MODULE: 2

Report on : Footprinting / Information gathering

-Atharva Katkar

TABLE OF CONTENTS – FOOTPRINTING

01. Introduction to Foot-printing
02. Foot-printing: A Focused Technique
03. Objectives of Foot-printing
04. Social media-printing
05. Foot-printing Techniques

---

06. Google Dorking
6.1 Footprinting through Search Engines
- Fig 1.1
- Fig 1.2
- Fig 1.3 (Google Hacks)
- Fig 1.4
- Fig 1.5
- Fig 1.6

6.2 Footprinting through Internet Research Services
6.2.1 Netcraft
- Fig 2.1
- Fig 2.2
- Fig 2.3
- Fig 2.4
- Fig 2.5

6.2.2 DNS Dumpster
- Fig 2.6
- Fig 2.7
- Fig 2.8
- Fig 2.9

---

07. Footprinting Through Social Networking Sites
7.1 Sherlock
- Fig 3.1
- Fig 3.2

---

08. Footprinting using WHOIS (GUI)

- WHOIS Lookup
- Fig 4.1
- Fig 4.2
- Fig 4.3

---

09. Footprinting using DNS

9.1 NS Lookup (CLI)

- Fig 5.1
- Fig 5.2
- Fig 5.3
- Fig 5.4

9.2 Kloth DNS / NS Lookup (GUI)

- Fig 5.5
- Fig 5.6
- Fig 5.7
- Fig 5.8

---

10. Network Footprinting

10.1 Tracert (CLI)

- Fig 6.1
- Fig 6.2

10.2 Linux Traceroute (CLI)

- Fig 6.3

---

11. Email Footprinting

11.1 GSA Email Spider

- Fig 7.1
- Fig 7.2
- Fig 7.3

11.2 MX Toolbox

- Fig 7.4
- Fig 7.5
- Fig 7.6
- Fig 7.7
- Fig 7.8
- Fig 7.9

---

12. Footprinting using Various Tools

12.1 Recon-ng

- Fig 8.1
- Fig 8.2
- Fig 8.3
- Fig 8.4
- Fig 8.5

Introduction of Foot-Printing

Foot-printing is the process of gathering information about a target system, network, or organization before conducting any actual hacking attempt. The main goal is to collect as much relevant data as possible to understand the target's structure, potential vulnerabilities, and entry points.

Example: Before trying to break into a building, a burglar might observe security guards' schedules, camera positions, and entry gates. Similarly, a hacker studies the digital "map" of a system through footprinting.

Importance of Foot-printing in Ethical Hacking

Foot-printing is the first and one of the most critical phases in the ethical hacking process. It helps ethical hackers:

1. **Understand the Target** – Knowing the target's systems, networks, and technologies gives a clear picture before testing.
2. **Identify Vulnerabilities Early** – The more information gathered, the easier it is to spot weak points before attackers do.
3. **Plan Attacks Efficiently** – It saves time and effort by focusing only on relevant entry points.
4. **Avoid Detection** – Passive foot-printing methods can collect valuable data without alerting the target.

In short, foot-printing lays the foundation for all further security testing. Without it, ethical hacking would be guesswork.

Foot-printing: A Focused Technique

Foot-printing is a focused part of reconnaissance that involves gathering specific information about a target system or network to assess its security posture. The main objective is to create a detailed profile of the target before performing any attack or vulnerability testing.

Footprinting techniques are broadly classified into two categories:

1. Passive Foot-printing-

This method collects information without directly interacting with the target, so the target remains unaware. Data sources include WHOIS databases, search engines, public websites, social media, and job postings. For example, a job listing for a "Linux Administrator" may reveal the operating systems in use.

2. Active Foot-printing-

This method interacts directly with the target to obtain more detailed data. Common techniques include network scanning, traceroute, DNS zone transfers, and banner grabbing. These methods help identify open ports, running services, and system configurations.

*Common Data Collected and Tools Used-

Data Collected	Tools Used
IP address ranges	Advanced ip scanner
Subdomains	Sublist3r, theHarvester
Domain registrars and WHOIS info	Whois Lookup tools
Domains Or Subdomains	Maltego
Usernames and email addresses	theHarvester,GSA Email Spider
Network paths and hops	Traceroute

Objectives of Foot-printing

Foot-printing is the very first step in ethical hacking. Its purpose is to gather as much information as possible about a target system or network. This helps in understanding the structure and discovering potential weaknesses before any testing begins.

1. Gathering Information About the Target

- Collect maximum details about the target's systems, networks, and employees.
- Examples of information collected: domain names, IP addresses, server details, contact info, social media data, DNS records.

2. Identifying the Security Posture

- To analyze the strengths and weaknesses of the target's security setup.
- Example: Discovering old software versions, unpatched servers, or weak firewall configurations.

3. Determining the Network Range

- To map out the network topology and find IP address ranges.
- Example: Using tools like Nmap to check active systems.

4. Identifying Active Machines and Services

- To find out which systems are running and what services (ports, applications) are available.
- Example: Detecting open ports like 21 (FTP), 80 (HTTP), 443 (HTTPS), 3386 (RDP).

5. Mapping the Target's Infrastructure

- To create a blueprint of the organization's network, servers, and technologies.
- Includes details of operating systems, web technologies, VPN gateways, cloud usage, etc.

6. Identifying Vulnerabilities

- To detect loopholes that can be exploited.
- Example: Unpatched software, misconfigured services, weak passwords, or outdated SSL certificates.

7. Collecting Employee s Organizational Information

- To gather personal and professional information about staff.
- Example: Names, emails, job roles, phone numbers from LinkedIn, company websites, or directories.

8. Assessing the Target's External Threat Landscape

- To understand what information is publicly accessible and how dangerous it could be if misused.
- Example: Leaked documents, code repositories, public-facing misconfigurations.

G. Establishing a Profile of the Target

- To create a comprehensive report about the target's assets, weaknesses, and possible attack vectors.
- This profile is the base for penetration testing, red teaming, or cyber-attack planning.

10. Planning Further Attacks or Defenses

- For attackers: Helps in designing strategies to exploit discovered weaknesses.
- For defenders: Helps in hardening security by fixing vulnerabilities before they are misused.

Social Media Foot-printing

What is Social Media Foot-printing?

Social Media Foot-printing means collecting information about a target by exploring their social media profiles. Platforms like LinkedIn, Facebook, Twitter, and Instagram often contain useful details such as employee names, email addresses, job titles, company structure,
locations, and even technology stacks.

Why use Social Media Foot-printing in Ethical Hacking?

Ethical hackers use social media to gather public information that can help build a profile of the target organization or individuals. This info is useful for identifying potential points of entry, understanding the company's structure, and planning social engineering attacks safely and legally.

What attackers look for:

1. Employee names, job titles, and emails.
2. Photos/videos revealing location or devices.
3. Company events, product launches, or security policies.

Risk:

1. Social engineering attacks (phishing, impersonation).
2. Password guessing using personal details.
3. Mapping organizational hierarchy.

Example: A hacker could use LinkedIn to find IT staff, then craft phishing emails pretending to be from HR.

GOOGLE DORKING

1. Footprinting through Search Engines:

Footprinting through search engines is a passive reconnaissance technique where attackers or ethical hackers gather information about a target by utilizing search engines like Google, Bing, or DuckDuckGo.

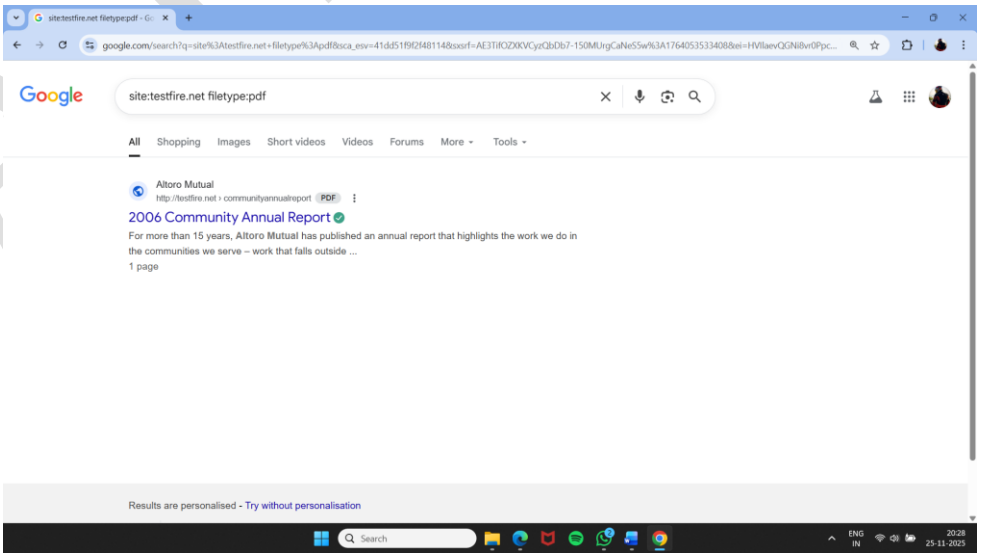
Objectives -: • Searching Cached Pages
• Finding Exposed Directories
• Extracting Metadata from Files
• Identifying Sensitive Information
• Gathering Email Addresses
• Discovering Subdomains
• Checking Indexed Pages

1) Gather Information using Advanced Google Hacking Techniques

- site:testfire.net filetype:pdf

The **filetype**: search operator is a powerful Google search tool that helps you find specific file types on the web. It's useful when searching for documents, presentations, spreadsheets, and more.

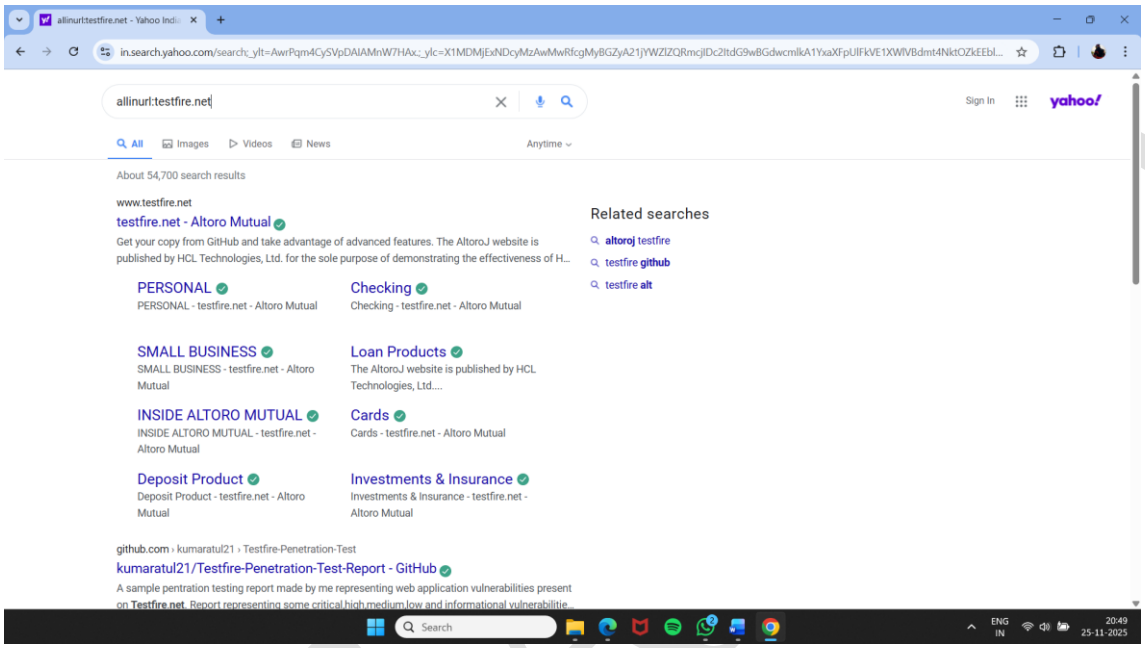
Note-: You can also give other filetypes like .XLS , .DOCX



Fig(1.1)

- allinurl:testfire.net

The **allinurl**: operator is a Google search tool that helps you find web pages containing specific keywords in their URL. This is especially useful for discovering targeted content like portals, login pages, or directories.



Fig(1.2)

- cache:testfire.net

The **cache:** operator allows you to view cached version of the web page. The query returns the cached version of the website testfire.net.

- allintitle:testfire.net

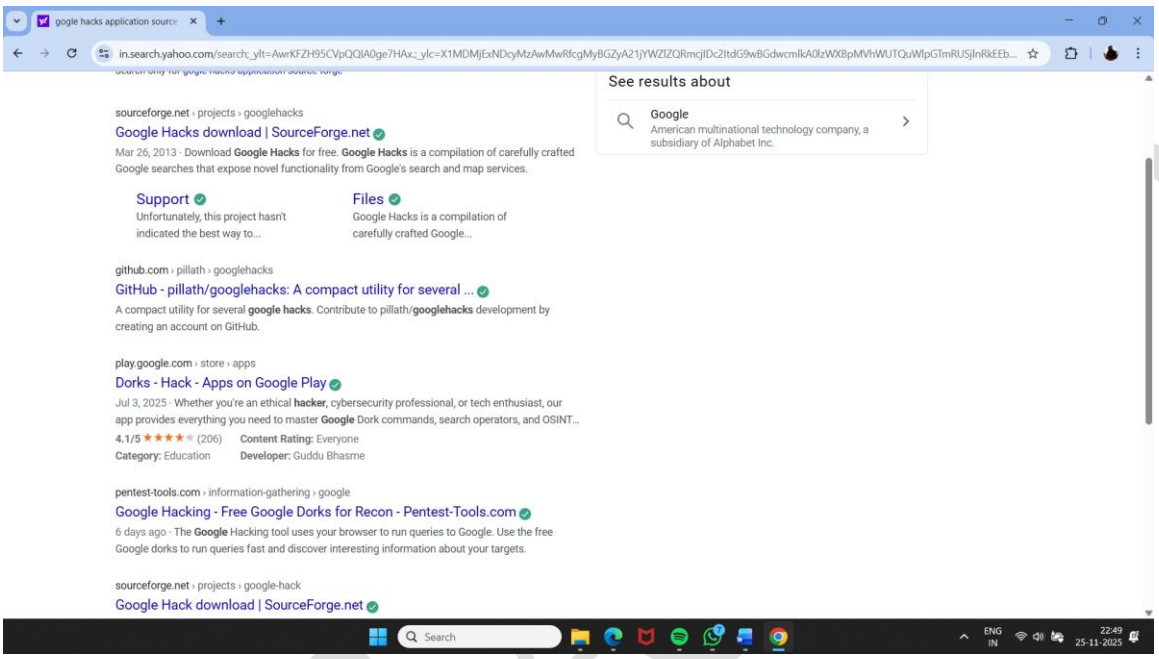
The **allintitle:** operator restricts results to pages containing all the query terms specified in the title. Query returns only pages containing the words "detect" and "malware" in the title.

- location:testfire.net

The **location:** operator finds information for a specific location. Query give you results based around the term EC-Council.

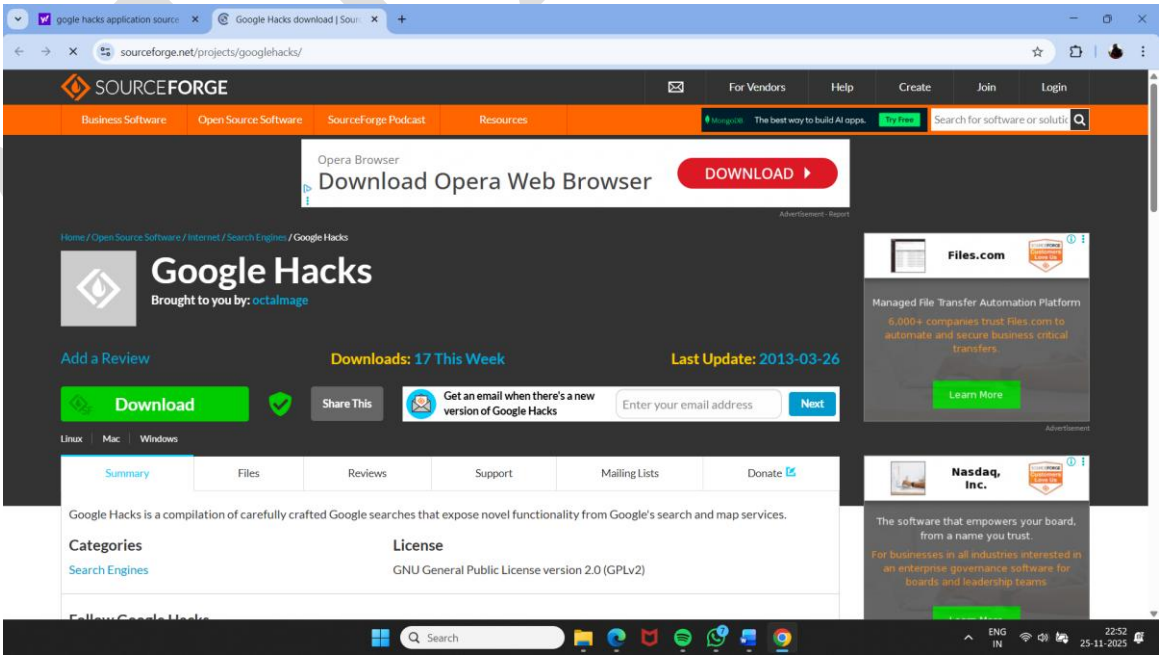
2) Gather Information Using Google hacks application.

Step 1 - : search Google hacks application
Step 2 -: open sourceforge Website



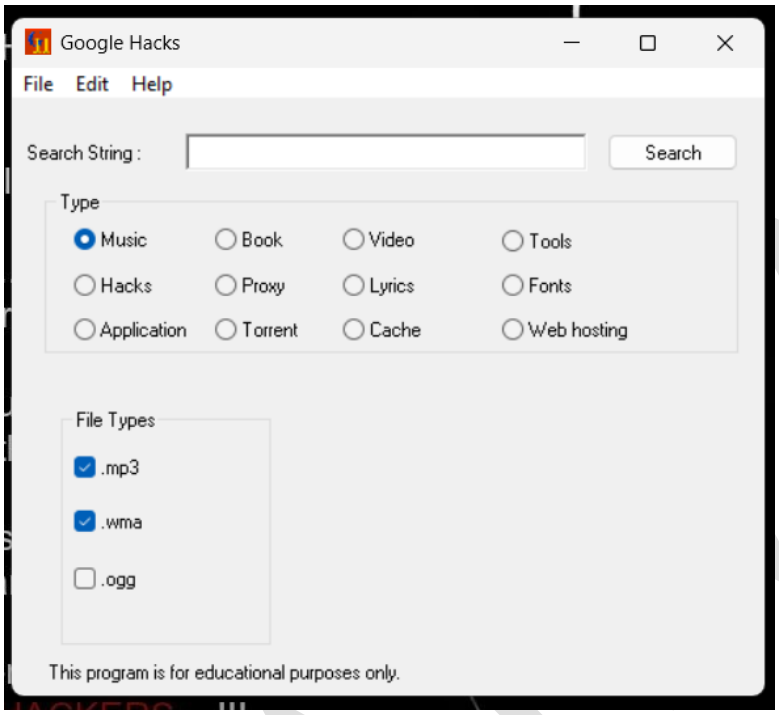
Fig(1.3)

Step 3 -: click on download button (Latest Verison).



