OSINT

Prepared By: Belan Rzgar & Payam Fayaq

Supervised and Editor: Bilal H Ali

Outline

- What is ISR?
- Types ISR?
- What Is OSINT?
- OSINT Cycle
- Advantages and disadvantages of OSINT
- Security Threats of OSINT
- Role of OSINT from cybersecurity perspective
- how hackers are using OSINT in their work
- Types of OSINT Data Used in Cyberattacks
- What types of OSINT do we have?
- OSINT Gathering Tactics
- The Best OSINT Tools
- Challenges of OSINT

What Is ISR?

- ❑ The amount of information collected by countries is called Intelligent Surveillance and Reconnaissance (ISR).

- ❑ Information collection methods like ISR are of three types:

  1. Open Source intelligence OSINT,
  2. human intelligence (HUMINT)
  3. technical intelligence (TECHINT).

✓ OSINT is the most basic method of collecting information, which is a form of collecting data through open sources (internet, broadcasting, papers, etc.) and processing them. As open information is used, there are advantages, e.g., the information is collected in real-time, and the data are accessed easily and collected at a low cost. However, the importance of the information is lower than that of other information collection methods.

What Is ISR?

- ✓ HUMINT indicates that humans extract or steal information. Simply, it refers to spies or secret agents. It has the advantage of obtaining high-quality information like first-class confidential information, however, there always exists a risk of betrayal and double espionage because people are involved.

- ✓ TECHINT emerged as an information collection method that uses technology and information assets to gather enemy intelligence. Here, the technology and information assets refer to devices that have the latest technologies for collecting information, such as imagery intelligence (IMINT) and signals intelligence (SIGINT). Its disadvantages are that the costs are high, and the reliability of the acquired information is low when a problem occurs in signals and radio waves.

OSINT?

Each of the three information collection methods has advantages and disadvantages, depending on the environment. In this chapter, we examine and explain OSINT, which is the basis for information-gathering methods. Currently, all users use OSINT technology when searching for data online. On this basis, users obtain information about the data they are looking for. However, from the perspective of cybersecurity, the use of data gathered by OSINT is a double-edged sword.

- ✓ (i) On the positive side, data gathered by OSINT can be used as a means of resolving cybersecurity threats, which can track down cybercriminals or prevent cyberattacks before occurring.
- ✓ (ii) On the negative side, data gathered by OSINT becomes the basis for attackers to create cybersecurity threats. In other words, an attacker can set a target to attack based on data, and after gathering related information, they can engage in various cybercrimes, such as hacking, malware, and denial-of-service (DoS) attacks .

What Is OSINT?

- OSINT is the acronym for Open Source Intelligence.
- It's a type of intelligence tool used to collect public data for various purposes.
- The open, or public, part of OSINT means there are no restrictions on how you can use the data you've discovered. this means it's legal to use OSINT as a data technique for cyberattacks.
- Cybersecurity pros often use OSINT for their own benefits.
- They observe vulnerable data that hackers and cybercriminals could use to break into a company's network.

OSINT Cycle

1. Planning and Direction (Identifying the source)

The first step in the OSINT cycle involves planning the priorities and requirements for the mission. Prior to collecting OSINT, operators should have a clear understanding of the types of information they need.

2. Collection (

After proper planning OSINT resources include any materials that are freely available online, such as news articles, social media posts, and blogs

3. Processing and Exploitation

Once you've acquired your data, you can start processing the information. Then, you'll want to compile it into a common evidence repository, timeline, or report.

4. Analysis and Production

After the initial processing of the collected data, your teams will then need to perform an in-depth analysis of the information. This is a crucial step in the OSINT cycle. as it will allow your teams to use the data they've acquired to interpret and anticipate events.

5. Dissemination and Integration

The final step in the OSINT cycle entails delivering the collected and analyzed intelligence to the proper stakeholders.

