EC-Council

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

NOTICE TO THE READER

Table of Contents

Footprinting and Reconnaissance

Module 02

Footprinting and Reconnaissance

Footprinting refers to collecting as much information as possible regarding a target network from publicly accessible sources.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Reconnaissance refers to collecting information about a target, which is the first step in any attack on a system. It has its roots in military operations, where the term refers to the mission of collecting information about an enemy. Reconnaissance helps attackers narrow down the scope of their efforts and aids in the selection of weapons of attack. Attackers use the gathered information to create a blueprint, or "footprint," of the organization, which helps them select the most effective strategy to compromise the system and network security.

Similarly, the security assessment of a system or network starts with the reconnaissance and footprinting of the target. Ethical hackers and penetration (pen) testers must collect enough information about the target of the evaluation before initiating assessments. Ethical hackers and pen testers should simulate all the steps that an attacker usually follows to obtain a fair idea of the security posture of the target organization.

In this scenario, you work as an ethical hacker with a large organization. Your organization is alarmed at the news stories concerning new attack vectors plaguing large organizations around the world. Furthermore, your organization was the target of a major security breach in the past where the personal data of several of its customers were exposed to social networking sites.

You have been asked by senior managers to perform a proactive security assessment of the company. Before you can start any assessment, you should discuss and define the scope with management; the scope of the assessment identifies the systems, network, policies and procedures, human resources, and any other component of the system that requires security evaluation. You should also agree with management on rules of engagement (RoE)—the "do's and don'ts" of assessment. Once you have the necessary approvals to perform ethical hacking, you should start gathering information about the target organization.

Once you methodologically begin the footprinting process, you will obtain a blueprint of the security profile of the target organization. The term "blueprint" refers to the unique system profile of the target organization as the result of footprinting.

The labs in this module will give you real-time experience in collecting a variety of information about the target organization from various open or publicly accessible sources.

Lab Objectives

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- **Organization Information**

  Employee details, partner details, weblinks, web technologies, patents, trademarks, etc.

- **Network Information**

  Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information

- **System Information**

  Operating systems, web server OSes, user accounts and passwords, etc.

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 200 Minutes

Overview of Footprinting

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Footprinting refers to the process of collecting information about a target network and its environment, which helps in evaluating the security posture of the target organization's IT infrastructure. It also helps to identify the level of risk associated with the organization's publicly accessible information.

Footprinting can be categorized into passive footprinting and active footprinting:

- **Passive Footprinting**: Involves gathering information without direct interaction. This type of footprinting is principally useful when there is a requirement that the information-gathering activities are not to be detected by the target.
- **Active Footprinting**: Involves gathering information with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Recommended labs that will assist you in learning various footprinting techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Footprinting Through Search Engines	√	√	√
	1.1 Gather Information using Advanced Google Hacking Techniques	√		√
	1.2 Gather Information from Video Search Engines		√	√
	1.3 Gather Information from FTP Search Engines		√	√
	1.4 Gather Information from IoT Search Engines		√	√
2	Perform Footprinting Through Web Services	√	√	√
	2.1 Find the Company's Domains and Sub-domains using Netcraft	√		√
	2.2 Gather Personal Information using PeekYou Online People Search Service		√	√
	2.3 Gather an Email List using theHarvester		√	√
	2.4 Gather Information using Deep and Dark Web Searching		√	√
	2.5 Determine Target OS Through Passive Footprinting		√	√
3	Perform Footprinting Through Social Networking Sites	√	√	√
	3.1 Gather Employees' Information from LinkedIn using theHarvester	√		√
	3.2 Gather Personal Information from Various Social Networking Sites using Sherlock		√	√
	3.3 Gather Information using Followerwonk		√	√
4	Perform Website Footprinting	√	√	√
	4.1 Gather Information About a Target Website using Ping Command Line Utility	√		√

	4.2 Gather Information About a Target Website using Website Informer		√	√
	4.3 Extract a Company's Data using Web Data Extractor		√	√
	4.4 Mirror a Target Website using HTTrack Web Site Copier	√		√
	4.5 Gather a Wordlist from the Target Website using CeWL		√	√
5	Perform Email Footprinting	√		√
	5.1 Gather Information About a Target by Tracing Emails using eMailTrackerPro	√		√
6	Perform Whois Footprinting	√		√
	6.1 Perform Whois Lookup using DomainTools	√		√
7	Perform DNS Footprinting	√	√	√
	7.1 Gather DNS Information using nslookup Command Line Utility and Online Tool	√		√
	7.2 Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon		√	√
8	Perform Network Footprinting	√	√	√
	8.1 Locate the Network Range		√	√
	8.2 Perform Network Tracerouting in Windows and Linux Machines	√		√
	8.3 Perform Advanced Network Route Tracing using Path Analyzer Pro		√	
9	Perform Footprinting using Various Footprinting Tools	√	√	√
	9.1 Footprinting a Target using Recon-ng	√		√
	9.2 Footprinting a Target using Maltego		√	√
	9.3 Footprinting a Target using OSRFramework		√	√
	9.4 Footprinting a Target using FOCA		√	√
	9.5 Footprinting a Target using BillCipher		√	√
	9.6 Footprinting a Target using OSINT Framework		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document all the results discovered in the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Perform Footprinting Through Search Engines

Search engines are the main information sources to extract critical information about a target organization from the Internet.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target organization by performing footprinting using search engines; you can perform advanced image searches, reverse image searches, advanced video searches, etc. Through the effective use of search engines, you can extract critical information about a target organization such as technology platforms, employee details, login pages, intranet portals, contact details, etc., which will help you in performing social engineering and other types of advanced system attacks.

Lab Objectives

- Gather information using advanced Google hacking techniques
- Gather information from video search engines
- Gather information from FTP search engines
- Gather information from IoT search engines

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

Lab Duration

Time: 20 Minutes

Overview of Search Engines

Search engines use crawlers, automated software that continuously scans active websites, and add the retrieved results to the search engine index, which is further stored in a huge database. When a user queries a search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed based on their relevance. Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

Lab Tasks

TASK 1 — Gather Information using Advanced Google Hacking Techniques

Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation

Note: Here, we will consider **EC-Council** as a target organization.

1. Turn on **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

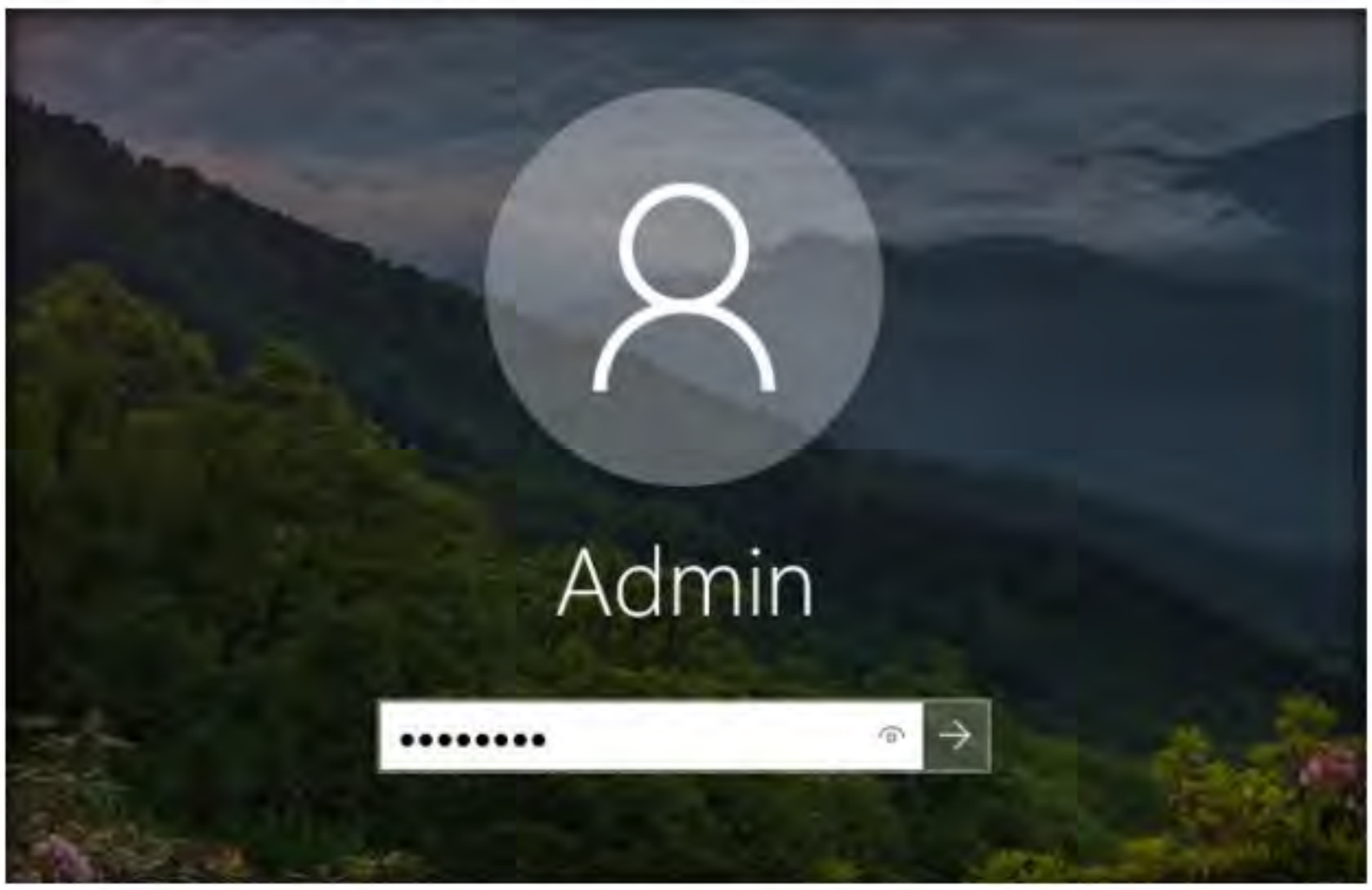


Figure 1.1.1: Login window

3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.google.com**.

Note:

- If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.

- If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.

Figure 1.1.2: Default browser pop-up window

4. Once the **Google** search engine appears, you should see a search bar.

Note: If any pop-up window appears at the top-right corner, click **No, thanks**

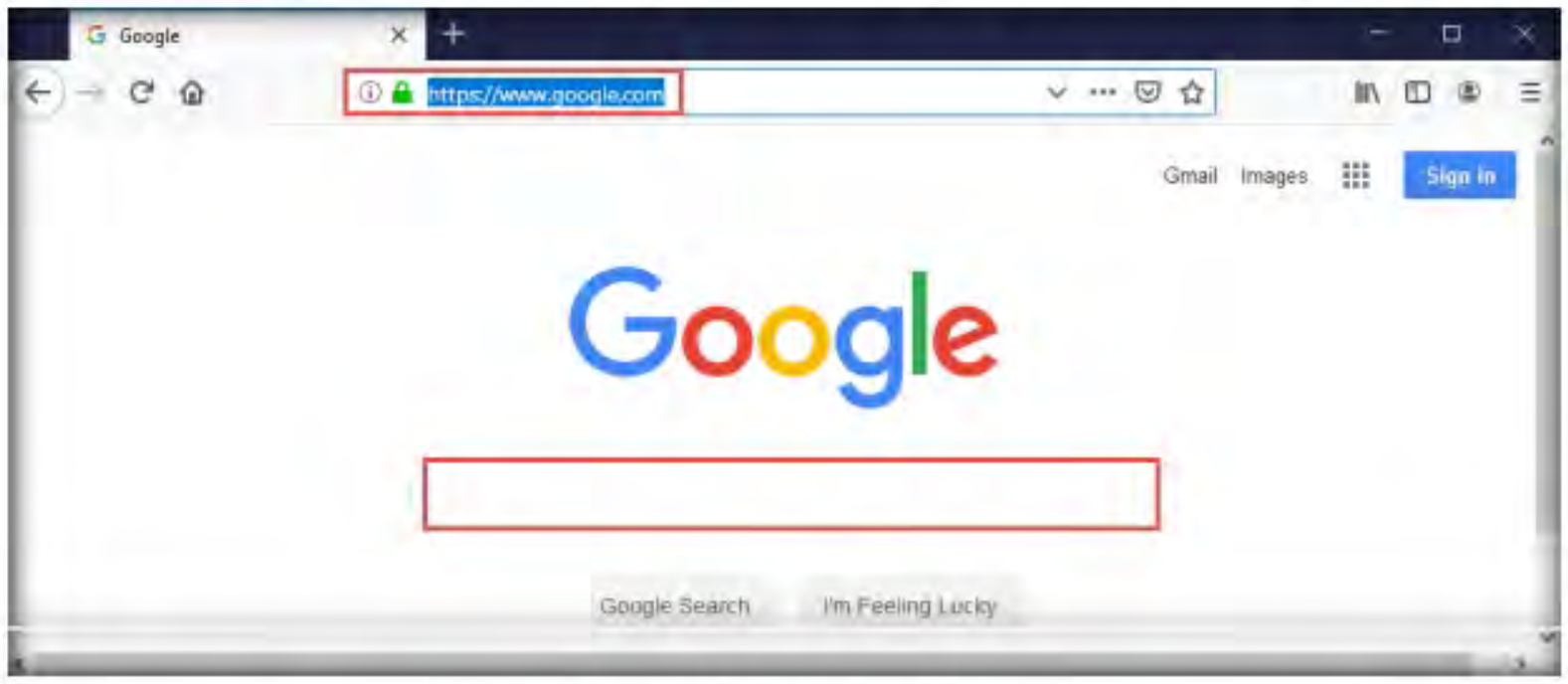


Figure 1.1.3: Google Search bar

TASK 1.1

Perform Advanced Google Hacking for Password Files

5. Type **intitle:password site:www.eccouncil.org** and press **Enter**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **www.eccouncil.org** website that contain the term **password** in the title. An example is shown in the screenshot below.

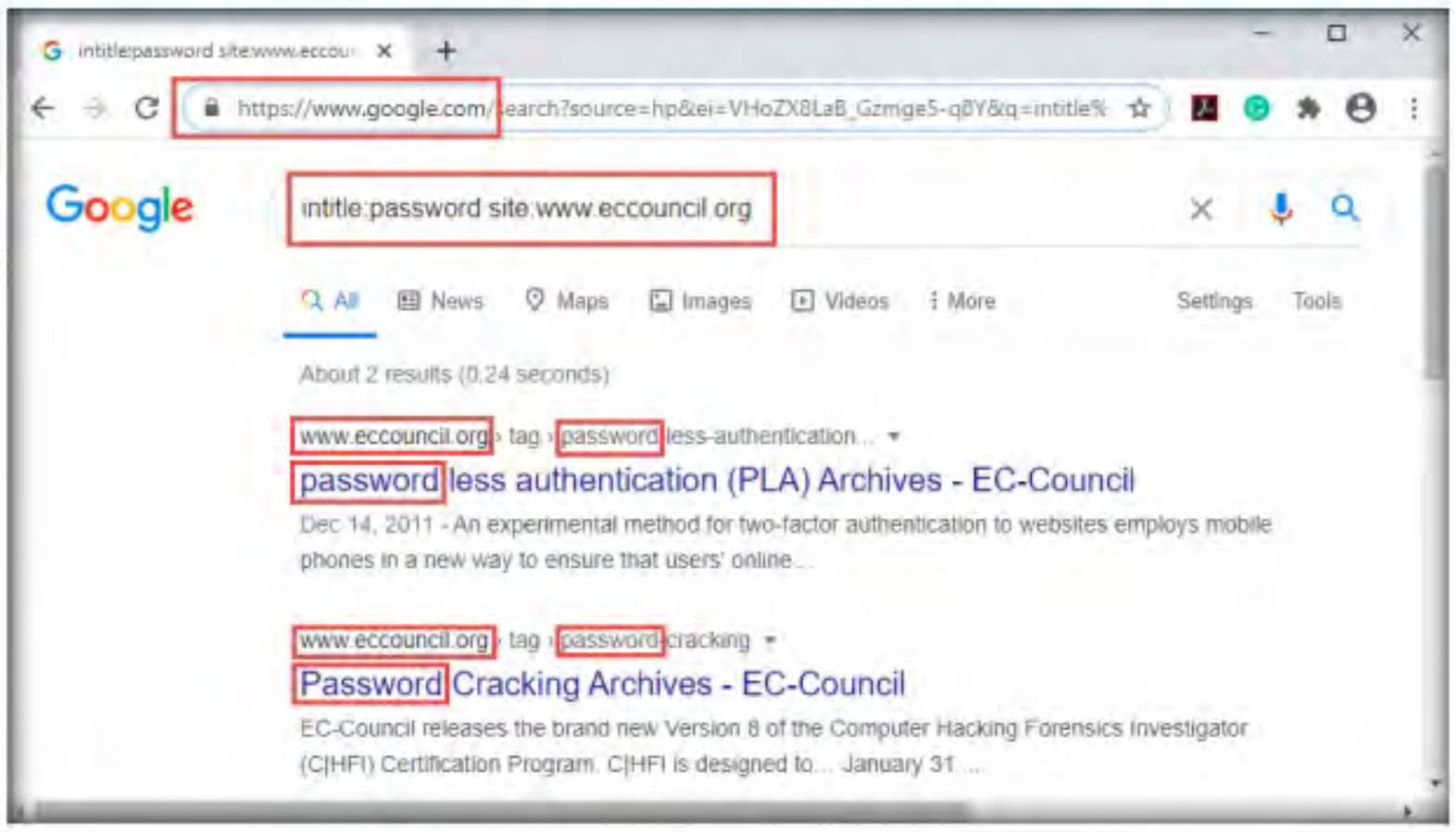


Figure 1.1.4: Search result with advanced google operators

TASK 1.2

Perform Advanced Google Hacking for PDF Files

6. Now, navigate back to **https://www.google.com**. In the search bar, type the command **EC-Council filetype:pdf** and press **Enter** to search your results based on the file extension.

Note: Here, the file type pdf is searched for the target organization EC-Council.

7. Now, click on any link from the results (here, first link) to view the pdf file.

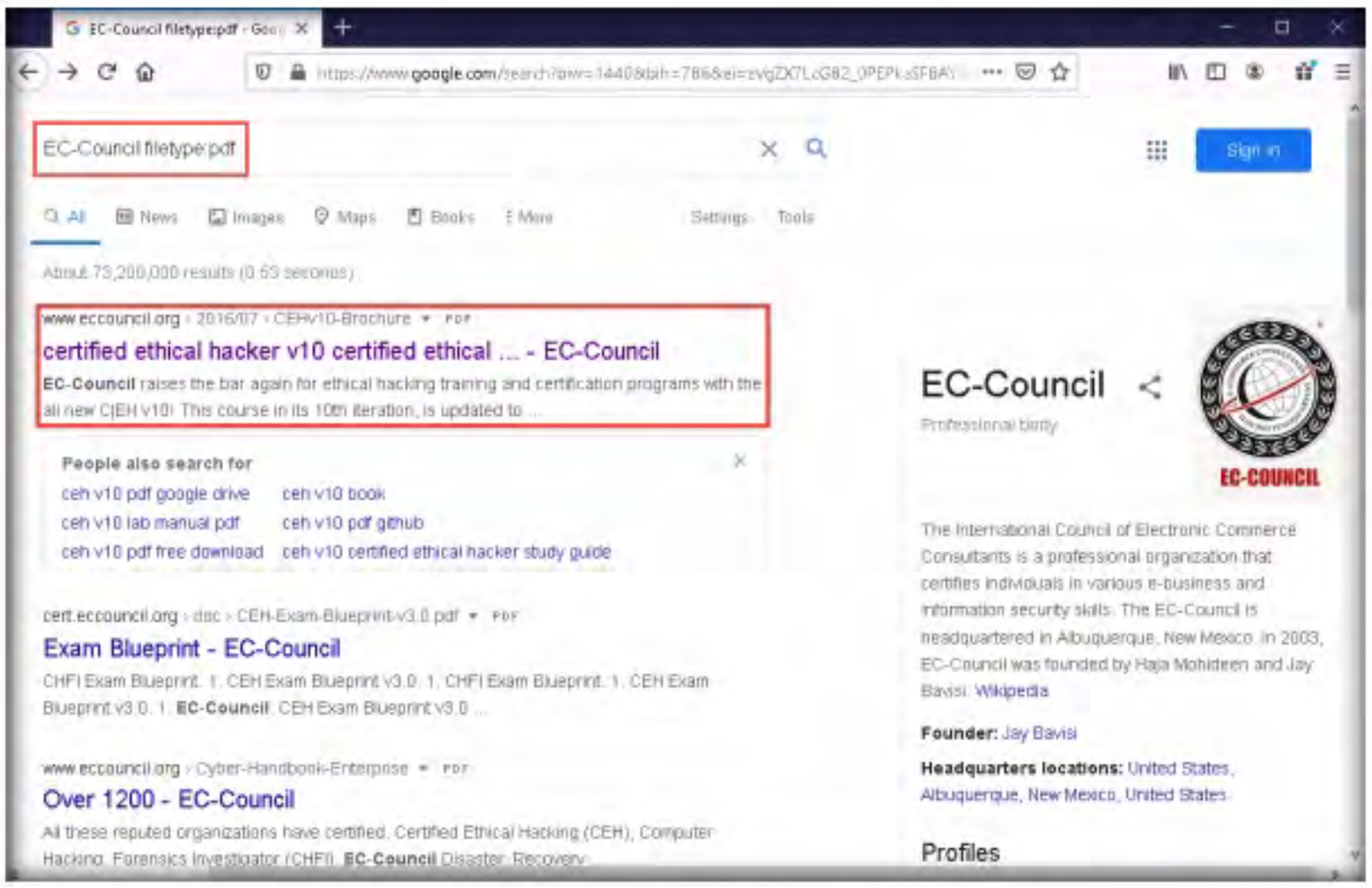


Figure 1.1.5: Results showing various pdf files

8. The page appears displaying the PDF file, as shown in the screenshot.

Figure 1.1.6: PDF file

9. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.

   - **cache**: This operator allows you to view cached version of the web page.

     [cache: www.google.com]- Query returns the cached version of the website www.google.com

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

     [allinurl: google career]—Query returns only pages containing the words "google" and "career" in the URL

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

     [inurl: copy site:www.google.com]–Query returns only pages in Google site in which the URL has the word "copy"

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

     [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title

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

     [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 pages containing all query terms specified in the anchor text on links to the page.

     [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"

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

     [link:www.googleguide.com]—Finds pages that point to Google Guide's home page

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

     [related:www.certifiedhacker.com]—Query provides the Google search engine results page with websites similar to certifiedhacker.com

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

  [info:gothotel.com]—Query provides information about the national hotel directory GotHotel.com home page

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

  [location: 4 seasons restaurant]—Query give you results based around the term 4 seasons restaurant

10. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
11. Close all open windows and document all the acquired information.

TASK 2 Gather Information from Video Search Engines

Here, we will perform an advanced video search and reverse image search using the YouTube search engine and Youtube DataViewer video analysis tool.

Video search engines are Internet-based search engines that crawl the web looking for video content. These search engines either provide the functionality of uploading and hosting the video content on their own web servers or they can parse the video content, which is hosted externally.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.youtube.com/**.
2. In the search bar, search for your target organization (here, **ec-council**). You will see all the latest videos uploaded by the target organization.

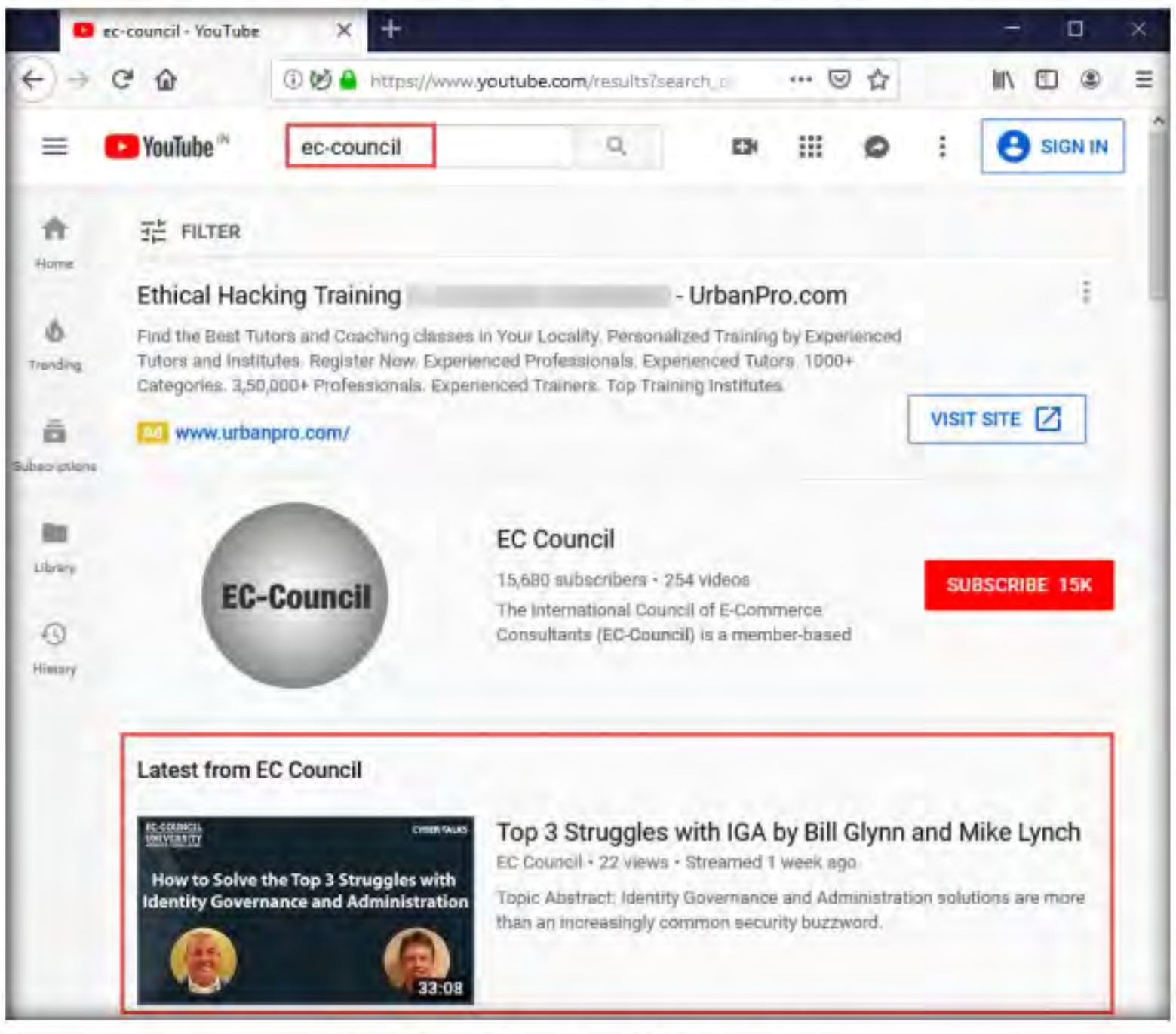


Figure 1.2.1: YouTube search result for ec-council query

3. Select any video of your choice, right-click on the video title, and click **Copy Link Location**. (here, **Top 3 Struggles with IGA by Bill Glynn and Mike Lynch**)

Figure 1.2.2: Copy Link Location option

4. After the video link is copied, open another browser tab in **Mozilla Firefox**, and then navigate to **https://citizenevidence.amnestyusa.org/**. In the **Enter YouTube URL** search box, paste the copied YouTube video link and click **Go**.

Figure 1.2.3: Paste copied YouTube Link

5. In the search result, you can observe the details related to the video such as **Topic Abstract**, **Video ID**, **Upload Date**, **Upload Time**, etc. You can also find **Thumbnails** to perform a reverse image search. Click on the **reverse image search** option for any thumbnail.

Figure 1.2.4: Youtube DataViewer Result

6. A new tab in **Google** opens, and the results for the reverse image search are displayed.

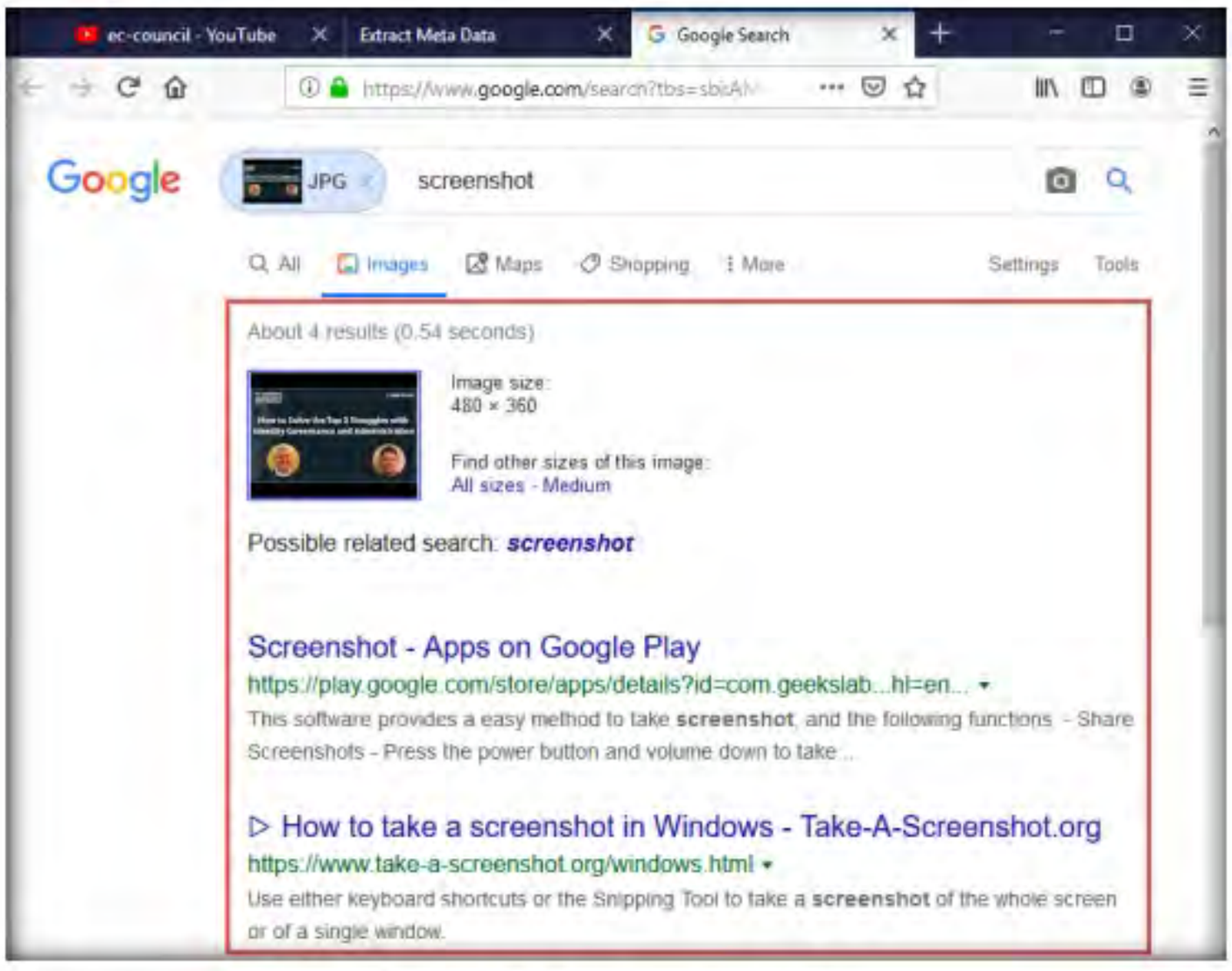


Figure 1.2.5: Reverse image search result

You can use other video search engines such as **Google videos** (https://video.google.com), **Yahoo videos** (https://video.search.yahoo.com), etc.; video analysis tools such as **EZGif** (https://ezgif.com), **VideoReverser.com**, etc.; and reverse image search tools such as **TinEye Reverse Image Search** (https://tineye.com), **Yahoo Image Search** (https://images.search.yahoo.com), etc. to gather crucial information about the target organization

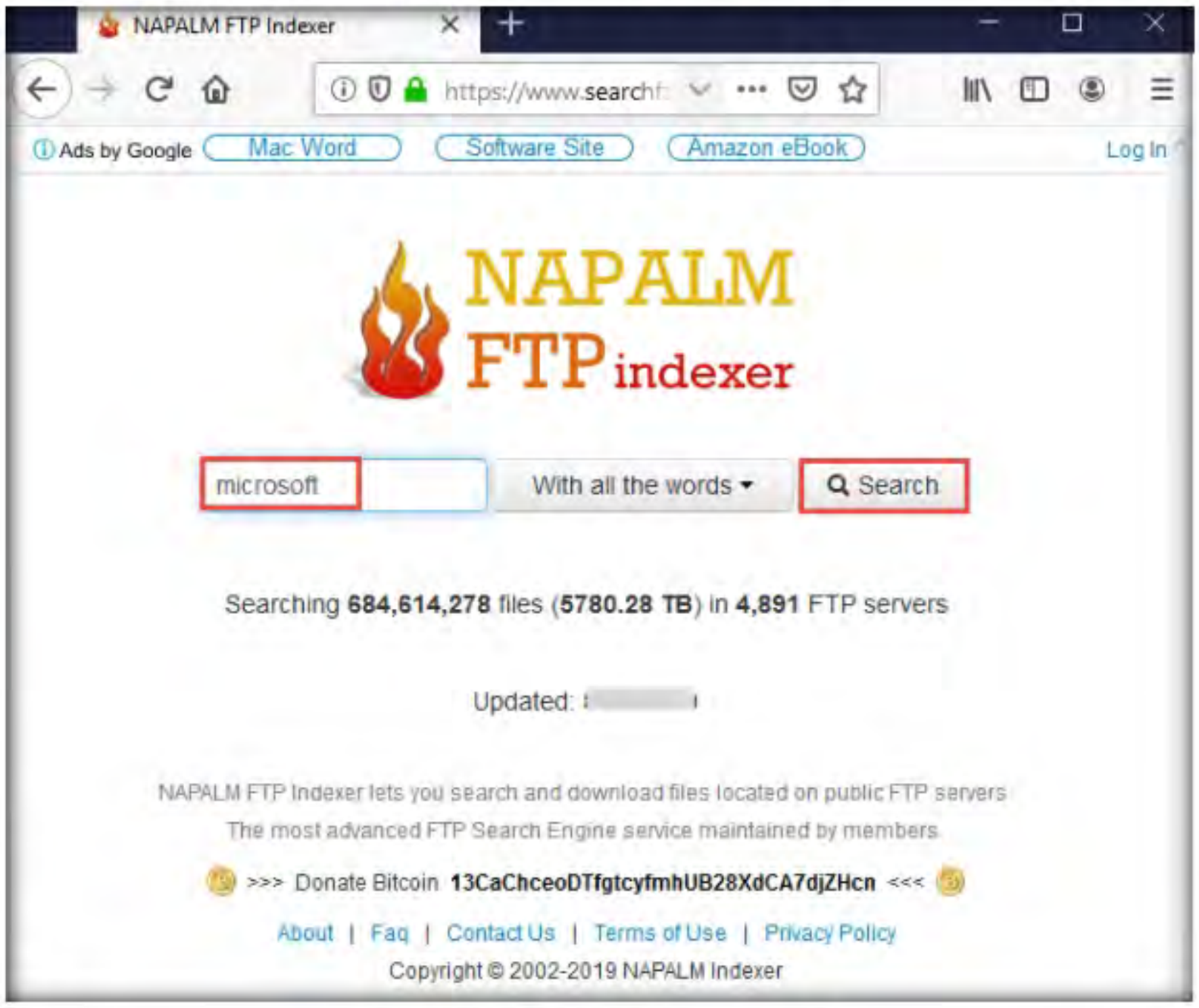
7. This concludes the demonstration of gathering information from the advanced video search and reverse image search using the YouTube search engine and Youtube DataViewer video analysis tool.
8. Close all open windows and document all acquired information.

TASK 3 Gather Information from FTP Search Engines

Here, we will use the NAPALM FTP indexer FTP search engine to extract critical FTP information about the target organization.

File Transfer Protocol (FTP) search engines are used to search for files located on the FTP servers; these files may hold valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to keep large file archives and other software that are shared among their employees.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.searchftps.net/**.
2. In the search bar, type **microsoft** and click **Search**.



FTP search engines provide information about critical files and directories, including valuable information such as business strategies, tax documents, employee's personal records, financial records, licensed software, and other confidential information

Figure 1.3.1: NAPALM FTP indexer search result

3. You will get the search results with the details of the FTP in the target organization, as shown in the screenshot.

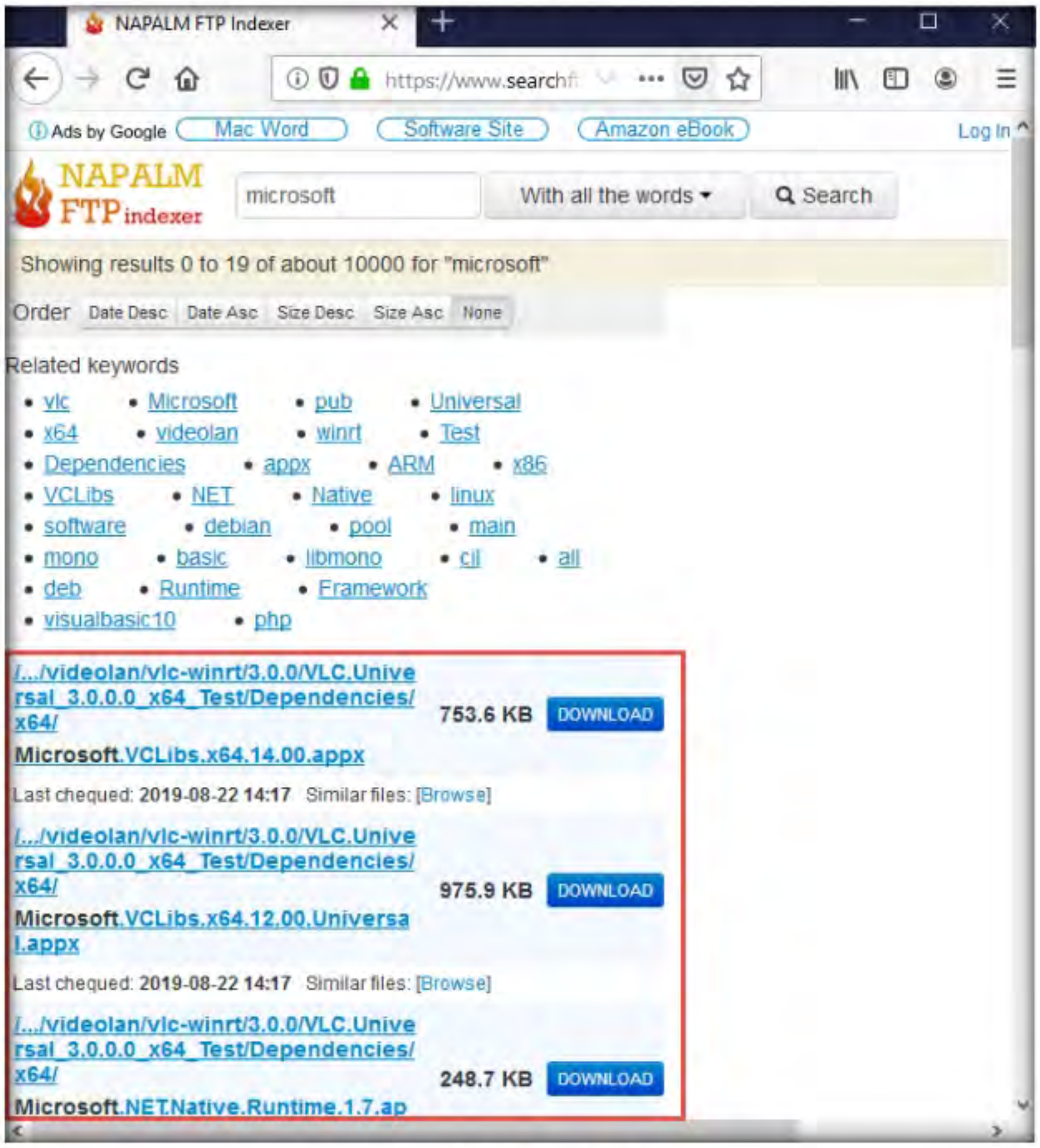


Figure 1.3.2: FTP search result

You can also use FTP search engines such as **Global FTP Search Engine** (https://globalfilesearch.com), **FreewareWeb FTP File Search** (http://www.freewareweb.com), etc. to gather crucial FTP information about the target organization.

4. This concludes the demonstration of gathering information from the FTP search engine.
5. Close all open windows and document all the acquired information.

TASK 4 Gather Information from IoT Search Engines

Here, we will search for information about any vulnerable IoT device in the target organization using the Shodan IoT search engine.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.shodan.io/**.
2. In the search bar, type **amazon** and press **Enter**. You will obtain the search results with the details of all the vulnerable IoT devices related to amazon in various countries, as shown in the screenshot.

IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances, CCTV cameras, etc.

Note: The screenshot might differ in your lab environment.

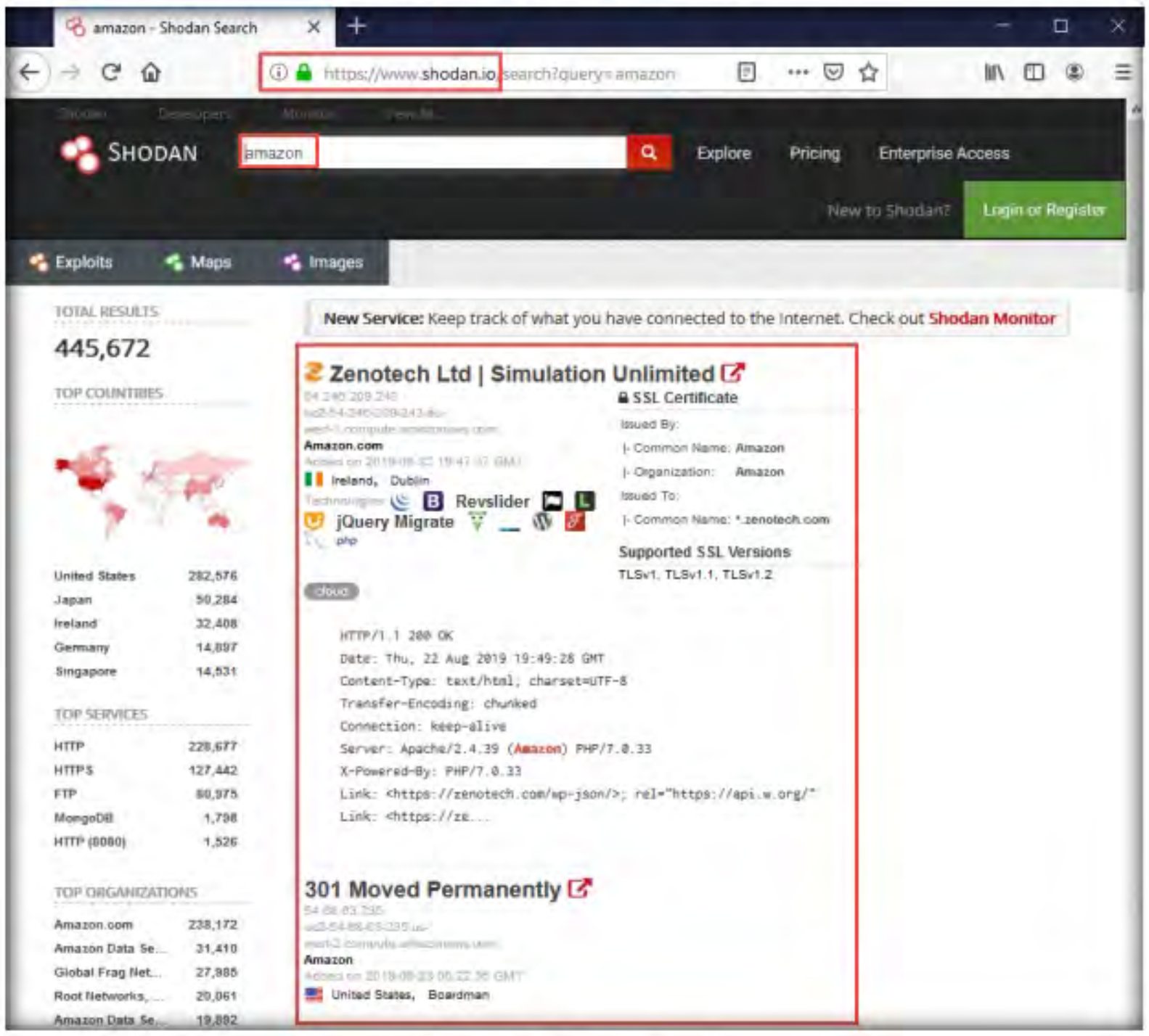


Figure 1.4.1: Shodan search result

3. This concludes the demonstration of gathering vulnerable IoT information using the Shodan search engine.
4. Close all open windows and document all the acquired information.
5. Turn off the **Windows 10** virtual machine.

You can also use **Censys** (https://censys.io), **Thingful** (https://www.thingful.net), etc., which are IoT search engines, to gather information such as manufacturer details, geographical location, IP address, hostname, open ports, etc.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Perform Footprinting Through Web Services

Web services are online applications or sources that provide a variety of publicly accessible information related to the target organization.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

As a professional ethical hacker or pen tester, you should be able to extract a variety of information about your target organization from web services. By doing so, you can extract critical information such as a target organization's domains, sub-domains, operating systems, geographic locations, employee details, emails, financial information, infrastructure details, hidden web pages and content, etc.

Using this information, you can build a hacking strategy to break into the target organization's network and can carry out other types of advanced system attacks.

Lab Objectives

- Find the company's domains and sub-domains using Netcraft
- Gather personal information using PeekYou online people search service
- Gather an email list using theHarvester
- Gather information using deep and dark web searching
- Determine target OS through passive footprinting

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

- Tor Browser located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Deep and Dark Web Footprinting Tools\Tor Browser**
- You can also download the latest version of Tor Browser from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 25 Minutes

Overview of Web Services

Web services such as social networking sites, people search services, alerting services, financial services, and job sites, provide information about a target organization; for example, infrastructure details, physical location, employee details, etc. Moreover, groups, forums, and blogs may provide sensitive information about a target organization such as public network information, system information, and personal information. Internet archives may provide sensitive information that has been removed from the World Wide Web (WWW).

Lab Tasks

TASK 1

Find the Company's Domains and Sub-domains using Netcraft

Here, we will extract the company's domains and sub-domains using the Netcraft web service.

Domains and sub-domains are part of critical network infrastructure for any organization. A company's top-level domains (TLDs) and sub-domains can provide much useful information such as organizational history, services and products, and contact information. A public website is designed to show the presence of an organization on the Internet and is available for free access.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open a web browser (here, **Mozilla Firefox**), type the URL **https://www.netcraft.com** in the address bar, and press **Enter**. The Netcraft website appears, as shown in the screenshot.

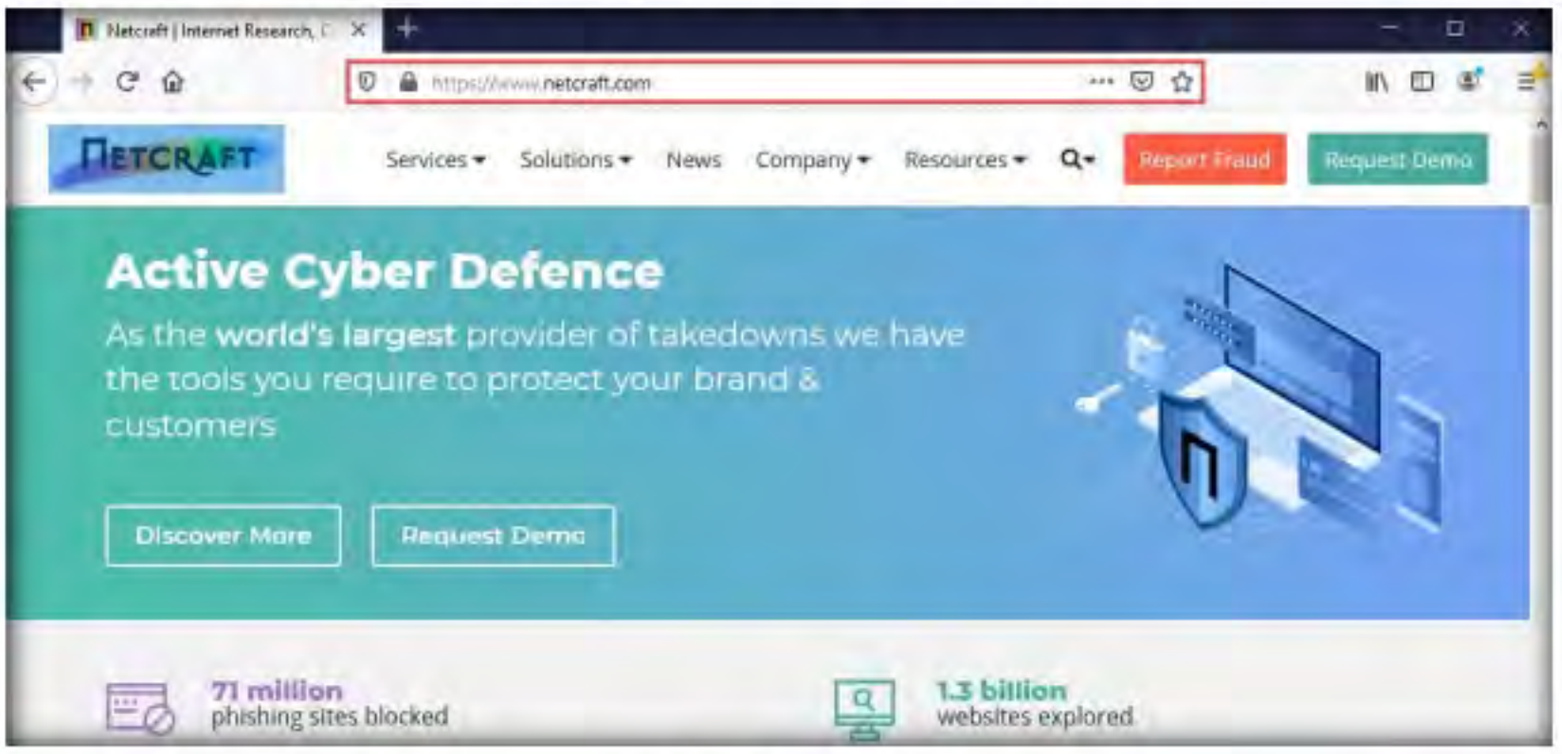


Figure 2.1.1: Netcraft website

4. Click the **Resources** tab from the menu bar and click on the **Site Report** link under the **Tools** section.

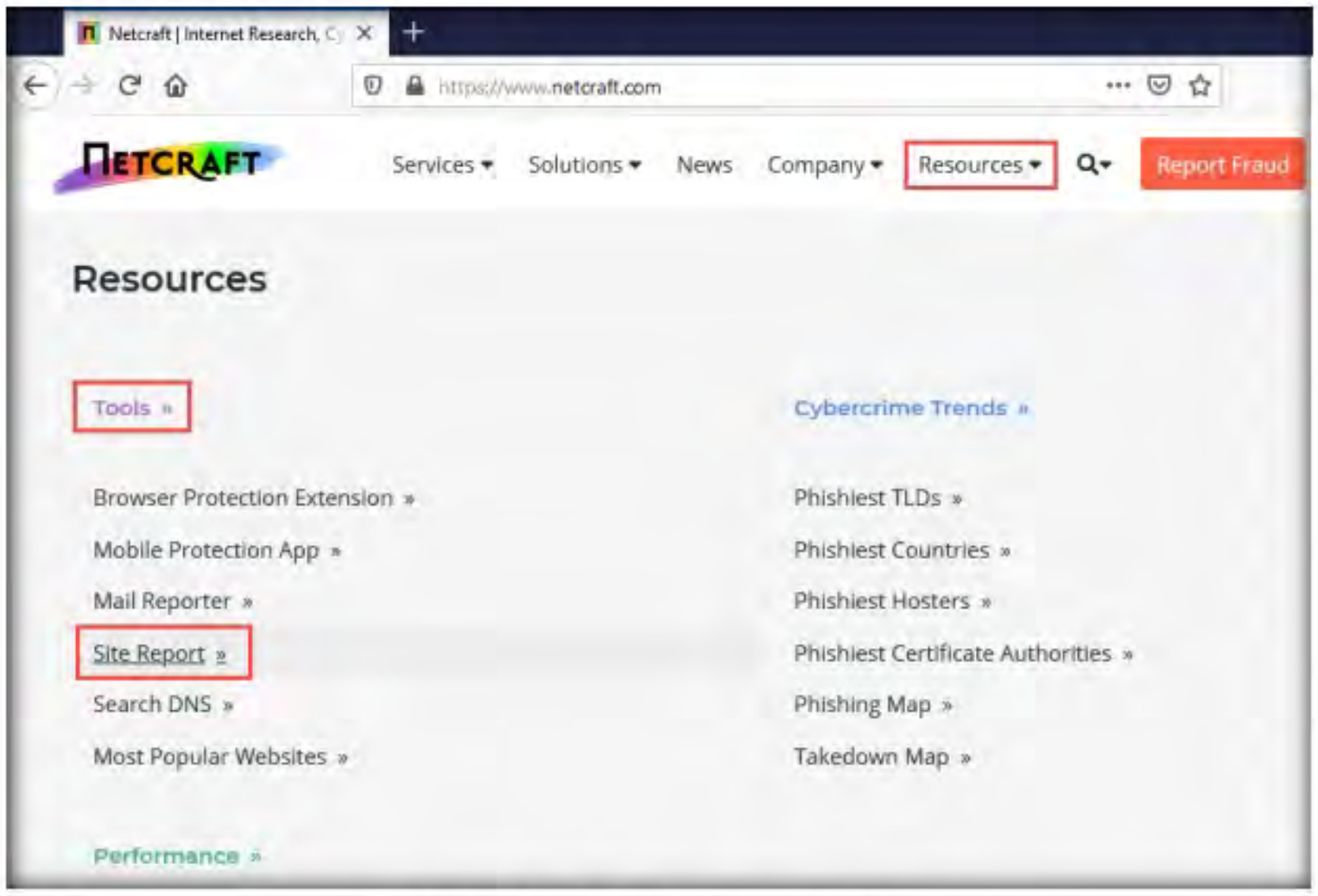


Figure 2.1.2: Netcraft website Resources tab options

5. The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.eccouncil.org**) in the text field, and then click the **Lookup** button, as shown in the screenshot.

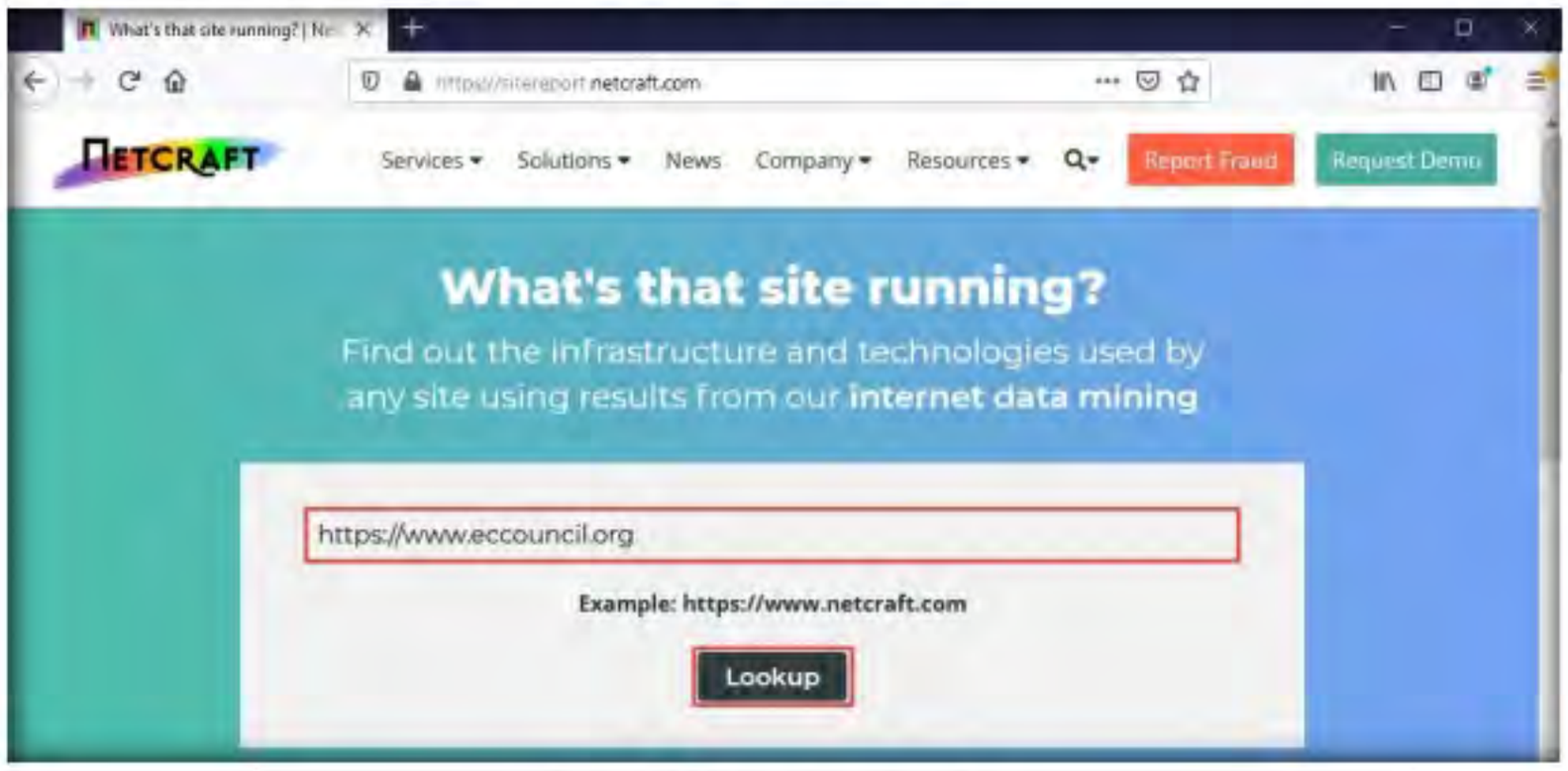


Figure 2.1.3: Enter the target website

6. The **Site report for https://www.eccouncil.org** page appears, containing information related to **Background**, **Network**, **Hosting History**, etc., as shown in the screenshot.

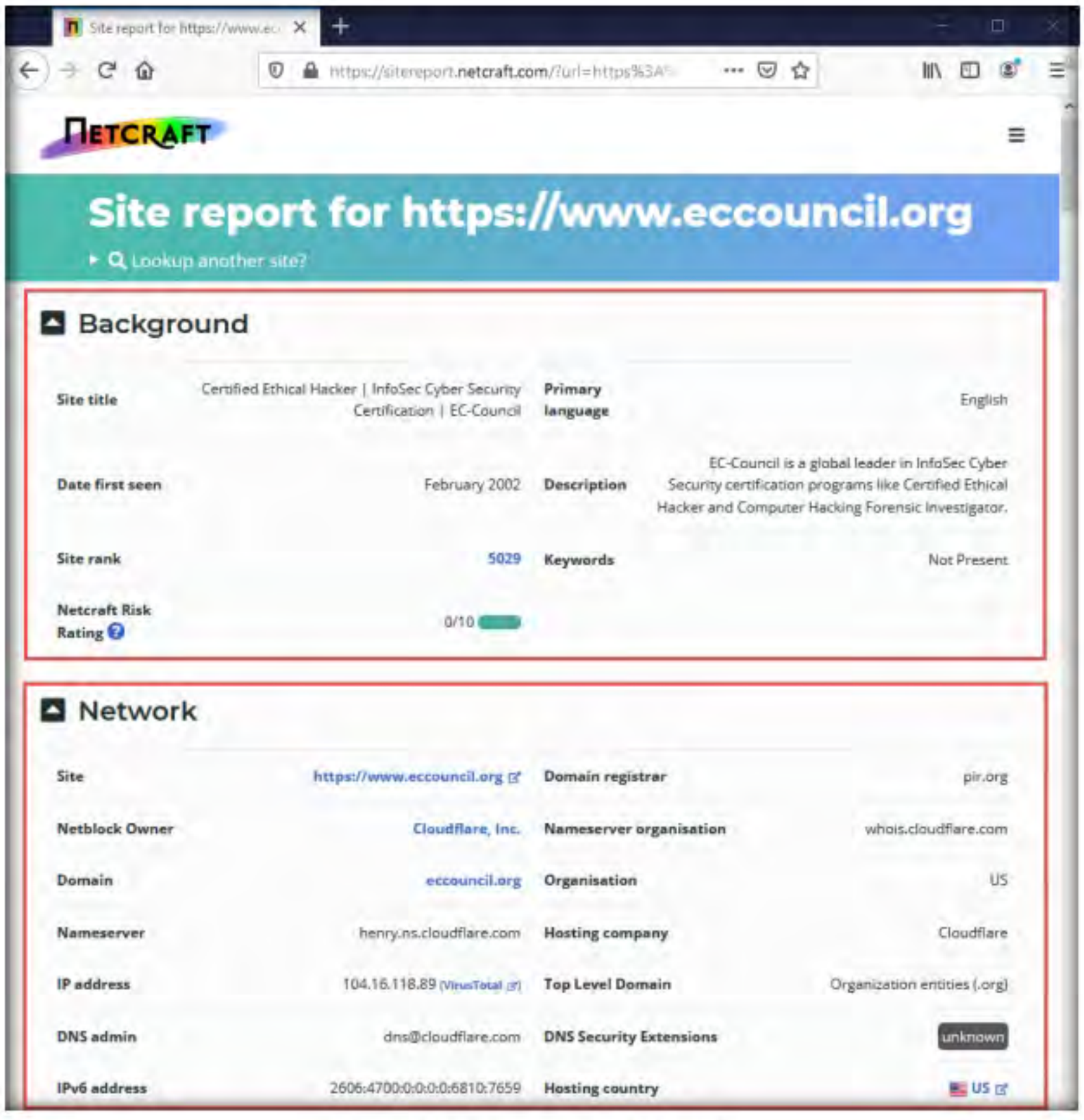


Figure 2.1.4: Report generated by Netcraft

7. In the **Network** section, click on the website link (here, **eccouncil.org**) in the **Domain** field to view the subdomains

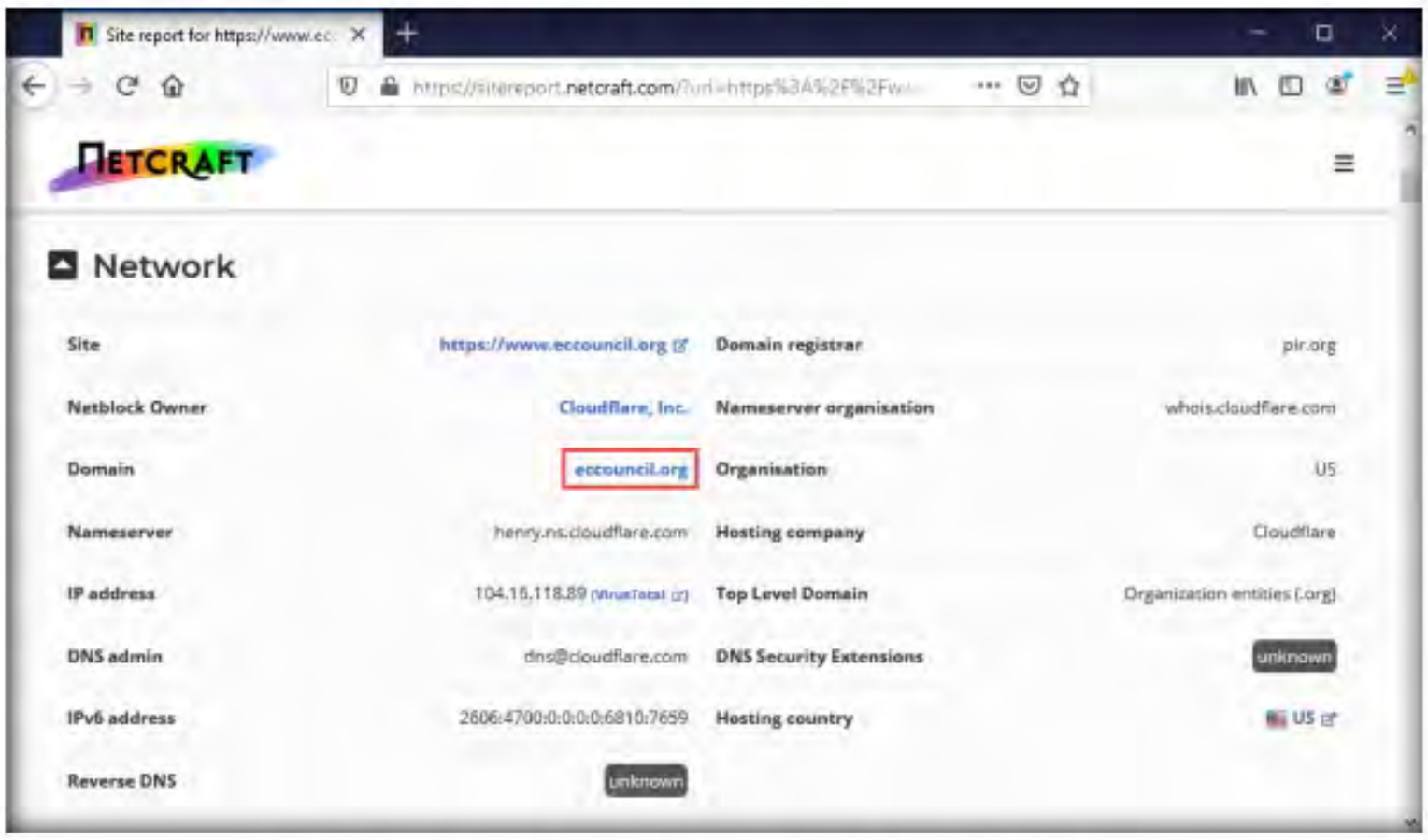


Figure 2.1.5: Report generated by Netcraft showing domain information

8. The result will display subdomains of the target website along with netblock and operating system information, as shown in the screenshot.

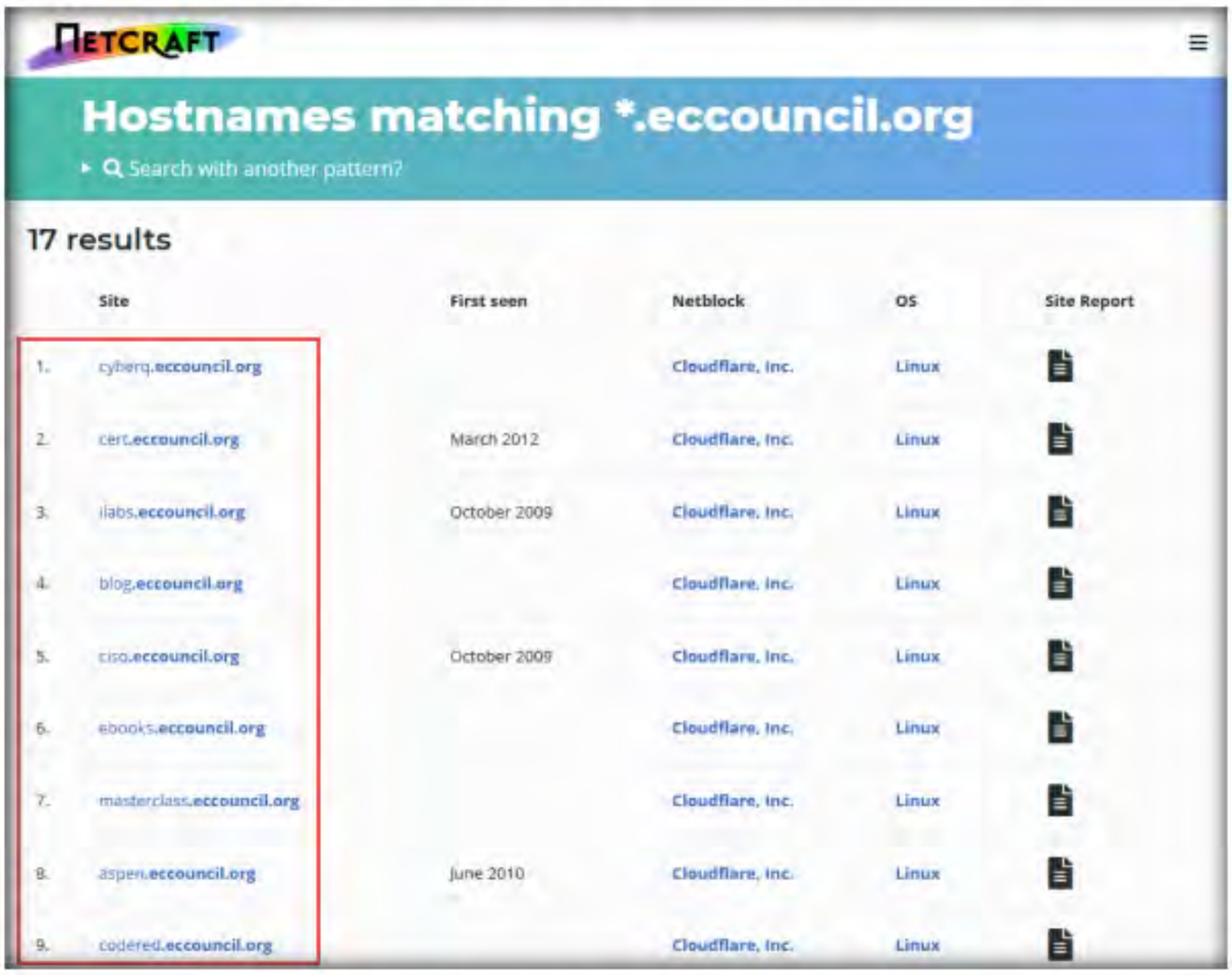


Figure 2.1.6: Report generated by Netcraft showing subdomains

You can also use tools such as **Sublist3r** (https://github.com), **Pentest-Tools Find Subdomains** (https://pentest-tools.com), etc. to identify the domains and sub-domains of any target website.

9. This concludes the demonstration of finding the company's domains and sub-domains using the Netcraft tool.
10. Close all open windows and document all the acquired information.

TASK 2

Gather Personal Information using PeekYou Online People Search Service

Here, we will gather information about a person from the target organization by performing people search using the PeekYou online people search service.

Online people search services, also called public record websites, are used by many individuals to find personal information about others; these services provide names, addresses, contact details, date of birth, photographs, videos, profession, details about family and friends, social networking profiles, property information, and optional background on criminal checks.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.peekyou.com**.
2. In the **First Name** and **Last Name** fields, type **Satya** and **Nadella**, respectively. In the **Location** drop-down box, select **Washington, DC**. Then, click the **Search** icon.

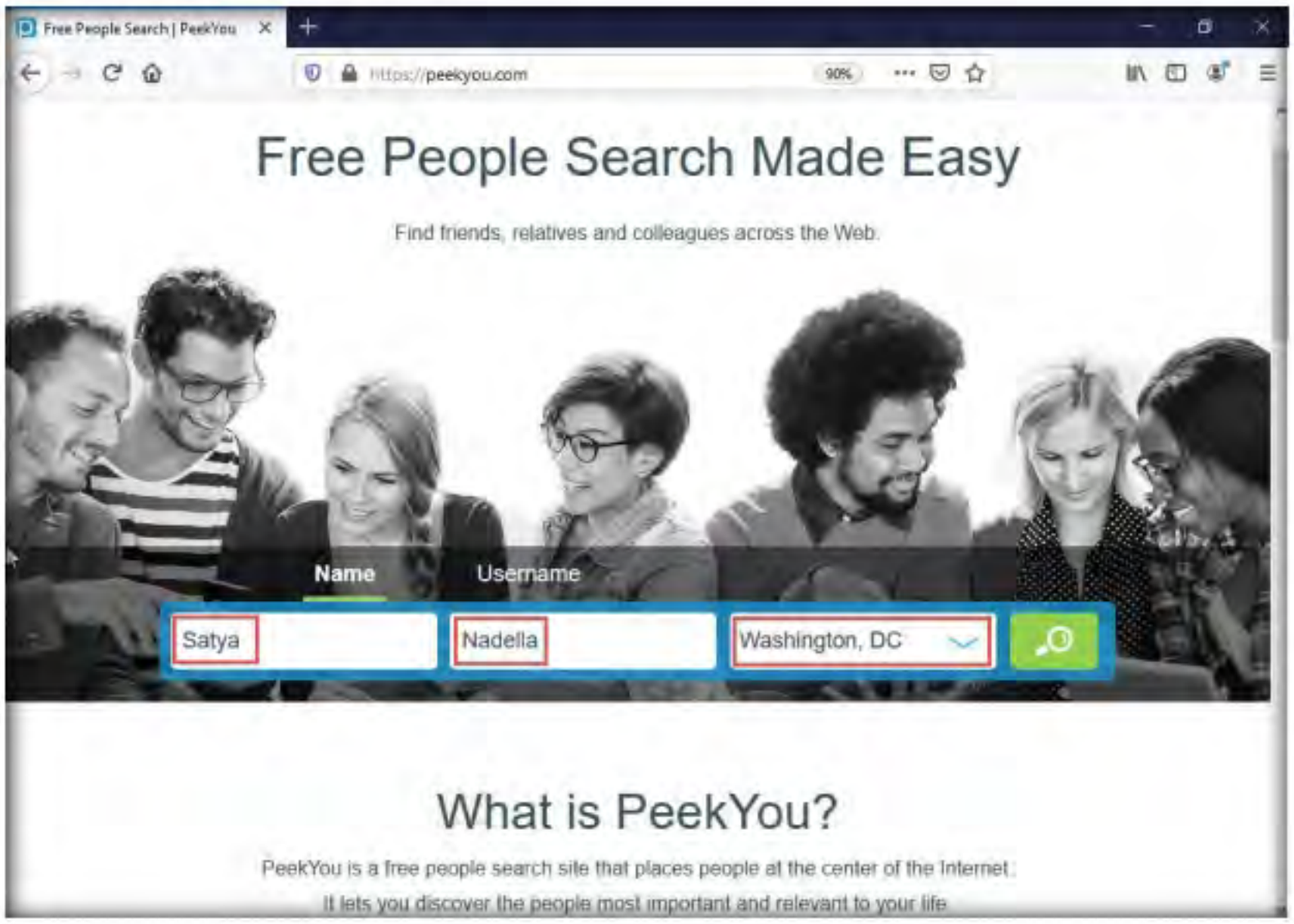


Figure 2.2.1: PeekYou Search Bar

3. The people search begins, and the best matches for the provided search parameters will be displayed.

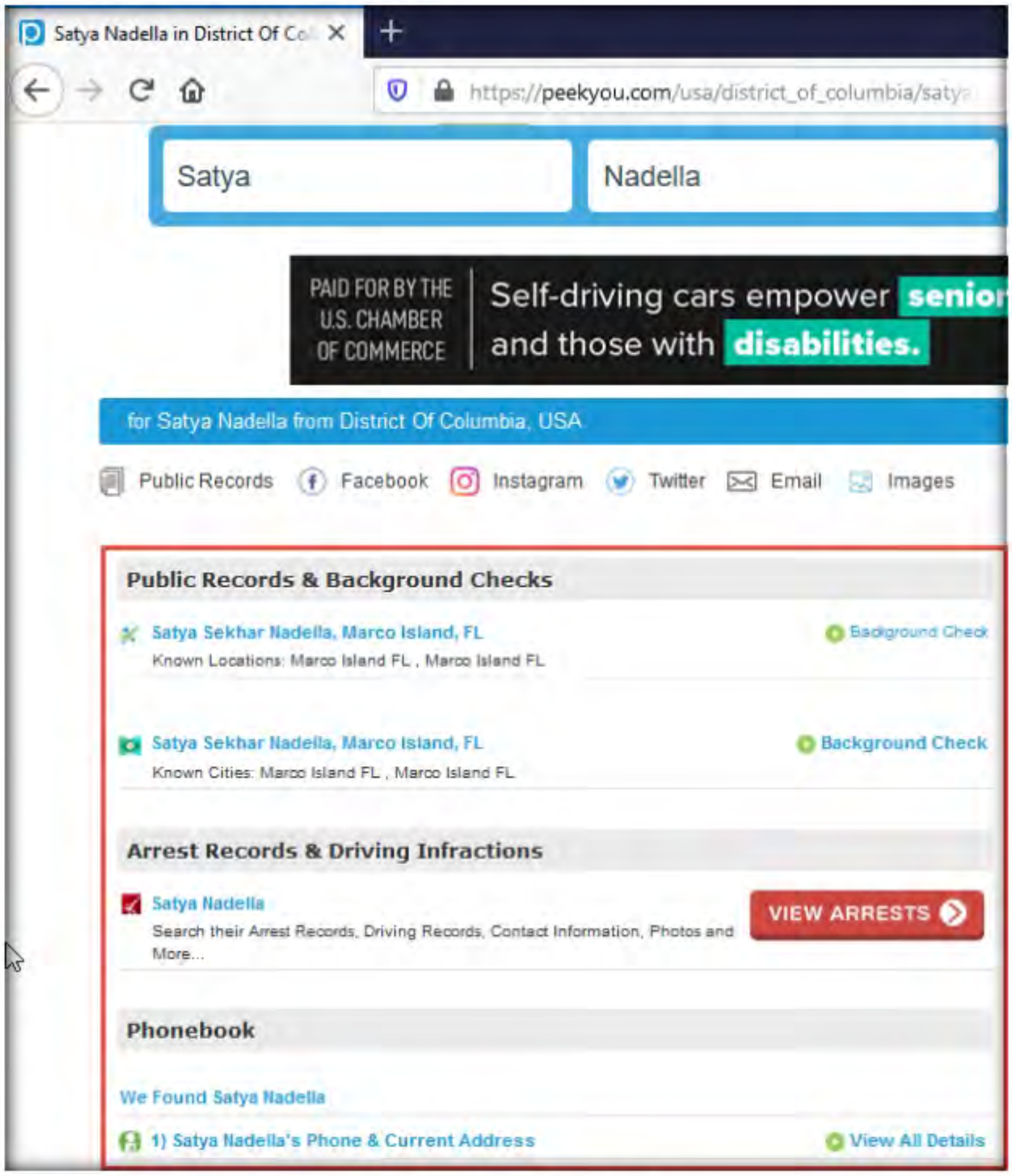


Figure 2.2.2: PeekYou Search Bar

4. You can further click on the appropriate result to view the detailed information about the target person to see a detailed information about the target person.

Note: After you click on any result, you will be redirected to a different website and it will take some time to load the information about the target.

5. Scroll down to view the entire information about the target person.

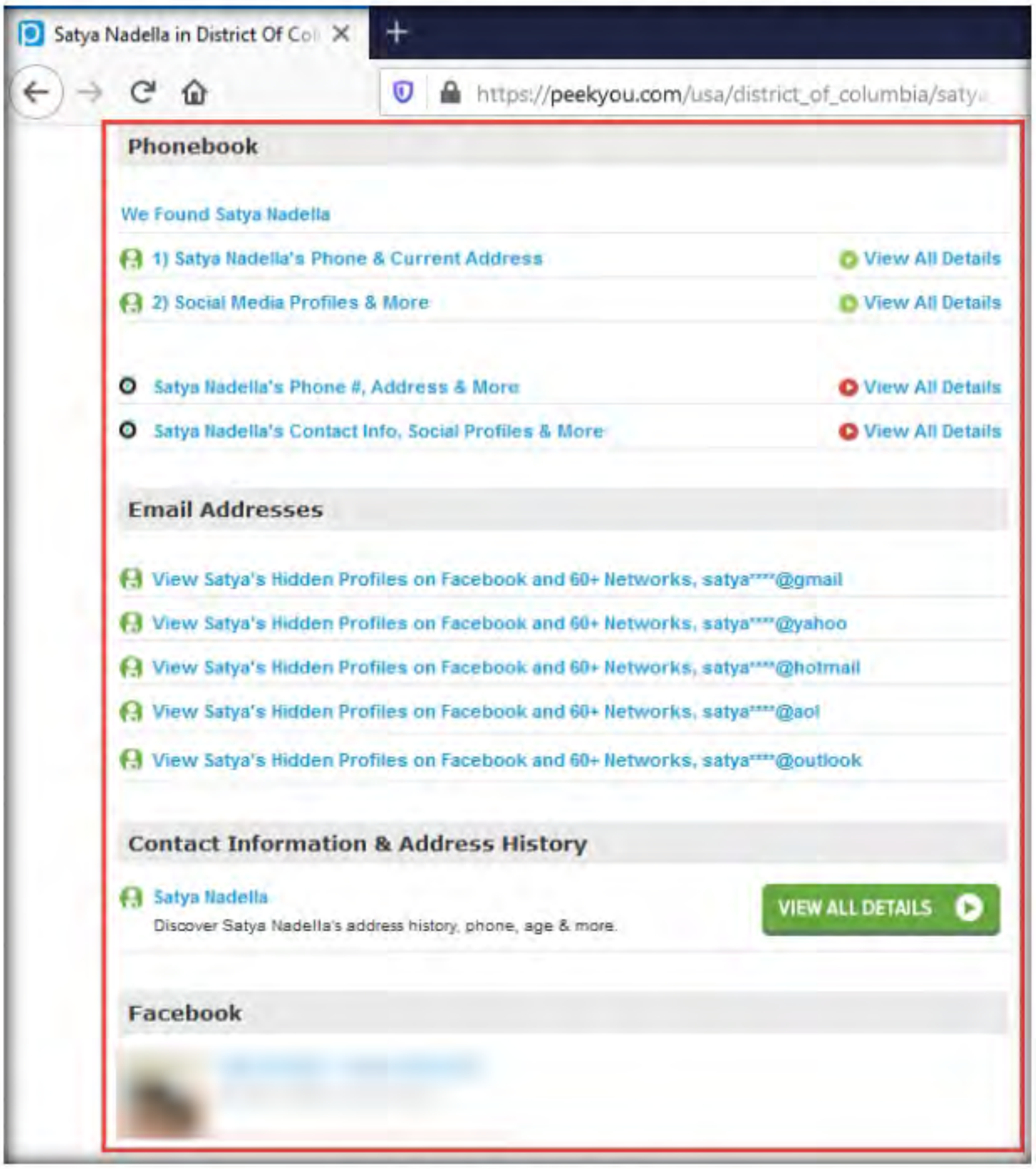


Figure 2.2.3: PeekYou Search result

You can also use **pipl** (https://pipl.com), **Intelius** (https://www.intelius.com), **BeenVerified** (https://www.beenverified.com), etc., which are people search services to gather personal information of key employees in the target organization

6. This concludes the demonstration of gathering personal information using the PeekYou online people search service.
7. Close all open windows and document all the acquired information.

TASK 3 Gather an Email List using theHarvester

Here, we will gather the list of email IDs related to a target organization using theHarvester tool.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

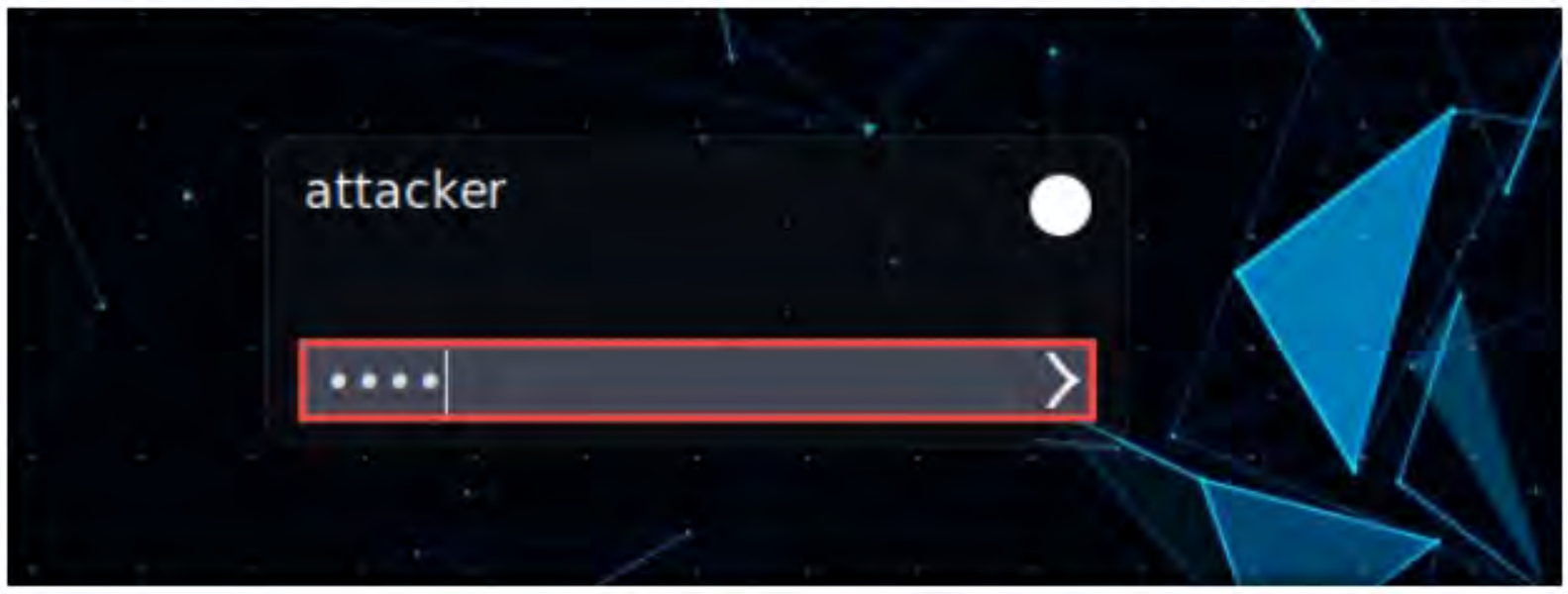


Figure 2.3.1: Parrot Security login page

Emails are messaging sources that are crucial for performing information exchange. Email ID is considered by most people as the personal identification of employees or organizations. Thus, gathering the email IDs of critical personnel is one of the key tasks of ethical hackers.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

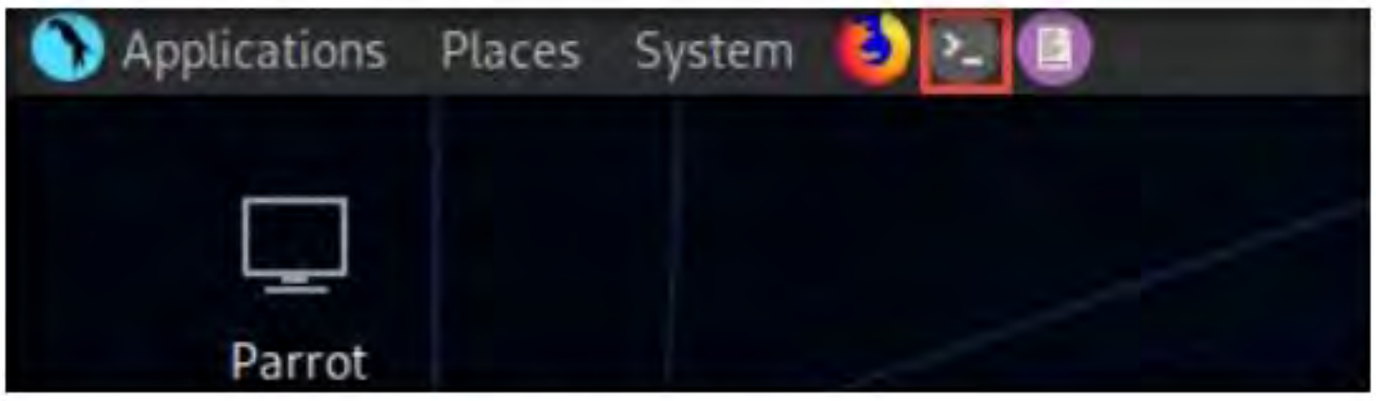


Figure 2.3.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

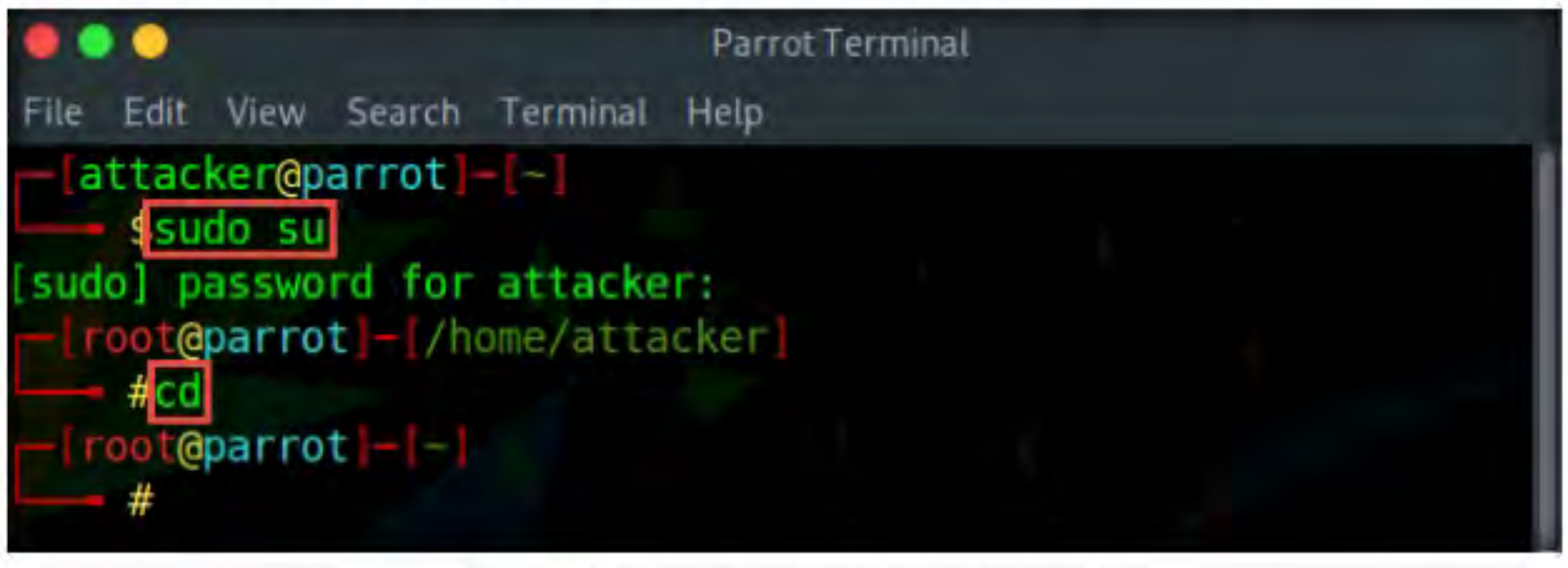


Figure 2.3.3: Running the programs as a root user

TASK 3.1

Extract Email List

theHarvester: This tool gathers emails, subdomains, hosts, employee names, open ports, and banners from different public sources such as search engines, PGP key servers, and the SHODAN computer database as well as uses Google, Bing, SHODAN, etc. to extract valuable information from the target domain. This tool is intended to help ethical hackers and pen testers in the early stages of the security assessment to understand the organization's footprint on the Internet. It is also useful for anyone who wants to know what organizational information is visible to an attacker.

7. In the terminal window, type **theHarvester -d microsoft.com -l 200 -b baidu** and press **Enter**.

Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source.

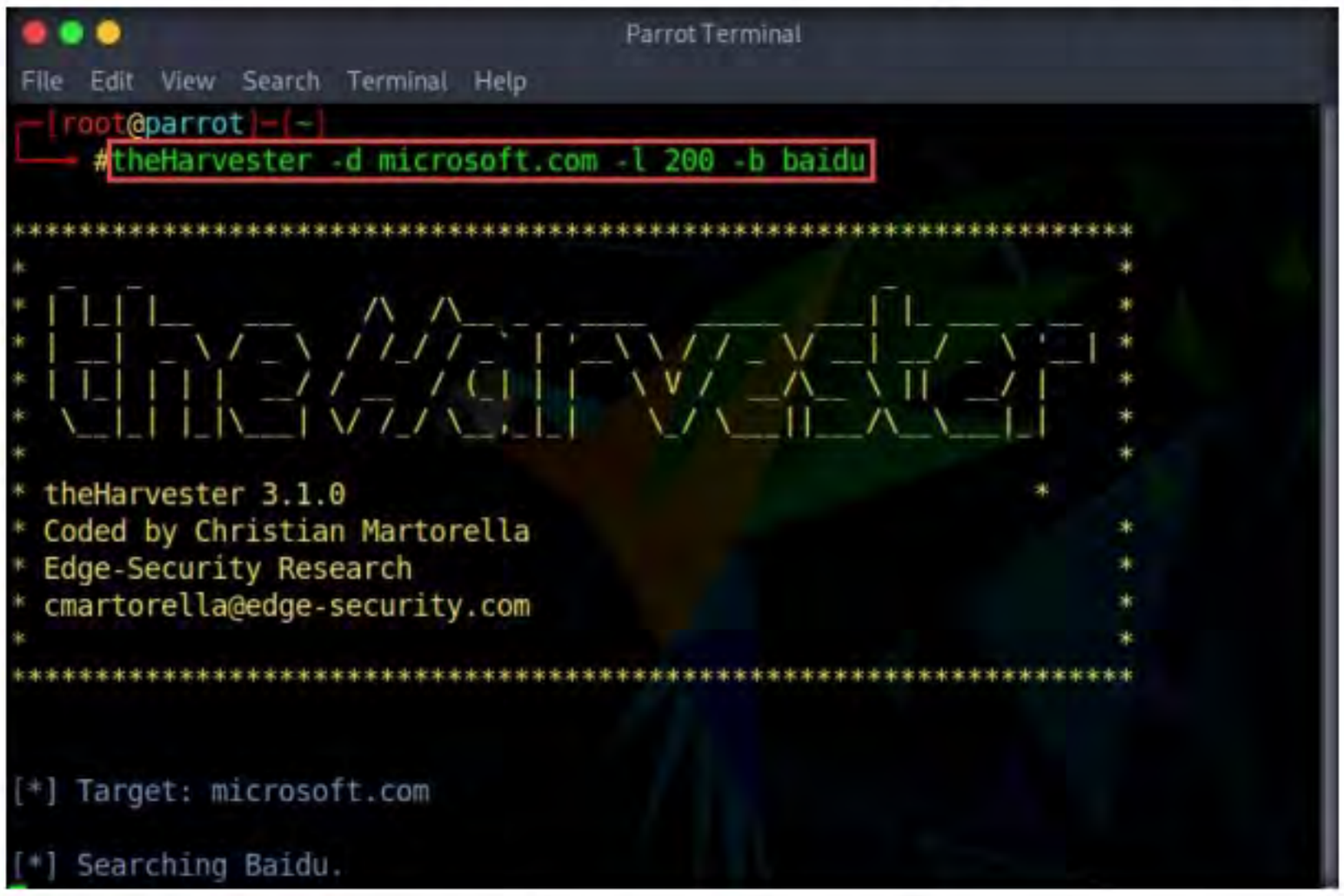


Figure 2.3.4: theHarvester search command

Note: Here, we specify Baidu search engine as a data source. You can specify different data sources (e.g., Baidu, bing, bingapi, dogpile, Google, GoogleCSE, Googleplus, Google-profiles, linkedin, pgp, twitter, vhost, virustotal, threatcrowd, crtsh, netcraft, yahoo, all) to gather information about the target.

8. theHarvester starts extracting the details and displays them on the screen. Scroll down to see the email IDs related to the target company from the Baidu source. It will also extract the target company hosts.

Note: Screenshots shown in this lab might differ.

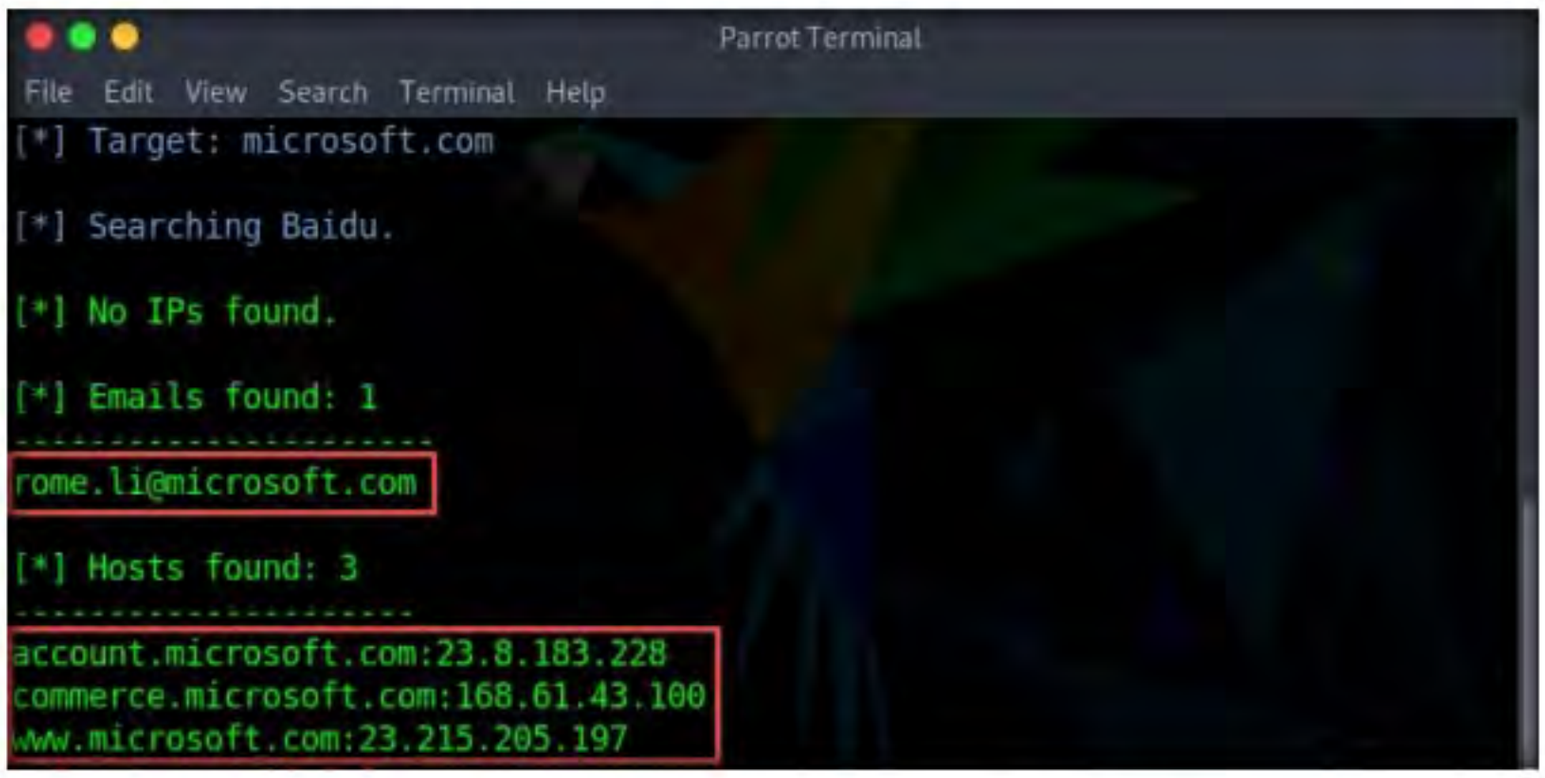


Figure 2.3.5: theHarvester result showing email list and hosts

9. This concludes the demonstration of gathering an email list using theHarvester.
10. Close all open windows and document all the acquired information.
11. Turn off the **Parrot Security** virtual machine.

TASK 4 Gather Information using Deep and Dark Web Searching

Here, we will understand the difference between surface web search and dark web search using Mozilla Firefox and Tor Browser.

1. Switch to the **Windows 10** virtual machine. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
2. Open a **File Explorer**, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Deep and Dark Web Footprinting Tools\Tor Browser**, and double-click **torbrowser-install-win64-8.5.4_en-US.exe**.
3. If the **Open File - Security Warning** window appears, click **Run**.
4. If the **User Account Control** pop-up appears, click **Yes**.
5. If the **Installer Language** window appears, select your preferred language (here, **English**) and click **OK**.
6. The **Tor Browser Setup** window appears. Follow the wizard steps (by selecting default options) to install Tor Browser.
7. After the installation is complete, click the **Finish** button to launch Tor Browser.

The deep web consists of web pages and content that are hidden and unindexed and cannot be located using a traditional web browser and search engines. It can be accessed by search engines such as Tor Browser and The WWW Virtual Library.

The dark web or dark net is a subset of the deep web, where anyone can navigate anonymously without being traced. Deep and dark web search can provide critical information such as credit card details, passports information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

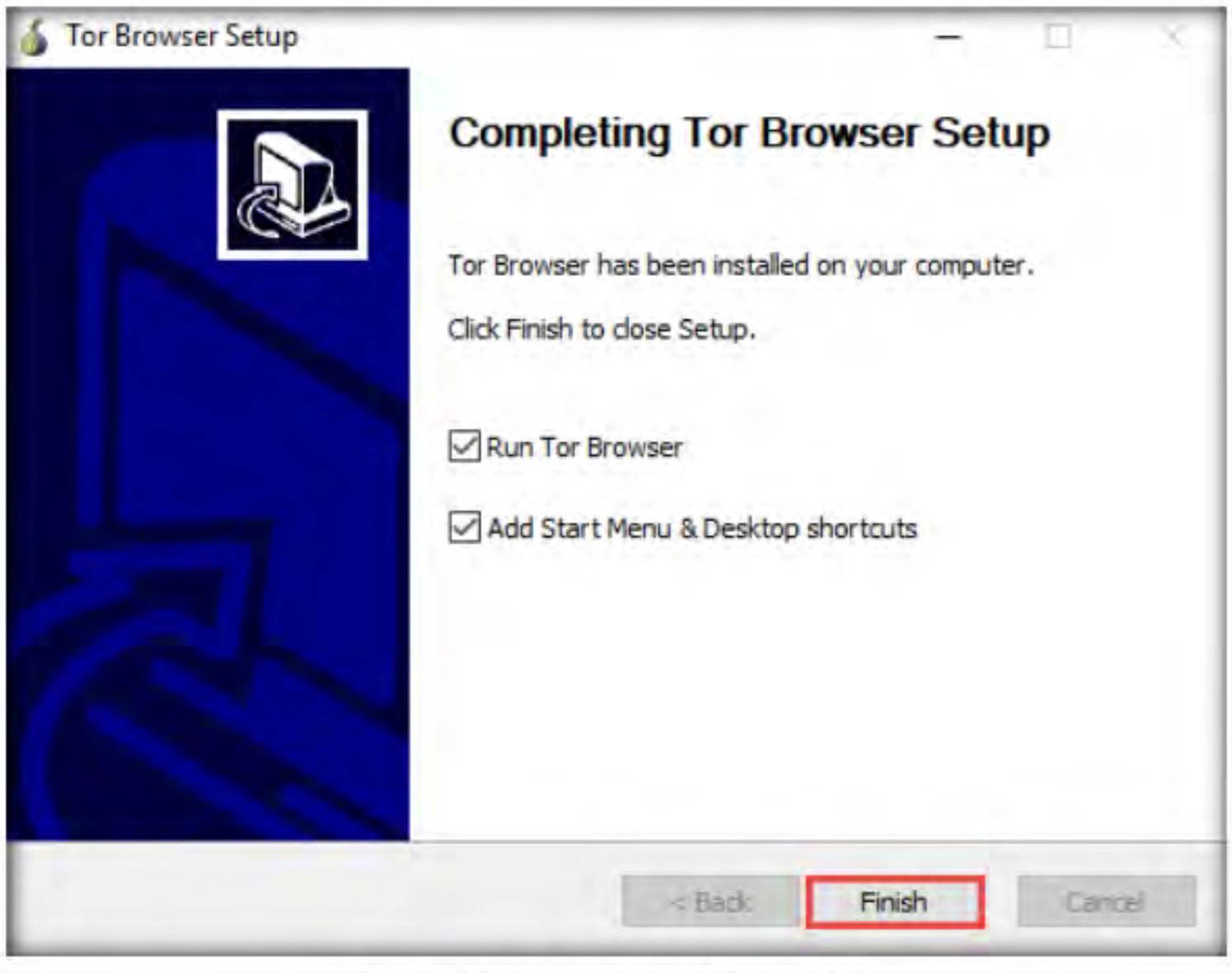


Figure 2.4.1: Tor Browser installation complete

8. The **Connect to Tor** window appears. Click the **Connect** button to directly browse through Tor Browser's default settings.

Note: If Tor is censored in your country or if you want to connect through Proxy, click the **Configure** button and continue.

Figure 2.4.2: Tor Browser – Connect button

9. After a few seconds, the Tor Browser home page appears. The main advantage of Tor Browser is that it maintains the anonymity of the user throughout the session.

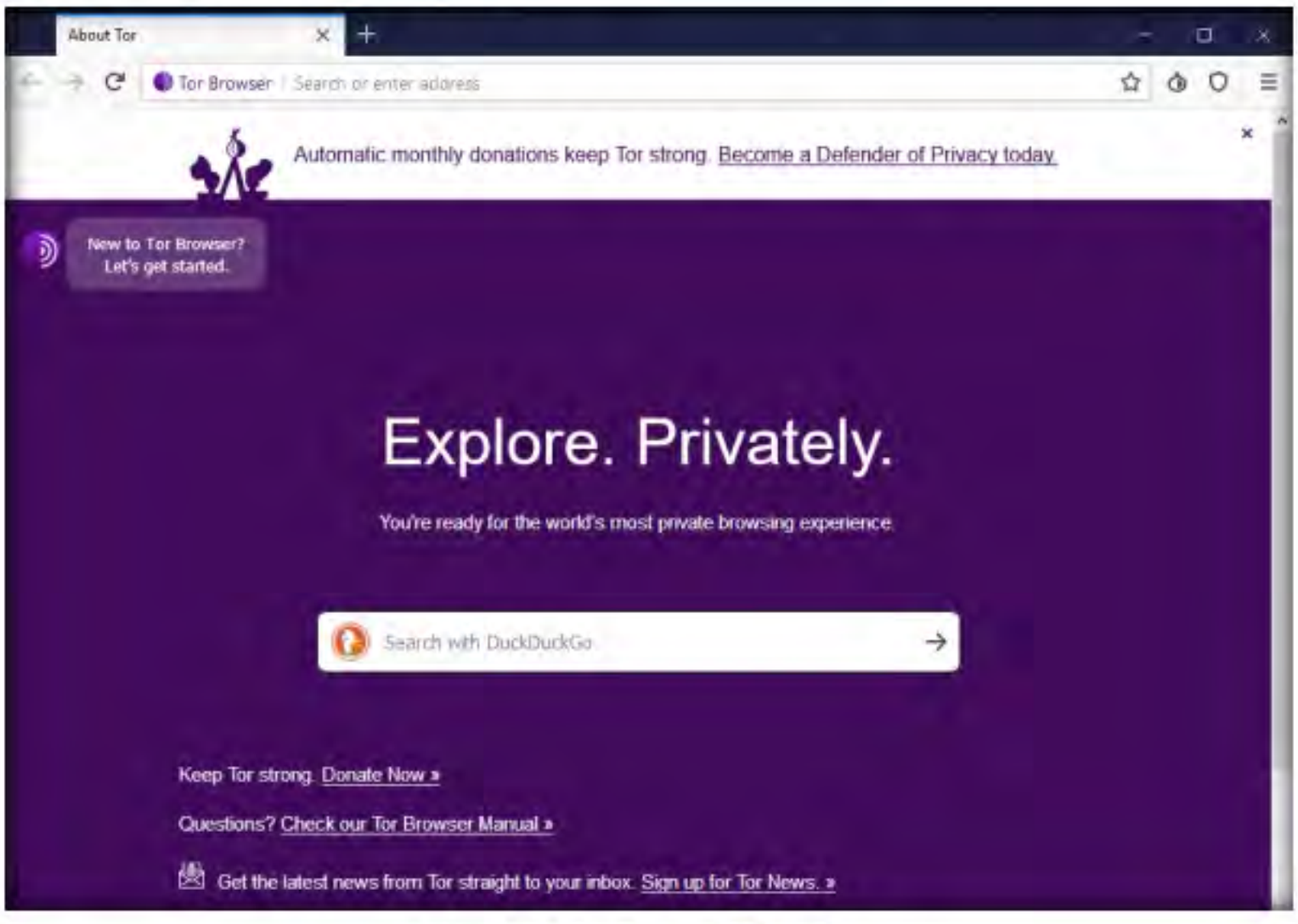


Figure 2.4.3: Tor Browser – Home Page

10. As an ethical hacker, you need to collect all possible information related to the target organization from the dark web. Before doing so, you must know the difference between surface web searching and dark web searching.

TASK 4.1

Perform Surface Web Search

11. To understand surface web searching, first, minimize **Tor Browser** and open **Mozilla Firefox**. Navigate to **www.google.com**; in the Google search bar, search for information related to **hacker for hire**. You will be presented with much irrelevant data, as shown in the screenshot.

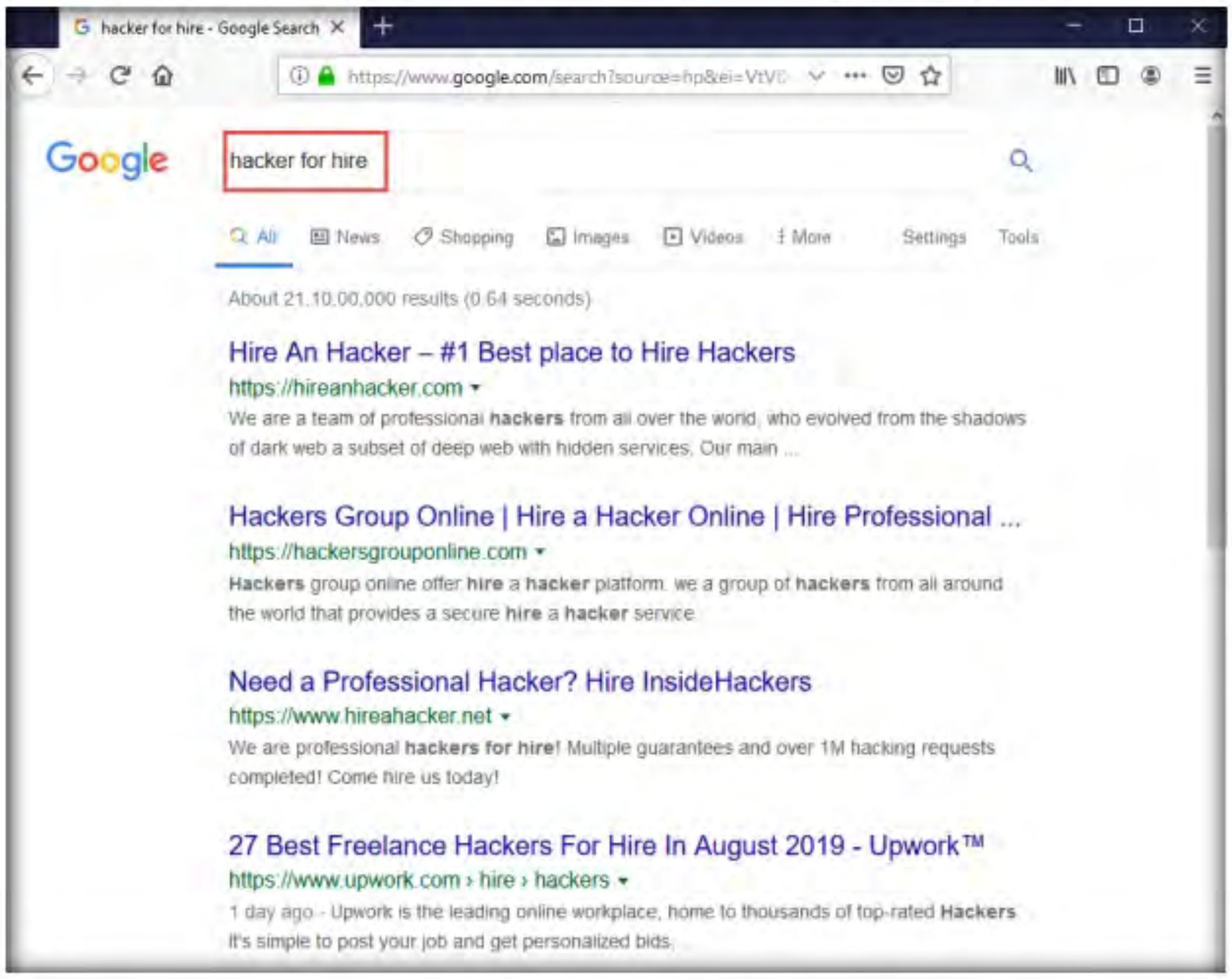


Figure 2.4.4: Normal search result

TASK 4.2

Perform Deep and Dark Web Search

12. Now switch to **Tor Browser** and search for the same (i.e., **hacker for hire**). You will find the relevant links related to the professional hackers who operate underground through the dark web.

Note: Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.

13. Now, click on the toggle button that specifies the country of VPN/Proxy (here, by default **Germany** is selected) and select a relevant country (here, **Australia**).

Note: The default country of VPN/Proxy may vary in your environment, since it is randomly chosen by Tor while initiating a session.

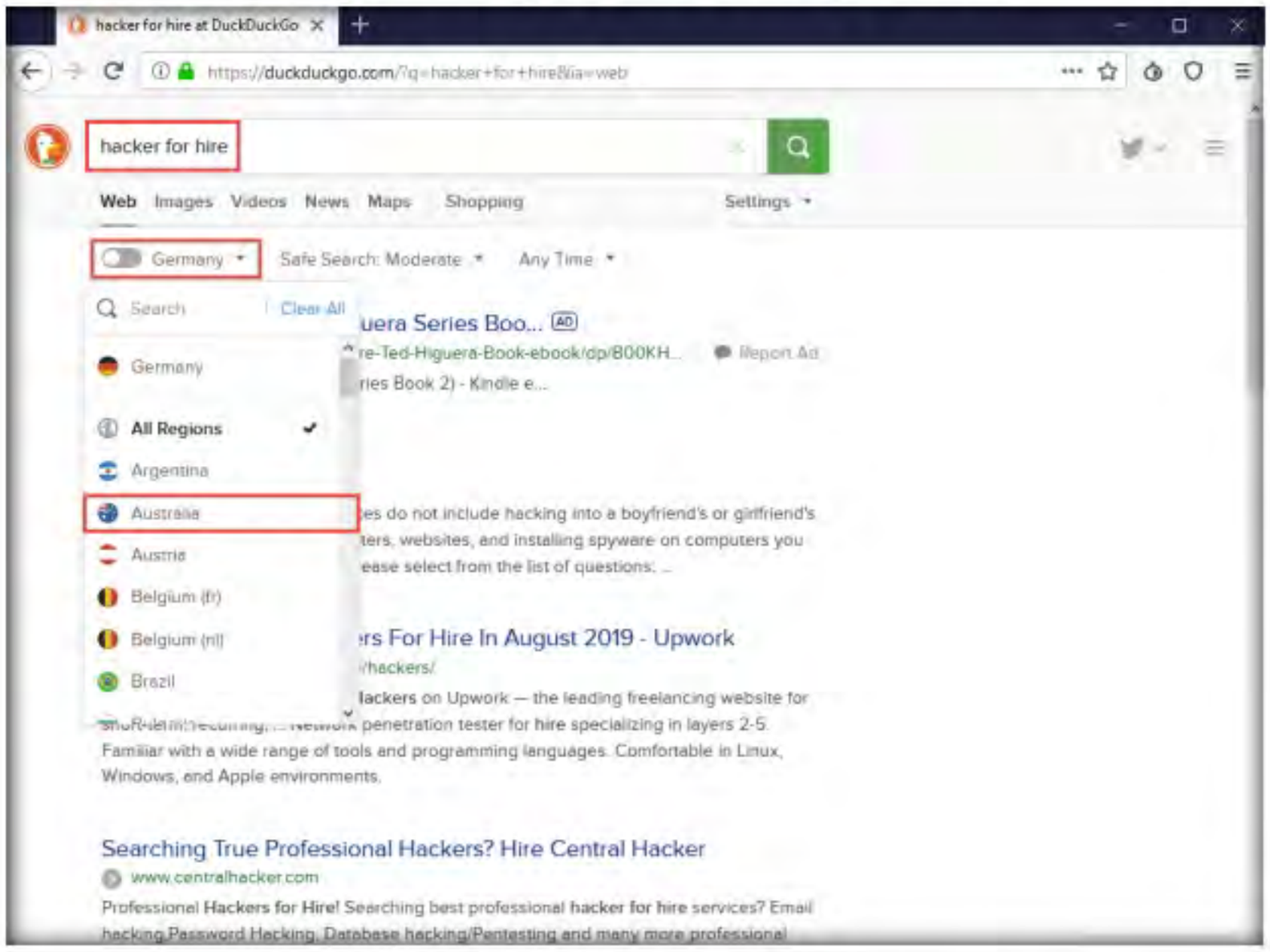


Figure 2.4.5: VPN/Proxy setting for search

14. Search results for **hacker for hire** will be loaded, as shown in the screenshot. Click to open any of the search results (here, **https://hackerforhire.com**).

