

## ETHICAL HACKING AND COUNTERMEASURES

# LAB MANUAL



## ETHICAL HACKING AND COUNTERMEASURES

# LAB MANUAL



# **Ethical Hacking and Countermeasures**

**Version 12**

**Lab Manual**

## EC-Council

Copyright © 2022 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

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

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at [legal@eccouncil.org](mailto:legal@eccouncil.org). In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at [legal@eccouncil.org](mailto:legal@eccouncil.org). If you have any issues, please contact us at [support@eccouncil.org](mailto:support@eccouncil.org).

## NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

# Table of Contents

Module Number	Module Name	Page No.
01	Introduction to Ethical Hacking	-
02	Footprinting and Reconnaissance	01
03	Scanning Networks	214
04	Enumeration	346
05	Vulnerability Analysis	470
06	System Hacking	560
07	Malware Threats	908
08	Sniffing	1105
09	Social Engineering	1245
10	Denial-of-Service	1301
11	Session Hijacking	1358
12	Evading IDS, Firewalls, and Honeypots	1405
13	Hacking Web Servers	1482
14	Hacking Web Applications	1531
15	SQL Injection	1704
16	Hacking Wireless Networks	1751
17	Hacking Mobile Platforms	1838
18	IoT and OT Hacking	1913
19	Cloud Computing	1954
20	Cryptography	1991

This page is intentionally left blank.

**CEH Lab Manual**

---

# **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.*

## 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 a real-time experience in collecting a variety of information about the target organization from various open or publicly accessible sources.

## Lab Objective

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

- **Organization Information:** Employee details, addresses and contact details, partner details, weblinks, web technologies, patents, trademarks, etc.
- **Network Information:** Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information

- **System Information:** Operating systems, web server OSes, location of web servers, user accounts and passwords, etc.

## **Lab Environment**

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

## **Lab Duration**

Time: 220 Minutes

## **Overview of Footprinting**

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**	CyberQ ***
1	Perform Footprinting Through Search Engines	√	√	√
	1.1 Gather Information using Advanced Google Hacking Techniques	√		√
	1.2 Gather Information from Video Search Engines		√	√

**Module 02 – Footprinting and Reconnaissance**

	1.3 Gather Information from FTP Search Engines		√	√
	1.4 Gather Information from IoT Search Engines		√	√
<b>2</b>	<b>Perform Footprinting Through Web Services</b>	√	√	√
	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		√	√
<b>3</b>	<b>Perform Footprinting Through Social Networking Sites</b>	√	√	√
	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		√	√
<b>4</b>	<b>Perform Website Footprinting</b>	√	√	√
	4.1 Gather Information About a Target Website using Ping Command Line Utility		√	√
	4.2 Gather Information about a Target Website using Photon	√		√
	4.3 Gather information about a Target Website using Central Ops		√	√
	4.4 Extract a Company's Data using Web Data Extractor		√	√
	4.5 Mirror a Target Website using HTTrack Web Site Copier	√		√
	4.6 Gather Information About a Target Website using GRecon		√	√
	4.7 Gather a Wordlist from the Target Website using CeWL		√	√
<b>5</b>	<b>Perform Email Footprinting</b>	√		√
	5.1 Gather Information About a Target by Tracing Emails using eMailTrackerPro	√		√
<b>6</b>	<b>Perform Whois Footprinting</b>	√		√
	6.1 Perform Whois Lookup using DomainTools	√		√

## Module 02 – Footprinting and Reconnaissance

<b>7</b>	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		√	√
	7.3 Gather Information of Subdomain and DNS Records using SecurityTrails	√		√
<b>8</b>	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		√	
<b>9</b>	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 CEHv12 volume 1 book.

\*\*\*CyberQ - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

### **Lab Analysis**

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

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

---

Lab

1

## Perform Footprinting Through Search Engines

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

### 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

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

### 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

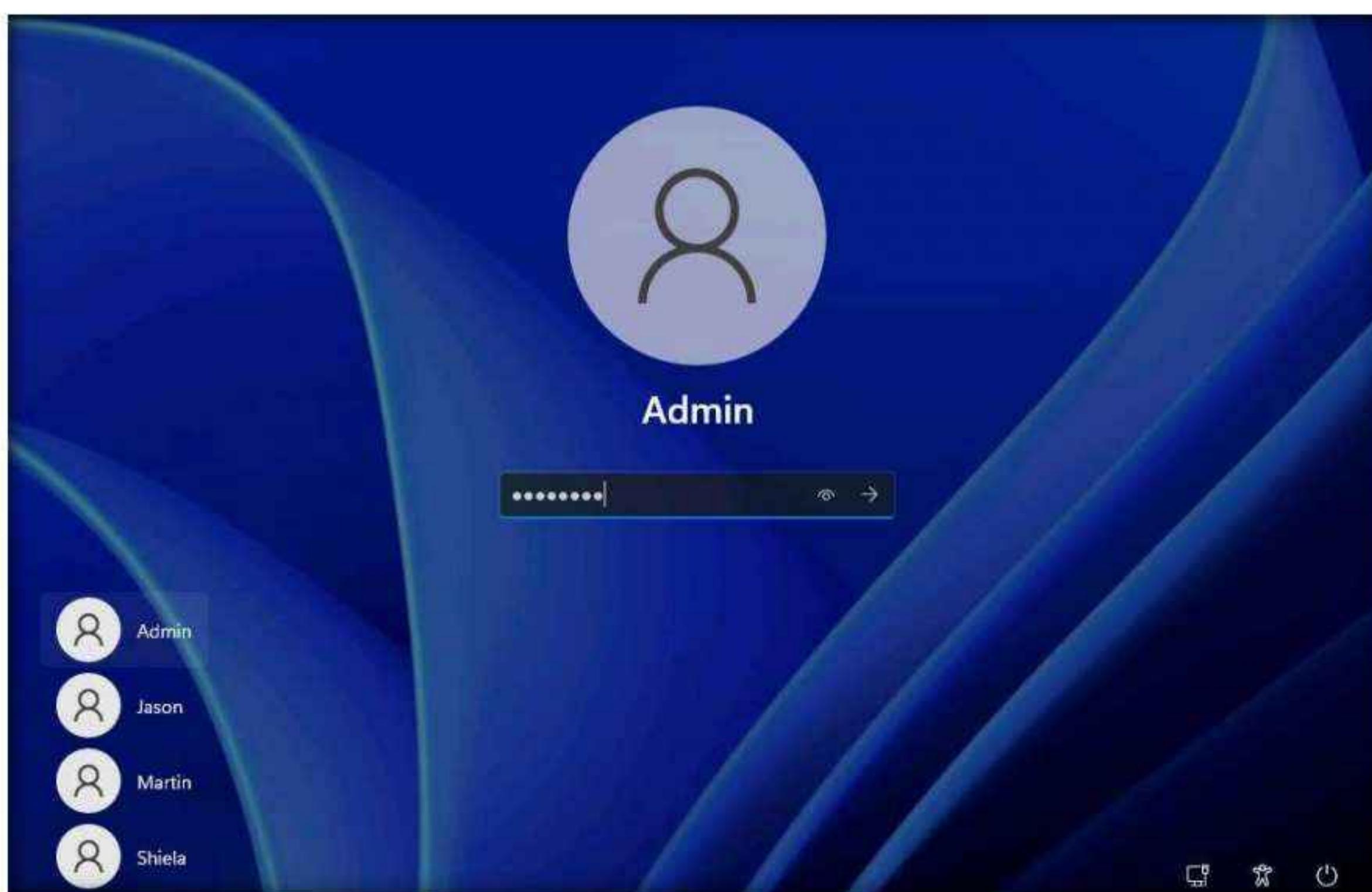
Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation.

**Note:** Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

**Note:** If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

**Note:** Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



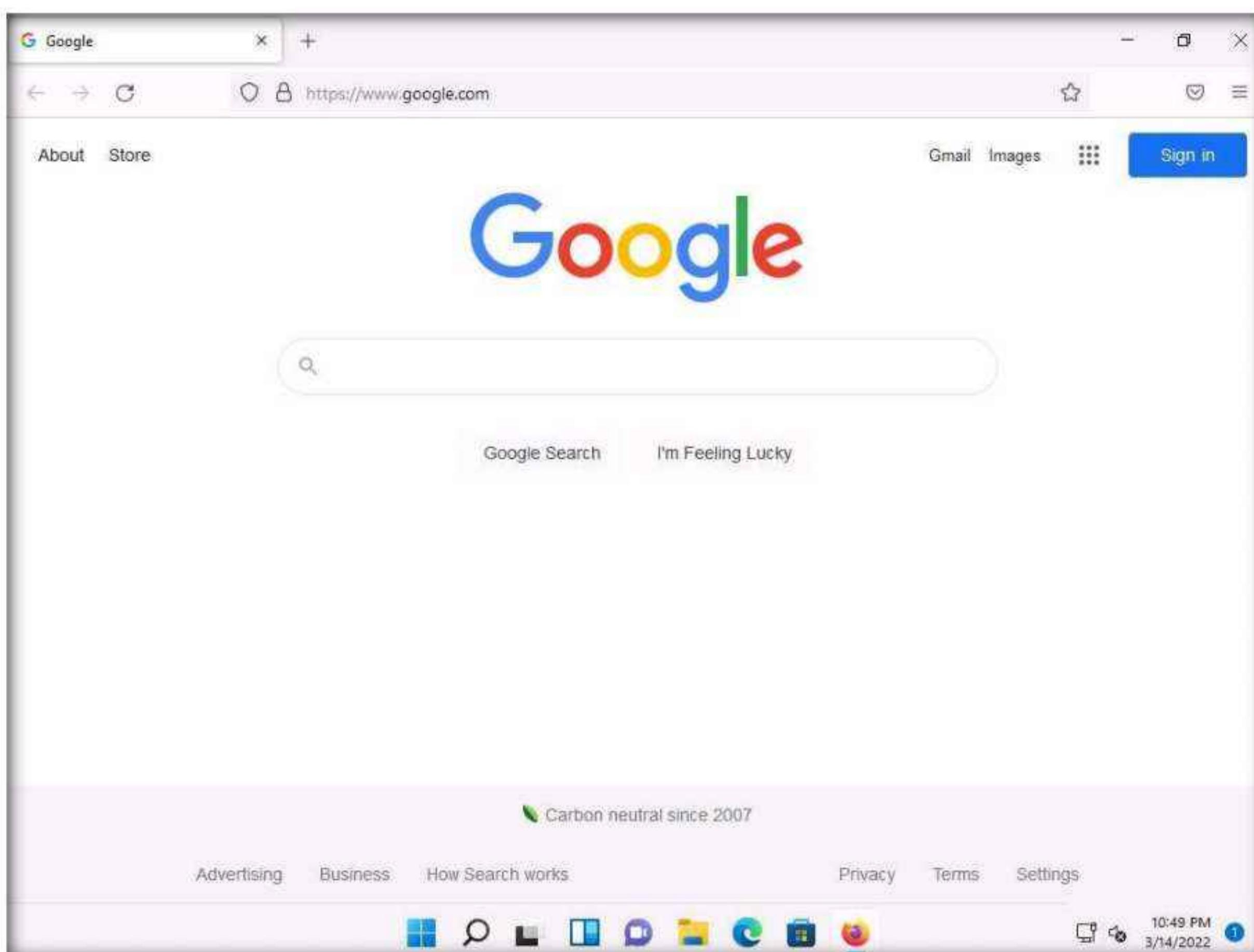
3. Launch any browser, in this lab, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.google.com** and press **Enter**.

**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 notification appears, click **Okay, Got it** to finish viewing the information.

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**.



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

**Note:** Here, this Advanced Google Search operator can help attackers and pen testers to extract login pages of the target organization's website. Attackers can subject login pages to various attacks such as credential brute-forcing, injection attacks and other web application attacks. Similarly, assessing the login pages against various attacks is crucial for penetration testing.

## Module 02 – Footprinting and Reconnaissance

The screenshot shows a Google search results page with the query "intitle:login site:eccouncil.org". The results list several login forms from the EC-Council website:

- <https://aspen.eccouncil.org> > Account > Login
- [Login - ASPEN - EC-Council](#)  
Type your username and password. Login. Username \*. Password \*
- <https://codered.eccouncil.org> > login
- [Login | CodeRed](#)  
Login to CodeRed for complete access to hundreds of classes by expert instructors!
- <https://ilabs.eccouncil.org> > login
- [Login to iLabs](#)  
May 18, 2017 — Get Connected to iLabs. Anytime. Anywhere. CEHproductimage, Computer Forensics Exercises, Security Analyst Exercises, Ec-Council Secure ...
- <https://cisomag.eccouncil.org> > tag > login-credentials
- [login credentials - Cyber Security Magazine - CISO Mag](#)  
Cybercriminals targeted around 1.3 million WordPress websites in a single day to steal database login credentials. It is found that... 2 years ago

6. Now, click back icon present on the top-left corner of the browser window to navigate back to <https://www.google.com>.

The screenshot shows the same Google search results page as before, but the back button in the browser's toolbar is highlighted with a red box. This indicates that the user is about to click the back button to return to the previous page.

## Module 02 – Footprinting and Reconnaissance

7. 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. The result might differ when you perform this task.

**Note:** The PDF and other documents from a target website may provide sensitive information about the target's products and services. They may help attackers to determine an attack vector to exploit the target.

EC-Council filetype:pdf

All News Books Videos Images More Tools

About 125,000,000 results (0.62 seconds)

<https://www.eccouncil.org> > CEHv11-Brochure PDF

**CERTIFIED ETHICAL HACKER v11 - EC-Council**

A Certified Ethical Hacker is a specialist typically working in a red team environment, focused on attacking computer systems and gaining access to networks ...  
13 pages

<https://www.eccouncil.org> > uploads > 2017/05 PDF

**Cyber-Handbook-Enterprise.pdf - EC-Council**

EC-Council creates content (course materials and exams) and certification delivered through our channel of authorized training centers which ...

**People also ask :**

Are EC-Council courses free?  
Is EC a Council of India?

**EC-Council EC-Council**

The International Council of Electronic Consultants is an American organization that provides cybersecurity certification, education, training, and services in various cybersecurity skills. EC-Council is headquartered in Albuquerque, New Mexico, USA. It has certified over 237,000 professionals from more than 150 countries. Wikipedia

**Founder:** Jay Bavisi  
**Headquarters location:** Albuquerque, NM

**EC-Council CEH book**

Ethical Hacking and Countermeasures, CEH V10, Threats and Defense Mechanisms

## Module 02 – Footprinting and Reconnaissance

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

Google search results for "EC-Council filetype:pdf". The first result is a link to "CERTIFIED ETHICAL HACKER v11 - EC-Council". The snippet shows it's a 13-page PDF. To the right, there's a sidebar with EC-Council's logo, a brief description, founder information, headquarters location, and links to CEH books.

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

PDF viewer showing the first page of the 'CEHv11-Brochure.pdf' document. The page features a man with glasses sitting at a keyboard, overlaid with various technical terms like 'Cloud Computing', 'Social Engineering', 'Vulnerability Analysis', 'Hacking Web Servers, Web Apps and Wireless Networks', 'Network Scanning', and 'System Hacking'.

10. 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.eccouncil.org]- Query returns the cached version of the website www.eccouncil.org
- **allinurl:** This operator restricts results to pages containing all the query terms specified in the URL.  
[allinurl: EC-Council career]—Query returns only pages containing the words “EC-Council” and “career” in the URL
- **inurl:** This operator restricts the results to pages containing the word specified in the URL  
[inurl: copy site:www.eccouncil.org]—Query returns only pages in EC-Council 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.eccouncil.org]—Finds pages that point to EC-Council’s home page
- **related:** This operator displays websites that are similar or related to the URL specified.  
[related:www.eccouncil.org]—Query provides the Google search engine results page with websites similar to eccouncil.org
- **info:** This operator finds information for the specified web page.  
[info:eccouncil.org]—Query provides information about the www.eccouncil.org home page
- **location:** This operator finds information for a specific location.  
[location: EC-Council]—Query give you results based around the term EC-Council

11. 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.
12. Close all open windows and document all the acquired information.

## Task 2: Gather Information from Video Search Engines

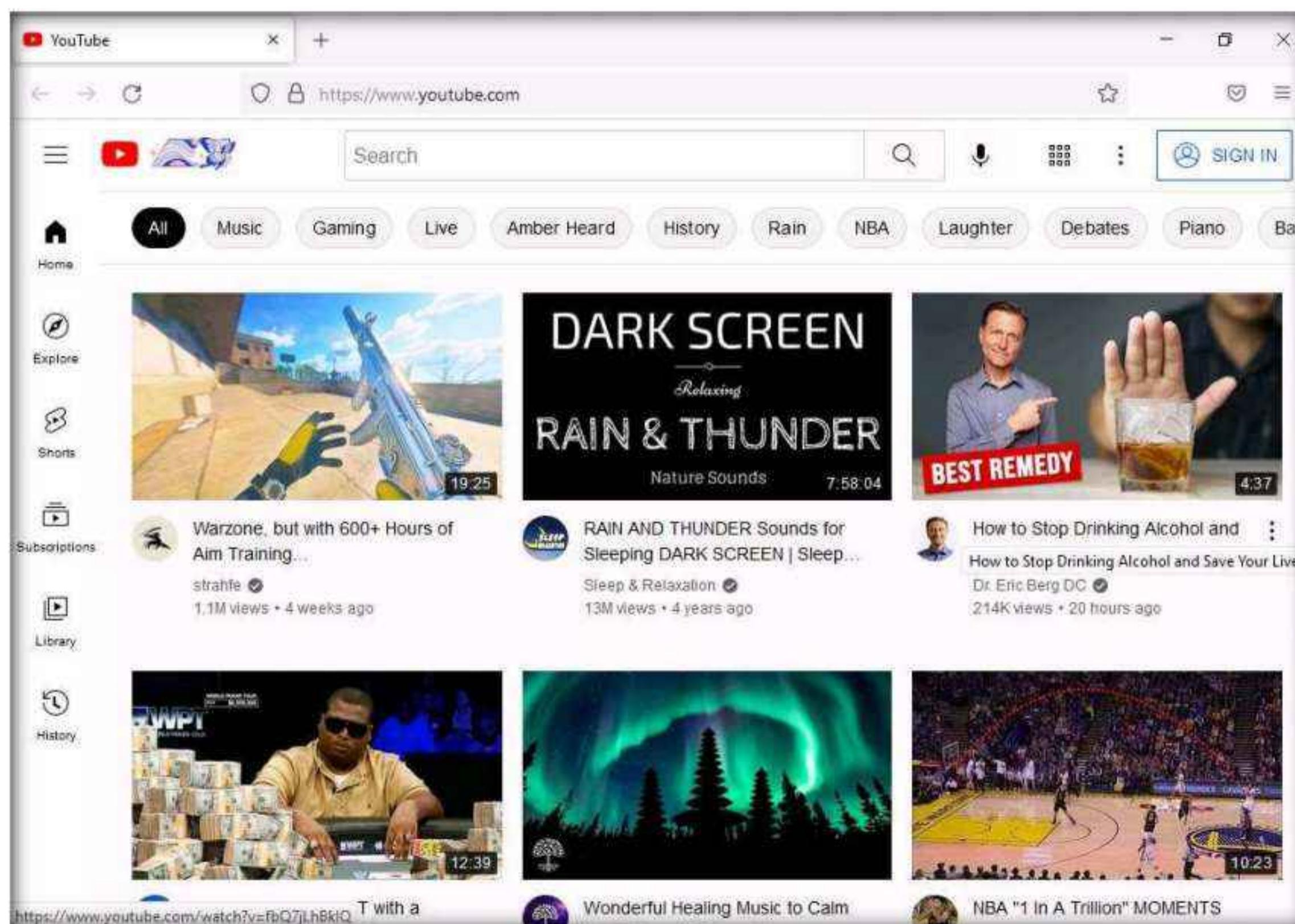
Video search engines are Internet-based search engines that crawl the web looking for video content. These search engines either provide the functionality of uploading and hosting the video content on their own web servers or they can parse the video content, which is hosted externally.

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

**Note:** Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

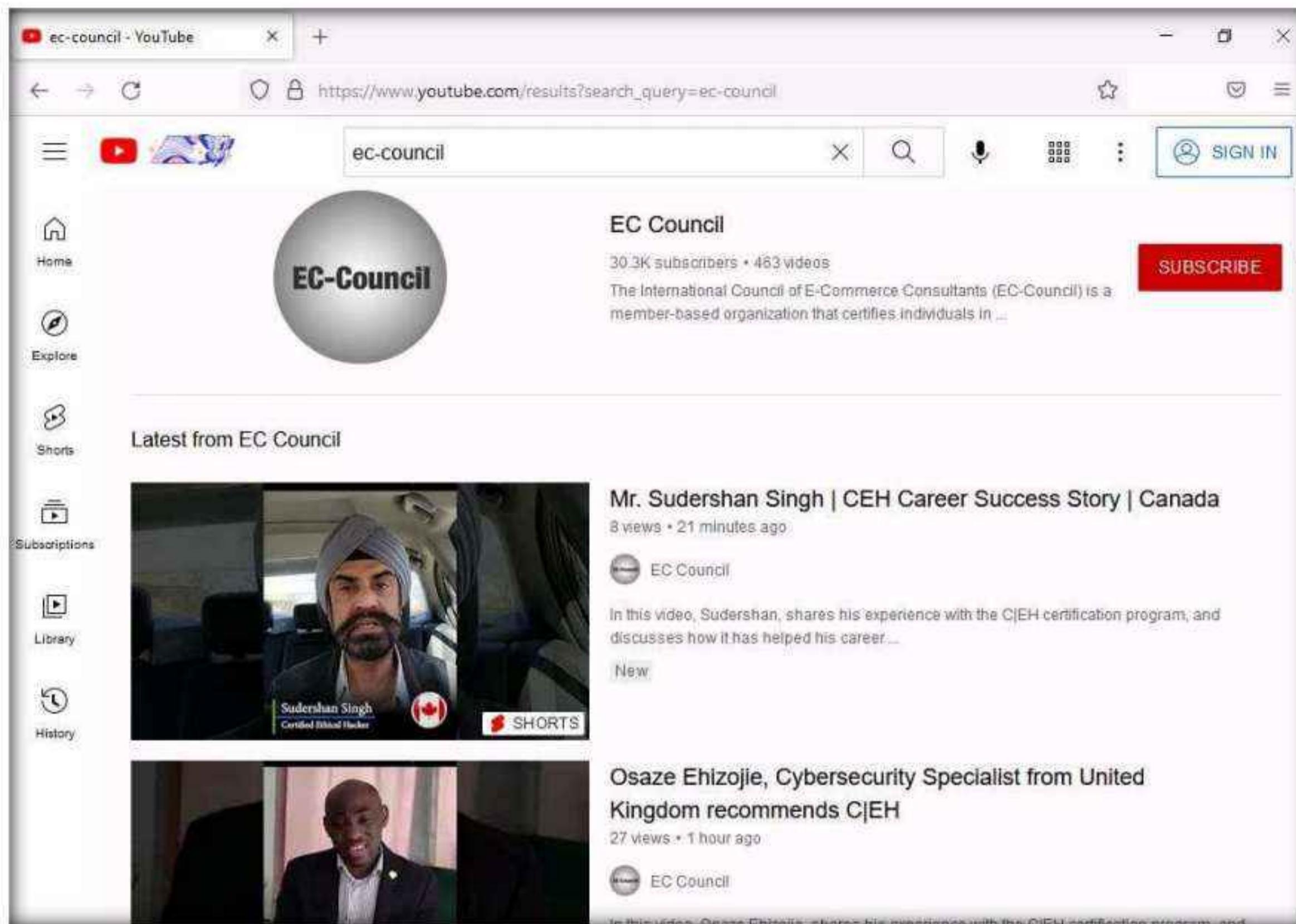
1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type <https://www.youtube.com> and press **Enter**. YouTube page appears as shown in the screenshot.

**Note:** If you choose to use another web browser, the screenshots will differ.

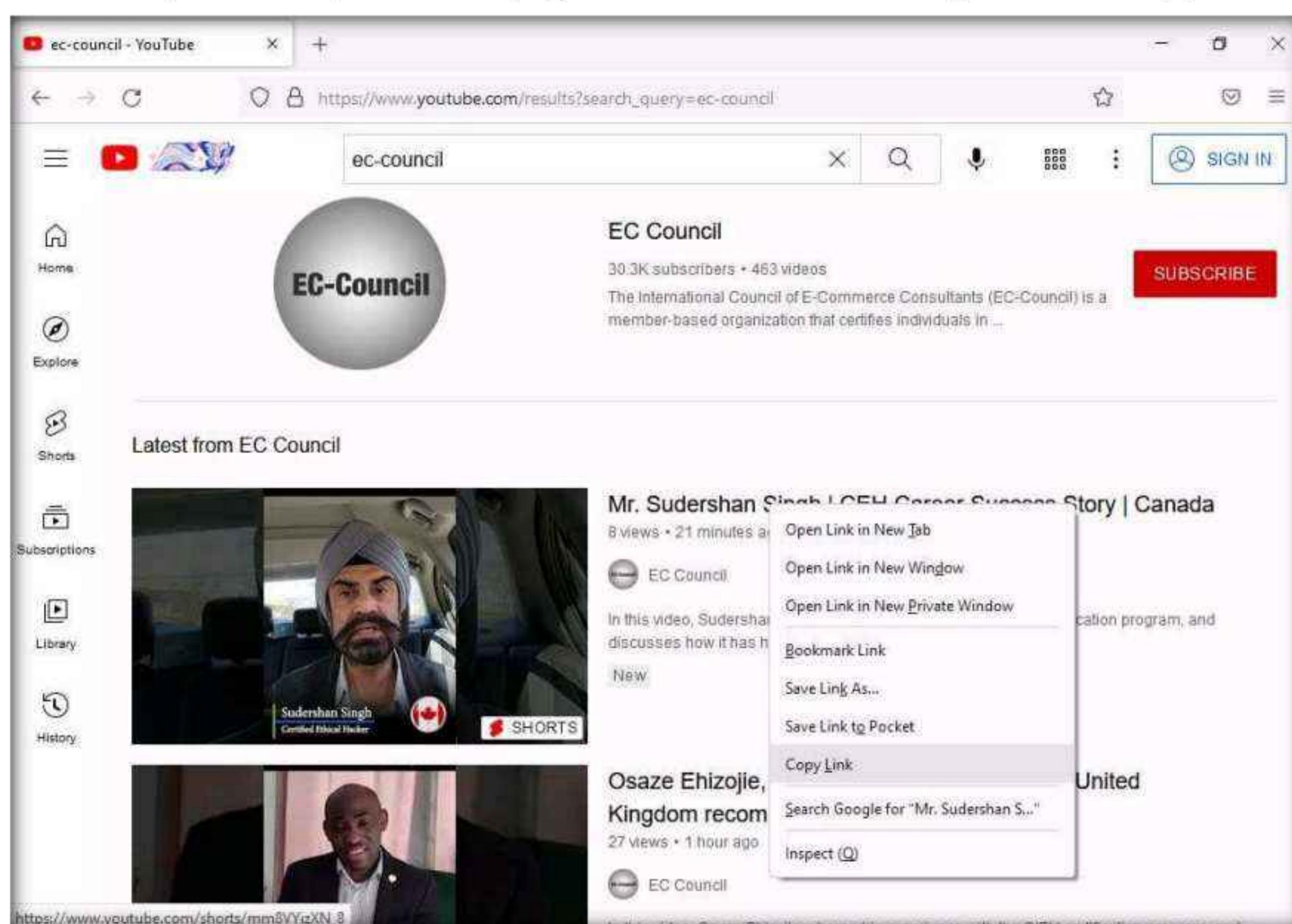


## Module 02 – Footprinting and Reconnaissance

2. In the search field, search for your target organization (here, **ec-council**). You will see all the latest videos uploaded by the target organization.



3. Select any video of your choice, right-click on the video title, and click **Copy Link**.



## Module 02 – Footprinting and Reconnaissance

- After the video link is copied, open a new tab in **Mozilla Firefox**, place your mouse cursor in the address bar and type <https://mattw.io/youtube-metadata/> and press **Enter**.

**Note:** To open a new tab, click + icon next to the first tab.

**Note: YouTube Metadata** tool collects singular details of a video, its uploader, playlist and its creator or channel.

01 YouTube Metadata Normal Bulk

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

Submit a link to a video, playlist, or channel

https://youtu.be/jaiVDqB\_NNw

Accepted formats

- [https://www.youtube.com/watch?v=video\\_id](https://www.youtube.com/watch?v=video_id)
- [https://youtube.com/shorts/video\\_id](https://youtube.com/shorts/video_id)
- [https://youtu.be/video\\_id](https://youtu.be/video_id)
- [https://www.youtube.com/playlist?list=playlist\\_id](https://www.youtube.com/playlist?list=playlist_id)
- [https://www.youtube.com/channel/channel\\_id](https://www.youtube.com/channel/channel_id)
- <https://www.youtube.com/user/username>
- [https://www.youtube.com/c/custom\\_url](https://www.youtube.com/c/custom_url) (may not work, see here)
- [https://www.youtube.com/custom\\_url](https://www.youtube.com/custom_url) (may not work, see here)
- Also accepts direct ids: [video\\_id](#), [playlist\\_id](#), [channel\\_id](#)

Export & Share

Save this result as a zip file or load from a previous export. Drag and drop supported.

Export Import

Contains file(s)

- YouTube Metadata** page appears, in the **Submit a link to a video, playlist, or channel** search field, paste the copied YouTube video location and click **Submit**.

01 YouTube Metadata Normal Bulk

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

Submit a link to a video, playlist, or channel

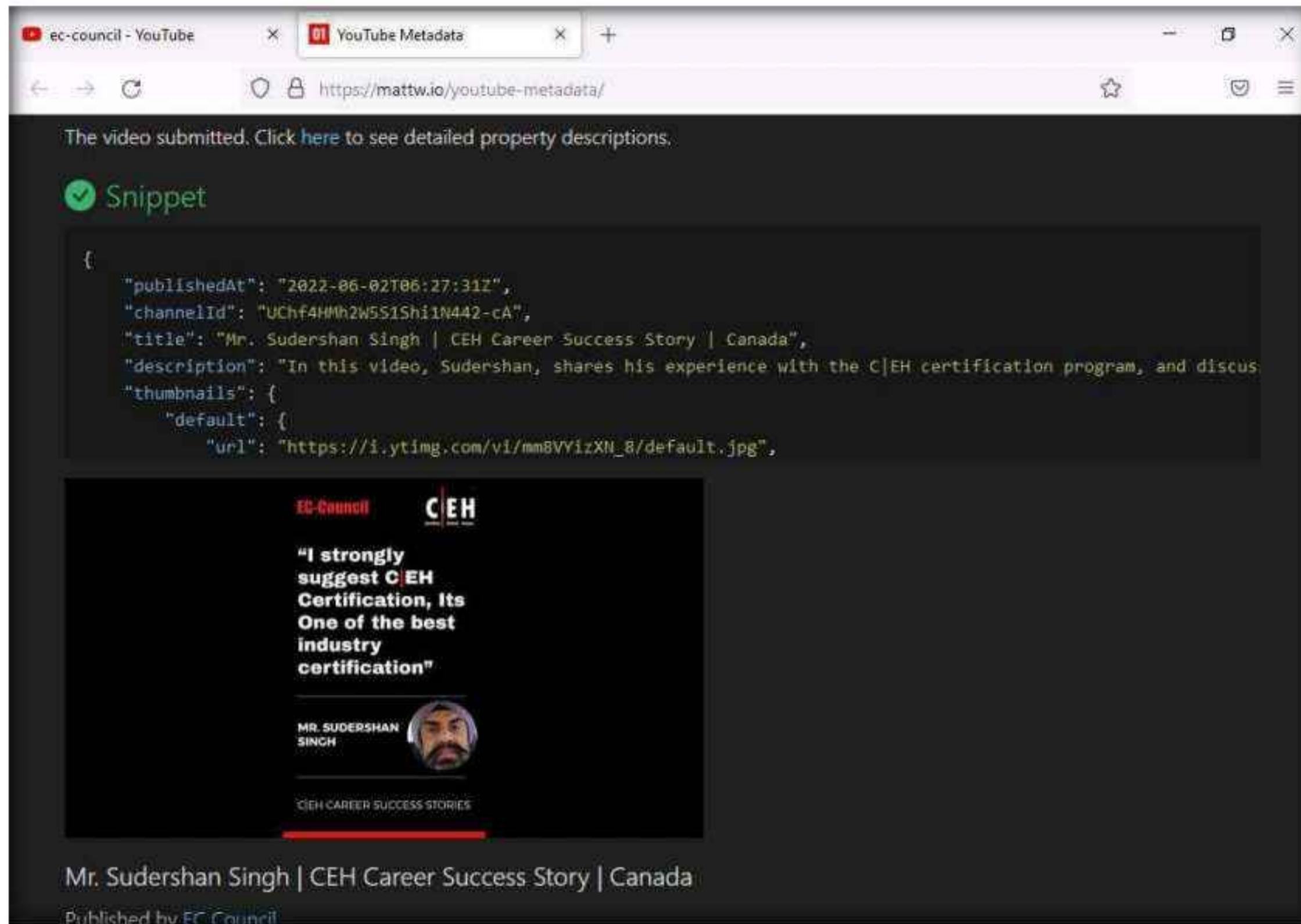
https://www.youtube.com/shorts/mm8VYizXN\_8

Accepted formats

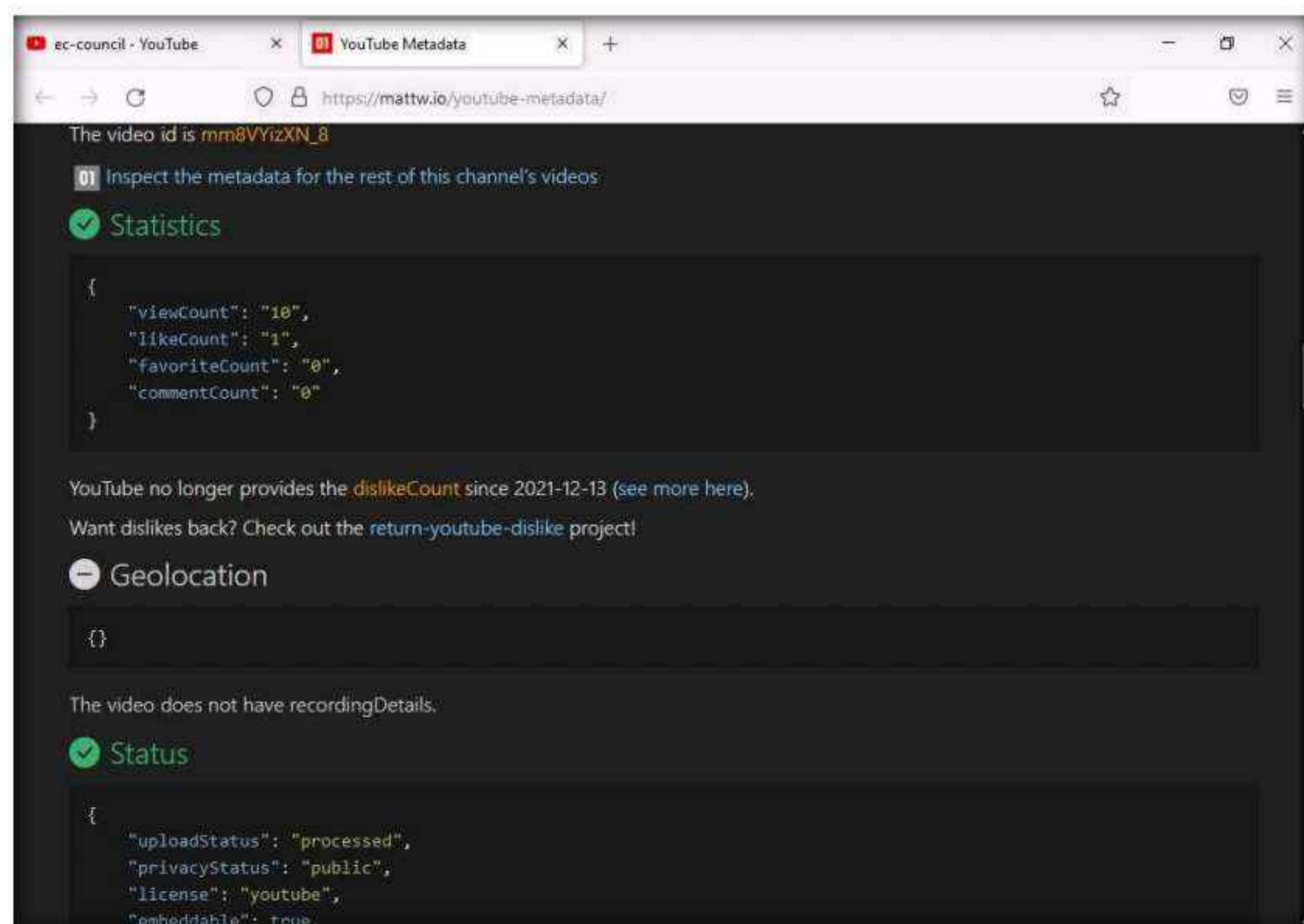
- [https://www.youtube.com/watch?v=video\\_id](https://www.youtube.com/watch?v=video_id)
- [https://youtube.com/shorts/video\\_id](https://youtube.com/shorts/video_id)
- [https://youtu.be/video\\_id](https://youtu.be/video_id)
- [https://www.youtube.com/playlist?list=playlist\\_id](https://www.youtube.com/playlist?list=playlist_id)
- [https://www.youtube.com/channel/channel\\_id](https://www.youtube.com/channel/channel_id)
- <https://www.youtube.com/user/username>

**Module 02 – Footprinting and Reconnaissance**

- Once the search is completed scroll down and you can observe the details related to the video such as **published date and time**, **channel Id**, **title**, etc., in the **Snippet** section.



7. Scroll down to check the additional information under the sections **Statistics**, **Geolocation**, **Status**, etc.



## Module 02 – Footprinting and Reconnaissance

- Under the **Thumbnail** section you can find the reverse image search results, click on the **Click to reverse image search** button under any thumbnail.

The screenshot shows a web browser window with three tabs: 'ec-council - YouTube', 'YouTube Metadata', and the current tab 'https://mattw.io/youtube-metadata/'. The main content area is titled 'Knowledge' and contains a section for 'Thumbnails'. It says 'Reverse image search all four thumbnail images.' Below this are four thumbnail images, each with a 'Click to reverse image search' button at the bottom. There is also a 'More' section with links to various sources.

- Archive.org (details) - youtube-mm8VYizXN\_8
- Archive.org (direct video 1) - mm8VYizXN\_8
- Archive.org (direct video 2) - mm8VYizXN\_8
- Archive.org (search) - Mr. Sudershan Singh | CEH Career Success Story | Canada
- Archive.org (web) - https://www.youtube.com/watch?v=mm8VYizXN\_8
- Filmot.com - https://filmot.com/video/mm8VYizXN\_8
- Google - "Mr. Sudershan Singh | CEH Career Success Story | Canada"
- Google - "mm8VYizXN\_8"

- A new tab in Google appears, and the results for the reverse image search are displayed.

The screenshot shows a Google search results page. The search query in the bar is 'language'. Below the search bar, there are filters for 'All', 'Images', 'Maps', 'Shopping', and 'More'. The results section shows one image result with the URL 'https://en.wikipedia.org/wiki/Language'. A snippet from Wikipedia defines language as a structured system of communication. Below the image result, there is a snippet from Britannica about language as a system of conventional spoken, manual (signed), or written symbols by means of which human beings, as members of a social group and participants...

- This concludes the demonstration of gathering information from the advanced video search and reverse image search using the YouTube search engine and YouTube Metadata tool.

11. You can use other video search engines such as **Google videos** (<https://www.google.com/videohp>), **Yahoo videos** (<https://in.video.search.yahoo.com>), etc.; video analysis tools such as **EZGif** (<https://ezgif.com>), **VideoReverser.com** (<https://www.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.
12. Close all open windows and document all acquired information.

## Task 3: Gather Information from FTP Search Engines

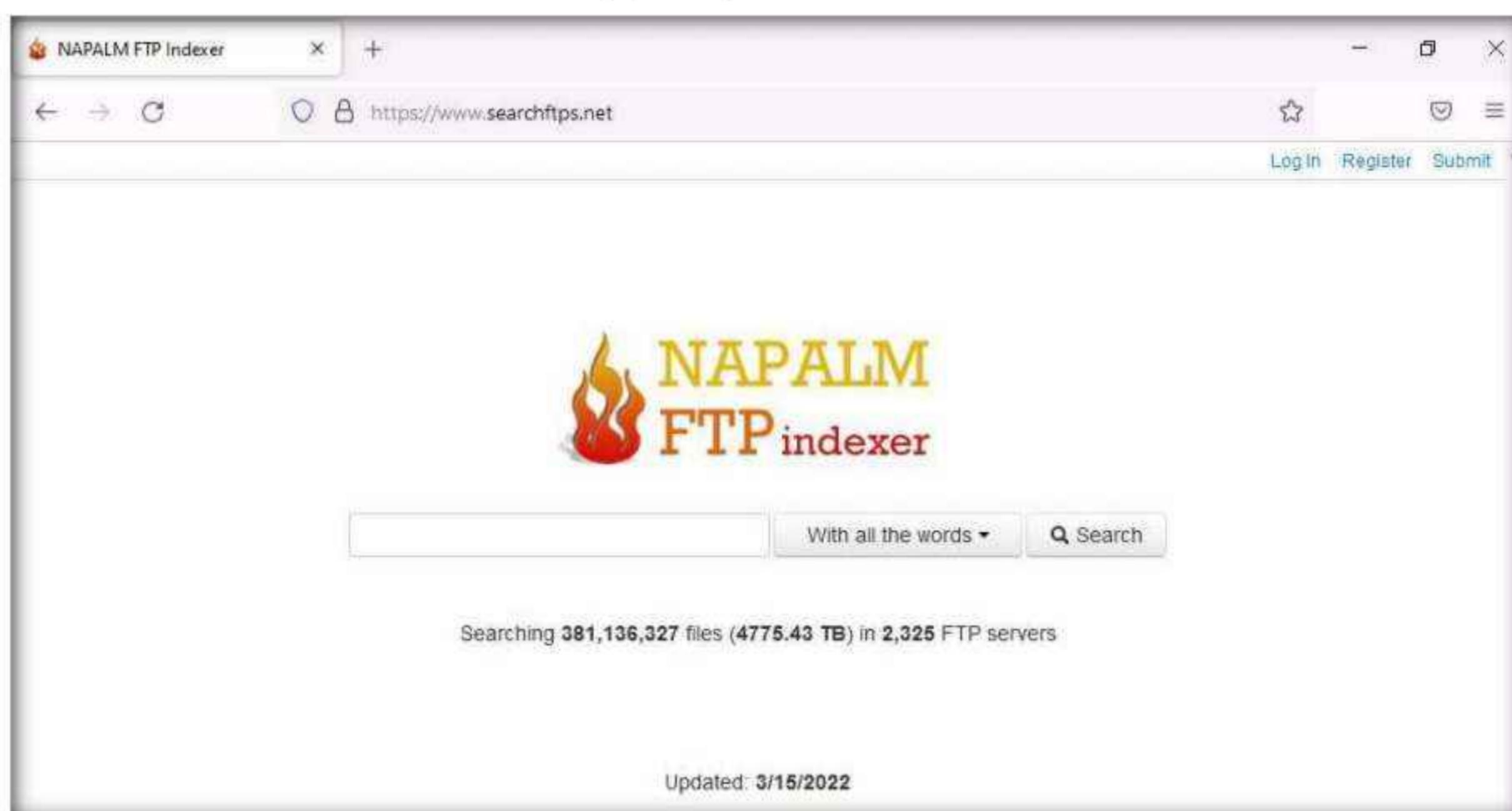
File Transfer Protocol (FTP) search engines are used to search for files located on the FTP servers; these files may hold valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to keep large file archives and other software that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

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

1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type <https://www.searchftps.net/> and press **Enter**.

**Note:** If you choose to use another web browser, the screenshots will differ.

2. NAPALM FTP indexer website appears, as shown in the screenshot.



## Module 02 – Footprinting and Reconnaissance

3. In the search bar, type **microsoft** and click **Search**.



4. You will get the search results containing critical files and documents related to the target organization, as shown in the screenshot.

A screenshot of the same NAPALM FTP Indexer search results page for "microsoft". The search bar now shows "microsoft". Below the search bar, it says "Showing results 0 to 19 of about 10000 for 'microsoft'". There are several download links listed:

- /linux/fedora-updates/32/Everything/ppc64le/Packages/p/ php-microsoft-tolerant-php-parser-0.0.23-1.fc32.noarch.rpm 85.6 KB DOWNLOAD
- /.../linux-fedora-buffer/fedora-secondary/development/35/Everything/s/390x/os/Packages/p/ php-microsoft-tolerant-php-parser-0.1.1-1.fc35.noarch.rpm 85.0 KB DOWNLOAD
- /pub/RedHat/fedora/linux/releases/35/Everything/x86\_64/os/Packages/p/ php-microsoft-tolerant-php-parser-0.1.1-1.fc35.noarch.rpm 85.0 KB DOWNLOAD
- /pub/RedHat/fedora/linux/releases/35/Everything/x86\_64/os/Packages/a/ ansible-collection-microsoft-sql-1.1.0-2.fc35.noarch.rpm 43.9 KB DOWNLOAD

Each download link includes a timestamp (e.g., "Last checked: 2022-03-14 20:58"), a "Similar files" link, and a "Browse" link. At the bottom right, it says "Tuesday, March 15, 2022".

5. This concludes the demonstration of gathering information from the FTP search engine.
6. You can also use FTP search engines such as **FreewareWeb FTP File Search** (<https://www.freewareweb.com>) to gather crucial FTP information about the target organization.
7. Close all open windows and document all the acquired information.

## Task 4: Gather Information from IoT Search Engines

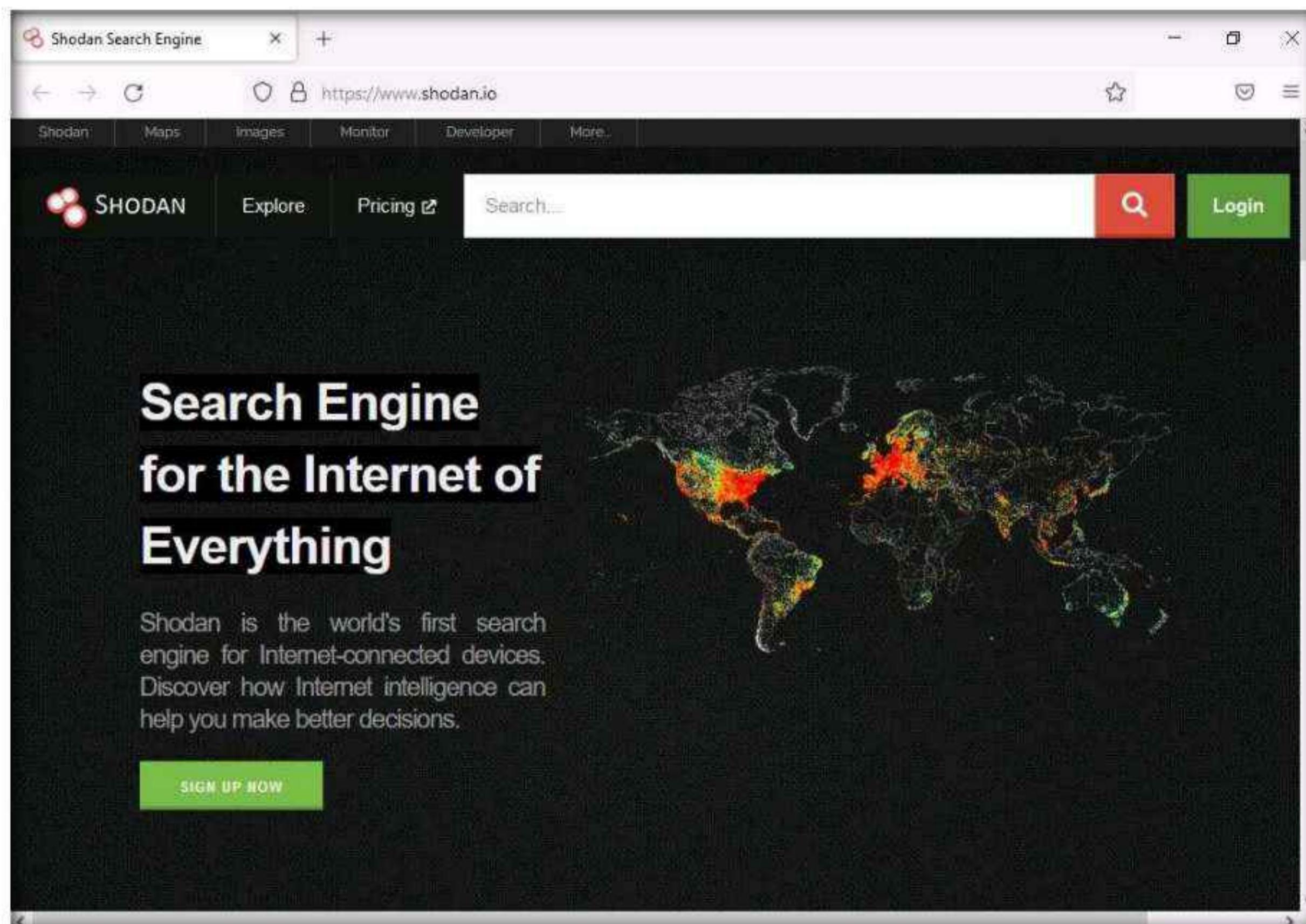
IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances,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

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 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type <https://www.shodan.io/> and press **Enter**.

**Note:** If you choose to use another web browser, the screenshots will differ.

2. **Shodan** page appears, as shown in the screenshot.



3. In the search bar, type **amazon** and press **Enter**.

**Note:** Here, we are searching for publicly available information on the target **amazon**. However, you can search on a target of your choice.

4. 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.

The screenshot shows the Shodan search interface with the query "amazon". The results page displays a total of 1,613,565 findings. On the left, there's a "TOP COUNTRIES" section with a world map and a table of top countries and their counts. On the right, there's a detailed view for the IP address 23.21.47.223, which is associated with an Amazon Data Services Nova instance in the United States. The SSL certificate details are shown, including the common name (ip-10-236-69-171), issuer (Amazon), and supported SSL versions (TLSv1, TLSv1.1, TLSv1.2). The page also includes a "TOP PORTS" section and a "301 Moved Permanently" entry for port 80.

5. This concludes the demonstration of gathering vulnerable IoT information using the Shodan search engine.
6. You can also use **Censys** (<https://censys.io>) IoT search engine, to gather information such as manufacturer details, geographical location, IP address, hostname, open ports, etc.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 11** virtual machine.

## Lab Analysis

Analyze and document the results of this lab exercise.

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

### Internet Connection Required

Yes

No

### Platform Supported

Classroom

CyberQ

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

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

### Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

### 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

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.

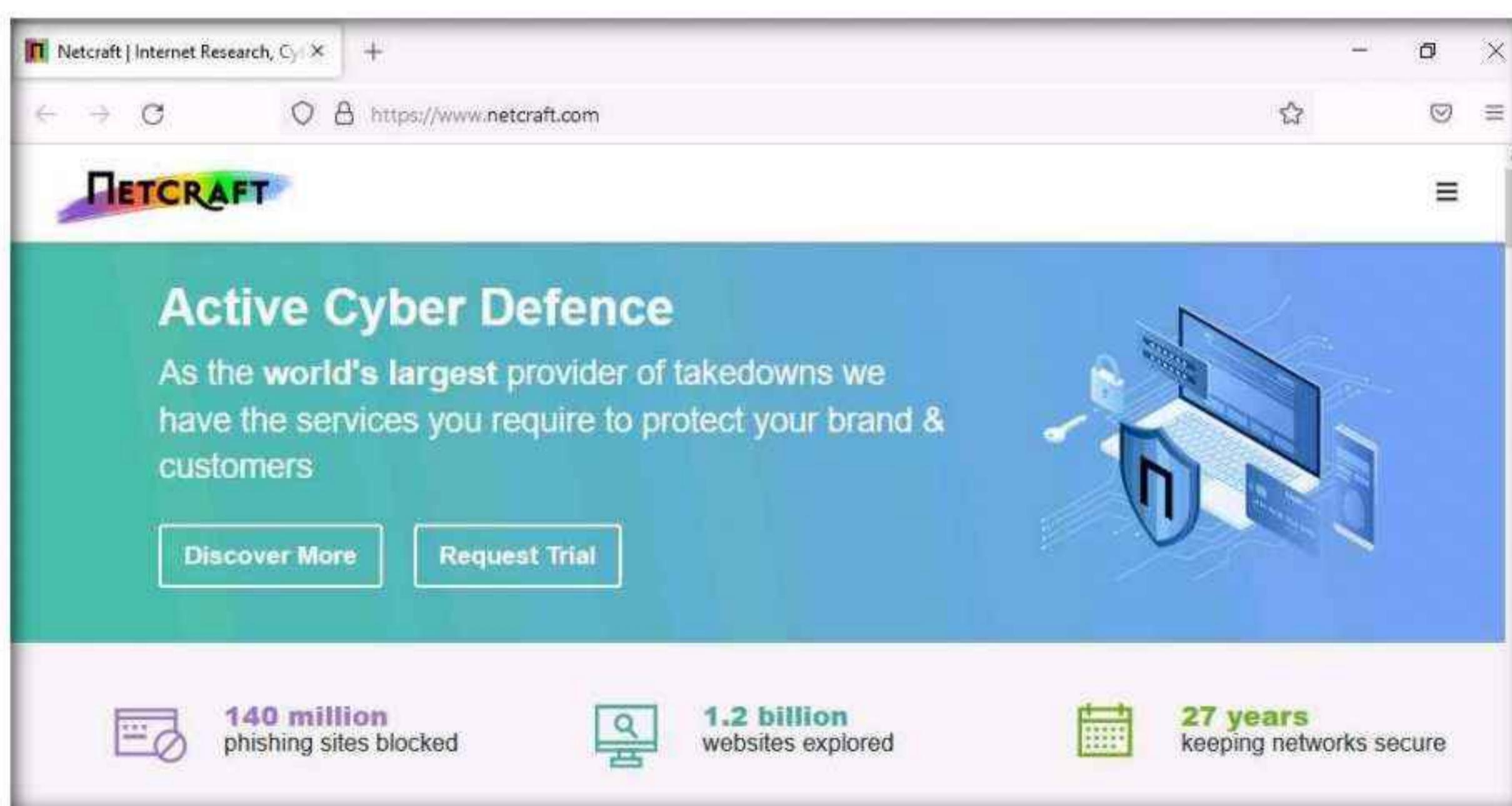
Here, we will extract the company's domains and sub-domains using the Netcraft web service.

1. Turn on the **Windows 11** virtual machine.
2. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type <https://www.netcraft.com> and press **Enter**.

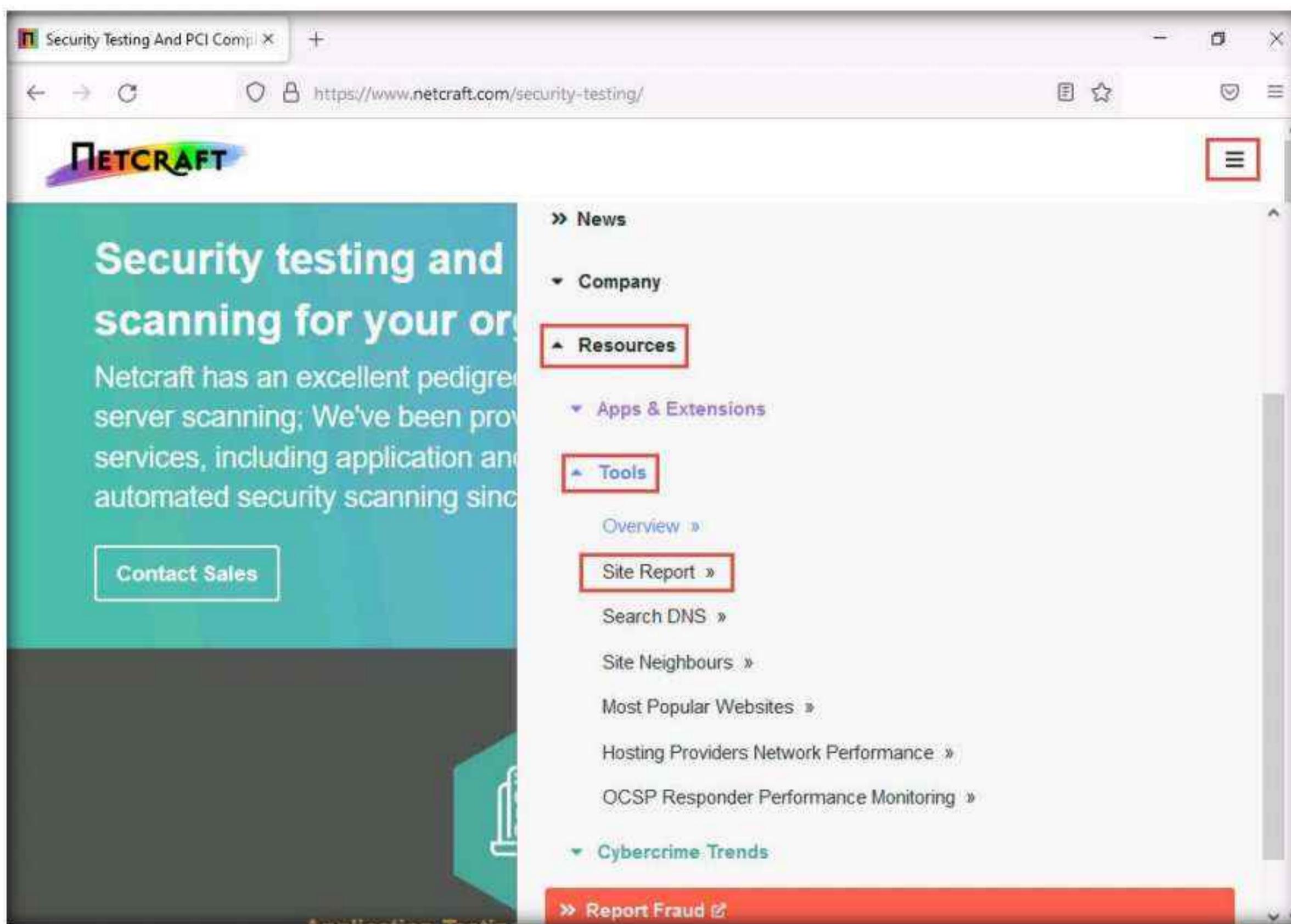
**Note:** If you choose to use another web browser, the screenshots will differ.

3. **Netcraft** page appears, as shown in the screenshot.

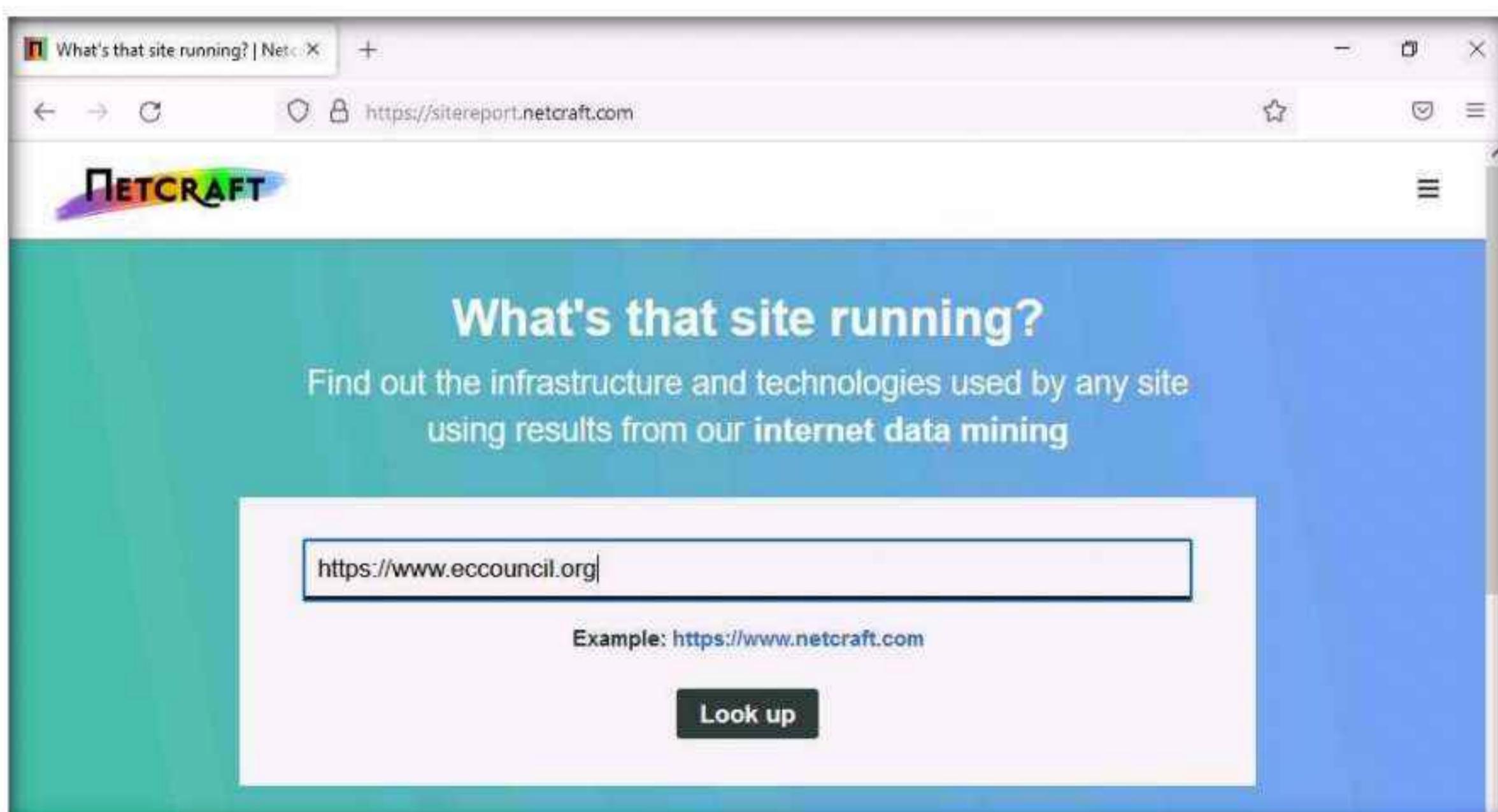
**Note:** If cookie pop-up appears at the lower section of the browser, click **Accept**.



4. Click on menu icon from the top-right corner of the page and navigate to the **Resources** -> **Tools** -> **Site Report**.



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 **Look up** button, as shown in the screenshot.



## Module 02 – Footprinting and Reconnaissance

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.

The screenshot shows the Netcraft Site report for <https://www.eccouncil.org>. The report includes sections for Background, Network, and Hosting History. In the Network section, the 'Domain' field for the site URL contains a link to [eccouncil.org](https://www.eccouncil.org).

**Background**

Site title	Certified Ethical Hacker   InfoSec Cyber Security Certification   EC-Council	Date first seen	March 2003
Site rank	1719	Netcraft Risk Rating	0/10
Description	EC-Council is a global leader in InfoSec Cyber Security certification programs like Certified Ethical Hacker and Computer Hacking Forensic Investigator.	Primary language	English

**Network**

Site	Domain	eccouncil.org
Netblock Owner	Cloudflare, Inc.	Nameserver
Hosting company	Cloudflare	Domain registrar
Hosting country	US	Nameserver organisation

7. In the **Network** section, click on the website link (here, [eccouncil.org](https://www.eccouncil.org)) in the **Domain** field to view the subdomains.

The screenshot shows the Netcraft Site report for <https://www.eccouncil.org>. The report includes sections for Background, Network, and Hosting History. In the Network section, the 'Domain' field for the site URL now displays the subdomains of [eccouncil.org](https://www.eccouncil.org).

**Background**

Site title	Certified Ethical Hacker   InfoSec Cyber Security Certification   EC-Council	Date first seen	March 2003
Site rank	1719	Netcraft Risk Rating	0/10
Description	EC-Council is a global leader in InfoSec Cyber Security certification programs like Certified Ethical Hacker and Computer Hacking Forensic Investigator.	Primary language	English

**Network**

Site	Domain	eccouncil.org
Netblock Owner	Cloudflare, Inc.	Nameserver
Hosting company	Cloudflare	Domain registrar
Hosting country	US	Nameserver organisation
IPv4 address	104.18.21.251 (VirusTotal)	Organisation
IPv4 autonomous systems	AS13335	DNS admin
IPv6 address	2606:4700:0:0:0:6812:15fb	Top Level Domain
IPv6 autonomous systems	AS13335	DNS Security Extensions
Reverse DNS	unknown	

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

The screenshot shows a browser window displaying the Netcraft search results for hostnames matching \*.eccouncil.org. The URL in the address bar is https://searchdns.netcraft.com/?host=\*.eccouncil.org. The page title is "Hostnames matching \*.eccouncil.org". There is a search bar with the placeholder "Search with another pattern?". Below the search bar, it says "17 results". A table follows, showing the following data:

Rank	Site	First seen	Netblock	OS	Site Report
838	aspen.eccouncil.org	June 2010	Cloudflare, Inc.	Linux	
1179	iclass.eccouncil.org	October 2009	Cloudflare, Inc.	unknown	
1356	codered.eccouncil.org	January 2020	Cloudflare, Inc.	Linux	
1487	cyberq.eccouncil.org	October 2018	Cloudflare, Inc.	Linux	
1724	www.eccouncil.org	February 2002	Cloudflare, Inc.	Linux	
8978	cert.eccouncil.org	March 2012	Cloudflare, Inc.	Linux	
11578	store.eccouncil.org	July 2013	Cloudflare, Inc.	Linux	Tuesday, March 15, 2022

The bottom of the screen shows a Windows taskbar with various icons and the date/time: 2:43 AM, 3/15/2022.

9. This concludes the demonstration of finding the company's domains and sub-domains using the Netcraft tool. The attackers can use this collected list of subdomains to perform web application attacks on the target organization such as injection attacks, brute-force attacks and Denial-of-Service (DoS) attacks.
10. 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.
11. Close all open windows and document all the acquired information.

## Task 2: Gather Personal Information using 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.

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

**Note:** Here, we are gathering information about **Satya Nadella** from **Microsoft** company.

1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type <https://www.peekyou.com> and press **Enter**.

**Note:** If you choose to use another web browser, the screenshots will differ.

2. **PeekYou** page appears, as shown in the screenshot.

**Note:** If cookie pop-up appears at the lower section of the browser, click **I agree**.



3. 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.

**Note:** The list of location might differ in your lab environment.



## Module 02 – Footprinting and Reconnaissance

4. The people search begins, and the best matches for the provided search parameters will be displayed.
5. The result shows information such as public records, background details, email addresses, contact information, address history, etc. This information helps attackers to perform phishing, social engineering, and other types of attacks.

The screenshot shows a web browser window for the URL [https://www.peekyou.com/usa/district\\_of\\_columbia/satya\\_nadella](https://www.peekyou.com/usa/district_of_columbia/satya_nadella). The search interface includes fields for Name (Satya) and Location (Nadella). A large green 'START' button is prominent. To the right of the search bar is an 'Easy Search Tool' icon with instructions: 1. Click 'Start', 2. Add Easy Search Tool™, 3. Enjoy Extension. Below the search bar, there are links for Public Records, Facebook, Instagram, Twitter, Email, and Images. The main results section is titled 'Public Records & Background Search' and lists three entries for 'Satya Nadella' with 'View Full Report' links. It also includes sections for 'Arrest Records & Driving Infractions' and 'Phonebook'. The bottom right corner of the browser window shows the date and time as 3:42 AM 3/15/2022.

6. You can further click on **View Full Report** hyperlink to view detailed information about the 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 person.

7. Scroll down to view the entire information about the person.

The screenshot shows a web browser window with the URL [https://www.peekyou.com/usa/district\\_of\\_columbia/satya\\_nadella](https://www.peekyou.com/usa/district_of_columbia/satya_nadella). The page displays search results for 'Satya Nadella' under the heading 'Phonebook'. It lists several items with 'Search Details' links:

- 1) Satya Nadella's Phone & Current Address
- 2) Social Media Profiles & More
- 3) Satya Nadella's Phone #, Address & More
- 4) Satya Nadella's Contact Info, Social Profiles & More

Below this, there is a section titled 'Email Addresses' with a list of email addresses:

- View Satya's Hidden Profiles on Facebook and 60+ Networks, satya\*\*\*\*@gmail
- View Satya's Hidden Profiles on Facebook and 60+ Networks, satya\*\*\*\*@yahoo
- View Satya's Hidden Profiles on Facebook and 60+ Networks, satya\*\*\*\*@hotmail
- View Satya's Hidden Profiles on Facebook and 60+ Networks, satya\*\*\*\*@aol
- View Satya's Hidden Profiles on Facebook and 60+ Networks, satya\*\*\*\*@outlook

At the bottom of the search results, there is a 'Contact Information & Address History' section featuring a search bar and a 'SEARCH DETAILS' button. The browser interface includes standard navigation buttons, a search bar, and a taskbar at the bottom.

8. This concludes the demonstration of gathering personal information using the PeekYou online people search service.
9. You can also use Spokeo (<https://www.spokeo.com>), **pipl** (<https://pipl.com>), **Intelius** (<https://www.intelius.com>), **BeenVerified** (<https://www.beenverified.com>), etc., people search services to gather personal information of key employees in the target organization.
10. Close all open windows and document all the acquired information.

### Task 3: Gather an Email List using theHarvester

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.

**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.

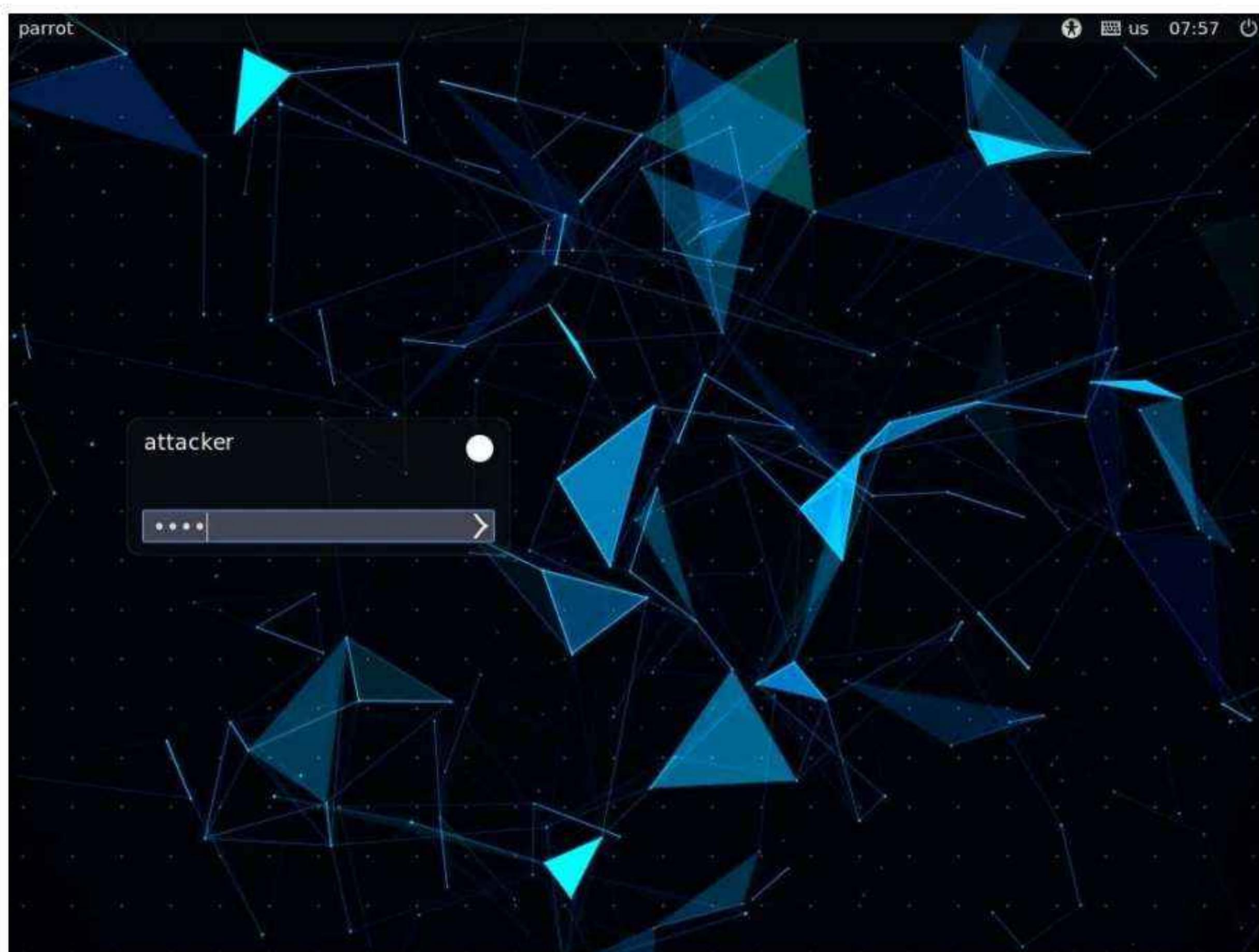
Here, we will gather the list of email IDs related to a target organization using theHarvester tool.

**Note:** Here, we will consider **Microsoft** as a target organization. However, you can select a target organization of your choice.

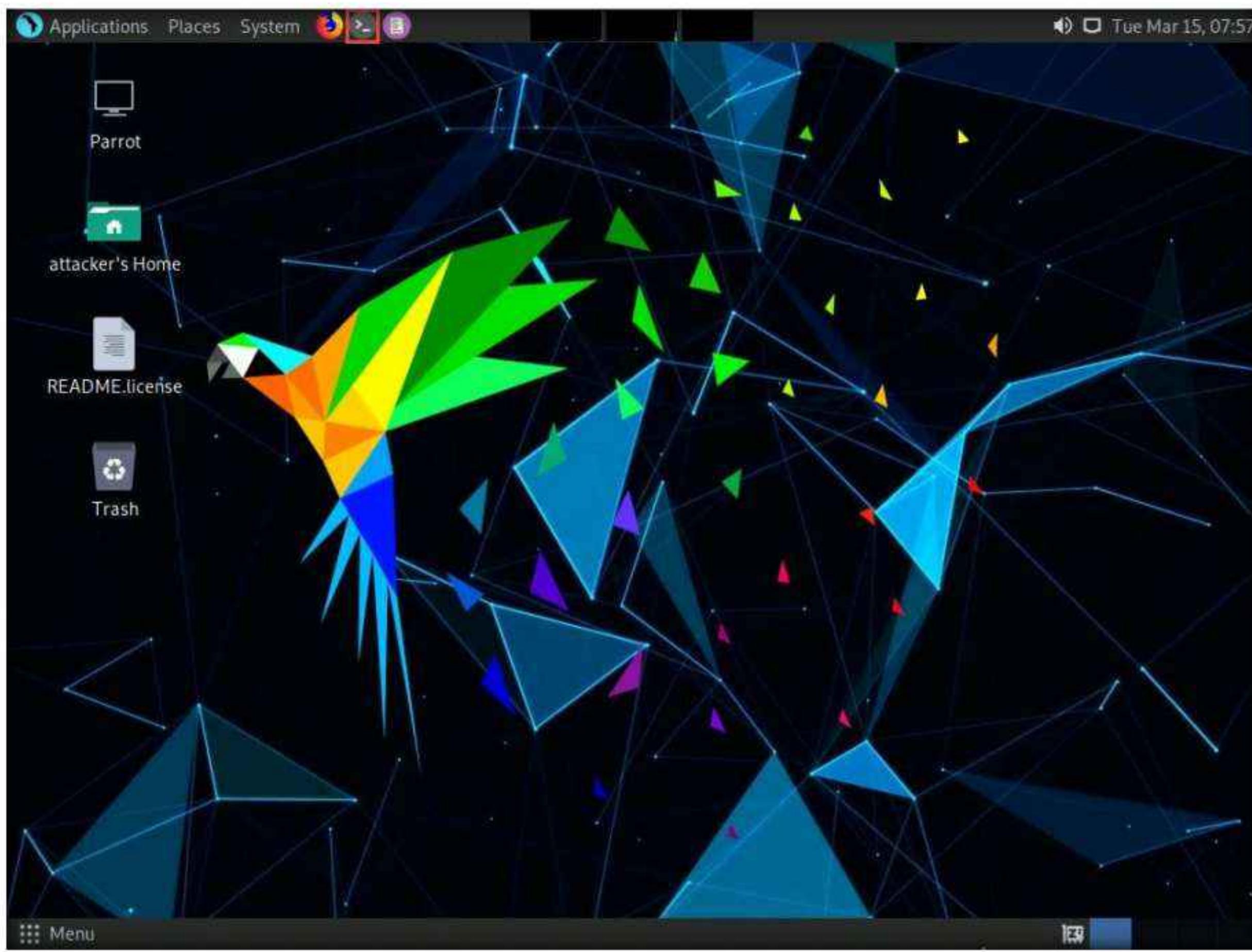
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

**Note:** 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** 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.

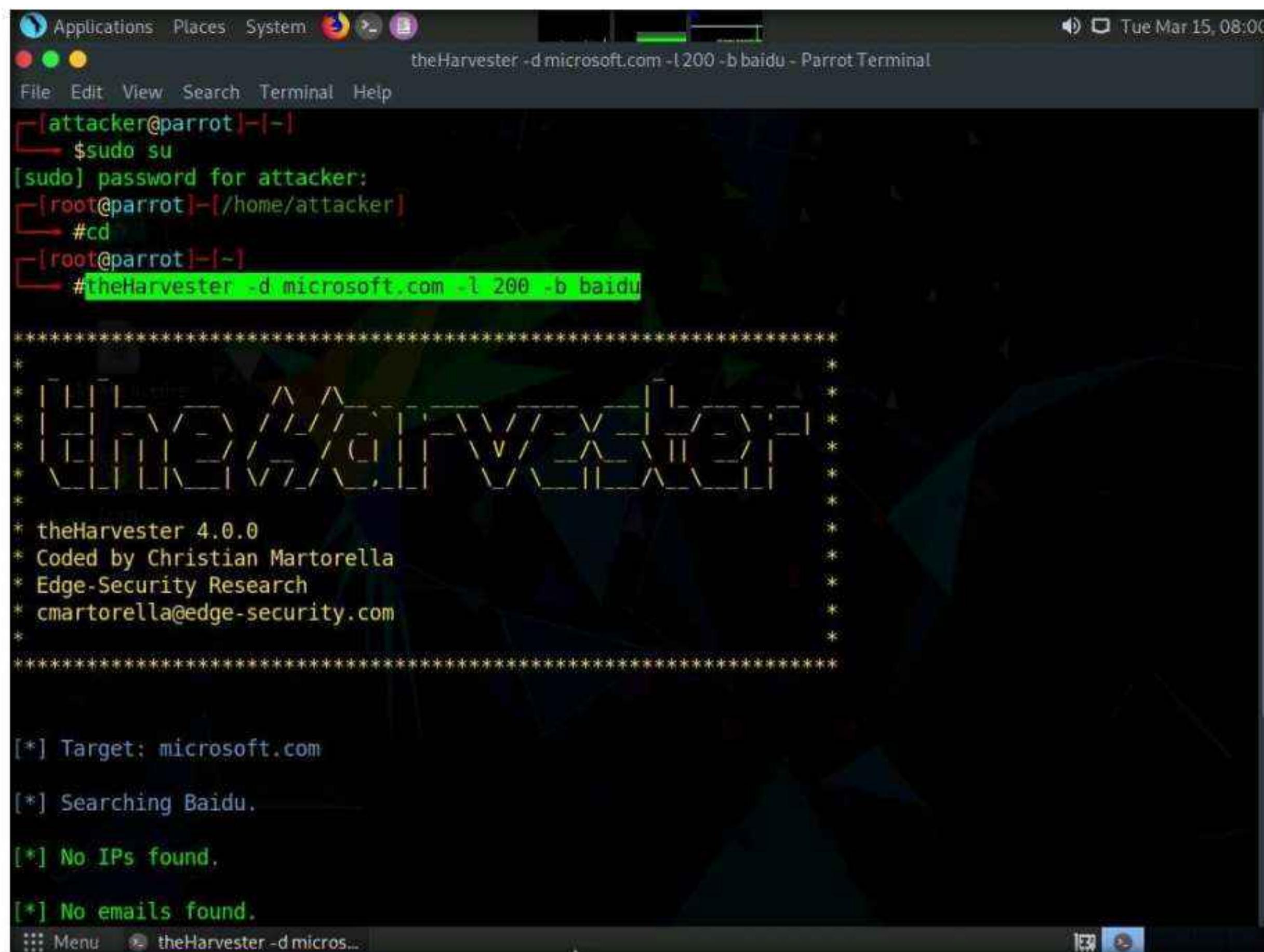
A screenshot of the Parrot Terminal window. The title bar says "cd - Parrot Terminal". The window shows a command-line session:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
#
```

The terminal uses color-coded syntax highlighting for commands and output. The user's input is in red, and the system responses are in green. The terminal window has a dark background with a green gradient bar at the top.

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.



The screenshot shows a terminal window titled "theHarvester -d microsoft.com -l 200 -b baidu - Parrot Terminal". The terminal session starts with the user "attacker" at the root prompt, entering "sudo su" and providing a password. The user then changes directory to "/home/attacker" and runs the "theHarvester" command with the specified parameters. The tool's logo, a stylized "THE HARVESTER", is displayed. The output indicates the target is "microsoft.com", it is searching Baidu, and no IP addresses or emails were found.

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd /home/attacker
[root@parrot] ~
# theHarvester -d microsoft.com -l 200 -b baidu
*****
* THE HARVESTER
* https://github.com/edge-security/theHarvester
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
[*] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] No emails found.

```

8. theHarvester starts extracting the details and displays them on the screen.
9. You can see the email IDs related to the target company and target company hosts obtained from the Baidu source, as shown in the screenshot. The attackers can use these email lists and usernames to perform social engineering and brute force attacks on the target organization.

**Note:** The results might differ when you perform this task.

**Note:** Here, we specify Baidu search engine as a data source. You can specify different data sources (e.g., Baidu, bing, binaryedge, bingapi, censys, google, linkedin, twitter, virustotal, threatcrowd, crtsh, netcraft, yahoo, etc.) to gather information about the target.

The screenshot shows a terminal window titled 'theHarvester -d microsoft.com -l 200 -b baidu - Parrot Terminal'. The window displays the results of a footprinting search for Microsoft.com. It starts with theHarvester version information, followed by search parameters, and then a list of hosts found. The hosts listed include various Microsoft domains and IP addresses, such as apps.dev.microsoft.com, support.microsoft.com, www.asia.microsoft.com, and www.microsoft.com, along with their corresponding IP ranges.

```
* [theHarvester 4.0.0]
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
[*] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 5
-----
apps.dev.microsoft.com:40.126.29.2, 40.126.29.0, 40.126.29.1, 40.126.29.20, 40.126.29.22, 40.126.29.23, 40.126.29.21
support.microsoft.com:23.193.120.116
www.asia.microsoft.com:40.76.4.15, 40.112.72.205, 40.113.200.201, 13.77.161.179, 104.215.148.63
www.microsoft.com:23.48.89.170
[root@parrot]-(~)
#
```

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

## Task 4: Gather Information using Deep and Dark Web Searching

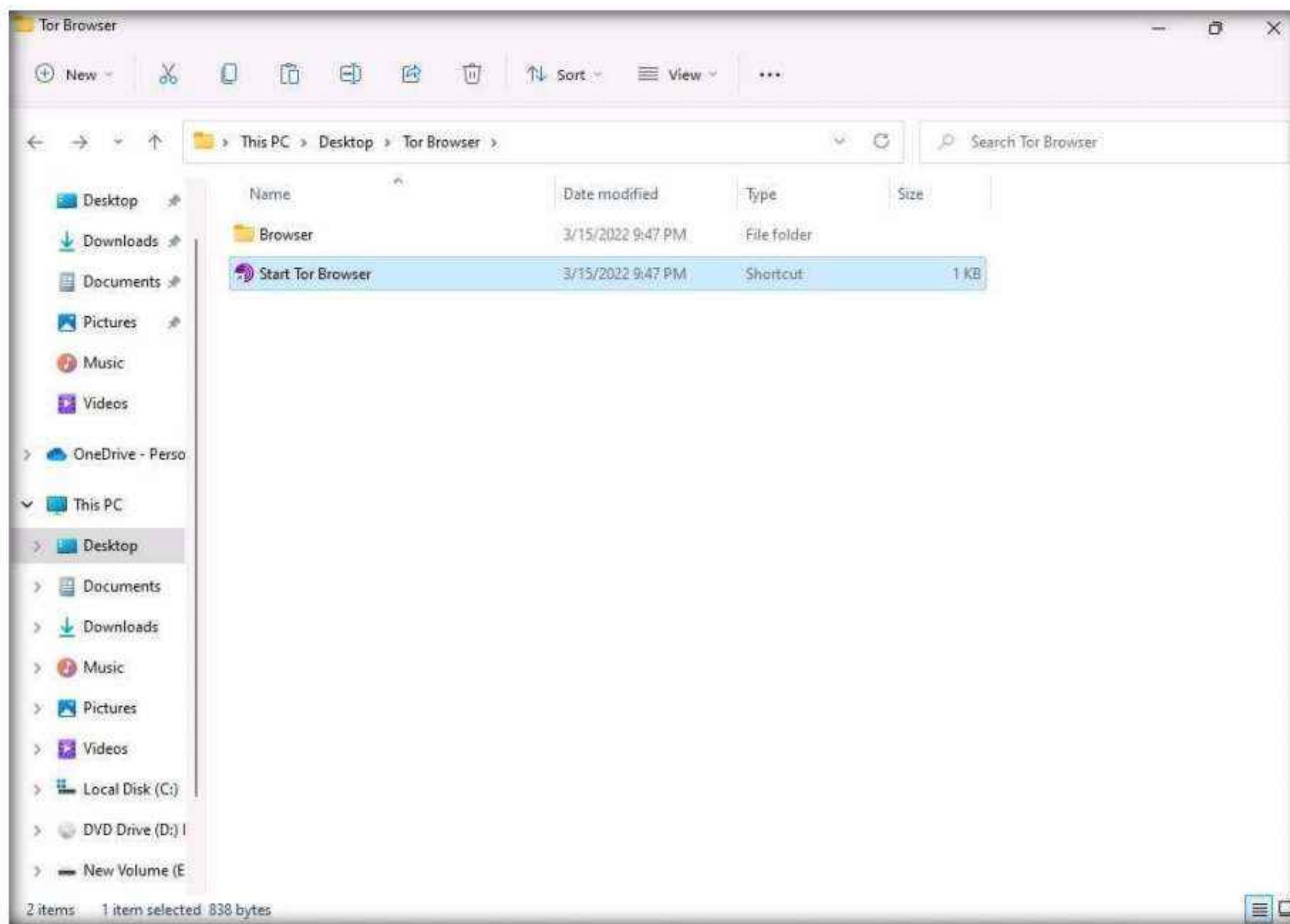
The deep web consists of web pages and content that are hidden and unindexed and cannot be located using a traditional web browser and search engines. It can be accessed by search engines such as Tor Browser and The WWW Virtual Library.