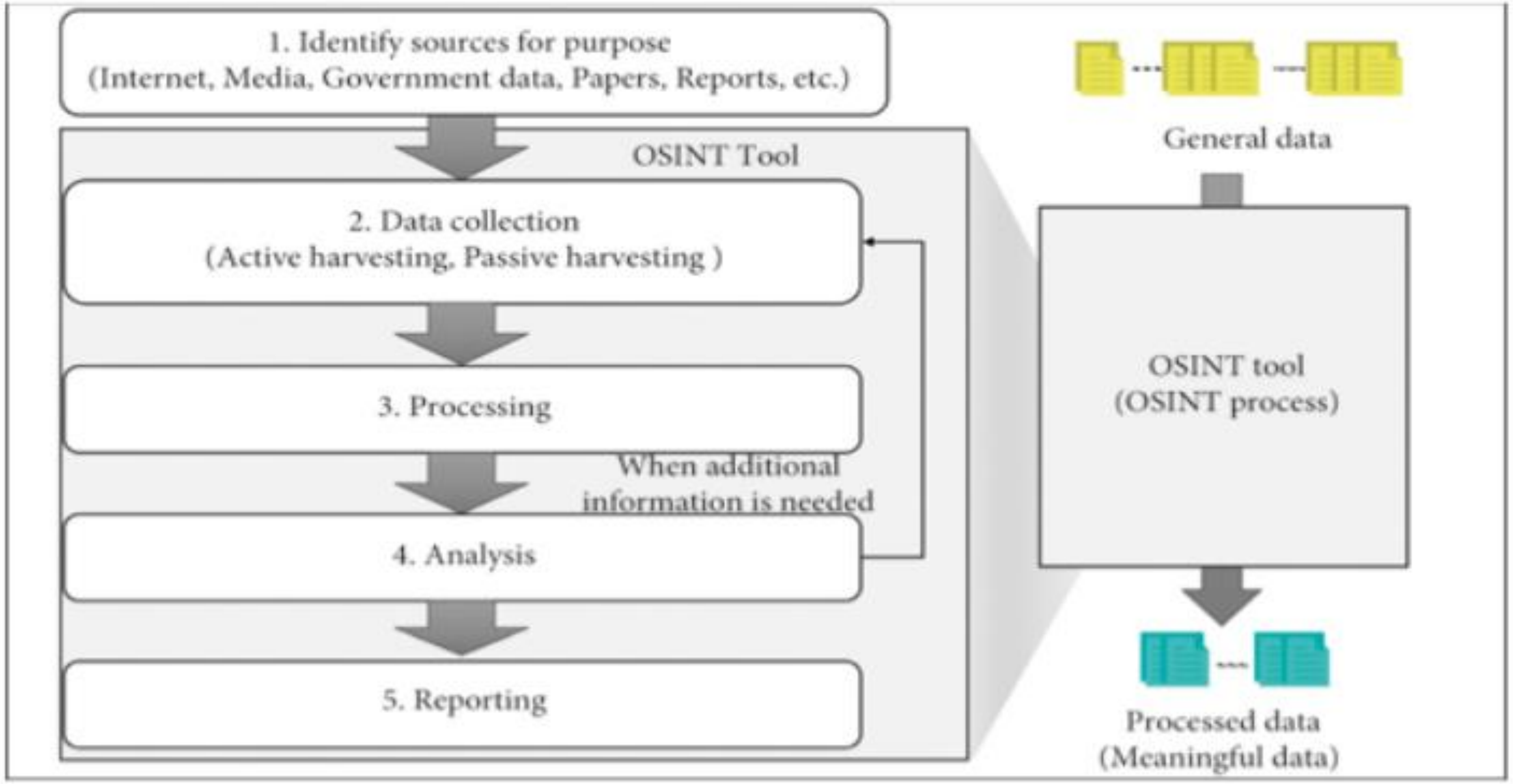


Figure 1

Structure of OSINT.

OSINT Harvesting Data

Passive

this is the “normal” way of digging for information; usually done by scouring the web with applications like Google search, Bing Maps, and Yandex images.
only archived information is collected.

Ex: Shodan, Netcraft, Google Hacking
(search engines)

Active

the information is collected by directly extracting it from the target, This type of probing can be detected because it involves scanning of networks to find open ports.

Ex: Nikito, Nessus, Nmap

Advantages and disadvantages of OSINT

❑ The advantages of using OSINT are as follows:

✓ Fast/real-time information collection: information collected by OSINT is quickly obtained through open sources, and the data are tracked in real-time.

✓ Secure acquisition of much data: the data collected by OSINT secures much data that supplements the gathering of secret intelligence.

✓ Clarity of sources: in HUMINT, the credibility of data is questionable because the source of the information that the agent obtains is unclear

✓ Convenience and ease of access: anyone can easily access information collected by OSINT and use data conveniently according to the user’s requirement.