Note: Screenshots shown in this lab might differ.

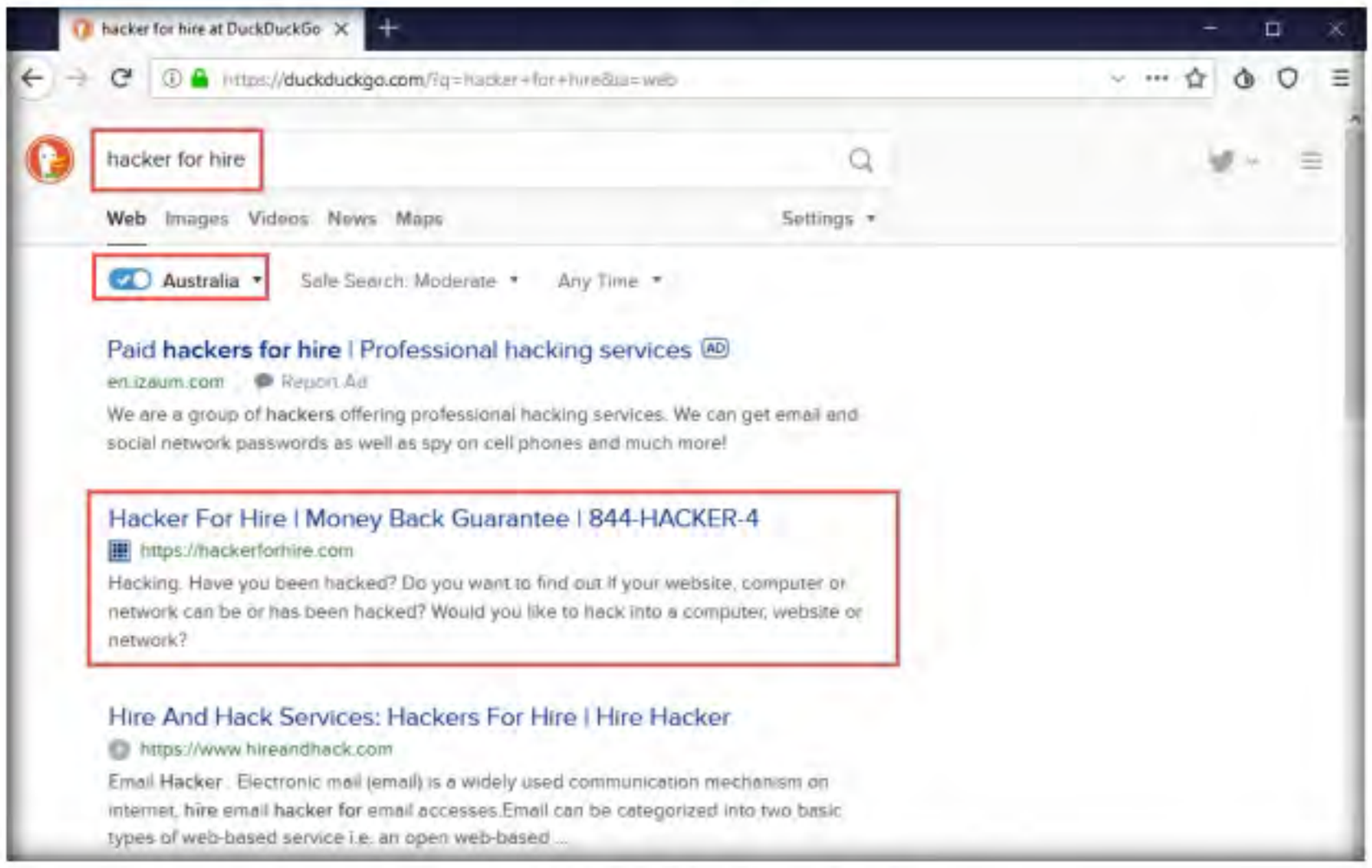


Figure 2.4.6: Tor dark web search result

15. The **https://hackerforhire.com** webpage opens up, as shown in the screenshot. You can see that the site belongs to professional hackers who operate underground.

Figure 2.4.7: hackerforhire.com website

16. Hackerforhire.com is an example. These search results will help you in identifying professional hackers. However, as an ethical hacker, you can gather critical and sensitive information about your target organization using deep and dark web search.

17. You can also anonymously explore the following onion sites using Tor Brower to gather other relevant information about the target organization:

    - **The Hidden Wiki** is an onion site that works as a Wikipedia service of hidden websites. (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page)
    - **FakeID** is an onion site for creating fake passports (http://fakeidskhfik46ux.onion/)
    - **The Paypal Cent** is an onion site that sells PayPal accounts with good balances (http://nare7pqnmnojs2pg.onion/)

18. This concludes the demonstration of gathering information using deep and dark web searching using Tor Browser.

19. Close all open windows and document all the acquired information.

You can also use tools such as **ExoneraTor** (https://metrics.torproject.org), **OnionLand Search engine** (https://onionlandsearchengine.com), etc. to perform deep and dark web browsing.

TASK 5

Determine Target OS Through Passive Footprinting

Operating system information is crucial for every ethical hacker. Ethical hackers can acquire details of the operating system running on the target machine by performing various passive footprinting techniques.

Here, we will gather target OS information through passive footprinting using the Censys web service.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://censys.io/domain?q=**.
2. In the **Websites** search bar, type the target website (here, **eccouncil.org**) and press **Enter**. From the results, click any result (here, **eccouncil.org**) from which you want to gather the OS details.

Note: Screenshots shown in this lab might differ.

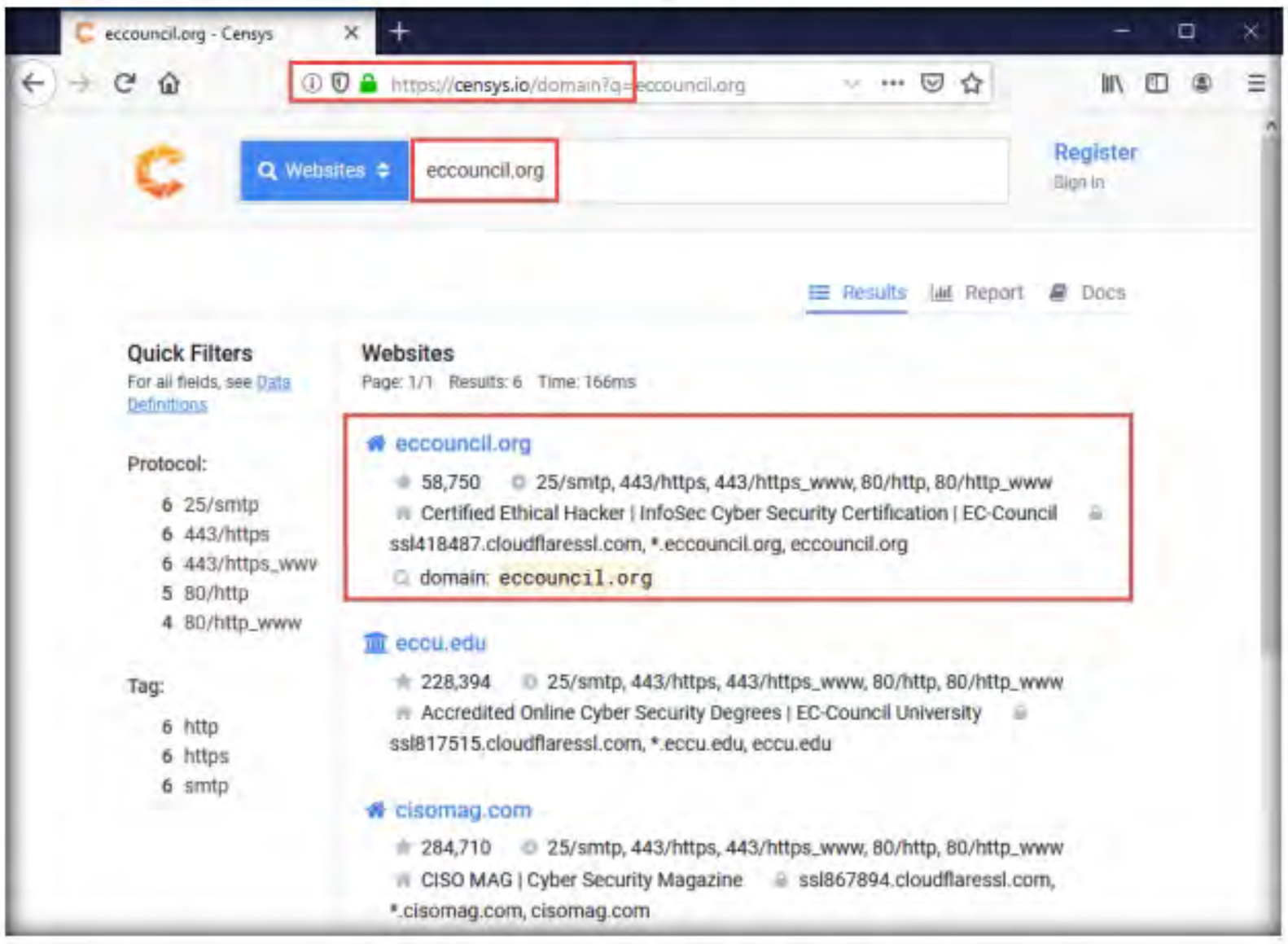


Figure 2.5.1: Censys result about the target website

3. The **eccouncil.org** page appears, as shown in the screenshot. Under the **Basic Information** section, you can observe that the **OS** is **Windows**. Apart from this, you can also observe that the **Server** on which the **HTTP** is running is **cloudflare**.

Note: Screenshots shown in this lab might differ.

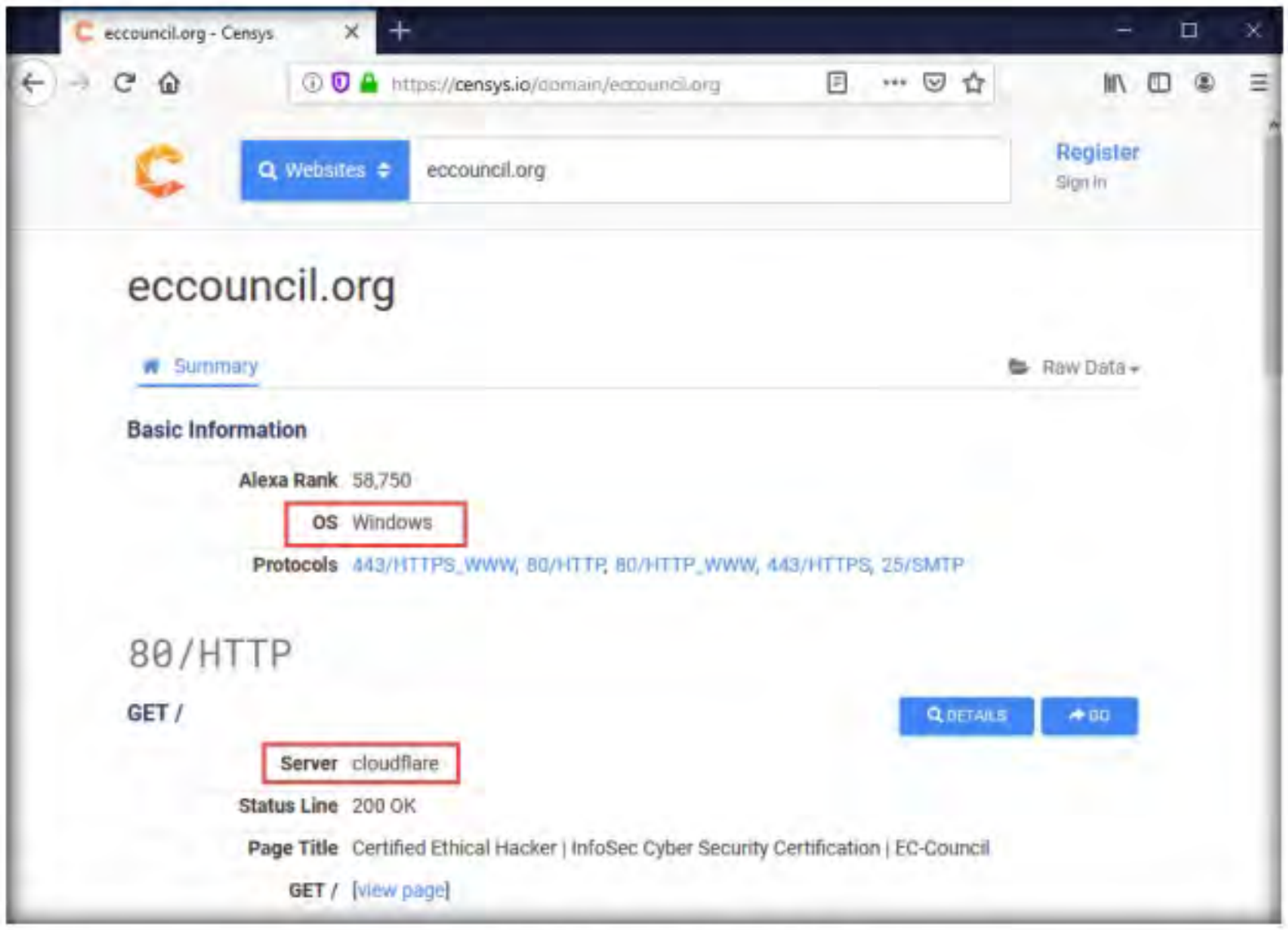


Figure 2.5.2: Censys result - OS details

You can also use web services such as **Netcraft** (https://www.netcraft.com), **Shodan** (https://www.shodan.io), etc. to gather OS information of target organization through passive footprinting.

4. This concludes the demonstration of gathering OS information through passive footprinting using the Censys web service.
5. Close all open windows and document all the acquired information.
6. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Perform Footprinting Through Social Networking Sites

Social networking services are online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker, during information gathering, you need to gather personal information about employees working in critical positions in the target organization; for example, the Chief Information Security Officer, Security Architect, or Network Administrator. By footprinting through social networking sites, you can extract personal information such as name, position, organization name, current location, and educational qualifications. Further, you can find professional information such as company or business, current location, phone number, email ID, photos, videos, etc. The information gathered can be useful to perform social engineering and other types of advanced attacks.

Lab Objectives

- Gather employees' information from LinkedIn using theHarvester
- Gather personal information from various social networking sites using Sherlock
- Gather information using Followerwonk

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Social Networking Sites

Social networking sites are online services, platforms, or other sites that allow people to connect and build interpersonal relations. People usually maintain profiles on social networking sites to provide basic information about themselves and to help make and maintain connections with others; the profile generally contains information such as name, contact information (cellphone number, email address), friends' information, information about family members, their interests, activities, etc. On social networking sites, people may also post their personal information such as date of birth, educational information, employment background, spouse's names, etc. Organizations often post information such as potential partners, websites, and upcoming news about the company. Thus, social networking sites often prove to be valuable information resources. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, etc.

Lab Tasks

TASK 1

Gather Employees' Information from LinkedIn using theHarvester

LinkedIn is a social networking website for industry professionals. It connects the world's human resources to aid productivity and success. The site contains personal information such as name, position, organization name, current location, educational qualifications, etc.

Here, we will gather information about the employees (name and job title) of a target organization that is available on LinkedIn using theHarvester tool.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Figure 3.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

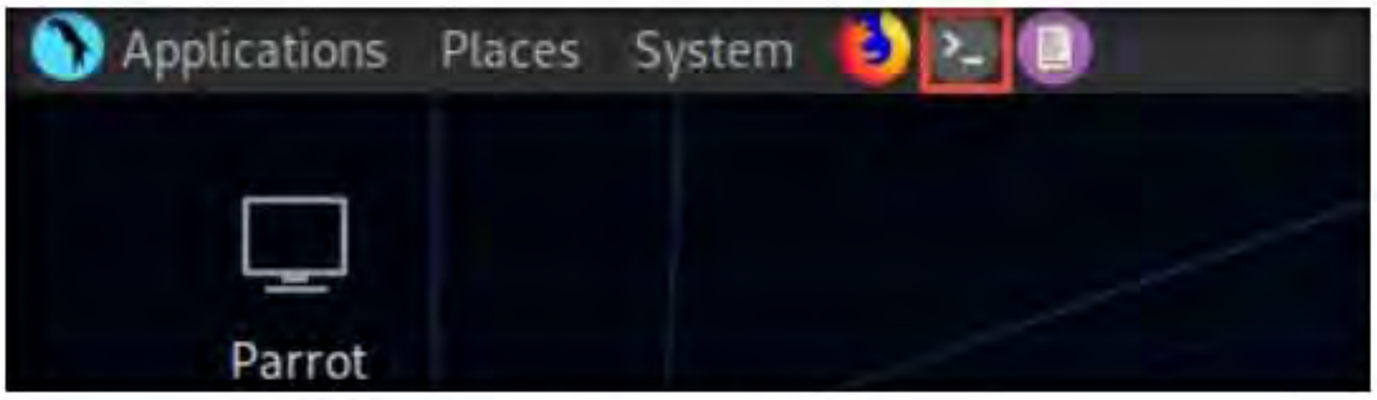


Figure 3.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

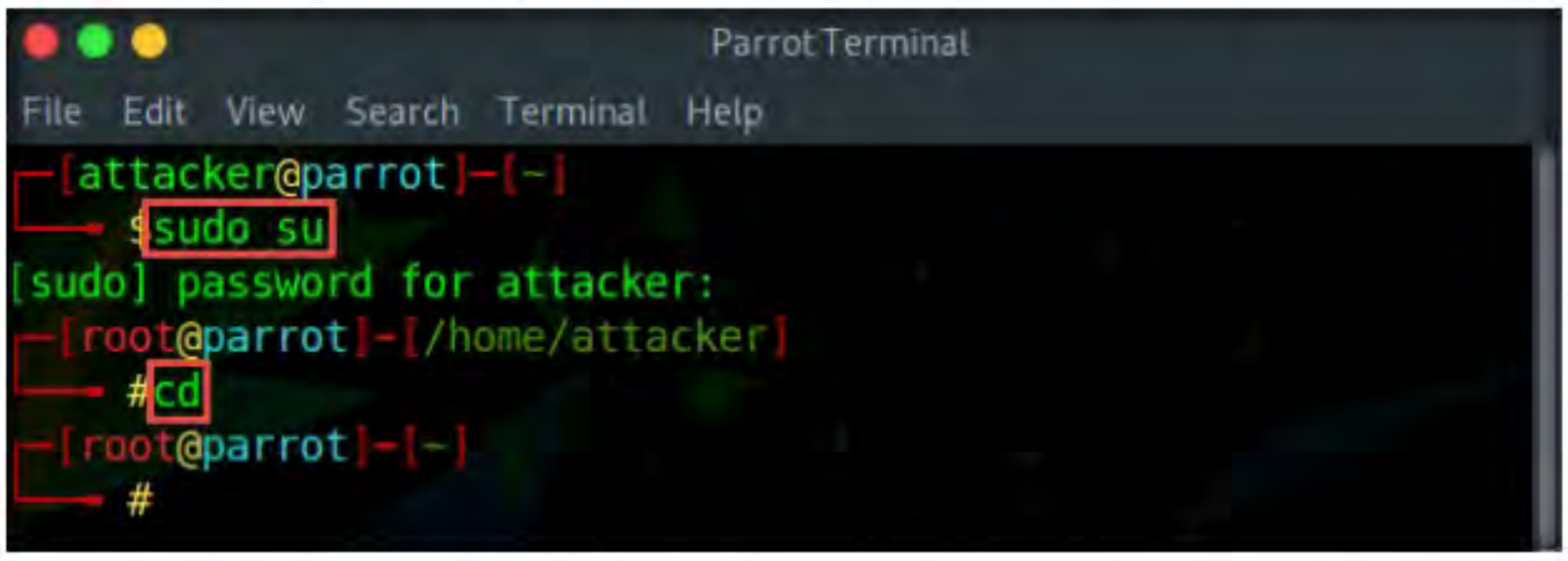


Figure 3.1.3: Running the programs as a root user

7. In the terminal window, type **theHarvester -d eccouncil -l 200 -b linkedin** and press **Enter** to see 200 results of EC-Council from the LinkedIn source. Scroll down to view all the 200 results of the employees of the EC-Council.

Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source as LinkedIn.

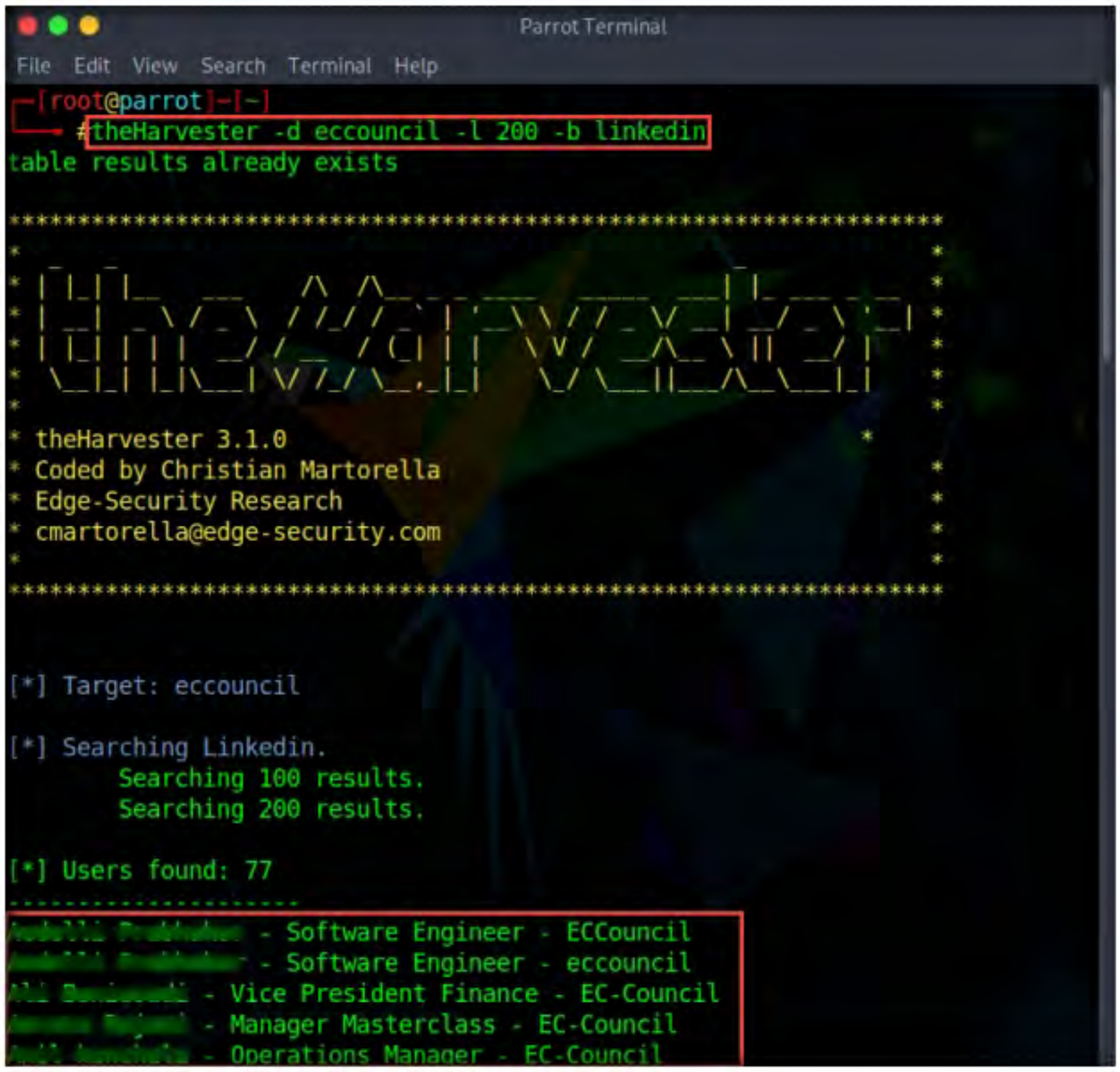


Figure 3.1.4: theHarvester result

8. This concludes the demonstration of gathering employees' information from LinkedIn using theHarvester.
9. Close all open windows and document all the acquired information.

TASK 2 Gather Personal Information from Various Social Networking Sites using Sherlock

Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target person.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

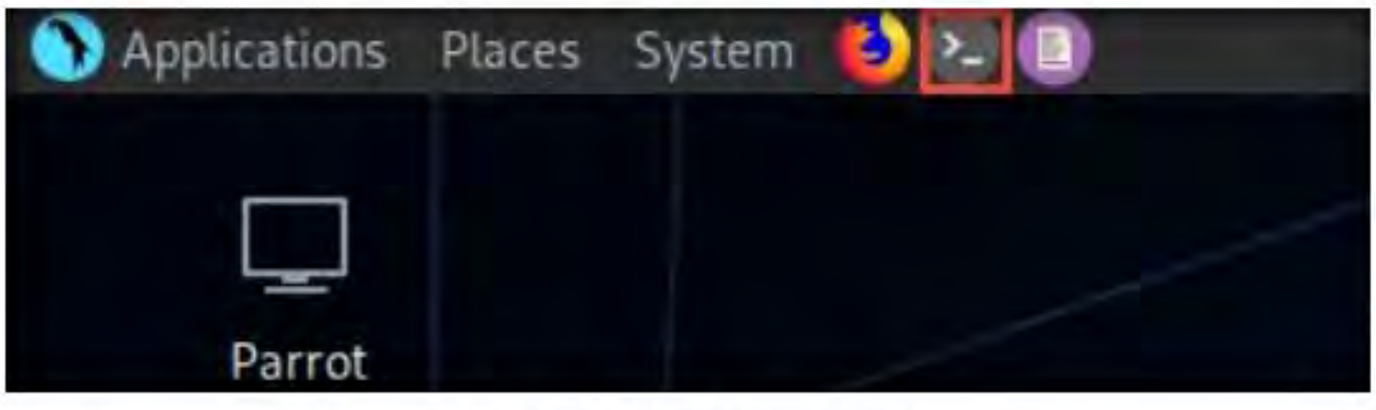


Figure 3.2.1: MATE Terminal Icon

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

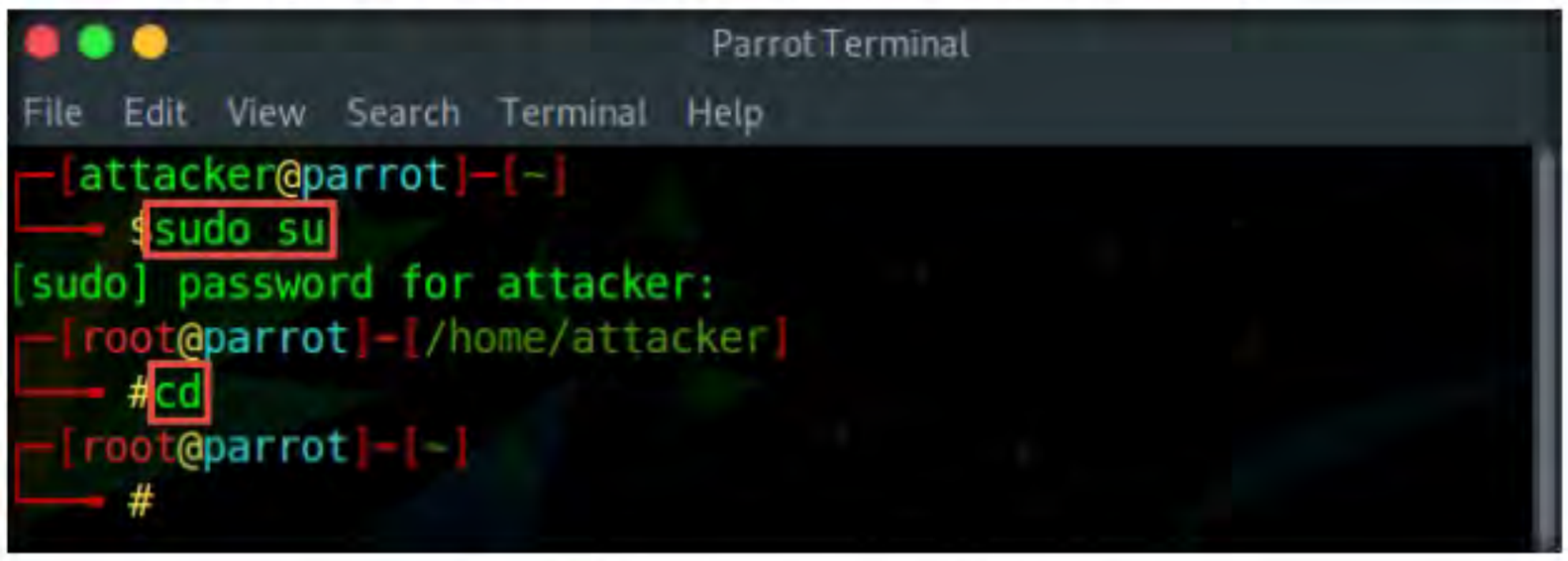


Figure 3.2.2: Running the programs as a root user

5. In the **Parrot Terminal** window, type **git clone https://github.com/sherlock-project/sherlock.git** and press **Enter**.

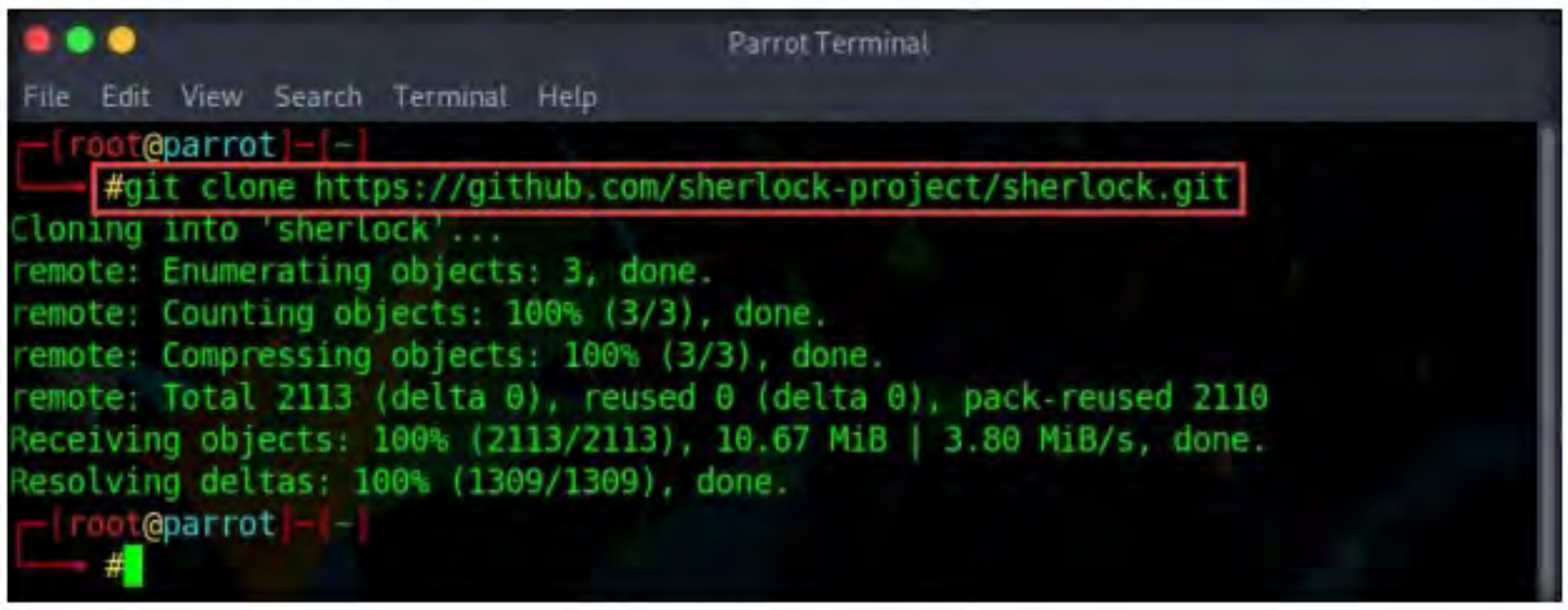


Figure 3.2.3: Cloning Sherlock tool

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

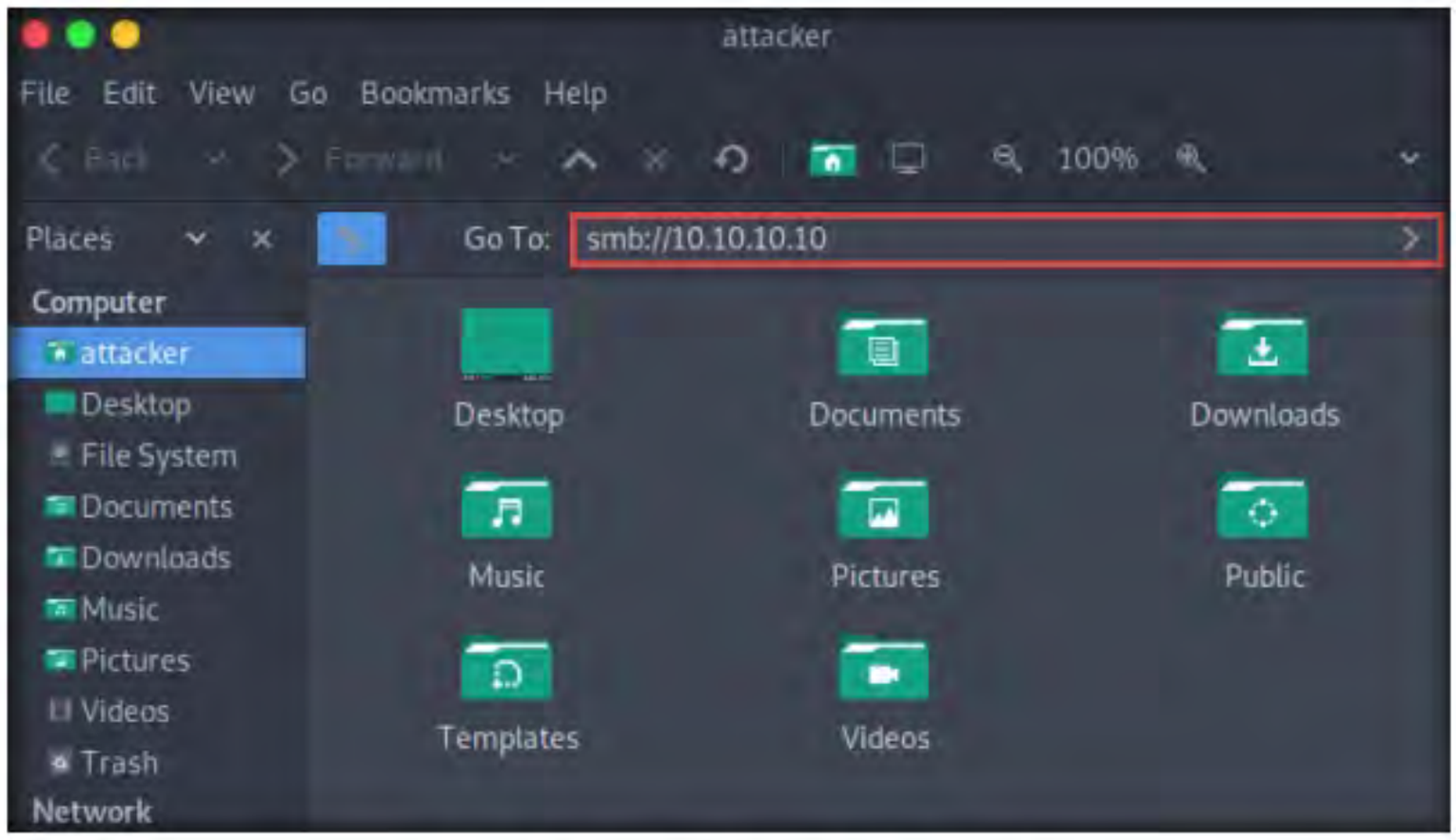


Figure 3.2.4: Accessing Windows 10 shared folder

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

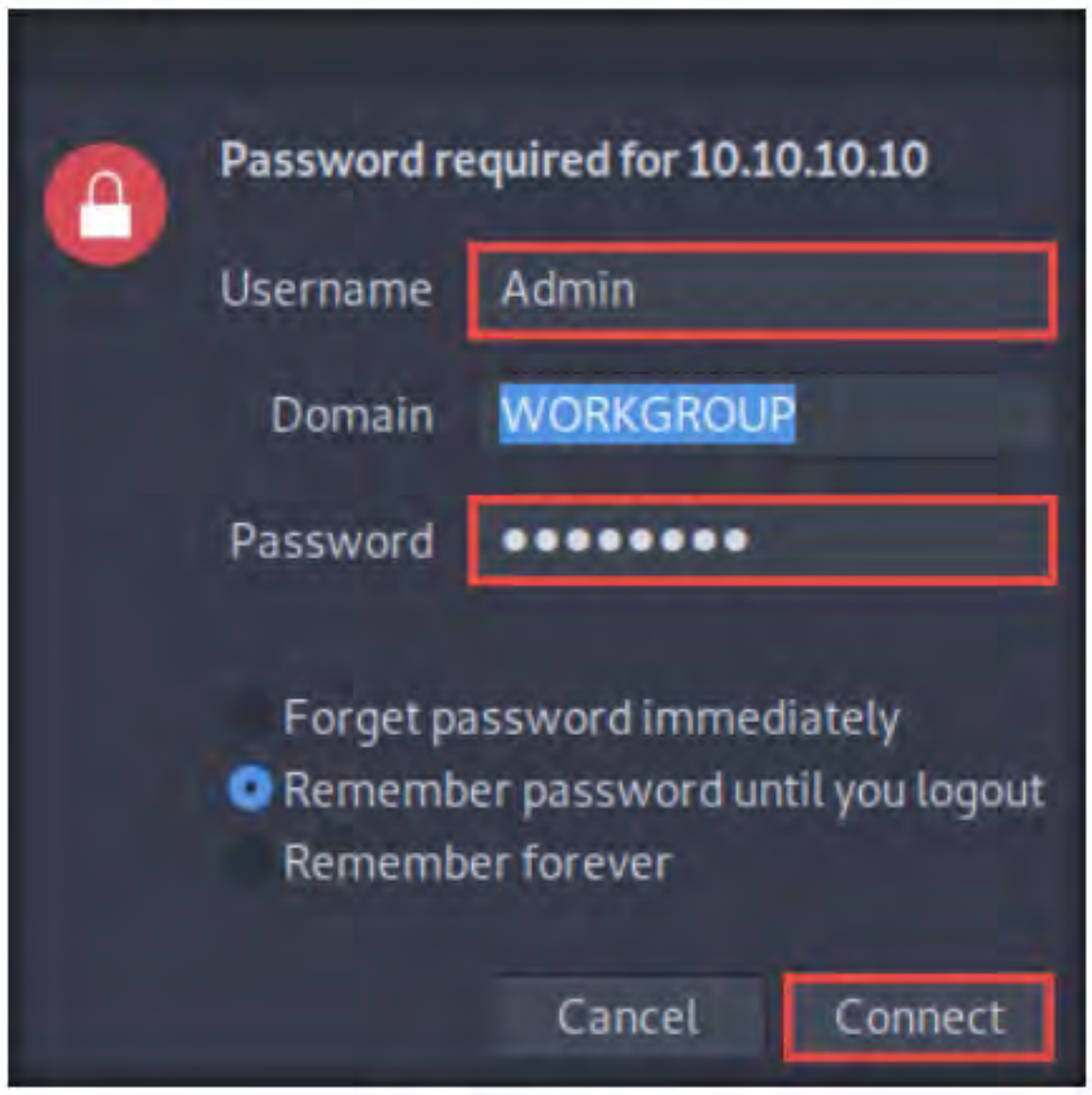


Figure 3.2.5: Security pop-up

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **sherlock** folder.

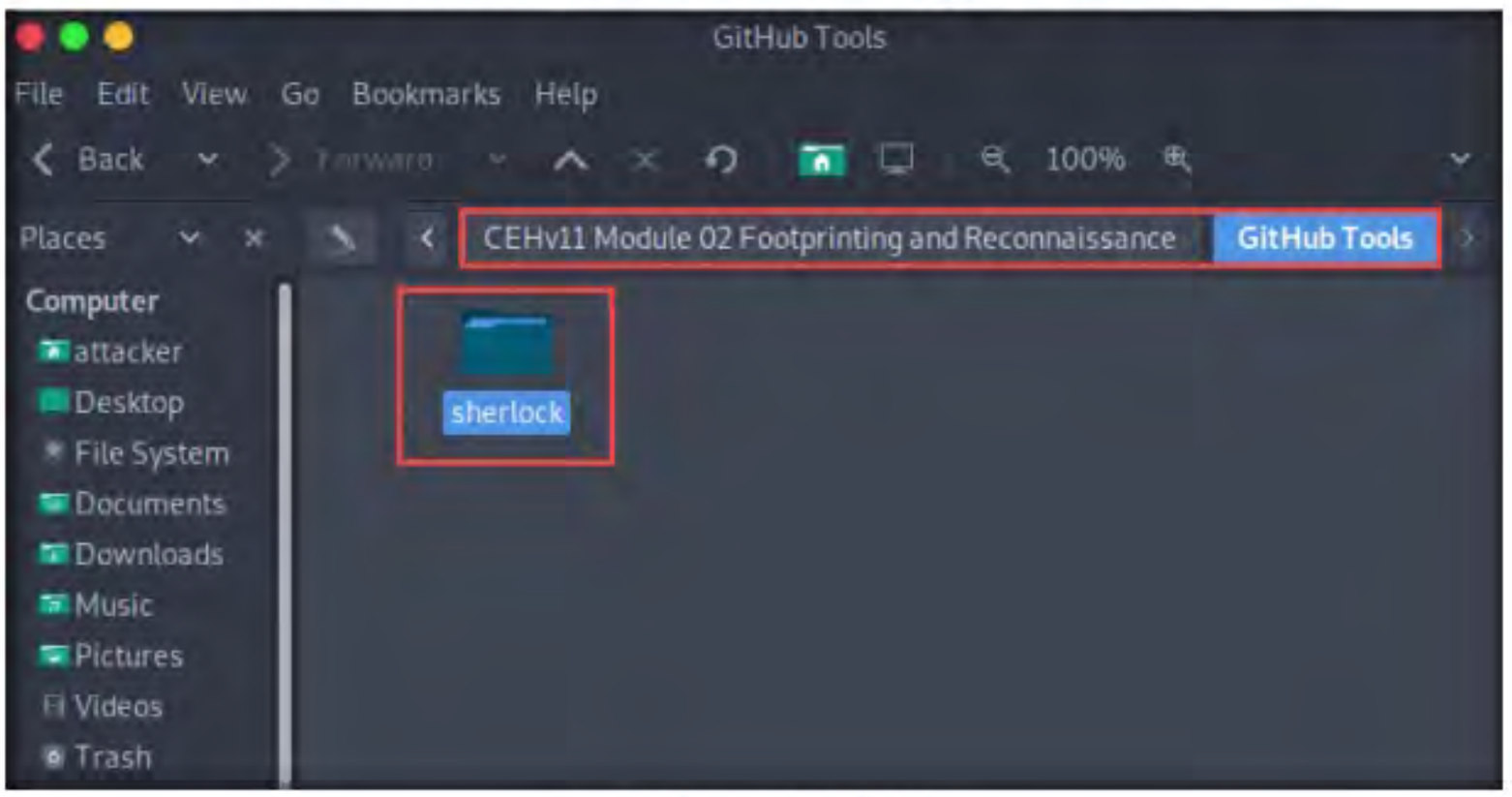


Figure 3.2.6: Copy sherlock folder

- Paste the copied **sherlock** folder on the location **/home/attacker/.**

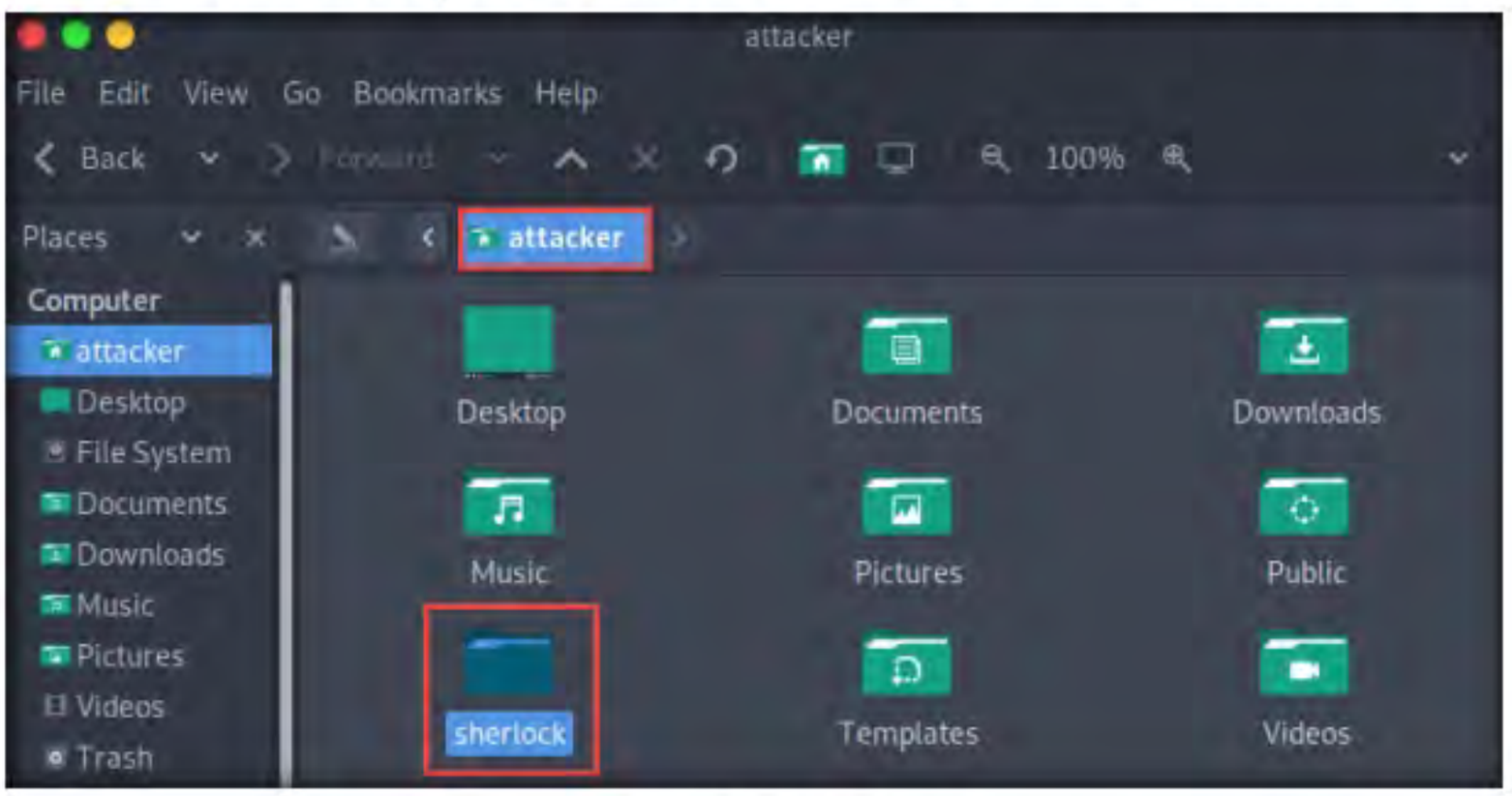


Figure 3.2.7: Paste the directory

- In the terminal window, type **mv /home/attacker/sherlock /root/.**

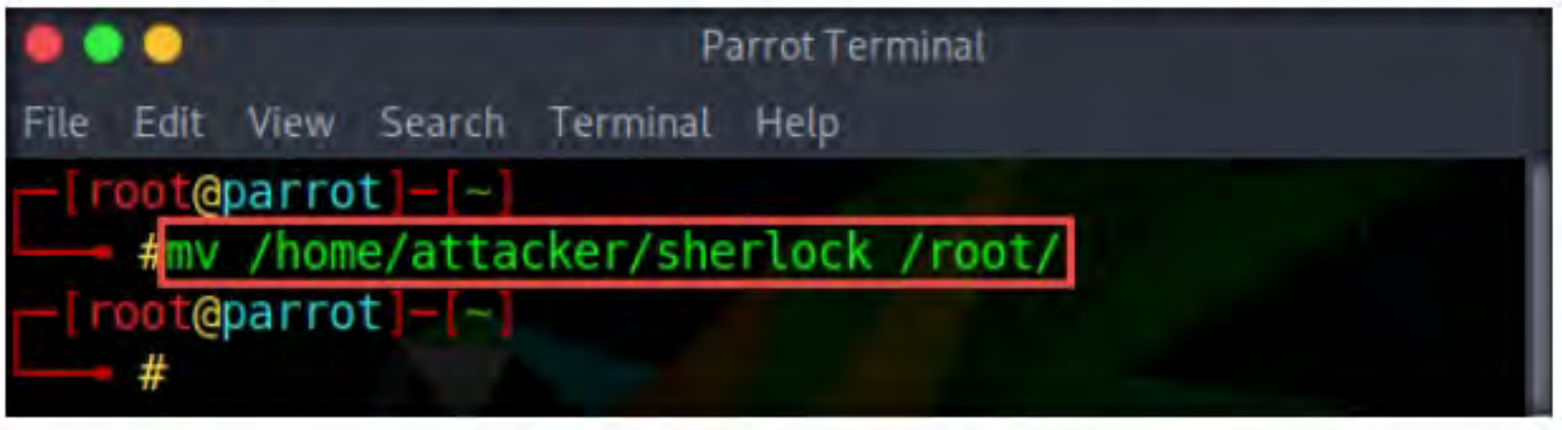


Figure 3.2.8: Move the directory to root folder

6. Type **cd sherlock** and press **Enter** to navigate to the **sherlock** folder. To install the python-pip requirements, type **python3 -m pip install -r requirements.txt** and press **Enter**.

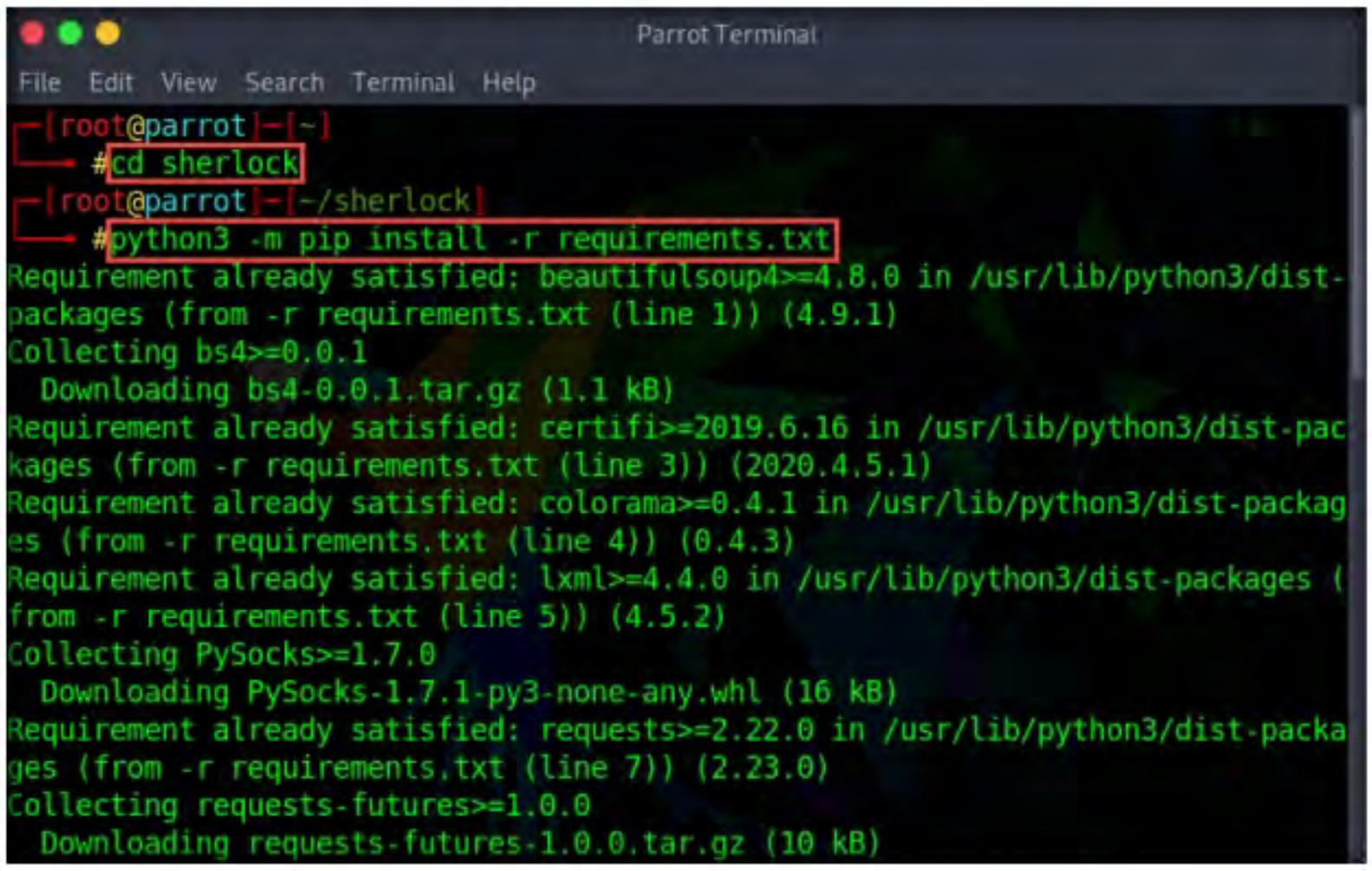


Figure 3.2.9: requirements.txt installation

7. Once the installation is complete, type **cd sherlock** and press **Enter**.

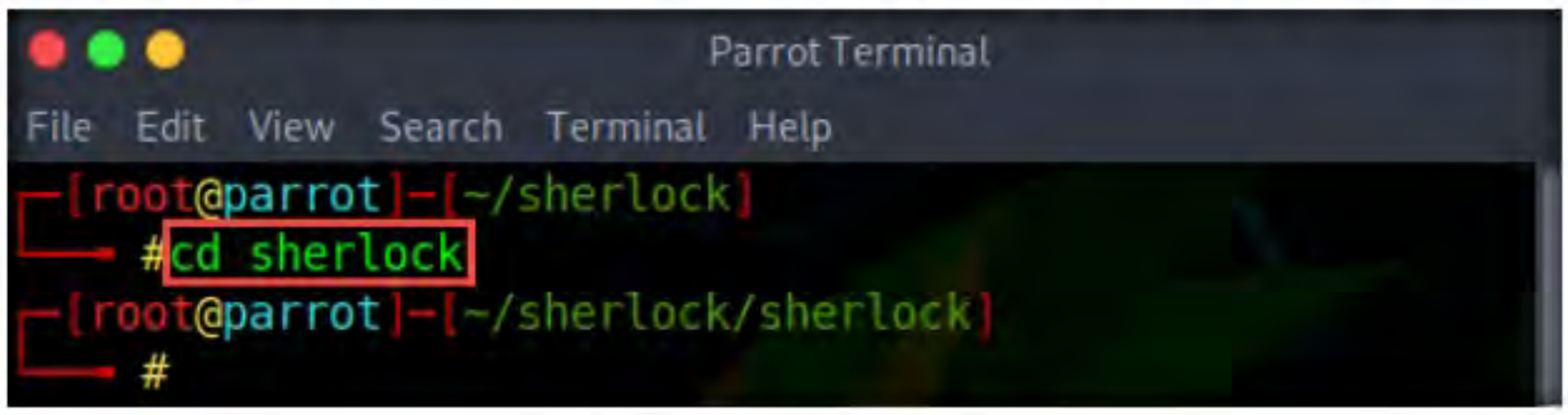


Figure 3.2.10: Navigate to the sherlock folder

8. Now, type **python3 sherlock.py satya nadella** and press **Enter**. You will get all the URLs related to Satya Nadella, as shown in the screenshot. Scroll down to view all the results.

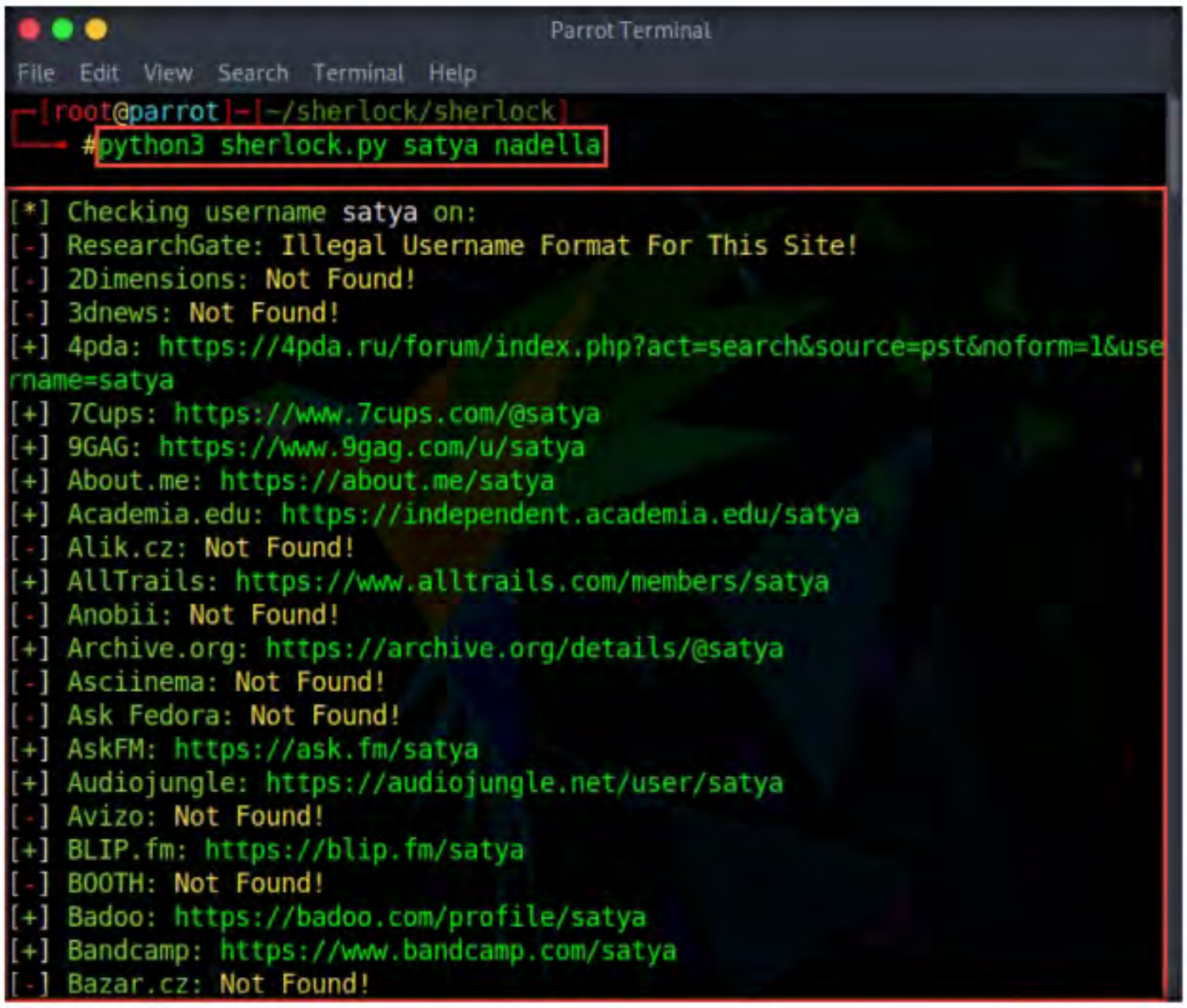


Figure 3.2.11: sherlock search result

You can also use tools such as **Social Searcher** (https://www.social-searcher.com), **UserRecon** (https://github.com), etc. to gather additional information related to the target company and its employees from social networking sites.

9. This concludes the demonstration of gathering person information from various social networking sites using Sherlock.
10. Close all open windows and document all the acquired information.
11. Turn off the **Parrot Security** virtual machine.

TASK 3 Gather Information using Followerwonk

Followerwonk is an online tool that helps you explore and grow your social graph, digging deeper into Twitter analytics; for example, Who are your followers? Where are they located? When do they tweet? This can be used to gather Twitter information about any target organization or individual.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://followerwonk.com/analyze**. In the **screen name** search bar, type your target individual's twitter tag (here, **@satyanadella**) and click the **Do it** button to analyze the users whom the target person follows.

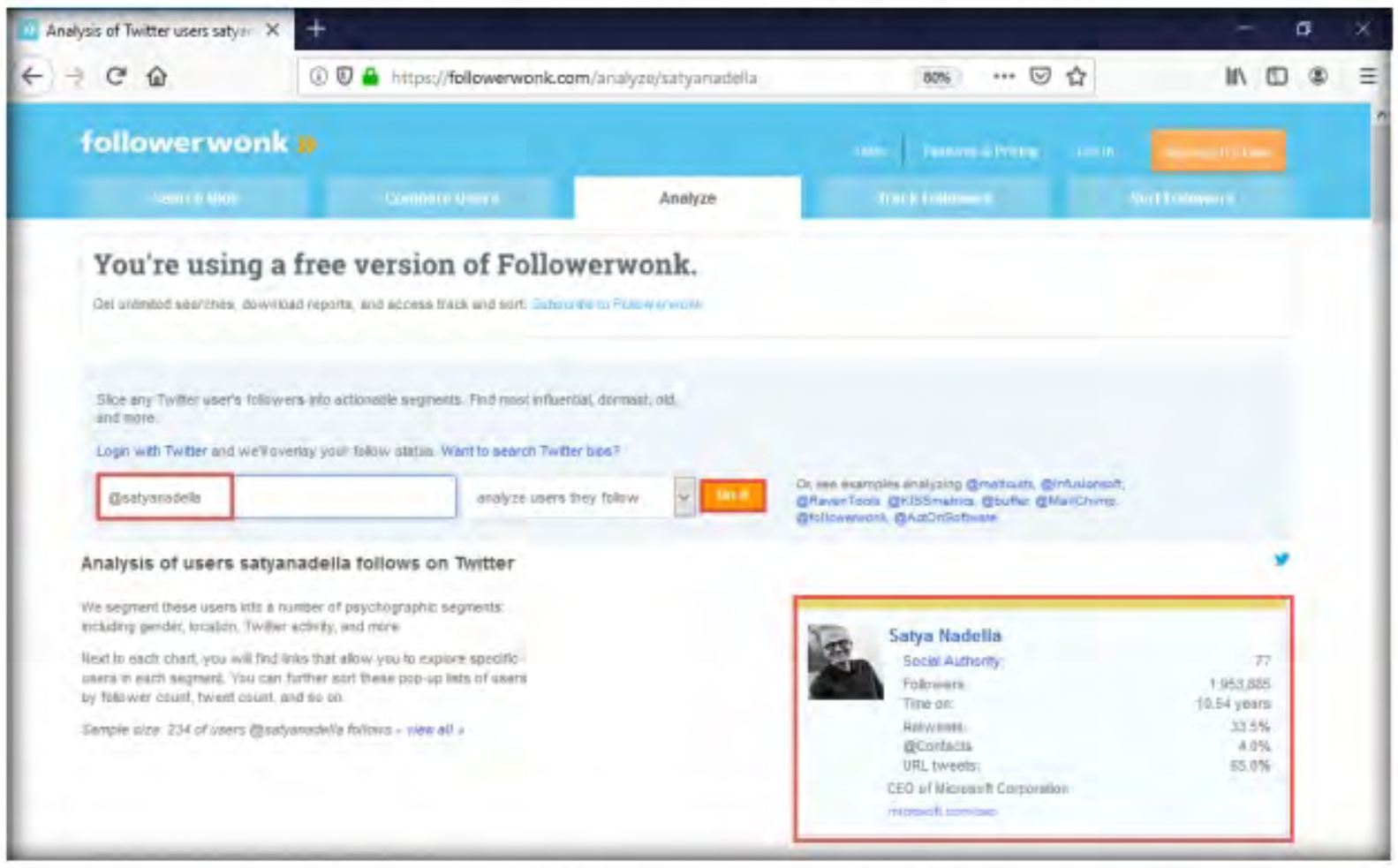


Figure 3.3.1: Followerwonk search result

4. Scroll down to view the detailed analysis, as shown in the screenshot.

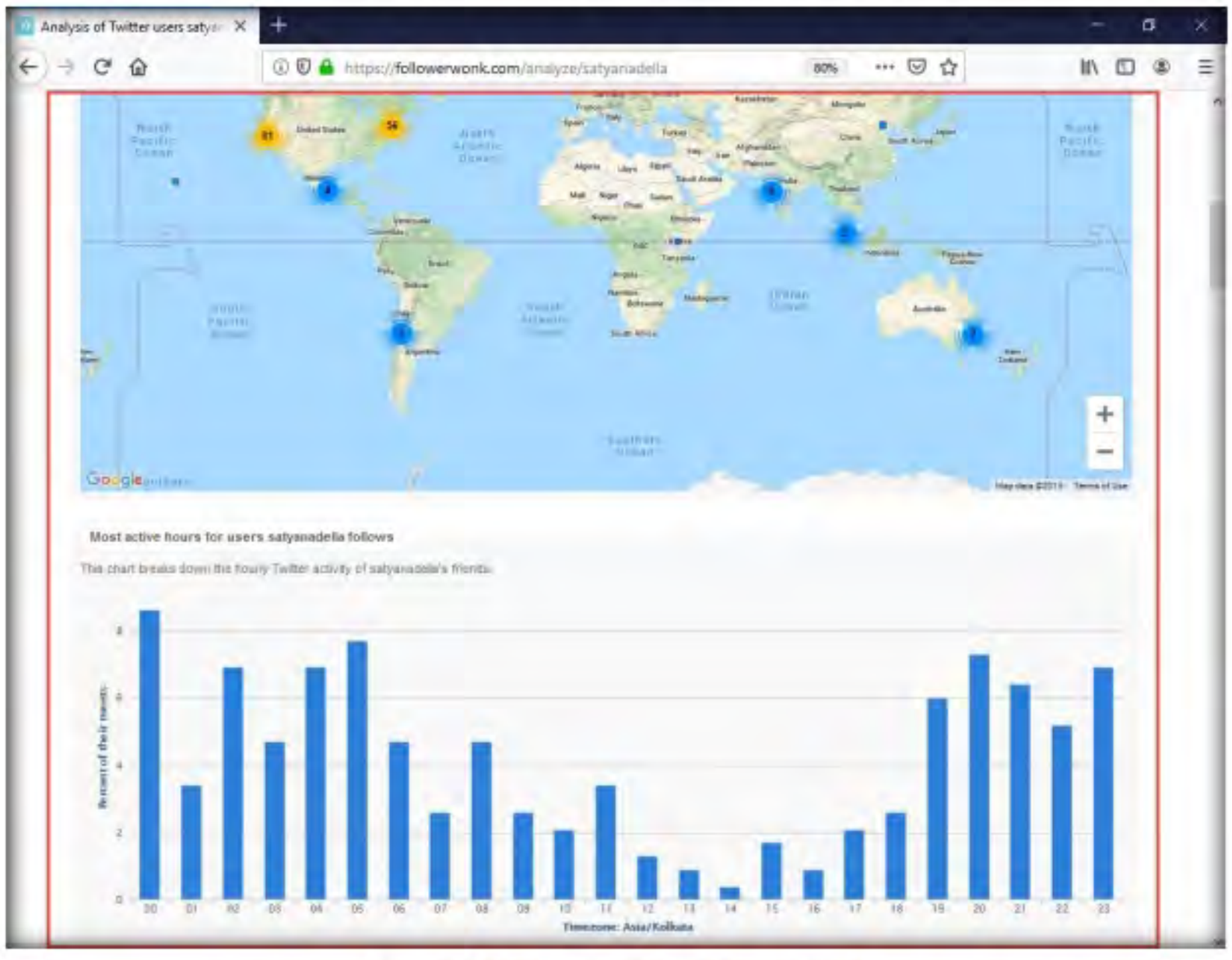


Figure 3.3.2: Followerwonk detailed search result

5. This concludes the demonstration of gathering information using Followerwonk.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 10** virtual machine.

You can also use **Hootsuite** (https://hootsuite.com), **Sysomos** (https://www.sysomos.com), etc. to gather additional information related to the target company and its employees from social networking sites

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 4

Perform Website Footprinting

Website footprinting refers to monitoring and analyzing the target organization's website for information.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

As a professional ethical hacker, you should be able to extract a variety of information about the target organization from its website; by performing website footprinting, you can extract important information related to the target organization's website such as the software used and the version, operating system details, filenames, paths, database field names, contact details, CMS details, the technology used to build the website, scripting platform, etc. Using this information, you can further plan to launch advanced attacks on the target organization.

Lab Objectives

- Gather information about a target website using ping command line utility
- Gather information about a target website using Website Informer
- Extract a company's data using Web Data Extractor
- Mirror the target website using HTTrack Web Site Copier
- Gather a wordlist from the target website using CeWL

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Web Data Extractor located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor**

- HTTrack Web Site Copier located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier**
- You can also download the latest versions of **Web Data Extractor** and **HTTrack Web Site Copier** from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 35 Minutes

Overview of Website Footprinting

Website footprinting is a technique used to collect information regarding the target organization's website. Website footprinting can provide sensitive information associated with the website such as registered names and addresses of the domain owner, domain names, host of the sites, OS details, IP details, registrar details, emails, filenames, etc.

Lab Tasks

TASK 1

Gather Information About a Target Website using Ping Command Line Utility

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Finding the IP Address of a Target Domain

3. Open the **Command Prompt** window. Type **ping www.certifiedhacker.com** and press **Enter** to find its IP address. The displayed response should be similar to the one shown in the screenshot.

Ping is a network administration utility used to test the reachability of a host on an IP network and measure the round-trip time for messages sent from the originating host to a destination computer

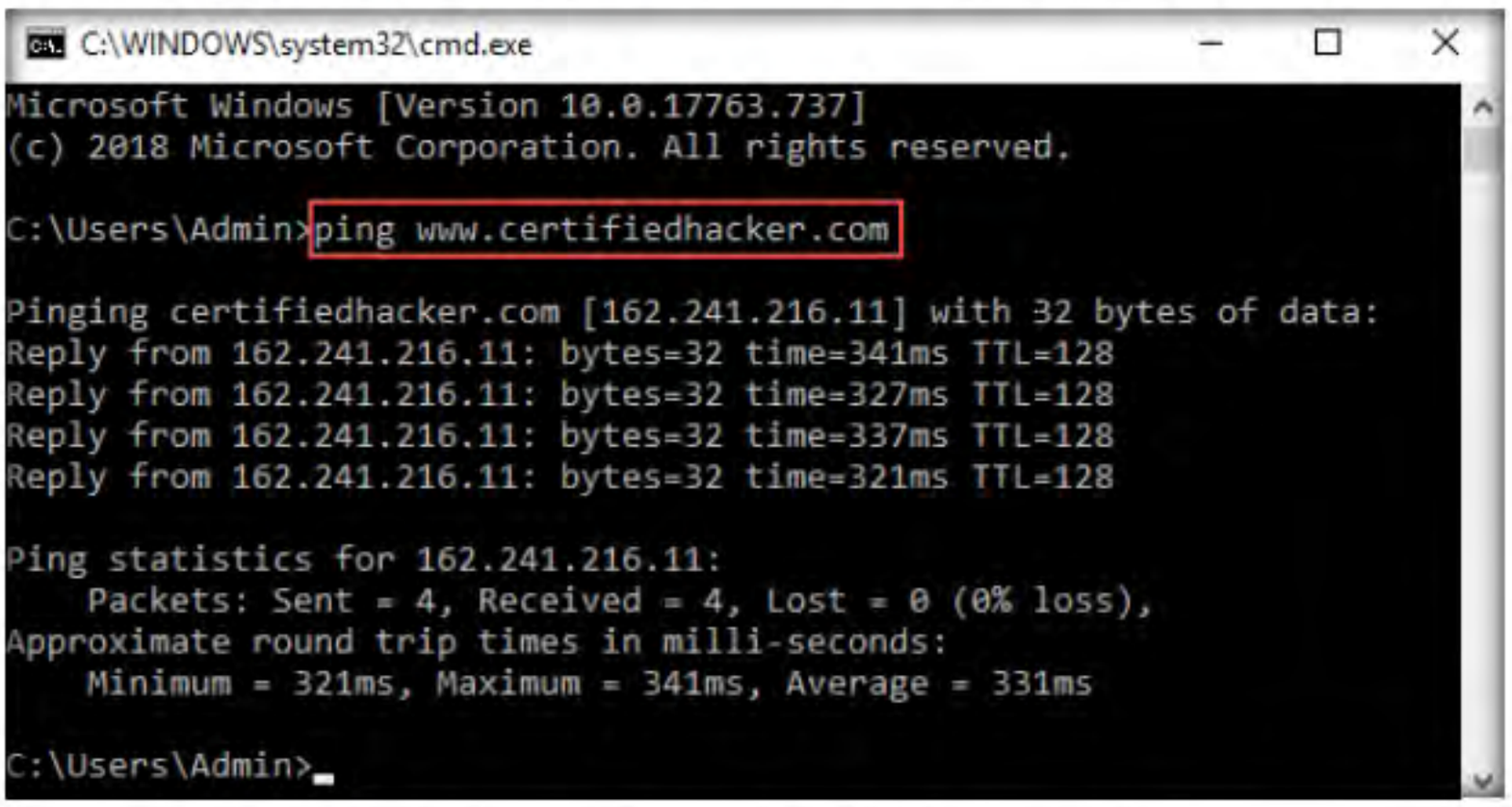


Figure 4.1.1: The ping command to extract the IP address for www.certifiedhacker.com

4. Note the target domain's IP address in the result above (here, **162.241.216.11**). You also obtain information on Ping Statistics such as packets sent, packets received, packets lost, and approximate round-trip time.

Note: The IP address of the target website may differ in your lab environment.

TASK 1.2

Finding Maximum Frame Size

5. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1500** and press **Enter**.

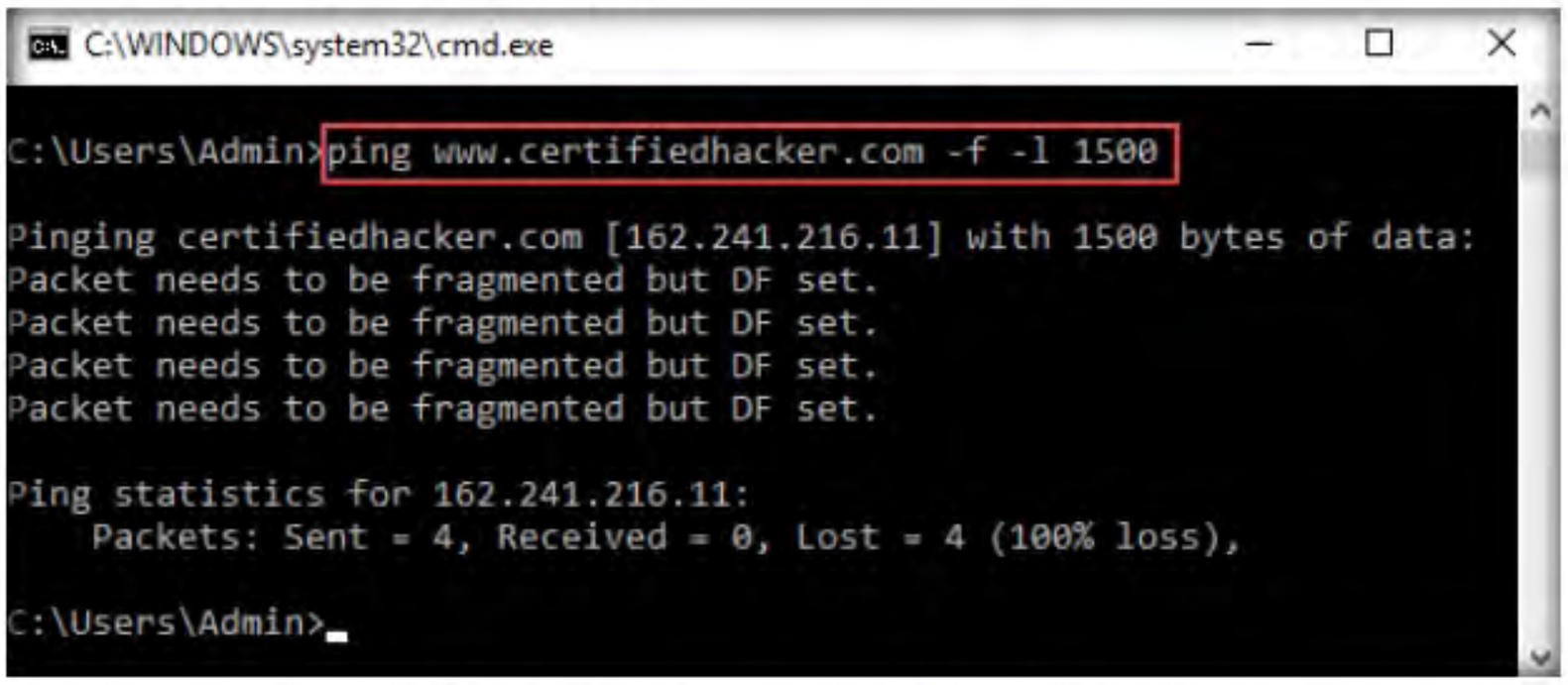


Figure 4.1.2: The ping command for www.certifiedhacker.com with -f -l 1500 options

The ping command sends an ICMP echo request to the target host and waits for an ICMP response. During this request-response process, ping measures the time from transmission to reception, known as round-trip time, and records any loss of packets. The ping command assists in obtaining domain information and the IP address of the target website.

6. The response, **Packet needs to be fragmented but DF set**, means that the frame is too large to be on the network and needs to be fragmented. The packet was not sent as we used the **-f** switch with the ping command, and the ping command returned this error.

7. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1300** and press **Enter**.

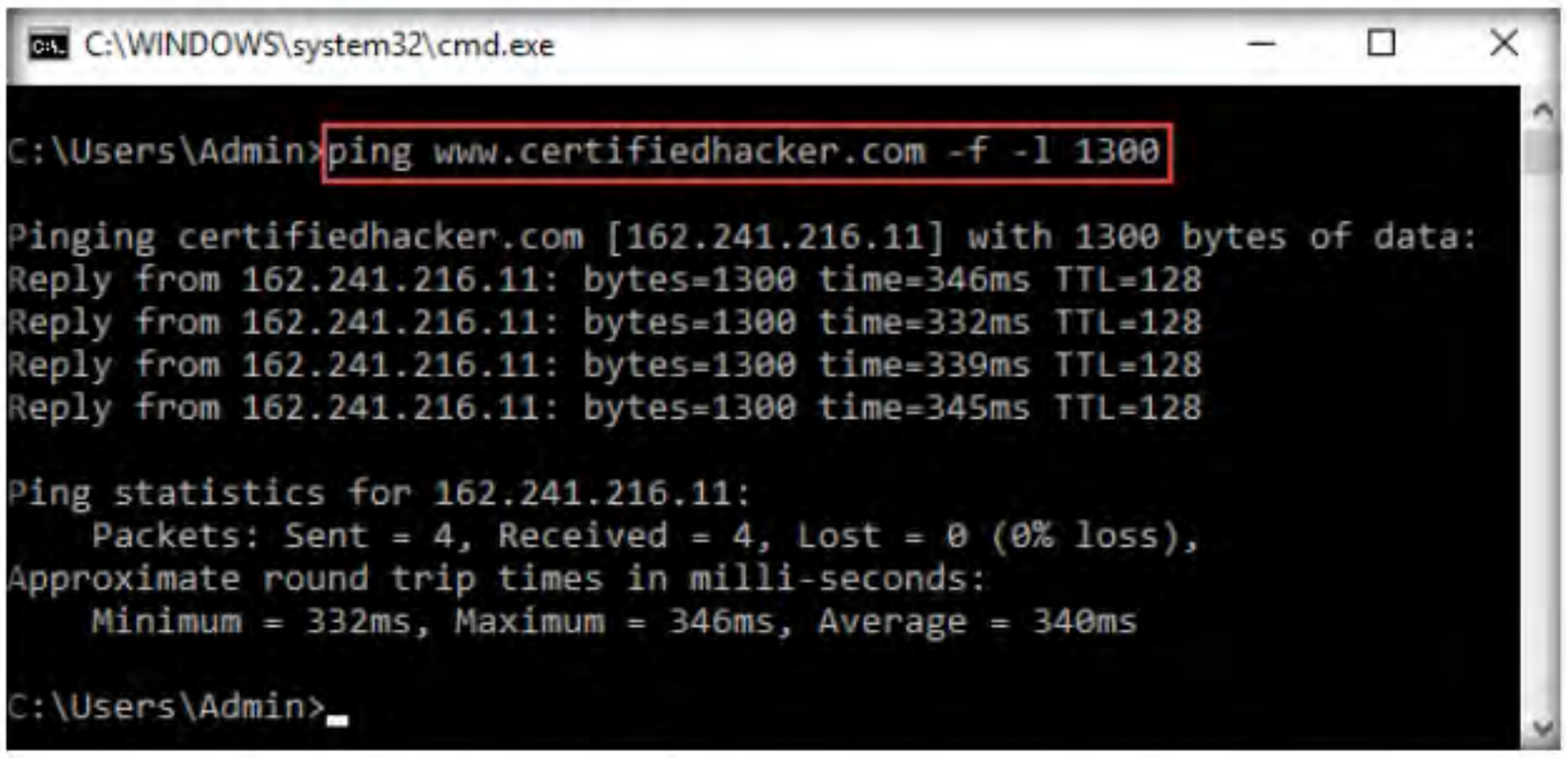


Figure 4.1.3: The ping command for www.certifiedhacker.com with -f -l 1300 options

8. Observe that the maximum packet size is less than **1500** bytes and more than **1300** bytes.

9. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com -f -l 1473** replies with **Packet needs to be fragmented but DF set**, and **ping www.certifiedhacker.com -f -l 1472** replies with a successful ping. It indicates that **1472** bytes are the maximum frame size on this machine's network.

Note: The maximum frame size will differ depending upon the target network.

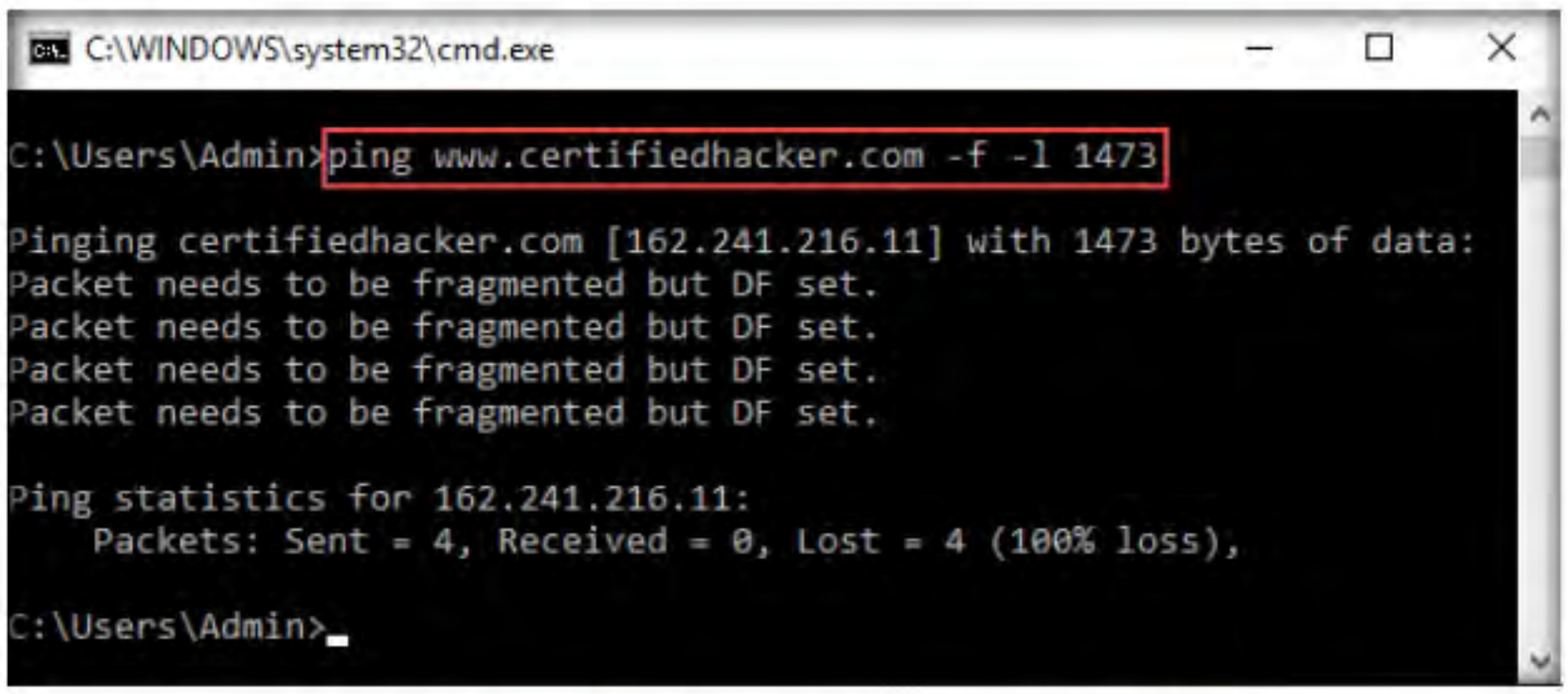


Figure 4.1.4: The ping command for www.certifiedhacker.com with -f -l 1473 options

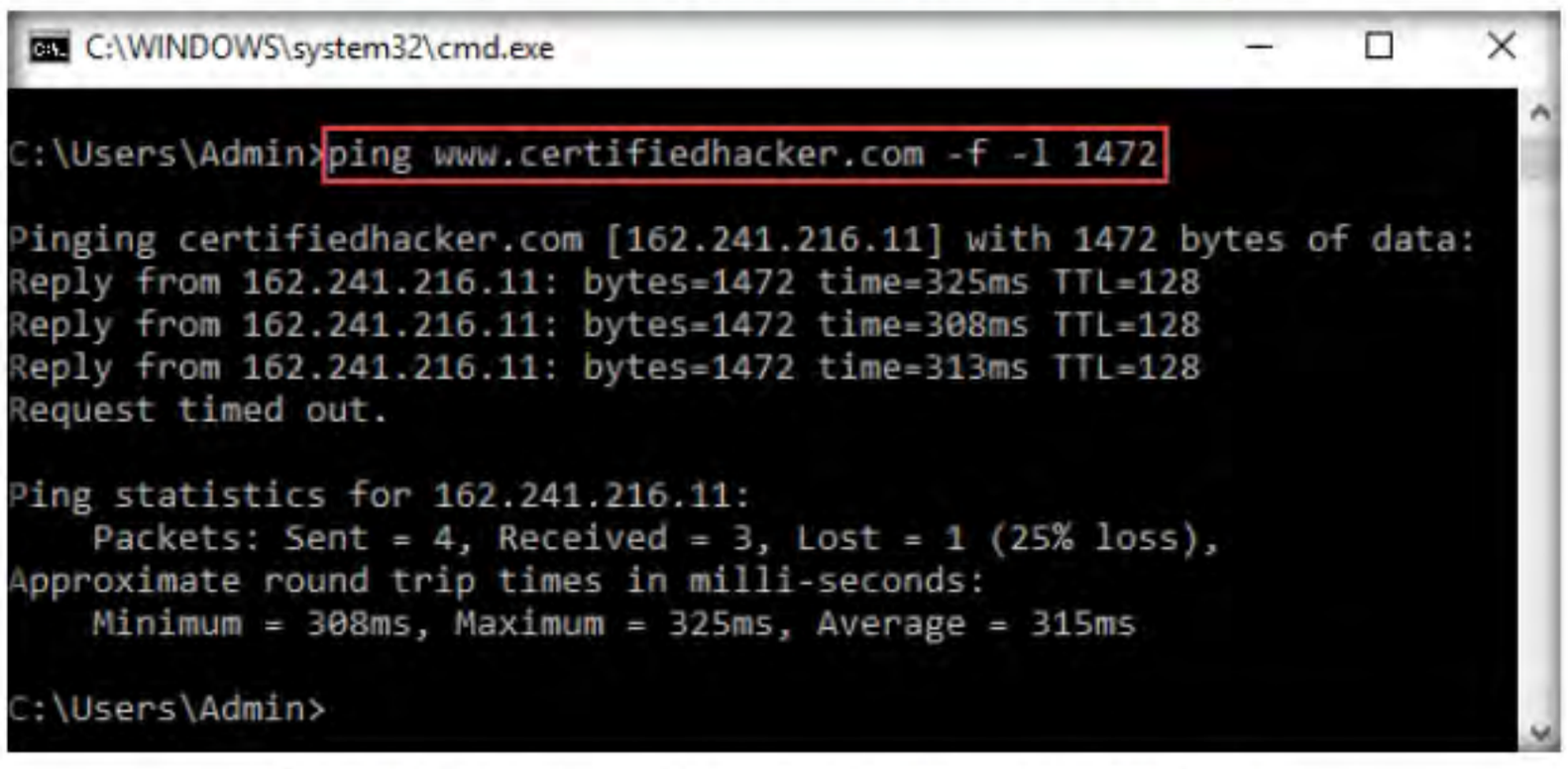


Figure 4.1.5: The ping command for www.certifiedhacker.com with -f -l 1472 options

10. Now, discover what happens when TTL (Time to Live) expires. Every frame on the network has TTL defined. If TTL reaches 0, the router discards the packet. This mechanism prevents the loss of packets.

TASK 1.3

Finding Hop Count using TTL Value

11. In **Command Prompt**, type **ping www.certifiedhacker.com -i 3** and press **Enter**. This option sets the time to live (**-i**) value as **3**.

Note: The maximum value you can set for TTL is 255.

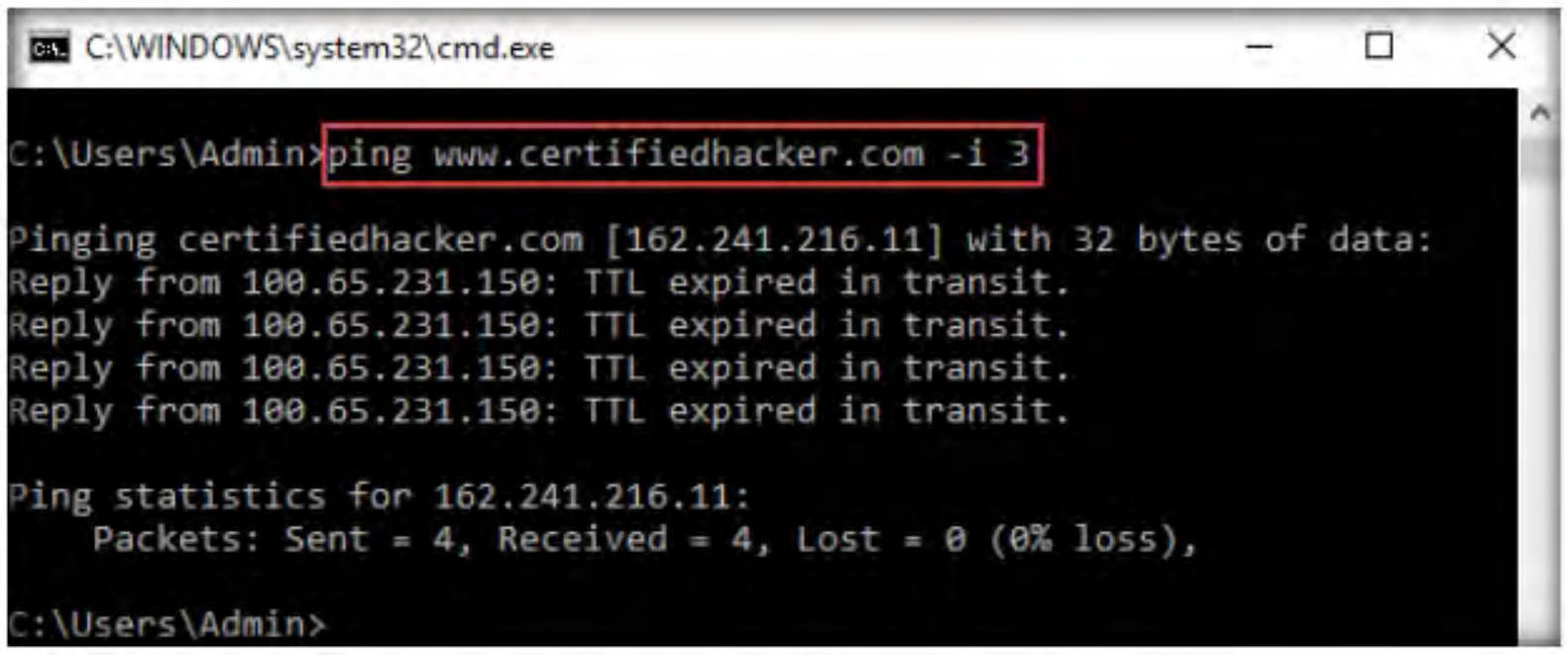


Figure 4.1.6: The ping command for www.certifiedhacker.com with –i 3 options

12. **Reply from 100.65.231.150: TTL expired in transit** means that the router (100.65.231.150, students will have some other IP address) discarded the frame because its TTL has expired (reached 0).

Note: The IP address 100.65.231.150 may vary in your lab environment.

Note: If you get the **Request timed out** reply for the above query, then use **Command Prompt of your host machine** instead of the Windows 10 virtual machine to run the query.

13. Minimize the command prompt shown above and launch a new **command prompt**. Type **ping www.certifiedhacker.com -i 2 -n 1** and press **Enter**. Here, we set the TTL value to **2** and the **-n** value to 1 to check the life span of the packet.

Note: **-n** specifies the number of echo requests to be sent to the target.

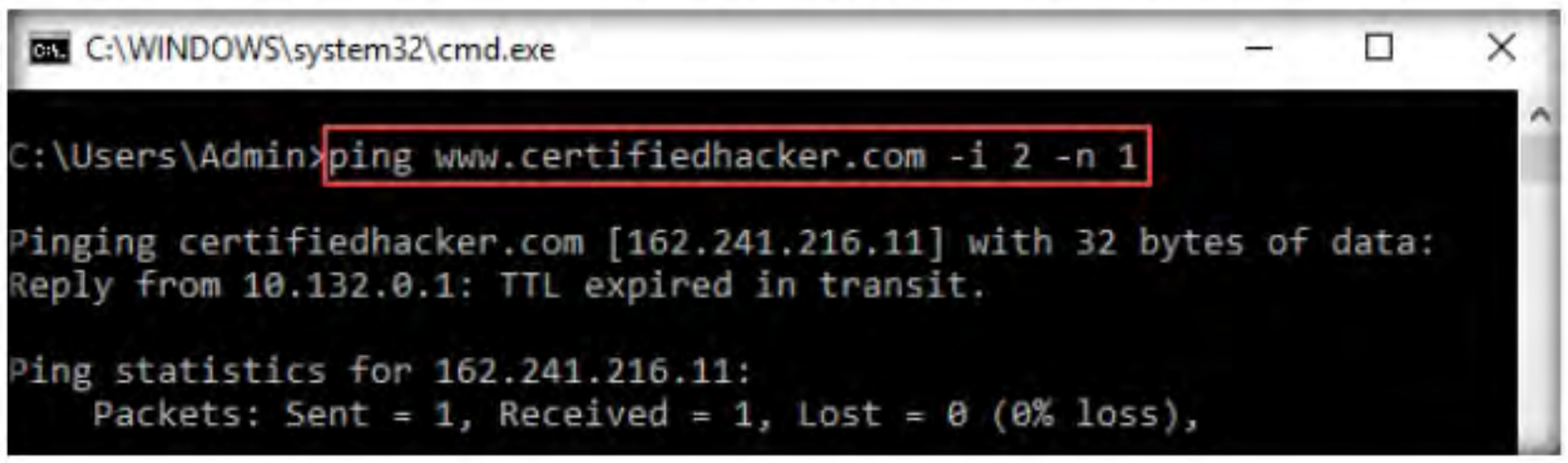


Figure 4.1.7: The ping command for www.certifiedhacker.com with –i 2 –n 1 options

14. Type **ping www.certifiedhacker.com -i 3 -n 1**. This sets the TTL value to **3**.

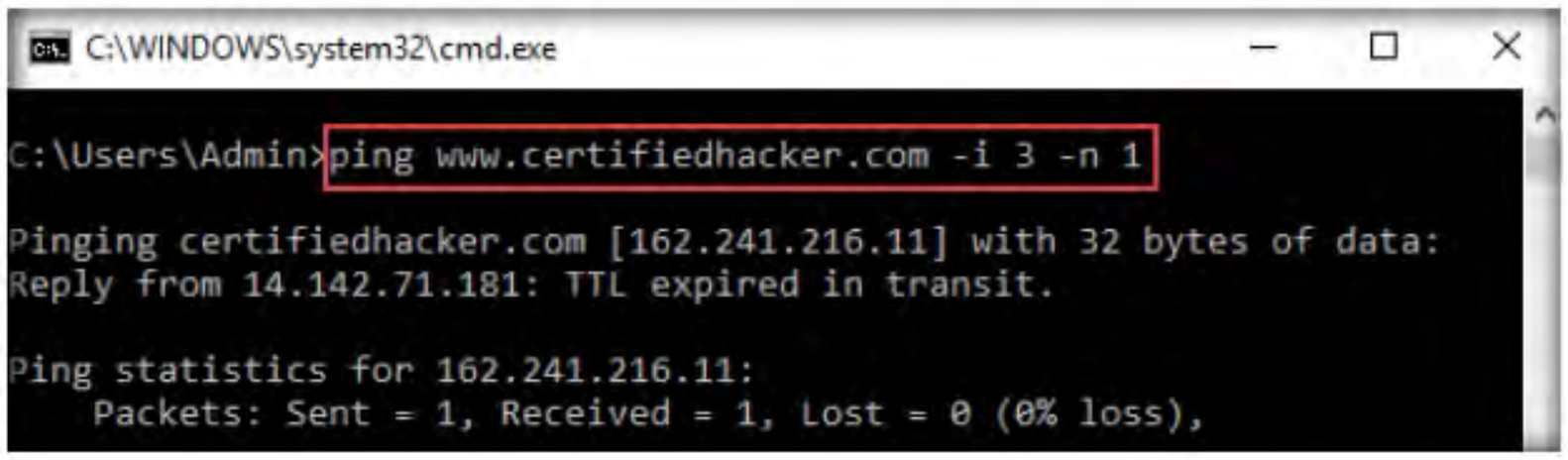


Figure 4.1.8: The ping command for www.certifiedhacker.com with –i 3 –n 1 options

15. Observe that there is a reply coming from the IP address **162.241.216.11**, and there is no packet loss.

Note: The result displayed in the above step might differ in your lab environment.

16. Now, change the time to live value to **4** by typing, **ping www.certifiedhacker.com -i 4 -n 1** and press **Enter**.

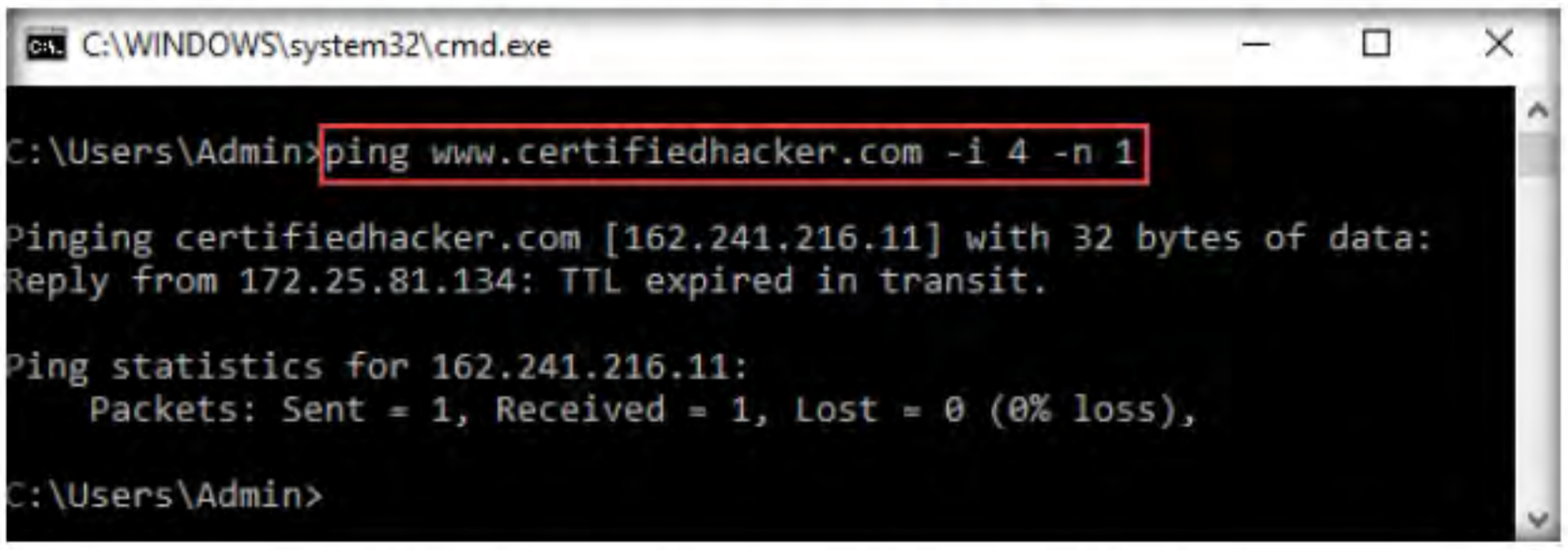


Figure 4.1.9: The ping command for www.certifiedhacker.com with –i 4 –n 1 options

17. Repeat the above step until you reach the IP address for **www.certifiedhacker.com** (in this case, **162.241.216.11**).

18. Here, the successful ping to reach **www.certifiedhacker.com** is **27** hops.

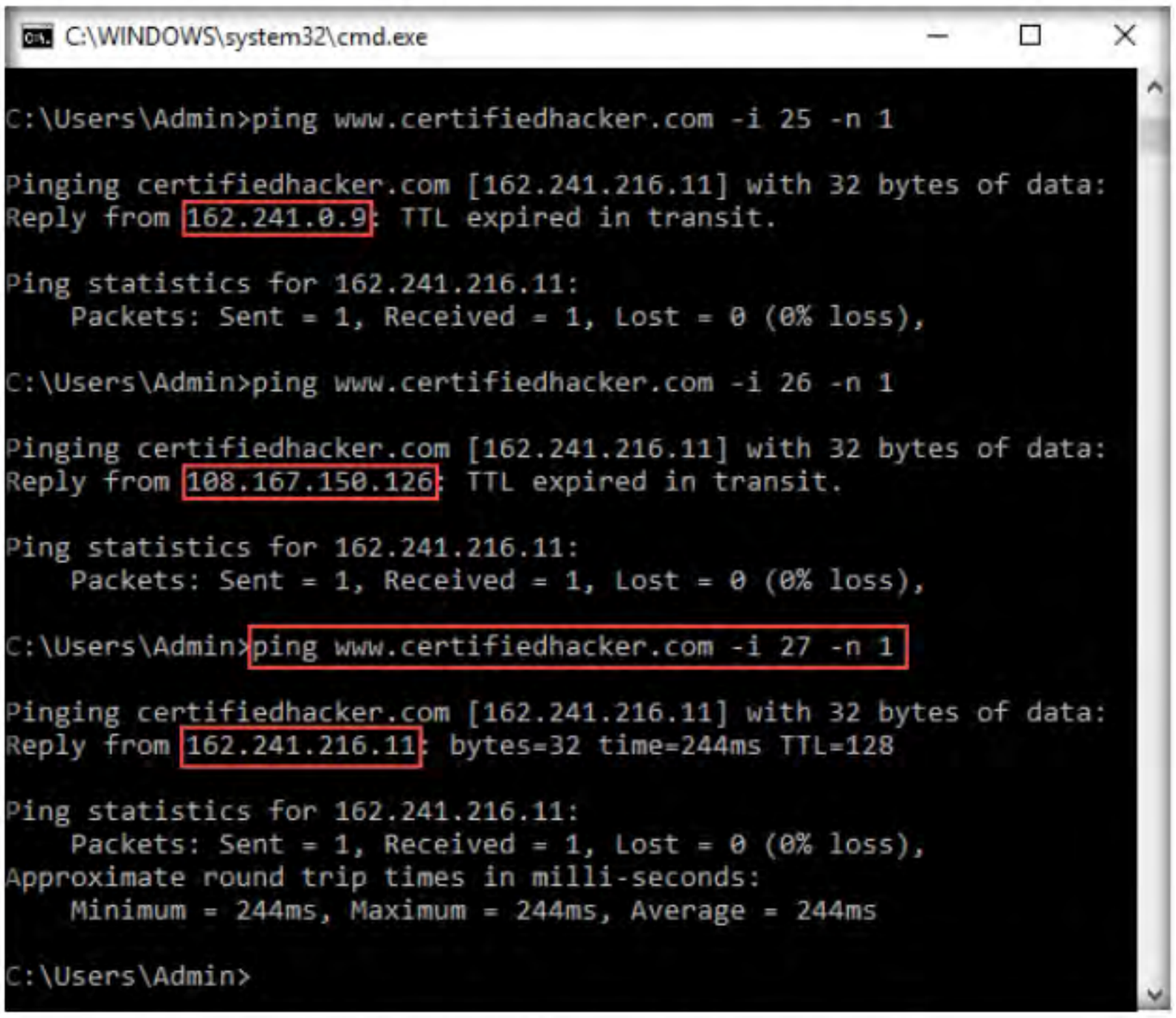


Figure 4.1.10: The ping command for www.certifiedhacker.com with –i 27 –n 1

19. This implies that, at a time to live value of **27**, the reply is received from the destination host (**162.241.216.11**).

Note: The result might vary in your lab environment.

20. This concludes the demonstration of gathering information about a target website using Ping command-line utility (such as the IP address of the target website, hop count to the target, and value of maximum frame size allowed on the target network).

21. Close all open windows and document all the acquired information.

TASK 2 Gather Information about a Target Website using Website Informer

Website Informer is an online tool that gathers detailed information on a website such as a website's traffic rank, daily visitors rate, page views, etc. Website Informer discovers the main competitors of the website, reveals DNS servers used by the website, and also obtains the Whois record of the target website.

1. In the **Windows 10** virtual machine, open a web browser (here, **Mozilla Firefox**), type **https://website.informer.com** in the address bar, and press **Enter**. The Website Informer website appears, as shown in the screenshot.

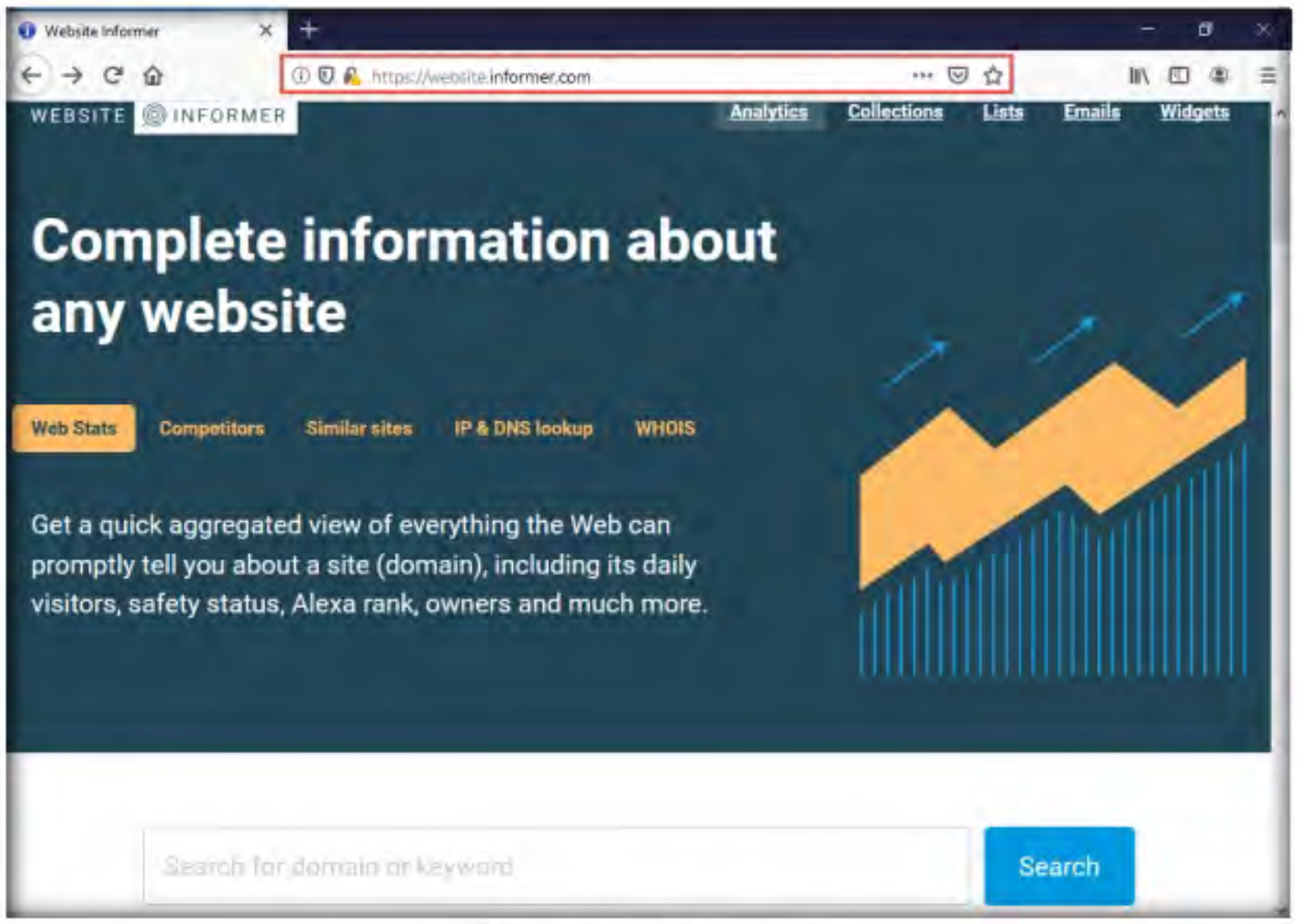


Figure 4.2.1: Website Informer website

2. To extract information associated with the target organization website, type the target website's URL (here, **www.certifiedhacker.com**) in the text field, and then click on the **Search** button, as shown in the screenshot below.

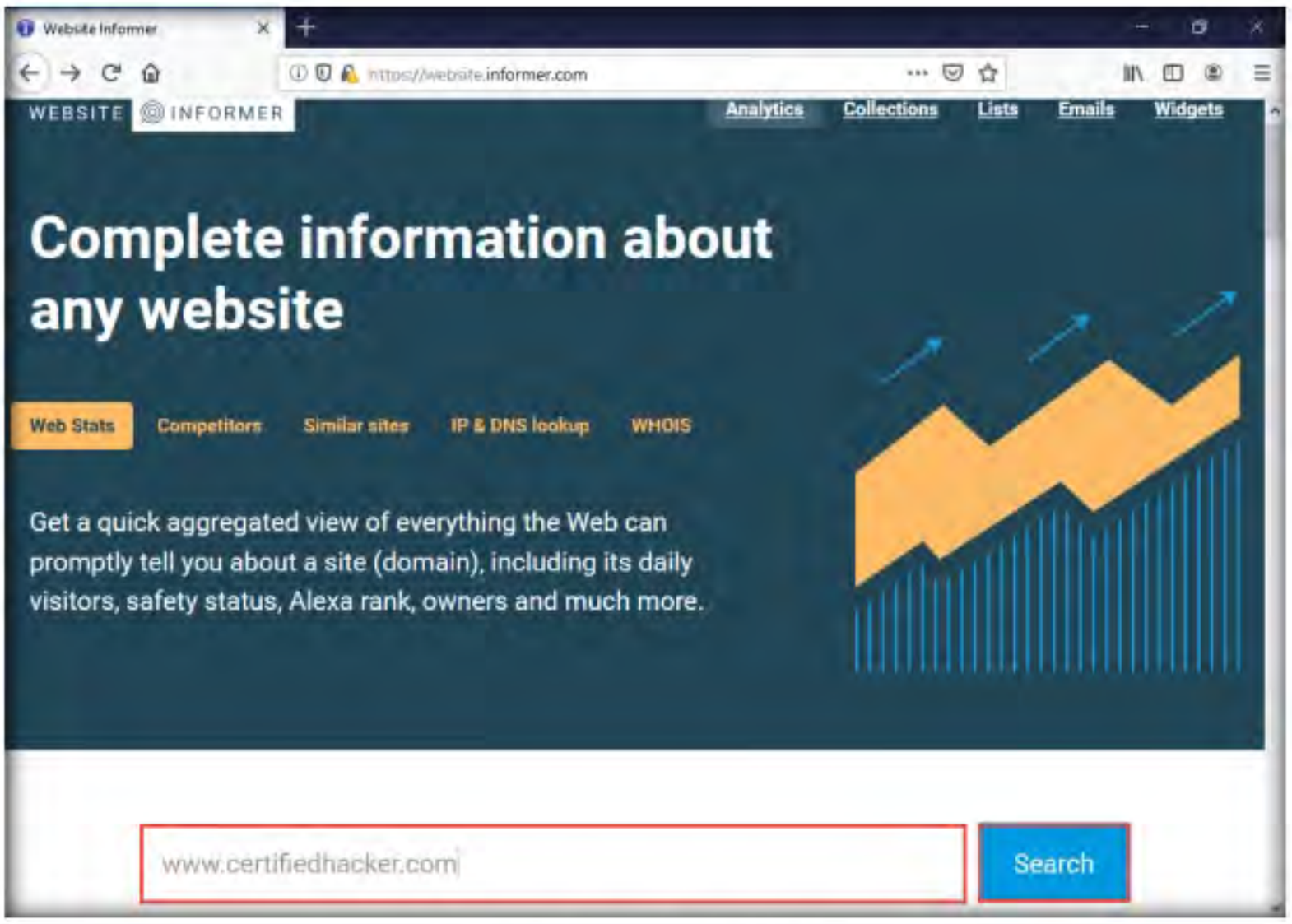


Figure 4.2.2: Enter the target website

3. A search result for **WWW.CERTIFIEDHACKER.COM** containing information such as **General Info**, **Stats & Details**, **Whois**, and **IP Whois** is displayed, as shown in the screenshot.

