

REPORT OF FOOTPRINTING AND RECONNAISSANCE

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.

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 :-

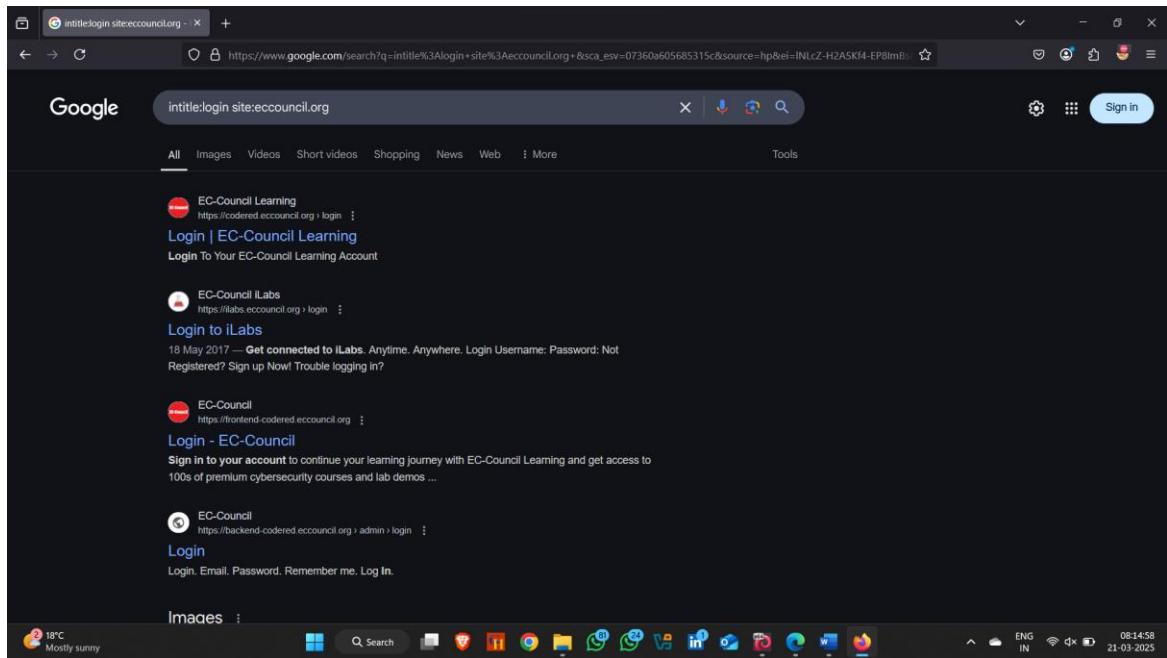
- Searching Cached Pages
- Finding Exposed Directories
- Extracting Metadata from Files
- Identifying Sensitive Information
- Gathering Email Addresses
- Discovering Subdomains
- Checking Indexed Pages

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**.

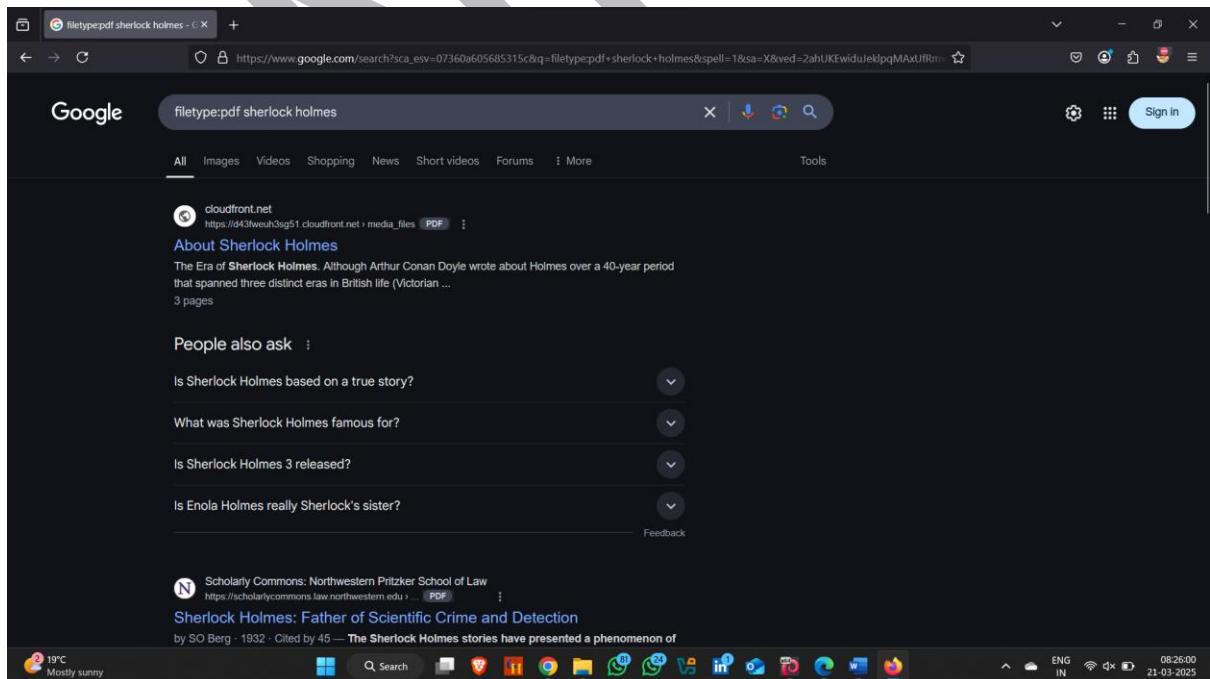
The **site:** keyword is a powerful search operator used in search engines like Google to restrict search results to a specific website or domain.



- **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.

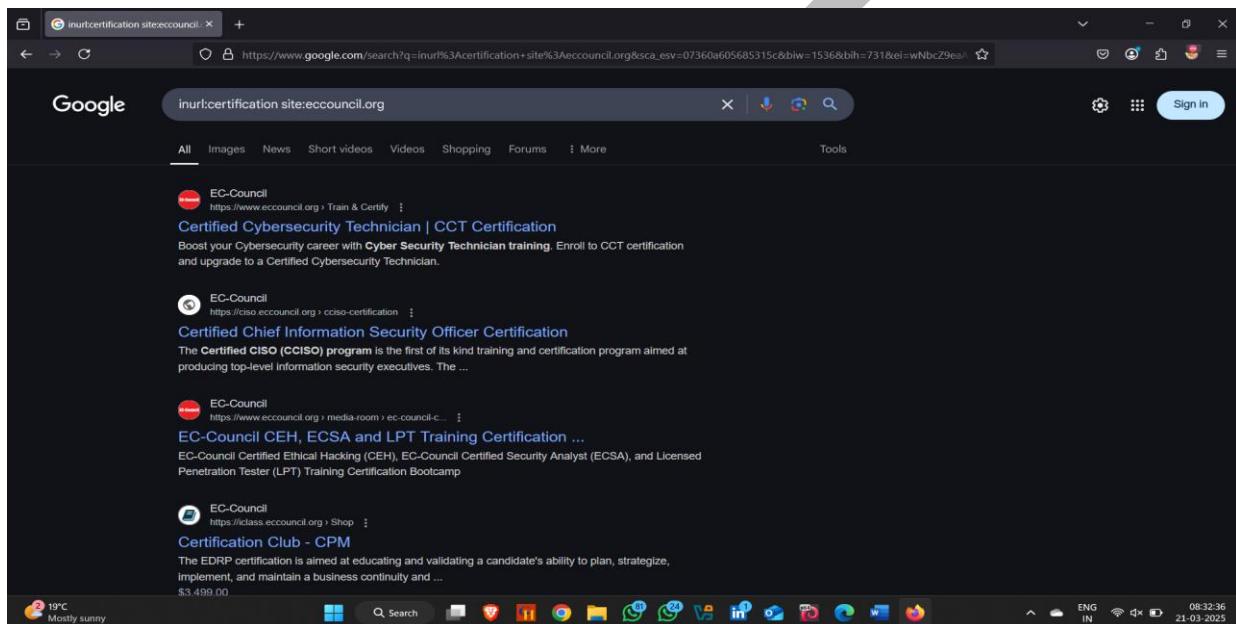
Note:- You can also give other filetypes like .XLS , .DOCX



- 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

Google

intitle:index of bollywood movies

All Videos Images Short videos Shopping Forums News More Tools

MOVIE CITY- http://103.145.232.246 › Data › movies › Bollywood › Index of /Data/movies/Bollywood/2024/

Index of /Data/movies/Bollywood/2024/ . J Aakir Palaayan Kab Tak.. (2024) 24-Feb-2024 15:16 - Ayushmati Geeta Matric Pass (2024) 25-Oct-2024 17:57 ...

MOVIE CITY- http://103.145.232.246 › Data › movies › Bollywood › Index of /Data/movies/Bollywood/

Index of /Data/movies/Bollywood/ .. 2000/ 10-Nov-2023 16:48 - 2007/ 21-Nov-2023 17:49 - 2008/ 21-Nov-2023 17:54 - 2011/ 11-Nov-2023 18:49 - 2012/ ...

103.102.136 http://103.102.136.106 › ftp › Movies › hindi-03 › Index of /ftp/cmclftp1/Movies/hindi-03

Index of /ftp/cmclftp1/Movies/hindi-03 ; [VID], Bunker-Hindi.mkv, 2020-07-30 06:00 ; [VID], Chhalang 2020 Hindi.mkv, 2020-11-18 10:10 ; [VID], Chhichhore.mp4 ...

MemsaabStory https://memsaabstory.com › hindi-film-index › Filmi Index (Alphabetical)

I - Ijaazat (1987) · Immaan Dharam (1977) · Imtihan (1974) · Insaniyat (1955) · Intaqam (1969) · International Crook (1974) · In Which Annie Gives It Those Ones (1989) ...

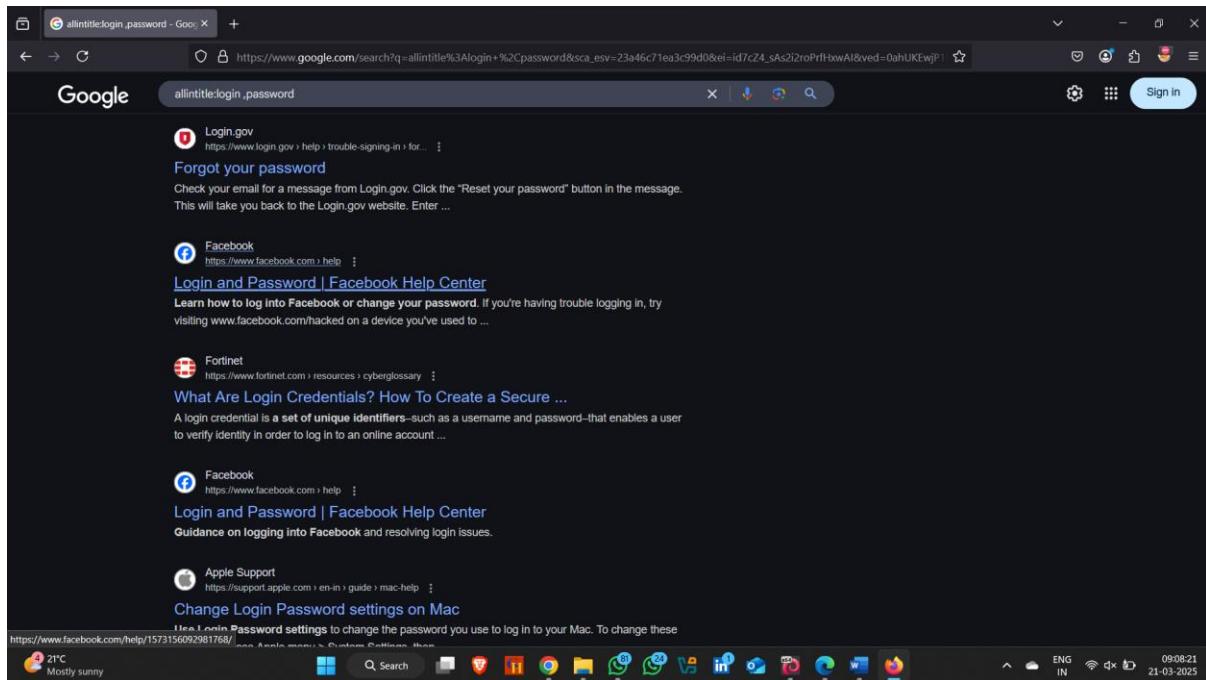
Sports headline Chinese Grand P... ENG IN 08:39:47 21-03-2025

Index of /Data/movies/Bollywood/2024/

Movie Title	Release Date	Notes
Aakhir Palaayan Kab Tak.. (2024)	24-Feb-2024 15:16	-
Ayushmati Geeta Matric Pass (2024)	25-Oct-2024 17:57	-
Accident or Conspiracy Godhra (2024)	14-Nov-2024 13:30	-
Adhunik (2024)	21-Sep-2024 10:30	-
Ae Watan Meri Watan (2024)	22-Mar-2024 18:44	-
Agni (2024)	06-Dec-2024 15:49	-
All India Rank (2023)	21-Jun-2023 13:54	-
Amar Akbar Prem Kahani (2024)	05-Oct-2024 11:48	-
Amar Singh Chauhan (2024)	14-Apr-2024 18:33	-
Article 370 (2024)	24-Feb-2024 15:21	-
Auron Mein Kahin Dum Tha (2024)	13-Aug-2024 13:24	-
Baby John (2024)	28-Dec-2024 06:54	-
Bad News (2024)	28-Jul-2024 18:34	-
Bade Mian Chote Miyan (2024)	14-Jun-2024 08:46	-
Bande Singh Chaudhary (2024)	02-Nov-2024 08:11	-
Barstar: The Naval Story (2024)	22-Mar-2024 18:47	-
Barstar: The Naval Story/	17-Mar-2024 16:54	-
Bhaiyya Ji (2024)	25-May-2024 15:49	-
Bhakshak (2024)	17-Feb-2024 02:56	-
Bholi Bhulaiya 3 (2024)	02-Nov-2024 08:31	-
Blackmail (2024)	09-Jun-2024 19:31	-
Bodyguard (2024)	28-Jul-2024 19:21	-
CTRL (2024)	05-Oct-2024 17:55	-
Chalti Rahe Zindagi (2024)	28-Jul-2024 19:23	-
Chandu Champion (2024)	22-Jun-2024 22:36	-
Chhota Bheem And The Curse Of Damyaan (2024)	03-Aug-2024 15:11	-
Chota Number (2020)	22-Jun-2024 22:43	-
Craek! Reesa... Toh Jiyegaa (2024)	29-Feb-2024 14:44	-
Cress (2024)	29-Mar-2024 23:53	-
Curry & Cyanide The Jolly Joseph Case (2023)	28-Jan-2024 17:44	-
Dange (2024)	05-Mar-2024 16:51	-
Dashai (2024)	28-Dec-2024 17:14	-
Dadhi Bipha Zameen (2024)	01-Jun-2024 23:18	-
Desi Doctor (2024)	14-Jun-2024 03:07	-
Do Aankhen Barah (2024)	27-Apr-2024 11:37	-
Do Patti (2024)	02-Nov-2024 08:56	-
Double Tsmart (2024)	17-Aug-2024 15:59	-
Dunk! (2023)	17-Feb-2024 03:50	-
Ek Aariajan Rishtey Ka Guilt 3 (2024)	11-May-2024 21:03	-
Fighter (2024)	30-Jan-2024 11:37	-
Ghudchadi (2024)	13-Aug-2024 13:28	-
Guillotine Girls (2024)	20-Jun-2024 18:07	-