✓ Low cost: OSINT has the advantage of obtaining data at a low cost, compared to the cost of training agents in HUMINT and the cost of collecting data using the latest equipment, such as satellites and unmanned aerial vehicles (UAV) in TECHINT.

Advantages and disadvantages of OSINT

❑ Disadvantages of using OSINT are as follows:

✓ The amount of information is too large: the more information the user has, the harder it is for the user to output reliable data using OSINT.

✓ Cornerstone of cybercrimes when misused: anyone can access the data collected by OSINT. However, there is the disadvantage that the data collected by OSINT can be the basis of committing cybercrimes because of users with malicious goals. Therefore, research is required on security requirements (measures) and technology that can minimize the damage of cybercrimes, even if users use OSINT’s data for malicious purposes.

Security Threats of OSINT

❑ The security threats that arise are as follows::

✓ **Data dissemination (release/misuse/deletion):** if the confidentiality of the collected data is not provided, attackers can obtain data and create various security threats based on them, which might cause the damage of data loss.

✓ **Data privacy breach**: if an attacker identified the contents of the collected data, the data for user information (personal information) included in the data could be collected, based on which various security threats could arise.

✓ **Data forgery and alteration:** attackers forged or altered the collected data, causing various security threats.

Security Threats of OSINT

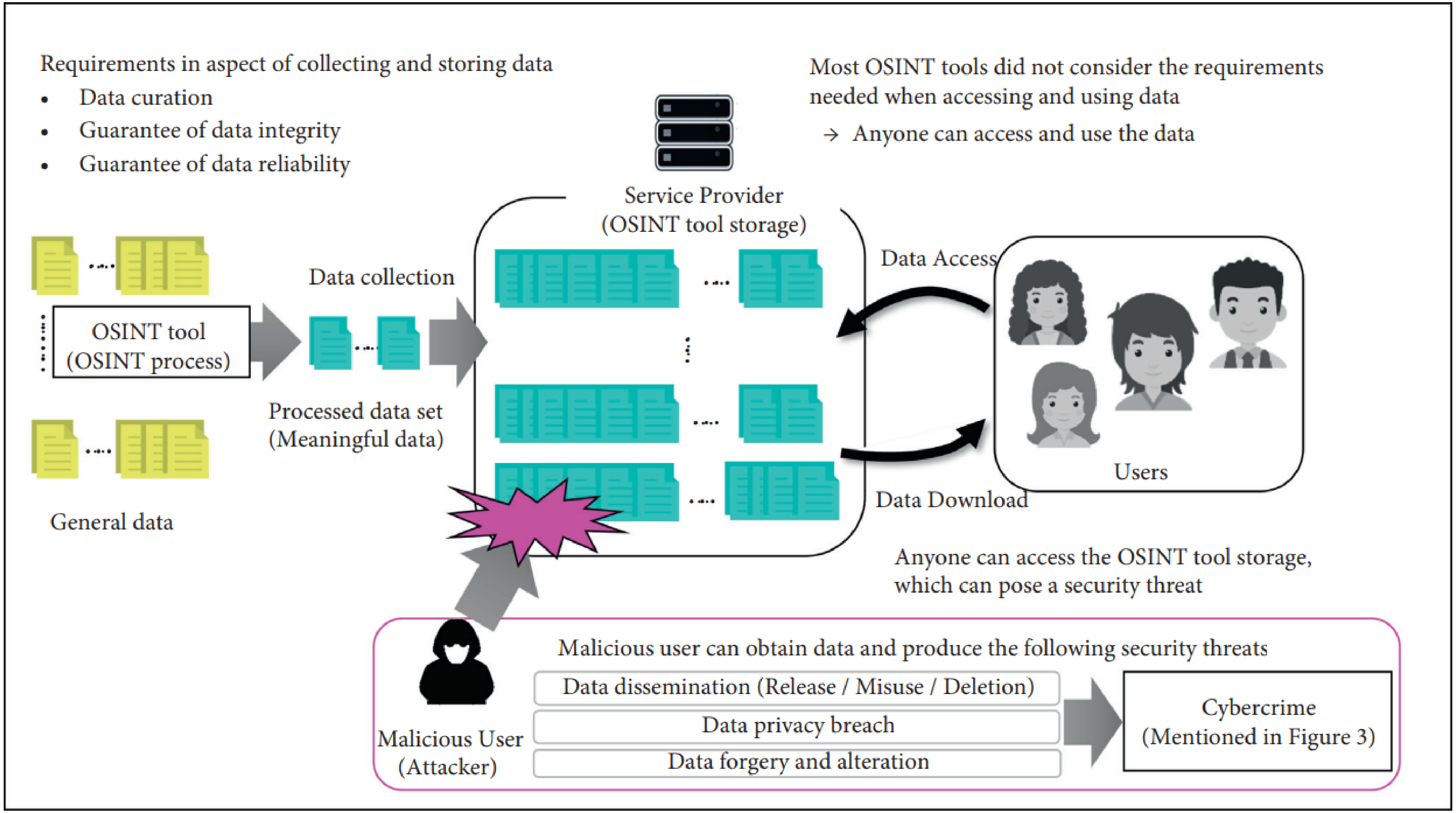

Requirements in aspect of collecting and storing data
• Data curation
• Guarantee of data integrity
• Guarantee of data reliability
Most OSINT tools did not consider the requirements needed when accessing and using data
→ Anyone can access and use the data
Service Provider
(OSINT tool storage)
OSINT tool
(OSINT process)
Data collection
Processed data set
(Meaningful data)
General data
Data Access
Data Download
Users
Anyone can access the OSINT tool storage, which can pose a security threat
Malicious user can obtain data and produce the following security threats
Data dissemination (Release / Misuse / Deletion)
Data privacy breach
Data forgery and alteration
Cybercrime
(Mentioned in Figure 3)
Malicious User
(Attacker)

Figure 2: OSINT process and possible security threats.

Role of OSINT from cybersecurity perspective

Role of OSINT from Cybersecurity Perspective

In this section, we explain the importance of OSINT from a cybersecurity perspective. Furthermore, we propose commonly needed security requirements to solve with security threats arising from the misuse of OSINT data.

1. Importance of OSINT for Cybersecurity

Regarding cybersecurity, the aspect of using data collected by OSINT could be viewed as a two-edged sword.

