebership Report / Join group 201355.352 for any sources / Join group 201355.352 for 1 5867 - 8089 [PSH, ACK] Seq.441 Ack-441 kin-586 Len-110 [TCP segment of a reassembled PDU] 2 5009 - 15557 [PSH, ACK] Seq.441 Ack-551 kin-558 Len-10 [TCP segment of a reassembled PDU] 2 15677 - 8089 [ACK] Seq.551 Ack-551 kin-558 Len-0
57 25.602559 112.134.160.1	Service Response nine	5 37967 + 4444 Len=104
<pre>&gt; Frame 1: 60 bytes on wire (480 bi &gt; Ethernet II, Src: currento_0e:be: &gt; Data (46 bytes)</pre>	DHCP (BOOTP) Statistics ONC-RPC Programs 29West ANCP	face \Device\NFF_{43886440-8808-4283-9700-CAFA21A6FBC8}, id 0 :ff:ff:ff:ff:ff)
	BACnet  Collectd DNS Flow Graph	
0000         ff ff ff ff ff ff 14 a7         2b 0e           0010         be ef 01 72 65 61 6c 74 65 6b         0020         61 63 6b 5f 64 65 74 65 63 74           0020         61 63 6b 5f 64 65 74 65 03 74         0030         74 00 00 00 00 00 00 00 00 00         00 06	HART-IP HPFEEDS HTTP + HTTP2	
Theraet: vive rantine in progress .	Sametime TCP Stream Graphs UDP Multicast Streams	Borketer 52 - Deckarde 52 (100.055)    Decline Data (4
Counce one taplate in program	F5  IPv4 Statistics  IPv6 Statistics	Original and another another and another anoth

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
✓ Frame	100.0	331	100.0	97214	8500	0	0	0
✓ Ethernet	100.0	331	4.8	4634	405	0	0	0
<ul> <li>Internet Protocol Version 4</li> </ul>	93.1	308	6.4	6176	540	0	0	0
User Datagram Protocol	18.1	60	0.5	480	41	0	0	0
Simple Service Discovery Protocol	1.2	4	0.7	692	60	4	692	60
Multicast Domain Name System	2.4	8	1.5	1456	127	8	1456	127
Domain Name System	3.0	10	0.7	703	61	10	703	61
<ul> <li>Transmission Control Protocol</li> </ul>	73.7	244	75.6	73453	6422	194	37858	3310
Transport Layer Security	13.3	44	64.1	62316	5448	43	62093	5429
<ul> <li>Hypertext Transfer Protocol</li> </ul>	0.9	3	1.2	1165	101	1	211	18
HTML Form URL Encoded	0.3	1	0.4	382	33	1	382	33
Apache JServ Protocol v1.3	0.6	2	1.6	1544	135	2	1544	135
Internet Group Management Protocol	1.2	4	0.1	128	11	4	128	11
Data	18.1	60	9.6	9346	817	60	9346	817
Address Resolution Protocol	1.2	4	0.2	148	12	4	148	12
r distar film.								

Wireshark creates a display window with all the data concerning the various protocols. If you have this data from regular traffic before problems occur, you can take another snapshot when problems emerge and compare them to try and recognize changes and probably the cause of the problem or issue.

# Analyzing Endpoints Using Wireshark

Sometimes we want to see where the traffic ends when doing the traffic analysis. We would like to see the endpoints of communication, in other words. This could be an IP or MAC address.

We can select Statistics, and then Endpoints, to see the communication endpoints with their statistics.

Capturing from Ethernet			-		×
File         Edit         Yiew         So         Capture         Amalyce         So           Apply         abgets         a	tatistics Telephony Wireless Tools Help Capture File Properties Cott+Alt+Shift+C Resolved Addresss Protocol Hierarchy Conversations Endpoints Packet Lengths J/O Graph	1n6 443 - 20722 [ACK] Seq-3909 Ack-1760 Min-32768 Len-0 443 - 4.8332 [ACK] Seq-45265 Ack-32659 Min-33024 Len-0 4 papLiaction Data 4 18332 - 443 [ACK] Seq-3269 Ack-4536 Min-130944 Len-0 4 43 - 2073 [ACK] Seq-3269 Ack-4548 Min-130944 Len-0			• + ^
8296_18466.764569 172.217.163.7 8296_18466.764724 192.168.1.36 > Frame 1: 60 bytes on wire (480 bi > Ethernet II, Src: currento_0e:be:- > Data (46 bytes)	Service gesponse Time   DHCF0 (BOOTP) Statistics ONC-RPC Programs 29West ANCP BACnet Collectd DNS Enw Gronb	3 Application Data 40733 443 [ACK] Seq=1458 Ack=5379 Win=130816 Len=0 40733 443 [ACK] Seq=1458 Ack=5379 Win=130816 Len=0 4764 Charles (MPF (43886040-0808-4283-9700-CAFA21A6FBC8), id 0 :ff:ff:ff:ff:ff)			
0000 ff ff ff ff ff ff ff 14 s7 2b 8c 0010 be ef 01 72 65 63 6c 74 65 63 0020 bi 65 76 46 57 45 53 7 0030 74 60 06 99 60 60 60 60 60 60 60	HART-IP HPFEEDS HTTP • HTTP2 Sametime TCP Stream Graphs •				
Ethernet:	UDP Multicast Streams	Parkets: 829653 • Displayed: 829653 (100.0%)	p	rofile: Del	fault

Additionally, by clicking the Endpoint Types button in the bottom right corner and selecting the protocol we want to filter for, we can filter these data by protocol.

Apply a c	display filte	n	-/>															
	Time.		Cource		D	ortisation		Oro	tocal (	annth Info							_	0
Wires	hark · End	points · E	thernet													-	U	×
Etherne	et·14	IPv4 · 48	3 IPv6 ·	5 TCP	2052	UDP • 207	7											
Address	s F	ackets	Bytes Tx P	ckets To	Bytes	Rx Packets	Rx Byt	tes Coun	itry City	AS Numb	er AS Organization							^
1.1.1.1		19	1386	0	0	1	9 1	1386 -	-	-	-							100
1.38.196	0.85	10	140	1	140		5	245	-		-							_
3.1.111.2	250	35	9313	17	7026	1	8 2	2287 -	828	_	_							
3.6.178.	123	53	13 k	24	9042	2	9 4	4118 -										
3.114.12	9.228	71	21 k	35	14 k	3	6 7	7002 —	-	-	( <del></del> )							
3.126.19	2.219	1,486	477 k	569	386 k	91	7 9	91 k -	8 <del>1 -</del> 8	-	-							
3.218.21	.200	861	389	360	125 k	50	2	180	8 <del>4</del> 8									
3.230.23	15.18	27	7861	13	6449	1	4 1	1412 -		_	-							
8.8.8.8	019932	37	4114	18	2728	1	9 1	1386 —	<u></u> :	8 <b>—</b> 8	2 <b>—</b> 2							
8.43.72.9	98	114	30 k	53	22 k	6	1 7	/379 —	8 <u>—</u> 31									
13.33.14	14.30	51	17 k	23	13 k	2	8 3	3949 — 121	0.000		3 <del></del>							
13.33.14	14.33 14.35	161	209 K 19 k	76	9121	20	5 0	9944	1		-							
13.33.14			00.10		6600		Q (2											
	4.40	24	8048	11	0090		3 1	1358			-							
13.33.14	14.40 14.49 resolution	24 216	24 k	101 splay filter	10 k	11	s 1 5	1358 — <u>13 k —</u>	-				_	Сору	• Мар	7 Close	Endpoint	✓ Types ▼ Help
13.33.14	14.40 14.49 resolution	24 216	24 k	11 101 splay filter	10 k	11	3 1 5 CP	1358 — 13 k — 60		-		6267	1	<ul> <li>Copy</li> <li>443 → 62671</li> </ul>	<ul> <li>Map</li> <li>[ACK] Seq</li> </ul>	7 Close	Endpoint	v Types▼ Help Blueto
13.33.14 Name 06:47 1 06:47 1	14.40 14.49 resolution 1.04.20.4 1.92.168.	24 216 15.29 1.36	24 k	11 101 splay filter 72.168. 3.207.1	0090 10 k	11 11	CP CP CP	1358 — 13 k — 60 55	-	-		626 17 443	1	<ul> <li>☑ Copy</li> <li>443 + 62671</li> <li>62697 + 443</li> <li>444</li> </ul>	▼ Map [ACK] Seq [ACK] Seq	<ul> <li>Close</li> <li>65 Ack=2 Will</li> <li>1 Ack=1 Win</li> </ul>	Endpoint F	v Types▼ Help Blueto Ethern
06:47 1 06:47 1 06:47 2	104,20,4 104,20,4 192,168, 13,207,1	24 216 \$5.29 1.36 1.54.15	24 k	10 101 splay filter 92.168. 3.207.1 32.168.	0090 10k 1.36 54.15 1.36	1 11 1 1 1 1 1 1	CP CP CP	1358 — 13 k — 60 55 66				6263 97 443 6269	<sup>71</sup>	Copy 443 + 62671 62697 + 443 443 + 62691	<ul> <li>Map</li> <li>[ACK] Seq=</li> <li>[ACK] Seq=</li> <li>[ACK] Seq=</li> </ul>	<ul> <li>Close</li> <li>65 Ack=2 Wil</li> <li>1 Ack=1 Win</li> <li>1 Ack=2 Win</li> </ul>	Endpoint	Types Types Help Blueto Ethern FC
13.33.14 Name 06:47 1 06:47 1 06:47 2 hark · En	14.40 14.49 resolution 104.20.4 192.168. 23.207.1 dpoints -	24 216 15.29 1.36 154.15 Ethernet	24 k	11 101 splay filter 92.168. 3.207.1 92.168.	0090 10k 1.36 54.15 1.36	11 11 T T	CP CP CP	1358 — 13 k — 13 k — 60 55 66				626 97 443 6269	71	Copy 443 + 62671 62697 + 443 443 + 62697	Map     [ACK] Seq=     [ACK] Seq=     [ACK] Seq=	<ul> <li>Close</li> <li>65 Ack=2 Win</li> <li>1 Ack=1 Win</li> <li>1 Ack=2 Win</li> </ul>	Endpoint	Types Types Help Blueto Ethern FC FDDi
13.33.14 Name 06:47 1 06:47 1 06:47 2 hark - En	14.40 14.49 resolution 1.04, 20, 4 192, 168, 13, 207, 1 dpoints - 10, 4, 18	24 216 15.29 1.36 154.15 Ethernet	24 k Limit to d 1 2 1 1 1 2 1 1 1 2 1	11 101 isplay filter 92.168. 3.207.1 92.168.	0090 10k	T T T T	ср СР СР	1358 — 13 k — 13 k — 60 55 66				626 97 443 6269	71 17	Copy 443 + 62671 62697 + 443 443 + 62697	Map     [ACK] Seq     [ACK] Seq     [ACK] Seq	<ul> <li>Close</li> <li>165 Ack=2 Win</li> <li>11 Ack=1 Win</li> <li>11 Ack=2 Win</li> </ul>	Endpoint	Types  Types  Help Blueto Ethem FC FDDI IEEE 8(
13.33.14 Name 06:47 1 06:47 2 hark · En	14.40 14.49 resolution 104.20.4 192.168. 23.207.1 dpoints - 1Pv4 · 18 Packets	24 216 15.29 1.36 154.15 Ethernet	24 k Limit to d 1 2 1 t TCP • 2	11 101 splay filter 32.168. 3.207.1 92.168.	0090 10k 1.36 54.15 1.36 • 14	T T T T	CP CP CP CP	1358 — 13 k — 13 k — 60 55 66	City	AS Number		6263 97 443 6269	<sup>71</sup> 17	Copy 443 → 62671 62697 + 443 443 → 62697	Map     [ACK] Seq     [ACK] Seq     [ACK] Seq	Close 165 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint	Types  Types  Fielp Blueto Ethern FC FDDI IEEE 80 IEEE 80
13.33.14 Name 06:47 1 06:47 1 06:47 2 hark · En tt · 4	14.40 14.49 resolution 104.20.4 192.168. 23.207.1 dpoints - IPv4 · 18 Packets 2	24 216 15.29 1.36 154.15 Ethernet IPv6 Bytes 121	24 k Limit to d 1 2 1 t TCP • 2 Tx Packets	11 101 isplay filter 92.168. 3.207.1 92.168. D UDP Tx Bytes 6	0090 10 k 1.36 54.15 1.36 • 14 • 14 Rx Pa	T T T ckets Rx	CP CP CP CP Bytes	1358 — 13 k — 60 55 66 Country	City	AS Number	443 626 443 AS Organization	626 17 443 6269	11	Copy 443 + 62671 62697 + 442 443 + 62691	Map     [ACK] Seq*     [ACK] Seq*     [ACK] Seq*	<ul> <li>Close</li> <li>G5 Ack=2 Win</li> <li>Ack=1 Win</li> <li>Ack=2 Win</li> </ul>	Endpoint	Types V Help Blueto Ethern FC FDDI IEEE 80 IEEE 80 IPX
13.33.14 Name 06:47 1 06:47 1 06:47 2 hark · En et · 4 54.15 54.15	14.40 resolution 104.20.4 192.168. 3.207.1 dpoints - IPv4 · 18 Packets 2 2	24 216 15.29 1.36 154.15 Ethernet IPv6 Bytes 121 121	24 k Limit to d 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1	11 101 isplay filter 92.168. 3.207.1 92.168. 0 UDP Tx Bytes 6 6	0090 10 k 1.36 54.15 1.36 • 14 • 14 • Rx Pa 6	T T T T r ckets Rx 1	CP CP CP CP CP CP S55 55	1358 — 13 k — 13 k — 60 55 66 Country —	City	AS Number	A43 626 443 AS Organization	6265 17 443 6269	71	Copy 443 + 62671 62697 + 443 443 + 62697	▼ Map [ACK] Seq= [ACK] Seq= [ACK] Seq=	Close 65 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint	FC FDDI IEEE 80 IPX IPv4
13.33.14 Name 06:47 1 06:47 1 06:47 2 hark · En t: • 4 54.15 54.15 1.140 4.189	14.40 resolution 104.20.4 192.168. 13.207.1 dpoints - IPv4 - 18 Packets 2 2 2	24 216 15.29 1.36 154.15 Ethernet IPv6 Bytes 121 121 143	1 Limit to d TCP · 2 TCP · 2	11 101 splay filter 92.168. 3.207.1 92.168. 0 UDP Tx Bytes 6 6 6 6	0090 10 k 1.36 54.15 1.36 **14 Rx Pa 6 8	T T T T Ickets Rx 1 1	CP CP CP CP CP Bytes 55 55 75	60 55 66 Country -	City	AS Number		6265 17 443 6265	71	<ul> <li>Copy</li> <li>443 + 62677</li> <li>443 + 62697</li> <li>443 + 62697</li> </ul>	<ul> <li>Map</li> <li>[ACK] Seq=</li> <li>[ACK] Seq=</li> </ul>	Cose 65 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint	V Types V Help Ethem FC FDDI IEEE 80 IEEE 80 IEEE 80 IPX IPv4 IPv6
13.33.14 Name 06:47 1 06:47 2 hark · En t: · 4 54.15 1.140 4.189 00.189	14.49 resolution 104.20.4 192.168. 13.207.1 dpoints - 1Pv4 - 18 Packets 2 2 2 2 2	24 216 1.36 1.54.15 Ethernet IPv6 Bytes 121 121 121 121 121 123 143	1 24 k Dimit to d 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1	11 101 splay filter 92.168. 3.207.1 92.168. 0 UDP Tx Bytes 6 6 6 6 6	0090 10 k 1.36 54.15 1.36 ** 14 Rx Pa 6 8 8	T T T Ickets Rx 1 1 1	CP CP CP CP Bytes 55 55 75 75	60 55 66 Country –		AS Number		626: 17 443 626:	71	Copy 443 + 62671 62697 + 443 443 + 62692	<ul> <li>Map</li> <li>[ACK] Seq*</li> <li>[ACK] Seq*</li> </ul>	Close 65 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint	Types  Ty
13.33.14 Name 06:47 1 06:47 1 06:47 2 hark · En t · 4 54.15 140 4.189 00.189 5.29	14.49 resolution 104.20.4 192.168. 23.207.1 dpoints - 1Pv4 - 18 Packets 2 2 2 2 2 1	24 216 1.36 1.36 1.54.15 Ethernet 121 121 121 143 143 93	24 k Limit to d TCP • 2 TCP • 2 TX Packets 1 1 1 1 1 1 1 1 1 1 1 1 1	11 101 splay filter 92.168. 3.207.1 92.168. 0 UDP Tx Bytes 6 6 6 6 6 6 9 9 9 9 9 9 9 9 9 9 9 9 9	0090 10 k 1.36 54.15 1.36 14 Rx Pa 6 8 8 8 3	rckets Rx 1 1 1 1 1 1 1 1 1	CP CP CP CP Bytes 55 55 75 75 75 0	1358 — 13 k — 13 k — 60 55 66 Country — — — — —	City	AS Number — — —		626 17 443 6269	<sup>11</sup> 17	Copy 443 + 62677 62697 + 44 443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq+</li> <li>[ACK] Seq+</li> <li>[ACK] Seq+</li> </ul>	<ul> <li>Zose</li> <li>Ack=2 Win</li> <li>Ack=2 Win</li> </ul>	Endpoint	V Types V Help Blueto Ethern FC FDDI IEEE 80 IEEE 80 IEEE 80 IPX IPv4 IPv6 JXTA MPTCI
13.33.14 Name 06:47 1 06:47 1 06:47 2 hark · En t · 4 54.15 .140 00.189 5.29 17.194	14.49 14.49 resolution 104.20.4 192.168. 23.207.1 dpoints - 1Pv4 · 18 Packets 2 2 2 2 1 7 7	24 216 1.36 1.54.15 Ethernet 121 121 143 93 453	24 k 24 k Umit to d 1 2 1 1 2 1 TCP · 2 Tx Packets 1 1 1 2 1 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1	11 101 splay filter 32.168. 3.207.1 32.168. D UDP Tx Bytes 6 6 6 6 6 6 6 6 6 6 6 6 6	0090 10 k 1.36 54.15 1.36 14 Rx Pa 	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CP CP CP CP CP Bytes 55 55 75 75 0 162	1358 — 13 k — 13 k — 55 66 Country — — — — — — —	City	AS Number		6265	17	Copy     443 + 62677     443 + 62697     443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq*</li> <li>[ACK] Seq*</li> </ul>	Close 65 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint	Types  Ty
13.33.14 Name 06:47 1 06:47 1 06:47 2 hark · En t· · 4 54.15 .140 4.189 00.189 5.29 17.194 .190 122	14.49 14.49 resolution 104.20.4 192.168. 23.207.1 dpoints - 1Pv4 · 18 Packets 2 2 2 2 1 7 2 2 2 2 2 2 2 2 2 2 2 2 2	24 216 216 15.29 1.36 154.15 Ethernet 121 143 93 453 121 143 93 2453	24k 24k imit to d imit to d TCP • 2 Tx Packets	11 101 splay filter 92.168. 3.207.1 92.168. 0 UDP Tx Bytes 6 6 6 6 6 6 6 6 6 6 6 7 29 6 7 101 101 101 101 101 101 101	0090 10 k 1.36 54.15 1.36 54.15 1.36 6 8 8 8 3 1 6 2 2	T T T T T T T T T T T T T T T T T T T	CP CP CP CP CP Bytes 55 55 55 75 75 75 0 162 55 52 50	1358 — 13 k — 13 k — 55 66 Country — — — — — — — —		AS Number		626; 17 443 6269	17	■ Copy 443 + 62677 62697 + 443 443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq*</li> <li>[ACK] Seq*</li> </ul>	<ul> <li>Close</li> <li>65 Ack=2 Wil</li> <li>1 Ack=1 Win</li> <li>1 Ack=2 Win</li> </ul>	Endpoint	Types V Help Blueto Etherm FC FDDI IEEE 80 IPX IPv4 IPv4 IPv6 JXTA MPTCI NCP
13.33.14 Name 366:47 1 366:47 1 366:47 2 hark · En 54.15 .140 4.189 00.189 52.9 17.194 190 132 3.98	14.40 resolution 104.20.4 92.168 23.207.1 dpoints - 2 2 2 2 2 2 2 2 3 6 388	24 216 216 15.29 1.36 154.15 154.15 121 121 121 121 121 121 143 123 121 3972 3972 19 k	24k 24k Umit to d 1 2 1 1 2 1 1 2 1 1 1 1 1 1 1 1 1 1 1	11 101 splay filter 32.168. 3.207.1 32.168. 0 UDP Tx Bytes 6 6 6 6 6 6 6 6 6 7 29 29 172 18	1.36 54.15 1.36 6 54.15 1.36 6 8 8 8 3 1 6 2 2 k	ICkets Rx 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CP CP CP CP CP Bytes 55 55 75 75 0 162 55 22500 1114	60 55 66 Country 		AS Number		6265 17 443 6269	<sup>11</sup> 17	Copy 443 + 62677 62697 + 44 443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq-</li> <li>[ACK] Seq-</li> </ul>	<ul> <li>Zose</li> <li>Ack=2 Win</li> <li>Ack=2 Win</li> </ul>	Endpoint	Blueto Ethem FC FDDI IEEE 80 IPX IPv4 IPv6 JXTA NCP RSVP
13.33.14 Name 96:47 1 96:47 1 96:47 2 hark · En t · 4 54.15 1.40 4.189 00.189 5.29 17.194 1.140 1.142 1.149 1.14	14.40 14.49 resolution 192.168 13.207.1 dpoints - 1Pv4 - 18 Packets 2 2 2 2 1 7 2 36 38 1	24 216 216 45.29 11.36 154.15 Ethernet 121 121 143 143 93 3453 143 143 93 72 19 k 137	24 k 24 k Limit to d 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 2 1 1 1 1 1 1 1 2 1 1 1 2 1 2 1 1 1 2 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1	11 101 101 101 101 101 102 168 10 102 168 102 168 102 168 102 168 102 168 102 168 102 168 102 103 102 103 103 103 103 103 103 103 103	1.36 54.15 1.36 54.15 1.36 6 8 8 8 3 1 6 2 k 0	I I I I I I I I I I I I I I I I I I I	CP CP CP CP CP CP CP CP CP CP CP CP CP C	1358 — 13 k — 13 k — 13 k — 60 55 66 Country — — — — — — — — — — — — —	City	AS Number 		6263 17 443 6269	17 17	Copy     443 + 6267     443 + 62697     443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq*</li> <li>[ACK] Seq*</li> <li>[ACK] Seq*</li> </ul>	Close 65 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint	Blueto Ethern FC FDDI IEEE 80 IPX IPv4 IPv6 JXTA MPTCI NCP RSVP SCTP
13.33.14 ■ Name ■ 66:47 1 ■ 66:47 2 ■ 86:47 2 ■ 86:47 2 ■ 86:47 2 ■ 86:47 2 ■ 86:47 2 ■ 86:47 1 ■ 8	4.40 (04, 20, 4 (192, 168, 3, 207, 1 dpoints - IPv4 - 18 2 2 2 2 2 2 2 2 2 2 2 2 2	24 216 216 45.29 11.36 154.15 Ethernet 121 143 143 93 453 93 121 143 143 121 13972 19k 137 75634	24k 24k Limit to d 1 2 1 1 5 TCP - 2 5 Tx Packets 1 1 1 1 1 1 2 1 1 1 1 2 1 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1	11 10 10 10 10 10 10 10 10 10	1.36 1.36 54.15 1.36  14  14  14  14  14  14  14  14  16  16  16  10 k 10 k 10 k 10 k 10 k 10 k 10 k 15 k 15 k	T T T T T T T T T T T T T T T T T T T	CP CP CP CP CP Bytes 55 55 75 75 0 162 52250 1114 137 3070	60 55 66 Country 		AS Number 		626 77 443 6260	<sup>11</sup> 17	■ Copy 443 + 62677 62697 + 443 443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq=</li> <li>[ACK] Seq=</li> </ul>	Close 65 Ack=2 Wil 1 Ack=1 Win 1 Ack=2 Win	Endpoint	Types V Help Blueto Ethern FC FDDI IEEE 80 IPX IPv4 IPv6 NCP RSVP SCTP SLL
13.33.14 ■ Name ■ 86:47 1 96:47 1 96:47 2 ■ 6:47 2 ■ 6:47 2 ■ 6:47 2 ■ 6:47 2 ■ 6:47 2 ■ 7.194 132 3.98 160.131 163.68 194.189	4.40 4.49 104.20.4 192.168. 33.207.1 192.4 182.208. 1 192.4 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	24 216 15.29 1.36 154.15 Ethernet 121 121 143 143 143 143 143 143 121 121 121 143 143 143 121 121 121 121 137 257 19 k	24 k 24 k Limit to d TCP - 2 1 Tx Packets 1 1 1 1 1 2 2 1 1 1 1 2 2 1 2 1 2 2 1 1 2 2 1 2 1 2 2 1 2 1 2 2 1 1 1 2 1 1 1 1 1 2 1	11 101 32.168. 3.207.1 3.207.1 22.168. 0 UDP Tk Bytes 6 6 6 6 6 6 6 6 6 7 2 2 5 6 6 7 2 2 5 8 1 7 1 7 1 8	1.36 1.36 54.15 1.36 	rckets Rx 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CP CP CP CP CP CP CP CP CP CP CP CP CP C	60 55 66 Country 		AS Number 	443 626 443 	6265 17 443 6269	71	Copy 443 + 62677 62697 + 44 443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq-</li> <li>[ACK] Seq-</li> </ul>	Z Gose 65 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint = 7; = 586 = 244 = ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	Types V Types V Blueto Ethern FC FDDI IEEE 8/ IPX IPV-4 IPV-6 JXTA MPTCI NCP SLL TCP
13.33.14 ■ Name ■ 86:47 1 136:47 1 96:47 2 hark · En +t · 4 ↓ 54.15 5.29 15.29 15.29 160.131 163.68 160.131 163.88 164.189 118.188	4.40 4.49 (04.20.4 (92.168.3) 3.207.1 (4) 92.168.3 (3.207.1 (4) 92.168.3 (3.207.1) 1 92.468 (2.2) 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	24 216 216 1.36 154.15 Ethernet 154.15 154.15 154.15 154.15 154.15 104 104 104 104 104 104 104 104 104 104	24k 24k Limit to d 1 1 1 1 1 1 1 1 1 1 1 1 1 2 1 1 2 1 1 1 1 2 1 1 2 1 1 2 1 1 1 2 1 1 1 2 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 1 2 1 1 1 1 1 2 1	101 101 32.168. 3.207.1 32.168. 3.207.1 32.168. 0 UOP Tk Byter 6 6 6 6 6 6 6 6 6 6 6 6 6 6 7 22 5 6 7 172 18 8 256 15 8 6 6 6 6 172 18 8 10 10 10 10 10 10 10 10 10 10 10 10 10	1.36 54,15 1.36 54,15 1.36 1.36 1.36 1.36 1.36 1.36 1.36 1.36	rckets Rx 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CCP CCP CCP CCP CCP CCP CCP CCP CCP CCP	60 55 66 Country             	City	AS Number 		6263 17 443 6269	72	☑ Copy 443 + 62677 443 + 62697 443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq*</li> <li>[ACK] Seq*</li> </ul>	Close 65 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint 1=7: -50! ✓ -24! -	Types V Types V Ethem FC FDDI IEEE 88 IPX IPV4 IPV6 JXTA MPTCI NCP SCTP SLL TCP Token
13.33.14 ■ Name ■ 66:47 1 96:47 2 96:47 2 hark - En t: 4 4 54.15 .140 00.189 5.29 1.12 .147 .147 .147 .149 1.132 .29 .149 .15 .140 .15 .140 .149 .148 .149 .148 .148 .149 .148 .149 .148 .256 .256 .257 .256	4.40 1.04, 20, 4 resolution 1.04, 20, 4 1.02, 1.68 1.3, 207, 1 1.04 1.0	212 216 216 216 217 218 219 211 221 221 221 221 221 221 221 221	24 k 24 k Limit to d 1 2 1 2 1 2 1 2 1 1 1 2 1 1 1 1 2 1 2	11 101 102.168.3.207.1 122.168. 0 UDF Tr Byter 6 6 6 6 6 6 6 6 6 7 2 18 17 18 256 15 6 16 16 16 16 17 17 18 10 10 10 10 10 10 10 10 10 10	1.36 54.15 1.36 54.15 1.36 6 6 6 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	rckets RX 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CP CP CP CP CP CP CP CP CP CP CP CP CP C	60 55 66 Country 	City	AS Number 		626 17 443 6265	71 17	■ Copy 443 + 62677 62697 + 443 443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq</li> <li>[ACK] Seq</li> </ul>	<ul> <li>Close</li> <li>65 Ack=2 Win</li> <li>1 Ack=1 Win</li> <li>1 Ack=2 Win</li> </ul>	Endpoint 	Types T Types T Help Blueto Ethern FC FDDI IEEE 80 IPX4 IPv4 IPv4 IPv4 NCP RSVP SCTP SLL TCP SLL TCPE UDP
13.33.14 Amme 266:47 1 266:47 1 266:47 2 266:47 2 264:47 2	4.40 1.49 1.92.168. 1.3.207.1 dpoints - 1.2.2 2 2 2 2 2 2 2 2 2 2 2 2 2	24 216 216 216 254 254 254 215 200 200 200 200 200 200 200 200 200 20	24 k 24 k Limit to d Limit to d 1 2 1 1 2 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1	11 101 102 103 102 102 102 102 102 102 102 102 102 102	1.36 1.36 54.15 1.36	rckets Rx 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CP CP CP CP CP CP CP CP CP CP CP CP CP C	60 60 55 66 	City	AS Number 	443 626 443 	6265 17 443 6269	71	Copy 443 + 62677 62697 + 44 443 + 62697	<ul> <li>Map</li> <li>[ACK] Seq-</li> <li>[ACK] Seq-</li> </ul>	Z Gose 65 Ack=2 Win 1 Ack=1 Win 1 Ack=2 Win	Endpoint 1=7; -50( ✓ -244 - - - - - - - - - - - - -	Types V Types V Help FC FDDI IEEE 80 IPX IPV4 IPV4 IPV4 IPV4 IPV4 IPV4 IPV5 SCTP SLL TCP Token UDP SLL SL

# Analyzing Conversations

While analyzing network traffic, we may at times want to see data on a two-end conversation. By choosing Statistics and then Conversations, we can do that.

d Capturing from Ethernet		– 🗆 X
<u>File Edit View Go Capture Analyze S</u>	tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
	Capture File Properties Ctrl+Alt+Shift+C	
Apply a display filter <ctrl-></ctrl->	Resolved Addresses	+
No. Time Source	Protocol Hierarchy	i Info
8315., 18701.312239 192.108.1.36 8315., 18701.707258 140.82.114.25 8315., 18702.343658 192.168.1.36 8315., 18702.343658 192.168.1.36 8315., 18703.393240 92.168.1.36 8315., 18703.395279 192.168.1.33	Conversations Endpoints Packet Lengths I/O Graph	5 [TCP Keep-Alive] 20689 + 443 [ACK] Seq=2179 Ack=4269 Win=131072 Len-1 5 [TCP Keep-Alive ACK] 443 + 20689 [ACK] Seq=4269 Ack=4369 Win=32768 Len=0 SLE=2179 SRE=2180 5 [TCP Keep-Alive] 1797 + 5228 [ACK] Seq=1238 Ack=4376 Win=130816 Len=1 5 [TCP Keep-Alive] ACK] 5228 + 17977 [ACK] Seq=4876 Ack=1231 Win=67072 Len=0 SLE=1230 SRE=1231 6 [TCP Keep-Alive] ACK] 5228 + 17977 [ACK] Seq=4876 Ack=1231 Win=67072 Len=0 SLE=1230 SRE=1231 7 [ACK] Seq=4876 Ack=48842 Win=130560 Len=110 [TCP segment of a reassemble 80909 + 70331 [SPH, ACK] Seq=48316 Ack=88429 Win=98616 Len=110 [TCP segment of a reassemble
<pre>ball_law_law_law_law_law_law_law_law_law_</pre>	Service gesponse lime  DHCP (BOOTP) Statistics ONC-RPC Programs 29West ANCP BACnet Collectd DNS	2033 + 8809 [ACK] SeeB429 AC+9102 kin=130844 Len=0 face \Device\WPF_{43886604D-08DB-4283-970D-CAFA21A6F8C8}, id 0 :ff:ff:ff:ff:ff)
0000 ff ff ff ff ff ff ff 14 a7 2b 90 0010 be ef 01 72 65 61 66 74 65 61 0028 61 63 6b 5f 64 65 74 65 63 74 0030 74 00 00 00 00 00 00 00 00 00 00 00	Flow Graph HART-IP HPFEEDS HTTP + HTTP2 Sametime TCP Stream Graphs +	
Ethernet: <li>Ethernet: sive capture in progress&gt;</li>	UDP Multicast Streams	Packets: 831577 * Displayed: 831577 (100.0%) Profile: Default

thernet · 38	IPv4 · 721	IPv6 · 18	TCP ·	3436 UDP *	4254						
ddress A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets $B \rightarrow A$	Bytes B → A Rel Start	Duration	Bits/s A → B	Bits/s B → A	
0.0.0	255.255.255.255	i 21	7382	21	7382	0	0 4532.35344	4048.7739	14		0
1.1.1	192.168.1.36	32	2333	0	0	32	2333 671.681222	17171.6112	0		1
38.196.85	192.168.1.36	1	146	1	146	0	0 121.594313	0.0000	_		—
192.193.112	192.168.1.36	10	1777	5	1432	5	345 7284.414668	2.6232	4367		1052
1.111.250	192.168.1.36	35	9313	17	7026	18	2287 1300.236792	60.6548	926		301
6.178.123	192.168.1.36	53	13 k	24	9042	29	41187724.939442	66.6897	1084		493
6.243.25	192.168.1.36	44	16 k	20	10 k	24	5133 2269.56476	28.9219	3016		1419
7.200.244	192.168.1.36	2	132	2	132	0	0 4567.39187	0.1243	8494		0
114.129.228	192.168.1.36	71	21 k	35	14 k	36	7002 3087.434232	2311.3390	50		24
126.192.219	192.168.1.36	1,486	477 k	569	386 k	917	91 k 675.447081	255.5962	12 k		2860
215.10.43	192.168.1.36	44	16 k	20	13 k	24	3196 4108.99947	9.8963	10 k		2583
218.21.200	192.168.1.36	716	94 k	297	52 k	419	42 k 4118.22718	4593.4384	90		73
223.110.241	192.168.1.36	1,417	583 k	593	202 k	824	381 k1272,74572	15154.8491	106		201
228.235.253	192.168.1.36	48	18 k	20	13 k	28	5786 2291.83113	6.8374	15 k		6769
230.235.18	192.168.1.36	27	7861	13	6449	14	1412 377.335890	84.0371	613		134
234.166.91	192.168.1.36	47	16 k	21	12 k	26	3336 2270.35846	28.3269	3595		942
8.8.8	192.168.1.36	63	6982	31	4649	32	2333 673 690243	17171.8489	2		1

Wireshark will open a window like this, showing every conversation and then statistics related to that conversation that includes number of packets, bytes, duration of the conversation etc.

# Analyzing traffic graphs

It is best to work with graphs when dealing with huge amounts of traffic, instead of scrolling down thousands of captured packets to identify errant packets. There are a couple of graphs within Wireshark which can be used.

# IO graphs

These graphs can be used to evaluate highs and lows in traffic. This is very important in tracking matters. To use an IO graph, select a packet and click "IO Graph" under "Statistics." Select "Statistics," then "IO Graph," to create an IO Graph.

d Capturing from Ethernet		- 🗆 X
<u>File Edit View Go Capture Analyze</u>	<u>Statistics</u> Telephony <u>Wireless</u> <u>T</u> ools <u>H</u> elp	
	Capture File Properties Ctrl+Alt+Shift+C	
Apply a display filter <ctrl-></ctrl->	Resolved Addresses	□ ·]+
No. Time Source	Protocol Hierarchy	1 Info
8334 18989.801943 35.170.0.145	<u>C</u> onversations	9 Application Data
8334 18989.801984 192.168.1.36	- Endpoints	4 16967 → 443 [ACK] Seq=153233 Ack=113138 Win=511 Len=0
8334 18990.587094 35.170.0.145	Endpoints Dacket Lengths	9 [TCP Spurious Retransmission] , Application Data
8334 18990.587160 192.168.1.36	Packet Lengths	6 [TCP Dup ACK 833452#1] 16967 → 443 [ACK] Seq=153233 Ack=113138 Win=511 Len=0 SLE=112813 SRE…
8334 18990.682016 192.168.1.36	J/O Graph	5 M-SEARCH * HTTP/1.1
8334 18990.687385 192.168.1.33	Service <u>R</u> esponse Time	6 37951 + 64487 Len=514
8554 18990.909789 192.188.1.55	DHCB (BOOTD) Statistics	2 membership keport / Join group 259.255.250 for any sources / Join group 224.0.0.251 for
> Frame 1: 60 bytes on wire (480 bi	Drice (BOOIP) statistics	face \Device\NPE {4388604D-08DB-4283-970D-C4F42146FBC8}, id 0
> Ethernet II, Src: currento 0e:be:	ONC-RPC Programs	f:ff:ff:ff:ff)
Data (46 bytes)	29West	
	ANCP	
	BACnet •	
	Collectd	
	DNS	
	Die Cred	
2000 If if if if if if it it it it	Flow Graph	
0000 11 11 11 11 11 11 14 87 20 00	HART-IP	
0020 61 63 6b 5f 64 65 74 65 63 74	HPFEEDS	
0030 74 00 00 00 00 00 00 00 00 00 00	HTTP +	
	HTTP2	
	Sametime	
	TCB Stream Granhr	
	icr arean diapits	
A Thursda day waters is successed	UDP Multicast Streams	Public opport Public dispatc (see op/)
Emernet: <ive capture="" in="" progress=""></ive>		Profile: Default



The data in the x-axis is the time in seconds, and the data in the y-axis, according to the graph above, represents the packets per tick. You can filter the graph to display graphs based on the daytime, interval and log scale, and you can even reset applied settings back to normal.

