What is OSINT

- "OSINT " refers to Open source intelligence, that is the act of gathering and analyzing publicly available data for intelligence purposes.
- Open source data means any information that is readily available to the public or can be made available by request.
- OSINT sources can include:
    - Newspaper and magazine articles, as well as media reports
    - Academic papers and published research
    - Books and other reference materials
    - Social media activity
    - Census data
    - Telephone directories
    - Court filings
    - Arrest records
    - Public trading data
    - Public surveys
    - Location context data
    - Breach or compromise disclosure information
    - Publicly shared cyber attack indicators like IP addresses, domain or file hashes
    - Certificate or Domain registration data
    - Application or system vulnerability data

What is OSINT Framework

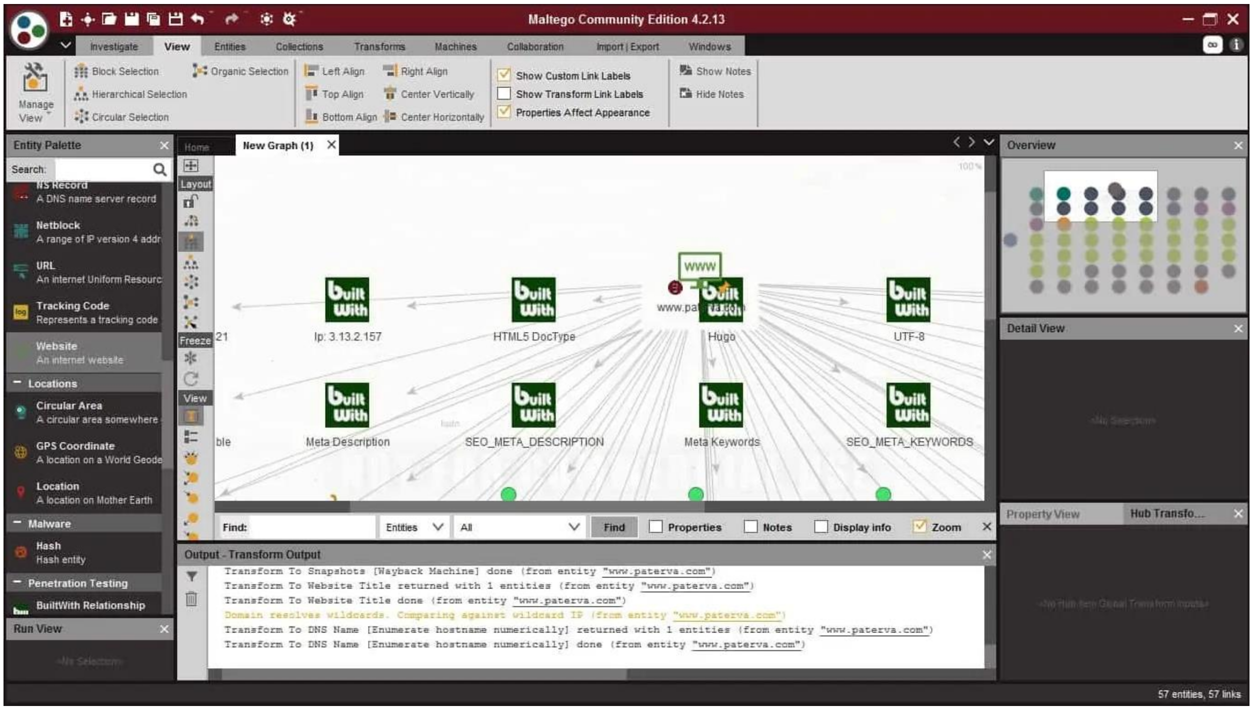
- The OSINT framework is a methodology that integrates data, processes, methods, free tools and techniques to help the security team identify information about an adversary or their actions quickly and accurately.
- The purpose of An OSINT framework can be:
    - To establish the digital footprint of a known threat
    - To gather all available intelligence about an adversary's activity, interests, techniques, motivation and habits
    - To categorize data by source, tool, method or goal
    - To identify opportunities to enhance the existing security posture through system recommendations

Some of the Important Tools Description are listed Below

Tool Name

1. Maltego

- This OSINT tool is used for finding information on individuals as well as organizations.
- But one will have to register with Maltego Community to start digging for information with this tool.