If the data collected by OSINT were used in the positive aspect, a considerable amount of data could be obtained compared to secret intelligence data.

If the data collected by OSINT were used in the negative aspect, the attacker could set the target based on profiling. Then, after gathering target information, the attacker commits various cybercrimes, such as SPAM, malware, hacking, DoS attack, phishing, the violation of digital property rights, confidential information infringement, and dissemination of false or confidential information.

Role of OSINT from cybersecurity perspective

2. Essential Security Requirements When Using OSINT

Various security threats existed in OSINT. To solve these problems, OSINT tools commonly needed additional basic security, The details of the requirements are as follows:

- ### Collecting and Storing OSINT Data
  - Data encoding/data encryption: in general, integrity existed in the data processed by OSINT, however, because they were publicly available information, data confidentiality must be provided, depending on the importance of the data.
  - Maintenance of data backup and recovery: damage caused by the loss of data because of system crashes, data alteration, and data deletion could not be ignored. Therefore, settings for the backup and recovery of data sets collected by OSINT were important.
  - Monitoring: if OSINT service providers provided additional security elements, such as security audits and security management, the security of the data collected by OSINT would be strengthened. In particular, monitoring should be performed in real-time to detect viruses and malware and prevent users from leaking data

Role of OSINT from cybersecurity perspective

2. Essential Security Requirements When Using OSINT

- **Security Requirements for Users to Access and Use OSINT Data**
  - User authentication: usually, the authentication process was performed to determine who the user was and whether the user had the right when the user tried to access and obtain data on IoT, cloud, or Web.
  - Access control: the term access control referred to a function that permitted or denied someone from using something (service).
  - Forward secrecy: Forward secrecy referred to the encrypted communications and sessions recorded in the past that could not be retrieved. In other words, it was to assume that the user had a token containing the rights for accessing the OSINT tool. If the user's registration period expires or the registration for the OSINT tool is withdrawn, the user's right to access the OSINT tool must expire.

How Hackers Are Using OSINT In Their Work

- Some may want to steal **personal data,** while others would like to use the information for more malicious purpose.
- These intentions could include **business surveillance or even hacking** entire companies.
- Cybersecurity teams can use OSINT to monitor for security breaches and attacks.
- They can use the tool to identify sensitive company information that malicious actors could use.

