Experiment No. – 5				
Date of Performance:				
Date of Submission:				
Program Execution/ formation/ correction/ ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 5
OSINT Framework

5.1Aim: Detect SQL injection vulnerabilities in a website database using SQLMap.

5.2Course Outcome: Illustrate the various tools and techniques used by attackers to launch their attacks.

5.3 Learning Objectives: Study of OSINT framework.

5.4 Requirement: Any type of web browser and Kali Linux

5.5 Related Theory:

OSINT Framework and its Functions:

The first phase in ethical hacking is reconnaissance, also known as footprinting and information collecting, in which we gather as much information about the target as possible. OSINT plays a critical role in obtaining information on the target. The OSINT framework plays such a crucial role in information retrieval.

What is OSINT Framework?

The OSINT framework is a cybersecurity structure that consists of a collection of OSINT technologies that may be used to find information about a target more quickly and easily. It is a web-based platform that allows you to browse several OSINT tools on various themes and goals based on your requirements. The OSINT framework focuses on acquiring data through open-source tools and resources. It can also be easily browsed looking at the OSINT tree and it provides excellent classification of all existing intel sources.

5.6 Related Theory:

OSINT Framework Classification

The OSINT Framework can be accessed from websites:
https://osintframework.com/

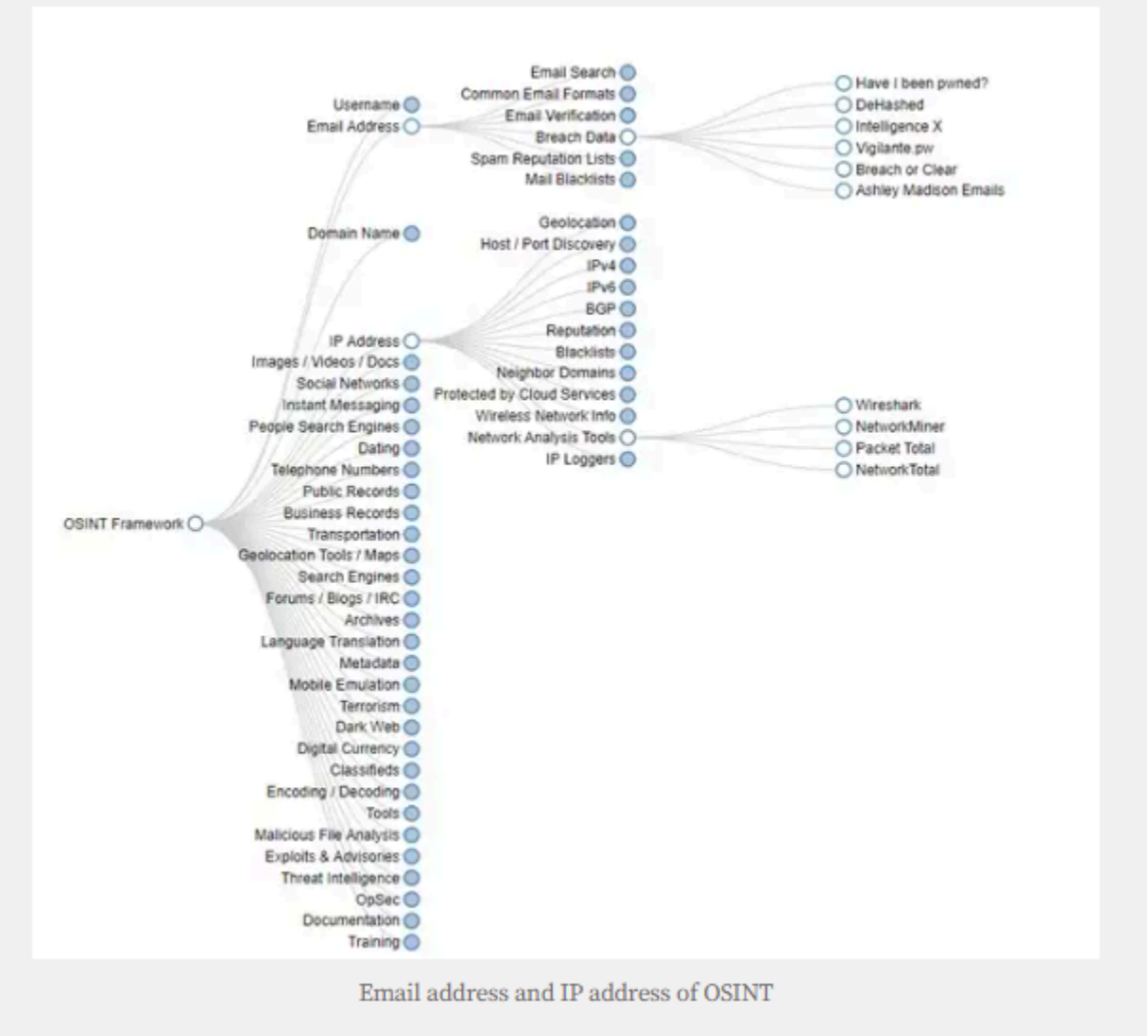
On the right top corner of the screen, you can find indicators for some of the listed tools.
(T) — Indicates a link to a tool that must be installed and run locally
(D) — Google Dork (or Google Hacking)
(R) — Requires registration
(M) — Indicates a URL that contains the search term and the URL itself must be edited manually

Figure 5.1 OSINT Framework

Many categories are given in the shape of a tree in the above image, including email address, username, domain name, IP address, social networks, and so on. When you click on any of the themes, a sub-tree of useful resources appears.
So, if you're looking for an email address, an IP address, or phone records, you can find them all in one place, which is why the OSINT framework is so important for cybersecurity and information discovery.