## Flow graphs

This gives us a column-type graph showing which connections we might use to troubleshoot, missing frames, retransmission traffic and much more. We can export those results in a text-based production. To construct a flow graph, pick "Statistics," and then "Flow Graph.". By doing so we were able to produce the graph below.

Capturing from Ethernet			( <u>~</u>	- 🗆 X
File         Edit         Yiew         Go         Capture         Analyze         S           Apply a display filter         Image: Control of the second se	tatistics         Telephony         Wireless         Iools         Help           Capture File Properties         Ctrl+Alt+Shift+C           Resolved Addresses         Protocol Hierarchy           Conversations         Endpoints	Info 9 Membership Report / Join group 23/ 9 Membership Report / Join group 23 9 Membership Report / Join group 23	4.0.0.251 for any sources 9.255.255.250 for any sources 9.255.255.250 for any sources / Join group 239.	255.3.22 fo
834219167.504932 140.82.113.25 834219167.504113 192.168.1.36 834219167.50429 192.168.1.36 834219167.787570 140.82.113.25 > Frame 1: 60 bytes on wire (480 bi > Ethernet II, Src: currento_0e:be: > Data (66 bytes)	Packet Lengths I/O Graph Service <u>Besponse Time</u> DHCP (BOOTP) Statistics ONC-RPC Programs 29West	<pre>&amp; Application Data # 20722 + 443 [ACK] Seq=2096 Ack=42: 2 Application Data # 443 + 20722 [ACK] Seq=4221 Ack=21: face \Device\NPF_{4388604D-08DB-428 :ff:ff:ff:ff;ff;</pre>	21 Win=130560 Len=0 24 Win=32768 Len=0 33-970D-CAFA21A6FBC8}, id 0	v
	ANCP BACnet > Collectd DNS Elow Graph			
0000         ff ff ff ff ff ff 14 a7         2b 0e           0010         be ef 01 72 65 61 6c 74 65 66         0020         61 63 6b 5f 64 65 74 65 63 74           0020         61 63 6b 5f 64 65 74 65 63 74         0030         74 00 00 00 00 00 00 00 00 00 00         00 00	HART-IP HPFEEDS HTTP HTTP2 Sametime			
Ethernet: <li>ive capture in progress&gt;</li>	TCP Stream Graphs  UDP Multicast Streams	-	Packets: 834249 · Displayed: 834249 (100.0%)	Profile: Default



# TCP stream graphs

These are a set of graphs representing network traffic in a graphical style distinct from the graphs above. Let's take a look:

## Round-trip time graphs

The round trip time is the amount that the ACK would receive for a packet sent. This occurs within TCP communication, where an ACK is received for every packet sent, confirming a packet delivery. Choose a packet, then navigate to "Statistics," then pick "TCP Stream Graph," then "Round Trip Time Graph" to construct a round trip time graph.

A couple of things to note:

The x-axis is the TCP sequence number and in seconds the y-axis is the RTT

The dots on the graph represent a packet's RTT. An empty graph can mean you have selected a packet in the opposite direction

You should look for a vertical line of plotted RTT points to define the latency. This could either suggest that the sending device has a queued-up packet, or duplicate ACKs that are suffering.

		50000	100000	150000	200000	250000
0.01-						
0.02 -						
0.03			•			
0.04 -						
0.05 -						
0.06-						•
0.07-						
0.08-						
0.09-						
0.10	÷.				•	•

## Throughput graphs

Similar to IO graphs, traffic direction is represented by the throughput graphs. Nonetheless, these graphs differ from the IO graphs in that they represent unidirectional traffic, whereas IO graphs depict traffic in both directions. Note that depending on the selected packet the data you'll see on the graph will be different.

The x-axis is the time in seconds in the graph, and the y-axis represents the bytes per second throughput.

#### Time-sequence graph (tcptrace)



Using this graph portrays the TCP traffic flow with time. The traffic is unidirectional, just as the throughput graphs are. Use this graph to inform you about segments currently moving, the acknowledgement of segments we have provided, and the buffer area that the customer can carry.

#### Open the capture or trace file

Choose any TCP packet (various will offer different results)

Select the option 'Statistics,' then select 'TCP Stream Graphs,' then select 'Time Series Graph (tcptrace)'

The y-axis in the graph represents the number of the TCP series, and the x-axis represents the time in seconds. The numbers of the TCP series are increased by the bytes sent with each packet. This means that if the number of the sequence is 1 and the packet sent has 10 bytes of data, the number of the sequence will be increased by 10, making the next number 11.



#### Customizing Display column according to our preferences

Default column display does not work effectively for the type of analysis, it's better to customize according to our preferences

Wireshark 's default columns: Number, Time, Source, Destination, Protocol, Length, and Info

	Apply a display filter <ctrl-></ctrl->										
No.	Time	Source	Destination	Protocol	Length Info	^					
	1101 84.441208	58.251.106.185	192.168.1.36	TCP	74 443 → 30033 [PSH, ACK] Seq=1 Ack=235 Win=15360 Len=20 [TCP segment of a reassembled PDU]						
	1102 84.441285	192.168.1.36	58.251.106.185	TCP	54 30033 → 443 [ACK] Seq=235 Ack=21 Win=65516 Len=0						
	1103 84.573504	18.219.117.14	192.168.1.36	TLSv1.2	98 Application Data						
	1104 84.573574	192.168.1.36	18.219.117.14	TCP	54 29697 → 443 [ACK] Seq=3244 Ack=1469 Win=512 Len=0						
	1105 84.573678	192.168.1.36	18.219.117.14	TLSv1.2	98 Application Data						
	1106 84.926192	192.168.1.36	18.219.117.14	UDP	99 55932 → 8801 Len=57						
	1107 85.041051	192.168.1.36	104.18.199.63	TCP	55 [TCP Keep-Alive] 29804 → 443 [ACK] Seg=1 Ack=1 Win=509 Len=1						

We can change this by go to Edit  $\rightarrow$  Preferences

	Сору	•	1 . E Q C	Q 🔢		
٩	Eind Packet	Ctrl+F				-
	Find Next	Ctrl+N	stination	Protocol	Length Info	
	Find Previous	Ctrl+B	.219.117.14	UDP	55 55931 → 8801 Len=13	
			2.168.1.36	UDP	60 8801 → 55931 Len=13	
	Mark/Unmark Packet	Ctrl+M	2.168.1.36	UDP	60 8801 → 55932 Len=13	
	Mark All Displayed	Ctrl+Shift+M	.219.117.14	UDP	55 55932 → 8801 Len=13	
	Unmark All Displayed	Ctrl+Alt+M	.219.117.14	UDP	55 55933 → 8801 Len=13	
	Nevt Mark	Ctrl+Shift+M	.219.117.14	UDP	99 55932 → 8801 Len=57	
	INCLE IVIDIR.	CHIPSHILPIN	2.168.1.36	UDP	60 8801 → 55933 Len=13	
	Ignore All Displayed	Ctrl+Shift+D	7.14, Dst: 192. Port: 55931	168.1.36	0:39:66 (80:1/:00:30:39:66)	
	Ignore All Displayed Unignore All Displayed	Ctrl+Shift+D Ctrl+Alt+D	7.14, Dst: 192. Port: 55931	168.1.36	b:9a:ce (00:1/:bD:9b:9a:ce)	
	Ignore All Displayed Unignore All Displayed Set/Unset Time Reference	Ctrl+Shift+D Ctrl+Alt+D Ctrl+T	7.14, Dst: 192. Port: 55931	168.1.36	biya:ee (00:1/:bD:96:9a:ce)	
	Ignore All Displayed Unignore All Displayed Set/Unset Time Reference Unset All Time References	Ctrl+Shift+D Ctrl+Alt+D Ctrl+T Ctrl+Alt+T	7.14, Dst: 192. Port: 55931	ist: Kiyon_ 168.1.36	biyaice (00:1/:bbiybiyaice)	
	Ignore All Displayed Unignore All Displayed Set/Unset Time Reference Unset All Time References Next Time Reference	Ctrl+Shift+D Ctrl+Alt+D Ctrl+T Ctrl+Alt+T Ctrl+Alt+N	7.14, Dst: 192. Port: 55931	ist: kiyon_ 168.1.36	b:94:ee (00:1/:bb:96:9a:ee)	
	Ignore All Displayed Unignore All Displayed Set/Unset Time Reference Unset All Time References Next Time Reference Previous Time Reference	Ctrl+Shift+D Ctrl+Alt+D Ctrl+Alt+T Ctrl+Alt+T Ctrl+Alt+N Ctrl+Alt+B	00 45 20 k	ist: klyon_ 168.1.36	юзча:ее (ФИ:1/:bb:96:9а:се) :Е	
	Ignore All Displayed Unignore All Displayed Set/Unset Time Reference Unset All Time Reference Next Time Reference Previous Time Reference Time Shift	Ctrl+Shift+D Ctrl+Alt+D Ctrl+Alt+T Ctrl+Alt+T Ctrl+Alt+N Ctrl+Alt+B Ctrl+Alt+B	00 45 20	st: Klyon_ 168.1.36	ibiyaice (00:1/:bbiyaice) :E	
	Ignore All Displayed Unignore All Displayed Set/Unset Time Reference Unset All Time References Next Time Reference Previous Time Reference Time Shift Packet Comment	Ctrl+Shift+D Ctrl+Alt+D Ctrl+Alt+T Ctrl+Alt+T Ctrl+Alt+N Ctrl+Alt+B Ctrl+Shift+T Ctrl+Alt+C	00 45 20	NQ #	юзээ:ее (ФИ:1/:bb:эb:эа:се) :Е 	 
	Ignore All Displayed Unignore All Displayed Set/Unset Time Reference Unset All Time Reference Previous Time Reference Time Shift Packet Comment Delete All Packet Comments	Ctrl+Shift+D Ctrl+Alt+D Ctrl+Alt+T Ctrl+Alt+T Ctrl+Alt+N Ctrl+Alt+N Ctrl+Alt+B Ctrl+Shift+T Ctrl+Alt+C	00 45 20 - k 00 45 20 - k 00 45 20 - k	st: klyon_ 168.1.36	юзча:ее (ФИ:1/:bb:96:9а:ce) Е Е	
	Ignore All Displayed Unignore All Displayed Set/Unset Time Reference Unset All Time Reference Previous Time Reference Time Shift Packet Comment Delete All Packet Comments Configuration Profiles	Ctrl+Shift+D Ctrl+Alt+D Ctrl+Alt+T Ctrl+Alt+T Ctrl+Alt+N Ctrl+Alt+B Ctrl+Alt+B Ctrl+Alt+C Ctrl+Alt+C	00 45 20 ··· k 00 45 20 ··· k 00 45 20 ··· k 00 76 56 ··· 5"	N0.#	юзча:ее (ФФ:1/:bb:96:9а:ce) -Е 	 

On there, extend Appearence  $\rightarrow$  Columns We can see the columns that appeared on wireshark analysis window there.

Appearance Columns Font and Colors Layout Capture Expert Filter Buttons Name Resolution Protocols RSA Keys Statistics Advanced	Displayed	Title No. Time Source Destination Protocol Length Info	Type Number Time (format as specified) Source address Destination address Protocol Packet length (bytes) Information	Fields	Field Occurence
	+ -	Show displ	ayed columns only	OK	Cascal Lia

There is an option of adding and deleting columns

- + for adding Columns
- for deleting columns

When we click on +, it will add a new column

Name that column according to your preference. By default, the column type will be Number we can change that by double clicking that column's type. It will drop down all available types.

Clicking – will delete that column.

Let us reset the time now to get analyzing easier. Change "Seconds After Capture Start" to "Date and Time of Day"

1	Appearance	Displayed	Title	Type	Fields
	Font and Colors		No.	Number	
	Lavout		Time	Time (format as specified	0
	Canture		Source	Source address	<i>.</i>
	Expert		Destination	Destination address	
	Filter Buttons		Protocol	Protocol	
	Name Resolution		Length	Packet length (bytes)	
ŝ	Protocols		Info	Information	
2	RSA Kevs		New Col	Number	2
>	Statistics Advanced			IEEE 802.11 TX rate IP DSCP Value Information Net dest a(resolved) Net scad(resolved) Net scr ad(resolved) Net scr adnresolved) Net scr adnresolved) Net scr adnresolved) Network dest addr Network scr addr Number	
5	>	+ - (	Show displ	ayed columns only	

Date and Time of Day (1970-01-01 01:02:03.123456)

Seconds Since Beginning of Capture Seconds Since Previous Captured Packet

UTC Time of Day (01:02:03.123456)

Automatic (from capture file)

Hundredths of a second

Seconds Tenths of a second

Milliseconds

Time of Day (01:02:03.123456)

Seconds Since 1970-01-01

Shift+Right

Shift+Left

Ctrl+Right

Ctrl+Shift+W

•

Ctrl+Shift+R

Ctrl+Left

Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)

Seconds Since Previous Displayed Packet UTC Date and Time of Day (1970-01-01 01:02:03.123456)

UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)

Ctrl+Alt+1

Ctrl+Alt+2

Ctrl+Alt+3

Ctrl+Alt+4

Ctrl+Alt+5

Ctrl+Alt+6

Ctrl+Alt+7

Ctrl+Alt+8

+ - Show displayed columns only

Go to: View → Time Display Format → Date and Time of Day.



Packet <u>B</u>ytes Time Display Forma

Zoom

Name Resolution

Expand Subtrees

Expand All

Resize Columns

Internals

0000 00 Colorize Packet List

Collapse <u>A</u>ll

Coloring Rules...

Colorize Conversation

Collapse Subtrees

Frame 1 Etherne Interne

User Di

Data (1

0020 01 0030 e4

🔘 🍸 еі

After that, as shown below (**View** — > **Time Display Format** — > **select "Seconds: 0**"), we will change the precision of the displayed time from automatic to "Seconds" Many of the columns are aligned to the right and can be corrected by right clicking the column and selecting the correct alignment

📶 📕 🙋 🛞 🛄 🖾 🔯 🍳 🖗 🗢 🗟 🖗 👼 🗮 🦉		
No.         Time         Source         Destination           1 2020-06-13 18:23:18         18:21.14         192.16           9 2020-06-13 18:23:18         157.240.16.35         192.166           10 2020-06-13 18:23:18         157.240.16.35         192.166           11 2020-06-13 18:23:18         157.240.16.35         192.166           13 2020-06-13 18:23:19         157.240.16.35         192.166           14 2020-06-13 18:23:19         157.240.16.35         192.166           14 2020-06-13 18:23:19         157.240.16.35         192.166           14 2020-06-13 18:23:19         157.240.16.35         192.166           15 0000 06:12 10:23:19         157.240.16.35         192.166           16 0000 06:13 10:23:19         157.240.16.35         192.166           17 0000 06:13 10:23:19         157.240.16.35         192.166           16 0000 06:13 10:23:19         157.240.16.35         192.166           17 0000 06:13 10:23:19         157.240.16.35         192.166           16 0000 06:13 10:23:19         157.240.16.35         192.166           17 0000 06:13 10:23:19         157.240.16.35         192.166           18 0000 06:13 10:23:19         157.240.16.35         192.166           17 0000 06:13 10:23:19         157.240.16.35         192.1	Align Left Align Center Align Right Column Preferences Edit Column Resize to Contents Resize Column to Width	eq=1 Ack=451 Win=351 Len=0 eq=1 Ack=490 Win=351 Len=0 eq=53 Ack=1659 Win=373 Len=0 > -08DB-4283-970D-CAFA21A6FBC8), id 0
<pre>&gt; Ethernet II, Src: currento_@e:be:c8 (14:a7:2b:@e:be:c6 &gt; Internet Protocol Version 4, Src: 18.219.117.14, Dst: &gt; User Datagram Protocol, Src Port: 8801, Dst Port: 5595 &gt; Data (13 bytes) 00000 00 17 6b 96 9a ee 14 a7 2b 0e be c8 08 00 45 20</pre>	Resolve Names       No.     Number       Time     Time (format as specified       Source     Source address       Destination     Destination address       Protocol     Protocol       Langth     Backs langth (http:)	0
0010         001 <td>Length Packet length (bytes)     Info Information     Remove this Column</td> <td></td>	Length Packet length (bytes)     Info Information     Remove this Column	

We can add Hosts to our panel. For that , filter on http.request, so we're only seeing the HTTP requests.

Right Click on Host $\rightarrow$ Apply	7 as	: Column
---	------	----------

4	Ethernet						— ć	ס	×
File	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	e <u>A</u> nalyze <u>S</u> tatistics 1	felephony <u>W</u> ireless <u>T</u> ools	<u>H</u> elp					
1	📕 🙋 💿 📄 🚍 📚 🖻	9 0 0 2 7 5	📜 🗏 Q Q Q 💵						
	http:request						X		- +
No.	Time	Source	Destination	Protocol	Length Info				^
	96 2020-06-14 10:59:	42 192.168.1.35	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1				
	98 2020-06-14 10:59:	43 192.168.1.35	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1				
	99 2020-06-14 10:59:	44 192.168.1.35	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1				
Г	131 2020-06-14 10:59:	55 192.168.1.36	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1				
+	133 2020-06-14 10:59:	56 192.168.1.36	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1				
	135 2020-06-14 10:59:	57 192.168.1.36	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1				
+	137 2020-06-14 10:59:	58 192.168.1.36	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1				
	227 2020-06-14 11:00:	53 192.168.1.35	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1				
	236 2020-06-14 11:00:	56 192.168.1.35	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1				
	250 2020-06-14 11:00:	59 192.168.1.35	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1				
	255 2020-06-14 11:01:	02 192.168.1.35	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1				
	268 2020-06-14 11:01:	05 192.168.1.35	239.255.255.250	SSUP	1/9 M-SEARCH * HTTP/1.1				12127
	2/4 2020-00-14 11:01:	00 192.100.1.35	239.233.235.230	550P	1/9 M-SEARCH - HTTP/1.1				~
	[Stream index: 5]								^
	> [Timestamps]								_
~	Simple Service Discovery	y Protocol							
1	> M-SEARCH * HTTP/1.1\r	r\n							
	HUS1: 239.255.255.2	Expand Subtrees		1					
	MX: 1/s/s	Collapse Subtrees							
	ST: ucn:dial_multic	Europed All							
	USER-AGENT: Google	Expand All							
	\c\n	Collapse All							
	[Full request URI:	Apply as Column	Ctrl+Shift+I	1					
	[HTTP request 3/4]								
	[Prev request in Tr	Apply as Filter							
	[Next request in Tr	Prepare as Filter	•						~
0.00	0 01 00 5e 7f ff fa	Conversation Filter	•	F -					
001	0 00 c9 03 67 00 00	Colorize with Filter	•	.5					
002	0 ff fa f3 d5 07 6c	Colonize Warrinter		SEAR					
003	10 43 48 20 2a 20 48	Follow	,	1 · · H					
004	4f 53 54 3a 20 32	Conv	•	.255					
005	22 32 35 30 38 31 22 73 73 64 79 3a	copy		AN:					
007	0 0a 4d 58 3a 20 31	Show Packet Bytes	Ctrl+Shift+O	urn:					
008	0 64 69 61 6c 2d 6d	Export Packet Bytes	Ctrl+Shift+X	reen					
009	0 2d 6f 72 67 3a 73			:dia					
008	0 20 47 6f 6f 67 6c	Wiki Protocol Page		me/8					
000	0 33 2e 30 2e 34 31	Filter Field Reference		Wind					
000	6f 77 73 0d 0a 0d	Protocol Preferences	•						
0	2 HTTP Host (bttp host)	Decode As				Packete: 6515 : Dienlaved: 265 (4 1%)	P	rofile D	<b>Nofault</b>
	in the rose (helphilose), i	Control Industry Designation				i ocicas osto Displayed, 200 (4.176)	10	Perint, D	- Count

# Analysing the Application Layer Layer 6/7

<sup>ву</sup> Ambadi MP

# Analyzing malware traffic through Wireshark

No	. Time	Source	Destination	Protocol	Length Host	Info	^
	4144 2020-06-14 11:28:24	192.168.1.36	13.33.171.104	HTTP	646 static.ts.360.com	GET /display/main.titlebar/20190918093403/active-Purple_rocket.png HTTP/1.1	
	4141 2020-06-14 11:28:24	192.168.1.36	13.33.171.104	HTTP	645 static.ts.360.com	GET /display/main.titlebar/20190918093403/hover-Purple_rocket.png HTTP/1.1	
	4140 2020-06-14 11:28:24	192.168.1.36	13.33.171.104	HTTP	644 static.ts.360.com	GET /display/main.titlebar/20190918093403/rest-Purple_rocket.png_HTTP/1.1	
	3917 2020-06-14 11:28:18	192.168.1.36	13.228.109.169	HTTP	596 spec.cloud.360safe.com	POST /commonquery HTTP/1.1 (application/x-www-form-urlencoded)	
	3914 2020-06-14 11:28:18	192.168.1.36	13.228.109.169	HTTP	588 spec.cloud.360safe.com	POST /commonquery HTTP/1.1 (application/x-www-form-urlencoded)	
	3888 2020-06-14 11:28:17	192.168.1.36	13.228.109.169	HTTP	612 spec.cloud.360safe.com	POST /commonquery HTTP/1.1 (application/x-www-form-urlencoded)	
	967 2020-06-14 11:06:37	192.168.1.36	54.179.144.160	HTTP	628 spec.cloud.360safe.com	POST /commonguery HTTP/1.1 (application/x-www-form-urlencoded)	
	1799 2020-06-14 11:13:20	192.168.1.36	109.201.159.48	HTTP	291 sdup.update.360safe.com	GET /lib/safeup_wl.cab?mid=79a0f5e8daeffd37db9ccb2870fe564d&ver=10.6.0.1285&lan=en&os=10	
	4448 2020-06-14 11:28:25	192.168.1.36	54.255.136.181	HTTP	329 s.360safe.com	GET /safei18n/promote_space.htm?location=main_titlebar&content=Main.Title.Cef.UpgradeNow	8
	4049 2020-06-14 11:28:23	192.168.1.36	54.255.136.181	HTTP	238 s.360safe.com	GET /safei18n/feature.htm?id=20001∣=79a0f5e8daeffd37db9ccb2870fe564d&ver=10.6.0.1285&	1
	3996 2020-06-14 11:28:18	192.168.1.36	54.255.136.181	HTTP	285 s.360safe.com	GET /safei18n/promoutil.htm?type=error&act=cloudsync&ecode=0&pver=8.6.0.1111&at=1∣=79	a
	3882 2020-06-14 11:28:17	192.168.1.36	54.255.136.181	HTTP	238 s.360safe.com	GET /safei18n/main.htm?mode=hidden∣=79a0f5e8daeffd37db9ccb2870fe564d&ver=10.6.0.1285&	1~
e						2	

# Extracting Objects from HTTP Traffic

Spreading of malware on networks is quite common. So, Security professionals may need to export objects from the pcaps for closer examination when reviewing packet captures (pcaps) of suspicious activity.

Let us see how to extract objects using Wireshark

For extracting files go to File → Export Objects We can see DICOM , HTTP , IMF , SMB , TFTP protocols there For files from HTTP Traffic

File  $\rightarrow$  Export Objects  $\rightarrow$  HTTP



Click Save All. Choose Location For saving those files. Files will be extracted and saved there.

# Extracting Objects from SMTP Traffic

But malwares are transferred not only though HTTP.SMTP is the other protocol that used for malware spreading.

Let's see how to extract emails from SMTP Traffic.

## Filter: **smtp.data.fragment**

## Click on File $\rightarrow$ Export Objects $\rightarrow$ IMF

Open	Ctrl+O	ો 🗿 📑 🧃 લ લ	Q II							
Open <u>R</u> ecent	۰ 📔									2
Merge		Destination	Protoco	Length Host		Info				
Import from Hex Dump.	-	98.137.159.2	6 SMTP/:	L 59		from: Your	Life <yourlife36@7162.com>, subject: Hurry up and p</yourlife36@7162.com>	ay! - ganjam	an, (text,	/F
<u>C</u> lose	Ctrl+W	98.137.159.2	5 SMTP/:	L 59		from: Your	Life <yourlife56@1598.com>, subject: Your password!</yourlife56@1598.com>	- dontscrew	, (text/p.	lā
Saue	CtrlaS	98.137.159.2	6 SMTP/	L., 59 L., 59		from: Your	Life(YourLife2908738.com), subject: No longer priv	d this! - as	da123456.	N.
Sava Ar	Ctrl+Shift+S	98.137.159.2	6 SMTP/	L 59		from: Your	Life <yourlife71@2261.com>, subject: I won't warn y</yourlife71@2261.com>	ou again! -	93irish89,	1
ance Dam	Curronners	98.137.159.2	6 SMTP/:	I 59		from: Your	Life <yourlife69@2844.com>, subject: Infected your</yourlife69@2844.com>	computer! -	dcjDik, (1	te
File Set	•	98.137.159.2	6 SMTP/:	L 59		from: Your	Life <yourlife39@9083.com>, subject: Recorded you m</yourlife39@9083.com>	astrubating!	- 09104654	41
Export Specified Dackets		98.137.159.2	6 SMTP/	L		from: Your	Life(YourLife5607082.com), subject: I got everythi	l - davrit	(text/pla	in
Export Dacket Dissection		98.137.159.2	6 SMTP/	L 59		from: Your	Life <yourlife91@3903.com>, subject: I can destroy</yourlife91@3903.com>	everything!	- 12345678	<u>,</u>
Export Packet Dissection	Chill Shife Y	98.137.159.2	6 SMTP/	I 59		from: Your	Life <yourlife02@7678.com>, subject: Your password!</yourlife02@7678.com>	- nafd111,	(text/pla:	ir
Export Packet bytes	Cut+shint+x	98.137.159.2	6 SMTP/:	I 59		from: Your	Life <yourlife59@3510.com>, subject: Data of you an</yourlife59@3510.com>	d your family	y! - peace	
Export PDOS to File										>
Export ILS Session Keys.	· _ D.	59 hytes captured (	472 bits)							
export Objects		urm dia Stan	lard . 🖉 Wire	shark - Export - IME obje	ect list			200		x
Print	Ctrl+P	HTIP		copore and obje					- 1	283
0.3	CHUO	IMF					Terres and a stream			+
Guir	Cui+Q	SMB 23000 se	onds Packet	Hostname	Content lype	Size	Filename			^
[Time delta from	previous display	TFTP 000000 s	338	YourLife36@7162.com	EML file	2458 bytes	s Hurry up and pay! - ganjaman.eml			
Frame Number: 338				YourLife56@1598.com	EML file	2461 bytes	s Your password! - dontscrew.eml			
Frame Length: 59 bytes (472 bits)			617	YourLife92@8738.com	EML file	2462 bytes	s No longer private! - 123456789.eml			
Capture Length: 59 bytes (472 bits)		630	YourLife29@8738.com	EML file	2465 bytes	s You better read this! - asda123456.eml				
[Frame is marked:	False]		714	YourLife71@2261.com	EML file	2473 bytes	s I won't warn you again! - 93irish89.eml			
[Protocols in fra	: raisej me: eth:ethertyne:i	o:tco:smto:imf:data-	ext 788	YourLife69@2844.com	EML file	2461 bytes	s Infected your computer! - dcjDik.eml			
[Coloning Dulo No	mer centeenereyperig	preepromepromition	814	YourLife39@9083.com	EML file	2471 bytes	Recorded you mastrubating! - 0910465419.eml			
0 20 e5 2a b6 93 f	1 00 08 02 1c 47 at	e 08 00 45 00 ·*·	840	YourLife42@9083.com	EML file	2456 bytes	a l got everything! - 121212.eml			
0 00 2d 07 2c 40 0	0 80 06 e6 8d 0a 06	5 01 68 62 89,	905	Vourl ife56@7082.com	EMI file	2453 hytes	Read carefully! - davrit eml			
6 fa 08 8f 01 00 0	9 e3 c2 ba cb 97 tt 8 0d 0a 2e 0d 0a	01 02 20 10		Vourl ife01@2002.com	EMI file	2469 bytes	L can destroy even thing - 12245679 em			
			045	Vaud if=02@7670	ENAL CL	2400 bytes	Very assured as fel 11 and			
			900	Vaul : 6-50@2510 and	ENTERNE	2432 Dytes	Dete of use and use for it is a set of the			
			9999	YOUILIEJ9@5J10.COII	ENL CL	2400 Dytes	Data of you and your family: - peace.emi			
			1023	YOUFLITEU1@60/3.com	EIVIL TILE	2445 bytes	s Pay: - 12345.emi			
			1030	YourLifeU1@60/3.com	EIVIL file	2444 bytes	s Pay: - tomcat.eml			
			1052	YourLife97@6073.com	EML file	2455 bytes	s Videos of you! - 122577.eml			
			1120	YourLife53@3510.com	EML file	2462 bytes	s I seen everything! - xbdmiy4.eml			
			1130	YourLife70@3953.com	EML file	2457 bytes	s Your private data! - 2645885.eml			
ne (59 bytes) Reassem	oled SMTP (2458 bytes)		1188	YourLife01@7417.com	EML file	2453 bytes	s You got owned! - jigabu.eml			
			1209	YourLife36@2231.com	EML file	2466 bytes	Take care next time! - 8380358.eml			
			1236	YourLife59@2231.com	EML file	2488 bytes	s Your ife about to get ruined! - computercomputer.er	ml		
			1299	YourLife29@5316.com	EML file	2465 bytes	s I won't warn you again! - saa124chel.eml			
			1661	YourLife15@6425.com	EML file	2451 bytes	Your privacy! - J4k4rt4.eml			
			1670	Yourl ife42@2656.com	EMI file	2468 bytes	Safe your privacy! - incretible.eml			
			1679	Yourl ife67@2656.com	EMI file	2466 hytes	Everyone will know! - iloveniki.eml			
			1709	Yourl ife62@2266.com	EMI file	2466 bytes	Vour private datal - britzelici emi			¥
			LL.C.G	Tensio 200 con	c.eo/0_tue	and budge	Contraction (1913) - Pritzeller ensi			-
			l'ext Filte	r:			4 <u>0. 1975 -</u>			_
							and the second sec	78000000	22422	111
							Save Save All	Close	Help	

Save these .eml files. These files can be checked with an email client or examined in a text editor.



# Extracting Objects from FTP Traffic

During malware infections some malware families are using FTP. Our malware executables retrieved from an FTP server, followed by information sent back to the same FTP server from the infected Windows Host.



## Filter: ftp.request.command

We can see Username, Password, and files in traffic using this filter.

Time Source	Destination	Protocol L	ength Host	Info	
227 2019-06-14 04:52:15 10.6.13.102	216.55.163.106	FTP	75	Request: USER ind@psg420.com	
231 2019-06-14 04:52:15 10.6.13,102	216.55.163.106	FTP	73	Request: PASS (6r 6e#TfT1p	
235 2019-06-14 04:52:16 10.6.13.102	216.55.163.106	FTP	62	Request: TYPE I	
239 2019-06-14 04:52:16 10.6.13.102	216.55.163.106	FTP	60	Request: PASV	
246 2019-06-14 04:52:16 10.6.13.102	216.55.163.106	FTP	66	Request: SIZE q.exe	
250 2019-06-14 04:52:16 10.6.13.102	216.55.163.106	FTP	66	Request: RETR q.exe	
1185 2019-06-14 04:52:16 10.6.13.102	216.55.163.106	FTP	62	Request: TYPE I	
1109 2019-06-14 04:52:16 10.6.13.102	216.55.163.106	FTP	60	Request: PASV	
1116 2019-06-14 04:52:16 10.6.13.102	216.55.163.106	FTP	66	Request: SIZE w.exe	
1120 2019-06-14 04:52:16 10.6.13.102	216.55.163.106	FTP	66	Request: RETR w.exe	
1289 2019-06-14 04:52:17 10.6.13.102	216.55.163.106	FTP	62	Request: TYPE I	
1293 2019-06-14 04:52:17 10.6.13.102	216.55.163.106	FTP	60	Request: PASV	
					>
[Time since reference or first frame: I Frame Number: 227	7.222377000 seconds]				
[Time since reference or first frame: I Frame Number: 227 Frame Length: 75 bytes (600 bits) Capture Length: 75 bytes (600 bits) [Frame is ignored: False] [Frame is ignored: False] [Promotes: in frame: thetherbox: int	7.222377000 seconds]				
[Time Since reference or first frame: I Frame length: 75 bytes (600 bits) Capture length: 75 bytes (600 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: ethicthertype:]pit [Falselman, but here. True	7.222377000 seconds] cp:ftp]				
[Time Since reference or first frame: 1           Frame Number: 127           Prace Length: 75 bytes (606 bits)           Capture Length: 75 bytes (606 bits)           [Frame Is sarked: Faile]           [Frame Is arked: Faile]           [Frame Is	7.222377000 seconds] cp:ftp] 6 00 45 00 * 6 66 d0 37 = 0 * 3 05 50 18 - j 5 \$ 5 6 64 40 78 - 00 US 1 5g420.com	б. Е. . f 7 I. с Р R Indфр			

We know which of the files that have been retrieved and sent, we can use an ftp-data filter to analyze traffic from the FTP data channel.

extracting-objects-from-pcap-example-05.pcap				- ø ×
Ele Edit View Go Capture Analyze Statistics	Telephony Wireless I	ools Help		
ftp-data				
ko, ftp-data Source	Destination	Protocol Length Host	Info	
254 2019-06-14 04:52:16 216.55.163.106	10.6.13.102	FTP-DA_ 1328	FTP Data: 1274 bytes (PASV) (SIZE p.exe)	
256 2019-06-14 04:52:16 216.55.163.106	18.6.13.182	FTP-DA., 1328	FTP Data: 1274 bytes (PASV) (SITE p.exe)	
257 2019-06-14 04:52:16 216.55.163.106	18.6.13.182	FTP-DA., 1328	FTP Data: 1274 bytes (PASV) (SIJE g.exe)	
258 2019-06-14 04:52:16 216.55.163.106	10.6.13.102	FTP-DA_ 1328	FTP Data: 1274 bytes (PASV) (SIZE g.exe)	
259 2019-06-14 04:52:16 216.55.163.106	10.6.13.102	FTP-DA., 1328	FTP Data: 1274 bytes (PASV) (SIZE g.exe)	
261 2019-06-14 04:52:16 216.55.163.106	10.6.13.102	FTP-DA., 1328	FTP Data: 1274 bytes (PASV) (SIZE g.exe)	
263 2019-06-14 04:52:16 216.55.163.106	18.6.13.182	FTP-DA., 1328	FTP Data: 1274 bytes (PASV) (SIZE g.exe)	
264 2019-06-14 04:52:16 216.55.163.106	10.6.13.102	FTP-DA., 1328	FTP Data: 1274 bytes (PASV) (SIZE g.exe)	
268 2019-06-14 04:52:16 216.55.163.106	18,6,13,102	FTP-DA_ 1328	FTP Data: 1274 bytes (PASV) (SIZE p.exe)	
270 2019-06-14 04:52:16 216.55.163.106	10.6.13.102	FTP-DA., 2328	FTP Data: 1274 bytes (PASV) (SIZE g.exe)	
272 2019-06-14 04:52:16 216.55.163.106	10.6.13.102	FTP-DA_ 1328	FTP Data: 1274 bytes (PASV) (SIZE g.exe)	
273 2019-06-14 04:52:16 216.55.163.106	10.6.13.102	FTP-DA., 1328	FTP Data: 1274 bytes (PASV) (SIZE g.exe)	
( )				>
[The shift for this packet: 0.00000000 second [The shift from previous descendent [The shift from previous descendent from [The shift ofference of first frame: 12 Frame Langth: 1328 bytes (18034 bits) [Frame Langth: 1328 bytes (18034 bits)]	0 seconds] e: 0.002186000 second ne: 0.00000000 secon 7.688385000 seconds] cp:ftp-data]	is] ds]		
0000 00 00 02 1c 47 ae 20 e5 2a b6 93 f1 00	3 00 45 00 🔛 G	*····E·		
ad 66 c7 91 c9 36 cc 93 87 a6 9h 77 62	33 50 18 . F	white		
0030 fa fe a4 87 00 00 4d 5a 90 00 03 00 00	0 00 04 00 ·····NZ			
10-40 00 00 ff ff 00 00 b8 00 00 00 00 00 00	00 40 00	·········		
8550 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00			
NGO 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00			
0070 00 00 10 00 00 00 00 11 ba 00 00 b4 09	o cd 21 b8			
20 63 61 62 62 67 74 70 62 65 70 72 67 07	6e 20 69 cannot	he run 1		
6e 28 44 4f 53 28 6d 6f 64 65 2e 8d 8d	1 8a 24 88 n DOS mo	de \$-		
00110 00 00 00 00 00 00 3a ef 14 08 7e Se 7a	5b 7e 8e	· · ~ · z[~ ·		
18c0 7a 5b 7e 8e 7a 5b 38 df a5 5b 5f 8e 7a	a 5b 38 df z[-z[8	·[z[8-		
90:00 9b 5b 3b 8e 7a 5b 38 df 9a 5b a5 8e 7a	s 5b a3 71 [; z[8	[··=[·q		
b1 5b 73 8e 7a 5b 7e 8e 7b 5b eb 8e 7a	5b 73 dc [s-z[~	{[2[5		
90 50 /T 80 /# 50 73 dc 9a 5b 7f 8e 7a	a SD /3 dc [··z[s	1.213		III 15 Yasheva
FIP Data: Protocol			Fackets: 2963 * Displayed: 1595 (53.8%)	Profile: Defa

In Wireshark, we cannot use the feature Export Objects to export such objects. We may therefore follow the TCP stream for each from the data channels. To select one of the TCP segments, left-click on any of the lines ending with (SIZE q.exe) Then right-click to open menu and click Follow  $\rightarrow$  TCP stream



For getting SHA256 hash of these executable file use this command on terminal.

shasum -a 256 filename

000000000570d5480e67a8e670059523ccccccc680d54800e56a8e70059c3ccccccc680d54800e55 a8e07005953ccccccccf152424800a3001f400c3ccccccc333df41444001b0be814480045564395 A900a3F6144904745568041f15182480805465674395 6ff151ce048008bd085d2742c803a00750433c9eb188bca578d79018a014184c075f92bcf5f5152b904f0 Packet 254. 0 client pkts. 467 server pkts. 0 turns. Click to select. Entire conversation (672 kB) V Show and save data as Raw  $\sim$  Stream 2 🗘 Find: Find Next Filter Out This Stream Print Save as... Back Close Help

eg: shasum –a 256 q.exe

ca34b0926cdc3242bbfad1c4a0b42cc2750d90db9a272d92cfb6cb7034d2a3bd

Search on Virus Total with that file's hash.