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.

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

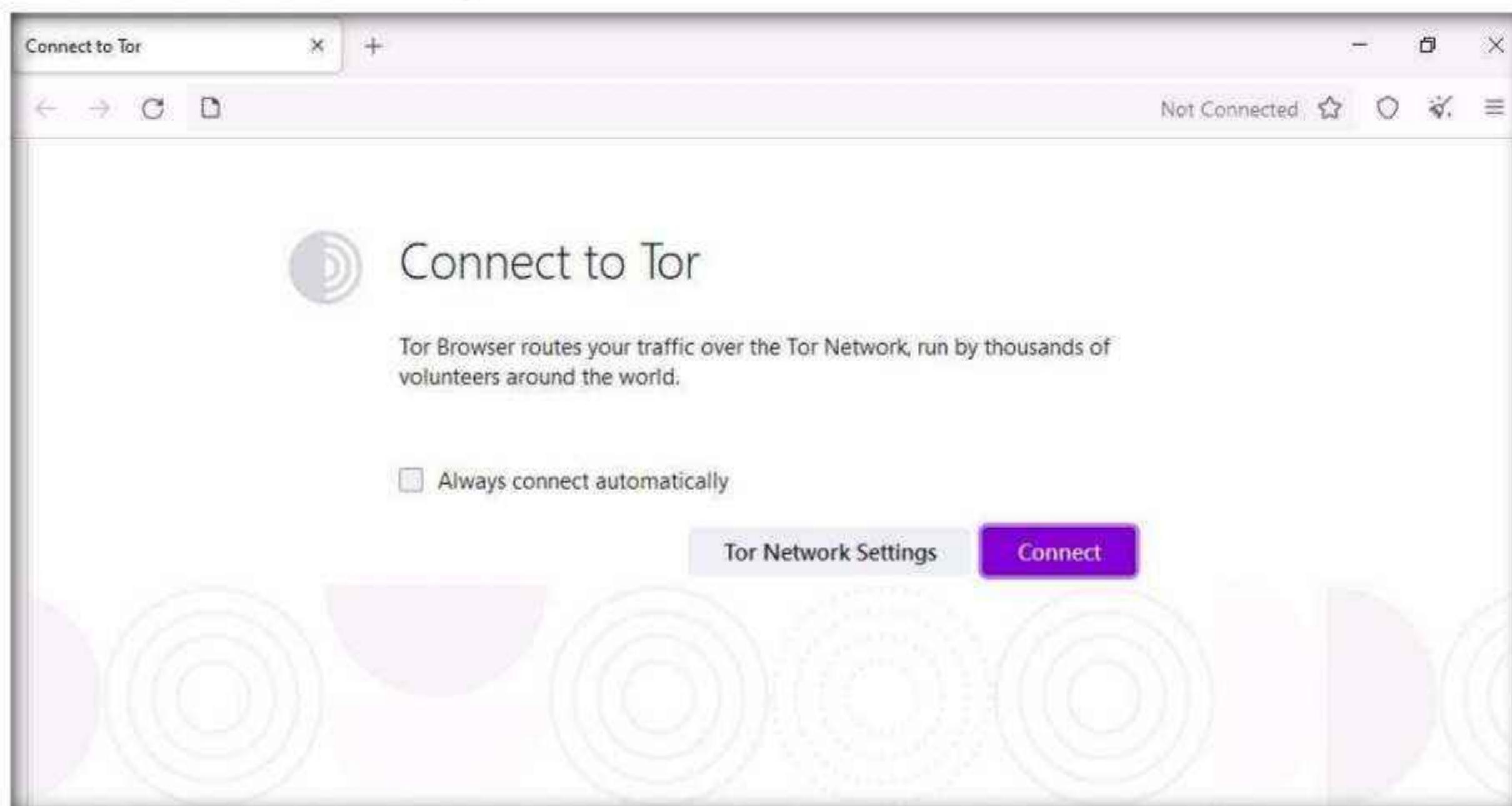
1. Switch to the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: Admin and Password: Pa\$\$w0rd.

2. Open a **File Explorer**, navigate to **C:\Users\Admin\Desktop\Tor Browser**, and double-click **Start Tor Browser**.

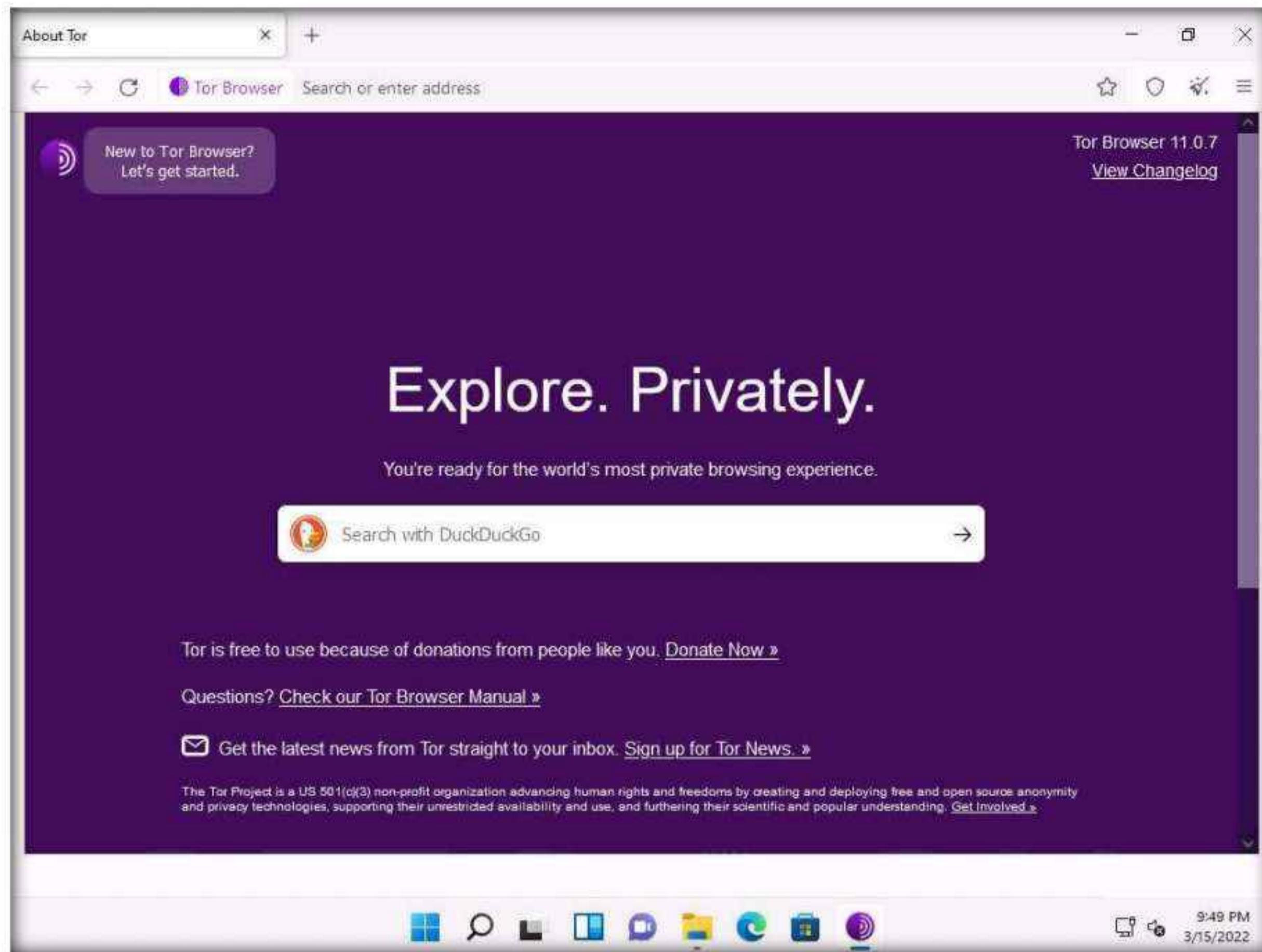


3. The **Connect to Tor** page appears. Click the **Connect** button to directly browse through Tor Browser's default settings.

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

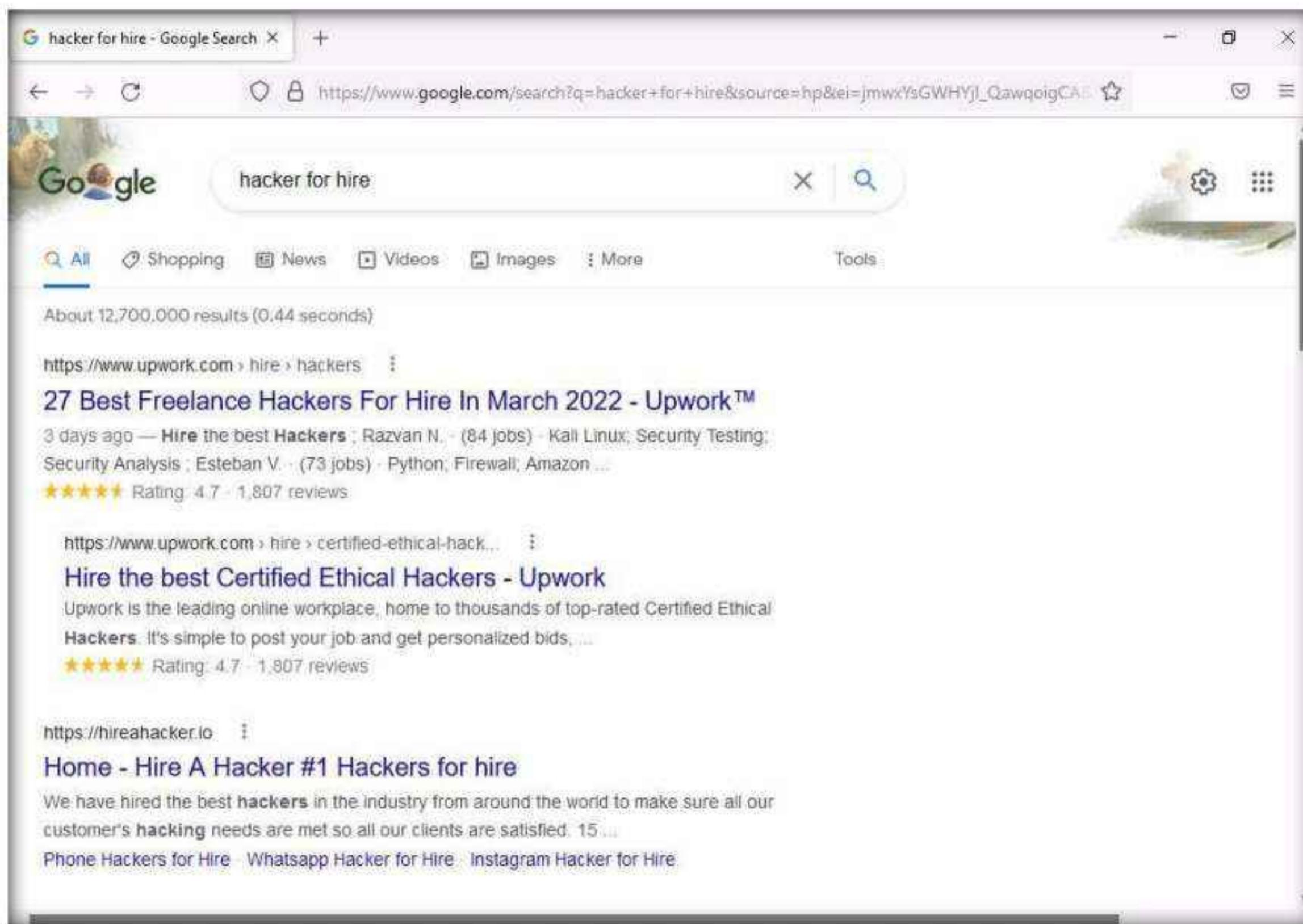


4. After a few seconds, the Tor Browser home page appears. The main advantage of Tor Browser is that it maintains the anonymity of the user throughout the session.



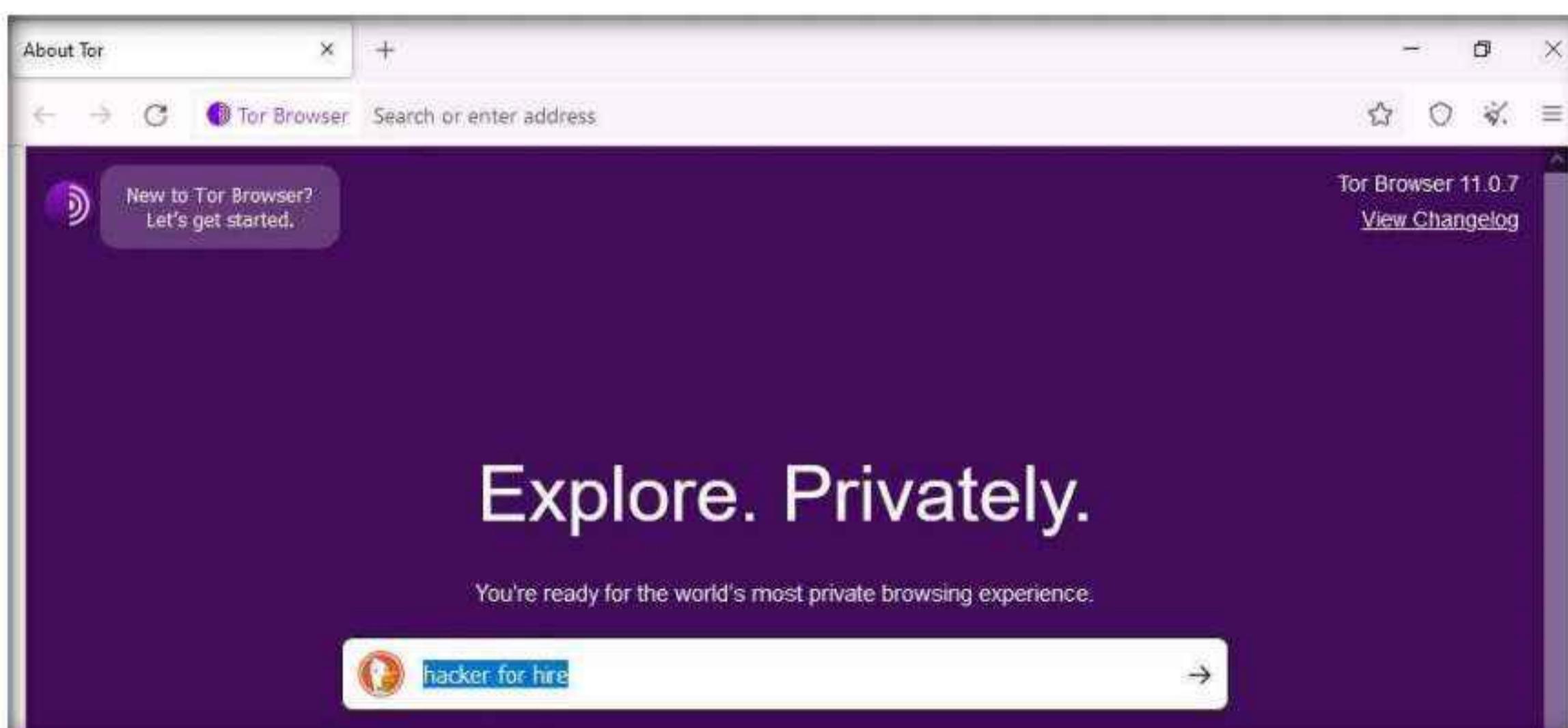
5. As an ethical hacker, you need to collect all possible information related to the target organization from the dark web. Before doing so, you must know the difference between surface web searching and dark web searching.

6. 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.



7. 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.

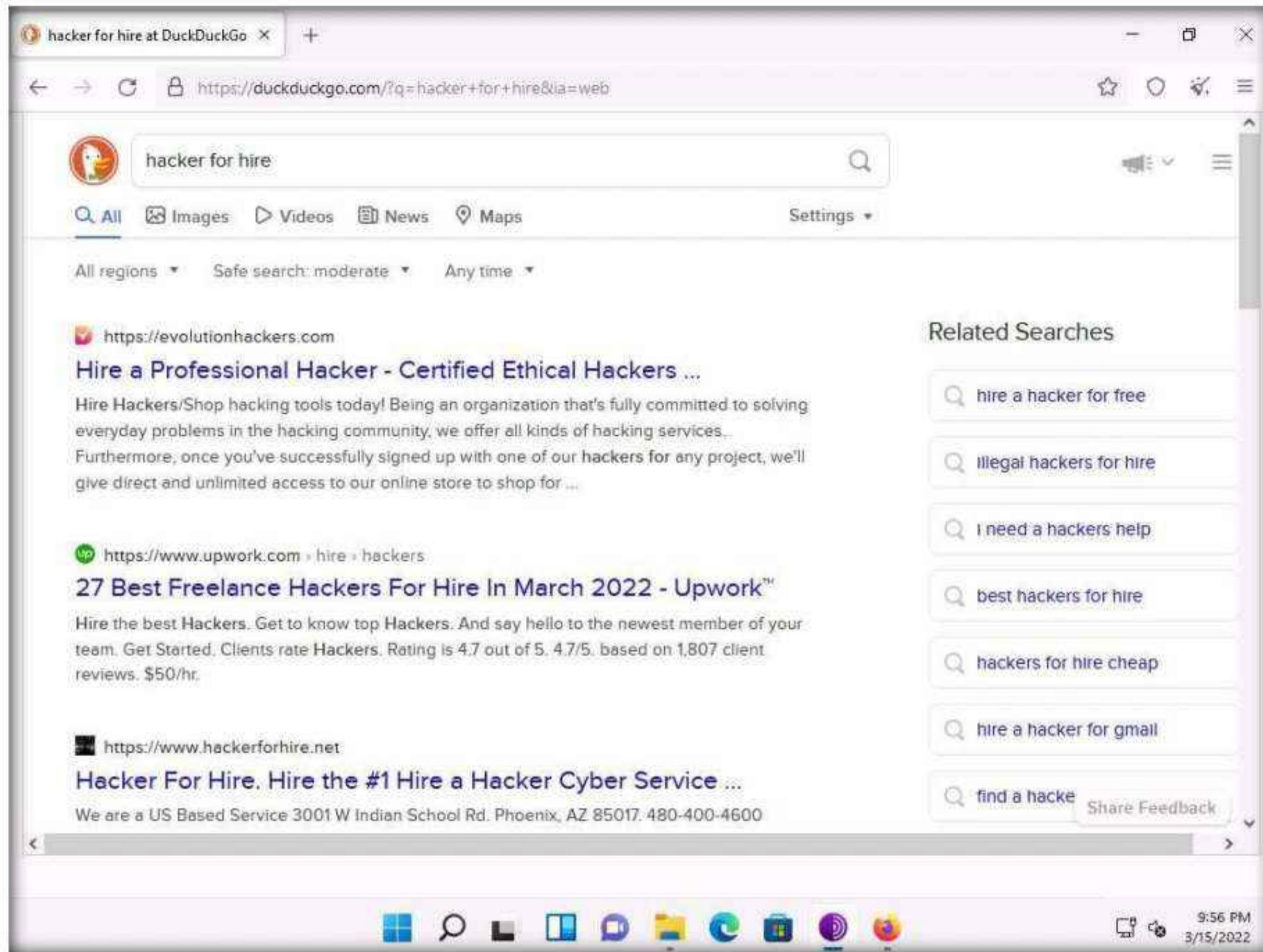
**Note:** Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.



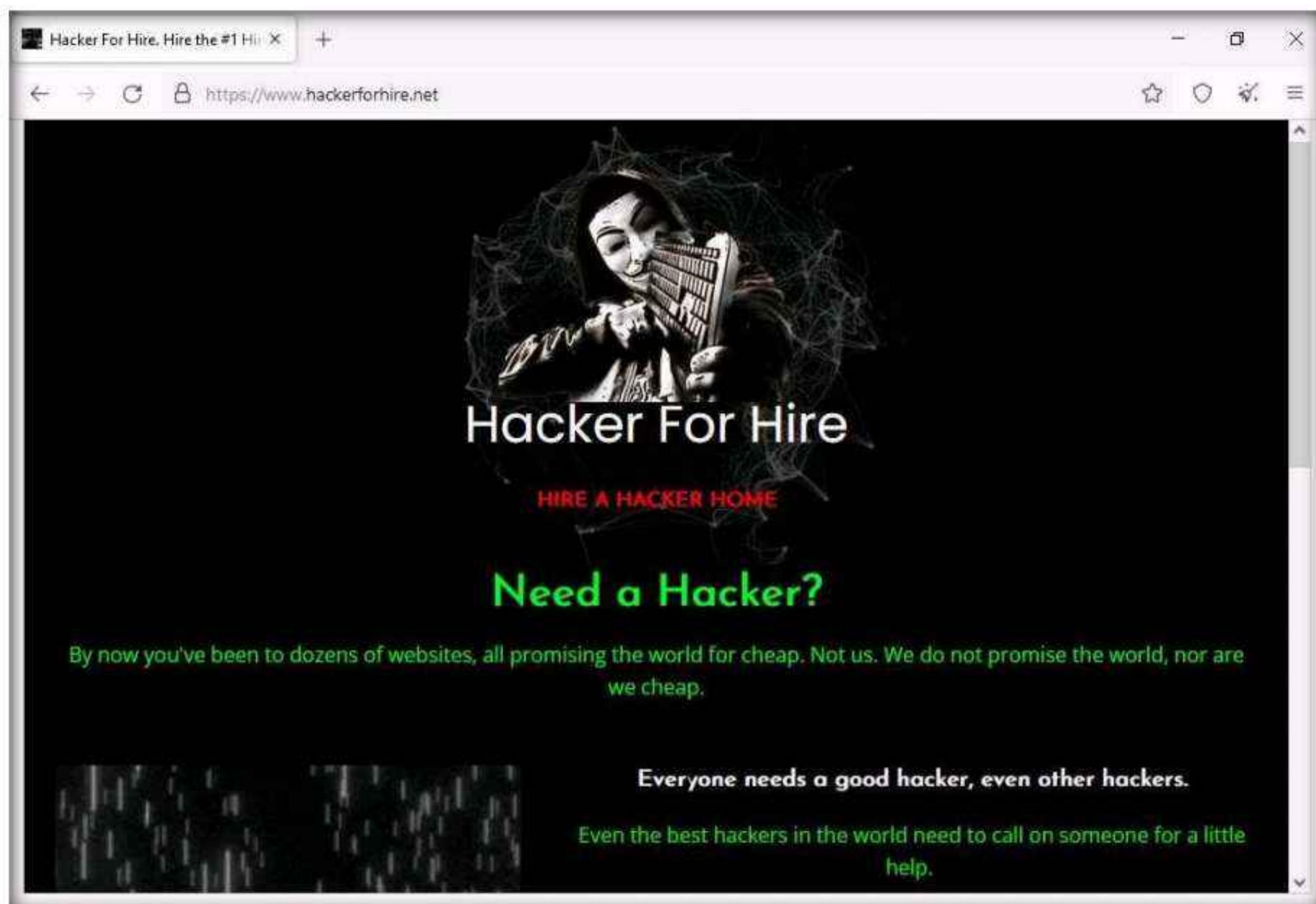
## Module 02 – Footprinting and Reconnaissance

8. By default, **All regions** search parameter is selected. However, you can click the down arrow to view the drop-down options and select a region of your choice, this specifies the country of VPN/Proxy.
9. Search results for **hacker for hire** will be loaded, as shown in the screenshot. Click to open any of the website from the search results (here, <https://www.hackerforhire.net>).

**Note:** The search results might differ when you perform this task.



10. The <https://www.hackerforhire.net> webpage opens up, as shown in the screenshot. You can see that the site belongs to professional hackers who operate underground.



11. hackerforhire 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.
12. 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://zqktlwluavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki>)
  - **FakeID** is an onion site for creating fake passports  
(<http://ymvhtqya23wqpez63gyc3ke4svju3mqsby2awnhd3bk2e65izt7baqad.onion>)
  - **Cardshop** is an onion site that sells cards with good balances  
(<http://s57divisqlcjtsyutxjz2ww77vlbwpxgodtijcsrgsuts4js5hnxkhqd.onion>)
13. 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.
14. This concludes the demonstration of gathering information using deep and dark web searching using Tor Browser.
15. Close all open windows and document all the acquired information.

## 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 and obtain other information such as the city, country, latitude/longitude, hostname, operating system, and IP address of the target organization.

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

**Note:** Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type <https://search.censys.io/?q=> and press **Enter**.
2. In the search field, type the target website (here, [www.eccouncil.org](http://www.eccouncil.org)) and press **Enter**. From the results, click any **Hosts** IP address which you want to gather the OS details.

**Note:** The result might differ, when you perform this lab task.

The screenshot shows the Censys search interface with the URL [https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per\\_page=25&virtual\\_hosts=0](https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=0). The search term is `www.eccouncil.org`. The results page has a sidebar with 'Host Filters' for Autonomous System (AMAZON-02, OVH, AMAZON-AES, DIGITALOCEAN-ASN, GOOGLE-CLOUD-PLATFORM) and Location (United States, France, Canada, Germany, Latvia). The main area shows 'Results: 22 Time: 8.70s'. It lists three hosts:

- 51.195.40.93**: Located in France, with ports 22/SSH, 80/HTTP, 123/NTP, 443/HTTP. Services include http with body: `services.http.response.body: href="http://www.eccouncil.org/Certification"`.
- 3.16.217.79**: Located in Ohio, United States, with ports 22/SSH, 80/HTTP. Services include http with body: `services.http.response.body: //www.eccouncil.org/programs/certified-ethical-hacker-ce...` and `services.http.response.body: //www.eccouncil.org/programs/certified-ethical...`.
- 2A00:ECE1:0000:001F:0000:0000:0181**: Located in Romania, with port 80/HTTP, 443/HTTP. Services include http with body: `services.http.response.body: href="https://www.eccouncil.org/programs...`.

3. The selected host page appears, as shown in the screenshot. Under the **Basic Information** section, you can observe that the **OS** is **Ubuntu**. Apart from this, you can also observe other details such as protocols running, software, host keys, etc. This information can help attackers in identifying potential vulnerabilities and finding effective exploits to perform various attacks on the target organization.

The screenshot shows the Censys web interface for host 3.16.217.79. At the top, there's a navigation bar with a back/forward button, a search bar containing 'https://search.censys.io/hosts/3.16.217.79?resource=hosts&sort=RELEVANCE&per\_page=25&virt...', and a 'Search' button. To the right are 'Register' and 'Log In' links. Below the header, the IP address '3.16.217.79' is displayed, with a note 'As of: Mar 16, 2022 12:40am UTC | Latest'. A navigation menu includes 'Summary' (which is selected), 'Explore', 'History', 'WHOIS', and 'Raw Data'. The 'Basic Information' section lists the OS as 'Ubuntu Linux 18.04', Network as 'AMAZON-02 (US)', Routing as '3.16.0.0/14 via AS16509', and Protocols as '22/SSH, 80/HTTP'. To the right is a map showing the location in Columbus, Ohio. The 'Software' section lists 'linux', 'Ubuntu Linux 18.04', and 'OpenBSD OpenSSH 7.6'. A 'VIEW ALL DATA' button is located next to the software list. The bottom of the screen shows a Windows taskbar with various icons and a system tray indicating the date and time.

4. This concludes the demonstration of gathering OS information through passive footprinting using the Censys web service.
5. 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.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 11** virtual machine.

## Lab Analysis

Analyze and document the results of this lab exercise.

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

### Internet Connection Required

Yes

No

### Platform Supported

Classroom

CyberQ

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.*

### 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

To carry out this lab, you need:

- Windows 11 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.

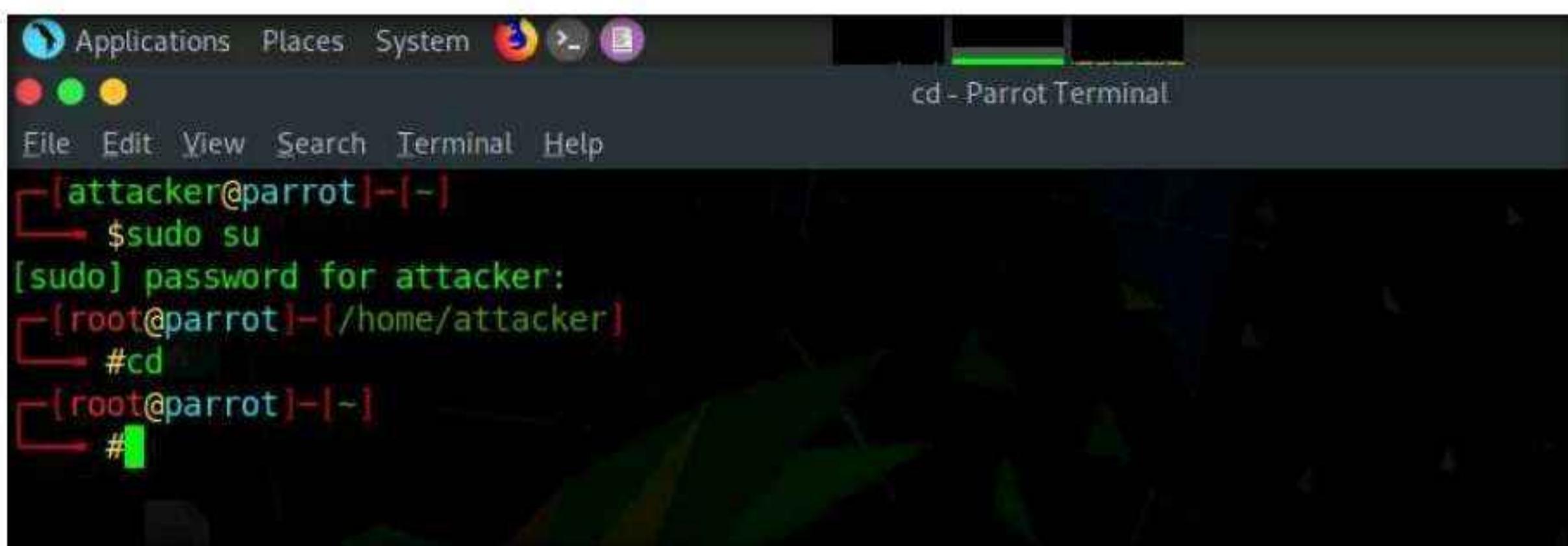
**Note:** Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. Turn on the **Parrot Security** virtual machine. 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.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
  4. 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.
  5. Now, type **cd** and press **Enter** to jump to the root directory.

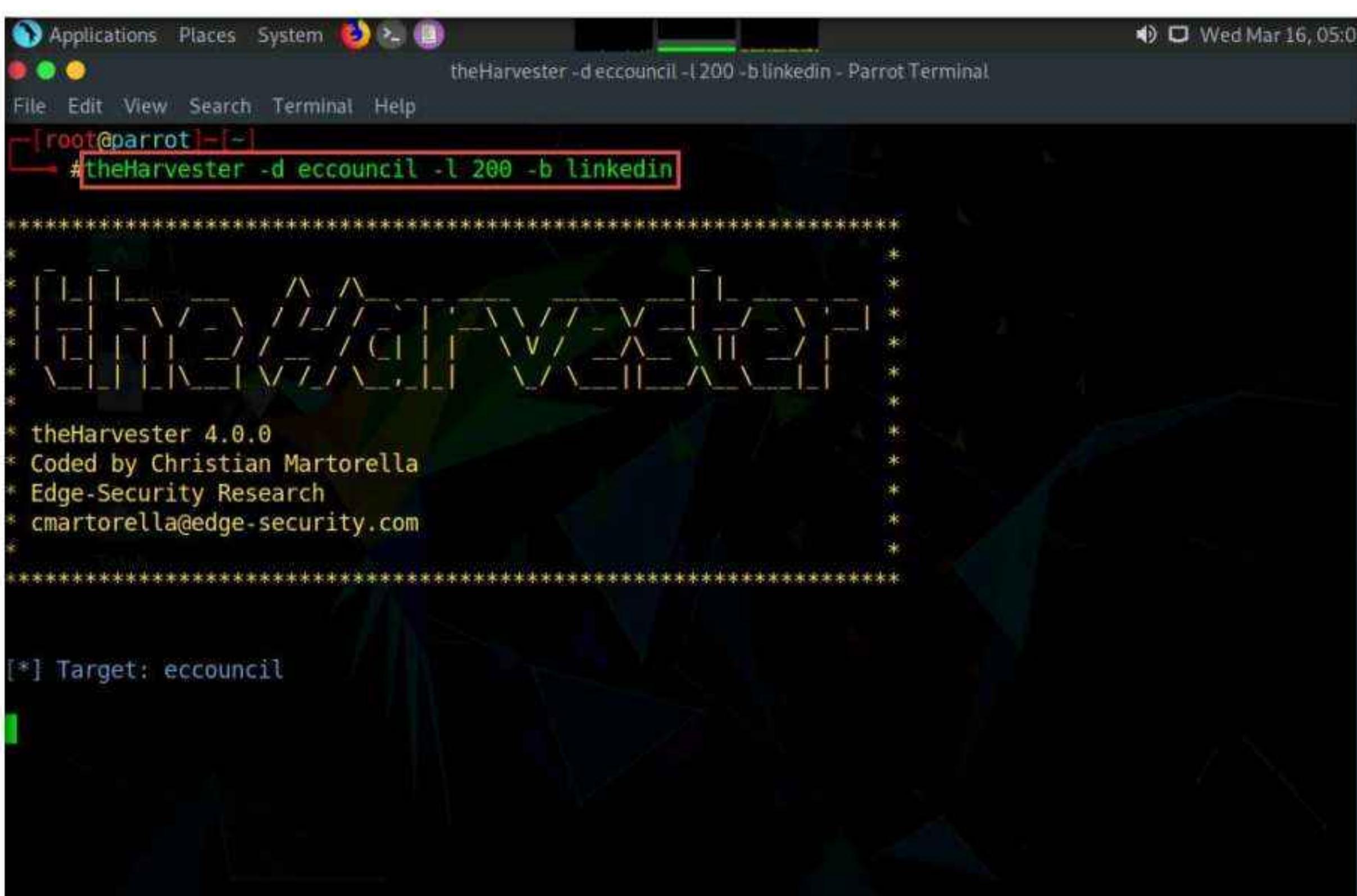
**Note:** The password that you type will not be visible.



6. In the terminal window, type **theHarvester -d eccouncil -I 200 -b linkedin** and press **Enter** to see 200 results of EC-Council from the LinkedIn source.

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

**Note:** The complete eccouncil domain is [eccouncil.org](http://eccouncil.org).



7. Scroll down to view the list of employees along with their job roles in EC-Council. This information from LinkedIn can help attackers in performing social engineering or phishing attacks.

The screenshot shows a terminal window titled 'theHarvester -deccouncil -l200 -b linkedin - Parrot Terminal'. The window displays the results of a search for the target 'ecouncil'. It shows three main sections of results:

- Section 1: Searching LinkedIn. It shows 197 LinkedIn users found, with some examples of job titles:
  - Software Engineer
  - Software Engineer
  - Vice President
- Section 2: Cyber Security Training Coordinator. It shows 1 user found, with one job title:
  - Vice President Finance
- Section 3: Manager Business Development. It shows 1 user found, with several job titles:
  - Manager Masterclass
  - Manager - Partner Outreach
  - Operations Manager
  - Software Engineer
  - EC-Council
  - Manager Business Development
  - Account Executive
  - Assistant Manager- International Sales
  - Security Consultant
  - Researcher
  - it security hobbyist
  - Senior Operations Executive
  - Research Specialist
  - SVP and Head of Americas

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

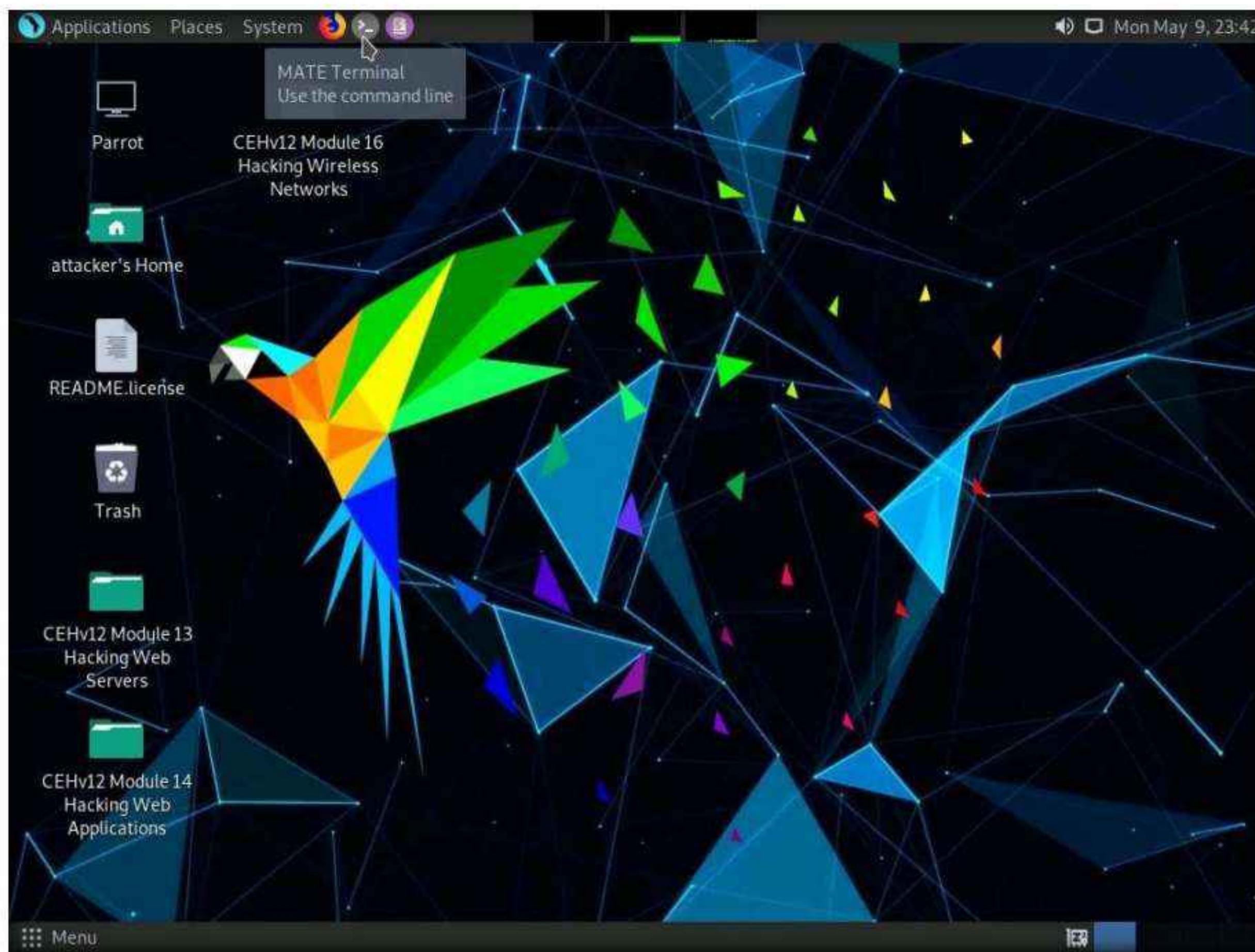
Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target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

Here, we will use Sherlock to gather personal information about the target from the social networking sites.

**Note:** Here, we are gathering information about **Satya Nadella**. However, you can select a target of your choice.

## Module 02 – Footprinting and Reconnaissance

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **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. Type **cd sherlock/sherlock/** and press **Enter** to navigate to the **sherlock** folder.

A screenshot of the Parrot Terminal window. The title bar shows the path "cd sherlock/sherlock/ - Parrot Terminal". The terminal window displays the following command history:

```
[attacker@parrot]~[-]$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]# cd sherlock/sherlock/
[root@parrot]~[/home/attacker/sherlock/sherlock]#
```

The terminal window has a dark background with light-colored text. The cursor is positioned at the end of the last command line.

5. 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.

**Note:** The results might differ when you perform this task. If you receive any error messages in between ignore them.

```
python3 sherlock.py satya nadella - Parrot Terminal
[+] Checking username satya on:
[+] 7Cups: https://www.7cups.com/@satya
[+] About.me: https://about.me/satya
[+] Academia.edu: https://independent.academia.edu/satya
[+] AllMyLinks: https://allmylinks.com/satya
[+] Anilist: https://anilist.co/user/satya/
[+] Apple Developer: https://developer.apple.com/forums/profile/satya
[+] Apple Discussions: https://discussions.apple.com/profile/satya
[+] Archive.org: https://archive.org/details/@satya
[+] Arduino: https://create.arduino.cc/projecthub/satya
[+] Audiojungle: https://audiojungle.net/user/satya
[+] BLIP.fm: https://blip.fm/satya
[+] Bandcamp: https://www.bandcamp.com/satya
[+] Behance: https://www.behance.net/satya
[+] Bikemap: https://www.bikemap.net/en/u/satya/routes/created/
[+] BinarySearch: https://binarysearch.io/@satya
[+] Blogger: https://satya.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/satya
[+] Bookcrossing: https://www.bookcrossing.com/mybookshelf/satya/
[+] BraveCommunity: https://community.brave.com/u/satya/
[+] BuyMeACoffee: https://buymeacoff.ee/satya
[+] BuzzFeed: https://buzzfeed.com/satya
[+] CNET: https://www.cnet.com/profiles/satya/
[+] Carbonmade: https://satya.carbonmade.com
[+] CloudflareCommunity: https://community.cloudflare.com/u/satya
[+] Codecademy: https://www.codecademy.com/profiles/satya
[+] Codechef: https://www.codechef.com/users/satya
[+] ColourLovers: https://www.colourlovers.com/lover/satya
```

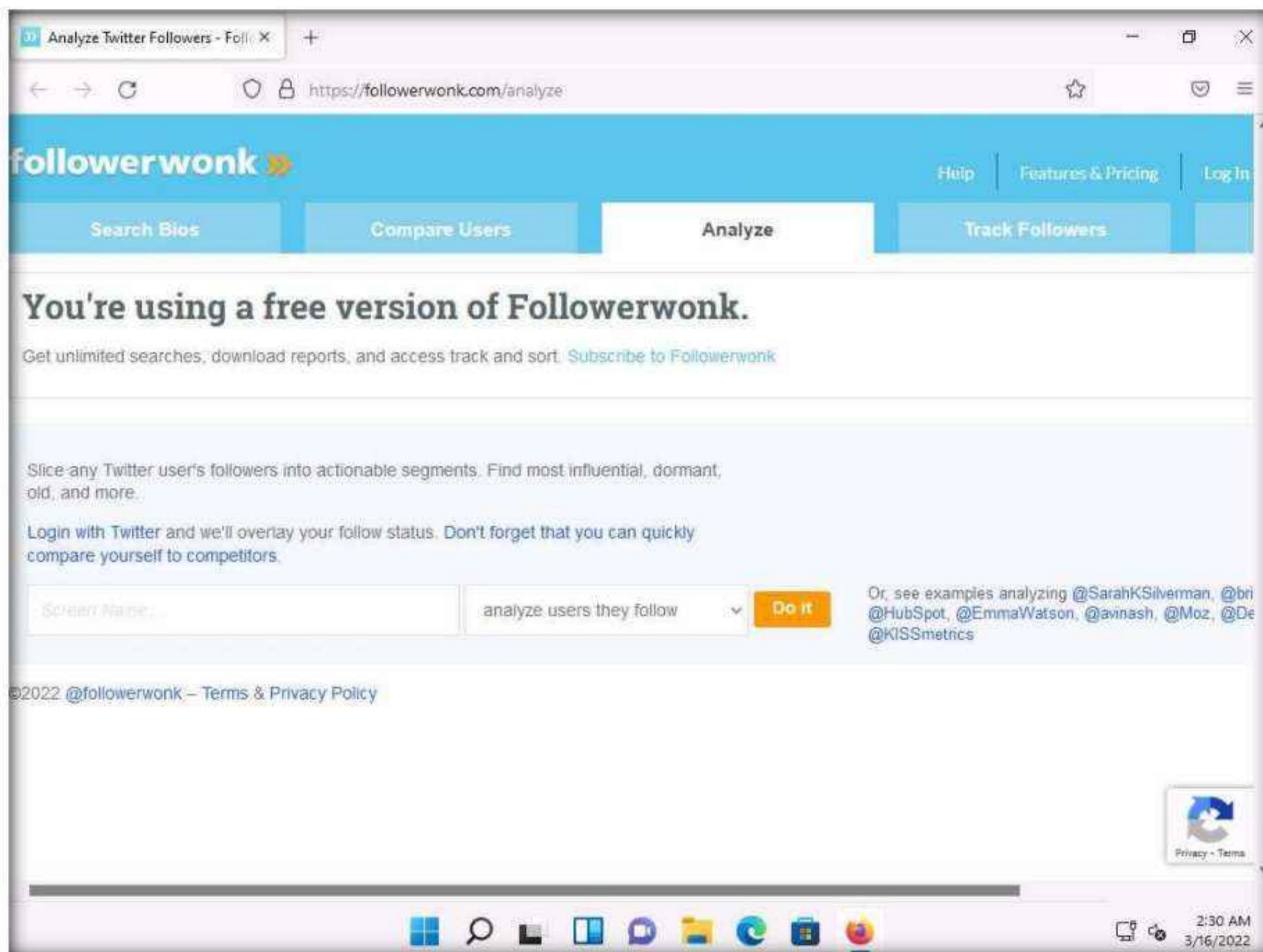
6. The attackers can further use the gathered URLs to obtain sensitive information about the target such as DOB, employment status and information about the organization that they are working for, including the business strategy, potential clients, and upcoming project plans.
7. This concludes the demonstration of gathering person information from various social networking sites using Sherlock.
8. 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. Close all open windows and document all the acquired information.
10. 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.

Here, we will use Followerwonk to gather information about the followers in social networking sites.

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://followerwonk.com/analyze** and press **Enter**.
3. **Followerwonk** website appears, as shown in the screenshot.



4. 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.

## Module 02 – Footprinting and Reconnaissance

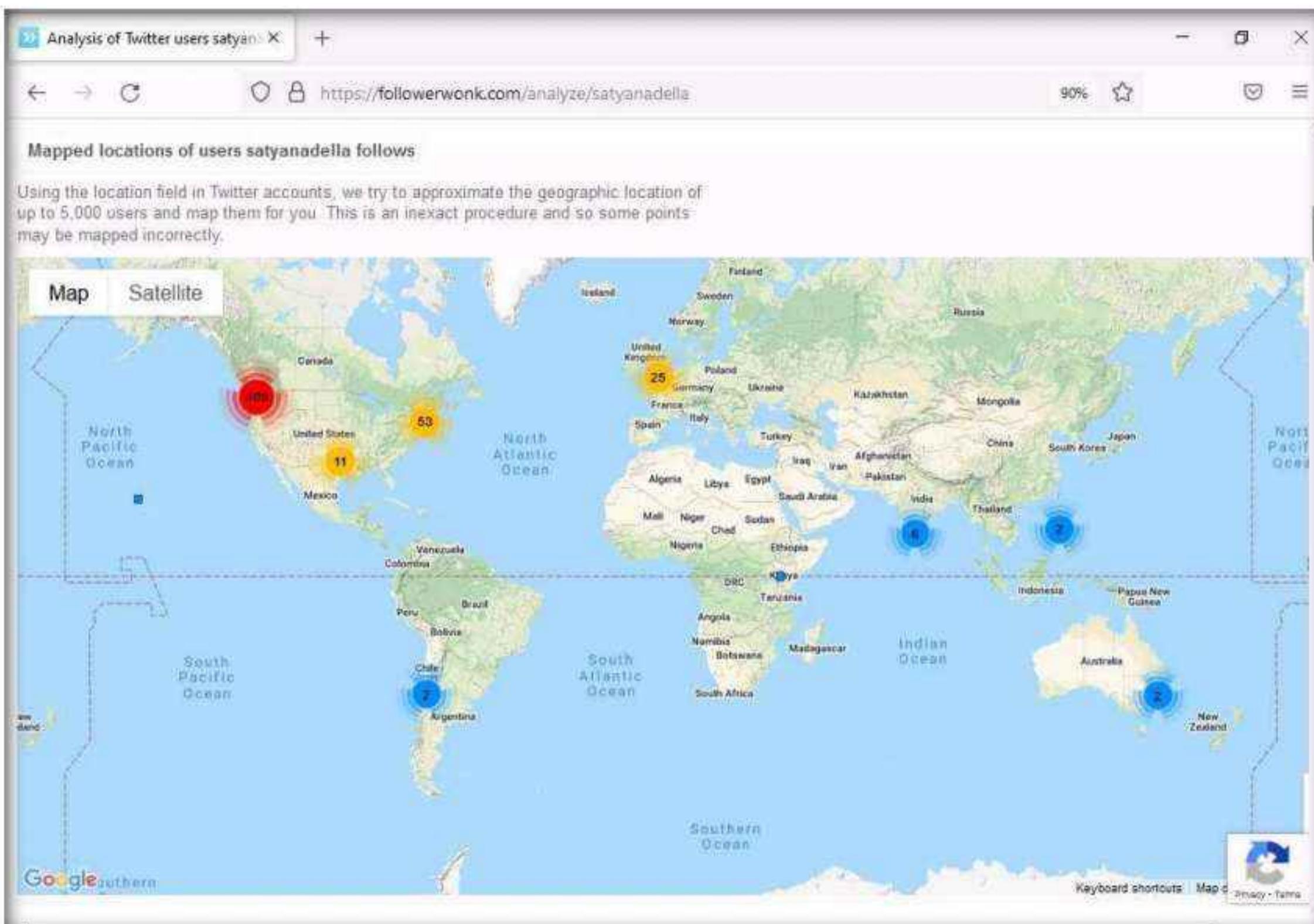
5. The results regarding the target appears, as shown in the screenshot.

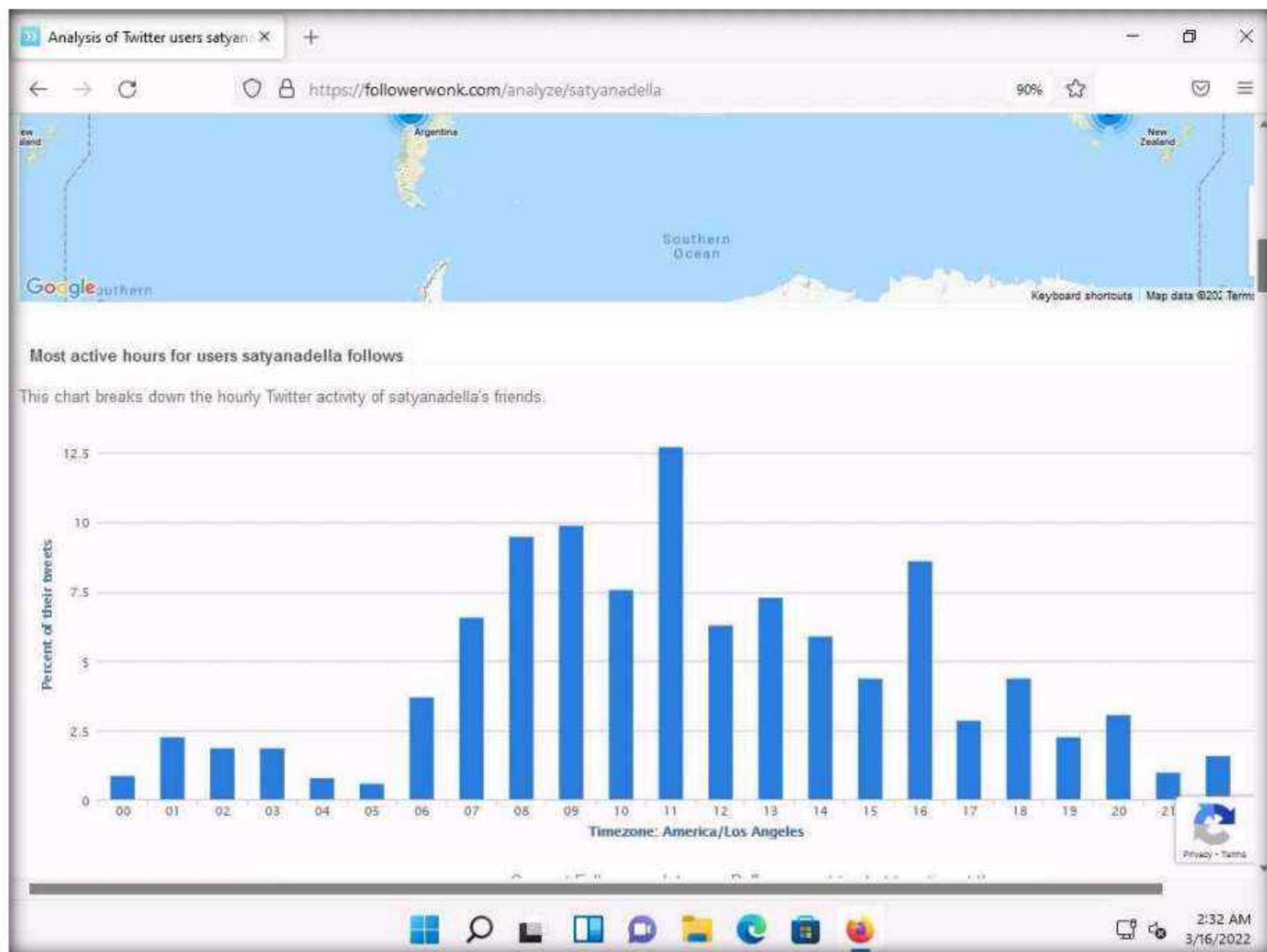
The screenshot shows the Followerwonk website interface. At the top, there's a navigation bar with tabs for 'Search Bio', 'Compare Users', 'Analyze', 'Track Followers', and 'Sort Followers'. A prominent orange button says 'Sign Up. It's Free!'. Below the navigation, a message says 'You're using a free version of Followerwonk.' and encourages users to subscribe for more features. A search bar contains the handle '@satyanadella' and a dropdown menu says 'analyze users they follow'. An orange 'Go!' button is next to it. To the right, there's a sidebar with examples of other users analyzed. The main content area is titled 'Analysis of users satyanadella follows on Twitter'. It includes a brief description of how users are segmented by psychographic factors like gender and location. On the right, there's a detailed profile box for 'Satya Nadella' with the following data:

Social Authority:	79
Followers:	2,776,415
Time on:	13.09 years
Retweets:	29.0%
@Contact:	5.5%
URL tweets:	69.0%
Chairman and CEO of Microsoft Corporation microsoft.com/ceo	

Below this, there's a section titled 'Mapped locations of users satyanadella follows' which includes a map of the world showing the approximate geographic locations of the users followed by Satya Nadella. The map highlights several clusters of followers in North America, Europe, and Asia.

6. Scroll down to view the detailed analysis on the geographical location and active hours of the followers. This information further helps attackers to perform various social engineering and non-technical attacks.





7. This concludes the demonstration of gathering information using Followerwonk.
8. You can also use **Hootsuite** (<https://www.hootsuite.com>), **Meltwater** (<https://www.meltwater.com>), etc. to gather additional information related to the target company and its employees from social networking sites.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows 11** virtual machine.

## Lab Analysis

Analyze and document the results of this lab exercise.

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

<b>Internet Connection Required</b>	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Platform Supported</b>	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> CyberQ

Lab

4

## Perform Website Footprinting

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

### Lab Scenario

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 Photon
- Gather information about a target website using Central Ops
- Extract a company's data using Web Data Extractor
- Mirror a target website using HTTrack Web Site Copier
- Gather information about a target website using GRecon
- Gather a wordlist from the target website using CeWL

### Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

## Lab Duration

Time: 45 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

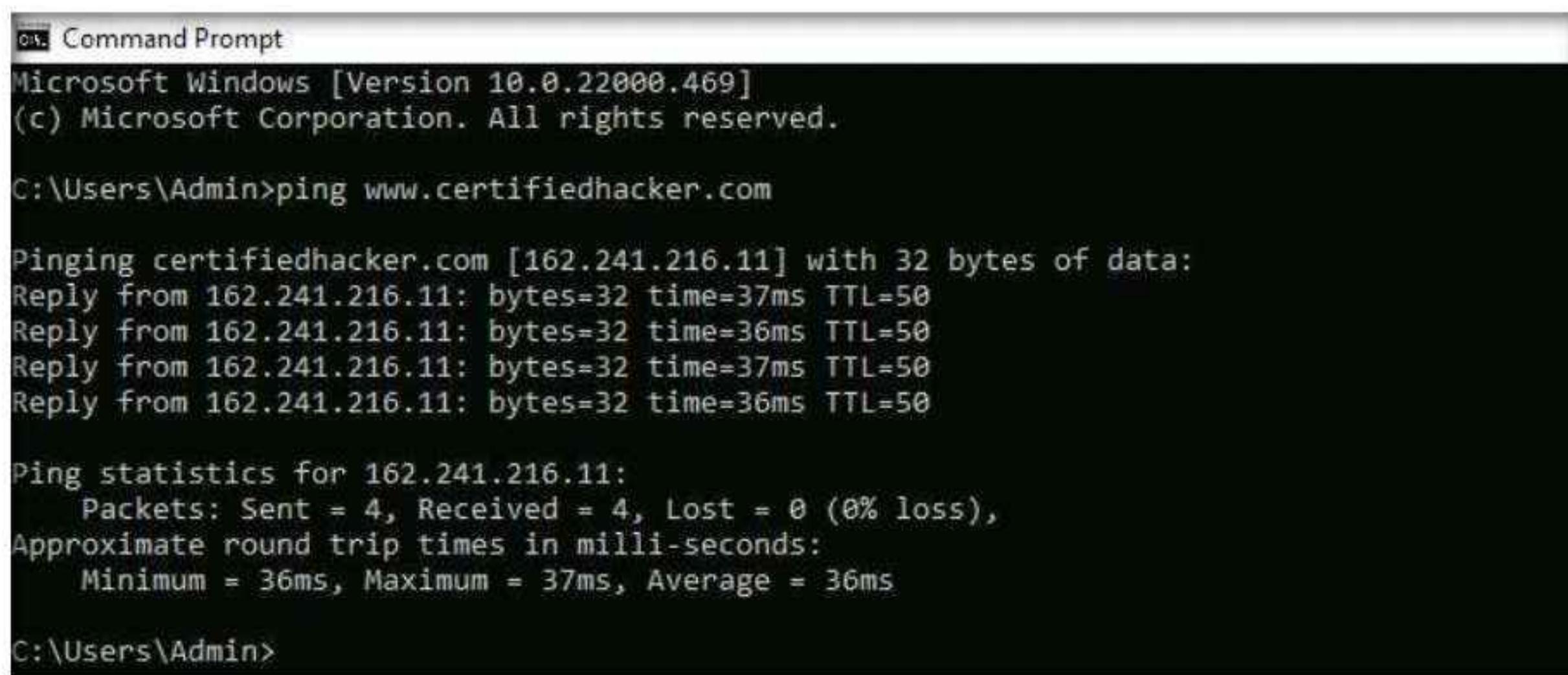
### Task 1: Gather Information About a Target Website using Ping Command Line Utility

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. 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.

Here, we will use ping command line utility to gather information about a target website.

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
2. 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.

**Note:** To open a **Command Prompt** window, click **Search** icon on the **Desktop**, type **cmd** and select **Command Prompt** from the results.



```
ps: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com

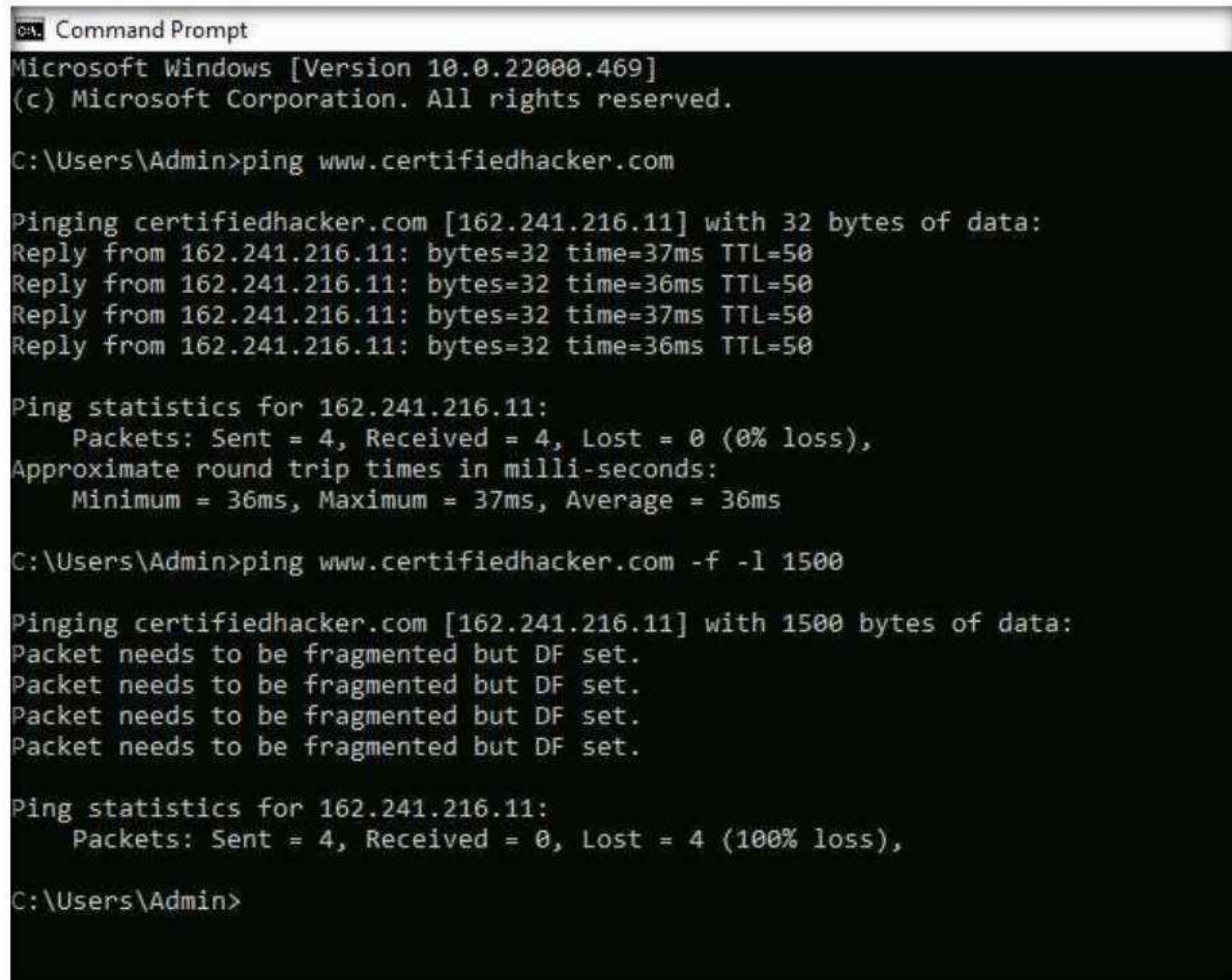
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>
```

3. 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.
4. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1500** and press **Enter**.

**Note:** Here, **-f**: Specifies setting not fragmenting flag in packet, **-l**: Specifies buffer size.



```
Windows PowerShell
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Admin>
```

5. 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.

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

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The output of the ping command is displayed:

```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1300

Pinging certifiedhacker.com [162.241.216.11] with 1300 bytes of data:
Reply from 162.241.216.11: bytes=1300 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1300 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1300 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1300 time=36ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>
```

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

```
C:\> Command Prompt  
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1473  
Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:  
Packet needs to be fragmented but DF set.  
  
Ping statistics for 162.241.216.11:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472  
Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:  
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50  
Reply from 162.241.216.11: bytes=1472 time=37ms TTL=50  
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50  
Reply from 162.241.216.11: bytes=1472 time=35ms TTL=50  
  
Ping statistics for 162.241.216.11:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 35ms, Maximum = 37ms, Average = 36ms  
  
C:\Users\Admin>
```

9. 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.
10. In the **Command Prompt** window, 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.

```
C:\> Command Prompt  
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1473  
Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:  
Packet needs to be fragmented but DF set.  
  
Ping statistics for 162.241.216.11:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472  
Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:  
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50  
Reply from 162.241.216.11: bytes=1472 time=37ms TTL=50  
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50  
Reply from 162.241.216.11: bytes=1472 time=35ms TTL=50  
  
Ping statistics for 162.241.216.11:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 35ms, Maximum = 37ms, Average = 36ms  
  
C:\Users\Admin>ping www.certifiedhacker.com -i 3  
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:  
Reply from 192.168.100.6: TTL expired in transit.  
  
Ping statistics for 162.241.216.11:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
  
C:\Users\Admin>
```

11. Reply from **192.168.100.6: TTL expired in transit** means that the router (192.168.100.6, you will have some other IP address) discarded the frame because its TTL has expired (reached 0).

**Note:** The IP address 192.168.100.6 might vary when you perform this task.

12. 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.

```
Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com -i 2 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.18.0.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

C:\Users\Admin>

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

```
Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com -i 2 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.18.0.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Admin>ping www.certifiedhacker.com -i 3 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 192.168.100.6: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

C:\Users\Admin>

14. Observe that there is a reply coming from the IP address **162.241.216.11**, and there is no packet loss.
15. Now, change the time to live value to **4** by typing, **ping www.certifiedhacker.com -i 4 -n 1** and press **Enter**.

The screenshot shows a Windows Command Prompt window with the title 'Command Prompt'. The window displays the following text:

```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com -i 2 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.18.0.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
C:\Users\Admin>ping www.certifiedhacker.com -i 3 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 192.168.100.6: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
C:\Users\Admin>ping www.certifiedhacker.com -i 4 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 103.152.3.225: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
C:\Users\Admin>
```

16. Repeat the above step until you reach the IP address for **www.certifiedhacker.com** (in this case, **162.241.216.11**).
17. Find the hop value by trying different TTL value to reach **www.certifiedhacker.com**.  
**Note:** Here, the hope value to reach **www.certifiedhacker.com** is 19, which might differ when you perform this task.
18. On successfully finding the TTL value it will imply that the reply is received from the destination host (**162.241.216.11**).
19. 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).
20. Close all open windows and document all the acquired information.

## Task 2: Gather Information About a Target Website using Photon

Photon is a Python script used to crawl a given target URL to obtain information such as URLs (in-scope and out-of-scope), URLs with parameters, email, social media accounts, files, secret keys and subdomains. The extracted information can further be exported in JSON format.

**Note:** Here, we will consider [www.certifiedhacker.com](http://www.certifiedhacker.com) as the target website. However, you can select a target domain of your choice.

1. Turn on the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. 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.
5. In the terminal window, type **cd Photon** and press **Enter** to navigate to the Photon repository.

A screenshot of the Parrot Terminal window. The title bar reads 'cd Photon - Parrot Terminal'. The window shows a command-line interface with the following session:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd Photon
[root@parrot] ~
#
```

The terminal uses color-coded syntax highlighting for commands and output.

6. Type **python3 photon.py -h** and press **Enter** to view the list of options that Photon provides.

```
python3 photon.py -h - Parrot Terminal
[root@parrot]~[/home/attacker/Photon]
#python3 photon.py -h

v1.3.2

usage: photon.py [-h] [-u ROOT] [-c COOK] [-r REGEX] [-e {csv,json}] [-o OUTPUT] [-l LEVEL]
                 [-t THREADS] [-d DELAY] [-v] [-s SEEDS [SEEDS ...]] [--stdout STD]
                 [--user-agent USER_AGENT] [--exclude EXCLUDE] [--timeout TIMEOUT] [-p PROXIES]
                 [--clone] [--headers] [--dns] [--keys] [--update] [--only-urls] [--wayback]

optional arguments:
  -h, --help            show this help message and exit
  -u ROOT, --url ROOT  root url
  -c COOK, --cookie COOK
  -r REGEX, --regex REGEX
  -e {csv,json}, --export {csv,json}
  -o OUTPUT, --output OUTPUT
  -l LEVEL, --level LEVEL
  -t THREADS, --threads THREADS
  -d DELAY, --delay DELAY
  -v, --verbose         verbose output
  -s SEEDS [SEEDS ...], --seeds SEEDS [SEEDS ...]
  --stdout STD          send variables to stdout
  --user-agent USER_AGENT
  --exclude EXCLUDE    exclude URLs matching this regex
  --clone               clone the target website
  --headers             add headers to requests
  --dns                perform DNS resolution
  --keys               extract keys from responses
  --update              update the database
  --only-urls           crawl only URLs
  --wayback             crawl Wayback Machine URLs

[...]
```

7. Type **python3 photon.py -u http://www.certifiedhacker.com** and press **Enter** to crawl the target website for internal, external and scripts URLs.

**Note:** **-u:** specifies the target website (here, www.certifiedhacker.com).

8. The results obtained are saved in **www.certifiedhacker.com** directory under Photon folder.

**Note:** The output might vary when you perform this task.

9. Type **ls** and press **Enter** to view the folder content.

10. You can observe that a directory named **www.certifiedhacker.com** is created, as shown in the screenshot.

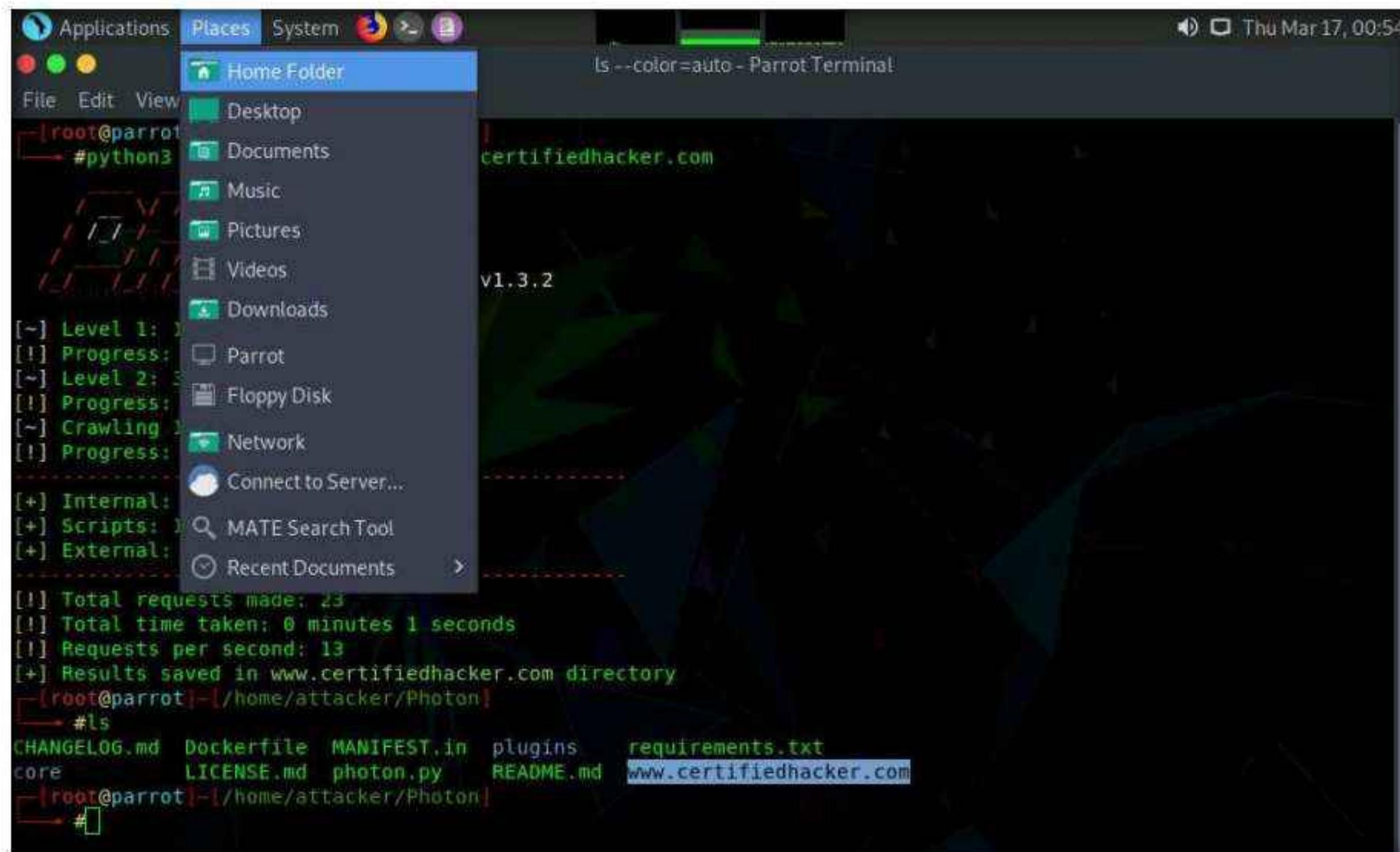
```
ls --color=auto - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Photon]
#python3 photon.py -u http://www.certifiedhacker.com

[~] Level 1: 1 URLs
[!] Progress: 1/1
[~] Level 2: 3 URLs
[!] Progress: 3/3
[~] Crawling 18 JavaScript files
[!] Progress: 18/18

[+] Internal: 4
[+] Scripts: 18
[+] External: 9

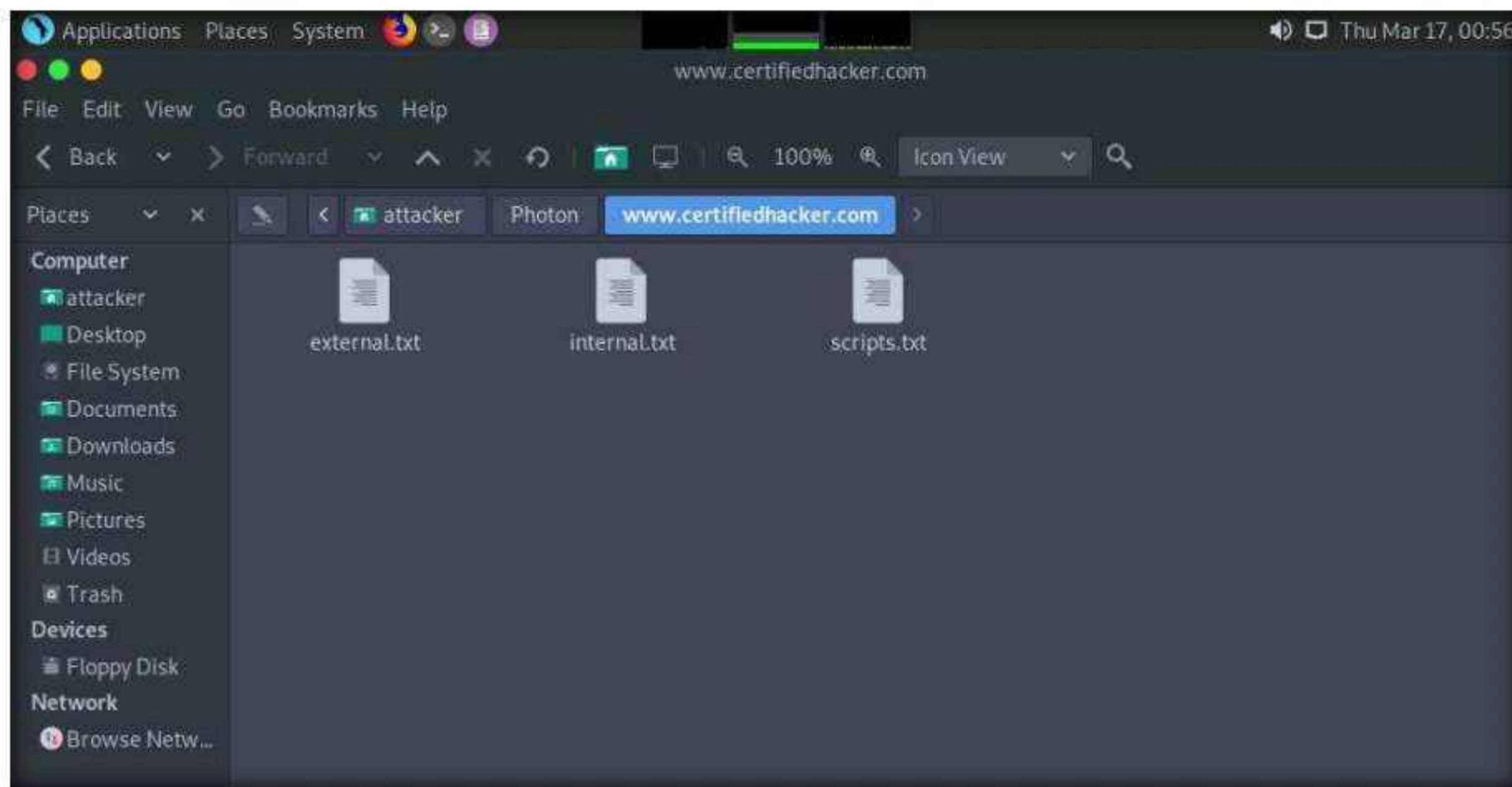
[!] Total requests made: 23
[!] Total time taken: 0 minutes 1 seconds
[!] Requests per second: 13
[+] Results saved in www.certifiedhacker.com directory
[root@parrot]~/home/attacker/Photon]
#ls
CHANGELOG.md  Dockerfile  MANIFEST.in  plugins  requirements.txt
core          LICENSE.md  photon.py   README.md  www.certifiedhacker.com
[root@parrot]~/home/attacker/Photon]
#
```

11. Now, click **Places** from the top-section of the **Desktop** and select **Home Folder**.



12. **attacker** window appears, navigate to **Photon** --> **www.certifiedhacker.com** folder.

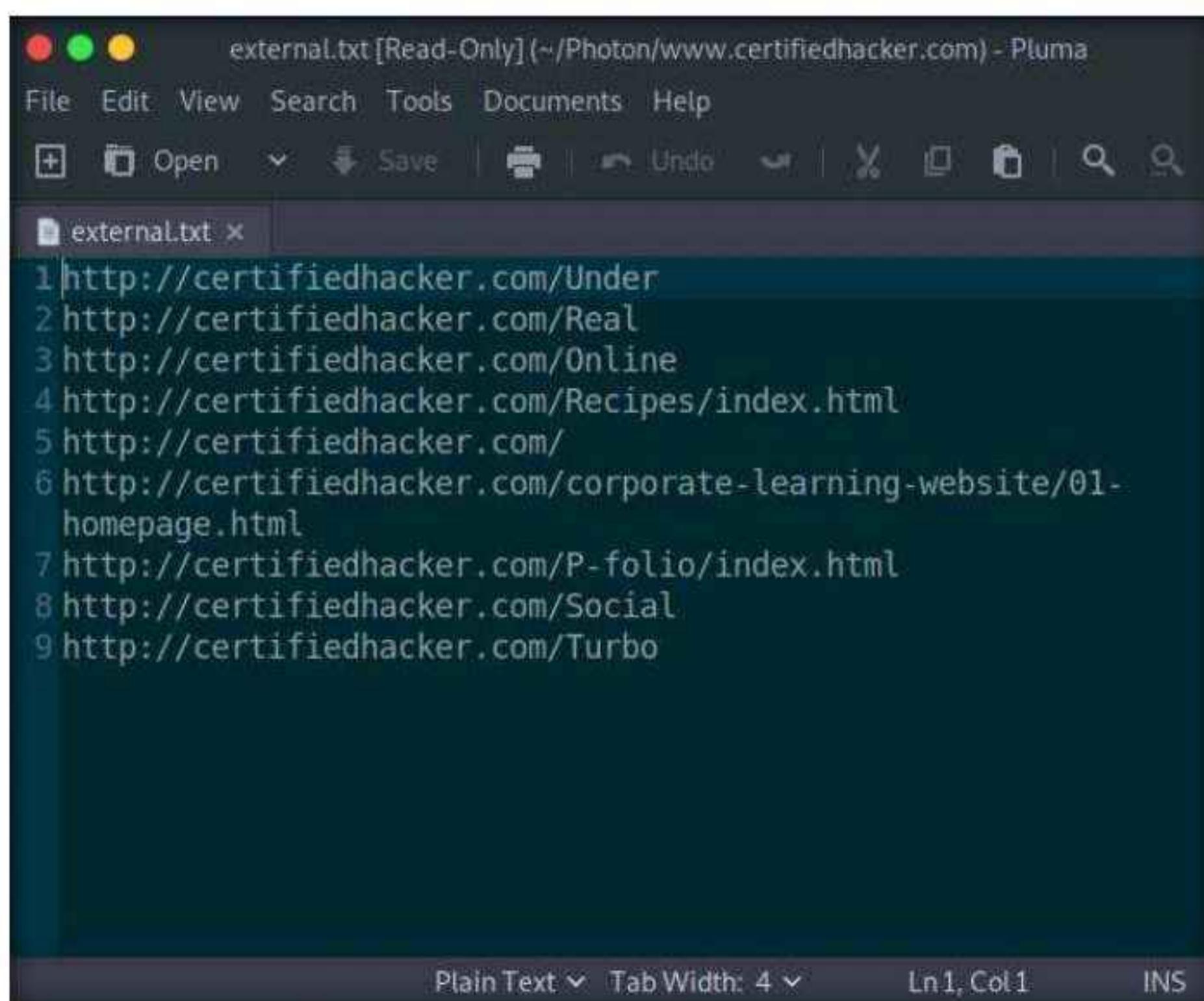
13. You can observe three text files in this folder: external, internal and scripts.



14. Double-click **external.txt** file to view the file content.

15. A **Pluma** text editor window appears showing the external URLs obtained using Photon.

**Note:** The output might vary when you perform the task.



16. Similarly, you can view internal and scripts text files containing URLs that are crawled by Photon tool.

17. Close **Pluma** text editor window and switch back to the **Terminal** window.

18. Now, type **python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 --wayback** and press **Enter** to crawl the target website using URLs from archive.org.

**Note:** -

- **-u:** specifies the target website (here, www.certifiedhacker.com)
- **-l:** specifies level to crawl (here, 3)
- **-t:** specifies number of threads (here, 200)
- **--wayback:** specifies using URLs from archive.org as seeds

**Note:** The output might vary when you perform the task.

```
python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 --wayback - Parrot Terminal
[~] Fetching URLs from archive.org
[+] Retrieved 0 URLs from archive.org
[~] Level 1: 2 URLs
[!] Progress: 2/2
[~] Level 2: 2 URLs
[!] Progress: 2/2
[~] Crawling 18 JavaScript files
[!] Progress: 18/18

[+] Internal: 4
[+] Scripts: 18
[+] External: 9

[!] Total requests made: 23
[!] Total time taken: 0 minutes 1 seconds
[!] Requests per second: 22
[+] Results saved in www.certifiedhacker.com directory
```

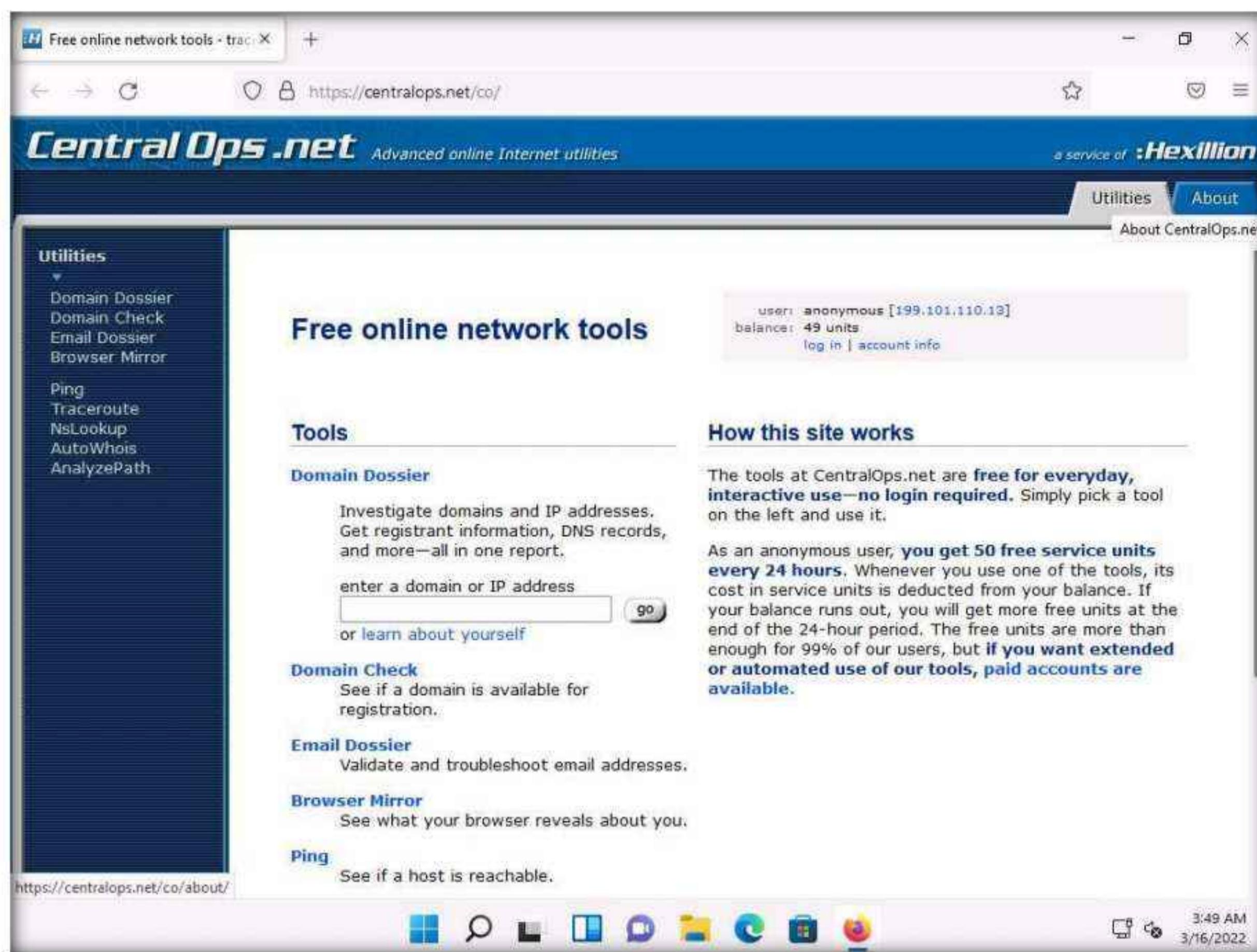
19. The results obtained are saved in **www.certifiedhacker.com** directory under Photon folder. You can navigate to the www.certifiedhacker.com folder to view the result.
20. You can further explore the Photon tool and perform various other functionalities such as the cloning of the target website, extracting secret keys and cookies, obtaining strings by specifying regex pattern, etc. Using this information, the attackers can perform various attacks on the target website such as brute-force attacks, denial-of-service attacks, injection attacks, phishing attacks and social engineering attacks.
21. This concludes the demonstration of gathering information on a target website using the Photon tool.
22. Close all open windows and document all the acquired information.
23. Turn off the **Parrot Security** virtual machine.

## Task 3: Gather Information About a Target Website using Central Ops

CentralOps ([centralops.net](https://centralops.net)) is a free online network scanner that investigates domains and IP addresses, DNS records, traceroute, nslookup, whois searches, etc.

**Note:** Here, we will consider [www.certifiedhacker.com](http://www.certifiedhacker.com) as a target website. However, you can select a target domain of your choice.

1. Switch to the **Windows 11** virtual machine. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type <https://centralops.net> and press **Enter**. The Central Ops website appears, as shown in the screenshot.



2. To extract information associated with the target organization website, type the target website's URL (here, [www.certifiedhacker.com](http://www.certifiedhacker.com)) in the **enter a domain or IP address** field, and then click on the **go** button, as shown in the screenshot below.

## Module 02 – Footprinting and Reconnaissance

The screenshot shows the CentralOps.net homepage. The URL in the address bar is https://centralops.net/co/. The page title is "Central Ops .net Advanced online Internet utilities". A banner at the top right says "a service of :Hexillion". On the left, a sidebar titled "Utilities" lists various tools: Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup, AutoWhois, and AnalyzePath. The main content area is titled "Free online network tools". It features a section titled "Tools" with a sub-section "Domain Dossier" which describes investigating domains and IP addresses. Below this are sections for "Domain Check", "Email Dossier", "Browser Mirror", and "Ping". A sidebar on the right titled "How this site works" explains that tools are free for everyday, interactive use (no login required) and mentions a 24-hour free unit limit. It also links to extended or automated use via paid accounts.

3. A search result for **WWW.CERTIFIEDHACKER.COM** containing information such as **Address lookup**, **Domain Whois record**, as shown in the screenshot.

The screenshot shows the "Domain Dossier" tool results for the domain www.certifiedhacker.com. The URL in the address bar is https://centralops.net/co/. The page title is "Central Ops .net Advanced online Internet utilities". The sidebar on the left remains the same. The main content area shows the "Domain Dossier" section with the sub-instruction "Investigate domains and IP addresses". It includes a form where "domain or IP address" is set to "www.certifiedhacker.com". Below the form are several checkboxes: "domain whois record" (checked), "DNS records" (checked), "traceroute" (unchecked), "network whois record" (checked), and "service scan" (unchecked). A "go" button is next to the checkboxes. At the bottom of this section, there is a user status message: "user: anonymous [199.101.110.13] balance: 48 units log in | account info". A note below the checkboxes states: "Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR." The "Address lookup" section shows the canonical name as "certifiedhacker.com.", aliases as "www.certifiedhacker.com", and address as "162.241.216.11". The "Domain Whois record" section shows the query to "whois.internic.net" for "dom certifiedhacker.com...". The results include the domain name "CERTIFIEDHACKER.COM", registry domain ID "88849376\_DOMAIN\_COM-VRSN", and registrar WHOIS Server "whois.networksolutions.com".

## Module 02 – Footprinting and Reconnaissance

4. Scroll-down to view information such as **Network Whois record** and **DNS records**, as shown in the screenshots. The attackers can use this information to perform injection attacks and other web application attacks on the target website.

The image displays two screenshots of the CentralOps.net website, which is a service of Hexillion. The top screenshot shows the 'Network Whois record' for the IP address 162.241.216.11. The results show details from rwhois.unifiedlayer.com and whois.arin.net. The bottom screenshot shows the 'DNS records' for the domain www.certifiedhacker.com, listing various A, CNAME, and NS records with their respective TTL values.

**Network Whois record**

Queried [rwhois.unifiedlayer.com](#) with "162.241.216.11"...