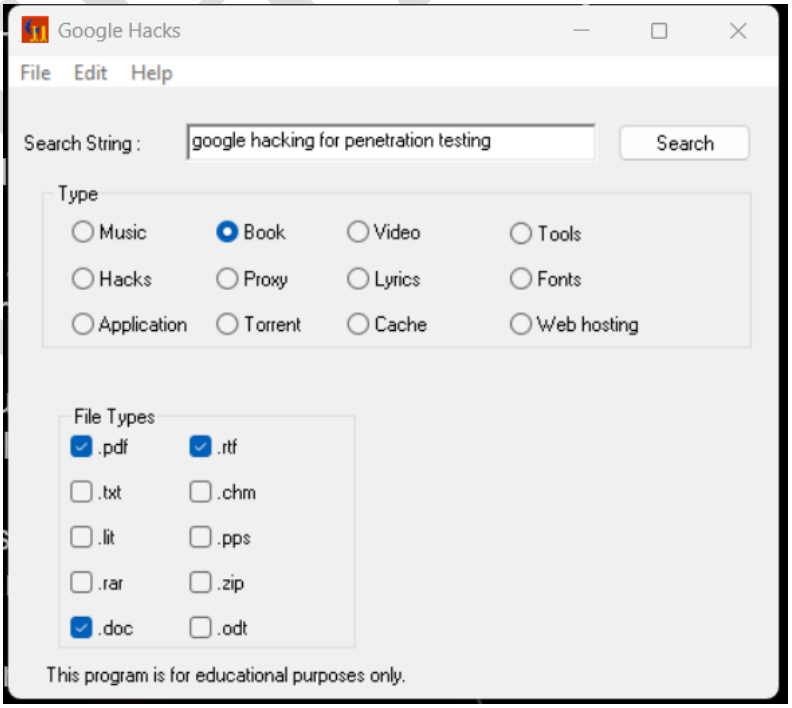
Fig(1.4)

Step 4 -: After downloading the application , install and open it.



Fig(1.5)

Step 5:- Now You can perform all the activity that you perform using web browser (like intitle , site and other switches)



Fig(1.6)

2.Footprinting through internet research services.

Performing footprinting through internet research services means using publicly available online information and tools to gather as much data as possible about a target system or network for security analysis. This is often done in the early stages of a penetration test to identify potential vulnerabilities without directly attacking the system, and it includes finding details like IP addresses, network topology, user information, and active services.

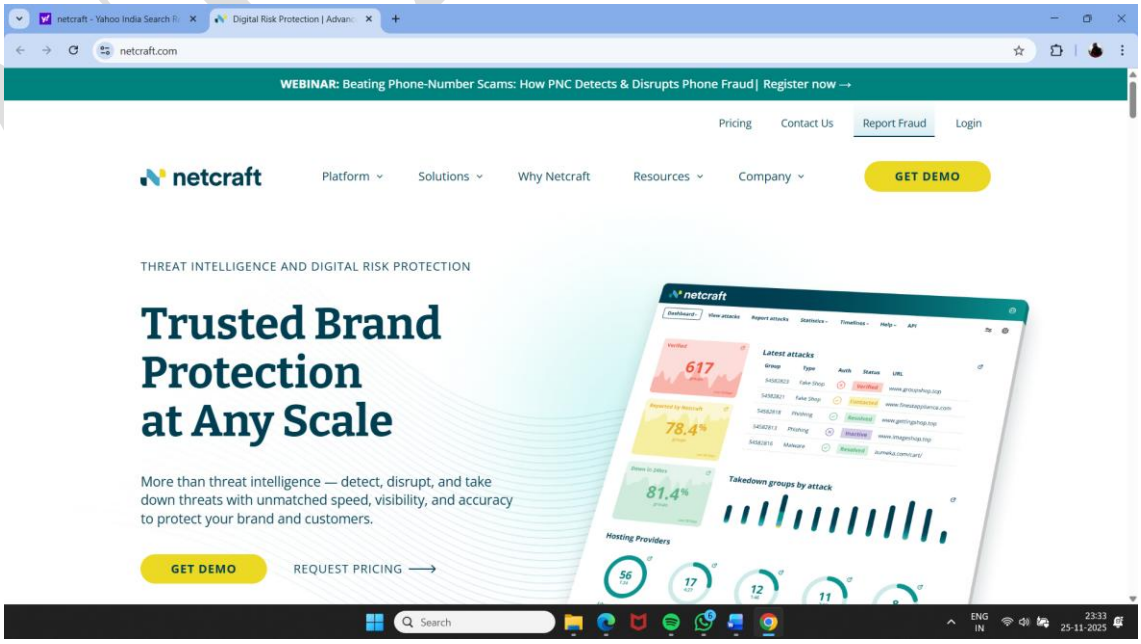
How it works:
1)Automated tools: Researchers use various online tools to scan for information, such as open ports, and identify the services running on a target system.

2)Network mapping: Techniques are used to create a map of the target's network topology, showing how different systems are connected.

3)Public data mining: Information is collected from public sources, including DNS records, company websites, social media, and other public-facing data.

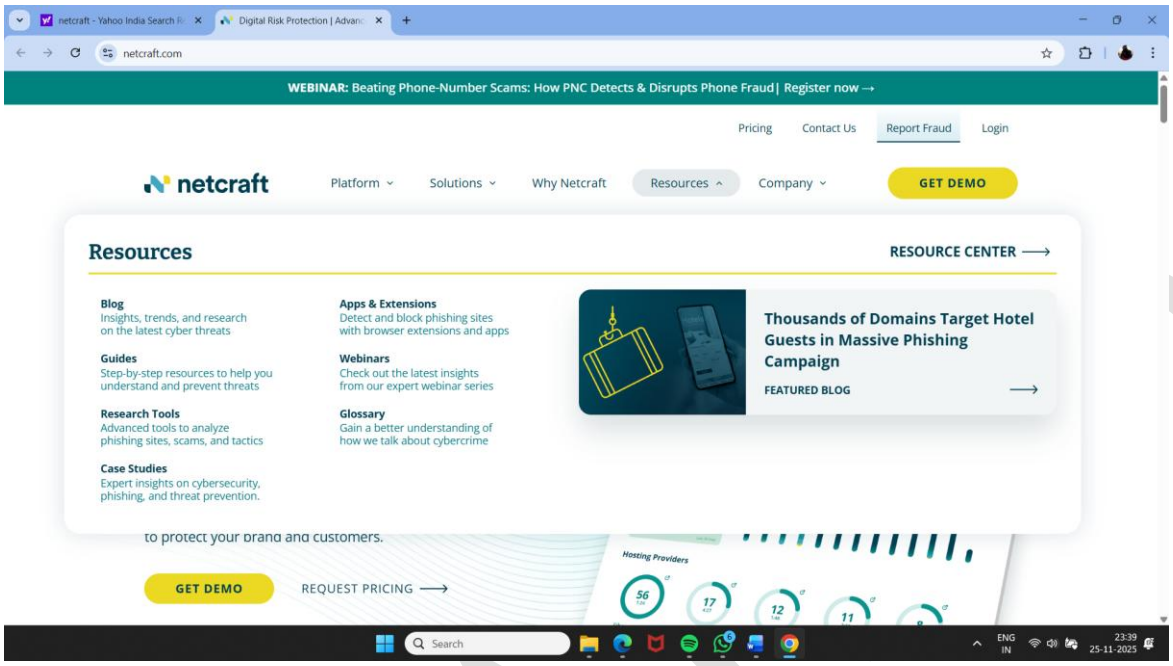
1) Footprinting Using NetCraft

Step 1: Go to https://www.netcraft.com.



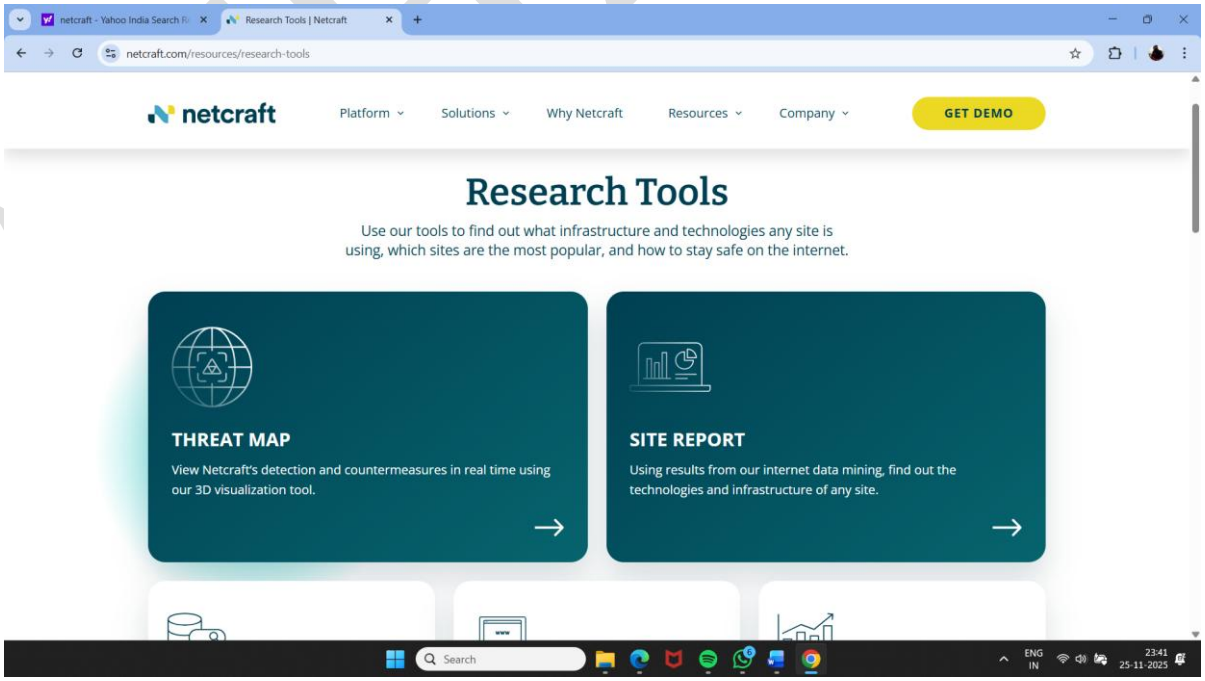
Fig(2.1)

Step 2: Click on Resources and click on research tools.



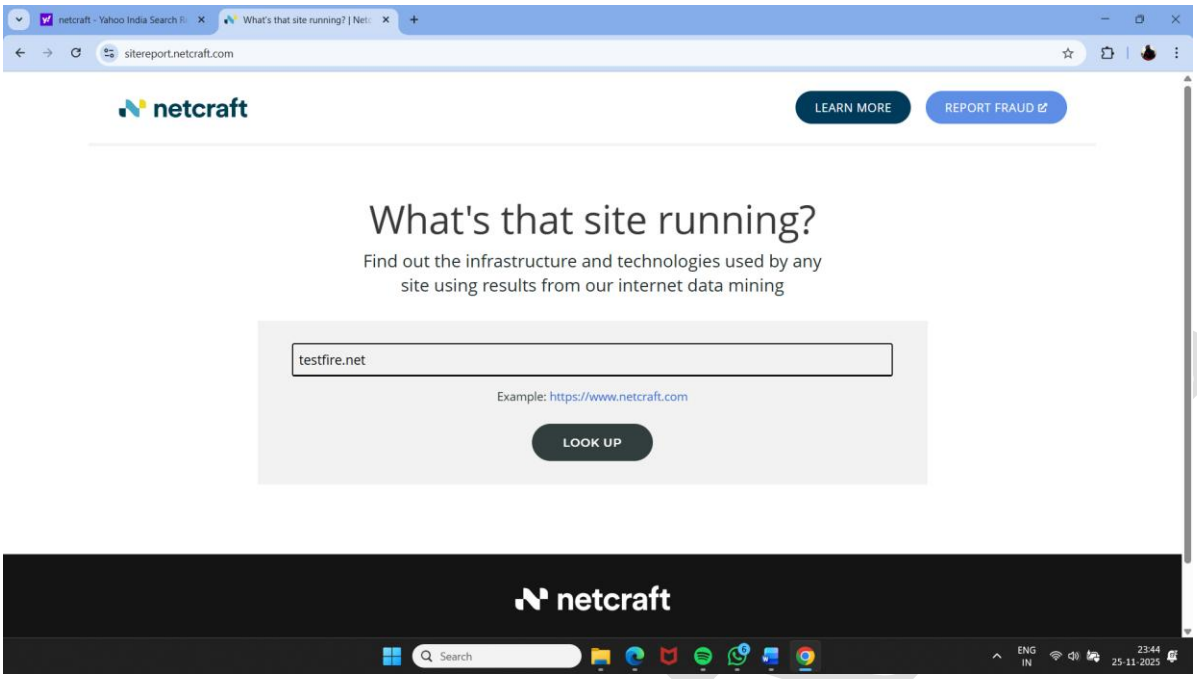
Fig(2.2)

Step 3: Click on site report.



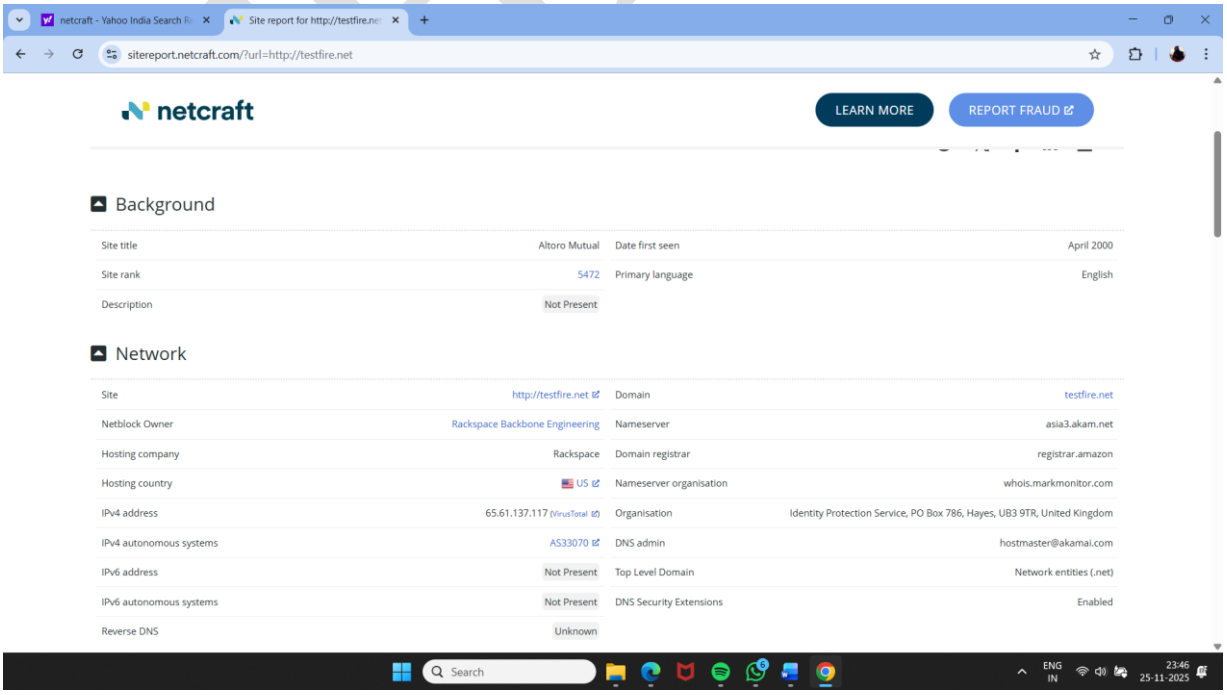
Fig(2.3)

Step 4: Provide Domain name & click on lookup.



Fig(2.4)

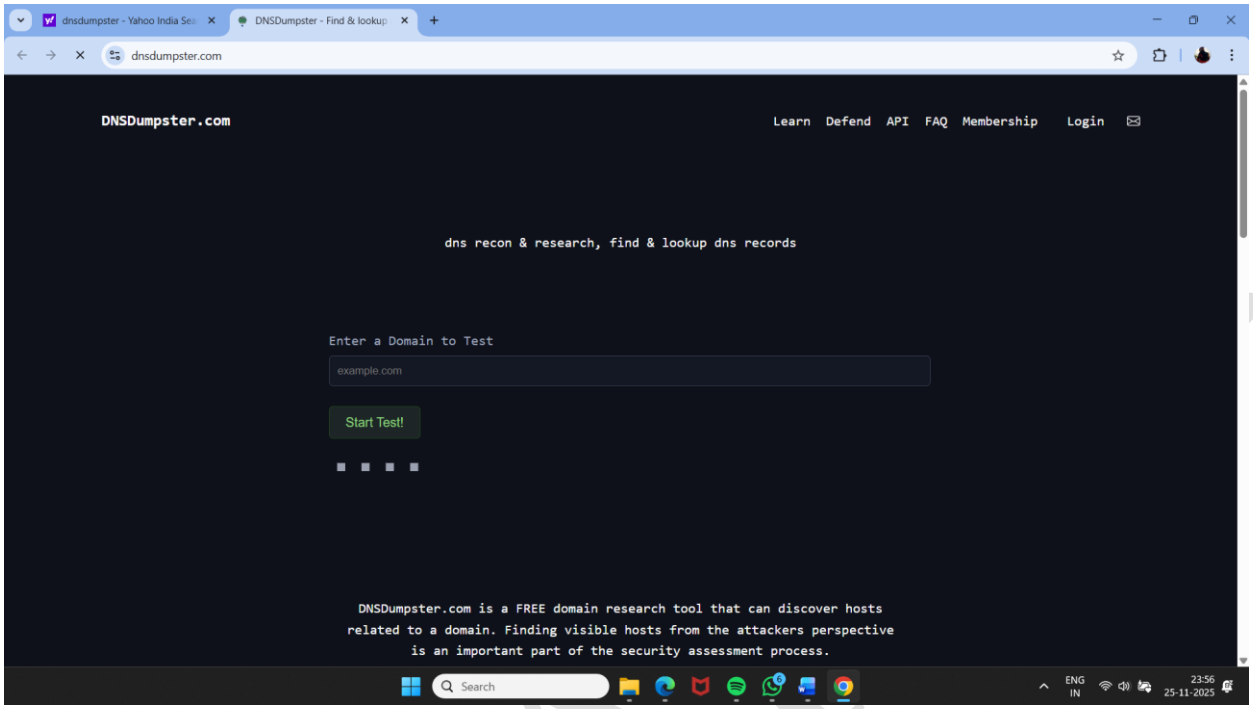
Step 5: It will give you full site report.



Fig(2.5)

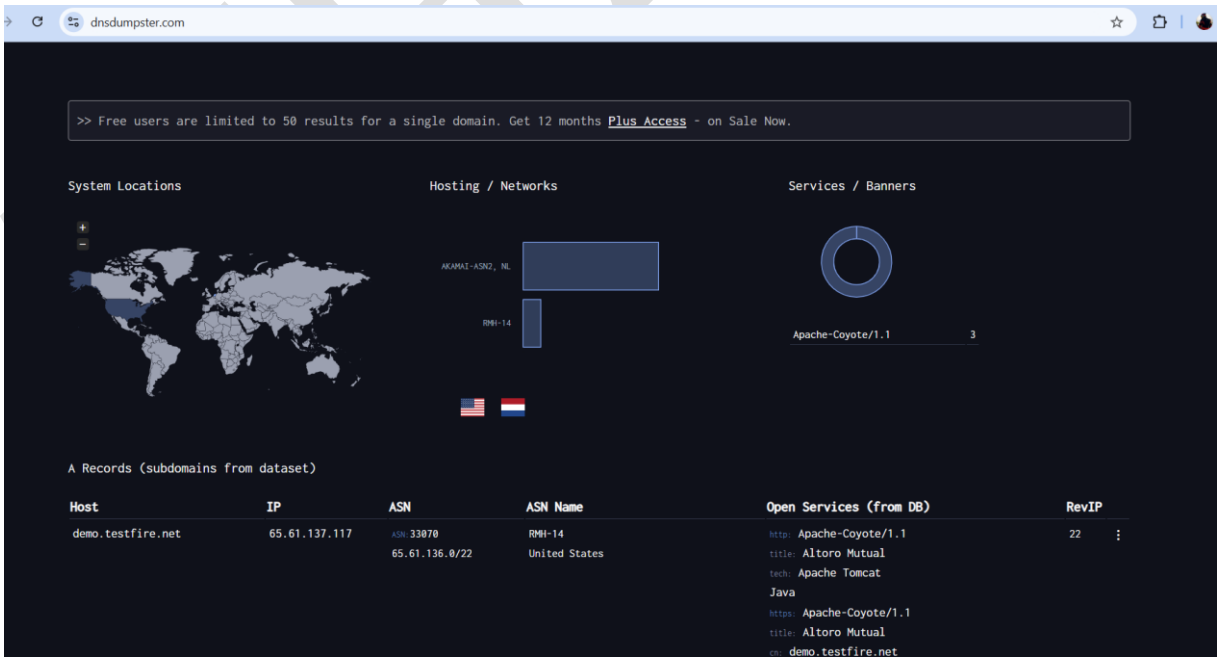
2) Footprinting Using DNS dumpster.

