ARKA KAPI

Bimonthly Cyber Security Magazine

08 November-December www.arkakapimag.com

Digital Security for Journalists

Device Monitoring with OSQuery and Logging to AWS

Home Style Cyber Threat Intelligence

Cyber Security in Critical Infrastructures

Through the Eyes of a Computer Forensics Analyst: Windows Forensic

From a Forensic Scientist's Pen: Windows Forensic

Gathering Intelligence with Maltego

Hunting the bans in Fantasia - How to open a website in the TOR Network

ISSN 2645-906X

9 772645 906009

Editor's Note

Hey everyone!

This 8th issue is December 2019 - January 2020 issue, so who knows - when you read this issue, maybe it will already be 2020! In such case, happy new year everyone! I hereby celebrate your Hanukkah and Christmas as well :)

Each day, we, as the whole world, embraced technology even more and took it more and more into our daily lives. Throughout the pages of our magazine, we talked about the methods of possible dangers in order to show you the ways of not falling for them. We talked about systems in general, we talked about hackers, and much more. 2019 has been a year full of incidents, good and bad. The very first photograph of a black hole was taken, and Julian Assange was taken into custody and got arrested, for example.

I hope that 2020 will bring you joy, more time with your loved ones and even more secure systems. And, I hope that 2020 will bring the world tranquillity and peace. Hoping that the only thing we worry about be forgetting our passwords!

Also, on 9th November 2019, we celebrated the very first year anniversary of the magazine with a (late) meetup as we promised - and for those who showed up, we showed our gratitude with pizza and cake! We once again remembered the joy of preparing the magazine and present it to your taste. Below are some photographs taken during the meetup.

We would like to thank Netsparker Ltd. for sponsoring this issue!

Cansu Topukçu
editor@arkakapimag.com

ARKAKAPI MAG

Cyber Security Magazine YEAR: 1 – SEP.-OCT. ISSUE: 6 Bimonthly - ISSN: 2645-906X www.arkakapimag.com

Editor in Chief: Ziyahan Albeniz • ziyahan@arkakapimag.com

Editorial Operations Manager: Cansu Topukçu • cansu@arkakapimag.com

Chief Business Officer: Oğuz Aydınyılmaz • oguz@arkakapimag.com

Publishing Coordinator: Şahin Solmaz • sahin@arkakapimag.com

Director of Web: Ömer Çıtak • omer@arkakapimag.com

Legal Advisor: Mehmet Pehlivan • mehmet@arkakapimag.com

Assistant research editor: Ayşenur Burak • nurayse47@gmail.com

Translators: Merthan Telli, Nuri Çilengir, Ulaş Fırat Özdemir, Zekvan Arslan

Social Media Directors: Nuri Çilengir, Tayfur Özkara

Social Media links: twitter.com/arkakapimag instagram.com/arkakapimag facebook.com/arkakapimag

We are proud to secure all our emails with Tutanota.

CONTENT

Ayşenur Burak • nurayse@gmail.com

Cyber Security Conferences

BLACK HAT EUROPE

December 02-05, 2019

London, United Kingdom

Black Hat Briefings and Trainings are held annually in the United States, Europe and Asia, providing a premier venue for elite security researchers and trainers to find their audience.

Info: *https://www.blackhat.com/upcoming.html*

SEATTLE CISO EXECUTIVE SUMMIT Q4

December 11, 2019

Seattle, Washington, United States

As a Governing Body, the event was designed to address innovative, practical real-world solutions to top challenges, from digital transformation to board engagement and keeping the company secure — ensuring an invaluable experience for every CIO and CISO who participates.

Info: *http://bit.ly/31H5Muc*

IFSEC INDIA 2019

December 19-21, 2019

New Delhi, India

The event attracts visitors and exhibitors from all over the country as well as top experts from around the world that are represented with pavilions at the fair. The visitors are able to inform themselves in detail and comprehensively on security, fire protection, energy and environment and on the latest developments, trends, services and products in the fields.

Info: *https://www.ifsec.events/india/*

CLUTE INTERNATIONAL ACADEMIC CONFERENCES (CIAC) - ORLANDO

December 29, 2019

Orlando, Florida, United States

This conference aims to bring together faculty and administration from all levels of education across the world. This conference includes: Accounting, auditing, banking, Computer Information, Information Systems, Business Technology...

Info: *http://bit.ly/2N9BOK7*

CYBLOCK

January 07, 2020

Bengaluru, India

The Cybersecurity and Blockchain Workshop will be held in conjunction with the 12th International Conference on COMmunication Systems & NETworkS (COMSNETS). This workshop aims to be a forum where researchers can discuss and meet the newest in cybersecurity topics as they apply to communications systems and identify new technologies for blockchain.

Info: *http://bit.ly/2OXqOAx*

NDC SECURITY

January 22-24, 2020

Oslo, Norway

NDC Security 2020 is a 3-day event with workshops 22-23 January followed by a 1-day conference 24 January. Both the workshops and the conference will be held at the Clarion Hotel Oslo (Bjørvika).

Info: *https://ndc-security.com/*

CYBERUSA CONFERENCE

January 16, 2020

College Park, Maryland, United States

CyberUSA is a collaboration of states focused on a common mission purpose of enabling innovation, education, workforce development, enhanced cyber readiness and resilience - all while connecting the cyber ecosystem of the United States and its allies.

Info: *http://bit.ly/2Lado31*

CISCO LIVE BARCELONA

January 27-31, 2020

Barcelona, Spain

Cisco Live is Cisco's world-renowned annual customer and partner conference designed to provide the foundation for your digital future, giving you training, connections and inspiration.

Info: *http://bit.ly/33Bgqn6*

Alper Atmaca • info@alperatmaca.com.tr

Digital Security for Journalists

The world is a dangerous place. Mass genocides, global climate change, the meteors that meet in orbit etc. are the realities that constantly threaten humanity and the planet, but because of the low risk, they have almost no place in our daily life concerns. There is another danger in our lives that requires us to be extremely worried that we all live constantly and seriously at risk; risks related to digital surveillance and data security.

This danger constantly posed by organized enemies, against individuals and society, unfortunately, is considered a difficult situation to avoid for most people. History is full of examples of countless evil actors who have benefited from the comfort of learned helplessness, and the free press, the most important foundation of today's democratic order, is the first institution to be protected in the light of rising digital surveillance tools.

Journalists in danger because of their job have developed methods for people and information they need to protect. Under the protection of the law and the pressure of society, this possibility of protection, which had worked relatively well in ancient times, is eroding in these days when the Internet and computers are dominant. Digital surveillance; can be almost invisible, continuous and extremely invading. Some of the unfortunate fate of Saudi journalist Kaşıkçı can shed light on the future.

Now, we will share our suggestions item by item with reasons.

1. The predicate of security is discipline

If you're not Rick Sanchez, nothing in the planet Earth is unrequited. There is no magic wand to protect you against your enemies without a fight! Therefore, you should present your threat model and prepare for it. Then, unconditionally, you need to depend on your plan. Because providing security can be an expensive job in terms of both time and cash.

a. Evaluate Potential Danger:

While you live, evaluate and list possible dangers to your profession and the information you protect. This can be the physical properties of your home and workplace door durability or reliability of the devices and systems you use. Or, there may also be spiritual elements that may be used against you, such as your habits or loyalties. Identifying hazards allows you to identify the attack surface area and tools.

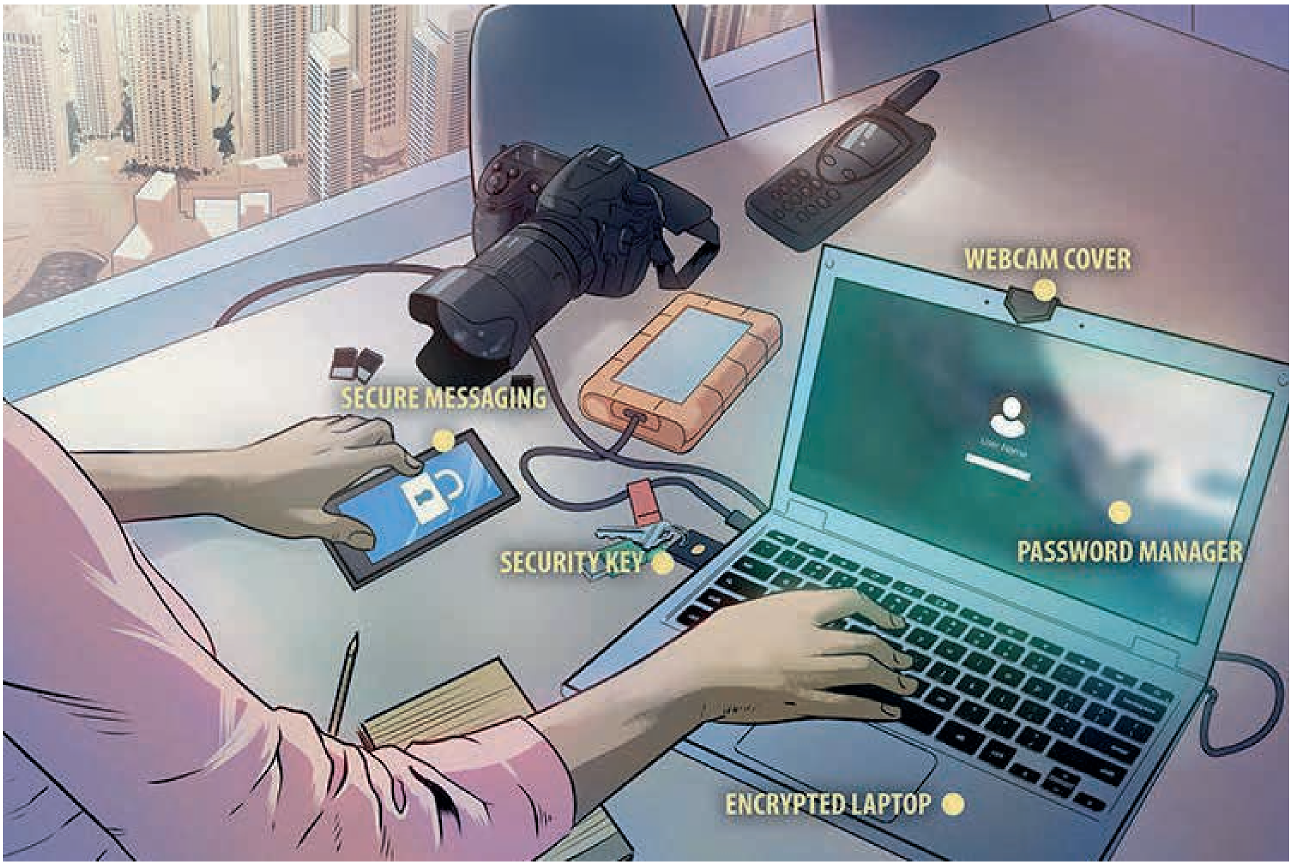
b. Assess Risk:

Risk is the probability that a hazard will occur. We may not take precautions against most dangers in our lives; like a meteor strike to Earth. We deal with hazards that are likely to happen and those that can be reduced. For this reason, consider the risk of danger to you that may make you a target for personal or business reasons. Questions like "Is it more likely for your computer to get lost or a group of black-dressed people come and steal it from your house?" will equate your security concern and your effort with reality. Not every journalist may be the target of the organized power of nation-states. But, it is a danger to everyone that someone who takes your phone can read all the information.

c. Take Measures Starting at the Highest Risk Level:

Once you have calculated your hazards and the risks of your hazards, you can start taking your precautions. Multiple measures can be taken against a hazard. For example, you can create unique passwords for your accounts and stored in the password manager and use multi-level authorization (2FA). Take precautions against all hazards in order, starting with the cheapest method. And do not compromise. Do not forget! You are the primary basis of every measure you take.

Unfortunately, you are the weakest link in all operational security. With social engineering or a moment of thoughtfulness, underestimating an improvement can endanger you and everyone who trusts you.



2. Follow the Security Chain:

Information security against digital tracking systems begins as a chain from the user. So, it starts with you. Then it switches to your device. It then follows the network you are connected to and the service you are using. It continues in the same order to the person you are communicating with. For this reason, your security will be as strong as the weakest link in this chain.

a. Human Security:

It is very important that you physically protect yourself and your devices and that you do not break your security discipline. This requires you to activate the screen lock when not near your device. It is also essential that you reliably generate and store the passwords you use.

i) Diceware, Password Manager and 2FA

ii) Really secure passwords are completely random and mixed. They must also be difficult for people to remember.

For this reason, passwords that are as random as they are difficult, but do not need to be remembered and written down, are needed. Diceware is a password generation method consisting of 7776 words and analogies, where you create your password using real physical dice. There are 7776 ^ 7 possibilities for guessing a 7-word password generated by this method. Difficult for computers but easy for people to remember! Use this password to assign unique and terribly difficult passwords to each account you use with the help of a password manager. For this, you can use free, Keepass or Pass.

Edit your password policy according to the conditions of use of the device. You may not need to change the password of your devices, such as your desktop and laptop, that you use on-screen passwords in more controlled environments. Mobile devices such as mobile phones are often used in environments with people and cameras. It is therefore advisable to change their passwords completely randomly, often. Mobile devices such as mobile phones are often used in environments with people and cameras. Therefore, passwords of mobile devices must be changed frequently, completely randomly. In any case, if in doubt, you should change your password without hesitation.

It is recommended that you evaluate 2FA on all your devices and accounts that offer multi-stage authorization (2FA) as well as password security. 2FA means that you can access your accounts with something you know (password) and something you have (your phone). Preferably, I want you to use this system with a code to be generated on your device through free software such as FreeOTP. In services that do not offer this possibility, it is better than nothing to provide the second stage by SMS.

iii) Hiding Password Entries:

Passwords are the most essential part of your information security. The use of this information is a constant danger, as it also means exposure to surveillance environments. To reduce the risk of this danger, you must ensure that the screens and keyboard on which you enter your passwords cannot be seen by others and by cameras. For this reason, it is recommended that you carefully select the locations where you use your computers. When entering a password on your phone, it is recommended that you close the screen manually. (see Edward Snowden).

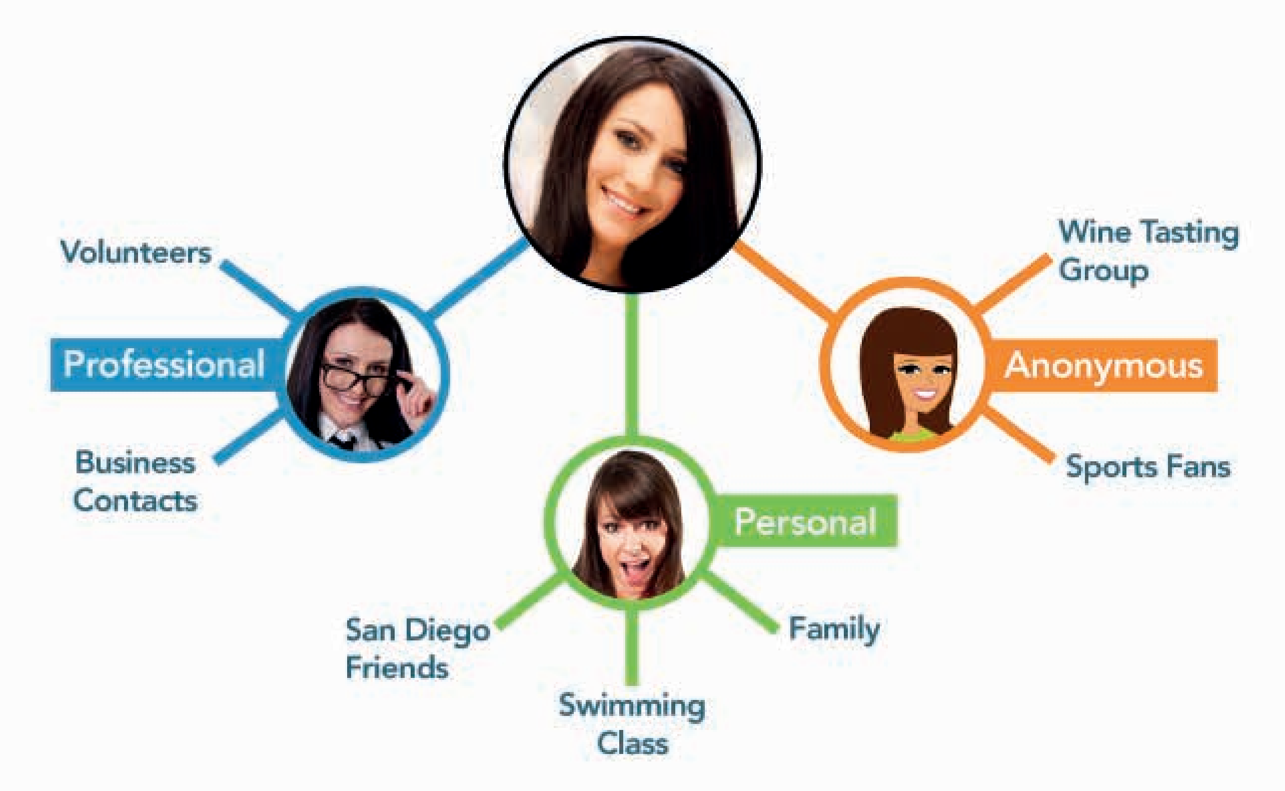
Similarly, you should protect your screen from unwanted viewers. For this, you need to get from movies that reduce the visibility angle of your screen. It is recommended that you use it on critical devices such as telephones and computers.

iv) Keep Your Communication With Doubt:

Never trust the content of the messages sent to you and the sender of the message. The easiest way to penetrate the system is human. Many known attacks have been successful in this way. The sender part of the e-mail can be easily imitated. Therefore, it is not easy to verify a person. Likewise, if potential malicious servers to which encrypted instant messaging software are connected are not authenticated, they may follow the communication by providing fraudulent encryption keys to the parties. To avoid the risk of phishing and malware, carefully approach the links or extensions that others send you, whether encrypted or unencrypted.

Separate your Identities

Do separate your business and private life. If your threat model requires extremes, you may use different devices and keep your social media accounts and email accounts separate. This way, you would isolate the harm in case of any breaches and you would not have to expose your identity while using.



Keep an eye on your devices

Having physical access to your devices provides a convenient medium for the attackers: they will have the opportunity of finding your device unlocked and also it will be possible for them to make changes that you probably will not notice. In this manner, retrieval of your encryption keys with high-quality attacks like Cold boot1, or making your device accessible by replacing pre-software installed on your operating system requires physical access, and the most effective way to prevent it is to keep your devices close to you in places you don't really trust. Protect your devices for the sake of not being a victim to *Evil Maid* attacks.

b. Device Security

All the precautions you take will be meaningless if you do not trust the devices you use. For sustainable operation

[1] *https://en.wikipedia.org/wiki/Cold_boot_attack*

integrity, it is a must-have that the hardware you use has been obtained from trusted sources, run reliable software and store all data in encrypted form.

Hardware

Do not purchase your products from traceable or predictable places and prefer the products of reliable and known brands. In this sense, the devices you will use must work with free software2. For this reason, a computer with a great GNU/Linux support and a cell phone that can run Lineageos3, a free Android distribution will serve you the best. Choose your USB hardware and storage devices in a similar manner and do not use or connect the unknown or found devices to your hardware. If you're serious about this issue, I recommend you check the devices of Purism4.

Use free software and keep them up to date

In every occasion possible, use free software on your devices and download them from trusted sources. This should start from the operating system and go on with all the software you use. There are plenty of software available for a modern business life that are substitutes for their proprietary versions. You can use Signal for communication5, Silence for SMS, LibreOffice for office software, Gimp for image editing, Kdenlive for video editing. Use alternativeto6 to find the free software alternatives of software. All GNU/Linux distributions come with their own software repositories and F-droid7 only contains free software for Android devices. Updating all of your software and operating system regularly will make you more difficult to take down.

Encrypt Everything!

Encryption is making the data in your devices' memory with the help of a key and cryptographic tool meaningless. Thanks to this, only those who have the key and the password can read the data. Not to be mistaken with screen unlock - since devices screen lock unlocks the device but for accessing files, password and key information needs to be known.

Although encryption is a deep subject, few fundamental distinctions can be made by means of its applications and the methods used. Basically, encryption systems divide into two as symmetric and asymmetric depending on the key. In symmetric encryption, the same key and password are used to encrypt and decrypt, whereas in asymmetric encryption is the method by which encryption and decryption operations are performed by different peers of a key pair. Encryption can also be divided by the area used. It is possible to encrypt communication, fully encrypt a record medium, encrypt a file system and specifically to encrypt a file. In this respect, every need requires its own technical preference. Serious Cryptography by Jean-Philippe Aumasson is recommended reading source.

Full disk encryption means encrypting a hard drive with all the information in it. This way, all information needs to be decrypted at each reboot. This prevents the acquisition of information from a stolen or captured computer. This method, which is considered the first line of defense for the data in a hardware, is naturally supported by Luks8 in Gnu / Linux distributions and can be provided with Veracrypt9 software for other operating systems. It is absolutely necessary that the password of each encrypted device is generated with Diceware and is different.

Despite full disk encryption, keeping your critical files encrypted will provide extra security. A second line of defense is an option to consider for your sensitive data, as full disk encryption will expose all the information

2 *https://www.gnu.org/philosophy/free-sw.html*

3 *https://lineageos.org/*

4 *https://puri.sm*

5 *https://www.signal.org/*

6 *https://alternativeto.net/*

7 *https://f-droid.org/*

8 *https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup*

9 *https://www.veracrypt.fr/en/Home.html*

on your drive when penetrated through. GPG software, which is also used in email encryption, can be recommended for this.

The most critical danger in encryption is that data recovery is almost impossible.

For this reason, you must memorize the passwords you use for encryption very well, secure your secret key for tools like GPG, and always make regular encrypted backups10 and keep them in a safe place.

Turn off GPS and Wireless Devices if not used

Location information can be obtained both by GPS - and other satellite-based positioning systems - and by the broadcast of your Wifi and Bluetooth devices. This information can pose great threats depending on the situation and allows you to be tracked with your device. Do not activate these tools especially in cases where you do not need the location information and, if possible, use only GPS for location.

Take precautions against purse-snatching

As an inexpensive method of bypassing the precautions taken for mobile devices, taking the device from the user while it is unlocked is a method actually used. It is recommended you use PlucklockEx found in F-droid against this attack11. This software locks the screen of your device in case of a sudden acceleration through gyroscope. This will prevent the attacker from accessing device functions of your phone if taken away from you while you're using it.

c. Network Security

Your connection to the internet starts from your device's network card. Wireless networks are now preferred for this purpose. The owner of the network can as well be the watcher of your whole communication, direct your device with malicious aims or expose your identity.

Do not connect to untrusted networks and use VPN

VPN (Virtual Private Network)12 is an encrypted communication line installed from your device to a remote server. This way, your communication cannot be controlled or modified by those who own the connection from the server to the infrastructure (or the whole network). Always use a reliable VPN service provider or set up your own VPN13. VPN does not make you anonymous enough, it just transfers the trust of the infrastructure to your VPN provider. For this reason, it should continuously used as a precaution.

Use TOR

TOR (The Onion Network) is used to hide your identity and location by relaying your devices connection in encrypted form through intermediaries run by volunteers from all around the world. When talking about anonymity, TOR is one of the inevitable tools in the world of journalists. The easiest way to use the TOR network is the TOR Browser14 for personal computers and mobile devices. You can use TOR all the time, but both the browser's actions can disrupt web pages, and blocks to TOR may make it difficult for you to access some sites. Therefore, when used in conjunction with VPN, it provides a multifaceted anonymity and security. However, you should maintain the discipline of your anonymity and when necessary, do not perform transactions that will reveal your identity through TOR.

Hide your MAC Address

The MAC address15 is a piece of information that clearly identifies your device's network hardware and allows you to be monitored just as a tracking device if associated with you. Now how to change the MAC address of your device and before connecting to an unknown network, randomly change this address with another address. Keeping your device's, especially mobile device's wireless and Bluetooth continuously turned on will broadcast your device's MAC address and infor-

[10] *https://www.olaganparanoya.com/194-2/*

[11] *https://www.olaganparanoya.com/telefonunuz-ile-ilgili-kolaylikla-alabileceginiz-14-onlem/*

[12] *https://en.wikipedia.org/wiki/Virtual_private_network*

[13] *https://www.kendibaglantim.com/*

[14] *https://www.torproject.org/*

[15] *https://en.wikipedia.org/wiki/MAC_address*

mation on previously connected networks continuously. So, turn off the wireless connection of your devices when you're not using them.

d. Account and Software Security

The software you use and the transactions you make through these software can make you recognisable. This covers a wide range of services, from the software you use to communicate to the browser you browse websites for.

Email

By its nature, email is an unsafe form of communication. Above all, stop using free email providers that track and market you. Instead, switch to an email service provider that will provide you with a reliable email service for a small fee per month. Posteo16 and Mailbox17 can be recommended as traditional email service providers, and Tutanota and Protonmail are remarkable service providers that come with built-in encryption capabilities.

If you are accessing your emails from a client you use on your computer, Thunderbird18, a free client. Take advantage of the security of free software and be ready to encrypt with GPG.

Encrypt your emails with GPG and get ready for encryption. GPG is an email and file encryption system that played a big role in the leaks of Edward Snowden. Such that; Glen Greenwald, a well-known journalist, was almost unheard of in the Snowden leak because he could not learn to use GPG. With GPG, you can encrypt your emails or sign them for proof that they come from you. With the Enigmail19 extension installed on Thunderbird, you can generate and manage a key and use it comfortably. You can have an integrated usage with email service providers that support GPG, such as Mailbox and Protonmail. GPG is a hard-to-use but highly effective tool. It is essential to get prepared and make it part of daily use before it is necessary. It is highly recommended to read Riseup's guide on the subject20.

Immediate chatting

Immediate chatting is one of the most important parts of daily communication. In this respect, it is in a position to expose the most critical information and people's social connections. The security of this chatting platforms is an inevitable element of overall operation integrity. In this respect, free, widespread and easily available Signal software, which has become the gold standard for journalists and everyone else around the world, can be recommended. Signal end-to-end encrypts the Signal provides end-to-end encryption of correspondence and provides voice and video conversation. As with any cryptographic tool, it is essential to verify the contact's encryption key. This way, it can be ensured that an attacker does not intervene and checks the communication.

Since Signal requires phone number when signing up, it is a software difficult to use anonymously. Here, old fellows XMPP21 and OTR22 cut in. It is necessary to state that these are two of the communication methods NSA could not get over in Snowden documents. Encrypted correspondence can easily be made by buying an anonymous account over the Calyx Institute23 and with Pidgin which uses OTR encryption. Since the OTR is based on trust, it also allows the person to verify the key via a common secret between two people. Riseup's guide can also be recommended24.

Although not frequently remembered nowadays, SMS

[16] *https://posteo.de/en*

[17] *https://mailbox.org/en/*

[18] *https://www.thunderbird.net/en-US/*

[19] *https://www.enigmail.net/index.php/en/*

[20] *https://riseup.net/en/security/message-security/openpgp*

[21] *https://en.wikipedia.org/wiki/Xmpp*

[22] *https://otr.cypherpunks.ca/*

[23] *https://www.calyxinstitute.org/projects/public_jabber_xmpp_server*

[24] *https://riseup.net/en/security/message-security/otr*

is a written means of communication that comes to mind every time there is a power cut. Because of its nature, SMS is not a secure communication system against attackers wholack a source problem. For this reason, Silence is one of the leading software that you can use instead of the default SMS software on your device, and that can provide end-to-end encrypted correspondence with other devices using Silence.

Web Surfing and Browser Security

Your web browsing allows for a detailed profile of yours to be created and even though you use tools that provide anonymity, may cause your identity to be revealed. In order to survive on the web, having the necessary common sense and following the right methods is an important step for one's numerical security.

Because of this, it is recommended that you use the free Firefox browser in your daily web uses. By making the necessary settings and adding add-ons, you can eliminate the information that your browser leaks and the dangers that affect your privacy and security. I recommend VikingVPN's 2019 guide for this25.

SSL (Secure Socket Layer)26, is the fundamental encryption method of the web. This technology, which is the reason why the green key appears in the address bar of browsers, is based on the trust of certificate providers. Opening pages that do not allow SSL connection or entering data on these pages can be a security risk, so it is a good idea to have an extension in your browser that will force an SSL connection, such as the HTTPS Everywhere extension.

Since opening pages that do not allow SSL connection or entering data on that pages,

You need to be aware of how you browse the web and the possible threats. First of all, learn to cope with cookies. Cookies are small files placed in your browser that are actually designed for the necessary functions you need to use web pages, but many advertising companies try to track and profile you using this system. For this reason, from the browser settings, block 3rd party cookies and with the CookieAutoDelete plugin, let your browser automatically clear cookies for each tab whenever you close it.

File Share

File sharing is critical, especially when the files are too large to be sent via email or instant correspondence software. In cases where parties do not use encryption, each corporation that serves a file share service has the right to read, change and detect those who have access to the incoming files. A related motto says "there are no clouds, only other people's computers".27 Just as you would not share your confidential sources and information with someone else, uploading them to someone's computer is also a problematic situation. It is generally considered necessary to use secure methods of file sharing.

For direct file sharing, OnionShare28 which uses the TOR Network might be the first choice. This way, without an intermediary, the file is directly transferred from one computer to another with the safety provided by the TOR network. Once you have uploaded the required files to OnionShare, you can share the TOR link it creates with the recipient. OnionShare will automatically close when the file is downloaded via the TOR browser.

In the case of "cloud" uses, where sharing only is not sufficient and storage is also needed, another method will be required. Since encryption makes it impossible for the other party to access the file, the ultimate single safe way is running your own server and requires you to have your device physically in hand. Nextcloud29 is a file sharing and collaboration software that you can run on your own server. This way, you can both create your own storage area and make encrypted storage with a tool like EncFS30 , and also share files with an open folder if needed. Nextcloud is an easy-to-install

[25] *https://vikingvpn.com/cybersecurity-wiki/browser-security/guide-hardening-mozilla-firefox-for-privacy-and-security*

[26] *https://en.wikipedia.org/wiki/SSL*

[27] *https://www.gnu.org/philosophy/who-does-that-server-really-serve.html*

[28] *https://onionshare.org/*

[29] *https://nextcloud.com/*

[30] *https://vgough.github.io/encfs/*

software that can easily run on older hardware or small devices such as a Raspberry Pi.

Account Management

The management of all online systems, including the social media accounts used, is also an important part of people's appearances on the Internet. The basic rule here is to protect the access requirements of the services used. In this respect, assigning random 16 and longer unique passwords to each service used from a password manager secured with a Diceware password prevents attackers from accessing the resulting data and other services if the service you are using cannot protect your information.

Some services like Facebook, Twitter etc. also serve means of communication with other people. When using these services, you should communicate through them as least as you can with minimal details and switch to another safe tool as soon as possible and delete the conversations. This will prevent your account from being compromised and your resource being disclosed.

Photograph and Exif31 Information

All photographs you take with a camera or mobile devices contain an attachment called Exif. Exif contains critical information like device information, location information and date. Uploading a photo containing such information on social media or sharing with someone may cause the transmit of information that identifies you greatly depending on the device you are using. In order to extract this information from the photos you are going to share, you can use Scrambled Exif32 for Android and Exiftool for GNU/Linux distributions.

2. Privacy Tools

a. Tails33

Tails is a GNU/Linux distribution. Unlike other distributions, only one purpose is intended; anonymity. In this respect, Tails is designed to work live and to forget any changes made. By writing Tails to a USB, or a better choice, an optical drive, you can run your device on these hardware. Tails has all the tools mentioned in this article (like TOR, XMPP, OTR). At every start asks you for the necessary settings you might need and after you close it, forgets everything. At the same time, the operating system and every software in it operates with the highest security and anti-monitoring measures. It is recommended that you do not change these settings and use Tails as it is.

You need to download and verify Tails from a trusted source and write it to a medium. In this respect, you can write a new Tails medium from the Tails installation of someone you trust. Therefore, the best way to start using Tails is to find someone you trust that uses Tails, and then keep track of Tails updates and support new users while maintaining that trust.

(i) Tails has been explained in detail in the 7th issue of Arka Kapi Magazine.

b. SecureDrop

SecureDrop34 is a file sharing system designed to allow secure access of documents and resources to journalists and institutions. With SecureDrop, it is possible for people to access the software running on a server a broadcast institution physically has via TOR. It is also possible for them to share documents anonymously and get in contact securely. Since the system is protected both with TOR and additional encryption precautions, it enables the safest transfer possible between two unacquainted people.

Since SecureDrop needs to be systematically operated and maintained, it is more likely that a press agency will operate and maintain this system. As every security system requires a continuous discipline of operation and has special conditions, it is recommended to proceed with the detailed documentation35 of SecureDrop..

c. Haven

[31] *https://en.wikipedia.org/wiki/Exif*

[32] *https://f-droid.org/en/packages/com.jarsilio.android.scrambledeggsif/*

[33] *https://tails.boum.org/*

[34] *https://securedrop.org/*

[35] *https://docs.securedrop.org/en/release-0.13.1/*

Haven, a free software developed by Guardian Project and Edward Snowden36, aims to protect physical environments with an unused or dedicated Android phone. What you need to do is to download Haven on a trusted device and after making the necessary settings, place it somewhere to watch there. Through the device's sensors like voice, light and camera, Haven notifies you via Signal or SMS when a change happens. Haven also opens a TOR server, allowing you to remotely access your recordings. In this way, it is possible to provide physical security in foreign places such as hotel rooms. Haven is still in beta stage but it needs to be mentioned that it is a beta that is well available. Haven also opens a TOR server, allowing you to remotely access your recordings. In this way, it is possible to provide physical security in foreign places such as hotel rooms. Haven is still in its beta stage but it needs to be mentioned that it is a strong beta worth using.

d. Reading list:

https://riseup.net/en/security

https://ssd.eff.org/

https://www.securityplanner.org/

https://network23.org/kame/

www.olaganparanoya.com

[36] *https://en.wikipedia.org/wiki/Edward_Snowden*

Güray Yıldırım & Aykut Yılmaz • guray@gurayyildirim.com.tr & ayktylmzse@gmail.com

Device Monitoring with OSQuery and AWS Logging

OSQuery is free software that allows us to obtain information through the operating system with SQL queries. You can access the OSQuery source code developed by Facebook via GitHub.

- Facebook says they developed OSQuery with passion.
- Having a free license makes it preferable for many people.
- It is possible to work with OSQuery regardless of the operating system of the server or personal computer - might be Windows, OS X, GNU/Linux and FreeBSD.

With OSQuery, you can send queries to the operating system just as sending queries to the database. In this way, open ports, plugged-in USBs, which computers should receive updates, user accounts information, and may more information can be gathered with SQL queries and schedule them to work periodically. We can also use YARA rules. (*YARA is a malware detection tool.*)

OSQuery has an installation package of about 20MB, you can install it in a short time by following the installation steps specified on their website. There are Choco packages for Windows operating systems and apt & rpm repositories for Linux systems.

Let's make an example for CentOS 7.

We pull repo information and add it on rpm.

```
$ curl -L https://pkg.OSQuery.io/rpm/GPG | sudo tee /etc/pki/rpm-gpg/RPM-
GPG-KEY-OSQuery
```

Then we add the OSQuery repo with yum-config-manager and then enable the rpm package.

```
$ sudo yum-config-manager --add-repo https://pkg.OSQuery.io/rpm/OSQuery-
s3-rpm.repo
$ sudo yum-config-manager --enable OSQuery-s3-rpm
```

In the last step, we start the OSQuery installation.

```
$ sudo yum install OSQuery
```

When creating the /etc/OSQuery/osquert.conf file and initializing the OSQuery daemon, we specify it as a config file.

In this configuration, we write the name of the hostname and queries that are designated as scheduled tasks. You can also send OSQuery's results of these scheduled queries to AWS Kinesis. To do this, you must use aws_kinesis, filesystem plug-ins, and specify aws information (aws_kinesis_stream,aws_access_key_id, aws_secret_access_key,aws_region) in the config file. The operations on Kinesis can be found in the following sections of the article.

```
{
 “options”: {
   “host_identifier”: “hostname01”,
   “schedule_splay_percent”: 10,
   “logger_plugin”: “aws_kinesis,filesystem”,
   “aws_kinesis_stream”: “**********************”,
   “aws_access_key_id”: “**********************”,
   “aws_secret_access_key”: “**********************”,
   “aws_region”: “**********************”
 },
 “schedule”: {
   “ssh_login”: {
     “query”: “SELECT * FROM last;”,
     “interval”: 2,
     “removed”: false
  },
  “time”: {
     “query”: “SELECT * FROM time;”,
     “interval”: 2,
     “removed”: false
   }
 }
}
```

To run the interactive shell mode, on the screen encountered, we just need to give the command osqueri and then get information about the system by typing various queries.

```
Using a virtual database. Need help, type ‘.help’

OSQuery>
```

1.) We can run the query “SELECT * FROM Uptime; “ to find out how long the system has been open.

```
Using a virtual database. Need help, type ‘.help’
OSQuery> SELECT * FROM Uptime;
```

```
+------+-------+---------+---------+--------------+

| days | hours | minutes | seconds | total_seconds |

+------+-------+---------+---------+--------------+

| 0    | 0     | 31      | 58      | 1918         |

+------+-------+---------+---------+--------------+
```

More examples can be given.