Watchlist Ideas ENG IN 08:41:14 21-03-2025

- 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:

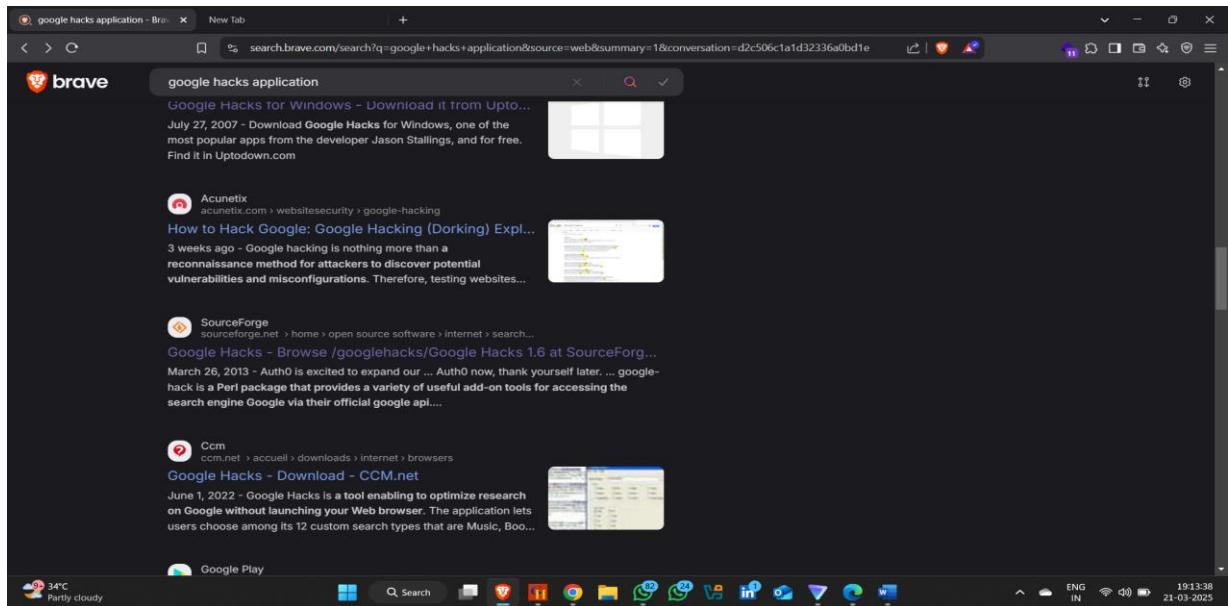
🔍 cybersecurity event location:Mumbai

➡ Lists news articles or content relevant to Mumbai.

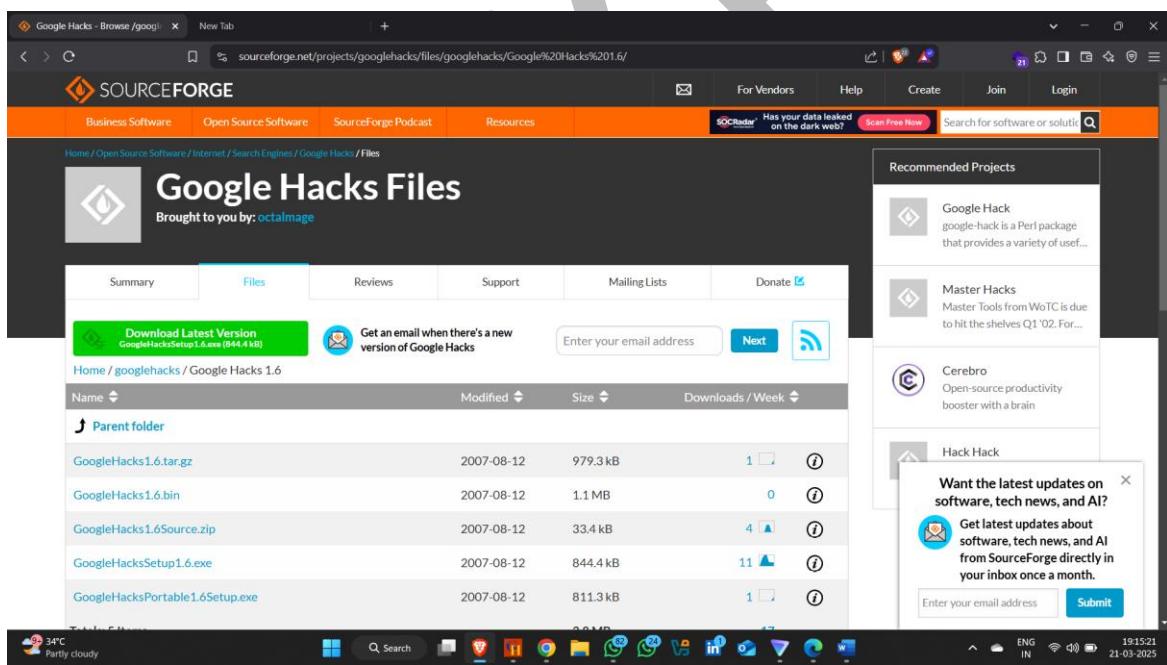
2. Gather Information Using Googlehacks application

Step 1 - : search Google hacks application

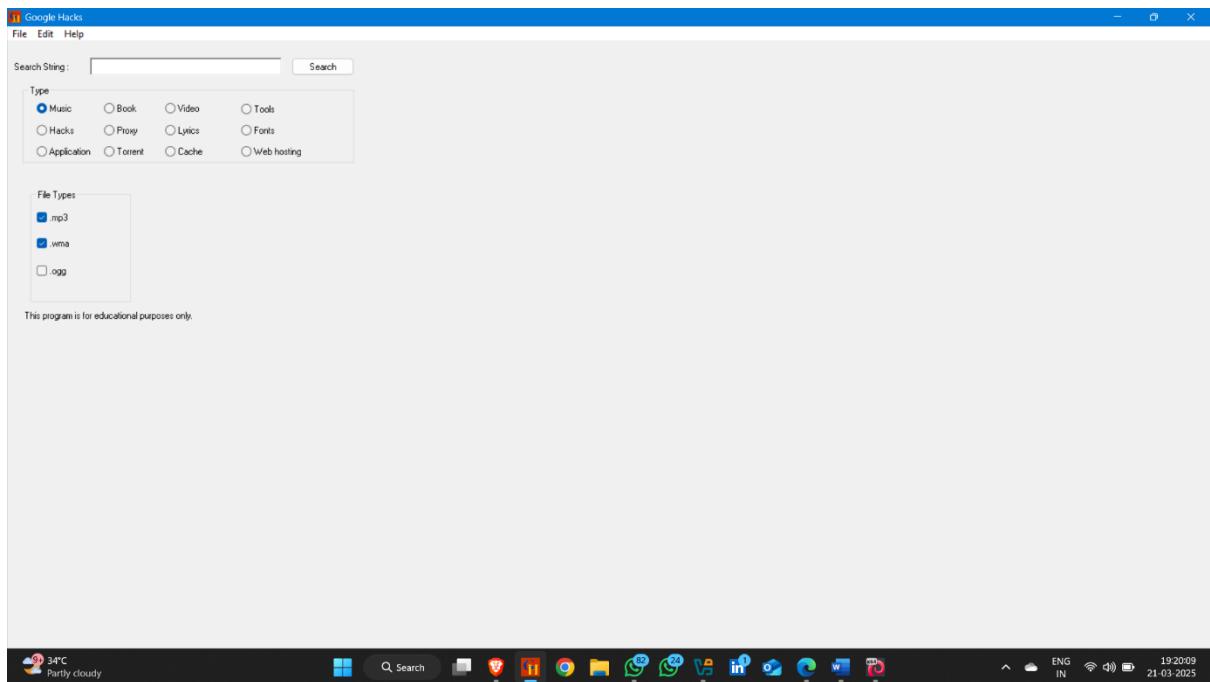
Step 2 -: open sourceforge Website



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



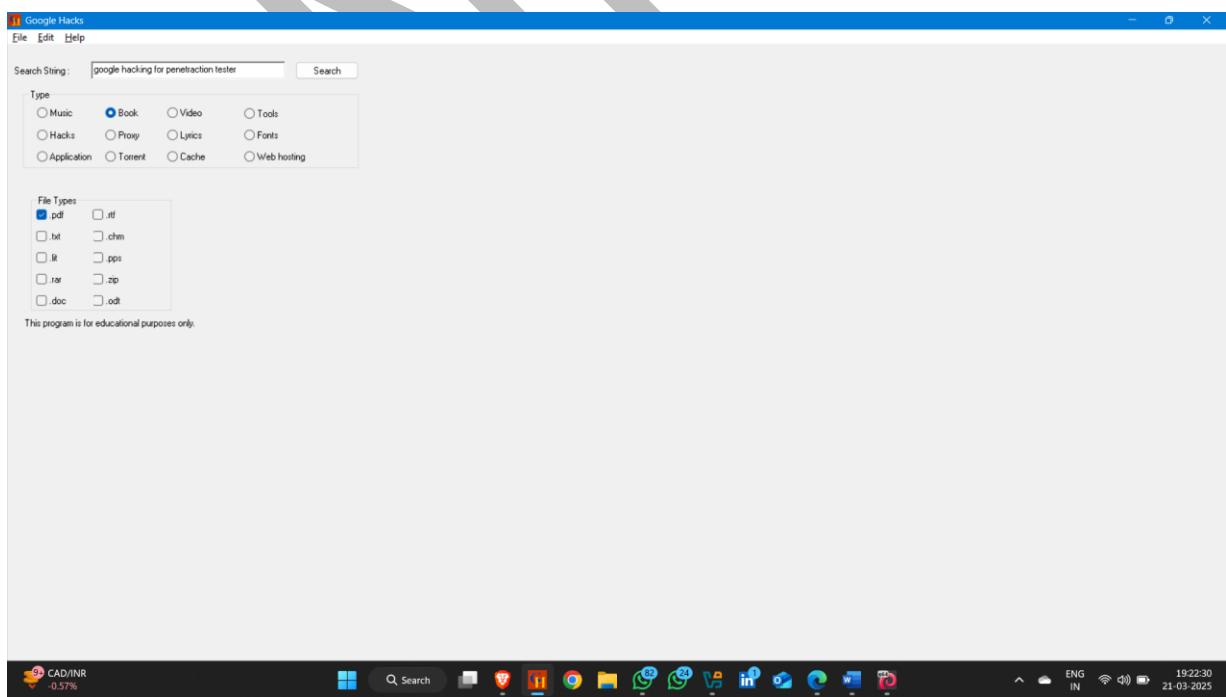
Step 4 :- After Download the application , install and open application