Step 1: Go to https://dnsdumpster.com/



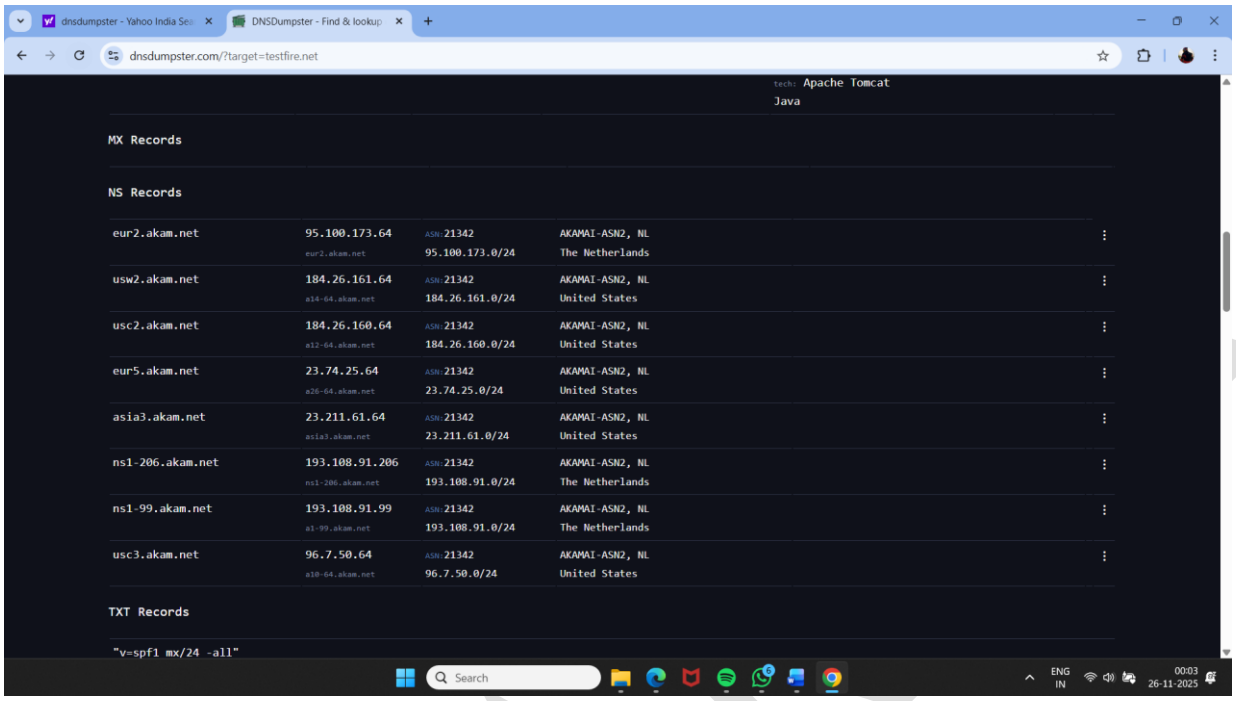
Fig(2.6)

Step 2: Provide Domain name & click on start test.



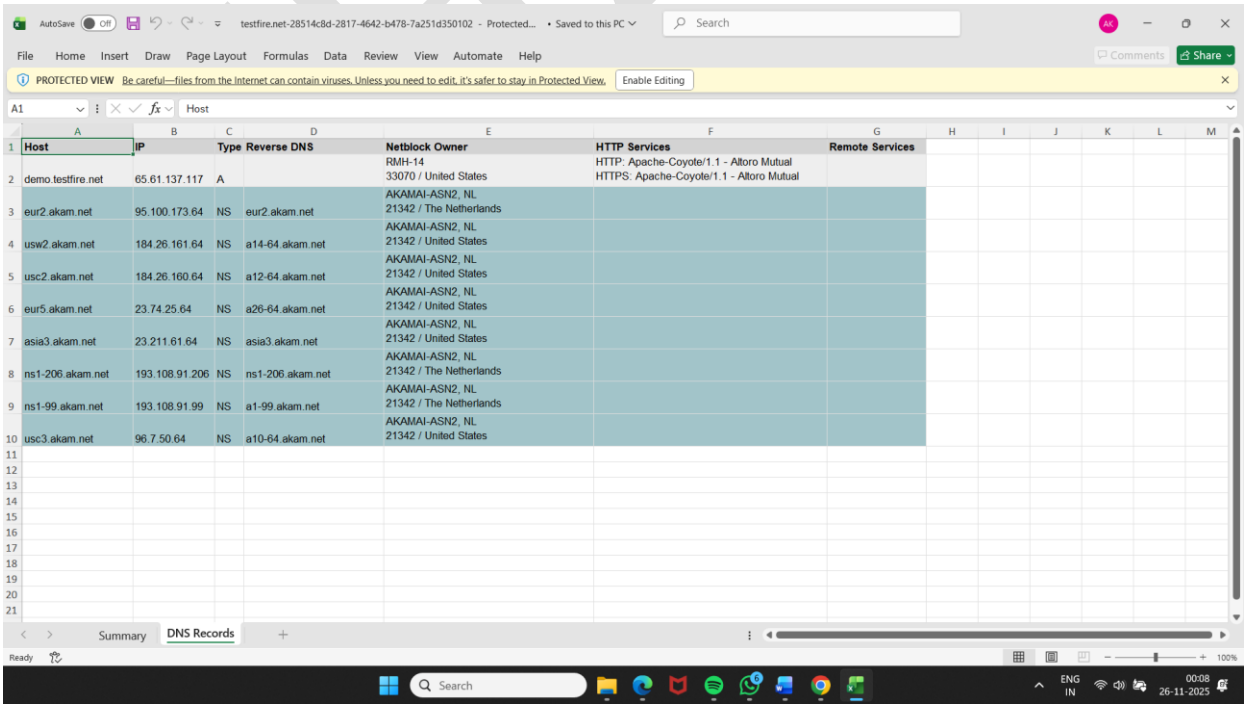
Fig(2.7)

Step 3: Scroll down to see MX records ,TXT records along with their ip addresses.



Fig(2.8)

Step 4: Click on Download .xlsx of Hosts button to download the list of hosts.



Host	IP	Type	Reverse DNS	Netblock Owner	HTTP Services	Remote Services
demo.testfire.net	65.61.137.117	A		RMH-14 33070 / United States	HTTP: Apache-Coyote/1.1 - Altoro Mutual HTTPS: Apache-Coyote/1.1 - Altoro Mutual	
eur2.akam.net	95.100.173.64	NS	eur2.akam.net	AKAMAI-ASN2, NL 21342 / The Netherlands		
usw2.akam.net	184.26.161.64	NS	a14-64.akam.net	AKAMAI-ASN2, NL 21342 / United States		
usc2.akam.net	184.26.160.64	NS	a12-64.akam.net	AKAMAI-ASN2, NL 21342 / United States		
eur5.akam.net	23.74.25.64	NS	a26-64.akam.net	AKAMAI-ASN2, NL 21342 / United States		
asia3.akam.net	23.211.61.64	NS	asia3.akam.net	AKAMAI-ASN2, NL 21342 / United States		
ns1-206.akam.net	193.108.91.206	NS	ns1-206.akam.net	AKAMAI-ASN2, NL 21342 / The Netherlands		
ns1-99.akam.net	193.108.91.99	NS	a1-99.akam.net	AKAMAI-ASN2, NL 21342 / The Netherlands		
usc3.akam.net	96.7.50.64	NS	a10-64.akam.net	AKAMAI-ASN2, NL 21342 / United States		

Fig(2.9)

3.Footprinting Through Social Networking Sites

Performing footprinting through social networking sites is the process of gathering publicly available information about a target from social media platforms like LinkedIn, Facebook, and Twitter to understand their digital footprint. This is a form of passive reconnaissance used in ethical hacking and security assessments to find details such as employee names, job titles, locations, technology mentions in posts, and relationship maps between individuals. The information is then used for social engineering or to identify potential vulnerabilities in an organization's infrastructure**.**

How it works

1) Identifying targets: Locating official company pages and employee profiles, and identifying key personnel like executives or IT staff.

2) Extracting information: Analyzing profiles for details like job titles, locations, and professional history; reviewing posts for mentions of technology or events; and examining photos for clues about office layouts or security measures.

3) Mapping relationships: Creating a network map of employee connections, which can reveal organizational hierarchies, partners, and communication structures.

1) Social Media Footprinting Using Sherlock (CLI)

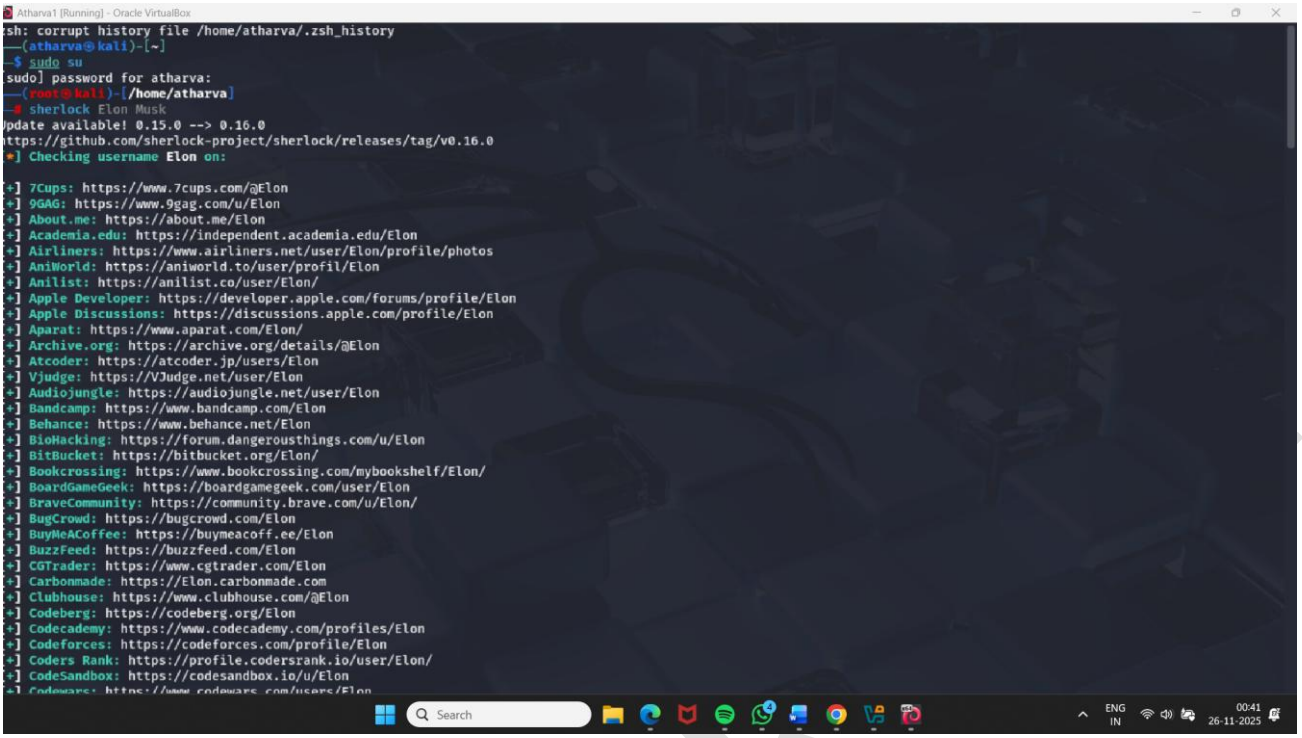
Step 1: Open Kali linux / Parrot OS.

Step 2: Open Terminal.

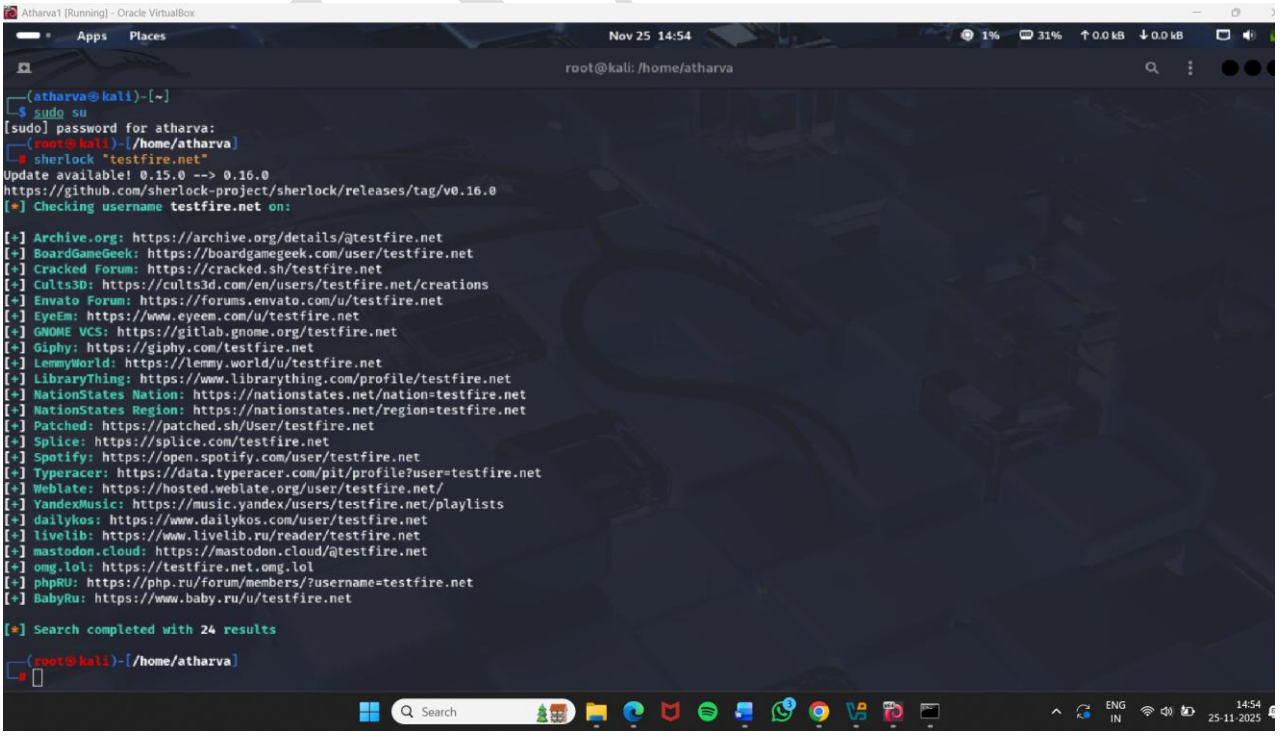
Step 3: Type apt install sherlock on terminal.

Step 4: It will install sherlock.

Step 4: After installing sherlock type username that you want to find social media accounts.
Example -: sherlock Elon Musk


Atharva1 [Running] - Oracle VirtualBox
zsh: corrupt history file /home/atharva/.zsh_history
(atharva㉿kali)-[~]
$ sudo su
[sudo] password for atharva:
(root㉿kali)-[/home/atharva]
sherlock Elon Musk
Update available! 0.15.0 --> 0.16.0
https://github.com/sherlock-project/sherlock/releases/tag/v0.16.0
[*] Checking username Elon on:
[+] 7Cups: https://www.7cups.com/@Elon
[+] 9GAG: https://www.9gag.com/u/Elon
[+] About.me: https://about.me/Elon
[+] Academia.edu: https://independent.academia.edu/Elon
[+] Airliners: https://www.airliners.net/user/Elon/profile/photos
[+] AniWorld: https://aniworld.to/user/profil/Elon
[+] Anilist: https://anilist.co/user/Elon/
[+] Apple Developer: https://developer.apple.com/forums/profile/Elon
[+] Apple Discussions: https://discussions.apple.com/profile/Elon
[+] Aparat: https://www.aparat.com/Elon/
[+] Archive.org: https://archive.org/details/@Elon
[+] Atcoder: https://atcoder.jp/users/Elon
[+] Vjudge: https://VJudge.net/user/Elon
[+] Audiojungle: https://audiojungle.net/user/Elon
[+] Bandcamp: https://www.bandcamp.com/Elon
[+] Behance: https://www.behance.net/Elon
[+] BioHacking: https://forum.dangerousthings.com/u/Elon
[+] BitBucket: https://bitbucket.org/Elon/
[+] Bookcrossing: https://www.bookcrossing.com/mybookshelf/Elon/
[+] BoardGameGeek: https://boardgamegeek.com/user/Elon
[+] BraveCommunity: https://community.brave.com/u/Elon/
[+] BugCrowd: https://bugcrowd.com/Elon
[+] BuyMeACoffee: https://buymeacoff.ee/Elon
[+] BuzzFeed: https://buzzfeed.com/Elon
[+] CGTrader: https://www.cgtrader.com/Elon
[+] Carbonmade: https://Elon.carbonmade.com
[+] Clubhouse: https://www.clubhouse.com/@Elon
[+] Codeberg: https://codeberg.org/Elon
[+] Codecademy: https://www.codecademy.com/profiles/Elon
[+] Codeforces: https://codeforces.com/profile/Elon
[+] Coders Rank: https://profile.codersrank.io/user/Elon/
[+] CodeSandbox: https://codesandbox.io/u/Elon
Search
ENG IN
00:41 26-11-2025

Fig(3.1)


Atharva1 [Running] - Oracle VirtualBox
Apps Places
Nov 25 14:54
1% 31% 0.0 kB 0.0 kB
root@kali: /home/atharva
(atharva㉿kali)-[~]
$ sudo su
[sudo] password for atharva:
(root㉿kali)-[/home/atharva]
sherlock "testfire.net"
Update available! 0.15.0 --> 0.16.0
https://github.com/sherlock-project/sherlock/releases/tag/v0.16.0
[*] Checking username testfire.net on:
[+] Archive.org: https://archive.org/details/@testfire.net
[+] BoardGameGeek: https://boardgamegeek.com/user/testfire.net
[+] Cracked Forum: https://cracked.sh/testfire.net
[+] Cults3D: https://cults3d.com/en/users/testfire.net/creations
[+] Envato Forum: https://forums.envato.com/u/testfire.net
[+] EyeEm: https://www.eyeem.com/u/testfire.net
[+] GNOME VCS: https://gitlab.gnome.org/testfire.net
[+] Giphy: https://giphy.com/testfire.net
[+] LemmyWorld: https://lemmy.world/u/testfire.net
[+] LibraryThing: https://www.librarything.com/profile/testfire.net
[+] NationStates Nation: https://nationstates.net/nation=testfire.net
[+] NationStates Region: https://nationstates.net/region=testfire.net
[+] Patched: https://patched.sh/User/testfire.net
[+] Splice: https://splice.com/testfire.net
[+] Spotify: https://open.spotify.com/user/testfire.net
[+] Typeracer: https://data.typeracer.com/pit/profile?user=testfire.net
[+] Weblate: https://hosted.weblate.org/user/testfire.net/
[+] YandexMusic: https://music.yandex/users/testfire.net/playlists
[+] dailykos: https://www.dailykos.com/user/testfire.net
[+] livelib: https://www.livelib.ru/reader/testfire.net
[+] mastodon.cloud: https://mastodon.cloud/@testfire.net
[+] omg.lol: https://testfire.net.omg.lol
[+] phpRU: https://php.ru/forum/members/?username=testfire.net
[+] BabyRu: https://www.baby.ru/u/testfire.net
[*] Search completed with 24 results
(root㉿kali)-[/home/atharva]
Search
ENG IN
14:54 25-11-2025

Fig(3.2)

4. Footprinting using WHOIS (GUI)

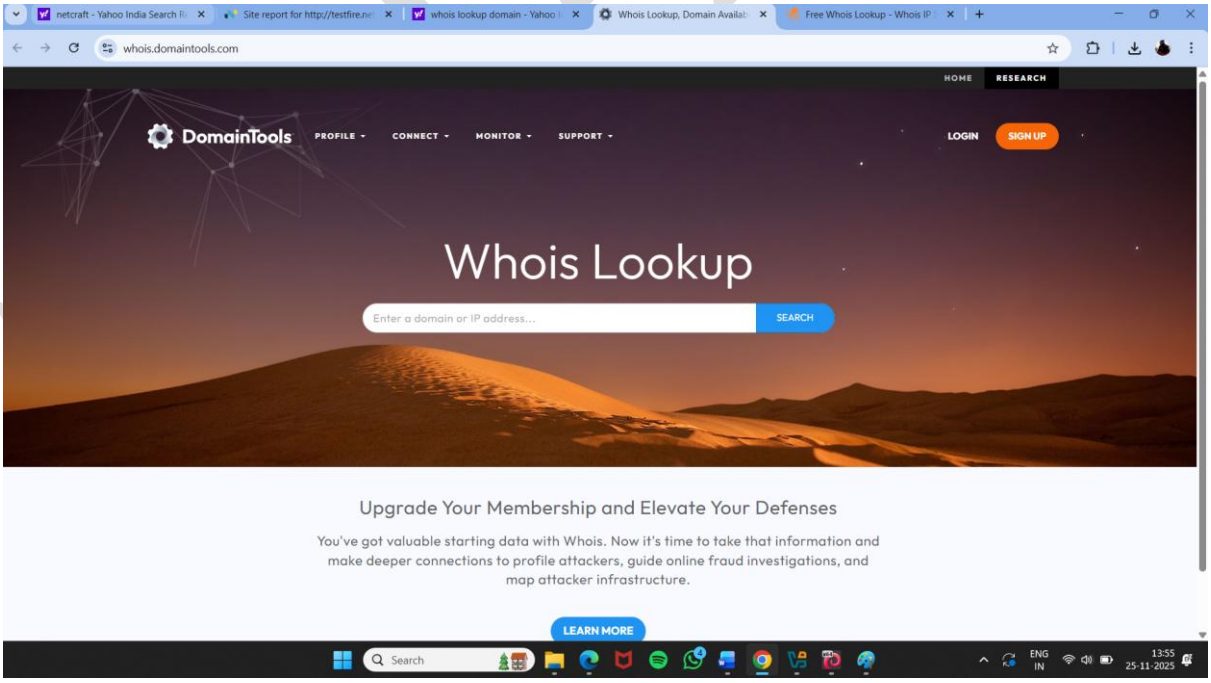
Footprinting using WHOIS lookup means gathering information about a target domain or IP address by querying the WHOIS database, which stores ownership and administrative details about registered domains.
It is a common step in reconnaissance (information gathering) for ethical hacking, penetration testing, or cybersecurity analysis.