```
rwhois V-1.5:000080:00 rwhois.unifiedlayer.com (by Unified Layer, V-1.0.0)
network:Class-Name:network
network:ID:NETBLK-UL.162.240.0.0/15
network:Auth-Area: 162.240.0.0/15
network:Network-Name: UL-162.240.0.0/15
network:IP-Network: 162.240.0.0/15
network:Organization: Unified Layer
network:Tech-Contact: netops@unifiedlayer.com
network:Admin-Contact: netops@unifiedlayer.com
network:Abuse-Contact: abuse@unifiedlayer.com
network:Created: 20121119
network:Updated: 20121119
network:Updated-By: netops@unifiedlayer.com

$ok

Queried whois.arin.net with "n 162.241.216.11"...

NetRange: 162.240.0.0 - 162.241.255.255
CIDR: 162.240.0.0/15
NetName: UNIFIEDLAYER-NETWORK-16
NetHandle: NET-162-240-0-0-1
Parent: NET162 (NET-162-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS46606
Organization: Unified Layer (BLUEH-2)
RegDate: 2013-08-22
Updated: 2013-08-22
Ref: https://rdap.arin.net/registry/ip/162.240.0.0

OrgName: Unified Layer
OrgState: ARUNN-2
```

**DNS records**

name	class	type	data	time to live
www.certifiedhacker.com	IN	CNAME	certifiedhacker.com	14400s (04:00:00)
certifiedhacker.com	IN	NS	ns2.bluehost.com	81194s (22:33:14)
certifiedhacker.com	IN	NS	ns1.bluehost.com	81194s (22:33:14)
certifiedhacker.com	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
certifiedhacker.com	IN	NS	ns2.bluehost.com	48108s (13:21:48)
certifiedhacker.com	IN	NS	ns1.bluehost.com	48108s (13:21:48)
11.216.241.162.in-addr.arpa	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
216.241.162.in-addr.arpa	IN	NS	ns2.unifiedlayer.com	4022s (01:07:02)
216.241.162.in-addr.arpa	IN	NS	ns1.unifiedlayer.com	4022s (01:07:02)

5. This concludes the demonstration of gathering information about a target website using the Central Ops online tool.
6. You can also use tools such as **Website Informer** (<https://website.informer.com>), **Burp Suite** (<https://portswigger.net>), **Zaproxy** (<https://www.zaproxy.org>), etc. to perform website footprinting on a target website.
7. Close all open windows and document all the acquired information.

## Task 4: Extract a Company's Data using Web Data Extractor

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. 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.

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

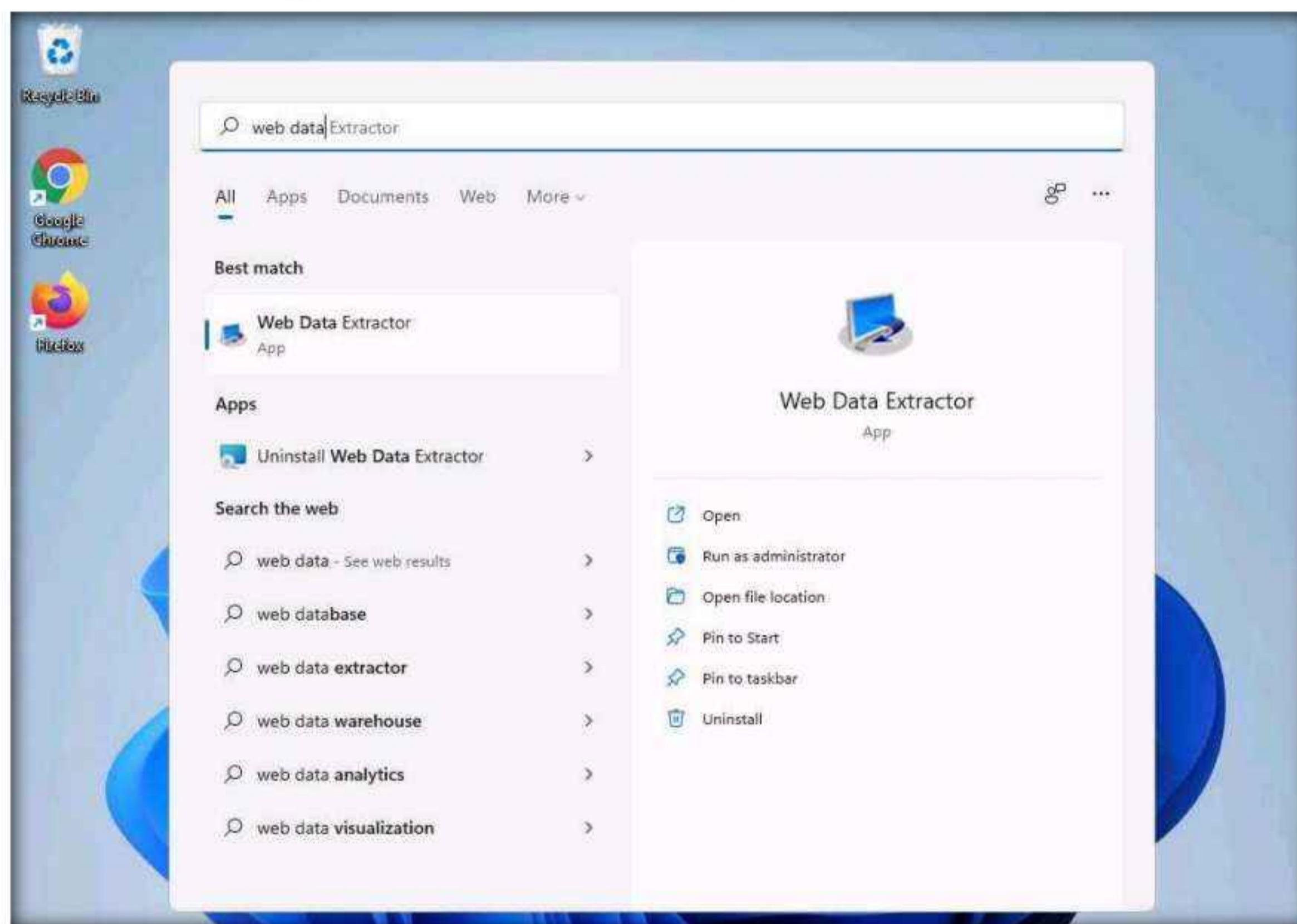
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wde.exe**.

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

2. If the **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard steps to install Web Data Extractor and click **Finish**.

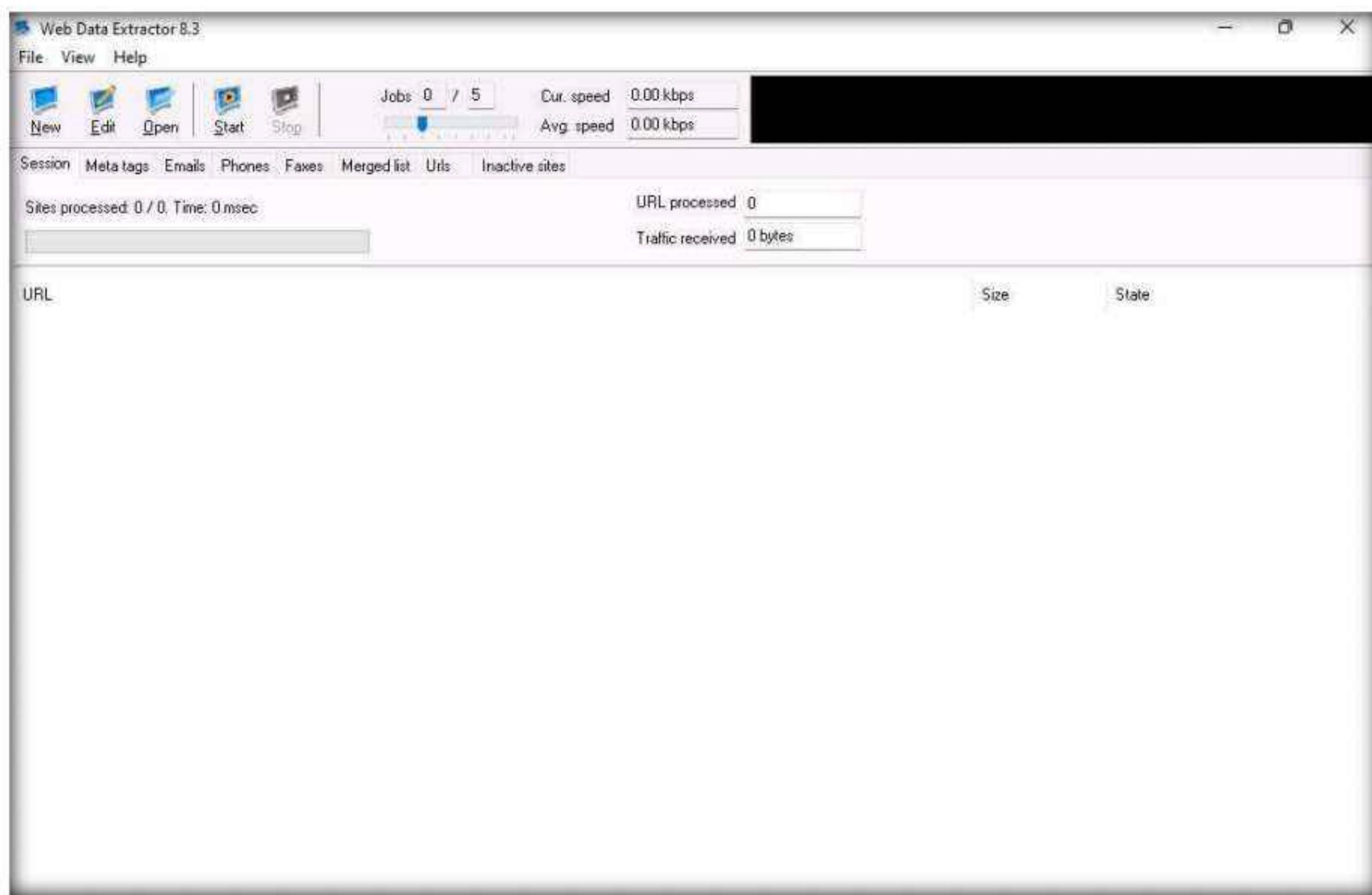


4. Click **Search icon** (🔍) on the **Desktop** and type **web data** in the search field. The **Web Data Extractor** appears in the results, click **Open** to launch it.

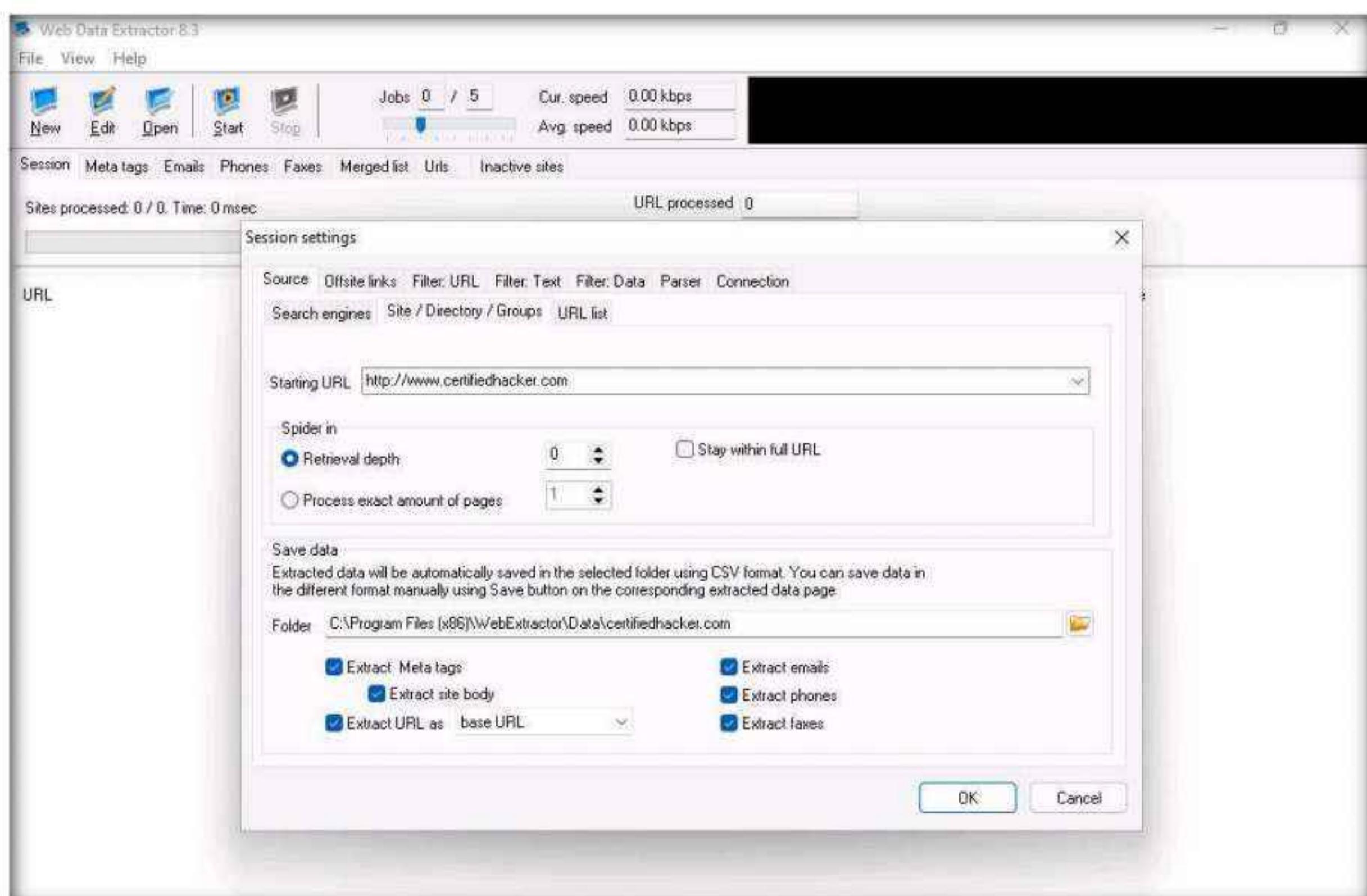


## Module 02 – Footprinting and Reconnaissance

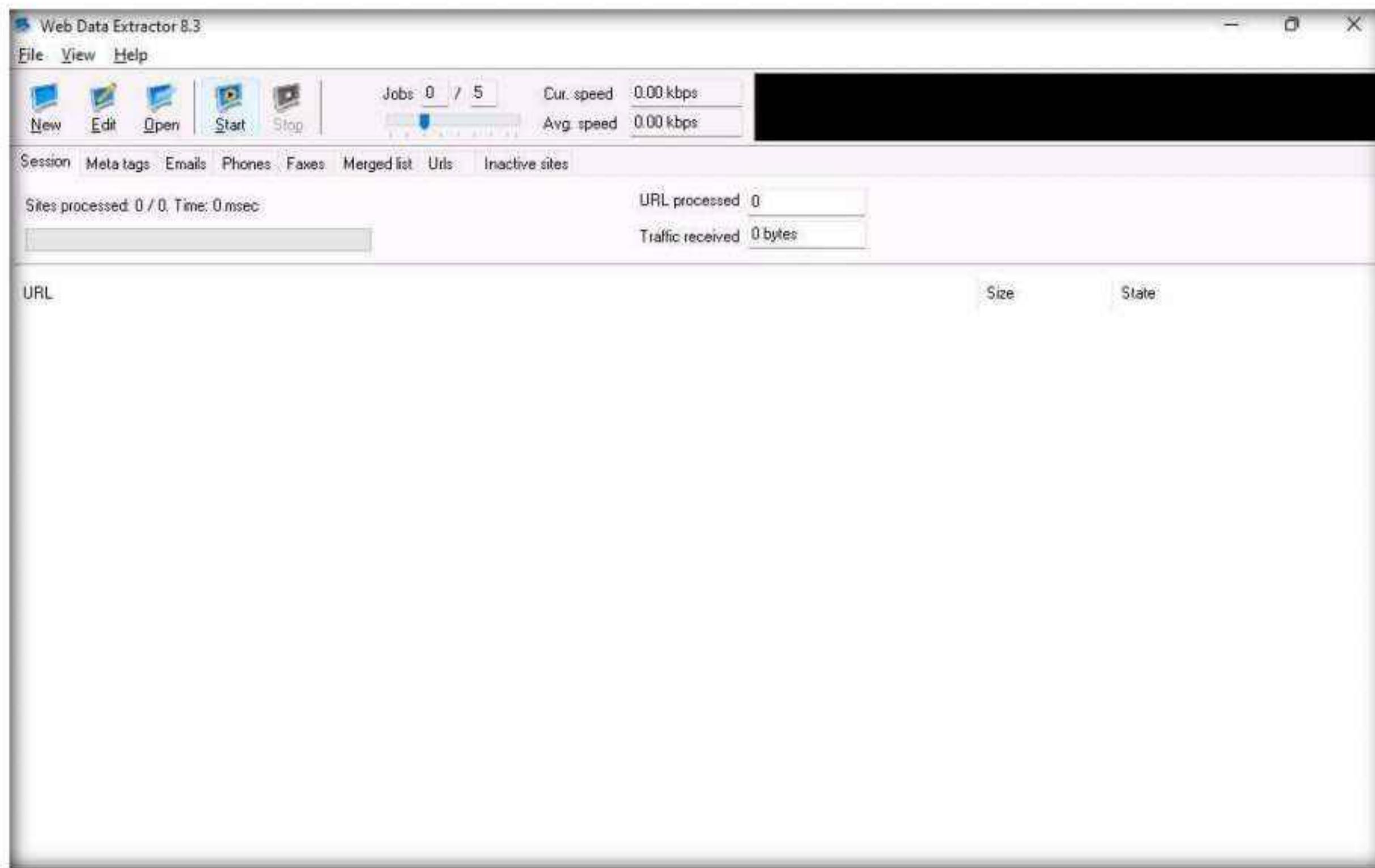
5. The **Web Data Extractor** main window appears. Click **New** to start a new session.



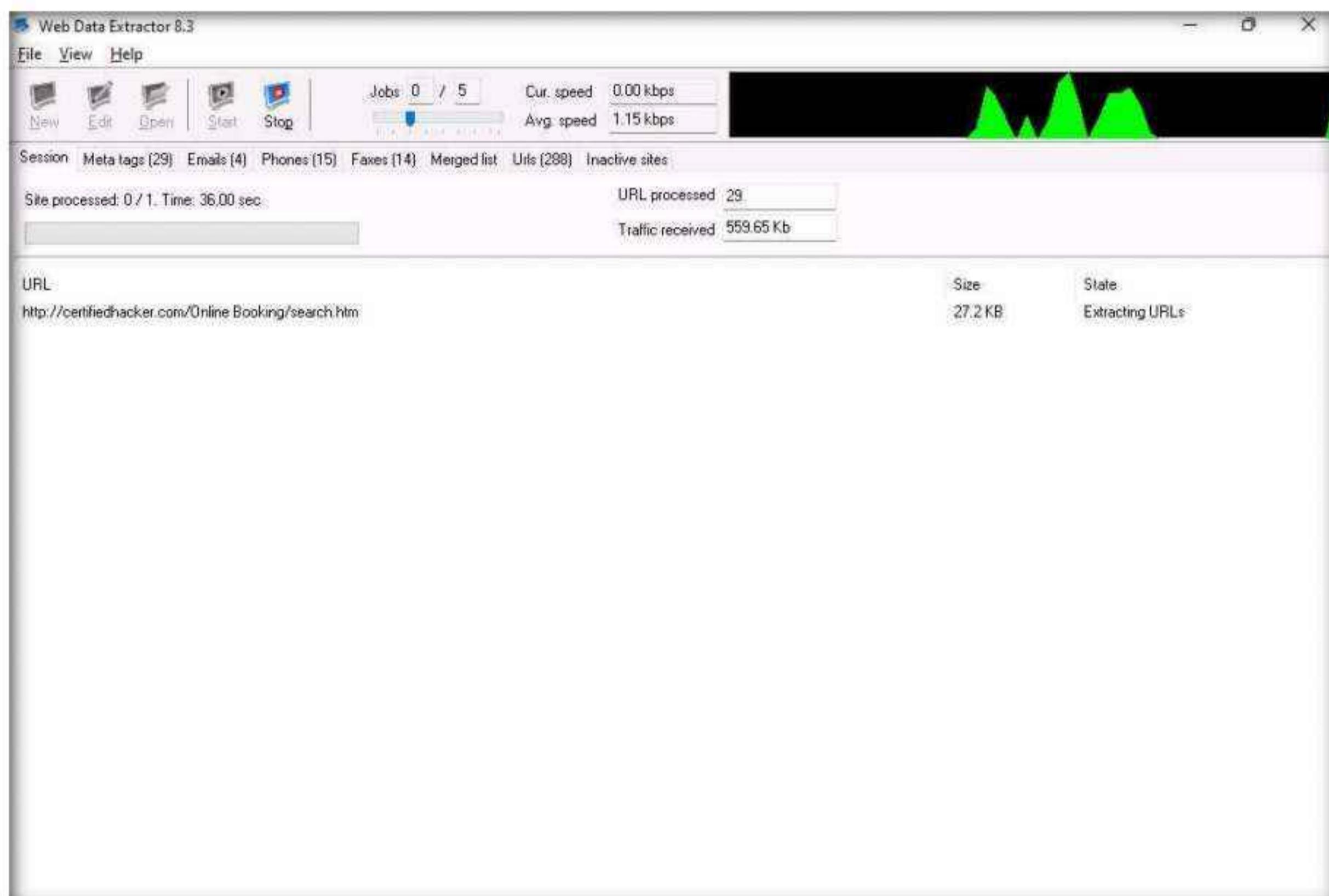
6. The **Session settings** window appears; type a URL (here, <http://www.certifiedhacker.com>) in the **Starting URL** field. Check all the options, as shown in the screenshot, and click **OK**.



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



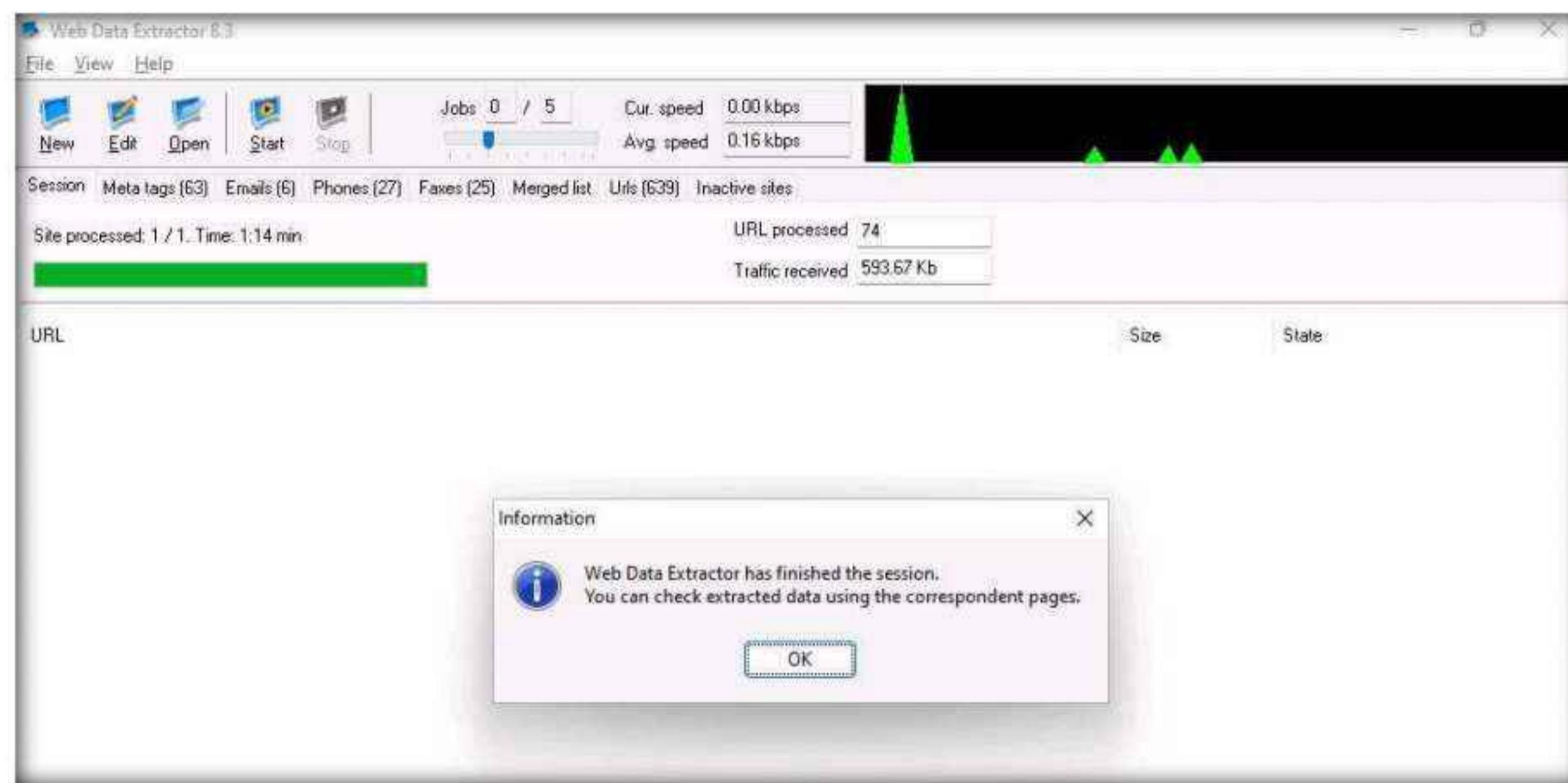
8. **Web Data Extractor** will start collecting information (**Session, Meta tags, Emails, Phones, Faxes, Merged list, URLs, and Inactive sites**).



## Module 02 – Footprinting and Reconnaissance

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

**Note:** The results might vary when you perform the task.



- View the extracted information by clicking the tabs.

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

URL	Title	Keywords	Description	Host	Domain	Page size	Page last modified	Key
http://certifiedhacker.com/Online Booking/ Online Booking: Hotel Info		booking, hotel, hote	Online Booking	http://certifiedha.com	39498	2/10/2011		
http://certifiedhacker.com/Online Booking/ Online Booking: Print Preview		booking, hotel, hote	Online Booking	http://certifiedha.com	5693	2/10/2011		
http://certifiedhacker.com/P-folio/about.htm P-Folio				http://certifiedha.com	9307	2/10/2011		
http://certifiedhacker.com/P-folio/blog.html P-Folio				http://certifiedha.com	9464	2/10/2011		
http://certifiedhacker.com/P-folio/contact.htm P-Folio				http://certifiedha.com	8531	2/10/2011		
http://certifiedhacker.com/P-folio/portfolio.htm P-Folio				http://certifiedha.com	10049	2/10/2011		
http://certifiedhacker.com/Real Estates/pa Professional Real Estate Service   Real Esta real estate, real est: Professional Real Estate Servic	Professional Real Estate Service   Real Esta real estate, real est: Professional Real Estate Servic	http://certifiedha.com	3683	2/10/2011				
http://certifiedhacker.com/Real Estates/pa Professional Real Estate Service   Real Esta real estate, real est: Professional Real Estate Servic	Professional Real Estate Service   Real Esta real estate, real est: Professional Real Estate Servic	http://certifiedha.com	4352	2/10/2011				
http://certifiedhacker.com/Real Estates/pa Professional Real Estate Service   Real Esta real estate, real est: Professional Real Estate Servic	Professional Real Estate Service   Real Esta real estate, real est: Professional Real Estate Servic	http://certifiedha.com	5767	2/10/2011				
http://certifiedhacker.com/Real Estates/pa Professional Real Estate Service   Real Esta real estate, real est: Professional Real Estate Servic	Professional Real Estate Service   Real Esta real estate, real est: Professional Real Estate Servic	http://certifiedha.com	5789	2/10/2011				
http://certifiedhacker.com/Recipes/about Your company - About us	Some keywords the A short description of your comp	http://certifiedha.com	5762	2/10/2011				
http://certifiedhacker.com/Recipes/apple_ Your company - Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	10147	2/10/2011				
http://certifiedhacker.com/Recipes/Chicke Your company - Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	10081	2/10/2011				
http://certifiedhacker.com/Recipes/Chicke Your company - Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	9594	2/10/2011				
http://certifiedhacker.com/Recipes/Chines Your company - Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	9635	2/10/2011				
http://certifiedhacker.com/Recipes/contact Your company - Contact us	Some keywords the A short description of your comp	http://certifiedha.com	5828	2/10/2011				
http://certifiedhacker.com/Recipes/honey_ Your company - Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	9355	2/10/2011				
http://certifiedhacker.com/Recipes/kebab_ Your company - Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	8397	2/10/2011				
http://certifiedhacker.com/Recipes/menu Your company - Menu	Some keywords the A short description of your comp	http://certifiedha.com	7909	2/10/2011				
http://certifiedhacker.com/Recipes/recipes Your company - Recipes	Some keywords the A short description of your comp	http://certifiedha.com	12716	2/10/2011				
http://certifiedhacker.com/Recipes/tando Your company - Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	8862	2/10/2011				
http://certifiedhacker.com/Recipes/recipes Your company - Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	10804	2/10/2011				
http://certifiedhacker.com/Recipes/menu Your company - Menu category	Some keywords the A short description of your comp	http://certifiedha.com	11584	2/10/2011				
http://certifiedhacker.com/Recipes/recipes Your company - Recipes category	Some keywords the A short description of your comp	http://certifiedha.com	12451	2/10/2011				
http://certifiedhacker.com/Social Media/at Unite - Together is Better (created by Parallel keywords, or phrase A brief description of this website)	http://certifiedha.com	13274	2/10/2011					
http://certifiedhacker.com/Social Media/sa Unite - Together is Better (created by Parallel keywords, or phrase A brief description of this website)	http://certifiedha.com	16239	2/10/2011					
http://certifiedhacker.com/Social Media/sa Unite - Together is Better (created by Parallel keywords, or phrase A brief description of this website)	http://certifiedha.com	12143	2/10/2011					
http://certifiedhacker.com/Social Media/sa	http://certifiedha.com	1489	2/10/2011					
http://certifiedhacker.com/Social Media/sa Unite - Together is Better (created by Parallel keywords, or phrase A brief description of this website)	http://certifiedha.com	16259	2/10/2011					
http://certifiedhacker.com/Turbo Max/hepn	http://certifiedha.com	5227	2/10/2011					
http://certifiedhacker.com/Under the trees/ Under the Trees	http://certifiedha.com	8593	2/10/2011					
http://certifiedhacker.com/Under the trees/ Under the Trees	http://certifiedha.com	2963	2/10/2011					
http://certifiedhacker.com/Under the trees/ Under the Trees	http://certifiedha.com	15932	2/10/2011					

## Module 02 – Footprinting and Reconnaissance

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

The screenshot shows the 'Emails' tab selected in the software interface. The table displays the following data:

Email	Name	URL	Title
contact@unite-magazine-community.com	contact	http://certifiedhacker.com/Social Media/index.html	Unite - Together is Better [created by Parallelus]
info@introspire.web	info	http://certifiedhacker.com/corporate-learning-website/contact	
sales@introspire.web	sales	http://certifiedhacker.com/corporate-learning-website/contact	
support@introspire.web	support	http://certifiedhacker.com/corporate-learning-website/contact	
aalia@alsan.com	aalia	http://certifiedhacker.com/P-folio/contact.html	P-Folio
contact@bonapetit.com	contact	http://certifiedhacker.com/Recipes/recipes.html	Your company - Recipes

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

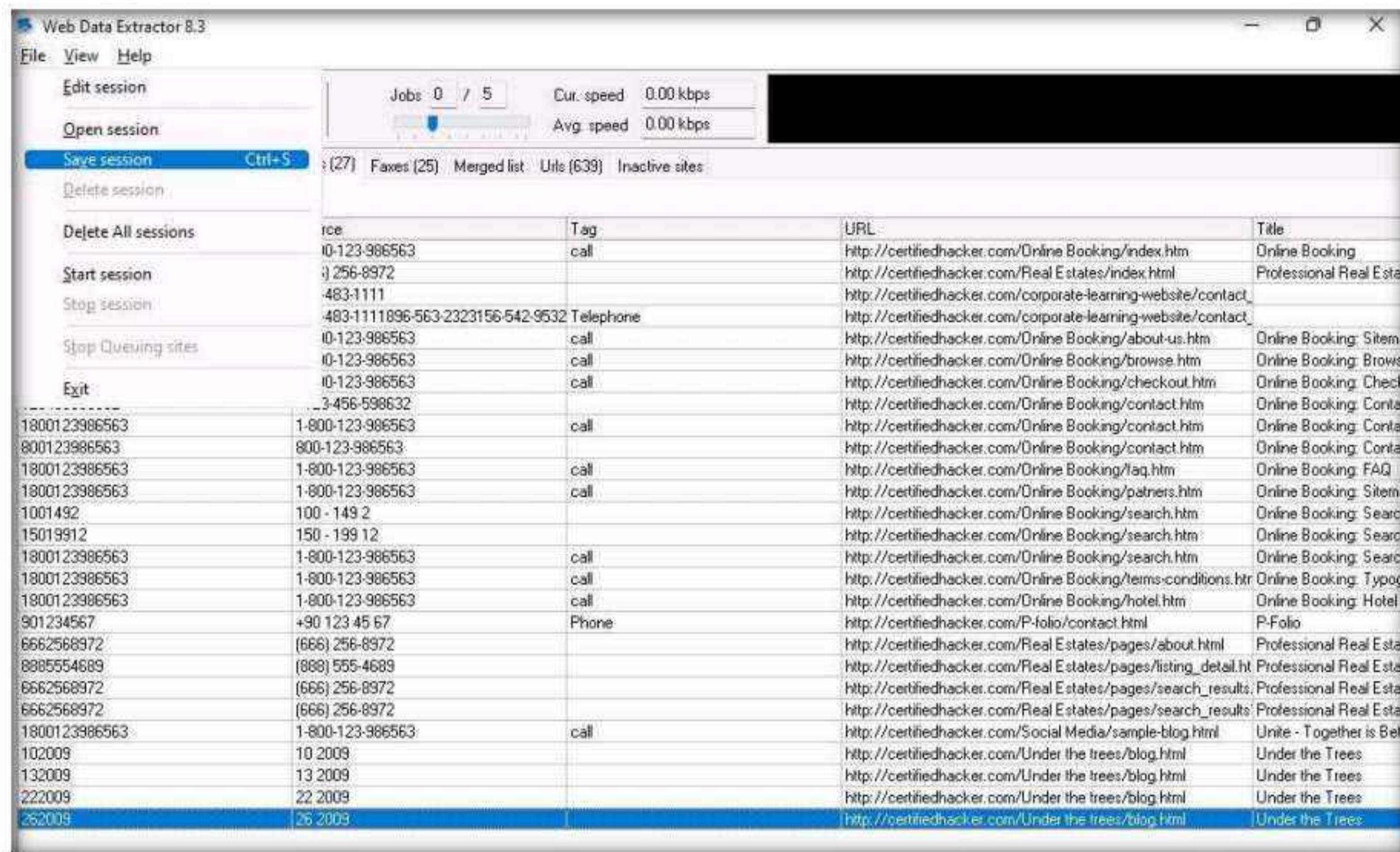
The screenshot shows the 'Phones' tab selected in the software interface. The table displays the following data:

Phone	Source	Tag	URL	Title
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/index.htm	Online Booking
6662568972	(666) 256-8972		http://certifiedhacker.com/Real Estates/index.html	Professional Real Estat
2024831111	202-483-1111		http://certifiedhacker.com/corporate-learning-website/contact	
202483111189656323231565429532	202-483-1111896-563-2323156-542-9532	Telephone	http://certifiedhacker.com/corporate-learning-website/contact	
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/about-us.htm	Online Booking: Sitem
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/browse.htm	Online Booking: Brows
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/checkout.htm	Online Booking: Check
123456598632	+123-456-598632		http://certifiedhacker.com/Online Booking/contact.htm	Online Booking: Conta
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/contact.htm	Online Booking: Conta
8000123986563	800-123-986563		http://certifiedhacker.com/Online Booking/contact.htm	Online Booking: Conta
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/faq.htm	Online Booking: FAQ
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/partners.htm	Online Booking: Sitem
1001492	100 - 149.2		http://certifiedhacker.com/Online Booking/search.htm	Online Booking: Search
15019912	150 - 199.12		http://certifiedhacker.com/Online Booking/search.htm	Online Booking: Search
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/search.htm	Online Booking: Search
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/terms-conditions.htm	Online Booking: Typog
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Online Booking/hotel.htm	Online Booking: Hotel
901234567	+90 123 45 67	Phone	http://certifiedhacker.com/P-folio/contact.html	P-Folio
6662568972	(666) 256-8972		http://certifiedhacker.com/Real Estates/pages/about.html	Professional Real Esta
8885554689	(888) 555-4689		http://certifiedhacker.com/Real Estates/pages/listing_detail.htm	Professional Real Esta
6662568972	(666) 256-8972		http://certifiedhacker.com/Real Estates/pages/search_results	Professional Real Esta
6662568972	(666) 256-8972		http://certifiedhacker.com/Real Estates/pages/search_results	Professional Real Esta
1800123986563	1-800-123-986563	call	http://certifiedhacker.com/Social Media/sample-blog.html	Unite - Together is Bell
102009	10 2009		http://certifiedhacker.com/Under the trees/blog.html	Under the Trees
132009	13 2009		http://certifiedhacker.com/Under the trees/blog.html	Under the Trees
222009	22 2009		http://certifiedhacker.com/Under the trees/blog.html	Under the Trees
262009	26 2009		http://certifiedhacker.com/Under the trees/blog.html	Under the Trees

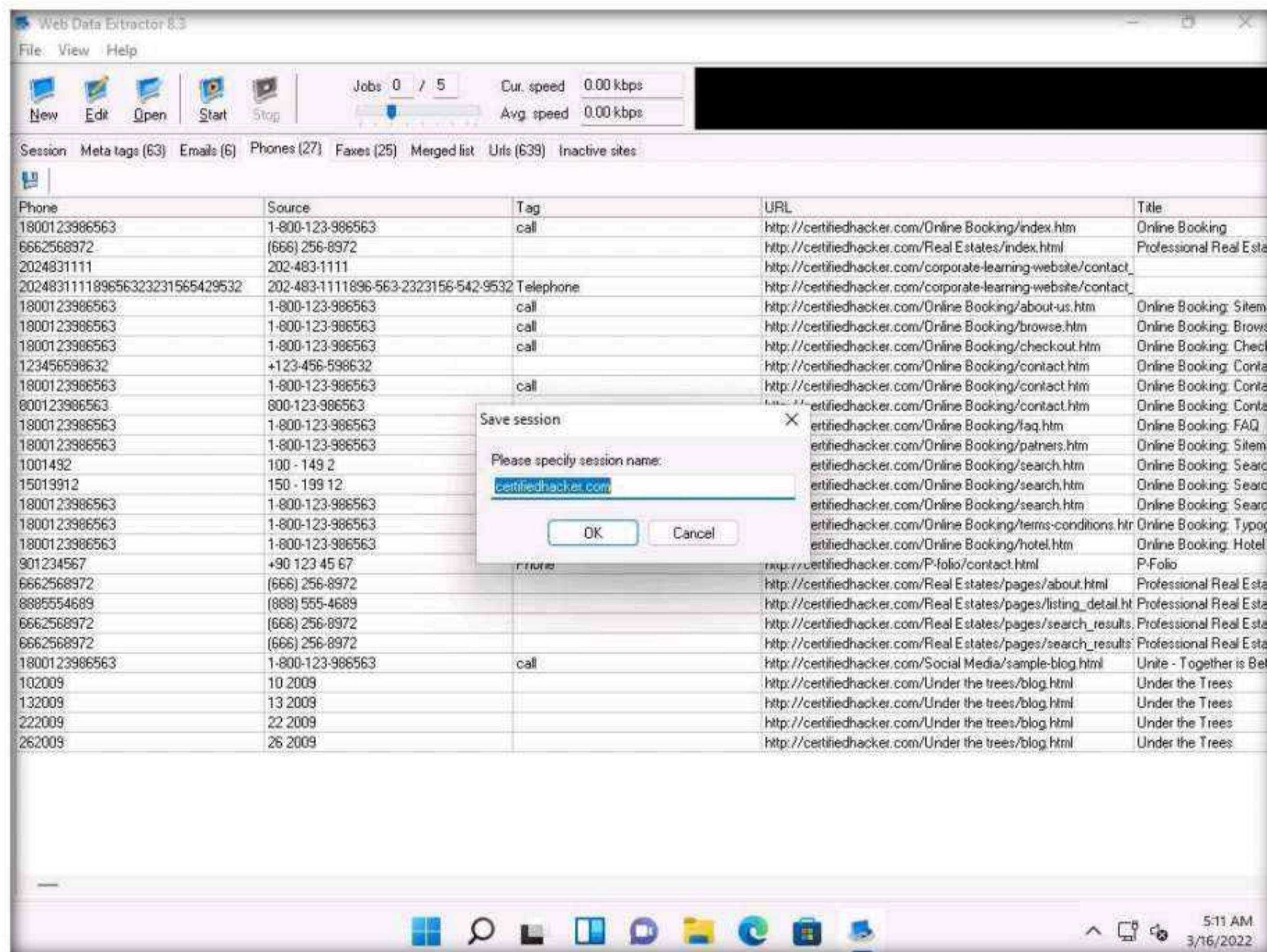
14. Check for more information under the **Faxes**, **Merged list**, **URLs**, and **Inactive sites** tabs.

## Module 02 – Footprinting and Reconnaissance

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



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



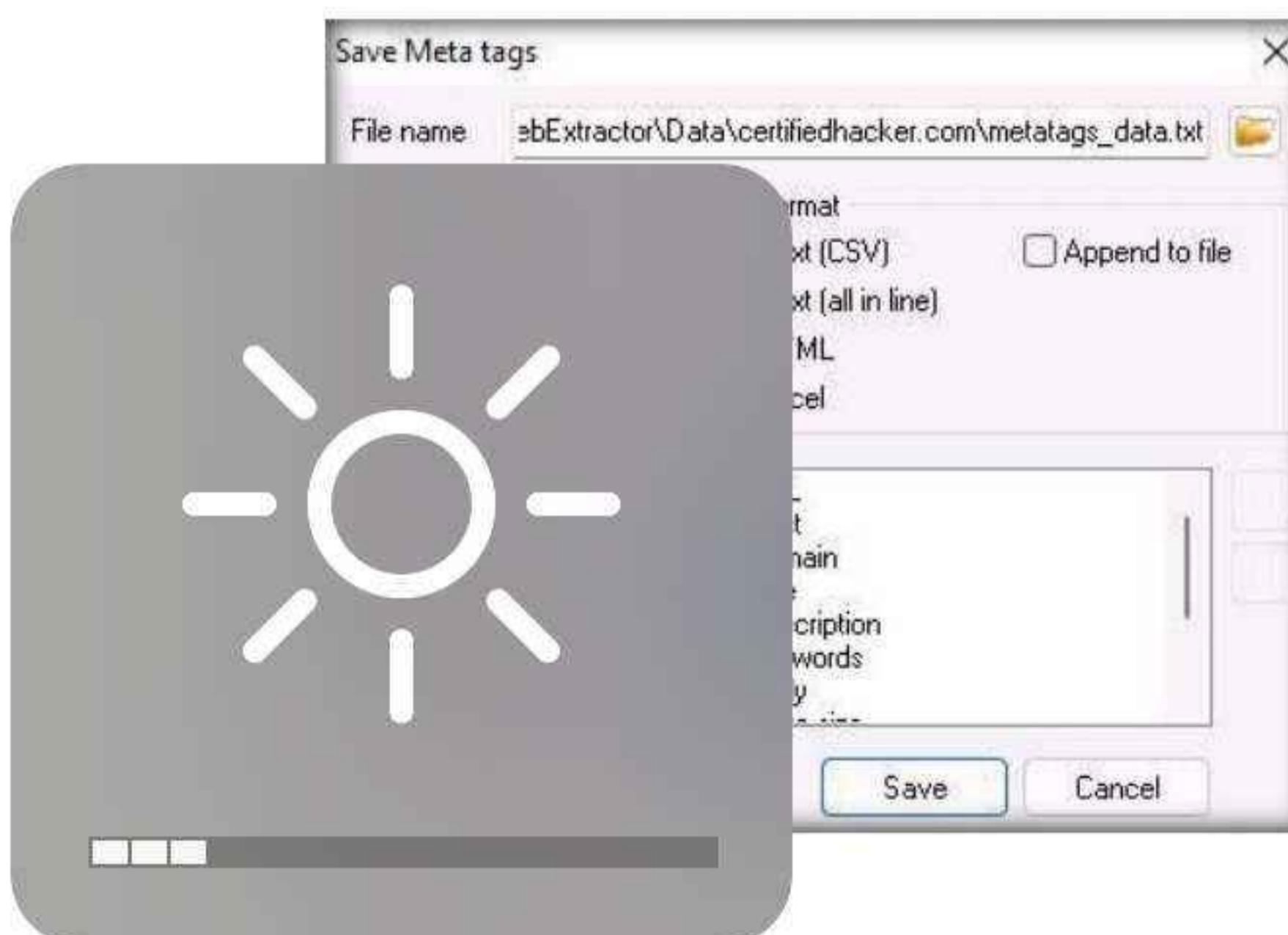
## Module 02 – Footprinting and Reconnaissance

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

URL	Title	Keywords	Description	Host	Domain	Page size	Page last modified	Key
http://certifiedhacker.com/Online Booking/ Online Booking: Hotel Info	Online Booking: Hotel Info	booking, hotel, hotel	Online Booking	http://certifiedha.com	33498	2/10/2011		
http://certifiedhacker.com/Online Booking/ Online Booking: Print Preview	Online Booking: Print Preview	booking, hotel, hotel	Online Booking	http://certifiedha.com	5693	2/10/2011		
http://certifiedhacker.com/P-folio/about hit P-Folio				http://certifiedha.com	9307	2/10/2011		
http://certifiedhacker.com/P-folio/blog.html P-Folio				http://certifiedha.com	9464	2/10/2011		
http://certifiedhacker.com/P-folio/contact.html P-Folio				http://certifiedha.com	8531	2/10/2011		
http://certifiedhacker.com/P-folio/portfolio.html P-Folio				http://certifiedha.com	10049	2/10/2011		
http://certifiedhacker.com/Real Estates/pa Professional Real Estate Service   Real Estate real estate, real est	Professional Real Estate Service   Real Esta real estate, real est	Professional Real Estate Servic	http://certifiedha.com	3683	2/10/2011			
http://certifiedhacker.com/Real Estates/pa Professional Real Estate Service   Real Esta real estate, real est	Professional Real Estate Service   Real Esta real estate, real est	Professional Real Estate Servic	http://certifiedha.com	4352	2/10/2011			
http://certifiedhacker.com/Real Estates/pa Professional Real Estate Service   Real Esta real estate, real est	Professional Real Estate Service   Real Esta real estate, real est	Professional Real Estate Servic	http://certifiedha.com	5767	2/10/2011			
http://certifiedhacker.com/Real Estates/pa Professional Real Estate Service   Real Esta real estate, real est	Professional Real Estate Service   Real Esta real estate, real est	Professional Real Estate Servic	http://certifiedha.com	5789	2/10/2011			
http://certifiedhacker.com/Recipes/about.html Your company - About us	Your company - About us	Some keywords the A short description of your comp	http://certifiedha.com	5762	2/10/2011			
http://certifiedhacker.com/Recipes/apple_ Your company - Recipes detail	Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	10147	2/10/2011			
http://certifiedhacker.com/Recipes/Chicks Your company - Recipes detail	Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	10081	2/10/2011			
http://certifiedhacker.com/Recipes/Chicken Your company - Recipes detail	Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	9594	2/10/2011			
http://certifiedhacker.com/Recipes/Chines Your company - Recipes detail	Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	9635	2/10/2011			
http://certifiedhacker.com/Recipes/contact Your company - Contact us	Contact us	Some keywords the A short description of your comp	http://certifiedha.com	5828	2/10/2011			
http://certifiedhacker.com/Recipes/honey_ Your company - Recipes detail	Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	9355	2/10/2011			
http://certifiedhacker.com/Recipes/kebab_ Your company - Recipes detail	Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	8397	2/10/2011			
http://certifiedhacker.com/Recipes/menu_ Your company - Menu	Menu	Some keywords the A short description of your comp	http://certifiedha.com	7909	2/10/2011			
http://certifiedhacker.com/Recipes/recipes_ Your company - Recipes	Recipes	Some keywords the A short description of your comp	http://certifiedha.com	12716	2/10/2011			
http://certifiedhacker.com/Recipes/tandoor_ Your company - Recipes detail	Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	8862	2/10/2011			
http://certifiedhacker.com/Recipes/recipes_ Your company - Recipes detail	Recipes detail	Some keywords the A short description of your comp	http://certifiedha.com	10804	2/10/2011			
http://certifiedhacker.com/Recipes/menus_ Your company - Menu category	Menu category	Some keywords the A short description of your comp	http://certifiedha.com	11584	2/10/2011			
http://certifiedhacker.com/Recipes/recipes_ Your company - Recipes category	Recipes category	Some keywords the A short description of your comp	http://certifiedha.com	12451	2/10/2011			
http://certifiedhacker.com/Social Media/at Unite - Together is Better (created by Parallel keywords, or phrase)	A brief description of this website	A brief description of this website	http://certifiedha.com	13274	2/10/2011			
http://certifiedhacker.com/Social Media/za Unite - Together is Better (created by Parallel keywords, or phrase)	A brief description of this website	A brief description of this website	http://certifiedha.com	16239	2/10/2011			
http://certifiedhacker.com/Social Media/za Unite - Together is Better (created by Parallel keywords, or phrase)	A brief description of this website	A brief description of this website	http://certifiedha.com	12143	2/10/2011			
http://certifiedhacker.com/Social Media/za			http://certifiedha.com	1489	2/10/2011			
http://certifiedhacker.com/Social Media/za Unite - Together is Better (created by Parallel keywords, or phrase)	A brief description of this website	A brief description of this website	http://certifiedha.com	16259	2/10/2011			
http://certifiedhacker.com/Turbo Max/epn			http://certifiedha.com	5227	2/10/2011			
http://certifiedhacker.com/Under the trees/ Under the Trees			http://certifiedha.com	8593	2/10/2011			
http://certifiedhacker.com/Under the trees/ Under the Trees			http://certifiedha.com	2963	2/10/2011			
http://certifiedhacker.com/Under the trees/ Under the Trees			http://certifiedha.com	5932	2/10/2011			

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

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**. The gathered information can be used by the attackers to launch attacks such as social engineering and web application attacks on the target website.



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

## **Task 5: Mirror a Target Website using HTTrack Web Site Copier**

---

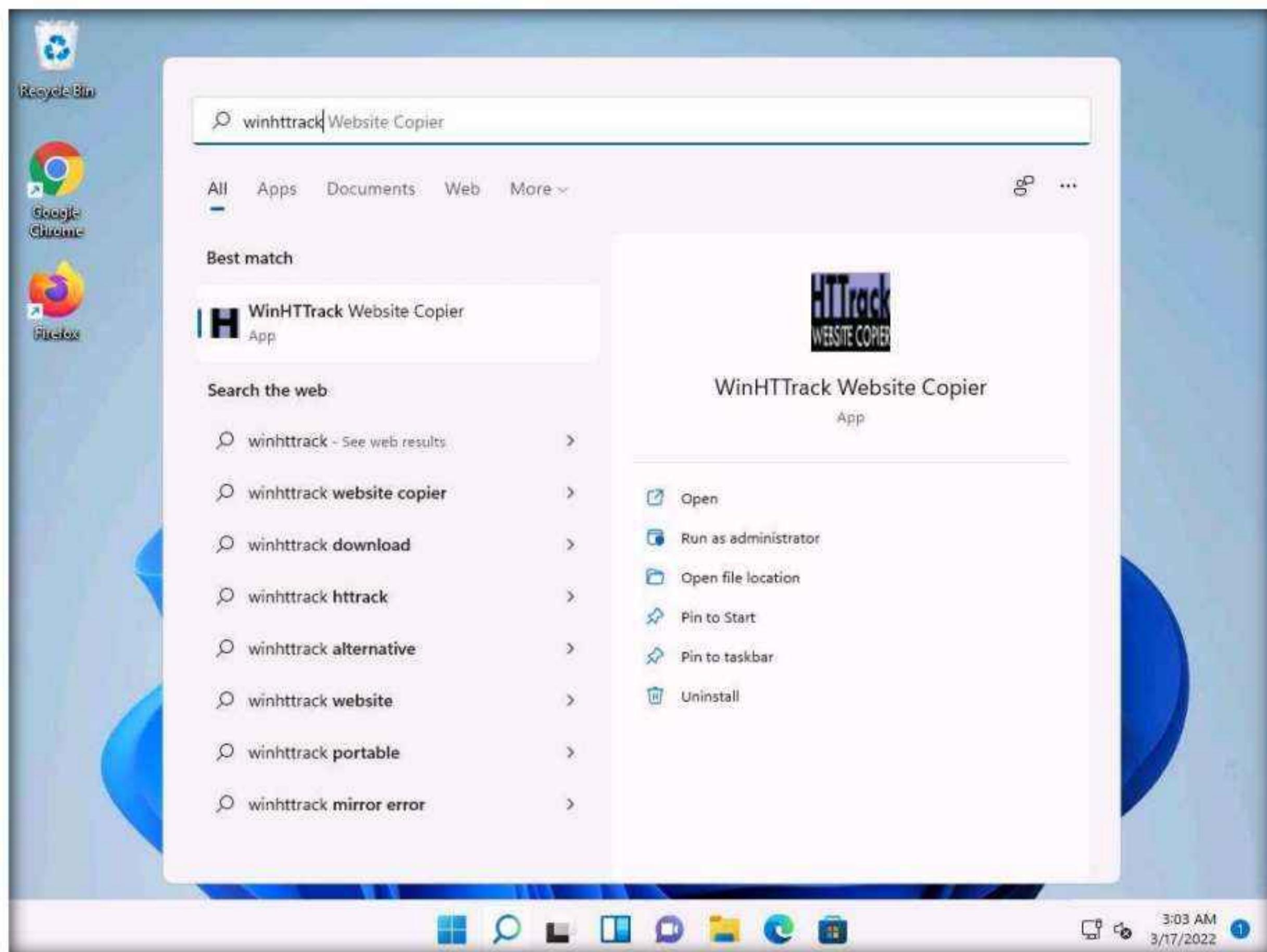
Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos,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

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.

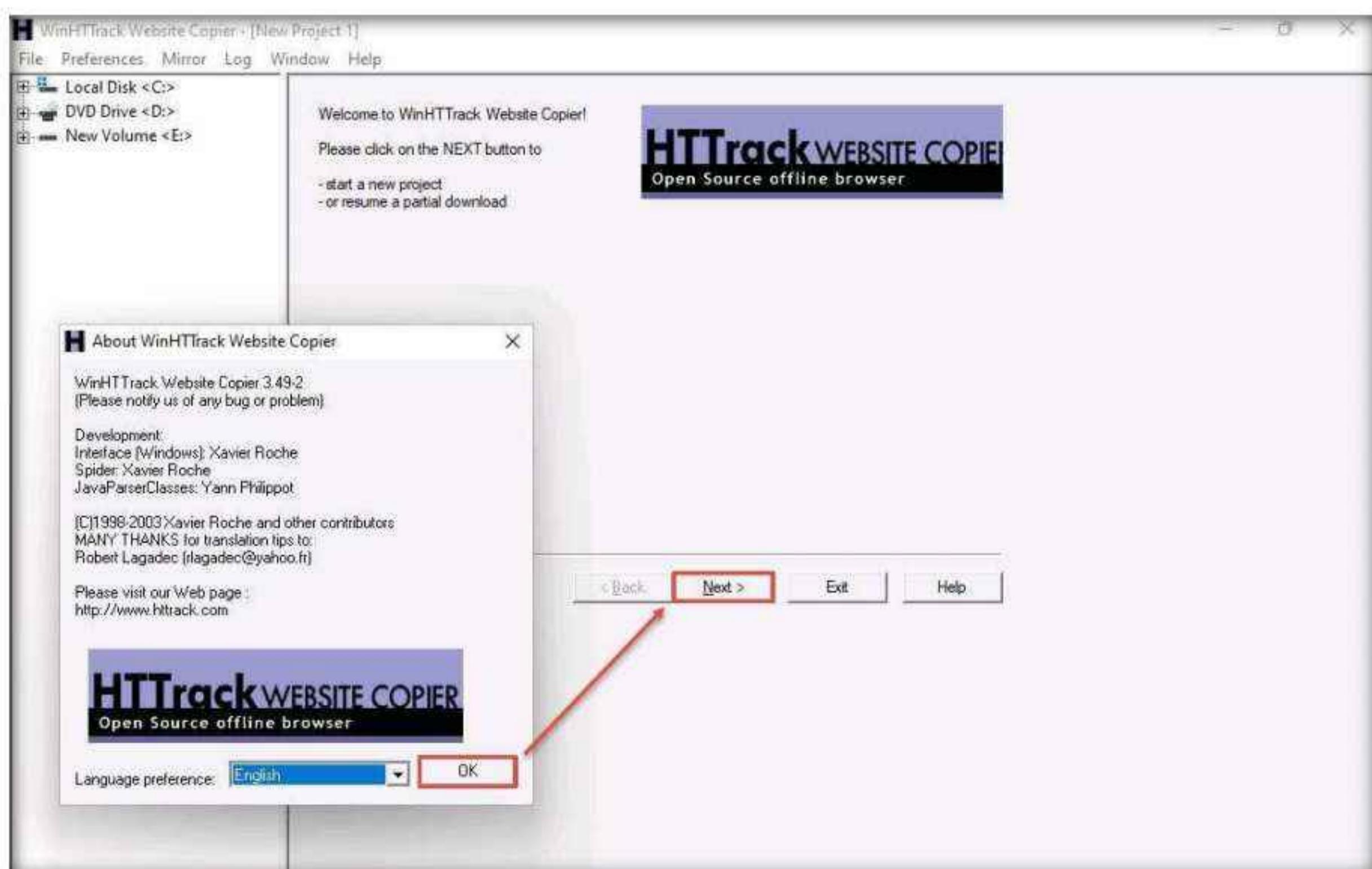
Here, we will use the HTTrack Web Site Copier tool to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

**Note:** Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. In the **Windows 11** virtual machine, click **Search icon** (  ) on the **Desktop** and type **winhttrack** in the search field. The **WinHTTrack Website Copier** appears in the results, click **Open** to launch it.

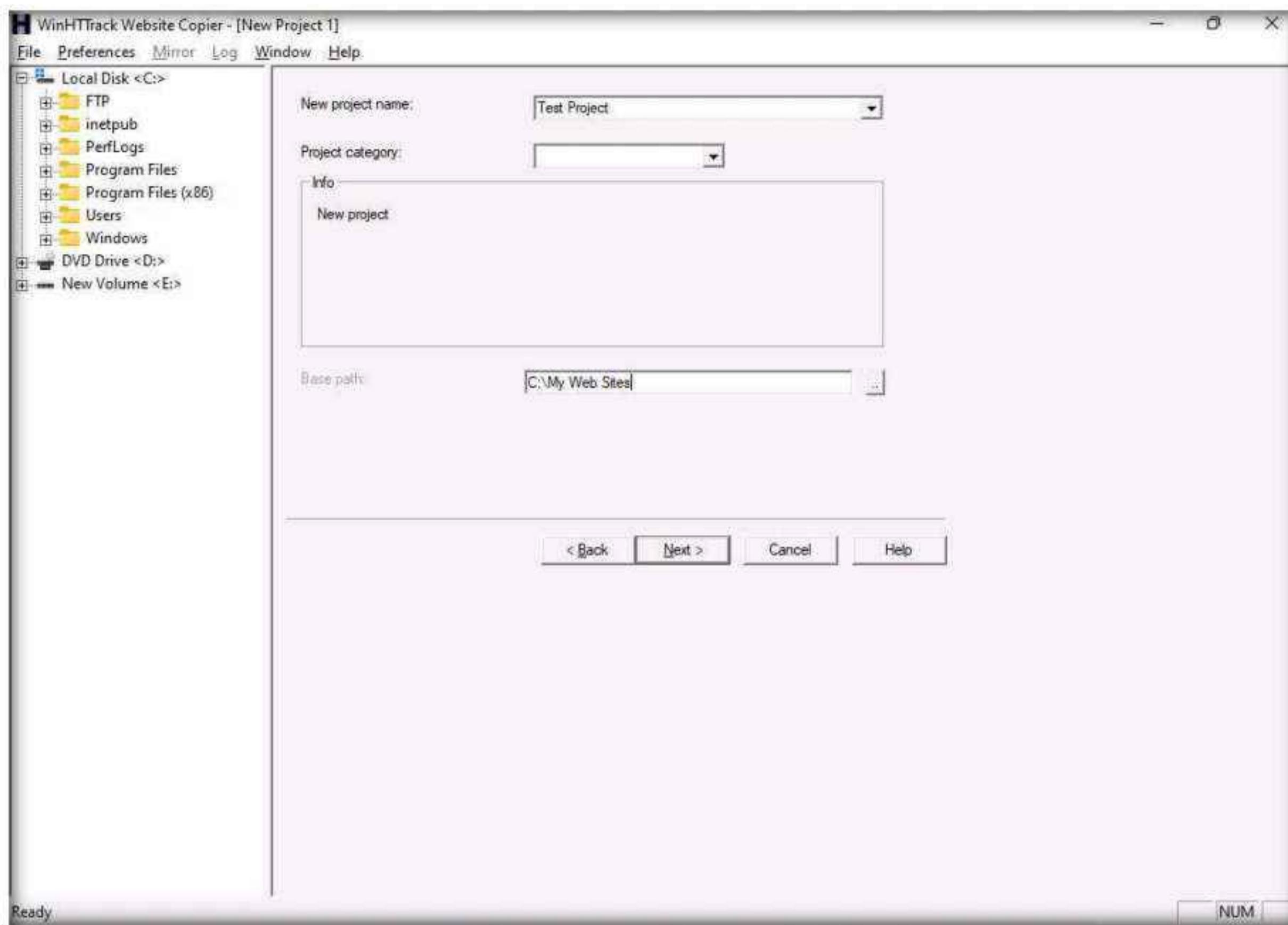


2. The **About WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.

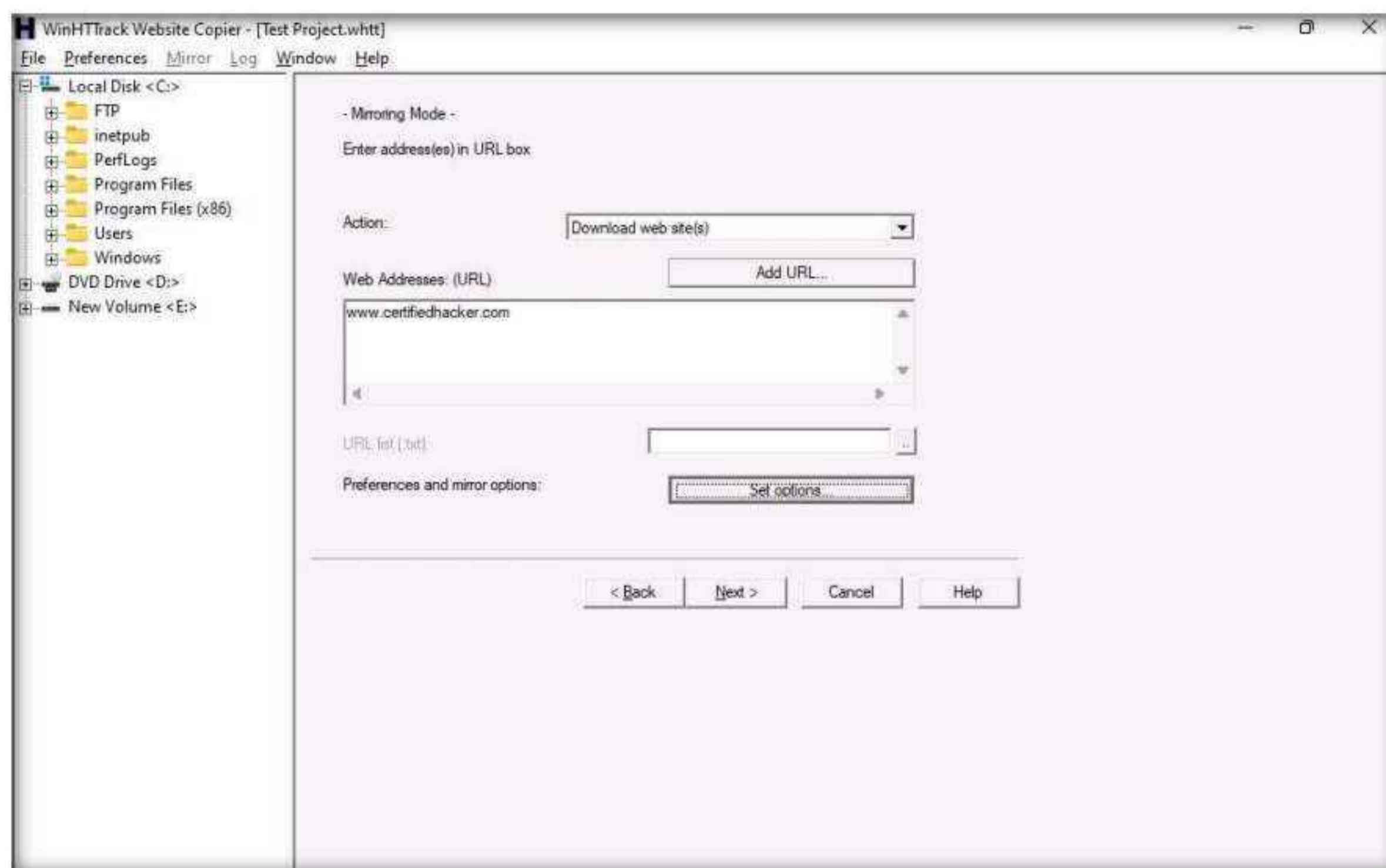


## Module 02 – Footprinting and Reconnaissance

3. 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 >**.

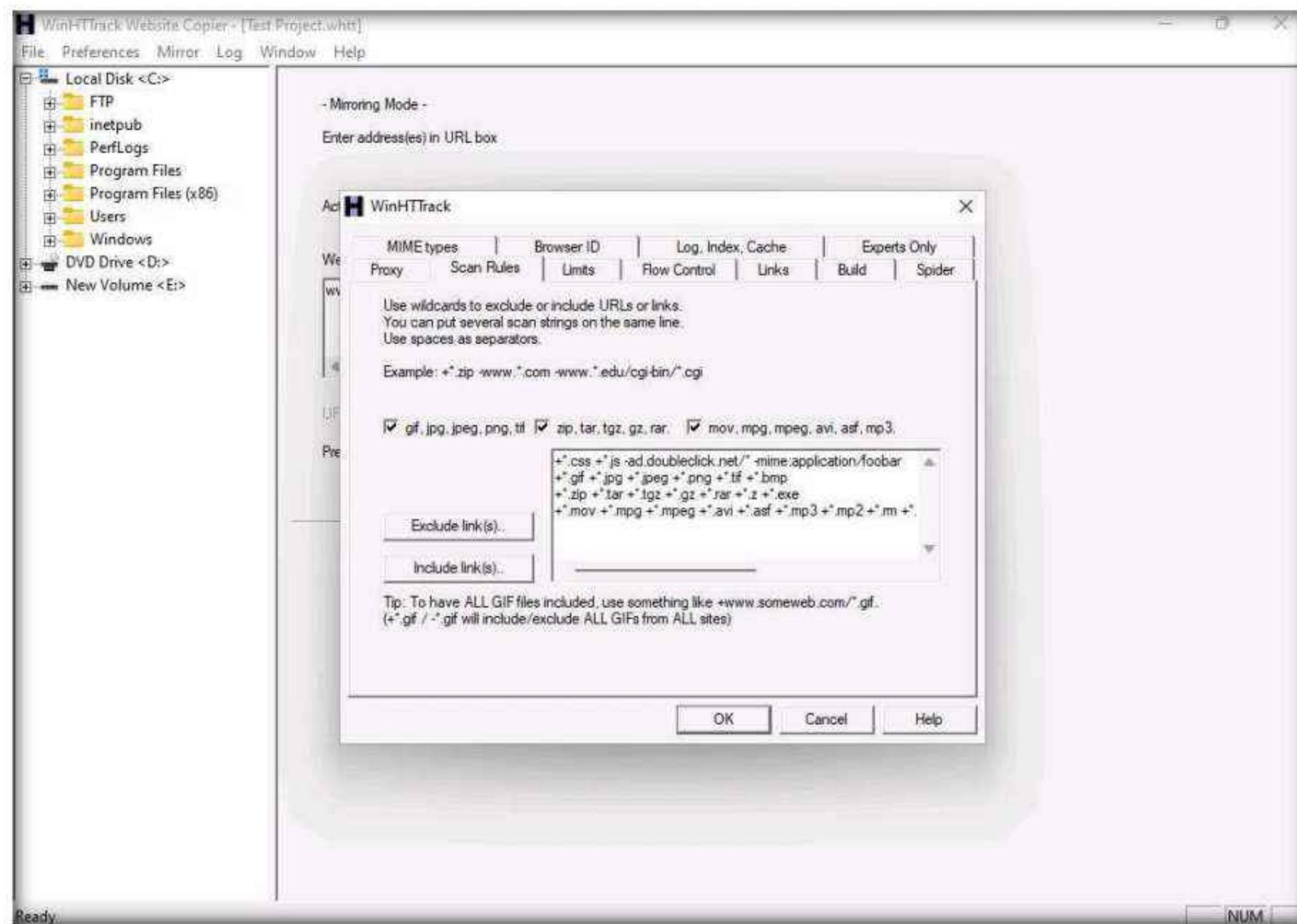


4. Enter a target URL (here, **www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options....**

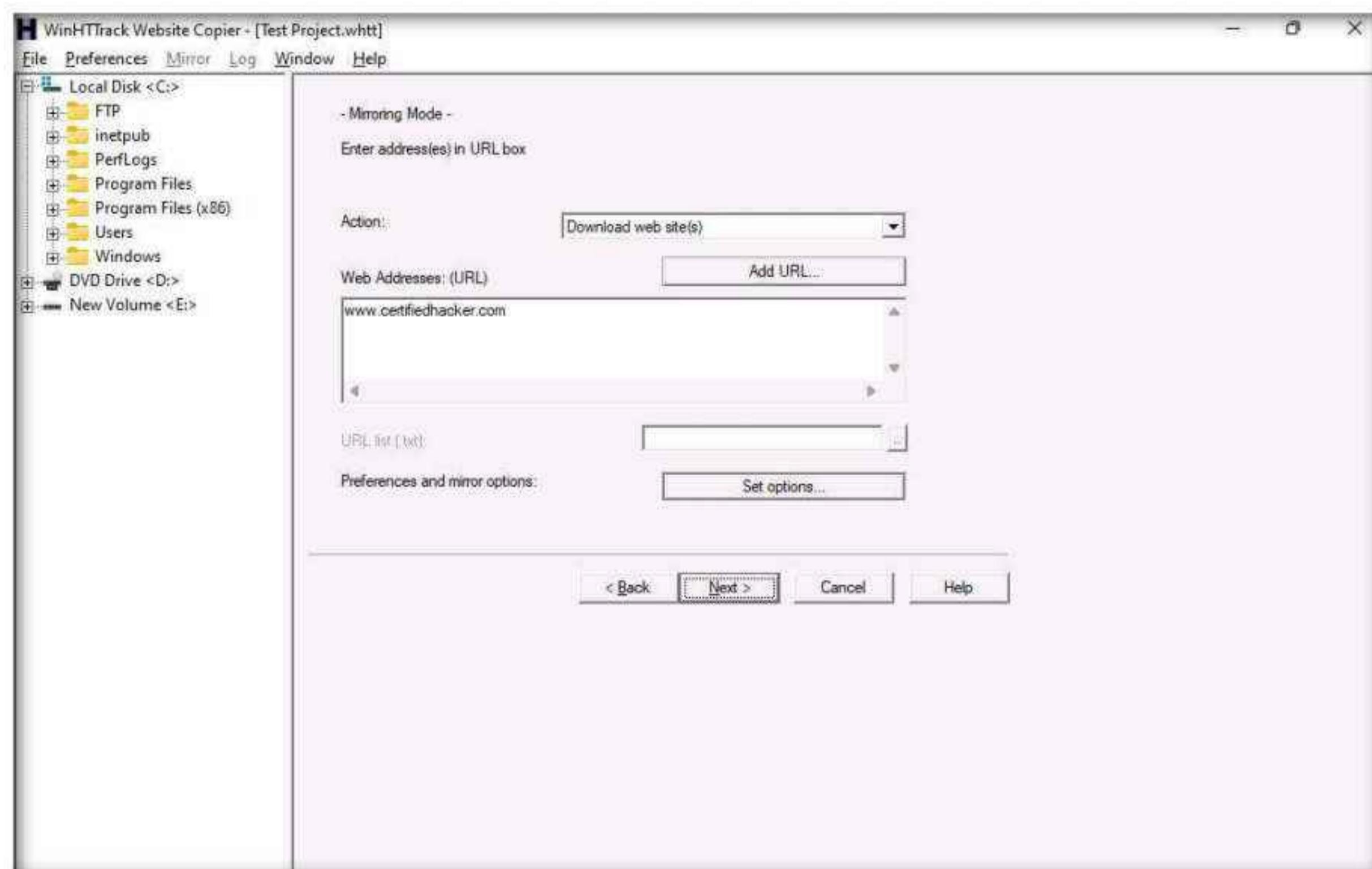


## Module 02 – Footprinting and Reconnaissance

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

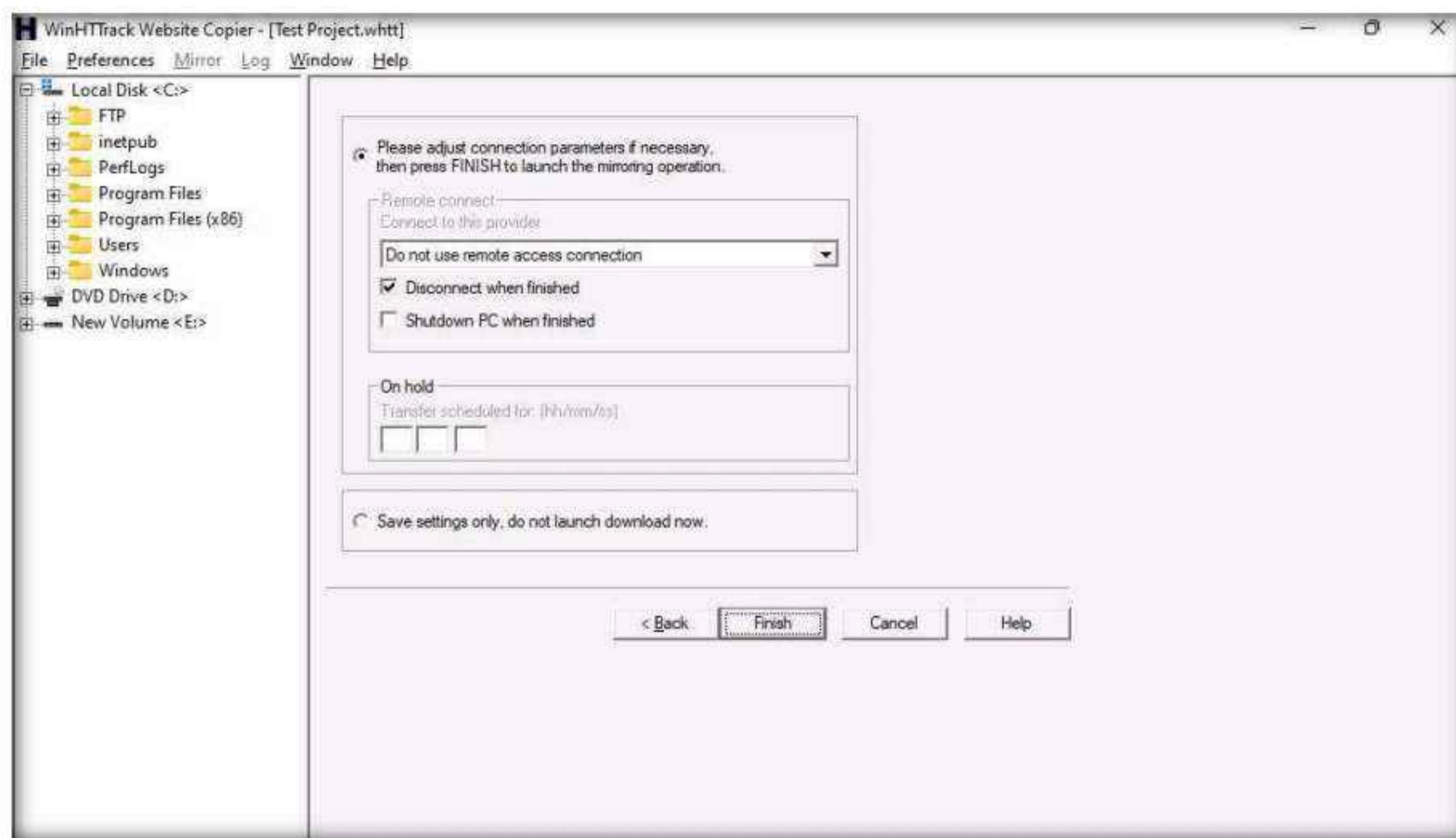


6. Click the **Next >** button.

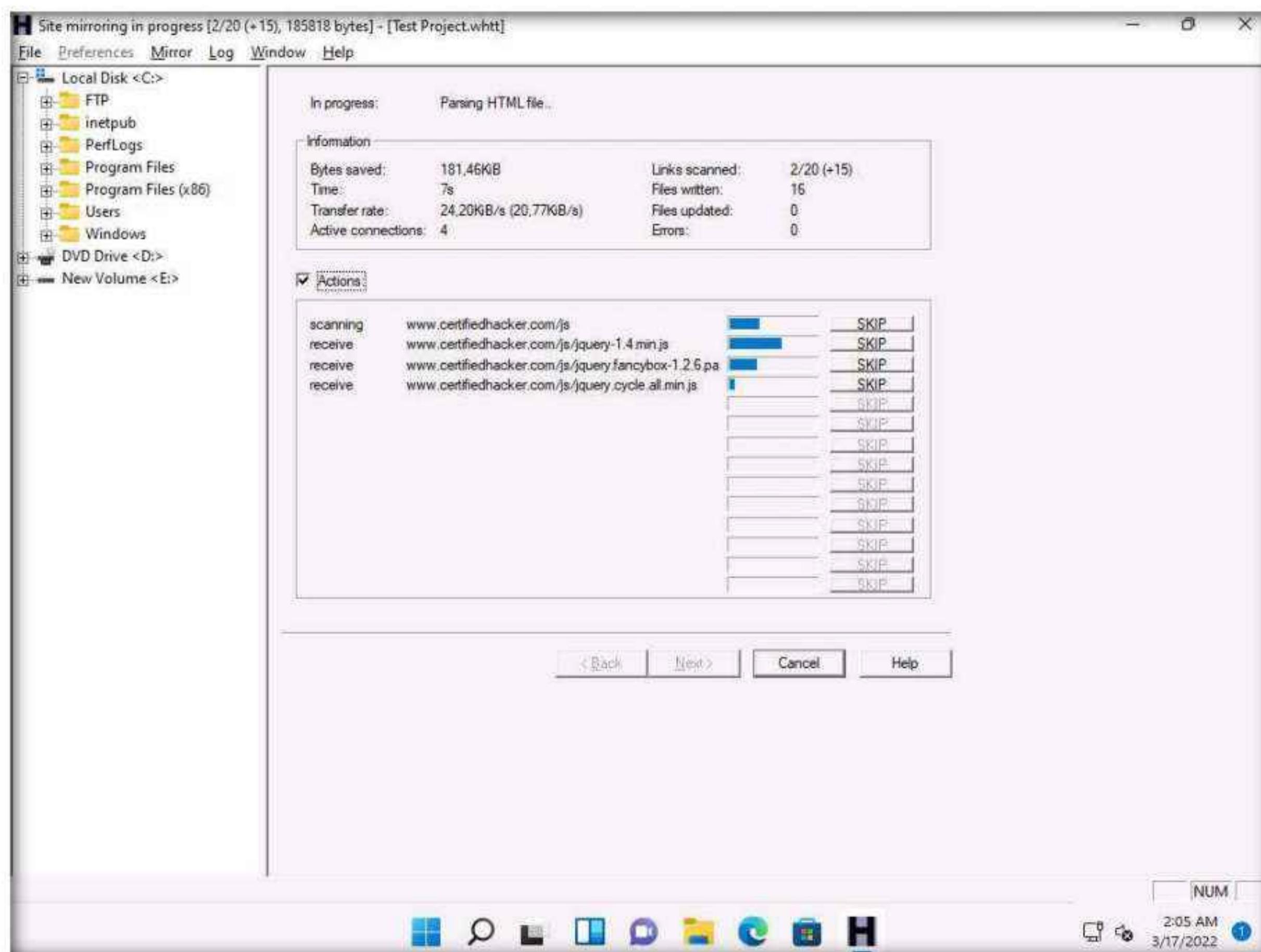


## Module 02 – Footprinting and Reconnaissance

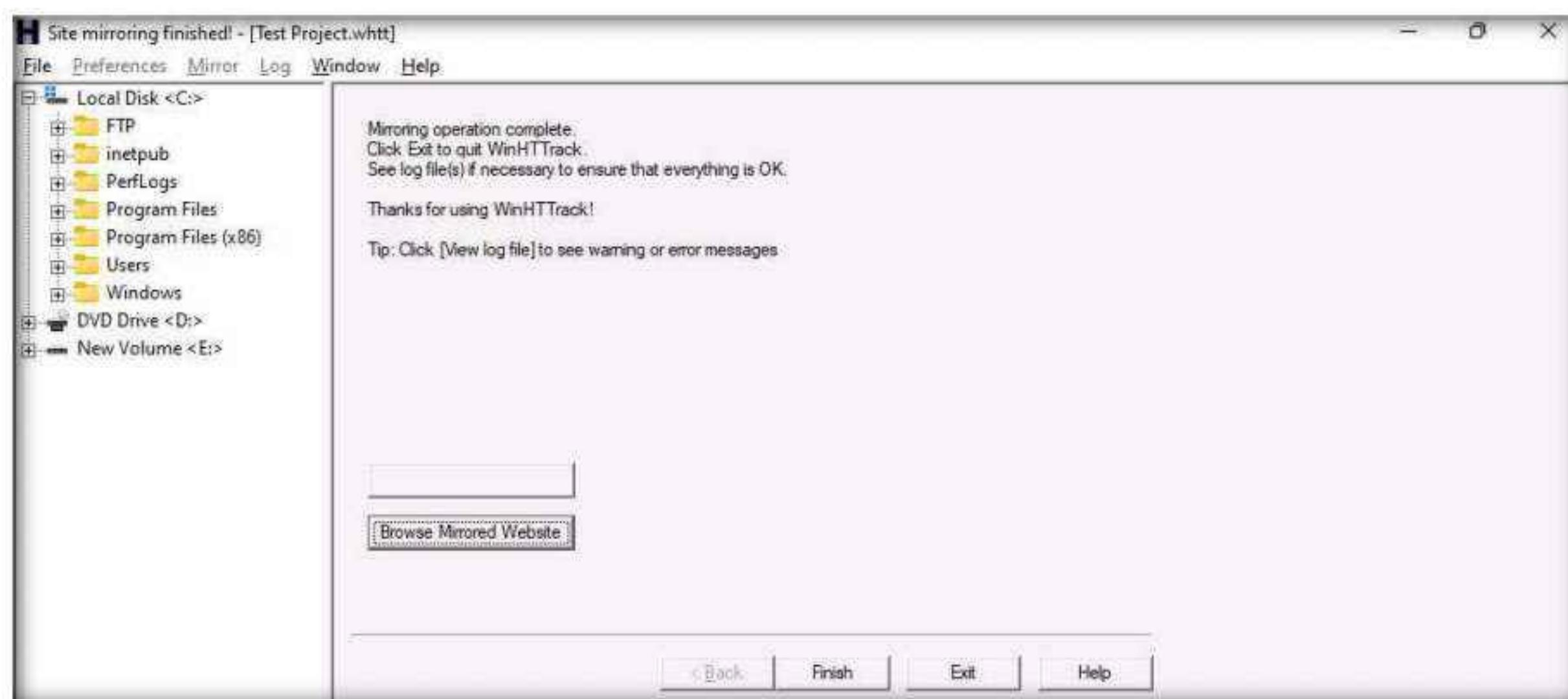
7. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.** Check **Disconnect when finished** and click **Finish** to start mirroring the website.



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

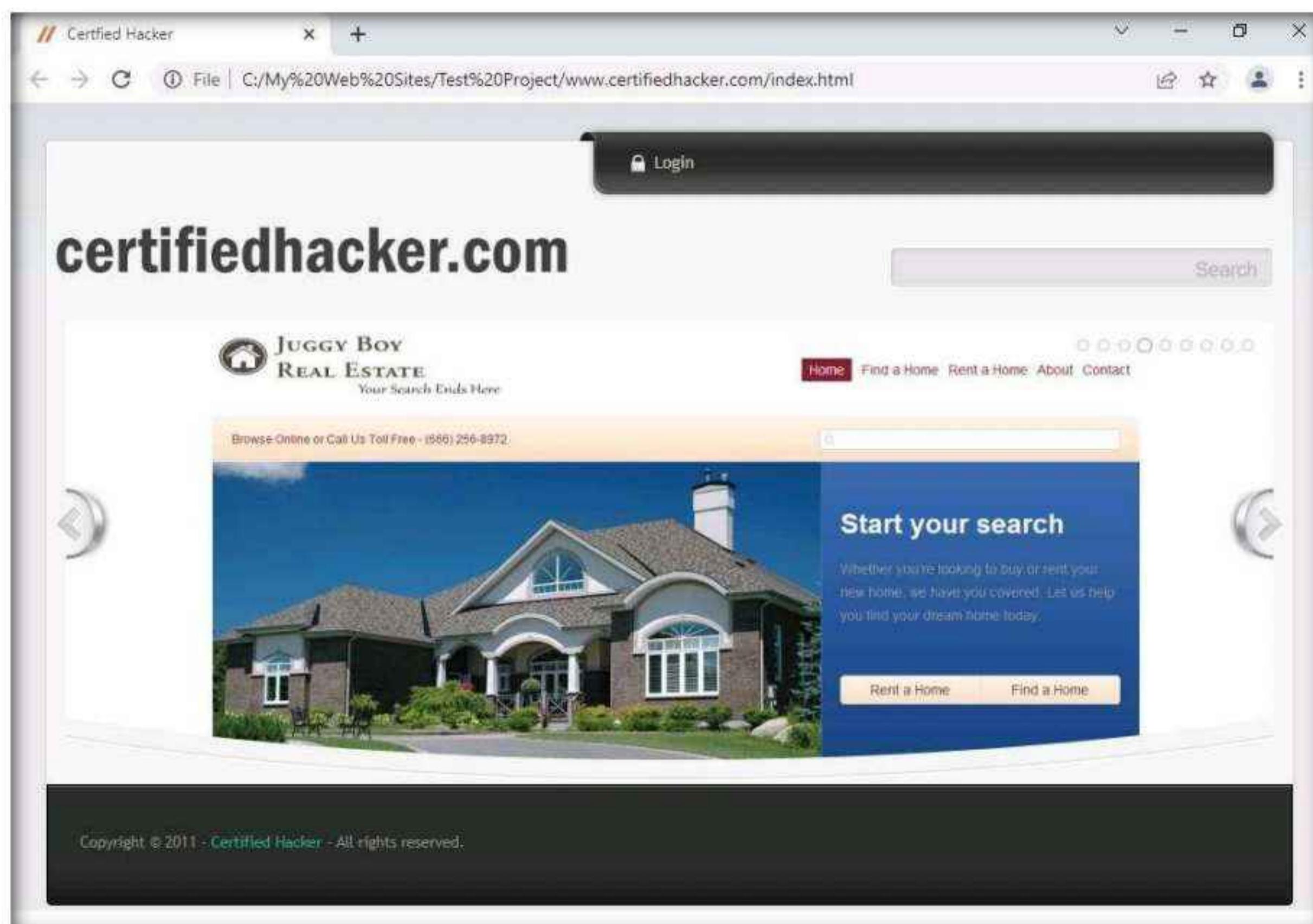


9. Once the site mirroring is completed, WinHTTrack displays the message **Mirroring operation complete**; click on **Browse Mirrored Website**.



10. If the **How do you want to open this file?** pop up appears, select any web browser and click **OK**.

11. 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.

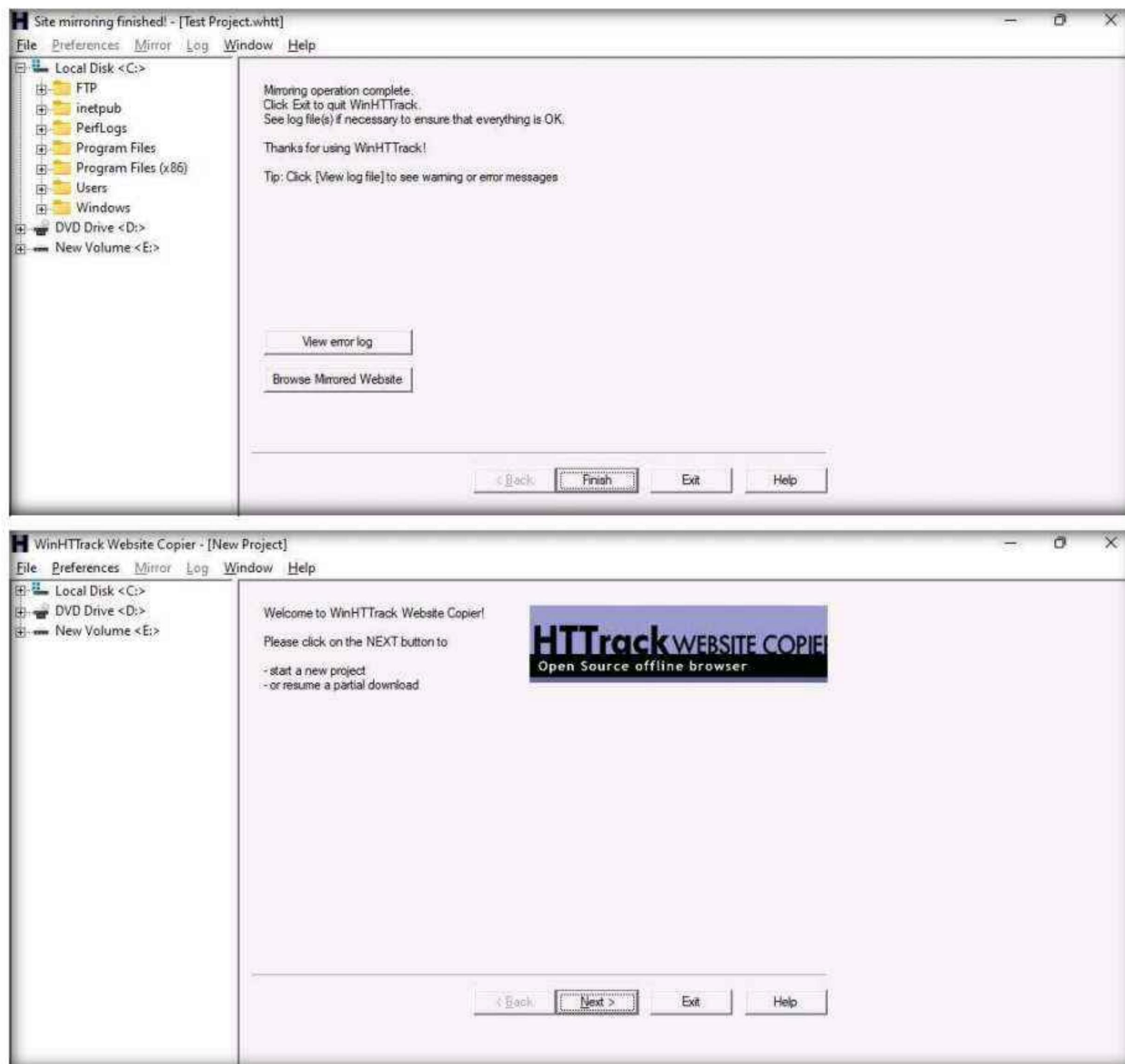


12. Analyze all directories, HTML, images, flash, videos, and other files available on the mirrored target website. You can also check for possible exploits and vulnerabilities. The site will work like a live hosted website.

## Module 02 – Footprinting and Reconnaissance

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

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



- Some websites are very large, and it might take a long time to mirror the complete site.
- The attackers can further use the vulnerabilities identified through **HTTrack Website Copier** to launch various web application attacks on target organization's website.
- This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.
- You can also use other mirroring tools such as **Cyotek WebCopy** (<https://www.cyotek.com>), etc. to mirror a target website.
- Close all open windows and document all the acquired information.
- Turn off the **Windows 11** virtual machine.

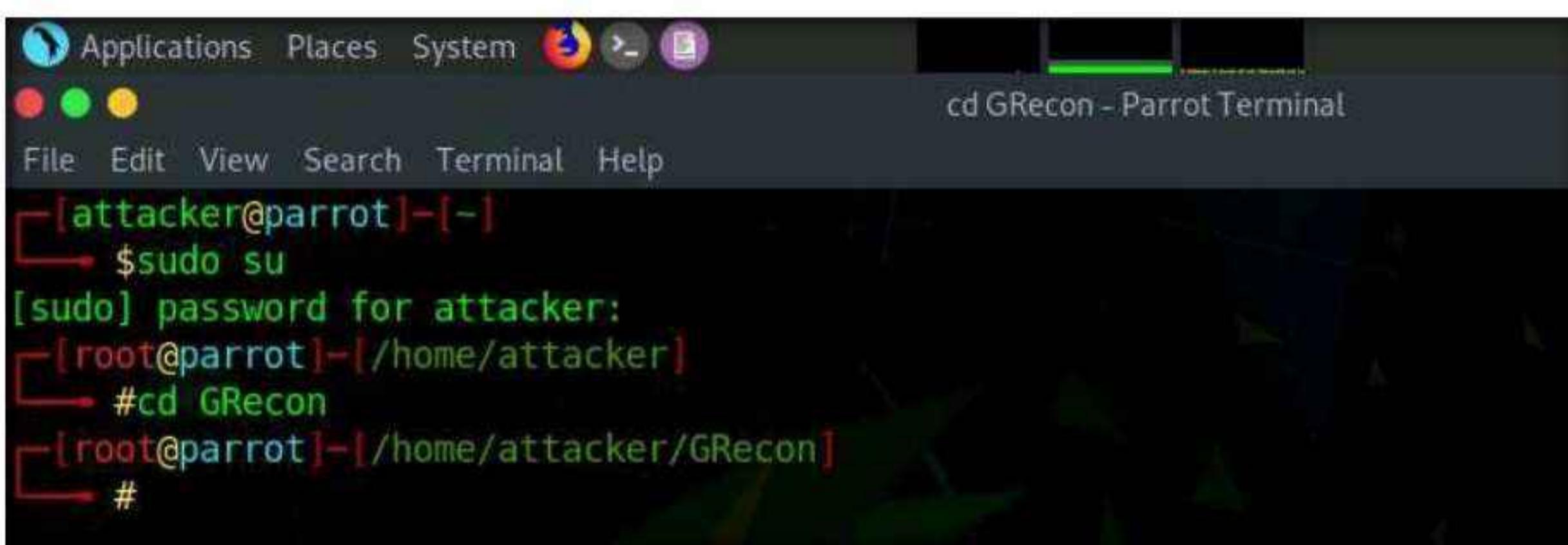
## Task 6: Gather Information About a Target Website using GRecon

GRecon is a Python tool that can be used to run Google search queries to perform reconnaissance on a target to find subdomains, sub-subdomains, login pages, directory listings, exposed documents, and WordPress entries.

1. Turn on the **Parrot Security** virtual machine. 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.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

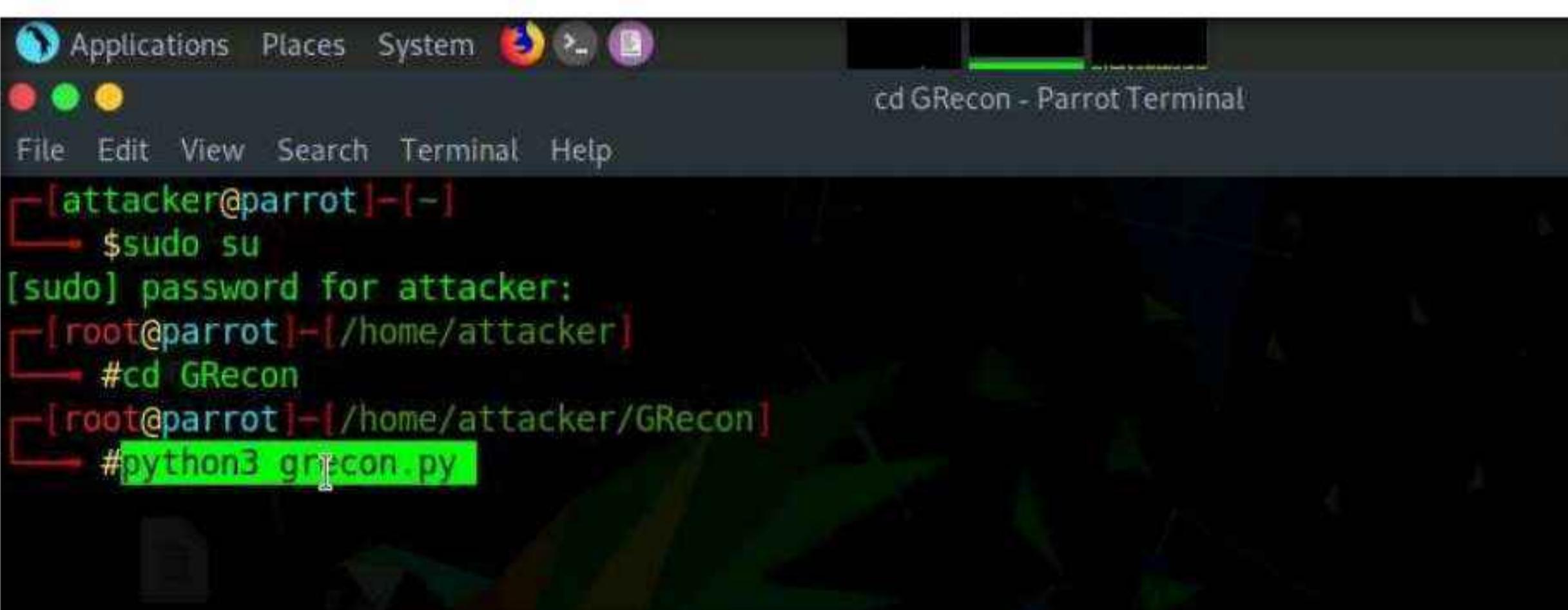
**Note:** The password that you type will not be visible.

5. Now type **cd GRecon** and press **Enter** to navigate to GRecon directory.