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

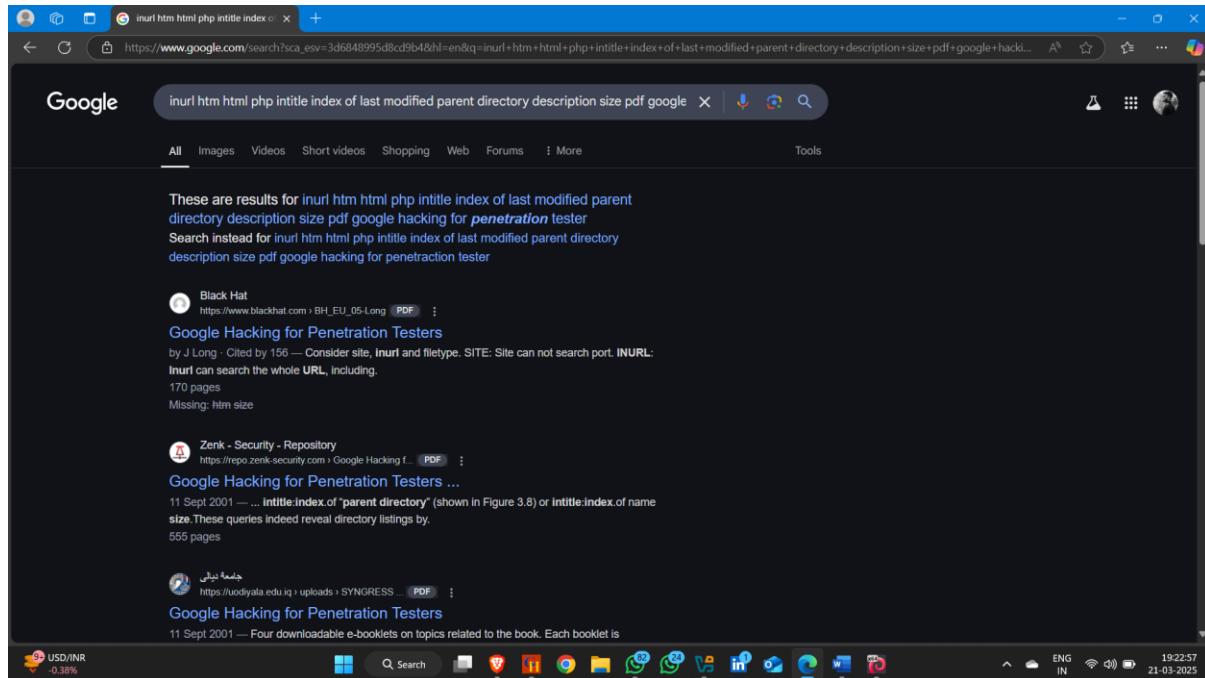
For Example – Search a book

- 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



A

2.EMAIL FOOTPRINTING

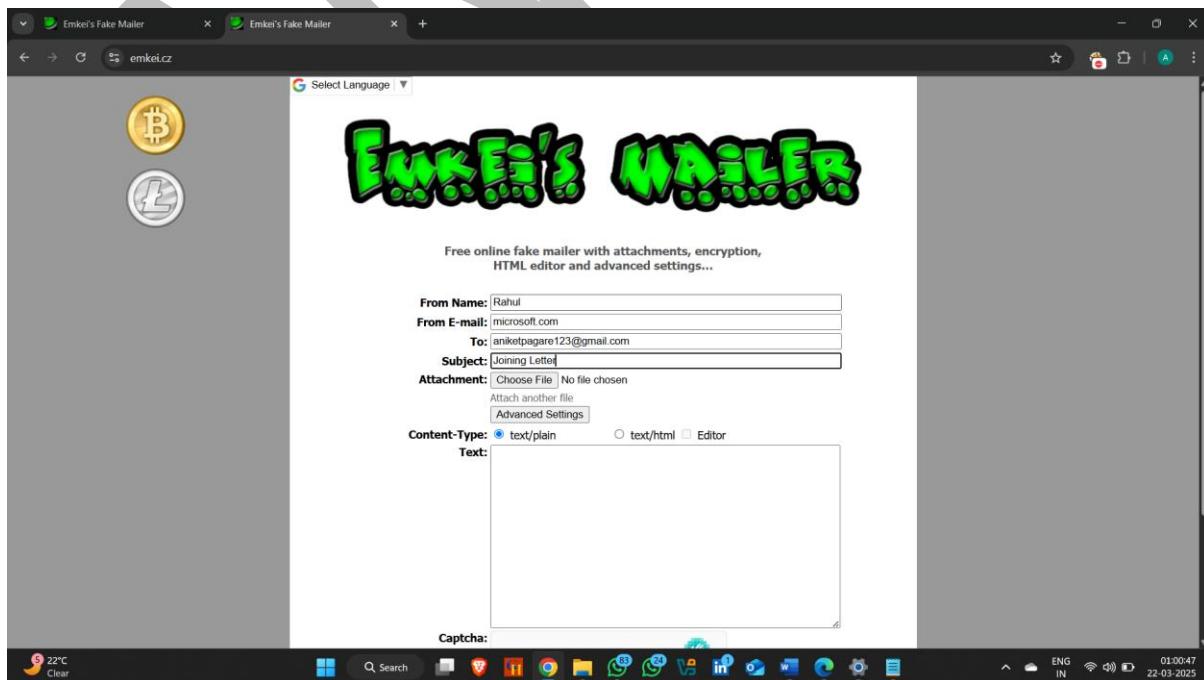
Email footprinting refers to the process of tracking and analyzing details about an email's origin, path, and related metadata to gather information about the sender or the infrastructure used to send the email.

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

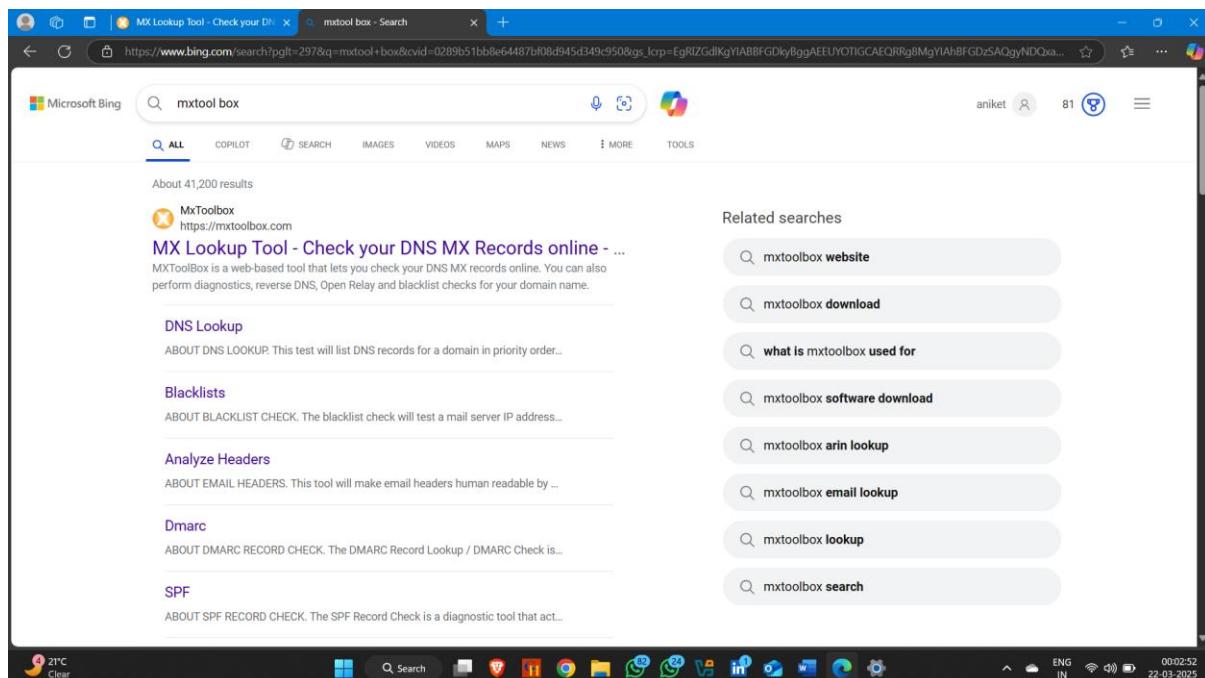


2.Email Footprinting using MX- TOOL BOX –

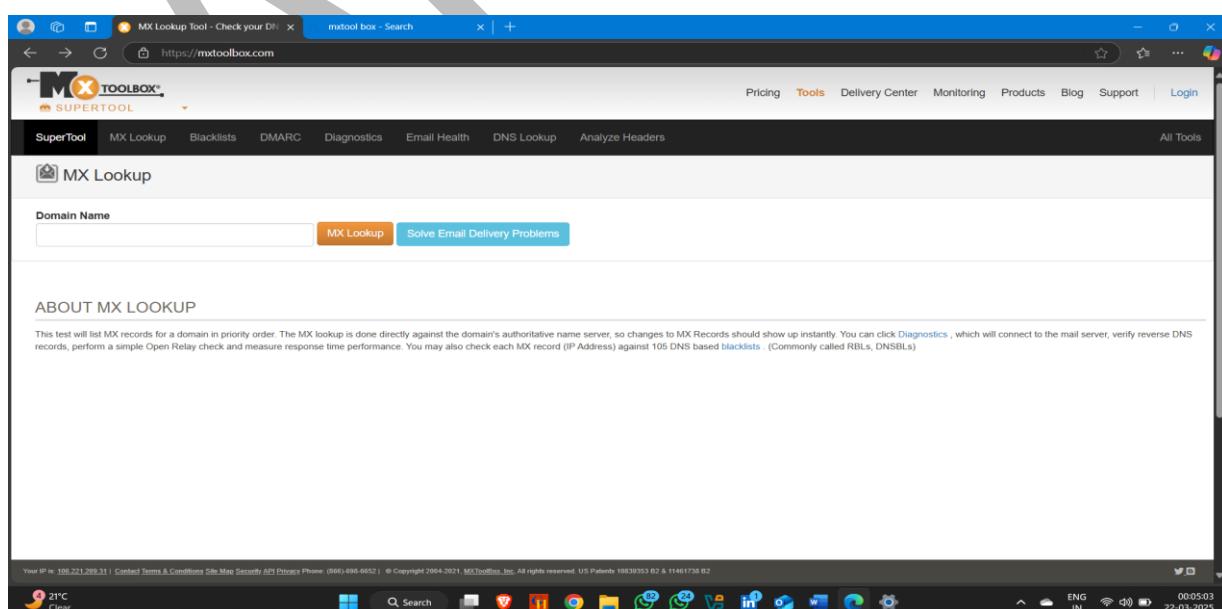
mxtool box are used to check received email are original or fake.

Step 1 :-: Search mx tool box on browser.

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



Step 3 :-: Click on Analyze Headers .



The screenshot shows a Microsoft Edge browser window with the URL <https://mxtoolbox.com/EmailHeaders.aspx>. The page is titled "Email Header Analyzer" and features a large text input field labeled "Paste Header:" with a placeholder "Paste Header". Below the input field is a "Analyze Header" button. At the top of the page, there's a navigation bar with links for Pricing, Tools, Delivery Center, Monitoring, Products, Blog, Support, and Login. The "Tools" menu is currently selected. A secondary navigation bar below the main one includes links for SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. The "Analyze Headers" link is highlighted. The bottom of the page contains a section titled "ABOUT EMAIL HEADERS" with a brief description and a note about the tool's purpose.

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.

The screenshot shows a Gmail inbox with a message from "Pagare Aniket Sunil, Study Abroad Without Financial Worries: Credila Has You Covered!". The message was sent on "Tue, Mar 11, 11:38PM (11 days ago)". A context menu is open on the right side of the message, listing options such as Reply, Forward, Filter messages like this, Print HTML message, Delete this message, Block "Credila", Report spam, Report phishing, Show original, Download message, Show HTML message, and Mark as unread. The message content itself is an advertisement for Credila, featuring a woman holding books and a red "APPLY NOW!" button.

- Copy entire header

```

Received: by 2002:a05:7810:3a03:bd:441157d:20a9 with SMTP id q19csp2035672mii;
Tue, 11 Mar 2025 11:08:55 -0700 (PDT)
X-Google-Smtp-Source: AGHfTgjueKsbaJ2zotwII6xvosv7UBom/nA4/jy/JVFauK/U6w7310nw6wCpmI/wlpGf6jJk0n
X-Received: by 2002:a05:6200:78f1:bd:441157d:7c5:c45:ca5b with SMTP id af79cd13be357-7c55cc4cc98mr682655585a.12.174171653324;
Tue, 11 Mar 2025 11:08:55 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
h=mime-version:feedback-id:list-unsubscribe:list-unsubscribe-post-
:message-id:subject:reply-to:from:to:dkim-signature
:dkim-signature;
bh=11nnmWVqB8+SuVMUzVA51v1gTqpvvVkrDs+10rXDsda1lwRfjoc56sAbbaVm5ir
fh=PlcaFtvwzv1puFfP99Q0cxKh0Tvdf1c13AS0ND120L0u;
bgBtJvyoDz2818gBfZ0a2/3C5gvpsQTG0002KFsyny2P0f040EYyJ5ANU1QArYzPH
KAx6i3SPNC1N@q4CzfzxK+6+2pUpTJRf2oh/1deSuccJ0jXYvLyAz2p1D1OxbpTsI
h9dkIyimxTypeAggb9k3k/f456FBuHE9mbbvvtLg1+bj9a1bxK1SVE41FgqowehM
X/HNGRQ8fRN10871t2nzmPjFxFe2d0+Nv8u4wE/qJvpfBLF8D04o9dlwStL1xb
SE1R0nDpsob5fbrc1/ljjsCnnyt8+vDmy+c5z2vVab9pn04goJwq4Z+66zzDpgsP
wcfw=-;
dara@google.com
ARC-Authentication-Results: i=1; mx.google.com;
dkim-pass header.i=@mailer.credila.com.header.s=nce2048.header.b=c6PTmr6e;
dkim-pass header.i=@ncm14.com.header.s=eme.header.b=Cnh4lQ0J;
spf=pass (google.com) client-ip=202.162.239.19; mfrom=mail.campaign-hdfcredi...
202.162.239.19 as permitted sender; mfrom=mail.campaign-hdfcredi...
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=credila.com
Return-Path: <campaign-hdfcredi...>181107-1425001-1948428-i-e@gmail.com@ncdelivery.mailer.credila.com>
Received: from pmta2.in-23919.ncm14.com (pmta2.in-23919.ncm14.com [202.162.239.19])
by mx.google.com with ESMTPS id af79cd13be357-059si1756984185a.555.2025.03.11.11.08.55
for <aniketpagare2024@gmail.com>
Version:TLS1.3 cipher:TLS-AES_128_GCM_SHA256 bits:128(128);
Tue, 11 Mar 2025 11:08:55 -0700 (PDT)
Received-SPF: pass (google.com domain of campaign-hdfcredi...181107-1425001-1948428-i-e@gmail.com@ncdelivery.mailer.credila.com designates
202.162.239.19 as permitted sender) client-ip=202.162.239.19;
Authentication-Results: mx.google.com;
dkim-pass header.i=@mailer.credila.com.header.s=nce2048.header.b=c6PTmr6e;
dkim-pass header.i=@ncm14.com.header.s=eme.header.b=Cnh4lQ0J;
spf=pass (google.com) client-ip=202.162.239.19; mfrom=mail.campaign-hdfcredi...
202.162.239.19 as permitted sender; mfrom=mail.campaign-hdfcredi...
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=credila.com

```

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

Email Header Analyzer

Header:

```
<!--[if mso | IE]>
<table align="center" border="0" cellpadding="0" cellspacing="0" class="" style="width: 700px; width:700" >
<br>
<td style="line-height:0px;font-size:0px;mso-line-height-rule:exactly;">
<![endif]-->
<div id="DIV23321217" class="" data-class="smt-element" style="text-align: center; font-size: 0px;padding: 0px;">
<table align="center" border="0" cellpadding="0" cellspacing="0" role="presentation" style="text-align: center; font-size: 0px; border: none; width: 100%;">
<tbody>
<br>
<td style=" ">
```

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.