A WHOIS lookup can provide:

- Registrant details (owner name, organization)
- Administrative and technical contact info
- Domain registration and expiration dates
- Registrar name
- Name servers
- Domain status
- Contact email for abuse or support

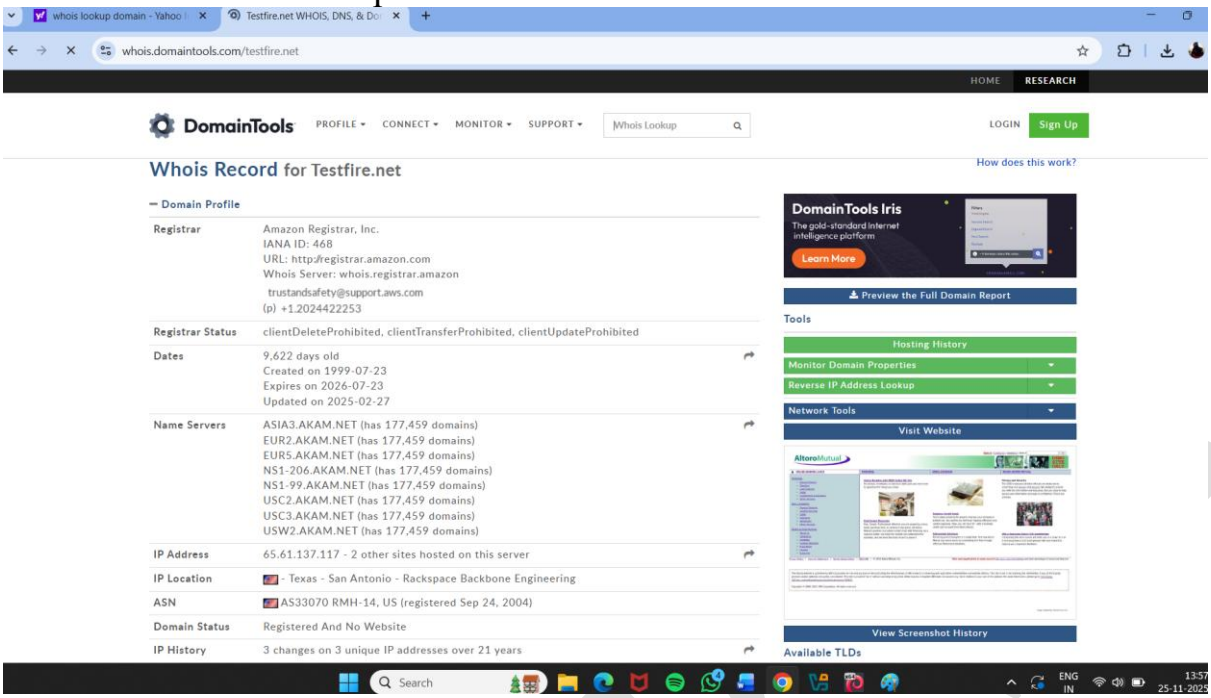
1) Footprinting using WHOIS (GUI) –

Step 1: Open Browser & Search WHOIS



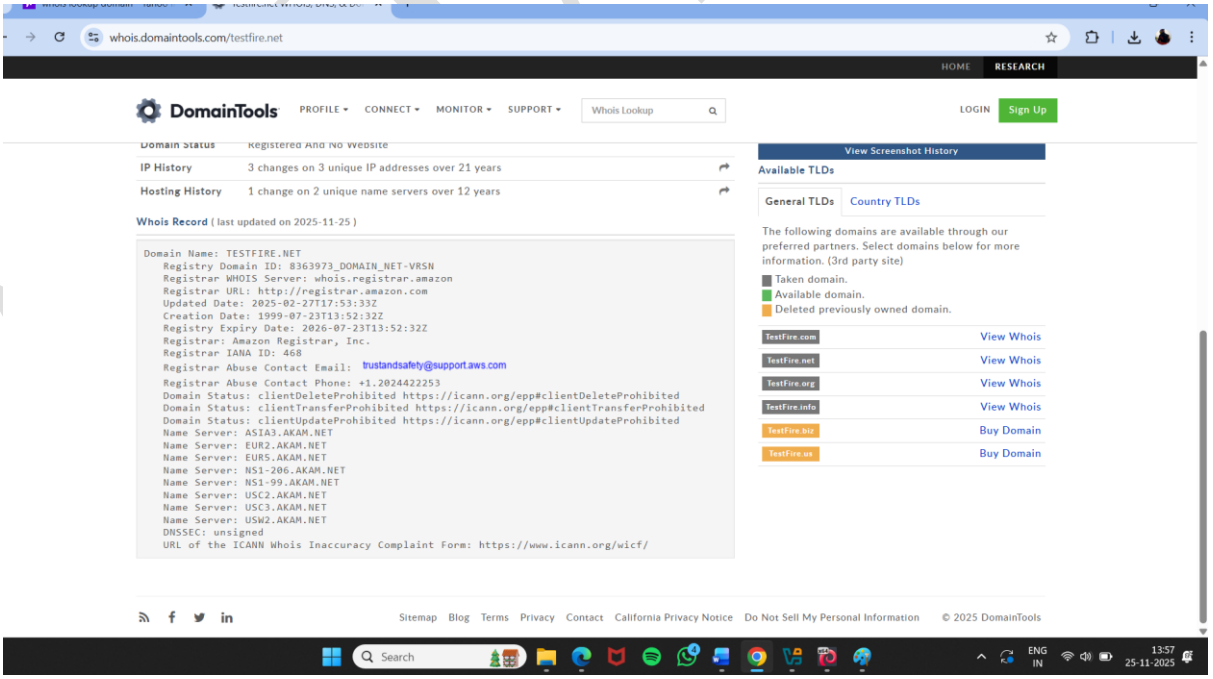
Fig(4.1)

Step 2: Search Domain name or ip address.



Fig(4.2)

This search result reveals the details associated with the URL entered, testfire.net , which includes organizational details such as registration details, name servers, IP address, location, etc.



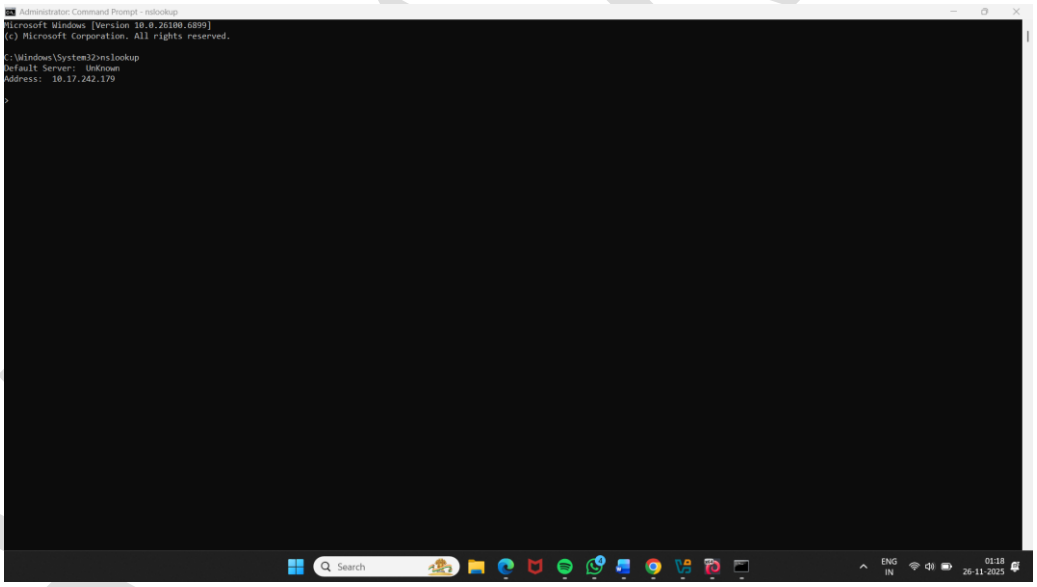
Fig(4.3)

5. DNS Footprinting

DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all IP addresses of the required application. DNS helps in converting the IP address to a more easily understandable domain format, which eases the burden on human beings.
DNS footprinting is the process of collecting information about a target organization or domain by querying the Domain Name System (DNS). It is an early stage of reconnaissance in ethical hacking or penetration testing, helping you understand the network infrastructure before any active testing.

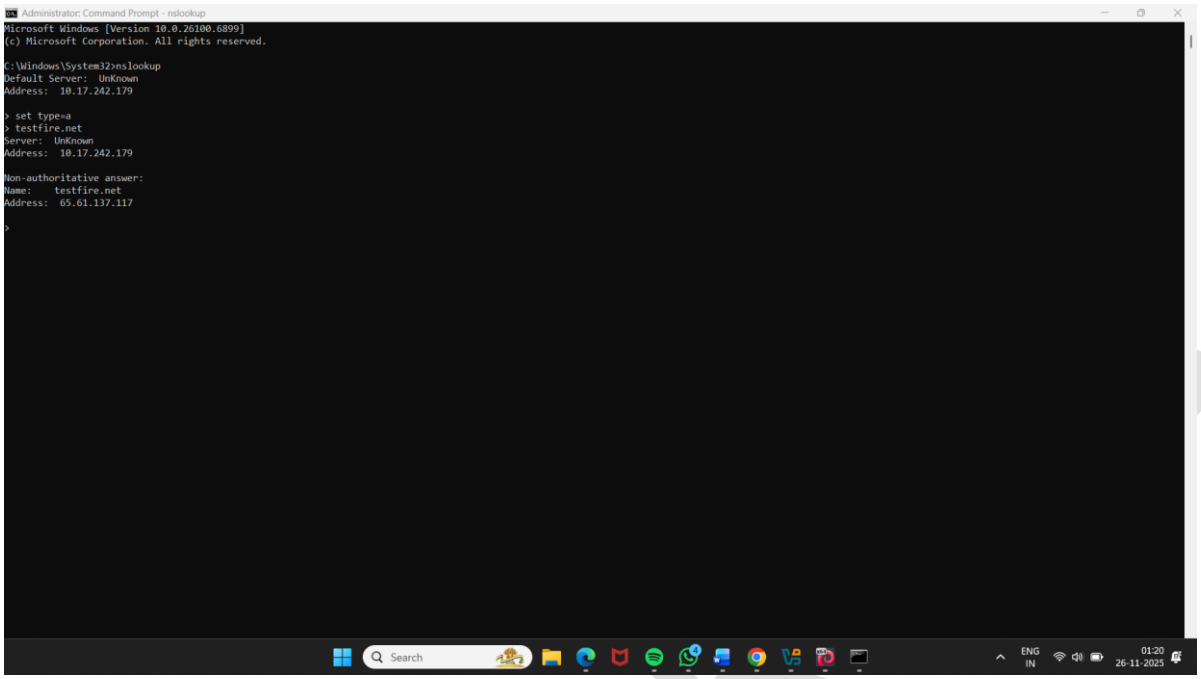
1) DNS Information using nslookup Command Line Utility and Online Tool

Step1: launch Command Prompt, and run nslookup command.



Fig(5.1)

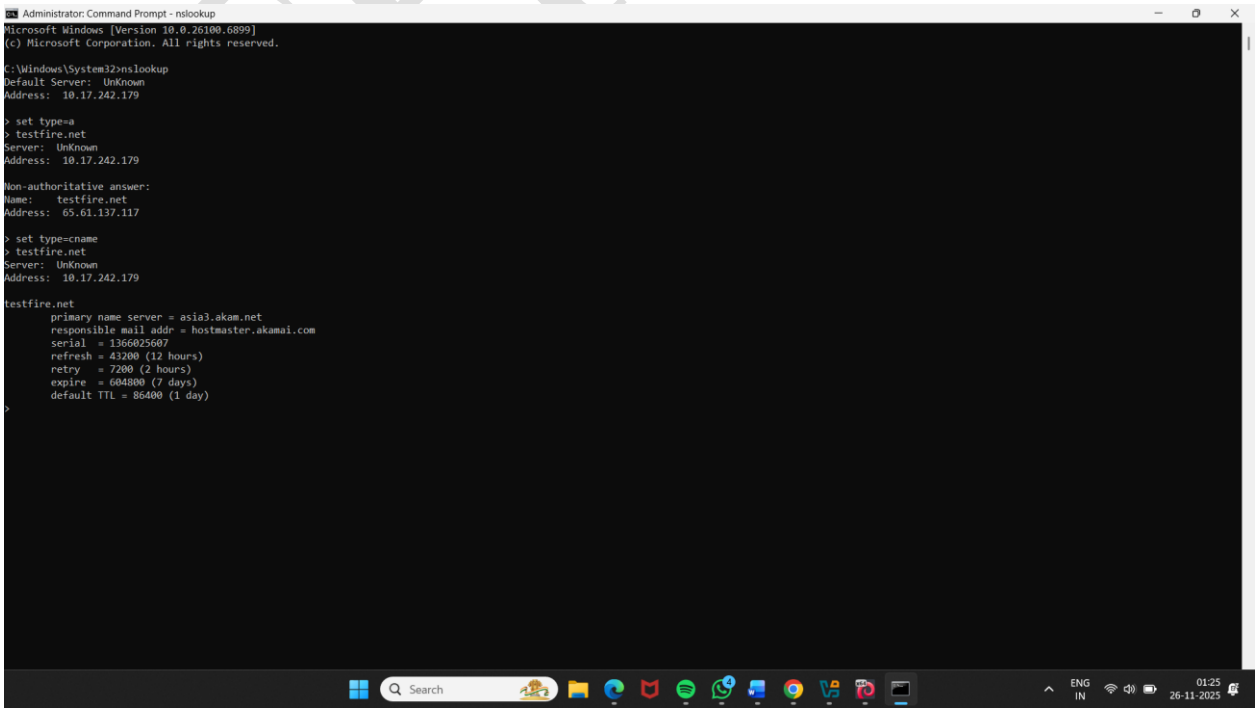
Step 2: In the nslookup interactive mode, type set type=a and press Enter.
Type the target domain and press Enter.



Fig(5.2)

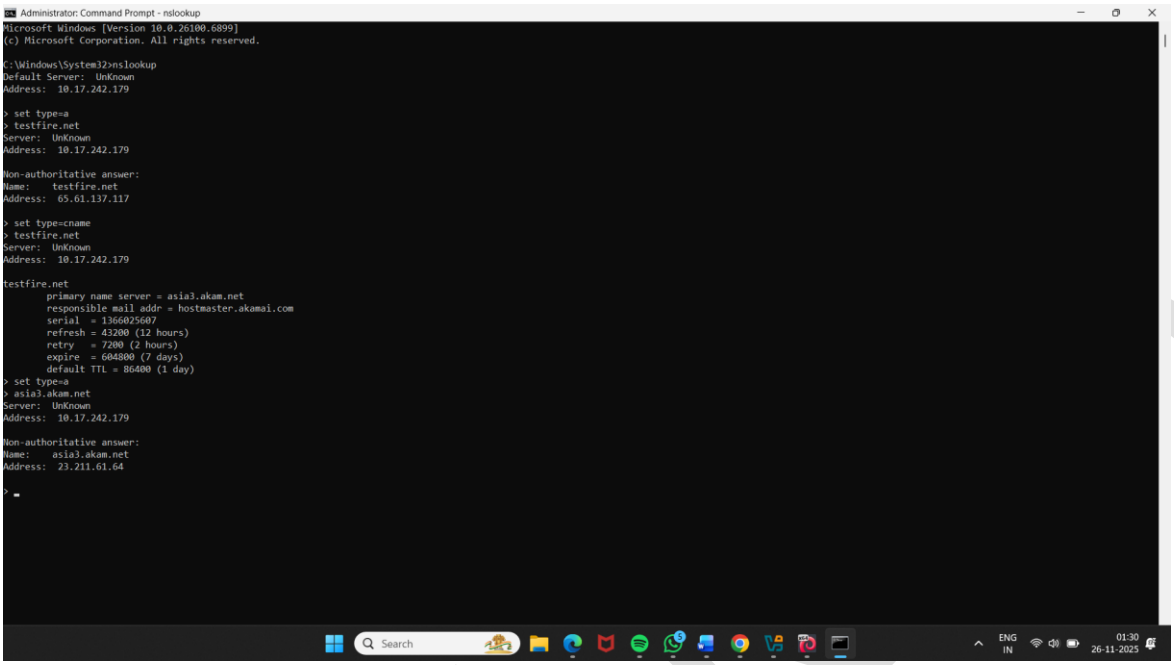
\

Step 3: Since the result returned is non-authoritative, you need to obtain the authoritative name server. Type set type=cname and press enter ,type the target domain and press Enter.



Fig(5.3)

Step 4: Issue the command set type=a and press Enter & type server name.