Output - Transform Output

```
Transform To Snapshots [Wayback Machine] done (from entity "www.paterva.com")
Transform To Website Title returned with 1 entities (from entity "www.paterva.com")
Transform To Website Title done (from entity "www.paterva.com")
Domain resolves wildcards. Comparing against wildcard IP (from entity "www.paterva.com")
Transform To DNS Name [Enumerate hostname numerically] returned with 1 entities (from entity "www.paterva.com")
Transform To DNS Name [Enumerate hostname numerically] done (from entity "www.paterva.com")
```

Usage

- To start the information-gathering process, we have to enter the main entity for which we are doing the research that can be an individual, organization, phone number, etc.
- Then we have to run the available transforms to see the results.
- It can be used to map networks to see how the servers on it are linked and if, perhaps, they have been compromised.
- The resulting information can be filtered or further “transformed” for even more in-depth data analysis.

Advantage

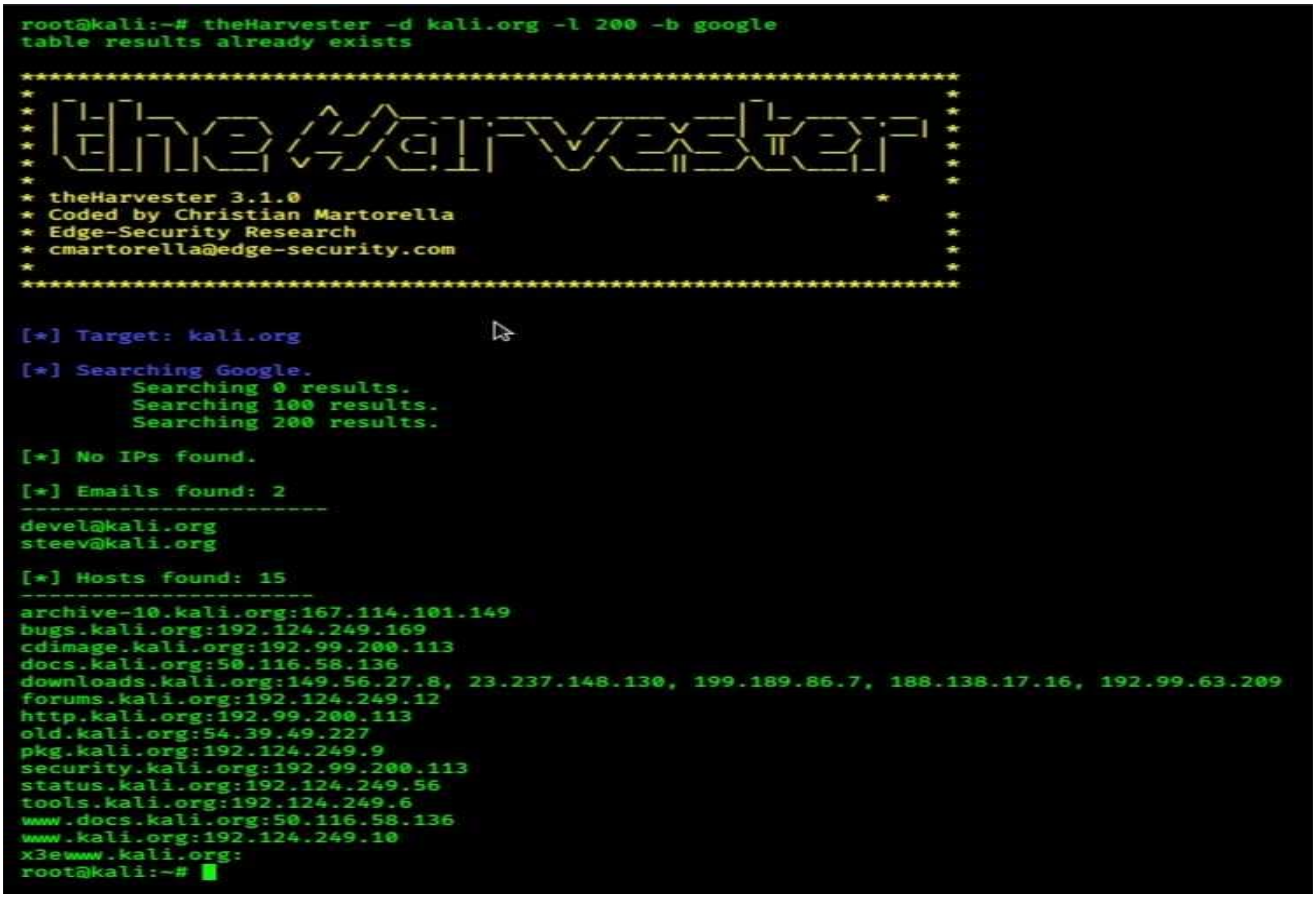
- This tool is highly visual, great for mapping complex networks and relationships
- The interface is very detailed but easy to learn in this method
- This tool highlights relationships between data points natively – new sources can be added via API