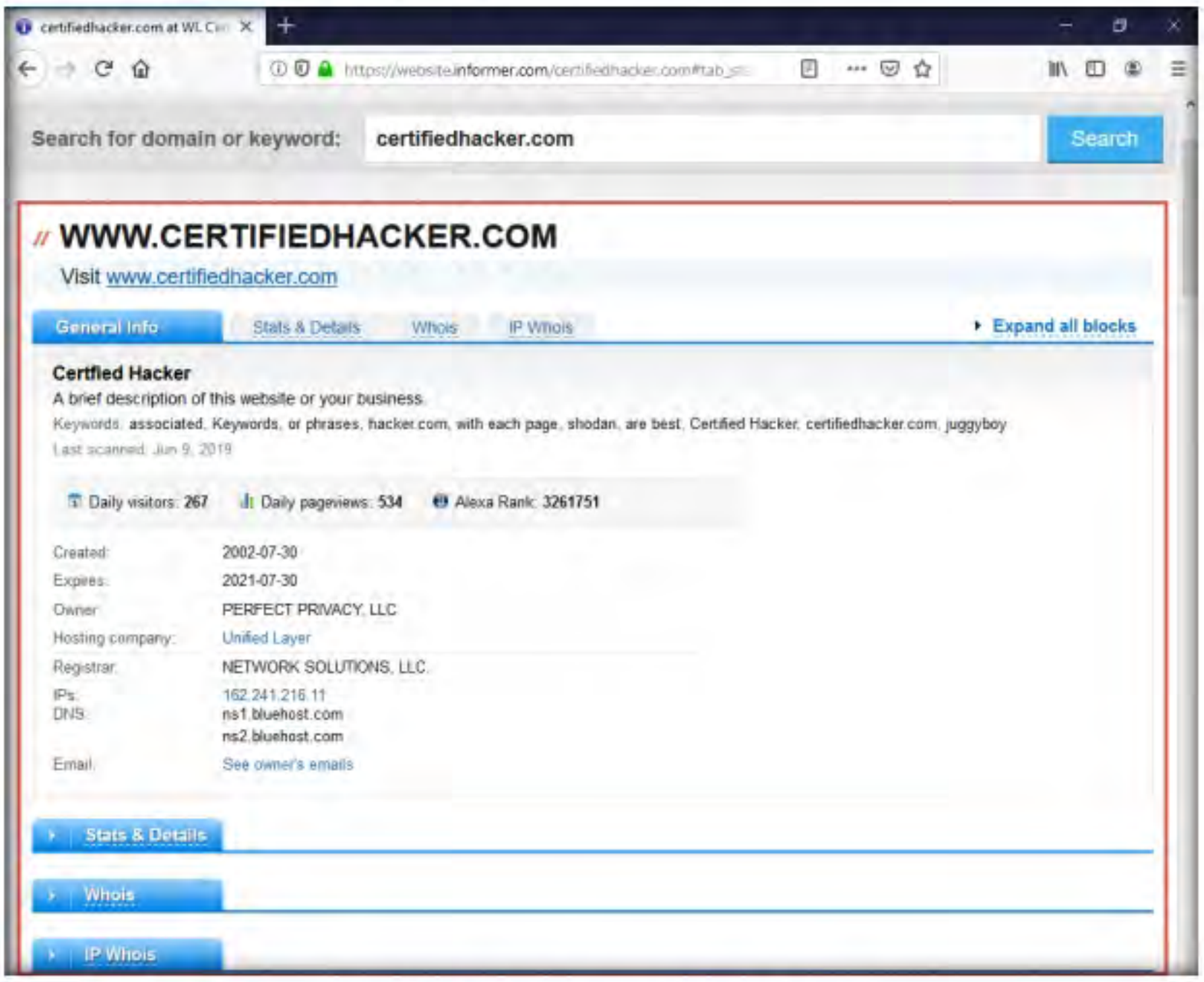


Figure 4.2.3: Search result generated by Website Informer

4. In the **General Info** tab, information such as **Created**, **Expires**, **Owner**, **Hosting company**, **Registrar**, **IPs**, **DNS**, and **Email** associated with the target website is displayed as shown in the screenshot.

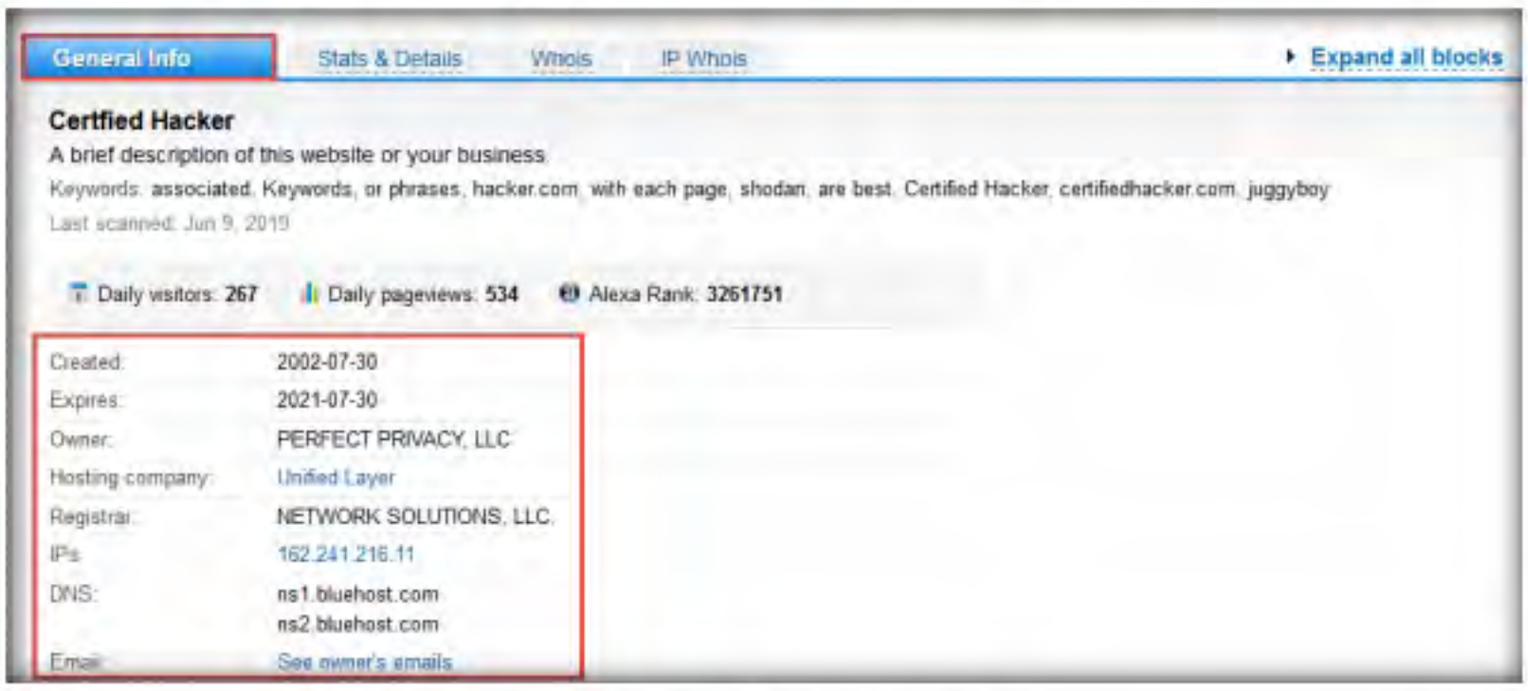


Figure 4.2.4: Website Informer General Info

5. Click on the **Whois** tab to view detailed Whois information about the target website, as shown in the screenshot.

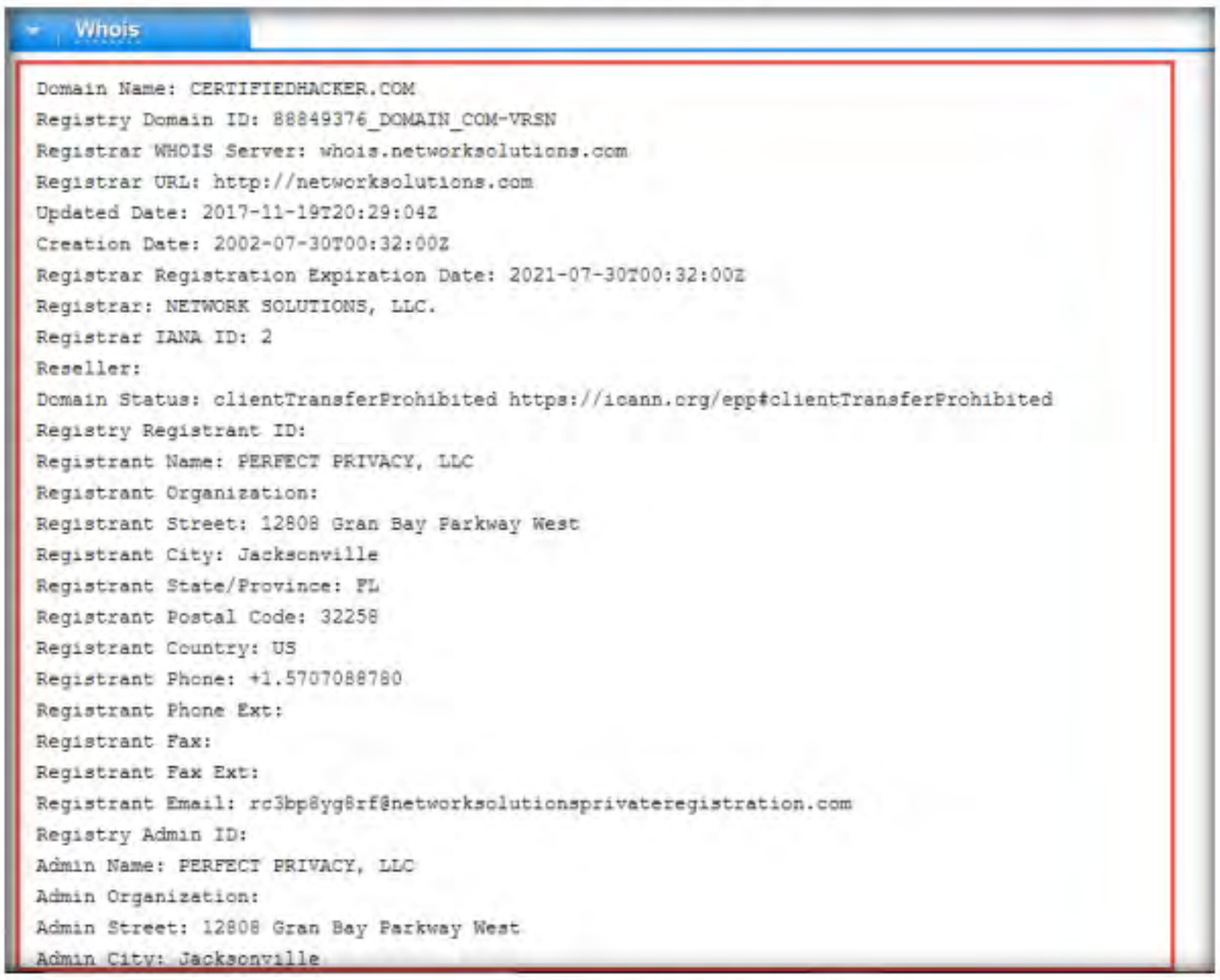


Figure 4.2.5: Website Informer Whois information

You can also use tools such as **Burp Suite** (https://portswigger.net), **Zaproxy** (https://www.owasp.org), etc. to perform website footprinting on a target website.

6. Similarly, you can click on the **Stats & Details** and **IP Whois** tabs to view the detailed information of the target website.
7. This concludes the demonstration of gathering information about a target website using the Website Informer online tool.
8. Close all open windows and document all the acquired information.

TASK 3 Extract a Company's Data using Web Data Extractor

Here, we will gather the target company's data using the Web Data Extractor tool.

TASK 3.1

Install Web Data Extractor

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wde.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard steps to install Web Data Extractor and click **Finish**.

Web data extraction is the process of extracting data from web pages available on the company's website. A company's data such as contact details (email, phone, and fax), URLs, meta tags (title, description, keyword) for website promotion, directories, web research, etc. are important sources of information for an ethical hacker.

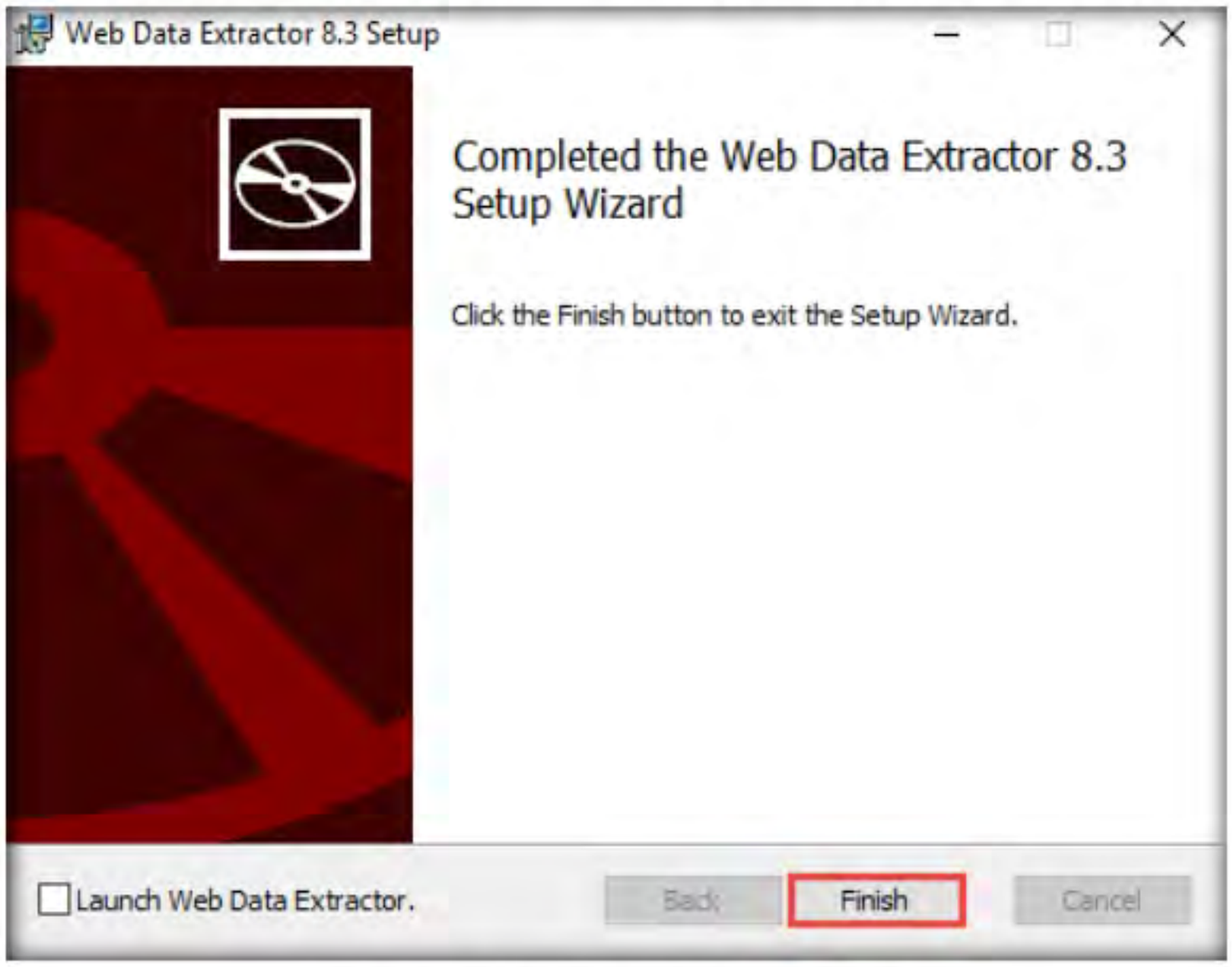


Figure 4.3.1: Web Data Extractor Setup Pop-up Wizard

Web spiders (also known as a web crawler or web robot) such as Web Data Extractor perform automated searches on the target website and extract specified information from the target website.

4. After installation, launch **Web Data Extractor** from **Desktop**.

Figure 4.3.2: Installed apps in Windows 10 - Selecting Web Data Extractor

TASK 3.2

Configure Web Data Extractor

5. The **Web Data Extractor** main window appears. Click **New** to start a new session.

Figure 4.3.3: The Web Data Extractor main window

6. The **Session settings** window appears; type a URL (here, **http://www.certifiedhacker.com**) in the **Starting URL** field. Check all the options, as shown in the screenshot, and click **OK**.

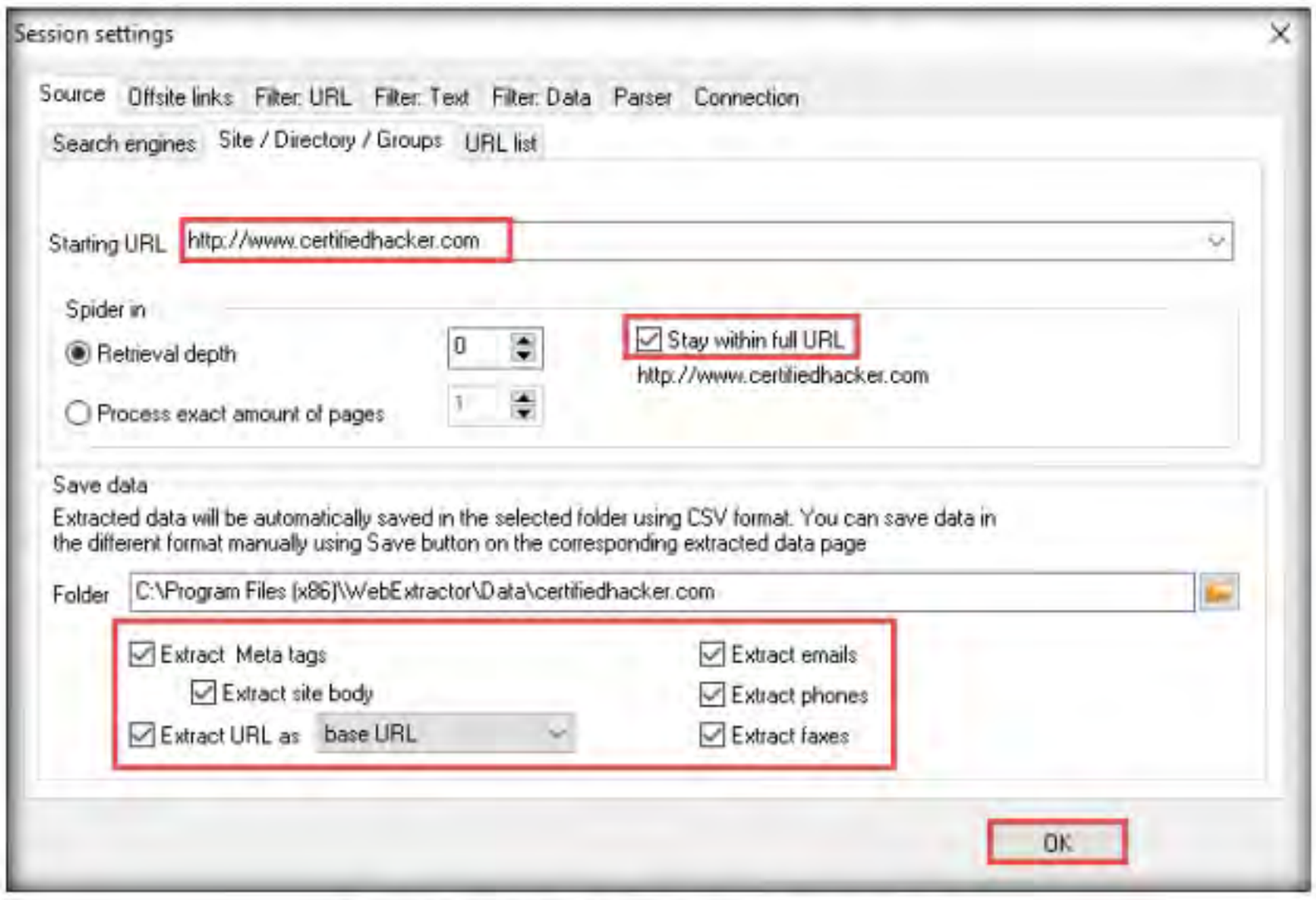


Figure 4.3.4: Web Data Extractor - Session settings window

TASK 3.3

Extract Target Website Data

7. Click **Start** to initiate the data extraction.

Figure 4.3.5: Web Data Extractor initiating the data extraction

8. Web Data Extractor will start collecting information (**Session**, **Meta tags**, **Emails**, **Phones**, **Faxes**, **Merged list**, **URLs**, and **Inactive sites**).

Figure 4.3.6: Web Data Extractor collecting information

9. Once the data extraction process is completed, an **Information** dialog box appears; click **OK**.

Figure 4.3.7: Web Data Extractor Data Extraction information window

10. View the extracted information by clicking the tabs.

TASK 3.4

Examine the Collected Data

Figure 4.3.8: Web Data Extractor Data Extraction window

11. Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, page size, etc.

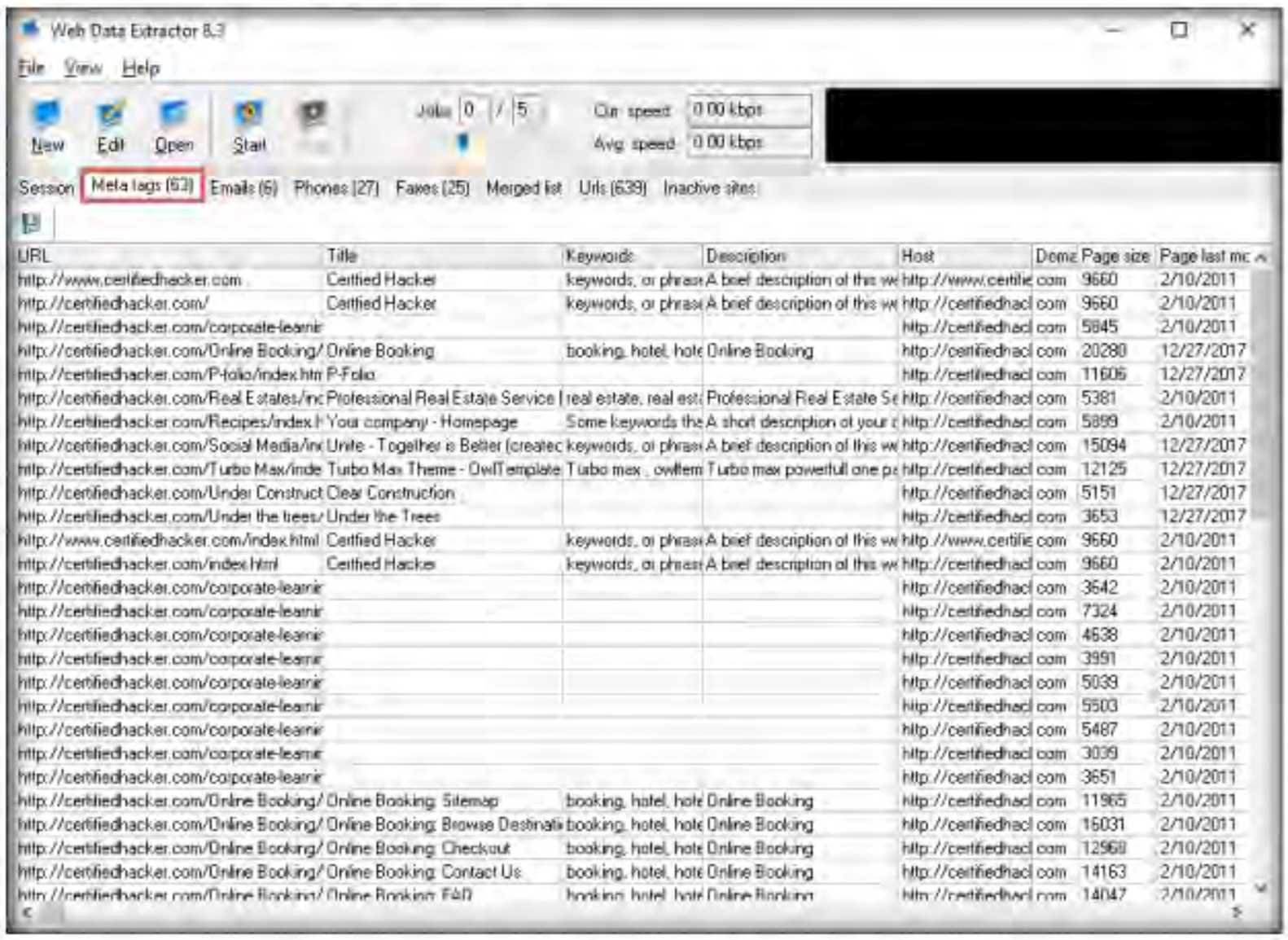


Figure 4.3.9: Web Data Extractor- Meta tags tab

12. Select the **Emails** tab to view information related to emails such as Email address, Name, URL, Title, etc.

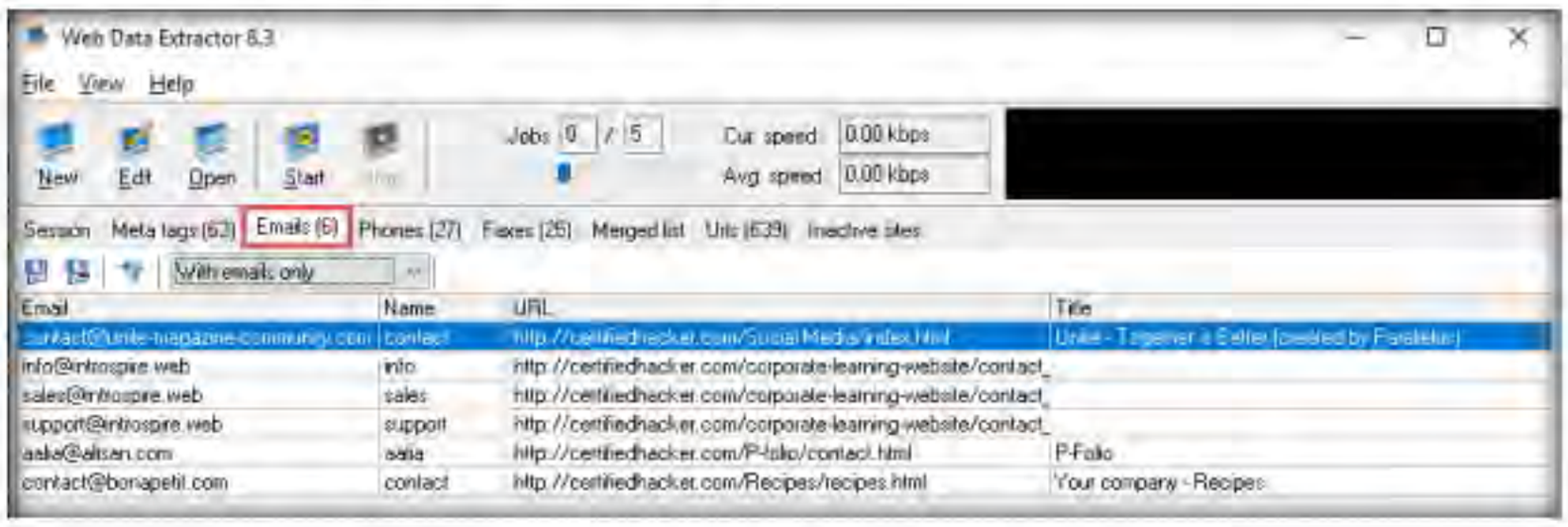


Figure 4.3.10: Web Data Extractor- Emails tab

13. Select the **Phones** tab to view the Phone, Source, Tag, URL, etc.

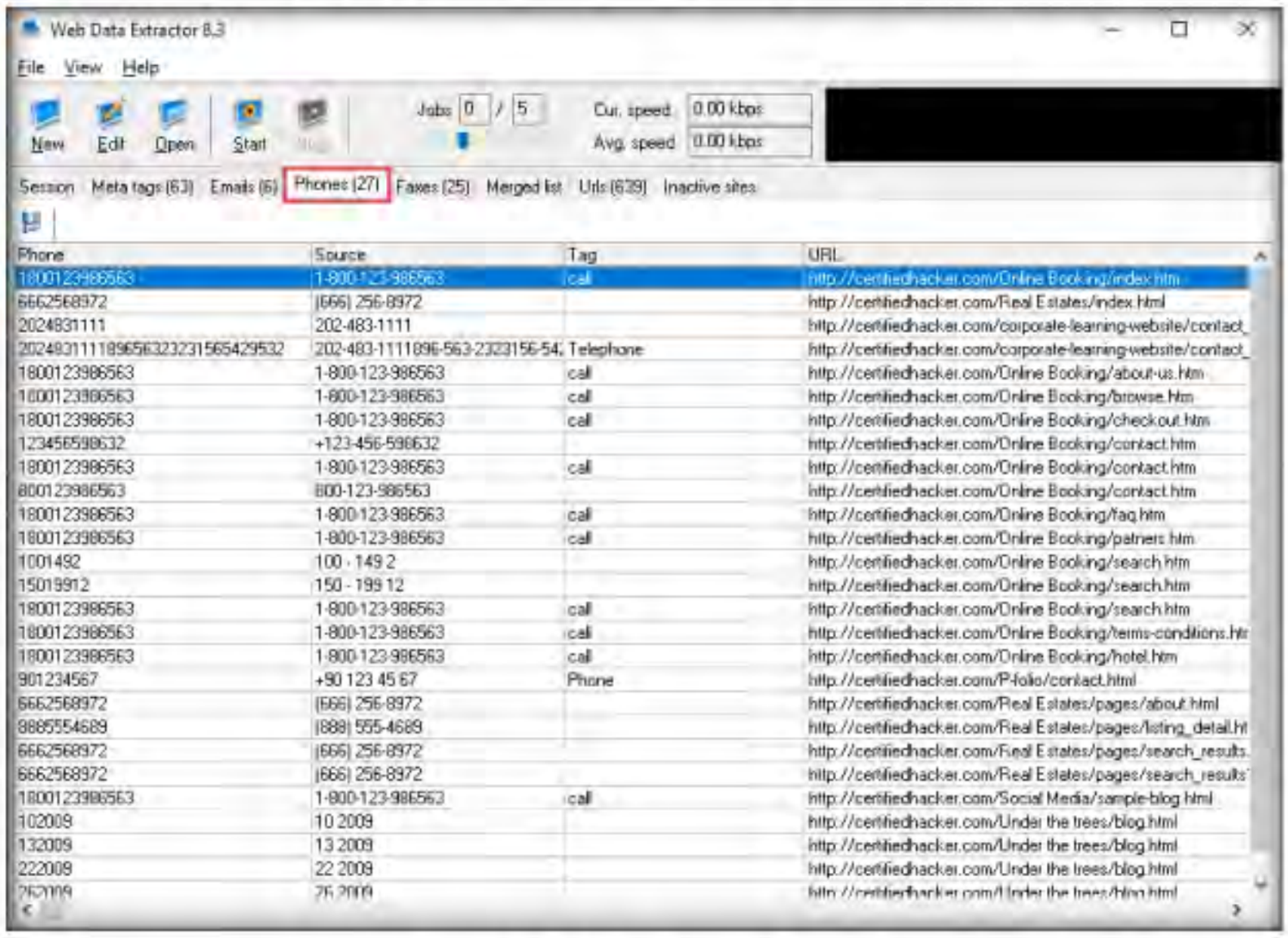


Figure 4.3.11: Web Data Extractor- Phones tab

14. Check for more information under the **Faxes**, **Merged list**, **URLs**, and **Inactive sites** tabs.

15. To save the session, choose **File** and click **Save session**.

TASK 3.5

Save a Session

Figure 4.3.12: Web Data Extractor session saving window

16. Specify the session name (here, **certifiedhacker.com**) in the **Save session** dialog box and click **OK**.

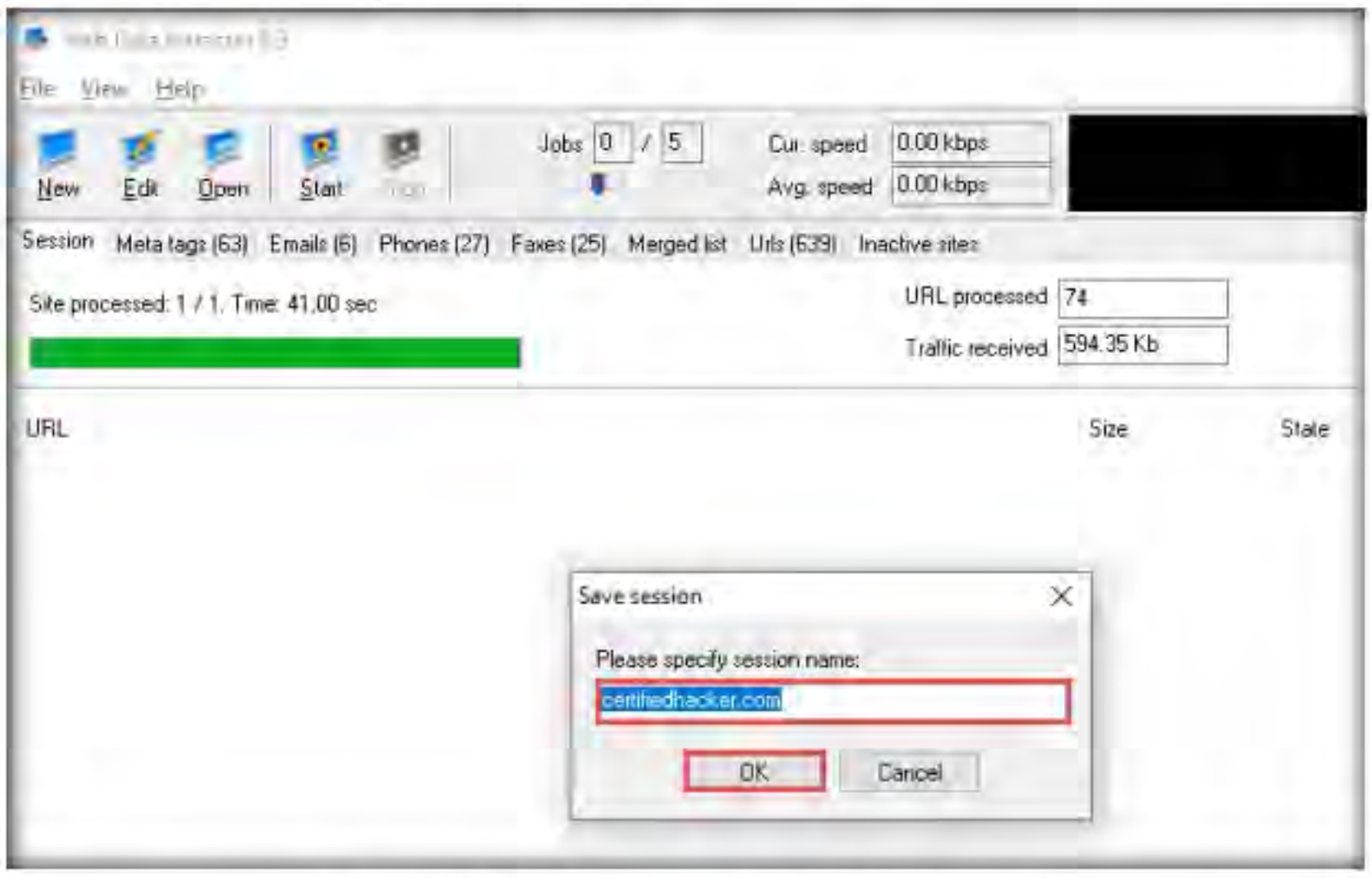


Figure 4.3.13: Web Data Extractor specifying the session name

17. Click the **Meta tags** tab, and then click the **floppy** icon.

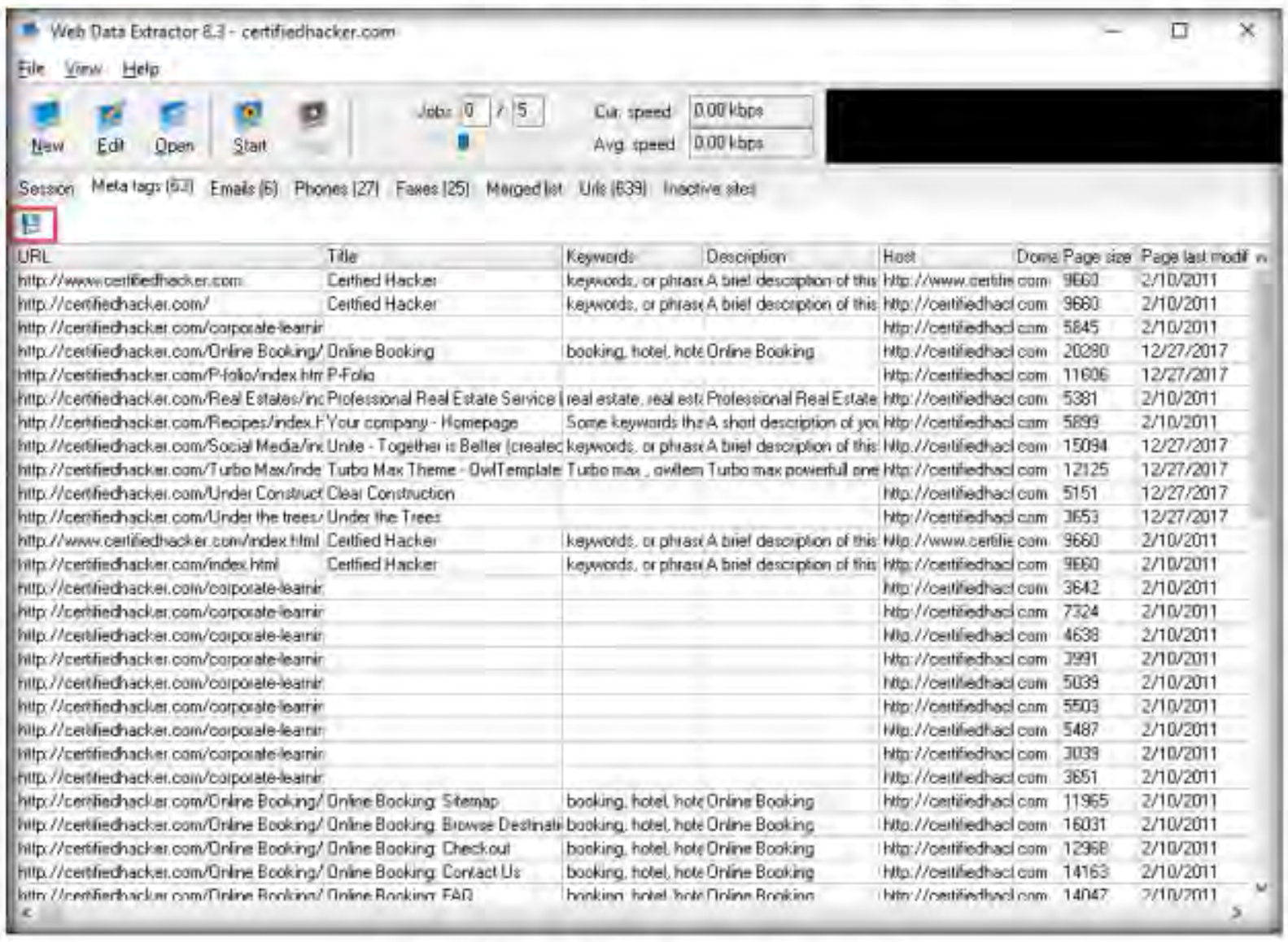


Figure 4.3.14: Web Data Extractor - Meta tags tab

18. An **Information** pop-up may appear with the message **You cannot save more than 10 records in Demo Version**; click **OK**.

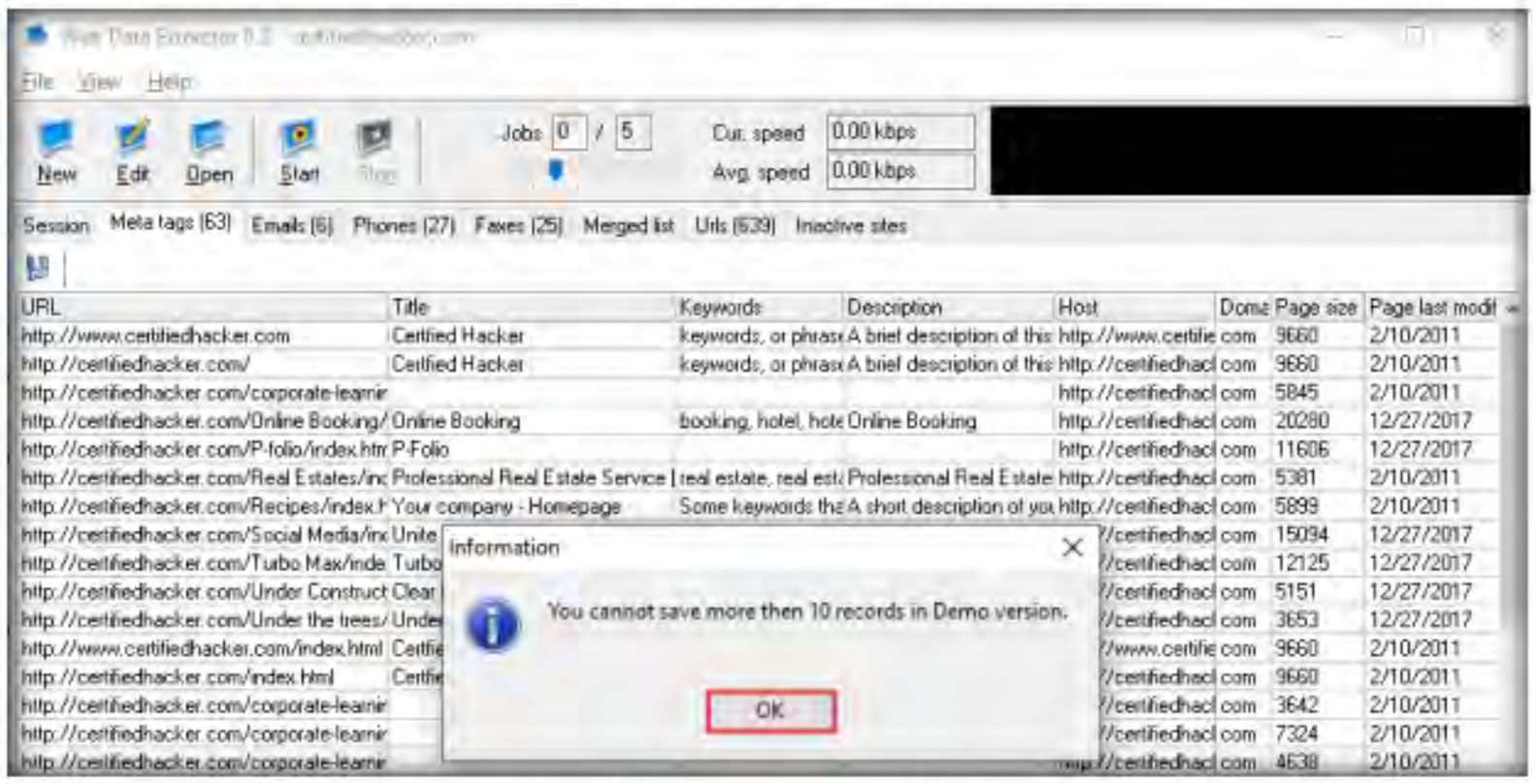


Figure 4.3.15: Web Data Extractor saving information window

19. The **Save Meta tags** window appears. In the **File name** field, click on the **folder icon**, select the location where you want to save the file, choose **File format**, and click **Save**.

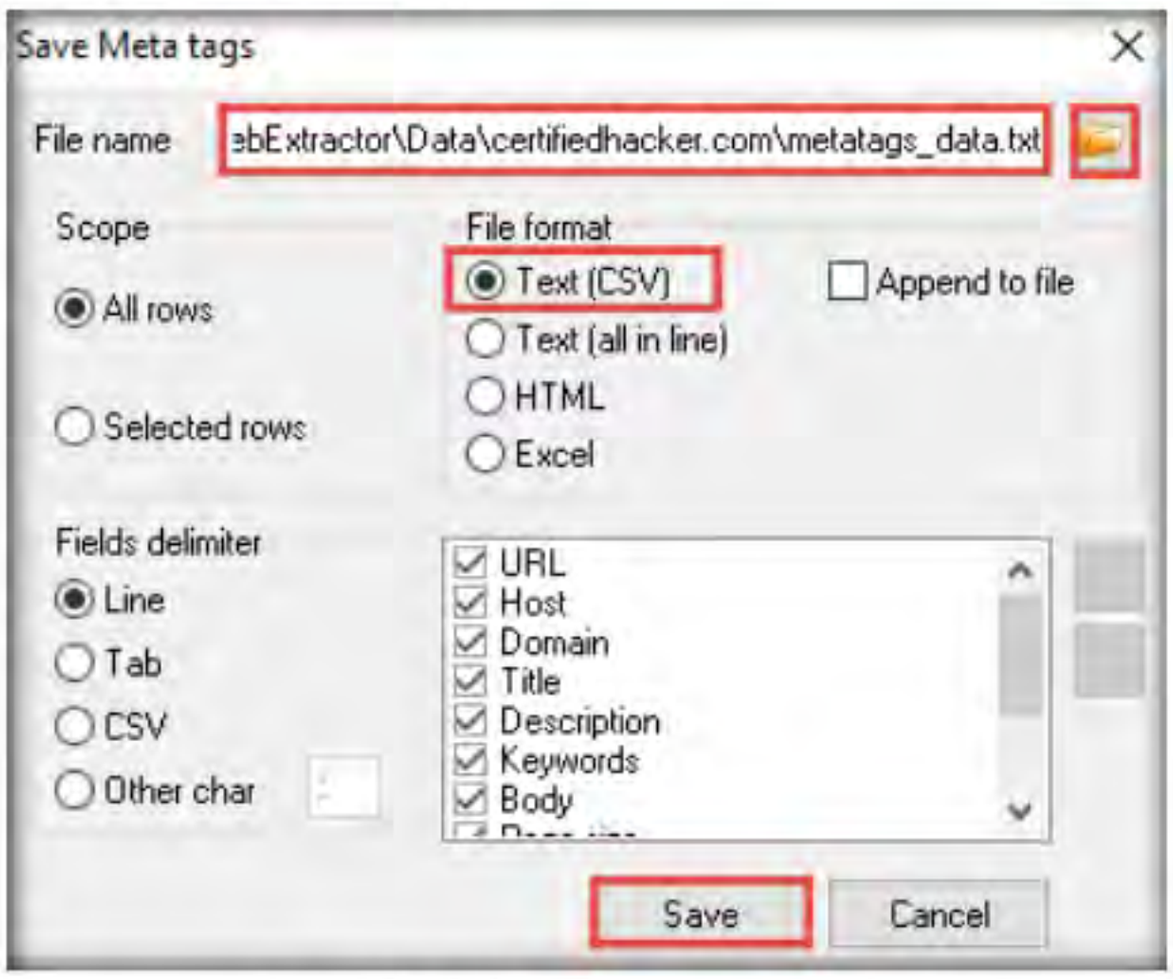


Figure 4.3.16: Web Data Extractor saving window

You can also use other web spiders such as **ParseHub** (https://www.parsehub.com), **SpiderFoot** (https://www.spiderfoot.net), etc. to extract the target organization's data.

20. By default, the session will be saved at **C:\Program Files (x86)\WebExtractor\Data\certifiedhacker.com**. You can choose your desired location to save the file.
21. This concludes the demonstration of extracting a company's data using the Web Data Extractor tool.
22. Close all open windows and document all the acquired information.

TASK 4 Mirror a Target Website using HTTrack Web Site Copier

Here, we will use the HTTrack Web Site Copier tool to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

TASK 4.1

Install HTTrack Web Site Copier

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier** and double-click **httrack-3.49.2.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard steps to install **HTTrack Web Site Copier**.
4. In the last step of the installation wizard, uncheck the **View history.txt file** option and click **Finish**.

Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos, and other files from the server on your computer.

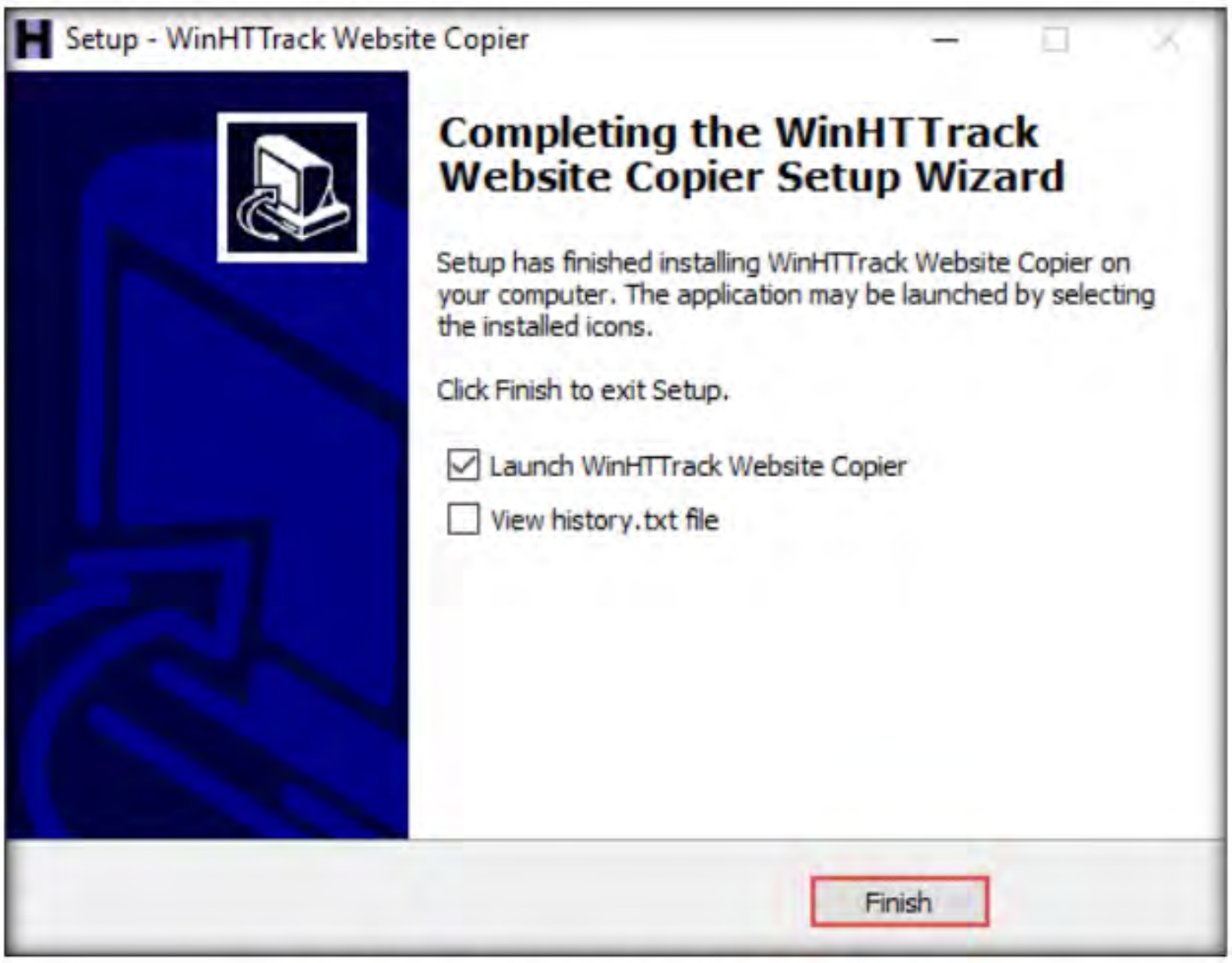


Figure 4.4.1: HTTrack Website Copier Setup Pop-up Wizard

TASK 4.2

Mirror the Target Website

5. The **WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.

Note: If the application does not launch, you can launch it manually from the **Apps** screen.

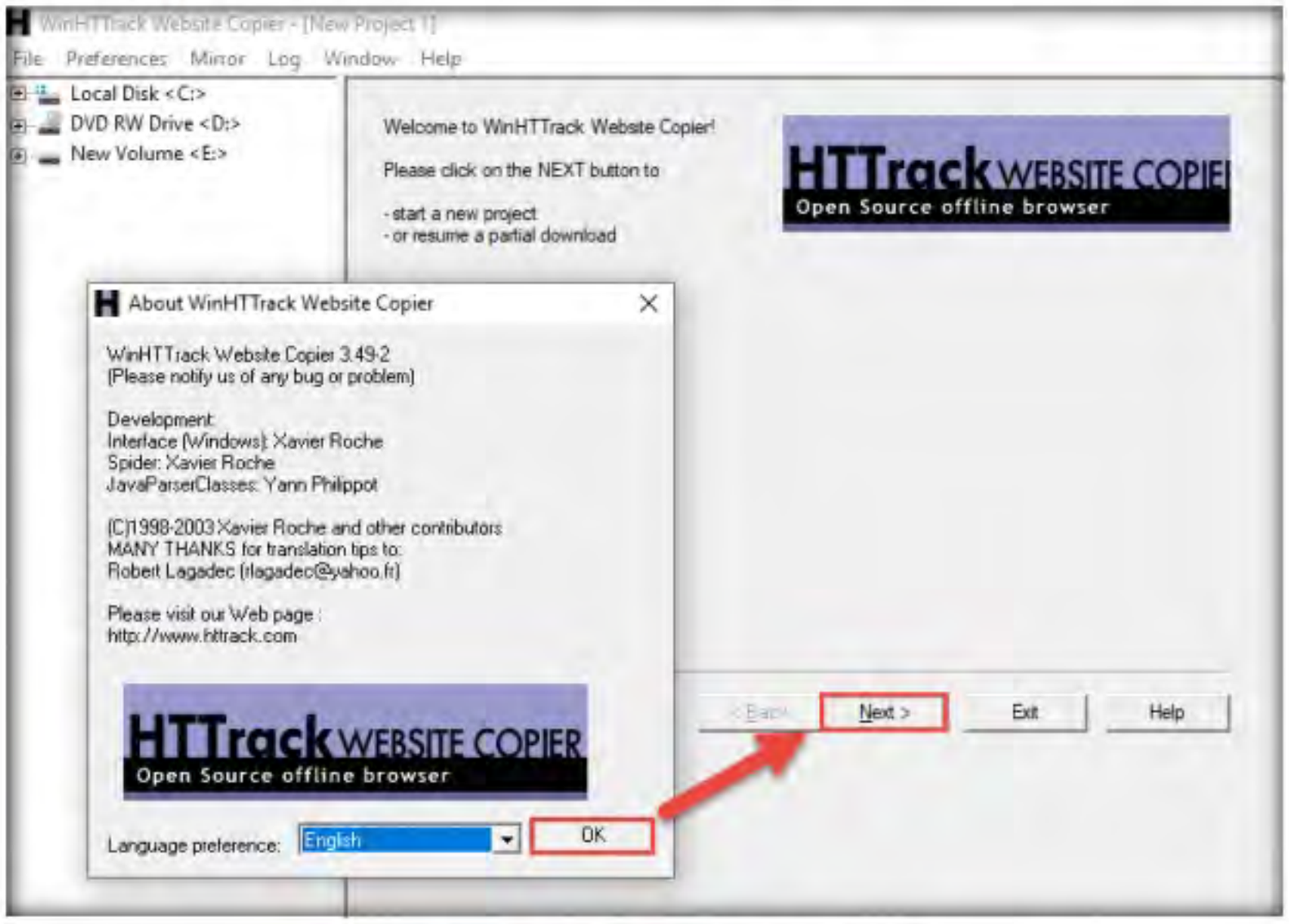


Figure 4.4.2: HTTrack Website Copier main window

You can duplicate websites by using website mirroring tools such as HTTrack Web Site Copier. HTTrack is an offline browser utility that downloads a website from the Internet to a local directory, builds all directories recursively, and transfers HTML, images, and other files from the webserver to another computer.

6. Enter the name of the project (here, **Test Project**) in the **New project name:** field. Select the **Base path:** to store the copied files; click **Next >**.

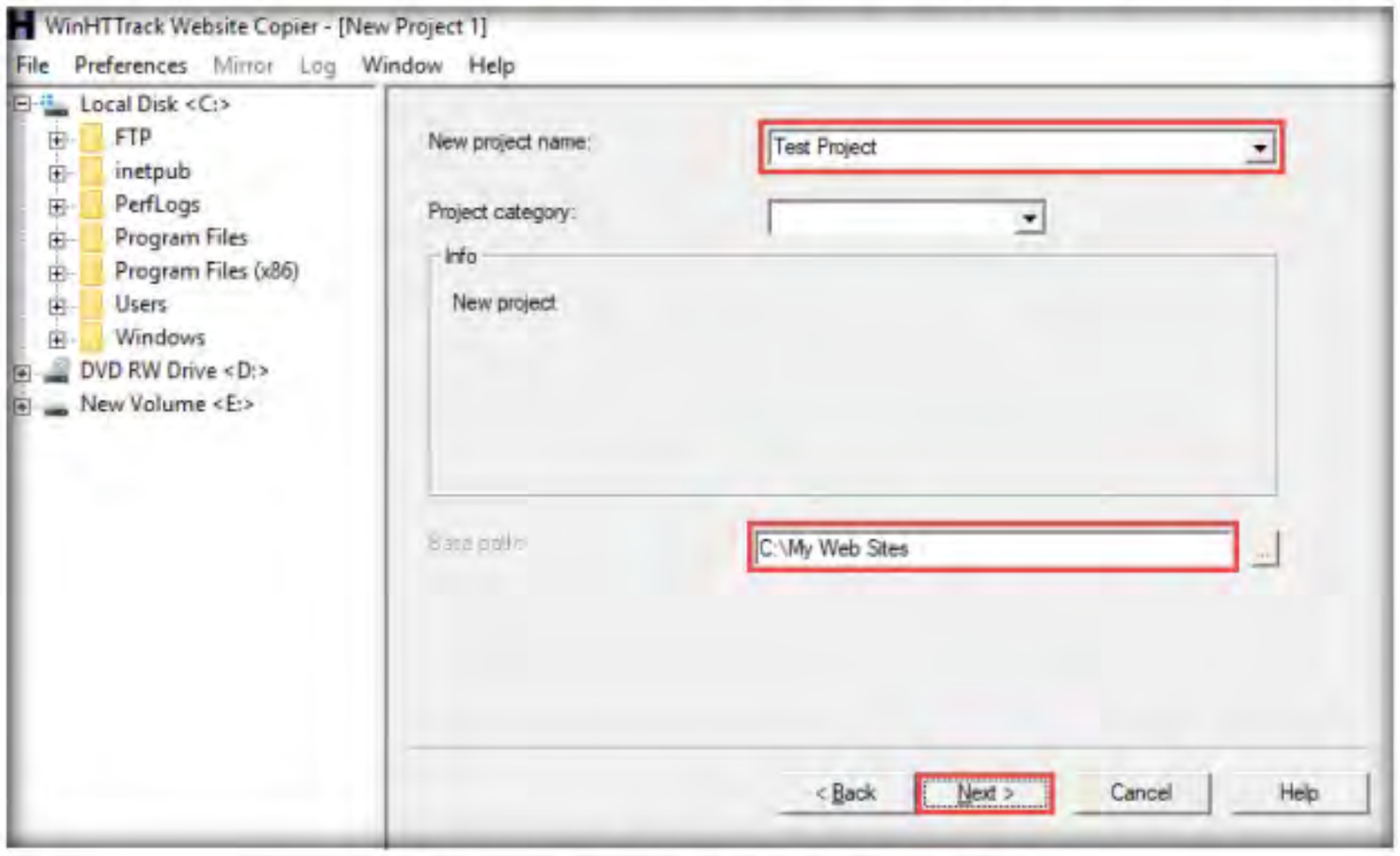


Figure 4.4.3: HTTrack Website Copier selecting a New Project

7. Enter a target URL (here, **www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options...**

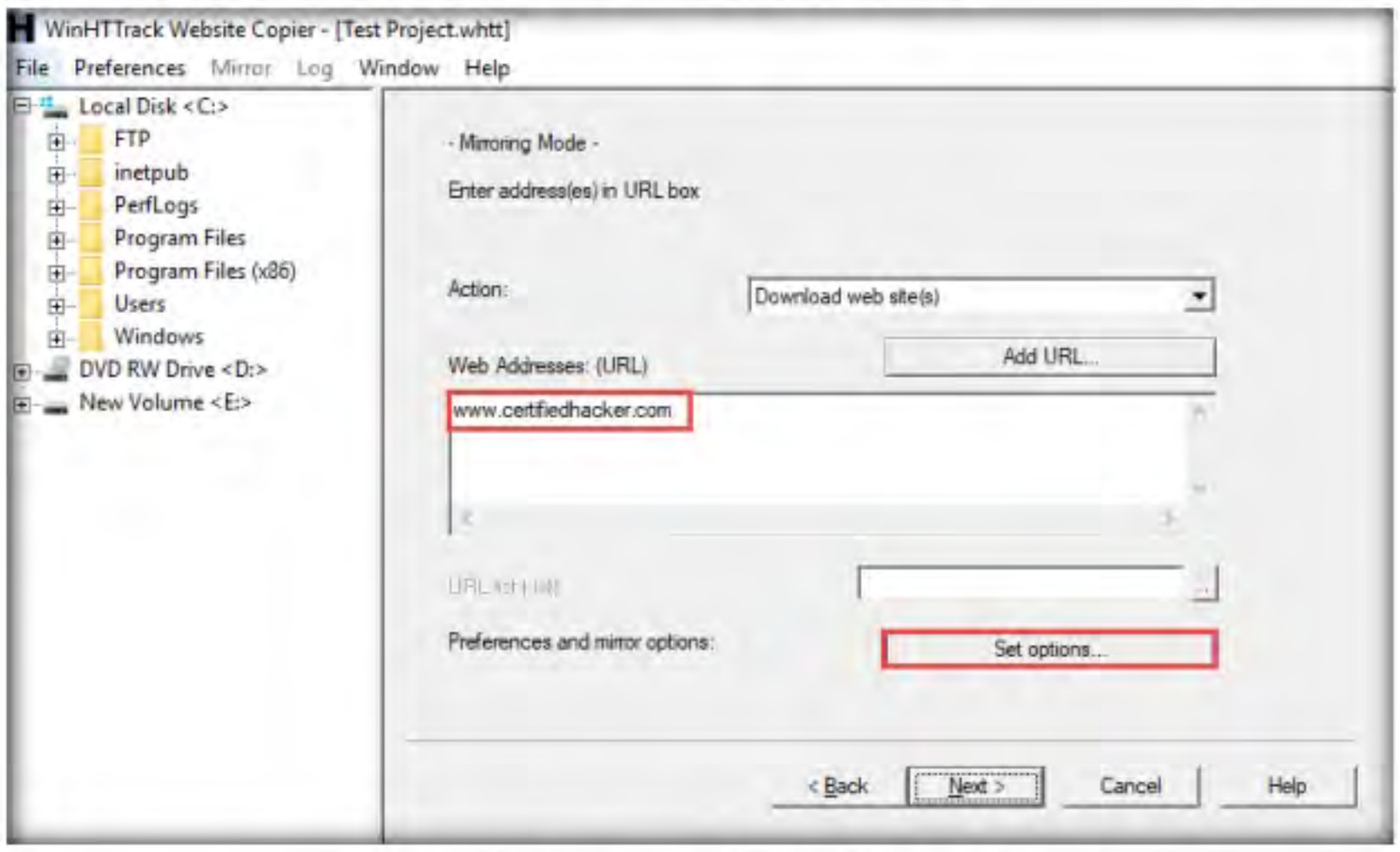


Figure 4.4.4: Setting options in HTTrack Website Copier

8. **WinHTTrack** window appears, click the **Scan Rules** tab and select the checkboxes for the file types as shown in the following screenshot; click **OK**.

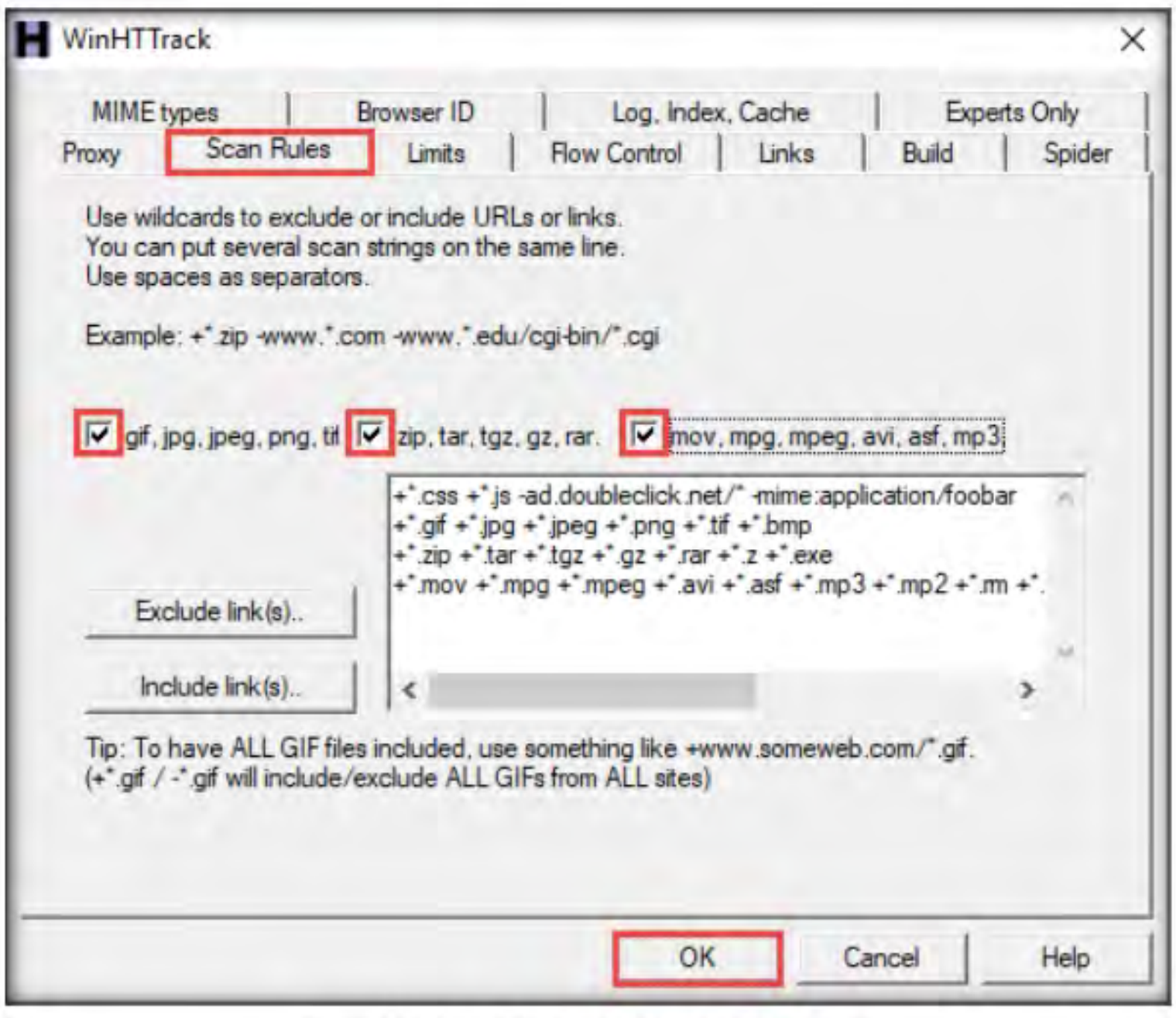


Figure 4.4.5: Scan Rules tab in HTTrack Website Copier

9. Click the **Next >** button.

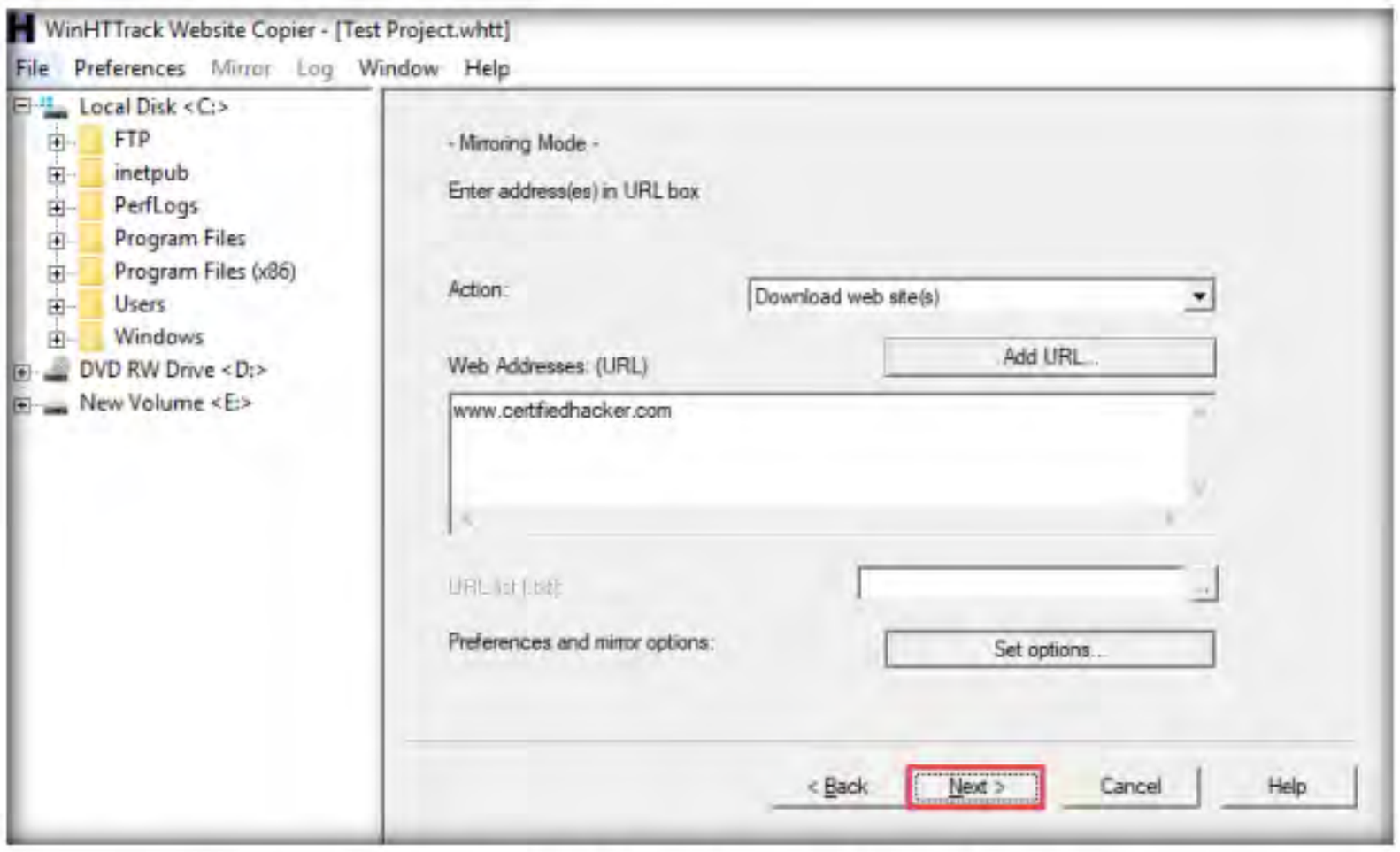


Figure 4.4.6: HTTrack Website Copier Select a project window

10. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation**. Check **Disconnect when finished** and click **Finish** to start mirroring the website.

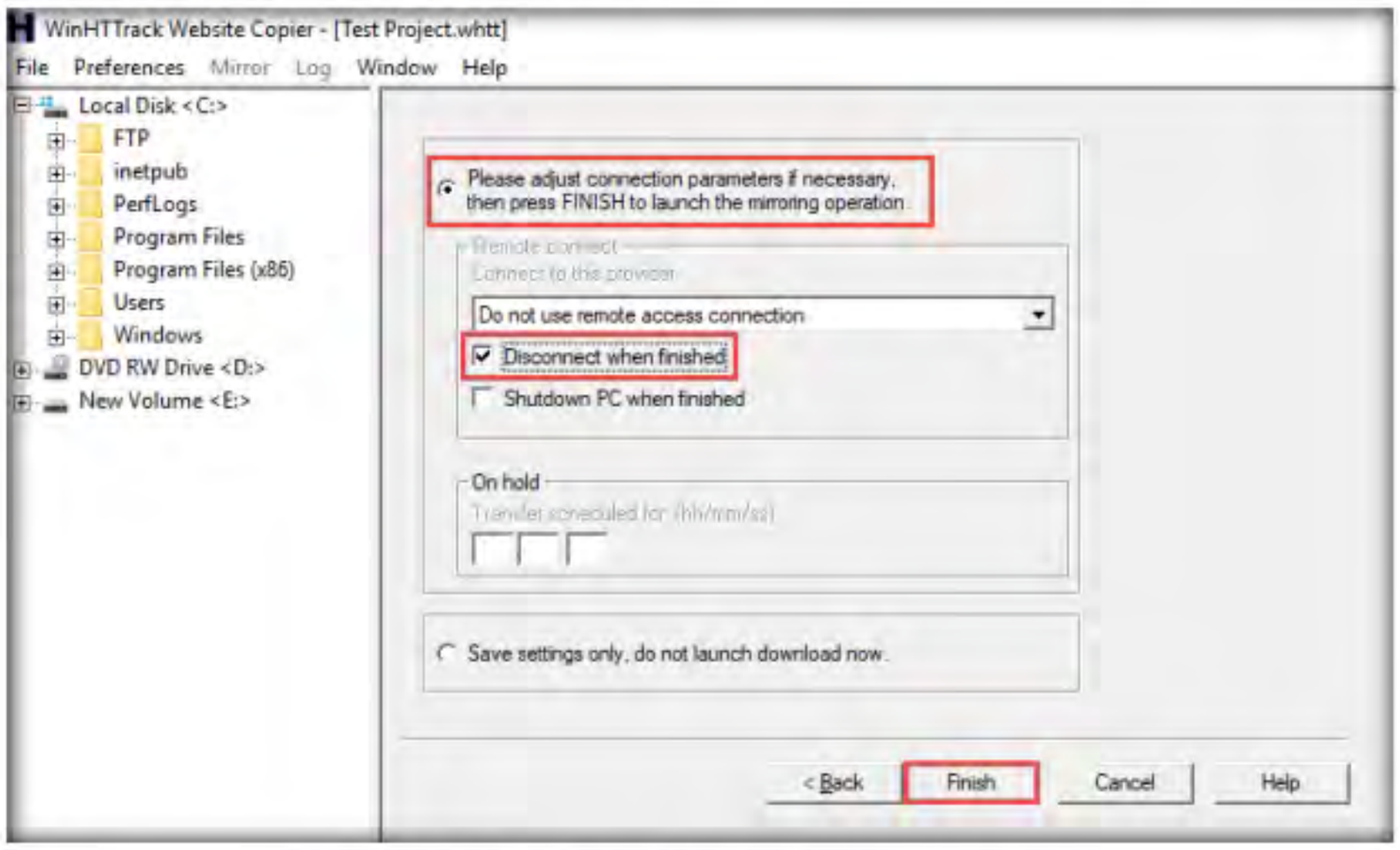


Figure 4.4.7: HTTrack Website Copier launching mirroring operation

11. Site mirroring progress will be displayed, as shown in the screenshot.

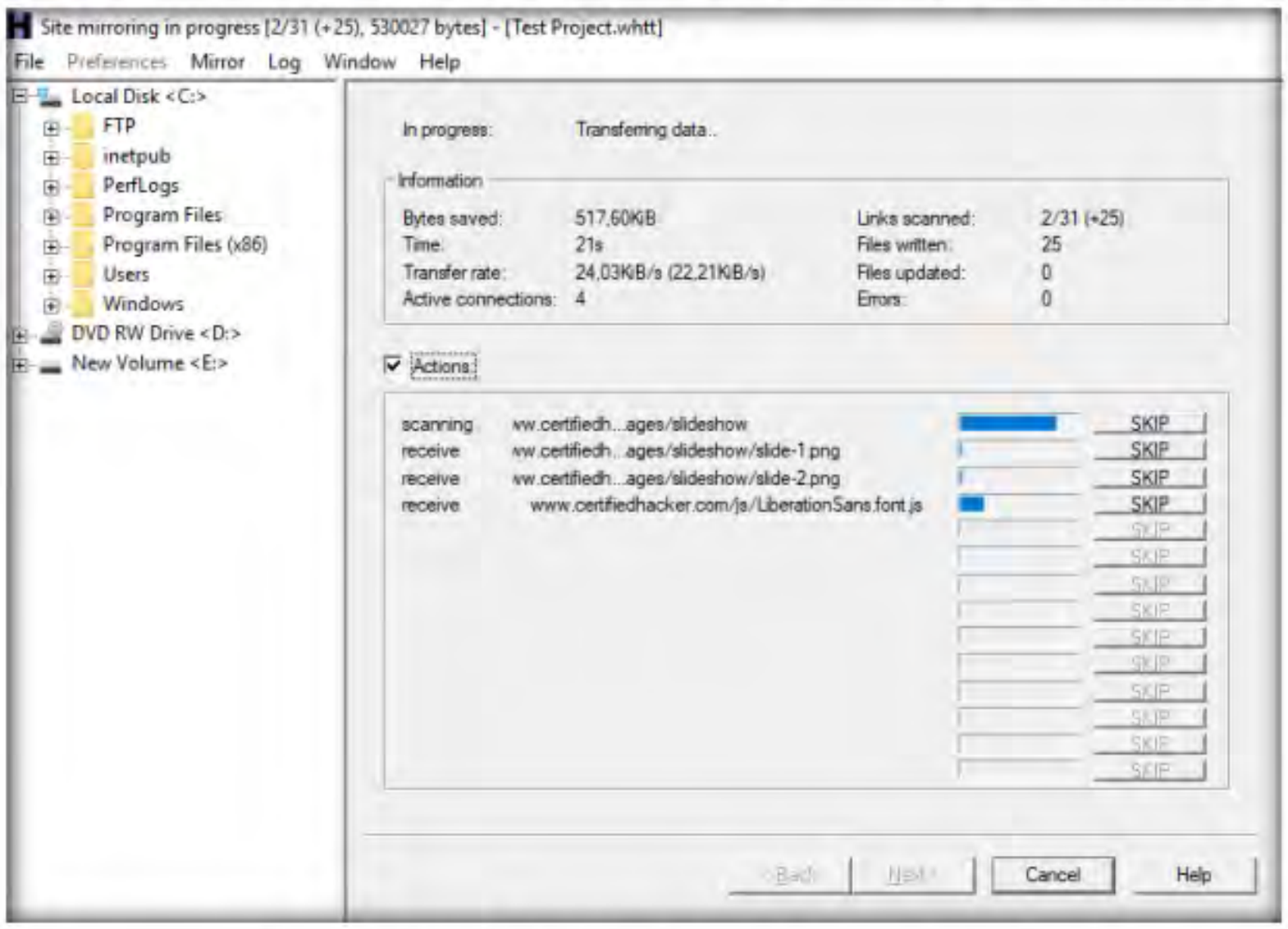


Figure 4.4.8: HTTrack Website Copier displaying site mirroring progress

12. Once the site mirroring is completed, WinHTTrack displays the message **Mirroring operation complete**; click on **Browse Mirrored Website**.

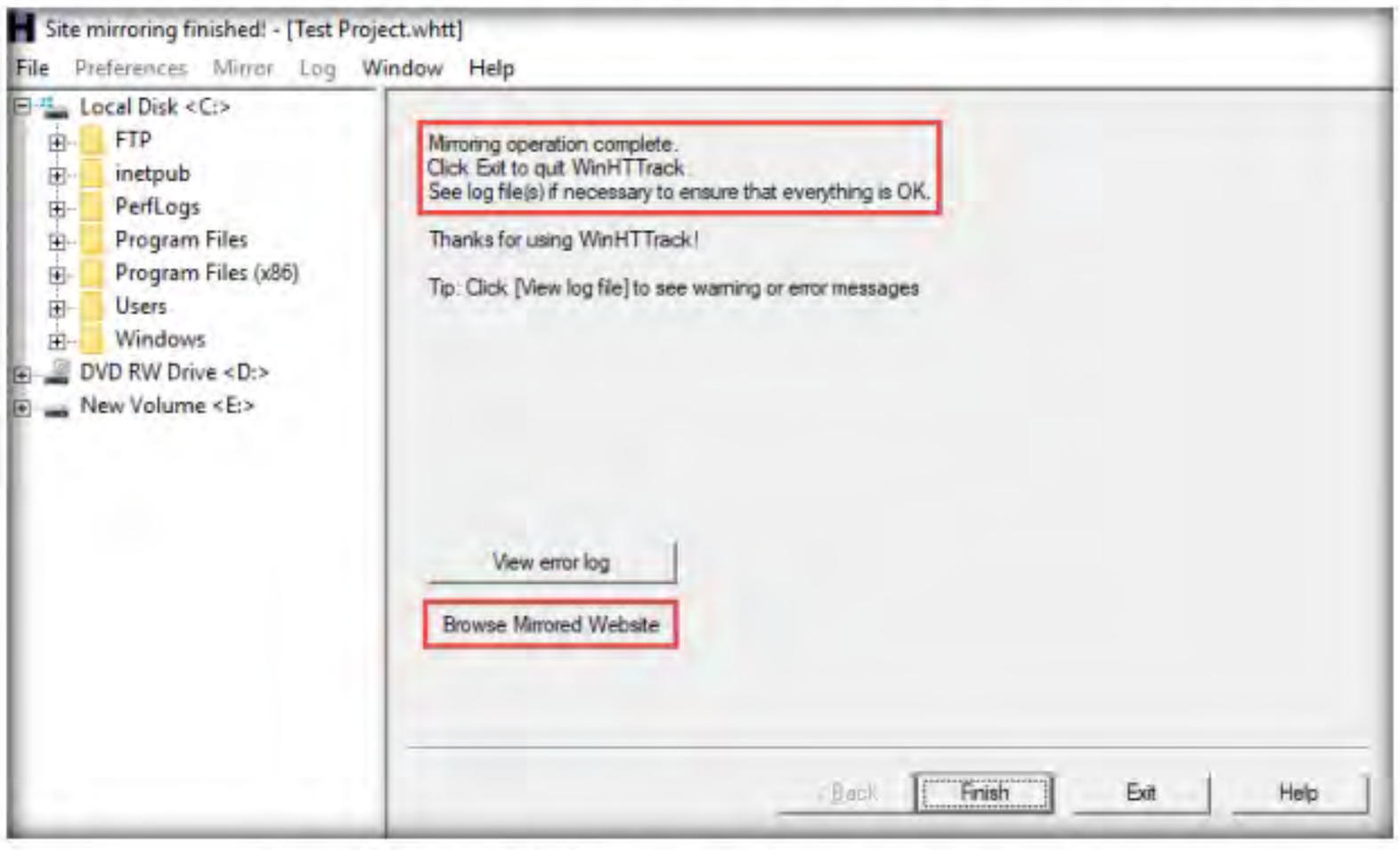


Figure 4.4.9: HTTrack Website Copier displaying site mirroring is complete

TASK 4.3

Browse the Mirrored Website

13. If the **How do you want to open this file?** pop up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

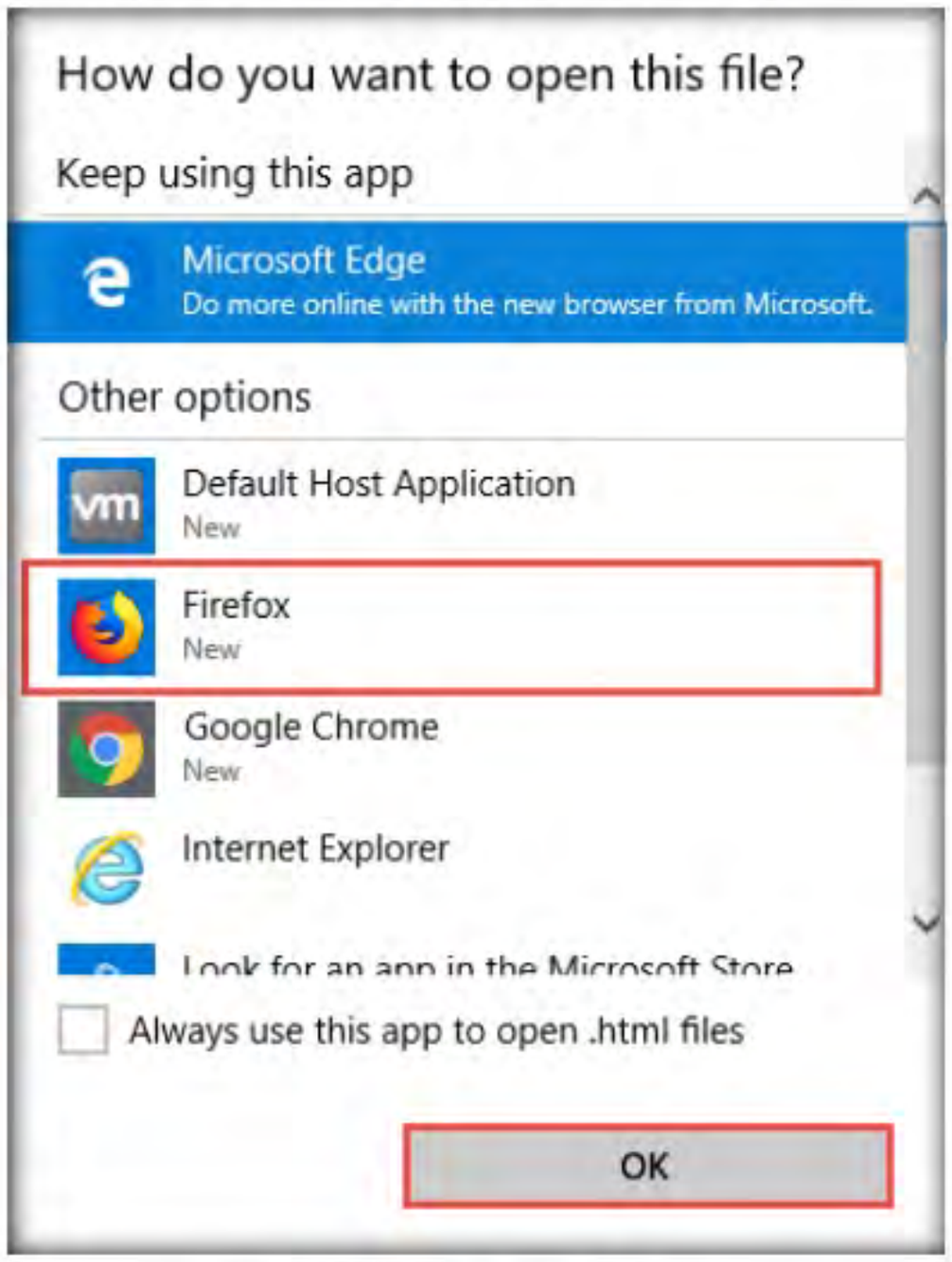


Figure 4.4.10: Selecting Mozilla Firefox

14. The mirrored website for **www.certifiedhacker.com** launches. The URL displayed in the address bar indicates that the website's image is stored on the local machine.

Figure 4.4.11: HTTrack Website Copier Mirrored Website Image

15. Analyze all directories, HTML, images, flash, videos, and other files available on the mirrored target website. You can also check for possible exploits and vulnerabilities. The site will work like a live hosted website.

Note: If the webpage does not open, navigate to the directory where you mirrored the website and open **index.html** with any browser.

16. Once done with your analysis, close the **Firefox** window and click **Finish** on the **WinHTTrack** window to complete the process

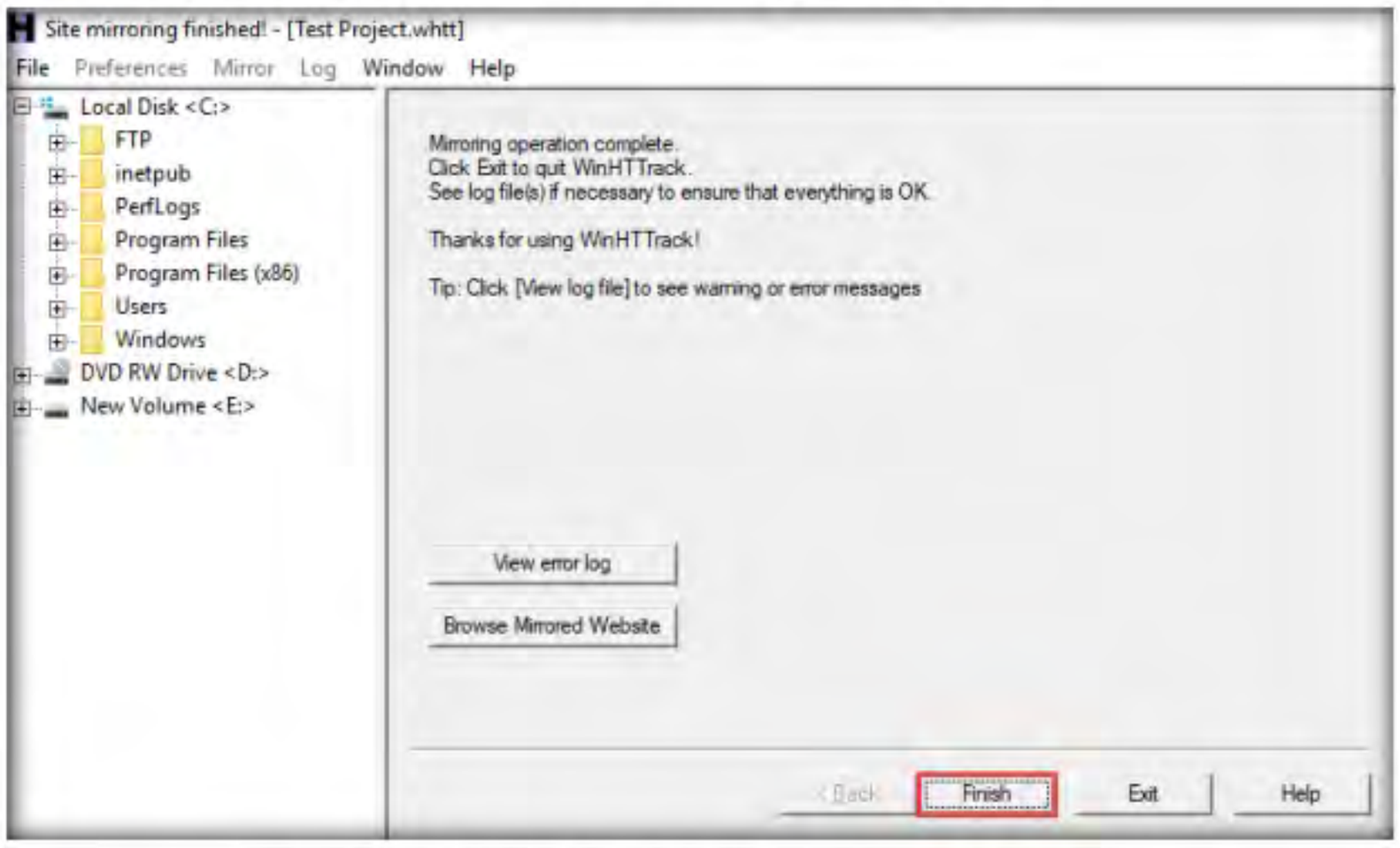


Figure 4.4.12: HTTrack Website Copier displaying site mirroring is complete

You can also use other mirroring tools such as **NCollector Studio** (http://www.calluna-software.com), **Cyotek WebCopy** (https://www.cyotek.com), etc. to mirror a target website.

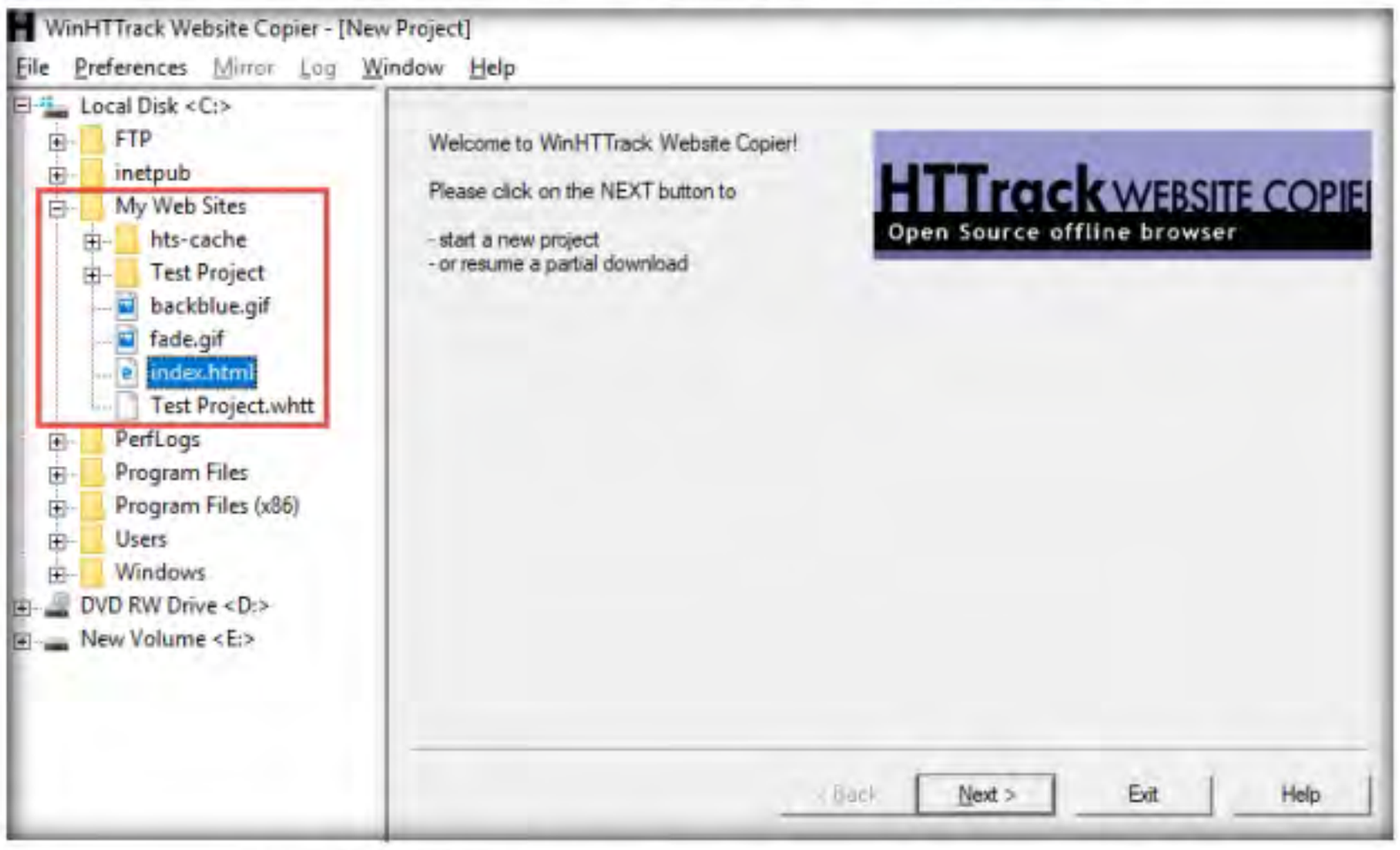


Figure 4.4.13: HTTrack Website Copier displaying mirrored website location

17. Some websites are very large, and it might take a long time to mirror the complete site.

18. This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** virtual machine.

TASK 5 Gather a Wordlist from the Target Website using CeWL

The words available on the target website may reveal critical information that can assist in performing further exploitation. CeWL is a ruby app that is used to spider a given target URL to a specified depth, optionally following external links, and returns a list of unique words that can be used for cracking passwords.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

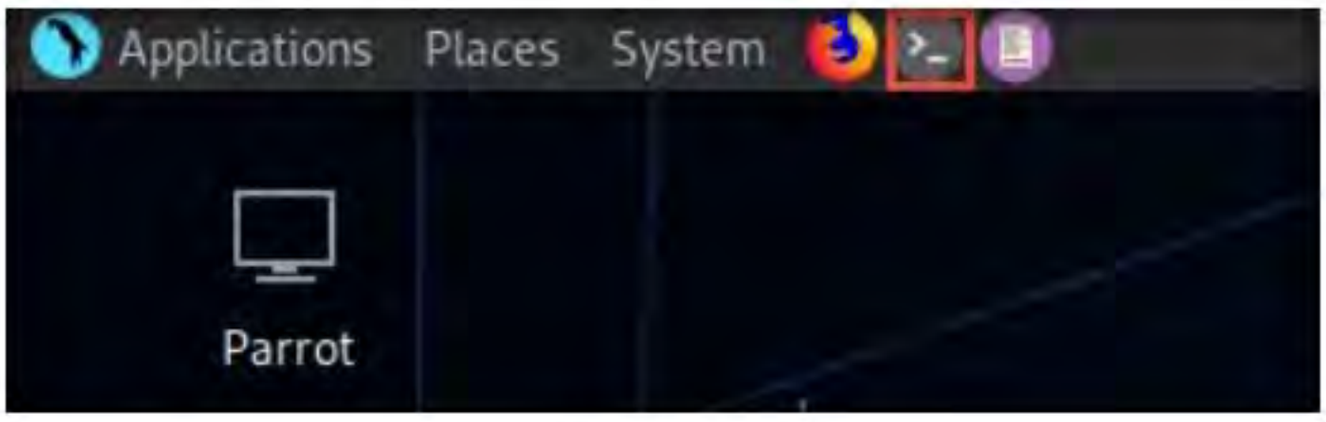


Figure 4.5.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

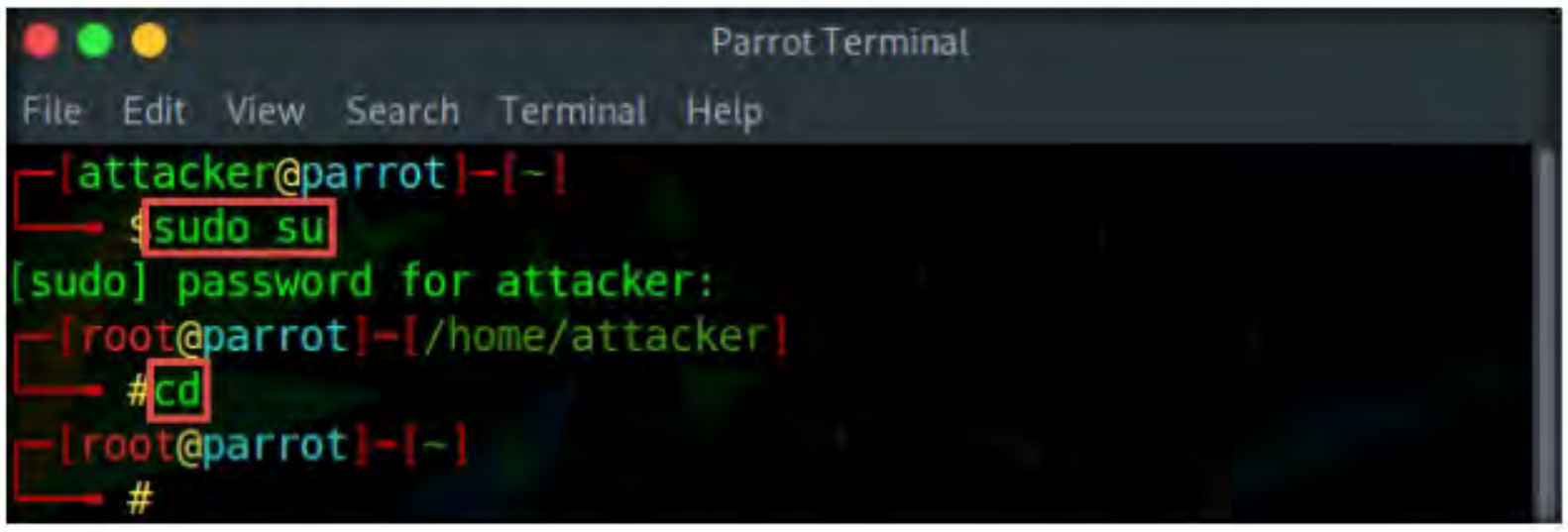


Figure 4.5.2: Running the programs as a root user

7. In the **Parrot Terminal** window, type **cewl -d 2 -m 5 www.certifiedhacker.com** and press **Enter**.

Note: **-d** represents the depth to spider the website (here, **2**) and **-m** represents minimum word length (here, **5**).

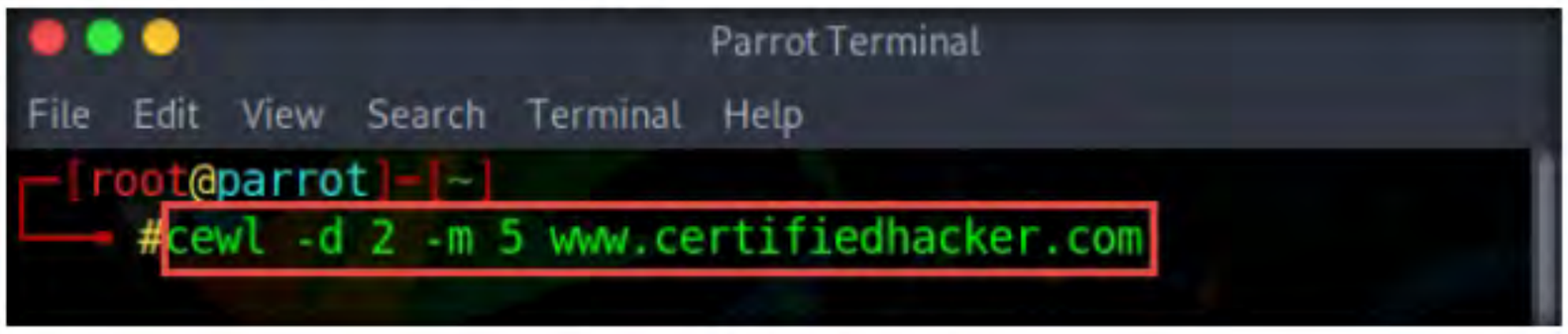


Figure 4.5.3: Gathering wordlist

8. A unique wordlist from the target website is gathered, as shown in the screenshot.

Note: The minimum word length is 5, and the depth to spider the target website is 2.

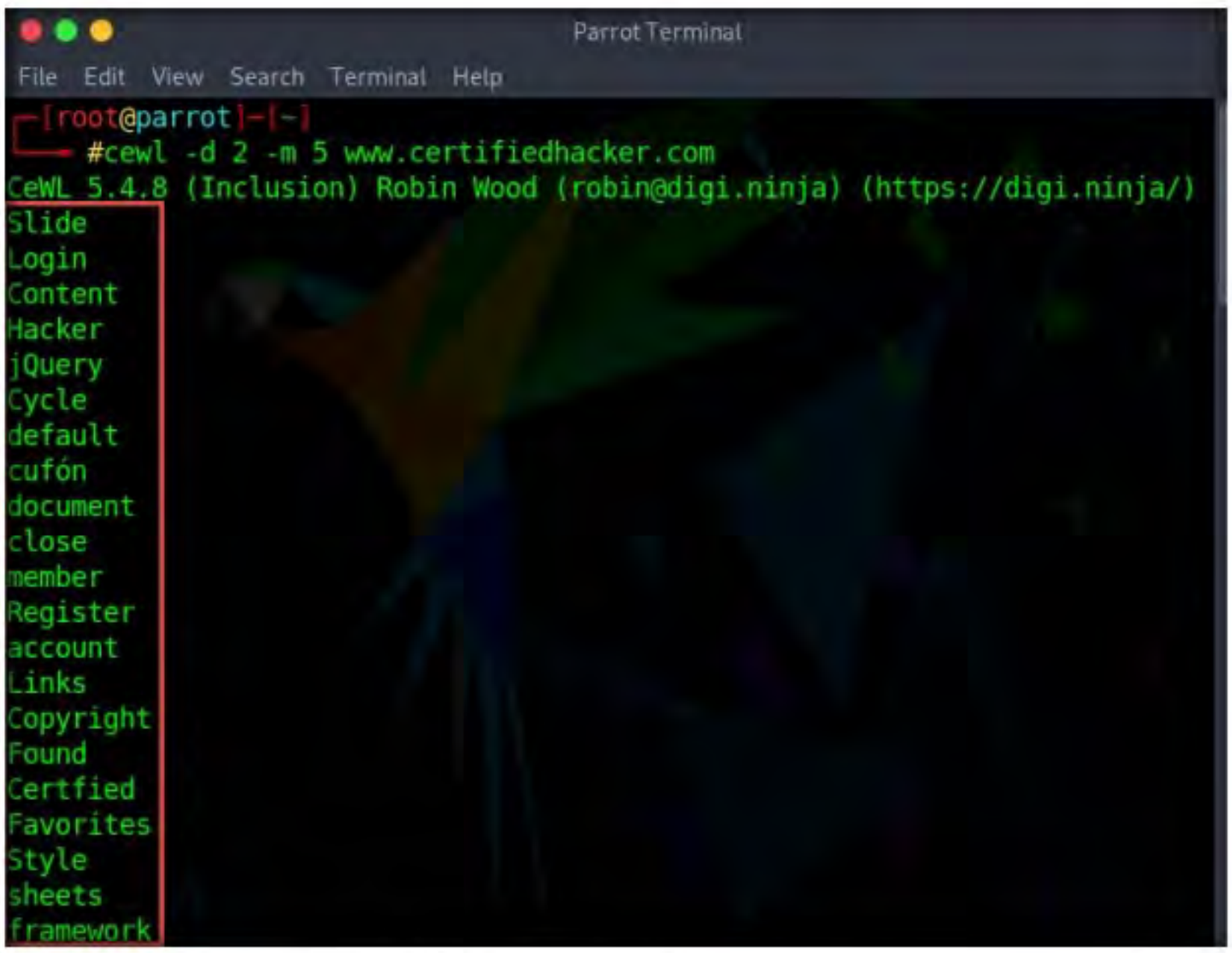


Figure 4.5.4: Wordlist gathered from the target website

9. Alternatively, this unique wordlist can be written directly to a text file by typing **cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com**.

Note: **-w** - Write the output to the file (here, **wordlist.txt**)

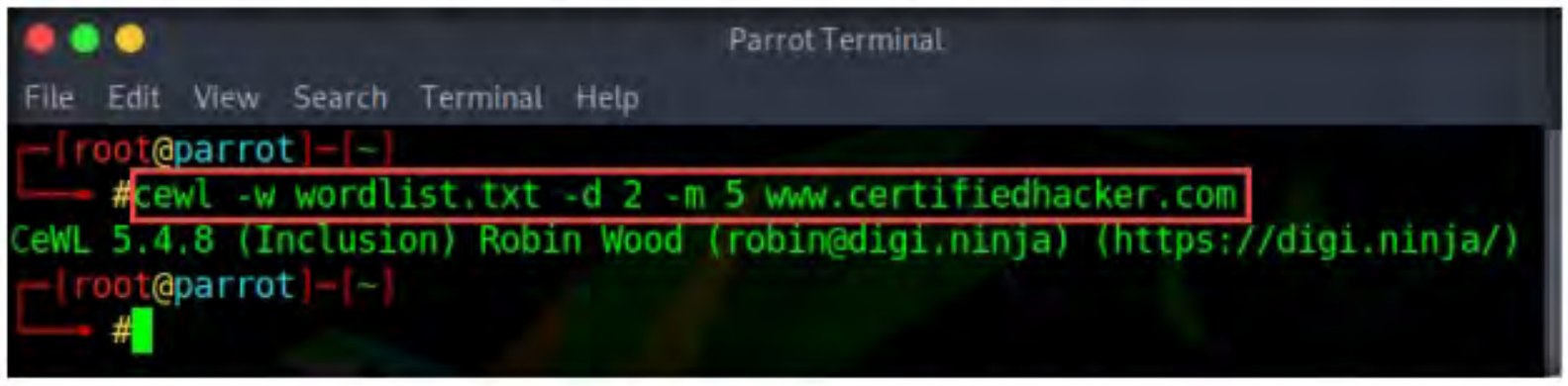


Figure 4.5.5: Wordlist written to wordlist.txt file

10. By default, the wordlist file gets saved in the **root** directory. Type **pluma wordlist.txt** and press **Enter** to view the extracted wordlist.

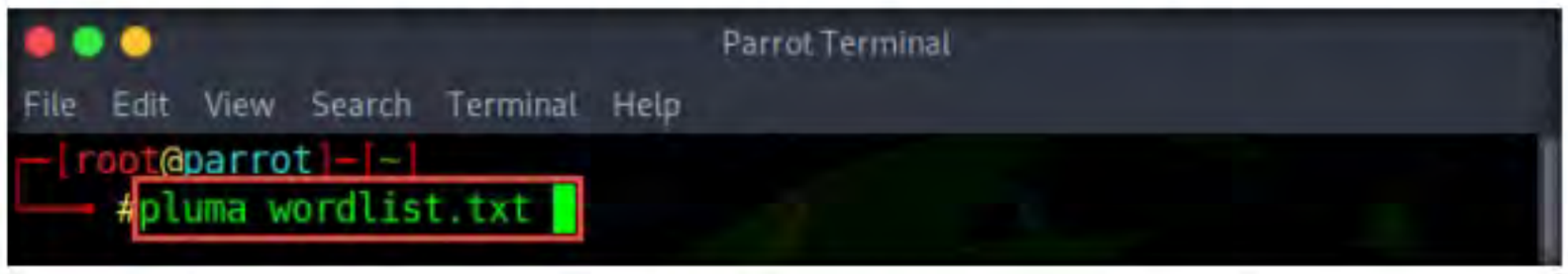


Figure 4.5.6: Open wordlist.txt file

11. The file containing a unique wordlist extracted from the target website opens, as shown in the screenshot.

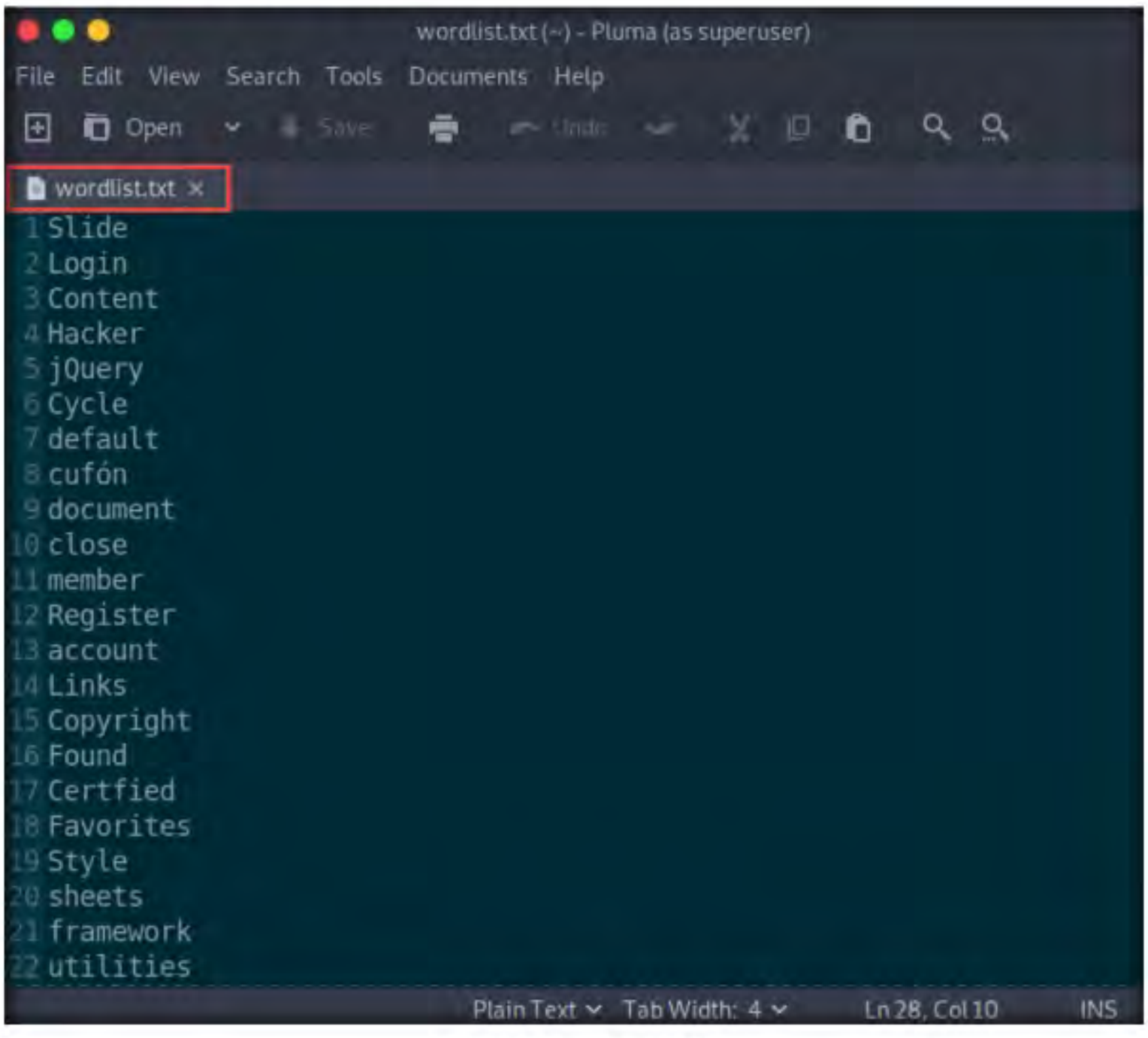


Figure 4.5.7: wordlist.txt file

12. This wordlist can be used further to perform brute-force attacks against the previously obtained emails of the target organization's employees.
13. This concludes the demonstration of gathering wordlist from the target website using CeWL.
14. Close all open windows and document all the acquired information.
15. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 5

Perform Email Footprinting

Email footprinting or tracing emails involves analyzing the email header to discover details about the sender.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

As a professional ethical hacker, you need to be able to track emails of individuals (employees) from a target organization for gathering critical information that can help in building an effective hacking strategy. Email tracking allows you to collect information such as IP addresses, mail servers, OS details, geolocation, information about service providers involved in sending the mail etc. By using this information, you can perform social engineering and other advanced attacks.

Lab Objectives

- Gather information about a target by tracing emails using eMailTrackerPro

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- eMailTrackerPro located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro**
- You can also download the latest version of eMailTrackerPro from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of Email Footprinting

E-mail footprinting, or tracking, is a method to monitor or spy on email delivered to the intended recipient. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email.

Email footprinting reveals information such as:

- Recipient's system IP address
- The GPS coordinates and map location of the recipient
- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages were set to expire after a specified time

Lab Tasks

TASK 1 — Gather Information about a Target by Tracing Emails using eMailTrackerPro

Here, we will gather information by analyzing the email header using eMailTrackerPro.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1 — Install eMailTrackerPro

3. Open **File Explorer** and navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
4. If the **User Account Control** pop-up appears, click **Yes**.
5. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.

The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email header helps ethical hackers to trace the routing path taken by an email before delivering it to the recipient.

6. After the installation is complete, in the **Completing the eMailTrackerPro Setup Wizard**, uncheck the **Show Readme** check-box and click the **Finish** button to launch the eMailTrackerPro.

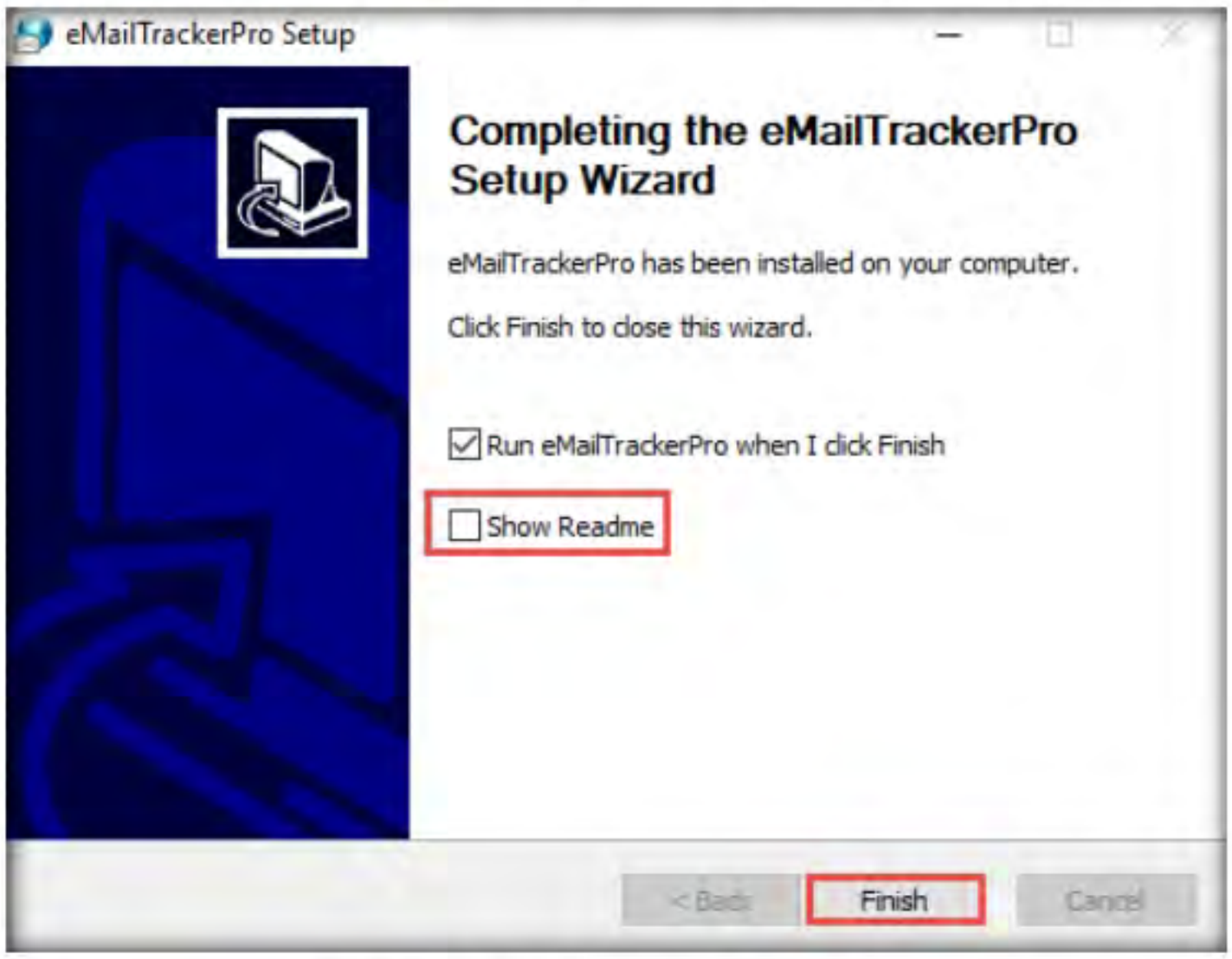


Figure 5.1.1: eMailTrackerPro installation Complete

7. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.