Email address and IP address OSINT:
When you are searching for a breached email address, then you can find many links to useful resources such as,
Have I been pwned?
Intelligence X

Vigilante.pw
Asley Madison Email , etc.
Similarly, if you are trying to analyze your network, then under IP address > Network Analysis Tool, you can find different tools to analyze the network such as
Wireshark
NetworkMiner
Packet Total
Network Total



Email address and IP address of OSINT

Figure 5.2 Expanded view of OSINT Framework

Nmap is a port scanning program that may be used to identify open ports, closed ports, and other information. However, there are numerous additional tools in the OSINT framework for identifying ways to scan ports, such as,
Zoom Eye
Scans.io

Shodan
Spyse
And many more.

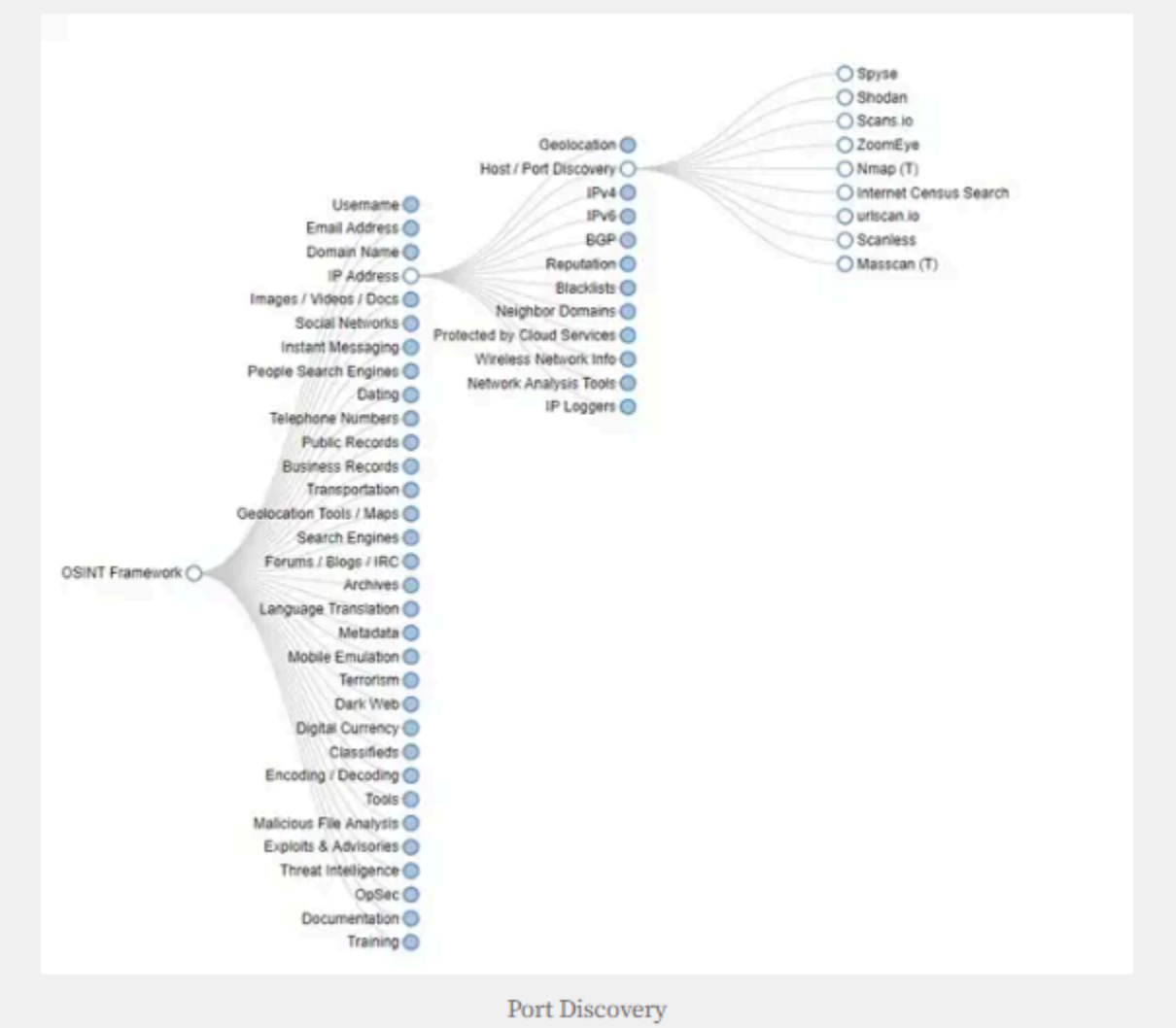
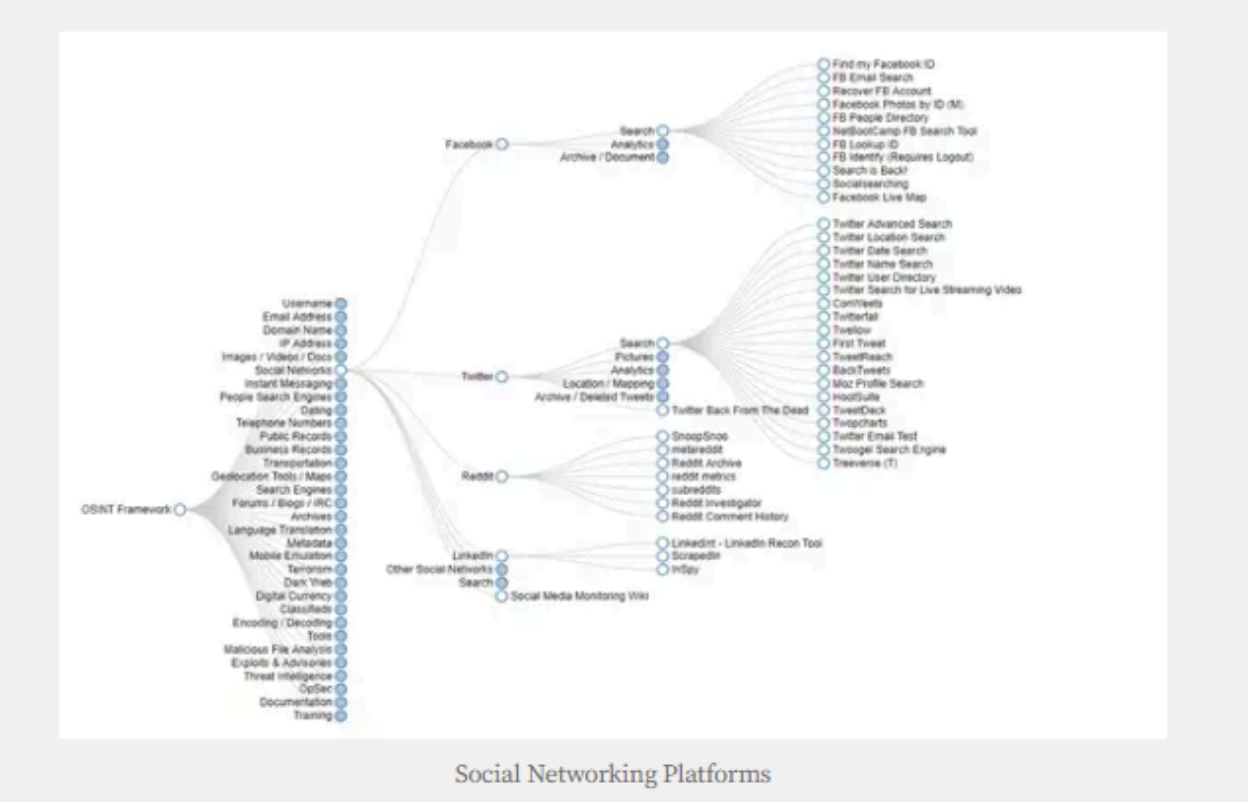