2.) To get the list of users on the system:

```
OSQuery> select uid, username, directory, shell from users;

+-------+------------------+---------------------+-------------------+

| uid   | username         | directory           | shell         |

+-------+------------------+---------------------+-------------------+

| 0     | root                    | /root              | /bin/bash        |

| 1     | daemon          | /usr/sbin          | /usr/sbin/nologin |

| 2     | bin                     | /bin               | /usr/sbin/nologin |

| 3     | sys                     | /dev               | /usr/sbin/nologin |

| 4     | sync                    | /bin               | /bin/sync        |

+-------+------------------+---------------------+-------------------+
```

3.) To list the packages installed on the operating system:

```
OSQuery> SELECT * FROM yum_sources;

+---------------------+-----------------------+---------+----------+------------------------------------------+

| name    | baseurl     | enabled | gpgcheck | gpgkey|

+---------------------+-----------------------+---------+----------+------------------------------------------+

| CentOS-$releasever - Base |  |  | 1 | file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7       |

| CentOS-$releasever - Updates | | | 1 | file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7    |

| CentOS-$releasever - Extras    | | | 1 | file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7   |

| CentOS-$releasever - Plus | | 0 | 1| file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7         |

+---------------------+-----------------------+---------+----------+------------------------------------------+
```

4.) To list the open ports:

```
OSQuery> select * from listening_ports;

+------+------+----------+--------+---------+

| pid  | port | protocol | family | address |

+------+------+----------+--------+---------+

| 2600 | 0    | 0        | 1      |         |

+------+------+----------+--------+---------+
```

5.) To get the hash information from users in the shadow file:

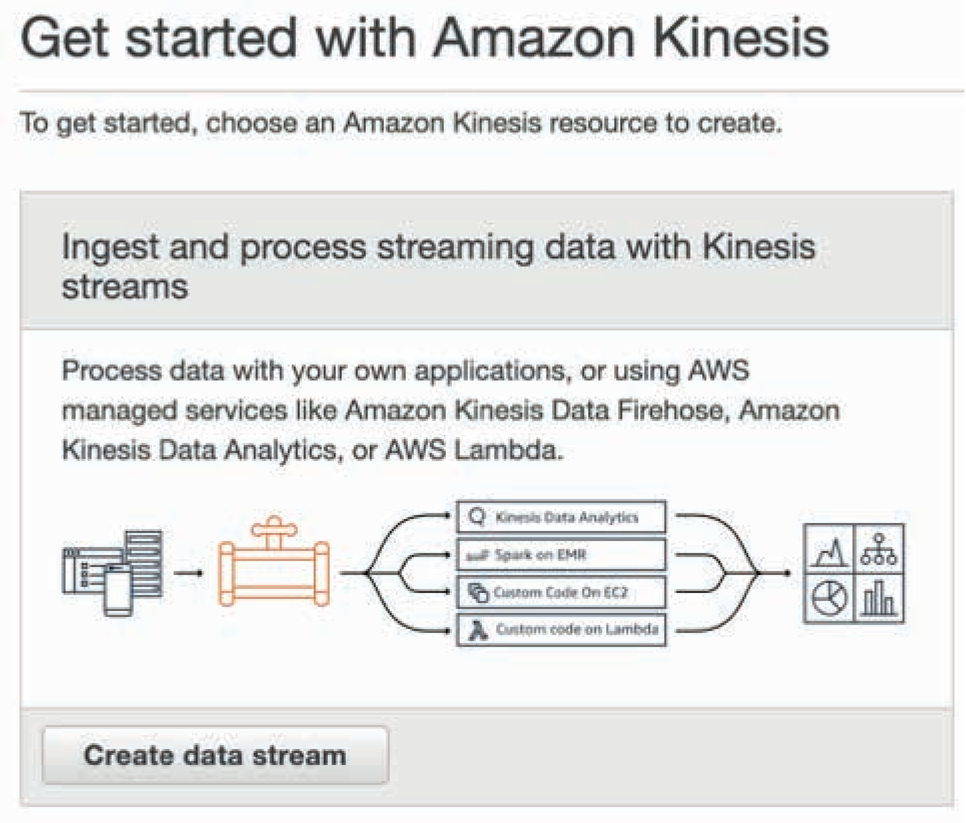
```
OSQuery> select * from hash where path = '/etc/shadow';

+-------------+-----------+--------------------+---------------------+----------------------------------------+

| path       | directory | md5                        | sha1                          | sha256                                                     |

+-------------+-----------+--------------------+---------------------+----------------------------------------+|    /
etc/shadow | /etc       | b6156e21a94627f1e010019438c73d82 | fa5ca2c15f080aa3c20b4bbb80961e0ef41fafb3 |
a4acb6e4f1f07b4e066e31b1f2e021b9184315d45b58950d6fd3bda231d8d833 |

+-------------+-----------+--------------------+---------------------+----------------------------------------+
```

6.) To list the USB devices:

```
OSQuery> select * from usb_devices;
```

Logging of records and query outputs to AWS

The services under Amazon Kinesis that can be used for receiving, querying, storing, and storing the flowing data can be used with OSQuery. For this step, the API access is defined by first creating an account via AWS IAM and selecting Programmatic Access at the account creation stage. In the authorization screen during account creation, user access information is saved after enabling Kinesis access under **Attach existing policies directly** option. **Kinesis** service opens on AWS. If it has not been used before, proceed with the **Get Started** button and click the **Create data stream** button:



Get started with Amazon Kinesis

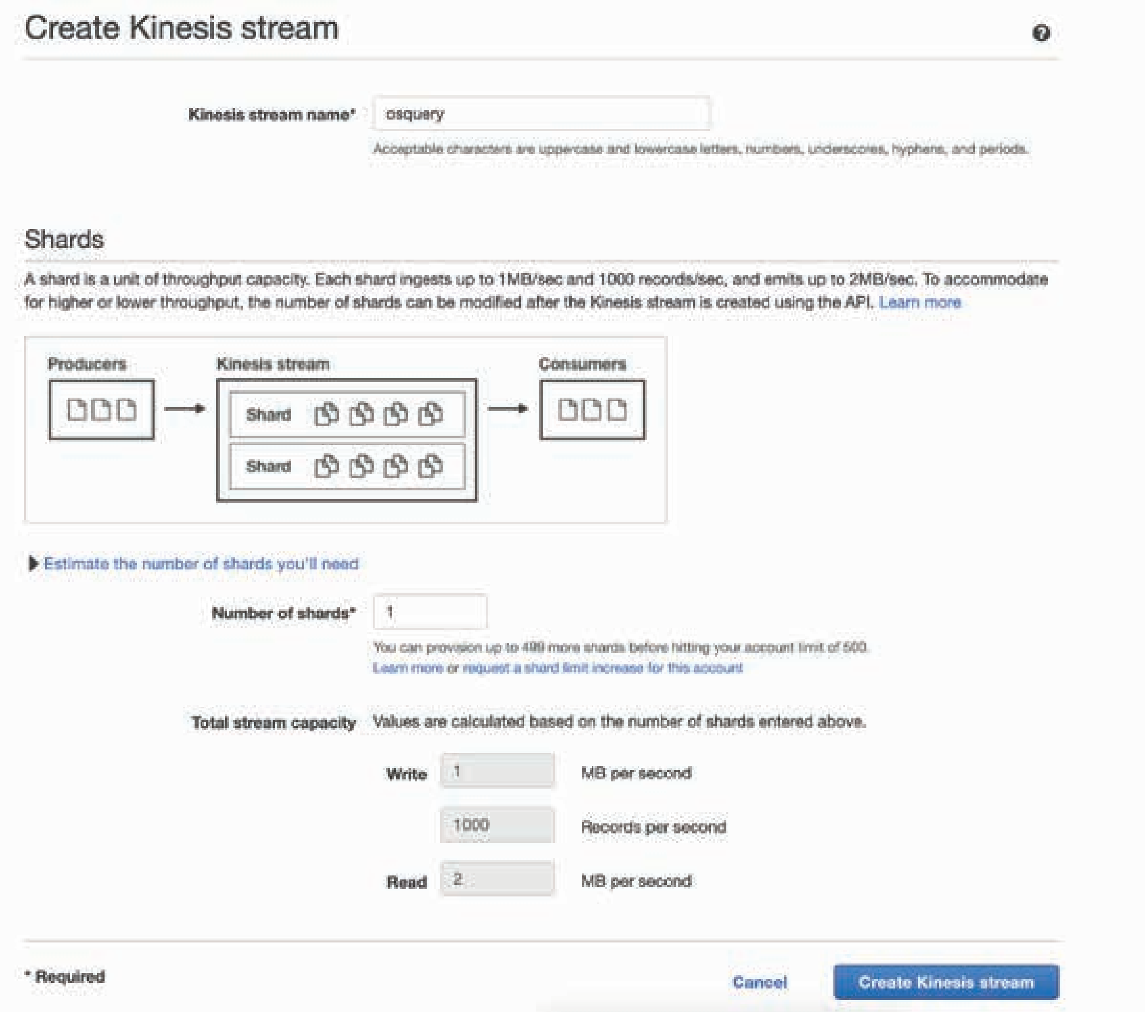
To get started, choose an Amazon Kinesis resource to create.

Ingest and process streaming data with Kinesis streams

Process data with your own applications, or using AWS managed services like Amazon Kinesis Data Firehose, Amazon Kinesis Data Analytics, or AWS Lambda.

A name is specified for the Kinesis stream on the display that opens. This example uses OSQuery. When selecting the Shard number, the choice can be made according to the amount of data that come.

When set to 1 like in the example, the information calculated by AWS about the total flow capacity appears. Considering factors such as infrastructure and output size of queries, the Shard number can be changed. Then, click the **Create Kinesis stream** button:



Create Kinesis stream

Kinesis stream name* osquery

Acceptable characters are uppercase and lowercase letters, numbers, underscores, hyphens, and periods.

Shards

A shard is a unit of throughput capacity. Each shard ingests up to 1MB/sec and 1000 records/sec, and emits up to 2MB/sec. To accommodate for higher or lower throughput, the number of shards can be modified after the Kinesis stream is created using the API. Learn more

▶ Estimate the number of shards you'll need

Number of shards* 1

You can provision up to 499 more shards before hitting your account limit of 500.
Learn more or request a shard limit increase for this account

Total stream capacity Values are calculated based on the number of shards entered above.

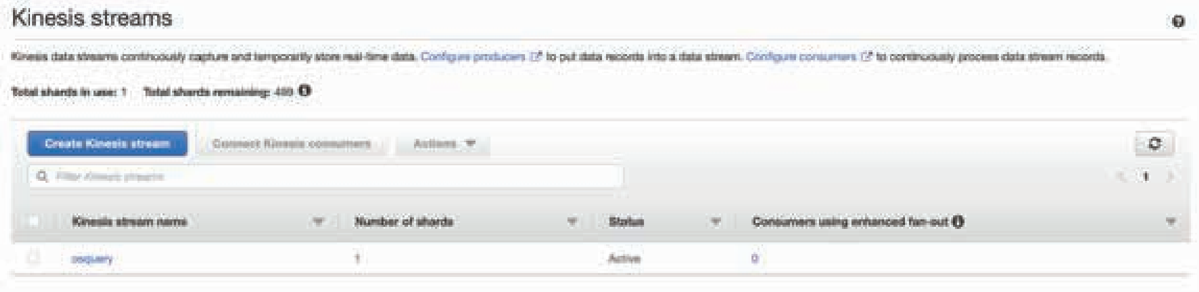
Write 1 MB per second

1000 Records per second

Read 2 MB per second

* Required

When the process is complete, the stream generated under the **Kinesis streams** can be displayed:



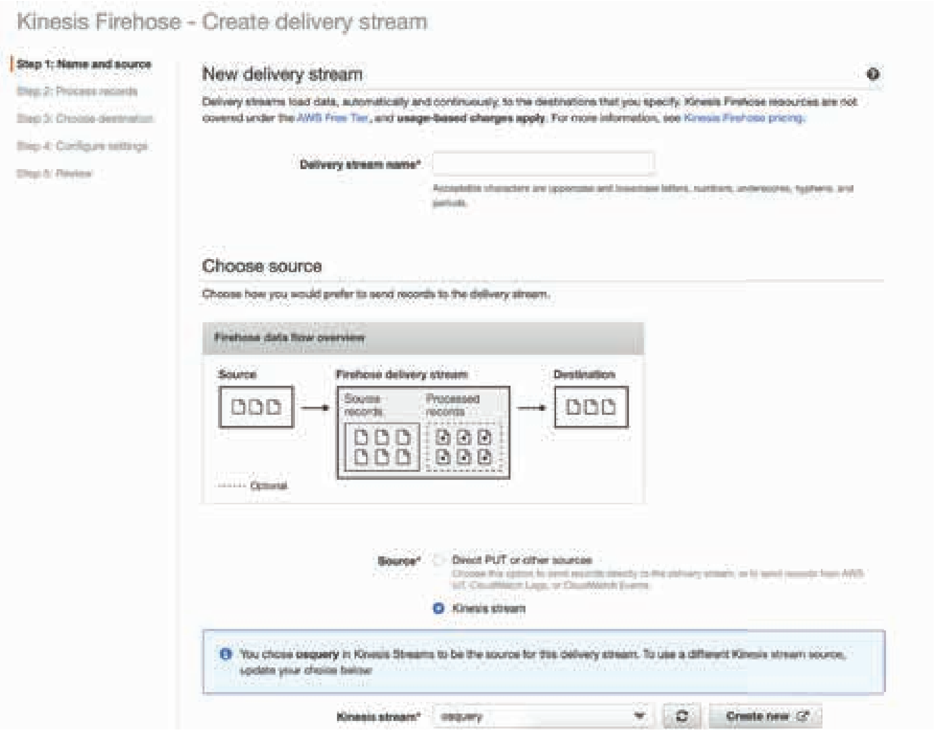
Kinesis streams

Kinesis data streams continuously capture and temporarily store real-time data. Configure producers to put data records into a data stream. Configure consumers to continuously process data stream records.

Total shards in use: 1 Total shards remaining: 499

□	Kinesis stream name	Number of shards	Status	Consumers using enhanced fan-out
□	osquery	1	Active	0

Next, a new **delivery stream** is created by selecting Kinesis Firehose so that the data can be retrieved and written over an S3 bucket. **OSQuery** can be used again for the name. In the Kinesis stream selection screen, the **OSQuery** flow created in the previous step is selected by proceeding:



Kinesis Firehose - Create delivery stream

Step 1: Name and source
Step 2: Process records
Step 3: Choose destination
Step 4: Configure settings
Step 5: Review

New delivery stream

Delivery streams load data, automatically and continuously, to the destinations that you specify. Kinesis Firehose resources are not covered under the AWS Free Tier, and **usage-based charges apply**. For more information, see Kinesis Firehose pricing.

Delivery stream name*

Acceptable characters are uppercase and lowercase letters, numbers, underscores, hyphens, and periods.

Choose source

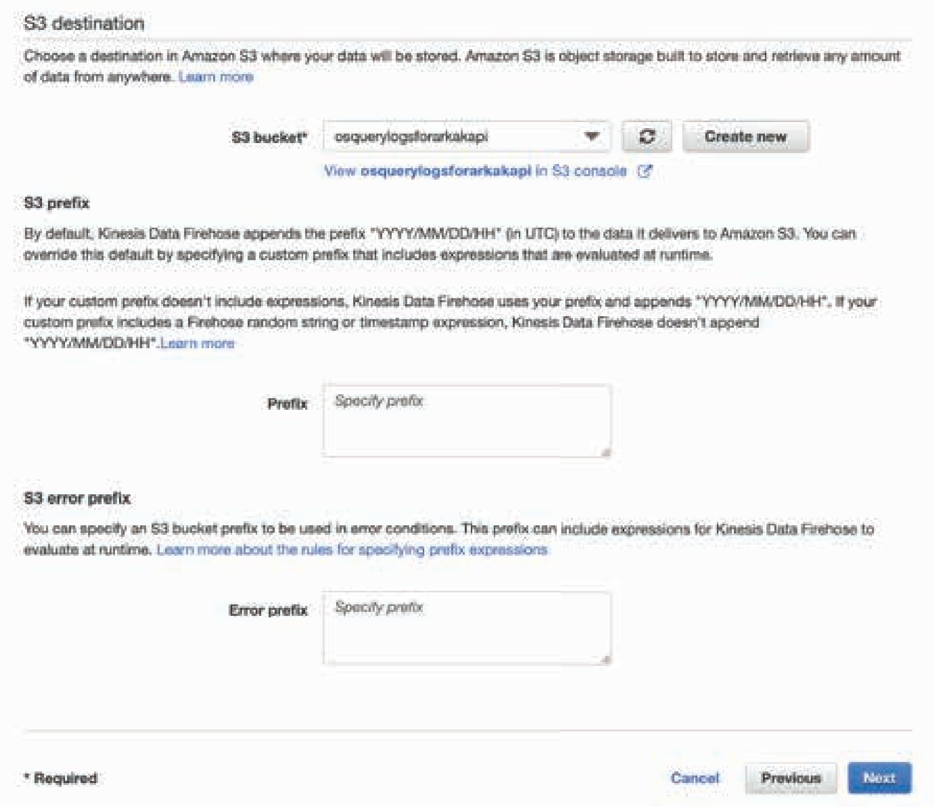
Choose how you would prefer to send records to the delivery stream.

Source* ○ Direct PUT or other sources
Choose this option to send records directly to the delivery stream, or to send records from AWS IoT, CloudWatch Logs, or CloudWatch Events.
● Kinesis stream

You chose **osquery** in Kinesis Streams to be the source for this delivery stream. To use a different Kinesis stream source, update your choice below.

Kinesis stream* osquery

Settings other than **Destination** and **IAM** are left by default. S3 is selected for Destination and a bucket is created using the **Create new** button on the **S3 bucket** selection screen. The given name must be unique:



S3 destination

Choose a destination in Amazon S3 where your data will be stored. Amazon S3 is object storage built to store and retrieve any amount of data from anywhere. Learn more

S3 bucket* osquerylogsforarkakapi

View **osquerylogsforarkakapi** in S3 console

S3 prefix

By default, Kinesis Data Firehose appends the prefix "YYYY/MM/DD/HH" (in UTC) to the data it delivers to Amazon S3. You can override this default by specifying a custom prefix that includes expressions that are evaluated at runtime.

If your custom prefix doesn't include expressions, Kinesis Data Firehose uses your prefix and appends "YYYY/MM/DD/HH". If your custom prefix includes a Firehose random string or timestamp expression, Kinesis Data Firehose doesn't append "YYYY/MM/DD/HH".Learn more

Prefix Specify prefix

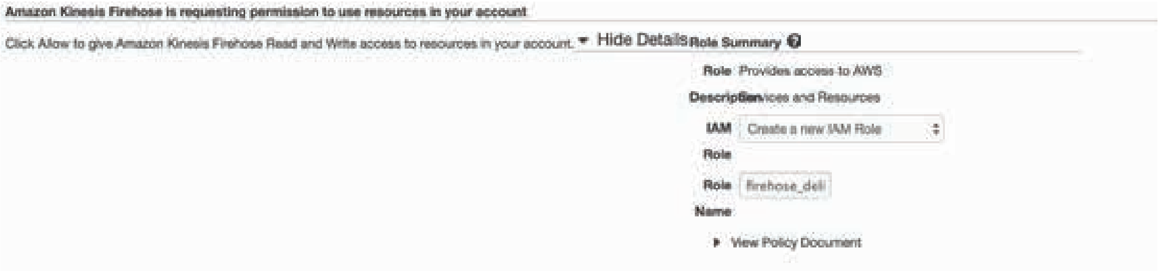
S3 error prefix

You can specify an S3 bucket prefix to be used in error conditions. This prefix can include expressions for Kinesis Data Firehose to evaluate at runtime. Learn more about the rules for specifying prefix expressions

Error prefix Specify prefix

* Required

While selecting IAM, a new role is created from the page that is opened by pressing the **Create new or choose button**. If a role has already been created for the same process, it can be modified.



Amazon Kinesis Firehose is requesting permission to use resources in your account

Click Allow to give Amazon Kinesis Firehose Read and Write access to resources in your account.

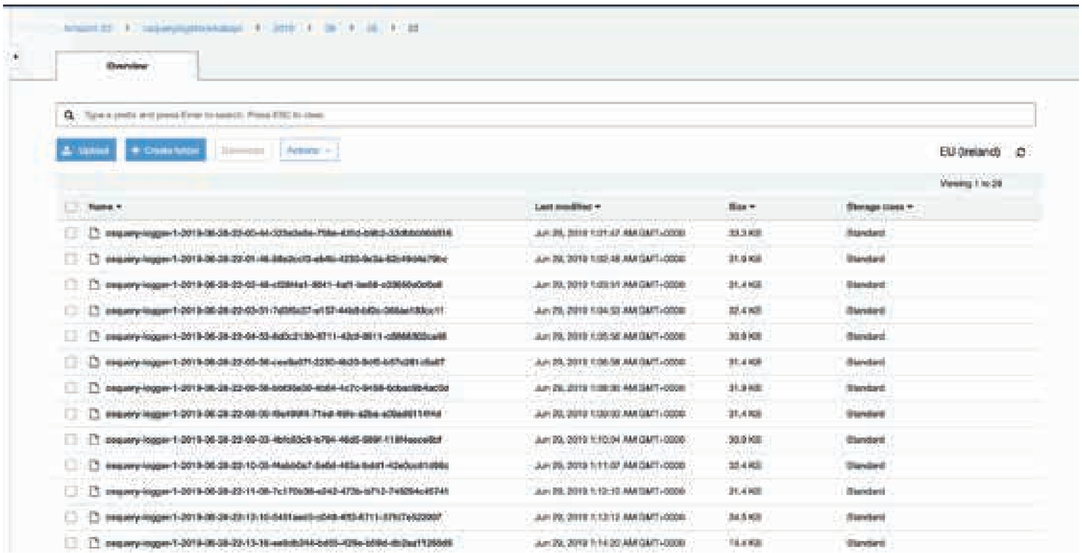
Role Summary

Role Description: Provides access to AWS Services and Resources

IAM Role: Create a new IAM Role

Role Name: firehose_deli

After waiting for a few minutes, the bucket created in the S3 service on AWS can be opened to view the incoming logs. Subdirectories in y/m/d format are created. Records can be displayed in directories:



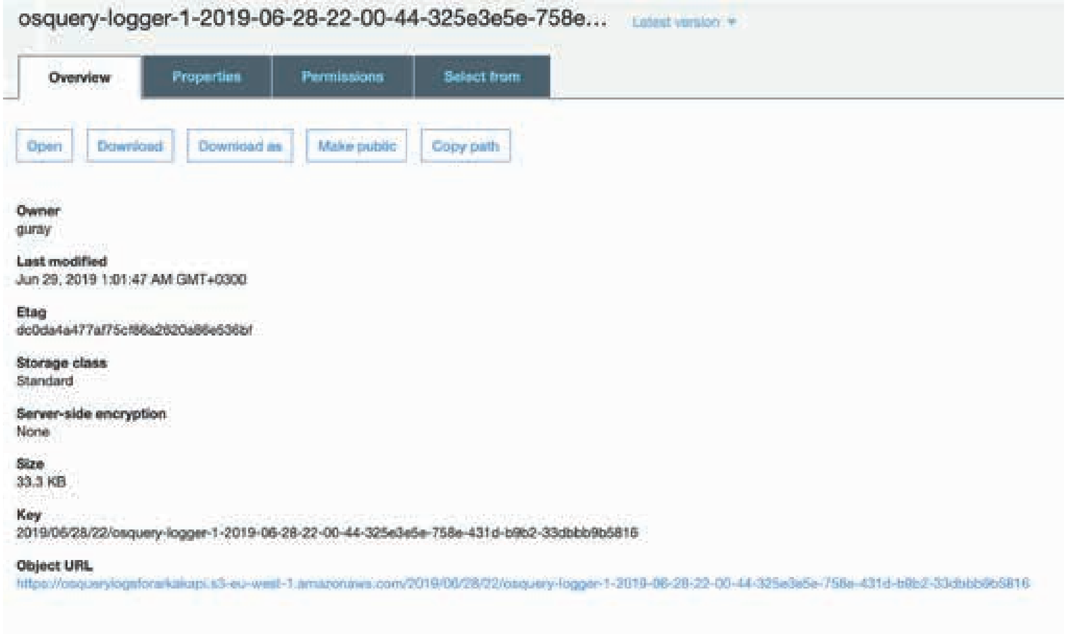
Amazon S3 › osquerylogsforarkakapi › 2019 › 06 › 28 › 22

Overview
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions
EU (Ireland)

Viewing 1 to 28

Name	Last modified	Size	Storage class
osquery-logger-1-2019-06-28-22-00-44-325e3e5e-758e-431d-b9b2-33dbbb9b5816	Jun 29, 2019 1:01:47 AM GMT+0300	33.3 KB	Standard
osquery-logger-1-2019-06-28-22-01-46-[illegible]	Jun 29, 2019 1:02:48 AM GMT+0300	31.9 KB	Standard
osquery-logger-1-2019-06-28-22-02-48-[illegible]	Jun 29, 2019 1:03:51 AM GMT+0300	31.4 KB	Standard
osquery-logger-1-2019-06-28-22-03-51-[illegible]	Jun 29, 2019 1:04:53 AM GMT+0300	32.4 KB	Standard
osquery-logger-1-2019-06-28-22-04-53-[illegible]	Jun 29, 2019 1:05:56 AM GMT+0300	30.9 KB	Standard
osquery-logger-1-2019-06-28-22-05-56-[illegible]	Jun 29, 2019 1:06:58 AM GMT+0300	31.4 KB	Standard
osquery-logger-1-2019-06-28-22-06-58-[illegible]	Jun 29, 2019 1:08:00 AM GMT+0300	31.9 KB	Standard
osquery-logger-1-2019-06-28-22-08-00-[illegible]	Jun 29, 2019 1:09:02 AM GMT+0300	31.4 KB	Standard
osquery-logger-1-2019-06-28-22-09-03-[illegible]	Jun 29, 2019 1:10:04 AM GMT+0300	30.9 KB	Standard
osquery-logger-1-2019-06-28-22-10-05-[illegible]	Jun 29, 2019 1:11:07 AM GMT+0300	32.4 KB	Standard
osquery-logger-1-2019-06-28-22-11-08-[illegible]	Jun 29, 2019 1:12:10 AM GMT+0300	31.4 KB	Standard
osquery-logger-1-2019-06-28-22-12-10-[illegible]	Jun 29, 2019 1:13:12 AM GMT+0300	34.5 KB	Standard
osquery-logger-1-2019-06-28-22-13-16-[illegible]	Jun 29, 2019 1:14:20 AM GMT+0300	14.4 KB	Standard

You can click on the desired record to download and view the details:



osquery-logger-1-2019-06-28-22-00-44-325e3e5e-758e...

Owner
guray

Last modified
Jun 29, 2019 1:01:47 AM GMT+0300

Etag
dc0da4a477af75cf86a2620a86e536bf

Storage class
Standard

Server-side encryption
None

Size
33.3 KB

Key
2019/06/28/22/osquery-logger-1-2019-06-28-22-00-44-325e3e5e-758e-431d-b9b2-33dbbb9b5816

Object URL
https://osquerylogsforarkakapi.s3-eu-west-1.amazonaws.com/2019/06/28/22/osquery-logger-1-2019-06-28-22-00-44-325e3e5e-758e-431d-b9b2-33dbbb9b5816

On AWS Kinesis, it is also possible to make live queries on incoming logs. With the **Data Analytics** in the Kinesis menu, which provides statistics, many possibilities can be obtained such as querying and anomaly detection on the flowing data.

Mert Sarıca • mert.sarica@gmail.com

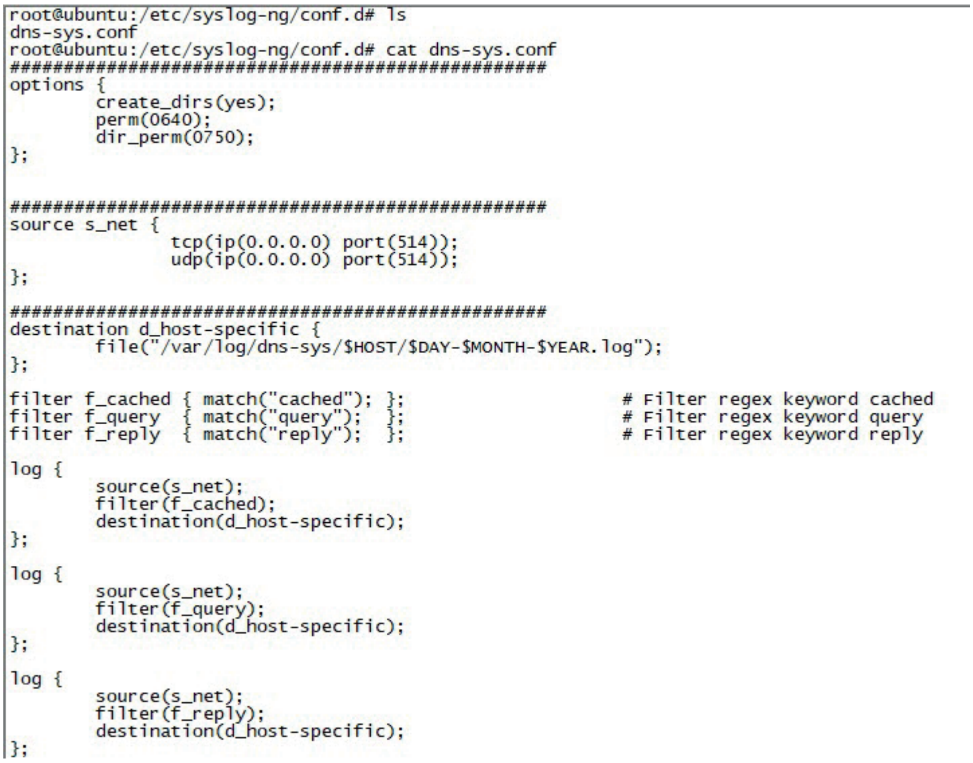
Homemade Cyber Threat Intelligence

Those of you who read my articles will remember that in the article titled “Escape from captivity”[1], I mentioned with great happiness the advantages of using a router whose security is provided by you and full of security features. As I mentioned in the article, I started using the dnscrypt-proxy tool to encrypt (DNS over HTTPS – DoH) DNS traffic.

In a world where the thermostats became smart, smart TVs equipped with cameras and water heaters and irons are used as spies; insecure objects connected to the home network (IoT) and infected software and devices that contain malware pose a great threat for our privacy. While I was thinking about how to detect systems on our home network that have been hacked, injected, and contain back doors, I remembered that I can also record DNS requests made by all systems, devices and devices connected to the home network thanks to the dnscrypt-proxy tool.

At the point where I could record DNS requests, I could make use of cyber threat intelligence services such as Open Threat Exchange (OTX), Critical Stack and detect malicious systems on my home network by asking these services for domain names and IP addresses in these DNS requests. Then, I immediately started to think about the list of needs to implement this idea.

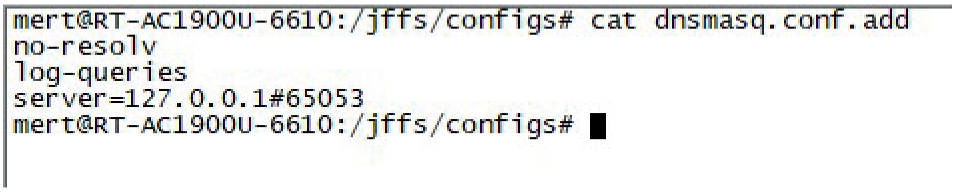
First, I decided to install the syslog-ng package on the Ubuntu operating system running on my Mini-PC, which is always helpful in such situations. After installing the package, I set the incoming DNS requests to be saved into the date.log file under the /var/log/dns-sys/sender-ip-address folder and save it to the /etc/syslog-ng/conf.d/dns-sys.conf file.



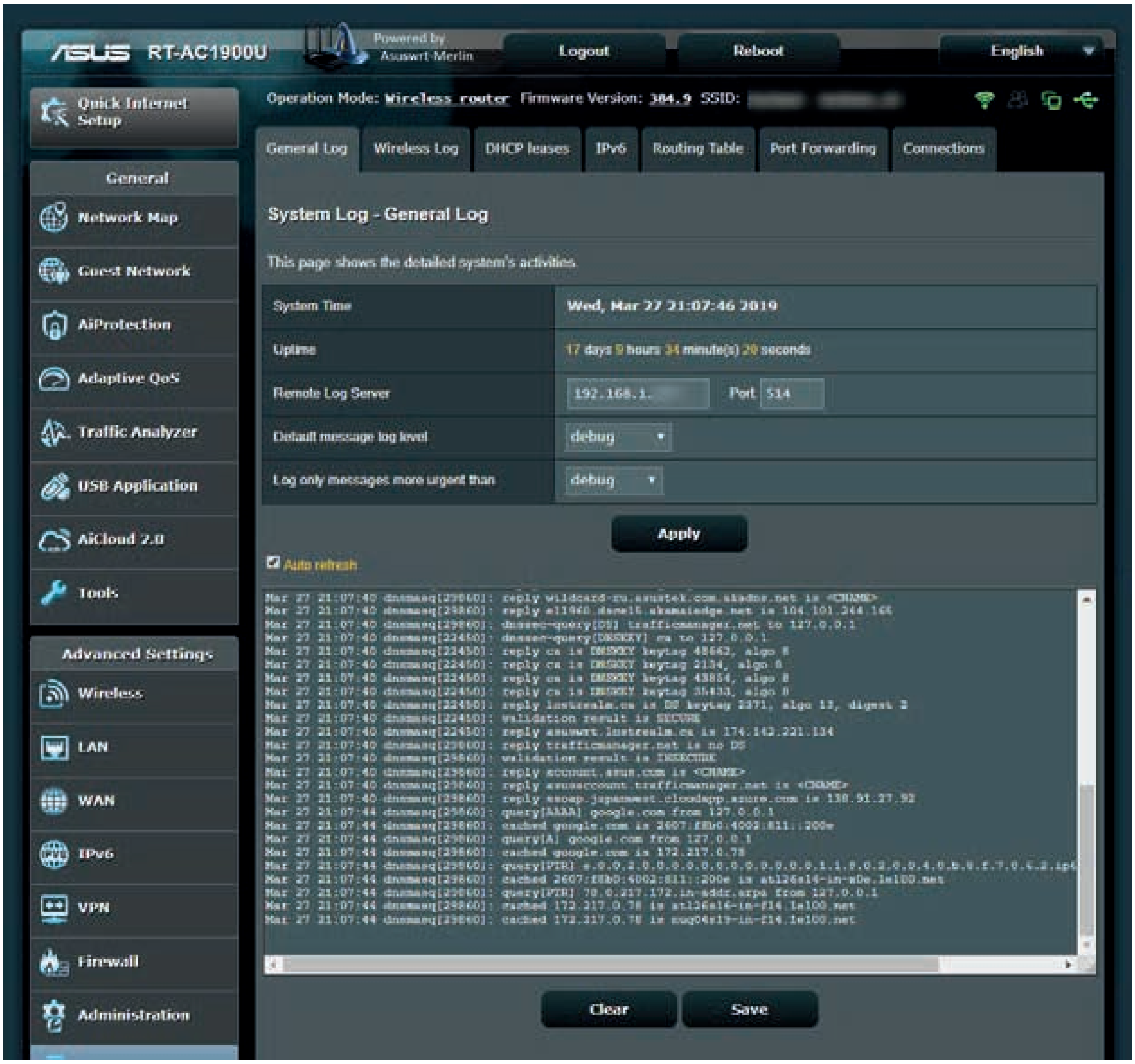
```
root@ubuntu:/etc/syslog-ng/conf.d# ls
dns-sys.conf
root@ubuntu:/etc/syslog-ng/conf.d# cat dns-sys.conf
##################################################
options {
        create_dirs(yes);
        perm(0640);
        dir_perm(0750);
};


##################################################
source s_net {
               tcp(ip(0.0.0.0) port(514));
               udp(ip(0.0.0.0) port(514));
};

##################################################
destination d_host-specific {
        file("/var/log/dns-sys/$HOST/$DAY-$MONTH-$YEAR.log");
};

filter f_cached { match("cached"); };                    # Filter regex keyword cached
filter f_query  { match("query");  };                    # Filter regex keyword query
filter f_reply  { match("reply");  };                    # Filter regex keyword reply

log {
        source(s_net);
        filter(f_cached);
        destination(d_host-specific);
};

log {
        source(s_net);
        filter(f_query);
        destination(d_host-specific);
};

log {
        source(s_net);
        filter(f_reply);
        destination(d_host-specific);
};
```

[1] https://www.mertsarica.com/esaretten-kacis/ will be translated to English in the upcoming issues.