Σ	ca34b0926cdc3242bbfa	d1c4a0b42cc2750d90db9a272d92cfb6cb7034d2a3bd		Q	Q	<u>^</u>	000	Sign in	
	47	① 47 engines detected this file		C* 858					
	Community Score	ca34b0926cdc3242bbfad1c4a0b42cc2750d90db9a272d92cfb6cb7034d2a3bd q.exe peexe	657 Size	657.00 KB 2020-02-08 19:39:55 UTC Size 4 months ago					
	DETECTION	DETAILS RELATIONS BEHAVIOR COMMUNITY							
	Acronis	① Suspicious	Ad-Aware	Trojan GenericKD 41370195					
	AhnLab-V3	Malware/Win32 Generic C2879518	Alibaba	() TrojanPSW:Win32/Tercen.057a7c	20				
	ALYac	() Trojan Agent.gen	Antiy-AVL	() Trojan/Win32.ParasiteStealer.a					
	SecureAge APEX	① Malicious	Arcabit	() Trojan Generic D2774253					
	Avast	() Win32:Trojan-gen	AVG	() Win32:Trojan-gen					
	BitDefender	() Trojan GenericKD.41370195	BitDefenderTheta	() Gen:NN.ZexaF.34084.PqW@aWI	СКср				
	CAT-QuickHeal	() Trojan Agent	Comodo	() Malware@#xm8rzc4z5mus					
	CrowdStrike Falcon	() Win/malicious_confidence_80% (W)	Cylance	() Unsafe					
	DrWeb	① Trojan MulDrop9.5080	Emsisoft	() Trojan GenericKD 41370195 (B)					
	Endgame	① Malicious (high Confidence)	eScan	Trojan.GenericKD.41370195					

When exporting the HTML files sent back to the FTP server from the infected Windows host we need to search more precisely. Why? For what? Because each time the same name for the file is used. Use filter ftp.request.command, select, and scroll to the end. We will see the same file name used to store stolen data (STOR) as an HTML to the FTP server

ftp.request.command						X
o. Time	Source	Destination	Protocol	Length Host	Info	
2855 2019-06-14 0	4:52:54 10.6.13.102	216.55.163.106	FTP	62	Request: TYPE A	
2859 2019-06-14 @	4:52:54 10.6.13.102	216.55.163.106	FTP	60	Request: PASV	
2866 2019-06-14 @	04:52:54 10.6.13.102	216.55.163.106	FTP	81	Request: STOR 1052543721_logs.html	
2882 2019-06-14 0	4:53:12 10.6.13.102	216.55.163.106	FTP	62	Request: TYPE A	
2886 2019-06-14 0	4:53:12 10.6.13.102	216.55.163.106	FTP	60	Request: PASV	
2893 2019-06-14 0	4:53:12 10.6. <mark>1</mark> 3.102	216.55.163.106	FTP	81	Request: STOR 1052543721_logs.html	
2909 2019-06-14 0	4:53:30 10.6.13.102	216.55.163.106	FTP	62	Request: TYPE A	
2913 2019-06-14 0	4:53:30 10.6.13.102	216.55.163.106	FTP	60	Request: PASV	
2920 2019-06-14 0	4:53:30 10.6.13.102	216.55.163.106	FTP	81	Request: STOR 1052543721_logs.html	
2936 2019-06-14 0	4:53:48 10.6.13.102	216.55.163.106	FTP	62	Request: TYPE A	
2940 2019-06-14 0	04:53: <mark>4</mark> 8 10.6.13.102	216.55.163.106	FTP	60	Request: PASV	
2947 2019-06-14 @	4:53:48 10.6.13.102	216.55.163.106	FTP	81	Request: STOR 1052543721_logs.html	

Use the filter ftp-data.command contains .html to see the associated files sent over the ftp data channel.

<pre>extracting-objects-from-pcap-example-05.pca</pre>	p			- 0 ×
<u>File Edit View Go Capture Analyze S</u>	tatistics Telephony <u>W</u> ireless <u>T</u> oo	ls <u>H</u> elp		
	2 î 🔬 <b>- 📃 e</b> e e e i	1		
() Tup-data.command.contains.num	18.16.5	622.2 g 15 //2/11a /		
No. Time Source	Destination	Protocol Length Host	Info	
2843 2019-06-14 04:52:36 10.6.13.1	02 216.55.163.106	FTP-DA 1514	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)	
2844 2019-06-14 04:52:36 10.6.13.1	02 216.55.163.106	FTP-DA 1514	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)	
2847 2019-06-14 04:52:36 10.6.13.1	02 216.55.163.106	FTP-DA 885	FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)	
2870 2019-06-14 04:52:54 10.6.13.1	02 216.55.163.106	FTP-DA 1514	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)	
2871 2019-06-14 04:52:54 10.6.13.1	02 216.55.163.106	FTP-DA 1514	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)	
2874 2019-06-14 04:52:54 10.6.13.1	02 216.55.163.106	FTP-DA 885	FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)	
2897 2019-06-14 04:53:12 10.6.13.1	02 216.55.163.106	FTP-DA 1514	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)	
2898 2019-06-14 04:53:12 10.6.13.1	02 216.55.163.106	FTP-DA 1514	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)	
2901 2019-06-14 04:53:12 10.6.13.1	02 216.55.163.106	FTP-DA 885	FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)	
2924 2019-06-14 04:53:30 10.6.13.1	02 216.55.163.106	FTP-DA 1514	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)	
2925 2019-06-14 04:53:30 10.6.13.1	02 216.55.163.106	FTP-DA 1514	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)	
2928 2019-06-14 04:53:30 10.6.13.1	02 216.55.163.106	FTP-DA 885	FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)	
<				>
Arrival Time: Jun 14, 2019 04:52 [Time shift for this packet: 0.06 Epoch Time: 1560460156.774184000 [Time delta from previous captur- [Time delta from previous display [Time since reference or first fi Frame Number: 2043 Frame Length: 1514 bytes (12112 Capture Length: 1514 bytes (12112 [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: teh:ethertyy [Colorean Pulo Numa, ICO]	<pre>36.774184000 India Standard 1 30000000 seconds] seconds seconds d frame: 0.000756000 seconds rame: 38.125866000 seconds] sits) 2 bits) e:ip:tcp:ftp-data:data-text</pre>	lime ] ] lines]		
0000 20 e5 2a b6 93 f1 00 08 02 1c 4	17 ae 08 00 45 00 ·*····	··G···E·		,
0010 05 dc 05 a8 40 00 80 06 5c 66 0	a 06 0d 66 d8 37 ····@····	ff.7		
0020 a3 6a c0 3d cb ea f0 c8 f5 32 1	11 52 56 c0 50 10 ·j·=····	2 · RV · P ·		
9030 ta t0 c2 99 00 00 3c 63 65 6e 7	74 65 72 3e 0d 0a ····· <c e<="" td=""><td>enter&gt;··</td><td></td><td></td></c>	enter>··		
8656 75 74 6c 6f 6f 6b 20 33 32 20 6	52 69 74 3c 2f 62 utlock 3	bitc/b		
8868 3e 8d 8a 3c 2f 63 65 6e 74 65	72 3e 3c 63 65 6e >	rer> <cen< td=""><td></td><td></td></cen<>		
0070 74 65 72 3e 0d 0a 0d 0a 3c 62	3e 53 75 62 4b 65 ter>	cb>SubKe		
0080 79 20 53 6f 66 74 77 61 72 65 5	5c 4d 69 63 72 6f y Softwa r	re\Micro		
0090 73 6f 66 74 5c 4f 66 66 69 63 6	55 5c 31 36 2e 30 soft\Off 3	ice\16.0		
00a0 5c 4f 75 74 6c 6f 6f 6b 5c 50 7	72 6f 66 69 6c 65 \Outlook \	Profile		
00b0 73 5c 4f 75 74 6c 6f 6f 6b 5c	39 33 37 35 43 46 s\Outloo H	<\9375CF		
00c0 46 30 34 31 33 31 31 31 64 33 4	42 38 38 41 30 30 F0413111 d	13688A00		
0000 01 30 34 42 32 41 35 36 37 36 2	20 4e of /4 20 4b 10482A66			
0000 01 73 00 04 20 30 21 02 30 00 0	72 3e 0d 0a 0d 0a tervicen 1	PP3++++		
G Z Frame Number (frame number)			Barkate: 2962 - Dimburd: 15 (0.5%)	Profile: Defini

The destination port changes to the FTP server each time the file (STOR) is stored. TCP port 52202 is used for the first time. TCP port 57791 is for the second time. Has TCP port 55045 for the third time. It has 57203 for the fourth time. And 61099 the fifth time.

ftp-data.command conta	ains .html						
lo. Time	Source	Destination	Protocol	Length Host	Source Port	Destination Port	Info
2843 2019-06-14	04:52:36 10.6.13.102	216.55.163.106	FTP-DA	1514	49213	52202	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2844 2019-06-14	04:52:36 10.6.13.102	216.55.163.106	FTP-DA.,	1514	49213	52202	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2847 2019-06-14	04:52:36 10.6.13.102	216.55.163.106	FTP-DA.,	885	49213	52202	FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
2897 2019-06-14	04:53:12 10.6.13.102	216.55.163.106	FTP-DA	1514	49215	55045	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2898 2019-06-14	04:53:12 10.6.13.102	216.55.163.106	FTP-DA	1514	49215	55045	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2901 2019-06-14	04:53:12 10.6.13.102	216.55.163.106	FTP-DA	885	49215	55045	FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
2924 2019-06-14	04:53:30 10.6.13.102	216.55.163.106	FTP-DA.	1514	49216	57203	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2925 2019-06-14	04:53:30 10.6.13.102	216.55.163.106	FTP-DA	1514	49216	57203	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2928 2019-06-14	04:53:30 10.6.13.102	216.55.163.106	FTP-DA	885	49216	57203	FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
2870 2019-06-14	04:52:54 10.6.13.102	216.55.163.106	FTP-DA	1514	49214	57791	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2871 2019-06-14	04:52:54 10.6.13.102	216.55.163.106	FTP-DA.,	1514	49214	57791	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2874 2019-06-14	04:52:54 10.6.13.102	216.55.163.106	FTP-DA	885	49214	57791	FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
2951 2019-06-14	04:53:48 10.6.13.102	216.55.163.106	FTP-DA	1514	49217	61099	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2952 2019-06-14	04:53:48 10.6.13.102	216.55.163.106	FTP-DA	1514	49217	61099	FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
2955 2019-06-14	04:53:48 10.6.13.102	216.55.163.106	FTP-DA	885	49217	61099	FTP Data: 831 bytes (PASV) (STOR 1052543721 logs.html)

We 're using the same process as we used to. Instead of concentrating on the file names, focus on the TCP ports. To any TCP line use port 52202 to follow the TCP stream. Change "Show and save data as" to "Raw" in the TCP stream window, then save that file.. Do the same in case of HTML file over TCP port 57791.

# Analyzing Torrent Traffic

Let us see how to analyze a torrent traffic and gather information. Before starting I'll explain what is BitTorrent?

BitTorrent is a file-distribution protocol. It identifies URL content and is designed to seamlessly integrate with the web. Its advantage over plain HTTP is that when multiple downloads of the same file occur simultaneously, the downloaders upload to each other, allowing the file source to support very large numbers of downloaders with only a modest increase in their load.

These entities comprise a distribution of BitTorrent files:

- A web server
- A static 'metainfo' file
- A Tracker
- An 'original' downloader
- End user's web browsers
- End user's downloaders

It is a great ability to either identify malicious activity or someone using your network for the wrong reasons (even if it is harmless) to be able to track BitTorrent activity Actually, In fact, if you have people who use it to download things like the Linux distribution that was seceded, you might want to allow BitTorrent on your network. If it means a user downloads copyrighted material or malware, you might not want to allow that either.

Time         Source         Destination         Protocol         Longh         Heat         Source Part         Destination Flort         Joint           151         2018-07.15         09.454.21         0.0.0.0.2         10.0.0.0         10.0.0.2 </th <th>Apply a display filter &lt;&lt; Ctrl-/&gt;</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	Apply a display filter << Ctrl-/>							
151 2018-07.15 0014543 10.0.0.2       10.0.0.2	Time Source	Destination	Protocol	Length Host	Source Port	Destination Port	Info	1
B       2018-07.19       90145041       Du0e       1355       389       4076       searchestnry(4) "40007"       searchestnry(4) success [1 results archestnry(3) "4007"       searchestnry(3) '4007"       searchestnry(	151 2018-07-15 09:45:43 10.0.0.2	10.0.0.201	CLDAP	246			<pre>searchResEntry(9) "<root>" searchResDone(9) success [1 re</root></pre>	su
43 2018-07.15 001-65.23 10.0.0.2       10.0.0.23	89 2018-07-15 09:45:43 10.0.0.2	10.0.0.201	I DAP	1355	389	49676	searchResEntry(4) " <root>"   searchResDone(4) success [1</root>	2
41 2018-07.15 09/45/3 10.0.0.2       10.0.0.201       CLDP 244       searchestatry(2) *6007* searchestone(2) success [1 results 2018-07.15 09/45/3 10.0.0.2       10.0.0.201       CLDP 244       searchestatry(2) *6007* searchestone(2) success [1 results 2018-07.15 09/45/3 10.0.0.2       10.0.0.201       CLDP 244       searchestatry(10) *6007* searchestone(1) success [1 results 2018-07.15 09/45/3 10.0.0.2       10.0.0.201       CLDP 244       searchestatry(10) *6007* searchestone(1) success [1 results 2018-07.15 09/45/3 10.0.0.2       10.0.0.201       CLDP 244       searchestatry(10) *6007* searchestone(1) success [1 results 2018-07.15 09/45/3 10.0.0.2       10.0.0.201       CLDP 244       searchestatry(10) *6007* searchestone(1) success [1 results 2018-07.15 09/45/3 10.0.0.2       10.0.0.201 <td>43 2018-07-15 09:45:43 10.0.0.2</td> <td>10.0.0.201</td> <td>CLDAP</td> <td>244</td> <td></td> <td></td> <td>searchResEntry(3) "<root>" searchResDone(3) success [1 re</root></td> <td></td>	43 2018-07-15 09:45:43 10.0.0.2	10.0.0.201	CLDAP	244			searchResEntry(3) " <root>" searchResDone(3) success [1 re</root>	
22 2010-07-19 09/354 20 0.0.0.2       10.0.0.201       LDAP       1335       389       4967       search8eshtty(1) *(0007*   search8esbne(2) success [ 1 m]         1389 2010-07-15 09/355 21 0.0.0.2       10.0.0.201       CLDAP       244       search8eshtty(1) *(0007* search8esbne(1) success [ 1 m]         1389 2010-07-15 09/355 21 0.0.0.2       10.0.0.201       CLDAP       244       search8eshtty(1) *(0007* search8esbne(1) success [ 1 m]         1379 2010-07-15 09/355 21 0.0.0.2       10.0.0.201       CLDAP       244       search8eshtty(1) *(0007* search8esbne(1) success [ 1 m]         246 2010-07-15 09/355 21 0.0.0.2       10.0.0.201       CLDAP       244       search8eshtty(1) *(0007* search8esbne(1) success [ 1 m]         246 2010-07-15 09/355 20 0.0.0.2       10.0.0.201       CLDAP       246       search8eshtty(1) *(0007* search8esbne(1) success [ 1 m]         246 2010-07-15 09/355 20 0.0.0.2       10.0.0.201       CLDAP       246       search8eshtty(1) *(0007* search8esbne(1) success [ 1 m]         246 2010-07-15 09/355 20 0.0.0.2       10.0.0.201       LDAP       246       search8eshtty(1) *(0007* search8esbne(1) success [ 1 m]         247 2010-07-15 09/355 20 0.0.0.2       10.0.0.2       10.0.0.2       10.0.0.2       10.0.0.2         248 2010-07-15 09/355 20 0.0.0.2       10.0.0.2       10.0.0.2       10.0.0.2       10.0.0.2         249 2010-07-15	41 2018-07-15 09:45:43 10.0.0.2	10.0.0.201	CLDAP	244			searchResEntry(2) " <root>" searchResDone(2) success [1 re</root>	su
3999 201-07-16 99 4753 20 0.0.0.2         10.0.0.201         CLDAP         244         search8estntry(10 '*G007'' search8esDon(17) success [1 net 144 2016-07-15 99 4555 20 0.0.0.2         10.0.0.201         CLDAP         244         search8estntry(15) '*G007'' search8esDon(15) success [1 net 347 2016-07-15 99 4555 20 0.0.0.2         10.0.0.201         CLDAP         244         search8estntry(15) '*G007'' search8esDon(15) success [1 net 320 2016-07-15 99 4555 20 0.0.0.2         10.0.0.201         CLDAP         244         search8estntry(10 '*G007'' search8esDon(15) success [1 net 320 2016-07-15 99 4555 20 0.0.0.2         10.0.0.201         CLDAP         244         search8estntry(10 '*G007'' search8esDon(15) success [1 net 320 2016-07-15 99 4555 20 0.0.0.2         10.0.0.201	22 2018-07-15 09:45:42 10.0.0.2	10.0.0.201	LDAP	1355	389	49667	searchResEntry(2) " <root>"   searchResDone(2) success [1</root>	r
1469 2010-07-15 09:455 10:0.0.2       10.0.0.201       CLDAP 244       searchessThr(15) "(ROOT)" searchesDone(15) success [1 ref         137 2010-07.15 09:454 10:0.0.2       10.0.0.201       CLDAP 244       searchessThr(15) "(ROOT)" searchesDone(15) success [1 ref         137 2010-07.15 09:454 10:0.0.2       10.0.0.201       CLDAP 244       searchessThr(11) "(ROOT)" searchesDone(14) success [1 ref         146 2010-07.15 09:454 10:0.0.2       10.0.0.201       CLDAP 246       searchesSThr(11) "(ROOT)" searchesDone(14) success [1 ref         150 2010-07.15 09:454 10:0.0.2       10.0.0.201       CLDAP 246       searchesSThr(11) "(ROOT)" searchesDone(14) success [1 ref         150 2010-07.15 09:454 10:0.0.2       10.0.0.201       CLDAP 246       searchesSThr(11) "(ROOT)" searchesDone(15) success [1 ref         150 2010-07.15 09:454 10:0.0.2       10.0.0.201       LDAP 1355       389 40976       searchesSThr(11) "(ROOT)" searchesDone(15) success [1 ref         150 2010-07.15 09:454 10:0.0.2       10.0.0.201       LDAP 1355       389 40970       searchesSThr(11) "(ROOT)" searchesDone(1) success [1 ref         150 2010-07.15 09:454 10:0.0.201       10.0.0.201       LDAP 1355       389 40970       searchesSThr(10) "(ROOT)" searchesDone(1) success [1 ref         150 2010-07.15 09:454 10:0.0.201       10.0.0.201       10.0.0.20       LDAP 1355       389 40970       searchesSThr(10) "(ROOT)" SearchesDone(1) success [1 ref <t< td=""><td>5390 2018-07-15 09:47:53 10.0.0.2</td><td>10.0.0.201</td><td>CLDAP</td><td>244</td><td></td><td></td><td>searchResEntry(17) "<root>" searchResDone(17) success [1</root></td><td>e</td></t<>	5390 2018-07-15 09:47:53 10.0.0.2	10.0.0.201	CLDAP	244			searchResEntry(17) " <root>" searchResDone(17) success [1</root>	e
144 201-07-15 09:45:12 10.0.0.2       10.0.0.201       CLDAP 244       searchessTrt(1) "(ROOT)" searchesDone(1) success [1 reginantes]         268 201-07-15 09:45:43 10.0.0.2       10.0.0.201       CLDAP 244       searchessTrt(1) "(ROOT)" searchesDone(1) success [1 reginantes]         268 201-07-15 09:45:43 10.0.0.2       10.0.0.201       CLDAP 246       searchessTrt(1) "(ROOT)" searchesDone(1) success [1 reginantes]         164 2010-07-15 09:45:43 10.0.0.2       10.0.0.201       CLDAP 240       searchessTrt(1) "(ROOT)" searchesDone(1) success [1 reginantes]         162 2010-07-15 09:45:43 10.0.0.2       10.0.0.201       CLDAP 240       searchessTrt(1) "(ROOT)" searchesDone(1) success [1 reginantes]         162 2010-07-15 09:45:43 10.0.0.2       10.0.0.201       LDAP 1355       309 4970       searchessTrt(1) "(ROOT)" searchesDone(1) success [4 reginantes]         163 2010-07-15 09:45:43 10.0.0.2       10.0.0.201       LDAP 1355       309 49701       searchessTrt(1) "(ROOT)" searchesDone(1) success [4 reginantes]         177 2010-07-15 09:45:43 10.0.0.2       10.0.0.2       CLDAP 245       searchesTrt(1) "(ROOT)" searchesDone(1) success [3 reginantes]       searchesTrt(1) "(ROOT)" searchesDone(1) success [4 reginantes]         178 2010-07-15 09:45:43 10.0.0.2       10.0.0.2       LDAP 1355       309 49701       searchesTrt(1) "(ROOT)" searchesDone(1) success [3 reginantes]         174 2010-07-15 09:45:43 10.0.0.2       LDAP 1355       309 49701       s	1496 2018-07-15 09:45:53 10.0.0.2	10.0.0.201	CLDAP	244			searchResEntry(16) " <root>" searchResDone(16) success [1</root>	e
372 2018-07-15 09:454 310.0.0.2       10.0.0.201       CLDAP 244       searchesEntry(1) "(KODT)" searchesDone(1) success [1 red)         262 2018-07-15 09:454 310.0.0.2       10.0.0.201       CLDAP 246       searchesEntry(1) "(KODT)" searchesDone(1) success [1 red)         39 2018-07-15 09:454 310.0.0.2       10.0.0.201       CLDAP 246       searchesEntry(1) "(KODT)" searchesDone(1) success [1 red)         10 2018-07-15 09:454 310.0.0.2       10.0.0.201       CLDAP 244       searchesEntry(1) "(KODT)" searchesDone(1) success [1 red)         10 2018-07-15 09:454 210.0.0.2       10.0.0.201       LDAP 1355       389 4073       searchesEntry(1) "(KODT)" searchesDone(1) success [1 red)         11 20 2018-07-15 09:454 210.0.0.2       10.0.0.201       LDAP 1355       389 4073       searchesEntry(1) "(KODT)" searchesDone(1) success [4 r)         12 20 2018-07-15 09:454 210.0.0.2       10.0.0.201       LDAP 1355       389 4073       searchesEntry(1) "(KODT)" searchesDone(1) success [4 r)         12 20 20 30-715 09:454 210.0.0.2       10.0.0.201       LDAP 1355       389 4073       searchesEntry(1) "(KODT)" searchesDone(1) success [4 r)         12 20 20 30-715 09:454 210.0.0.2       10.0.0.201       LDAP 1355       389 4073       searchesEntry(1) "(KODT)" searchesDone(1) success [4 r)         12 20 20 30-715 09:454 210.0.0.201       10.0.0.201       LDAP 1355       389 4073       searchesEntry(1) "(KODT)" searchesDone(1) success [4 r)	1494 2018-07-15 09:45:52 10.0.0.2	10.0.0.201	CLDAP	244			searchResEntry(15) " <root>" searchResDone(15) success [1</root>	e
202 201-07-15 09:45:43 10.0.0.2       10.0.0.201       CLDAP 246       searchesEntry(1) "(ROOT)" searchesDone(1) success [1 regines to the searchesDone(1) succes [1	537 2018-07-15 09:45:45 10.0.0.2	10.0.0.201	CLDAP	244			searchResEntry(14) " <root>" searchResDone(14) success [1</root>	e
242 201-07-15 09:45:41 10.0.0.2       10.0.0.201       CLDAP 246       searchestmr(1) '(x007)' searchestme(1) success [1 rew         15 2010-07-15 09:45:41 10.0.0.2       10.0.0.201       CLDAP 244       searchestmr(1) '(x007)' sea	260 2018-07-15 09:45:43 10.0.0.2	10.0.0.201	CLDAP	244			searchResEntry(11) " <root>" searchResDone(11) success [1</root>	'e
39 2018-07-15 09:45:43 10.0.0.2       10.0.0.201       CLDAP 200       search6estmr(1) 'co007' search6estmr(2) 'co00	246 2018-07-15 09:45:43 10.0.0.2	10.0.0.201	CLDAP	246			searchResEntry(10) " <root>" searchResDone(10) success [1</root>	e
11 2018-07-15 09:45:42 10.0.0.2       10.0.0.201       CLDAP       244       search@cstmrt(1) ' <moort' 'smoort'="" 'smoort'<="" carch@cstmrt(1)="" is="" td=""><td>39 2018-07-15 09:45:43 10.0.0.2</td><td>10.0.0.201</td><td>CLDAP</td><td>260</td><td></td><td></td><td><pre>searchResEntry(1) "<root>" searchResDone(1) success [1 re</root></pre></td><td>su</td></moort'>	39 2018-07-15 09:45:43 10.0.0.2	10.0.0.201	CLDAP	260			<pre>searchResEntry(1) "<root>" searchResDone(1) success [1 re</root></pre>	su
5462 2018-07-15 99147,53 10.0.0.2       10.0.0.201       LDAP       1355       389       49876       scarchestmetry(1) *c007*       scarchestmetry(1) *c	16 2018-07-15 09:45:42 10.0.0.2	10.0.0.201	CLDAP	244			<pre>searchResEntry(1) "<root>" searchResDone(1) success [1 re</root></pre>	su
1362 2018-07-15 09:45:310.0.0.2       10.0.0.201       LDAP       1355       389       49739       searchResThr(1) 'sc007*	5462 2018-07-15 09:47:53 10.0.0.2	10.0.0.201	LDAP	1355	389	49876	<pre>searchResEntry(1) "<root>"   searchResDone(1) success [4</root></pre>	r
372 2018-07-15 09:45:410.0.0.2       10.0.0.201       LDAP       1355       389       49701       searchestmet(1) (1) *(007)*       searchestmet(1) (1) *(007)*       searchestmet(1) *(007)	1502 2018-07-15 09:45:53 10.0.0.2	10.0.0.201	LDAP	1355	389	49739	searchResEntry(1) " <root>"   searchResDone(1) success [4</root>	r
349 2018-07-15 09:45:41 10.0.0.201       100.0.0.201       LDAP       1355       389       49693       searchResEntr(1)       *COOT> <sup>5</sup> searchResUte(3)       *COOT> <sup>5</sup> baseDip(1)       *COOT> <sup>5</sup> baseDip(1)       searchResUte(3)       *COOT> <sup>5</sup> baseDip(1)       *Coot       <	578 2018-07-15 09:45:45 10.0.0.2	10.0.0.201	LDAP	1355	389	49701	searchResEntry(1) " <root>"   searchResDone(1) success [4</root>	r
149 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       245       searchRequest(9) "KOOT>" baseObject         7 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       340       49076 399       searchRequest(9) "KOOT>" baseObject         7 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       310       searchRequest(3) "KOOT>" baseObject         7 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       310       searchRequest(3) "KOOT>" baseObject         7 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       310       searchRequest(3) "KOOT>" baseObject         7 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       310       searchRequest(3) "KOOT>" baseObject         7 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       310       searchRequest(3) "KOOT>" baseObject         7 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       310       searchRequest(3) "KOOT>" baseObject         7 2018-07-15 09:45:43 10.0.0.201       10.0.0.2       CLDAP       310       searchRequest(3) "KOOT>" baseObject         8 2019-07-15 09:45:43 10.0.0.201       10.0.0.2       10.0.0.2       10.0.0.2       10.0.0.2         9 7 5ff 7f 6f 40.40 40 45 15 fr 20 70 10 10 10 10 10 10 5 60 20 00 00 00 00 00 00 10 10 10 10 10 10 5 60 20 00 00 00 00 00 10 10 10 10 10 10 10 10	349 2018-07-15 09:45:44 10.0.0.2	10.0.0.201	LDAP	1355	389	49693	<pre>searchResEntry(1) "<root>"   searchResDone(1) success [3</root></pre>	r i
87 2018-07-15 89:45:43 10.0.0.201       10.0.0.22       LDAP       404       49676       389       searchRequest(4) ":ROOT>" baseDbject         42 2018-07-15 89:45:43 10.0.0.201       10.0.0.22       CLDAP       310       searchRequest(4) ":ROOT>" baseDbject         42 2018-07-15 89:45:43 10.0.0.201       10.0.0.21       10.0.0.2       CLDAP       310       searchRequest(4) ":ROOT>" baseDbject         *       *       *       *       *       *       *       *         *	149 2018-07-15 09:45:43 10.0.0.2	01 10.0.0.2	CLDAP	245			searchRequest(9) " <root>" baseObject</root>	
4 2 2018-07-15 99:45:43 10.0.0.201 10.0.0.21 10.0.0.2 CLDP 310 searchRequest(3) "GROTA" baseObject > From 1: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) Ethernet II, Src: Not. 18:66:c8 (003:66:17):18:66:c8 (003:66:18):19:67 (103:67):18:66:c8 (003:66:18):19:67 (103:67):18:66:c8 (003:66:18):19:67 (103:67):18:66:c8 (003:66:18):19:67 (103:67):18:66:c8 (003:66:18):19:67 (103:67):18:66:c8 (003:66:18):19:67 (103:67):18:66:c8 (003:66:18):19:67 (103:67):19:67 (103:	87 2018-07-15 09:45:43 10.0.0.2	01 10.0.0.2	LDAP	404	49676	389	searchRequest(4) " <root>" baseObject</root>	
Frame 1: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits)         Ehrment II, Sr: Msl_186:66:04 (000:1617:186:630), bots madcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	42 2018-07-15 09:45:43 10.0.0.2	01 10.0.0.2	CLDAP	310			searchRequest(3) " <root>" baseObject</root>	
Frame 1: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits)         Ethernet II, Src: MsL18:66:68 (00:166:17):18:66:68), DSL: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:			C1040				In LIAL BURGET BIL OLD I	
0       ff	thernet II, Src: Nsi_18:66:c8 (00 nternet Protocol Version 4, Src: User Datagram Protocol, Src Port: Jynamic Host Configuration Protoco	115), 579 bytes Captured (365 116:17:18:66:c8), Dst: Broadc 0.0.0.0, Dst: 255.255.255.255 68, Dst Port: 67 1 (Request)	ast (ff:ff:1	ff:ff:ff:ff)				
00       00 <td< td=""><td>6 ff ff ff ff ff ff 00 16 17 18 0 01 6d 4b 36 00 00 80 11 ee 4a</td><td>66 c8 08 00 45 00 00 00 00 00 ff ff mK6</td><td>···f···E·</td><td></td><td></td><td></td><td></td><td></td></td<>	6 ff ff ff ff ff ff 00 16 17 18 0 01 6d 4b 36 00 00 80 11 ee 4a	66 c8 08 00 45 00 00 00 00 00 ff ff mK6	···f···E·					
	20 TT TT 00 44 00 43 01 59 TE 2/	01 01 05 00 20 54 ····D·C·Y	· · · · · a					
00         00<		55 c2 00 00 00 00 00 00						
10       10 <td< td=""><td>50 00 00 00 00 00 00 00 00 00 00 00 00</td><td>00 00 00 00 00 00</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	50 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00						
10       00 <td< td=""><td>00 00 00 00 00 00 00 00 00 00 00</td><td>00 00 00 00 00 00</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00						
	00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00						
00       00 <td< td=""><td>00 00 00 00 00 00 00 00 00 00 00</td><td>00 00 00 00 00 00 00 00</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00						
0         0	00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00						
	0 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00						
e 80 66 69 69 69 69 69 69 69 69 69 69 69 69		00 00 00 00 00 00 00 00 00 00 00 00 00						
	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00						

158

Use filter **bittorrent** for filtering BitTorrent requests.

attorrent								
Time	Source	Destination	Protocol	Length Host	Source Port	Destination Port	Info	
4520 2018-07-15 09:47:37	10.0.0.201	62.210.200.57	BitTorrent	122	49846	55020	Handshake	
4542 2018-07-15 09:47:37	62.210.200.57	10.0.201	BitTorrent	242	55020	49846	Handshake Extended	
4543 2018-07-15 09:47:37	10.0.201	62.210.200.57	BitTorrent	766	49846	55020	Extended Bitfield, Len:@	x1cb Port
4549 2018-07-15 09:47:37	10.0.201	61.245.142.233	BitTorrent	122	49845	51413	Handshake	
4581 2018-07-15 09:47:37	62.210.200.57	10.0.201	BitTorrent	513	55020	49846	Bitfield, Len:0x1cb	
4684 2018-07-15 09:47:37	61.245.142.233	10.0.201	BitTorrent	122	51413	49845	Handshake	
4685 2018-07-15 09:47:37	10.0.201	61.245.142.233	BitTorrent	397	49845	51413	Extended Have All Allow	ed Fast, Pi
4701 2018-07-15 09:47:38	10.0.201	82.102.24.163	BitTorrent	122	49851	42232	Handshake	
4710 2018-07-15 09:47:38	82.102.24.163	10.0.0.201	BitTorrent	242	42232	49851	Handshake Extended	
4711 2018-07-15 09:47:38	10.0.0.201	82.102.24.163	BitTorrent	766	49851	42232	Extended Bitfield, Len:0	x1cb Port
4726 2018-07-15 09:47:38	61.245.142.233	10.0.201	BitTorrent	361	51413	49845	Extended Have All Port	Extended
4735 2018-07-15 09:47:38	82.102.24.163	10.0.201	BitTorrent	513	42232	49851	Bitfield, Len:0x1cb	
4754 2018-07-15 09:47:39	10.0.201	23.82.53.139	BitTorrent	122	49853	49544	Handshake	
4760 2018-07-15 09:47:39	23.82.53.139	10.0.201	BitTorrent	242	49544	49853	Handshake Extended	
4761 2018-07-15 09:47:39	10.0.201	23.82.53.139	BitTorrent	764	49853	49544	Extended Bitfield, Len:0	x1cb Port
4768 2018-07-15 09:47:39	23.82.53.139	10.0.201	BitTorrent	513	49544	49853	Bitfield, Len:0x1cb	
4789 2018-07-15 09:47:40	10.0.201	96.237.60.19	BitTorrent	122	49854	51413	Handshake	
4815 2018-07-15 09:47:41	96.237.60.19	10.0.201	BitTorrent	122	51413	49854	Handshake	
4816 2018-07-15 09:47:41	10.0.201	96.237.60.19	BitTorrent	395	49854	51413	Extended Have All Allow	ed Fast, Pi
4818 2018-07-15 09:47:41	96.237.60.19	10.0.201	BitTorrent	197	51413	49854	Extended Have All Port	
				***				3
thernet II, Src: Msi_18:66:c8 nternet Protocol Version 4, Sr ransmission Control Protocol, MitTorrent	(00:16:17:18:66:c8), Dst c: 10.0.0.201, Dst: 62.2 Src Port: 49846, Dst Por	t: Cisco_27:al:3e (00 210.200.57 rt: 55020, Seq: 1, Ack	:09:b7:27:a1:3e) k: 1, Len: 68					

We want to know which file is downloaded, use this filter:

http.request.uri contains .torrent

It means filter all urls with .torrent files.

Eile	2018-07-15-traffic-analysis-exe <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> aptur	rcise.pcap e <u>A</u> nalyze <u>S</u> tatistics Telephon <u>y</u>	<u>Wireless Tools H</u> elp		-	ð	×
4	= 🦽 🛛 📙 🖻 🗙 🖻	۹ 👄 🕾 Ŧ 🛓 📃 📃	Q Q Q II				
	http.request.uri contains .torrent					$\times$	* +
	Protocol	Length Host	Source Port Destination Port	Info			
4	HTTP	589 www.publicdomaintorren	ts.com 49834 80	GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1			
<							>
-	0 0000 0000 0000	Fragment offset: 0					^
	Time to live: 128						
	Protocol: TCP (6)						
	Header checksum: 0x00	39 [validation disabled]					
	[Header checksum stat	tus: Unverified]					
	300/02. 10.0.0.201						~
001 002 002 002 002 002 002 002 002 002	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	0         6         6         29         00 <td><pre>// vig - 9 // vig - 9 // vig - 20 // vig - 20 //</pre></td> <td></td> <td></td> <td></td> <td></td>	<pre>// vig - 9 // vig - 9 // vig - 20 // vig - 20 //</pre>				
0	7 Source (p.src), 4 bytes		Carro Contra de	Parkets: 16358 • Displayed: 1 (0,0%)	1	Profile	∨ Default
							and a state of the

#### Now Right Click on that and **Follow** → **TCP Stream**

<pre>type=torrent&amp;file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1 Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Accept-Language: en-US Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Upgrade-Insecure-Requests: 1 Accept-Encoding: gzip, deflate Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive</pre>
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Accept-Language: en-US Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Upgrade-Insecure-Requests: 1 Accept-Encoding: gzip, deflate Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Accept-Language: en-US Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Upgrade-Insecure-Requests: 1 Accept-Encoding: gzip, deflate Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
<pre>Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Accept-Language: en-US Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Upgrade-Insecure-Requests: 1 Accept-Encoding: gzip, deflate Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive</pre>
Accept-Language: en-US Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Upgrade-Insecure-Requests: 1 Accept-Encoding: gzip, deflate Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Upgrade-Insecure-Requests: 1 Accept-Encoding: gzip, deflate Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
<pre>Upgrade-Insecure-Requests: 1 Accept-Encoding: gzip, deflate Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive</pre>
Accept-Encoding: gzip, deflate Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Host: www.publicdomaintorrents.com Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Connection: Keep-Alive HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
HTTP/1.1 200 OK Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Date: Sun, 15 Jul 2018 04:17:27 GMT Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Server: Apache Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent" Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/ Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/x-bittorrent
204c
d8:announce53:http://files.publicdomaintorrents.com/bt/announce.php13:creation
datei1129376933e4:infod6:lengthi105383936e4:name40:Betty Boop Rhythm on the Reservati
on.avi12:piece lengthi262144e6:pieces8060:6jf.zR
{3Z&=.~>:[WK.Lw'v.c/.m.S.xB.Z
acket 4268. 1 <u>client</u> pkt, 7 server pkts, 1 turn, Click to select.
Entire conversation (9160 bytes) V Show and save data as ASCII V Stream 165
ind:

By analyzing the tcp stream .torrent file name is Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent



In HTTP, we may search for "announce" or "scrape" URLs for finding torrent tracker traffic and seeing if any other files are torrenting.

