



# REPORT OF FOOTPRINTING AND RECONNAISSANCE

BY SACHCHITANAND YADAV

# Footprinting and Reconnaissance

MODULE - 2

## Learning Objectives -

- Explain Footprinting and Reconnaissance Concepts
- Demonstrate Footprinting through Search Engines
- Demonstrate Footprinting through Internet Research Services
- Demonstrate Footprinting through Social Networking Sites
- Use Different Techniques for Whois Footprinting
- Use Different Techniques for DNS Footprinting
- Use Different Techniques for Network and Email Footprinting
- Demonstrate Footprinting through Social Engineering
- Automate Footprinting Tasks using Advanced Tools and AI
- Explain Footprinting Countermeasures

# Table of Contents

<b>1. Footprinting and Reconnaissance Concepts.....</b>	<b>4</b>
1.1 Introduction to Footprinting and Reconnaissance	
1.2 Key Information Gathered	
1.3 Associated Threats and Risks	
<b>2. Footprinting through Search Engines.....</b>	<b>6</b>
2.1 What is Shodan?	
2.2 Advanced Google Hacking Techniques	
2.3 Google Advanced Search	
2.4 Google Advanced image search	
2.5 Gathering Information from Video Search Engines	
2.6 Gathering Information from Meta Search Engines	
2.7 FTP Search Engines	
2.8 Gathering Information from IoT Search Engines	
<b>3. Footprinting through Internet Research Services.....</b>	<b>22</b>
3.1 Tools to Search Company Sub-Domains (Netcraft, DNSdumpster, Pentest-Tools)	
3.2 Finding a Company's TLDs & Subdomains with AI	
3.3 Using Sublist3r to Gather Subdomains	
3.4 Extracting Website Information using Archive.org (Wayback Machine)	
3.5 Using Photon to Retrieve Archived URLs	
3.6 Footprinting Through People Search Services (Spokeo)	
3.7 Dark Web Footprinting	
3.8 Determining the Operating System (OS Fingerprinting - Netcraft, Censys)	
3.9 Competitive Intelligence (CI) Gathering	
3.10 Gathering Information from Public Source-Code Repositories (Recon-ng)	
<b>4. Footprinting through Social Networking Sites .....</b>	<b>39</b>
4.1 People Search on Social Networking Sites	
4.2 TheHarvester (Employee Contact Gathering)	
4.3 Harvesting Email Lists	
4.4 Tools for Social Network Footprinting (Sherlock, Social Searcher)	
<b>5. Whois Footprinting Techniques.....</b>	<b>44</b>
5.1 Understanding Whois Footprinting	
5.2 Whois Lookup Results	

- 5.3 Using Batch IP Converter
- 5.4 IP Geolocation Lookup Tools (IP2Location)

## **6. DNS Footprinting Techniques.....48**

- 6.1 DNS Footprinting Overview
- 6.2 Extracting DNS Information (DNS Records)
- 6.3 MXToolbox
- 6.4 Fierce
- 6.5 Reverse DNS Lookup (DNSRecon)
- 6.6 DNS Footprinting using Dig (CLI)

## **7. Network and Email Footprinting.....59**

### **7.1 Network Footprinting**

- 7.1.1 Using Windows tracert (CLI)
- 7.1.2 Using Linux traceroute (CLI)

### **7.2 Email Footprinting**

- 7.2.1 Emkei Mailer
- 7.2.2 Email Footprinting using MXToolbox
- 7.2.3 Email Footprinting using GSA Email Spider

## **8. Footprinting through Social Engineering.....66**

- 8.1 Social Media Footprinting
- 8.2 Social Media Footprinting using Peekyou
- 8.3 Social Media Footprinting using Sherlock (CLI)

## **9. Automating Footprinting using Advanced Tools & AI.....69**

- 9.1 Automating Footprinting (Maltego, OSINT Framework, Subfinder)
- 9.2 AI-Powered OSINT Tools
- 9.3 The Role of AI in OSINT
- 9.4 Tools: Taranis AI, OSS Insight, DorkGPT, Gemini-CLI AI

## **10. Footprinting Countermeasures.....75**

- 10.1 Footprinting Countermeasures Overview
- 10.2 Technical & Configuration Controls
- 10.3 Administrative & Policy Controls
- 10.4 Proactive Measures
- 10.5 Module Summary

# 1. Footprinting and Reconnaissance Concepts: -

## Introduction to Footprinting and Reconnaissance

**Reconnaissance** is the first and most critical phase of any security assessment or potential attack. It is a preparatory phase that involves exploring and collecting as much information as possible about a target system or organization.

Within this phase, **footprinting** is the specific process of creating a comprehensive profile—or "footprint"—of a target. This involves systematically gathering data to map out the organization's IT infrastructure, security posture, and potential vulnerabilities. The ultimate goal is to build an effective strategy for a security audit or a simulated attack.

## Key Information Gathered

The intelligence gathered during footprinting is typically organized into three main categories:

- **Organizational Information:** This includes details about the company's structure and personnel.
  - Employee names, contact information, and designations
  - Physical addresses and branch locations
  - Company partners and background details
  - Patents, trademarks, and legal documents
  - News articles and press releases
- **Network Information:** This focuses on the target's digital and network infrastructure.
  - Domain and sub-domain names
  - IP network blocks and active IP addresses
  - Whois and DNS records
  - Network topology, including trusted routers and firewall locations
- **System Information:** This involves identifying specific details about the target's active systems.
  - Operating systems used on servers and workstations
  - Web server locations and technologies
  - Publicly available email addresses, usernames, and passwords

## Footprinting Methodologies

Footprinting techniques are categorized based on the level of interaction with the target's systems.

## Passive Footprinting

This approach involves gathering information from publicly available sources **without directly interacting** with the target's systems. It is a stealthy method that is difficult to detect. Think of it as researching a company using public records, news articles, and social media.

Common techniques include:

- **Search Engines:** Using advanced search queries (e.g., Google Hacking) to uncover sensitive information.
- **Internet Research Services:** Utilizing tools like SHODAN to find internet-connected devices or archive.org to view historical versions of websites.
- **Social Networking Sites:** Monitoring social media to gather intelligence on employees and company culture.
- **Whois Footprinting:** Querying public databases to get domain registration details.

## Active Footprinting

This approach involves **directly interacting** with the target's infrastructure to gather information. This method can yield more detailed and accurate data but also creates "noise," which increases the risk of being detected by security systems like firewalls and Intrusion Detection Systems (IDS).

Common techniques include:

- **DNS Footprinting:** Performing DNS interrogation and reverse DNS lookups to map network hosts.
- **Network and Email Footprinting:** Using tools like Traceroute to map network paths or tracking emails to gather server information.
- **Social Engineering:** Actively engaging with employees through methods like impersonation or dumpster diving to extract information.

## Associated Threats and Risks

Successful footprinting can expose an organization to significant threats, including:

- **Social Engineering:** Attackers can use employee details to manipulate staff into revealing sensitive data.
- **System and Network Attacks:** Information on system configurations and software helps attackers identify and exploit known vulnerabilities to gain control of the network.
- **Information Leakage & Privacy Loss:** A breach can expose sensitive corporate data, leading to a loss of privacy for both the organization and its personnel.
- **Corporate Espionage & Business Loss:** Competitors can use footprinting to gather intelligence, potentially leading to the theft of trade secrets, undermining market position, and causing significant financial damage.

## 2. Footprinting with Search Engines

### What is Shodan?

Think of Shodan as Google's rebellious cousin who decided to index **Internet-connected devices** instead of webpages.

Cameras, routers, servers, traffic lights, refrigerators (yep), industrial systems — if it's online, Shodan can sniff it out.

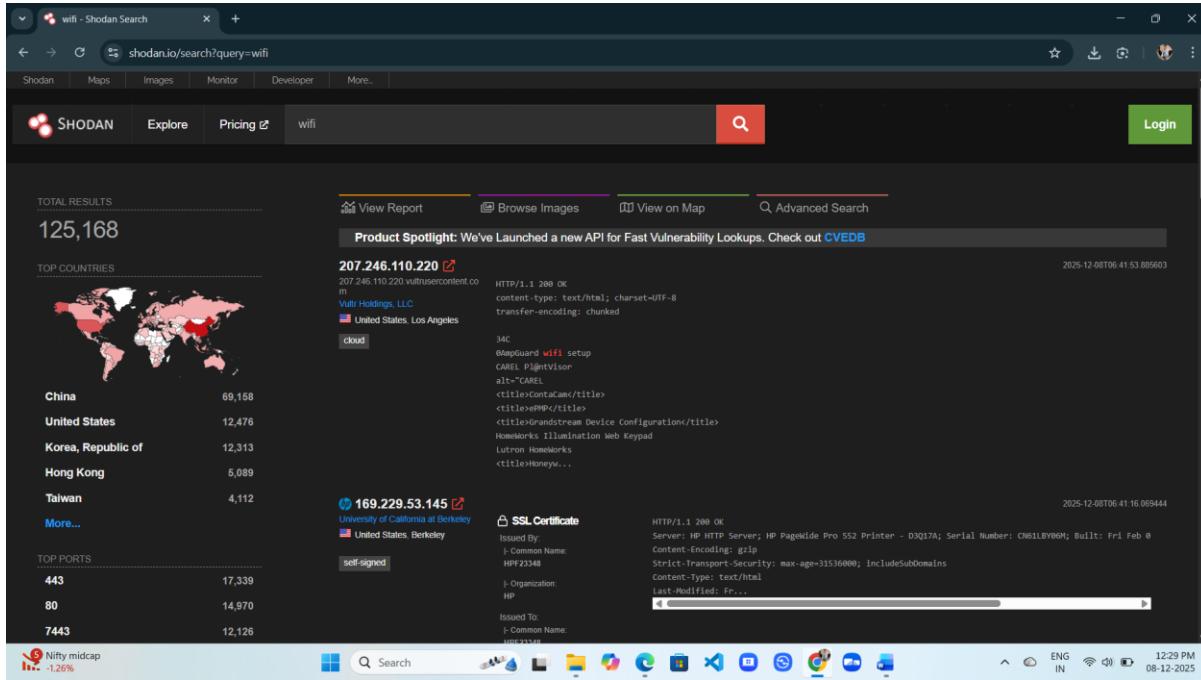
### Purpose:

- Spot vulnerable devices
- Help in ethical hacking & security testing
- Monitor exposed systems
- Track IoT/servers open on the internet

**Website:** - <https://www.shodan.io/>

The screenshot shows the Shodan search interface for the query "camera". The total results count is 3,414,793. Key sections include:

- TOP COUNTRIES:** United States (484,468), Viet Nam (377,301), Germany (186,749), United Kingdom (123,363), China (121,306).
- TOP PORTS:** 80 (913,683), 443 (422,201), 81 (240,465).
- Results for 76.97.4.88:** IP: 76.97.4.88, Hostname: Comcast Cable Communications, Inc., Location: United States, Atlanta. Response headers include: Date: Mon, 08 Dec 2025 01:22:16 GMT, Server: webserver, X-Frame-Options: SAMEORIGIN, ETag: "387-258-61734942", Content-Length: 608, Content-Type: text/html, Connection: close, Last-Modified: Sat, 23 Oct 2021 05:58:42 GMT. Status message: Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.
- Results for 180.220.2.210:** IP: 180.220.2.210, Hostname: host210.190.220.2.telmex.net.ar, Organization: OFIDIRECT S.A., Location: Argentina, Buenos Aires. Response headers include: Date: Mon, 08 Dec 2025 02:51:55 GMT, Server: Web, X-Frame-Options: SAMEORIGIN, ETag: "0-3e9-1e0", Content-Length: 488, Content-Type: text/html, Connection: keep-alive, Keep-Alive: timeout=60, max=99, Last-Modified: Sun, 28 Jun 2020 02:17:11 GMT. Status message: Hikvision IP Camera: Web Version: 4.0.51 build 211022...



## Footprinting Using Advanced Google Hacking Techniques

A Google search could reveal submissions to forums by security personnel, disclosing the brands of firewalls or antivirus software used by the target. This information helps the attacker in identifying vulnerabilities in such security controls.

For example, consider an organization, perhaps Microsoft. Type Microsoft in the Search box of a search engine and press Enter; this will display the results containing information about Microsoft. Browsing the results often provides critical information such as physical location, contact addresses, services offered, number of employees, and so on, which may prove to be a valuable source for hacking.

Here is the extracted text exactly as it appears:

---

**site:** This operator restricts search results to the specified site or domain.

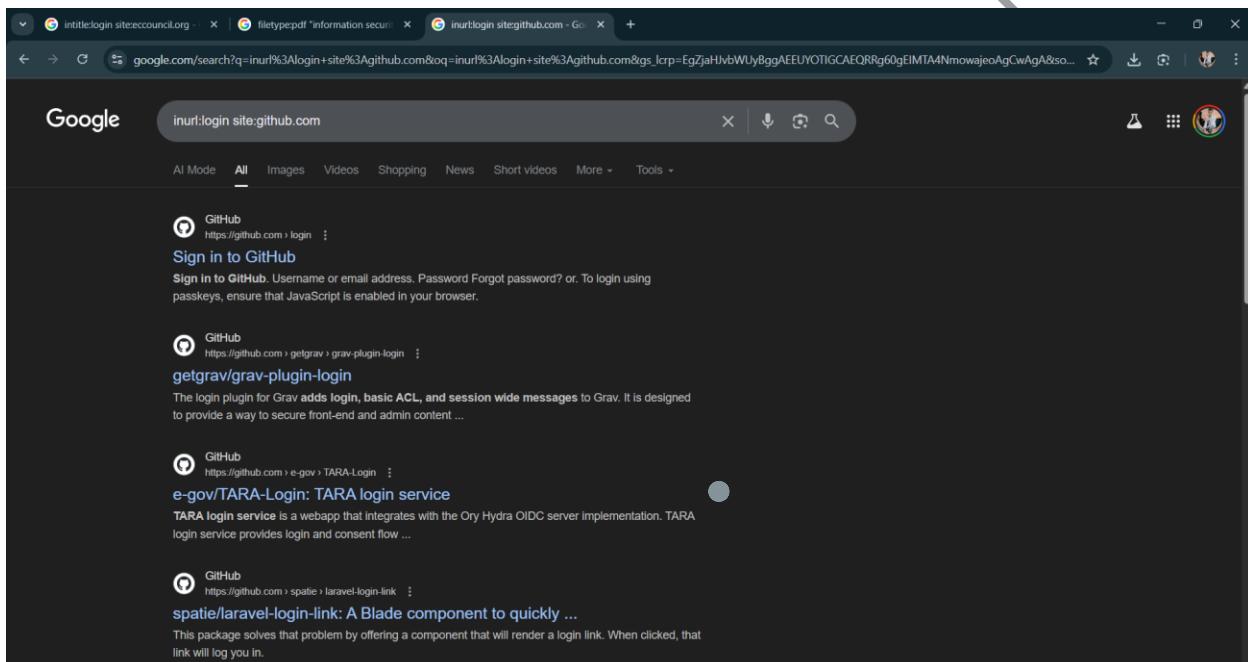
*Example:* The [games site: www.certifiedhacker.com] query gives information on games from the certifiedhacker site.

**allinurl:** This operator restricts results to only the pages containing all the query terms specified in the URL.

*Example:* The [allinurl: google career] query returns only pages containing the words “google” and “career” in the URL.

**inurl:** This operator restricts the results to only the pages containing the specified word in the URL.

*Example:* The [inurl: copy site:www.google.com] query returns only Google pages in which the URL has the word “copy.”



**intext:** This operator displays the results containing the specific keyword within the body of the webpage.

*Example:* The [intext:"vpn configuration"] query returns the pages containing the phrase “vpn configuration” in their body text.

**allintitle:** This operator restricts results to only the pages containing all the query terms specified in the title.

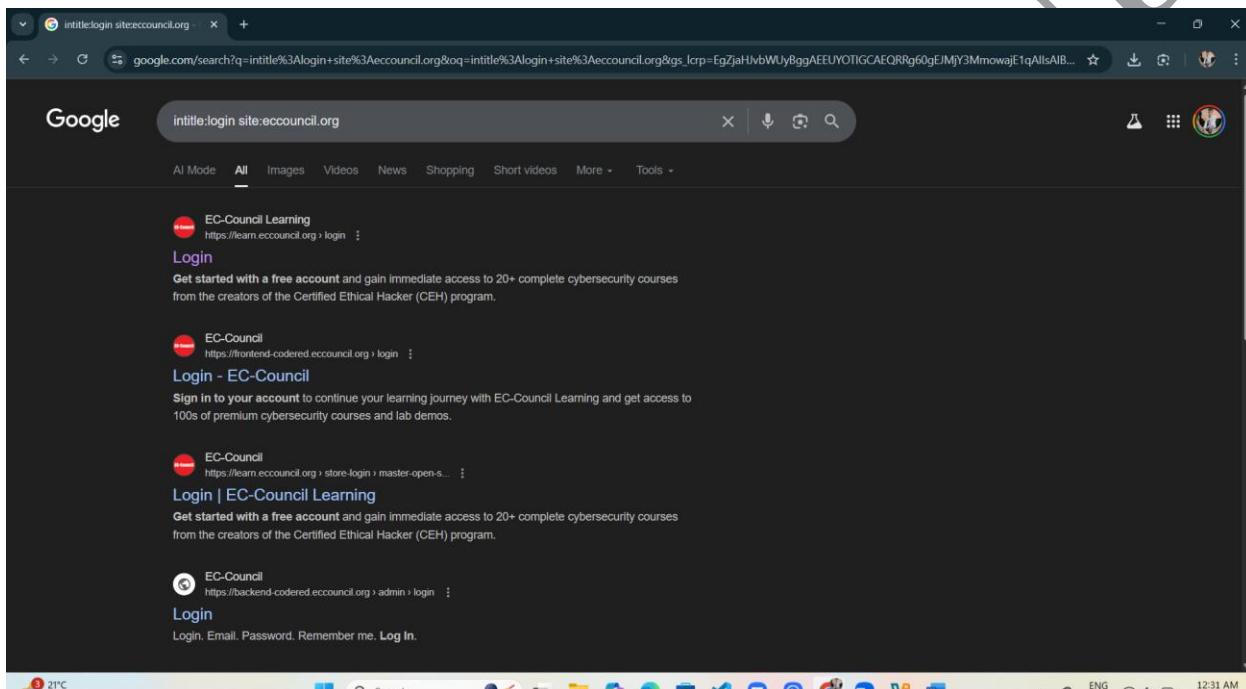
*Example:* The [allintitle: detect malware] query returns only pages containing the words “detect” and “malware” in the title.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

Here is the extracted text exactly as it appears:

**intitle:** This operator restricts results to only the pages containing the specified term in the title.

*Example:* The [malware detection intitle:help] query returns only pages that have the term “help” in the title, and the terms “malware” and “detection” anywhere within the page.



**inanchor:** This operator restricts results to only the pages containing the query terms specified in the anchor text on links to the page.

*Example:* The [Anti-virus inanchor:Norton] query returns only pages with anchor text on links to the pages containing the word “Norton” and the page containing the word “Anti-virus.”

**allinanchor:** This operator restricts results to only the pages containing all query terms specified in the anchor text on links to the pages.

*Example:* The [allinanchor: best cloud service provider] query returns only pages for which the anchor text on links to the pages contains the words “best,” “cloud,” “service,” and “provider.”

**cache:** This operator displays Google's cached version of a web page instead of the current version of the web page.

*Example:* [cache:www.eff.org] will show Google's cached version of the Electronic Frontier Foundation home page.

**link:** This operator searches websites or pages that contain links to the specified website or page.

*Example:* [link:www.google|guide.com] finds pages that point to Google Guide's home page.

*Note:* According to Google's documentation, "you cannot combine a link: search with a regular keyword search."

Also note that when you combine link: with another advanced operator, Google may not return all the pages that match.

**related:** This operator displays websites that are similar or related to the URL specified.

*Example:* [related:www.microsoft.com] provides the Google search engine results page with websites similar to microsoft.com.

**info:** This operator finds information for the specified web page.

*Example:* [info:gotohotel.com] provides information about the national hotel directory GotHotel.com home page.

**location:** This operator finds information for a specific location.

*Example:* [location: 4 seasons restaurant] will give you results based on the term "4 seasons restaurant."

Here is the extracted text exactly as it appears:

---

**filetype:** This operator allows you to search for results based on a file extension.

*Example:* [jasmine:jpg] will provide jpg files based on jasmine.

**source:** This operator displays information from a specific website in Google News.

*Example:* [Malware news source:"Hacker News"] returns articles from Hacker News containing the word "Malware".

**phonebook:** This operator finds the residential and business phone numbers of a person or organization.

*Example:* [phonebook:Sundar Pichai] will provide Sundar Pichai's phone number.

**before:** This operator filters search results to include only content published before a specified date.

*Example:* [ransomware before:2020-06-29] will give results about the ransomware that occurred before June 29, 2020.

**after:** This operator finds information that was published after a certain date.

*Example:* [site:wikipedia.org after:2023-01-01 artificial intelligence] will retrieve Wikipedia articles about artificial intelligence published after January 1, 2023.

## Google Advanced Search

It's basically Google's "pro mode," letting you search with precision instead of vibes.

### What it's used for:

- Find info *exactly* where you want it
- Filter by file type, website, date, words, etc.
- Search specific phrases
- Exclude certain terms
- Get more accurate results than normal Google search

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

The screenshot shows the Google Advanced Search interface. In the search bar, the query "tri-colour rat terrier" is entered. The search results page displays a large watermark reading "DATA".

**Find pages with...**

- all these words:
- this exact word or phrase:
- any of these words:
- none of these words:
- numbers ranging from:  to

**To do this in the search box.**

- Type the important words: `tri-colour rat terrier`
- Put exact words in quotes: `"rat terrier"`
- Type OR between all the words you want: `miniature OR standard`
- Put a minus sign just before words that you don't want: `-rodent, -"Jack Russell"`
- Put two full stops between the numbers and add a unit of measurement: `10..35 kg, £300..£500, 2010..2011`

**Then narrow your results by...**

- language:  any language
- region:  any region
- last update:  anytime
- site or domain:
- terms appearing:  anywhere in the page

**Find pages in the language that you select.**

**Find pages published in a particular region.**

**Find pages updated within the time that you specify.**

**Search one site (like wikipedia.org) or limit your results to a domain like .edu .org or .gov**

**Search for terms in the whole page, page title or web address, or links to the page you're looking for.**

At the bottom, the status bar shows: 7 26°C Sunny, ENG IN, 12:43 PM, 08-12-2025.

The screenshot shows the Google Advanced Search interface. In the search bar, the query "Footprinting" is entered. The search results page displays a large watermark reading "DATA".

**Find pages with...**

- all these words:  Footprinting
- this exact word or phrase:
- any of these words:
- none of these words:
- numbers ranging from:  to

**To do this in the search box.**

- Type the important words: `tri-colour rat terrier`
- Put exact words in quotes: `"rat terrier"`
- Type OR between all the words you want: `miniature OR standard`
- Put a minus sign just before words that you don't want: `-rodent, -"Jack Russell"`
- Put two full stops between the numbers and add a unit of measurement: `10..35 kg, £300..£500, 2010..2011`

**Then narrow your results by...**

- language:  any language
- region:  any region
- last update:  anytime
- site or domain:
- terms appearing:  anywhere in the page
- file type:  Adobe Acrobat PDF (.pdf)
- usage rights:  not filtered by licence

**Find pages in the language that you select.**

**Find pages published in a particular region.**

**Find pages updated within the time that you specify.**

**Search one site (like wikipedia.org) or limit your results to a domain like .edu .org or .gov**

**Search for terms in the whole page, page title or web address, or links to the page you're looking for.**

At the bottom, the status bar shows: NIFTY -0.62%, ENG IN, 12:48 PM, 08-12-2025.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

Footprinting filetype:pdf

cybersecurityhoy.com  
https://cybersecurityhoy.com/uploads/2021/07/ PDF  
2-footprinting-and-reconnaissance.pdf - CybersecurityHoy  
1. Footprinting: Collecting information about an organization in a passive manner. 2. Scanning:  
Using active reconnaissance methods, such as nmap scanning, ...  
152 pages

People also ask :

- What do you mean by footprinting?
- Who is India's no. 1 ethical hacker?
- What is the difference between footprinting and reconnaissance?
- What is a footprint in technology?

Feedback

جامعة بابل  
https://cdx.ubabylon.edu.iq/lectures/ PDF  
Lecture 3:Footprinting and Reconnaissance I  
Footprinting is the first step of any attack on information system in which an attacker collects

NIFTY -0.62%

Advanced Search

Find pages with...

all these words: user name and password  
Type the important words: tri-colour rat terrier

this exact word or phrase:  
Put exact words in quotes "rat terrier"

any of these words:  
Type OR between all the words you want: miniature OR standard

none of these words:  
Put a minus sign just before words that you don't want: -rodent, -"Jack Russell"

numbers ranging from: to  
Put two full stops between the numbers and add a unit of measurement: 10..35 kg, £300..£500, 2010..2011

Then narrow your results by...

language: any language  
Find pages in the language that you select.

region: any region  
Find pages published in a particular region.

last update: anytime  
Find pages updated within the time that you specify.

site or domain:  
Search one site (like wikipedia.org) or limit your results to a domain like .edu, .org or .gov

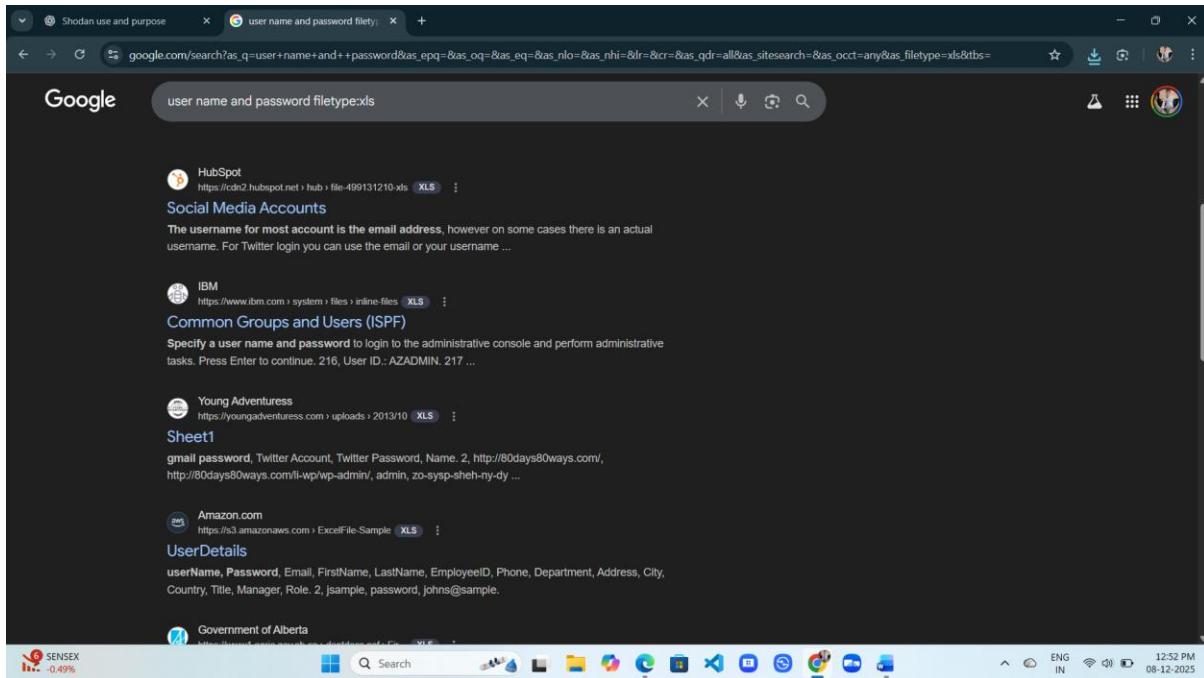
terms appearing: anywhere in the page  
Search for terms in the whole page, page title or web address, or links to the page you're looking for.

file type: Microsoft Excel (.xls)  
Find pages in the format that you prefer.

usage rights: not filtered by licence  
Find pages that you are free to use yourself.