```
Applications Places System cd GRecon - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd GRecon
[root@parrot] ~
#
```

6. In the terminal window type **python3 grecon.py** and press **Enter**.



```
Applications Places System cd GRecon - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd GRecon
[root@parrot] ~
# python3 grecon.py
```

7. GRecon initializes, in the Set Target (site.com): field type **certifiedhacker.com** and press Enter.

The screenshot shows a terminal window titled "python3 grecon.py - Parrot Terminal". The terminal session starts with the user navigating to their home directory, becoming root, and running the GRecon tool. It then performs a check for updates and displays the current micro-plugins available. Finally, it prompts the user to set a target site.

```
[attacker@parrot]~[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd GRecon
[root@parrot]~[/home/attacker/GRecon]
#python3 grecon.py

Cheking Update...
Update Status...[NO UPDATE]
GRecon V1.0
Resuming...

Current Micro Plugins :

[>] Subdomains...[UP]
[>] Sub-Subdomains...[UP]
[>] Signup/Login pages...[UP]
[>] Dir Listing...[UP]
[>] Exposed Docs...[UP]
[>] WordPress Entries...[UP]
[>] Pasting Sites...[UP]

/ \ ) 
\ )| \(-(-_-) | - ) V1.0
GRecon by @TebbaaX (Adnane)

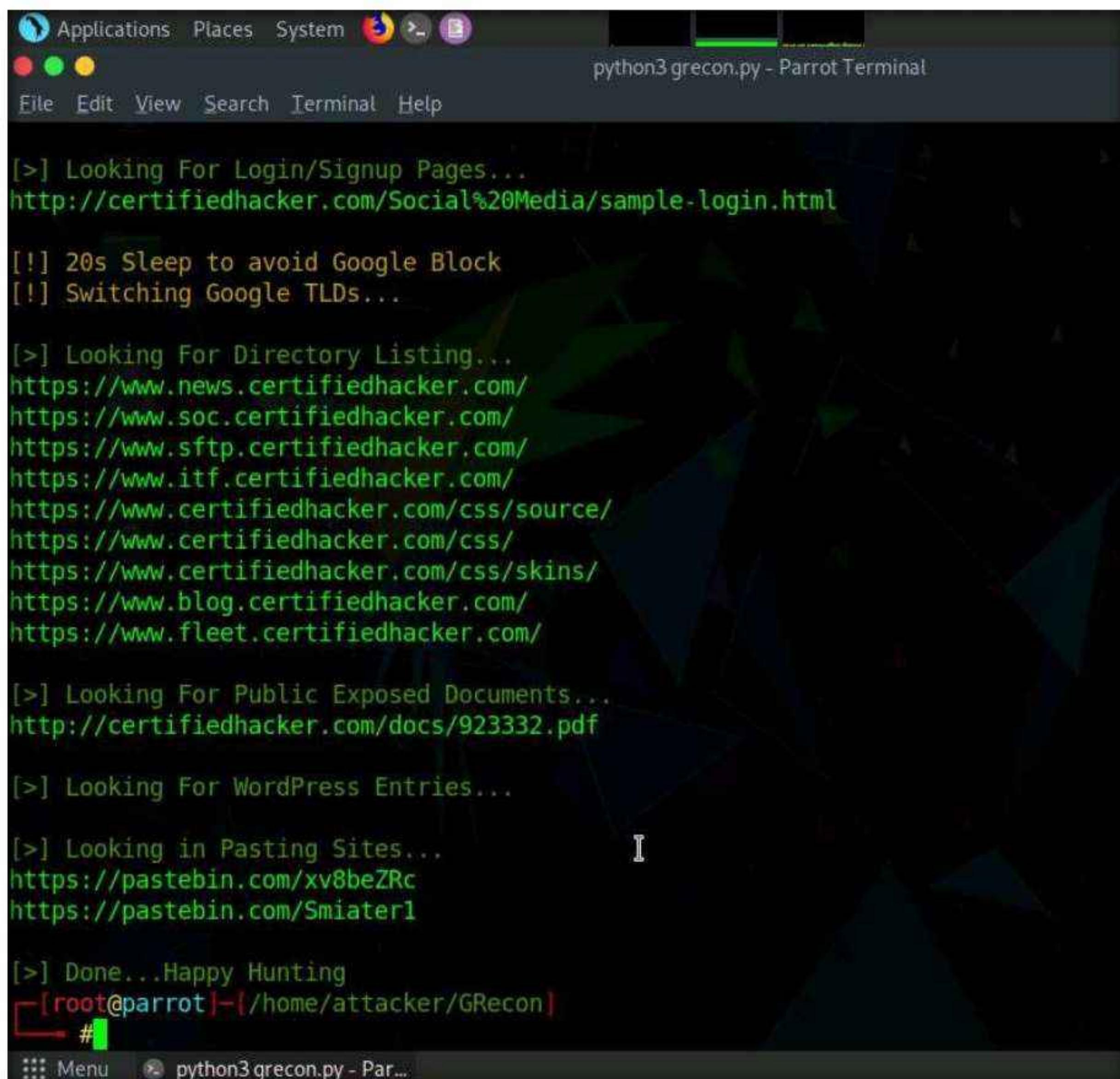
[+] Set Target (site.com) : certifiedhacker.com
```

8. **GRecon** searches for available subdomains, sub-subdomains, login pages, directory listings, exposed documents, WordPress entries and pasting sites and displays the results.

**Note:** It will take approximately 5 minutes to complete the search.

The screenshot shows a terminal window titled "python3 grecon.py - Parrot Terminal". The window contains the output of the GRecon tool. The output includes:

- Tool version information: "/ \ )\ V1.0 GRecon by @TebbaaX (Adnane)
- [+] Set Target (site.com) : certifiedhacker.com
- [>] Looking For Subdomains...  
http://certifiedhacker.com/  
https://www.certifiedhacker.com/  
https://www.news.certifiedhacker.com/  
https://www.fleet.certifiedhacker.com/  
https://www.itf.certifiedhacker.com/  
https://www.blog.certifiedhacker.com/  
https://www.soc.certifiedhacker.com/  
https://www.sftp.certifiedhacker.com/
- [>] Looking For Sub-Subdomains...
- [>] Looking For Login/Signup Pages...  
http://certifiedhacker.com/Social%20Media/sample-login.html
- [!] 20s Sleep to avoid Google Block
- [!] Switching Google TLDs...
- [>] Looking For Directory Listing...  
https://www.news.certifiedhacker.com/  
https://www.soc.certifiedhacker.com/  
https://www.sftp.certifiedhacker.com/  
https://www.itf.certifiedhacker.com/  
https://www.certifiedhacker.com/css/source/



The screenshot shows a terminal window titled "python3 grecon.py - Parrot Terminal". The window displays the output of the GRecon.py script, which is performing a footprinting scan on the target website "http://certifiedhacker.com". The output includes messages about looking for login/signup pages, directory listings, public documents, and WordPress entries, along with URLs found during the scan.

```
[>] Looking For Login/Signup Pages...
http://certifiedhacker.com/Social%20Media/sample-login.html

[!] 20s Sleep to avoid Google Block
[!] Switching Google TLDs...

[>] Looking For Directory Listing...
https://www.news.certifiedhacker.com/
https://www.soc.certifiedhacker.com/
https://www.sftp.certifiedhacker.com/
https://www.itf.certifiedhacker.com/
https://www.certifiedhacker.com/css/source/
https://www.certifiedhacker.com/css/
https://www.certifiedhacker.com/css/skins/
https://www.blog.certifiedhacker.com/
https://www.fleet.certifiedhacker.com/

[>] Looking For Public Exposed Documents...
http://certifiedhacker.com/docs/923332.pdf

[>] Looking For WordPress Entries...

[>] Looking in Pasting Sites...
https://pastebin.com/xv8beZRc
https://pastebin.com/Smiater1

[>] Done...Happy Hunting
[root@parrot]-(~/home/attacker/GRecon]
#
```

9. Attackers can further use the gathered information to perform various web application attacks on the target website.
10. This concludes the demonstration of gathering information about a target website using GRecon.
11. Close all open windows and document all the acquired information.

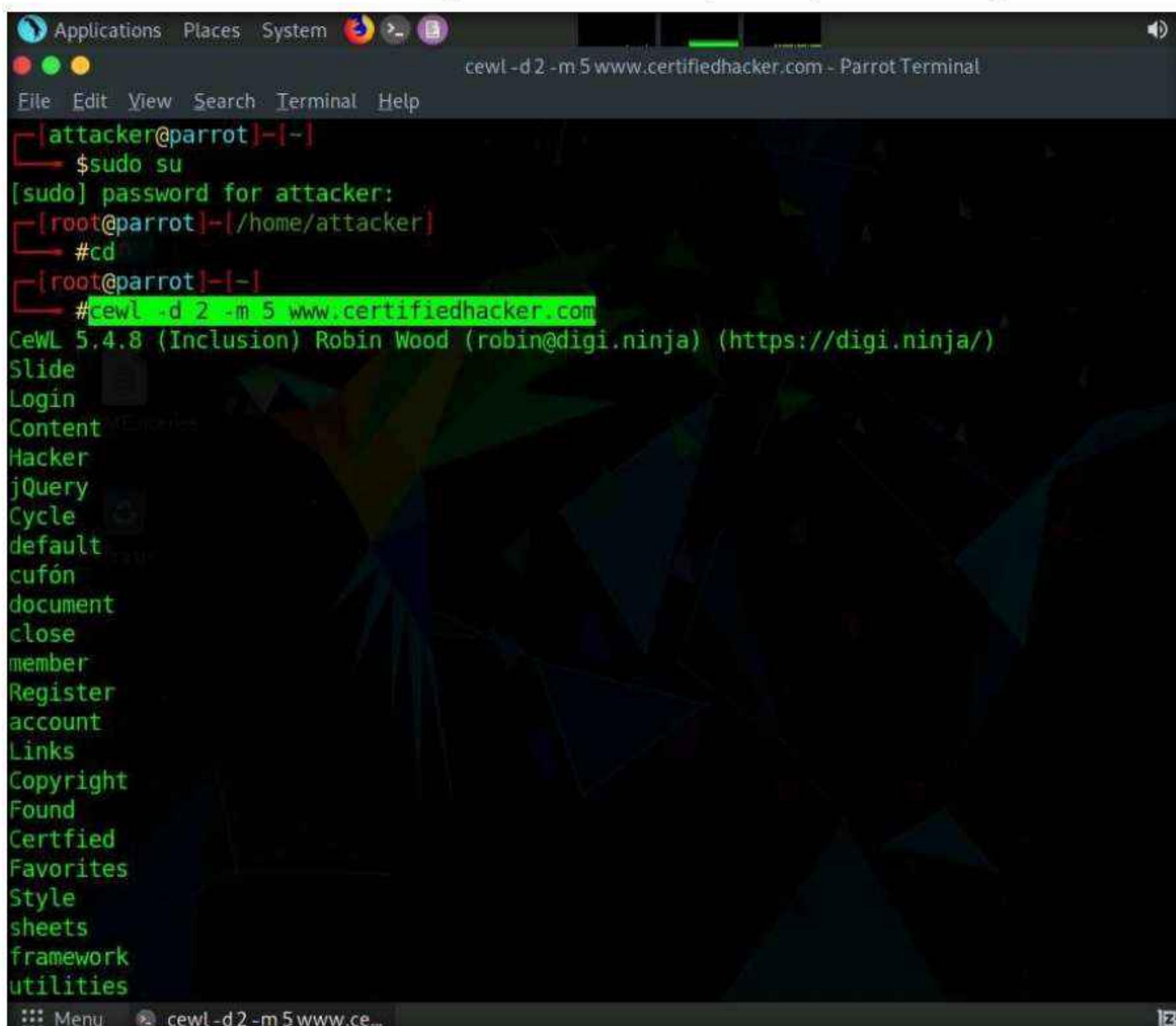
## Task 7: Gather a Wordlist from the Target Website using CeWL

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.

**Note:** Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. In the **Parrot Security** virtual machine, Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **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.
5. In the 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**).
6. 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.



The screenshot shows a terminal window titled "cewl -d 2 -m 5 www.certifiedhacker.com - Parrot Terminal". The terminal output displays a wordlist generated by the CeWL tool. The wordlist includes various words such as "Applications", "Places", "System", "File", "Edit", "View", "Search", "Terminal", "Help", "attacker", "parrot", "root", "home", "attacker", "cd", "certifiedhacker", "com", "CeWL", "5.4.8", "Inclusion", "Robin", "Wood", "robin@digi.ninja", "https://digi.ninja/", "Slide", "Login", "Content", "Hacker", "jQuery", "Cycle", "default", "cufón", "document", "close", "member", "Register", "account", "Links", "Copyright", "Found", "Certified", "Favorites", "Style", "sheets", "framework", "utilities". The terminal window has a dark background with light-colored text. The title bar and menu bar are visible at the top.

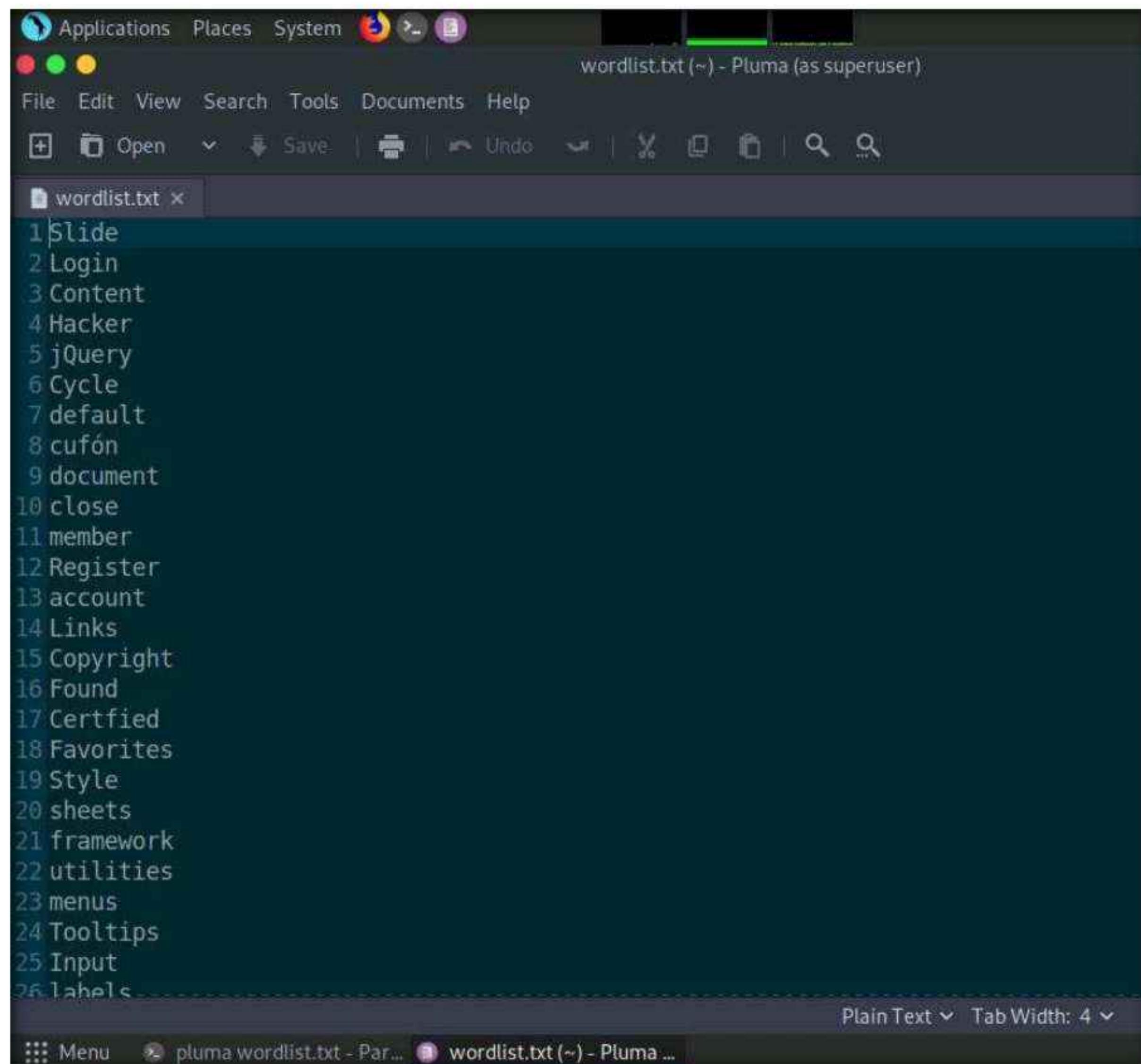
7. Alternatively, this unique wordlist can be written directly to a text file. To do so, type **cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com** and press **Enter**.

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

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

The screenshot shows a terminal window titled "cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com - Parrot Terminal". The terminal displays a large list of words extracted from the website, including "Column", "Certified", "rights", "reserved", "legal", "Activate", "Replacement", "brief", "description", "website", "business", "keywords", "phrases", "associated", "requested", "found", "server", "Additionally", "error", "encountered", "while", "trying", "ErrorDocument", "handle", and "request". Below this, the command "#cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com" is shown along with the CeWL version information: "CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)" and the command "#pluma wordlist.txt". The terminal is running on a Parrot OS desktop environment, as indicated by the window title and the desktop icons visible at the top.

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



A screenshot of a Linux desktop environment showing a terminal window titled "wordlist.txt (~) - Pluma (as superuser)". The window contains a list of words, each preceded by a number from 1 to 26. The words are:

```
1 $lide
2 Login
3 Content
4 Hacker
5 jQuery
6 Cycle
7 default
8 cufón
9 document
10 close
11 member
12 Register
13 account
14 Links
15 Copyright
16 Found
17 Certfied
18 Favorites
19 Style
20 sheets
21 framework
22 utilities
23 menus
24 Tooltips
25 Input
26 lables
```

The terminal window has a dark theme and includes standard Linux window controls (red, green, yellow buttons) and a title bar with the application name and file path. The bottom of the window shows the status bar with "Plain Text" and "Tab Width: 4".

10. Type **cewl --help** and press Enter in the parrot terminal to view the list of options that cewl provides.

```
cewl --help - Parrot Terminal
[...]-[root@parrot]-[~]
# cewl --help
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Usage: cewl [OPTIONS] ... <url>

OPTIONS:
-h, --help: Show help.
-k, --keep: Keep the downloaded file.
-d <x>,--depth <x>: Depth to spider to, default 2.
-m, --min_word_length: Minimum word length, default 3.
-o, --offsite: Let the spider visit other sites.
--exclude: A file containing a list of paths to exclude
--allowed: A regex pattern that path must match to be followed
-w, --write: Write the output to the file.
-u, --ua <agent>: User agent to send.
-n, --no-words: Don't output the wordlist.
--lowercase: Lowercase all parsed words
--with-numbers: Accept words with numbers in as well as just letters
--convert-umlauts: Convert common ISO-8859-1 (Latin-1) umlauts (ä-ae, ö-oe, ü-ue, ß-ss)
-a, --meta: include meta data.
--meta_file file: Output file for meta data.
-e, --email: Include email addresses.
--email_file <file>: Output file for email addresses.
--meta-temp-dir <dir>: The temporary directory used by exiftool when parsing files, default /tmp.
-c, --count: Show the count for each word found.
-v, --verbose: Verbose.
--debug: Extra debug information.

Authentication
```

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

## Lab Analysis

Analyze and document the results of this lab exercise.

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

### Internet Connection Required

Yes

No

### Platform Supported

Classroom

CyberQ

Lab

5

## Perform Email Footprinting

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

### Lab Scenario

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

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

### 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**

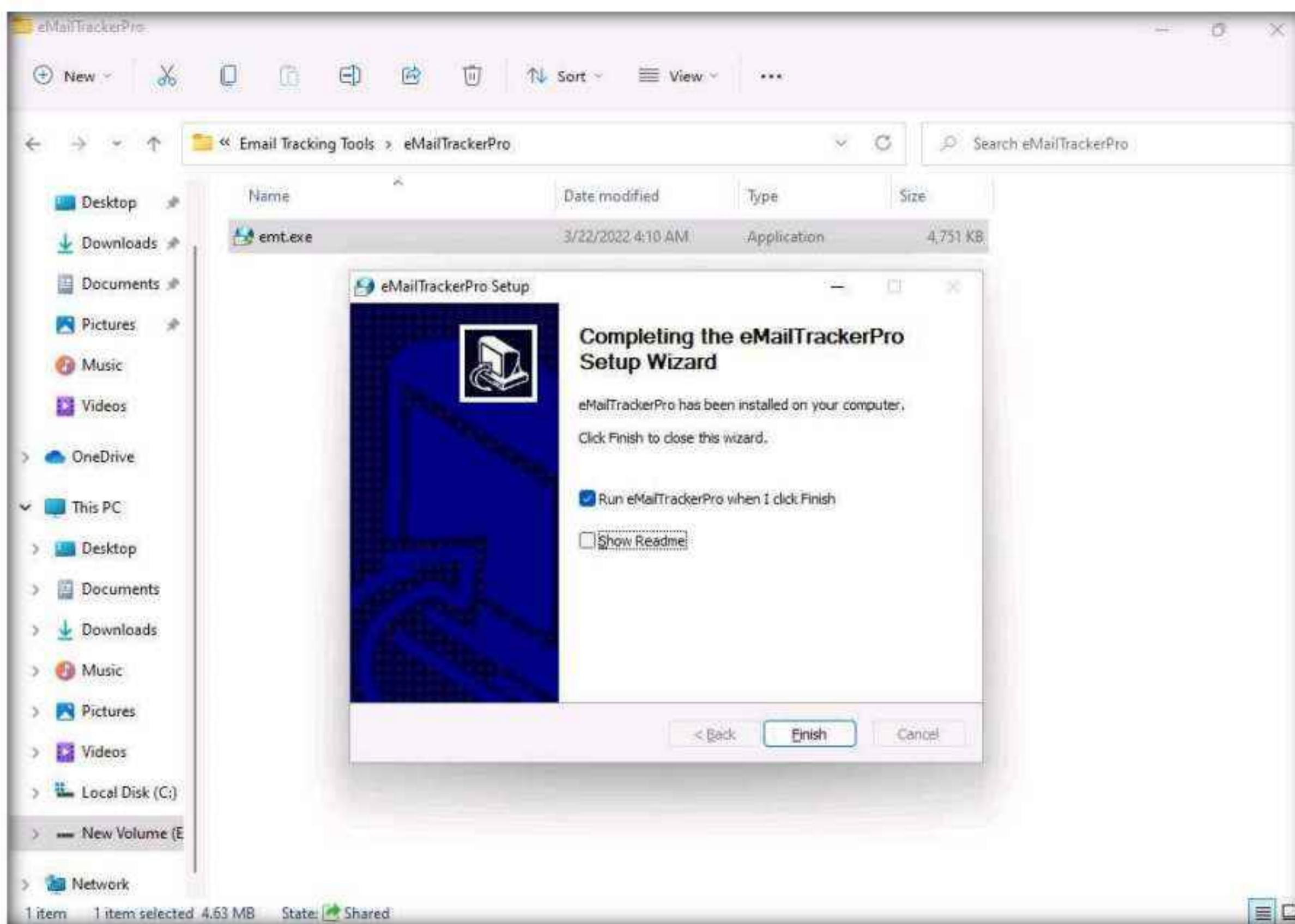
---

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.

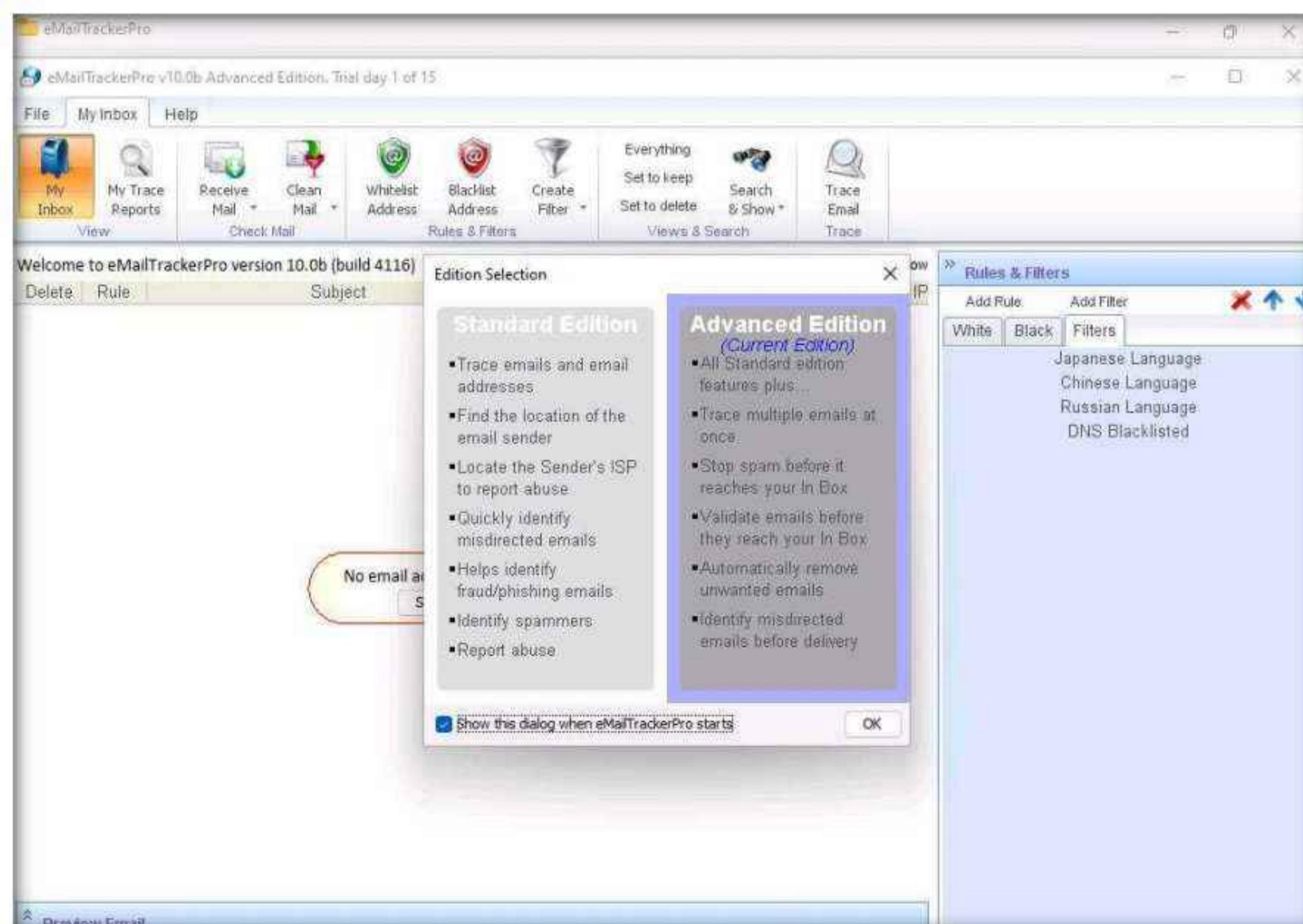
Here, we will gather information by analyzing the email header using eMailTrackerPro.

1. Turn on the **Windows 11** virtual machine. Login with Username: **Admin** and Password: **Pa\$\$w0rd**. Navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance>Email Tracking Tools\EmailTrackerPro** and double-click **emt.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.
4. 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.

## Module 02 – Footprinting and Reconnaissance

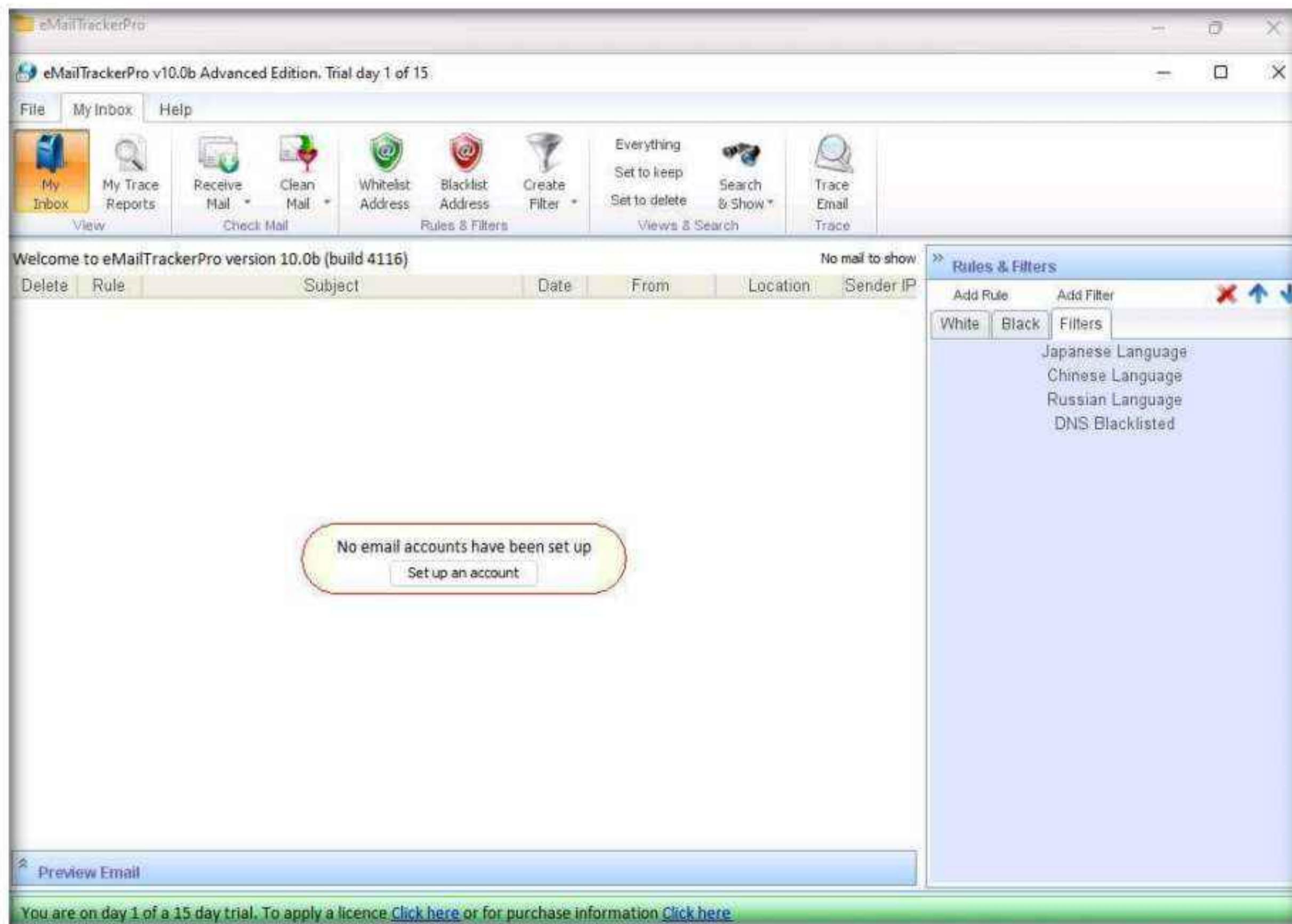


5. The main window of eMailTrackerPro appears along with the Edition Selection pop-up; click OK.

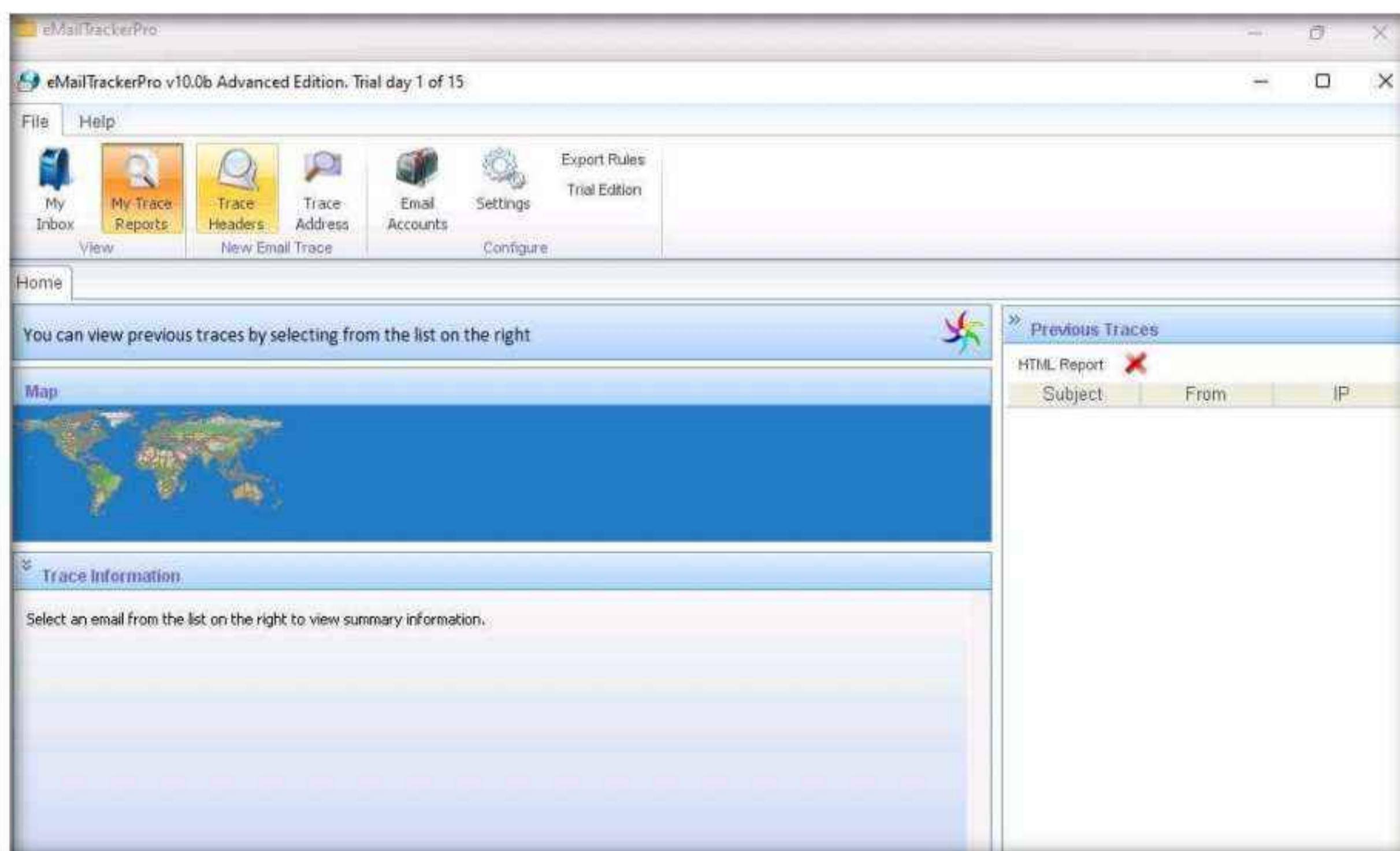


## Module 02 – Footprinting and Reconnaissance

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

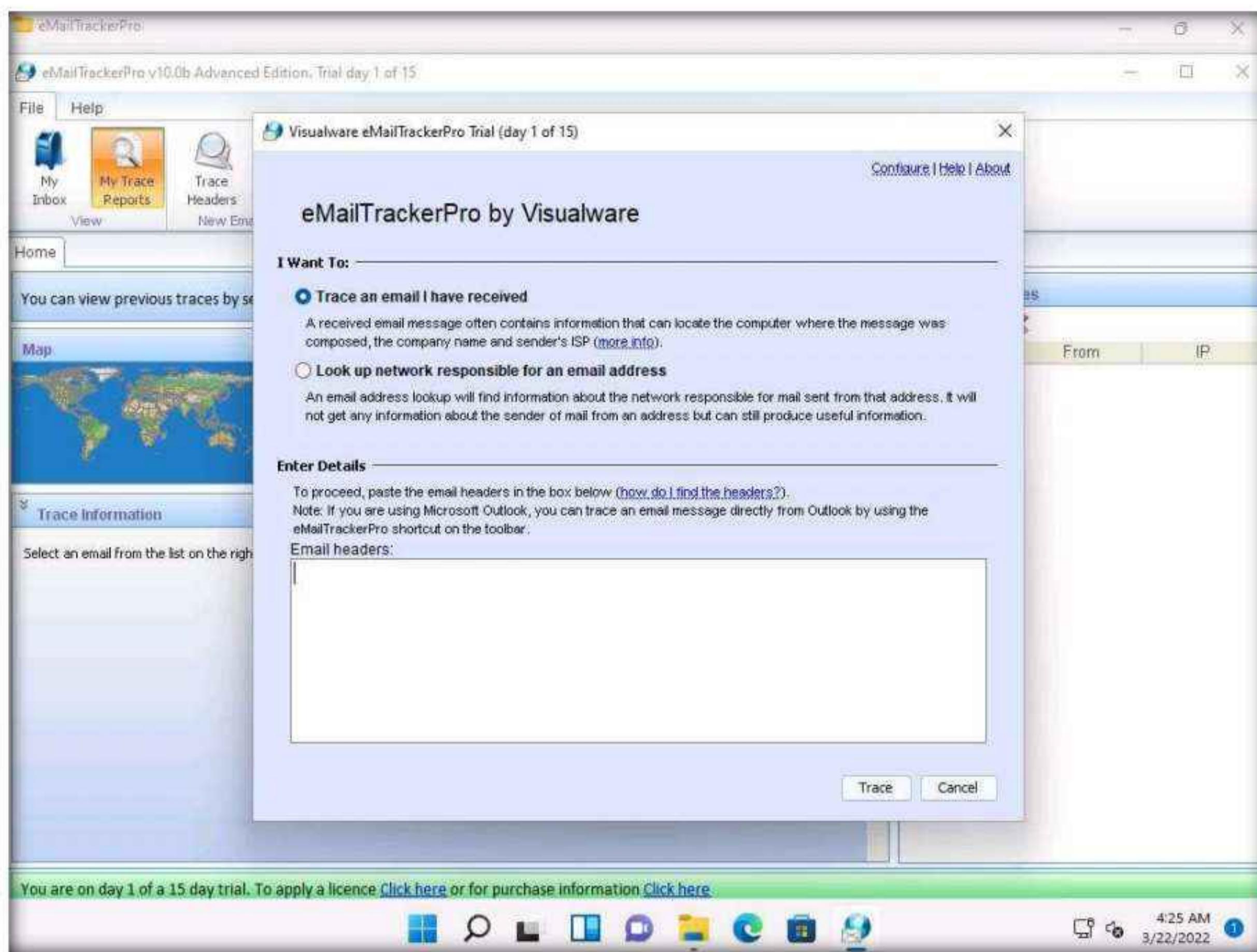


7. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header).  
8. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.



## Module 02 – Footprinting and Reconnaissance

9. 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.

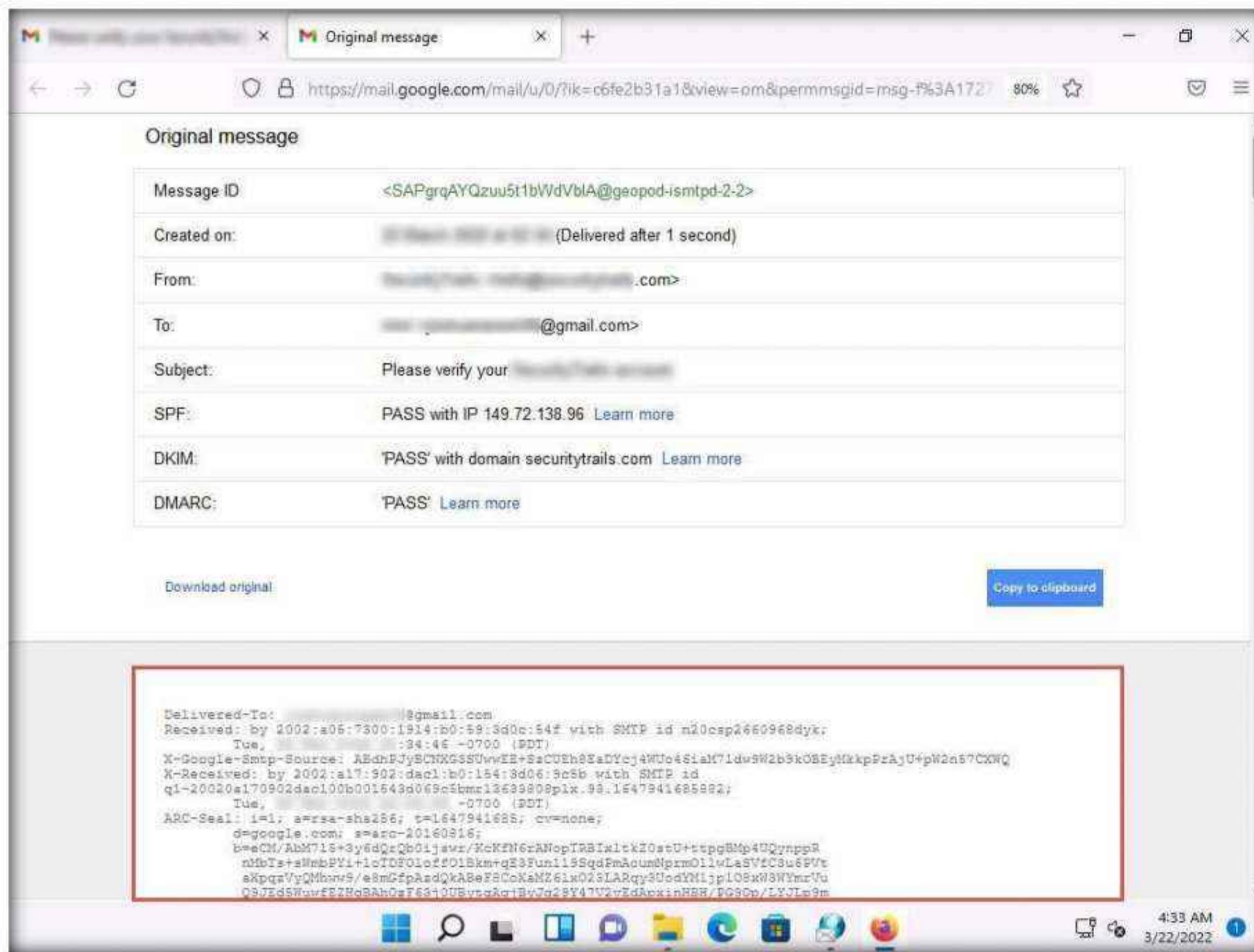


## Module 02 – Footprinting and Reconnaissance

10. 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.

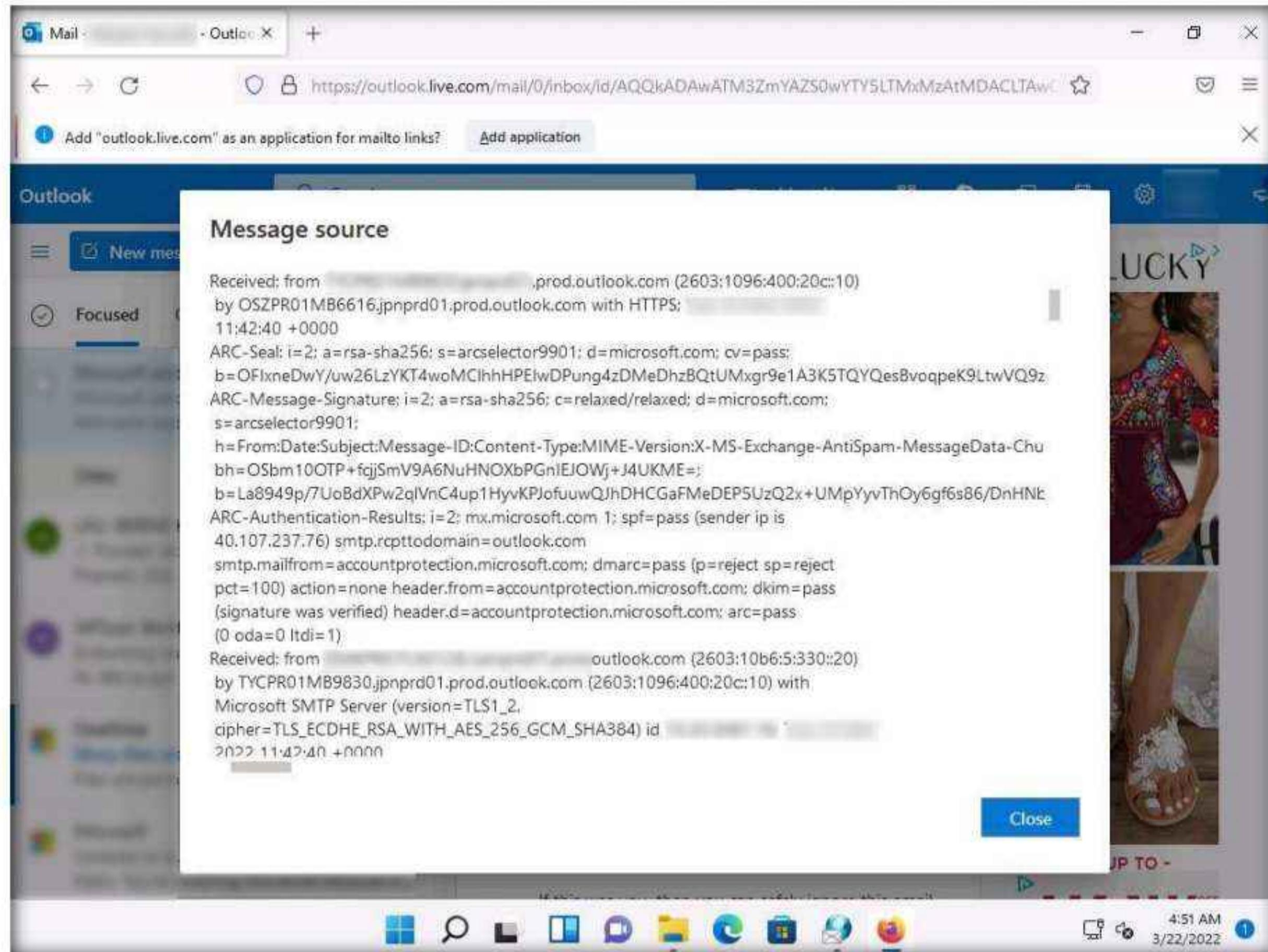
**Note:** In Gmail, find the email header by following the steps:

- 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



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

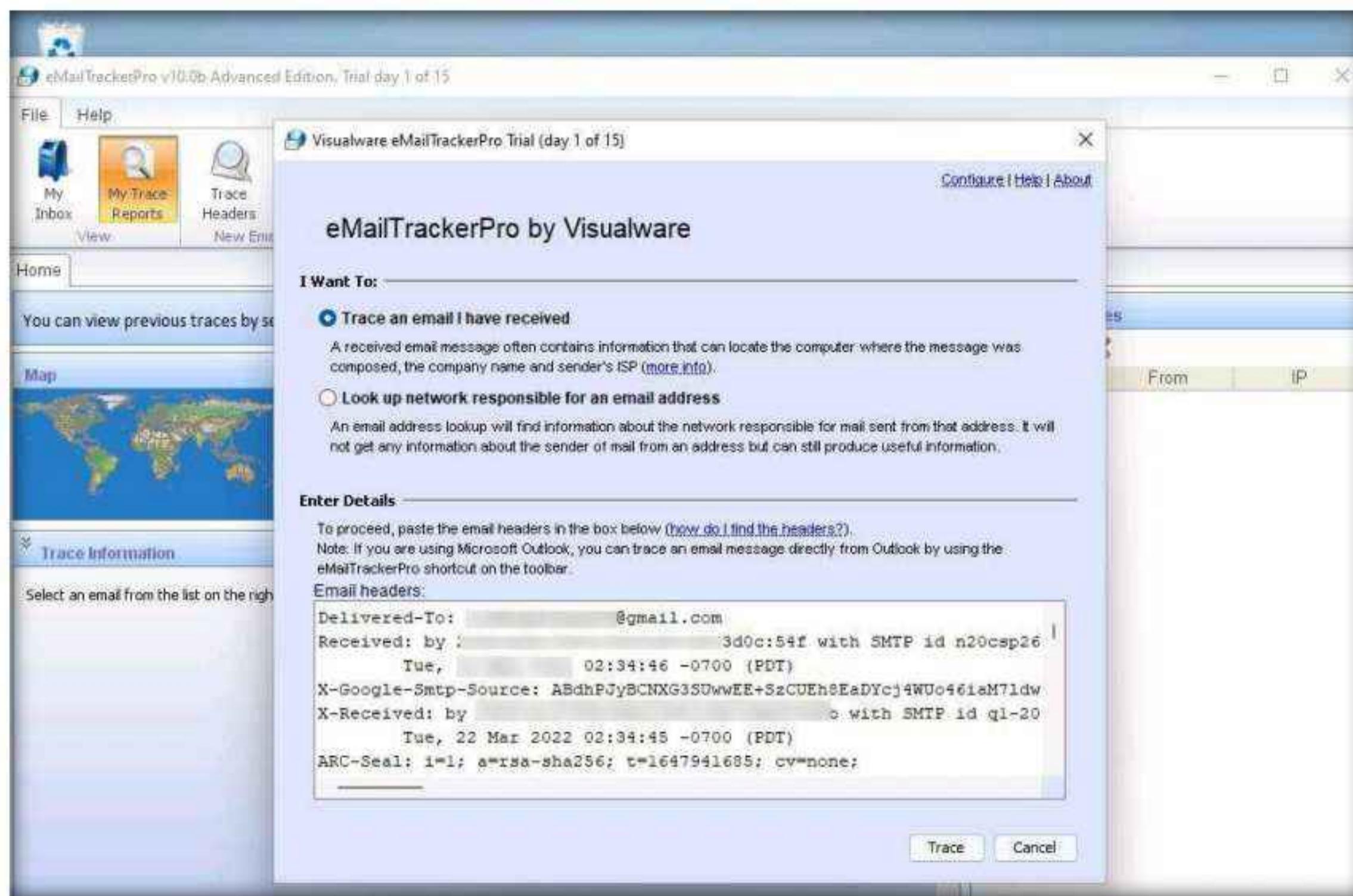
- Double-click the email to open it in a new window
- Click the ... (**More actions**) icon present at the right of the message-pane to open message options
- From the options, click **View**
- The **view message source** window appears with all the details about the email, including the email header



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

**Note:** Here, we are analyzing the email header from Gmail account. However, you can also analyze the email header from outlook account.

## Module 02 – Footprinting and Reconnaissance



12. The **My Trace Reports** window opens.

13. 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.

#	Hop IP	Hop Name	Location
1	10		
2	172		
3	192		
4	103		(Europe)
5	38		(America)
6	154	te0-3-0-5_rcr21.tpa01.atlas.cogent	Tampa, FL, USA
7	154	be2320_ccr22_mia01.atlas.cogent	Miami, FL, USA
8	154	be2027_ccr22_mia03.atlas.cogent	Miami, FL, USA
9	154	level3.mia03.atlas.cogentco.com	Miami, FL, USA

## Module 02 – Footprinting and Reconnaissance

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

The screenshot shows the eMailTrackerPro interface. At the top, there's a menu bar with File, Help, and various icons like My Inbox, My Trace Reports (which is selected), Trace Headers, Trace Address, Email Accounts, Settings, Export Rules, Trial Edition, and Configure. Below the menu is a toolbar with Home, Subject: Please verify..., New Trace, and View Report buttons. The main area has a title bar "The trace is complete, the information found is displayed on the right". On the left is a world map with a red line and a callout bubble pointing to "America". On the right is a panel titled "Email Summary" containing recipient and header analysis. Below the map is a table titled "Table" with columns "Hop IP", "Hop Name", and "Location". The table lists several hops, with some names like "Europe" and "America" appearing in parentheses. A green banner at the bottom says "You are on day 1 of a 15 day trial. To apply a licence Click here or for purchase information Click here".

15. 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**.

16. Expand each section to view detailed information.

The screenshot shows a web browser window titled "eMailTrackerPro Report" with the URL "file:///C:/Users/Admin/eMailTrackerPro/V8/reports/report-20220322-0500-0.html". The page has a blue header with the eMailTrackerPro logo and navigation links. Below it is a yellow box titled "Identification Report for 'Please verify your SecurityTrails account'". It contains a message about the trial period and a note that Computer 149 has been found. The "Network Contact Information" section shows icons for a person, envelope, phone, and location, with "US" indicated. There's a link to "Click here to hide the in-depth information on this email (more info)". Below this are three bullet points: "The sender's IP was - 149", "A time stamp claimed to be added by a server along the emails route is not valid. This is a mistake by the spammer that means a header in this email is fake.", and "The sender of this email appeared to have the address [redacted].com. This information is easily faked so should not be treated as conclusive."

17. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
18. 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. Close all open windows and document all the acquired information.
20. Turn off the **Windows 11** virtual machine.

## **Lab Analysis**

Analyze and document the results of this lab exercise.

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

---

<b>Internet Connection Required</b>	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Platform Supported</b>	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> CyberQ

Lab

6

## Perform Whois Footprinting

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

### 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 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

### Lab Duration

Time: 5 Minutes

### Overview of Whois Footprinting

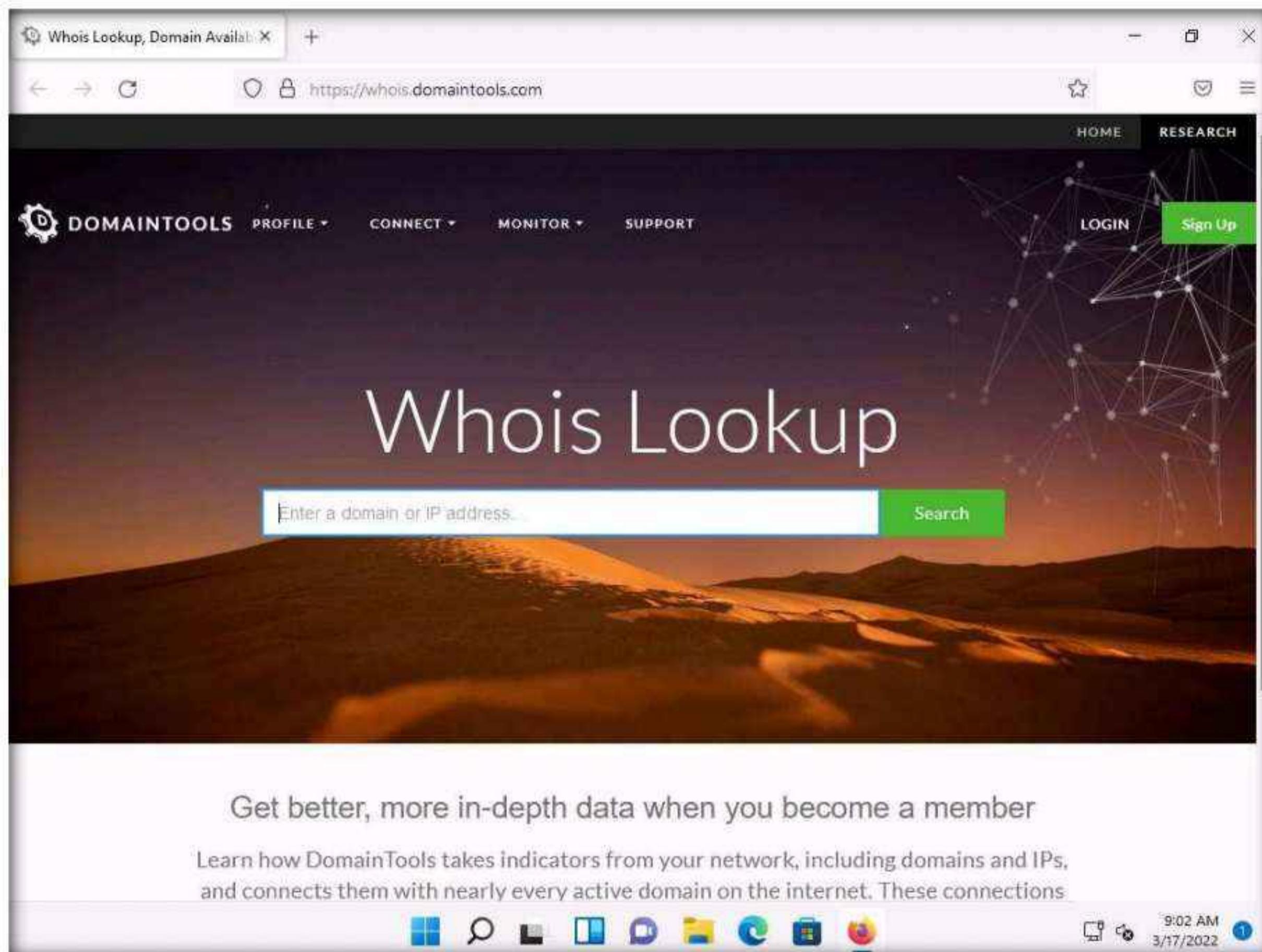
This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens 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

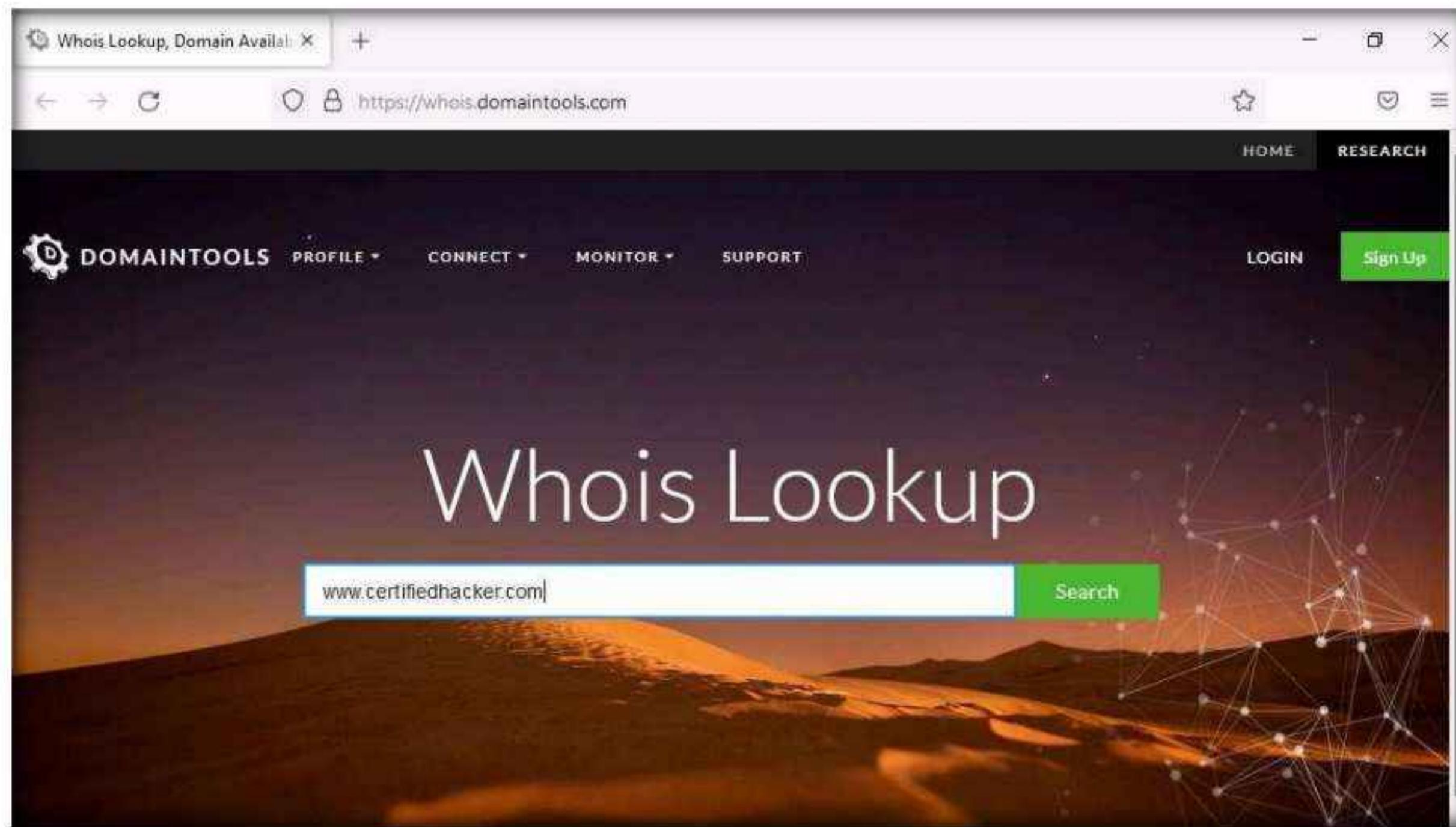
### Task 1: Perform Whois Lookup using DomainTools

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

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **http://whois.domaintools.com** and press **Enter**. The Whois Lookup website appears, as shown in the screenshot.



3. Now, in the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.



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.

A screenshot of the DomainTools website showing the Whois Record for "CertifiedHacker.com". The page title is "Whois Record for CertifiedHacker.com". The left side displays a table of registration details, including the Registrant (PERFECT PRIVACY, LLC), Registrar (Network Solutions, LLC), Dates (7,171 days old, Created on 2002-07-29, Expires on 2022-07-29, Updated on 2021-08-22), Name Servers (NS1.BLUEHOST.COM, NS2.BLUEHOST.COM), and Tech Contact (PERFECT PRIVACY, LLC). The right side features a sidebar with various tools: "DomainTools Iris" (Learn More), "Preview the Full Domain Report", "Tools" (Hosting History, Monitor Domain Properties, Reverse IP Address Lookup, Network Tools, Visit Website), and a preview of the website "certifiedhacker.com".

## Module 02 – Footprinting and Reconnaissance

The screenshot shows the DomainTools WHOIS lookup interface for the domain CertifiedHacker.com. The main left panel displays various domain details such as IP Address (162.241.216.11), IP Location (Utah - Provo - Unified Layer), ASN (AS26337 OIS1, US registered Oct 09, 2013), and domain status (Registered And Active Website). It also shows IP History, Registrar History, and Hosting History. Below this is a section for website analysis, including Website Title (Certified Hacker), Server Type (nginx/1.19.10), Response Code (200), Terms (36 Unique: 28, Linked: 7), Images (10 Alt tags missing: 0), and Links (16 Internal: 12, Outbound: 0). At the bottom of this panel is a Whois Record box showing the domain's registration information: Domain Name: CERTIFIEDHACKER.COM, Registry Domain ID: 88849376\_DOMAIN\_COM-VRSN, and Registrar WHOIS Server: whois.networksolutions.com. The right side of the interface features a sidebar for "Available TLDs" with tabs for "General TLDs" and "Country TLDs". It lists several domain extensions for purchase, including .com, .net, .org, .info, .biz, and .us, each with a "View Whois" or "Buy Domain" button. A legend at the top of the sidebar defines the colors: dark grey for "Taken domain", green for "Available domain", and orange for "Deleted previously owned domain".

5. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
6. 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.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 11** virtual machine.

## Lab Analysis

Analyze and document the results of this lab exercise.

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

### Internet Connection Required

Yes

No

### Platform Supported

Classroom

CyberQ

Lab

7

## Perform DNS Footprinting

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

### 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
- Gather information of subdomain and DNS records using SecurityTrails

### Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

### Lab Duration

Time: 20 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

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.

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 11** and **Parrot Security** virtual machines.
2. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**. Launch a **Command Prompt**, type **nslookup** and press **Enter**. This displays the default server and its address assigned to the **Windows 11** machine.

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

>
```

3. 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.
4. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set type=a
> www.certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

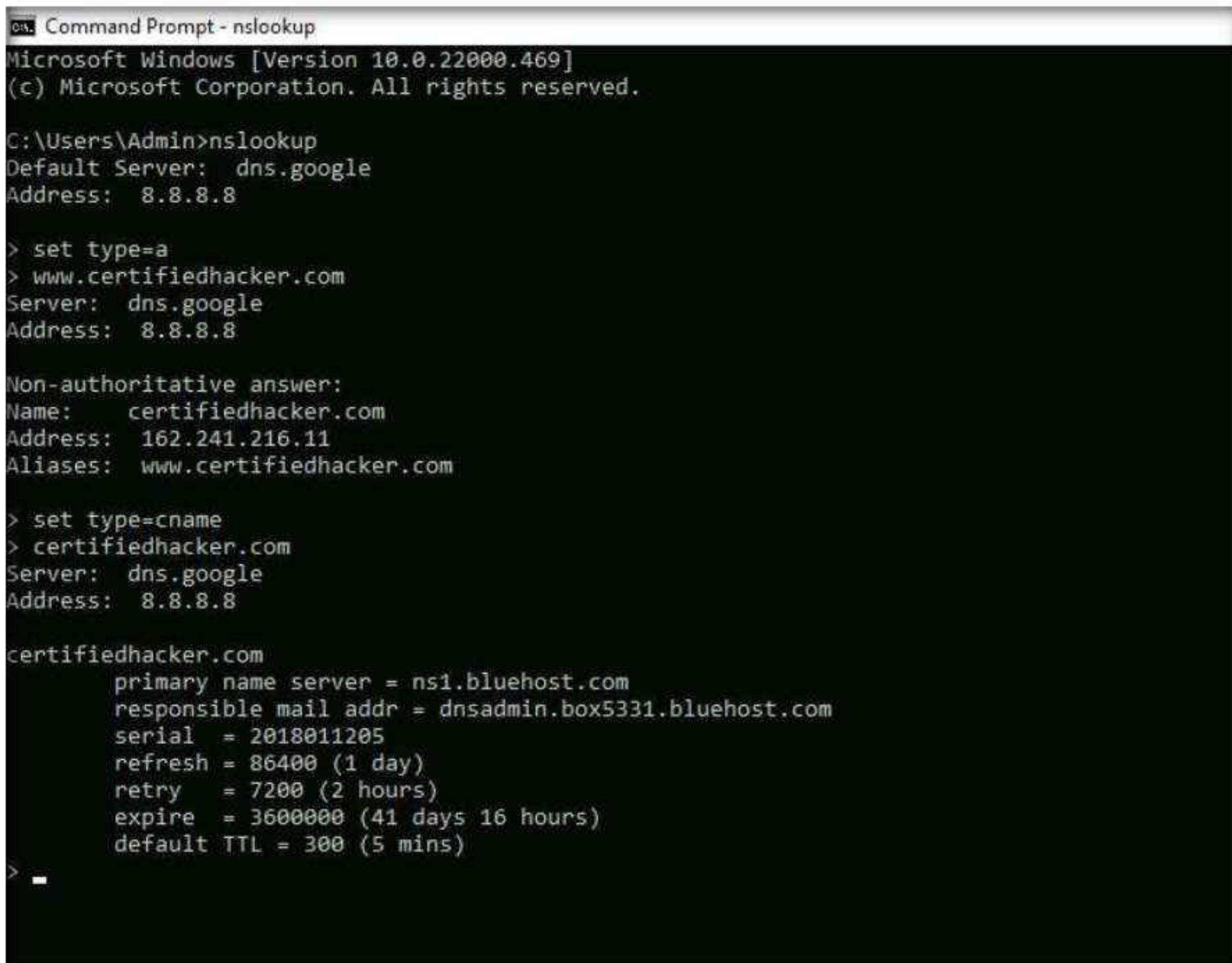
>
```

5. 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 11**) that resolves your requested domain.

6. 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**.
7. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.
8. 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.
9. Type **certifiedhacker.com** and press **Enter**.
10. 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.



```
on: Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set type=a
> www.certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

> set type cname
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
>
```

11. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.
12. Issue the command **set type=a** and press **Enter**.

13. 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.

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set type=a
> www.certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

> set type=cname
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
> set type=a
> ns1.bluehost.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: ns1.bluehost.com
Address: 162.159.24.80

> -
```

14. 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.
15. 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.
16. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.
17. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type <http://www.kloth.net/services/nslookup.php> and press **Enter**.

18. NSLOOKUP website appears, as shown in the screenshot.

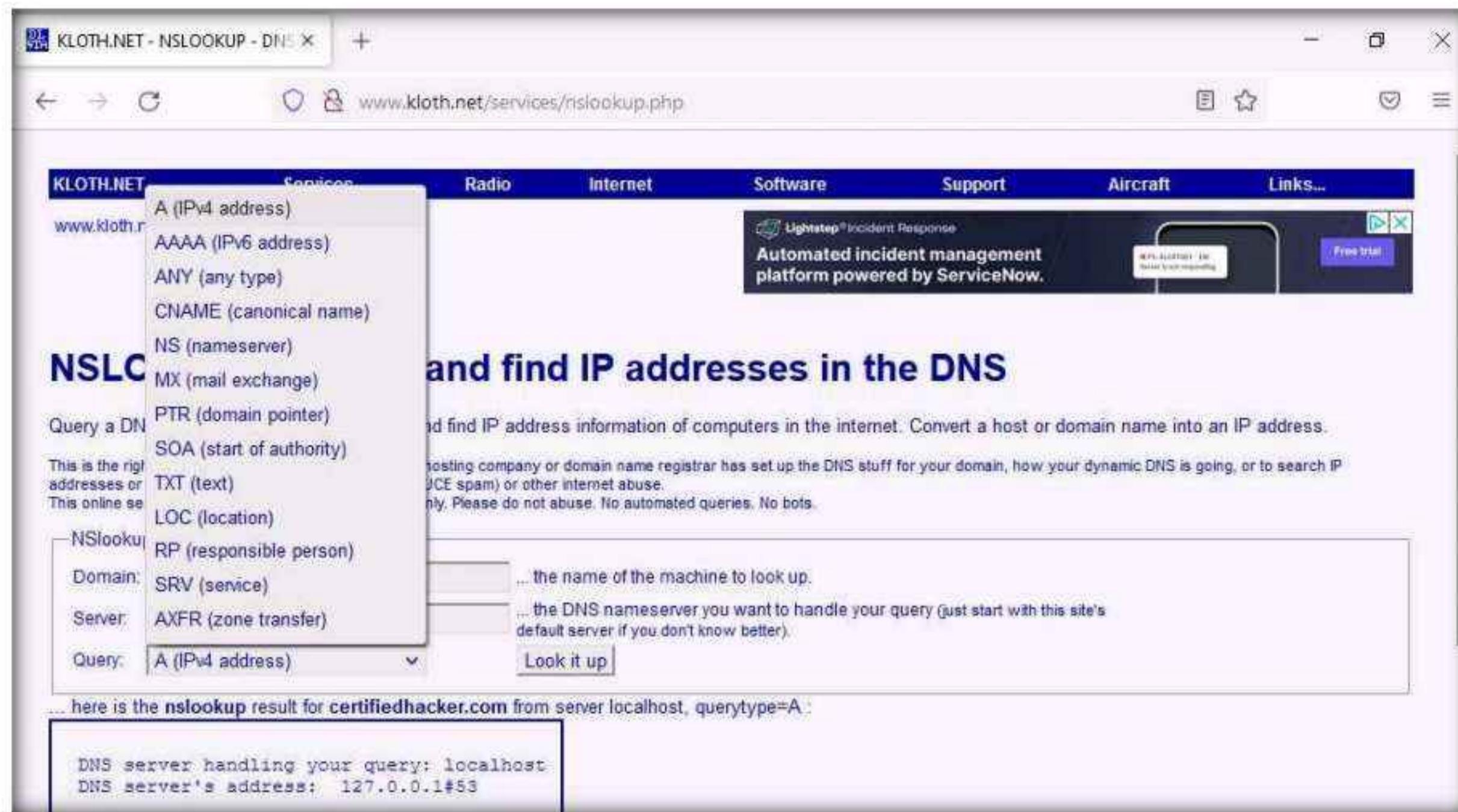
The screenshot shows a web browser window titled "KLOTH.NET - NSLOOKUP - DNS". The URL in the address bar is "www.kloth.net/services/nslookup.php". The page content includes a navigation menu with links like "KLOTH.NET", "Services", "Radio", "Internet", "Software", "Support", "Aircraft", and "Links...". A sidebar on the right displays a "FNT GmbH" advertisement for "White Paper Cable Management" with a "OPEN" button. The main content area is titled "NSLOOKUP: look up and find IP addresses in the DNS". It contains instructions for using the service to check DNS records. Below this is a "NSlookup" form with fields for "Domain" (containing "certifiedhacker.com"), "Server" (containing "localhost"), and "Query" (set to "A (IPv4 address)"). A "Look it up" button is present. At the bottom of the page, there is a note about the nslookup utility and its usage.

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.

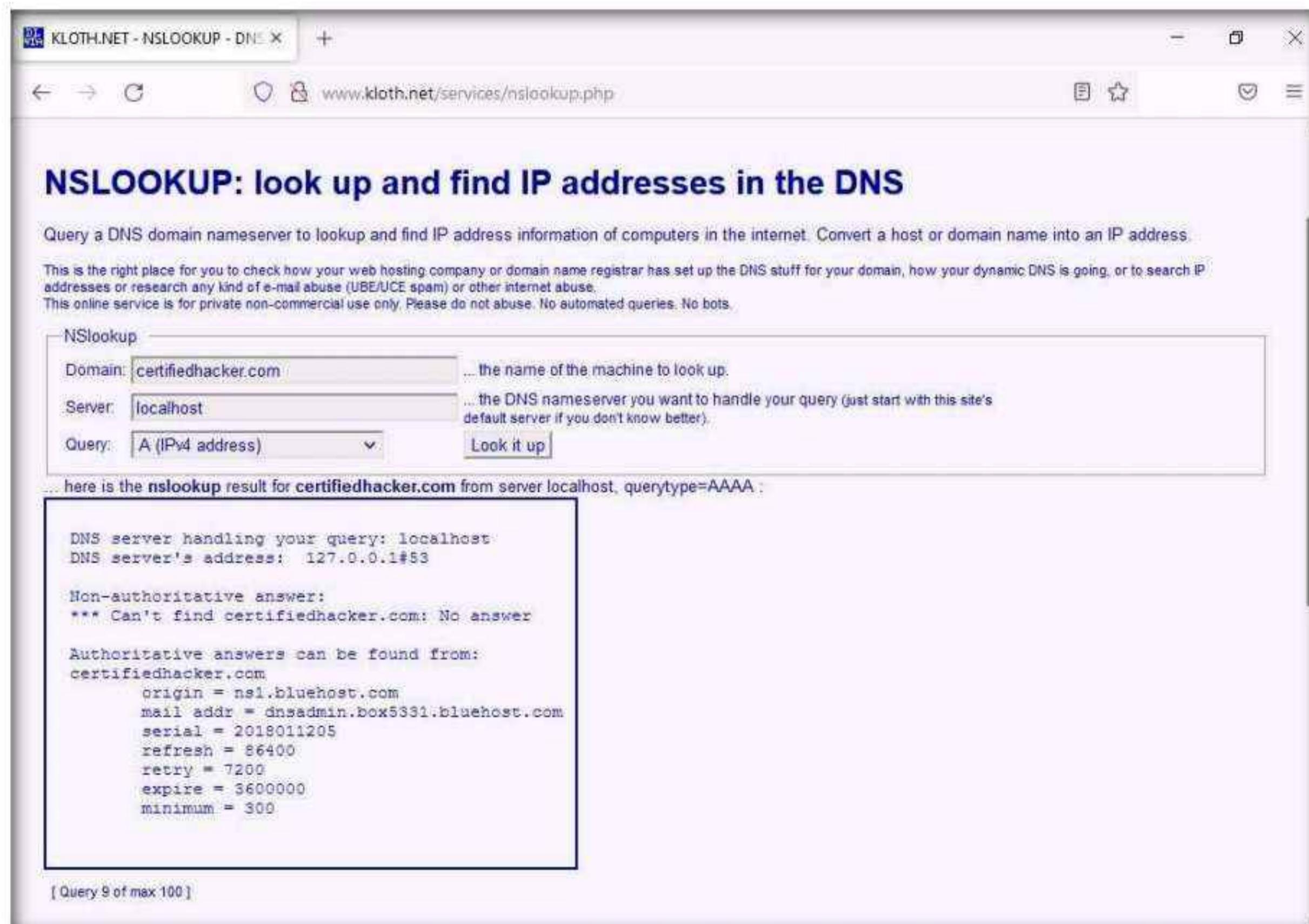
The screenshot shows the same web browser window as the previous one, but now displaying the results of the nslookup query for "certifiedhacker.com". The "NSlookup" form has been populated with "certifiedhacker.com" in the "Domain" field and "A (IPv4 address)" in the "Query" dropdown. The "Look it up" button has been clicked, and the results are displayed in a large text box below the form. The results show the DNS server handling the query is "localhost" and the IP address is "162.241.216.11". There is also some additional text at the bottom of the results box.

## Module 02 – Footprinting and Reconnaissance

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



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.



22. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.
23. You can also use DNS lookup tools such as **DNSdumpster** (<https://dnsdumpster.com>), **DNS Records** (<https://network-tools.com>), etc. to extract additional target DNS information.
24. Close all open windows and document all the acquired information.

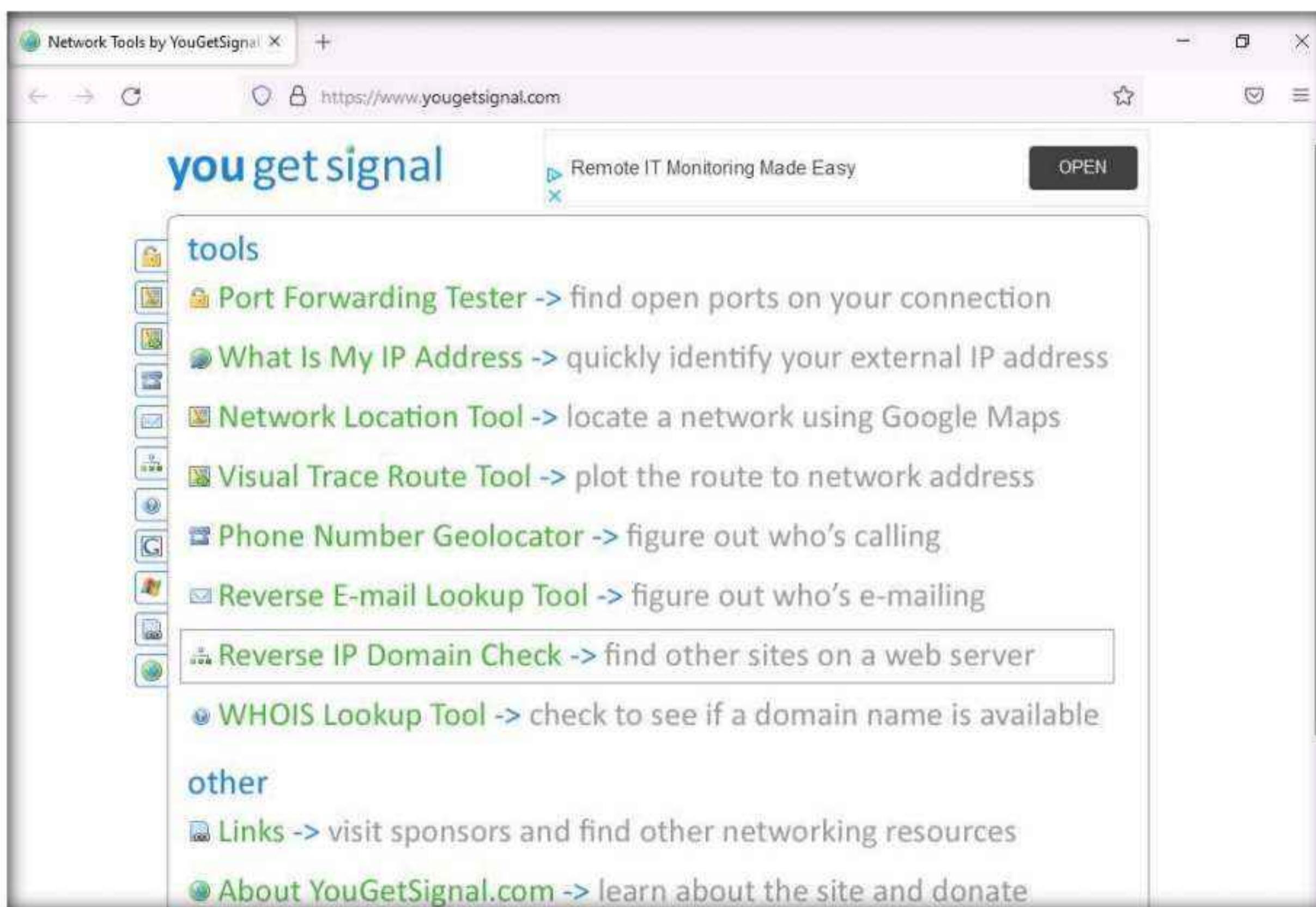
## Task 2: Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

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.

1. In the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type <https://www.yougetsignal.com> and press **Enter**.
2. **you get signal** website appears, click **Reverse IP Domain Check**.



3. 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.

yougetsignal

Reverse IP Domain Check

Remote Address: www.certifiedhacker.com Check

Found 12 domains hosted on the same web server as www.certifiedhacker.com (162.241.216.11).

100wwcbeaufort.org	bongakile.com	certifiedhacker.com	gaelicmemoriesphotography.ie	eakoffer.com	www.certifiedhacker.com	biosis.ae	box5331.bluehost.com	eis.qa	humancarehealth.com	www.certifiedhacker.com	www.1ststl.org
--------------------	---------------	---------------------	------------------------------	--------------	-------------------------	-----------	----------------------	--------	---------------------	-------------------------	----------------

**about**

Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this [domain list for purchase](#).

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides interesting visual [reverse IP lookup](#) tool. Knowing the other web sites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on [shared web hosting](#) plans.

[More about this tool.](#) [Set an API Key](#)

help me pay for school (PayPal)

**START NOW**

1. Click "Start Now"  
2. Download Now  
3. Enjoy Easy Search Tool

Easy Search Tool

©2009 Kirk Ouimet Design. All rights reserved. [Privacy Policy](#). Hosted by [VPSServer.com](#).

4. Now, switch to the **Parrot Security** virtual machine.
5. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
6. In the **Parrot Terminal** window, type **cd dnsrecon** and press **Enter** to enter into **dnsrecon** directory.
7. Type **chmod +x ./dnsrecon.py** and press **Enter**.

```
[attacker@parrot] ~
$ cd dnsrecon
[attacker@parrot] ~
$ chmod +x ./dnsrecon.py
[attacker@parrot] ~
$
```

8. Now type `./dnsrecon.py -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.

```
[attacker@parrot] ~
$ cd dnsrecon
[attacker@parrot] ~
$ chmod +x ./dnsrecon.py
[attacker@parrot] ~
$ ./dnsrecon.py -r 162.241.216.0-162.241.216.255
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[+] PTR 162-241-216-1.unifiedlayer.com 162.241.216.1
[+] PTR 162-241-216-0.unifiedlayer.com 162.241.216.0
[+] PTR 162-241-216-2.unifiedlayer.com 162.241.216.2
[+] PTR 162-241-216-3.unifiedlayer.com 162.241.216.3
[+] PTR 162-241-216-4.unifiedlayer.com 162.241.216.4
[+] PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
[+] PTR 162-241-216-10.unifiedlayer.com 162.241.216.10
[+] PTR 162-241-216-7.unifiedlayer.com 162.241.216.7
[+] PTR 162-241-216-6.unifiedlayer.com 162.241.216.6
[+] PTR 162-241-216-9.unifiedlayer.com 162.241.216.9
[+] PTR 162-241-216-8.unifiedlayer.com 162.241.216.8
[+] PTR box5331.bluehost.com 162.241.216.11
[+] PTR box5348.bluehost.com 162.241.216.17
[+] PTR 162-241-216-12.unifiedlayer.com 162.241.216.12
[+] PTR 162-241-216-13.unifiedlayer.com 162.241.216.13
[+] PTR 162-241-216-15.unifiedlayer.com 162.241.216.15
[+] PTR 162-241-216-16.unifiedlayer.com 162.241.216.16
[+] PTR box5334.bluehost.com 162.241.216.14
[+] PTR 162-241-216-18.unifiedlayer.com 162.241.216.18
[+] PTR box5350.bluehost.com 162.241.216.20
[+] PTR 162-241-216-19.unifiedlayer.com 162.241.216.19
[+] PTR 162-241-216-21.unifiedlayer.com 162.241.216.21
[+] PTR 162-241-216-22.unifiedlayer.com 162.241.216.22
```

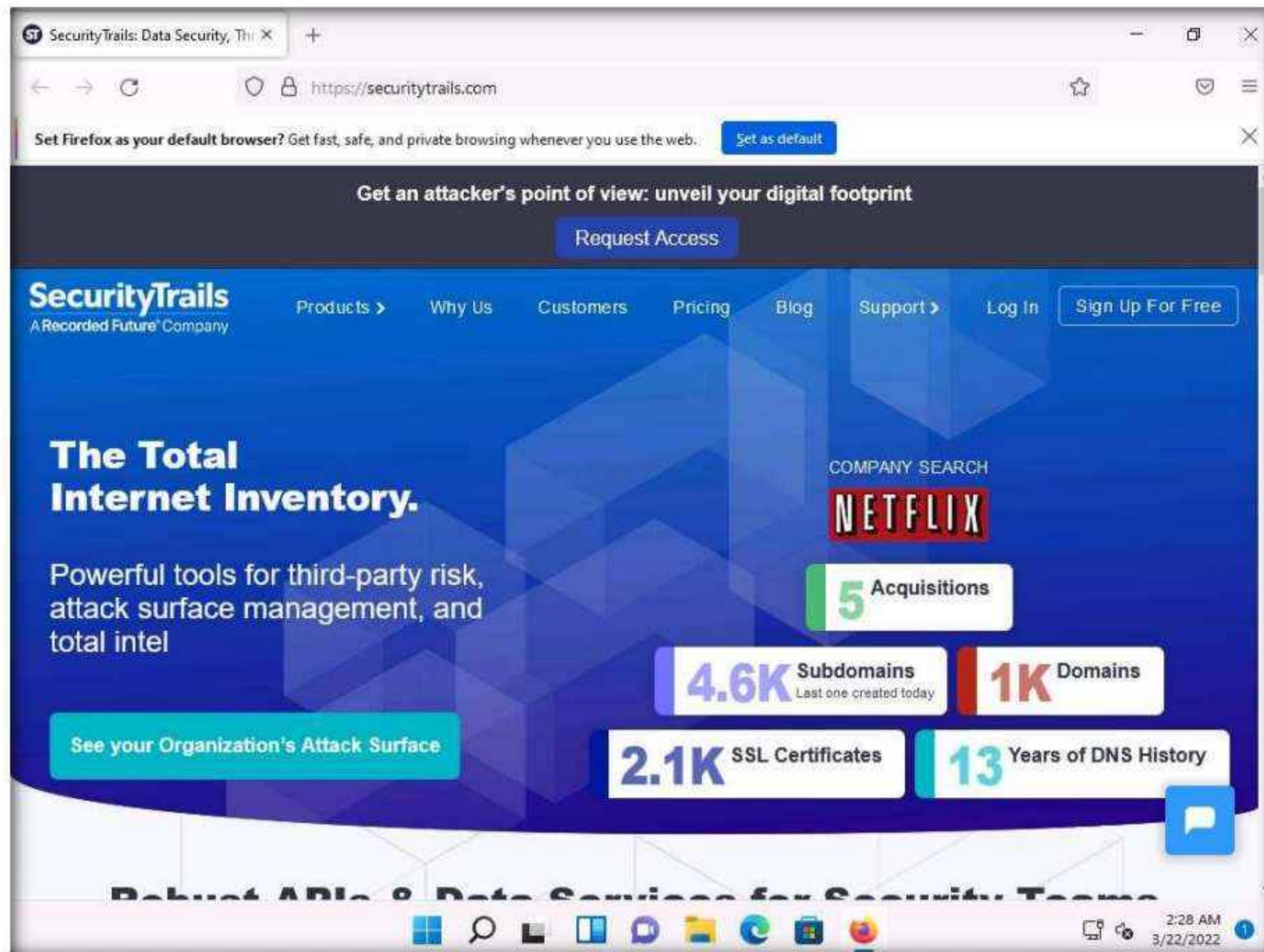
9. This concludes the demonstration of gathering information about a target organization by performing reverse DNS lookup using “you get signal’s” Reverse IP Domain Check and DNSRecon tool.
10. Close all open windows and document all the acquired information.
11. Turn off the **Parrot Security** virtual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

## Task 3: Gather Information of Subdomain and DNS Records using SecurityTrails

SecurityTrails is an advanced DNS enumeration tool that is capable of creating a DNS map of the target domain network. It can enumerate both current and historical DNS records such as A, AAAA, NS, MX, SOA, and TXT, which helps in building the DNS structure. It also enumerates all the existing subdomains of the target domain using brute-force techniques.

Here, we will use SecurityTrails to gather information regarding the subdomains and DNS records of the target website.

1. Switch to the **Windows 11** virtual machine.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type <https://securitytrails.com/> and press **Enter**.
3. **SecurityTrails** website appears, In the website, click on **Sign Up For Free** button at the top right corner of the page.



4. **Sign up-Free** page appears, enter the required details and check the terms and conditions check box. Click **Sign up for free**.

The screenshot shows the 'Sign up - Free' section of the SecurityTrails Signup page. It includes fields for Name, Email, and Company, along with a 'Reasons to join free:' sidebar.

**Reasons to join free:**

- Discover Historical DNS Records**: Find historical changes in the blink of an eye. Access 10+ years of data, including: A, AAA, MX, NS, SOA, and TXT records.
- Find Unseen Subdomains**: We update over 5 billion DNS records daily to ensure you're aware of every change. See the unseen, in mere seconds.
- Reveal Associated Domains**: Understand the relationship between domains. Unveil any associated domains.

SecurityTrails v2.11.0 © 2022 | Light Mode |

The screenshot shows the completed 'Sign up for free' form. The Company field contains 'ccc', and the Password field contains a masked password. The 'I accept the Terms of Service and Privacy Policy' checkbox is checked. The 'Sign up for free' button is visible at the bottom.

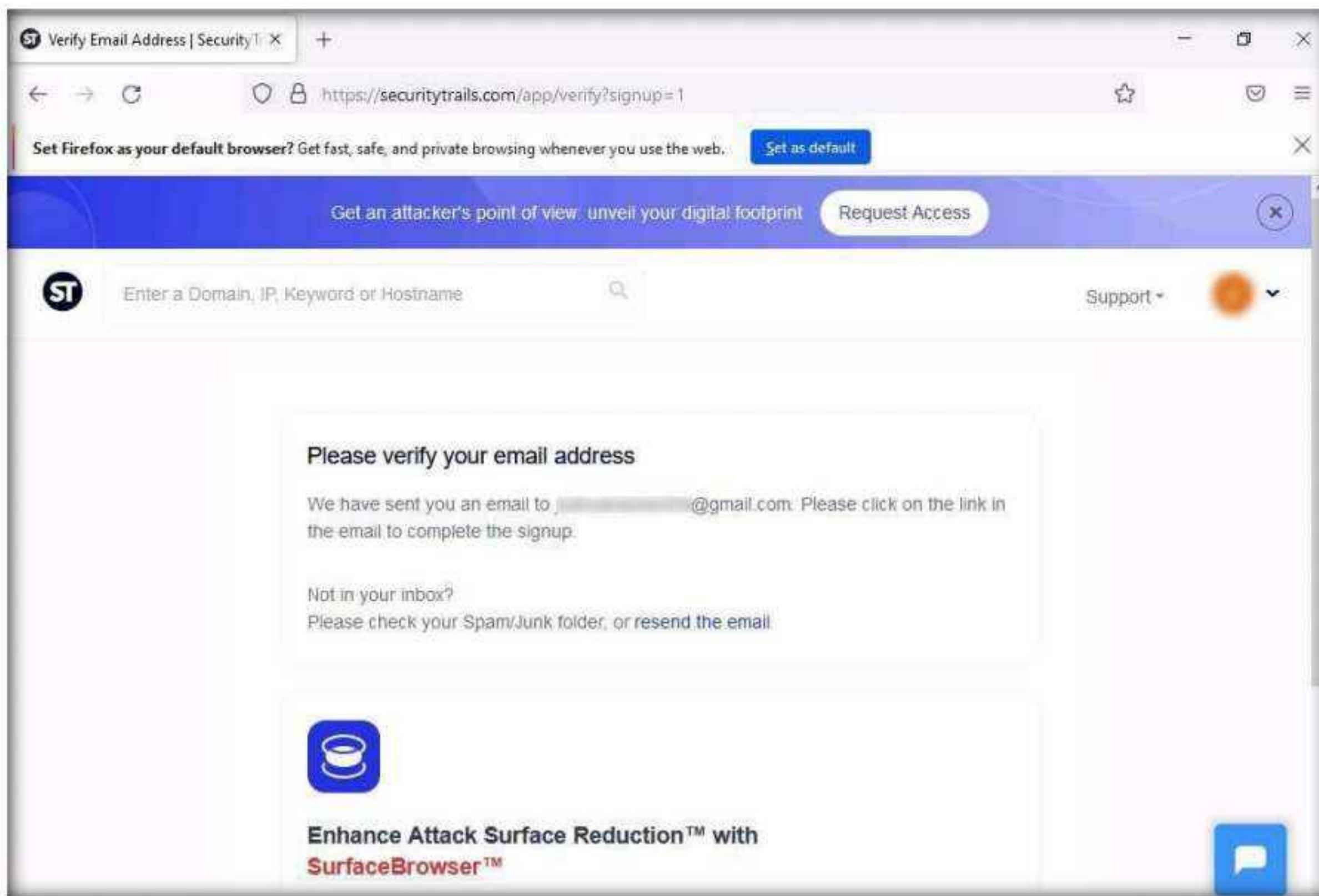
already have an account? [Sign in](#)

**Reveal Associated Domains**  
Understand the relationship between domains, companies, and individuals. Unveil any associated domains.

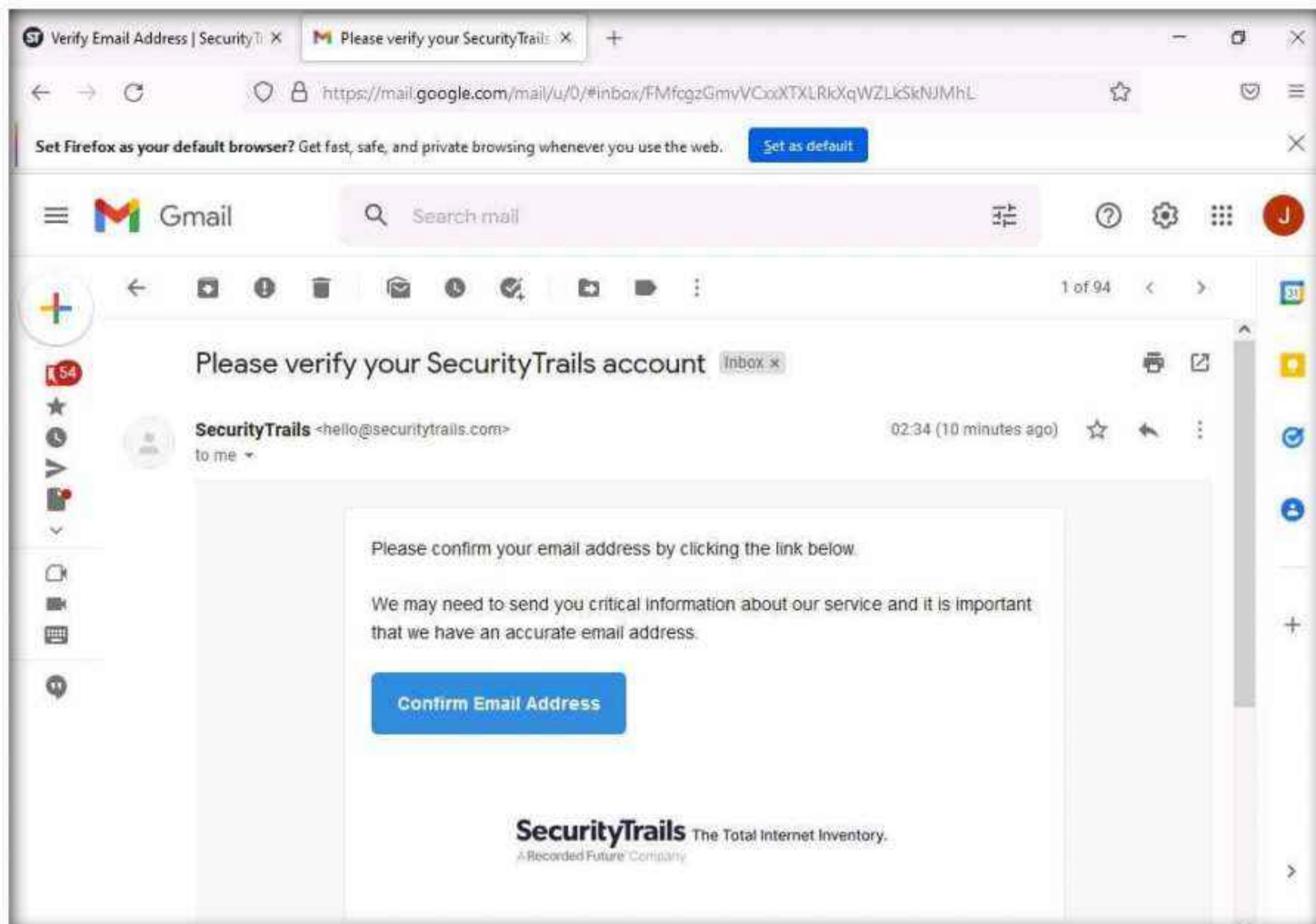
**Built for Modern Applications**  
Find code samples for Curl, JS, Python, PHP, Go, and other programming languages.

## Module 02 – Footprinting and Reconnaissance

5. A verification email will be sent to the email address.

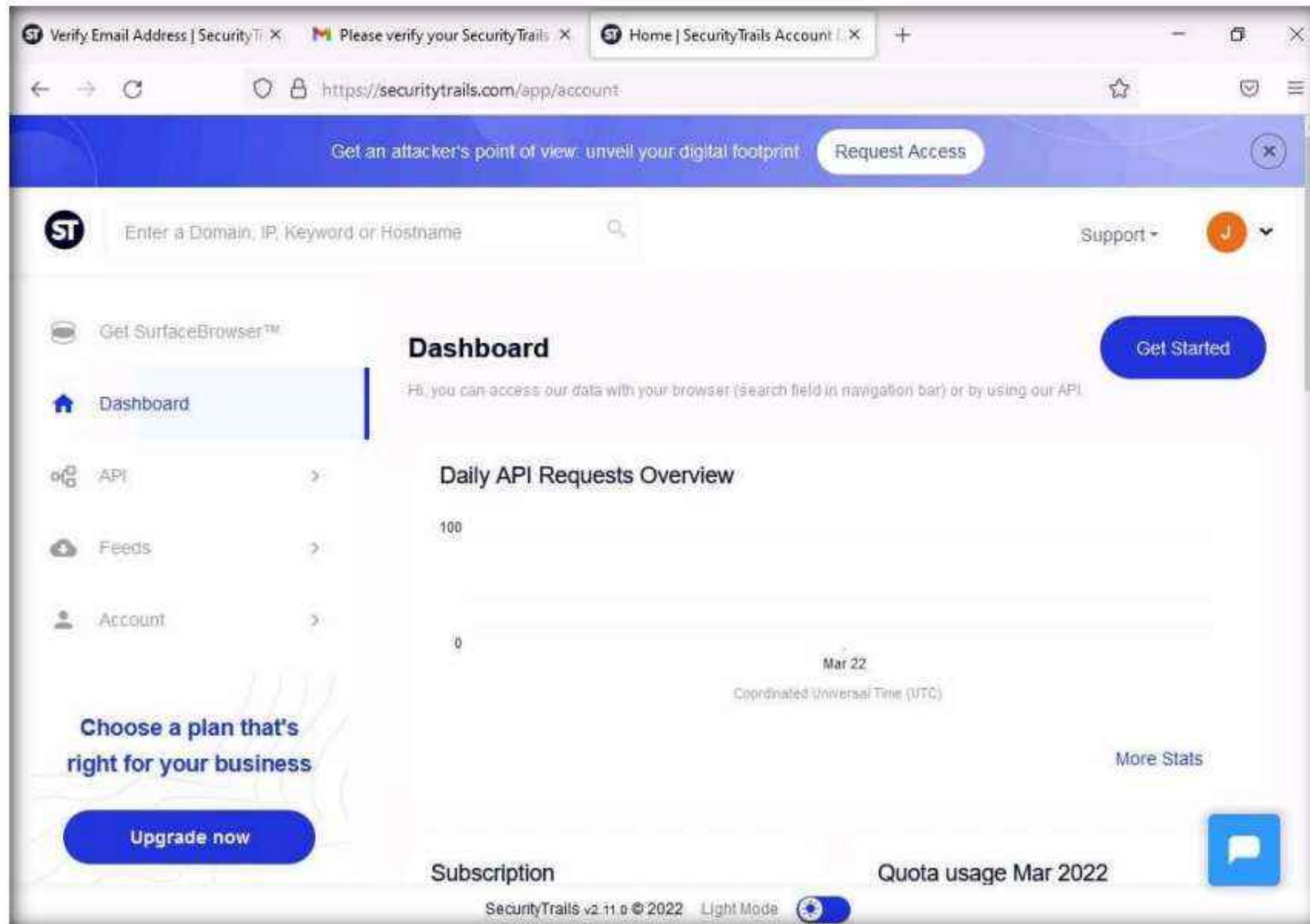


6. Open a new tab in the browser and login to the email account provided during sign up. Open the mail received from SecurityTrails and click on **Confirm Email Address**.



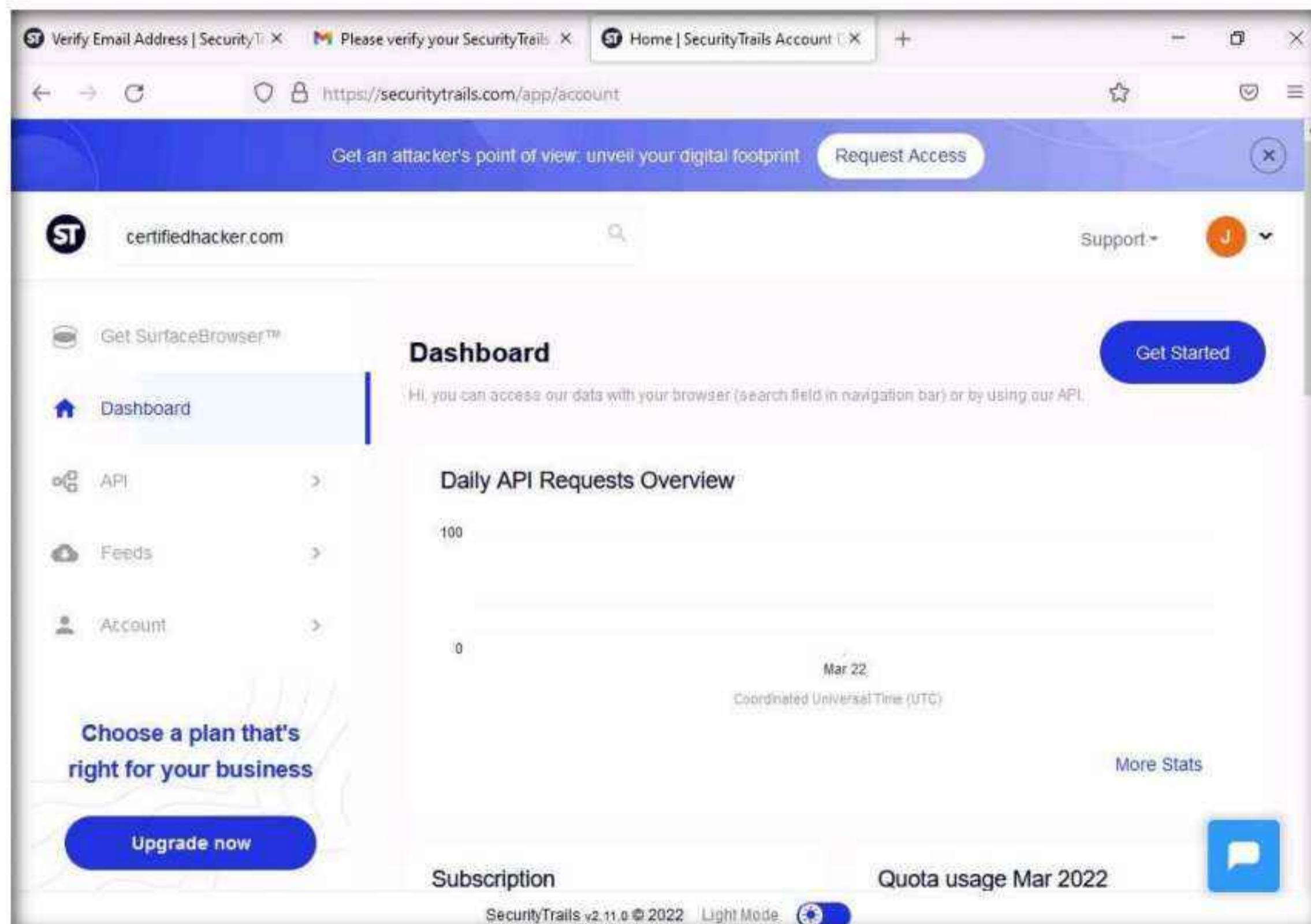
## Module 02 – Footprinting and Reconnaissance

7. After successful verification, you will be redirected to the **Dashboard** in SecurityTrails website.



The screenshot shows the SecurityTrails dashboard. At the top, there are three tabs: 'Verify Email Address' (SecurityTR), 'Please verify your SecurityTrails...', and 'Home | SecurityTrails Account'. The URL in the address bar is <https://securitytrails.com/app/account>. A banner at the top says 'Get an attacker's point of view: unveil your digital footprint' and has a 'Request Access' button. Below the banner, there's a search bar with the placeholder 'Enter a Domain, IP, Keyword or Hostname'. To the right of the search bar are 'Support' and a user icon. On the left, there's a sidebar with links for 'Get SurfaceBrowser™', 'Dashboard' (which is selected and highlighted in blue), 'API', 'Feeds', and 'Account'. The main content area is titled 'Dashboard' and contains a message: 'Hi, you can access our data with your browser (search field in navigation bar) or by using our API.' Below this is a section titled 'Daily API Requests Overview' with a chart showing 100 requests on Mar 22, Coordinated Universal Time (UTC). There's also a 'Choose a plan that's right for your business' section with a 'Upgrade now' button, and a 'Subscription' and 'Quota usage Mar 2022' section. At the bottom, it says 'SecurityTrails v2.11.0 © 2022' and has a 'Light Mode' toggle switch.

8. In the **Enter a Domain, IP, Keyword or Hostname** field, type **certifiedhacker.com** and press **Enter**.



This screenshot shows the same SecurityTrails dashboard as the previous one, but with the search term 'certifiedhacker.com' entered into the search bar. The rest of the interface is identical, including the sidebar, main dashboard content, and footer information.

## Module 02 – Footprinting and Reconnaissance

9. DNS records of certifiedhacker.com will appear, containing **A records, AAAA records, MX records, NS records, SOA records, TXT, and CNAME records**, as shown below.

The screenshot shows the SecurityTrails.com interface for the domain `certifiedhacker.com`. The left sidebar has options for DNS Records, Historical Data, and Subdomains. The main panel displays the DNS records as of March 22, 2022. Under the **A records** section, there is one entry: `162.241.216.11` (with 35,942 occurrences). The **AAAA records** section shows "NO RECORDS". The **MX records** section shows "NO RECORDS". A blue banner at the bottom encourages upgrading to SurfaceBrowser™.

This screenshot shows the same SecurityTrails.com interface for the domain `certifiedhacker.com`. The left sidebar is identical. The main panel now displays the **MX records** section, which lists one entry: `mail.certifiedhacker.com` (with 1 occurrence). The **NS records** section lists three entries: `Cloudflare, Inc.`, `ns2.bluehost.com` (with 2,069,456 occurrences), and `ns1.bluehost.com` (with 2,069,544 occurrences). A blue banner at the bottom encourages upgrading to SurfaceBrowser™.

## Module 02 – Footprinting and Reconnaissance

The image displays two screenshots of the SecurityTrails website, both showing the same domain information for `certifiedhacker.com`.

**Screenshot 1 (Top): DNS Records**

- SOA records:**
  - ttl: 86400
  - email: dnsadmin.box5331.bluehost.com
- TXT:**
  - v=spf1 a mx ptr include.bluehost.com ?all
- CNAME records pointed here:**
  - ftp.certifiedhacker.com
  - www.certifiedhacker.com

**Screenshot 2 (Bottom): CNAME Records**

- CNAME records pointed here:**
  - ftp.certifiedhacker.com
  - www.certifiedhacker.com
- View more certifiedhacker.com CNAME records**

## Module 02 – Footprinting and Reconnaissance

10. After examining the DNS records tab switch to **Historical Data** tab where you can find historical data of **A, AAAA, MX, NS, SOA** and **TXT** records.

The screenshot shows the SecurityTrails.com interface for the domain `certifiedhacker.com`. On the left sidebar, under the 'DOMAIN' section, the 'Subdomains' tab is selected, showing 86 subdomains. The main content area is titled 'certifiedhacker.com historical A data'. It displays a table of historical A records with the following columns: IP Addresses, Organization, First Seen, Last Seen, and Duration Seen. The data includes:

IP Addresses	Organization	First Seen	Last Seen	Duration Seen
162.241.216.11	Oso Grande IP Services, LLC	2020-10-30 (1 year)	2022-03-22 (today)	1 year
-	-	2020-10-30 (1 year)	2020-10-30 (1 year)	1 day
162.241.216.11	Oso Grande IP Services, LLC	2017-11-14 (4 years)	2020-10-30 (1 year)	3 years
69.89.31.193	Unified Layer	2016-12-31 (5 years)	2017-11-14 (4 years)	11 months

11. Now switch to **Subdomains** tab where you can find all the subdomains pertaining to `certifiedhacker.com`.

The screenshot shows the SecurityTrails.com interface for the domain `certifiedhacker.com`. On the left sidebar, under the 'DOMAIN' section, the 'Subdomains' tab is selected, showing 89 subdomains. The main content area is titled 'certifiedhacker.com subdomains'. It displays a table with the following columns: Domain, Rank, Hosting Provider, and Mail Provider. The data includes:

Domain	Rank	Hosting Provider	Mail Provider
cpcalendars.certifiedhacker.com	-	Oso Grande IP Services, LLC	-
cpanel.trustcenter.certifiedhacker.com	-	Oso Grande IP Services, LLC	-
www.events.certifiedhacker.com	-	Unified Layer	-
www.news.certifiedhacker.com	-	Unified Layer	-

12. DNS records provide important information about the locations and types of servers which attackers can use to further launch web application attacks.
13. This concludes the demonstration of gathering information on the subdomain and DNS records of a target organization using SecurityTrails.
14. You can also use **DNSChecker** (<https://dnschecker.org>), and **DNSdumpster** (<https://dnsdumpster.com>), etc. to perform DNS footprinting on a target website.
15. Close all open windows and document all the acquired information.
16. Turn off the **Windows 11** virtual machine.

## **Lab Analysis**

Analyze and document the results of this lab exercise.

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

---

### **Internet Connection Required**

Yes

No

### **Platform Supported**

Classroom

CyberQ

Lab

8

## Perform Network Footprinting

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

### 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:

- Windows 11 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 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

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.

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

**Note:** Here, we will consider [www.certifiedhacker.com](http://www.certifiedhacker.com) as a target website. However, you can select a target domain of your choice.

1. Turn on the **Windows 11** virtual machine. Login with Username: **Admin** and Password: **Pa\$\$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type <https://www.arin.net/about/welcome/region> and press **Enter**.  
**Note:** If **More secure, encrypted DNS lookups** notification appears at the top section of browser, click **Disable**.
3. ARIN website appears, 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.

## Module 02 – Footprinting and Reconnaissance

The screenshot shows a web browser window for the American Registry for Internet (ARIN) at <https://www.arin.net>. The page displays the ARIN logo and navigation menu. A search bar at the top contains the IP address `162.241.216.11`. Below the search bar, a message states: "ARIN is a nonprofit, member-based organization that administers IP addresses & ASNs in support of the operation and growth of the Internet." At the bottom of the main content area, there are five icons with corresponding links: "New to ARIN" (info icon), "Request IP Addresses & ASNs" (plus icon), "Transfers" (recycling icon), "IPv6 Info" (globe icon), and "Get Involved" (handshake icon).

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

The screenshot shows a web browser window for the ARIN Whois/RDAP search results. The URL is https://search.arin.net/rdap/?query=162.241.216.11. The search bar contains "162.241.216.11". The main content area displays the following details for the network range:

Source Registry	ARIN
Net Range	162.240.0.0 – 162.241.255.255
CIDR	162.240.0.0/15
Name	UNIFIEDLAYER-NETWORK-16
Handle	NET-162-240-0-0-1
Parent	NET-162-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	AS46606
Registration	Thu, 22 Aug 2013 18:57:53 GMT (Thu Aug 22 2013 local time)
Last Checked	Thu, 22 Aug 2013 18:57:54 GMT (Thu Aug 22 2013 local time)

The right sidebar includes links for "Related" topics: Report Whois Inaccuracy, Whois/RDAP Documentation, ARIN Technical Discussion, Mailing List, and FAQs.

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

## Task 2: Perform Network Tracerouting in Windows and Linux Machines

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.

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

**Note:** Here, we will consider [www.certifiedhacker.com](http://www.certifiedhacker.com) as a target website. However, you can select a target domain of your choice.

1. In the **Windows 11** 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.
2. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The user has run the command `tracert www.certifiedhacker.com`. The output displays the traceroute path from the user's machine to the target website, listing 19 intermediate hops. The first hop is the local machine at 10.10.1.2. Subsequent hops include various routers and network providers, ending at the final destination at 162.241.216.11. After the route is traced, the user runs `tracert /?` to see the available options for the command.

```
C:\Users\Admin>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

 1   1 ms    1 ms    <1 ms  10.10.1.2
 2   <1 ms    1 ms    1 ms  172.18.0.1
 3   1 ms    <1 ms    1 ms  192.168.100.6
 4   2 ms    2 ms    1 ms  103.152.3.225
 5   2 ms    1 ms    1 ms  38.140.226.249
 6   3 ms    2 ms    2 ms  te0-3-0-5.rcr21.tpa01.atlas.cogentco.com [154.24.5.181]
 7   8 ms    8 ms    8 ms  be2261.ccr21.mia01.atlas.cogentco.com [154.54.5.81]
 8   9 ms    8 ms    8 ms  be3400.ccr21.mia03.atlas.cogentco.com [154.54.47.18]
 9   10 ms   8 ms    8 ms  ntt.mia03.atlas.cogentco.com [154.54.9.42]
10   9 ms    9 ms    8 ms  ae-4.r22.miamfl02.us.bb.gin.ntt.net [129.250.4.88]
11   32 ms   38 ms   36 ms  ae-8.r20.dllstx14.us.bb.gin.ntt.net [129.250.2.219]
12   33 ms   33 ms   33 ms  ae-1.r00.dllstx16.us.bb.gin.ntt.net [129.250.7.121]
13   33 ms   33 ms   32 ms  ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net [128.242.179.18]
14   32 ms   34 ms   32 ms  xe-2-0-0.rtrn1.dal1.net.unifiedlayer.com [162.215.243.9]
15   32 ms   35 ms   32 ms  162-215-243-21.unifiedlayer.com [162.215.243.21]
16   33 ms   33 ms   34 ms  162-241-0-30.unifiedlayer.com [162.241.0.30]
17   33 ms   33 ms   33 ms  po100.router2a.hou1.net.unifiedlayer.com [162.241.0.3]
18   33 ms   33 ms   33 ms  108-167-150-118.unifiedlayer.com [108.167.150.118]
19   33 ms   33 ms   32 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
                [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout   Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr   Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.
```

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

```
04. Command Prompt
 9   10 ms    8 ms    8 ms  ntt.mia03.atlas.cogentco.com [154.54.9.42]
10   9 ms     9 ms    8 ms  ae-4.r22.miamfl02.us.bb.gin.ntt.net [129.250.4.88]
11   32 ms    38 ms   36 ms  ae-8.r20.dllstx14.us.bb.gin.ntt.net [129.250.2.219]
12   33 ms    33 ms   33 ms  ae-1.r00.dllstx16.us.bb.gin.ntt.net [129.250.7.121]
13   33 ms    33 ms   32 ms  ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net [128.242.179.18]
14   32 ms    34 ms   32 ms  xe-2-0-0.rtrn1.dal1.net.unifiedlayer.com [162.215.243.9]
15   32 ms    35 ms   32 ms  162-215-243-21.unifiedlayer.com [162.215.243.21]
16   33 ms    33 ms   34 ms  162-241-0-30.unifiedlayer.com [162.241.0.30]
17   33 ms    33 ms   33 ms  po100.router2a.hou1.net.unifiedlayer.com [162.241.0.3]
18   33 ms    33 ms   33 ms  108-167-150-118.unifiedlayer.com [108.167.150.118]
19   33 ms    33 ms   32 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout    Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr    Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.

C:\Users\Admin>tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

  1   1 ms    <1 ms    <1 ms  10.10.1.2
  2   2 ms     1 ms     1 ms  172.18.0.1
  3   1 ms    <1 ms     1 ms  192.168.100.6
  4   2 ms     1 ms    <1 ms  103.152.3.225
  5   2 ms     2 ms      3 ms  38.140.226.249

Trace complete.

C:\Users\Admin>
```

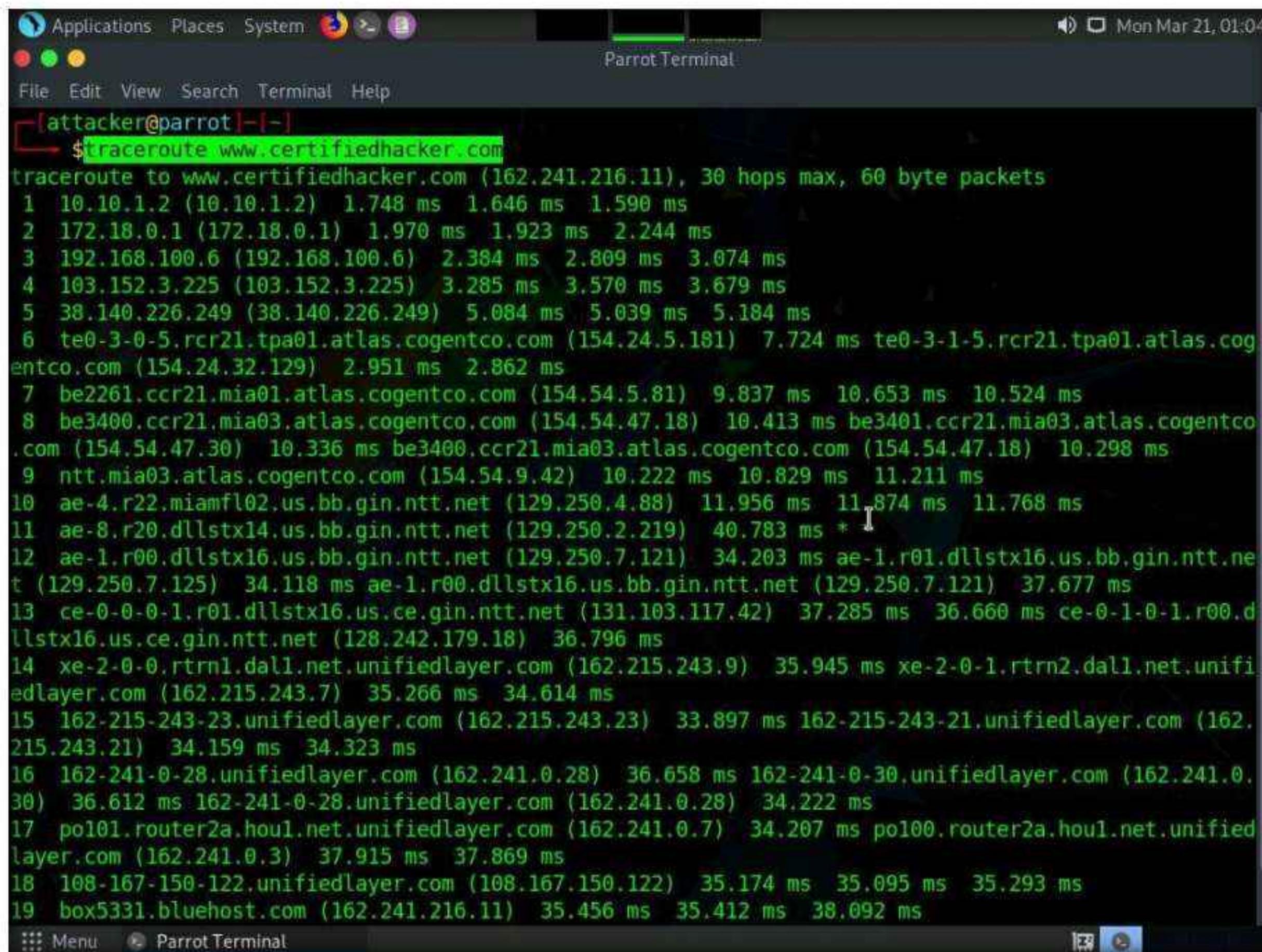
4. After viewing the result, close the command prompt window.  
 5. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press **Enter** to log in to the machine.

**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-left corner of the **Desktop** to open a **Terminal** window.
7. A **Parrot Terminal** window appears. 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.



The screenshot shows a terminal window titled "Parrot Terminal" with the command \$ traceroute www.certifiedhacker.com entered. The output displays the path taken by network packets from the source to the target, listing 19 distinct hops. The hops include various IP addresses and names of intermediate routers and servers along the route to www.certifiedhacker.com.

```
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  1.748 ms  1.646 ms  1.590 ms
 2  172.18.0.1 (172.18.0.1)  1.970 ms  1.923 ms  2.244 ms
 3  192.168.100.6 (192.168.100.6)  2.384 ms  2.809 ms  3.074 ms
 4  103.152.3.225 (103.152.3.225)  3.285 ms  3.570 ms  3.679 ms
 5  38.140.226.249 (38.140.226.249)  5.084 ms  5.039 ms  5.184 ms
 6  te0-3-0-5.rcr21.tpa01.atlas.cogentco.com (154.24.5.181)  7.724 ms te0-3-1-5.rcr21.tpa01.atlas.cogentco.com (154.24.32.129)  2.951 ms  2.862 ms
 7  be2261.ccr21.mia01.atlas.cogentco.com (154.54.5.81)  9.837 ms  10.653 ms  10.524 ms
 8  be3400.ccr21.mia03.atlas.cogentco.com (154.54.47.18)  10.413 ms be3401.ccr21.mia03.atlas.cogentco.com (154.54.47.30)  10.336 ms be3400.ccr21.mia03.atlas.cogentco.com (154.54.47.18)  10.298 ms
 9  ntt.mia03.atlas.cogentco.com (154.54.9.42)  10.222 ms  10.829 ms  11.211 ms
10  ae-4.r22.miamfl02.us.bb.gin.ntt.net (129.250.4.88)  11.956 ms  11.874 ms  11.768 ms
11  ae-8.r20.dllstx14.us.bb.gin.ntt.net (129.250.2.219)  40.783 ms *
12  ae-1.r00.dllstx16.us.bb.gin.ntt.net (129.250.7.121)  34.203 ms ae-1.r01.dllstx16.us.bb.gin.ntt.net (129.250.7.125)  34.118 ms ae-1.r00.dllstx16.us.bb.gin.ntt.net (129.250.7.121)  37.677 ms
13  ce-0-0-0-1.r01.dllstx16.us.ce.gin.ntt.net (131.103.117.42)  37.285 ms  36.660 ms ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net (128.242.179.18)  36.796 ms
14  xe-2-0-0.rtrn1.dall.net.unifiedlayer.com (162.215.243.9)  35.945 ms xe-2-0-1.rtrn2.dall.net.unifiedlayer.com (162.215.243.7)  35.266 ms  34.614 ms
15  162-215-243-23.unifiedlayer.com (162.215.243.23)  33.897 ms 162-215-243-21.unifiedlayer.com (162.215.243.21)  34.159 ms  34.323 ms
16  162-241-0-28.unifiedlayer.com (162.241.0.28)  36.658 ms 162-241-0-30.unifiedlayer.com (162.241.0.30)  36.612 ms 162-241-0-28.unifiedlayer.com (162.241.0.28)  34.222 ms
17  pol01.router2a.hou1.net.unifiedlayer.com (162.241.0.7)  34.207 ms pol00.router2a.hou1.net.unifiedlayer.com (162.241.0.3)  37.915 ms  37.869 ms
18  108-167-150-122.unifiedlayer.com (108.167.150.122)  35.174 ms  35.095 ms  35.293 ms
19  box5331.bluehost.com (162.241.216.11)  35.456 ms  35.412 ms  38.092 ms
```

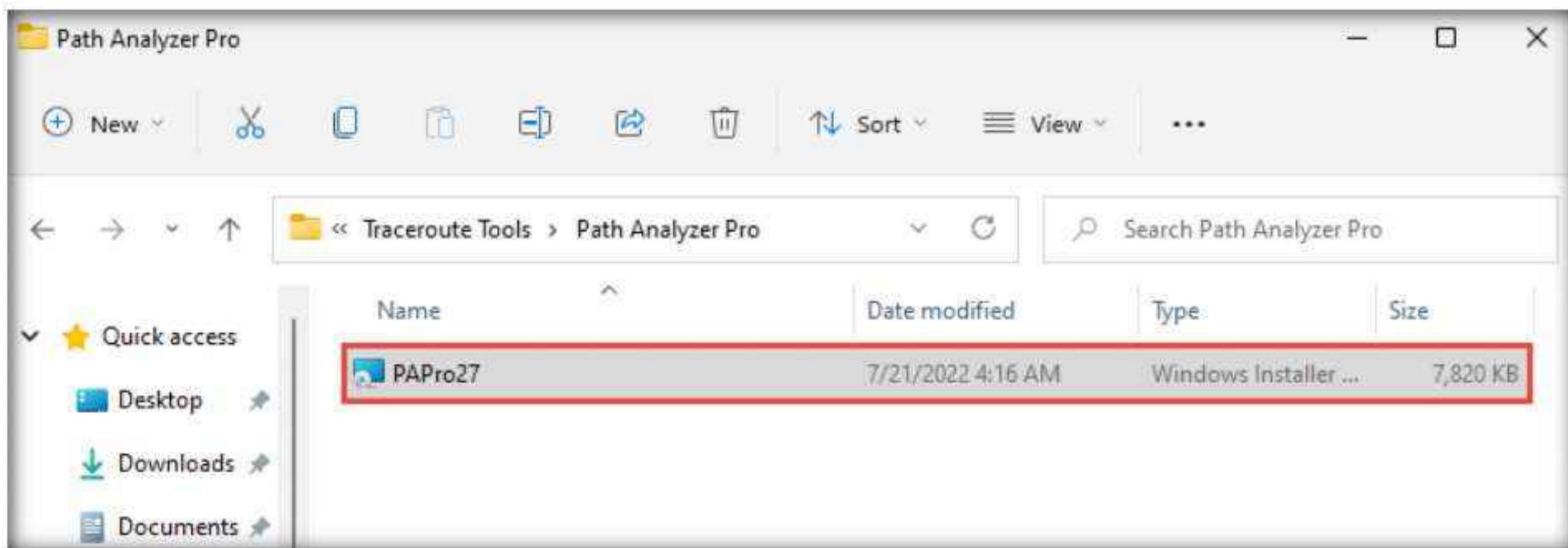
8. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
9. You can also use other traceroute tools such as **VisualRoute** (<http://www.visualroute.com>), **Traceroute NG** (<https://www.solarwinds.com>), etc. to extract additional network information of the target organization.
10. Close all open windows and document all acquired information.
11. Turn off the **Parrot Security** virtual machine.

## Task 3: Perform Advanced Network Route Tracing Using Path Analyzer Pro

Path Analyzer Pro performs network route tracing with performance tests, DNS, Whois, and network resolution to investigate network issues.

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

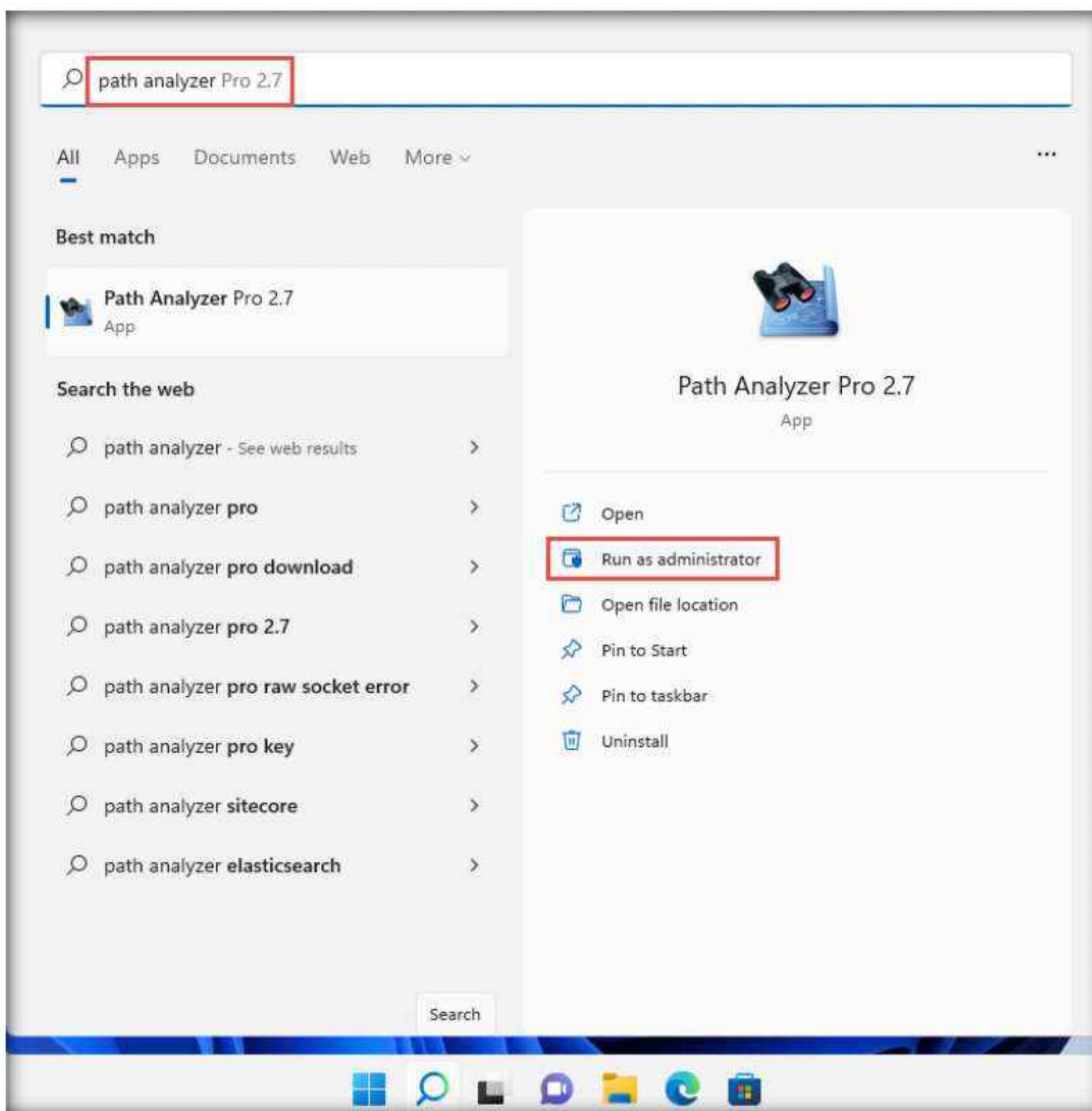
1. In the **Windows 11** virtual machine, open **File Explorer** and navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro** and double-click **PAPro27.msi**.



2. The **Path Analyzer Pro 2.7** setup window appears.
3. Follow the wizard steps (by selecting default options) to install Path Analyzer Pro.

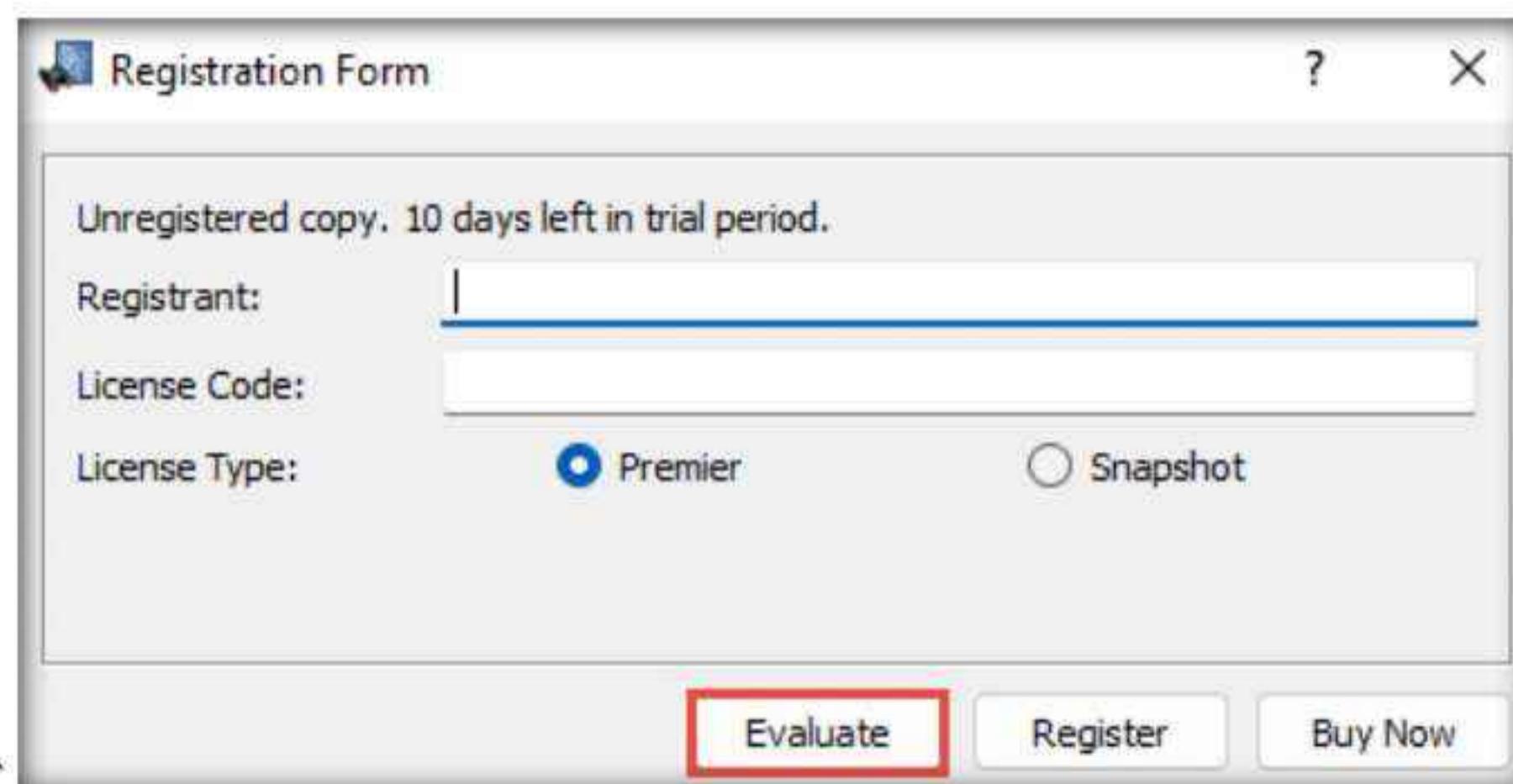
**Note:** If a **User Account Control** window appears, click **Yes**.

4. Click **Search icon** (  ) on the **Desktop**. Type **path analyzer** in the search field, the **Path Analyzer Pro 2.7** appears in the result, click **Run as administrator** to launch it.



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

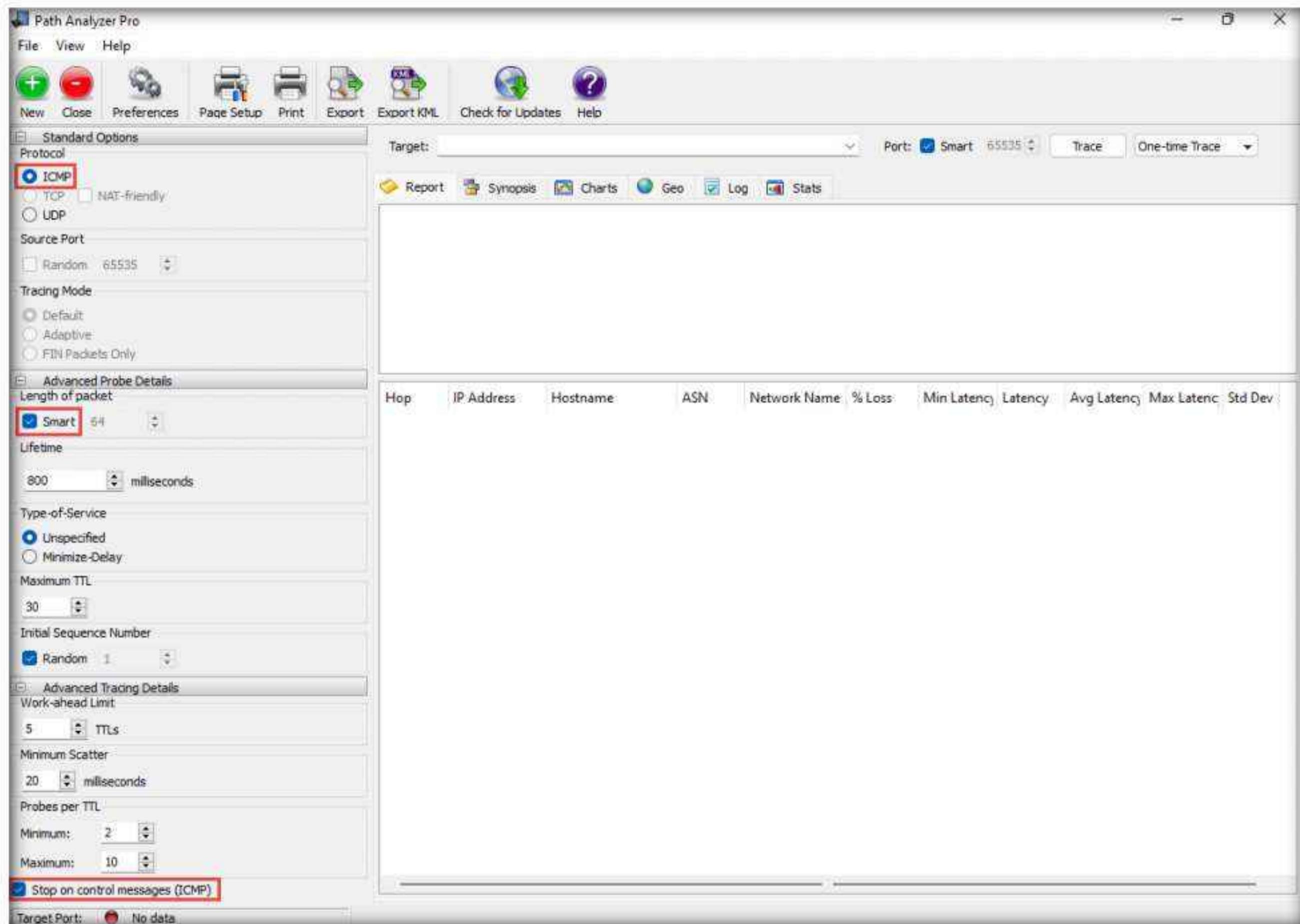
5. The **Path Analyzer Pro** window appears along with a **Registration Form** pop-up; click **Evaluate** in the pop-up.



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.

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.

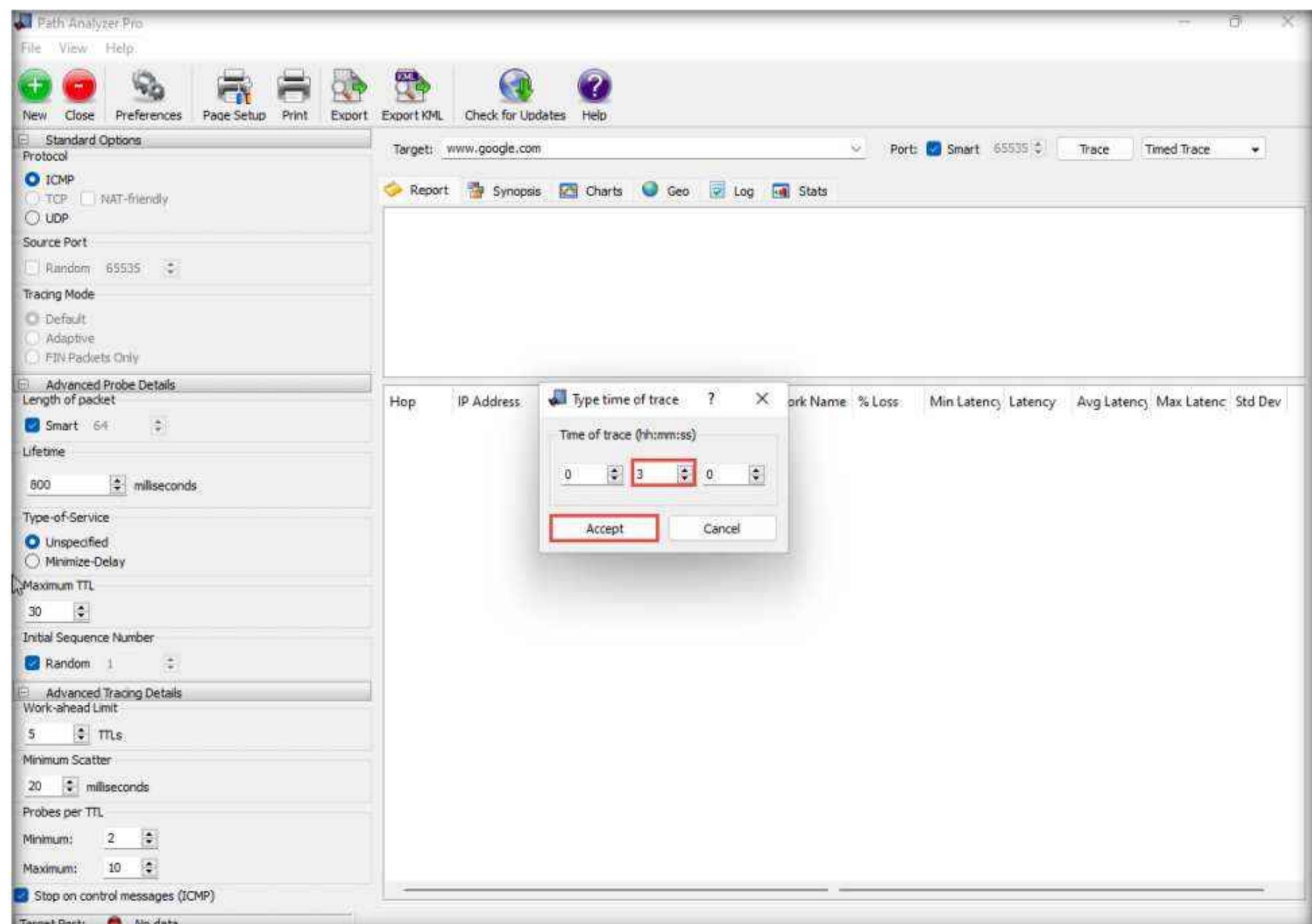


## Module 02 – Footprinting and Reconnaissance

- 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**.



- 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**.

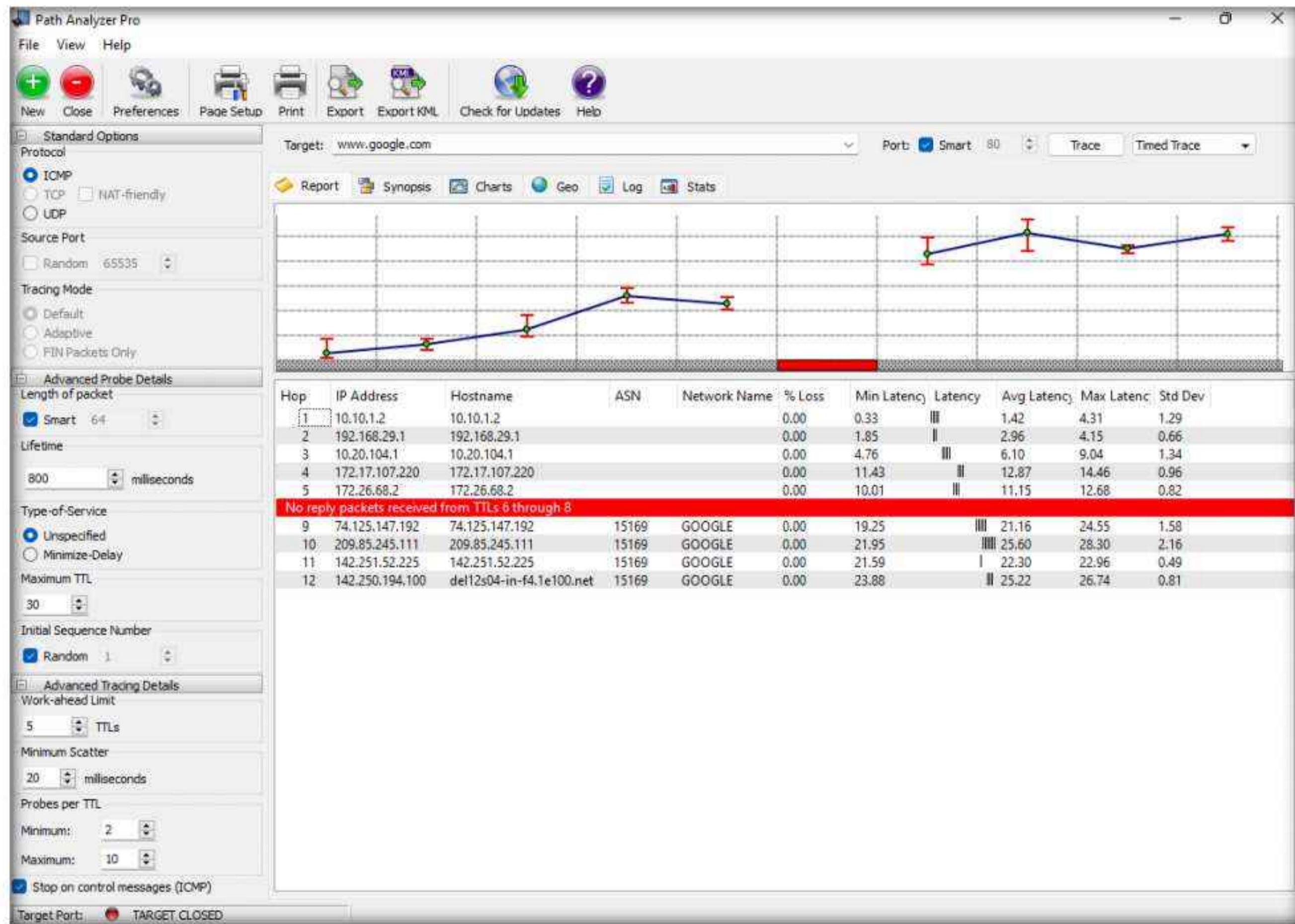


- While Path Analyzer Pro performs this trace, the **Trace** button changes automatically to **Stop**.

**Note:** If a **read** pop-up appears click **OK**.

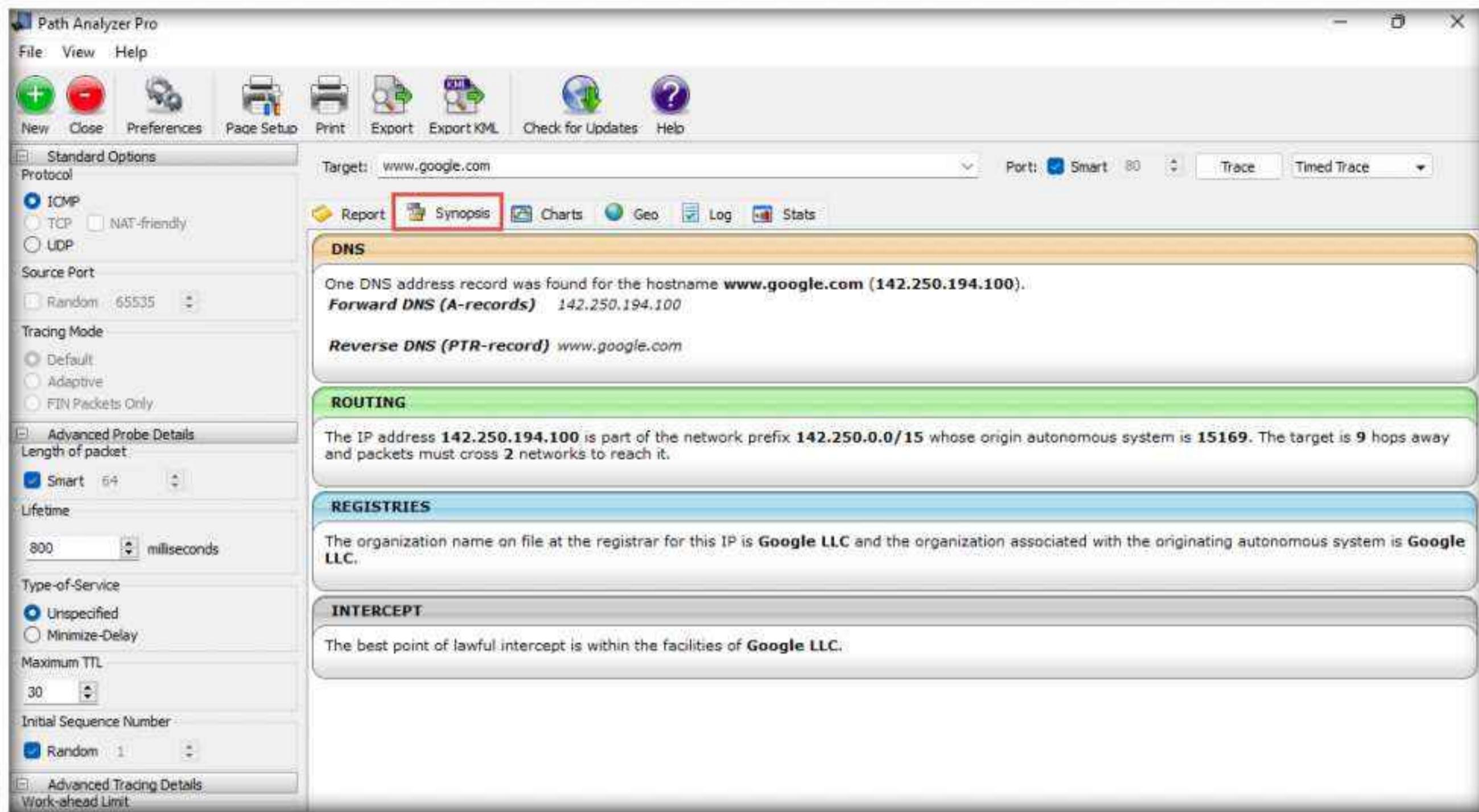
## Module 02 – Footprinting and Reconnaissance

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.

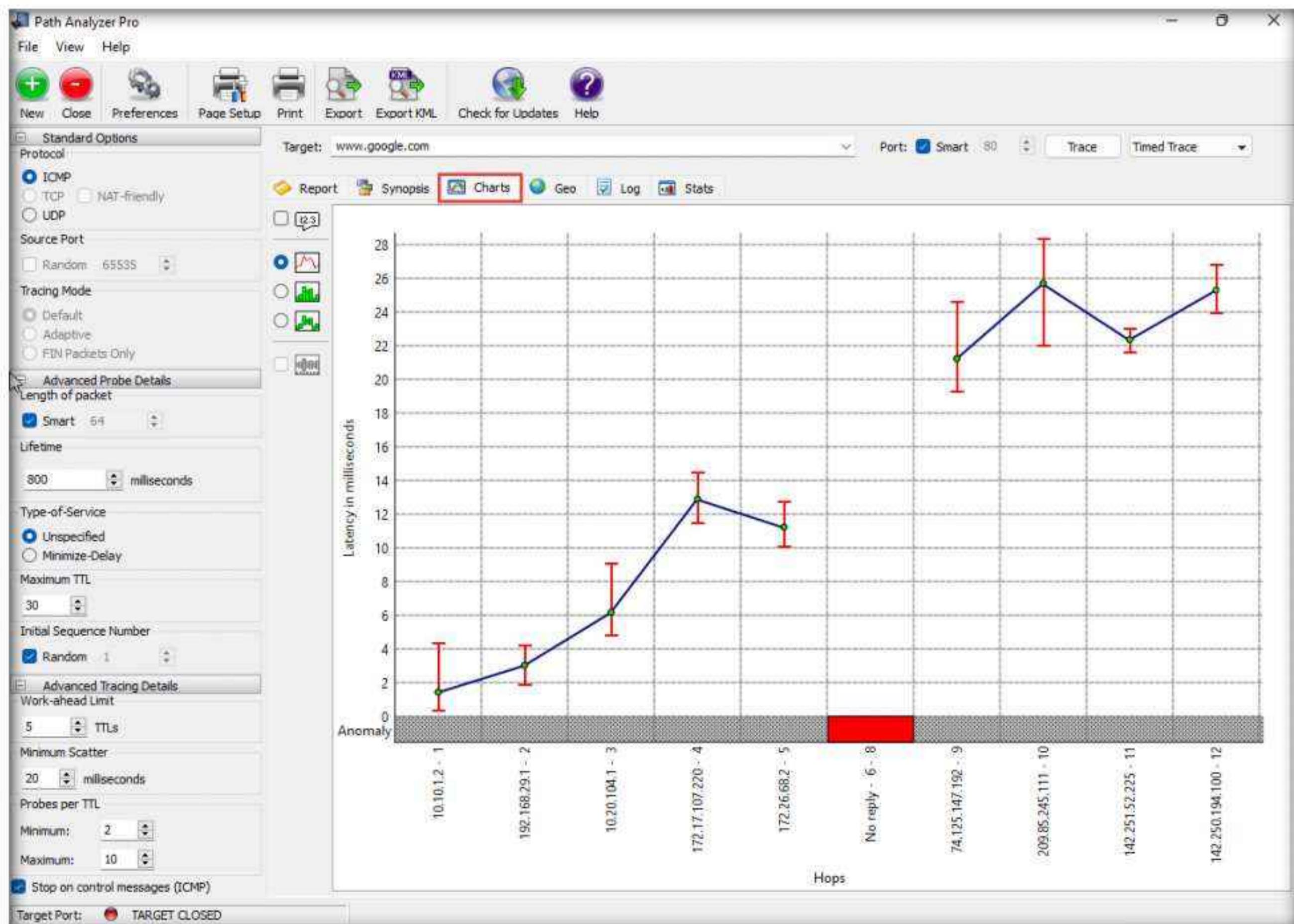


## Module 02 – Footprinting and Reconnaissance

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

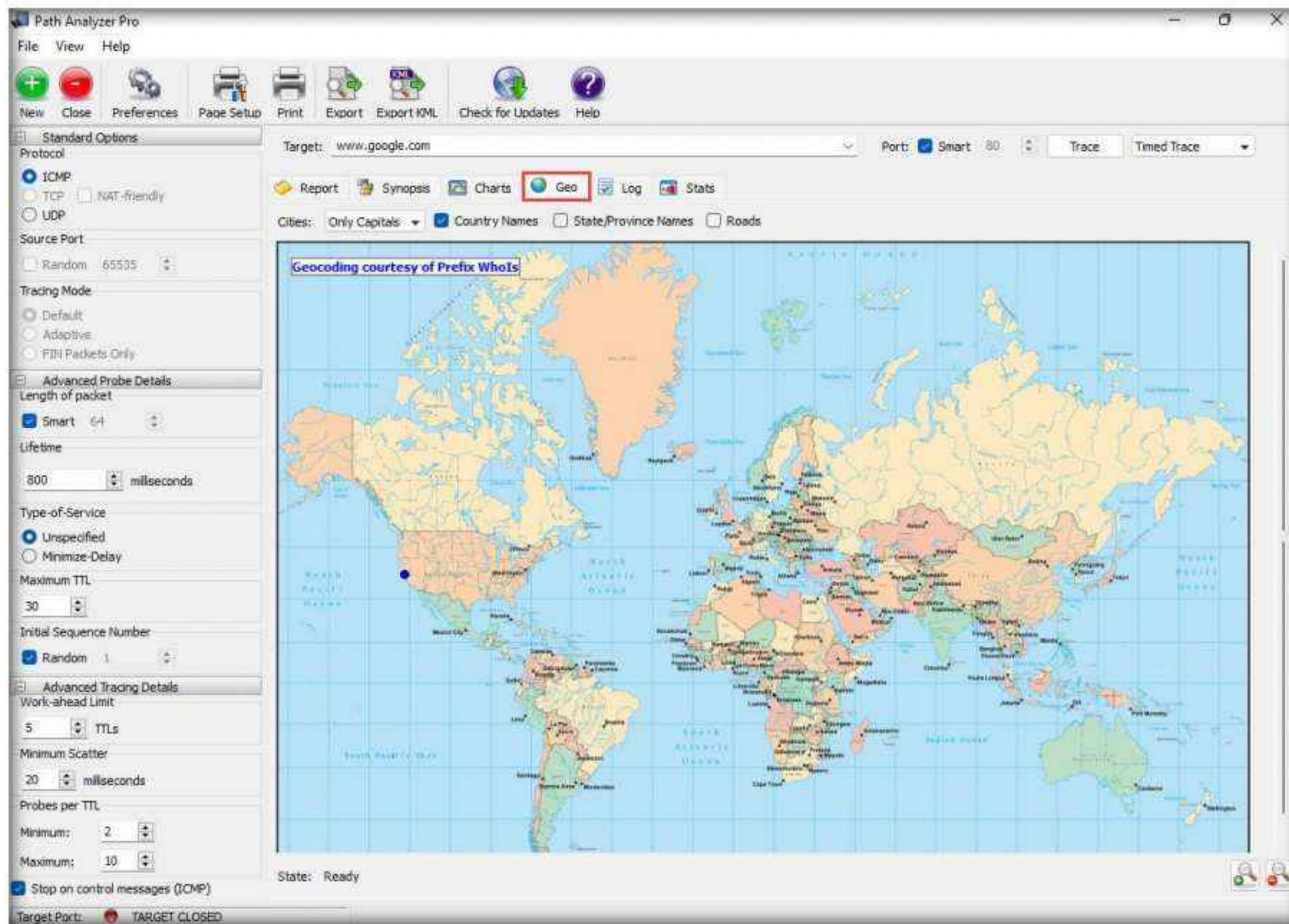


13. Click the **Charts** tab to view the results of the trace.

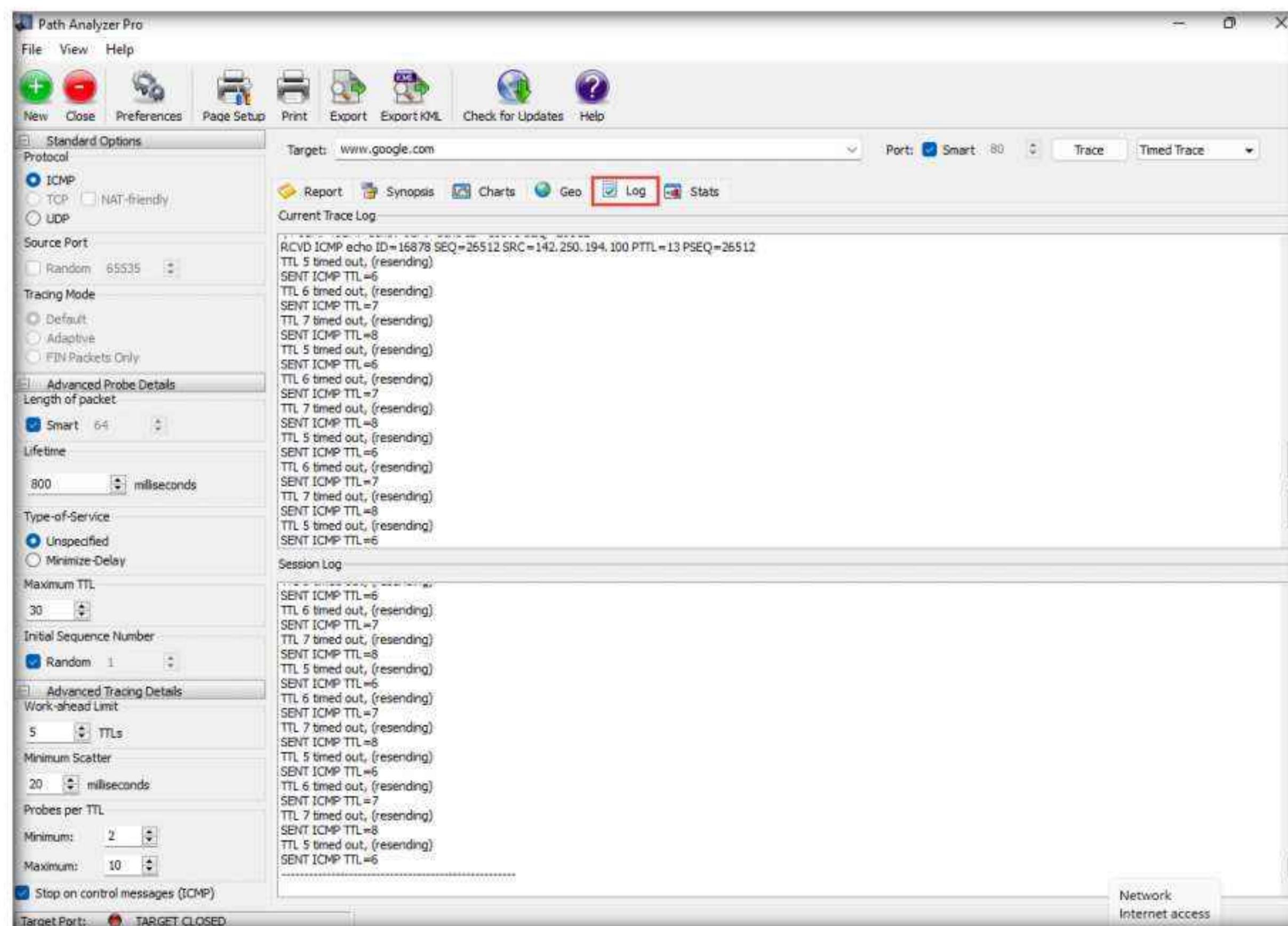


## Module 02 – Footprinting and Reconnaissance

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

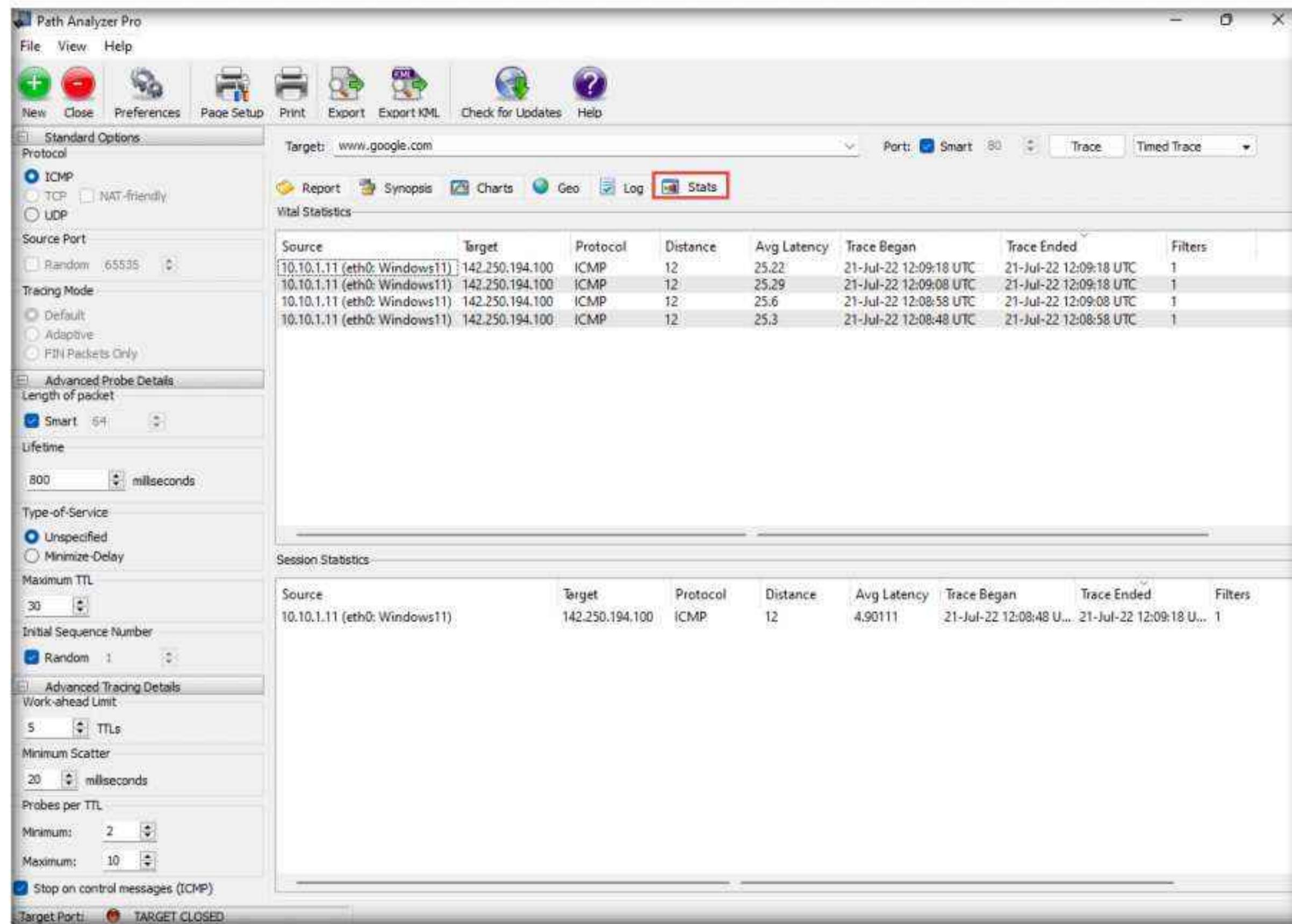


15. Click the **Log** tab to view Current Trace Log and Session Log.

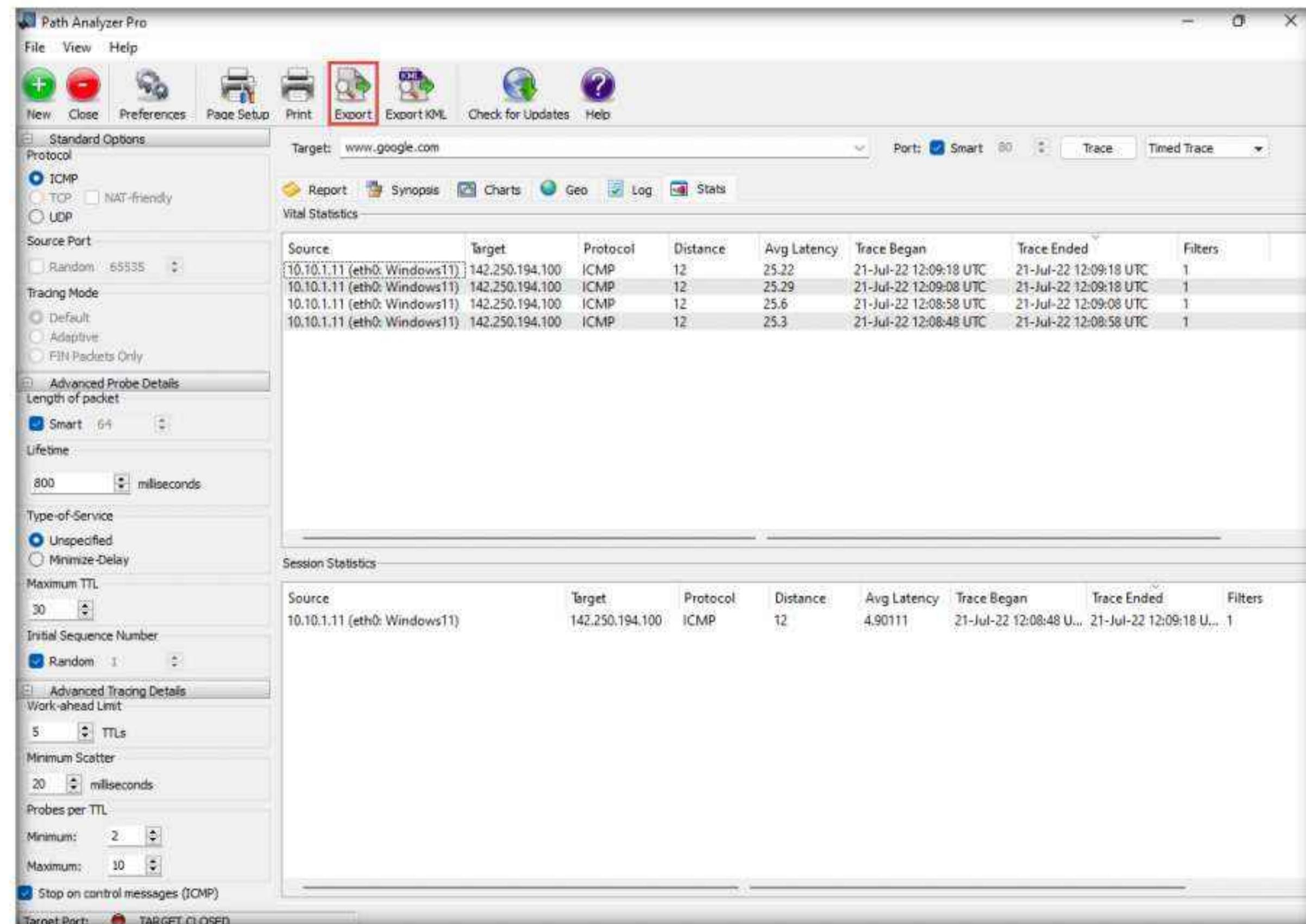


## Module 02 – Footprinting and Reconnaissance

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

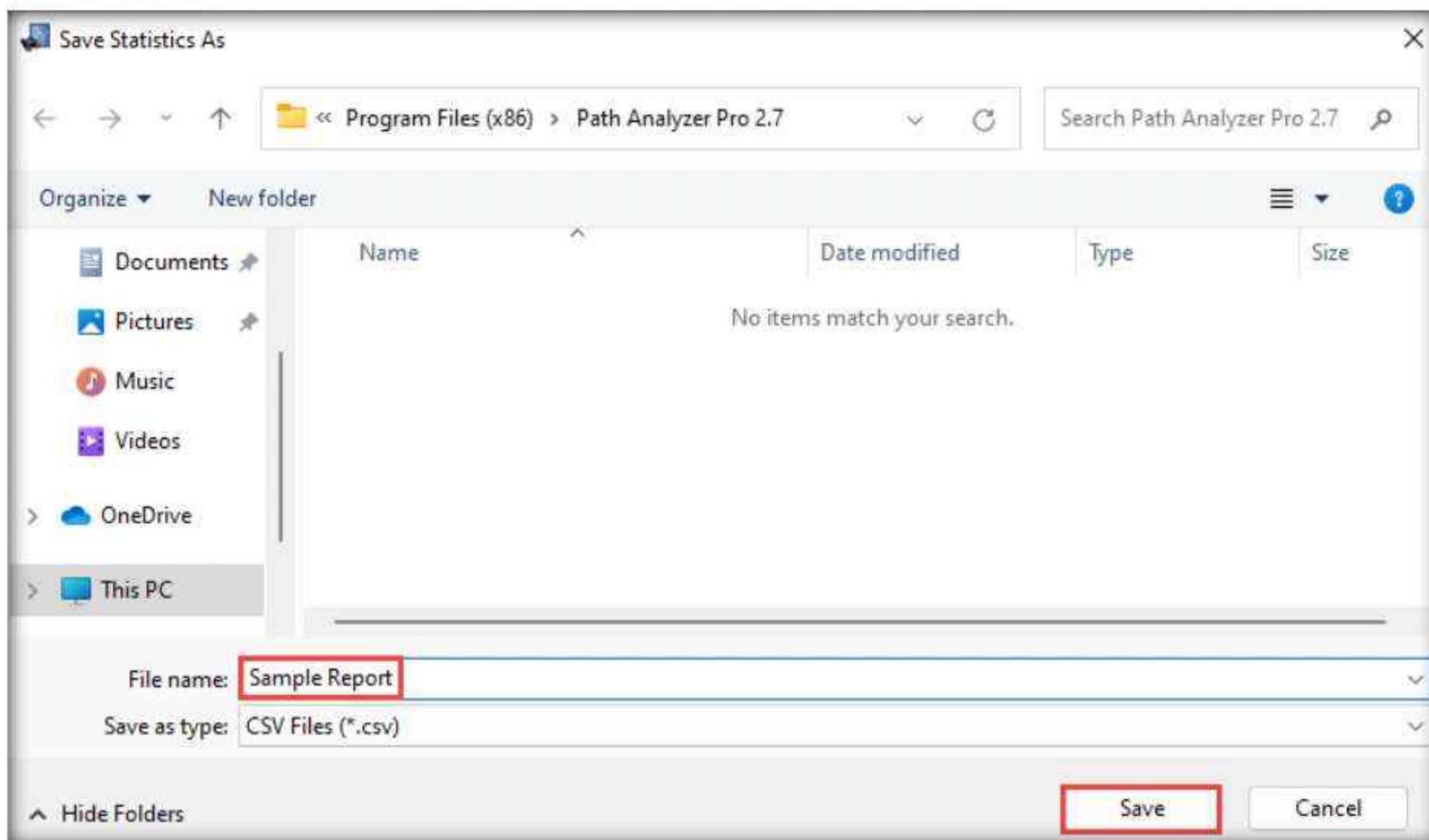


17. Click **Export** in the toolbar to export the report.



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.



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 11** virtual machine.

## Lab Analysis

Analyze and document the results of this lab exercise.

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

<b>Internet Connection Required</b>	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Platform Supported</b>	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> CyberQ

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.*

### 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

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

## 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: Footprinting a Target using Recon-ng

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.

**Note:** Here, we will consider [www.certifiedhacker.com](http://www.certifiedhacker.com) as a target website. However, you can select a target domain of your choice.

**Note:** The results obtained might differ when you perform this lab task.

1. Turn on the **Parrot Security** virtual machine. 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.

2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.

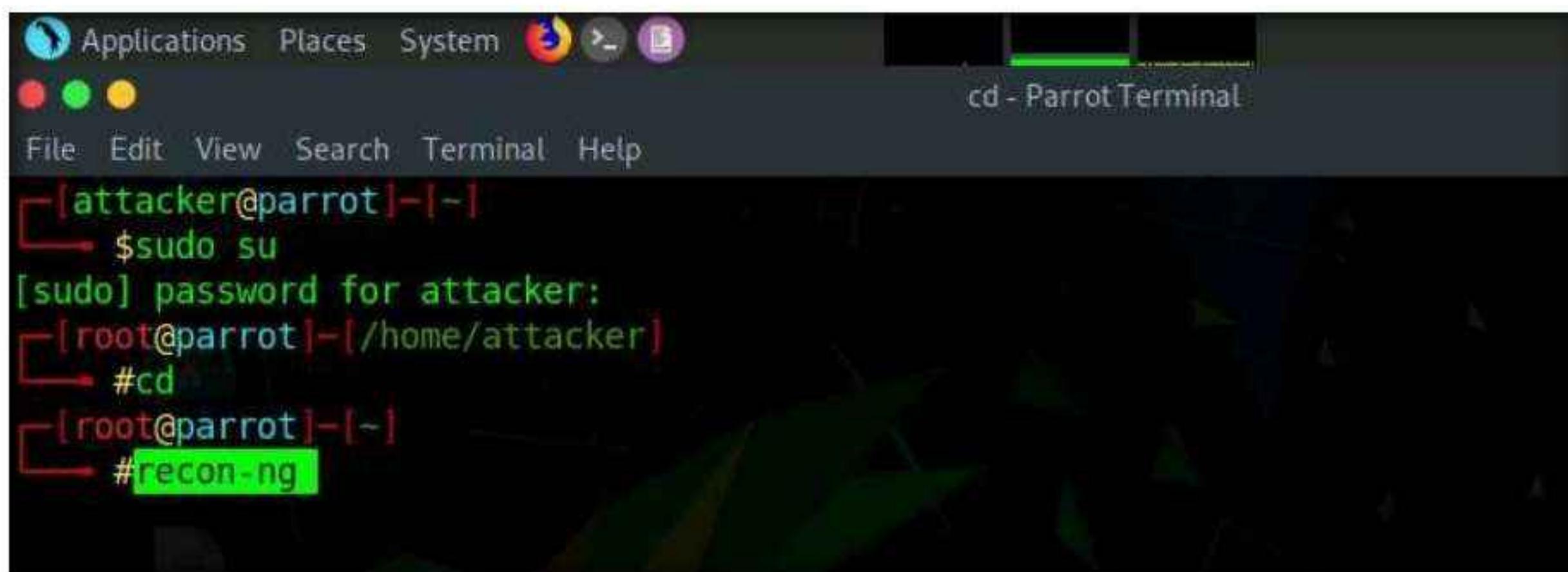
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

4. 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.

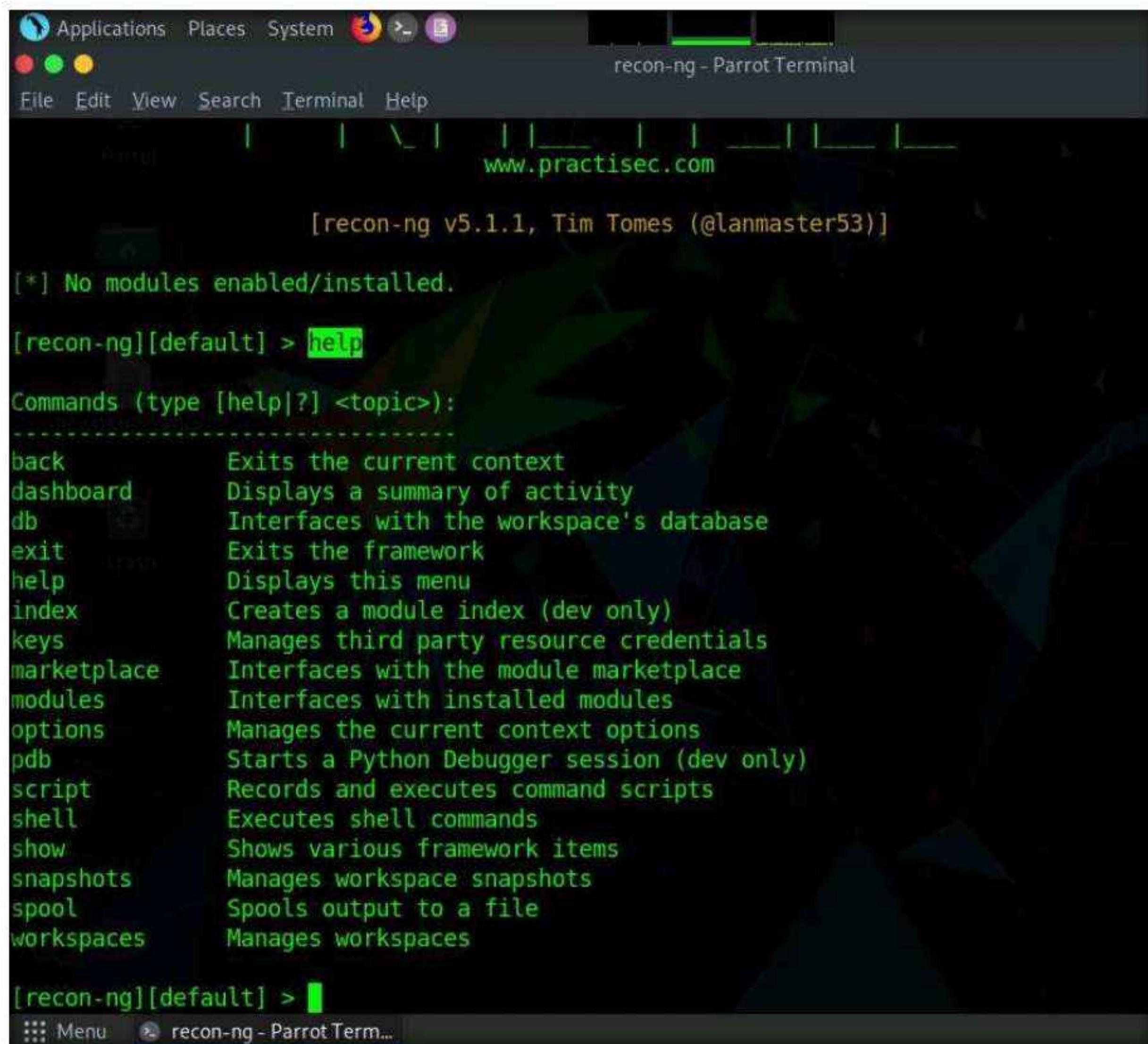
5. Now, type **cd** and press **Enter** to jump to the root directory.

6. In the **Terminal** window, type the command **recon-ng** and press **Enter** to launch the application.



```
[attacker@parrot] -[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] -[/home/attacker]
└─# cd
[root@parrot] -[~]
└─# recon-ng
```

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



```
[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]
```

[\*] No modules enabled/installed.

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

Commands (type [help|?] <topic>):

```
-----
```

back	Exits the current context
dashboard	Displays a summary of activity
db	Interfaces with the workspace's database
exit	Exits the framework
help	Displays this menu
index	Creates a module index (dev only)
keys	Manages third party resource credentials
marketplace	Interfaces with the module marketplace
modules	Interfaces with installed modules
options	Manages the current context options
pdb	Starts a Python Debugger session (dev only)
script	Records and executes command scripts
shell	Executes shell commands
show	Shows various framework items
snapshots	Manages workspace snapshots
spool	Spools output to a file
workspaces	Manages workspaces

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

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

**Note:** Ignore the errors while running the command.

```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
```

9. After the installation of modules, type the **modules search** command and press **Enter**. This displays all the modules available in recon-ng.

```
[recon-ng][default] > modules search
Discovery
-----
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files

Exploitation
-----
exploitation/injection/command_injector
exploitation/injection/xpath_bruter

Import
-----
import/csv_file
import/list
import/masscan
import/nmap

Recon
-----
recon/companies-contacts/bing_linkedin_cache
recon/companies-contacts/pen
recon/companies-domains/pen
recon/companies-domains/viewdns_reverse_whois
recon/companies-domains/whoxy_dns
recon/companies-multi/github_miner
recon/companies-multi/shodan_org
recon/companies-multi/whois_miner
recon/contacts-contacts/abc
```

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

The screenshot shows a terminal window with the title 'recon-ng - Parrot Terminal'. The window contains the following text:

```
File Edit View Search Terminal Help
recon/ports-hosts/ssl_scan
recon/profiles-contacts/bing_linkedin_contacts
recon/profiles-contacts/dev_diver
recon/profiles-contacts/github_users
recon/profiles-profiles/namechk
recon/profiles-profiles/profiler
recon/profiles-profiles/twitter_mentioned
recon/profiles-profiles/twitter_mentions
recon/profiles-repositories/github_repos
recon/repositories-profiles/github_commits
recon/repositories-vulnerabilities/gists_search
recon/repositories-vulnerabilities/github_dorks

Reporting
-----
reporting/csv
reporting/html
reporting/json
reporting/list
reporting/proxifier
reporting/pushpin
reporting/xlsx
reporting/xml

[recon-ng][default] > workspaces
Manages workspaces

Usage: workspaces <create|list|load|remove> [...]
```

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

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

```
[recon-ng][default] > workspaces create CEH
[!] 'bing_api' key not set. bing_linkedin cache module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email address' disabled. Dependency required: 'censys'.
[!] Module 'recon/companies-domains/censys_subdomains' disabled. Dependency required: 'censys'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-hosts/censys_org' disabled. Dependency required: 'censys'.
[!] Module 'recon/companies-hosts/censys_tls_subjects' disabled. Dependency required: 'censys'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'hipp_api' key not set. hipp_breach module will likely fail at runtime. See 'keys add'.
[!] 'hipp_api' key not set. hipp_paste module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-companies/censys_companies' disabled. Dependency required: 'censys'.
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: 'PyPDF3'.
[!] Module 'recon/domains-credentials/pwnedlist/account_creds' disabled. Dependency required: 'pyaes'.
[!] 'pwnedlist_api' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-credentials/pwnedlist/domain_creds' disabled. Dependency required: 'pyaes'.
[!] 'pwnedlist_api' key not set. domain_ispwned module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. domain_ispwned module will likely fail at runtime. See 'keys add'
```

14. 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.

```
[recon-ng][CEH] > workspaces list
+-----+
| Workspaces | Modified       |
+-----+
| CEH        | 2022-03-21 01:30:48 |
| default    | 2022-03-21 01:23:19 |
+-----+
```

15. Add a domain in which you want to perform network reconnaissance.
16. Type the command **db insert domains** and press **Enter**.
17. 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.
18. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal displays the following commands and their outputs:

```
[recon-ng] [CEH] > workspaces list
+-----+
| Workspaces | Modified |
+-----+
| CEH        | 2022-03-21 01:30:48 |
| default    | 2022-03-21 01:23:19 |
+-----+
[recon-ng][CEH] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains
+-----+
| rowid | domain      | notes | module   |
+-----+
| 1     | certifiedhacker.com | user_defined | 
+-----+
[*] 1 rows returned
[recon-ng][CEH] >
```

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

```
Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
| CEH | 2022-03-21 01:30:48 |
| default | 2022-03-21 01:23:19 |
+-----+
[recon-ng][CEH] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
(*) 1 rows affected.
[recon-ng][CEH] > show domains

+-----+
| rowid | domain | notes | module |
+-----+
| 1 | certifiedhacker.com | user_defined |
+-----+
[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
-----
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS

[recon-ng][CEH] >
```

21. To load the **recon/domains-hosts/brute\_hosts** module, type the **modules load recon/domains-hosts/brute\_hosts** command and press **Enter**.

```
Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS

[recon-ng][CEH] > show domains

+-----+
| rowid | domain | notes | module |
+-----+
| 1 | certifiedhacker.com | user_defined |
+-----+
[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
-----
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS

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

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

```
Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
Recon
-----
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS

[recon-ng][CEH] > modules load recon/domains-hosts/brute_HOSTS
[recon-ng][CEH][brute_HOSTS] > run

CERTIFIEDHACKER.COM
[*] No Wildcard DNS entry found.
01.certifiedhacker.com => No record found.
0.certifiedhacker.com => No record found.
1.certifiedhacker.com => No record found.
10.certifiedhacker.com => No record found.
14.certifiedhacker.com => No record found.
12.certifiedhacker.com => No record found.
13.certifiedhacker.com => No record found.
03.certifiedhacker.com => No record found.
02.certifiedhacker.com => No record found.
16.certifiedhacker.com => No record found.
19.certifiedhacker.com => No record found.
11.certifiedhacker.com => No record found.
2.certifiedhacker.com => No record found.
17.certifiedhacker.com => No record found.
15.certifiedhacker.com => No record found.
18.certifiedhacker.com => No record found.
20.certifiedhacker.com => No record found.
4.certifiedhacker.com => No record found.

[recon-ng][CEH][brute_HOSTS] >
```

23. Observe that hosts have been added by running the **recon/domains-hosts/brute\_HOSTS** module.

```
Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
wyoming.certifiedhacker.com => No record found.
wy.certifiedhacker.com => No record found.
xmail.certifiedhacker.com => No record found.
x-ray.certifiedhacker.com => No record found.
xp.certifiedhacker.com => No record found.
xi.certifiedhacker.com => No record found.
ye.certifiedhacker.com => No record found.
yankee.certifiedhacker.com => No record found.
y.certifiedhacker.com => No record found.
yu.certifiedhacker.com => No record found.
yt.certifiedhacker.com => No record found.
yellow.certifiedhacker.com => No record found.
z.certifiedhacker.com => No record found.
xml.certifiedhacker.com => No record found.
zera.certifiedhacker.com => No record found.
young.certifiedhacker.com => No record found.
zeus.certifiedhacker.com => No record found.
zlog.certifiedhacker.com => No record found.
za.certifiedhacker.com => No record found.
zebra.certifiedhacker.com => No record found.
z-log.certifiedhacker.com => No record found.
zm.certifiedhacker.com => No record found.
zulu.certifiedhacker.com => No record found.
zw.certifiedhacker.com => No record found.

-----
SUMMARY
-----
[*] 22 total (19 new) hosts found.
[recon-ng][CEH][brute_HOSTS] >
```

24. 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.

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

- **back**
- **modules load recon/domains-hosts/bing\_domain\_web**
- **run**

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

26. Type **modules load reverse\_resolve** command and press **Enter** to view all the modules associated with the reverse\_resolve keyword. In this task, we will be using the **recon/hosts-hosts/reverse\_resolve** module.

27. Type the **modules load recon/hosts-hosts/reverse\_resolve** command and press **Enter** to load the module.

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal displays the following text:

```
[*] yu.certifiedhacker.com => No record found.  
[*] yt.certifiedhacker.com => No record found.  
[*] yellow.certifiedhacker.com => No record found.  
[*] z.certifiedhacker.com => No record found.  
[*] xml.certifiedhacker.com => No record found.  
[*] zera.certifiedhacker.com => No record found.  
[*] young.certifiedhacker.com => No record found.  
[*] zeus.certifiedhacker.com => No record found.  
[*] zlog.certifiedhacker.com => No record found.  
[*] za.certifiedhacker.com => No record found.  
[*] zebra.certifiedhacker.com => No record found.  
[*] z-log.certifiedhacker.com => No record found.  
[*] zm.certifiedhacker.com => No record found.  
[*] zulu.certifiedhacker.com => No record found.  
[*] zw.certifiedhacker.com => No record found.  
  
-----  
SUMMARY  
----  
[*] 22 total (19 new) hosts found.  
[recon-ng][CEH][brute_hosts] > modules load reverse_resolve  
[*] Multiple modules match 'reverse_resolve'.  
  
Recon  
----  
recon/hosts-hosts/reverse_resolve  
recon/netblocks-hosts/reverse_resolve  
  
[recon-ng][CEH][brute_hosts] > modules load recon/hosts-hosts/reverse_resolve  
[recon-ng][CEH][reverse_resolve] >
```

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

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal output is as follows:

```
SUMMARY
[*] 22 total (19 new) hosts found.
[recon-ng][CEH][brute_hosts] > modules load reverse_resolve
[*] Multiple modules match 'reverse_resolve'.

Recon
-----
recon/hosts-hosts/reverse_resolve
recon/netblocks-hosts/reverse_resolve

[recon-ng][CEH][brute_hosts] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][CEH][reverse_resolve] > run
[*] Country: None
[*] Host: box5331.bluehost.com
[*] Ip Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] 127.0.0.1 => No record found.

SUMMARY
[*] 1 total (1 new) hosts found.
[recon-ng][CEH][reverse_resolve] >
```

29. 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.

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal output is as follows:

```
SUMMARY
[*] 1 total (1 new) hosts found.
[recon-ng][CEH][reverse_resolve] > show hosts
+-----+
| rowid | host | ip_address | region | country | latitude | longitude |
| notes | module | | | | | |
+-----+
| 1 | autodiscover.certifiedhacker.com | 162.241.216.11 | | | | |
| | brute_hosts | | | | | |
| 2 | blog.certifiedhacker.com | 162.241.216.11 | | | |
| | brute_hosts | | | | | |
| 3 | events.certifiedhacker.com | 162.241.216.11 | | | |
| | brute_hosts | | | | | |
| 4 | certifiedhacker.com | | | | | |
| | brute_hosts | | | | | |
| 5 | ftp.certifiedhacker.com | | | | | |
| | brute_hosts | | | | | |
| 6 | imap.certifiedhacker.com | | | | | |
| | brute_hosts | | | | | |
| 7 | mail.certifiedhacker.com | | | | | |
| | brute_hosts | | | | | |
| 8 | | | | | | |
| | brute_hosts | | | | | |
| 9 | | | | | | |
| | brute_hosts | | | | | |

[recon-ng][CEH][reverse_resolve] >
```

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

```

Applications Places System
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
| 9 | imap.certifiedhacker.com | 162.241.216.11 |
| 10 | brute hosts |
| localhost.certifiedhacker.com | 127.0.0.1 |
| 11 | brute hosts |
| mail.certifiedhacker.com | 162.241.216.11 |
| 12 | brute hosts |
| news.certifiedhacker.com | 162.241.216.11 |
| 13 | brute hosts |
| pop.certifiedhacker.com | 162.241.216.11 |
| 14 | brute hosts |
| smtp.certifiedhacker.com | 162.241.216.11 |
| 15 | brute hosts |
| 16 | smtp.certifiedhacker.com | 162.241.216.11 |
| 17 | brute hosts |
| webmail.certifiedhacker.com | 162.241.216.11 |
| 18 | brute hosts |
| www.certifiedhacker.com | 162.241.216.11 |
| 19 | www.certifiedhacker.com | 162.241.216.11 |
| 20 | brute hosts |
| box5331.bluehost.com | 162.241.216.11 |
| reverse_resolve |
+-----+
[*] 20 rows returned
[recon-ng][CEH]> back
[recon-ng][CEH]>

```

31. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.

32. 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**.

33. Type the **modules load reporting/html** command and press **Enter**.

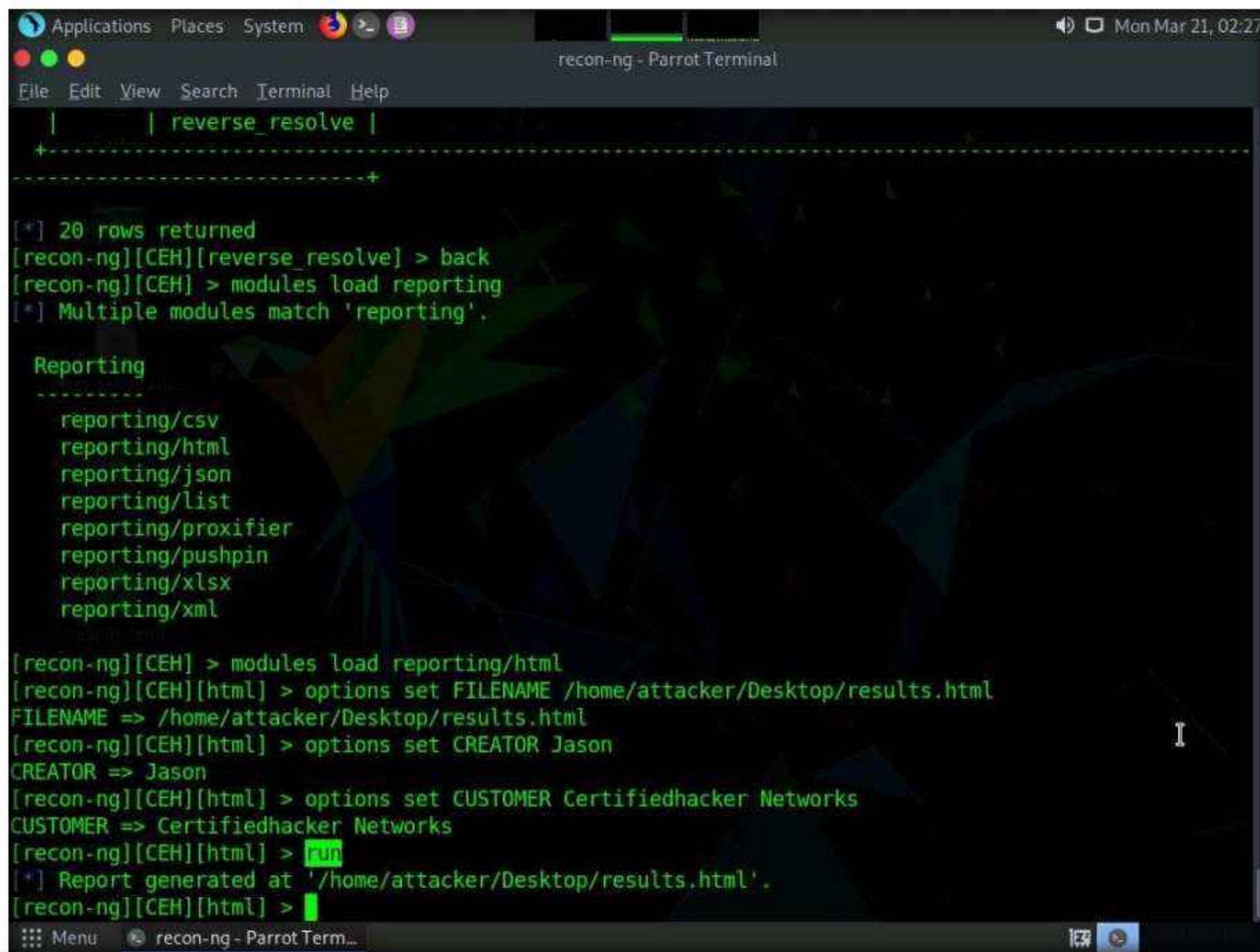
34. Observe that you need to assign values for **CREATOR** and **CUSTOMER** options while the **FILENAME** value is already set, and you may change the value if required.

35. Type:

- **options set FILENAME /home/attacker/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**.
- **options set CREATOR [your name]** (here, **Jason**) and press **Enter**.
- **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain) and press **Enter**.

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

## Module 02 – Footprinting and Reconnaissance



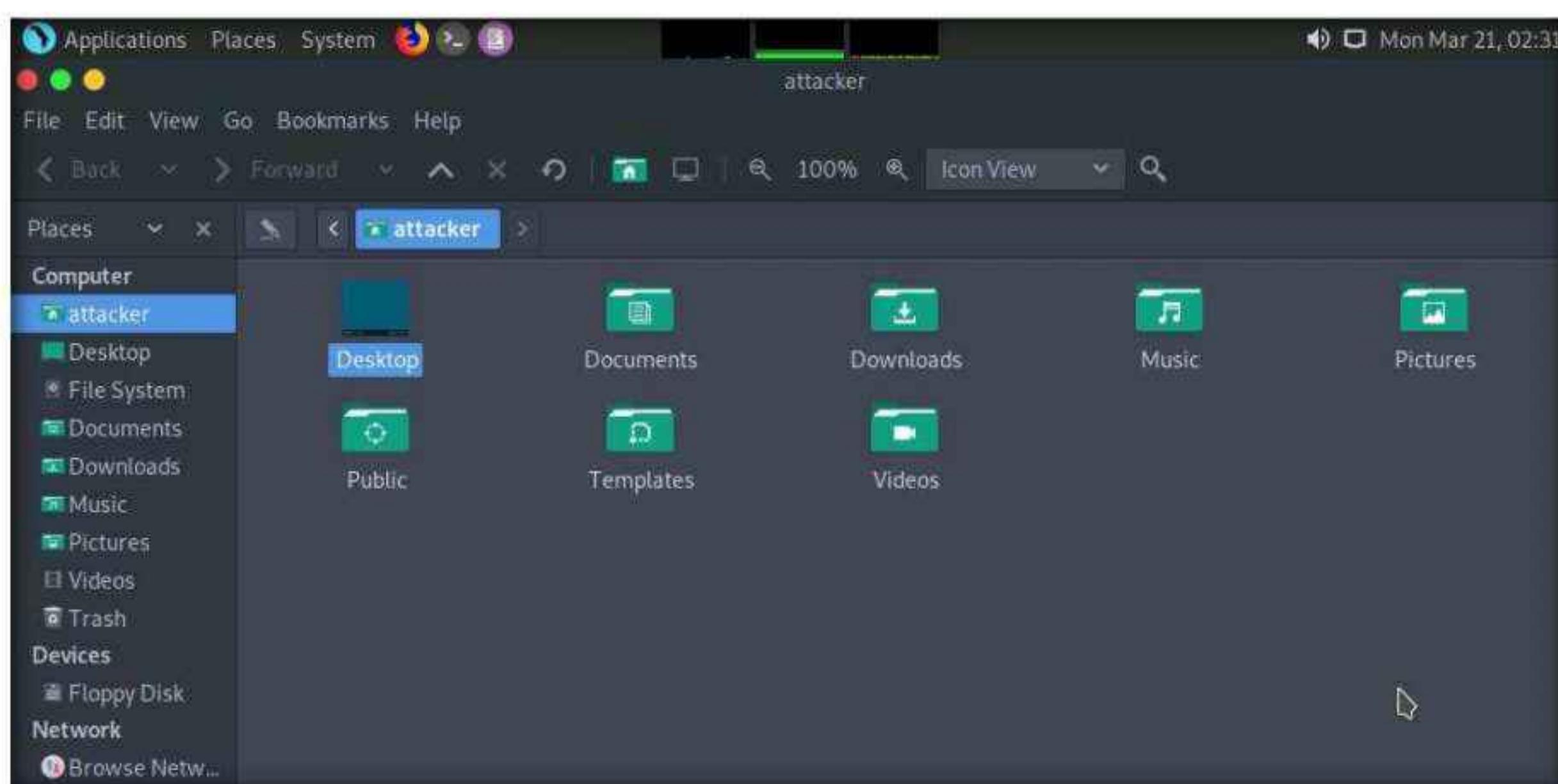
The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal output is as follows:

```
[*] 20 rows returned
[recon-ng][CEH][reverse_resolve] > back
[recon-ng][CEH] > modules load reporting
[*] Multiple modules match 'reporting'.

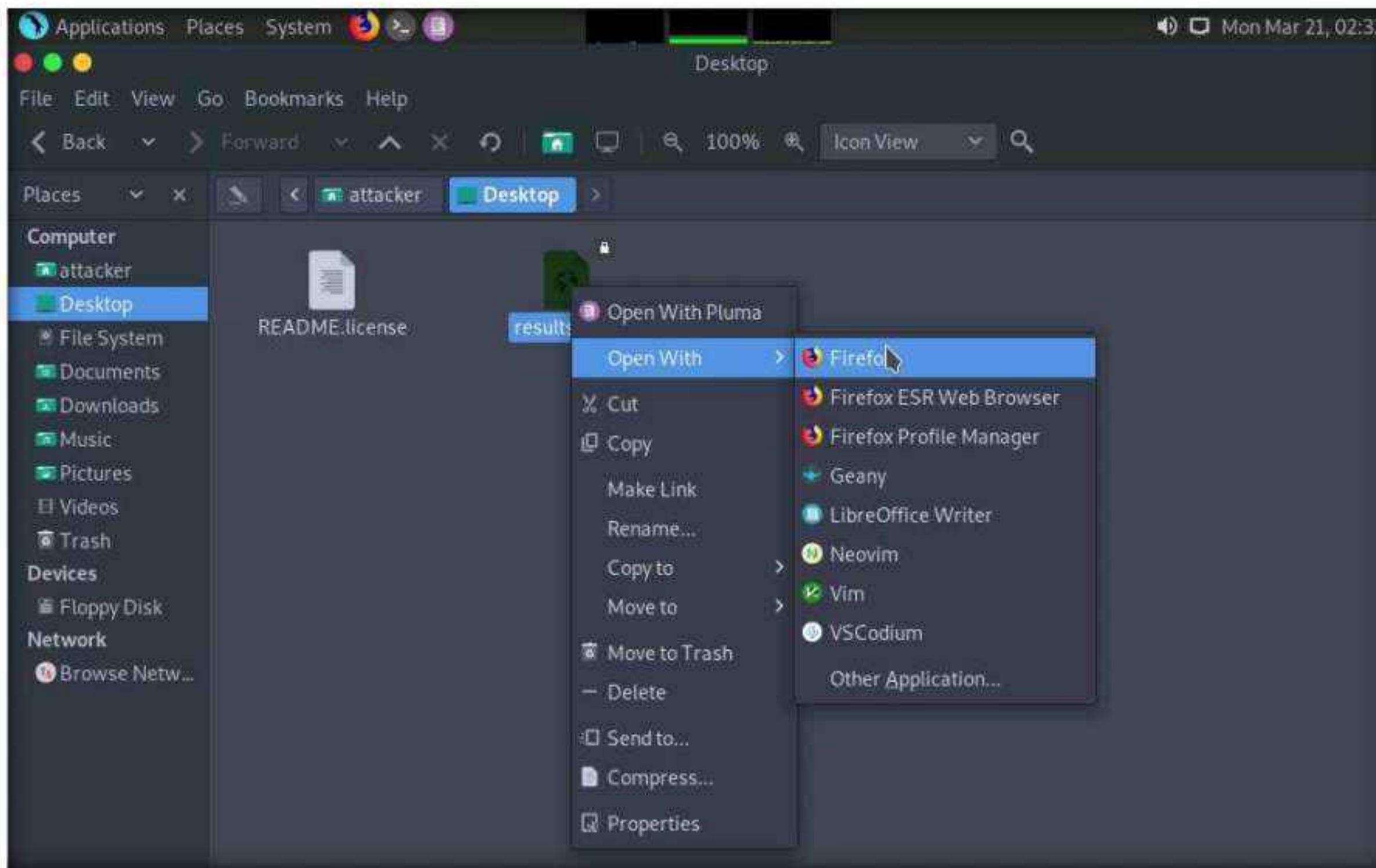
Reporting
-----
reporting/csv
reporting/html
reporting/json
reporting/list
reporting/proxifier
reporting/pushpin
reporting/xlsx
reporting/xml

[recon-ng][CEH] > modules load reporting/html
[recon-ng][CEH][html] > options set FILENAME /home/attacker/Desktop/results.html
FILENAME => /home/attacker/Desktop/results.html
[recon-ng][CEH][html] > options set CREATOR Jason
CREATOR => Jason
[recon-ng][CEH][html] > options set CUSTOMER Certifiedhacker Networks
CUSTOMER => Certifiedhacker Networks
[recon-ng][CEH][html] > run
[*] Report generated at '/home/attacker/Desktop/results.html'.
[recon-ng][CEH][html] >
```

37. The generated report is saved to **/home/attacker/Desktop/**.
38. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.
39. The **attacker** window appears.
40. In the **attacker** window, double-click **Desktop**.



41. Desktop window appears, right-click on the **results.html** file, click on **Open With**, and select the **Firefox** browser from the available options.



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

A screenshot of the Mozilla Firefox browser window titled "Recon-ng Reconnaissance Report - Mozilla Firefox". The address bar shows the URL "file:///home/attacker/Desktop/results.html". The main content area displays a "Certifiedhacker Networks" Recon-ng Reconnaissance Report. At the top, there is a summary table:

table	count
domains	1
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	20
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

Below the table are two expandable sections: "[+] Domains" and "[+] Hosts". At the bottom of the page, it says "Created by: Jason" and "Mon, Mar 21 2022 02:26:56".

## Module 02 – Footprinting and Reconnaissance

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

host	ip_address	region	country	latitude	longitude	notes	module
autodiscover.certifiedhacker.com	162.241.216.11						brute_hosts
blog.certifiedhacker.com	162.241.216.11						brute_hosts
box5331.bluehost.com	162.241.216.11						reverse_resolve
certifiedhacker.com							brute_hosts
events.certifiedhacker.com	162.241.216.11						brute_hosts
ftp.certifiedhacker.com							brute_hosts
ftp.certifiedhacker.com	162.241.216.11						brute_hosts
imap.certifiedhacker.com							brute_hosts
imap.certifiedhacker.com	162.241.216.11						brute_hosts
localhost.certifiedhacker.com	127.0.0.1						brute_hosts
mail.certifiedhacker.com							brute_hosts
mail.certifiedhacker.com	162.241.216.11						brute_hosts
news.certifiedhacker.com	162.241.216.11						brute_hosts
pop.certifiedhacker.com							brute_hosts
pop.certifiedhacker.com	162.241.216.11						brute_hosts
smtp.certifiedhacker.com							brute_hosts
smtp.certifiedhacker.com	162.241.216.11						brute_hosts
webmail.certifiedhacker.com	162.241.216.11						brute_hosts
www.certifiedhacker.com							brute_hosts
www.certifiedhacker.com	162.241.216.11						brute_hosts

Created by: Jason  
Mon, Mar 21 2022 02:26:56

44. Close all open windows.
45. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain
46. Now, we will use Recon-ng to gather personnel information.
47. Open a new **Parrot Terminal** window, In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
48. 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.
49. Now, type **cd** and press **Enter** to jump to the root directory.
50. Type **recon-ng**, and press **Enter**.

```
[attacker@parrot] ~
└─$ sudo su
[sudo] password for attacker:
[root@parrot] ~
└─# cd
[root@parrot] ~
└─# recon-ng
```

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

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The window contains the following text:

```
Sponsored by...
BLACK HILLS
www.blackhillsinfosec.com

PRACTISEC
www.practise.com

[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[84] Recon modules
[14] Disabled modules
[8] Reporting modules
[4] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] > workspaces create reconnaissance
```

52. Set a domain and perform footprinting on it to extract contacts available in the domain.
53. 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.
54. Type the **info command** and press **Enter** to view the options required to run this module.
55. 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.

```
[recon-ng][reconnaissance] > modules load recon/domains-contacts/whois_pocs
[recon-ng][reconnaissance][whois_pocs] > info command

    Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0

Description:
    Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
    'contacts' table with the results.

Options:
    Name      Current Value   Required   Description
    SOURCE    default        yes        source of input (see 'info' for details)

Source Options:
    default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>    string representing a single input
    <path>       path to a file containing a list of inputs
    query <sql>  database query returning one column of inputs

[recon-ng][reconnaissance][whois_pocs] > options set SOURCE facebook.com
[recon-ng][reconnaissance][whois_pocs] >
```

56. 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

```
FACEBOOK.COM
-----
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST1B4-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First_Name: Brandon
[*] Last_Name: Stout
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
[*] Title: Whois contact
[*]
```

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

```
Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First Name: Brandon
[*] Last Name: Stout
[*] Middle Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] -----
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First Name: None
[*] Last Name: Operations
[*] Middle Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
[*] Title: Whois contact
[*] -----
SUMMARY
[*] 2 total (2 new) contacts found.
[recon-ng][reconnaissance][whois_pocs] > back
[recon-ng][reconnaissance] >
```

58. Until now, we have obtained contacts related to the domains. Note down these contacts' names.
59. Now, we will validate the existence of names (usernames) on specific websites.
60. 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**.
61. Type the **modules load recon/profiles-profiles/namechk** command and press **Enter** to load this module.
62. 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.
63. Type **run** and press **Enter**. This begins the search for the keyword MarkZuckerberg on various websites.
64. 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!**”. Here, no results are obtained.

## Module 02 – Footprinting and Reconnaissance

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal displays footprinting results for two contacts. The first contact is "MarkZuckerberg" with the following details:

- First Name: Brandon
- Last Name: Stout
- Middle Name: None
- Notes: None
- Phone: None
- Region: Chicago, IL
- Title: Whois contact

The second contact is also "MarkZuckerberg" with the following details:

- URL: <http://whois.arin.net/rest/poc/OPERA82-ARIN>
- Country: United States
- Email: domain@facebook.com
- First Name: None
- Last Name: Operations
- Middle Name: None
- Notes: None
- Phone: None
- Region: Menlo Park, CA
- Title: Whois contact

At the bottom of the terminal, there is a "SUMMARY" section:

- 2 total (2 new) contacts found.

The command history at the bottom shows the following steps:

```
[*] [recon-ng][reconnaissance][whois_pocs] > back
[*] [recon-ng][reconnaissance] > modules load recon/profiles-profiles/namechk
[*] [recon-ng][reconnaissance][namechk] > options set SOURCE MarkZuckerberg
[*] SOURCE => MarkZuckerberg
[*] [recon-ng][reconnaissance][namechk] > run
[*] [recon-ng][reconnaissance][namechk] > F
```

65. Type the **back** command and press **Enter** to go back to the workspaces (reconnaissance) terminal.
66. To find the existence of user-profiles on various websites, you need to load the **recon/profiles-profiles/profiler** module.
67. Type the **modules load recon/profiles-profiles/profiler** command and press **Enter**.
68. Type the **options set SOURCE MarkZuckerberg** command and press **Enter**.
69. 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 any errors received in the results.

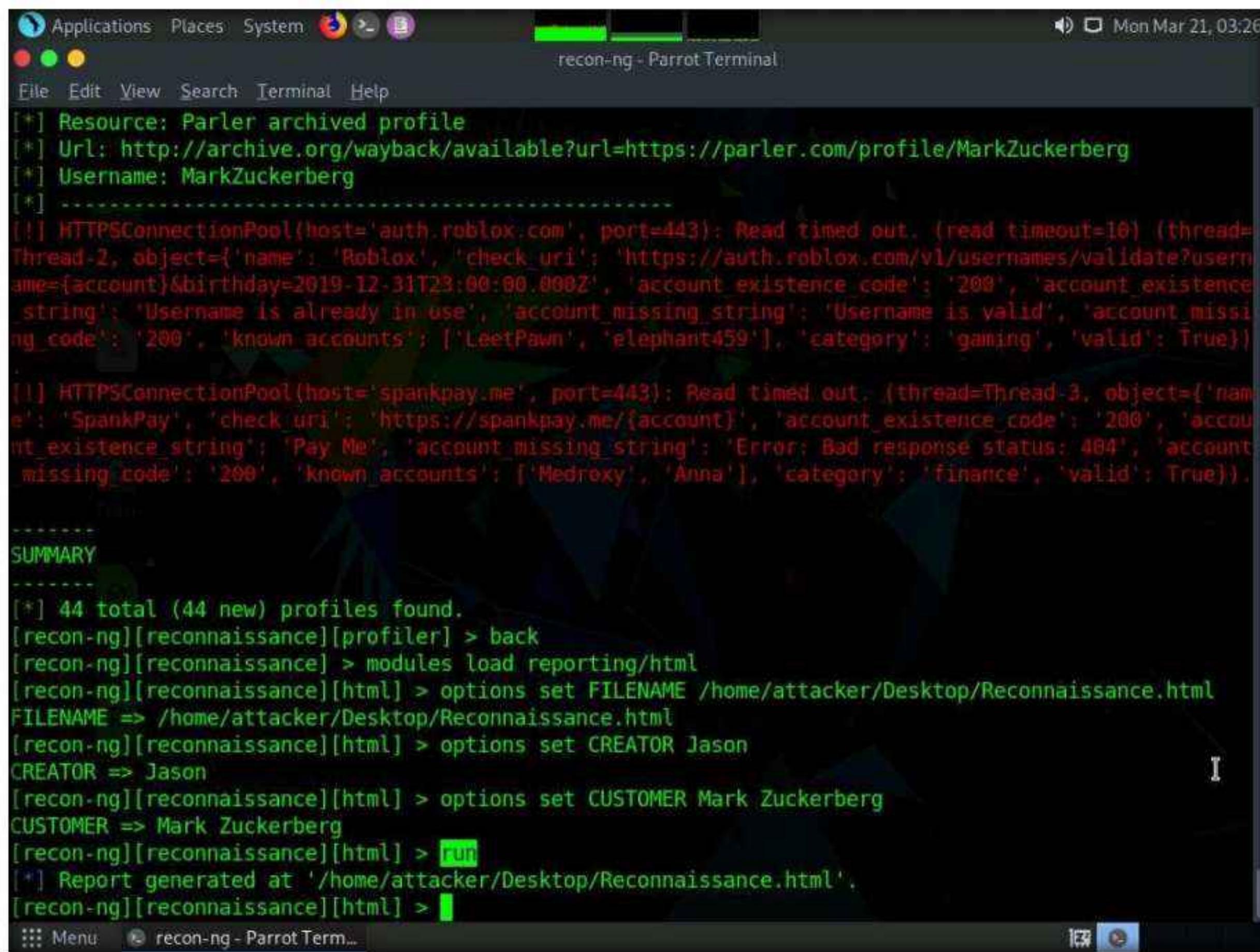
**Note:** The results might differ when you perform this task.

```
[recon-ng][reconnaissance][namechk]> back
[recon-ng][reconnaissance] > modules load recon/profiles/profiler
[recon-ng][reconnaissance][profiler] > options set SOURCE MarkZuckerberg
SOURCE => MarkZuckerberg
[recon-ng][reconnaissance][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.json
...
Looking Up Data For: Markzuckerberg
-----
[*] Checking: 7cup
[*] Checking: Artists & Clients
[*] Checking: Ameblo
[*] Checking: Aminoapps
[*] Checking: Anilist
[*] Checking: AnimePlanet
[*] Checking: Apex Legends
[*] Checking: asciinema
[*] Checking: Audiojungle
[*] Checking: Avid Community
[!] ('Connection aborted.', ConnectionResetError(104, 'Connection reset by peer')) (thread=Thread-7,
object={'name': 'Apex Legends', 'check url': 'https://apex.tracker.gg/apex/profile/origin/{account}/overview', 'account existence code': '200', 'account existence string': 'Overview', 'account missing code': '404', 'account missing string': 'PLAYER NOT FOUND', 'known accounts': ['tttcheekyttt', 'RollsRoyce_Dawn'], 'category': 'gaming', 'valid': True})
[*] Checking: Bookcrossing
[*] Checking: buymeacoffee
[*] Checking: carrd.co
[*] Checking: CastingCallClub
[*] Checking: championat
...
Menu  recon-ng - Parrot Term...
```

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

**Note:** In this task, we are saving the report in HTML format; therefore, **reporting/html** module is used.
73. Type:
  - **options set FILENAME /home/attacker/Desktop/Reconnaissance.html** and press **Enter**. By issuing this command, you are setting the report name as **Reconnaissance.html** and the path to store the file as **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**.
74. 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.

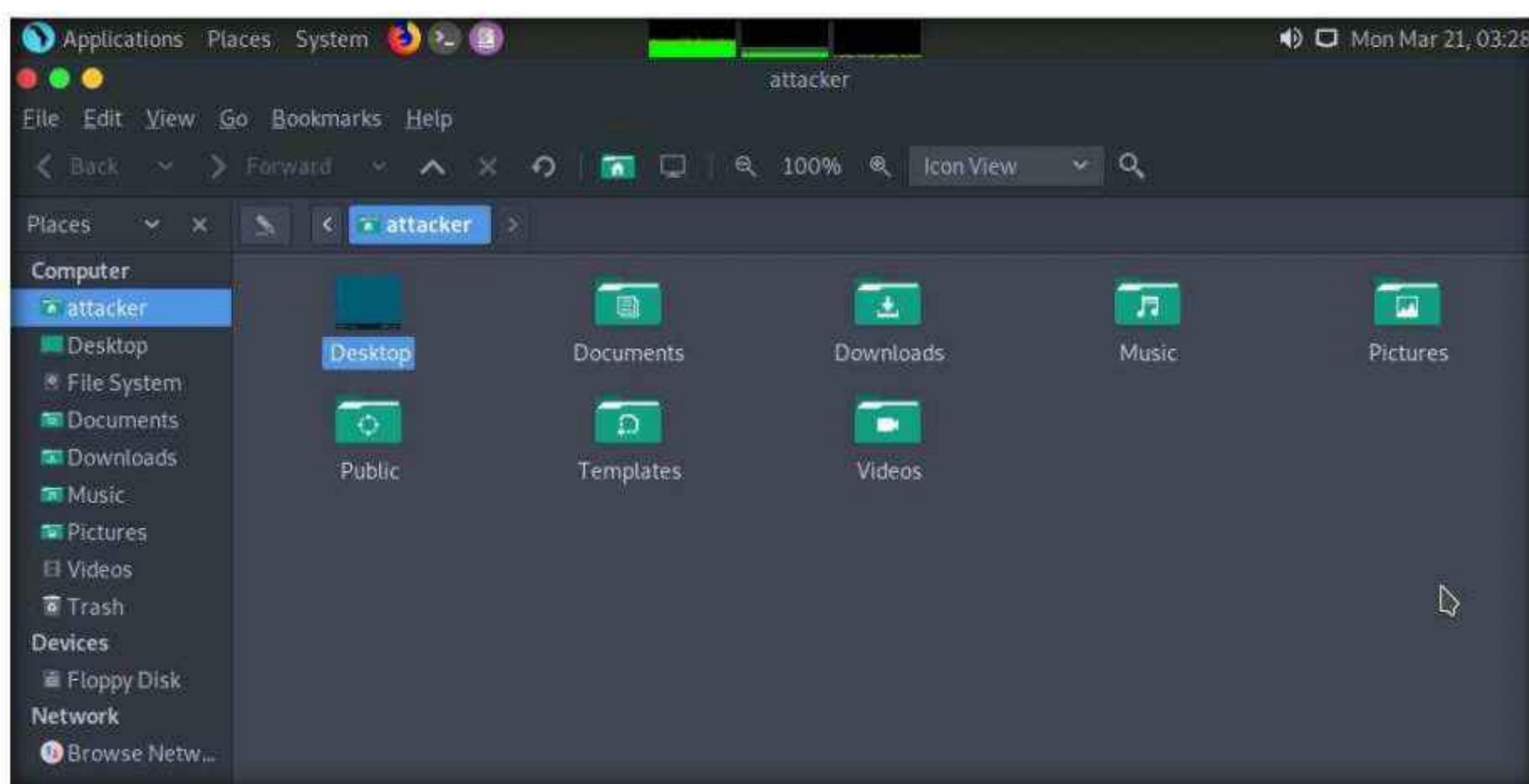
## Module 02 – Footprinting and Reconnaissance



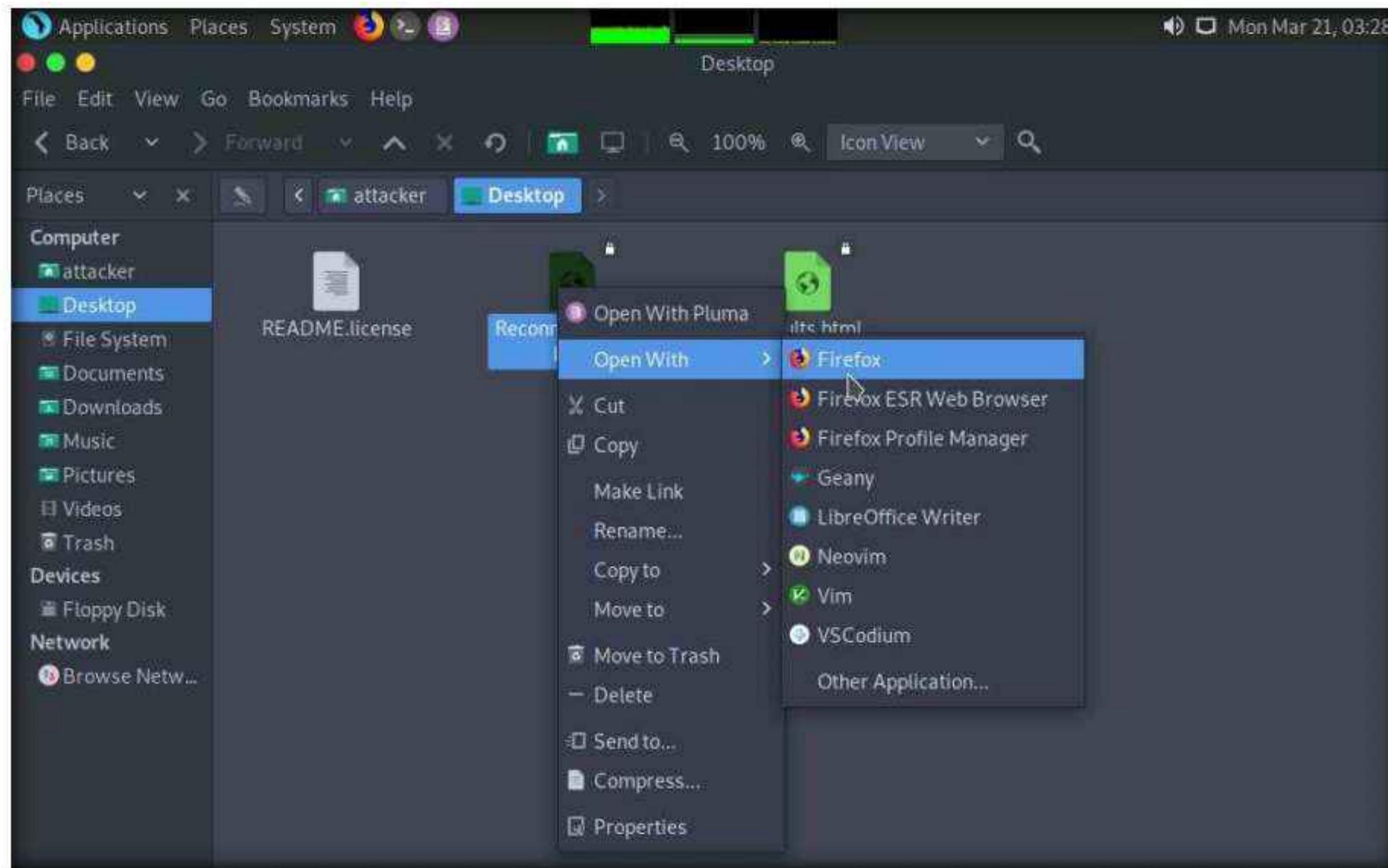
```
[*] Resource: Parler archived profile
[*] Url: http://archive.org/wayback/available?url=https://parler.com/profile/MarkZuckerberg
[*] Username: MarkZuckerberg
[*]
[*] HTTPSConnectionPool(host='auth.roblox.com', port=443): Read timed out. (read timeout=10) (thread=Thread-2, object={'name': 'Roblox', 'check_uri': 'https://auth.roblox.com/v1 usernames/validate?username={account}&birthday=2019-12-31T23:00:00.000Z', 'account_existence_code': '200', 'account_existence_string': 'Username is already in use', 'account_missing_string': 'Username is valid', 'account_missing_code': '200', 'known_accounts': ['LeetPawn', 'elephant459'], 'category': 'gaming', 'valid': True})
[*] HTTPSConnectionPool(host='spankpay.me', port=443): Read timed out. (thread=Thread-3, object={'name': 'SpankPay', 'check_uri': 'https://spankpay.me/{account}', 'account_existence_code': '200', 'account_existence_string': 'Pay Me', 'account_missing_string': 'Error: Bad response status: 404', 'account_missing_code': '200', 'known_accounts': ['Medroxy', 'Anna'], 'category': 'finance', 'valid': True})

-----  
SUMMARY  
-----  
[*] 44 total (44 new) profiles found.  
[recon-ng][reconnaissance][profiler] > back  
[recon-ng][reconnaissance] > modules load reporting/html  
[recon-ng][reconnaissance][html] > options set FILENAME /home/attacker/Desktop/Reconnaissance.html  
FILENAME => /home/attacker/Desktop/Reconnaissance.html  
[recon-ng][reconnaissance][html] > options set CREATOR Jason  
CREATOR => Jason  
[recon-ng][reconnaissance][html] > options set CUSTOMER Mark Zuckerberg  
CUSTOMER => Mark Zuckerberg  
[recon-ng][reconnaissance][html] > run  
[*] Report generated at '/home/attacker/Desktop/Reconnaissance.html'.  
[recon-ng][reconnaissance][html] >
```

75. The generated report is saved to **/home/attacker/Desktop/**.
76. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.
77. The **attacker** window appears.
78. In the **attacker** window, double-click **Desktop**.



79. Desktop window appears, right-click on the **Reconnaissance.html** file, click on **Open With**, and select the **Firefox** browser from the available options.



80. 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.

A screenshot of the Firefox web browser. The title bar says 'Recon-ng Reconnaissance Report - Mozilla Firefox'. The address bar shows the URL 'file:///home/attacker/Desktop/Reconnaissance.html'. The main content area displays the 'Recon-ng Reconnaissance Report' for 'Mark Zuckerberg'. At the top, it says 'Recon-ng Reconnaissance Report'. Below that is a table titled '[+] Summary' with columns 'table' and 'count'. The data in the table is as follows:

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	0
contacts	2
credentials	0
leaks	0
pushpins	0
profiles	44
repositories	0

[+] Contacts

[+] Profiles

Created by: Jason  
Mon, Mar 21 2022 03:26:13

## Module 02 – Footprinting and Reconnaissance

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

**Note:** To view detailed information about **Profiles** in the report scroll to the right.

The screenshot shows two Firefox browser windows displaying the Recon-ng Reconnaissance Report. The top window shows the main statistics table and the 'Contacts' section. The bottom window shows the 'Profiles' section.

**Statistics Table:**

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	0
contacts	2
credentials	0
leaks	0
pushpins	0
profiles	44
repositories	0

**[+] Contacts**

first_name	middle_name	last_name	email	title	region	country	phone	notes	module
Brandon		Stout	bstout@facebook.com	Whois contact	Menlo Park, CA	United States			whois_pocs
				Whois contact	Chicago, IL	United States			whois_pocs

**[+] Profiles**

Created by: Jason  
Mon, Mar 21 2022 03:26:13

**[+] Profiles**

username	resource
MarkZuckerberg	7cup: https://www.7cups.com/@MarkZuckerberg
MarkZuckerberg	Linktree: https://linktr.ee/MarkZuckerberg
MarkZuckerberg	Kickstarter: https://www.kickstarter.com/profile/MarkZuckerberg
MarkZuckerberg	MyAnimeList: https://myanimelist.net/profile/MarkZuckerberg
MarkZuckerberg	about.me: https://about.me/MarkZuckerberg
MarkZuckerberg	Behance: https://www.behance.net/MarkZuckerberg
MarkZuckerberg	Bandlab: https://www.bandlab.com/api/v1.3/users/MarkZuckerberg
MarkZuckerberg	Bitbucket: https://bitbucket.org/MarkZuckerberg/
MarkZuckerberg	Blogspot: http://MarkZuckerberg.blogspot.com
MarkZuckerberg	BuzzFeed: https://www.buzzfeed.com/MarkZuckerberg
MarkZuckerberg	BodyBuilding.com: http://api.bodybuilding.com/api-proxy/bbc/get?slug=MarkZuckerberg
MarkZuckerberg	devRant: https://devrant.com/users/MarkZuckerberg
MarkZuckerberg	diigo: https://www.diigo.com/interact_api/load_profile_info?name=MarkZuckerberg
MarkZuckerberg	F3: https://f3.cool/MarkZuckerberg
MarkZuckerberg	Fodors Forum: https://www.fodors.com/community/profile/MarkZuckerberg/forum-activity
MarkZuckerberg	Flipboard: https://flipboard.com/@MarkZuckerberg
MarkZuckerberg	FurAffinity: https://www.furaffinity.net/user/MarkZuckerberg
MarkZuckerberg	Geocaching: https://www.geocaching.com/p/?u=MarkZuckerberg
MarkZuckerberg	Hacker News: https://news.ycombinator.com/user?id=MarkZuckerberg
MarkZuckerberg	imgur: https://api.imgur.com/account/v1/accounts/MarkZuckerberg?client_id=546c25a59c58ad7&include=trophies%2Cmedallions
MarkZuckerberg	InsaneJournal: https://MarkZuckerberg.insanejournal.com/profile
MarkZuckerberg	Keybase: https://keybase.io/MarkZuckerberg

82. We have now gathered information about the employee working in a target organization. Close all the open windows.

83. Now, we will use Recon-*ng* to extract a list of subdomains and IP addresses associated with the target URL.
84. Open a new **Parrot Terminal** window, In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
85. 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.
86. Now, type **cd** and press **Enter** to jump to the root directory.
87. Type **recon-*ng***, and press **Enter**.
88. To extract a list of subdomains and IP addresses associated with the target URL, we need to load the **recon/domains-hosts/hackertarget** module.
89. Type the **modules load recon/domains-hosts/hackertarget** command and press **Enter**.
90. Type the **options set SOURCE certifiedhacker.com** command and press **Enter**.
91. Type the **run** command and press **Enter**. The **recon/domains-hosts/hackertarget** module searches for list of subdomains and IP addresses associated with the target URL and returns the list of subdomains and their IP addresses.