Figure 5.3 Port discovery

Social Networking Platforms OSINT:
You can learn about social networking platforms such as Facebook, Twitter, Reddit, LinkedIn, and others. You can locate your Facebook and Twitter accounts, as well as a variety of other details. LinkedIn, on the other hand, does not make as much information available to the public. However, there are a few tools available, like as
LinkedInt — LinkedIn Recon Tool
ScrapedIn
InSpy



Social Networking Platforms

Figure 5.4 Social Networking Platforms

Exploits and Advisories OSINT

Exploits and Advisories is another intriguing topic in the OSINT framework. Default passwords is an area where you may search for various links to default password databases, lists, lookup utilities, and so on.

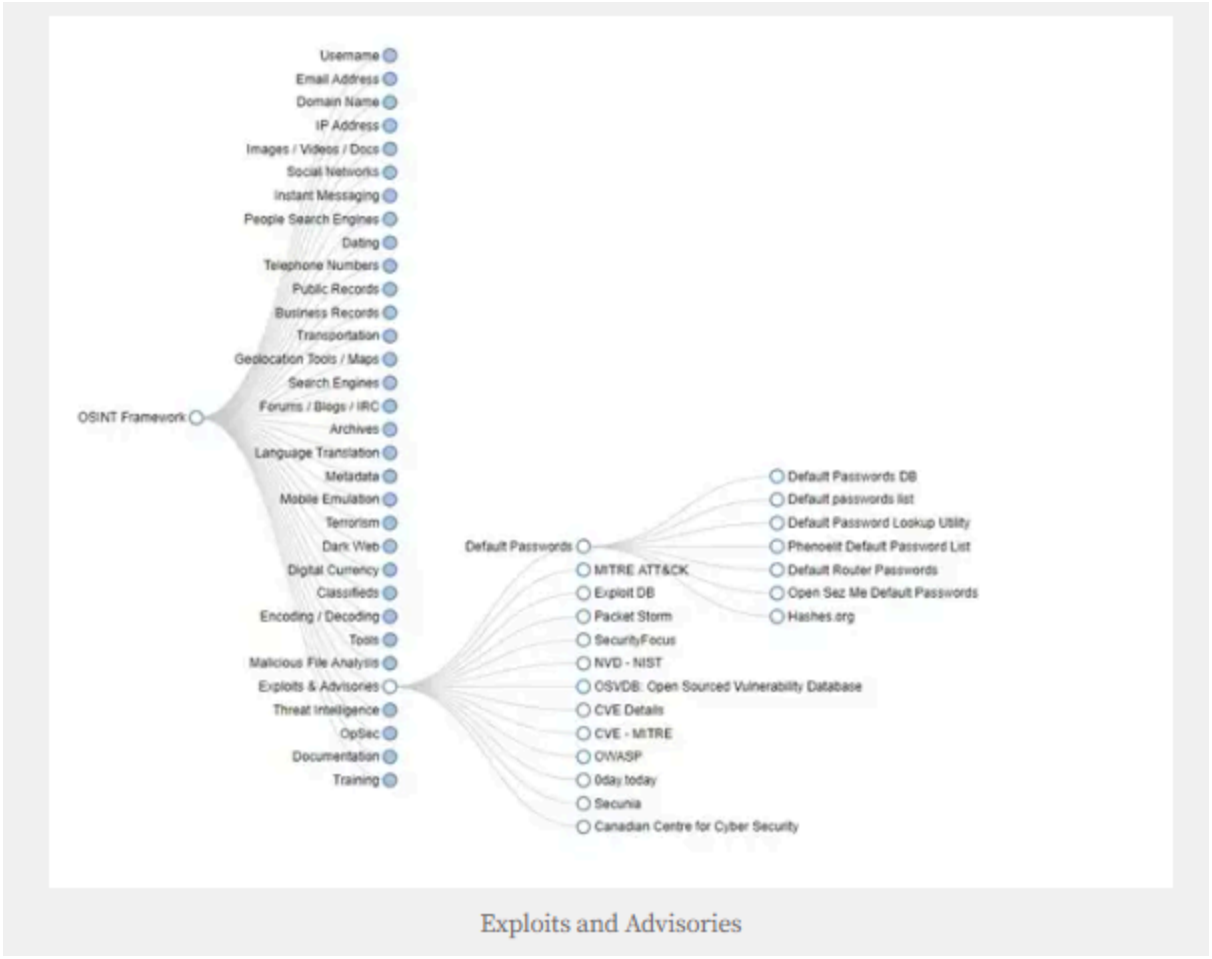


Figure 5.5 Exploits and advisories

Dark Web OSINT

Do you want to access the Dark Web? You can find information such as general information available about deep web, dark web, and onion from reddit link? You can find information about the client by downloading tools such as Tor Download and I2P Anonymous Network.

You can also find links to Onion scan, TorBot, TorScan, etc. If you want to search on TOR, you can find different links to Onion Cab, Onion Link, Candle, etc. Links to TOR directories such as Hidden Wiki, Core.onion and Onion Tree. Other links to Dark Web are Tor2web, Web O Proxy and IACA Dark Web Investigation Support.

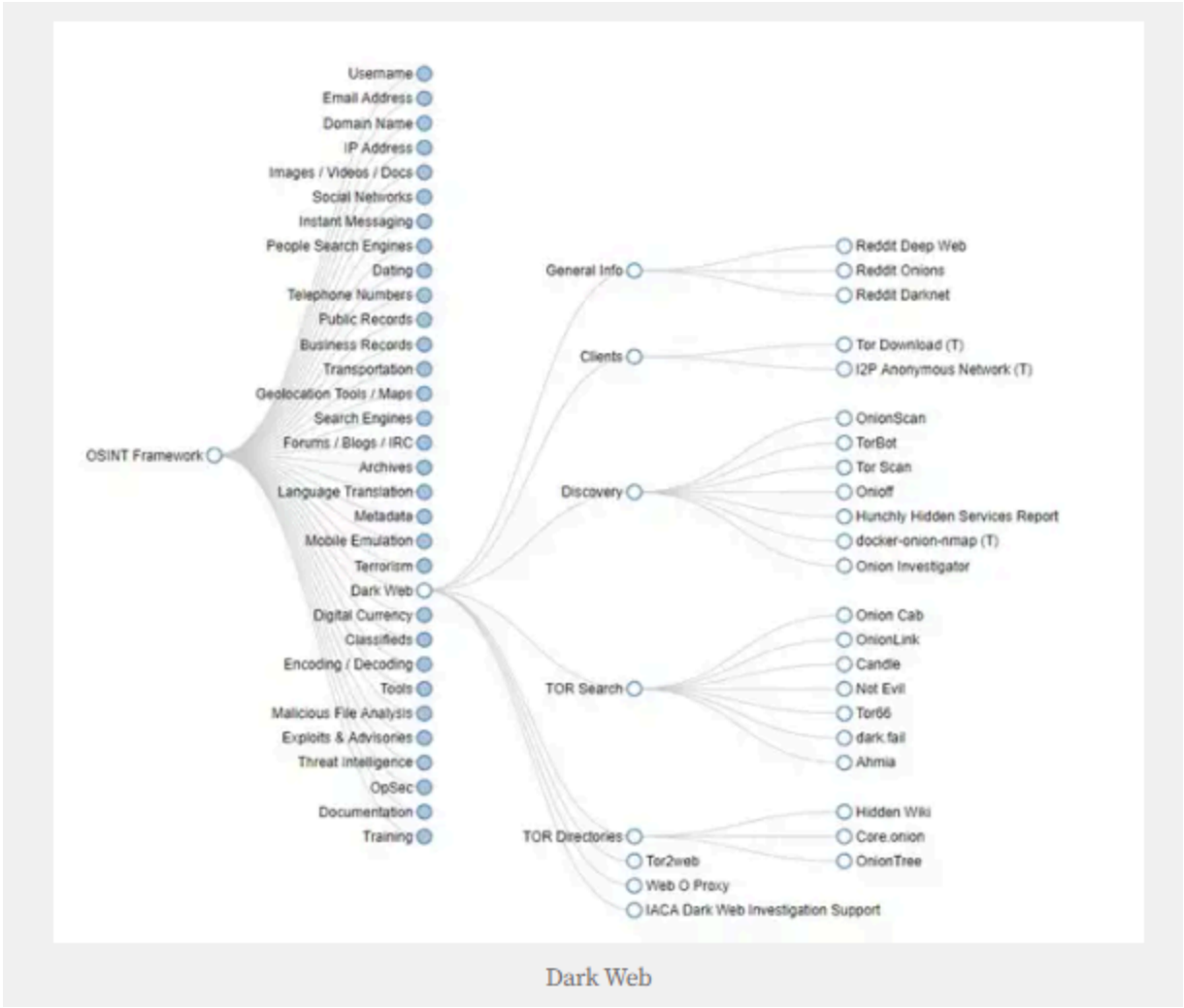


Figure 5.6 Dark web

Digital Currency OSINT

Information on Digital Currency such as Bitcoin, Ethereum and Monero can be found within OSINT Framework.