SENSEX -0.49%

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

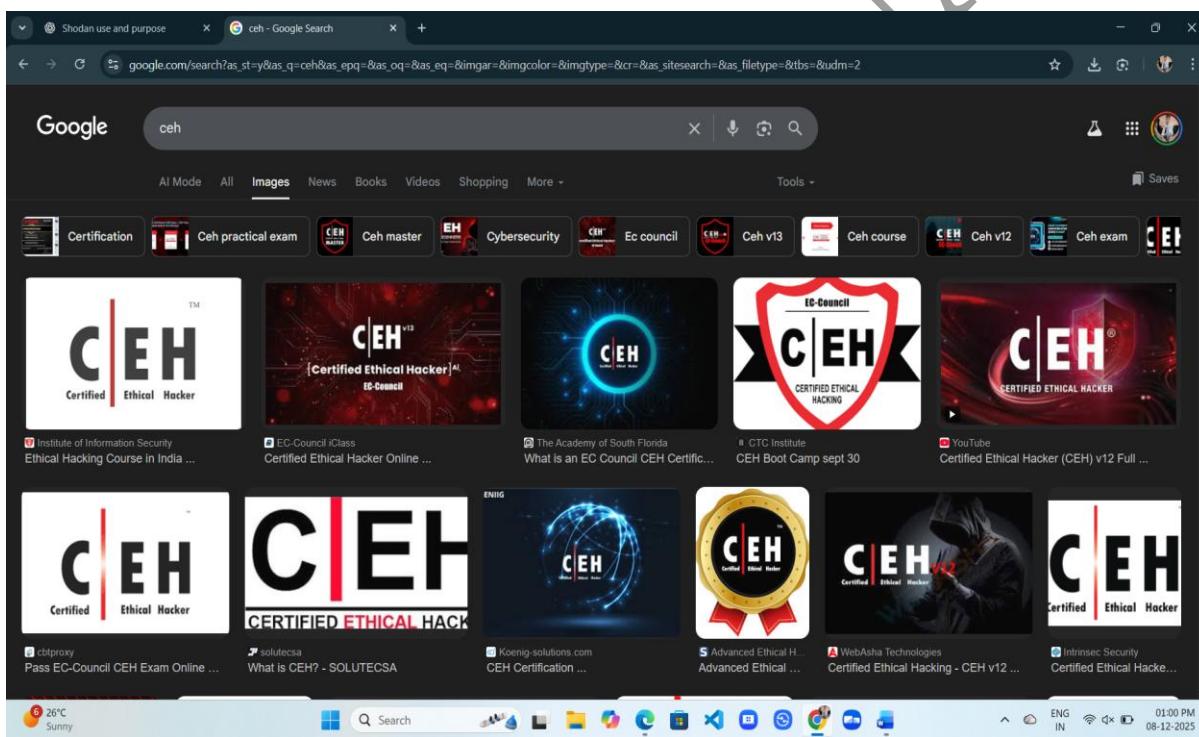
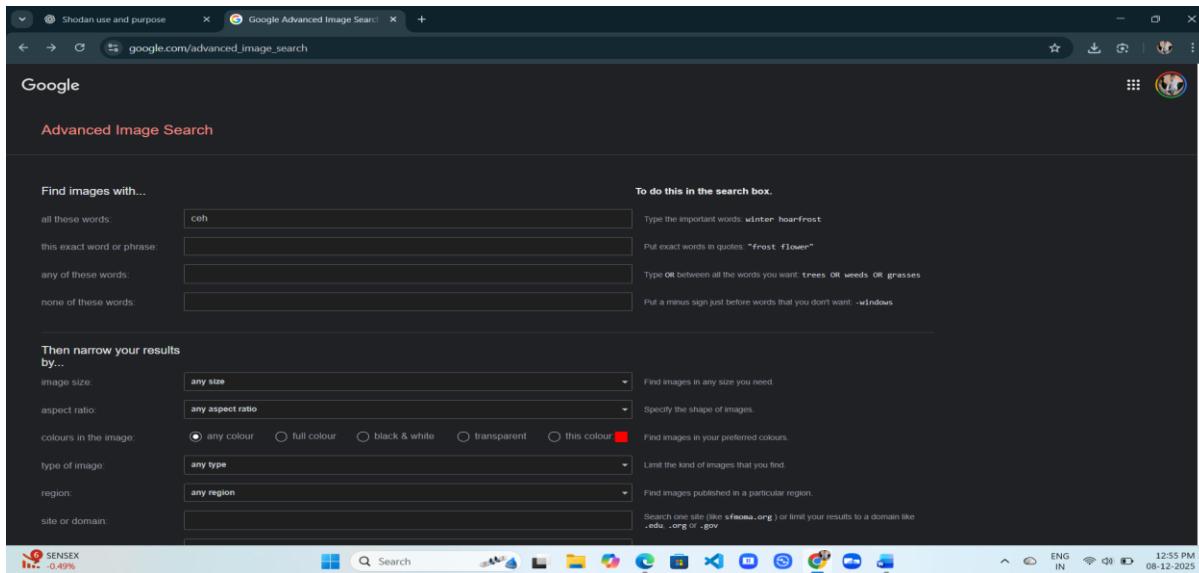


### Google Advanced image search

[https://www.google.com/advanced\\_image\\_search](https://www.google.com/advanced_image_search) in the address bar. Advanced image

search allows you to tweak your image search in a number of ways. You can search based on image color, domain, file type, size, keyword, and so on. To do this, you choose a field. Then, enter the string you want to search for in the field's text box and click on the Advanced Search button.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

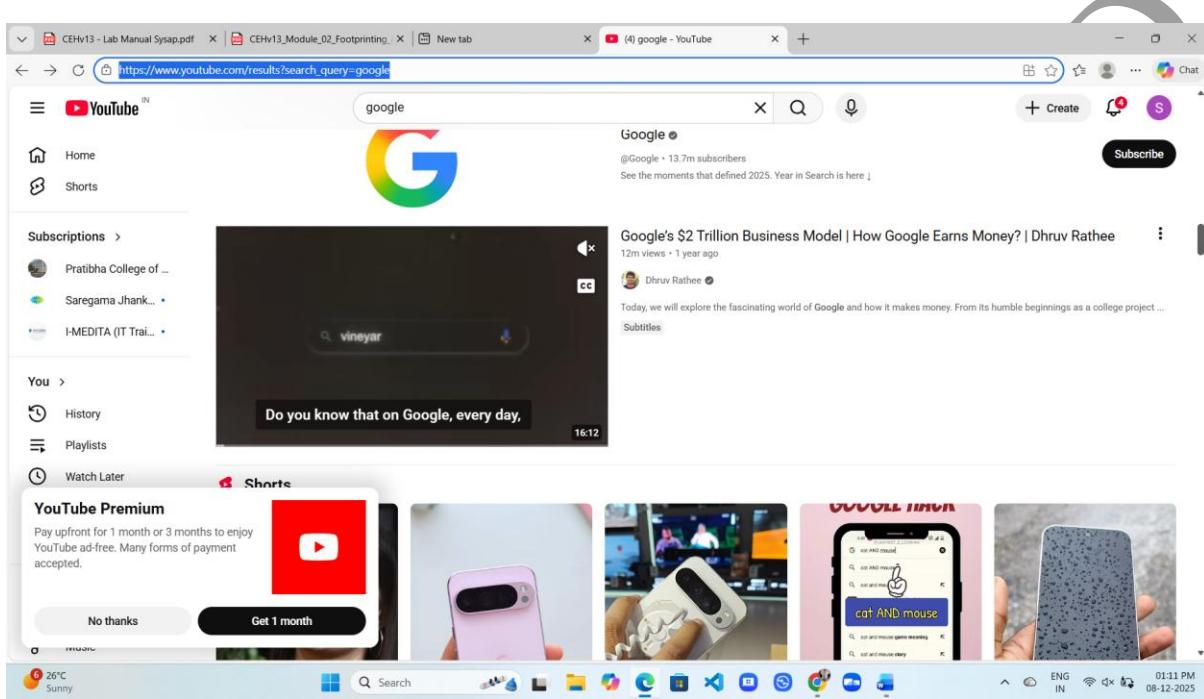


## Gathering Information from Video Search Engines

Video search engines are Internet-based search engines that crawl the web for video content. These video search engines either provide the functionality of uploading and hosting video content on their own web servers or parse video content that is hosted externally. The video content obtained from video search engines is of high value, as it can be used for gathering information about the target. Video search engines such as YouTube, Google videos, Yahoo videos, and Bing videos allow attackers to search for video content based on the format type and duration.

## MW Metadata :-

**Website:** - <https://mattw.io/youtube-metadata/>



01 MW Metadata Normal Bulk Search

MW Metadata normal grabs singular details about a YouTube video and its uploader, playlist and its creator, or channel.

Submit a link or id to a video, playlist, or channel

Accepted formats

- [https://www.youtube.com/watch?v=video\\_id](https://www.youtube.com/watch?v=video_id)
- [https://youtube.com/shorts/video\\_id](https://youtube.com/shorts/video_id)
- [https://youtu.be/video\\_id](https://youtu.be/video_id)
- [https://www.youtube.com/playlist?list=playlist\\_id](https://www.youtube.com/playlist?list=playlist_id)
- [https://www.youtube.com/channel/channel\\_id](https://www.youtube.com/channel/channel_id)
- <https://www.youtube.com/user/username>
- [https://www.youtube.com/@channel\\_handle](https://www.youtube.com/@channel_handle)
- [https://www.youtube.com/c/custom\\_url](https://www.youtube.com/c/custom_url)
- [https://www.youtube.com/c/custom\\_url](https://www.youtube.com/c/custom_url)
- Also accepts direct ids: `video_id, playlist_id, channel_id`

**Share**

Share this result:

What happened to export?

**Video**

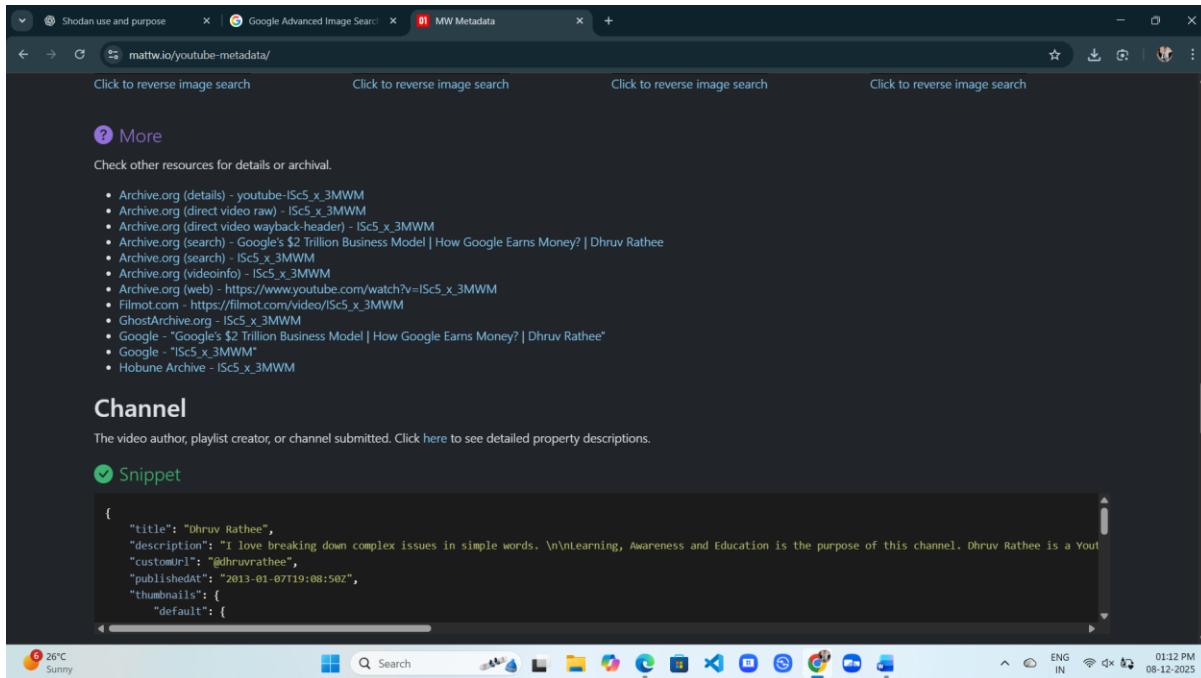
The video submitted. Click [here](#) to see detailed property descriptions.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

The screenshot shows a web browser window with three tabs: 'Shodan use and purpose', 'Google Advanced Image Search', and 'mattw.io/youtube-metadata'. The main content area displays the metadata for a video titled 'Google's \$2 Trillion Business Model | How Google Earns Money? | Dhruv Rathee'. The video thumbnail features two men, one with glasses and a dollar sign on his head, and the other pointing. The video was published at 2024-06-19T10:23:24Z. The metadata includes a JSON snippet and a preview image.

This screenshot shows the same browser window with the 'mattw.io/youtube-metadata' tab active. It provides detailed metadata for the video, including publication date (Wed, 19 Jun 2024 10:23:24 GMT), tags (Dhruv Rathee, Dhruv, Rathee, Dhruv Rathee latest video, Indian YouTuber, Khan Sir, Khan Sir Patna, dhruvrathee, dhruv rathee youtube, dhruv rathee latest video, google, how google makes money, sundar pichai, story of google, business model of google, google business strategy, google business model explained, google financials, google revenue model, google pay, google model paper, podcast, case study, business case study, business model), category ID (27), default language (EN), audio language (HI), and video ID (15c5\_x\_3MWM). It also includes a link to inspect more videos and a statistics section showing view count, like count, favorite count, and comment count.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



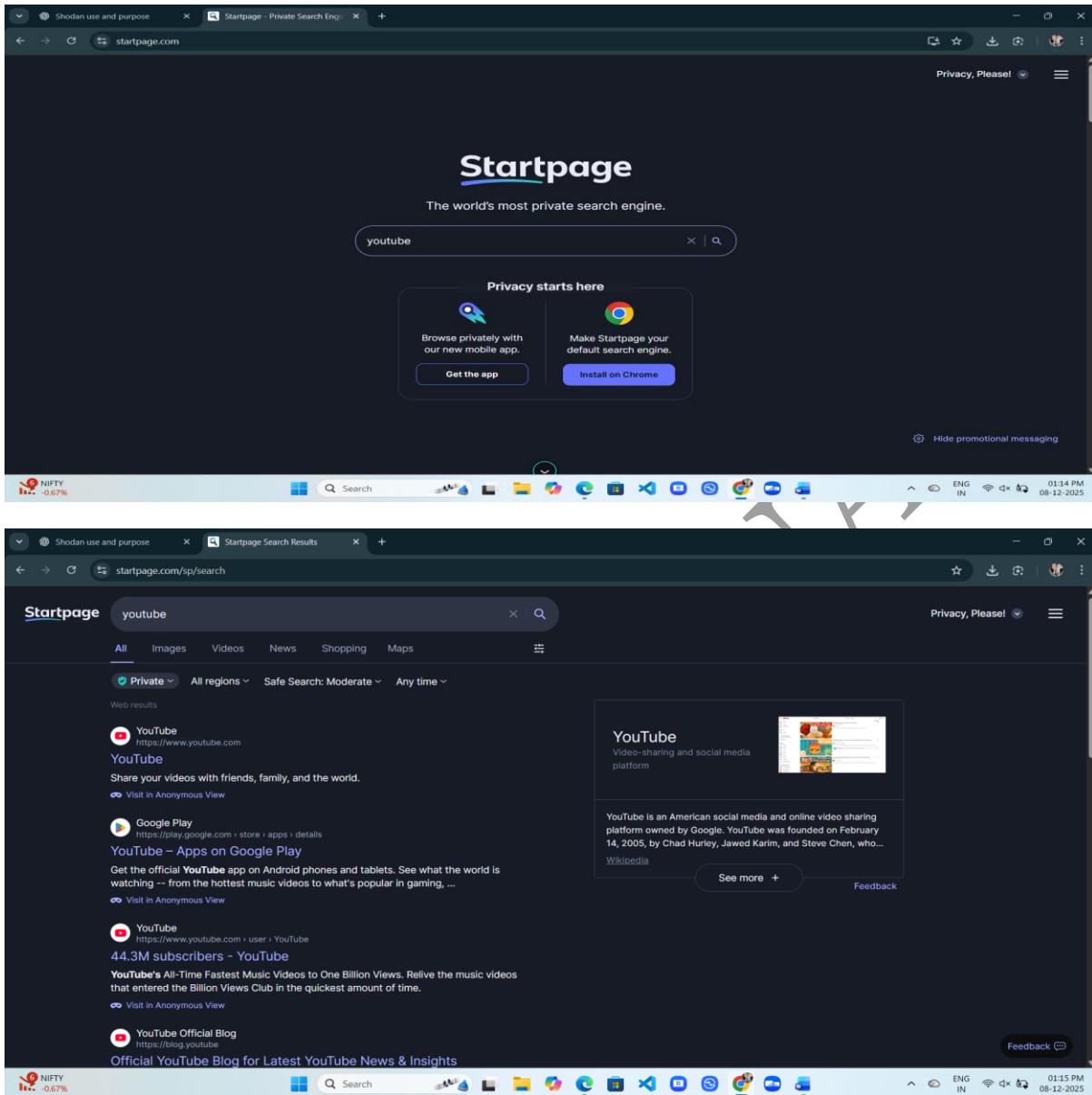
## Gathering Information from Meta Search Engines

**Meta search engines** (like Startpage, MetaGer, eTools.ch) don't have their own index — they send your query to multiple search engines at once, gather all results, remove duplicates, rank them, and show you a combined list. They're useful because you get **more results with the same effort**, making information gathering way faster and deeper.

**Startpage:** -

**Website:** - <https://www.startpage.com/>

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

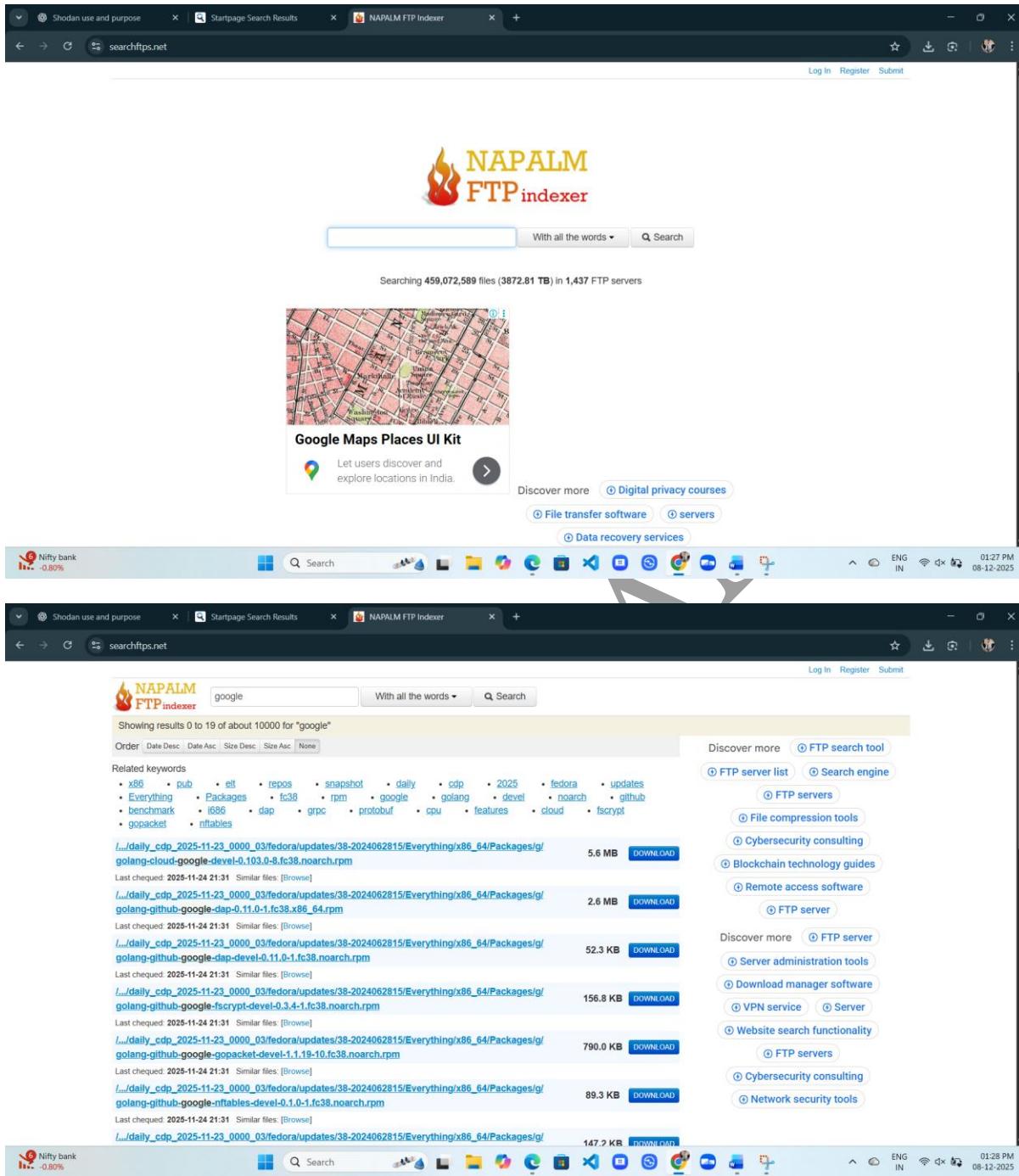


## FTP search engines

**FTP search engines** help you find files stored on public or poorly secured FTP servers.

Organizations often use FTP to store big archives, software, and internal files — and if those servers aren't protected properly, anyone can access them through a browser or an FTP client like FileZilla.

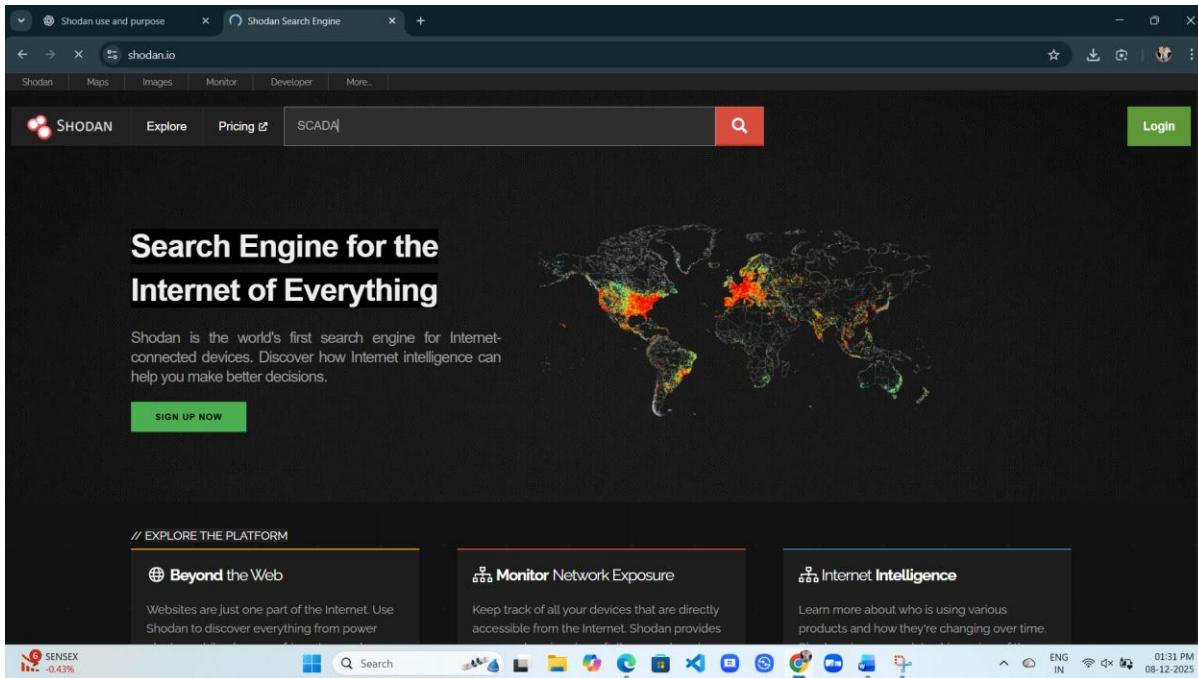
## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



## Gathering Information from IoT Search Engines

**IoT search engines** scan the internet to find publicly accessible IoT devices. Attackers can use them to discover exposed systems like SCADA, traffic controls, CCTV cameras, and smart appliances. Many IoT devices are weakly secured or still using default passwords, making them easy targets to exploit

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



**Search Engine for the Internet of Everything**

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

**SIGN UP NOW**

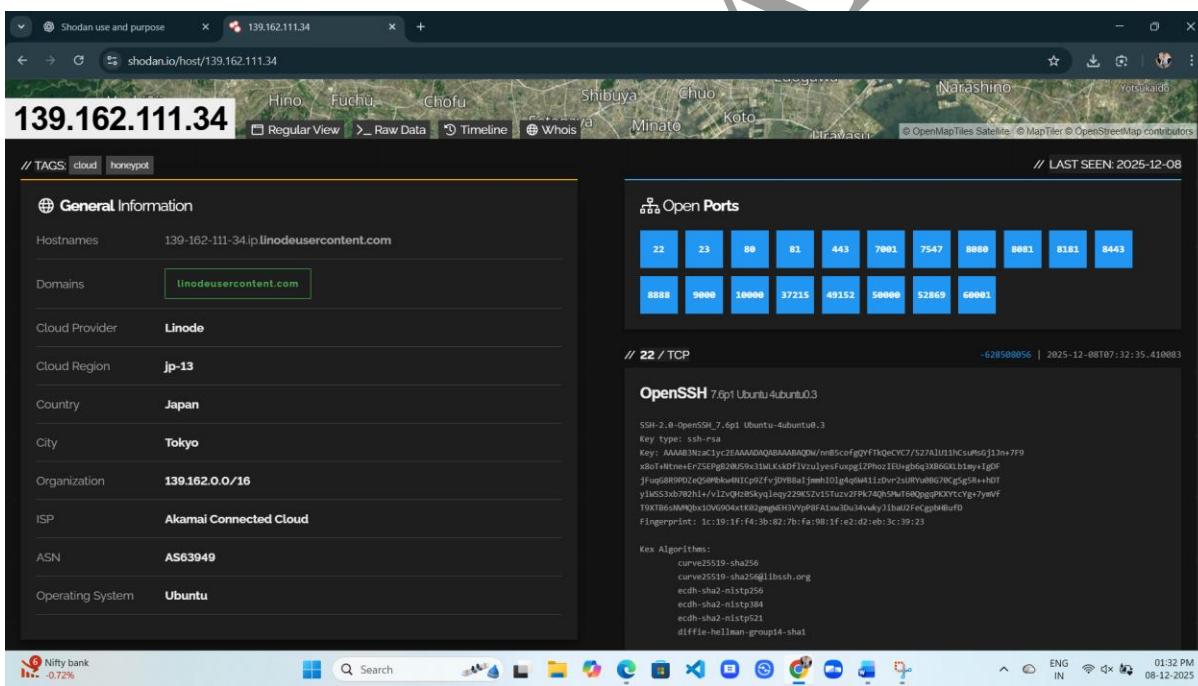
**Beyond the Web**  
Websites are just one part of the Internet. Use Shodan to discover everything from powerplants to medical devices.

