**Foot printing and Reconnaissance**

**Index:**

|  |  |
| --- | --- |
| 1. **What is foot printing? Types and how to do it.** | 1 |
| 1. **Google hacking** | 2-3 |
| 1. **Finding a Company’s Top level domains and Sub-domains** | 3 |
| 1. **Gathering information from LinkedIn** | 4-5 |
| 1. **Determining the operating system** | 5-6 |
| 1. **Website Footprinting** | 6-7 |
| 1. **Whois Lookup** | 7 |
| 1. **Extracting DNS information** | 8 |
| 1. **WinHTTrack website copier** | 9-11 |
| 1. **Using Traceroute** | 12-13 |
| 1. **Recon-ng** | 14-18 |

**What is Footprinting?**

Footprinting in ethical hacking is the process of gathering information about a target system or network to understand its structure, vulnerabilities, and potential entry points. It involves passive or active techniques to collect data, aiding in planning penetration tests effectively.

**Types of Footprinting:**

1. Passive Footprinting: without direct interaction
2. Active Footprinting: with direct interaction

**How can we do this Footprinting?**

Using search engines.

Here are some major search engines:

1. Google – Most popular, widely used globally.

2. Bing – Microsoft’s search engine.

3. Yahoo! – Powered by Bing.

4. DuckDuckGo – Focuses on privacy.

5. Baidu – Dominant in China.

6. Yandex – Popular in Russia.

7. Ecosia – Eco-friendly, plants trees with revenue.

8. Ask.com – Known for Q&A-based searches.

9. Wolfram Alpha – Specialized in computational knowledge.

10. Startpage – Privacy-oriented, pulls results from Google.

Here are search engines and tools widely used for information gathering in ethical hacking, reconnaissance, and OSINT (Open Source Intelligence):

1. Shodan – Specialized in discovering IoT devices and servers exposed online.

2. Censys – Focuses on collecting data about internet-facing assets, like certificates and devices.

3. Google Dorks – Using advanced Google search queries for specific information leaks or vulnerabilities.

4. Maltego – An OSINT tool that aggregates data from various public sources for visualization.

5. ZoomEye – Similar to Shodan, scans open ports, services, and devices.

6. Recon-ng – A web-based reconnaissance tool for gathering information from APIs.

7. Wayback Machine (Archive.org) – Retrieves historical versions of websites.

8. Have I Been Pwned – Checks for compromised credentials in data breaches.

9. SpiderFoot – An automation tool for collecting OSINT data, such as IPs, domains, and emails.

10. Whois – Used to gather domain registration and ownership information.

**Google hacking:**

Google hacking involves using advanced search operators, called Google Dorks, to find sensitive information or vulnerabilities unintentionally exposed online, such as passwords, files, or misconfigured systems, aiding in ethical hacking and security audits.

Here are some popular Google advanced search operators used in ethical hacking and information gathering:

1. site: – Searches within a specific domain (e.g., `site:example.com`).

2. filetype: – Finds specific file types (e.g., `filetype:pdf`).

3. intitle: – Searches for keywords in the page title (e.g., `intitle:"index of"`).

4. inurl: – Searches for keywords in the URL (e.g., `inurl:login`).

5. cache: – Displays Google’s cached version of a webpage (e.g., `cache:example.com`).

6. related: – Finds sites similar to the given URL (e.g., `related:example.com`).

7. link: – Identifies pages linking to a specific website (e.g., `link:example.com`).

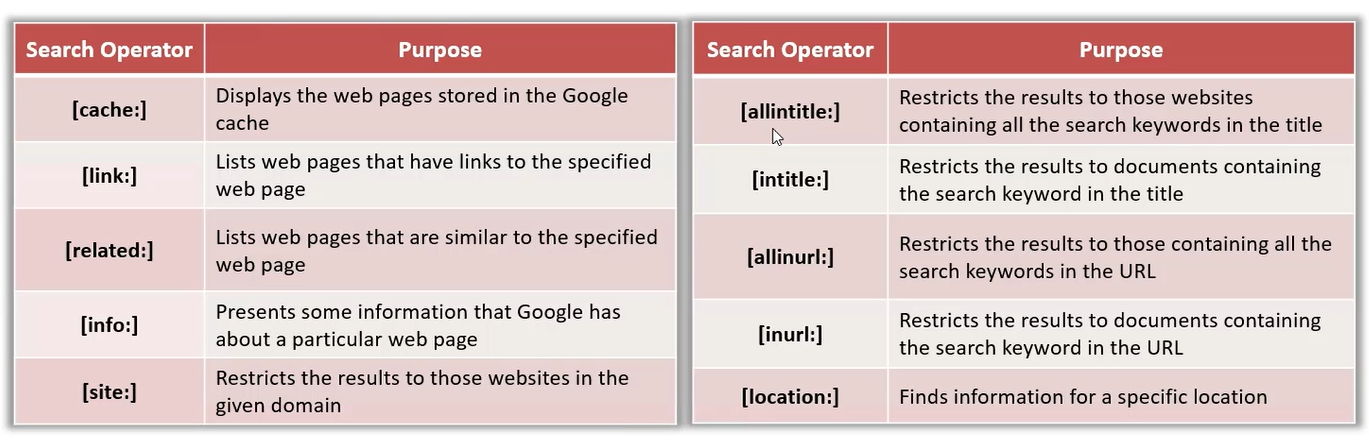
8. " " (Quotes) – Finds exact matches for the enclosed phrase (e.g., `"admin login"`).

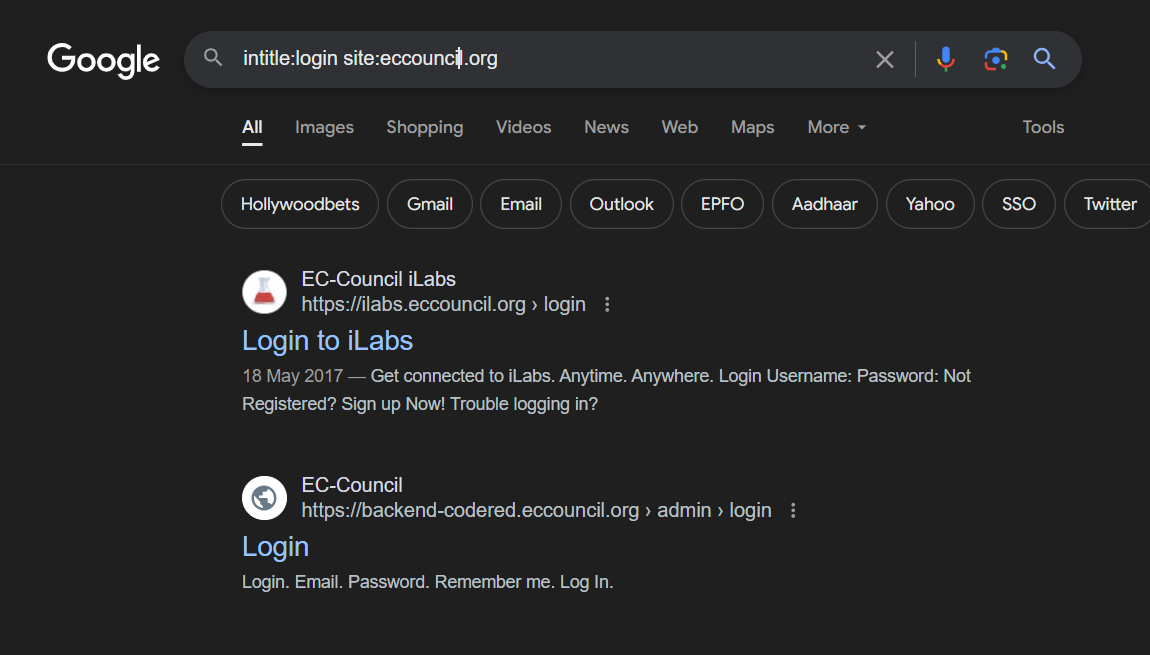
9. - (Minus) – Excludes terms from search results (e.g., `password -twitter`).