In the next step, I added the log-queries line to the **/jffs/configs/dnsmasq.conf.add** file so that the **dnscrypt-proxy** tool can record DNS requests to the router's syslog. Then I set the **Default message log level** and **Log only messages more urgent than** values to **debug** to allow the router to display these requests on the syslog page. In order to redirect these messages to the syslog-ng application running on Ubuntu, I have defined the value of **Remote Log Server** as the IP address of Ubuntu.



```
mert@RT-AC1900U-6610:/jffs/configs# cat dnsmasq.conf.add
no-resolv
log-queries
server=127.0.0.1#65053
mert@RT-AC1900U-6610:/jffs/configs# █
```



Operation Mode: Wireless router Firmware Version: 384.9 SSID: [redacted]

System Log - General Log

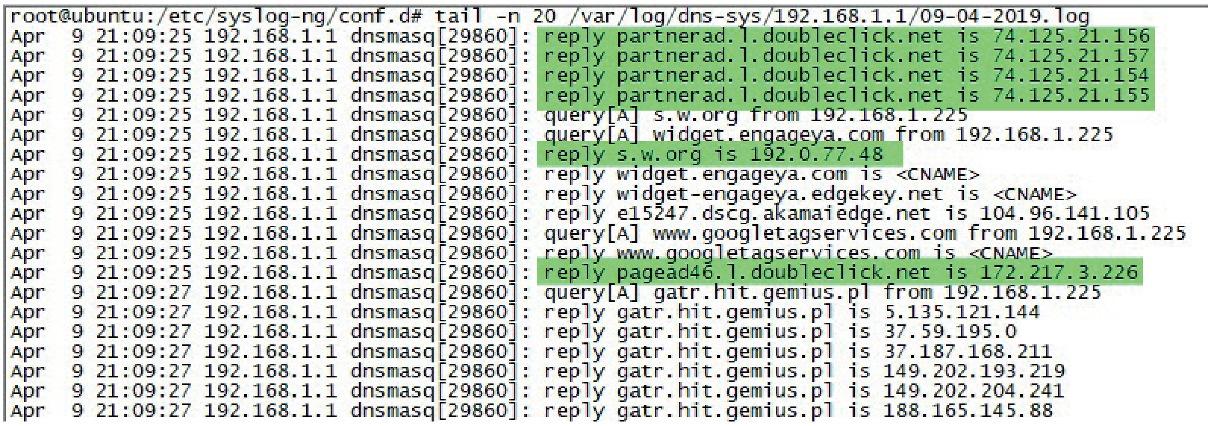
This page shows the detailed system's activities.

System Time	Wed, Mar 27 21:07:46 2019
Uptime	17 days 9 hours 34 minute(s) 20 seconds
Remote Log Server	192.168.1.[redacted] Port 514
Default message log level	debug
Log only messages more urgent than	debug

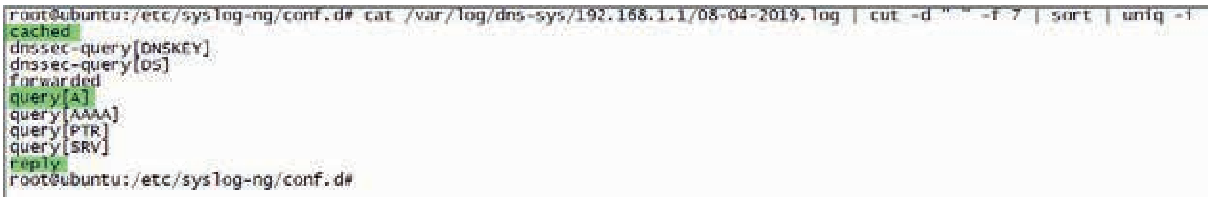
☑ Auto refresh

```
Mar 27 21:07:40 dnsmasq[29860]: reply wildcard-ru.asustek.com.akadns.net is <CNAME>
Mar 27 21:07:40 dnsmasq[29860]: reply e11960.dsne15.akamaiedge.net is 104.101.244.166
Mar 27 21:07:40 dnsmasq[29860]: dnssec-query[DS] trafficmanager.net to 127.0.0.1
Mar 27 21:07:40 dnsmasq[22450]: dnssec-query[DNSKEY] ca to 127.0.0.1
Mar 27 21:07:40 dnsmasq[22450]: reply ca is DNSKEY keytag 48662, algo 8
Mar 27 21:07:40 dnsmasq[22450]: reply ca is DNSKEY keytag 2134, algo 8
Mar 27 21:07:40 dnsmasq[22450]: reply ca is DNSKEY keytag 43854, algo 8
Mar 27 21:07:40 dnsmasq[22450]: reply ca is DNSKEY keytag 31433, algo 8
Mar 27 21:07:40 dnsmasq[22450]: reply lostrealm.ca is DS keytag 2371, algo 13, digest 2
Mar 27 21:07:40 dnsmasq[22450]: validation result is SECURE
Mar 27 21:07:40 dnsmasq[22450]: reply asuswrt.lostrealm.ca is 174.142.221.134
Mar 27 21:07:40 dnsmasq[29860]: reply trafficmanager.net is no DS
Mar 27 21:07:40 dnsmasq[29860]: validation result is INSECURE
Mar 27 21:07:40 dnsmasq[29860]: reply account.asus.com is <CNAME>
Mar 27 21:07:40 dnsmasq[29860]: reply asusaccount.trafficmanager.net is <CNAME>
Mar 27 21:07:40 dnsmasq[29860]: reply asoap.japaneast.cloudapp.azure.com is 138.91.27.92
Mar 27 21:07:44 dnsmasq[29860]: query[AAAA] google.com from 127.0.0.1
Mar 27 21:07:44 dnsmasq[29860]: cached google.com is 2607:f8b0:4002:811::200e
Mar 27 21:07:44 dnsmasq[29860]: query[A] google.com from 127.0.0.1
Mar 27 21:07:44 dnsmasq[29860]: cached google.com is 172.217.0.78
Mar 27 21:07:44 dnsmasq[29860]: query[PTR] e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.1.1.8.0.2.0.0.4.0.b.8.f.7.0.6.2.ip6
Mar 27 21:07:44 dnsmasq[29860]: cached 2607:f8b0:4002:811::200e is atl26s14-in-x0e.1e100.net
Mar 27 21:07:44 dnsmasq[29860]: query[PTR] 78.0.217.172.in-addr.arpa from 127.0.0.1
Mar 27 21:07:44 dnsmasq[29860]: cached 172.217.0.78 is atl26s14-in-f14.1e100.net
Mar 27 21:07:44 dnsmasq[29860]: cached 172.217.0.78 is mug04s19-in-f14.1e100.net
```

After, I started to examine the Syslog-ng records one by one and looked at what kind of records I should focus on in the name of threat intelligence. After I learned that I could use the **query[A], cached** and **reply** information found in the records, I thought that I could send these records to Security Onion, which can be integrated with OTX. After installing and running Security Onion's 16.04.5.6 operating system, I realised that the logstash service (so-logstash) was somehow not working. After many attempts, I couldn't be successful, so I started researching for alternative ways.



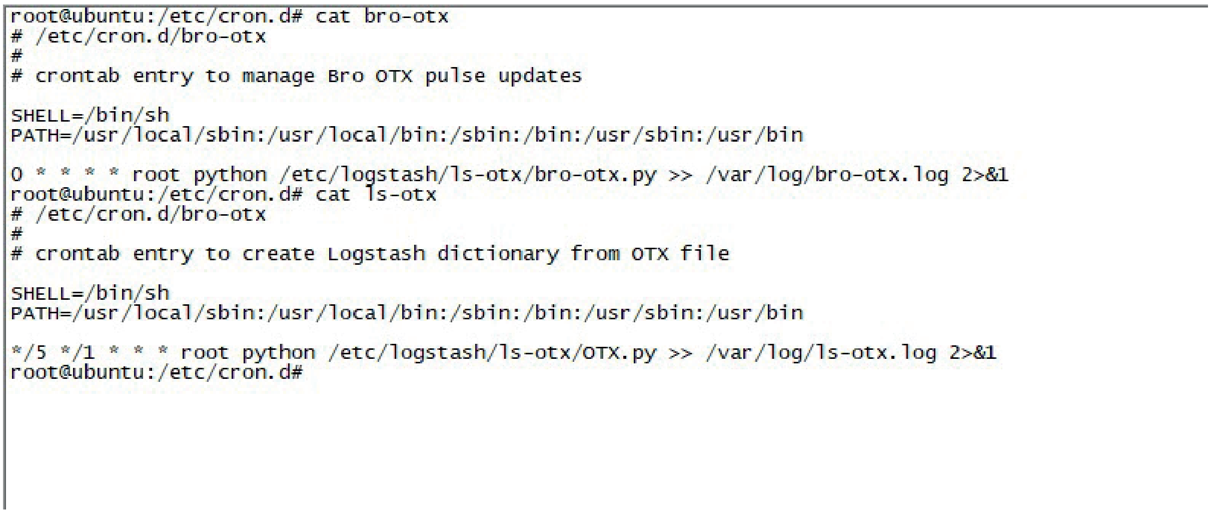
```
root@ubuntu:/etc/syslog-ng/conf.d# tail -n 20 /var/log/dns-sys/192.168.1.1/09-04-2019.log
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.156
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.157
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.154
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.155
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] s.w.org from 192.168.1.225
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] widget.engageya.com from 192.168.1.225
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply s.w.org is 192.0.77.48
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply widget.engageya.com is <CNAME>
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply widget-engageya.edgekey.net is <CNAME>
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply e15247.dscg.akamaiedge.net is 104.96.141.105
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] www.googletagservices.com from 192.168.1.225
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply www.googletagservices.com is <CNAME>
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply pagead46.l.doubleclick.net is 172.217.3.226
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: query[A] gatr.hit.gemius.pl from 192.168.1.225
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 5.135.121.144
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 37.59.195.0
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 37.187.168.211
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 149.202.193.219
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 149.202.204.241
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 188.165.145.88
```



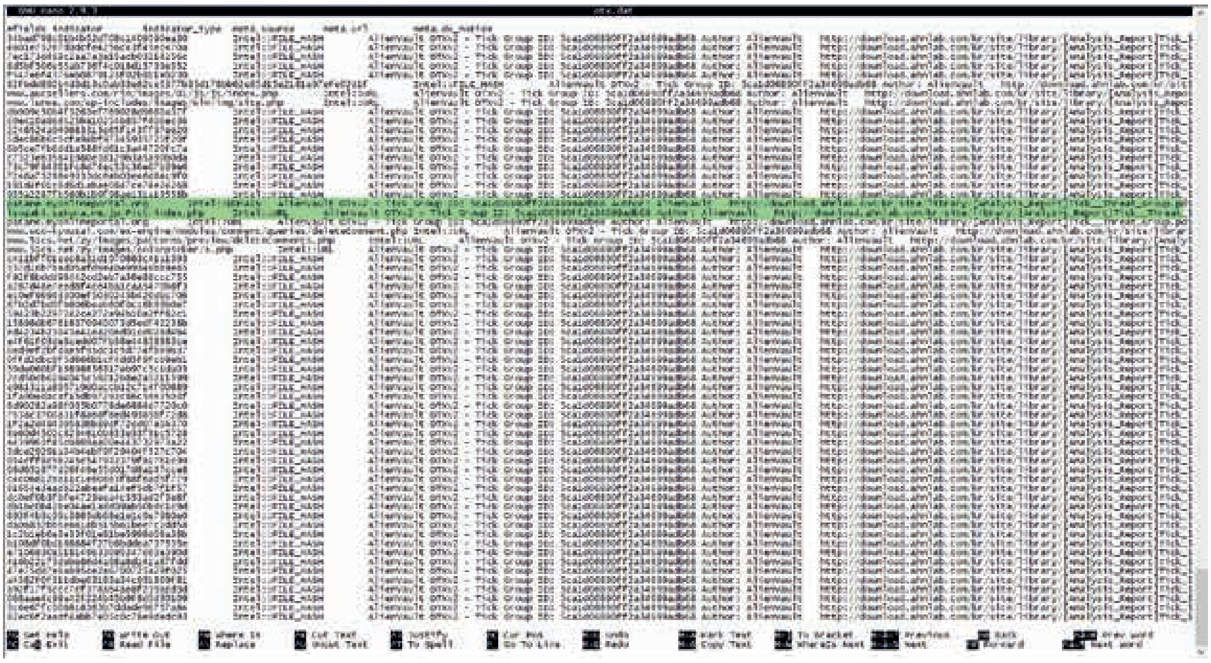
```
root@ubuntu:/etc/syslog-ng/conf.d# cat /var/log/dns-sys/192.168.1.1/08-04-2019.log | cut -d " " -f 7 | sort | uniq -i
cached
dnssec-query[DNSKEY]
dnssec-query[DS]
forwarded
query[A]
query[AAAA]
query[PTR]
query[SRV]
reply
root@ubuntu:/etc/syslog-ng/conf.d#
```

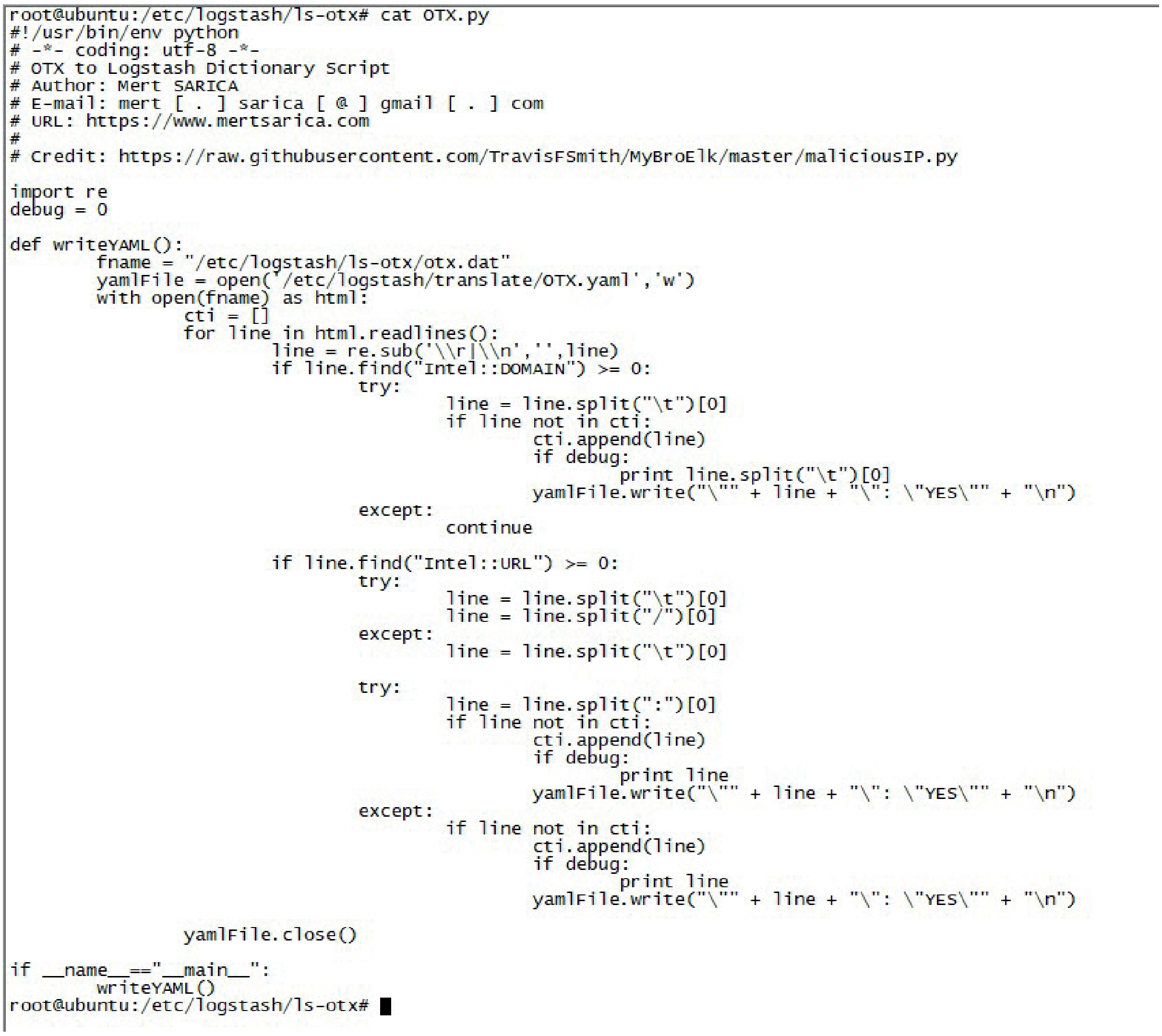
When I shared a message on Twitter that I needed to set up an ELK, I received messages saying that I could benefit from cloud and ready ELK systems. While I was thinking about whether I should install ELK on Ubuntu or use a cloud system, I found out that Logstash, which has **Grok filter** and **Translate filter** extensions, is the perfect fit for this job.

I started editing the securityonion-otx script file for Security Onion – OTX integration according to my own needs. I've set up file **bro-otx** to record threat intelligence information from OTX into file **/etc/logstash/ls-otx/otx.dat** at the start of every hour. In the fifth minute of every hour, I made sure that the **OTX.py** file was saved as the **/etc/logstash/translate/OTX.yaml** file to be read by the **Translate filter,** taking only the domain name information from the malicious URL and DOMAIN records in the **otx.dat** file.

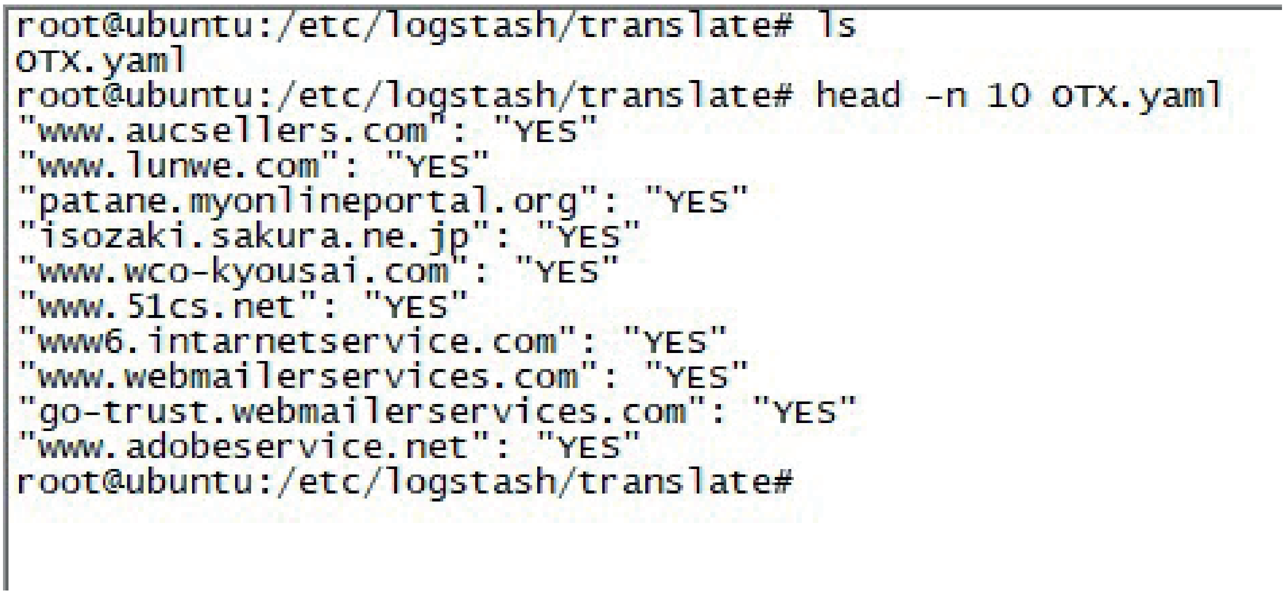


```
root@ubuntu:/etc/cron.d# cat bro-otx
# /etc/cron.d/bro-otx
#
# crontab entry to manage Bro OTX pulse updates

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

0 * * * * root python /etc/logstash/ls-otx/bro-otx.py >> /var/log/bro-otx.log 2>&1
root@ubuntu:/etc/cron.d# cat ls-otx
# /etc/cron.d/bro-otx
#
# crontab entry to create Logstash dictionary from OTX file

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

*/5 */1 * * * root python /etc/logstash/ls-otx/OTX.py >> /var/log/ls-otx.log 2>&1
root@ubuntu:/etc/cron.d#
```



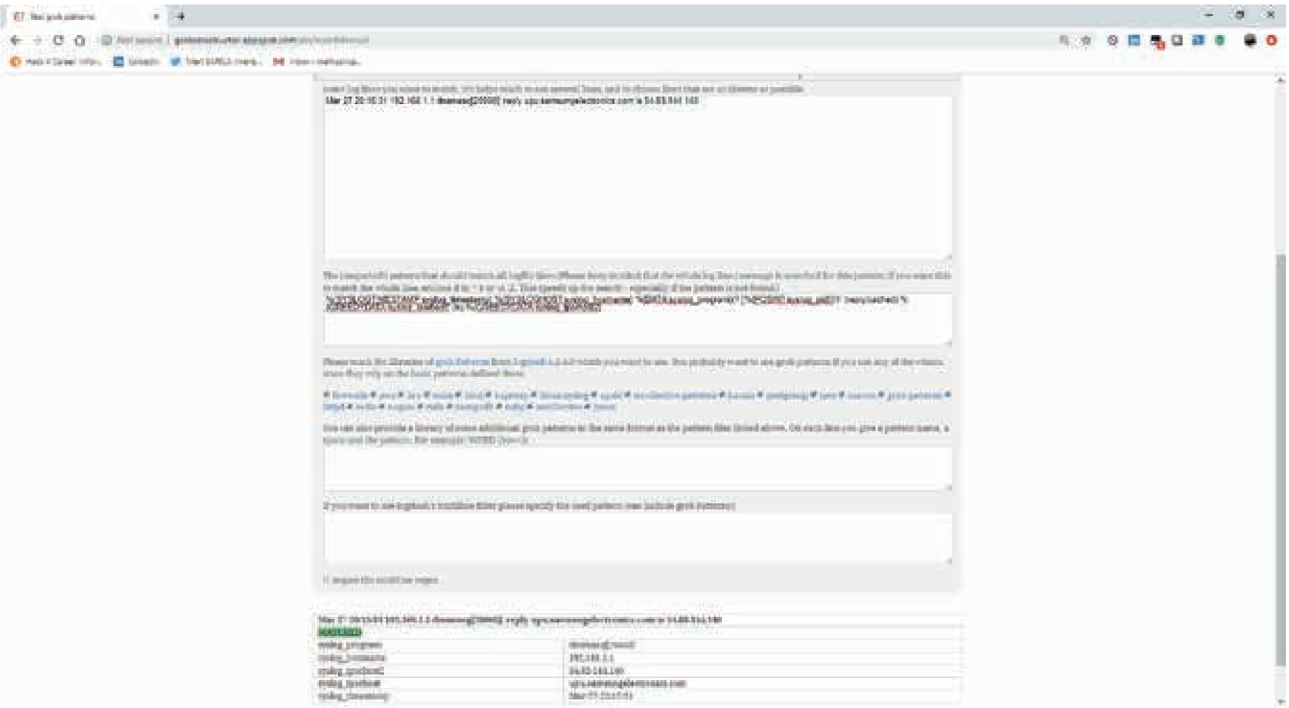


```
root@ubuntu:/etc/logstash/ls-otx# cat OTX.py
#!/usr/bin/env python
# -*- coding: utf-8 -*-
# OTX to Logstash Dictionary Script
# Author: Mert SARICA
# E-mail: mert [ . ] sarica [ @ ] gmail [ . ] com
# URL: https://www.mertsarica.com
#
# Credit: https://raw.githubusercontent.com/TravisFSmith/MyBroElk/master/maliciousIP.py

import re
debug = 0

def writeYAML():
        fname = "/etc/logstash/ls-otx/otx.dat"
        yamlFile = open('/etc/logstash/translate/OTX.yaml','w')
        with open(fname) as html:
                cti = []
                for line in html.readlines():
                        line = re.sub('\\r|\\n','',line)
                        if line.find("Intel::DOMAIN") >= 0:
                                try:
                                        line = line.split("\t")[0]
                                        if line not in cti:
                                                cti.append(line)
                                                if debug:
                                                        print line.split("\t")[0]
                                                yamlFile.write("\"" + line + "\": \"YES\"" + "\n")
                                except:
                                        continue

                        if line.find("Intel::URL") >= 0:
                                try:
                                        line = line.split("\t")[0]
                                        line = line.split("/")[0]
                                except:
                                        line = line.split("\t")[0]

                                try:
                                        line = line.split(":")[0]
                                        if line not in cti:
                                                cti.append(line)
                                                if debug:
                                                        print line
                                                yamlFile.write("\"" + line + "\": \"YES\"" + "\n")
                                except:
                                        if line not in cti:
                                                cti.append(line)
                                                if debug:
                                                        print line
                                                yamlFile.write("\"" + line + "\": \"YES\"" + "\n")

                yamlFile.close()

if __name__=="__main__":
        writeYAML()
root@ubuntu:/etc/logstash/ls-otx# 
```

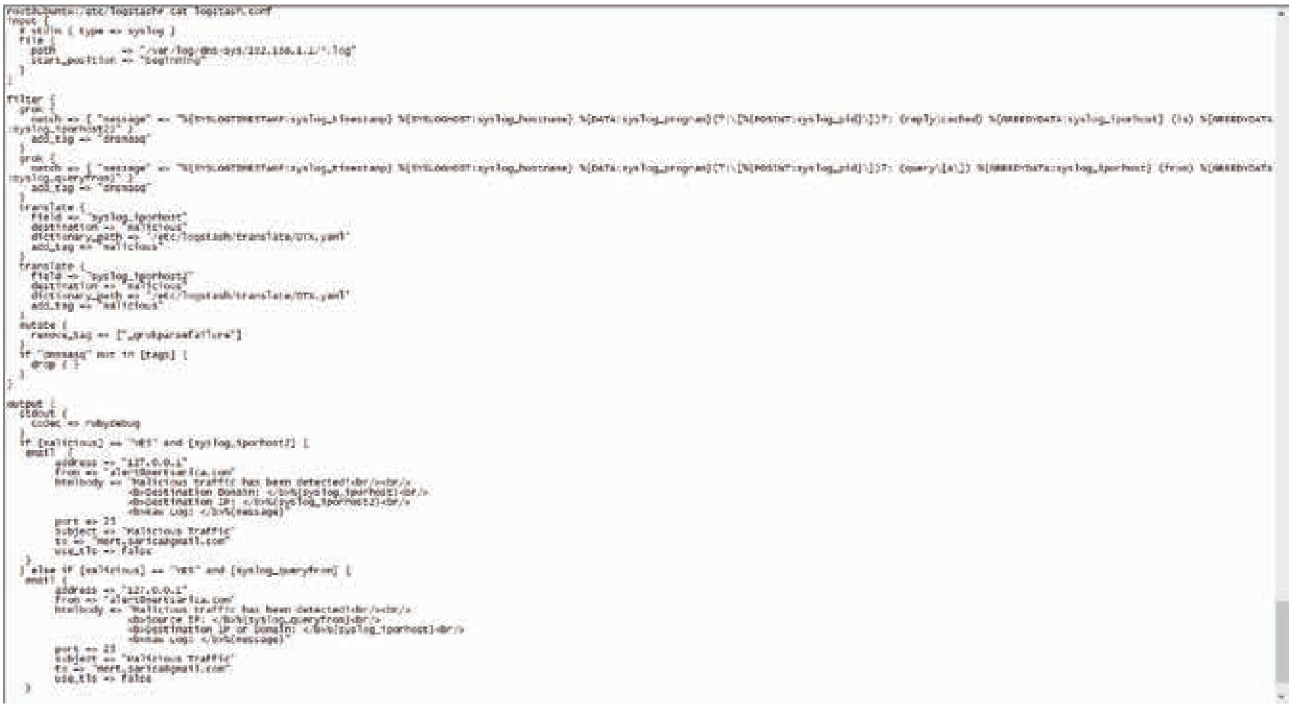


```
root@ubuntu:/etc/logstash/translate# ls
OTX.yaml
root@ubuntu:/etc/logstash/translate# head -n 10 OTX.yaml
"www.aucsellers.com": "YES"
"www.lunwe.com": "YES"
"patane.myonlineportal.org": "YES"
"isozaki.sakura.ne.jp": "YES"
"www.wco-kyousai.com": "YES"
"www.51cs.net": "YES"
"www6.intarnetservice.com": "YES"
"www.webmailerservices.com": "YES"
"go-trust.webmailerservices.com": "YES"
"www.adobeservice.net": "YES"
root@ubuntu:/etc/logstash/translate#
```

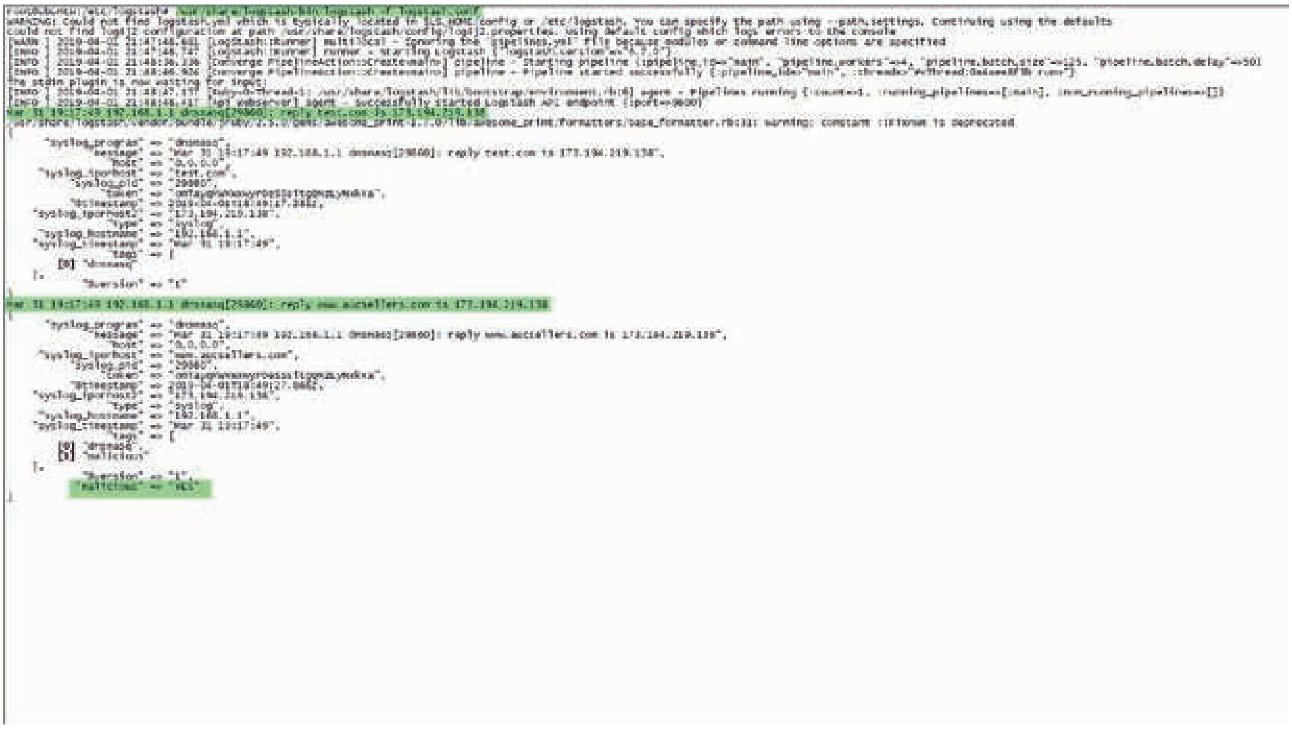
I made the declarations to read the DNS records registered with syslog-ng on Logstash's configuration file(logstash.conf) with Grok filter and send an alarm via e-mail if any of the IP addresses or domain names listed here with Translate filter are in the OTX.yaml file. Then, when I started Logstash again and queried **nslookup** to the **www[.]aucsellers[.]com** address in the **OTX.yaml** file, an alarm got succesffully generated and e-mailed to me. In short, I have successfully implemented the Home type threat intelligence service.