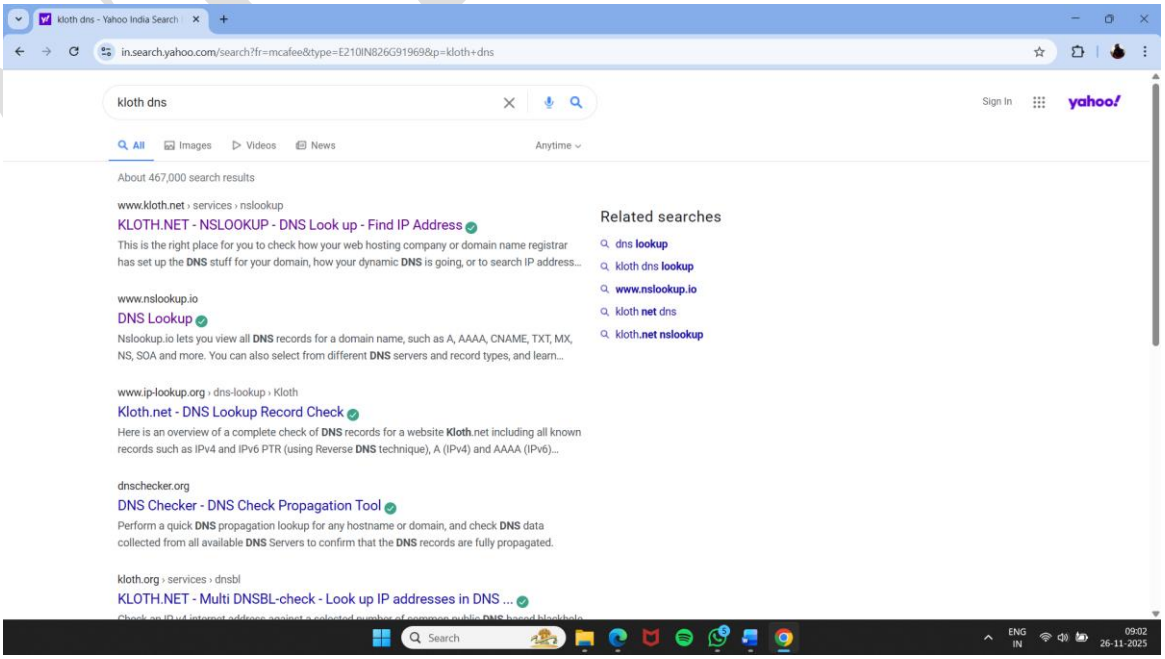


Fig(5.4)

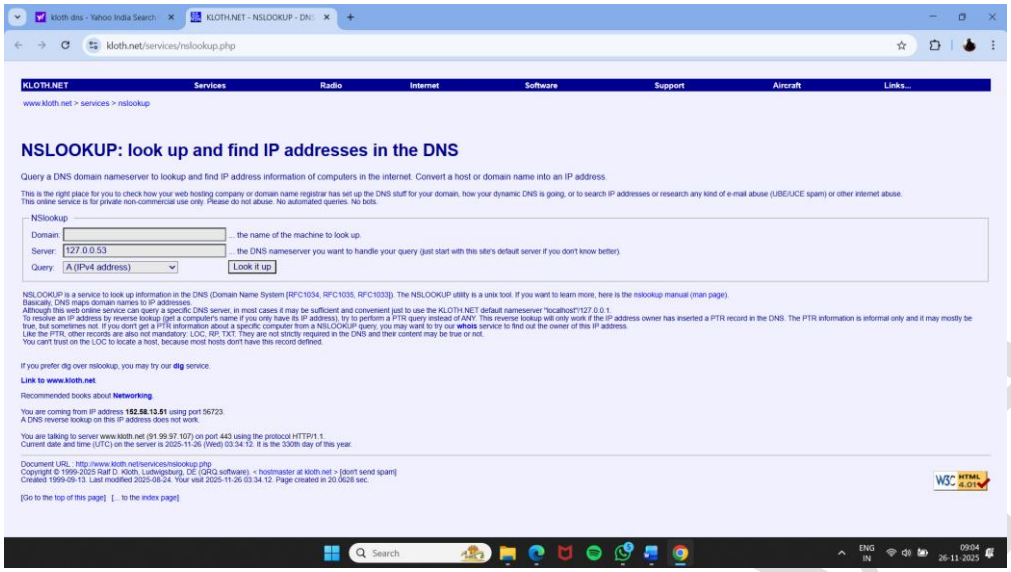
2) Footprinting Using Kloth DNS / nslookup (GUI):-

How to do it:-

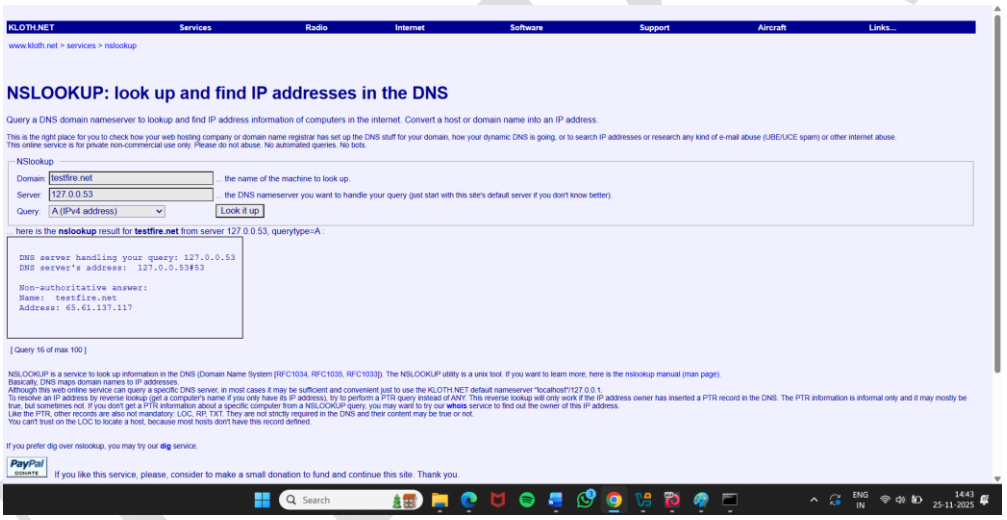
- Open Brower.
- Search Kloth DNS .
- Click on First website.



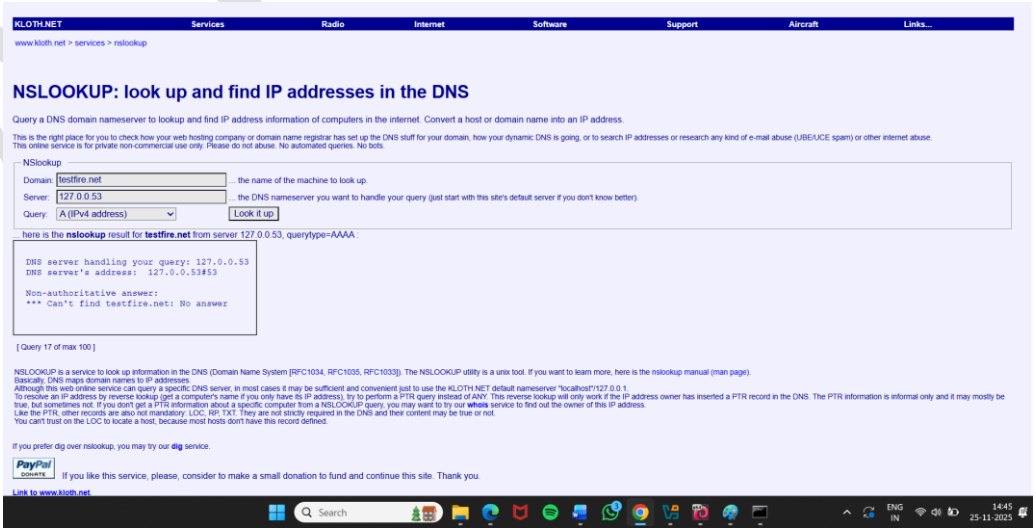
- Type domain name and search .



Fig(5.5)



Fig(5.6)



Fig(5.7)

6. NETWORK FOOTPRINTING

Network footprinting is the process of gathering information about a target network to understand its structure, devices, and potential vulnerabilities.

Objectives-:

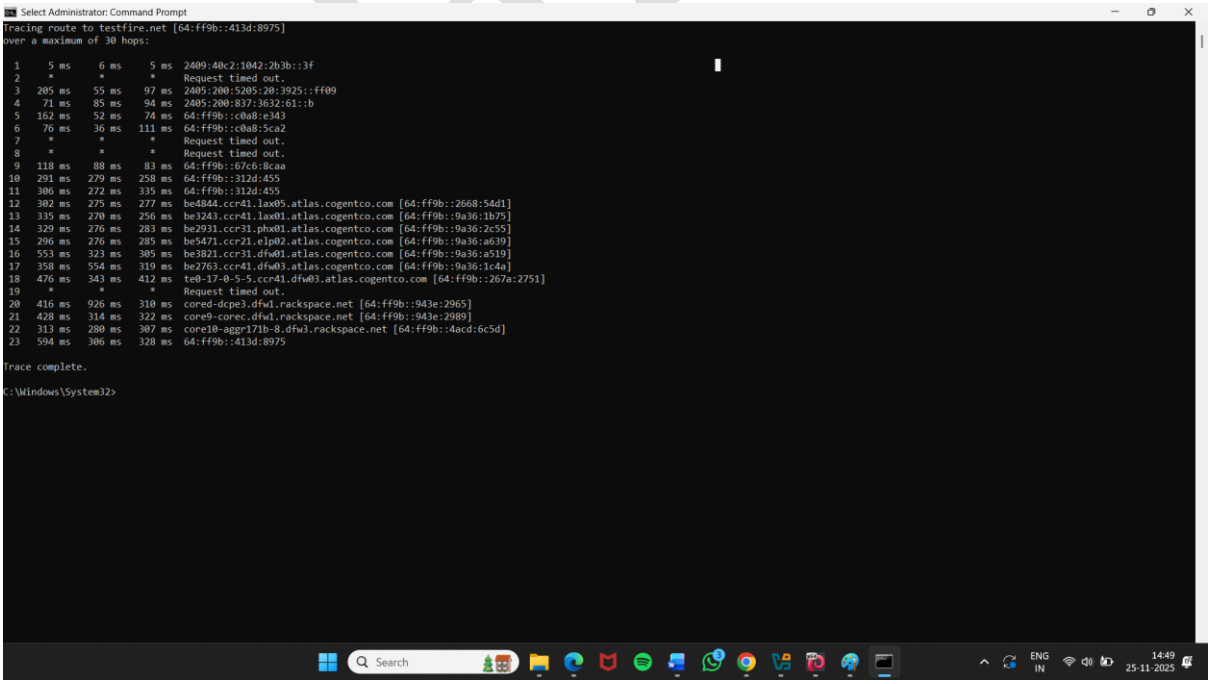
- Identifying IP Addresses
- Gathering DNS Information
- Extracting WHOIS Data
- Mapping Subdomains

1)Network Footprinting Using windows tracert (CLI):-

Tracert, short for "Trace Route," is a built-in Windows command line tool used to map the path that data packets take from your computer to a specified destination, like a website or server.

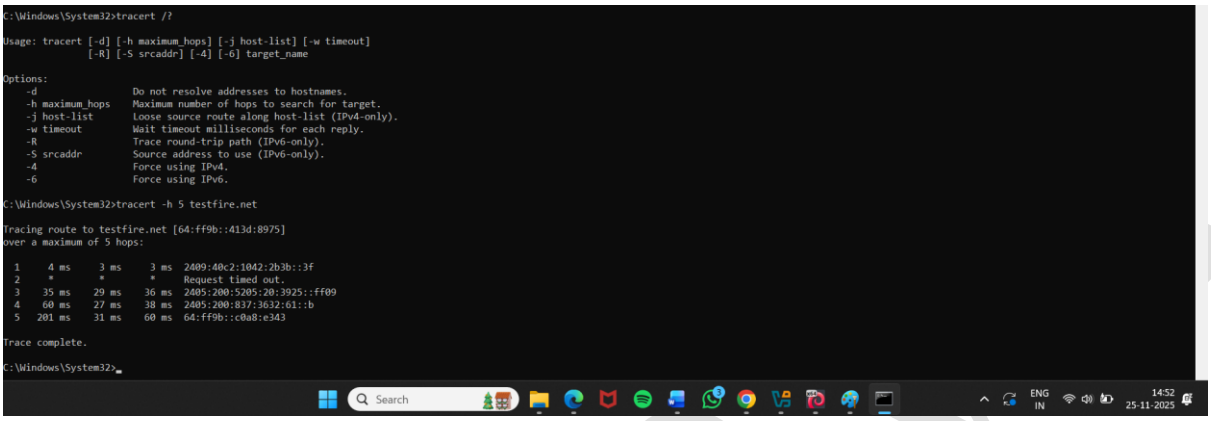
How to do it:-

- Open Command Prompt (type cmd in the Windows search bar and hit Enter).
- Type tracert followed by a destination, like tracert testfire.net, and press Enter.
- You'll see output like this:



Fig(6.1)

- Run tracet/? command to view the different options for the command.
- Run tracert -h 5 testfire.net command to perform the trace, but with only 5 maximum hops allowed.



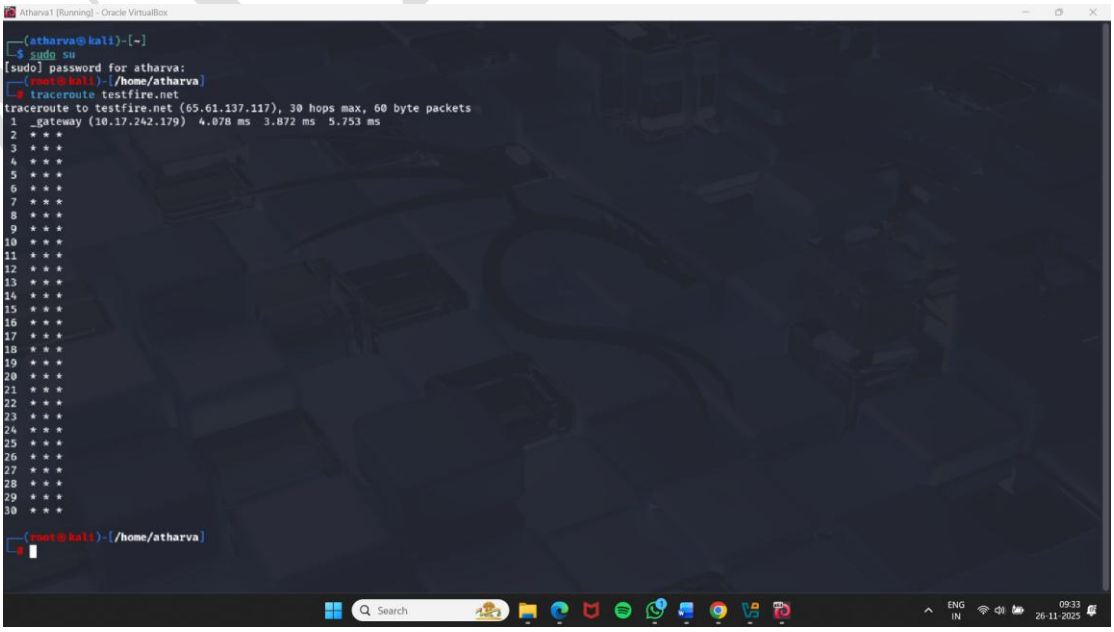
Fig(6.2)

2)Network Footprinting Using Linux traceroute (CLI):-

Traceroute on Linux is a network diagnostic tool similar to Windows' tracert.It traces the route that packets take from your machine to a destination, showing each hop along the way routers or network nodes and the time it takes to reach them.

How to do It:-

- Open a terminal.
- Type traceroute followed by a destination, like testfire.net and hit Enter.
- Output looks something like this:



Fig(6.3)

7. Email Footprinting

E-mail footprinting, or tracking, is a method to monitor or spy on email delivered to the intended recipient. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email.

It helps identify:

- Email service provider
- IP address (sometimes from email headers)
- User's name or username pattern
- Domain details (company info)
- Technologies used in email servers
- Possible vulnerabilities
- Social engineering opportunities

1)Email Footprinting using GSA Email Spider

How to do it:-

- Search GSA Email Spider download On Browser& clickon first website.

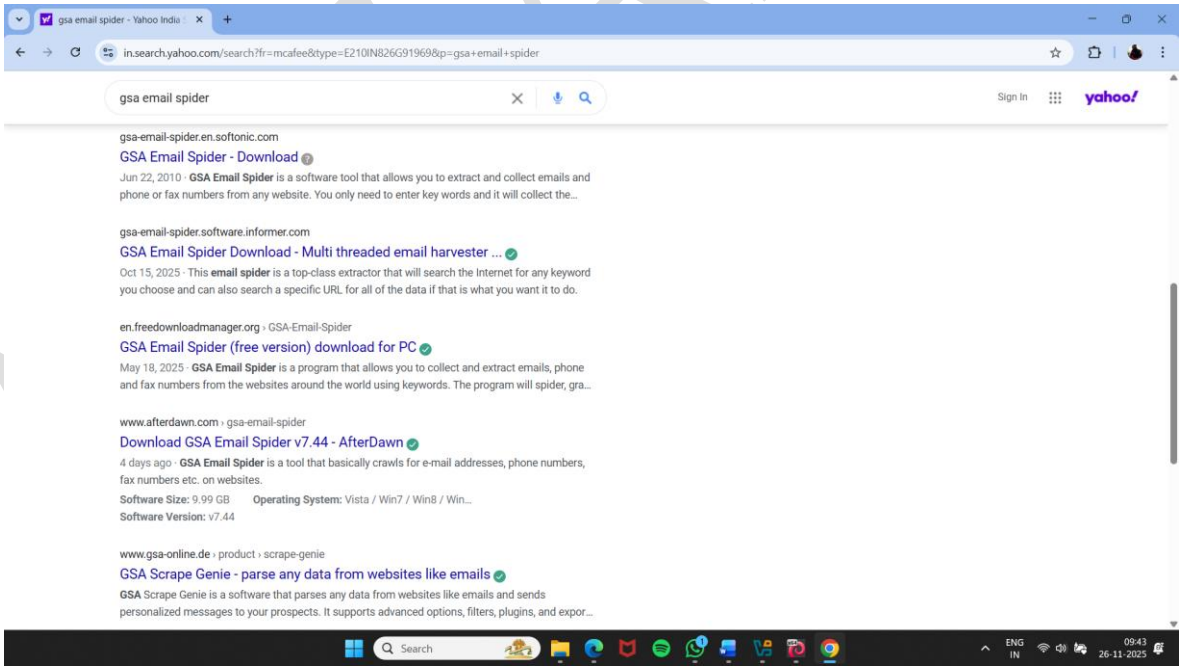
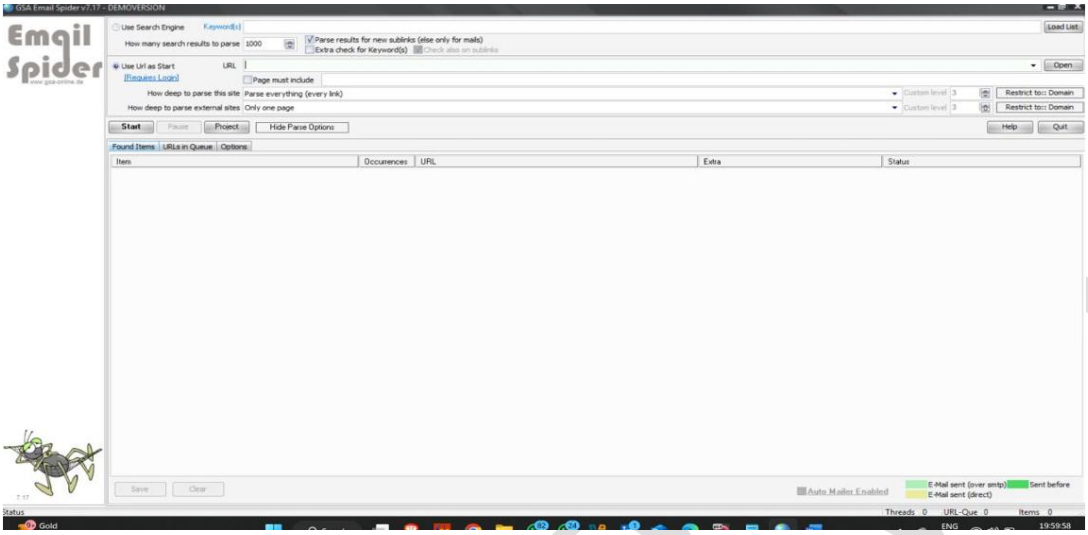


Fig (7.1)

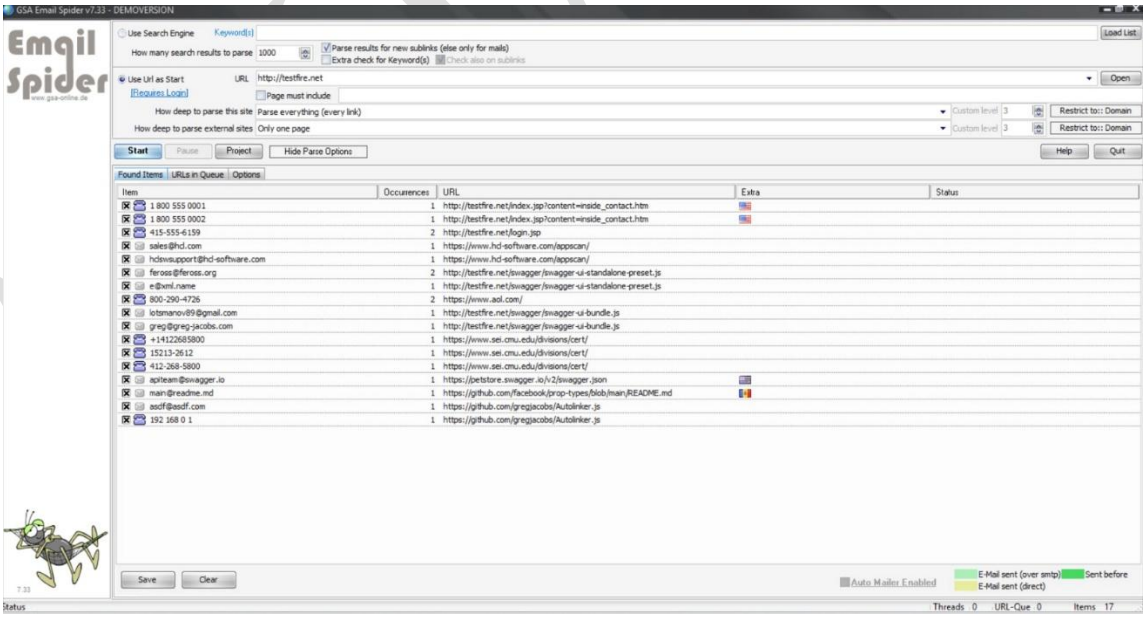
- Click on Download and Download it .
- After completing installation process then setup the app.