10. OR – Finds results containing either one term or another (e.g., `login OR register`).

These operators enhance search precision, often used in reconnaissance to uncover specific data or vulnerabilities.

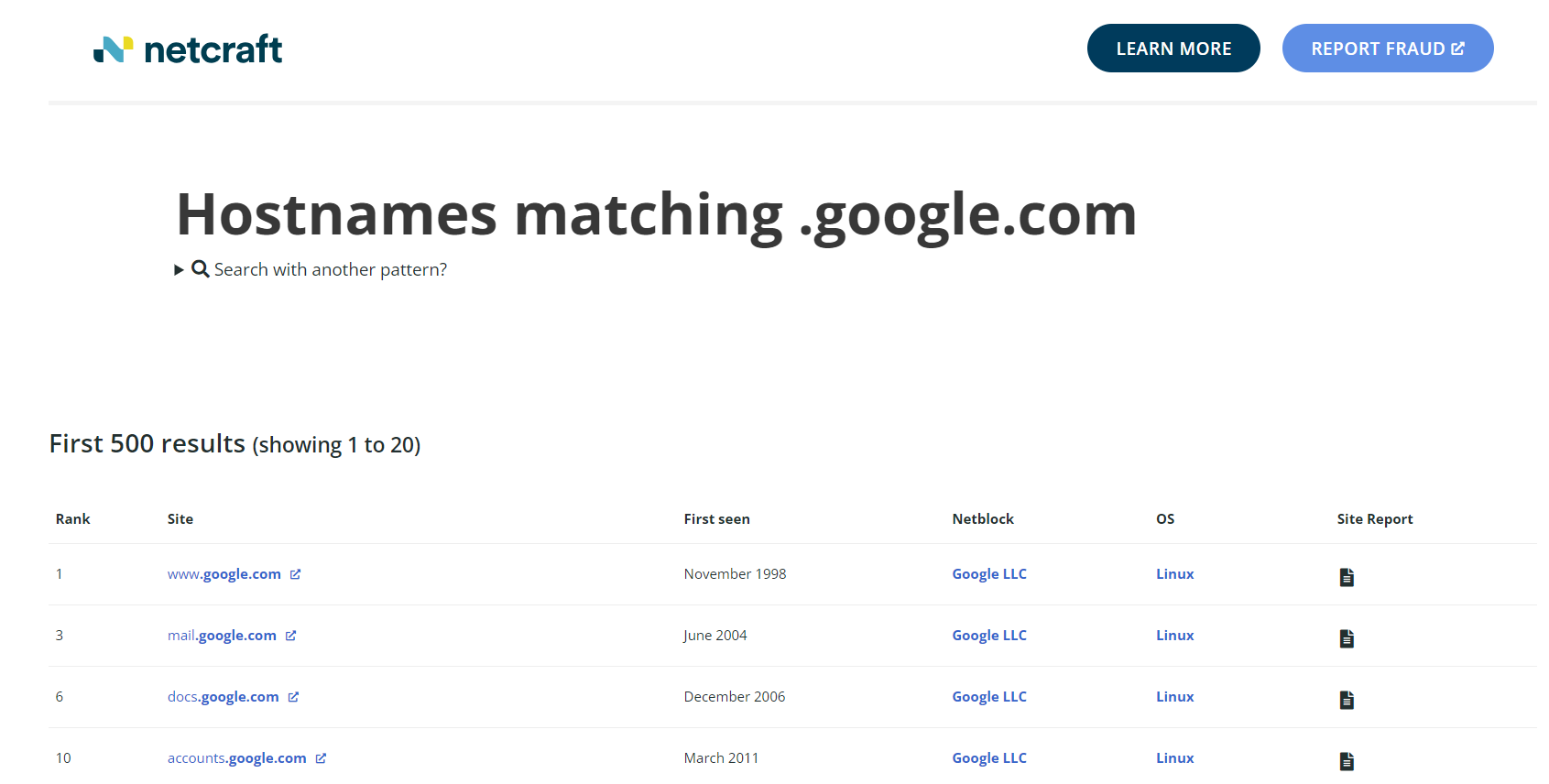
Some more operators:





**Finding a Company’s Top level domains and Sub-domains:**

We can use websites as Netcraft:

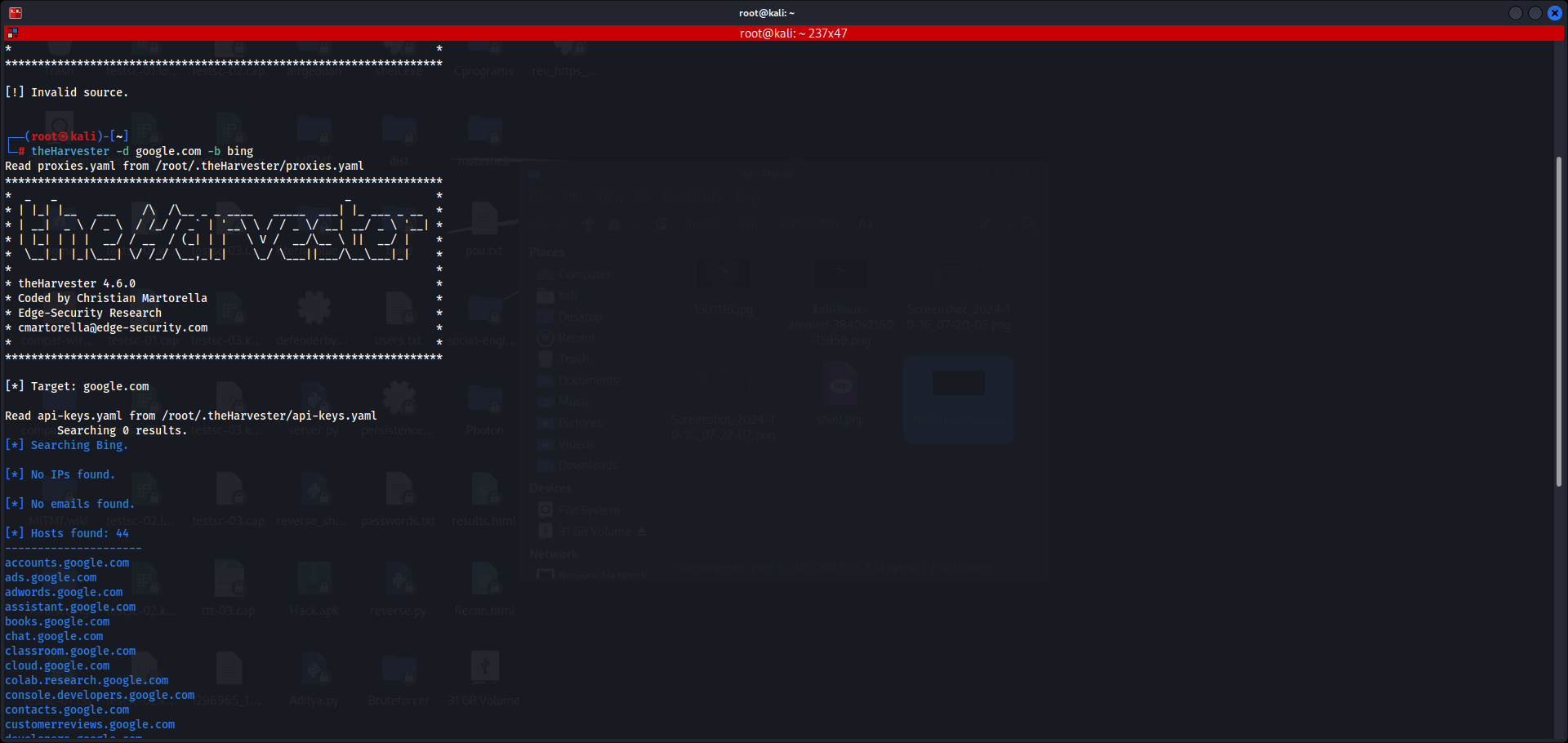


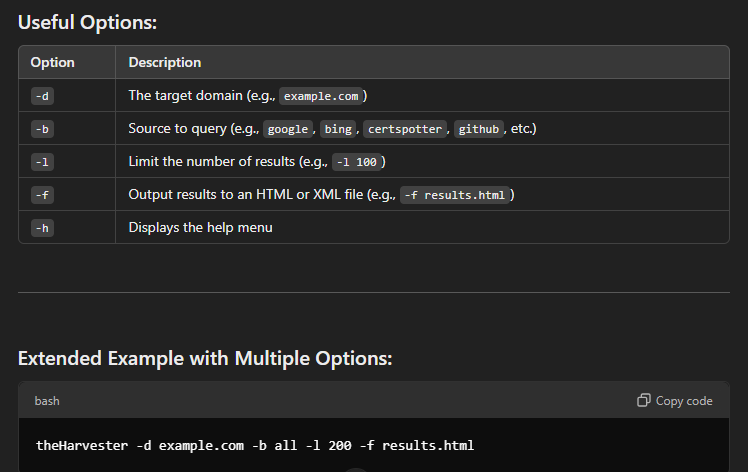
**Gathering information from linkedin:**

We can use tools ‘theHarvester’ and ‘Email spider’ to gather the target email address.

In theHarvester we will use the syntax:

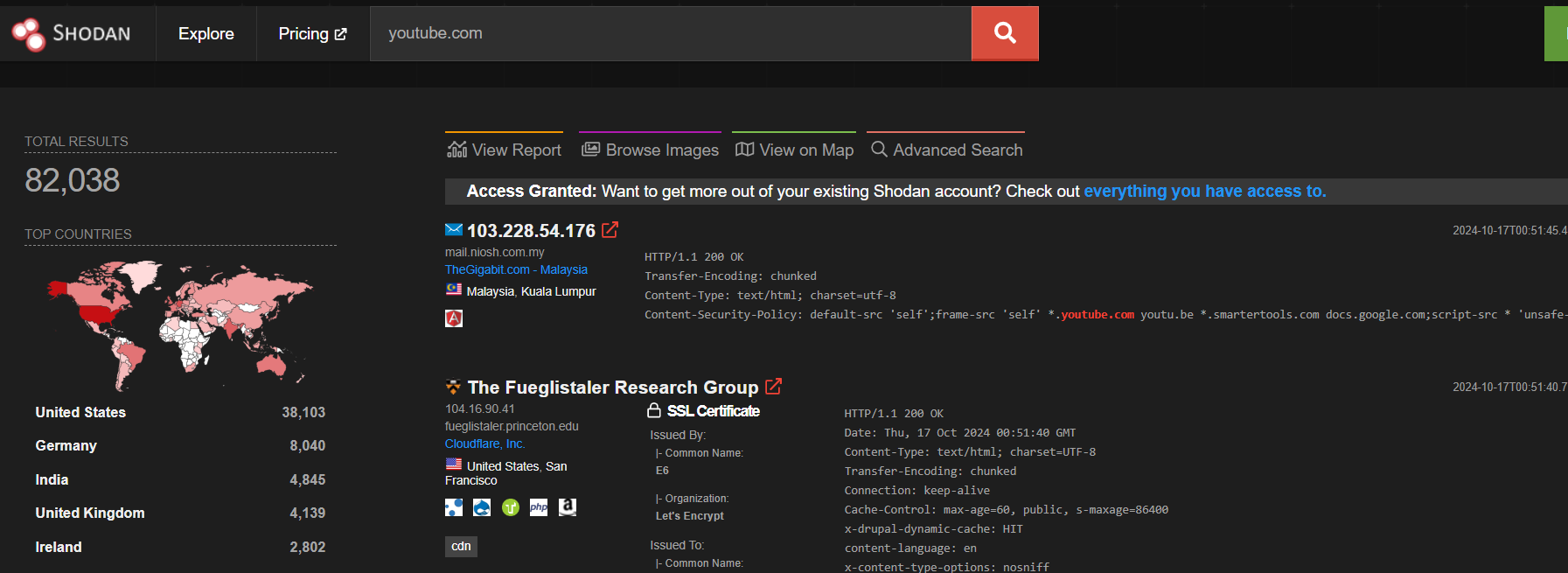
**theHarvester -d <domain> -b <source>**

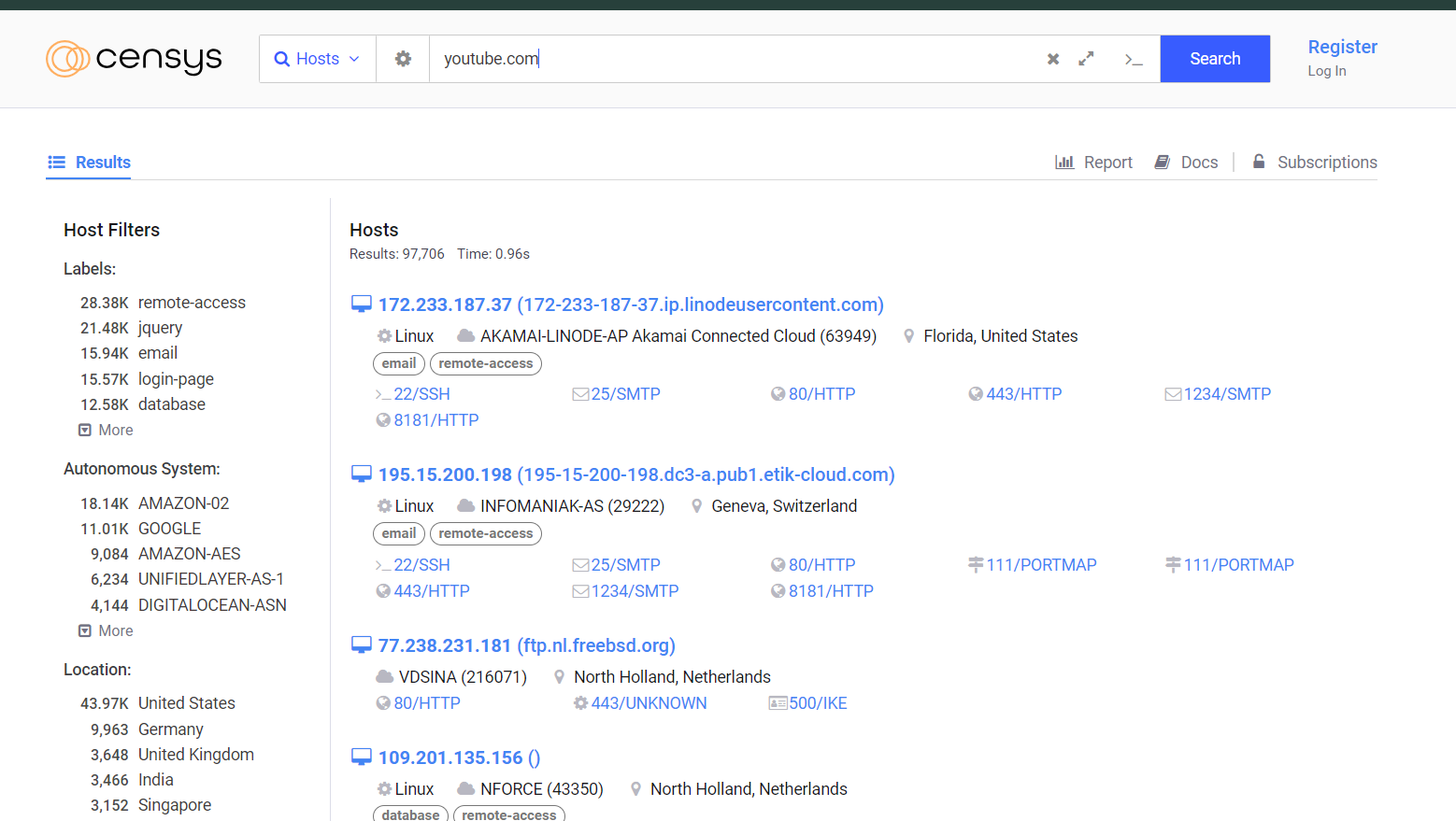


****

**Determining the operating system:**

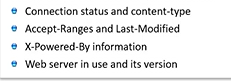
We can use services such as SHODAN and Censys