Your IP is 106.221.212.42 | [Contact](#) [Terms & Conditions](#) [Site Map](#) [Security API](#) [Privacy Policy](#) (066)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10039353 B2 & 11461738 B2

Now you see that type result --

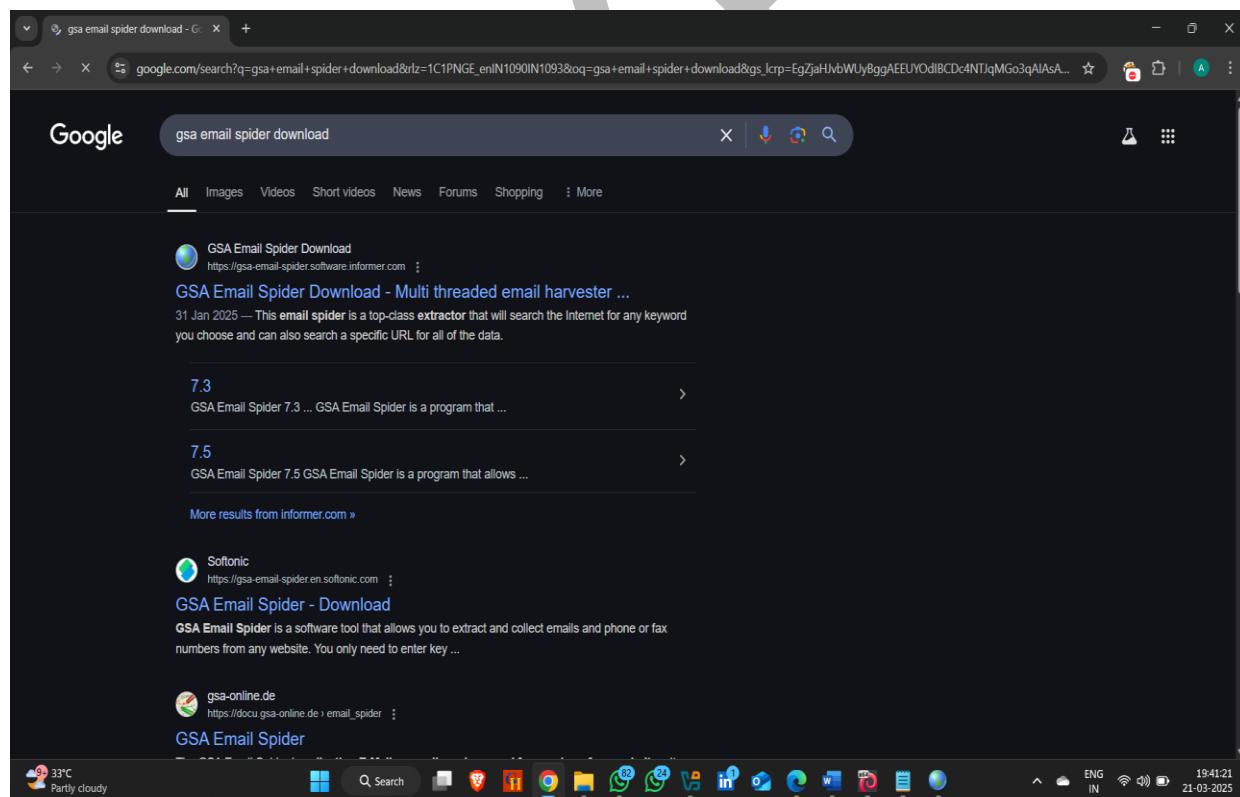
SPF	PASS with IP 202.162.239.19 Learn more
DKIM	'PASS' with domain mailer.credila.com Learn more
DMARC	'PASS' Learn more

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

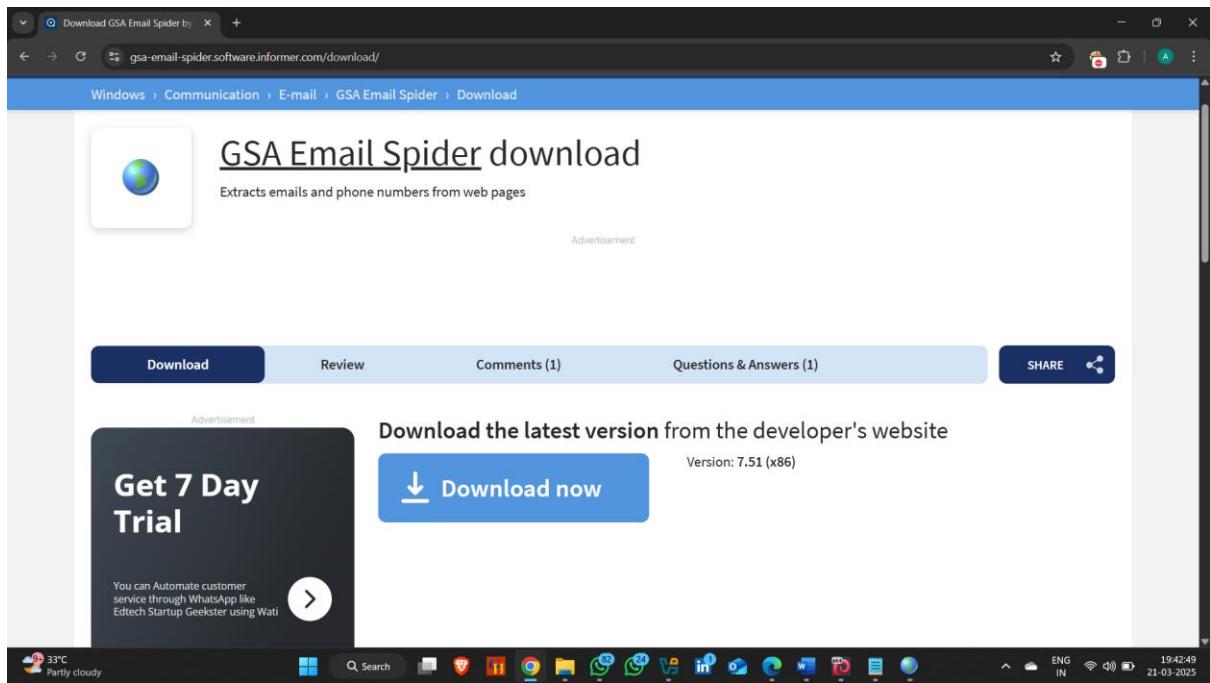
3.Email Footprinting Using GSA Email Spider Application :-

Installation Process :-

Step 1 :- Search GSA Email Spider On Browser



Step 2 :- click on first Website



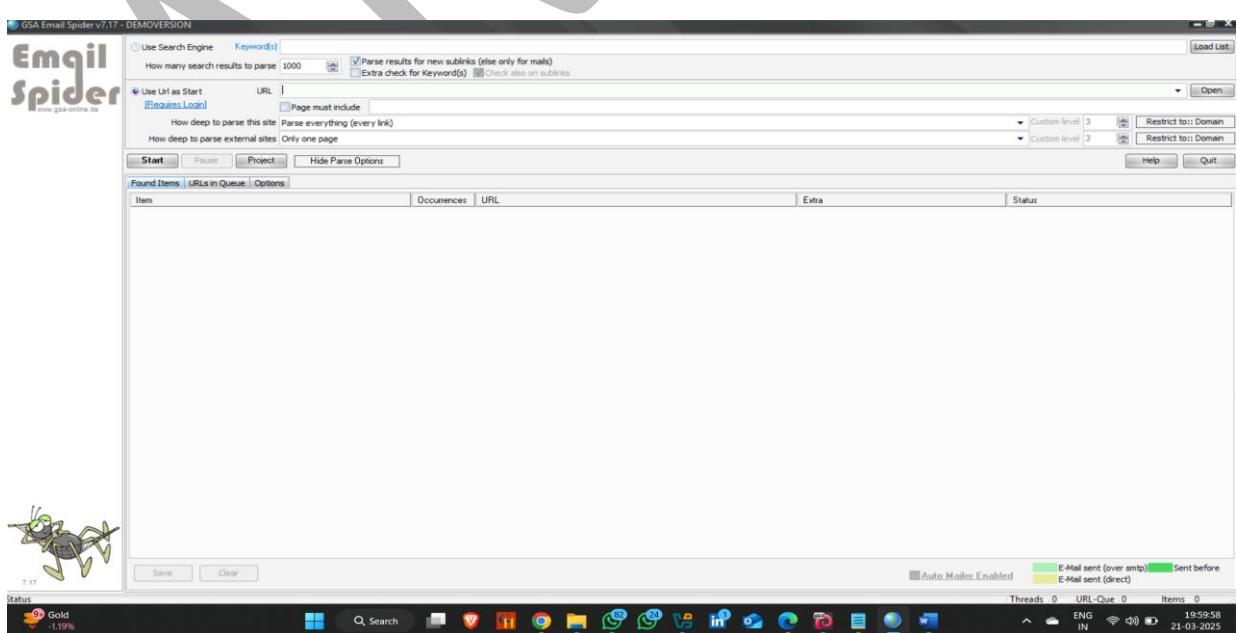
Step 3 :- click on Download and Download it .

After completing installation process then setup the app

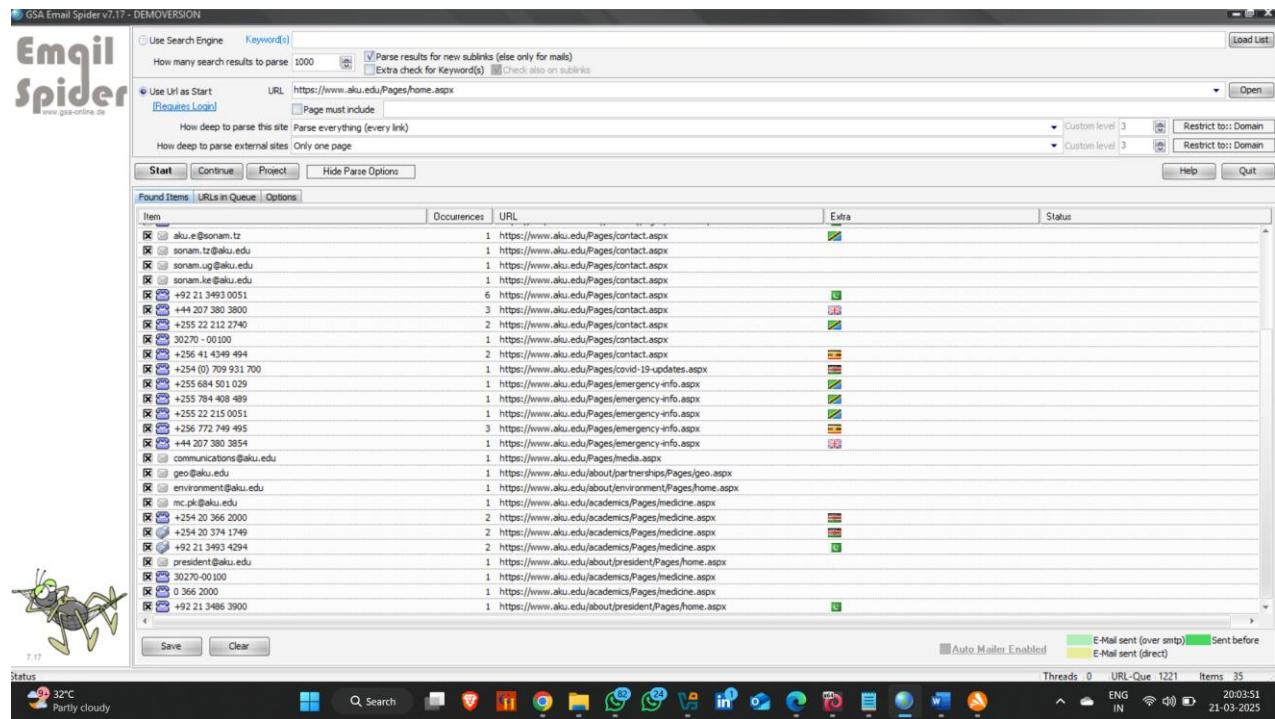
Step 4 :- Copy url that you want to perform email footprinting

Step 5 :- Paste URL in url section.

Step 6 :- Click on Start button.



Step 7 :- Then you see the result



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:-

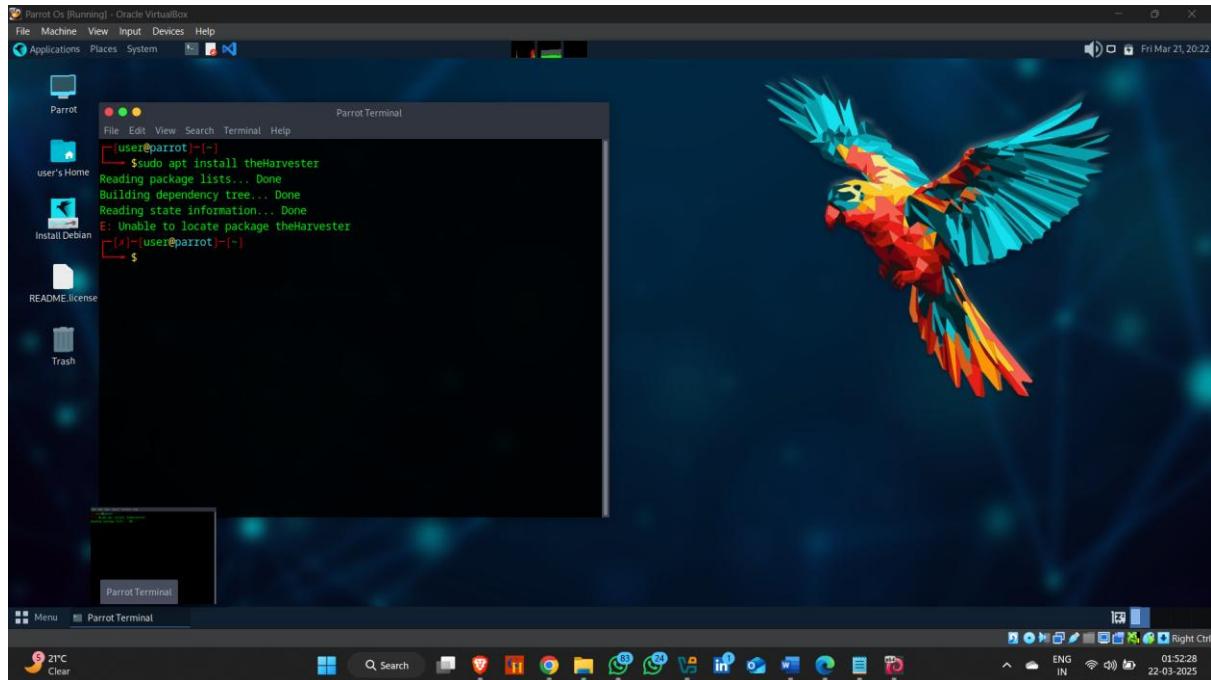
- 1.Identifying domain information (WHOIS lookup).
 2. Finding subdomains.
 3. Extracting DNS records (A, MX, NS, TXT, etc.).
 4. Discovering IP addresses of target servers.
 5. Performing reverse DNS lookups.
 6. Exploiting DNS zone transfers (if misconfigured)
- Types of DNS Records -: DNS Records 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