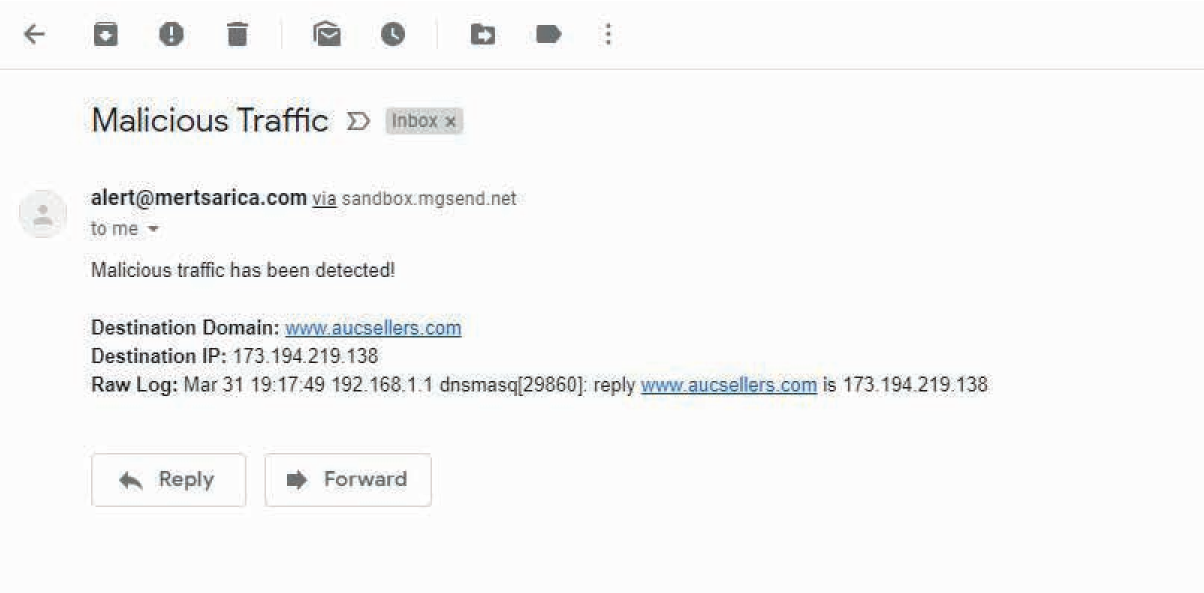
```
Mar 27 20:10:31 192.168.1.1 dnsmasq[20000]: reply [illegible] is 54.83.144.140
```



```
root@ubuntu:/etc/logstash# cat logstash.conf
input {
  # stdin { type => syslog }
  file {
    path           => "/var/log/dns-sys/192.168.1.1/*.log"
    start_position => "beginning"
  }
}

filter {
  grok {
    match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?: (reply|cached) %{GREEDYDATA:syslog_iporhost} (is) %{GREEDYDATA
:syslog_iporhost2}" }
    add_tag => "dnsmasq"
  }
  grok {
    match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?: (query\[A\]) %{GREEDYDATA:syslog_iporhost} (from) %{GREEDYDATA
:syslog_queryfrom}" }
    add_tag => "dnsmasq"
  }
  translate {
    field => "syslog_iporhost"
    destination => "malicious"
    dictionary_path => "/etc/logstash/translate/OTX.yaml"
    add_tag => "malicious"
  }
  translate {
    field => "syslog_iporhost2"
    destination => "malicious"
    dictionary_path => "/etc/logstash/translate/OTX.yaml"
    add_tag => "malicious"
  }
  mutate {
    remove_tag => ["_grokparsefailure"]
  }
  if "dnsmasq" not in [tags] {
    drop { }
  }
}

output {
  stdout {
    codec => rubydebug
  }
  if [malicious] == "YES" and [syslog_iporhost2] {
   email {
        address => "127.0.0.1"
        from => "alert@mertsarica.com"
        htmlbody => "Malicious traffic has been detected!<br/><br/>
                     <b>Destination Domain: </b>%{syslog_iporhost}<br/>
                     <b>Destination IP: </b>%{syslog_iporhost2}<br/>
                     <b>Raw Log: </b>%{message}"
        port => 25
        subject => "Malicious Traffic"
        to => "mert.sarica@gmail.com"
        use_tls => false
   }
  } else if [malicious] == "YES" and [syslog_queryfrom] {
   email {
        address => "127.0.0.1"
        from => "alert@mertsarica.com"
        htmlbody => "Malicious traffic has been detected!<br/><br/>
                     <b>Source IP: </b>%{syslog_queryfrom}<br/>
                     <b>Destination IP or Domain: </b>%{syslog_iporhost}<br/>
                     <b>Raw Log: </b>%{message}"
        port => 25
        subject => "Malicious Traffic"
        to => "mert.sarica@gmail.com"
        use_tls => false
   }
```



```
root@ubuntu:/etc/logstash# /usr/share/logstash/bin/logstash -f logstash.conf
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Continuing using the defaults
Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2.properties. Using default config which logs errors to the console
[WARN ] 2019-04-01 21:47:48,601 [LogStash::Runner] multilocal - Ignoring the 'pipelines.yml' file because modules or command line options are specified
[INFO ] 2019-04-01 21:47:48,717 [LogStash::Runner] runner - Starting Logstash {"logstash.version"=>"6.7.0"}
[INFO ] 2019-04-01 21:48:38,336 [Converge PipelineAction::Create<main>] pipeline - Starting pipeline {:pipeline_id=>"main", "pipeline.workers"=>4, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50}
[INFO ] 2019-04-01 21:48:46,936 [Converge PipelineAction::Create<main>] pipeline - Pipeline started successfully {:pipeline_id=>"main", :thread=>"#<Thread:0x[illegible] run>"}
The stdin plugin is now waiting for input:
[INFO ] 2019-04-01 21:48:47,177 [Ruby-0-Thread-1: /usr/share/logstash/lib/bootstrap/environment.rb:6] agent - Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
[INFO ] 2019-04-01 21:48:48,417 [Api Webserver] agent - Successfully started Logstash API endpoint {:port=>9600}
Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply test.com is 173.194.219.138
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/awesome_print-1.7.0/lib/awesome_print/formatters/base_formatter.rb:31: warning: constant ::Fixnum is deprecated
{
      "syslog_program" => "dnsmasq",
             "message" => "Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply test.com is 173.194.219.138",
                "host" => "0.0.0.0",
     "syslog_iporhost" => "test.com",
          "syslog_pid" => "29860",
               "token" => "[illegible]",
          "@timestamp" => 2019-04-01T18:49:27.286Z,
    "syslog_iporhost2" => "173.194.219.138",
                "type" => "syslog",
     "syslog_hostname" => "192.168.1.1",
    "syslog_timestamp" => "Mar 31 19:17:49",
                "tags" => [
        [0] "dnsmasq"
    ],
            "@version" => "1"
}
Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply www.aucsellers.com is 173.194.219.138
{
      "syslog_program" => "dnsmasq",
             "message" => "Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply www.aucsellers.com is 173.194.219.138",
                "host" => "0.0.0.0",
     "syslog_iporhost" => "www.aucsellers.com",
          "syslog_pid" => "29860",
               "token" => "[illegible]",
          "@timestamp" => 2019-04-01T18:49:27.286Z,
    "syslog_iporhost2" => "173.194.219.138",
                "type" => "syslog",
     "syslog_hostname" => "192.168.1.1",
    "syslog_timestamp" => "Mar 31 19:17:49",
                "tags" => [
        [0] "dnsmasq",
        [1] "malicious"
    ],
            "@version" => "1",
           "malicious" => "YES"
}
```



alert@mertsarica.com via sandbox.mgsend.net
to me

Malicious traffic has been detected!

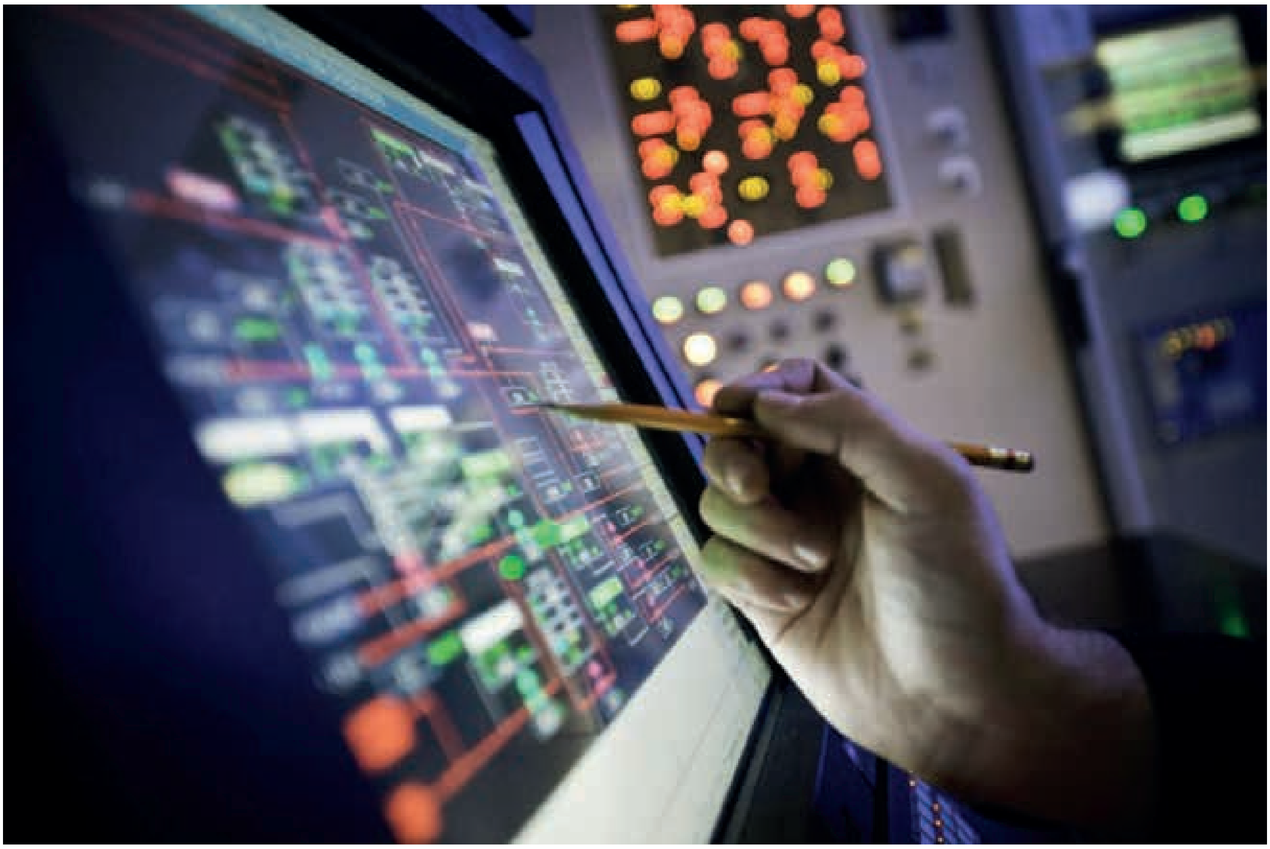
Destination Domain: www.aucsellers.com
Destination IP: 173.194.219.138
Raw Log: Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply www.aucsellers.com is 173.194.219.138

Have a secure day everyone! :)

Erhan Yakut • yakuter@gmail.com

Cyber Security in Critical Infrastructures

For a long time, technologies independent from the outer world, managed by people based on special protocols and software were in use on industrial systems. With the lack of networks to conduct attacks by hackers, the aforementioned systems didn't experience cyber attack incidents. Besides, the only way to penetrate through these systems was through entering facilities with physical security measures (electrical and barbed wires, guards, locked doors and even guard dogs) and accessing hand terminals directly. IT (Information Technology) and OT (Operation Technology) were rarely integrated and because of that, had totally different and independent vulnerabilities.



Nowadays, industrial systems, which are seen to be able to achieve new capabilities and efficiencies through technological integrations, are quickly being brought online. To put it simply, analytical evaluation of large data obtained from the plants showed that efficiency increases considerably. Additionally, remote monitoring and control of sensors have led to the conclusion that systems can be better managed.

This transition from closed to open systems has created a number of new security risks and vulnerabilities that need to be addressed.

What are the Critical Infrastructures?

Before going deeply into the above-mentioned vulnerabilities, the concept of critical infrastructures should be further explained.

The term "Critical Infrastructure" was first used in the "United States Presidential Commission"'s report on the Protection of Critical Infrastructure" dating October 1997. The term means interconnected systems and infrastructures that enable these systems to work in the desired course in order to operate the society and state order in a healthy way.

In our country (Turkey), the "**Cyber Security Council**" was established in 2012 to ensure national cybersecurity and the "**National Cyber Security Strategy and 2013-2014 Action Plan**" was accepted at the first meeting of this committee. In Article 5 of the action plan, the critical infrastructures of Turkey have been determined by the Cyber Security Council in the first place as follows:

1. Electronic Communications,
2. Energy,
3. Banking and Finance,
4. Critical Public Services,
5. Transport
6. Water Management

Some of the critical infrastructures listed use general and known information technologies, while others are monitored or managed by special information systems called Industrial Control Systems (ICS). Industrial Control Systems are divided into SCADA and DCS, according to the topology and the components they contain.

What is SCADA and DCS?

The word SCADA is an abbreviation of "Supervisory Control and Data Acquisition". SCADA, which is a comprehensive and integrated database control and monitoring system, can control, monitor and report the results of all equipment belonging to a facility or business. Basically, SCADA software is expected to perform monitoring, control, data collection, data recording and storage. Common areas that use SCADA systems are as follows:

1. Water treatment and promotion centres,
2. Oil and gas pipelines,
3. Gas power stations,
4. Dams,
5. Electricity transmission and distribution sites,
6. Wind Energy stations,
7. Communication systems,
8. Metro stations,
9. Airports,
10. Ships and docks,
11. Space stations,
12. Nuclear energy stations.

DCS which means “Distributed Contol System” is similar to SCADA in terms of general functions and usage areas. The differences are as follows:

1. While DCS is process-oriented, SCADA aims to collect data.
2. DCS runs on its local network while SCADA has no network restrictions.
3. DCS regularly checks the operation and does not save the process parameters to the database. SCADA, on the other hand, performs transactions according to the changed data recorded in the database without controlling data regularly.
4. DSC processes are performed with closed-loop control. There is no such control with SCADA.

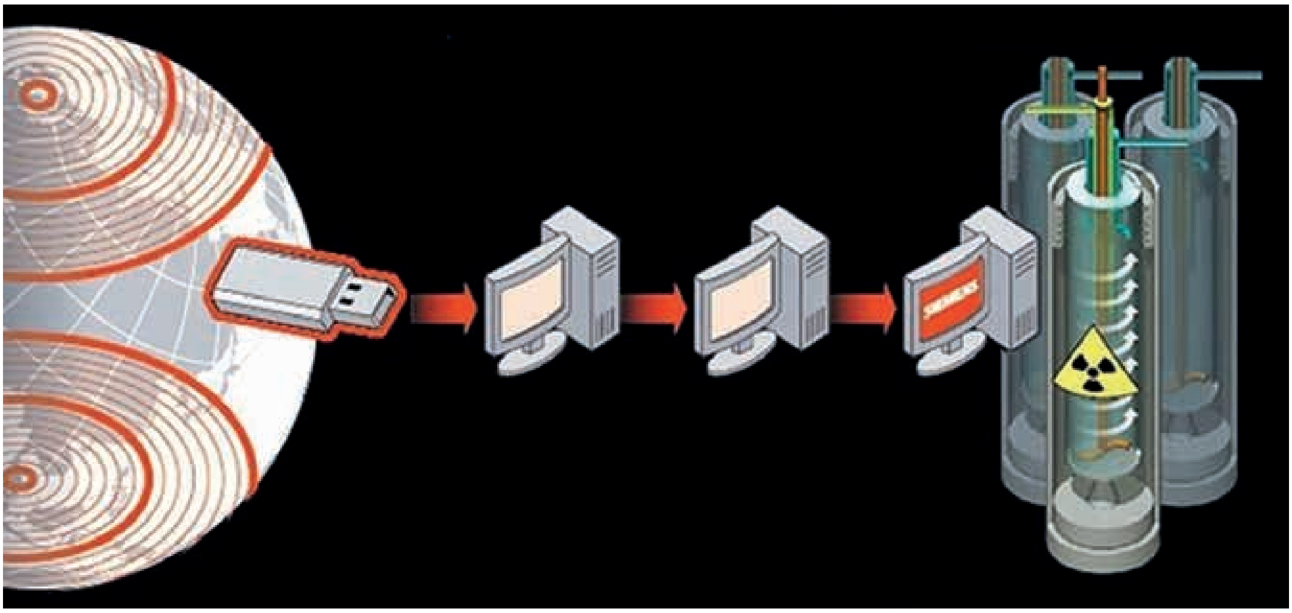
Why is Critical Infrastructure Security Important?

In information security, a variable asset to protect is information, while in critical infrastructures, it is process. That is, maintaining the current operational state of the systems is the number one task of a facility. Because a failure in this process, for example, interruption of city electricity due to a problem in the power plant, affects not only this plant but also the people of the country and paralyzes life. The loss is therefore too high to be expressed in any currency.

Most Known Critical Infrastructure Attacks

Stuxnet / IRAN

Stuxnet is the name of a cyber weapon noticed in June 2010, which was developed to attack Iran’s Natanz nuclear development facility. This attack was not officially undertaken by any state. The aforementioned weapon (Stuxnet) aimed at damaging the uranium enrichment process by affecting the rotational speeds of uranium-enriching centrifuges to reduce their lifetime at the Uranium enrichment plant in Natanz, Iran. In order to prevent the situation from being noticed by the operators, Stuxned had forced SCADA to repeatedly show the 21-second screen image it has taken over and over again, thus misleading the control engineers. The measurable result is $ 800 million of material damage with the deactivation of 984 centrifuges.



Ukraine

For the first time in history, a major cyberattack on a country's critical infrastructure (energy) was made on December 23, 2015, and people living in the area were severely affected and left without electricity. The number of people affected by the incident is expressed in hundreds of thousands with a mention of a power outage of about six hours. Unlike Stuxnet, more than one organisation was targeted and more than one attack method was preferred. The methods used are known as Malware (BlackEnergy), Phishing, KillDisk, GCat backdoor screen capture and Keylogger applications.

How to Ensure Critical Infrastructure Security?

The measures taken for information technology security also apply to critical infrastructures (strong password usage, preventing unauthorized users from accessing the system, etc.). However, the key concept here is the communication protocols used in the infrastructure. Known communication protocols such as HTTP, SSL, SMTP used in the Internet environment are replaced by lesser known protocols such as Modbus, DNP3, Profibus. However, the communication protocols used vary from device to device, and from industry to industry. For example, Siemens PLCs use the S7COMM protocol, while Allen Bradley PLCs generally use the Controlnet and Devicenet protocols. On the other hand, Ethernet / IP, GE SRTP, MODBUS, OPC DA are used in the oil and gas industry while DNP3, ICCP TASE.2, IEC60870-104, IEC61850, OPC... protocols are used in power plants. Naturally, the existing firewall, antivirus, IDS and IPS software on the market are insufficient for industrial control systems and cannot capture attacks and vulnerabilities in network traffic. In order to monitor the network traffic and to detect suspicious behaviour, critical infrastructures must work with cybersecurity companies that provide services in ICS and SCADA security fields. It is also known that local companies which have started to make themselves known all over the world recently have started to work in this field as well.

One way to ensure critical infrastructure security is to familiarise oneself with the devices used in these facilities. Again, in comparison with information technologies, the main components of a network are computers, modems and routers, whereas the main components of industrial control systems are PLCs, RTUs, IEDs and HMIs. Naturally, the operating logic of these devices should be fully understood and existing security vulnerabilities should be addressed by evaluating the protocols used.

Epilogue

Critical infrastructures play an important role in ensuring the safe and uninterrupted provision of services when needed. Essential services such as energy, water, food, health, finance, communication and security, which concern the society beyond the individual, must be provided in a safe, uninterrupted and intact manner. Disruptions in these categories of services due to cyber attacks can have unacceptable effects and seriously disturb society's peace and harm trust.

Particularly in the energy sector, despite all security measures taken, it may be considered that there may be interruptions due to attacks or other reasons, and the necessary plans are made to provide the needs from alternative sources is a measure that will take critical infrastructure security to a higher level.

Sources

- Protection of Critical Energy Infrastructures and Cyber Security - Zühre AYDIN
  https://www.academia.edu/24839120/Siber_Güvenlik_Kritik_Enerji_Altyapıları_Zühre_Aydın
- Document of Base Security Measures of Critical Information System Architectures - TÜBİTAK

http://bit.do/eXNRR

- What is OT Security?

https://www.forcepoint.com/tr/cyber-edu/ot-operational-technology-security

- Vast Differences Between IT and OT Cyber Security
  https://www.novotek.com/en/solutions/cyber-security-for-production-and-process-networks/vast-differences-between-it-and-ot-cyber-security
- Stuxnet and International Law: Anatomy of a cyber attack
  https://siberbulten.com/makale-analiz/stuxnet-ve-uluslararasi-hukuk-bir-siber-saldirinin-anatomisi/
- BTK - Cyber Security Board
  https://www.btk.gov.tr/siber-guvenlik-kurulu
- Effects of Cyber Attacks on Critical Infrastructures - Ender Şahinaslan, Önder Şahinaslan, Selçuk Selimli
  https://ab.org.tr/ab13/kitap/sahinaslan_sahinaslan_AB13.pdf

İbrahim Baloğlu • ibrahimbaloglu@yahoo.com

Through the Eyes of a Computer Forensics Analyst: Windows Forensics

Fellow Arka Kapı readers,

I have been working in the forensic informatics and cybersecurity fields since I was a student at Fırat University - Forensic Information Engineering. In this article, we are going to take a look at "Windows Forensic". It will be more of a guiding article and I would like to talk about some of the forensic concepts I used in the article before starting the article.

Forensic Informatics: A branch of science consisting of transferring all the digitally obtained shreds of evidence to different environments in a way that can be examined and accepted and then evaluating, analyzing and reporting these pieces of evidence in a plan and sequence.

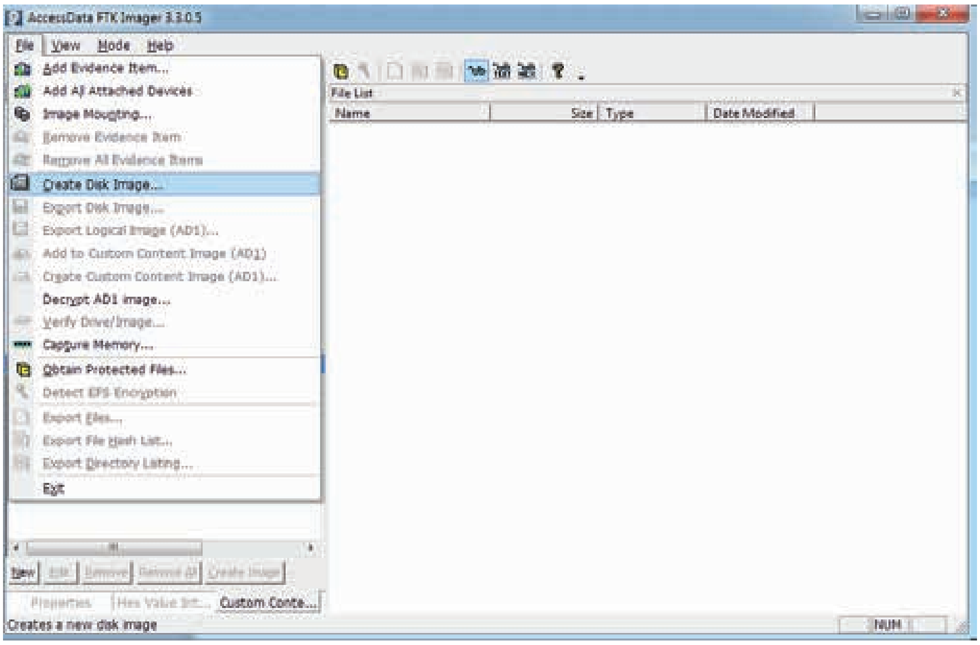
Image (Exact Copy): It is an exact copy of any storage device for inspection. E01 (developed by Encase, compresses the raw data) and DD (the raw data without applying any compression) formats are widely used.

Hash: It is a one-way summary function, and is like a fingerprint of files. Used to determine if files have been modified.

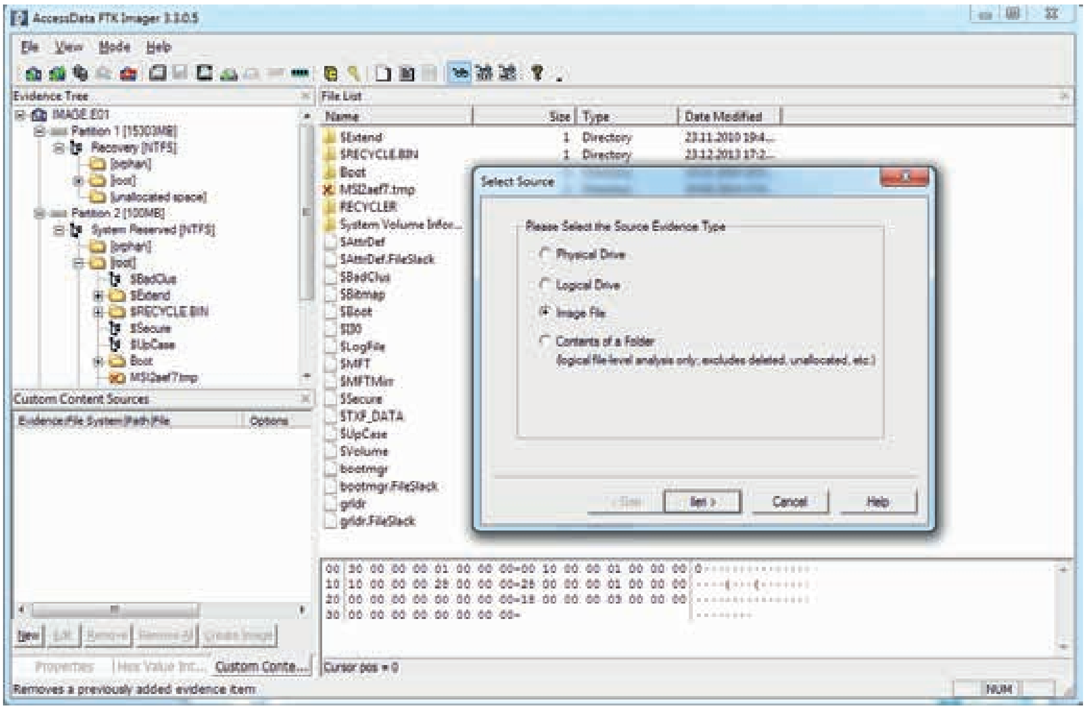
1. Image Capturing Using FTK Imager Software:

FTK Imager is free software produced by Access Data. FTK Imager software can be installed on the computer and can be run with Lite version. I recommend using the Lite version when taking an image during the event response, as you don't need any installation on the computer and it saves you time to get started with the image taking process as soon as possible. With the FTK Imager, you can take the image of RAM and storage devices and perform hash calculation and verification.

You can perform image acquisition with FTK Imager by selecting **File> Create Disk Image.**



You can import the image file into the FTK Imager by selecting **File> Add Evidence Item**.

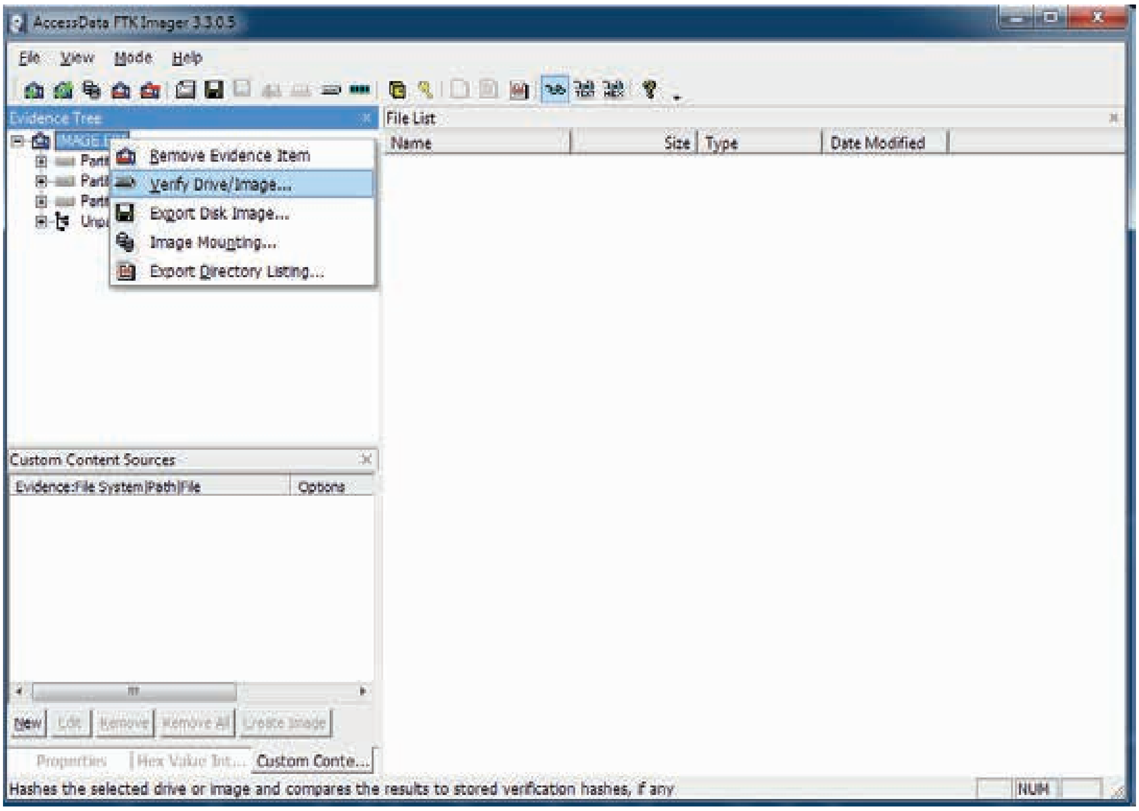


Please Select the Source Evidence Type

○ Physical Drive
○ Logical Drive
● Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

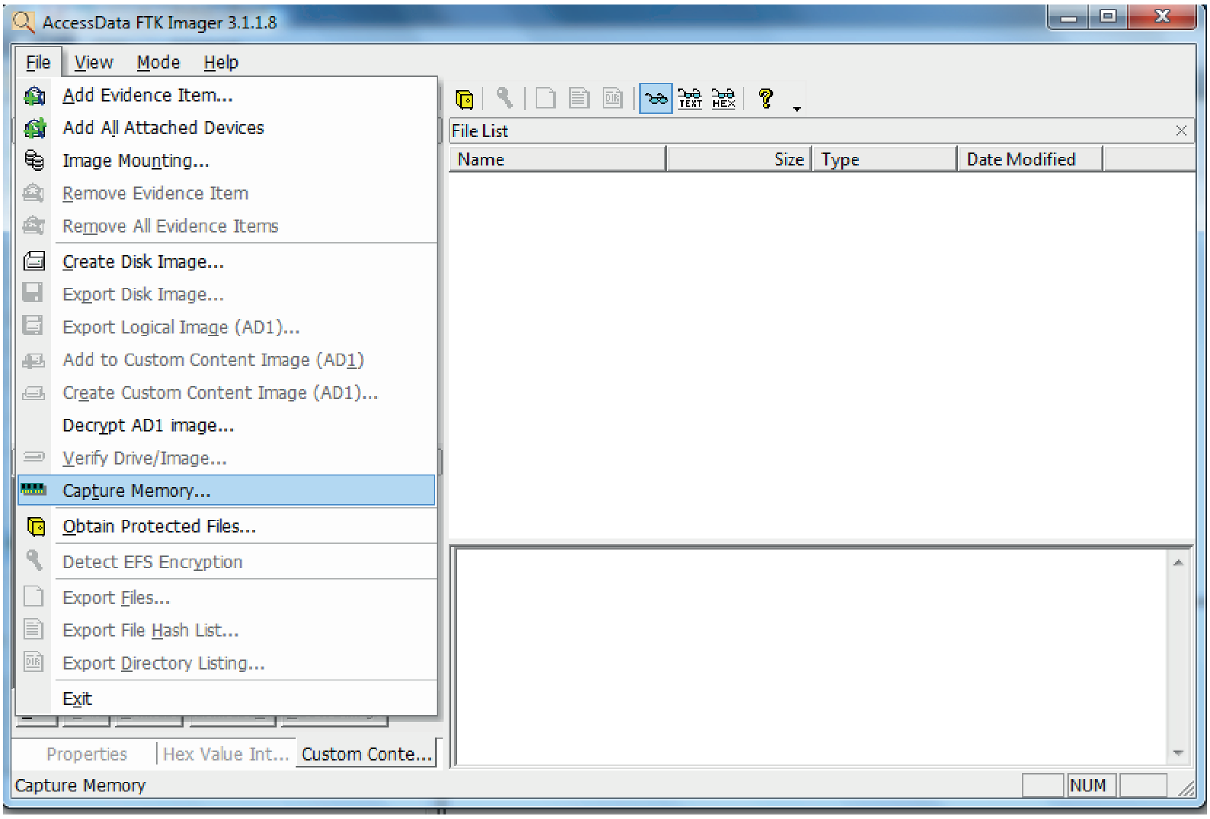
Removes a previously added evidence item

You can perform hash verification of the image file with FTK Imager by selecting **File> Verify Drive / Image.**



Hashes the selected drive or image and compares the results to stored verification hashes, if any

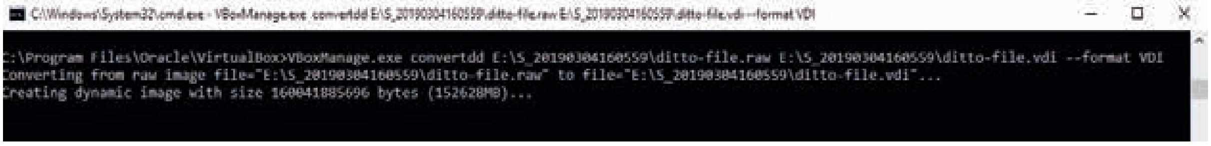
By selecting **File> Verify Drive / Image**, you can perform the RAM image acquisition with the FTK Imager.



2. Image File run Processing:

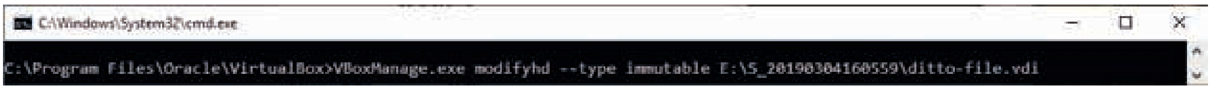
An existing image file can be run manually as an operating system without the need for any licensed software. If you write the image file with this process, you can examine it as it was a protected computer. In order to perform this process, you need to have the virtualisation software called VirtualBox installed on your computer.

Step 1: Using **VBoxManage** tool in VirtualBox virtualization software, an image file is converted to * .vdi format by using the "**VBoxManage.exe convertdd ImajDosyası.raw neximg.vdi --format VDI**" command.



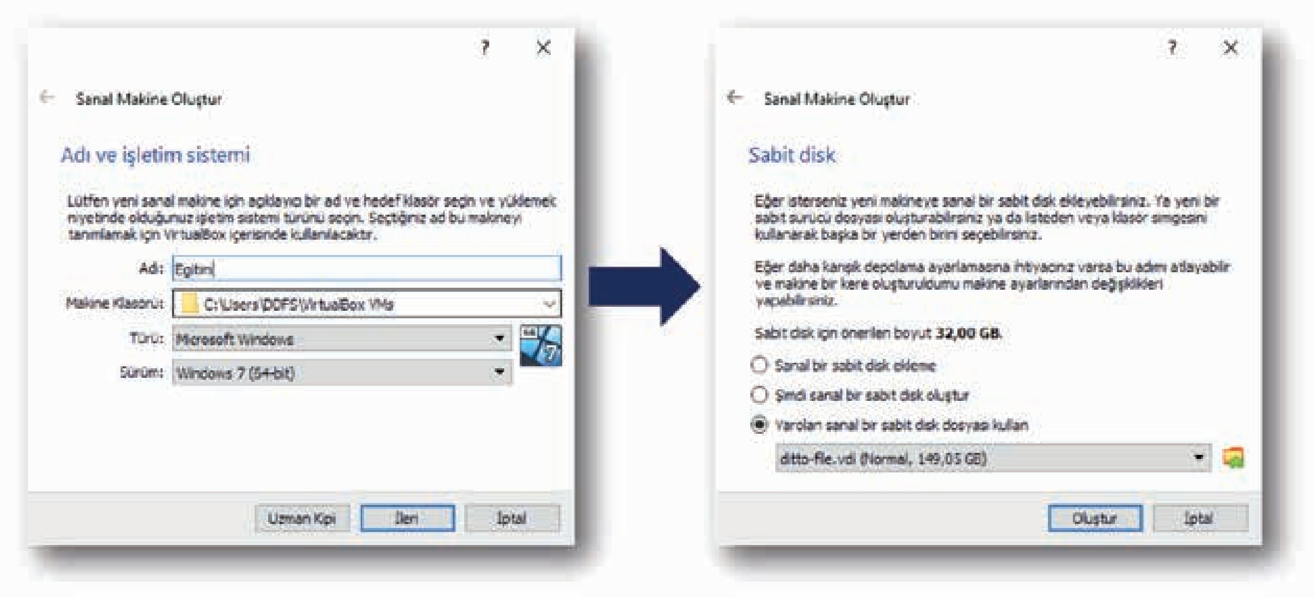
```
C:\Windows\System32\cmd.exe - VBoxManage.exe convertdd E:\S_20190304160559\ditto-file.raw E:\S_20190304160559\ditto-file.vdi --format VDI

C:\Program Files\Oracle\VirtualBox>VBoxManage.exe convertdd E:\S_20190304160559\ditto-file.raw E:\S_20190304160559\ditto-file.vdi --format VDI
Converting from raw image file="E:\S_20190304160559\ditto-file.raw" to file="E:\S_20190304160559\ditto-file.vdi"...
Creating dynamic image with size 160041885696 bytes (152628MB)...
```

Step 2: The resulting * .vdi file is only readable using the "VBoxManage.exe modifyhd --type immutable YeniHali.vdi" command.



```
C:\Windows\System32\cmd.exe

C:\Program Files\Oracle\VirtualBox>VBoxManage.exe modifyhd --type immutable E:\S_20190304160559\ditto-file.vdi
```

Step 3: The resulting * .vdi file is transferred to the VirtualBox virtualization software and run live.



Sanal Makine Oluştur

Adı ve işletim sistemi

Lütfen yeni sanal makine için açıklayıcı bir ad ve hedef klasör seçin ve yüklemek niyetinde olduğunuz işletim sistemi türünü seçin. Seçtiğiniz ad bu makineyi tanımlamak için VirtualBox içerisinde kullanılacaktır.

Adı: Egitim

Makine Klasörü: C:\Users\DDFS\VirtualBox VMs

Türü: Microsoft Windows

Sürüm: Windows 7 (64-bit)

Sanal Makine Oluştur

Sabit disk

Eğer isterseniz yeni makineye sanal bir sabit disk ekleyebilirsiniz. Ya yeni bir sabit sürücü dosyası oluşturabilirsiniz ya da listeden veya klasör simgesini kullanarak başka bir yerden birini seçebilirsiniz.

Eğer daha karışık depolama ayarlamasına ihtiyacınız varsa bu adımı atlayabilir ve makine bir kere oluşturulduğunu makine ayarlarından değişiklikleri yapabilirsiniz.