****

****

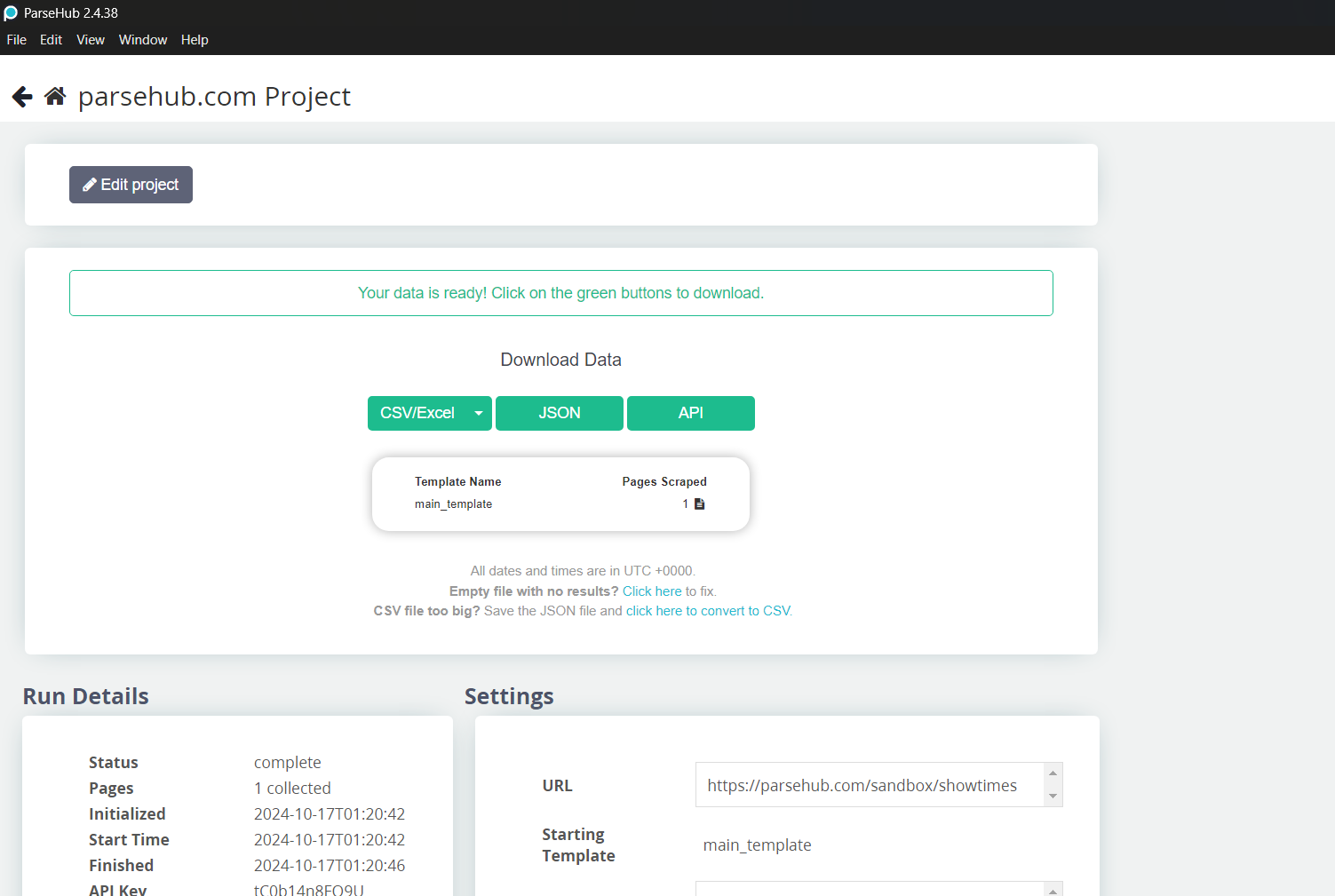
**Website Footprinting:**

We can use the Burpsuite, Zaproxy, Wappalyzer, CentralOps, Website informer etc to view headers that provide the following info:



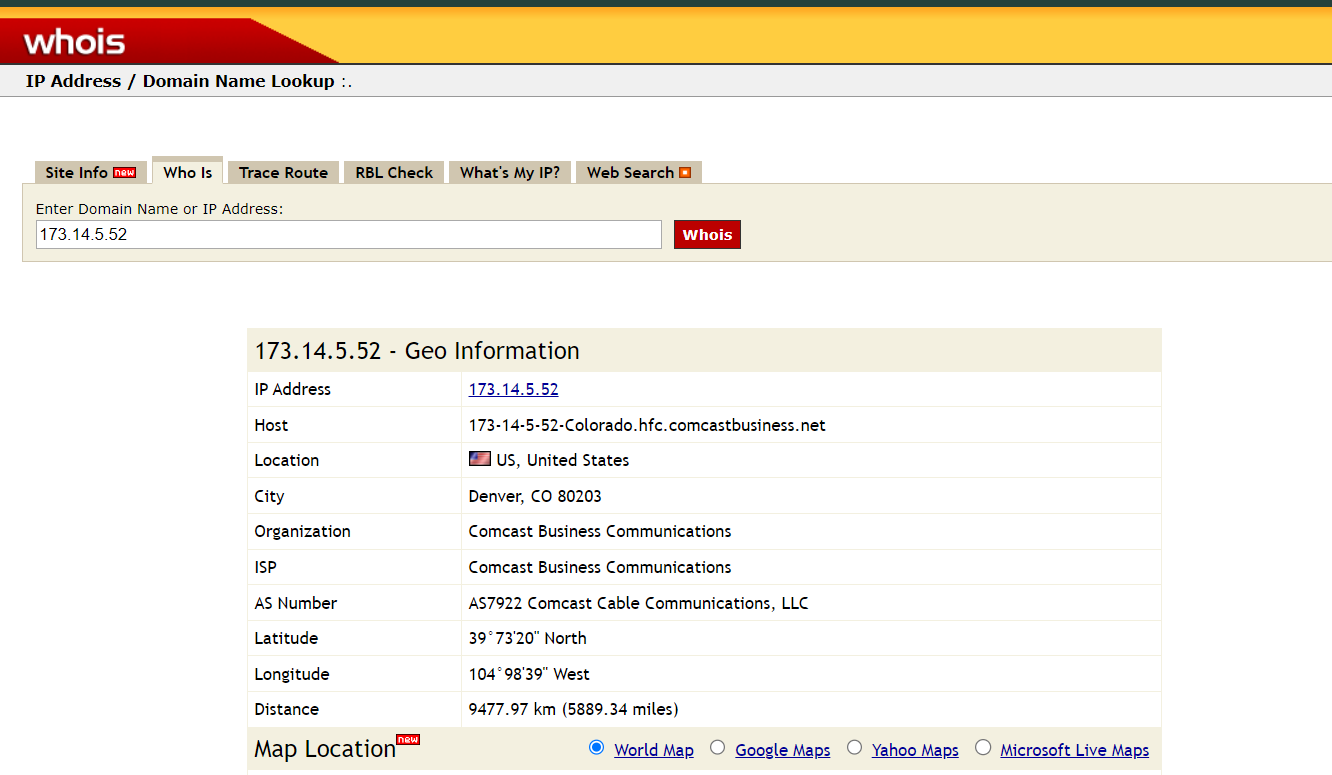
We can also examine the HTML source code to get some information from the comment sections. We can also examine cookies of the website.