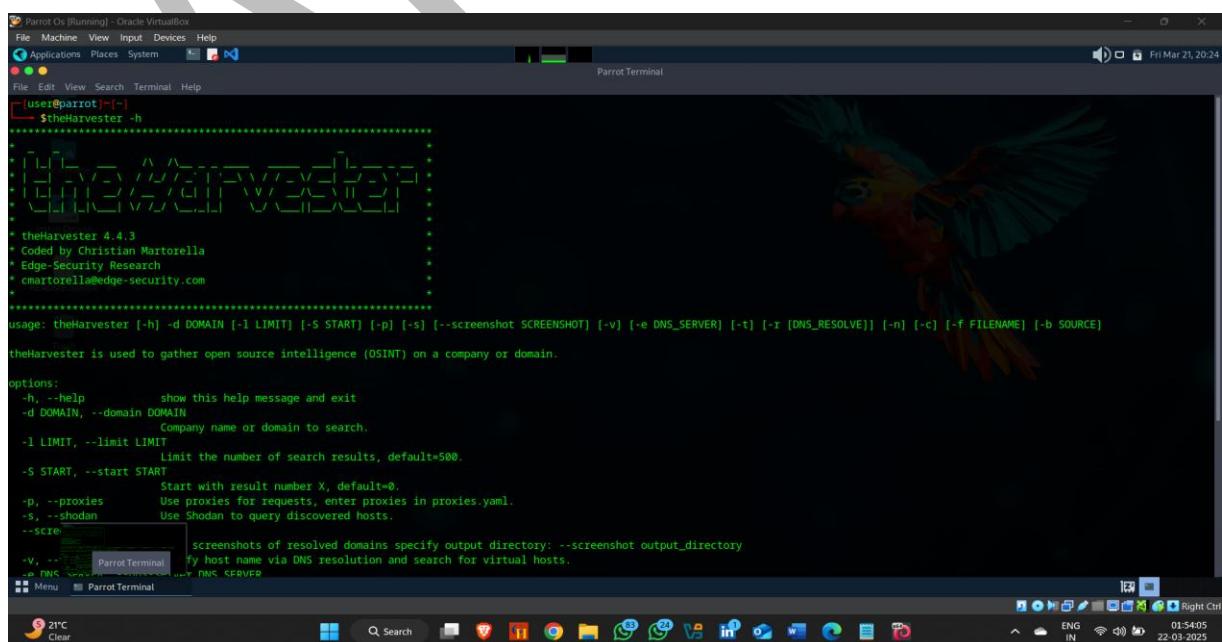
1. DNS Footprinting Using TheHarvester (CLI Tool)

TheHarvester install process –

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

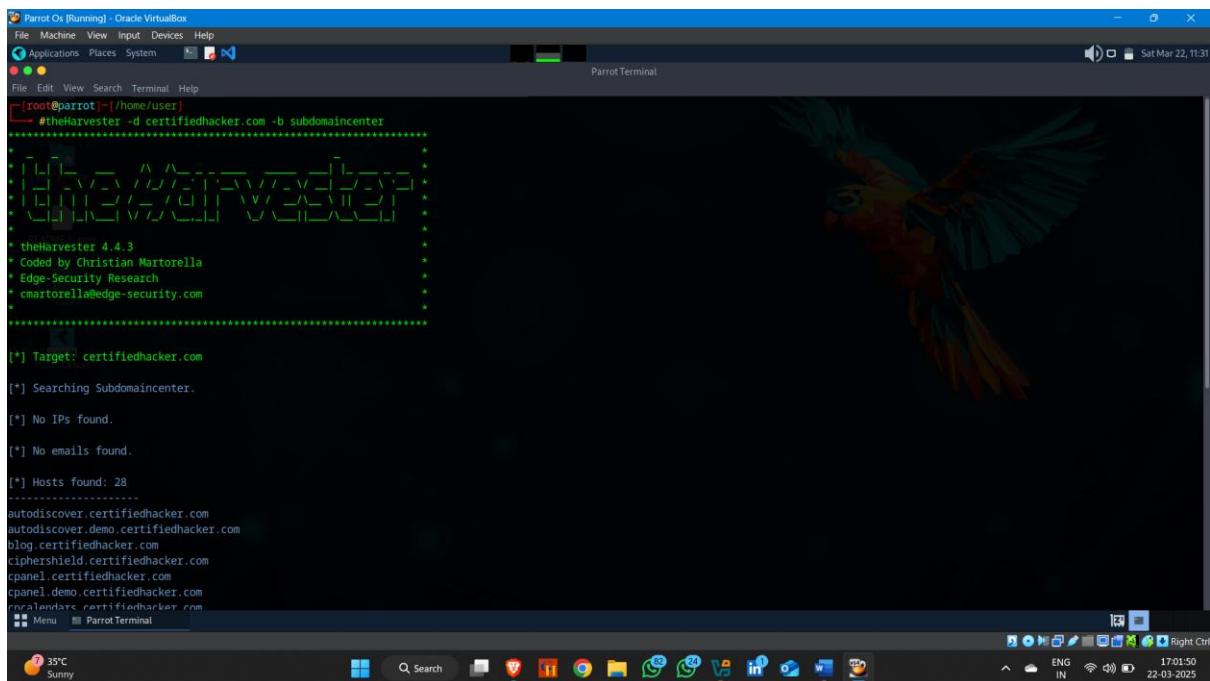


3. Search theHarvester -h (-h = help)



Commands –

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



The screenshot shows a terminal window titled "Parrot Os [Running] - Oracle VirtualBox" running on Parrot OS. The terminal is executing the command: "#theHarvester -d certifiedhacker.com -b subdomaincenter". The output of the command is displayed in green text. It includes the version information for theHarvester (4.4.3), the target domain (certifiedhacker.com), and a list of 28 hosts found, such as autodiscover.certifiedhacker.com, blog.certifiedhacker.com, and cpanel.certifiedhacker.com. The terminal window is set against a background of a colorful parrot logo.

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



```
Parrot Os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
Auto capture keyboard ...
Mouse integration ...
[root@parrot]~[/home/user]
# dig ns certifiedhacker.com

; <>> DIG 9.18.28-1-deb12u2-Debian <>> ns certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 21265
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com. IN NS

;; ANSWER SECTION:
certifiedhacker.com. 86400 IN NS ns2.bluehost.com.
certifiedhacker.com. 86400 IN NS ns1.bluehost.com.

;; Query time: 240 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sat Mar 22 18:51:34 UTC 2025
;; MSG SIZE rcvd: 93

[root@parrot]~[/home/user]
#
```

- Using mx records



```
Parrot Os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
Sun Mar 23, 10:36
[root@parrot]~[/home/user]
# dig mx certifiedhacker.com

; <>> DIG 9.18.28-1-deb12u2-Debian <>> mx certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 3109
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com. IN MX

;; ANSWER SECTION:
certifiedhacker.com. 14400 IN MX 0 mail.certifiedhacker.com.

;; ADDITIONAL SECTION:
mail.certifiedhacker.com. 14400 IN A 162.241.216.11

;; Query time: 326 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sun Mar 23 10:36:48 UTC 2025
;; MSG SIZE rcvd: 85

[root@parrot]~[/home/user]
#
```

- Using txt records



```
Parrot Os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
[root@parrot]~[/home/user]
[root@parrot]# dig txt certifiedhacker.com

; <>> DIG 9.18.28-1-deb12u2-Debian <>> txt certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 48108
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      TXT

;; ANSWER SECTION:
certifiedhacker.com. 14400  IN      TXT      "v=spf1 a mx ptr include:bluehost.com ?all"

;; Query time: 346 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sun Mar 23 10:38:44 UTC 2025
;; MSG SIZE rcvd: 102

[root@parrot]~[/home/user]
[root@parrot]#
```

- Using SOA records



```
Parrot Os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
[root@parrot]~[/home/user]
[root@parrot]# dig SOA certifiedhacekr.com

; <>> DIG 9.18.28-1-deb12u2-Debian <>> SOA certifiedhacekr.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 18176
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1280
;; QUESTION SECTION:
;certifiedhacekr.com.      IN      SOA

;; AUTHORITY SECTION:
com.          900   IN      SOA     a.gtld-servers.net. nstld.verisign-grs.com. 1742726357 1800 900 604800 900

;; Query time: 439 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sun Mar 23 10:39:35 UTC 2025
;; MSG SIZE rcvd: 121

[root@parrot]~[/home/user]
[root@parrot]#
```

- Using AXFR zone transfer

```
[root@parrot]~[~/home/user]
# dig SOA certifiedhacekr.com

; <>> DIG 9.18.28-1-debian2u2-Debian <>> SOA certifiedhacekr.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NODATA, id: 18176
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacekr.com. IN SOA

;; AUTHORITY SECTION:
com. 900 IN SOA a.gtld-servers.net. nstld.verisign-grs.com. 1742726357 1800 900 604800 900

;; Query time: 439 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sun Mar 23 10:39:35 UTC 2025
;; MSG SIZE rcvd: 121

[root@parrot]~[~/home/user]
# dig @a.gtld-servers.net. certifiedhacker.com axfr

; <>> DIG 9.18.28-1-debian2u2-Debian <>> @a.gtld-servers.net. certifiedhacker.com axfr
; (2 servers found)
;; global options: +cmd
; Transfer failed.
[root@parrot]~[~/home/user]
```

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**'

Parrot Os [Running] - Oracle VirtualBox

```
[root@parrot] ~
File Machine View Input Devices Help
Applications Places System
Parrot Terminal
root@parrot:~# apt install sublist3r
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
sublist3r
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 620 kB of additional disk space will be used.
Get:1 https://deb.parrot.sh/parrot lory/main amd64 sublist3r all 1.1-3 [620 kB]
Fetched 620 kB in 3s (198 kB/s)
```

35°C Sunny

17:32:55 22-03-2025

Commands for sublist3r - -

- **man sublist3r - - to show all description about sublist3r**

Parrot Os [Running] - Oracle VirtualBox

```
sublist3r(1) tool designed to enumerate subdomains of websites using OSINT sublist3r(1)
NAME
sublist3r - tool designed to enumerate subdomains of websites using OSINT
SYNOPSIS
sublist3r [ARGS] ...
DESCRIPTION
This package contains a Python security tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting over the network. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS.
Subbrute was integrated with Sublist3r to increase the possibility of finding more subdomains using brute-force with an improved wordlist.
OPTIONS
-h, --help
Show this help message and exit
-d DOMAIN, --domain DOMAIN
Domain name to enumerate it's subdomains
-b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
Enable the subbrute bruteforce module
-p PORTS, --ports PORTS
Scan the found subdomains against specified TCP ports
-v [VERBOSE], --verbose [VERBOSE]
Enable verbosity and display results in realtime
Manual page sublist3r(1) line 1 (press h for help or q to quit)
```

35°C Sunny

17:35:54 22-03-2025

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

```

Parrot Os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
Sat Mar 22, 12:07
[root@parrot] ~ /home/user]
# sublist3r -d certifiedhacker.com -b
[+] Enumerating subdomains now for certifiedhacker.com
[+] Searching now in Baidu..
[+] 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..
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/sublist3r.py", line 269, in run
    domain_list = self._enumerate()
                  ^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self._get_csrftoken(resp)
            ^^^^^^^^^^^^^^
[root@parrot] ~ /home/user]

```

4.DNS Footprinting using WHOIS (GUI) –

How to do it -

- Open Browser.
- Search WHOIS

WHOIS Search, Domain Name: +

Premium Domains Transfer Features Login Sign Up

who.is

WHOIS Search, [Domain Name](#), Website, and IP Tools

Domain names or IP addresses...

Your IP address is [106.221.212.42](#)

Looking to get a website? [Web Hosting](#) [Website Builder](#) [SSL Certificates](#)

See Website Information [On Demand Domain Data](#) [Register Domain Names](#)

Search the whois database, look up domain and IP owner information, and check out dozens of other statistics.

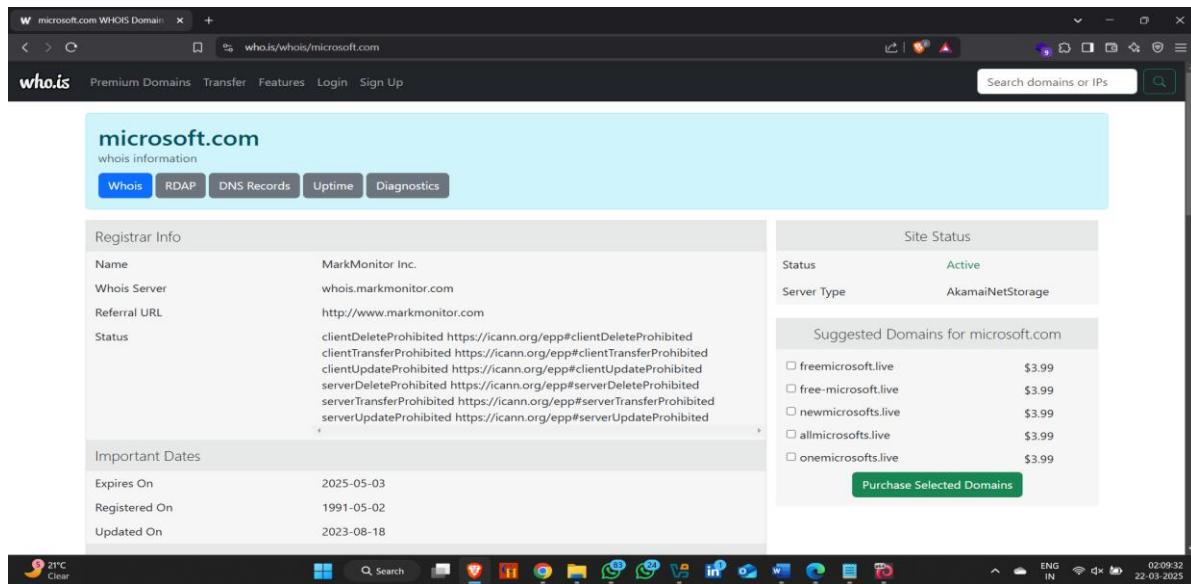
Get all the data you need about a domain and everything associated with that domain anytime with a single search.

