REPORT OF FOOTPRINTING AND RECONNAISSANCE

ANIKET

Aniket Sunil Pagare

Footprinting and Reconnaissance

MODULE - 2

Footprinting and Reconnaissance --

Footprinting refers to the process of collecting information about a target network and its environment, which helps in evaluating the security posture of the target organization's IT infrastructure.

Reconnaissance refers to collecting information about a target, which is the first step in any attack on a system.

Objective-:

The objective of the lab is to extract information about the target organization that includes -:

- **Organization Information -:** Employee details, addresses and contact details, partner details, weblinks, web technologies, patents, trademarks, etc.
- **Network Information -:** Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information
- **System Information -:** Operating systems, web server OSes, location of web servers, user accounts and passwords, etc.

Footprinting can be categorized into passive footprinting and active footprinting:

- **Passive Footprinting** : Passive footprinting involves gathering information about a target without directly interacting with the target system.
- **Active Footprinting** : Active footprinting involves directly interacting with the target system to gather information.

ANIKET

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

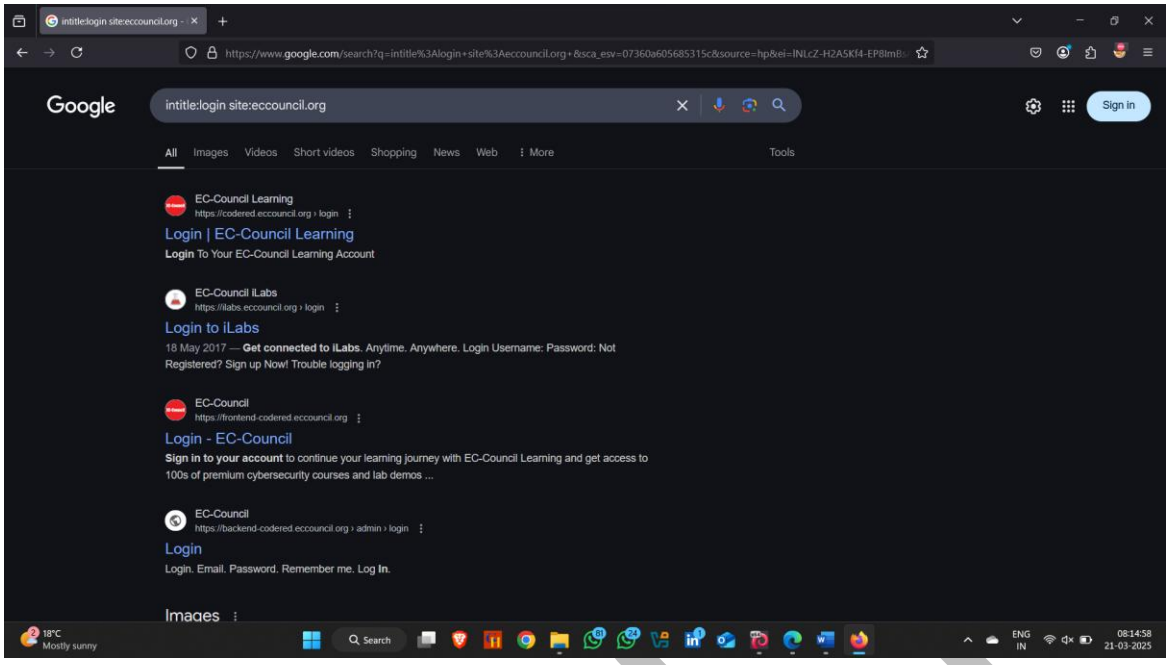
1. Gather Information using Advanced Google Hacking Techniques

- Intitle:login site:eccouncil.org

The **intitle:** keyword is a Google search operator used to find web pages with specific words in their **title tags**.

The **site**: keyword is a powerful search operator used in search engines like Google to restrict search results to a specific website or domain.

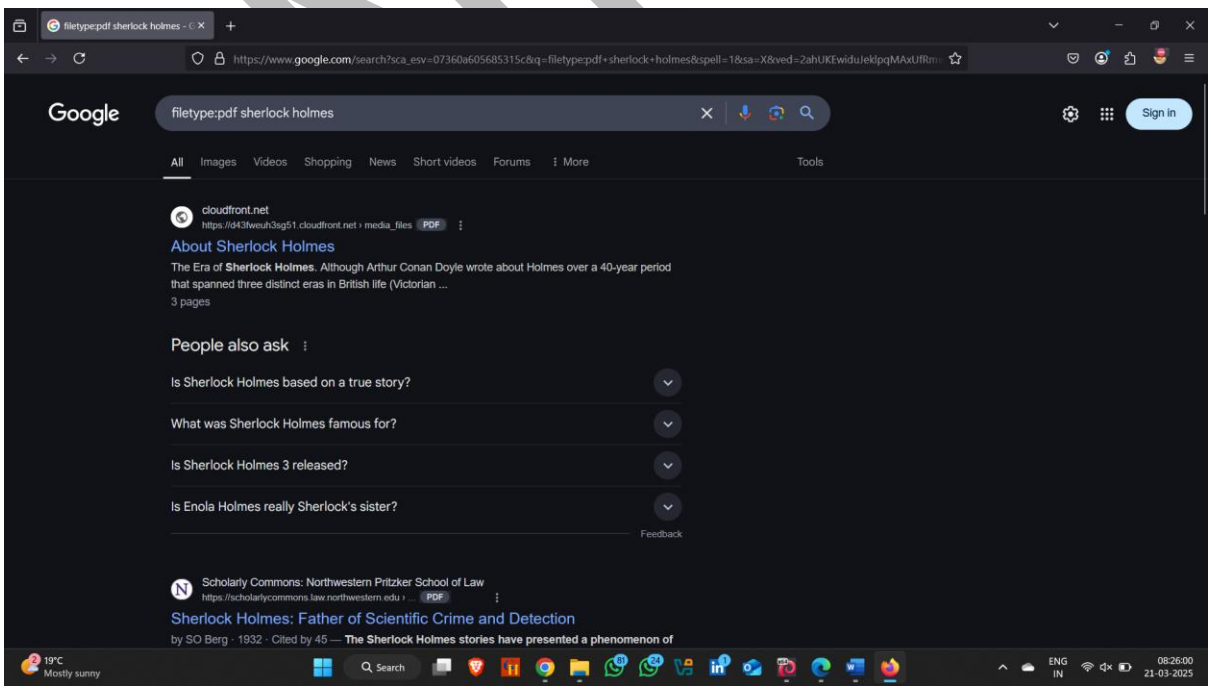
ANIKET



- Filetype :pdf sherlock holmes

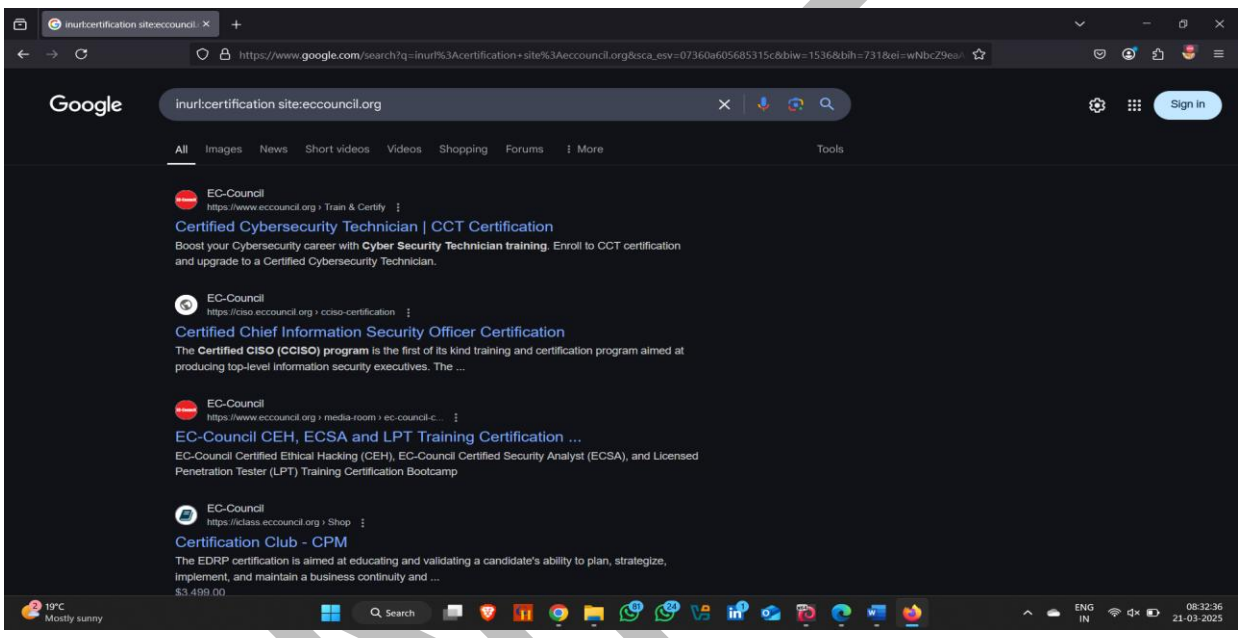
  The **filetype:** search operator is a powerful Google search tool that helps you find specific file types on the web. It's useful when searching for documents, presentations, spreadsheets, and more.

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



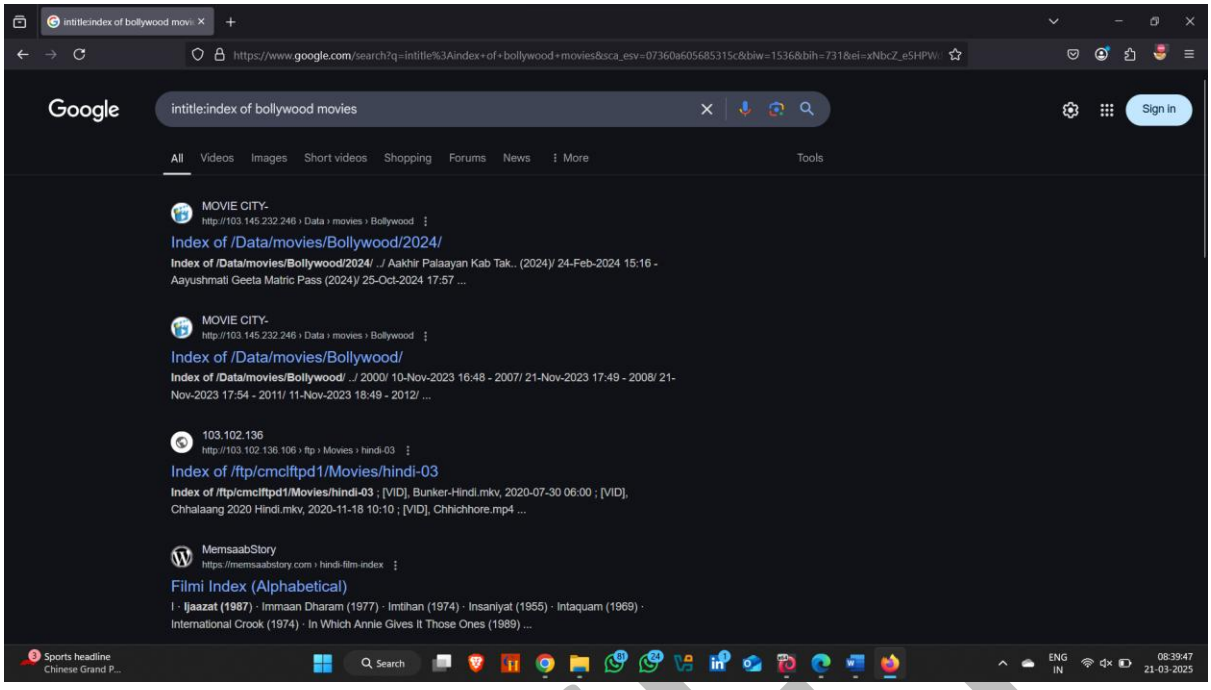
- Inurl :certification site:eccouncil.org

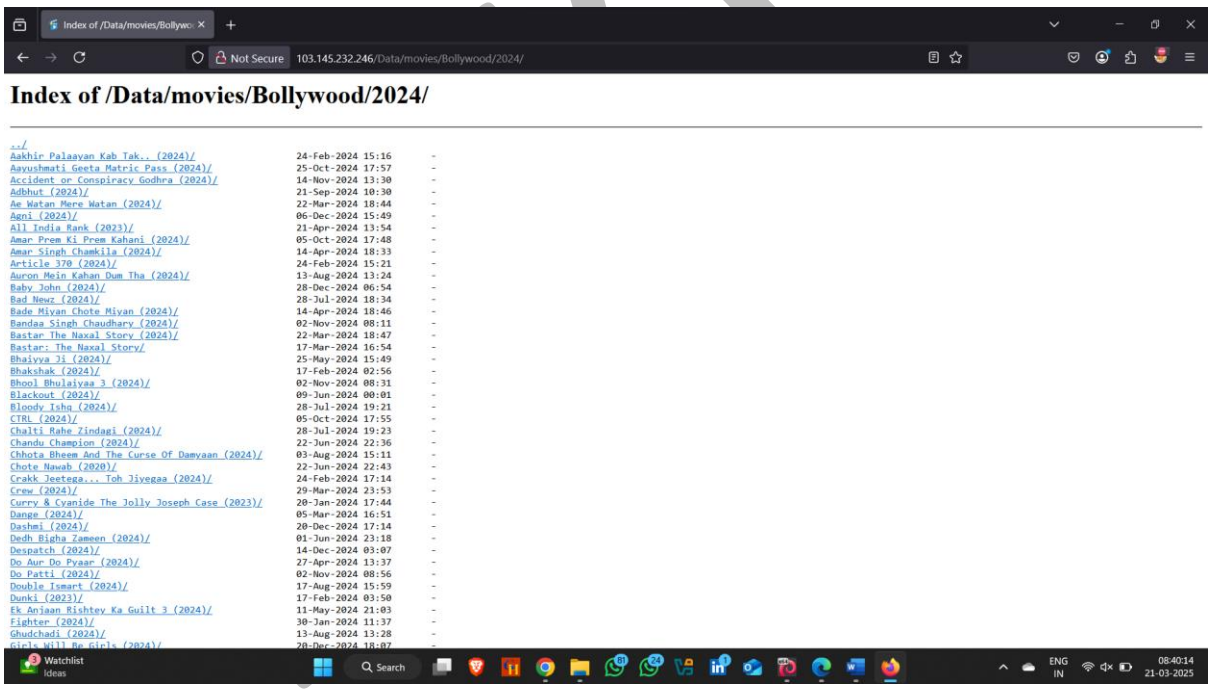
  The **inurl:** operator is a Google search tool that helps you find web pages containing specific **keywords in their URL**. This is especially useful for discovering targeted content like portals, login pages, or directories.
  The **site:** operator is a powerful Google search tool used to restrict search results to a specific website or domain.



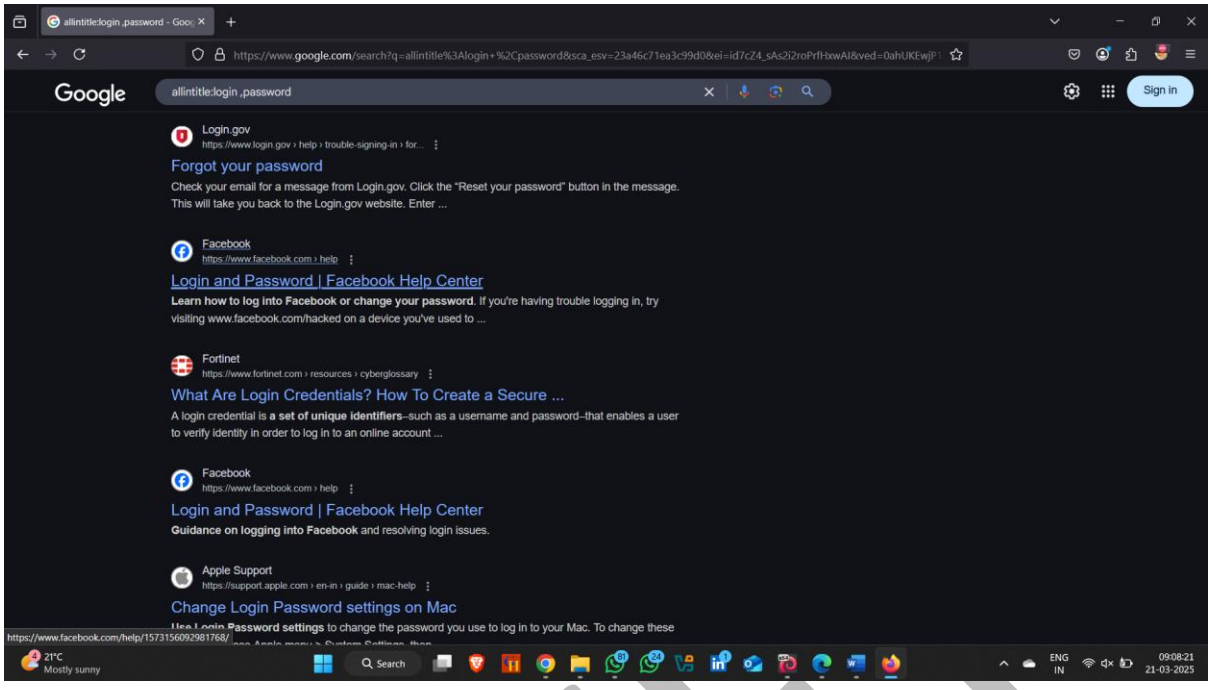
- The **intitle:** operator is a powerful Google search tool that helps you find web pages with specific **keywords in their title tags**.

Note-: you can also find other kind of stuffs like index of Hacking Books





- The **allintitle :** operator is a Google search tool that helps you find web pages where **all the specified keywords appear in the page title**. It's similar to intitle: but with stricter matching criteria.



You can also use the following operators to perform an advanced search to gather information about the target organization from publicly available sources.

- **anchor:** Finds pages that contain links with specific anchor text (the clickable text in hyperlinks).
  Syntax: anchor:<keyword>
  Example:
  🔍 anchor:download
  ➡️ Displays pages with links labeled "**Download**".

- **inanchor:** Finds pages linked with one specific keyword in the anchor text.
  Syntax: inanchor:<keyword>
  Example:
  🔍 inanchor:cybersecurity
  ➡️ Displays pages linked with "cybersecurity" as their anchor text.

- **related:** Finds websites with content similar to a given URL.
  Syntax: related:<URL>

Example:

🔍 related:eccouncil.org

➡️ Lists sites related to **EC-Council**, such as cybersecurity training platforms.

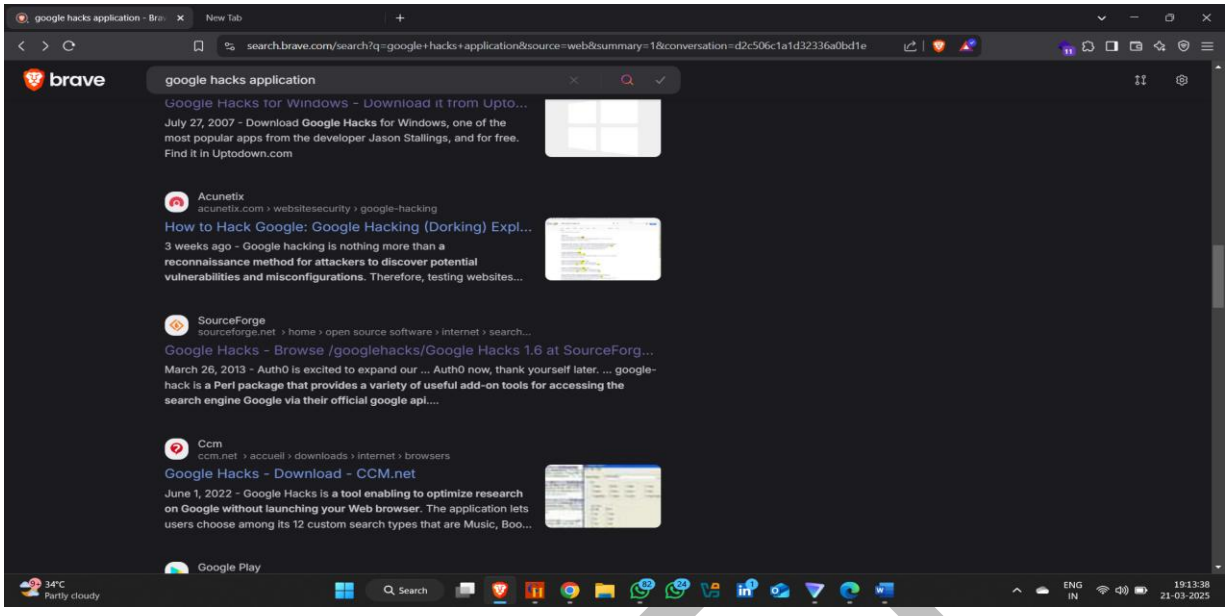
- **info:** Displays key information about a specific website, including its cache, backlinks, and similar pages.
  Syntax: info:<URL>
  Example:
  🔍 info:eccouncil.org
  ➡️ Provides insights into **EC-Council**, including its cached version, links to it, and similar sites.
- **location:** Targets search results based on a specific geographic location.
  Syntax: location:<city>
  Example:
  🔍 cybersecurity event location:Mumbai
  ➡️ Lists news articles or content relevant to Mumbai.

ANIKET

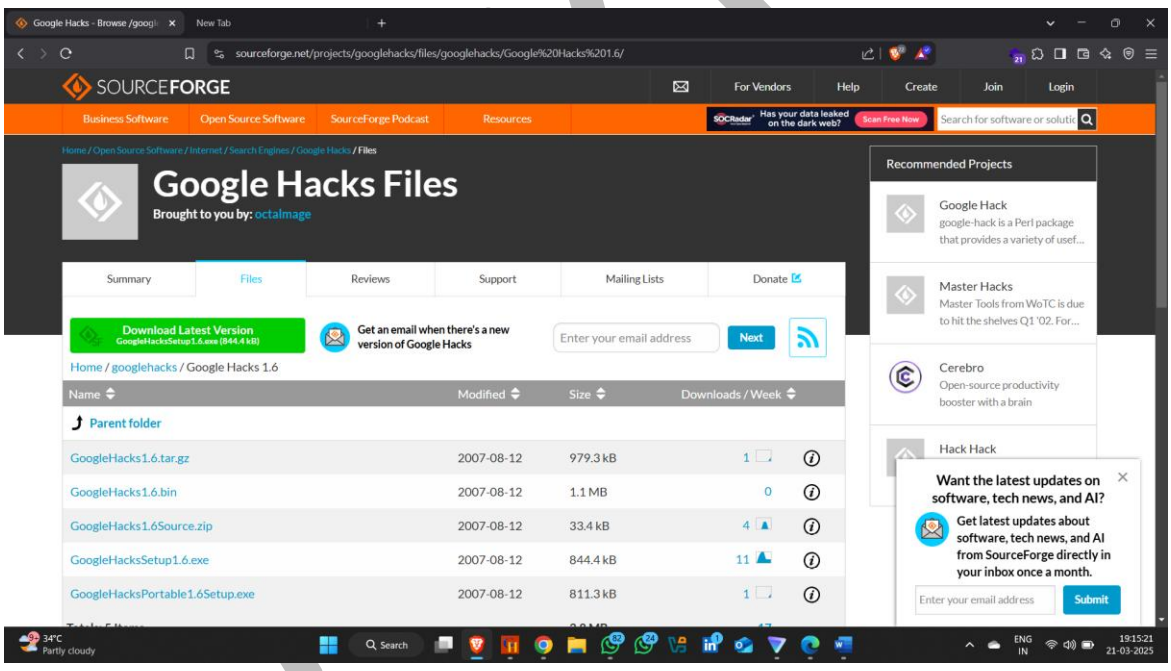
2. Gather Information Using Googlehacks application

Step 1 - : search Google hacks application

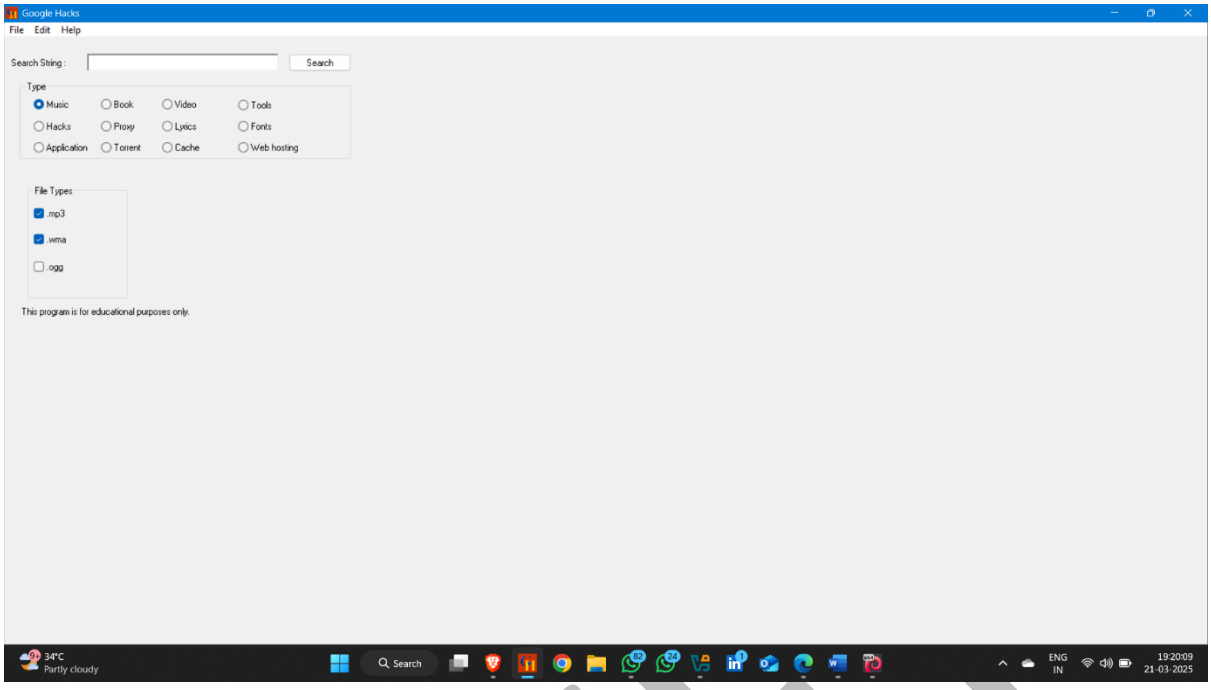
Step 2 -: open sourceforge Website



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



Step 4 -: After Download the application , install and open application

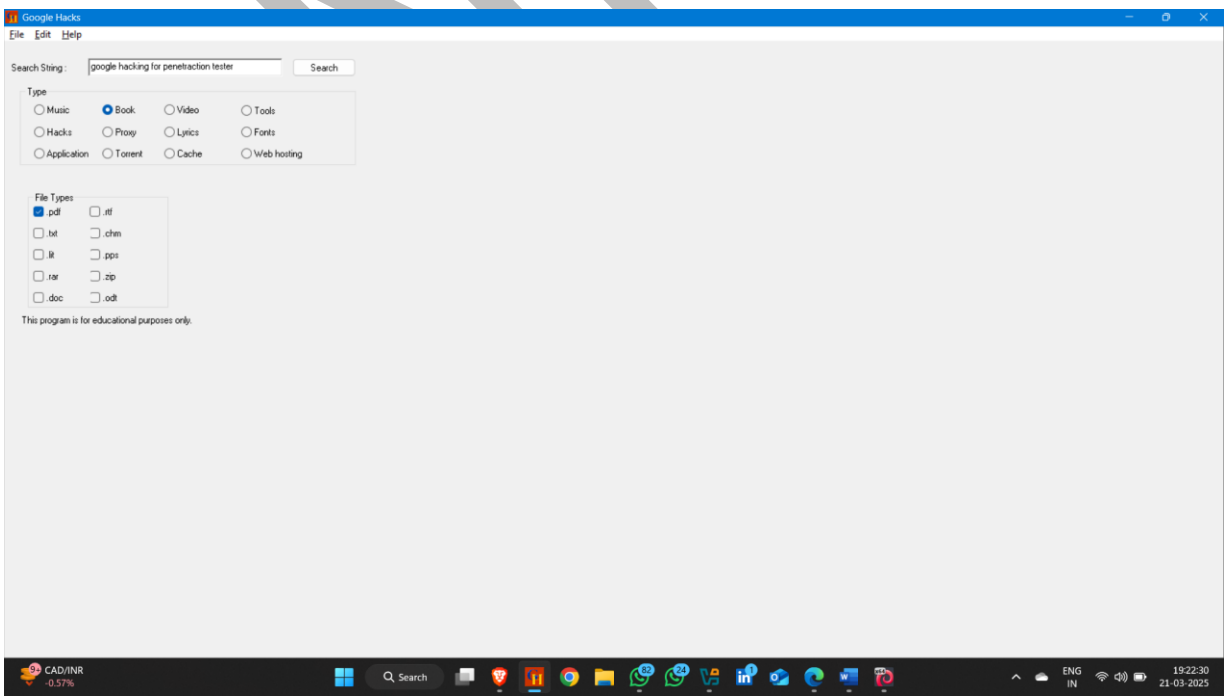


Now You can perform all the activity that you perform using web browser (like intitle , site and other switches)

For Example – Search a book

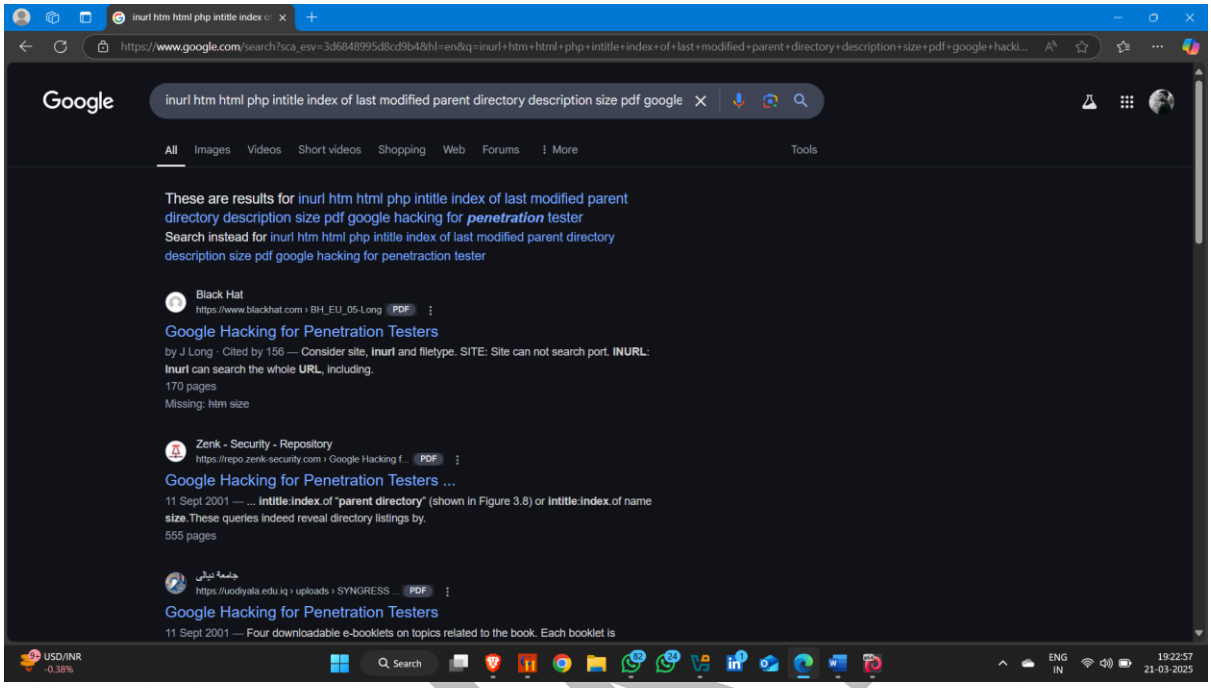
1) Click on radio button -book

2) Then select filetype option (pdf , txt, doc)



3) click on search button

Now you can see all result



2.EMAIL FOOTPRINTING

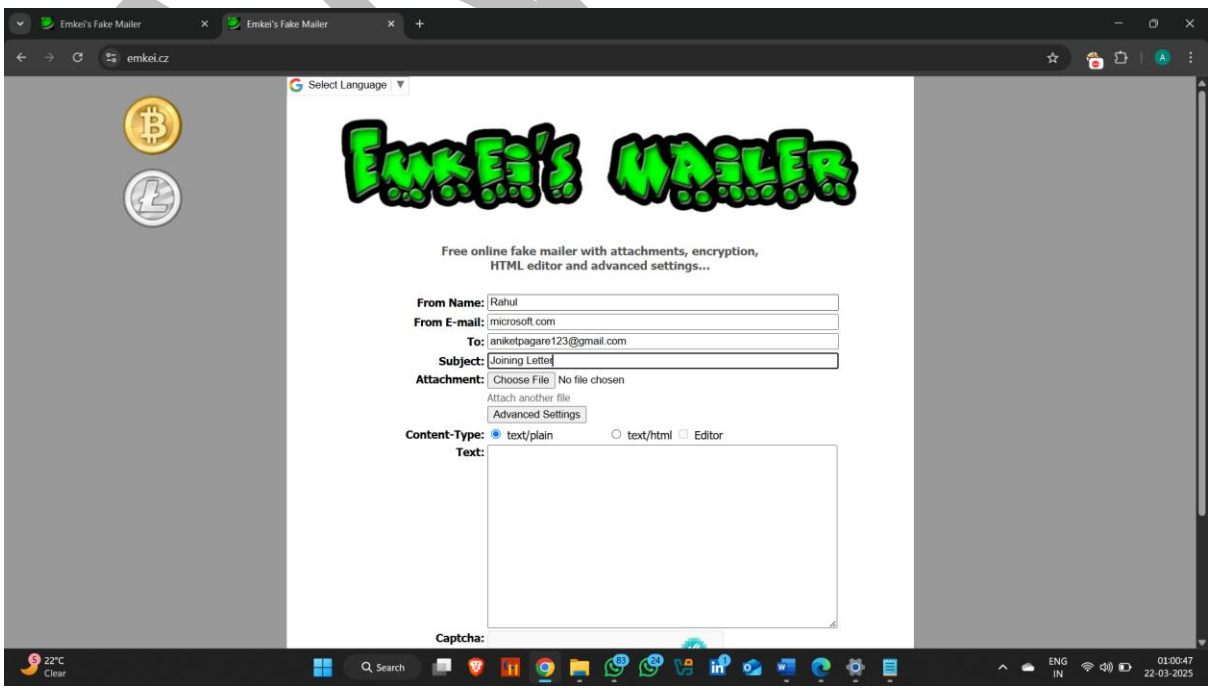
Email footprinting refers to the process of tracking and analyzing details about an email's origin, path, and related metadata to gather information about the sender or the infrastructure used to send the email.

Objectives-:

- identifying Mail Server
- Checking SPF & DKIM Records
- Harvesting Email Addresses
- Checking Breach Data
- Social Engineering
- Checking MX Records

1. Emkei Mailer

– Used for sending fake email



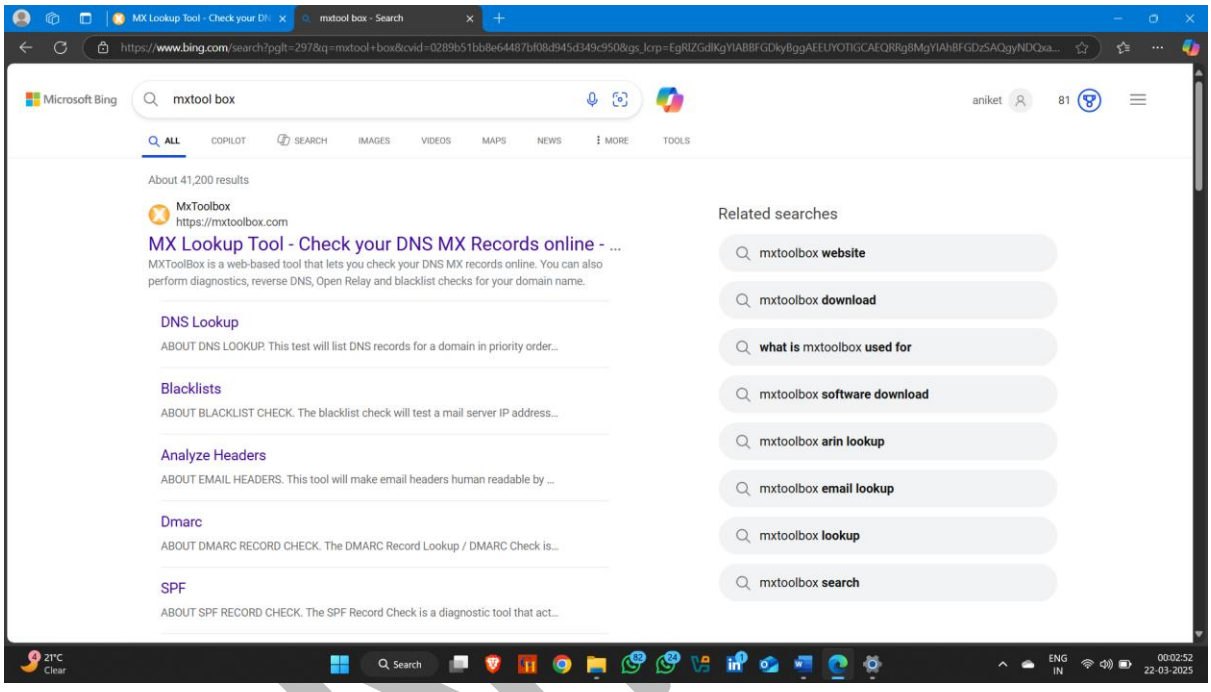
ANIKET

2.Email Footprinting using MX-TOOL BOX –

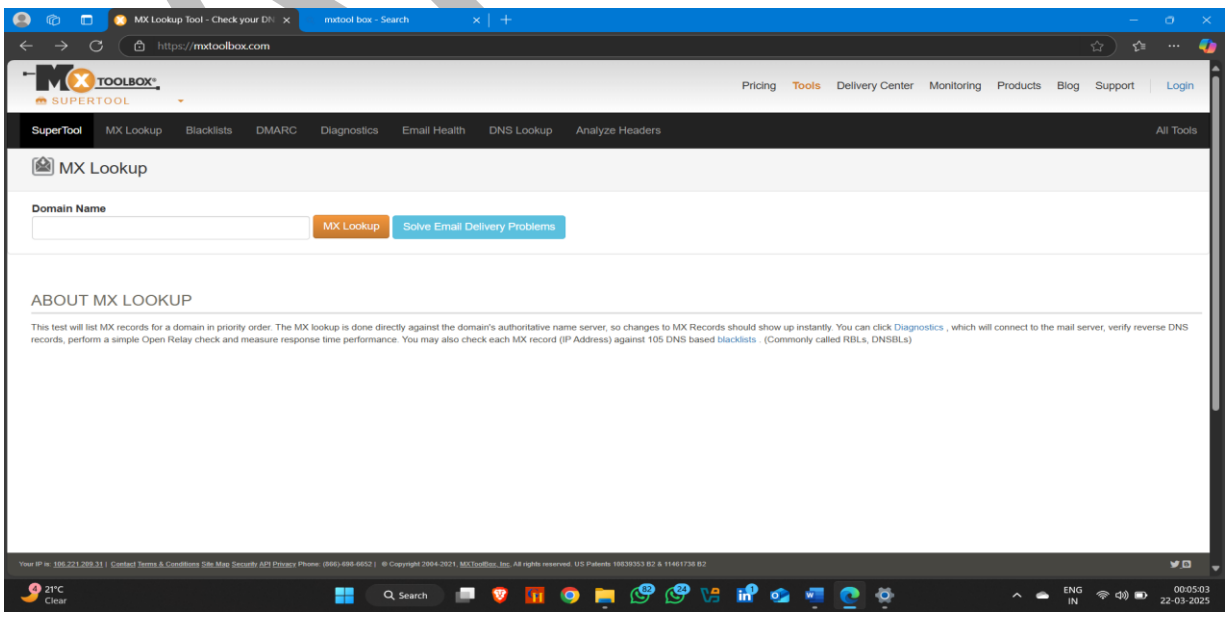
mxtool box are used to check received email are original or fake.

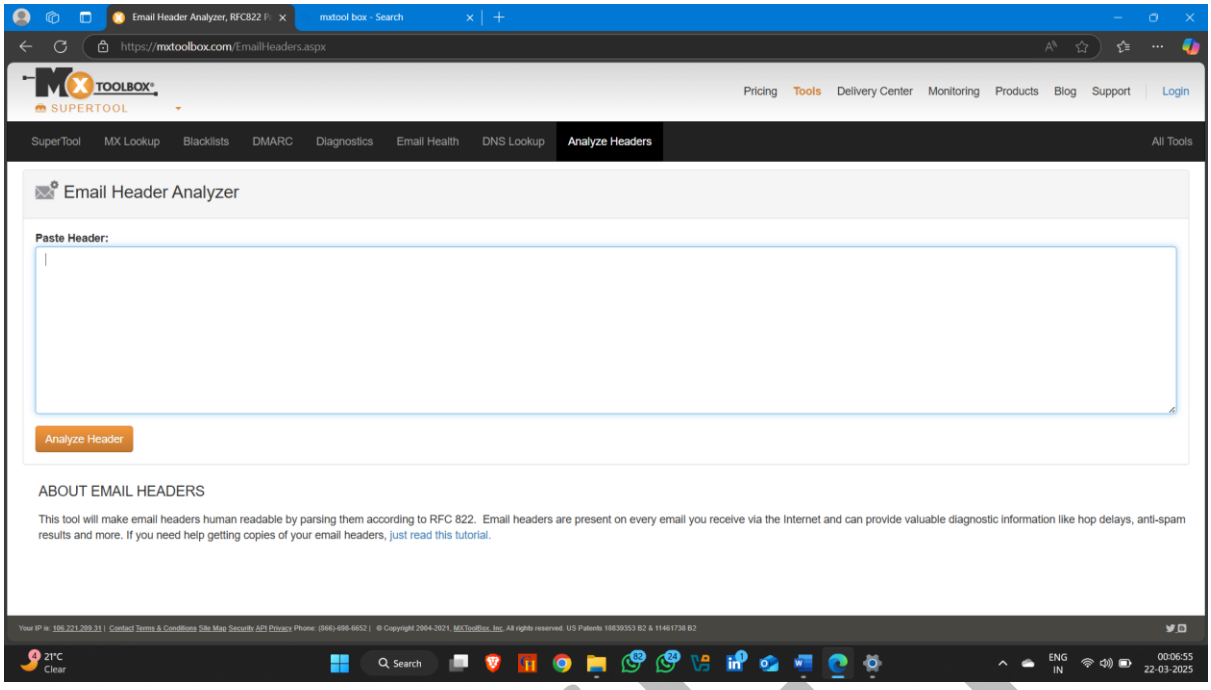
Step 1 –: Search mx tool box on browser.

Steps 2 -: Click on official mx tool box website.



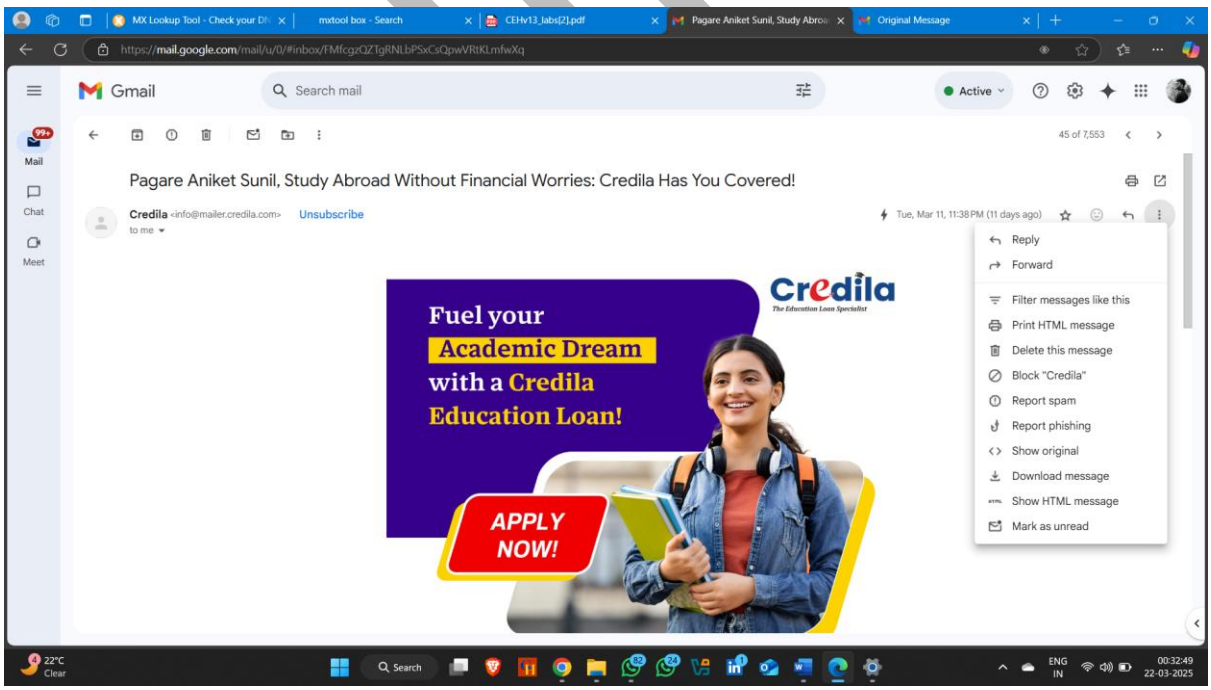
Step 3 -: Click on Analyze Headers .



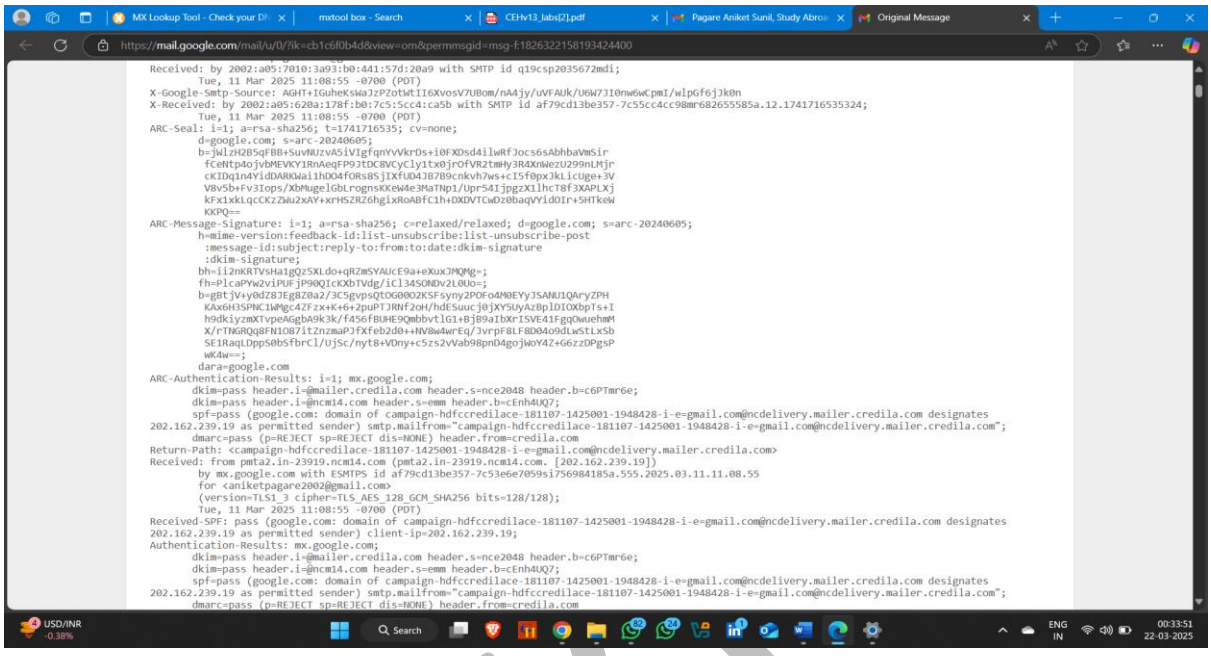


Now open email and click on those mail that you want to check its original or fake .

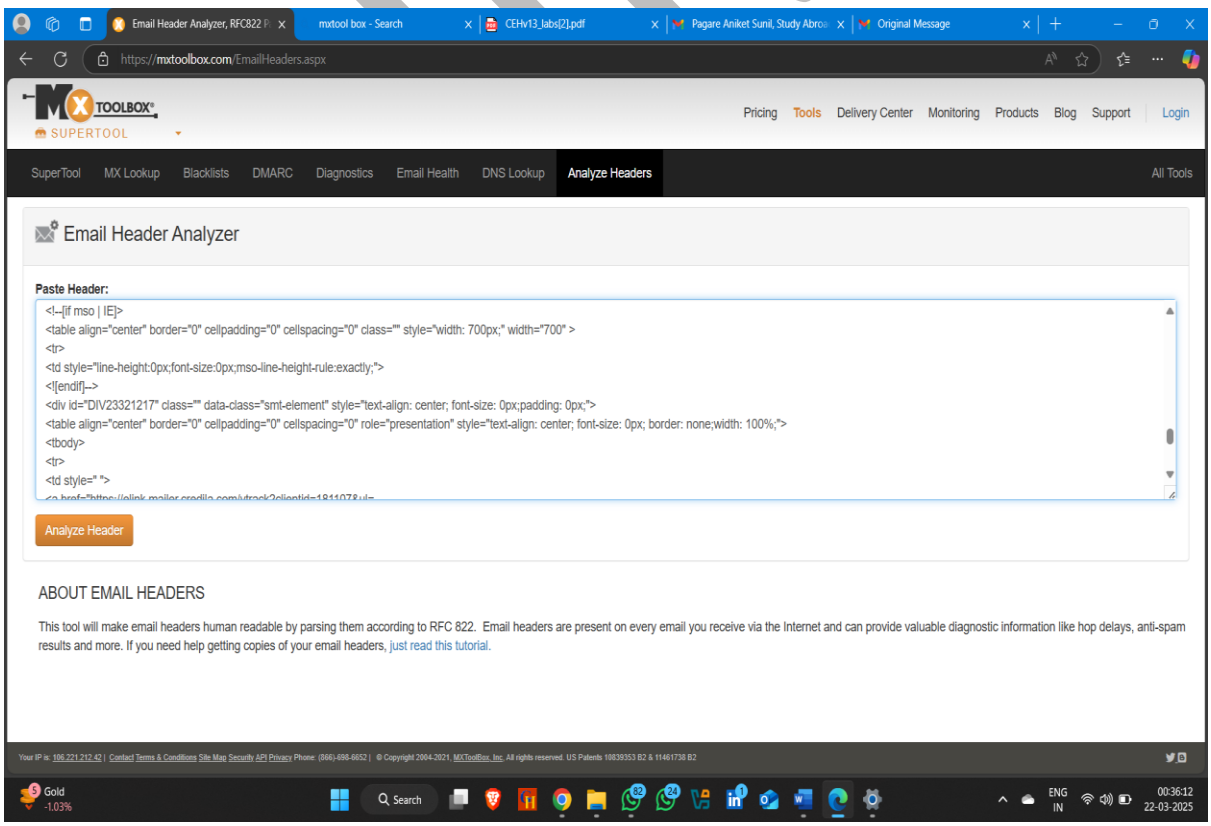
- Then click on **Three dot** on right site.
- Then click on **show original** option.



- Copy entire header



- And Paste on MX-TOOL BOX .
- Click on Analyze Header



Now you see that type result --

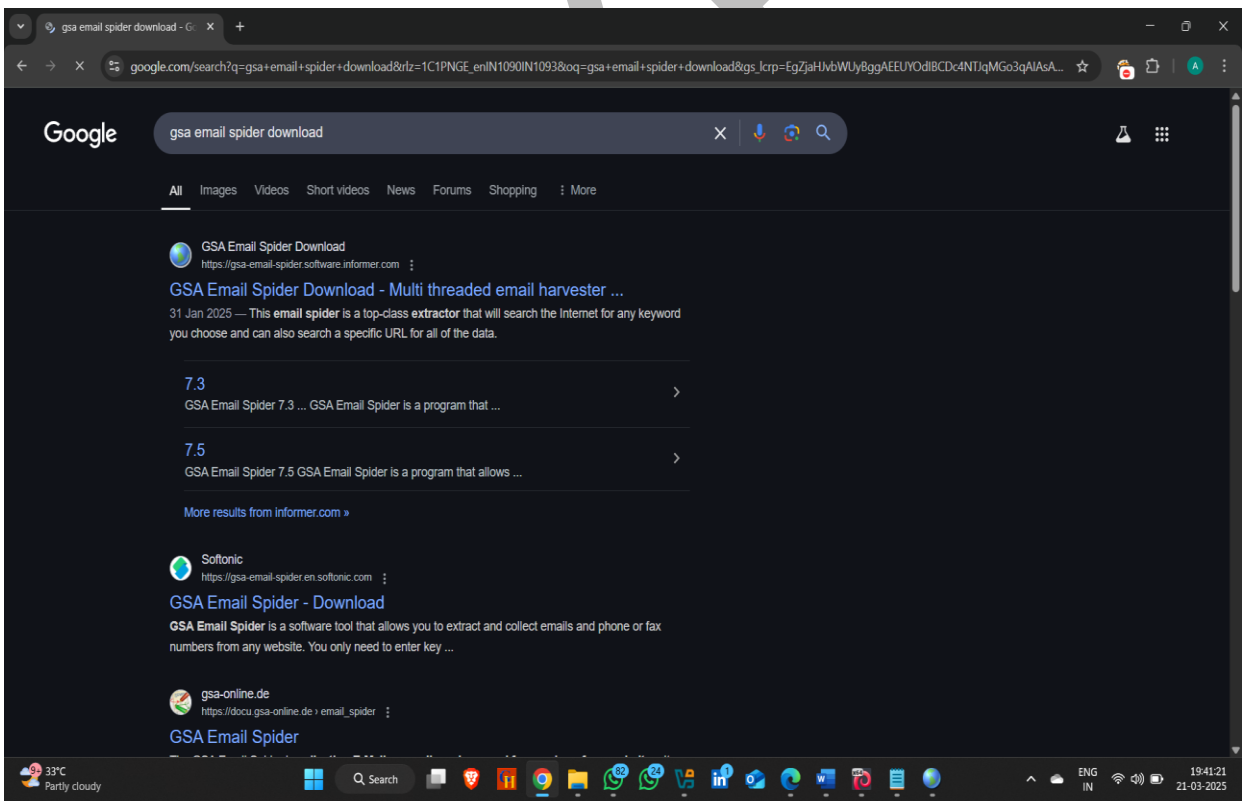
SPF	PASS with IP 202.162.239.19 Learn more
DKIM	'PASS' with domain mailer.credila.com Learn more
DMARC	'PASS' Learn more

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

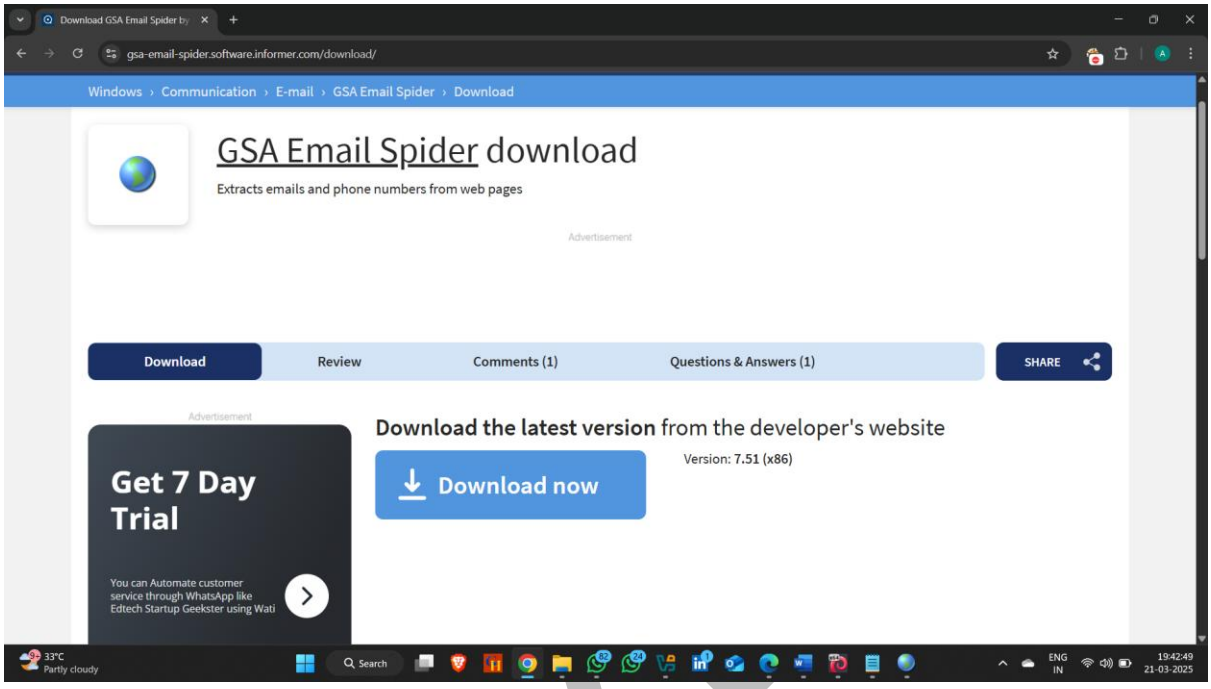
3.Email Footprinting Using GSA Email Spider Application -:

Installation Process -:

Step 1 -: Search GSA Email Spider On Browser



Step 2 -: click on first Website



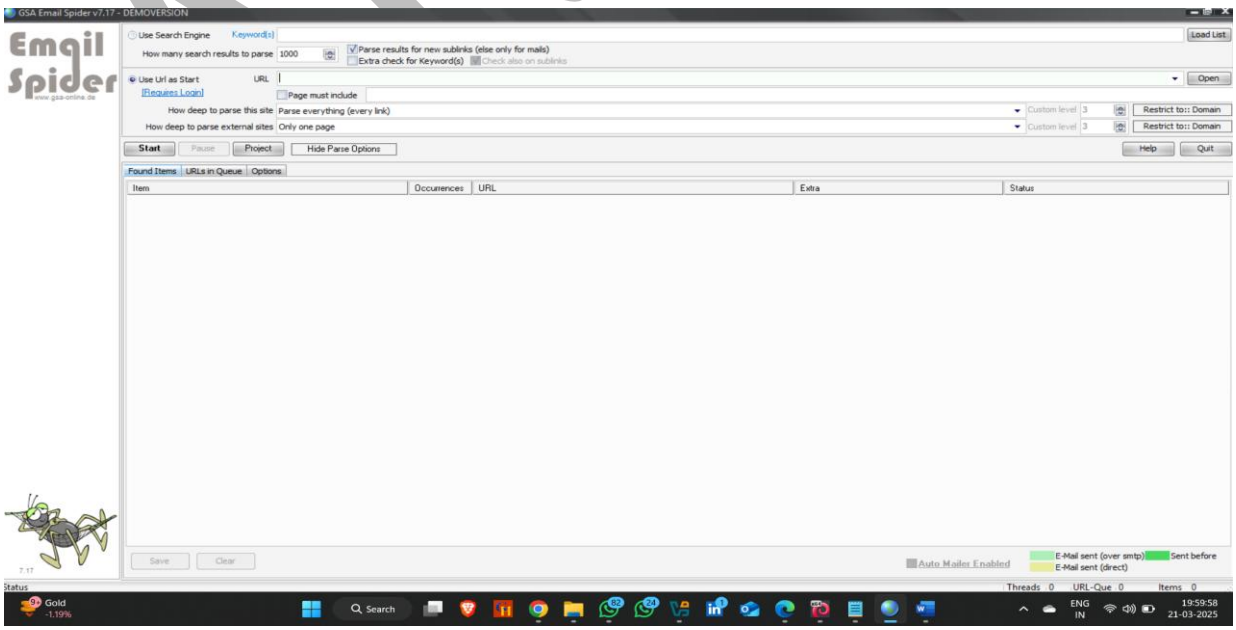
Step 3 -: click on Download and Download it .

After completing installation process then setup the app

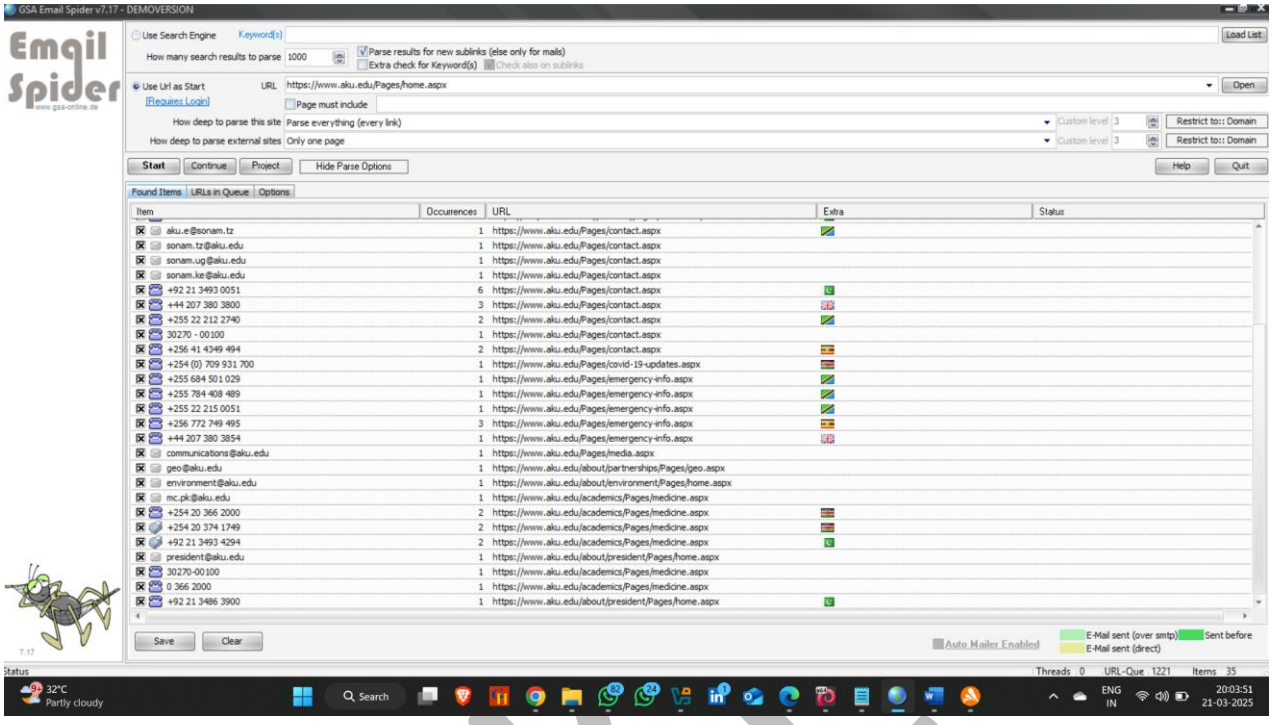
Step 4 -: Copy url that you want to perform email footprinting

Step 5 -: Paste URL in **url section**.

Step 6 -: Click on **Start** button.



Step 7 -: Then you see the result



ANIKET

3. DNS FOOTPRINTING

DNS Footprinting obtained gather information about DNS servers , DNS records and types of servers used by the organization .DNS zone data include DNS domain names ,computer names , IP addresses , domain mail servers , service records and much more about target network.

Objectives-:

1.Identifying domain information (WHOIS lookup).

2. Finding subdomains.

3. Extracting DNS records (A, MX, NS, TXT, etc.).

4. Discovering IP addresses of target servers.

5. Performing reverse DNS lookups.

6. Exploiting DNS zone transfers (if misconfigured)

- Types of DNS Records -: DNS Records provides important information about location and type of server.

Types of DNS Records

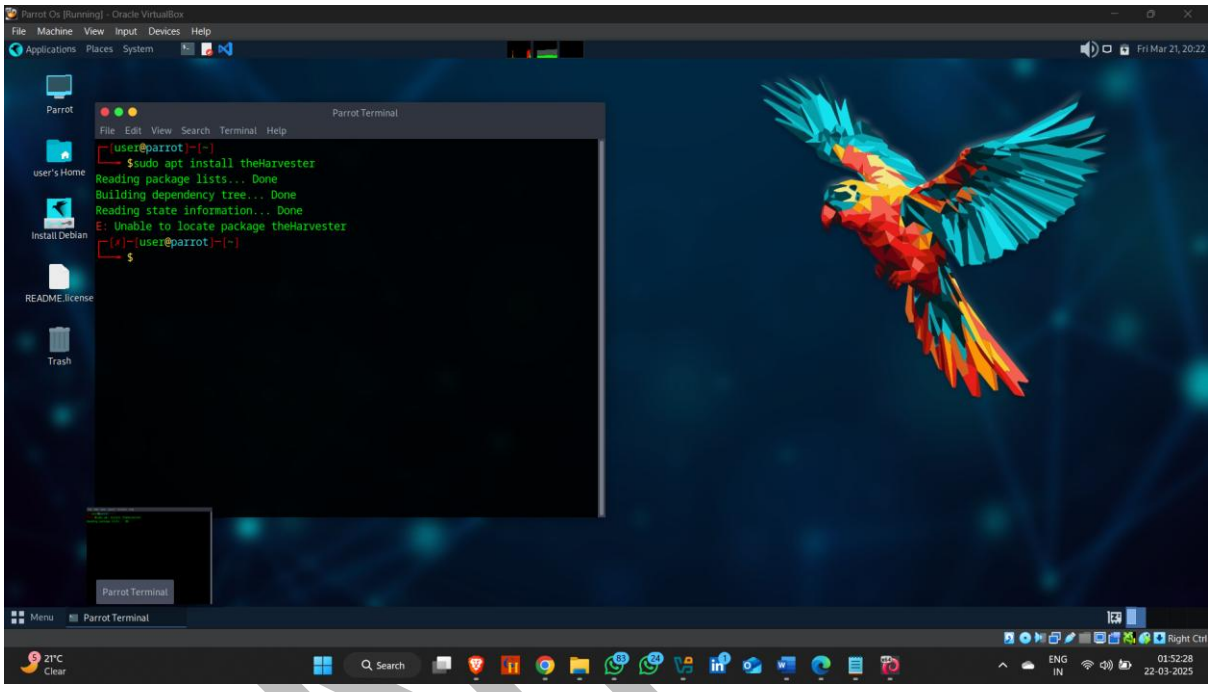
Type	Description	Function
A	Address record	Link the domain or subdomain to IPv4 address
NS	Name server record	Delegates a DNS zone to use the given authoritative name servers
MX	mail exchange record	Directs email to servers for a domain with the order of priority
CNAME	Canonical name records	Aliases for A records
TXT	Text record	Uses for SPF, Domain Key etc
SOA	Start of [a zone of] authority record	Specifies authoritative information about a DNS zone

NIKET

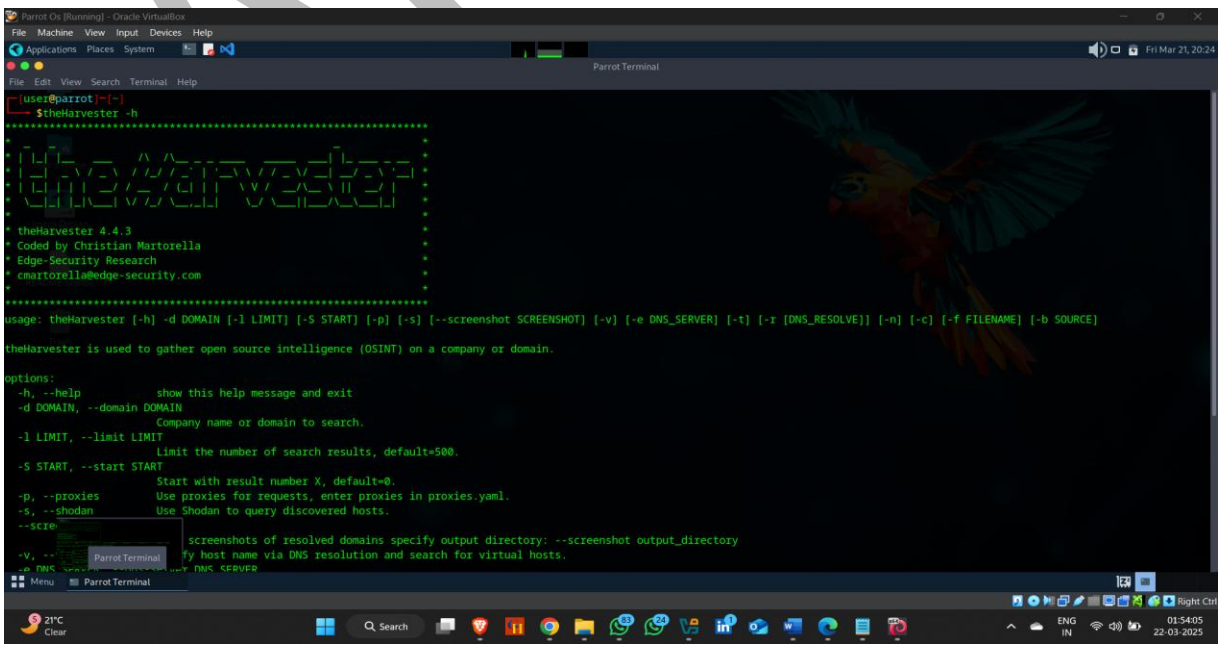
1. DNS Footprinting Using TheHarvester (CLI Tool)

TheHarvester install process –

1. Open Parrot Os
2. Type sudo apt install theHarvester.

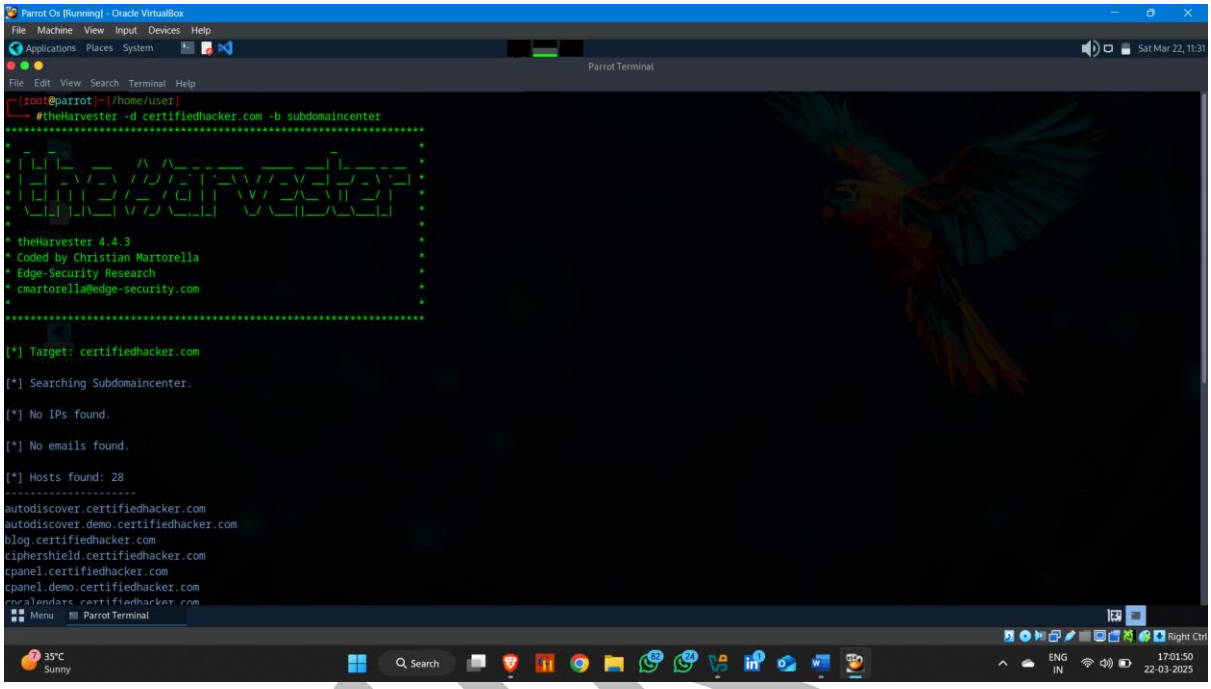


3. Search theHarvester -h (-h = help)



Commands –

- theHarvester -d certifiedhacker.com -b subdomaincenter
  - -d -- domain
  - -b – source



2. DNS Footprinting Using Dig (CLI).

dig (Domain Information Groper) is a powerful command-line tool in Kali Linux (and other Linux distributions) used for querying DNS (Domain Name System) servers.

A record: dig example.com A.

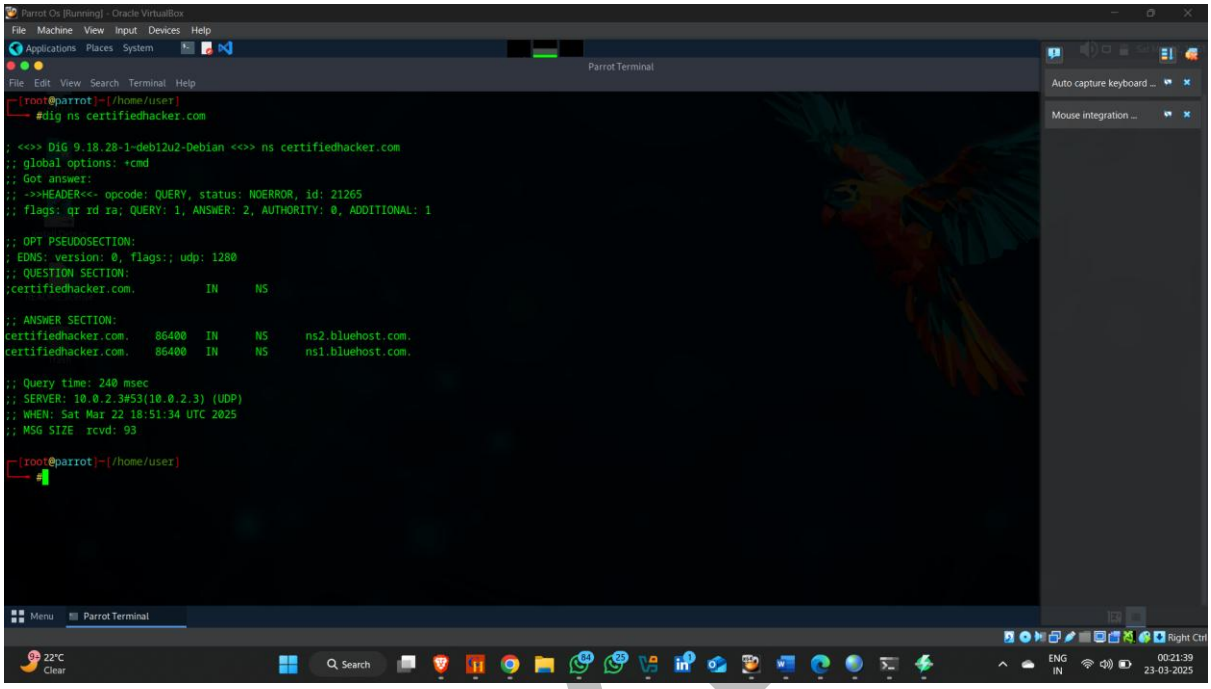
MX record: dig example.com MX.

NS record: dig example.com NS.

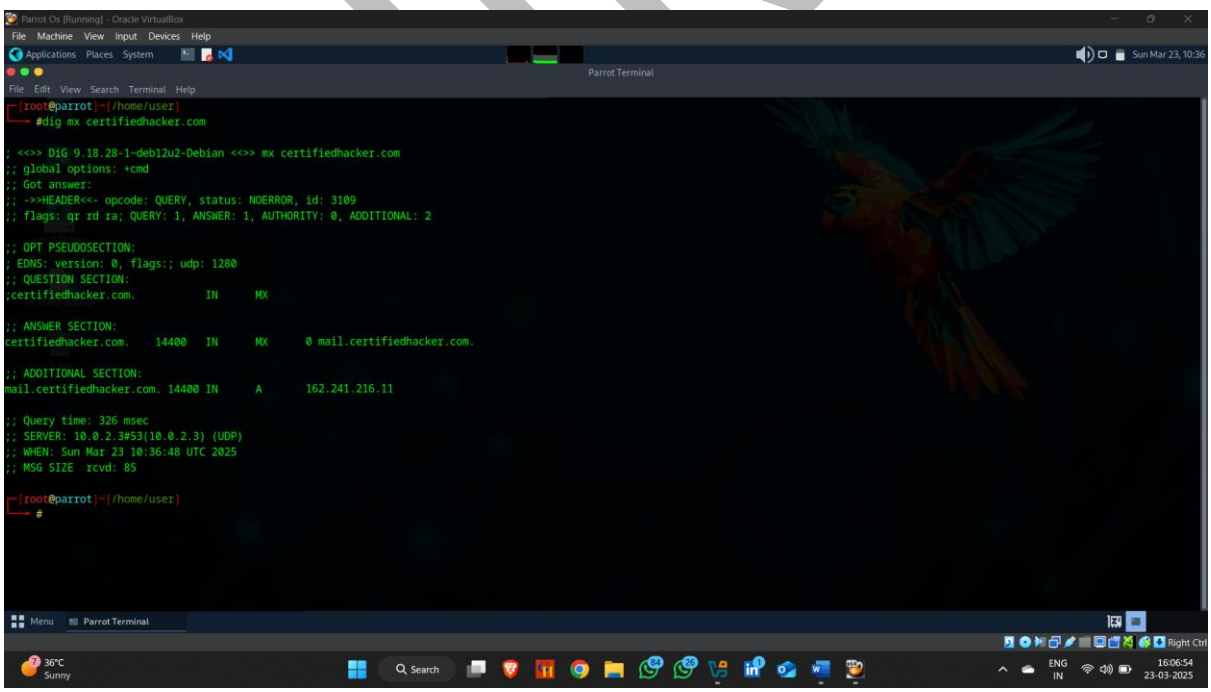
TXT record: dig example.com TXT.

The AXFR (Asynchronous Full Transfer Zone) query type is used to attempt a zone transfer.

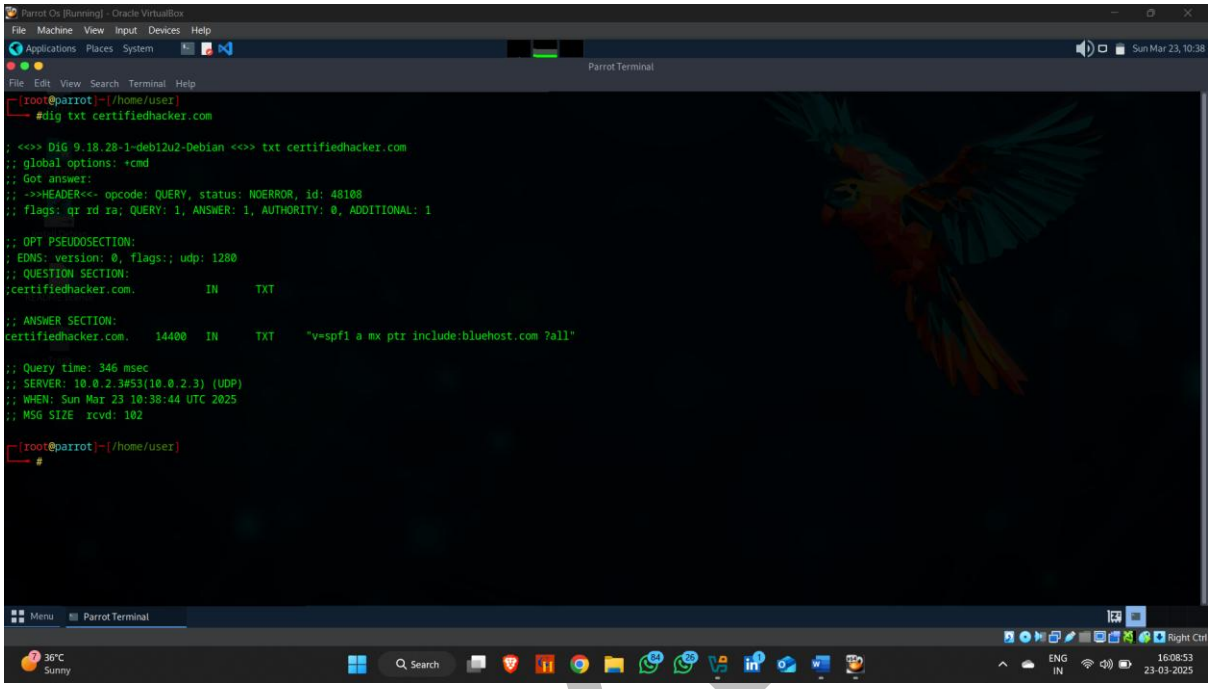
- Using ns record



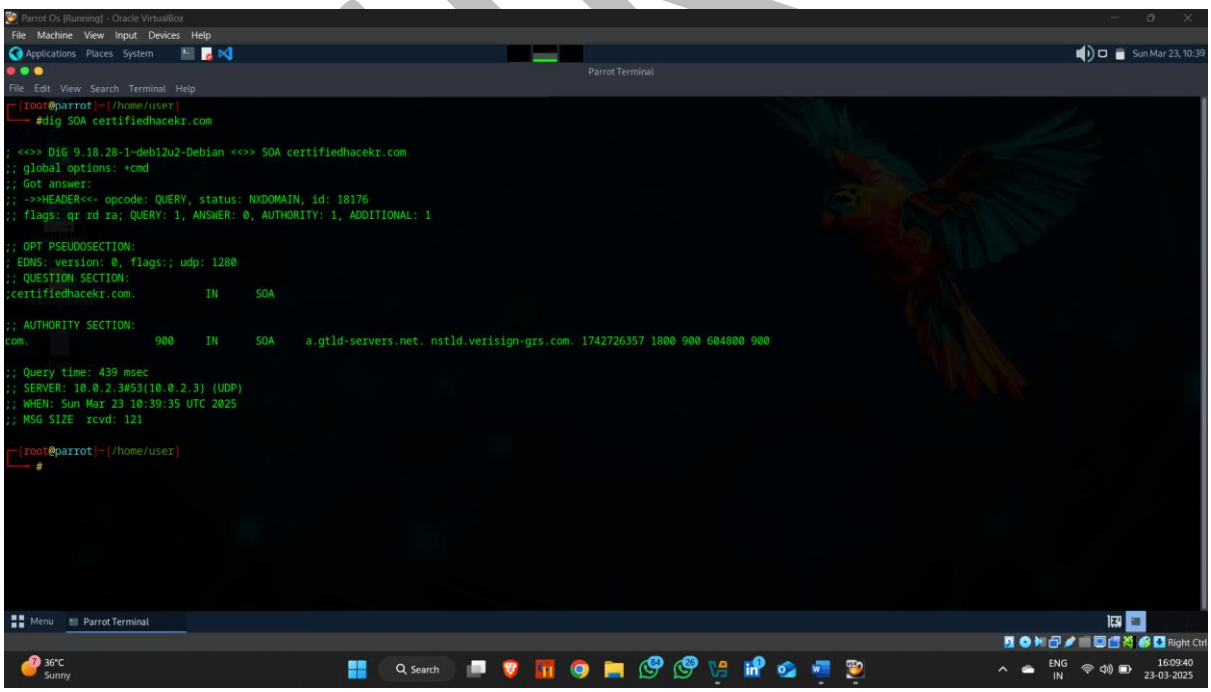
- Using mx records



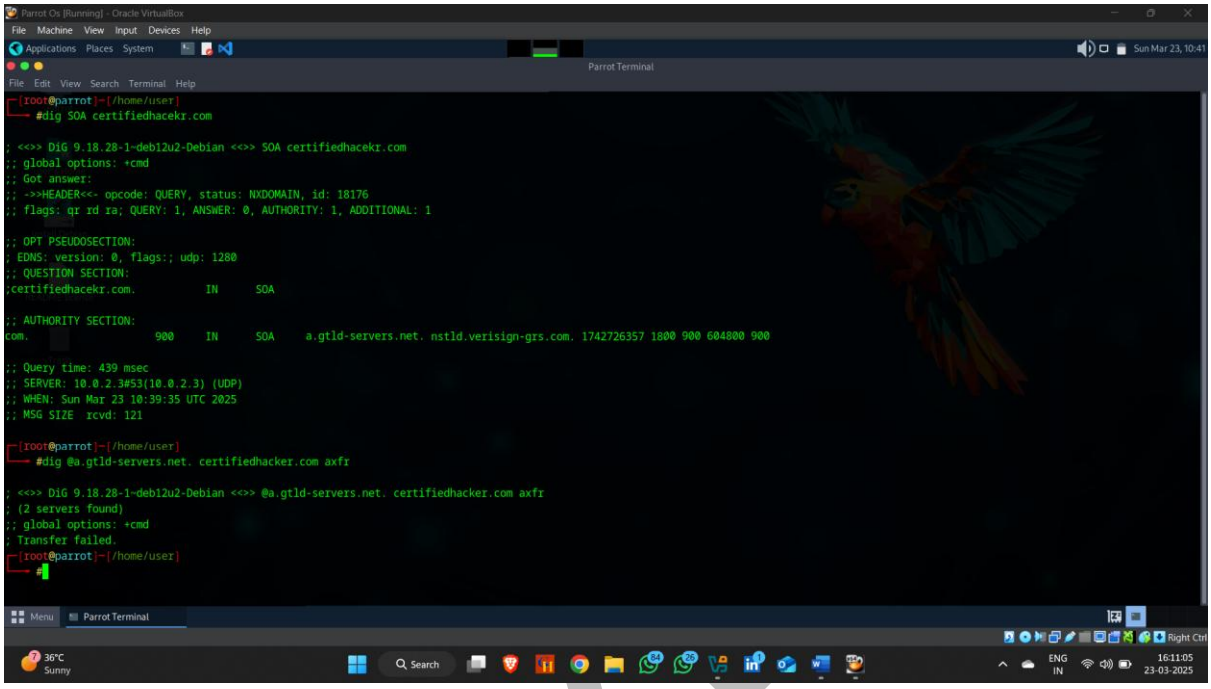
- Using txt records



- Using SOA records



- Using AXFR zone transfer

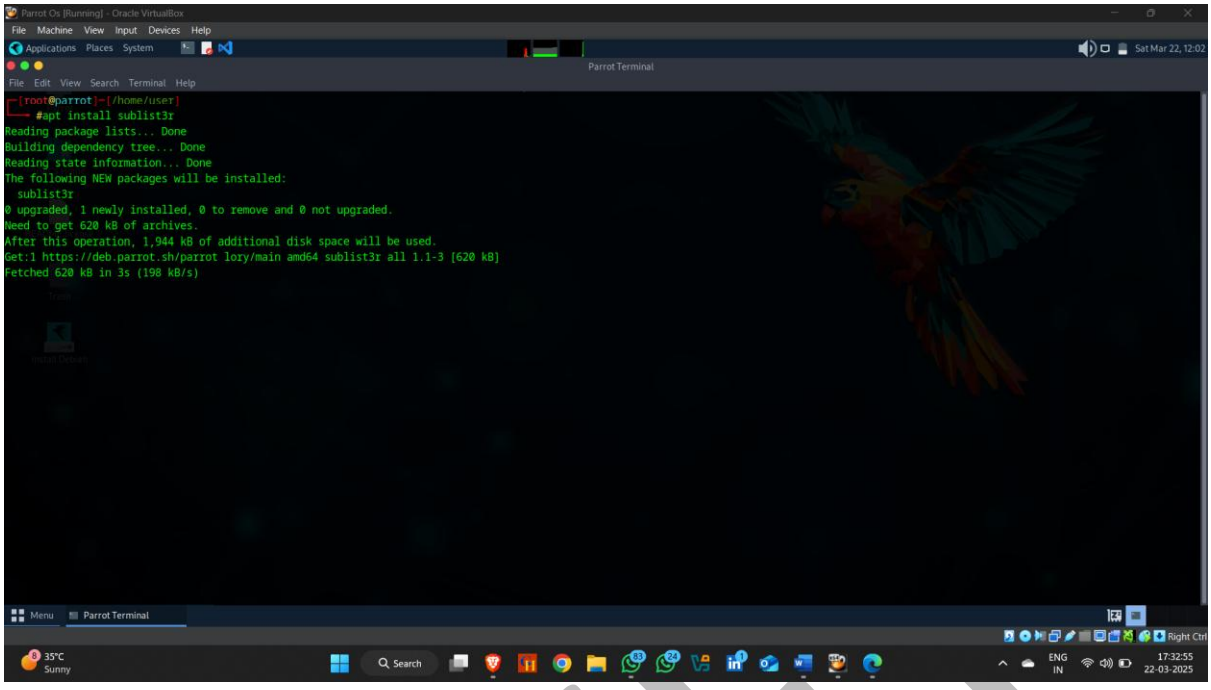


2. DNS Footprinting Using Sublist3r (CLI)

Sublist3r automates the process of gathering subdomains by querying multiple search engines and data sources.

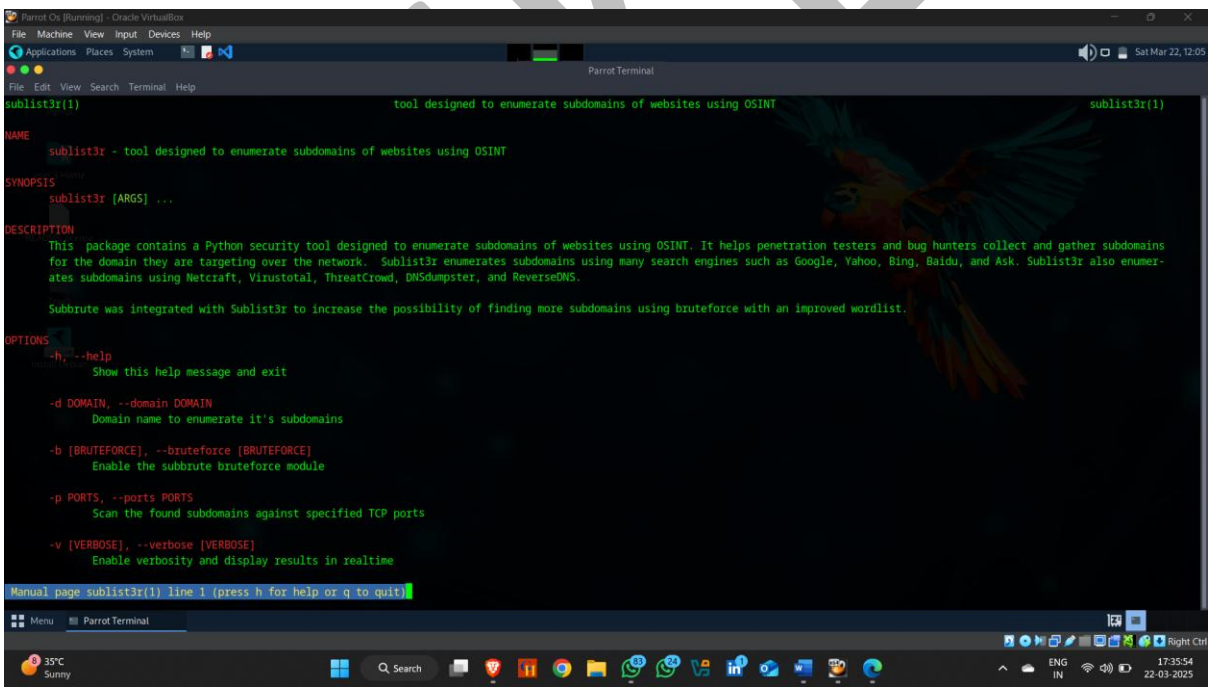
Sublist3r Installation Process-

- Open Kali Linux/Parrot OS terminal
- Type **‘apt install sublist3r’**

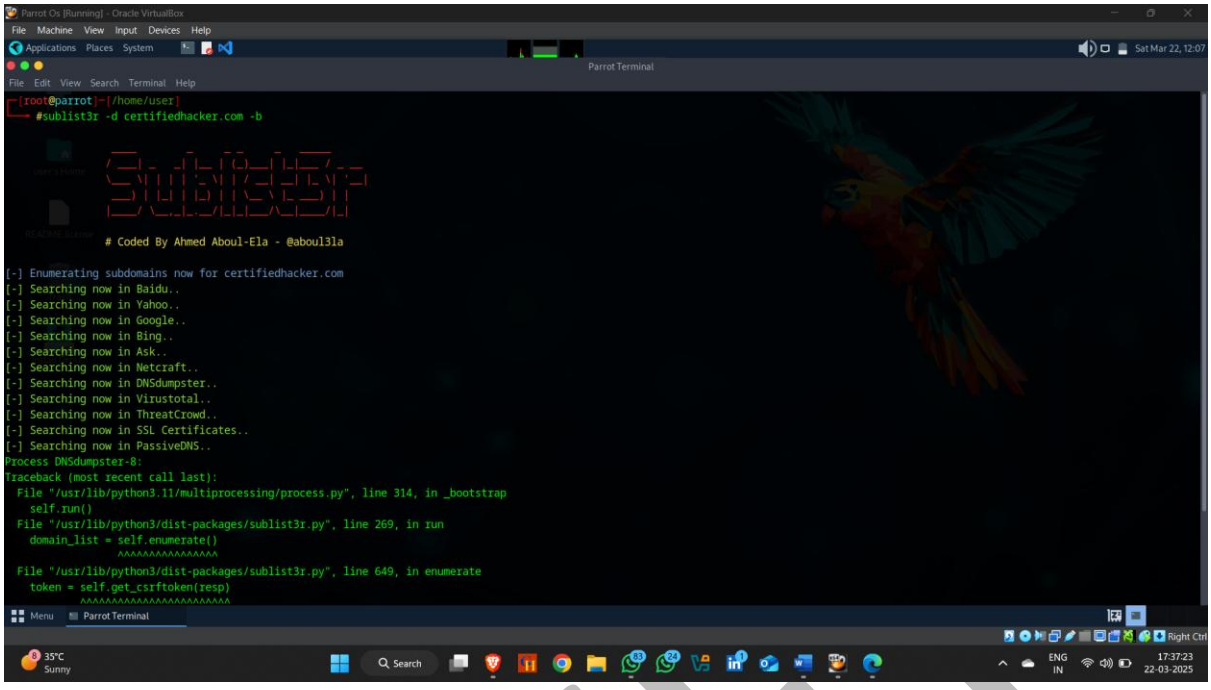


Commands for sublist3r - -

- man sublist3r - - to show all description about sublist3r



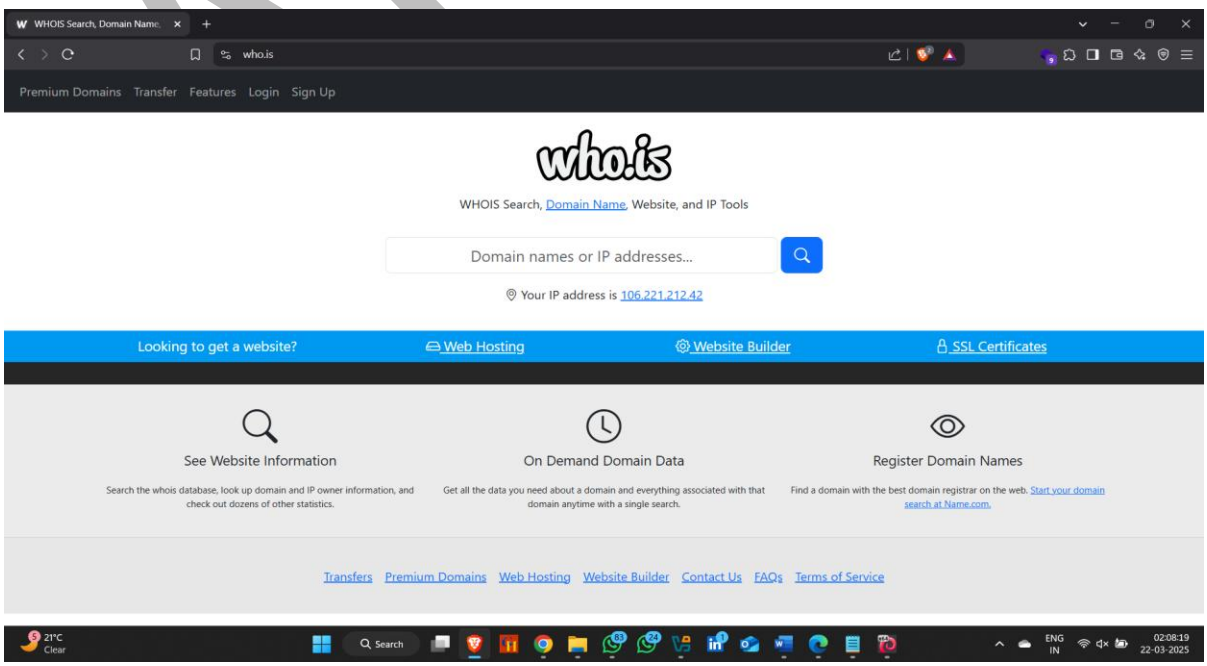
- sublist3r -d <domain name > -b
  - -d - - domain
  - -b - - bruteforce



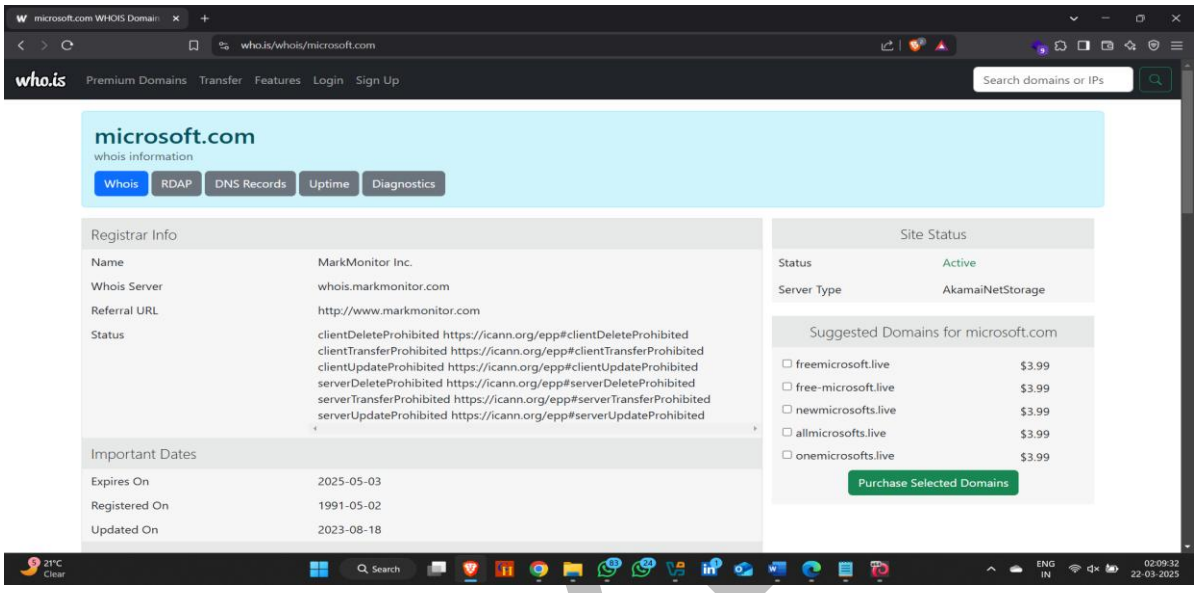
4.DNS Footprinting using WHOIS (GUI) –

How to do it -

- Open Browser.
- Search WHOIS



- Search Domain name or ip address.
- Search .

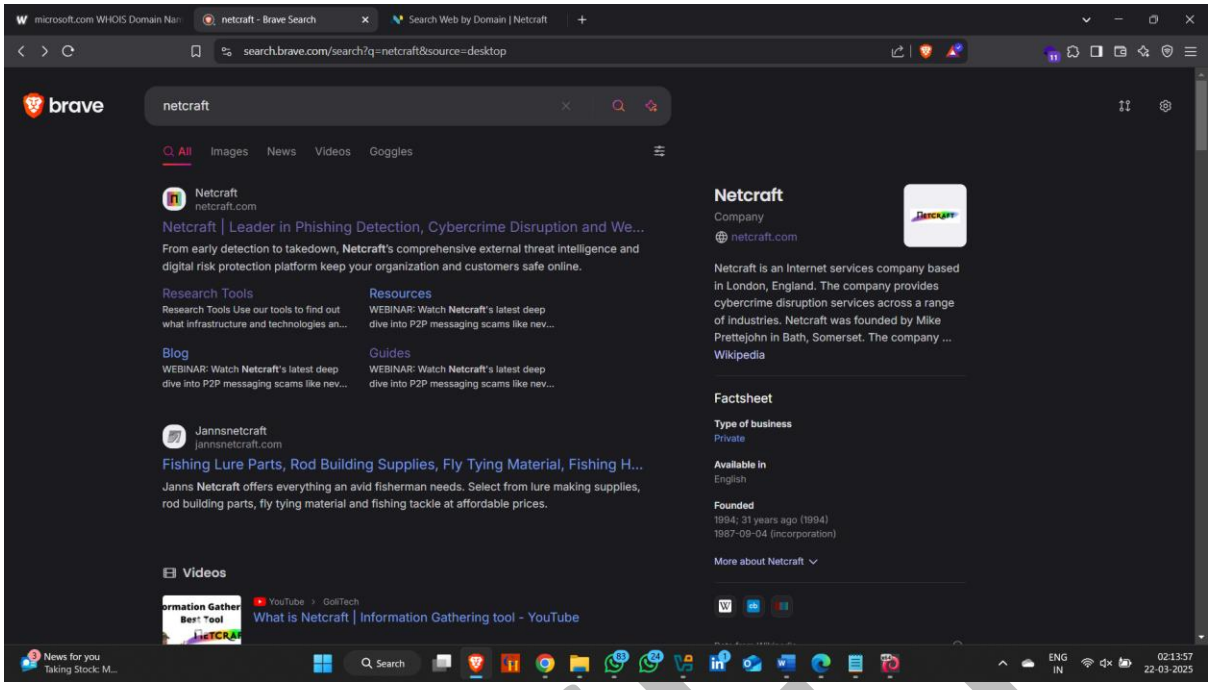


4. DNS Footprinting Using NetCraft (GUI) –

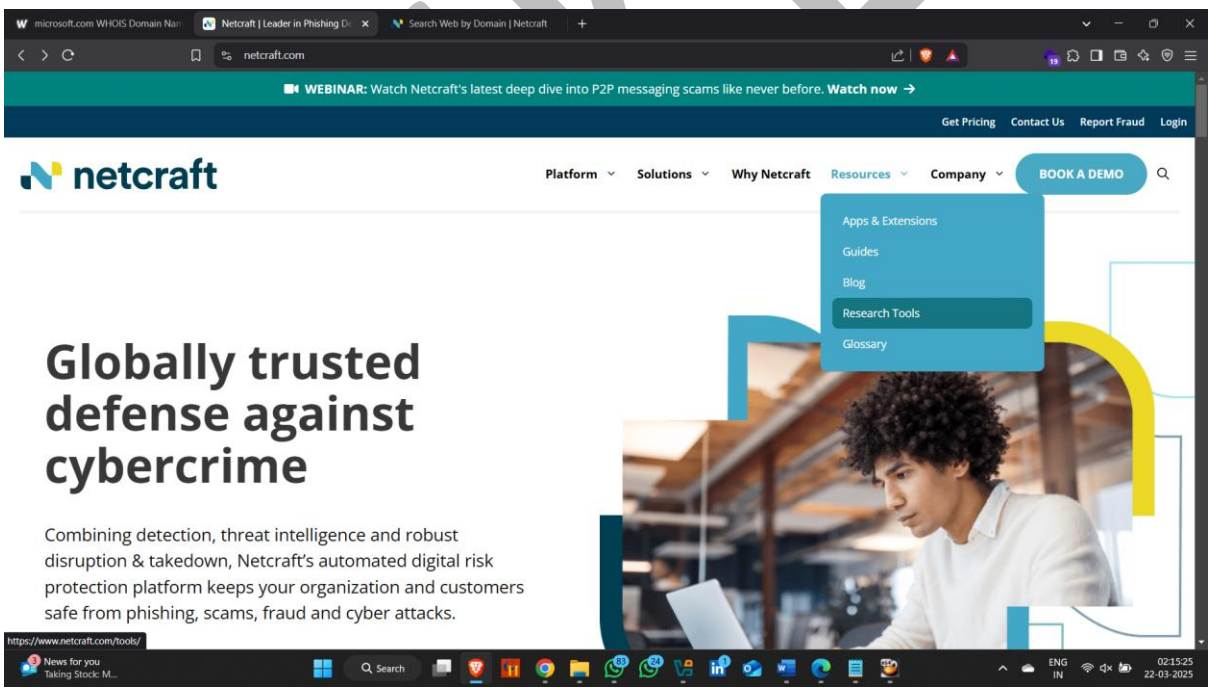
How to do it

- Open Browser .
- Search Netcraft
- Open official netcraft website.