Features

- It Identifies relationships between data
- Its output generates a data map
- This tool runs on Windows, Linux, and macOS

2. theHarvester

- theHarvester is a very useful alternative to fetch valuable information about any subdomain names, virtual hosts, open ports and email address of any company or website.



```
root@kali:~# theHarvester -d kali.org -l 200 -b google
table results already exists

*******************************************************************
*                                                                 *
*                                                                 *
*                                                                 *
*                                                                 *
*                                                                 *
*                                                                 *
* theHarvester 3.1.0                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: kali.org

[*] Searching Google.
        Searching 0 results.
        Searching 100 results.
        Searching 200 results.

[*] No IPs found.

[*] Emails found: 2
----------------------
devel@kali.org
steev@kali.org

[*] Hosts found: 15
---------------------
archive-10.kali.org:167.114.101.149
bugs.kali.org:192.124.249.169
cdimage.kali.org:192.99.200.113
docs.kali.org:50.116.58.136
downloads.kali.org:149.56.27.8, 23.237.148.130, 199.189.86.7, 188.138.17.16, 192.99.63.209
forums.kali.org:192.124.249.12
http.kali.org:192.99.200.113
old.kali.org:54.39.49.227
pkg.kali.org:192.124.249.9
security.kali.org:192.99.200.113
status.kali.org:192.124.249.56
tools.kali.org:192.124.249.6
www.docs.kali.org:50.116.58.136
www.kali.org:192.124.249.10
x3ewww.kali.org:
root@kali:~# █
```

Usage

- The sources that theHarvester uses include popular search engines like Bing and Google, as well as lesser known ones like dogpile, DNSdumpster and the Exalead metadata engine.
- It also uses Netcraft Data Mining and the AlienVault Open Threat Exchange.
- It can even tap the Shodan search engine to discover open ports on discovered hosts.