For that use filters

http.request.uri contains announce http.request.uri contains scrape

4	2018-07-15-traffic-an	alysis-exercise.pcap								- 0	×
Eile	e <u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analy:	ze Statistics Telephony	<u>Wireless Tools H</u> elp							
4	I 🖉 🕢 📘 🗖	🗙 🖸 🭳 🧁		Q Q Q II							
	http.reguest.uri contair	is announce								X	+
No.	Time	<u>^</u>	Source	Destination	Protocol	Length Host	Source Port	Destination Port	Info		
	4312 2018-07-1	15 09:47:33	10.0.0.201	91.189.95.21	HTTP	423 torrent.ubuntu.com:6969	49842	6969	GET /announce?info_hash=%e	4%be%9eM8	b8v%e3%e3
	4538 2018-07-1	15 09:47:37	10.0.0.201	168.215.194.14	HTTP	434 files.publicdomaintorrents	49847	80	GET /bt/announce.php?info_	hash=%1d9	da%0dH%a8
	4568 2018-07-1	15 09:47:37	10.0.0.201	168.215.195.227	HTTP	434 tracker.publicdomaintorren	49848	6969	GET /announce?info hash=%1	d%da%0dH9	a8%98%bd9
4	2018-07-15-traffic-an	alysis-exercise.pcap								- 0	×
Eie	e Edit Yiew Go	Cepture Analys	e Statistics Telephony	<u>Wireless</u> <u>T</u> ools <u>H</u> elp							
		209=	* H V + T H	6 6 8 <u>B</u>							
1	http:request.un.conten	es senape								8	+ +
NO.	Time	~	Source	Destination	Protocol	Length Host	Source Port	Destination Port	Info		
+	4652 2010-07-1	15 89:47:37	18.0.0.201	160.215.194.14	HTTP	253 files.publicdomaintorrents.	49849	80	GET /bt/scrape.php?info ha	sh-%1d%ca	SodHSask:
-	4682 2010-07-1	15 09:47:37	10.0.0.201	168,215,195,227	HTTP	253 tracker.publicdomaintorren.	49958	6999	GET /scrape?info_hash-%id%	daNeditKas	N98%bd%aj

HTTP request headers from tracker traffic should also give us the torrent client in the UserAgent string.

In addition to tracker traffic to two publicdomaintorrents.com domains, the results also show tracker traffic to torrent.ubuntu.com.

Length	Host	Source Port	Destination Port	Info
423	<pre>torrent.ubuntu.com:6969 files.publicdomaintorrents.com tracker.publicdomaintorrents.com:6969</pre>	49842	6969	GET /announce?info_hash=%e4%b
434		49847	80	GET /bt/announce.php?info_has
434		49848	6969	GET /announce?info_hash=%1d%c
Length	Host	Source Port	Destination Port	Info
253	files.publicdomaintorrents.com	49849	80	GET /bt/scrape.php?info_hash=
253	tracker.publicdomaintorrents.com:6969	49850	6969	GET /scrape?info_hash=%1d%da%

The results also show the tracker traffic to two publicdomaintorrents.com domains Tracker to Torrent.ubuntu.com.

For the first HTTP request, follow the TCP stream, of torrent.ubuntu.com. Check out the User-agent string, it is Deluge 1.3.15.(Deluge is a torrent client deluge-torrent.org/)

What is tracking that traffic? You can find out that from the value of info hash. Select the value right after info hash= in the same HTTP GET request



info\_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be

### after decoding url encoding the hash will be: e4be9e4db876e3e3179778b03e906297be5c8dbe

Search that hash on Google and it comes up with:

in citiza (	🖬 You lube 🦞 Maps 🔟 29 Hosts to Glory 🦉 FuzzySecurity   Win 🧐 G intitler"Index of" "hi 📆 Drvirus1911's Paste 📓 elearnSecurity   Pe 🎯 Information Sec	urit									
oogle	e4be9e4db876e3e3179778b03e906297be5c8dbe 🗙 🔳 🌷 🔍										
	🔍 તમામ 🛇 Maps 🖾 છબીઓ 🖸 વિડિઓઝ 🧷 શોપિંગ : વયુ પસંદગી સાધનો										
	વગભગ 216 પરિષ્રામો (0.37 સેકંડ)										
	linuxtracker.org∋id=e ≠ આ પુષ્ઠનો અનુવાદ કરો										
	ubuntu-18.04-desktop-amd64 at Linuxtracker										
	27 એપ્લિ, 2018 - Info Hash, <b>e4be9e4db876e3e3179778b03e906297be5c8dbe</b> . Who thanks. tokopan gerinho sverre26. Description, Ubuntu is a complete										
	Ubuntu-18.04-desktop-amd64 Linuxtracker .::. Index->Torrent Torrent, ubuntu-18.04-desktop										
	anioda in you need a billottetti Enioxitacket is suin neret linuxtracker.org H[ย] qนู นโจญเห) »										
	memo.cash > torrent 👻 આ પુષ્ઠનો અનુવાદ કરો										
	Tag - torrent - Memo										
	magnet:?xt=um.btih:e4be9e4db876e3e3179778b03e306297be5c8dbe #ubuntu #BiglyBT. This is a test. Message [184]. Cancel Creating Broadcasting.										
	memo.cash › profile 👻 આ પુષ્ઠનો અનુવાદ કરો										
	1Dqc7VMb6WUUnrnQ's Profile - Memo										
	magnet:?xt=urn:btih:e4be9e4db876e3e3179778b03e906297be5c8dbe #ubuntu #BiglyBT. This										
	is a test. Message [184]. Cancel Creating Broadcasting.										
	Password: Login Create account Recover password										
User:											
User:	Support US Torrent's details										
User:	Support US         Torrent's details           KEEP THIS         ubuntu-18.04-desktop-amd64										
User:	Support US         Torrent's details           Image: Support US         ubuntu-18.04-desktop-amd64           Inite Atline moth: 11%         ubuntu-18.04-desktop-amd64										

and it is a bar of the day has		
Donations this month: 11% Goal : \$ 850 Due: 2020-12-31	Torrent	ubuntu-18.04-desktop-amd64 If you need a Bittorrent client, try TransmissionBT on MacOS or Linux
Main Menu	Forum	/index.php?page=forum&action=viewtopic&topicid=14996
Index Torrents Extra Stats	Magnet Link	4
News Login	Info Hash	e4be9e4db876e3e3179778b03e906297be5c8dbe
Sponsored Links	Who thanks	tokopan_gerinho.sverre26 Say Thank You!
<b>Distro</b> Watch	Description	Ubuntu is a complete desktop Linux operating system, freely available with both community and professional support. The Ubuntu community is built on the ideas enshined in the Ubuntu Manifesto: that software should be available free of charge, that software tools should be usable by people in their local language and despite any disabilities, and that people should have the freedom to customize and alter their software in whatever way they see fit. "Ubuntu" is an ancient African word, meaning "humanity to others". The Ubuntu distribution brings the spint of Ubuntu to the software world. For More Information, visit Distrowatch
Manadian	Screenshots	
Your Audience	Category	Ubuntu
LEARN HOW	Home Page	http://www.ubuntu.com/
N RevResponse	Support Forums	http://ubuntuforums.org/
Categories Categories	Rating	Rating: 3.5 out of 5.0 (Votes: 4) For your upload!

It is an ubuntu18.04-desktop-and64.iso file let us decode it using url decoder

IDqc7VMb6WUUnrnQ 762d
#torrent ubuntu-18.04-desktop-amd64.iso
magnet:?xt=urn:btih:e4be9e4db876e3e3179778b03e906297be5c8dbe
#ubuntu #BiglyBT
This is a test

 ★ B

Use the same for tracker traffic on the other HTTP requests.



Hash is 1dda0d48a898bd815c7d32ee83366f03097960fe



That is an info hash for the "*Betty Boop*" cartoon rhythm on the reservation we found earlier from that .torrent file.

For determining if any torrent files are seeded by BitTorrent .info\_hash filtering in Wireshark

	·							- 0	2
ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nal	/ze <u>S</u> tatistics Telephony <u>\</u>	<u>N</u> ireless <u>T</u> ools <u>H</u> elp							
( 🔳 🧟 🛞 📙 🖻 🔀 🖻 ९ 🤞	・ ※ 答 不 🧕 📃 📒 🤇	a e e 🎹							
bittorrent.info_hash								×	
. Time	Source	Destination	Protocol	Length Host	Source Port	Destination Port	Info		
4520 2018-07-15 09:47:37	10.0.0.201	62.210.200.57	BitTorrent	122	49846	55020	Handshake		
4542 2018-07-15 09:47:37	62.210.200.57	10.0.201	BitTorrent	242	55020	49846	Handshake	Extended	
4549 2018-07-15 09:47:37	10.0.0.201	61.245.142.233	BitTorrent	122	49845	51413	Handshake		
4684 2018-07-15 09:47:37	61.245.142.233	10.0.201	BitTorrent	122	51413	49845	Handshake		
4701 2018-07-15 09:47:38	10.0.201	82.102.24.163	BitTorrent	122	49851	42232	Handshake		
4710 2018-07-15 09:47:38	82.102.24.163	10.0.0.201	BitTorrent	242	42232	49851	Handshake	Extended	
4754 2018-07-15 09:47:39	10.0.0.201	23.82.53.139	BitTorrent	122	49853	49544	Handshake		
4760 2018-07-15 09:47:39	23.82.53.139	10.0.0.201	BitTorrent	242	49544	49853	Handshake	Extended	
4789 2018-07-15 09:47:40	10.0.201	96.237.60.19	BitTorrent	122	49854	51413	Handshake		
4815 2018-07-15 09:47:41	96.237.60.19	10.0.201	BitTorrent	122	51413	49854	Handshake		
4823 2018-07-15 09:47:41	10.0.0.201	91.160.64.33	BitTorrent	122	49855	32776	Handshake		
4830 2018-07-15 09:47:41	91.160.64.33	10.0.201	BitTorrent	122	32776	49855	Handshake		
4850 2018-07-15 09:47:43	10.0.0.201	85.17.122.98	BitTorrent	122	49858	63925	Handshake		
4855 2018-07-15 09:47:43	85,17,122,98	10.0.201	BitTorrent	457	63925	49858	Handshake	Extended	н
4870 2018-07-15 09:47:44	10.0.0.201	79.197.60.22	BitTorrent	122	49859	16881	Handshake		
4882 2018-07-15 09:47:45	10.0.0.201	104.62.139.198	BitTorrent	122	49862	51413	Handshake		
4887 2018-07-15 09:47:45	104.62.139.198	10.0.0.201	BitTorrent	242	51413	49862	Handshake	Extended	
4895 2018-07-15 09:47:45	79,197,60,22	10.0.201	BitTorrent	122	16881	49859	Handshake		
4925 2018-07-15 09:47:47	10.0.201	37,187,6,237	BitTorrent	122	49863	45000	Handshake		
4930 2018-07-15 09:47:47	10.0.201	37,187,0.55	BitTorrent	122	49864	54978	Handshake		
		** * * ***				*****			
									<u> </u>
0 0000 0000 0000 = Fragm	≥nt offset: 0								
Time to live: 128									
Protocol: TCP (6)									
Header checksum: 0xe205 [va	lidation disabled]								
[Header checksum status: Un	verified]								
Source: 10.0.0.201									
000 00 09 b7 27 a1 3e 00 16 1	7 18 66 c8 08 00 45 00	····'·>·· ··f···E·							•••••
010 00 6c 06 b2 40 00 80 06 e	2 05 0a 00 00 c9 3e d2	·1··@··							
	1 51 66 69 05 3e 50 18	·9·····k !Qfi·>P·							
020 c8 39 c2 b6 d6 ec 98 6b 2.	3 74 F4 CE 70 70 CF C-	D ALT STREET							
020 c8 39 c2 b6 d6 ec 98 6b 2 030 fa f0 89 d5 00 00 13 42 69	9 74 54 6T 72 72 65 6e	B itiorren							
020         c8         39         c2         b6         d6         ec         98         6b         2           030         fa         f0         89         d5         00         00         13         42         60           040         74         20         70         72         6f         74         6f         63         66	f 6c 00 00 00 00 00 10	t protoc ol							
020         c8         39         c2         b6         d6         e         98         6b         2           030         fa         f0         89         d5         00         00         13         42         6           040         74         20         70         72         6f         74         6f         63         6           050         06         05         e4         b9         e4         b8         76         e3           07         b7         b7         b9         b9         b4         b8         b76         e3	f 6c 00 00 00 00 00 10 s e3 17 97 78 b0 3e 90 i 31 23 46 20 24 56 60	t protoc ol							
020         c8         39         c2         b6         d6         c         98         6b         2           030         fa         f0         89         d5         90         00         13         42         6           040         74         20         70         72         67         74         6f         6           050         90         05         e4         be         9e         4d         b8         76         e2           060         05         e4         be         9e         4d         b8         76         e2           070         72         65         55         8d         be         2d         44         4           07         70         55         75         75         75         79         96         79         76         76         79         76	5 74 54 6T 72 72 65 6e f 6c 00 00 00 00 00 10 3 e3 17 97 78 b0 3e 90 5 31 33 46 30 2d 56 6e 76	t protoc ol 							
020         c8         39         c2         b6         d6         c2         98         b6         2           036         fa         f0         89         d5         60         00         13         42         6           040         74         20         70         72         67         74         66         63         6           040         05         e4         be         9e         44         87         76         53         52         46         38         5a         50         39         65           070         7a         5a         52         46         38         5a         50         39         65	6 74 54 67 72 72 65 6e F 6c 00 00 00 00 00 10 3 e3 17 97 78 b0 3e 90 3 11 33 46 30 2d 56 6e 3 76	t protoc ol· ···································							
020         C8         39         c2         b6         d6         c         98         b5         06         0         13         42         6           030         fa         f0         89         d5         06         00         13         42         6           04         74         20         70         72         6f         74         6f         63         68         08         05         e4         be         94         b8         56         e         62         79         76         5a         52         46         38         5a         50         39         65           70         5a         52         46         38         5a         50         39         65	5 74 54 67 72 72 65 66 6 c 00 00 00 00 00 00 00 3 e3 17 97 78 b0 3e 90 5 31 33 46 30 2d 56 6e 3 76	t proto ol M.V · · · · X · > b · \ · · -D E13F0-Vn pZRF8ZP9 iv							
020         c8         39         c2         b6         d6         c9         60           03         03         04         09         13         42         6           04         74         20         70         72         67         74         66         63         69         69         64         74         46         63         64 <td>9 74 54 67 72 72 65 66 6 60 00 00 00 00 00 00 10 3 e3 17 97 78 b0 3e 90 5 31 33 46 30 2d 56 6e 3 76</td> <td>b Itlorren t protoc ol </td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	9 74 54 67 72 72 65 66 6 60 00 00 00 00 00 00 10 3 e3 17 97 78 b0 3e 90 5 31 33 46 30 2d 56 6e 3 76	b Itlorren t protoc ol 							
020         c8         39         c2         b6         d6         c9         66         b0         13         c2         b6         b0         b7         b8         b8         b7         b8         b8         b7         b7         b8         b7	9 /4 34 6T 72 72 65 66 f 66 00 00 00 00 00 10 3 e3 17 97 78 b0 3e 90 5 31 33 46 30 2d 56 6e 9 76	M v v x x b V v D E13F0-Vn pZRF8ZP9 iv							
020 c8 39 c2 b6 d6 cc 98 cb 2 020 c8 39 c2 b6 d9 c0 13 42 c 040 74 20 70 72 cf 74 cf 63 c 040 65 c4 be 9e 44 b8 76 c 06 65 c4 be 9e 44 b8 76 c 06 62 97 be 5c 84 be 24 44 4 70 5a 52 46 38 5a 50 39 c BitTorrent Protocol Name Length: 19	9 /4 34 61 72 72 65 66 6 60 00 00 00 00 00 10 3 e3 17 97 78 b0 3e 90 3 13 33 46 30 2d 56 6e 3 76	trote ol M.vx.> b.\D E13F0-Vn pZRF8ZP9 iv							
020         c8         39         c2         b6         d6         c9         66         c9         c6         c7	9 /4 34 67 /2 /2 05 66 f 66 00 60 00 00 00 10 3 e3 17 97 78 b0 3e 90 3 13 34 6 30 2d 56 6e 9 76	yroto ol M.vx.> b.\pise-No pZRF8ZP9 iv							
020         c8         39         c2         b6         d6         c9         66         b7         b8         b3         b8         00         b3         b2         b3         b2         b3         b2         b3         b2         b3         b2         b3         b2         b3	9 /4 34 67 /2 /2 05 66 6 C 60 60 60 60 60 61 3 e 3 17 97 76 16 3e 99 3 1 33 46 30 2d 56 6e 3 76	trotocil Nv							
020         c8         39         c2         b6         d6         c9         66         c9         c6         c7         c7         c6         c7	9 /4 34 67 /2 /2 05 66 f 6C 40 80 40 80 40 80 3 e 3 17 97 78 b 3 e 90 5 13 33 46 30 2d 56 6e 3 76 otocol 00000000100005 s adbu92ddh076e1p3170772	throng of the second s							

You can copy that field's hexadecimal value by copying it as a hex-stream. Then, if needed, paste it into a Google search. In this case it is the same SHA1 hash we found earlier for the Ubuntu 18.04 ISO package.

Time	Source	Destinatio	Expand Subtrees Collapse Subtrees	Ī	
4520 2018-07-15 09:47:37 4542 2018-07-15 09:47:37 4549 2018-07-15 09:47:37 4684 2018-07-15 09:47:37	10.0.0.201 62.210.200.57 10.0.0.201 61.245.142.233	62.210. 10.0.0. 61.245. 10.0.0.	Expand All Collapse All		
4701 2018-07-15 09:47:38 4710 2018-07-15 09:47:38	10.0.0.201 82.102.24.163	82.102.	Apply as Column	Ctrl+Shift+I	
4754 2018-07-15 09:47:39 4760 2018-07-15 09:47:39 4789 2018-07-15 09:47:40 4815 2018-07-15 09:47:41 4823 2018-07-15 09:47:41 4830 2018-07-15 09:47:41	10.0.0.201 23.82.53.139 10.0.0.201 96.237.60.19 10.0.0.201 91.160.64.33	23.82.5 10.0.0. 96.237. 10.0.0. 91.160. 10.0.0.	Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter Follow	> > > >	
4850 2018-07-15 09:47:43 4855 2018-07-15 09:47:43 4870 2018-07-15 09:47:44 4882 2018-07-15 09:47:45 4887 2018-07-15 09:47:45 4887 2018-07-15 09:47:45	10.0.0.201 85.17.122.98 10.0.0.201 10.0.0.201 104.62.139.198 79.197.60.22	85.17.1 10.0.0. 79.197. 104.62. 10.0.0.	Copy Show Packet Bytes Export Packet <u>B</u> ytes	Ctrl+Shift+O Ctrl+Shift+X	All Visible Items All Visible Selected Tree Items Description Field Name
4925 2018-07-15 09:47:47 4930 2018-07-15 09:47:47	10.0.0.201 10.0.0.201	37.187. 37.187.	Wiki Protocol Page Filter Field Reference Protocol Preferences	•	Value As Filter
BitTorrent Protocol Name Length: 19 Protocol Name: BitTorrent pr Beserved Extension Bytes: 00	otocol		Decode <u>A</u> s Go to Linked Packet	Mindous	Copy Bytes as Hex + ASCII Dum as Hex Dump as Printable Text
SHA1 Hash of info dictionary Peer ID: 2d4445313346302d560	<pre>/: e4be9e4db876e3e317977: 5e705a5246385a50396976 / 18 66 c8 08 00 45 00</pre>	3b03e906297pe	SCOODE		as a Hex Stream as Raw Binary as Escaped String

Also, you can apply that value as a column, so you can quickly see all the SHA1 hashes seeded in the pcap.

