

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 fsociety

Footprinting and Reconnaissance

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 cheat sheet

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

filetype:pdf npam cheat sheets

About 38,000 search results

[Nmap Cheat Sheet - netriders.academy](https://netriders.academy/wp-content/uploads/2024/12/nmap_cheat_sheet_v7.pdf)

Step 1: Nmap sends a SYN/ACK to the zombie workstation to induce a RST in return. This RST frame contains the initial IPID that nmap will remember for later. Step 2: Nmap sends a SYN frame...

[Nmap Cheat Sheet - Comparitech](https://cdn.comparitech.com/2019/06/Nmap-Cheat-Sheet-Comparitech.pdf)

comparitech . Created Date: 6/17/2019 9:33:48 AM Title: Untitled

File Size: 1MB Page Count: 1

[nmap cheatsheet Cheat Sheet - Cheatography.com](https://cheatography.com/netwrkspider/cheat-sheets/nmap-cheatsheet/)

Sep 3, 2015 · nmap cheatsheet Cheat Sheet by Abhishek (netwrkspider) via cheatography.com/23282/cs/5099/ Basic Scanning with Nmap Scan a single target nmap [target]...

[Nmap Cheat Sheet - Amazon Web Services, Inc.](https://s3-us-west-2.amazonaws.com/stationx-public/Nmap-Cheat-Sheet.pdf)

Nmap Cheat Sheet Switch Example Description nmap 192.168.1.1 Scan a single IP nmap 192.168.1.1 192.168.2.1 Scan specific IPs nmap 192.168.1.1-254 Scan a range nmap...

https://netriders.academy/wp-content/uploads/2024/12/nmap_cheat_sheet_v7.pdf

PowerPoint Presentation

Nmap Cheat Sheet

Switch	Example	Description
-S	nmap 192.168.1.1	Scan single IP
-T	nmap 192.168.1.1-192.168.2.1	Scan specific IPs
-R	nmap 192.168.1.1-254	Scan a range
-D	nmap scanme.nmap.org	Scan a domain
-C	nmap 192.168.1.0/24	Scan using CIDR notation
-L	nmap -iL targets.txt	Scan targets from a file
-R	nmap -iR 100	Scan 100 random hosts
-E	nmap -exclude 192.168.1.1	Exclude listed hosts

Switch	Example	Description
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (Default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan
-sW	nmap 192.168.1.1 -sW	TCP Window port scan
-sM	nmap 192.168.1.1 -sM	TCP Maimon port scan

Switch	Example	Description
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sN	nmap 192.168.1.1-24 -sN	Disable port scanning
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x. Port 80 by default
-PA	nmap 192.168.1.1-5 -PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Switch	Example	Description
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-p	nmap 192.168.1.1 -p 21-100	Port range
-p	nmap 192.168.1.1 -p U53,T:21-25,80	Port scan multiple TCP and UDP ports

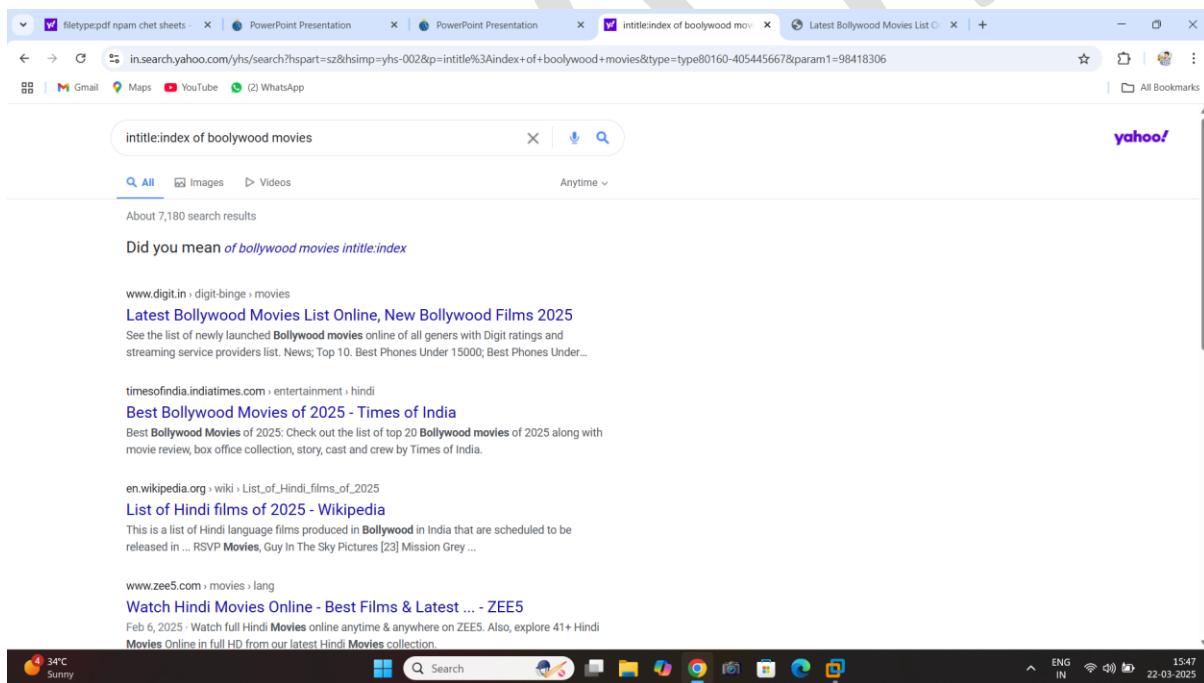
Description:

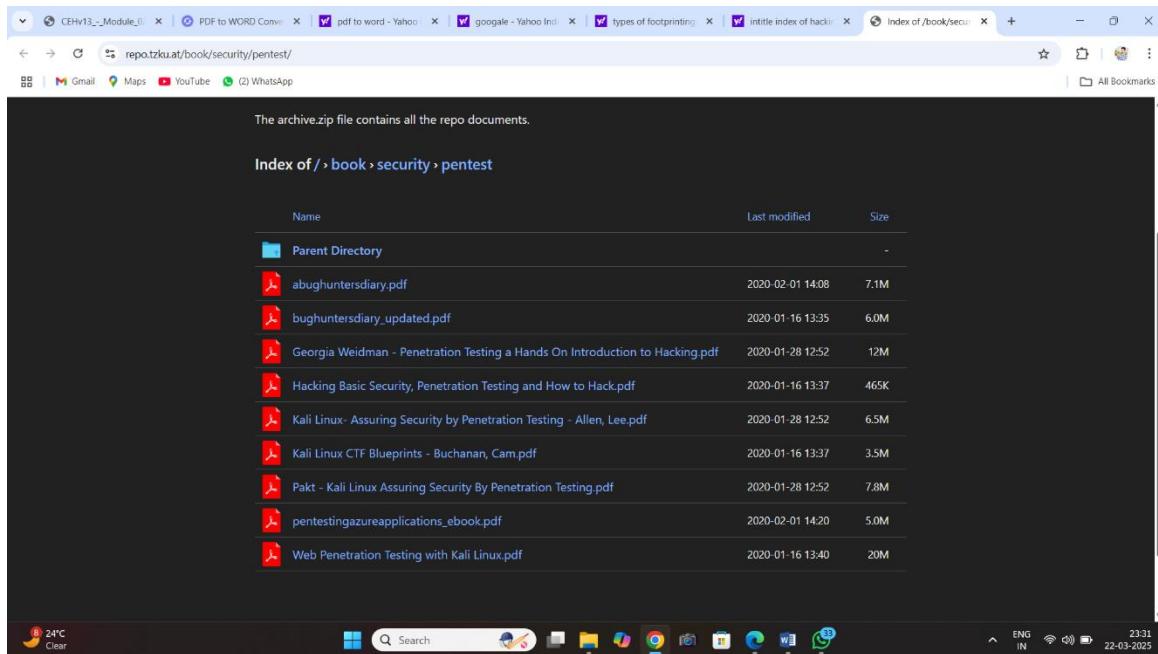
1 The filetype: dork restricts the returned web addresses to the designated file type, such as PDF

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 bollywood 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

The image contains two side-by-side screenshots of web browsers. Both screens show search results for the query "inurl:admin page asp".

Top Screenshot (Yahoo Search Results):

- URL: in.search.yahoo.com/yhs/search/?hspart=sz&hsimp=yhs-002&p=inurl%3Aadmin+page+asp&ttype=type80160-405445667¶m1=439242510
- Search term: inurl:admin page asp
- Results: About 614,000 search results
- Highlighted result: "c# - Creating admin page in asp.net application - Stack Overflow" (Question ID: 9166177)
- Description of result: "Feb 6, 2012 - I am considering best option to create multi-purpose admin page in my asp.net application. In that section should be searching users in database, adding users, review single..."
- Comments: Two comments are shown in boxes:
 - "Between the two options presented, #1 is probably better – at least you won't have to deal with the horrors of maintaining state between 2 dozen ..."
 - "I think that the best option is create a MasterPage, an different aspx, so is more organized. But it always will depends of many pages do you have..."
- Source: seemantaengg.ac.in › jobfair › login
- SEMANTA ENGINEERING COLLEGE
- Search terms: home about us departments academics staff placement student life facilities alumni downloads
- Related link: codinginfinite.com › creating-admin-panel-asp-net
- Related link: Creating Admin Panel in Asp.net Core MVC – Step by Step Tutorial
- Details: Oct 30, 2018 - This is the first Article on Creating Admin Panel in Asp.net Core MVC. We'll divide this tutorial into parts & cover every required feature of Admin Panel Skip to content

Bottom Screenshot (Stack Overflow Question Page):

- URL: stackoverflow.com/questions/9166177/creating-admin-page-in-asp-net-application
- Search term: inurl:admin page asp
- Question title: Creating admin page in asp.net application
- Details: Asked 13 years, 1 month ago Modified 13 years, 1 month ago Viewed 4k times
- Body of question:

 - I am considering best option to create multi-purpose admin page in my asp.net application. In that section should be searching users in database, adding users, review single users or whole groups, etc. I have two ways, how to do it:
 - create single page for every option. It means: on first page will be some text box and search button, on second will be form with multiple textboxes to add new user, and so on.
 - place all needed controls to one page. Then use query string (something like aspx? mode=userAdd) to determine desired task and hide unneeded controls.
 - Please, give me best idea, which one is better. (Or maybe you know completely different approach).