Types Of OSINT Data Used In Cyberattacks

- ❑ Personal Data

Personal info may include **names, addresses, phone numbers, birth dates**, and social media profiles like LinkedIn

- ❑ Professional Data

This type of data can include items like **employment history, education**, and any other information that's found on a person's professional networking sites.

- ❑ Technical Data

Technical data includes information like **IP addresses, server names**, application versions, and any other information that's used to further a hacker's goals.

What Types Of OSINT Do We Have?

Discovery tools

are used to search for the information that is out there. A great example would be Google.

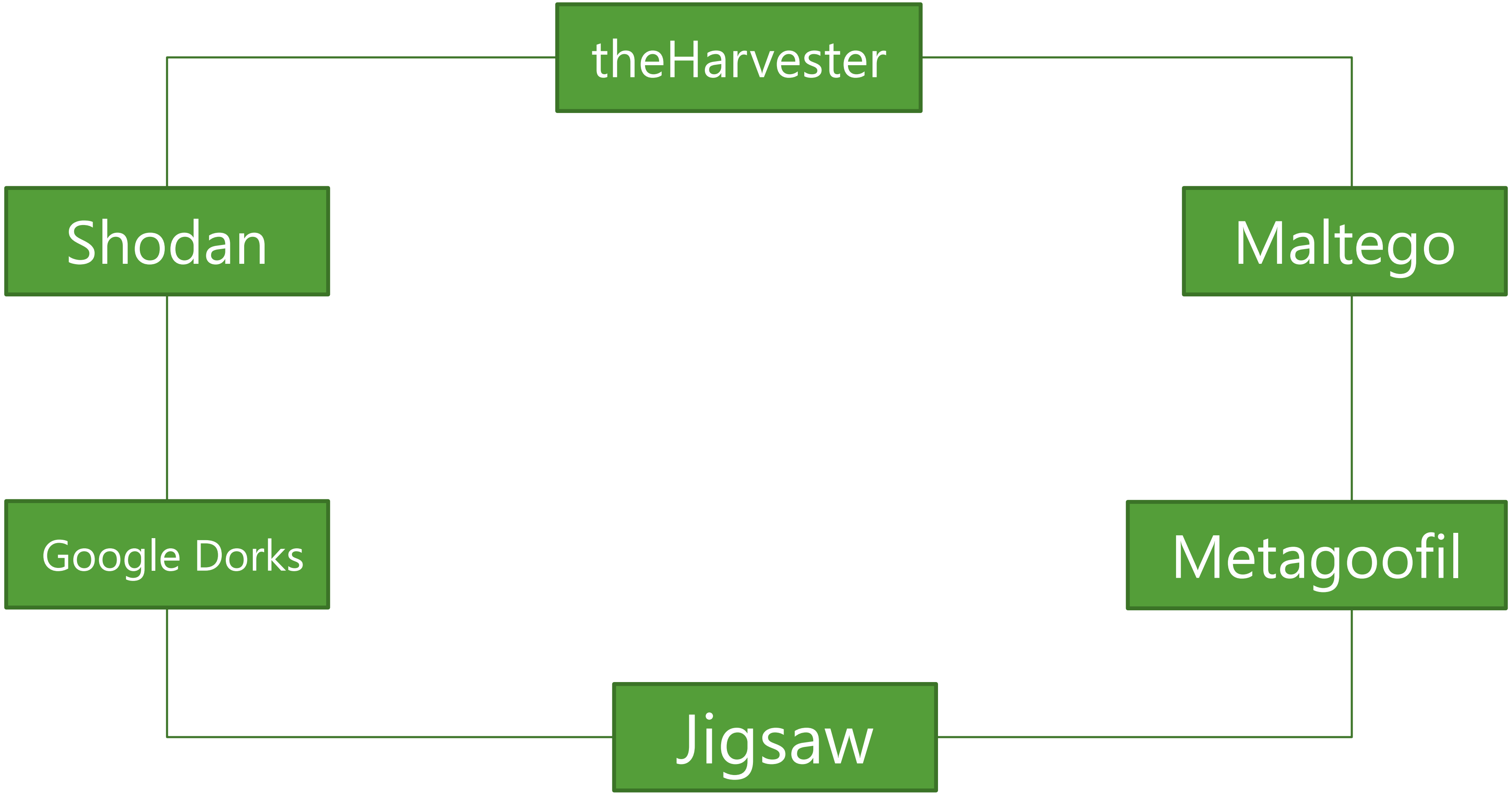
Scraping tools

once discovered, the data must be “scraped” and collected somewhere safe.