Fig(7.2)

- Copy url that you want to perform email footprinting
- Paste URL in url section
- Click on Start button.

RESULT:



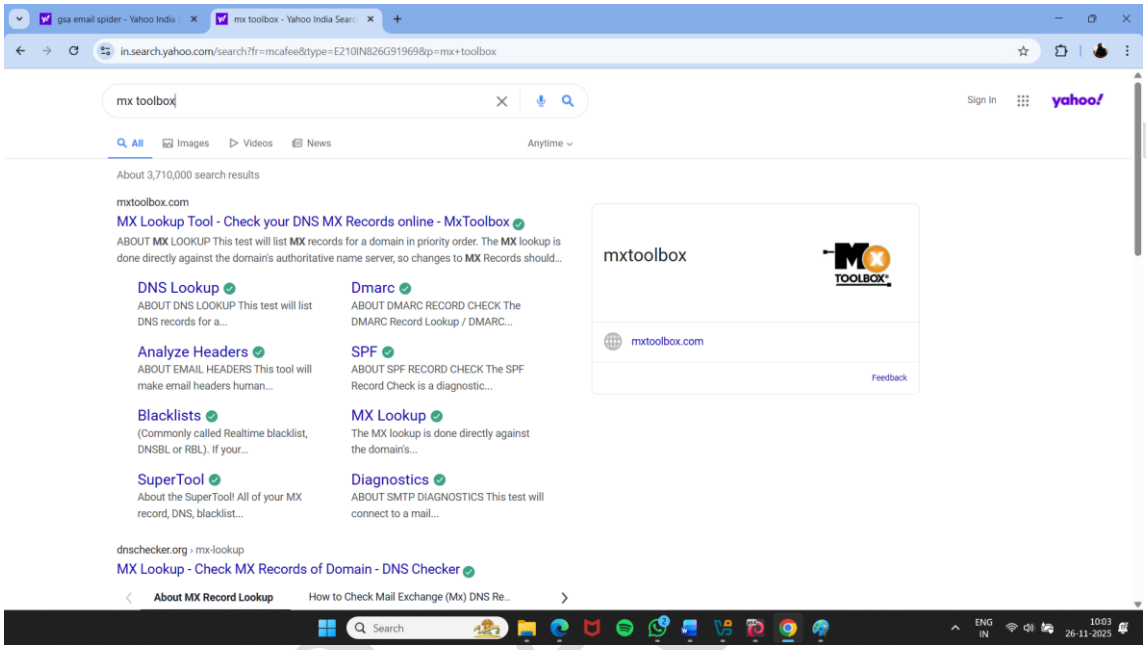
Fig(7.3)

2)Email Footprinting using MX TOOL BOX :-

- Mxtool box is used to check received email are original or fake.

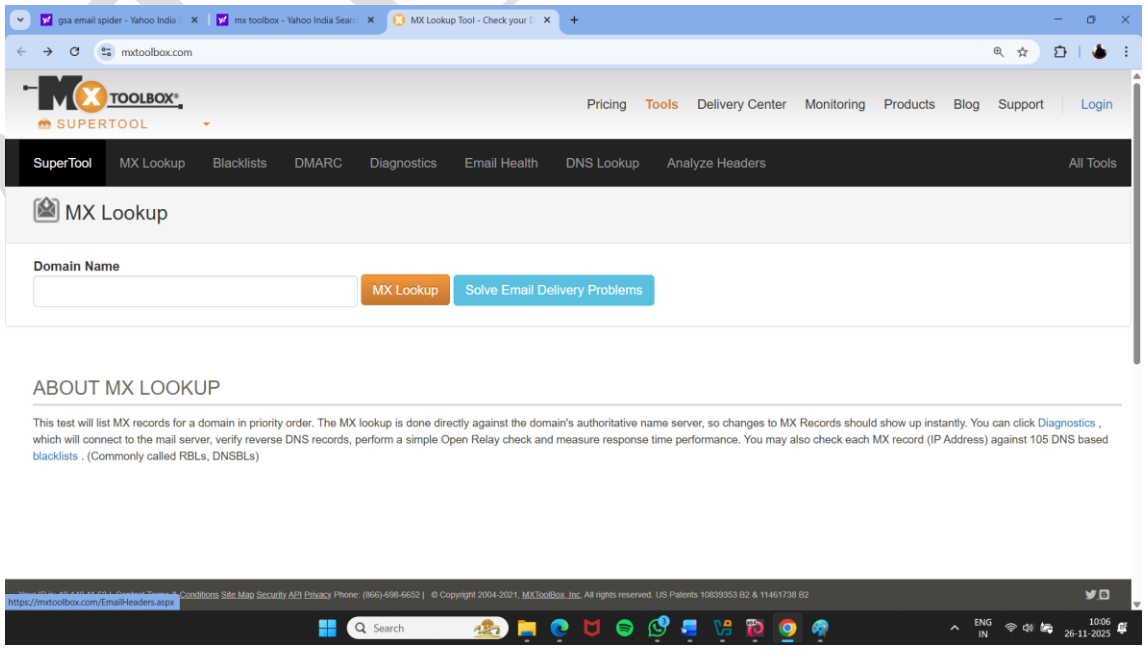
How to do it:-

- Search mx tool box on browser.
- Click on official mx tool box website.



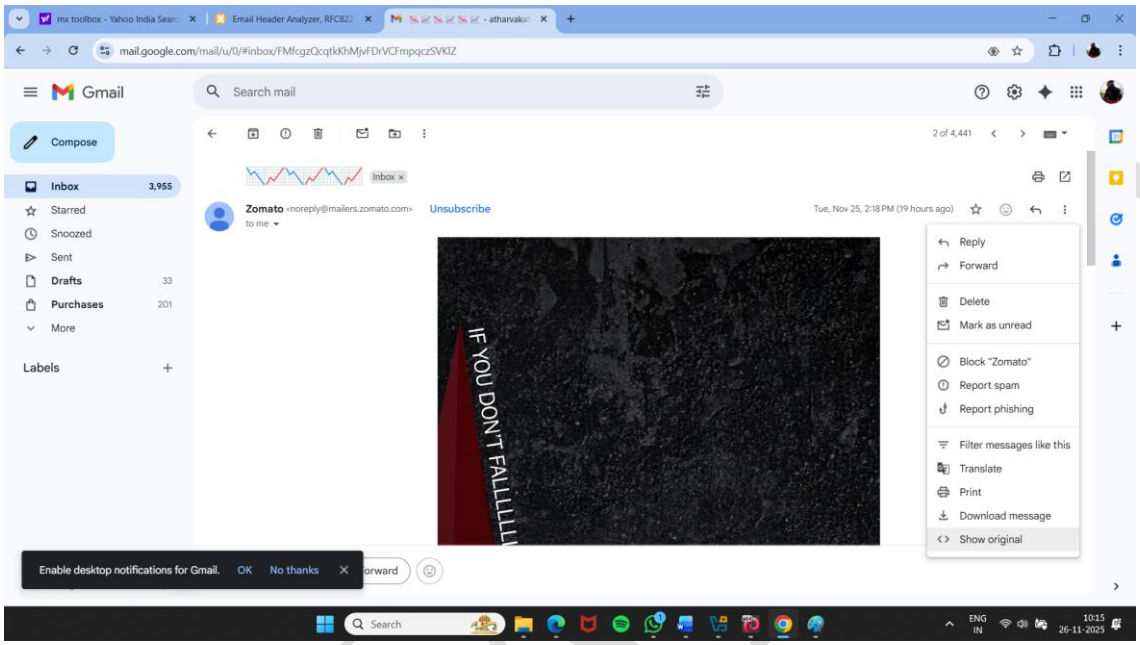
Fig(7.4)

- Open and Click on Analyze Headers



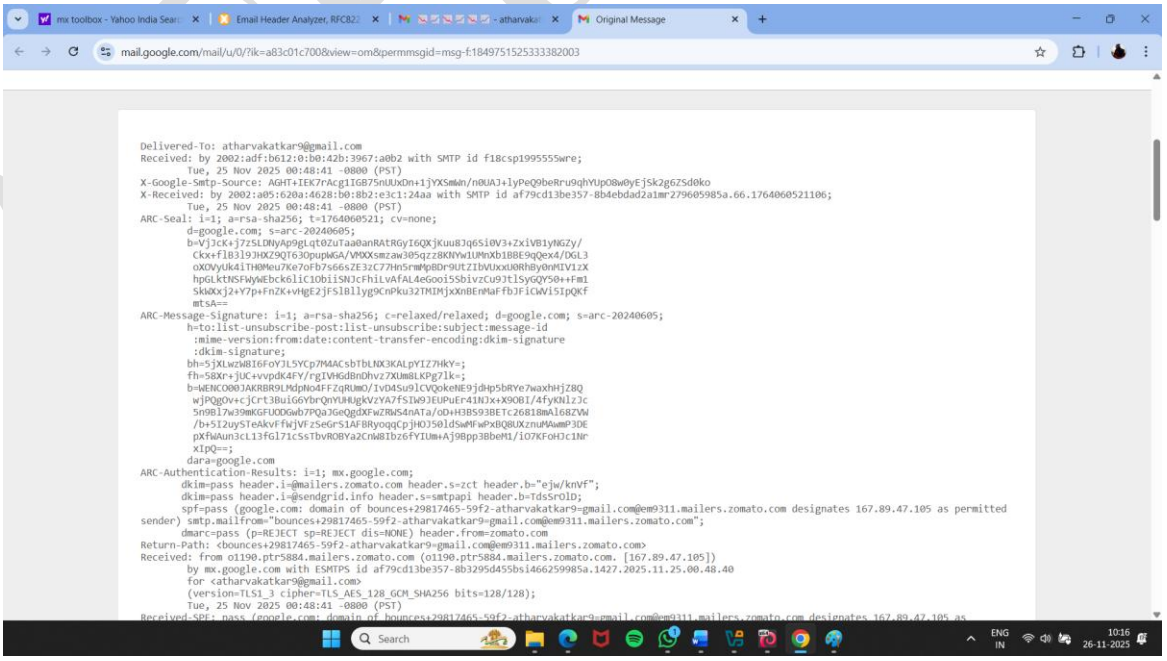
Fig(7.5)

- Now open email and click on those mail that you want to check its original or fake
- Then click on three dot on right site.
- Then click on show original option.

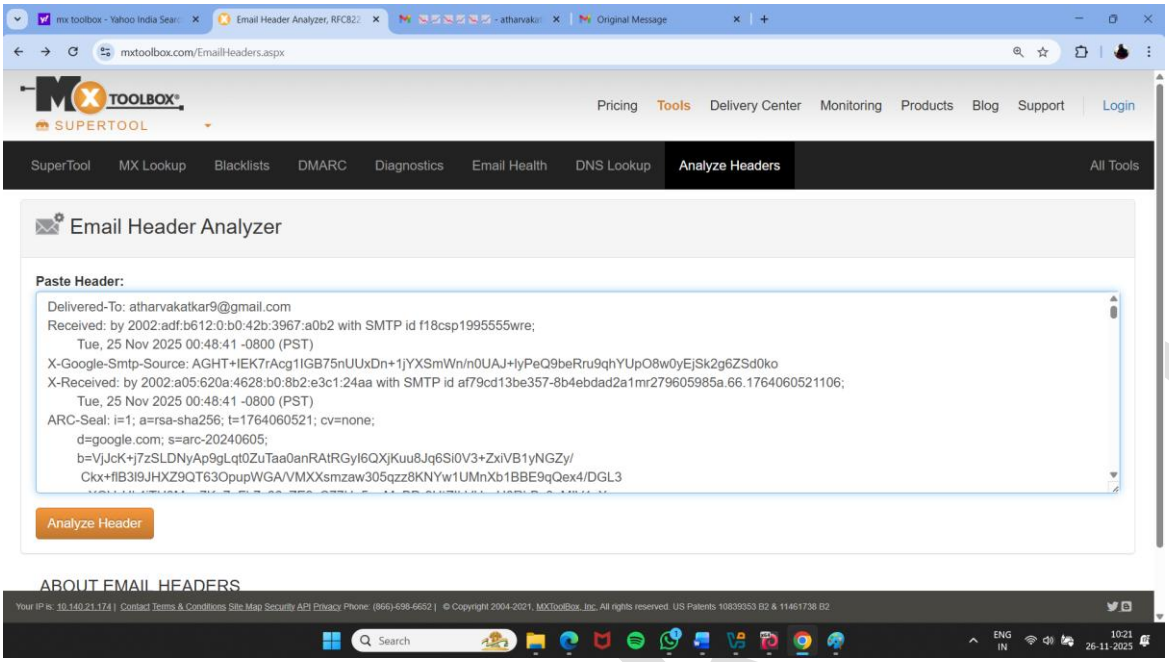


Fig(7.6)

- Copy entire header.

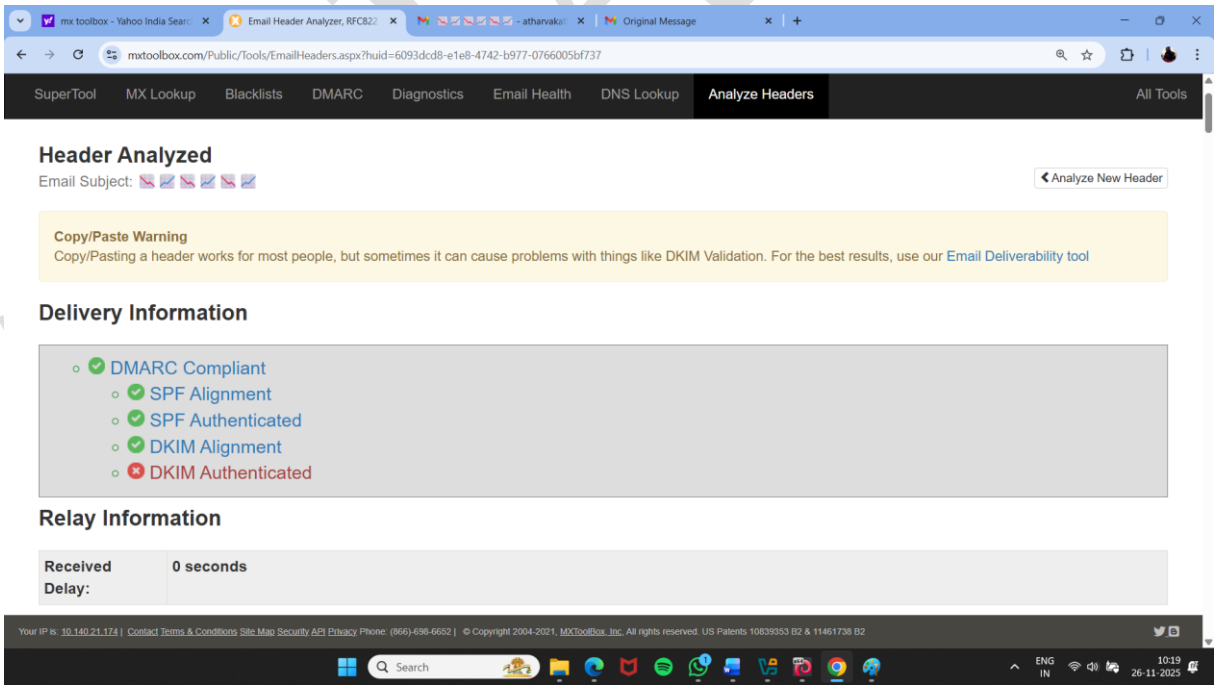


Fig(7.7)



Fig(7.8)

A "pass" result is generally good — it indicates the email's authenticity checks were successful.



Fig(7.9)

8.Footprinting using various footprinting tools

Footprinting tools are used to collect basic information about the target systems in order to exploit them. Information collected by the footprinting tools contains the target's IP location Information, routing information, business information, address, phone number and social security number, details about the source of an email and a file, DNS information, domain information, etc.

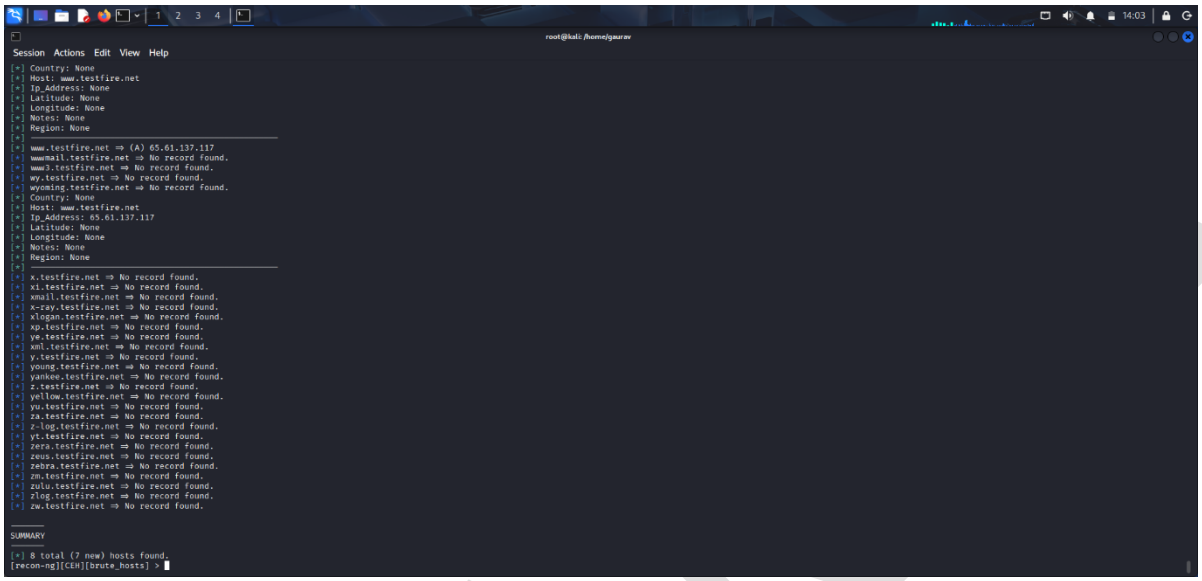
1)Footprinting a target using Recon-ng:

Recon-ng is a powerful open-source reconnaissance framework built into Kali Linux, designed for web-based information gathering using Open Source Intelligence (OSINT).

Step1:Go on Kali terminal and type recon-ng
Step2: Run help command to view all the commands that allow you to add/delete records to a database, query a database, etc.
Step3: Creating workspace list on recon-ng then inserting domains and view it and modules to load brute.

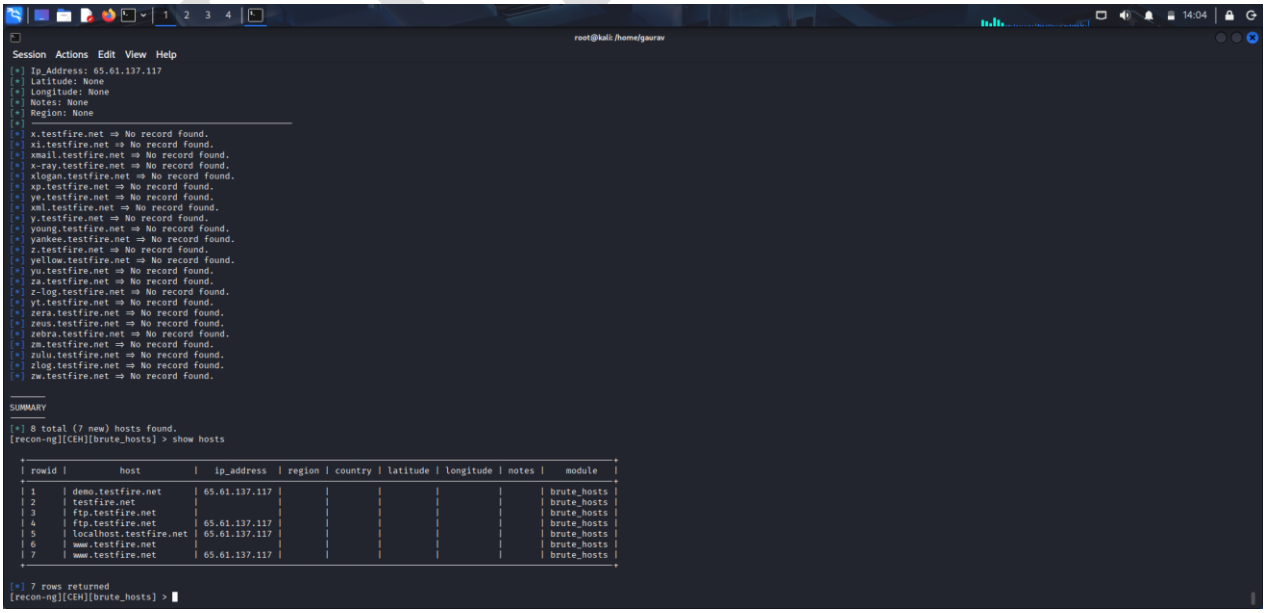
Fig(8.1)

Step4:After run prcess we obtain the information of testfire.net then it shows the hosts and other Information.



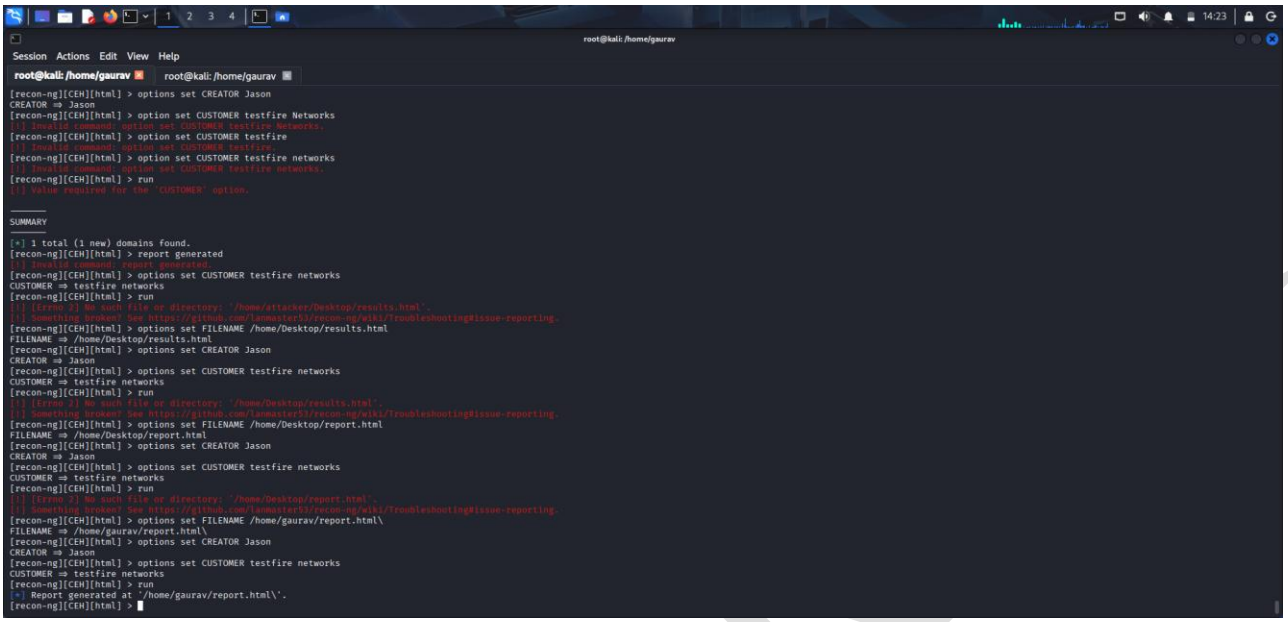
Fig(8.2)

Step 5:after run process we obtain the information of testfire.net then it shows the hosts,ip address etc.

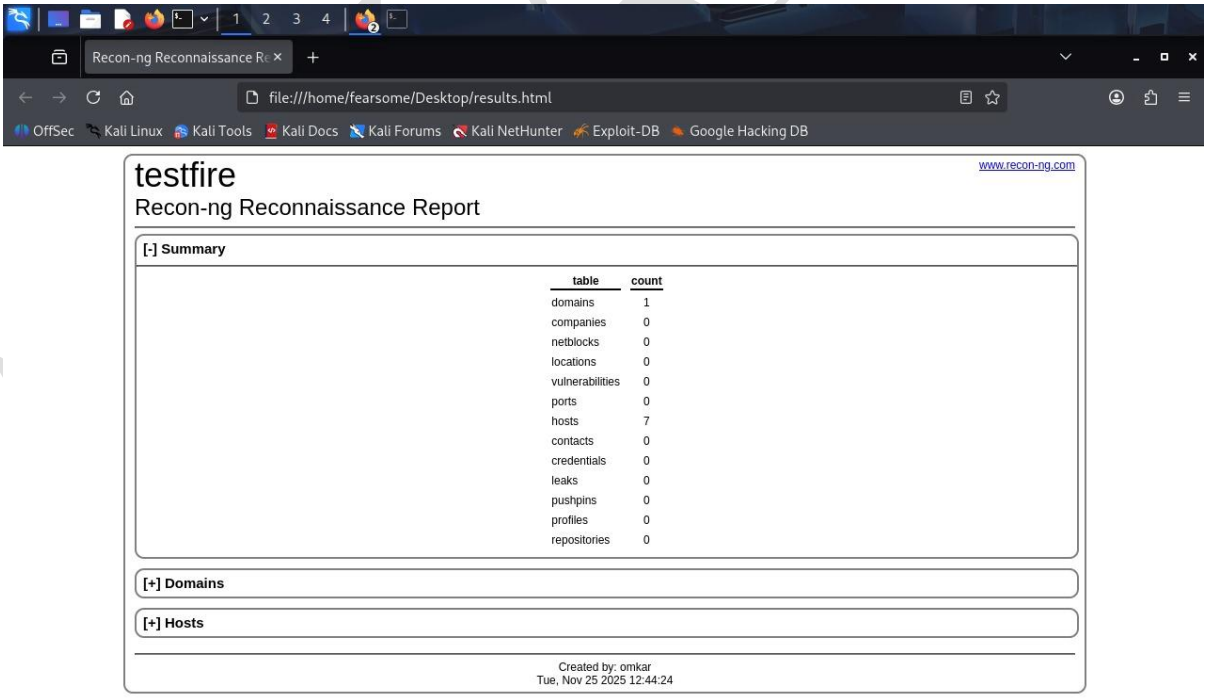


Fig(8.3)

Step 6:saving the details of the hosts by creating file in system



Fig(8.4)



Fig(8.5)

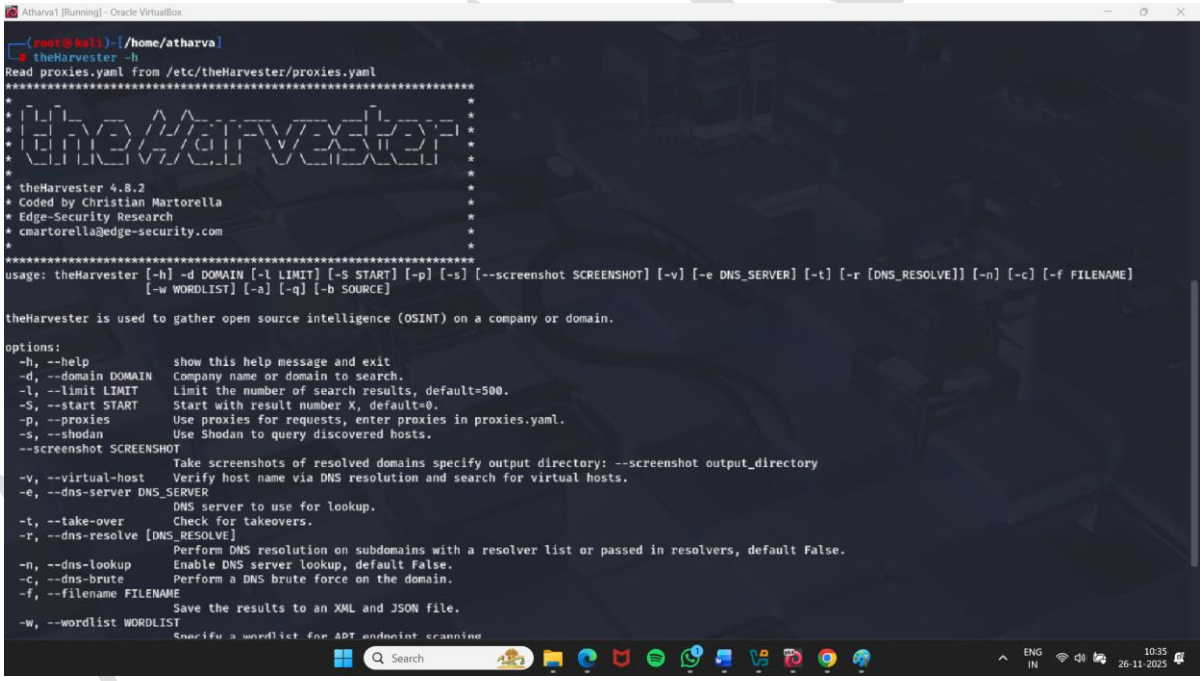
9.Additional tools:

1)Footprinting Using TheHarvester (CLI Tool):

TheHarvester is an open-source OSINT (Open Source Intelligence) tool used for passive information gathering about a target during the reconnaissance phase of ethical hacking and penetration testing. It collects publicly available information from various search engines, social networks, and online data sources.

How to do it:

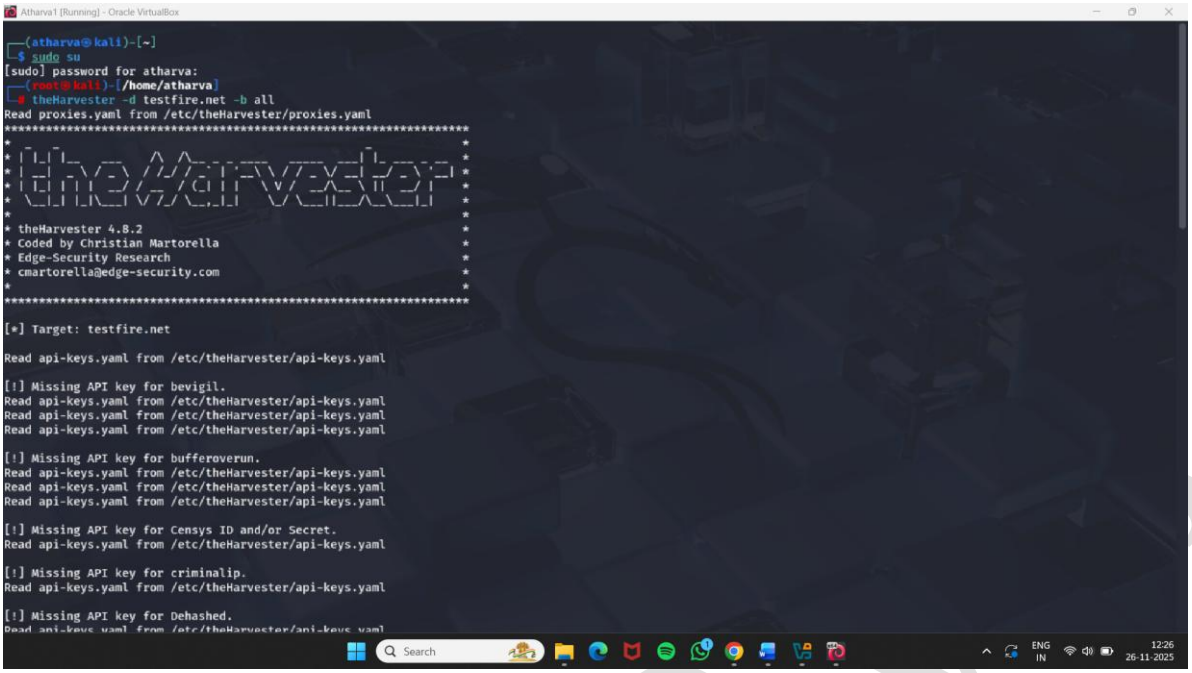
- Open Kali Linux
- Type sudo apt install theHarvester (It will install the tool).
- Search theHarvester -h (-h = help)



Fig(9.1)

Command:

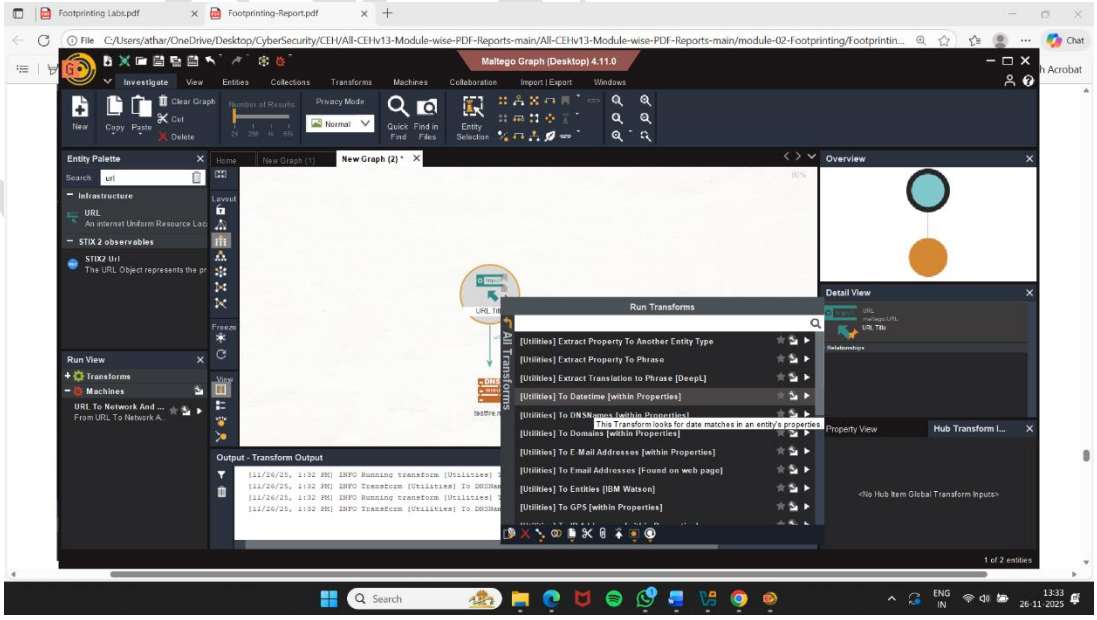
- theHarvester -d testfire.net -b subdomaincenter
- -d = domain
- -b =source



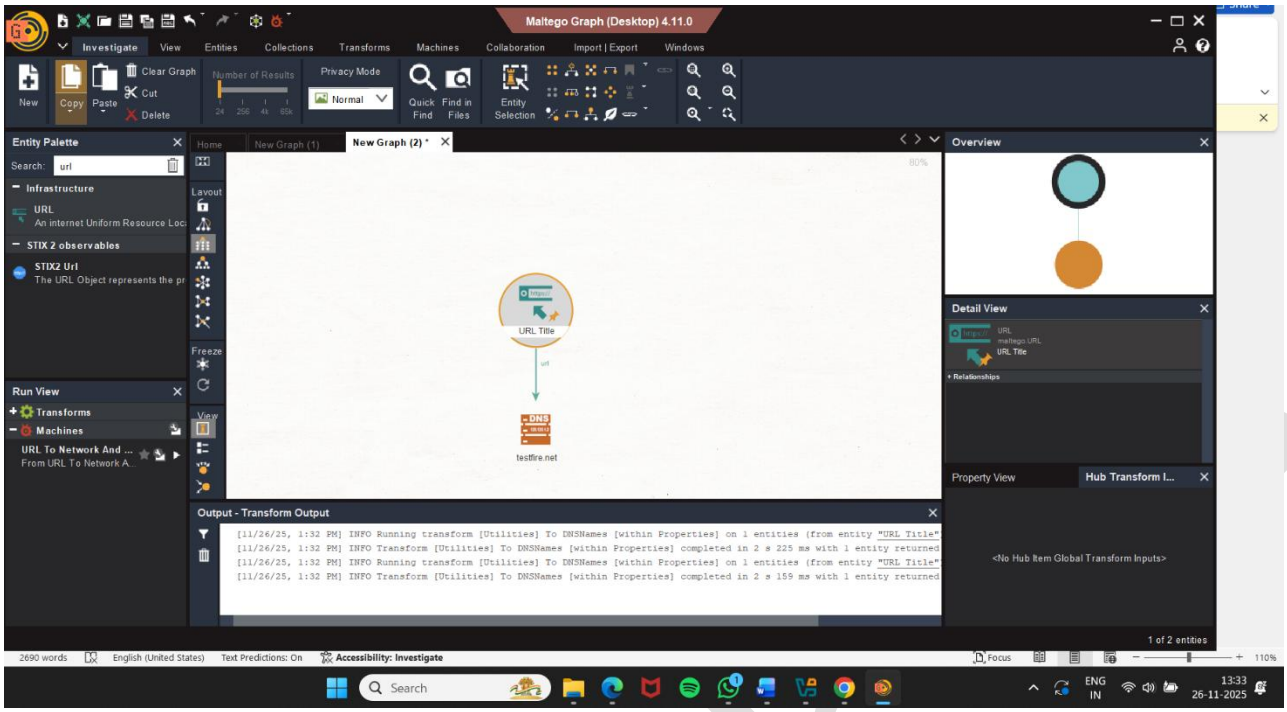
Fig(9.2)

2)Footprinting Using Maltego:

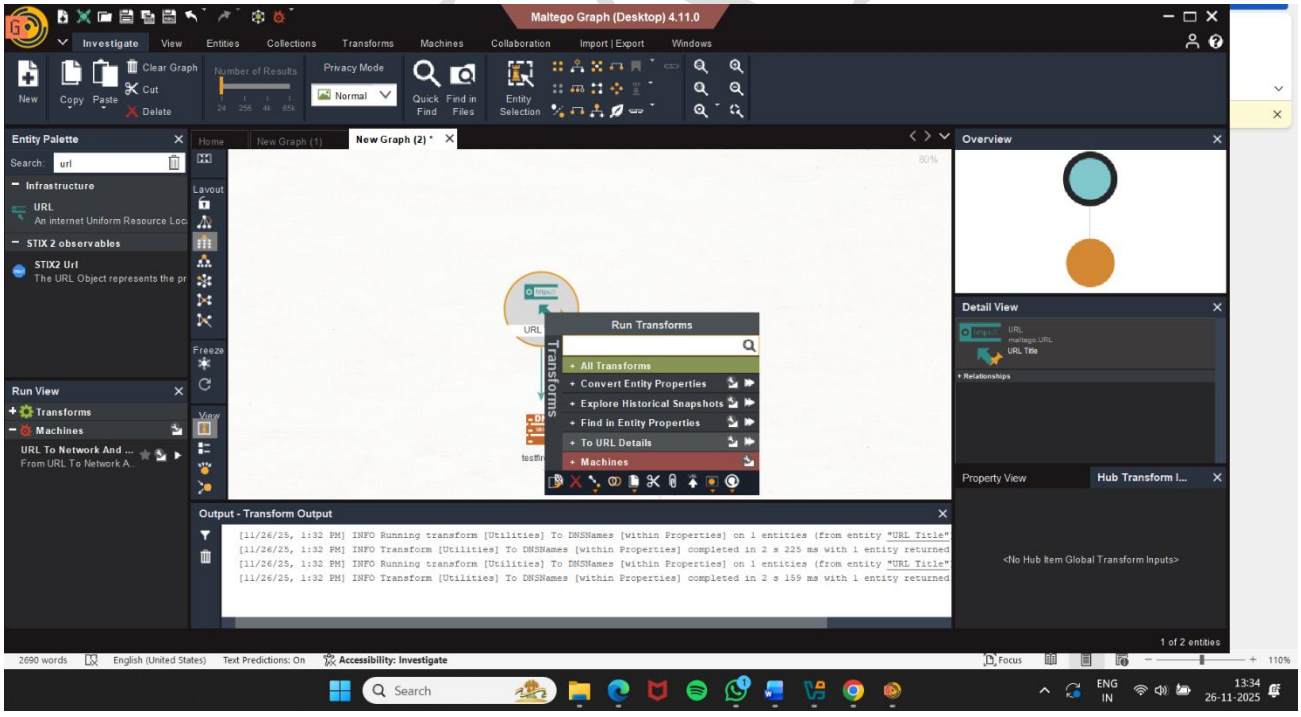
Maltego is a powerful information-gathering (OSINT) tool used in cybersecurity, ethical hacking, and digital investigations.
It helps you collect, link, and visualize data about people, websites, companies, IPs, emails, social media accounts, etc.
It shows all this information in the form of graphs (nodes and links) which makes it easy to understand relationships.