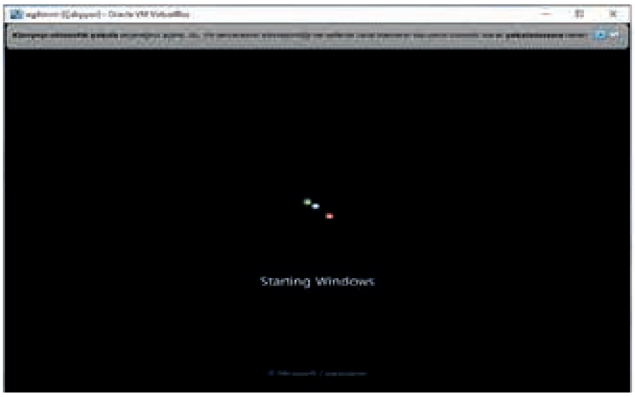
Sabit disk için önerilen boyut **32,00 GB**.

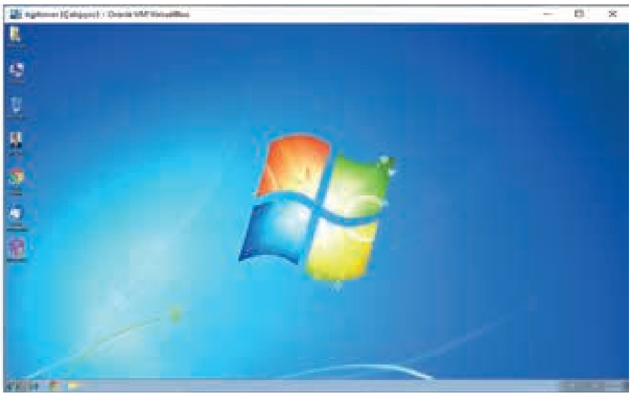
○ Sanal bir sabit disk ekleme

○ Şimdi sanal bir sabit disk oluştur

● Varolan sanal bir sabit disk dosyası kullan

ditto-file.vdi (Normal, 149,05 GB)

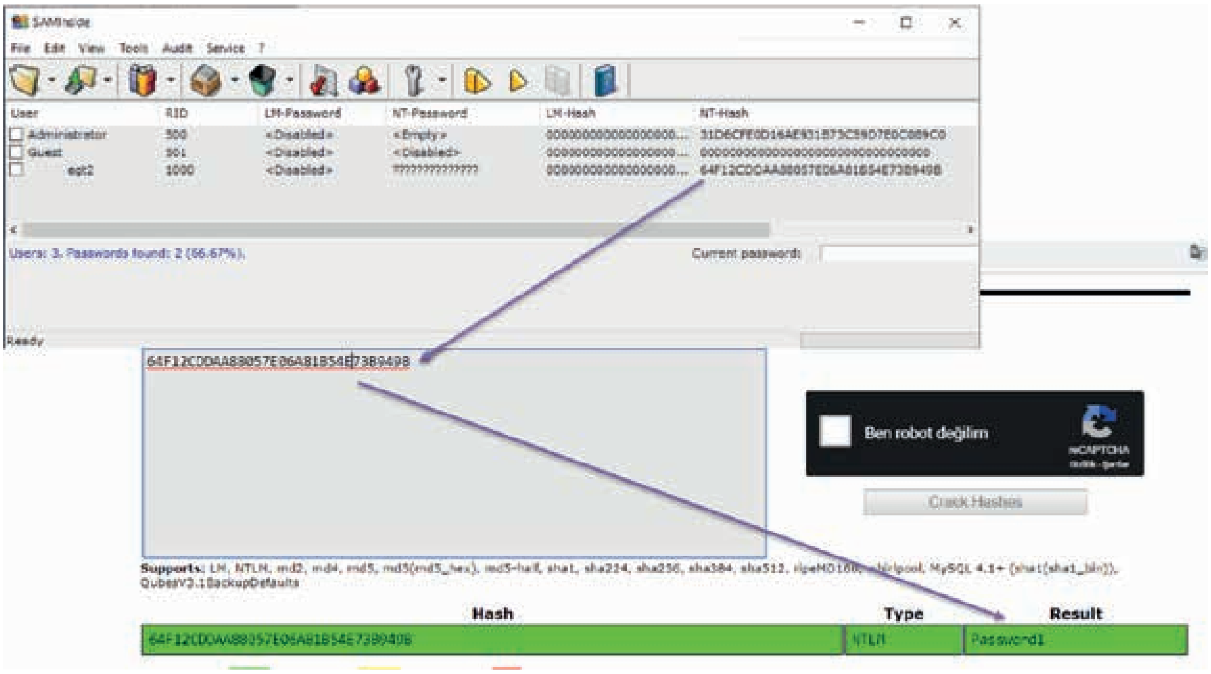




3. Obtaining User Accounts and Password Information Using SAM and SYSTEM Files:

You can copy the SAM and SYSTEM files found under the **C:\WINDOWS\system32\config** directory to the **C:\** directory using the "**C:\WINDOWS\system32\config >reg save hklm\sam C:\sam**" and "**C:\WINDOWS\system32\config >reg save hklm\system C:\system**" commands.

You can parse SAM and SYSTEM files with the SAMInside software. After parsing, you can obtain user accounts on the computer and NTLM-encrypted user passwords for these accounts. You can obtain the password that corresponds to the NTLM hash value obtained by using the web sites that allow the comparison with rainbow tables.



User	RID	LM-Password	NT-Password	LM-Hash	NT-Hash
□ Administrator	500	<Disabled>	<Empty>	0000000000000000...	31D6CFE0D16AE931B73C59D7E0C089C0
□ Guest	501	<Disabled>	<Disabled>	0000000000000000...	00000000000000000000000000000000
□ egt2	1000	<Disabled>	??????????????	0000000000000000...	64F12CDDAA88057E06A81B54E73B949B

Users: 3. Passwords found: 2 (66.67%).

Current password:

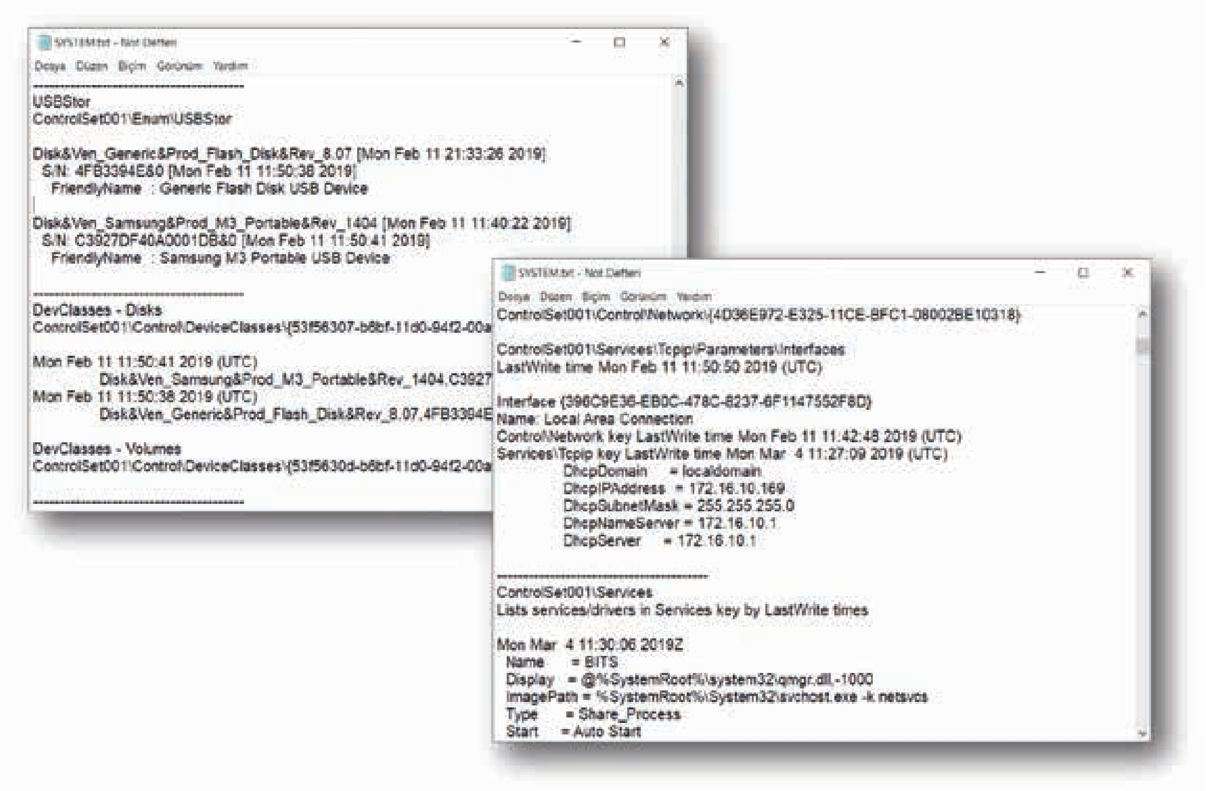
Ready

64F12CDDAA88057E06A81B54E73B949B

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
64F12CDDAA88057E06A81B54E73B949B	NTLM	Password1

You can also parse the SYSTEM file with the software named Regripper. You can obtain information about the external storage devices attached in the computer and many other data, such as the last IP address the computer has received. RegRipper is an automatic Registry parser that can parse SAM, SYSTEM, SOFTWARE and NTUSER.DAT files.


SYSTEM.txt - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
SYSTEM.txt - Not Defteri
Dosya Düzen Biçim Görünüm Yardım

```
----------------------------------------
USBStor
ControlSet001\Enum\USBStor

Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07 [Mon Feb 11 21:33:26 2019]
  S/N: 4FB3394E&0 [Mon Feb 11 11:50:38 2019]
    FriendlyName  : Generic Flash Disk USB Device
|
Disk&Ven_Samsung&Prod_M3_Portable&Rev_1404 [Mon Feb 11 11:40:22 2019]
  S/N: C3927DF40A0001DB&0 [Mon Feb 11 11:50:41 2019]
    FriendlyName  : Samsung M3 Portable USB Device

----------------------------------------
DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a

Mon Feb 11 11:50:41 2019 (UTC)
        Disk&Ven_Samsung&Prod_M3_Portable&Rev_1404,C3927
Mon Feb 11 11:50:38 2019 (UTC)
        Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07,4FB3394E

DevClasses - Volumes
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a

----------------------------------------
```

```
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}

ControlSet001\Services\Tcpip\Parameters\Interfaces
LastWrite time Mon Feb 11 11:50:50 2019 (UTC)

Interface {396C9E36-EB0C-478C-8237-6F1147552F8D}
Name: Local Area Connection
Control\Network key LastWrite time Mon Feb 11 11:42:48 2019 (UTC)
Services\Tcpip key LastWrite time Mon Mar  4 11:27:09 2019 (UTC)
        DhcpDomain     = localdomain
        DhcpIPAddress  = 172.16.10.169
        DhcpSubnetMask = 255.255.255.0
        DhcpNameServer = 172.16.10.1
        DhcpServer     = 172.16.10.1

----------------------------------------
ControlSet001\Services
Lists services/drivers in Services key by LastWrite times

Mon Mar  4 11:30:06 2019Z
  Name      = BITS
  Display   = @%SystemRoot%\system32\qmgr.dll,-1000
  ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
  Type      = Share_Process
  Start     = Auto Start
```

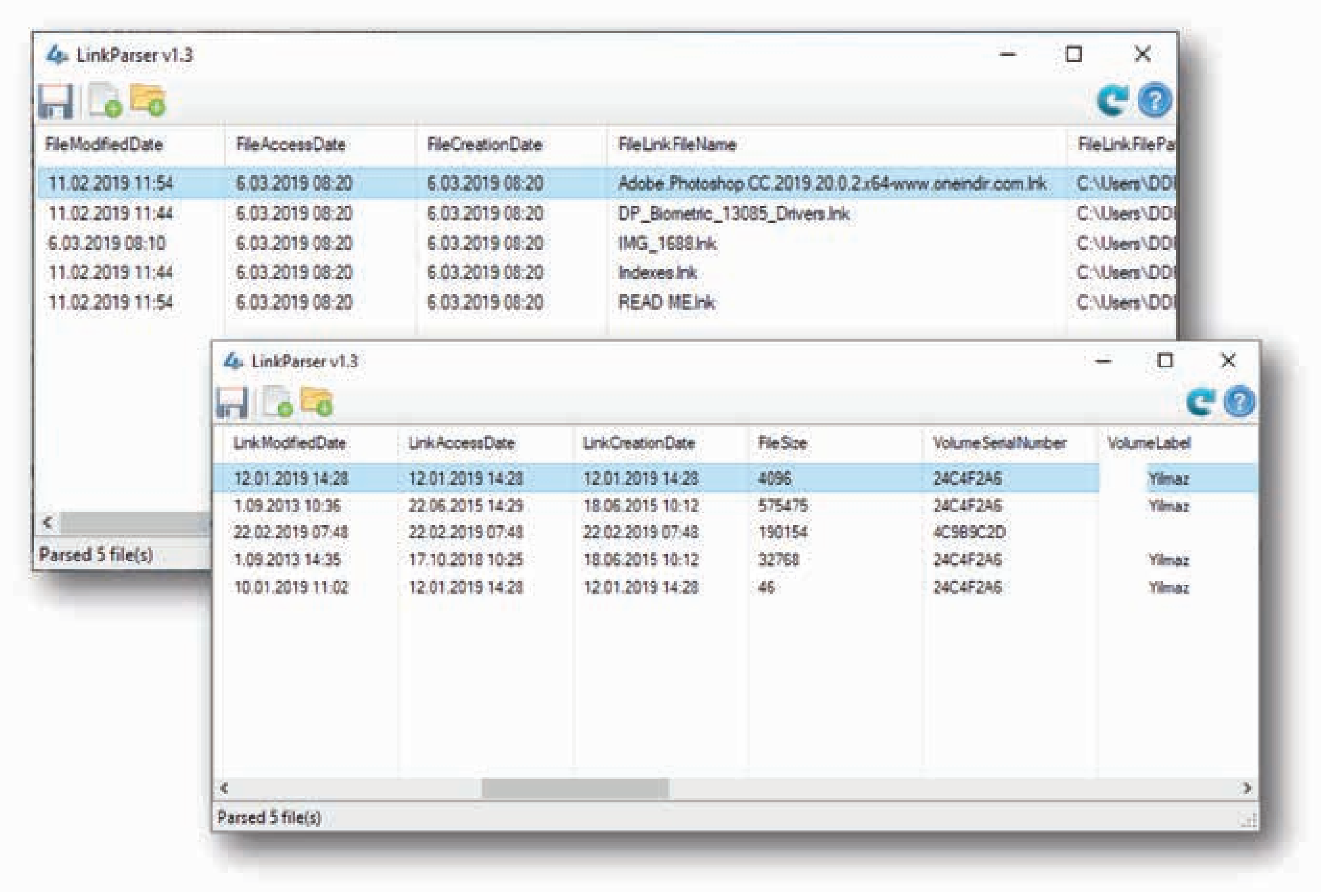
4. Analysis of ARTIFACT Files:

a. **LNK file:**

It is used in forensic examinations to determine which applications and which files were last opened by the user. If a deleted file is viewed before deleting, an **lnk** file of that file will be created, so that information about the deleted file can be obtained. When the lnk file, which is approximately 2 KB in size, is analyzed with LinkParser software; represents the creation date of the file, the modified date, the location of the file and the MAC address of the device on which the file can be obtained.

The location of lnkFiles varies according to the operating system.

- **C:\Documents and Settings\<username>\Recent\** on Windows XP
- **C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\** on Windows Vista/7/10



FileModifiedDate	FileAccessDate	FileCreationDate	FileLink.FileName	FileLink.FilePa
11.02.2019 11:54	6.03.2019 08:20	6.03.2019 08:20	Adobe.Photoshop.CC.2019.20.0.2.x64-www.oneindir.com.lnk	C:\Users\DD
11.02.2019 11:44	6.03.2019 08:20	6.03.2019 08:20	DP_Biometric_13085_Drivers.lnk	C:\Users\DD
6.03.2019 08:10	6.03.2019 08:20	6.03.2019 08:20	IMG_1688.lnk	C:\Users\DD
11.02.2019 11:44	6.03.2019 08:20	6.03.2019 08:20	Indexes.lnk	C:\Users\DD
11.02.2019 11:54	6.03.2019 08:20	6.03.2019 08:20	READ ME.lnk	C:\Users\DD

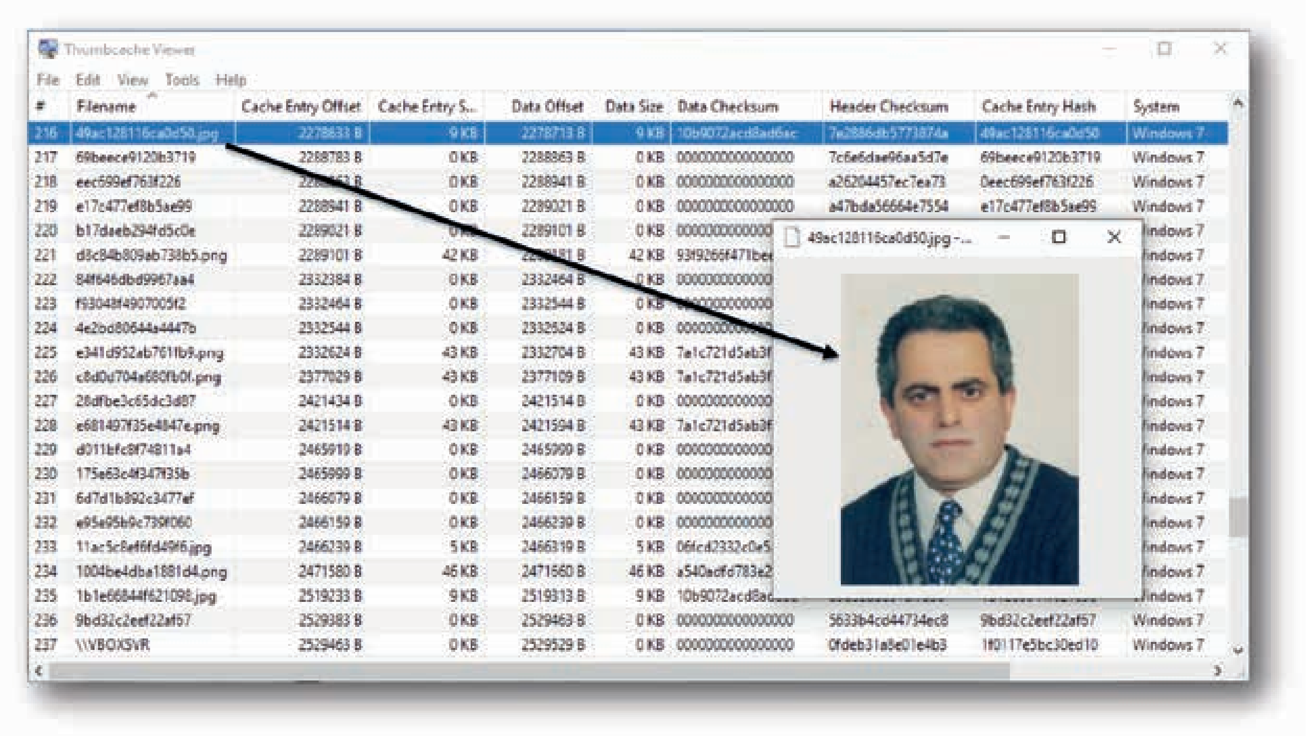
Parsed 5 file(s)

LinkModifiedDate	LinkAccessDate	LinkCreationDate	FileSize	VolumeSerialNumber	VolumeLabel
12.01.2019 14:28	12.01.2019 14:28	12.01.2019 14:28	4096	24C4F2A6	Yilmaz
1.09.2013 10:36	22.06.2015 14:29	18.06.2015 10:12	575475	24C4F2A6	Yilmaz
22.02.2019 07:48	22.02.2019 07:48	22.02.2019 07:48	190154	4C9B9C2D	
1.09.2013 14:35	17.10.2018 10:25	18.06.2015 10:12	32768	24C4F2A6	Yilmaz
10.01.2019 11:02	12.01.2019 14:28	12.01.2019 14:28	46	24C4F2A6	Yilmaz

Parsed 5 file(s)

b. **Thumbnail file:**

It is the database file that holds the small cached images of the windows and images displayed by the user. Thumbcache Viewer software is used to obtain cached thumbnails. Thumbnail files are located under **C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer\** directory.



#	Filename	Cache Entry Offset	Cache Entry S...	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System
216	49ac128116ca0d50.jpg	2278633 B	9 KB	2278713 B	9 KB	10b9072acd8ad6ac	7e2886db5773874a	49ac128116ca0d50	Windows 7
217	69beece9120b3719	2288783 B	0 KB	2288863 B	0 KB	0000000000000000	7c6e6dae96aa5d7e	69beece9120b3719	Windows 7
218	eec699ef763f226	[illegible]	0 KB	2288941 B	0 KB	0000000000000000	a26204457ec7ea73	0eec699ef763f226	Windows 7
219	e17c477ef8b5ae99	2288941 B	0 KB	2289021 B	0 KB	0000000000000000	a47bda56664e7554	e17c477ef8b5ae99	Windows 7
220	b17daeb294fd5c0e	2289021 B	0 KB	2289101 B	0 KB	000000000000			indows 7
221	d8c84b809ab738b5.png	2289101 B	42 KB	[illegible]	42 KB	93f9266f471be			indows 7
222	84f646dbd9967aa4	2332384 B	0 KB	2332464 B	0 KB	000000000000			indows 7
223	f93048f4907005f2	2332464 B	0 KB	2332544 B	0 KB	000000000000			indows 7
224	4e2bd80644a4447b	2332544 B	0 KB	2332624 B	0 KB	000000000000			indows 7
225	e341d952ab761fb9.png	2332624 B	43 KB	2332704 B	43 KB	7a1c721d5ab3f			indows 7
226	c8d0d704a680fb0f.png	2377029 B	43 KB	2377109 B	43 KB	7a1c721d5ab3f			indows 7
227	28dfbe3c65dc3d87	2421434 B	0 KB	2421514 B	0 KB	000000000000			indows 7
228	e681497f35e4847e.png	2421514 B	43 KB	2421594 B	43 KB	7a1c721d5ab3f			indows 7
229	d011bfc8f74811a4	2465919 B	0 KB	2465999 B	0 KB	000000000000			indows 7
230	175e63c4f347f35b	2465999 B	0 KB	2466079 B	0 KB	000000000000			indows 7
231	6d7d1b892c3477ef	2466079 B	0 KB	2466159 B	0 KB	000000000000			indows 7
232	e95a95b9c739f060	2466159 B	0 KB	2466239 B	0 KB	000000000000			indows 7
233	11ac5c8ef6fd49f6.jpg	2466239 B	5 KB	2466319 B	5 KB	06fcd2332c0e5			indows 7
234	1004be4dba1881d4.png	2471580 B	46 KB	2471660 B	46 KB	a540acfd783e2			indows 7
235	1b1e66844f621098.jpg	2519233 B	9 KB	2519313 B	9 KB	10b9072acd8ad			indows 7
236	9bd32c2eef22af57	2529383 B	0 KB	2529463 B	0 KB	0000000000000000	5633b4cd44734ec8	9bd32c2eef22af57	Windows 7
237	\\VBOXSVR	2529463 B	0 KB	2529529 B	0 KB	0000000000000000	0fdeb31a8e01e4b3	1f0117e5bc30ed10	Windows 7

c. **Recycle.bin file:**

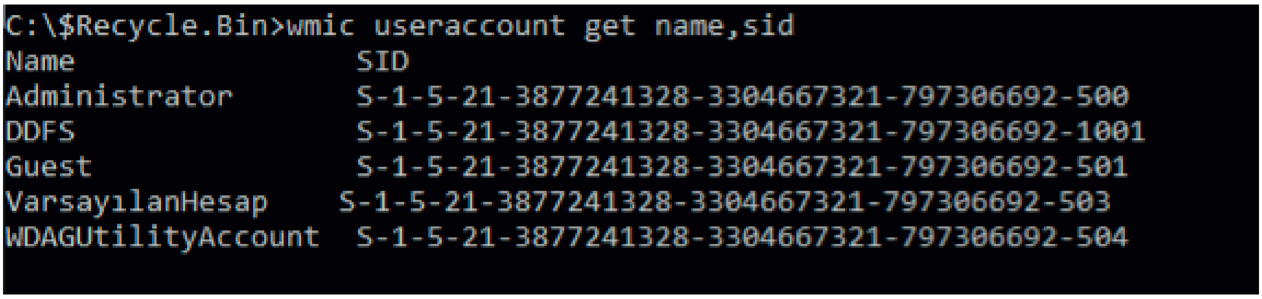
This is the file that keeps the information of the files you deleted from the recycle bin. You can recover the deleted files from the recycle bin by following the steps specified below.

The location of the Recycle.bin file varies depending on the operating system.

- **C:\RECYCLE** on Windows XP
- **C:\$Recycle.bin** on Windows Vista/7/10

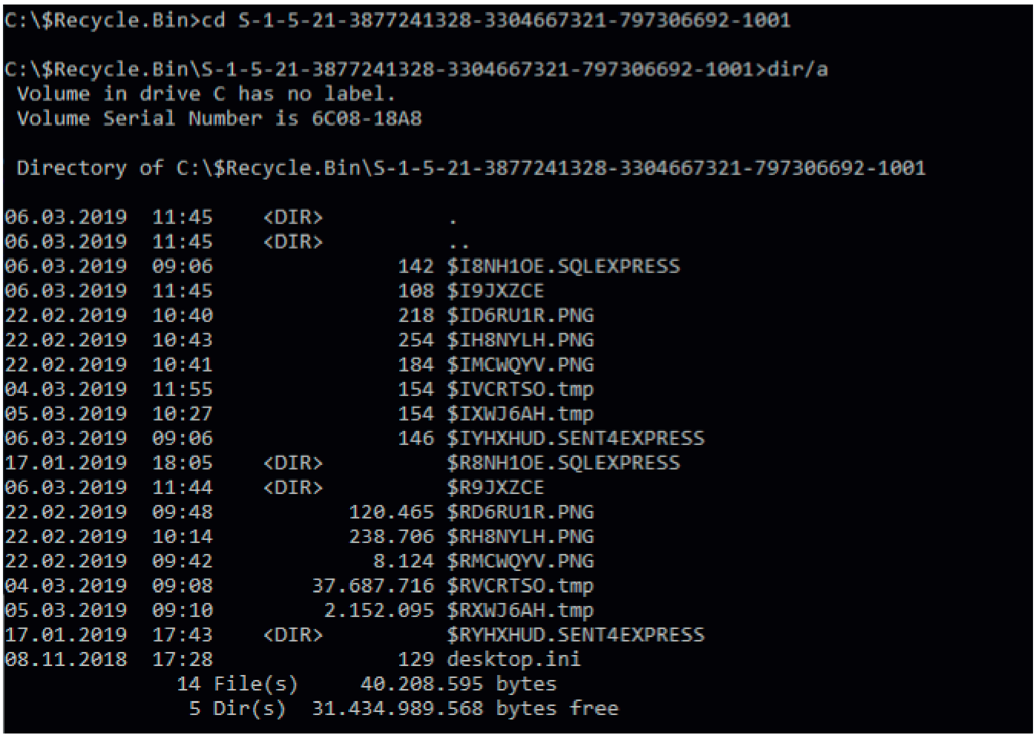
Step 1: You can obtain information about users with **wmic useraccount get name,sid** on C: \ $ Recycle.bin location from the console screen.

Changing the directory to **C:\$Recycle.bin** from the command line, the information of the user can be obtained using the **wmic useraccount get name,sid** command.



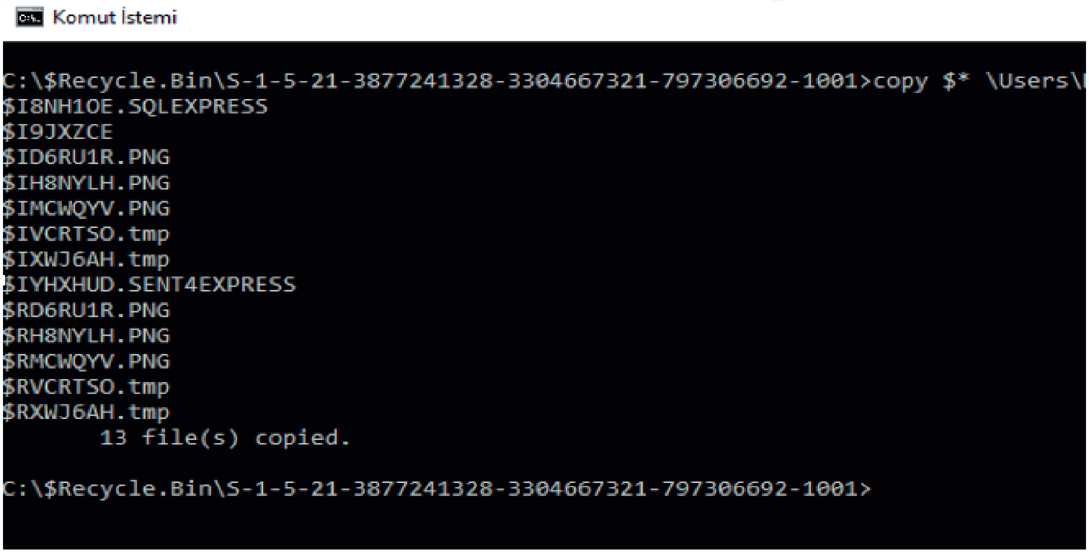
```
C:\$Recycle.Bin>wmic useraccount get name,sid
Name                  SID
Administrator         S-1-5-21-3877241328-3304667321-797306692-500
DDFS                  S-1-5-21-3877241328-3304667321-797306692-1001
Guest                 S-1-5-21-3877241328-3304667321-797306692-501
VarsayılanHesap      S-1-5-21-3877241328-3304667321-797306692-503
WDAGUtilityAccount    S-1-5-21-3877241328-3304667321-797306692-504
```

Step 2: From the obtained user information, you can log into the SID file of the user you are using cd command with and then view the files in the directory with **dir\a** command.



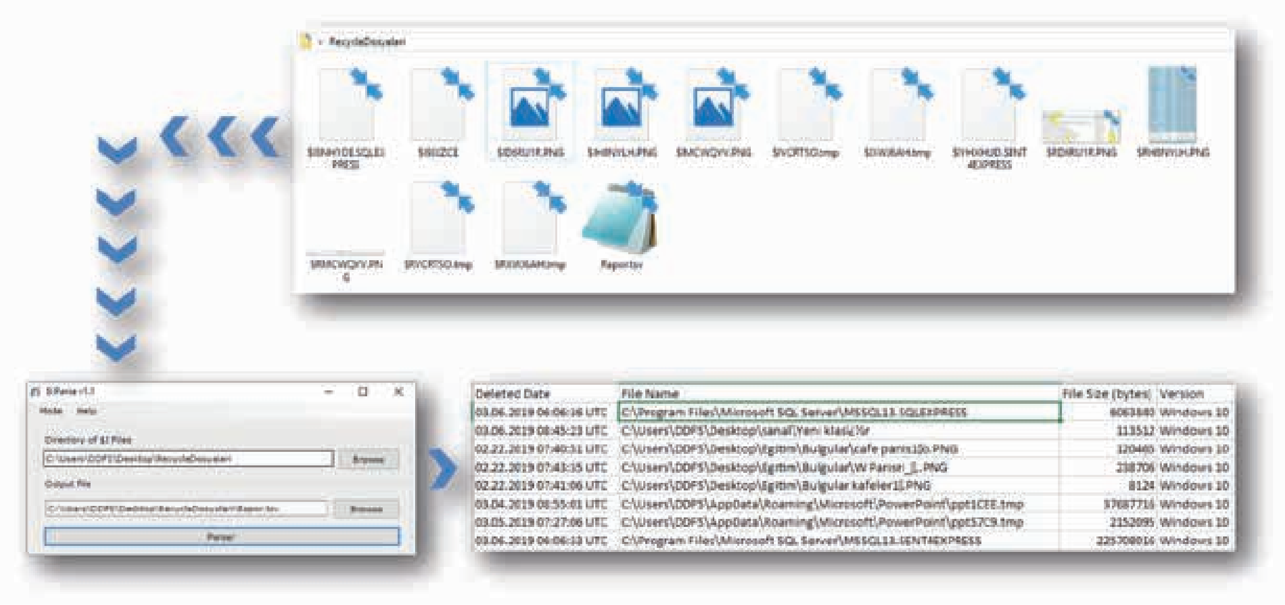
```
C:\$Recycle.Bin>cd S-1-5-21-3877241328-3304667321-797306692-1001

C:\$Recycle.Bin\S-1-5-21-3877241328-3304667321-797306692-1001>dir/a
 Volume in drive C has no label.
 Volume Serial Number is 6C08-18A8

 Directory of C:\$Recycle.Bin\S-1-5-21-3877241328-3304667321-797306692-1001

06.03.2019  11:45    <DIR>          .
06.03.2019  11:45    <DIR>          ..
06.03.2019  09:06               142 $I8NH1OE.SQLEXPRESS
06.03.2019  11:45               108 $I9JXZCE
22.02.2019  10:40               218 $ID6RU1R.PNG
22.02.2019  10:43               254 $IH8NYLH.PNG
22.02.2019  10:41               184 $IMCWQYV.PNG
04.03.2019  11:55               154 $IVCRTSO.tmp
05.03.2019  10:27               154 $IXWJ6AH.tmp
06.03.2019  09:06               146 $IYHXHUD.SENT4EXPRESS
17.01.2019  18:05    <DIR>          $R8NH1OE.SQLEXPRESS
06.03.2019  11:44    <DIR>          $R9JXZCE
22.02.2019  09:48           120.465 $RD6RU1R.PNG
22.02.2019  10:14           238.706 $RH8NYLH.PNG
22.02.2019  09:42             8.124 $RMCWQYV.PNG
04.03.2019  09:08        37.687.716 $RVCRTSO.tmp
05.03.2019  09:10         2.152.095 $RXWJ6AH.tmp
17.01.2019  17:43    <DIR>          $RYHXHUD.SENT4EXPRESS
08.11.2018  17:28               129 desktop.ini
              14 File(s)     40.208.595 bytes
               5 Dir(s)  31.434.989.568 bytes free
```

Step 3: The detected files are exported with the command "**copy** *$**I <Address-to-Copy>**".



```
C:\$Recycle.Bin\S-1-5-21-3877241328-3304667321-797306692-1001>copy $* \Users\
$I8NH1OE.SQLEXPRESS
$I9JXZCE
$ID6RU1R.PNG
$IH8NYLH.PNG
$IMCWQYV.PNG
$IVCRTSO.tmp
$IXWJ6AH.tmp
$IYHXHUD.SENT4EXPRESS
$RD6RU1R.PNG
$RH8NYLH.PNG
$RMCWQYV.PNG
$RVCRTSO.tmp
$RXWJ6AH.tmp
        13 file(s) copied.

C:\$Recycle.Bin\S-1-5-21-3877241328-3304667321-797306692-1001>
```

Step 4: The extracted files are parsed and made meaningful with **$I Parser** software. After the parsing process; file names, locations, deletion dates, and lots of information is obtained.



Directory of $I Files: C:\Users\DDFS\Desktop\RecycleDosyalari

Output File: C:\Users\DDFS\Desktop\RecycleDosyalari\Rapor.tsv

Deleted Date	File Name	File Size (bytes)	Version
03.06.2019 06:06:16 UTC	C:\Program Files\Microsoft SQL Server\MSSQL13.SQLEXPRESS	6063840	Windows 10
03.06.2019 08:45:23 UTC	C:\Users\DDFS\Desktop\sanal\Yeni klasör	113512	Windows 10
02.22.2019 07:40:31 UTC	C:\Users\DDFS\Desktop\Egitim\Bulgular\cafe paris10.PNG	120460	Windows 10
02.22.2019 07:43:15 UTC	C:\Users\DDFS\Desktop\Egitim\Bulgular\W Parise_1.PNG	238706	Windows 10
02.22.2019 07:41:06 UTC	C:\Users\DDFS\Desktop\Egitim\Bulgular kafeler1.PNG	8124	Windows 10
03.04.2019 08:55:01 UTC	C:\Users\DDFS\AppData\Roaming\Microsoft\PowerPoint\ppt1CEE.tmp	37687716	Windows 10
03.05.2019 07:27:06 UTC	C:\Users\DDFS\AppData\Roaming\Microsoft\PowerPoint\ppt57C9.tmp	2152095	Windows 10
03.06.2019 06:06:13 UTC	C:\Program Files\Microsoft SQL Server\MSSQL13.SENT4EXPRESS	225708016	Windows 10

Since I always believe that engineering/expertise can be used to review any system manually without using licensed software, I try to explain on my knowledge and experience in the fields of Forensic Computing and Cyber Security.