Find a domain with the best domain registrar on the web. [Start your domain search at Name.com](#).

Transfers Premium Domains Web Hosting Website Builder Contact Us FAQs Terms of Service

27°C Clear ENG IN 02:08:19 22-03-2025

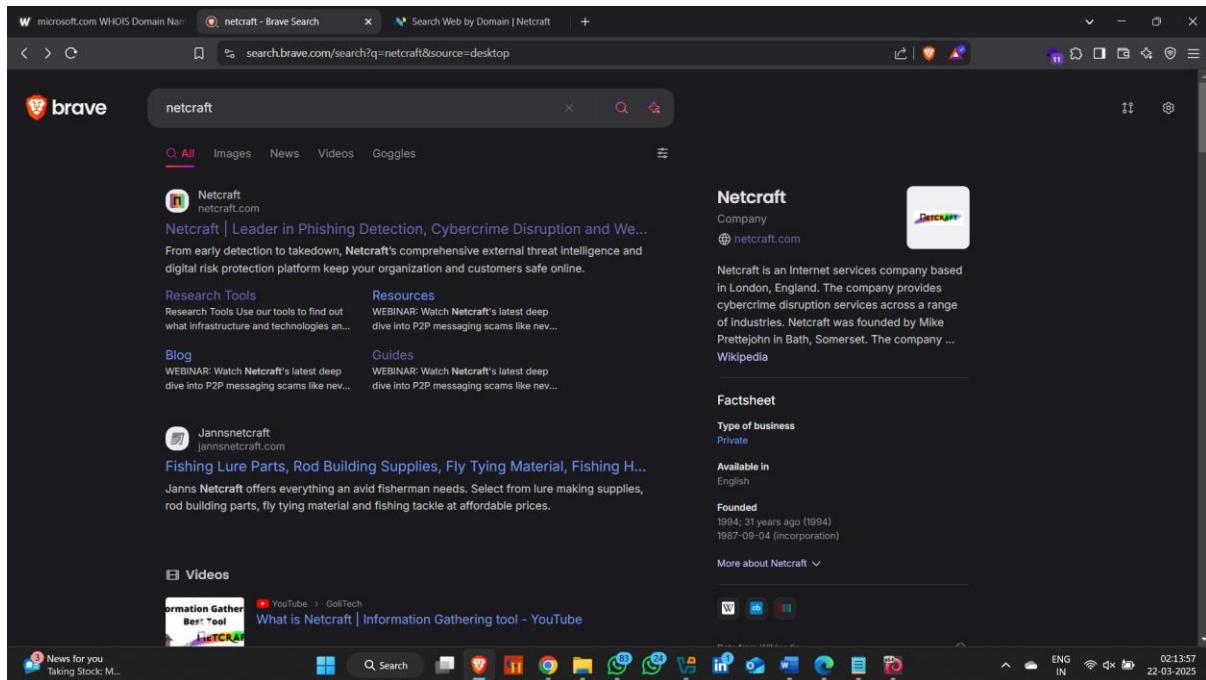
- Search Domain name or ip address.
- Search .



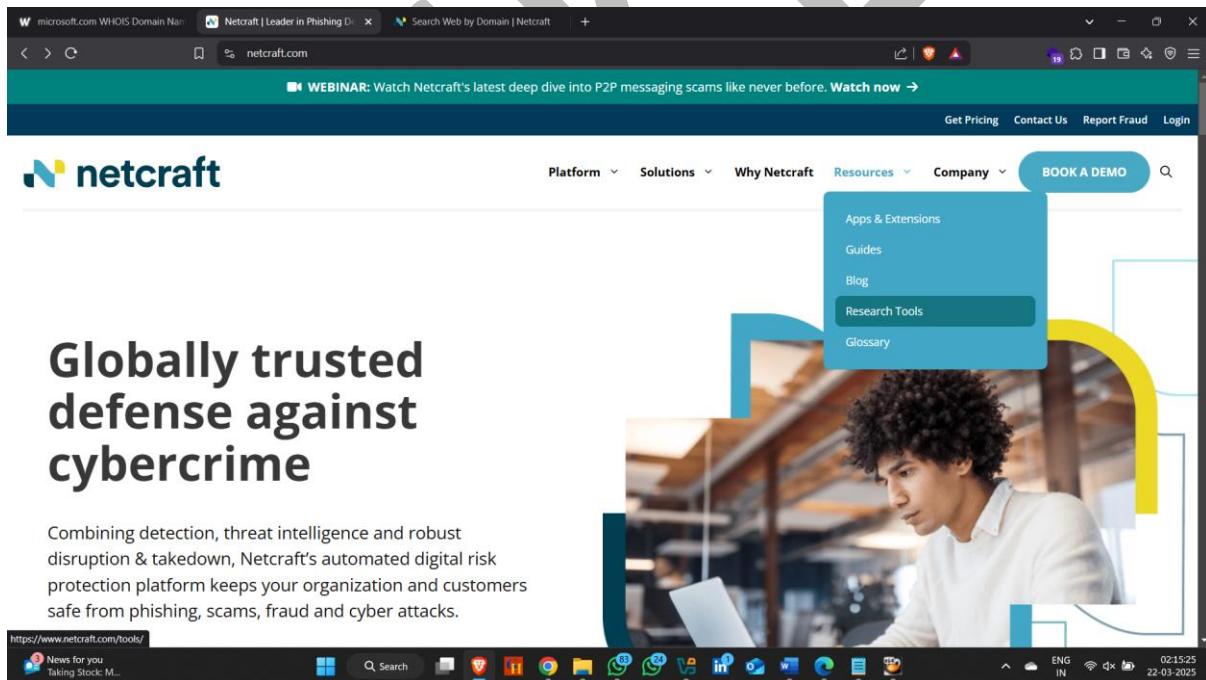
4. DNS Footprinting Using NetCraft (GUI) –

How to do it

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



- Click on Resources and click on research tools.



- Click on Search DNS

The screenshot shows the Netcraft Tools website. At the top, there are tabs for "microsoft.com WHOIS Domain Name", "Tools | Netcraft", and "Search Web by Domain | Netcraft". A banner at the top of the page reads "WEBINAR: Watch Netcraft's latest deep dive into P2P messaging scams like never before. Watch now →". Below the banner, there are navigation links for "Get Pricing", "Contact Us", "Report Fraud", and "Login". The main header features the "netcraft" logo and a search bar. A secondary navigation bar includes "Platform", "Solutions", "Why Netcraft", "Resources", "Company", and a "BOOK A DEMO" button. The main content area is titled "Research Tools" and contains a sub-section titled "Internet Research Tools". It features three circular icons: "Threat Map" (a hooded figure), "Site Report" (a computer monitor), and "Search DNS" (a server rack). The URL in the browser address bar is <https://www.netcraft.com/tools/#internet-research-tools>. The taskbar at the bottom of the screen shows various application icons.

- Provide Domain name.
- Click on search .

The screenshot shows the Netcraft Tools website. The top navigation bar includes "Google Translate", "Hacker Target Pty Ltd", "Have I Been Pwned: Check if your email has been compromised", "Tools | Netcraft", and "Search Web by Domain | Netcraft". Below the navigation, there are two buttons: "LEARN MORE" and "REPORT FRAUD". The main content area is titled "Search Web by Domain" and includes a sub-section titled "Explore websites visited by users of the Netcraft extensions". A search form is present, with a dropdown menu set to "Site contains" and the input field containing "microsoft.com". Below the input field is an example text: "Example: site contains .netcraft.com". There is a "SEARCH" button and a "Search tips" link. The URL in the browser address bar is <https://searchdns.netcraft.com>. The taskbar at the bottom of the screen shows various application icons.

microsoft.com WHOIS Domain Name | Tools | Netcraft Hostnames matching microsoft.com | Search Web by Domain | Netcraft

LEARN MORE REPORT FRAUD

Hostnames matching microsoft.com

▶ Search with another pattern?

489 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS	Site Report
52	learn.microsoft.com	July 2015	Akamai Technologies, Inc.	unknown	
53	www.microsoft.com	August 1995	Akamai Technologies	Linux	
62	teams.microsoft.com	November 2016	Microsoft Corporation	Windows Server 2008	
83	support.microsoft.com	October 1997	Akamai Technologies, Inc.	Linux	
157	admin.microsoft.com	September 2017	Microsoft Corporation	Windows Server 2008	

EUR/INR -0.72% 02:17:29 22-03-2025

5. DNS Footprinting Using DNS Dumster -

How to do it

Step 1 - Open your Browser .

Step 2 - Search DNS dumster .

DNSDumpster - Find & lookup dns records

dns recon & research, find & lookup dns records

Enter a Domain to Test

example.com

Start Test!

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.

22°C Clear 01:32:12 22-03-2025

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

Step 4 – click on start test.

The screenshot shows a web browser window titled "DNSDumpster - Find & lookup" with the URL "dnsdumpster.com". The main content is a table titled "A Records (subdomains from dataset)". The table has columns: Host, IP, ASN, ASN Name, Open Services (from DB), and RevIP. The data includes:

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
064-smtp-in-2a.microsoft.com	157.54.41.37	ASN 3598	MICROSOFT-CORP-AS		1
064-smtp-in-2a.microsoft.com	157.54.0.0/16		United States		
publisher-aircap1 TPP.microsoft.com	20.119.8.43	ASN 8075	MICROSOFT-CORP-MSN-AS-BLOCK	http: unknown server title: Microsoft Azure Web App - Error 404 https: unknown server title: Microsoft Azure Web App - Error 404 cn: azurewebsites.net o: Microsoft Corporation	43
LORM-CXP-Staging.microsoft.com	20.94.235.245	ASN 8075	MICROSOFT-CORP-MSN-AS-BLOCK	http: Apache title: POST data tech: Apache HTTP Server https: Apache title: LORM-CXP-Staging.microsoft.com cn: Microsoft Corporation tech: Apache HTTP Server	2
Minervavaultstg.microsoft.com	20.106.112.106	ASN 8075 20.64.0.0/10	MICROSOFT-CORP-MSN-AS-BLOCK United States		1
a000001.ms.a.microsoft.com	23.204.152.18	ASN 20940 a23-204-152-	AKAMAI-ASNI , NL United States	http: AkamaiGHost title: Invalid URL https: AkamaiGHost title: Invalid URL cn: a248.e.akamai.net o: Akamai Technologies, Inc.	11

The browser's status bar at the bottom shows "22°C Clear", "ENG IN", "01:35:45", and the date "22-03-2025".

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

How to do it

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

Brave

kloth dns

Q All Images News Videos Goggles

Kloth kloth.net > services > nslookup.php
KLOTH.NET - NSLOOKUP - DNS Look up - Find IP Address
October 20, 2003 - NSLOOKUP - online web tool to lookup and find IP address information in the DNS (Domain Name System)

Kloth kloth.net > services > dig.php
KLOTH.NET - DIG - DNS lookup - find IP address
November 20, 2003 - DIG - use this online web tool to query a DNS nameserver to look up and find IP address information of computers in the internet

Nslookup nslookup.io
DNS Lookup
Find all DNS records for a domain name with this online tool.
Nslookup shows A, AAAA, CNAME, TXT, MX, SPF, NS, SOA and more.

Ns ns.tools > www.kloth.net
Check DNS, MX and whois test domain www.kloth.net
December 11, 2024 - Smtp servers that are listed in DNS area must be accessible, otherwise, there is a risk that emails may be lost. — WWW.KLOTH.NET . mostly about radio and

Mx dns record not published
community.spiceworks.com > t > mx-dns-rec...

Hi ,
I can send emails but i can not recieve emails .
I am getting an error mx dns record not published.
Answer from deepsingh2 on community.spiceworks.com

21°C Clear 02:23:22 22-03-2025

- Type domain name.
- And search .

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: ... the name of the machine to look up.

Server: ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query:

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page). Basically, DNS maps domain names to IP addresses.

Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"!257 0.1. To reverse lookup an IP address, enter the IP address in the "Domain" field. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly be true, but sometimes not. If you don't get a PTR information about a specific computer from a NSLOOKUP query, you may want to try our whois service to find out the owner of this IP address. Like the PTR, other records are also not mandatory. LOC, RP, TXT. They are not strictly required in the DNS and their content may be true or not.

You can't trust on the LOC to locate a host, because most hosts don't have this record defined.

If you prefer dig over nslookup, you may try our [dig](#) service.

This page is also available in [German](#), [French](#) and [Portuguese](#). Enjoy.

>>> If you would like to see this service in [your](#) or any other language, please send a translation.

PayPal If you like this service, please consider to make a small donation to fund and continue this site. Thank you.

[Link to www.kloth.net](#)

Recommended books about Networking

You are coming from IP address **106.221.212.42** using port 63165.
A DNS reverse lookup on this IP address does not work.

You are talking to server www.kloth.net (78.46.75.45) on port 80 using the protocol HTTP/1.1.
Current date and time (UTC) on the server is 2025-03-21 (Fri) 20:55:57. It is the 80th day of this year.

Document URL: <http://www.kloth.net/services/nslookup.php>
Copyright © 1999-2025 Ralf D. Kloth, Ludwigsburg, DE (GRO.software). <hostmaster at kloth.net> [don't send spam]
Created 1999-09-13. Last modified 2011-01-30. Your visit 2025-03-21 20:55:57. Page created in 0.0563 sec.

21°C Clear 02:25:58 22-03-2025



Search Web by Domain | Netcraft KLOTH.NET - NSLOOKUP - DN... +

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: ... the name of the machine to look up.