**Monitor Network Exposure**  
Keep track of all your devices that are directly accessible from the Internet. Shodan provides real-time monitoring and alerting.

**Internet Intelligence**  
Learn more about who is using various products and how they're changing over time.

**SENSER** -0.43%

139.162.111.34



**General Information**

- Hostnames: 139-162-111-34.ip.linodeusercontent.com
- Domains: linodeusercontent.com
- Cloud Provider: Linode
- Cloud Region: jp-13
- Country: Japan
- City: Tokyo
- Organization: 139.162.0.0/16
- ISP: Akamai Connected Cloud
- ASN: AS63949
- Operating System: Ubuntu

**Open Ports**

22	23	80	81	443	7001	7547	8080	8081	8181	8443
8888	9000	10000	37215	49152	50000	52868	60001			

**SSH 22 / TCP**

Fingerprint: 1c:19:1f:f4:3b:82:7b:fa:98:1f:e2:d2:eb:3c:39:23

Key Algorithms:

```
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group14-sha1
```

SS

### 3. Footprinting through Internet Research Services

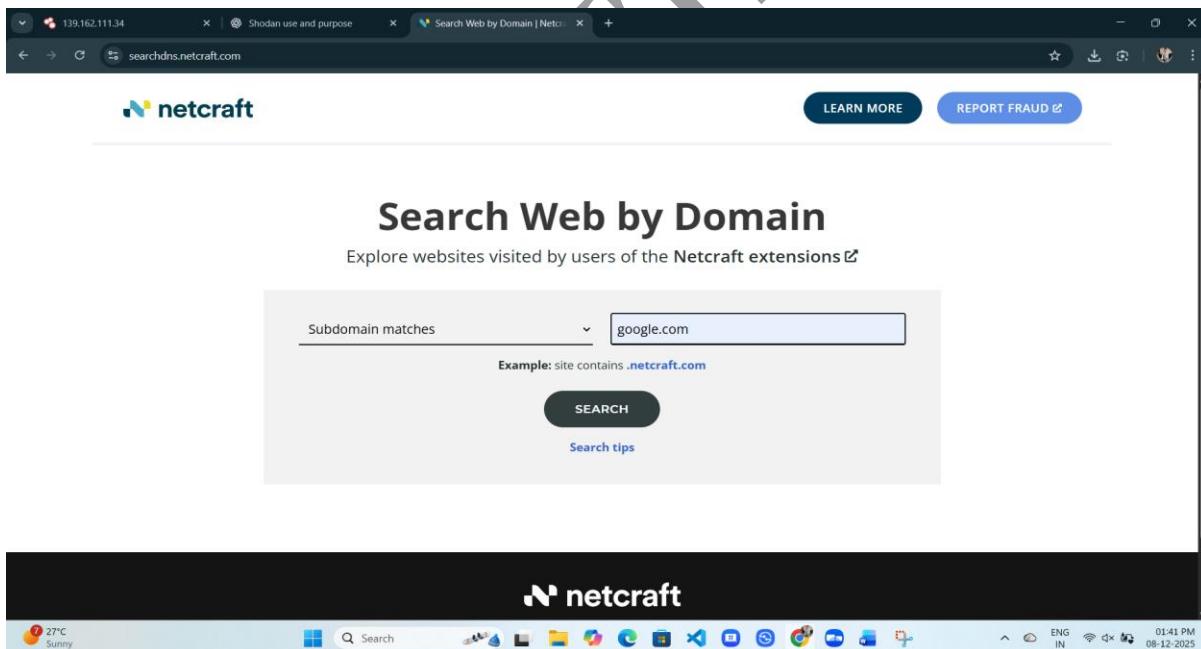
#### Tools to Search Company's Sub-domains

**Netcraft:** -

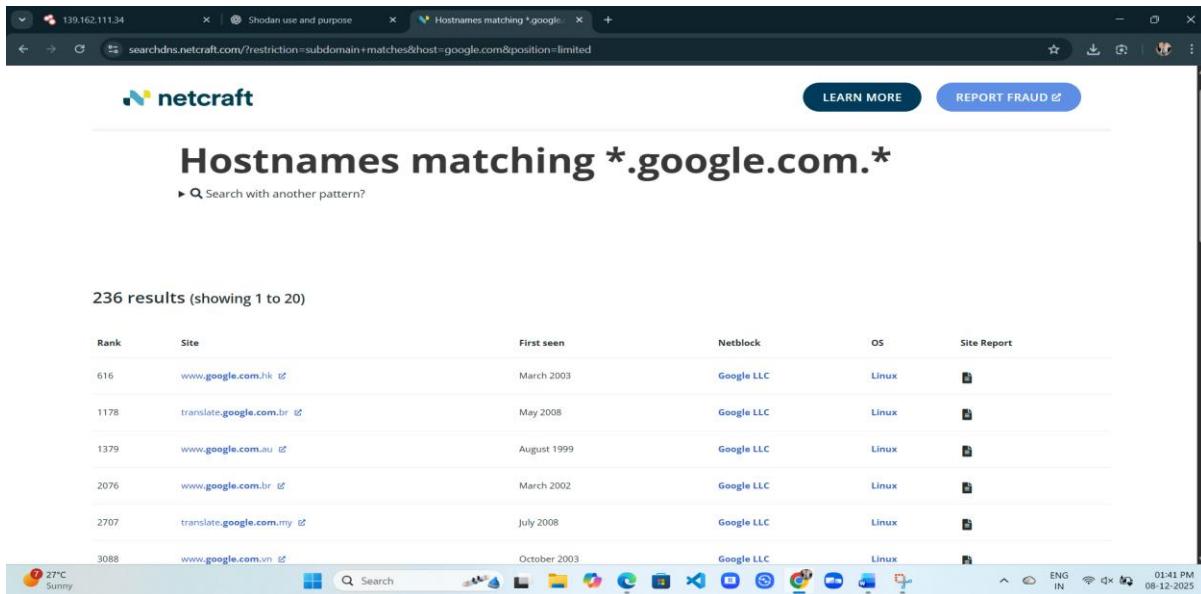
**Source:** <https://www.netcraft.com>

**Netcraft** is a security and internet analytics service that can reveal a company's **sub-domains**.

Attackers (and analysts) use it to check all domains linked to a target, along with details like hosting info, server tech, SSL data, and more — basically mapping the target's online footprint in one sweep.



## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



A screenshot of a web browser showing search results from Netcraft. The query is "Hostnames matching \*.google.com.\*". The results table shows 236 entries, with columns for Rank, Site, First seen, Netblock, OS, and Site Report. The first few entries include www.google.com.hk, translate.google.com.br, www.google.com.au, www.google.com.br, and translate.google.com.my. The browser interface includes a toolbar with various icons and a status bar at the bottom.

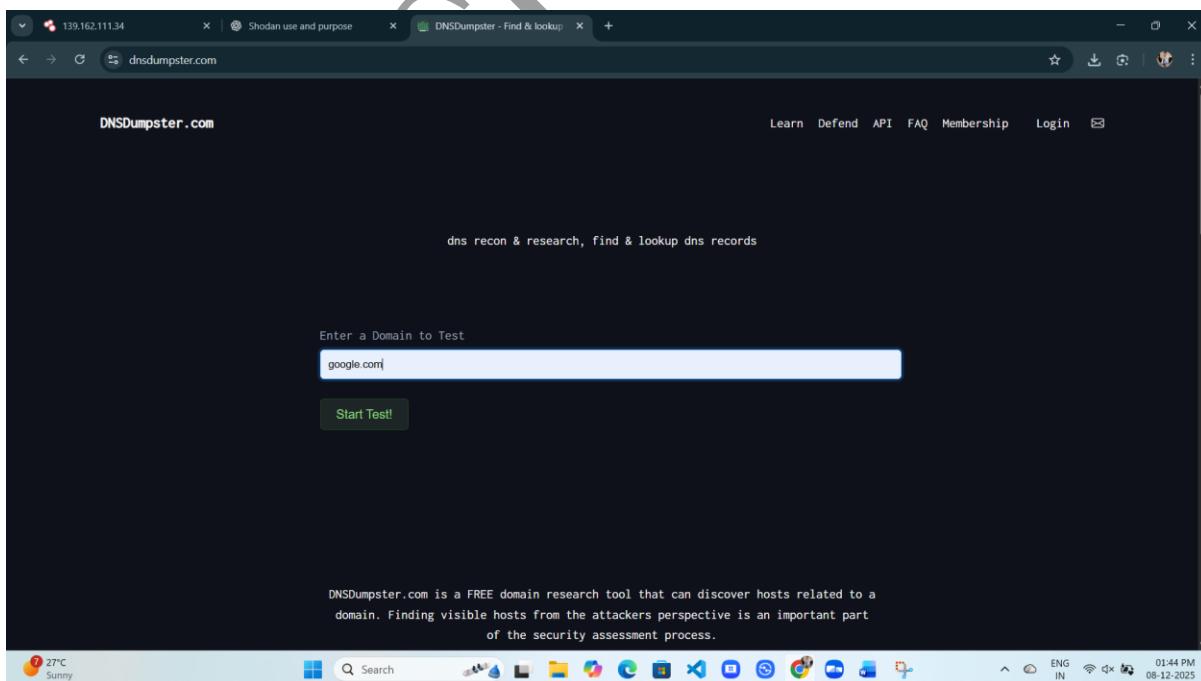
Rank	Site	First seen	Netblock	OS	Site Report
616	www.google.com.hk	March 2003	Google LLC	Linux	[link]
1178	translate.google.com.br	May 2008	Google LLC	Linux	[link]
1379	www.google.com.au	August 1999	Google LLC	Linux	[link]
2076	www.google.com.br	March 2002	Google LLC	Linux	[link]
2707	translate.google.com.my	July 2008	Google LLC	Linux	[link]
3088	www.google.com.vn	October 2003	Google LLC	Linux	[link]

## DNSdumpster: -

Source: <https://dnsdumpster.com>

**DNSdumpster** is a domain research tool used to find all hosts linked to a target domain.

Attackers use it to uncover subdomains, IP addresses, DNS servers, and other domain details — giving them a clearer map of the company's online structure.



A screenshot of a web browser showing search results from DNSdumpster. The query is "Enter a Domain to Test" followed by "google.com". The results page has a dark background with white text. It includes a subdomain search bar and a "Start Test!" button. A descriptive text at the bottom explains the tool's purpose: "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." The browser interface includes a toolbar with various icons and a status bar at the bottom.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

>> 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

Showing 50 records out of a total of 27166 found.

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
216-239-45-10.google.com	216.239.45.10	AS15169	GOOGLE		1
216-239-45-18.google.com	216.239.32.0/19		United States		
216-239-45-32.google.com	216.239.45.32	AS15169	GOOGLE		1
216-239-45-32.google.com	216.239.32.0/19		United States		
216-239-45-33.google.com	216.239.45.33	AS15169	GOOGLE		1
216-239-45-33.google.com	216.239.32.0/19		United States		

admin.google.com      172.217.12.110      AS15169      GOOGLE      United States      http: gws      285

at126s14-in-f14.firebaseio.net      172.217.12.0/24      United States      https: gws      title: 301 Moved      tech: Google Web Server

admob.google.com      142.250.141.101      AS15169      GOOGLE      United States      http: gws      2

dd-in-f18.firebaseio.net      142.250.141.0/24      United States      https: gws      title: 301 Moved      tech: Google Web Server

ads.google.com      142.251.46.238      AS15169      GOOGLE      United States      http: gws      179

sfb03s27-in-f14.firebaseio.net      142.251.46.0/24      United States      https: gws      title: 301 Moved      tech: Google Web Server

adscreativestudio.google.com      142.250.189.174      AS15169      GOOGLE      United States      http: gws      188

sfb03s24-in-f14.firebaseio.net      142.250.189.0/24      United States      https: gws      title: 301 Moved      tech: Google Web Server

## Pentest-Tools Find Subdomains

Source: <https://pentest-tools.com>

**Pentest-Tools Find Subdomains** is an online tool that identifies a domain's subdomains along with their IPs and technical details.

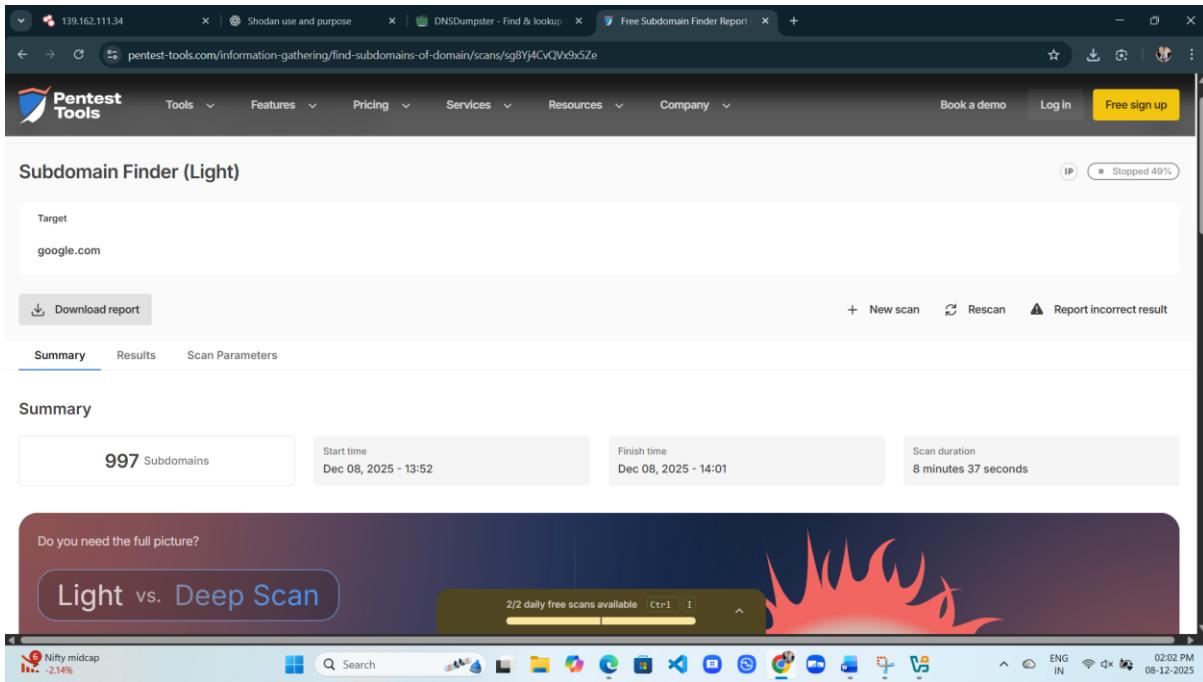
Attackers use it to gather info like servers, operating systems, technologies, and web platforms tied to the target — basically mapping the whole tech stack.

The screenshot shows the Pentest-Tools Subdomain Finder page. At the top, there are tabs for 'Light scan' and 'Deep scan'. A 'Target' field contains 'google.com'. Below the target field is a large yellow 'Start scan' button. On the left side of the page, there is a section titled 'Subdomain Finder' with a brief description of its capabilities. At the bottom of the main content area, there is a 'Scan with a Free account' button. The browser status bar at the bottom indicates '2/2 daily free scans available'.

The screenshot shows the results page of the Pentest-Tools Subdomain Finder. The top navigation bar includes 'Summary', 'Results' (which is selected), and 'Scan Parameters'. A message box says 'Scan stopped' and 'Scan stopped at 49%'. The main table lists subdomains and their corresponding IP addresses. The table has two columns: 'Subdomain' and 'IP Address'. Some subdomains listed include 'redbeard.mtv.corp.google.com', 'google-proxy-66-249-84-191.google.com', and 'mail-sor-f72.google.com'. The browser status bar at the bottom indicates '2/2 daily free scans available'.

Subdomain	IP Address
redbeard.mtv.corp.google.com	N/A
google-proxy-66-249-84-191.google.com	66.249.84.191
orchid-color.printer.corp.google.com	N/A
ccure-mon-proxy02.cbf.corp.google.com	N/A
rate-limited-proxy-203-208-38-52.google.com	203.208.38.52
rate-limited-proxy-74-125-151-188.google.com	74.125.151.188
antiviruspre02-1.cache.l.google.com	N/A
google-proxy-64-233-173-120.google.com	64.233.173.120
mail-sor-f72.google.com	209.85.220.72

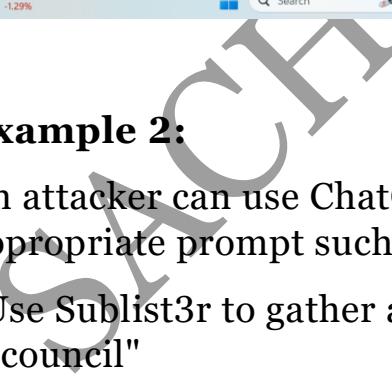
## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



## Finding a Company's Top-Level Domains (TLDs) and Sub-domains with AI

### Example 1:

A prompt like “*Find subdomains of google.com using dig*” can make AI generate a technical lookup command.

```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Gemini - gemini-cli
Session Actions Edit View Help
2. Be specific for the best results.
3. Create GEMINI.md files to customize your interactions with Gemini.
4. /help for more information.

> Discover all the subdomains of 'google.com' using dig command
• This command will attempt to perform a DNS zone transfer (AXFR) for the domain 'google.com'. This can reveal all subdomains configured for that domain, although it is often restricted by DNS servers for security reasons.
  ✓ Shell dig axfr google.com (This command will attempt to perform a DNS zone transfer (AXFR) for the domain 'google.com'. This can reveal all subdomains configured for that domain, although it is often restricted by DNS servers for security reasons.
    ☐ Connection to 192.168.1.103(192.168.1.1) for google.com failed: timed out.
    ☐ no servers could be reached
    ☐ Connection to 192.168.1.103(192.168.1.1) for google.com failed: timed out.
    ☐ no servers could be reached
    ☐ Connection to 192.168.1.103(192.168.1.1) for google.com failed: timed out.
    ☐ Connection to fe80::a291:caff:fe02:bb01%2#3(fe80::a291:caff:fe02:bb01%2#2) for google.com failed: timed out.
    ☐ no servers could be reached
  • The previous attempt to discover subdomains using a zone transfer failed, likely because it's disabled for google.com. I will now try to find subdomains by querying for some common ones.

  ✓ Shell dig www.google.com (This command will query the DNS for the subdomain 'www.google.com'.)
    ☐ exec: 0 > /usr/bin/dig www.google.com
    ☐ global options: +cmd
    ☐ Got answer:
      =HEADER=  opcode: QUERY, status: NOERROR, id: 31804
      Flags: qr rd ra QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 3
      OPT PSEUDOSECTION:
      EDNS: version: 0, flags: +udt
      SECTION:
      www.google.com.          IN   A
      ANSWER SECTION:
      www.google.com.      52   IN   A   142.251.222.100
    ☐ Query time: 26 msec
    ☐ TTL: 1747 sec
    ☐ WHEN: Mon Dec 08 14:10:57 IST 2025
    ☐ MSG SIZE rcvd: 59
  • Okay, www.google.com resolved. Now I'll check for mail, ftp, and blog subdomains in parallel.call:run_shell_command[command]:
    ? Shell dig mail.google.com (This command will query the DNS for the subdomain 'mail.google.com'.) +
      dig mail.google.com
      Allow execution of: 'dig'?
      • 1. Yes, allow once

```

### Example 2:

An attacker can use ChatGPT to perform this task by using an appropriate prompt such as:

"Use Sublist3r to gather a list of subdomains of the target organization eccouncil"

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Shell dig ftp.google.com (This command will query the DNS for the subdomain 'ftp.google.com'.)
> use Sublist3r to gather a list of subdomains of the target organization ecouncil
* This command will use Sublist3r to find subdomains of ecouncil.org.
v Shell sublist3r -d ecouncil.org (This command will use Sublist3r to find subdomains of ecouncil.org.)
bash: line 1: sublist3r: command not found
* sublist3r failed. I'll try gobuster dns instead. First, I'll check if gobuster is installed, then I'll try to find a wordlist and run it against ecouncil.org.
v Shell gobuster -h (This command checks if gobuster is installed and shows its help message.)
NAME: gobuster - the tool you love
USAGE: gobuster command [command options]
VERSION: 3.0
AUTHORS:
  Christian Mehlmauer (@firefart)
  Tim Reeves (@TheColonial)
COMMANDS:
  dir  Uses directory/file enumeration mode
  vhost  Uses VHOST enumeration mode (you most probably want to use the IP address as the URL parameter)
  dns  Uses DNS subdomain enumeration mode
  fuzz  Uses Fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body
  trtf  Uses TRTF enumeration mode
  s3  Uses aws Bucket enumeration mode
  gcs  Uses gcs Bucket enumeration mode
  help, h  Shows a list of commands or help for one command
GLOBAL OPTIONS:
  --help, -h  show help
  --version, -v  print the version
* Okay, gobuster is installed. I'll find a wordlist for it, starting with /usr/share/wordlists/dirb/common.txt, and if that fails, I'll search for an alternative. I'll use ls to check for the file.
v Shell ls /usr/share/wordlists/dirb/common.txt (This command checks for the existence of the wordlist file '/usr/share/wordlists/dirb/common.txt'.)
/usr/share/wordlists/dirb/common.txt
* Okay, I'm using gobuster with the common.txt wordlist to find subdomains of ecouncil.org.
[+] Shell gobuster dns -d ecouncil.org -w /usr/share/wordlists/dirb/common.txt (This command will use gobuster to enumerate subdomains of ecouncil.org using a common wordlist.) *
```

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
v Shell ls /usr/share/wordlists/dirb/common.txt (This command checks for the existence of the wordlist file '/usr/share/wordlists/dirb/common.txt'.)
/usr/share/wordlists/dirb/common.txt
* Okay, I'm using gobuster with the common.txt wordlist to find subdomains of ecouncil.org.
v Shell gobuster dns -d ecouncil.org -w /usr/share/wordlists/dirb/common.txt (This command will use gobuster to enumerate subdomains of ecouncil.org using a common wordlist.)
Incorrect Usage: invalid value "ecouncil.org" for flag -d: parse error
NAME: gobuster dns - Uses DNS subdomain enumeration mode
USAGE: gobuster dns command [command options] [arguments ...]
COMMANDS:
  help, h  Shows a list of commands or help for one command
OPTIONS:
  --domain value, -d value      The target domain
  --check-cname, -c              Also check CNAME records (default: False)
  --timeout value, -t value     DNS resolver timeout (default: 1s)
  --wildcard, -w value          Force continued operation when wildcard found (default: False)
  --dns value, -d value         Do a DNS search by adding dot to the domain, so the resolver uses the DNS search domain (default: False)
  --resolver value, -r value    Use custom DNS server (format server.com or server.com:port)
  --protocol value, -p value    Use either 'udp' or 'tcp' as protocol on the custom resolver (default: "udp")
  --threads value, -t value    Number of concurrent threads (default: 10)
  --delay value, -d value      Time each thread waits between requests (e.g. 150ms) (default: 0s)
  --threads-offset value, -mo value  Resume from a given position in the wordlist (default: 0)
  --max-tries value, -m value   Maximum number of tries to connect (default: 3)
  --quiet, -q                  Don't print the banner and other noise (default: False)
  --no-progress, --np           Don't display progress (default: False)
  --no-error, --ne              Don't display errors (default: False)
  --pattern-value, -p value    File containing replacement patterns
  --discover-pattern value, -dp value  File containing replacement patterns applied to successful guesses
  --no-color, --nc              Disable color output (default: False)
  --no-output, --no             suppress output (default: False)
  --help, -h                   show help
2023/08/20 14:15:38 invalid value "ecouncil.org" for flag -d: parse error
Running the subdomain scan (esc to cancel, 8s)

2 Type your message or @path/to/file
/usr/lib/gemini-cl1
no sandbox (see /docs)
gemini-2.5-pro (99% context left)
```

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

```
[ERRONEOUS] error on word mp: lookup ap.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word root: lookup wwwroot.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word wwwsql: lookup wwwsql.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word wwwthreads: lookup wwwthreads.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word wwwxml: lookup wwwxml.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word wysiwyg: lookup wysiwyg.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word ajax: lookup ajax.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word search: lookup search.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word cache: lookup cache.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word zips: lookup zips.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word zones: lookup zones.eccouncil.org.: i/o timeout
[ERRONEOUS] error on word zt: lookup zt.eccouncil.org.: i/o timeout

* Have successfully found a number of subdomains for eccouncil.org.
Here is a list of the subdomains that were found:
- affiliate.eccouncil.org
- affiliates.eccouncil.org
- blog.eccouncil.org
- campaign.eccouncil.org
- careers.eccouncil.org
- cert.eccouncil.org
- community.eccouncil.org
- dev.eccouncil.org
- ebooks.eccouncil.org
- events.eccouncil.org
- foundation.eccouncil.org
- helpdesk.eccouncil.org
- identity.eccouncil.org
- learning.eccouncil.org
- learn.eccouncil.org
- learning.eccouncil.org
- payment.eccouncil.org
- payments.eccouncil.org
- staging.eccouncil.org
- test.eccouncil.org
- www.eccouncil.org

> Type your message or <path/to/file
```

/usr/lib/gemini-cli no sandbox (see /docs) gemini-2.5-pro (98% context left)

27°C Sunny 02:21 PM 08-12-2025

### Using Sublist3r to Gather Subdomains

#### Command:

```
sublist3r -d eccouncil.org -o eccouncil_subdomains.txt
```

#### What it does:

1. **sublist3r** – This calls the Sublist3r tool. Think of it as your digital telescope for spotting all the little corners (subdomains) of a website.
2. **-d eccouncil.org** – The **-d** flag tells Sublist3r, “Hey, focus on this domain.” In this example, it’s `eccouncil.org`. That’s your target organization.
3. **-o eccouncil\_subdomains.txt** – The **-o** flag is for output. All the subdomains Sublist3r finds are neatly dumped into this file, so you don’t have to scroll endlessly in the terminal. Here, it’s saved as `eccouncil_subdomains.txt`.