The Windows Forensic issue is quite deep and long, and I have only mentioned some parts of it in hopes that it will provide some guidance to you.

My best regards.

Ata Şahan Erdemir • erdemir.ata@gmail.com

GATHERING INTELLIGENCE WITH MALTEGO

Before we start, I would like to state that this article had been prepared for educational uses only, and no responsibility is taken for its bad uses.

In recent times when cross-national and social incidents have increased, the matter of intelligence has gained much importance. There is a remarkable increase in the number of cyber-attacks performed compared to the past. Countries are literally competing against gaining each other's military, economic and other confidential information through cyber intelligent methods. Last year, the number of APT groups who are especially concerned with this kind of stuff has incremented. The most known among these is the APT40[1] as named by FireEye. This is just an example yet tens of known and unknown groups exist.

Being aware of the current time we're in, understanding the dynamics it creates and knowing where one fits in in the cyber world are necessary to protect oneself from the threats. If we can't correctly analyse the situation we're in and not know what to concentrate on, we can't take the necessary precautions. This is why vulnerabilities emerge. Cyber attackers work nonstop for days, weeks and months in order to find weaknesses. Of course, the most important part of investigating and analysing a system is gathering information about the system or person. The better the attackers know the system or person, the better they know about the vulnerabilities or vulnerabilities that the person or the system has - they thus determine the attack methods and cyber weapons accordingly. Active and passive intelligence gathering techniques are used for this. Maltego is a tool that enables us to actively gather information. Let's go deeper.

Source: http://bit.ly/2kcrbMg

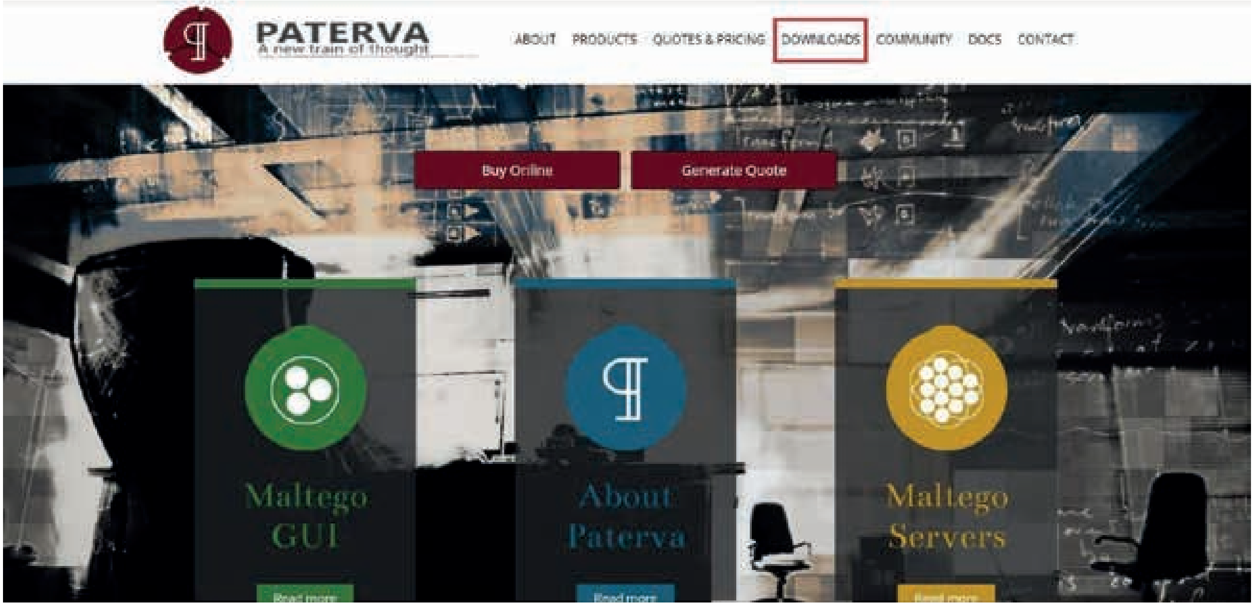
[1] https://www.fireeye.com/current-threats/apt-groups.html

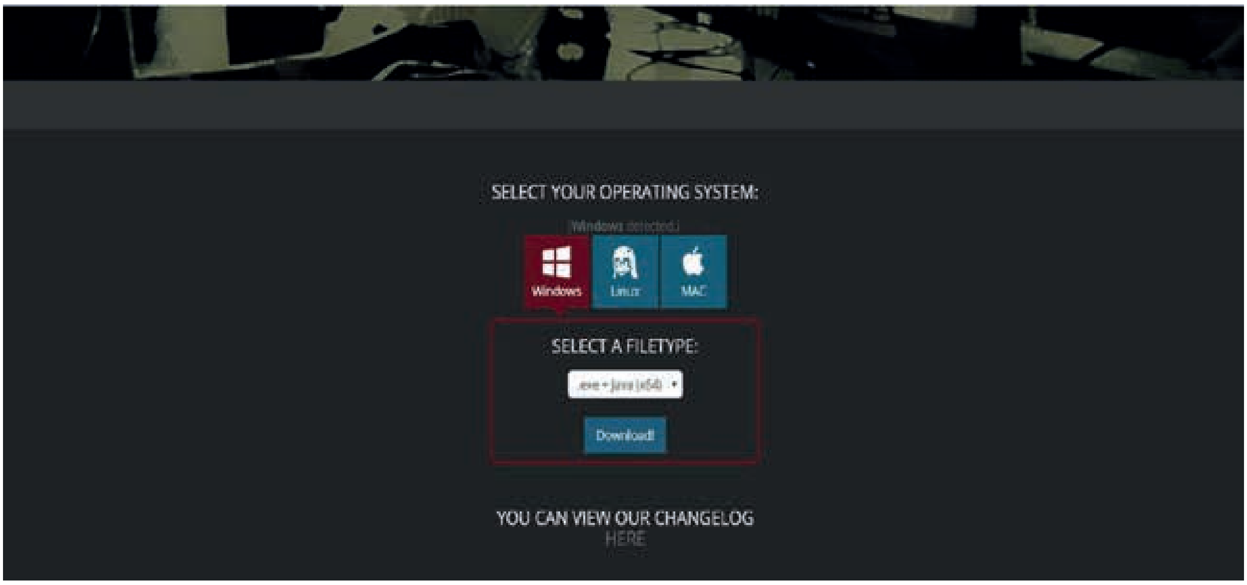
Among the most popular and practical cyber intelligence tools, Maltego is a very practical information-gathering program that can be found built-in in Kali Linux. Its producer "Paterva" is a program actively used in penetration testing and intelligence gathering processes.

Maltego's special packets for commercial use are also available and these packets are of extra charge, however, you can download the *Community* packet for free and use it for non-commercial uses.

Installing Maltego for,

Windows:

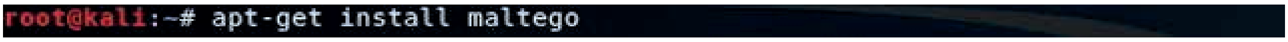




You can choose the download option suitable according to the architecture of your computer (32-64 bit). There are also options for Linux and MAC.

Linux:

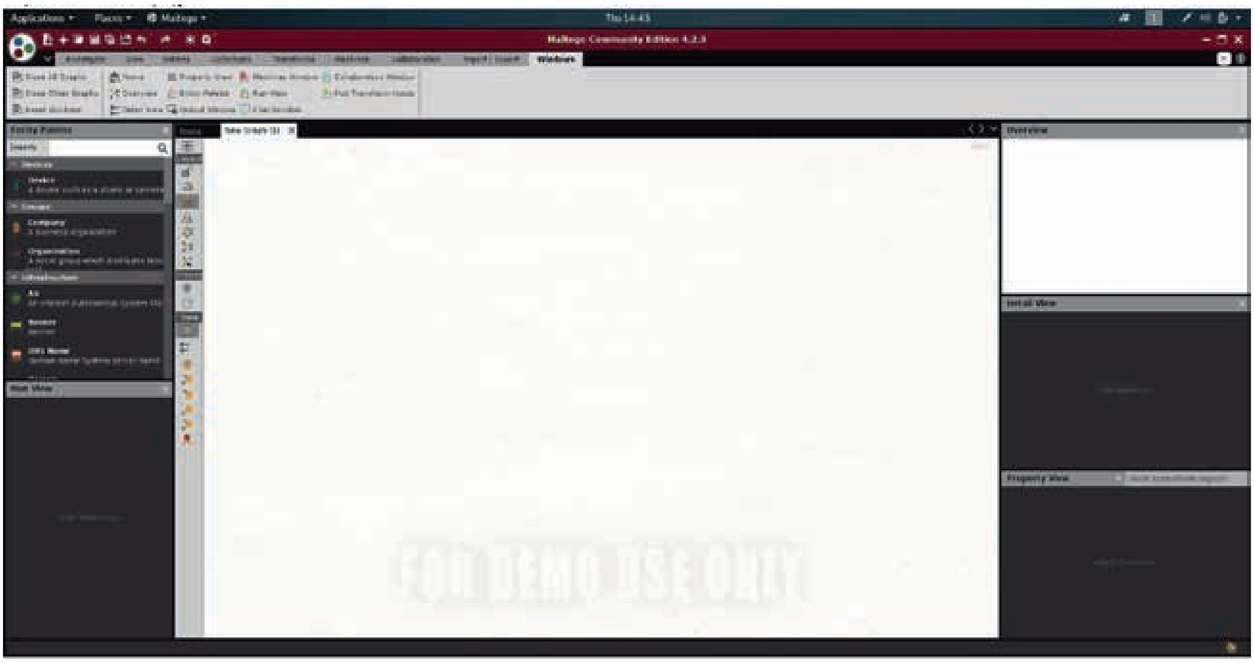
Maltego is usually built-in in security-based Linux distributions. For cases where it is not, the process goes like this:



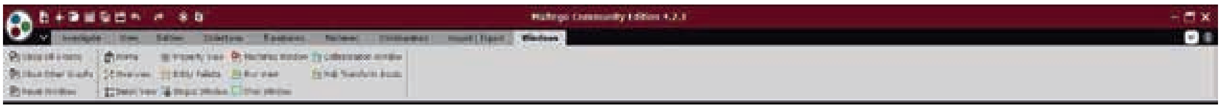
```
root@kali:~# apt-get install maltego
```

With the command above, you can install Maltego.

When you open Maltego, it will ask you to log in. You can obtain a membership from Paterva's website or directly sign up with the screen the program requests.



The screen after Maltego is opened and logged in.

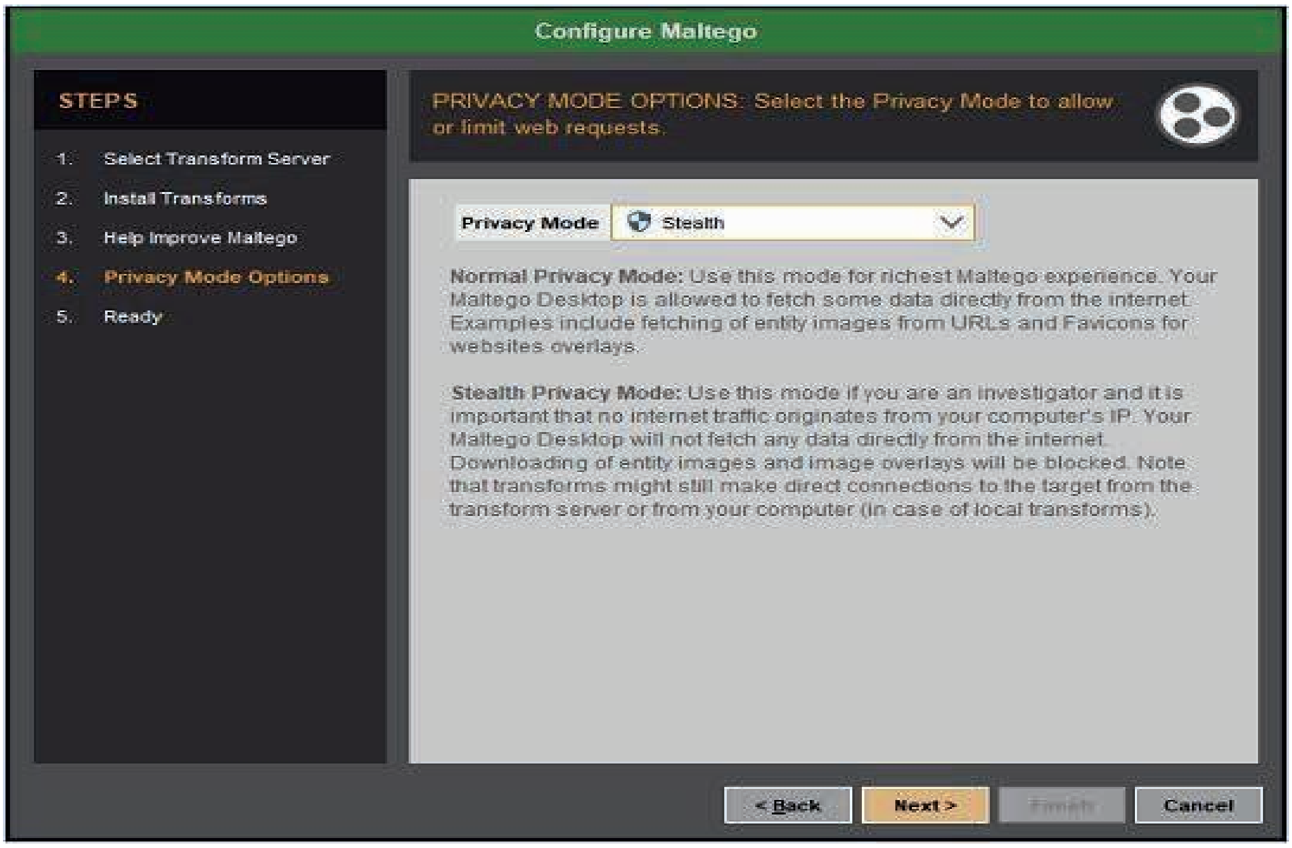


The menu has some titles like,

- Investigate
- View
- Entities
- Collections
- Transforms
- Machines
- Collaboration
- Import/Export
- Windows

Investigate

Investigate is where the investigation modification, diagram preparation etc. are features are used. Now, has *Privacy Mode* with the new version.



Configure Maltego

STEPS

1. Select Transform Server
2. Install Transforms
3. Help Improve Maltego
4. Privacy Mode Options
5. Ready

PRIVACY MODE OPTIONS: Select the Privacy Mode to allow or limit web requests.

Privacy Mode: Stealth

Normal Privacy Mode: Use this mode for richest Maltego experience. Your Maltego Desktop is allowed to fetch some data directly from the internet. Examples include fetching of entity images from URLs and Favicons for websites overlays.

Stealth Privacy Mode: Use this mode if you are an investigator and it is important that no internet traffic originates from your computer's IP. Your Maltego Desktop will not fetch any data directly from the internet. Downloading of entity images and image overlays will be blocked. Note that transforms might still make direct connections to the target from the transform server or from your computer (in case of local transforms).

Source : https://maltego.freshdesk.com/support/discussions/topics/15000005039

This is a module especially designed for researchers. This module does not generate any queries that contain your IP. The title also prevents from downloading images. However, there is still no guarantee that a precise direct connection will be established. Of course, the disadvantage of this is that it will not offer a user experience as it does in normal mode, so it may not produce rich content. In addition to this feature, the quick find option is also included in this tab.

View

This is the part used to edit the display and hierarchy of the results. This is where organic hierarchy and other hierarchy layouts are found. Adjusting the layout of your work can improve your ability to study it.

Entities

Here, you can add or edit entities. This is the section where you can make designs according to your needs. You can add or remove new entity types, or edit existing entities.

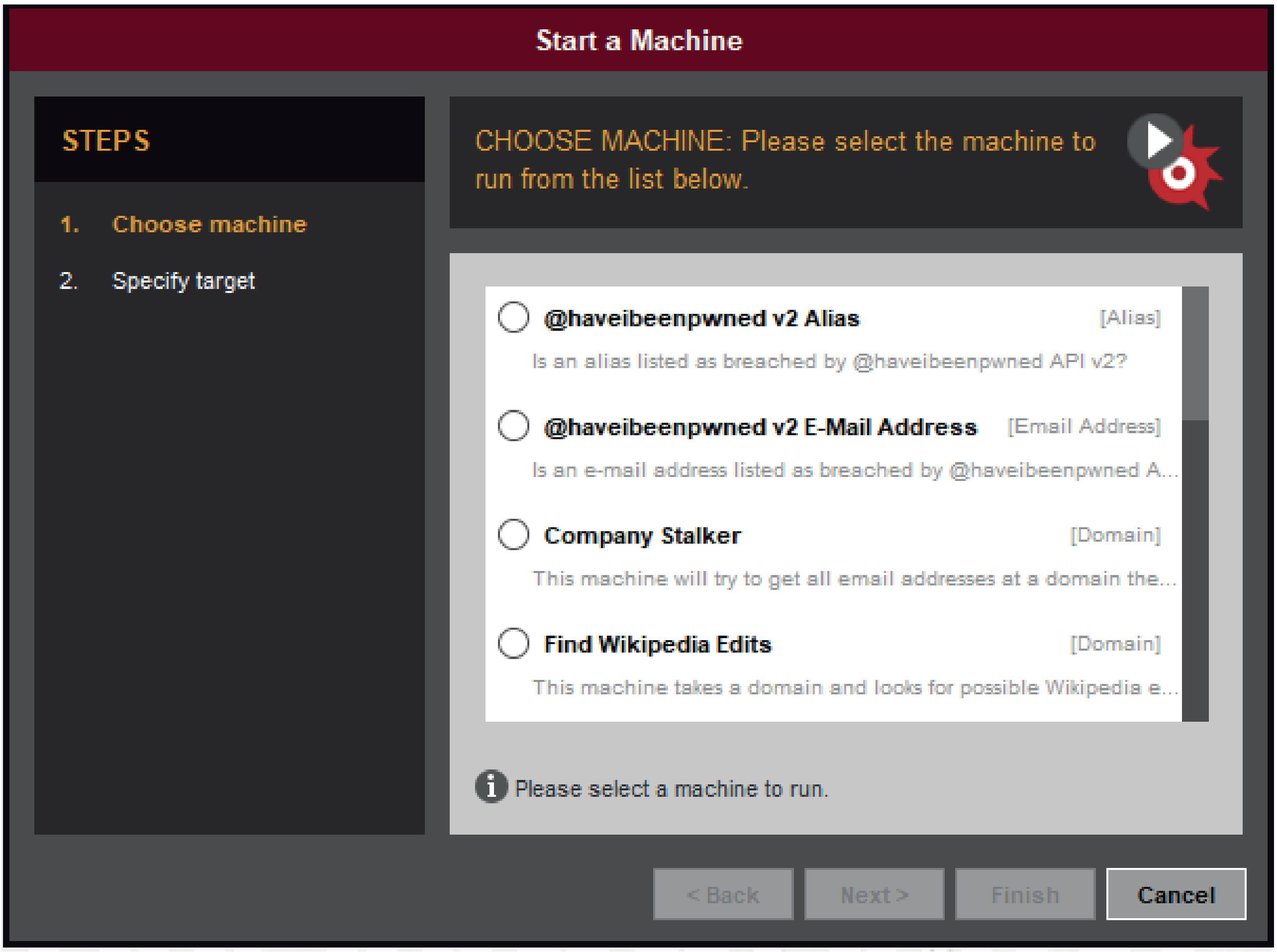
Collections

In this section, simplifying is done in order to understand the collected data. It collects the data of same types in a square and simplifies the image. You can also specify how many of the findings to be displayed.

Transforms

Here, you can manage, add or remove used services. If you right-click on the things like domain, person etc., you can see some options lik "to IP" etc.

Machines



Start a Machine

STEPS

1. Choose machine

2. Specify target

CHOOSE MACHINE: Please select the machine to run from the list below.

○ @haveibeenpwned v2 Alias [Alias]
Is an alias listed as breached by @haveibeenpwned API v2?

○ @haveibeenpwned v2 E-Mail Address [Email Address]
Is an e-mail address listed as breached by @haveibeenpwned A...

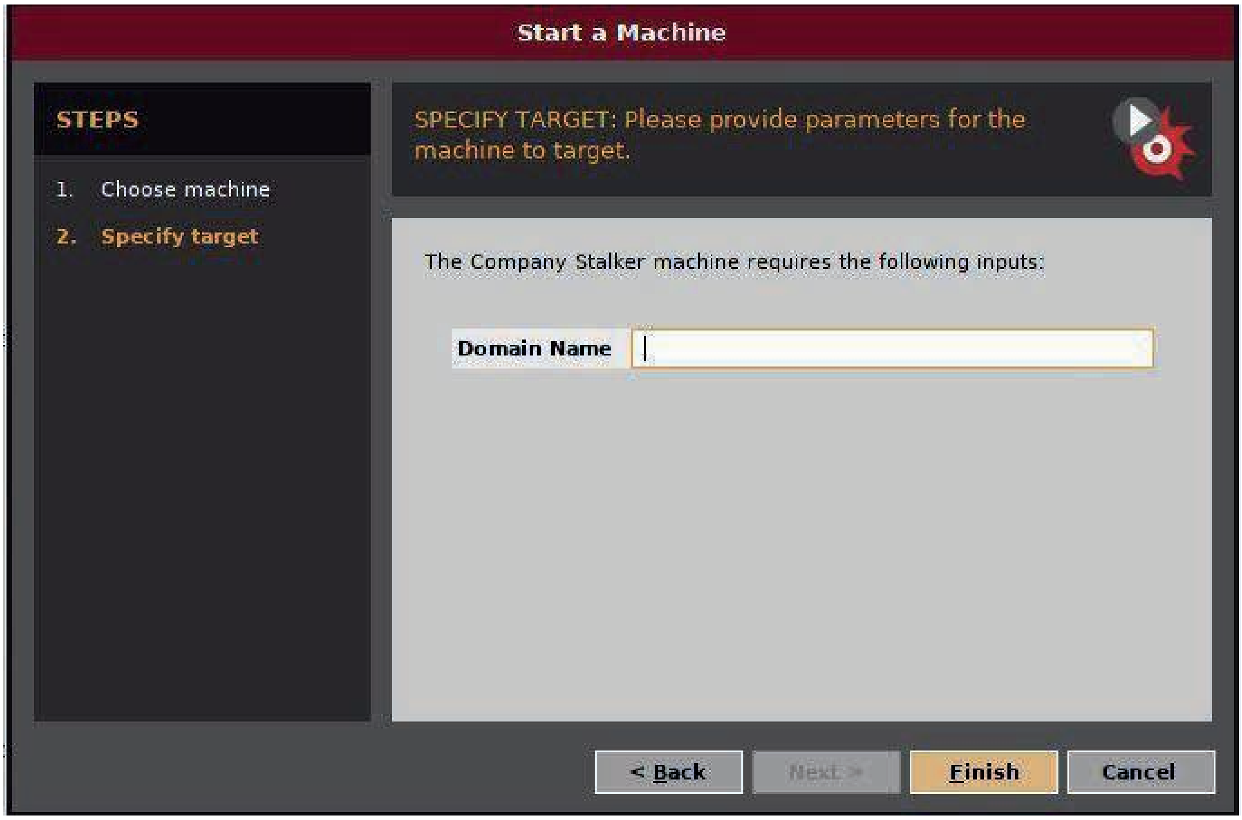
○ Company Stalker [Domain]
This machine will try to get all email addresses at a domain the...

○ Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia e...

Please select a machine to run.

This is where the automated tools are found. It contains queries specially prepared for the person, company, domain, etc. that you want to collect information about.

You can select any option as in the image.



Start a Machine

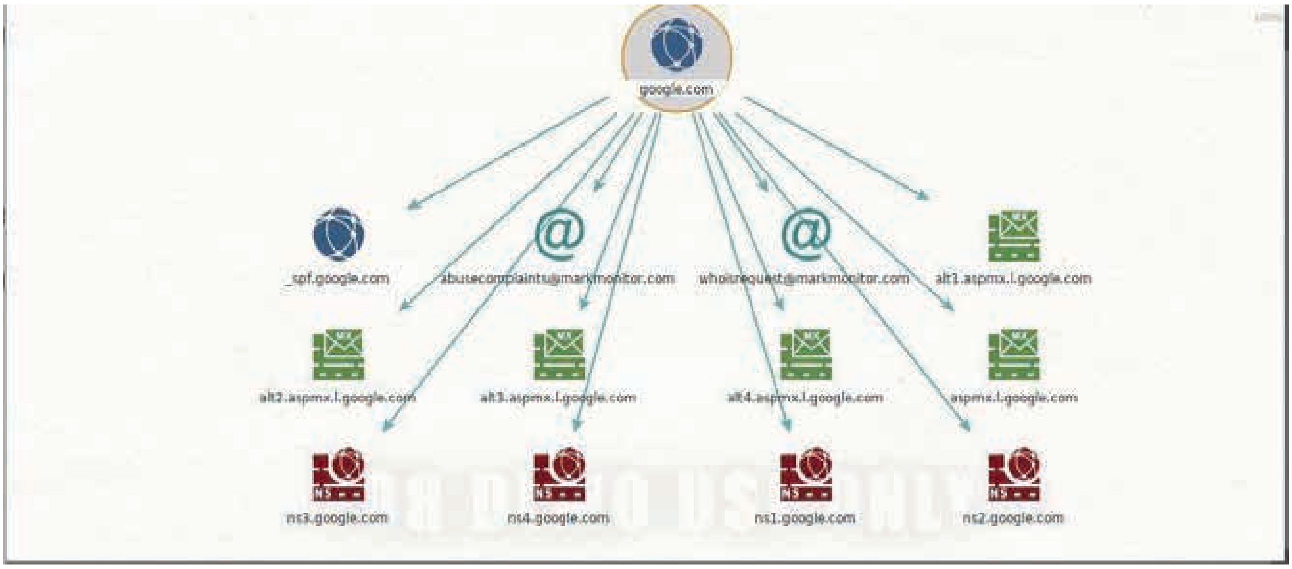
STEPS

1. Choose machine
2. Specify target

SPECIFY TARGET: Please provide parameters for the machine to target.

The Company Stalker machine requires the following inputs:

Domain Name

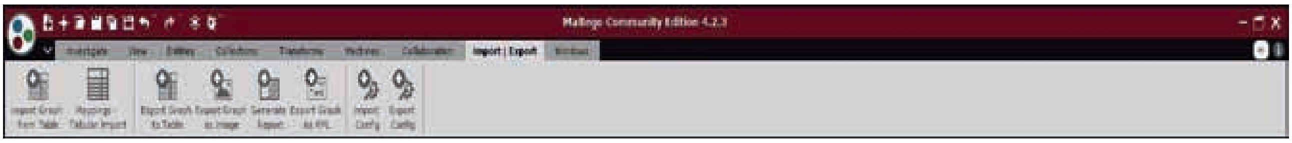


As an example we are going to performing reconnaissance on a company. Queries will be automatically done after you provide the domain name (domain of the company). This queries contain such functions as scanning any document belonging to the company, finding email addresses and socail media accounts etc.

Collaboration

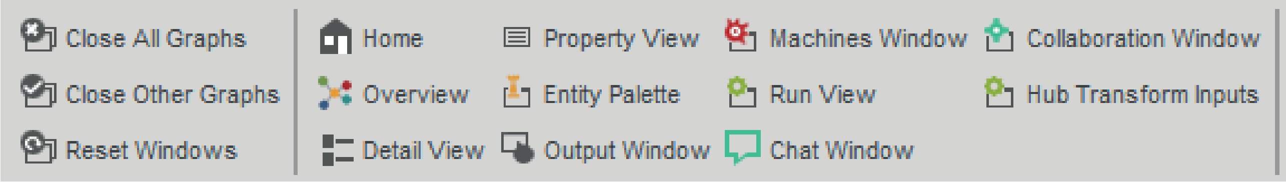
In this section, you can share the graphics, images, diagrams that you have created with someone else and discuss them on a chat window.

Import/Export



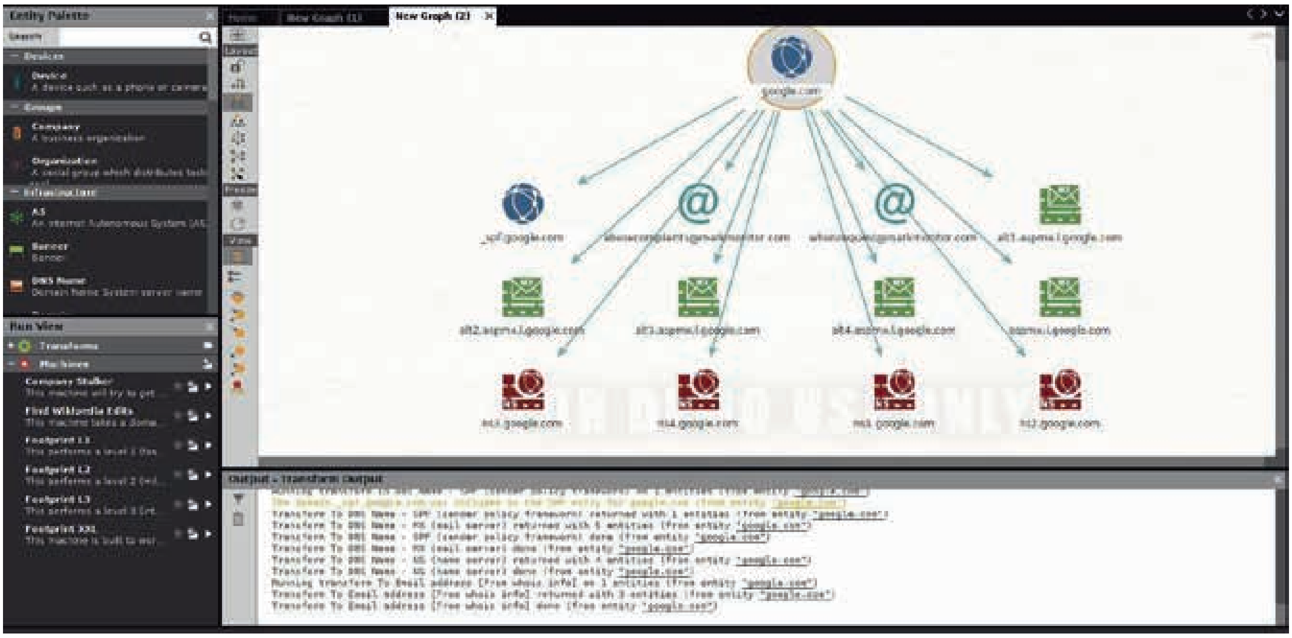
In this section, you can import/export the graphics of the investigation you made, can output the graph as a table or image and export it. Options are given to manage the reports.

Windows



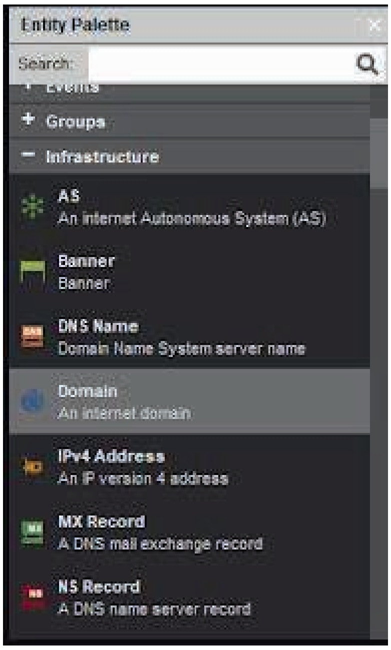
All editing functions of the program are available in the Windows section. Options such as *Close All Graphs*, and *Reset Windows* can be found here. You can manage as you wish.

Palette



```
Running transform To DNS Name - SPF (sender policy framework) on 1 entities (from entity "google.com")
The domain _spf.google.com was included in the SPF entry for google.com (from entity "google.com")
Transform To DNS Name - SPF (sender policy framework) returned with 1 entities (from entity "google.com")
Transform To DNS Name - MX (mail server) returned with 5 entities (from entity "google.com")
Transform To DNS Name - SPF (sender policy framework) done (from entity "google.com")
Transform To DNS Name - MX (mail server) done (from entity "google.com")
Transform To DNS Name - NS (name server) returned with 4 entities (from entity "google.com")
Transform To DNS Name - NS (name server) done (from entity "google.com")
Running transform To Email address [From whois info] on 1 entities (from entity "google.com")
Transform To Email address [From whois info] returned with 3 entities (from entity "google.com")
Transform To Email address [From whois info] done (from entity "google.com")
```

The *Palette* section works in a drag&drop fashion, contains many categories. Among these categories, the one that responds to the intelligence need is chosen and dropped to the white page in the middle. Let's collect information about a domain as an example.



AS
An internet Autonomous System (AS)

Banner
Banner

DNS Name
Domain Name System server name

Domain
An internet domain

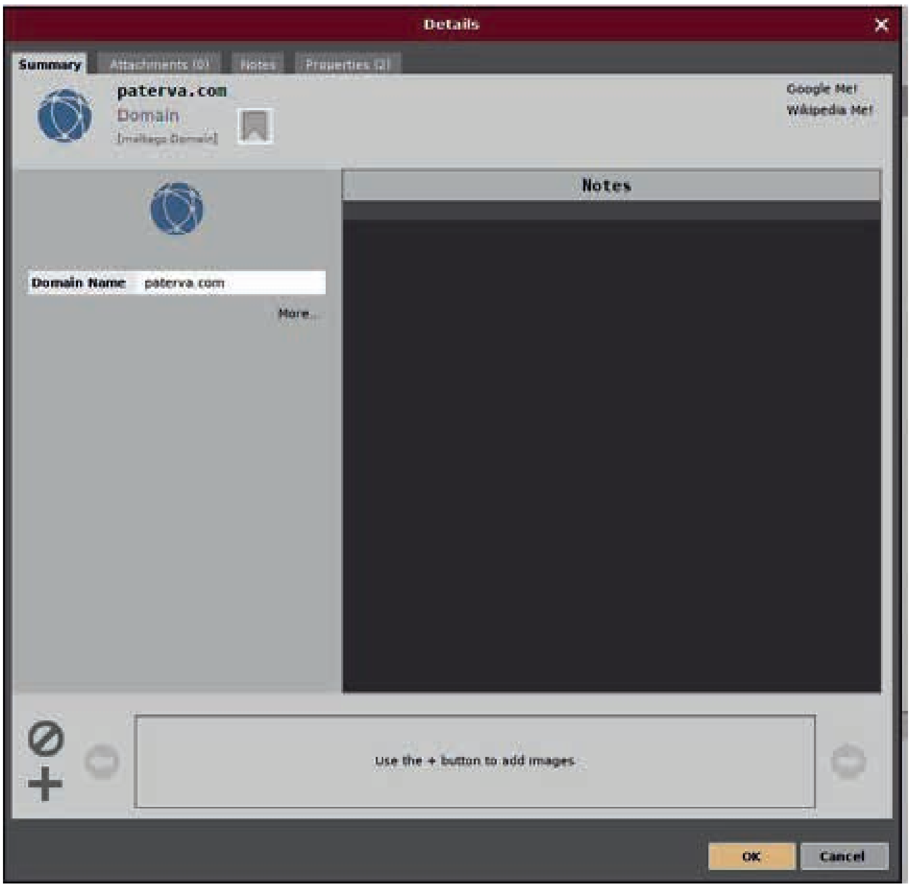
IPv4 Address
An IP version 4 address

MX Record
A DNS mail exchange record

NS Record
A DNS name server record

Let's select *Domain* in the *Infrastructure* section.

Drag and drop the Domain option into the blank page found on the right. After dropping, double-click and write the domain without the *www* at the beginning.