We can also use Web data extractor/Parsehub etc to do so.

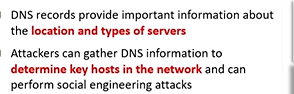


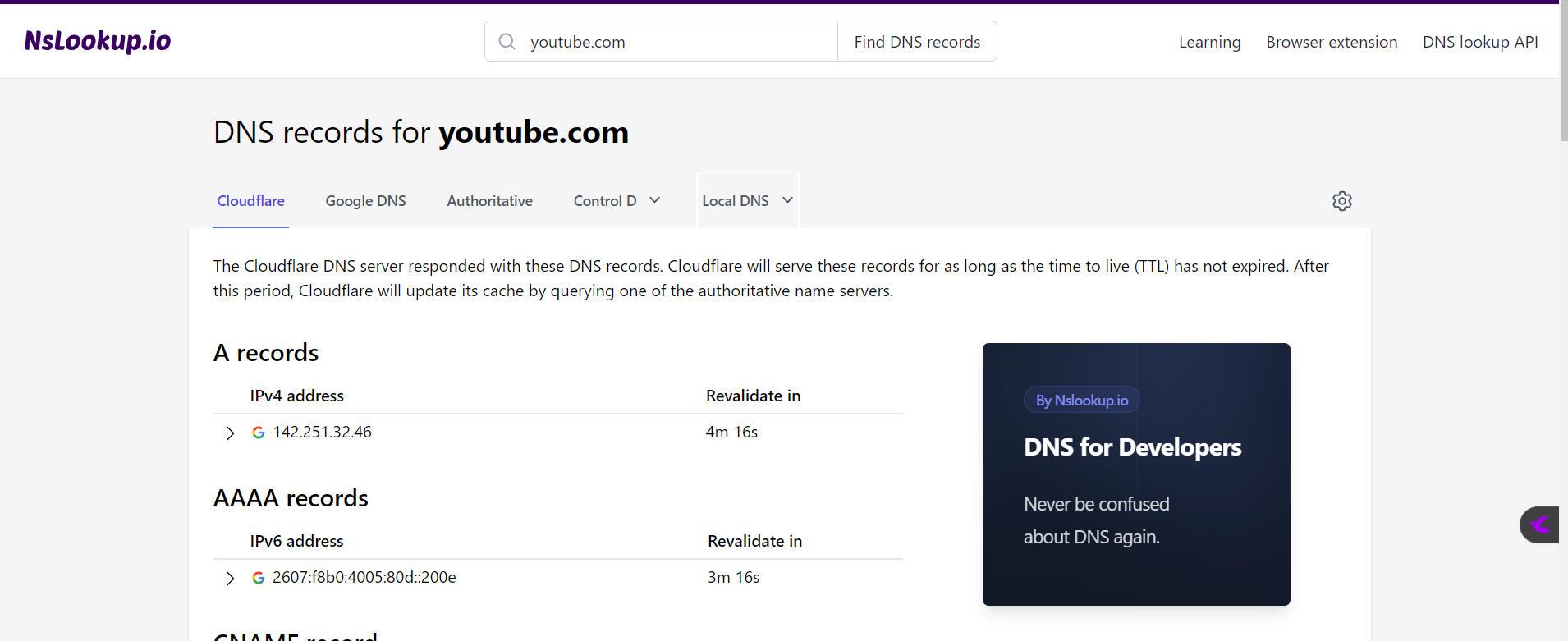
**Whois Lookup:**

This allows us to know the important information about any IP address



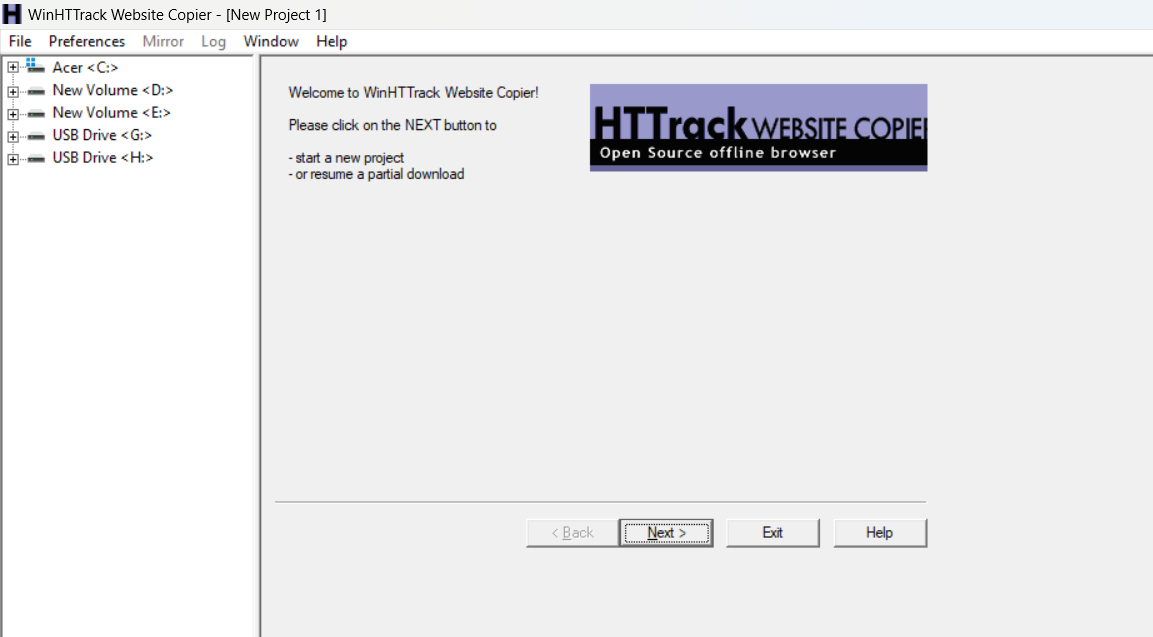
**Extracting DNS information:**

****

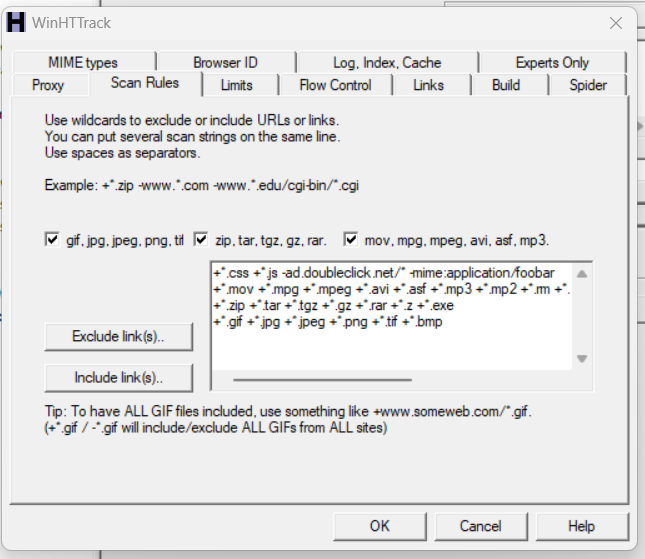


**WinHTTrack website copier:**

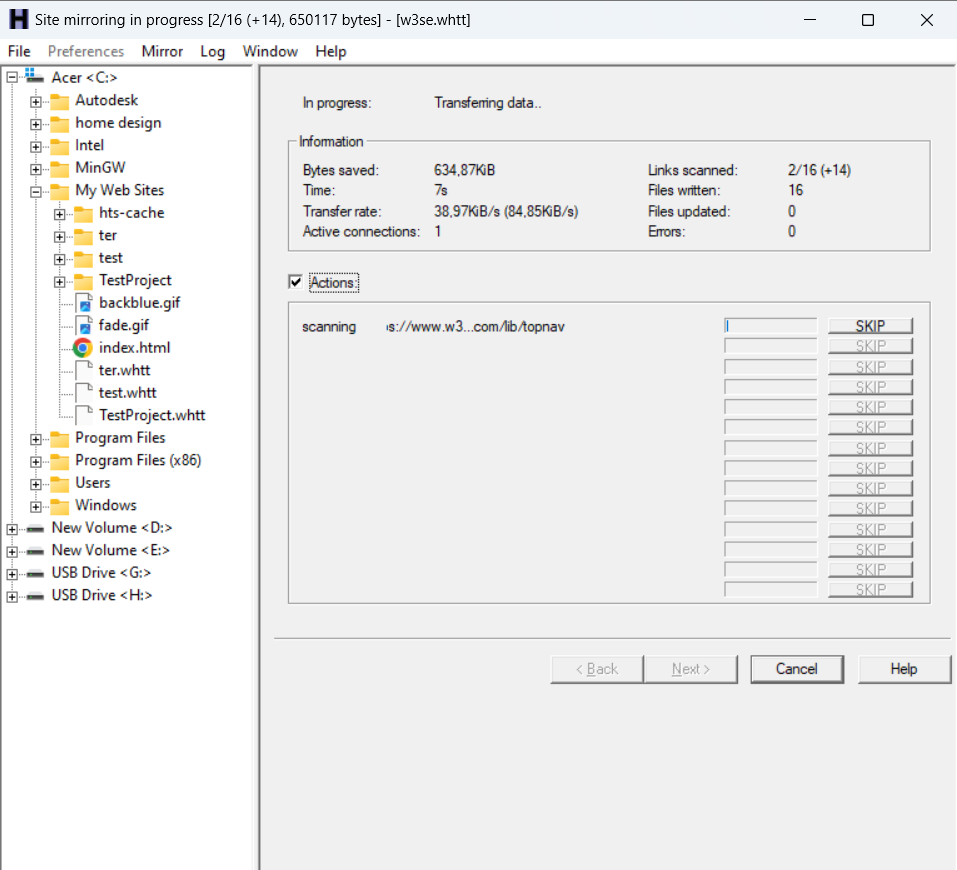
It allows to copy the whole website offline and to allow work on penetration testing on it.

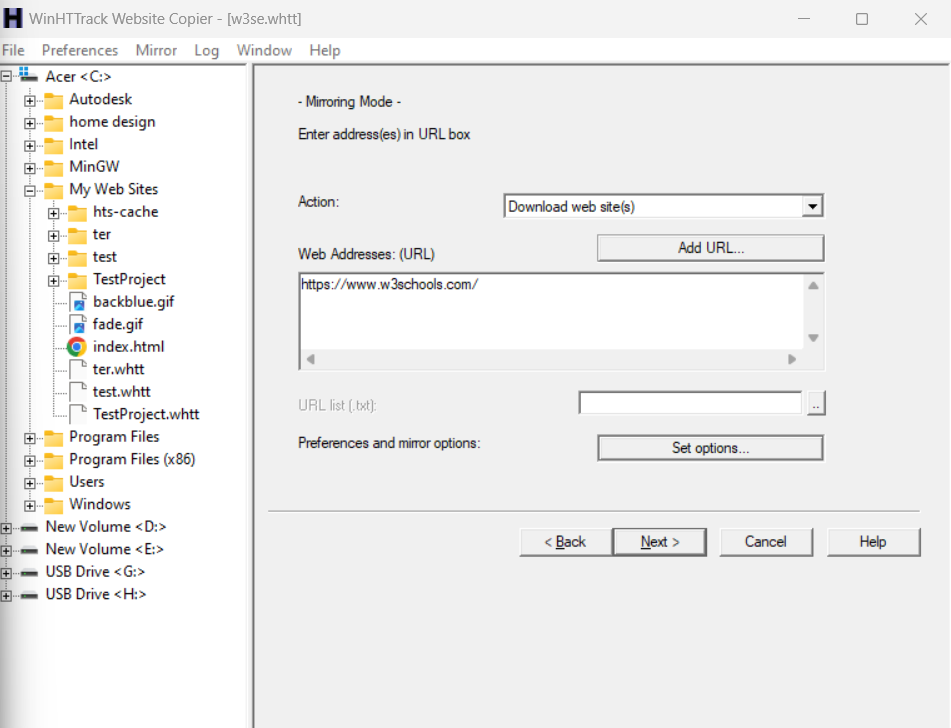


The below image is to show that all the extension are included:

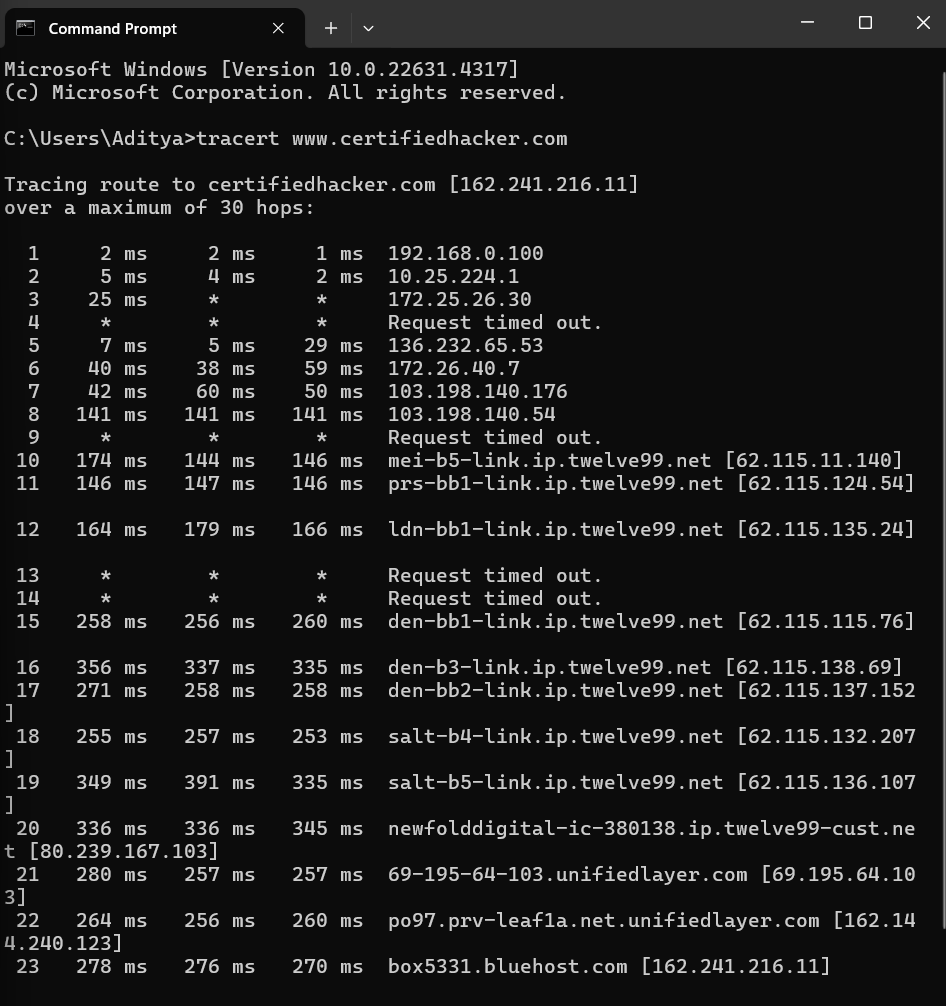


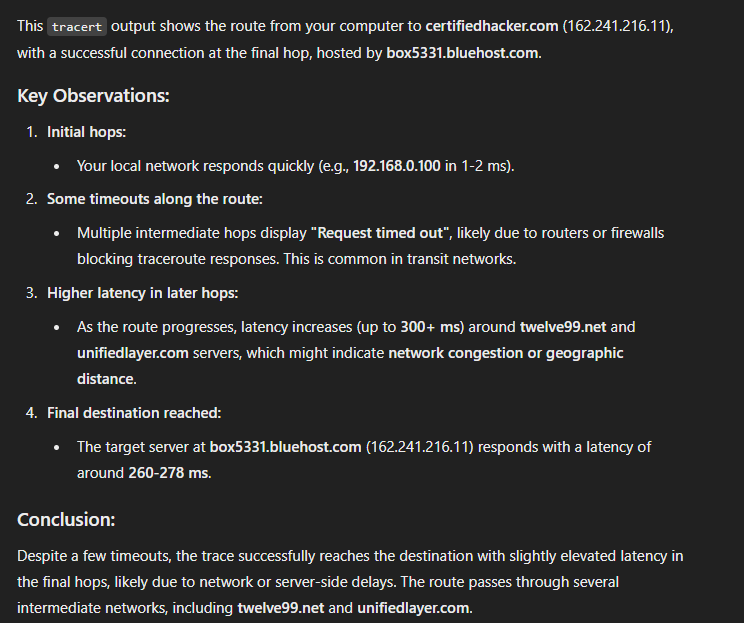
The below ss indicates that the copying process begun:





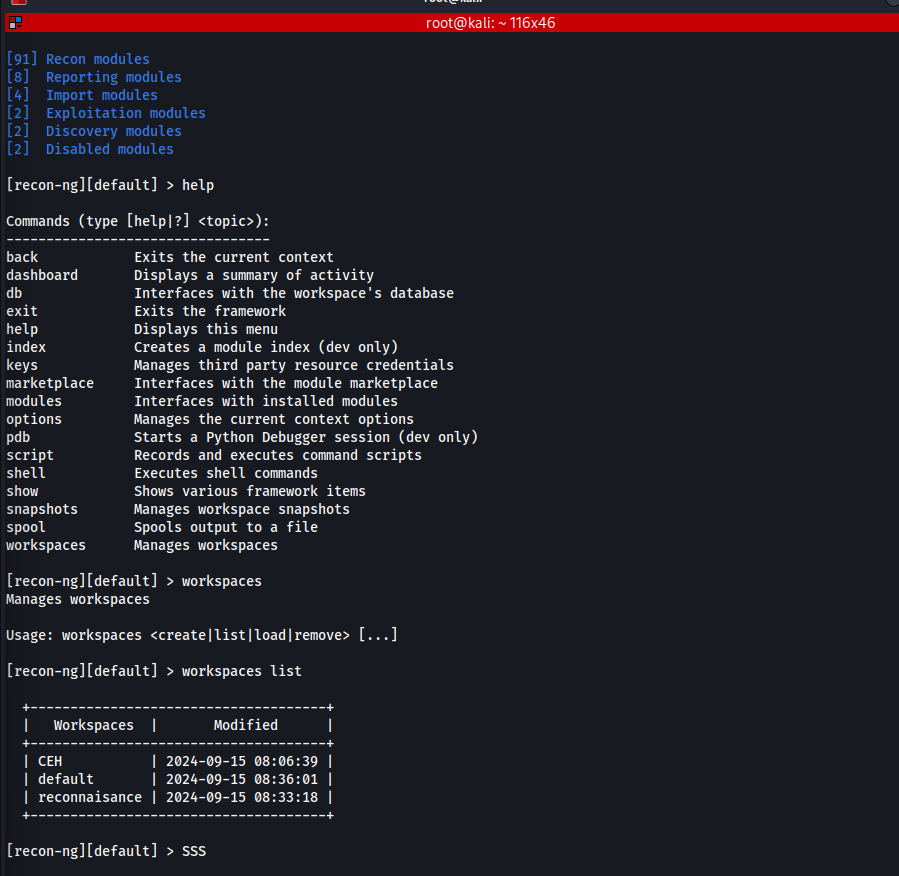
**Using Traceroute:**



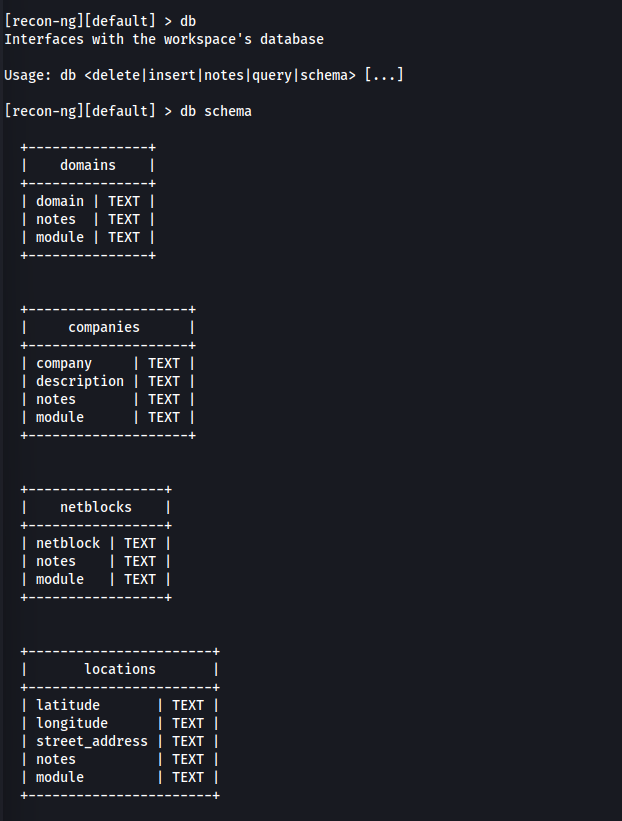


**Recon-ng:**

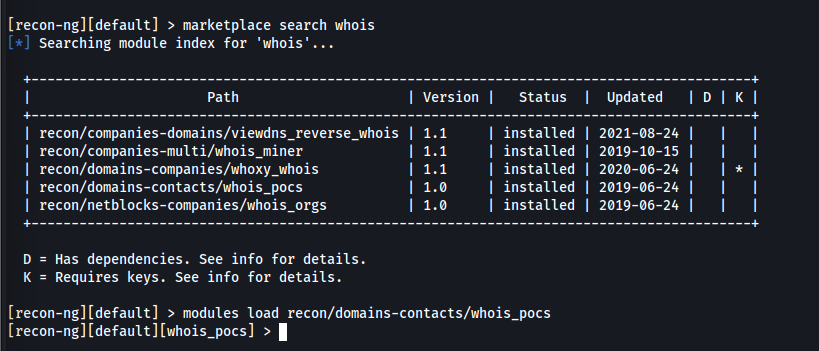
****

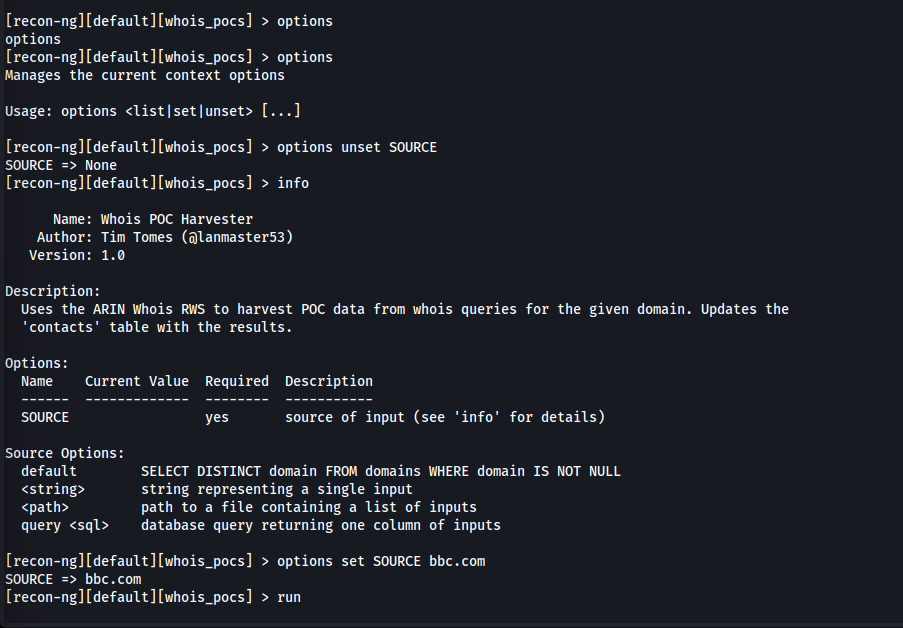
****

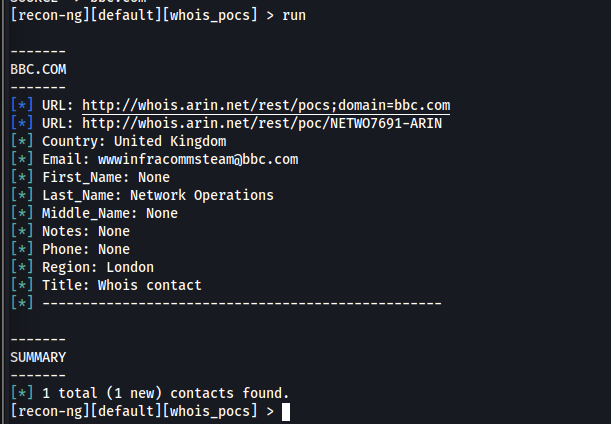
The above screenshot indicates the list of workspaces in recon-ng, also we can switch between the workspaces as well as delete the one we want.