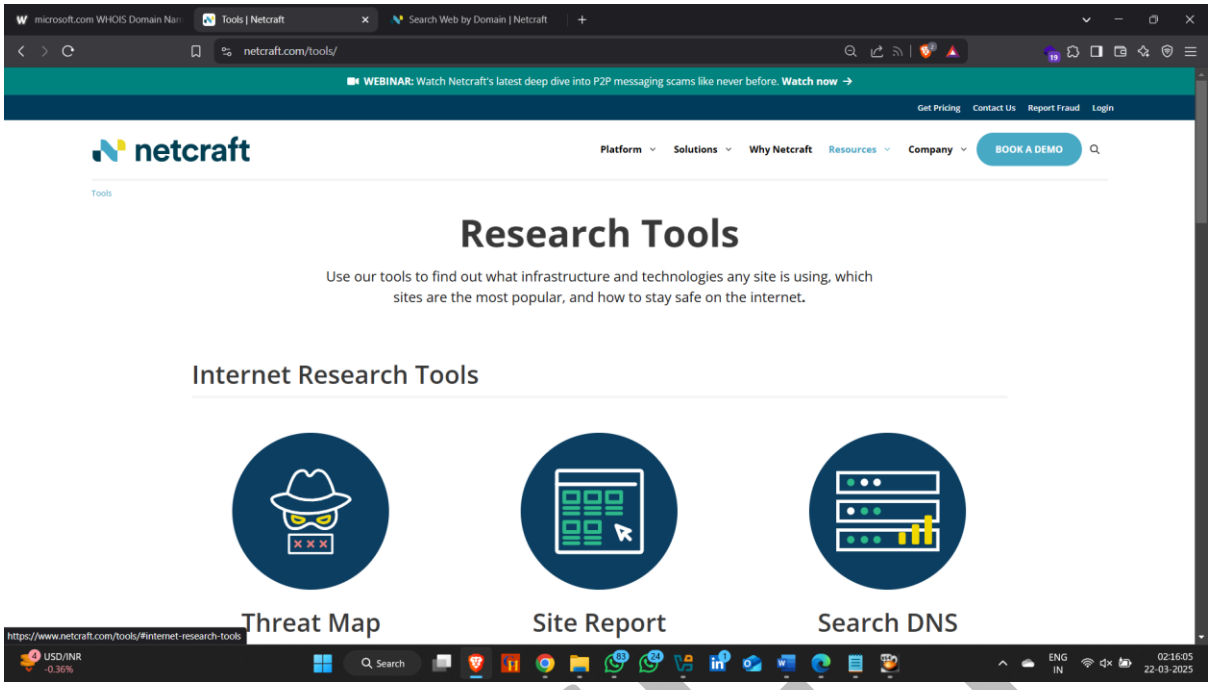
ANIKET



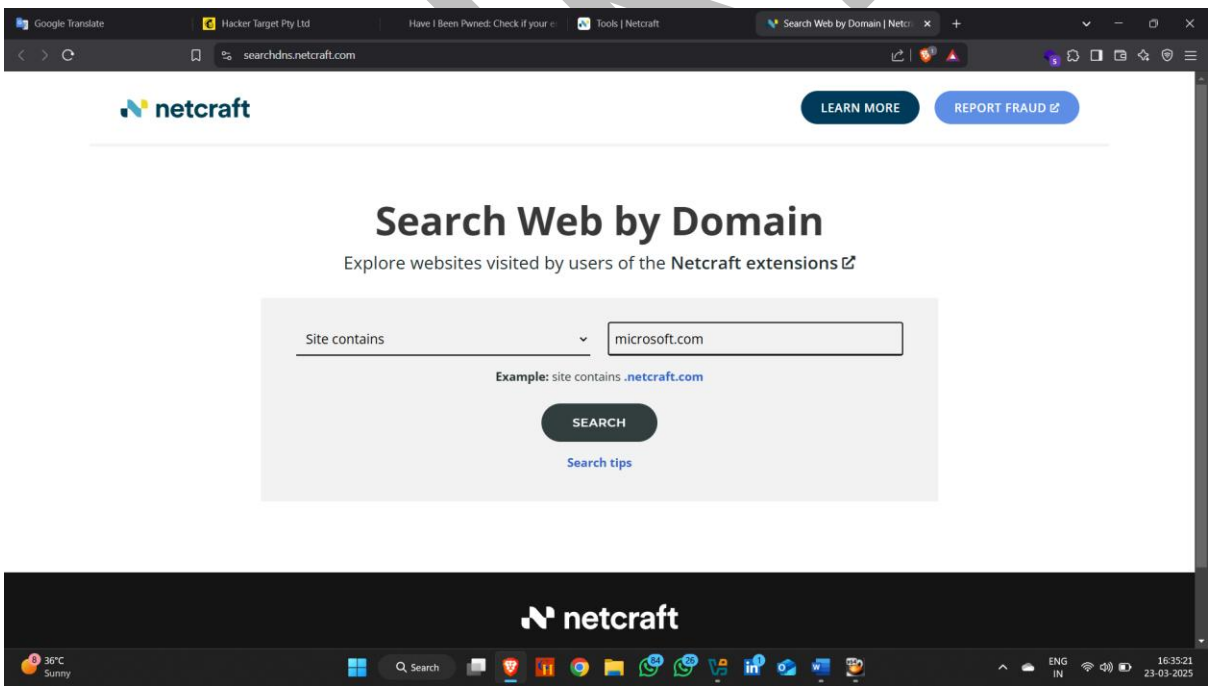
- Click on Resources and click on research tools.

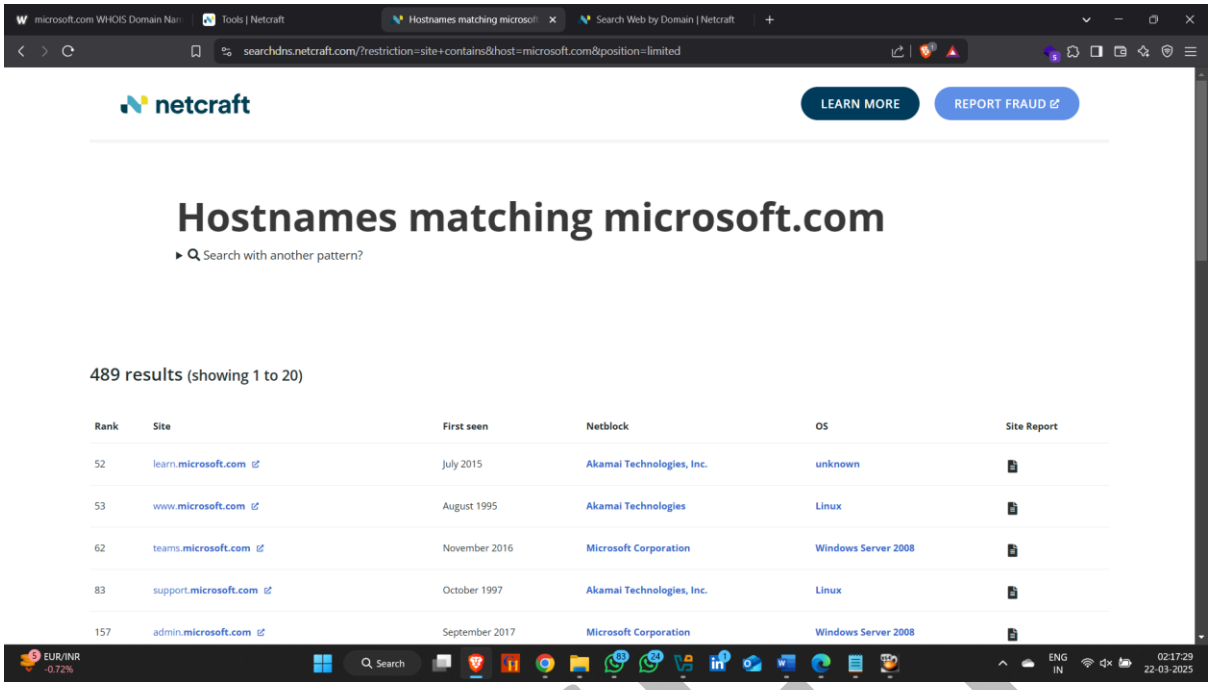


- Click on Search DNS



- Provide Domain name.
- Click on search .



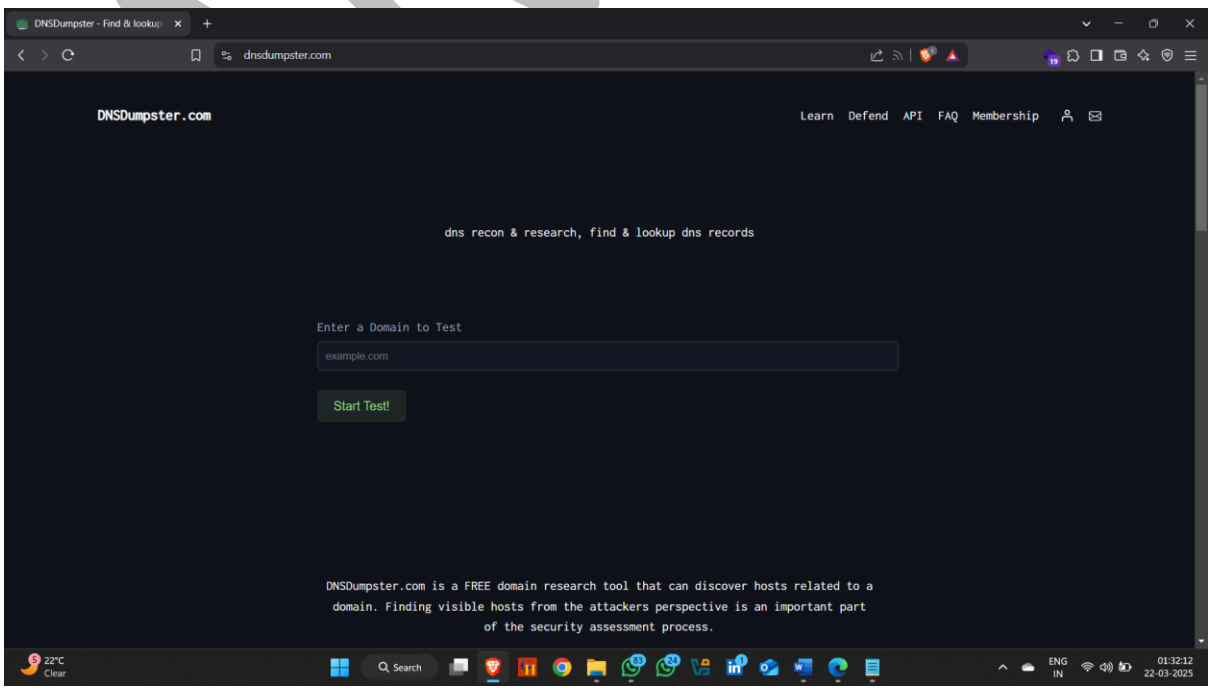


5. DNS Footprinting Using DNS Dumster -

How to do it

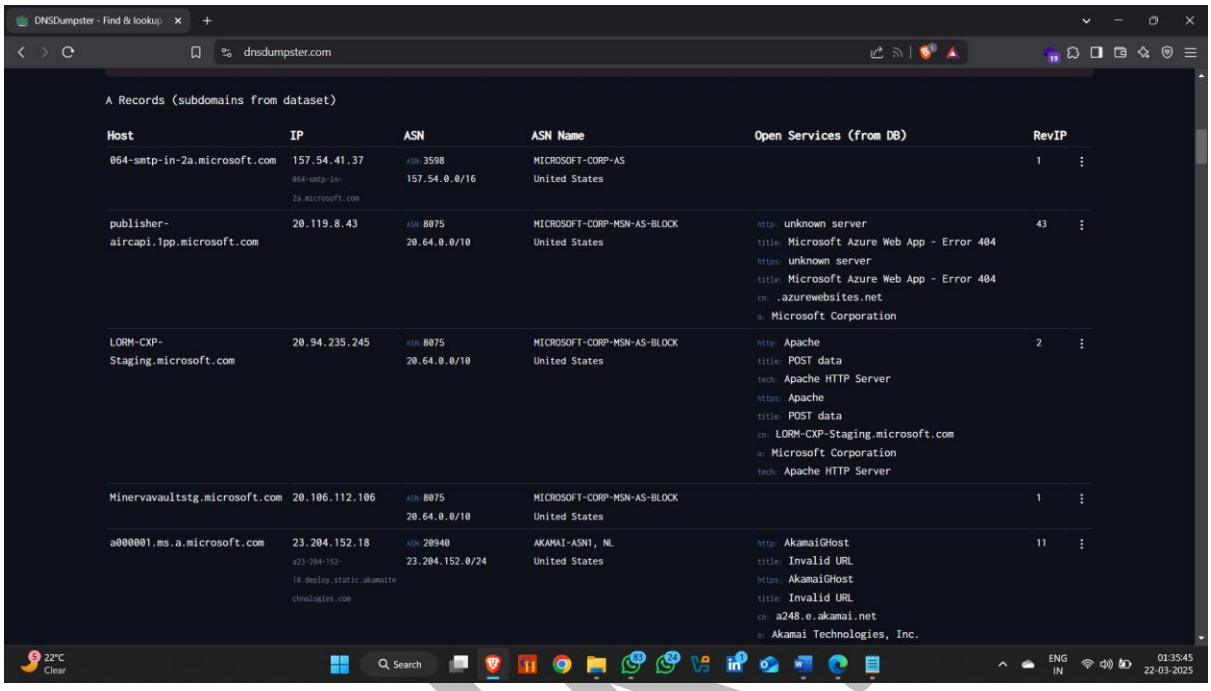
Step 1 - Open your Browser .

Step 2 - Search DNS dumster .



Step 3 – Search a domain (eg – Microsoft.com)

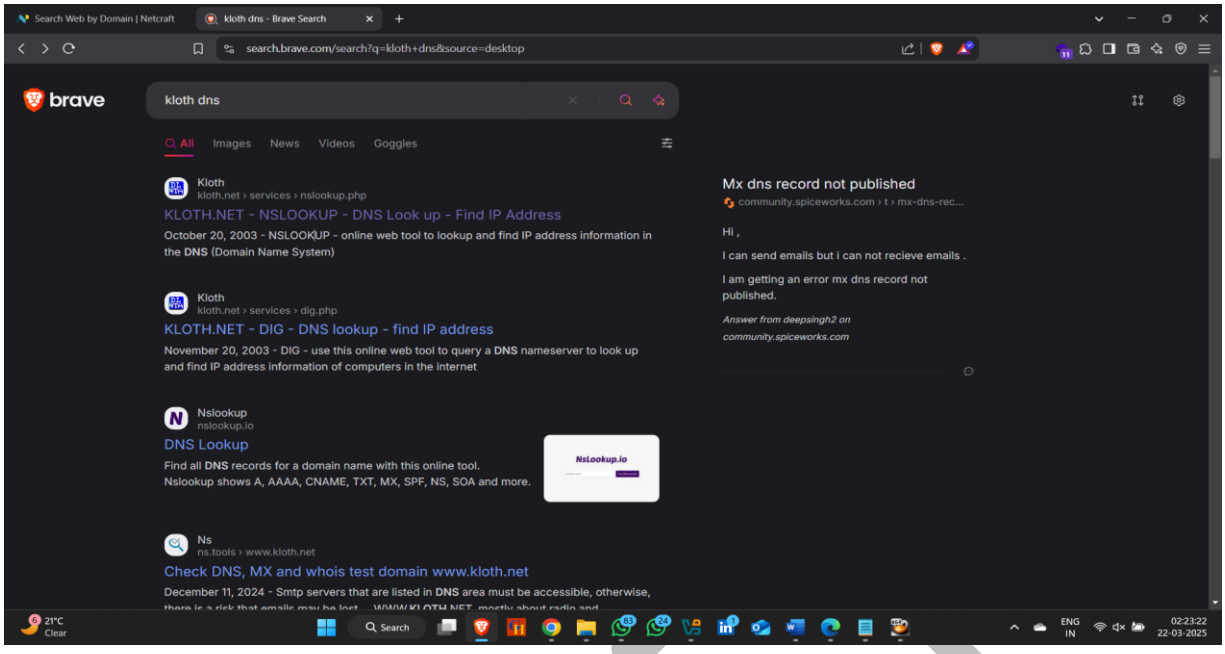
Step 4 – click on start test.



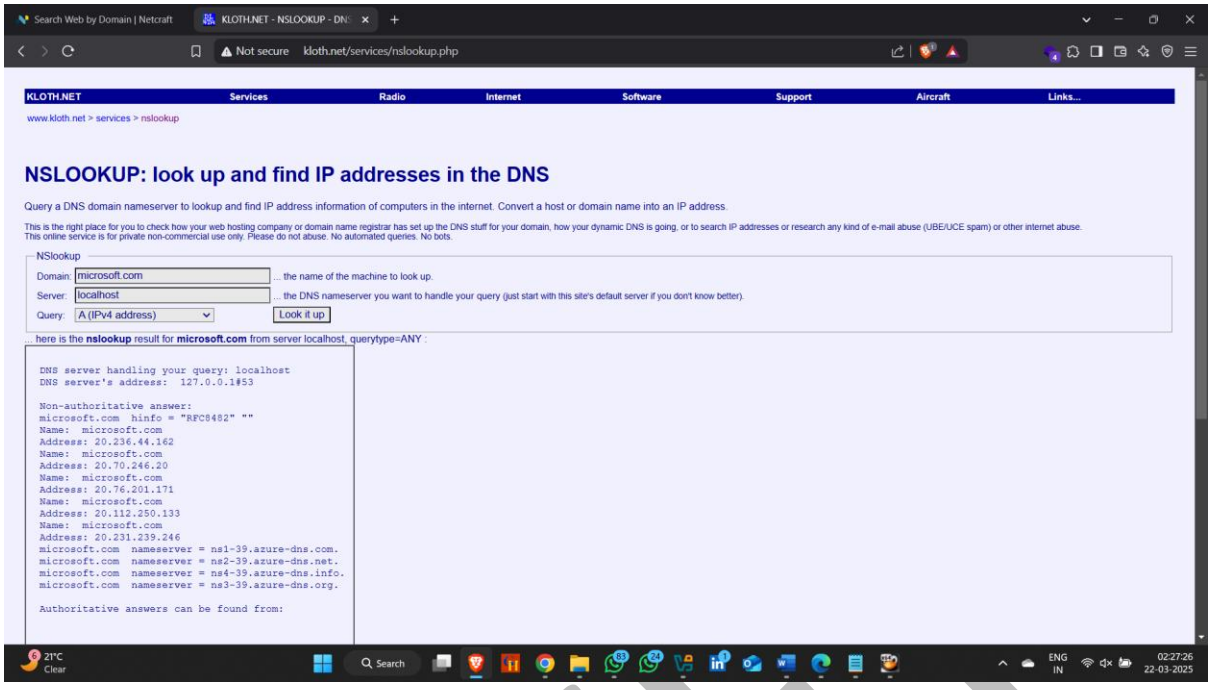
6. DNS Footprinting Using Kloth DNS / nslookup (GUI)

How to do it

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



- Type domain name.
- And search .


Search Web by Domain | Netcraft
KLOTH.NET - NSLOOKUP - DNS
Not secure
kloth.net/services/nslookup.php
KLOTH.NET
Services
Radio
Internet
Software
Support
Aircraft
Links...
www.kloth.net > services > nslookup
NSLOOKUP: look up and find IP addresses in the DNS
Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.
This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.
This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.
NSlookup
Domain: microsoft.com ... the name of the machine to look up.
Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).
Query: A (IPv4 address)
Look it up
... here is the nslookup result for microsoft.com from server localhost, querytype=ANY :
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53
Non-authoritative answer:
microsoft.com hinfo = "RFC8482" ""
Name: microsoft.com
Address: 20.236.44.162
Name: microsoft.com
Address: 20.70.246.20
Name: microsoft.com
Address: 20.76.201.171
Name: microsoft.com
Address: 20.112.250.133
Name: microsoft.com
Address: 20.231.239.246
microsoft.com nameserver = ns1-39.azure-dns.com.
microsoft.com nameserver = ns2-39.azure-dns.net.
microsoft.com nameserver = ns4-39.azure-dns.info.
microsoft.com nameserver = ns3-39.azure-dns.org.
Authoritative answers can be found from:
21°C
Clear
Search
ENG
IN
02:27:26
22-03-2025