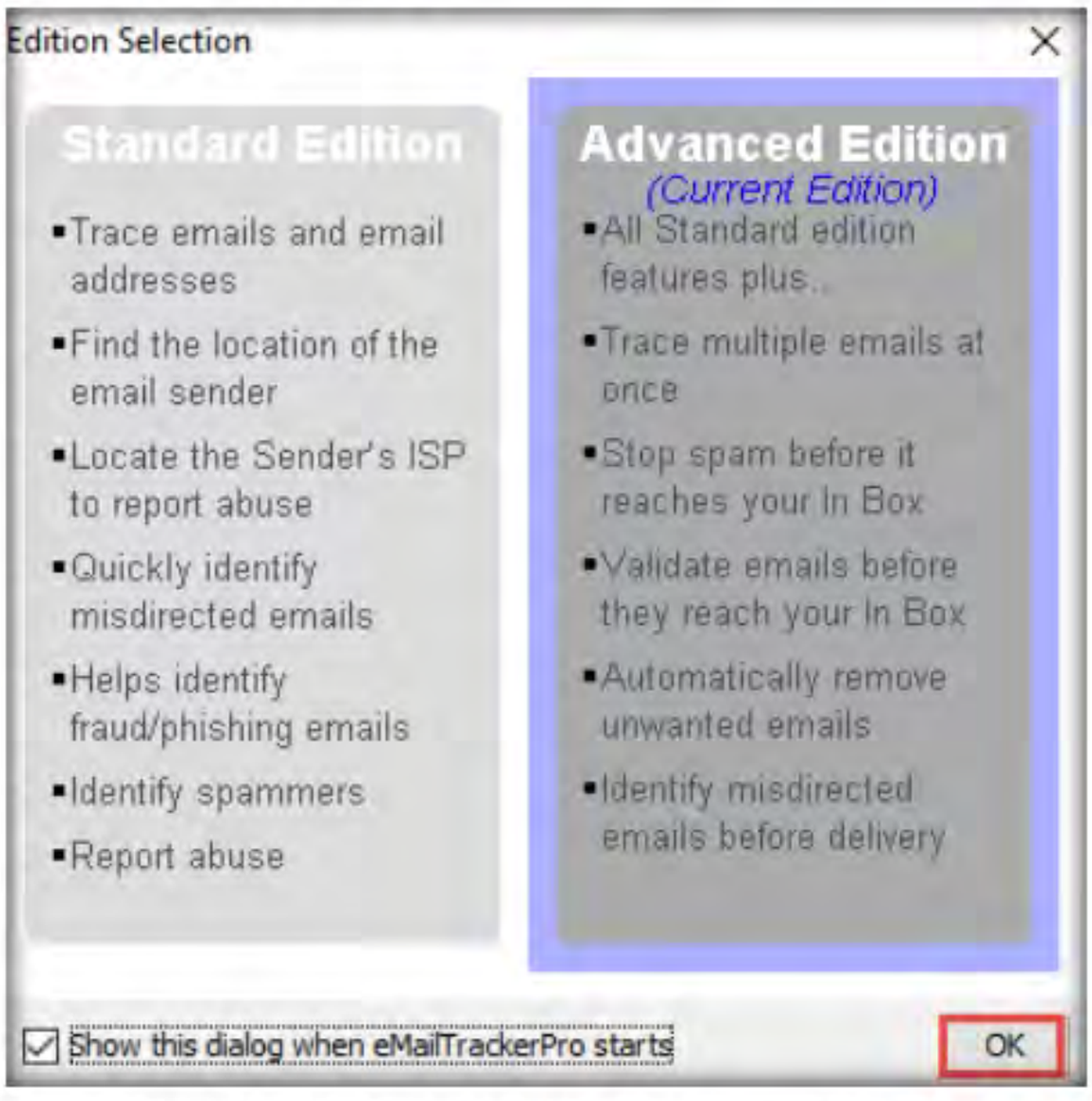


Figure 5.1.2: eMailTrackerPro - Edition Selection pop-up window

8. The **eMailTrackerPro** main window appears, as shown in the screenshot.

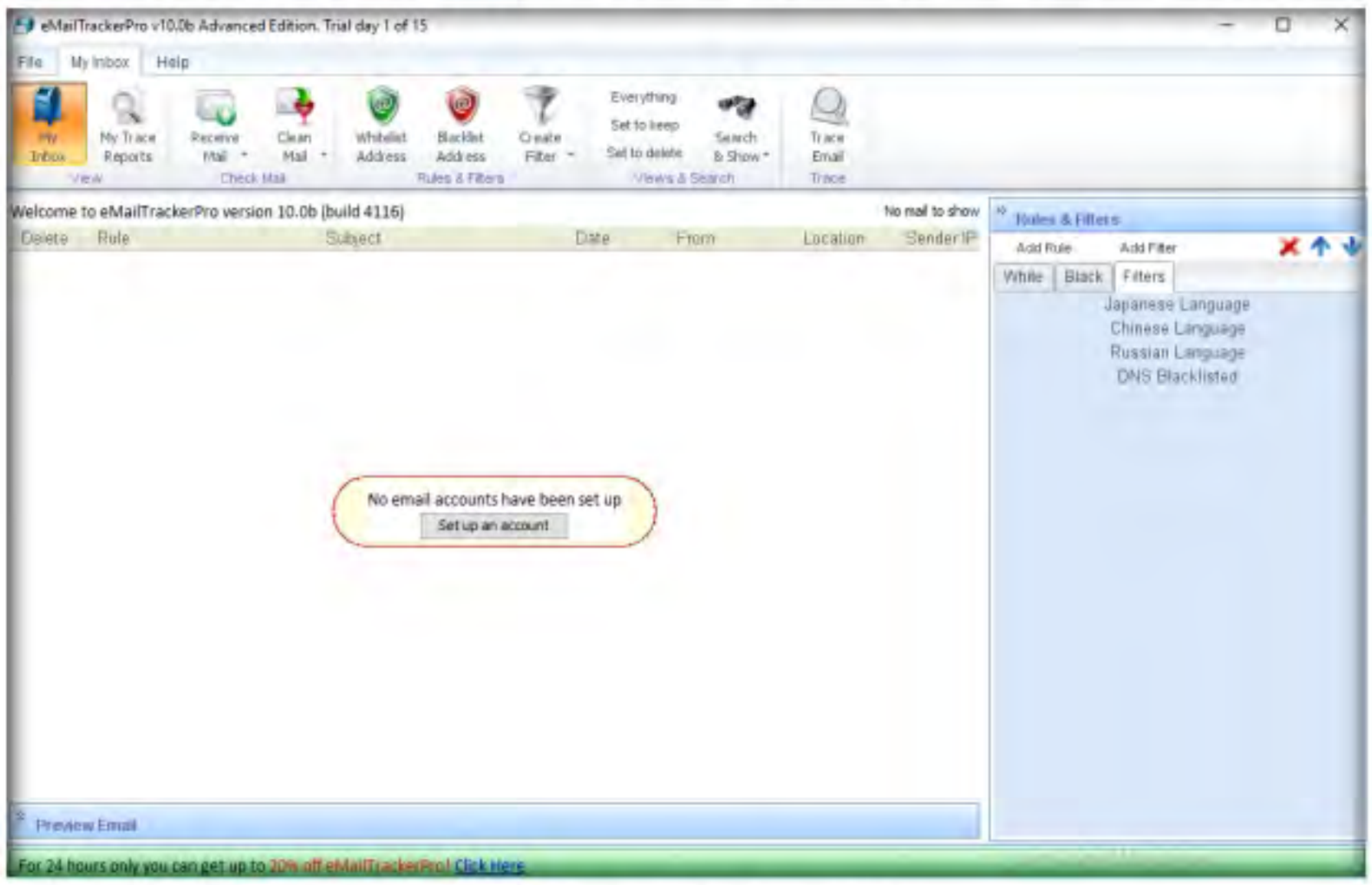


Figure 5.1.3: eMailTrackerPro main window

TASK 1.2

Trace Email Header

9. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header)
10. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.

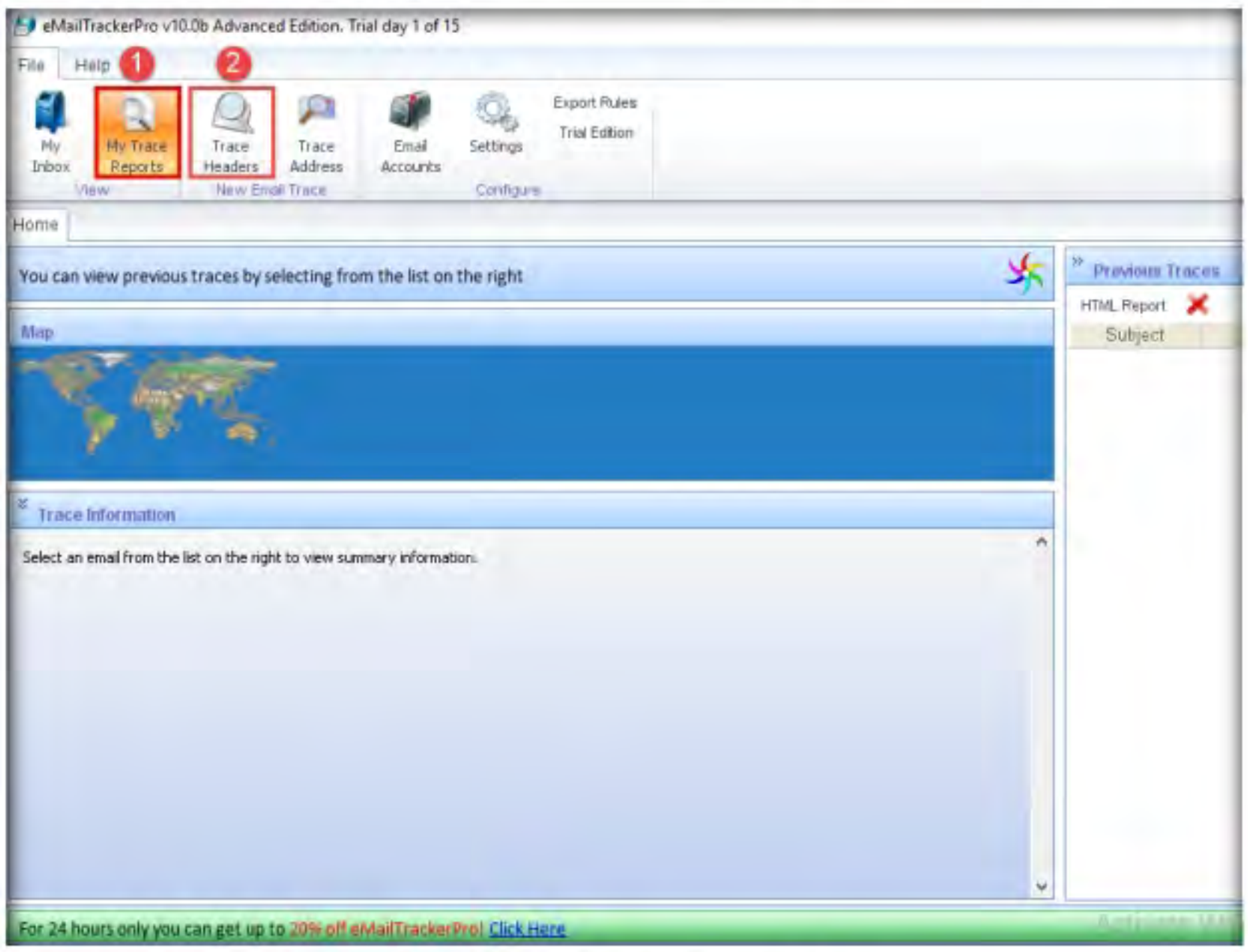


Figure 5.1.4: The eMailTrackerPro main window

11. A pop-up window will appear; select **Trace an email I have received**. Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers:** field under **Enter Details** section.

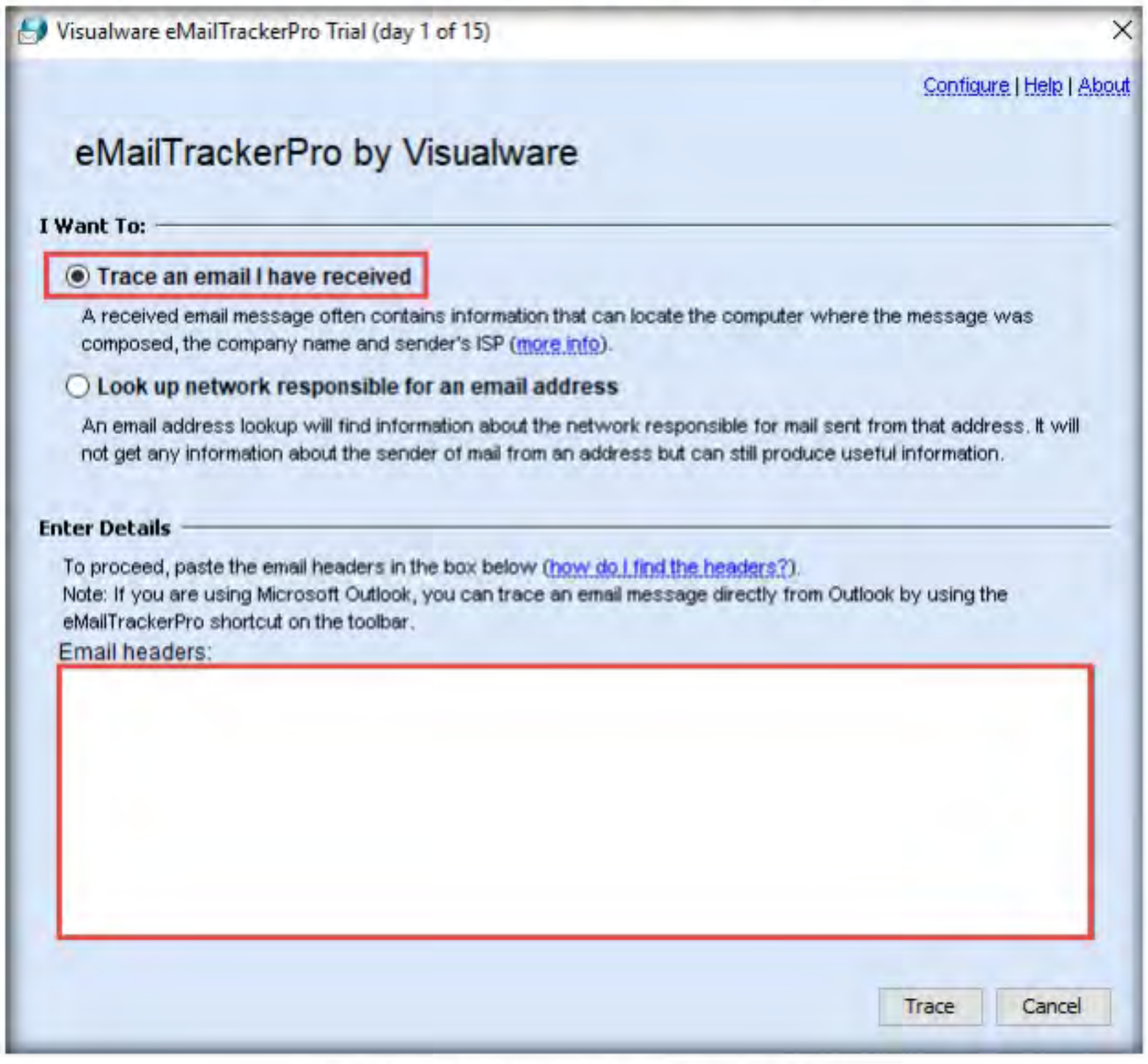


Figure 5.1.5: The eMailTrackerPro entering details window

12. For finding email headers, open any web browser and log in to any email account of your choice; from the email inbox, open the message you would like to view headers for.

Note: In **Gmail**, find the email header by following the steps:

- Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.
- Select **Show original** from the list.
- The **Original Message** window appears in a new browser tab with all the details about the email, including the email header.

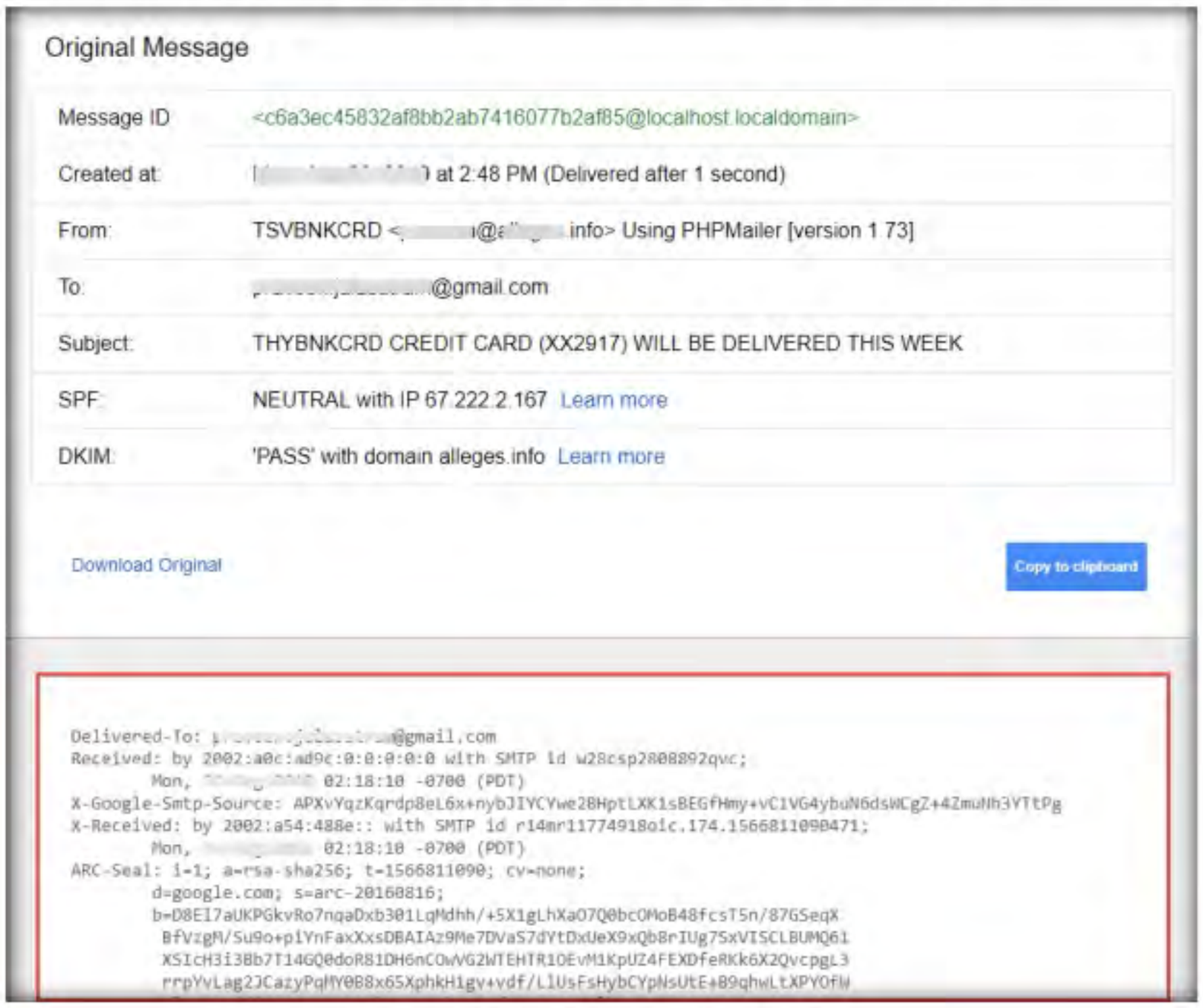


Figure 5.1.6: Sample Email Header in Gmail

Note: In **Outlook**, find the email header by following the steps:

- Double-click the email to open it in a new window
- Click the **...** (**More actions**) icon present at the right of the message-pane to open message options
- From the options, click **View message details**
- The **message details** window appears with all the details about the email, including the email header

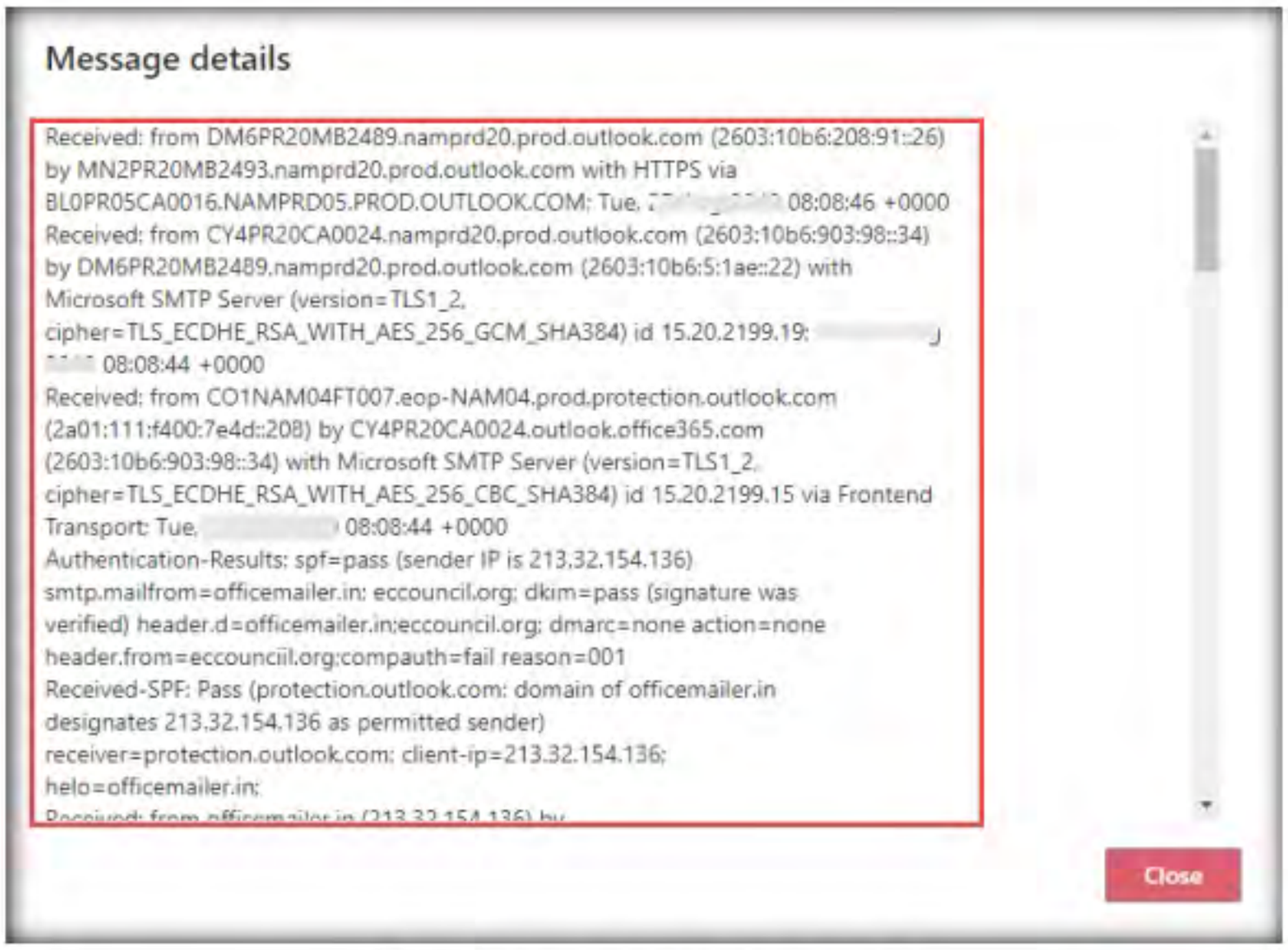


Figure 5.1.7: Sample Email Header in Outlook

13. Copy the entire email header text and paste it into the **Email headers:** field of eMailTrackerPro, and click **Trace**.

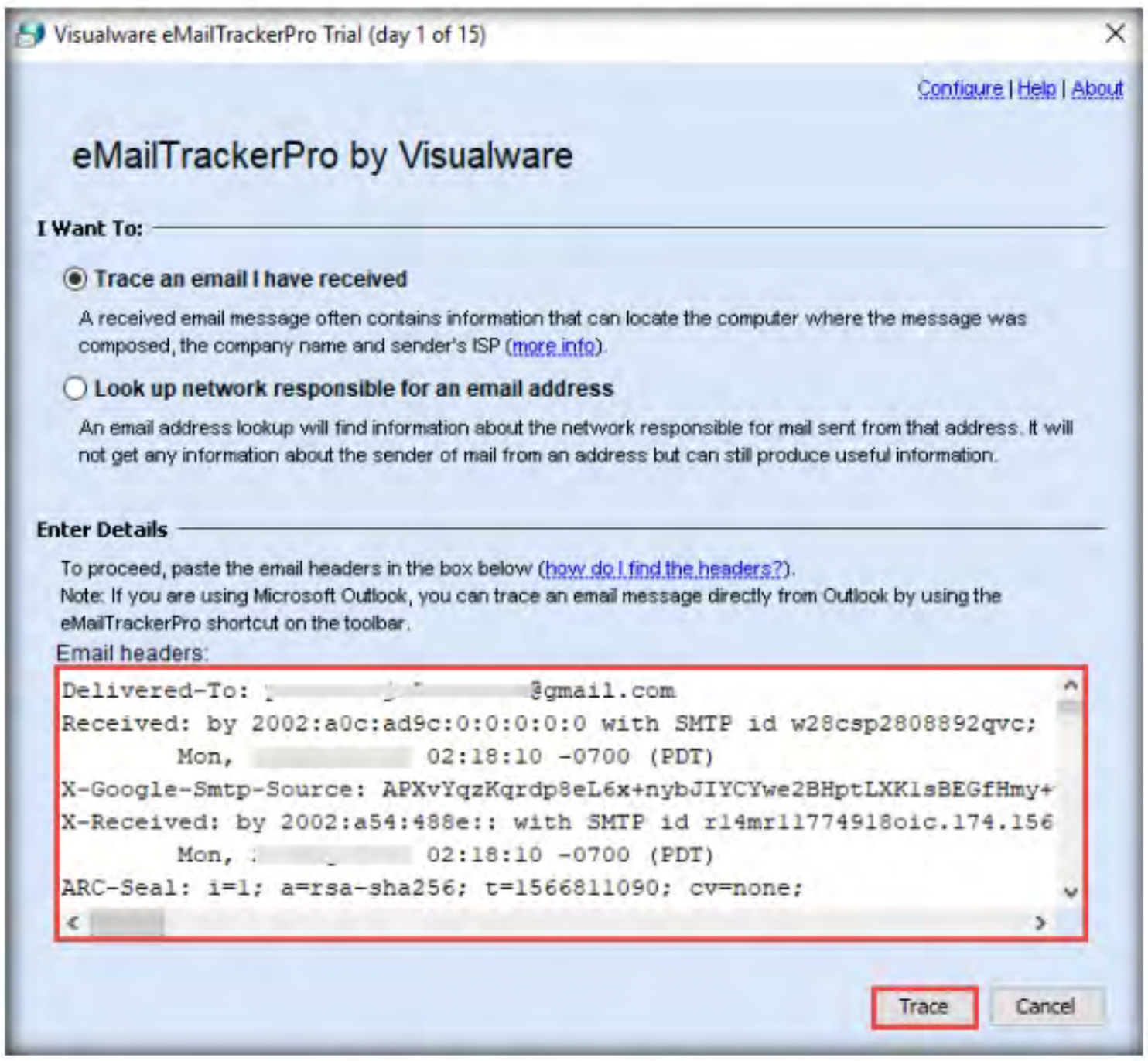


Figure 5.1.8: Email headers and Tracing emails

14. The **My Trace Reports** window opens.
15. The email location will be traced in a **Map** (world map GUI). You can also view the summary by selecting **Email Summary** on the right-hand side of the window. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.

Note: The location and IP addresses may vary according to your email header.

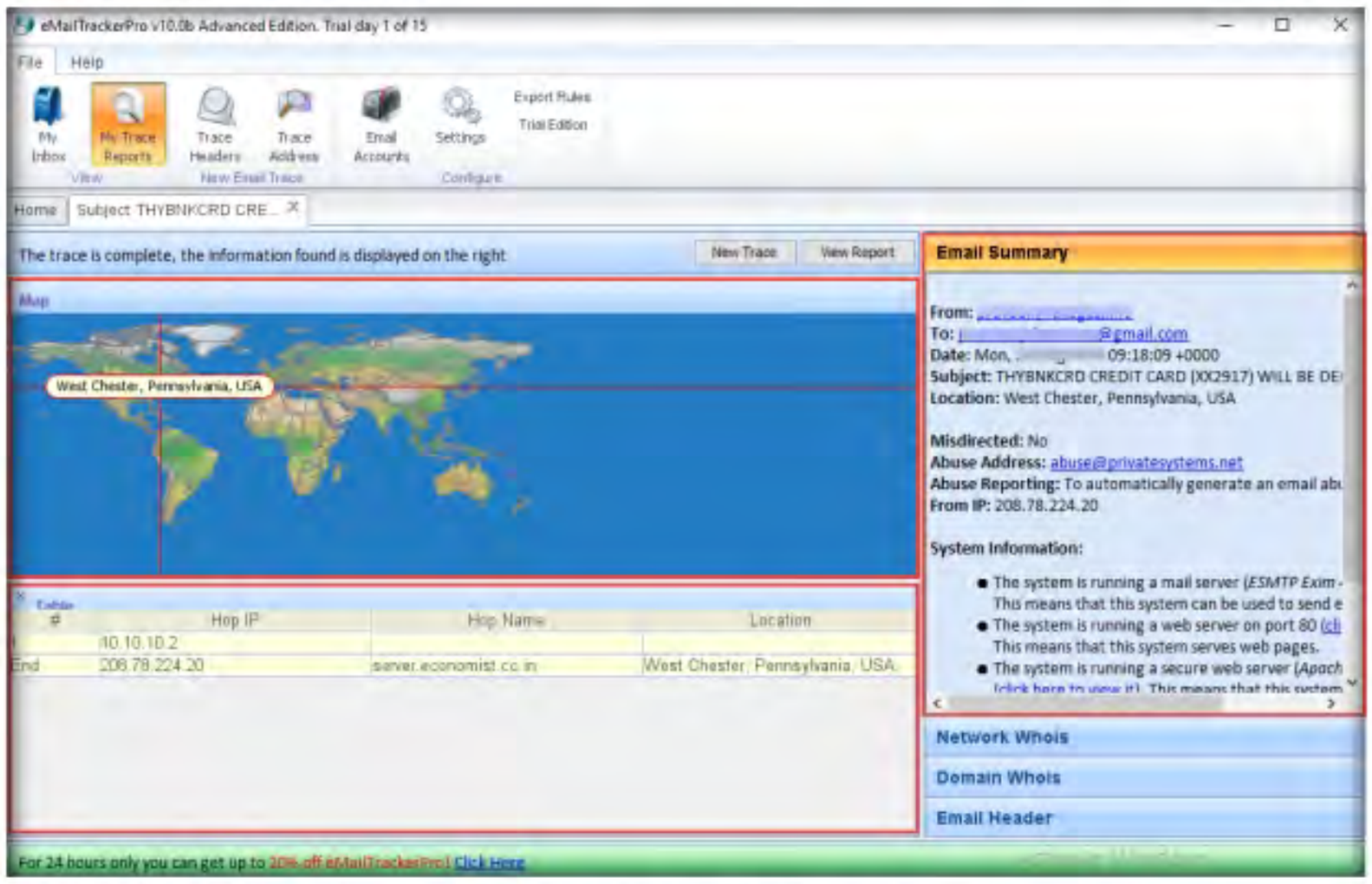


Figure 5.1.9: eMailTrackerPro – Email Trace Report

TASK 1.3

Examine the Report

16. To examine the report, click the **View Report** button above **Map** to view the complete trace report.

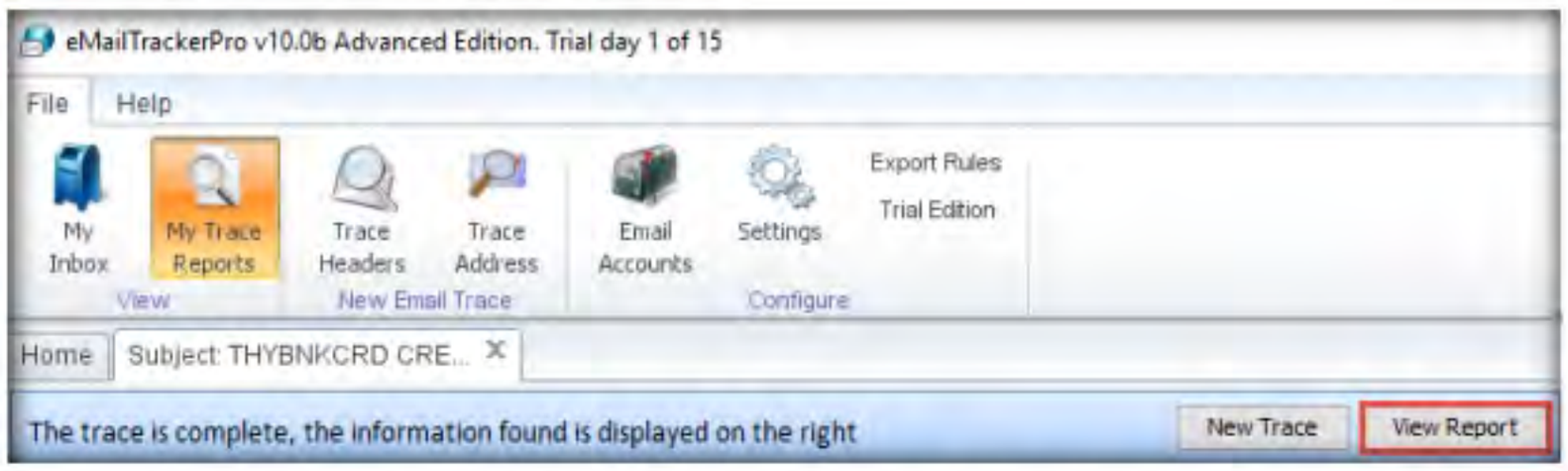


Figure 5.1.10: The eMailTrackerPro – My Trace Reports tab

17. The complete report appears in the default browser.

Note: If a pop-up window appears asking for a browser to be selected, select **Firefox** and click **OK**.

18. Expand each section to view detailed information.

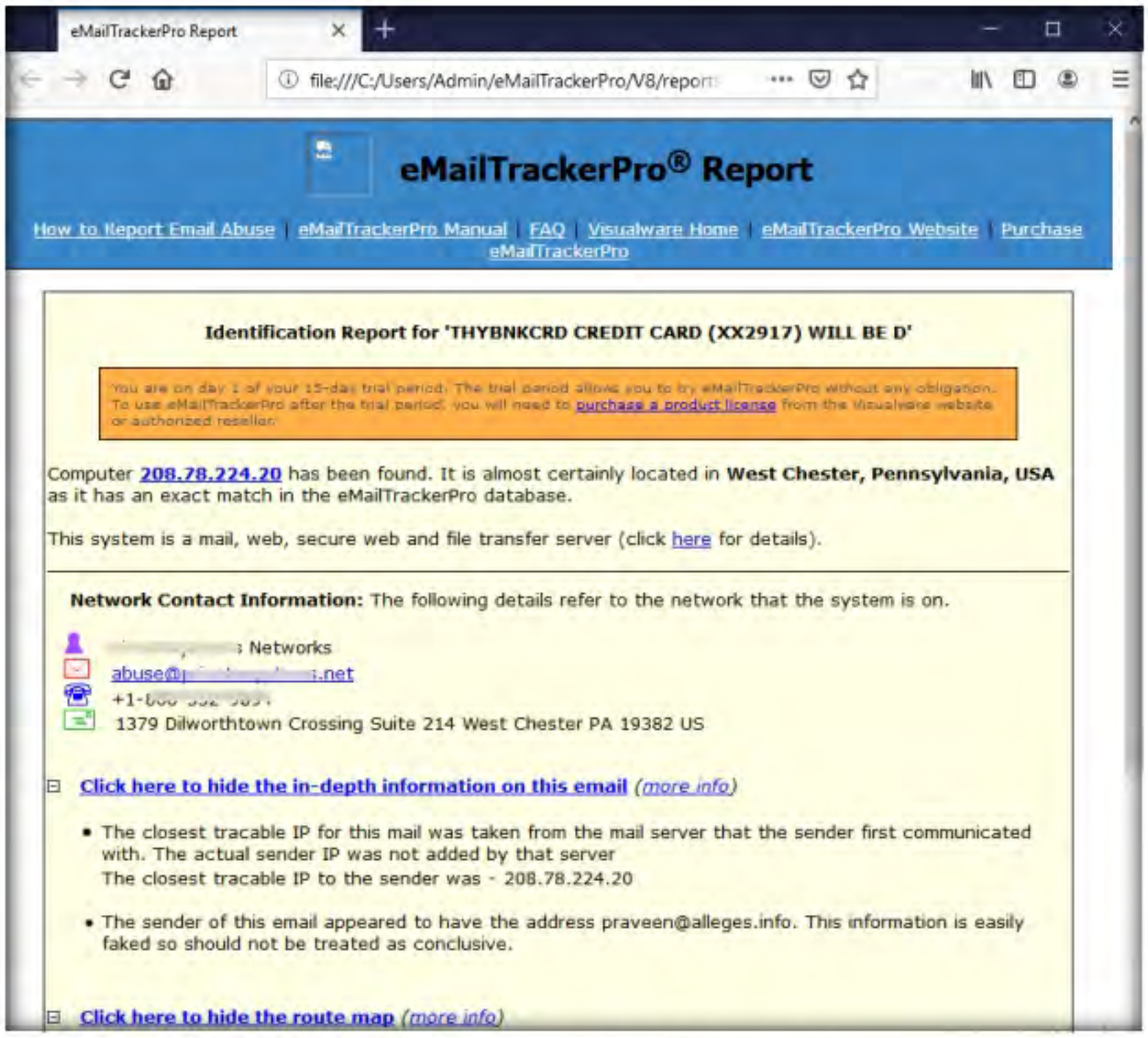


Figure 5.1.11: eMailTrackerPro – detailed information Report

You can also use email tracking tools such as **Infoga** (https://github.com), **Mailtrack** (https://mailtrack.io), etc. to track an email and extract target information such as sender identity, mail server, sender's IP address, location, etc.

19. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
20. Close all open windows and document all the acquired information.
21. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 6

Perform Whois Footprinting

Whois lookup reveals available information on a hostname, IP address, or domain

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

During the footprinting process, gathering information on the target IP address and domain obtained during previous information gathering steps is important. As a professional ethical hacker or penetration tester, you should be able to perform Whois footprinting on the target; this method provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc. Using this information, you can create a map of the organization's network, perform social engineering attacks, and obtain internal details of the network.

Lab Objectives

- Perform Whois lookup using DomainTools

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Lab Duration

Time: 5 Minutes

Overview of Whois Footprinting

This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database

provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

Lab Tasks

TASK 1 Perform Whois Lookup using DomainTools

Here, we will gather target information by performing Whois lookup using DomainTools.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**) and navigate to **http://whois.domaintools.com**. In the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.

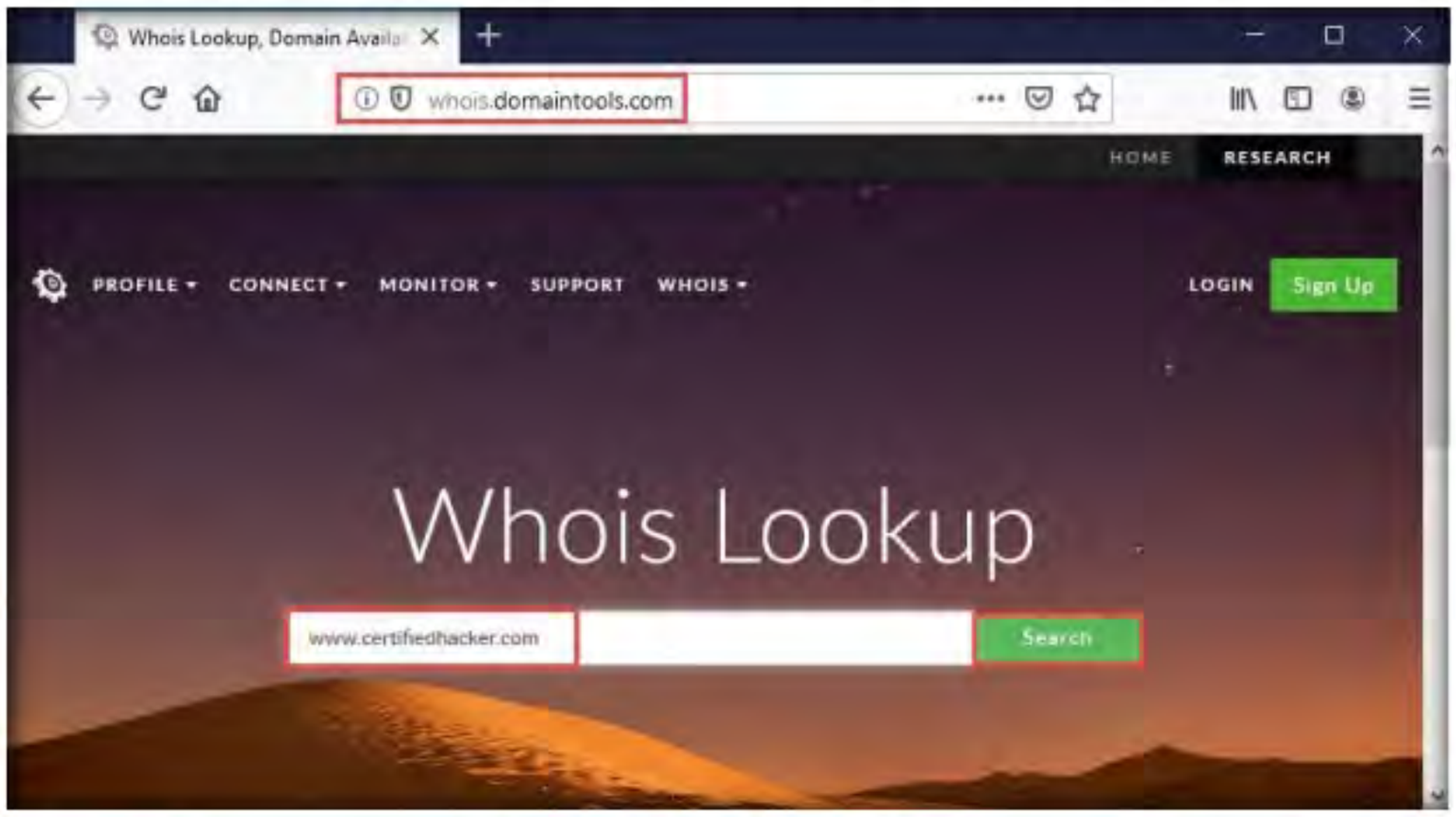


Figure 6.1.1: Whois Domain website

4. This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.

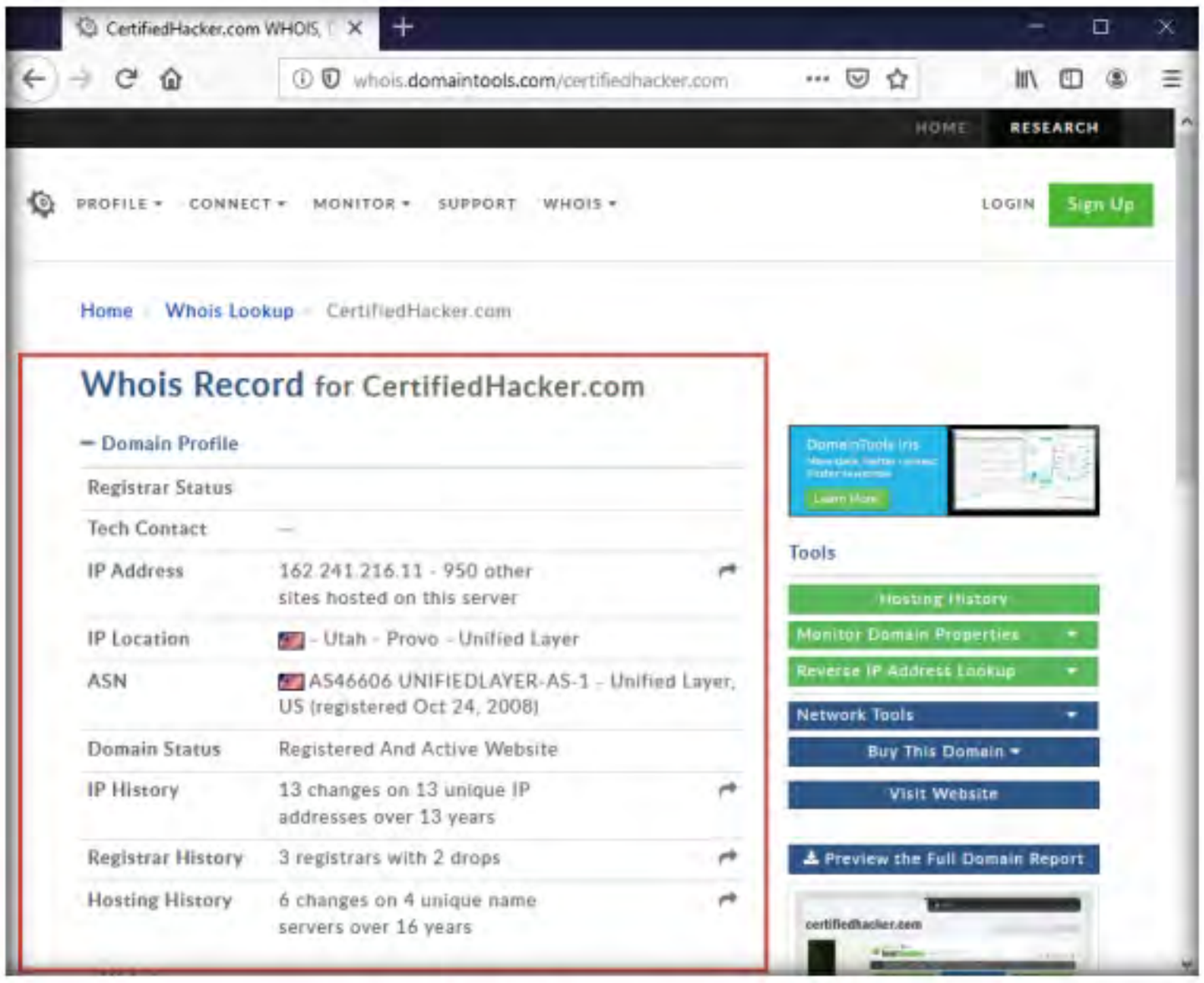


Figure 6.1.2: whois.domaintools.com search results

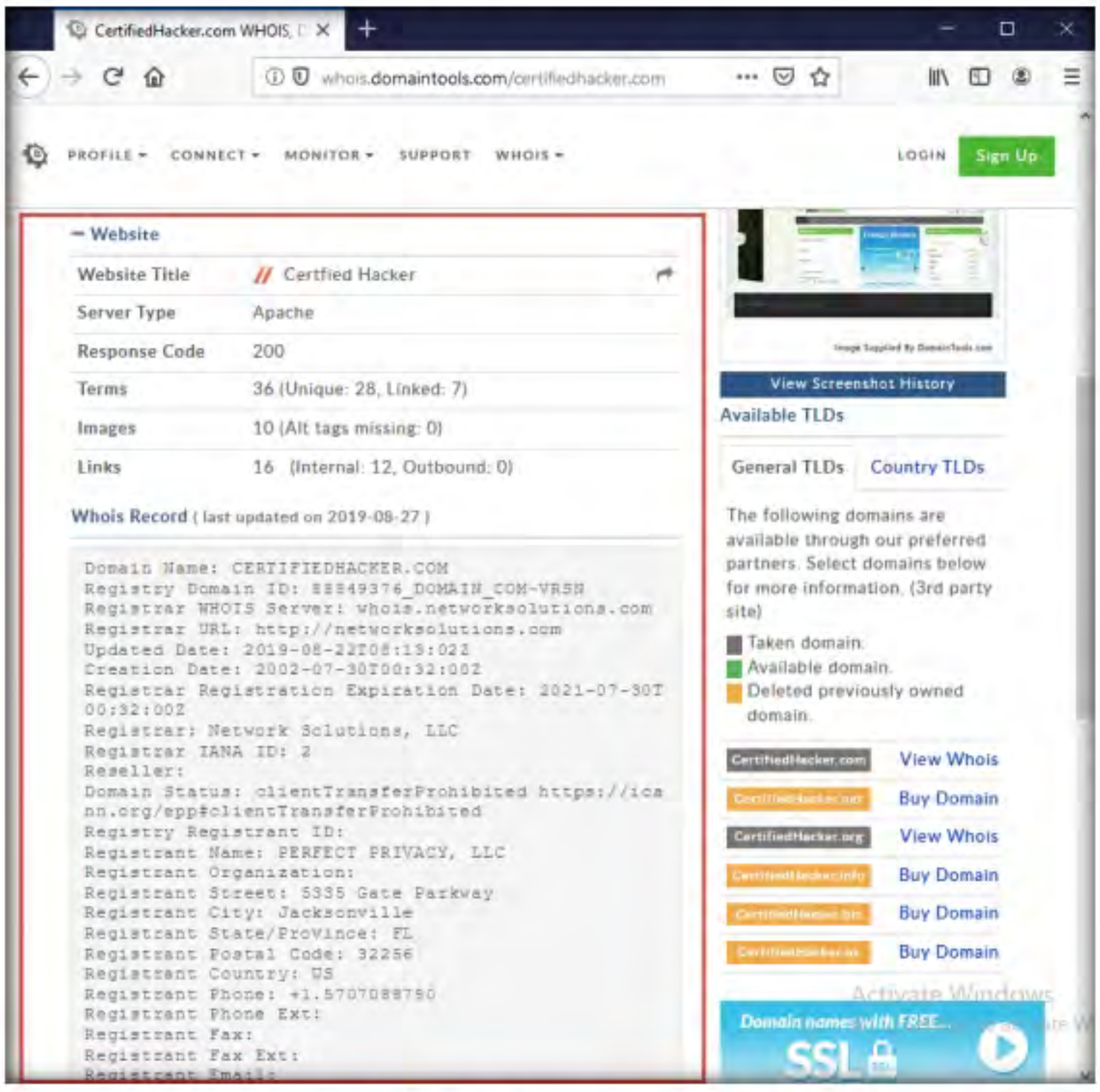


Figure 6.1.3: whois.domaintools.com search results

You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.

5. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 7

Perform DNS Footprinting

DNS, or Domain Name System, footprinting reveals information about DNS zone data.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker, you need to gather the DNS information of a target domain obtained during the previous steps. You need to perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, and much more about a target network.

Using this information, you can determine key hosts connected in the network and perform social engineering attacks to gather even more information.

Lab Objectives

- Gather DNS information using nslookup command line utility and online tool
- Perform reverse DNS lookup using reverse IP domain check and DNSRecon

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Lab Duration

Time: 10 Minutes

Overview of DNS

DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all IP addresses of the required application. DNS helps in converting the IP address to a more easily understandable domain format, which eases the burden on human beings.

Lab Tasks

TASK 1 — Gather DNS Information using nslookup Command Line Utility and Online Tool

Here, we will perform DNS information gathering about target organizations using the nslookup command-line utility and NSLOOKUP web application.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1 — Launch nslookup Terminal

3. Launch a command prompt, type **nslookup**, and press **Enter**. This displays the default server and its address assigned to the **Windows 10** virtual machine.

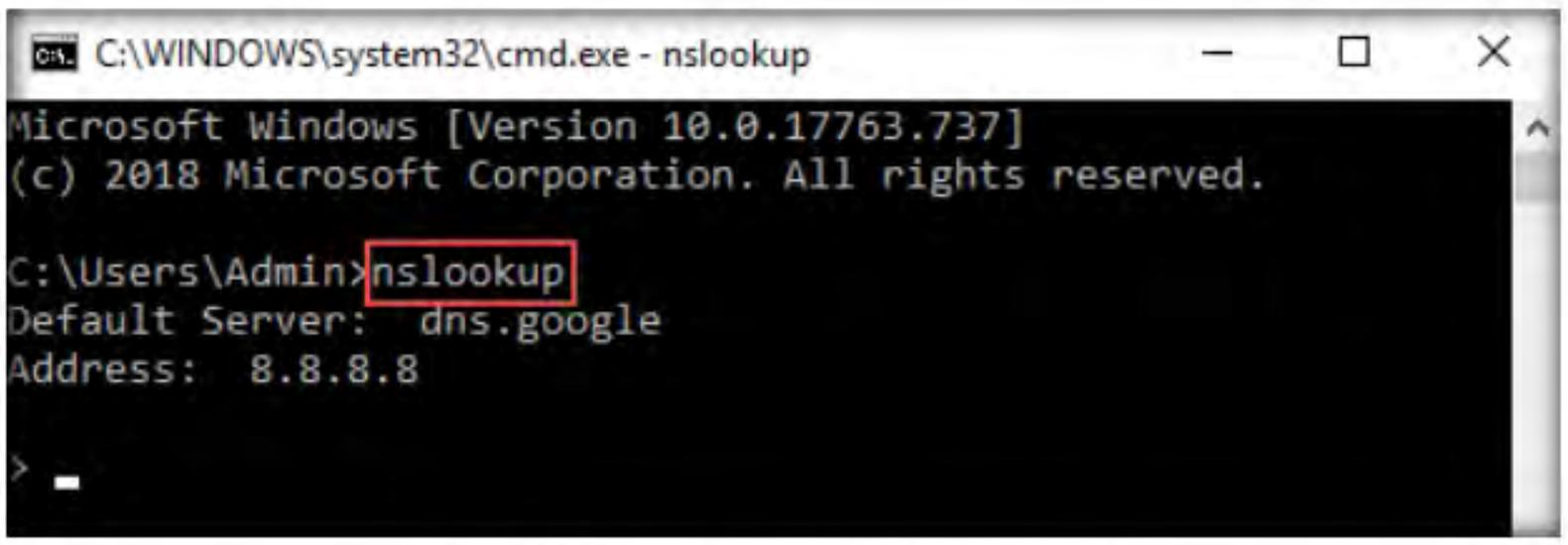


Figure 7.1.1: Command prompt with nslookup command

Note: The DNS server address (8.8.8.8) may differ in your lab environment.

TASK 1.2 — Obtain the IP Address of the Target Domain using nslookup

4. In the nslookup **interactive** mode, type **set type=a** and press **Enter**. Setting the type as "**a**" configures nslookup to query for the IP address of a given domain.

5. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.

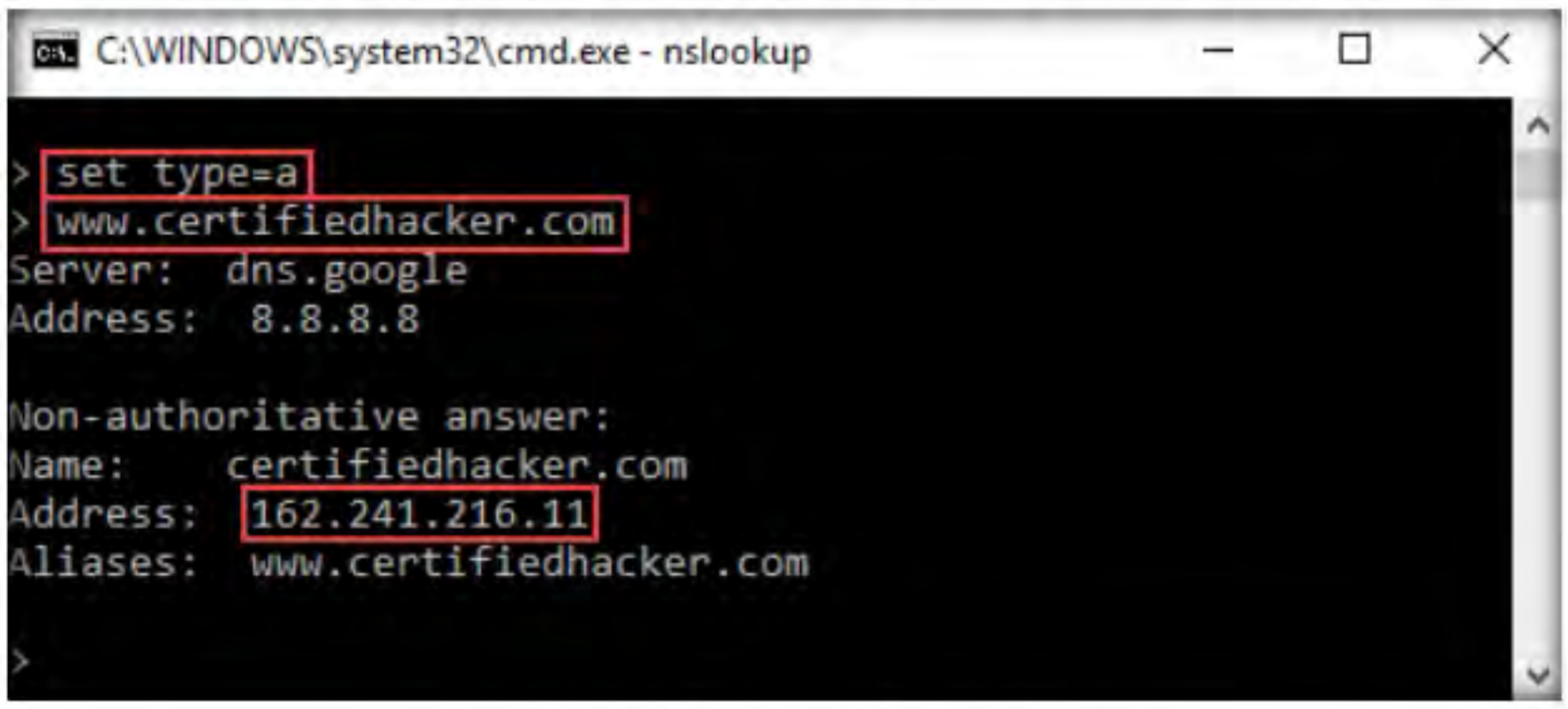


Figure 7.1.2: In nslookup command, set type=a option

nslookup is a network administration command-line utility, generally used for querying the DNS to obtain a domain name or IP address mapping or for any other specific DNS record. This utility is available both as a command-line utility and web application.

6. The first two lines in the result are:

   Server: dns.google and **Address: 8.8.8.8**

   This specifies that the result was directed to the default server hosted on the local machine (**Windows 10**) that resolves your requested domain.

7. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**; it is considered to be a non-authoritative answer. Here, the IP address of the target domain **www.certifiedhacker.com** is **162.241.216.11**.

Note: The IP address of the target may differ in your lab environment.

8. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.

TASK 1.3

Find Cname

9. Type **set type=cname** and press **Enter**. The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.
10. Type **certifiedhacker.com** and press **Enter**.
11. This returns the domain's authoritative name server (**ns1.bluehost.com**), along with the mail server address (**dnsadmin.box5331.bluehost.com**), as shown in the screenshot.

Note: The results may differ in your lab environment.

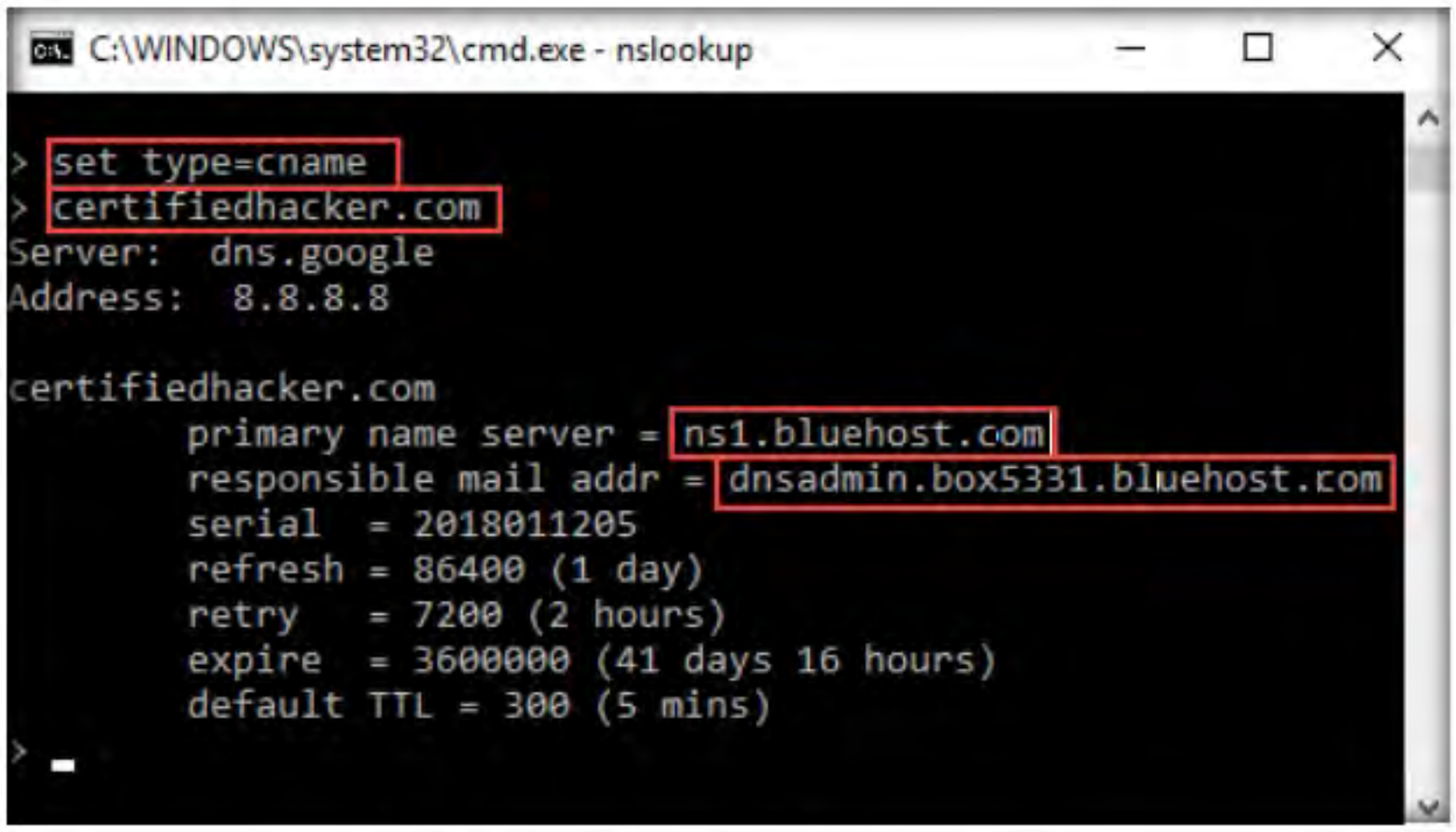


Figure 7.1.3: In nslookup command, set type=cname option

12. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.

TASK 1.4

Obtain the IP Address of the Primary Name Server

13. Issue the command **set type=a** and press **Enter**.
14. Type **ns1.bluehost.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server, as shown in the screenshot.

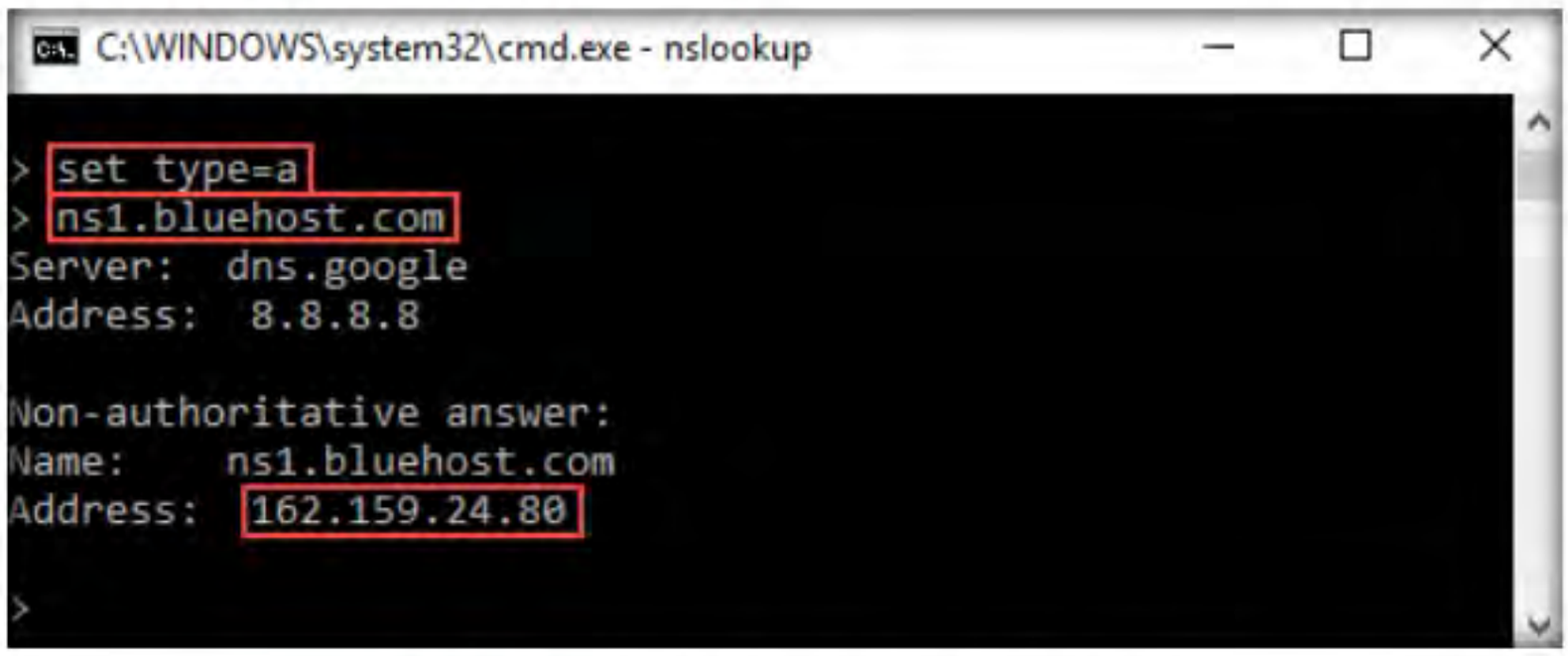


Figure 7.1.4: Screenshot showing returns the IP address of the server

15. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.
16. You can also perform the same operations using the NSLOOKUP online tool. Conduct a series of queries and review the information to gain familiarity with the NSLOOKUP tool and gather information.
17. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.

TASK 1.5

Perform DNS Footprinting using NSLOOKUP Online Utility

18. Open any web browser (here, **Mozilla Firefox**) and navigate to **http://www.kloth.net/services/nslookup.php**.
19. Once the site opens, in the **Domain:** field, enter **certifiedhacker.com**. Set the **Query:** field to default [**A (IPv4 address)**] and click the **Look it up** button to review the results that are displayed.

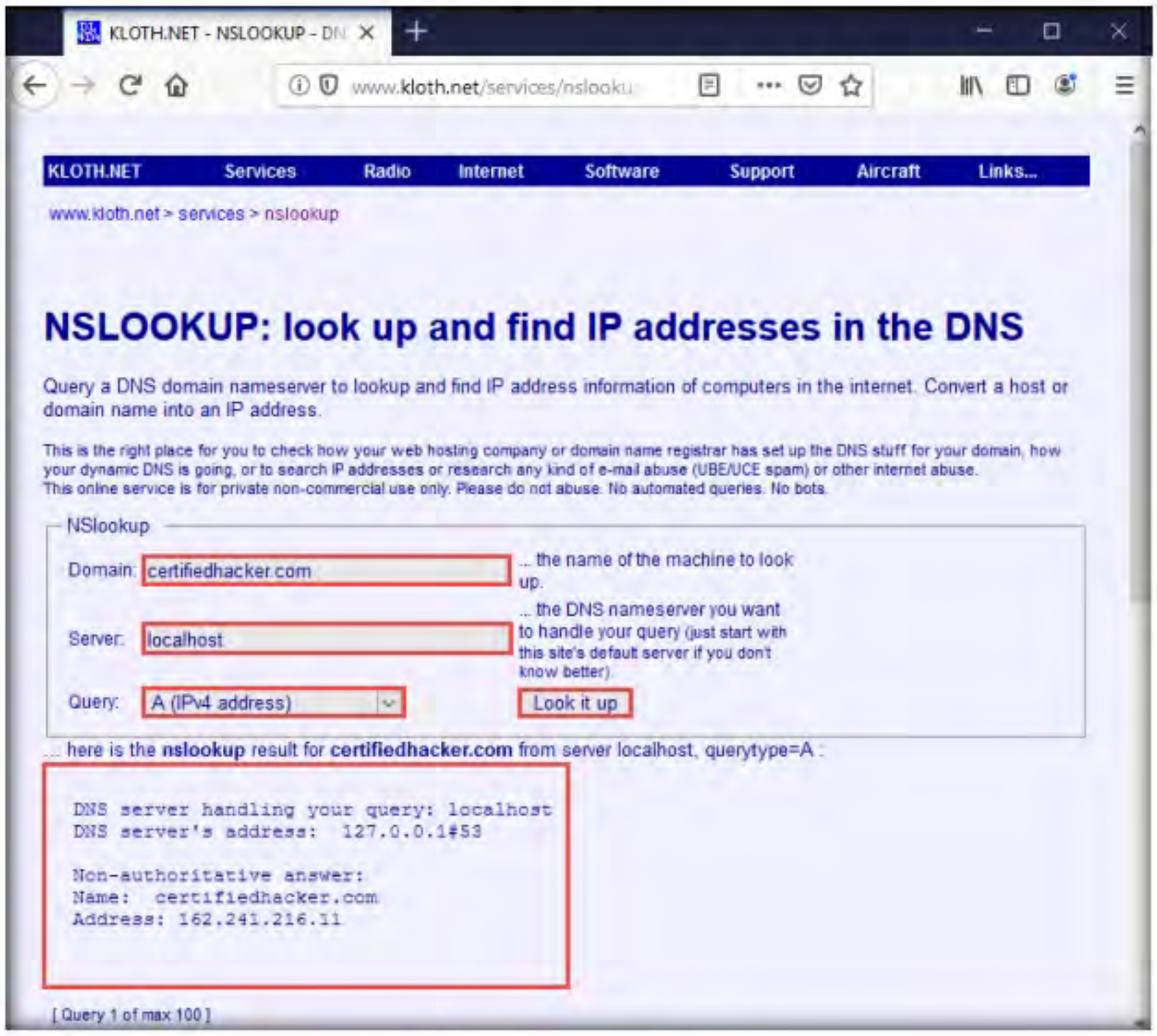


Figure 7.1.5: NSLOOKUP search page

20. In the **Query:** field, click the drop-down arrow and check the different options that are available, as shown in the screenshot.

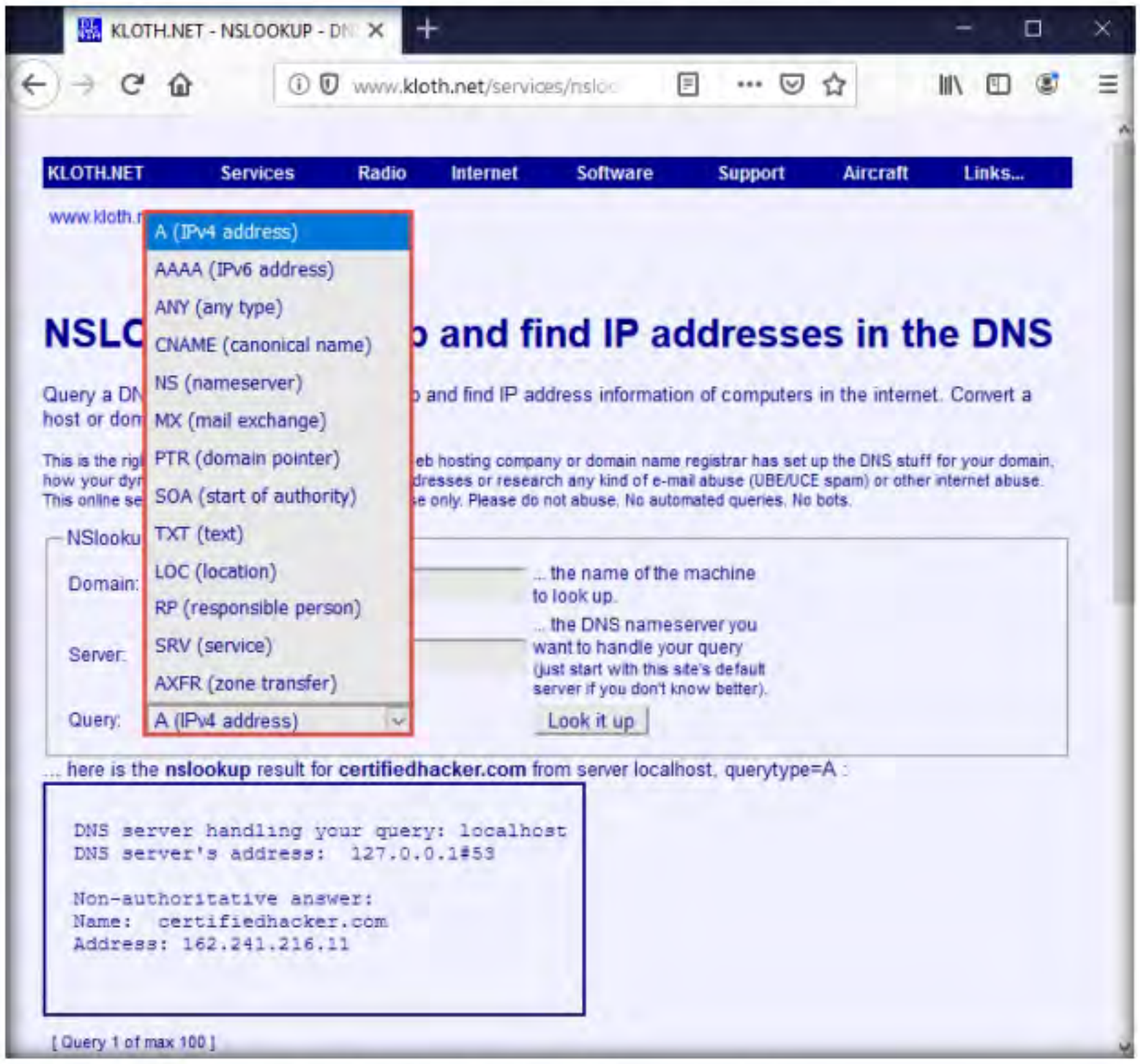


Figure 7.1.6: Screenshot showing different options for the query

21. As you can see, there is an option for **AAAA (IPv6 address)**; select that and click **Look it up**. Perform queries related to this, since there are attacks that are possible over IPv6 networks as well.

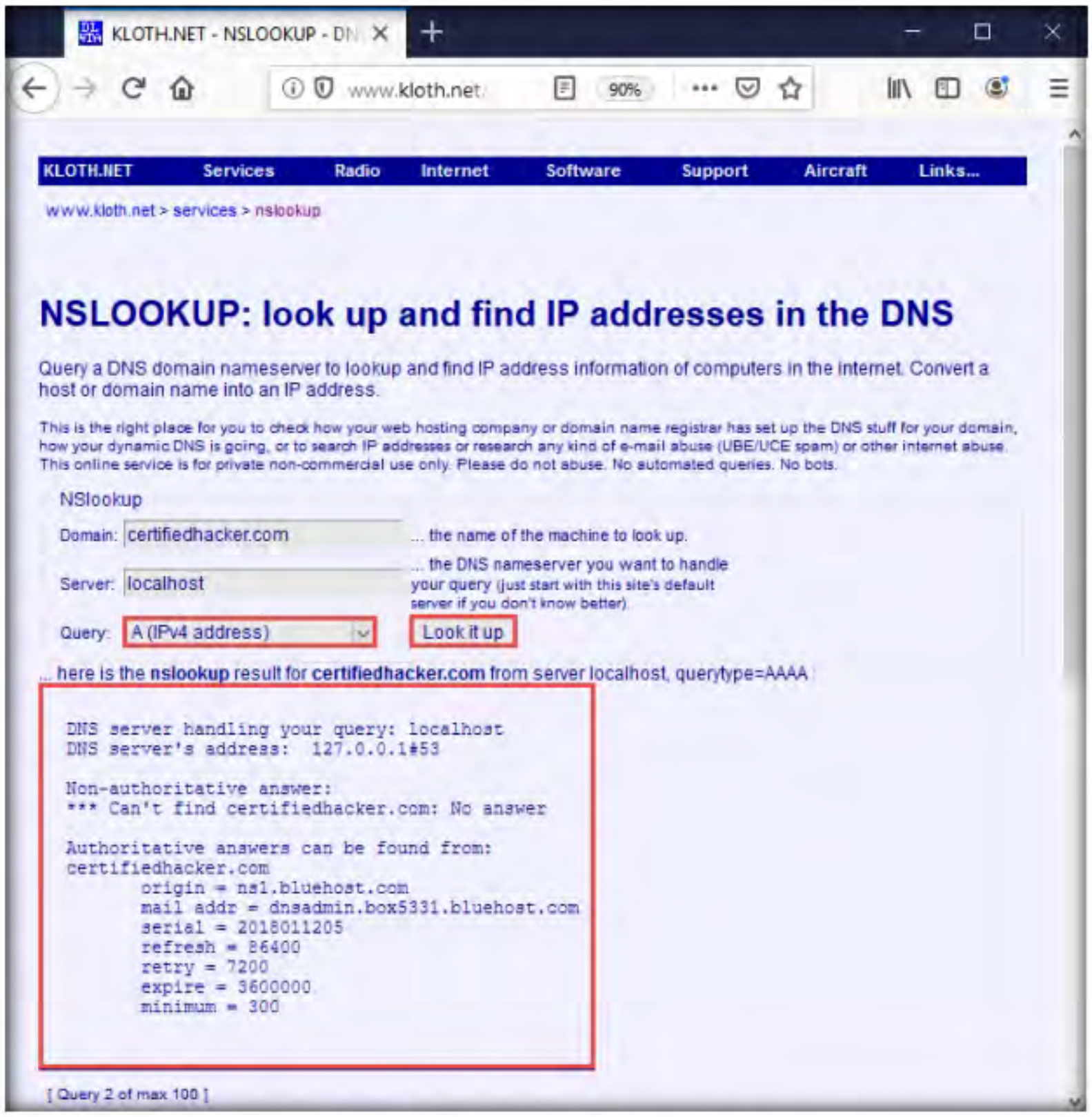


Figure 7.1.7: Screenshot showing IPv6 query results

You can also use DNS lookup tools such as **Professional Toolset** (https://tools.dnsstuff.com), **DNS Records** (https://network-tools.com), etc. to extract additional target DNS information.

22. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.
23. Close all open windows and document all the acquired information.

TASK 2

Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address.

Here, we will perform reverse DNS lookup using you get signal's Reverse IP Domain Check tool to find the other domains/sites that share the same web server as our target server.

Here, we will also perform a reverse DNS lookup using DNSRecon on IP range in an attempt to locate a DNS PTR record for those IP addresses.

TASK 2.1

Perform Reverse DNS Lookup using Reverse IP Domain Check

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.yougetsignal.com**. On the website, click **Reverse IP Domain Check**.

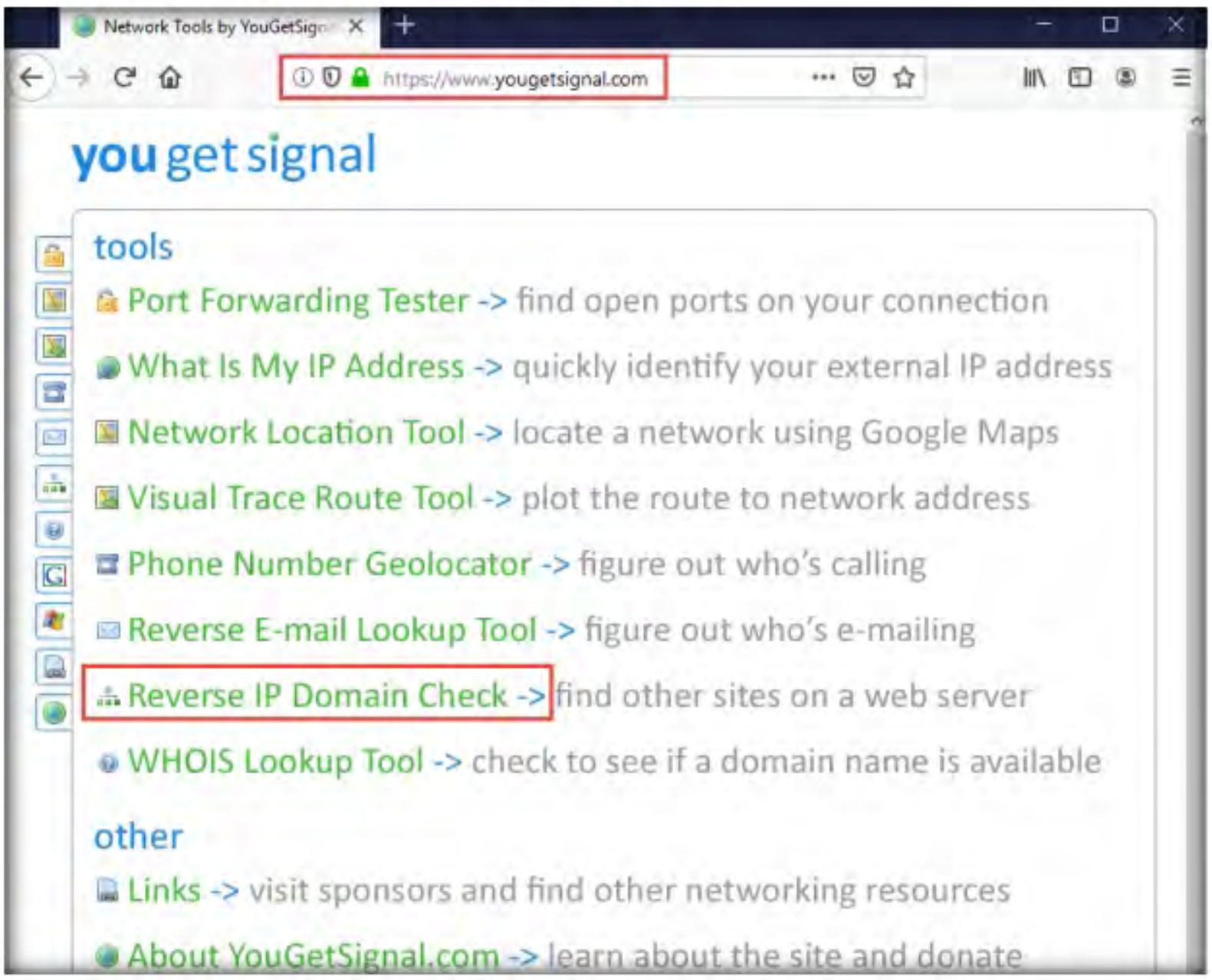


Figure 7.2.1: You Get Signal website

2. On the **Reverse IP Domain Check** page, enter **www.certifiedhacker.com** in the **Remote Address** field and click **Check** to find other domains/sites hosted on a certifiedhacker.com web server. You will get the list of domains/sites hosted on the same server as **www.certifiedhacker.com,** as shown in the screenshot

Figure 7.2.2: Reverse IP Domain Check

TASK 2.2

Perform Reverse DNS Lookup using DNSRecon

3. Close all open windows, document all the acquired information, and then turn off the **Windows 10** virtual machine
4. Turn on **Parrot Security** virtual machine.
5. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

9. Now, type **cd** and press **Enter** to jump to the root directory.

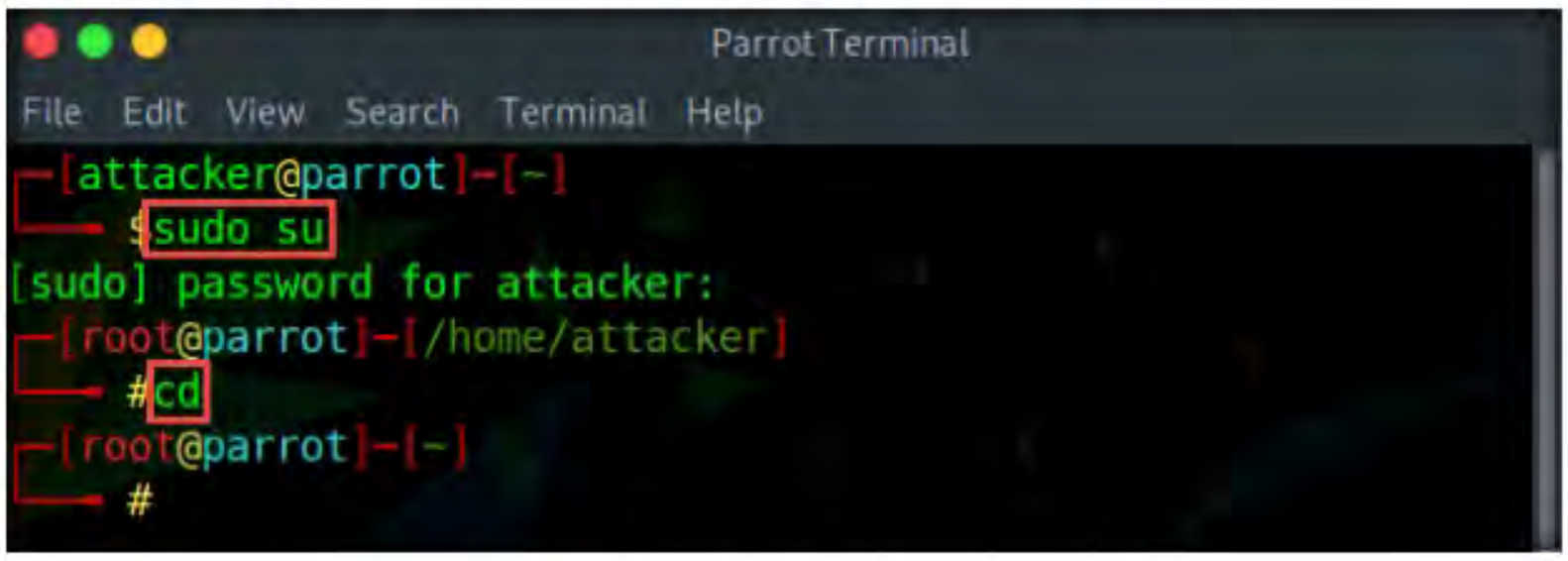


Figure 7.2.3: Running the programs as a root user

10. In the **Parrot Terminal** window, type **dnsrecon -r 162.241.216.0-162.241.216.255** and press **Enter** to locate a DNS PTR record for IP addresses between 162.241.216.0 - 162.241.216.255.

Note: Here, we will use the IP address range, which includes the IP address of our target, that is, the certifiedhacker.com domain (162.241.216.11), which we acquired in the previous steps.

Note: -r option specifies the range of IP addresses (first-last) for reverse lookup brute force.

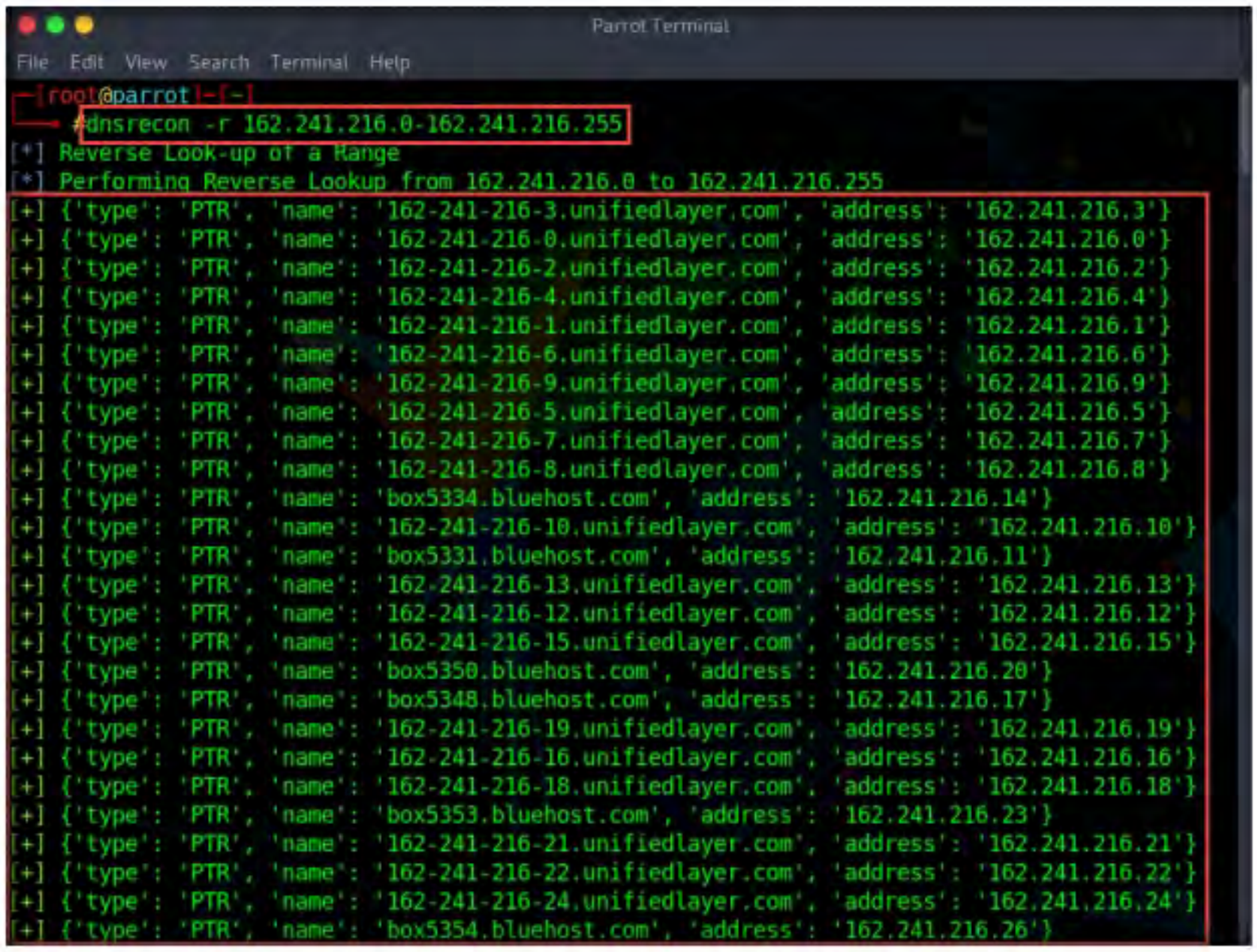


Figure 7.2.4: Reverse IP Domain Check using DNSRecon

11. This concludes the demonstration of gathering information about a target organization by performing reverse DNS lookup using "you get signal's" Reverse IP Domain Check and DNSRecon tool.
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 8

Perform Network Footprinting

Network footprinting is a process of gathering network-related information of a target organization.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With the IP address, hostname, and domain obtained in the previous information gathering steps, as a professional ethical hacker, your next task is to perform network footprinting to gather the network-related information of a target organization such as network range, traceroute, TTL values, etc. This information will help you to create a map of the target network and perform a man-in-the-middle attack.

Lab Objectives

- Locate the network range
- Perform network tracerouting in Windows and Linux Machines
- Perform advanced network route tracing using Path Analyzer Pro

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Path Analyzer Pro located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro**
- You can also download the latest version of Path Analyzer Pro from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 15 Minutes

Overview of Network Footprinting

Network footprinting is a process of accumulating data regarding a specific network environment. It enables ethical hackers to draw a network diagram and analyze the target network in more detail to perform advanced attacks.

Lab Tasks

TASK 1

Locate the Network Range

Here, we will locate the network range using the ARIN Whois database search tool.

Network range information assists in creating a map of the target network. Using the network range, you can gather information about how the network is structured and which machines in the networks are alive. Further, it also helps to identify the network topology and access the control device and operating system used in the target network.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.arin.net/about/welcome/region**.
4. In the search bar, enter the IP address of the target organization (here, the target organization is **certifiedhacker.com**, whose IP is **162.241.216.11**), and then click the **Search** button.

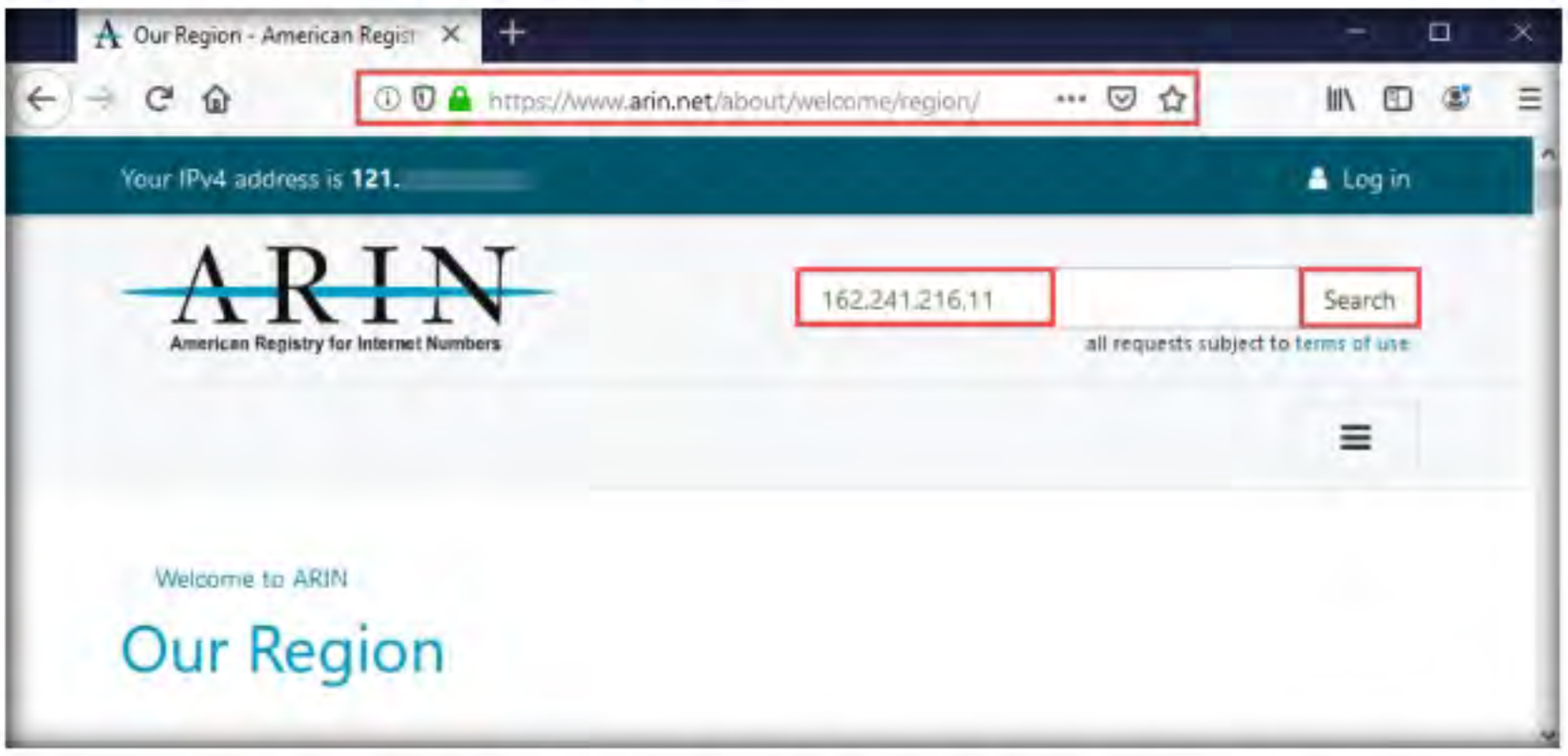


Figure 8.1.1: Entering the target IP address in the ARIN whois database search tool

5. You will get the information about the network range along with the other information such as network type, registration information, etc.

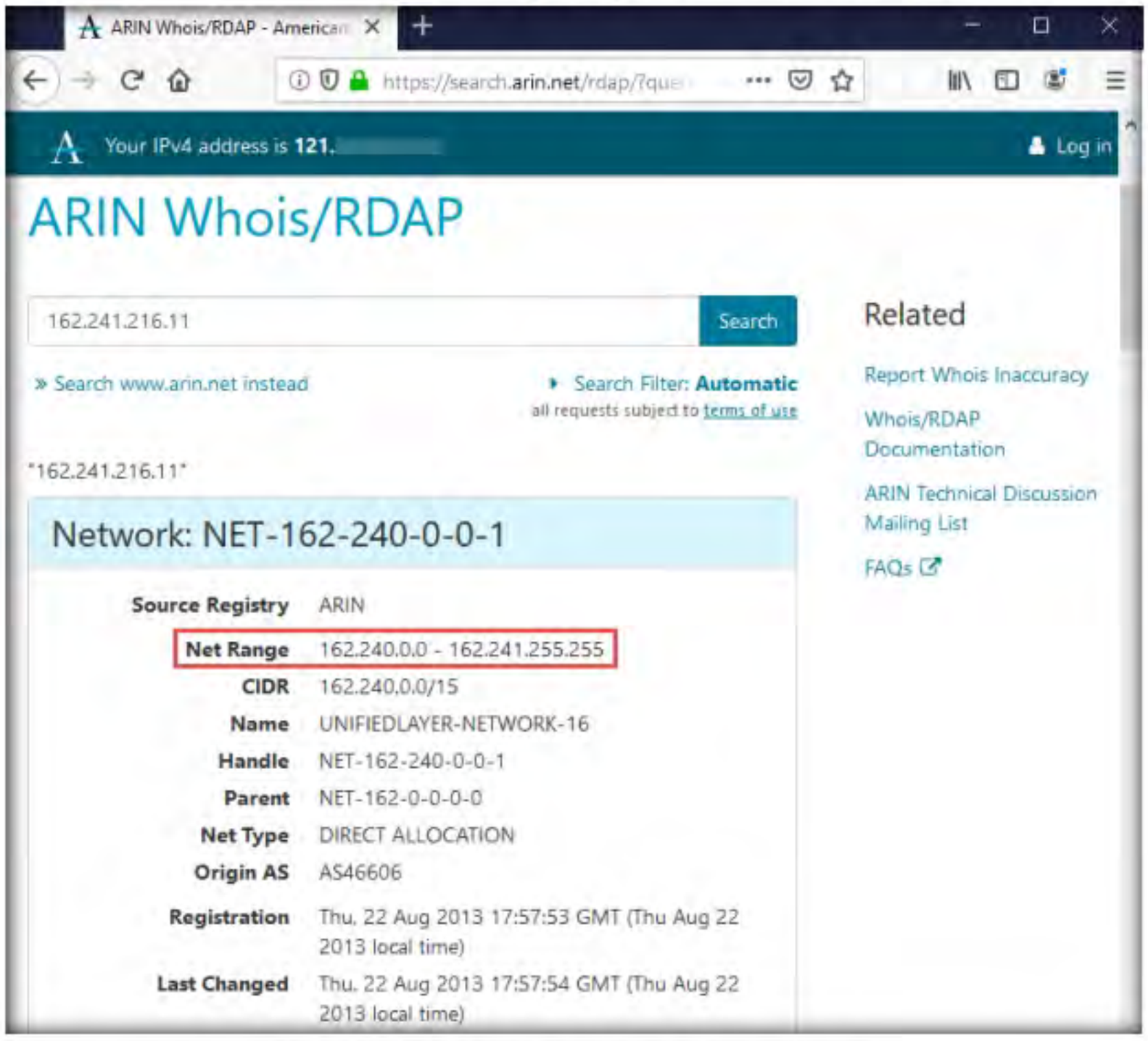


Figure 8.1.2: Network range information of the target organization

6. This concludes the demonstration of locating network range using the ARIN Whois database search tool.
7. Close all open windows and document all the acquired information.

TASK 2 Perform Network Tracerouting in Windows and Linux Machines

Here, we will perform network tracerouting using both Windows and Linux machines.

TASK 2.1 Tracerouting using Windows Machine

1. In the **Windows 10** virtual machine, open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

Note: If you get the **Request timed out** reply for the above query, then use **Command Prompt of your host machine** instead of the Windows 10 virtual machine to run the query.

The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between the source and destination, which enables you to map the network topology of the organization. Traceroute can be used to extract information about network topology, trusted routers, firewall locations, etc.

Note: Screenshots may vary depending on the target destination.

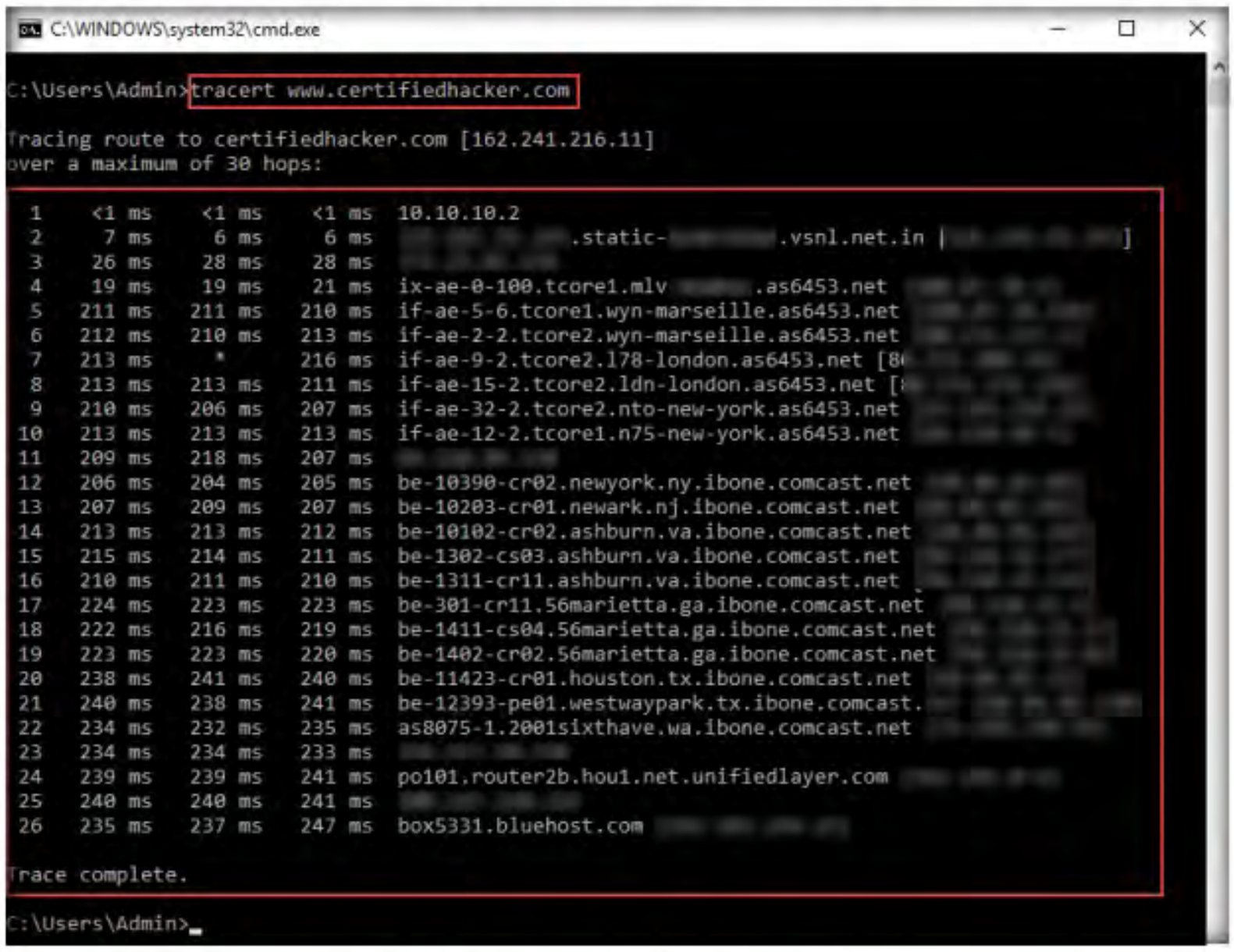


Figure 8.2.1: tracert command in windows machine

2. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.

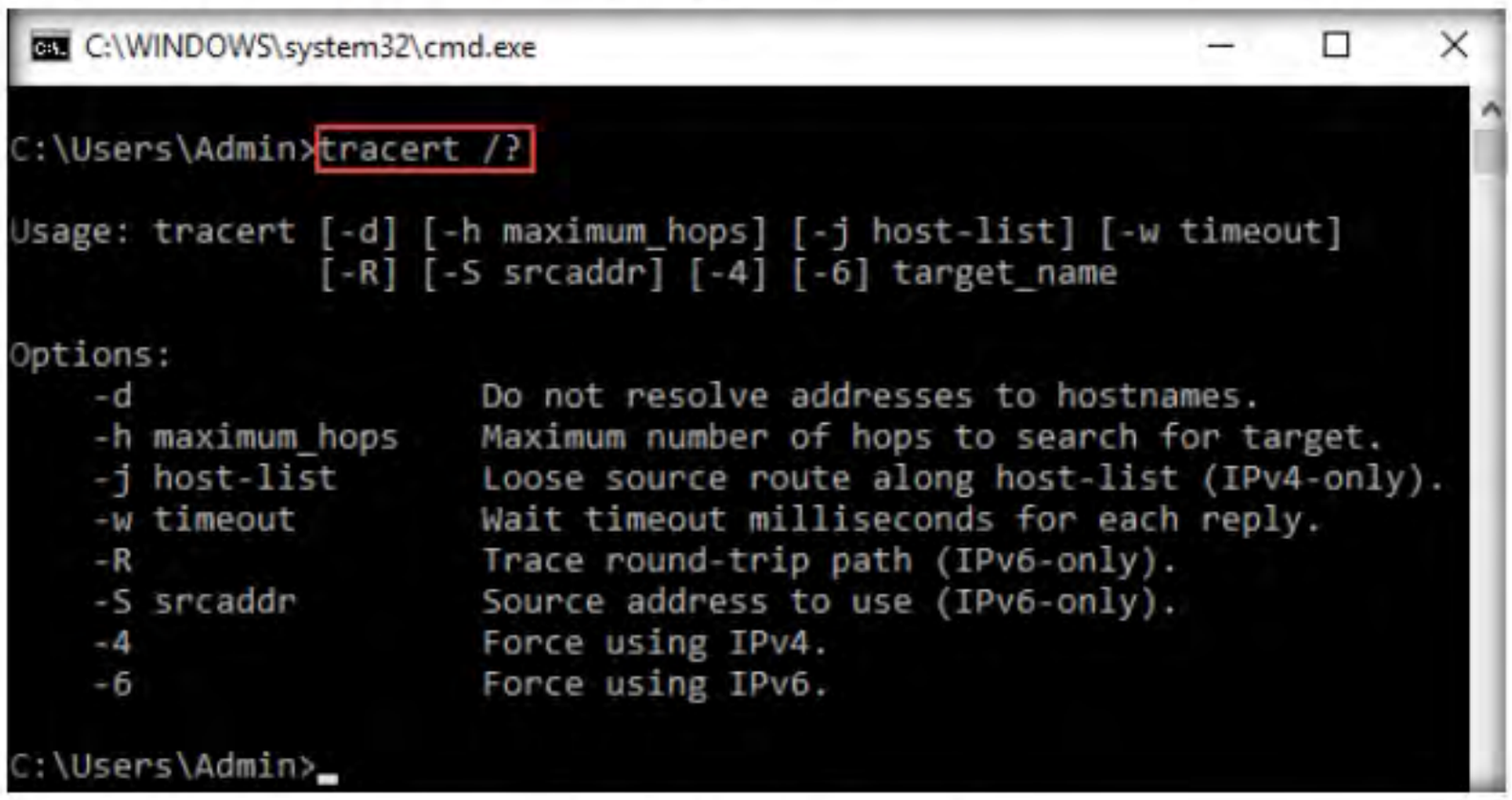


Figure 8.2.2: Tracert help command

3. Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

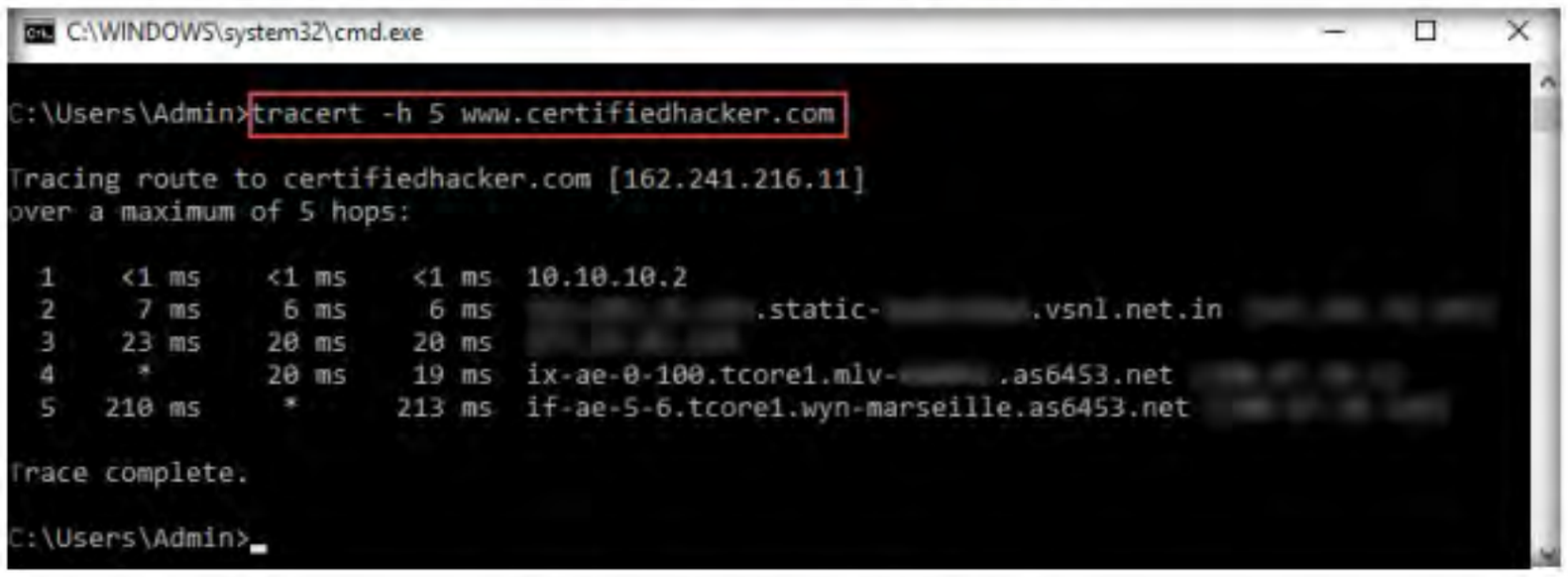


Figure 8.2.3: tracing the route with only 5 hops

4. After viewing the result, close the command prompt window.

TASK 2.2

Traceroute using Linux Machine

5. Turn on the **Parrot Security** virtual machine.
6. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

10. Now, type **cd** and press **Enter** to jump to the root directory.

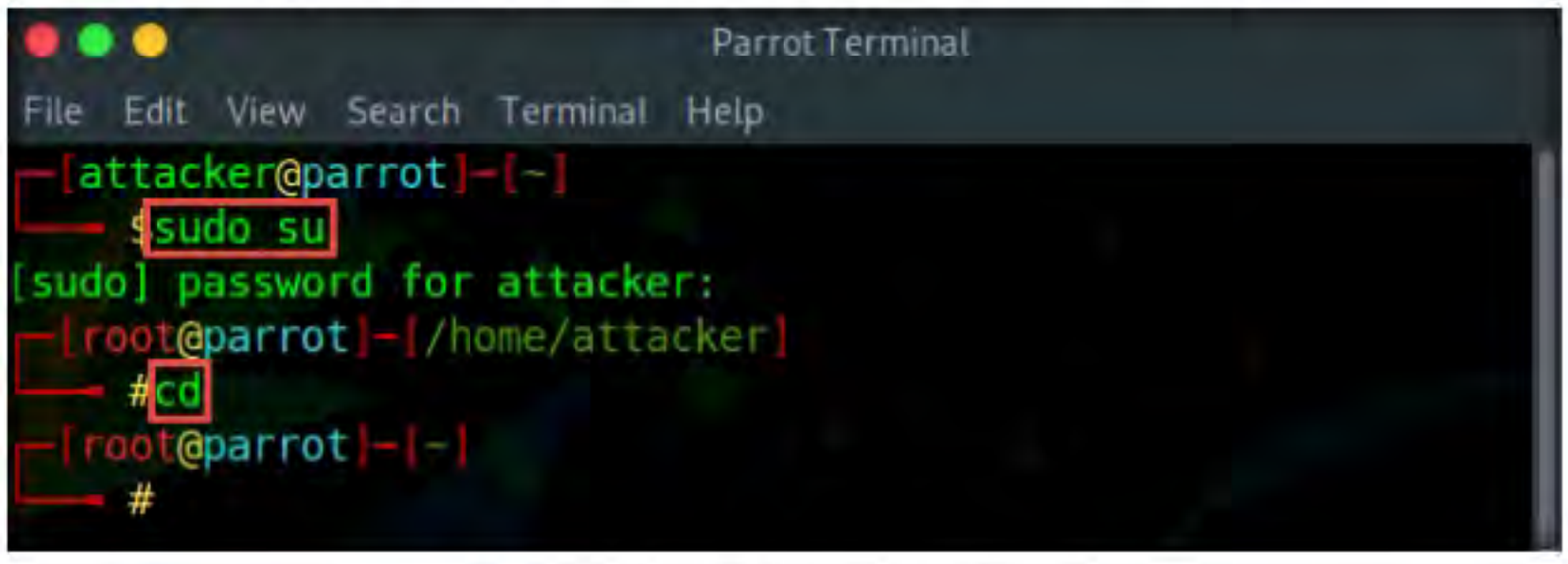


Figure 8.2.4: Running the programs as a root user

11. In the terminal window, type **traceroute www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

Note: Since we have set up a simple network, you can find the direct hop from the source to the target destination. However, screenshots may vary depending on the target destination.