Aggregation tools

once the data has been stored safely, it needs to be mined and sifted through to convert it into usable These tools.

The 6 Best OSINT Tools



theHarvester

Maltego

Metagoofil

Jigsaw

Google Dorks

Shodan

Jigsaw

- ❑Jigsaw is used to gather information about any company employees.
- ❑This tool works perfectly for companies like Google, Linkedin, or Microsoft, where we can just pick up one of their domain names (like google.com), and then gather all their employee's emails on the different company departments.
- ❑we depend entirely on what information they allow us to explore inside their database.
- ❑You will be able to find information about big companies, but if you are exploring a not so famous startup then you may be out of luck.

theHarvester

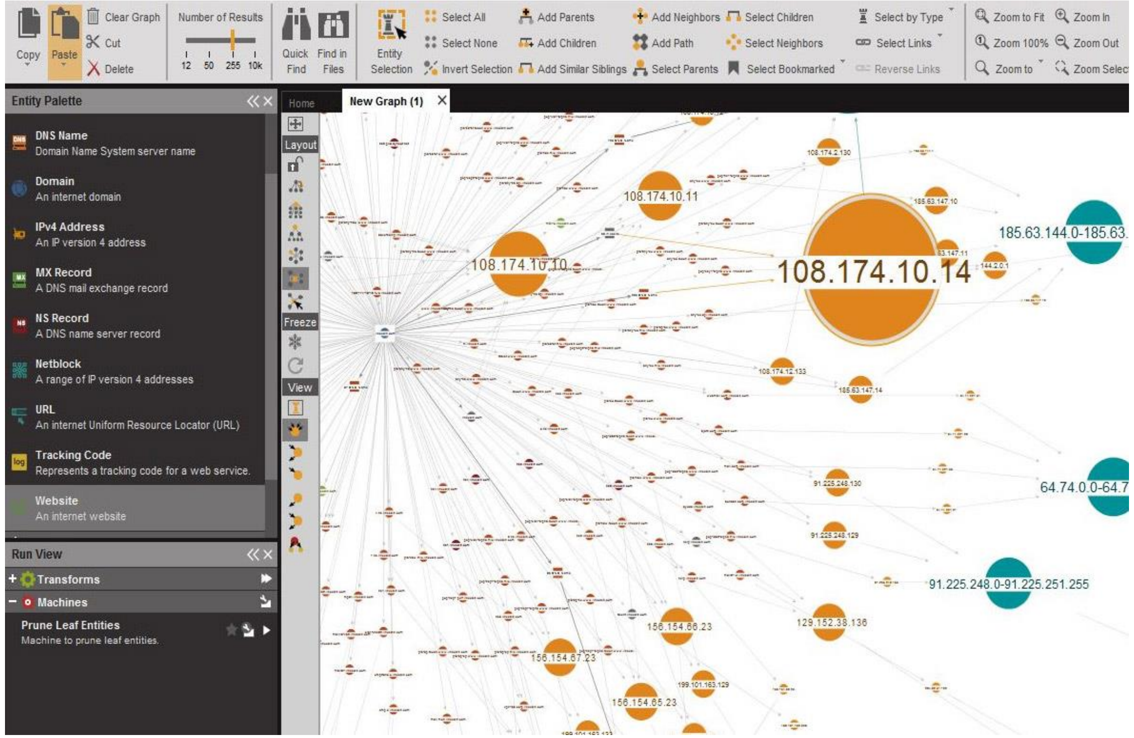
- ❑ theharvester has the ability to get tremendous amount of information.
- ❑ theHarvester is a penetration testing tool used to gather information about emails, subdomains, hosts, employee names, open ports, and banners from different public sources like search engines, PGP key servers, and SHODAN computer database.
- ❑ This is especially useful when you are in the first steps of a penetration test against your own local network.
- ❑ theHarvester uses many resources to fetch the data like PGP key servers, Bing, Yahoo and Google search engine, and also social networks like LinkedIn, Twitter and Google Plus.