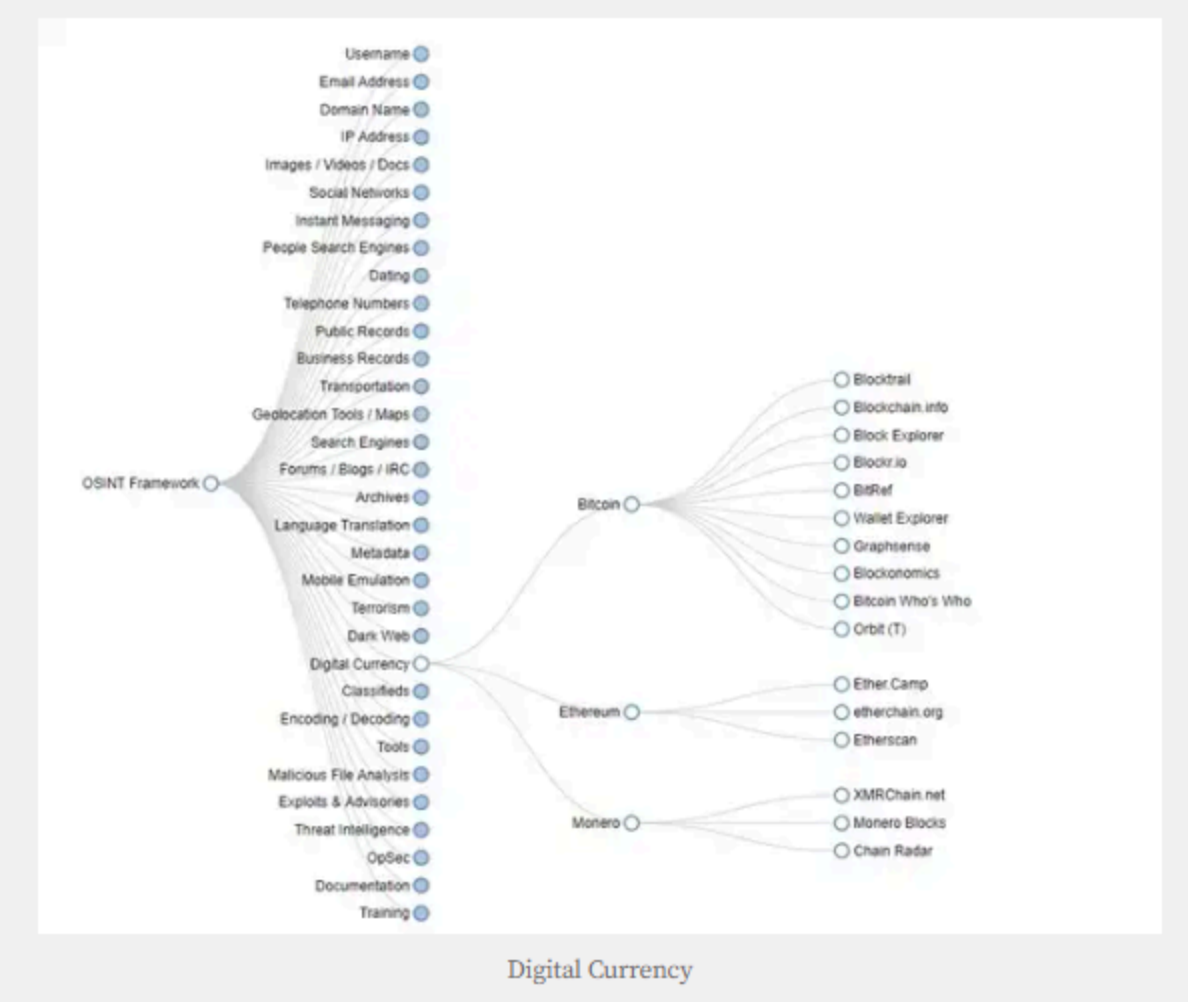
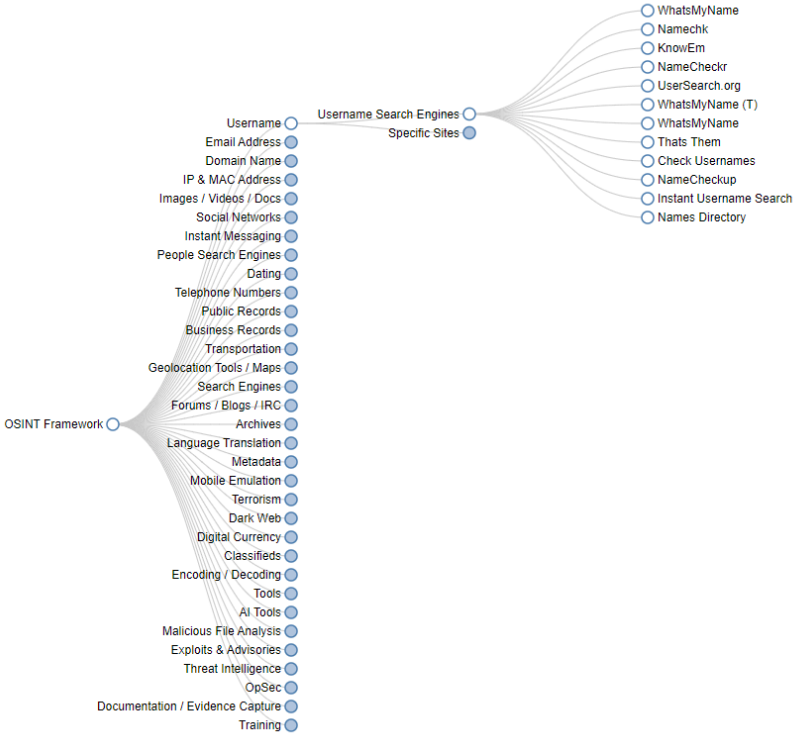
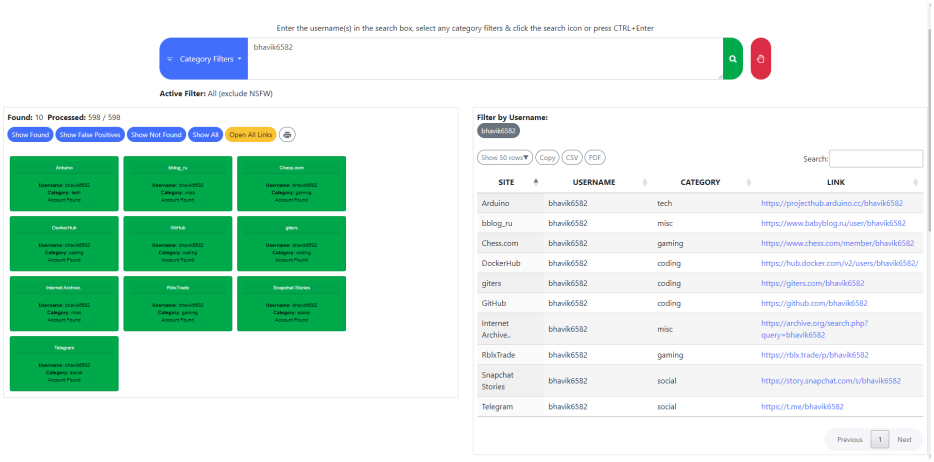