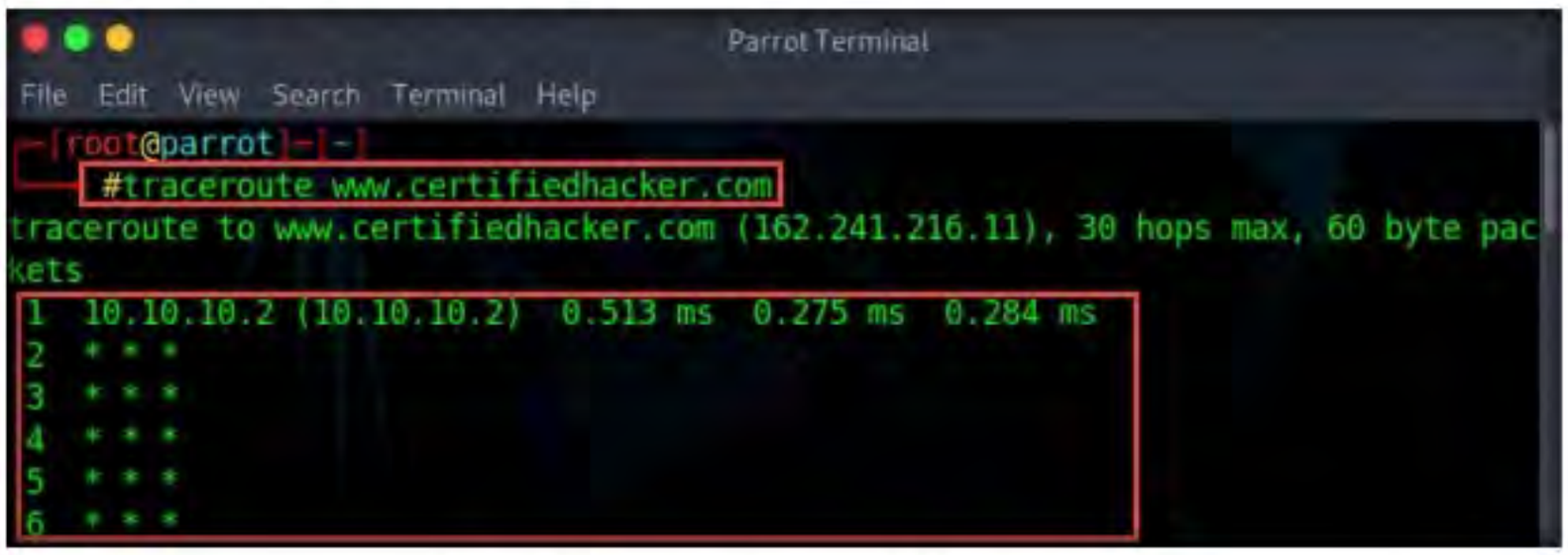


Figure 8.2.5: traceroute command in Linux machine

12. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
13. Close all open windows and document all the acquired information.
14. Turn off the **Parrot Security** virtual machine.

TASK 3

Perform Advanced Network Route Tracing Using Path Analyzer Pro

Traceroute is a system administrator utility to trace the route IP packets take from a source system to some destination system, and Path Analyzer Pro summarizes a given trace to any destination within seconds by generating a simple report with all the important information on the target. Path Analyzer Pro is an advanced network tracerouting tool where you can input any of the target details such as IP address, a hostname, or an email address.

Here, we will perform network tracerouting using Path Analyzer Pro.

1. In the **Windows 10** virtual machine, open **File Explorer** and navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro** and double-click **PAPro27.msi**.
2. The **Path Analyzer Pro 2.7** setup window appears.
3. Follow the wizard steps (by selecting default options) to install Path Analyzer Pro.

Note: If a **User Account Control** window appears, click **Yes**.

4. Click the **Start** menu and right-click **Path Analyzer Pro 2.7**. Expand **More** and click the **Run as administrator** options.

Note: If a **User Account Control** window appears, click **Yes**.

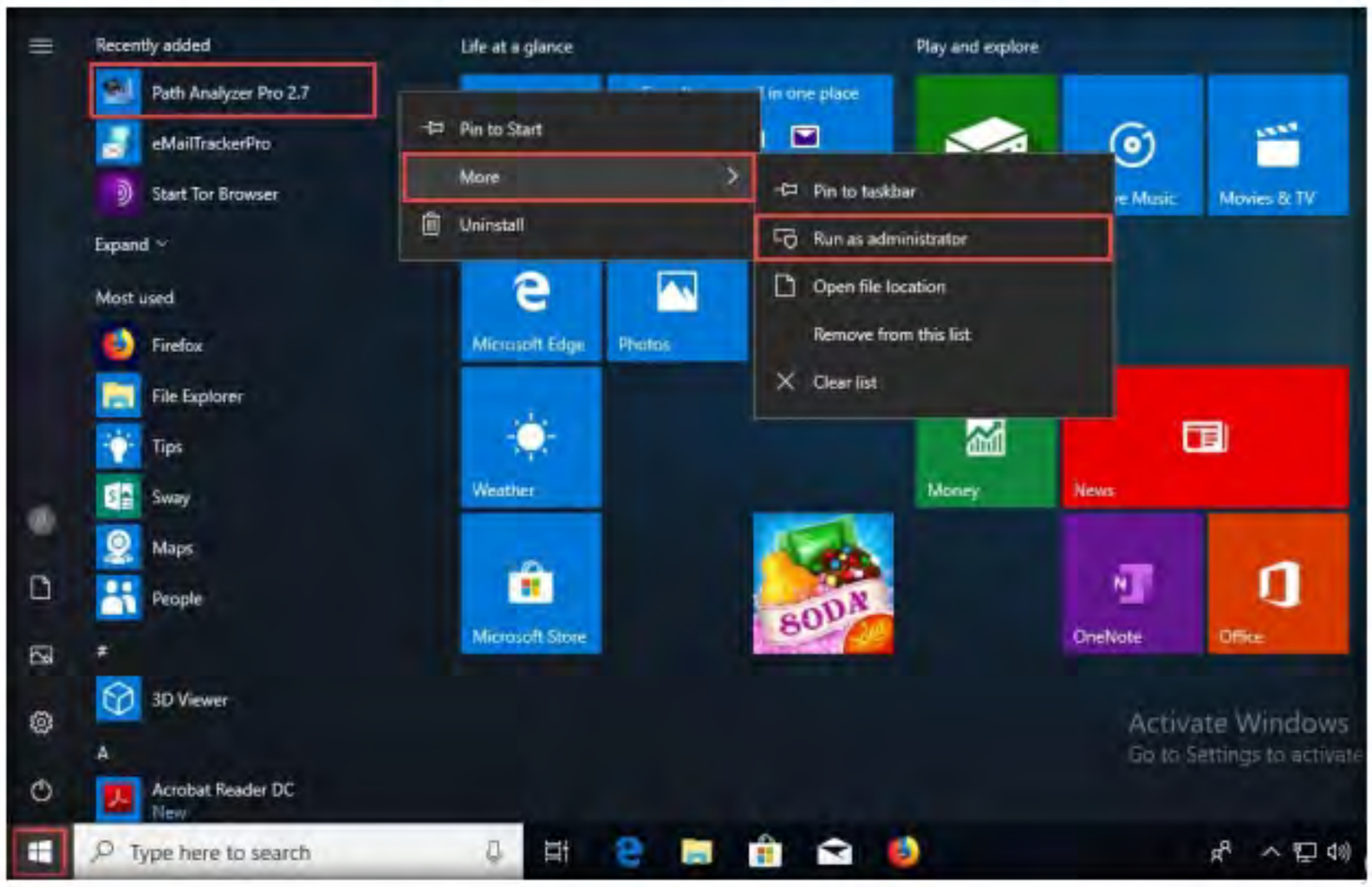


Figure 8.3.1: Launch Path Analyzer Pro 2.7

5. The **Path Analyzer Pro** window appears along with a **Registration Form** pop-up; click **Evaluate** in the pop-up.

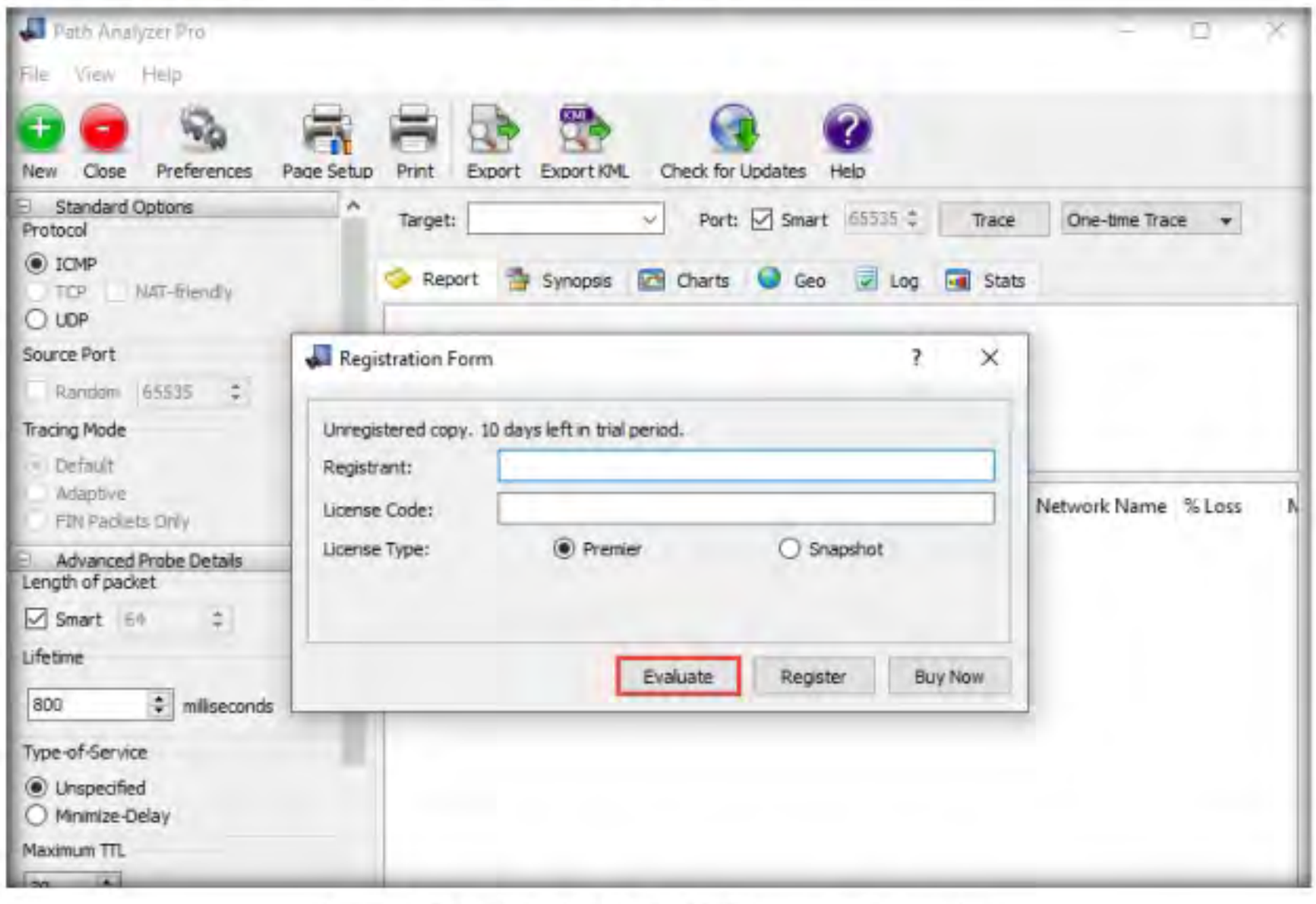


Figure 8.3.2: Path Analyzer Pro 2.7 Registration Form window

TASK 3.1

Trace a Target Network

6. In the left-pane of the **Path Analyzer Pro** window, a few options are set to default in the **Standard Options** and **Advanced Probe Details** sections. Ensure that the **ICMP** radio button under the **Protocol** field of **Standard Options** is selected and the **Smart** option under the **Length of packet** field of the **Advanced Probe Details** section is checked.

Note: If you have a firewall, it must be disabled for appropriate output.

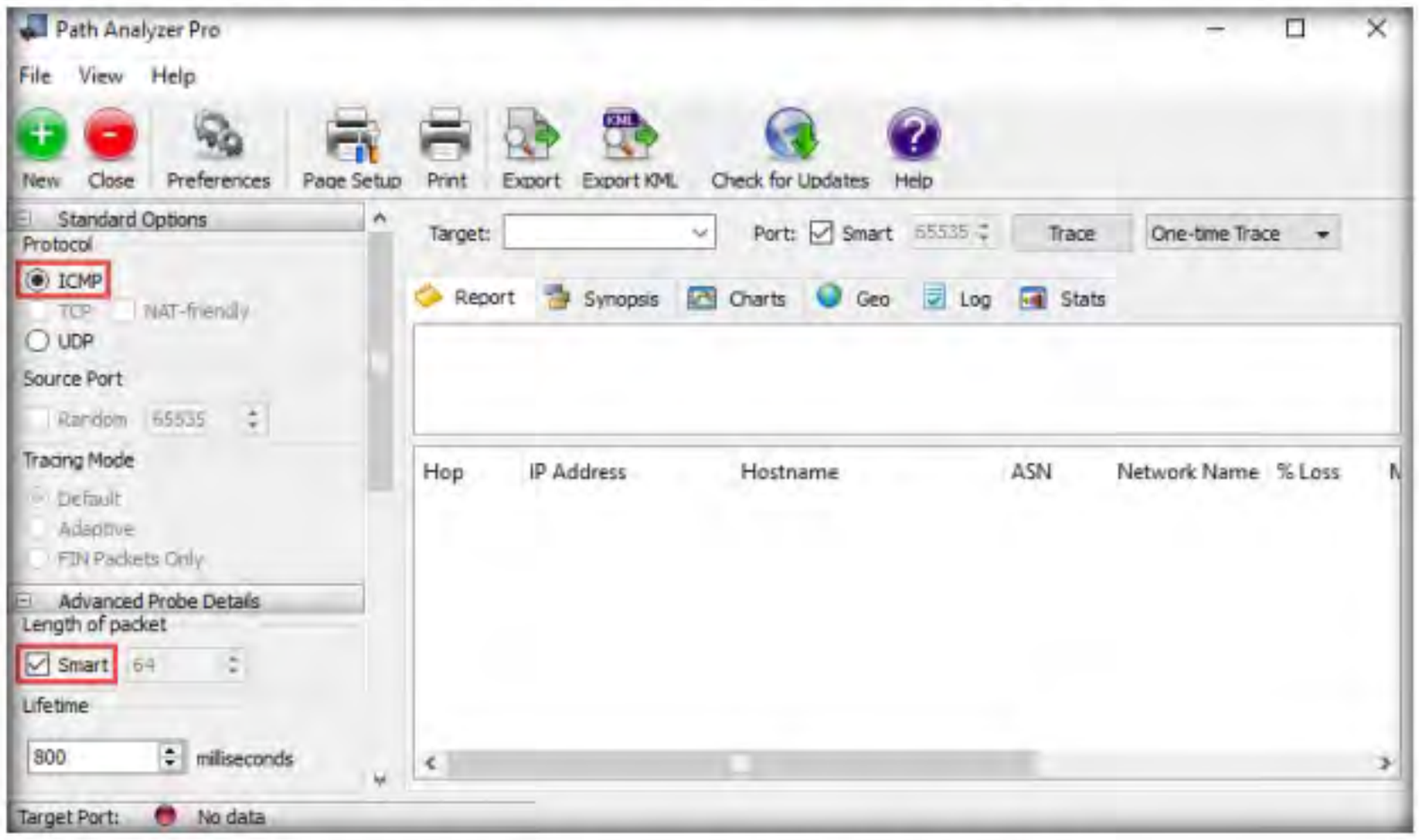


Figure 8.3.3: The Path Analyzer Pro Advanced Probe Details window

7. In the **Advanced Tracing Details** section, a few options are set to default. Ensure that the **Stop on control messages (ICMP)** option is checked in the **Advanced Tracing Details** section.

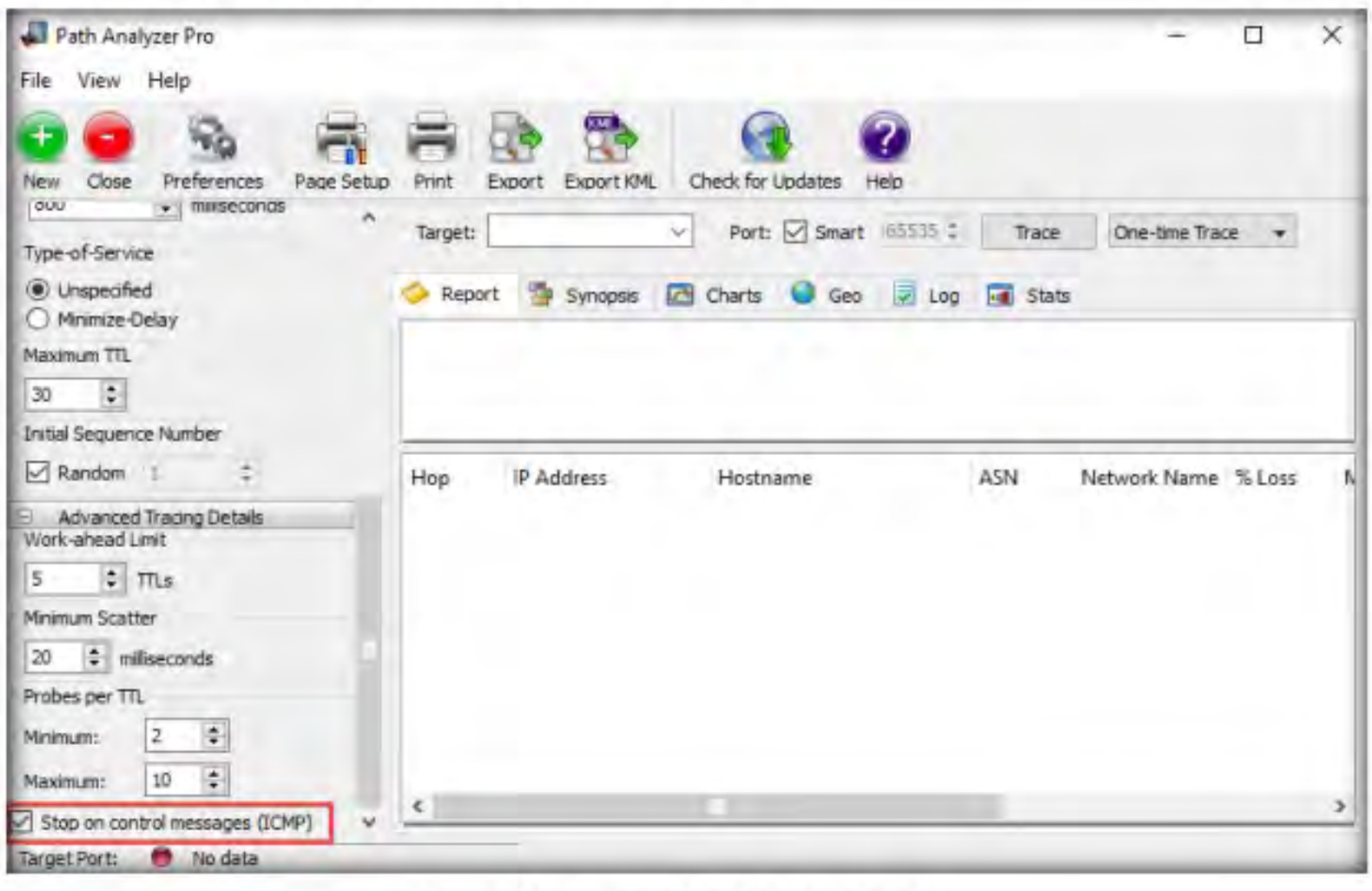


Figure 8.3.4: Advanced Tracing Details window

8. To perform the trace, enter the hostname in the **Target:** field (for instance, **www.google.com**) and ensure that **Smart** under the **Port:** field is checked (here, default is **65535**). From the drop-down menu, choose **Timed Trace** and click **Trace**.

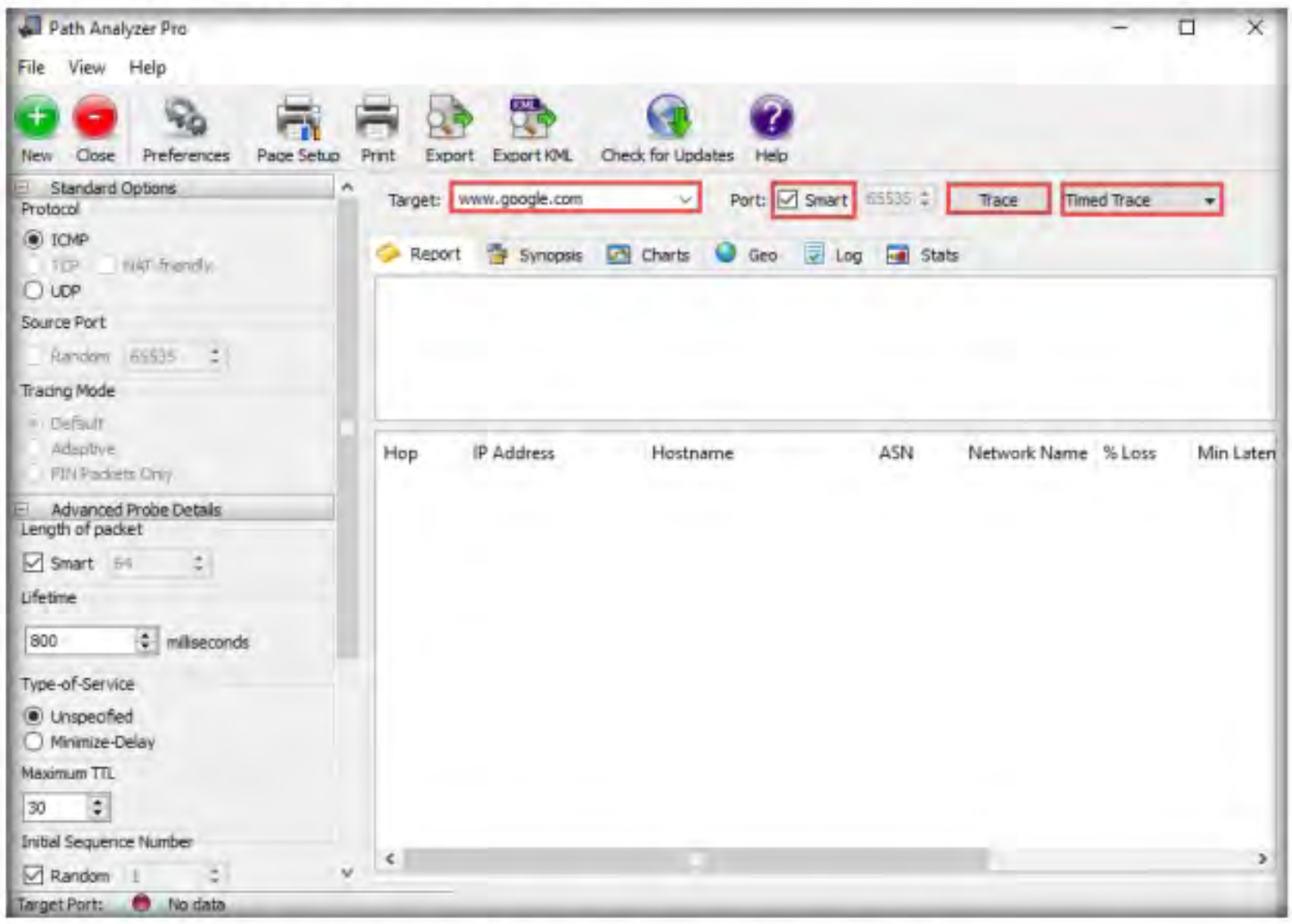


Figure 8.3.5: A Path Analyzer Pro Advanced Tracing Details option

9. The **Type time of trace** dialog box appears. Specify the time of trace (here, **mm** is changed to **3**) in the **hh: mm: ss** format and click **Accept**.

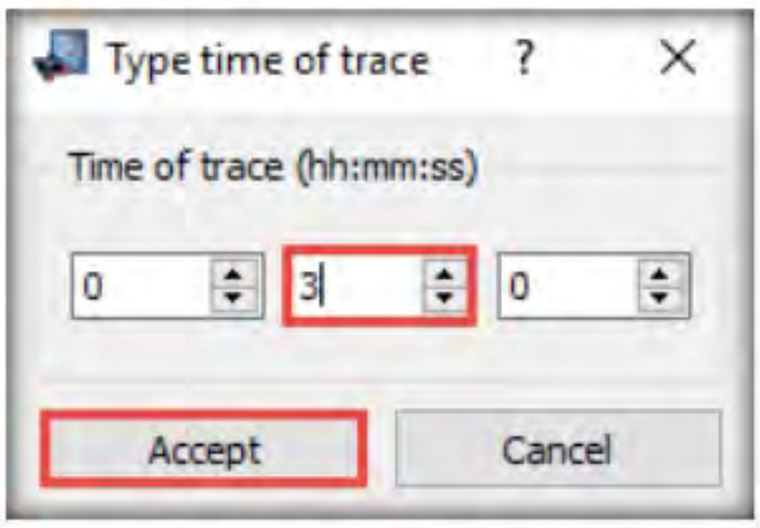


Figure 8.3.6: The Path Analyzer Pro Type time of trace option

10. While Path Analyzer Pro performs this trace, the **Trace** button changes automatically to **Stop**.

TASK 3.2

Examine the Results

11. After the trace is complete, the trace results are displayed under the **Report** tab in the form of a **linear chart** depicting the number of hops between you and the target.

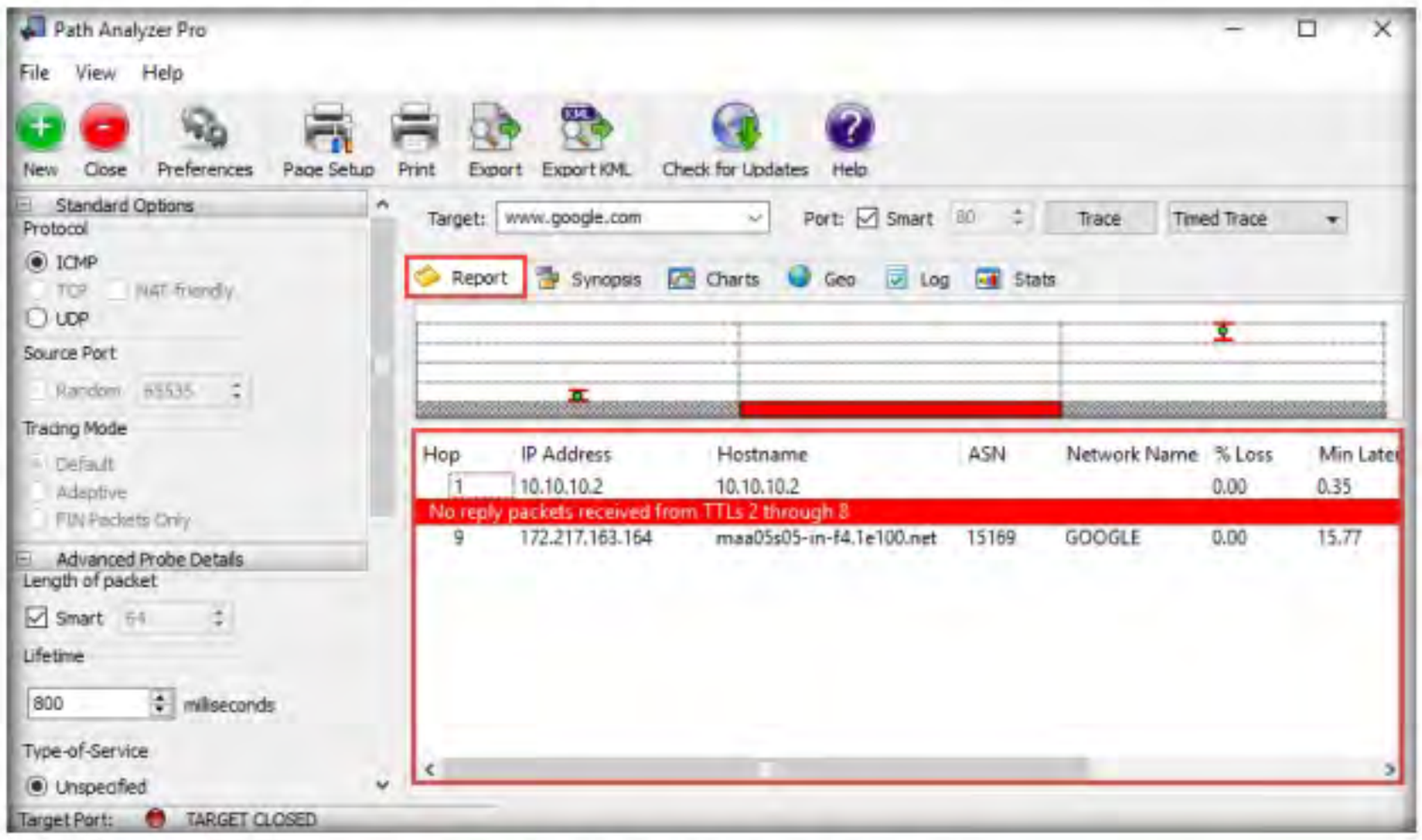


Figure 8.3.7: A Path Analyzer Pro Target option

12. Click the **Synopsis** tab, which displays a one-page summary of trace results.

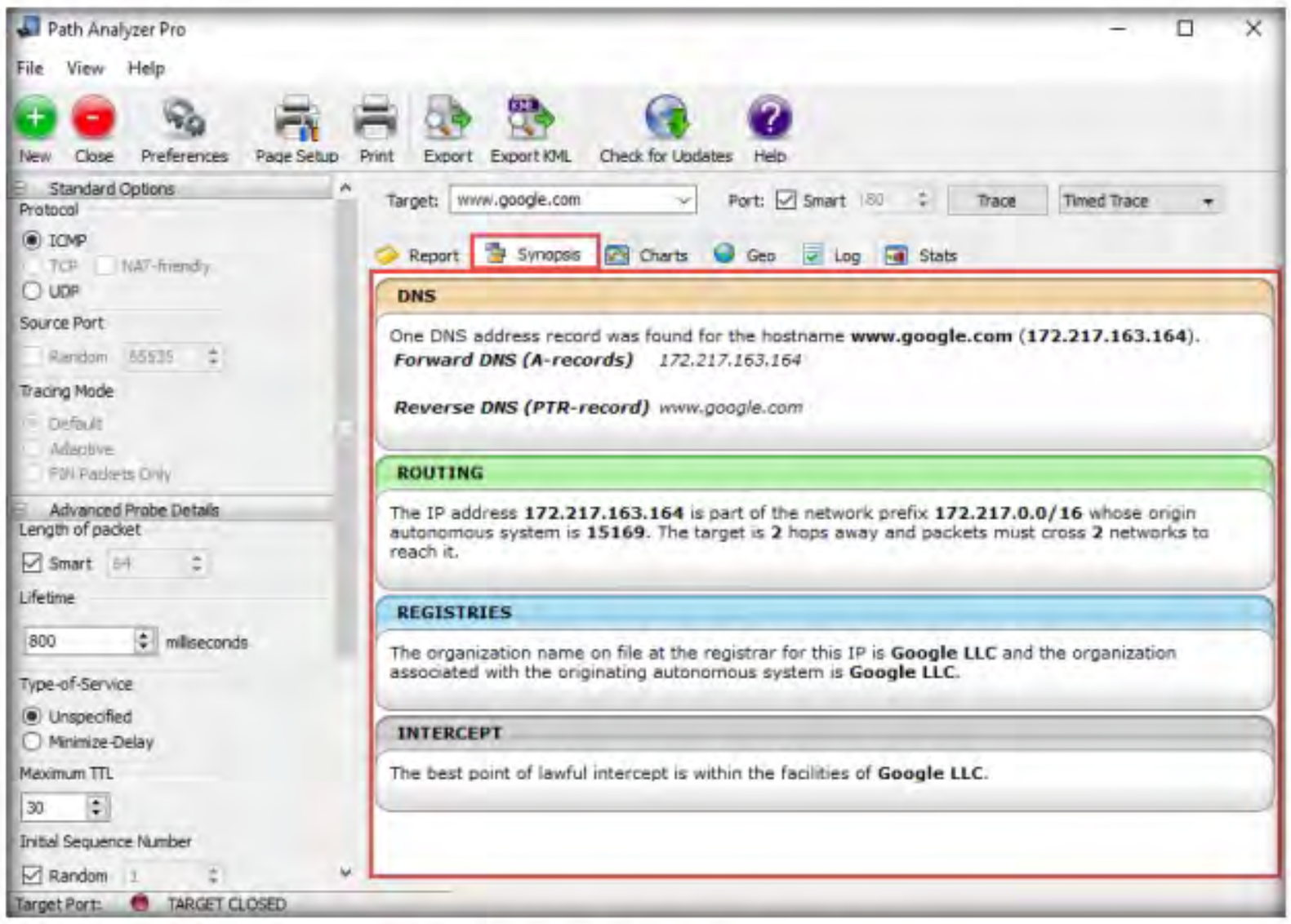


Figure 8.3.8: A Path Analyzer Pro Target option

TASK 3.3

View Charts

13. Click the **Charts** tab to view the results of the trace.

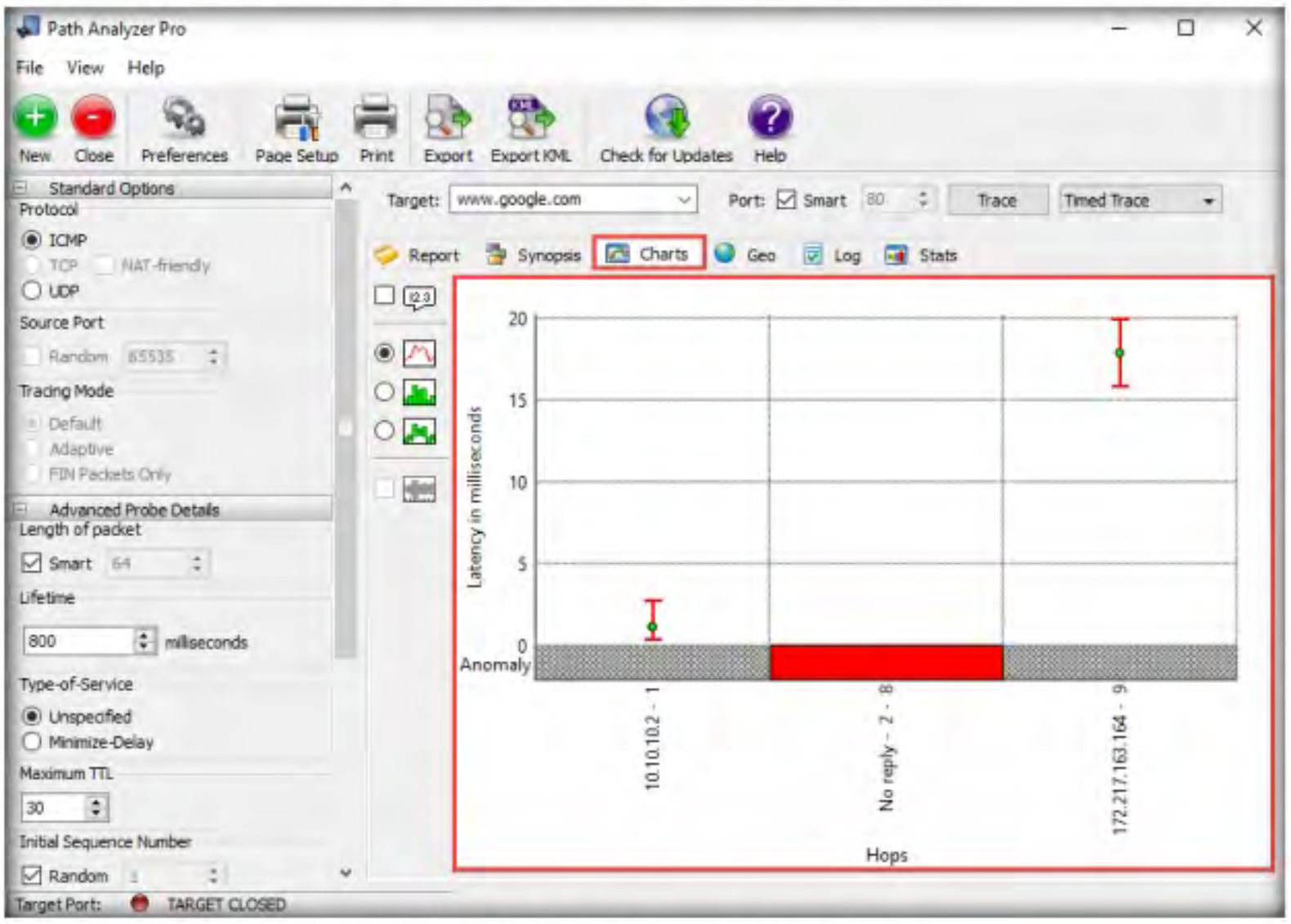


Figure 8.3.9: The Path Analyzer Pro Chart Window

TASK 3.4

Inspect the Geographical Location

14. Click **Geo**, which displays a world map of the traceroute.

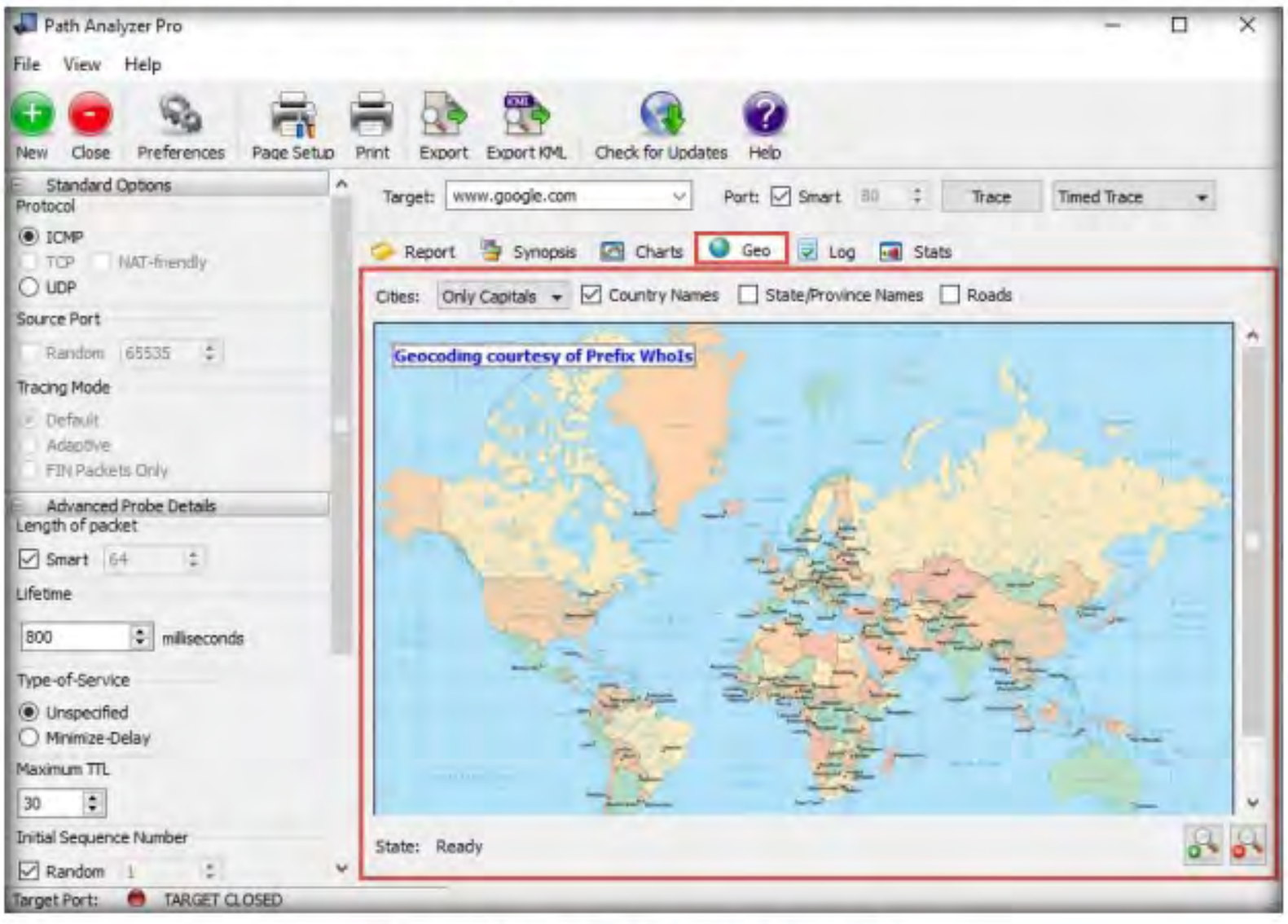


Figure 8.3.10: The Path Analyzer Pro chart window

TASK 3.5

Examine the Logs

15. Click the **Log** tab to view **Current Trace Log** and **Session Log**.

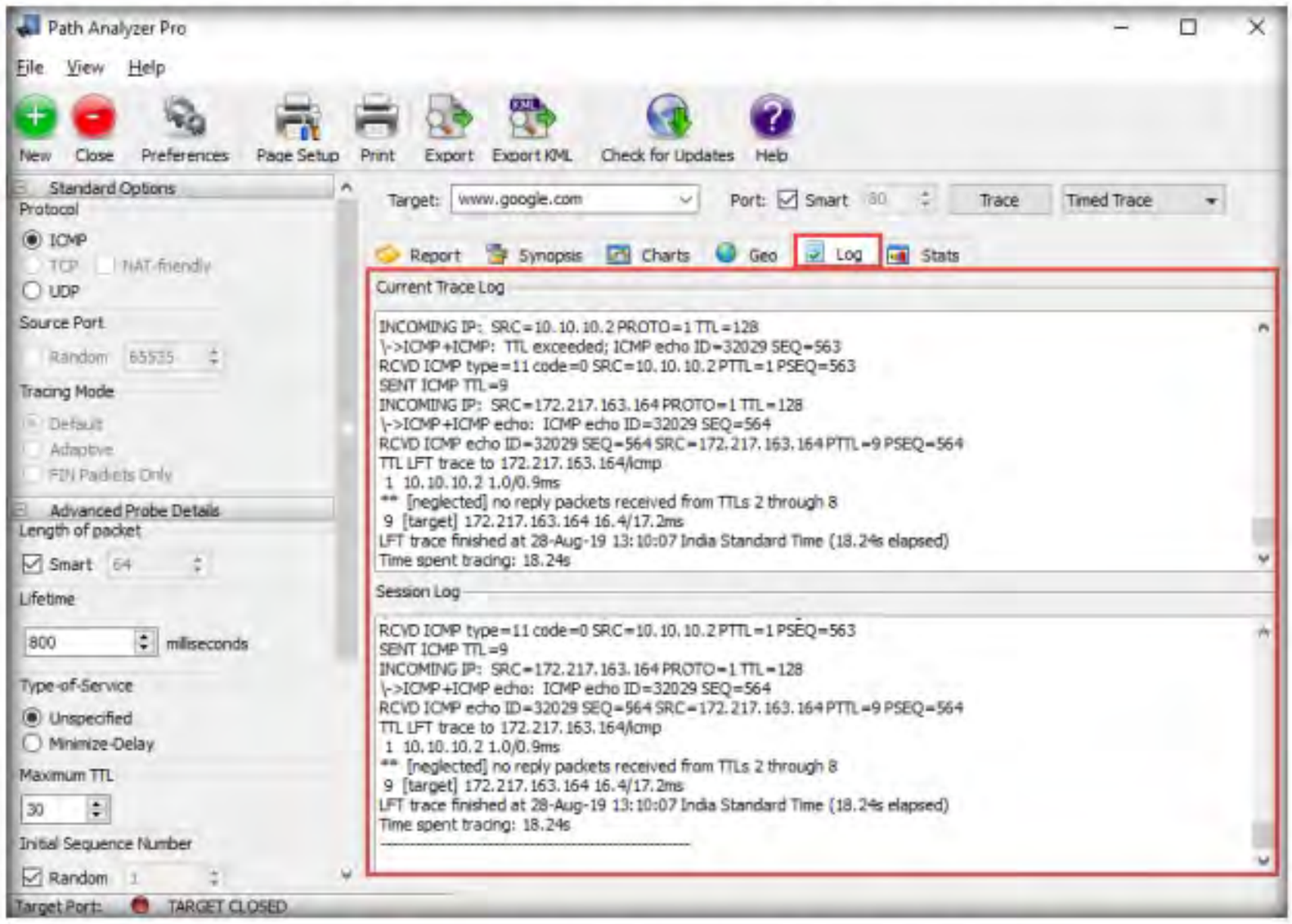


Figure 8.3.11: The Path Analyzer Pro Current Trace Log and Session Log window

TASK 3.6

Observe the Statistics

16. Click the **Stats** tab, which features the current trace's **Vital Statistics**.

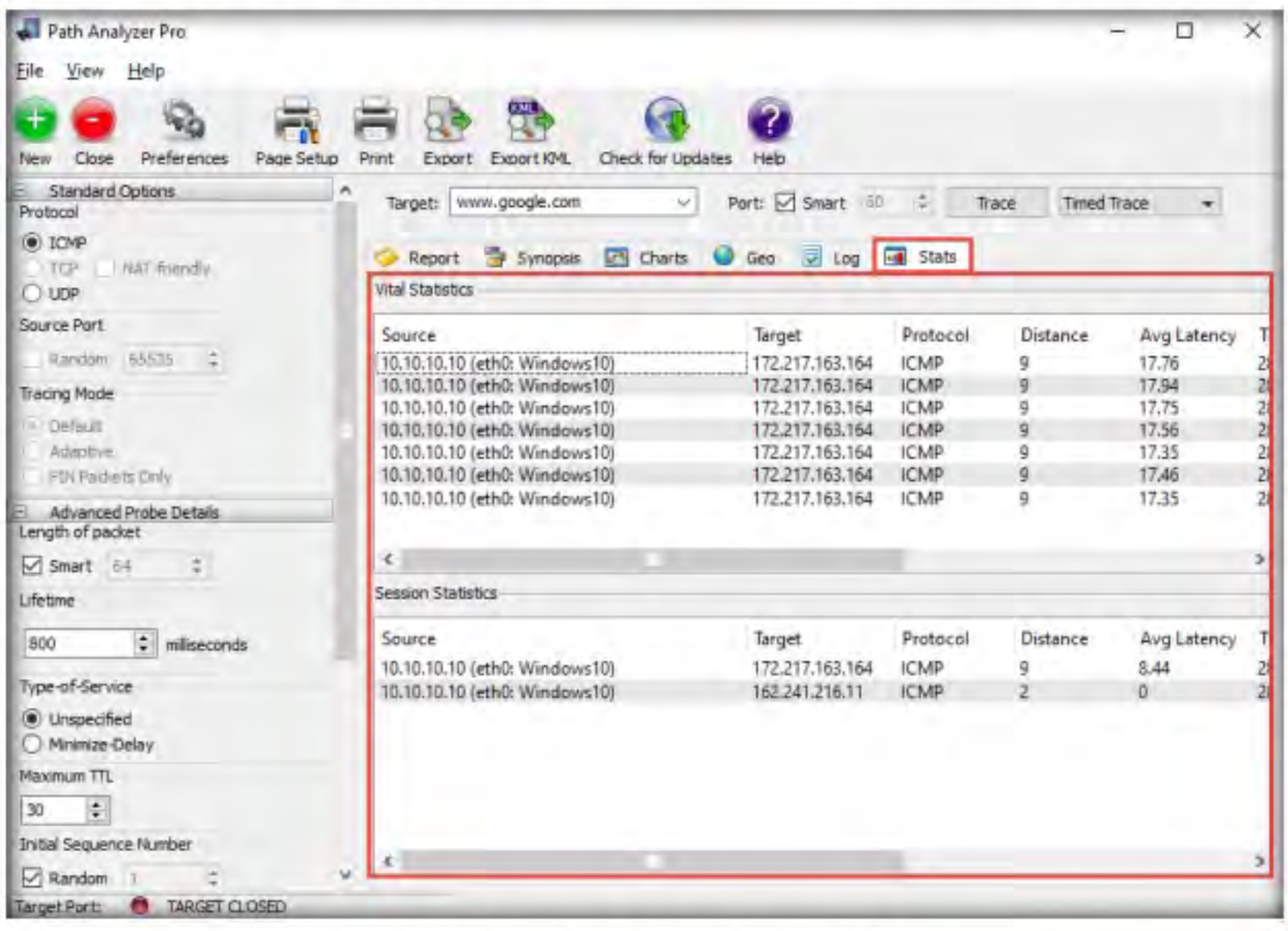


Figure 8.3.12: The Path Analyzer Pro Statistics window

TASK 3.7

Export Results

17. Click **Export** in the toolbar to export the report.

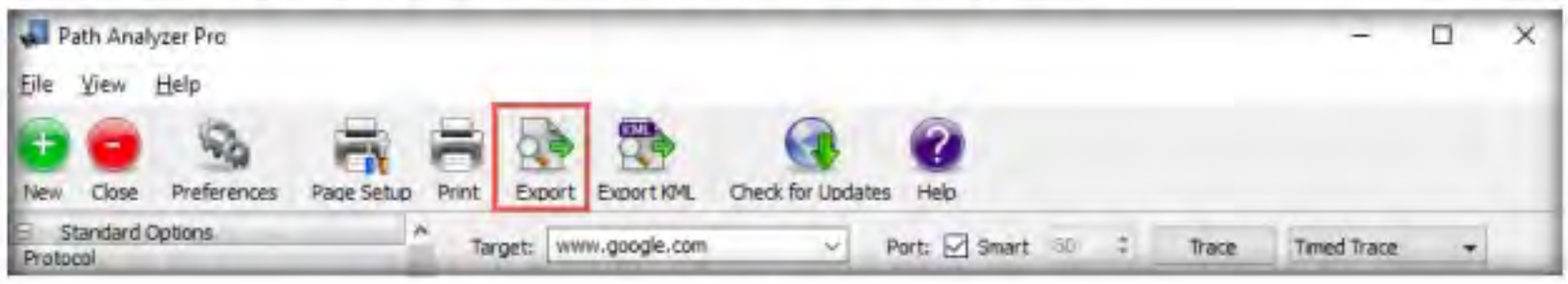


Figure 8.3.13: The Path Analyzer Pro Save Report As window

18. The **Save Statistics As** window appears. Specify your desired name for the file in **File name:** field (here, **Sample Report**) and click **Save**.

Note: By default, the report will be saved at **C:\Program Files (x86)\Path Analyzer Pro 2.7**. However, you may change it to your preferred location.

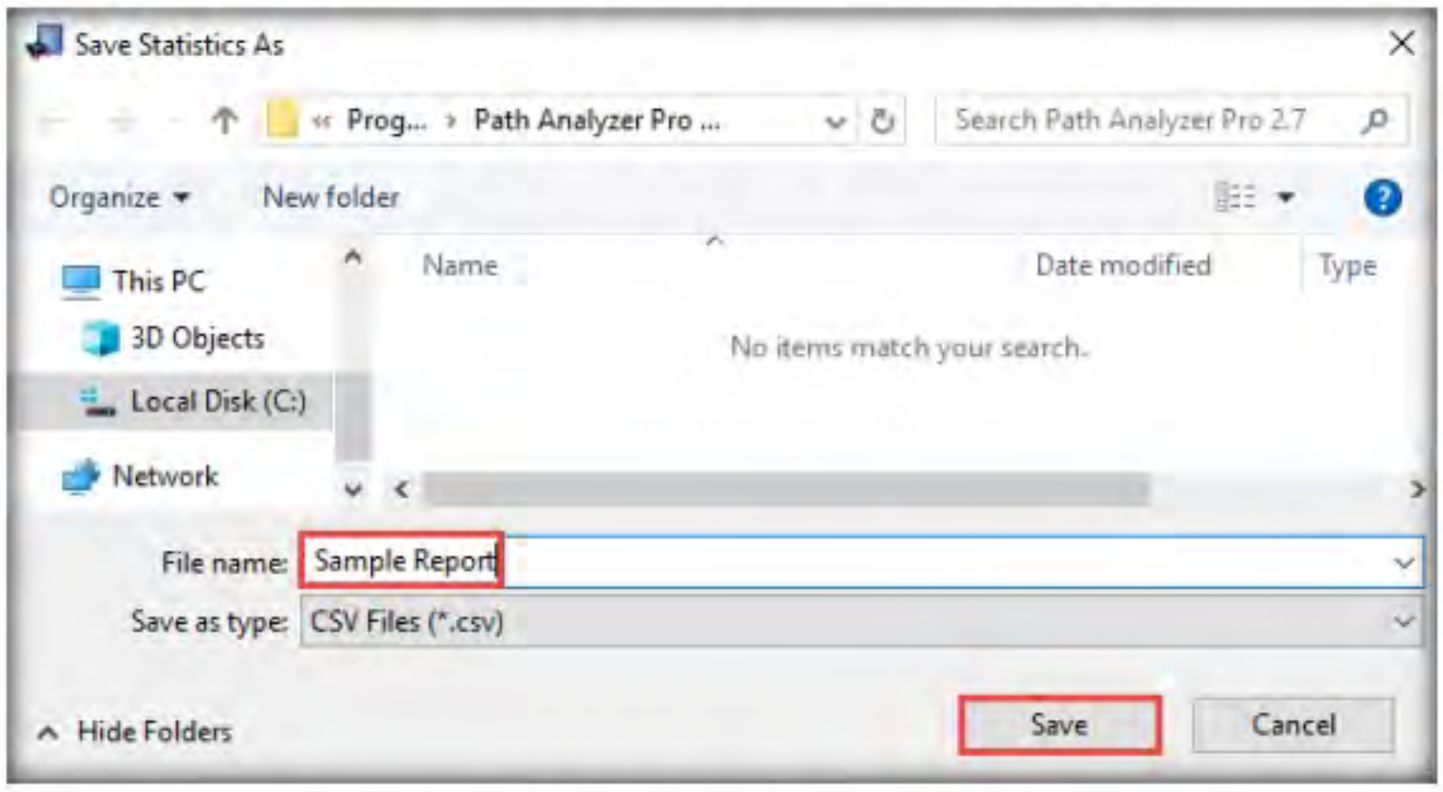


Figure 8.3.14: The Path Analyzer Pro Save Report As window

19. This concludes the demonstration of gathering information about a target organization by performing network tracerouting using Path Analyzer Pro.
20. Close all open windows and document all acquired information.
21. Turn off the **Windows 10** virtual machine.

You can also use other traceroute tools such as **VisualRoute** (http://www.visualroute.com), **Traceroute NG** (https://www.solarwinds.com), etc. to extract additional network information of the target organization.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 9

Perform Footprinting using Various Footprinting Tools

Ethical hackers and penetration testers perform footprinting with the help of various tools that make information gathering an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The information gathered in the previous steps may not be sufficient to reveal the potential vulnerabilities of the target. There could be more information available that could help in finding loopholes in the target. As an ethical hacker, you should look for as much information as possible about the target using various tools. This lab activity will demonstrate what other information you can extract from the target using various footprinting tools.

Lab Objectives

- Footprinting a target using Recon-ng
- Footprinting a target using Maltego
- Footprinting a target using OSRFramework
- Footprinting a target using FOCA
- Footprinting a target using BillCipher
- Footprinting a target using OSINT Framework

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

- FOCA located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA\bin**
- You can also download the latest version of FOCA from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 65 Minutes

Overview of Footprinting Tools

Footprinting tools are used to collect basic information about the target systems in order to exploit them. Information collected by the footprinting tools contains the target's IP location information, routing information, business information, address, phone number and social security number, details about the source of an email and a file, DNS information, domain information, etc.

Lab Tasks

TASK 1

Recon-ng is a web reconnaissance framework with independent modules and database interaction that provides an environment in which open-source web-based reconnaissance can be conducted. Here, we will use Recon-ng to perform network reconnaissance, gather personnel information, and gather target information from social networking sites.

Footprinting a Target using Recon-ng

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

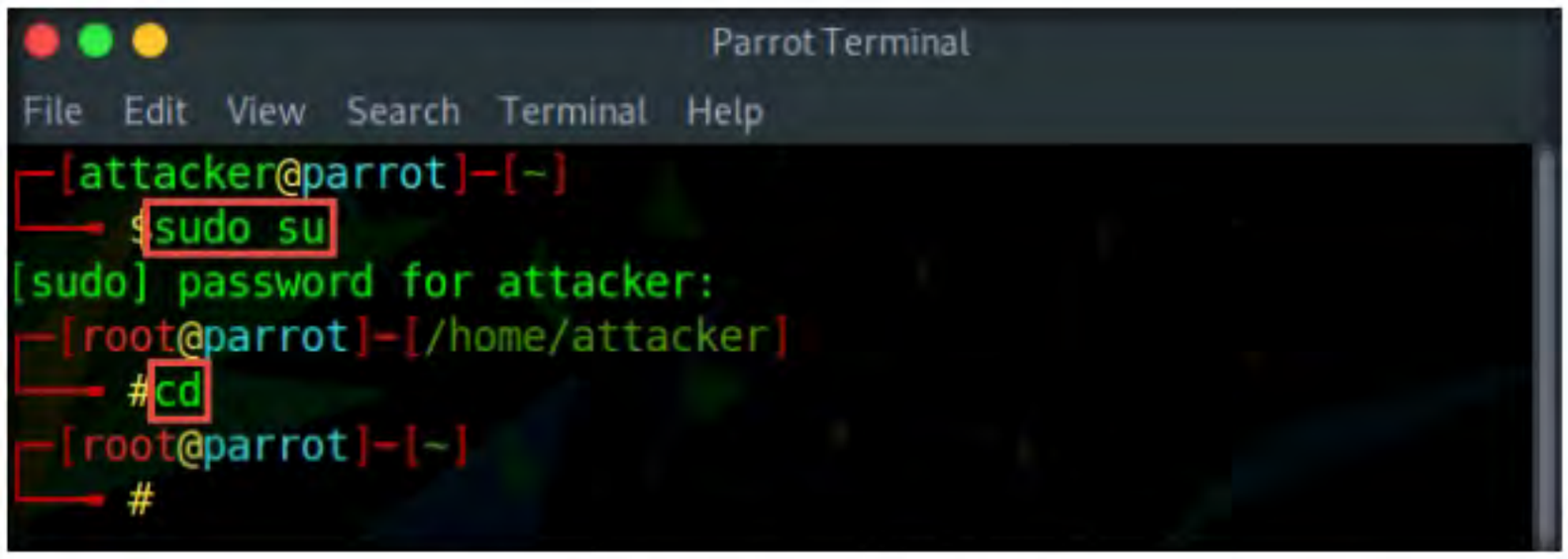


Figure 9.1.1: Running the programs as a root user

7. Type the command **recon-ng** and press **Enter** to launch the application.

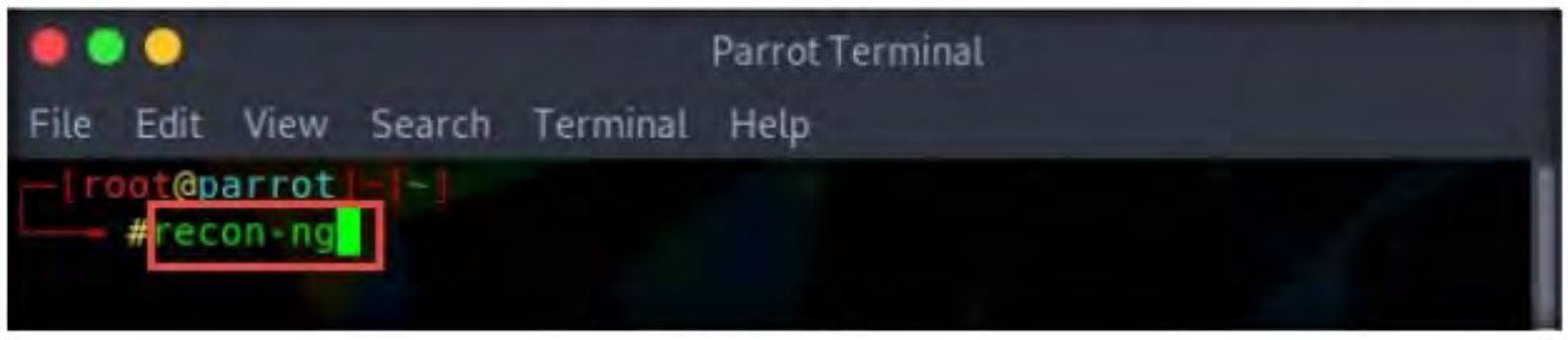


Figure 9.1.2: Launching recon-ng

8. Type **help** and press **Enter** to view all the commands that allow you to add/delete records to a database, query a database, etc.

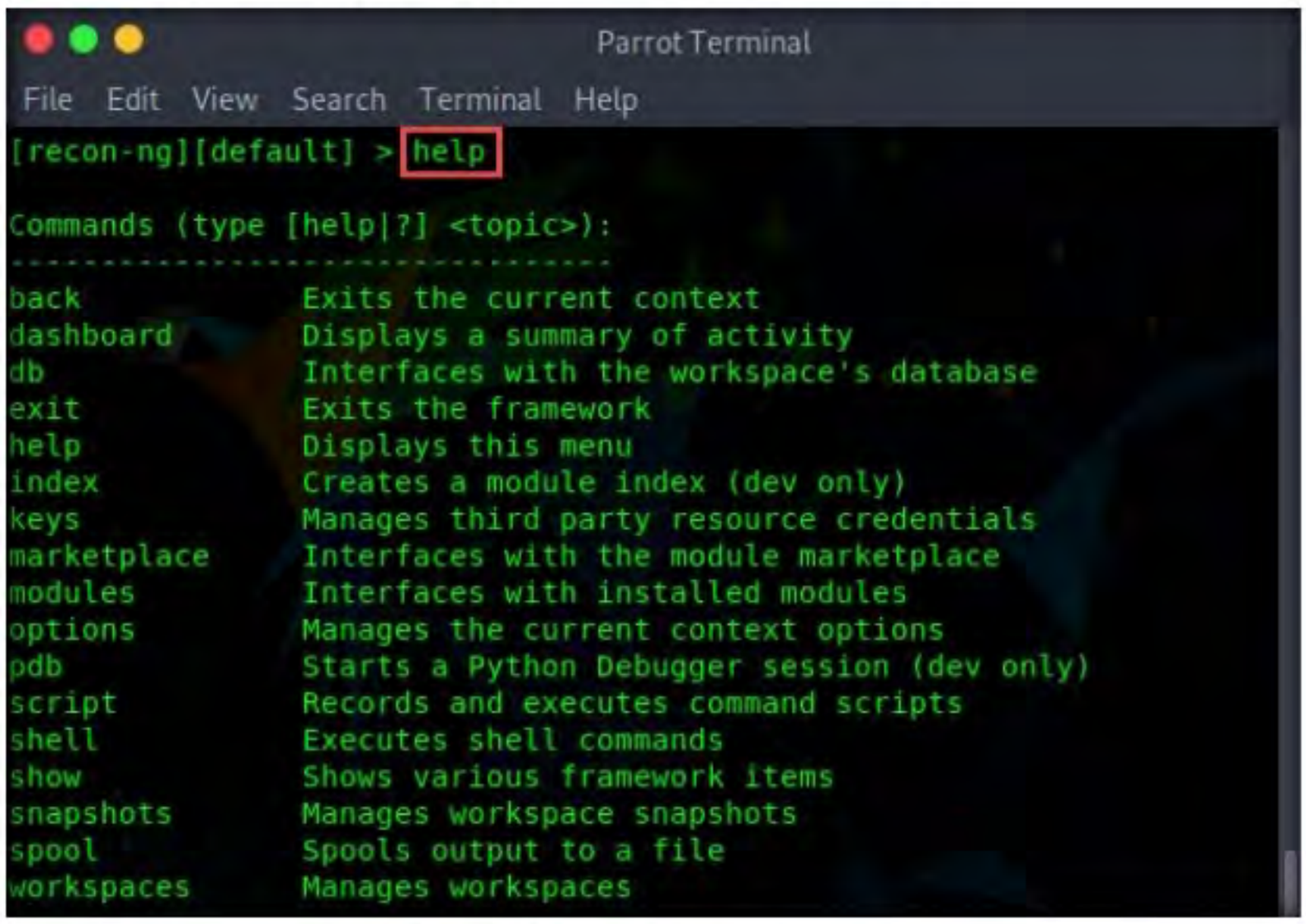


Figure 9.1.3: Viewing recon-ng Commands

9. Type **marketplace install all** and press **Enter** to install all the modules available in recon-ng.

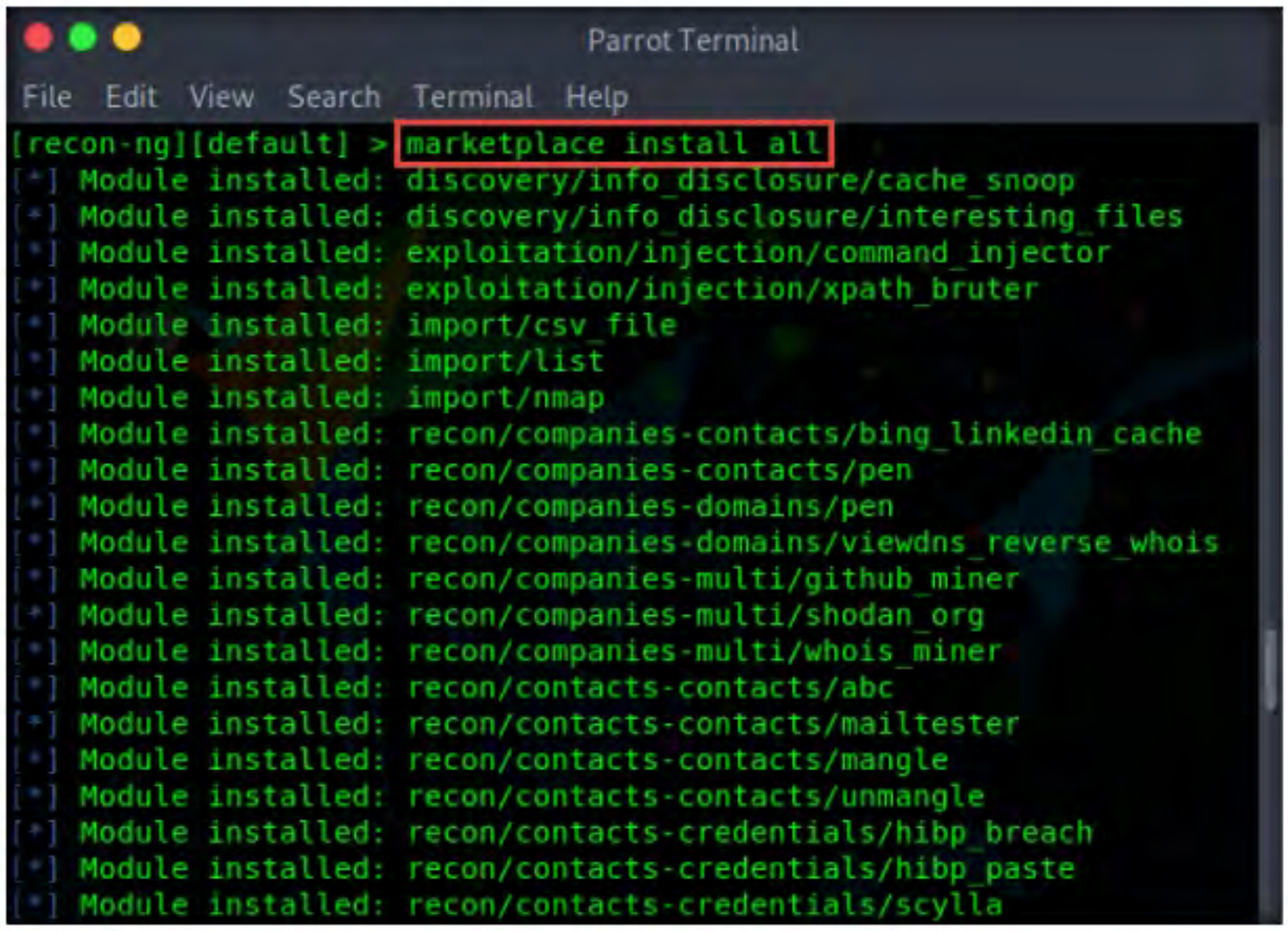


Figure 9.1.4: Installing Modules

10. Type the **modules search** command and press **Enter**. This displays all the modules available in recon-ng.

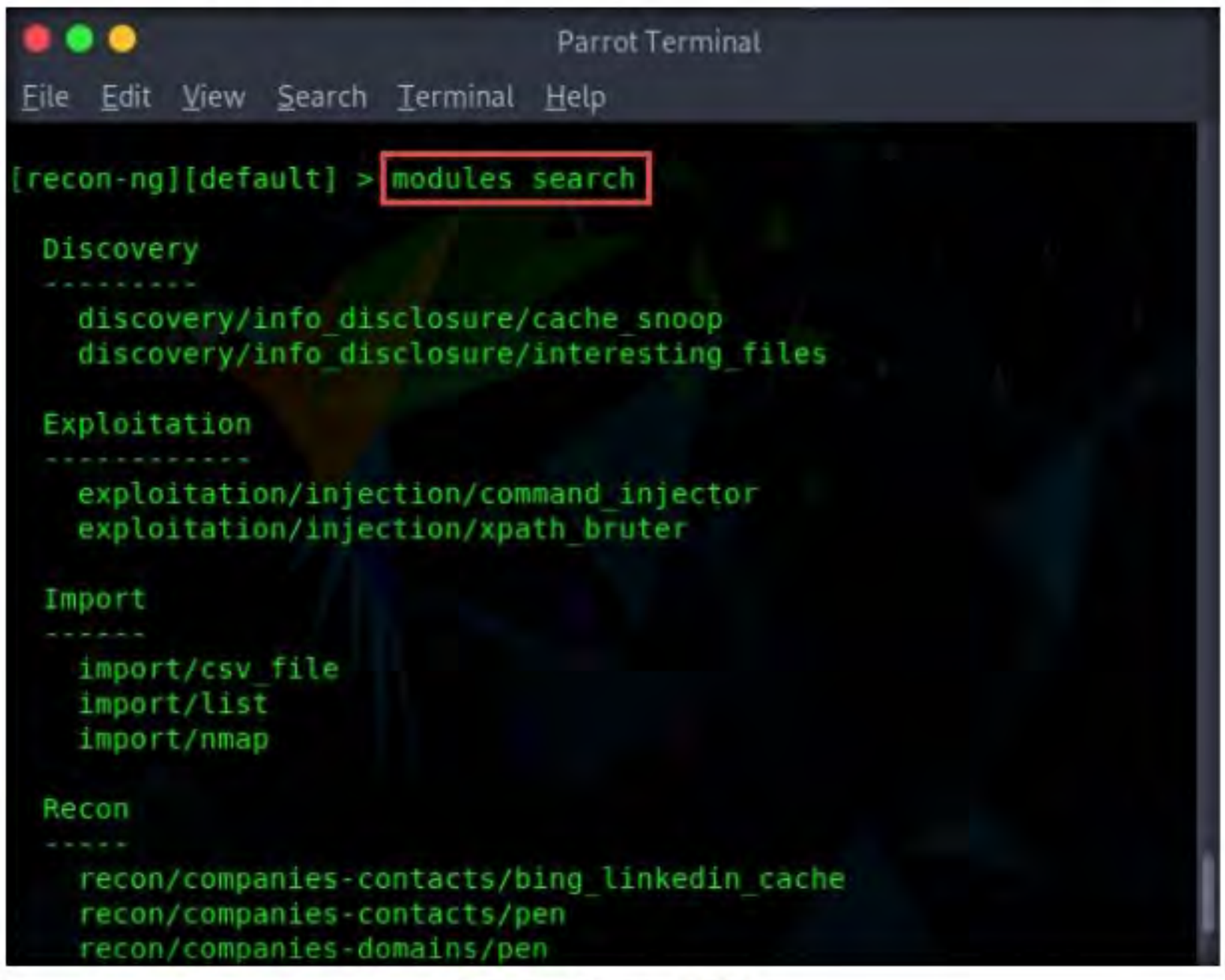


Figure 9.1.5: Viewing Modules

11. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.
12. Type the **workspaces** command and press **Enter**. This displays the commands related to the workspaces.

TASK 1.1

Create a Workspace

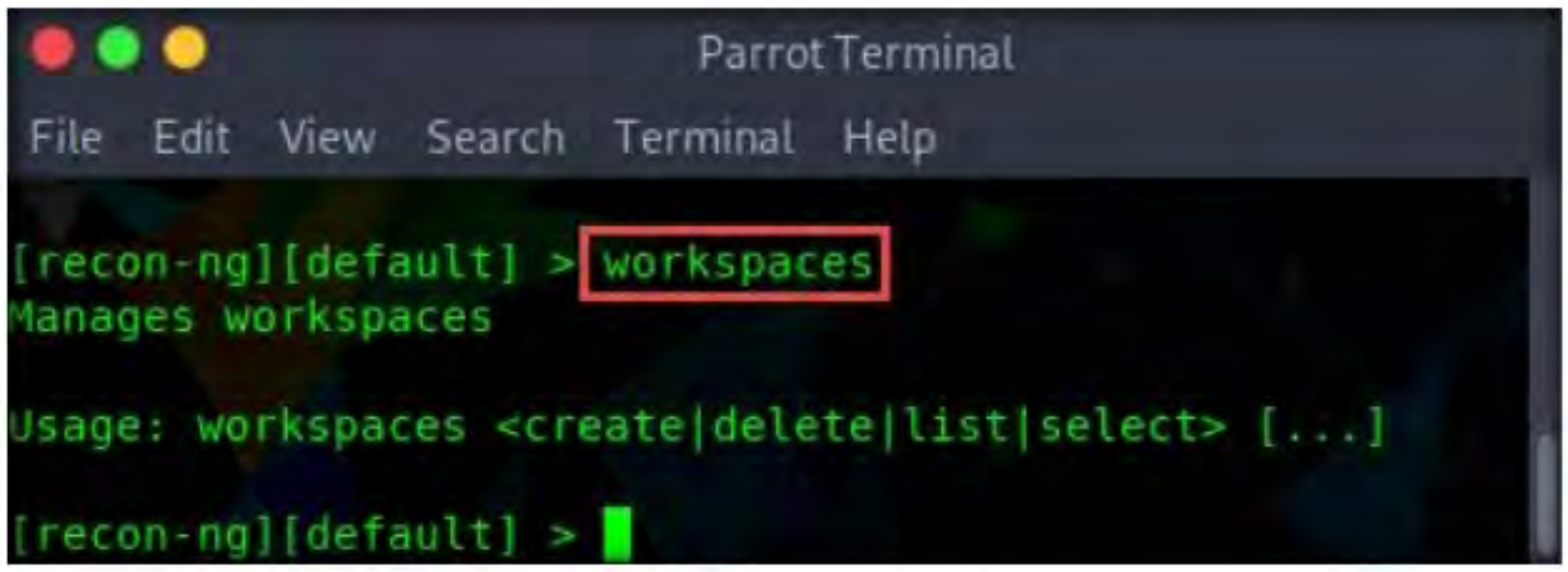


Figure 9.1.6: Viewing Workspaces Related Commands

13. Create a workspace in which to perform network reconnaissance. In this lab, we shall be creating a workspace named **CEH**.
14. To create the workspace, type the command **workspaces create CEH** and press **Enter**. This creates a workspace named CEH.

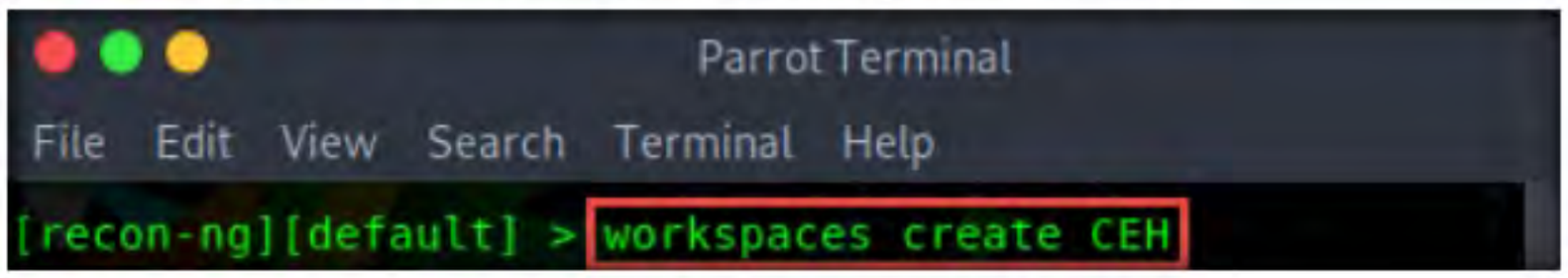


Figure 9.1.7: Creating a Workspace

Note: You can alternatively issue the command **workspaces select CEH** to create a workspace named CEH. Ignore the errors while running the commands

15. Enter **workspaces list**. This displays a list of workspaces (along with the workspace added in the previous step) that are present within the workspaces databases.

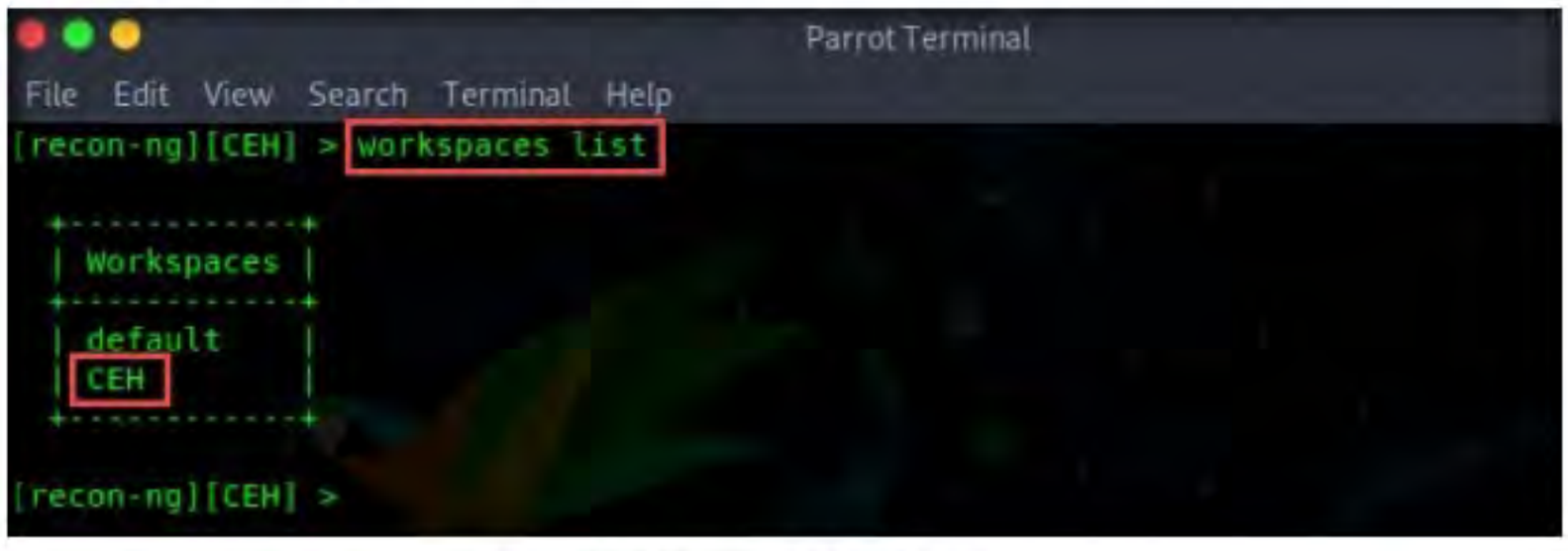


Figure 9.1.8: Viewing the Added Workspaces

TASK 1.2

Add a Domain

16. Add a domain in which you want to perform network reconnaissance
17. Type the command **db insert domains** and press **Enter**.
18. In the **domain (TEXT)** option, type **certifiedhacker.com** and press **Enter**. In the **notes (TEXT)** option, press **Enter**. This adds certifiedhacker.com to the present workspace.
19. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

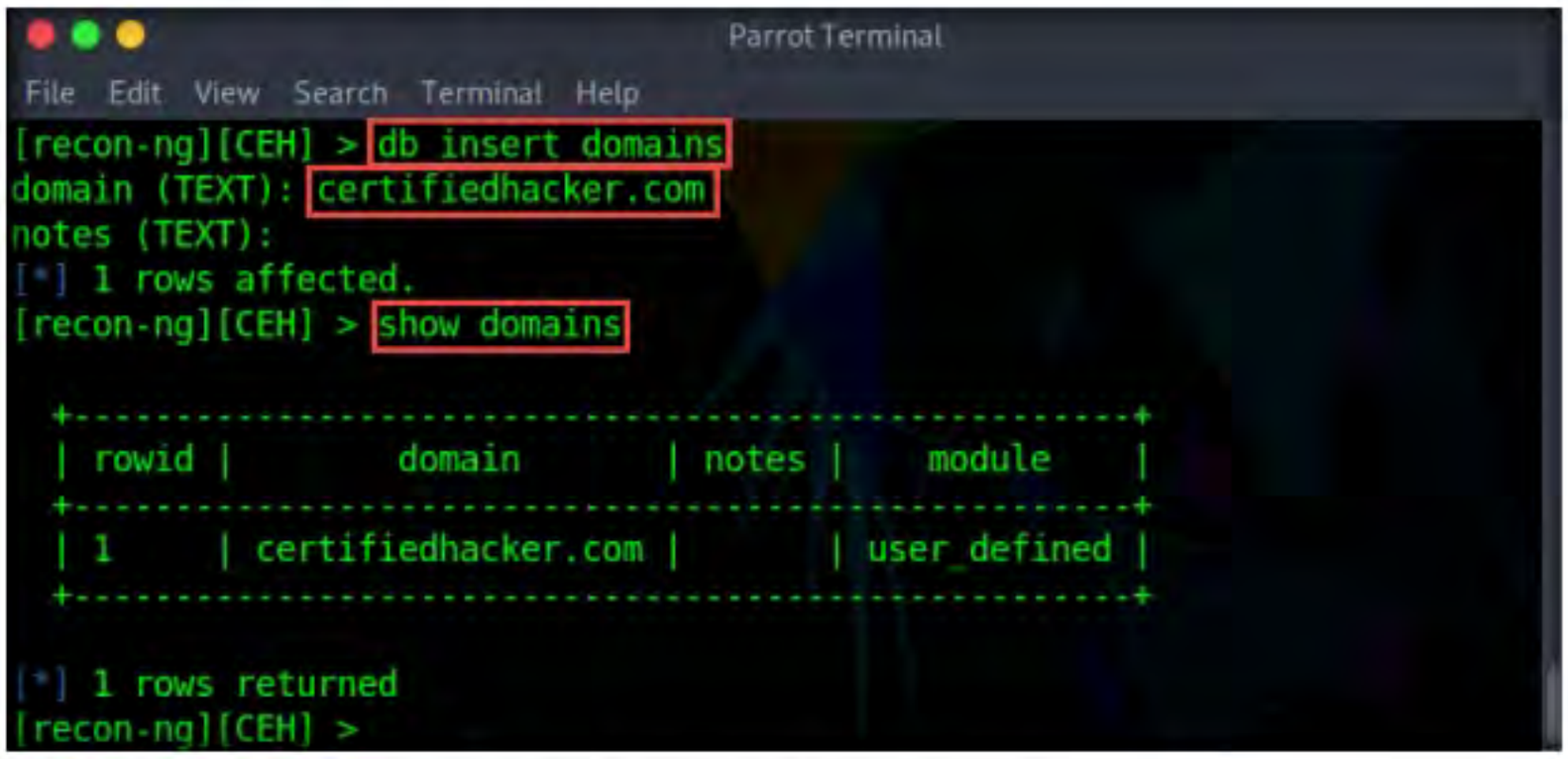


Figure 9.1.9: Viewing the Added Domain

TASK 1.3

Resolve Hosts Using brute_hosts Module

20. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as brute_hosts, Netcraft, and Bing.
21. Type **modules load brute** and press **Enter** to view all the modules related to brute forcing. In this lab, we will be using the **recon/domains-hosts/brute_hosts** module to harvest hosts.

Figure 9.1.10: Searching for brute Module

22. To load the **recon/domains-hosts/brute_hosts** module, type the **modules load recon/domains-hosts/brute_hosts** command and press **Enter**.

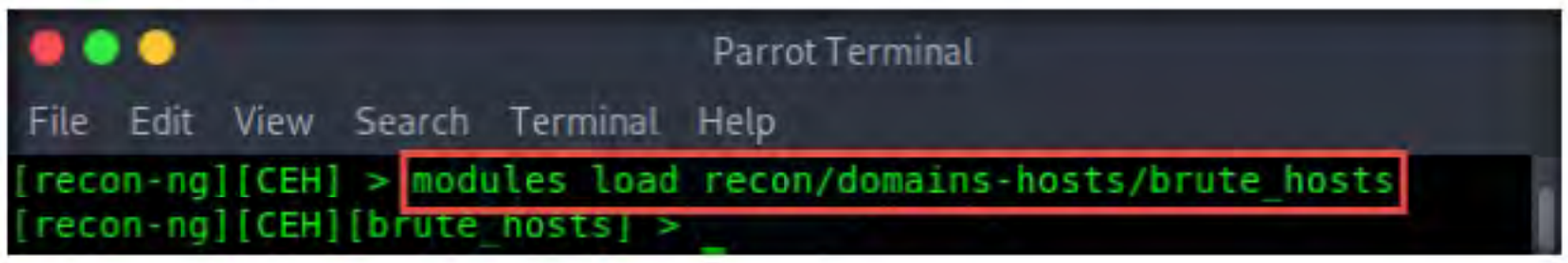


Figure 9.1.11: Loading brute Module

23. Type **run** and press **Enter**. This begins to harvest the hosts, as shown in the screenshot.

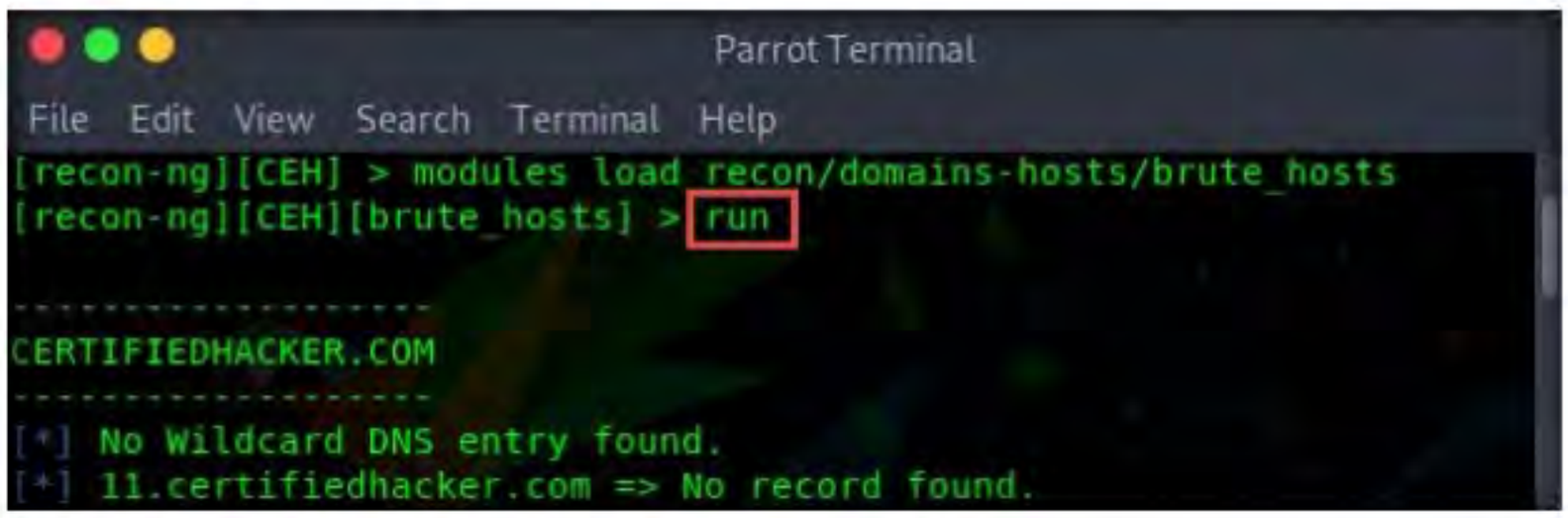


Figure 9.1.12: Running brute Module

24. Observe that hosts have been added by running the **recon/domains-hosts/brute_hosts** module.

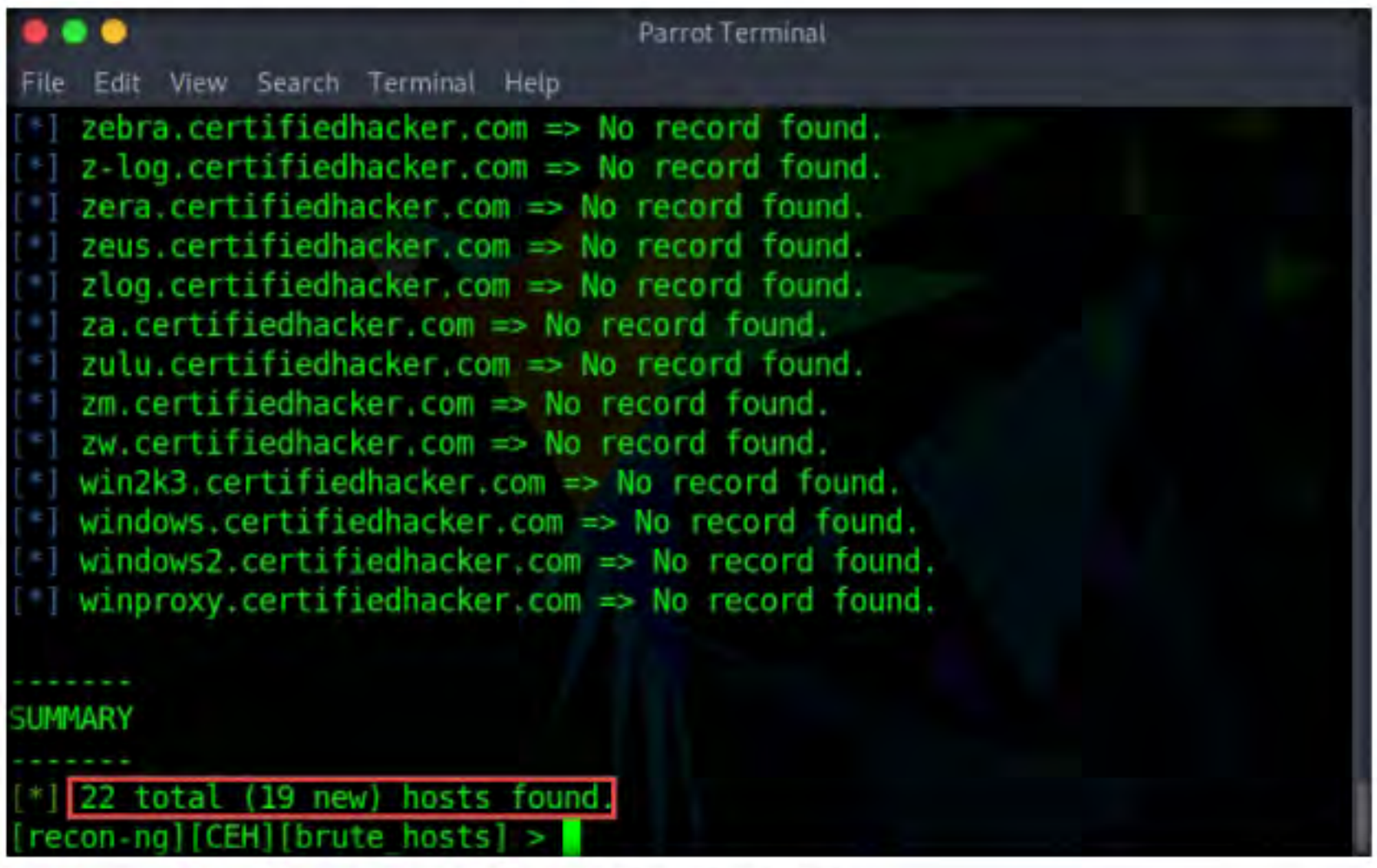


Figure 9.1.13: Newly Added Hosts

25. You have now harvested the hosts related to certifiedhacker.com using the brute_hosts module. You can use other modules such as Netcraft and Bing to harvest more hosts.

Note: Use the **back** command to go back to the CEH attributes terminal

To resolve hosts using the Bing module, use the following commands:

- **back**
- **modules load recon/domains-hosts/bing_domain_web**
- **run**

26. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

TASK 1.4

Perform Reverse Lookup Using reverse_resolve module

27. Type **modules load reverse_resolve** command and press **Enter** to view all the modules associated with the reverse_resolve keyword. In this lab, we will be using the **recon/hosts-hosts/reverse_resolve** module.
28. Type the **modules load recon/hosts-hosts/reverse_resolve** command and press **Enter** to load the module.

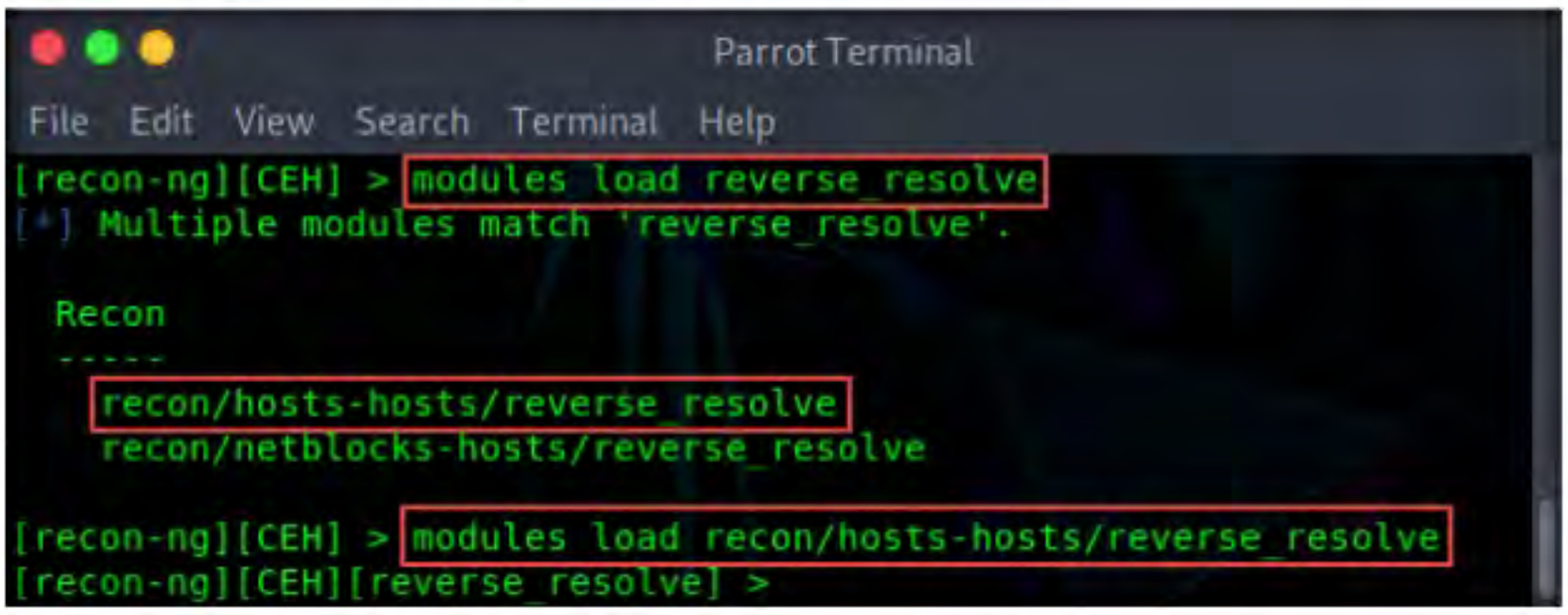


Figure 9.1.14: Search for reverse_resolve Module

29. Issue the **run** command to begin the reverse lookup

Note: Ignore the if any Syntax Error occurs.

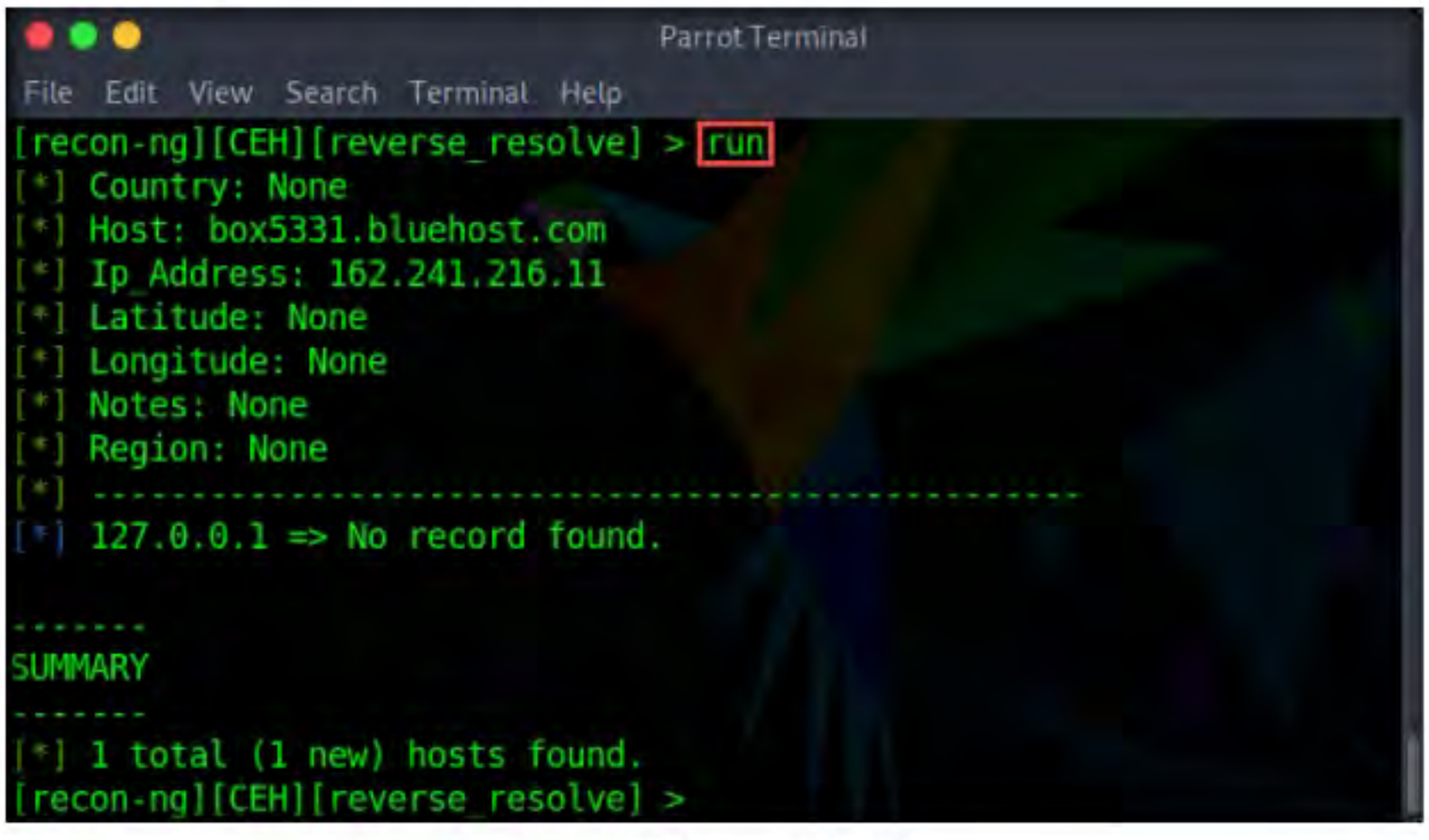


Figure 9.1.15: Running the Module

30. Once done with the reverse lookup process, type the **show hosts** command and press **Enter**. This displays all the hosts that are harvested so far, as shown in the screenshot.

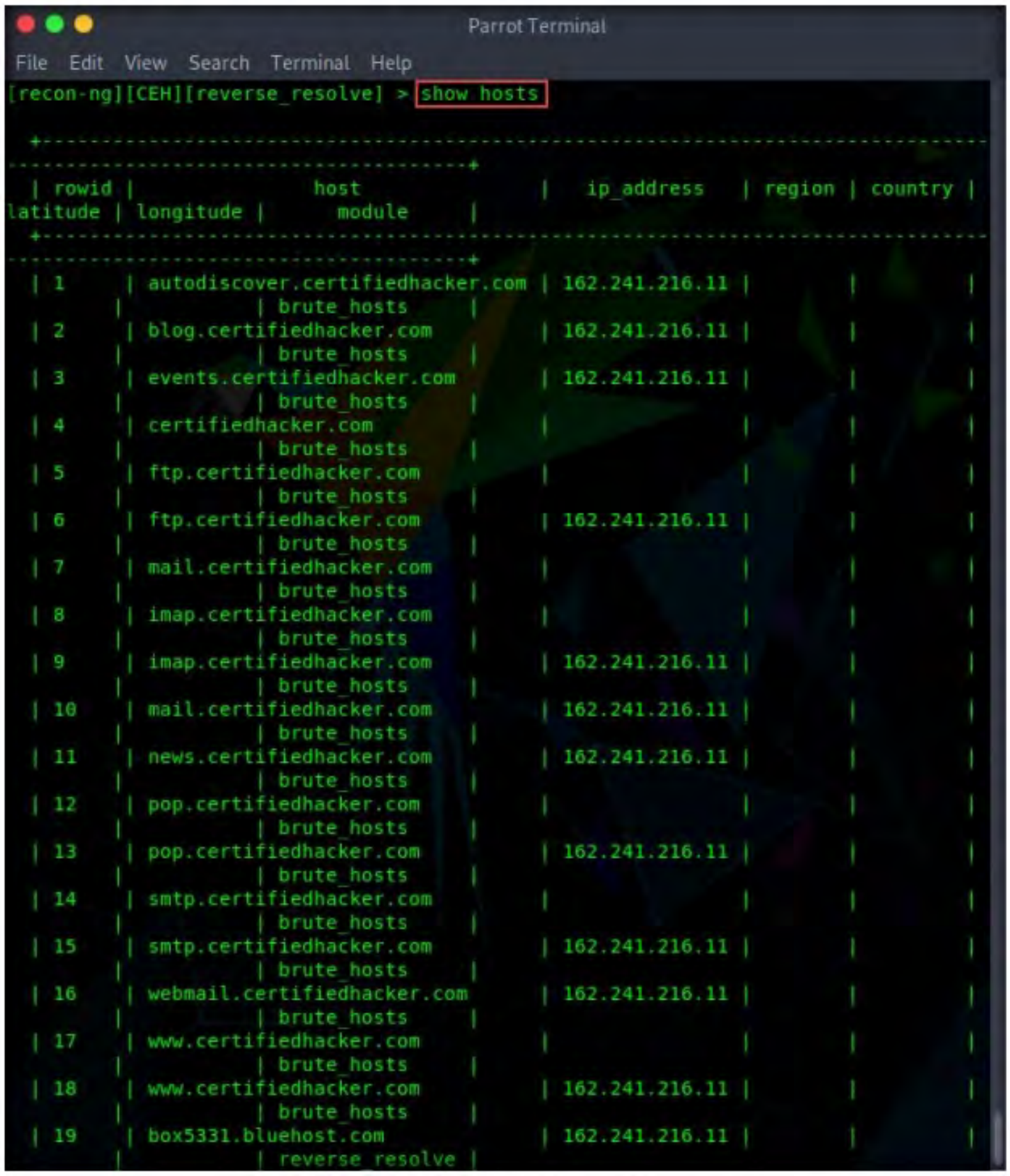


Figure 9.1.16: Viewing the Harvested Hosts

31. Now, type the **back** command and press **Enter** to go back to the **CEH** attributes terminal

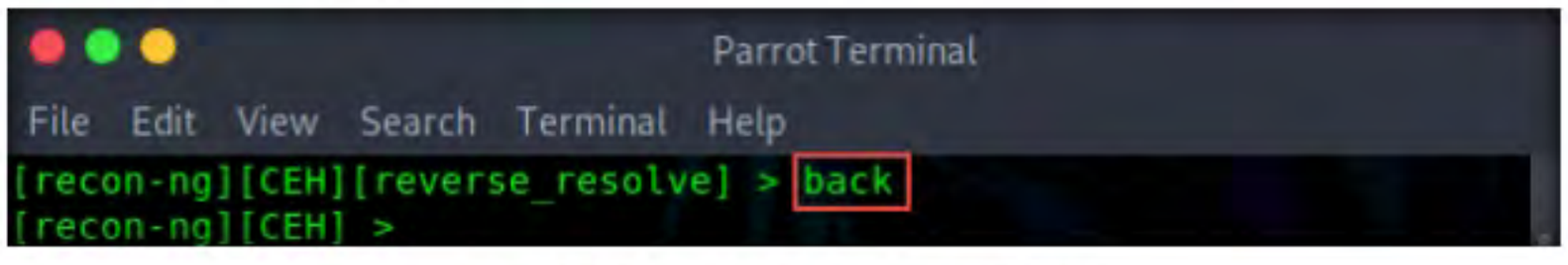


Figure 9.1.17: Going back to the Attributes Section

TASK 1.5

Generate a Report

32. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.
33. Type the **modules load reporting** command and press **Enter** to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is **reporting/html**.

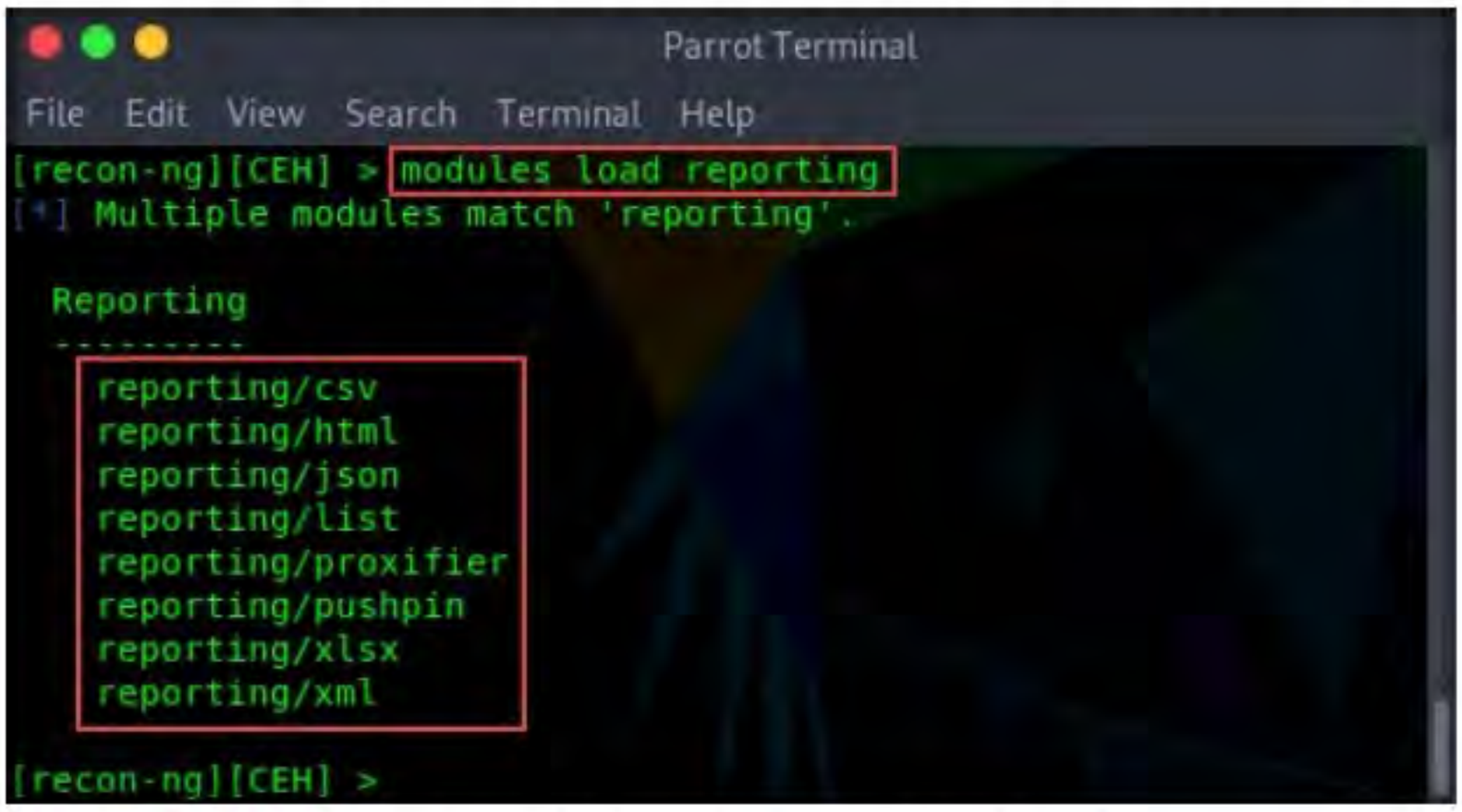


Figure 9.1.18: Searching for reporting Module

34. Type the **modules load reporting/html** command and press **Enter**.
35. Observe that you need to assign values for **CREATOR** and **CUSTOMER** options while the **FILENAME** value is already set, and you may change the value if required.
36. Type:
    a. **options set FILENAME /root/Desktop/results.html** and press **Enter**. By issuing this command, you are setting the report name as **results.html** and the path to store the file as **Desktop**.
    b. **options set CREATOR [your name]** (here, **Jason**) and press **Enter**.
    c. **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain) and press **Enter**.

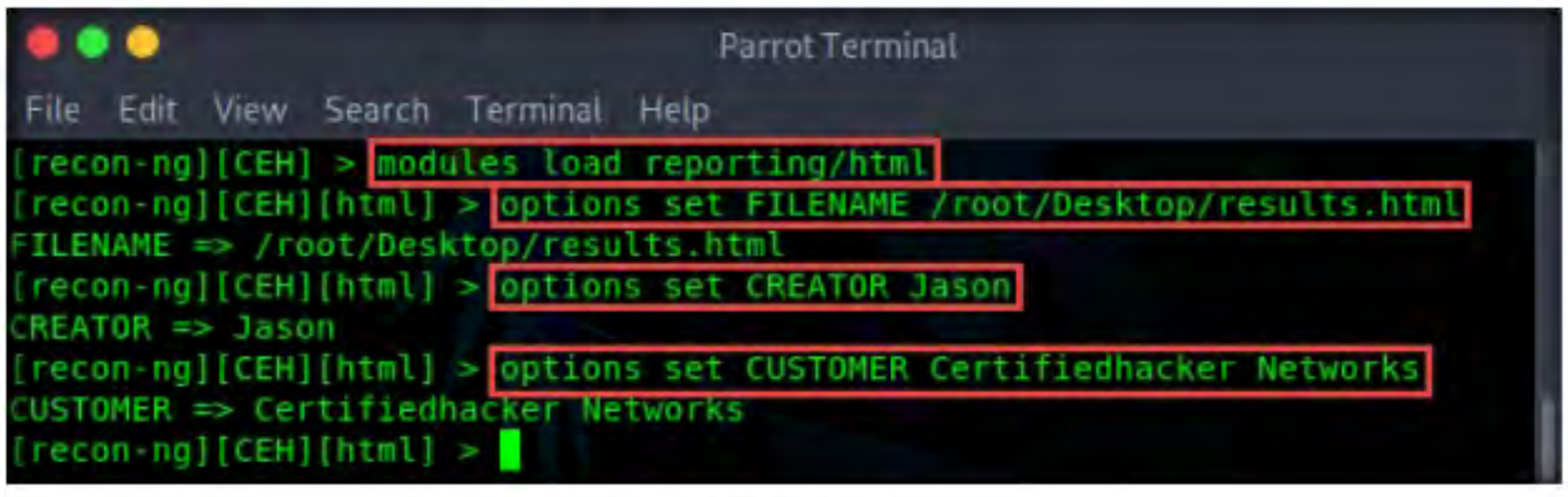


Figure 9.1.19: Saving a Report

37. Type the **run** command and press **Enter** to create a report for all the hosts that have been harvested.

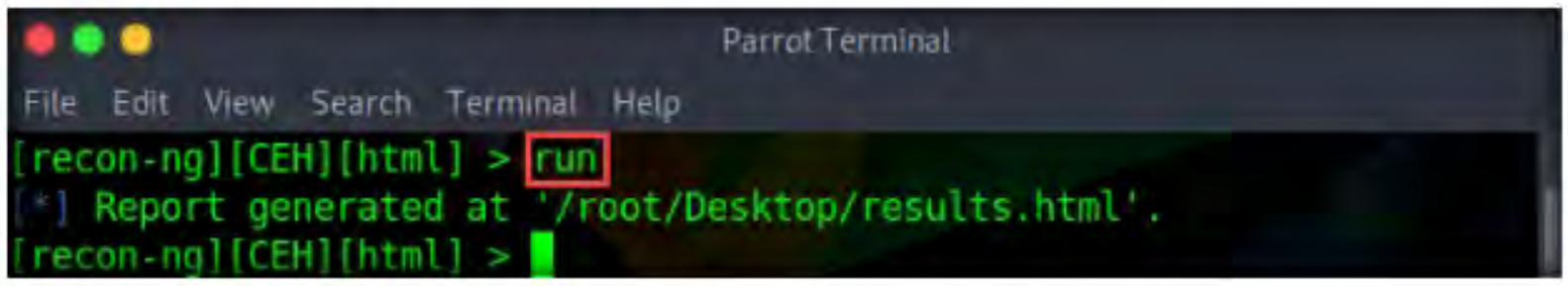


Figure 9.1.20: Running the Module

38. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

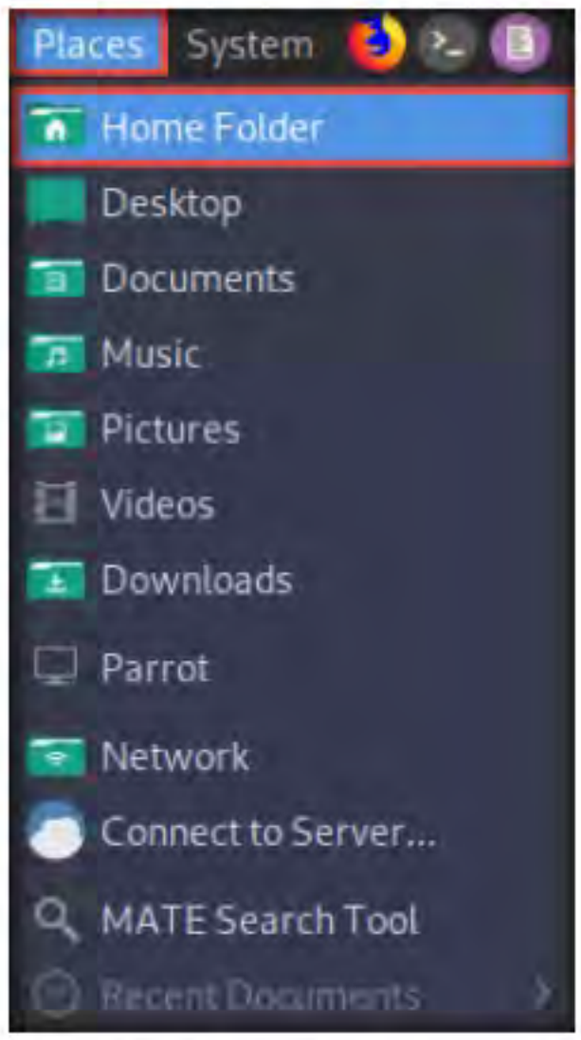


Figure 9.1.21: Navigate to the Home Folder

39. The **attacker** window appears, click **File System** from the left-pane and navigate to the location **root/Desktop**.

40. The generated report is saved to **/root/Desktop/**. Navigate to the location, right-click on the **results.html** file, click on **Open With**, and select the **Firefox** browser from the available options.