Advantages

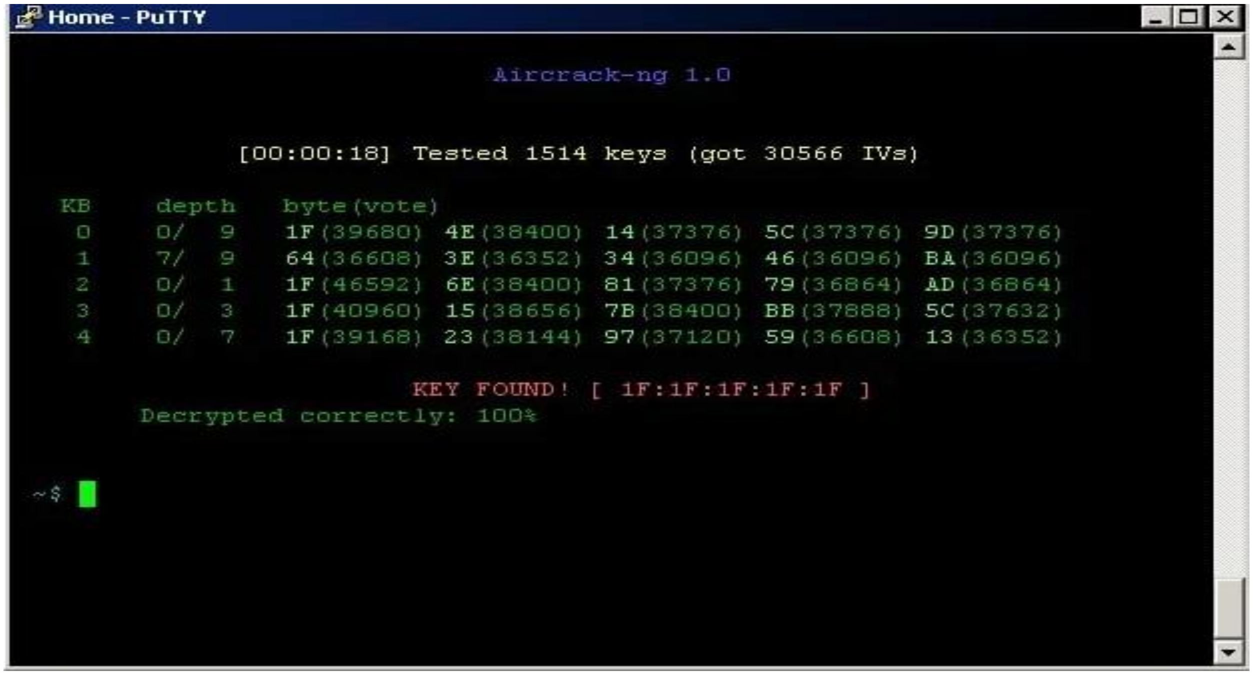
- This tool could be used as both Active & passive Reconnaissance tool.
- But the passive reconnaissance abilities of this tool makes it suitable for blue or purple teams, depending on the situation.

Features

- It is Linux-based tool, which is already Pre-installed on Kali.
- This tool is Freely available on git-hub.
- This tool is developed in Python.
- It can Take screenshots of subdomains that were found.

3. Aircrack-ng

- Aircrack-ng is a wireless network security penetration testing tool.



```
                              Aircrack-ng 1.0


                 [00:00:18] Tested 1514 keys (got 30566 IVs)

   KB    depth   byte(vote)
    0    0/  9   1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376)
    1    7/  9   64(36608) 3E(36352) 34(36096) 46(36096) BA(36096)
    2    0/  1   1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864)
    3    0/  3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
    4    0/  7   1F(39168) 23(38144) 97(37120) 59(36608) 13(36352)

                         KEY FOUND! [ 1F:1F:1F:1F:1F ]
      Decrypted correctly: 100%


~$
```

Usage

It has 4 main functions as listed below:

- Packet monitoring – Capturing of frames and collecting WEP IVs (Initialization Vectors); if a GPS is added, it can log the position of APs (access points).
- Penetration testing – By performing packet injection attacks, fake access points, replay attacks, and more to test a network’s security.
- Performance analysis – Testing wifi and driver capabilities.
- Password security testing – Password cracking on WEP and WPA PSK (WPA 1 and 2).