			~~~ _	
Ditt	corrent.into_nash	lar in	Expand Subtrees	
0.	Time	Source	C.I. S. L.	
	4520 2018-07-15 09:47:37	10.0.201	Collapse Subtrees	
	4542 2018-07-15 09:47:37	62.210.200.57	Expand All	
	4549 2018-07-15 09:47:37	10.0.0.201	Collapse All	
	4684 2018-07-15 09:47:37	61.245.142.233	101 10 10200	
	4/01 2018-07-15 09:47:38	10.0.0.201	Apply as Column	Ctrl+Shift+I
	4710 2010-07-15 09:47:30	10 0 0 201	Apply of Filter	
	4760 2018-07-15 09:47:39	23 82 53 139	Apply as tricer	
	4789 2018-07-15 09:47:40	10 0 0 201	Prepare as Filter	
	4815 2018-07-15 09:47:41	96.237.60.19	Conversation Filter	
	4823 2018-07-15 09:47:41	10.0.0.201	Colorize with Filter	
	4830 2018-07-15 09:47:41	91.160.64.33	Follow	
	4850 2018-07-15 09:47:43	10.0.201	101000	
	4855 2018-07-15 09:47:43	85.17.122.98	Сору	
	4870 2018-07-15 09:47:44	10.0.201		
	4882 2018-07-15 09:47:45	10.0.201	Show Packet Bytes	Ctrl+Shift+O
	4887 2018-07-15 09:47:45	104.62.139.198	Export Packet Bytes	Ctrl+Shift+X
	4895 2018-07-15 09:47:45	79.197.60.22		
	4925 2018-07-15 09:47:47	10.0.201	Wiki Protocol Page	
	4930 2018-07-15 09:47:47	10.0.0.201	Filter Field Reference	
1			Protocol Preferences	)
Bi	tTorrent		Decode Ac	
	Protocol Name Length: 19		Decode <u>A</u> s	
	Protocol Name: BitTorrent pro	otocol	Go to Linked Packet	
	Reserved Extension Bytes: 00	30000000100005	Show Linked Packet in New V	/indow
	SHA1 Hash of info dictionary	: e4be9e4db876e3e31797	70003490029704360004	
	Peer 10: 2044453155465020566	2/02452465658505969/6		
000	00 09 b7 27 a1 3e 00 16 17	18 66 c8 08 00 45 00	····'·>···f···E·	
010	00 6c 06 b2 40 00 80 06 e2	05 0a 00 00 c9 3e d2	·1··@··· ····>·	
020	fa fo 89 d5 00 00 13 43 60	74 54 6f 72 72 65 66	B itTorren	
040	74 20 70 72 6f 74 6f 63 6f	6c 00 00 00 00 00 10	t protoc ol	
0050	00 05 e4 be 9e 4d b8 76 e3	e3 17 97 78 b0 3e 90	•••••M•v ••••ו>•	
0060	62 97 be 5c 8d be 2d 44 45	31 33 46 30 2d 56 6e	b···\·D E13F0-Vn	
00.00	70 5a 52 46 38 5a 50 39 69	76	n7RE87P9 iv	

	Source	Destination	Protocol	Length Host	2018	-07-15-traffic-analysis-exercise.pcap			
9:47:37	10.0.201	62.210.200.57	BitTorrent	122	<b>E</b> 1. 1		C	WC 1	
9:47:37	62.210.200.57	10.0.0.201	BitTorrent	242	Fue 3	dit view Go Capture Analyz	e Statistics lelephony	wireless loois Help	
9:47:37	10.0.201	61.245.142.233	BitTorrent	122	4 =	🥂 🔘 📙 🗔 🗙 🔂 🍳 👄	🐵 🥸 😱 👢 📃 🔳	0.0.0.1	
99:47:37	61.245.142.233	10.0.0.201	BitTorrent	122	(				
9:47:38	10.0.201	82.102.24.163	BitTorrent	122	boot	p			
99:47:38	82.102.24.163	10.0.0.201	BitTorrent	242	No	Time	Source	Destination	Protocol
9:47:39	10.0.201	23.82.53.139	BitTorrent	122	1101	3 3018 07 15 00 45 43	10.0.0.1	10.0.0.201	DUCD
9:47:39	23.82.53.139	10.0.0.201	BitTorrent	242		2 2010-07-15 09:45:42	10.0.0.1	10.0.0.201	DHCP
9:47:40	10.0.201	96.237.60.19	BitTorrent	122	er	1 2018-07-15 09:45:42	0.0.0.0	255.255.255.255	DHCP
9:47:41	96.237.60.19	10.0.0.201	BitTorrent	122	<				
9:47:41	10.0.201	91.160.64.33	BitTorrent	122					
9:47:41	91.160.64.33	10.0.0.201	BitTorrent	122		.000 0000 0000 0000 = Rese	rved flags: 0x0000		
9:47:43	10.0.201	85.17.122.98	BitTorrent	122		Client IP address: 0.0.0.0			
9:47:43	85.17.122.98	10.0.0.201	BitTorrent	457		Your (client) IP address: 0.0	.0.0		
99:47:44	10.0.201	79.197.60.22	BitTorrent	122		Next server TP address: 0.0.0	1.0		
9:47:45	10.0.201	104.62.139.198	BitTorrent	122		Palay agent TD address . 0.0			
9:47:45	104.62.139.198	10.0.0.201	BitTorrent	242		Client MC address Mai 10.00		-9)	
9:47:45	79.197.60.22	10.0.0.201	BitTorrent	122		LITENC MAC address: MSI_10:00	0:00 (00:10:17:10:00		
09:47:47	10.0.201	37.187.6.237	BitTorrent	122	2	Llient hardware address padd:	ng: 0000000000000000	30000	
09:47:47	10.0.201	37.187.0.55	BitTorrent	122		Server host name not given			
		** * * ***		~ * *		Boot file name not given			
					3	Magic cookie: DHCP			
					2	Ontion: (53) DHCP Message Tv	(Request)		

To locate IP address with the DHCP's MAC address and host name use filter

Bootp

	Cli	ent	IP	ade	ires	55:	0.	0.0.	0											
	You	r (	cli	ent	IF	a	ddr	ess:	0.1	0.6	.0									
	Nex	t s	erve	er 1	IP a	add	res	s: 0	.0.1	0.6										
	Rel	ay a	agei	nt :	IP a	add	res	5: 0	.0.1	0.6										
	cli	ent	MA	c a	Idre	255	: M	si_1	8:6	6:c	8 (1	00:	16:	17:	18:	66:0	(8)			
	Cli	ent	hai	rdwa	are	ad	dre	ss p	add	ing	: 00	999	000	000	000	0000	000			
	Ser	ver	ho	st i	ame	e ne	ot	give	n											
	Boo	t f	ile	nar	ne r	not	gi	ven												
	Mag	ic	cool	kie	Dł	ICP														
>	Opt	ion	: (!	53)	DHO	IP (	Mes	sage	Ty	pe	(Red	que	st)							
>	Opt	ion	: (1	51)	c1:	Len	t i	dent	ifi	en										
~	Opt	ion	: (	50)	Red	que	ste	d IP	Ad	dre	55 1	(10	.0.	0.2	01)					
	1	Leng	th	: 4								-			0					
		Regi	lest	ted	IP	Add	dres	ss:	10.0	9.0	. 201	1								
×	Opt	ion	: (	12)	Hos	st I	Nam	e												
	-	Lens	gth:	: 14	i i i															
	- 1	Host	E Na	ame :	BL	ANG	0-02	DESK	TOP											
	areand		. 0	81)	c1:	Len	t Fi	ully	Qui	ali	fie	d D	oma	in	Nam	e				
>	Opt	ion																		
>	Opt	ion	. ()																	 
>	Opt ff	ff	ff	ff	ff	ff	00	16	17	18	66	c8	08	00	45	00		· · f ·	E	 
>	Opt ff 01 ff	ff 6d	ff 4b	ff 36	ff 00	ff 00	00 80	16 11	17 ee	18 4a	66 00	c8 00	08 00	00 00	45 ff	00 ff	mK6	•••f• • J ••	E	 
> 3000 3010 3020 3020	Opt ff 01 ff 02	ff 6d ff 55	ff 4b 00	ff 36 44 90	ff 00 00	ff 00 43	00 80 01	16 11 59	17 ee fe	18 4a 27 90	66 00 01	c8 00 01	08 00 06	00 00 00	45 ff 20	00 ff 64 00	- mK6 D - C - Y	· · f · · J · · · ·	E d	 
> 3000 3010 3020 3030 3030	Opt ff 01 ff 02 00	10n ff 6d ff 55 00	ff 4b 00 00	ff 36 44 00	ff 00 00 00	ff 00 43 00	00 80 01 00 00	16 11 59 00 16	17 ee fe 00 17	18 4a 27 00 18	66 00 01 00 66	c8 00 01 00 c8	08 00 06 00	00 00 00 00	45 ff 20 00	00 ff 64 00 00	mK6 DCY U	• • f • • J • • • • • •	E d	 
> 8000 8010 8020 8030 8030 8040 8050	0pt ff 01 ff 02 00 00	10n ff 6d ff 55 00 00	ff 4b 00 00 00	ff 36 44 00 00	ff 00 00 00 00	ff 00 43 00 00	00 80 01 00 00	16 11 59 00 16 00	17 ee fe 00 17 00	18 4a 27 00 18 00	66 00 01 00 66 00	c8 00 01 00 c8 00	08 00 06 00 00	00 00 00 00 00	45 ff 20 00 00	00 ff 64 00 00	тКб - D-С-Ү - U	···f· · J··· · · · ·	đ	 
> 0000 0010 0020 0030 0040 0050 0050	0pt ff 01 ff 02 00 00 00	10n ff 6d ff 55 00 00 00	ff 4b 00 00 00 00	ff 36 44 00 00 00	ff 00 00 00 00 00	ff 00 43 00 00 00	00 80 01 00 00 00	16 11 59 00 16 00 00	17 ee fe 00 17 00 00	18 4a 27 00 18 00 00	66 00 01 00 66 00 00	c8 00 01 00 c8 00 00	08 00 06 00 00 00	00 00 00 00 00 00	45 ff 20 00 00 00	00 ff 64 00 00 00	-mK6 D-C-Y -U	· · f · · J · · · · · ·	d	
> 8000 8010 8020 8030 8050 8050 8050 8060 8050	0pt ff 01 ff 02 00 00 00 00	10n ff 6d ff 55 00 00 00 00	ff 4b 00 00 00 00 00 00	ff 36 44 00 00 00 00 00	ff 00 00 00 00 00 00	ff 00 43 00 00 00 00 00	00 80 01 00 00 00 00 00	16 11 59 00 16 00 00 00	17 ee fe 00 17 00 00 00	18 4a 27 00 18 00 00 00	66 00 01 00 66 00 00 00	<ul> <li>c8</li> <li>00</li> <li>01</li> <li>00</li> <li>c8</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> </ul>	08 00 06 00 00 00 00	00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00	00 ff 64 00 00 00 00 00	-mK6 D-C-Y -U	· · f ·	d	
> 0000 0010 0020 0040 0040 0050 0050 0050 0050 005	0pt ff 01 ff 02 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00	ff 00 00 00 00 00 00 00	ff 00 43 00 00 00 00 00 00	00 80 01 00 00 00 00 00 00	16 11 59 00 16 00 00 00 00	17 ee fe 00 17 00 00 00 00	18 4a 27 00 18 00 00 00 00	66 00 01 00 66 00 00 00 00	<ul> <li>c8</li> <li>00</li> <li>01</li> <li>00</li> <li>c8</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> </ul>	08 00 06 00 00 00 00 00	00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00	-mK6 	f.	d	
> 0000 0010 0020 0030 0040 0050 0050 0050 0050 0050 005	Opt ff 01 ff 02 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00	ff 00 43 00 00 00 00 00 00 00	00 80 01 00 00 00 00 00 00 00	16 11 59 00 16 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00	66 00 01 66 00 00 00 00 00	<ul> <li>c8</li> <li>00</li> <li>01</li> <li>00</li> <li>c8</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> <li>00</li> </ul>	08 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00	- mК6 	· · f ·	d	
> 0000 0010 0020 0040 0050 0050 0050 0050 0050 005	0pt ff 01 ff 02 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00	ff 00 43 00 00 00 00 00 00 00 00 00	00 80 01 00 00 00 00 00 00 00	16 11 59 00 16 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00	66 00 01 00 66 00 00 00 00 00 00	<ul> <li>c8</li> <li>00</li> <li>01</li> <li>00</li> <li>c8</li> <li>00</li> &lt;</ul>	08 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00	- mK6 D · C · Y - U · Y	· · f · . J · . · f ·	d	
> 0000 0010 0020 0030 0040 0050 0050 0050 0050 0050 005	Opt ff 01 ff 02 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 43 00 00 00 00 00 00 00 00 00 00	00 80 01 00 00 00 00 00 00 00 00 00	16 11 59 00 16 00 00 00 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00 00	66 00 01 00 66 00 00 00 00 00 00 00	c8 00 01 00 00 00 00 00 00 00 00	98 90 96 90 90 90 90 90 90 90	00 00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00 00 00 00	- mK6 - D · C · Y - U	· · f · · · · · · · · · · · · · · · · ·	d	
> 0000 0010 0020 0040 0050 0050 0050 0050 0050 005	Opt ff 01 ff 02 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00 00 00 00 00 0	ff 00 43 00 00 00 00 00 00 00 00 00 00	00 80 01 00 00 00 00 00 00 00 00 00	16 11 59 00 16 00 00 00 00 00 00 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00 00 00 00	56 00 01 66 00 00 00 00 00 00 00 00 00	c8 00 01 00 00 00 00 00 00 00 00 00	98 90 90 90 90 90 90 90 90 90 90	00 00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00 00 00 00 00 00	тк6 D-С-Ү U	• f • • • • • • • • • • • • • • • • • •	d	
> 0000 0010 0020 0040 0050 0050 0050 0050 0050 005	Opt ff 01 ff 02 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00 00 00 00 00 0	ff 00 43 00 00 00 00 00 00 00 00 00 00 00	00 80 01 00 00 00 00 00 00 00 00 00 00 00	16 11 59 00 16 00 00 00 00 00 00 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00 00 00 00 00 00	56 00 01 66 00 00 00 00 00 00 00 00 00 00 00	c8 00 01 00 00 00 00 00 00 00 00 00 00 00	98 90 90 90 90 90 90 90 90 90 90 90 90	00 00 00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00 00 00 00 00 00	- mK6 - D · C · Y - U		d	
> 00000 0010 0020 0040 0050 0050 0050 0050 0050 005	Opt ff 01 ff 02 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00 00 00 00 00 0	ff 00 43 00 00 00 00 00 00 00 00 00 00 00 00 00	00 80 01 00 00 00 00 00 00 00 00 00 00 00 00	16 11 59 00 16 00 00 00 00 00 00 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00	56 00 01 66 00 00 00 00 00 00 00 00 00 00 00 00	<ul> <li>c8</li> <li>00</li> <li>01</li> <li>00</li> <li>c8</li> <li>00</li> &lt;</ul>	98 90 90 90 90 90 90 90 90 90 90 90 90 90	00 00 00 00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00 00 00 00 00 00	- mK6 - D - C - Y - U		d	
> 00000 0010 0020 0040 0040 0050 0050 0050 0050 005	Opt ff 01 ff 02 00 00 00 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00 00 00 00 00 0	ff 00 43 00 00 00 00 00 00 00 00 00 00 00 00 00	00 80 01 00 00 00 00 00 00 00 00 00 00 00 00	16 11 59 00 16 00 00 00 00 00 00 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00	56 00 01 00 00 00 00 00 00 00 00 00 00 00	<ul> <li>c8</li> <li>00</li> <li>01</li> <li>00</li> <li>c8</li> <li>00</li> &lt;</ul>	98 90 90 90 90 90 90 90 90 90 90 90 90 90	00 00 00 00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00 00 00 00 00 00	- mK6 	f .j  	·E·	
> 00000 0010 0020 0020 0020 0020 0020 00	Opt ff 01 ff 02 00 00 00 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00 00 00 00 00 0	ff 00 43 00 00 00 00 00 00 00 00 00 00 00 00 00	80 80 80 80 80 80 80 80 80 80 80 80 80 8	16 11 59 00 16 00 00 00 00 00 00 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00	66 00 01 00 00 00 00 00 00 00 00 00 00 00	28 00 01 00 00 00 00 00 00 00 00 00 00 00	98 90 90 90 90 90 90 90 90 90 90 90 90 90	00 00 00 00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00 00 00 00 00 00	- mK6 - D-C-Y U	. f . J 	- E - d	
> 00000 0010 0026 00300 00500 00000 00000 00000 00000 00000 00000 0000	Opt ff 01 ff 02 00 00 00 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00 00 00 00 00 0	ff 00 43 00 00 00 00 00 00 00 00 00 00 00 00 00	80 80 00 00 00 00 00 00 00 00 00 00 00 0	16 11 59 00 16 00 00 00 00 00 00 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00	66 00 01 66 00 00 00 00 00 00 00 00 00 00 00 00	<pre>c8 00 01 00 c8 00 00 00 00 00 00 00 00 00 00 00 00 00</pre>	08 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00 00 00 00 00 00	- mK6 D- C - Y - U		-E d = BL	
> 50000 6010 60200 60300 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 60400 6040000000000	Opt ff 01 ff 02 00 00 00 00 00 00 00 00 00	10n ff 6d ff 55 00 00 00 00 00 00 00 00 00	ff 4b 00 00 00 00 00 00 00 00 00 00 00 00 00	ff 36 44 00 00 00 00 00 00 00 00 00 00 00 00	ff 00 00 00 00 00 00 00 00 00 00 00 00 0	ff 00 43 00 00 00 00 00 00 00 00 00 0	00 80 00 00 00 00 00 00 00 00 00 00 00 0	16 11 59 00 16 00 00 00 00 00 00 00 00 00 00 00 00 00	17 ee fe 00 17 00 00 00 00 00 00 00 00 00 00 00 00 00	18 4a 27 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00	66 00 01 66 00 00 00 00 00 00 00 00 00 00 00 00	<pre>c8 00 01 00 c8 00 00 00 00 00 00 00 00 00 00 00 00 00</pre>	08 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00	45 ff 20 00 00 00 00 00 00 00 00 00 00 00 00	00 ff 64 00 00 00 00 00 00 00 00 00 00 00 00 00	-mK6 D-C-Y -1)	f f f s c s c s c s	e d	

The Bootstrap Protocol (BOOTP) is a computer networking protocol used by Internet Protocol networks to automatically assign an IP address from a configuration server to the network devices.

From this filter we can see:

### MAC Address: 00:16:17:18:66:c8 IP Address: 10.0.0.201 Host Name: BLANCO-DESKTOP

#### Use filter kerberos.CnameString

To find the name of a Windows user account.

Windows host names and user account names are represented by the **CNameString** values. Upon location of any **CNameString** value in the frame details panel, add it as A column, so you can find your associated user account quickly from your column display.

🚄 2018-07-15-traffic-analysis-e	xercise.pcap	0.9995) ISI - 028597	ine odk te testist							10 <b></b> 11	٥	×
File Edit View Go Capt	ture <u>A</u> nalyze <u>S</u> tatistics	Telephony Win	reless <u>T</u> ools <u>H</u> elp . Q. Q. III									
kerberos. CNameString										1	×I →	-
Packet list 🚽 I	Narrow & Wide 🛛 🗸 🗍	Case sensitive	Display filter 🗸 🗸						F	ind	Cano	el
No. Time	Source		Destination	Protocol	Length Host		Source Port	Destination Port	SHA1 Hash of	info diction	ary	
1538 2018-07-15 09:	45:53 10.0.	0.201	10.0.0.2	KRB5	382		49742	88				
1596 2018-07-15 09:	46:52 10.0.	0.201	10.0.0.2	KRB5	290		49744	88			1	
1604 2018-07-15 09:	46:52 10.0.	0.201	10.0.0.2	KRB5	370		49745	88				
100 2018-07-15 09:	45:43 10.0.	.0.2	10.0.0.201	KRB5	250		88	49677				
114 2018-07-15 09:	45:43 10.0.	.0.2	10.0.0.201	KRB5	250		88	49679				
<		~ ~	** * * ***				~~				>	
✓ Kerberos												
> Record Mark: 324 by	ytes											
✓ as-req												
pvno: 5												
msg-type: krb-as	s-req (10)											
> padata: 2 items												
✓ req-body												
Padding: 0												
> kdc-options:	40810010											
✓ cname												
name-type:	kRB5-NT-PRINCIPAL (:	1)										
✓ cname-stri	ng: 1 item	3										
CNameSt	ring: BLANCO-DESKTOPS	5										
realm: DOGOFT	HEYEAR.NET											- 1
> sname												
till: 2037-09	9-13 02:48:05 (UTC)											
rtime: 2037-0	09-13 02:48:05 (UTC)											
nonce: 135764	152											
> etype: 6 item	15	0.00										- 11
> addresses: 1	item BLANCO-DESKTOP<	20>										
0030 08 05 81 8b 00 00	00 00 01 44 6a 82 0	1 40 30 82	····· <b>Dj··@</b> 0·	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	***************************************							
0040 01 3c a1 03 02 01	05 a2 03 02 01 0a a	3 63 30 61	<c0a< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></c0a<>									
0050 30 4c a1 03 02 01	02 a2 45 04 43 30 4	1 a0 03 02 0	E-COA									1.1
0060 01 12 a2 3a 04 38	7b 13 39 97 66 cf 9	d e0 e9 a5	3 h hm 11 le7									
9888 50 21 17 5c e9 d4	4a d1 3d aa 35 54 1	d 88 f3 c3 P	21.\									
0090 2e 9a 5e e1 91 39	6f 10 59 42 7a 98 6	e 2a 30 11 .	-^90- YBz-n*0-									
00a0 a1 04 02 02 00 80	a2 09 04 07 30 05 a	0 03 01 01										
00b0 ff a4 81 ca 30 81	c7 a0 07 03 05 00 4	0 81 00 10	····@···· @····									
00c0 al 1c 30 1a a0 03	02 01 01 a1 13 30 1	1 1b 0f 42	-0B									
0000 4c 41 4e 45 4t 2d	44 45 53 40 54 41 5	0 24 a2 12 L	ANCO-DE SKIOPS									
00f0 45 54 a3 25 30 23	a0 03 02 01 02 a1 1	c 30 1a 1h F	T %0#									
0100 06 6b 72 62 74 67	74 1b 10 44 4f 47 4	f 46 54 48	krbtgt · DOGOFTH									
0110 45 59 45 41 52 2e	4e 45 54 a5 11 18 0	f 32 30 33 E	YEAR.NE T 203									
The size of this PDU /to	n.ndu.size), 328 hytes					Parkater 1	6358 · Displayed · 28	(0.2%)		11	Profile	Defa
- Size of this PDO (to	provinsiech and pares					Founcis. 1	osso ospidyeu. 20	012101			invite.	Juliau

Packet list 🚽 Narrow & Wide	Case sensitive	Display filter 🗸 🗸 🗸 🗸 🗸 🗸 🗸						Find	Cano	el
Time	Source	Destination	Protocol	Length Host	Source Port	Destination Port	CNameString SHA1 Hash of info dictionary	1		
1640 2018-07-15 09:46:52	10.0.2	10.0.0.201	KRB5	303	88	49749	elmer.blanco			
1618 2018-07-15 09:46:52	10.0.0.2	10.0.0.201	KRB5	175	88	49746	elmer.blanco			
1552 2018-07-15 09:45:53	10.0.0.2	10.0.201	KRB5	199	88	49743	BLANCO-DESKTOP\$			
403 2018-07-15 09:45:44	10.0.2	10.0.201	KRB5	114	88	49697	BLANCO-DESKTOP\$			
391 2018-07-15 09:45:44	10.0.0.2	10.0.0.201	KRB5	293	88	49696	BLANCO-DESKTOP\$			
362 2018-07-15 09:45:44	10.0.2	10.0.201	KRB5	227	88	49694	BLANCO-DESKTOP\$			
309 2018-07-15 09:45:43	10.0.0.2	10.0.201	KRB5	293	88	49692	BLANCO-DESKTOP\$			
219 2018-07-15 09:45:43	10.0.2	10.0.201	KRB5	114	88	49685	BLANCO-DESKTOP\$			
207 2018-07-15 09:45:43	10.0.0.2	10.0.201	KRB5	273	88	49684	BLANCO-DESKTOP\$			
126 2018-07-15 09:45:43	10.0.0.2	10.0.201	KRB5	293	88	49680	BLANCO-DESKTOP\$			
1604 2018-07-15 09:46:52	10.0.201	10.0.0.2	KRB5	370	49745	88	elmer.blanco			
1596 2018-07-15 09:46:52	10.0.201	10.0.0.2	KRB5	290	49744	88	elmer.blanco			
1538 2018-07-15 09:45:53	10.0.201	10.0.0.2	KRB5	382	49742	88	BLANCO-DESKTOP\$			
1530 2018-07-15 09:45:53	10.0.201	10.0.0.2	KRB5	302	49741	88	BLANCO-DESKTOP\$			

- Host names are end with \$.
- User account names are without the \$ sign at the end.

#### User: elmer.blanco Host: BLANCO-DESKTOP

For finding which version of Windows is host running use filter, check the User-Agent string for normal web browsing traffic in the HTTP request headers.

We can filter For finding which version of Windows is host running by **http.request** and! (udp.port eq 1900)

To view publicdomaintorrents.info viewed by the user. Then, Right click and Follow TCP stream.



### The User-Agent reveals this is a 64-bit Windows 10 host

# Analyzing a MODBUS DoS attack on SCADA

Attacks on SCADA / ICS systems are not intended for confidential information, but for the process itself. While a DDoS attack on a web server can be costly and inconvenient, a DDoS attack on a SCADA system may be life threatening!

Another key difference between the traditional IT systems and SCADA systems is the communication protocol. SCADA / ICS is composed of existing seria protocols such as modbus and DNP3. While now encapsulated for external communication in TCP / IP, internally they are still very simple serial protocols.

## Finding modbus Traffic

Let's analyze and separate SCADA/ICS traffic using WireShark. Let's look at the ubiquitous modbus over TCP packet, perhaps the SCADA/ICS protocol most widely used. While modbus was originally designed for use on a serial medium such as RS232 or RS485, it was modified for use over TCP / IP networks.



hackers-arise.com

Let's open some sample modbus traffic using Wireshark. We'll be using a pcap file of some modbus test data in this tutorial. To open this, use Wireshark to open modbus test data part1.pcap (File —> Open).

Now that we've loaded this capture file, we can use Wireshark to do research. First, let's create some modbus-traffic filters. The most basic filter in modbus would be;

### mbtcp

This would filter all traffic, but the TCP traffic modbus over.

Filter: mbt	ср		-	Expression Clear Apply Save
ime	Source	Destination	Protocol	Length Info
15.266493	10.0.0.57	10.0.0.3	Modbus	/ 66 Query: Trans: 0; Unit: 10, Func: 8/ 1: Force I
15.268405	10.0.0.3	10.0.0.57	Modbus/	/ 63 Response: Trans: 0; Unit: 10, Func: 8: Diagnostics
15.268888	10.0.0.57	10.0.3	Modbus/	/ 66 Query: Trans: 0; Unit: 10, Func: 8/ 1: Force I
15.271020	10.0.0.3	10.0.0.57	Modbus/	/ 63 Response: Trans: 0; Unit: 10, Func: 8: Diagnostics
15.271447	10.0.0.57	10.0.0.3	Modbus/	/ 66 Query: Trans: 0; Unit: 10, Func: 8/ 1: Force I
15.273608	10.0.0.3	10.0.0.57	Modbus	/ 63 Response: Trans: 0; Unit: 10, Func: 8: Diagnostics
25.889380	10.0.0.57	10.0.3	Modbus/	/ 66 Query: Trans: 0; Unit: 10, Func: 8/ 1: Restart
25.891231	10.0.0.3	10.0.0.57	Modbus	/ 63 Response: Trans: 0; Unit: 10, Func: 8: Diagnostics
25.891714	10.0.0.57	10.0.0.3	Modbus	/ 66 Query: Trans: 0; Unit: 10, Func: 8/ 1: Restart
25.893737	10.0.0.3	10.0.0.57	Modhus	/ 66 Response: Trans: 0: Unit: 10. Func: 8/ 1: Restart
•				III.
Etherno	et II, Src: Run et Protocol Ver ion: 4	top_00:62:0d (00:20:78 sion 4, src: 10.0.0.57	(10.0.0.5	ed (328 bits) ), Dst: Intel_ce:70:51 (00:02:b3:ce:70:51) 57), Dst: 10.0.0.3 (10.0.0.3)
	er Tength: 20 b erentiated Serv l Length: 52 tification: 0x8 s: 0x02 (Don't	ytes ices Field: 0x00 (DSCF 583 (34179) Fragment)	0x00: Def	fault; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
0000 00	02 b3 ce 70 51	00 20 78 00 62 0d 08	00 45 00	po, x,b,E.
0010 00	34 85 83 40 00	80 06 61 05 0a 00 00	39 0a 00	.4@ a9
0020 00	03 0a 12 01 f6	61 97 f1 83 70 f1 ad	1b 50 18	aрР.
0030 fa	TU 19 52 00 00	00 00 00 00 00 06 0a	08 00 04	R
0040 00	00			

hackers-arise.com

Clicking on any of those packets will allow us to start a more detailed review of the packets. We can see their destination port and protocol (respectively 502 and mbap), expanding the TCP header.



hackers-arise.com

If we scroll down a bit, we will get into the fields of Modbus and Modbus / TCP and read their values there.



hackers-arise.com

Click on the Expression tab next to the filter window to add more complex modbus filters and open the Expression Creator. Within the field name sub-window we will scroll down to the M's before we get to modbus.

Field name	Relation	Value (Protocol)
MIIME multipart - MIIME Multipart Media Encapsu MIIME_FILE - MIIME frile MIDP - Unreliable Multicast Inter-ORB Protocol MIPv6 - Mobile IPv6 / Network Mobility MMS - MMS MMSE - MMS Message Encapsulation MNDP - Mikrotik Neighbor Discovery Protocol Mobile IP - Mobile IP Modbus - Modbus Modbus RTU - Modbus RTU Modbus/TCP - Modbus/TCP Mojito - Mojito DHT	is present == != > < >= <= contains matches	Predefined values:
MoldUDP - MoldUDP     +		Range (offset:length)
E H		

hackers-arise.com

As you can see above there are three (3) field names with modbus within them. Let's extend each and every one and see what they contain. The Modbus / TCP filter includes only fields special to the TCP implementation of modbus. In the original modbus protocol all fields are found in the Modbus protocol.

eld name	Relation	Value (Protocol)
modbus.register.uint32 - Register (UINT32)	is present	
modbus.word_cnt - Word Count	==	Predefined values:
modbus.write_reference_num - Write Reference	!=	
modbus.write_word_cnt - Write Word Count	>	
Modbus RTU - Modbus RTU	<	
mbrtu.crc16 - CRC-16	>=	
mbrtu.unit_id - Unit ID	<=	
Modbus/TCP - Modbus/TCP	contains	
mbtcp.len - Length	matches	
mbtcp.prot_id - Protocol Identifier		
mbtcp.trans_id - Transaction Identifier		
mbtcp.unit_id - Unit Identifier		
🗄 Mojito - Mojito DHT		Range (offset:length)
< III >		

hackers-arise.com

If we are searching for different fields in the Modbus protocol, we will use these fields instead of modbus implementing TCP / IP.

# Modbus Diagnostic Codes Filtering

We can do that by entering; in the filter window, **modbus.diagnostic** code

<u>Eile E</u> dit	View Go Cap	ture <u>Analyze Statistics</u> Telepho	ony Iools Inter	nals <u>H</u>	jelp								
0 0		3 🖹 🗶 🛃 🔍 🔶 🌳 🕯			0,00			36	H				
Filter: mo	dbus.diagnostic_d	ode		Expressi	on Clear A	Apply Save							
ime	Source	Destination	Protocol L	ength	Info								
5.266493	8 10.0.0.57	10.0.0.3	Modbus/	66	Query:	Trans:	0;	Unit:	10,	Func:	8/	1:	Force
5.268888	3 10.0.0.57	10.0.0.3	Modbus/	66	Query:	Trans:	0;	Unit:	10,	Func:	8/	1:	Force
5.271447	10.0.0.57	10.0.3	Modbus/	66	Query:	Trans:	0;	Unit:	10,	Func:	8/	1:	Force
5.889380	10.0.0.57	10.0.3	Modbus/	66	Query:	Trans:	0;	Unit:	10,	Func:	8/	1:	Restar
5.891714	10.0.0.57	10.0.0.3	Modbus/	66	Query:	Trans:	0;	Unit:	10,	Func:	8/	1:	Restar
5.893737	10.0.0.3	10.0.0.57	Modbus/	66	Response:	Trans:	0;	Unit:	10,	Func:	8/	1:	Restar
1.321606	5 10.0.0.57	10.0.0.3	Modbus/	66	Query:	Trans:	0;	Unit:	10,	Func:	8/	1:	Restan
1.323382	10.0.0.3	10.0.0.57	Modbus/	66	Response:	Trans:	0;	Unit:	10,	Func:	8/	1:	Restan
1.263839	10.0.0.57	10.0.3	Modbus/	66	Query:	Trans:	0;	Unit:	10,	Func:	8/	1:	clear
1.265675	5 10.0.0.3	10.0.0.57	Modbus/	66	Response:	Trans:	01	unit:	10.	Func:	8/	1:	clear
(G [B [SEQ [B [PDU	Good Checksum Bad Checksum ACK analysi Bytes in flig Size: 12]	n: False] False] Is] ht: 12]											
Modbus Tran Prot Lenn	TCP saction Ider cocol Identif	ntifier: 0 fier: 0											
Unit B Modbus	Identifier	: 10											
Diag	tion Code: D nostic Code: 1: 0000	Diagnostics (8) Force Listen Only Mode	(4)										

hackers-arise.com

Wireshark retrieves all packets of modbus filled in with diagnostic code If we analyze one of those packets and scroll down to Modbus protocol fields, you can see that this one has a Diagnostic Code = 4 or "Force Listen Only Mode" We might filter on and search for packets with that Diagnostic Code only by creating such a filter;

## modbus\_diagnostic\_code ==4

Wireshark found that only 3 packets contained Diagnostic Code.

Eile Edit View Go	Capture Analyze Statistics	Telephony Iools Int	ternals Help				
0 0 🖌 🔳 🙇	X - X	* * * 7 2 0			5 % 1	II.	
Filter modbus.diagno	stic_code ==4		Expression Clear	Apply Save			
ime Source	Destination	Protocol	Length Info				-
15.266493 10.0.0.	.57 10.0.0.3	Modbus,	/ 00 Query	: Trans:	0; Unit:	10, Func:	8/ 1: Force
15.271447 10.0.0.	.57 10.0.0.3	Modbus	66 Query	: Trans:	0; Unit:	10, Func:	8/ 1: Force
⟨Bad Check B [SEQ/ACK ana [This is a [The RTT t]	sum: False] lysis] n <u>ACK to the segment i</u> o ACK the segment was	in frame: 11) : 0.000427000 seco	m onds]				
[Bytes in [PDU Size: 1	flight: 12]						
Modbus/TCP Transaction Protocol Ide Length: 6 Unit Identif	Identifier: 0 ntifier: 0 ier: 10						
Modbus							
Diagnostic C Data: 0000	ode: Force Listen Only	y Mode (4)					

hackers-arise.com

In some SCADA DoS attacks, the modbus frame with this diagnostic code was used, as it sends a signal to "Power Listen Only" to the PLC and does not send data to the actuators, alarms or other PLCs with which it communicate.Could have disastrous consequences!

# Filtering Suspicious Modbus Packets

We can build a lot of different filters that are looking for packets that meet certain field criteria. Here we search for "restart communications" by creating the following filter;

modbus.diagnostic\_restart\_communication\_option

```
Filter: modbus.diagnostic.restart_communication_option

    Expression... Clear Apply Save

                             Destination
                                                 Protocol Length Info
lime
          Source
25.889380 10.0.0.57
                             10.0.0.3
                                                 Modbus/
                                                           66
                                                                 Query: Trans:
                                                                                    0; Unit: 10, Func:
                                                                                                          8/ 1: Restart
25.891714 10.0.0.57
                                                 Modbus/
                                                                 Query: Trans:
                                                                                   0; Unit: 10, Func: 8/ 1: Restart
                             10.0.0.3
                                                           66
25.893737 10.0.0.3
                                                                                                         8/ 1: Restart
                             10.0.0.57
                                                 Modbus/
                                                           66 Response: Trans:
                                                                                    0; Unit: 10, Func:
31.321606 10.0.0.57
                             10.0.0.3
                                                 Modbus/
                                                           66
                                                                 Query: Trans:
                                                                                    0; Unit: 10, Func: 8/ 1: Restart
31.323382 10.0.0.3
                             10.0.0.57
                                                 Modbus/ 66 Response: Trans:
                                                                                 0; Unit: 10, Func: 8/ 1: Restart
٠ 📃
  Checksum: 0x1931 [validation disabled]
       [Good Checksum: False]
       [Bad Checksum: False]
  □ [SEQ/ACK analysis]
      [Bytes in flight: 12]
    [PDU Size: 12]
Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 10
Modbus
    Function Code: Diagnostics (8)
    Diagnostic Code: Restart Communications Option (1)
    Restart Communication Option: Leave Log (0x0000)
```

hackers-arise.com

You may also use this diagnostic code to trigger a DoS attack, as it sends a signal to restart the PLC.

## **Reading Registers**

Look for packets that read 16-bit registry contents by creating a filter such as;

### modbus.register.uint16

hackers-arise.com

These packets indicate that an attacker attempts to read the data values in the register to understand its pre-attack role (a form of recognition) or add them to something with malicious content and effect.

With Wireshark we can catch data packets to allow a more thorough analysis. This tool is geared towards tracking data traffic within a network. Such a tool allows the user to scan for network protocol errors and issues on his / her own computer. Accordingly, Wireshark is also gaining popularity within information technology and network-internal communication, as the identification of irregularities will prevent risks to the Computer and its components. From a security perspective it must be considered that such a system is helpful in detecting and preventing hacker attacks. Especially among people working in the industry, this can be beneficial if sensitive data are stored on their computer which should never touch third parties.

Wireshark can also be used to assess SCADA / ICS attacks if you know what to look for. Any security engineer working in SCADA / ICS technology must be knowledgeable in Wireshark or other Protocol Analyzers along with the details of the communication protocol used at their facility for this type of research to be properly prepared. This strong approach helps us analyze network traffic to the finest degree in granular. Improving your understanding of this process will have to pay major dividends in your forensic career!

### References

```
hackers-arise.com. (n.d.).
```

Retrieved from hackers-arise.com/post/2018/09/27/network-forensics-part-2-detectingand-analyzing-a-scada-dos-attack.

```
malware-traffic-analysis (n.d.).
```

Retrieved from malware-traffic-analysis.net/

```
hackers-arise.com. (n.d.).
```

Retrieved from hackers-arise.com/post/2018/10/31/network-forensics-wireshark-basicspart-2

```
hackingarticles.in. (n.d.).
```

```
Retrieved from hackingarticles.in/network-packet-forensic-using-wireshark/
```

```
kunbus.com. (n.d.).
```

```
Retrieved from kunbus.com/wireshark.html.
```

```
nystec.com. (n.d.).
```

```
Retrieved from nystec.com/insights/network-forensics-101/
```

```
resources.infosecinstitute.com. (n.d.).
```

```
Retrieved from resources.infosecinstitute.com/category/certifications-training/network-traffic-analysis-for-incident-response/how-to-use-traffic-analysis-for-wireshark/. resources.infosecinstitute.com. (n.d.).
```