**Result:** You end up with a list of subdomains like `mail.eccouncil.org`, `blog.eccouncil.org`, etc., which can be super useful for reconnaissance or penetration testing exercises.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

```
root@kali:~/home/sachet
File Machine View Input Devices Help
Session Actions Edit View Help
/usr/lib/python3/dist-packages/sublist3r.py:287: SyntaxWarning: invalid escape sequence '\'
/usr/lib/python3/dist-packages/sublist3r.py:287: SyntaxWarning: invalid escape sequence '\'
/usr/lib/python3/dist-packages/sublist3r.py:287: SyntaxWarning: invalid escape sequence '\'
line = re.sub('<(.V)7b>', "", link)
/usr/lib/python3/dist-packages/sublist3r.py:440: SyntaxWarning: invalid escape sequence '\'
line = re.compile('<(.V)7b>.*>').findall(link)
/usr/lib/python3/dist-packages/sublist3r.py:688: SyntaxWarning: invalid escape sequence '\'
tbl_regex = re.compile('<a name="hostanchor"></a>Host Records:<table>.*</table>', re.S)
/usr/lib/python3/dist-packages/sublist3r.py:690: SyntaxWarning: invalid escape sequence '\'
domain_check = re.compile('^(http|https)://[a-zA-Z0-9]+([\\.,][a-zA-Z0-9]+)*([\\.,][a-zA-Z0-9]+[2,4])$')
Processing triggers for kali-menu (2.025.4.2) ...
Processing triggers for man-db (2.13.1-1) ...
Reading package lists...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (QEMU) binaries on this host.
root@kali:~/home/sachet]
└─# sublist3r -d ecncouncil.org -o ecncouncil_subdomains.txt

Sublist3r v1.0.0
# Coded By Ahmed Aboul-Ela - @aboulla

[-] Enumerating subdomains now for ecncouncil.org
[-] Searching now in Baidu...
[-] Searching now in Yahoo...
[-] Searching now in Bing...
[-] Searching now in Ask...
[-] Searching now in DuckDuck...
[-] Searching now in DNSdumpster...
[-] Searching now in VirusTotal...
[-] Searching now in Shodan...
[-] Searching now in SSL Certificates...
[-] Searching now in PassivesON...
[-] Error: VirusTotal probably now is blocking our requests
[+] Saving results to file: ecncouncil_subdomains.txt
[+] Found 38 subdomains found: 38
ecncouncil.org
affiliate.ecncouncil.org
aspen.ecncouncil.org
associate-ciso.ecncouncil.org
aware.ecncouncil.org
hosting.ecncouncil.org
campaign.ecncouncil.org
cert.ecncouncil.org
ctfteam.ecncouncil.org
ciso.ecncouncil.org
codered.ecncouncil.org
cohort.ecncouncil.org
codered-instructors.ecncouncil.org
coderedcheckout.ecncouncil.org
coderedmarketing.ecncouncil.org
community.ecncouncil.org
ctfevent-dev.ecncouncil.org
cybersec.ecncouncil.org
cybersecurity.ecncouncil.org
dev-gravity.ecncouncil.org
esca-grandfathering.ecncouncil.org
egg.ecncouncil.org
ethicalhacking.ecncouncil.org
Frontend-coded.ecncouncil.org
ITX.ecncouncil.org
identity.ecncouncil.org
labs.ecncouncil.org
administrator-coded.ecncouncil.org
lambdas.ecncouncil.org
learn.ecncouncil.org
nextgen.ecncouncil.org
nxtgen.ecncouncil.org
store.ecncouncil.org
ust-learn.ecncouncil.org
wissen.ecncouncil.org
[+] 38
[+] 38
[+] 38
```

```
root@kali:~/home/sachet
File Machine View Input Devices Help
Session Actions Edit View Help
file "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
IndexError: list index out of range
[-] Saving results to file: ecncouncil_subdomains.txt
[+] Found 38 subdomains found: 38
ecncouncil.org
affiliate.ecncouncil.org
aspen.ecncouncil.org
associate-ciso.ecncouncil.org
aware.ecncouncil.org
hosting.ecncouncil.org
campaign.ecncouncil.org
cert.ecncouncil.org
ctfteam.ecncouncil.org
ciso.ecncouncil.org
codered.ecncouncil.org
cohort.ecncouncil.org
codered-instructors.ecncouncil.org
coderedcheckout.ecncouncil.org
coderedmarketing.ecncouncil.org
community.ecncouncil.org
ctfevent-dev.ecncouncil.org
cybersec.ecncouncil.org
cybersecurity.ecncouncil.org
dev-gravity.ecncouncil.org
esca-grandfathering.ecncouncil.org
egg.ecncouncil.org
ethicalhacking.ecncouncil.org
Frontend-coded.ecncouncil.org
ITX.ecncouncil.org
identity.ecncouncil.org
labs.ecncouncil.org
administrator-coded.ecncouncil.org
lambdas.ecncouncil.org
learn.ecncouncil.org
nextgen.ecncouncil.org
nxtgen.ecncouncil.org
store.ecncouncil.org
ust-learn.ecncouncil.org
wissen.ecncouncil.org
[+] 38
[+] 38
[+] 38
```

### Extracting Website Information from <https://archive.org>

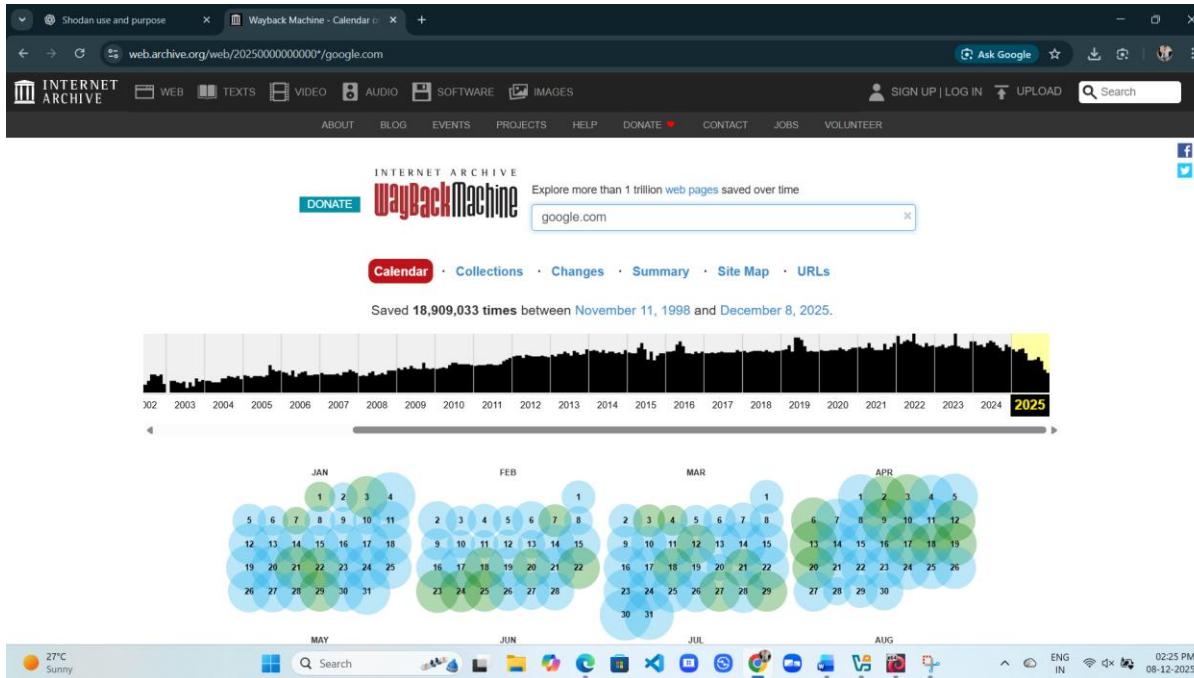
Source: <https://archive.org>

**Archive.org (Wayback Machine)** stores old versions of websites.  
Attackers can use it to view past pages, deleted content, images, files, and other

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

info a company once had online.

This old data can help them craft phishing attacks or understand how the website evolved.



## Using Photon to Retrieve Archived URLs from archive.org

### Photon: -

Attackers often turn to tools like **Photon** to uncover archived pages of a target website. Why? Because the past never really disappears—old URLs, outdated endpoints, and forgotten directories often sit preserved on **archive.org (Wayback Machine)**, waiting to be rediscovered.

To collect these archived URLs, the following Photon command is used:

```
python3 photon.py -u <URL_of_Target_Website> -l 3 -t 200 --wayback
```

### Explanation of the Command

- **python3 photon.py**  
Launches the Photon crawler.
- **-u <URL\_of\_Target\_Website>**  
Specifies the target website you want to analyze.  
Replace this placeholder with something like:  
-u https://example.com

## **MODULE – 2 FOOTPRINTING AND RECONNAISSANCE**

- **-l 3**  
Sets the crawl depth to level 3, allowing Photon to dig a few layers deep into the site structure.
  - **-t 200**  
Runs the scan with 200 threads to speed up processing.
  - **--wayback**  
Instructs Photon to fetch URLs preserved on **archive.org**, helping uncover older or deleted pages that may still expose sensitive information.

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
--timeout TIMEOUT http request timeout
--proxy PROXIES Proxy server IP or DOMAIN:PORT
--check-links check website locally
--headers add headers
--dns enumerate subdomains and DNS data
--filter filter URLs
--update update photon
--only-urls only extract URLs
--wayback fetch URLs from archive.org as seeds

[+] root@kali:[/home/sachet/Photon]
# python3 photon.py -u URL_of_Target_Website -l 3 -t 200 --wayback
zsh: no such file or directory: URL_of_Target_Website

[+] root@kali:[/home/sachet/Photon]
# python3 photon.py -u URL_of_Target_Website -l 3 -t 200 --wayback
zsh: no such file or directory: URL_of_Target_Website

[+] root@kali:[/home/sachet/Photon]
# python3 photon.py -u URL_of_Target_Website -l 3 -t 200 --wayback
zsh: no such file or directory: URL_of_Target_Website

[+] root@kali:[/home/sachet/Photon]
# python3 photon.py -u certifiedhacker.com -l 3 -t 200 --wayback
/home/sachet/photon/photon.py:19: SyntaxWarning: invalid escape sequence '\'
/ %s\%s V %s ____ /____ __

[!] Fetching URLs from archive.org
[+] Retrieved 1 URLs from archive.org
[+] Level 1: 1 URLs
Progress: 1/1
[+] Internal: 1 URLs
[+] External: 0 URLs
[+] Progress: 2/2
[+] Crawling 0 JavaScript files

[+] Internal: 0
[+] External: 2

[!] Total requests made: 4
[!] Total time taken: 0 minutes 12 seconds
[!] Total size per download: 0 bytes
[!] Results saved in certifiedhacker.com directory

[+] root@kali:[/home/sachet/Photon]
# BSE midcap -1.89%
[?] Search
ENG IN 02:38 PM 08-12-2025
```

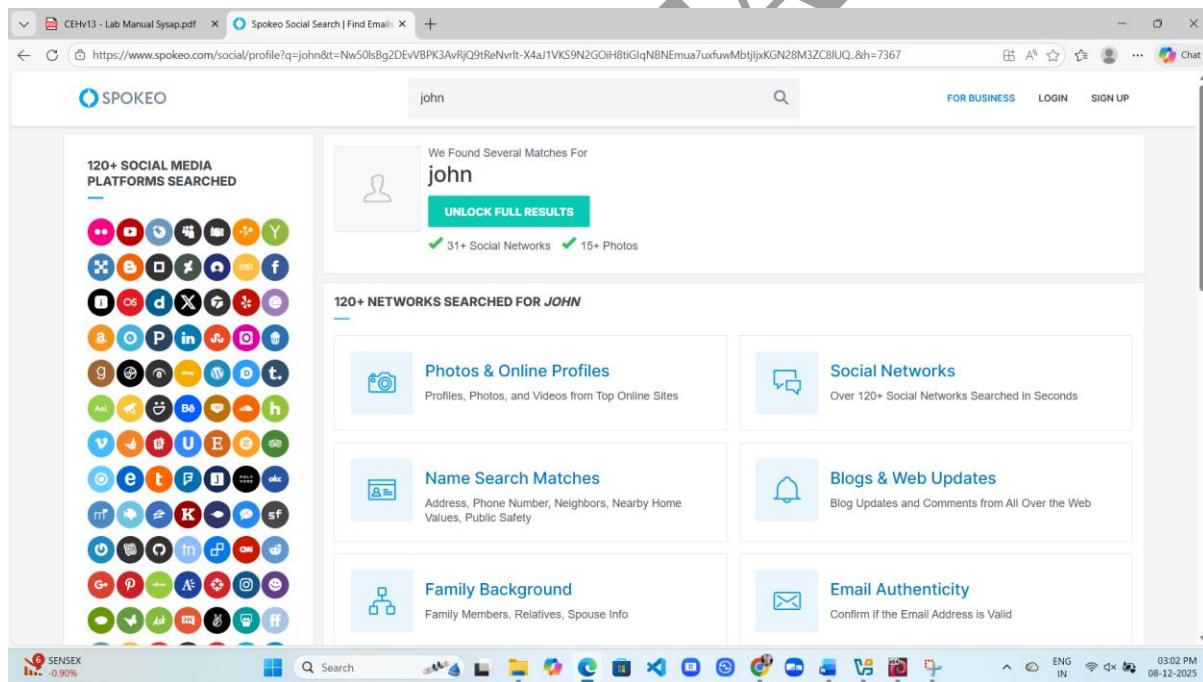
## Footprinting Through People Search Services

When attackers go digging for clues, they don't always start with firewalls and fancy exploits. Sometimes the softest spots are the humans themselves. Public record websites—those people-search platforms everyone forgets they ever signed up for—can spill more than folks realize.

### People Search Service – Spokeo

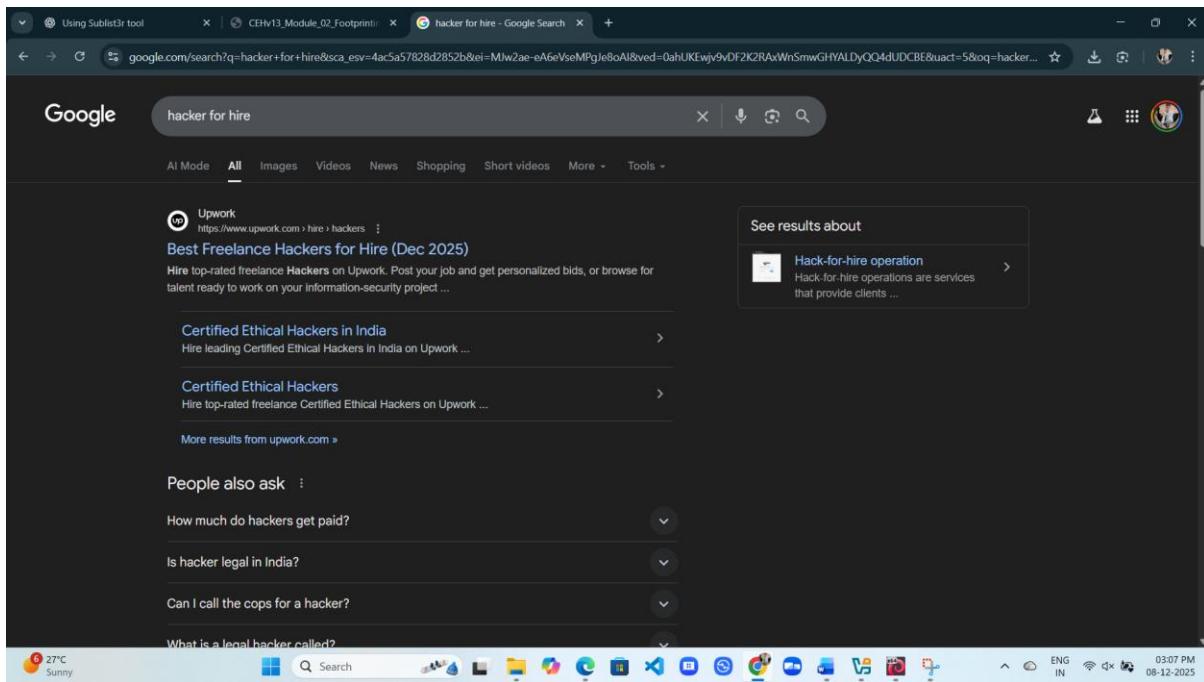
**Source:** <https://www.spokeo.com>

Attackers may use **Spokeo**, a popular online people-search service, to look up individuals associated with a target organization. By entering a person's name, email address, phone number, or location, Spokeo aggregates information from public records and online sources.



## Dark Web Footprinting

When investigators or attackers want to move beyond the visible internet, they step past the familiar glow of the **surface web** and into the shadows beneath it. Understanding these layers is key to knowing how information is discovered, hidden, or exploited.



## Determining the Operating System

Attackers use various online tools such as **Netcraft**, **Shodan**, and **Censys** to detect the operating system used by the target organization. These tools scan the Internet for connected devices such as routers, servers, and IoT devices belonging to the target organization.

Using these tools, attackers can gather information such as:

- City and country
- Latitude and longitude
- Hostname
- Operating system
- IP address

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

### Netcraft:-

**Source:** <https://www.netcraft.com>

The technique of obtaining information about the target network's operating system is known as **OS fingerprinting**.

The screenshot shows the Netcraft site report for <http://google.com>. The report includes the following sections:

- Background:** Site title: Google, Date first seen: November 1998; Site rank: 92, Primary language: English. Description: Search the world's information, including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking for.
- Network:** Shows a screenshot of a Windows taskbar with various icons and network status (27°C Sunny, ENG IN, 03:15 PM 08-12-2025).
- Domain:** Site: <http://google.com>, Domain: google.com. Details include: Netblock Owner: Google LLC, Nameserver: ns1.google.com; Hosting company: Google, Domain registrar: markmonitor.com; Hosting country: US, Nameserver organisation: whois.markmonitor.com; IPv4 address: 172.253.116.102 (VirusTotal), Organisation: Google LLC, United States; IPv4 autonomous systems: AS15169, DNS admin: dns-admin@google.com; IPv6 address: 2404:6800:4004:821:0:0:200e, Top Level Domain; IPv6 autonomous systems: AS15169, DNS Security Extensions; Reverse DNS: dj-in-f102.1e100.net.
- IP delegation:** IP Geolocation: We use multilateration to independently determine the location of a server. Read more. A map shows a blue line connecting locations in Europe, specifically highlighting Stockholm, Helsinki, and Tallinn.
- Geolocation:** A map showing the geographical location of the target server, with a blue line indicating its path through Europe.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

Rank	Site	First seen	Netblock	OS	Site Report
1	www.google.com	November 1998	Google LLC	Linux	<a href="#">Site Report</a>
3	mail.google.com	June 2004	Google LLC	Linux	<a href="#">Site Report</a>
5	docs.google.com	December 2006	Google LLC	Linux	<a href="#">Site Report</a>
10	accounts.google.com	March 2011	Google LLC	Linux	<a href="#">Site Report</a>
13	drive.google.com	January 2012	Google LLC	Linux	<a href="#">Site Report</a>
18	calendar.google.com	December 2005	Google LLC	Linux	<a href="#">Site Report</a>
27	translate.google.com	October 2008	Google LLC	Linux	<a href="#">Site Report</a>
29	gemini.google.com	April 2024	Google LLC	Linux	<a href="#">Site Report</a>
31	meet.google.com	October 2016	Google LLC	Linux	<a href="#">Site Report</a>
49	classroom.google.com	July 2014	Google LLC	Linux	<a href="#">Site Report</a>

27°C Sunny 03:16 PM 08-12-2025

## Censys:-

Source: <https://censys.io>

Censys is like the all-seeing lighthouse of the Internet — scanning, tracking, and revealing every server or device that dares to show its face online. It continuously monitors global Internet infrastructure to uncover known and unknown assets belonging to an organization.

Host	Labels	Services
62.109.8.5 (google.com)	RU-JSC-OT (2018)   Moscow, Russia   2.08M remote-access   647.92K vue.js   431.85K extjs   366.21K login-page   213.80K network.device.vpn	22/SSH   25/SMTP   53/DNS   80/HTTP   110/POP3   143/IMAP   443/HTTP   465/SMTP   587/SMTP   8083/HTTP   993/IMAP
193.24.123.252	Ubuntu Linux   PROSPERO-AS (200593)   St-Petersburg, Russia   4.86M GOOGLE-CLOUD-PLATFORM   125.33K GOOGLE   123.92K GOOGLE-2   69.26K KIXS-AS-KR Korea Telecom   65.09K GOOGLE-FIBER	21/FTP   22/SSH   53/DNS   80/HTTP   110/POP3   143/IMAP   443/HTTP   8083/HTTP   993/IMAP
209.74.89.117	NAMECHEAP-NET (22612)   California, United States   3.59M United States   319.56K Belgium   249.60K Germany   199.53K Netherlands	21/FTP   22/SSH   25/SMTP   53/DNS   80/HTTP   111/PORTMAP   111/PORTMAP   143/IMAP   995/POP3   2077/HTTP   443/HTTP   587/SMTP   993/IMAP   2087/HTTP   8083/TCP-HTTP

27°C Sunny 03:20 PM 08-12-2025

## Competitive Intelligence (CI) Gathering

Competitive intelligence is basically playing detective—but the *ethical*, no-crime version. You’re scouting out what other businesses are doing, how they position their products, and what customers think about them—without breaking the law or sneaking around. Think of it as *learning from the battlefield without firing a shot*.

### Sources of Competitive Intelligence

CI can be gathered **directly** or **indirectly**:

#### 1. Direct Approach:

- Primary, hands-on method.
- Examples: Trade shows, talking to employees or customers (social engineering ethically!), attending industry events.

#### 2. Indirect Approach:

- Gather info from publicly available online sources.
- Examples:
  - Company websites & job postings
  - Customer reviews and support forums

## Gathering Information from Public Source-Code Repositories

Public source-code repositories—think **GitHub**, **GitLab**, **SourceForge**, **BitBucket**—are treasure troves for devs, but also for attackers. They’re basically online vaults where software pros stash:

- Configuration files
- SSH & SSL keys
- Source code files
- Dynamic libraries
- Custom software tools

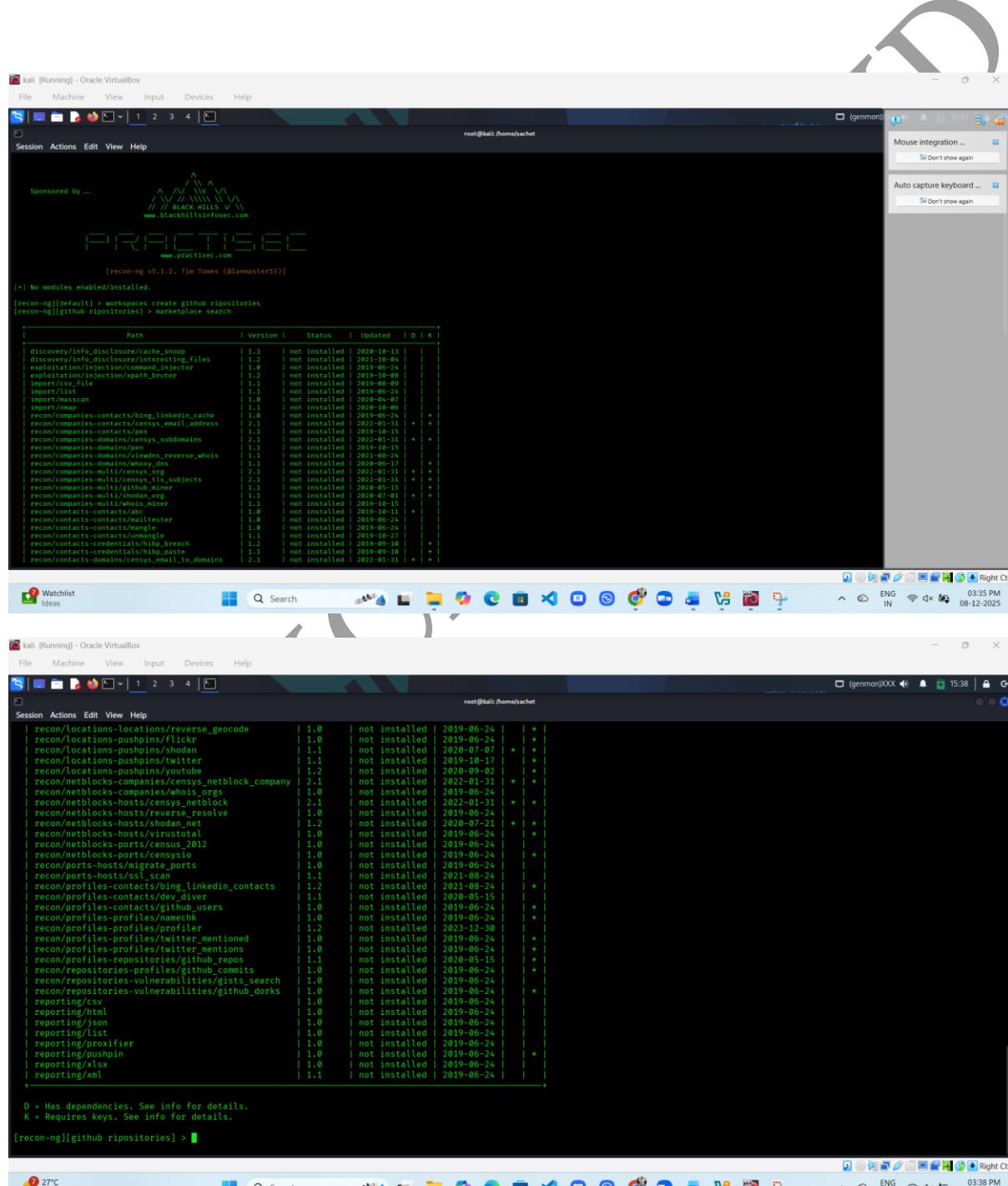
Developers use these repositories to **speed up development, patch apps quickly, and save costs**, often sharing code publicly or privately. But here’s the catch: even a tiny misstep can leak sensitive info.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

# Recon-**ng**

**Source:** <https://github.com>

Recon-*ng* is a full-blown reconnaissance framework built to make web-based recon feel less like a chore and more like a well-oiled operation. It gives attackers (and ethical hackers) a powerful, modular environment to sweep the Internet for intel—fast, structured, and dangerously efficient.

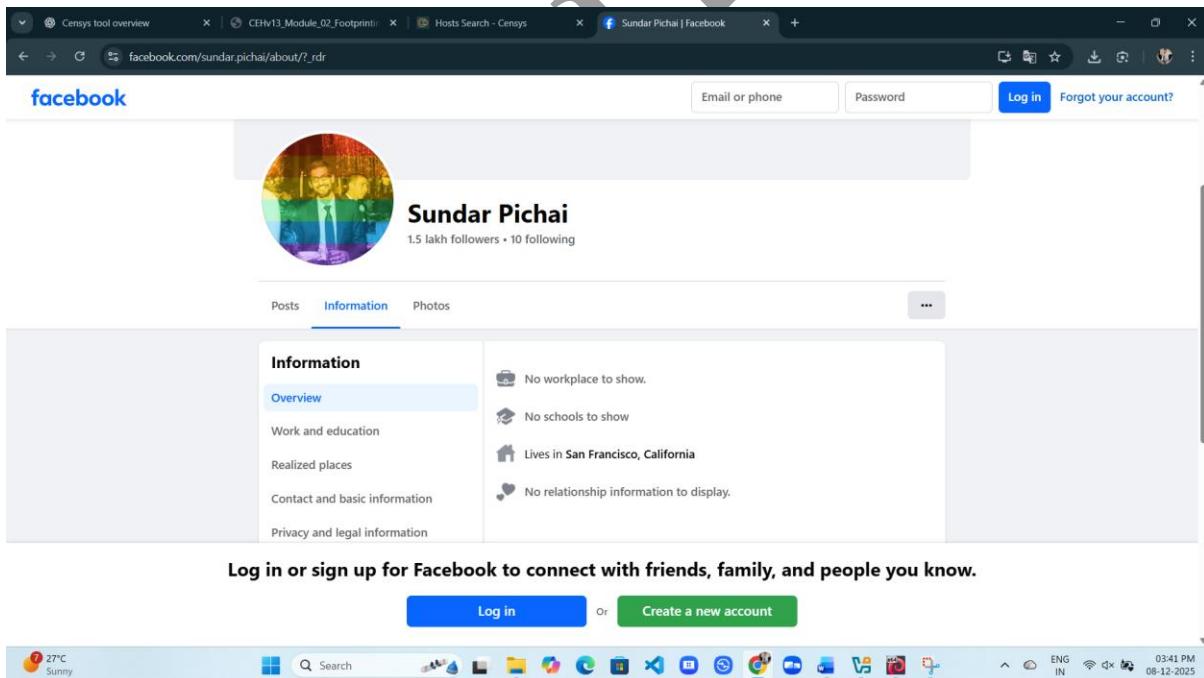


## 4. Footprinting through Social Networking Sites

Footprinting through social networking sites isn't the same game as social engineering—though they overlap like cousins who look suspiciously alike. In social engineering, the attacker *manipulates* people into spilling information. But in social-network footprinting, the attacker simply scoops up whatever users have already thrown onto the Internet, wide open and unguarded.

### People Search on Social Networking Sites

Social networking sites make finding someone almost painfully easy—like, “type their name and boom, their whole life pops up.” These platforms are built for connection, which means users willingly pour their details into profiles: where they work, what they like, who they know, and sometimes even where they are *right now*.



# theHarvester

**Source:** <https://github.com>

theHarvester is one of those classic early-stage penetration testing tools — the kind that's been around long enough to earn respect, but still hits hard in modern recon. It's made for open-source intelligence gathering, helping attackers map out a company's **external threat surface** by digging up public data across the Internet.