Server: ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query:

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 = "RFC0482" ""
Name: microsoft.com
Address: 20.236.44.162
Name: microsoft.com
Address: 20.70.246.20
Name: microsoft.com
Address: 20.70.201.171
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 Q Search ENG IN 02:27:26 22-03-2025

NETWORK FOOTPRINTING

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

Objectives:-

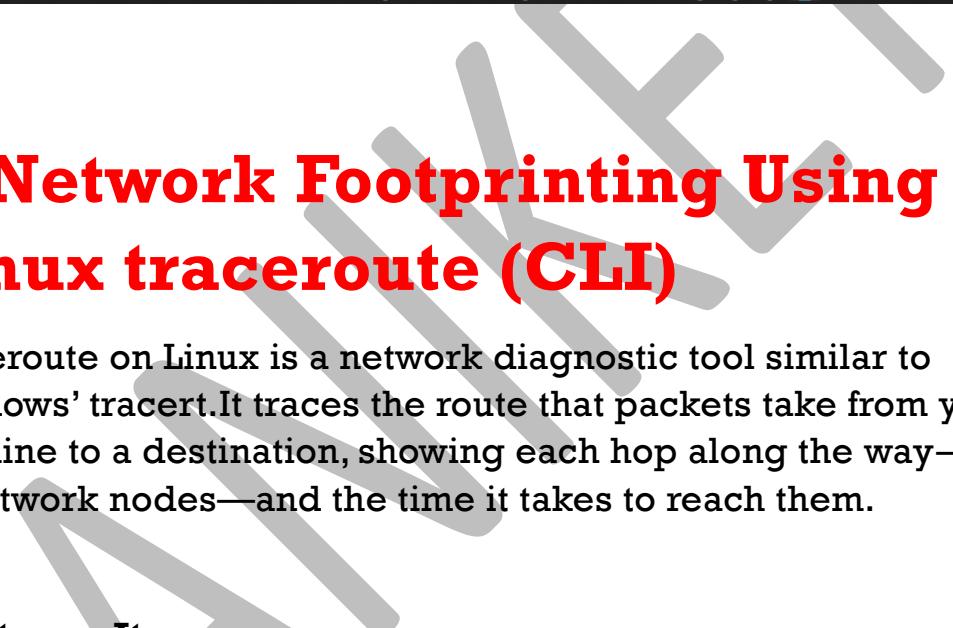
- Identifying IP Addresses
- Gathering DNS Information
- Extracting WHOIS Data
- Mapping Subdomains

1. Network Footprinting Using windows tracert (CLI)

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

How to 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:



```
Command Prompt
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Users\anike>tracert google.com

Tracing route to google.com [142.250.70.46]
over a maximum of 30 hops:

 1   4 ms    3 ms    3 ms  192.168.41.104
 2  237 ms   199 ms   229 ms  192.168.17.10
 3  119 ms    52 ms    39 ms  192.168.16.29
 4  111 ms    57 ms    70 ms  192.168.19.20
 5   95 ms    38 ms    46 ms  192.168.19.33
 6   70 ms    72 ms    56 ms  192.168.252.42
 7   61 ms    58 ms   113 ms  125.20.207.126
 8   46 ms    44 ms    37 ms  125.20.207.125
 9  126 ms    78 ms    77 ms  116.119.36.22
10   87 ms    76 ms    40 ms  116.119.73.94
11   86 ms   113 ms   116 ms  72.14.213.254
12   82 ms    79 ms    77 ms  142.251.225.9
13   96 ms    78 ms    83 ms  192.178.86.245
14   94 ms    75 ms    50 ms  pnbomb-aa-in-f14.1e100.net [142.250.70.46]

Trace complete.

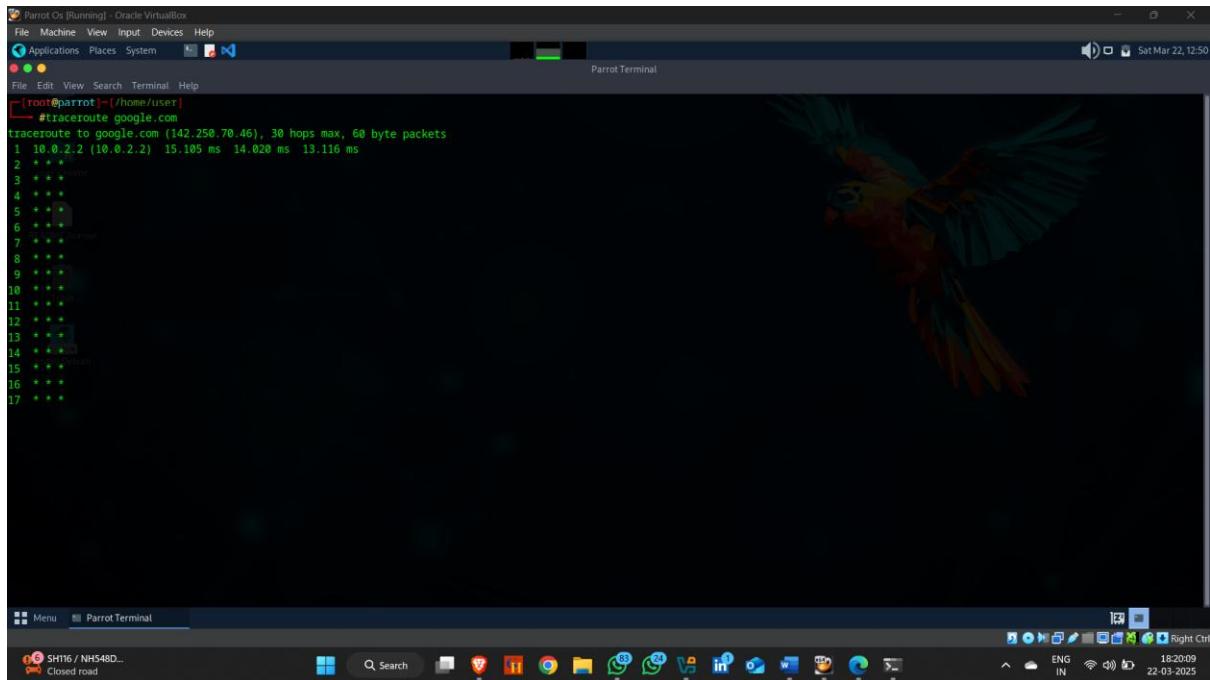
C:\Users\anike>
```

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

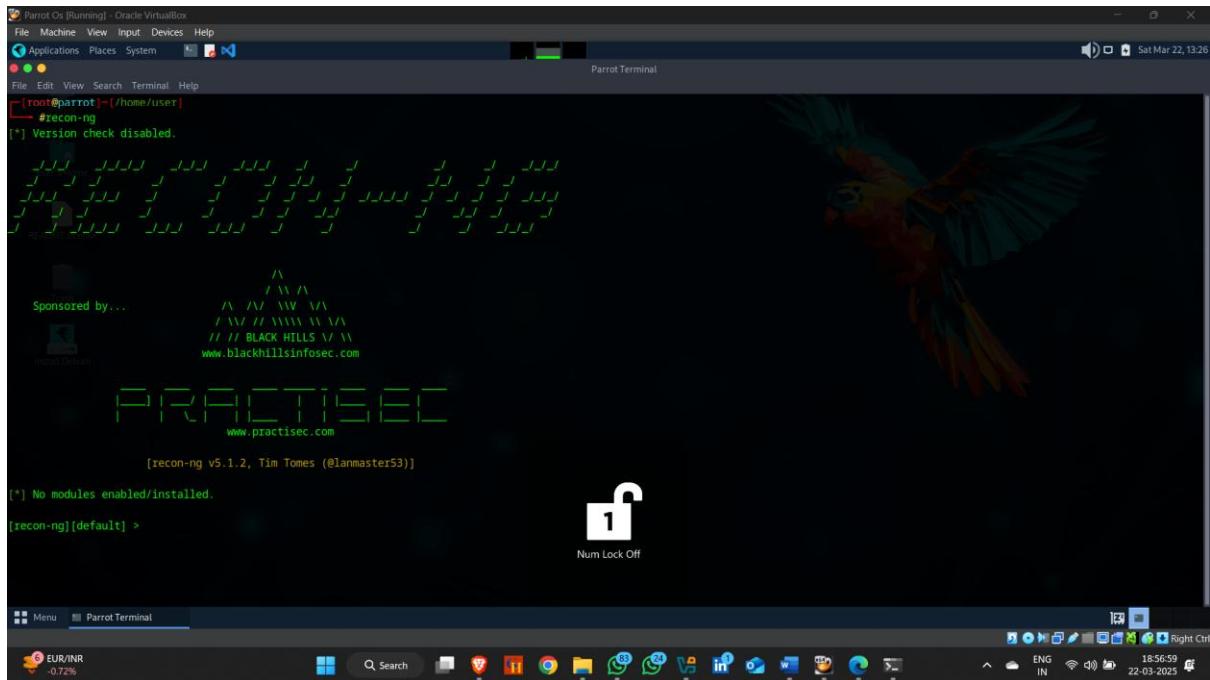
Recon-ng is a powerful open-source reconnaissance framework built into Kali Linux, designed for web-based information gathering using Open Source Intelligence (OSINT).

How to Use Recon-ng in Kali Linux

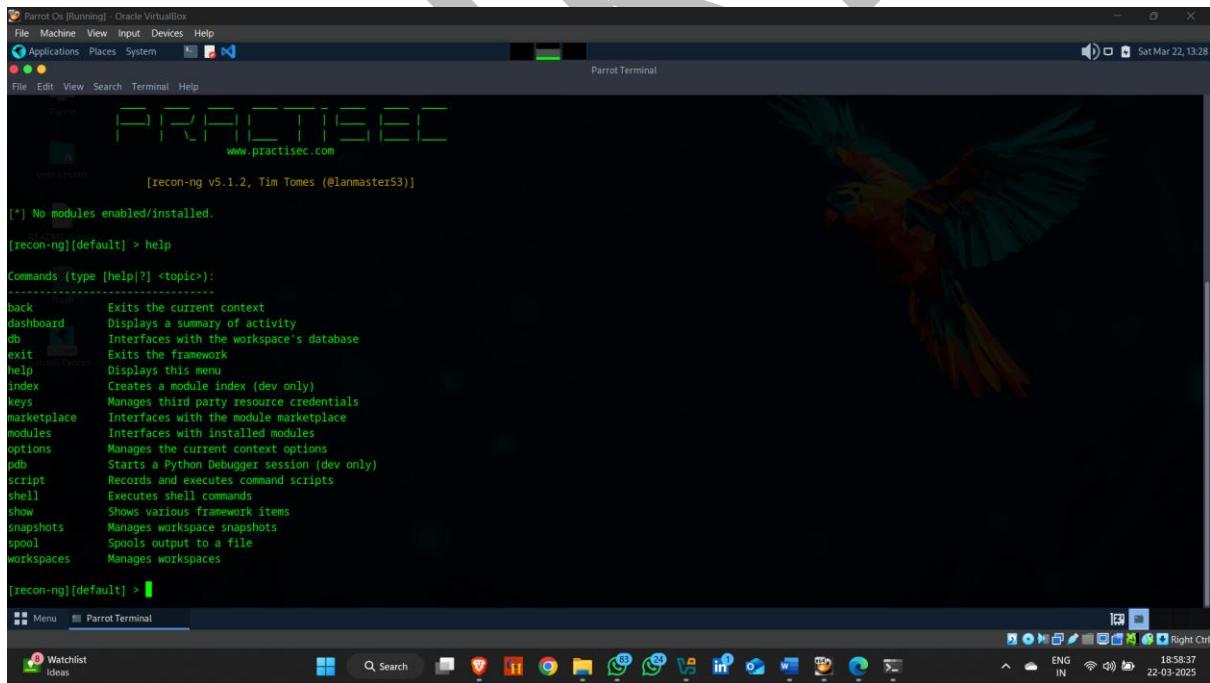
Here's a step-by-step guide to get started with Recon-ng on Kali Linux:

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

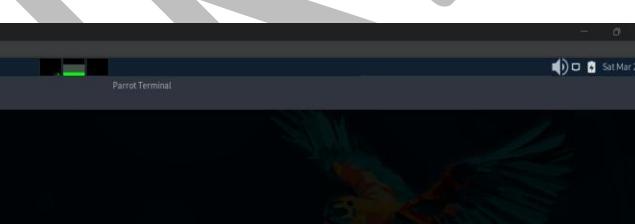


```
Parrot OS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
Sponsored by...
Recon-NG Home
PractiseC www.practise.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.

[recon-ng][default] > workspaces create CehV13
[recon-ng][CehV13] > workspaces list
+-----+
| Workspaces | Modified |
+-----+
| CehV13 | 2025-03-22 13:36:32 |
| default | 2025-03-22 13:24:35 |
+-----+
[recon-ng][CehV13] >
[Menu ParrotTerminal]
34°C Partly cloudy Q Search ENG IN 180642 22-03-2025 Right Ctrl
```

Install Modules

- Marketplace install all



```
Parrot OS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
Sponsored by...
Recon-NG Home
PractiseC www.practise.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.

[recon-ng][default] > workspaces create CehV13
[recon-ng][CehV13] > workspaces list
+-----+
| Workspaces | Modified |
+-----+
| CehV13 | 2025-03-22 13:36:32 |
| default | 2025-03-22 13:24:35 |
+-----+
[recon-ng][CehV13] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[Menu ParrotTerminal]
34°C Partly cloudy Q Search ENG IN 190959 22-03-2025 Right Ctrl
```

Now create a domain

- Db insert domains
- Press enter
- Type domain name

- Show domain

A screenshot of a Parrot OS desktop environment. The desktop background features a colorful parrot. A terminal window titled "Parrot Terminal" is open, displaying the recon-ng framework. The terminal shows the following command history:

```
[recon-ng] [default] > modules load brute
[recon-ng] [default] [xpath_bruter] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng] [default] [xpath_bruter] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng] [default] [xpath_bruter] >
```

The taskbar at the bottom includes icons for File, Applications, Places, System, Home, Search, Terminal, Help, and several system status indicators like battery level and network.

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**.

Parrot Os [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places System

Parrot Terminal

```
[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpins module will likely fail at runtime. See 'keys add'.
[recon-ng][CehV13] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 0 rows affected.

[recon-ng][CehV13] > modules load brute
[*] Multiple modules match 'brute'.
```

Exploitation

exploitation/injection/xpath_bruter

Recon

recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

```
[recon-ng][CehV13] > modules load recon/domains-hosts/brute_hosts
[recon-ng][CehV13][brute_hosts] > run
```

CERTIFIEDHACKER.COM

* No Wildcard DNS entry found.
[*] 0.certifiedhacker.com => No record found.
[*] 12.certifiedhacker.com => No record found.
[*] 1.certifiedhacker..nd.
[*] 10.certifiedhacker..nd.
[*] 01.certifiedhacker..nd.
[*] 11.certifiedhacker..nd.