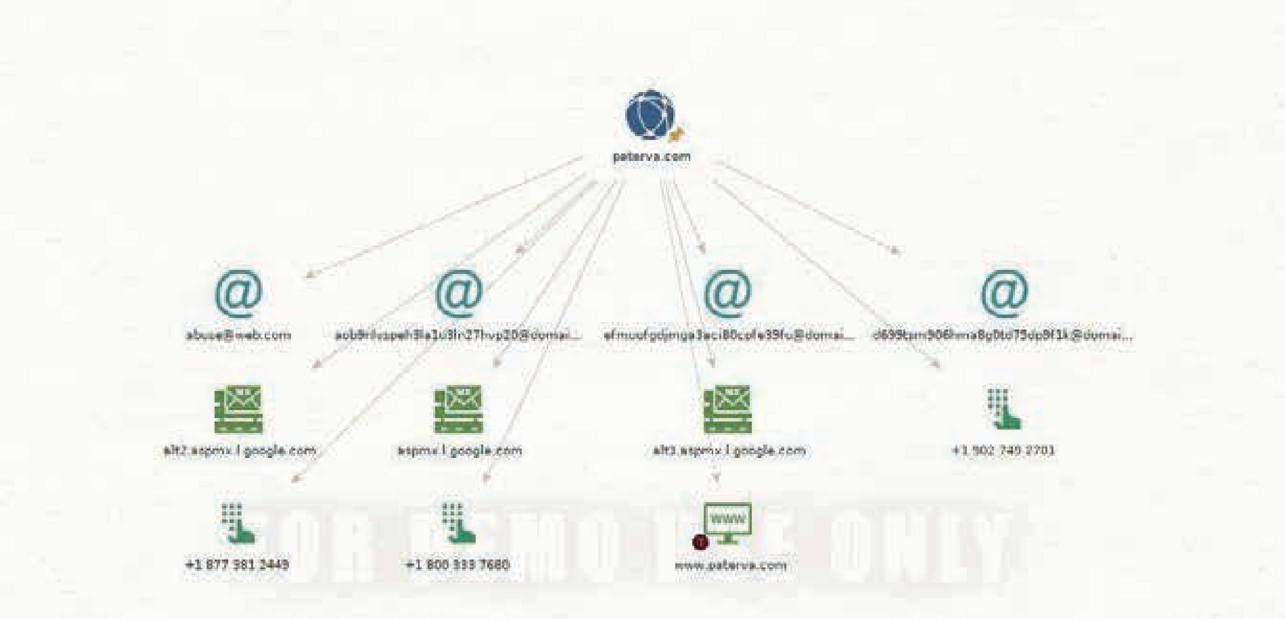


paterva.com
Domain
[maltego.Domain]

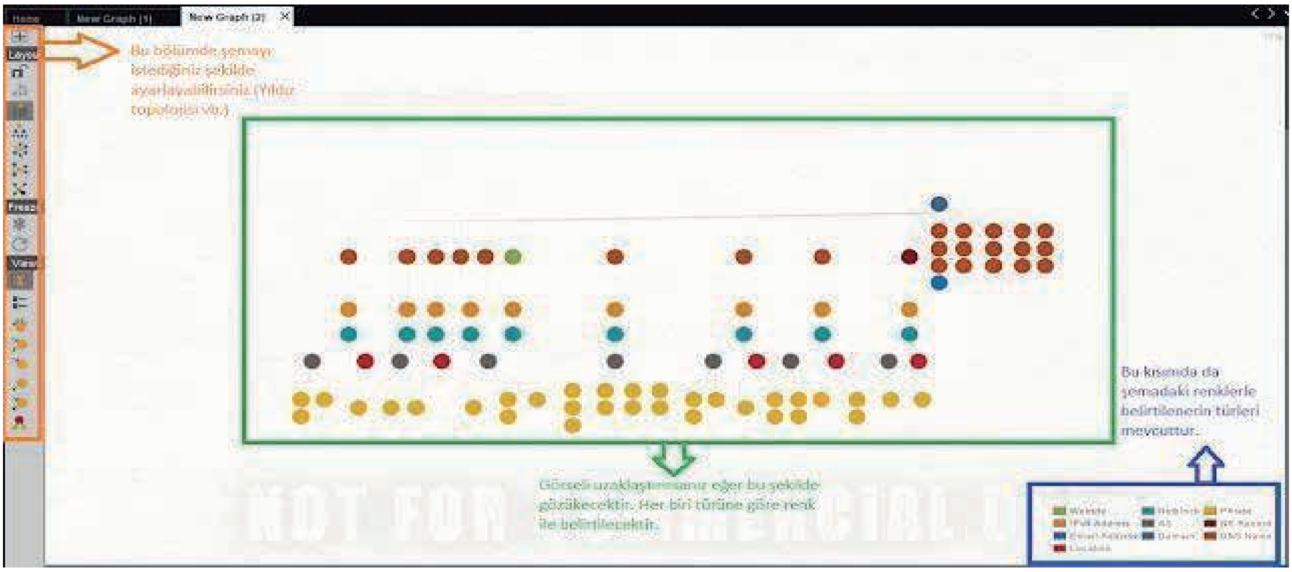
Domain Name: paterva.com

Then you can right-click the domain you want to query at the desired level, and perform the queries you want by right-clicking on the resulting subqueries.

The resulting image will be as follows:



On this images, you can work on the desired intelligence tool you want to gather information with. Thanks to Maltego, you can obtain information like the network architecture of the company, the domain addresses, email addresses and numbers of the employees and use these information to do social engineering or system pentesing through technical information.

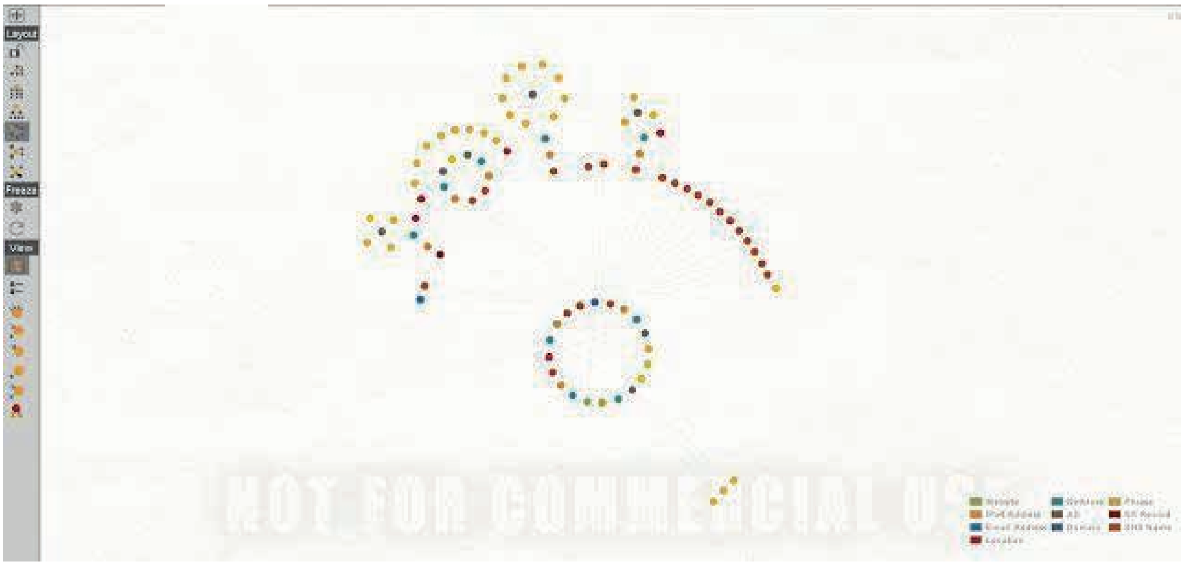


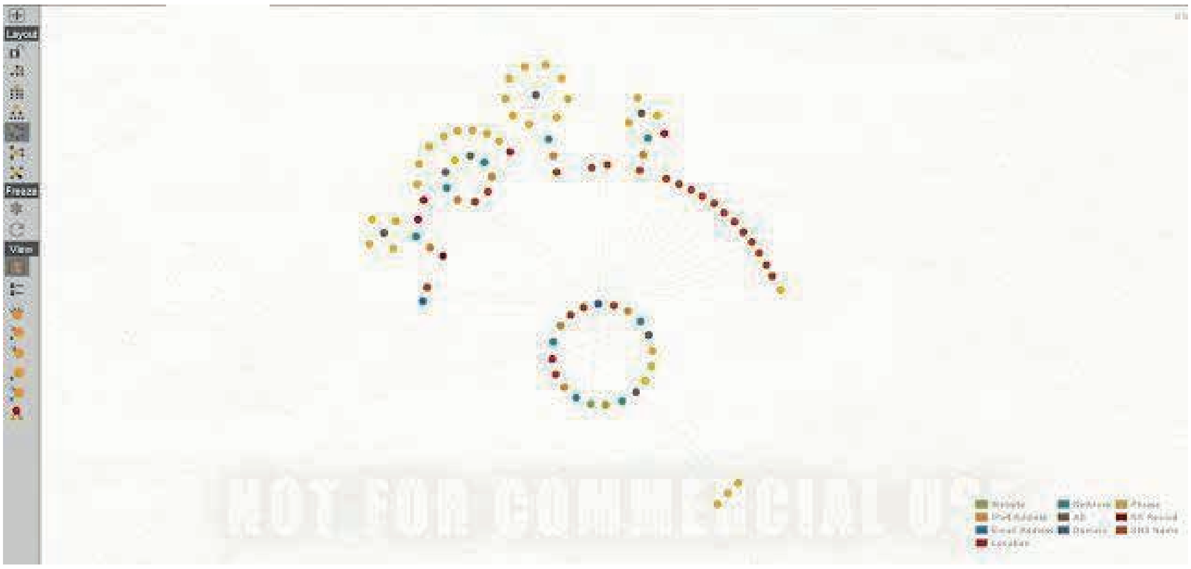
Bu bölümde şemayı isteğiniz şekilde ayarlayabilirsiniz (Yıldız topolojisi vb.)

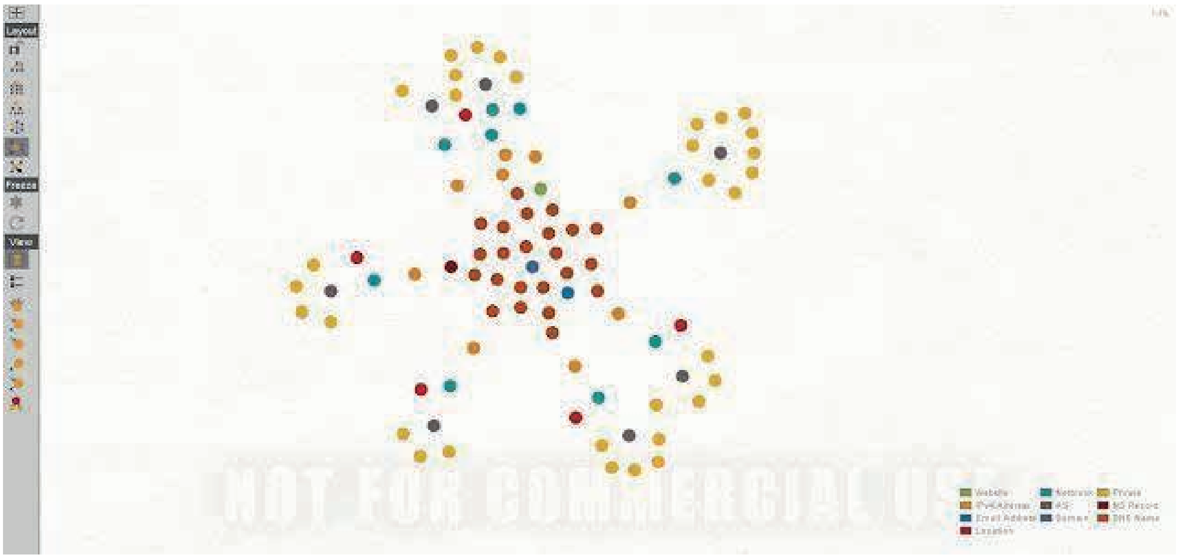
Görseli uzaklaştırırsanız eğer bu şekilde gözükecektir. Her biri türüne göre renk ile belirtilecektir.

Bu kısımda da şemadaki renklerle belirtilenerin türleri mevcuttur.

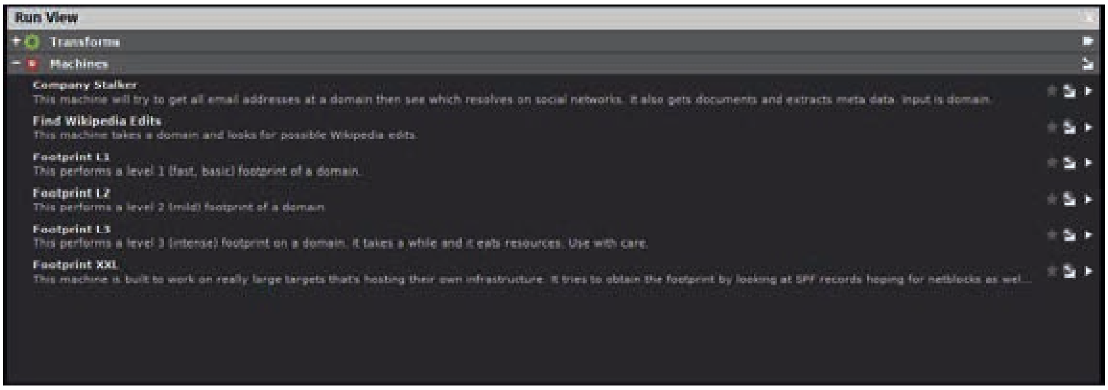
Other visualisation styles:


Layout
Freeze
View
NOT FOR COMMERCIAL USE
Website
IPv4 Address
Email Address
Location
Netblock
AS
Domain
Phone
NS Record
DNS Name


Layout
Freeze
View
NOT FOR COMMERCIAL USE
Website
IPv4 Address
Email Address
Location
Netblock
AS
Domain
Phone
NS Record
DNS Name


Layout
Freeze
View
NOT FOR COMMERCIAL USE
Website
IPv4 Address
Email Address
Location
Netblock
AS
Domain
Phone
MX Record
DNS Name

Run View



Company Stalker
This machine will try to get all email addresses at a domain then see which resolves on social networks. It also gets documents and extracts meta data. Input is domain.

Find Wikipedia Edits
This machine takes a domain and looks for possible Wikipedia edits.

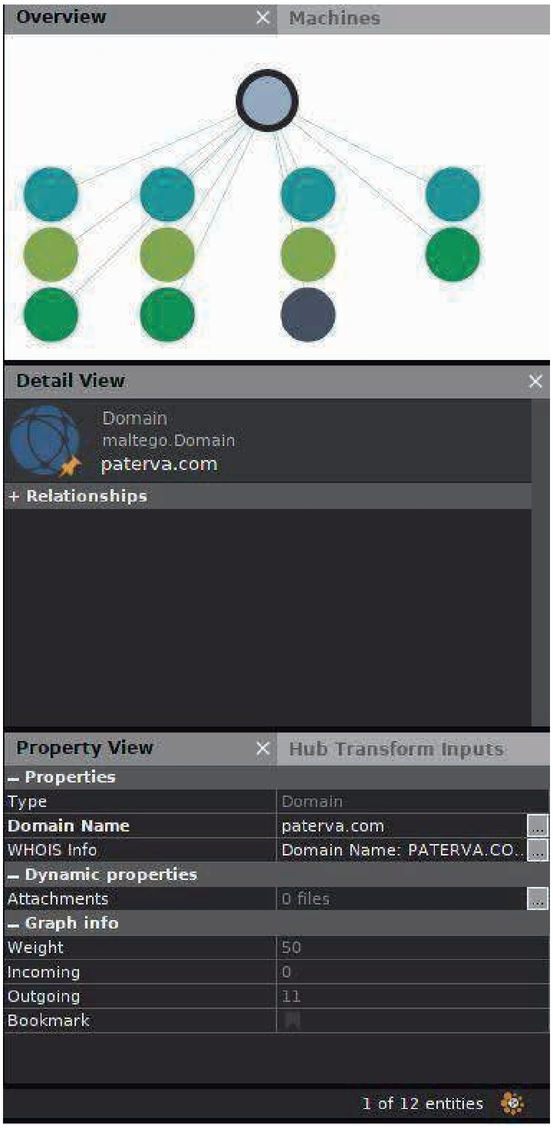
Footprint L1
This performs a level 1 (fast, basic) footprint of a domain.

Footprint L2
This performs a level 2 (mild) footprint of a domain.

Footprint L3
This performs a level 3 (intense) footprint on a domain. It takes a while and it eats resources. Use with care.

Footprint XXL
This machine is built to work on really large targets that's hosting their own infrastructure. It tries to obtain the footprint by looking at SPF records hoping for netblocks as wel...

In this section, you can adjust the performance at your desired level. You can use fast, detailed and wide search types.



Domain
maltego.Domain
paterva.com

– Properties
Type: Domain
Domain Name: paterva.com
WHOIS Info: Domain Name: PATERVA.CO...
– Dynamic properties
Attachments: 0 files
– Graph info
Weight: 50
Incoming: 0
Outgoing: 11
Bookmark

1 of 12 entities

The basic use of the Maltego tool is like this. The quality and method of the research may differ according to the purpose and the deepness of the research.

Ziyahan Albeniz • ziyahan@arkakapidergi.com

Hunting the bans in Fantasia – How to open a website in the TOR Network

So far, humanity has undergone many revolutions. We found the fire, tamed the animals and worked the soil. The scientific and industrial developments, the increase in soil fertility, can be classified as some of these revolutions. But the Internet, which met with the masses in the late 90s, was a completely different process in which all these revolutions were crowned.

After the revolution of the internet, sharing and producing information became unbelievably easy. It was easy to open a website and share knowledge and ideas with people on the other side of the world. States and technology giants work together and try tricking this environment where ideas sprout freely. They do sometimes succeed.

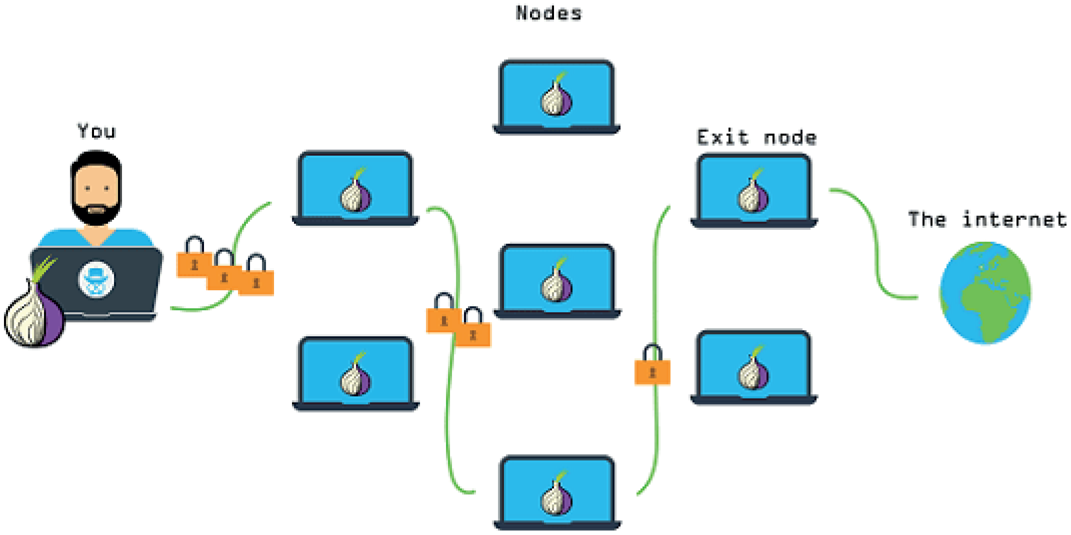
In a dystopian country which is called Fantasia, the situation is darker. It is now almost impossible to open a website without their permission. Even if you open a new one, it can be closed with a declaration in a short period of time.

You, as a service provider, and your visitors can be tracked step by step. In Fantasia and other repressive regimes in the world, you may be subject to various crimes due to the website you visit.

Put more generally, can the free-thinking, innovative citizens in Fantasia open a web site without fearing and asking the permission of an authority? Of course not! We are not at their mercy. All over the world, those loyal to the hacker culture find new ways to oppress the authorities.

One of them is the TOR Network and the Onion Services, which continue their lives with the support of volunteers. These services allow you to open websites independent of all authorities, subservient service providers and domain providers.

In this article, we will try to explain how to set up a website on the TOR Network.



Who wouldn't want to have a website on the TOR network?

In summary, the TOR network is a protocol that transmits internet packets over relay computers to hide the user's IP. The details of how this protocol's work is not the subject of this article.

However, the TOR article written by Muhammet Enes Özen in the 7th issue of Arka Kapı Magazine explains this issue with all its details. ("Stay Hidden on the Internet: The Onion Router.")

TOR has started its life as a browser add-on under the name of "TOR Button" in 2003 then continued its life as a browser.

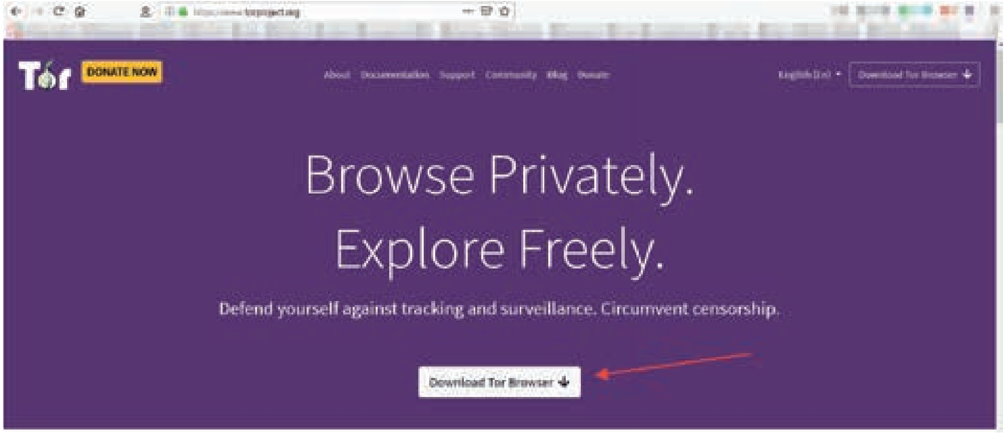
After 2004, TOR Services added a completely different service, called ONION Services. Apart from hiding the IPs of users, ONION Services also the website owners an opportunity to serve their own websites on the TOR network! In this way, without being condemned to neither domain providers nor hosting providers in the TOR network, you will be able to serve the website while maintaining your privacy.

This article is based on Windows since an average reader uses Windows OS as their operating system. Most of the instructions apply to * Nix operating systems.

ONION Services Details

In the following, we will use the term ONION Services for the web pages served through the TOR Network. In other words, having a website on TOR Network actually means starting an ONION Service on your computer.

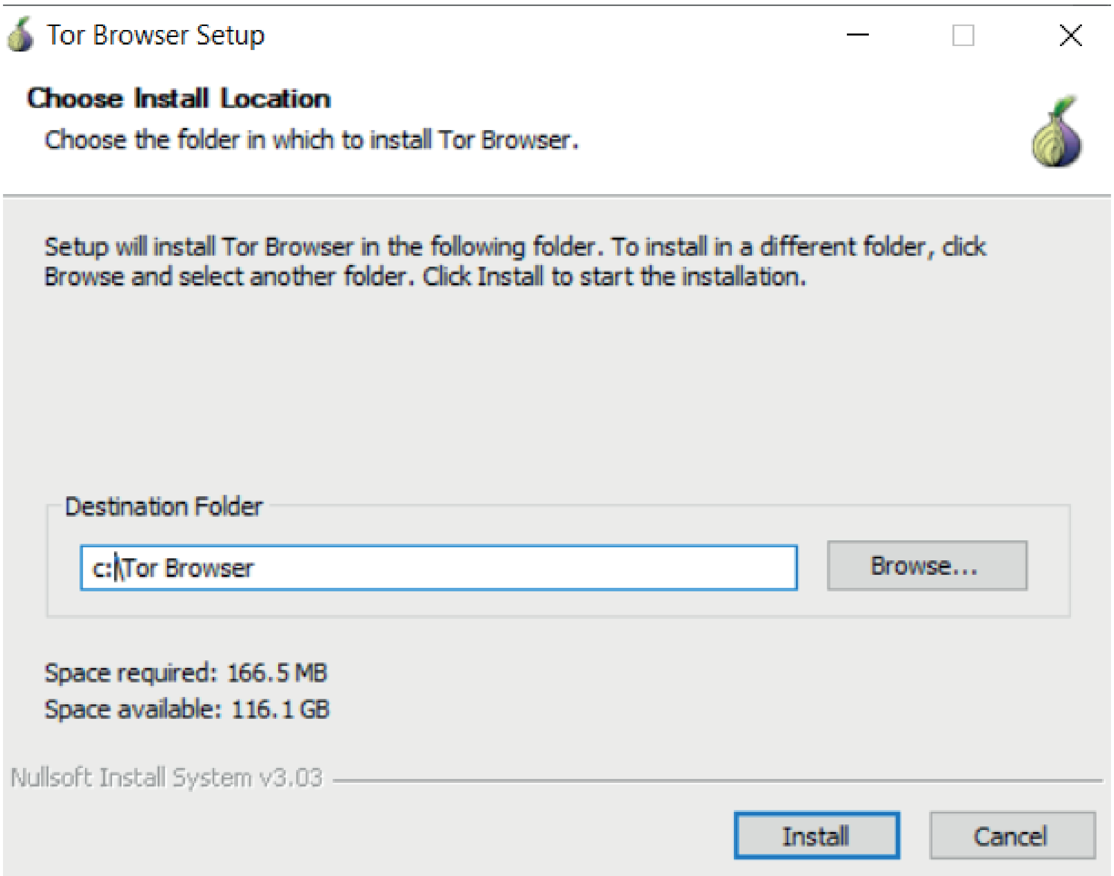
You can install the TOR Browser Bundle on your computer at www.torproject.org. Mozilla Firefox based TOR Browser and TOR service will be installed on your system.



Browse Privately.
Explore Freely.

Defend yourself against tracking and surveillance. Circumvent censorship.

After downloading the Tor Browser installation file, you can start the installation by clicking the corresponding file.



Tor Browser Setup

Choose Install Location

Choose the folder in which to install Tor Browser.

Setup will install Tor Browser in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

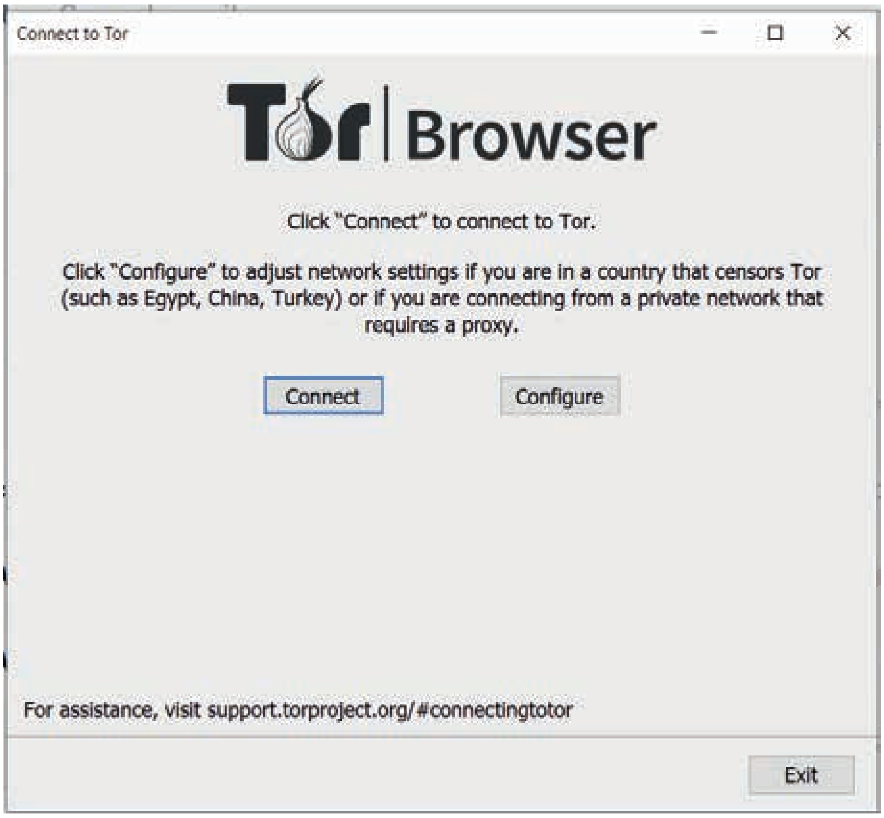
Destination Folder: c:\Tor Browser

Space required: 166.5 MB
Space available: 116.1 GB

Nullsoft Install System v3.03

I have chosen c:\Tor Browser as the path to install Tor Browser. We will also refer to this folder for further settings in this article.

When you open the TOR Browser after the installation is complete, a screen will appear for you to connect to the TOR Network.



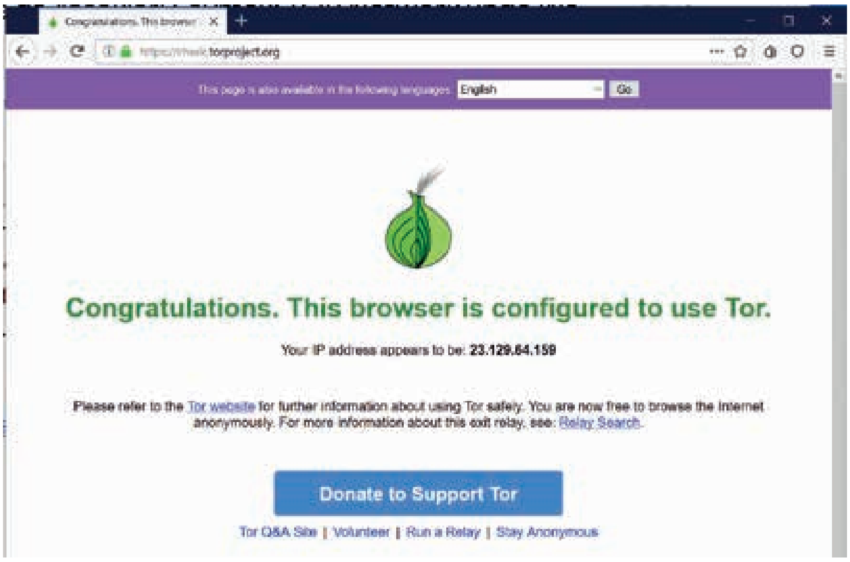
Click "Connect" to connect to Tor.

Click "Configure" to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.

For assistance, visit support.torproject.org/#connectingtotor

In this screen, you can choose to connect directly to TOR Network. If you live in countries like Fantasia, you can use the option to connect to the TOR Network via a Bridge by clicking Configure, probably because authorities have denied access to the TOR Network. Details are available in the article referred to at the beginning of this article.

Now that we're settled, we can visit https://check.torproject.org to test that our computer is properly connected to the TOR Network:



Congratulations. This browser
https://check.torproject.org
This page is also available in the following languages: English
Go

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: 23.129.64.159

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Relay Search.

Donate to Support Tor
Tor Q&A Site | Volunteer | Run a Relay | Stay Anonymous

Yeah! We can now move on.

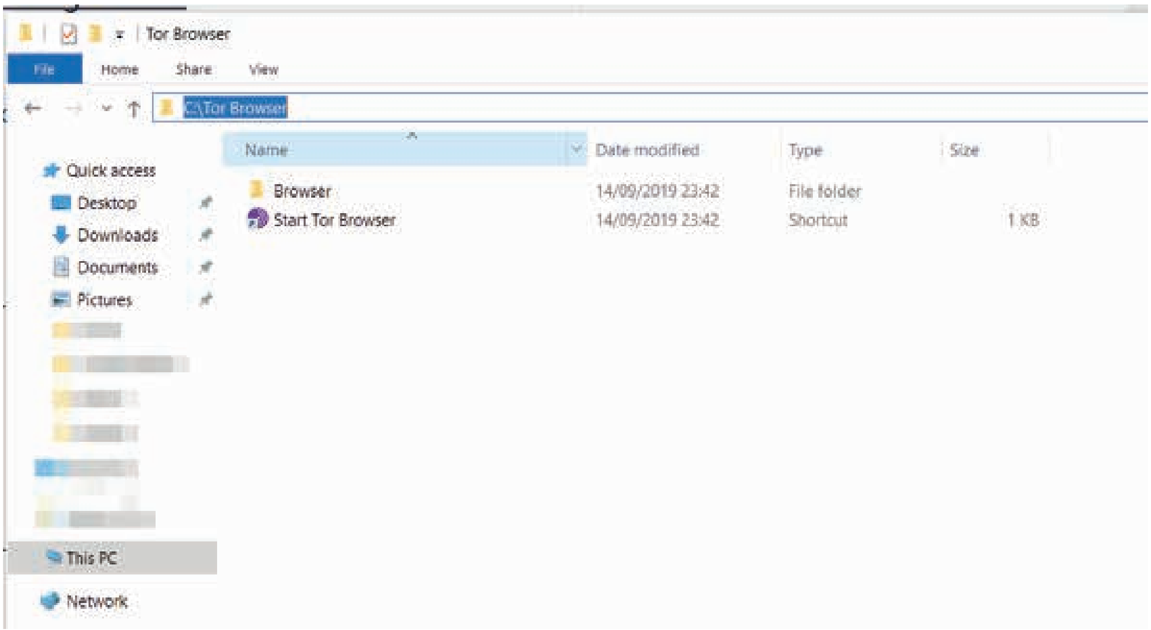
A Little Nuance in the TOR Browser

A careful reader will notice it. The access via TOR Browser is transferred to the destination only via the TOR Network. On other browsers, your web traffic arrives at the destination as it should, and your IP address is revealed.

Another issue is that if we publish a website on the TOR Network, the service must continue uninterruptedly. So should the TOR Browser always stay open?

Of course not! Now with a few small settings, we will convert the TOR service (installed on the TOR browser, but only starts when the browser is run) into a Windows service.

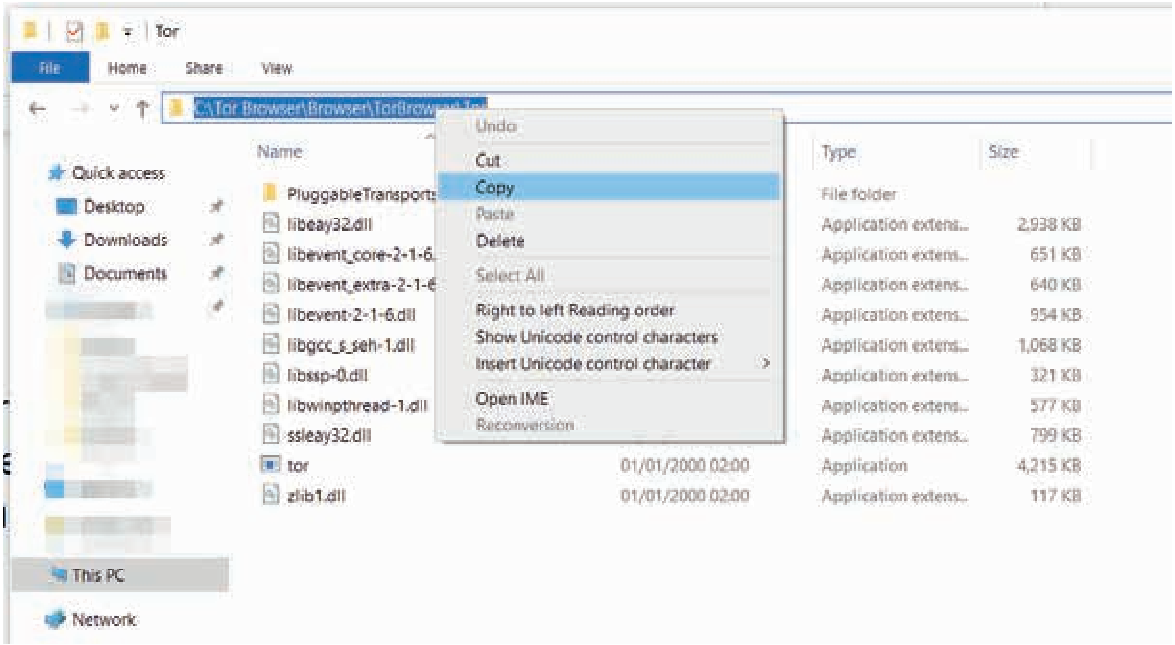
If you remember, we mentioned that TOR Browser should be copied to c:\Tor Browser. Now let's go to this directory:



C:\Tor Browser

Name	Date modified	Type	Size
Browser	14/09/2019 23:42	File folder	
Start Tor Browser	14/09/2019 23:42	Shortcut	1 KB

Enter Browser\Tor Browser\Tor directory in this directory and copy the directory path:



C:\Tor Browser\Browser\TorBrowser\Tor

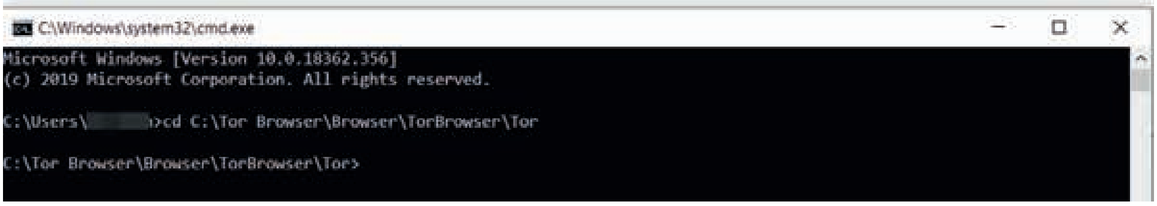
Name	Date modified	Type	Size
PluggableTransports		File folder	
libeay32.dll		Application extens...	2,938 KB
libevent_core-2-1-6.		Application extens...	651 KB
libevent_extra-2-1-6		Application extens...	640 KB
libevent-2-1-6.dll		Application extens...	954 KB
libgcc_s_seh-1.dll		Application extens...	1,068 KB
libssp-0.dll		Application extens...	321 KB
libwinpthread-1.dll		Application extens...	577 KB
ssleay32.dll		Application extens...	799 KB
tor	01/01/2000 02:00	Application	4,215 KB
zlib1.dll	01/01/2000 02:00	Application extens...	117 KB

Now we are going to open the Windows Command Prompt and change the current directory.