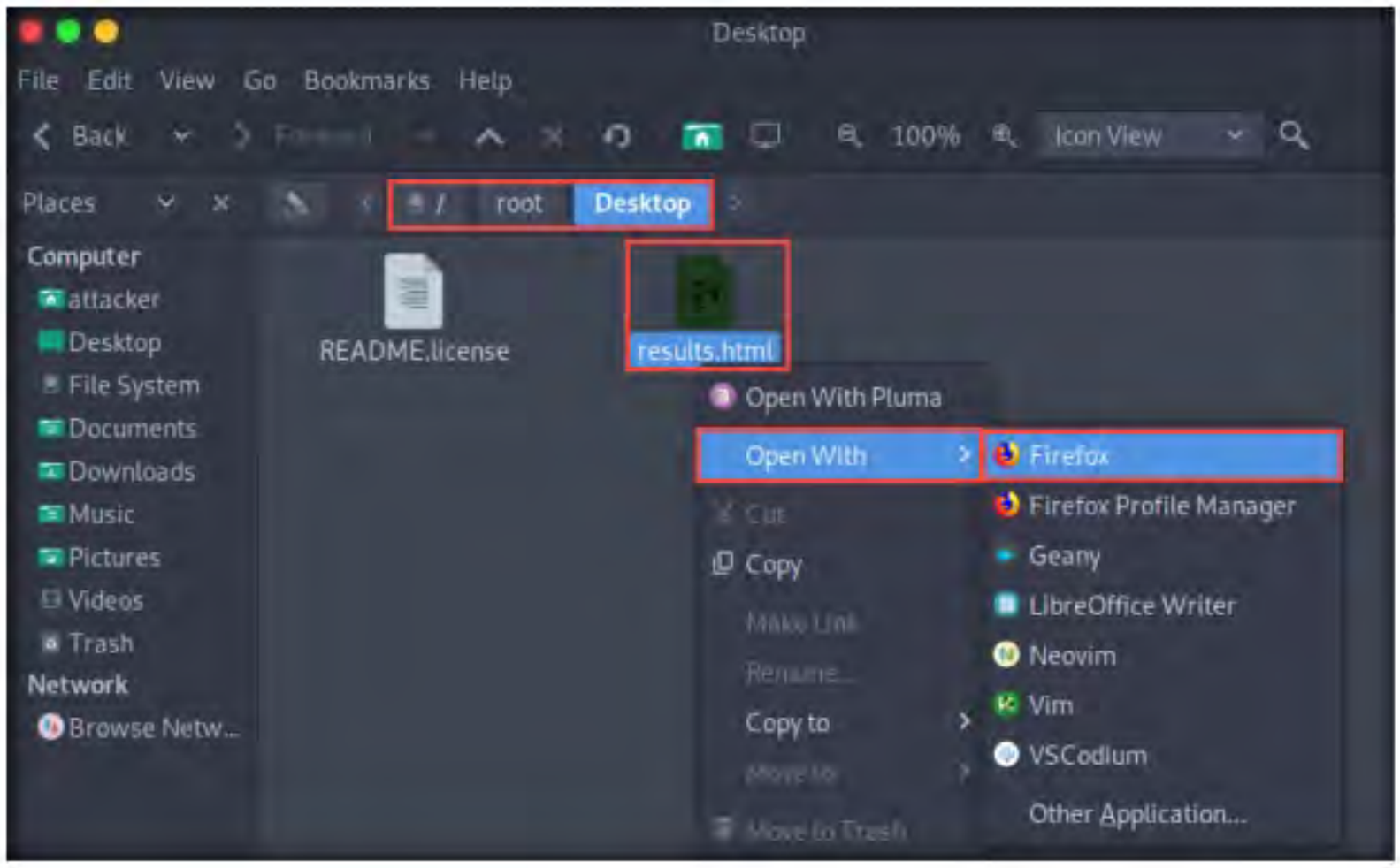


Figure 9.1.22: Viewing the Report

41. The generated report appears in the **Firefox** browser, displaying the summary of the harvested hosts.

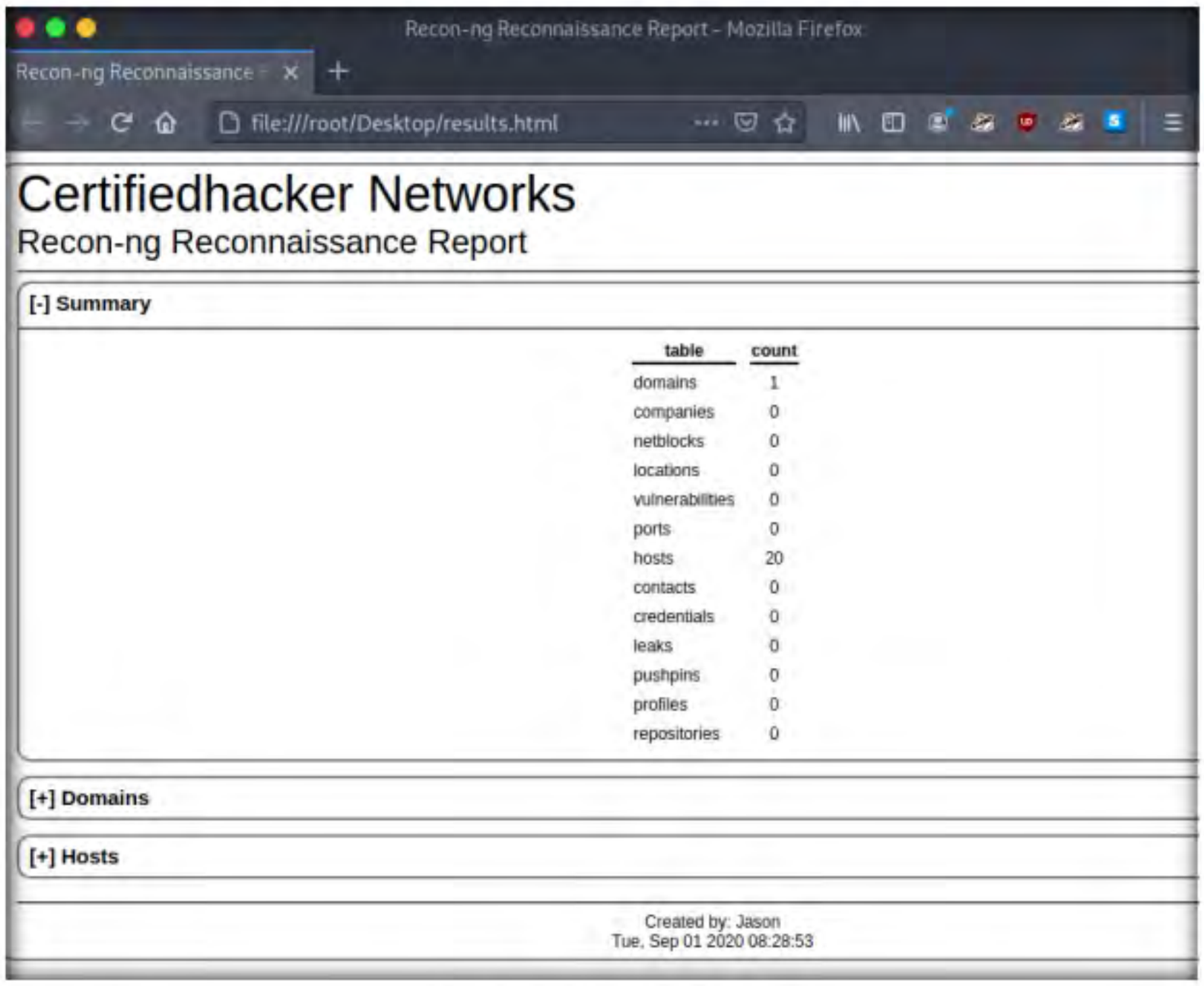


Figure 9.1.23: Viewing the Report

42. You can expand the **Hosts** node to view all the harvested hosts, as shown in the screenshot.

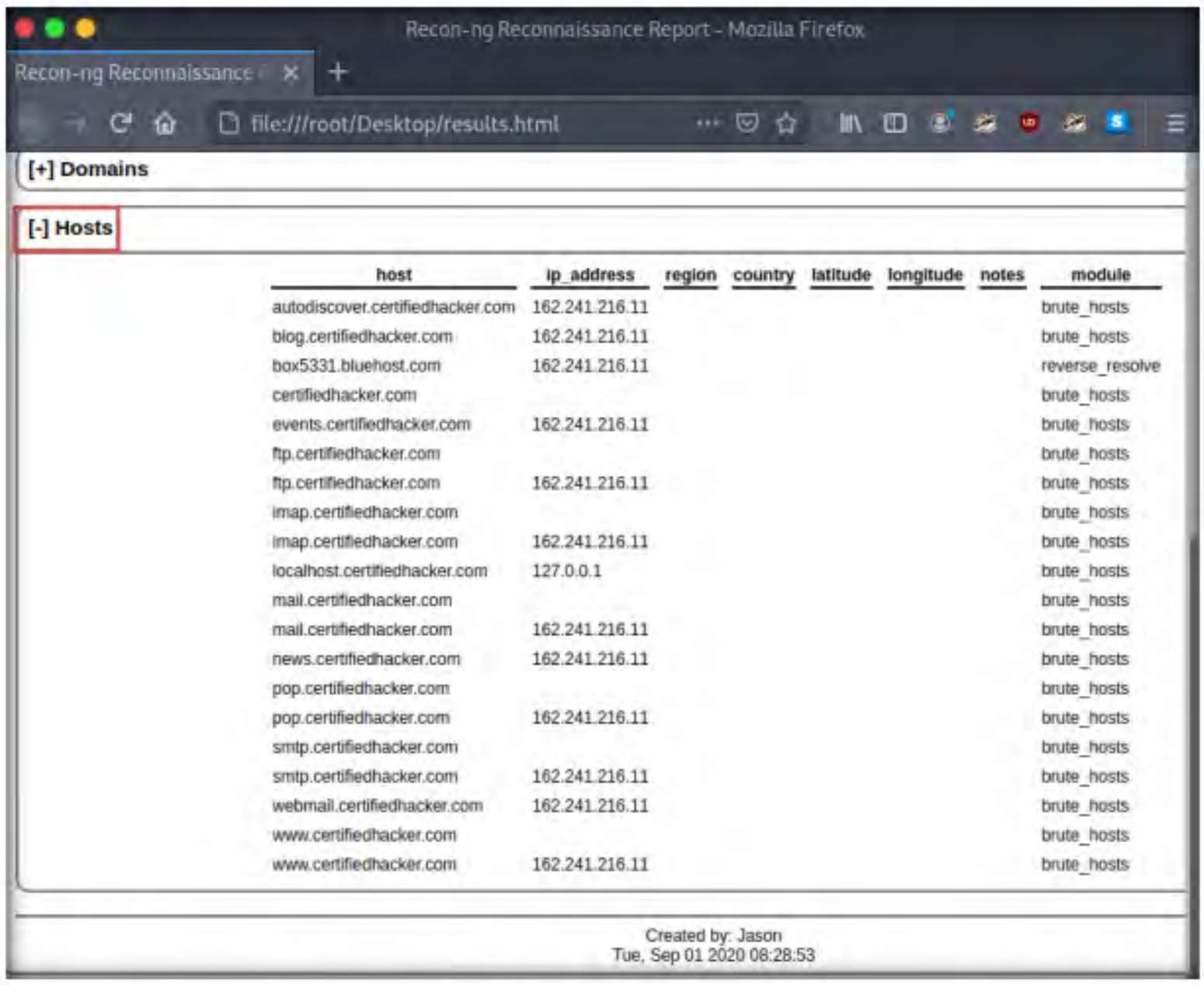


Figure 9.1.24: Expanding Hosts tab

43. Close the **Firefox** window.
44. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain.
45. Now, we will use Recon-ng to gather personnel information.

TASK 1.6

Create a Workspace

46. Open a new **Parrot Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
47. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Type **cd** and press **Enter** to jump to the root directory.
48. Now, type **recon-ng**, and press **Enter**.

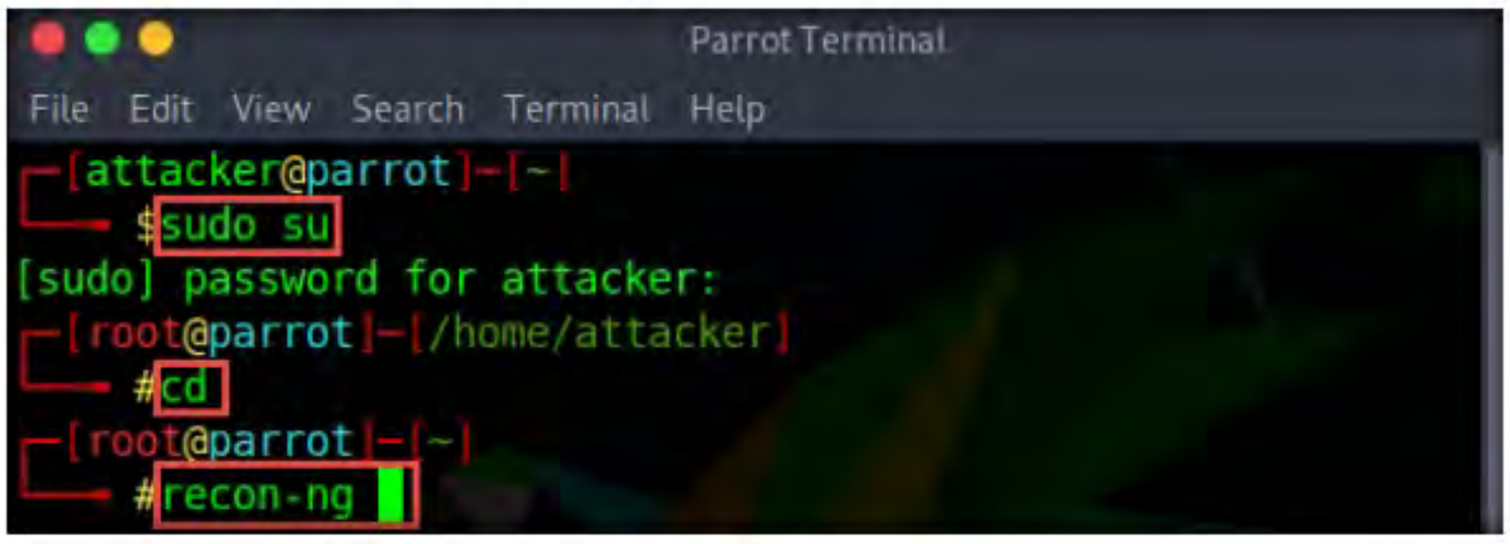


Figure 9.1.25: Launch recon-ng

49. Add a workspace by issuing the command **workspaces create reconnaissance** and press **Enter**. This creates a workspace named reconnaissance.

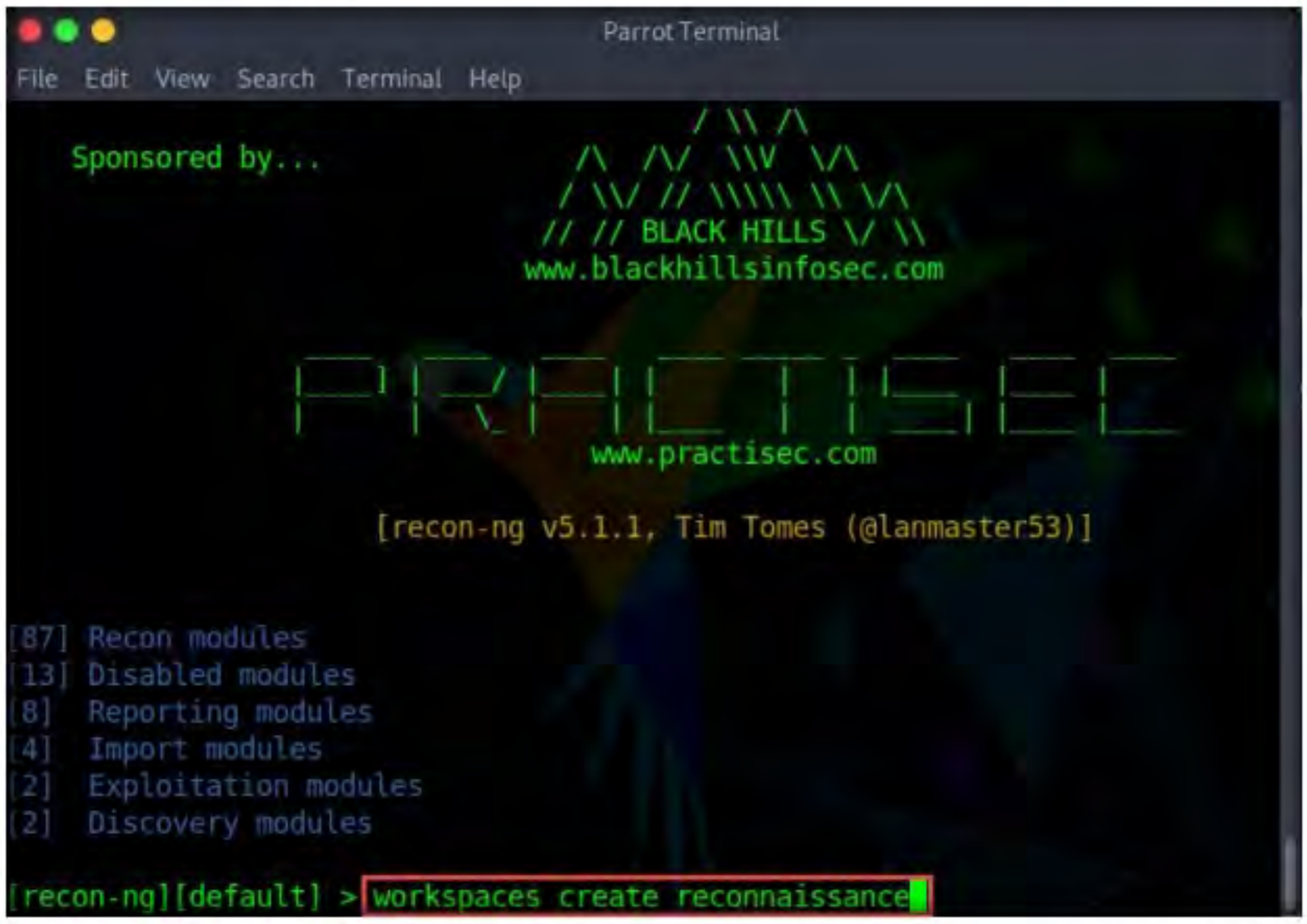


Figure 9.1.26: Launching recon-ng

TASK 1.7

Gather Contacts Associated with a Domain

50. Set a domain and perform footprinting on it to extract contacts available in the domain.
51. Type **modules load recon/domains-contacts/whois_pocs** and press **Enter**. This module uses the ARIN Whois RWS to harvest POC data from Whois queries for the given domain.
52. Type the **info** command and press **Enter** to view the options required to run this module.
53. Type **options set SOURCE facebook.com** and press **Enter** to add facebook.com as a target domain.

Note: Here, we are using facebook.com as a target domain to gather contact details.

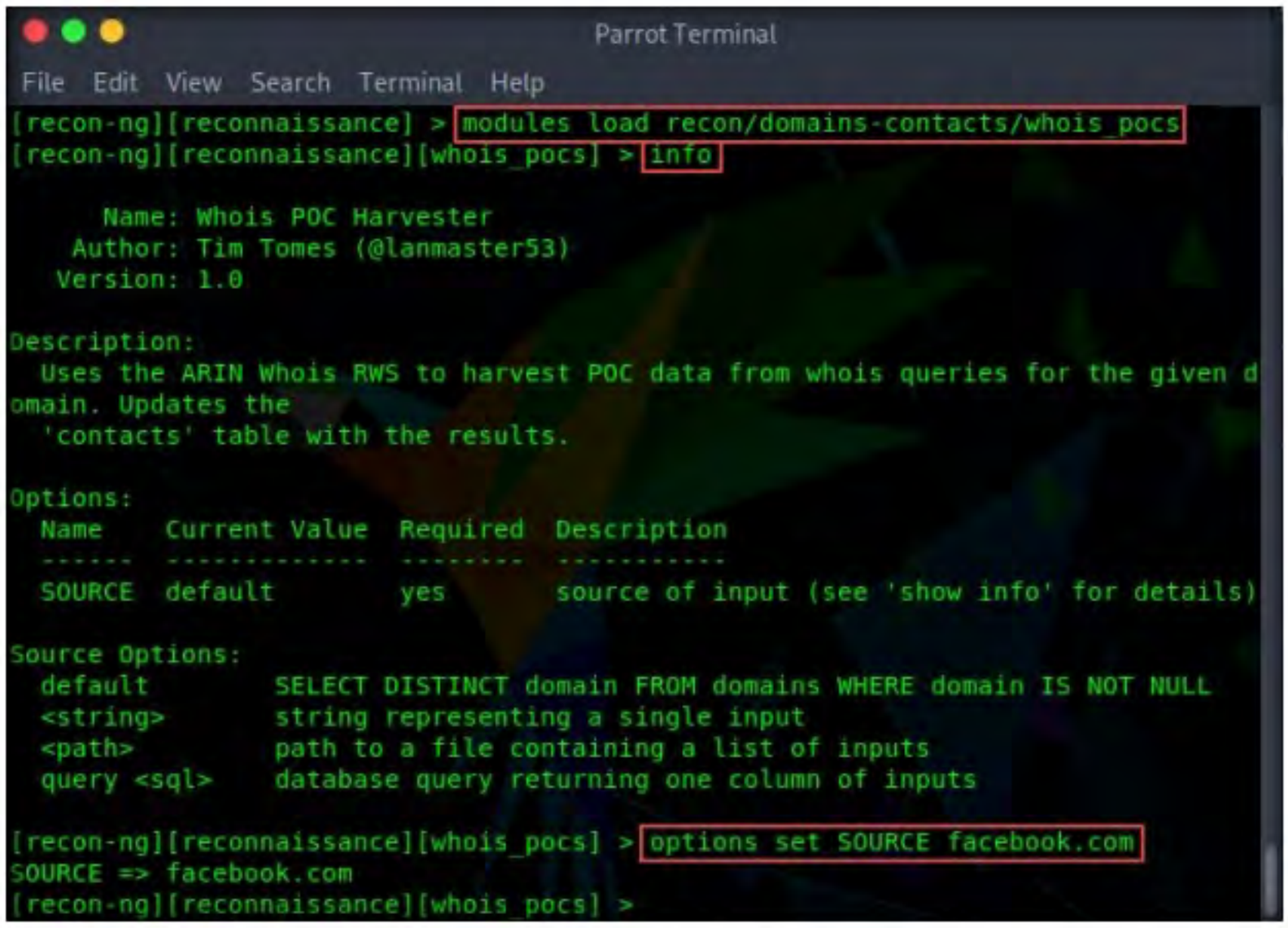


Figure 9.1.27: Harvesting Contacts from Domain

54. Type the **run** command and press **Enter**. The **recon/domains-contacts/whois_pocs** module extracts the contacts associated with the domain and displays them, as shown in the screenshot.

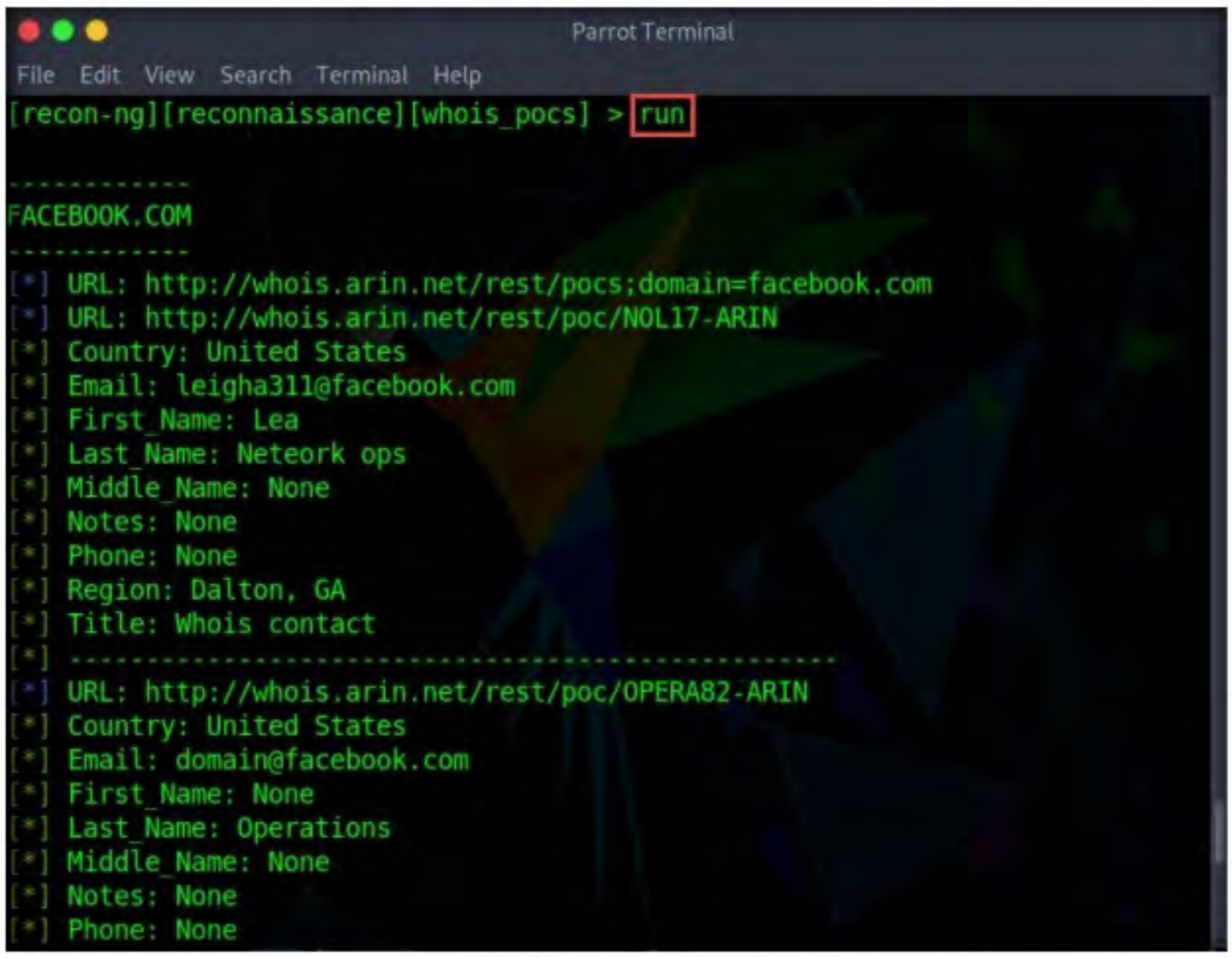


Figure 9.1.28: Running Module

55. Type **back** and press **Enter** to go back to the workspaces (**reconnaissance**) terminal

Figure 9.1.29: Going back to workspaces terminal

TASK 1.8

Check for User Existence

56. Until now, we have obtained contacts related to the domains. Note down these contacts' names
57. Now, we will validate the existence of names (usernames) on specific websites.
58. The **recon/profiles-profiles/namechk** module validates the username existence of a specified contact. The contact we will use in this lab is **Mark Zuckerberg**.
59. Type the **modules load recon/profiles-profiles/namechk** command and press **Enter** to load this module
60. Type **options set SOURCE MarkZuckerberg** and press **Enter**. This command sets MarkZuckerberg as the source for which you want to find the user existence on specific websites.
61. Type **run** and press **Enter**. This begins the search for the keyword MarkZuckerberg on various websites.
62. Recon-ng begins to search the Internet for the presence of the username on websites and, if found, it returns the result stating "**User Exists!**".

Note: Here, no results are obtained.

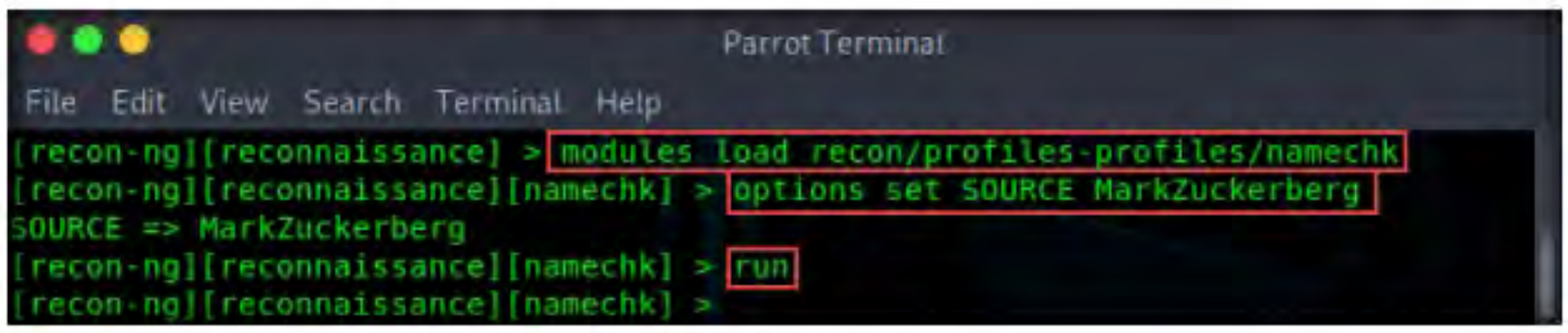


Figure 9.1.30: Running a Module

TASK 1.9

Check for Profile Existence

63. Type the **back** command and press **Enter** to go back to the workspaces (reconnaissance) terminal.
64. To find the existence of user-profiles on various websites, you need to load the **recon/profiles-profiles/profiler** module.
65. Type the **modules load recon/profiles-profiles/profiler** command and press **Enter**

66. Type the **options set SOURCE MarkZuckerberg** command and press **Enter**.

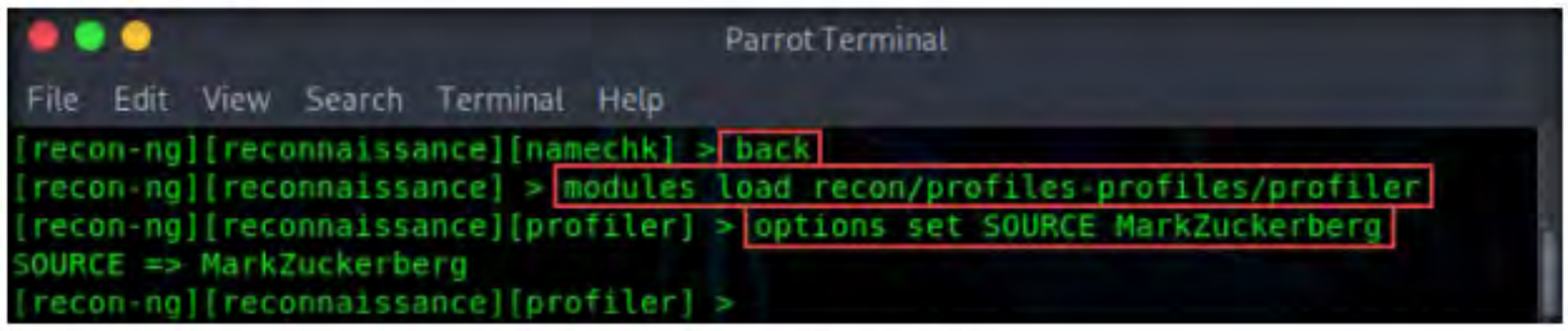


Figure 9.1.31: Configuring Module

67. Type the **run** command and press **Enter**. The recon/profiles-profiles/profiler module searches for this username and returns the URL of the profile (found with the matching username):

Note: Ignore the Errors.

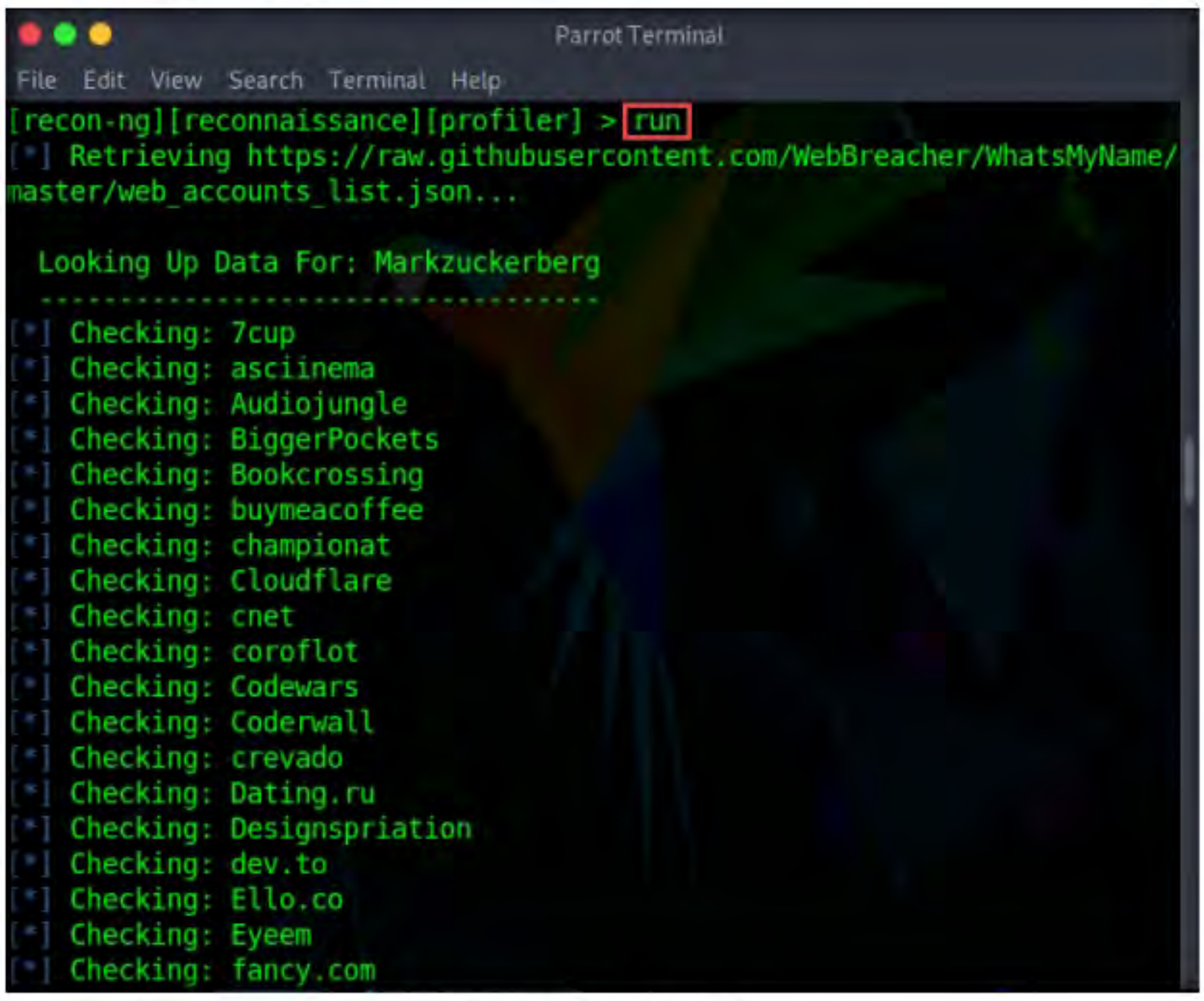


Figure 9.1.32: Running Module

TASK 1.10

Generate a Report

68. Type **back** and press **Enter** to go back to the workspaces terminal.
69. Now that we have verified the user existence and obtained the profile URL, we will prepare a report containing the result.
70. Type the **modules load reporting/html** command and press **Enter**. Assign values for **FILENAME**, **CREATOR**, and **CUSTOMER**.

Note: In this lab, we are saving the report in HTML format; therefore, **reporting/html** module is used.

71. Type:

- **options set FILENAME /root/Desktop/Reconnaissance.html** and press **Enter**. By issuing this command, you are setting the report name as **Reconnaissance**.

Note: Here, the Reconnaissance.html is saved at location **/root/Desktop/**

- **options set CREATOR [your name]** (here, **Jason**) and press **Enter**
- **options set CUSTOMER Mark Zuckerberg** (since you have performed information gathering on the name of **Mark Zuckerberg**) and press **Enter**.

72. After entering the above details, type the **run** command and press **Enter** to create a report for all the hosts that have been harvested, as shown in the screenshot.

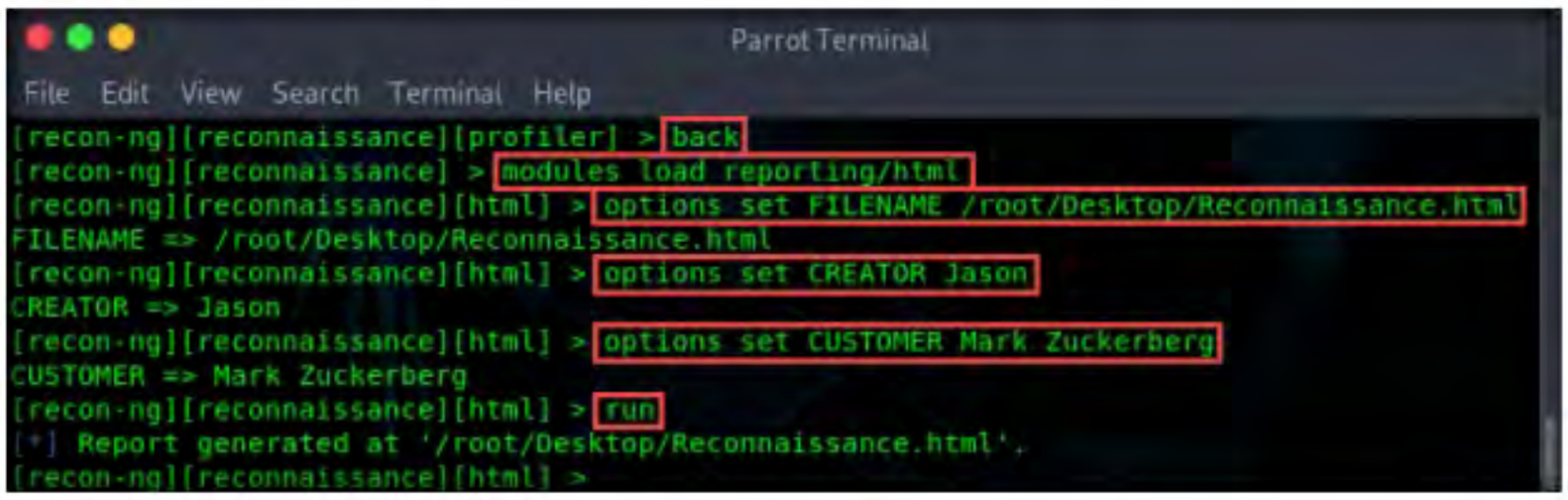


Figure 9.1.33: Configuring and running the Report module

73. The generated report is saved to **/root/Desktop/**. Navigate to the location, right-click on the **Reconnaissance.html** file, click on **Open With**, and select the **Firefox** browser from the available options.

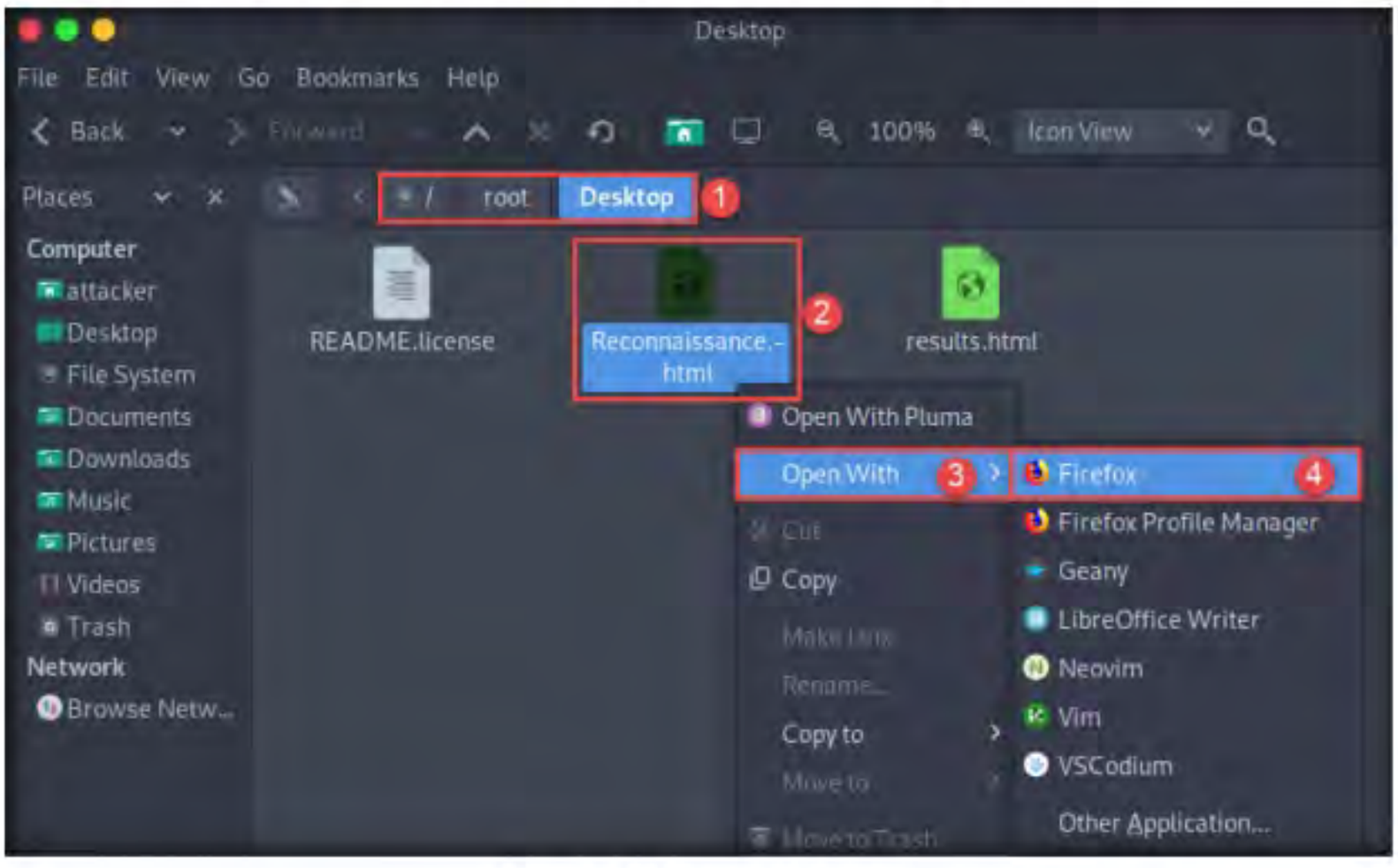


Figure 9.1.34: Viewing the Report

74. The generated report appears in the **Firefox** browser, displaying a summary of the result. You can expand the **Contacts** and **Profiles** nodes to view all the obtained results.

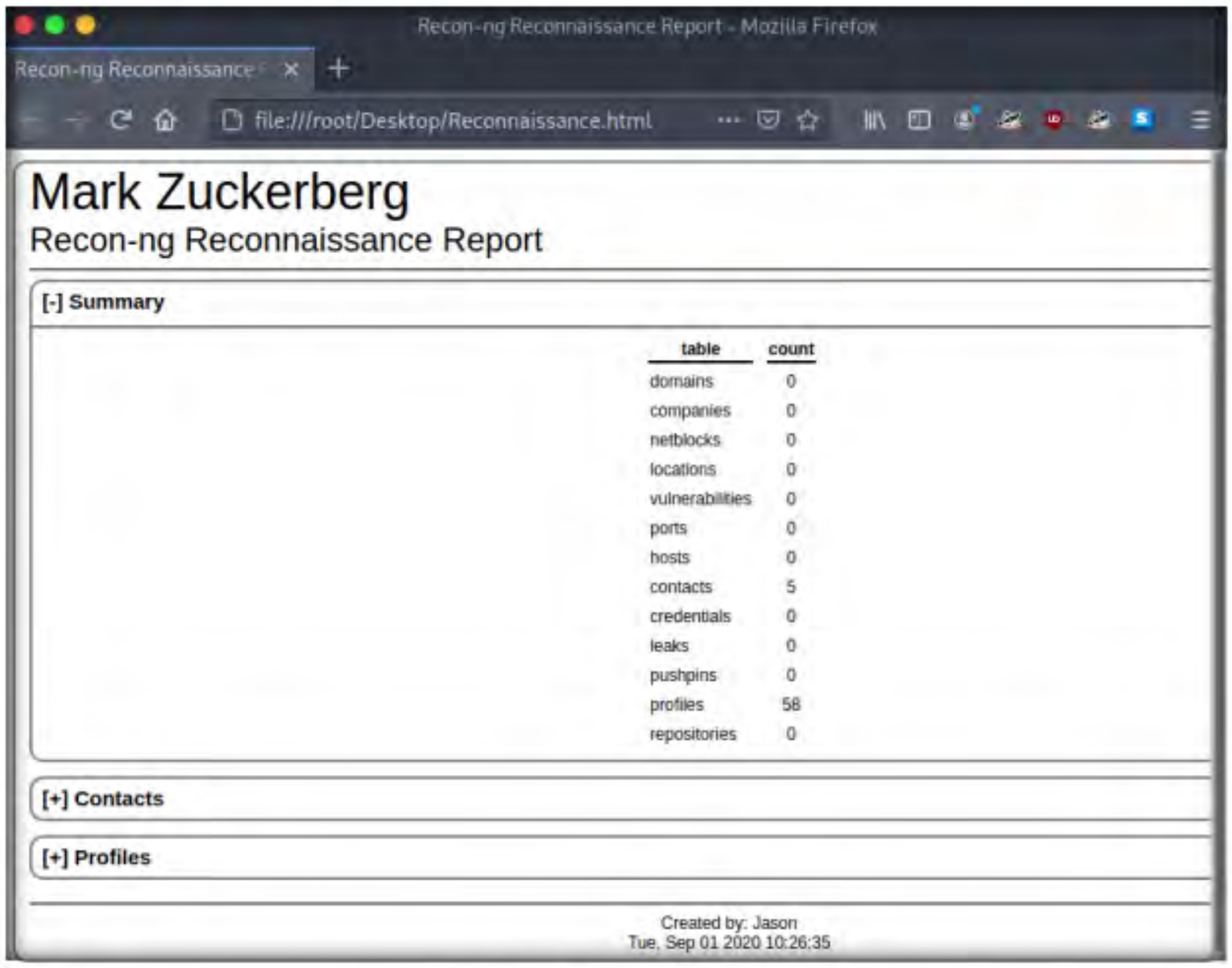


Figure 9.1.35: Viewing the Report

75. You can further expand the **Contacts** and **Profiles** node to view detailed information about the target.

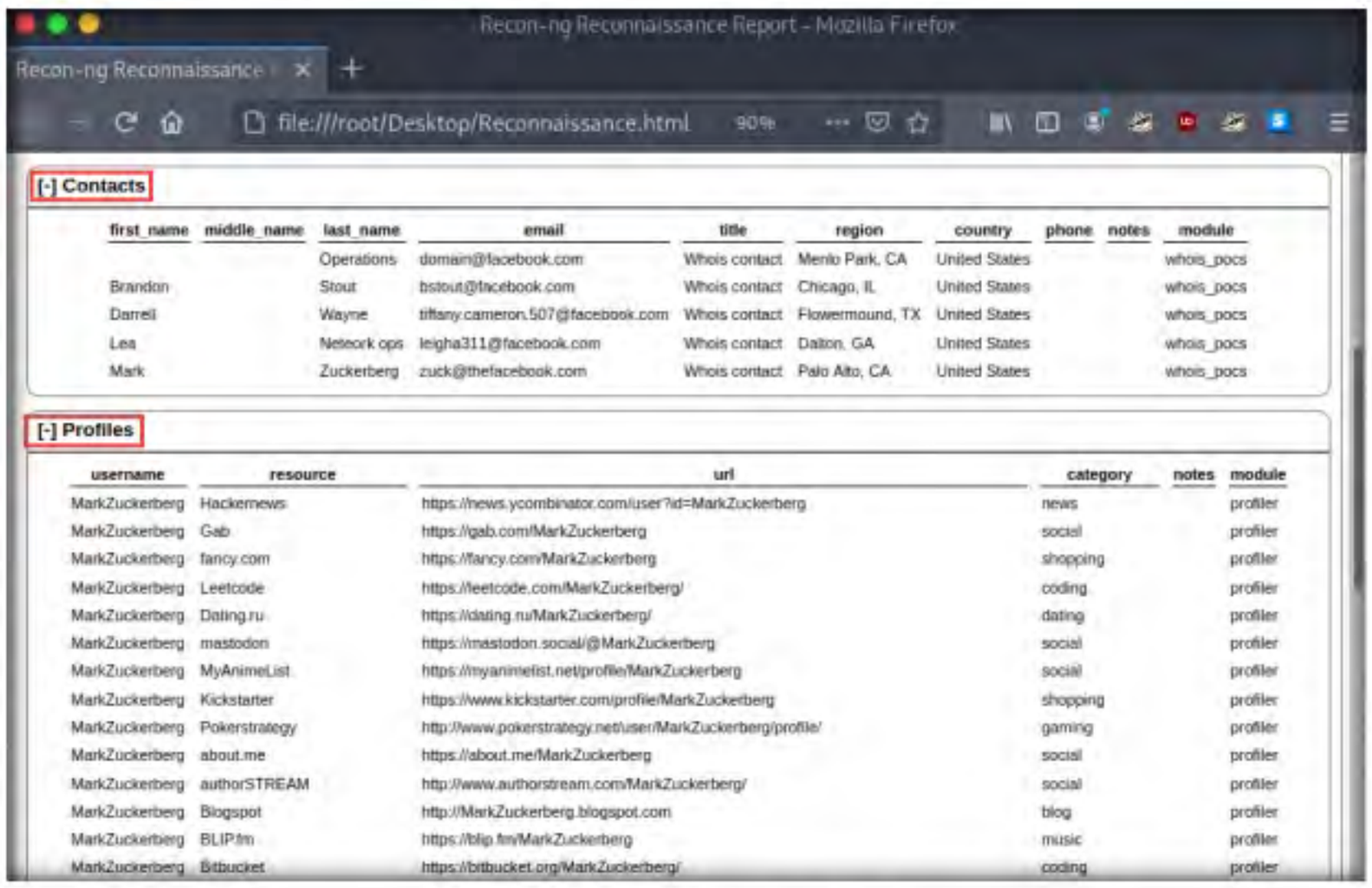


Figure 9.1.36: Expand Contacts and Profiles

76. We have now gathered information about the employee working in a target organization.
77. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.
78. Close all open windows and document all the acquired information.

TASK 2 Footprinting a Target using Maltego

Here, we will gather a variety of information about the target organization using Maltego.

TASK 2.1

Configure Maltego

1. In the **Parrot Security** virtual machine, launch **Maltego** by navigating to **Applications → Pentesting → Information Gathering → maltego**, as shown in the screenshot.

Maltego is a footprinting tool used to gather maximum information for the purpose of ethical hacking, computer forensics, and pentesting. It provides a library of transforms to discover data from open sources and visualizes that information in a graph format, suitable for link analysis and data mining.

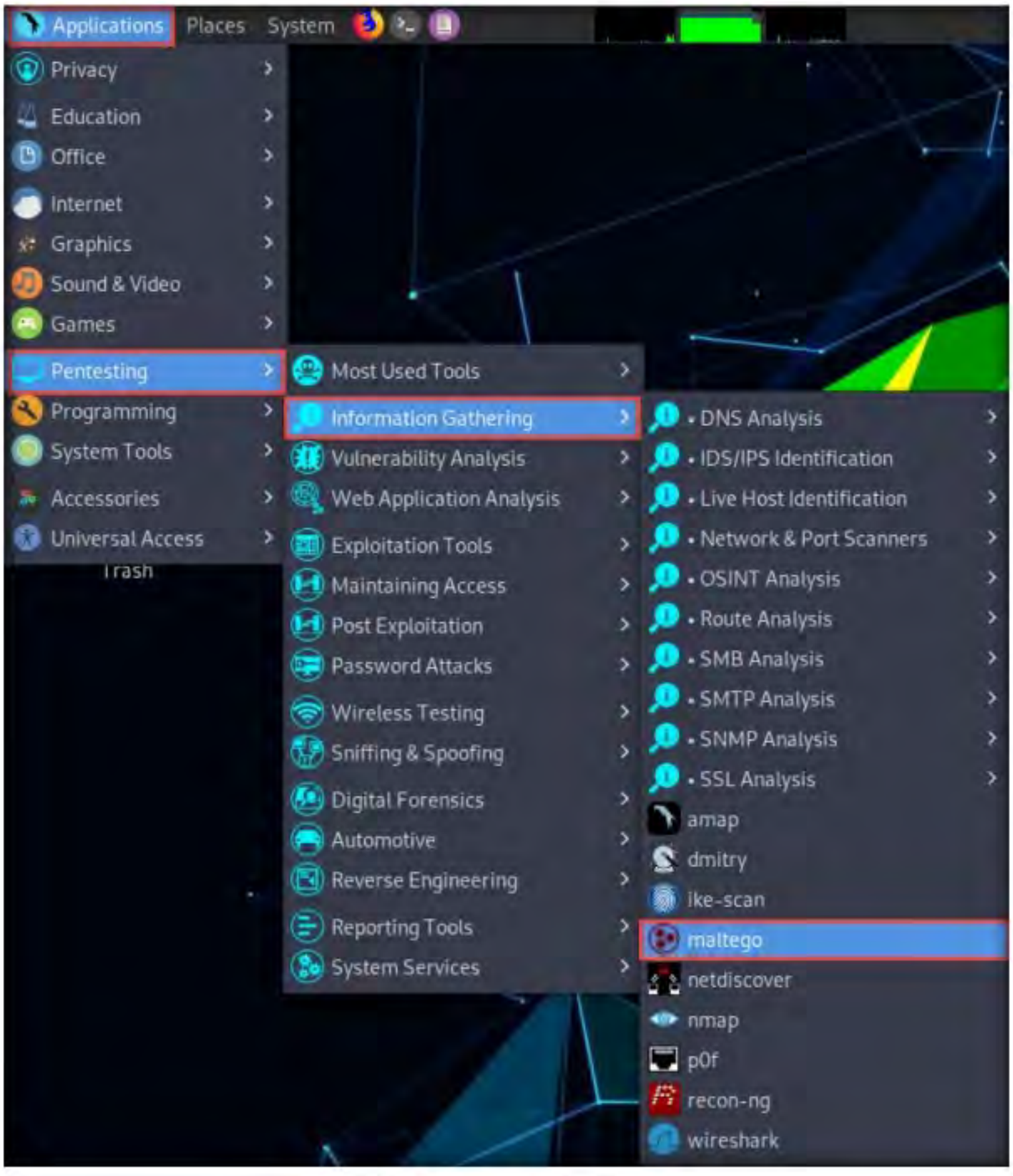


Figure 9.2.1: Maltego Product Selection wizard

2. A security pop-up appears, enter password as **toor** in the **Password** field and click **OK**.
3. A **Product Selection** wizard appears on the Maltego GUI; click **Run** from **Maltego CE (Free)** option.

Note: If the **Memory Settings Optimized** pop-up appears, click **Restart Now**.

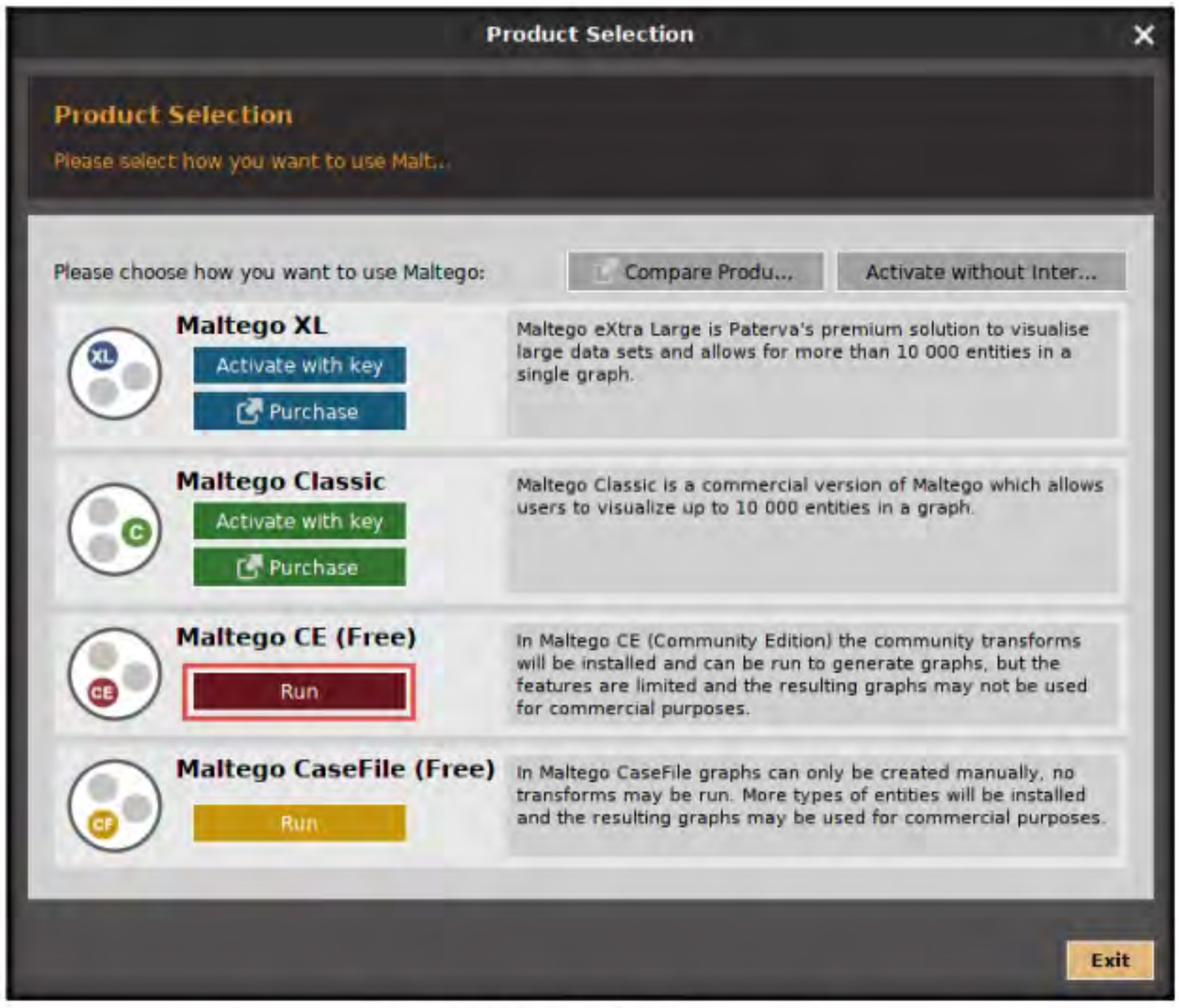


Figure 9.2.2: Maltego Product Selection wizard

Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate, and even making it possible to see hidden connections.

4. As the **Configure Maltego** window appears along with a **LICENSE AGREEMENT** form, check the **Accept** checkbox and click **Next**.

5. You will be redirected to the **Login** section; leave the **Maltego** window as it is and click **Firefox** icon from the top-section of the window to launch the Firefox browser.

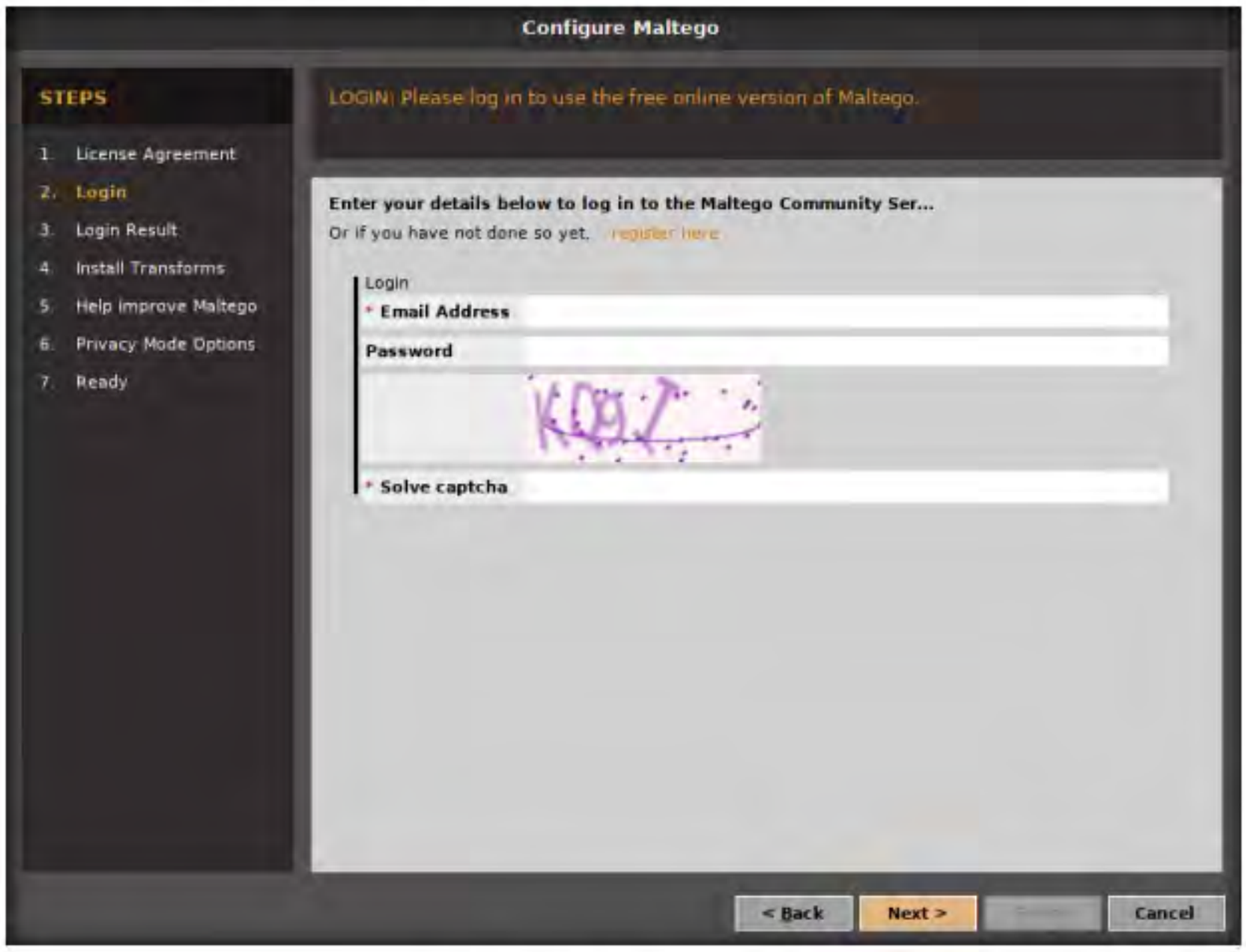


Figure 9.2.3: Maltego Login section

6. The **Firefox** window appears, in the address type **https://www.maltego.com/ce-registration** and press **Enter**
7. A **Register a Maltego CE Account** page appears, enter your details and confirm the captcha, and click **REGISTER** button to register your account and activate it.

Note: Please provide a working email ID at the time of registration. Once the registration is done, you will receive an activation email. Activate your account as instructed in the email to use the tool.

Note: If cookie notification appears in the lower section of the browser, click **Accept**.

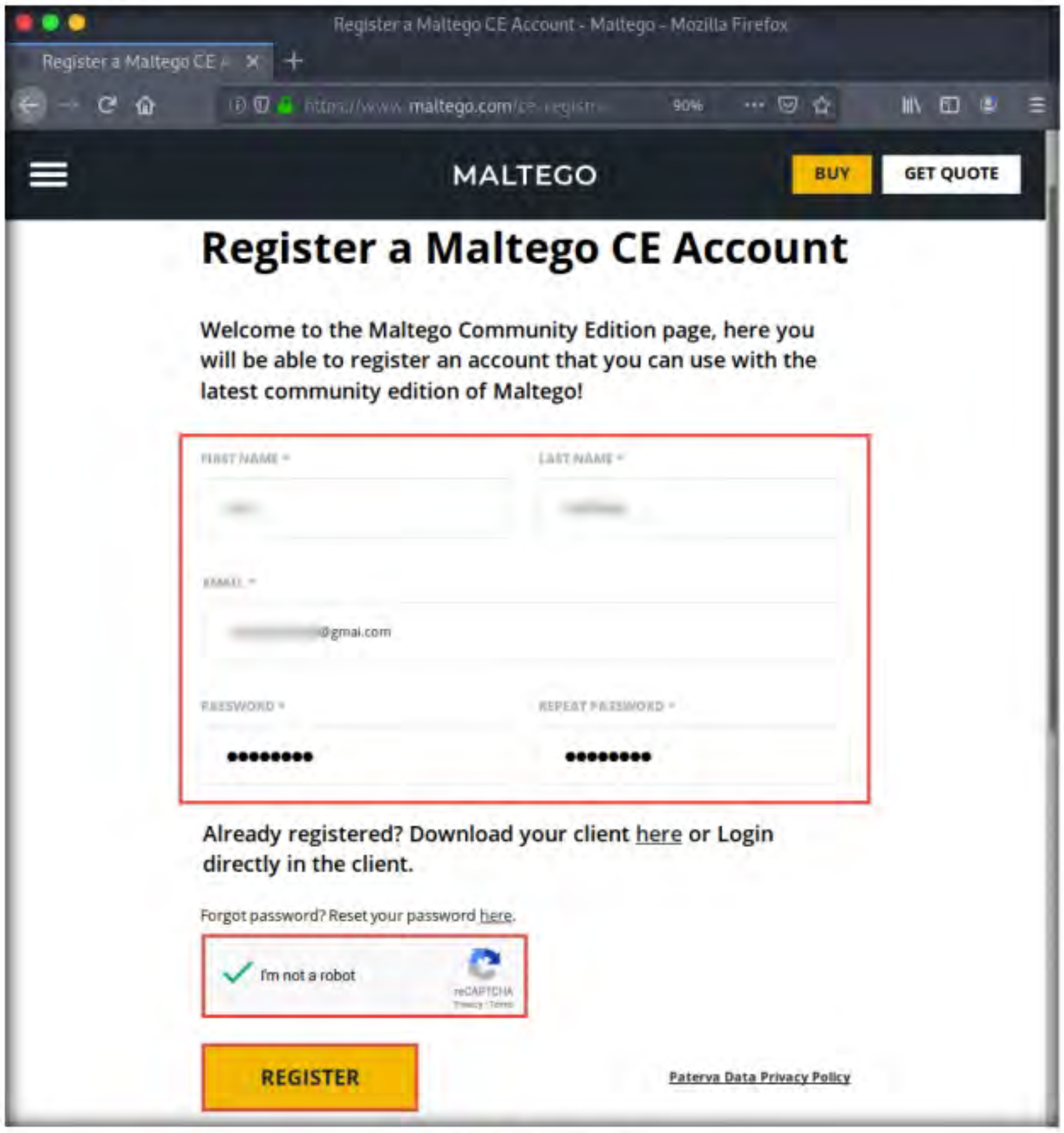


Figure 9.2.4: Registration Section

8. Minimize the web browser and go back to the setup wizard and enter the **Email Address** and **Password** specified at the time of registration; solve the **captcha** and click **Next**.

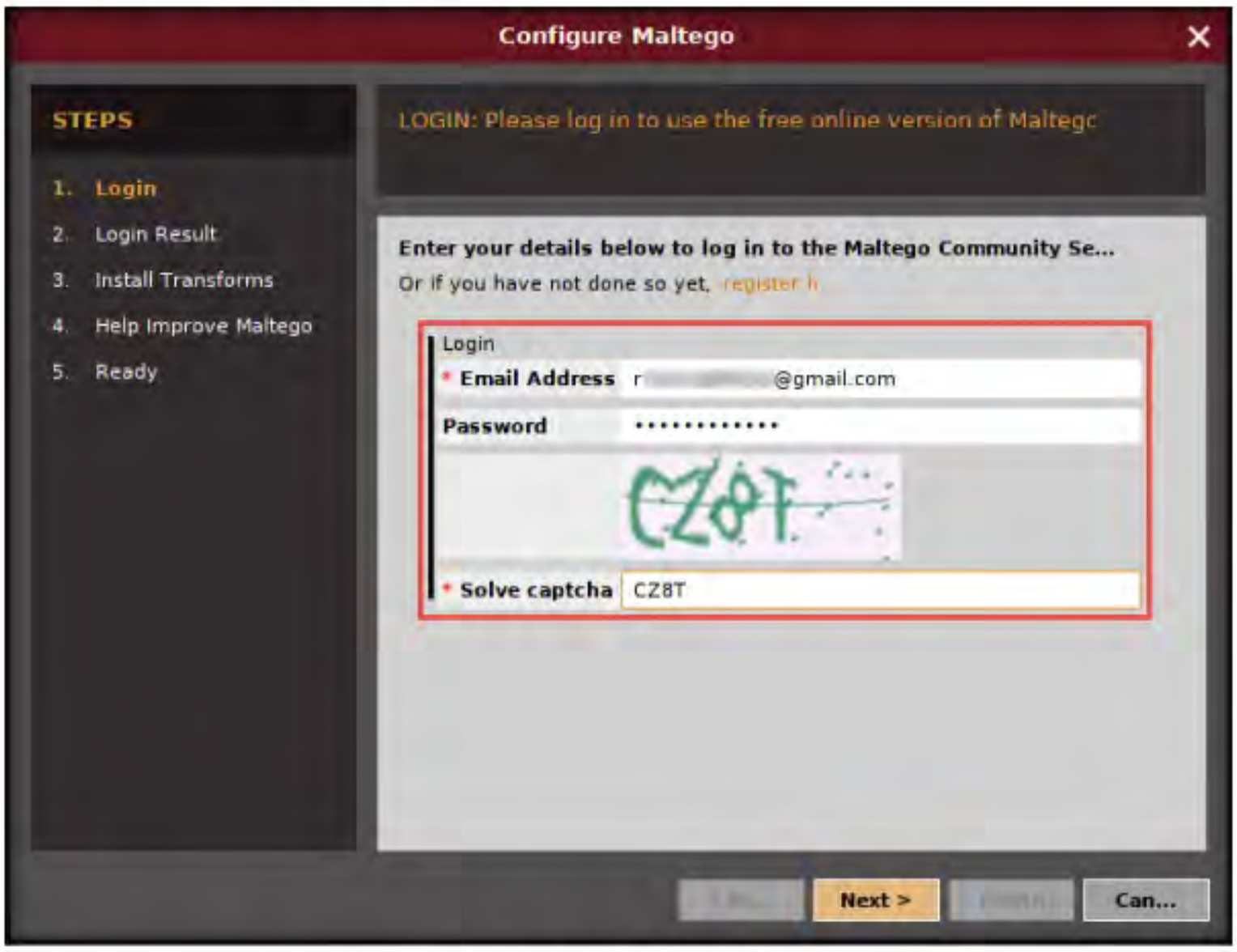


Figure 9.2.5: Maltego Login Section

9. The **Login Result** section displays your personal details; click **Next**.

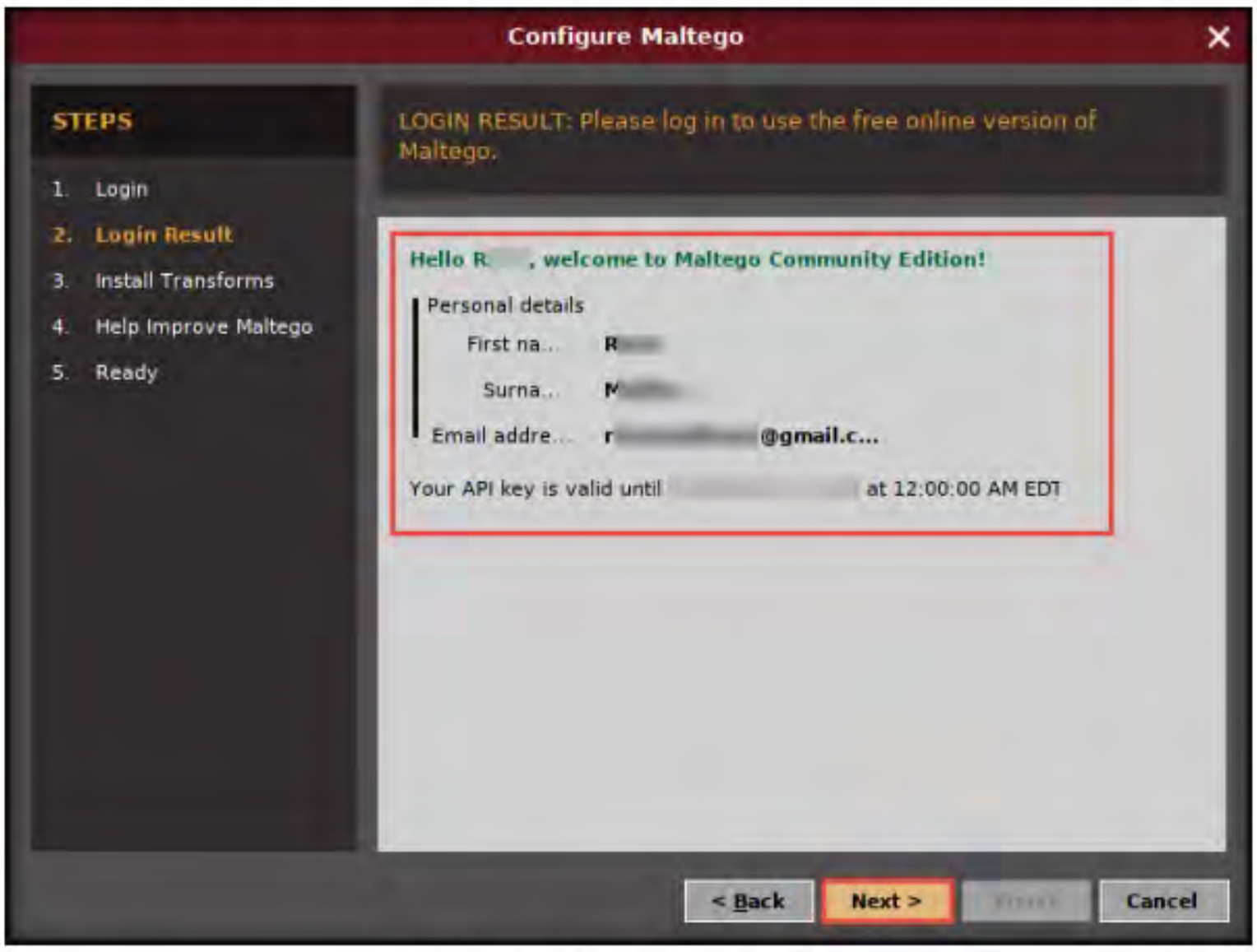


Figure 9.2.6: Maltego Login result section

10. The **Install Transforms** section appears, which will install items from the chosen transform server. Leave the settings to default and click **Next**.

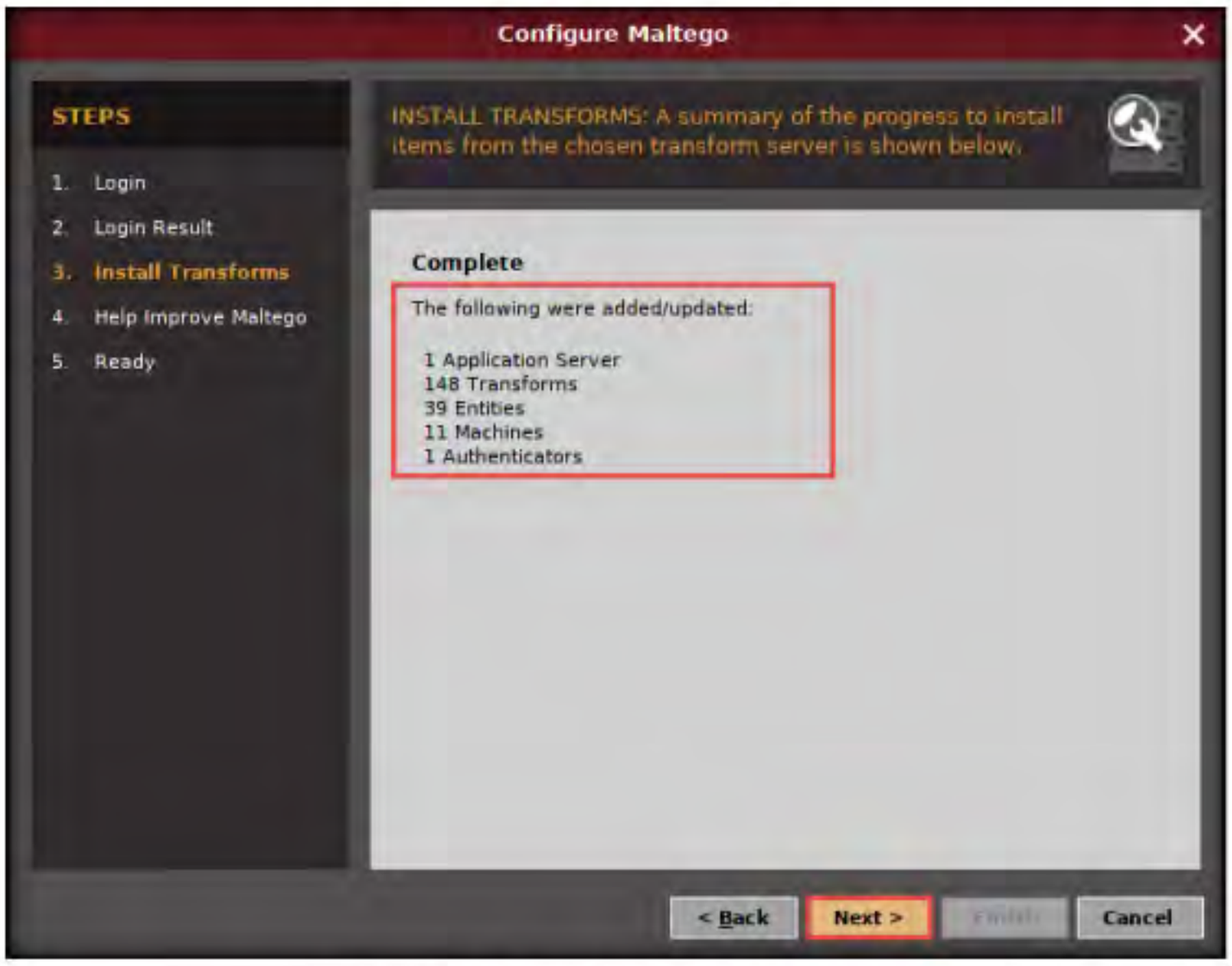


Figure 9.2.7: Maltego Install Transforms section

11. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.

Note: The screenshot might differ in your lab environment.

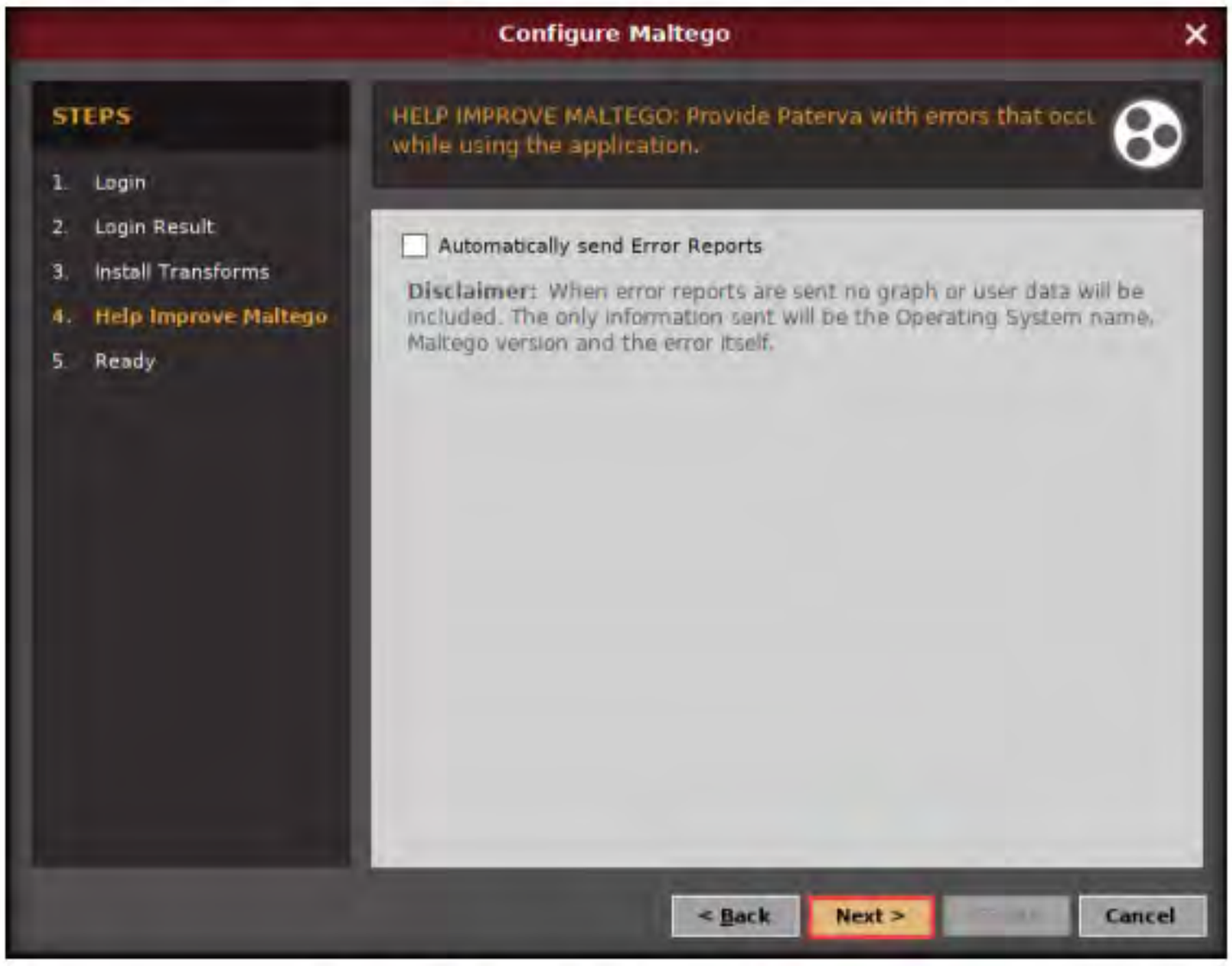


Figure 9.2.8: Maltego Help Improve Maltego section

12. The **Ready** section appears. Select the radio button of **Open a blank graph and let me play around** and click **Finish** to perform footprinting manually.

Note: If the **Privacy Policy Change Notice** appears, click **Acknowledge**.

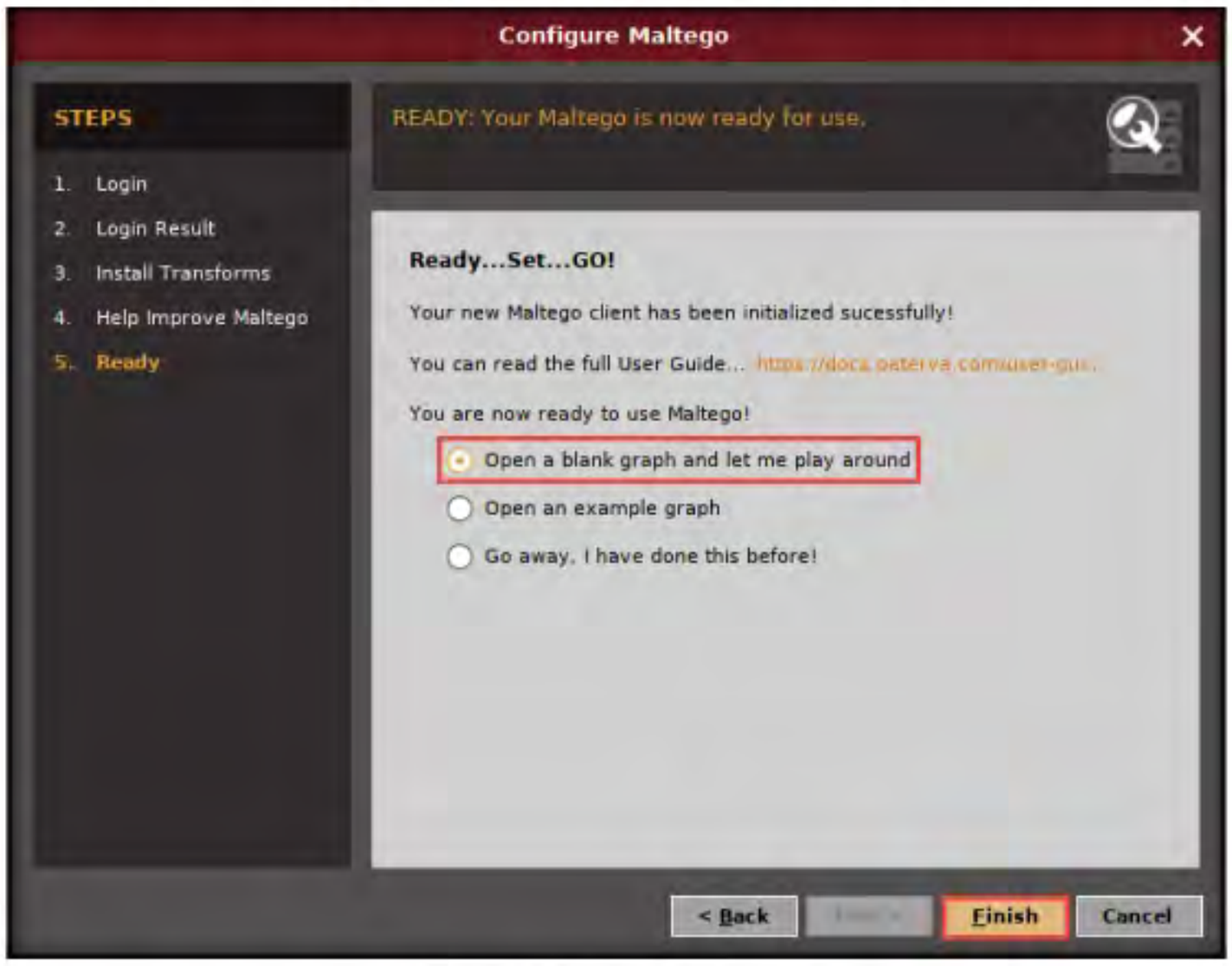


Figure 9.2.9: Maltego Ready wizard

13. The **Maltego Community Edition** GUI appears, and the **New Graph (1)** window will be automatically launched, as shown in the screenshot.

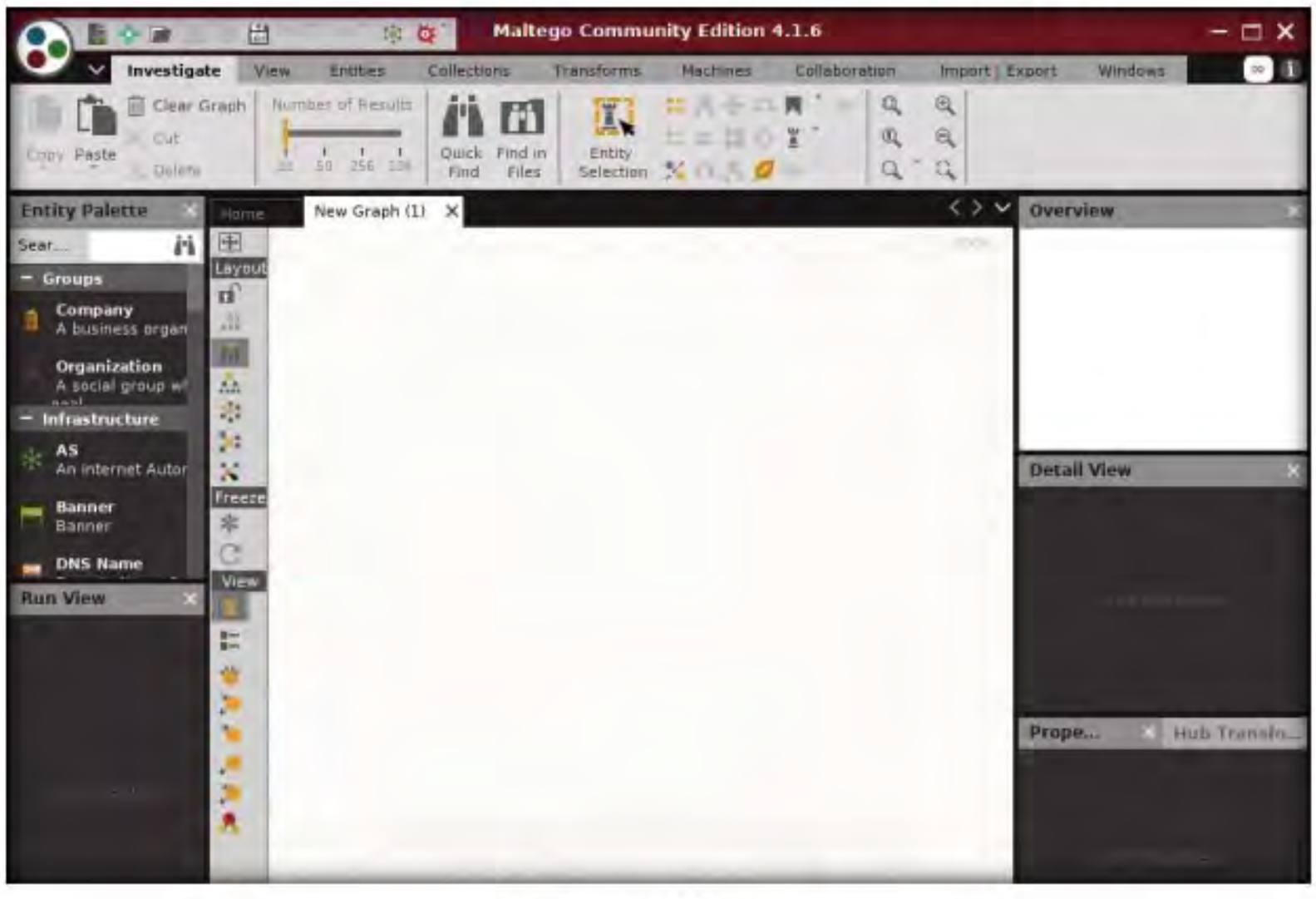


Figure 9.2.10: Maltego GUI

Note: If the **New Graph (1)** window does not open automatically, click the icon located at the top-left corner of the GUI (in the toolbar) to start a new graph.

Figure 9.2.11: Maltego Toolbar

TASK 2.2

Add a Domain Entity

14. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS**, **DNS Name**, **Domain**, **IPv4 Address**, **URL**, **Website**, etc.
15. Drag the **Website** entity onto the **New Graph (1)** window.

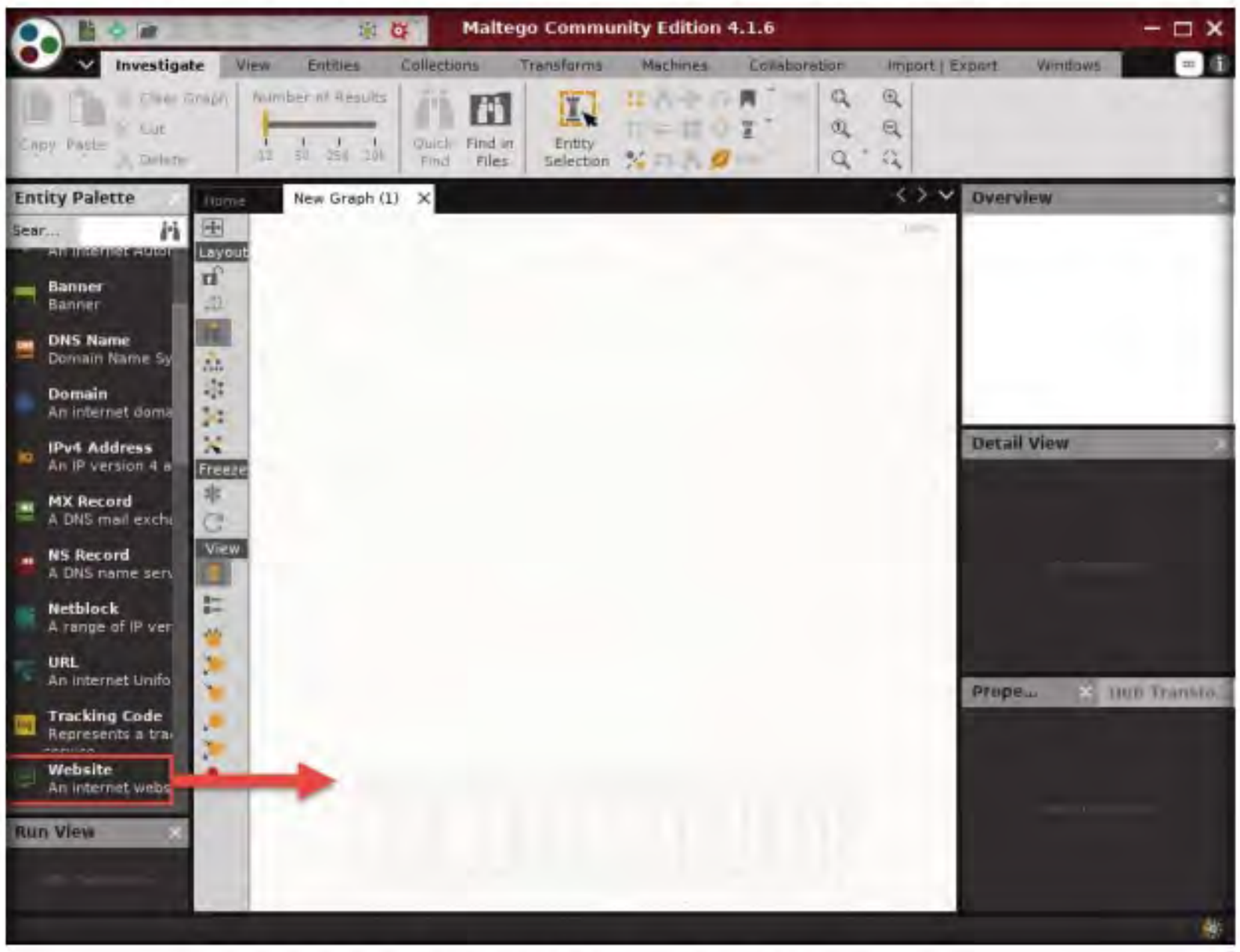


Figure 9.2.12: Selecting a Website Entity

16. The entity appears on the new graph, with the **www.paterva.com** URL selected by default.

Note: If you are not able to view the entity as shown in the screenshot, click in the **New Graph (1)** window and **scroll up**, which will increase the size of the entity.

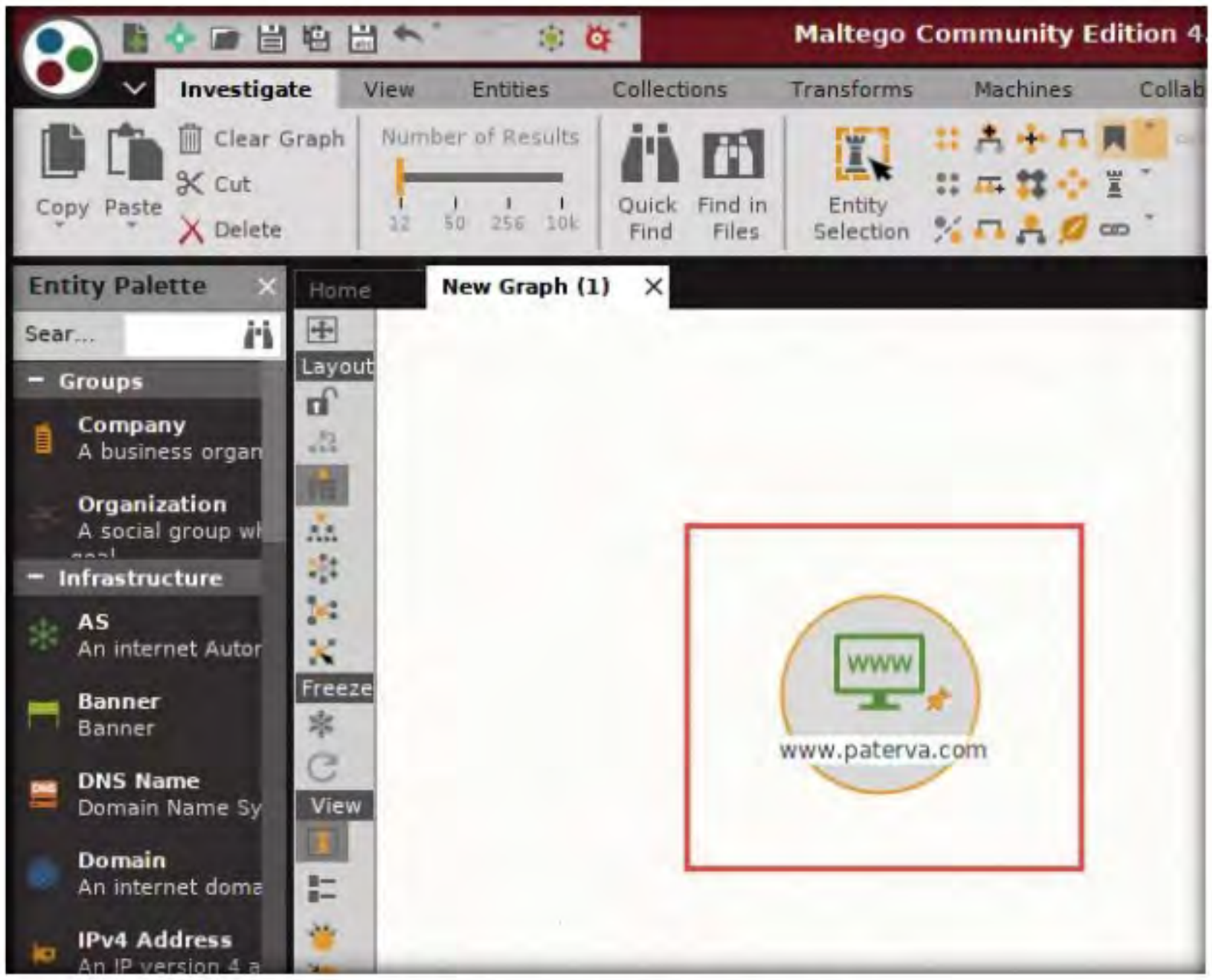


Figure 9.2.13: Website Entity in the New Graph (1) Section

17. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press **Enter**.

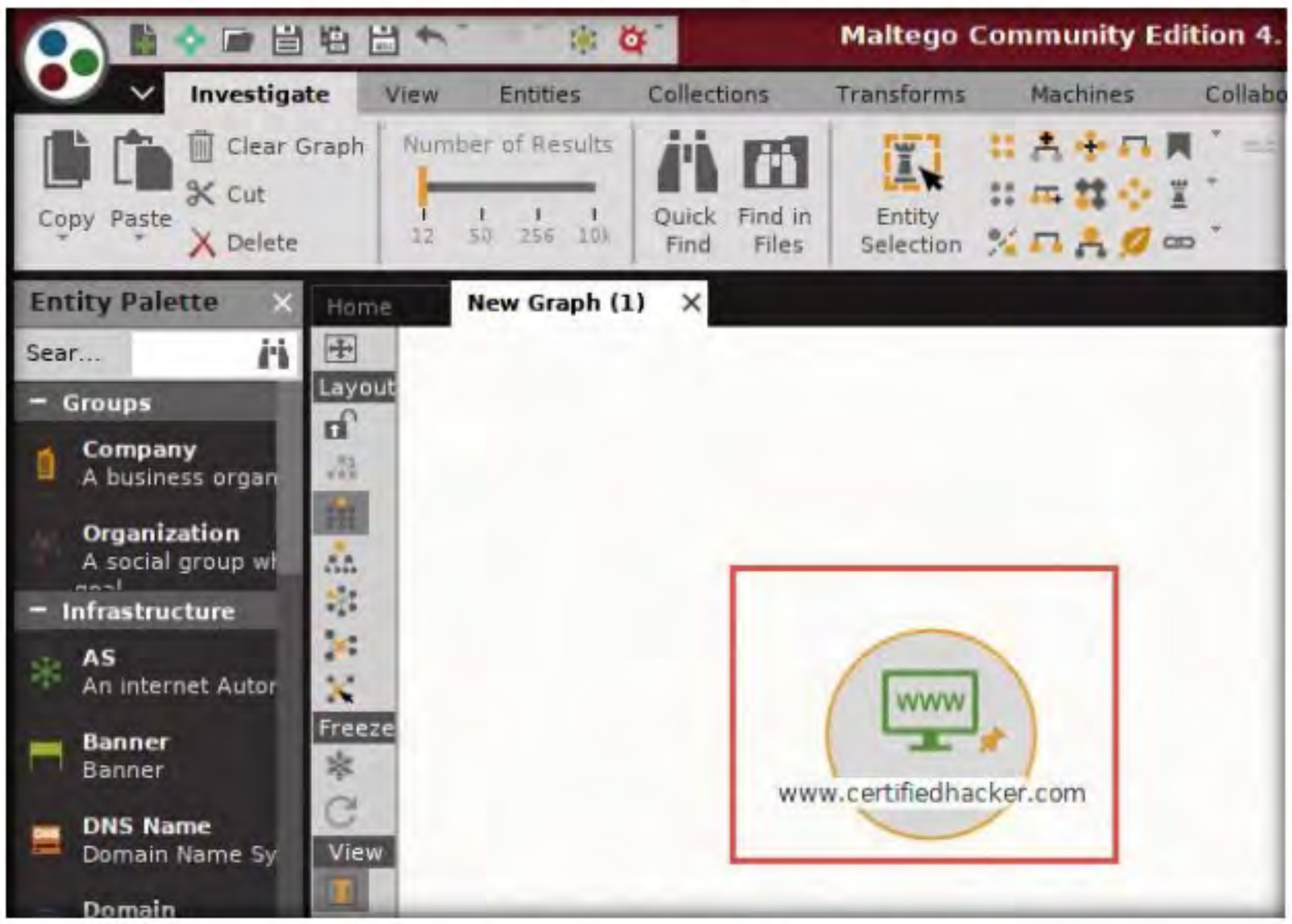


Figure 9.2.14: Website Entity in the New Graph (1) Section

TASK 2.3

Identify the Server-Side Technology

18. Right-click the entity and select **All Transforms**.

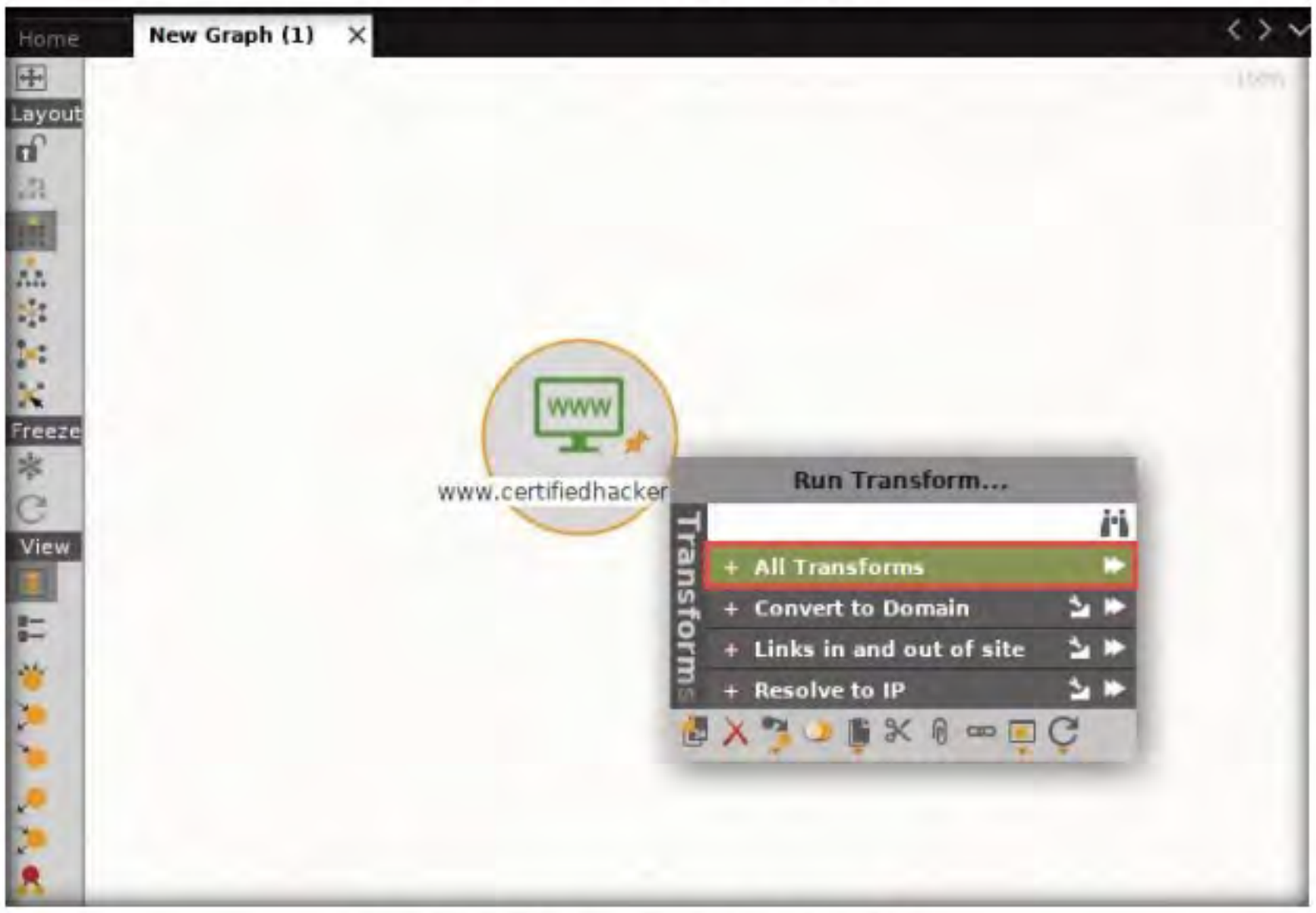


Figure 9.2.15: Selecting to Server Technologies Website

19. The **Run Transform(s)** list appears; click **To Server Technologies [Using BuiltWith]**.

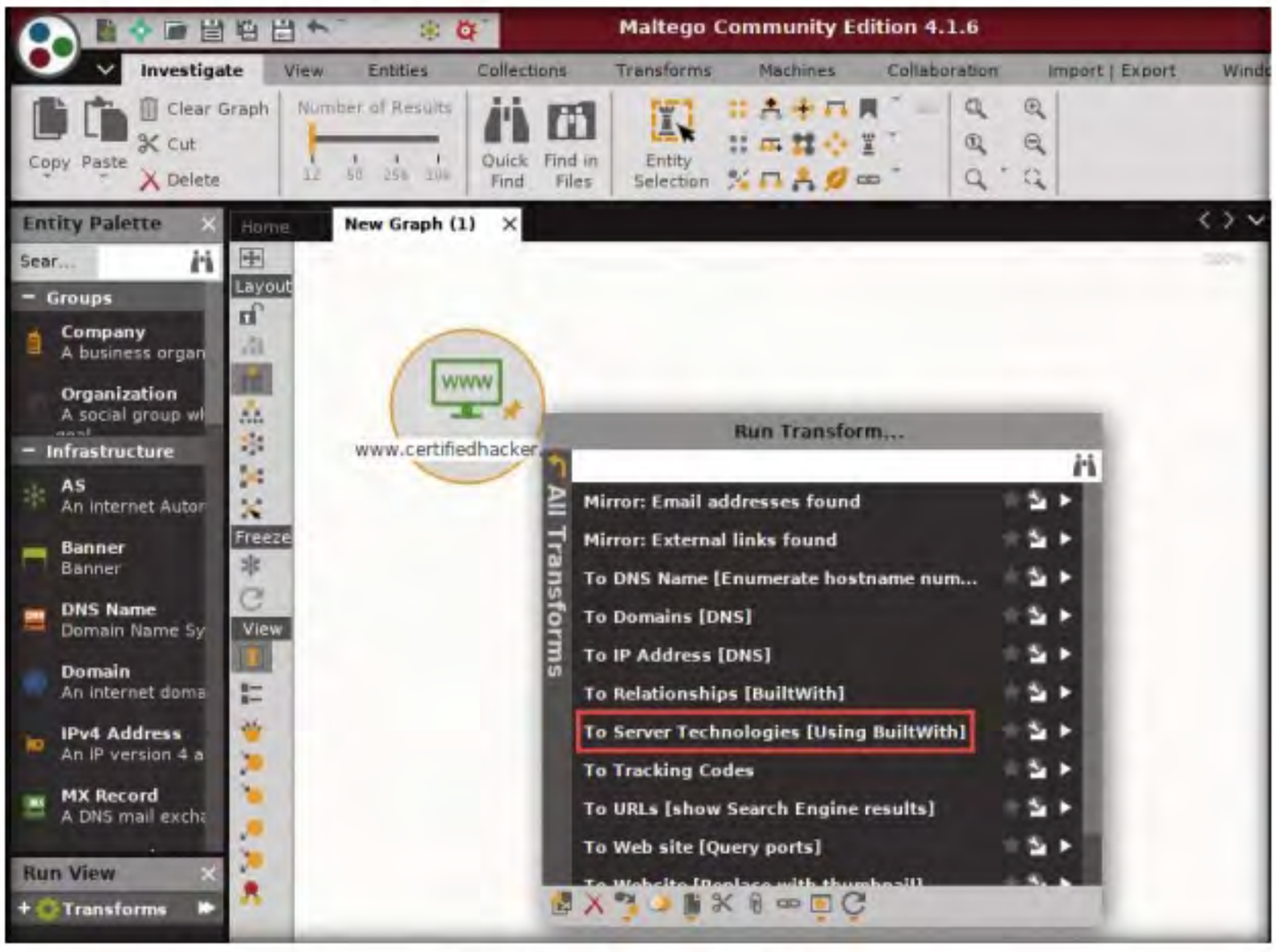


Figure 9.2.16: Run Transform(s) list

20. Maltego starts running the transform the **To Server Technologies [Using BuiltWith]** entity. Observe the status in the progress bar.

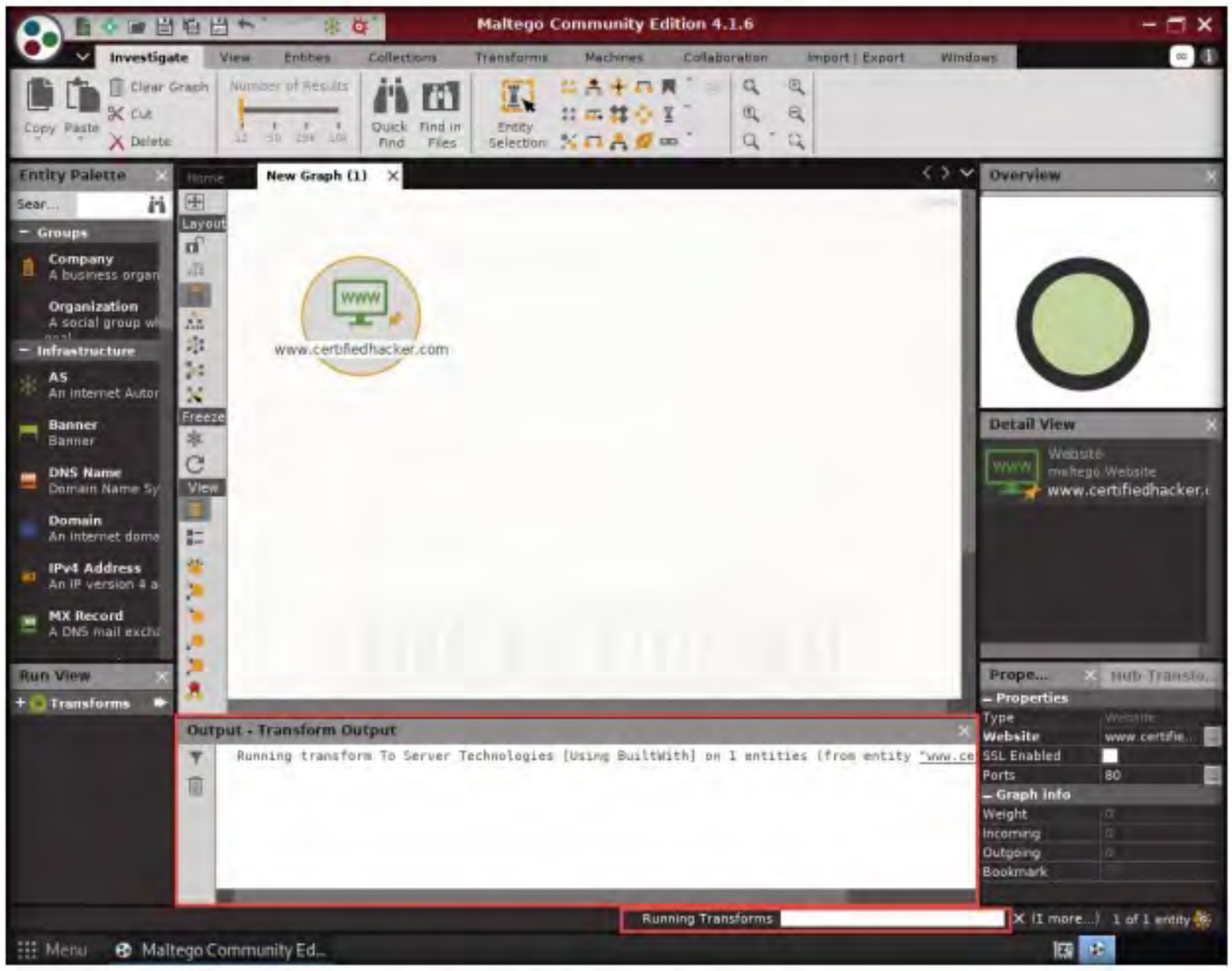


Figure 9.2.17: Progress bar pop-up

21. Once Maltego completes the transforming server-side technologies, it displays the technology implemented on the server that hosts the website, as shown in the following screenshot.

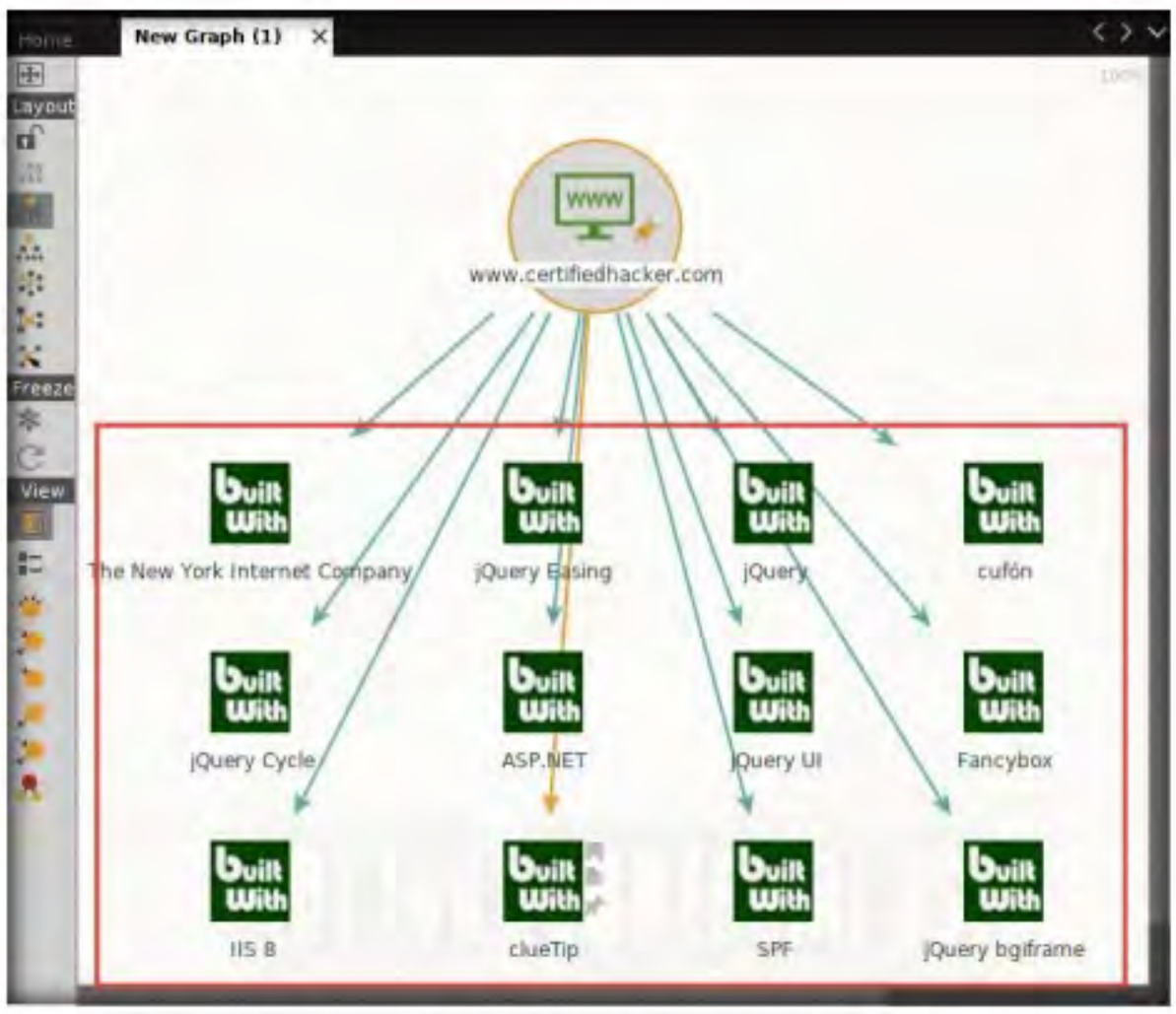


Figure 9.2.18: Server-Side Technologies in www.certifiedhacker.com

22. After obtaining the built-in technologies of the server, you can search for related vulnerabilities and simulate exploitation techniques to hack them.
23. To start a new transform, select all the entities, excluding the **www.certifiedhacker.com** website entity, and press **Delete**.
24. A **Delete** pop-up appears; click **Yes**.