```
theHarvester -d microsoft -l 200 -b linkedin
```

## Where:

-d → Domain or company name you want to search

**-l** → Number of results to retrieve (200 here)

-b → Data source, which is linkedin in this case

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

(root@kali) [~/home/sachet]

```
# theHarvester -d microsoft -l 200 -b linkedin

Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
* theHarvester 4.8.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorellab@edge-security.com
*
[!] Target: microsoft

[!] No LinkedIn users found.

[!] LinkedIn Links found: 0

[!] No IPs found.

[!] No emails found.

[!] No people found.

[!] No hosts found.

[root@kali] ~
```

27°C Sunny

Search

15:49 08-12-2025

ENG IN

# Harvesting Email Lists

Collecting email addresses of employees from a target organization might look small on the surface, but trust me—this step becomes *deadly important* in the later stages of an attack. Once an attacker knows who works where and what their email

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

IDs look like, the door to phishing, social engineering, and brute-force attempts swings wide open.

**Source:** <https://github.com>

Attackers often use **theHarvester** to extract email addresses linked to a particular domain. For instance, to harvest email IDs from **microsoft.com** using the Baidu search engine, they'd run:

```
theHarvester -d microsoft.com -l 200 -b baidu
```

Where:

- **-d** → Target domain
  - **-l** → Limit results to 200 entries
  - **-b** → Data source (here it's Baidu, but Google/Bing/Yahoo can be used too)

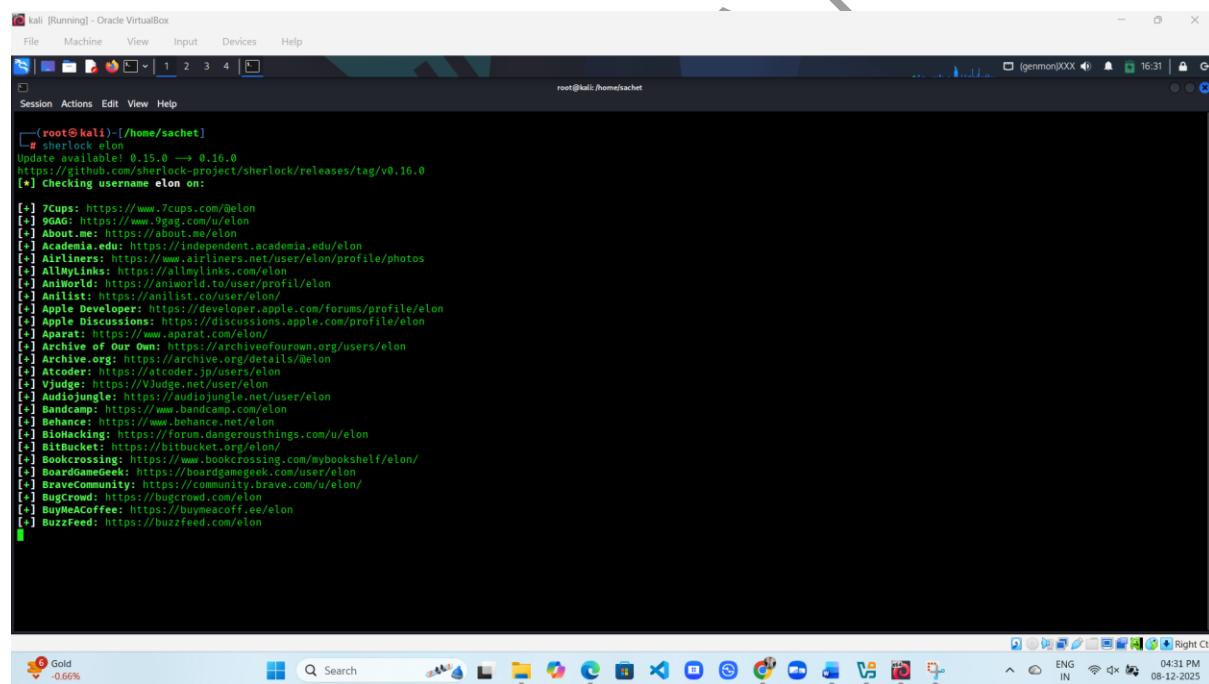
## Tools for Footprinting through Social Networking Sites

When it comes to digging through social media for intel, attackers don't just scroll like casual users—they roll in with specialized tools that sweep across multiple platforms at once. Tools like **Sherlock** and **Social Searcher** help attackers gather sensitive personal data from sites such as Twitter, Instagram, Facebook, and Pinterest.

### Sherlock

**Source:** <https://github.com>

Sherlock is like a username bloodhound. You feed it a username once, and it hunts across dozens—even hundreds—of social networking sites to find matching profiles. No magic tricks, no manipulation—just pure open-source intelligence.



```
(root㉿kali)-[~/home/sachet]
# sherlock elon
Update available! 0.15.0 → 0.16.0
https://github.com/sherlock-project/sherlock/releases/tag/v0.16.0
[*] Checking username elon on:
[*] 7cups: https://www.7cups.com/elon
[*] pg4g: https://www.pg4g.com/u/elon
[*] About.me: https://about.me/elon
[*] Academia.edu: https://independent.academia.edu/elon
[*] Airliners: https://www.airliners.net/user/elon/profile/photos
[*] AllMyLinks: https://allmylinks.com/elon
[*] AniWorld: https://aneworld.to/user/profil/elon
[*] Anilist: https://anilist.co/user/elon/
[*] Apple Developer: https://developer.apple.com/forums/profile/elon
[*] Apple Discussions: https://discussions.apple.com/profile/elon
[*] Apoorv: https://apoorv.ml/elon/
[*] Archive of Our Own: https://archiveourown.org/users/elon
[*] Archive.org: https://archive.org/details/@elon
[*] Atcoder: https://atcoder.jp/users/elon
[*] Vjudge: https://Vjudge.net/user/elon
[*] AudioJungle: https://audiojungle.net/user/elon
[*] Bandcamp: https://www.bandcamp.com/elon
[*] Behance: https://www.behance.net/elon
[*] BookCrossing: https://forum.dreamcrossings.com/u/elon
[*] GitHubNet: https://github.net/elon/
[*] Bookcrossing: https://www.bookcrossing.com/mybookshelf/elon/
[*] BoardGameGeek: https://boardgamegeek.com/user/elon
[*] BraveCommunity: https://community.brave.com/u/elon/
[*] BugCrowd: https://bugcrowd.com/elon
[*] BuyMeACoffee: https://buyamecoff.ee/elon
[*] BuzzFeed: https://buzzfeed.com/elon
```

### Social Searcher

**Source:** <https://www.social-searcher.com>

Social Searcher allows attackers to search for content on social networks in real time and provides deep analytics data. Attackers use this tool to track a target user on various social networking sites and obtain information such as complete URLs to their profiles, their postings, and other personal information.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

The screenshot shows a browser window with the Social Searcher extension active. The search bar contains 'bill gates'. Below the search bar, there's a large dark card titled 'Google Maps Places UI Kit' with a link to 'Bring the power of Google Places to any map with a few lines of code with Places UI Kit'. Below this card, there are several social media sharing icons. The main search results area shows a result for 'Bill Gates - Facebook' with a snippet about climate action. Below the snippet, there's a quote from Bill Gates: 'I look forward to every trip to India because I leave inspired by the ...'. The results are sorted by relevance. The browser status bar at the bottom shows it's 04:07 PM on 08-12-2025, the weather is 29°C and sunny, and the system language is ENG IN.

This screenshot shows the same browser setup as the first one, but the search results have changed. The results now include a video from Al Jazeera English about Bill Gates talking to them. Other results mention Bill Gates extending birthday wishes to PM Modi and a video from MyGovIndia. The browser status bar at the bottom shows it's 04:07 PM on 08-12-2025, the weather is 29°C and sunny, and the system language is ENG IN.

## 5. Whois Footprinting

When attackers start plotting an attack, one of the first things they reach for is **Whois information**. It's the old-school public phonebook of the Internet—straightforward, brutally honest, and packed with details most people don't even realize they've exposed.

Whois footprinting helps gather domain-level intelligence about a target organization, including:

- **Domain owner**
- **Registrar details**
- **Registration and expiration dates**
- **Administrative & technical contacts**
- **Name servers**
- **Associated IP addresses and geolocation**

### WHOIS LOOKUP RESULT

To dig into a target's domain details, attackers turn to Whois lookup services—simple tools with the power to expose a surprising amount of information. Websites like [whois.domaintools.com](http://whois.domaintools.com) and [tamos.com](http://tamos.com) let you punch in a domain or IP address and instantly pull up registration data, ownership details, and server information.

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

- Tab Bar:** CEHV13\_Module\_02\_Footprint, WHOIS search results, Censys tool overview.
- Address Bar:** in.godaddy.com/whois/results.aspx?itc=dip\_domain\_whois&domain=google.com
- Left Panel (WHOIS search results):**
  - Domain Information:**
    - Name: GOOGLE.COM
    - Registry Domain ID: 2138514\_DOMAIN\_COM-VRSN
    - Registered On: 1997-09-15T04:00:0Z
    - Expires On: 2028-09-14T04:00:0Z
    - Updated On: 2019-09-09T15:39:04Z
    - Domain Status: client delete prohibited, client transfer prohibited, client update prohibited, server delete prohibited, server transfer prohibited, server update prohibited
    - Name Servers: NS1.GOOGLE.COM, NS2.GOOGLE.COM, NS3.GOOGLE.COM, NS4.GOOGLE.COM
- Right Panel (Sidebar):**
  - Find your Domain:** A search bar with placeholder "Find your perfect domain".
  - Take a look at these alternate options:**
    - PREMIUM** googlesearchs.com: ₹ 2,32,432.43 + ₹ 1,499.00/yr
    - PREMIUM** googlecomcn.com: ₹ 17,927.92 + ₹ 1,499.00/yr
    - PREMIUM** heygoogle.com: ₹ 8,91,801.80 + ₹ 1,499.00/yr

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

Registrant Contact

Name	REDACTED REGISTRANT
Organization	Google LLC
Phone	REDACTED FOR PRIVACY
Fax	-
Email	REDACTED FOR PRIVACY
Mailing Address	REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY

Technical Contact

Name	-
Organization	-
Phone	-
Fax	-
Email	<a href="https://domains.markmonitor.com/whois/contact/google.com">https://domains.markmonitor.com/whois/contact/google.com</a>

## Using Batch IP Converter

Batch IP Converter

File Function View Help

IP Domain Converter

Domain Name: www.yahoo.com

IP Address: 8.8.8.8

IP Neighborhood: 20

IP Neighborhood will find IP address and do a resolve for the last and next number IPs. This is not often found, but can be very useful to see what other website domains are hosted by the same ISP.

Host Name:

Batch Conversion

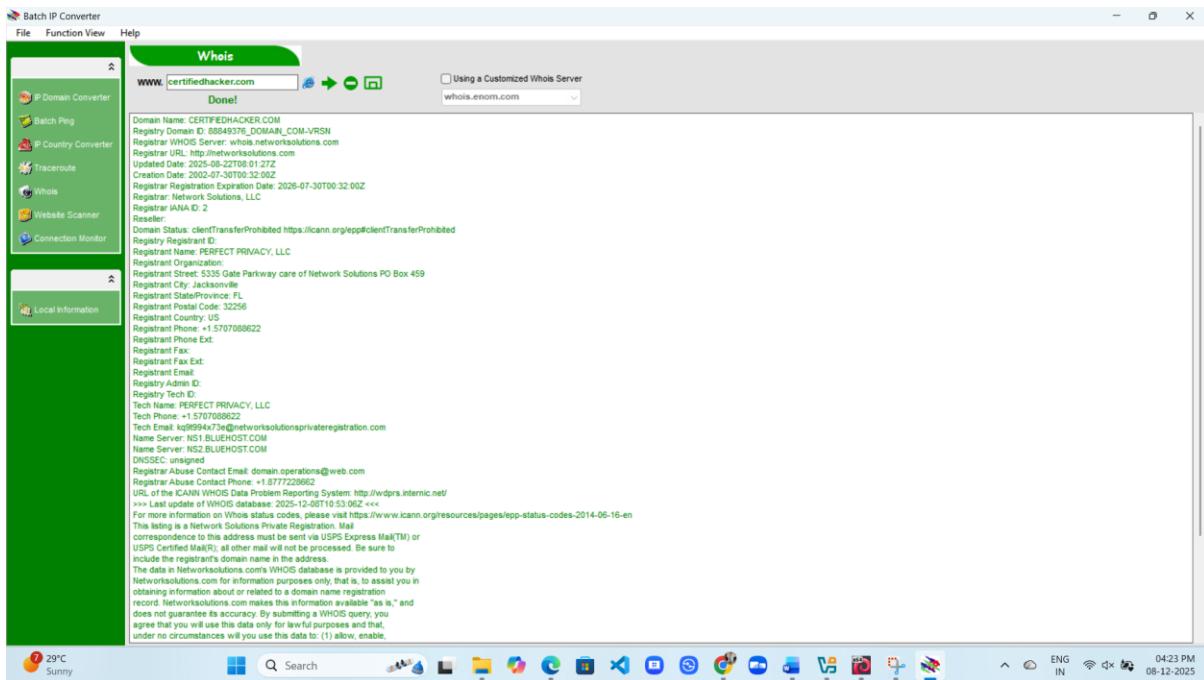
From Domain / Host Name to IP Address

From IP Address to Domain / Host Name

Total

Finished Successful Failed

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



SACHCHITANAND YADAV

## IP Geolocation Lookup Tools

### IP2Location

Source: <https://www.ip2location.com>

As shown in the screenshot, attackers use IP2Location tool to identify a visitor's geographical location, i.e., country, region, city, latitude and longitude of city, ZIP code, time zone, connection speed, ISP, domain name, IDD country code, area code, weather station code and name, mobile carrier, elevation, and usage type information using aproprietary IP address lookup database and technology.

The screenshot shows the IP2LOCATION website interface. At the top, there is a search bar containing the IP address 2401:4900:8f56:2ee3:6cd1:b18c:9650:d9c5 and a blue "LOOK UP" button. Below the search bar, the results are displayed in a grid format:

IP Address 2401:4900:8f56:2ee3:6cd1:b18c:9650:d9c5	Country India	Region Maharashtra	City Pune
Coordinates of City 18.519663, 73.854508	ISP Bharti Airtel Ltd.	Time Zone UTC +05:30	Local Time 2025-12-08 16:25:39
Domain airtel.in	Net Speed DSL	IDD & Area Code (91) 020	ZIP Code 412415
Weather Station Poona (INXX0164)	Mobile Carrier AirTel	Mobile Country Code 404	Mobile Network Code 02/03/10/16/31/40/45/49/70/90/92/93/94/95/96/97/98/51/52/53/54/5
Elevation 562m	Usage Type (ISP) Fixed Line ISP, (MOB) Mobile ISP	Address Type (U) Unicast	Category (IAB19-18) Internet Technology
District Pune Division	Fraud Score 0	Is Proxy No	Proxy Type -
Proxy ASN	Security Threat	Proxy Last Seen -	Proxy Provider -
ASN	AS Domain	AS CIDR	AS Usage Type -

At the bottom of the page, there is a cookie consent banner with options for "MANAGE COOKIES" and "ACCEPT COOKIES". The browser taskbar at the bottom shows various icons and the date/time: 04:25 PM, 08-12-2025.

## 6. DNS Footprinting

Once attackers finish digging through Whois data, they move straight into **DNS footprinting**—the next major step in the recon chain. This phase focuses on pulling information from the Domain Name System to understand how the target’s online infrastructure is laid out.

### Extracting DNS Information

DNS footprinting gives attackers a peek behind the curtain of a target’s network. The DNS zone data it exposes—domain names, hostnames, IP addresses, and more—basically acts like a directory of who lives where in the digital neighborhood. Once an attacker knows which machines exist, they can start narrowing down the “important” hosts and even use that knowledge to push social engineering attacks later on.

DNS footprinting helps identify several key DNS records, each revealing a different piece of the organization’s infrastructure. Here are the major ones:

<b>Record Type</b>	<b>Description</b>
<b>A</b>	Points to a host’s IPv4 address
<b>AAAA</b>	Points to a host’s IPv6 address
<b>MX</b>	Shows the domain’s mail server
<b>NS</b>	Identifies the domain’s name server
<b>CNAME</b>	Canonical name record; creates aliases for a host
<b>SOA</b>	Indicates the start of authority for a domain
<b>SRV</b>	Service records, listing available services
<b>PTR</b>	Maps an IP address back to a hostname (reverse lookup)

Record Type	Description
<b>RP</b>	Responsible person record
<b>HINFO</b>	Host information, like CPU type and operating system
<b>TXT</b>	Unstructured text records—often used for SPF, DKIM, or other verification data

## MXToolbox

**Source:** <https://mxtoolbox.com>

MXToolbox is a versatile online tool for **DNS and email infrastructure analysis**. It lets you query a target domain to uncover:

- **MX records** (mail servers)
- **A/AAAA records** (host IPs)
- **NS records** (name servers)
- **SPF, DKIM, and DMARC records** (email authentication)

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

**DNS Lookup Results for google.com:**

Type	Domain Name	IP Address	TTL
A	google.com	142.251.16.100 Google LLC (AS15169)	5 min
A	google.com	142.251.16.101 Google LLC (AS15169)	5 min
A	google.com	142.251.16.102 Google LLC (AS15169)	5 min
A	google.com	142.251.16.113 Google LLC (AS15169)	5 min
A	google.com	142.251.16.138 Google LLC (AS15169)	5 min
A	google.com	142.251.16.139 Google LLC (AS15169)	5 min

**Test Results:**

- dns check:** DNS Record Published
- mx lookup:** DNS Record found
- dmarc lookup:** N/A
- spf lookup:** N/A
- dns propagation:** N/A

**DNS Check Results for dns.google.com:**

Type	Domain Name	IP Address	TTL	Status	Time (ms)	Auth	Parent	Local
NS	ns1.google.com	216.239.32.10 Google LLC (AS15169)	4 days	✓	4	✓	✓	✓
NS	ns2.google.com	216.239.34.10 Google LLC (AS15169)	4 days	✓	11	✓	✓	✓
NS	ns3.google.com	216.239.36.10 Google LLC (AS15169)	4 days	✓	12	✓	✓	✓
NS	ns4.google.com	216.239.38.10 Google LLC (AS15169)	4 days	✓	4	✓	✓	✓

**Result:**

- SOA Serial Number Format is Invalid  
ns1.google.com reported Serial 841358126 : Suggested serial format is YYYYmmddss where ss is a two-digit sequence number within the day. [More Info](#)
- SOA Refresh Value is outside of the recommended range  
ns1.google.com reported Refresh 900 : Refresh is recommended to be between 1200 and 43200. [More Info](#)
- SOA Expire Value out of recommended range  
ns1.google.com reported Expire 900 : Expire is recommended to be between 1200 and 36000. [More Info](#)

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

The screenshot shows the mxtoolbox.com/DNSCheck interface. At the top, there's a navigation bar with tabs for IP Address to IP Location and Pro, Network Tools: DNS, IP, Email, and a search bar with the URL https://mxtoolbox.com/SuperTool.aspx?action=mx%3agoogle.com&run=toolpage. Below the search bar, there's a dropdown menu set to 'dns'.

The main content area displays two tables of DNS records:

- ns1.google.com (SOA)**

Type	Domain Name	IP Address	TTL
NS	ns1.google.com	216.239.32.10 Google LLC (AS15169)	4 days
NS	ns2.google.com	216.239.34.10 Google LLC (AS15169)	4 days
NS	ns3.google.com	216.239.36.10 Google LLC (AS15169)	4 days
NS	ns4.google.com	216.239.38.10 Google LLC (AS15169)	4 days
- ns2.google.com (Matches SOA)**

Type	Domain Name	IP Address	TTL
NS	ns1.google.com	216.239.32.10 Google LLC (AS15169)	4 days
NS	ns2.google.com	216.239.34.10 Google LLC (AS15169)	4 days
NS	ns3.google.com	216.239.36.10 Google LLC (AS15169)	4 days
NS	ns4.google.com	216.239.38.10 Google LLC (AS15169)	4 days
- ns3.google.com (Matches SOA)**

Type	Domain Name	IP Address	TTL
NS	ns1.google.com	216.239.32.10 Google LLC (AS15169)	4 days
NS	ns2.google.com	216.239.34.10 Google LLC (AS15169)	4 days
NS	ns3.google.com	216.239.36.10 Google LLC (AS15169)	4 days
NS	ns4.google.com	216.239.38.10 Google LLC (AS15169)	4 days

On the right side of the interface, there's a sidebar with various monitoring services offered by MXToolBox:

- Get one (1) Free Monitor to alert you to Email Delivery Issues
- Delivery Center**: Real-time insight into the Email Deliverability
- Inbox Placement**: Know if your campaigns will make the inbox
- Recipient Complaints**: Get feedback on how recipients perceive your email: complaints, unsubscribes, failures, and more...
- Adaptive Blacklist Monitoring**: Real-time monitoring of all your domain's sending IPs
- Mailflow Monitoring**: Round-trip monitoring of your email latency
- SPF Flattening**: Prevent soft delivery failures and easily manage complex SPF configurations

At the bottom of the browser window, there's a status bar showing the IP address (10.149.25.105), a 'Moderate' rating, the date (08-12-2025), and the time (04:33 PM).

## Fierce

**Source:** <https://github.com>

Fierce is a powerful DNS reconnaissance utility designed to uncover hidden corners of a target domain. It helps attackers enumerate **subdomains**, discover **non-contiguous IP ranges**, and map **hostnames** tied to a specific domain or its subdomains. With this information, an attacker can sketch out the target's network layout and pinpoint systems that may be vulnerable.

Attackers commonly use Fierce to:

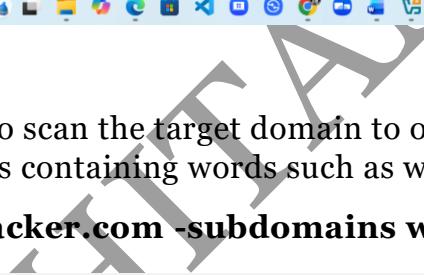
- Identify forgotten or exposed subdomains
- Locate scattered IP spaces belonging to the same organization
- Reveal hosts that aren't directly visible through standard DNS queries

### Example Command

To run a basic scan on the target domain (*certifiedhacker.com*):

```
fierce --domain certifiedhacker.com
```

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

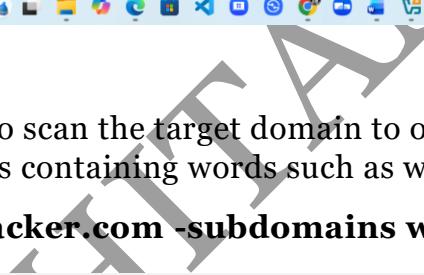


```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
(root@kali)-[~/home/sachet]
# fierce --domain certifiedhacker.com
NS: ns1.bluehost.com, ns2.bluehost.com.
SOA: ns1.bluehost.com. (162.159.24.60)
Zone: failure
Wildcard: failure
Found: blog.certifiedhacker.com. (162.241.216.11)
Nearby:
{'162.241.216.10': '162-241-216-10.unifiedlayer.com.',
 '162.241.216.11': 'box5331.bluehost.com.',
 '162.241.216.12': '162-241-216-12.unifiedlayer.com.',
 '162.241.216.13': '162-241-216-13.unifiedlayer.com.',
 '162.241.216.14': 'box5334.bluehost.com.',
 '162.241.216.15': '162-241-216-15.unifiedlayer.com.',
 '162.241.216.16': '162-241-216-16.unifiedlayer.com.',
 '162.241.216.6': '162-241-216-6.unifiedlayer.com.',
 '162.241.216.7': '162-241-216-7.unifiedlayer.com.',
 '162.241.216.8': '162-241-216-8.unifiedlayer.com.',
 '162.241.216.9': '162-241-216-9.unifiedlayer.com.'}
Found: demo.certifiedhacker.com. (162.241.216.11)
Found: ftp.certifiedhacker.com. (162.241.216.11)
Found: imap.certifiedhacker.com. (162.241.216.11)
Found: localhost.certifiedhacker.com. (127.0.0.1)
Nearby:
{'127.0.0.1': 'localhost.'}
Found: mail.certifiedhacker.com. (162.241.216.11)
Found: news.certifiedhacker.com. (162.241.216.11)
Found: pop.certifiedhacker.com. (162.241.216.11)