Advantage

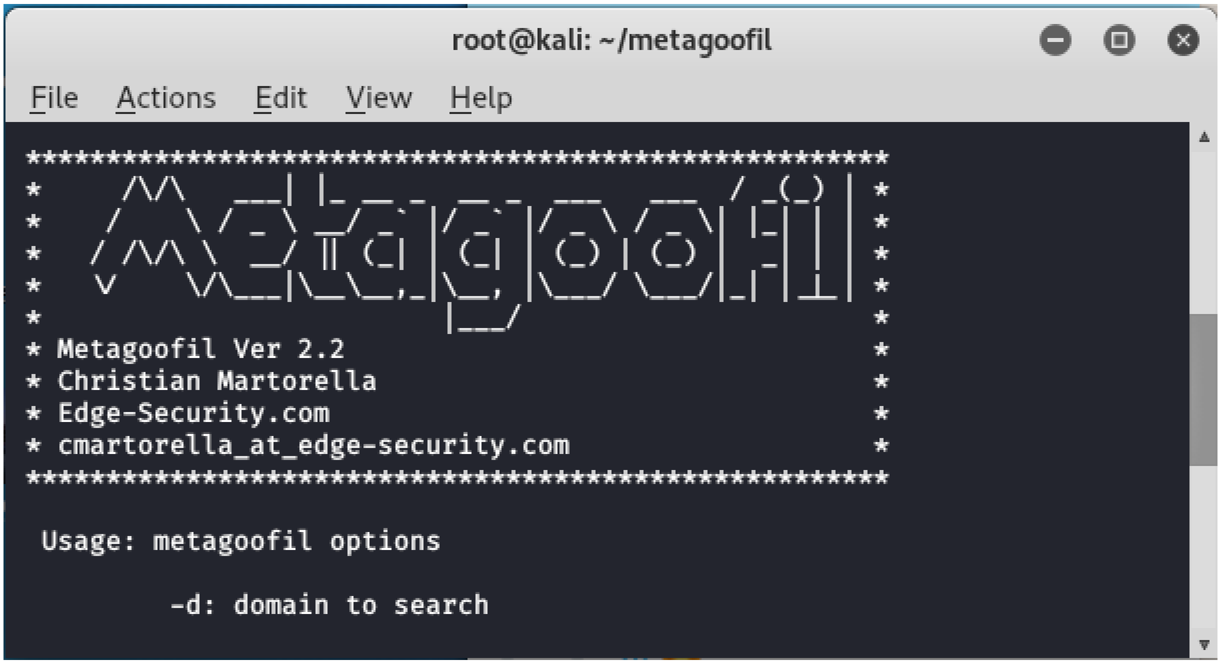
- This tool focuses heavily on wireless security, making it One of the most widely supported wireless security tools.
- It has been a great tool for routine audits or field pen tests.
- This tool can audit wifi security as well as crack weak wireless encryption.

Features

- It can scan wireless channels
- This tool is free to use
- It runs on Linux, FreeBSD, macOS, and Windows

4. Metagoofil

This is a great intellingenge-reconnaissance tool, freely available on git-hub 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 etc.