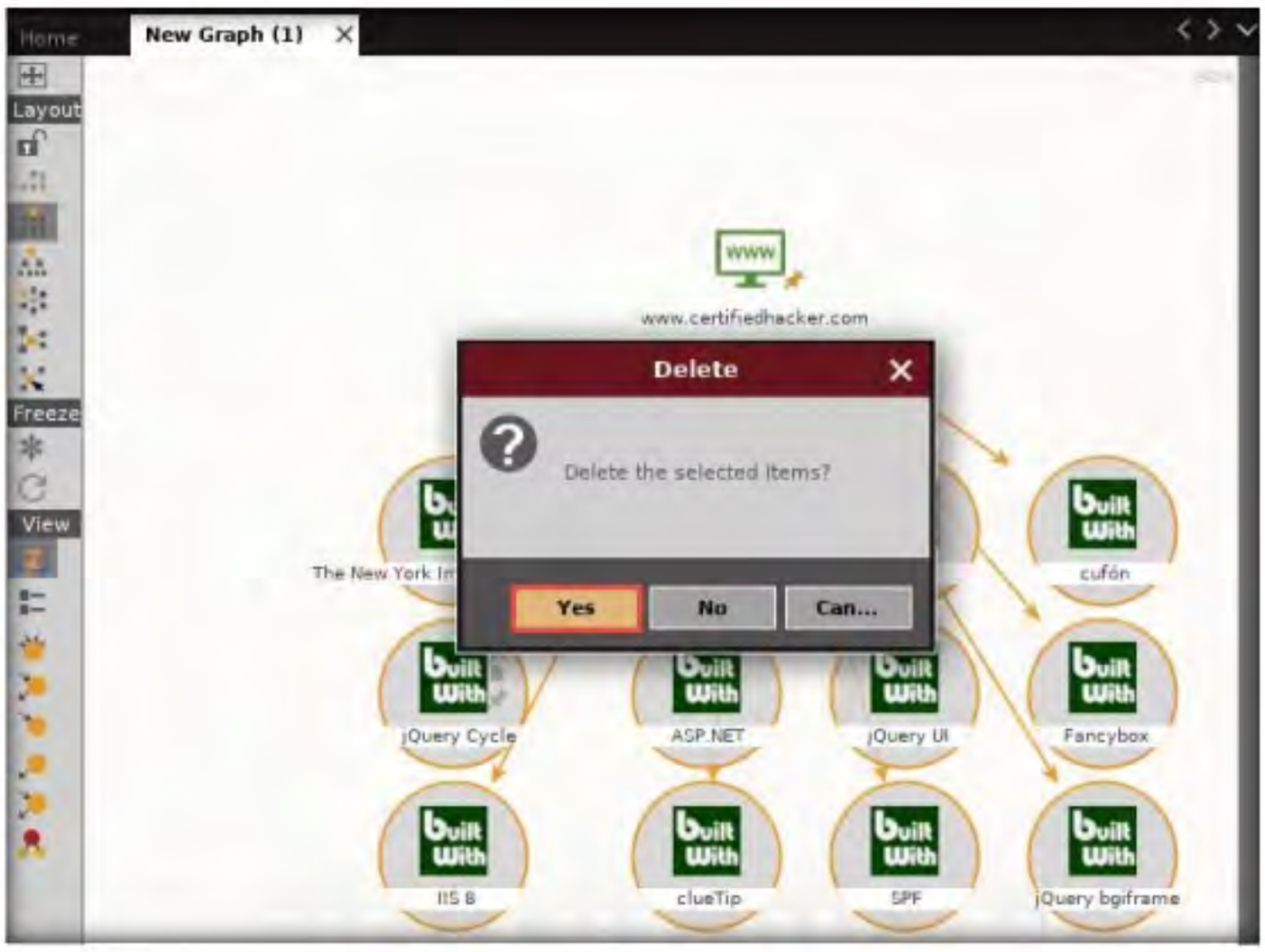


Figure 9.2.19: Delete pop-up

TASK 2.4

Identify the Domain

25. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms → To Domains [DNS]**.

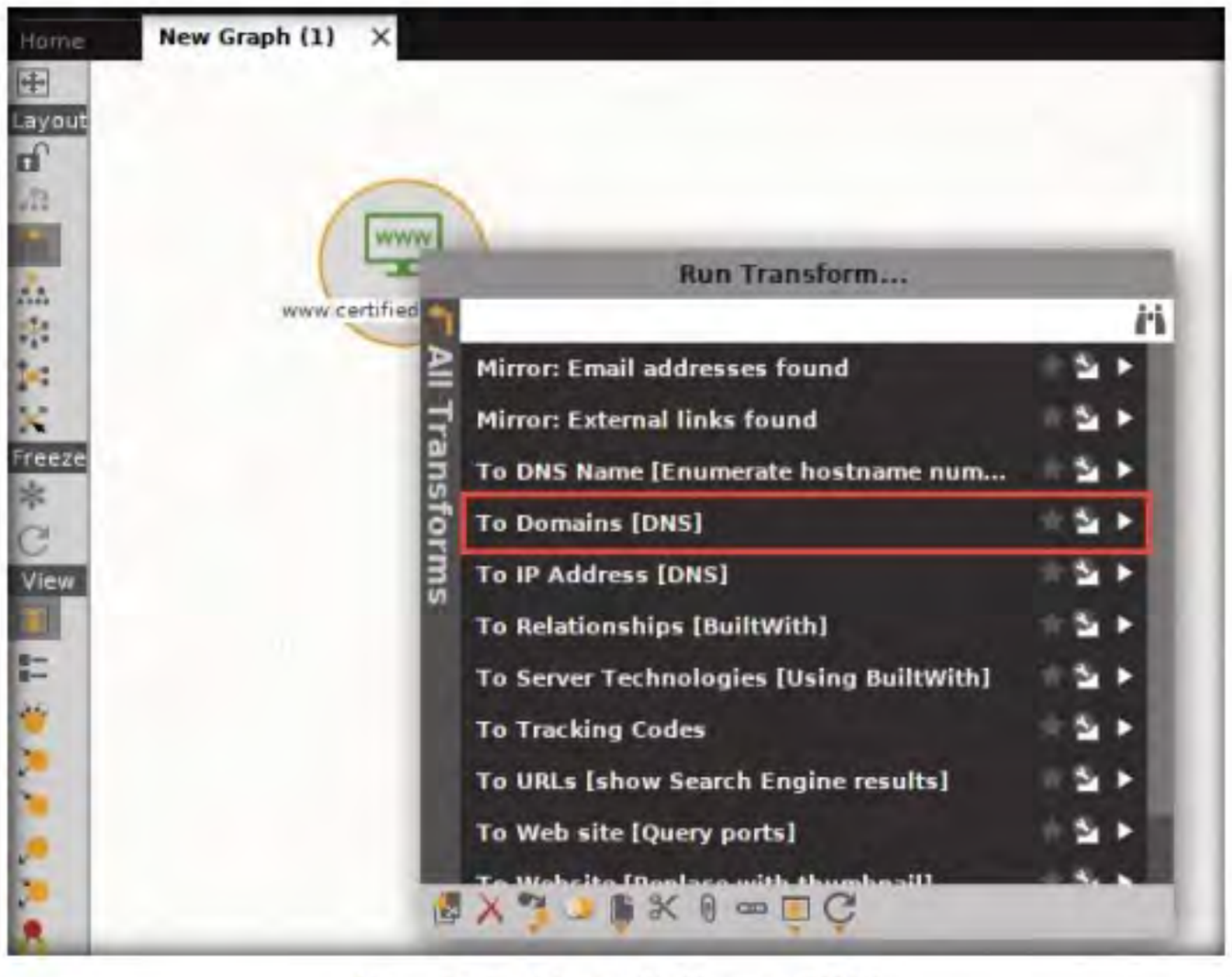


Figure 9.2.20: Selecting To Domains [DNS]

26. The domain corresponding to the website displays, as shown in the following screenshot.

Note: Screenshots may differ in your lab environment.

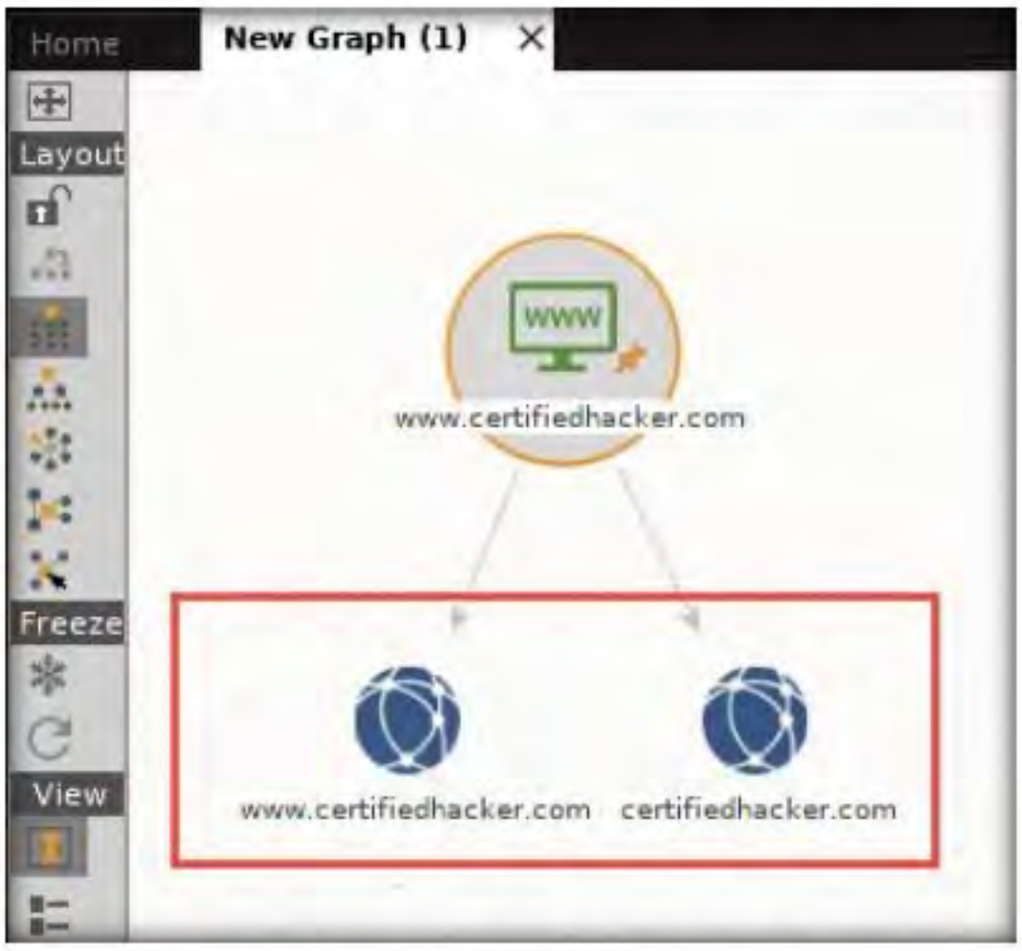


Figure 9.2.21: Domain Name of the Corresponding Website

TASK 2.5

Identify the Domain Name Schema

27. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name [Using Name Schema diction...]**.

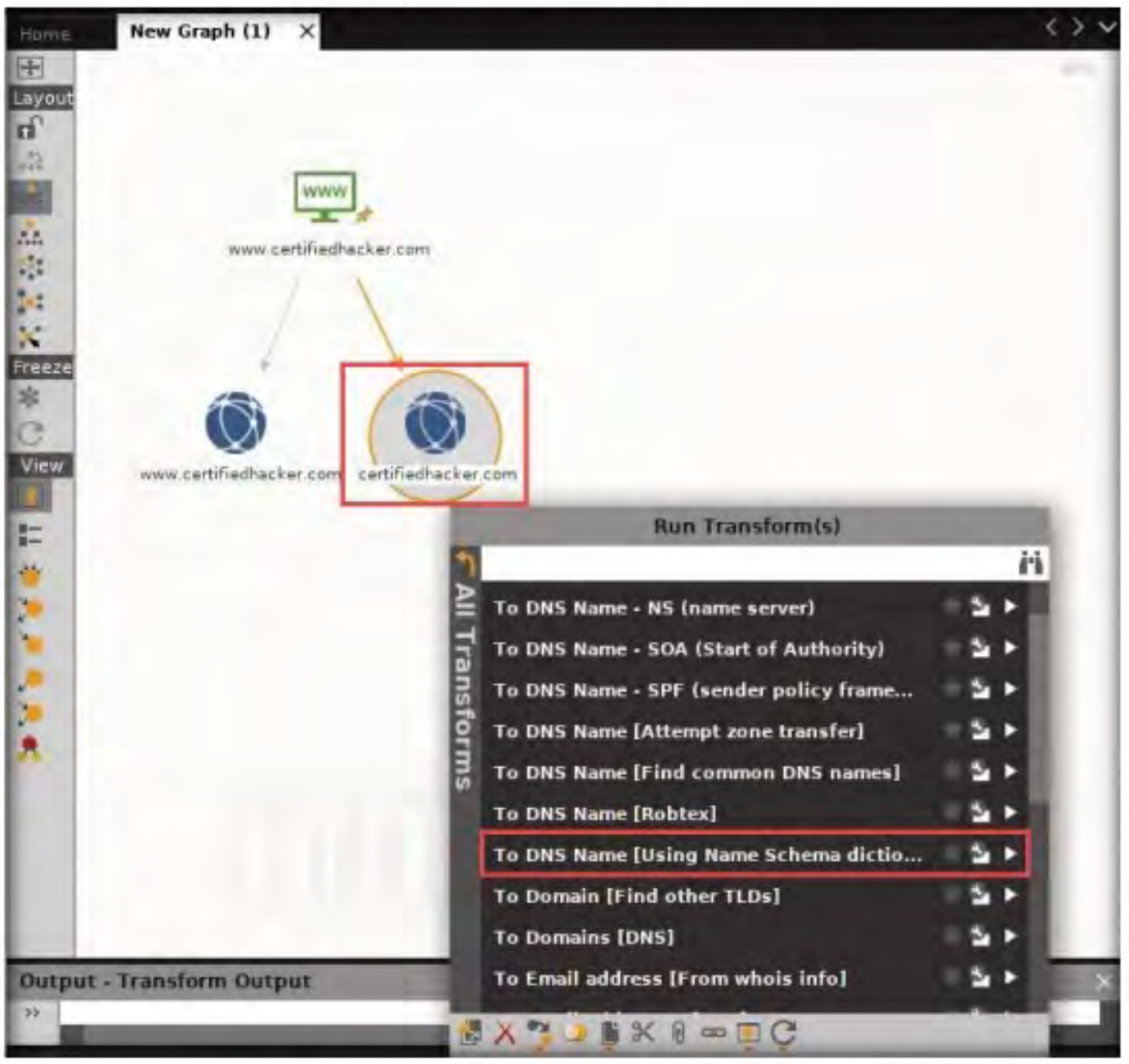


Figure 9.2.22: Selecting To DNS Name [Using Name Schema diction…]

28. Observe the status in the progress bar. This transform will attempt to test various name schemas against a domain and try to identify a specific name schema for the domain, as shown in the following screenshot.

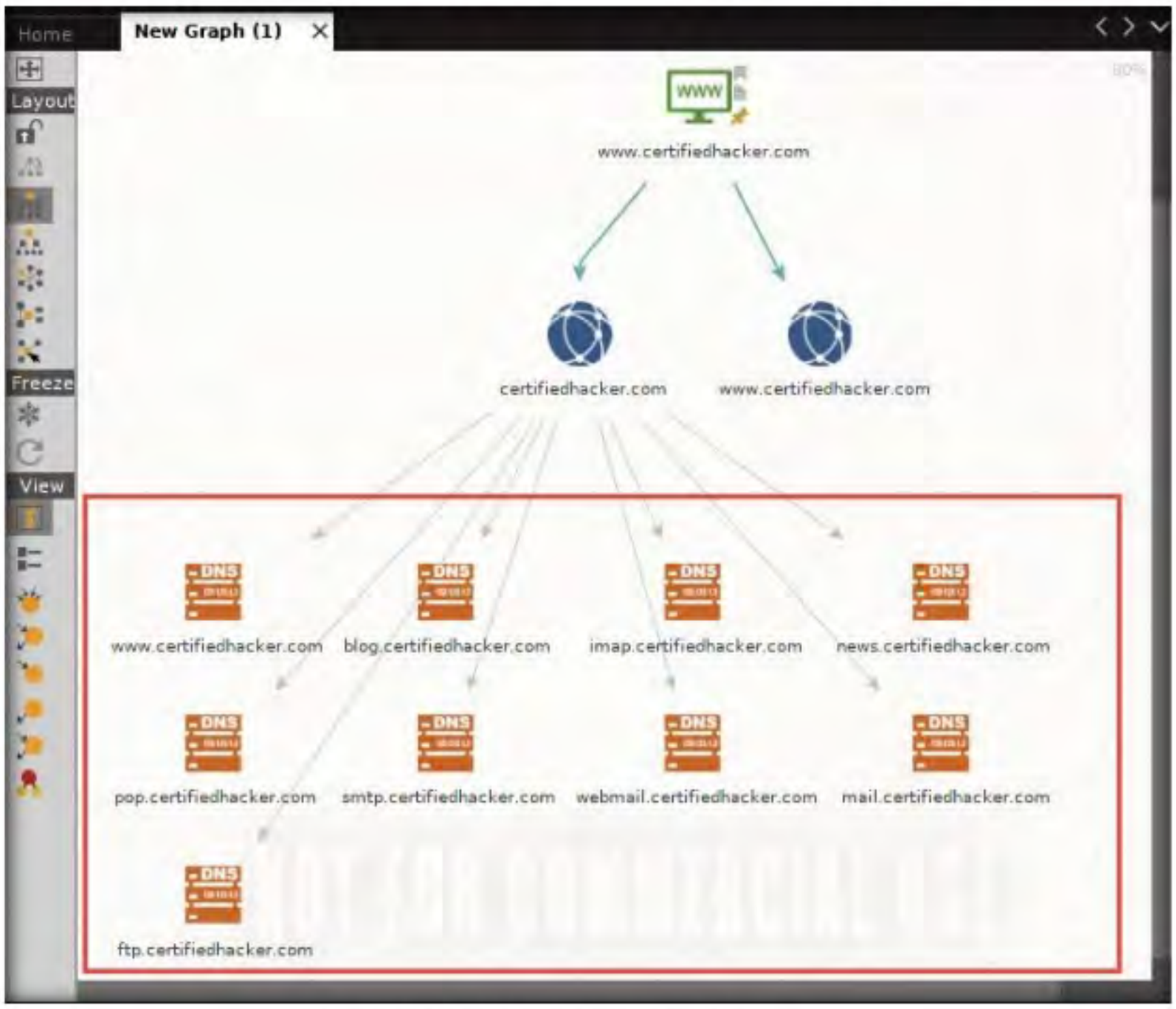


Figure 9.2.23: DNSNameSchema of certifiedhacker.com

29. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential information.
30. Select only the name schemas by dragging and deleting them.

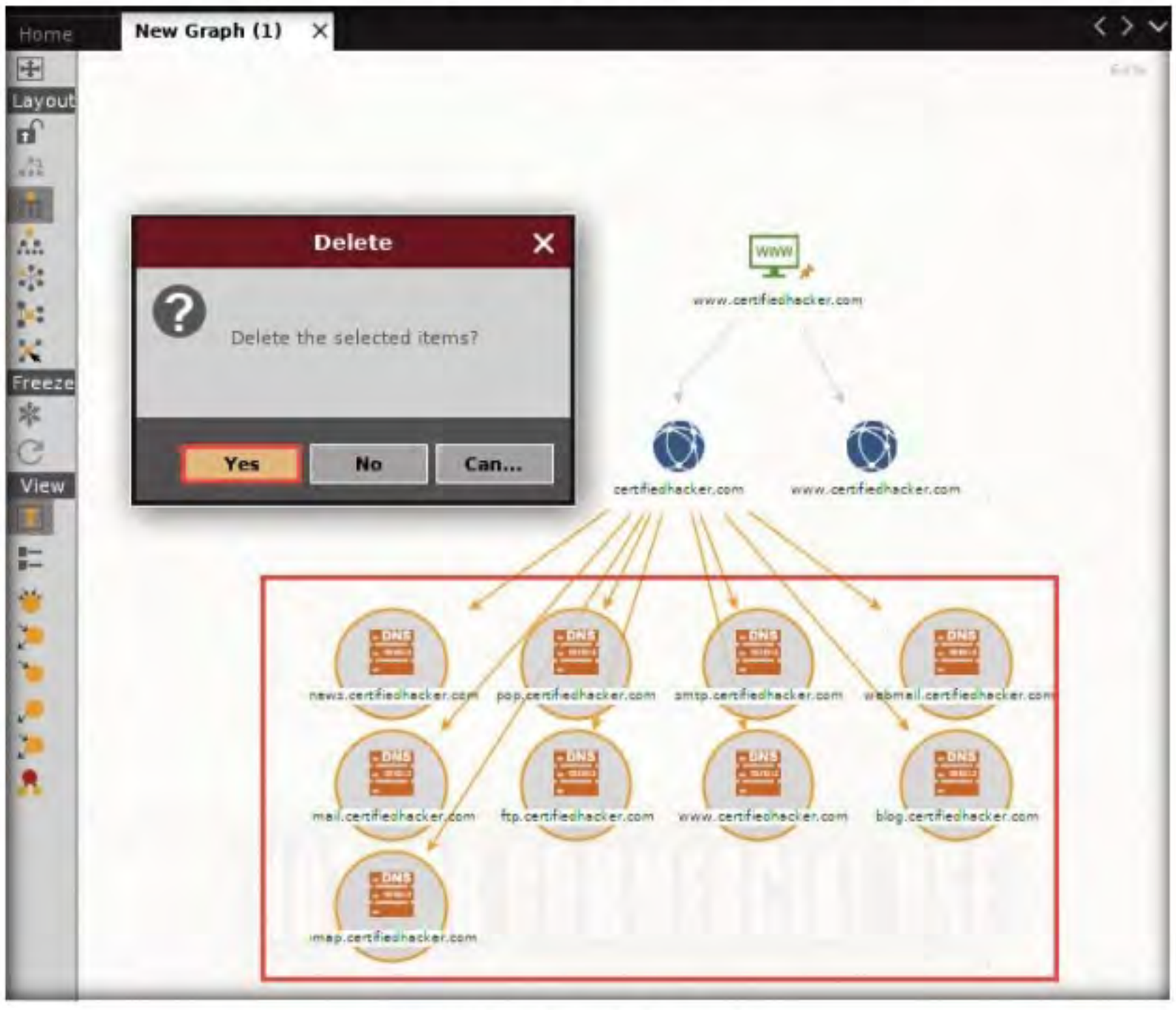


Figure 9.2.24: Deleting the Name Schemas

TASK 2.6

Identify the Service Oriented Architecture (SOA) Information

31. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - SOA (Start of Authority)**.

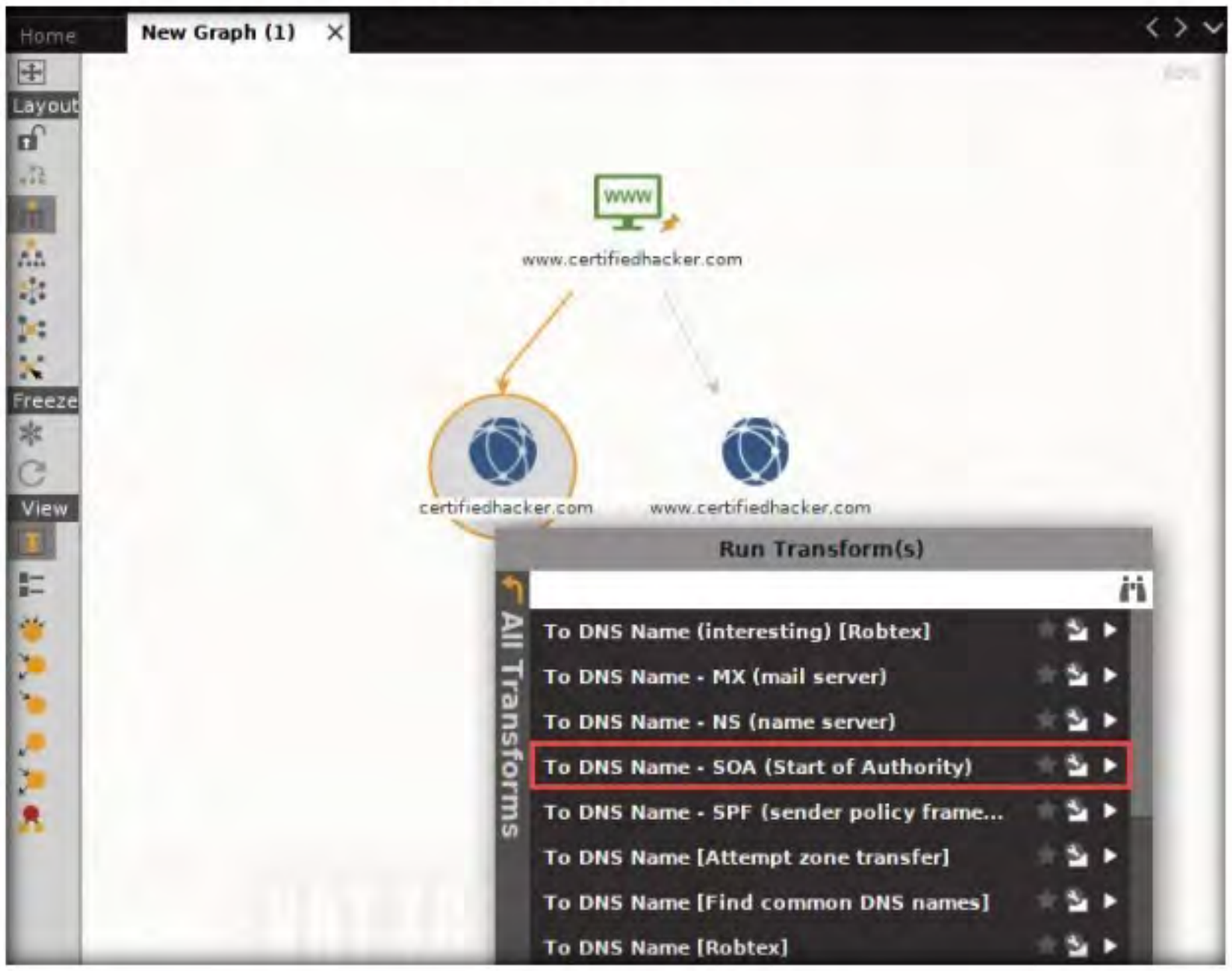


Figure 9.2.25: Selecting To DNS Name - SOA

32. This returns the primary name server and the email of the domain administrator, as shown in the following screenshot.

Figure 9.2.26: Primary Name Server and the Email of the Domain

33. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.
34. Select both the name server and the email by dragging and deleting them.

Figure 9.2.27: Deleting the Primary Name Server and the Email of the Domain

TASK 2.7

Identify the Mail Exchanger

35. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - MX (mail server)**.

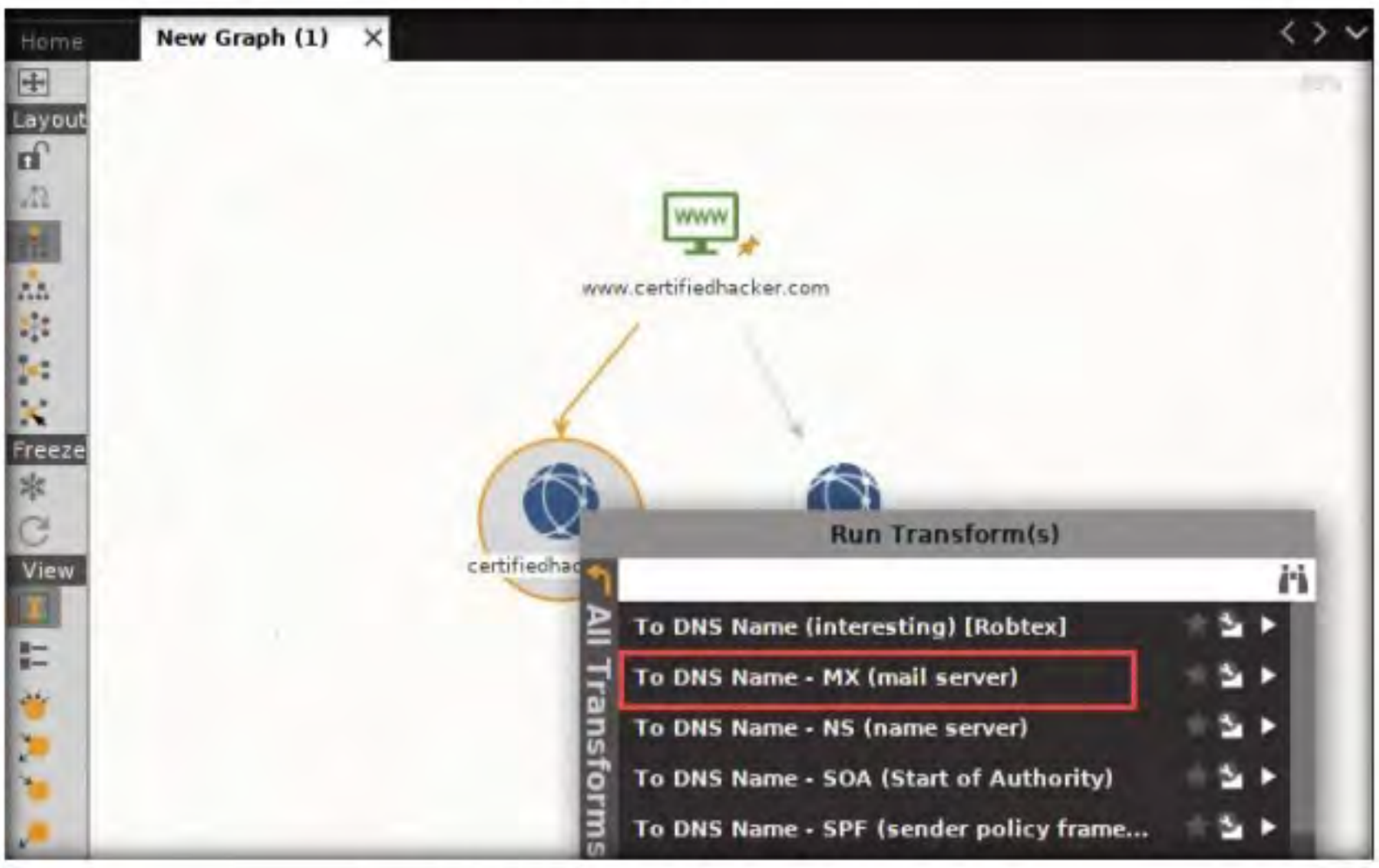


Figure 9.2.28: Selecting To DNS Name - MX (mail server)

36. This transform returns the mail server associated with the certifiedhacker.com domain, as shown in the following screenshot.

Figure 9.2.29: Mail Server Associated with the certifiedhacker.com

37. By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and, thereby, use it to perform malicious activities such as sending spam e-mails.

38. Select only the mail server by dragging and deleting it.

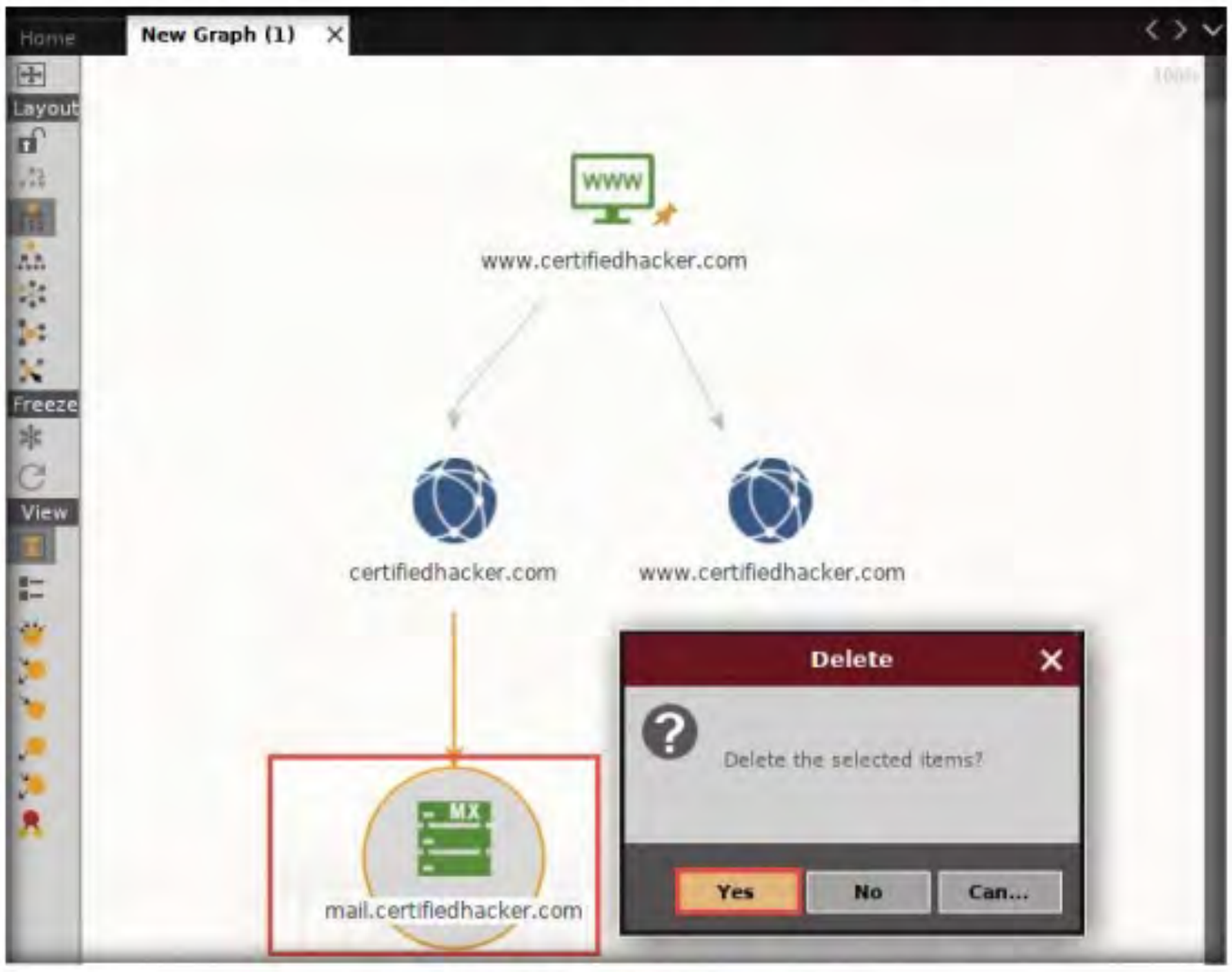


Figure 9.2.30: Deleting the Mail Server Entity

TASK 2.8

Identify the Name Server

39. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - NS (name server)**.

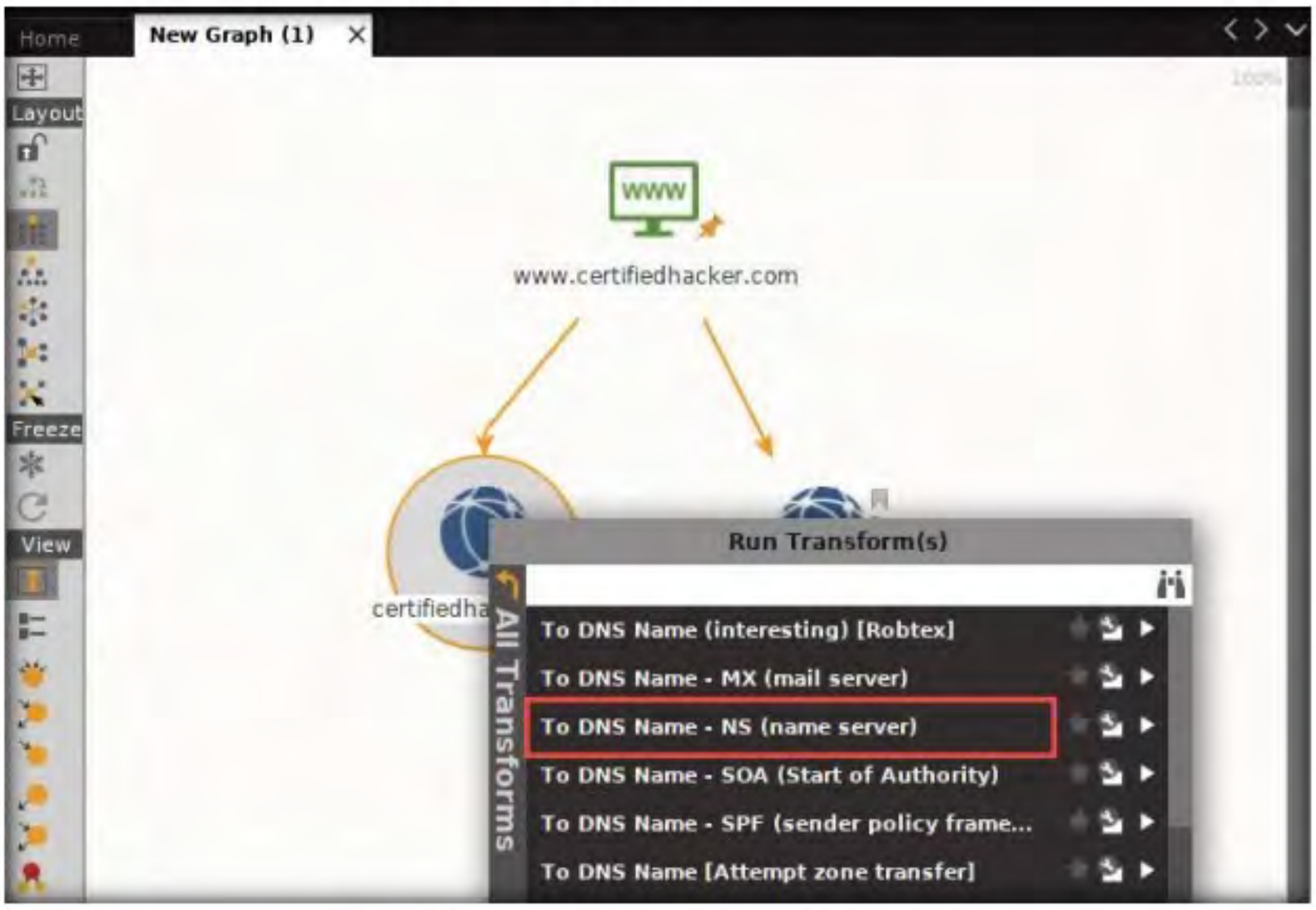


Figure 9.2.31: Selecting To DNS Name - NS (name server)

40. This returns the name servers associated with the domain, as shown in the following screenshot.

Figure 9.2.32: Name Server Associated with the Domain

41. By identifying the primary name server, an attacker can implement various techniques to exploit the server and thereby perform malicious activities such as DNS Hijacking and URL redirection.
42. Select both the domain and the name server by dragging and deleting them.

Figure 9.2.33: Delete Name Server and the Domain

TASK 2.9

Identify the IP Address

43. Right-click the entity and select **All Transforms → To IP Address [DNS]**.

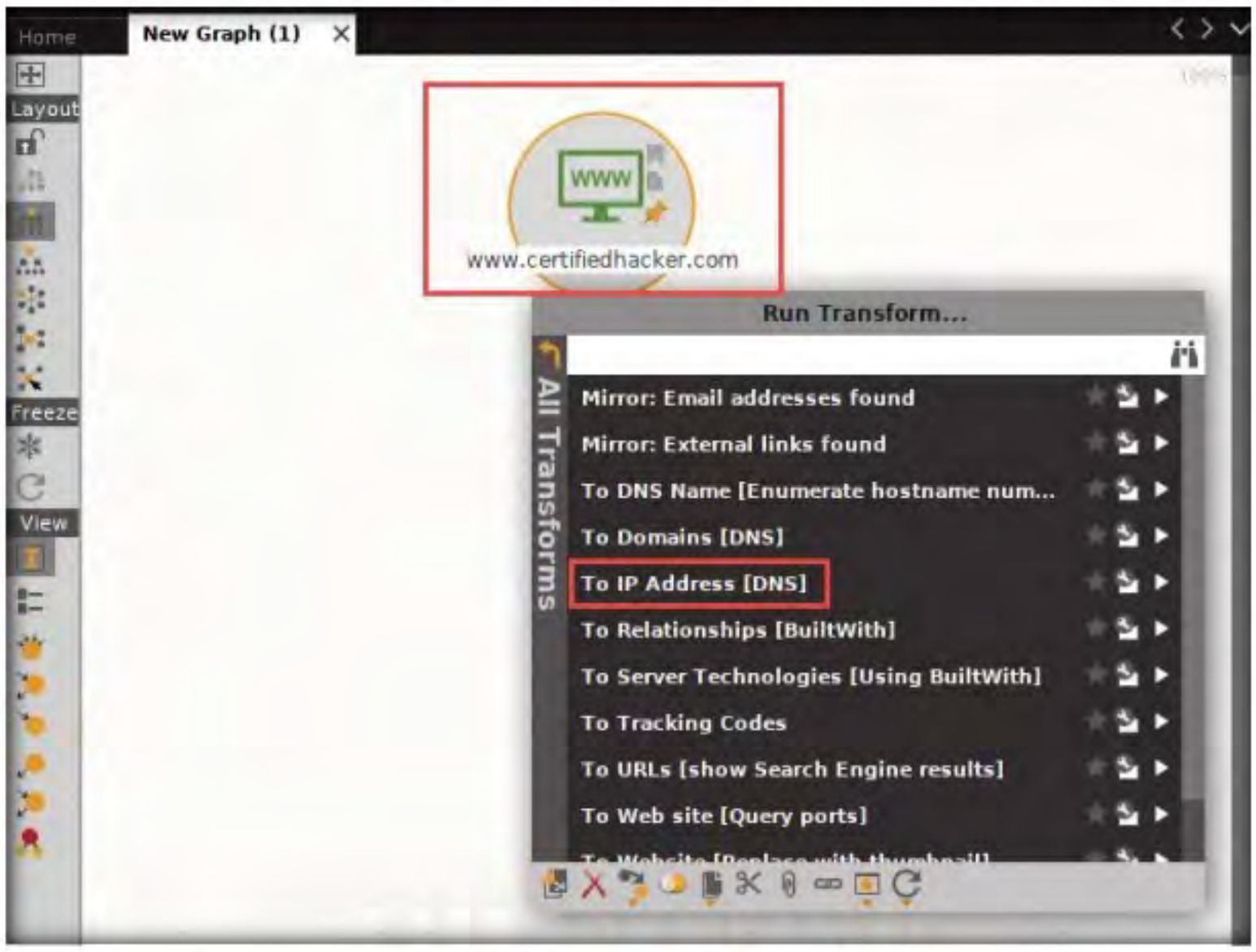


Figure 9.2.34: Selecting To IP Address [DNS]

44. This displays the IP address of the website, as shown in the following screenshot.

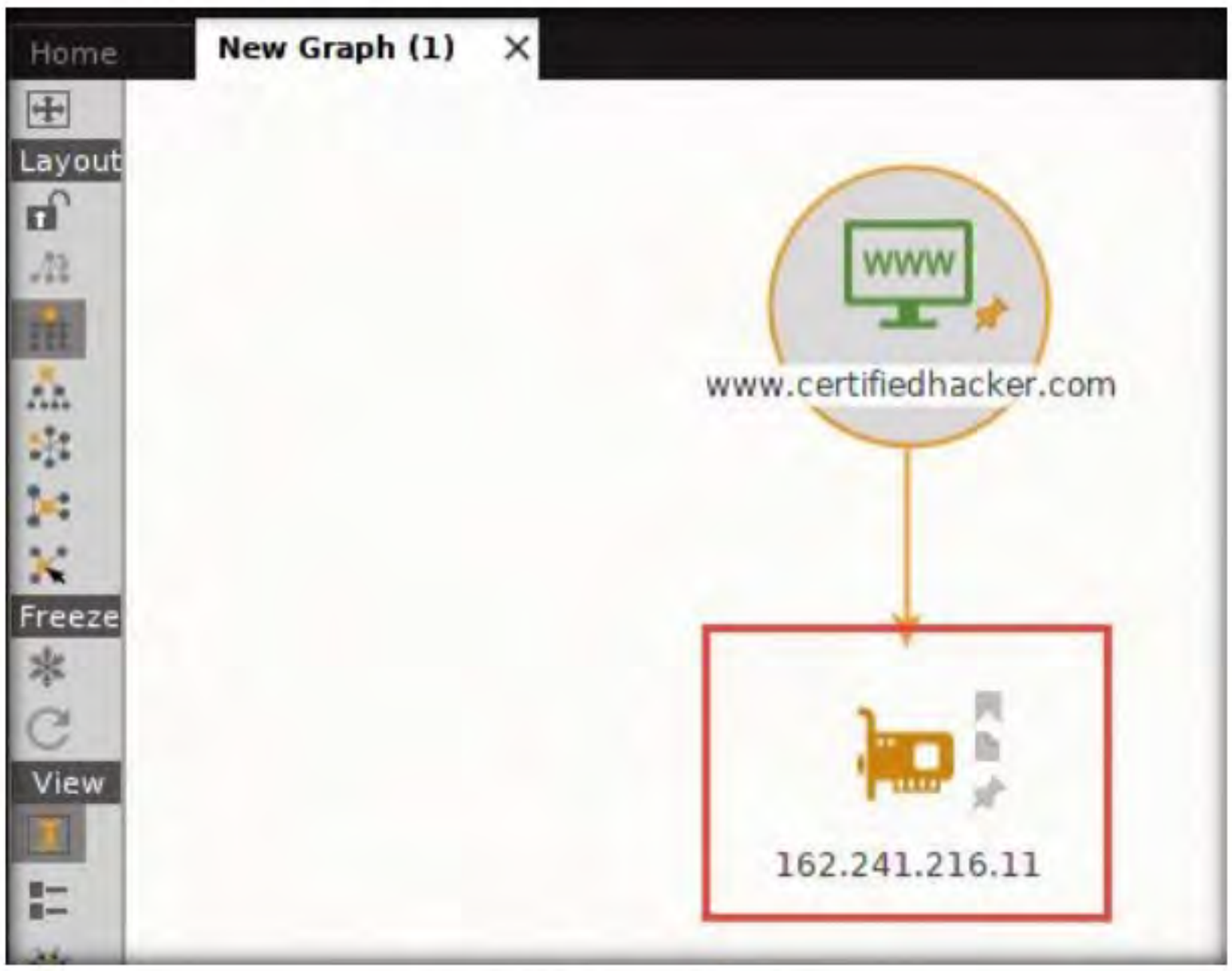


Figure 9.2.35: IP address of the website

45. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

TASK 2.10

Identify the Geographical Location

46. Right-click the IP address entity and select **All Transforms → To location [city, country]**.

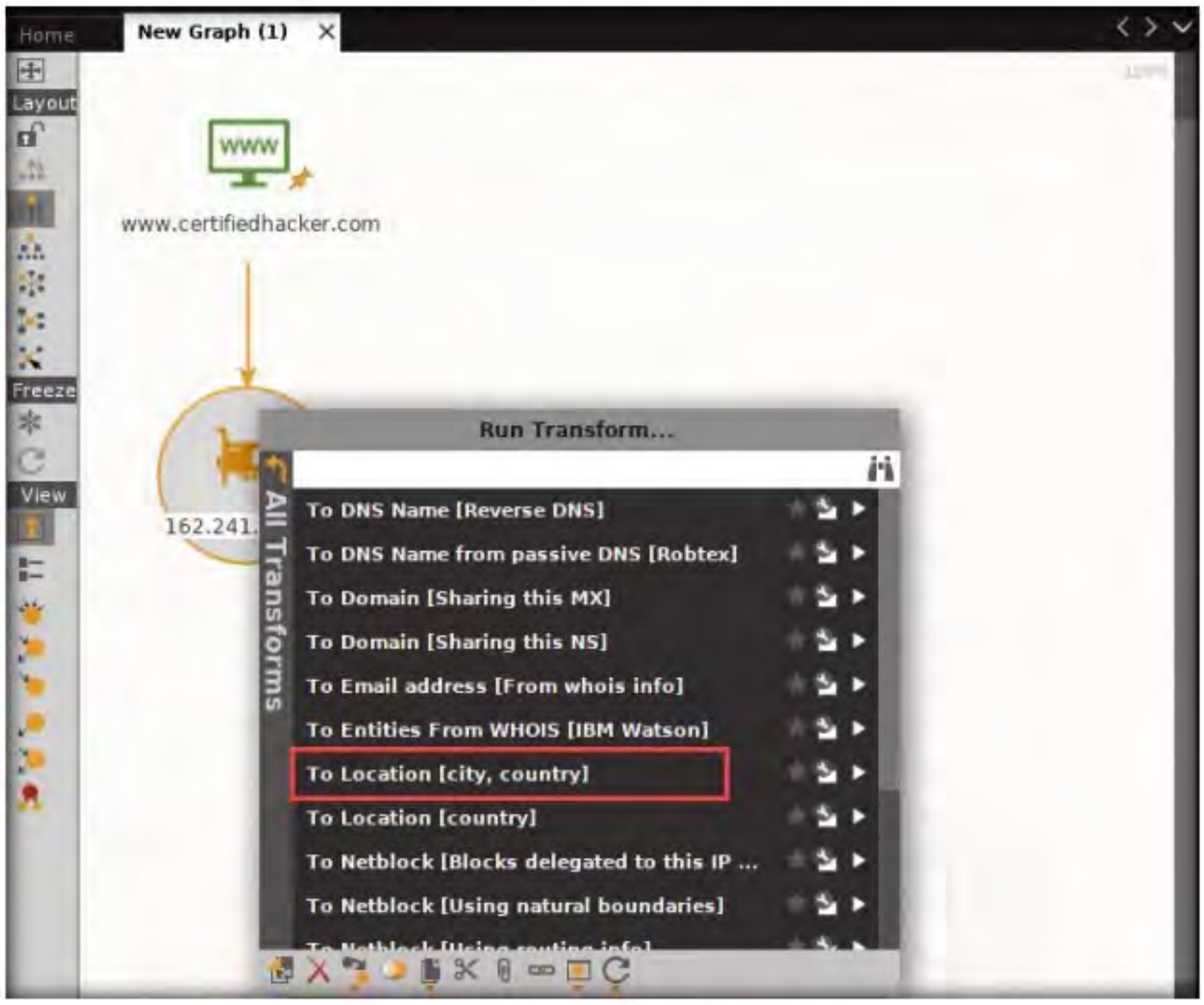


Figure 9.2.36: Selecting To location [city, country]

47. This transform identifies the geographical location of the IP address, as shown in the following screenshot.

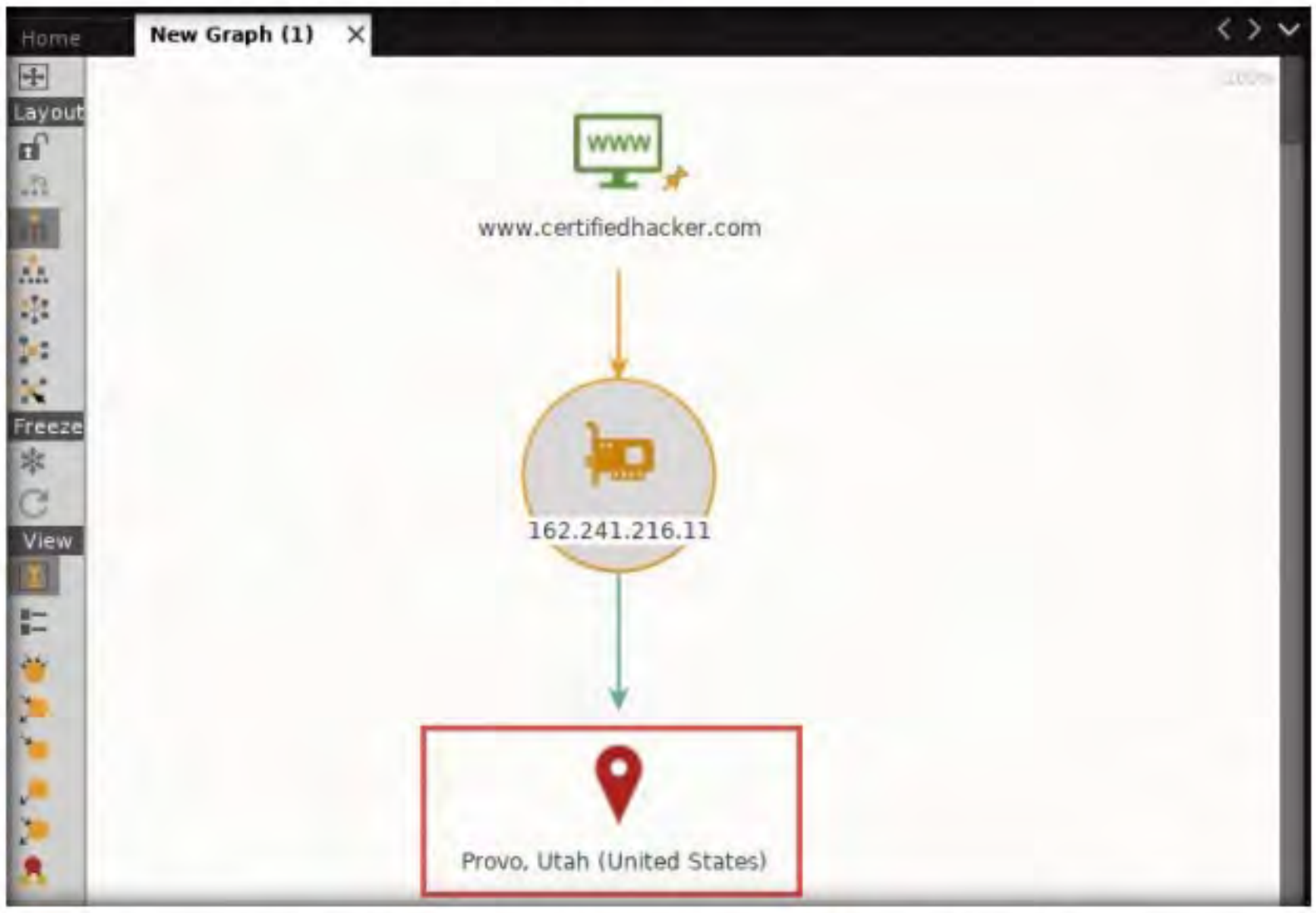


Figure 9.2.37: Geographical Location where the IP Address is Located

48. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

49. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms → To Domains [DNS]**. The domains corresponding to the website display, as shown in the screenshot.

Figure 9.2.38: Domain Name Corresponding to the Website

TASK 2.11

Identify the Entities

50. Right-click the domain entity (**certifiedhacker.com**) and select **All Transform → To Entities from WHOIS [IBM Watson]**.

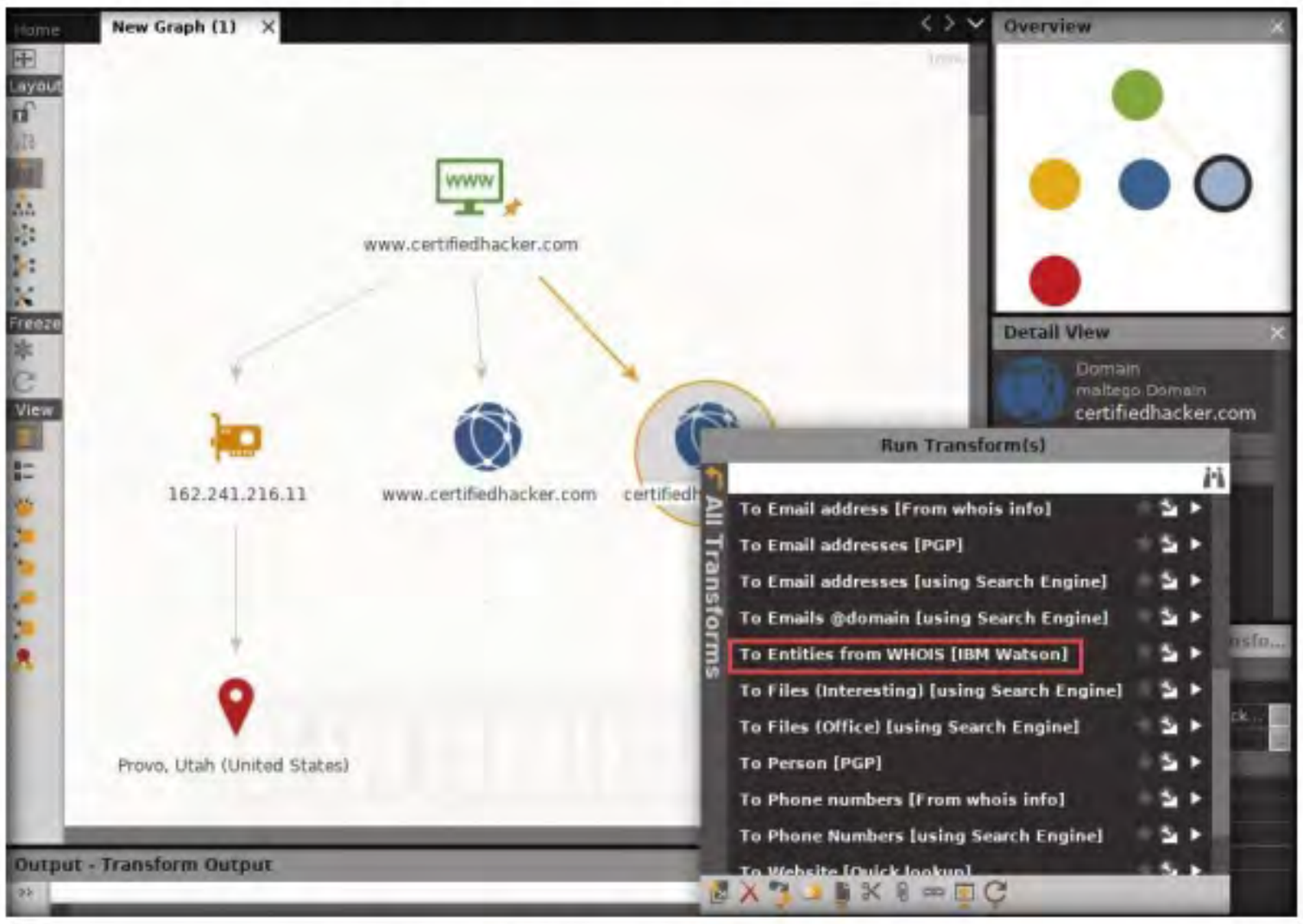


Figure 9.2.39: Selecting To Entities from whois [Alchemy]

51. This transform returns the entities pertaining to the owner of the domain, as shown in the following screenshot.

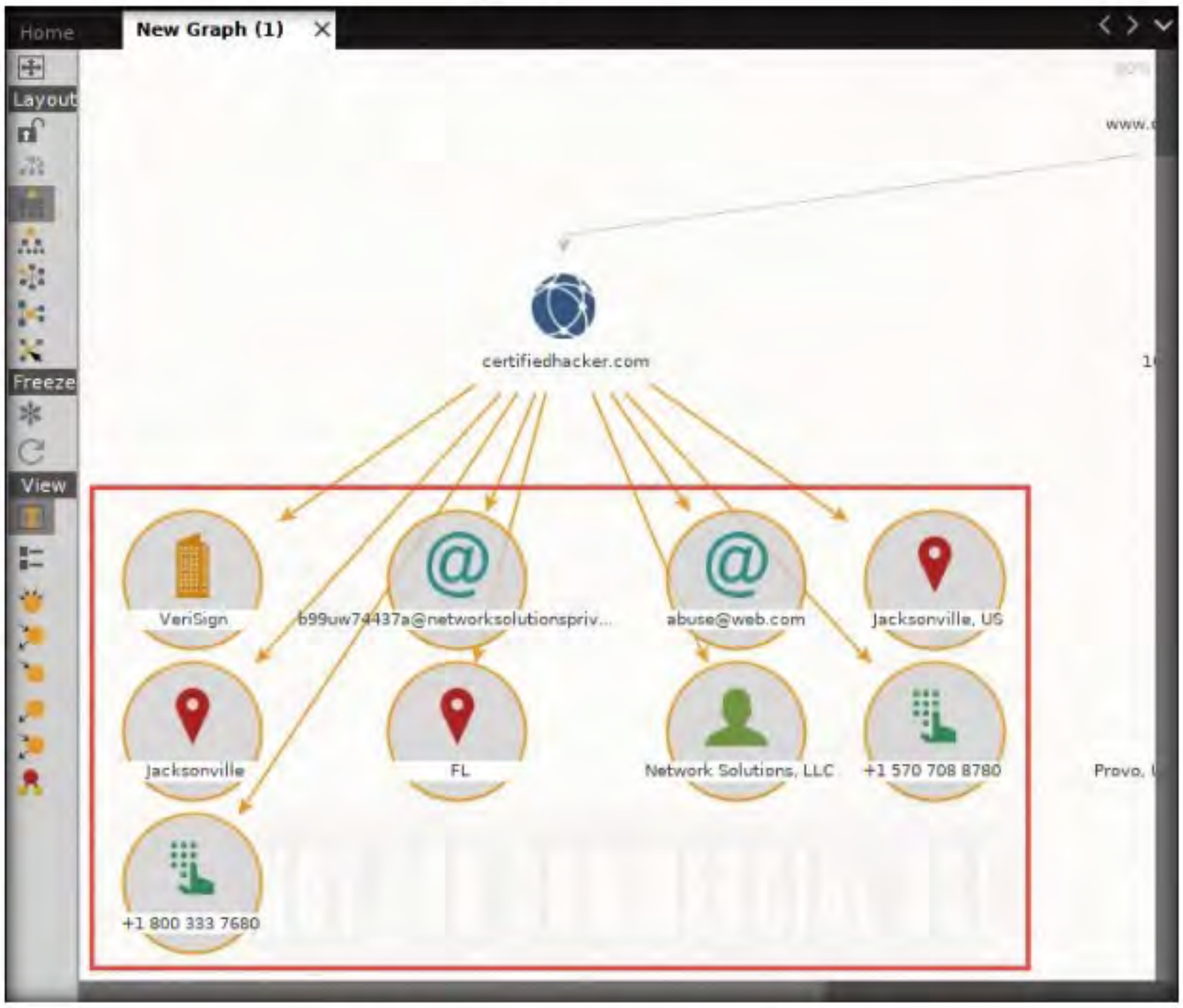


Figure 9.2.40: Entities Pertaining to the Owner of the Domain

52. By obtaining this information, you can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack into the admin mail account and send phishing emails to the contacts in that account.

TASK 2.12
Extract Other Information

53. Apart from the aforementioned methods, you can perform footprinting on the critical employee from the target organization to gather additional personal information such as email addresses, phone numbers, personal information, image, alias, phrase, etc.

54. In the left-pane of the Maltego GUI, click the **Personal** node under **Entity Palette** to observe a list of entities such as **Email Address**, **Phone Numbers**, **Image**, **Alias**, **Phrase**, etc.

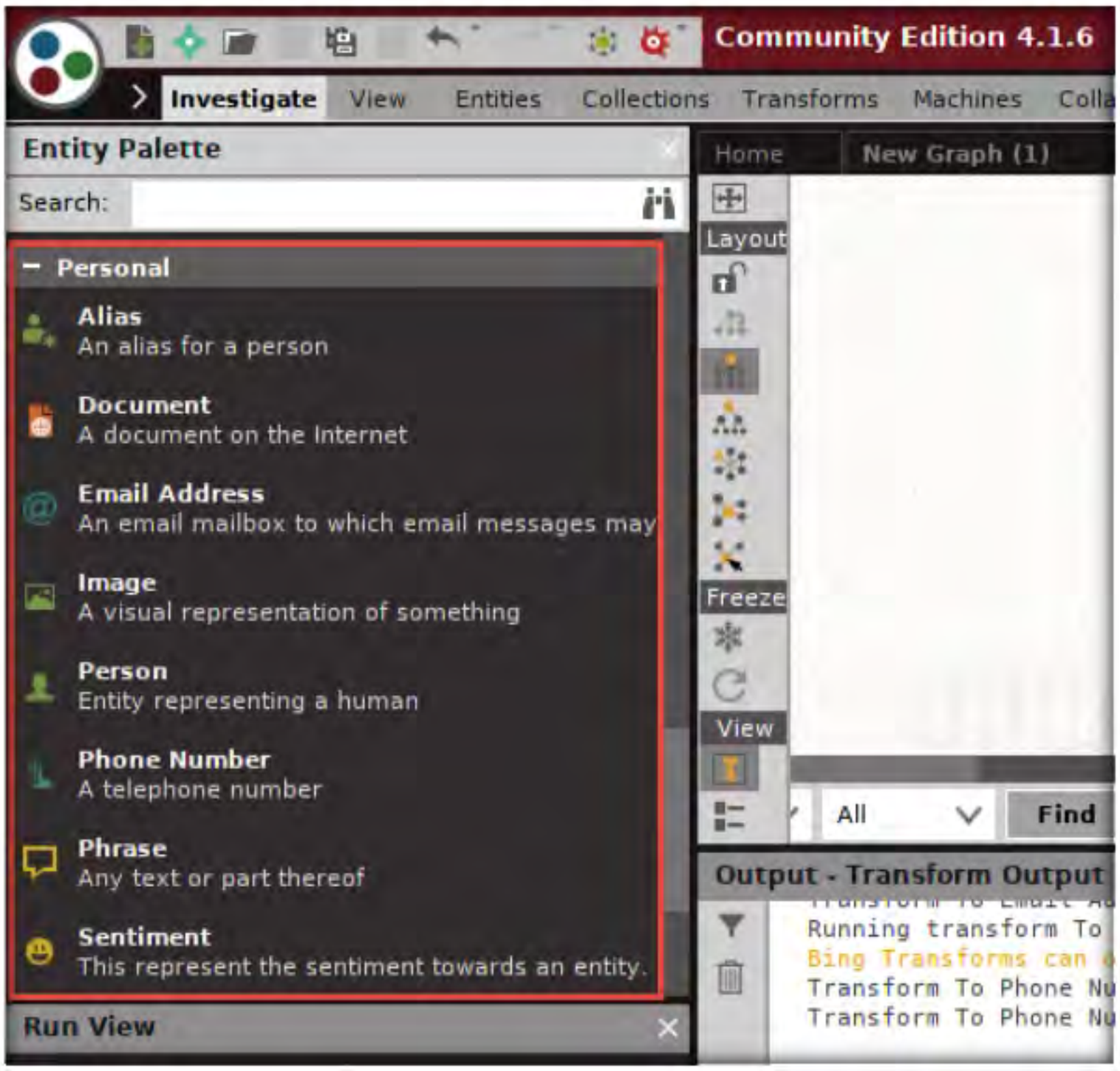


Figure 9.2.41: List of transforms to gather personal information

55. Apart from the transforms mentioned above, other transforms can track accounts and conversations of individuals who are registered on social networking sites such as Twitter. Extract all possible information.
56. By extracting all this information, you can simulate actions such as enumeration, web application hacking, social engineering, etc., which may allow you access to a system or network, gain credentials, etc.
57. This concludes the demonstration of footprinting a target using Maltego.
58. Close all open windows and document all the acquired information.

TASK 3 Footprinting a Target using OSRFramework

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Parrot Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 3.1

Install OSRFramework

5. In the **Parrot Terminal** window, type **git clone https://github.com/i3visio/osrframework** and press **Enter**.

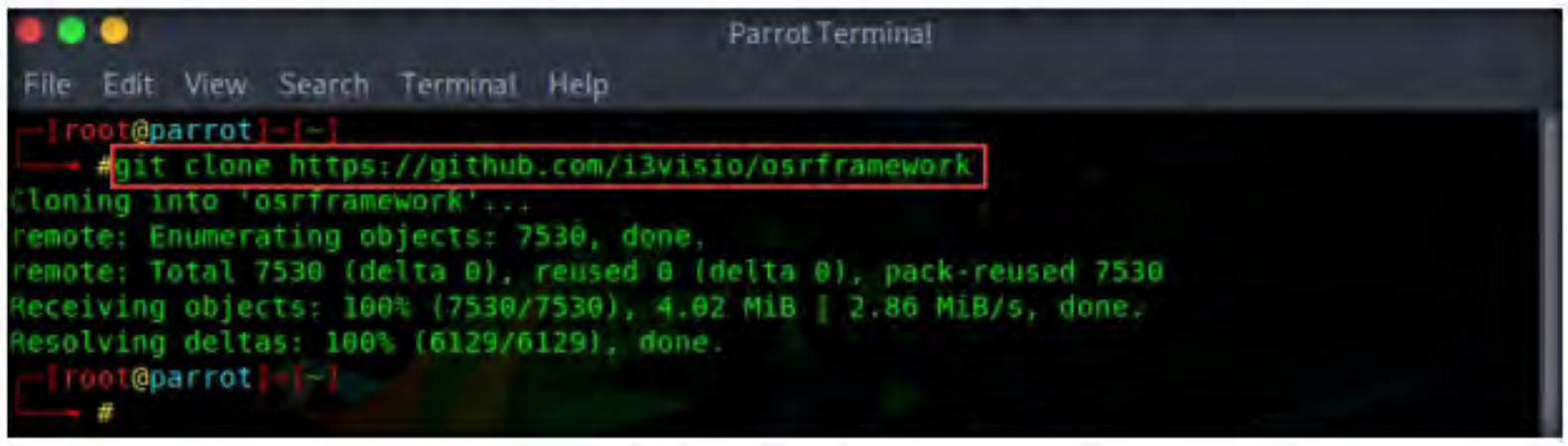


Figure 9.3.1: Cloning OSRFramework tool

OSRFramework is a set of libraries that are used to perform Open Source Intelligence tasks. They include references to many different applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, and many others. It also provides a way of making these queries graphically as well as several interfaces to interact with such as OSRFConsole or a Web interface.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **osrframework** folder.
- Paste the copied **osrframework** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/osrframework /root/**.

6. Type **pip3 install osrframework** and press **Enter** to install the OSRFramework.

Note: If **osrframework** is already installed, skip to **Step #8**.

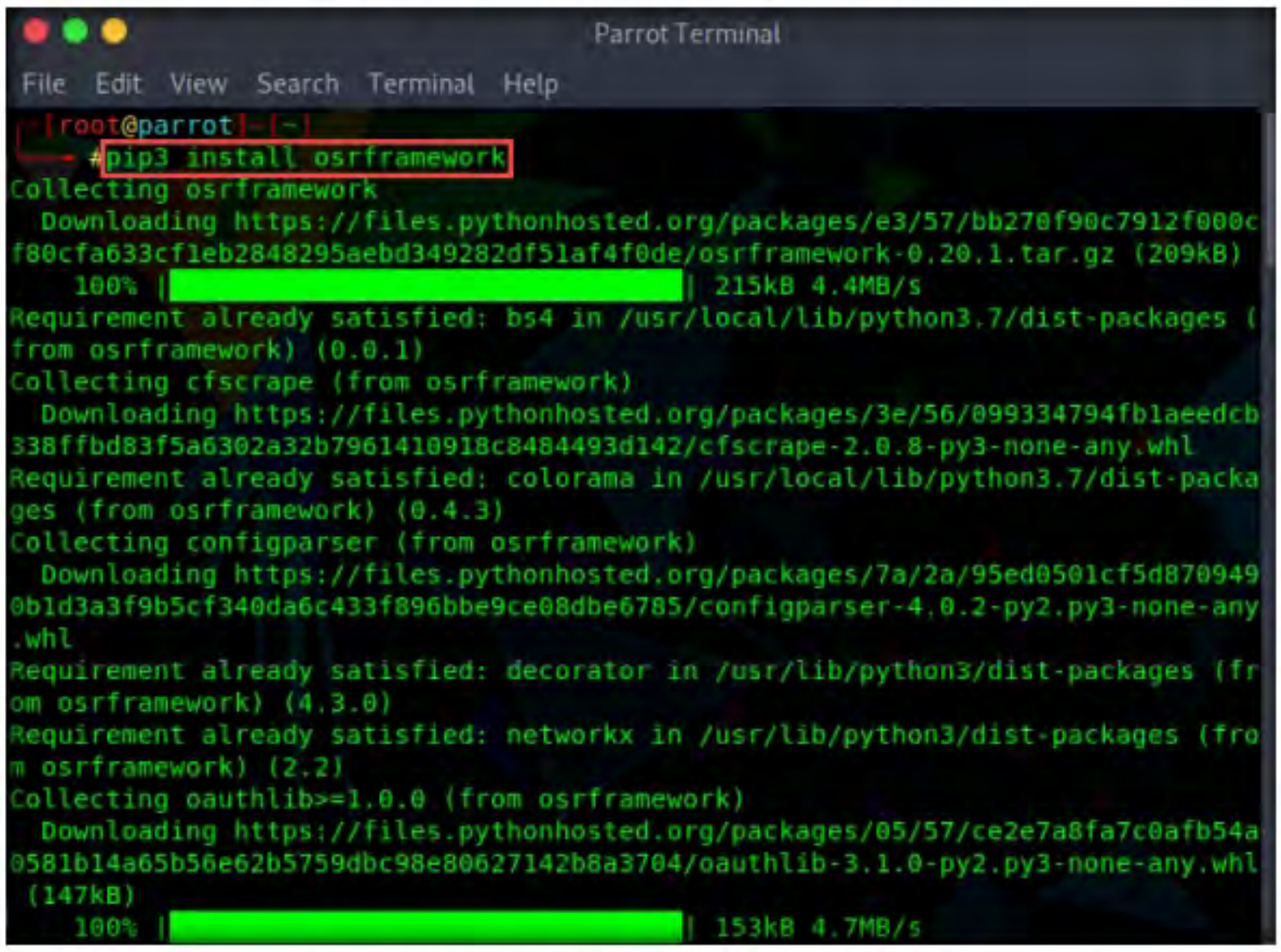


Figure 9.3.2: Installing OSRFramework through command line

7. To upgrade the OSRFramework to its latest version, type **pip3 install osrframework --upgrade** and press **Enter**. If the tool is not updated, the updates will start installing, as shown in the screenshot.

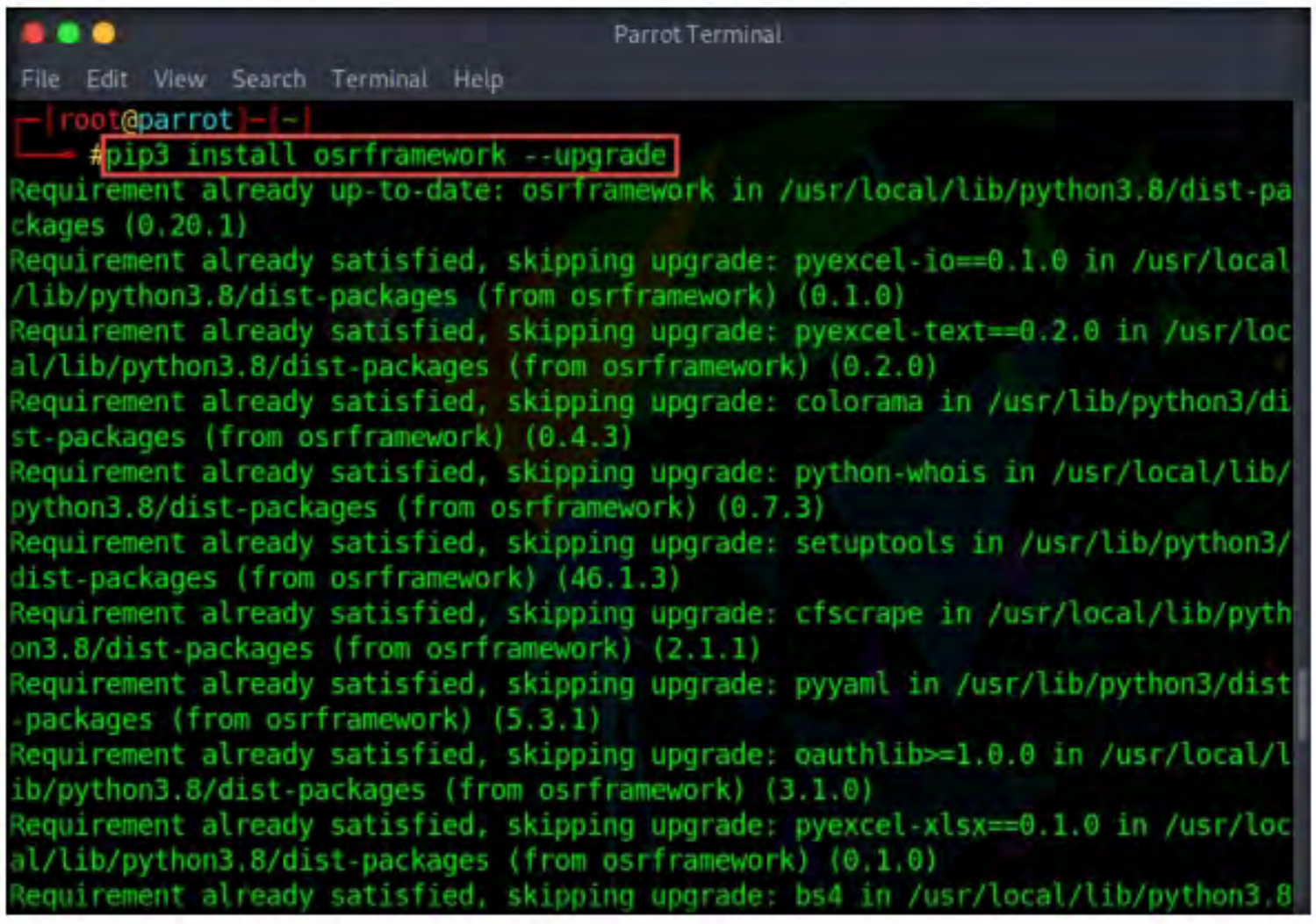


Figure 9.3.3: Upgrading OSRFramework

TASK 3.2

Check the Target User Profile on Social Networking Platforms

8. Use **usufy.py** to check for the existence of a profile for given user details on different social networking platforms. Type **usufy.py -n <target user name or profile name> -p <target platform>** (here, the target user name or profile is **Mark Zuckerberg** and the target platforms are **twitter**, **facebook**, and **youtube**) and press **Enter**.

Note: -n is the list of nicknames to process and **-p** is for the platform for search.

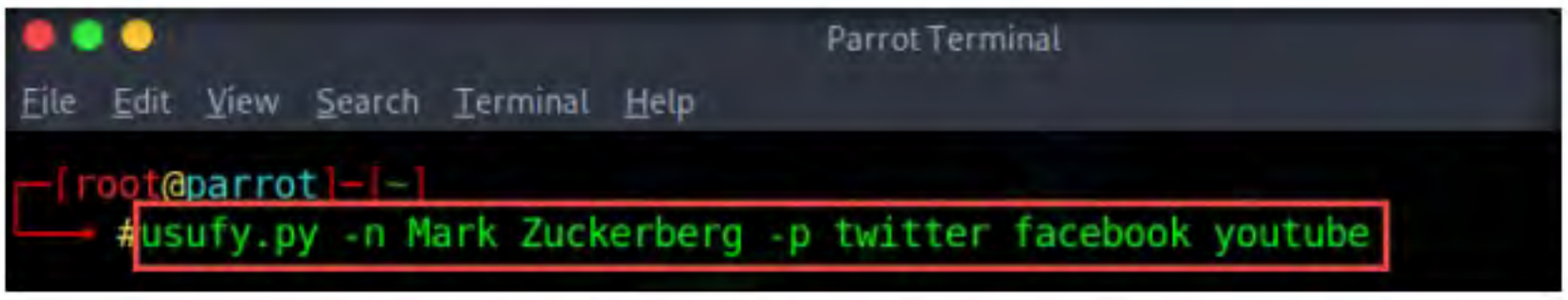


Figure 9.3.4: Using usufy.py to search twitter, facebook, and youtube for users

9. The usufy.py will search the user details in the mentioned platforms and will provide you with the existence of the user, as shown in the screenshot.

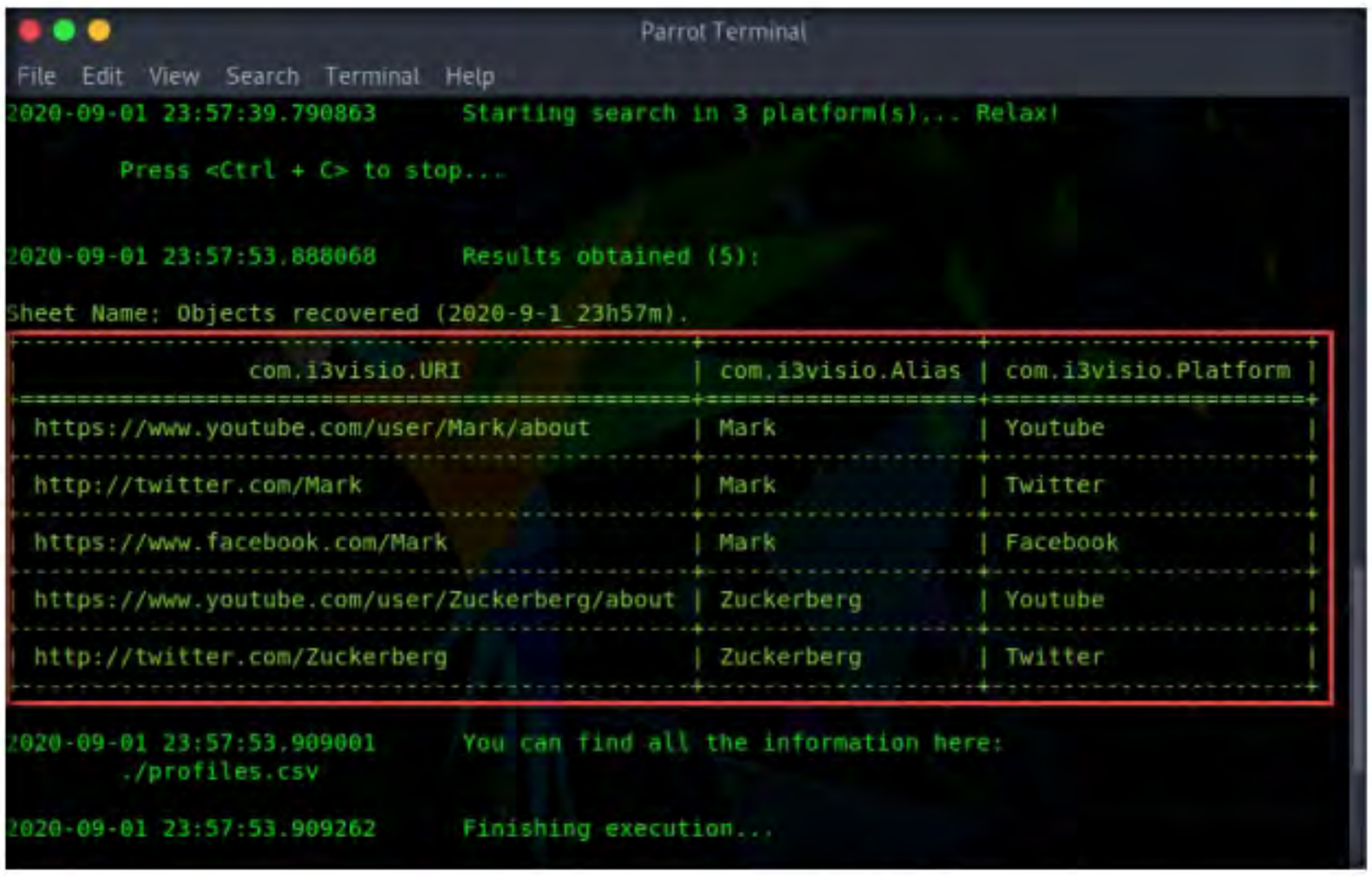


Figure 9.3.5: usufy.py showing a summary of the results obtained through search

TASK 3.3

Check the Pages of a Target on Social Networking Platforms

10. Use **domainfy.py** to check with the existing domains using words and nicknames. Type **domainfy.py -n [Domain Name] -t all** (here, the target domain name is **eccouncil**) and press **Enter**.

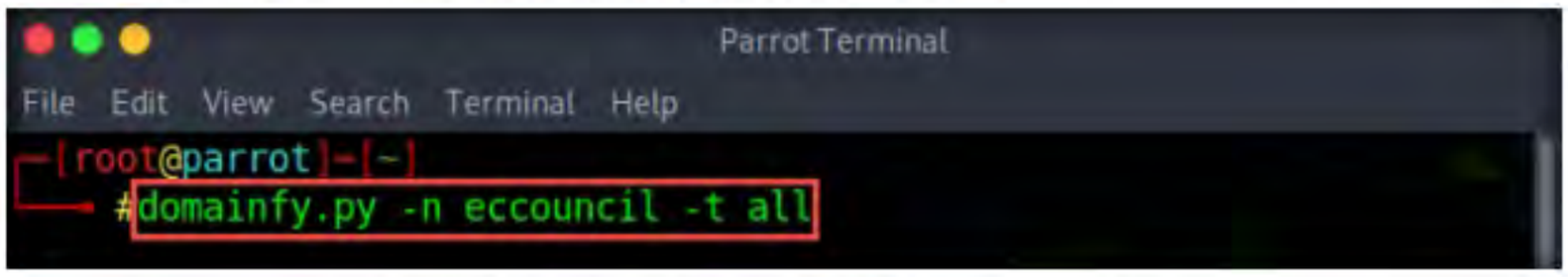


Figure 9.3.6: using searchfy.py with ECCOUNCIL as a target page

11. The tool will retrieve all the domains related to the target domain.

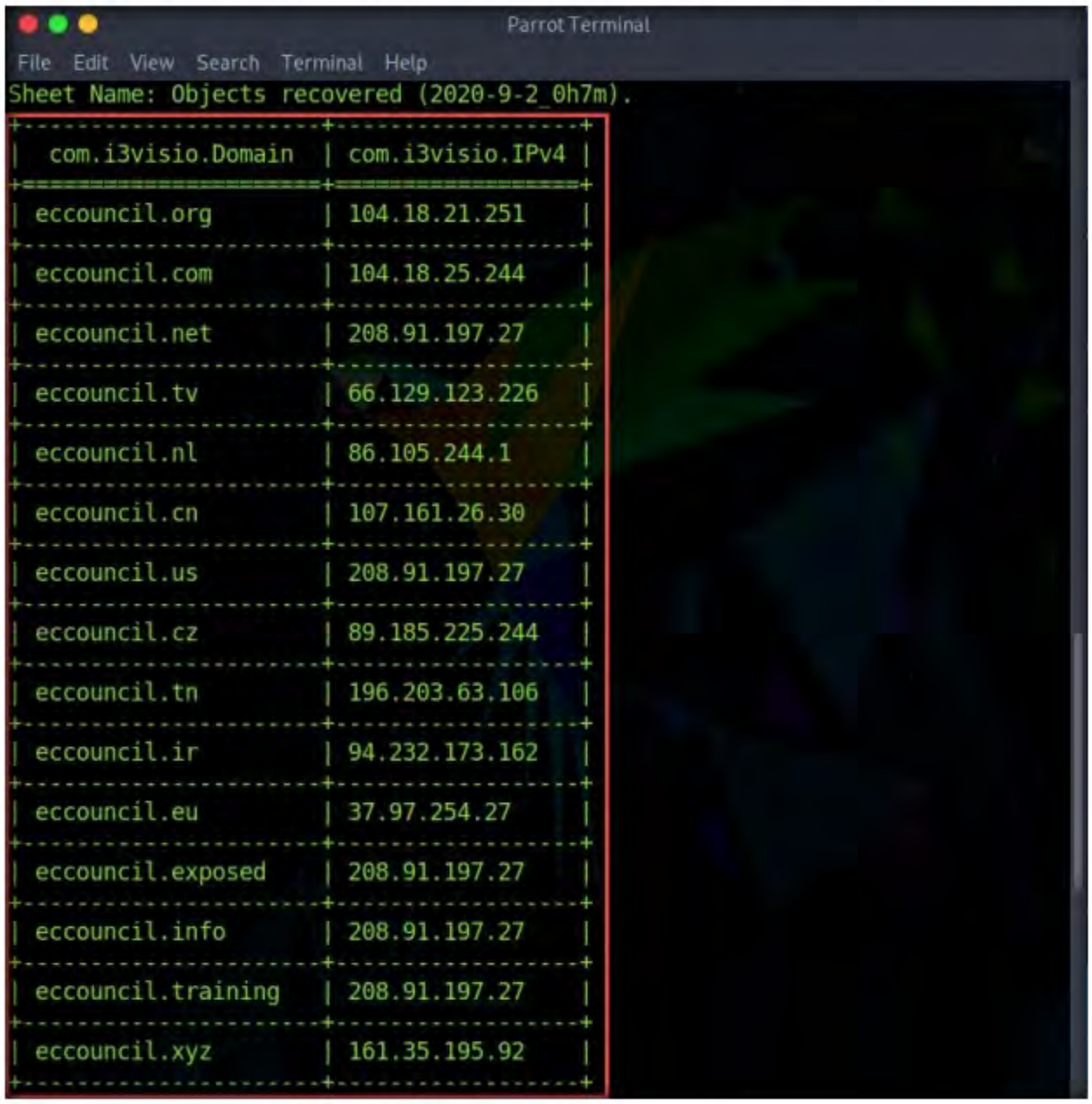


Figure 9.3.7: List of users on targeted social webpages

12. Similarly, you can use following OSRFramework packages to gather information about the target.
    - **searchfy.py** – Gathers information about the users on social networking pages
    - **mailfy.py** – Gathers information about email accounts
    - **phonefy.py** – Checks for the existence of a given series of phones
    - **entify.py** – Extracts entities using regular expressions from provided URLs
13. This concludes the demonstration of gathering information about the target user aliases from multiple social media platforms using OSRFramework.
14. Close all open windows and document all the acquired information.
15. Turn off the **Parrot Security** virtual machine.

TASK 4 Footprinting a Target using FOCA

1. Turn on the **Windows 10** virtual machine.

TASK 4.1

Launch FOCA

2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. To launch **FOCA**, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA\bin** and double-click **FOCA.exe**.
4. The **FOCA** main window appears, as shown in the screenshot.

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and shrouded data. It examines a wide mixture of records, with the most widely recognized being Microsoft Office, Open Office, or PDF documents. It may also work with Adobe InDesign or SVG files. These archives may be on-site pages and can be downloaded and dissected with FOCA.

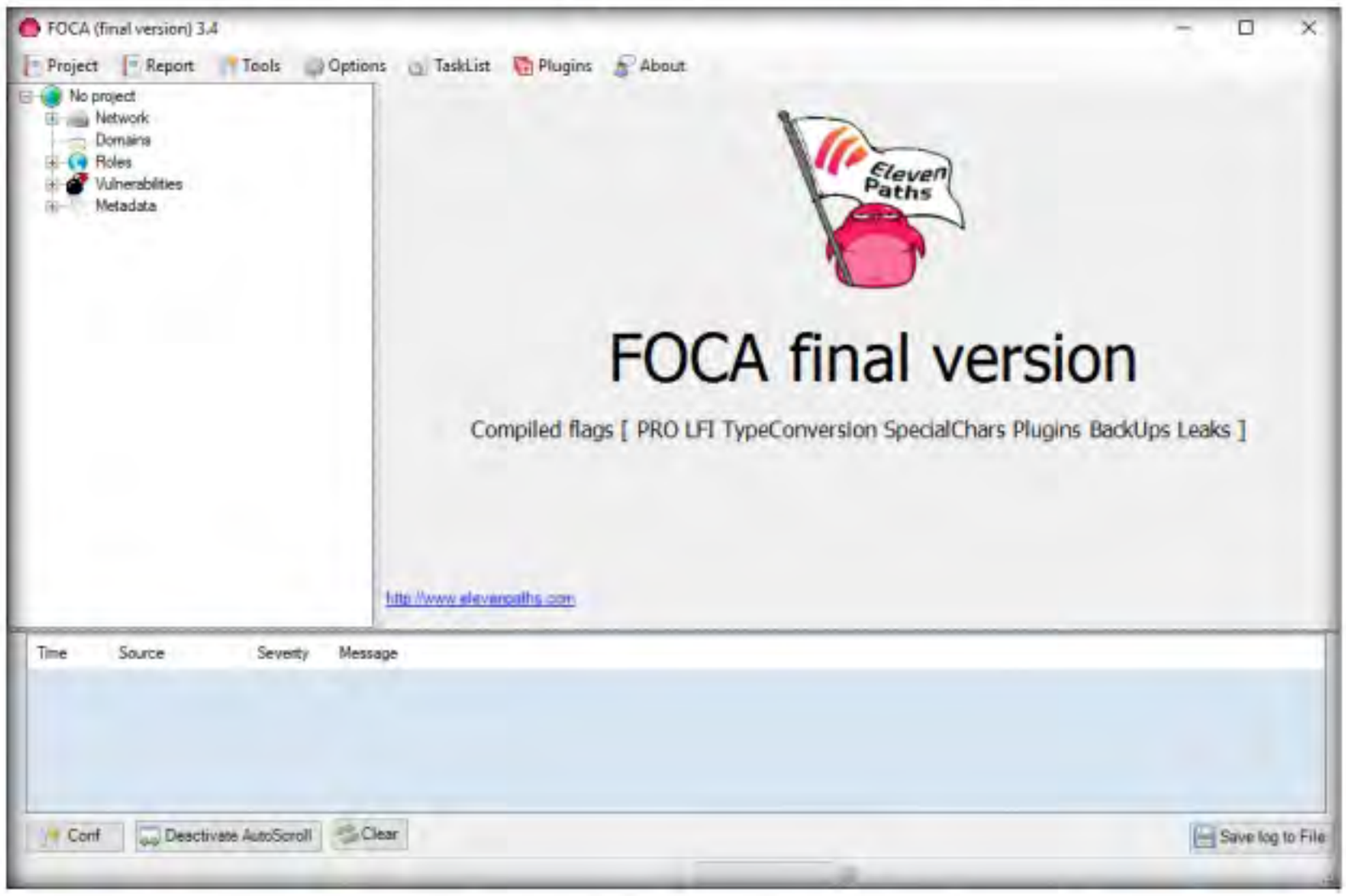


Figure 9.4.1: FOCA main window

TASK 4.2

Create a New Project

5. Create a new project by navigating to **Project** and click **New project** on the menu bar.

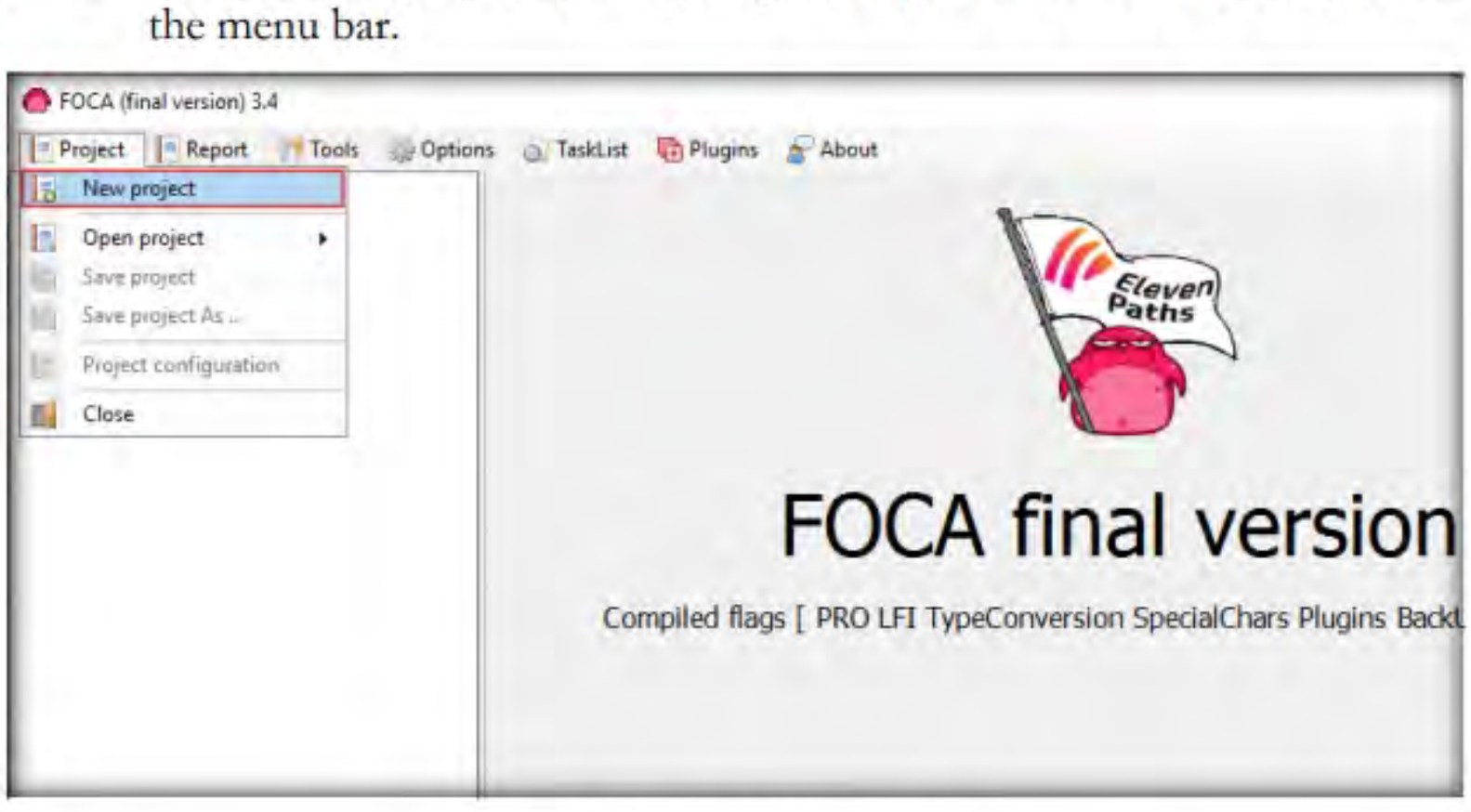


Figure 9.4.2: FOCA creating a new project

6. The **FOCA** new project wizard appears:
   a. Enter a project name in the **Project name** field (here, **Project of www.eccouncil.org**).
   b. Enter the domain website in the **Domain website** field (here, **www.eccouncil.org**).
   c. You can leave the optional **Alternative domains** field empty.
   d. Under the **Folder where save documents** field, click on the **Folder** icon. When the **Browse For Folder** pop up window appears, select the location to save the document that is extracted by FOCA (here, **Desktop**) and click **OK**.
   e. Leave the other settings to default and click the **Create** button.

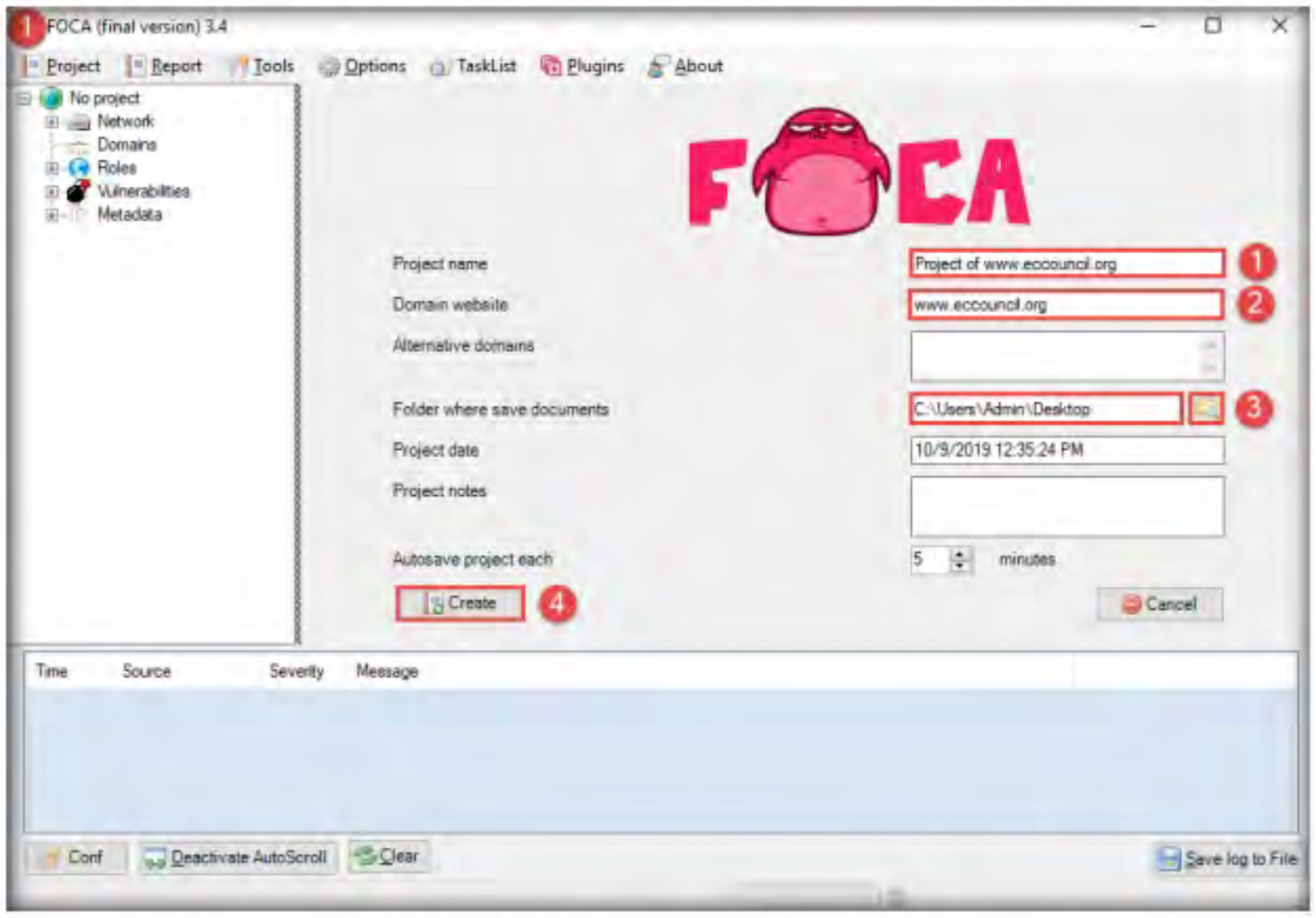


Figure 9.4.3: FOCA providing details for a new project

7. The **Save project as ...** window appears. Provide the desired location (here, **Desktop**) to save the FOCA project and type a file name in the **File name** field and click **Save**.

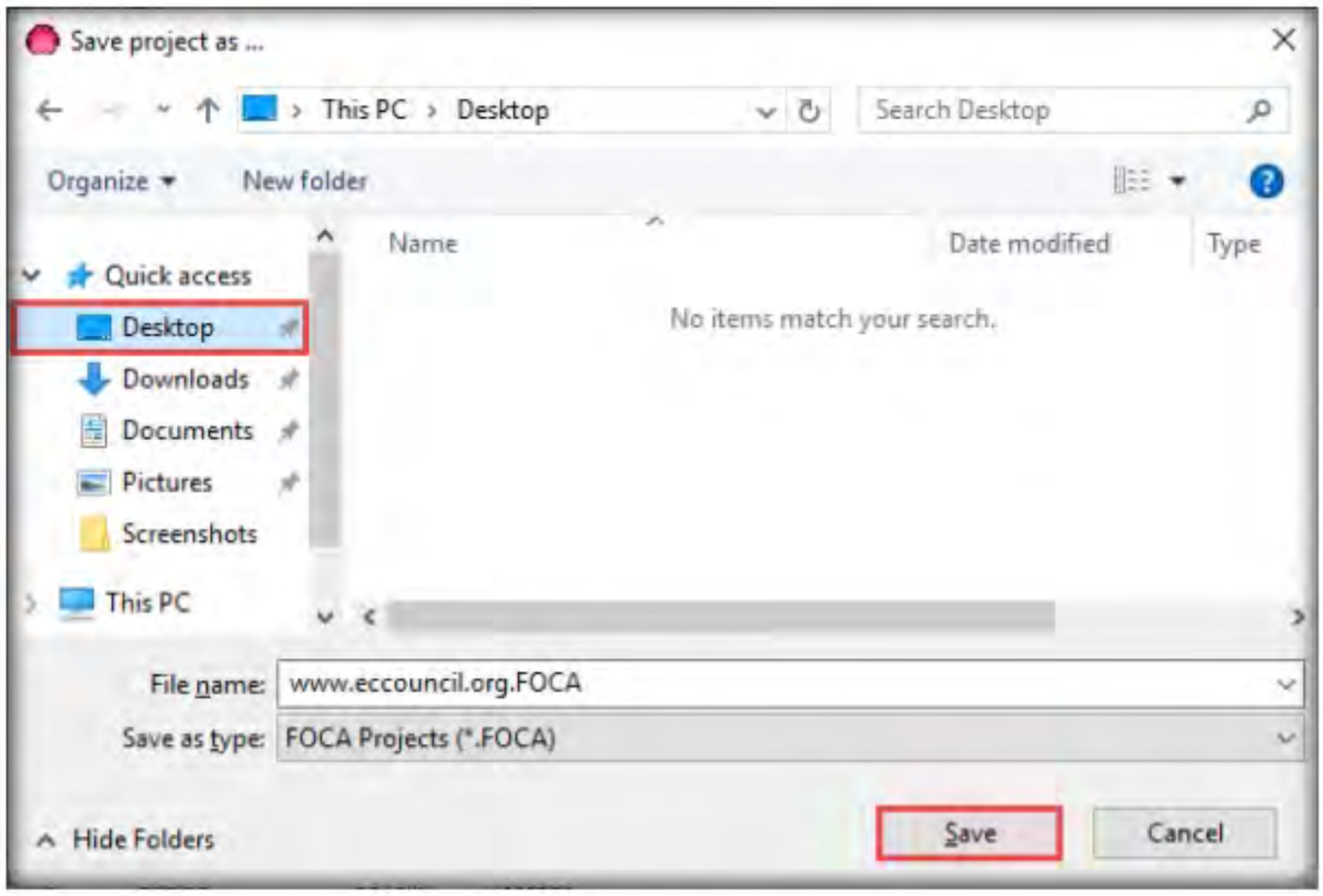


Figure 9.4.4: FOCA Save project as window

8. The **Project saved successfully!** pop-up window appears; click **OK**.

Figure 9.4.5: FOCA Project Saved

TASK 4.3

Extract Metadata of a Target Domain

9. To extract the information of the targeted domain, select all three search engines (**Google**, **Bing**, and **Exalead**) present under **Search engines**, and then click the **Search All** button.

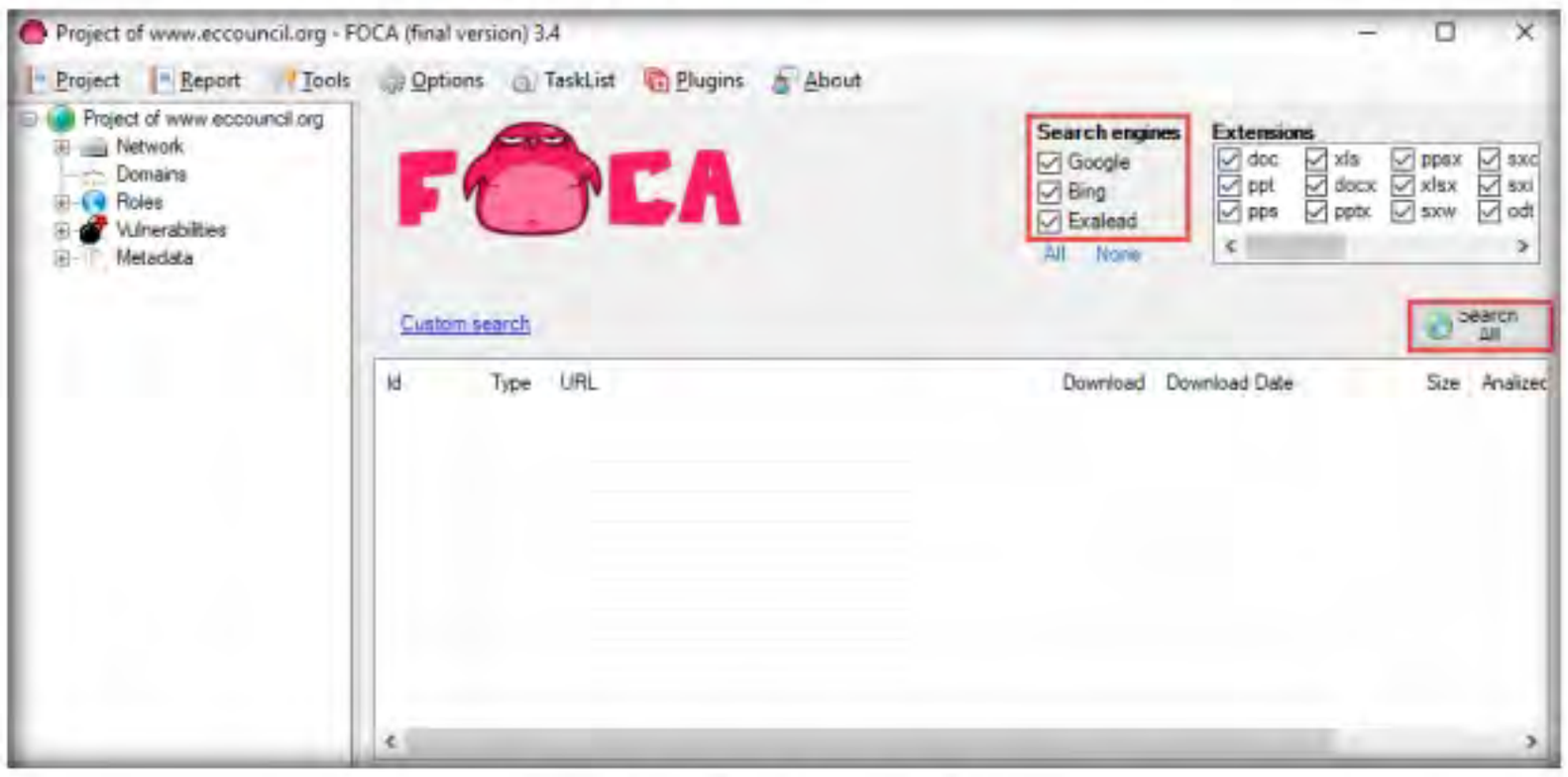


Figure 9.4.6: FOCA selecting Search engines

10. The **Search All** button automatically toggles the **Stop** button, and you can see the result in the lower panes.

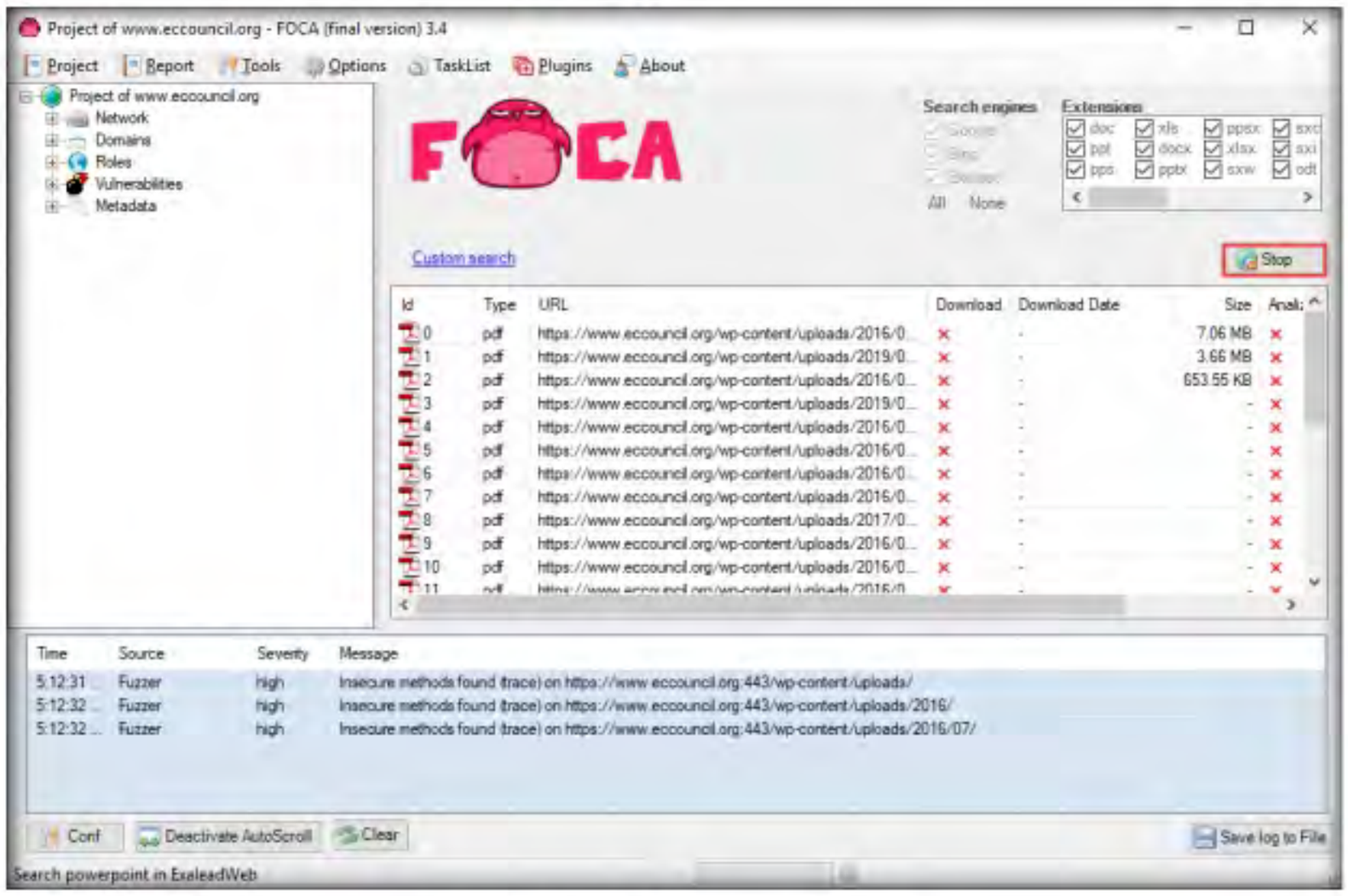


Figure 9.4.7: FOCA Extracted Information

11. After the scans complete, the **Stop** button automatically toggles back to the **Search All** button. The gathered result on the **Metadata** associated with the target domain appears, as shown in the screenshot.

Note: The gathered result includes various sub-domains associated with the target domains consisting of metafiles.