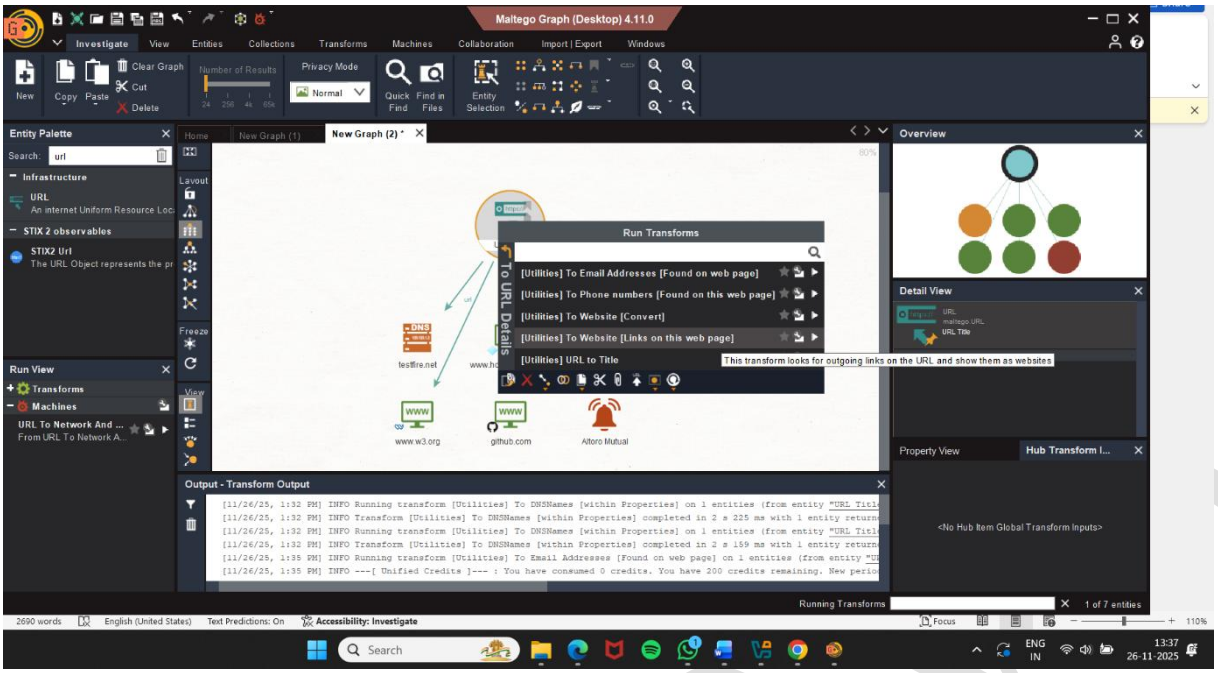
Searched for all DNS
Fig(9.3)



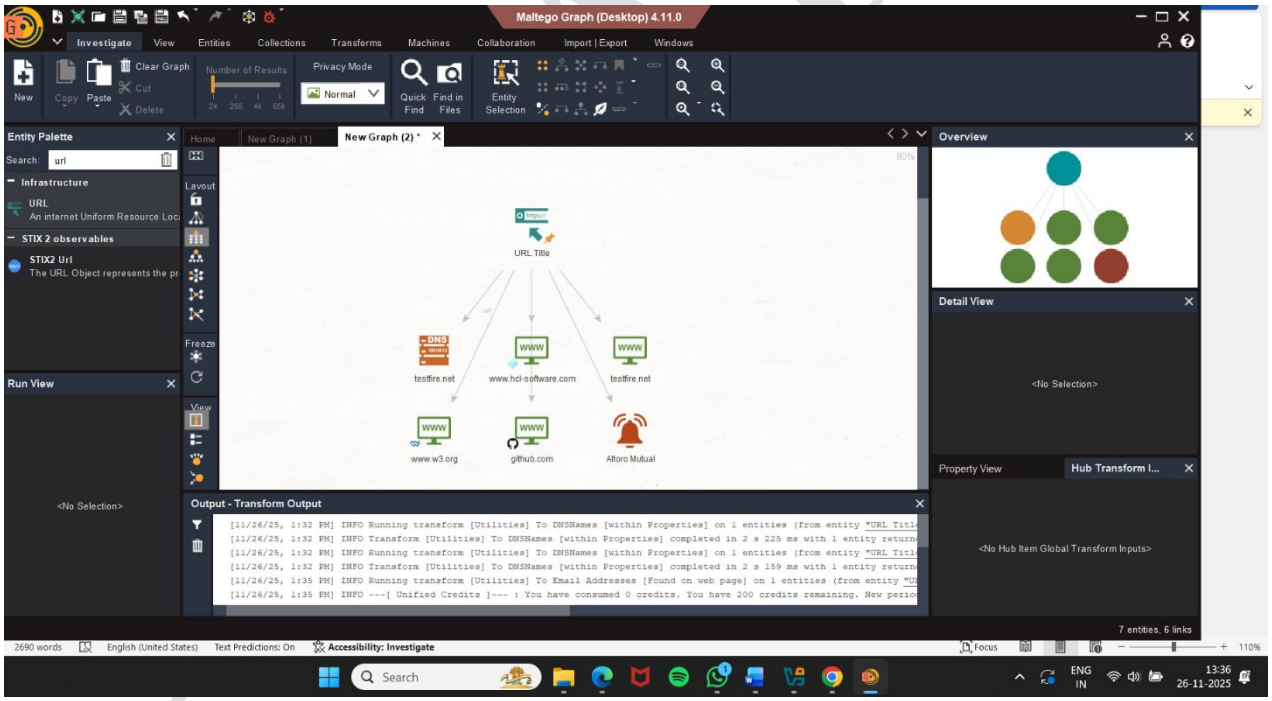
Output:testfire.net



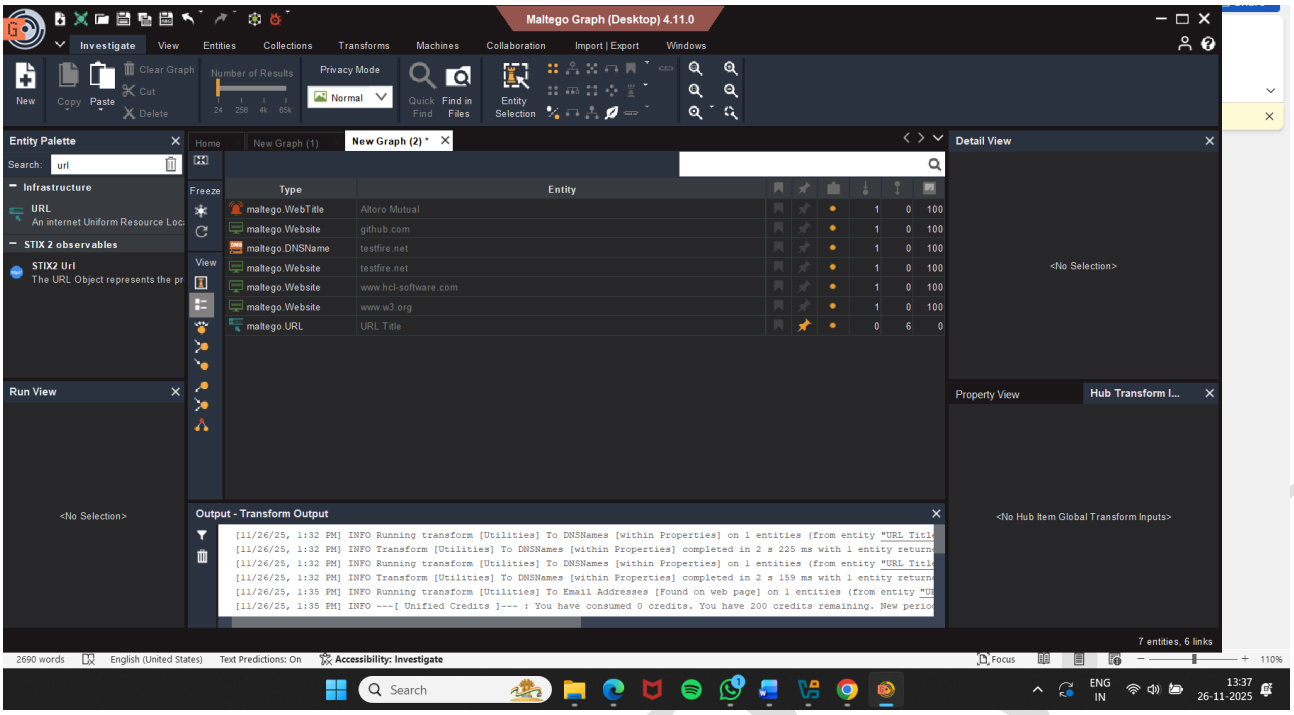
Click on All transforms
Fig(9.5)



By using this transformation we get all the accessible links on the webpages.
Fig(9.6)



Output : total six links available on this webpage.
Fig(9.7)



Following image is the List view of the graph
Fig(9.8)

3) Napalm FTP Indexer

Napalm FTP Indexer is an online search engine that scans the internet for publicly accessible FTP servers and lists their files.

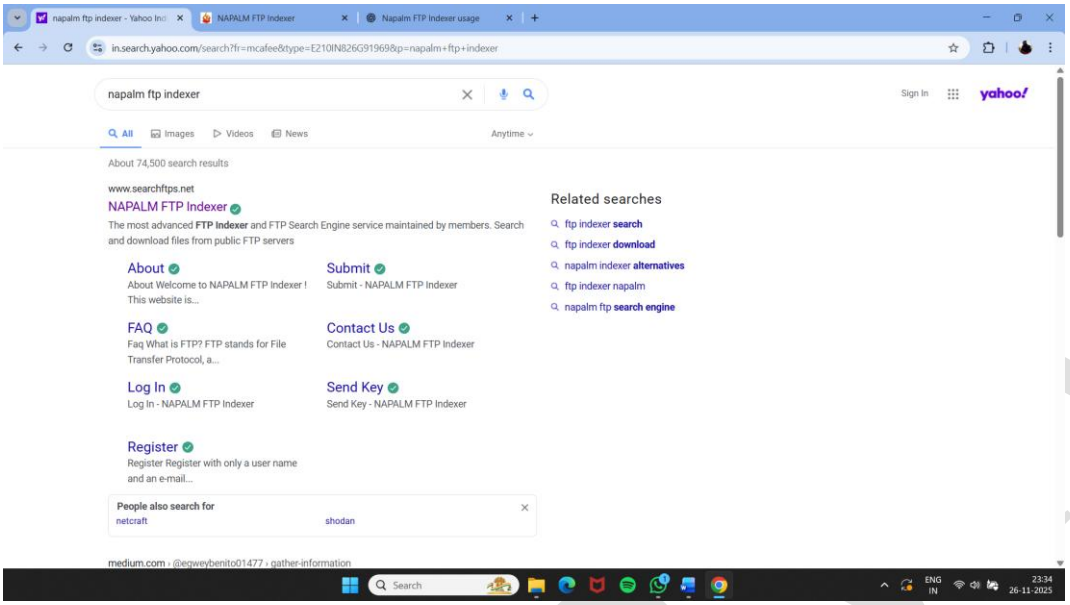
What Napalm FTP Indexer can find:
You can search for:

- PDFs, images, videos
- Configuration files
- Backup files
- Publicly exposed directories

The indexer shows:

- File name
- File link
- File size
- FTP server address

Step 1 -Open Website (Napalm FTP Indexer)

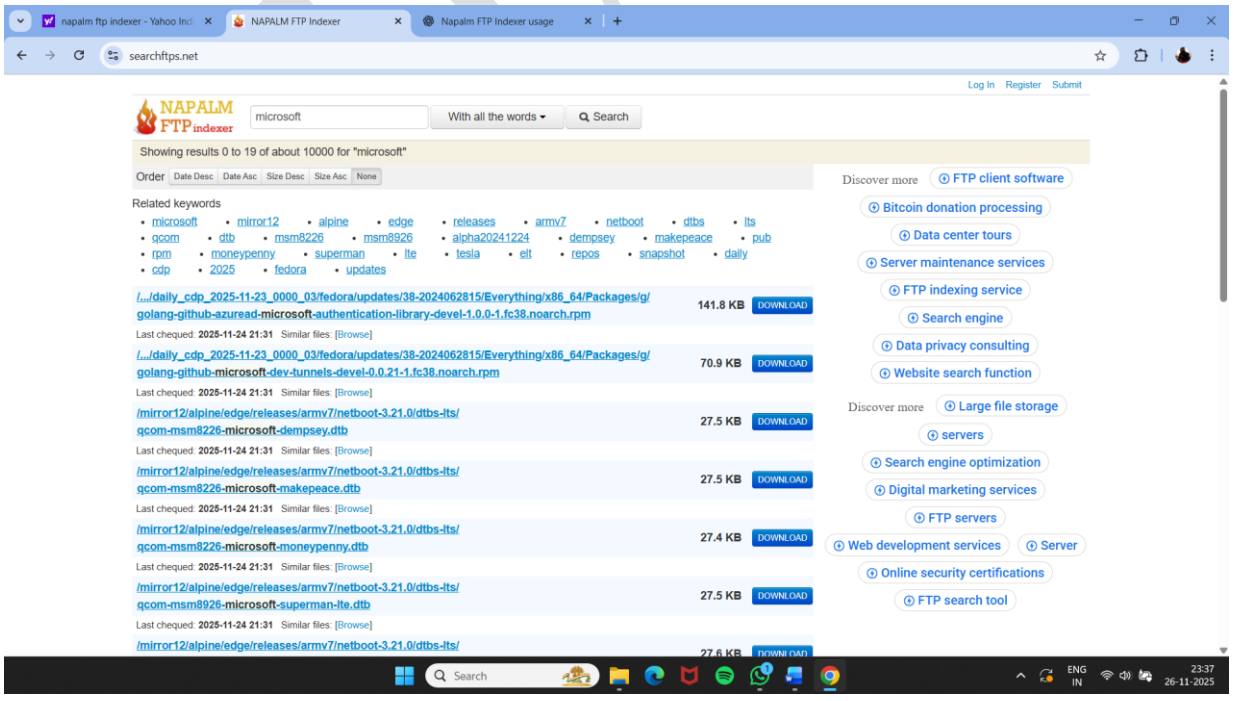


fig(9.9)

Step 2 - Use the Search Bar
Type anything you want to find:
Examples:

- pdf
- Microsoft

You'll get the result.



fig(9.10)

Step performed:

- A keyword search (microsoft.com) was entered into the FTP indexing engine.
- The tool scanned its database of indexed public FTP directories and returned entries where the term appears in file paths or metadata.
- This is a passive information-gathering step no interaction with any target server occurs beyond viewing already indexed information.

Observed output:

- Multiple FTP directory listings referencing microsoft.com appeared.
- Listings include paths such as:
  - public /pub/windows/nt/ directories
  - archived game files and ISO images
  - old Usenet-mirrored folders
- Metadata such as file size, last-checked timestamps, and "similar files" were shown.

This indicates that the indexing tool has captured numerous public FTP sources that contain filenames mentioning Microsoft-related terms

4) OSINT Framework

OSINT Framework is a collection of tools and websites used for Open-Source Intelligence (OSINT)—information gathering from publicly available sources. It does NOT gather data by itself. It simply organizes hundreds of OSINT tools in a clean tree structure.

You can perform OSINT on:

People

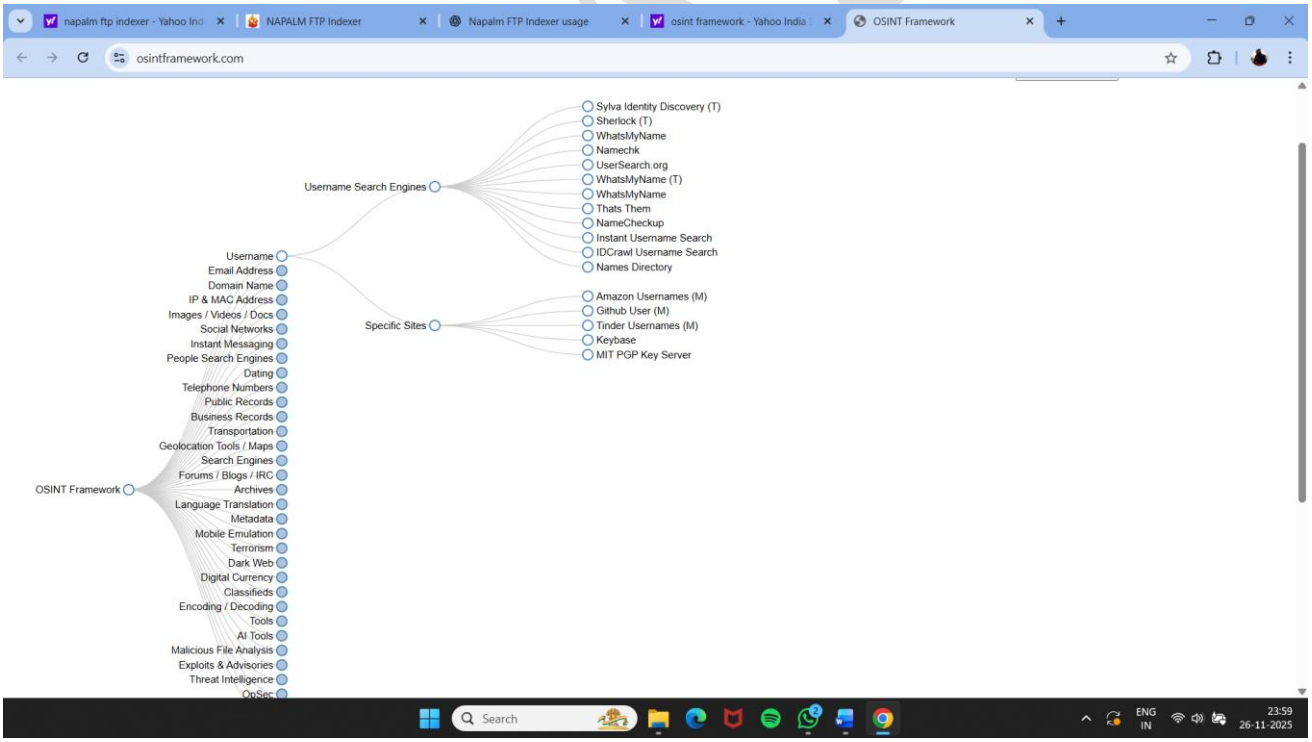
- Username search
- Email lookups
- Social media investigation
- Breach data

🌐 Domains & IPs

- Whois lookup
- DNS records
- Subdomain discovery
- Website analysis

📱 Social Networks

- Facebook/Instagram tools
- Twitter/X tools
- LinkedIn OSINT
- TikTok lookups



fig(9.11)