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

 Usage: metagoofil options

        -d: domain to search
```

Usage

- This app performs a deep search on search engines like Google, focusing on these above mentioned types of files.
- Once it detects such a file, it will download it to the local storage, then proceed to extract all of its valuable data.
- Once the extraction is complete, we'll find full report with usernames, software banners, app versions, hostnames and much more useful informations.

Advantage

- It includes a number of options to filter the types of files to search & hence its results are refined.
- Output tweaking is possible with this tool.
- It also maps the paths of how to get to those documents, which in turn would provide things like server names, shared resources and directory tree information about the host organization.
- Data gathered from its output can makes it easy for the attacker to launch a Brute-force attack.

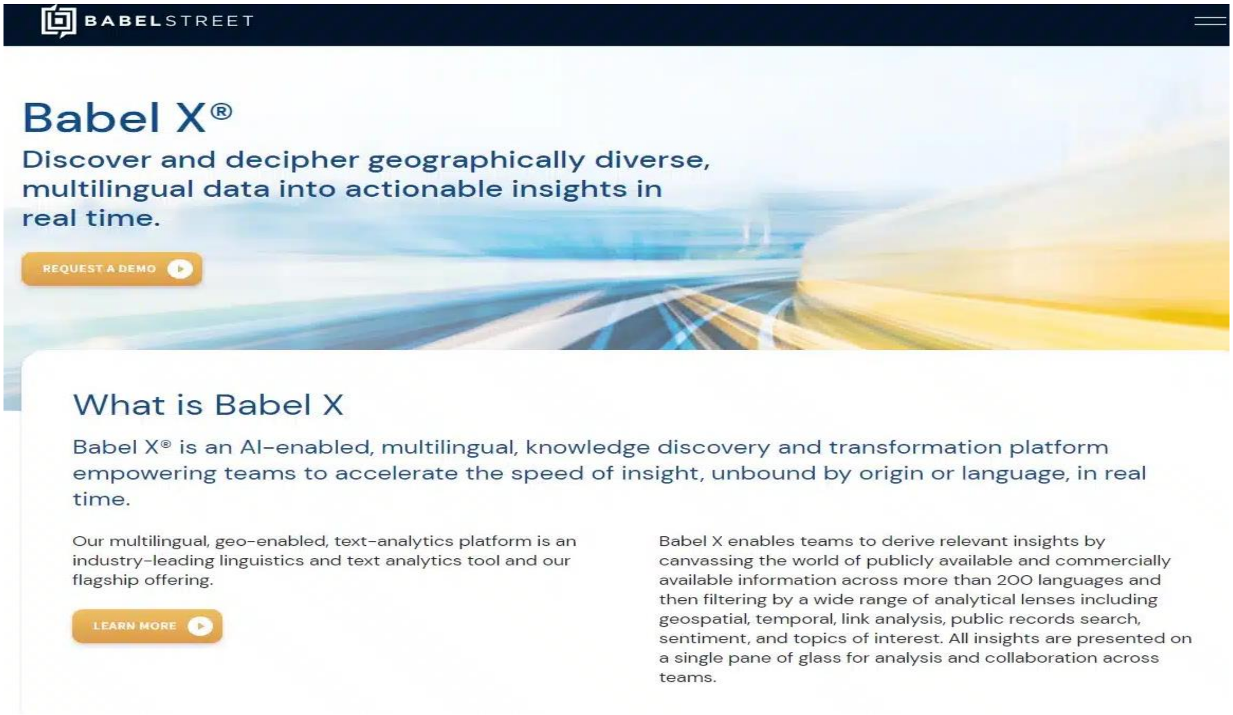
Features

- This tool will generate a report with all the vital informations about the target, After extraction.
- This tool can also extract MAC addresses from Microsoft office documents.

- This tool can give information about the hardware of the system by which they generated the report of the tool.
- This is a Linux-based tool.

5. Babel X

- This tool from Babel street, is a multilingual, AI-enabled knowledge discovery & transformation Platform.



Babel X®

Discover and decipher geographically diverse, multilingual data into actionable insights in real time.

What is Babel X

Babel X® is an AI-enabled, multilingual, knowledge discovery and transformation platform empowering teams to accelerate the speed of insight, unbound by origin or language, in real time.

Our multilingual, geo-enabled, text-analytics platform is an industry-leading linguistics and text analytics tool and our flagship offering.

Babel X enables teams to derive relevant insights by canvassing the world of publicly available and commercially available information across more than 200 languages and then filtering by a wide range of analytical lenses including geospatial, temporal, link analysis, public records search, sentiment, and topics of interest. All insights are presented on a single pane of glass for analysis and collaboration across teams.

Usage

- This search tool is used for the public internet including blogs, social media, message boards and news sites.
- It also searches the dark web, including Onion sites, and some deep web content that Babel X can access through agreements or licensing from the content owners.
- The product is able to geo-locate the source of information it finds, and it can perform text analysis to identify relevant results.
- It is currently capable of searching in more than 200 languages.

Advantage

- It builds and depicts networks of attackers.
- It links together seemingly unrelated events.
- This tool searches in 200 languages, using AI in translation.

Features

- It searches all the social media, message boards and even news sites.
- It has access to thousands of public data sources
- It does multi-national searches.

References:

https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/#:~:text=The%20OSINT%20framework%20is%20a,footprint%20of%20a%20known%20threat

https://github.com/lockfale/OSINT-Framework

https://www.comparitech.com/net-admin/osint-tools/#:~:text=The%20collection%20of%20OSINT%20tools,So%2C%20proceed%20with%20caution.

https://www.csoonline.com/article/567859/what-is-osint-top-open-source-intelligence-tools.html#:

https://securitytrails.com/blog/osint-tools

https://www.geeksforgeeks.org/metagoofil-tool-to-extract-information-from-docs-images-in-kali-linux/

https://www.geeksforgeeks.org/python-theharvester-how-to-use-it/

https://securitytrails.com/blog/theharvester-tool

End of the Report