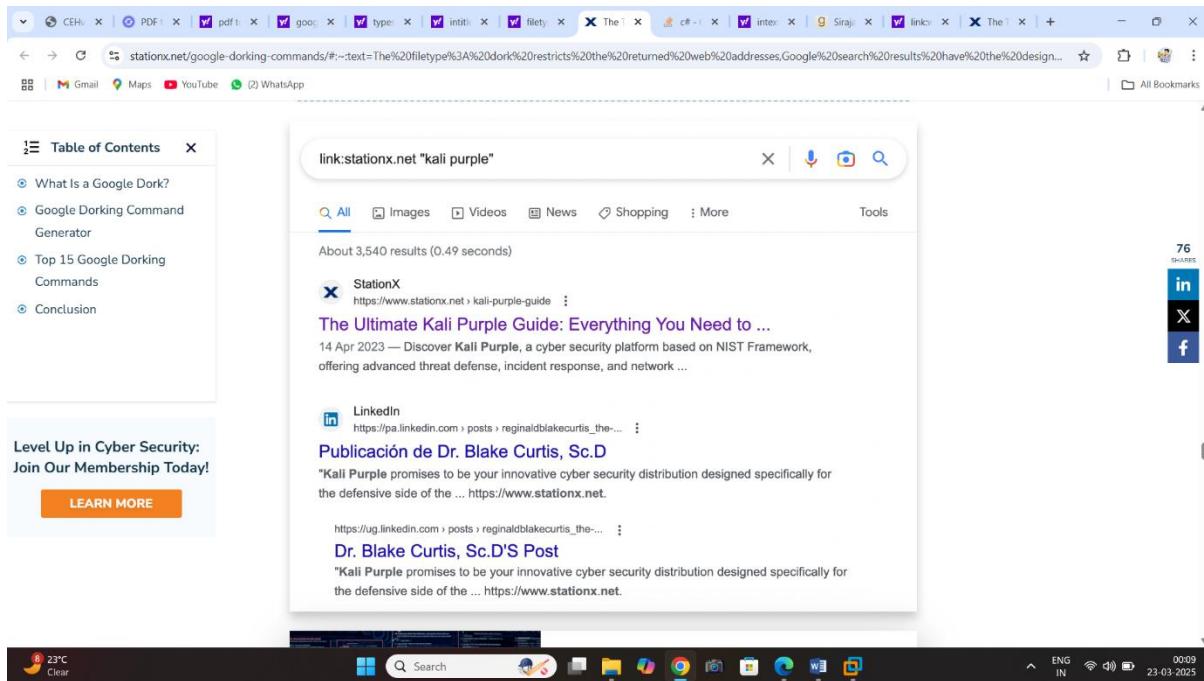
- Tags: c# asp.net
- Comments: Thanks
- Share: Improve this question Follow
- Asked: Feb 6, 2012 at 19:42
- Right sidebar (The Overflow Blog):
 - WIBIT #5: Building a framework to lure web devs to mobile
 - An AI future free of slop
- Featured on Meta:
 - Community Asks Sprint Announcement - March 2025
 - Experimenting with a new experiment opt-out option
 - Policy: Generative AI (e.g., ChatGPT) is banned

Discription

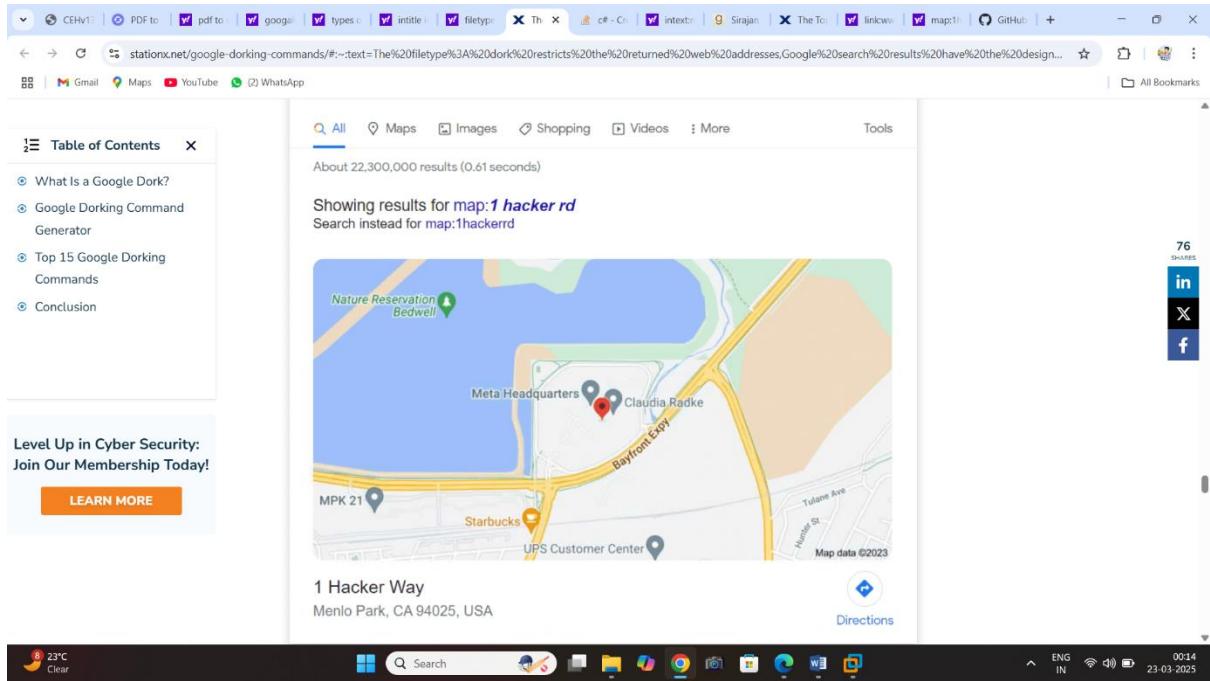
The **inurl:** dork finds URLs containing the character string. You can see the query string in the URL of each Google search result returned. In the example below, the additional dork is to

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

Australia [edit]

Further information: [Telephone numbers in Australia](#)

Per the Australian Communications and Media Authority:^[19]

- Premium rate number
 - 1900 654 321
- Geographic numbers
 - Central East (covering NSW and ACT): (02) 5550 xxxx and (02) 7010 xxxx
 - South East (covering VIC and TAS): (03) 5550 xxxx and (03) 7010 xxxx
 - North East (covering QLD): (07) 5550 xxxx and (07) 7010 xxxx
 - Central West (covering SA, WA and NT): (08) 5550 xxxx and (08) 7010 xxxx
- Mobile numbers
 - 0491 570 006, 0491 570 156, 0491 570 157, 0491 570 158
 - 0491 570 159, 0491 570 110, 0491 570 313, 0491 570 737
 - 0491 571 266, 0491 571 491, 0491 571 804, 0491 572 549
 - 0491 572 665, 0491 572 983, 0491 573 770, 0491 573 087
 - 0491 574 118, 0491 574 632, 0491 575 254, 0491 575 789
 - 0491 576 398, 0491 576 801, 0491 577 426, 0491 577 644
 - 0491 578 957, 0491 578 148, 0491 578 888, 0491 579 212
 - 0491 579 760, 0491 579 455,
- Freephone and local rate numbers
 - 1800 160 401
 - 1800 975 707, 1800 975 708, 1800 975 709, 1800 975 710, 1800 975 711
 - 1300 975 707, 1300 975 708, 1300 975 709, 1300 975 710, 1300 975 711

France [edit]

The French telephone numbering plan is established by the Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse (ARCEP). It reserves six blocks of 10,000 phone numbers for use in audiovisual productions.^[20]

- +33 1 99 00 xx xx (geographic, Île-de-France)
- +33 2 61 91 xx xx (geographic, North-west, Réunion, Mayotte)
- +33 3 53 01 xx xx (geographic, North-east)
- +33 4 65 71 xx xx (geographic, South-east)
- +33 5 36 49 xx xx (geographic, South-west, Overseas)
- +33 6 39 98 xx xx (mobile)

Germany [edit]

Further information: [Telephone numbers in Germany](#)

The Federal Network Agency, the primary authority of the telephone numbering plan in Germany, marked off a 1,000-number block of landline numbers in each of five major cities as so-called "Drama Numbers", to be used in media productions. Additionally, certain mobile providers have also marked off a range of mobile numbers for that purpose.^[21]

Landline Area	First number	Last number
Berlin	(0)30-23125 000	(0)30-23125 999
Frankfurt am Main	(0)69-90009 000	(0)69-90009 999
Hamburg	(0)40-66969 000	(0)40-66969 999
Cologne	(0)221-4710 000	(0)221-4710 999
Munich	(0)89-99998 000	(0)89-99998 999