```
Retrieved from resources.infosecinstitute.com/category/certifications-training/network-traffic-analysis-for-incident-response/how-to-use-traffic-analysis-for-wireshark/.
```
### Analyzing the Trickbot Malware Layer 3/4

<sup>By</sup> Nitin Sharma

# "If you know the enemy and know yourself, you need not fear the result of a hundred battles."

- The Art of War, Sun Tzu

In the modern world, Cybercrime landscape has changed a lot considering the cyberwarfare from malware perspective. Early malwares were primitive, often spreading entirely offline via floppy disks carried from computer to computer by human hands. As networking and the Internet matured, malware authors were quick to adapt their malicious code and take advantage of the new communication medium.



Photo by The Digital Artist, Pixabay [1]

It is getting more and more difficult to devise strategies for detection of malwares in the computer systems. There are so many phishing campaigns, botnets, C2 servers currently interacting with numerous legit systems in an unauthorized manner. Creating a havoc in the business world, these sophisticated pieces of malware can do even more damage when combined with each other. One such wreaking example is "Emotet, Ryuk, Trickbot: Loader-Ransomware-Banker Trifecta" [2]. This has already caused millions of dollars in damages and ransoms paid.

In this paper, we will be discussing about Trickbot malware as a banking trojan, its spamming and malware delivery process, detection, confinement strategies and much more. Evolution of Trickbot till date to its latest version and modular enhancements will be the focus for this paper.

# Trickbot: The Beginning

First seen in 2016, Trickbot is a malware that steals system information, login credentials and other sensitive data from vulnerable Windows hosts.

Trickbot is one of the most recent banking trojans with many of its original features inspired by Dyre, another banking Trojan. According to Fidelis Cybersecurity <sup>[3]</sup>, the loader for Trickbot, which has been around since at least September 2016, uses the same



custom crypter as Cutwail, a favorite of the group which spread Dyre via spam and social engineering campaigns. The loader is responsible for determining whether it's running on a 32- or 64-bit system. After conducting a bit check, it downloads the resources necessary to load up the Trickbot malware.

# **Trickbot: Capabilities**

Trickbot has evolved a lot since its first appearance in 2016.

- 1. Stealing banking credentials (man-in-the-browser attack).
  - a. Static Injection Involves replacing the banking site's legitimate login page with a fake one that looks almost exactly like it.
  - b. Dynamic Injection/Server-Side Injection Redirects the web browser to a server under the trojan operator's control whenever the user enters the URLs for the targeted banking sites.
- 2. Stealing from Bitcoin Wallets.
- 3. With the help of different modules, can get local and other user account details, tax information, system, and network information and so on.
- 4. Connecting infected devices to malicious, criminally controlled networks over the Internet, giving criminals full control of them
- 5. Spread across a victim's network by infecting other devices, including those on trusted domains (known as lateral movement), often using SMB shares.
- 6. Downloading further malicious files such as Remote Access Tools, VNC clients and ransomware.

# **Trickbot: Infection Vectors**

According to Malpedia<sup>[4]</sup>, the important infection vector paths for Trickbot are:

- 1. Phish → Link MS Office → Macro Enabled → Downloader → Trickbot
- 2. Phish → Attached MS Office → Macro Enabled → Downloader → Trickbot
- 3. Phish → Attached MS Office → Macro enabled → Trickbot installed



Trickbot Phishing Mail based on Office 365 ATP data, Microsoft Security Intelligence [5]

Trickbot is often distributed through malspam. Emails from these campaigns contain links to download malicious files disguised as invoices, images, or documents. These files may be Windows executable files for Trickbot, or they may be some sort of downloader for the Trickbot executable. In some cases, links from these emails return a zip archive that contains a Trickbot executable or downloader <sup>[6]</sup>. There are a lot of malspam campaigns seen luring COVID-19. According to Microsoft Security Intelligence, Trickbot is the most prolific malware operation using COVID-19 themed lures. They have used several hundreds of unique macro-laced document attachments in emails that pose as message from a non-profit offering free COVID-19 test. It has been found that the macro uses CHOICE.EXE to wait 20 seconds before downloading the info-stealing payload. Trickbot campaigns are known to delay malicious activities to evade emulation or sandbox analysis.

# Flowchart from a Trickbot infection from malspam in September 2019 <sup>[6]</sup>

Trickbot is also found to be frequently distributed through other malware. It is commonly seen as follow up malware to Emotet infections and sometimes from IcedID and Ursnif infections.



Flowchart for Emotet with Trickbot activity<sup>[6]</sup>

# Trickbot: Symptoms of Infection

Once an endpoint is infected with Trickbot, there will not be any significant change to be observed. However, a network admin will likely see changes in traffic flows or attempts to reach out to blacklisted IPs and domains, as the malware will communicate with Trickbot's C2 server to exfiltrate data and receive tasks. The traffic with C2 server is found to be encrypted over TCP port 443, 447, or 449 being GET/POST requests.

## How Trickbot works

We have already observed the ways, how Trickbot is disseminated via malspam campaigns and secondary payload by other malwares. The Multi-State Information Sharing and Analysis Center (MS-ISAC) has released a security primer on Trickbot malware<sup>[7]</sup>.

The malspam campaigns that deliver Trickbot use third party branding familiar to the recipient. The emails typically include an attachment, such as a Microsoft Word or Excel document. The opened attachment will prompt the user to enable macros, which executes a VBScript to run a Powershell script to download the malware. Trickbot runs checks to ensure it is not in the sandbox environment and then attempts to disable antivirus programs, such as Microsoft's Windows Defender. Once executed, Trickbot redeploys itself in the "%AppData%" folder and creates a scheduled task that provides persistence <sup>[8]</sup>.

Trickbot sends HTTP requests to the following websites to determine the infected host's public IP address:

- hxxp://myexternalip.com/raw
- hxxp://api.ipify.org
- hxxp://icanhazip.com
- hxxp://bot.whatismyipaddress.com
- hxxp://ip.anysrc.net/plain/clientip

At this point, Trickbot starts receiving instructions from the command and control (C2) server and is ready to download modules which are sent with a configuration file. The modules are delivered as Dynamic Link Libraries. After receiving the infected host's system information, the initial Trickbot C2 sends an expiration time and a new IP address that will be used to download further modules. The C2 servers constantly change and the Trickbot infection is updated with this new information. Trickbot uses HTTP/HTTPS GET and POST requests to download modules and report stolen information/credentials to the C2 server. Trickbot uses web injects - Static and Dynamic

(as already discussed in Trickbot Capabilities) to steal financial information from online banking sessions to defraud its victims. Trickbot's distributors are using group tags (gtags) to uniquely identify specific Trickbot campaigns. The gtag and a unique bot identifier are included in the URIs when Trickbot communicates with its C2 servers.



The following is an overview of common Trickbot modules and configuration files, but this not an exhaustive list since Trickbot is constantly adding new features.

Artifacts for Trickbot modules on an infected Windows 7 client<sup>[10]</sup>

Visual Representation	of Trickbot and	d its modules <sup>[9]</sup>
-----------------------	-----------------	------------------------------

🌒 🕞 🗣 📙 « AppData 🕨	Roaming	▶ data ▶ 🔹	Search date
Organize • Include in I	ibrary • Share with •	New folder	
Name	Date modified	Туре	Size
👃 injectDll64_configs	1/14/2020 8:35 PM	File folder	
👃 networkDll64_configs	1/14/2020 8:27 PM	File folder	
l pwgrab64_configs	1/14/2020 7:48 PM	File folder	
👃 tabDll64_configs	1/14/2020 8:47 PM	File folder	
importDll64	1/14/2020 8:18 PM	File	7,516 KB
injectDll64	1/14/2020 8:35 PM	File	476 KB
mshareDll64	1/14/2020 8:43 PM	File	17 KB
mwormDll64	1/14/2020 8:43 PM	File	27 KB
networkDll64	1/14/2020 8:27 PM	File	24 KB
pwgrab64	1/14/2020 7:48 PM	File	1,464 KB
tabDll64	1/14/2020 8:47 PM	File	822 KB

- Banking Information Stealers
  - **LoaderDll/InjectDll** Monitors for banking website activity and uses web injects (e.g. pop ups and extra fields) to steal financial information.
  - *Sinj* This file contains information on the online banks targeted by Trickbot and it uses redirection attacks (also known as web fake injections).
  - **Dinj** This file contains information on the online banks targeted by Trickbot and it uses server-side web injections. (See more in Trickbot Targeting)
  - Dpost Includes an IP address and port for stolen banking information. If the user enters banking information for one of the listed banks, the information is sent to the dpost IP address. Most of the data exfiltrated by TrickBot is sent to the dpost IP address.
- System/Network Reconnaissance
  - *Systeminfo* Harvests system information so that the attacker knows what is running on the affected system.
  - *Mailsearcher* Compares all files on the disk against a list of file extensions.
  - *NetworkDll* Collects more system information and maps out the network.
- Credential and User Information Harvesting
  - ModuleDll/ImportDll Harvests browser data (e.g. cookies and browser configurations)
  - **DomainDll** Uses LDAP to harvest credentials and configuration data from domain controller by accessing shared SYSVOL files.
  - OutlookDll Harvests saved Microsoft Outlook credentials by querying several registry keys.
  - SqulDll Force-enables WDigest authentication and utilizes Mimikatz to scrape credentials from LSASS.exe. The worming modules use these credentials to spread Trickbot laterally across networks.
  - *Pwgrab* Steals credentials, autofill data, history, and other information from browsers as well as several software applications.
- Network Propagation
  - WormDll and ShareDll These are worming modules that abuse Server Message Block (SMB) and Lightweight Directory Access Protocol (LDAP) to move laterally across networks.
  - *TabDll* Uses the EternalRomance exploit (CVE-2017-0147) to spread via SMBv1.



### TRICKBOT PROPAGATION TO DOMAIN CONTROLLER FROM SEPTEMBER 2019 THROUGH MARCH 2020



### **Trickbot Targeting**

Trickbot target information has been revealed in a research by @GarWarner<sup>[12]</sup>, where the configuration files of Trickbot were decoded to see what the current collection of URLs in the DINJ file is targeting. The DINJ file for Trickbot contain lists of URL patterns labeled with markup tags. There were 84 "igroups" containing 329 URL patterns, targeting 131 named domains.



DINJ file breakdown <sup>[12]</sup>

- The most common target was Japanese banks and financial institutions. US Banks were second in popularity and then the German Banks.
- Many other targets were found related to Brokerages, Big Retails, Crypto-Currency Exchanges/Companies, Payroll companies, etc.

### Preventive Actions for Trickbot Infection

- Provide social engineering and phishing training to employees.
- If you do not have a policy regarding suspicious emails, consider creating one and specify that all suspicious emails should be reported to the security and/or IT departments.
- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
- Apply applicable patches and updates immediately after appropriate testing.
- Implement filters at the email gateway for emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- To lower the chance of spoofed or modified emails, implement Domain Message Authentication Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards. (CIS Subcontrol 7.8)
- Organizations should consider using application whitelisting technology on all assets to ensure that only authorized software executes, and all unauthorized software is blocked from executing on assets (CIS Subcontrol 2.7). Organizations should also ensure that the application whitelisting software only allows authorized, digitally signed scripts (such as \*.ps1, \*.py, macros, etc.) to run on a system (CIS Subcontrol 2.9).
- Adhere to the principal of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.
- Implement a centrally managed, up-to-date anti-malware solution (CIS Subcontrol 8.2). In addition to valuable preventive and corrective capabilities, detective controls provided by anti-malware software are beneficial in providing awareness of any threats which may become active within the environment.
- If not already being done, consider implementing an Intrusion Detection System (IDS) to detect command and control (C2) activity and other potentially malicious network activity, such as the MS-ISAC's Albert system.
- Ensure that systems are hardened with industry-accepted guidelines, such as those provided by the CIS Benchmarks division. (cisecurity.org/cis-benchmarks/)
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against Network Propagation modules used by TrickBot.

### How to tackle Trickbot Infections

- Disable Internet access at the affected site to help minimize the extent of exfiltration of credentials associated with external, third-party resources.
- Review impacted subnets to identify multi-homed systems which may adversely impact containment efforts. Also, consider temporarily taking the network offline to perform identification, prevent reinfections, and stop the spread of the malware.
- Identify, shutdown, and take the infected machines off the network.
- Heighten monitoring of SMB communication or outright block it between workstations and configure firewall rules to only allow access from known administrative servers.
- Assess the need to have ports 445 (SMB) open on systems and, if required, consider limiting connections to only specific, trusted hosts.
- Start with remediation of multi-homed systems (e.g. Domain Controller, File Server) as these can communicate across Virtual Local Area Networks (VLANs) and can be a potential means for spreading malware.
- Create clean VLANs that do not have access to infected VLANs. After the systems have been reimaged or restored from a known good backup, place them on the clean VLAN.
- Do not login to infected systems with domain or shared local administrator accounts. This is the best remediation strategy since TrickBot has several ways of gaining access to credentials.
- As TrickBot is known for scraping both domain and local credentials, it is recommended that a network-wide password reset take place. This is best done after the systems have been cleaned and moved to the new VLAN. This is recommended so new passwords are not scraped by the malware.
- Apply host-based isolation via Windows Firewall Group Policy Objects (GPOs), host-based intrusion detection system/network intrusion detection system (HIDS/NIDS) products, a Private Virtual Local Area Network (pVLAN), or similar means to help mitigate propagation.
- Determine the infection vector (patient zero) to determine the root cause of the incident.

# Walkthrough: Trickbot PCAP Analysis

In this walkthrough, we will discuss about Wireshark GUI briefly and analyze a small PCAP file for Trickbot examination. Feel free to go through the previous in-depth article about Trickbot malware.

Pre-requisites for this walkthrough to follow along:

- 1. Kali Linux VM where Wireshark comes inbuilt.
  - a. Kali 2019 (5.2.0-kali2-amd64)
  - b. Wireshark 3.0.3
- 2. Trickbot PCAP Exercise Catbomber<sup>[13]</sup>

Wireshark is a free and open-source packet analyzer release under the terms of GNU General Public License, used for network troubleshooting, analysis, software and communications protocol development, and education. It is a cross platform tool designed with Qt widget toolkit widely used to analyze PCAP files in its GUI version. There is also a terminal-based (non-GUI) version called TShark.<sup>[14]</sup>

### Wireshark Calibration

Before starting with Trickbot PCAP analysis, we need to calibrate the Wireshark GUI platform with specific attributes/fields.

1. Start with checking Wireshark version. For this walkthrough, we prefer to go with 3.x versions as there are some differences with older 2.x versions.



2. For calibration process, we will set the capture to "eth0" interface of our VM. Double click on "eth0" and proceed.

	The Wires	hark Network Analyzer		000
<u>File</u> <u>E</u> dit <u>\</u>	<u>/</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telepho	ny <u>W</u> ireless <u>T</u> ools <u>H</u> elp		
	+ 6. + + 2 3 4 6 3	* <b>_</b> @ @ @	<u> </u>	
Apply a dis	splay filter <ctrl-></ctrl->		Expression +	basic basic
	Welcome to Wireshark			
	Open			
	/root/Desktop/trickbot-apalysis/2020-05-28-t	traffic-analysis-exercise pcap (812	7 KB)	
	Capture			
	using this filter		All interfaces shown *	
	danig this fitter.		Aumenaces shown	
	ethO			
	eth1			
	eth2 Loopback: lo			
	any	m	my	
	nflog			
			1.01	
	Learn			
	User's Guide 🔸 Wiki 🔸 Questions and Answe	rs 🕖 Mailing Lists		
	You are running Wireshark 3.0.3 (Git v3.0.3 page	:kaged as 3.0.3-1).		
7 Ready to	a load or capture	No Packets	P	rofile. Default
. icuary ic	a court of capital c	Norackets		ionici Deluute

3. In the Firefox Browser of Kali VM, I have searched for some websites like, "informationwarfarecenter.com", "cve.circle.lu", "Netflix", etc. to generate some dummy traffic for adjusting attributes in Wireshark.

Display	File Edit View Go Capture Analyze	Statistics Telephony	Wireless Tools Help	
Display	🛋 🔳 🧟 💿 📙 🛅 🗙 🔄 🔍 👄	🗢 🕾 T 🛓 📃 🔳	0,0,0,1	
Filter	Apply a display filter <ctrl-></ctrl->			
[Filter	No. Time Source	Destination Pr	otocol Length Tofo	
Toolbar]	343 65.142415 192.168.0.21	174.129.249.228 T	CP 66 40555 → 80 [ACK]	Seg=1 Ack=1 Win=5888 Len=0 TSval=49
	344 65.142715 192.168.0.21	174.129.249.228 H	TTP 253 GET /clients/net	lix/flash/application.swf?flash_ver
	345 65.230738 174.129.249.228	192.168.0.21 T	IP 66 80 → 40555 [ACK]	Seq=1 Ack=188 Win=6864 Len=0 TSval=
	346 65.240742 174.129.249.228	192.168.0.21 H	TTP 828 HTTP/1.1 302 Move	ed Temporarily
Column	347 65.241592 192.168.0.21	174.129.249.228 T	CP 66 40555 → 80 [ACK]	Seq=188 Ack=763 Win=7424 Len=0 TSva
Column D: 1	→ 348 65.242532 192.168.0.21	192.168.0.1 D	IS 77 Standard query 0:	(2188 A cdn-0.nflximg.com
Display	- 349 65.2/68/0 192.168.0.1	192.168.0.21 DI	15 489 Standard query r	Sponse 0x2188 A cdn-0.nflximg.com C
[Packet	350 65.2//992 192.166.0.21	102 168 0 21 T	P 74 57065 → 80 [STN]	ACK1 Seg-0 Ack-1 Win-5702 Len-0 MSS
List Panel	352 65,298396 192,168,0,21	63.80.242.48 T	P 66 37063 → 80 [ACK]	Seg=1 Ack=1 Win=5888 Len=0 TSval=49
List Fallej	353 65,298687 192,168,0,21	63.80.242.48 H	TTP 153 GET /us/nrd/clie	ts/flash/814540.bun HTTP/1.1
	354 65.318730 63.80.242.48	192.168.0.21 T	CP 66 80 → 37063 [ACK]	Seg=1 Ack=88 Win=5792 Len=0 TSval=3
	355 65.321733 63.80.242.48	192.168.0.21 T	IP 1514 [TCP segment of a	reassembled PDU]
	<			
Frame Details [Packet Details Pane]	<pre>&gt; Ethernet II, Src: Globalsc_00:3b &gt; Internet Protocol Version 4, Src &gt; User Datagram Protocol, Src Port &gt; Domain Name System (response)</pre>	:0a (f0:ad:4e:00:3b): : 192.168.01, Dst: : 53 (53), Dst Port: response, No error class IN	9a), Dst: Virio_14:8a:e1 (00:15 92.168.0.3 34036 (34036)	:9d:14:8a:e1)
Hexadecimal View [Packet Bytes Pane]	Authoritative nameservers     Authoritative nameservers     Authoritative nameservers     Authoritative nameservers     O220 00 15 00 35 84 f4 01 c7 83     O330 00 04 00 90 09 09 53 64     O44 07 86 96 d5 70 35 6f 6d 00     O55 00 01 00 00 05 29 00 22     O666 07 6e 65 74 66 6c 69 78 03     O77 55 73 75 69 74 65 03 6e 65     O     ✓ Identification of transaction (dns.id), 2	3f 21 80 81 80 00 01 6e 2d 30 07 6e 66 6c 00 01 00 01 c0 0c 00 06 69 6d 61 67 65 73 63 6f 6d 09 65 64 67 74 00 c0 2f 00 05 00		Packets: 10299 · Displayed: 10299 (100.0%)

4. In the Column Display, right click on any of the column header to bring up the column header menu and set/check the display to show only following attributes: Time, Source, Destination, and Info.

Time Source	Alian Left		Info
145.103572662 10.0. 145.103945390 216.5	3.1 3.2 Align Center	95	45610 → 80 [FIN, ACK] Seq=4 80 → 45610 [ACK] Seq=702 Ac
149.501531682 13.10	🔼 🗌 Align Right		443 → 49328 [RST, ACK] Seq=
163.457170826 216.5 163.457216968 10.0.	3.2 3.1 Column Preferences	95	80 → 45610 [FIN, ACK] Seq=7 45610 → 80 [ACK] Seq=439 Ac
168.703991496 PcsCo	npi Edit Column	35:02	Who has 10.0.3.2? Tell 10.0
100.704101505 Realt	Resize To Contents	11:02	10.0.3.2 15 at 52.54.00.12.
▶ Frame 629: 60 byt	es 🗌 Resolve Names	tes cap	tured (480 bits) on interface
<ul> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> </ul>	V No.	1:12:35: .8, Dst	02), Dst: PcsCompu_ba:f1:d2 ( : 10.0.3.15
Transmission Cont	ro. 🗸 Time	Dst Po	rt: 40304, Seq: 3414, Ack: 76
	✓ Source		
1 0000 08 00 27 bo 1	✓ Destination	00 45 00	
0010 00 28 58 55 0	0 Protocol	98 0a 00	0 (XU · @ [·· ···
0020 03 0f 01 bb 9 0030 ff ff b6 f3 0	d Length	5d 50 10	Ðp. ₩.t]]P.
	✓ Info		
🔘 🝸 eth1: <live captur<="" td=""><td>e ir Remove This Column</td><td>Packe</td><td>ets: 1478 · Displayed: 1478 (100.0%)</td></live>	e ir Remove This Column	Packe	ets: 1478 · Displayed: 1478 (100.0%)

5. In the same menu, select "Column Preferences" then "Columns". Click on "+" button to add new columns for "Source Port" and "Destination Port".

			(	Capturing from eth1		
			Wiresha	rk · Preferences		
•	Appearance Columns Font and Colors Layout Capture Expert Filter Buttons Name Resolution Protocols RSA Keys Statistics Advanced	Displayed	Title No. Time Source Destination Protocol Length Info Source Port New Column	Type Number Time (format as specified) Source address Destination address Protocol Packet length (bytes) Information Src port (unresolved) Number	Fields	
		4				

- a. Rename the "New Column" title as "Source Port" and select "Src port (unresolved)" from the "Type" drop down where "Number" is present.
- b. Similarly, add new column using "+" button, rename the column title as "Destination Port" and select "Dest port (unresolved)"

After completing this step, you will be able to see the Column Display Headers as below.

												Wir	resh	ark									
File	<u>E</u> dit	Vie	w	<u>G</u> o	Cap	oture	<u>A</u>	nalyze	<u>S</u> tat	istic	s T	elep	hon	y Y	<u>N</u> irel	ess ]	<u>r</u> ools	Ŀ	lelp				
			۲	Ð	1		<	0			• .	Ç	+	•			•	2	Q	Q	8		
App	oly a d	lispla	ay fi	lter .	<c< td=""><td>trl-/</td><td>&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>C</td><td>•</td><td>E&gt;</td></c<>	trl-/	>														C	•	E>
	Pack	et lis	it	~	Na	arrov	v & \	Vide		×		Case	sen	sitiv	e D	isplay	filte	r		•		Fi	nd
Time			S	ourc	e			Source	Port	t I	Dest	inati	on		De	stinat	ion P	ort		Info			
145.1	0357	266	2 1	0.0	.3.	15			456	10	216	.58.	200	.1					80	456	10 -	80	[F
145.1	.0394	539	0 2	16.	58.	200.	1			80 :	10.0	9.3.	15					45	610	80 -	+ 45	610	[A
149.5	0153	168	21	3.1	07.	246.	.10		4	43 :	10.0	9.3.	15					49	328	443	- 4	932	8 [
163.4	5717	082	6 2	16.	58.	200.	1			80	10.0	9.3.	15					45	610	80 -	→ 45	610	[F
163.4	5721	696	8 1	0.0	.3.	15			456	10	216	.58.	200	.1					80	456	10 -	80	[A
168.7	0399	149	6 P	csC	omp	u_ba	a :			1	Real	Ltek	(U_1	2:						Who	has	10	.0.
168.7	0418	150	5 R	eal	tek	U_12	2:			1	Pcs	Comp	u_b	a:						10.0	9.3.	2 i	s a
4																							
<ul> <li>Fra</li> <li>Eth</li> <li>Int</li> <li>Tra</li> </ul>	ame 6 nerne cerne ansmi	29: t I t P ssi	60 I, rot on	by Src oco Con	tes : R l V tro	on eal ers: 1 Pi	wir tekl ion roto	re (48 J_12:3 4, Sr ocol,	0 b: 5:02 c: : Src	its) 2 (5 192 Por	), 6 52:5 .124 rt:	0 b 4:0 .24 443	yte 0:1 9.8 , D	s c 2:3 , D st	aptu 5:02 st: Port	red 2), D 10.0 10.0	(480 st: .3.2 304,	9 b Pc 15 , S	its sCo eq:	) on mpu_ 341	int ba:f 4, A	erf 1:d .ck:	ace 2 ( 76
4																							
0000	08	00	27	ba	f1	d2	52	54 0	9 12	35	02	08	00	45	00	* *	1. 1. 1	RT	· · 5	E			
0010	00	28	58	55	00	00	40	06 5	o e7	c0	7c	f9	08	0a	00	• ()	(U	@•	[ • • ]	1	*		
0020	03	0f	01	bb	9d	70	0e	f9 0'	f 57	17	74	5d	5d	50	10	4. 4	• • p		- W -	t]]F			
0030	ff	ff	b6	f3	00	00	00	00 0	9 00	00	00												
0 7	Rea	ady t	o lo	ad o	r cap	oture	e e							Pa	ckets	1490	·Dis	spla	yed:	1490	(100	.0%	)

6. Now, let us change the Time Column format. Click "View" → "Time Display Format".
a. Select "UTC Date and Time of Day (1970-01-01 01:02:03.123456)" and "Seconds".

✓ Main Toolbar		Internals	
Eilter Toolbar		Show Packet in New <u>W</u> indow	
Wireless Toolbar		Reload as File Format/Capture	0
✓ Status Bar	Date and Time of Day (1970-01-01 01:02	2:03.123456)	Ctrl+Alt+1
Eull Screen	Year, Day of Year, and Time of Day (1970	)/001 01:02:03.123456)	
✓ Packet List	Time of Day (01:02:03.123456)		Ctrl+Alt+2
✓ Packet <u>D</u> etails	Seconds Since 1970-01-01		Ctrl+Alt+3
✓ Packet Bytes	Seconds Since Beginning of Capture		Ctrl+Alt+4
Time Display For	Seconds Since Previous Captured Packet	t	Ctrl+Alt+5
Name Resol <u>u</u> tio	Seconds Since Previous Displayed Packe	t	Ctrl+Alt+6
Zoom	UTC Date and Time of Day (1970-01-01	01:02:03.123456)	Ctrl+Alt+7
Expand Subtrees	UTC Year, Day of Year, and Time of Day (	(1970/001 01:02:03.123456)	
Collapse Subtree	UTC Time of Day (01:02:03.123456)		Ctrl+Alt+8
Expand All	Automatic (from capture file)		
Collapse All	Seconds		
Colorize Packet I	Tenths of a second		
Coloring Rules	Hundredths of a second		
Colorize Convers	Milliseconds		
Reset Lavout	Microseconds		
Resize Columns	Nanoseconds		
C Z Ready to lo	Display Seconds With Hours and Minute	s	

7. There is an important custom column we require to get the Host information. For this, apply a display filter as "*http.request*" and examine the frame for "Hypertext Transfer Protocol". Expand the same to reveal "Host:" which is HTTP host name. Right click the same and select "Apply as Column" in menu appeared.

	Expand Subtrees	00
<u>File Edit View Go Capture Analyze</u>	Collapse Subtrees	lelp
	Expand All	Θ 0 💷
	Collapse All	
http.request	Apply as Column	• Expression +
Time Source	Apply as Filter	on Port Info 🔶
2020-06-12 08:41:49 10.0.3.15	Apply as filler	80 Reques
2020-06-12 08:41:49 10.0.3.15	Prepare a Filter	80 Reques
2020-06-12 08:42:35 10.0.3.15	Conversation Filter >	80 Reques
2020-06-12 08:42:35 10.0.3.15	Colorize with Filter	80 Reques
2020-06-12 08:42:35 10.0.3.15	Follow >	80 Reques
2020-06-12 08:42:56 10.0.3.15	Copy	80 GET / C-
•	Show Dacket Butes	• •
Frame 4241: 487 bytes on wire	Show Packet Bytes	B96 bits) on in▲
Ethernet II, Src: Pcscompu_ba:1 Internet Protocol Version 4 St	Export Packet <u>B</u> ytes	altekU_12:35:02
<ul> <li>Transmission Control Protocol,</li> </ul>	Wiki Protocol Page	q: 868, Ack: 14
<ul> <li>Hypertext Transfer Protocol</li> </ul>	Filter Field Reference	
POST /gts101 HTTP/1.1\r\n Host: ocsp.pki.goog\r\n	Protocol Preferences	
User-Agent: Mozilla/5.0 (X11	Decode As	00101 Firefox/6
Accept: text/html,applicatio	Ce to Unked Decket	*/*;q=0.8\r\n
Accept-Language: en-US.en:g=	Go to Linked Packet	• • •
0000 52 54 00 12 35 02 08 00 2	Show Linked Packet in New Window	'Е.
0010 01 d9 c5 96 40 00 40 06 c5	7b 0a 00 03 0f d8 3a@.@.	·{····:
0030 f9 8a af d8 00 00 50 4f 53	54 20 2f 67 74 73 31	ST /ats1

8. The next display header column, we would like to have is "Server Name". For this, apply a display filter as "*tls.handshake.type* == 1".

	Expand Subtrees	00
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatist	Collapse Subtrees	
	<u>E</u> xpand All	X C
	Collapse All	
tls.handshake.type = = 1	Apply as Column	ession +
Time Source Source	Apply as Filter	Host
2020-06-12 08:42:13 10.0.3.15	Prepare a Filter	443
2020-06-12 08:42:13 10.0.3.15 2020-06-12 08:42:14 10.0.3.15	Conversation Filter	443 443
2020-06-12 08:42:16 10.0.3.15	Colorize with Filter	143
2020-06-12 08:42:35 10.0.3.15	Follow >	443
2020-06-12 08:42:35 10:0:3:15	Сору	443
Extensions Length: 407 - Extension: server_name (len=34 Type: server_name (0) Length: 34 - Server Name Indication exter Server Name list length: Server Name Type: host_nam Server Name length: 29	Show Packet Bytes Export Packet <u>By</u> tes Wiki Protocol Page Filter Field Reference Protocol Preferences	
Server Name: pagead2.goog.	Decode <u>A</u> s	
<ul> <li>Extension: extended master sec</li> </ul>	Go to <u>L</u> inked Packet	• • •
00a0         01         00         01         97         00         00         02         00         20         00           00b0         65         61         64         32         2e         67         6f         67         6c         65           00c0         63         61         74         69         6f         6e         2e         63         6f         6d         00           00d0         00         01         00         00         0a         00         0c         00         0c         00         1c	Show Linked Packet in New Window           5         73         79         6e         64         69         ead2.goo glesy           5         17         00         00         ff         01         cation.c om            1         00         17         00         18         00	hag ndi

b. Examine the frame details for "Handshake Protocol: Client Hello"  $\rightarrow$  "Extension: server\_name"  $\rightarrow$  "Server Name Indication extension"  $\rightarrow$  "Server Name:". Apply this "Server Name:" as column by right click in the appeared menu as above.

📕 htt	p.re	que	st o	r tls.handshake.type = = 1						×	Expressi
Title:	me	Ту	pe:	Custom	•	Fields:	me	Occurre	nce:	0	Scancel
ition P	ort		Hos	st	Server Nan	ne		•	Info		
		80	int	formationwarfarecenter.com	ľ				GET	/1	mages/header
		80	int	na.amazon-adsystem.com					GET	/e.	/1r?t=cybers
		80	003	sp.pki.goog	5				Reg	ues	t
	4	143			adservic	e.goog	le.	com	Cli	ent	Hello
	4	443			apis.goo	gle.co	m		Cli	ent	Hello
	4	443			cve.circ	l.lu			Cli	ent	Hello
4	4	143			cve.circ	1.lu			Cli	ent	Hello

c. The calibration is complete now. Stop the capture pushing the red square "Stop Capturing" button from the Main Toolbar. We are ready to ride the Wireshark fun.

An email with a malicious

Office document somehow

gets past your mail filters.

Microsoft Office disables macros and provides a

security warning.

warning and enable macros.

### Trickbot PCAP Analysis – Scenario

There is a Trickbot infection in an Active Directory (AD) environment where the infection spreads to the Domain Controller (DC).

LAN segment data:

- LAN segment range: 10.5.28.0/24 People disregard the security
- Domain: catbomber.net
- Domain Controller: 10.5.28.8 Catbomber-DC
- LAN segment gateway: 10.5.28.1
- LAN segment broadcast address: 10.5.28.255

#### **Questions:**

- 1. Based on the Trickbot infection's HTTP POST traffic, what is the IP address, hostname and user account name for the infected Windows client?
- 2. What is the other user account name and other Windows client host name found in the Trickbot HTTP POST traffic?
- 3. What is the infected user's email password?
- 4. Two Windows executable files are sent in the traffic. What are the SHA256 file hashes for these files?

#### Analysis:

- 2. Load the PCAP file into Wireshark.
  - a. Click "File"  $\rightarrow$  "Open"  $\rightarrow$  <PCAP File>
  - b. Select the <PCAP File> (here it is the one highlighted in blue) and open it.
  - c.

	Wiresh	ark · Open Captu	re File					0
Look in:	Toot/Desktop/trickbot-analy	/sis		• +	+ 4			
Comput	er Name		Size	Туре	Date N	/odifie	ed	
root	Cthers			Folder	6/19/2	0 8:11	AM	
1000	📠 2020-05-28-trafficlysi	s-exercise.pcap	7.94 MiB	pcap File	6/1/20	3:43	PM	
	2020-05-28-traffics-e	xercise.pcap.zip	5.86 MiB	zip File	6/12/2	0 2:52	PM	
						-		
File <u>n</u> ame:	2020-05-28-traffic-analysis-ex	ercise.pcap					<u>■</u> 0p	en
File <u>n</u> ame:	2020-05-28-traffic-analysis-ex	ercise.pcap					■ <u>O</u> p <u>© C</u> ar	oen Icel
File <u>n</u> ame: Files of type:	2020-05-28-traffic-analysis-ex All Files	ercise.pcap					<u>©р</u> <u>© C</u> ar Пғ	en Icel
File <u>n</u> ame: Files of type: Automatical	2020-05-28-traffic-analysis-ex All Files y detect file type	ercise.pcap Format:	Wireshark	:/tcpdump;	/ pca	- [ - [ p	<mark>© _</mark> о <u>_</u> аг Пе	en Icel
File <u>n</u> ame: Files of type: Automatical	2020-05-28-traffic-analysis-ex All Files y detect file type *	ercise.pcap Format: Size:	Wireshark 8,127 KiB,	:/tcpdump, 12,953 dai	/ pca ta recore	P ds	<u>©р</u> О <u>С</u> аг Пне	en icel
File <u>n</u> ame: Files of type: Automatical	2020-05-28-traffic-analysis-ex All Files y detect file type *	ercise.pcap Format: Size: Start / elapsed:	Wireshark 8,127 KiB, 2020-05-	:/tcpdump, 12,953 dai 28 12:56:1	/ pca ta recore 3 / 00:2:	P ds 1:32	■ <u>O</u> p <u>© C</u> ar 2 He	oen ncel elp

- 3. Apply "basic" filter → "(http.request or tls.handshake.type == 1) and !(ssdp)" and observe the traffic.
  - a. HTTPS/SSL/TLS traffic over TCP port 447 and 443 (in the purple highlight)

	2020-05-28-traffic-	analysis-exercise.pcap	000
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	Analyze Statistics Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp	
	(¢ ≠ + .) (¢ ≠	📃 🔍 ୧ ୧ ୩	
(http.request or tls.handshake.ty	/pe == 1) and !(ssdp)	Expression	on + basic basic+
Time Source	Source Port Destination I	Destination Port 👻 Host Server Name	Info
2020-05-28 10.5.28.229	49210 50.19.115.217	80 api.ipi	GET / HTTP
2020-05-28 10.5.28.229	49219 36.89.106.69	80 36.89.1	POST /yas3
2020-05-28 10.5.28.229	49220 36.89.106.69	80 36.89.1	POST /yas3
2020-05-28 10.5.28.229	49221 36.89.106.69	80 36.89.1	POST /yas3
2020-05-28 10.5.28.229	49222 36.89.106.69	80 36.89.1	POST /yas3
2020-05-28 10.5.28.8	51395 162.216.0.163	80 162.216	GET /ico/V
2020-05-28 10.5.28.229	49281 162.216.0.163	80 162.216	GET /ico/V
2020-05-28 10.5.28.229	49285 69.195.159	80 wtfismy	GET /text
2020-05-28 10.5.28.8	51402 116.202.55	80 icanhaz	GET / HTTP
2020-05-28 10.5.28.229	49286 162.216.0.163	80 162.216	GET /image
2020-05-28 10.5.28.229	49564 162.216.0.163	80 162.216	GET /image
2020-05-28 10.5.28.229	49208 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49211 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49213 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49216 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49217 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49218 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49226 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51396 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49282 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49376 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49549 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51426 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51427 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49565 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51444 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51445 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51446 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49568 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51448 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51456 5.1.81.68	443	Client Hel
4			
Erame 1867: 181 bytes on	wire (1448 hits) 191 but	es cantured (1448 hits)	12.1
0000 20 e5 2a b6 93 f1 00	0.08 0.02 1c 47 ae 0.8 00 45	00 ·*···· ··G···F·	*
2020-05-28-traffic-analysis	sis-exercise.pcap	Packets: 12953 · Displayed: 39 (0.3	3%) Profile: Default

b. HTTP traffic over TCP port 8082 (at the bottom in green highlight)

	2020-05-28-traffic-a	nalysis-exercise.pcap	000
<u>File Edit View Go</u> Capture	<u>Analyze</u> Statistics Telephony <u>M</u>	/ireless <u>T</u> ools <u>H</u> elp	
🚄 🔳 🖉 💿 🛅 🕱	€ + 5. € + 2	📜 🖲 २ २ १ 🎹	
(http.request or tls.handshake.	type == 1) and !(ssdp)	Expre	ession + basic basic+
Time Source	Source Port Destination De	estination Port 🔹 Host Server Na	me Info
2020-05-28 10.5.28.8	51402 116.202.55	80 icanhaz	GET / HTTP
2020-05-28 10.5.28.229	49286 162.216.0.163	80 162.216	GET /image
2020-05-28 10.5.28.229	49564 162.216.0.163	80 162.216	GET /image
2020-05-28 10.5.28.229	49208 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49211 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49213 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49216 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49217 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49218 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49226 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51396 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49282 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49376 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49549 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51426 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51427 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49565 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51444 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51445 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51446 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49568 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51448 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51456 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.8	51457 5.1.81.68	443	Client Hel
2020-05-28 10.5.28.229	49215 192.3.247.116	447	Client Hel
2020-05-28 10.5.28.229	49224 192.3.247.116	447	Client Hel
2020-05-28 10.5.28.229	49234 192.3.247.116	447	Client Hel
2020-05-28 10.5.28.8	51421 23.92.93.227	447	Client Hel
2020-05-28 10.5.28.229	49567 192.3.247.122	447	Client Hel
2020-05-28 10.5.28.229	49233 203.176.135	8082 203.176	POST /yas3
2020-05-28 10.5.28.8	51455 203.176.135	8082 203.176	POST /jim7
4			
▶ Frame 1867: 181 bytes o	n wire (1448 bits), 181 byte	s captured (1448 bits)	<u>^</u>
0000 20 e5 2a b6 93 f1 0	00 08 02 1c 47 ae 08 00 45 0	90 ·*····G···E·	*
😑 🍸 2020-05-28-traffic-anal	ysis-exercise.pcap	Packets: 12953 · Displayed: 39	(0.3%) Profile: Default

- Apply "basic+" filter → "(http.request or tls.handshake.type == 1 or tcp.flags eq 0x0002) and !(ssdp)" and observe the traffic.
  - a. We found some "Bad TCP" requests with TCP port 447 in black color in Column Display. Looking at the last two lines in the Frame's Packet Details pane confirms about the coloring rule and string.

8	2020-05-28-traffic-analysis-exer	cise.pcap	000
<u>File Edit View Go Capture Analyze Sta</u>	tistics Telephon <u>y W</u> ireless <u>T</u> oo	ols <u>H</u> elp	
📕 🖩 🖉 💿 📅 🖺 🕱 🖉 🔍 🗸	• • • • • • •	e e e 🎹	
(http.request or tls.handshake.type = = 1 or tcp	e.flags eq 0x0002) and !(ssdp)	Expression	. + basic basic+
Time Source Source Port	Destination Destination Po	ort 🔻 Host Server Name	Info
2020-05-28 10.5.28.229 4922	4 192.3.247.116	447	Client Hel