Figure 5.7 Digital Currency

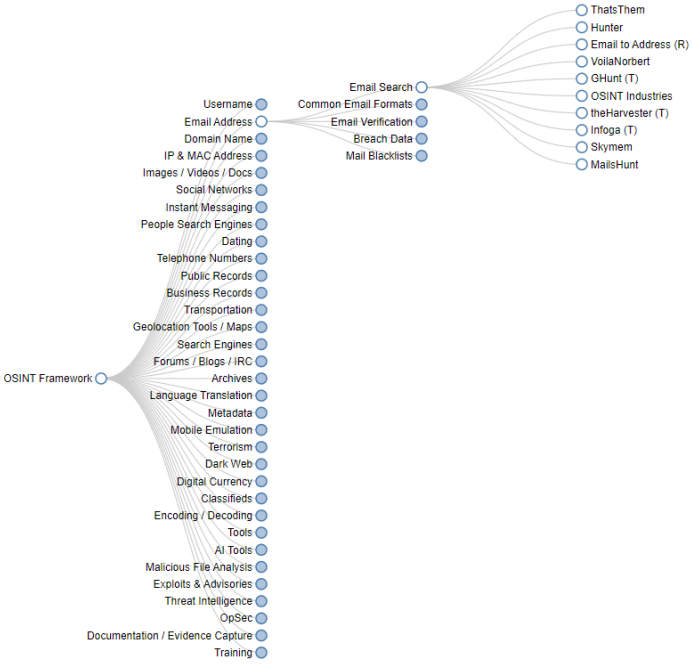
5.7 Simulated output:

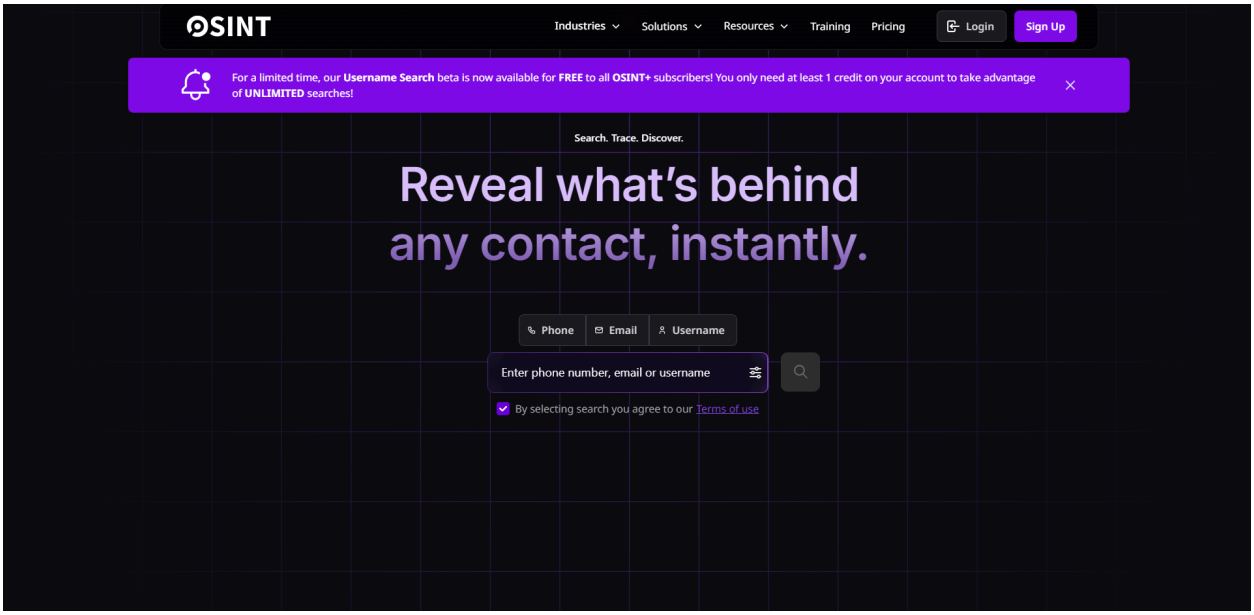
WhatsmyName



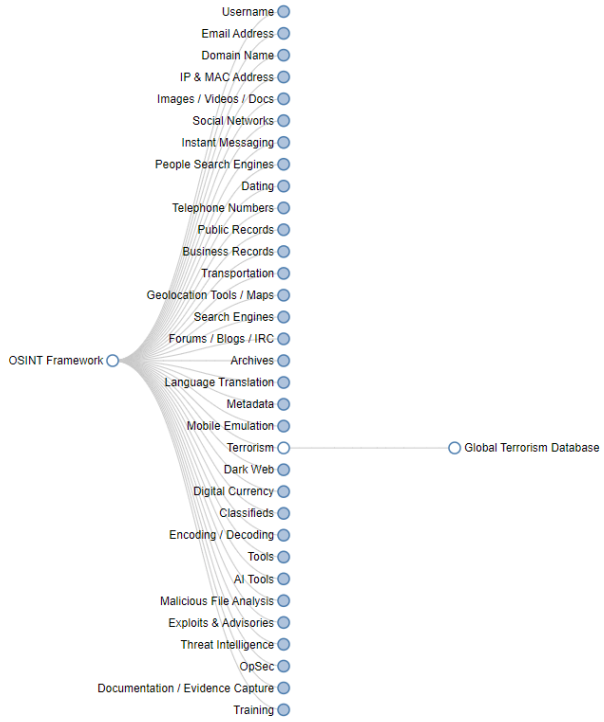


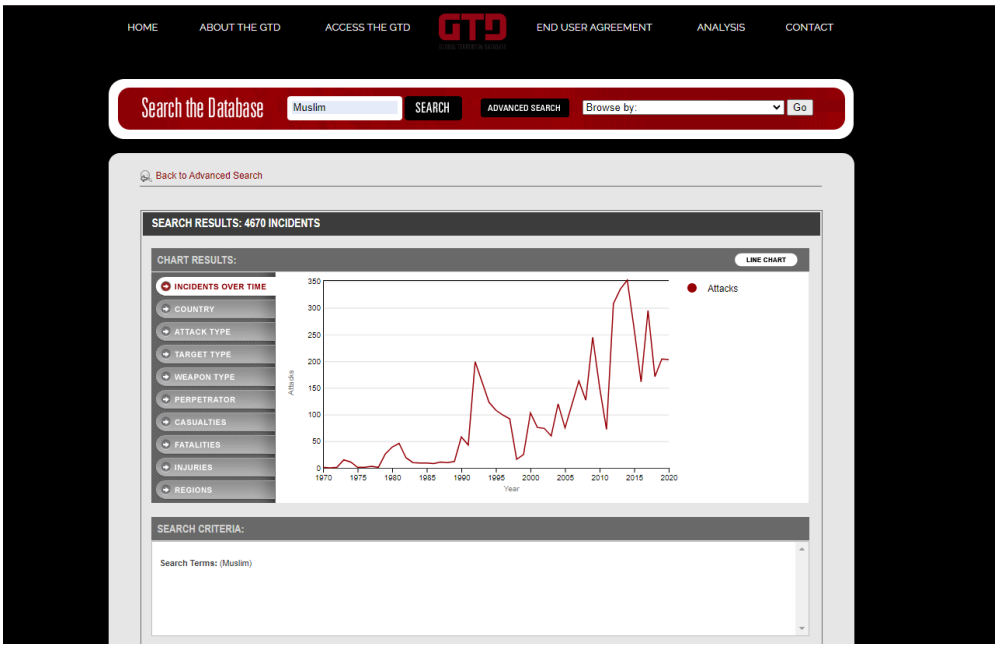
OSINT Industries



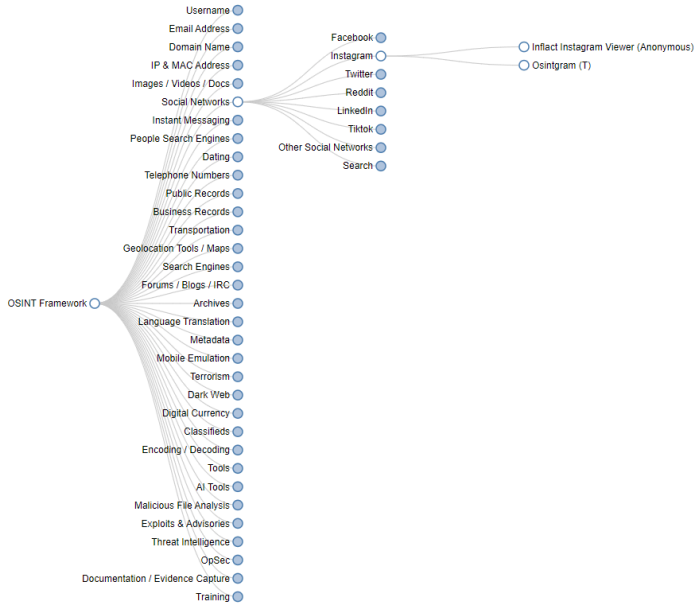


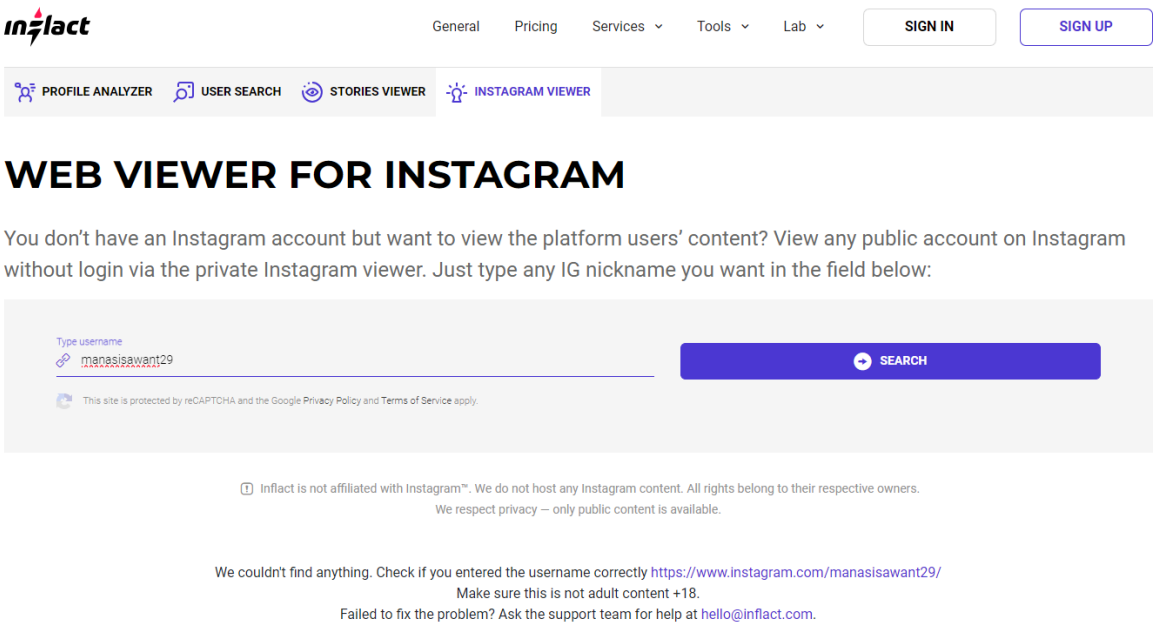
Global Terrorism Database



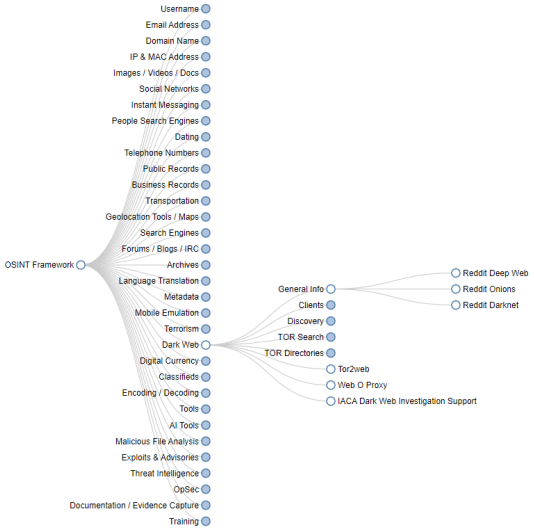


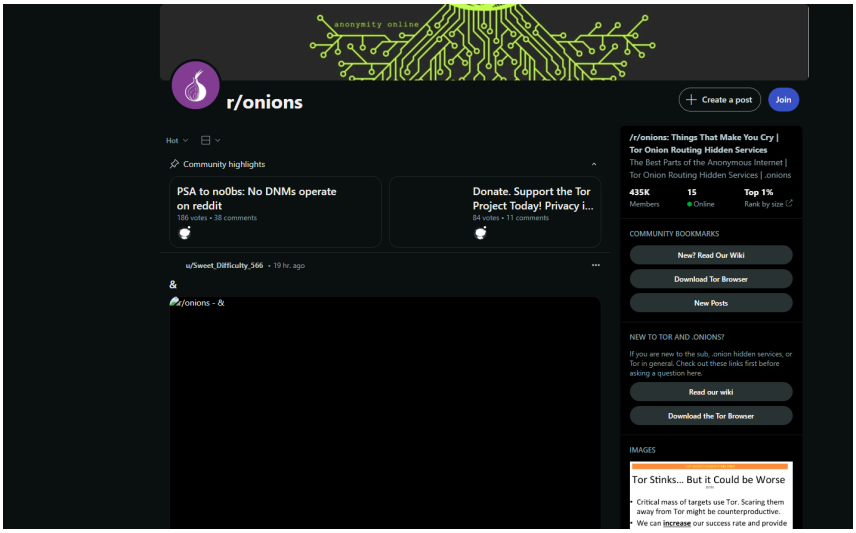
Inflact Instagram Viewer (Anonymous)





Reddit Onions





5.8 Conclusion:

Hence we learned about OSINT Framework

5.9 Questions:

1. Open-source intelligence (OSINT) involves gathering publicly accessible data from sources like:
   -> Social media, Search engines, Public records, Websites and forums

2. The best OSINT tools include:
   -> Maltego, Shodan, TheHarvester, Recon-ng, SpiderFoot

3. The OSINT framework can be used for:
   -> Threat intelligence, Cyber investigations, Competitive analysis, Research