(root@kali)-[~/home/sachet]
#
```

Run the following command to scan the target domain to obtain specific subdomains(here, subdomains containing words such as write, admin, and mail):

**fierce -domain certifiedhacker.com -subdomains write admin mail**



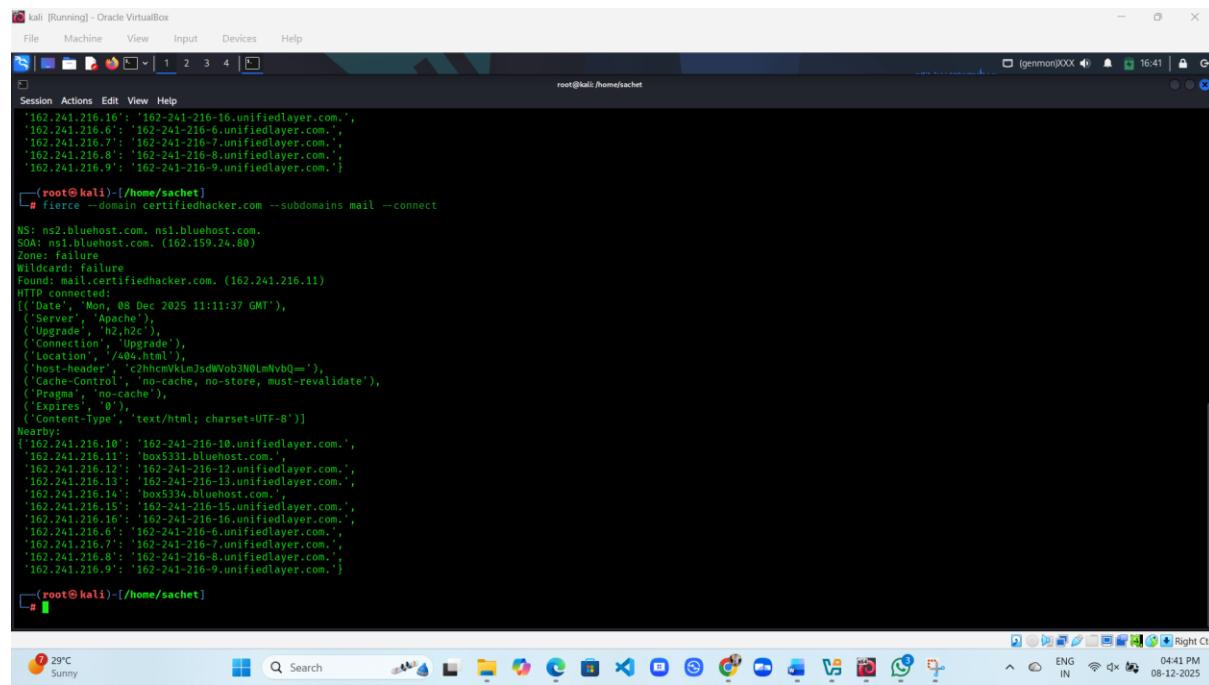
```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~/home/sachet
# fierce -domain certifiedhacker.com -subdomains write admin mail
usage: fierce [-h] [--domain DOMAIN] [--connect] [--traverse TRAVERSE] [--search SEARCH [SEARCH ...]] [--range RANGE] [--delay DELAY] [--subdomains SUBDOMAINS [SUBDOMAINS ...]] [--subdomain-file SUBDOMAIN_FILE] [--dns-servers DNS_SERVERS [DNS_SERVERS ...]] | --dns-file DNS_FILE] [-tcp]
fierce: error: unrecognized arguments: -domain certifiedhacker.com -subdomains write admin mail
(root@kali)-[~/home/sachet]
# fierce -domain certifiedhacker.com --subdomains write admin mail
NS: ns2.bluehost.com, ns1.bluehost.com.
SOA: ns1.bluehost.com. (162.159.24.60)
Zone: failure
Wildcard: failure
Found: mail.certifiedhacker.com. (162.241.216.11)
Nearby:
{'162.241.216.10': '162-241-216-10.unifiedlayer.com.',
 '162.241.216.11': 'box5331.bluehost.com.',
 '162.241.216.12': '162-241-216-12.unifiedlayer.com.',
 '162.241.216.13': '162-241-216-13.unifiedlayer.com.',
 '162.241.216.14': 'box5334.bluehost.com.',
 '162.241.216.15': '162-241-216-15.unifiedlayer.com.',
 '162.241.216.16': '162-241-216-16.unifiedlayer.com.',
 '162.241.216.6': '162-241-216-6.unifiedlayer.com.',
 '162.241.216.7': '162-241-216-7.unifiedlayer.com.',
 '162.241.216.8': '162-241-216-8.unifiedlayer.com.',
 '162.241.216.9': '162-241-216-9.unifiedlayer.com.'}

(root@kali)-[~/home/sachet]
#
```

Run the following command to attempt an HTTP connection on the discovered domains of the target:

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

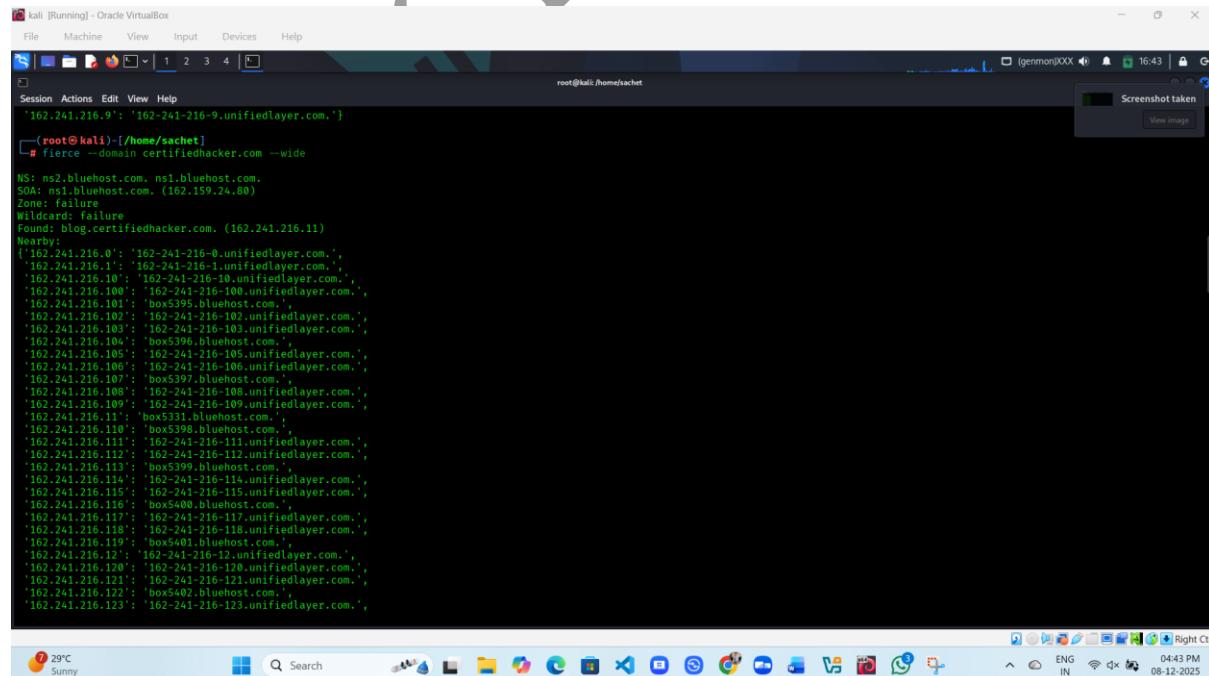
### fierce -- domain certifiedhacker.com -- subdomains mail – connect



```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~/home/sachet
# fierce --domain certifiedhacker.com --subdomains mail --connect
NS: ns2.bluehost.com. ns1.bluehost.com.
SOA: ns1.bluehost.com. (162.159.24.80)
Zone: failure
Wildcard: failure
Found: mail.certifiedhacker.com. (162.241.216.11)
HTTP connected:
[{"Date": "Mon, 08 Dec 2025 11:11:37 GMT", "Server": "Apache"}, {"Upgrade": "1.1", "Connection": "Upgrade"}, {"Location": "/404.html"}, {"Host-Header": "C2hhcmVklmJsdWob3N0ImNvbQ=="}, {"Cache-Control": "no-cache, no-store, must-revalidate"}, {"Pragma": "no-cache"}, {"Expires": "0"}, {"Content-Type": "text/html; charset=UTF-8"}]
Nearby:
{'162.241.216.10': '162-241-216-10.unifiedlayer.com.', '162.241.216.11': 'box5311.bluehost.com.', '162.241.216.12': '162-241-216-12.unifiedlayer.com.', '162.241.216.13': '162-241-216-13.unifiedlayer.com.', '162.241.216.14': 'box5334.bluehost.com.', '162.241.216.15': '162-241-216-15.unifiedlayer.com.', '162.241.216.16': '162-241-216-16.unifiedlayer.com.', '162.241.216.17': '162-241-216-17.unifiedlayer.com.', '162.241.216.18': '162-241-216-18.unifiedlayer.com.', '162.241.216.19': '162-241-216-19.unifiedlayer.com.'}
(root@kali)~[/home/sachet]
# 
```

Run the following command to scan all the discovered records of the target domain, i.e., a full detailed scan:

### fierce -- domain certifiedhacker.com -- wide



```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~/home/sachet
# fierce --domain certifiedhacker.com --wide
NS: ns2.bluehost.com. ns1.bluehost.com.
SOA: ns1.bluehost.com. (162.159.24.80)
Zone: failure
Wildcard: failure
Found: blog.certifiedhacker.com. (162.241.216.11)
Nearby:
{'162.241.216.0': '162-241-216-0.unifiedlayer.com.', '162.241.216.1': '162-241-216-1.unifiedlayer.com.', '162.241.216.10': '162-241-216-10.unifiedlayer.com.', '162.241.216.100': 'box5395.bluehost.com.', '162.241.216.101': '162-241-216-101.unifiedlayer.com.', '162.241.216.102': '162-241-216-102.unifiedlayer.com.', '162.241.216.103': '162-241-216-103.unifiedlayer.com.', '162.241.216.104': 'box5396.bluehost.com.', '162.241.216.105': '162-241-216-105.unifiedlayer.com.', '162.241.216.106': '162-241-216-106.unifiedlayer.com.', '162.241.216.107': 'box5397.bluehost.com.', '162.241.216.108': '162-241-216-108.unifiedlayer.com.', '162.241.216.109': '162-241-216-109.unifiedlayer.com.', '162.241.216.11': 'box5331.bluehost.com.', '162.241.216.110': 'box5398.bluehost.com.', '162.241.216.111': '162-241-216-111.unifiedlayer.com.', '162.241.216.112': '162-241-216-112.unifiedlayer.com.', '162.241.216.113': 'box5399.bluehost.com.', '162.241.216.114': '162-241-216-114.unifiedlayer.com.', '162.241.216.115': '162-241-216-115.unifiedlayer.com.', '162.241.216.116': 'box5400.bluehost.com.', '162.241.216.117': '162-241-216-117.unifiedlayer.com.', '162.241.216.118': '162-241-216-118.unifiedlayer.com.', '162.241.216.119': 'box5401.bluehost.com.', '162.241.216.120': '162-241-216-120.unifiedlayer.com.', '162.241.216.121': '162-241-216-121.unifiedlayer.com.', '162.241.216.122': 'box5402.bluehost.com.', '162.241.216.123': '162-241-216-123.unifiedlayer.com.'}
Screenshot taken
View image
(root@kali)~[/home/sachet]
# 
```

## Reverse DNS Lookup

Reverse DNS lookup is the process of obtaining a **domain name from a known IP address**. While a normal DNS lookup converts a domain name into its corresponding IP (using A or AAAA records), a reverse lookup uses **PTR records** to map an IP address back to its domain.

## DNSRecon

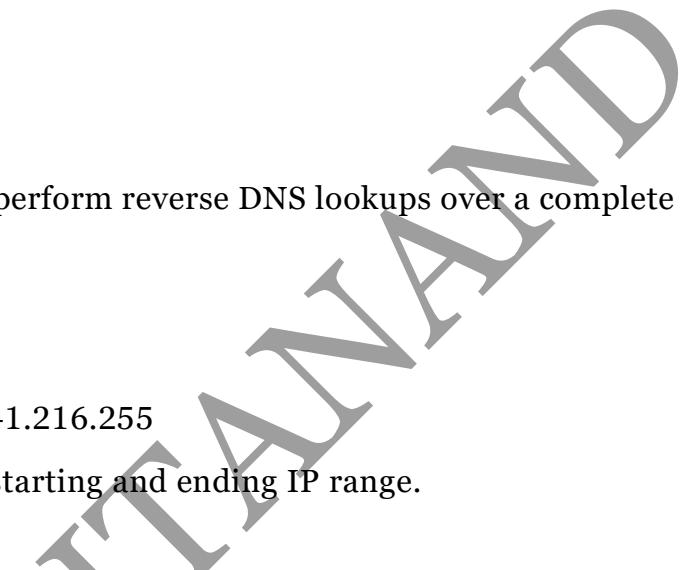
**Source:** <https://github.com>

Attackers often use DNSRecon to perform reverse DNS lookups over a complete range of IP addresses.

### Example Command:

`dnsrecon -r 162.241.216.0-162.241.216.255`

- The **-r** option specifies the starting and ending IP range.



```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:[/home/sachet]
# dnsrecon -r 162.241.216.0-162.241.216.255
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[*] PTR 162.241.216.4.unifiedlayer.com 162.241.216.4
[*] PTR 162.241.216.1.unifiedlayer.com 162.241.216.1
[*] PTR 162.241.216.0.unifiedlayer.com 162.241.216.0
[*] PTR 162.241.216.2.unifiedlayer.com 162.241.216.2
[*] PTR 162.241.216.5.unifiedlayer.com 162.241.216.5
[*] PTR 162.241.216.7.unifiedlayer.com 162.241.216.7
[*] PTR 162.241.216.6.unifiedlayer.com 162.241.216.6
[*] PTR 162.241.216.8.unifiedlayer.com 162.241.216.8
[*] PTR 162.241.216.10.unifiedlayer.com 162.241.216.10
[*] PTR 162.241.216.9.unifiedlayer.com 162.241.216.9
[*] PTR box5331.bluehost.com 162.241.216.11
[*] PTR 162.241.216.12.unifiedlayer.com 162.241.216.12
[*] PTR 162.241.216.13.unifiedlayer.com 162.241.216.13
[*] PTR box5332.bluehost.com 162.241.216.14
[*] PTR 162.241.216.15.unifiedlayer.com 162.241.216.15
[*] PTR box5348.bluehost.com 162.241.216.17
[*] PTR 162.241.216.18.unifiedlayer.com 162.241.216.18
[*] PTR 162.241.216.19.unifiedlayer.com 162.241.216.19
[*] PTR box5350.bluehost.com 162.241.216.20
[*] PTR 162.241.216.21.unifiedlayer.com 162.241.216.21
[*] PTR 162.241.216.16.unifiedlayer.com 162.241.216.16
[*] PTR 162.241.216.22.unifiedlayer.com 162.241.216.22
[*] PTR box5351.bluehost.com 162.241.216.23
[*] PTR 162.241.216.25.unifiedlayer.com 162.241.216.25
[*] PTR 162.241.216.24.unifiedlayer.com 162.241.216.24
[*] PTR 162.241.216.3.unifiedlayer.com 162.241.216.3
[*] PTR box5354.bluehost.com 162.241.216.26
[*] PTR box5359.bluehost.com 162.241.216.29
[*] PTR 162.241.216.27.unifiedlayer.com 162.241.216.27
[*] PTR 162.241.216.30.unifiedlayer.com 162.241.216.30
[*] PTR 162.241.216.28.unifiedlayer.com 162.241.216.28
[*] PTR 162.241.216.31.unifiedlayer.com 162.241.216.31
[*] PTR 162.241.216.34.unifiedlayer.com 162.241.216.34
[*] PTR box5364.bluehost.com 162.241.216.35
[*] PTR box5363.bluehost.com 162.241.216.32

```

## Reverse Lookup

Source: <https://mxtoolbox.com>

As shown in the screenshot, the Reverse Lookup tool performs a reverse IP lookup by taking an IP address and locating a DNS PTR record for that IP address.

The screenshot shows the MXToolbox SuperTool interface. In the search bar, the IP address '162.241.216.11' is entered. Below the search bar, there is a 'Reverse Lookup' button. The results table shows one entry:

Type	IP Address	Domain Name	TTL
PTR	162.241.216.11 Oracle Corporation (AS31896)	box5331.bluehost.com	24 hrs

Below the table, under the 'Test' section, it says 'DNS Record Published' and 'Result' shows 'DNS Record found'. A note at the bottom left says 'An error has occurred with your lookup. Please try again.' On the right side of the interface, there is a sidebar with various monitoring tools and services offered by MXToolbox.

## 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.

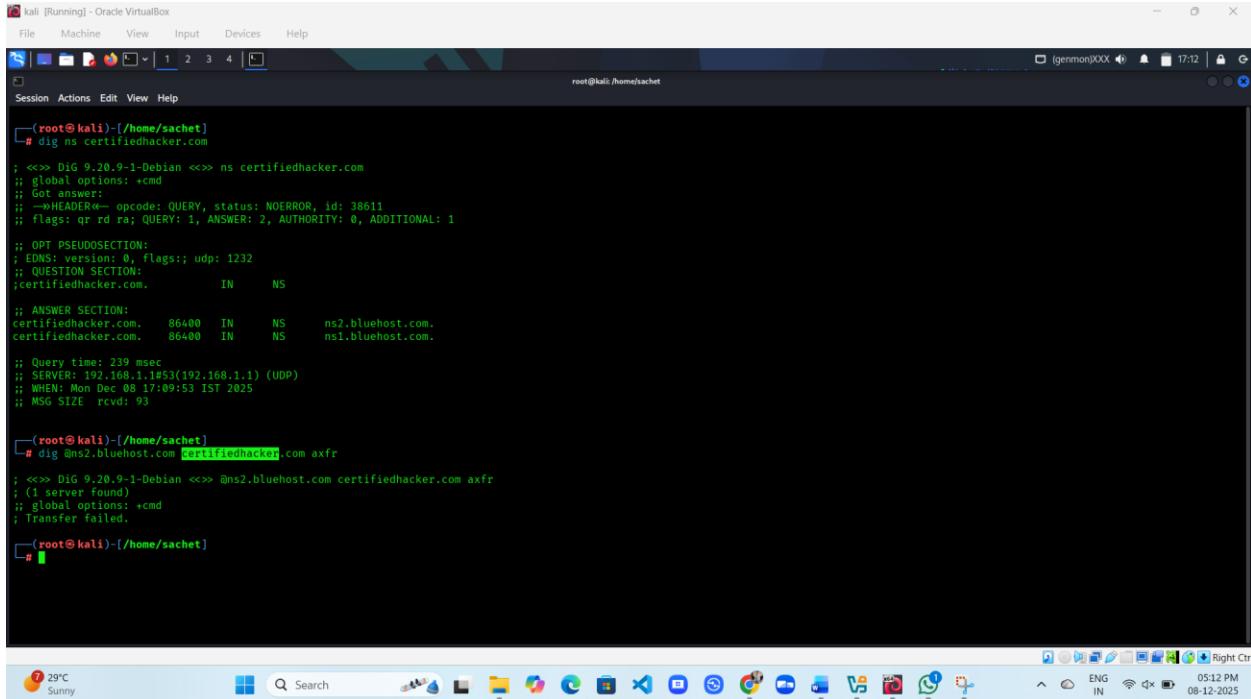
**NS record:** dig example.com NS.

**TXT record:** dig example.com TXT.

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

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

- Using ns record
- Using AXFR zone transfer



```
(root㉿kali)-[~/home/sachet]
# dig ns certifiedhacker.com

; <>> DIG 9.20.9-1-Debian <>> ns certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 38611
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;certifiedhacker.com. IN NS

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

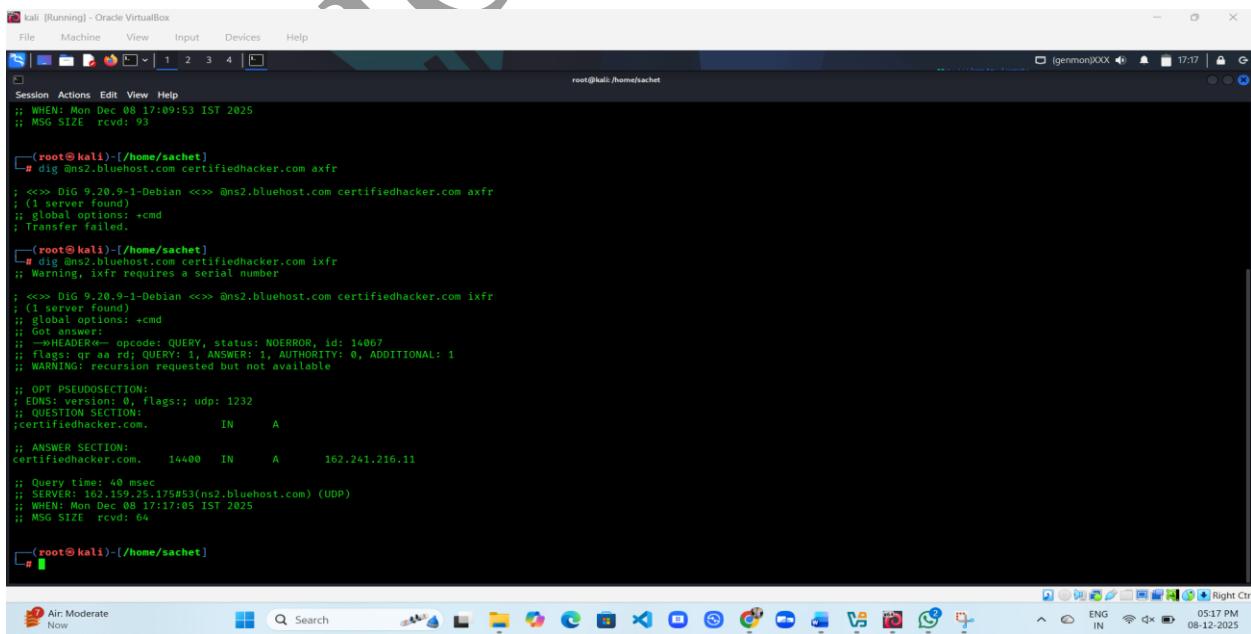
;; Query time: 239 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon Dec 08 17:09:53 IST 2025
;; MSG SIZE rcvd: 93

(root㉿kali)-[~/home/sachet]
# dig @ns2.bluehost.com certifiedhacker.com axfr

; <>> DIG 9.20.9-1-Debian <>> @ns2.bluehost.com certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.

(root㉿kali)-[~/home/sachet]
#
```

- Using IXFR zone transfer



```
(root㉿kali)-[~/home/sachet]
# dig @ns2.bluehost.com certifiedhacker.com axfr

; <>> DIG 9.20.9-1-Debian <>> @ns2.bluehost.com certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.

