Report

Modules 2

1 Footprinting Concept

Gathering information about a target

2 Types of Footprinting/Recoonnaissnc

- Passive Footprinting
- Active Footprinting
- Common Methods

Task1 Footprinting Through Google Dorking Technique

- What is Google Dorking
- Google Dorking Technique

- **Uses Google Hacking Database**
- **What is the Shodan Search Engine?**

Task2 Information gathering using website

- **mata.io**
- Netcraft
- Who is .com
- DNS-Dumster

NAPALM FTP Indexer

3 Task Fotprinting through Social media networking

- **sublister3r**

Task4 Email Footprinting Using GSA Email spider

- **DNS Footprintig**
- **What are DNS record types?**

- **Find the different type Dns recode using mxtool box**
- **Traceroot**
- **DNS Transfer Zone**

Task5 find the domain information using Recon-ng toolkit

Extra activity using the Harvester

Extra activity using the maltego

Extra activity using the fsocity

Footprinting and Reconnaissanc

Footprinting Concept

Gathering information about a target

- Footprinting involves gathering information about a target typically related to its network infrastructure, systems, and users without actually committing an

attack. Footprinting can be performed manually or using automated tools·

Types of Footprinting/Recoonnaissnc

Passive Footprinting

This involves gathering information without directly interacting with the target. The goal is to avoid detection.

Common Methods:

WHOIS lookups: To find domain registration information.

Social engineering: Gathering info from social media, forums, company websites.

Search engines (Google hacking): Using search operators to find sensitive data.

DNS interrogation: Using public DNS records to map domain infrastructure.

Website analysis: Using tools like Netcraft, BuiltWith, or just checking HTML source

Task1 Footprinting Through Google Dorking Technique

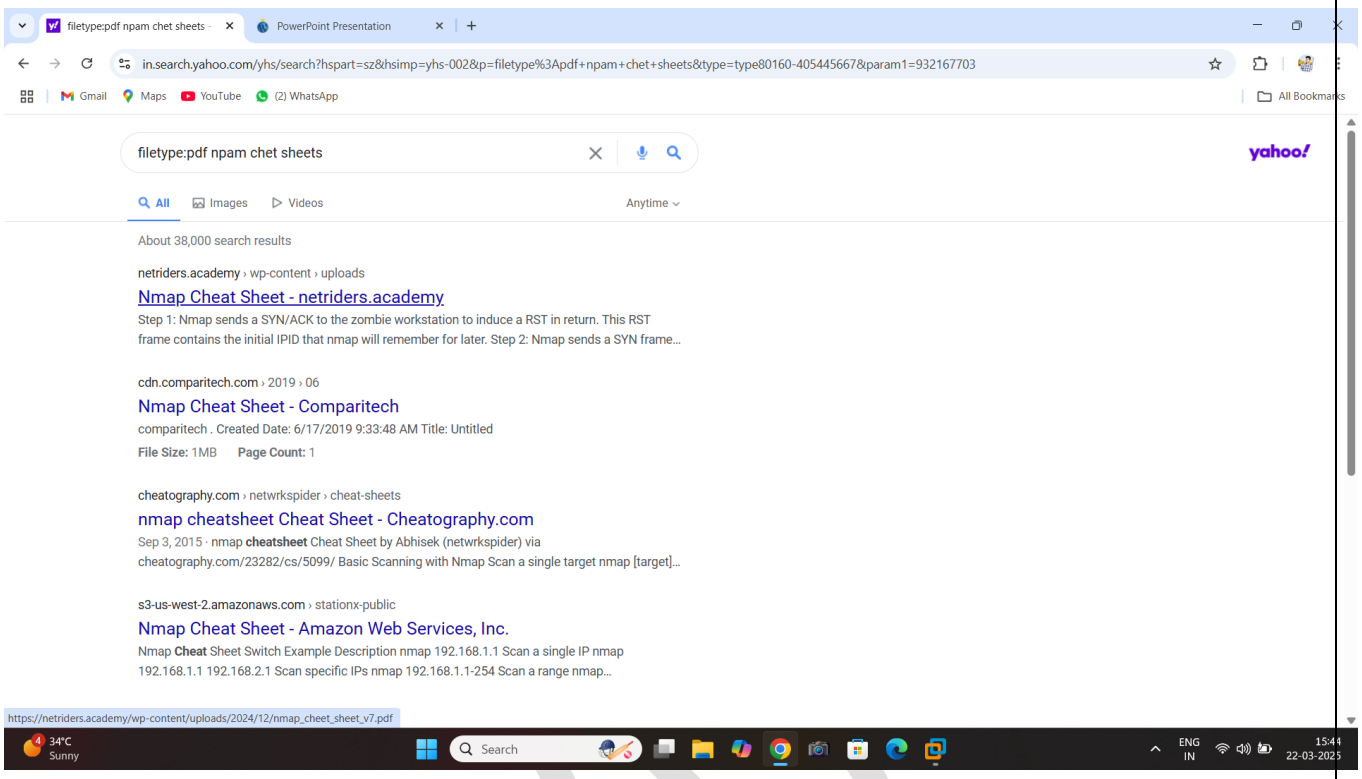
What is Google Dorking.

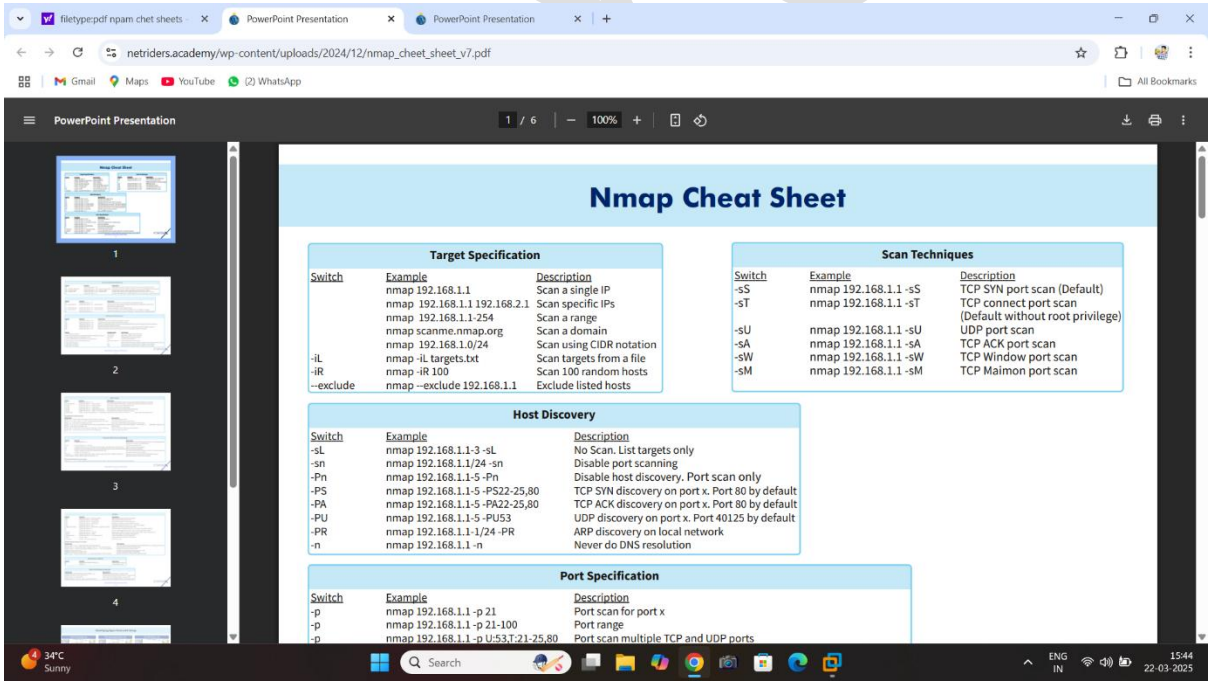
Google hacking, also named Google dorking, is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using

Google Dorking Technique

filetype: pdf nmap cheet sheet

uses: this command are use any file and, pdf clone





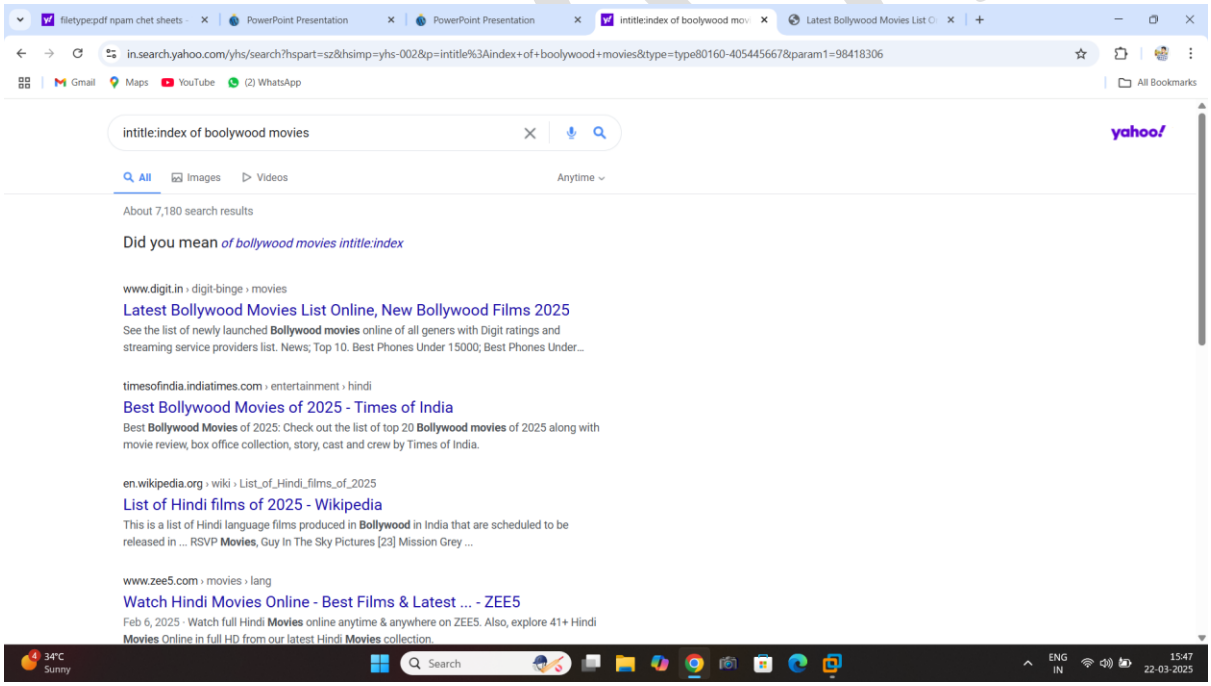
Description:

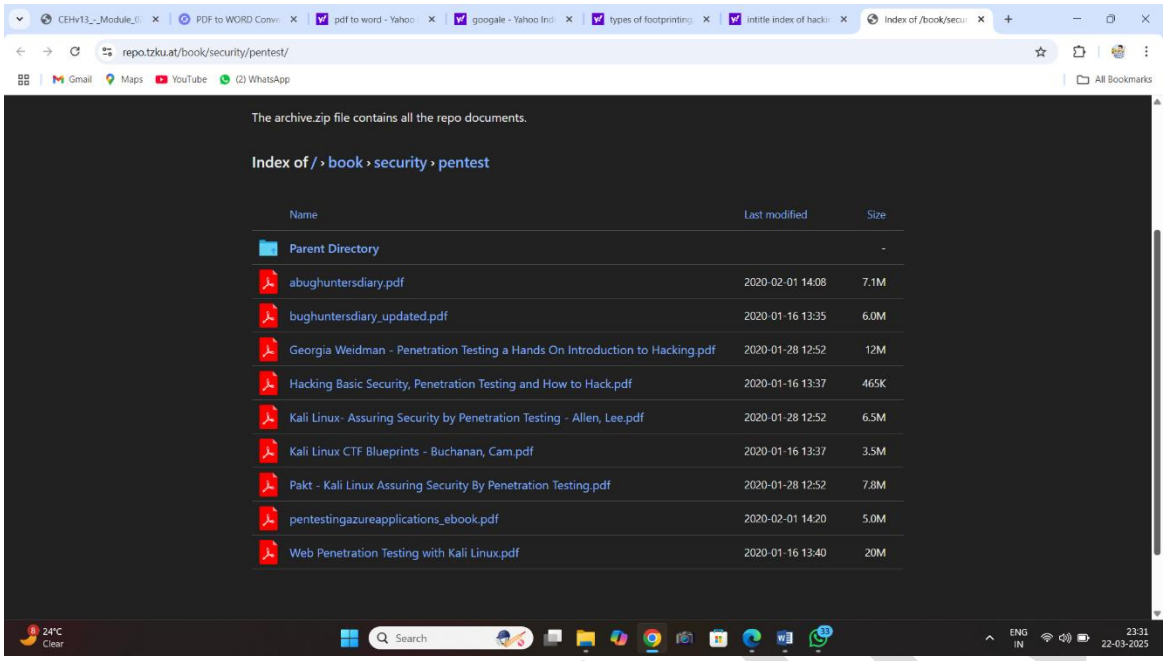
1 The filetype: dork restricts the returned web addresses to the designated file type, such as PDF

or XLS. Unlike most other dorks, it **requires additional keywords/dorks** in the search bar, or it'll return no results. The Google search results have the designated file type. It's necessary for pentests such as bypassing paywalls to access resources.

2 Intitle: index of boolywood movies

Uses : this command are use any index of information



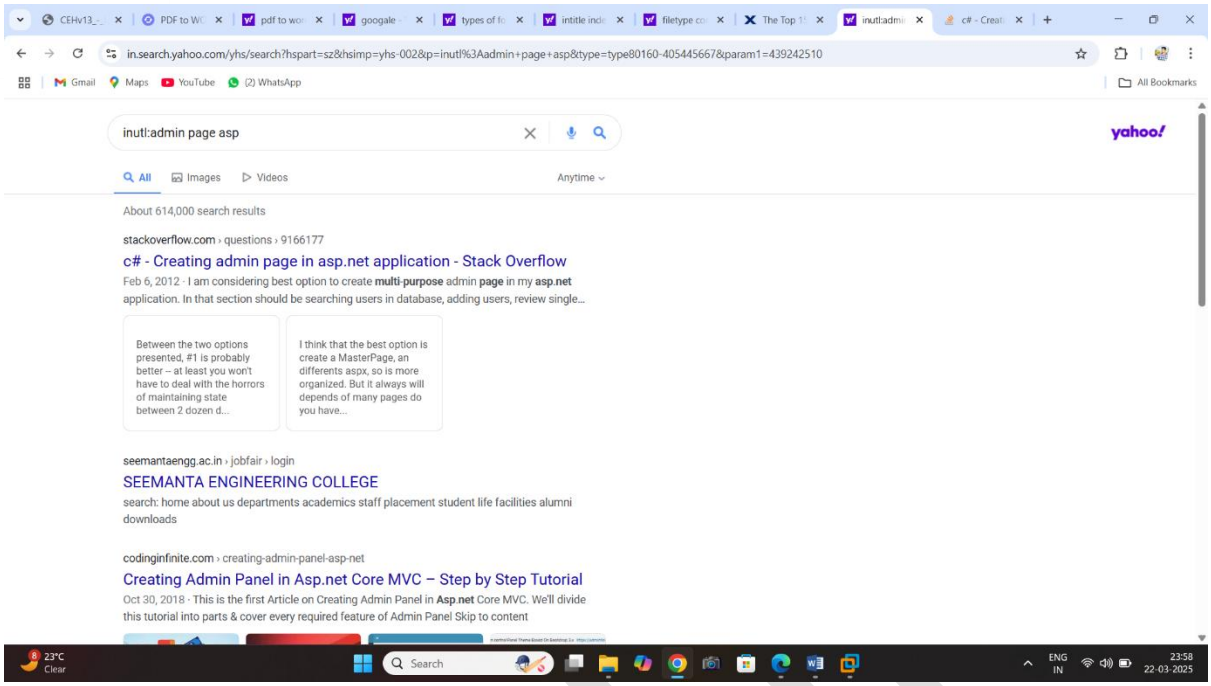


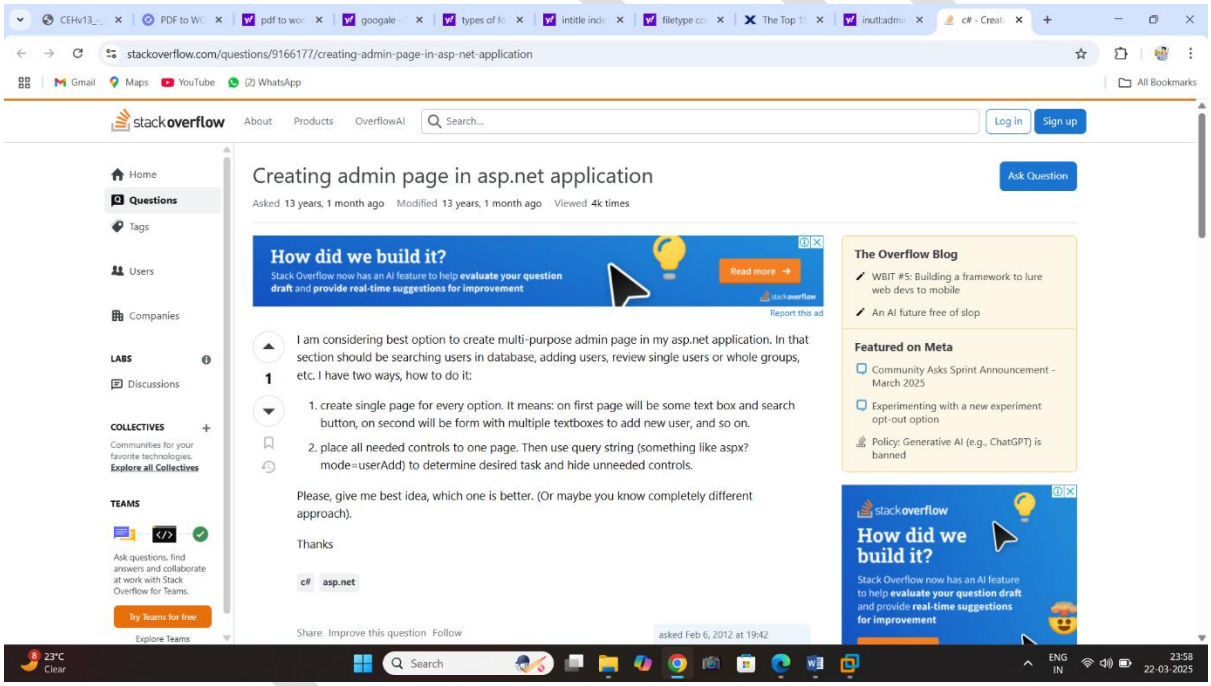
Description:

The **intitle:** dork looks for pages with titles containing the search terms. You can see the query string in the title of each Google search result returned. It's useful when the title of your desired web resource contains a certain keyword. In the example below, we look for all our pages containing "google" in the title.

3 Inurl: admin page asp

uses: this command are use any admin page information and login page language



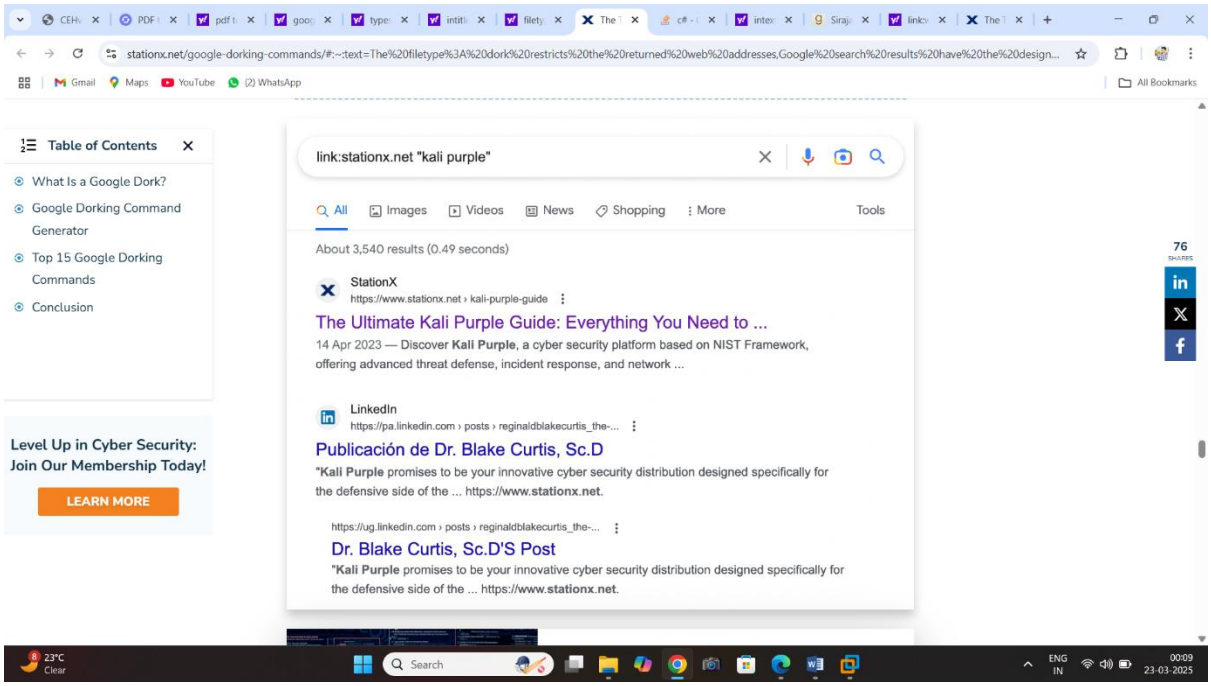


Discription

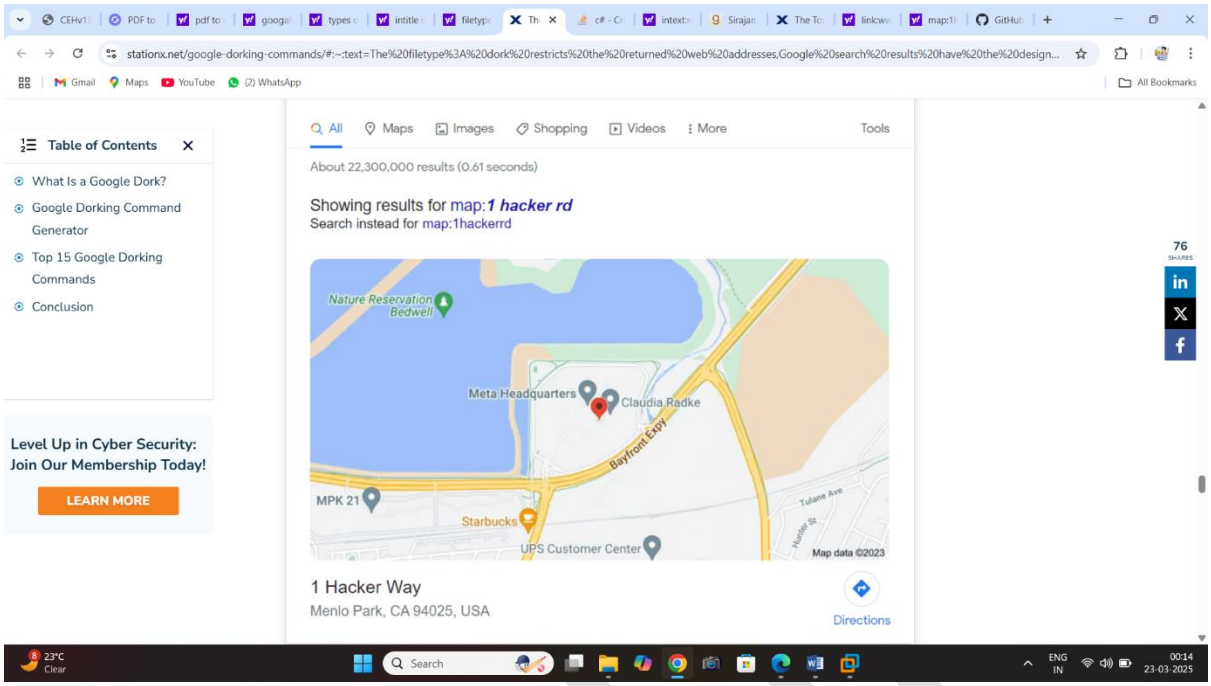
The **inurl:** dork finds URLs containing the character string. You can see the query string in the URL of each Google search result returned. In the example below, the additional dork is to

exclude search results from our website. It’s a handy dork when your desired URLs follow a certain pattern.

4 Linke link: www.stationx.net "kali purple"



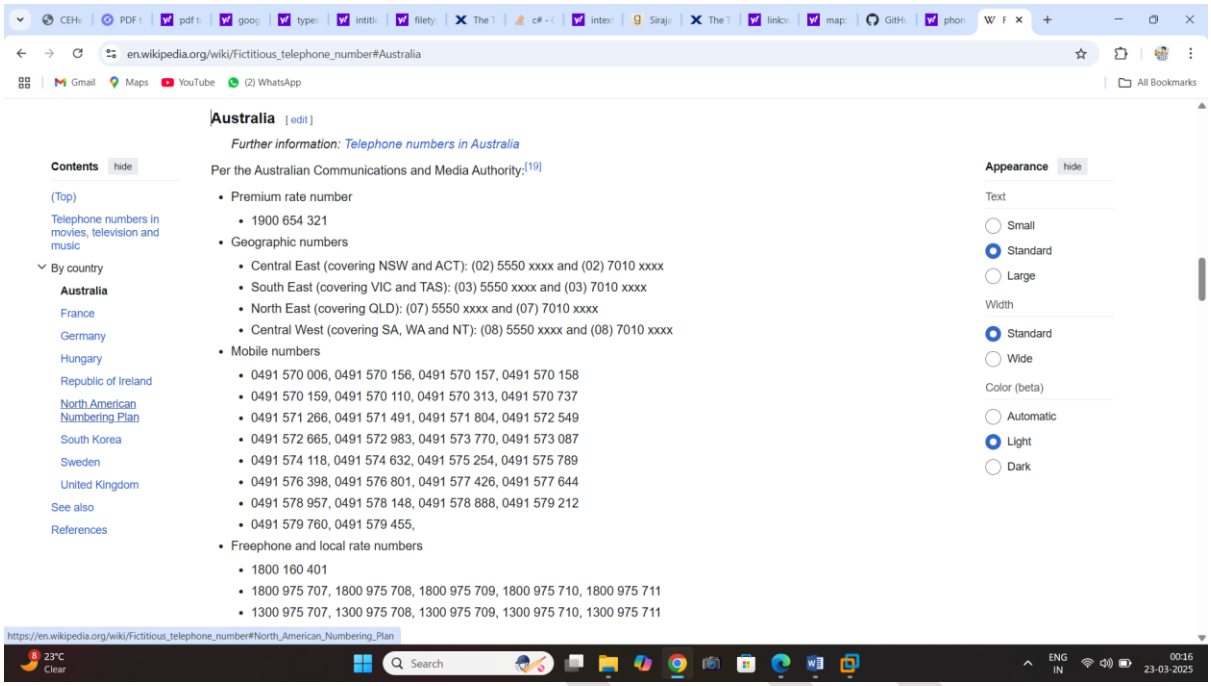
5 map: 1hackerrd

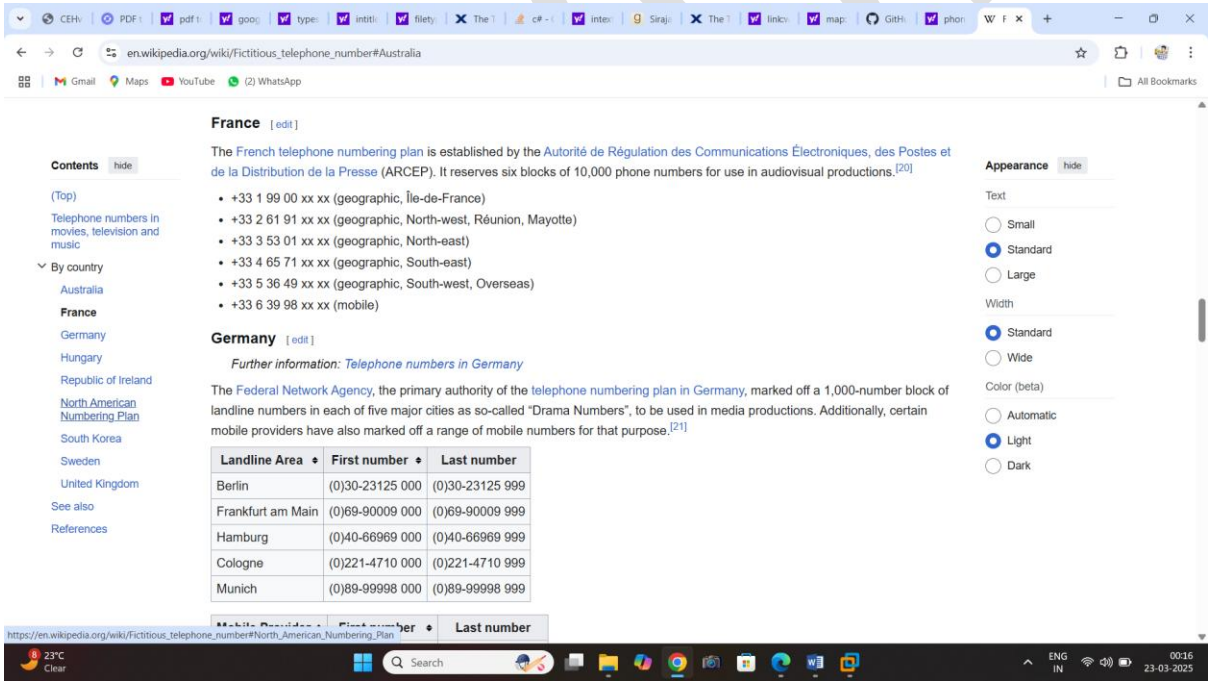


Discription

The **map:** dork is for getting a map of the given location. Google returns with the map you're seeking. On macOS, you may see a prompt to open the Maps application. It's useful when you want a quick map of your desired location

6 phonebook: 555-555-5555





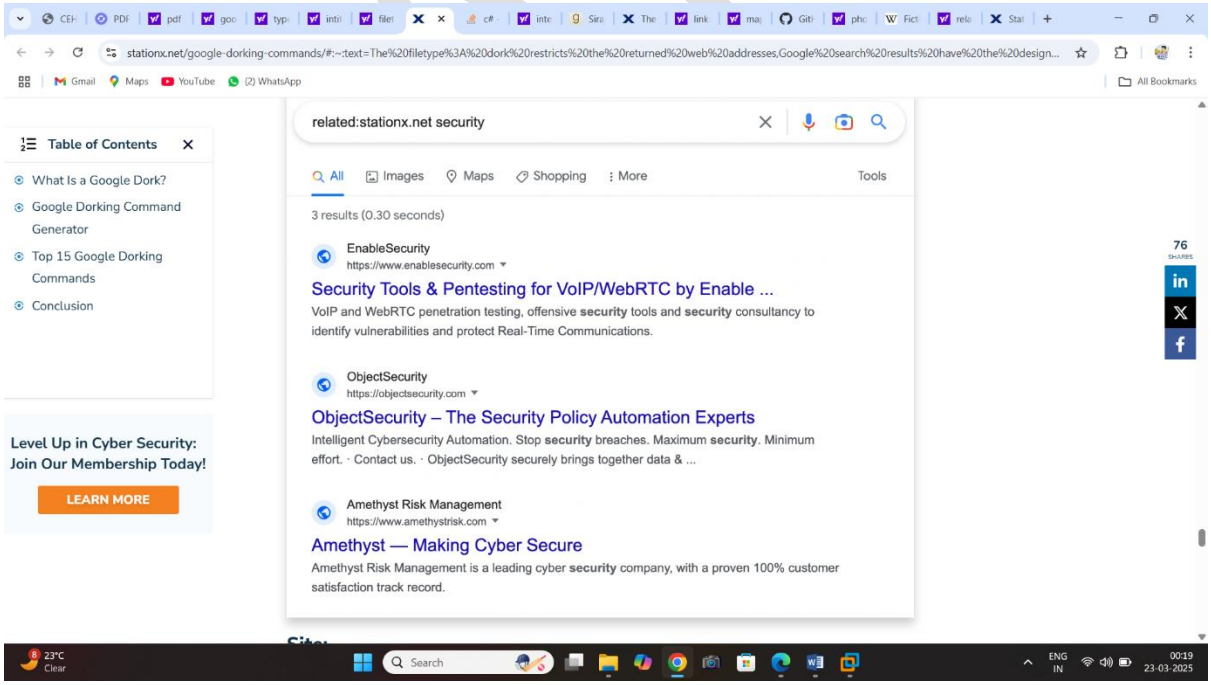
Discription

Phonebook:

The **phonebook:** dork is for getting a specific person or business's phone numbers

and contact information. The Google search may return no results or several. The screenshot demonstration below has to do with **fictional US phone numbers**. This command is helpful when you want to look up caller IDs.

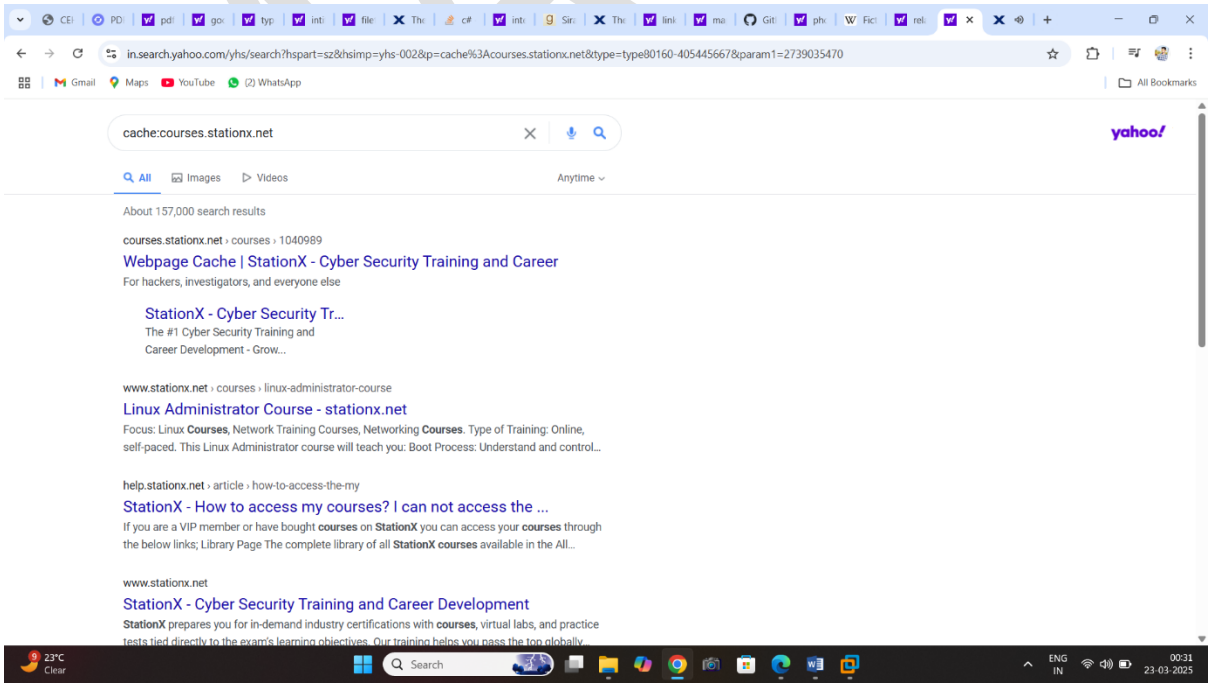
7 related: `www.stationx.net security`

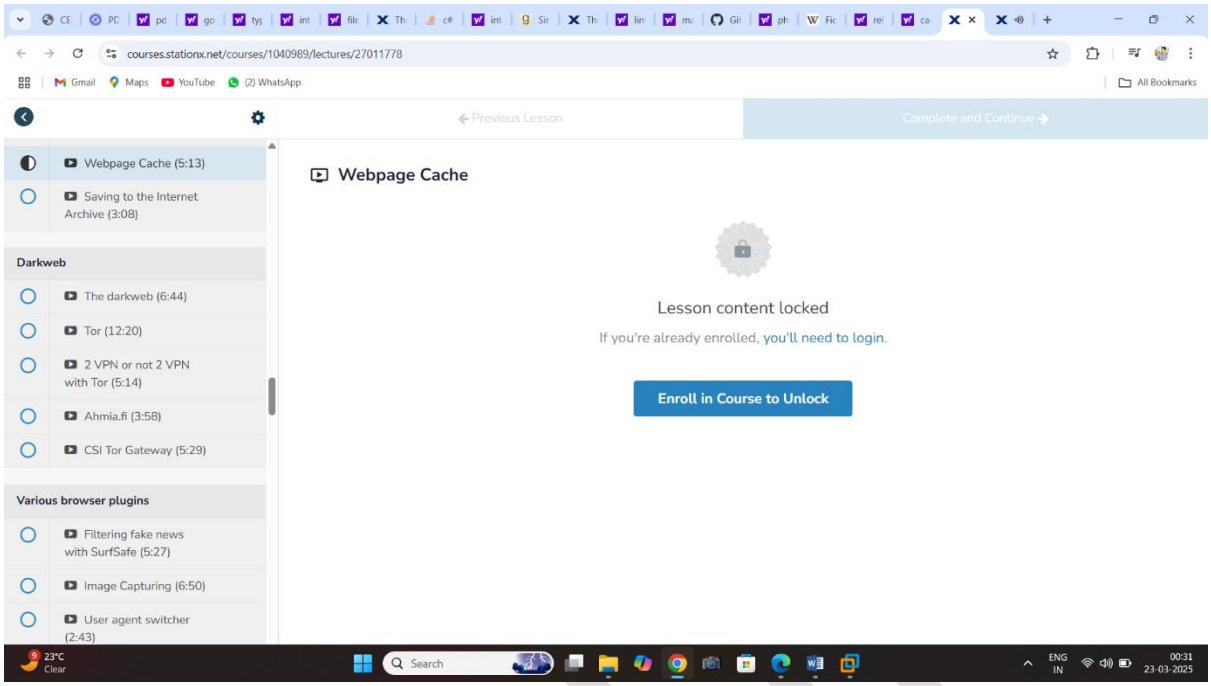


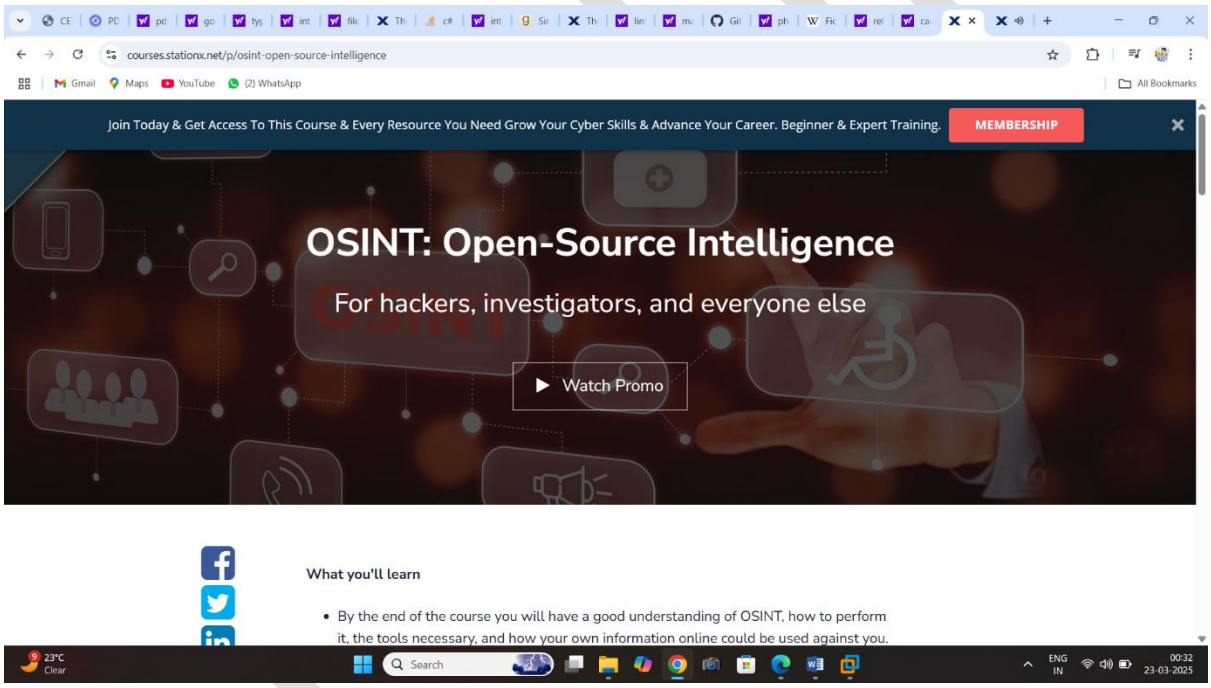
Discription

The **related:** dork returns websites about a given website. The Google search results are similar websites as the one specified. This dork is convenient when you want to broaden your scope and need help figuring out where to start.

8 cache:courses.stationx.net



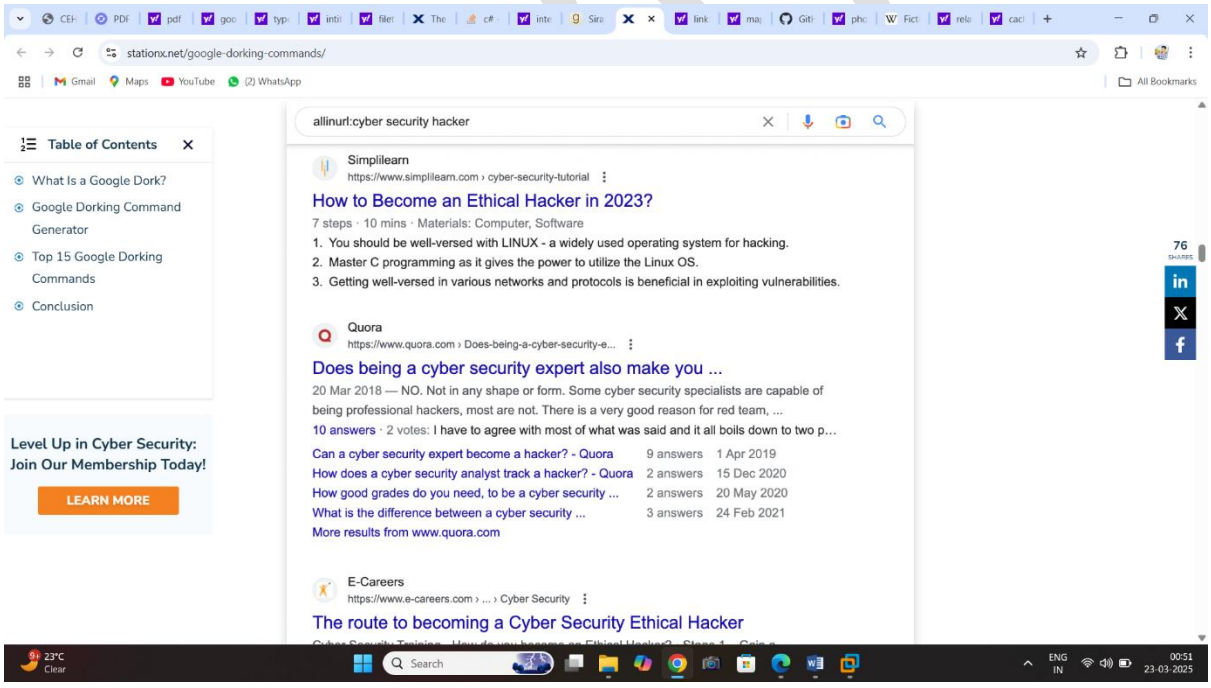




Discription

cache: dork, when you press **Enter/Return**, the Google search console fetches the last saved copy of a particular website (Google cache) if it exists and displays it. It's useful for rediscovering a website before its downtime or latest update.

allinurl: cyber security hacker



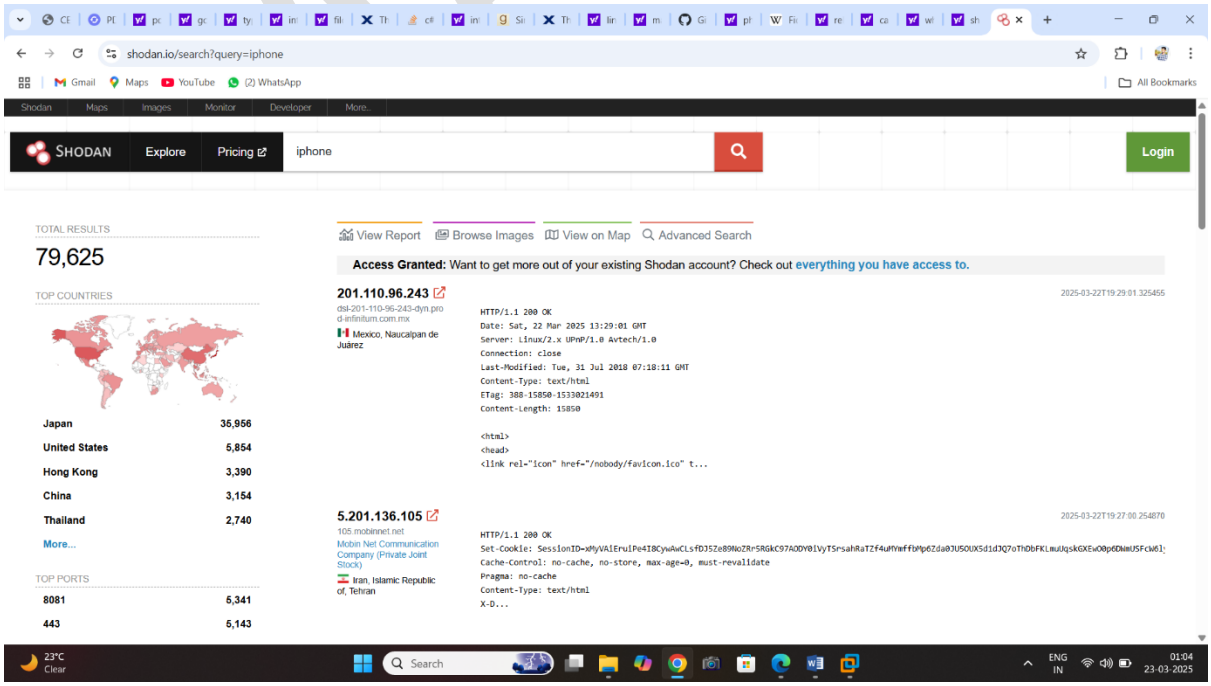
Uses Google Hacking Database

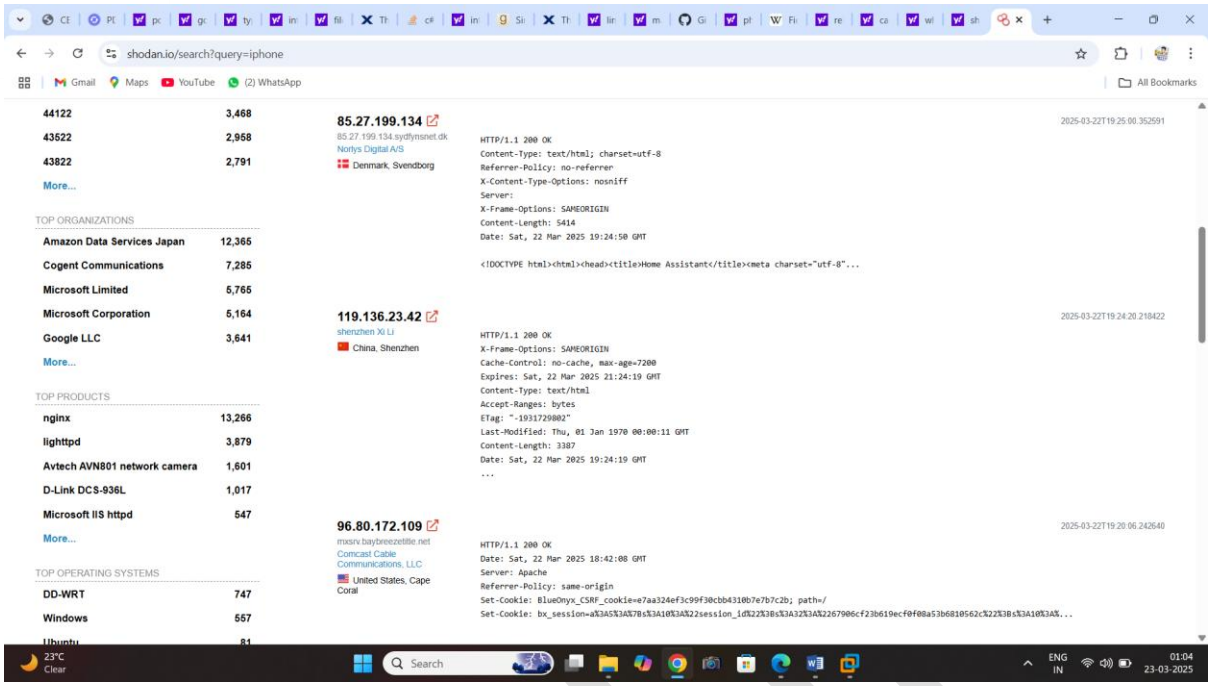
The (GHDB) is an index of search queries (we call them dorks) used to find publicly available information, intended for pentration tester and security researchers.

1 footprinting through shodan search engine optimization

What is the Shodan Search Engine?

Internet-connected devices are everywhere. It's estimated that over 30 billion "Internet of things" or IoT devices are currently active. However, these devices can have security flaws, making them vulnerable to cyber-attacks.

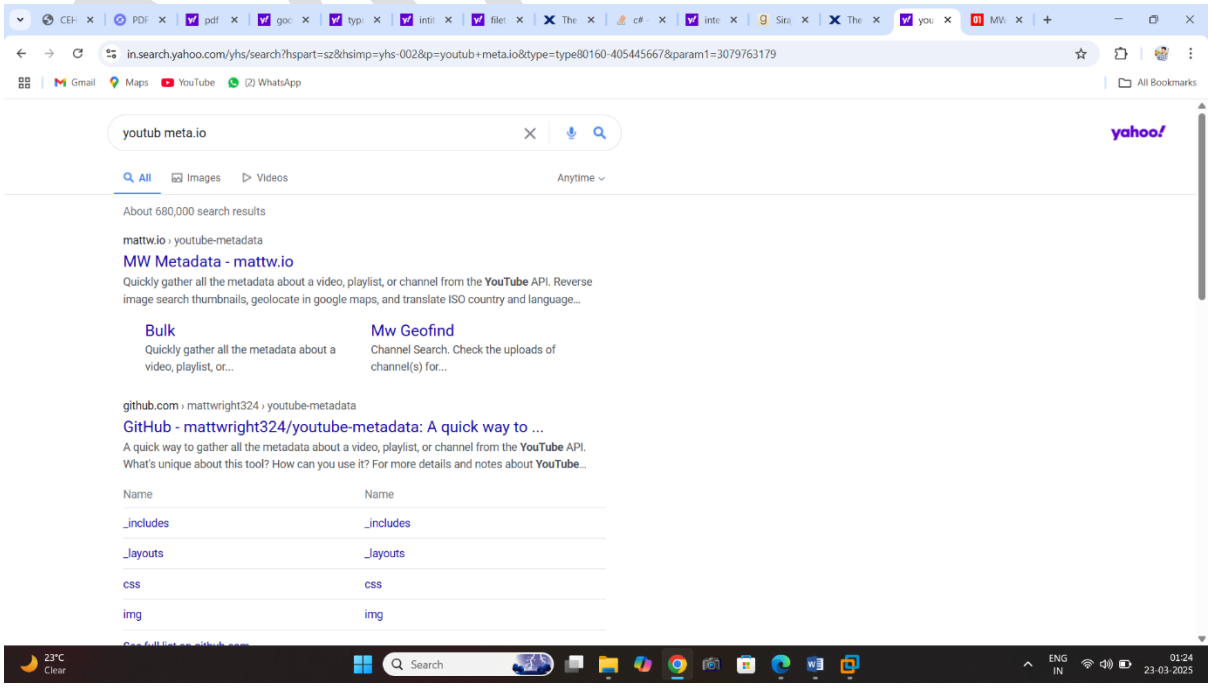


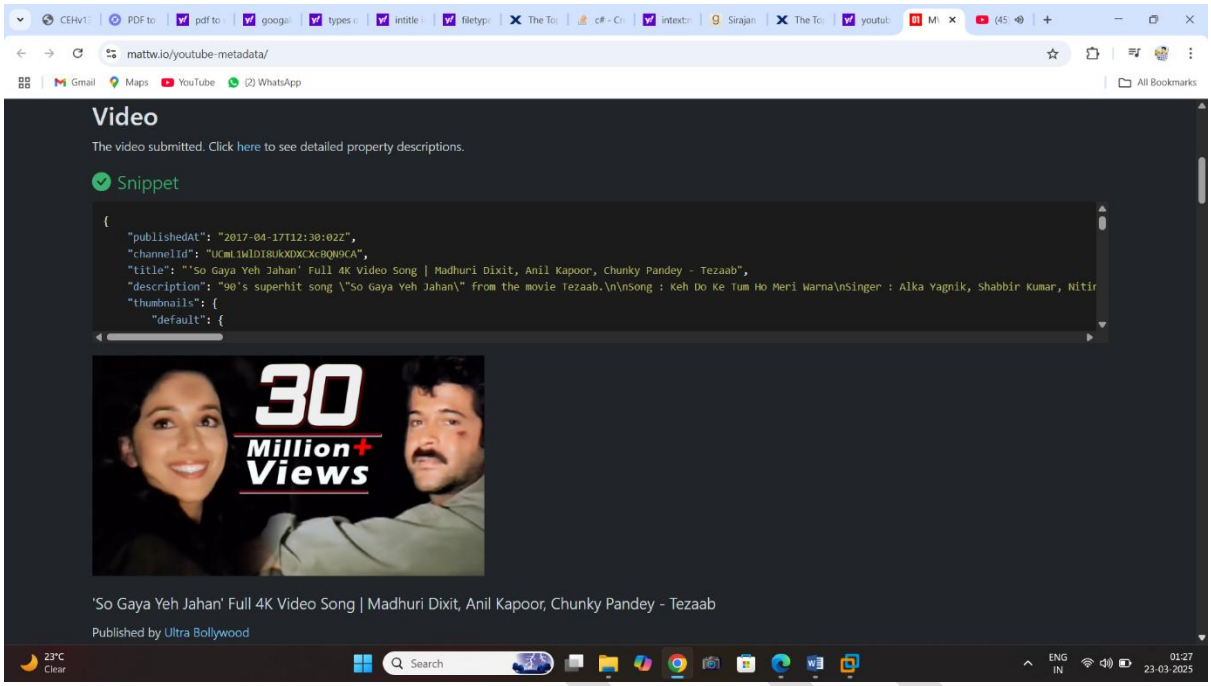


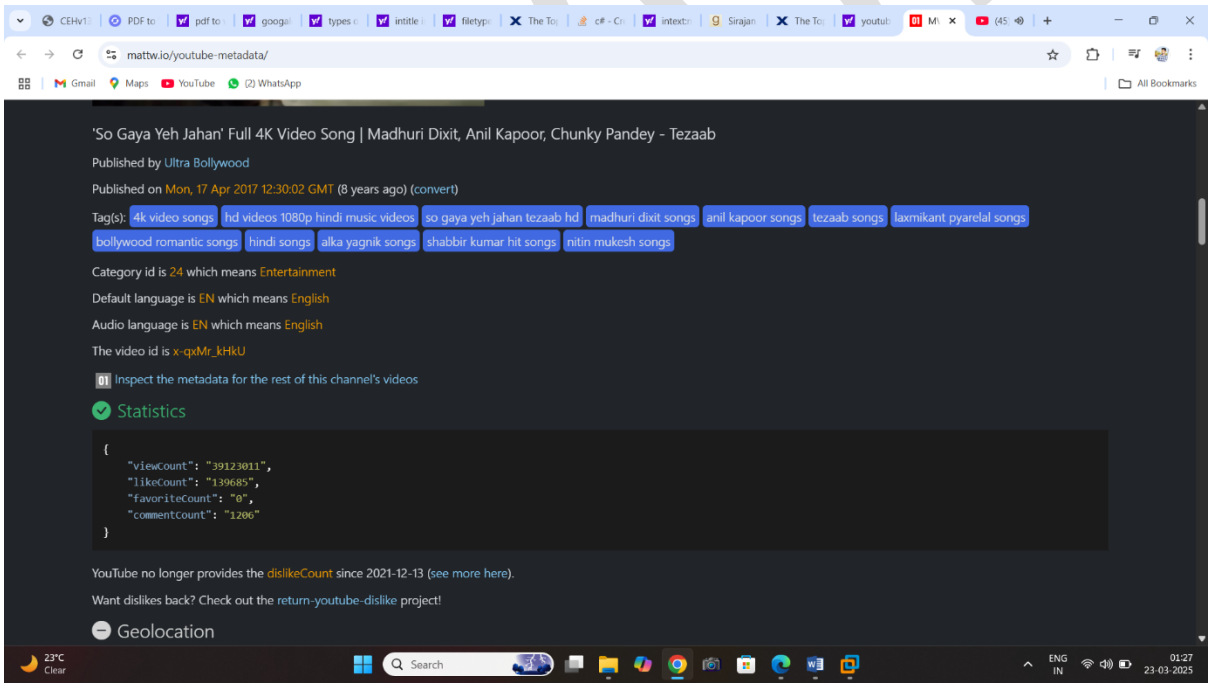
Task2 Information gathering using website

1mata.io

Uses any video information

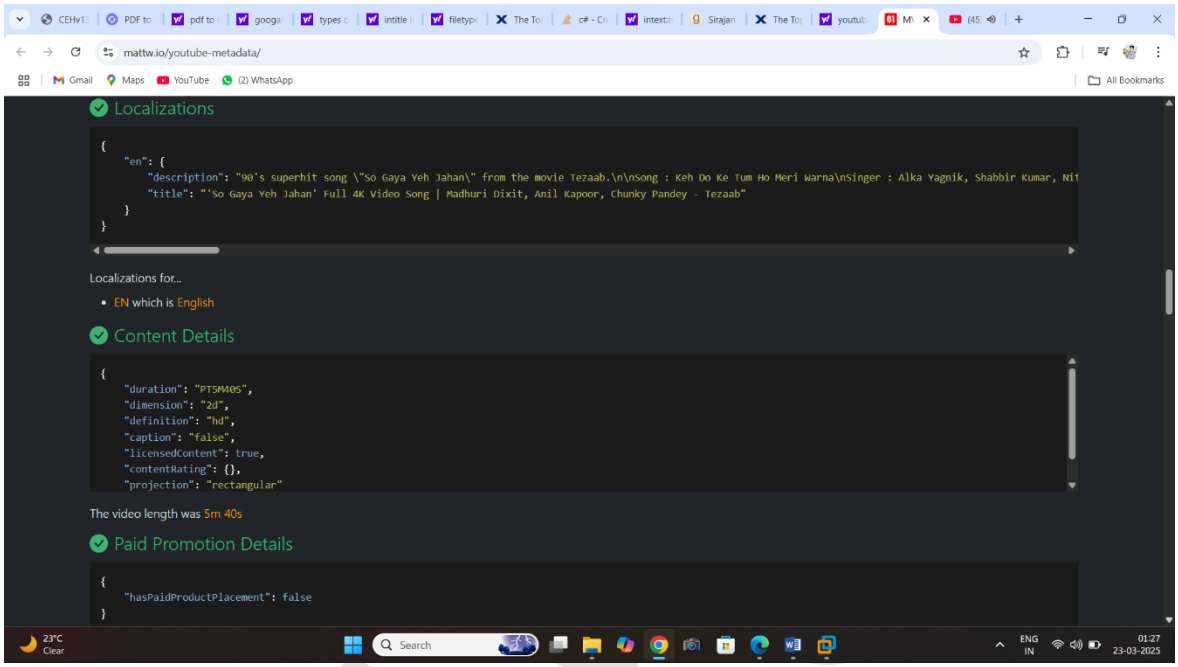






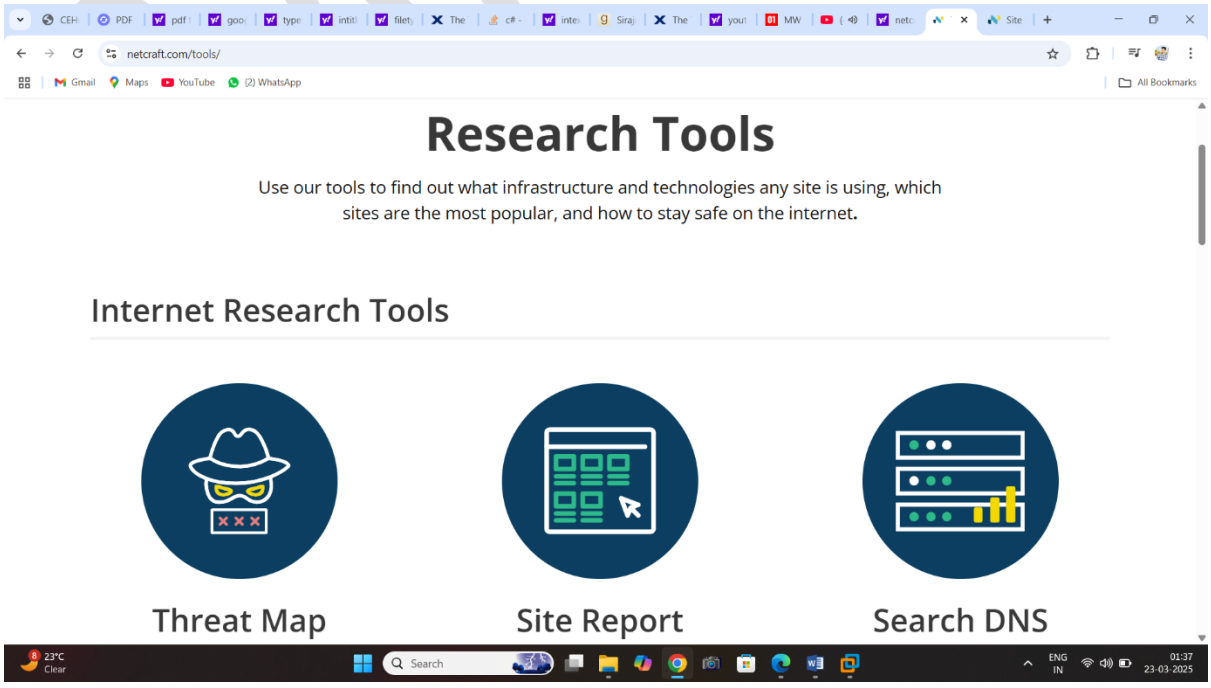
Discription: Quickly gather all the metadata about a video, playlist, or channel from the YouTube API. Reverse image search

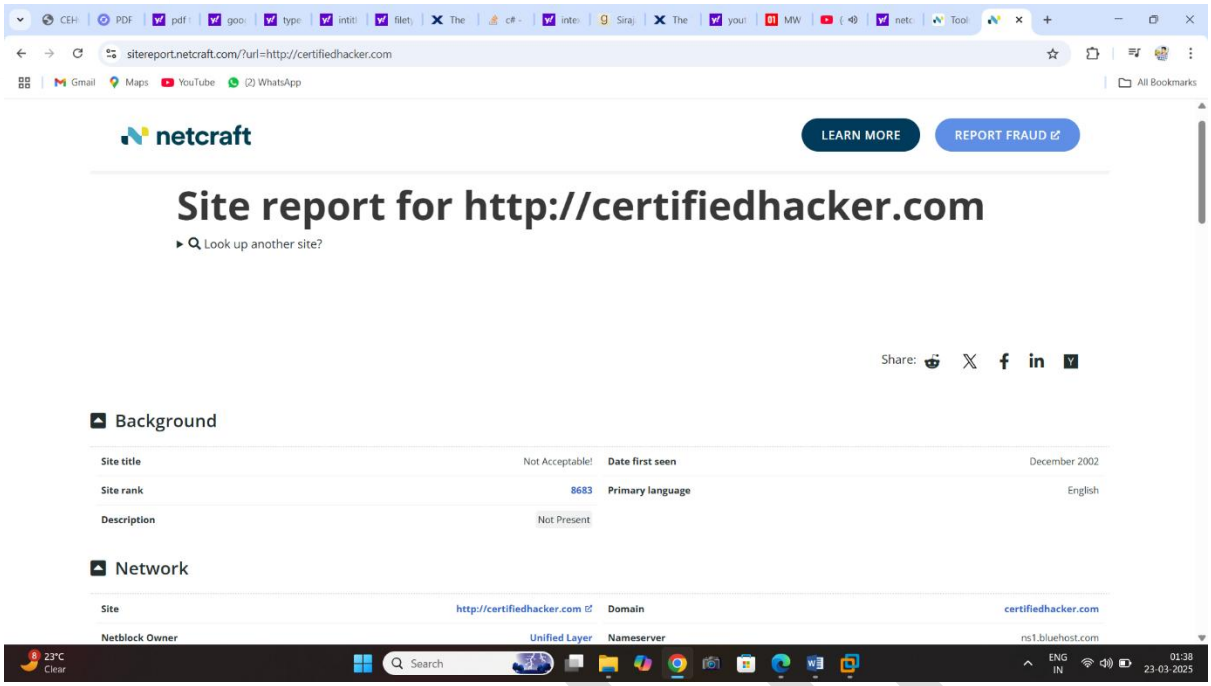
thumbnails, geolocate in google maps, and translate ISO country and language

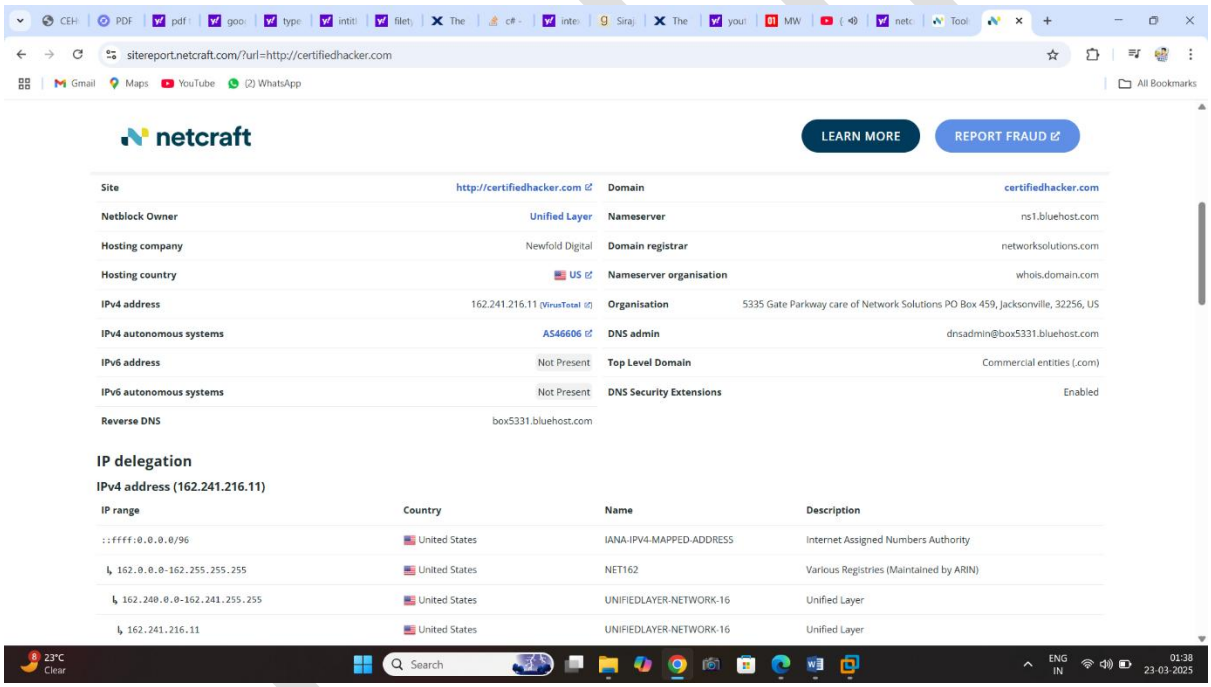


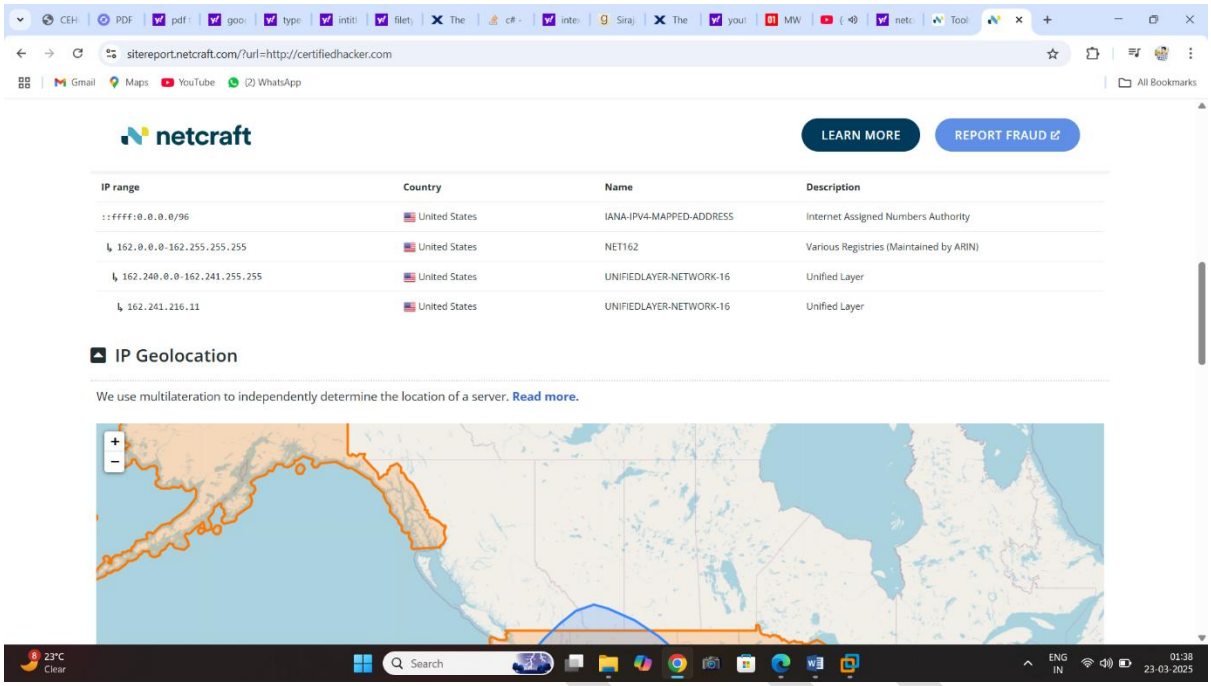
2 Netcraft:

Uses: for Domain ,ip add,Ipv6,server information




sitereport.netcraft.com/?url=http://certifiedhacker.com
netcraft
LEARN MORE
REPORT FRAUD
Site report for http://certifiedhacker.com
Look up another site?
Share:
Background
Site title
Not Acceptable!
Date first seen
December 2002
Site rank
8683
Primary language
English
Description
Not Present
Network
Site
http://certifiedhacker.com
Domain
certifiedhacker.com
Netblock Owner
Unified Layer
Nameserver
ns1.bluehost.com

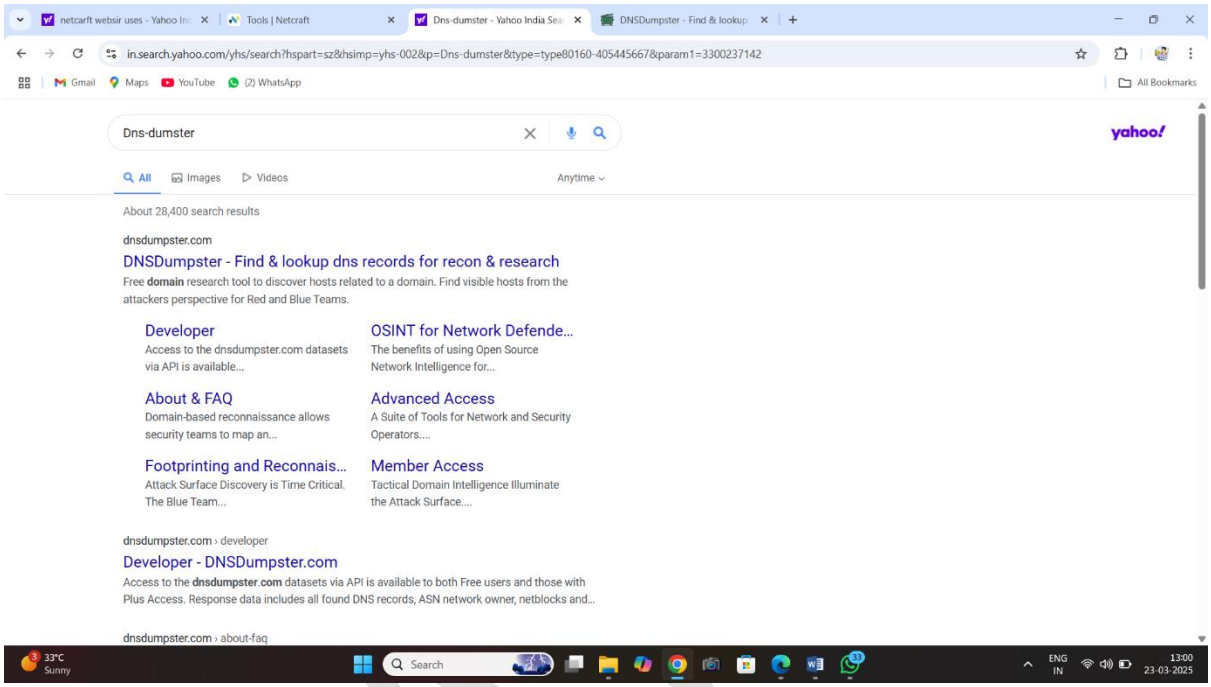

sitereport.netcraft.com/?url=http://certifiedhacker.com
netcraft
LEARN MORE
REPORT FRAUD
Site
http://certifiedhacker.com
Domain
certifiedhacker.com
Netblock Owner
Unified Layer
Nameserver
ns1.bluehost.com
Hosting company
Newfold Digital
Domain registrar
networksolutions.com
Hosting country
US
Nameserver organisation
whois.domain.com
IPv4 address
162.241.216.11
Organisation
5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US
IPv4 autonomous systems
AS46606
DNS admin
dnsadmin@box5331.bluehost.com
IPv6 address
Not Present
Top Level Domain
Commercial entities (.com)
IPv6 autonomous systems
Not Present
DNS Security Extensions
Enabled
Reverse DNS
box5331.bluehost.com
IP delegation
IPv4 address (162.241.216.11)
IP range
Country
Name
Description
::ffff:0.0.0.0/96
United States
IANA-IPV4-MAPPED-ADDRESS
Internet Assigned Numbers Authority
162.0.0.0-162.255.255.255
United States
NET162
Various Registries (Maintained by ARIN)
162.240.0.0-162.241.255.255
United States
UNIFIEDLAYER-NETWORK-16
Unified Layer
162.241.216.11
United States
UNIFIEDLAYER-NETWORK-16
Unified Layer

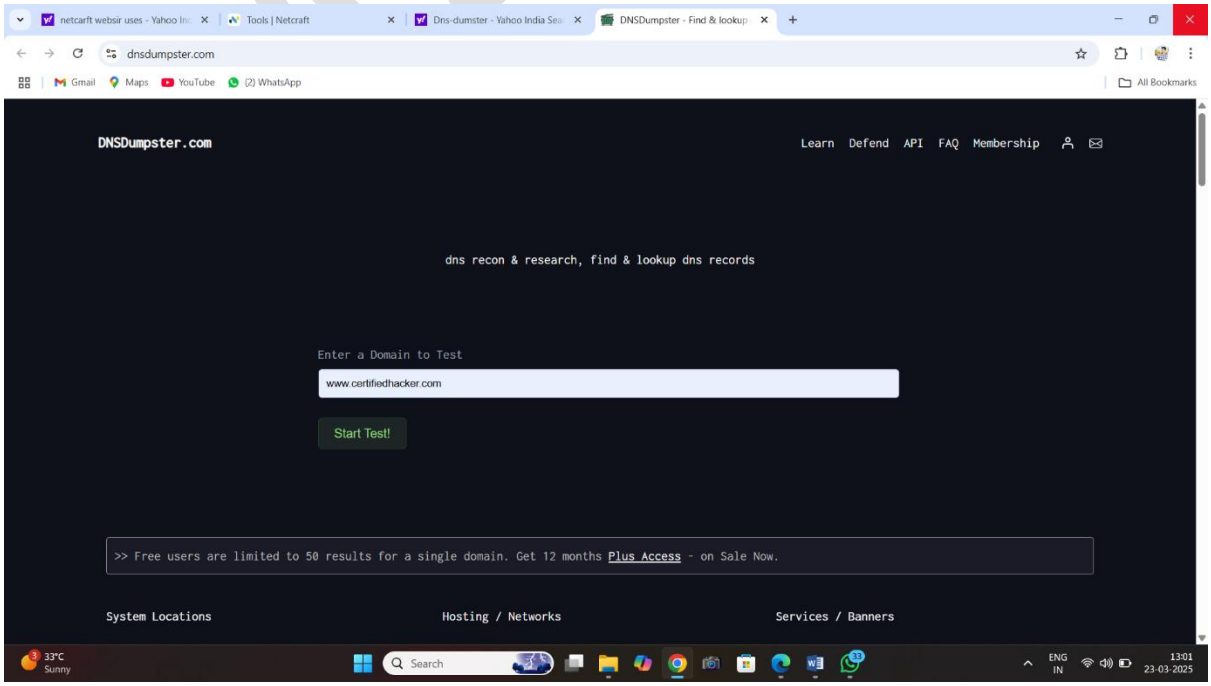


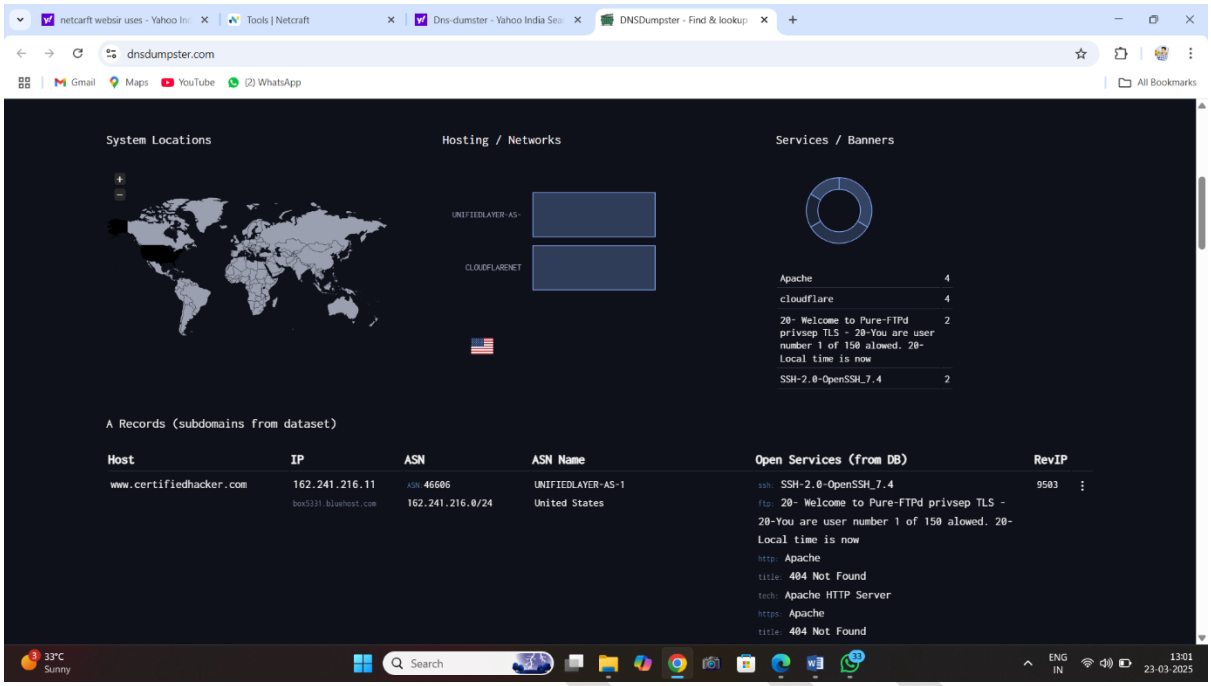
Discription Use our tools to find out what infrastructure and technologies any site is using, which sites are the most popular, and how to stay safe on the internet. View Netcraft's detection and countermeasures

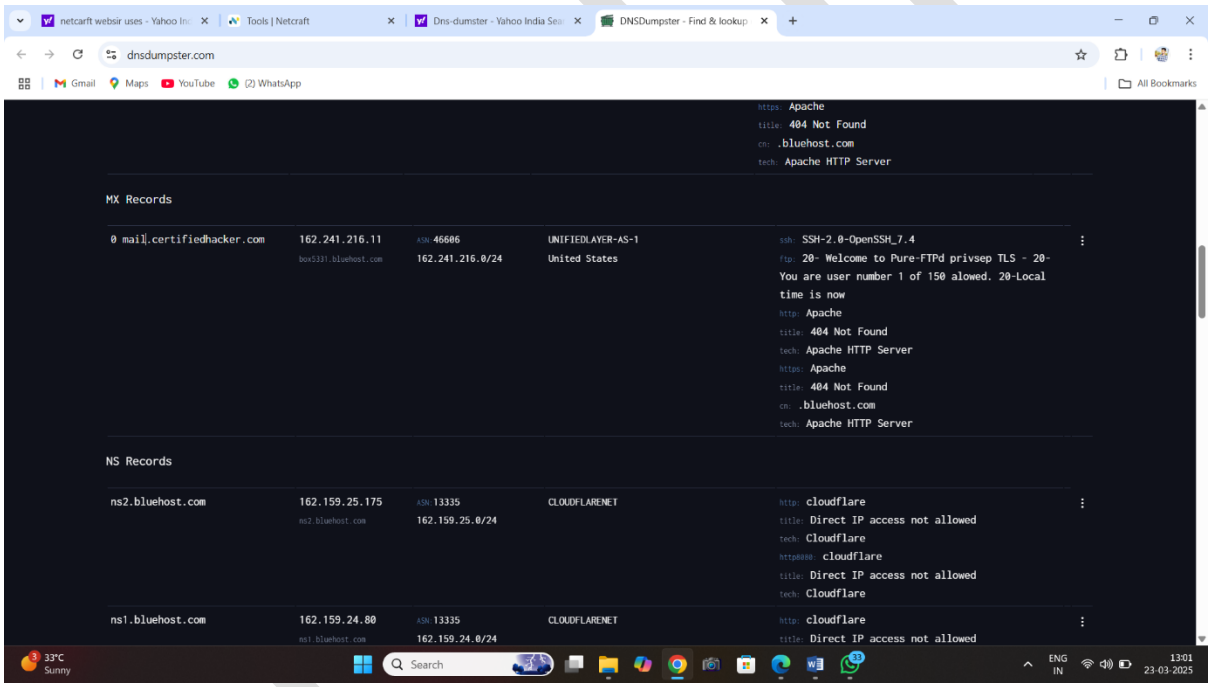
3 DNS-Dumster

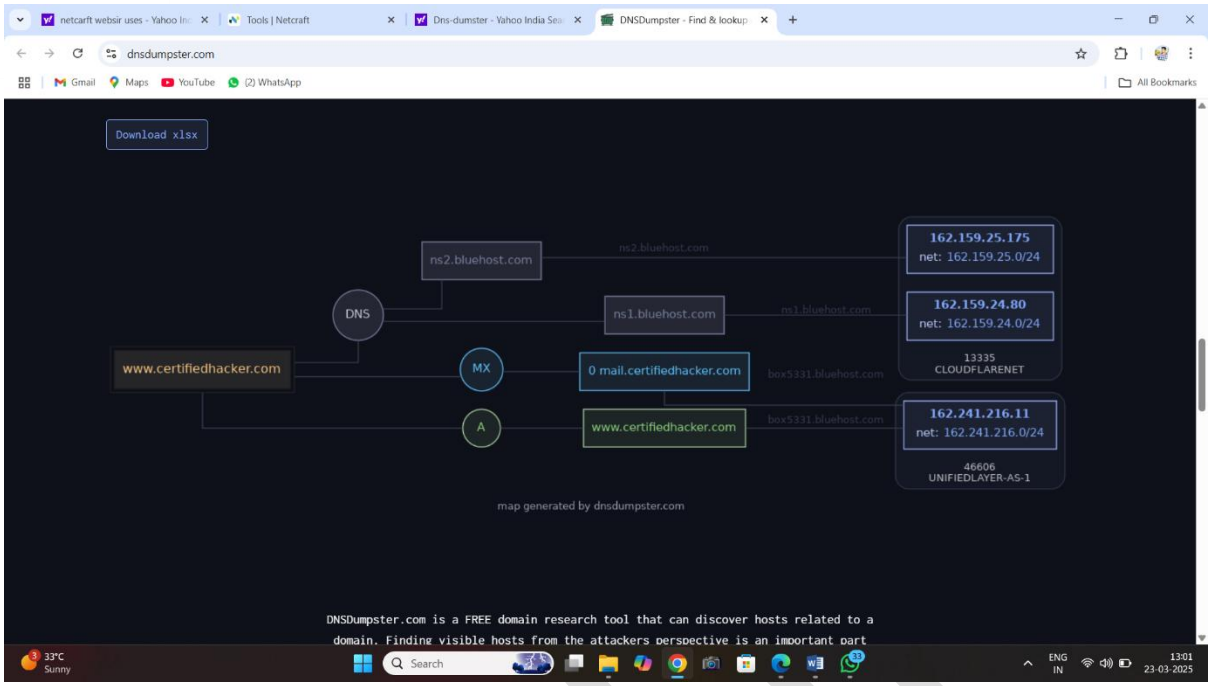
Uses: this website are uses for sub domain information





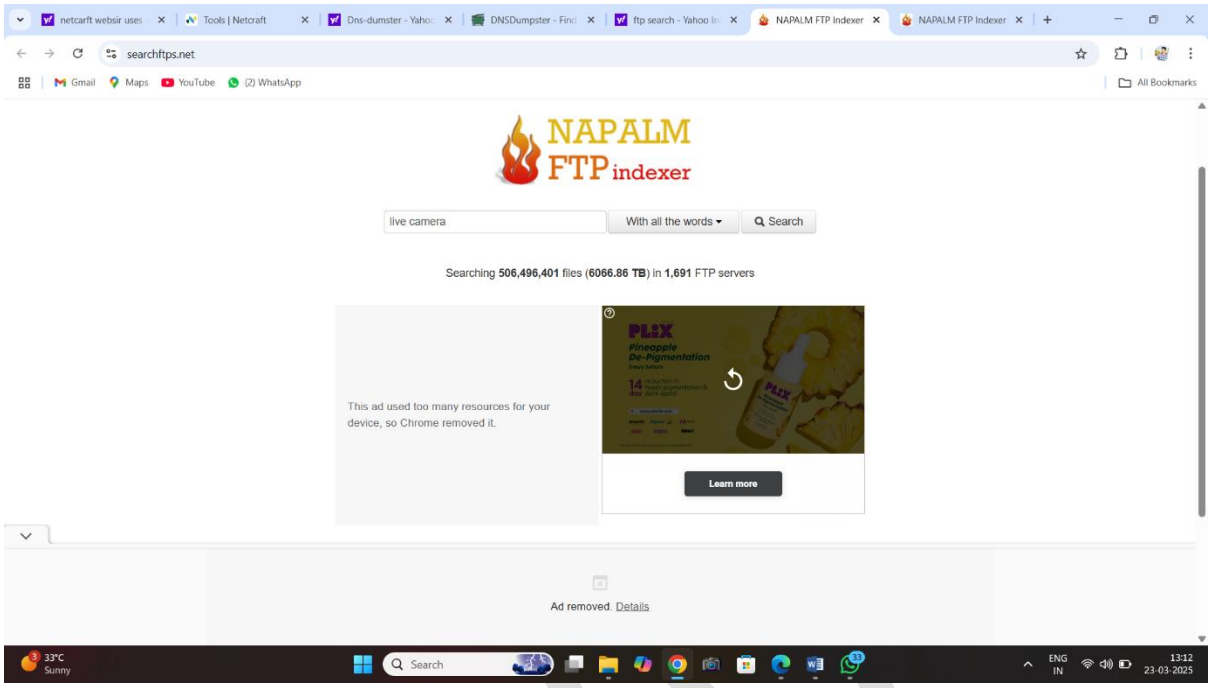

dnsdumpster.com
System Locations
Hosting / Networks
Services / Banners
UNIFIEDLAYER-AS-
CLOUDFLARENET
Apache 4
cloudflare 4
20- Welcome to Pure-FTPd privsep TLS - 20-You are user number 1 of 150 alowed. 20-Local time is now 2
SSH-2.0-OpenSSH_7.4 2
A Records (subdomains from dataset)
Host
IP
ASN
ASN Name
Open Services (from DB)
RevIP
www.certifiedhacker.com
162.241.216.11
box5331.bluehost.com
ASN 46606
162.241.216.0/24
UNIFIEDLAYER-AS-1
United States
ssh: SSH-2.0-OpenSSH_7.4
ftp: 20- Welcome to Pure-FTPd privsep TLS - 20-You are user number 1 of 150 alowed. 20-Local time is now
http: Apache
title: 404 Not Found
tech: Apache HTTP Server
https: Apache
title: 404 Not Found
9503

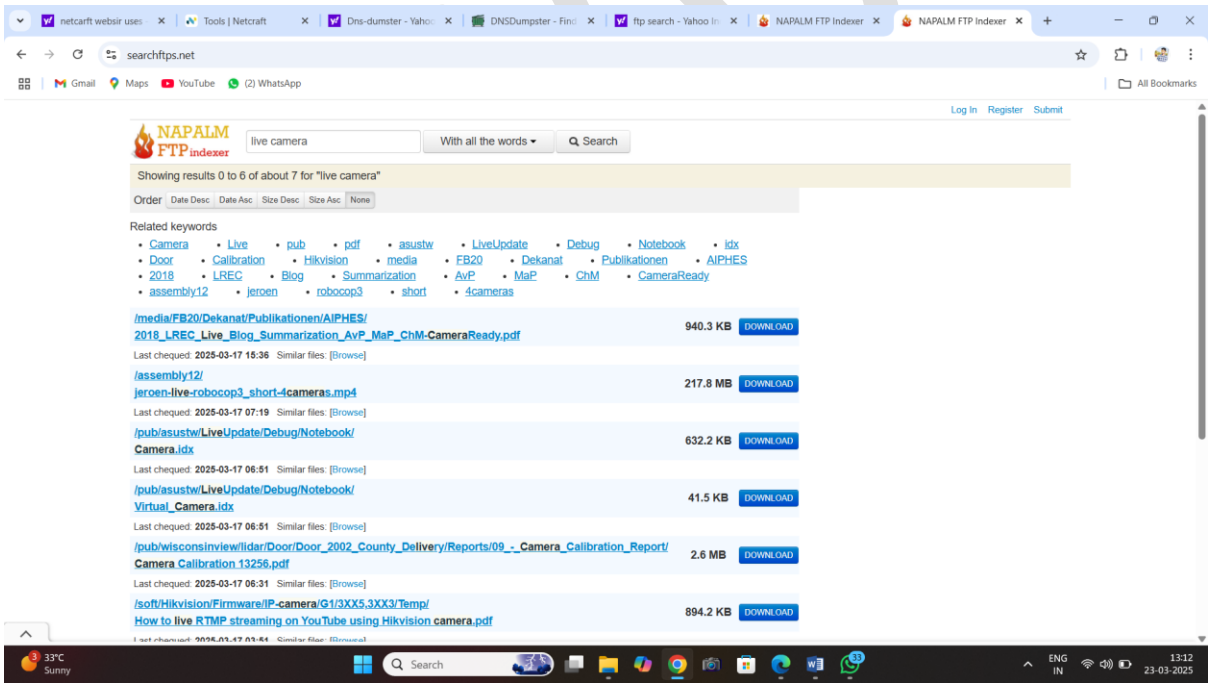

dnsdumpster.com
https: Apache
title: 404 Not Found
cn: .bluehost.com
tech: Apache HTTP Server
MX Records
0 mail.certifiedhacker.com
162.241.216.11
box5331.bluehost.com
ASN 46606
162.241.216.0/24
UNIFIEDLAYER-AS-1
United States
ssh: SSH-2.0-OpenSSH_7.4
ftp: 20- Welcome to Pure-FTPd privsep TLS - 20-You are user number 1 of 150 alowed. 20-Local time is now
http: Apache
title: 404 Not Found
tech: Apache HTTP Server
https: Apache
title: 404 Not Found
cn: .bluehost.com
tech: Apache HTTP Server
NS Records
ns2.bluehost.com
162.159.25.175
ns2.bluehost.com
ASN 13335
162.159.25.0/24
CLOUDFLARENET
http: cloudflare
title: Direct IP access not allowed
tech: Cloudflare
http8080: cloudflare
title: Direct IP access not allowed
tech: Cloudflare
ns1.bluehost.com
162.159.24.80
ns1.bluehost.com
ASN 13335
162.159.24.0/24
CLOUDFLARENET
http: cloudflare
title: Direct IP access not allowed



Discription : DNSDumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process

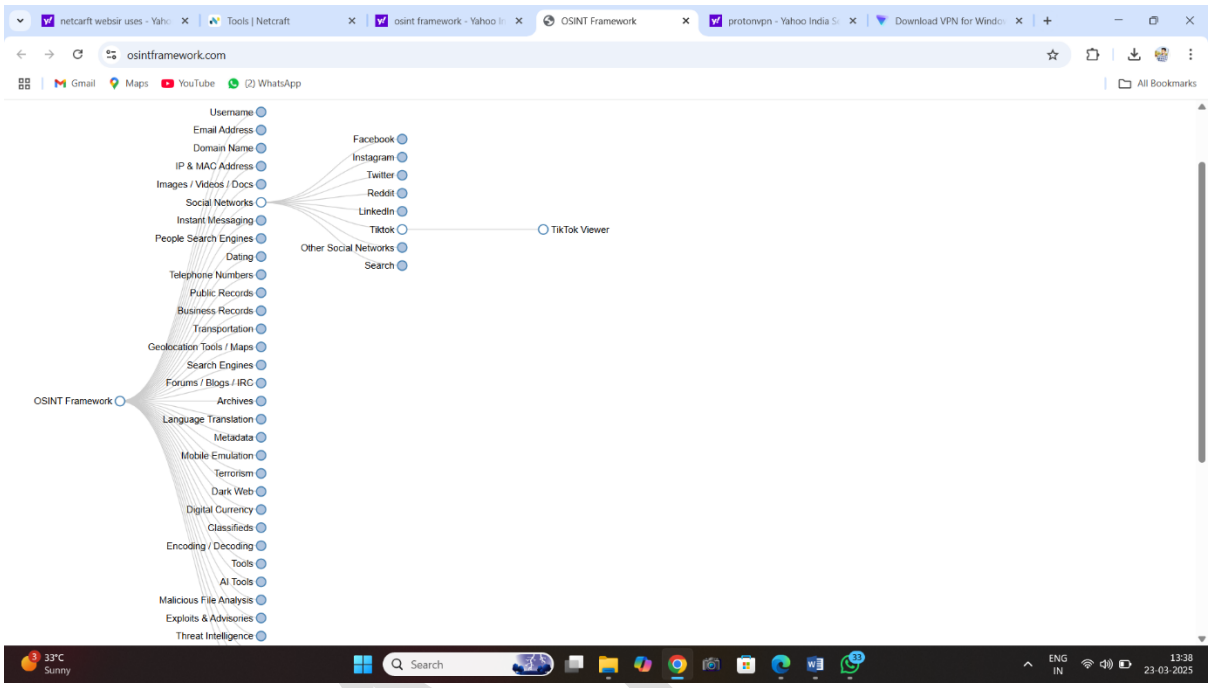
NAPALM FTP Indexer





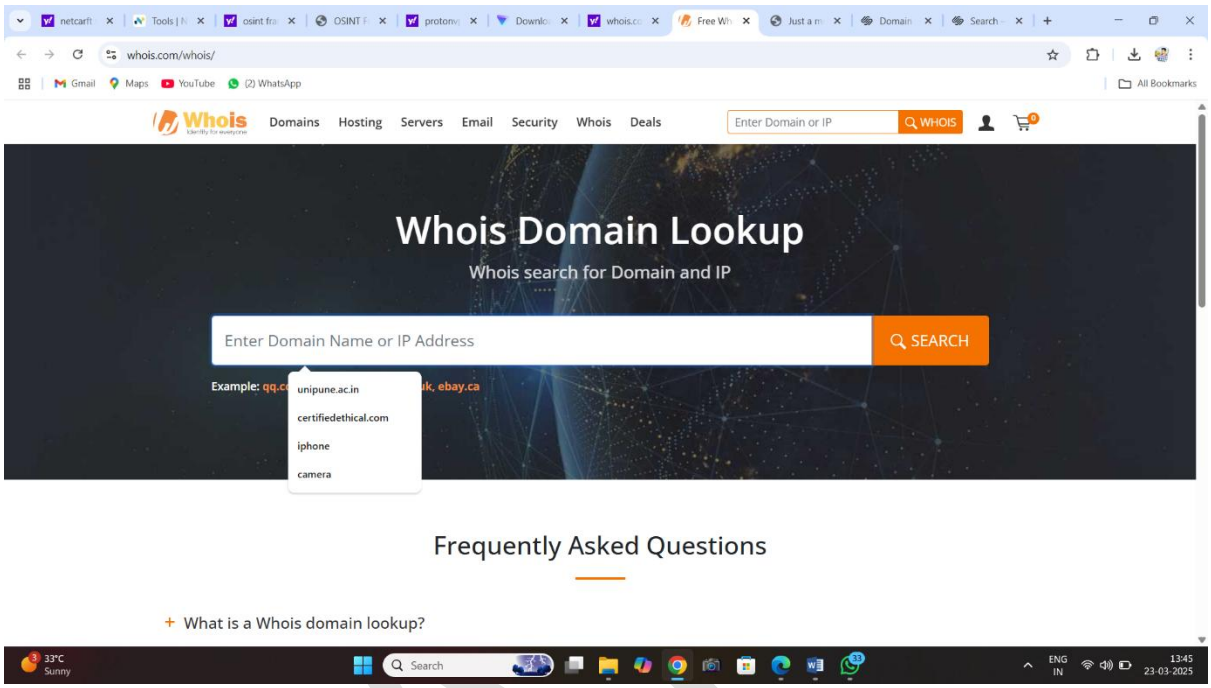
Discription: NAPALM FTP Indexer lets you search and download files located on public FTP servers. The most advanced FTP Search Engine service maintained by members.

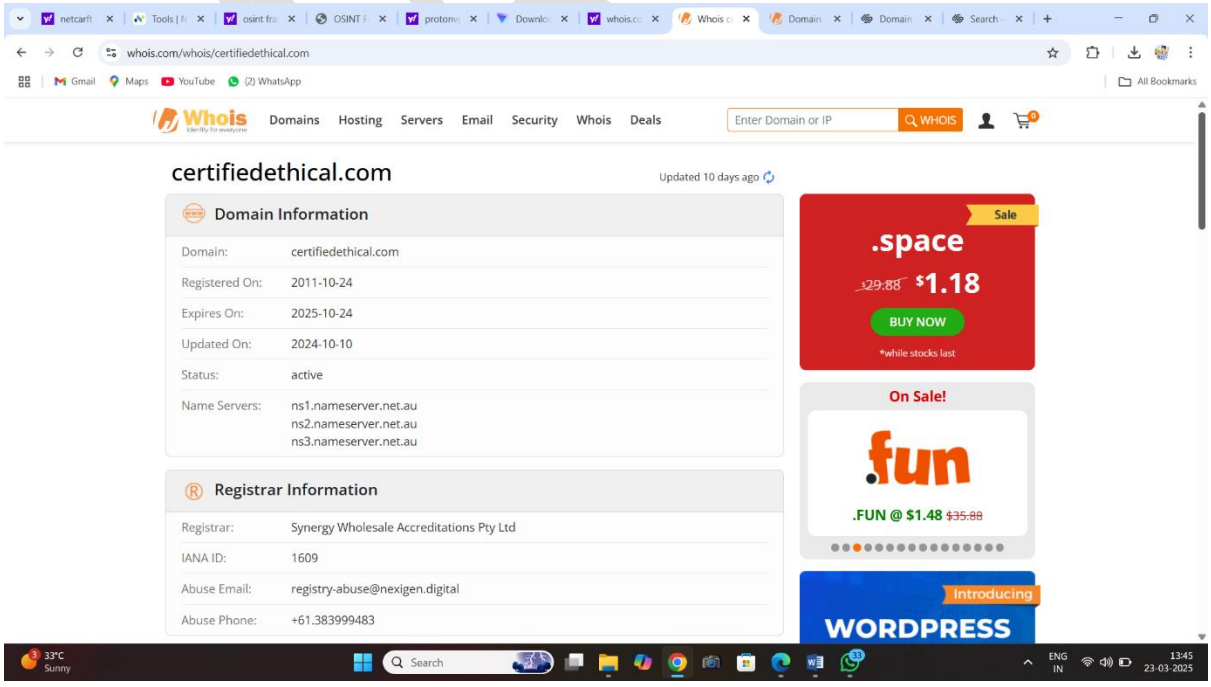
OSINT FRAMWORK

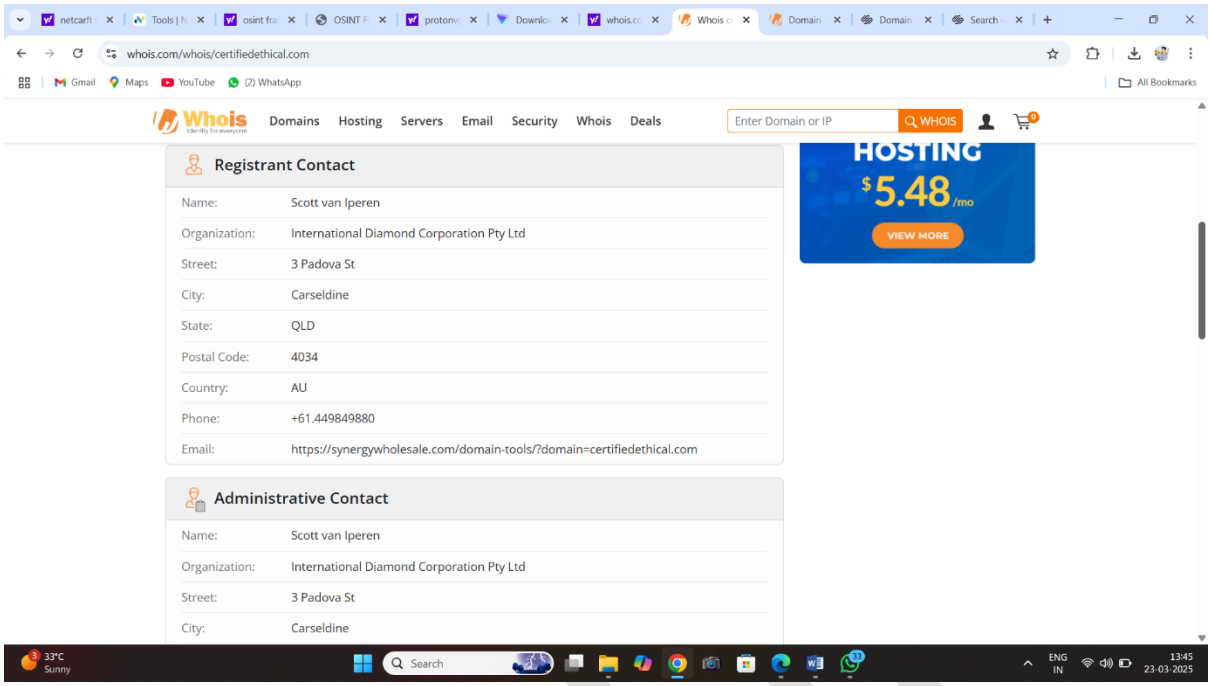


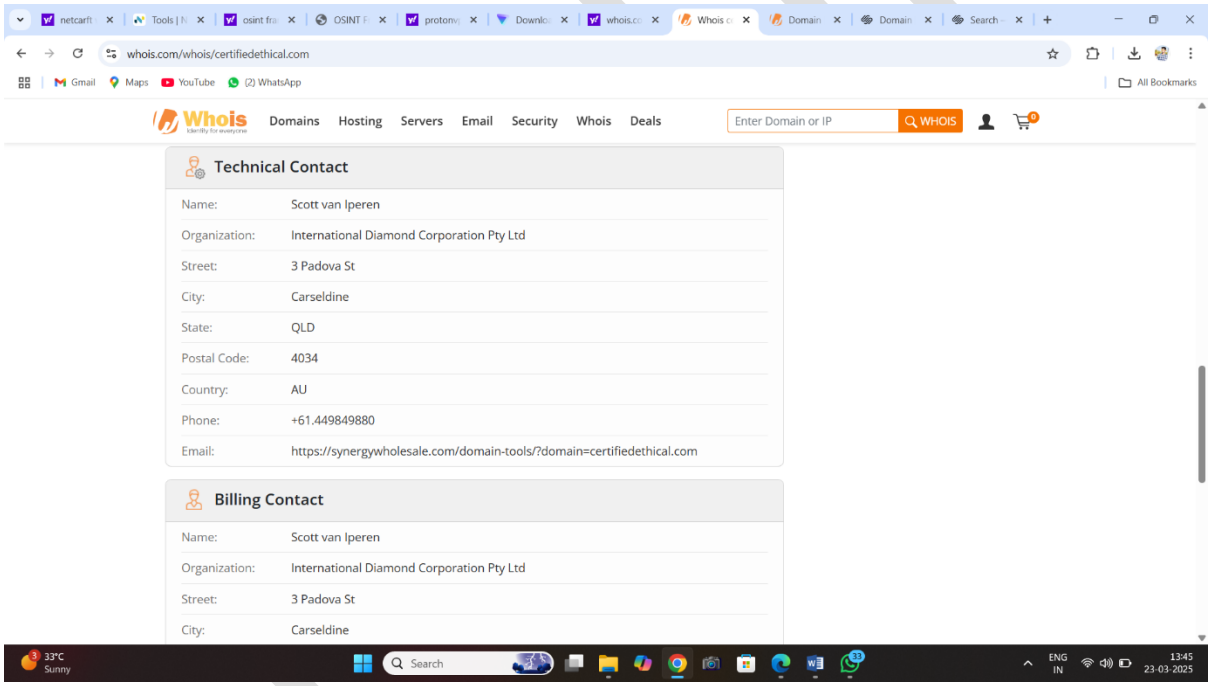
Discrption: OSINT Framework is a website that helps people find free OSINT resources and tools for various purposes. It covers topics such as threat intelligence, exploits, malware analysis, AI, encryption,

Web site: Who is .com









Description: Whois.com allows you to trace the ownership and tenure of a domain name or an IP address. You can also find available domains, register new domains, and protect your privacy with Whois.com.

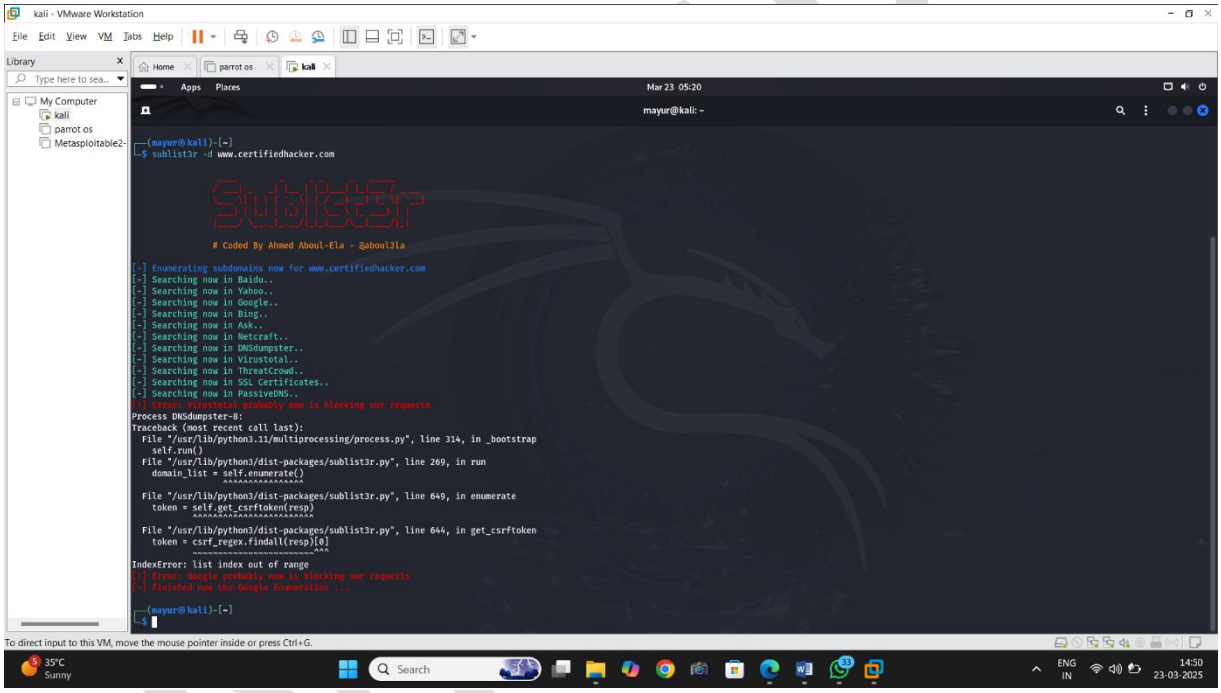
3 Task Fotprinting through Social media networking

1 sublister3r

Uses: (for use sub Domain information)

Work: sublister-d www.certifiedhcker.com

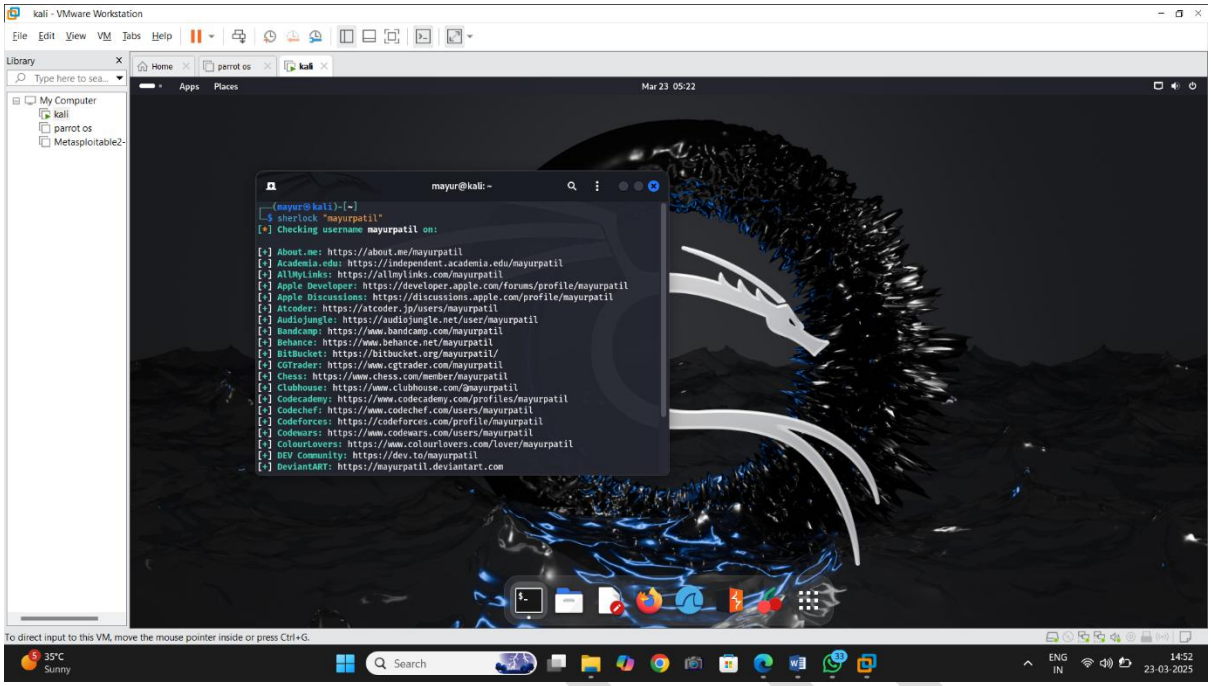
tli

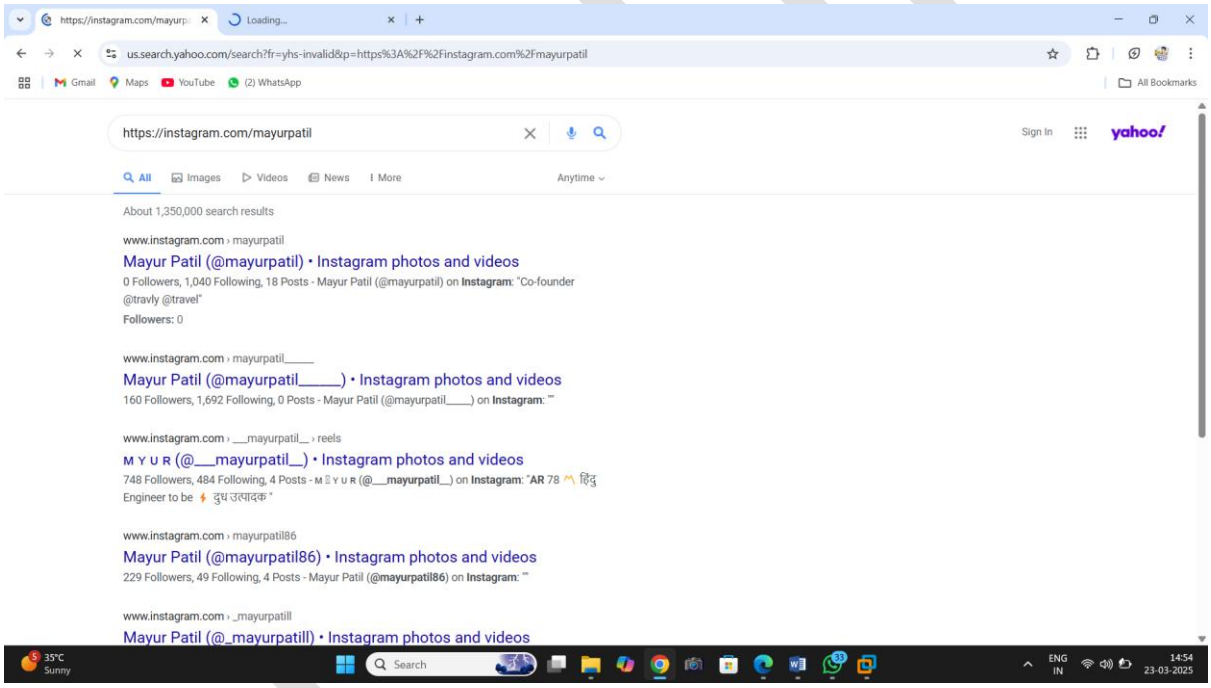


Sherlock

Command: Sherlock”domain name”

Uses: for any one social media information



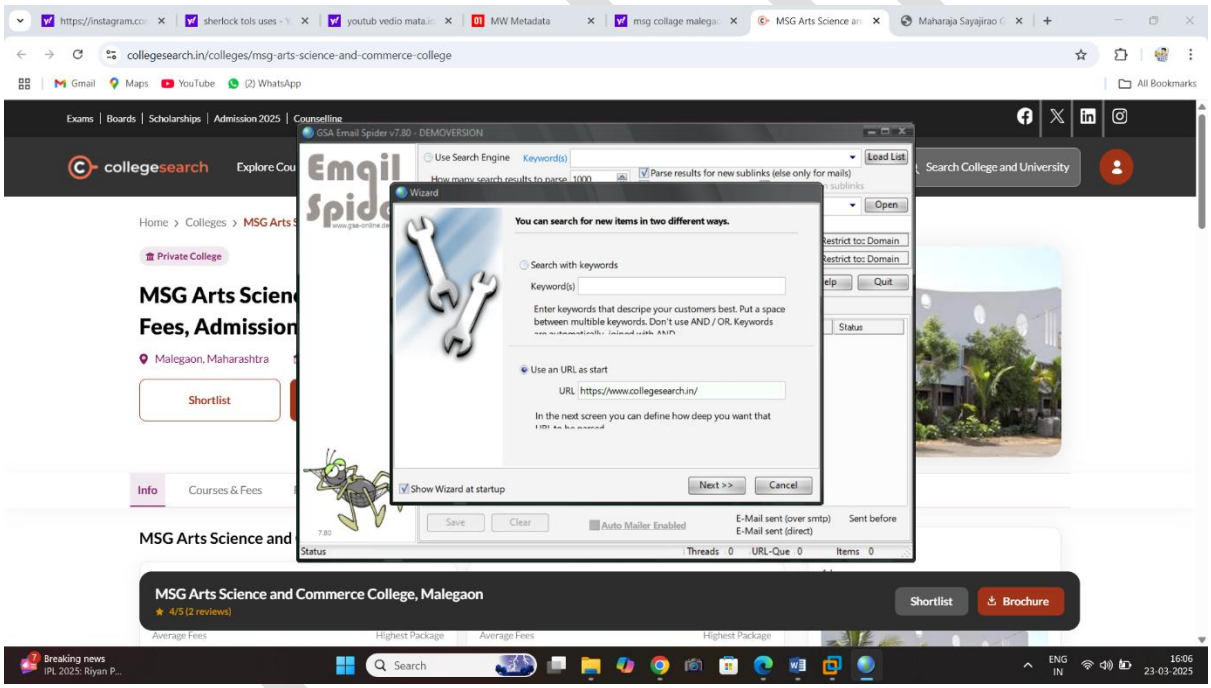


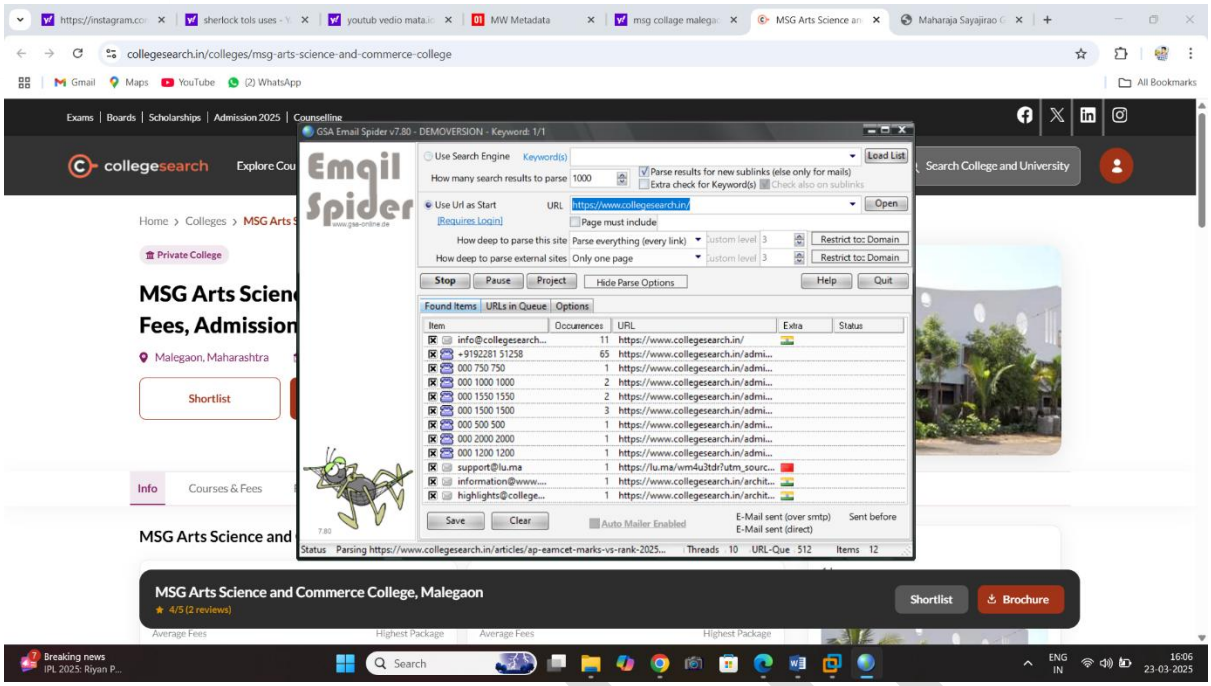
Discription:

Sherlock is a free and open-source tool available on **GitHub**. This tool is free you can download it from Github and can use it for free of cost. Sherlock is used to finding usernames on social

media on 300 sites. As you know many users register themselves on social media platforms using their own name. Suppose we need to find someone on any social media website such as Facebook, Instagram etc.

Task4 Email Footprinting Using GSA Email spider





DNS Footprintig

The domain name system, or DNS, is a global system

responsible for mapping human-readable hostnames

to their corresponding Internet Protocol (IP)

addresses. For example, if you want to access a

website using a domain name like example.com, that

domain name must point to a valid IP address

: What are DNS record types?

DNS record types are records that provide important

information about a hostname or domain. These

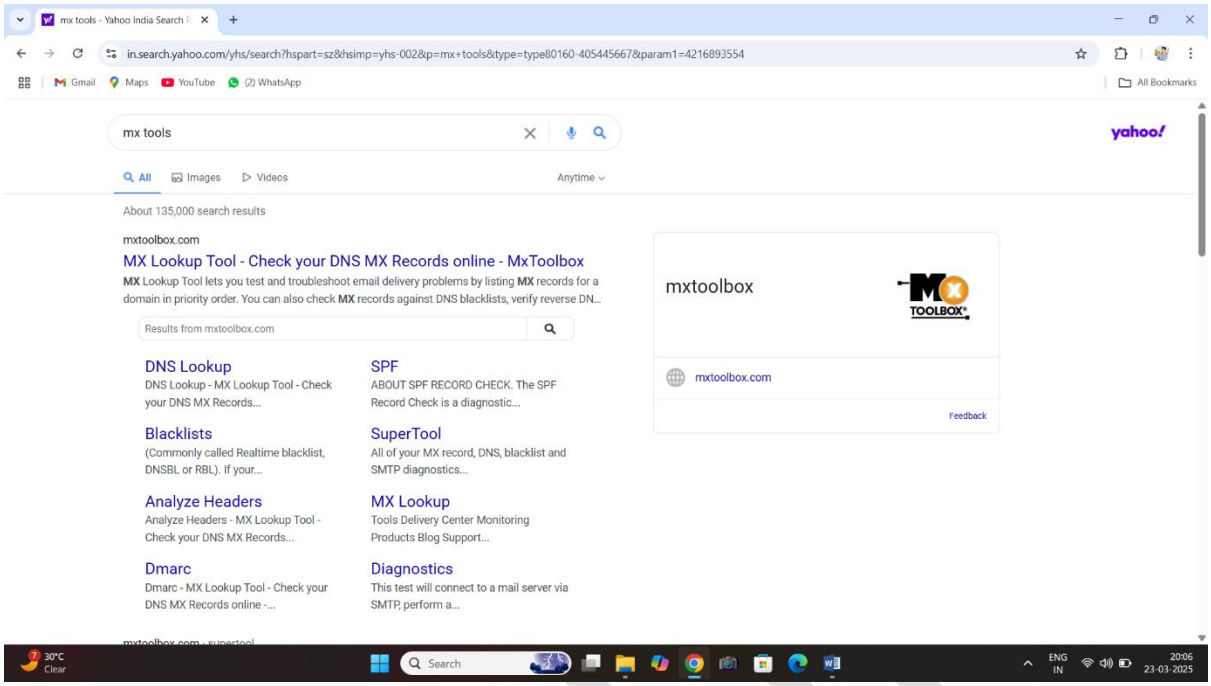
records include the current IP address for a domain.

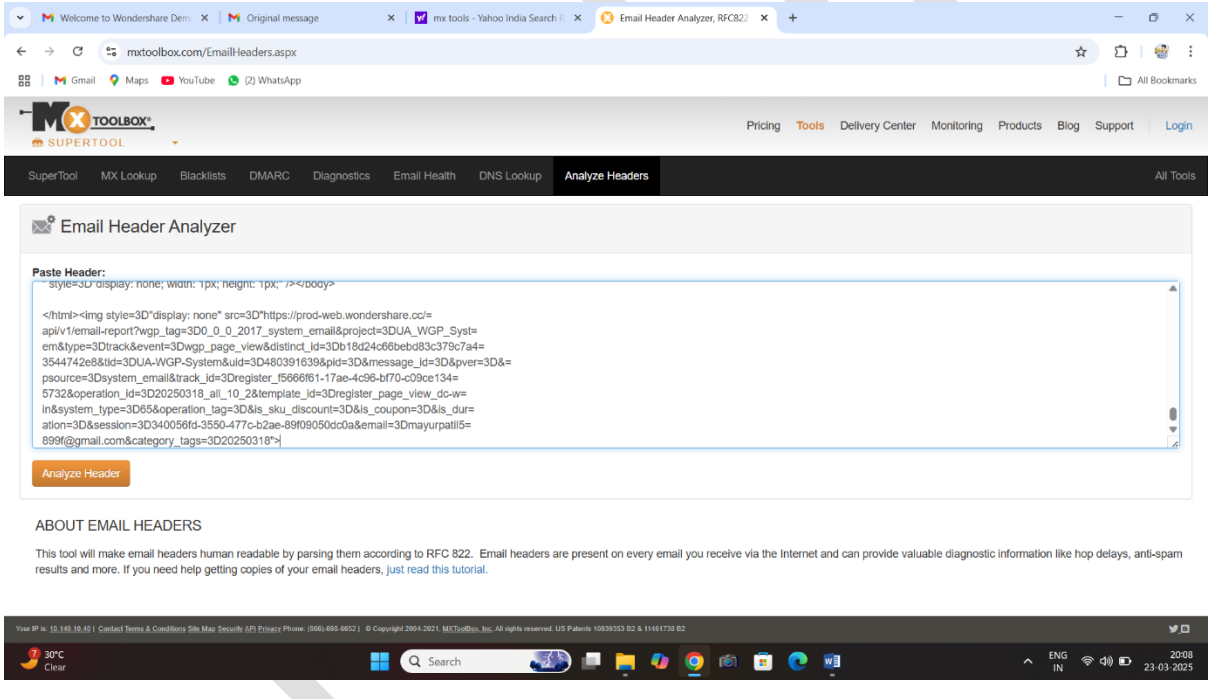
Also, DNS records are stored in text files (zone files)

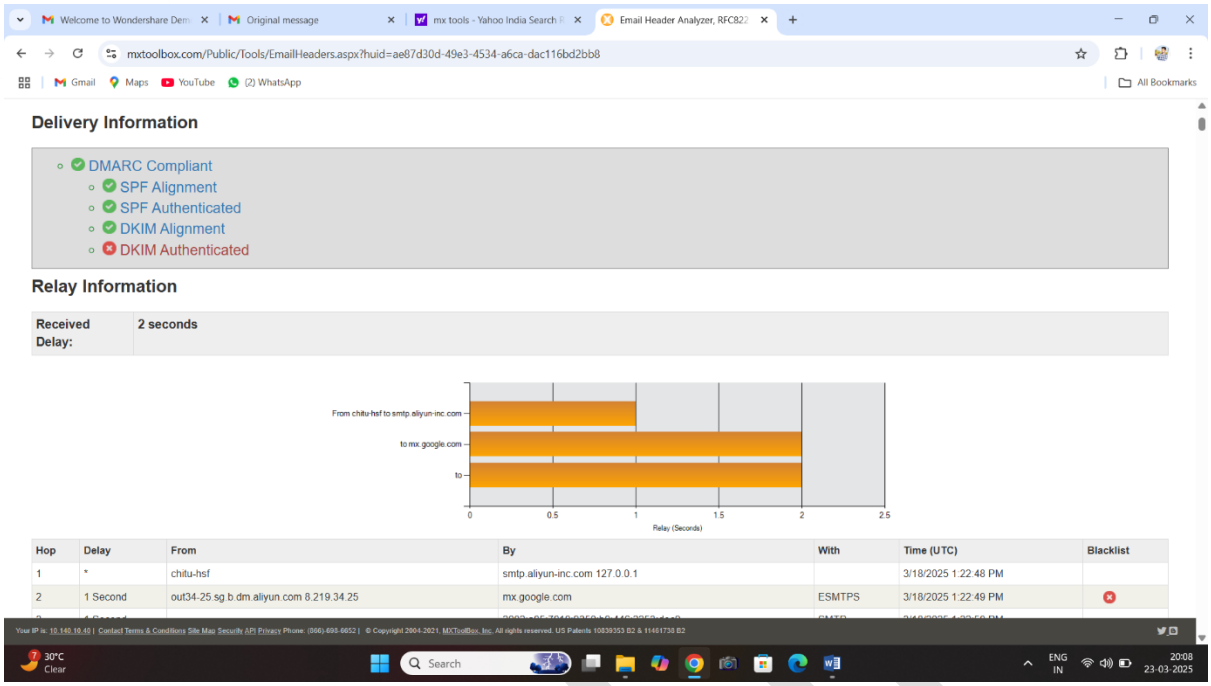
on the authoritative DNS server. The content of a DNS

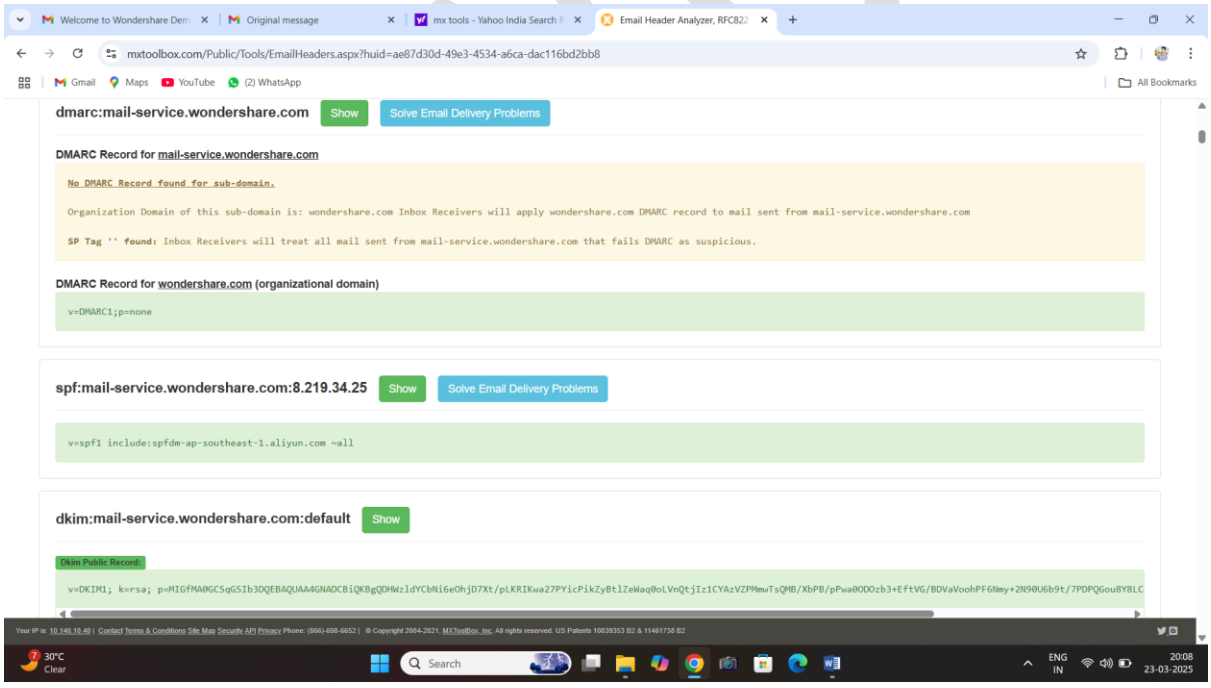
record file is a string with special commands that the DNS server understands.

MX Tool box


mx tools - Yahoo India Search
in.search.yahoo.com/yhs/search?hspart=sz&hsimp=yhs-002&p=mx+tools&type=type80160-405445667&param1=4216893554
mx tools
yahoo!
All
Images
Videos
Anytime
About 135,000 search results
mxtoolbox.com
MX Lookup Tool - Check your DNS MX Records online - MxToolbox
MX Lookup Tool lets you test and troubleshoot email delivery problems by listing MX records for a domain in priority order. You can also check MX records against DNS blacklists, verify reverse DN...
Results from mxtoolbox.com
DNS Lookup
DNS Lookup - MX Lookup Tool - Check your DNS MX Records...
SPF
ABOUT SPF RECORD CHECK. The SPF Record Check is a diagnostic...
Blacklists
(Commonly called Realtime blacklist, DNSBL or RBL). If your...
SuperTool
All of your MX record, DNS, blacklist and SMTP diagnostics...
Analyze Headers
Analyze Headers - MX Lookup Tool - Check your DNS MX Records...
MX Lookup
Tools Delivery Center Monitoring Products Blog Support...
Dmarc
Dmarc - MX Lookup Tool - Check your DNS MX Records online -...
Diagnostics
This test will connect to a mail server via SMTP, perform a...
mxtoolbox
mxtoolbox.com
Feedback
30°C
Clear
Search
ENG
IN
20:06
23-03-2025

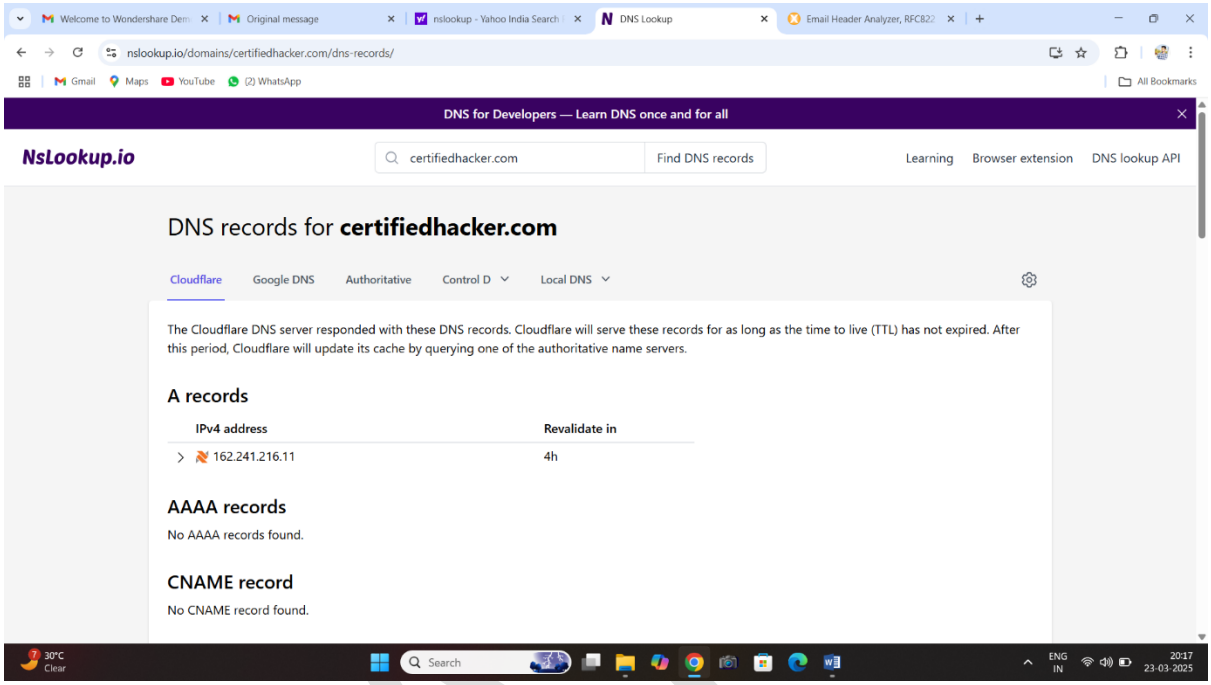

Welcome to Wondershare Demo
Original message
mx tools - Yahoo India Search
Email Header Analyzer, RFC822
mxtoolbox.com/EmailHeaders.aspx
TOOLBOX
SUPERTOOL
Pricing
Tools
Delivery Center
Monitoring
Products
Blog
Support
Login
SuperTool
MX Lookup
Blacklists
DMARC
Diagnostics
Email Health
DNS Lookup
Analyze Headers
All Tools
Email Header Analyzer
Paste Header:
style=3D"display: none; width: 1px; height: 1px;" /></body>
</html><img style=3D"display: none" src=3D"https://prod-web.wondershare.cc/=
api/v1/email-report?wgp_tag=3D0_0_0_2017_system_email&project=3DUA_WGP_Syst=
em&type=3Dtrack&event=3Dwgp_page_view&distinct_id=3Db18d24c66bebd83c379c7a4=
3544742e8&tid=3DUA-WGP-System&uid=3D4803916398pid=3D&message_id=3D&pver=3D&=
psource=3Dsystem_email&track_id=3Dregister_f5666f61-17ae-4c96-bf70-c09ce134=
5732&operation_id=3D20250318_all_10_2&template_id=3Dregister_page_view_dc-w=
in&system_type=3D65&operation_tag=3D&is_sku_discount=3D&is_coupon=3D&is_dur=
ation=3D&session=3D340056fd-3550-477c-b2ae-89f09050dc0a&email=3Dmayurpatil5=
899f@gmail.com&category_tags=3D20250318">
Analyze Header
ABOUT EMAIL HEADERS
This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.
30°C
Clear
Search
ENG
IN
20:08
23-03-2025





Discription: MX Lookup Tool lets you test and troubleshoot email delivery problems by listing MX records for a domain in priority order.

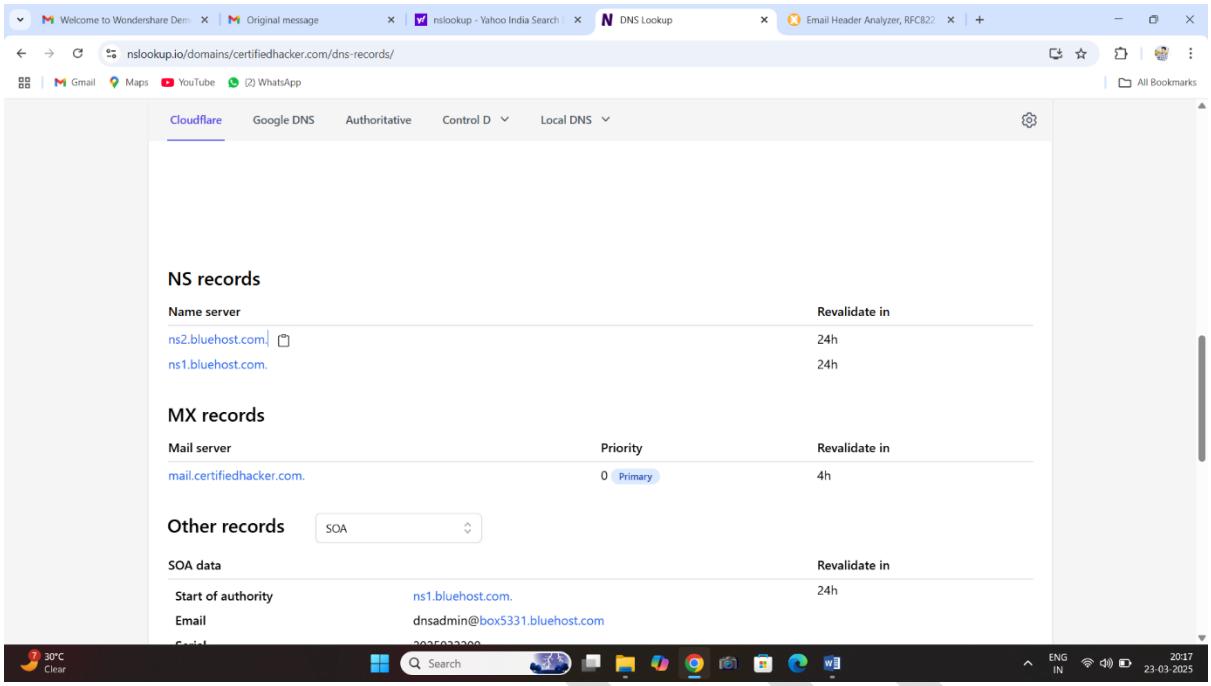
DNS Transefer zone



1 A Maps a domain to an IPv4 address.

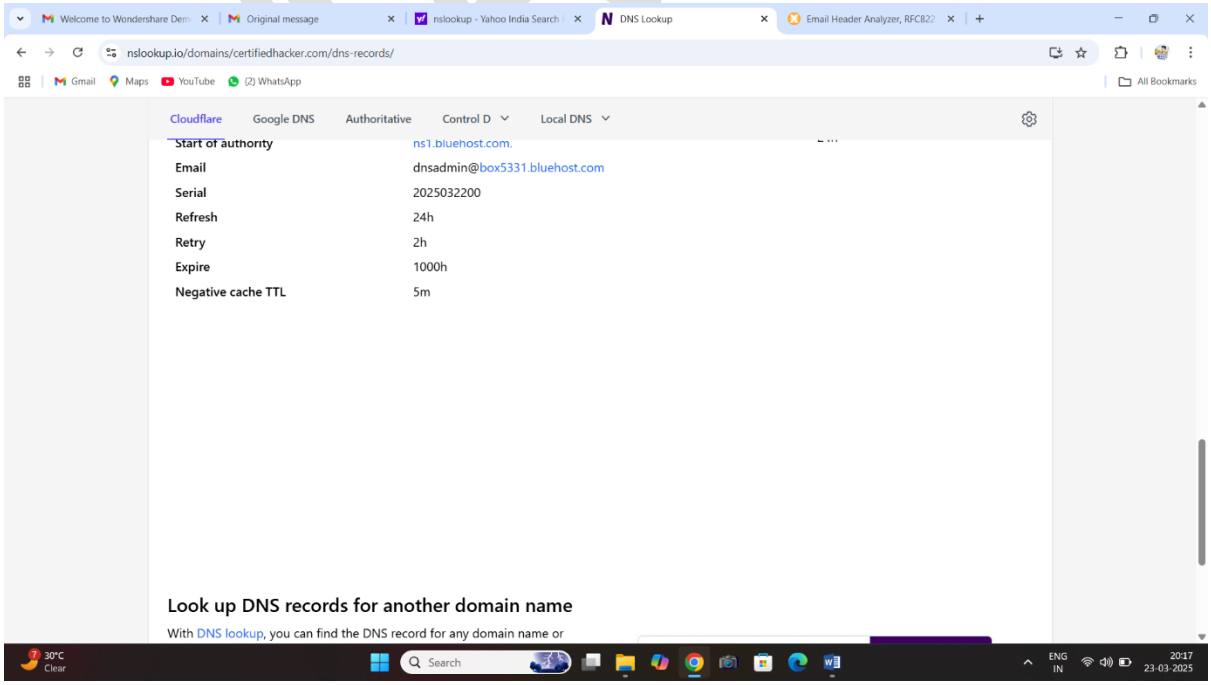
2 AAAA Maps a domain to an IPv6 address.

CNAME Aliases one domain name to another.



4 MX Directs email to mail servers.

5 NS Specifies the authoritative Name server for a domain.



6 SOA Provides important details about a

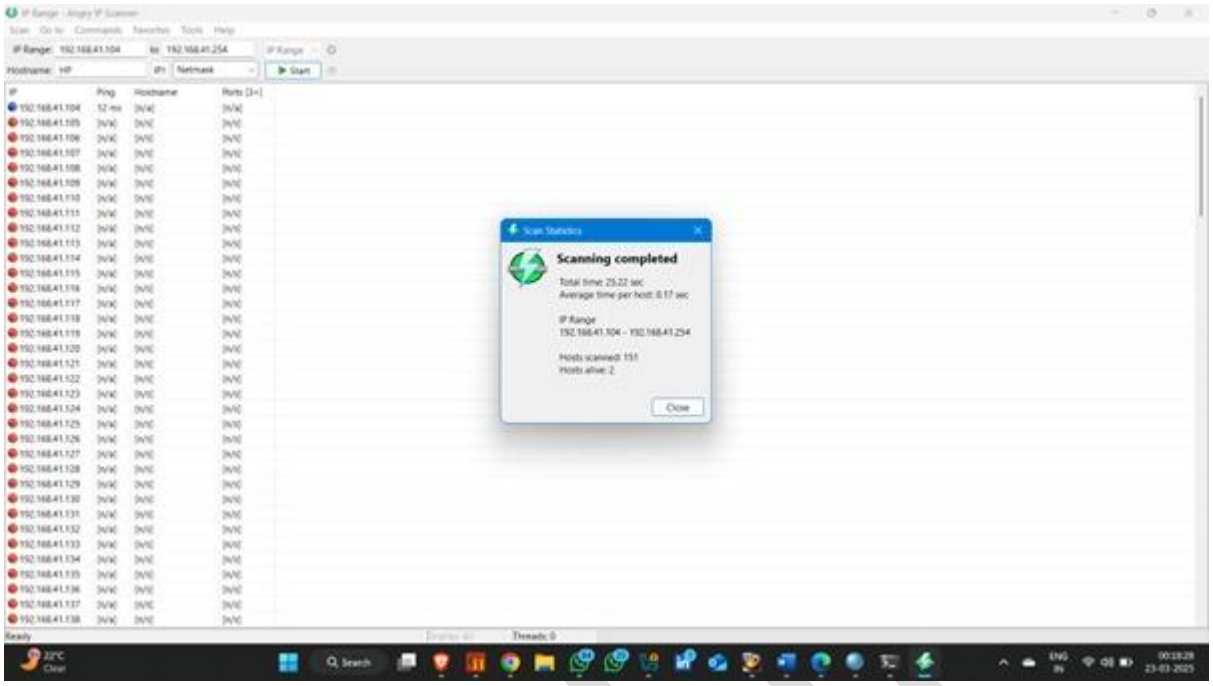
	DNS zone; required for every DNS
7 TXT	Stores text information, often used for verification.
8 SRV	Specifies a service location for

Traceroot command

Uses: `traceroute` command is used to trace the path that packets take from your machine to a destination on the internet or a specific network host

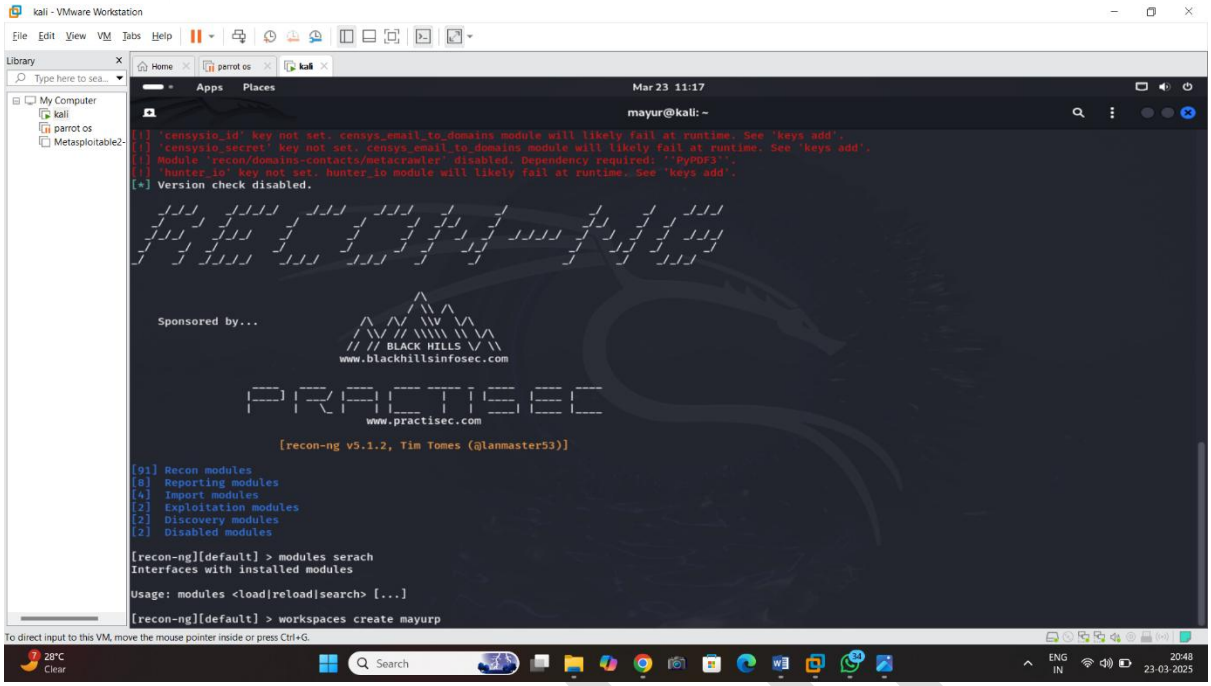
Angary Ip Scanner:

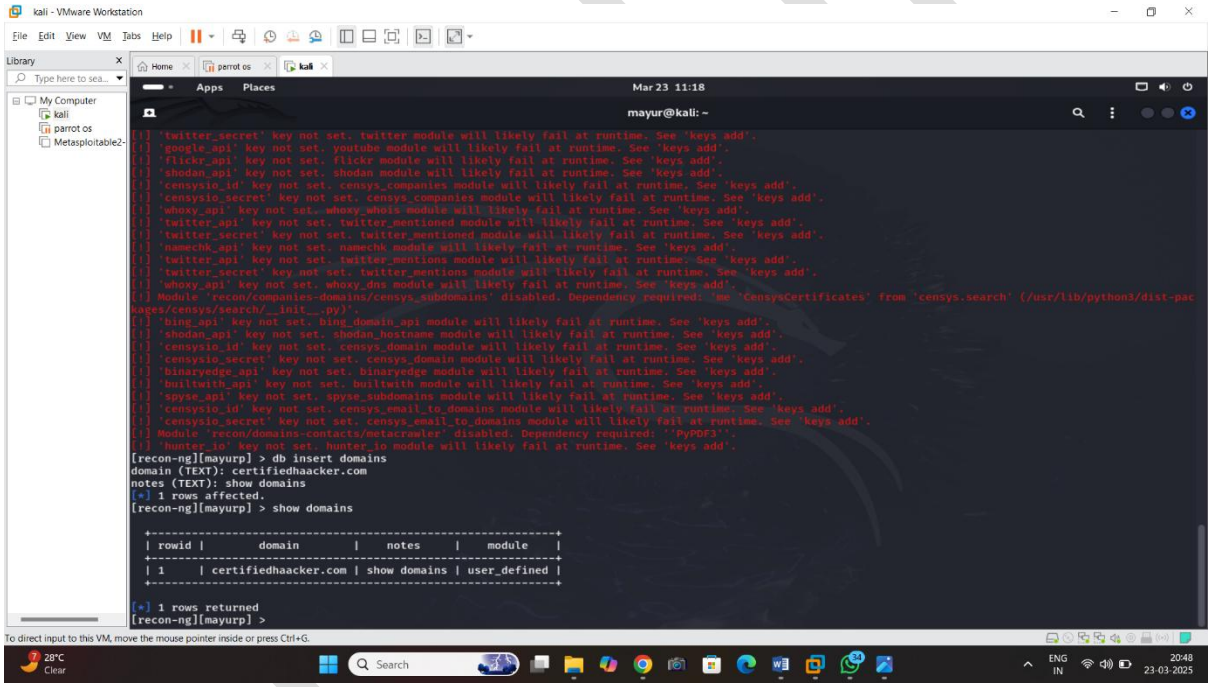
Uses: Angry IP Scanner is a popular, fast, and lightweight network scanning tool used to discover active devices in a local network or across IP ranges. It is often used for network reconnaissance, discovering devices, and gathering information about connected systems.

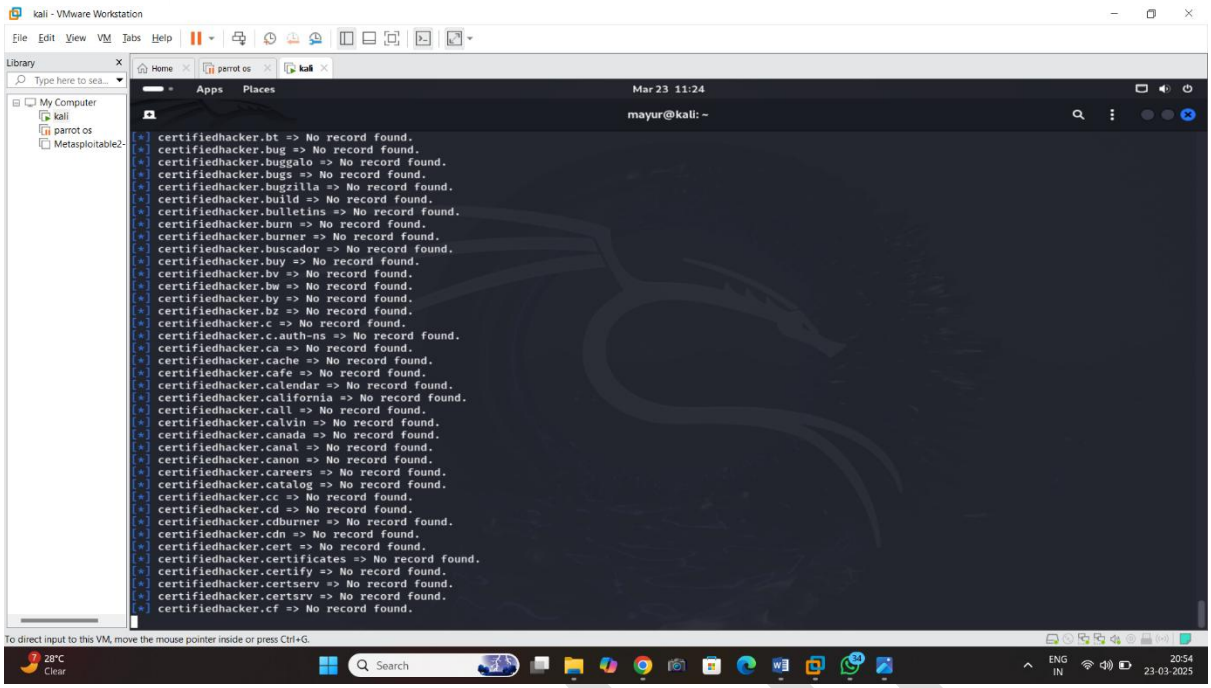


Task5 find the domain information using Recon-ng toolkit

Uses: Recon-ng is an open-source reconnaissance framework used primarily
for gathering intelligence on targets. Designed for security professionals, penetration testers, and ethical hackers, Recon-ng

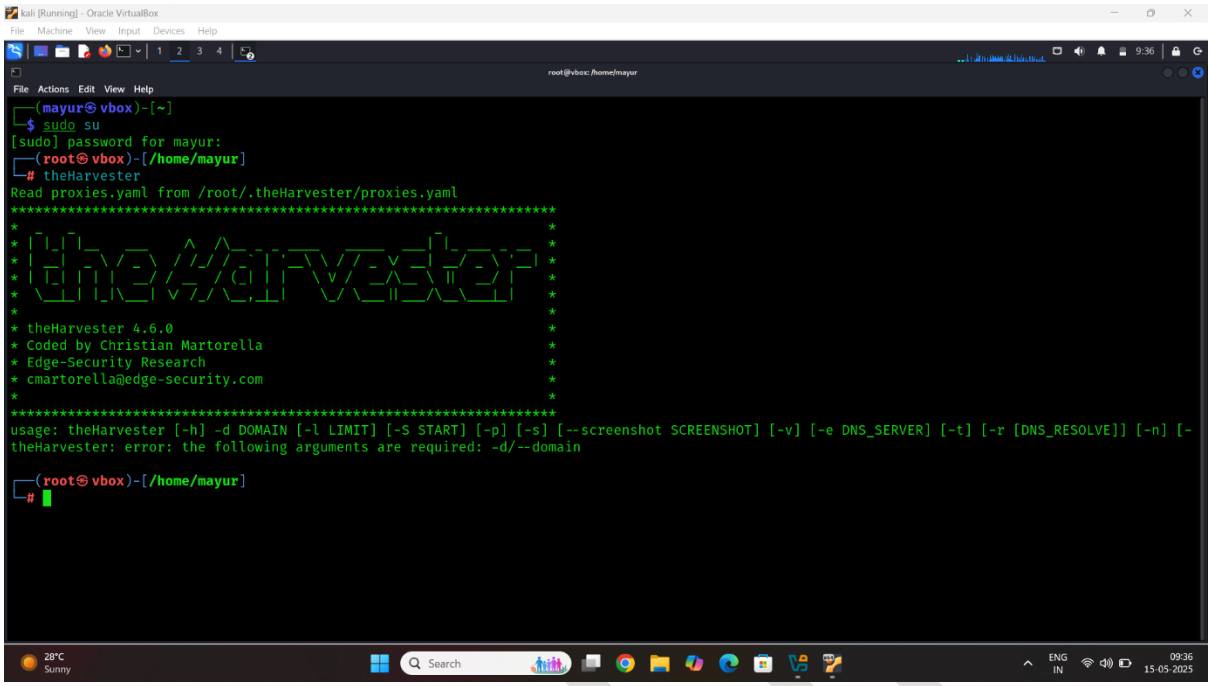

kali - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search...
My Computer
kali
parrot os
Metasploitable2-
Home
parrot os
kali
Apps Places
Mar 23 11:17
mayur@kali: ~
[!] 'censysio_id' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: ''PyPDF3''.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[*] Version check disabled.
Sponsored by...
BLACK HILLS
www.blackhillsinfosec.com
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[91] Recon modules
[8] Reporting modules
[4] Import modules
[2] Exploitation modules
[2] Discovery modules
[2] Disabled modules
[recon-ng][default] > modules serach
Interfaces with installed modules
Usage: modules <load|reload|search> [...]
[recon-ng][default] > workspaces create mayurp
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
28°C
Clear
Search
ENG
IN
20:48
23-03-2025


kali - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search...
My Computer
kali
parrot os
Metasploitable2-
Home
parrot os
kali
Apps Places
Mar 23 11:18
mayur@kali: ~
[!] 'twitter_secret' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. youtube module will likely fail at runtime. See 'keys add'.
[!] 'flickr_api' key not set. flickr module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_companies module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_companies module will likely fail at runtime. See 'keys add'.
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-domains/censys_subdomains' disabled. Dependency required: 'me 'CensysCertificates' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] 'bing_api' key not set. bing_domain_api module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_hostname module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'builtwith_api' key not set. builtwith module will likely fail at runtime. See 'keys add'.
[!] 'spyse_api' key not set. spyse_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: ''PyPDF3''.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[recon-ng][mayurp] > db insert domains
domain (TEXT): certifiedhaacker.com
notes (TEXT): show domains
[*] 1 rows affected.
[recon-ng][mayurp] > show domains
| rowid | domain | notes | module |
| 1 | certifiedhaacker.com | show domains | user_defined |
[*] 1 rows returned
[recon-ng][mayurp] >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
28°C
Clear
Search
ENG
IN
20:48
23-03-2025

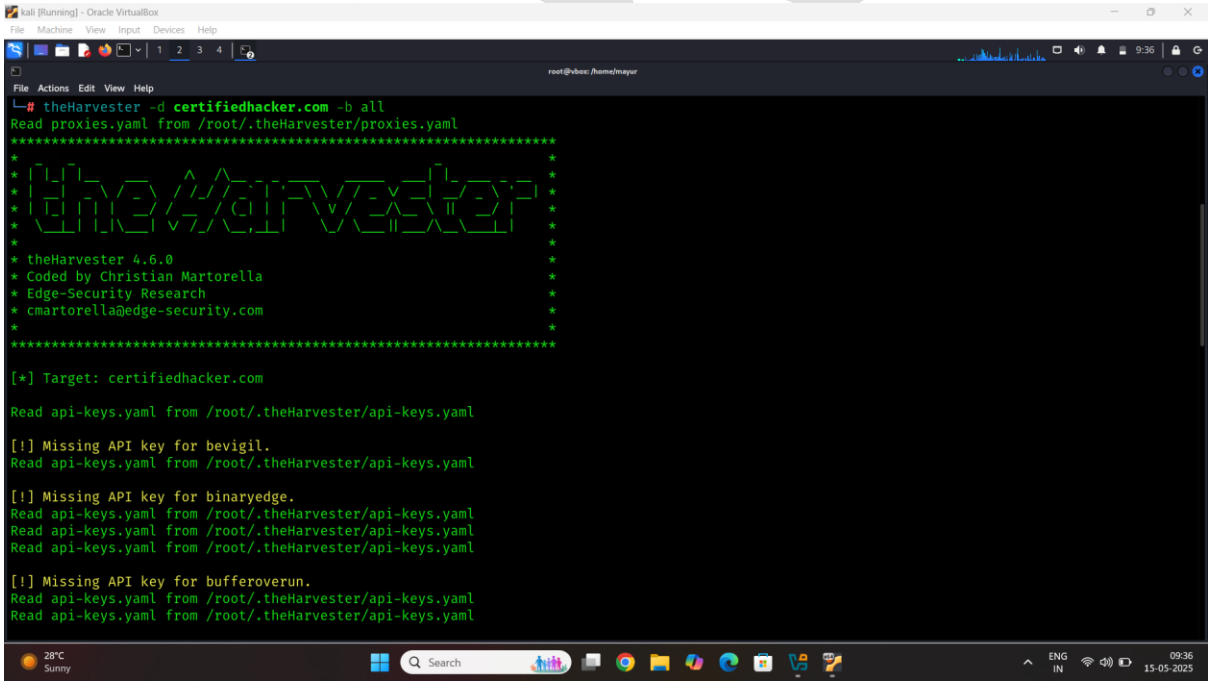


Extra activity using the Harvester

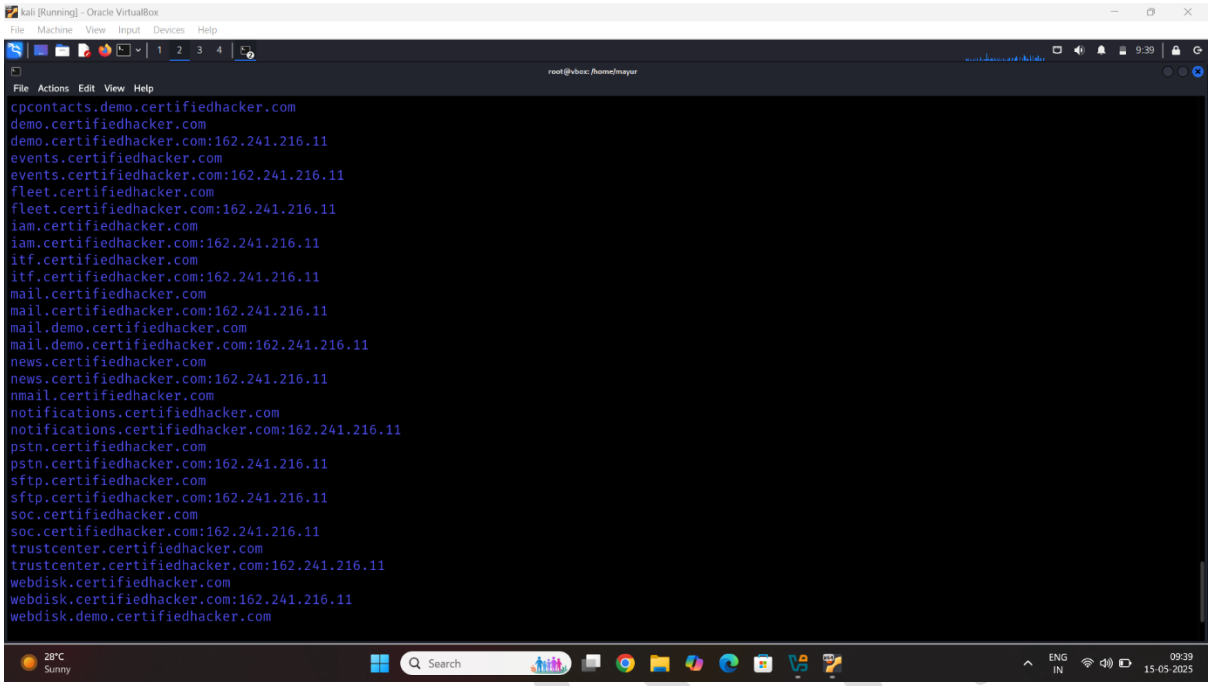
Step1: open kali linux terminal and type it theHarvester



Command: theHarvester –d certifiedhacker.com –b all



Result:

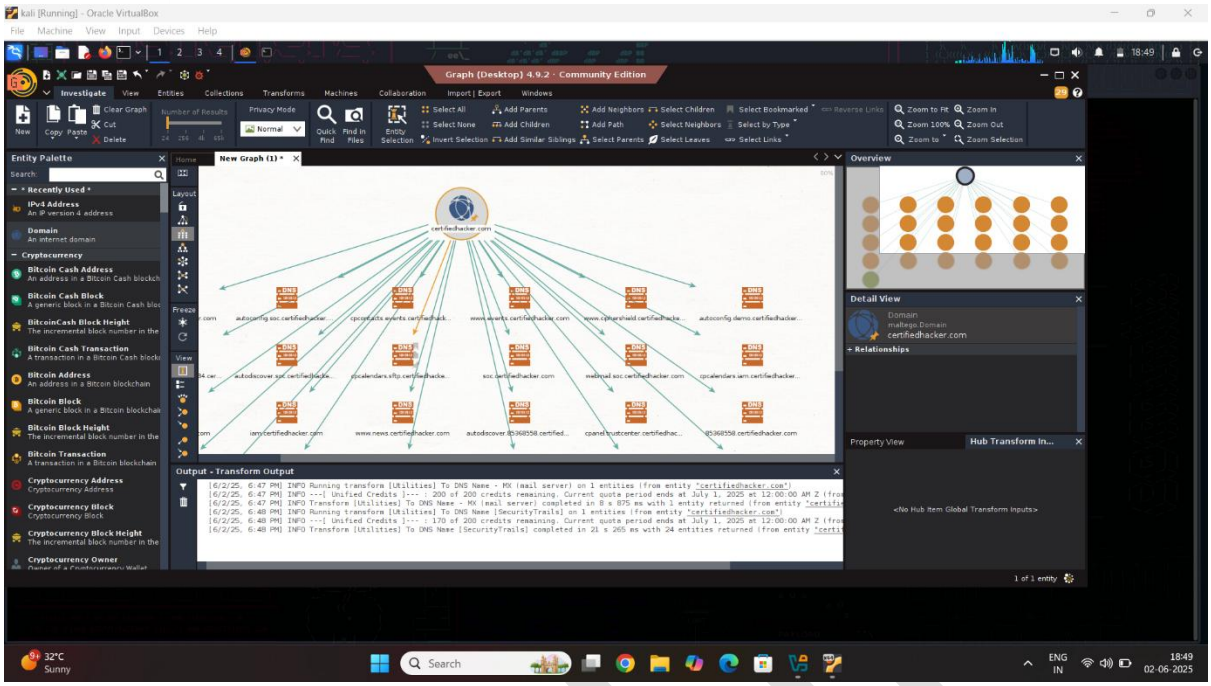


Extra activity using the maltego

Open the kali linux terminal search the maltego

Step1: Open the maltegao
Step2: click on new file and select the options
Example: ip, domain name, phone number

I am find the information domain throw


kali [Running] - Oracle VirtualBox
Graph (Desktop) 4.9.2 - Community Edition
Entity Palette
New Graph (1) *
Overview
Detail View
Property View
Hub Transform In...
Output - Transform Output
certifiedhacker.com
32°C
Sunny
Search
ENG
IN
18:49
02-06-2025