2020-05-28 10.5.28.229 4923	4 192.3.247.116	447	49234 - 44
2020-05-28 10.5.28.229 4923	4 192.3.247.116	447	Client Hel
2020-05-28 10.5.28.8 5142	0 62.108.35.43	447	51420 - 44
2020-05-28 10.5.28.8 5142	0 62.108.35.43	447	[TCP Retra
2020-05-28 10.5.28.8 5142	0 62.108.35.43	447	[TCP Retra
2020-05-28 10.5.28.8 5142	1 23.92.93.227	447	51421 → 44
2020-05-28 10.5.28.8 5142	1 23.92.93.227	447	Client Hel
2020-05-28 10.5.28.229 4956	7 192.3.247.122	447	49567 → 44
2020-05-28 10.5.28.229 4956	7 192.3.247.122	447	Client Hel
2020-05-28 10.5.28.229 4923	1 10.5.28.8	3268	49231 → 32
2020-05-28 10.5.28.229 4923	6 10.5.28.8	3268	49236 → 32
2020-05-28 10.5.28.229 4923	3 203.176.135	8082	49233 → 80
2020-05-28 10.5.28.229 4923	3 203.176.135	8082 203.176	POST /yas3
2020-05-28 10.5.28.8 5145	5 203.176.135	8082	51455 → 80
	E 202 176 12E	0000 000 176	DOCT /iim7
[Frame is ignored: False]			*
[Protocols in frame: eth:etherty	pe:ip:tcp]		
[Coloring Rule Name: Bad TCP]			
[Coloring Rule String: tcp.analy	sis.flags && !tcp.analysis	.window update]	
Ethernet II, Src: Netgear_b6:93:f1	(20:e5:2a:b6:93:f1), Dst:	Netgear_b6:93:f1 (20:e5:2a	:b6:93:f1)
Internet Protocol Version 4, Src:	10.5.28.8, Dst: 62.108.35.	43	
<ul> <li>Transmission Control Protocol, Src</li> </ul>	Port: 51420, Dst Port: 44	7, Seq: 0, Len: 0	
4	Sentences and the set and set and set and		×
0000 20 e5 2a b6 93 f1 20 e5 2a b6	93 f1 08 00 45 00 ·*·	·· · *····E·	
0010 00 34 1a 0e 40 00 80 06 59 12	0a 05 1c 08 3e 6c ·4··(	@··· Y····>1	
0020 23 2b c8 dc 01 bf 51 b2 2c ce	00 00 00 00 80 02 #+	···Q· , ······	
0030 20 00 7e 50 00 00 02 04 05 b4	01 03 03 08 01 01 ·~P		
0040 04 02			

5. Analyze the POST requests made over TCP port 8082 found via "basic" filter results.a. Filter the requests with "(http:request and tcp.port eq 8082)".

		2020	-05-28-traffic-analys	is-exercise.pcap	000
<u>F</u> ile <u>E</u> dit <u>V</u>	iew <u>G</u> o <u>C</u> apture	Analyze Statistics	Telephony <u>W</u> irele	ss <u>T</u> ools <u>H</u> elp	
	🐵 to 🖺 🕅	🙆 ९ 🗢 🗕	🚛 🖛 ୶ 🦕	۹ ۹ ۹ 🖿	
http.reques	t and tcp.port eq 80	82		Expre	ession + basic   basic+
Time	Source	Source Port Des	tination	Destination Port · Host	Server Name Info
2020-05-28	10.5.28.229	49233 203	3.176.135.102	8082 203.176.13	5.102 PO
2020-05-28	10.5.28.8	51455 203	3.176.135.102	8082 203.176.13	5.102 PO:
)					•
- POST /	yas33/CAT-BOMB-	W7-PC_W617601.1	071BE9788304FBD0	C52B1EE36701166/90 HTTP/1.1	vr\n
▶ [Exp Requ Requ Requ Connec Conten	ert Info (Chat/ est Method: POS est URI: /yas33 est Version: HT tion: Keep-Aliv t-Type: multipa	Sequence): POST T //CAT-BOMB-W7-PC TP/1.1 e\r\n rt/form-data; b	/yas33/CAT-BOMB _W617601.1071BE9 oundary=WebKi	-W/-PC_W61/661.10/18E9/8830 788304FBD0C52B1EE36701166/9 tFormBoundary7MA4YWxkTrZu0gi	%+BD0C52B1EE367011667 0 √\r\n ▼
4					<b>▶</b>
0010 42 4	T 53 54 20 2T 7 F 4d 42 2d 57 3	9 61 73 33 33 7 2d 50 43 5f	2T 43 41 54 20 57 36 31 37 36	POST /ya s33/CAT- BOMB-W7- PC W6176	<u></u>
0020 30 3	1 2e 31 30 37 3	1 42 45 39 37	38 38 33 30 34	01.1071B E9788304	
0030 46 4	2 44 30 43 35 3	2 42 31 45 45	33 36 37 30 31	FBD0C52B 1EE36701	
0040 31 3	0 30 21 39 30 2 3 6f 6e 6e 65 6	3 74 69 6f 6e	21 31 2e 31 00 3a 20 4h 65 65	Connect ion: Kee	
0060 70 2	d 41 6c 69 76 6	5 0d 0a 43 6f	6e 74 65 6e 74	p-AliveContent	
0070 <b>2d 5</b>	4 79 70 65 3a 2	0 6d 75 6c 74	69 70 61 72 74	-Type: m ultipart	-

b. Follow the TCP stream for all the requests found. [Several machine details and other user details found!]

2020-05-28-traff	ic-analysis-exercise.pcap	• •	0
File Edit View Go Capture Analyze Statistics Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp		
▲ ■ 2 ③ 5 🖹 🕈 • →	ا 📃 🔳 🔍 ۹ م 🎹		
http.request and tcp.port eq 8082		Expression + basic   t	basic+
Time Source Source Port Destination	Destination Port 🔹 Host	Server Name	Info
2020-05-28          10.5.28.229         49233         203.176.135.2           2020-05-28          10.5.28.8         51455         203.176.135.2	Mark/Unmark Packet Ignore/Unignore Packet Set/Unset Time Reference Time Shift Packet Comment Edit Resolved Name Apply as Filter Prepare a Filter Conversation Filter Colorize Conversation	76.135.102 76.135.102	Pos
	SCTP	•	•
<pre>&gt; [SEQ/ACK analysis] &gt; [Timestamps]</pre>	Follow	TCP Stream	Î
TCP segment data (1442 bytes)	Сору	UDP Stream	
<pre>&gt; [4 Reassembled TCP Segments (4626 bytes): #2250(</pre>	Protocol Preferences	ILS Stream	-
<ul> <li>Hypertext Transfer Protocol</li> <li>POST /vas33/cAT-ROMR-W7-PC W617601 10718E97883</li> </ul>	Decode <u>A</u> s	HTTP Stream	
A	Show Packet in New <u>W</u> indow		E C
0000         20         e5         2a         b6         93         f1         00         08         02         1c         47         ae         08         00         4           0010         05         ca         06         b1         40         00         08         06         7         47         co         ao         51         ce         50           0020         87         66         co         51         1f         92         f9         57         72         02         3b         4c         7b         75         50         66         61         73         20         66         61         73         20         66         61         73         20         66         66         73         65         72         76         65         72         73         66         67         72         67         65         72         73         66         67         72         67         65         72         73         2         67         66         73         67         66         73         65         72         66         73         65         72         66         67         72         66	45       00       .*		*

c. Process list information found.

Wireshark · Follow TCP Stream (tcp.stream eq 21) · 2020-05-28-traffic-analysis-exercise.pc	ap O	0	0
PROCESS LIST			•
[System Process]			
System			
smss.exe			
csrss.exe			
wininit.exe			
csrss.exe			
winlogon.exe			
services.exe			
lsass.exe			
lsm.exe			
svchost.exe			
spoolsv.exe			
svchost.exe			
svchost.exe			
svcnost.exe			
Lasknost.exe			
awi .exe			
NOTRISE, exe			
sychost exe			
Svenser.exc			
proclisttest			
WebKitFormBoundary7MA4YWxkTrZu0gW			
Content-Disposition: form-data; name="sysinfo"			
ipconfig /all			
4 client okts. 1 server okt. 1 turn.			Ŧ
Entire conversation (4,746 bytes) Show and save data as ASCII	Strear	n 21	÷

d. Other User's detail and Local Machine data found.



#### 6. Analyzing traffic for mail related information sent out via a POST request.

a. Filter the requests with "http.request and ip contains mail".



b. Follow the TCP stream for further analysis. [Credential exfiltration: Password found!]

Wireshark · Follow TCP Stream (tcp.stream eq 9) · 2020-05-28-traffic-analysis-exercise.pcap 🏮 🏮 🔇
POST /yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/81/ HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=ARXRPHEBMXNZHSSP Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 36.89.106.69
Content-Length: 260
Cache-Control: no-cache
ARXRPHEBMXNZHSSP
Content-Disposition: form-data; name="data"
pop3://mail.catbomber.net:995 phillip.ghent  <mark>gh3ntf@st</mark>
ARXRPHEBMXNZHSSP
Content-Disposition: form-data; name="source"
Outlook passwords
ARXRPHEBMXNZHSSP
НТТР/1.1 200 ОК
connection: close
server: Cowboy
date: Thu, 28 May 2020 18:04:12 GMT
content_length: 3
concent-type: text/plain
/1/

- 7. Analyzing traffic for any Windows executable files in this PCAP.
  - a. Filter this using → http contains "DOS mode" and look for Request URI in the Hypertext Transfer Protocol in Frame Details. [The suspicious files found are is imgpaper.png and cursor.png]



b. Follow TCP stream. [MZ is the header for executable file format.]



- 8. As we know, two executable files are present here, lets export them and save in Trickbot Analysis folder.
  - a. Go to File  $\rightarrow$  Export Objects  $\rightarrow$  HTTP.

	2020	0-05-28-traffic-ana	lysis-exercise.pcap	000
File Edit View Go Capture	<u>Analyze</u> <u>S</u> tatistics	Telephony <u>W</u> ir	eless <u>T</u> ools <u>H</u> elp	
Open Open Pacent	Ctrl+O		۹.۹۹ 🖬	
Morgo			Exp	oression + basic basic+
I Interget		tination	Destination Port * Host	Server Name Info
import nom Hex Dump		5.28.229	49286	HT
<u>C</u> lose	Ctrl+W	5.28.229	49564	HT
Save	Ctrl+S			
Save <u>A</u> s	Ctrl+Shift+S			•
File Set	,	s), 223 bytes	captured (1784 bits)	<b>*</b>
Export Packet Dissections Export Packet <u>B</u> ytes Export PDUs to File Export TLS Session Keys	↓ Ctrl+Shift+X	ytes): #9238(: -\n	1358), #9239(1358), #9241(13	58), #9242(1358), #924-
Export Objects		DICOM	amyryn	
Print	Ctrl+P	HTTP		
Quit	Ctrl+Q	IMF		
[Time since request: [Request in frame: 9	2.320724000 sec 236]	SMB		
[Request URI: http:/	/162.216.0.163/i		ng]	
- Media Type	tes			Ŧ
1	04 05 04 00 00	- 20 20 20 AF 4		•
00000010 0a 53 65 72 76	65 72 3a 20 6e	67 69 6e 78 2	f 31 Server: nginx/1	
00000020 2e 36 2e 32 0d	0a 44 61 74 65	3a 20 54 68 7	5 2c .6.2••Da te: Thu,	-

b. Download both the image files we found in the previous step and save in our Trickbot-analysis directory.

			Wireshark · Export	· HTTP object	t list 🗢 🖲
- 0	Packet 🔻	Hostname	Content Type	Size	Filename
- 0	22	api.ipify.org	text/plain	15 bytes	1
	1561	36.89.106.69	multipart/form-data	282 bytes	83
	1568	36.89.106.69	text/plain	3 bytes	83
me	1600	36.89.106.69	multipart/form-data	260 bytes	81
he	1602	36.89.106.69	text/plain	3 bytes	81
te	1665	36.89.106.69	multipart/form-data	219 bytes	81
ап	1669	36.89.106.69	text/plain	3 bytes	81
72	1686	36.89.106.69	multipart/form-data	210 bytes	81
pe	1688	36.89.106.69	text/plain	3 bytes	81
HT	2256	203.176.135.102:8082	multipart/form-data	4,362 bytes	90
Se	2258	203.176.135.102:8082	text/plain	3 bytes	90
Da	2835	162.216.0.163	content-type:	106 kB	VidT6cErs
Cc	2975	162.216.0.163	content-type:	105 kB	VidT6cErs
CC	3036	wtfismyip.com	text/plain	16 bytes	text
C¢	3047	icanhazip.com	text/plain	16 bytes	1
M	4585	162.216.0.163	content-type:	503 kB	imgpaper.png
1	9771	162.216.0.163	content-type:	503 kB	cursor.png
r.	12886	203.176.135.102:8082	multipart/form-data	4,343 bytes	90
4	12892	203.176.135.102:8082	text/plain	3 bytes	90

9. Calculate the hash for both image files using **shasum** utility.

root@4hathacker-IWC: ~	×	root@4hathacker-IWC: ~/Desktop/trickb ×	٠	•
<pre>root@4hathacker-IWC:~# cd ~/Dest root@4hathacker-IWC:~/Desktop/t 2020-05-28-traffic-analysis-exe 2020-05-28-traffic-analysis-exe root@4hathacker-IWC:~/Desktop/t 4e76d73f3b303e481036ada80c2eeba 934c84524389ecfb3b1dfcb28f9697a root@4hathacker-IWC:~/Desktop/t</pre>	ktop/t rickbo rcise. rcise. rickbo 8db2f3 2b52ea rickbo	rickbot-analysis/ t-analysis# ls pcap cursor.png Others pcap.zip imgpaper.png t-analysis# shasum -a 256 *.png 06cbc9323748560843c80b2fed1 cursor.j 0ebcaa510469f0d2d9086bcc79a imgpape t-analysis#	Host ng .png	

- 10. Check the hash values in Virus Total or Recorded Future.
  - a. Cursor.png

URL, IP address,	domáin, or file hash		Q (	λ <u>★</u> BBB Sign
43	(1) 43 engines detected this file			C B
Community Score	4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843 cursor.png checks-user-input direct-cpu-clock-access peexe runtim	c80b2fed1 e-modules	492.00 K Size	B
DETECTION	DETAILS RELATIONS BEHAVIOR COMI	MUNITY 2		
Ad-Aware	() Trojan.GenericKDZ.67476	AegisLab	<ol> <li>Trojan.Win32.Mansabo</li> </ol>	b.4lc
AhnLab-V3	() Malware/Win32.RL_Generic.R338752	Alibaba	() Trojan:Win32/Mansabo	0.80692ca9
ALYac	① Trojan.GenericKDZ.67476	SecureAge APEX	① Malicious	
Arcabit	(1) Trojan. Generic. D10794	Avast	() Win32:Trojan-gen	
Avira (no cloud)	① TR/Kryptik.cxxvm	BitDefender	Trojan, Generic KDZ, 67	476
CAT-QuickHeal	① Trojan.Mansabo	Comodo	TrojWare.Win32.Emote	et.SL@8sg2qb

#### b. Imgpaper.png

934c8452438	89ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a		Q	Q	☆ 🚟 Sign in
43	① 43 engines detected this file				o X
Community Score	934c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc7 Imgpaper.png checks-user-input direct-opu-clock-access peexe runtime-modul	79a es	492.0 Size	0 KB	EXE
DETECTION	DETAILS RELATIONS BEHAVIOR COMMUNIT	Y ()			
Acronis	() Suspicious	Ad-Aware	() Trojan.GenericKDZ	67476	
AegisLab	① Trojan.Win32.Mansabo.4tc	AhnLab-V3	() Malware/Win32.RL_	Generic.	R338752
Alibaba	① Trojan:Win32/Mansabo.758a4924	ALYac	Trojan.GenericKDZ	.67476	
SecureAge APEX	① Malicious	Arcabit	() Trojan.Generic.D10	794	
Avast	() Win32:Trojan-gen	AVG	U Win32:Trojan-gen		
Avira (no cloud)	① TR/Kryptik.oltoc	BitDefender	Trojan.GenericKDZ	67476	
BitDefenderTheta	() Gen:NN.ZexaF.34122.EqW@aS73j8ci	CrowdStrike Falcon	() Win/malicious_conf	idence_6	0% (W)

### Answers:

- 1. Infected Windows Client Details:
  - a. IP Address: 10.5.28.229
  - b. Host Name: Cat-Bomb-W7-PC
  - c. User Account Name: phillip.ghent
- 2. Another user account:
  - a. Host Name: CAT-BOMB-W10-PC
  - b. User Account Name: timothy.sizemore
- 3. Infected user's email password: gh3ntf@st
- 4. SHA256 hashes for the two EXE files:
  - a. 4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843c80b2fed1
  - b. 34c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a

### Lessons Learnt

Network Forensics encompasses law, cyber-crime, technology and even business firms. It has equal importance in Govt. Investigations as well as Business Data Breach Investigations. We have discussed about different forms of investigations based on different frames of time and mindset. Technical approaches to handle evidence and its legal advantage have also been discussed.

The difference between network flow analysis and packet capture analysis is unique however both should be used together along with other tools and processes to withstand modern scenarios of threats and cyber-crimes. Similar to what we have seen during Trickbot PCAP Analysis, there are other Ransomware and APTs ready to attack your system or already have disguised you to go beyond your firewall and defenses.

### References

[1] Ransomware-cyber-crime-malware-2321110 [Photograph], TheDigitalArtist, Pixabay. Last accessed on June 21, 2020. - pixabay.com/illustrations/ransomware-cyber-crime-malware-2321110/

[2] Emotet, Ryuk, Trickbot: Loader-Ransomware-Banker Trifecta, Mathew J. Schwartz, Data Breach Today. Published on April 15, 2020. Last Accessed on June 21, 2020. - databreachtoday.com/emotet-ryuk-trickbot-loader-ransomware-banker-trifecta-a-14126

[3] TrickBot: We missed you, Dyre, Threat Research Team. Published on Oct. 15, 2016. Last Accessed on June 21, 2020. Link: fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre/

[4] TrickBot, Malpedia. Last Accessed on June 21, 2020. – malpedia.caad.fkie.fraunhofer.de/details/win.trickbot

[5] Microsoft Security Intelligence (@MsftSecIntel) [Photo], Twitter. Published on Apr 17, 2020. Last Accessed on June 21, 2020. -twitter.com/MsftSecIntel/status/1251181180281450498/photo/2

[6] Wireshark Tutorial: Examining Trickbot Infections, Brad Duncan, Unit 42, Palo Alto Networks. Published on Nov. 8, 2019. Last Accessed on June 21, 2020. Link: unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/

[7] MS-ISAC Releases Security Primer on Trickbot Malware, Current Activity Landing, National Cyber Awareness System, US-CERT. Published on Mar. 14, 2019. Last Accessed on June 21, 2020. – us-cert.gov/ncas/current-activity/2019/03/14/MS-ISAC-Releases-Security-Primer-TrickBot-Malware

[8] Security Primer – Trickbot, White Papers, Center for Internet Security. Last Accessed on June 21, 2020. - cisecurity.org/white-papers/security-primer-trickbot/

[9] A visual representation of Trickbot and its modules [Photo], Goodbye Mworm, Hello Nworm: Trickbot Updates Propagation Module, Brad Duncan, Unit 42, Palo Alto Networks. Published on May 28, 2020. Last Accessed on June 21, 2020. - unit42.paloaltonetworks.com/wp-content/uploads/2020/05/Figure-1.-A-visual-representation-of-TrickBot-and-its-modules.jpeg

[10] Example of artifacts for Trickbot modules on an infected Windows 7 client [Photo], Goodbye Mworm, Hello Nworm: Trickbot Updates Propagation Module, Brad Duncan, Unit 42, Palo Alto Networks. Published on May 28, 2020. Last Accessed on June 21, 2020. - unit42.paloaltonetworks.com/wpcontent/uploads/2020/05/Figure-2.-Example-of-artifacts-for-TrickBot-modules-on-an-infected-Windows-7-client..jpeg

[11] Trickbot propagation flow chart from September 2019 through March 2020 [Photo], Goodbye Mworm, Hello Nworm: Trickbot Updates Propagation Module, Brad Duncan, Unit 42, Palo Alto Networks. Published on May 28, 2020. Last Accessed on June 21, 2020. - unit42.paloaltonetworks.com/wp-content/uploads/2020/05/Figure-3.-TrickBot-propagation-flow-chart-from-September-2019-through-March-2020.jpeg

[12] What sites is Trickbot targeting, CyberCrime & Doing Time, Gary Warner. Published on Mar 5, 2020. Last Accessed on June 21, 2020. - garwarner.blogspot.com/2020/03/what-sites-is-trickbot-targeting.html [13] The History of Computing Project, Timeline: Chronology of the history of computing, The History of Computing Foundation, Maurik, The Netherlands, 2010. Last Accessed on June 18, 2020. - thocp.net/timeline/timeline.htm

[14] Mark Pollitt. A History of Digital Forensics. 6th IFIP WG 11.9 International Conference on Digital Forensics (DF), Jan 2010, Hong Kong, China. pp.3-15, ff10.1007/978-3-642-15506-2\_1ff. ffhal-01060606f. Last Accessed on June 18, 2020. - hal.inria.fr/hal-01060606/document

[15] University of Washington [Photo], Seattle, United States, Taylor Vick, Unsplash. Last Accessed on June 18, 2020. - unsplash.com/photos/M5tzZtFCOfs

[16] Guide to Integrating Forensic Techniques into Incident Response, Timothy Grance, Suzanne Chevalier, Karen Kent Scarfone, Hung Dang, Special Publication (NIST SP) – 800-86, Published on September 1, 2006. Last Accessed on June 18, 2020. - nist.gov/publications/guide-integrating-forensic-techniques-incident-response

[17] Introduction to Network Forensics Handbook Final V1.1, Cybersecurity ENISA Training, Published August 2019. Last Accessed on June 18, 2020. - enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf

[18] A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation, Junwei Huang, Yinjie Chen, Zhen Ling, Kyungseok Choo, Xinwen Fu University of Massachusetts Lowell, USA + Southeast University, China. Last Accessed on June 18, 2020. pdfs.semanticscholar.org/10b8/8debc818ca1da825fb9848cfaf8dccf2aa9f.pdf

[19] Privacy and Search, Expectation of Privacy, Wikipedia. Last Accessed on June 18, 2020. - en.wikipedia.org/wiki/Expectation\_of\_privacy#Privacy\_and\_search

[20] H. Marshall Jarrett and Michael W. Bailie, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Washington, DC: Office of Legal Education Executive Office, 2009). Last Accessed on June 18, 2020. - justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ssmanual2009.pdf

[21] Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 2701-2712), Wikipedia. Last Accessed on June 18, 2020. - en.wikipedia.org/wiki/Stored\_Communications\_Act

[22] Legal Considerations, Guidelines for Evidence Collection and Archiving, RFC3227. Last Accessed on June 18, 2020. - tools.ietf.org/html/rfc3227

[23] Network Forensics, Wikipedia. Last accessed on June 19, 2020. - en.wikipedia.org/wiki/Network\_forensics#Overview

[24] Flow Analysis Versus Packet Analysis, What should you Choose, Netfort.com. Last Accessed on June 19, 2020. - netfort-prod.k8s.corpwebsite.gcp.rapid7.com/content/uploads/PDF/WhitePapers/NetFlow-Vs-Packet-Analysis-What-Should-You-Choose.pdf

[25] Traffic analysis exercise – Catbomber, Malware-traffic-analysis.net. Published on May 28, 2020. Last Accessed on June 19, 2020. - malware-traffic-analysis.net/2020/05/28/index.html

[26] Wireshark, From Wikipedia, the free encyclopedia. Last Accessed on June 19, 2020. - en.wikipedia.org/wiki/Wireshark

# Email Forensic Analysis

Lyer 6

By Nitin Sharma "Like almost everyone who uses e-mail, I receive a ton of spam every day. Much of it offers to help me get out of debt or get rich quick. It would be funny if it weren't so irritating." - Bill Gates

Communication is one of the most important art one should possess, especially in business context. It impacts every aspect regarding the relationship with employees, suppliers and customers. 90% of messages are conveyed through non-verbal communication, while most companies utilize email or other forms of electronic messaging as a means of written communication.



Email communication is the mode of written communication which provides more formal structure and official perspective. Attackers find business emails as the easiest medium to spread malware through deceptive spam emails convincing target victims to click open the attachments or links that comes along. By opening the link or attachments, the users are directed to malicious websites or end up opening a malicious document by this way the attackers install the malware from backend on to the user's system and therefore gains access to business network resulting a security breach.

Necessity of securing emails therefore arises, and businesses should validate their email security services. In this paper, email forensics has been discussed thoroughly for

malicious email header detection in spam and illicit emails. At the end, a practical walkthrough is included with some email hygiene and security best practices.

Photo by @bermixstudio, unsplash.com [1]

### **Email: OSI Perspective**

Email runs on SMTP (Simple Mail Transfer Protocol) which is Layer 7 (Application Layer) protocol.

When an email is sent, the data passes through all the layers to the physical layer where the data is put onto the network cabling, and then sent to the receiving computer where the process reverses and the data travels up through the layers to the application layer of the receiving computer.

In this process, Layer 6 (Presentation Layer) introduces a set of syntax and semantics to the information transmitted through the lower protocol layer that will be the focus of upcoming discussion. Please see below the flow of sending email from Alice to Bob with OSI Layer functions.



### **Email Headers**

An Email message consists of a number of header fields and a body (optional). Header fields consist of name-value pairs that are delimited by a colon. Mandatory headers provide information on the sender and the recipient of the message and the date the message was sent. Other headers may give information on the subject or contents of the message and how it was routed through the Internet. The blank line separating the header fields from the body is an ASCII carriage return character (CR) followed by an ASCII linefeed character (LF) on a line by itself.

- 1. Mandatory Headers Date, From, To.
- 2. Optional Headers Subject, Comment, Keywords, Encrypted, CC and BCC.

Other headers include Dynamic and User Defined headers usually written for custom email applications.

#### MIME Header Fields

The Multipurpose Internet Mail Extensions (MIME) protocol is an extension to the Standard for the Format of ARPA Internet Text Messages. This protocol has defined the standard format of textual mail messages on the Internet since it came out in 1982. It describes the format of message headers but it tells little about the content of the body of the message which is limited to 7-bit ASCII characters. The MIME protocol provides the necessary extension to the MAIL protocol in order to transfer possible multi-part textual and non-textual data object in the body of a MAIL message. <sup>[2]</sup>

MIME headers come in two flavors:

- 1. MIME message headers additional RFC 822-style headers. They denote that a message is MIME compliant and inform a receiving MUA (Mail User Agent) of the structure and encoding of the message.
- 2. MIME part headers reside in a message body and describe the contents of each part of a multipart message.

Note: If a MIME header is part of a message header block, it applies to the entire message. If it appears at the beginning of a message part, it applies only to that part. A Mail User Agent (MUA) also referred to as an email client, is a computer application that allow you to send and retrieve email.

MIME message headers are <sup>[3]</sup>:

- 1. <u>MIME Version</u> To declare the version of the Internet message body format standard in use. e.g. MIME-Version: 1.0
- <u>Content-Type</u> Specifies the nature of the data in the body of an entity by giving media type and subtype identifiers, and by providing auxiliary information that may be required for certain media types. Top Level media types are: text, image, audio, video, application, multipart, message.
- **3.** <u>Content-Transfer-Encoding</u> Shows the type of encoding performed on a message or message part and therefore gives information on how to decide it. The SMTP limits email messages to US-ASCII 7-bit characters and lines of fewer

than 998 data characters, per RFC 821. Content-Transfer-Encoding values can be: 7bit, 8bit, binary, quoted-printable, base64, Custom, or user-defined schemes. The first three do not require any decoding.

- **4.** <u>Content-ID</u> This header is uncommon and optional but becomes mandatory if a Content-Type of message/external-body is used. This is also used to augment the multipart/alternative media type.
- 5. <u>Content-Description</u> It is an optional header to add textual description to file attached to an email.

### MIME Encoding

When creating a mail message, one must decide how to encode each part of the message.

- <u>7-bit dat</u>a It is simple US-ASCII text, with the restrictions placed on it by RFC 821. No octets with ASCII decimal values of zero or more than 127 are allowed. No encoding required.
- <u>8-bit data</u> Decimal values over 127 are also allowed. Allowable on some systems but might get translated to 7-bit by intervening mail servers if any. When creating a mail destined to route directly onto the Internet, don't use this encoding type.
- **3.** <u>Binary data</u> It may contain any type of octets, irrespective of their possible translation to ASCII. The same restrictions and notes for 8-bit data apply to binary. Do not use this encoding type for Internet use via SMTP. Translate binary data into Base64 encoding type.
- **4.** <u>Quoted-Printable</u> Should be used for data that is nominally text and humanreadable but not "7-bit clean". The simple rules that follow quoted printable method are,
  - **a.** Convert the original data into an octet stream by ensuring that the bits are in big endian format.
  - **b.** Any octet, except a CRLF line-break in the original data, may be changed to an equal sign (=) followed by a two-character hexadecimal representation of the octet's character value. An octet must be so changed unless another rule allows an alternative method.
  - **c.** Octets with ASCII decimal values of 33 through 60 and 62 through 126 may be represented as their ASCII character representations.
  - **d.** Whitespace (tabs, ASCII decimal value 9, and spaces, ASCII decimal value 32) may be left as those values unless they would fall at the end of a line, then they must be encoded by 4a.
  - e. Line breaks in the original data should be converted to the CRLF form.
  - **f.** No line may be longer than 76 characters, not including the ending CRLF characters. If the original data includes lines longer than 76 characters, a

"soft" line-break may be added by ending a line with an equal sign (=) followed by the normal CRLF sequence.

- 5. <u>Base64</u> This encoding takes three octets (24 bits) and maps them into four 6-bit blocks, then represents each 6-bit block with a character in a 64-character alphabet (2<sup>6</sup> = 64). Because of this mapping, base 64 encoded information is about one-third larger than the original data. The complete rule set for base64 encoding looks like this,
  - **a.** Convert the original data into an octet stream by ensuring that the bits are in big-endian format.
  - **b.** If the data to be encoded is textual, line breaks must be converted to CRLF form first.
  - c. Remove three octets at a time from the stream and convert them into four
    6-bit indexes into the base64 alphabet.
  - **d.** Convert the four 6-bit indexes into four characters from the base64 table.
  - **e.** Ensure that each line of encoded information is less than 76 characters long, not including the terminating line break (CRLF).
  - **f.** When you reach the end of the original data, you may have one or two octets left over. If octets are left over, you will have to "pad" the encoding. If the number of octets in the original data was divisible by 3, no padding is necessary.
  - **g.** To pad the encoding, add zero bit onto the end of the stream until you have an integral number of 6-bit blocks. Apply 5c, to get the base64 characters, as normal. Then add either one or two equal signs (=) onto the end of the encoding until the total number of characters is evenly divisible by 4.

### Advantages of MIME

- **1.** It is able to send multiple attachments with a single message.
- **2.** Unlimited message length.
- **3.** Binary attachments (executables, images, audio, or video files) which may be divided if needed.
- **4.** MIME provided support for varying content types and multi-part messages.

### **Email Authentication**

Email authentication is used to block harmful or fraudulent uses of email such as phishing and spam.

In general, the email authentication works like below, <sup>[4]</sup>

- **1.** A business or organization that sends email establishes a policy that defines rules by which email from its domain name can be authenticated.
- **2.** The email sender configures its mail server and other technical infrastructure to implement and publish these rules.
- **3.** A mail server that receives email authenticate the message it receives by checking details about an incoming email message against the rules defined by the domain owner.
- **4.** The receiving mail server acts upon the results of this authentication to deliver, flag or even reject the message.



The most commonly used email authentication standards are,

**a. SPF - Sender Policy Framework** (Allows senders to define which IP addresses are allowed to send mail for a particular domain i.e., Path Based Authentication).

Example: SPF Record

TXT @ "v=spf1 a include:\_spf.google.com ~all"

#### Explanation:

- **TXT** [The DNS zone record type; SPF records are written as TXT records]
- [In a DNS file, the "@" symbol is a placeholder used to represent the "current domain"]
- v=spf1 [Identifies the TXT record as an SPF record, utilizing SPF
  Version 1]
- a [Authorizes the host(s) identified in the domain's A record(s) to send e-mail]
- **include:** [Authorizes mail to be sent on behalf of the domain from google.com]
- ~all [Denotes that this list is all inclusive, and no other servers are allowed to send e-mail]

**b. DKIM – Domain Keys Identified Mail** (Provides an encryption key and digital signature that verifies that an email message was not faked or altered i.e., Content Based Authentication).

#### Example: DKIM Record

dk1024-2012.\_domainkey.xyzpath.com. 600 IN TXT "v=DKIM1\; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1TaNgLlSyQMNWVL NLvyY/neDgaL2oqQE8T5illKqCgDtFHc8eHVAU+nlcaGmrKmDMw9dbgiGk10 cgZ56NR4ycfUHwQhvQPMUZw0cveel/8EAGoi/UyPmqfcPibytH81NFtTMAx UeM4Op8A6iHkvAMj5qLf4YRNsTkKAV;"

#### Explanation:

- **dk1024-2012** [Indicates the selector record name used with the domain to locate the public key in DNS. The value is a name or number created by the sender]
- **xyzpath.com** [Indicates the domain used with the selector record to locate the public key]

DKIM1 [Optional tag representing the version of DKIM record] MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1TaNgLlSyQM NWVLNLvyY/neDgaL2oqQE8T5illKqCgDtFHc8eHVAU+nlcaGmr KmDMw9dbgiGk1ocgZ56NR4ycfUHwQhvQPMUZw0cveel/8EAG oi/UyPmqfcPibytH81NFtTMAxUeM4Op8A6iHkvAMj5qLf4YRNs TkKAV [Required tag representing the public key used by a mailbox provider to match to the DKIM signature generated using the private key. It is generated along with its corresponding private key during the DKIM set-up process]

**c. DMARC** – **Domain-based Message Authentication, Reporting and Conformance** (utilizes the SPF and DKIM authentication mechanisms into a common framework and allows domain owners to declare how they would like email from that domain to be

Explanation:

v=DMARC1 [DMARC Protocol version]
p=reject [Protocol for domain, reject will cancel the message at SMTP
layer]
pct=100 [Percentage of message subjected to filtering]

rua=mailto:postmaster@dmarcdomain.com [Reporting UTI of aggregate report]

<u>Note</u>: These standards were deigned to supplement SMTP, the basic protocol used to send email, because SMTP does not itself include any AUTH(N) mechanisms.


## Authentication Work Flow:

With SPF and DKIM, it is up to the ISP to decide what to do with the results. DMARC takes it a step further and gives the org/company full control to set a policy to approve, reject or quarantine emails from sources the org/company do not know or trust, all based on the results of DKIM and SPF.<sup>[5]</sup>

For Example, ABC company publish a DMARC record that says if DKIM or SPF fails, reject the message. Participating ISPs will look at this policy and discard the emails that fail.

DMARC lets the ABC company tell ISPs how they want them to behave if SPF and DKIM fail or are not present. The flow chart above explains this.

## Walkthrough: Email Header Analysis

In this walkthrough, we will go through a malicious email sent by unknown person. This email also has a text file attachment. You can follow the exercise by proceeding in a similar fashion for any email within your mailbox.

Pre-requisites: There is no specific pre-requisites to go through this walkthrough. We will be going to cover the header information we have discussed so far.

## A. <u>Capturing Headers from Malicious Email</u>

1. The Standard Email Header details shown below describes the source and destination information for the mail. However, the source email is very suspicious with spelling errors and the destination e-mail is different from my email.

<u>Note</u>: Many spam mails will have "From:" and "To:" addresses we have never heard of. My email address might have been covered in the BCC (Blind Carbon Copy).

		from:	AZDS <pricecliams@yahoo.com.my></pricecliams@yahoo.com.my>
× .	You have blocked priceclia	reply-to:	AZDS <pricecliams@yahoo.com.my></pricecliams@yahoo.com.my>
		to:	"jameschristopher62@hotmail.com" <jameschristopher62@hotmail.com< td=""></jameschristopher62@hotmail.com<>
		date:	Jun 24, 2020, 10:22 AM
		subject:	Att
		mailed-by:	yahoo.com.my
		signed-by:	yahoo.com.my
		security:	Standard encryption (TLS) Learn more

2. To get all the header details, Click the three dots at right side of mail window and select "Show Original".



3. All the details of Original Message and respective email header will appear as shown below. Save the header information in a text file.

#### **Original Message**

Message ID	<784297485.2423248.1592974333884@mail.yahoo.com>
Created at:	Wed, Jun 24, 2020 at 10:22 AM (Delivered after 4 seconds)
From:	AZDS <pricecliams@yahoo.com.my> Using WebService/1.1.16138 YMailNorrin Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36</pricecliams@yahoo.com.my>
To:	"jameschristopher62@hotmail.com" <jameschristopher62@hotmail.com></jameschristopher62@hotmail.com>
Subject:	Att
SPF:	PASS with IP 106.10.242.37 Learn more
DKIM:	'PASS' with domain yahoo.com.my Learn more
DKIM: DMARC:	'PASS' with domain yahoo.com.my Learn more 'PASS' Learn more
DKIM: DMARC:	'PASS' with domain yahoo.com.my Learn more 'PASS' Learn more

Delivered-	Co: equal.com
Received: 1	by 2002:ac8:6619:0:0:0:0:0 with SMTP id c25csp314345qtp;
Tu	e, 23 Jun 2020 21:52:17 -0700 (PDT)
X-Google-S	tp-Source:
ABdhPJzdmDl	pFwVQE4jTCGAxvknh1kk+RAmbgWnSK9rii5pUt8wE0EoAtieTIfGLNryWnb5
atiU	
X-Received	by 2002:a17:90a:950e:: with SMTP id
t14mr24438	953pio.99.1592974337805;
Tu	2. 23 Jun 2020 21:52:17 -0700 (PDT)
ARC-Seal:	=1: a=rsa-sha256: t=1592974337: cv=none:
d=	mogle com: s=arc-20160816:

- B. <u>Analyzing Details from Header Information using MxToolBox</u>
- **1.** Copy the saved header details and paste them in MxToolBox Email Analyzer <sup>[6]</sup>. And Click "Analyze Header".



**2.** The result here, shows us that the delivery is not DMARC Compliant which is due to failure of SPF AUTH(N) and DKIM AUTH(N).

Header Analyzed Email Subject: Att					< Analyze I	New Heade
Delivery Information						
> 3 DMARC Compliant						
> SPF Alignment						
> 8 SPF Authenticated						
DKIM Alignment						
> 8 DKIM Authenticated						
Relay Information Received Delay: 1 seconds						
	7					
From sonic.gate.mail.ne1.yahoo.com to sonic303.consmr.mail.sg3.yaho	io.com —					
to mx.goog	le.com —					
	to -	Je				
			-			
	0	0.5	1	1.5	2	2.5

**3.** The SPF Authentication Failure means the IP address 106.10.242.37 is not authorized to send from the domain. The SPF record does not contain the sending server or IP address used for sending email to the mailbox provider. Notice the hops in between From and To Address also as above. And the result below where, IP Address is not present in the SPF record. You can even compare the results for SPF Lookup to find this IP.

spf:ya	hoo.com.	my:106.10.242.37	Hide		
v=sp	f1 redirect	=_spf.mail.yahoo.com			
Prefix	Туре	Value	PrefixDesc	Description	
Prefix	Туреч	Valuespf1	PrefixDesc	DescriptionThe SPF record version	
Prefix+	Typeredirect	Value_spf.mail.yahoo.com	PrefixDescPass	DescriptionThe SPF record for Value current record.	replaces the
	Test		Result		
Status NameSPF Authentication			ResponseSPF	Failed for IP - 106.10.242.37	More     Info

4. The DKIM Authentication Failure means the body hash verification fails, the computed hash of the message body does not agree with the body hash value stored in the "bh=" tag of the DKIM signature. [Note: The reasons for such failure might be the email body modification or wrong public key in DKIM-Signature Header/DNS]

dkim:ya	hoo.com.my:s2048	Show	
Dkim Public	Record:		
k=rsa;	p=MIIBIjANBgkqhkiG9w0E	BAQEFAAOCAQ8AMIIBCgKCAQEAu	oWufgbWw58MczUGbMv176RaxdZG0MkQmn8(
Dkim Signa	ture:		
t=159297	4336; bh=HcWDedQC0/FpZ	JOOxqm/f/Vi+619y6JLmqXGkR	[4z9Q=; h=Date:From:Reply-To:To:Sub

- 5. Now, we will come to the MIME types and the mail body.
  - a. All the red highlights in the image shown below are MIME details.
  - b. There are five **Content-Type** headers in this email example. The one on the message header is a composite type (multipart/mixed), allowing it to have message parts under it.
  - c. The second **Content-Type** (multipart/alternative) is syntactically identical to previous one (multipart/mixed). In particular, each of the parts is an "alternative" version of the same information. The user agent should either choose the "best" type based on the user's environment and preferences or offer the user the available alternatives. We have here, text/plain and text/html.
  - d. The last **Content-Type** is for the TXT document file attached, as we can see Content-Disposition: attachment.

e. The green box highlight actually contains the text message in **base64** encoded format.