(root㉿kali)-[~/home/sachet]
# dig @ns2.bluehost.com certifiedhacker.com ixfr

; <>> DIG 9.20.9-1-Debian <>> @ns2.bluehost.com certifiedhacker.com ixfr
; (1 server found)
;; global options: +cmd
; Warning, ixfr requires a serial number

; <>> DIG 9.20.9-1-Debian <>> @ns2.bluehost.com certifiedhacker.com ixfr
; (1 server found)
;; global options: +cmd
; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 14067
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;certifiedhacker.com. IN A

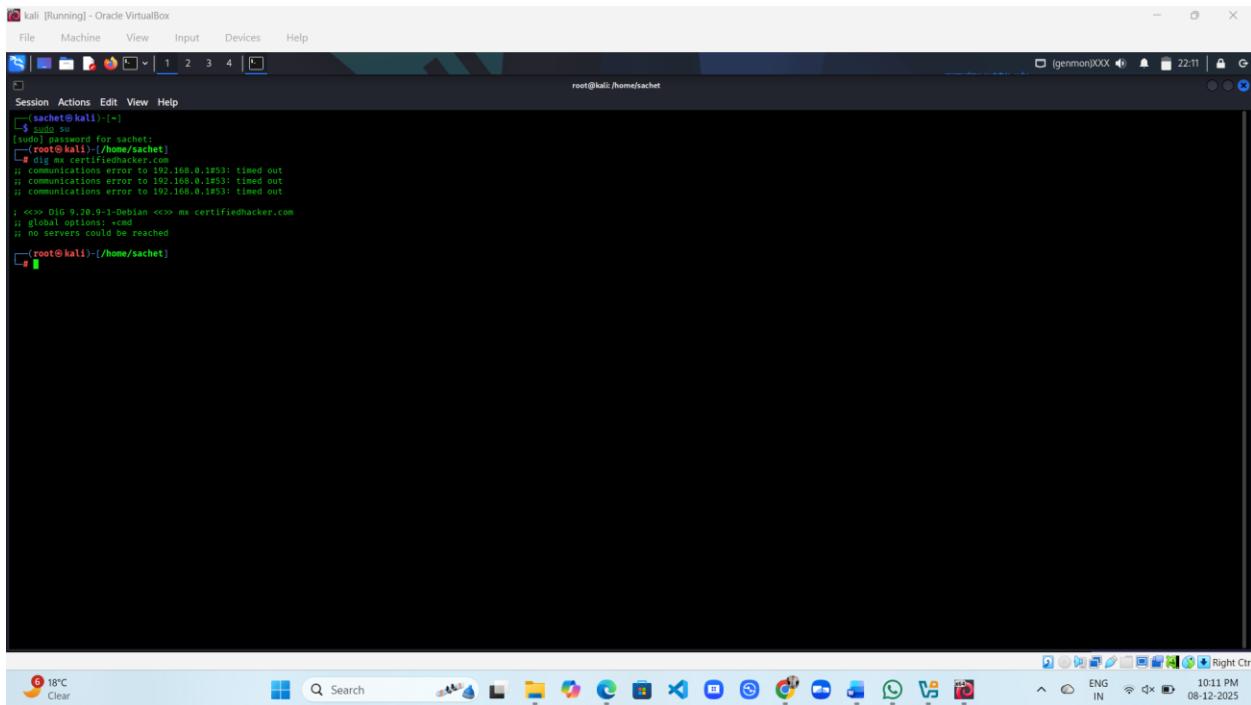
;; ANSWER SECTION:
certifiedhacker.com. 14400 IN A 162.241.216.11

;; Query time: 40 msec
;; SERVER: 162.159.25.175#53(ns2.bluehost.com) (UDP)
;; WHEN: Mon Dec 08 17:17:05 IST 2025
;; MSG SIZE rcvd: 64

(root㉿kali)-[~/home/sachet]
#
```

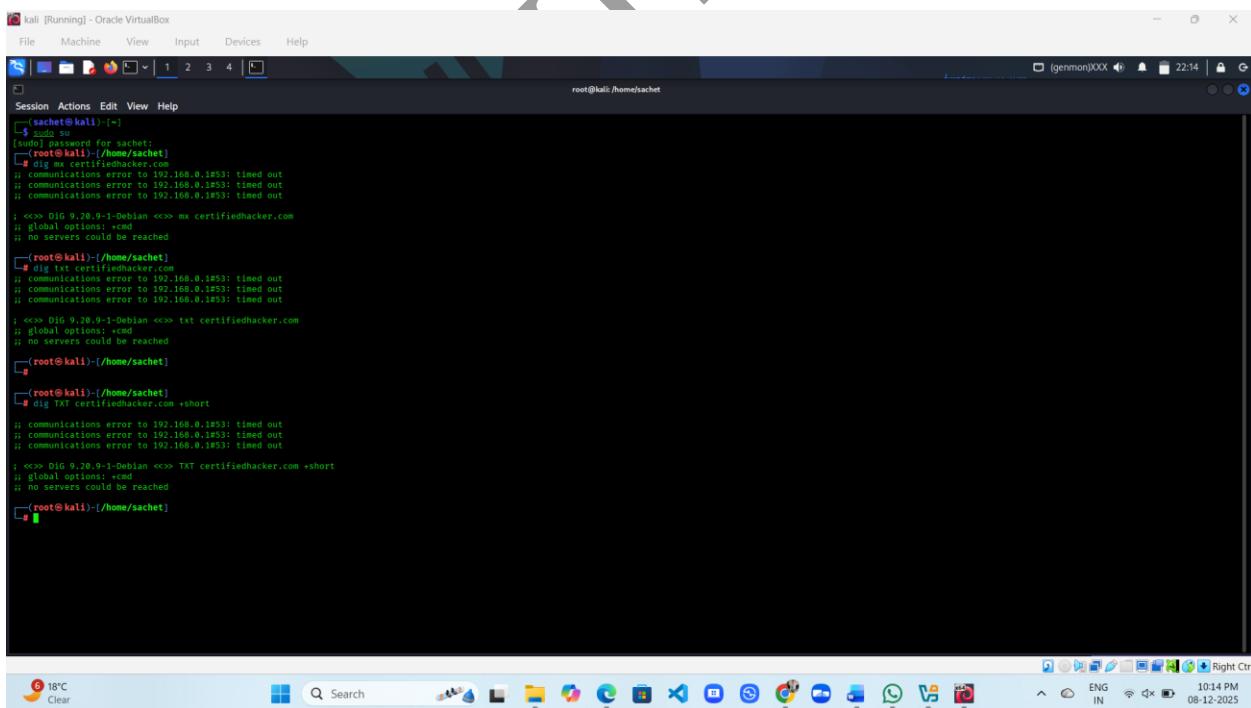
## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

- Using mx records



```
sachet@kali:~$ [sudo] password for sachet:
[sudo] password for sachet:
[root@sachet:/home/sachet]
# dig mx certifiedhacker.com
; <> SIG 9.20.9-1-Debian <>> mx certifiedhacker.com
;; global options: +cmd
;; no servers could be reached
[root@sachet:/home/sachet]
```

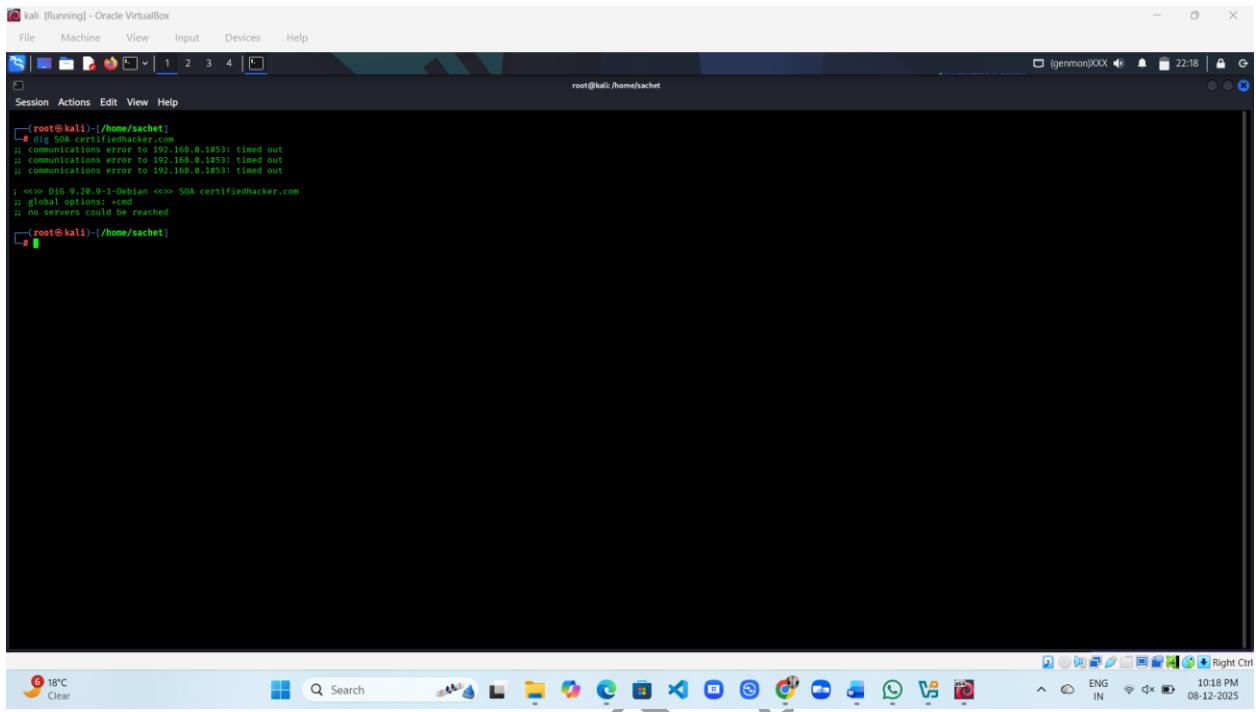
- Using txt records



```
sachet@kali:~$ [sudo] password for sachet:
[sudo] password for sachet:
[root@sachet:/home/sachet]
# dig mx certifiedhacker.com
; <> SIG 9.20.9-1-Debian <>> mx certifiedhacker.com
;; global options: +cmd
;; no servers could be reached
[root@sachet:/home/sachet]
# dig txt certifiedhacker.com
;; communications error to 192.168.0.1<1>; timed out
;; communications error to 192.168.0.2<1>; timed out
;; communications error to 192.168.0.3<1>; timed out
;; communications error to 192.168.0.4<1>; timed out
;; communications error to 192.168.0.5<1>; timed out
[root@sachet:/home/sachet]
# dig DIG 9.20.9-1-Debian <>> TXT certifiedhacker.com +short
;; global options: +cmd
;; no servers could be reached
[root@sachet:/home/sachet]
```

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

- Using SOA records



```
(root@kali:[/home/sachet]
# dig SOA certifiedhacker.com
;; communications error to 192.168.0.1#53: timed out
;; communications error to 192.168.0.1#53: timed out
;; communications error to 192.168.0.1#53: timed out
; dig 9.20.0-1-Debian <>> SOA certifiedhacker.com
;; global options: +cmd
;; no servers could be reached
# (root@kali:[/home/sachet]
```

SACHCHITANAND YADAV

## 7. Network and Email Footprinting

### NETWORK FOOTPRINTING

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

#### Objectives-:

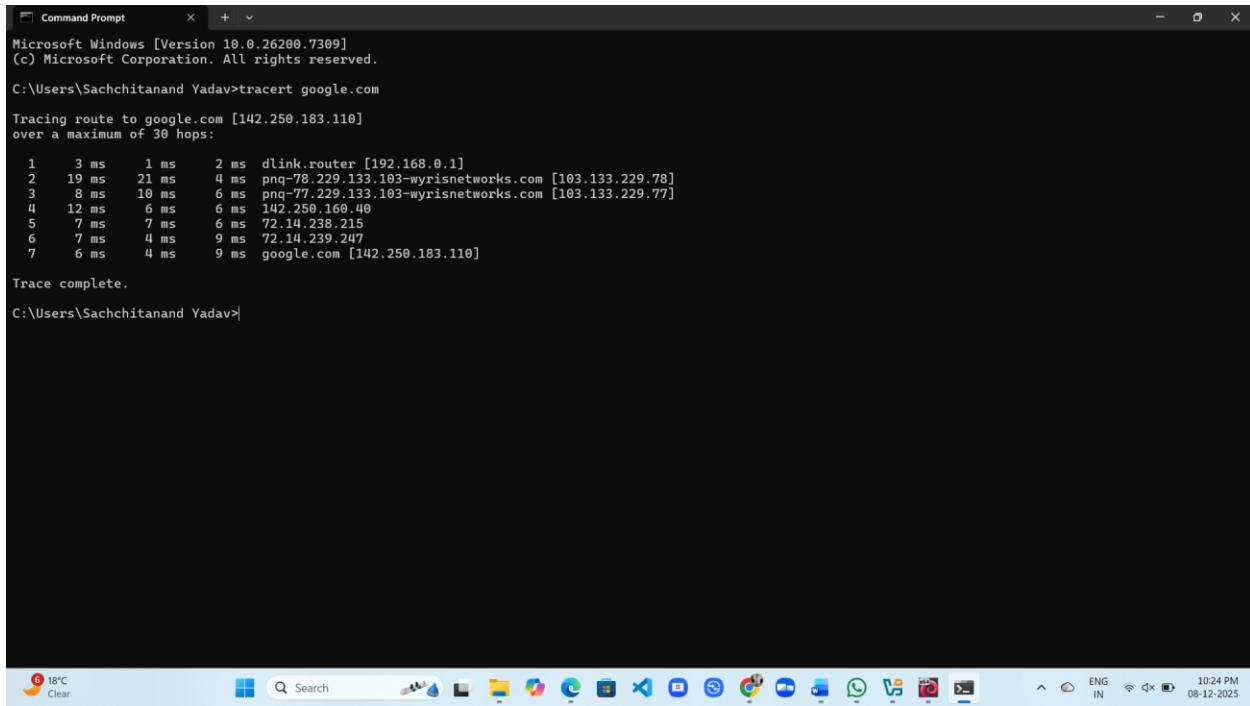
- Identifying IP Addresses
- Gathering DNS Information
- Extracting WHOIS Data
- Mapping Subdomains

### 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 10.0.26200.7309]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sachchitanand Yadav>tracert google.com

Tracing route to google.com [142.250.183.110]
over a maximum of 30 hops:

 1   3 ms    1 ms    2 ms  dlink.router [192.168.0.1]
 2  19 ms    21 ms   4 ms  pnq-78.229.133.103-wyrisnetworks.com [103.133.229.78]
 3   8 ms    10 ms   6 ms  pnq-77.229.133.103-wyrisnetworks.com [103.133.229.77]
 4   12 ms   6 ms    6 ms  142.250.160.40
 5    7 ms   7 ms    6 ms  72.14.238.215
 6    7 ms   4 ms    9 ms  72.14.239.247
 7    6 ms   4 ms    9 ms  google.com [142.250.183.110]

Trace complete.

C:\Users\Sachchitanand Yadav>
```

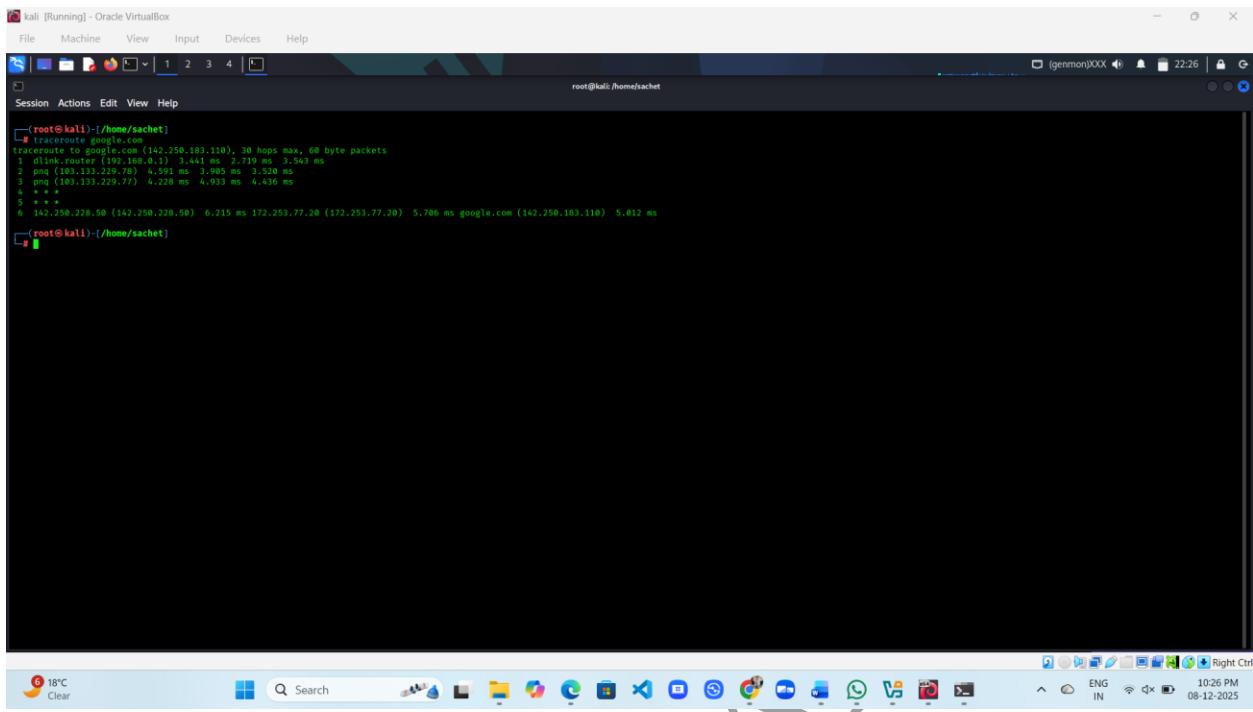
## 2. Network Footprinting Using Linux traceroute (CLI)

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:

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



The screenshot shows a terminal window titled "kali [Running] - Oracle VirtualBox". The terminal is running on a Kali Linux system with root privileges. The user has run the command "traceroute to google.com" and the output is displayed. The traceroute shows the path from the local machine to Google's servers, listing various routers and their latencies. The terminal window is set against a dark background with light-colored text. The desktop environment includes a taskbar at the bottom with icons for various applications like file explorer, browser, and messaging.

```
[root@kali:~/home/sachet]
# traceroute to google.com (142.250.183.110), 30 hops max, 60 byte packets
1 dlink.router (192.168.0.1) 3.441 ms 2.719 ms 3.563 ms
2 ping (193.133.229.78) 4.591 ms 3.900 ms 3.520 ms
3 ping (193.133.229.77) 4.228 ms 4.930 ms 4.156 ms
4 *
5 *
6 142.250.228.50 (142.250.228.50) 6.215 ms 172.253.77.20 (172.253.77.20) 5.706 ms google.com (142.250.183.110) 5.612 ms
```

## EMAIL FOOTPRINTING

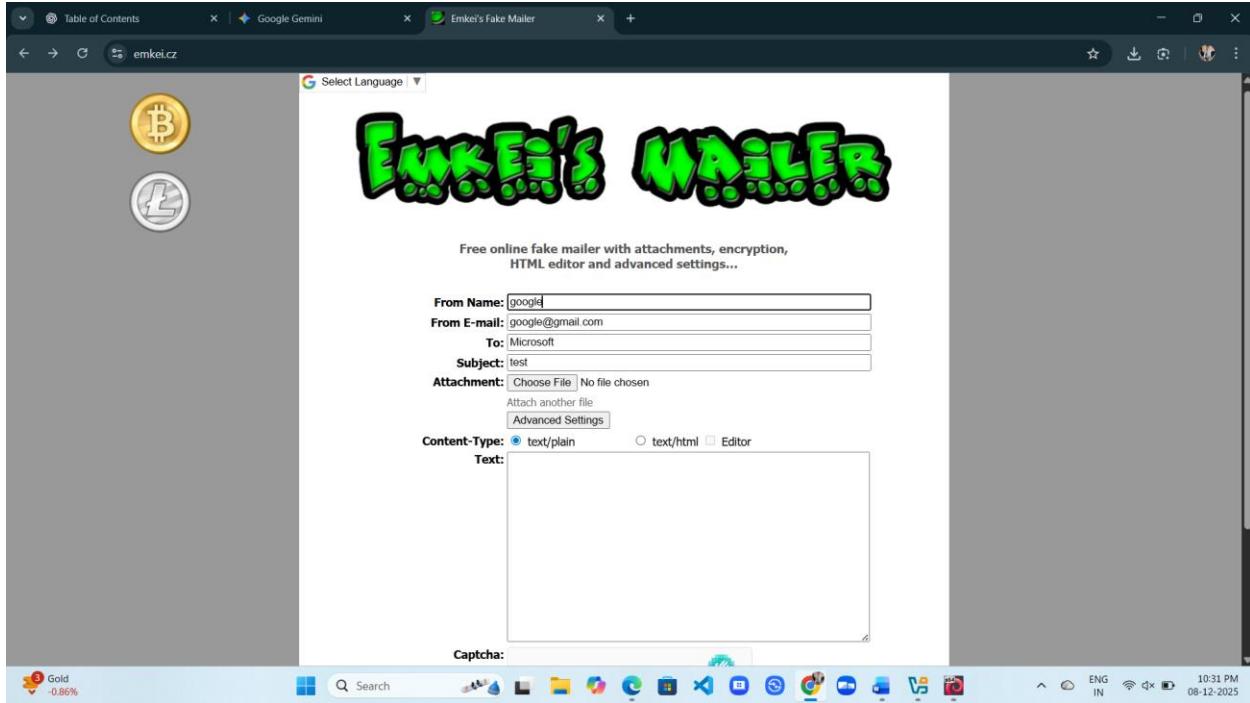
Email footprinting refers to the process of tracking and analyzing details about an email's origin, path, and related metadata to gather information about the sender or the infrastructure used to send the email.

### 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.

- Search mx tool box on browser.
- Click on official mx tool box website.
- Click on Analyze Headers .

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

The screenshot shows a browser window with multiple tabs open. The active tab is 'mxtoolbox.com/Email-Headers.aspx'. The page title is 'Email Header Analyzer'. Below the title, there's a section titled 'Paste Header:' containing the following email header text:

```
_--_006_5375b3d53dbb45378ef0f93aae485d26infosyscom_
Content-Type: image/png; name="image003.png"
Content-Description: image003.png
Content-Disposition: inline; filename="image003.png"; size=6861; creation-date="Fri, 05 Dec 2025 08:30:01 GMT"; modification-date="Fri, 05 Dec 2025 08:32:20 GMT"
Content-ID: <image003.png@01DC3F5B.D848D6D>
Content-Transfer-Encoding: base64
_--_006_5375b3d53dbb45378ef0f93aae485d26infosyscom_--
```

Below the header text is a button labeled '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](#).

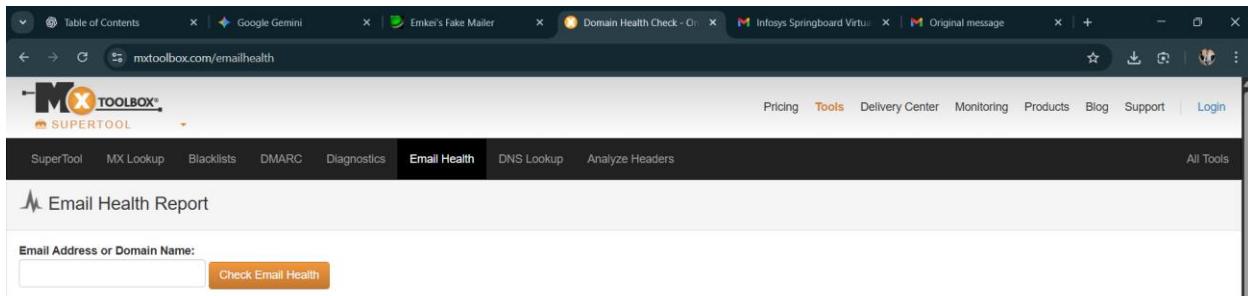


Now you see that type result –

The screenshot shows a browser window with multiple tabs open. The active tab is 'mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=3eba7481-2b09-4d3f-a0ae-64ef3f9b1142'. The page title is 'Header Analyzed'. Below the title, it says 'Email Subject: Infosys Springboard Virtual Internship 6.0 Last opportunity'. There is a 'Copy/Paste Warning' message: 'Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability](#) tool'. A 'Delivery Information' section shows a list of green checkmarks under 'DMARC Compliant': SPF Alignment, SPF Authenticated, DKIM Alignment, and DKIM Authenticated. A 'Relay Information' section shows 'Received 146 seconds' and 'Delay:'. At the bottom of the page, there is a footer with the text 'Your IP is: 103.127.164.149 | 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' and a system status bar showing '18°C Clear', 'Search', and other system icons.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

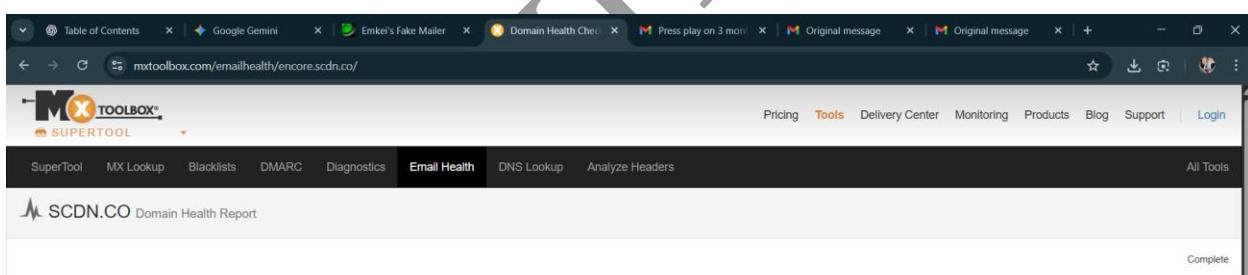
### Check Email Health



The Email Health Check will execute hundreds of domain/email/network performance tests to make sure all of your systems are online and performing optimally. The report will then return results for your domain and highlight critical problem areas for your domain that need to be resolved.

**How it works:** The report uses DNS to obtain the hostnames of your Mail Server, Web Server, and DNS Servers and then queries them to identify potential problems.

- Get full visibility of your email's health status in one concise report
- Identify every problem facing your email, including **blacklist, mail server, web server, and dns issues**



These results are for **scdn.co**. Did you really mean to run **encore.scdn.co**? [Click Here](#)

 Fuel Your Email Success

with MxToolbox Delivery Center

Problems		
	6 Errors	
	12 Warning	
	558 Passed	

Blacklist		
	0 Errors	
	0 Warning	
	492 Passed	

Mail Server		
	5 Errors	
	7 Warning	
	55 Passed	

Web Server		
	1 Errors	
	0 Warning	
	0 Passed	

DNS		
	0 Errors	
	5 Warning	
	11 Passed	

18 Problems



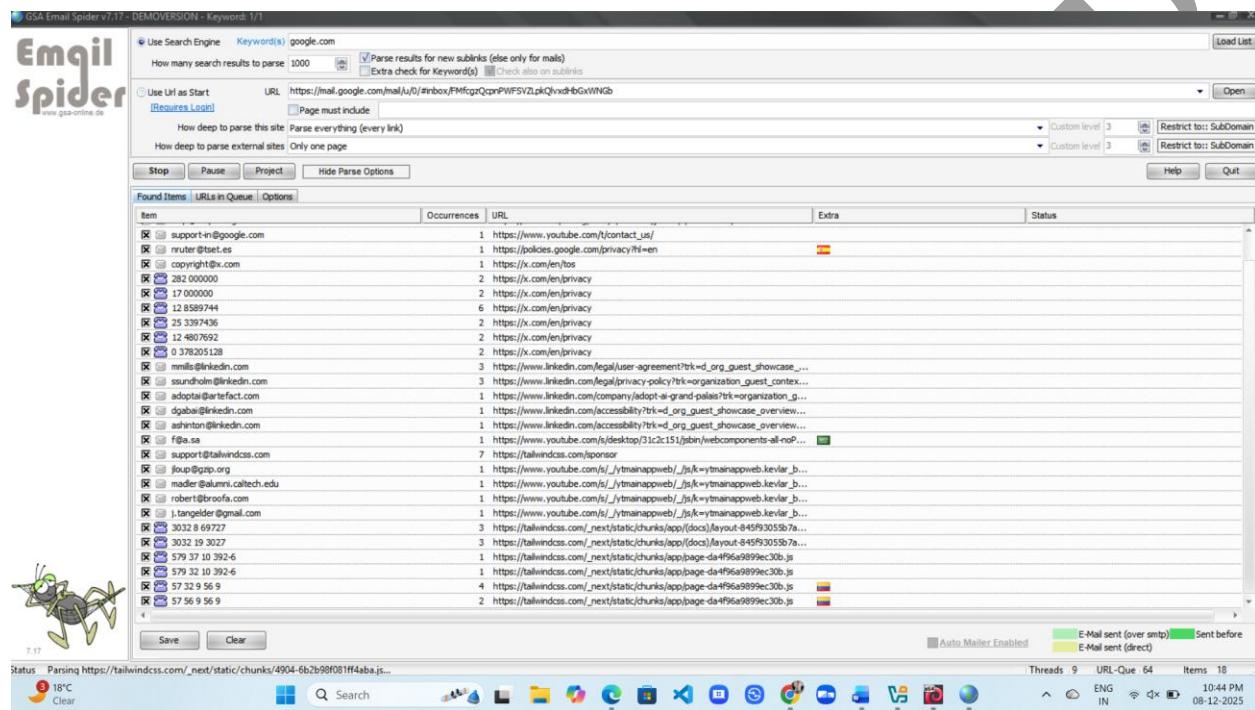
### 3.Email Footprinting Using GSA Email Spider Application :-

After completing installation process then setup the app

Copy url that you want to perform email footprinting

Paste URL in url section.

Click on Start button.



## 8. Demonstrate Footprinting through Social Engineering

### 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

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

The screenshot shows the peekyou.com search interface for the query "Elon Musk". The search bar at the top has "PEOPLE" selected, with "Elon" in the first input field and "Musk" in the second. A dropdown menu for "All States" is open. Below the search bar, the results for "Elon Musk" are displayed. The main result is a card for "Elon Musk" from Texas, Kentucky, and Massachusetts. It includes a "Page Overview" section with a summary of records found, a "Public Records & Background Search" section with a TruthFinder sponsored result for "Elon Musk, age 53, Louisville, KY", and links for "Public Records", "Phonebook", "Email", "Facebook", "Instagram", and "Web Results". To the right, a sidebar shows "Found in Cities" with Austin (TX), Louisville (KY), and Somerville (MA). The browser's status bar at the bottom indicates it's 10:48 PM on 08-12-2025.

The screenshot shows the peekyou.com search interface for the query "sachet023". The search bar at the top has "USERNAME" selected, with "sachet023" in the input field. Below the search bar, the results for "sachet023" are displayed. The main result is a card for "sachet023" showing "8 Profiles Found", "36 Platforms Searched", and "100% Free Search". It includes an "About Username sachet023" section with a note about checking the username across various platforms, and a "Want More Detailed Information?" section with links to contact reports for "sachet023@gmail.com" and "sachet023@yahoo.com". The browser's status bar at the bottom indicates it's 10:49 PM on 08-12-2025.

## 2. Social Media Footprinting Using Sherlock (CLI)

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

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE

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

Example :- sherlock Sundar Pichai

A screenshot of a Kali Linux desktop environment. The top window is a terminal window titled 'root [Running] - Oracle VirtualBox' with the command 'root@kali:~/home/sachet'. It displays a list of over 60 URLs found for a user named 'Sundar' across various platforms like LinkedIn, GitHub, and various forums. The bottom part of the image shows the Windows taskbar with multiple pinned icons and the system tray indicating the date as 08-12-2025.

## 9. Automate Footprinting Tasks using Advanced Tools and AI

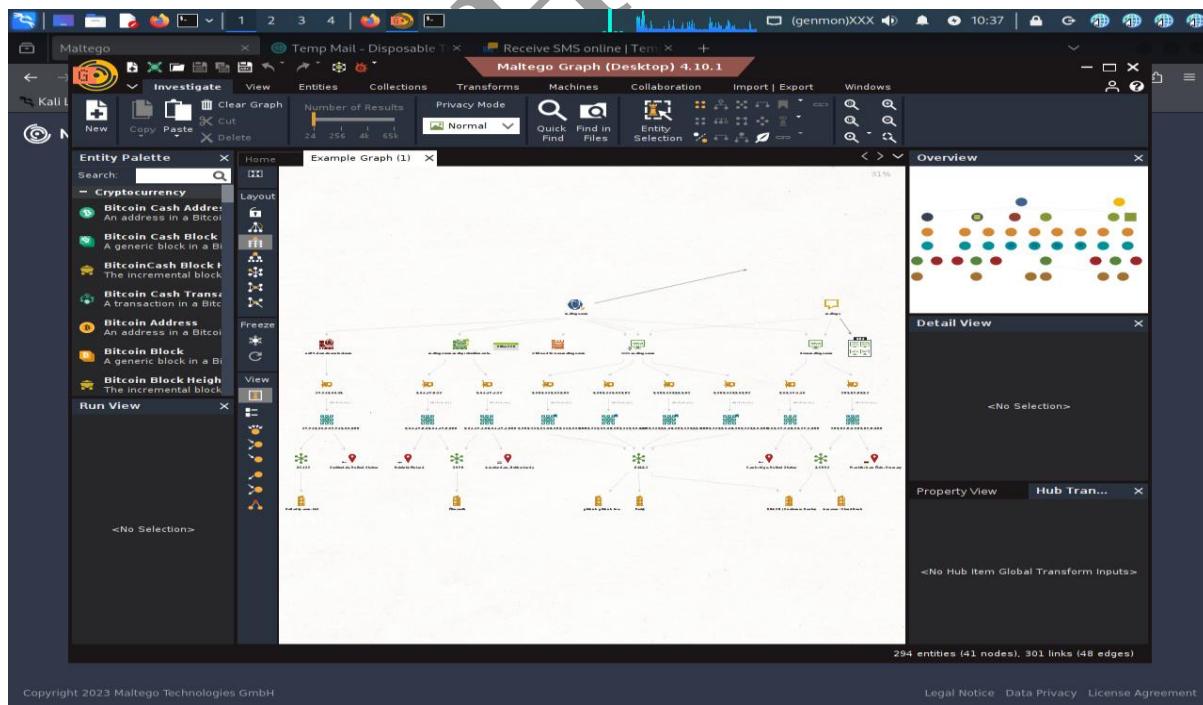
Footprinting tools help gather detailed information about a target system, including its IP location, routing, DNS, and domain information. These tools automate data collection from various online sources to support reconnaissance activities.

### Automate Footprinting Tasks using Advanced Tools

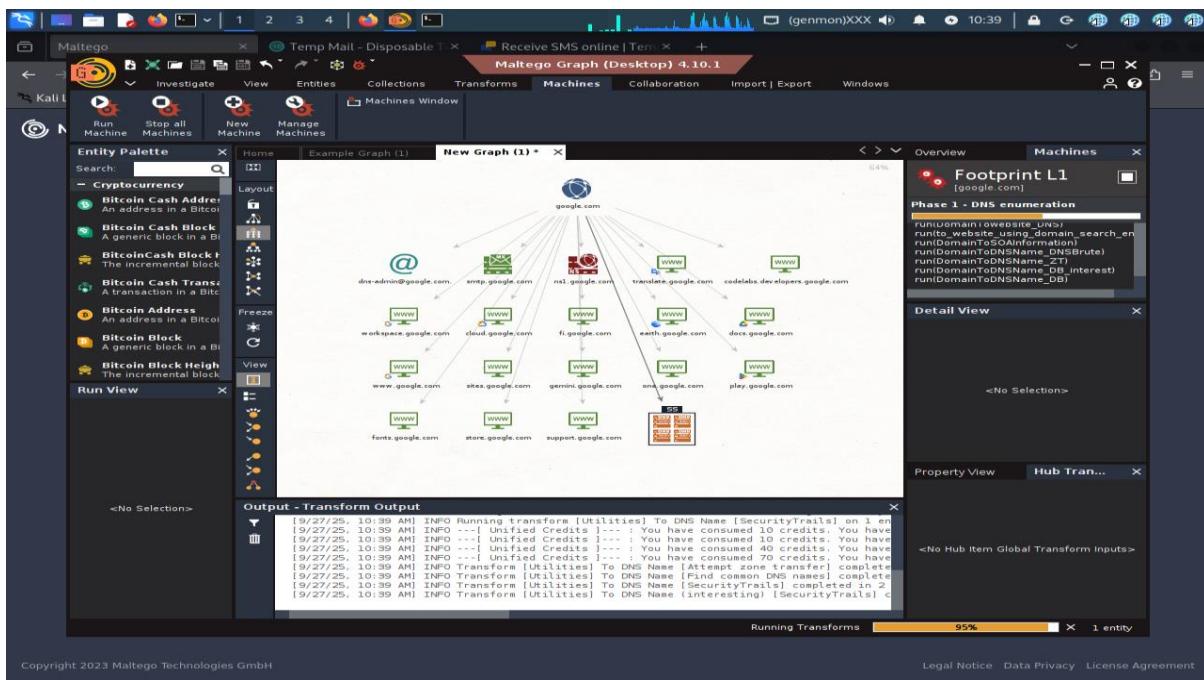
#### Maltego

Source: <https://www.maltego.com>

Maltego is an automated tool that can be used to determine the relationships and real-world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc. Attackers can use different entities available in the tool to obtain information such as email addresses, a list of phone numbers, and a target's Internet infrastructure (domains, DNS names, Netblocks, IP addresses information). As shown in the screenshot, attackers add a **Website entity**, rename it with the target's domain, and obtain the email addresses and phone numbers associated with the target.



## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



## OSINT Framework

Source: <https://osintframework.com>

The **OSINT Framework** is an open-source platform used for **automated footprinting, reconnaissance, and intelligence gathering**. It focuses on free online tools and resources, arranged in a **tree-style web interface** categorized by function.

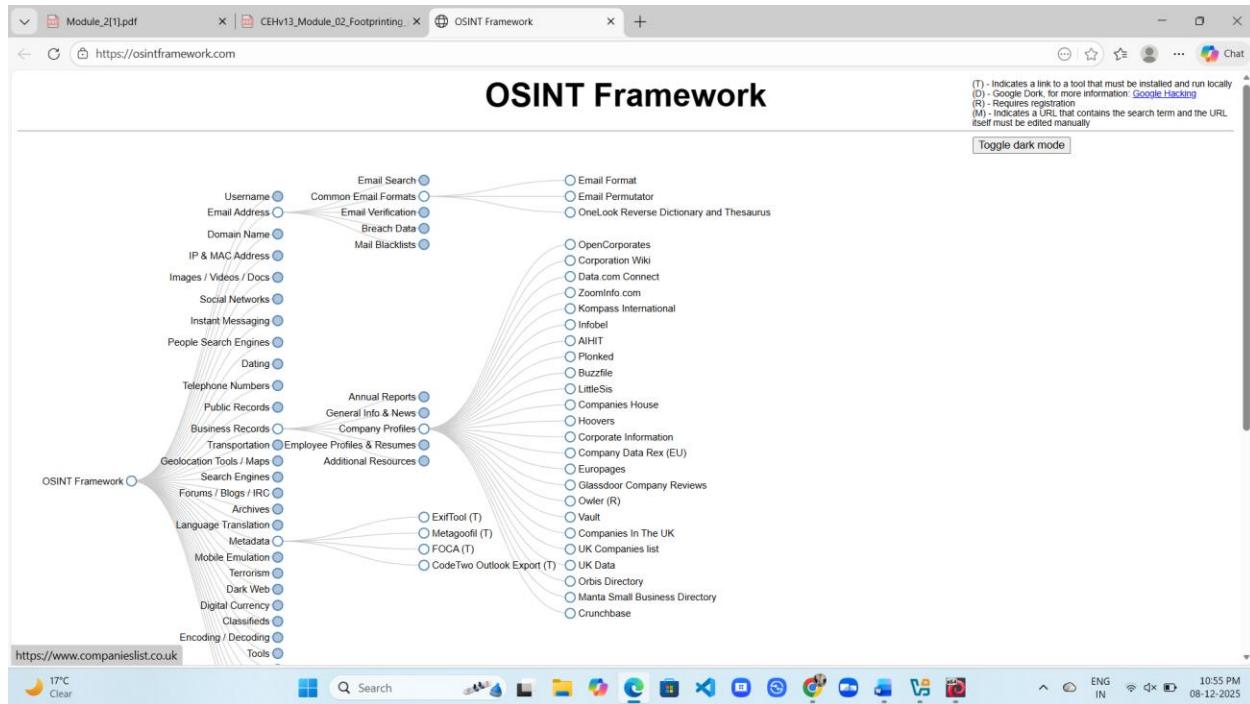
### Indicators used in the framework:

- **(T)** – Tool must be installed and run locally
- **(D)** – Google dork (special search query)
- **(R)** – Requires registration
- **(M)** – Manual URL edit needed (search term inserted manually)

### Use:

Security professionals use it to quickly find tools for gathering domain, network, or personal information during investigations.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



### Subfinder

Source: <https://github.com>

**Subfinder** is a **subdomain discovery tool** that identifies valid subdomains of websites using **passive online sources** (no active scanning).

It supports multiple **output formats** such as **JSON**, **file**, and **stdout**, making it easy to use in automation or reporting.

#### Use:

Security professionals use it for **reconnaissance** to map website infrastructure and find hidden subdomains.

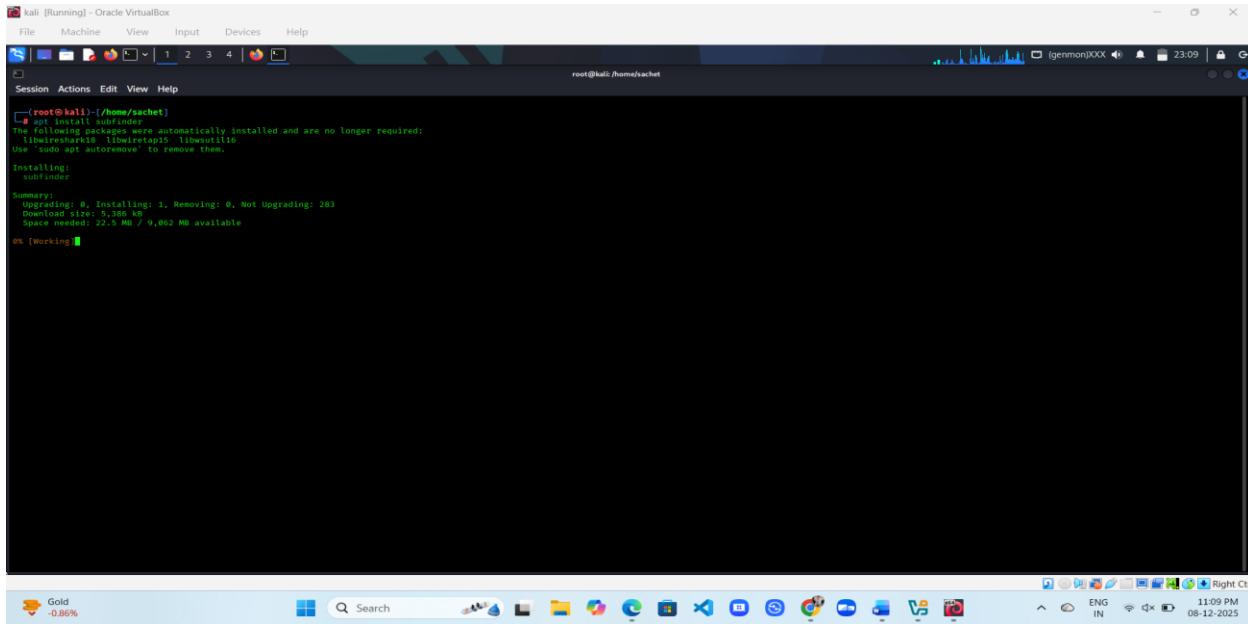
#### How to use It

Open Kali linux / Parrot OS.

Open Terminal.

Type **apt install subfinder** on terminal.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



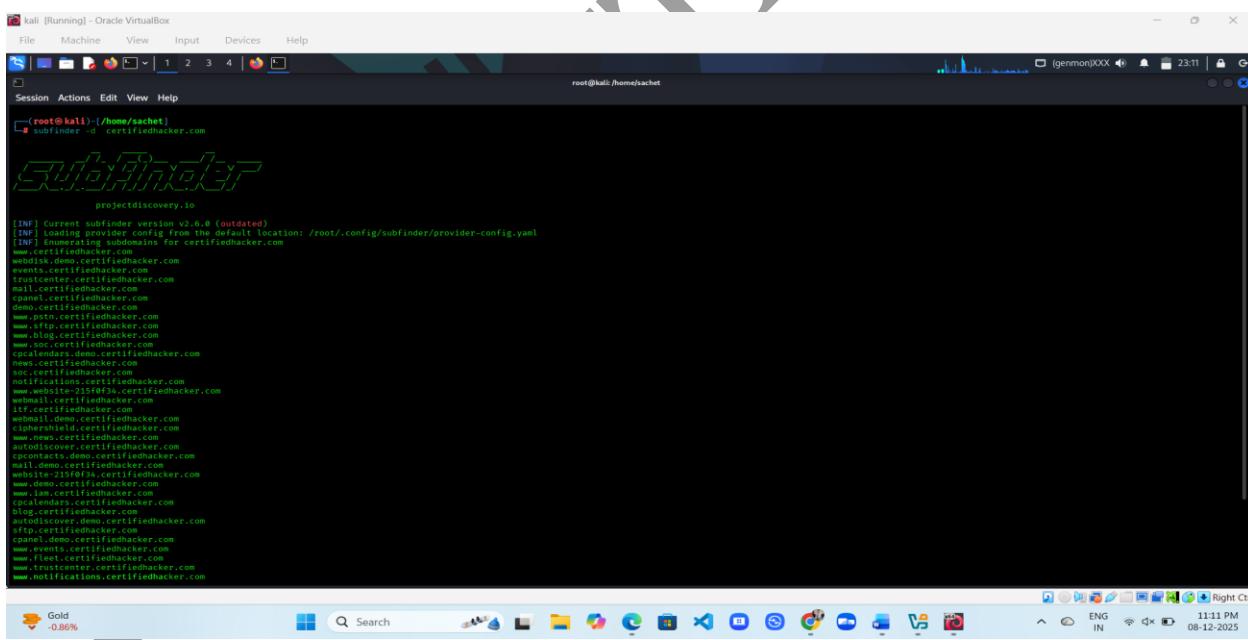
```
(root㉿kali:~/home/sachet)
└─# subl install subfinder
The following packages were automatically installed and are no longer required:
libnmap-ncurses2 libnmap-p3 libnmap-util16
Use 'apt autoremove' to remove them.

Installing:
subfinder

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 20
Download size: 5,386 kB
Space needed: 22.5 MB / 9,062 MB available
0% [working]
```

- subfinder -d certifiedhacker.com

-d - - domain



```
(root㉿kali:~/home/sachet)
└─# subfinder -d certifiedhacker.com
[!] Subfinder v2.6.0 - Subdomain Enumerator for Pentesters
[!] https://github.com/projectdiscovery/subfinder
[!] https://www.projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from the default location: /root/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for certifiedhacker.com
www.certifiedhacker.com
mail.certifiedhacker.com
events.certifiedhacker.com
trustcenter.certifiedhacker.com
mail.demo.certifiedhacker.com
cpanel.certifiedhacker.com
demo.certifiedhacker.com
news.certifiedhacker.com
mail.demo.certifiedhacker.com
www.certifiedhacker.com
www.ftp.certifiedhacker.com
www.blog.certifiedhacker.com
www.certifiedhacker.com
cpaneldomains.demo.certifiedhacker.com
news.certifiedhacker.com
mail.certifiedhacker.com
notifications.certifiedhacker.com
www.website-215f0f3a.certifiedhacker.com
www.certifiedhacker.com
http.certifiedhacker.com
https.certifiedhacker.com
www.news.certifiedhacker.com
autodiscover.certifiedhacker.com
cpaneldomains.demo.certifiedhacker.com
mail.demo.certifiedhacker.com
website-215f0f3a.certifiedhacker.com
mail.certifiedhacker.com
www.iam.certifiedhacker.com
cpaneldomains.certifiedhacker.com
bing.certifiedhacker.com
autodiscover.demo.certifiedhacker.com
SFTP.certifiedhacker.com
cpaneldomains.certifiedhacker.com
www.events.certifiedhacker.com
www.victims.certifiedhacker.com
www.certifiedhacker.com
www.notifications.certifiedhacker.com
```

## AI-Powered OSINT Tools.

### The Role of AI in Open-Source Intelligence (OSINT)

Artificial Intelligence (AI) has significantly enhanced OSINT by improving data collection, analysis, and prediction capabilities. AI automates data processing and extracts relevant insights more efficiently than traditional methods.

## Taranis AI

Link- <https://taranis.ai>

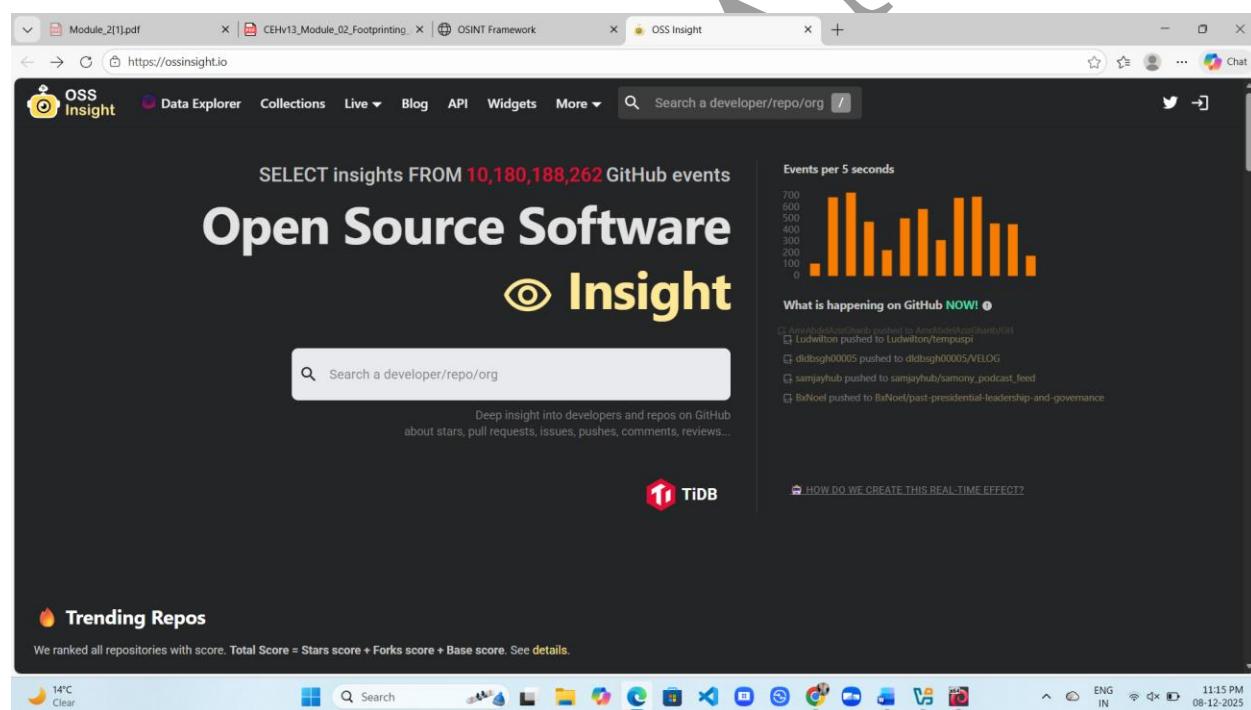
Taranis AI is an open-source intelligence tool that uses AI to **gather, analyze, and interpret** publicly available data.

It helps ethical hackers **identify security threats, vulnerabilities**, and related information from multiple internet sources.

## OSS Insight

Link- <https://ossinsight.io>

OSS Insight uses AI to analyze **over 5 billion GitHub events**, giving deep insights into the open-source ecosystem — from repository analytics to developer productivity data.

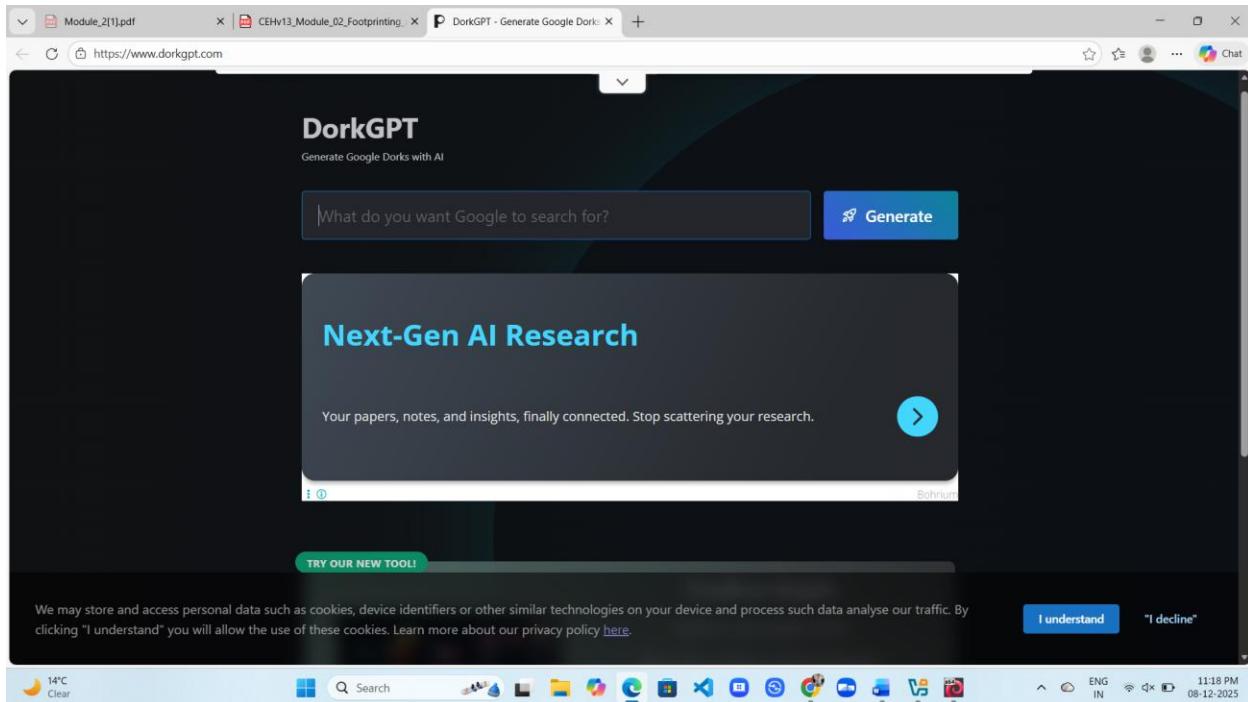


## Other AI OSINT Tools

- **DorkGPT:** <https://dorkgpt.com>

Uses AI to generate advanced Google dorks for finding hidden or sensitive information online.

## MODULE – 2 FOOTPRINTING AND RECONNAISSANCE



## Using Gemini-cli AI

A screenshot of a Kali Linux terminal window titled "kali [Running] - Oracle VirtualBox". The terminal is running the Gemini-cli application. The user has run the command "dig subdomains of google.com using dig". The output shows an attempt to perform a zone transfer (AXFR) on google.com, which failed due to connection refused from multiple servers. The user then tried a web search for "subdomains of google.com" using GoogleSearch, which returned several results. Finally, the user lists some common subdomains of google.com. The terminal window is set against a background watermark of the word "HITA". The system tray at the bottom shows the date and time as 08-12-2025 and 11:28 PM, along with other system icons.

## 10. Explain Footprinting Countermeasures.

### Footprinting Countermeasures

Footprinting countermeasures are defensive strategies and techniques used to minimize an organization's publicly available information, making it harder for attackers to gather intelligence and map out potential attack vectors.

#### Technical and Configuration Controls

These measures involve configuring systems and services to reduce information exposure.

- **Secure Web Servers:** Properly **configure web servers** to prevent information leakage, such as hiding server version banners and disabling directory browsing.
- **Control Search Engine Indexing:** Prevent **search engines** from caching sensitive web pages and utilize anonymous domain registration services to hide ownership details.

#### Administrative and Policy Controls

These countermeasures focus on creating policies and providing training to employees.

- **Restrict Social Media Access:** Limit or **block employee access** to social networking sites from the corporate network to prevent accidental information disclosure.
- **Employee Education:** Train employees to use pseudonyms when participating in public blogs, groups, and forums to avoid linking their online persona to the organization.
- **Manage Public Information:** Be careful **not to reveal critical information** in public documents like press releases, annual reports, or product catalogs. The overall amount of information published on websites or the internet should be limited.

#### Proactive Measures

This involves actively searching for your own organization's exposed information.

- **Perform Self-Footprinting:** Actively **use footprinting techniques** on your own organization to discover and remove any sensitive information that has become publicly available.

## Module Summary

The module provided a comprehensive overview of **footprinting**, starting with its core concepts and objectives. It detailed various techniques for information gathering, including the use of search engines, internet research services, and social networking sites.

### Key Topics Covered

The module explored several specific methods of footprinting in detail:

- **Technical Footprinting:** It explained **Whois and DNS footprinting**, as well as network footprinting which includes traceroute analysis.
- **Communication-Based Footprinting:** It discussed techniques for **email footprinting**.
- **Human-Based Footprinting:** The module also covered footprinting through **social engineering**.

### Tools and Defense

Finally, the module presented an overview of important **footprinting tools** used by security professionals. It concluded with a detailed discussion of **countermeasures** that organizations can implement to defend against footprinting and reconnaissance activities. The text notes that the subsequent module will cover network scanning.

THANK YOU  
SACHCHITANAND