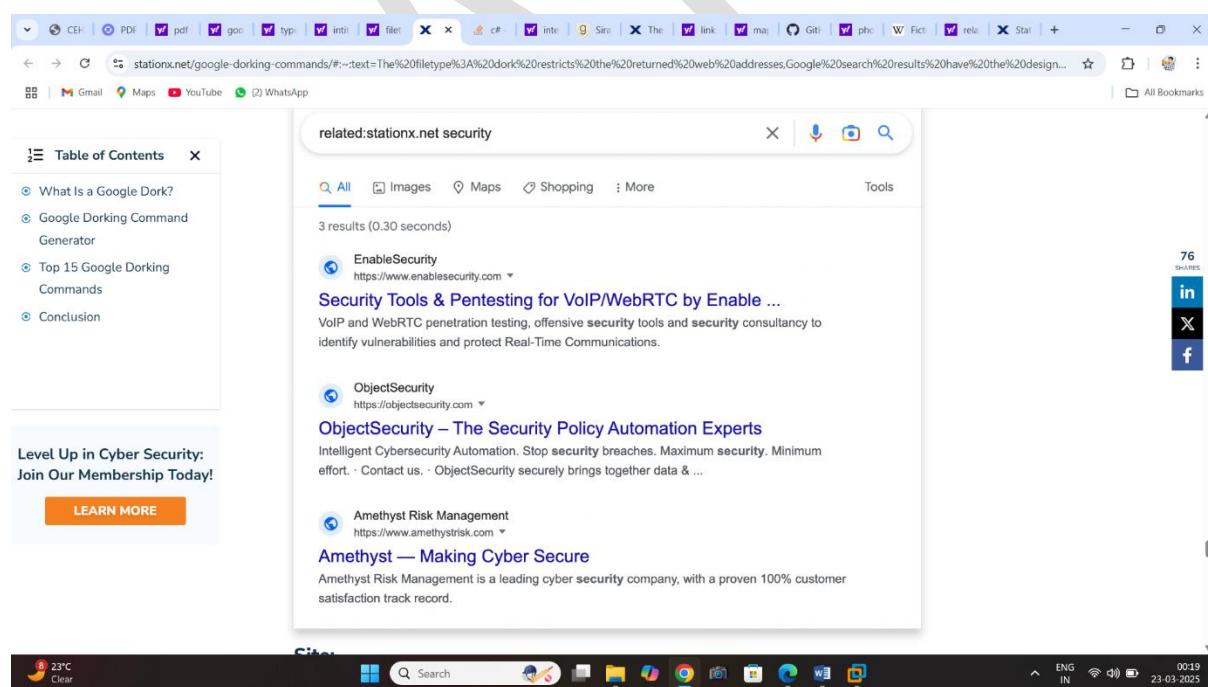
Discription

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

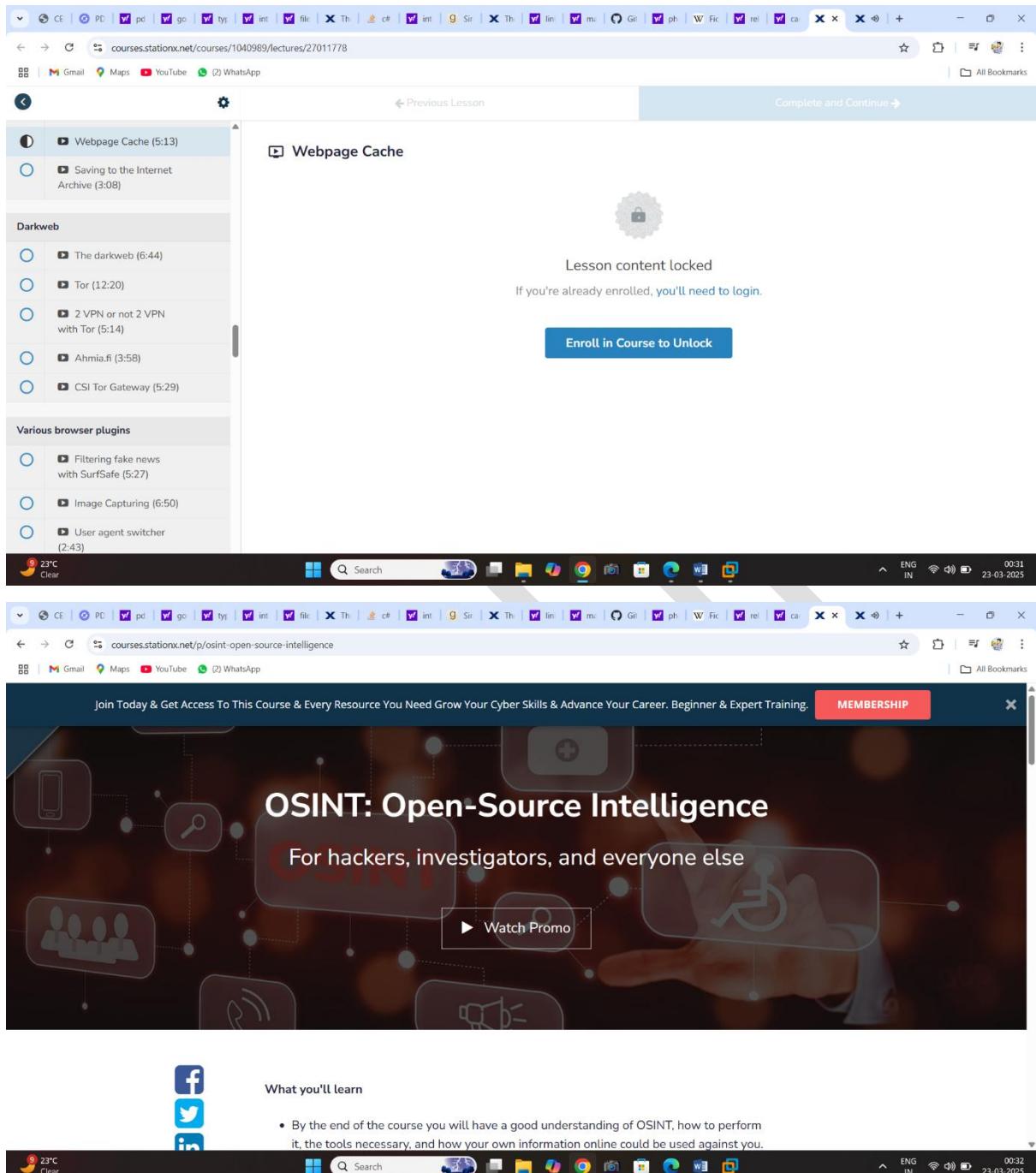


Discription

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

The screenshot shows a web browser window with the URL in.search.yahoo.com/yhs/search?hspart=sz&hsimp=yhs-002&p=cache%3Acourses.stationx.net&type=type80160-405445667¶m1=2739035470 in the address bar. The search query is "cache:courses.stationx.net". The results page displays approximately 157,000 search results. The top result is a link to "Webpage Cache | StationX - Cyber Security Training and Career" for hackers, investigators, and everyone else. Other visible results include links to "Linux Administrator Course - stationx.net" and "StationX - Cyber Security Training and Career Development". The browser interface includes a toolbar with various icons, a search bar, and a navigation bar with back, forward, and search buttons.



Discription

cachē: 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

The screenshot shows a web browser window with the following details:

- Address Bar:** stationsx.net/google-dorking-commands/
- Search Bar:** allinurl: cyber security hacker
- Left Sidebar:**
 - Table of Contents:**
 - What Is a Google Dork?
 - Google Dorking Command Generator
 - Top 15 Google Dorking Commands
 - Conclusion
 - Level Up in Cyber Security:** Join Our Membership Today!
 - LEARN MORE** button
- Search Results:**
 - Simplilearn** - How to Become an Ethical Hacker in 2023?
 - 7 steps · 10 mins · Materials: Computer, Software
 - 1. You should be well-versed with LINUX - a widely used operating system for hacking.
 - 2. Master C programming as it gives the power to utilize the Linux OS.
 - 3. Getting well-versed in various networks and protocols is beneficial in exploiting vulnerabilities.
 - Quora** - Does being a cyber security expert also make you ...
 - 20 Mar 2018 — NO. Not in any shape or form. Some cyber security specialists are capable of being professional hackers, most are not. There is a very good reason for red team, ...
 - 10 answers · 2 votes. I have to agree with most of what was said and it all boils down to two p...
 - Can a cyber security expert become a hacker? - Quora
 - How does a cyber security analyst track a hacker? - Quora
 - How good grades do you need, to be a cyber security ...
 - What is the difference between a cyber security ...
 - E-Careers** - The route to becoming a Cyber Security Ethical Hacker
- Bottom Status Bar:** 23°C Clear, Search bar, and system icons (ENG IN, 00:51, 23-03-2025).

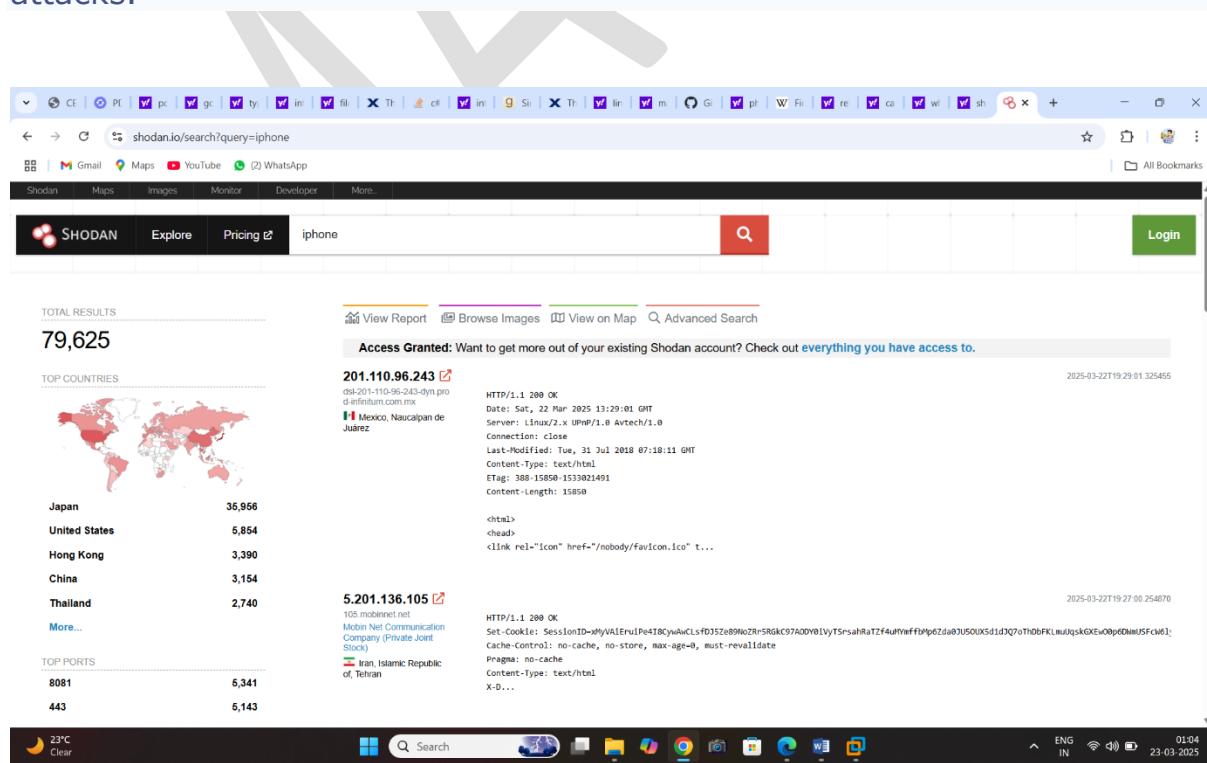
Uses Google Hacking Database

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



The screenshot shows the Shodan search interface with the query 'iphone'. The results page displays 79,625 total results. A world map highlights the top countries where devices were found: Japan (36,956), United States (5,854), Hong Kong (3,390), China (3,154), Thailand (2,740), and more. Below this, a table shows the top ports: 8081 (5,341) and 443 (5,143). Two specific device entries are shown in detail:

- 201.110.96.243**: A device located in Mexico, Naucalpan de Juarez. The IP is associated with d-infinium.com.mx and the port 80. The response header shows:


```
HTTP/1.1 200 OK
Date: Sat, 22 Mar 2025 13:29:01 GMT
Server: Linux/2.x U/PHP/8.0 Avtech/1.0
Connection: close
Last-Modified: Tue, 31 Jul 2018 07:18:11 GMT
Content-Type: text/html
ETag: 388-19850-1533021491
Content-Length: 15850
```

 The content includes HTML code and a favicon link.
- 5.201.136.105**: A device located in Iran, Islamic Republic of, Tehran. The IP is associated with 105.motahare.net and the port 80. The response header shows:


```
HTTP/1.1 200 OK
Set-Cookie: SessionID=xMyVALeru1Pe4tB0CywAwC1sfD35ze89Wo2Rr5RGKc9AOV01Vyt5rsahRaTzf4uhMefffbp6Zda@U50UXd1dJQ7oTh0dFKLmuLjskGXeu0p0DmUFSe6I;
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Content-Type: text/html
X-D...
```

The bottom of the screen shows a taskbar with various icons and system status indicators.

shodan.io/search?query=iphone

TOP ORGANIZATIONS

Organization	Count
Amazon Data Services Japan	12,365
Cogent Communications	7,285
Microsoft Limited	5,765
Microsoft Corporation	5,164
Google LLC	3,641

TOP PRODUCTS

Product	Count
nginx	13,266
lighttpd	3,879
Avtech AVN801 network camera	1,601
D-Link DCS-936L	1,017
Microsoft IIS httpd	547

TOP OPERATING SYSTEMS

OS	Count
DD-WRT	747
Windows	557
Ubuntu	81

Task2 Information gathering using website

1mata.io

Uses any video information

in.search.yahoo.com/yhs/search?hspart=sz&himp=yhs-002&p=youtub+meta.io&type=type80160-40545667¶m1=3079763179

youtub meta.io

About 680,000 search results

[mattw.io > youtube-metadata](#)

MW Metadata - mattw.io
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...

[Bulk](#)
Quickly gather all the metadata about a video, playlist, or...

[Mw Geofind](#)
Channel Search. Check the uploads of channel(s) for...

[github.com / mattwright324 / youtube-metadata](#)

GitHub - mattwright324/youtube-metadata: A quick way to ...
A quick way to gather all the metadata about a video, playlist, or channel from the YouTube API. What's unique about this tool? How can you use it? For more details and notes about YouTube...

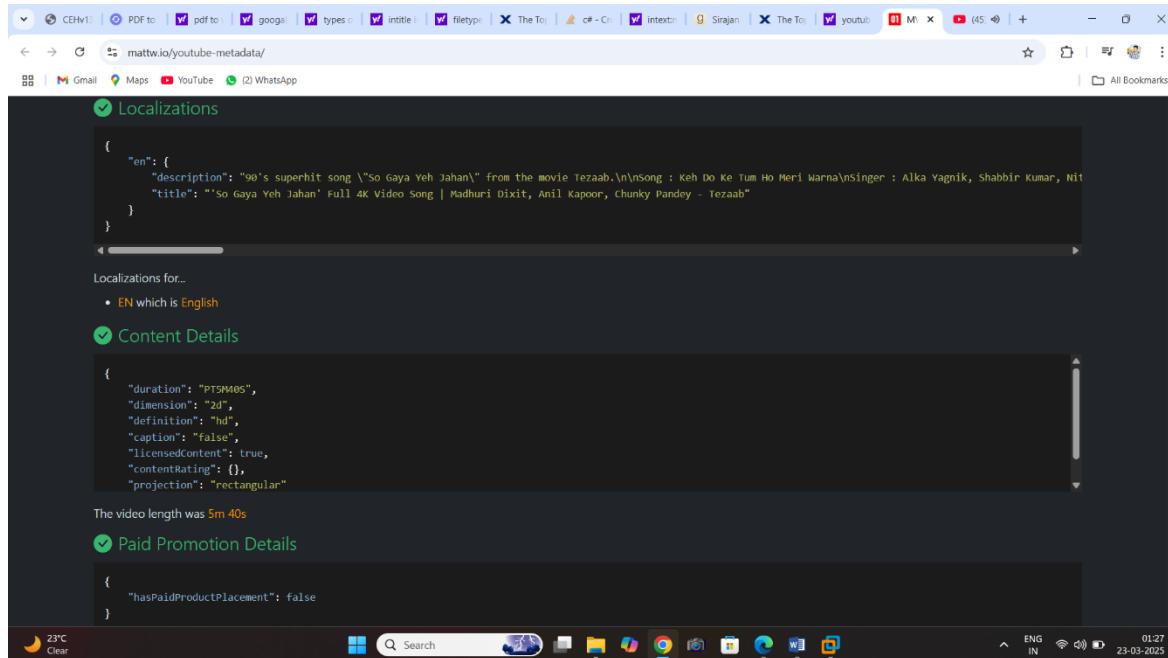
Name	Name
_includes	_includes
_layouts	_layouts
css	css
img	img

The screenshot shows a web browser window with the URL mattw.io/youtube-metadata/. The page displays the JSON metadata for a video titled "'So Gaya Yeh Jahan' Full 4K Video Song | Madhuri Dixit, Anil Kapoor, Chunky Pandey - Tezaab". Below the JSON code, there is a thumbnail image of a woman and a man smiling, with the text "30 Million+ Views" overlaid. The browser's status bar at the bottom shows the date as 23-03-2025.

This screenshot shows the same web browser window with the URL mattw.io/youtube-metadata/. It provides a detailed breakdown of the video's metadata, including its title, published date (Mon, 17 Apr 2017 12:30:02 GMT), and various tags such as "4k video songs", "hd videos 1080p hindi music videos", and "so gaya yeh jahan tezaab hd". It also includes information about the channel's category (Entertainment), default language (English), audio language (English), and the video ID (x-qxMr_kHU). The browser's status bar at the bottom shows the date as 23-03-2025.

Description: 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



```

Localizations
{
  "en": {
    "description": "90's superhit song \"So Gaya Yeh Jahan\" from the movie Tezaab.\n\nsong : Keh Do Ke Tum Ho Meri Warna\nsinger : Alka Yagnik, Shabbir Kumar, Nitin Sawant\nlyrics : Gulzar\nmusic : R.D. Burman\n\nTitle: So Gaya Yeh Jahan' Full 4K Video Song | Madhuri Dixit, Anil Kapoor, Chunky Pandey - Tezaab"
  }
}

Localizations for...
• EN which is English

Content Details
{
  "duration": "PT3M40S",
  "dimension": "2d",
  "definition": "hd",
  "caption": "false",
  "licensedContent": true,
  "contentRating": 0,
  "projection": "rectangular"
}

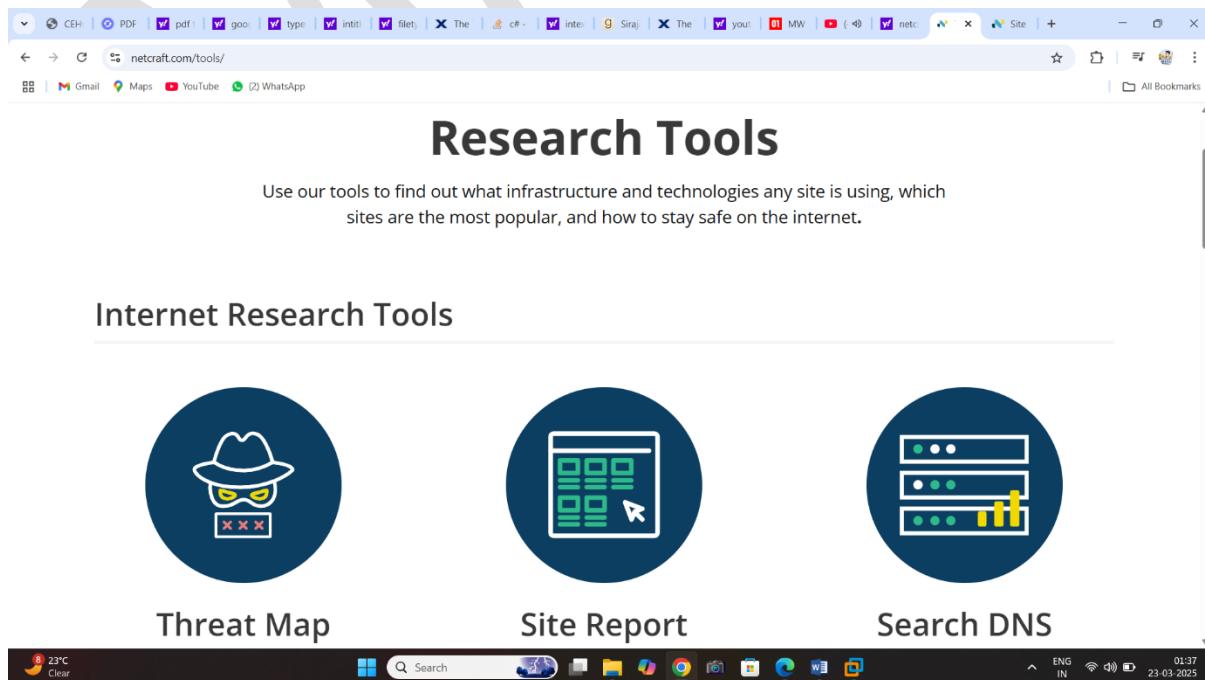
The video length was 5m 40s

Paid Promotion Details
{
  "hasPaidProductPlacement": false
}

```

2 Netcraft:

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



Research Tools

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.

Internet Research Tools

- Threat Map** (Icon: Masked figure)
- Site Report** (Icon: Website structure)
- Search DNS** (Icon: Server stack)

<http://certifiedhacker.com>

Site report for http://certifiedhacker.com

► Look up another site?

Share: [Email](#) [X](#) [f](#) [in](#) [Y](#)

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
23°C Clear	Search	Eng IN 23-03-2025	

<http://certifiedhacker.com>

► Look up another site?

Share: [Email](#) [X](#) [f](#) [in](#) [Y](#)

netcraft

LEARN MORE REPORT FRAUD

IP delegation

IPv4 address (162.241.216.11)

IP range	Country	Name	Description
::ffff: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

23°C Clear

Search Eng IN 23-03-2025

The screenshot shows a browser window with the URL <http://certifiedhacker.com> in the address bar. The page itself is from Netcraft, displaying IP geolocation information. At the top right are 'LEARN MORE' and 'REPORT FRAUD' buttons. Below this is a table with columns for IP range, Country, Name, and Description. The table lists four entries, all from the United States. The last section, 'IP Geolocation', includes a map of North America with a blue dot indicating the location of the server. The Windows taskbar at the bottom shows various icons and the date/time as 23-03-2025.

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	United States	NET162	Various Registries (Maintained by ARIN)
↳ 162.240.0.0-162.241.255	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer
↳ 162.241.216.11	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer

IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)

23°C Clear

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

Dns-dumster

About 28,400 search results

dnsdumpster.com

DNSDumpster - Find & lookup dns records for recon & research

Free domain research tool to discover hosts related to a domain. Find visible hosts from the attackers perspective for Red and Blue Teams.

Developer
Access to the dnsdumpster.com datasets via API is available...

About & FAQ
Domain-based reconnaissance allows security teams to map an...

Footprinting and Reconnaiss...
Attack Surface Discovery is Time Critical. The Blue Team...

Advanced Access
A Suite of Tools for Network and Security Operators...

Member Access
Tactical Domain Intelligence Illuminate the Attack Surface...

dnsdumpster.com : developer
Developer - DNSDumpster.com
Access to the dnsdumpster.com datasets via API is available to both Free users and those with Plus Access. Response data includes all found DNS records, ASN network owner, netblocks and...

dnsdumpster.com : about-faq

DNSDumpster.com

dns recon & research, find & lookup dns records

Enter a Domain to Test

www.certifiedhacker.com

Start Test!

>> Free users are limited to 50 results for a single domain. Get 12 months [Plus Access](#) - on Sale Now.

System Locations Hosting / Networks Services / Banners

System Locations

Hosting / Networks

UNIFIEDLAYER-AS-1	
CLOUDFLARENET	

Services / Banners

Apache	4
cloudflare	4
20- Welcome to Pure-FTPd	2
privsep TLS - 20- You are user number 1 of 150 allowed. 20-	
Local time is now	
SSH-2.0-OpenSSH_7.4	2

A Records (subdomains from dataset)

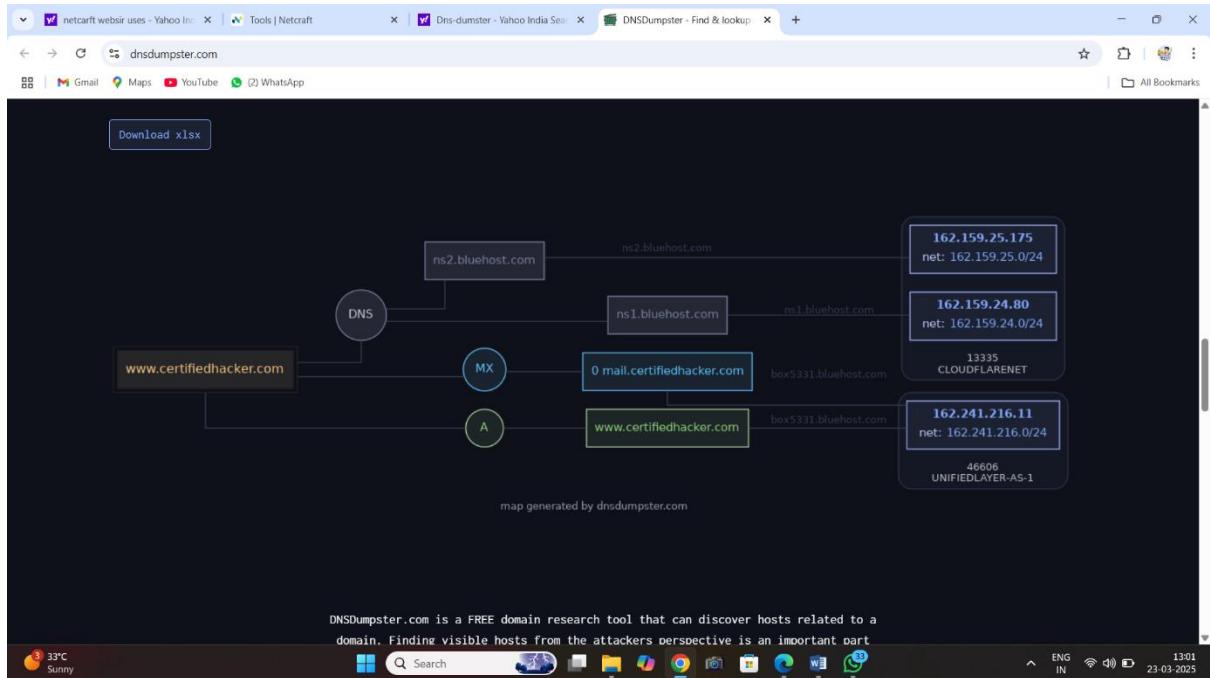
Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
www.certifiedhacker.com	162.241.216.11	ASN 46686	UNIFIEDLAYER-AS-1	ssh: SSH-2.0-OpenSSH_7.4 ftp: 20- Welcome to Pure-FTPd privsep TLS - 20- You are user number 1 of 150 allowed. 20- Local time is now http: Apache title: 404 Not Found tech: Apache HTTP Server https: Apache title: 404 Not Found	9503
box5331.bluehost.com	162.241.216.0/24		United States		

MX Records

0 mail.certifiedhacker.com	162.241.216.11	ASN 46686	UNIFIEDLAYER-AS-1	ssh: SSH-2.0-OpenSSH_7.4 ftp: 20- Welcome to Pure-FTPd privsep TLS - 20- You are user number 1 of 150 allowed. 20-Local time is now http: Apache title: 404 Not Found tech: Apache HTTP Server https: Apache title: 404 Not Found cm: .bluehost.com tech: Apache HTTP Server
box5331.bluehost.com	162.241.216.0/24		United States	

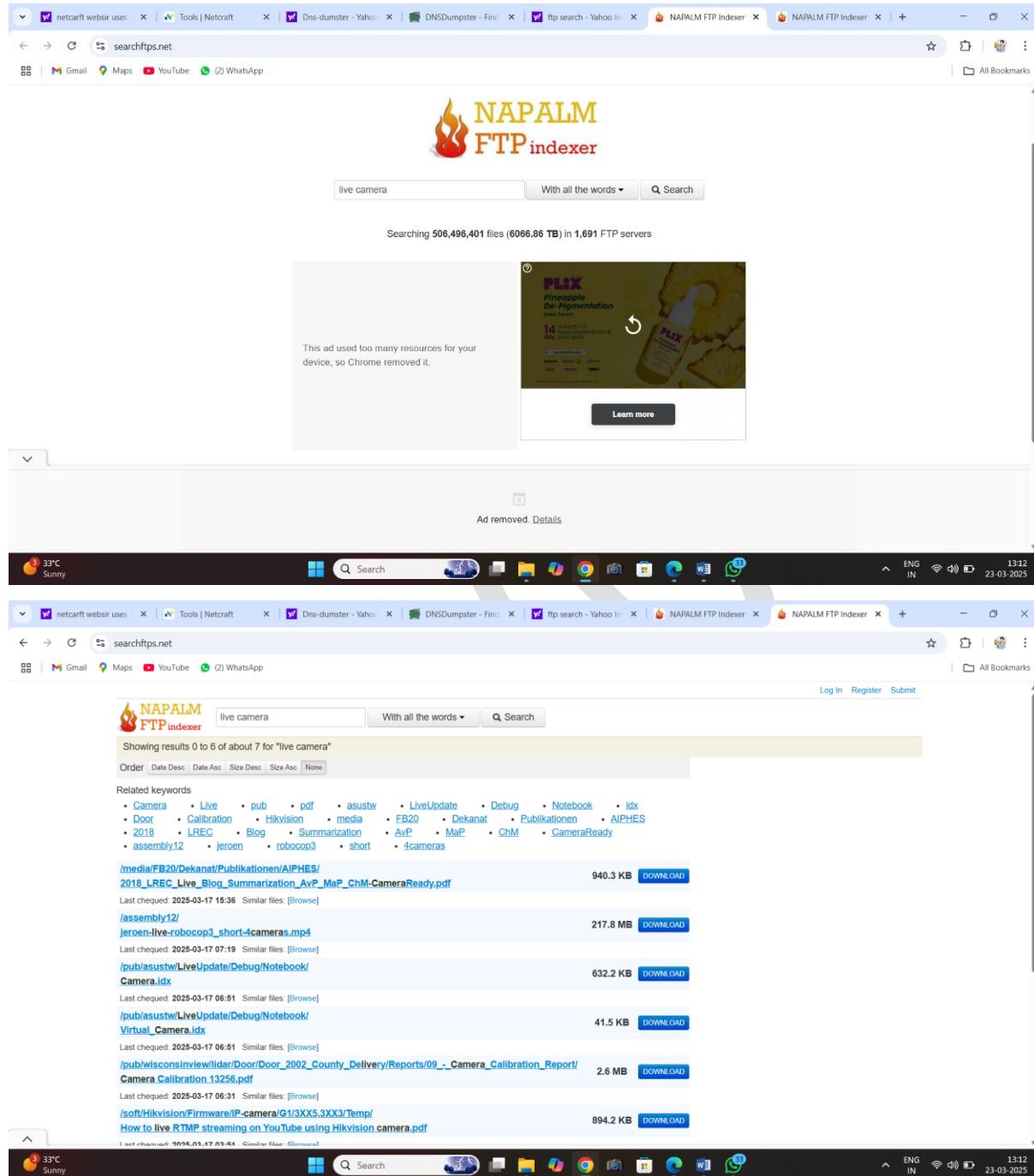
NS Records

ns2.bluehost.com	162.159.25.175	ASN 13335	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare http://cloudflare title: Direct IP access not allowed tech: Cloudflare
ns2.bluehost.com	162.159.25.0/24			
ns1.bluehost.com	162.159.24.80	ASN 13335	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed
ns1.bluehost.com	162.159.24.0/24			



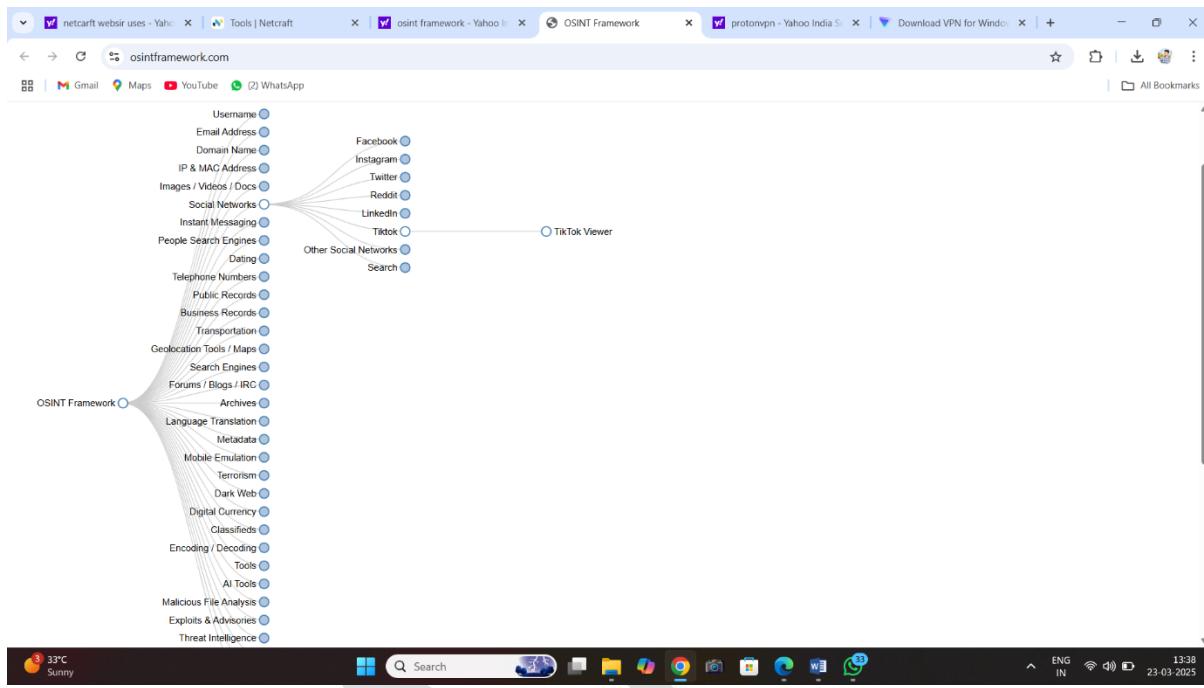
Description : DNSDumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process

NAPALM FTP Indexer



Description: 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 FRAMEWORK



Description: 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

The screenshot shows the Whois.com homepage with a dark background featuring a network of nodes. At the top, there's a navigation bar with links for Domains, Hosting, Servers, Email, Security, Whois, and Deals. Below the navigation is a search bar with the placeholder "Enter Domain or IP Address" and an orange "SEARCH" button. A dropdown menu is open over the search bar, showing suggestions like "qq.co", "unipune.ac.in", "certifiedethical.com", "iphone", and "camera". The main heading "Whois Domain Lookup" is centered above the search area.

Frequently Asked Questions

- + What is a Whois domain lookup?

A screenshot of a Windows taskbar. It includes pinned icons for File Explorer, Mail, Photos, OneDrive, Edge, and File Explorer. The system tray shows the date (23-03-2025), time (13:45), battery level (ENG IN), signal strength, and a weather icon indicating 33°C and sunny conditions.

The screenshot shows the Whois.com results for the domain `certifiedethical.com`. The page is titled "certifiedethical.com" and indicates the information was updated 10 days ago. The "Domain Information" section lists the following details:

Domain:	certifiedethical.com
Registered On:	2011-10-24
Expires On:	2025-10-24
Updated On:	2024-10-10
Status:	active
Name Servers:	ns1.nameserver.net.au ns2.nameserver.net.au ns3.nameserver.net.au

The "Registrar Information" section shows:

Registrar:	Synergy Wholesale Accreditations Pty Ltd
IANA ID:	1609
Abuse Email:	registry-abuse@nexigen.digital
Abuse Phone:	+61.383999483

On the right side of the page, there are promotional banners for ".space" and ".fun" domains, both offered at \$1.18. There is also a banner for "WORDPRESS". The bottom of the screen shows a standard Windows taskbar with pinned icons for File Explorer, Mail, Photos, OneDrive, Edge, and File Explorer, along with the system tray showing the same date, time, battery level, signal strength, and weather information.

The screenshot shows two identical browser windows side-by-side, both displaying the Whois.com website for the domain `certifiedethical.com`. The top window displays the **Registrant Contact** information:

Name:	Scott van Iperen
Organization:	International Diamond Corporation Pty Ltd
Street:	3 Padova St
City:	Carseldine
State:	QLD
Postal Code:	4034
Country:	AU
Phone:	+61.449849880
Email:	https://synergywholesale.com/domain-tools/?domain=certifiedethical.com

The bottom window displays the **Administrative Contact** information, which is identical to the Registrant Contact information.

Both windows also show the **Technical Contact** and **Billing Contact** sections, both of which also contain identical information to the other sections. The Whois.com navigation bar at the top includes links for Domains, Hosting, Servers, Email, Security, Whois, and Deals. A search bar and a "WHOIS" button are also present. A sidebar advertisement for hosting services is visible on the right.

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

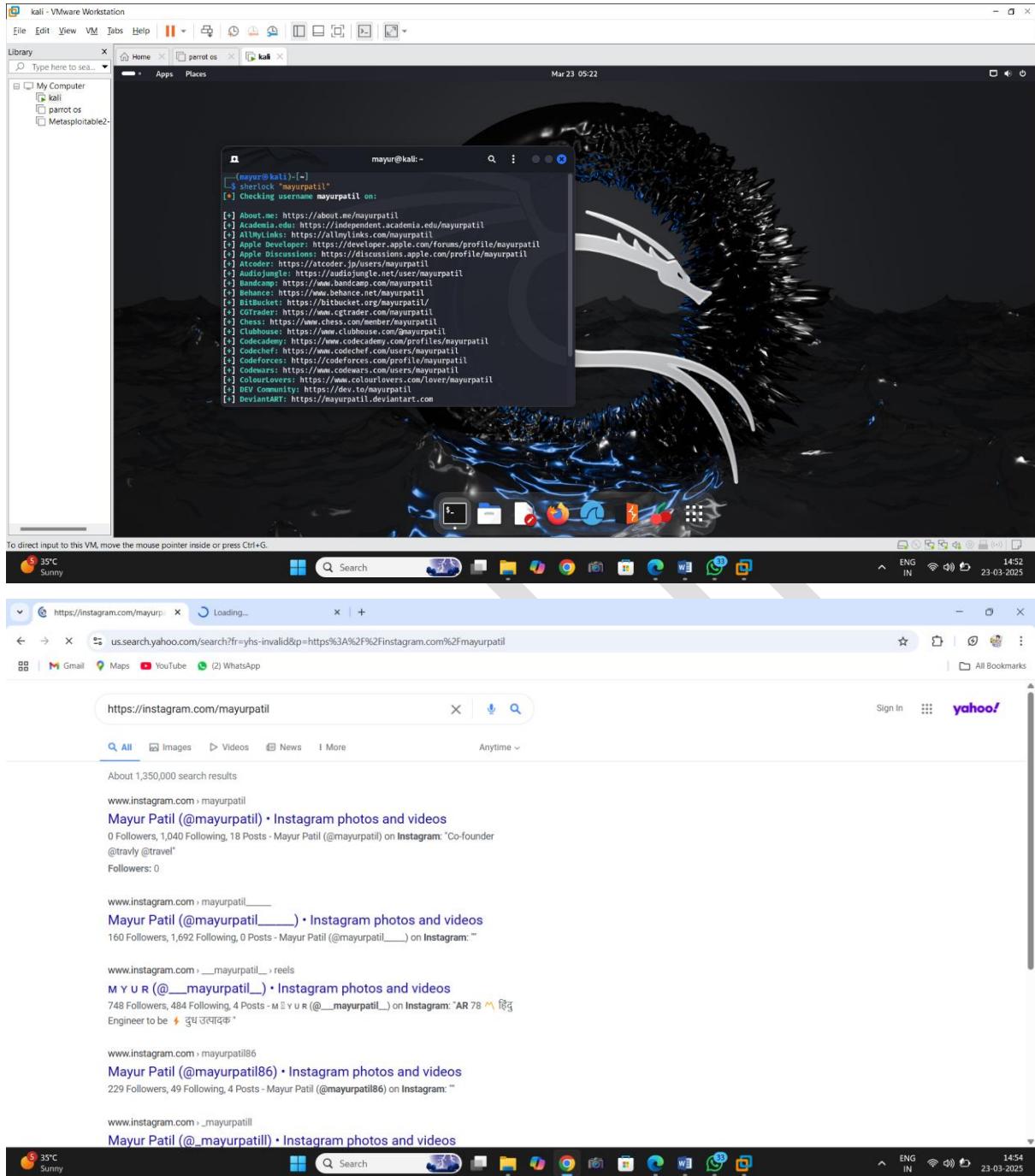
```
(mayur㉿kali)-[~] $ sublister3r -d www.certifiedhcker.com
Sublister3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for www.certifiedhcker.com
[-] Searching now in Yandex..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in VirusTotal..
[-] Searching now in Threatcrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Error: Google probably now is blocking our requests
Process DNSdumpster-B:
Traceback (most recent call last):
  File "/usr/lib/python3.11/multiprocessing/process.py", line 314, in _bootstrap
    self._run()
  File "/usr/lib/python3/dist-packages/sublister3r.py", line 269, in run
    domain_list = self._enumerate()
                   ^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/sublister3r.py", line 649, in enumerate
    token = self._get_csrftoken(resp)
            ^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/sublister3r.py", line 644, in _get_csrftoken
    token = csrf_regex.findall(resp)[0]
                   ^^^
IndexError: list index out of range
[-] Error: Google probably now is blocking our requests
[-] Finished now the Google enumeration ...
[-] (mayur㉿kali)-[~]
```

Sherlock

Command: Sherlock "domain name"

Uses: for any one social media information

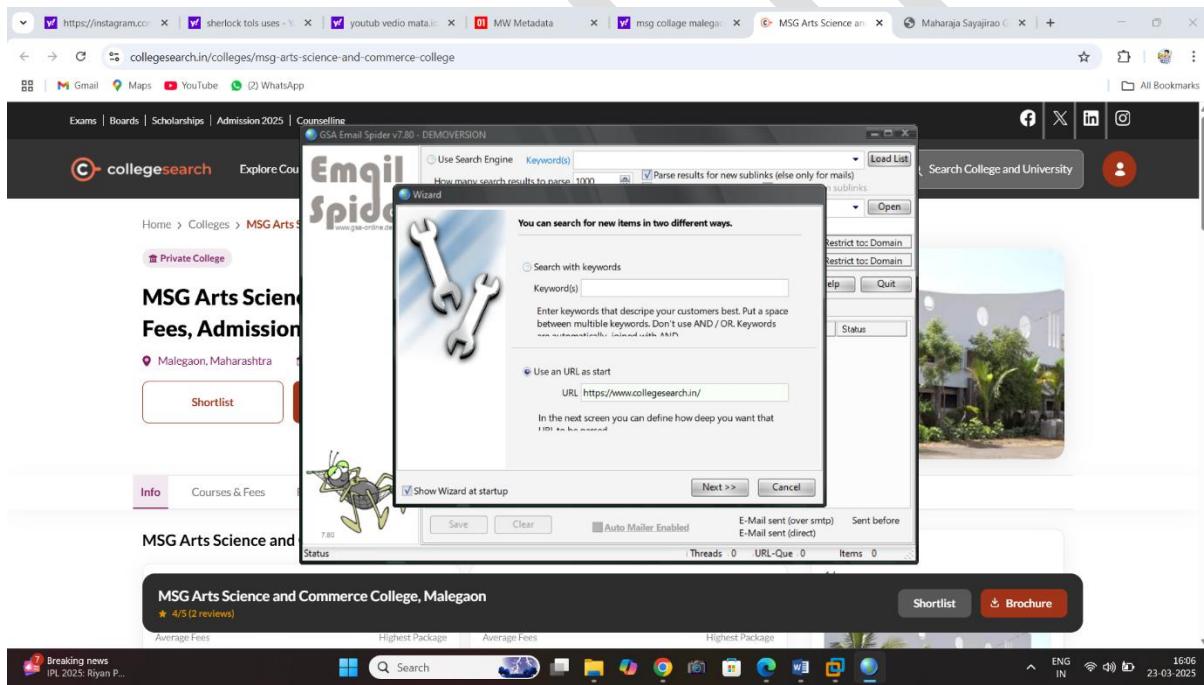


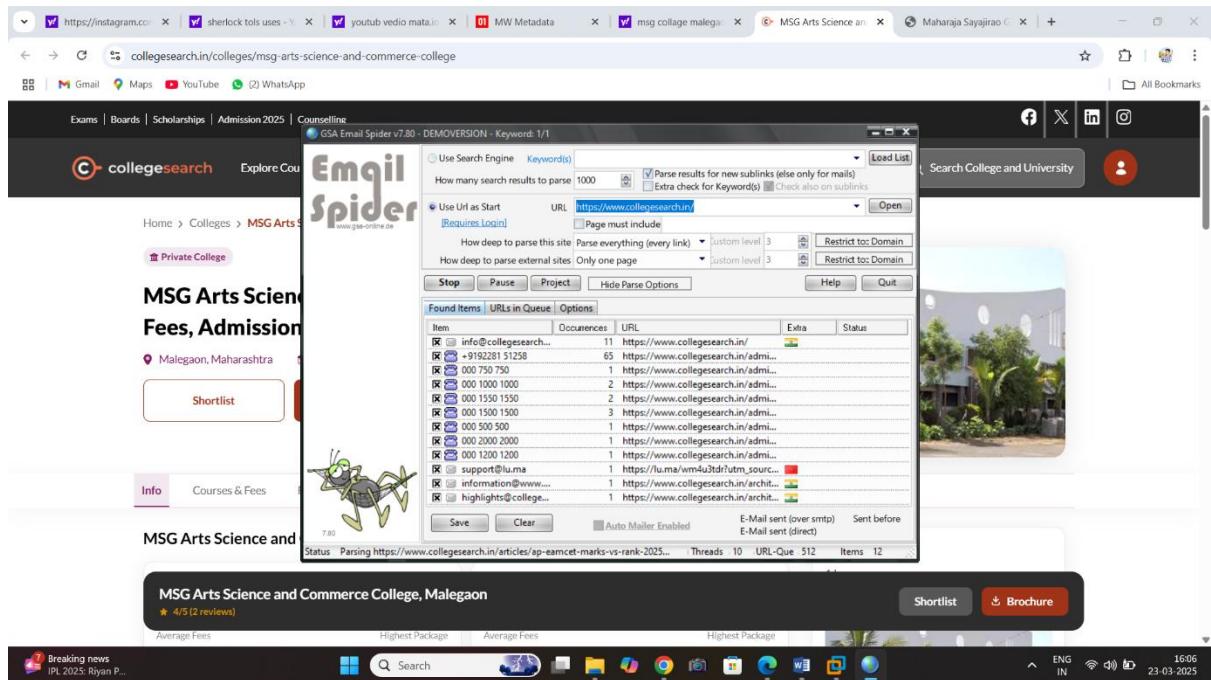
Discription:

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 Footprinting

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¶m1=4216893554

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...

Blacklists
(Commonly called Realtime blacklist, DNSBL or RBL). If your...

Analyze Headers
Analyze Headers - MX Lookup Tool - Check your DNS MX Records...

Dmrc
Dmrc - MX Lookup Tool - Check your DNS MX Records online -...

SPF
ABOUT SPF RECORD CHECK. The SPF Record Check is a diagnostic...

SuperTool
All of your MX record, DNS, blacklist and SMTP diagnostics...

MX Lookup
Tools Delivery Center Monitoring Products Blog Support...

Diagnostics
This test will connect to a mail server via SMTP, perform a...

mxtoolbox.com - supertool

Welcome to Wondershare Dem... | Original message | mx tools - Yahoo India Search | Email Header Analyzer, RFC822

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>#U{display: none; width: 1px; height: 1px; }</style>
<html>*</span> |
| 3                                                                                               | 4 Seconds |                                         |                               | CMD    | 3/18/2025 1:22:50 PM |                                   |

Your IP is: 10.149.10.49 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866) 698-6652 | © Copyright 2004-2021 MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2

30°C Clear

**dmarc:mail-service.wondershare.com** Show Solve Email Delivery Problems

**DMARC Record for mail-service.wondershare.com**

No DMARC Record found for sub-domain.

Organization Domain of this sub-domain is: wondershare.com Inbox Receivers will apply wondershare.com DMARC record to mail sent from mail-service.wondershare.com

SP Tag '' found: Inbox Receivers will treat all mail sent from mail-service.wondershare.com that fails DMARC as suspicious.

**DMARC Record for wondershare.com (organizational domain)**

v=DMARC1;p=none

**spf:mail-service.wondershare.com:8.219.34.25** Show Solve Email Delivery Problems

v=spf1 include:spfdm-ap-southeast-1.aliyun.com ~all

**dkim:mail-service.wondershare.com:default** Show

Dkim Public Record

v=DKIM1; k=rsa; p=MIGFMABGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDHwzldYChN16eOhJD7Xt/pLKRICKwa27PVicPiKzYBtIzeMaq0oLVnQtjIz1CYazVZPMeuTsQMB/XbPB/pPwa0DDOzb3+EftVG/BDVaVoohPF6My+2H90U6g9t/7PDQGou8YBLC

Your IP is: 10.149.10.49 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866) 698-6652 | © Copyright 2004-2021 MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2

30°C Clear

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

# DNS Transfer zone

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

**A records**

| IPv4 address     | Revalidate in |
|------------------|---------------|
| > 162.241.216.11 | 4h            |

**AAAA records**  
No AAAA records found.

**CNAME record**  
No CNAME record found.

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.

**NS records**

| Name server       | Revalidate in |
|-------------------|---------------|
| ns2.bluehost.com. | 24h           |
| ns1.bluehost.com. | 24h           |

**MX records**

| Mail server               | Priority  | Revalidate in |
|---------------------------|-----------|---------------|
| mail.certifiedhacker.com. | 0 Primary | 4h            |

**Other records**

| SOA                                                                                              | Revalidate in |
|--------------------------------------------------------------------------------------------------|---------------|
| Start of authority ns1.bluehost.com.<br>Email dnsadmin@box5331.bluehost.com<br>Serial 2025032200 | 24h           |

**4 MX**

Directs email to mail servers.

**5 NS**

Specifies the authoritative Name server for a domain.

**Start of authority**

|                   |
|-------------------|
| ns1.bluehost.com. |
|-------------------|

**Email** dnsadmin@box5331.bluehost.com

**Serial** 2025032200

**Refresh** 24h

**Retry** 2h

**Expire** 1000h

**Negative cache TTL** 5m

**Look up DNS records for another domain name**

With [DNS lookup](#), you can find the DNS record for any domain name or

**6 SOA**

Provides important details about a

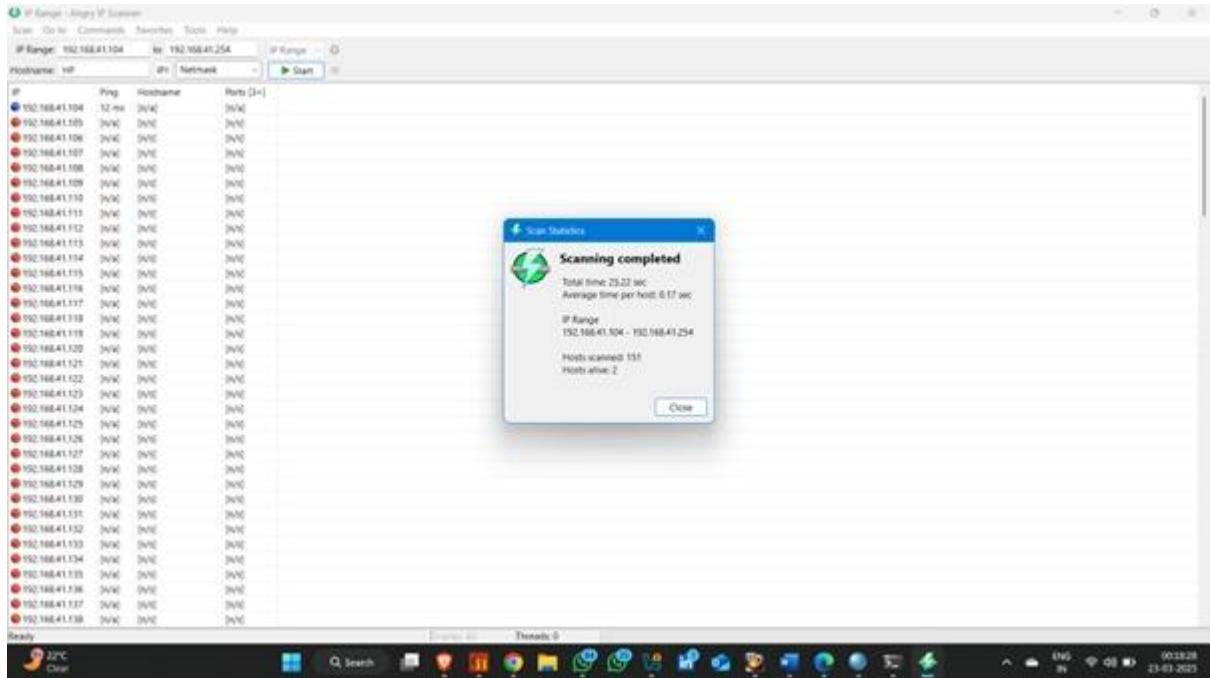
|       |                                                       |
|-------|-------------------------------------------------------|
|       | DNS zone; required for every DNS                      |
| 7 TXT | Stores text information, often used for verification. |
| 8 SRV | Specifies a service location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



**PRACTISESEC**  
www.practisesec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

- [+] Recon modules
- [+] Reporting modules
- [+] Import modules
- [+] Exploitation modules
- [+] Discovery modules
- [+] 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 2048 23-03-2025

kali - VMware Workstation

File Edit View VM Tabs Help

Library Type here to sea... ▾ 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. oxy_whoxy module will likely fail at runtime. See 'keys add'.
[+] 'whoxy_secret' key not set. oxy_whoxy 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-pac
net/censys/search/v1/Company.py:76)'
```

[+] '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'.
[+] 'spysye\_api' key not set. spysye\_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 2048 23-03-2025



```
[*] certifiedhacker.bt => No record found.
[*] certifiedhacker.bug => No record found.
[*] certifiedhacker.buggalo => No record found.
[*] certifiedhacker.bugs => No record found.
[*] certifiedhacker.bugzilla => No record found.
[*] certifiedhacker.build => No record found.
[*] certifiedhacker.bulletins => No record found.
[*] certifiedhacker.burn => No record found.
[*] certifiedhacker.burp => No record found.
[*] certifiedhacker.buscador => No record found.
[*] certifiedhacker.buy => No record found.
[*] certifiedhacker.bv => No record found.
[*] certifiedhacker.bw => No record found.
[*] certifiedhacker.by => No record found.
[*] certifiedhacker.bz => No record found.
[*] certifiedhacker.c => No record found.
[*] certifiedhacker.caithness => No record found.
[*] certifiedhacker.ca => No record found.
[*] certifiedhacker.cache => No record found.
[*] certifiedhacker.cafe => No record found.
[*] certifiedhacker.calendar => No record found.
[*] certifiedhacker.california => No record found.
[*] certifiedhacker.call => No record found.
[*] certifiedhacker.calvin => No record found.
[*] certifiedhacker.camila => No record found.
[*] certifiedhacker.camal => No record found.
[*] certifiedhacker.canon => No record found.
[*] certifiedhacker.careers => No record found.
[*] certifiedhacker.catalog => No record found.
[*] certifiedhacker.cc => No record found.
[*] certifiedhacker.cd => No record found.
[*] certifiedhacker.cdburner => No record found.
[*] certifiedhacker.cdn => No record found.
[*] certifiedhacker.cert => No record found.
[*] certifiedhacker.certified => No record found.
[*] certifiedhacker.certify => No record found.
[*] certifiedhacker.certserv => No record found.
[*] certifiedhacker.certsrv => No record found.
[*] certifiedhacker.cf => No record found.
```

## Extra activity using the Harvester

**Step1:** open kali linux terminal and type it  
theHarvester

```
File Machine View Input Devices Help
File Actions Edit View Help
[(mayur@vbox)-[~]
$ sudo su
[sudo] password for mayur:
[root@vbox]~/home/mayur]
theHarvester
Read proxies.yaml from /root/.theHarvesterproxies.yaml

* [!] [-] - \^/ / \^- - \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* theHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*

usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-n]
theHarvester: error: the following arguments are required: -d/--domain

[root@vbox]~/home/mayur]
#
```

## Command: theHarvester –d certifiedhacker.com –b all

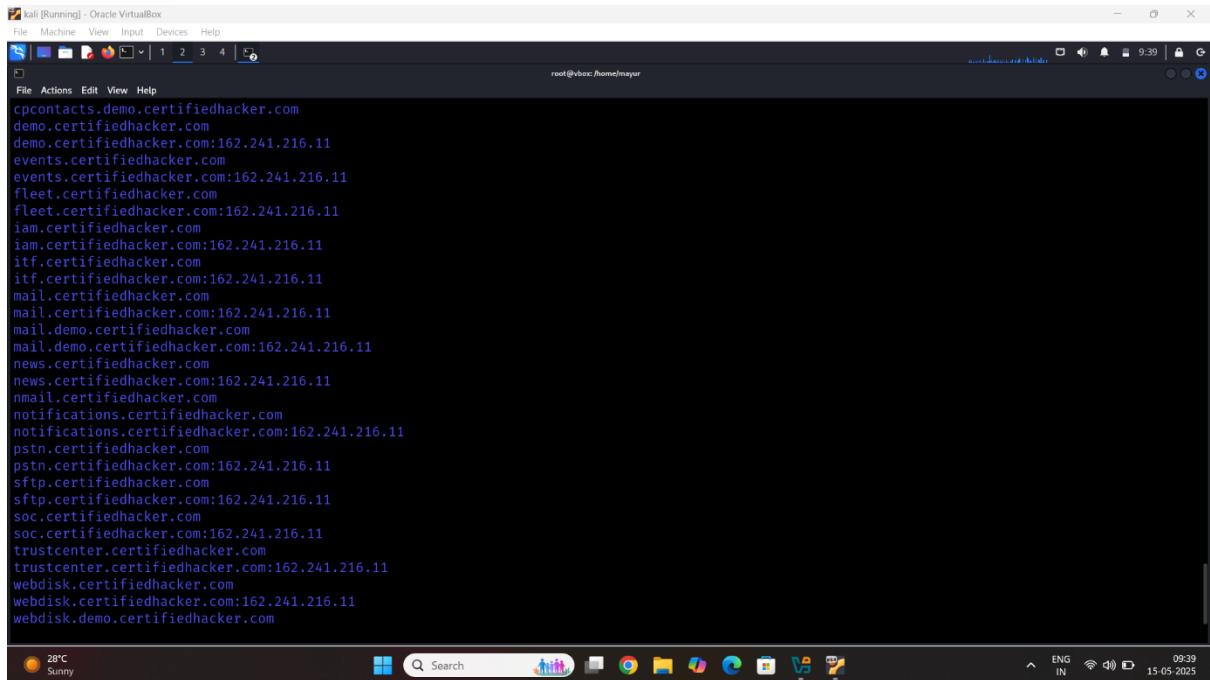
```
File Machine View Input Devices Help
File Actions Edit View Help
[(mayur@vbox)-[~]
theHarvester -d certifiedhacker.com -b all
Read proxies.yaml from /root/.theHarvesterproxies.yaml

* [!] [-] - \^/ / \^- - \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* [!] [-] - \^/ / / \^/ \^/\^/\^/ v \- [^] - \^/- | *
* theHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*

[*] Target: certifiedhacker.com
Read api-keys.yaml from /root/.theHarvesterapi-keys.yaml
[!] Missing API key for bevigil.
Read api-keys.yaml from /root/.theHarvesterapi-keys.yaml
[!] Missing API key for binaryedge.
Read api-keys.yaml from /root/.theHarvesterapi-keys.yaml
Read api-keys.yaml from /root/.theHarvesterapi-keys.yaml
Read api-keys.yaml from /root/.theHarvesterapi-keys.yaml
[!] Missing API key for bufferoverun.
Read api-keys.yaml from /root/.theHarvesterapi-keys.yaml
Read api-keys.yaml from /root/.theHarvesterapi-keys.yaml

[root@vbox]~/home/mayur]
#
```

## Result:



```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
cococontacts.demo.certifiedhacker.com
demo.certifiedhacker.com
demo.certifiedhacker.com:162.241.216.11
events.certifiedhacker.com
events.certifiedhacker.com:162.241.216.11
fleet.certifiedhacker.com
fleet.certifiedhacker.com:162.241.216.11
iam.certifiedhacker.com
iam.certifiedhacker.com:162.241.216.11
itf.certifiedhacker.com
itf.certifiedhacker.com:162.241.216.11
mail.certifiedhacker.com
mail.certifiedhacker.com:162.241.216.11
mail.demo.certifiedhacker.com:162.241.216.11
news.certifiedhacker.com
news.certifiedhacker.com:162.241.216.11
nmail.certifiedhacker.com
notifications.certifiedhacker.com
notifications.certifiedhacker.com:162.241.216.11
pstn.certifiedhacker.com
pstn.certifiedhacker.com:162.241.216.11
sftp.certifiedhacker.com
sftp.certifiedhacker.com:162.241.216.11
soc.certifiedhacker.com
soc.certifiedhacker.com:162.241.216.11
trustcenter.certifiedhacker.com
trustcenter.certifiedhacker.com:162.241.216.11
webdisk.certifiedhacker.com
webdisk.certifiedhacker.com:162.241.216.11
webdisk.demo.certifiedhacker.com

```

28°C Sunny 09:39 15-05-2025 ENG IN

## 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