```
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][hackertarget] > run

CERTIFIEDHACKER.COM
[*] Country: None
[*] Host: www.fleet.certifiedhacker.com
[*] Ip Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: iam.certifiedhacker.com
[*] Ip Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www.sftp.certifiedhacker.com
[*] Ip Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
::: Menu  recon-ng - Parrot Term...
```

92. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.
93. Close all open windows and document all the acquired information.

## Task 2: Footprinting a Target using Maltego

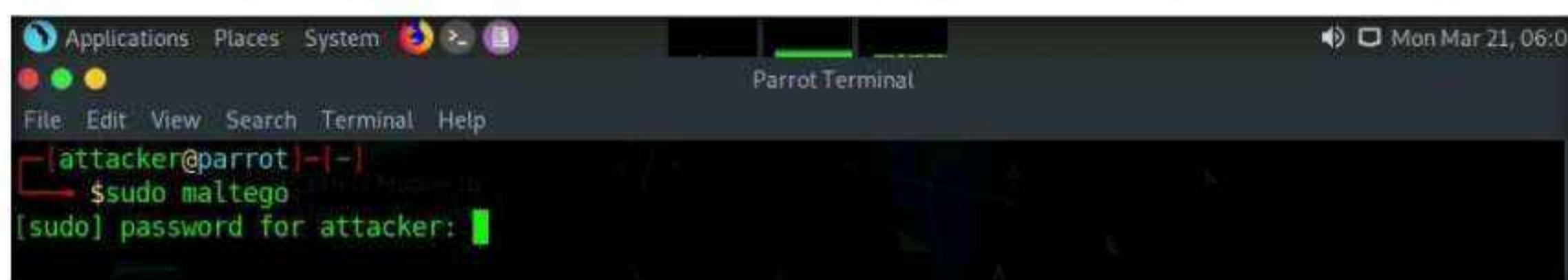
Maltego is a footprinting tool used to gather maximum information for the purpose of ethical hacking, computer forensics, and pentesting. It provides a library of transforms to discover data from open sources and visualizes that information in a graph format, suitable for link analysis and data mining. Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate, and even making it possible to see hidden connections.

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

**Note:** Here, we will consider [www.certifiedhacker.com](http://www.certifiedhacker.com) as a target website. However, you can select a target domain of your choice.

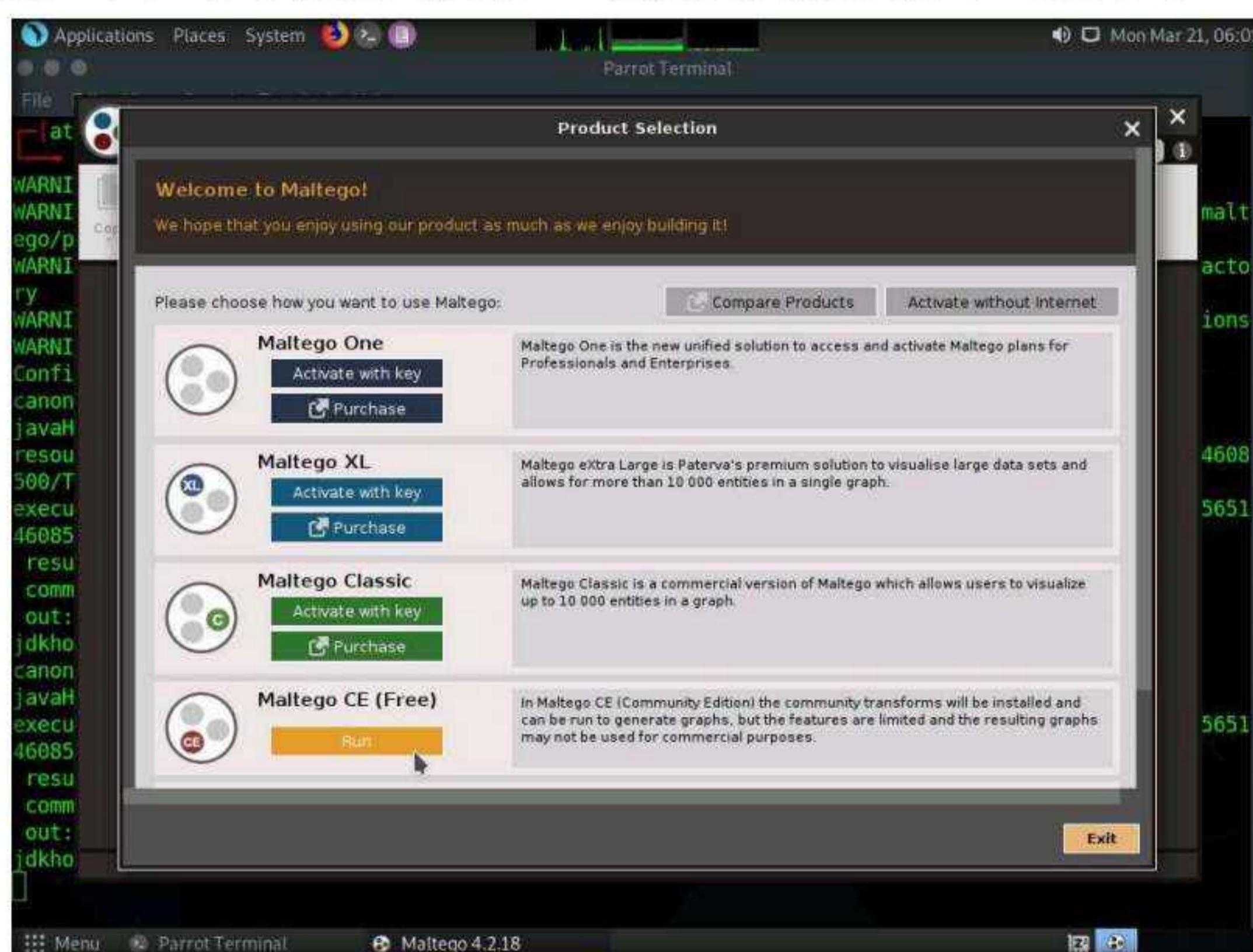
1. In the **Parrot Security** virtual machine, open a terminal and type **sudo maltego** and press **Enter** to launch Maltego.

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

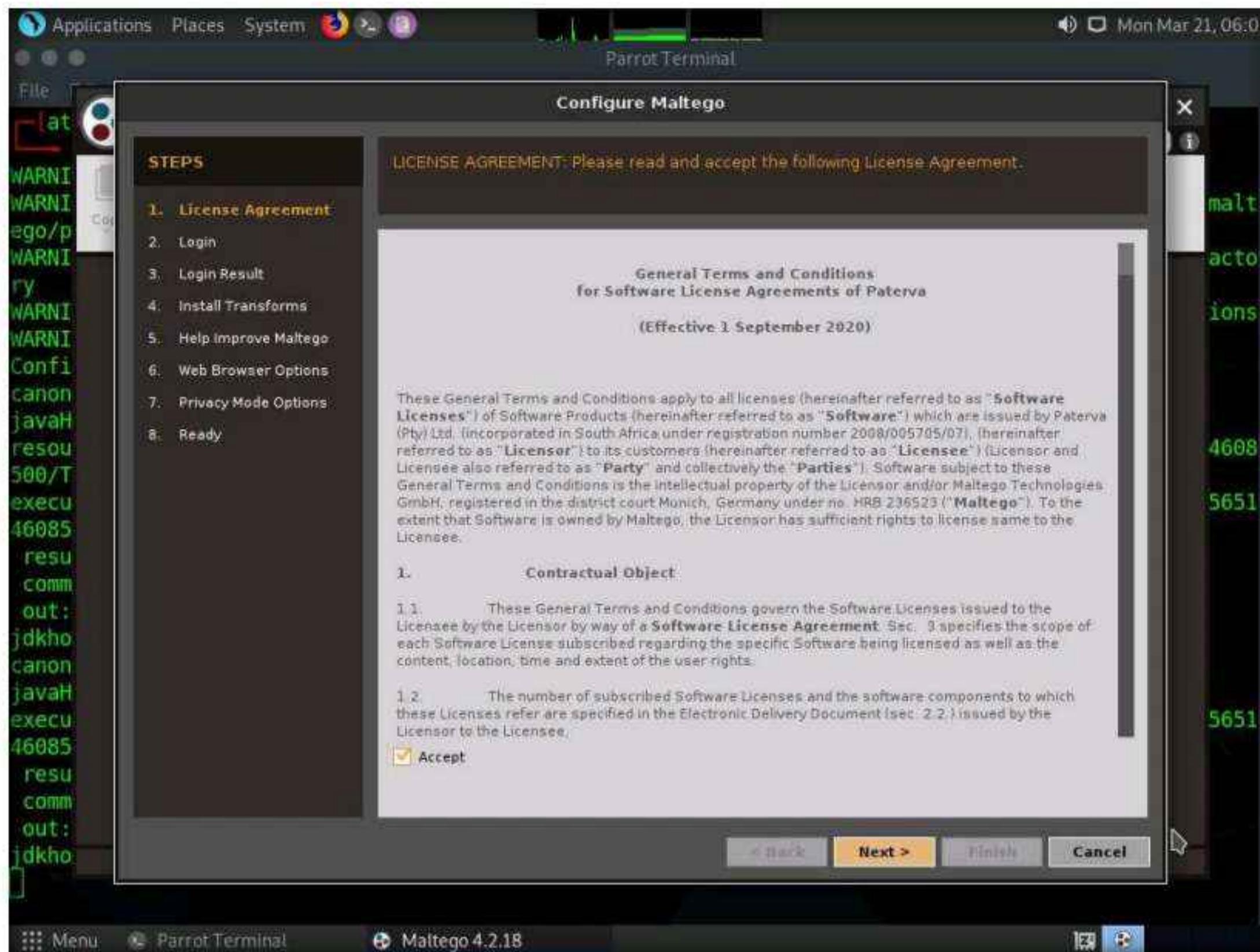


2. A **Product Selection** wizard appears on the Maltego GUI; click **Run** from **Maltego CE (Free)** option.

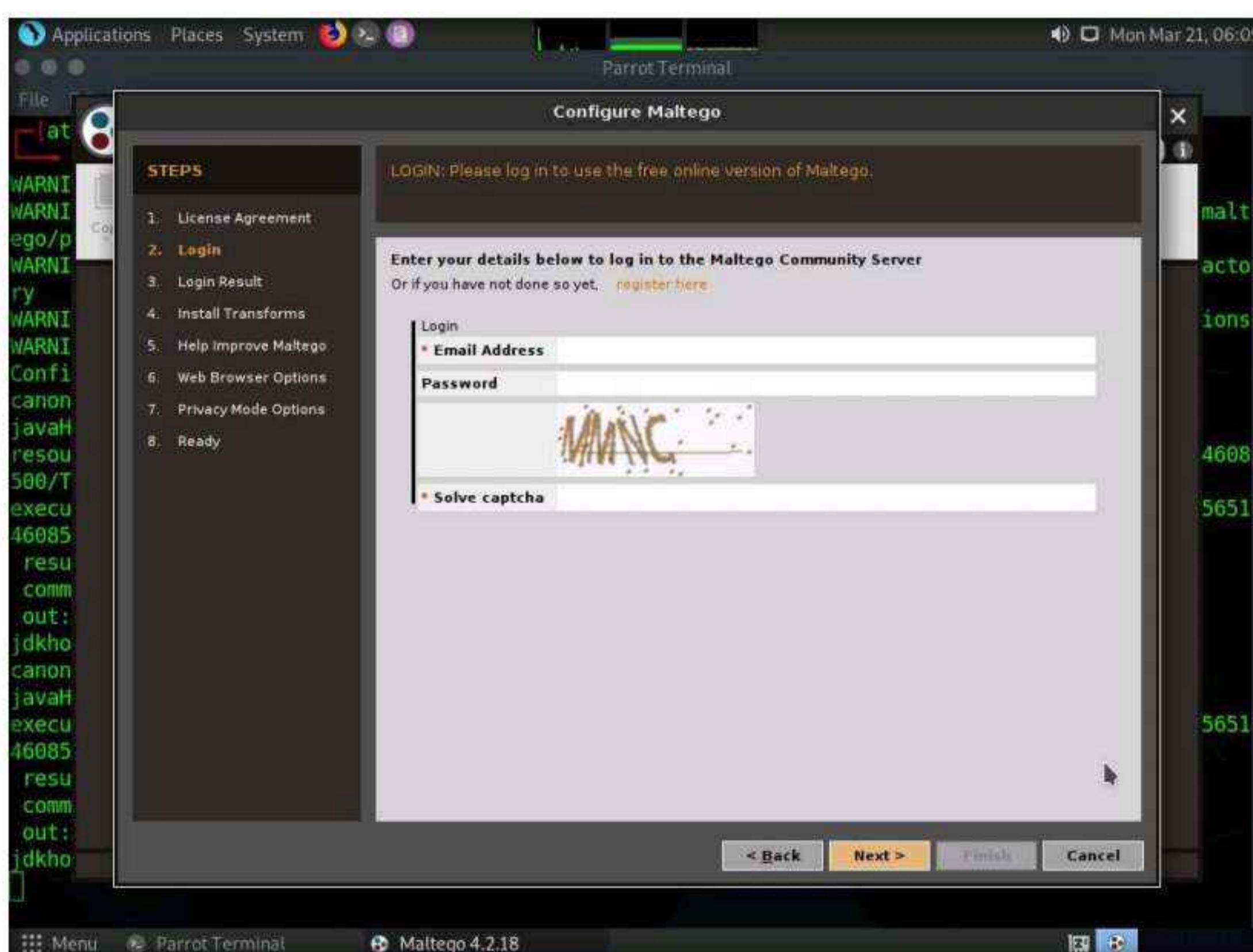
**Note:** If the **Memory Settings Optimized** pop-up appears, click **Restart Now**.



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

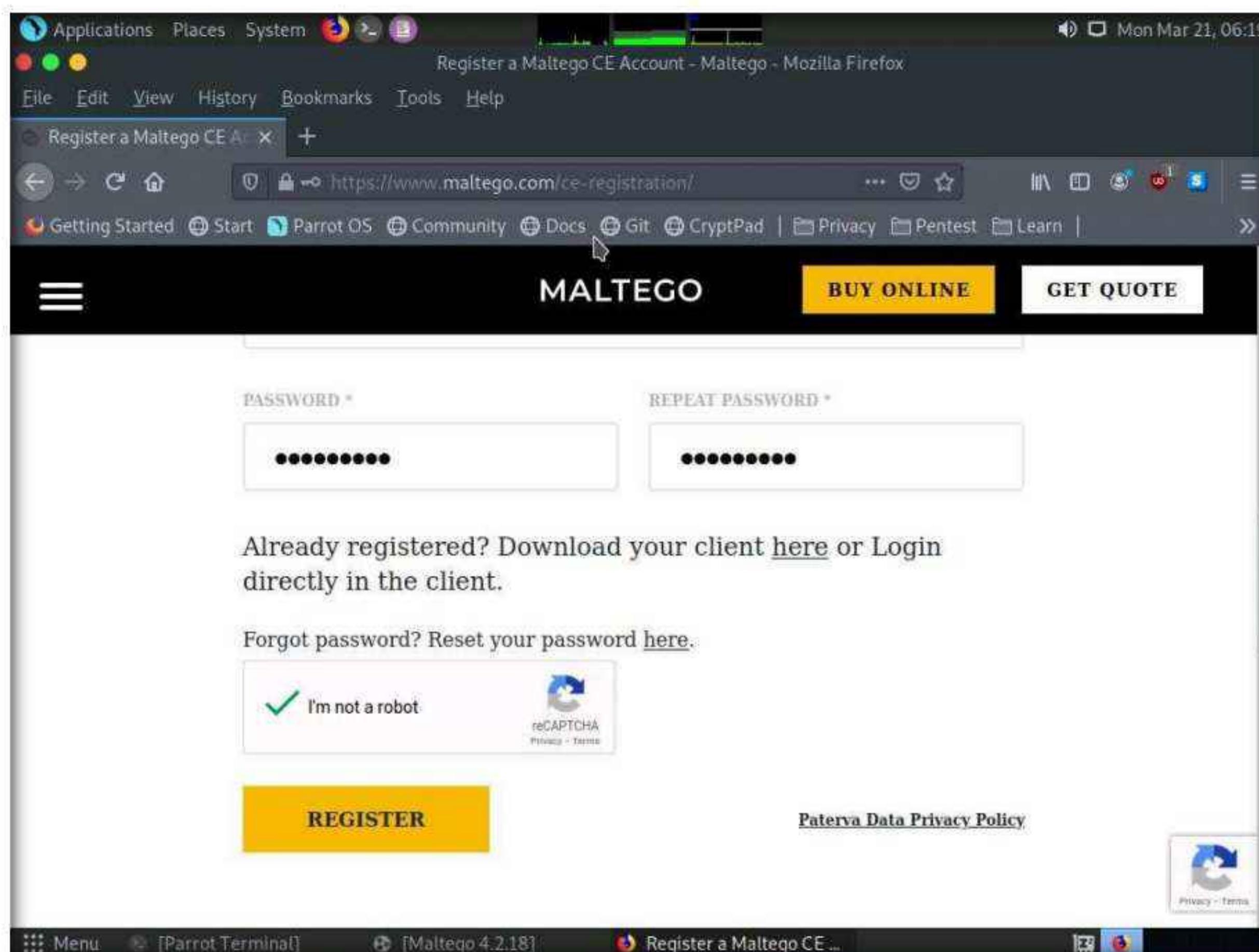


- You will be redirected to the **Login** section; leave the **Maltego** window as it is and click **Firefox** icon from the top-section of the window to launch the Firefox browser.



5. The **Firefox** window appears in the address type <https://www.maltego.com/ce-registration> and press **Enter**.
6. 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:** If cookie notification appears in the lower section of the browser, click **Accept**.

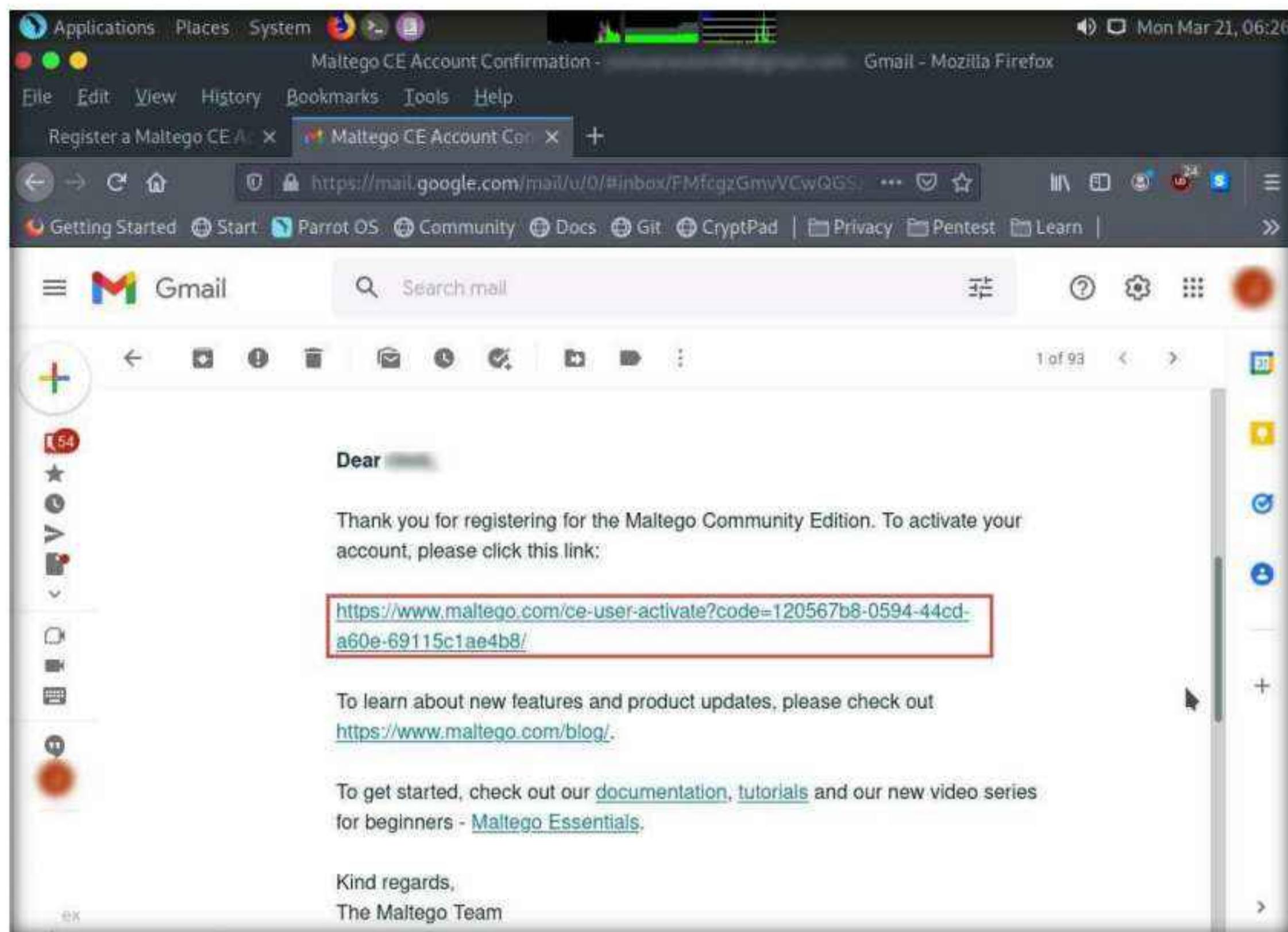


7. **Mail Sent!** notification appears, click **close** button.

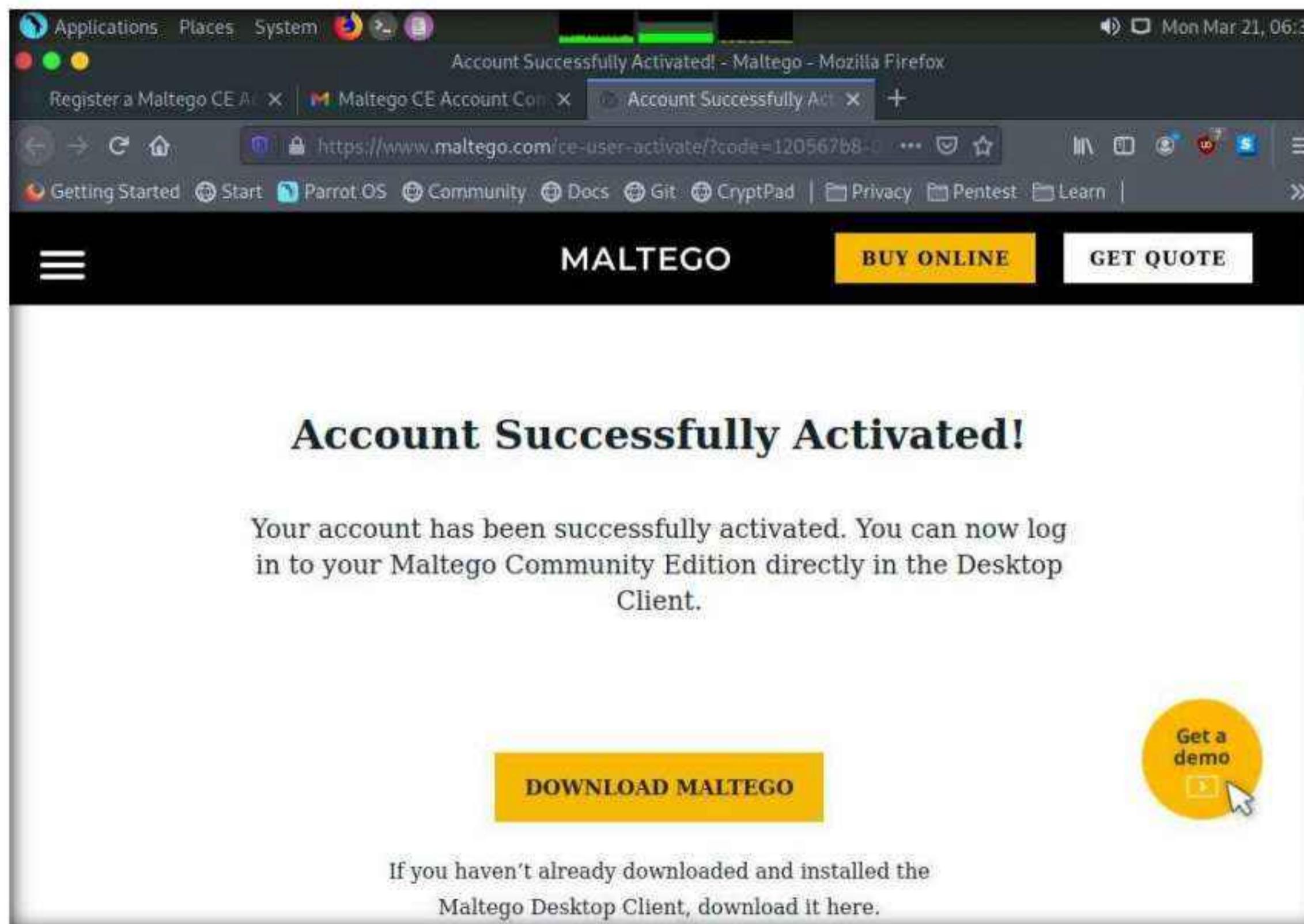


## Module 02 – Footprinting and Reconnaissance

- Now, in the browser window, click '+' icon to open a new tab. Open the email account given at the time of registration in **Step#6**. Open the mail from **Maltego** and click on the activation link.

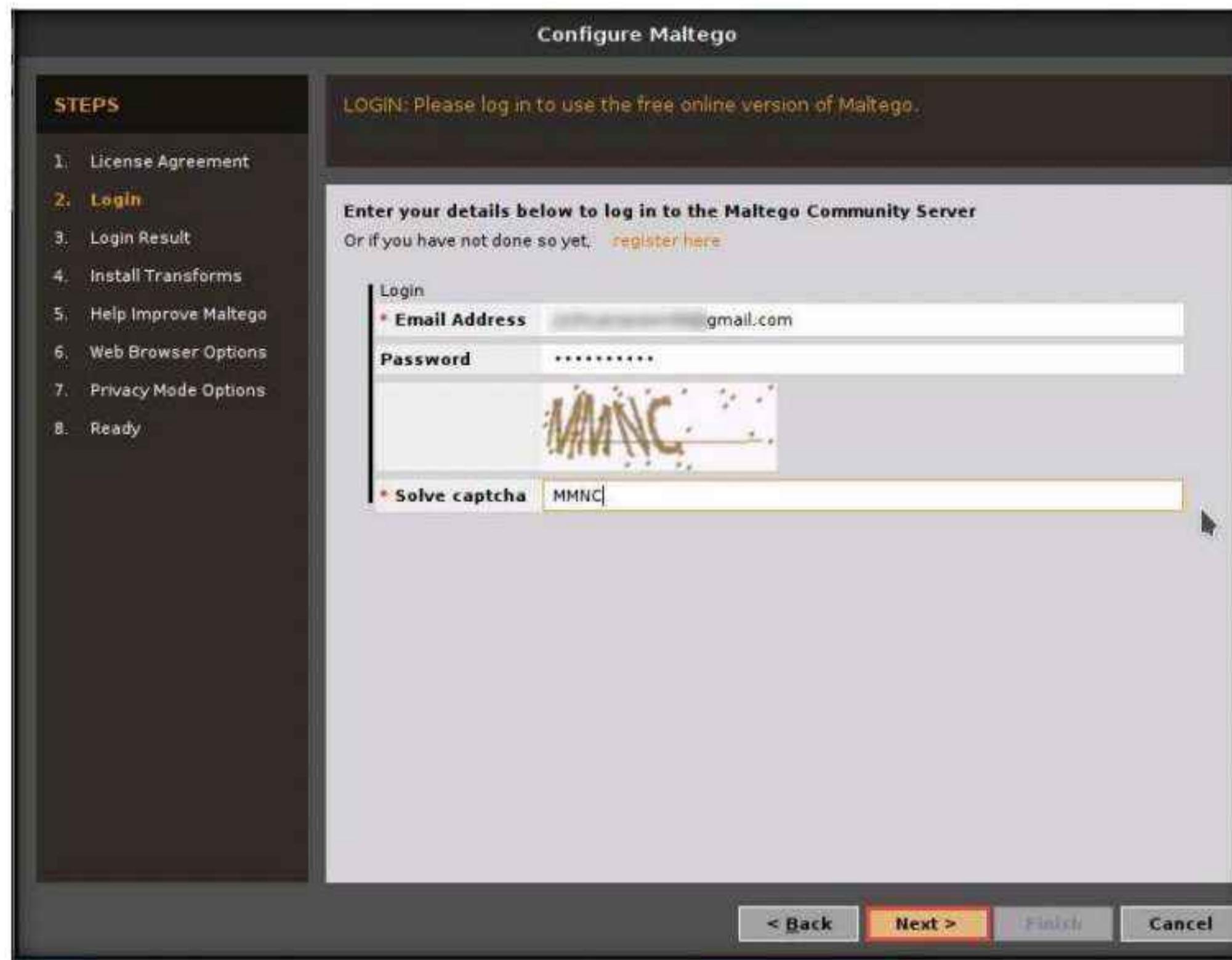


- Account Successfully Activated!** page appears, as shown in the screenshot.

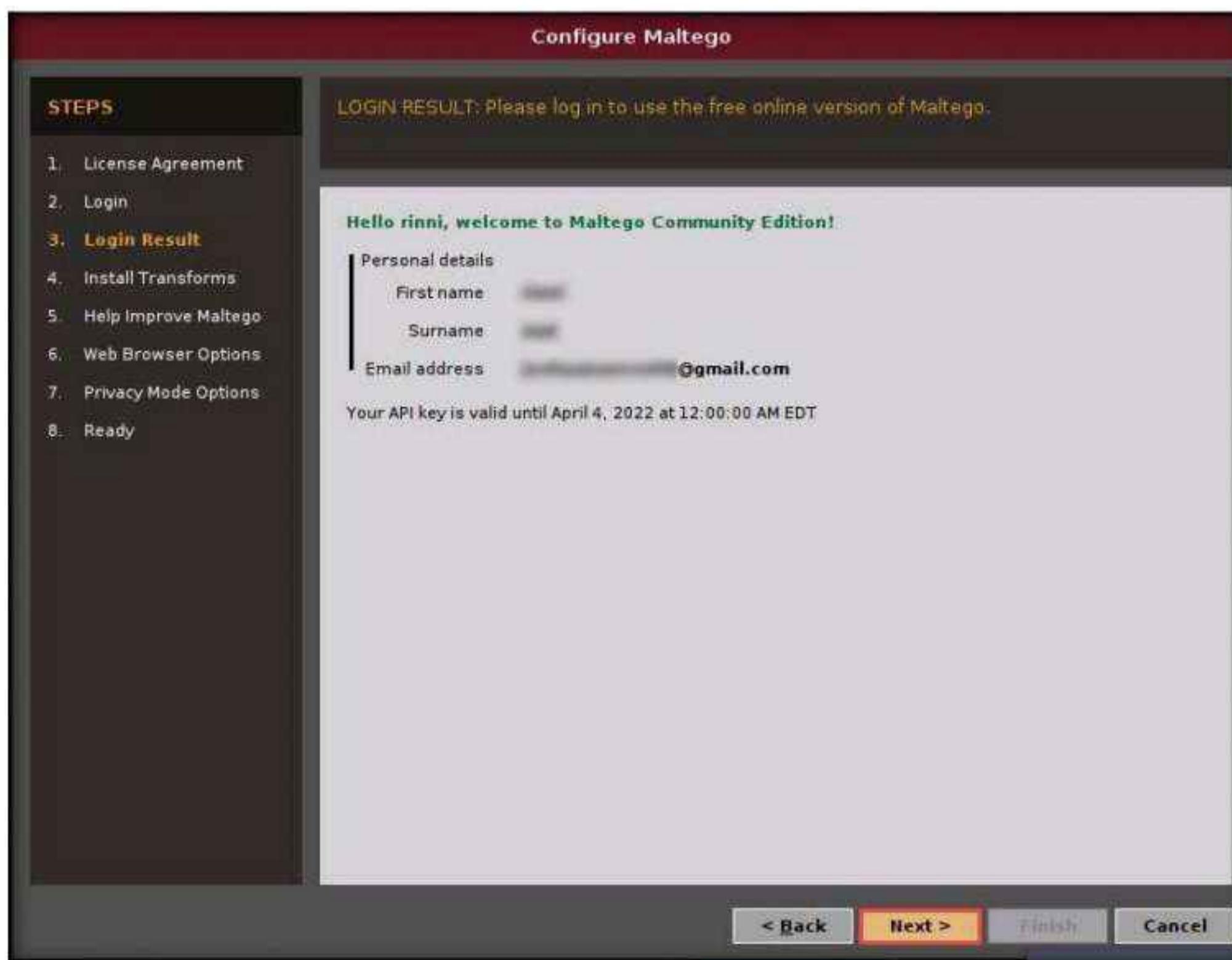


## Module 02 – Footprinting and Reconnaissance

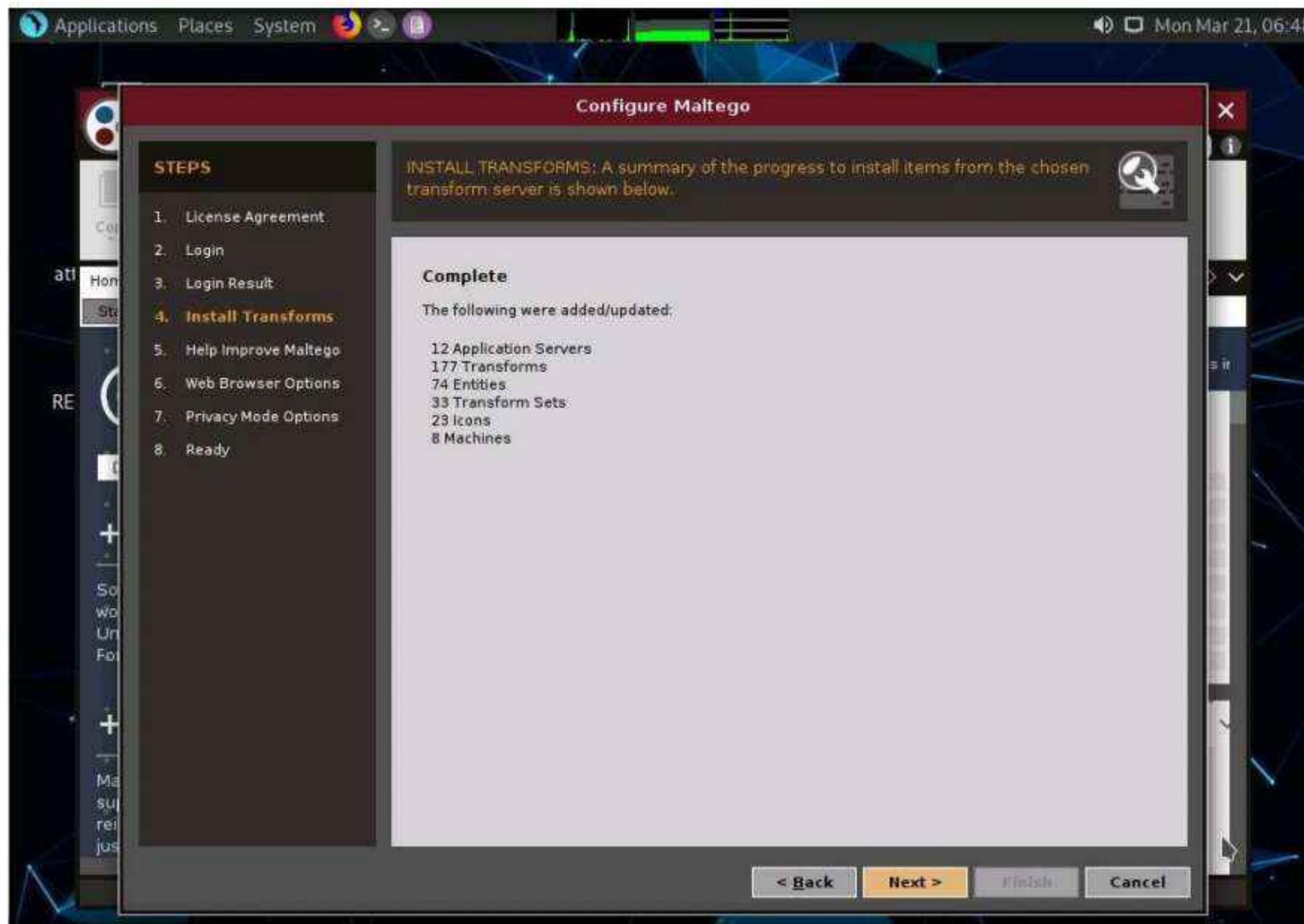
10. Minimize the web browser and go back to the setup wizard and enter the **Email Address** and **Password** specified at the time of registration; solve the captcha and click **Next**.



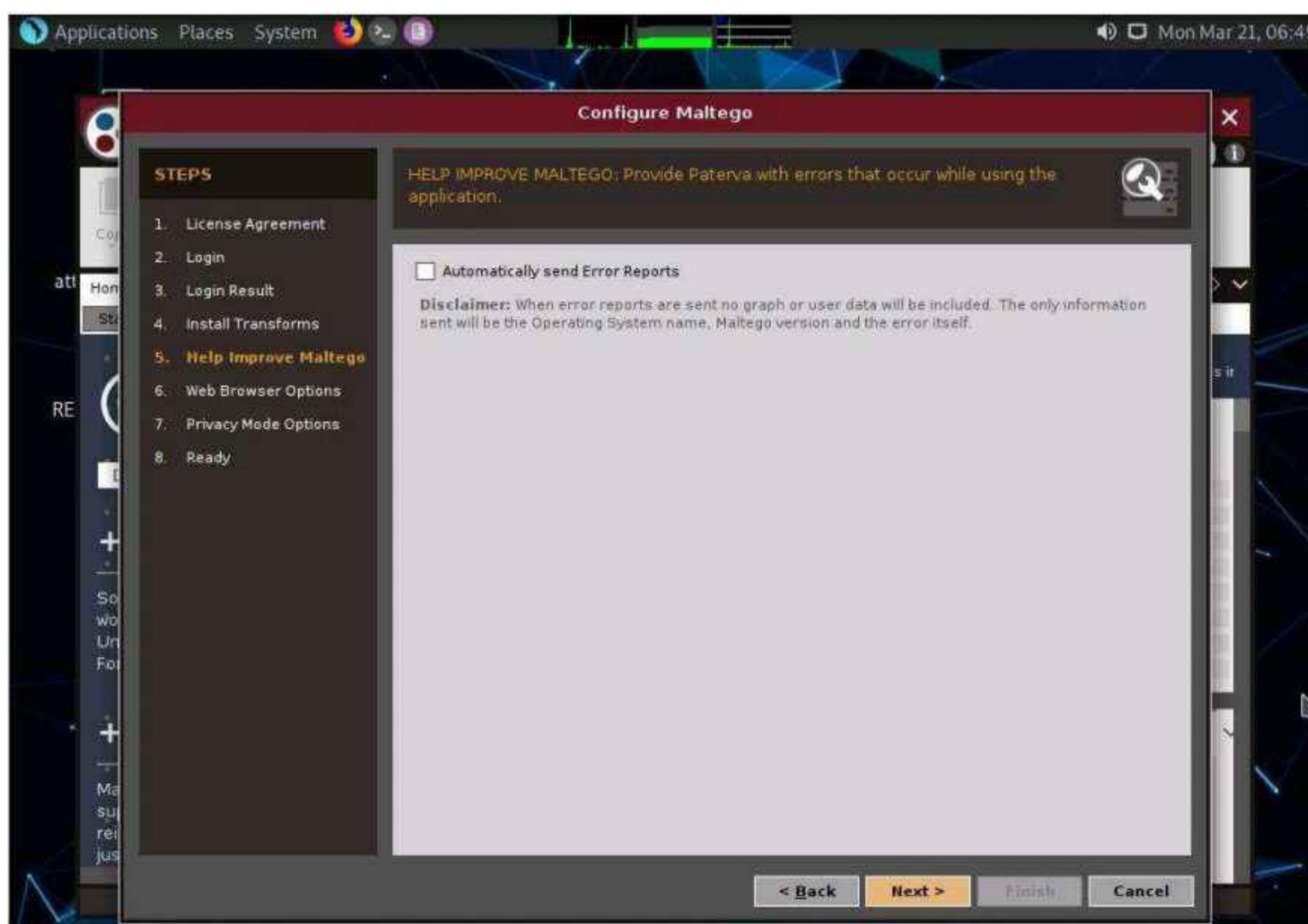
11. The **Login Result** section displays your personal details; click **Next**.



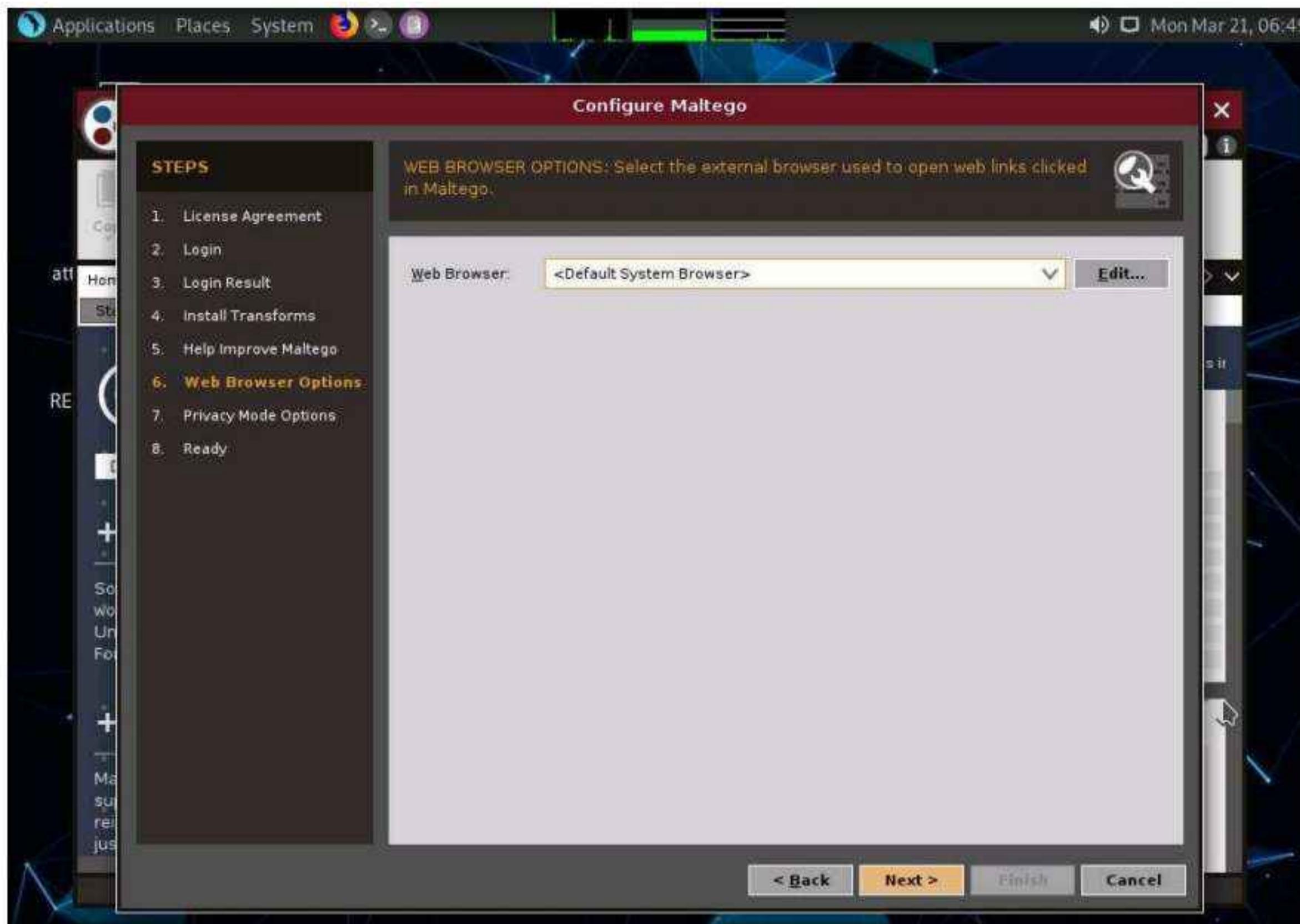
12. The **Install Transforms** section appears, which will install items from the chosen transform server. Leave the settings to default and click **Next**.



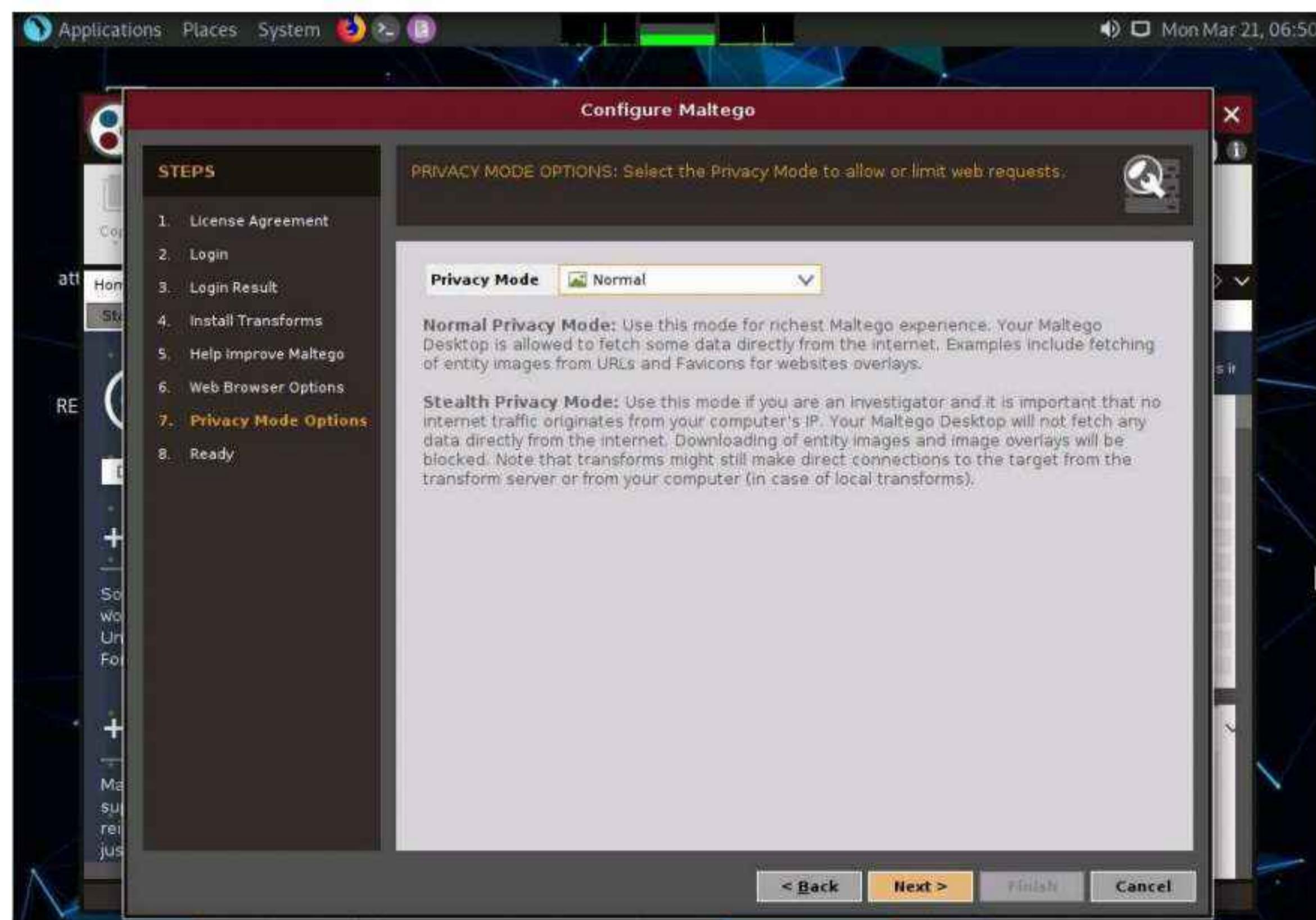
13. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.



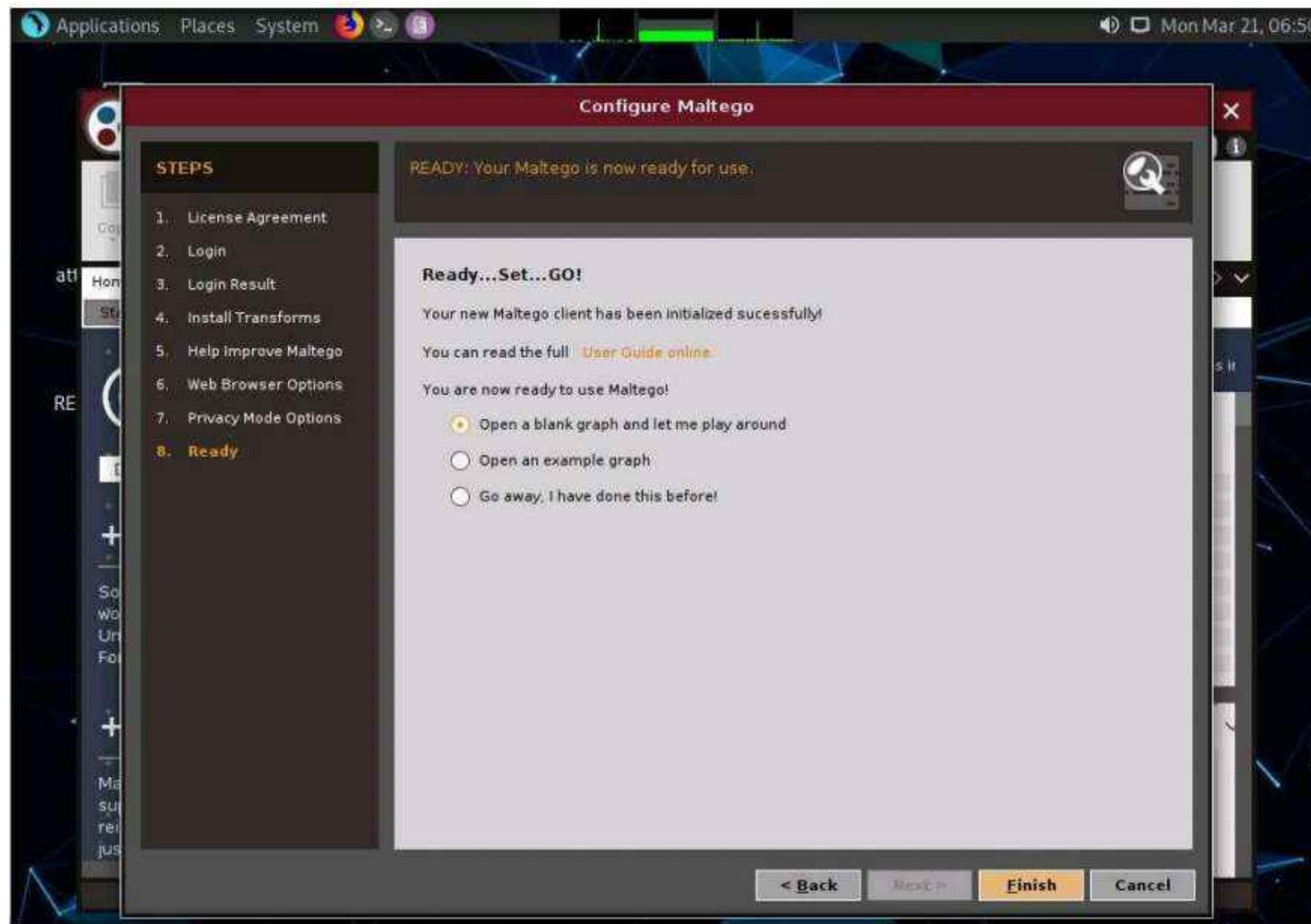
14. The **Web Browser Options** section appears. Leave the options set to default and click **Next**.



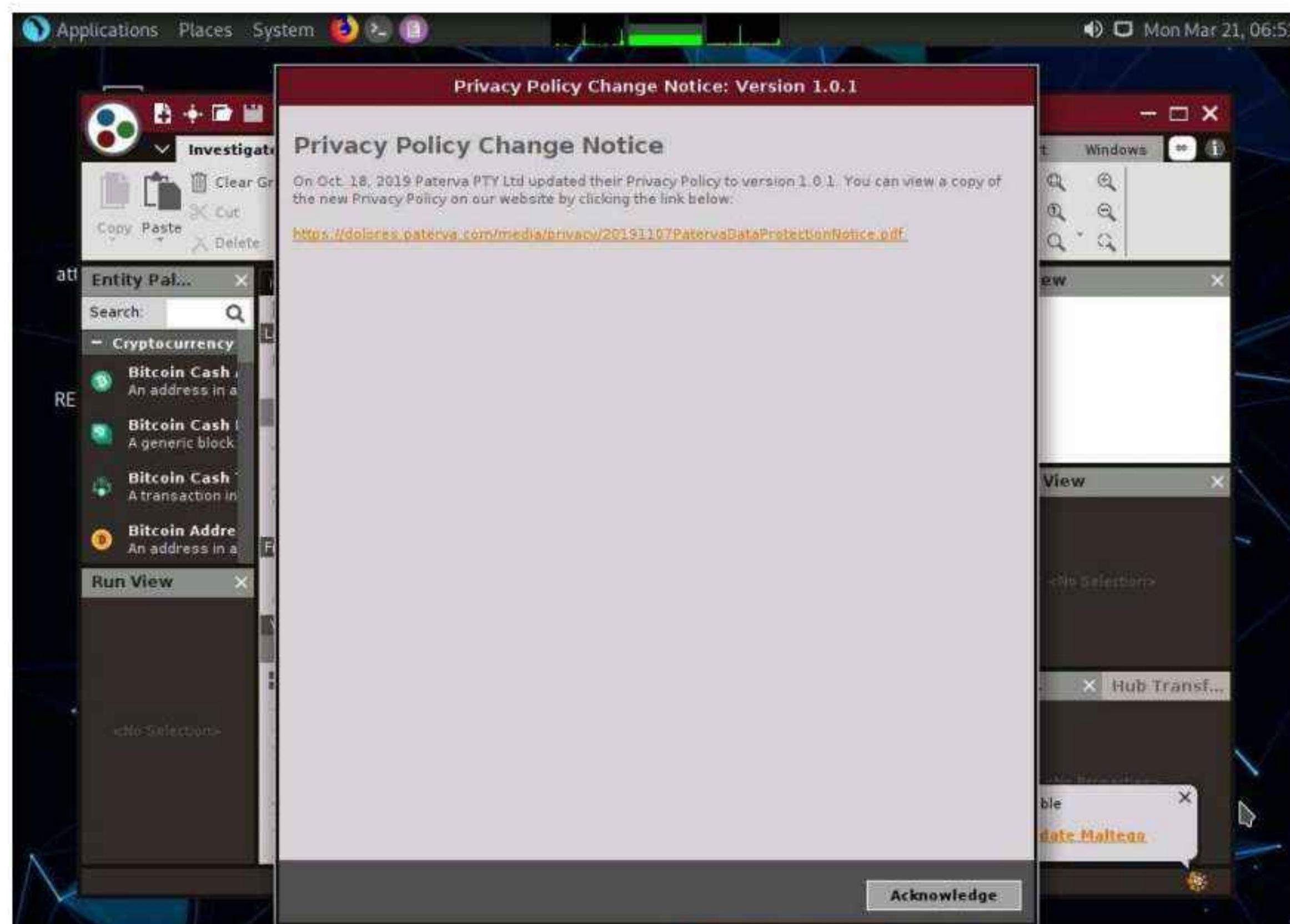
15. The **Privacy Mode Options** section appears. Leave the options set to default and click **Next**.



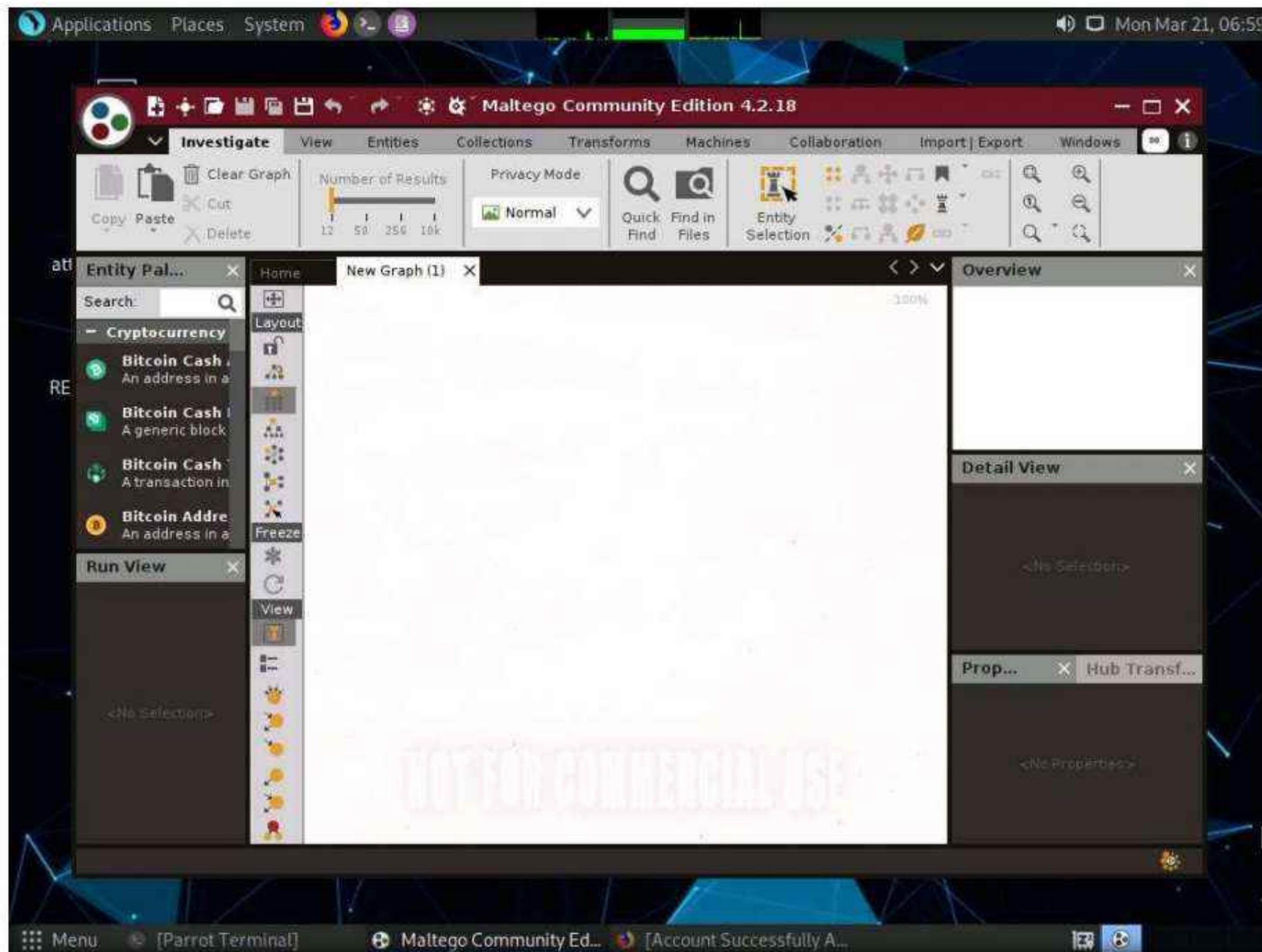
16. The Ready section appears, select **Open a blank graph and let me play around** option and click **Finish**.



17. The **Maltego Community Edition** GUI appears, along with **Privacy Policy Change Notice**, click **Acknowledge** button.



18. The **Maltego Community Edition** window along with the **New Graph (1)** window appears, as shown in the screenshot.



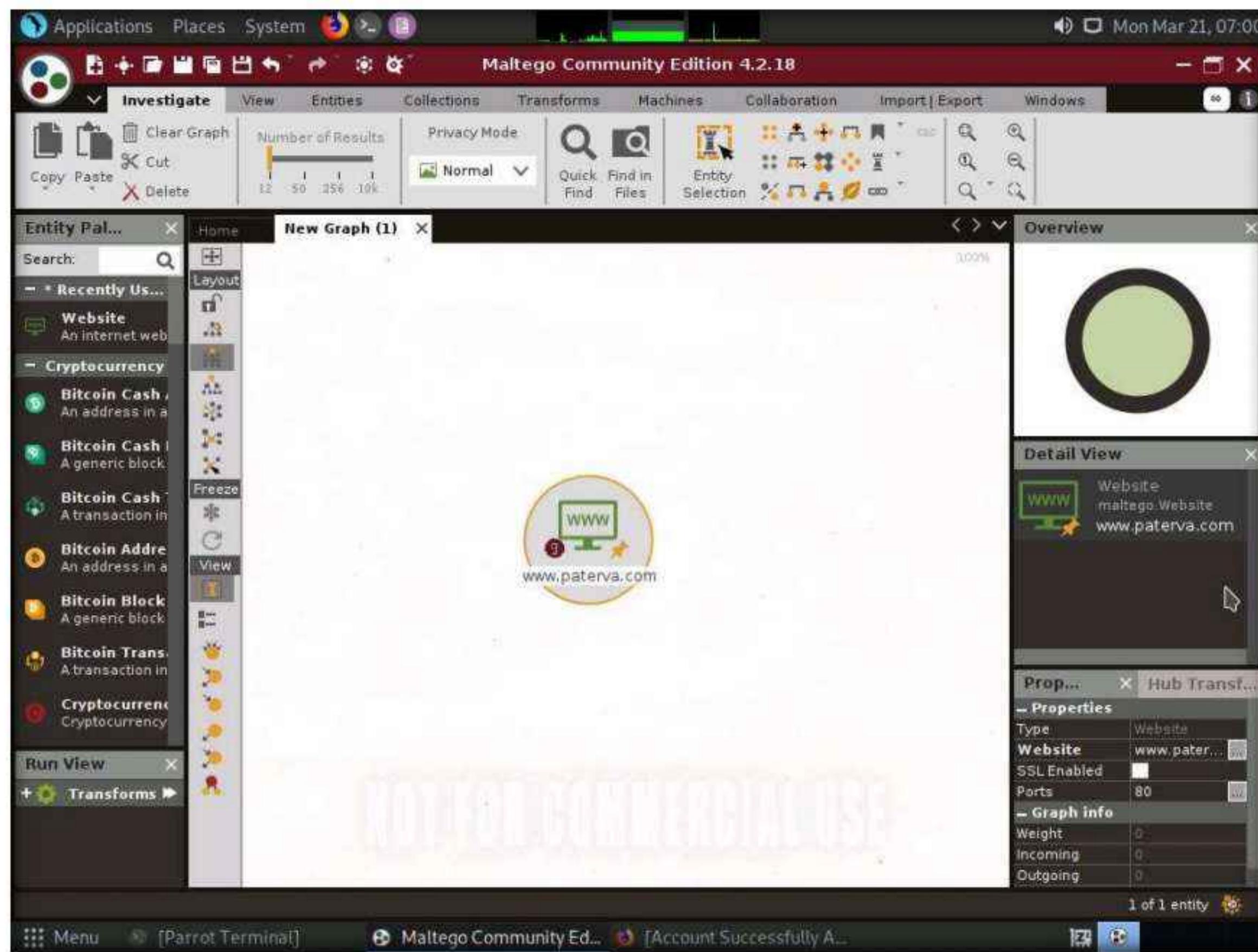
19. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS**, **DNS Name**, **Domain**, **IPv4 Address**, **URL**, **Website**, etc.

20. Drag the **Website** entity onto the **New Graph (1)** window.

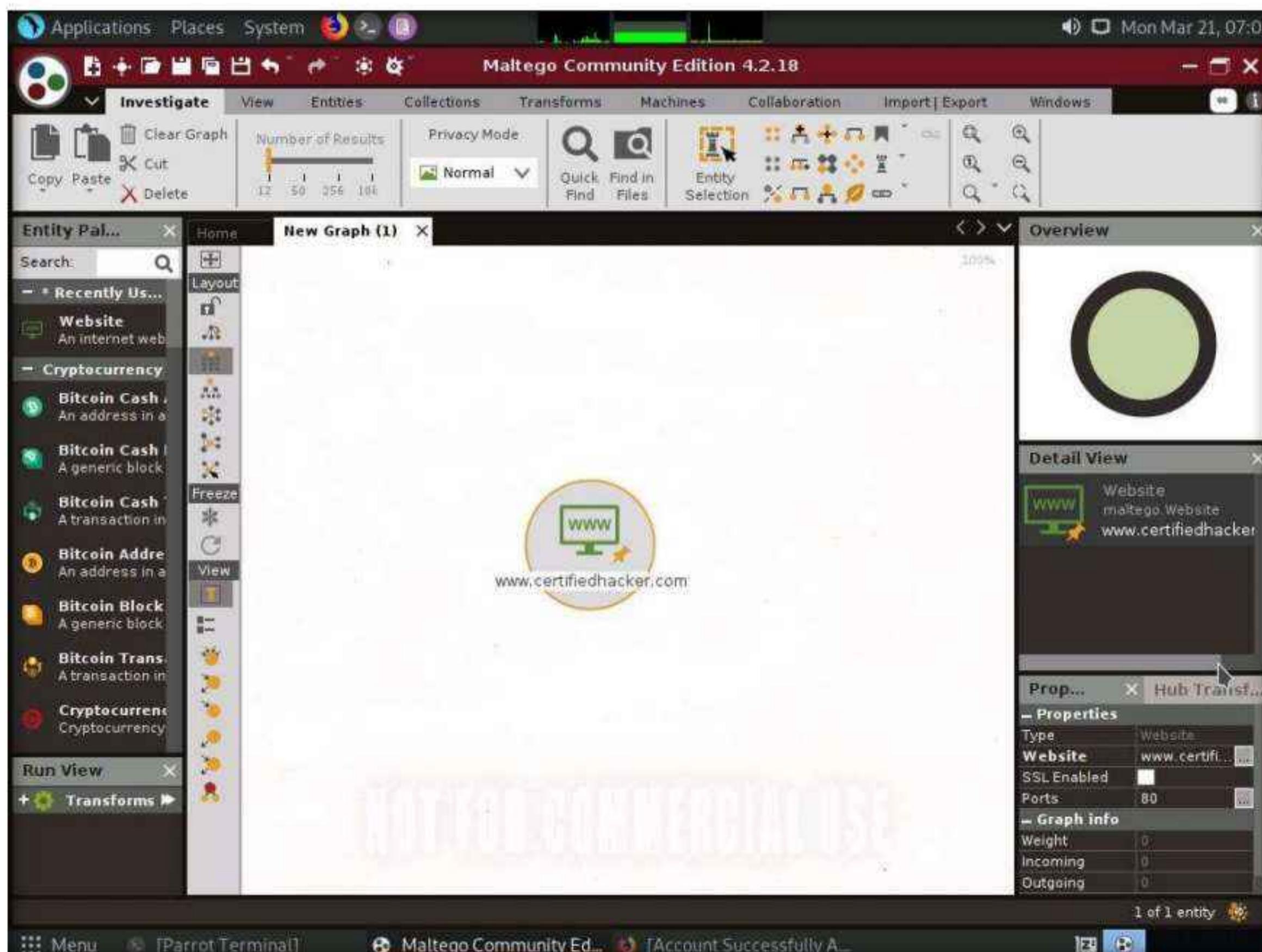
21. The entity appears on the new graph, with the **www.paterva.com** URL selected by default.

**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.

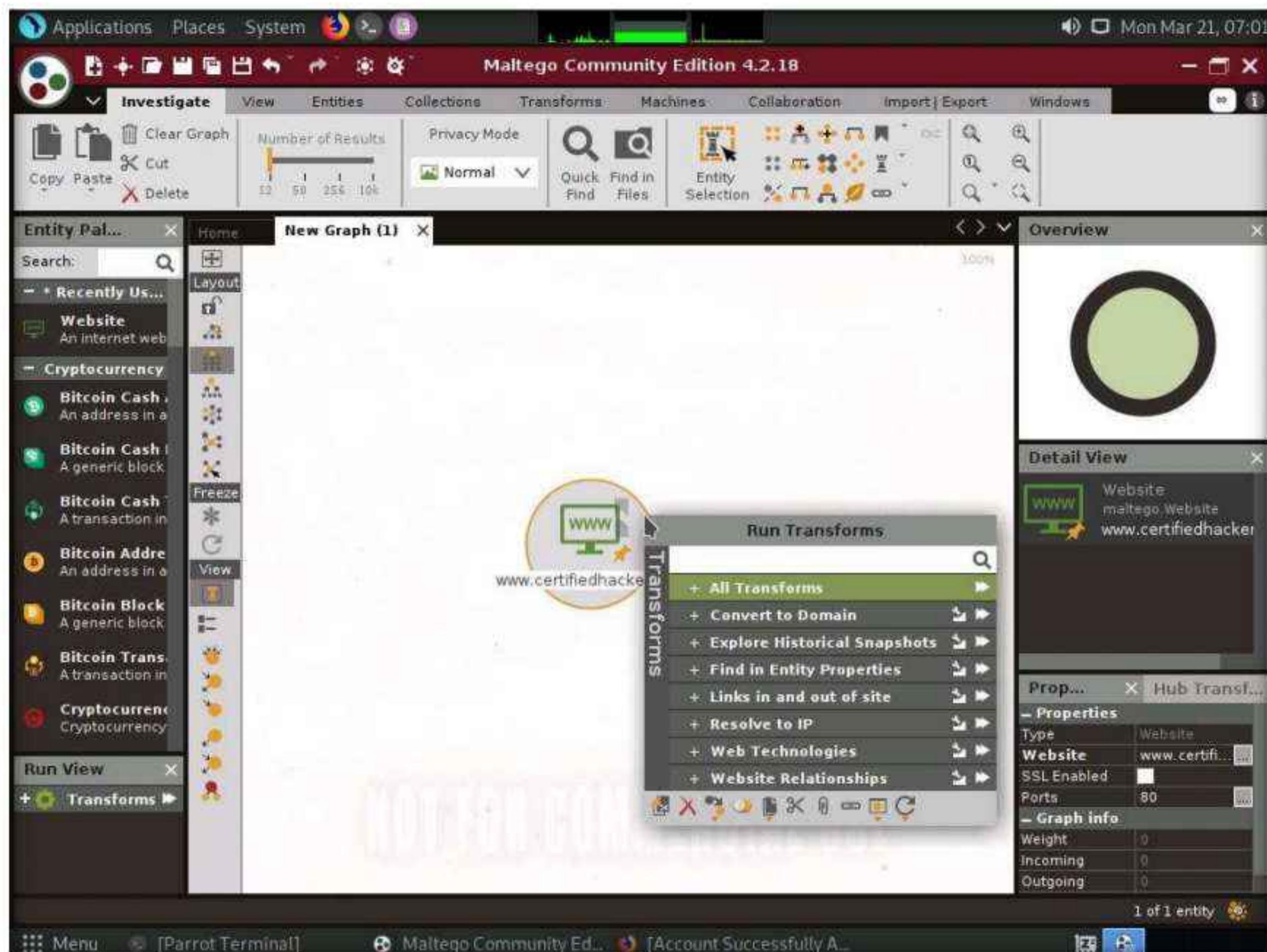
## Module 02 – Footprinting and Reconnaissance



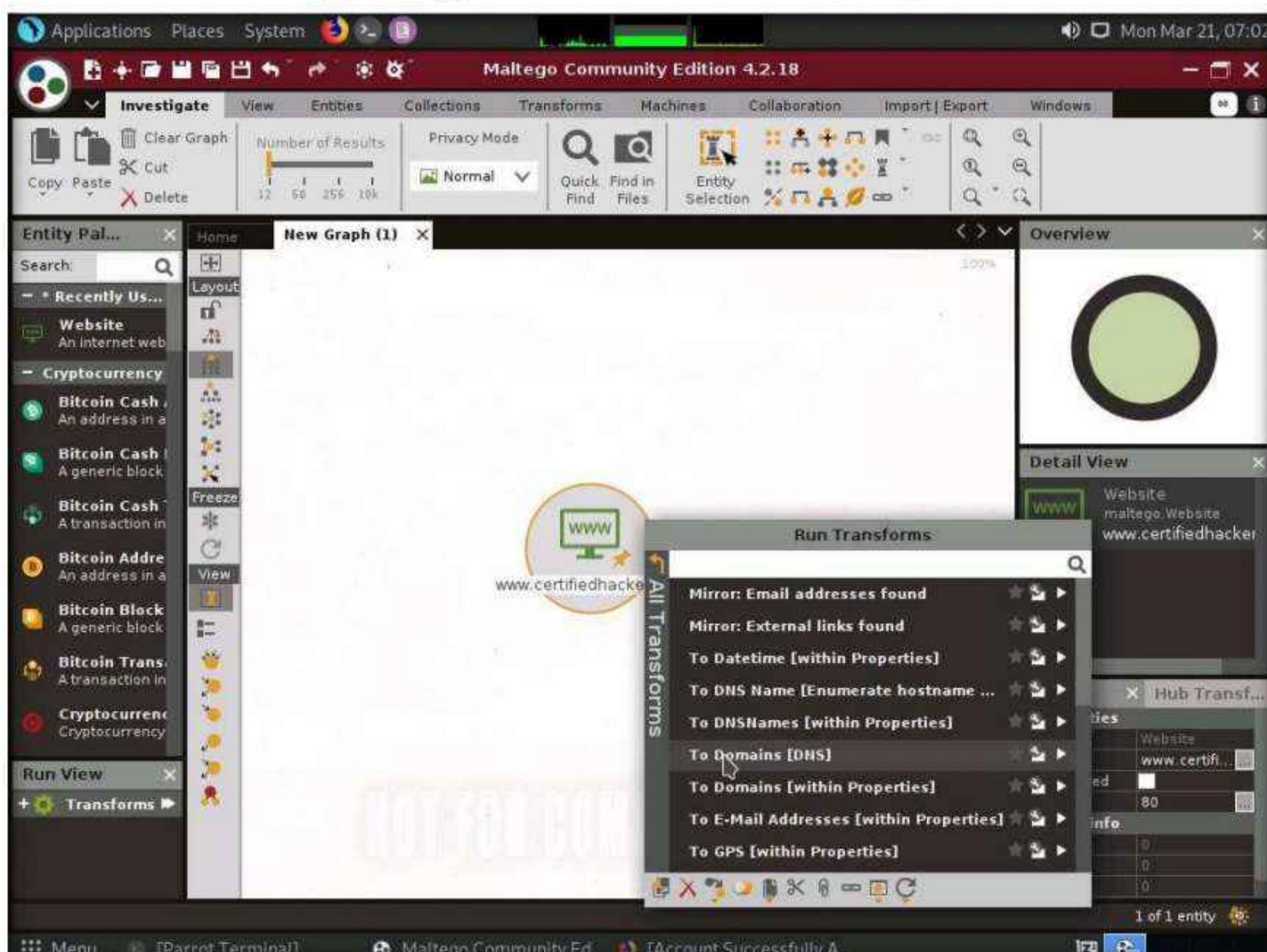
22. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press Enter.



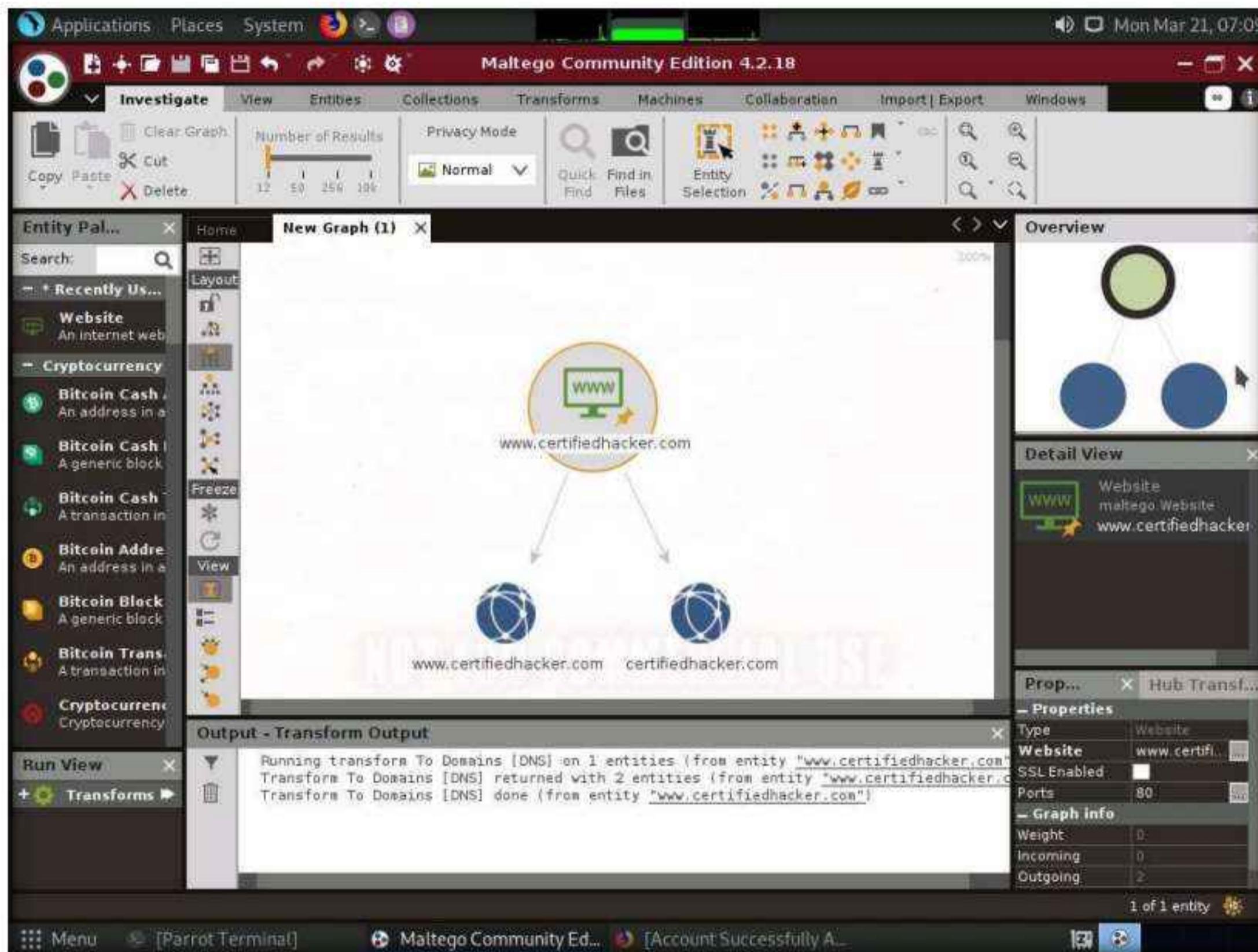
23. Right-click the entity and select All Transforms.



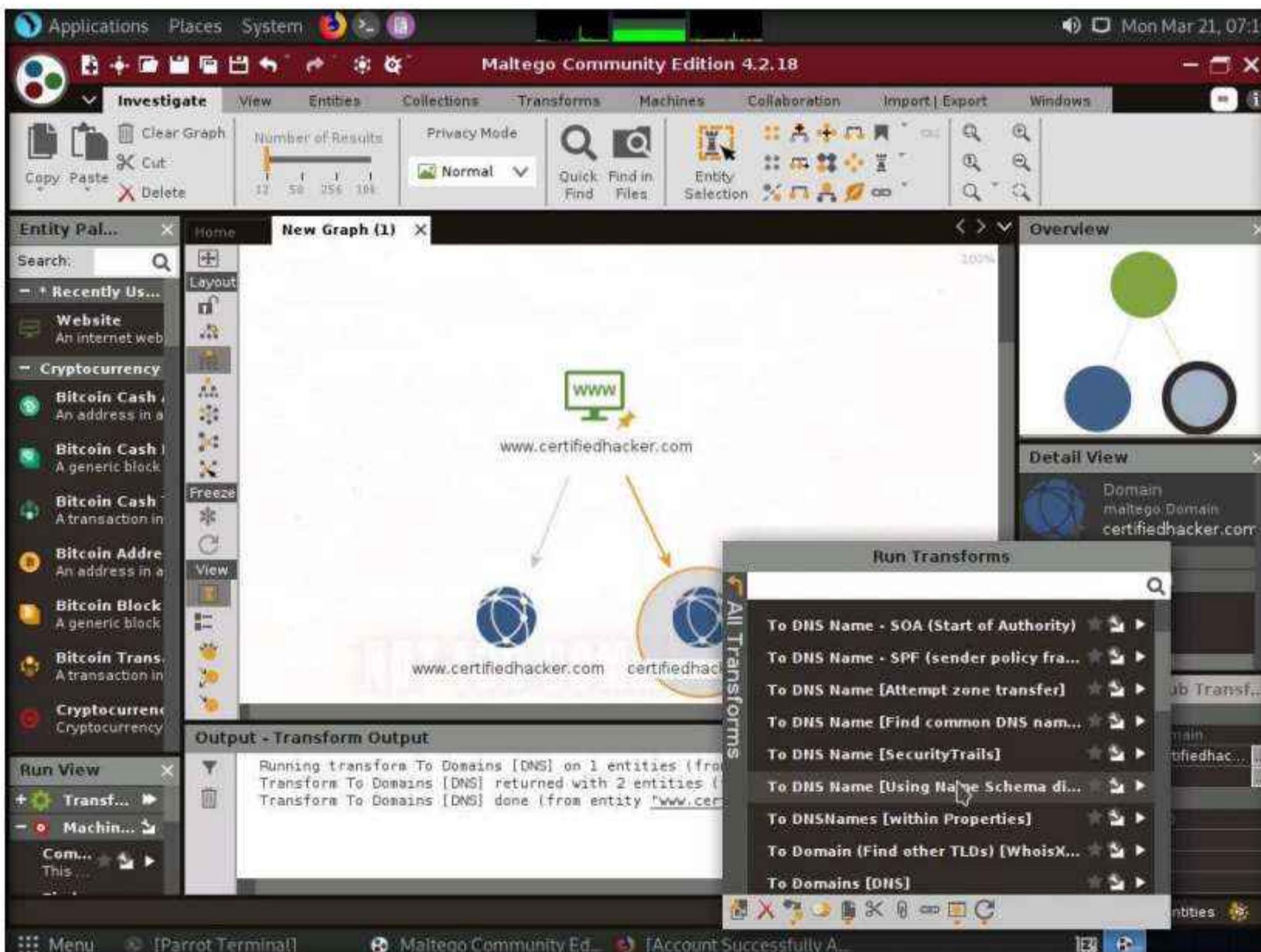
24. The Run Transform(s) list appears; click To Domains [DNS].



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

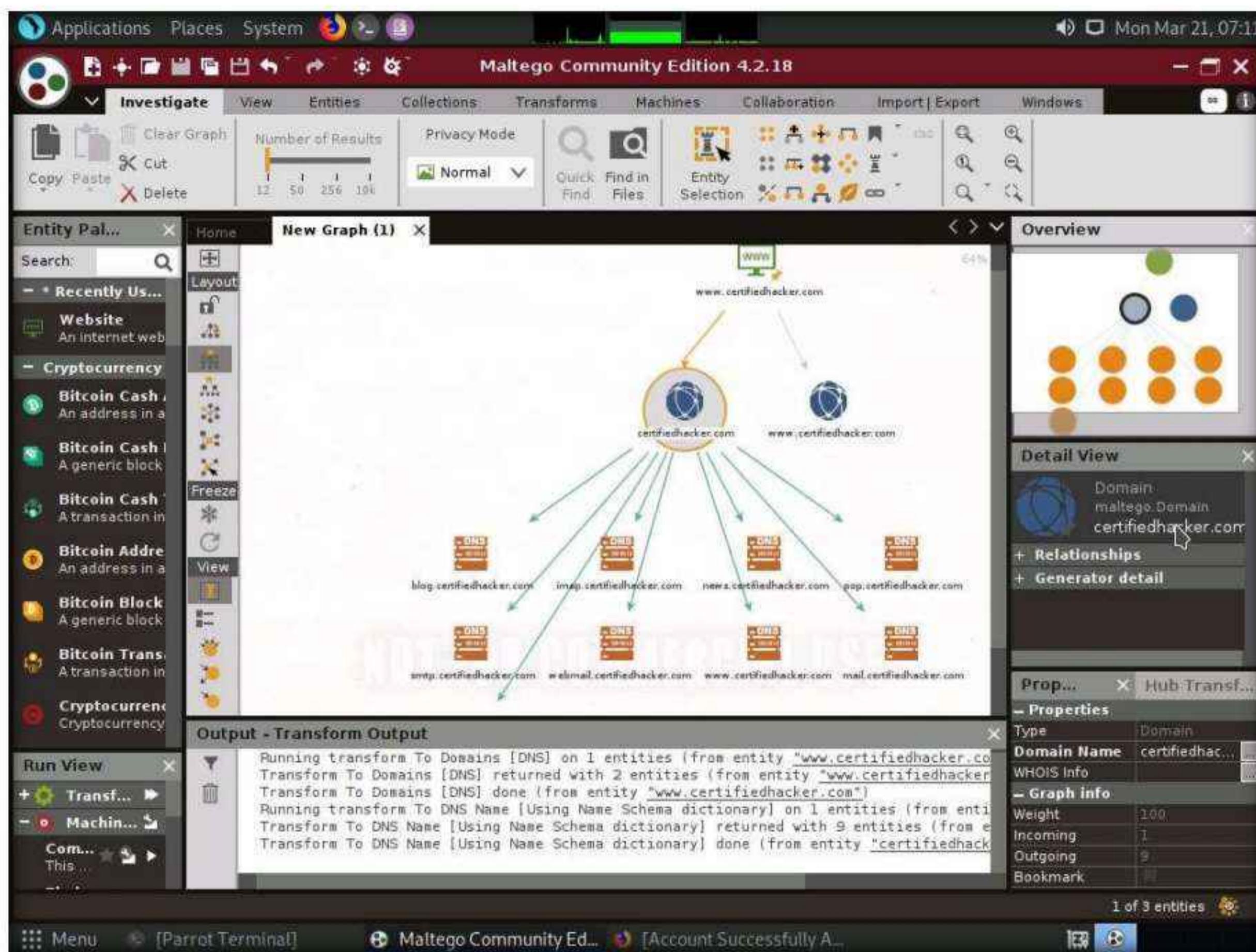


26. Right-click the **certifiedhacker.com** entity and select All Transforms ---> To DNS Name [Using Name Schema dict...].



## Module 02 – Footprinting and Reconnaissance

27. 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.



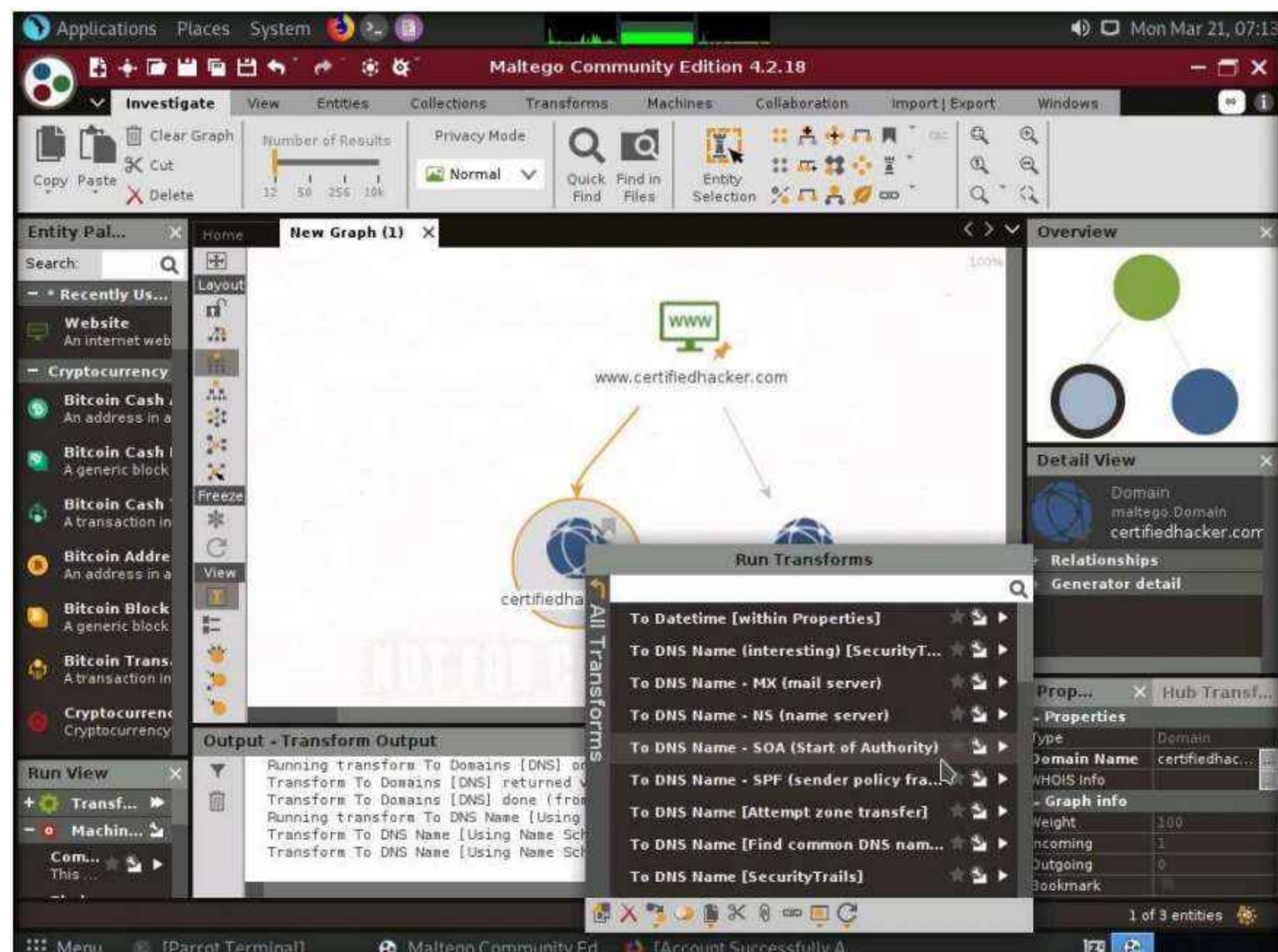
28. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential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

29. Select only the name schemas by dragging and deleting them.

## Module 02 – Footprinting and Reconnaissance

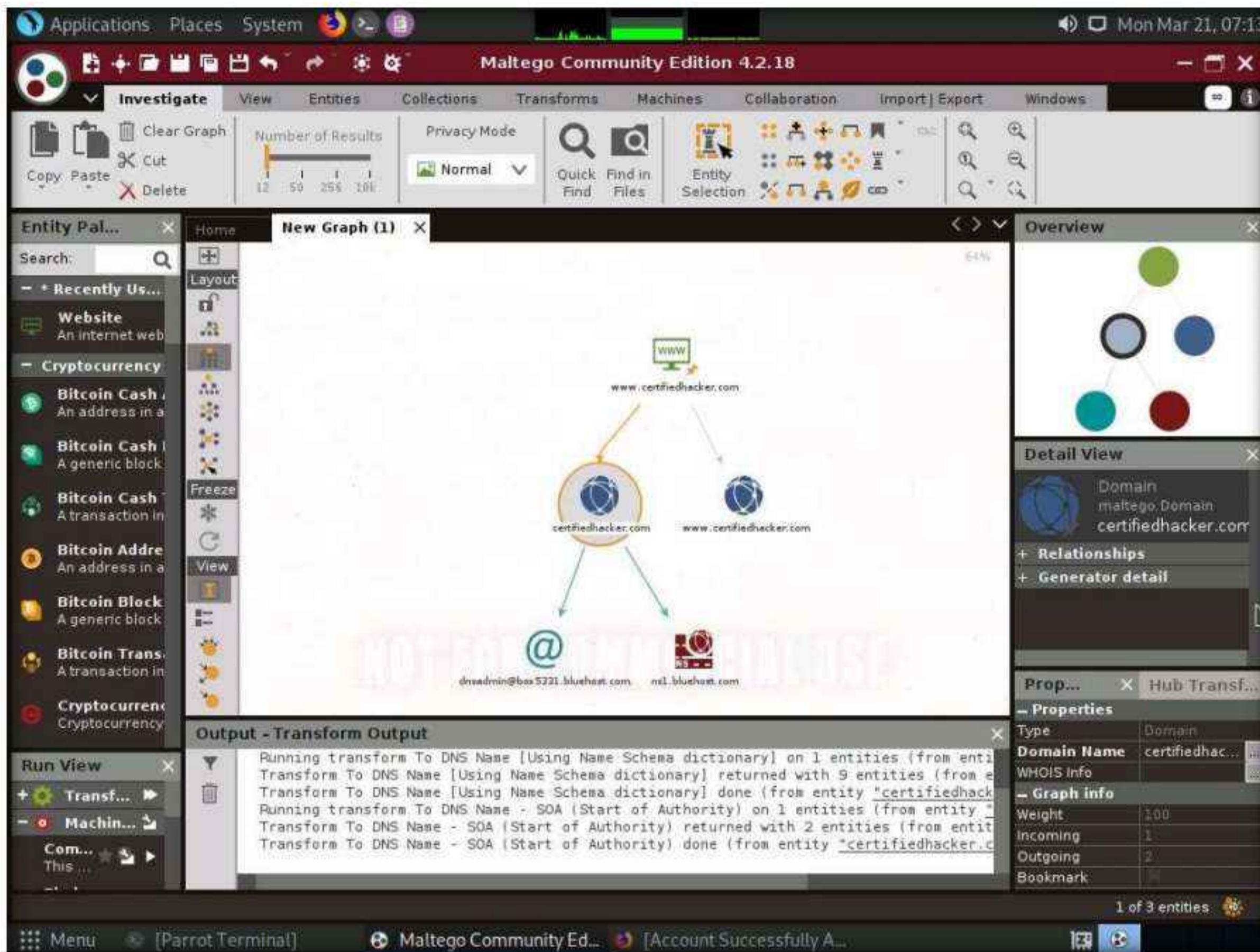


30. Right-click the **certifiedhacker.com** entity and select All Transforms --> To DNS Name - SOA (Start of Authority).



## Module 02 – Footprinting and Reconnaissance

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

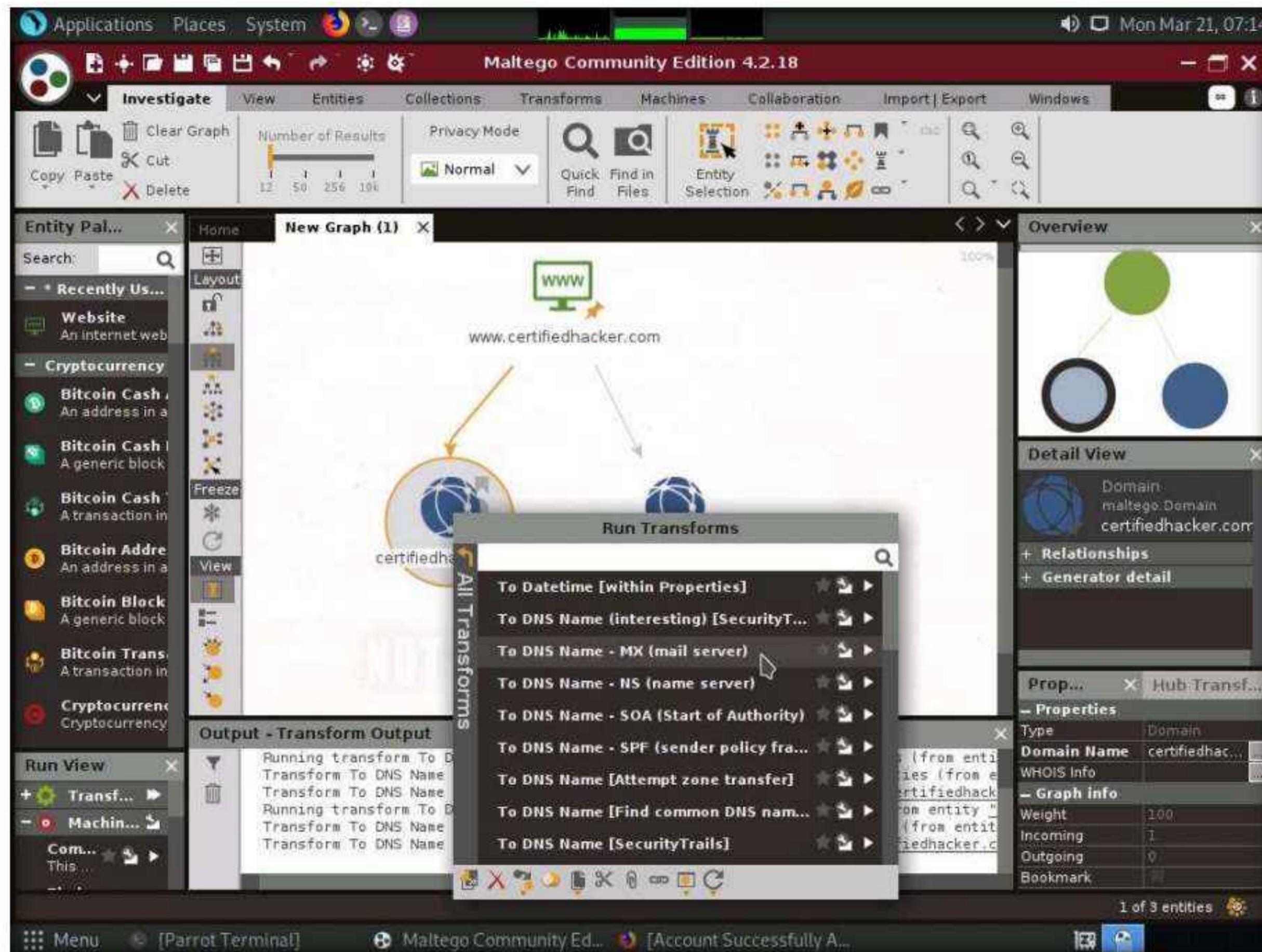


32. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.

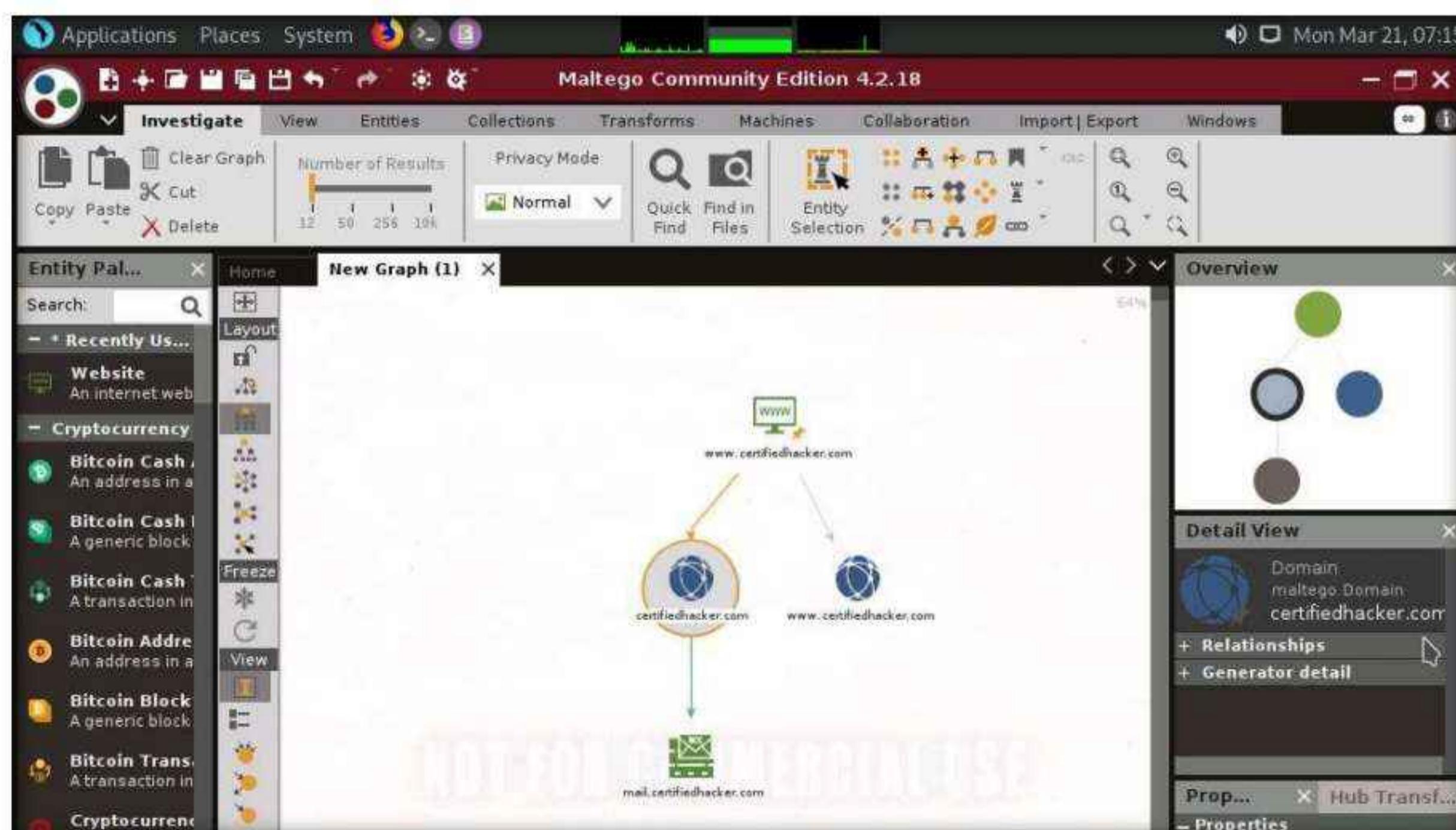
33. Select both the name server and the email by dragging and deleting them.



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



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

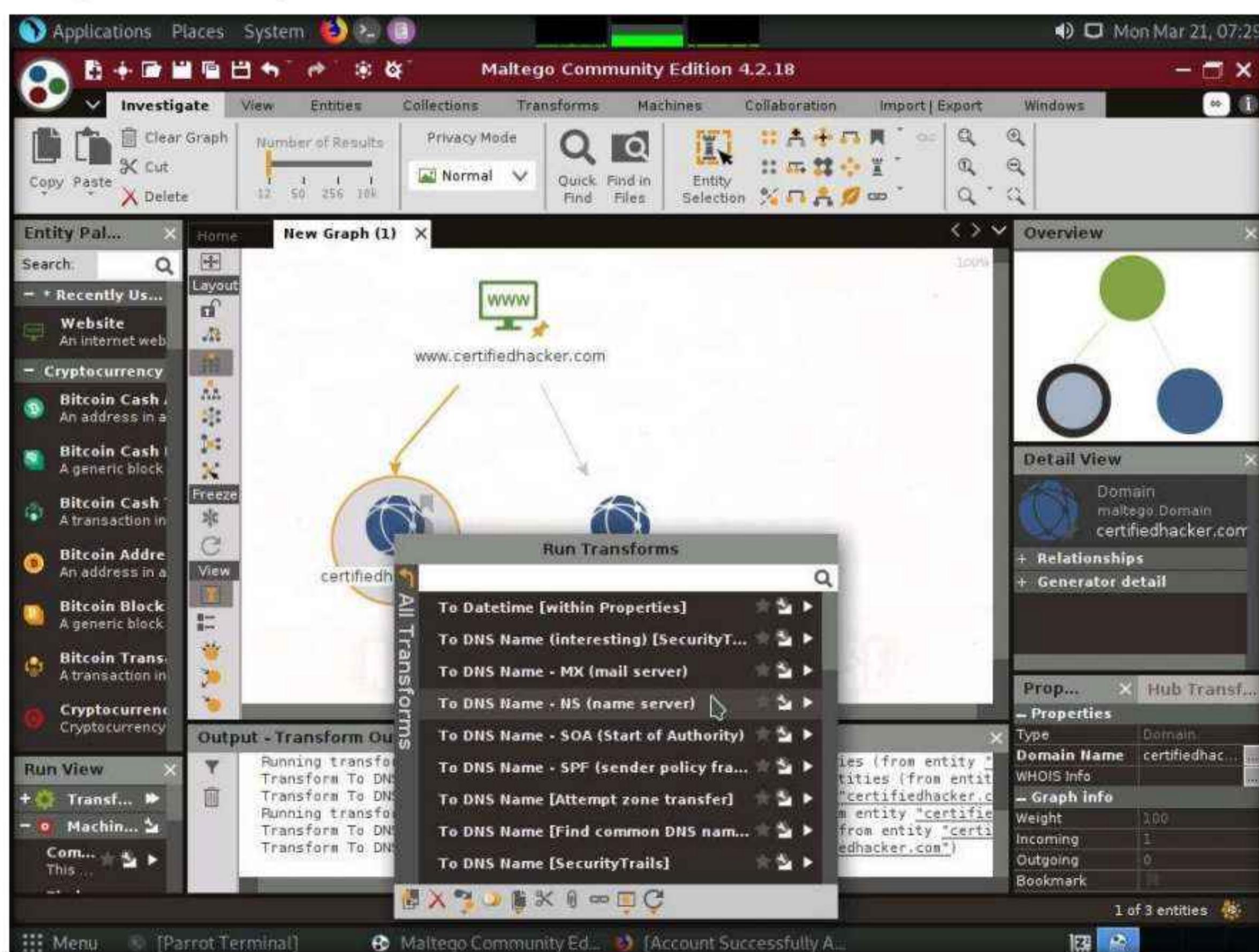


## Module 02 – Footprinting and Reconnaissance

36. 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.
37. Select only the mail server by dragging and deleting it.



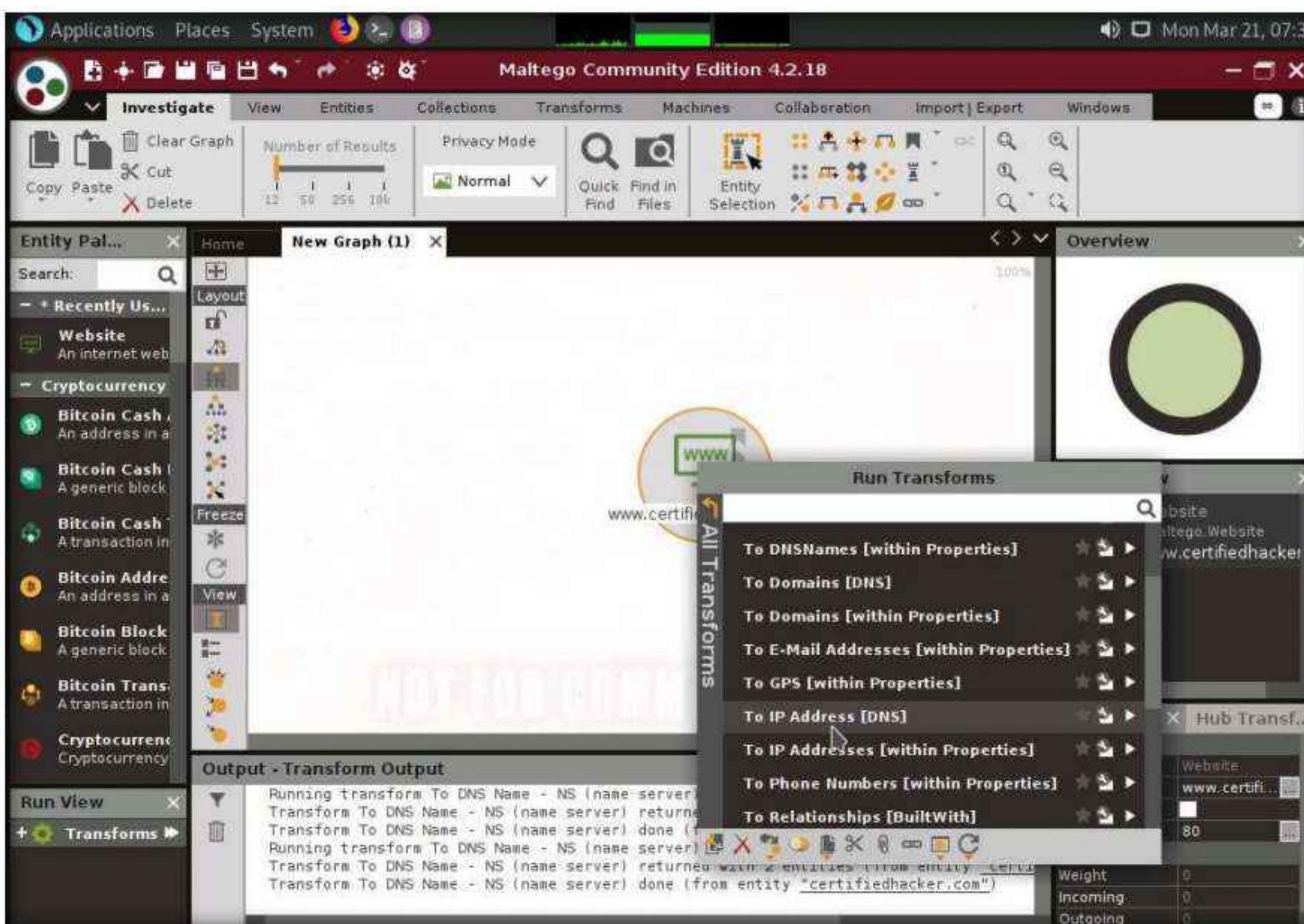
38. Right-click the **certifiedhacker.com** entity and select All Transforms --> To DNS Name - NS (name server).



39. This returns the name servers associated with the domain, as shown in the following screenshot.
40. 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.
41. Select both the domain and the name server by dragging and deleting them.

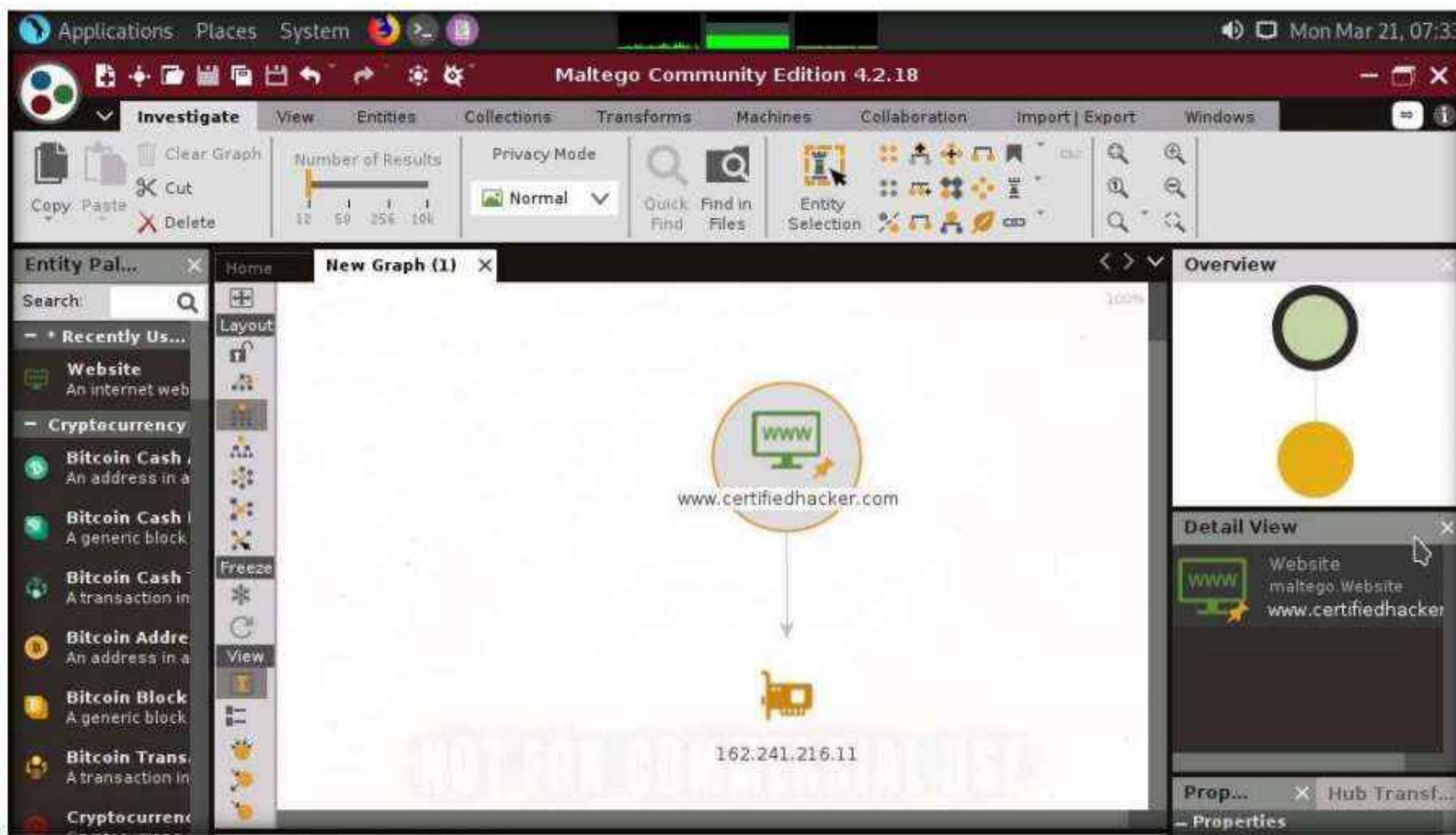


42. Right-click the entity and select All Transforms --> To IP Address [DNS].



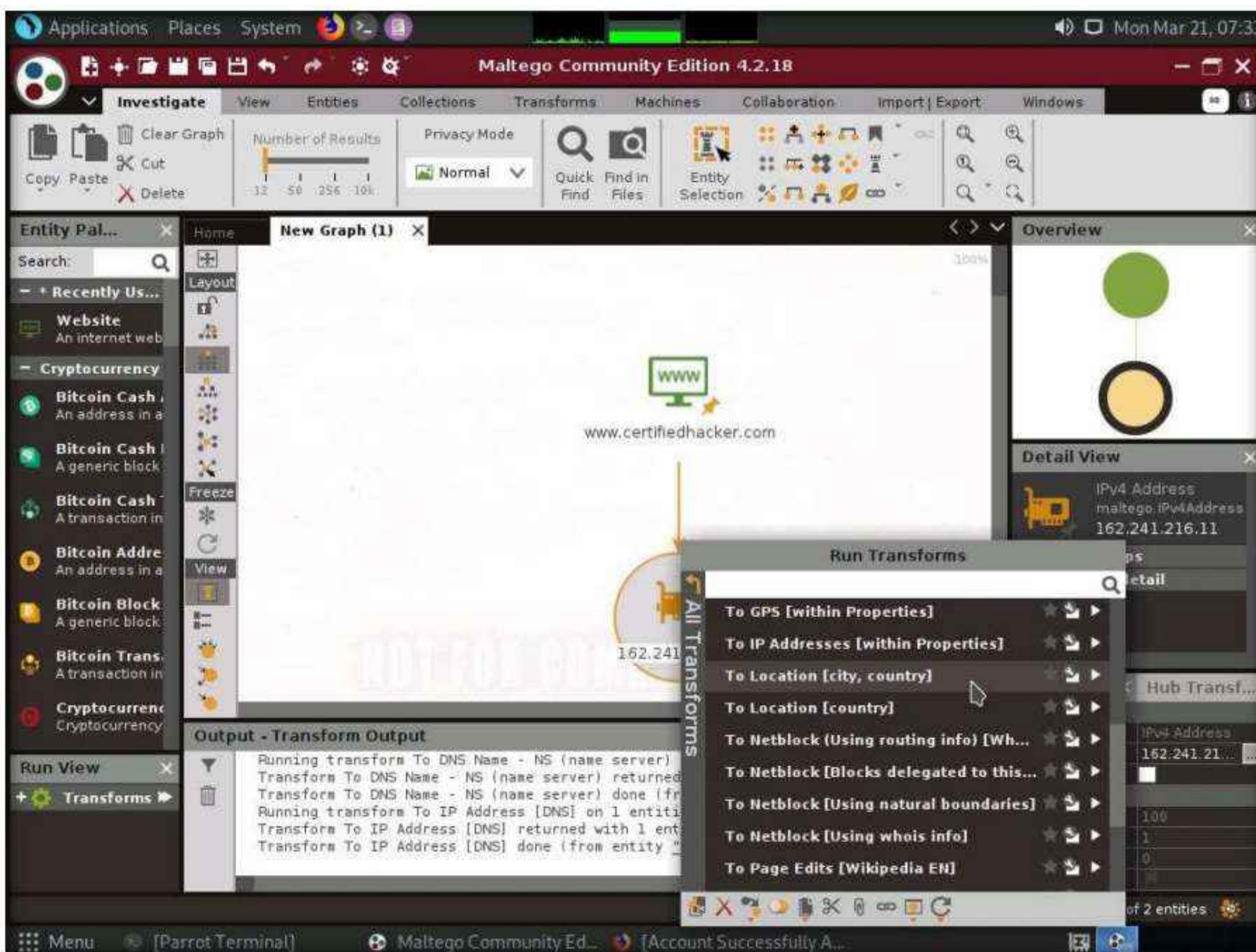
## Module 02 – Footprinting and Reconnaissance

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

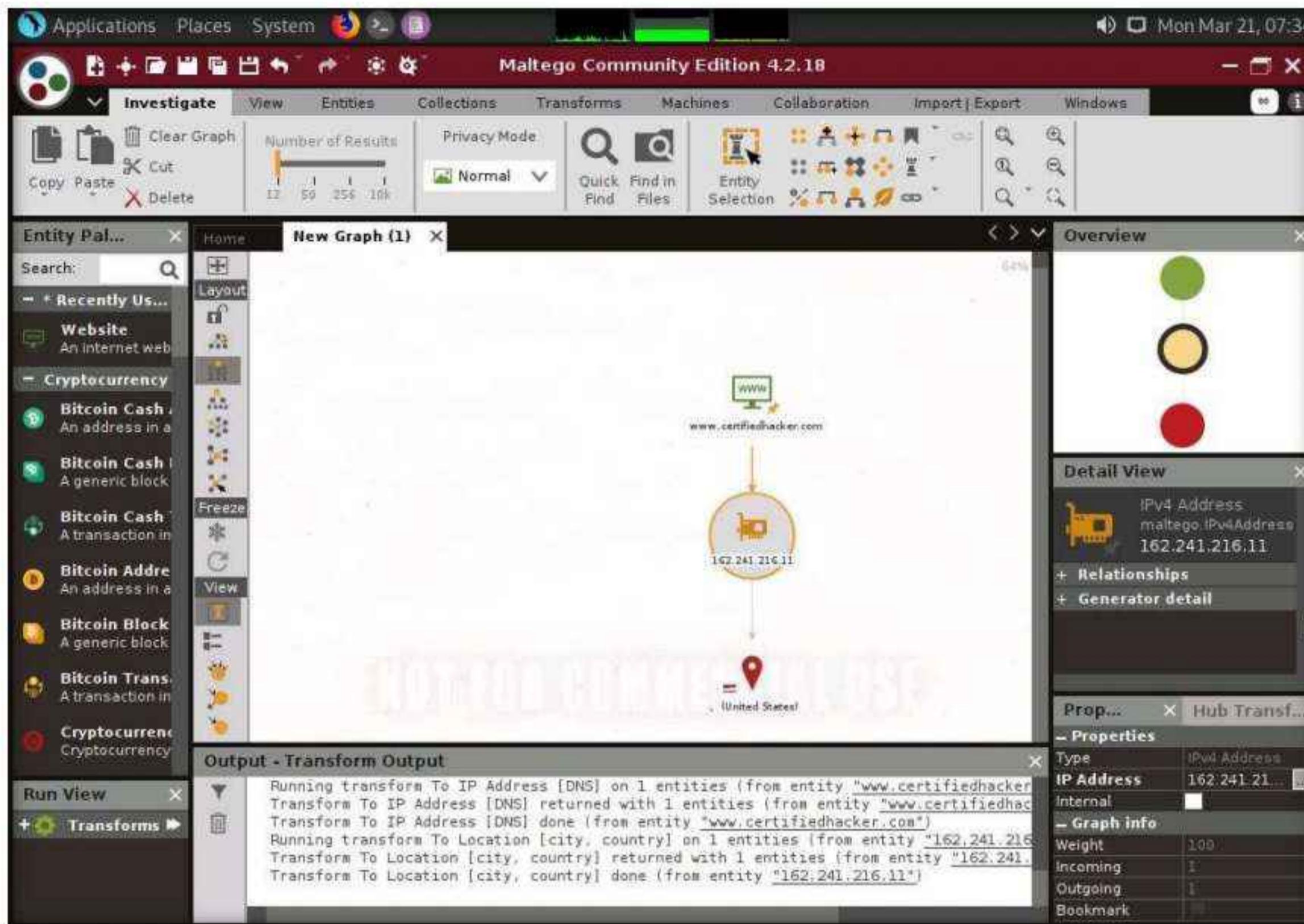


44. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

45. Right-click the IP address entity and select All Transforms --> To location [city, country].



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



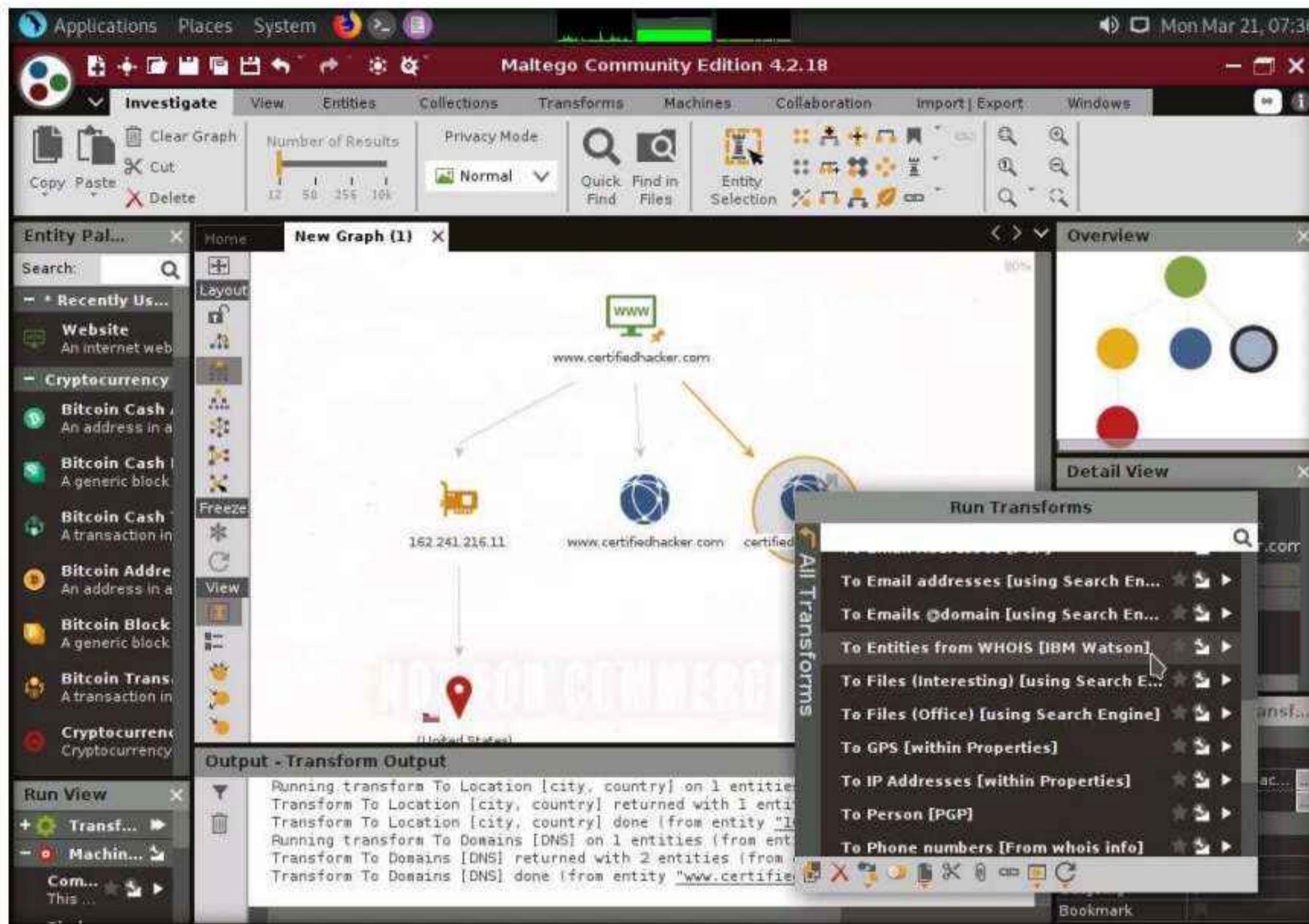
47. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

48. 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.

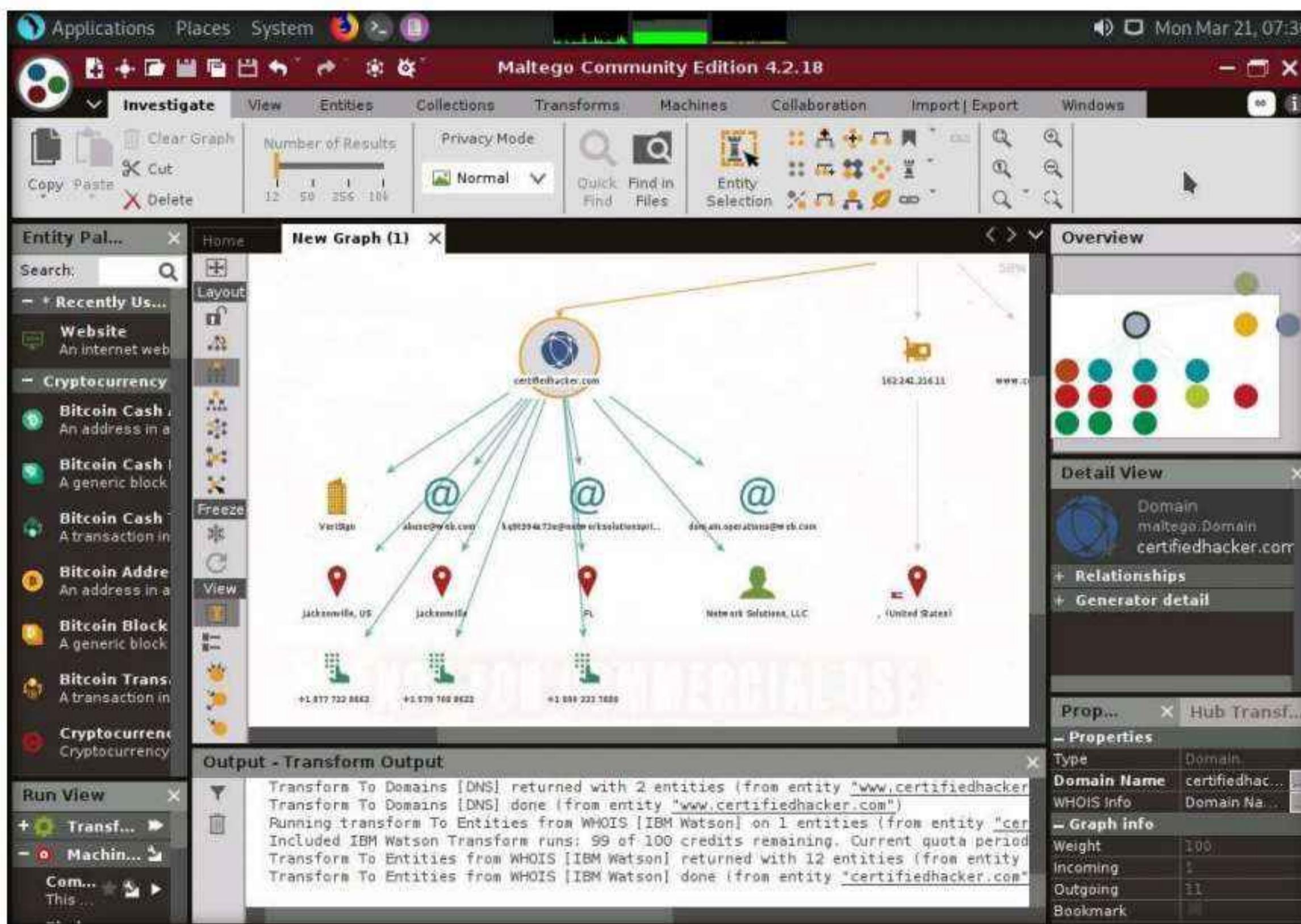


## Module 02 – Footprinting and Reconnaissance

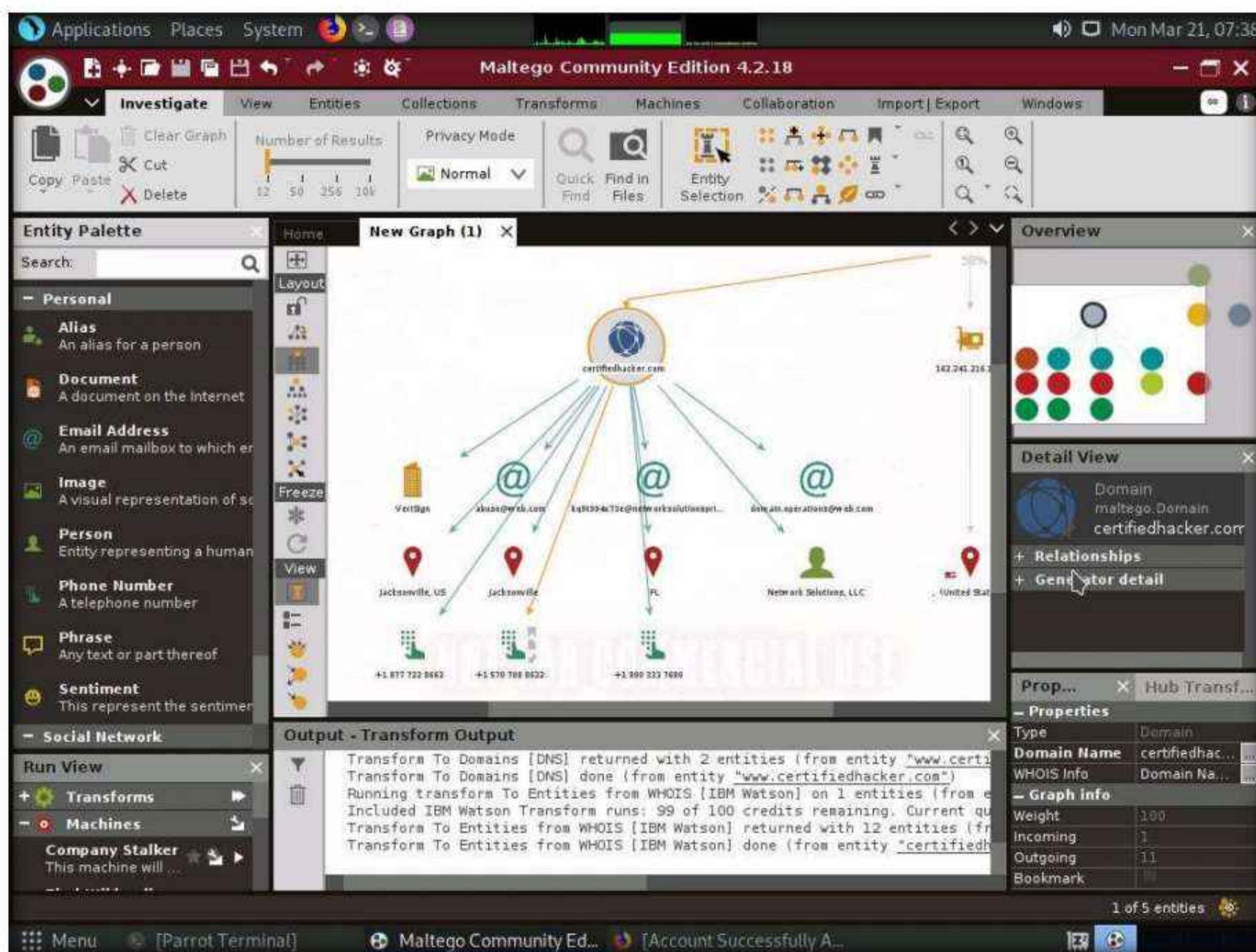
49. Right-click the domain entity (`certifiedhacker.com`) and select All Transform --> To Entities from WHOIS [IBM Watson].



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



51. 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.
52. 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.
53. 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.



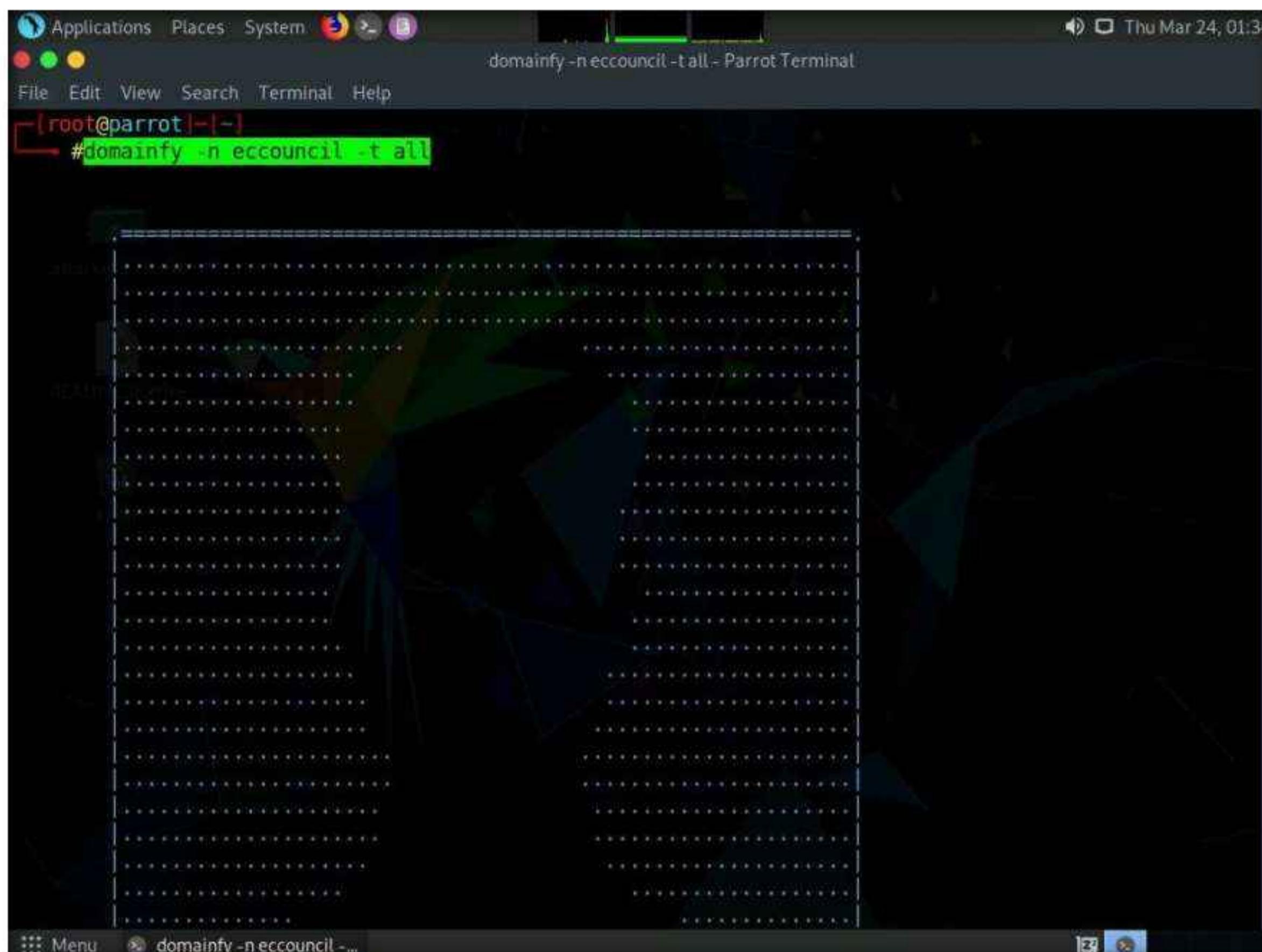
54. Apart from the transforms mentioned above, other transforms can track accounts and conversations of individuals who are registered on social networking sites such as Twitter. Extract all possible information.
55. By extracting all this information, you can simulate actions such as enumeration, web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

## Task 3: Footprinting a Target using OSRFramework

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.

1. In the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **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.
5. Use **domainfy** to check with the existing domains using words and nicknames. Type **domainfy -n [Domain Name] -t all** (here, the target domain name is **ECCOUNCIL**) and press **Enter**.

**Note:** **-n:** specifies a nickname or a list of nicknames to be checked. **-t:** specifies a list of top-level domains where nickname will be searched.



The screenshot shows a terminal window titled "domainfy -n eccouncil -t all - Parrot Terminal". The window is running on a Parrot Security virtual machine. The terminal prompt is "[root@parrot] ~" and the command "#domainfy -n eccouncil -t all" is entered. The background of the terminal window shows a dark, abstract pattern. The desktop environment includes a menu bar with "Applications", "Places", "System", and icons for "File Manager", "Terminal", and "Help". The taskbar at the bottom shows the title "domainfy -n eccouncil -..." and a system tray with icons for battery, signal, and volume.

## Module 02 – Footprinting and Reconnaissance

6. The tool will retrieve all the domains along with their IP addresses related to the target domain. Using this information, attackers can further find vulnerabilities in the subdomains of the target website and launch web application attacks.