Type *cmd* in Start> Run and press enter. You will see the Windows Command Prompt on a black screen.

By typing `cd C:\Tor Browser\Browser\TorBrowser\Tor`

Let's enter the directory:

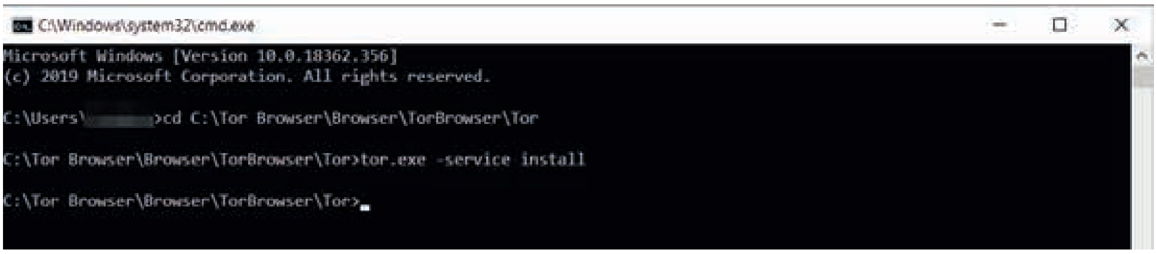


```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>cd C:\Tor Browser\Browser\TorBrowser\Tor

C:\Tor Browser\Browser\TorBrowser\Tor>
```

We will now instruct the tor.exe program to start as a Windows service on every operating system startup. This way, you can send the Internet traffic of any program via Tor Network, whether or not Tor Browser is open.

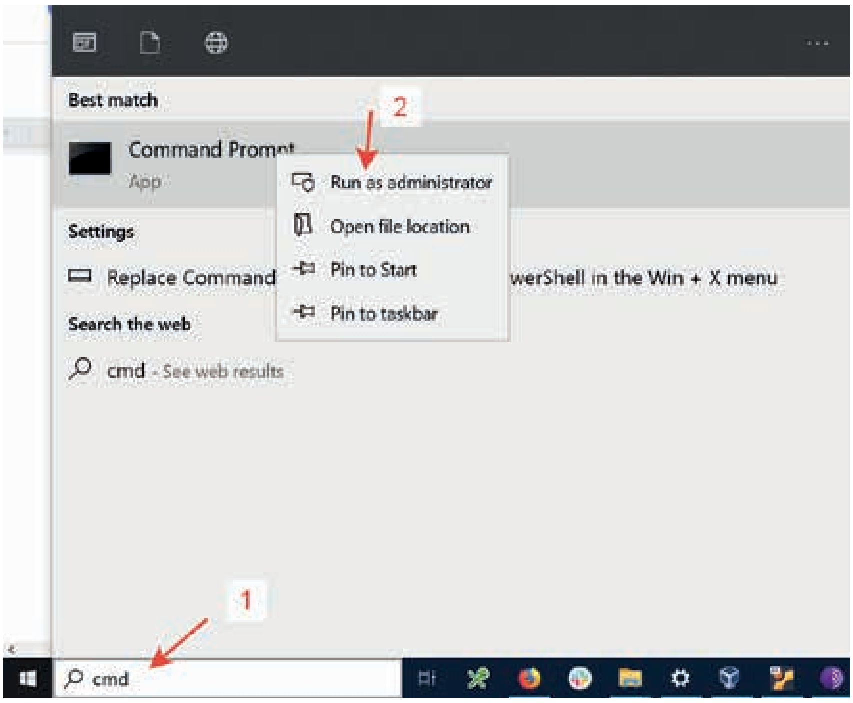
Our command:

```
tor.exe -service install
```



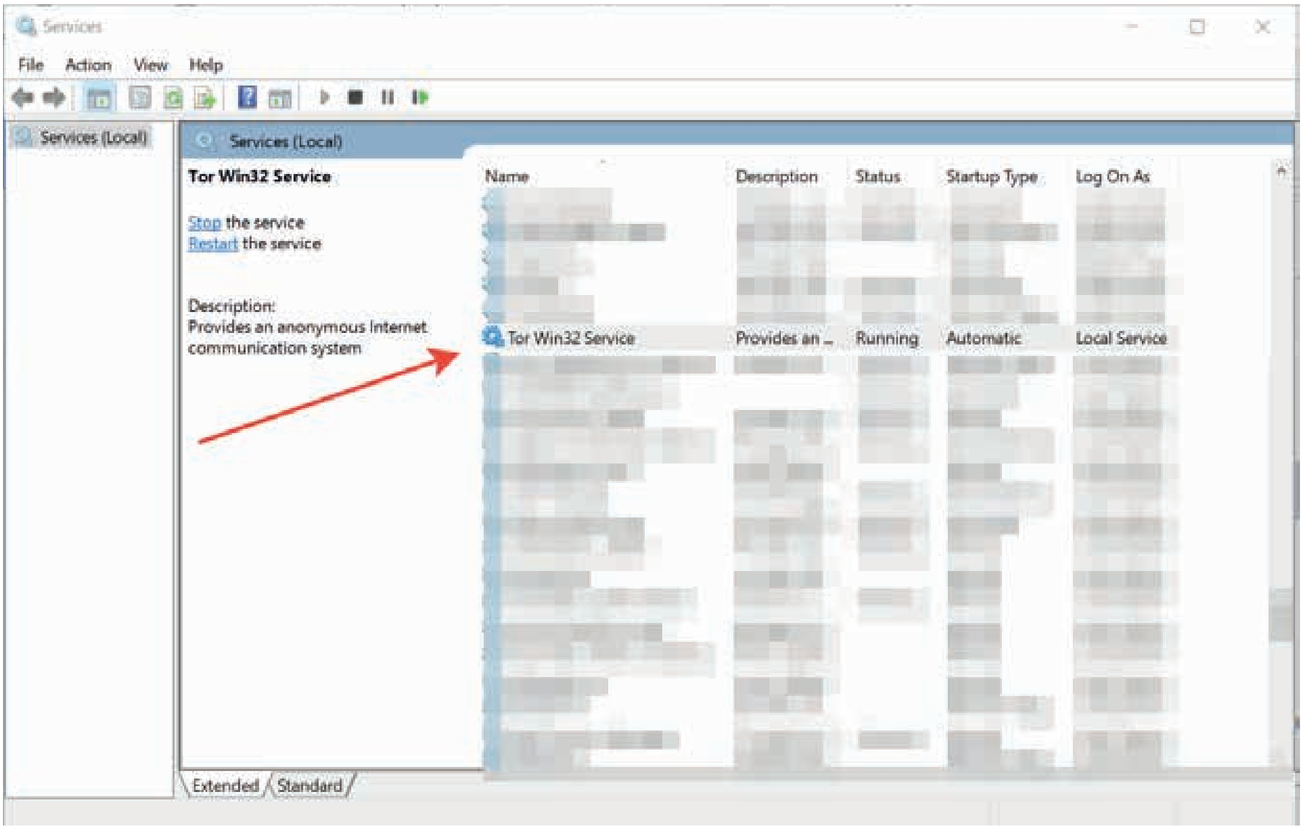
```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>cd C:\Tor Browser\Browser\TorBrowser\Tor

C:\Tor Browser\Browser\TorBrowser\Tor>tor.exe -service install

C:\Tor Browser\Browser\TorBrowser\Tor>_
```

Note: the command will not work if the account you are currently using does not have administrator privileges on the Windows operating system. If you will open Windows Command Prompt with administrator privileges then you can repeat the same process:



The application called tor.exe is now available as a Windows service. You can verify the result by taking a look at the Windows services:

By typing `services.msc` on the `Start> Run` screen, you can access the list of all services in Windows and check for the entry Tor Win32 Service in the list:



Tor Win32 Service

Stop the service
Restart the service

Description:
Provides an anonymous Internet communication system

Name	Description	Status	Startup Type	Log On As
Tor Win32 Service	Provides an ...	Running	Automatic	Local Service

You can now browse websites through the TOR Network without having to open the TOR Browser, by entering `127.0.0.1` port `9150` of SOCKS5 type from any browser's proxy settings. After that, I suggest you visit `https://check.torproject.org` to verify that the traffic flows through the TOR network.

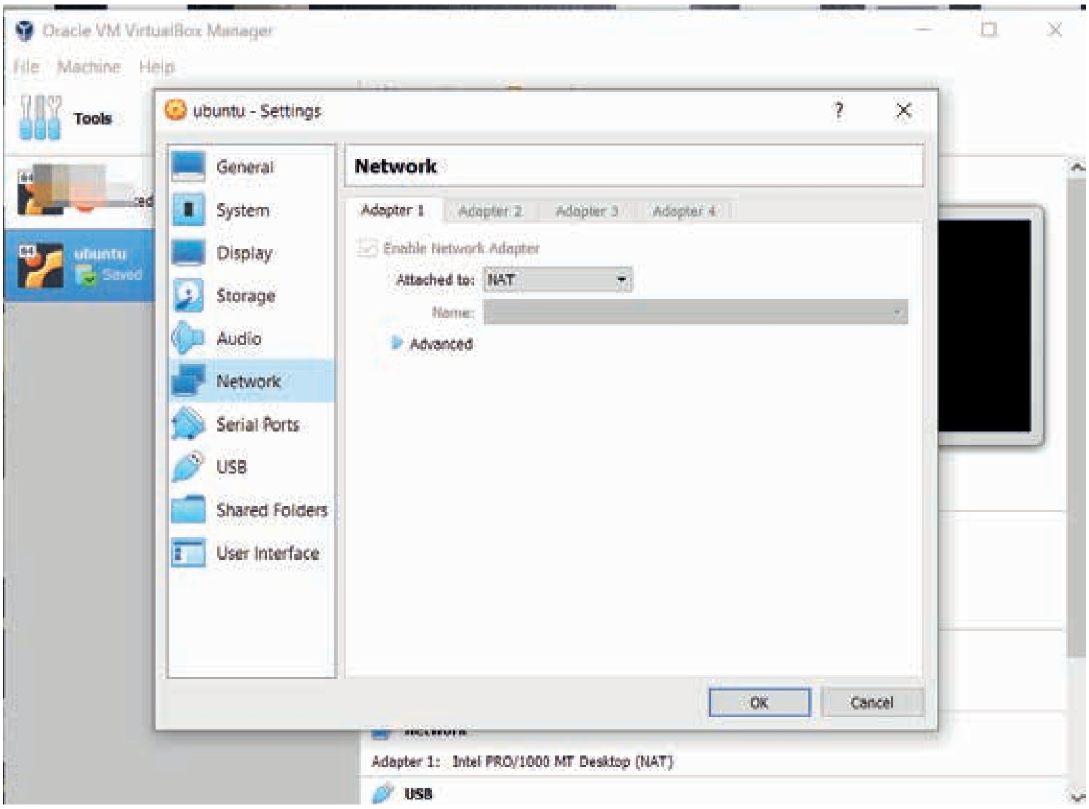
We have completed the first stage. We can now look at the ONION Services.

Preparing the Server

We said that we'd have a website and we will host our website ourselves.

I will use a machine on VirtualBox as the virtualization software.

I have set up a Ubuntu machine configured with NAT as the network setting. So this virtual machine can only be accessed through the host machine (my machine). Any external request will be closed.



☑ Enable Network Adapter

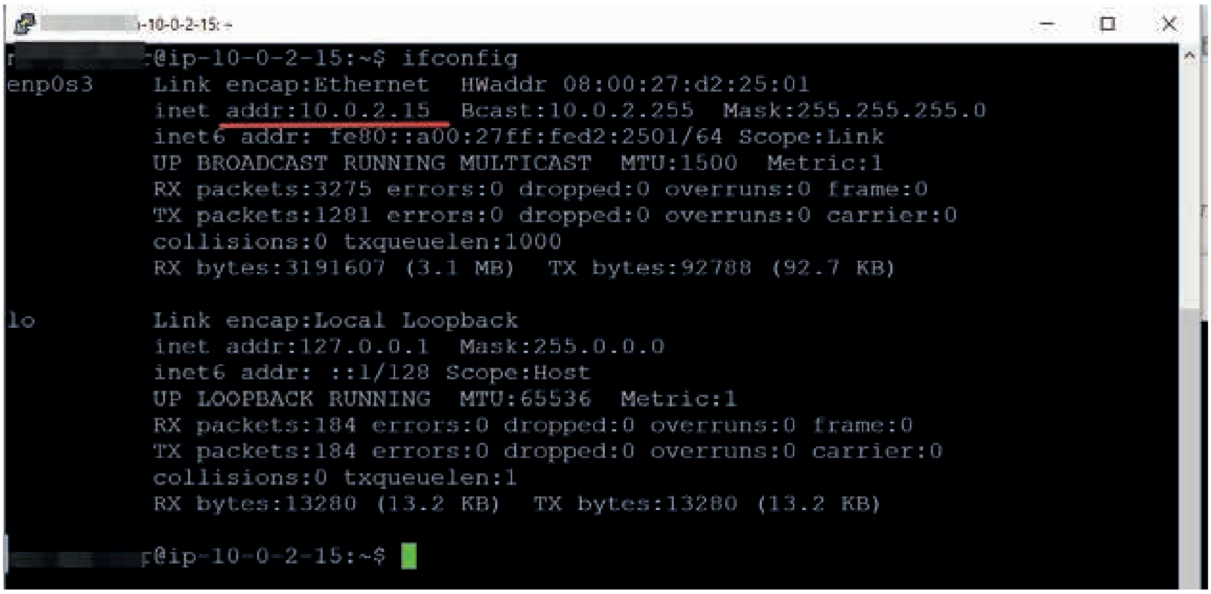
Attached to: NAT

Name:

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

I have used Nginx as a Web Server (www.nginx.com). As a matter of fact, Nginx is one of the recommended server software on TOR's website for ONION service operators.

As it can be seen from the screenshot below, my server uses the 10.0.2.15 IP address behind NAT:



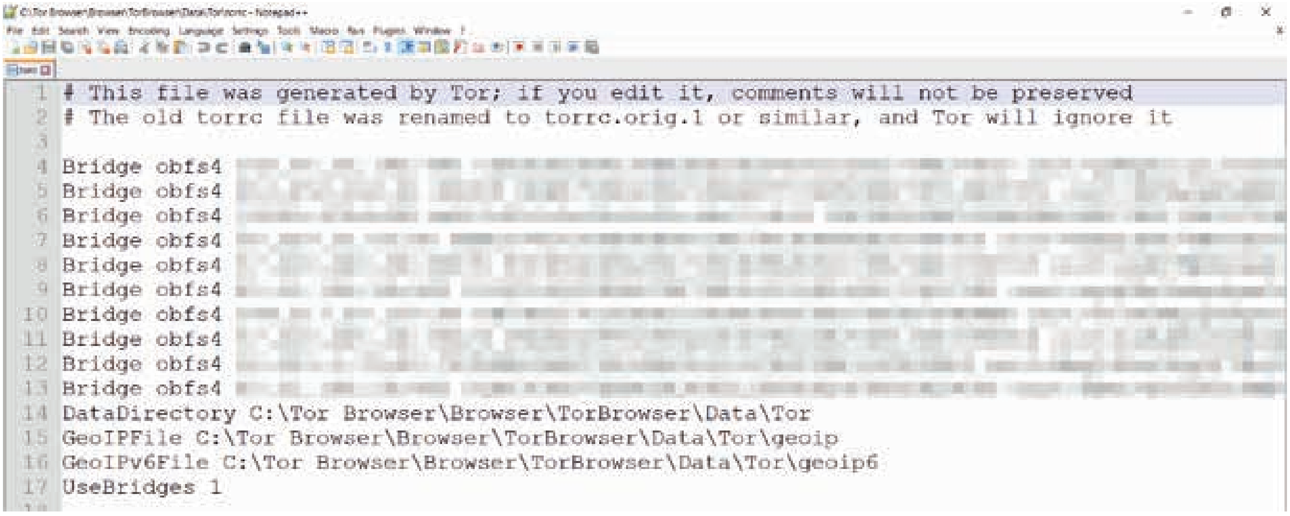
```
[redacted]-10-0-2-15: ~
[redacted]@ip-10-0-2-15:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:d2:25:01
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed2:2501/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1281 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3191607 (3.1 MB)  TX bytes:92788 (92.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:13280 (13.2 KB)  TX bytes:13280 (13.2 KB)

[redacted]@ip-10-0-2-15:~$
```

Now let's go to our ONION Service settings.

torrc: You Rock!

torrc is a configuration file that TOR uses. We will also state that we want to start an ONION service via this configuration file.

You can use the path `C:\Tor Browser\Browser\TorBrowser\Data\Tor` to access the torrc file, and view it with any text editor:



```
# This file was generated by Tor; if you edit it, comments will not be preserved
# The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it

Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
Bridge obfs4 [redacted]
DataDirectory C:\Tor Browser\Browser\TorBrowser\Data\Tor
GeoIPFile C:\Tor Browser\Browser\TorBrowser\Data\Tor\geoip
GeoIPv6File C:\Tor Browser\Browser\TorBrowser\Data\Tor\geoip6
UseBridges 1
```

The way to say that "we want to use an ONION service in TOR" is to add the following lines to this file:

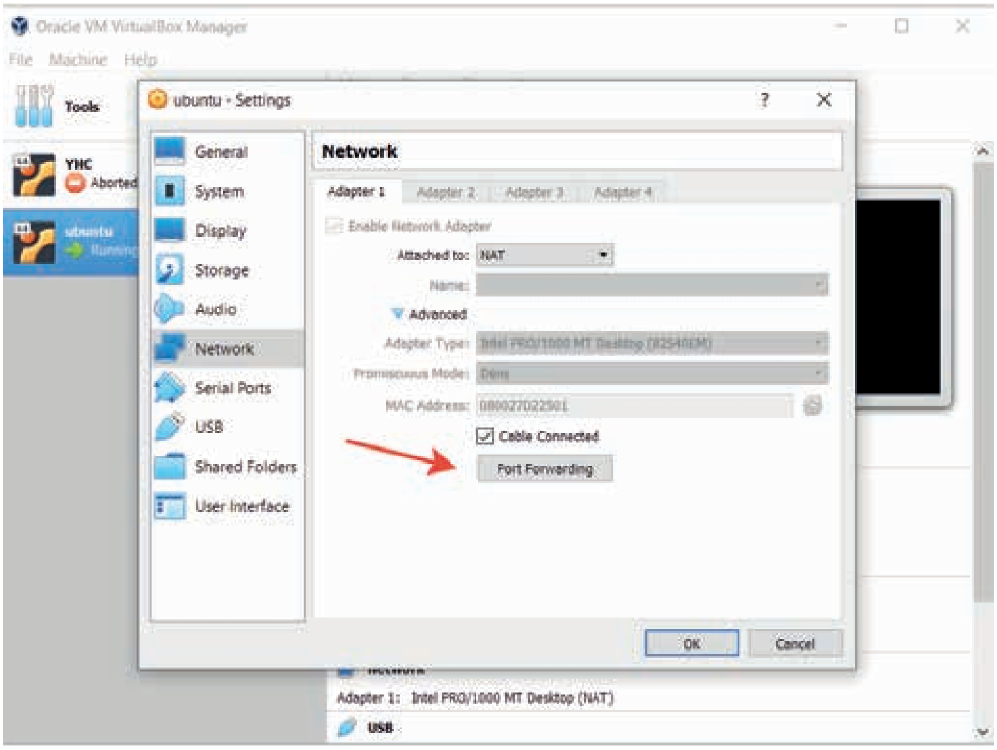
```
HiddenServiceDir C:\my_onion_service
HiddenServicePort 2023 127.0.0.1:2023
HiddenServiceVersion 2
```

What do all of this mean?

The directory *HiddenServiceDir* is all of the settings and address for the service started are found. This directory is very important.

With the HiddenServicePort instruction, we tell TOR to listen to the port 2023 and forward the requests to port 2023 at 127.0.0.1.

Our server was so-called in the virtual machine. We will now make a small setting to routing the requests that come to 127.0.0.1's 2023 port, i.e., the loopback address, to port 2023 of 10.0.2.15 behind NAT. This setting consists of defining a port forwarding to our virtual machine via VirtualBox. In VirtualBox, we will perform this operation from the networking settings of the respective virtual machine:



Network

Enable Network Adapter

Attached to: NAT

Name:

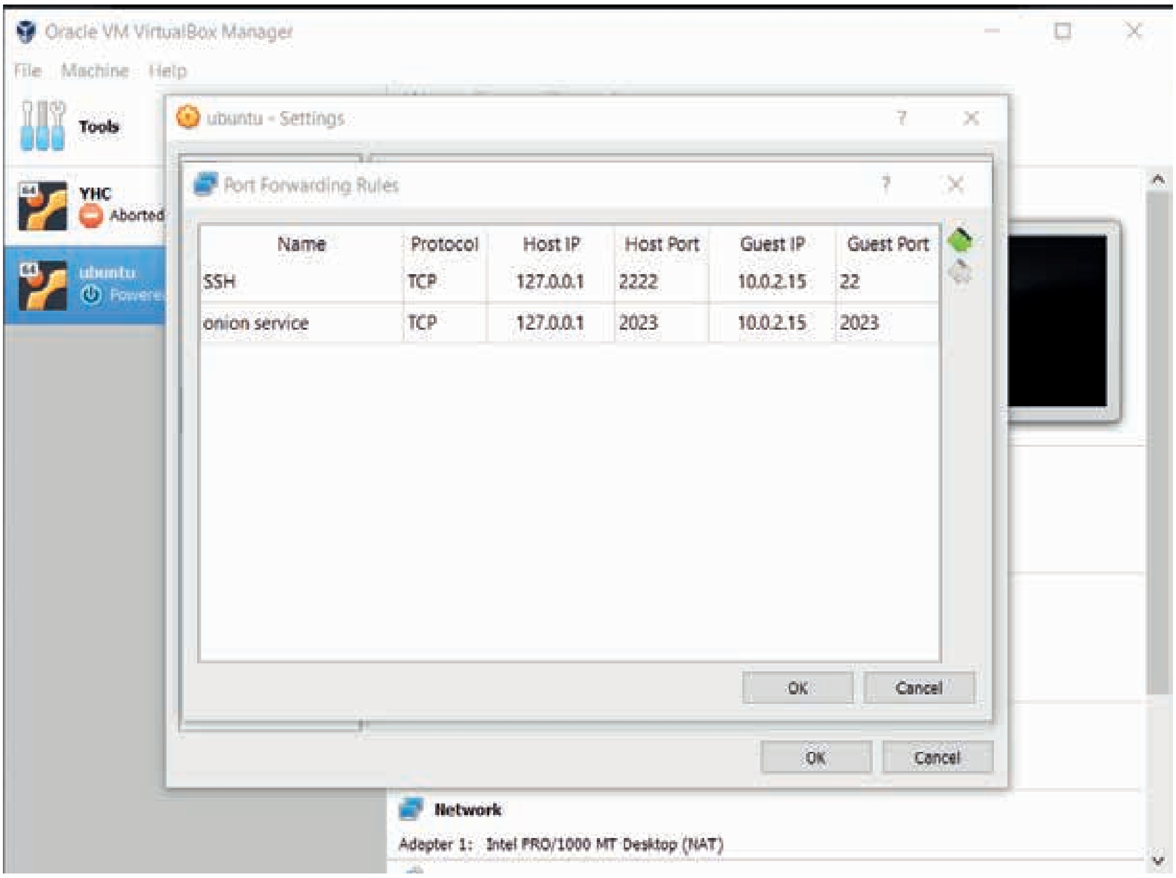
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027D22501

☑ Cable Connected

Adapter 1: Intel PRO/1000 MT Desktop (NAT)



Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
SSH	TCP	127.0.0.1	2222	10.0.2.15	22
onion service	TCP	127.0.0.1	2023	10.0.2.15	2023

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

You must restart your virtual machine after applying these settings.

Now we have to make a configuration on our Nginx server to listen on port 2023. In addition, we need to know the address of our website. With the address, we will make Nginx's *server name* setting so that it only responses to the requests that come with that specific Host information.

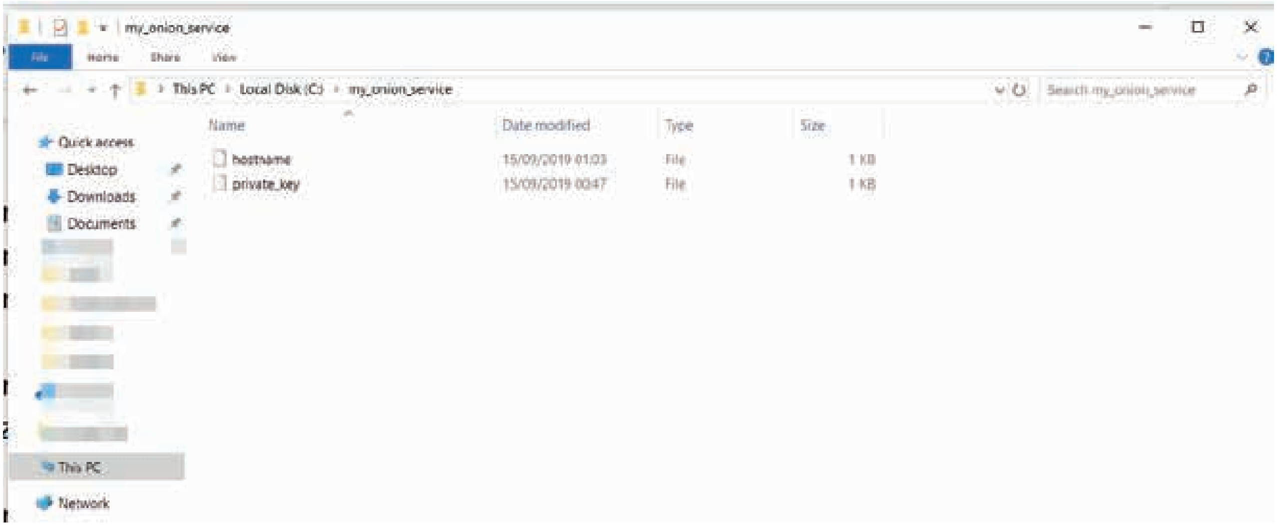
What is my website address?

Earlier, we added three lines to the torrc file:

```
HiddenServiceDir C:\my_onion_service
HiddenServicePort 2023 127.0.0.1:2023
HiddenServiceVersion 2
```

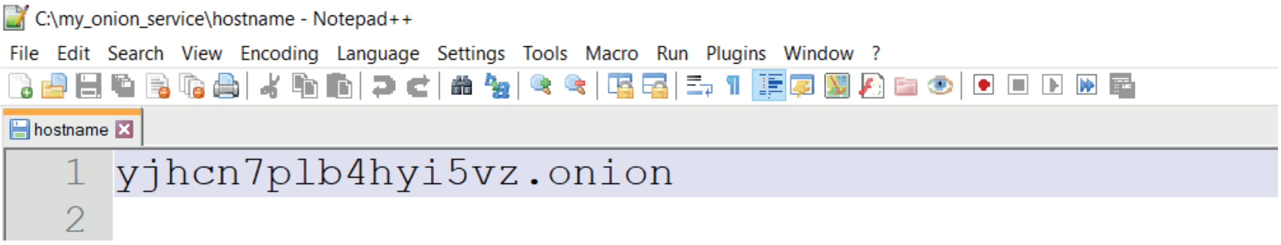
`HiddenServiceDir` directory is a critical directory. We will learn the domain name assigned by Onion Service to our website.

`HiddenServiceDir` directory contains two files: hostname and privatekey



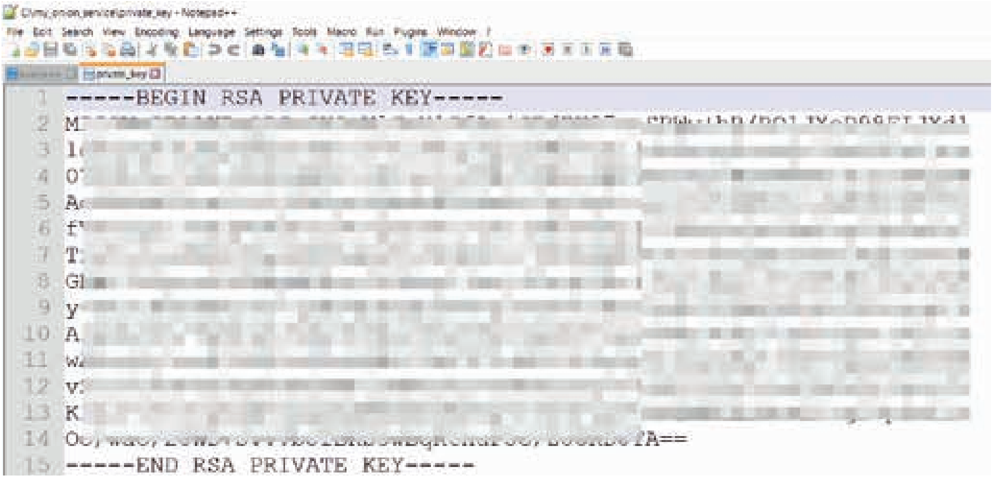
Name	Date modified	Type	Size
hostname	15/09/2019 01:03	File	1 KB
private_key	15/09/2019 00:47	File	1 KB

These files were prepared when the Tor service was started according to the information in the torrc file. The hostname file contains a piece of surprise information; the address of our website:



```
yjhcn7plb4hyi5vz.onion
```

yjhcn7plb4hyi5vz.onion! What the hell is this address? This address was created by using the private_key (the private_key of the end-to-end encryption used to access the website.) in the same directory.


C:\my_onion_service\private_key - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
private_key

```
-----BEGIN RSA PRIVATE KEY-----
[redacted]
-----END RSA PRIVATE KEY-----
```

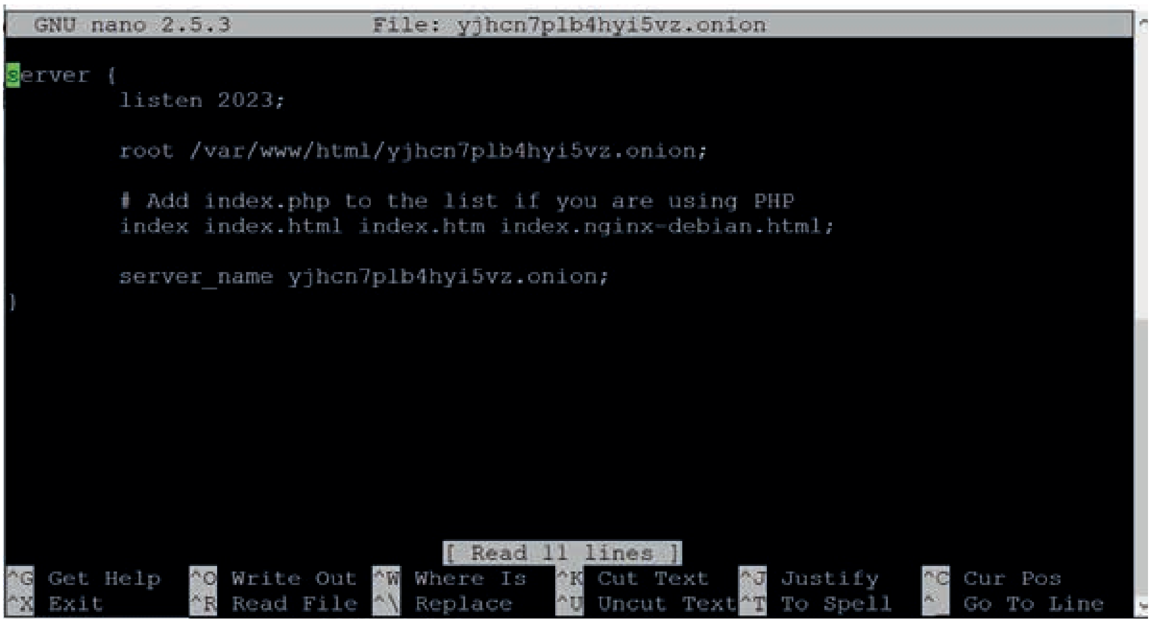
The TOR service first took the SHA1 hash of the public key extracted from the private key. The first 80 bits of this summary were encoded using base32 encoding and a 16-character address was reached.

The mechanism here is beautifully designed. Since your domain name is directly associated with the public key, you are using a self-signed certificate over some kind of domain name.

Let me give a further explanation for those disliking the hash algorithm SHA1: in Version 3 (prepared using Version 2) of this Onion Service, more powerful algorithms and longer addresses await you. Details can be found on TOR's website.

Now that we know the address of our website, everything is ready for us to configure our Nginx server!

We create a file which will hold our website name under **/etc/nginx/sites-available: yjhcn7plb4hyi5vz.onion**



```
  GNU nano 2.5.3            File: yjhcn7plb4hyi5vz.onion

server {
        listen 2023;

        root /var/www/html/yjhcn7plb4hyi5vz.onion;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;

        server_name yjhcn7plb4hyi5vz.onion;
}
```

[Read 11 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

Now we need to move this file to the folder named `sites-enabled:`

```
sudo cp yjhcn7plb4hyi5vz.onion ../sites-enabled/
```

Remember to restart the Nginx server after the settings:

```
/etc/init.d/nginx restart
```

Our website can be accessed at yjhcn7plb4hyi5vz.onion using the TOR Browser!

Now let's move on to some questions.

Can I have a better domain name?

Yes, it is possible to have a more legible domain, which is called a vanity domain in the TOR literature. For example, Facebook's Onion Service address is facebookcorewwwi.onion

At the beginning of the article, we mentioned that the Onion Service domain name is a process that starts with taking the SHA1 summary of the public key extracted from the private key.

If you have a powerful CPU, you can generate RSA key pairs, get the SHA1 hash, then encode with base32, and check if the first 16 characters contain the domain name you want.

There are also sites that offer this as a service. However, I personally would not recommend the use of these sites. Because you will transfer the process of generating the private key-public key value pair, which is vital for your site, to someone else. Thus someone with these keys can gain ownership of your domain.

The fact that your system is accessible depends on hosting, i.e, depends on the computer on which you host the website files standing and online. Unlike other sites, the TOR service must also be started.

Through Onion Services, you can not only access other SSH but also the services behind NAT.

Onion Services offer many useful features. I strongly recommend that you look at version 3. In addition, the matter of security exceeds the limits of this article. Running the website on an isolated machine is one of the most important steps. But this step alone is not enough. You should also definitely check the documentation on server security such as doing the necessary configurations to prevent the disclosure of the server information in the HTTP response.

How someone can find my domain?

You can register your website with directory services such as The Hidden Wiki, which is one of the first stops of TOR Network.

Will my website with .onion extension be accessible by normal browsers?

The answer is both yes and no. At the beginning of the article, we talked about how TOR can be started as an independent service in the operating system. If the browser is set to TOR as a Proxy via SOCK, it can access your site.

But in many cases, even if the TOR Network is used to access websites, the operating system will refer to the DNS servers of your ISP, that is, your service provider for address resolution, a.k.a DNS Leak. Unfortunately, these DNS servers will not be able to resolve domains with the extension .onion, and the information about which site you want to access will be disclosed.

When more people use TOR, or even use the TOR Browser for this job, such possibilities will not be a problem.

Hope that this article contributes to the idea of free thought and knowledge production.

Knowledge is power!

CALL FOR PAPERS

ARKA KAPI

Do you want your article to be published on Arka Kapi Magazine? Submit now to be featured in the next issue! Your article can be of any title as long as it fits to the cyber security context. Make sure it's an original article that isn't previously published elsewhere.

Email your articles to:
editor@arkakapimag.com

FEEDBACK

Got any feedback about Arka Kapi Magazine? Found a bug? Want us to add or remove something? Let us know!

follow us

Don't miss the news!

arkakapimag