Shodan

- It is often called the 'search engine for hackers', as it lets you find and explore a different kind of devices connected to a network like servers, routers, webcams, and more.
- It can be used to gather information on servers belonging to businesses or even cities.
- Shodan is offered as a service, much like Google, it will show you things that are more related to the interest of IT security researchers like SSH, FTP, SNMP, Telnet, RTSP, IMAP and HTTP server banners and public information.
- Very user friendly, even for non-technical users

Maltego

- ❑ This OSINT tool is helpful in finding information on individuals as well as organizations.
- ❑ It can run on Linux, Windows, and macOS.
- ❑ The interface is very detailed but easy to learn.
- ❑ Identifies relationships between data



DNS Name
Domain Name System server name

Domain
An internet domain

IPv4 Address
An IP version 4 address

MX Record
A DNS mail exchange record

NS Record
A DNS name server record

Netblock
A range of IP version 4 addresses

URL
An internet Uniform Resource Locator (URL)

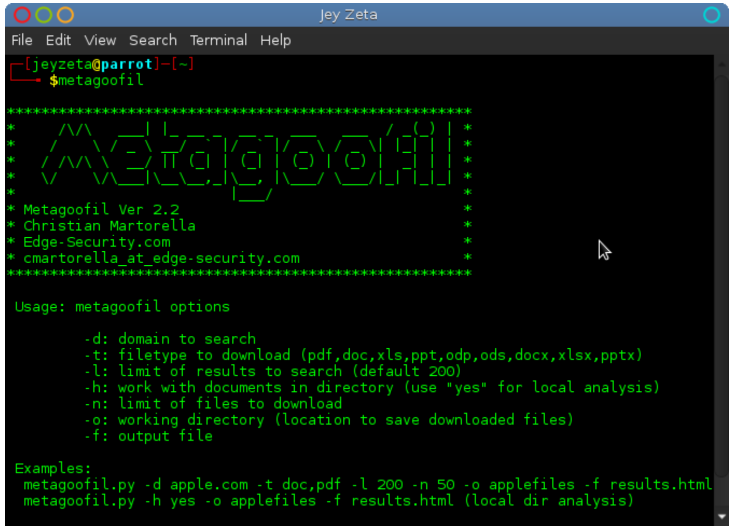
Tracking Code
Represents a tracking code for a web service.

Website
An internet website

Prune Leaf Entities
Machine to prune leaf entities.

Metagoofil

- ❑ is another great intel-reconnaissance tool that aims to help infosec researchers, IT managers, and red teams to extract metadata from different types of files, such as: doc, docx, pdf, xls, xlsx, ppt, pptx.
- ❑ This app performs a deep search on search engines like Google, focusing on these types of files.
- ❑ Once it detects such a file, it will download it to your local storage, then proceed to extract all of its valuable data.



```
┌─[jeyzeta@parrot]─[~]
└──╼ $metagoofil

*************************************************************
*     /\/\   ___| |_ __ _  __ _  ___   ___  / _(_) |  *
*    /    \ / _ \ __/ _` |/ _` |/ _ \ / _ \| |_| | |  *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | |  *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_|  *
*                         |___/                       *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*************************************************************

 Usage: metagoofil options

         -d: domain to search
         -t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
         -l: limit of results to search (default 200)
         -h: work with documents in directory (use "yes" for local analysis)
         -n: limit of files to download
         -o: working directory (location to save downloaded files)
         -f: output file

 Examples:
  metagoofil.py -d apple.com -t doc,pdf -l 200 -n 50 -o applefiles -f results.html
  metagoofil.py -h yes -o applefiles -f results.html (local dir analysis)
```

Challenges of OSINT

- ❑ Efficient and reliable data filtering: to extract the data that the user wants from OSINT, much data should be collected and effectively filtered [13]. It consumes a huge amount of time and human resources, depending on the amount of data. Organizations or users will utilize automation tools (organizations have their own AI filtering tools) and skill sets to filter data according to purpose.
- ❑ Provides data transparency: the reliability of the collected data was a critical issue in the aspect of the users using OSINT's data. In particular, the verification of sources for claiming the legitimacy of data during the OSINT process increased data reliability significantly. However, in the case of obtaining OSINT data by illegal means, the user might intentionally discard or hide important sources, however, no countermeasure existed in OSINT.

END