ANIKET

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

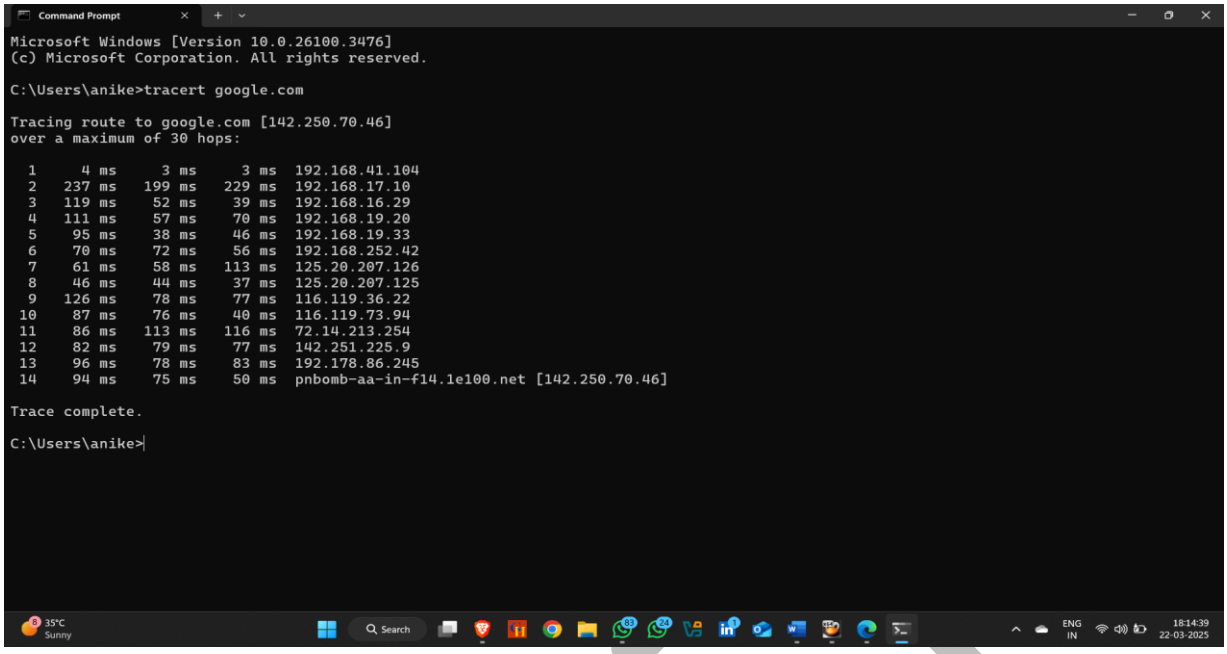
ANIKET

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 Use It

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

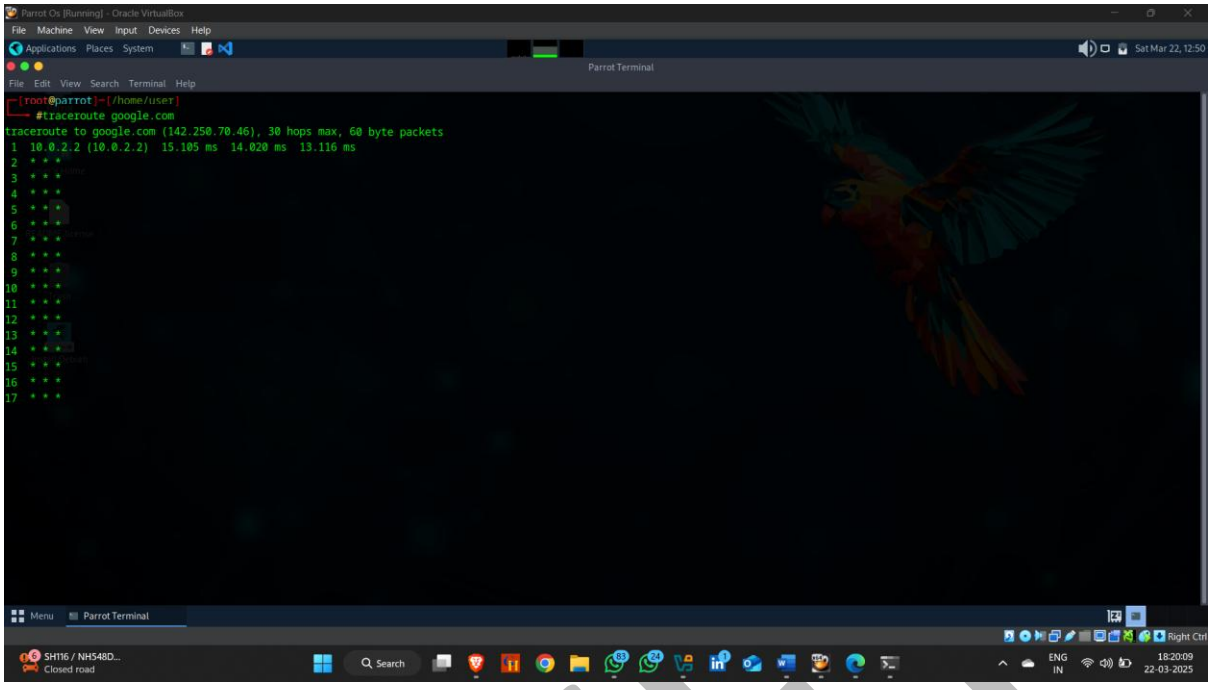


2. Network Footprinting Using Linux traceroute (CLI)

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 use It

1. Open a terminal.
2. Type traceroute followed by a destination, like traceroute google.com, and hit Enter.
3. Output looks something like this:



3. Network Footprinting Using Recon-ng Tool

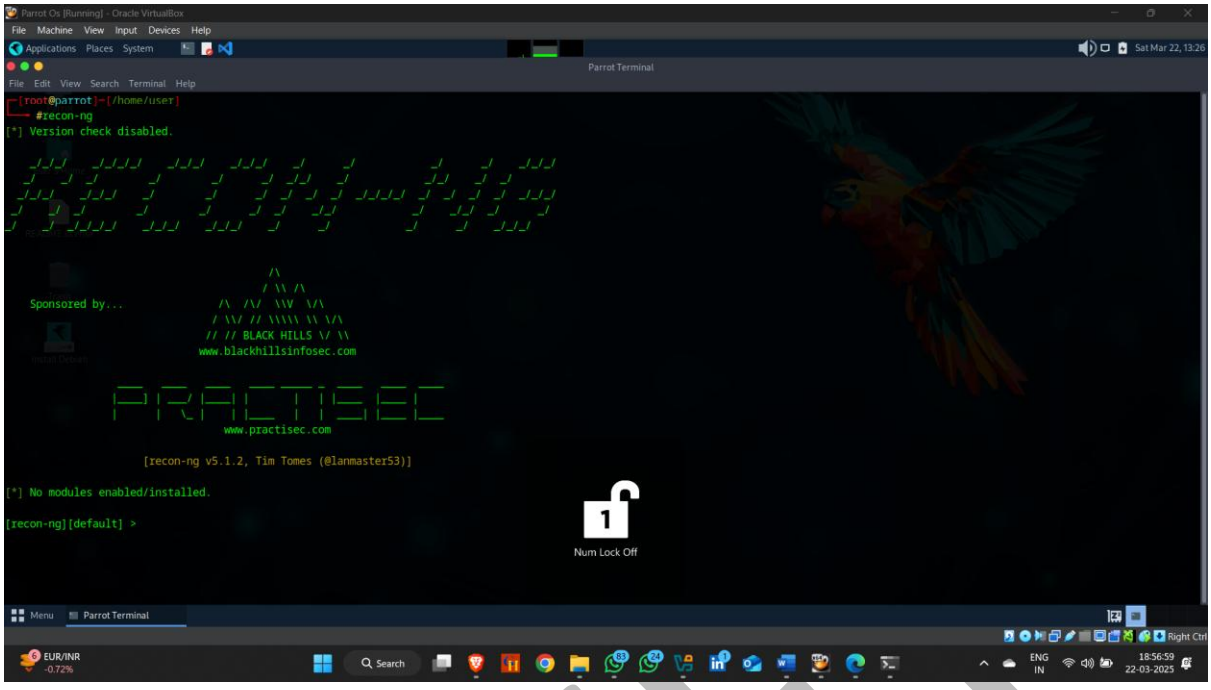
Recon-ng is a powerful open-source reconnaissance framework built into Kali Linux, designed for web-based information gathering using Open Source Intelligence (OSINT).

How to Use Recon-ng in Kali Linux

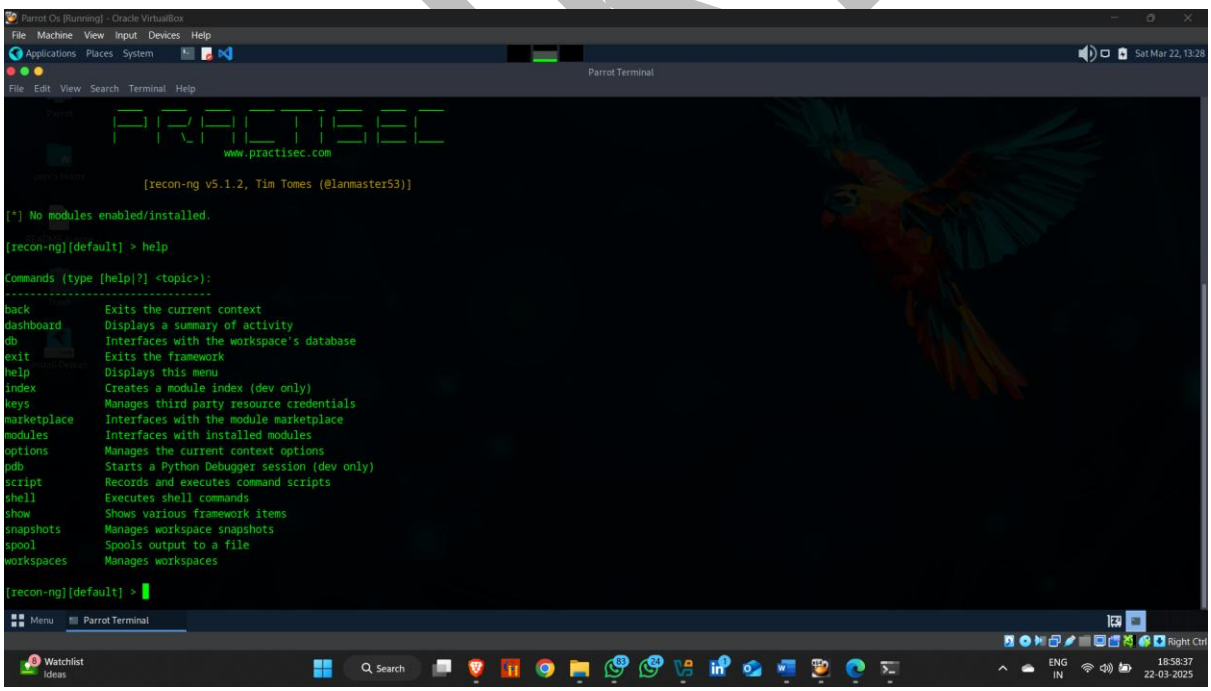
Here's a step-by-step guide to get started with Recon-ng on Kali Linux:

Launch Recon-ng

1. Open a terminal in Kali Linux
2. Type recon-ng



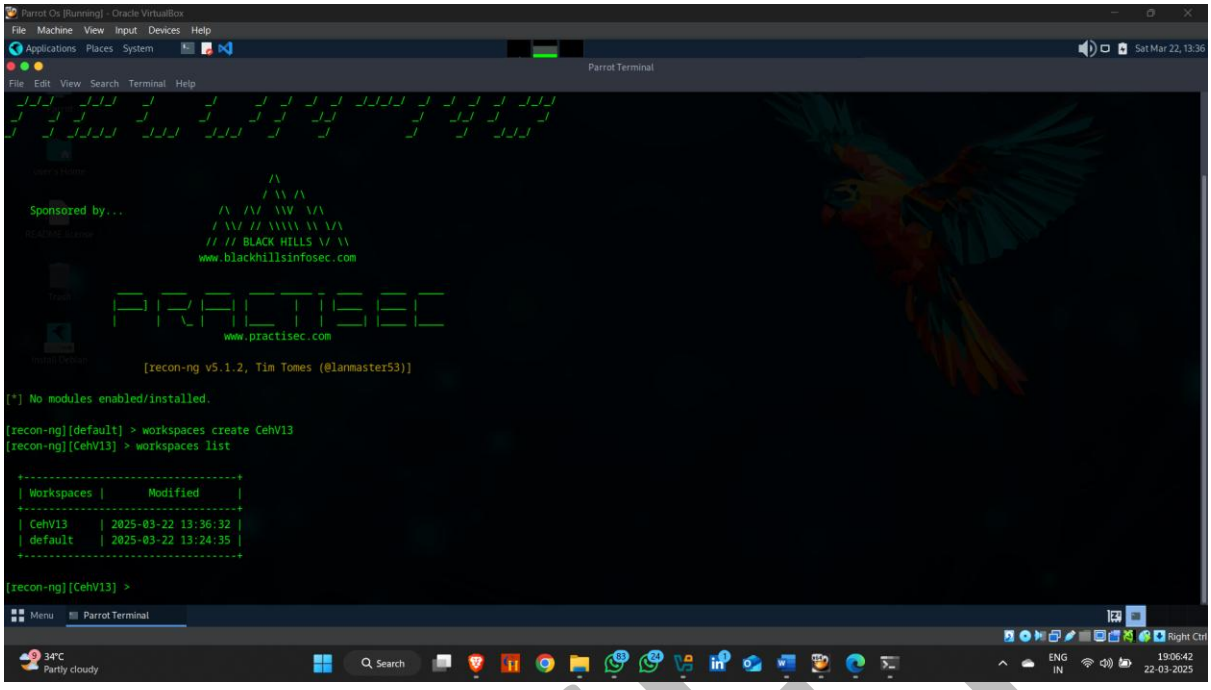
1. Check Available Commands
2. To view the list of commands, type: help



3. Common commands include marketplace, modules, workspaces, db, options, and run.

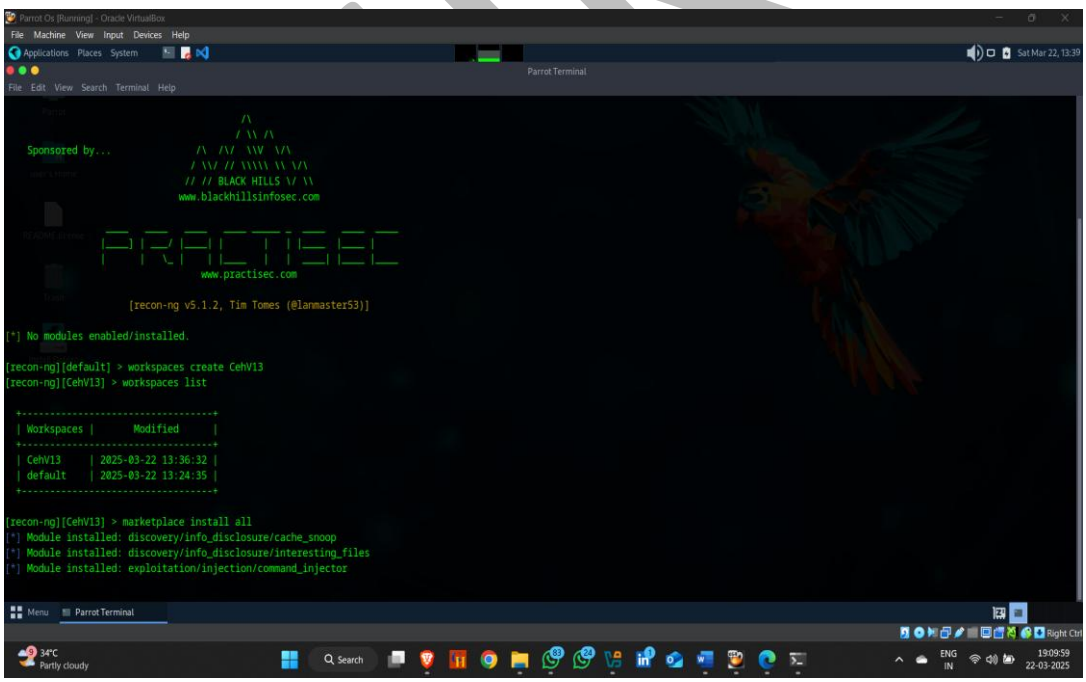
Create a Workspace

- Workspaces Create CehV13



Install Modules

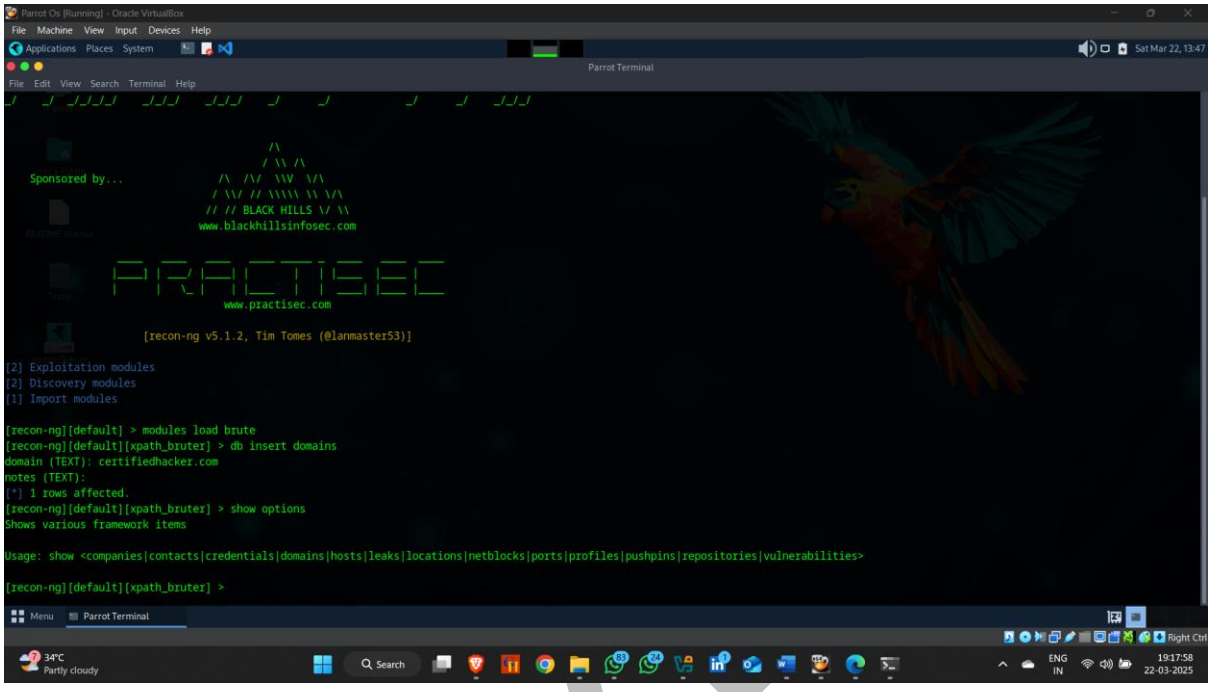
- Marketplace install all



Now create a domain

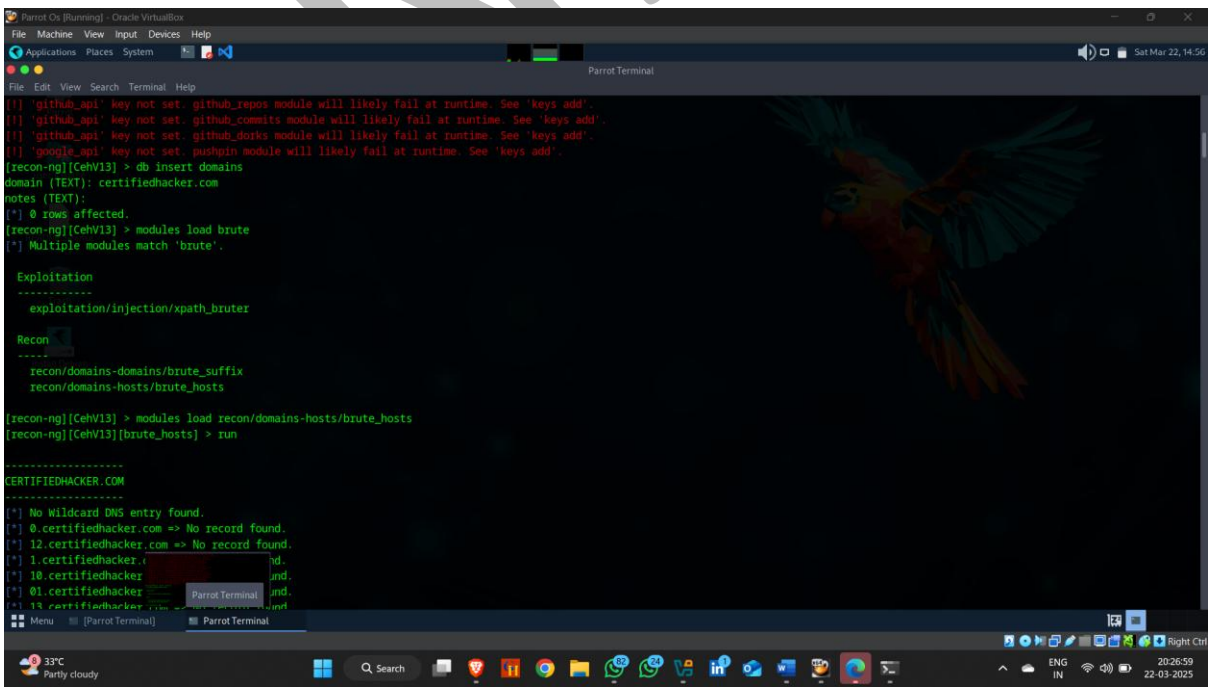
- Db insert domains
- Press enter
- Type domain name

- Show domain



Load a Module

- Modules load <module name>.
- Copy module or type manually.
- Then type modules load <paste module> .
  - **modules load recon/domains-hosts/brute-hosts**
- And type **run.**



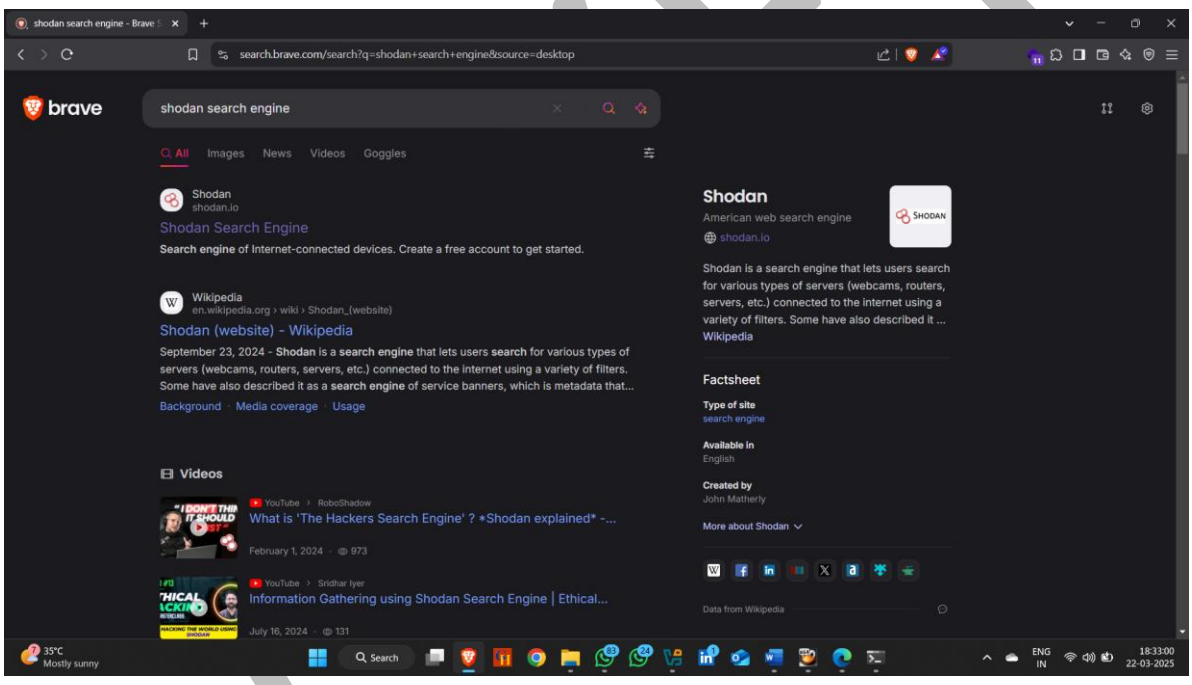
4. Network Footprinting Using Shodan Search Engine

Shodan scans the internet for devices such as servers, routers, webcams, IoT devices, and more, cataloging their IP addresses, open ports, and services running on them.

How to use It

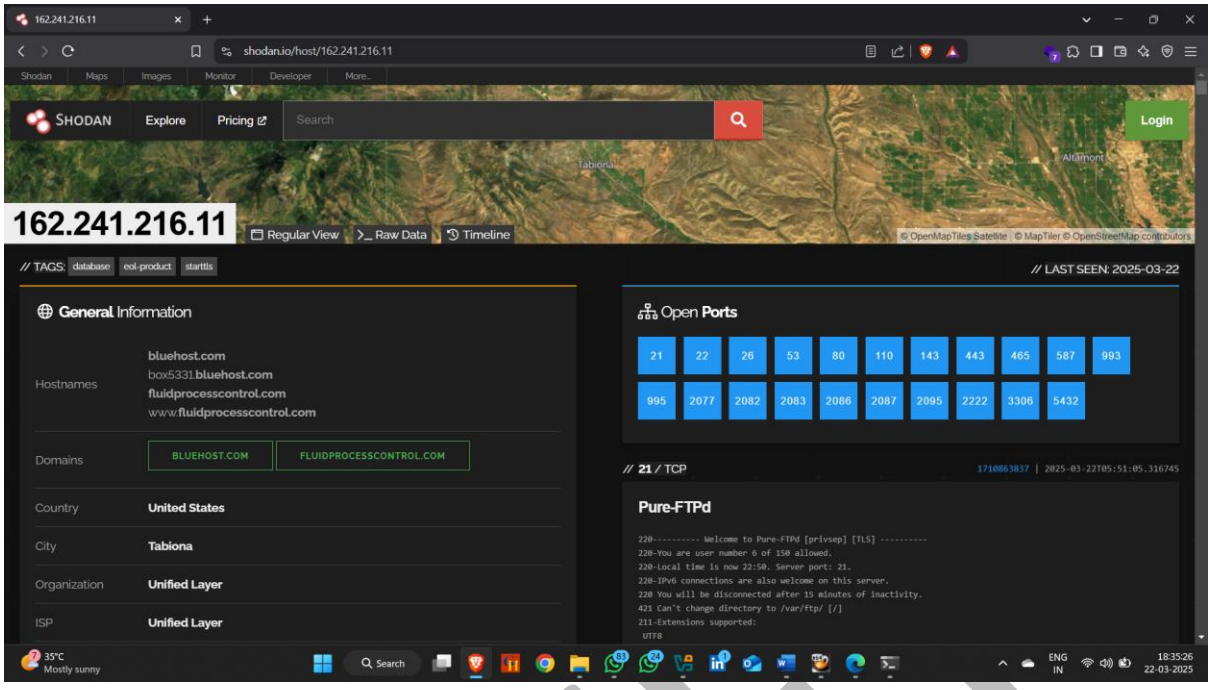
1.Open Browser.

2.Search Shodan Search Engine .



3.Click on first website .

4.Enter a ip address of target domain.


162.241.216.11
shodan.io/host/162.241.216.11
SHODAN
Explore
Pricing
Search
Login
Tabiona
Altamont
162.241.216.11
Regular View
Raw Data
Timeline
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
// TAGS: database eol-product starttls
// LAST SEEN: 2025-03-22
General Information
Hostnames
bluehost.com
box5331.bluehost.com
fluidprocesscontrol.com
www.fluidprocesscontrol.com
Domains
BLUEHOST.COM
FLUIDPROCESSCONTROL.COM
Country
United States
City
Tabiona
Organization
Unified Layer
ISP
Unified Layer
Open Ports
21 22 26 53 80 110 143 443 465 587 993
995 2077 2082 2083 2086 2087 2095 2222 3306 5432
// 21 / TCP
1710863837 | 2025-03-22T05:51:05.316745
Pure-FTPd
220--------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 6 of 150 allowed.
220-Local time is now 22:50. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
421 Can't change directory to /var/ftp/ [/]
211-Extensions supported:
UTF8
35°C
Mostly sunny
Search
ENG
IN
18:35:26
22-03-2025

SOCIA MEDIA FOOTPRINTING

Social media footprinting refers to the trail of digital information that individuals or organizations leave behind on social media platforms.

Objectives -:

1. Collecting Public Profiles
2. Analyzing Posts and Comments
3. Extracting Metadata from Images
4. Identifying Friends and Connections
5. Tracking Location Data

ANIKET

1. Social Media Footprinting Using Peekyou Website

PeekYou is a **people search engine** that aggregates publicly available information about individuals from across the internet.

How to use It

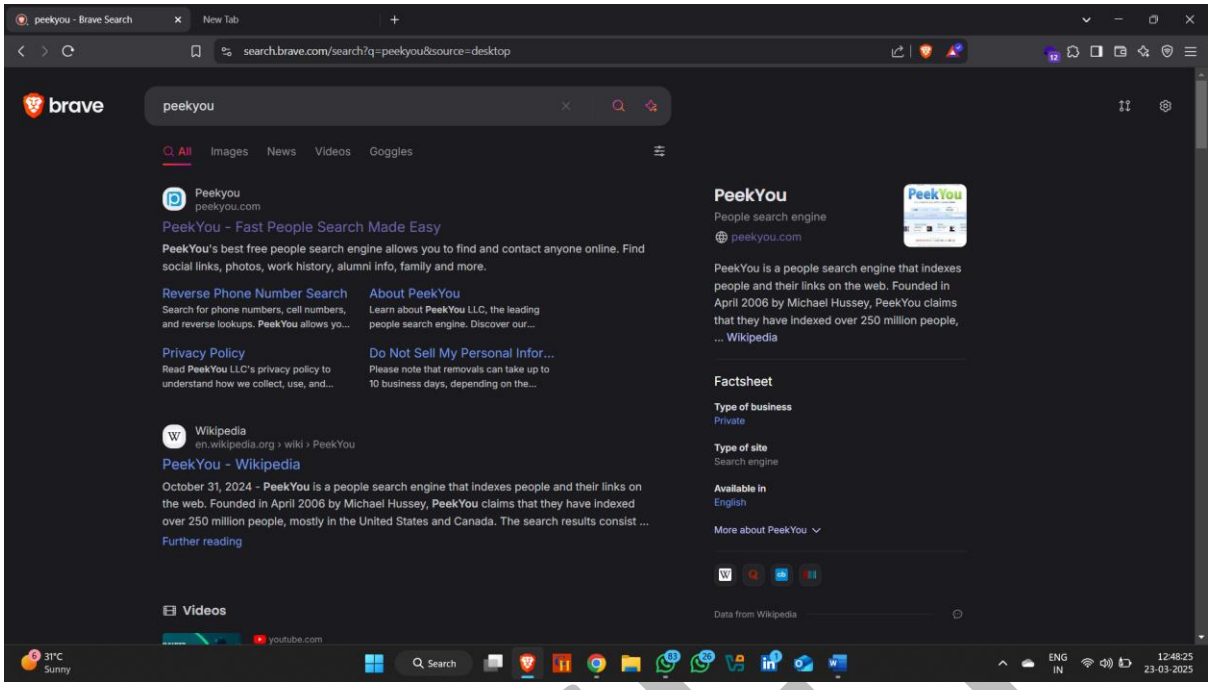
1.Open Browser.

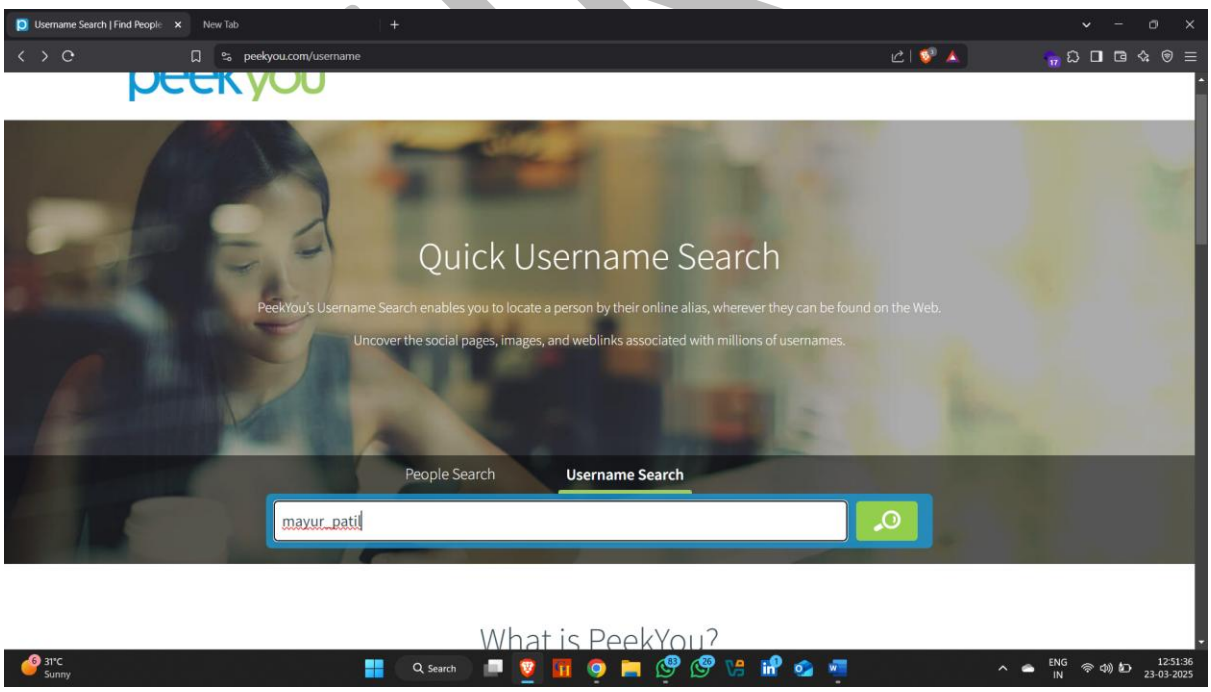
2.Search peekyou

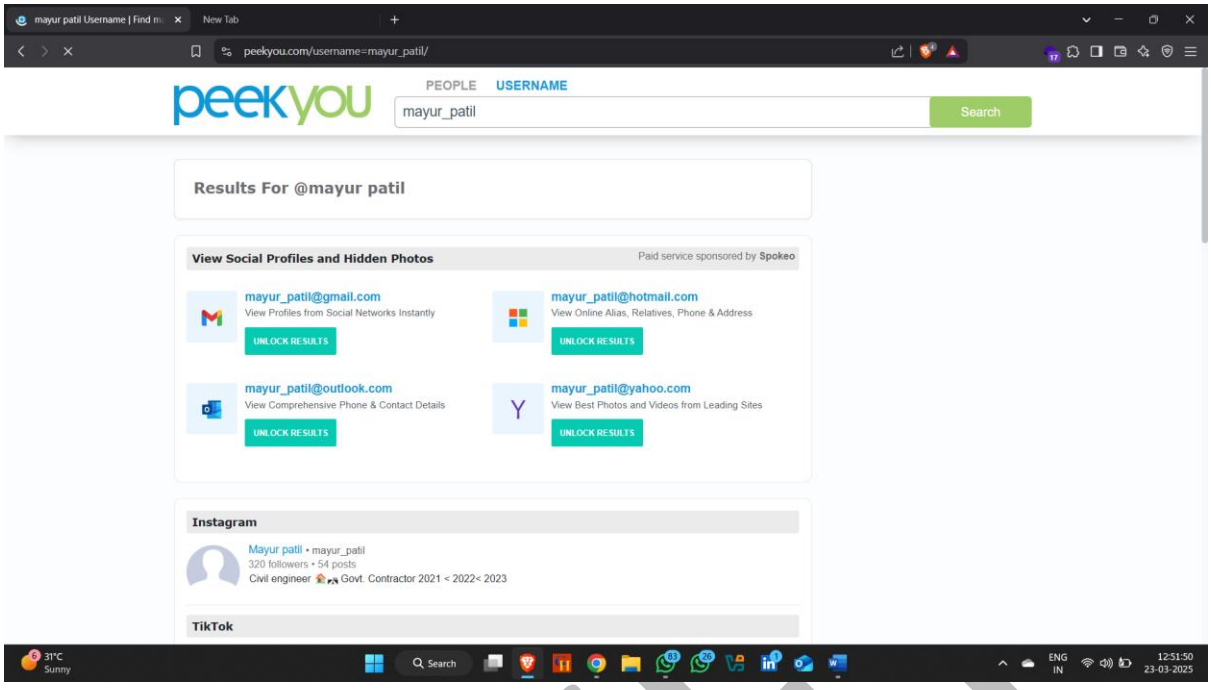
3.open official peekyou website

4.click on **username** tab.

5. Enter username of person that you want to gather social media information


peekyou - Brave Search
New Tab
search.brave.com/search?q=peekyou&source=desktop
brave
peekyou
All
Images
News
Videos
Goggles
Peekyou
peekyou.com
PeekYou - Fast People Search Made Easy
PeekYou's best free people search engine allows you to find and contact anyone online. Find social links, photos, work history, alumni info, family and more.
Reverse Phone Number Search
Search for phone numbers, cell numbers, and reverse lookups. PeekYou allows yo...
About PeekYou
Learn about PeekYou LLC, the leading people search engine. Discover our...
Privacy Policy
Read PeekYou LLC's privacy policy to understand how we collect, use, and...
Do Not Sell My Personal Infor...
Please note that removals can take up to 10 business days, depending on the...
Wikipedia
en.wikipedia.org › wiki › PeekYou
PeekYou - Wikipedia
October 31, 2024 - PeekYou is a people search engine that indexes people and their links on the web. Founded in April 2006 by Michael Hussey, PeekYou claims that they have indexed over 250 million people, mostly in the United States and Canada. The search results consist ...
Further reading
Videos
youtube.com
PeekYou
People search engine
peekyou.com
PeekYou is a people search engine that indexes people and their links on the web. Founded in April 2006 by Michael Hussey, PeekYou claims that they have indexed over 250 million people, ... Wikipedia
Factsheet
Type of business
Private
Type of site
Search engine
Available in
English
More about PeekYou
Data from Wikipedia
31°C
Sunny
Search
ENG
IN
12:48:25
23-03-2025


Username Search | Find People
New Tab
peekyou.com/username
peekyou
Quick Username Search
PeekYou's Username Search enables you to locate a person by their online alias, wherever they can be found on the Web.
Uncover the social pages, images, and weblinks associated with millions of usernames.
People Search
Username Search
mayur_patil
What is PeekYou?
31°C
Sunny
Search
ENG
IN
12:51:36
23-03-2025

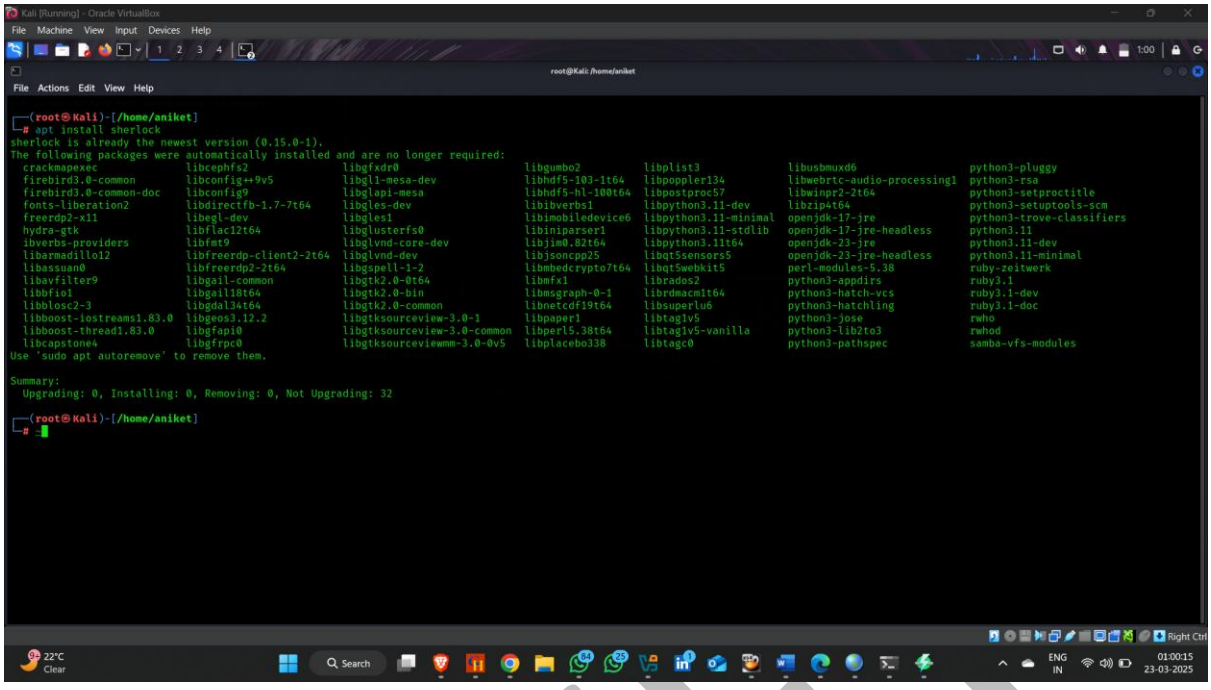


2. Social Media Footprinting Using Sherlock (CLI)

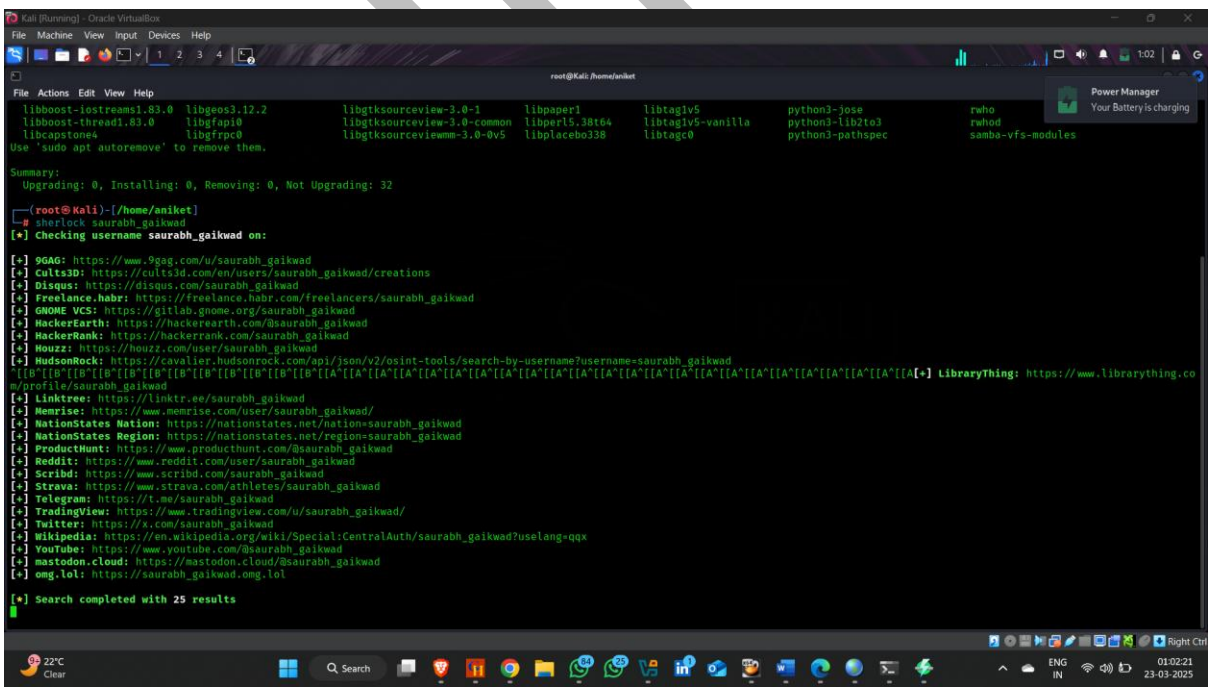
Sherlock is a powerful OSINT (Open Source Intelligence) tool available in Kali Linux that helps you find usernames across social networks.

How to use It

1. Open Kali linux / Parrot OS.
2. Open Terminal.
3. Type **apt install sherlock** on terminal.



4. After install sherlock type username that you want to find social media accounts using sherlock
   Example -: sherlock suarabh_gaikwad



ANIKET