Also, we can look for the databases and look for the schema of the database as shown above.

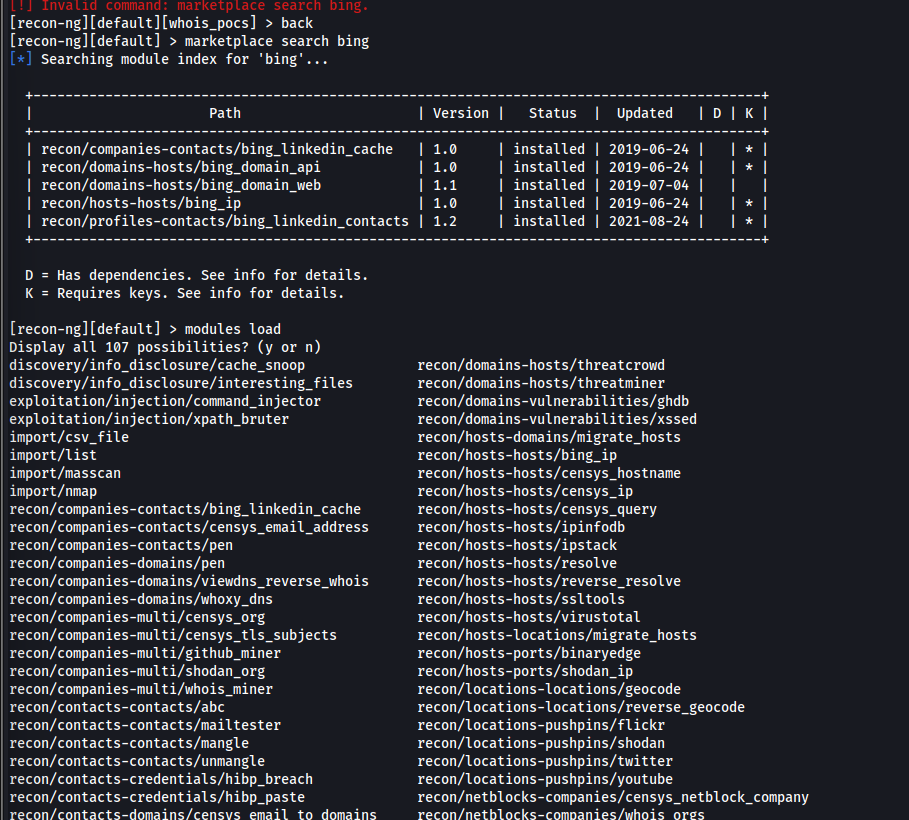
So, how to use a module:

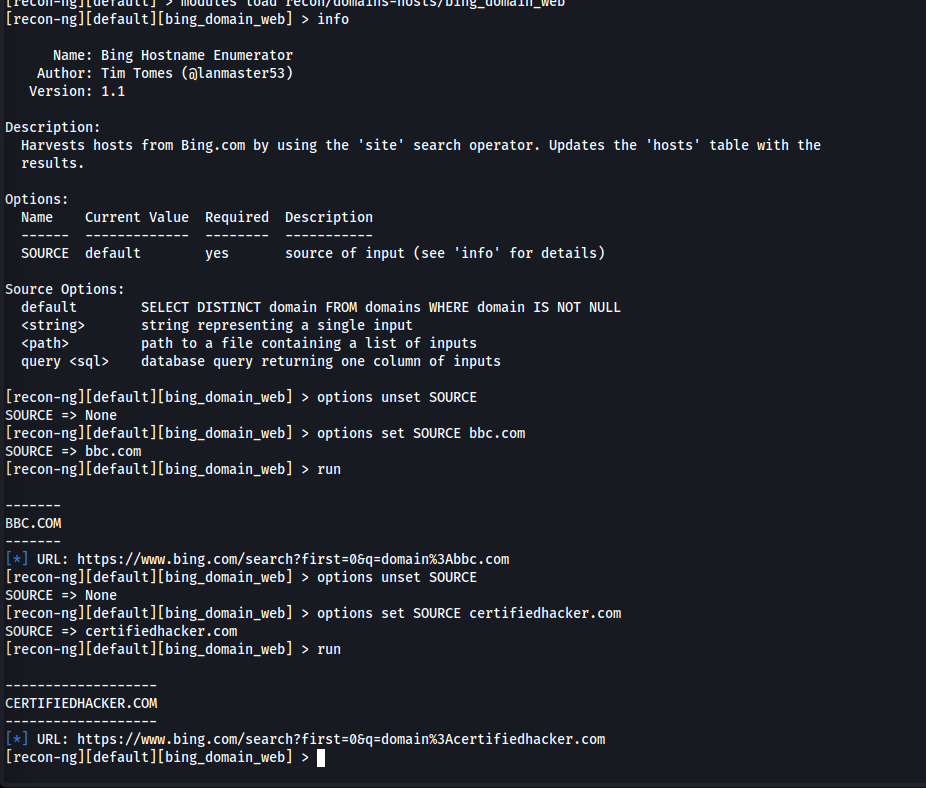






Now, changing modules:



  
Since I don’t have the API key, thus no major urls obtained.

Now, using google related modules:

