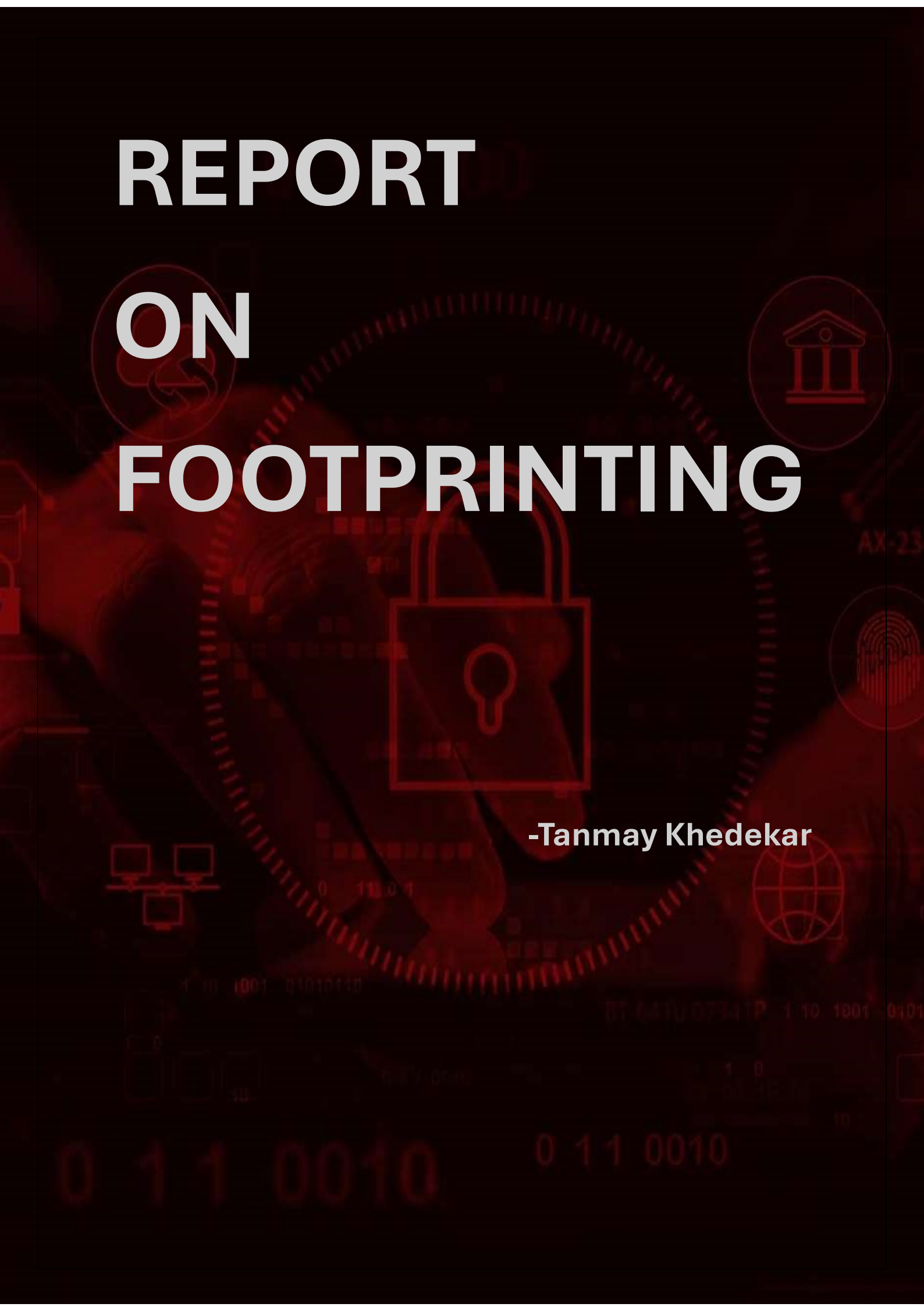
REPORT ON FOOTPRINTING



-Tanmay Khedekar

Table of Contents: -

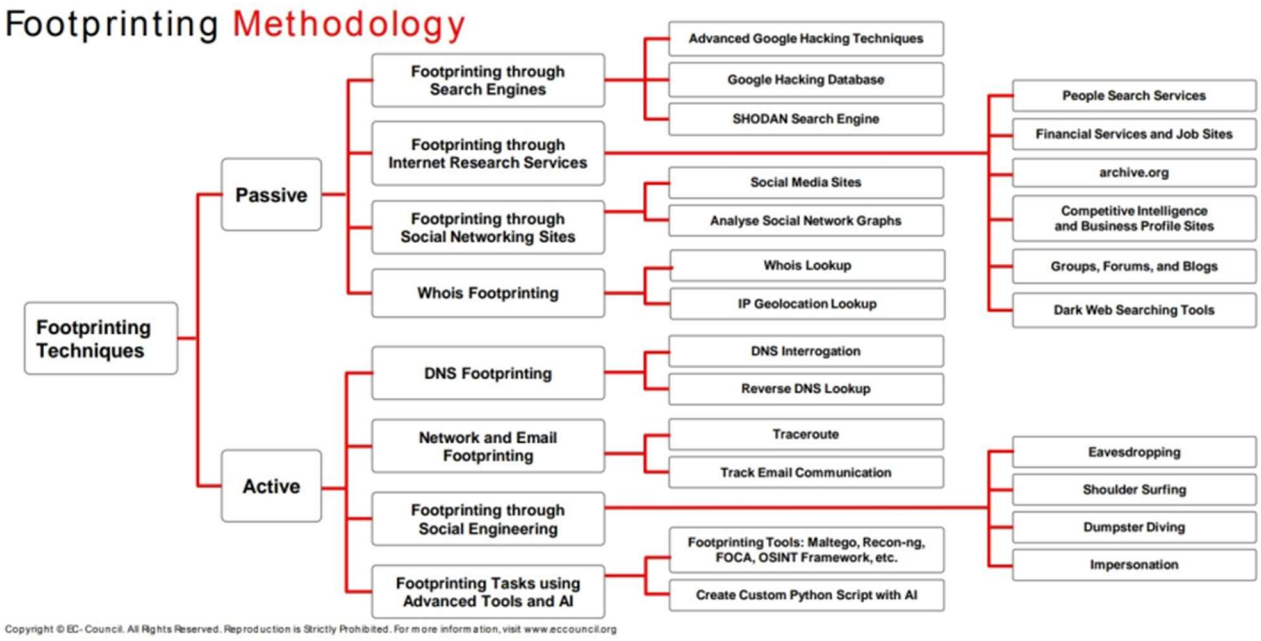
1.Introduction

Footprinting is the initial phase of cyber security where information about a target system or organization is collected before performing any active testing. The goal is to gather publicly available data such as domains, IP addresses, technologies, network structure, and user details. This information helps identify potential entry points and understand the overall security posture of the target. Footprinting is essential for planning further penetration testing steps and reducing blind spots in the assessment.

1.1The main goals are:

- Identify the target's public information
- Find the attack surface
- Understand how the system works
- Discover weak points that can be attacked later
- Reduce blind spots before testing

1.2Types of Footprinting-



2.Footprinting Using Search Engine (Google Dorking):

These Google advanced search operators are used to collect publicly available information about a target during the reconnaissance phase. They help identify indexed pages, exposed data, and potential misconfigurations without directly interacting with the system. This improves the quality and depth of the security assessment.

Popular Google advanced search operators

Search Operator	Purpose
[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to the specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain

Search Operator	Purpose
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[location:]	Finds information for a specific location

Fig.2.1 – Popular Google advance search engine

How to Use it: -Open Browser and Search Google and after search google Type Advance search operators:

Ex.a) intitle:login site: testfire.net

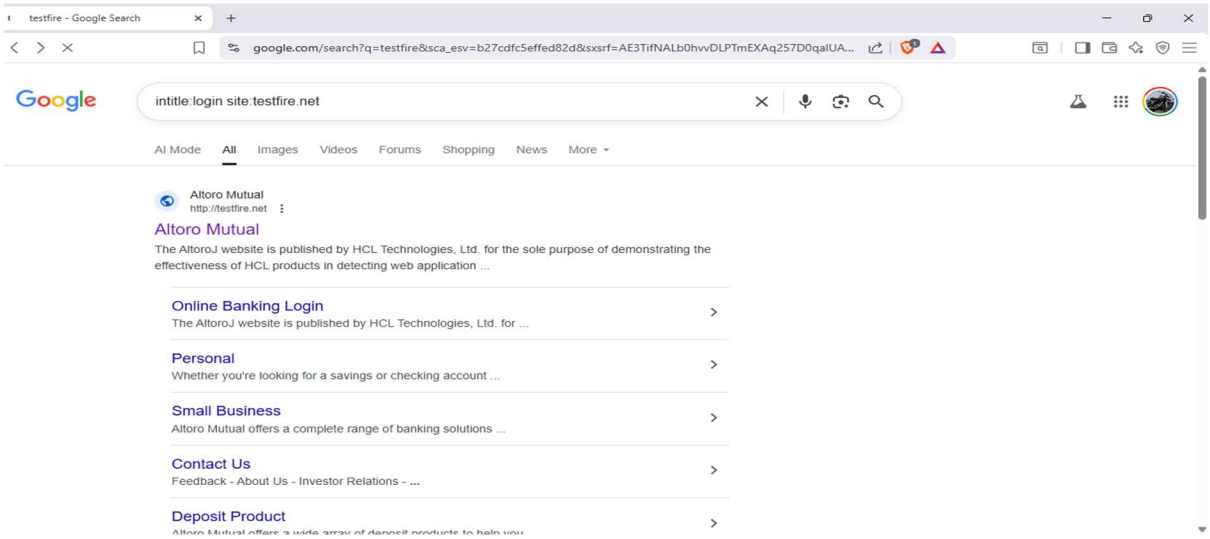


Fig.2.2 – Google Dorking using this get direct login page

b)info: testfire.net

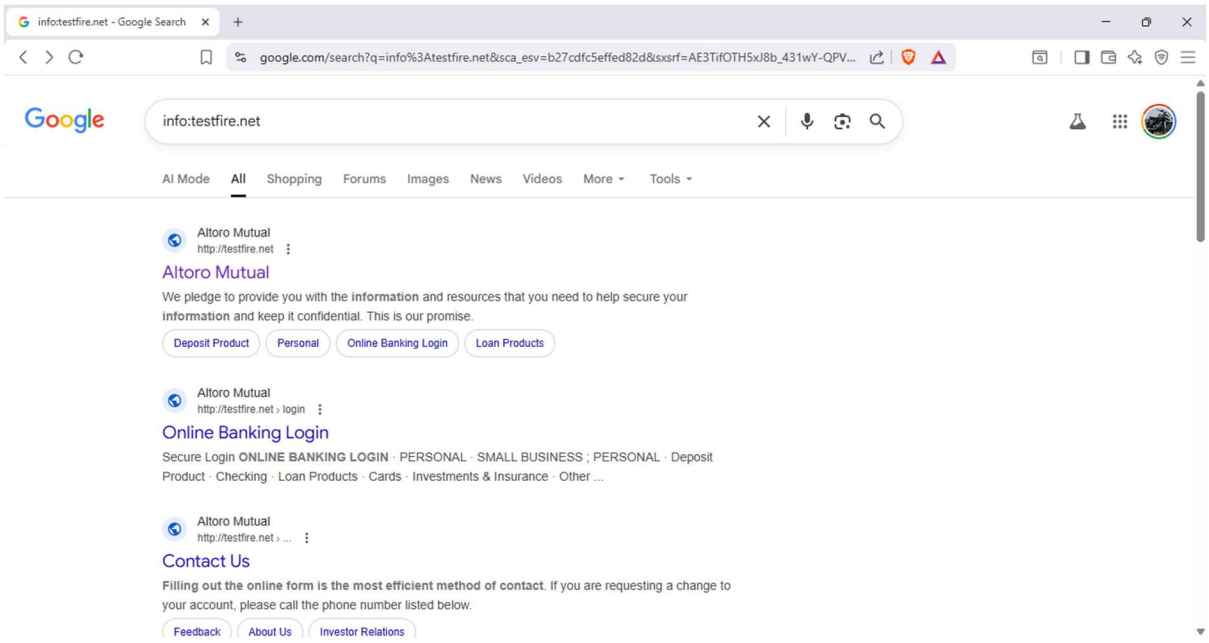


Fig.2.3 – Google Dorking, using we get target info.

c)intext: personal site: testfire.net

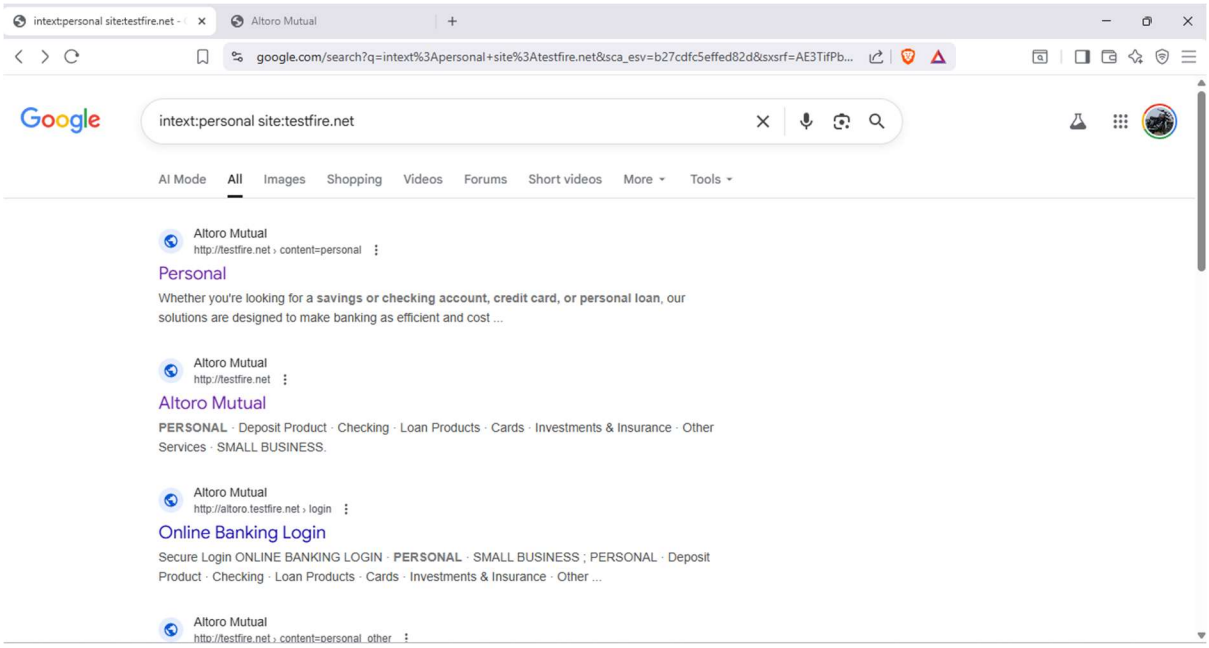


Fig.2.4 – Google Dorking, using we get personal intext of that target.

d)allintitle: testfire.net

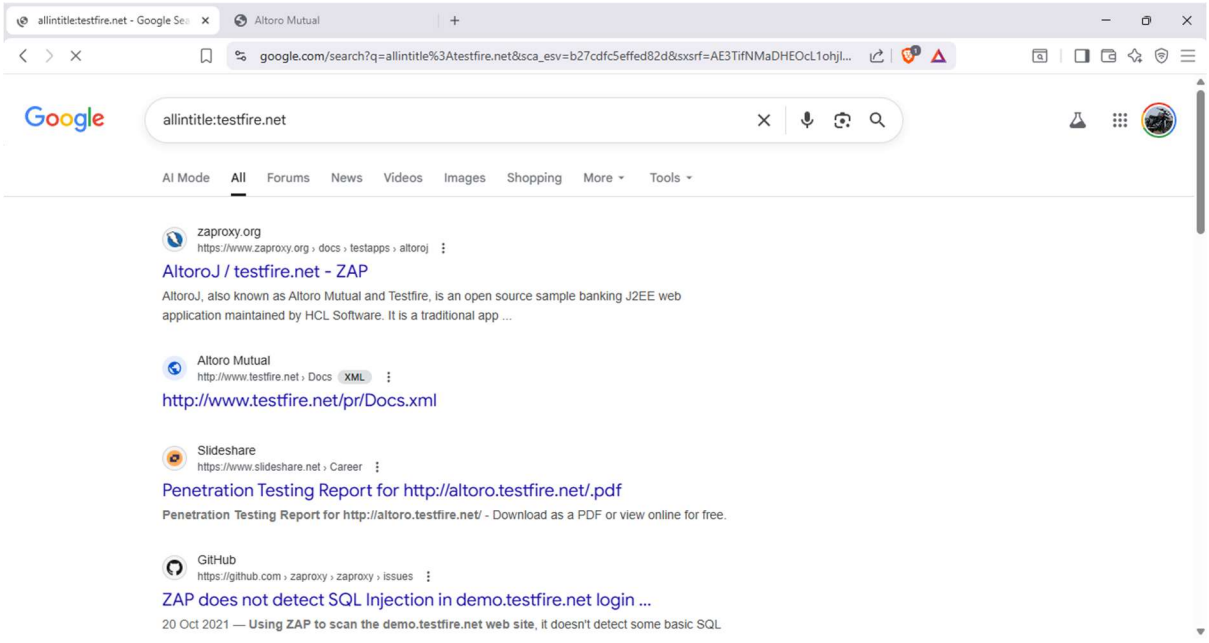


Fig.2.5 – Google Dorking, using we get related all title of that target.

e)testfire.net inanchor:admin

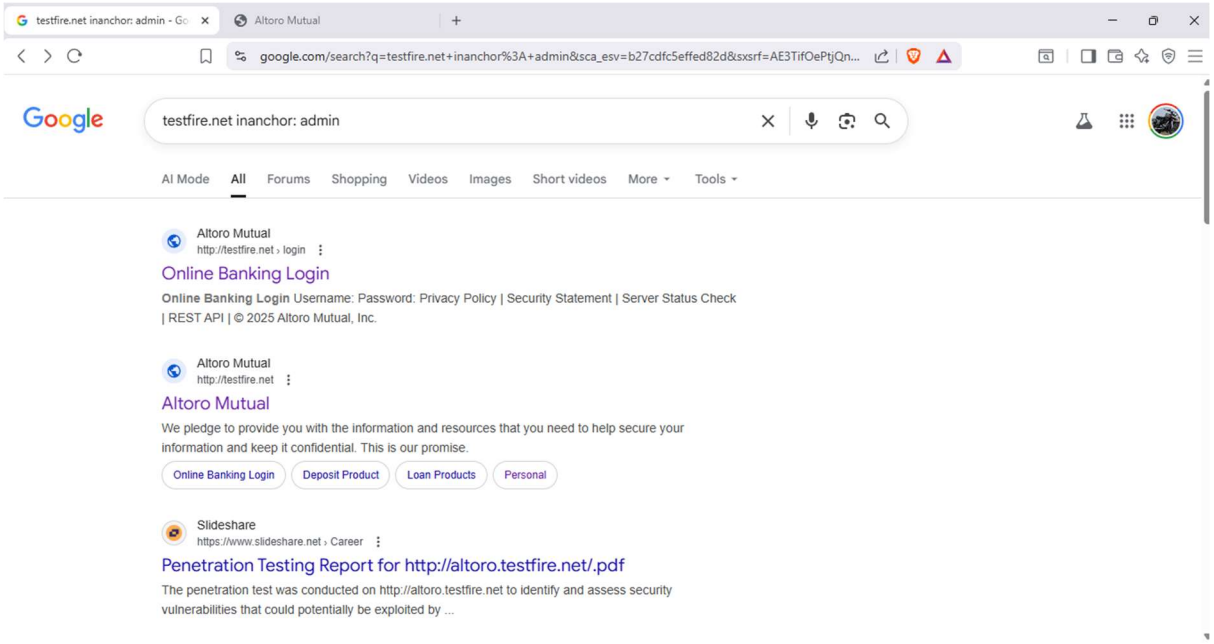


Fig.2.6 – Google Dorking, using find webpages that other sites link to using specific anchor text.

3. Footprinting using Netcraft (Web base tool):

Netcraft Website is a **public online database** that provides detailed information about who owns a **domain name, IP address, server names, subdomains, operating System**.

How to use it: - Open Browser search Netcraft and open Netcraft website after opening website gives targeted domain.

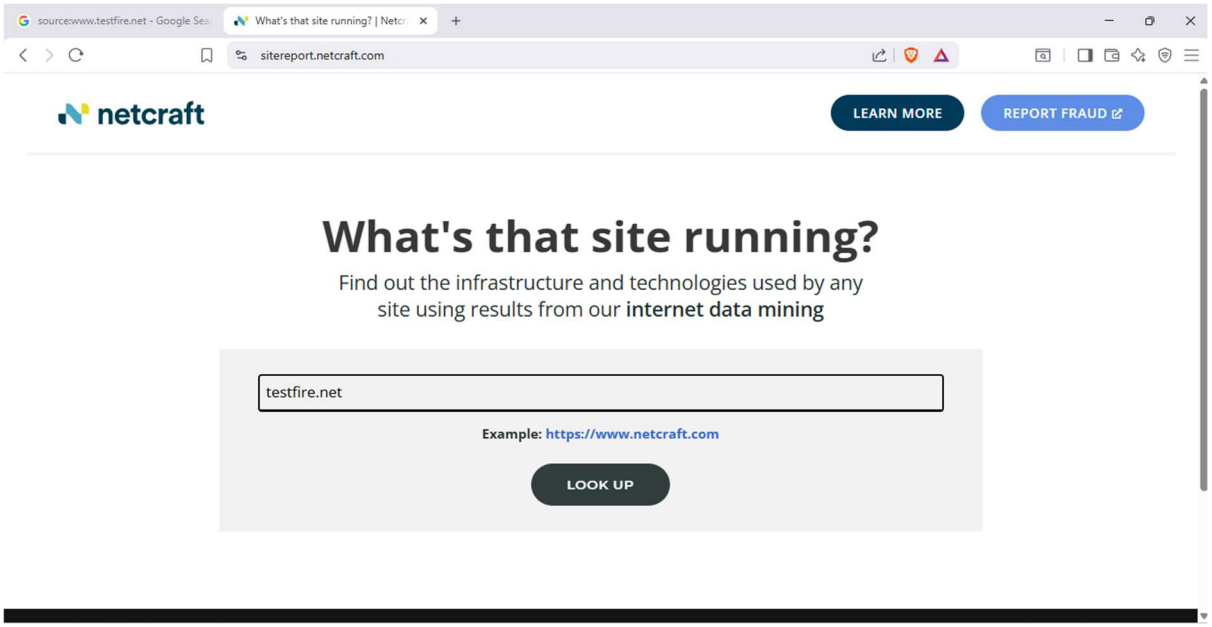


Fig.3.1 – shows netcraft website

- Here it finds some Name server and other information

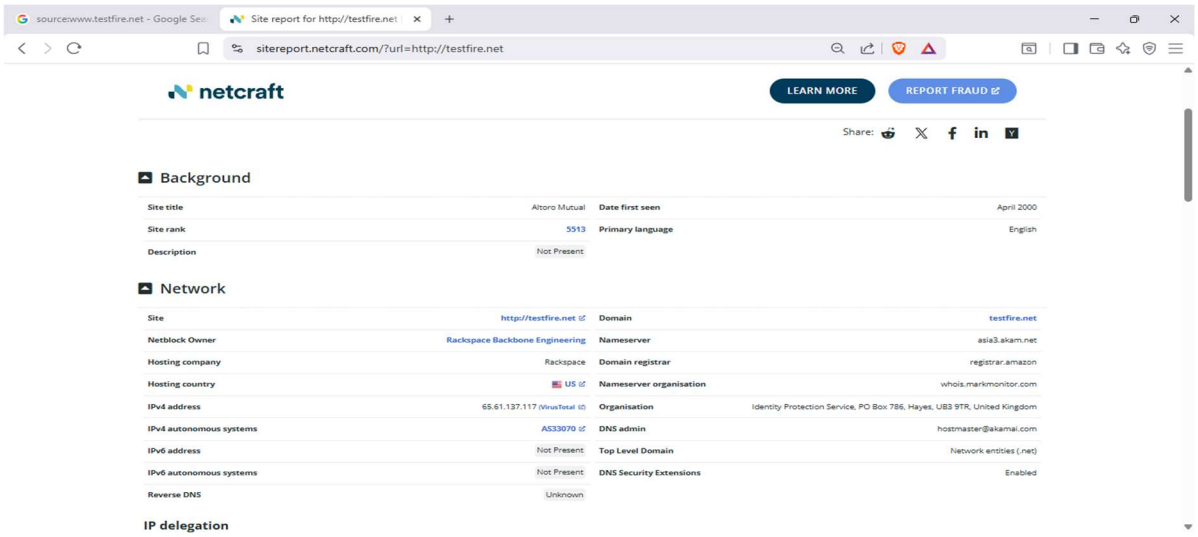


Fig.3.2 – shows target related information using netcraft.

- Hostnames matching testfire.net

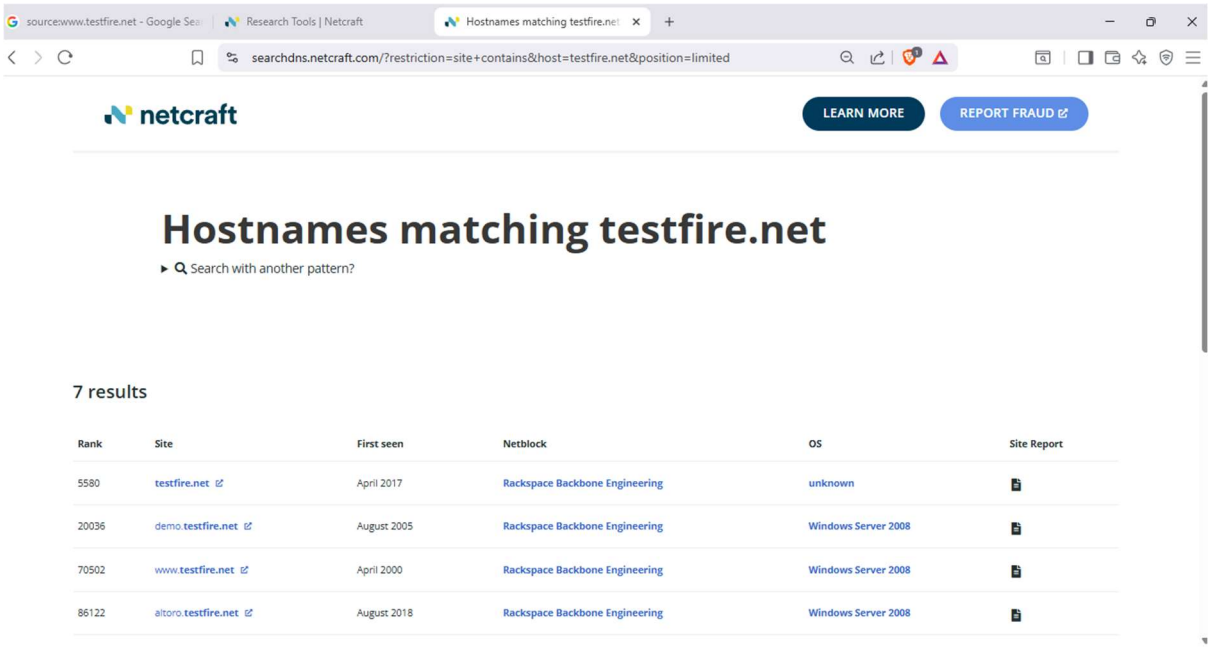


Fig.3.3 – shows target related information using netcraft.

4.Footprinting Using DNS dumpster (Web base tool):

A **DNS dumpster Website** is an online tool that helps you **find the IP address, DNS records, and server details** of a domain name.

How to use it: -search DNS dumpster on browser and open DNS dumpster website after opening website gives targeted domain.

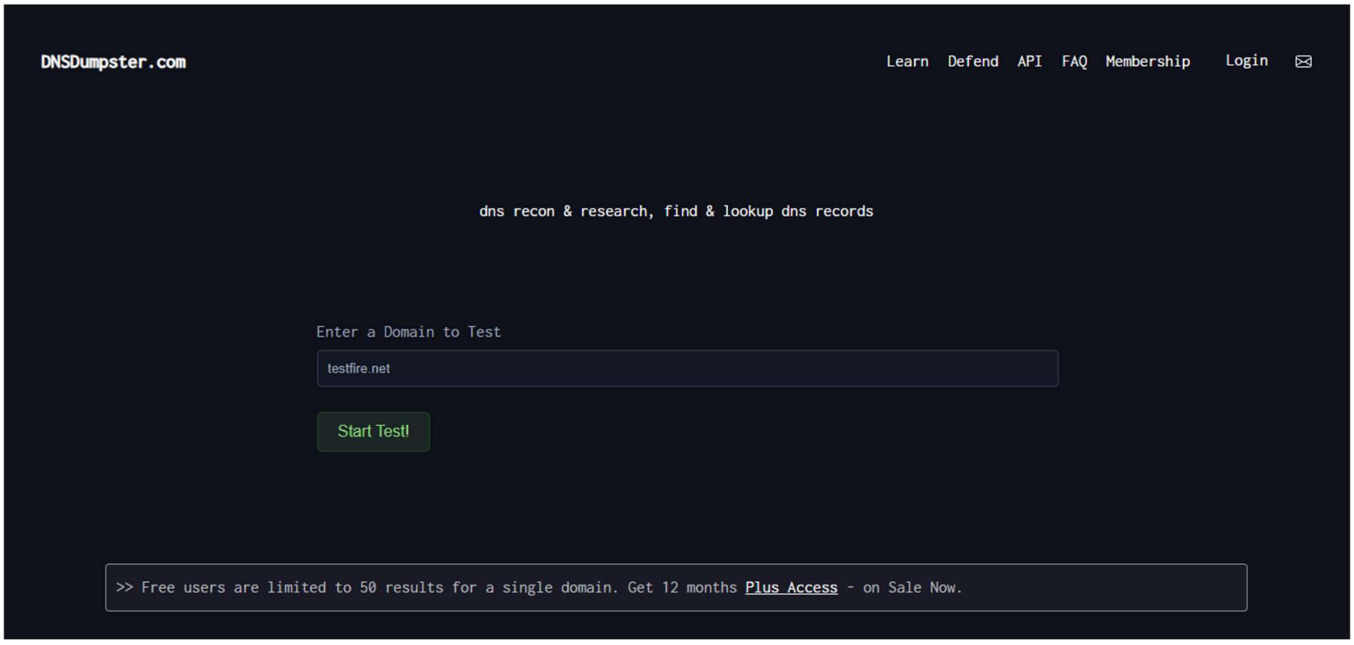


Fig.4.1 – shows DNS dumpster interface

- Shows geographical system location

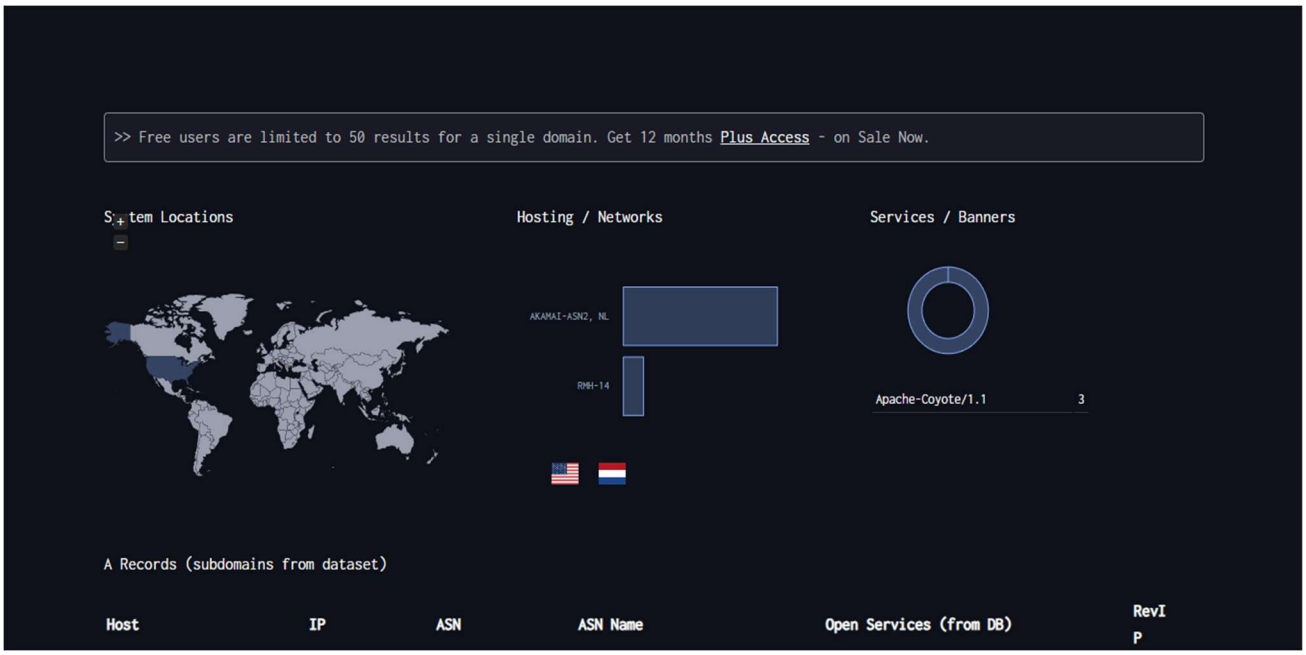


Fig.4.2 – shows target related geographical information.

- Graphical Representation shows DNS report and ip's

Fig.4.3 – shows graphical presentation of target

5.Footprinting Using Whois (Web base tool):

WHOIS Website is a **public online database** that provides detailed information about who owns a domain name or IP address.

How to use it: -Search Whois on browser and open Whois website after opening website gives targeted domain.

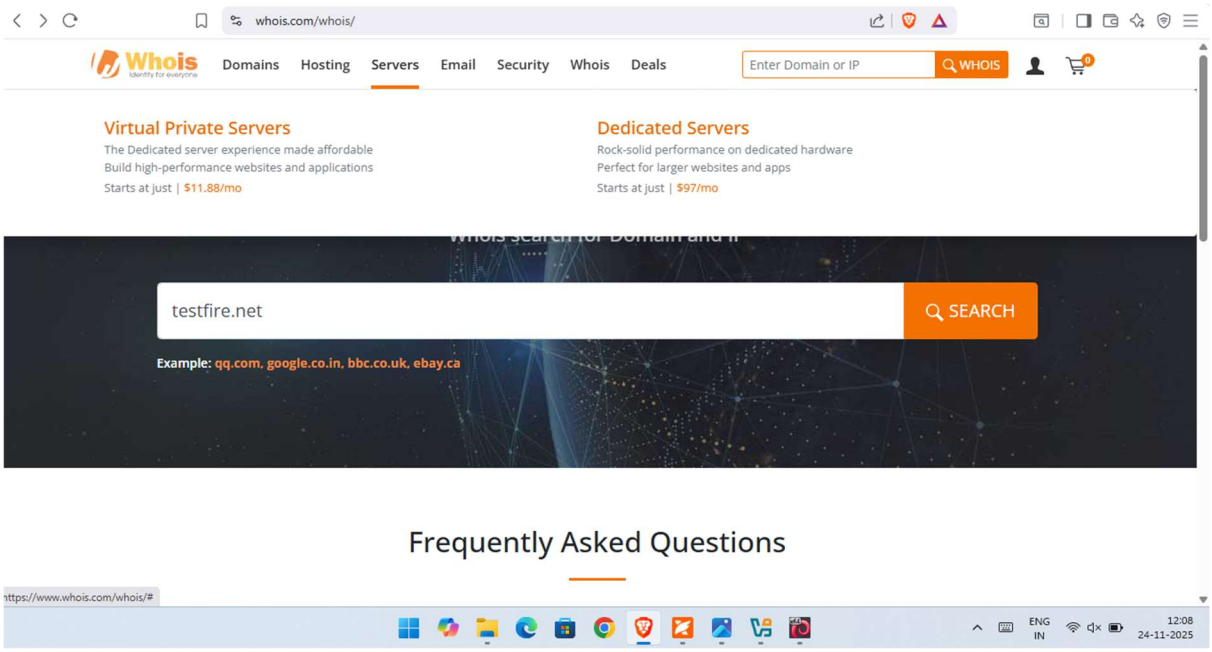


Fig.5.1 – whois interface

- Here it finds some Domain information

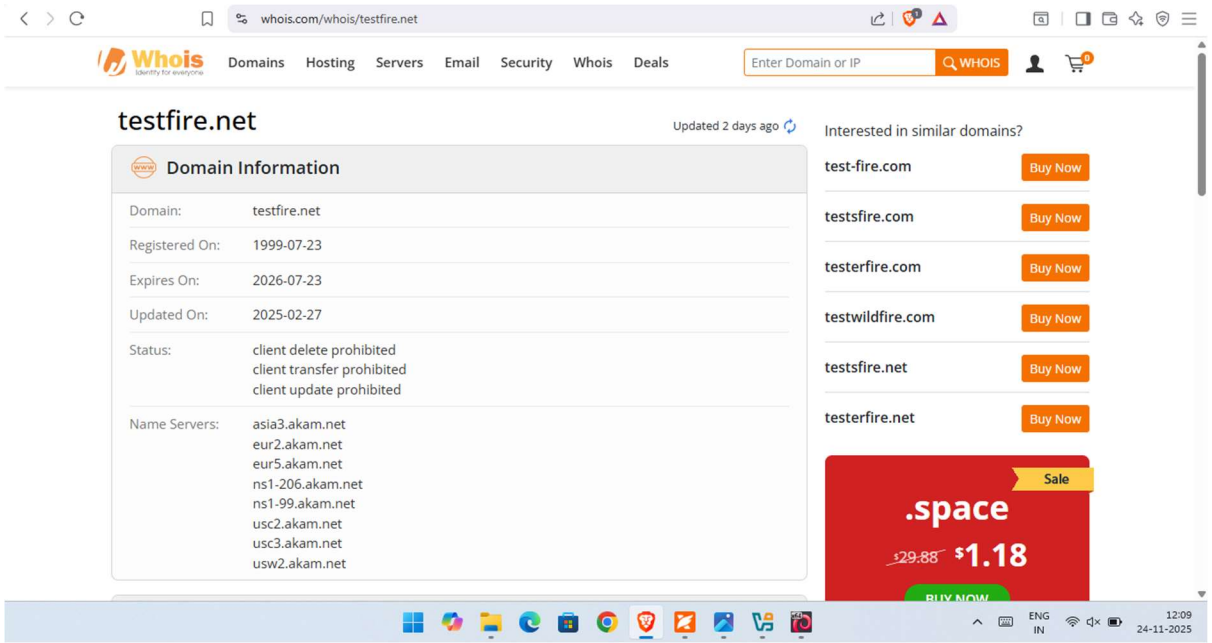


Fig.5.2 – shows target related information.

- Registrar Information and Registrant Contact

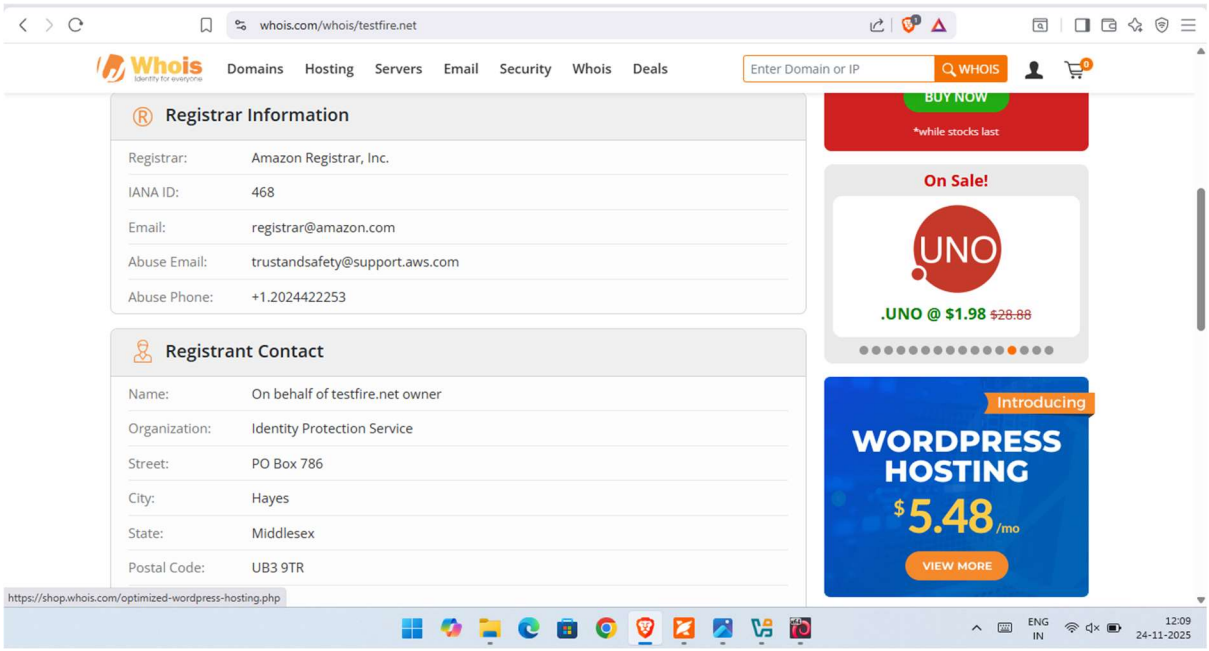


Fig.5.3 – shows target more information

6.Footprinting Using DNS Lookup (Web base tool):

A **DNS Lookup Website** is an online tool that helps you **find the IP address, DNS records, and server details** of a domain name.

How to use it: -Search Nslookup on browser and open Nslookup website after opening website gives targeted domain.

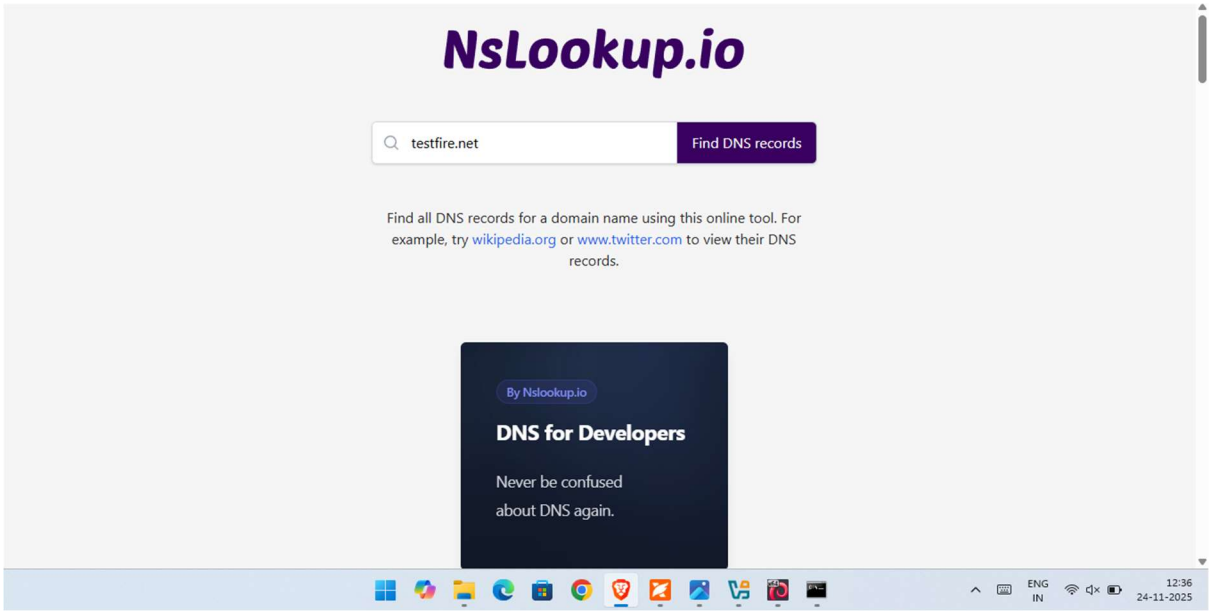


Fig.6.1- nslookup interface

- DNS Record Result

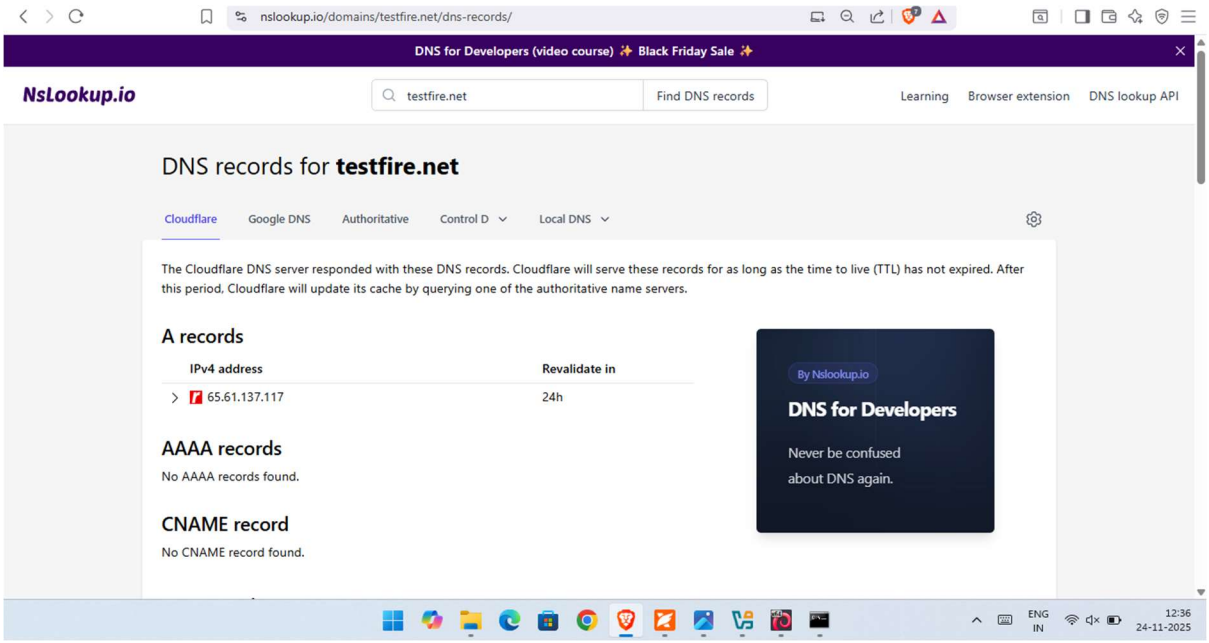


Fig.6.2- shows dns record of target.

- Ns Records/ MX records

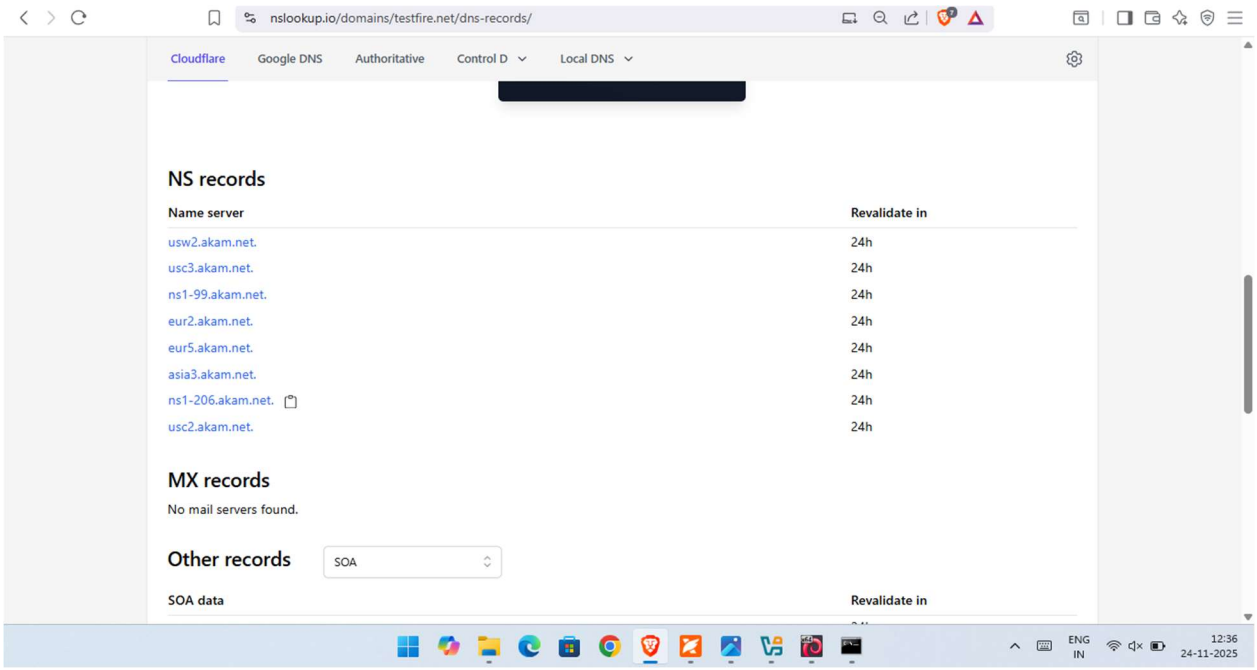


Fig.6.3- shows ns records of target.

7. Footprinting Using Sublister CLI Tool: -

How to use it: - Open Kali Linux and run Terminal**.**

Command- sublist3r -d testfire.net using this command, we get sub domains. Here **-d** use to put domain in command line.

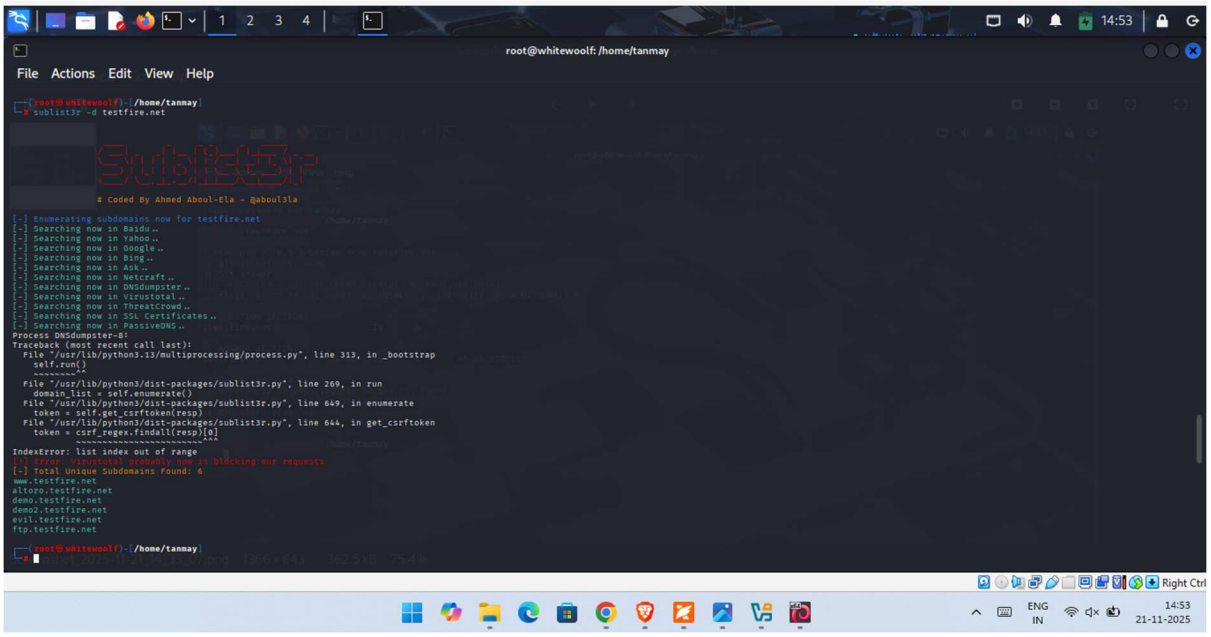


Fig.7.1- shows sub domain using sublister.

8. Footprinting Using Traceroute CLI Tool: -

How to use it: - Open Kali Linux and run Terminal**.**

Command- traceroute testfire.net using this command, we get hopes.

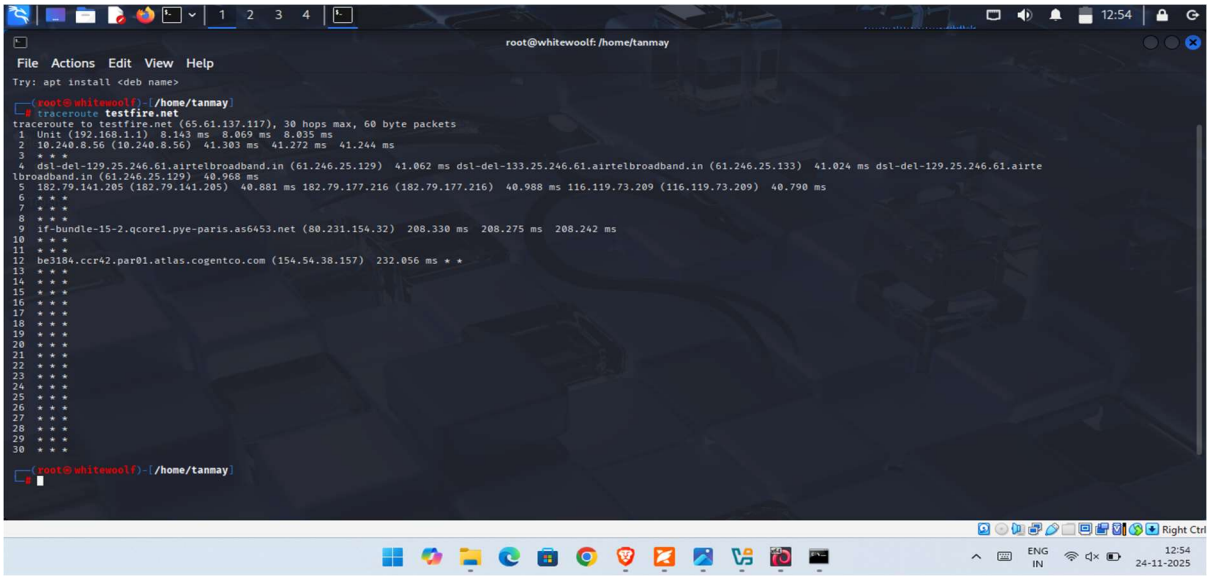


Fig.8.1- shows in between hopes

9. Footprinting Using recon-ng CLI Tool: -

How to use it: - Open Kali Linux and run Terminal**.**

Command- recon-ng using this command tool get start. As shown below-

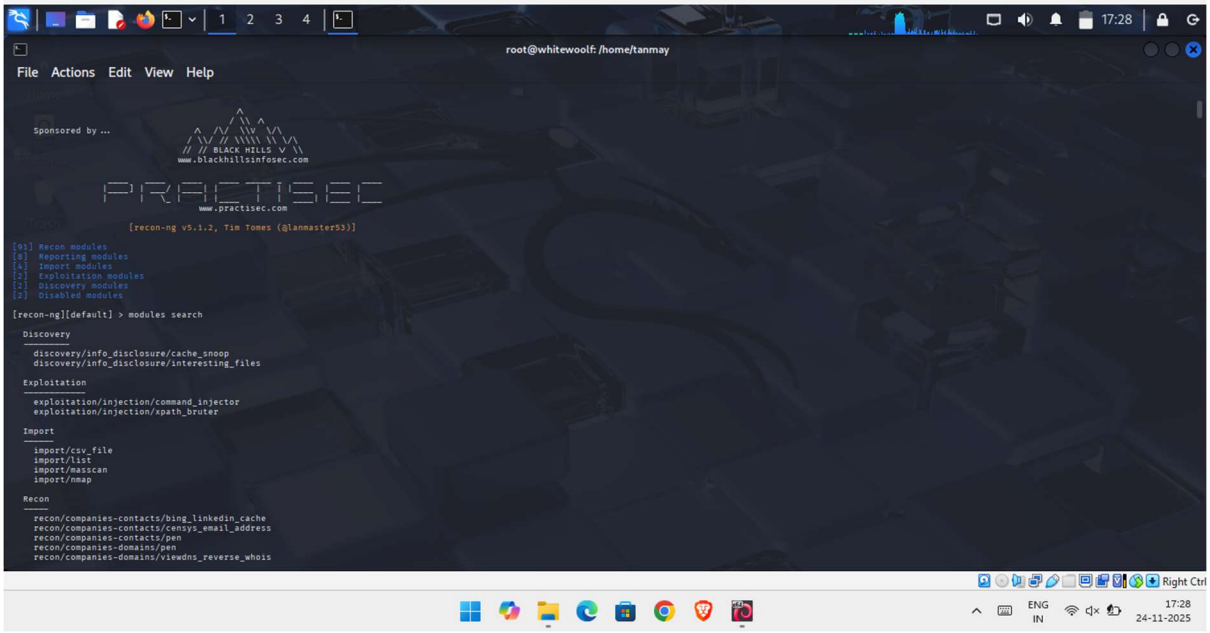


Fig.9.1- Starting of tool

- **Create Workspace using command- workspace create CEH**

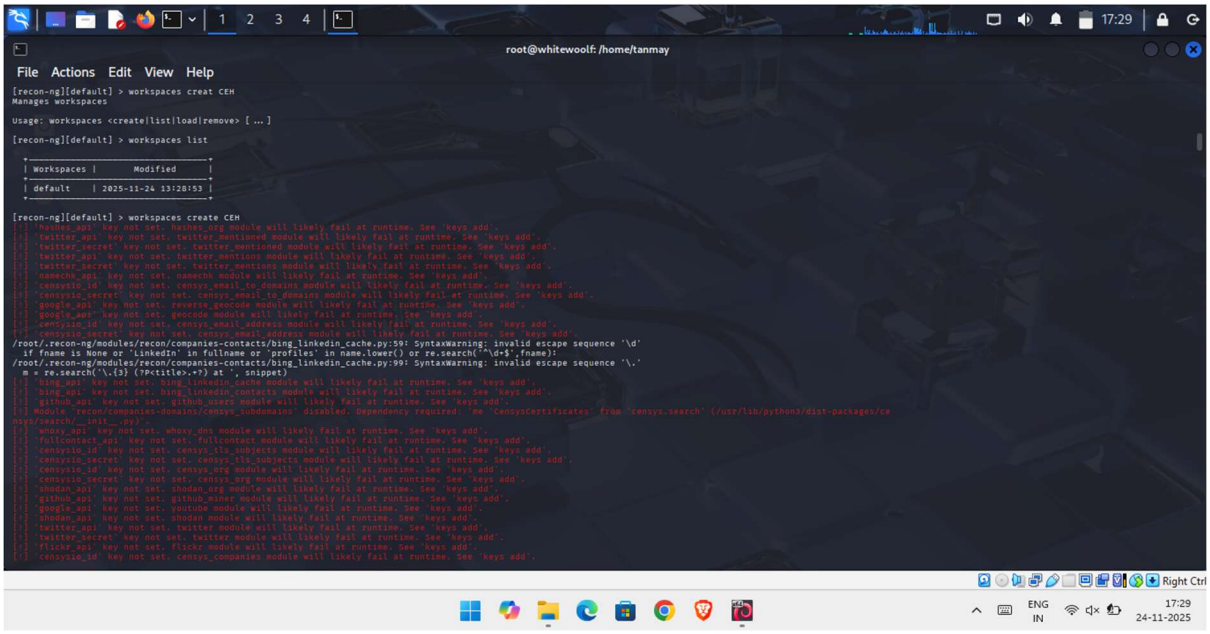


Fig.9.2- Creating work space.

- To check work space is created or not **Command – workspace list**

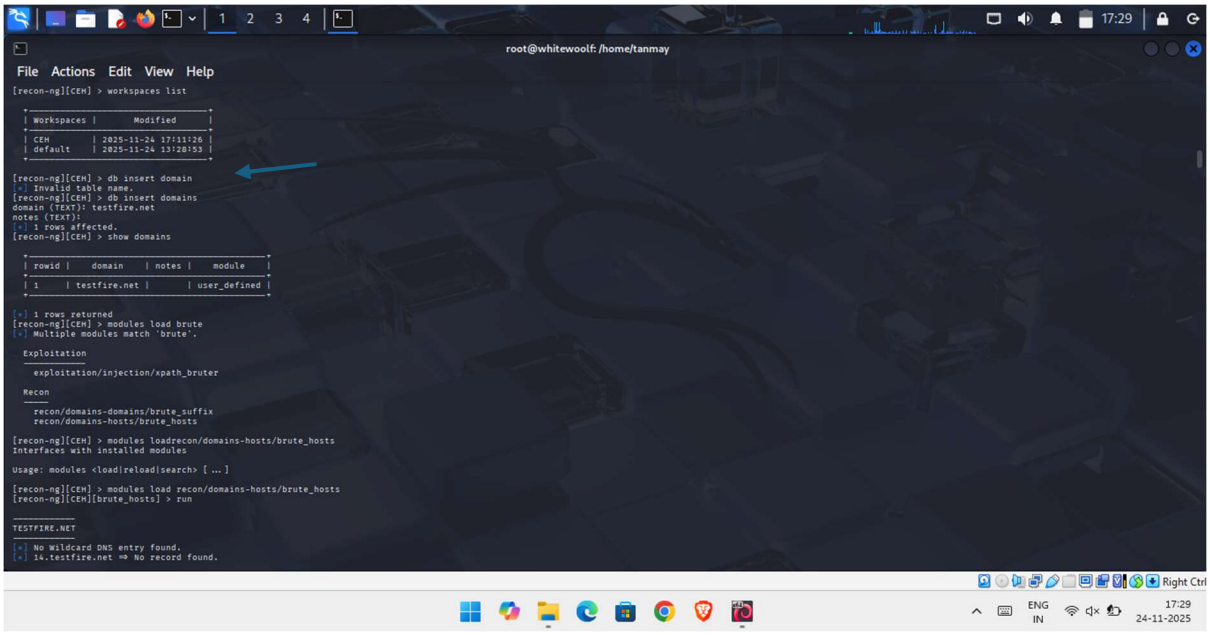


Fig.9.3- shows work list

- To insert Domain in workspace **Command- db insert domains** and press **enter** after pressing enter insert domain and press **enter.**

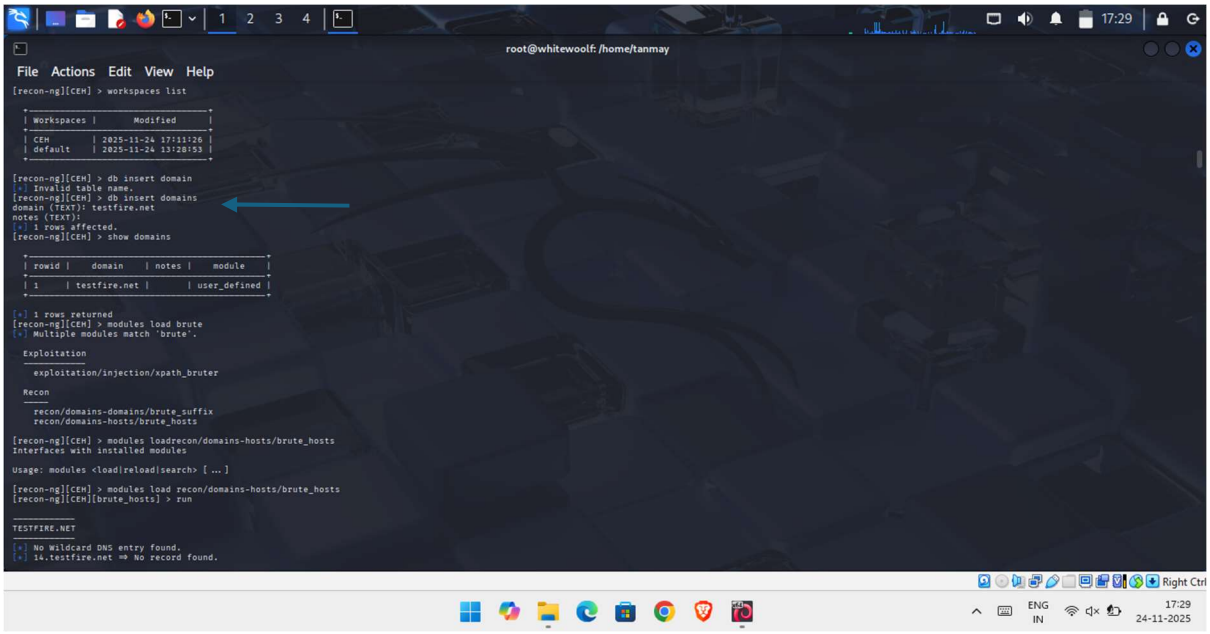


Fig.9.4- Adding target in database.

- To check domain is created in workspace or not **Command-Show domains**

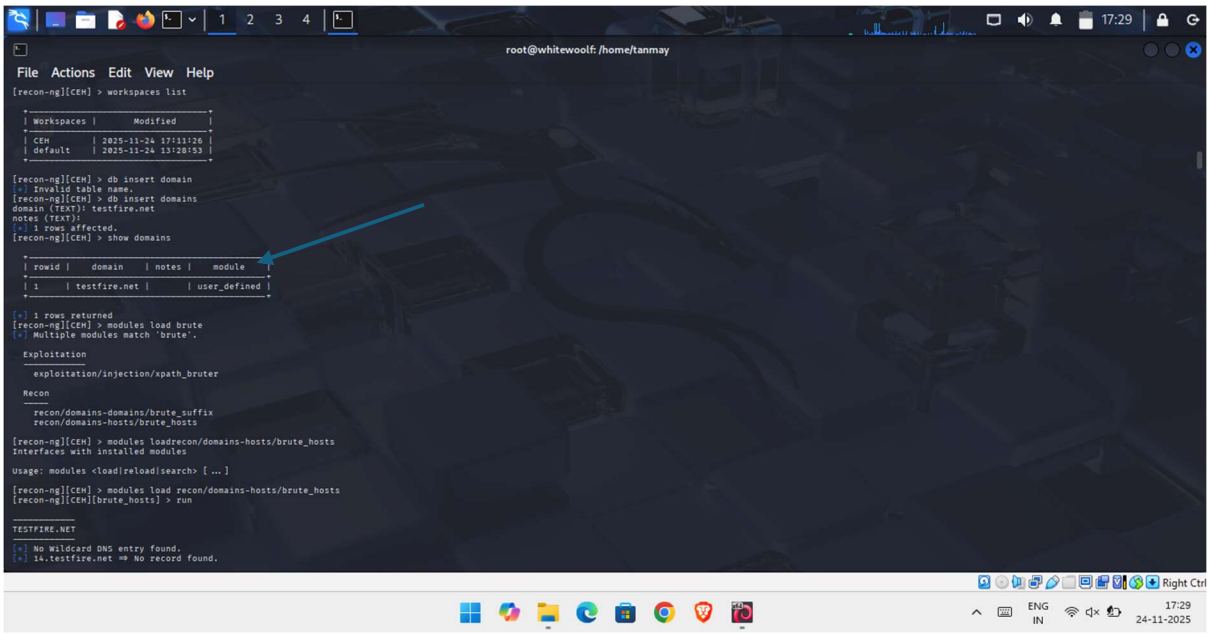


Fig.9.5- shows added list of domains.

- Then Load module **Command- modules load brute**

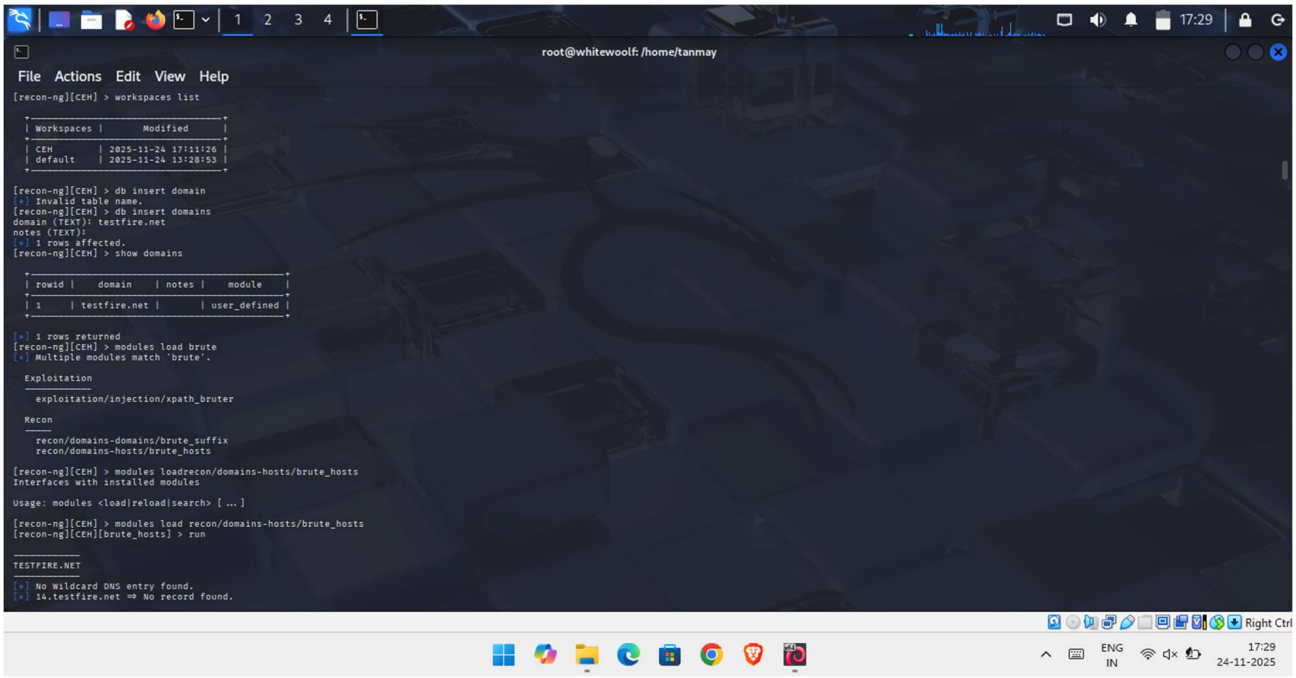


Fig.9.6- Selecting recon.

- Then recon model load
  Command- modules load recon/domain-hosts/brute_hosts and press **enter.**
  For work this command give **Command- Run.**

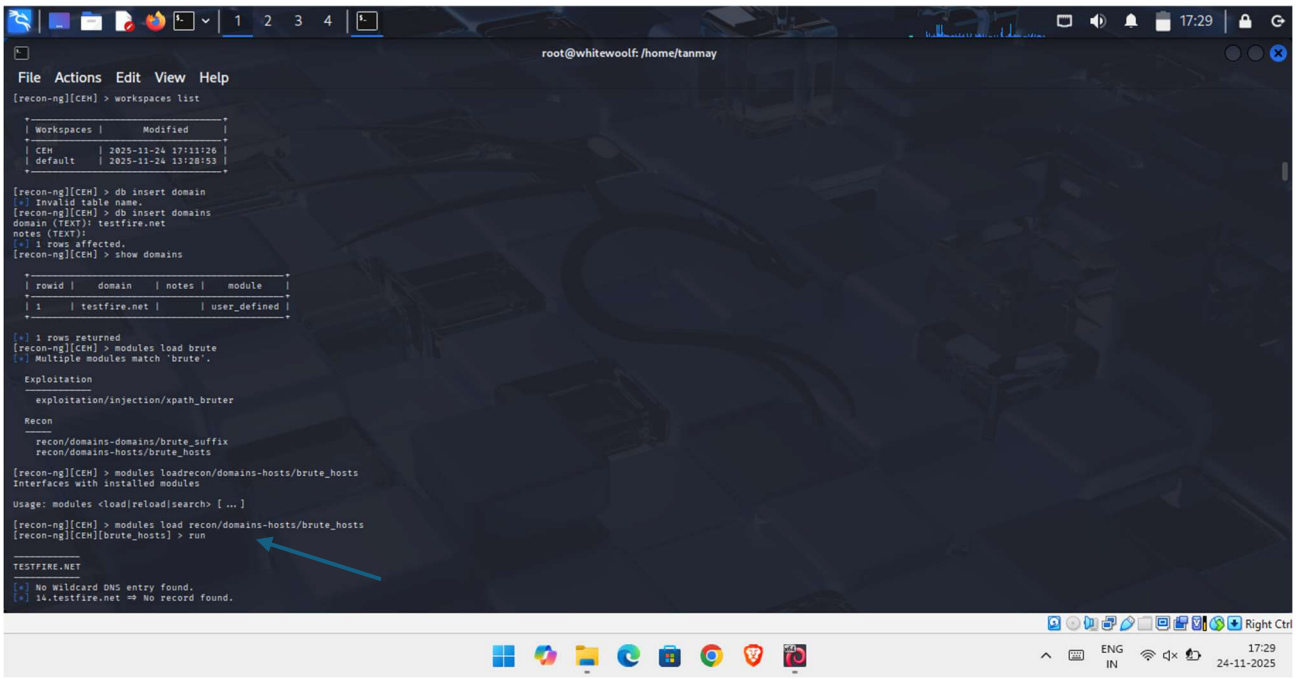


Fig.9.7- Running recon.

- After running above commands, it shows hosts as result for seeing that hosts.
  Command-Show host

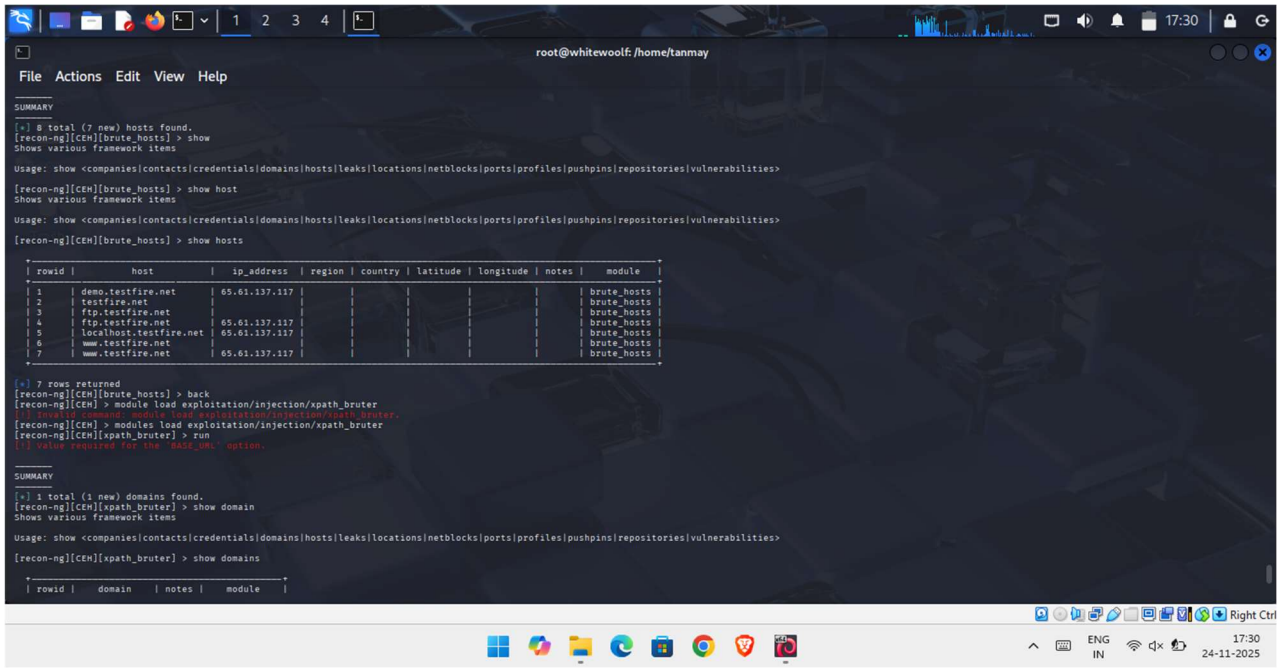


Fig.9.8- Showing subdomain.

10. Footprinting Using Nikto CLI Tool: -

How to use it: - Open Kali Linux and run Terminal**.**

Command- nikto -host testfire.net

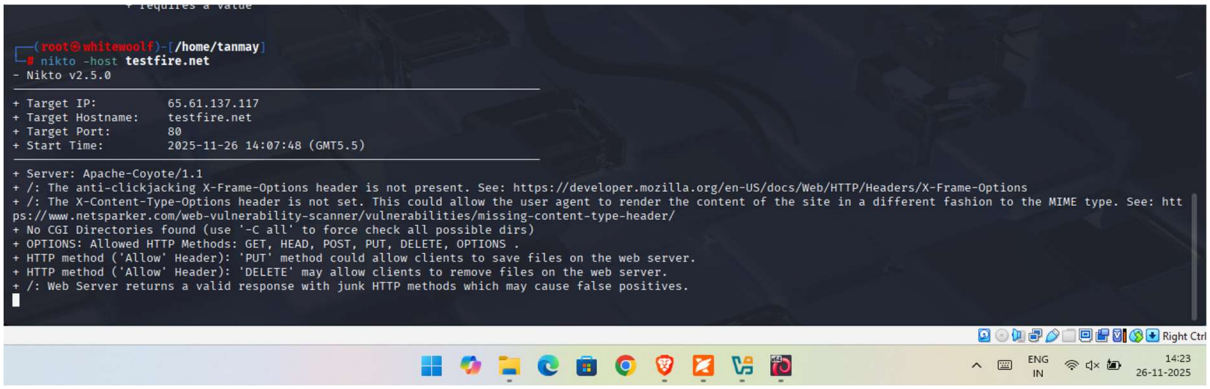


Fig.10.1- Running nikto tool.

11. Footprinting Using NAPALM FTP indexer (web base tool): -

How to use it: - Open any browser and search napalm ftp indexer**.** After searching in browser open first website shown after that give domain name to search for ex.microsoft using this tool we get all the words related data.

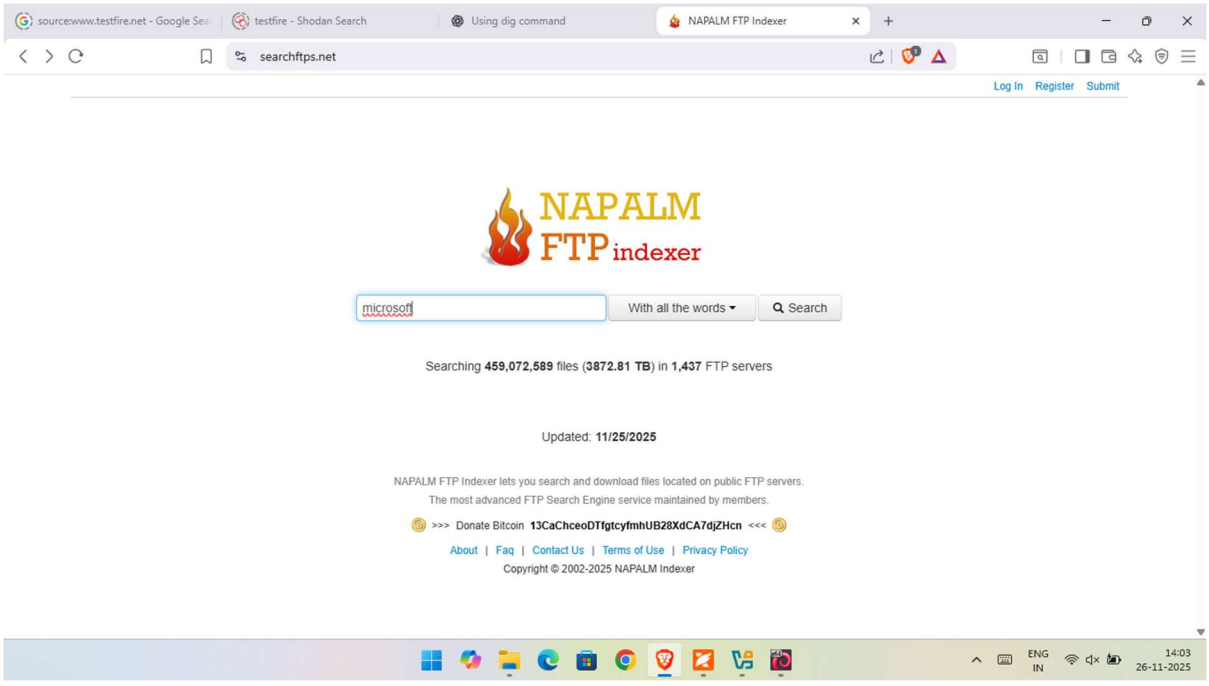


Fig.11.1- NAPALM interface.

- Result

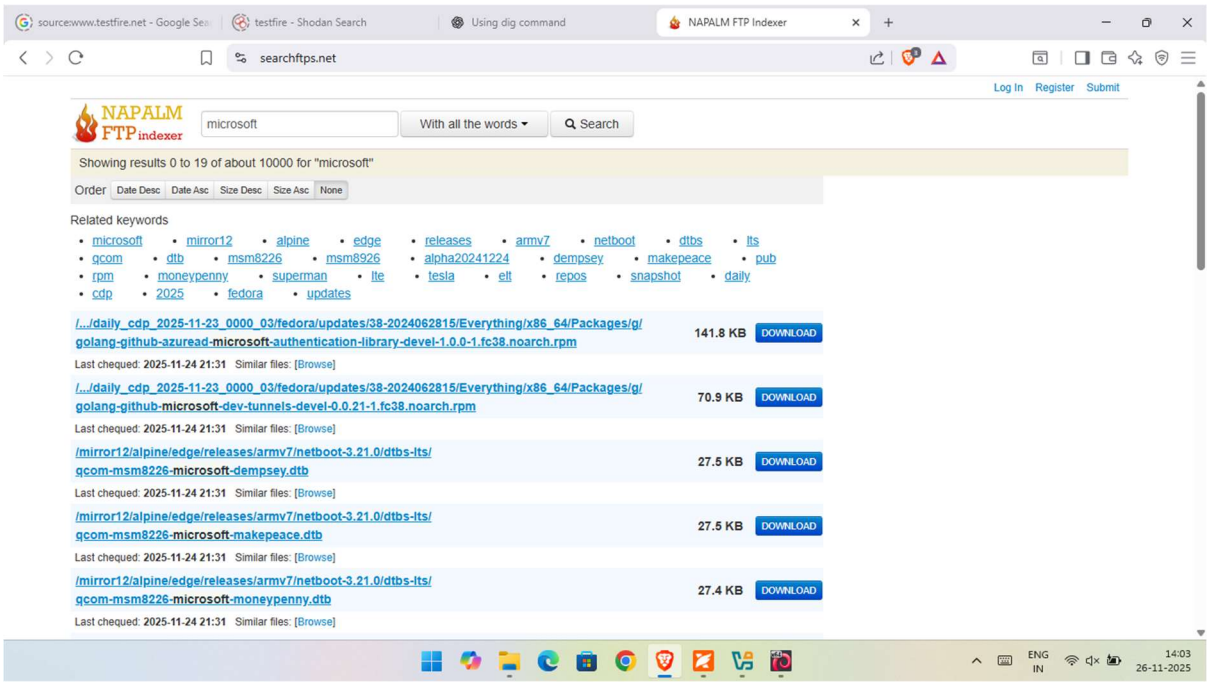


Fig.11.2- Showing Result.

12. Footprinting Using OSINT Framework (web base tool): -

How to use it: - Open any browser and search osint framework**.** After searching in browser open first website.

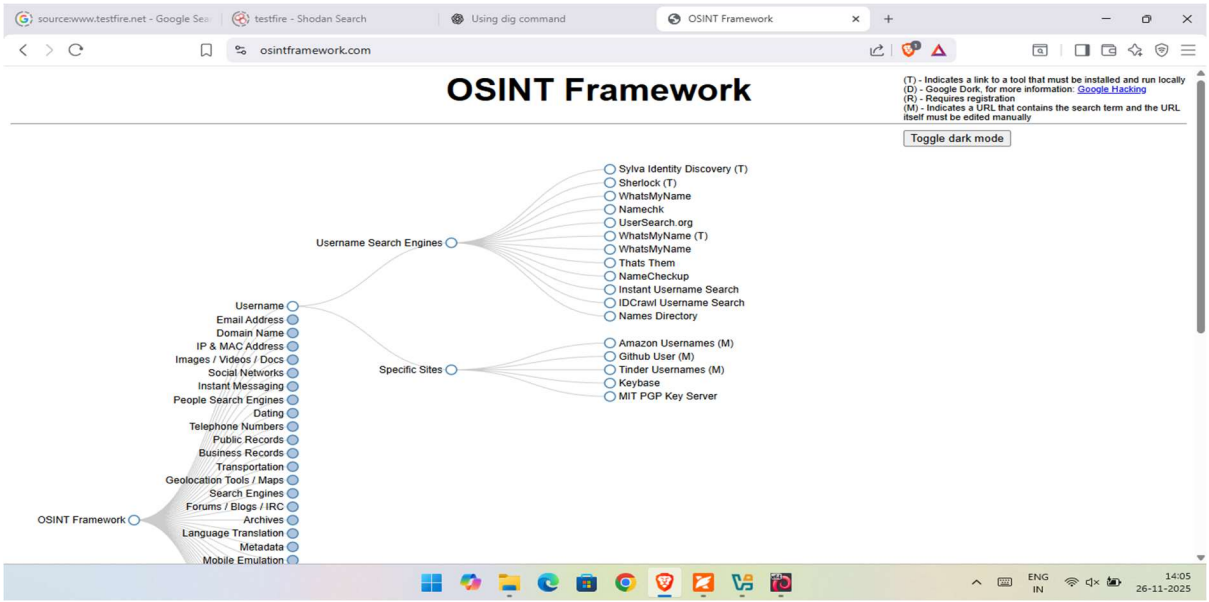


Fig.12.1- Interface of OSINT.

- Deep Result

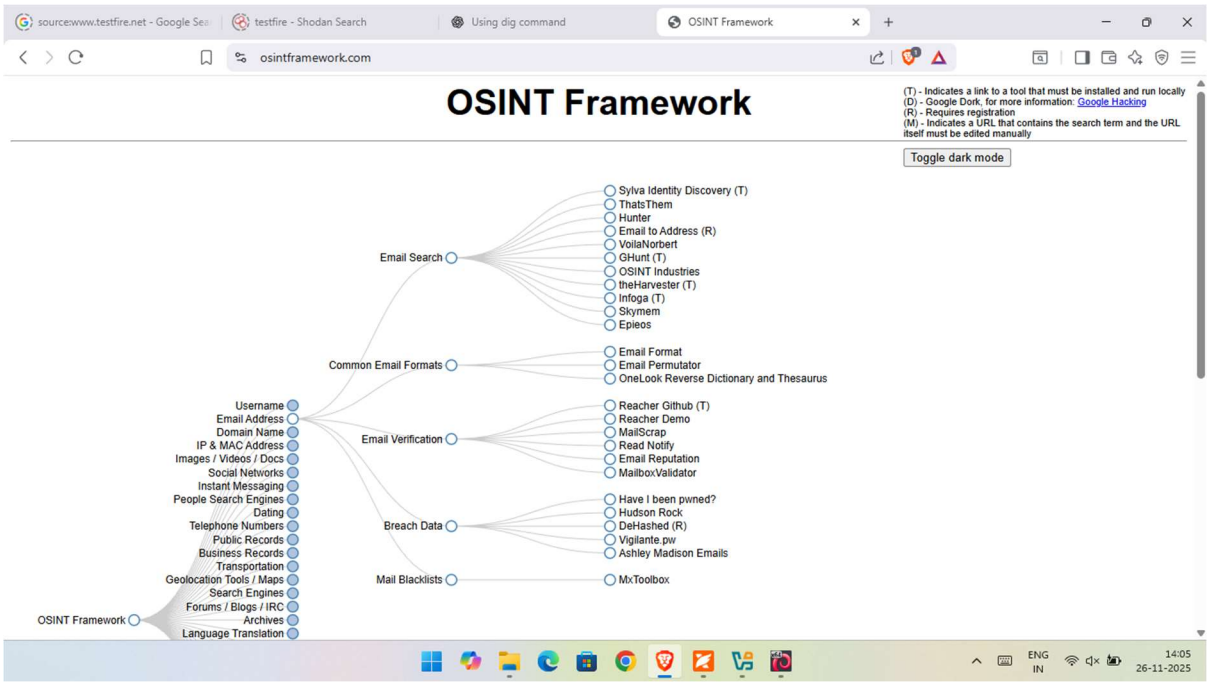


Fig.12.2 – Shows email OSINT.

- Results

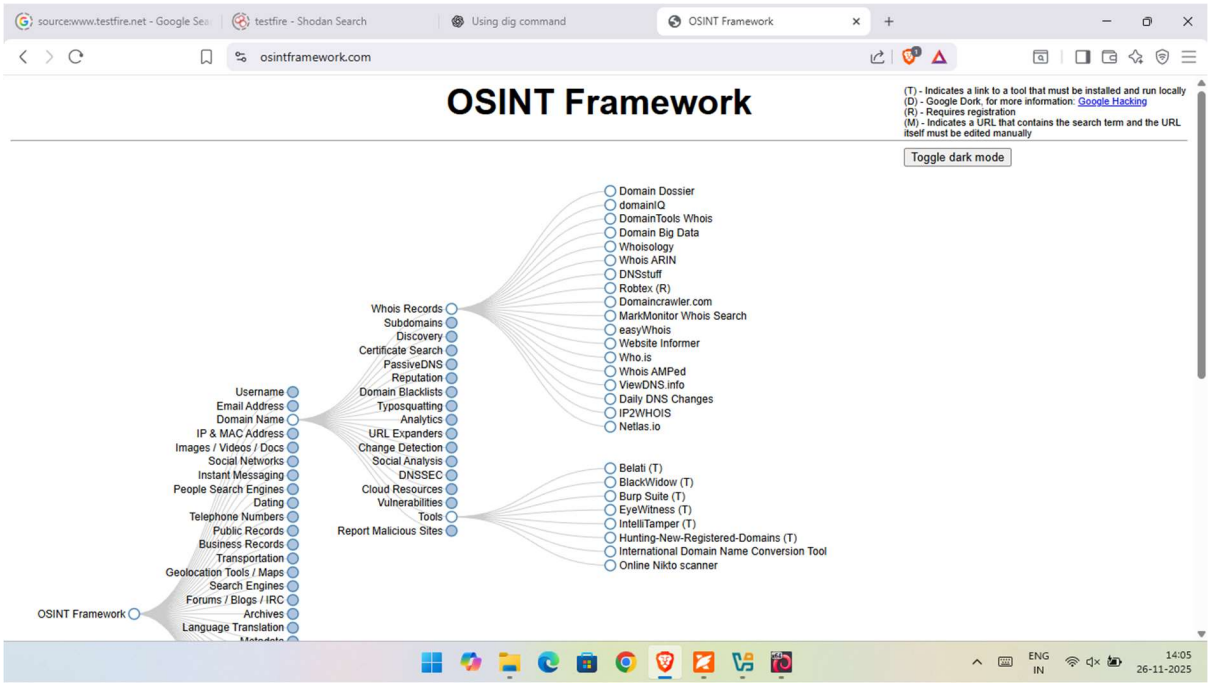


Fig.12.3- shows OSINT.

13. Footprinting Using email spider (software base tool): -

How to use it: - open the tool and in URL box give the URL of target and click on start button.

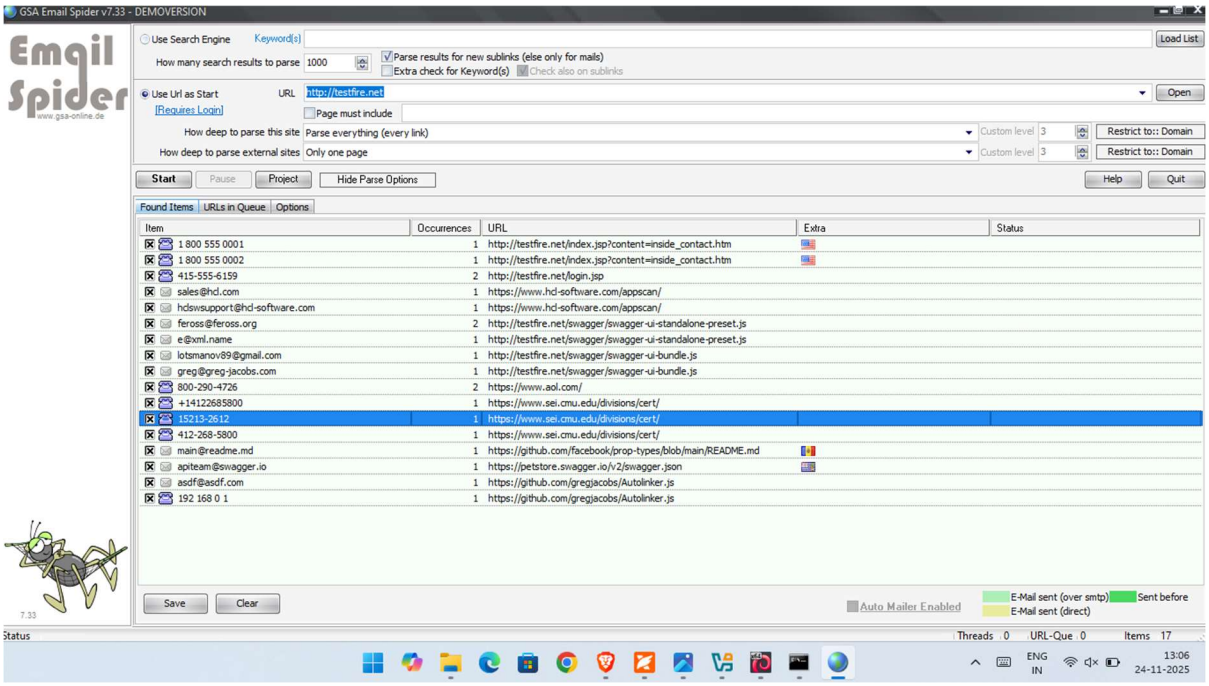


Fig.13.1- shows Email spider result.

14. Footprinting Using dig (CLI base tool): -

How to use it: - Open Kali Linux and run Terminal**.**

Command – dig ns certifiedhacker.com here **ns** use for find ns records.

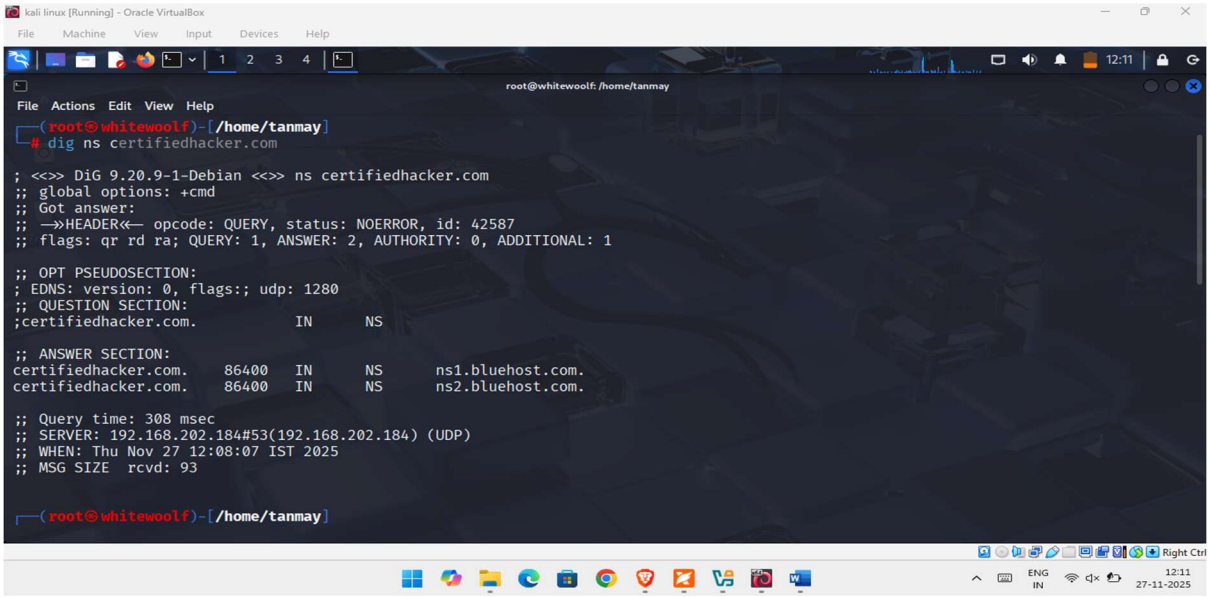


Fig.14.1- Shows ns records.

- here using NS record transferring zone. If transfer is successful then zone transfer is completed and if that failed means dns is stopping to transfer.

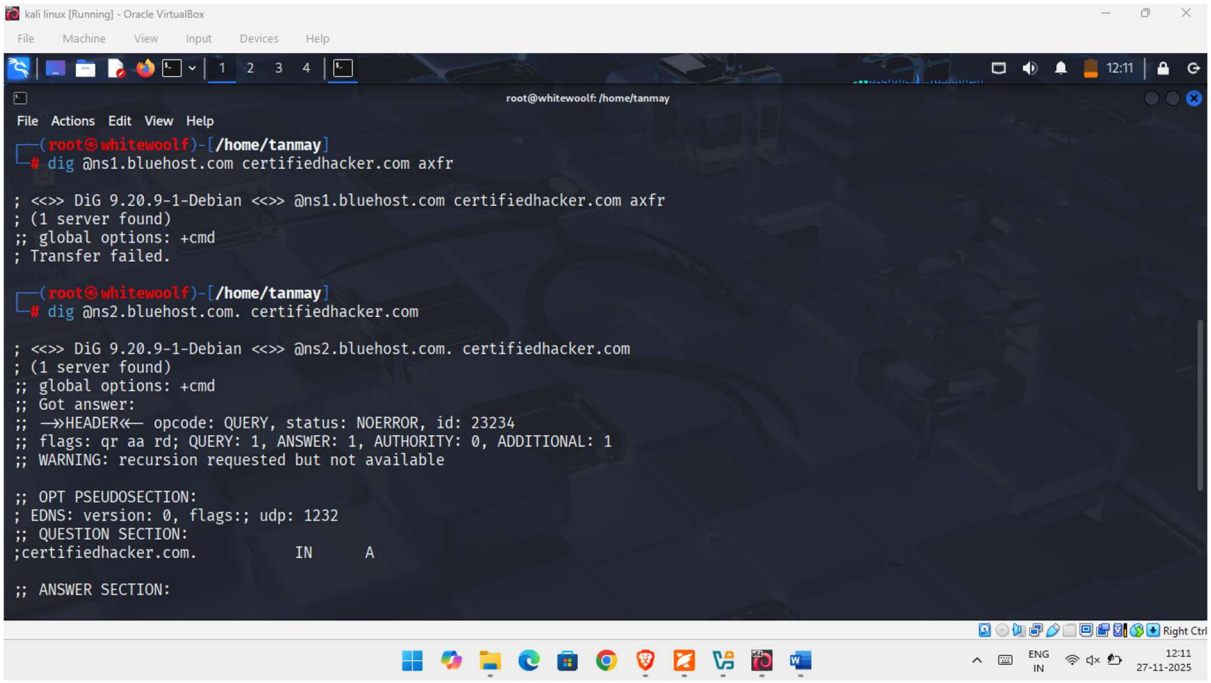


Fig.14.2- Shows Zone transfer result.

15. Footprinting Using dnsenum (CLI base tool): -

How to use it: - Open Kali Linux and run Terminal**.**

Command – dnsenum -enum certifiedhacker.com it is automated tool that using this command automatically transfer the zone.

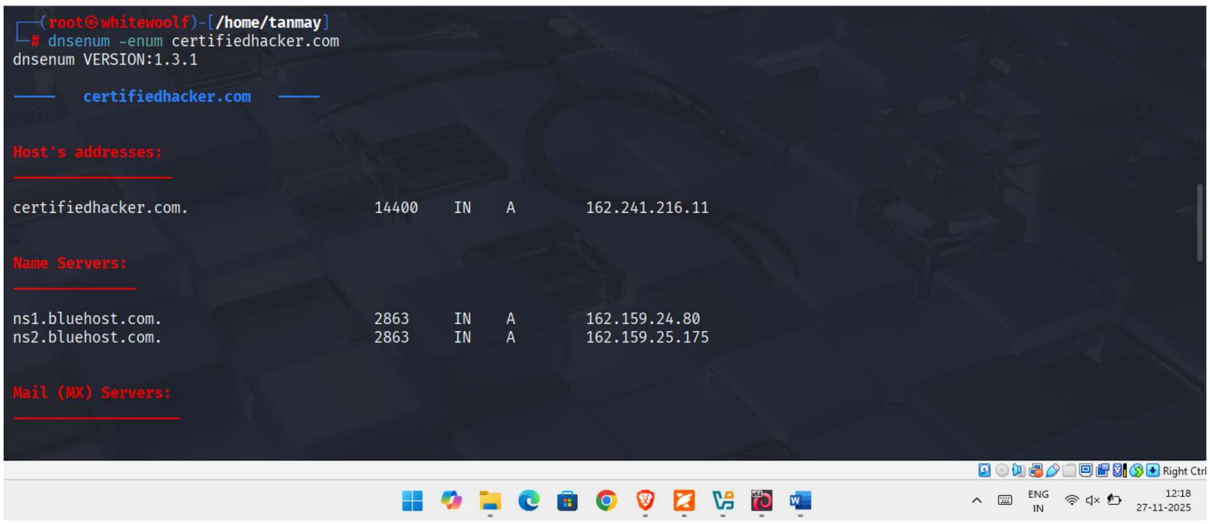


Fig.15.1- Shows NS record result.

- here it started to zone transfer

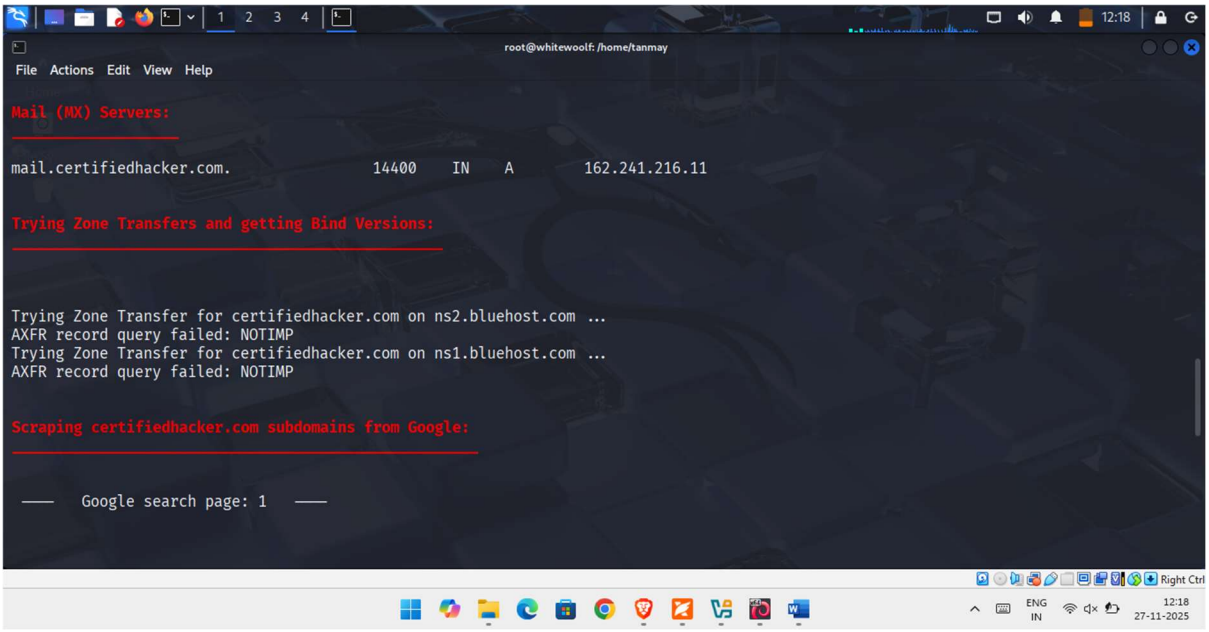


Fig.15.2- Shows Zone transfer result.

16. Objective

- To gather publicly available information about a target system or organization.
- To identify domains, IP addresses, network structure, and technologies used.
- To discover potential vulnerabilities, entry points, and weak security areas.
- To understand the target's attack surface before performing deeper testing.
- To support planning for scanning and penetration testing with accurate information.