Parrot Terminal

File Edit View Search Terminal Help

33°C Partly cloudy

Search

ENG IN

22-03-2025

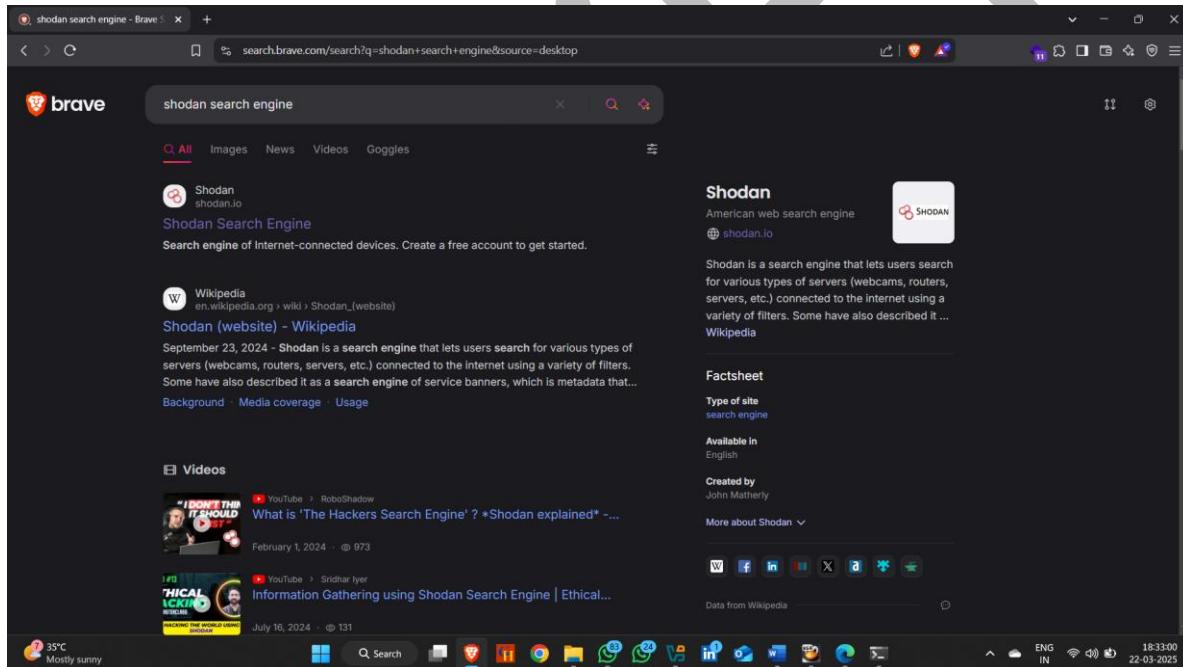
20:26:59

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.



A screenshot of the Shodan search interface showing results for the IP address 162.241.216.11. The page includes a map view, a list of open ports, and a terminal window displaying a Pure-FTPd session.

General Information

Hostnames: bluehost.com, boxx331.bluehost.com, fluidprocesscontrol.com, www.fluidprocesscontrol.com

Domains: BLUEHOST.COM, FLUIDPROCESSCONTROL.COM

Country: United States

City: Tabiona

Organization: Unified Layer

ISP: Unified Layer

Temperature: 35°C Mostly sunny

Open Ports

Port	Protocol
21	TCP
22	TCP
26	TCP
53	TCP
80	TCP
110	TCP
143	TCP
443	TCP
465	TCP
587	TCP
993	TCP
995	TCP
2077	TCP
2082	TCP
2083	TCP
2086	TCP
2087	TCP
2095	TCP
2222	TCP
3306	TCP
5432	TCP

Pure-FTPd

```
220----- Welcome to Pure-FTPd [privsep] [TLS]
220-You are user number 6 of 150 allowed.
220-Local time is now 22:58. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
211-Can't change directory to /var/ftp/ [/]
211-Extensions supported:
      UTF8
```

LAST SEEN: 2025-03-22

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

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

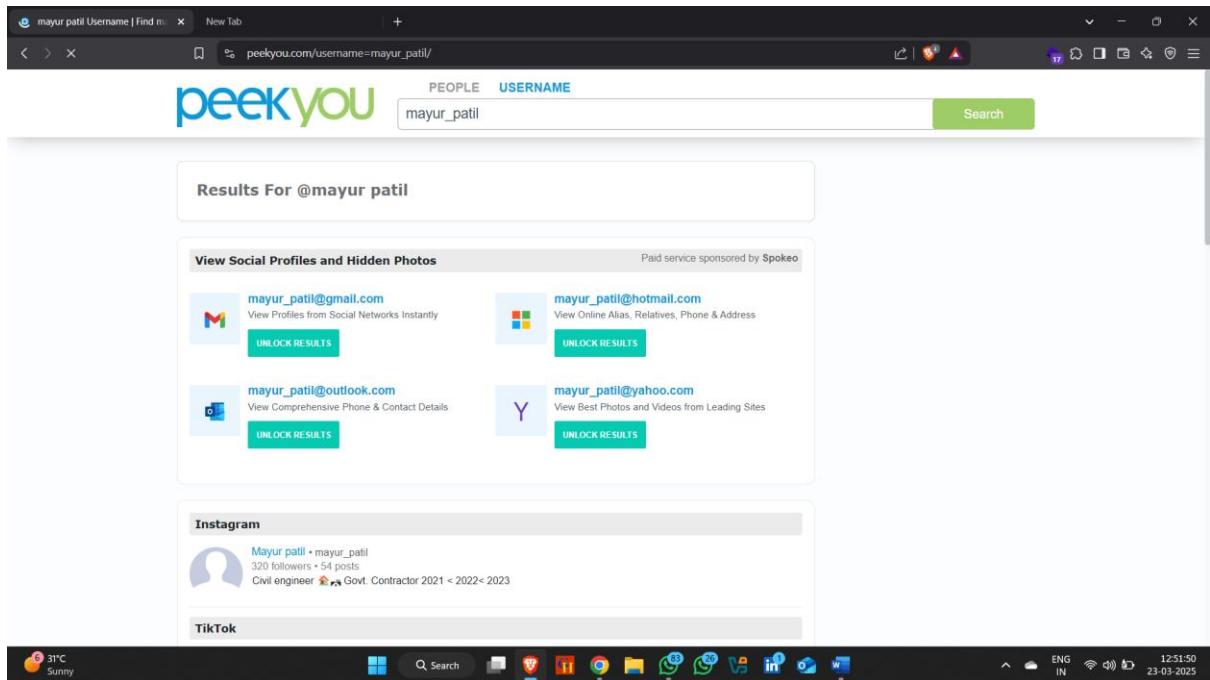
1. Open Browser.
2. Search peekyou
3. open official peekyou website
4. click on **username** tab.
5. Enter username of person that you want to gather social media information

The screenshot shows a Brave browser window with a dark theme. The search bar at the top contains the query "peekyou". Below the search bar, there are several search results:

- PeekYou** - People search engine peekyou.com: A snippet from Wikipedia describes PeekYou as a people search engine that indexes people and their links on the web, founded in April 2006 by Michael Hussey. It claims over 250 million indexed users.
- PeekYou - Fast People Search Made Easy**: A snippet from the official website states that PeekYou is a free people search engine allowing users to find and contact anyone online through social links, photos, work history, and more.
- Reverse Phone Number Search**: A snippet from the website explains how to search for phone numbers, cell numbers, and reverse lookups.
- About PeekYou**: A snippet from the website provides information about the company, mentioning it is the leading people search engine.
- Privacy Policy**: A snippet from the website details the privacy policy of PeekYou LLC.
- Do Not Sell My Personal Info...**: A snippet from the website informs users that removals can take up to 10 business days.
- Wikipedia**: A snippet from Wikipedia provides a detailed overview of PeekYou's history and features.

At the bottom of the search results, there is a "Videos" section showing a thumbnail for a YouTube video from "youtube.com". The browser's status bar at the bottom right shows the date as 23-03-2025 and the time as 12:48:25.

The screenshot shows a Microsoft Edge browser window with a light theme. The address bar displays "peekyou.com/username". The main content area features a large image of a woman looking at a screen, with the text "Quick Username Search" overlaid. Below the image, a subtext reads: "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." At the bottom of the page, there is a search bar with the placeholder "People Search" and "Username Search". The "Username Search" tab is active, and the search term "mayur_patil" is entered into the input field. The browser's status bar at the bottom right shows the date as 23-03-2025 and the time as 12:51:36.

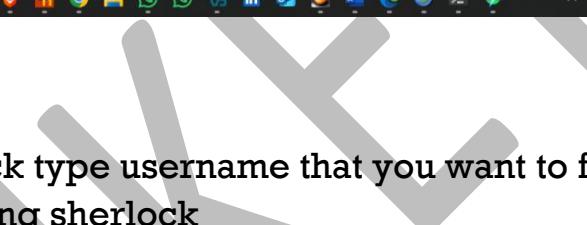


2. Social Media Footprinting Using Sherlock (CLI)

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.



Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@Kali:/home/aniket

```
# apt install sherlock
sherlock is already the newest version (0.15.0-1).
The following packages were automatically installed and are no longer required:
  crackmapexec  libglibxdr0  libgumbo2  libplist3  libusbmuxd6  python3-pluggy
  firebird3.0-common  libconfig++9v5  libgl-mesa-dev  libhdbsql-100-1t64  libpoppler134  python3-rsa
  firejail3.0-common-doc  libconfig++9v5  libgl-mesa  libhdbsql-100t64  libpoppler134  python3-setproctitle
  forensics-liberation2  libfb-dev-1.7-7t64  libglel-dev  libhdbsql11-dev  libpoppler134  python3-setuptools-scm
  freerdp2-0.1  libegl-dev  libgles1  libimobiledevice6  libpython3.11-minimal  openjdk-17-jre  python3-trove-classifiers
  hydra-gtk  libflac12t64  libglusterfs0  libiniarser1  libpython3.11-stdlib  openjdk-17-jre-headless  python3.11
  iverbts-providers  libfmt9  libglvnd-core-dev  libjim0.82t64  libpython3.11t64  openjdk-23-jre  python3.11-dev
  libharadillo12  libfreerdp-client2-2t64  libglvnd-dev  libjsoncp25  libqt5sensors5  openjdk-23-jre-headless  python3.11-minimal
  libassuan0  libfreerdp2-2t64  libgspell-1-2  libmbcrypto7t64  libqt5webkit5  perl-modules-5.38  ruby-zeitwerk
  libayfilter9  libgail-common  libgtk2-0-t64  libmfx1  librados2  python3-appdirs
  libbbfiel  libgall18t64  libgtk2-0-bin  libmsgraph-0-1  librdmacm1t64  python3-hatch-vcs
  libbblos-2-3  libgal34t64  libgtk2-0-common  libnetcdf19t64  libsuperflub  python3-hatchling
  libboost-iostreams1.83.0  libgeos3.12.2  libgtksourceview-3.0-3  libpapi  libtag1v5  python3-jose
  libboost-thread1.83.0  libgfaio  libgtksourceview-3.0-common  libperl5.38t64  libtag1v5-vanilla  python3-lib2to3
  libcapstone4  libgrpc0  libgtksourceviewmm-3.0-0v5  libplacebo338  libtagc0  python3-pathspec
  Use 'sudo apt autoremove' to remove them.

Summary:
 Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 32

[root@Kali:/home/aniket]
#
```

22°C Clear

Search ENG IN 01:00:15 23-03-2025

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

Example :-: sherlock saurabh_gaikwad



Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@Kali:/home/aniket

```
libboost-iostreams1.83.0  libgeos3.12.2      libgtksourceview-3.0-1    libpaper1   libtag1v5      python3-jose      rwho
libboost-thread1.83.0    libgfaio          libgtksourceview-3.0-common libperl5.38t64 libtag1v5-vanilla python3-lib2to3  rwhod
libcapstone4             libgrpc0          libgtksourceviewmm-3.0-0v5 libplacebo338 libtagc0       python3-pathspec sambo-vfs-modules

Use 'sudo apt autoremove' to remove them.

Summary:
 Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 32

[root@Kali:/home/aniket]
# sherlock saurabh_gaikwad
[*] Checking username saurabh_gaikwad on:

[*] 9GAG: https://www.9gag.com/u/saurabh_gaikwad
[*] Cults3D: https://cults3d.com/en/users/saurabh_gaikwad/creations
[*] Disqus: https://disqus.com/saurabh_gaikwad
[*] Freelance.habr: https://Freelance.habr.com/freelancers/saurabh_gaikwad
[*] GitHub: https://github.com/saurabh_gaikwad
[*] HackerEarth: https://hackerearth.com/saurabh_gaikwad
[*] HackerRank: https://hackerrank.com/saurabh_gaikwad
[*] Houzz: https://houzz.com/user/saurabh_gaikwad
[*] HudsonRock: https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=saurabh_gaikwad
[*] LinkedIn: https://www.linkedin.com/in/saurabh_gaikwad
[*] Linktree: https://linktree.ee/saurabh_gaikwad
[*] Memrise: https://www.memrise.com/user/saurabh_gaikwad/
[*] NationsStates Region: https://nationsstates.net/regions/saurabh_gaikwad
[*] ProductHunt: https://www.producthunt.com/@saurabh_gaikwad
[*] Reddit: https://www.reddit.com/user/saurabh_gaikwad
[*] Scribd: https://www.scribd.com/saurabh_gaikwad
[*] Strava: https://www.strava.com/athletes/saurabh_gaikwad
[*] Telegram: https://t.me/saurabh_gaikwad
[*] TradingView: https://www.tradingview.com/u/saurabh_gaikwad/
[*] Twitter: https://www.twitter.com/saurabh_gaikwad
[*] Wikipedia: https://en.wikipedia.org/w/index.php?title=Special:CentralAuth/saurabh_gaikwad&oldid=11260787
[*] YouTube: https://www.youtube.com/@saurabh_gaikwad
[*] mastodon.cloud: https://mastodon.cloud/@saurabh_gaikwad
[*] omg.iol: https://saurabh_gaikwad.omg.iol

[*] Search completed with 25 results
```

22°C Clear

Search ENG IN 01:02:21 23-03-2025

AMKET