```
Applications Places System domainfy -n eccouncil -t all - Parrot Terminal
File Edit View Search Terminal Help
2022-03-24 01:33:57.009035      21 results obtained:
Sheet Name: Objects recovered (2022-3-24_1h33m).
+-----+-----+
| com.i3visio.Domain | com.i3visio.IPV4 |
+-----+-----+
| eccouncil.net       | 208.91.197.27  |
+-----+-----+
| eccouncil.org       | 104.18.21.251  |
+-----+-----+
| eccouncil.com       | 104.18.25.244  |
+-----+-----+
| eccouncil.in        | 34.102.136.180 |
+-----+-----+
| eccouncil.ir        | 94.232.173.162 |
+-----+-----+
| eccouncil.cz        | 89.185.225.244 |
+-----+-----+
| eccouncil.us        | 208.91.197.27  |
+-----+-----+
| eccouncil.tv        | 66.129.123.226 |
+-----+-----+
| eccouncil.cf        | 195.20.52.168  |
+-----+-----+
| eccouncil.cn        | 107.161.26.30  |
+-----+-----+
| eccouncil.co        | 172.67.170.166 |
+-----+-----+
| eccouncil.me        | 34.102.136.180 |
+-----+-----+
☰ Menu ⌂ domainfy -n eccouncil -...
```

```
Applications Places System domainfy -n eccouncil -t all - Parrot Terminal
File Edit View Search Terminal Help
| eccouncil.biz       | 34.102.136.180  |
+-----+-----+
| eccouncil.academy   | 208.91.197.27  |
+-----+-----+
| eccouncil.training   | 208.91.197.27  |
+-----+-----+
| eccouncil.tel        | 52.50.143.27  |
+-----+-----+
| eccouncil.exposed    | 208.91.197.27  |
+-----+-----+
| eccouncil.institute  | 172.67.188.240 |
+-----+-----+
2022-03-24 01:33:57.036178      You can find all the information collected in the following files:
./profiles.csv

2022-03-24 01:33:57.036249      Finishing execution...

Total time used:      0:00:07.748734
Average seconds/query: 0.00891684004602992 seconds

Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
https://github.com/i3visio/osrfframework/issues
Note that otherwise, we won't know about it!
```

7. Use **searchfy** to check for the existence of a given user details on different social networking platforms such as Github, Instagram and Keyserverubuntu. Type **searchfy -q "target user name or profile name"** (here, the target user name or profile is **Tim Cook** and it is searched in all the social media platforms) and press **Enter**.

**Note:** **-q:** specifies the query or list of queries to be performed.

The screenshot shows a terminal window titled 'searchfy -q "Tim Cook" - Parrot Terminal'. The terminal window is located on a desktop environment with a dark background. The window title bar includes the application menu icon, window control buttons (red, green, blue), the title 'searchfy -q "Tim Cook" - Parrot Terminal', and the date/time 'Thu Mar 24, 01:40'. The menu bar contains 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal itself has a black background with white text. It displays the command '#searchfy -q "Tim Cook"' followed by a large amount of output that is mostly illegible due to the terminal's scrollback feature. The bottom of the terminal window shows the status bar with 'Menu' and the same search query 'searchfy -q "Tim Cook" ...'. The desktop icons visible include a trash can, a file folder, and a network icon.

8. The **searchfy** will search the user details in the social networking platforms and will provide you with the existence of the user. These profile links of the target user can be used by the attackers to perform social engineering attacks.

## Module 02 – Footprinting and Reconnaissance

The image shows two terminal windows side-by-side, both titled "searchfy -q 'Tim Cook' - Parrot Terminal". The top window displays search results from i3visio, while the bottom window displays results from KeyServerUbuntu.

**Top Terminal (i3visio Results):**

Source	User	Link	Notes
com.i3visio.Platform	com.i3visio.Alias	com.i3visio.Email	com.i3visio.URI com.i3visio.Domain
Github	timothyfcook	https://github.com/timothyfcook	N/A
Github	cookieguru	https://github.com/cookieguru	N/A
Github	twcook	https://github.com/twcook	N/A
Github	timjcook	https://github.com/timjcook	N/A
Github	TimEnglart	https://github.com/TimEnglart	N/A

**Bottom Terminal (KeyServerUbuntu Results):**

Source	User	Link	Notes
KeyServerUbuntu	tim	https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=index&search=tim@openparadigms.com	tim@openparadigms.com openparadigms.com
KeyServerUbuntu	tim	https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=index&search=tim@trcooke.co.uk	tim@trcooke.co.uk trcooke.co.uk
KeyServerUbuntu	ahughes2005	https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=index&search=ahughes2005@gmail.com	ahughes2005@gmail.com gmail.com
KeyServerUbuntu	ahughes	https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=index&search=ahughes@ndaviess.k12.in.us	ahughes@ndaviess.k12.in.us ndaviess.k12.in.us
KeyServerUbuntu	adedina	https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=index&search=adedina@ndaviess.k12.in.us	adedina@ndaviess.k12.in.us ndaviess.k12.in.us
KeyServerUbuntu	algraber	https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=index&search=algraber@ndaviess.k12.in.us	algraber@ndaviess.k12.in.us ndaviess.k12.in.us
KeyServerUbuntu	asutton	https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=index&search=asutton@ndaviess.k12.in.us	asutton@ndaviess.k12.in.us ndaviess.k12.in.us

```

Applications Places System searchfy -q "Tim Cook" - Parrot Terminal
searchfy -q "Tim Cook" - Parrot Terminal
| KeyServerUbuntu | twcook
ex&search=twcook@shaw.ca
|
+-----+
| KeyServerUbuntu | pourhaus
ex&search=pourhaus@gmail.com
|
+-----+
| KeyServerUbuntu | 923350
ex&search=923350@ican.net
|
+-----+
2022-03-24 01:37:13.491782      You can find all the information collected in the following files:
./profiles.csv
2022-03-24 01:37:13.491893      Finishing execution...
Total time used:      0:00:03.132000
Average seconds/query: 3.132 seconds

Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!

```

9. Similarly, you can use following OSRFramework packages to gather more information about the target:
  - **usufy** - Gathers registered accounts with given usernames.
  - **mailfy** – Gathers information about email accounts
  - **phonefy** – Checks for the existence of a given series of phones
  - **entify** – Extracts entities using regular expressions from provided URLs
10. This concludes the demonstration of gathering information about the target user aliases from multiple social media platforms using OSRFramework.
11. Close all open windows and document all the acquired information.

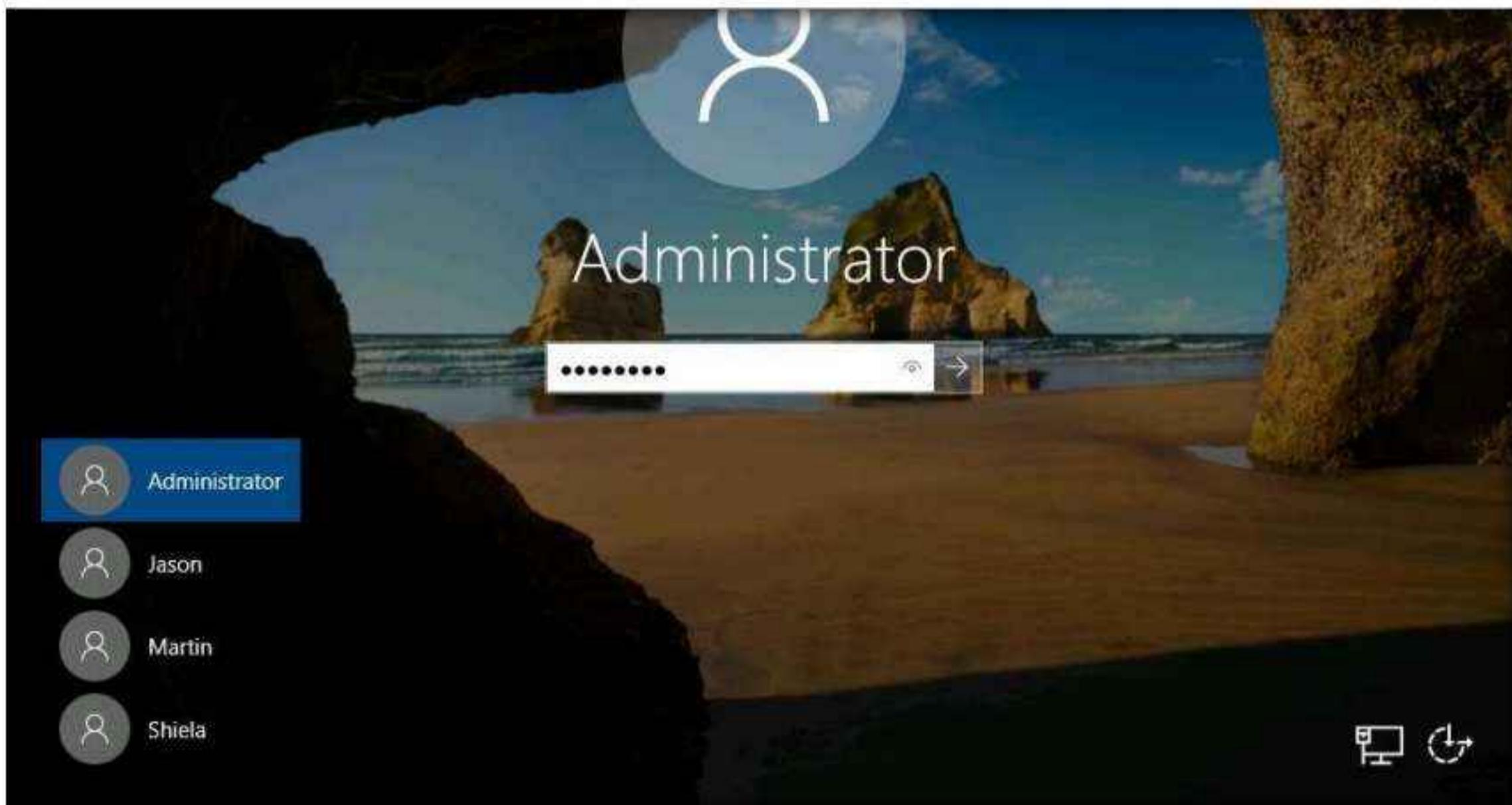
## Task 4: Footprinting a Target using FOCA

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and hidden information in scanned documents. These documents are searched for using three search engines: Google, Bing, and DuckDuckGo. The results from the three engines amounts to a lot of documents. FOCA examines a wide variety of records, with the most widely recognized being Microsoft Office, Open Office and 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.

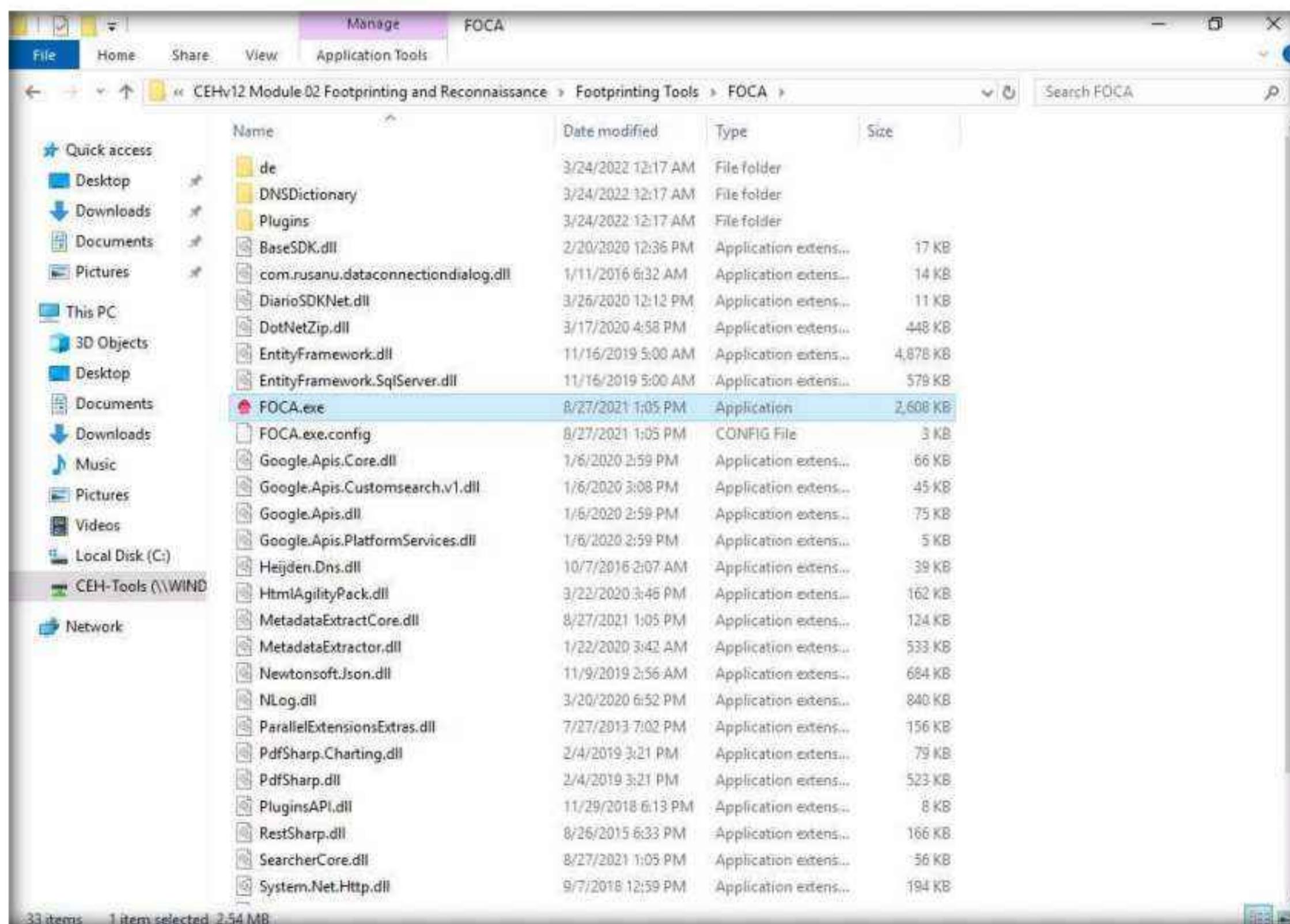
## Module 02 – Footprinting and Reconnaissance

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. In the **Windows Server 2019** virtual machines, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

**Note:** Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

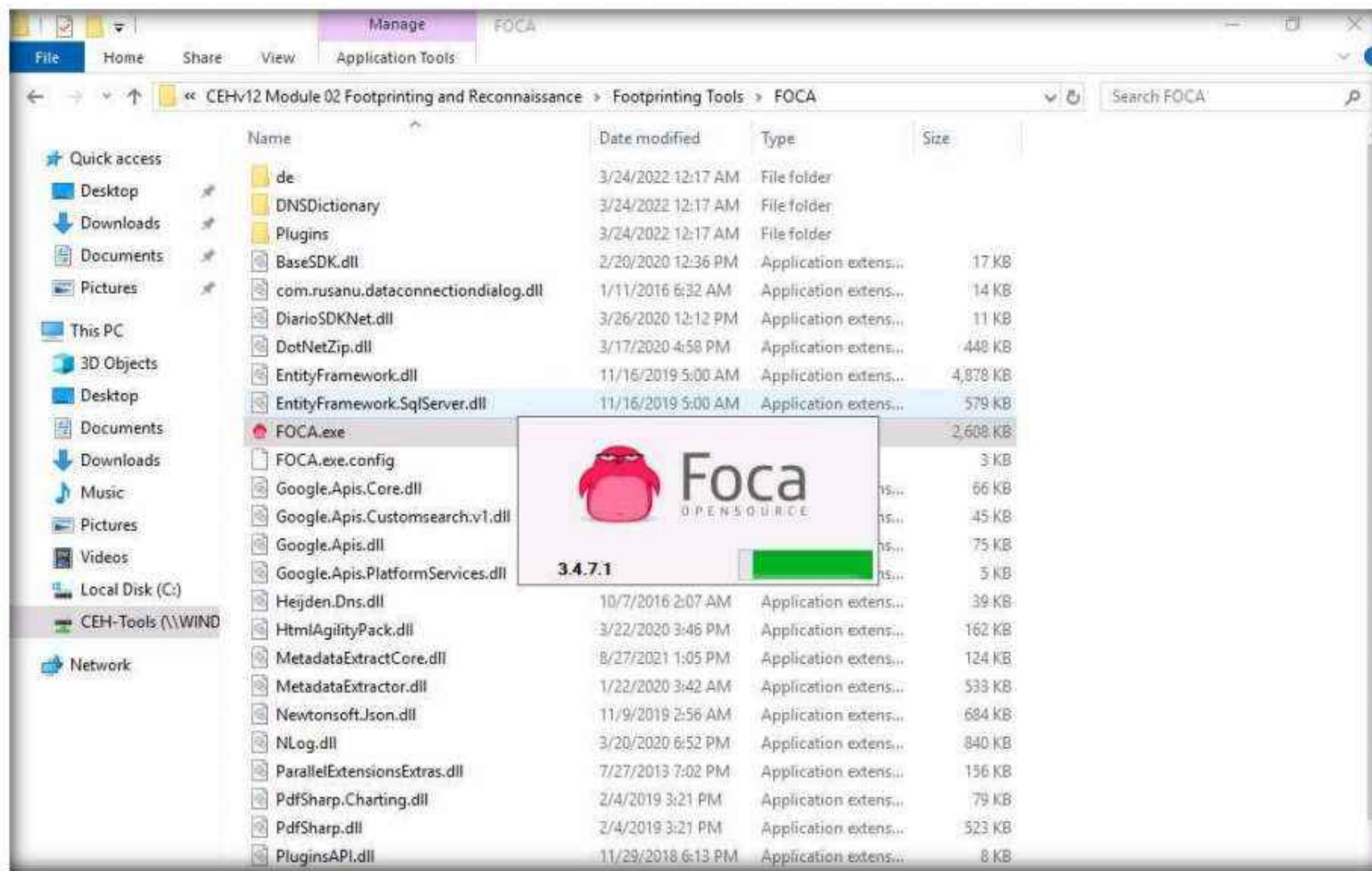


3. To launch FOCA, navigate to **Z:\CEHv12 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA** and double-click **FOCA.exe**.

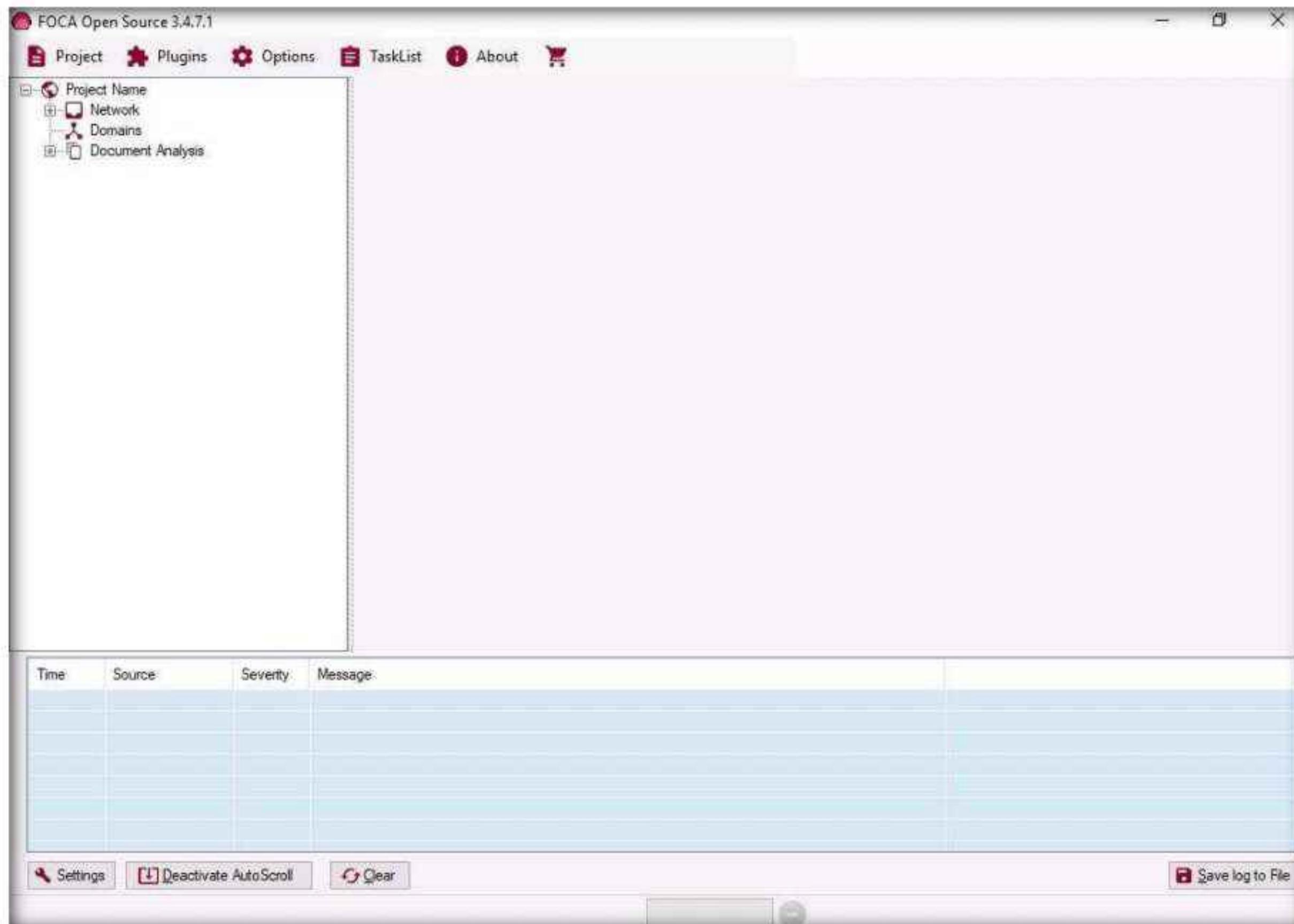


## Module 02 – Footprinting and Reconnaissance

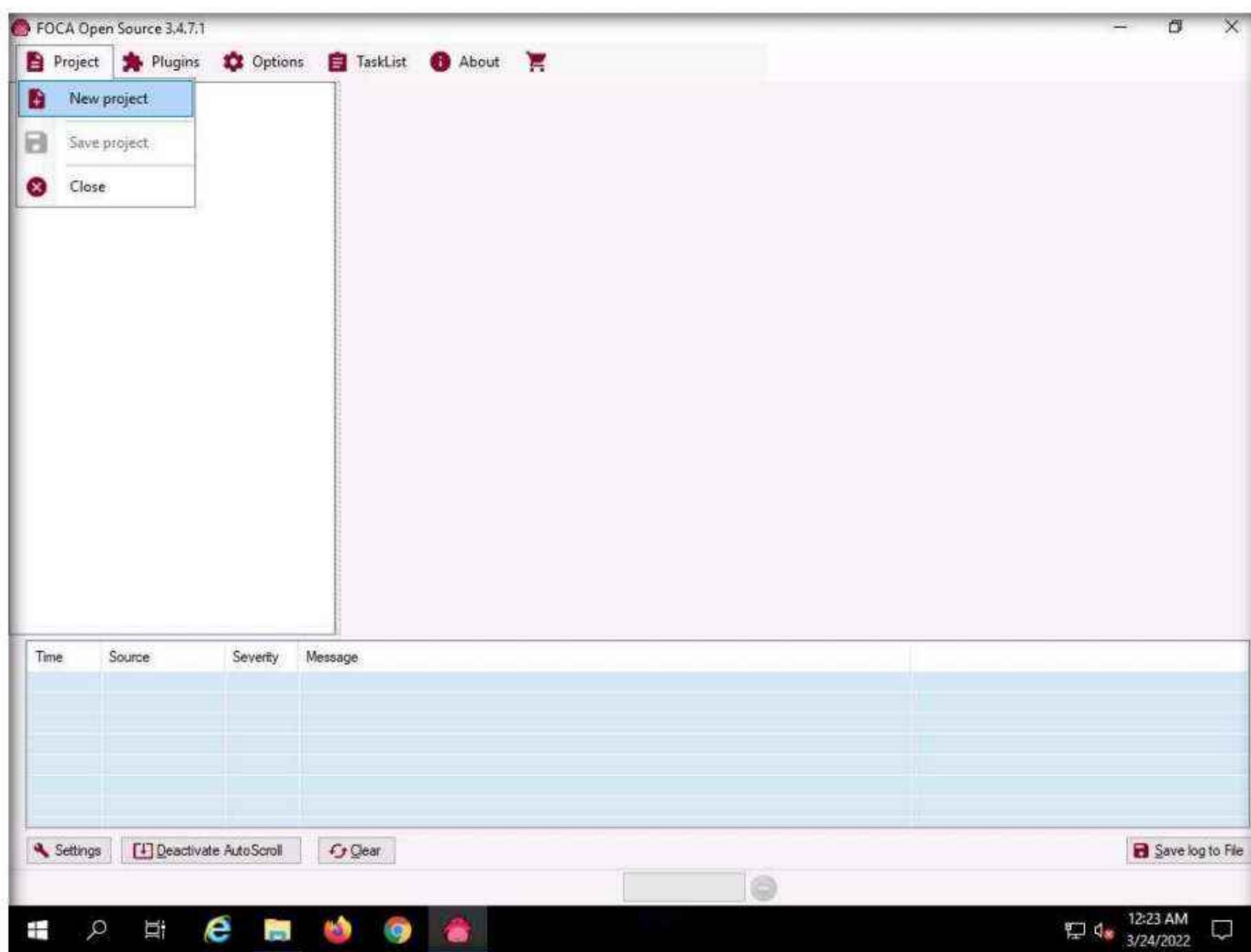
4. The FOCA dialog-box appears, wait for the initialization to complete.



5. The FOCA main window appears, as shown in the screenshot



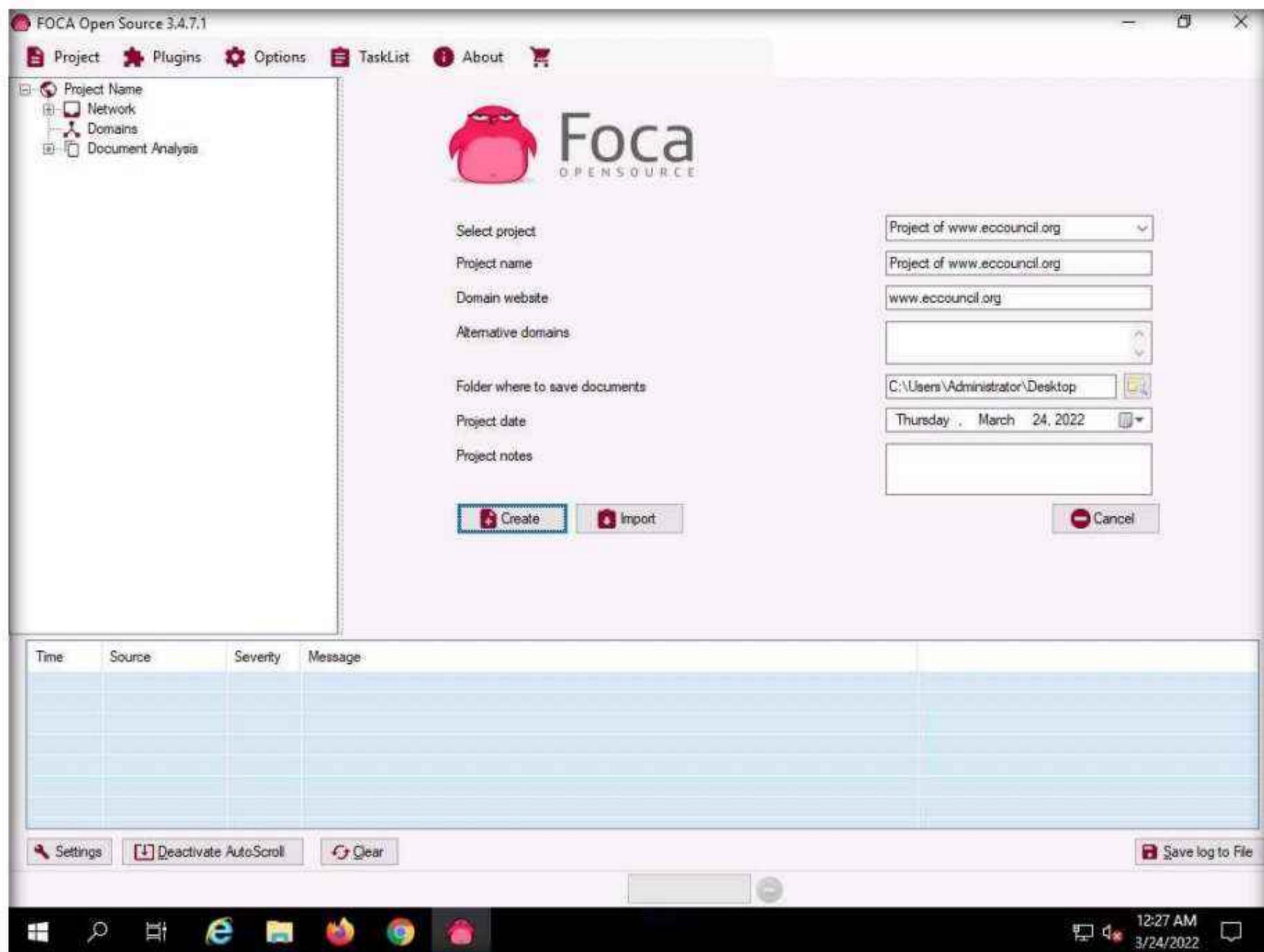
6. Create a new project by navigating to **Project** and click **New project** on the menu bar.



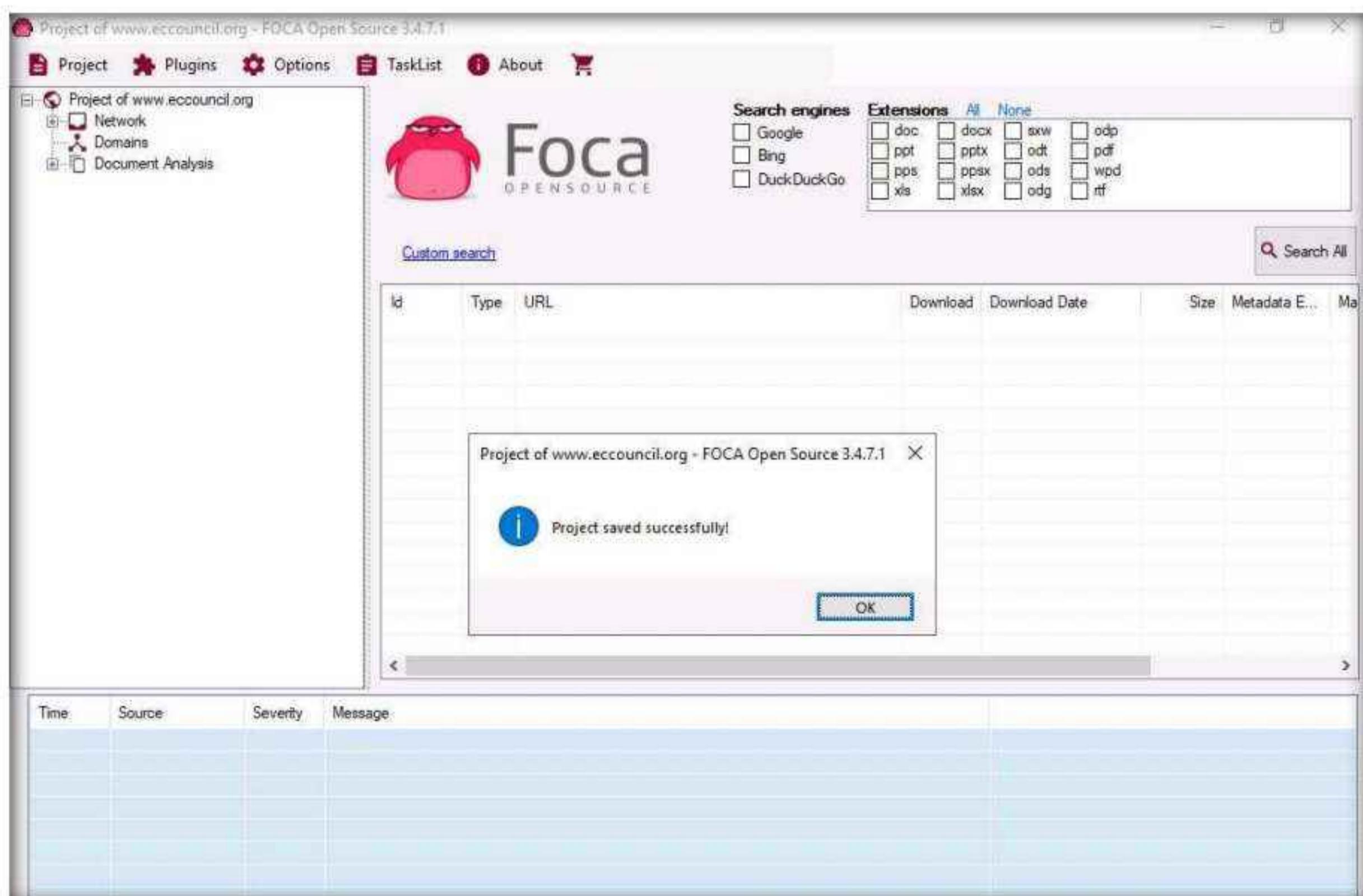
7. The FOCA new project wizard appears, follow the steps below:

- Enter a project name in the **Project name** field (here, **Project of www.eccouncil.org**).
- Enter the domain website in the **Domain website** field (here, **www.eccouncil.org**).
- You can leave the optional **Alternative domains** field empty.
- Under the **Folder where to 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**.
- Leave the other settings to default and click the **Create** button.

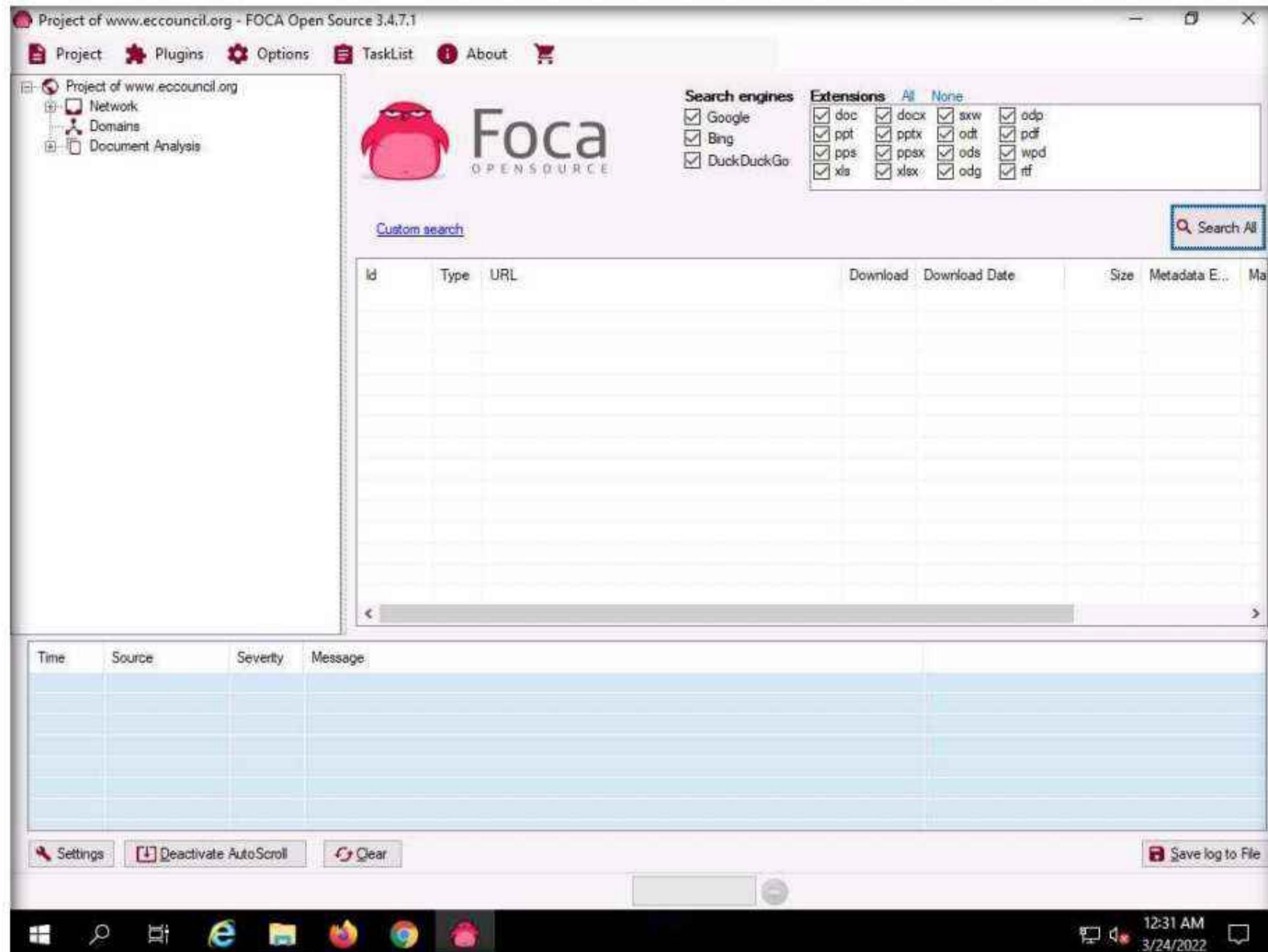
## Module 02 – Footprinting and Reconnaissance



8. The Project saved successfully pop-up appears, click OK to close it.



9. To extract the information of the targeted domain, select all three search engines (**Google**, **Bing**, and **DuckDuckGo**) present under **Search engines** section. Similarly, under **Extensions** section, click **All** option to choose all the given extensions and then click the **Search All** button.



10. The **Search All** button automatically toggles the **Stop** button, and begins gathering information on the target domain in the middle pane.
11. After the scans are completed, 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

## Module 02 – Footprinting and Reconnaissance

The screenshot shows the FOCA Open Source 3.4.7.1 application window. The main area displays a table of search results for the domain www.eccouncil.org. The columns include Id, Type, URL, Download, Download Date, Size, Metadata E., Malware An., and Modified Date. The results show various documents such as PDFs, Word documents, and Powerpoint presentations. Below the results table is a log viewer showing search logs with columns for Time, Source, Severity, and Message. The log entries indicate successful Bing and Google searches and an error message regarding a DuckDuckGo search. At the bottom of the interface, there is a context menu with options like Download, Extract Metadata, Analyze Malware, Delete, etc.

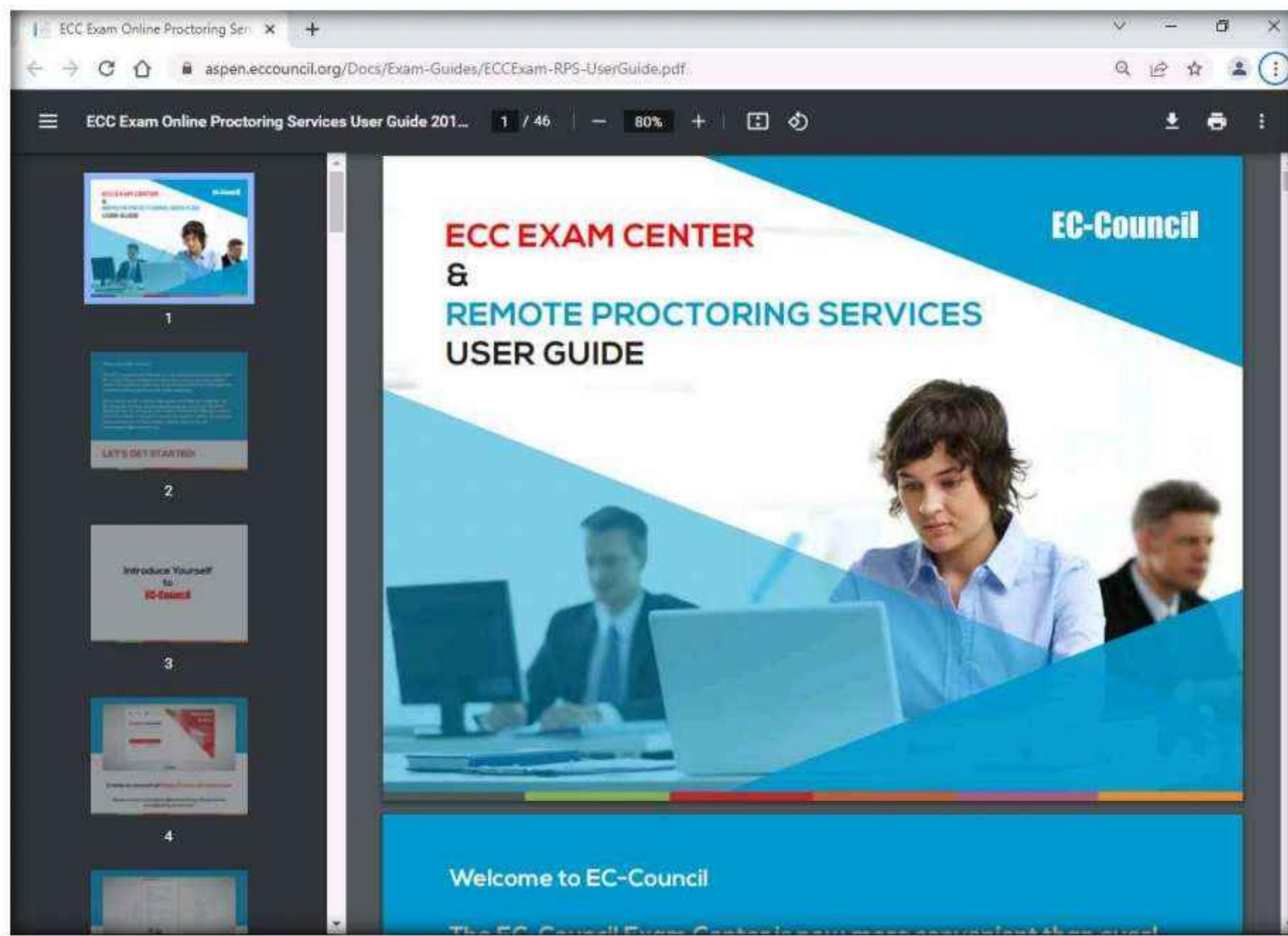
12. To view the file information stored in the sub-domain, right-click on any URL and click **Link(s)** --> **Open in browser** from the context menu.

**Note:** If a **How do you want to open this?** pop up appears, select any web browser (here, **Google Chrome**) and click **OK**.

This screenshot shows the same FOCA interface as the previous one, but with a context menu open over the first item in the results table. The menu is expanded to show options like Download, Extract Metadata, Analyze Malware, Delete, etc. The 'Link(s)' option is highlighted, and a submenu is open, showing 'Open in browser' as the selected option. This indicates that the user has right-clicked on a URL and chosen to open it in their web browser.

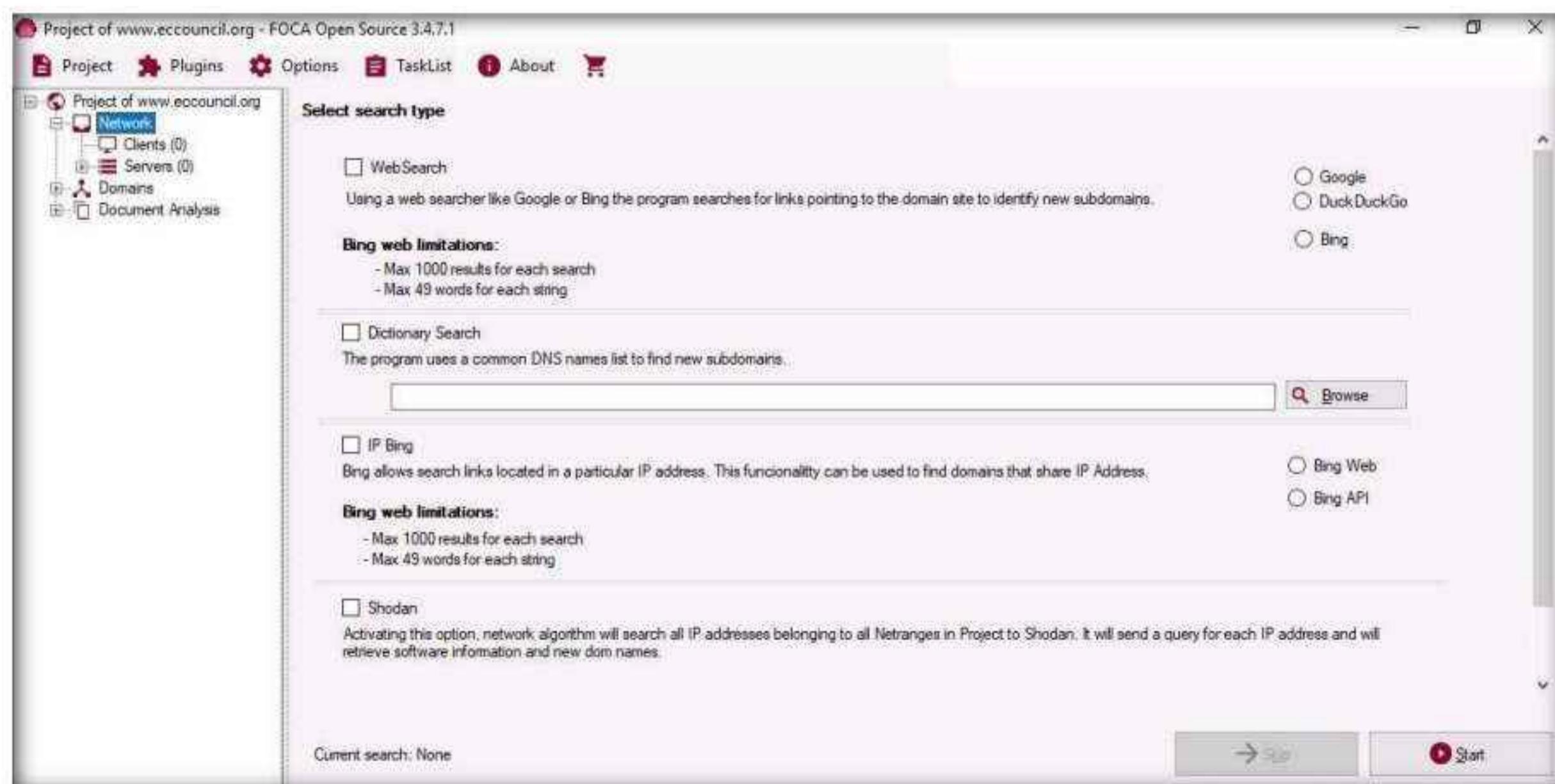
## Module 02 – Footprinting and Reconnaissance

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



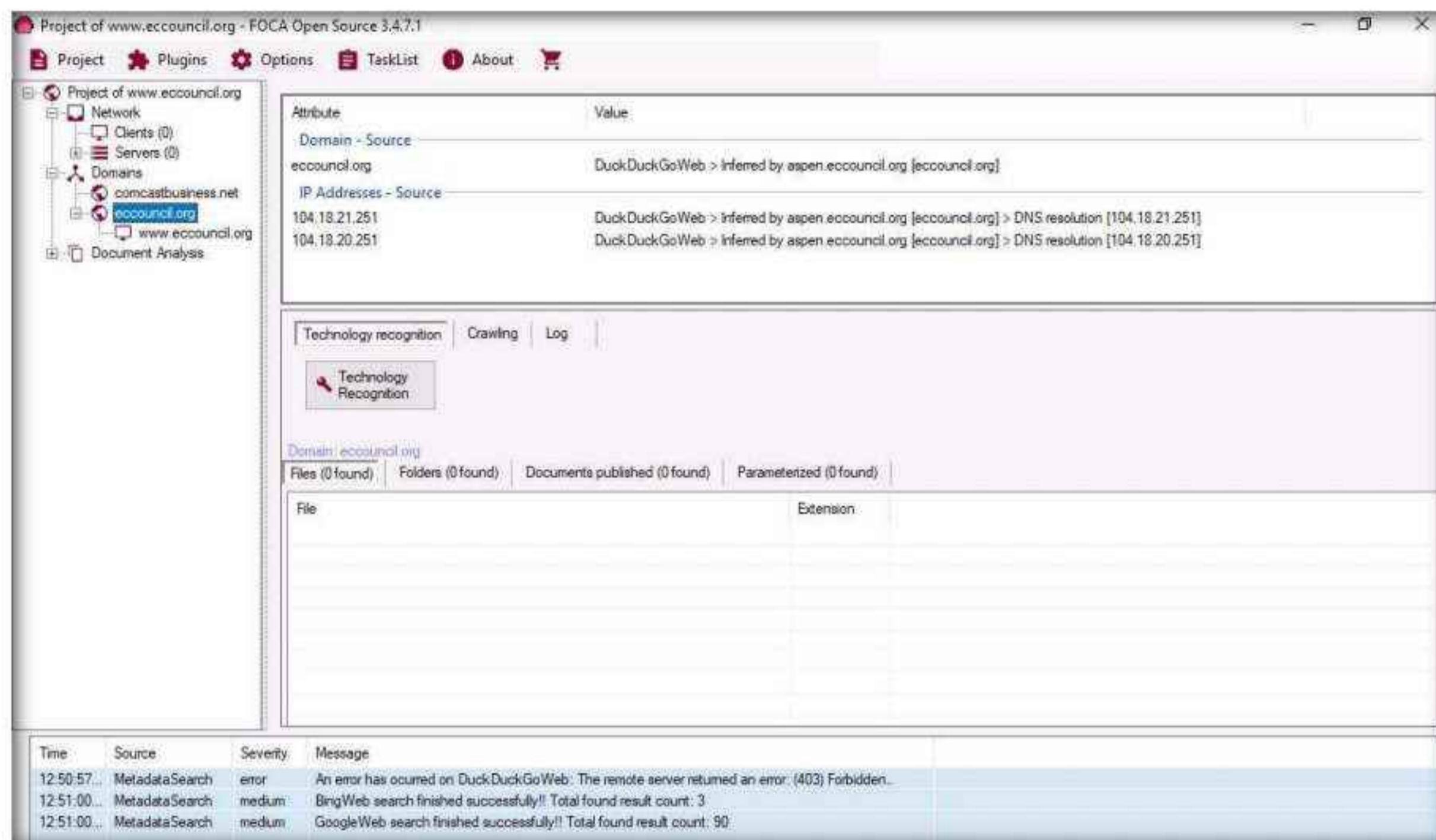
14. Close the web browser.
15. Navigate back to the FOCA window and click the **Network** node to expand the node in the left pane of the window to view the network structure.

**Note:** The domain we used does not have associated clients or servers.



## Module 02 – Footprinting and Reconnaissance

16. If the domain has any of the associated **Clients** or **Servers**, it displays the related information.
17. Expand the **Domains** node and click on the target domain (here, **eccouncil.org**) to view the domain-related information.



18. In the right-pane, click **Crawling** tab and then click **Google** crawling button.