```
Date: Wed, 24 Jun 2020 04:52:13 +0000 (UTC)
From: AZDS <pricecliams@yahoo.com.my>
Reply-To: AZDS <pricecliams@yahoo.com.my>
To: "jameschristopher62@hotmail.com"
<jameschristopher62@hotmail.com>
Message-ID: <784297485.2423248.1592974333884@mail.yahoo.com>
Subject: Att
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----
= Part 2423247 202191035.1592974333884"
References: <784297485.2423248.1592974333884.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.16138 YMailNorrin Mozilla/5.0 (Windows
NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.106 Safari/537.36
Content-Length: 1096
-----= Part 2423247 202191035.1592974333884
Content-Type: multipart/alternative; boundary="----
= Part 2423243 1077152613.1592974333850"
-----= Part 2423243 1077152613.1592974333850
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit
 ----= Part 2423243 1077152613.1592974333850
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit
<html><head></head><div class="yahoo-style-wrap"
style="font-family:Helvetica Neue, Helvetica, Arial, sans-
serif;font-size:13px;"><div></div></div></body></html>
-----= Part 2423243 1077152613.1592974333850--
-----= Part 2423247 202191035.1592974333884
Content-Type: text/plain
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="-1.txt"
Content-ID: <31fc33ff-26c7-2f8f-76ff-48d6121427ef@yahoo.com>
SGkgU2lyL0lhDQpJIHdhbnQgdG8gcGFydG5lcnNoaXAgd2l0aCB5b3UgaW4gdHJhb
nNmZXIgb2Yg
ozMsNTE3LDAwMC4wMCEqQ29udGFjdCBtZSBmb3IqbW9yZSBkZXRhaWxzIG15ICBpZ
DogamFtZXNj
aHJpc3RvcGhlcjYyQGhvdG1haWwuY29tICAgDQpUaGFua3MNCk1yIEphbWVzIENoc
```

-----= Part 2423247 202191035.1592974333884--

mlzdG9waGVy

**6.** We can get the actual message from text file attachment without opening the file by decoding the Green box text at base64decode.org <sup>[7]</sup>.

#### **Decode from Base64 format**

Simply enter your data then push the decode button. ozMsNTE3LDAwMC4wMCEgQ29udGFjdCBtZSBmb3lgbW9yZSBkZXRhaWxzIG15ICBpZDogamFtZXNj aHJpc3RvcGhlcjYyQGhvdG1haWwuY29tlCAgDQpUaGFua3MNCk1ylEphbWVzIENocmlzdG9waGVy I For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page. UTF-8 ✓ Source character set. Decode each line separately (useful for multiple entries). O Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set). < DECODE > Decodes your data into the textarea below. Hi Sir/Ma I want to partnership with you in transfer of 3,517,000.00! Contact me for more details my id: jameschristopher62@hotmail.com Thanks Mr James Christopher

## C. IP Blacklist Check

1. Checking the email origin IP Address in publicly available blacklists is also a way to find out spam. Many of the lists have already been prepared with the help of different reporting procedures.

106.10.242.	37 🛄 Blac	klist Check 👻			
blacklist:	:106.10.242.37	onitor This			
Solve Ema	ail Delivery Problems		C blac	klist	
	<b>KLISTING</b> isn't the ONLY	email delivery issue	LEARN MOR	E 📀	
M We n	otice you are on a bla	cklist			
o vie i	lottee you are on a bla	Skilot.			
Click by	are for some supportions.				
Click he	ere for some suggestions				
Click he	ere for some suggestions				
Click he	ere for some suggestions 06.10.242.37 against 87 k	nown blacklists			
Click he Checking 10 Listed 3 time	ere for some suggestions 06.10.242.37 against 87 k es with 1 timeouts	nown blacklists			
Click he Checking 10 Listed 3 time	offer for some suggestions 06.10.242.37 against 87 k es with 1 timeouts Blacklist	nown blacklists Reason	TTL	ResponseTime	
Click he Checking 10 Listed 3 time Status	Definition of the second state of the second s	nown blacklists Reason Reason106.10.242.37	<b>TTL</b> TTL3600	ResponseTime 109	Ignore
Click he Checking 10 Listed 3 time Status	Definition of the source of th	Reason Reason106.10.242.37 was listed Detail	<b>TTL</b> TTL3600	ResponseTime 109	Ignore
Click he Checking 10 Listed 3 time Status LISTED Status	Definition of the source of th	Reason Reason106.10.242.37 was listed Detail Reason106.10.242.37	<b>TTL</b> TTL3600 TTL300	ResponseTime 109 0	Ignore
Click he Checking 10 Listed 3 time Status LISTED Status LISTED	Blacklist       Name0SPAM       NameLASHBACK	Reason Reason106.10.242.37 was listed Detail Reason106.10.242.37 was listed Detail	<b>TTL</b> TTL3600 TTL300	ResponseTime 109 0	Ignore
Click he Checking 10 Listed 3 time Status & LISTED Status & LISTED Status &	Blacklist       NameUASHBACK       NameSORBS SPAM	Reason Reason106.10.242.37 was listed Detail Reason106.10.242.37 was listed Detail Reason106.10.242.37	<b>TTL</b> TTL3600 TTL300 TTL3600	ResponseTime 109 0	Ignore Ignore

## Best Practices for Email Security

- 1. Use strong passwords with upper and lower-case letters, numbers and special characters, random numbers, avoiding common-letter substitutions.
- 2. Use multi-factor authentication while logging in your email.
- 3. For emails received from unknown senders, do not click any link, or open the attachments downloading to your system.
- 4. Use spam filters, antivirus, and antimalware solutions.
- 5. Do not use your business email addresses for personal outcomes like online shopping, online gaming, etc.
- 6. Never access company email from public Wi-Fi without using a VPN.
- 7. Never click "Unsubscribe" link in spam emails. It might steal some information from your system or create a backdoor.
- 8. Use SPF, DKIM and DMARC as a part of business email setup.
- 9. Security Awareness training is the best way to ensure safety recommendations provided to the business folks.
- 10. Exercise caution when enabling Macros in Office Suite from the email attachments.

## Lessons Learnt

Email forensics and security is very important in order to keep an organization as well as individual safe from spam and phishing. We have covered here OSI Email perspective, Message encoding schemes, MIME types and their importance, Email authentication methods and a simple walkthrough for Email Header Analysis. Following a set of guidelines and adoption of security best practices can help to tackle email compromise in modern digital and connected world.

## References

[1] Anonymous computer hacker in white mask and hoodie [Photo], Bermix Studio, Unsplash. Last Accessed on June 23, 2020.-<u>images.unsplash.com</u>

[2] Presentation Layer Protocols, Henrik Frystyk, Published in July, 1994. Last Accessed on June 23, 2020. - <u>w3.org/People/Frystyk/thesis/Presentation.html</u>

[3] Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, RFC-2045, Published in Nov., 1996. Last Accessed on June 23, 2020. - tools.ietf.org/html/rfc2045#page-8

[4] Email Authentication basics for SaaS teams, Sparkpost.com. Last Accessed on June 23, 2020. - <u>sparkpost.com</u>

[5] DMARC: Monitor and secure your email delivery, Chris Nagele, Postmarkapp.com. Published on June 2, 2020. Last Accessed on June 23, 2020. postmarkapp.com/guides/dmarc

[6] MXtoolbox Email Header Analyzer [Online Tool], Last Accessed on June 23, 2020. - <u>mxtoolbox.com/EmailHeaders.aspx</u>

[7] Base64 – Decode and Encode [Online Tool], Last Accessed on June 23, 2020. base64decode.org/

# Kibana, ElasticSearch, and Logstash Visualizing your Data Layer 2/3/4/5/6/7

By Richard Medlin The Kibana Dashboard is used for searching, visualizations, and maps for you to view any type of data that you ship to ElasticSearch. The dashboard gives you the ability to look at data in as much depth as you configure it to go. The dashboard itself gives you a lot of flexibility for performing analysis of information in a side-by-side manner. Once you make dashboards you can edit and view the data that is displayed, or you can use some of the preconfigured dashboard visualizations that are already built into Kibana. You can customize the visualizations to set up a custom SIEM to monitor events on your network. Kibana provides an interface for you to see what is happening in your network environment, and can be used to display the information in a way that is quick and easy to drill down on anomalies in system and network behavior, while also providing signature based detection of potential malicious activity on the network.

Once you import data into ElasticSearch — using whatever method you decide — Kibana can take that data and provide multiple formats to visualize your data. You can use piecharts, bar-charts, sunbursts, heat, region and coordinate maps, data tables, tag clouds, and histograms to name a few. Kibana allows you to add controls, radio sliders, and filters — this makes for a very versatile option when viewing data. Kibana uses metric aggregation and bucket aggregation to match search criteria in documents. Once you setup your desired dashboard panel using the visualization method, you can save the result and build a dashboard that you can access anytime.

In this section of the write-up we are going to cover how to make a Kibana Dashboard. In order to create a dashboard, you need to first create visualizations. The visualizations will be the different panes that will make up your dashboard. We are going to cover some of the basics for creating a dashboard similar to the one built for CSI Linux that can be downloaded at <u>csilinux.com</u>. Go ahead and launch ELK stack and ensure you have collected some logs with Zeek (Bro). At this point you should be in your web browser and open up Kibana by using the IP address for your SIEM.

## This write-up will cover the following:

- Creating Visualizations for the SIEM Dashboard
- GeoHeat Map
- Saving Visualizations
- Viewing the Newly Created Visualization
- GeoIP Unique Count
- Top Network Traffic Generation, Network Applications, and Traffic Destination
- Average Missed Bytes
- Sum of Bytes
- Notices Generated
- Building the Dashboard

# Creating Visualizations for the SIEM Dashboard

## GeoHeat Map

We will start by creating a heat map that shows the location of external network traffic. This will allow you to see where your network communications are coming from externally, and where your internal network nodes are sending traffic to. This is helpful for identifying malicious traffic, and you can also setup caching for your proxy server if you have one on the network. That will help cut down some of the wait times for your network nodes and allow you to optimize your network speeds.

## Left Click on Visualize:

				192.100.1.20
	Discover			
9	New Save Open Share	e Inspect		
0	🕒 🧹 Search			KQL 🛱 🗸 May 1!
	Visualize			
F	logstash-* (change)			
â	Q Search field na		May 15, 2020	0 @ 12:00:00.000 - May
<u>®</u>	<ul> <li>Filter by type</li> <li>O</li> </ul>	5000 4000		
(; i)	Selected fields	3000 2000		
ନ୍ଦ୍ର	Available fields	1000 0		
50	@timestamp	12	2:00 13:00 14:00	15:00 16:00 17
Ē	t @version			(OI
	© AA	Time 🗸		_source
9	€ RA	> May 15,	2020 @ 18:44:24.359	agent.ephemeral_id:
₿	C RD			agent.hostname: csi 83d4a57828e0 agent.t
안	C TC			/usr/sbin/sendmail n
ŵ	# TTLs			log.offset: 2,665 1
ê	# Z	> May 15,	2020 @ 18:44:23.359	ts: May 15, 2020 @ 1
	t_id			_geoip_lookup_failur

V I	Sudiizations			
Q	Search			
	Title	Туре	Description	Action
0	Bytes Timeline [Filebeat NATS] ECS	<u>I∕i</u> Line		Ø
0	ASA Events Over Time [Filebeat Cisco]	<u> </u> M Vertical Bar		Ũ
0	ASA Firewall Blocked by Source [Filebeat Cisco]	🗐 Data Table		Ũ
	ASA Flows by Network Bytes [Filebeat Cisco]	🔟 Vertical Bar		Ø
	ASA Top ACL by Blocked [Filebeat	_		

Left Click on the Coordinate Map icon:



Note: Take a minute to explore the Visualization area and see the different types of panels you can create. There is a lot of flexibility for what you can do with the Kibana visualization dashboard.

## Type log - or logstash and Left **Click logstash-\*:**

**Left Click** the **+ Add** selection under Buckets and click Geo coordinates:

=

Data

logstash-\*

Metrics

**Buckets** 

Options

+ Add filter

## New Coordinate Map / Choose a source



**Left Click the Aggregation** drop down and **select Geohash** — **Left Click** the **Field** drop down and **Left Click geo.iplocation**, and the **Left Click** the **play** radio button as highlighted below:

ogstash-*	0	A 7
ata Options D X		
Metrics		Ħ
> Value Count		• 2.35
Buckets		
$\lor$ Geo coordinates		NORTH
Aggregation oconasi neip		AMERICA
Geohash 🗸		
Field		Le la
geoip.location $\checkmark$		and the
Change precision on map zoom	:	L'autre
Place markers off grid (use geocentroid)		SS-AP
Only request data around map extent		SOUTH
Custom label		5
> Advanced		

Left Click Options and select Heatmap, and then click the Save radio button as shown below:



Note: If you use a WMS Map Server you can have the selected data display over that map, you just need to click the radio button to turn that on and enter you WMS URL, along with the appropriate layers, version, and format. Assign WMS Attribution strings, and then you can use comma separated lists of WMS Server supported styles if you use them, but you can leave that blank as well. Some servers use transparent layers, so you will need to use a png file type for the WMS Format if that is the case, or it will be transparent and won't display very clearly.

You should now have an output like the following. Remember, you can adjust the cluster size in the options pane if you want to make the heatmap circles larger — it's a preference for how you would like to see the heat map. Next, we need to save the Visualization — I will detail how to do that, and once you do one, you can repeat the same process each time. In the steps after this one, I will just display how to generate the visualization to save space.

Refer back to the following steps to save your visualizations. The rest of these visualizations will give you a great idea of how to make your own custom visualizations. Feel free to play around with different visualizations and create a dashboard that works for you. I will provide the basic dashboard that I found important for my setup.



# Saving Visualizations

## Left Click Save:

K	D Visualize / Create			
G	Save Share Inspect Refresh			
Ø	🖫 🗸 Search	KQL		Ma
	🗐 — + Add filter			
	logstash-*	E	20	1
	Data Options	1	1	
O	Map type ti	÷.,	~	6
		~ . *	CANAI	DA
Q		8	-	
	Legend position	in the second		
	Bottom right V	12-1	2 -	
	Show tooltip	1-1	10	UNI
<u> </u>	O Desaturate tiles	1.	, en	STA
<u>س</u>	Base layer settings	Los Ang	eles	~
Ч	O WMS map server		3. 1	

**Fill out** the **Title** Information that you want to name the Visualization, the **description** and **Left Click Save** in the lower right corner.

Note: You should get a pop up in the lower right corner of the Kibana page that shows saved and the name of the visualization.



# View the Newly Created Visualization

## Left Click Visualizations:

K	D Visualize
٩	
Ø	Visualizati
<u>}</u>	VIOGUNZUCK
50	Q Search
Ê	Title
8	

**Type** the name of the Visualization that you created and **Left Click** it from the list provided:



Note: Once you select the Visualization you will be back at the editing menu for it. This is how you can go back and change your Visualization. We will go over how to do this from your dashboard as well, but you can change any specific Visualization and it be relayed to the dashboard because the dashboard is built off the Visualization itself, so if it's change, the dashboard will reflect too.



## GeoIP Unique Count

This Visualization is going to allow you to show the specific unique counts of network traffic that correlates to your heat map you just created. The heatmap shows the large area of usage, while this will show specific counts based off of a color chart.

## Left Click on Visualize:

Left Click on Create Visualization:



Vi	sualizations	Œ	Create visualization	
Q	Search			
	Title	Туре	Description	Action
0	Bytes Timeline [Filebeat NATS] ECS	<u> </u> √ Line		Ũ
0	ASA Events Over Time [Filebeat Cisco]	<u> </u> N Vertical Bar		Ũ
0	ASA Firewall Blocked by Source [Filebeat Cisco]	🗐 Data Table		Ũ
0	ASA Flows by Network Bytes [Filebeat Cisco]	<u> </u> Vertical Bar		Ũ
	ASA Top ACL by Blocked [Filebeat	-		ñ

## Left Click Coordinate Map:



**Type log** — or **logstash** and **Left Click logstash-\***:

#### New Coordinate Map / Choose a source

Q log	8	Sort $\lor$	Types 2 🗸					
🛱 logstash-*								
Q All ASA Logs [Filebeat Cisco]								
Q All logs [Filebeat Kafka] ECS								
○ Error logs [Filebeat MongoDB] ECS								
Q All logs [Filebeat MongoDB] ECS								
$\rm Q$ Apache errors log [Filebeat Apache] ECS								
Q Apache access logs [Filebeat Apache] ECS	○ Apache access logs [Filebeat Apache] ECS							
Q Error Logs [Filebeat AWS]								
< 1 2 3 4 >								

logstash-\*

**Left Click the Value** drop down and **Left Click** the **Aggregation** text box, and scroll down and **Left Click Unique Count**:

Left Click the Field drop down, and scroll down until you see geo\_point, and Left Click geoip.location:

In the Buckets pane, **Left Click Add** and the **Left Click Geo coordinates**:

Left Click Geo Coordinates and then Left Click the Select an Aggregation drop down, and Left Click Geohash:

Buckets

Aggregation

Geohash

✓ Geo coordinates

Select an aggregation

ata Options			×
Vetrics			
$\lor$ Value			
Aggregation	Uni	que Count he	Ip
Unique Count		~	
Field			
geoip.location	ĩ	$\sim$	
Custom label			
> Advanced			
Buckets	🔁 Add		
AI	D BUCKET		
G	eo coordinates		



231

×

0

**Left Click** the **Save** radio button just like the last Visualization:

Note: Ensure that geoip.location is selected in the Field drop down just like the heat map we created earlier. Mine was auto populated, but if it isn't just select it.

ogstasn-*			•			CAN	
ata Options		~	e se		> -	2	
Aggregation Unique C	ount help		Ju ta y			~	
Unique Count	$\sim$	1					
Field			ince R	upert	$\sim$		
geoip.location	$\sim$		e a	6.	Edmo	onton	
Custom label				Ê.	Calg	ary	aska
> Advanced				Vancou Se Portla	tle H	lelena	-
Buckets				0	REGON Boise	WY	омі
arsigma Geo coordinates		:			Salt NEVADA	Lake City	۷ [
Aggregation Geo	hash help			San Fra	cisco		
Geohash	$\sim$				Las Veg	as	Sar
Field					Los Angeles P	hoenix	

Note: Once you hit play you can see an output of dots similar to the picture above. You can go to options and change the colors if you want, but the default for mine is reds. Once you are finished save this Visualization — I named this Visualization SIEM GeoIP Unique Count — just like the last one and name it something you'll remember.

# Top Network Traffic Generation

We are going to create a pie chart that can quickly show you which IP Addresses are generating the most network traffic on the network you are monitoring.

Left Click on Visualiz	e:							
Left Click on Create Visualization:						Open rch	Share	Inspe
Vicualizations				Visua ogstar	alize sh-*	ilter (change eld na	e) 0	50
VISUAIIZACIOLIS				lization	<b>1</b>	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
Cl Search								
Title	Туре	Description		Actions				
ASA Events Over Time [Filebeat Cisco]	<ul> <li>M Vertical Bar</li> </ul>			ı ı	1			
ASA Firewall Blocked by Source [Filebeat Cisco]	🗐 Data Table			^				-
ASA Flows by Network Bytes [Filebeat Cisco]	<u>ोग</u> Vertical Bar			Ν	lew \	Visua	lizatio	n
ASA Top ACL by Blocked [Filebeat	-		_		C Filter	r		
<b>Go to Visualizations</b> , previous steps, and th	and <b>create Visuali</b> : en <b>Left Click Pie</b> :	<b>zation</b> just like	the		ين Lens	B	Area	Col
<b>Type Log</b> and <b>Left Cli</b> a source popup:	Гуре Log and Left Click logstash-* at the New Pie / Choose a source popup:						Gauge	G
	New Pie / Ch	noose a source	1		Horizonta	Il Bar	Line	M
	<ul> <li>Q log</li> <li>∰ logstash-*</li> <li>Q All ASA Logs</li> </ul>	[Filebeat Cisco]	F		8 Metrie	c	Pie	[ Regio
							~	

Left Click + Add — under the Buckets pane —

Left Click Split Slices:

Left click Aggregation

**Left Click Significant Terms** — once the Field menu pops up —

**Left Click id\_orig\_host.keyword** — you may have to scroll down to it — and the **type 10** in under size and press return, or hit the play button for it to update the pie chart with those settings:

**Save** the **Visualization** the way we saved it in the previous steps — I saved mine as SIEM Top Network Traffic Generation.

Buckets	
$ \lor $ Split slices	© ×
Aggregation	Significant Terms help
Significant Terms	$\checkmark$
Field	
id_orig_host.keyword	~
Size	
10	٢
Custom label	
> Advanced	
A 🕀	Add

logstash-*			0
Data Options		$\triangleright$	$\times$
Metrics			
✓ Slice siz	e		
Aggregation		Count he	elp
Count		$\sim$	/
Custom label			
> Advanc	ed		
Buckets			
	🕀 Add		:
	ADD BUCKET		
	<u>Split slices</u>		
	Split chart		



## **Top Network Applications**

This Visualization will show you the top network Applications based off the OSI Presentation Layer 6 data that is traversing your network. This Visualization will help you see what kind of data is being sent across the network, and what applications may be running.

### Left Click on Visualize:

### Left Click on Create Visualization:

Note: Now that you should have a good idea of how to create a Visualization and save it, I will start combining some of the steps, and show what selections you should make to create the Visualization. If you need to see anything new I will slow down and show the steps one at a time.

Go to Visualizations, and create Visualization just like the previous steps, and then Left Click Pie:



Q Search				
ew Visu	alizatio	n		
ζ Filter				
Lens B	Area	Controls	Ocoordinate Map	<b>Type Log</b> and <b>Left Click logstash-*</b> at the Net Choose a source popup:
Data Table	Gauge	Goal	00 Heat Map	New Pie / Choose a source
Horizontal Bar	Line	Maps	[Ţ] Markdown	
8 Metric	Pie	CC Region Map	<mark>П.</mark> TSVB	<ul> <li>All ASA Logs [Filebeat Cisco]</li> <li>All Logs [Filebeat Kafka] ECS</li> </ul>
		<u> </u>		

Left Click the + Add selection under Buckets

Left Click Split Slices:

Left Click Significant Terms under Aggregation

Left Click service.keyword under Field

Type 10 under Size

Data Options

Left Click play or press Enter / Return:

Note: At this point you should see something similar to the above picture. I didn't generate that many logs for this example, so I'm only showing http, https, and SSL. The Size of 10 means you will see up to the top 10 presentation or session layer types.

Metrics		( <b></b> )	
	170		
	n	Count be	In
Count		~	
Custom lab	el		
> Adva	nced		
Buckets			
DUCKEIS	Add 🕀		
	ADD BUCKET		
	Split slices		
	Split chart		



At this point you need to save the Visualization and name it — I named this Visualization as **SIEM Top Network Applications**.

# **Top Network Traffic Destination**

This Visualization is going to show you the top Network Traffic Destinations. This is good for knowing what your big traffic producers are. When combined with the Zeek (Bro) Signature for detected exfiltration, this can come in handy. It's also good to know because you can also tweak some network settings — if needed — to accommodate the large producers on the network for load balancing and overall throughput. You always want to have a good idea of what is generating or receiving the most traffic on the network.

## Left Click on Visualize:

K	Discover		
C	New Save Open Share	Ir	spect
Ø	🖫 🗸 Search		
	Visualize		
5	logstash-* (change)		
寙	Q Search field na		
0	Filter by type 0		5000
	Selected fields	Int	4000
,00		õ	2000

## Left Click on Create Visualization:

Vi	sualizations	Œ	Create visualization	
Q	Search			
0	Title	Туре	Description	Actions
	Bytes Timeline [Filebeat NATS] ECS	<u> ∕∕</u> Line		Ø
0	ASA Events Over Time [Filebeat Cisco]	旧 Vertical Bar		Ø
0	ASA Firewall Blocked by Source [Filebeat Cisco]	📰 Data Table		Ø
0	ASA Flows by Network Bytes [Filebeat Cisco]	<u>ति</u> Vertical Bar		Ø
	ASA Top ACL by Blocked [Filebeat	_		-

**Go to Visualizations** and **create Visualization** just like the previous steps. **Left Click Pie**:



## **Type Log** and **Left Click logstash-\*** at the New Pie / Choose a source popup:

New Pie / Choose a source				~	
Q log	۵	Sort $\checkmark$	Types	2 ~	
n logstash-*					
○ All ASA Logs [Filebeat Cisco]					
Q All logs [Filebeat Kafka] ECS					
$\bigcirc$ Error logs [Filebeat MongoDB] ECS					
$\bigcirc$ All logs [Filebeat MongoDB] ECS					
$\mathbb{Q}$ Apache errors log [Filebeat Apache] ECS					
$\mathbb{Q}$ Apache access logs [Filebeat Apache] ECS	ŧ.				
Q Error Logs [Filebeat AWS]					
$\langle$ 1 2 3 4 $\rangle$					
Left Click + Add — under the Buckets pane —					

### Left Click Split Slices:

Left Click Significant Terms under Aggregation,

## Left Click id\_resp\_host.keyword under Field

## Type 10 under Size

## Left Click play or press Enter / Return:

Buckets		
$ \lor $ Split slices	© ×	
Aggregation	Significant Terms help	
Significant Terms	~	
Field		
id_resp_host.keyword	ı ~	Note: You sh
Size		following. I am
10	Q	top hand right
Custom label		
> Advanced		
4	Add	

Note: You should see an output similar to the following. I am not placing the IP addresses from the top hand right corner legend, for privacy.

At this point you need to save the Visualization and name it — I named this Visualization as **SIEM Top Network Traffic Destinations**.



## **Average Missed Bytes**

This Visualization will show you a gauge that uses metrics to determine if your SIEM / IDS is missing any network packets. You do not want there to be a high number here, because that means something is not working right. This will allow you to trouble shoot any issues that could arise and will quickly point out that something is wrong.



**Type Log** and **Left Click logstash-\*** at the New Metric / Choose a source popup:

**Left Click Aggregation** drop down

Left Click Average

Left Click Field

		Q All logs [Filebeat Kafka] ECS
eft Click missed_b	ytes	Q Apache errors log [Filebeat Apache] ECS
		Q Apache access logs [Filebeat Apache] ECS
<b>eft Click</b> the <b>save</b> r	adio button:	Q All Logs [Filebeat PostgreSQL] ECS
		C Error logs [Filebeat MongoDB] ECS
ogstash-*		C All logs [Filebeat MongoDB] ECS
Options	⊳ ×	< 1 2 3 4 >
Metrics		
✓ Metric		
Aggregation	Average help	
Average	$\sim$	
Field		
miss	$\sim$	
number	logstash-*	0
missed_bytes	Metrics	
missing_byt missed_bytes	Metric Aggregation Average help	
> Advanced	Average V	
🕀 Add	missed_bytes ~	
	> Advanced  Add	
Buckets	Buckets	
🕀 Add	Add	
		- Average missed_bytes
_		
		L
		Average missed_bytes

New Metric / Choose a source

C All ASA Logs [Filebeat Lisco]

Q log

🕂 logstash-\*

X

Sort  $\checkmark$  Types 2  $\checkmark$ 

0

Note: You should see an output similar to the following. Zero missed bytes is a good thing, and I tested this out by making some tweaks with Zeek (Bro), and the SIEM will pick up if anything is missing.

# Sum of Bytes

This Visualization will show you the total Sum of Bytes captured on the network. It's important to quickly see that your SIEM is working and capturing traffic, and this metric allows you to do just that.



Go to Visualizations and create Visualization just like the previous steps.

## Left Click Metric:



**Type Log** and **Left Click logstash-\*** at the New Metric / Choose a source popup:

Left Click Aggregation drop down. × New Metric / Choose a source Left Click Sum Q log ٢ Sort  $\lor$  Types 2  $\lor$ 📱 logstash-\* Left Click Field Q All ASA Logs [Filepeat Cisco] Q All logs [Filebeat Kafka] ECS Left Click total\_bytes ○ Apache errors log [Filebeat Apache] ECS ○ Apache access logs [Filebeat Apache] ECS Left Click the save radio button: ○ All Logs [Filebeat PostgreSQL] ECS ○ Error logs [Filebeat MongoDB] ECS Q All logs [Filebeat MongoDB] ECS logstash-\* < 1 2 3 4 > Data Options X Metrics ✓ Metric You should get an output similar to the Aggregation Sum help following picture. Sum Field total\_bytes  $\sim$ **Custom label** • 0 + 50 50 + 75 • 75 + 100 > Advanced Ac **Buckets** O Ado 🕀 Ac O Add Sum of total\_bytes 6,098,441 Sum of total\_bytes

## **Notices Generated**

This Visualization is one of the most important ones you will have — notices generated by Zeek(Bro). This is a quick way to show you how many notices have occurred. These notices are generated by Zeek (Bro) when it detects an anomaly on the network — signatures are used to generate the notices and you can use many different kinds of signatures for whatever reason you choose.



Go to Visualizations and create Visualization just like the previous steps.

### Left Click TSVB:



**Left Click** the Color Box that is green and make it a color you want to stand out - I chose red:

Left Click Label and type Notices:

Note: You can put any label

name that is of interest for you on your specific network

and make another Time

Series metric for that data.

This is a useful way of

looking for specifics over

time on your network.

Left Click Panel options and Type the following under Panel filter:

## actions.keyword :\*

Auto apply Data Panel options Annotations				The changes	will be automatically appl
Data Index pattern	Time field	4		Interval	Drop last bucket?
logstasn-* Default index pattern is used. To query all indexes use *	(@time	istamp		Examples: auto, 1m, 1d, 7d, 1y, >=1m	]
Panel filter actions.keyword :*				KQL	Ignore global filter?
Style					
Axis min	Axis max	Axis position Left	Axis s	rmal	~
Background color: 📈 ×	Show legend? • Yes · No	Legend position Right	∼ Di	splaygrid 💽 Yes 🚫 No	

The final output for this Visualization should look similar to the following:



# Building the Dashboard

The Dashboard is an important tool for looking at information in your SIEM. It is essentially the view of your SIEM and built off of Visualizations. You can build this however you want, and you can use any visualization you choose. In the following steps I'm going to show you how to create your own dashboard. I had previously setup a dashboard for CSI Linux, so I will be using the Visualizations from that just to make it easy, and show what CSI Linux has available — it's a great digital forensic tool, and can be located at csilinux.com.



Note: You will get an output similar to the following. In order to move the panes around just click the top portion in the area where I highlighted, and you can also drag the dotted edges and re-size the panes. You can arrange this area any way you like, play around with it and see how you want it. You can click add up top and add more panes too.


I added a highlight to the corner where you need to drag to re-size the panes as follows:

Save Cancel Add Options Share	
😰 🗸 Search	KQL  ( → Apr 20, 2020 @ 00:00:00. → Apr 21, 2020 @ 00:00:00. C Refresh
·── + Add filter	
CSI-SIEM GeolP Unique Count() (CSI-SIEM GeolP Unique Count()	IP Heat-Map
Calgary Regina Winnipeg Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouver Vancouve	Calgary         Saskatoon Regina         Winnipen           uver         Thunder Bay         Quebpc         Charlottetown           and         Pierre         Minneapolionstin         Corroto         Boston           Salt Lake City         Pierre         Minneapolionstin         Toronto         Boston           Salt Lake City         Derwer Stattes         Saint Louis         Washington         Saint Louis         Washington           Incisco         Las Vegas         Santa Fe         Oklahoma City         Merr         Norfolk           Los Angeles         Phoenix         Dallas         Jacon         Coresta         Hamilton           Chiltrahus         Houston         Heast         Oper@restature         Coresta         Saint Louis         Oper@restature
CSI - [SIEM] Notices Generated	101
3	Notice 0
0000 0300 0600 0500 1200 per 10 minutes	15:00 18:00 21:00

Now your dashboard is complete, we need to save the dashboard.

## Saving the Dashboard

### Left Click Save:

	Dashboard / Editing New Dashboard (unsaved)
C	Save Cancel Add Options Share
Ø	B ∨ Search
	(⇒) - + Add filter
80	CSI-SIEM GeoIP Unique Count ()
ŵ	Vancouver     Vancouver     Vancouver
0	Seotle Helena Bismarck Québec
(***)	ti Portland Pierre Minneapolisonsin + Ottawa MAINE Charles Ha
ු	Boise WYOMING Chicago Detroit Boston
	Salt Lake City UNITED INDIANA Pittsburgh New York

### Left Click the title and Type the title you want to use, and Left Click Save:

Nov will

<i>v</i> when you go to the Dashboards menu you see your dashboard:		SIEM Dashboard Description	
Da	ashboards		
Q	Search		
	Title	Description	
	CSI - SIEM [Zeek] Dashboard		X Store time with dashboard
	SIEM Dashboard		This changes the time fitter to the currently selected time each time this dashboard is loaded.
	[Filebeat AWS] S3 Server Access Log Overview	Filebeat AWS S3 Server Access Log Ov	
0	[Filebeat Apache] Access and error logs ECS	Filebeat Apache module dashboard	
0	[Filebeat Auditd] Audit Events ECS	Dashboard for the Auditd Filebeat module	0
	Ten i a a a a a a	This dashboard provides expanded alerts of	overview for

Save dashboard

٦

Title

That concludes the entire ELK Stack SIEM process. We learned how to set up Zeek (Bro), PF\_Ring, ElasticSearch, Logstash, Filebeat, Kibana, and create a SIEM Dashboard. I challenge you to continue to create and modify your ELK Stack and use it to the best of your ability.

# AWS Phishing Layer 8

<sup>By</sup> Nitin Sharma

## Introduction

At the source of every error which is blamed on the computer, you will find at least two human errors, one of which is the error of blaming it on the computer. - Tom Gilb

Cybersecurity is evolving at a rapid pace and so is the pace of Threat Landscape today. Sophisticated cyber-attacks are capable of bringing down enormous business empires. Staying resilient, responding intelligently and recovering quickly are the major aspects organizations are looking in cybersecurity enthusiasts. However, there is no change in human nature.



Photo by Chris Yang on Unsplash

All the technologies and inventions till date are considered as a boon for mankind. Instead of acting as enablers or force multipliers, these could go wrong with simple human error. Even the smartest ever solutions, need human intervention for successful operation thus becoming highly prone to human errors. Manipulation of human behavior creating new normal, to make them to believe in something, is psychologically possible too. One can say, people are an organization's most valuable asset, but they can also be its greatest vulnerability.

With all such scenarios keeping in mind, some additional layers to OSI model have been defined and adopted informally.

## Extended OSI Model

Bruce Schneier and the company RSA Security LLC invented the concept of layers above the OSI layer. <sup>[1]</sup>



Extended OSI Model

As far as we have discussed about the 7-layer abstract model which describes an architecture of data communications for networked computers, the concern remains solely from technical perspective. To induce the feel of human intervention, these three layers were added <sup>[2]</sup>,

- 1. Layer 8 (Individual/Human Layer) covers the realm for human interactions where people deal with technology interfaces. This is where we engineer solutions and architectures which allow for the human factors, psychology, and sociology. E.g. DLP (Data Loss Prevention Solution).
- 2. Layer 9 (Organization Layer) covers the modularity aspect of people involved in business who work in a collective fashion to deal with technical aspects. Organizations are complex entities, and few people indeed have a handle on just how complex they are. As they get larger, organizational complexity increases exponentially against linear organization growth, because the number of linkages, data flows and relationships exponentially multiply. Example includes eGRC (Governance, Risk and Compliance) solutions like RSA Archer.
- 3. Layer 10 (Legal and Compliance Layer) covers the legal aspect of human involvement which encompasses technology layers with a set of compliance rules to be met. This is where an organization government or non-government specifies requirements which the organization must comply with. Often there are penalties for non-compliance, and sometimes those penalties drive controls right down the stack.

The primary concern for adding these layers is to bring user-in-the-loop factor to the traditional OSI model. Considering from a security perspective, let's assume a bank is going to be robbed. To achieve this, hackers target banking servers to attack. While attacking, they will not be able to bypass the banking firewalls, IDSs, IPSs. Now, they want another way for information to get into the banking servers. The prime target for such kind of attacks are people who work in that bank. Hackers will observe, follow, and extract the information from the behavior of bank employees. These all aspects are covered in a single term called Social Engineering which is an art of manipulating people. The extended OSI model comes to rescue when considering social engineering and similar attempts.

### Layer 8: Perspective and Use Cases

Layer 8 hypothesis include all user errors to be considered while managing troubleshooting efforts. When the users do not know about the solution to a problem, they try to judge and devise their own solutions and commit mistakes. This is one of the causes and use cases for Layer 8. However, it does not mean that everything is done unknowingly – "BY MISTAKE". When people go beyond authorized well defined rules trying to help someone or to achieve early completion of assigned tasks, they commit human errors knowingly.

In a web-application, when someone input a wrong field value in a form, he often sees it as, not found, or non-applicable upon submission of form. Even if he knows this, and he will submit a series of such values, once he will reach a point to be able to break into the application, irrespective of the time and process constraints. If you observe the minute details, this time constraint could be reduced, and process constraint could be improved. In Layer 8, the same applies to human behavior which acts as a web application form field, give the input, observe the output, and improvise upon this.

We have more often heard about the acronyms generally utilized to cite "USER ERROR" in a more anticipated and humorous fashion like,

- Fault Isolated in Layer 8
- Problem in Chair, Not in Computer (PICNIC)
- Problem Exists between Keyboard and Chair (PEBKAC)
- Code 18 Error which implies problem is sitting about 18" away from the screen.

Some more Layer 8 use cases include,

- Employees who find a prepared USB stick in the company car park and plug it into the USB slot of a company computer.
- Users who receive a telephone call where the other person pretends to be their boss and advises an urgent bank transfer.
- The careless handling of classic phishing emails containing malicious content.

### Layer 8: The OSINT Connection

Open-Source intelligence (OSINT) are gathered from open sources, the publicly available information. OSINT can be further segmented by the source type: Internet/General, Scientific/Technical, and various HUMINT specialties, e.g. trade shows, association, meetings, and interviews.

Human beings are "social animal". Aspects, definable as social, such as self-representation, community and interaction are classical of real life, common to everyone, even though they also deeply define the online behavior of the same people whom equally feel the necessity to create a self-representation in the world they live in (real or virtual), to build up ties with who is around (real or virtual subjects) and to interact with the people sharing common experiences.<sup>[3]</sup>

In the online world, tools such as retweet, likes and shares have been adapted to facilitate a complex system of indirect methods to get in touch with the other. Obviously, there is nothing wrong in this. And this is great to amplify or diffuse the message to the public, to entertain or inform a specific audience, to comment a tweet, re-posting it and adding new contents, to demonstrate the presence as listener, etc. However, if you orient towards the perspective of an intelligence analyst, this could be really interesting. For example, a bank executive from ABC bank often tweets about his daily running status 9 am every morning and a running posture excerpt from a fitness running app.

Interesting things that one can observe from this daily activity includes,

- Estimate of his/her morning schedule.
- Estimate of track information for his running.

[Bit more information]

- Where he/she lives?
- Where he/she took a break on the way to his home?
- How many break intervals during long running schedules?
- How much time is he/she out of his house?
- At how much pace, he/she can run?

See the following sample tweet.



**Morning Run** 

Utility of all such instances is vital when aggregated and correlated for predicting behaviors of concern. The inevitable surveillance of personal data might result in harmful or malicious circumstances with the technology combinations and OSINT and can make businesses to bear huge losses.

### Analysis: AWS Phishing Campaign

Phishing is a classic example of the failure to engineer strong Layer 8 solutions. Most of the people receive emails from organizations which invite the receiver of email to log into portals using links embedded in the email, which don't go to the organization's main website. Those logins often aren't protected by SSL/TLS or use in-house CAs.

AWS Phishing Campaign is a very recent example where attackers tried to steal AWS accounts through phishing. [Detected by researchers from Cado Security<sup>[4]</sup> and Abnormal Security<sup>[5]</sup>]

1. The attack was seen in the mid of May, 2020 in which people received phishing emails from attackers disguised as AWS Support.



- The links present in the email sends the user to "howitfix[.]com/app/aws which is an AWS phishing page hosted on a compromised server.
- 3. Researchers discovered that it was not an isolated attack. A network of AWS Phishing sites were using exactly the







Visit aws.amazon.com/free for full offer terms

same AWS phishing template, served from compromised domains.



The investigation revealed that phishing emails are being sent from rented server, using an email address from an Irish web-hosting company.

#### **Consequences and Compromise:**

The victims when click the phishing email link will be redirected to an AWS Phishing page – a look alike with AWS login page. Submitting user credentials for an AWS account will result in a user compromise with all the resources an AWS IAM user has access to. However, submitting Root login credentials will compromise complete AWS account.

These compromised AWS accounts will be traded for as little as \$4 (for free tier account) onwards. Also, these accounts could be utilized for phishing via Amazon Simple Email Service (SES).

### Lessons Learnt

The Extended OSI Model has advantages when considering the other 3 layers while defining the IT security policies for an organization. Defining AUPs and restricting the control definitions appropriately provides an opportunity to monitor employees and their workflow.

OSINT philosophy and usage with Human Interaction Layer is a great way to find out and fulfilling the gaps in an IT security strategy. There is a need to think about business personnel as an integral part of organizational security aspect, such that both the personnel's as well as organizational security concerns will be considered. Security awareness trainings, phishing email exercises, etc. are some of the measures to follow and tighten the enterprise security posture.

We have seen the example for AWS Phishing Campaign which was carried recently. Now, that keeping in mind one can think of Google Cloud Platform Phishing Campaign or may be Azure next. There is no limit to social engineering as it always come up beyond one's expectation and imagination.

### References

[1] Is it possible to Monitor OSI Model Layer 8, Sascha Neumeier, IT Insights, Paessler. Published on Sept. 9, 2019, Last Updated on June 15, 2020. Last Accessed on June 30, 2020. - <u>blog.paessler.com/is-it-possible-to-monitor-osi-model-layer-8</u>

[2] Engineering Security Solutions at Layer 8 and Above, Sam Curry. Published on Dec.
 7, 2010. Last Accessed on June 30, 2020. web.archive.org/web/20130524214239/blogs.rsa.com/engineering-security solutions-at-layer-8-and-above/

[3] From SOCMINT to Digital Humint: re-frame the use of social media within the

Intelligence Cycle, Marco Lombardi, Todd Rosenblum, Alessandro Burato. Last Accessed on June 30, 2020. - <u>fondazionedegasperi.org/wp-</u> <u>content/uploads/2016/10/Paper-From-SOCMINT-to-Digital.pdf</u>

[4] An ongoing AWS Phishing Campaign, Chris and James, cadosecurity.com. Published on Jun. 11, 2020. Last Accessed on June 30, 2020. - <u>cadosecurity.com/2020/06/11/an-ongoing-aws-phishing-campaign/</u>

[5] Abnormal Attack Stories: AWS Phishing, abnormalsecurity.com. Published on May 27, 2020. Last Accessed on June 30, 2020. - <u>abnormalsecurity.com/blog/abnormal-attack-stories-aws-phishing/</u>

# **CIR** Contributors

Amy Martin, Editor Carlyle Collins, Editor Daniel Traci, Editor/Design Jeremy Martin, Editor/Author Richard K. Medlin, Editor/Author Nitin Sharma, Editor/Author Justin Casey, Author LaShanda Edwards, Author Mossaraf Zaman Khan, Author Ambadi MP, Author If you are interested in writing an article or walkthrough for the Cyber Intelligence Report, please send an email to cir@InformationWarfareCenter.com

If you are interested in contributing to the CSI Linux project, please send an email to: csilinx@informationwarfarecenter.com

I wanted to take a moment to discuss some of the projects we are working on here at the Information Warfare Center. They are a combination of commercial, community driven, & Open Source projects.

## Cyber WAR (Weekly Awareness Report)

Everyone needs a good source for Threat Intelligence and the Cyber WAR is one resource that brings together over a dozen other data feeds into one place. It contains the latest news, tools, malware, and other security related information.

### InformationWarfareCenter.com/CIR

### CSI Linux (Community Linux Distro)

LINUX CSI Linux is a freely downloadable Linux distribution that focuses on Open Source Intelligence (OSINT) investigation, traditional Digital Forensics, and Incident Response (DFIR), and Cover Communications with suspects and informants. This distribution was designed to help Law Enforcement with Online Investigations but has evolved and has been released to help anyone investigate both online and on the dark webs with relative security and peace of mind.

At the time of this publication, CSI Linux 2020.3 was released.

### CSILinux.com

(Si

### Cyber "Live Fire" Range (Linux Distro)

This is a commercial environment designed for both Cyber Incident Response Teams (CIRT) and Penetration Testers alike. This product is a standalone bootable external drive that allows you to practice both DFIR and Pentesting on an isolated network, so you don't have to worry about organizational antivirus, IDP/IPS, and SIEMs lighting up like a Christmas tree, causing unneeded paperwork and investigations. This environment incorporates Kali and a list of vulnerable virtual machines to practice with. This is a great system for offline exercises to help prepare for Certifications like the Pentest+, Licensed Penetration Tester (LPT), and the OSCP.

### Cyber Security TV

We are building a site that pulls together Cyber Security videos from various sources to make great content easier to find.



### **Cyber Secrets**

Cyber Secrets originally

aired in 2013 and

covers issues ranging from Anonymity on the Internet to Mobile Device forensics using Open Source tools, to hacking. Most of the episodes are technical in nature. Technology is constantly changing, so some subjects may be revisited with new ways to do what needs to be done.

### Just the Tip

Just the Tip is a video series that covers a specific challenge and solution within 2 minutes. These solutions range from tool usage to samples of code and contain everything you need to defeat the problems they cover.

### **Quick Tips**

This is a small video series that discusses quick tips that covers syntax and other command line methods to make life easier

### CyberSec.TV



Active Facebook Community: Facebook.com/groups/cybersecrets

# Information Warfare Center Publications



Threat Intelligence and Hacking training. The Cyber Intelligence Report series covers hacking, forensics, threat intelligence, and everything in between. This issue will focus on a little SCADA/ICS, Dark Web, and how to identify a vulnerability and write an exploit for it. Here is a list of some of the chapters: Triton... The Russia-Linked Cyber ICS WMD, Advanced Persistent Threats, The Cyber Kill Chain, Securing Data at Rest and Data in Transit Anonymity on the Internet, Zeek (Bro) IDS - Installation & Configuration, and VulnServer: TRUN Buffer Overflow walk through. amzn.to/2MI2xxI

Dive Into the 5th Domain: Threat Intelligence includes: Cyber

Attacks Can Kill, Dark Web News and Dark Market Exit Scams, OSINT & Online Investigation Tips, Online and Dark Web Investigations: CSI Linux, CSI Linux Forensic Challenge, Chain of Custody Template, Data destruction & recoverability, Anonymity on the Web (Tor and Privoxy), OSINT Reconnaissance (Recon-ng walkthrough), Autopsy Installation in Linux, Elastic Stack with Zeek (Bro) IDS Integration, Configuring Zeek (Bro) IDS Signatures, and more... amzn.to/37gPfBE





Red Teaming Around Your Backyard While Drinking Our Juice

in The Hood includes OIT, Cyber Scams and Attacks, Software Defined Radio (SDR fun), Dark Web Information, Tools and Tips, Iranian Backed Fox Kitten APT, Red Team War Story, Post Exploit: Island Hopping/Pivoting, Hacking Challenge, Reverse Engineering using Ghidra Challenge, Online Privacy/Anonymity, Offensive Tactics, Reconnaissance with SpiderFoot, CVE Vulnerability Scanning using NMAP, Using NMAP for Exploitation, Penetration Testing and Exploitation Using NMAP and tools, SEH Buffer Overflow Exploitation on Windows 10, and more... amzn.to/3f4HT6W

A network defender's GUIde to threat detection: Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more. This book covers the entire installation and setup of your own SOC in a Box with ZEEK IDS, Elasticstack, with visualizations in Kibana. amzn.to/2AZqBJW





Do you want to learn how to conduct vulnerability assessments or penetration tests but don't know where to start? Are you getting into computer forensics and want some

more hands on practice with more tools and environments? Well, we have something that might just save you some time and money. amzn.to/30xOvGX