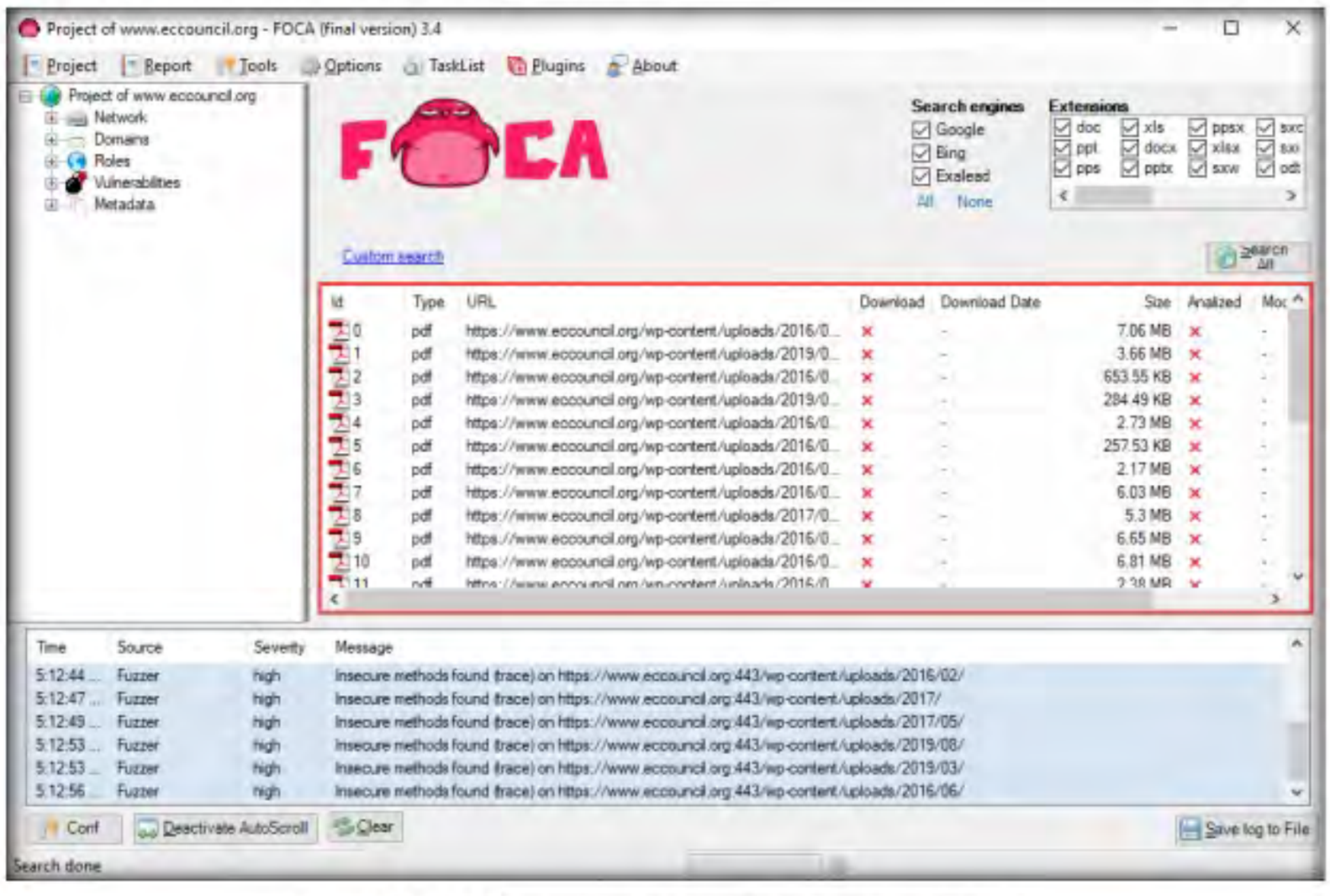


Figure 9.4.8: FOCA examining the extracted information of the file

12. To view the file information stored in the sub-domain, right-click on any URL and click **Link → Open in browser** from the context menu.

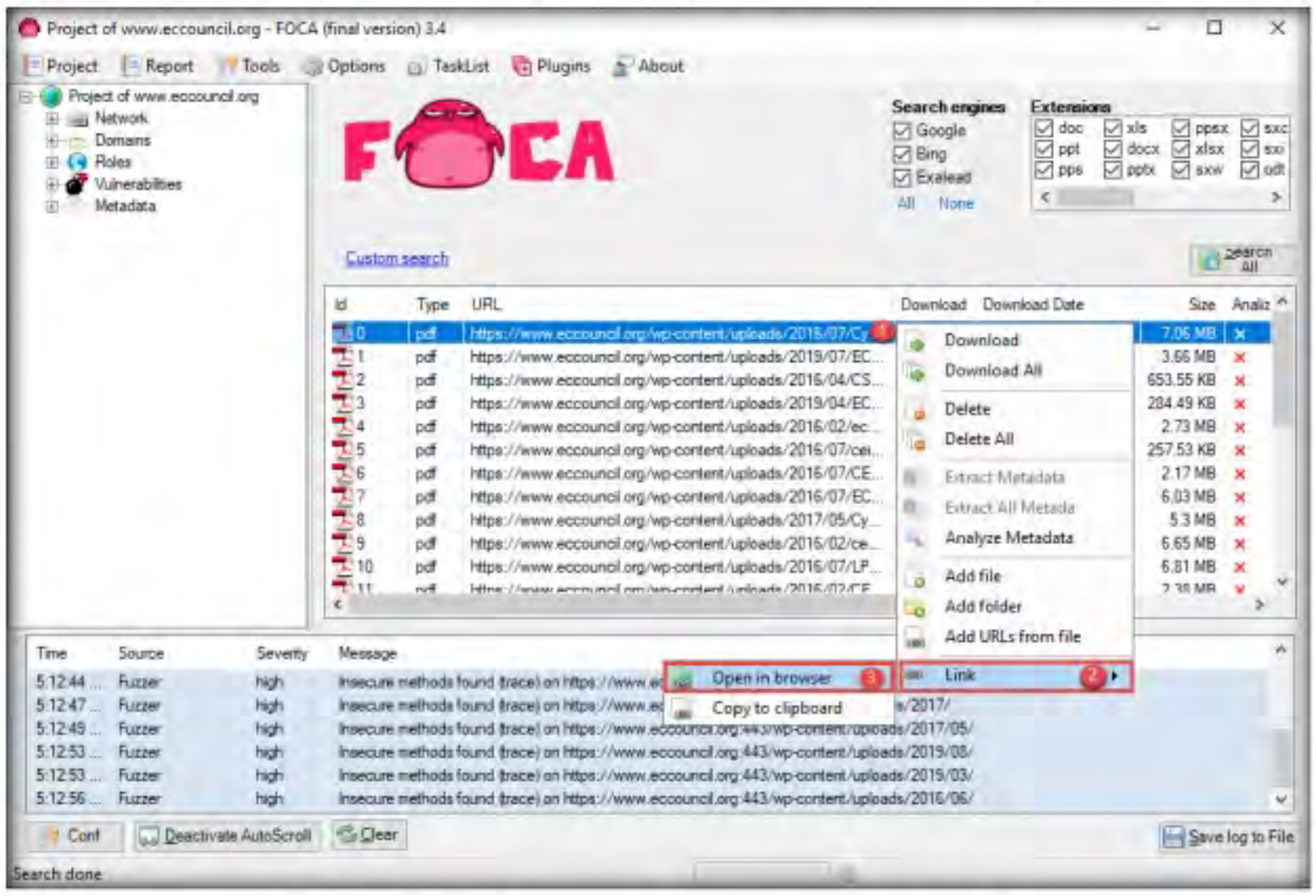


Figure 9.4.9: FOCA examining the extracted information of the file

13. If a **How do you want to open this?** pop up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

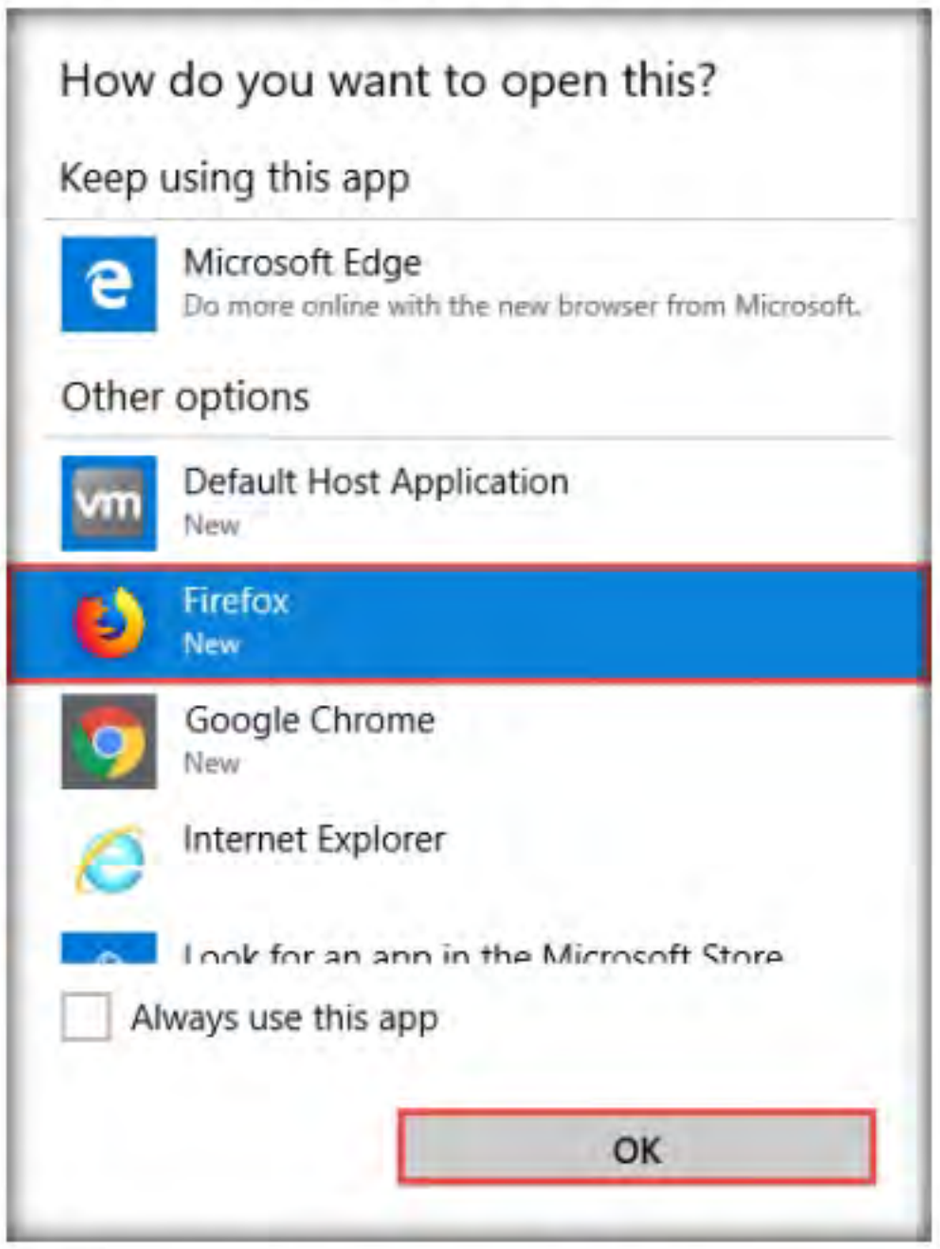


Figure 9.4.10: Selecting Mozilla Firefox

14. The extracted file from the domain by using **FOCA** appears on the web browser, as shown in the screenshot.

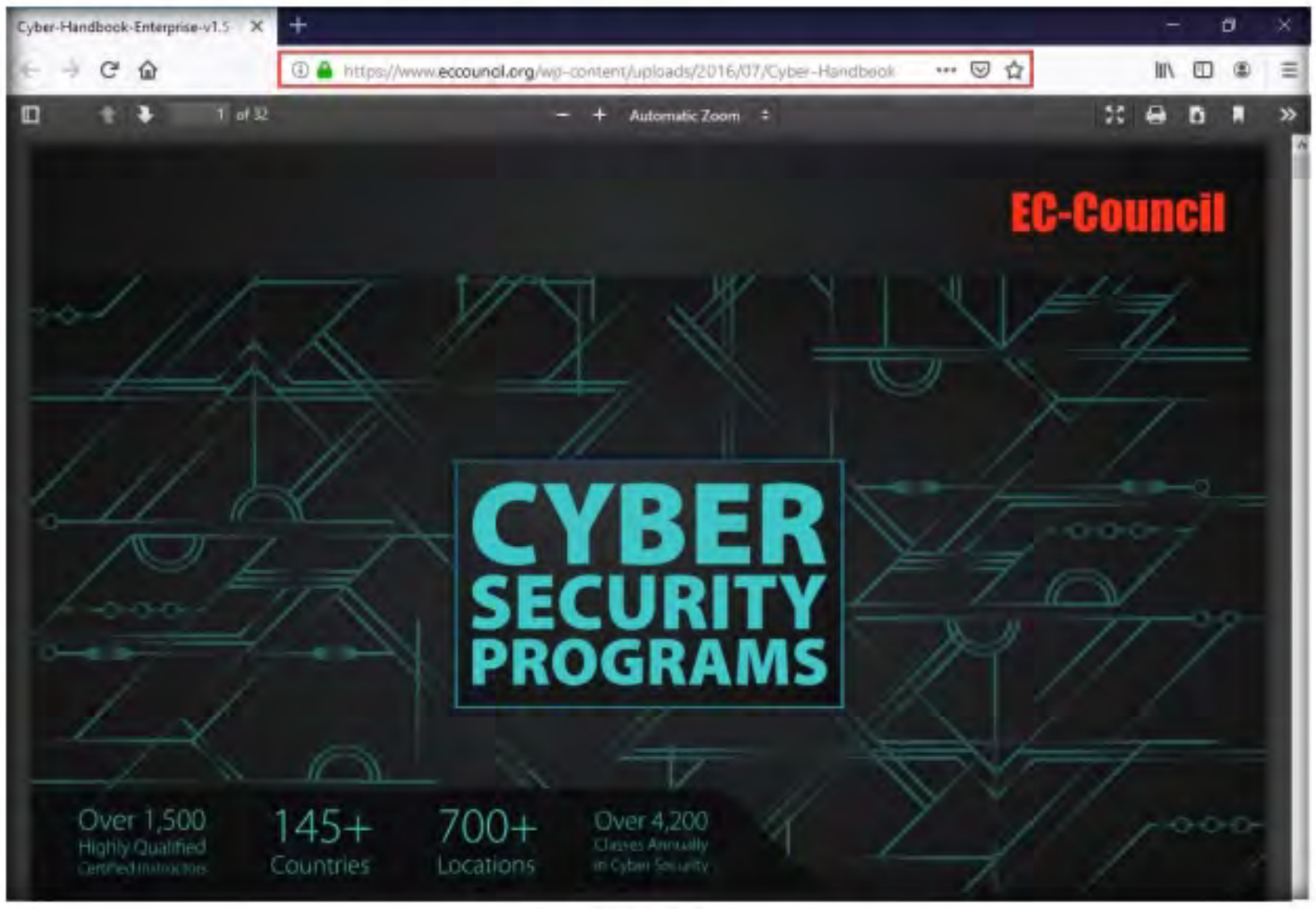


Figure 9.4.11: FOCA Extracted file

TASK 4.4

Extract Network Structure Information

15. Close the web browser.
16. Navigate back to the FOCA window and click the **Network** node to expand the node in the left pane of the window to view the network structure.

17. If the domain has any of the associated **Clients** or **Servers**, it displays the related information.

Note: In this lab, the domain we used does not have associated clients or servers.

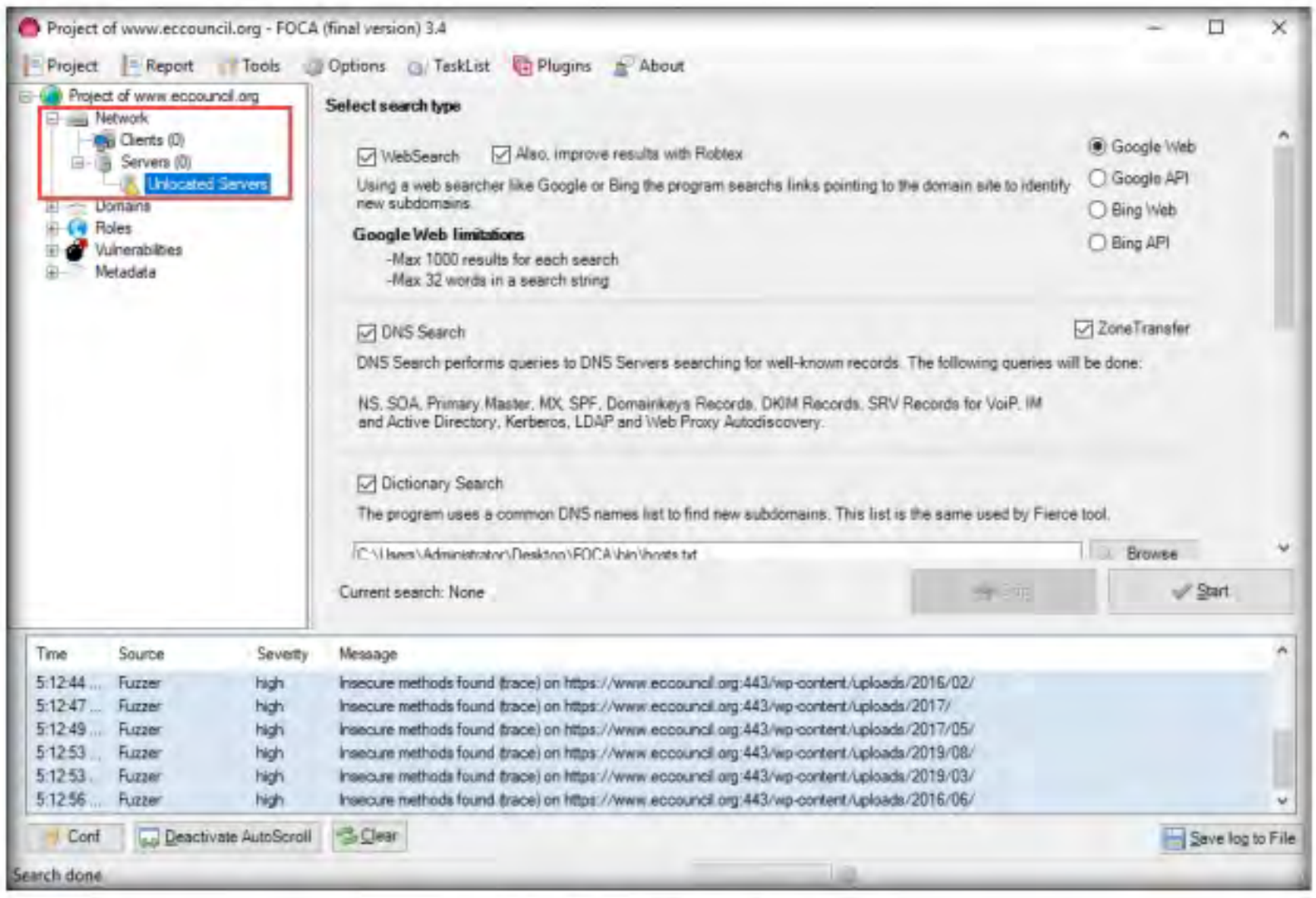


Figure 9.4.12: FOCA Network Information

TASK 4.5

Extract Domain Information

18. Expand the **Domains** node and click on the target domain (here, **eccouncil.org**) to view the domain-related information.

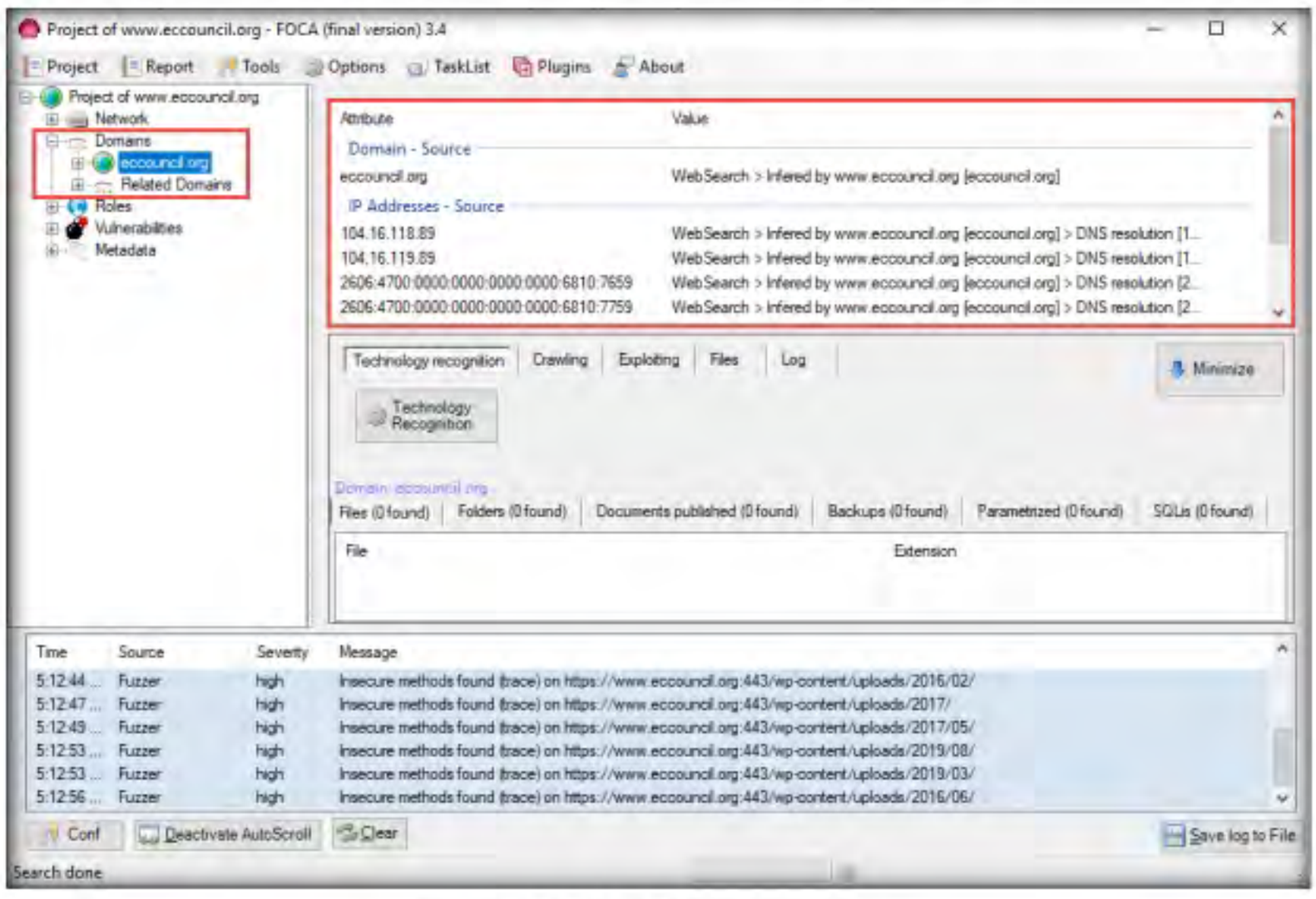


Figure 9.4.13: FOCA Domain Information

TASK 4.6

Extract Https Information

19. Expand the **Roles** node; further expand the **Https** node and click on the target domain (here, **www.eccouncil.org**) to see the detailed information such as **IP - Source**, **Roles in IP**, **Domains in IP - Source**, **FingerPrinting – HTTP**, and **HTML Title** in the righthand pane.

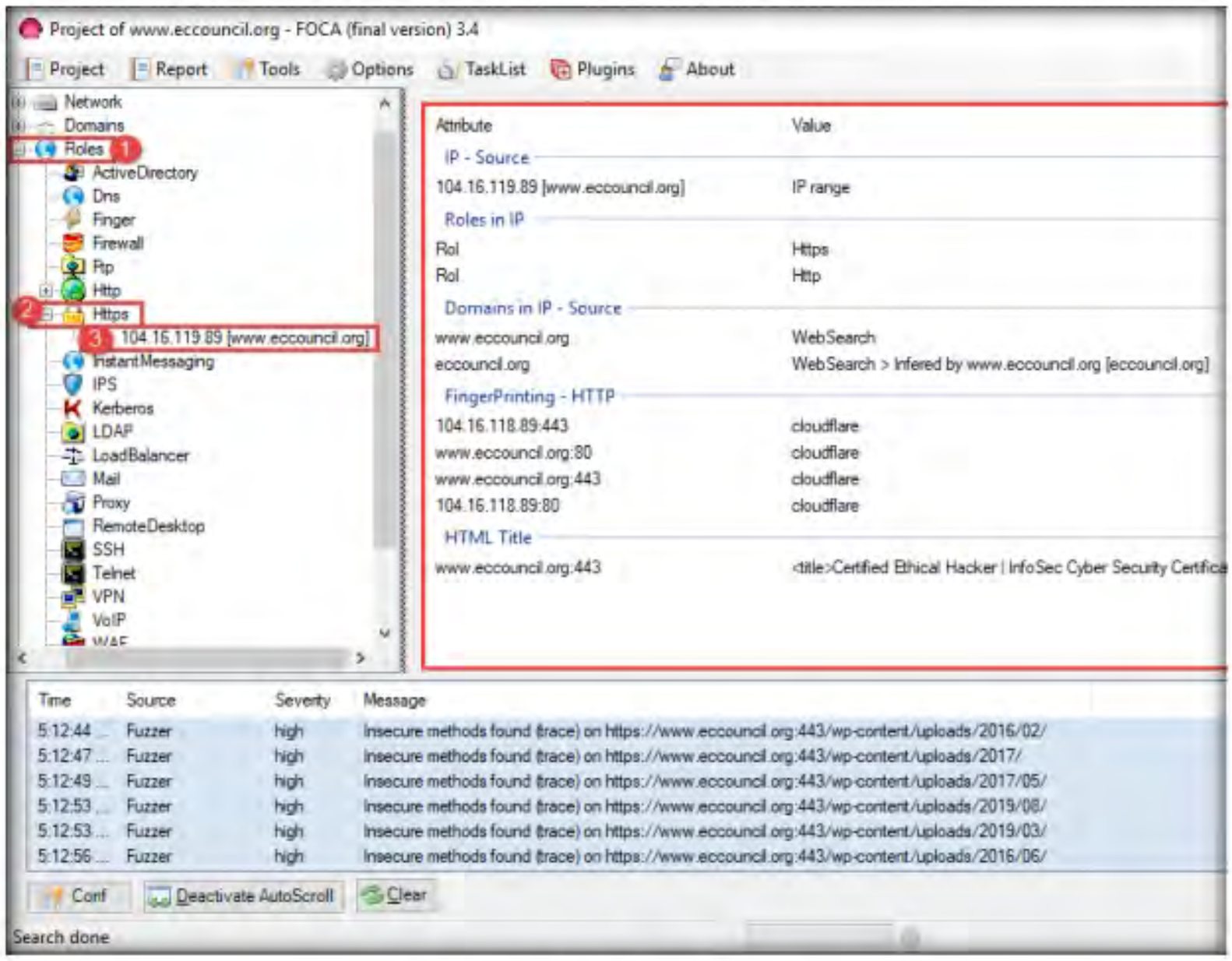


Figure 9.4.14: FOCA Https Information

20. This concludes the demonstration of gathering useful information about the target organization using the FOCA tool.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows 10** virtual machine.

TASK 5

Footprinting a Target using BillCipher

Here, we will use the BillCipher tool to footprint a target website URL.

BillCipher is an information gathering tool for a Website or IP address. Using this tool, you can gather information such as DNS Lookup, Whois lookup, GeoIP Lookup, Subnet Lookup, Port Scanner, Page Links, Zone Transfer, HTTP Header, etc.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

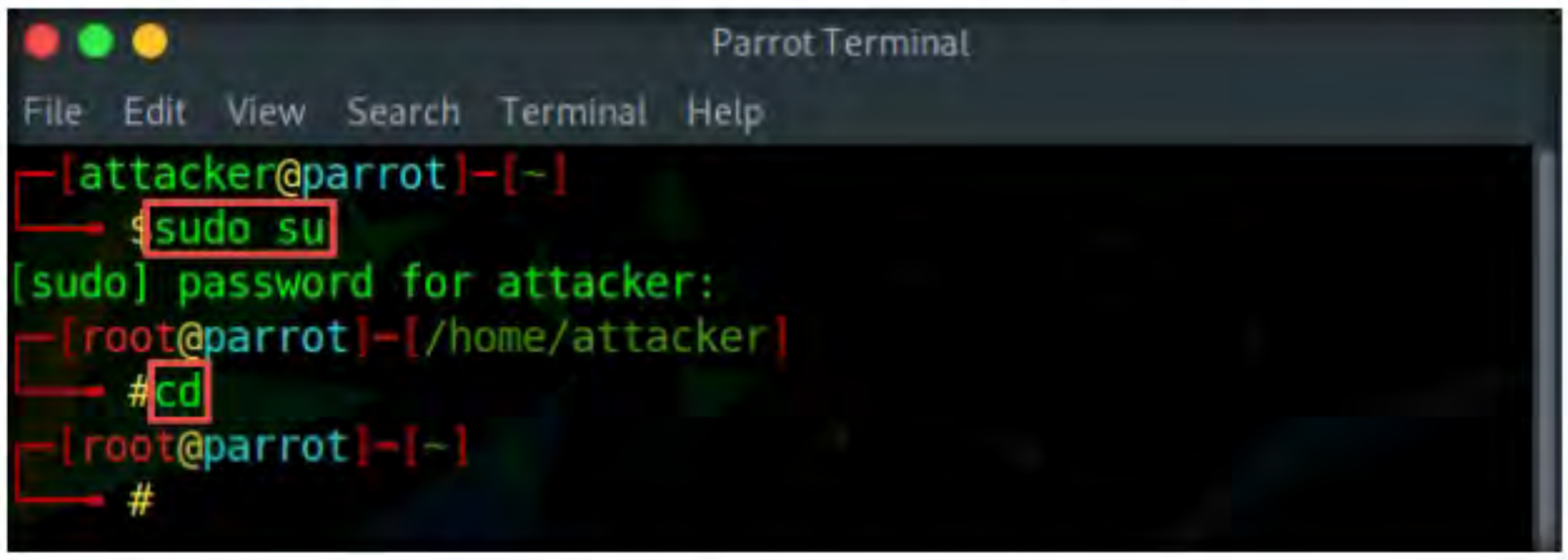


Figure 9.5.1: Running the programs as a root user

TASK 5.1

Clone and Launch BillCipher

7. In the **Parrot Terminal** window, type **git clone https://github.com/GitHackTools/BillCipher** and press **Enter** to clone the **BillCipher** directory.

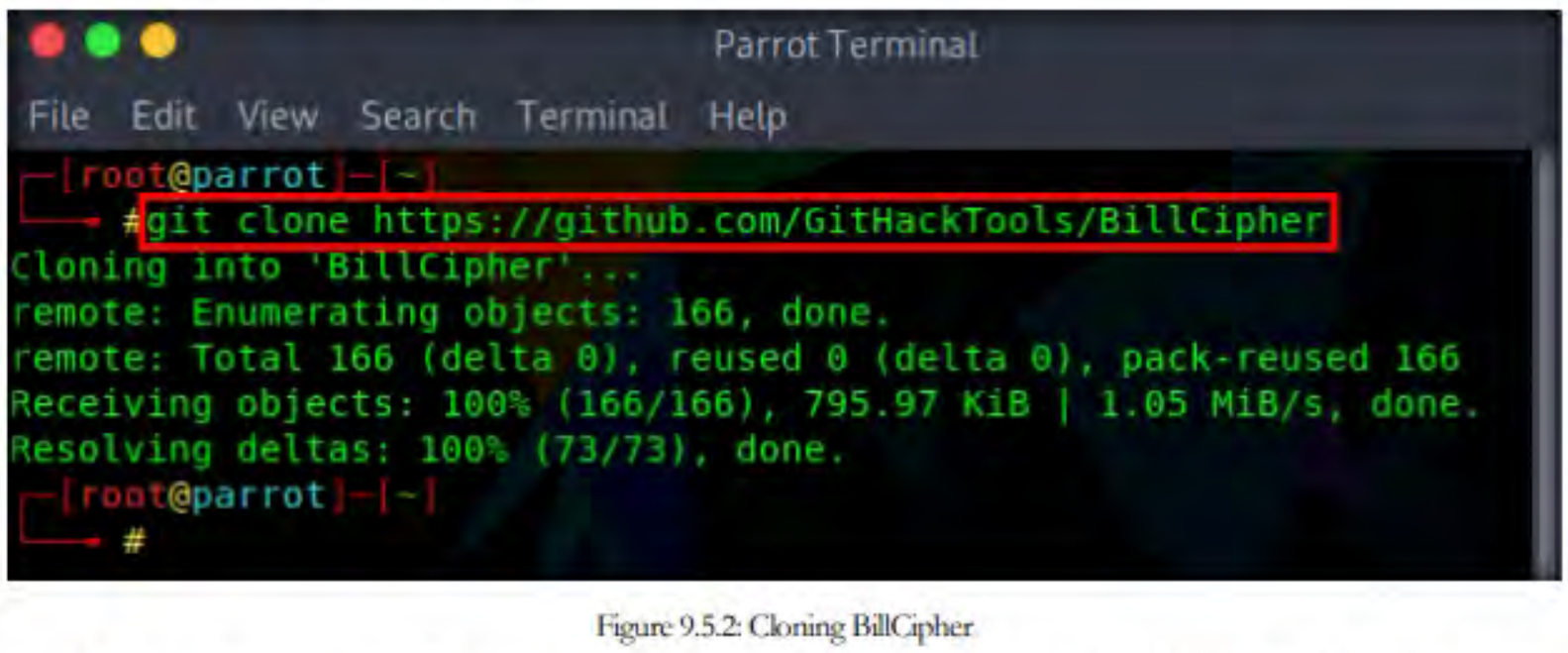


Figure 9.5.2: Cloning BillCipher

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **BillCipher** folder.
- Paste the copied **BillCipher** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/BillCipher /root/**.

8. In the terminal window, type **cd BillCipher** and press **Enter** to navigate to the **BillCipher** directory.

Note: By default, BillCipher application gets cloned to the **/root** directory.

9. Now, type **python3 billcipher.py** and press **Enter** to launch the application.

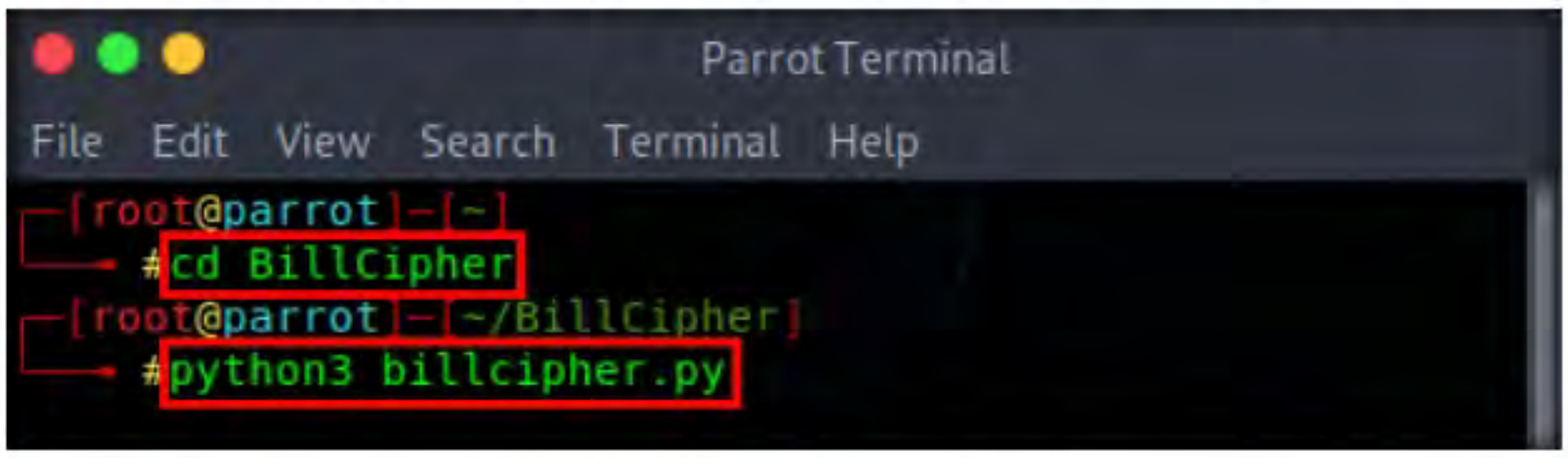


Figure 9.5.3: Launching BillCipher application

10. BillCipher application initializes. In the **Do you want to collect information of a website or IP address?** option, type **website** and press **Enter**.
11. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

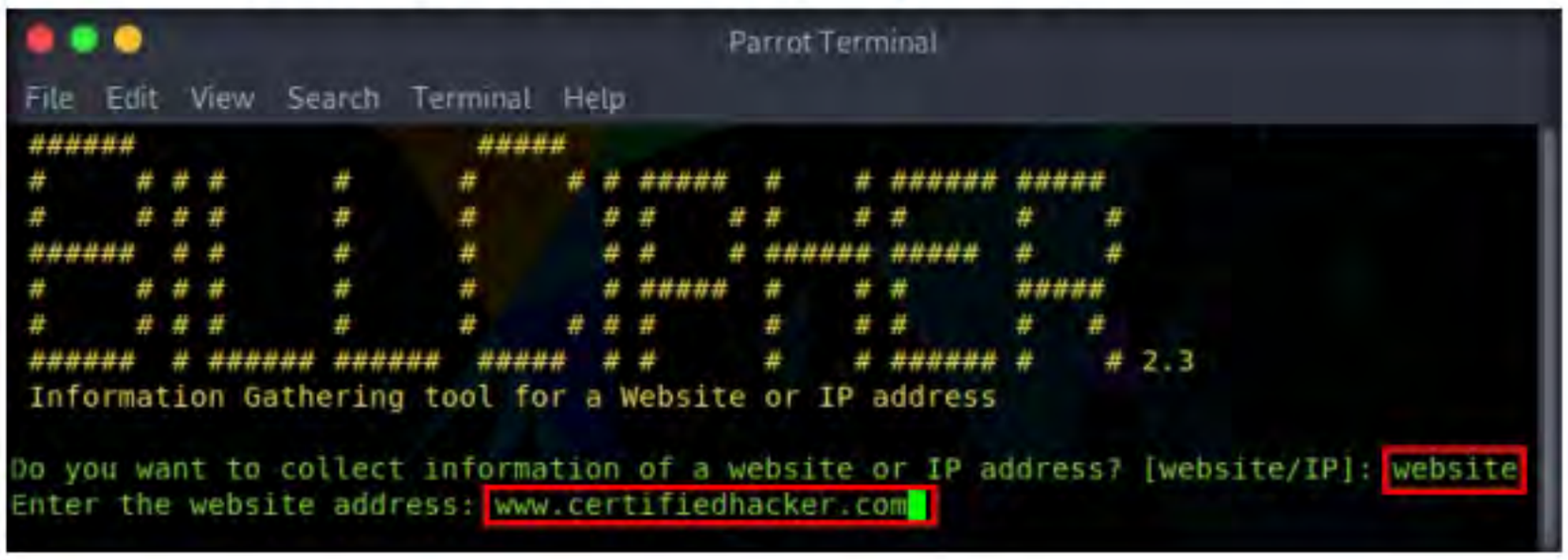


Figure 9.5.4: BillCipher initializes

TASK 5.2

Perform Information Gathering

12. BillCipher displays various available options that you can use to gather information regarding a target website.
13. In the **What information would you like to collect?** option, type **1** to choose the **DNS Lookup** option and press **Enter**.

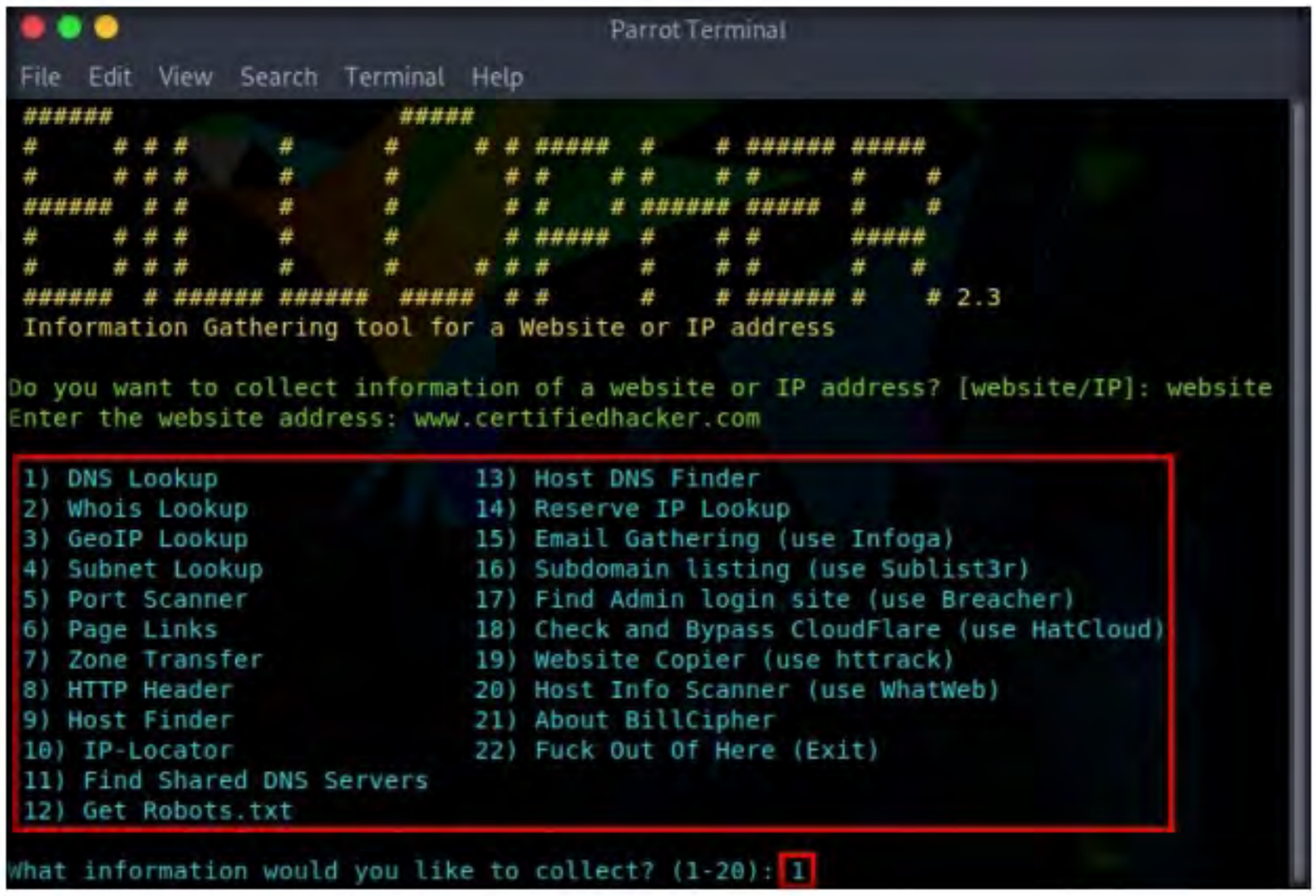


Figure 9.5.5: BillCipher options

14. The result appears, displaying the DNS information regarding the target website, as shown in the screenshot.

15. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

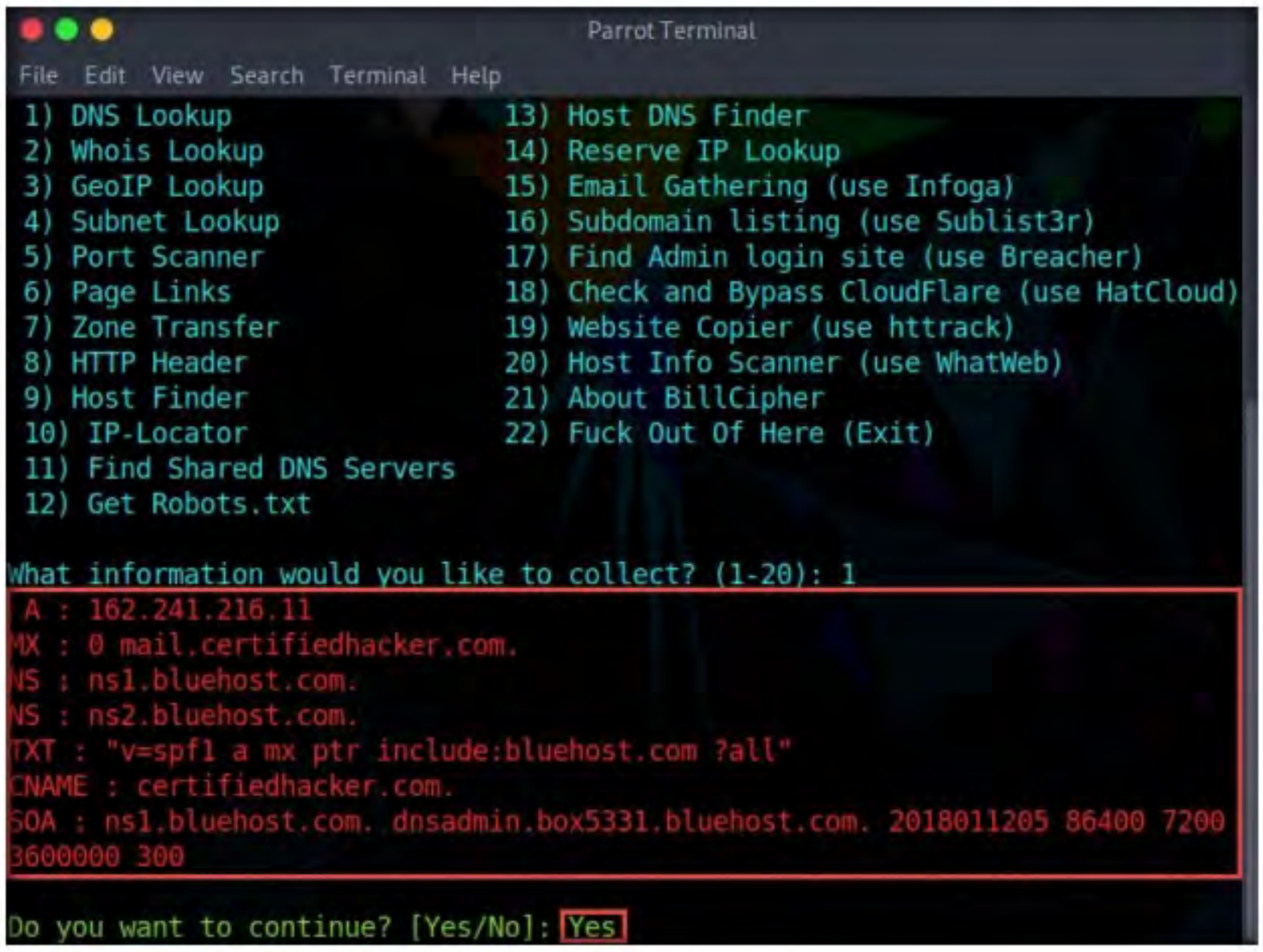


Figure 9.5.6: DNS Lookup result

16. **Do you want to collect information of a website or IP address?** option appears, type **website** and press **Enter**.
17. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
18. Now, type **3** and press **Enter** to choose the **GeoIP Lookup** option from the available information gathering options.

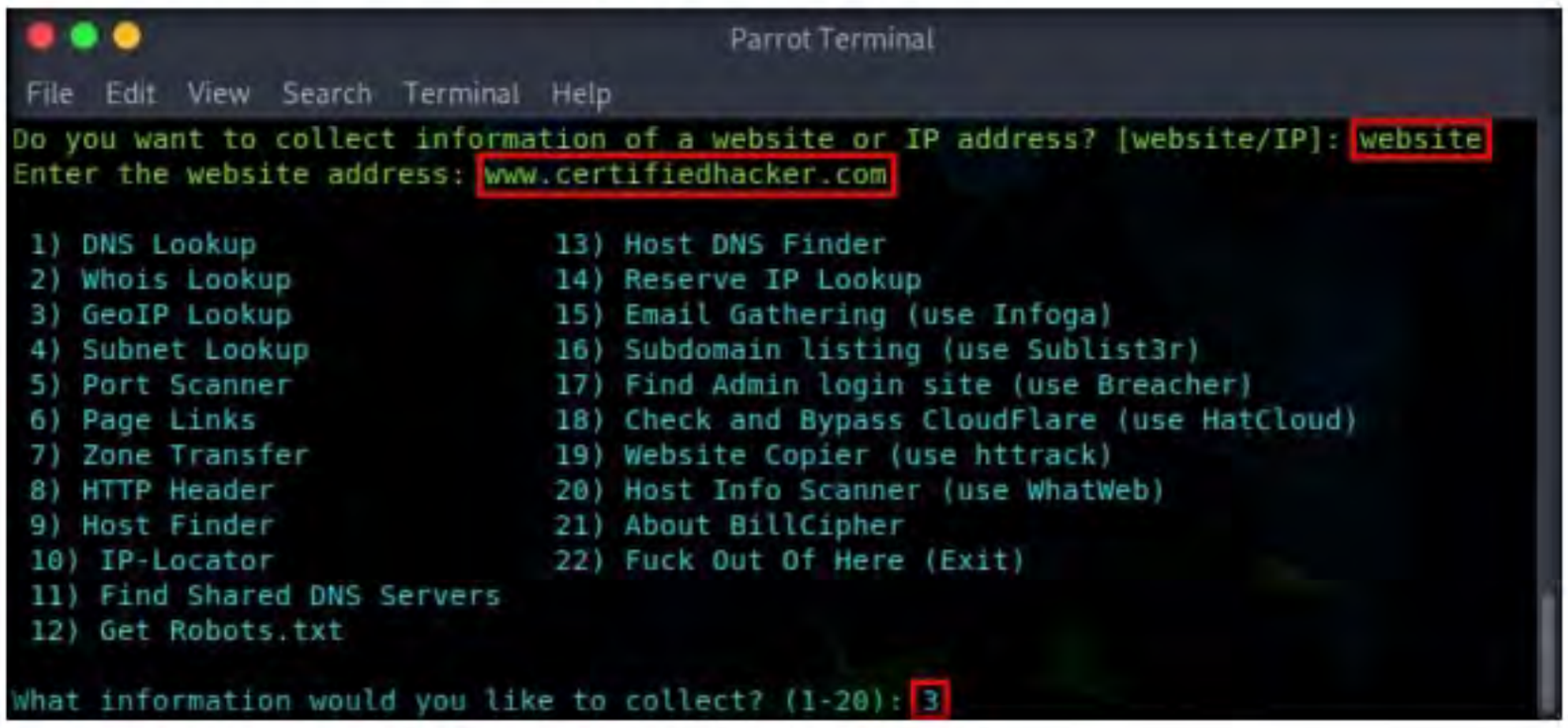


Figure 9.5.7: Choose option 3

19. The result appears, displaying the **GeoIP Lookup** information of the target website, as shown in the screenshot.
20. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

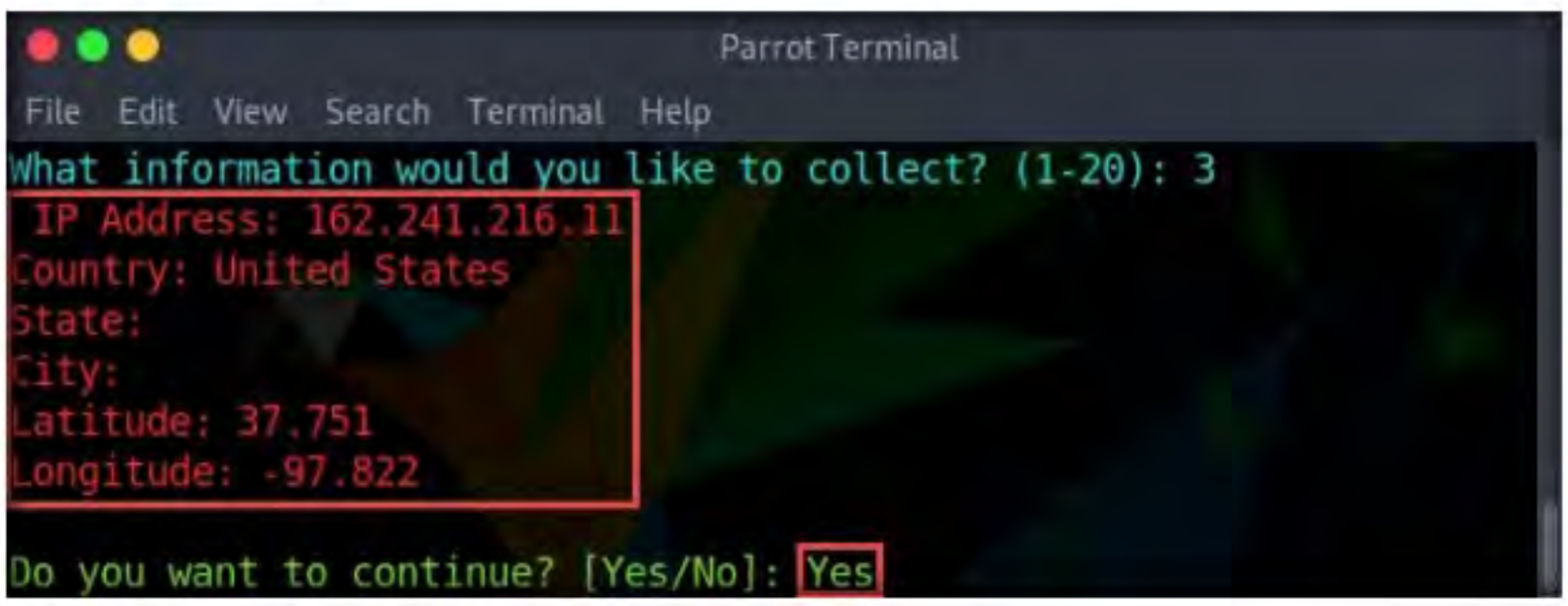


Figure 9.5.8: GeoIP Lookup result

21. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
22. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
23. Now, type **4** and press **Enter** to choose the **Subnet Lookup** option from the available information gathering options.

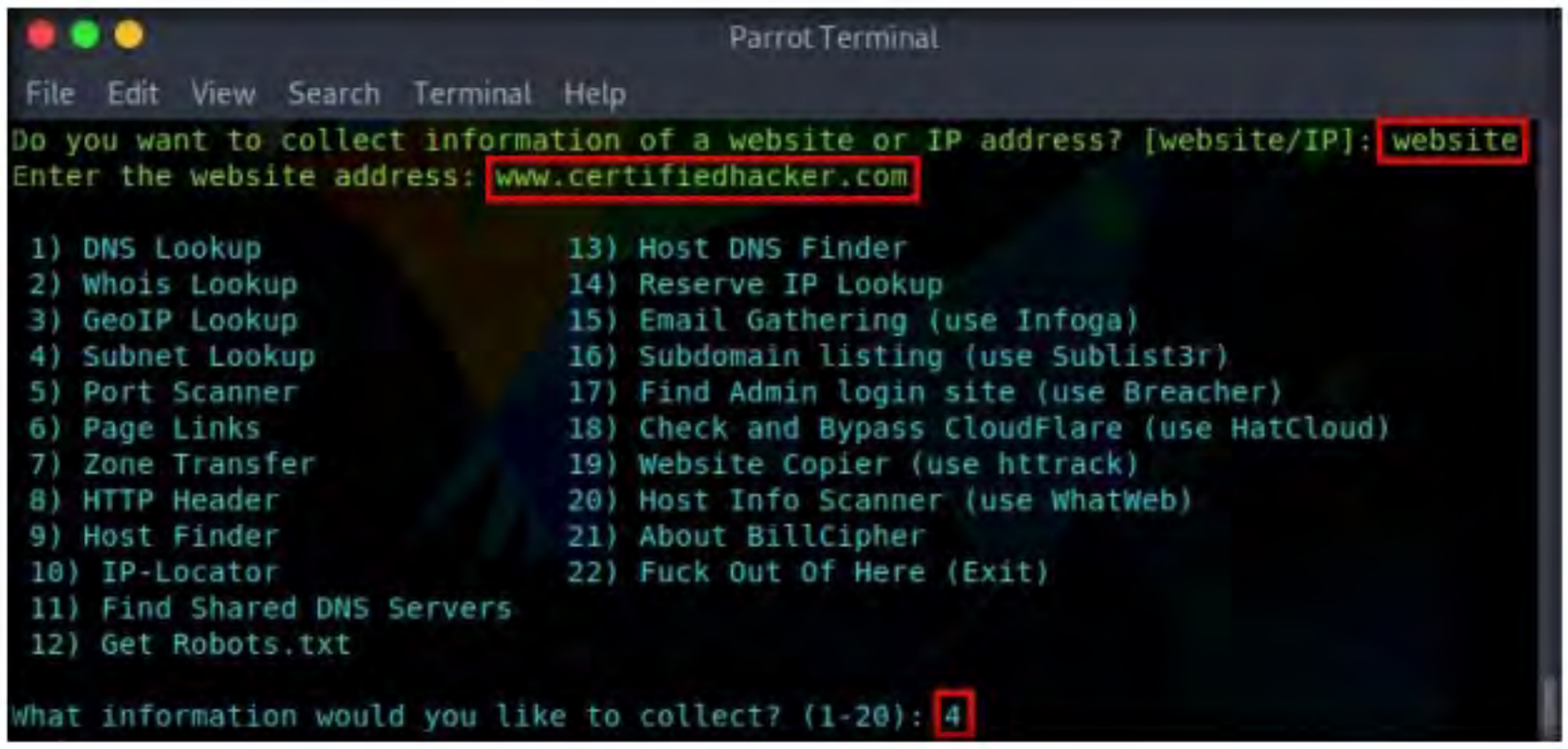


Figure 9.5.9: Choose option 4

24. The result appears, displaying the **Subnet Lookup** information of the target website.
25. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

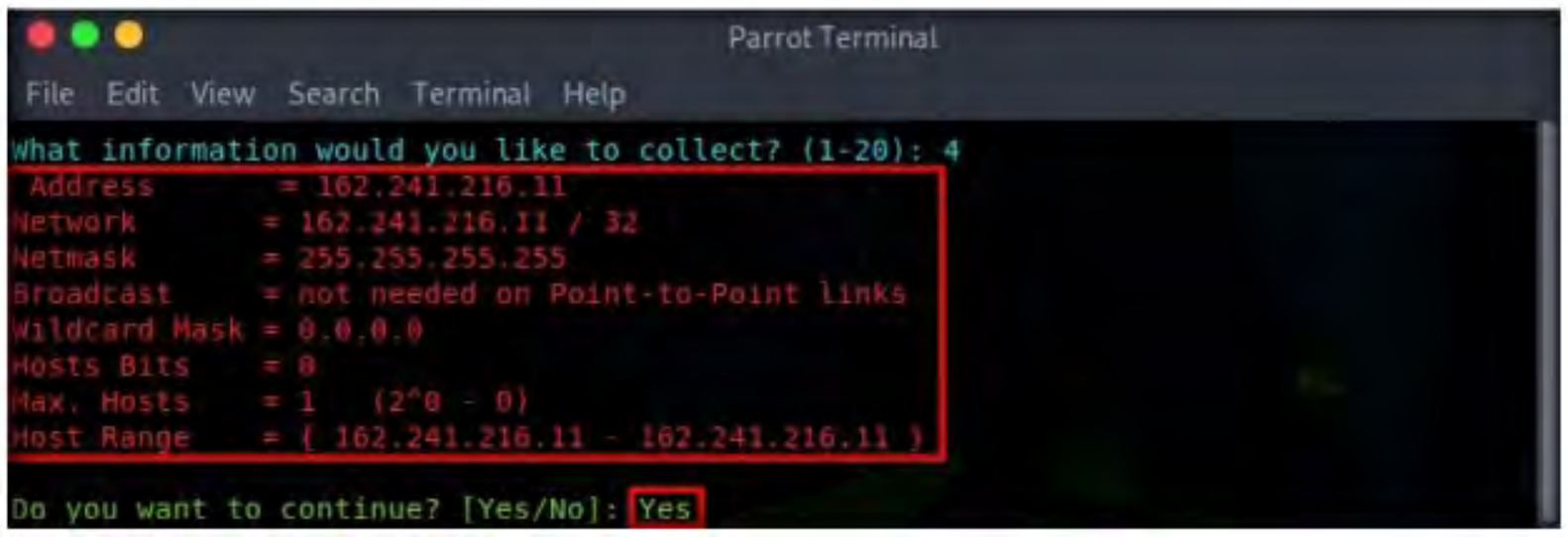


Figure 9.5.10: Choose option 4

26. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
27. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
28. Now, type **6** and press **Enter** to choose the **Page Links** option from the available information gathering options.
29. The result appears, displaying a list of **Visible links** and **Hidden links** of the target website, as shown in the screenshot.
30. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

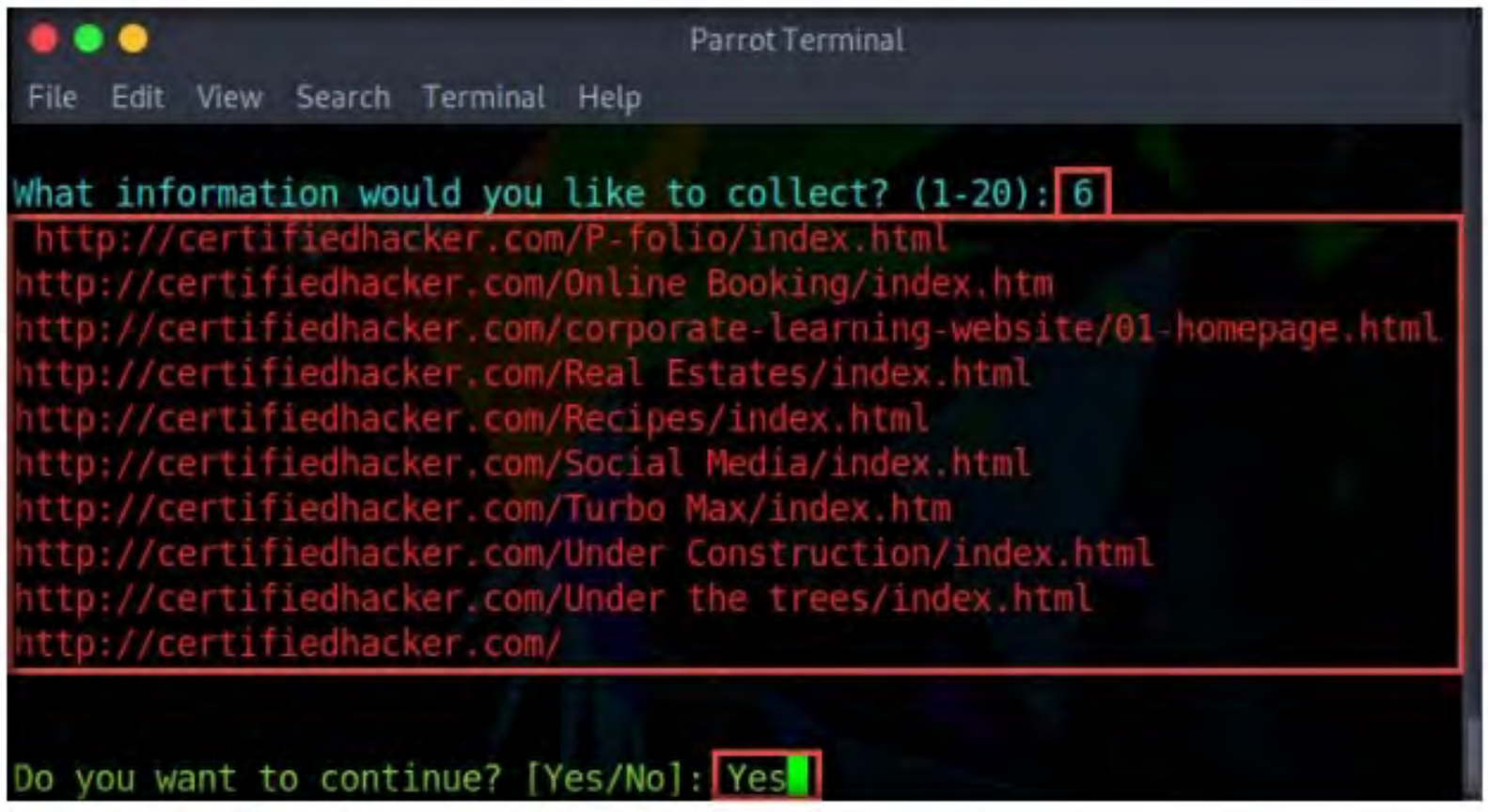


Figure 9.5.11: Page Links option results

31. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
32. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
33. Now, type **8** and press **Enter** to choose the **HTTP Header** option from the available information gathering options.
34. The result appears, displaying information regarding the HTTP header of the target website, as shown in the screenshot.
35. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

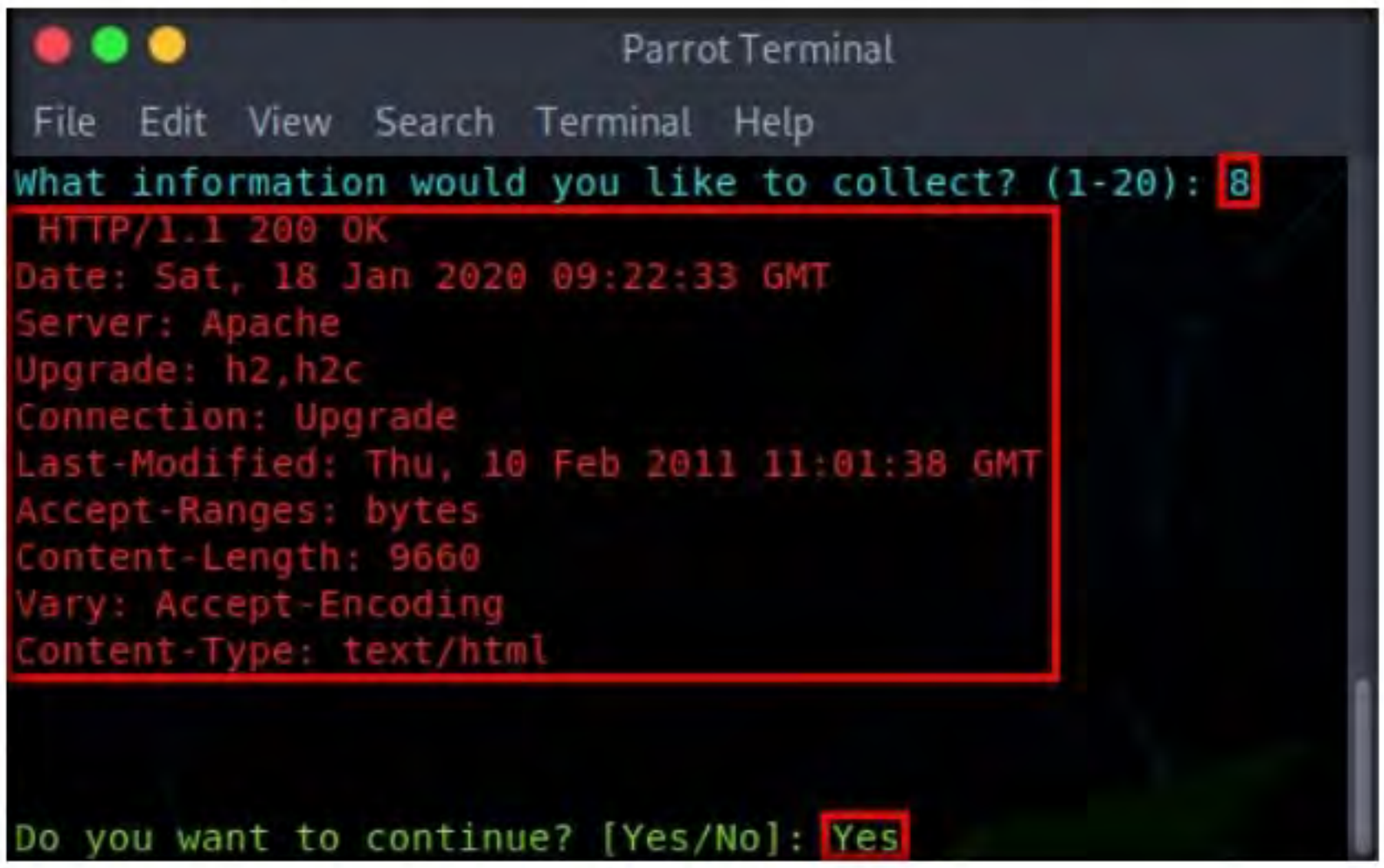


Figure 9.5.12: HTTP Header option results

36. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
37. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
38. Now, type **9** and press **Enter** to choose **Host Finder** option from the available information gathering options.
39. The result appears, displaying information regarding the IP address of the target website, as shown in the screenshot.
40. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

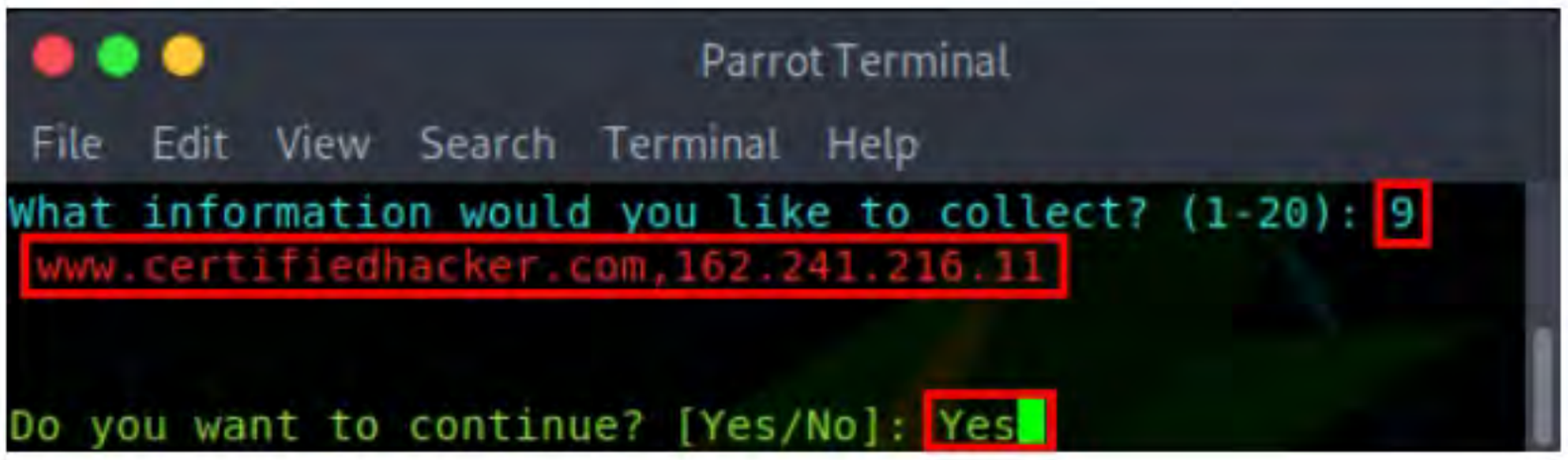


Figure 9.5.13: Host Finder option results

41. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
42. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
43. Now, type **13** and press **Enter** to choose **Host DNS Finder** option from the available information gathering options.
44. The result appears, displaying information regarding host DNS of the target website, as shown in the screenshot.
45. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

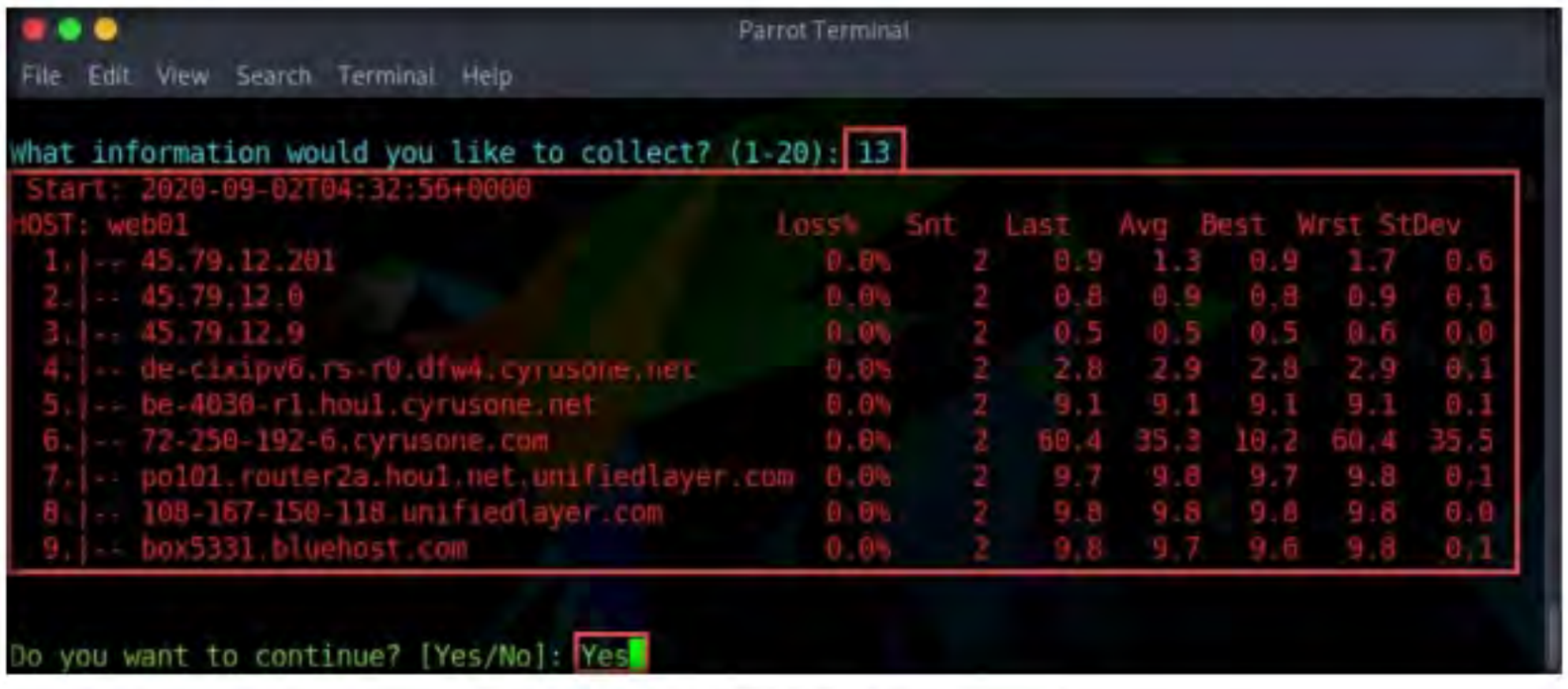


Figure 9.5.14: Host DNS Finder option results

46. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
47. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
48. Now, type **19** and press **Enter** to choose the **Website Copier (use httrack)** option from the available information gathering options.
49. The tool starts mirroring the target website; this will take approximately 5 minutes.
50. After completion of the mirroring process, the mirrored website gets saved in the folder **websource**, as shown in the screenshot.

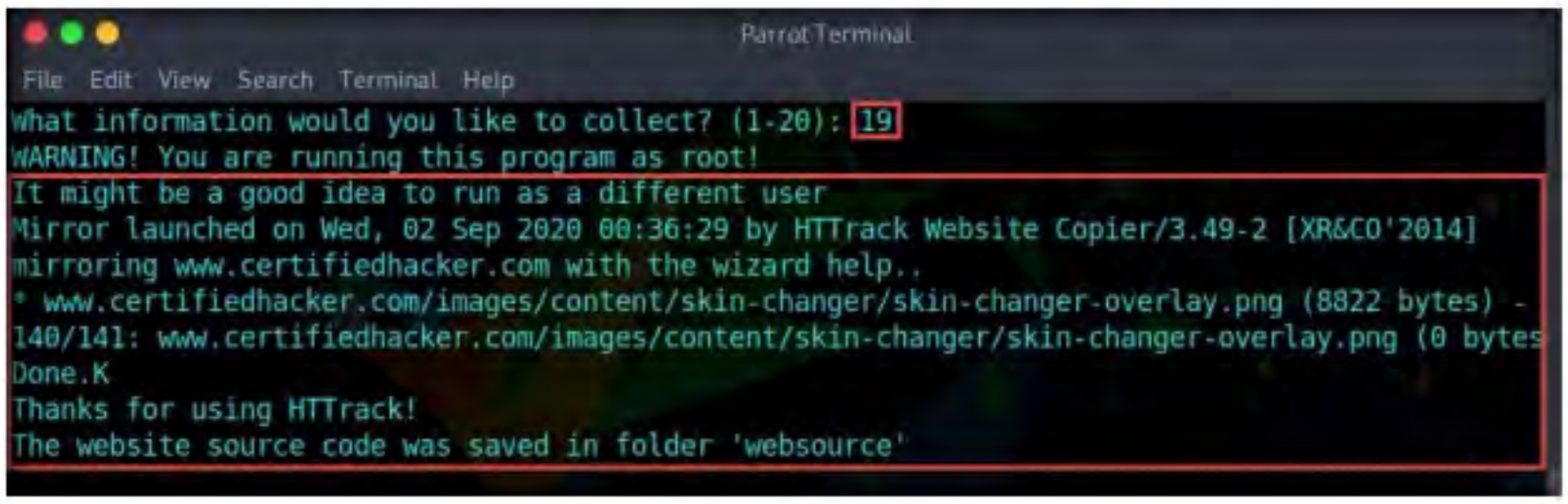


Figure 9.5.15: Copying website

51. Press **Ctrl+C** to exit BillCipher and close the terminal window.
52. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

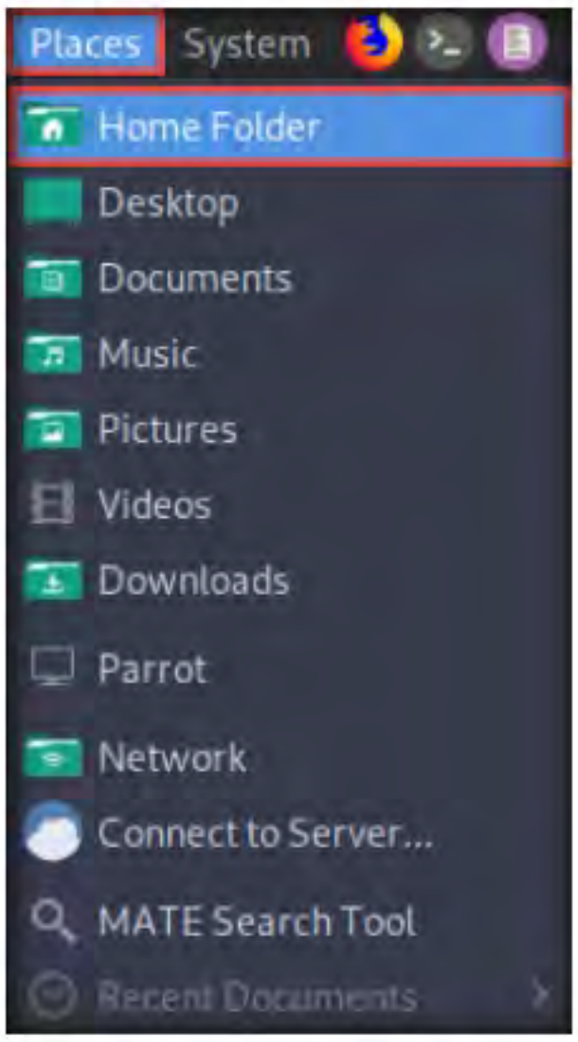


Figure 9.5.16: Navigate to the Home Folder

53. The **attacker** window appears, click **File System** from the left-pane and navigate to the location **root**.

54. The **root** directory window appears; navigate to **BillCipher** → **websource** → **www.certifiedhacker.com** → **www.certifiedhacker.com**. Right-click the **index.html** file and navigate to **Open With** → **Firefox** to open the mirrored website.

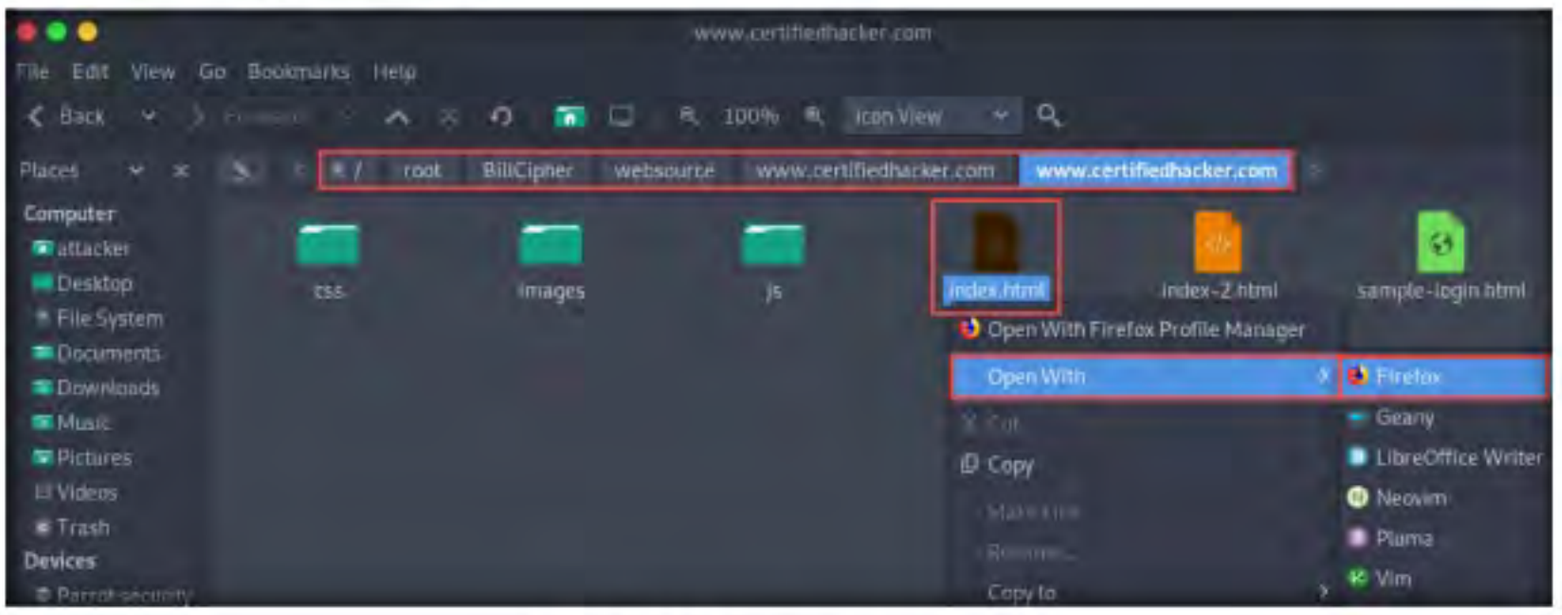


Figure 9.5.17: Opening index.html file

55. The mirror target website (**www.certifiedhacker.com**) appears in the **Mozilla Firefox** browser, as shown in the screenshot.

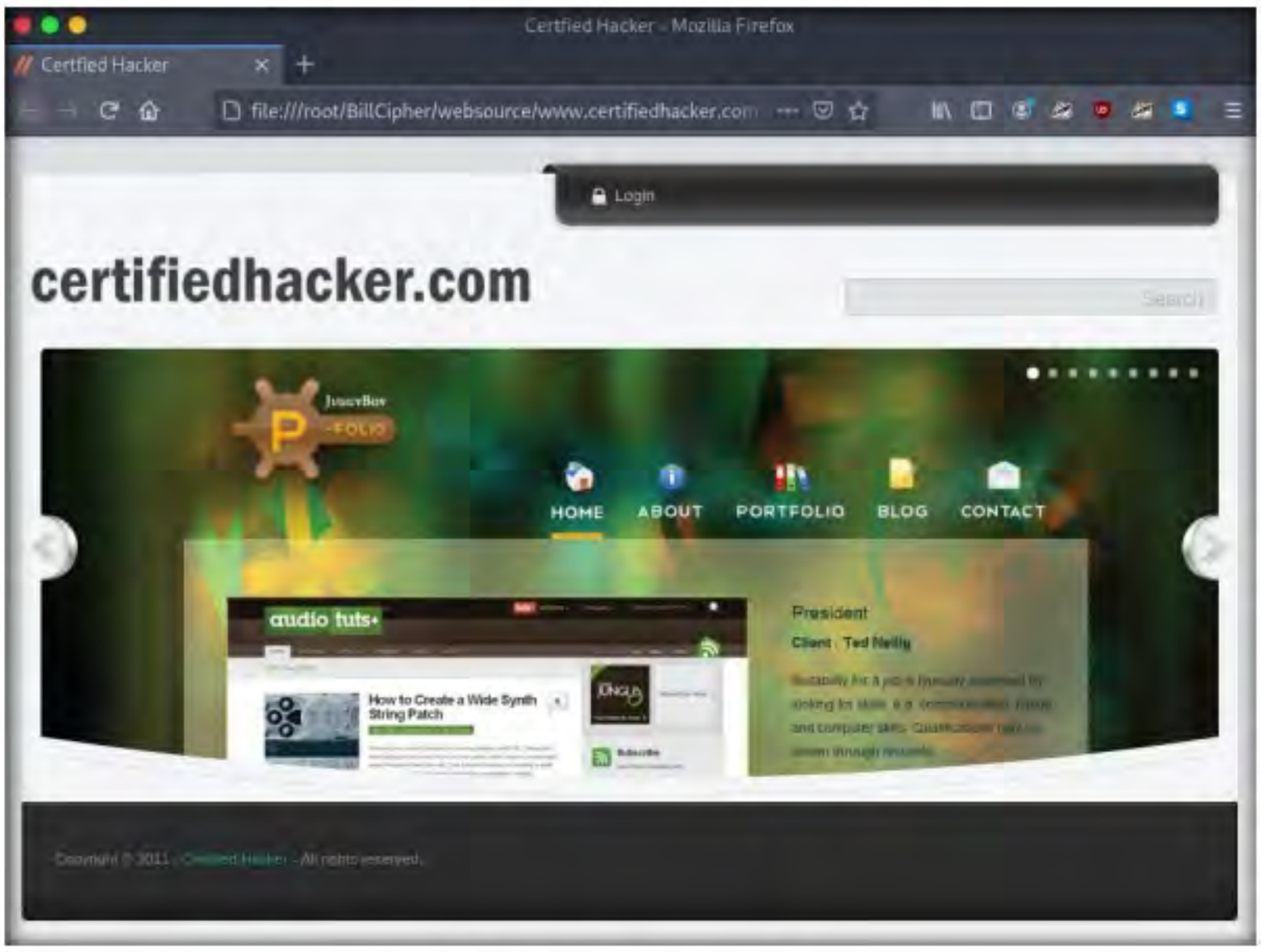


Figure 9.5.18: Mirrored target website

56. Similarly, you can use other information gathering options to gather information about the target.
57. This concludes the demonstration of footprinting the target website URL using BillCipher.
58. Close all open windows and document all the acquired information.
59. Turn off the **Parrot Security** virtual machine.

You can also use footprinting tools such as **Recon-Dog** (https://www.github.com), **Th3Inspector** (https://github.com), **Raccoon** (https://github.com), **Orb** (https://github.com), etc. to gather additional information related to the target company.

TASK 6 Footprinting a Target using OSINT Framework

Here, we will use the OSINT Framework to explore footprinting categories and associated tools.

1. Turn on the **Windows 10** virtual machine and login with credentials **Admin/Pa$$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**); type **https://osintframework.com/** in the address bar and press **Enter**.

TASK 6.1

Navigate to OSINT Framework

3. **OSINT Framework** website appears; you can observe the OSINT tree on the left side of screen, as shown in the screenshot.

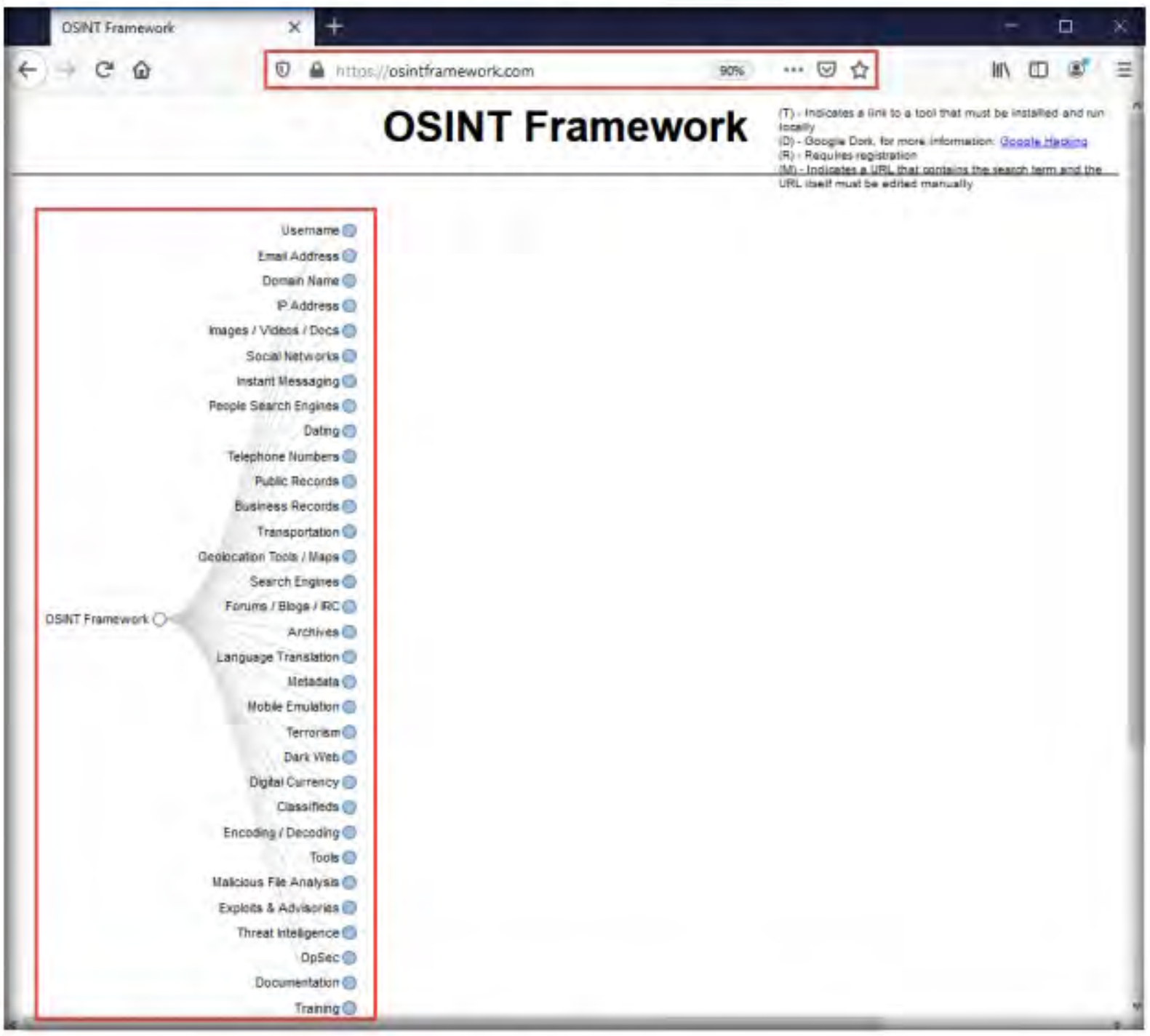


Figure 9.6.1: OSINT tree

OSINT Framework is an open source intelligence gathering framework that helps security professionals for performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering. It is focused on gathering information from free tools or resources. This framework includes a simple web interface that lists various OSINT tools arranged by category and is shown as an OSINT tree structure on the web interface.

TASK 6.2

View Username Category

4. Clicking on any of the categories such as **Username**, **Email Address**, or **Domain Name** will make many useful resources appear on the screen in the form of a sub-tree.
5. Click the **Username** category and click to expand the **Username Search Engines** and **Specific Sites** sub-categories.
6. You can observe a list of OSINT tools filtered by sub-categories (**Username Search Engines** and **Specific Sites** sub-categories).

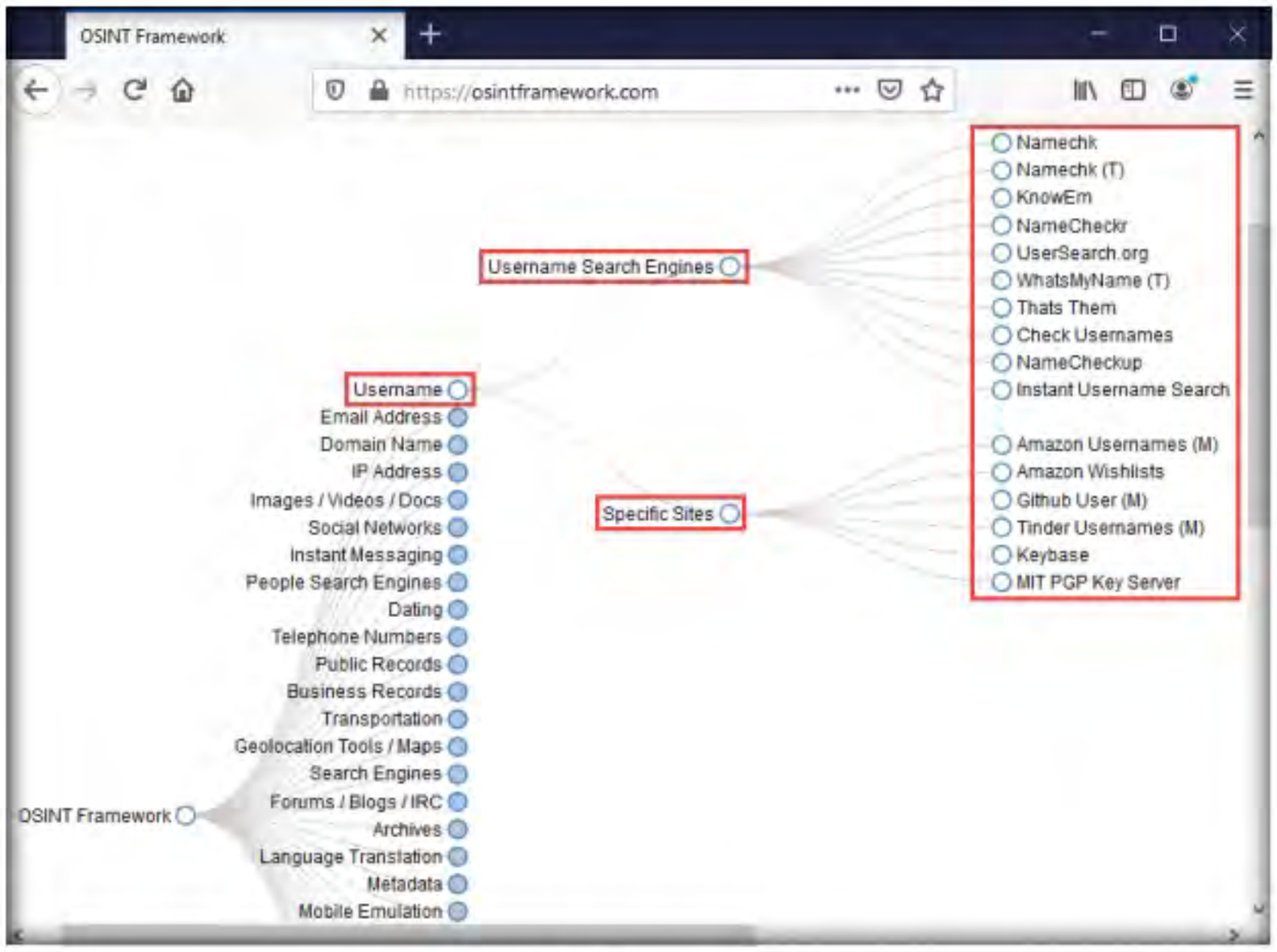


Figure 9.6.2: Username categories

7. From the list of available tools under the **Username Search Engines** category, click on the **Namechk** tool to navigate to the **Namechk** website.

Note: If a cookie notification appears at the lower section of the window, click **Got it!** and close the ads appearing on the screen.

8. The **Namechk** website appears, as shown in the screenshot.

Note: Namechk is used to see if your desired username or vanity URL is still available at dozens of popular social networking and social bookmarking websites. You can also find the best username with Namechk.

The OSINT Framework includes the following indicators with the available tools:

- **(T)** - Indicates a link to a tool that must be installed and run locally
- **(D)** - Google Dork
- **(R)** - Requires registration
- **(M)** - Indicates a URL that contains the search term and the URL itself must be edited manually.

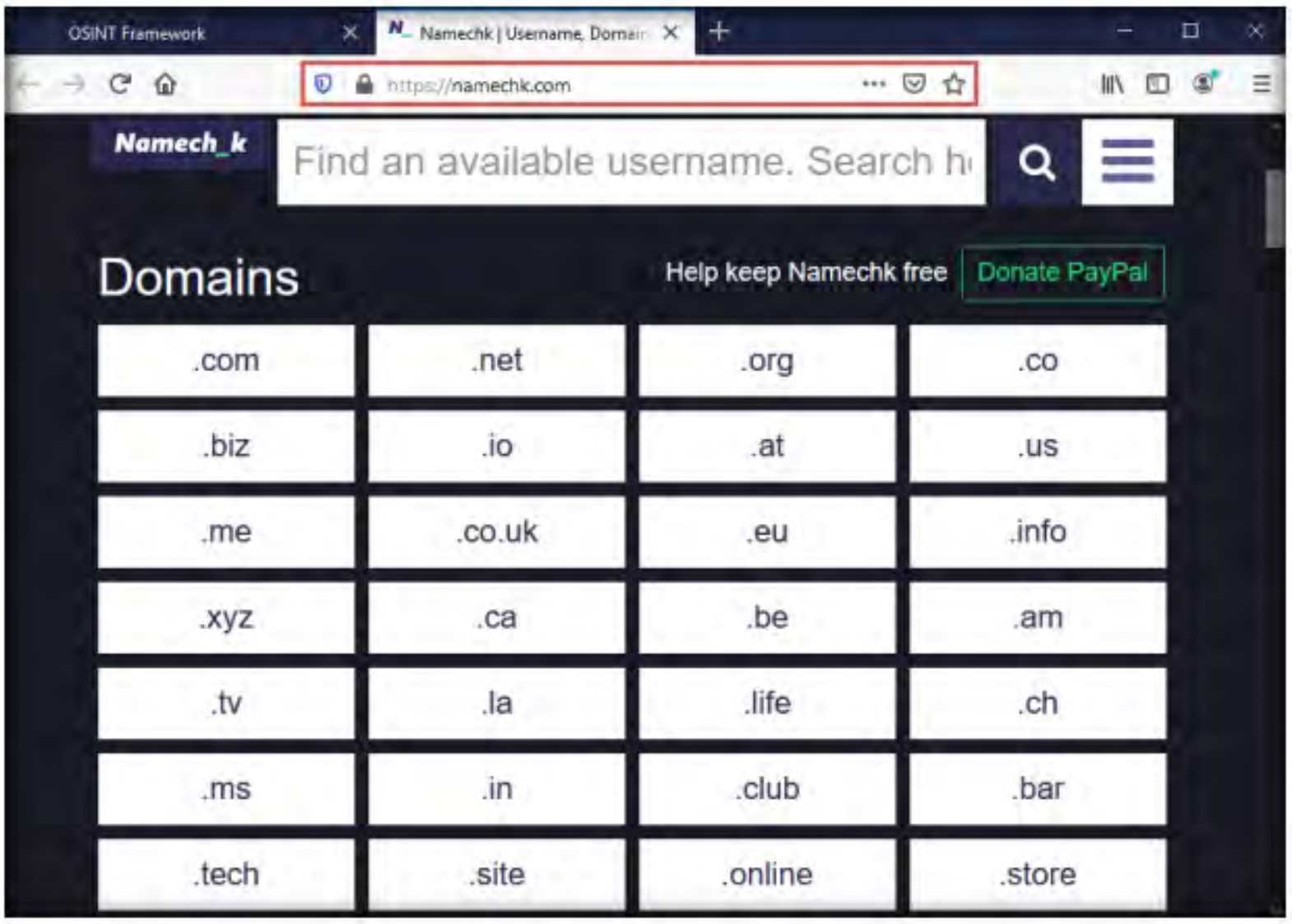


Figure 9.6.3: Namechk website

9. Close the current tab to navigate back to the **OSINT Framework** webpage.
10. Similarly, you can explore other tools from the list of mentioned tools under the **Username Search Engines** and **Specific Sites** sub-categories.

TASK 6.3

View Domain Name Category

11. Now, click the **Domain Name** category, and its sub-categories appear. Click to expand the **Whois Records** sub-category.
12. A list of tools under the **Whois Records** sub-category appears; click the **Domain Dossier** tool.

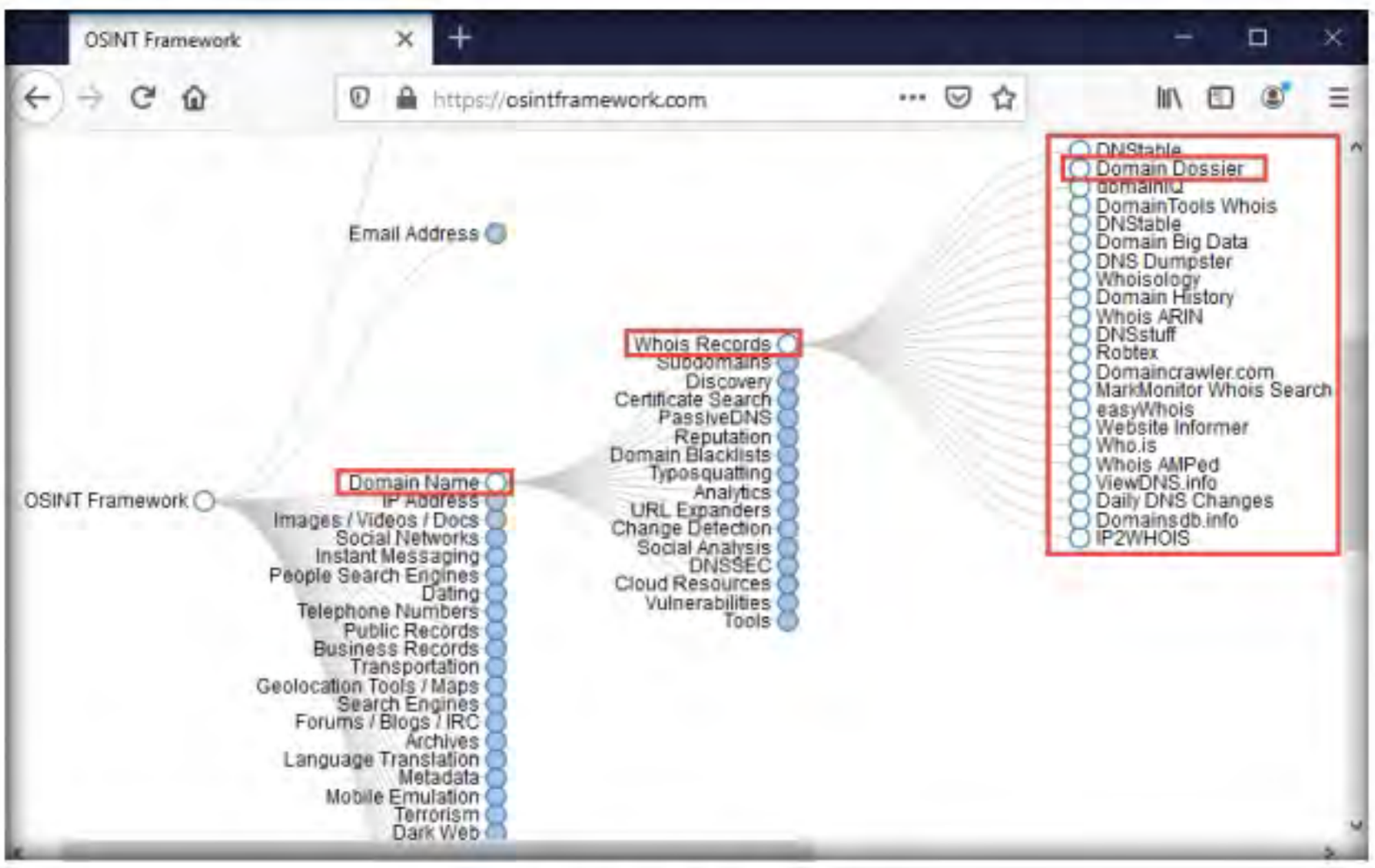


Figure 9.6.4: Clicking on Domain Dossier

13. The **Domain Dossier** website appears, as shown in the screenshot.

Note: The Domain Dossier tool generates reports from public records about domain names and IP addresses to help solve problems, investigate cybercrime, or just to better understand how things are set up.

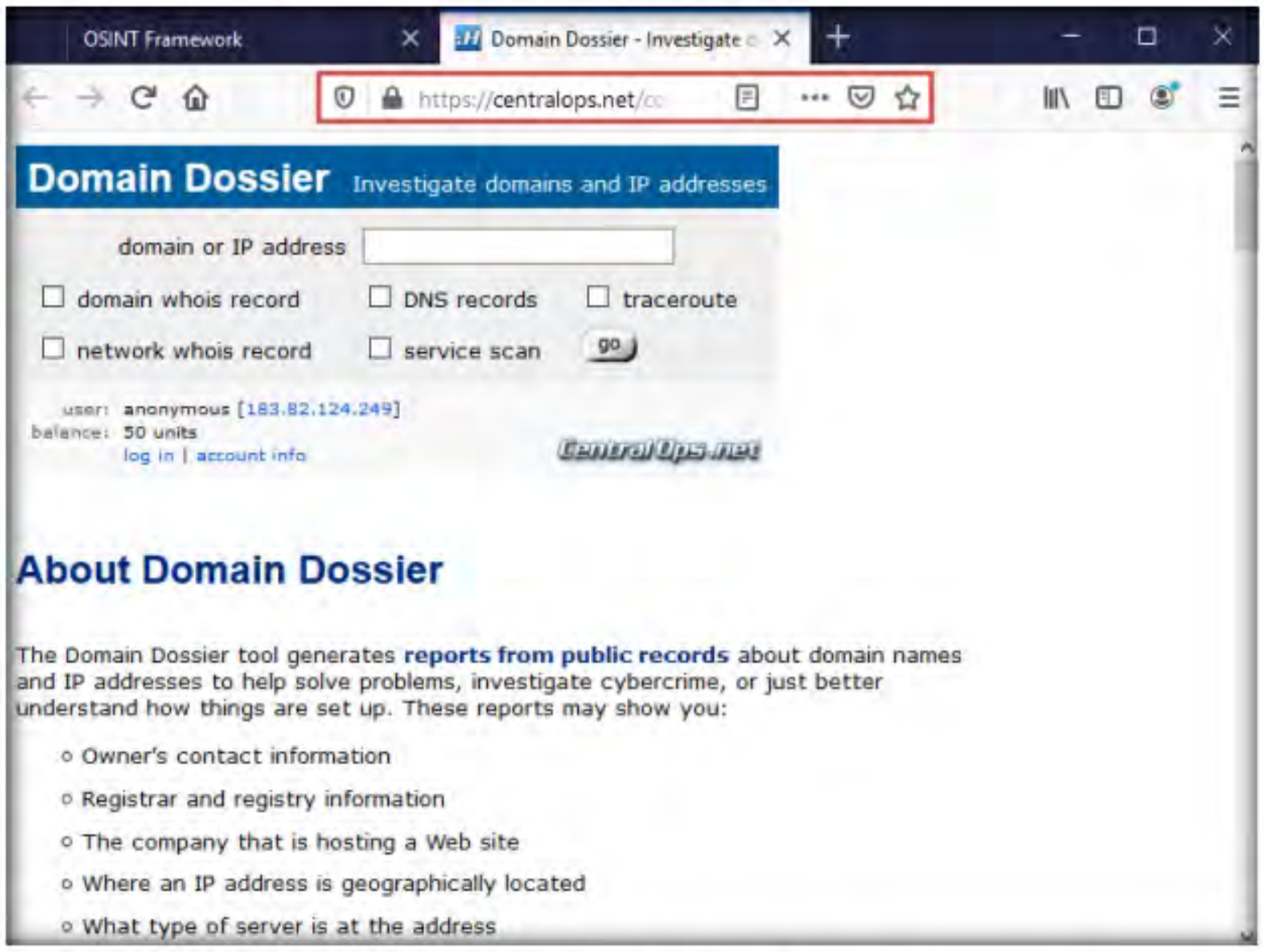


Figure 9.6.5: Domain Dossier website

14. Close the current tab to navigate back to the **OSINT Framework** webpage.

TASK 6.4

View Metadata Category

15. Now, click the **Metadata** category and click the **FOCA** tool from a list of available tools.

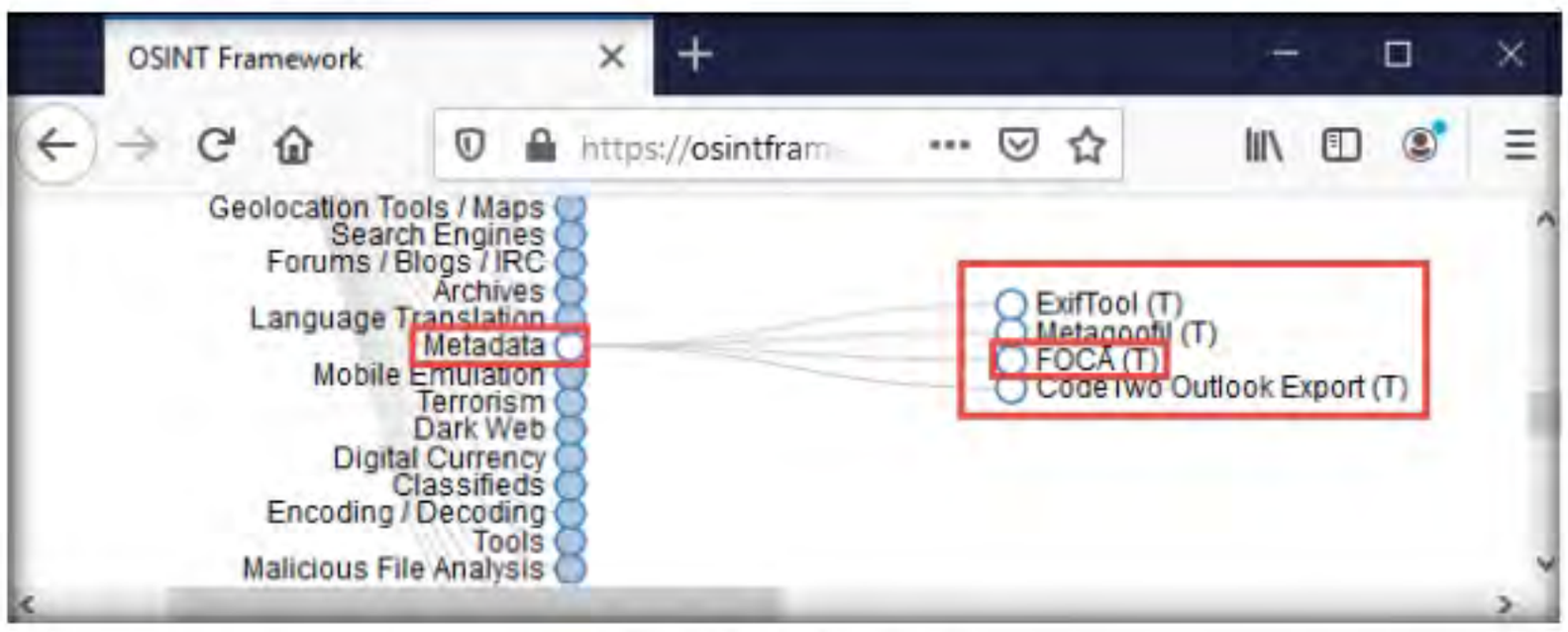


Figure 9.6.6: Metadata category

16. The **FOCA** website appears, displaying information about the tool along with its download link, as shown in the screenshot.

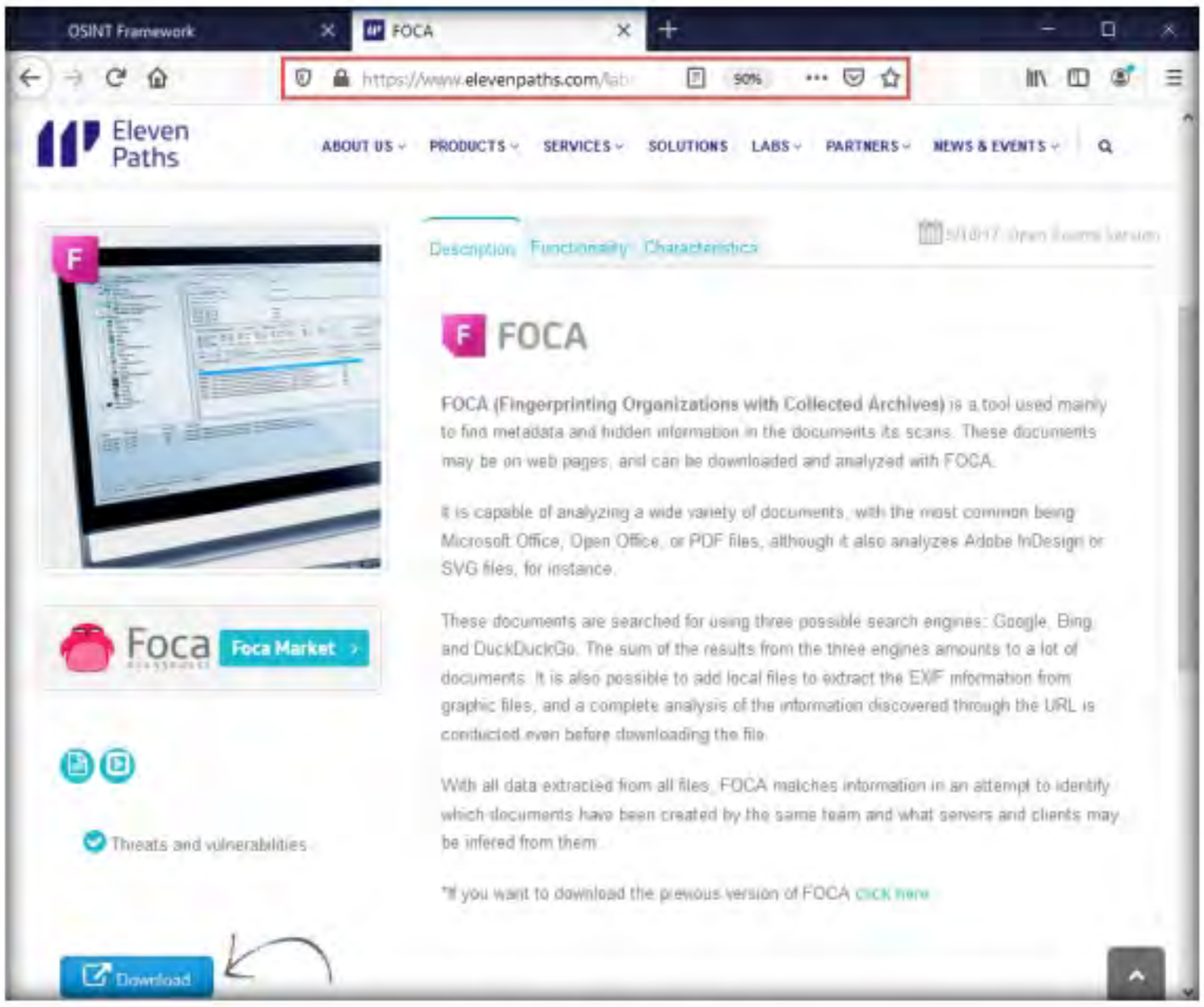


Figure 9.6.7: FOCA website

17. Similarly, you can explore other available categories such as **Email Address**, **IP Address**, **Social Networks**, **Instant Messaging**, etc. and the tools associated with each category. Using these tools, you can perform footprinting on the target organization.
18. This concludes the demonstration of performing footprinting using the OSINT Framework.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Scanning Networks

Module 03

Scanning a Target Network

Network scanning refers to a set of procedures performed to identify the hosts, ports, and services running in a network.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Earlier, you gathered all possible information about the target such as organization information (employee details, partner details, web links, etc.), network information (domains, sub-domains, IP addresses, network topology, etc.), and system information (OS details, user accounts, passwords, etc.).

Now, as an ethical hacker, or as a penetration tester (hereafter, pen tester), your next step will be to perform port scanning and network scanning on the IP addresses that you obtained in the information-gathering phase. This will help you to identify an entry point into the target network.

Scanning itself is not the actual intrusion, but an extended form of reconnaissance in which the ethical hacker and pen tester learns more about the target, including information about open ports and services, OSes, and any configuration lapses. The information gleaned from this reconnaissance helps you to select strategies for the attack on the target system or network.

This is one of the most important phases of intelligence gathering, which enables you to create a profile of the target organization. In the process of scanning, you attempt to gather information, including the specific IP addresses of the target system that can be accessed over the network (live hosts), open ports, and respective services running on the open ports and vulnerabilities in the live hosts.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Port scanning will help you identify open ports and services running on specific ports, which involves connecting to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) system ports. Port scanning is also used to discover the vulnerabilities in the services running on a port.

The labs in this module will give you real-time experience in gathering information about the target organization using various network scanning and port scanning techniques.

Lab Objectives

The objective of this lab is to conduct network scanning, port scanning, analyzing the network vulnerabilities, etc.

Network scans are needed to:

- Check live systems and open ports
- Identify services running in live systems
- Perform banner grabbing/OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts