Module 02: Footprinting and Reconnaissance

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.

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.

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:

1. Perform footprinting through search engines
    - 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

2. Perform footprinting through web services
    - 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
3. Perform footprinting through social networking sites
    - Gather employees' information from LinkedIn using theHarvester
    - Gather personal information from various social networking sites using Sherlock
4. Perform website footprinting
    - 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
5. Perform email footprinting
    - Gather information about a target by tracing emails using eMailTrackerPro
6. Perform Whois footprinting
    - Perform Whois lookup using DomainTools
7. Perform DNS footprinting
    - 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
8. Perform network footprinting
    - Locate the network range
    - Perform network tracerouting in Windows and Linux Machines
9. Perform footprinting using various footprinting tools
    - 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 1: Perform Footprinting Through Search Engines

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

Overview of Search Engines

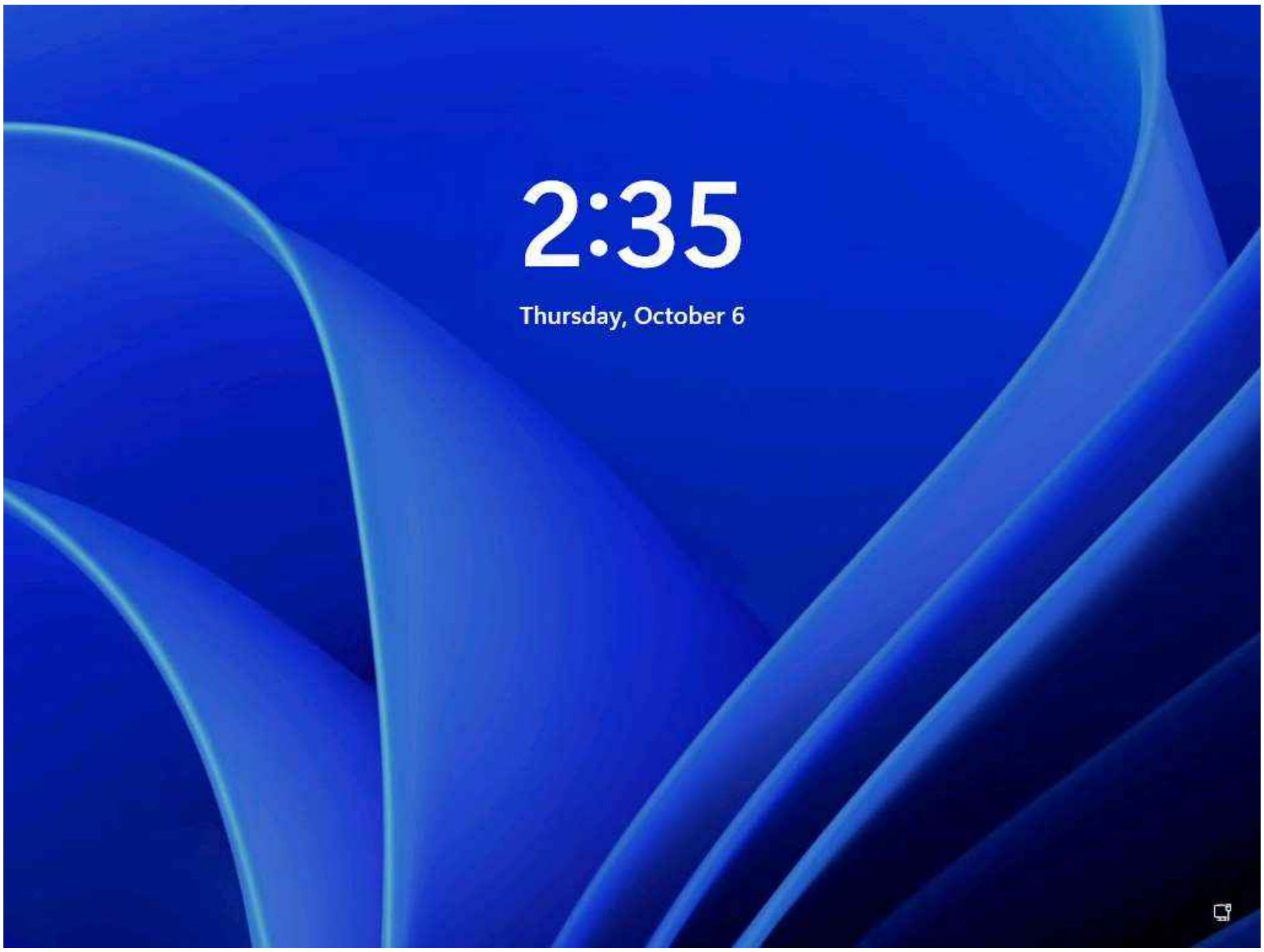
Search engines use crawlers, automated software that continuously scans active websites, and add the retrieved results to the search engine index, which is further stored in a huge database. When a user queries a search engine index, it returns a list of Search Engine Results Pages (SERPs). These results 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.

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.

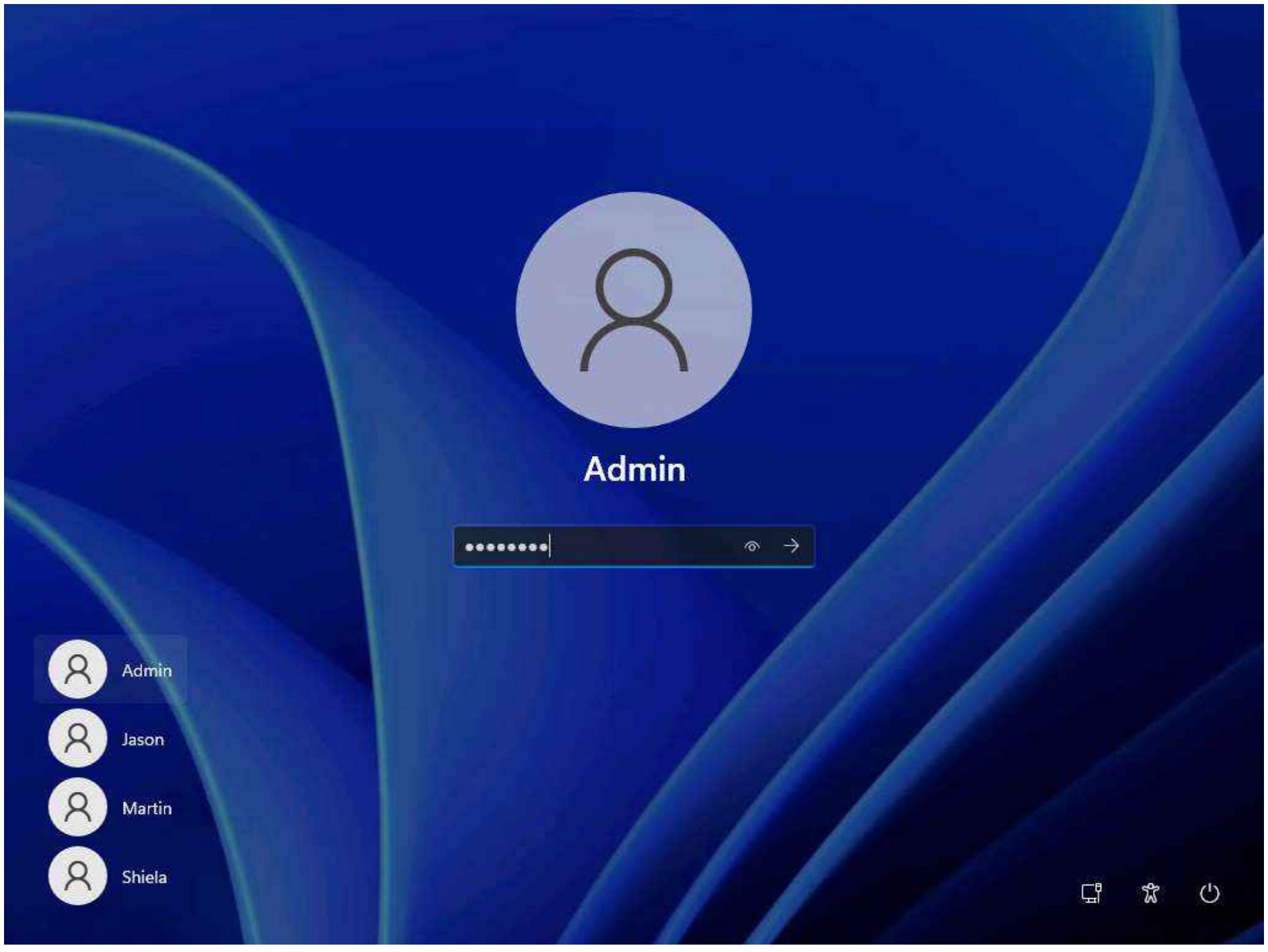
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**.



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.

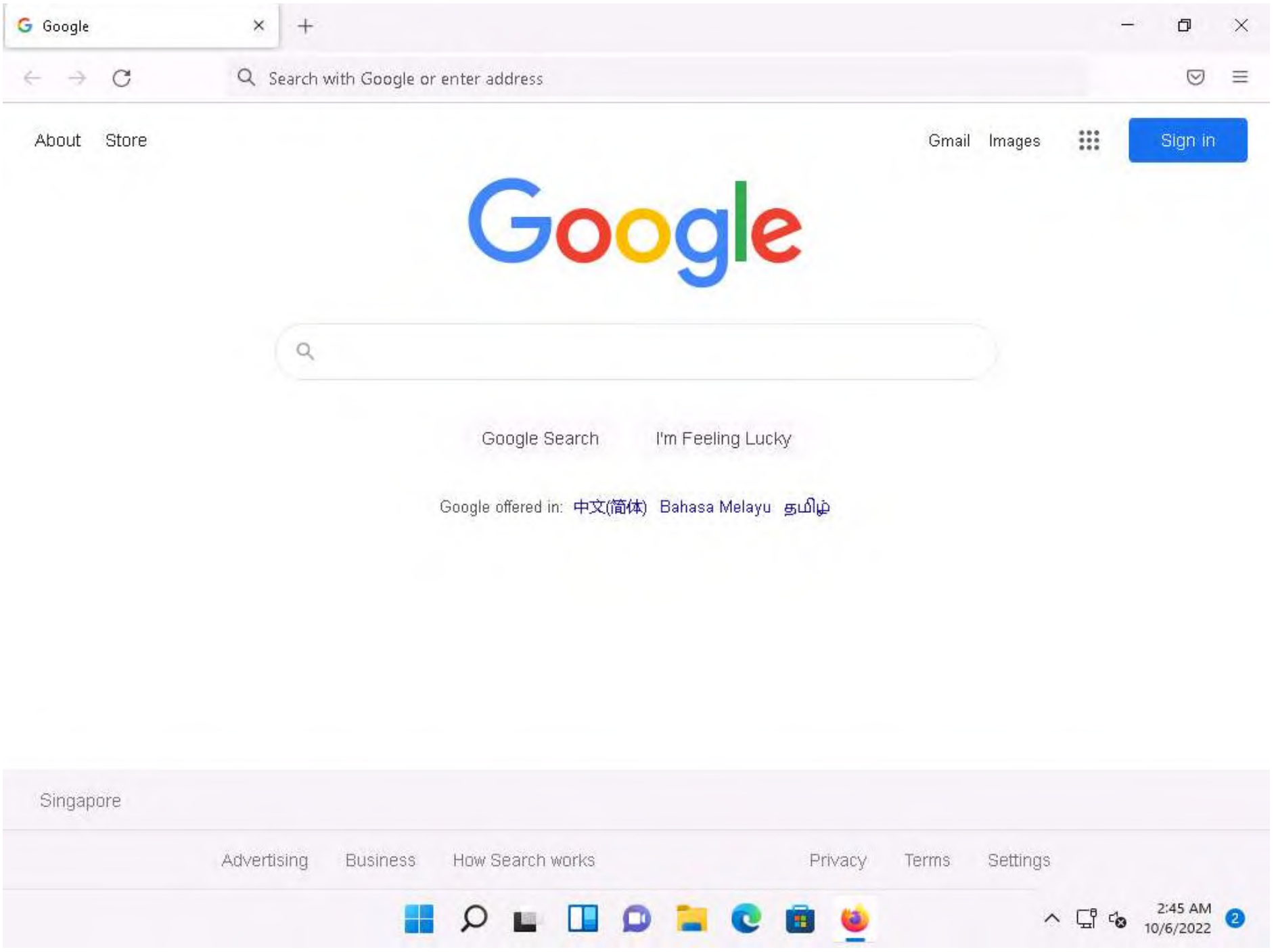


3. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.google.com** and press **Enter**.

> 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.

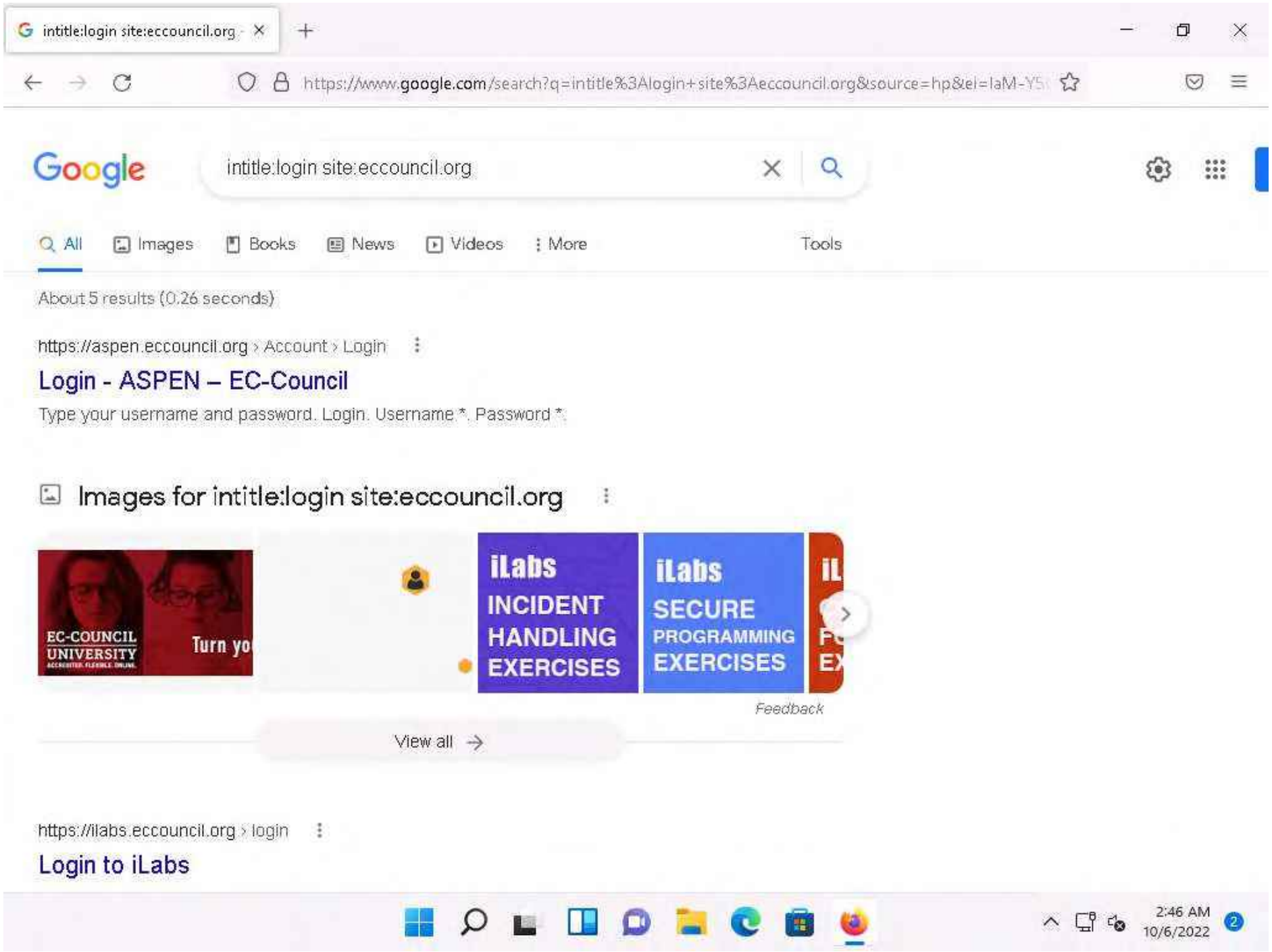
4. Once the **Google** search engine appears, you should see a search bar.

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

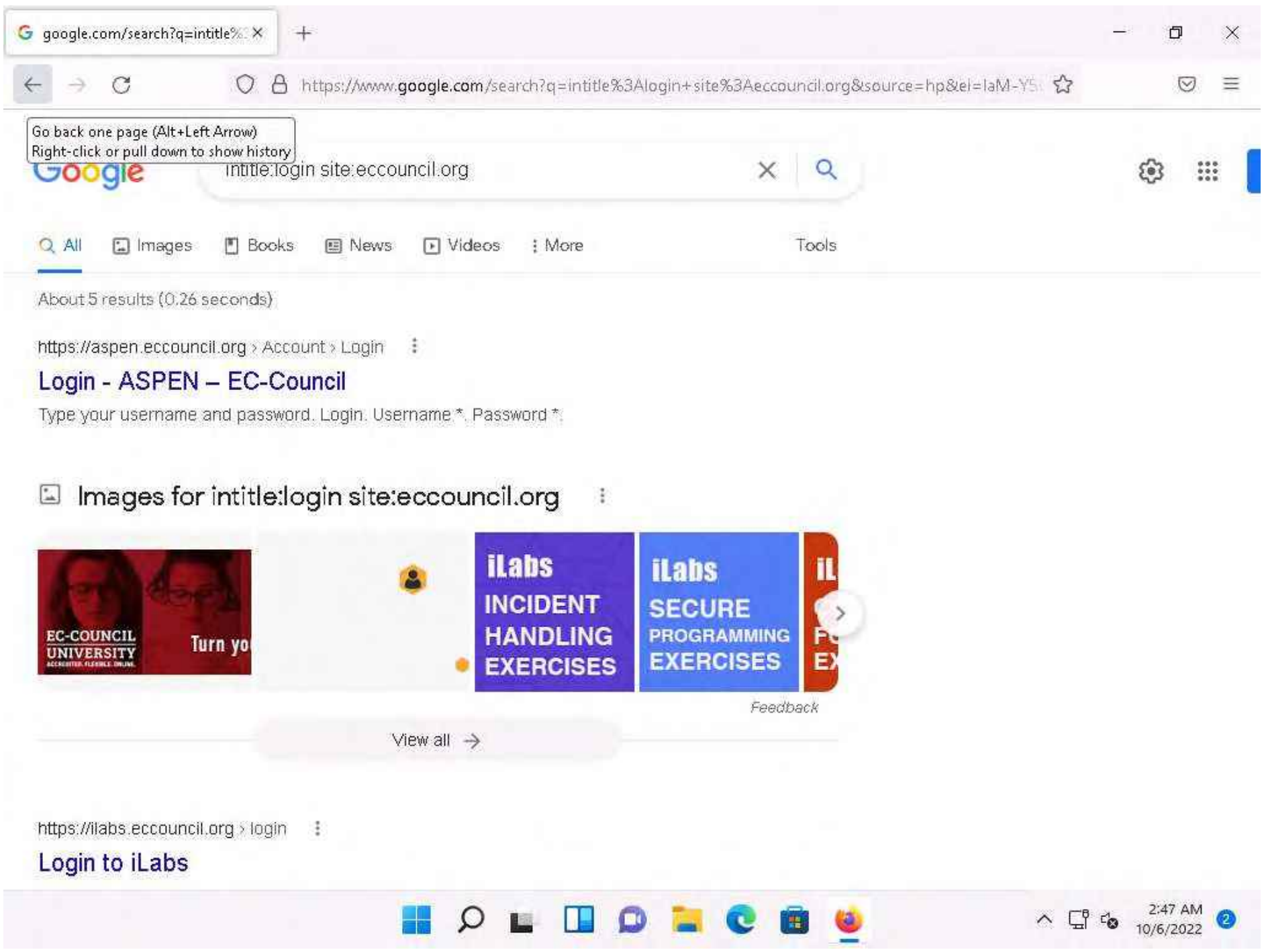


5. Type **intitle:login site:eccouncil.org** and press **Enter**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **eccouncil.org** website that contain the **login** pages. An example is shown in the screenshot below.

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 bruteforcing, injection attacks and other web application attacks. Similarly, assessing the login pages against various attacks is crucial for penetration testing.



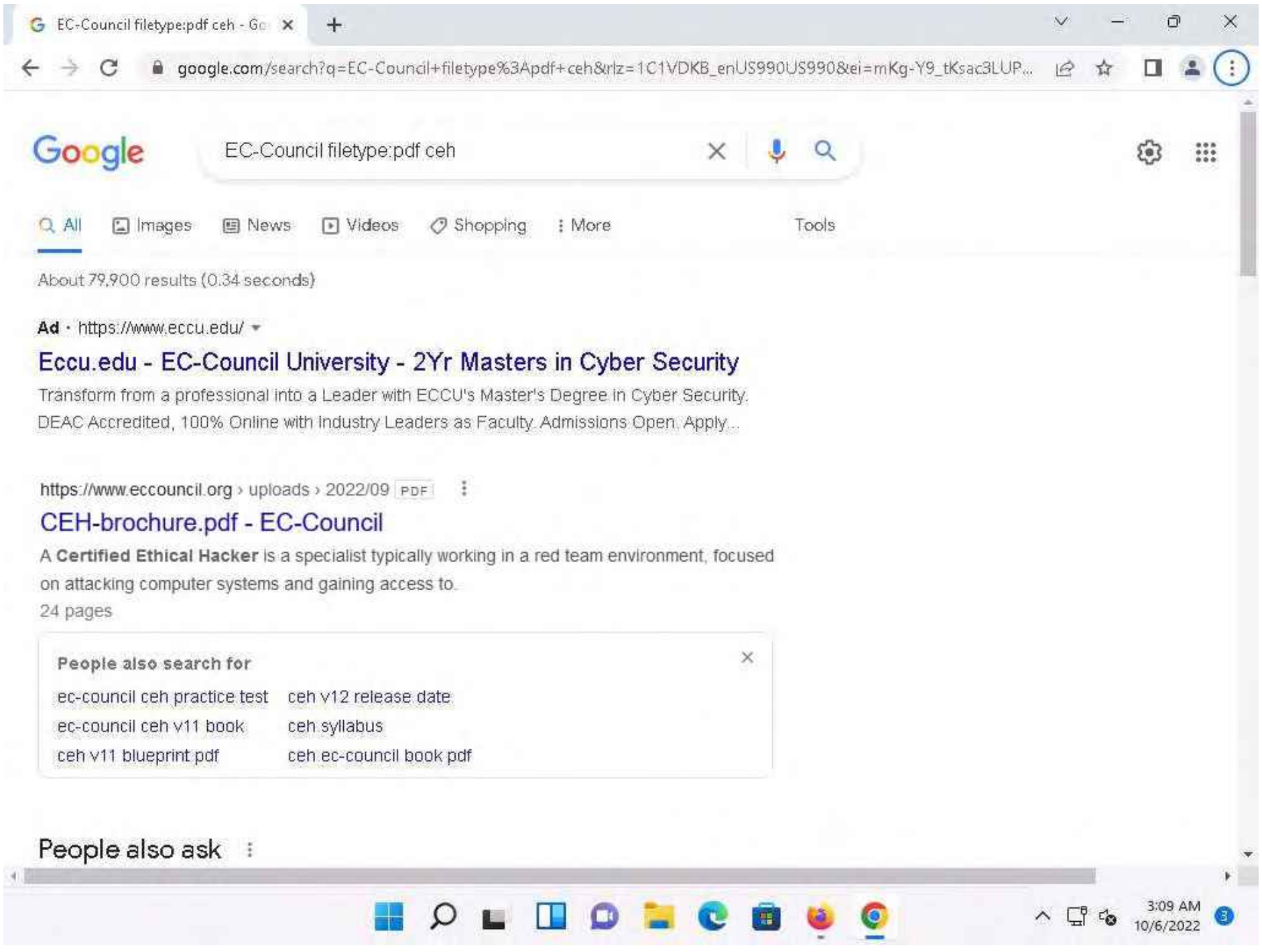
6. Now, click back icon present on the top-left corner of the browser window to navigate back to **https://www.google.com**.



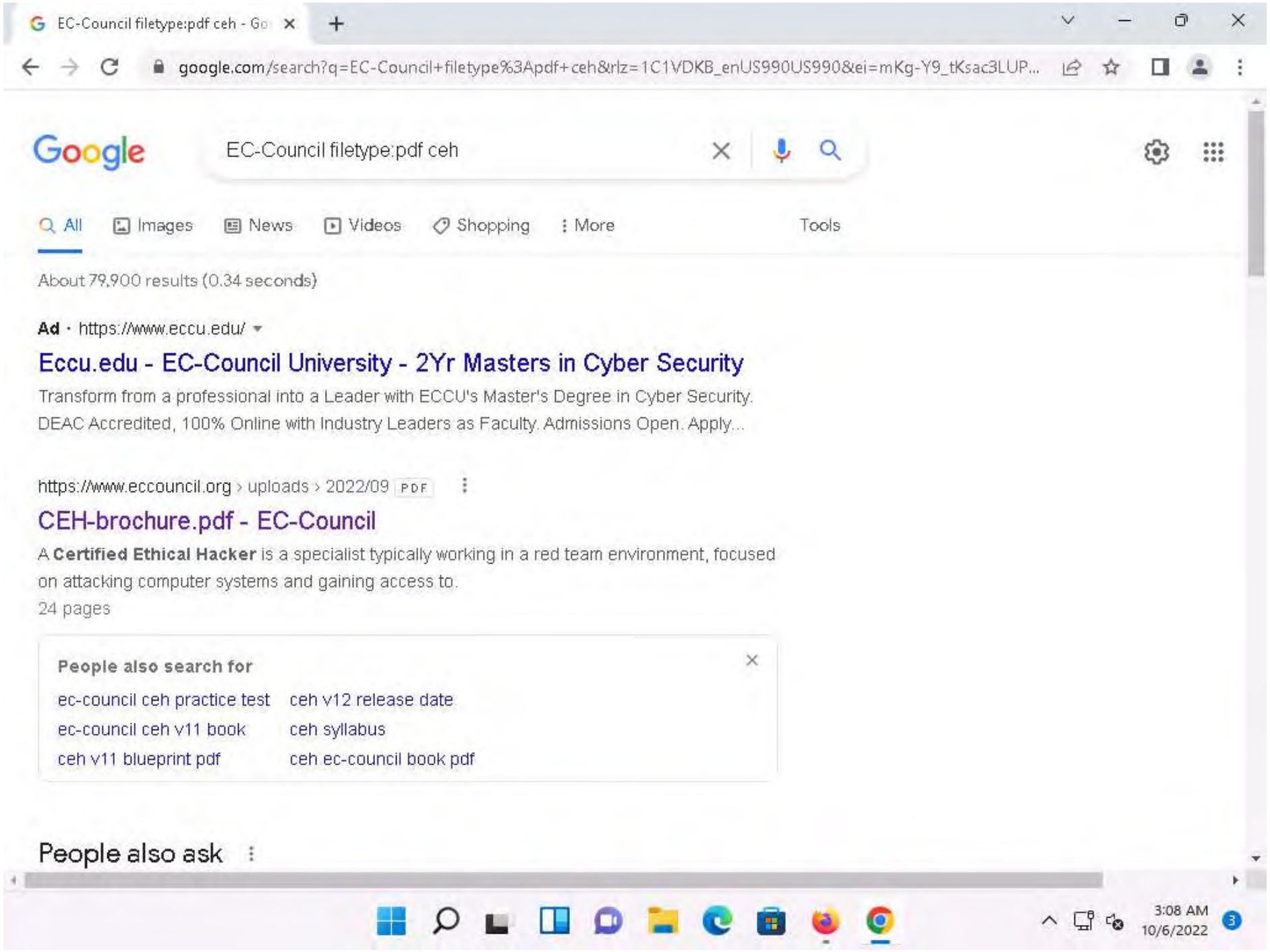
7. In the search bar, type the command **EC-Council filetype:pdf ceh** and press **Enter** to search your results based on the file extension and the keyword (here, **ceh**).

Note: Here, the file type pdf is searched for the target organization EC-Council. The result might differ when you perform this task.

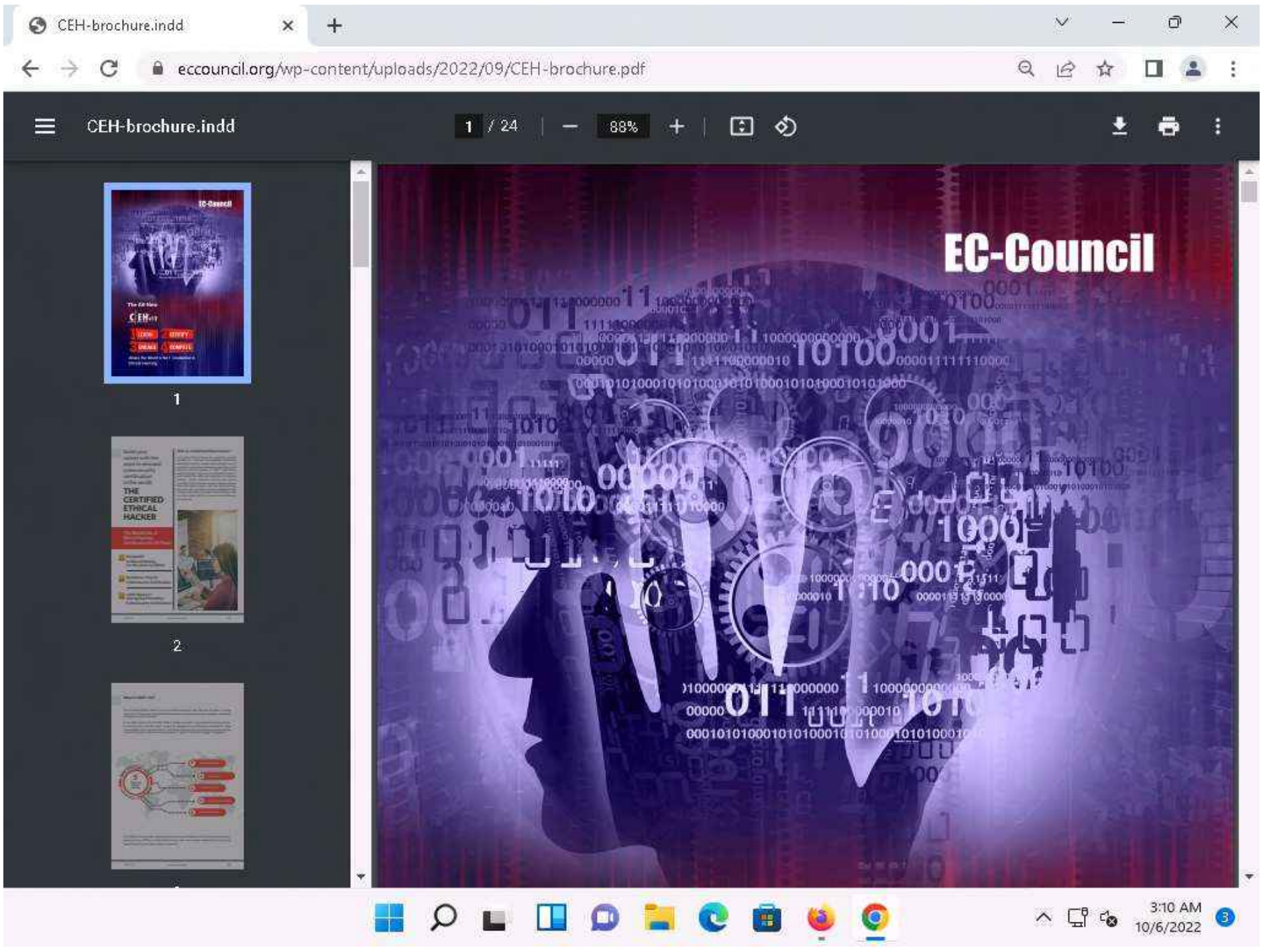
Note: The PDF and other documents from a target website may provide sensitive information about the target's products and services. They may help attackers to determine an attack vector to exploit the target.



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



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



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

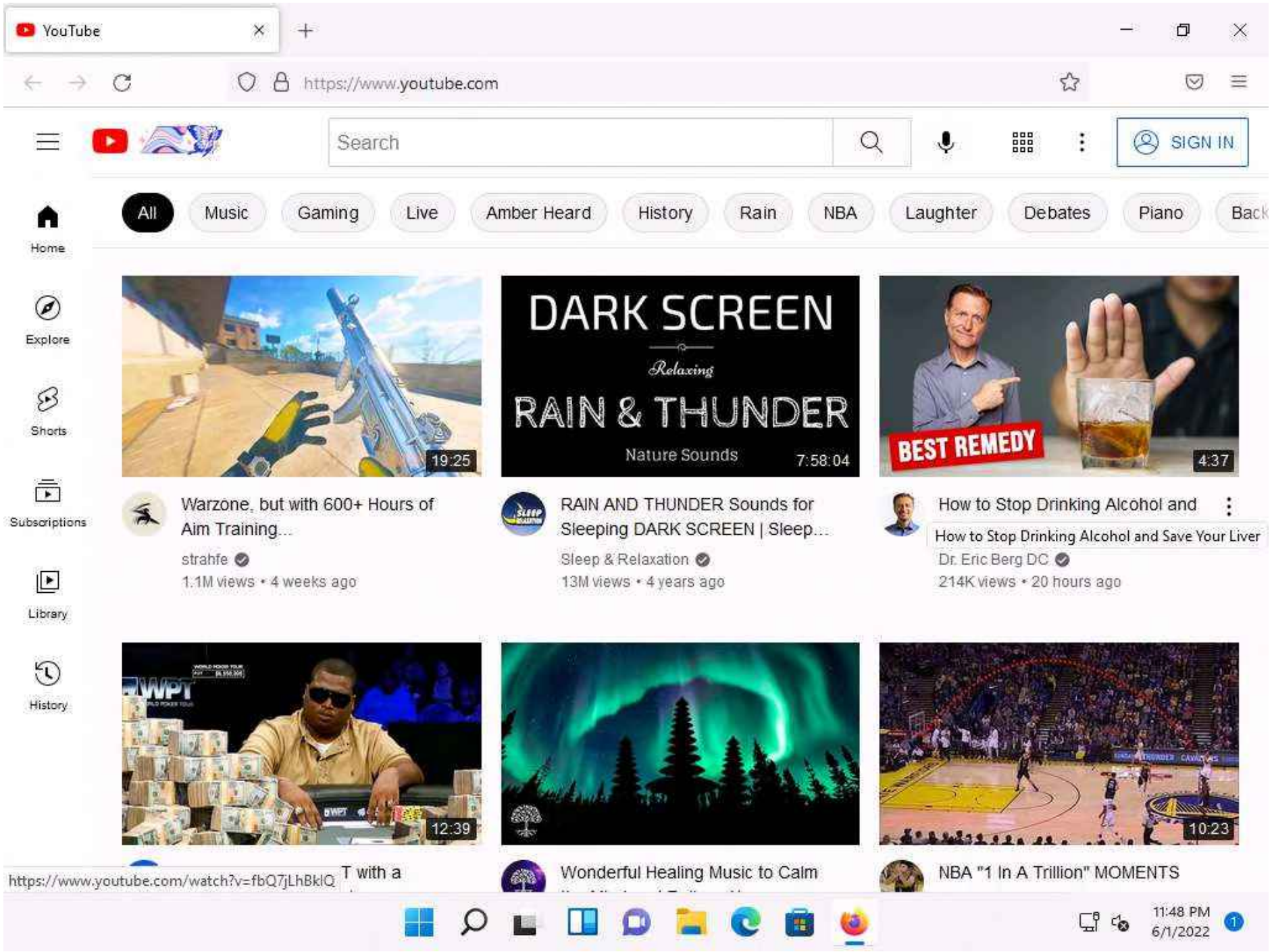
Video search engines are Internet-based search engines that crawl the web looking for video content. These search engines either provide the functionality of uploading and hosting the video content on their own web servers or they can parse the video content, which is hosted externally.

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

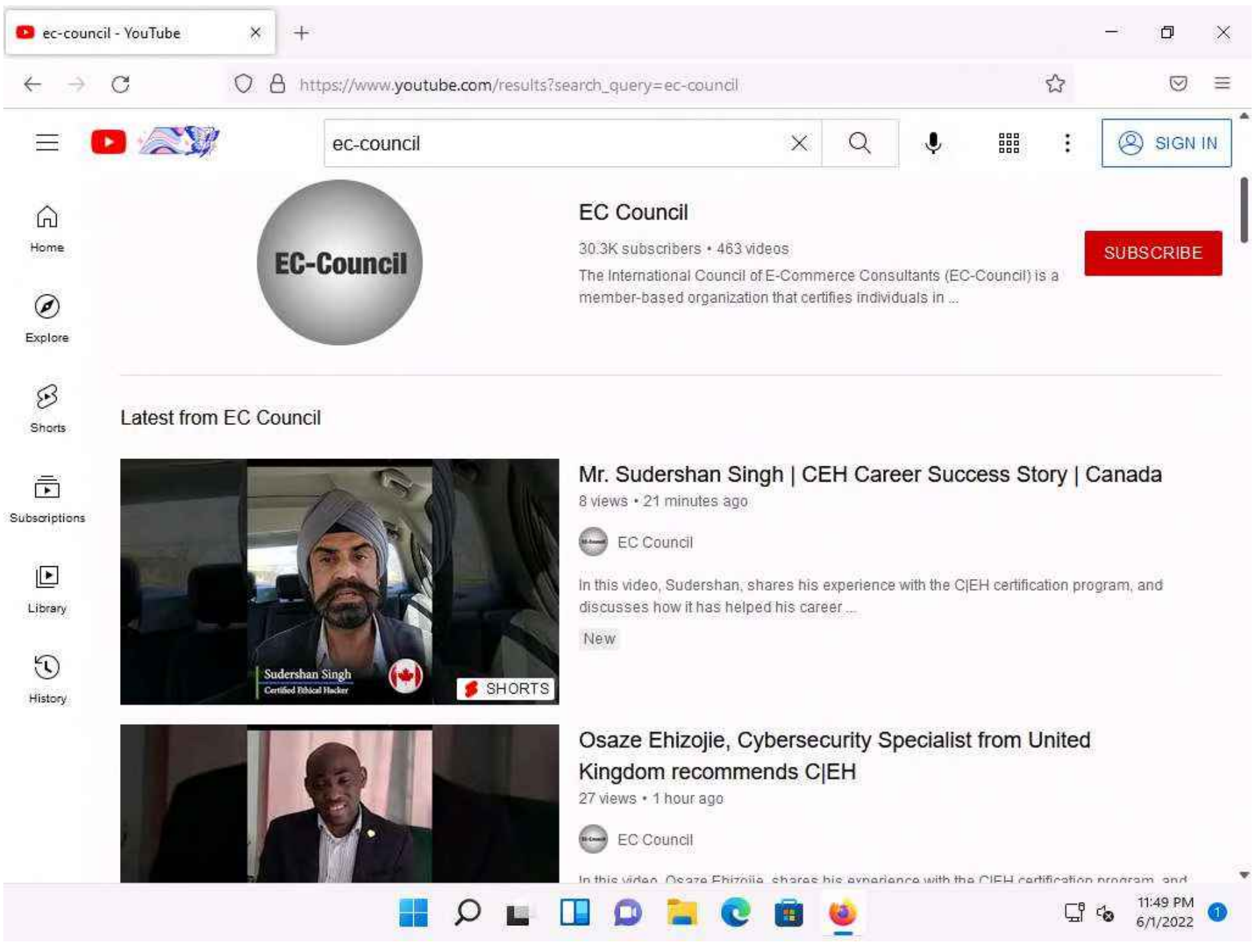
> Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. 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.

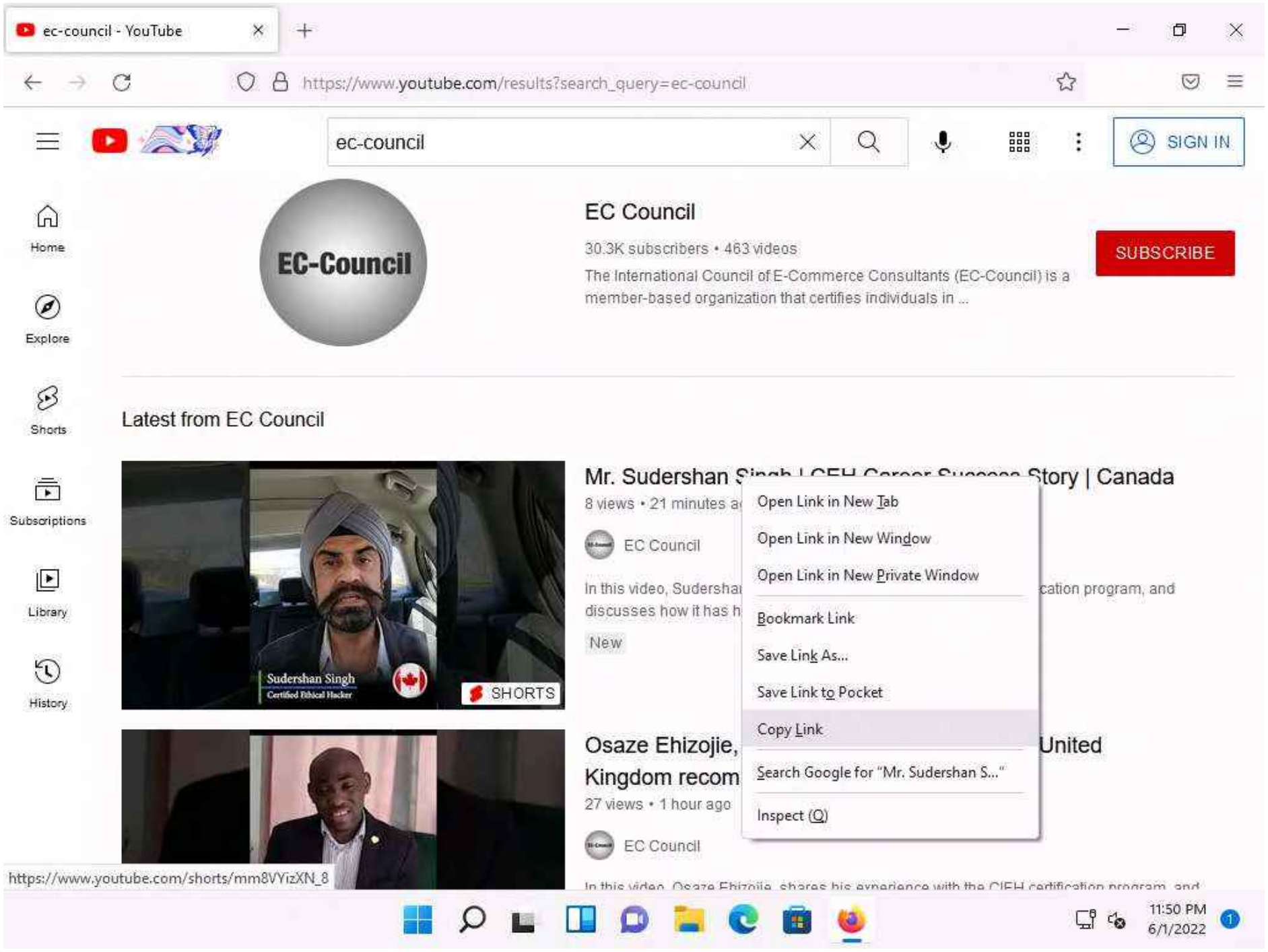
> Note: If you choose to use another web browser, the screenshots will differ.



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.

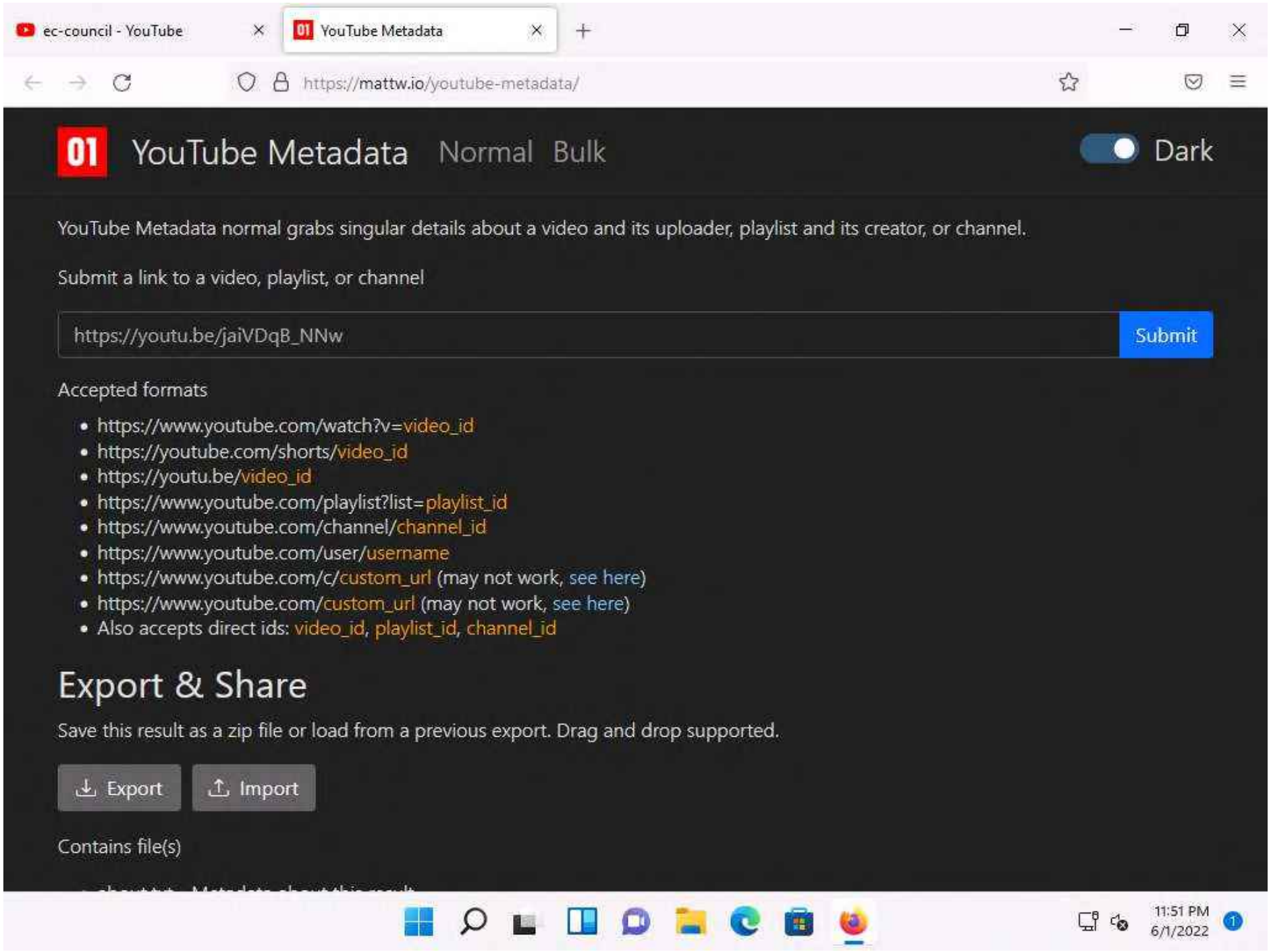


3. Select any video of your choice, right-click on the video title, and click **Copy Link**.

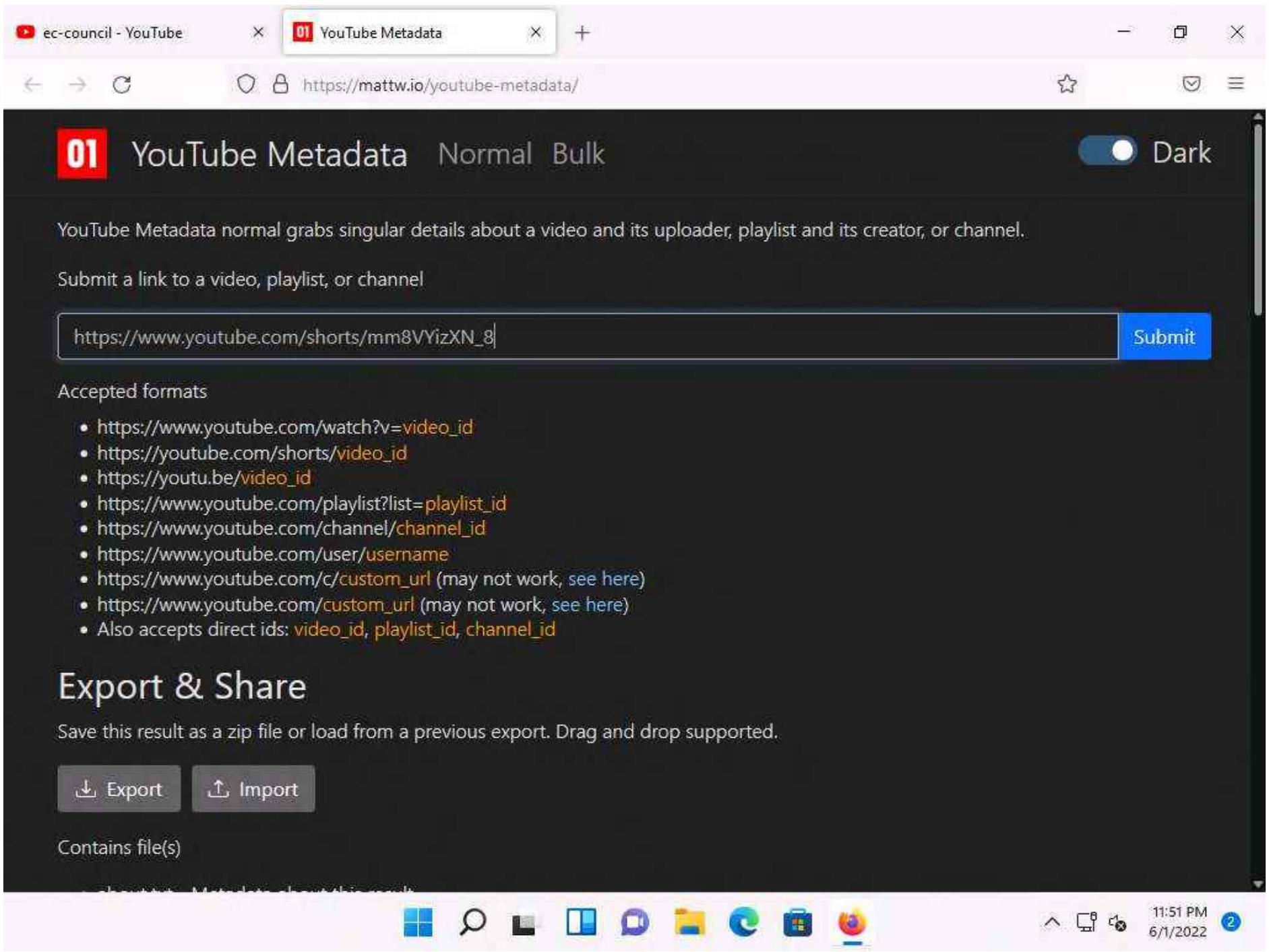


4. After the video link is copied, open a new tab in **Mozilla Firefox**, place your mouse cursor in the address bar and type **https://mattw.io/youtube-metadata/ ** and press **Enter**.

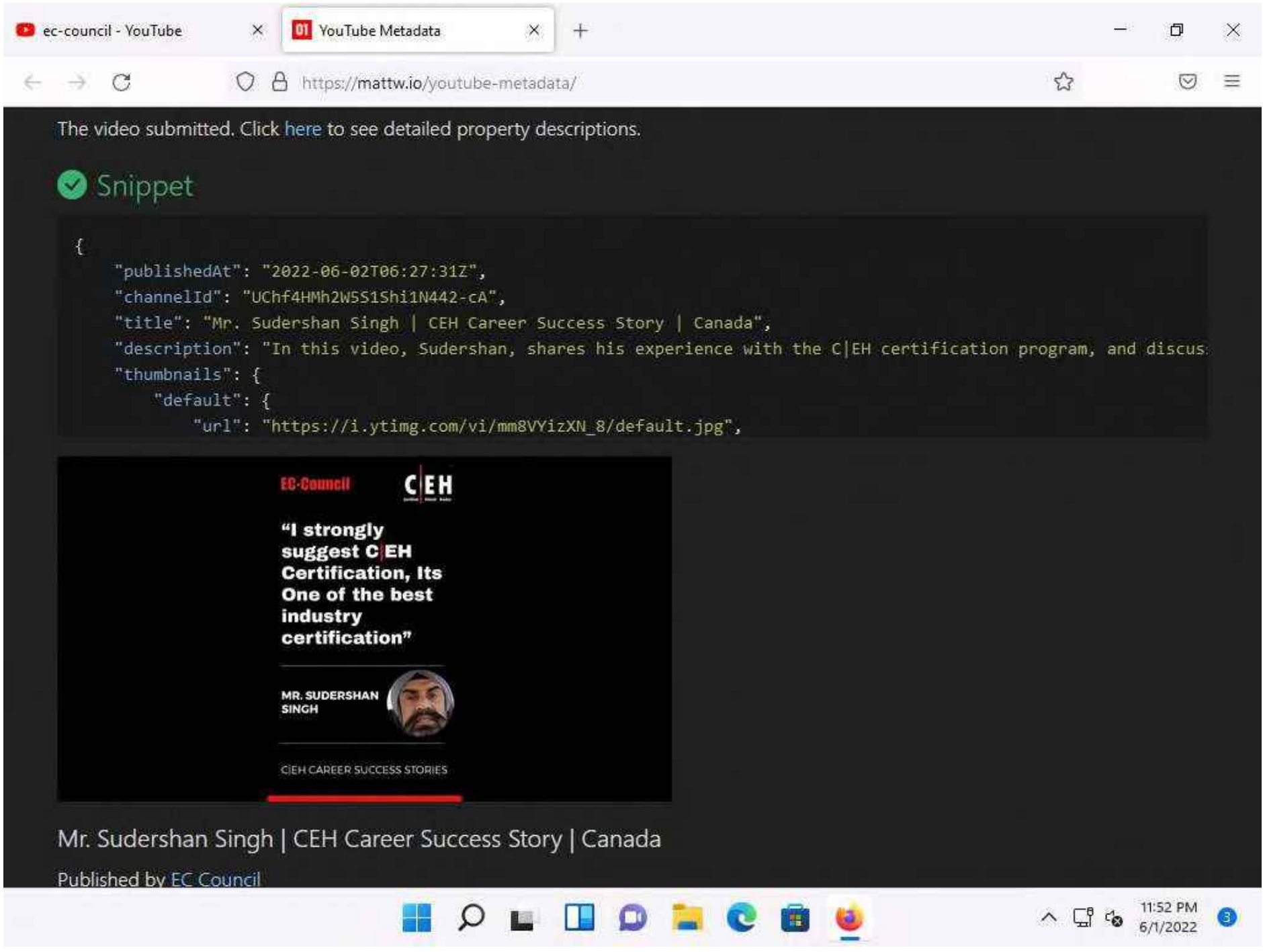
Note: To open a new tab, click **+** icon next to the first tab. Note: **YouTube Metadata** tool collects singular details of a video, its uploader, playlist and its creator or channel.



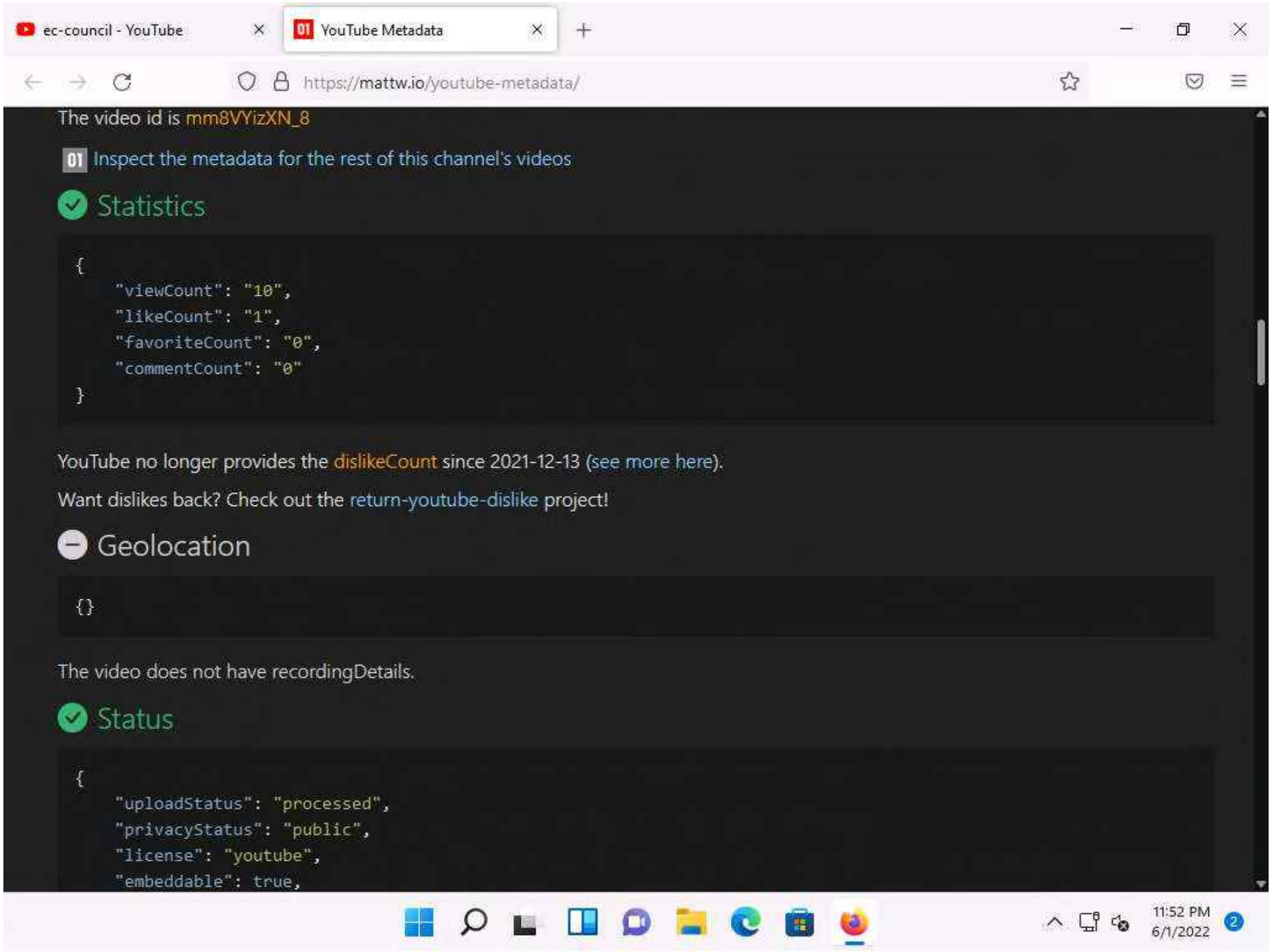
5. **YouTube Metadata** page appears, in the **Submit a link to a video, playlist, or channel** search field, paste the copied YouTube video location and click **Submit**.



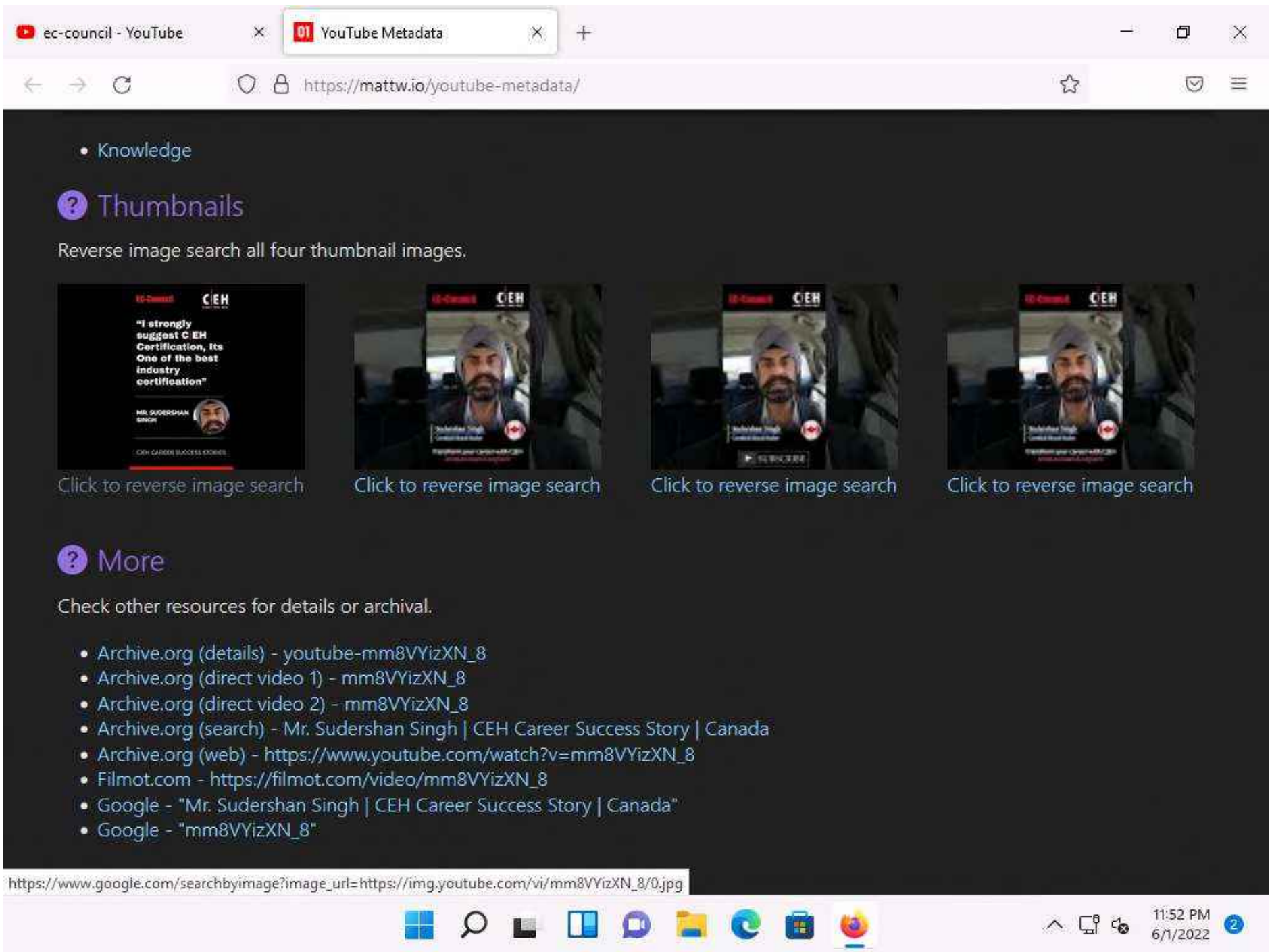
6. Once the search is completed scroll down and you can observe the details related to the video such as **published date and time**, **channel Id**, **title**, etc., in the **Snippet** section.



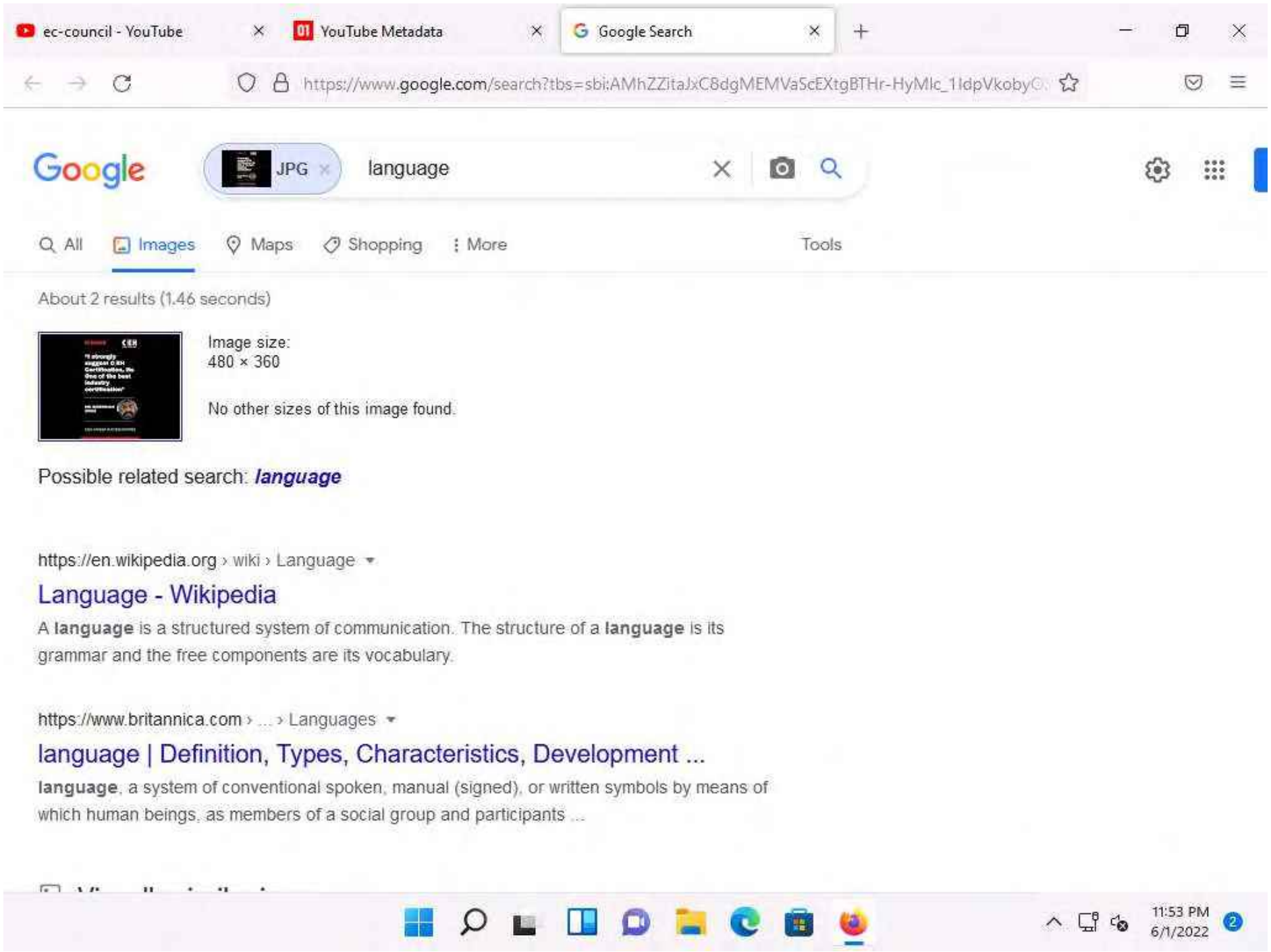
7. Scroll down to check the additional information under the sections **Statistics**, **Geolocation** , and **Status** etc.



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



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



10. 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

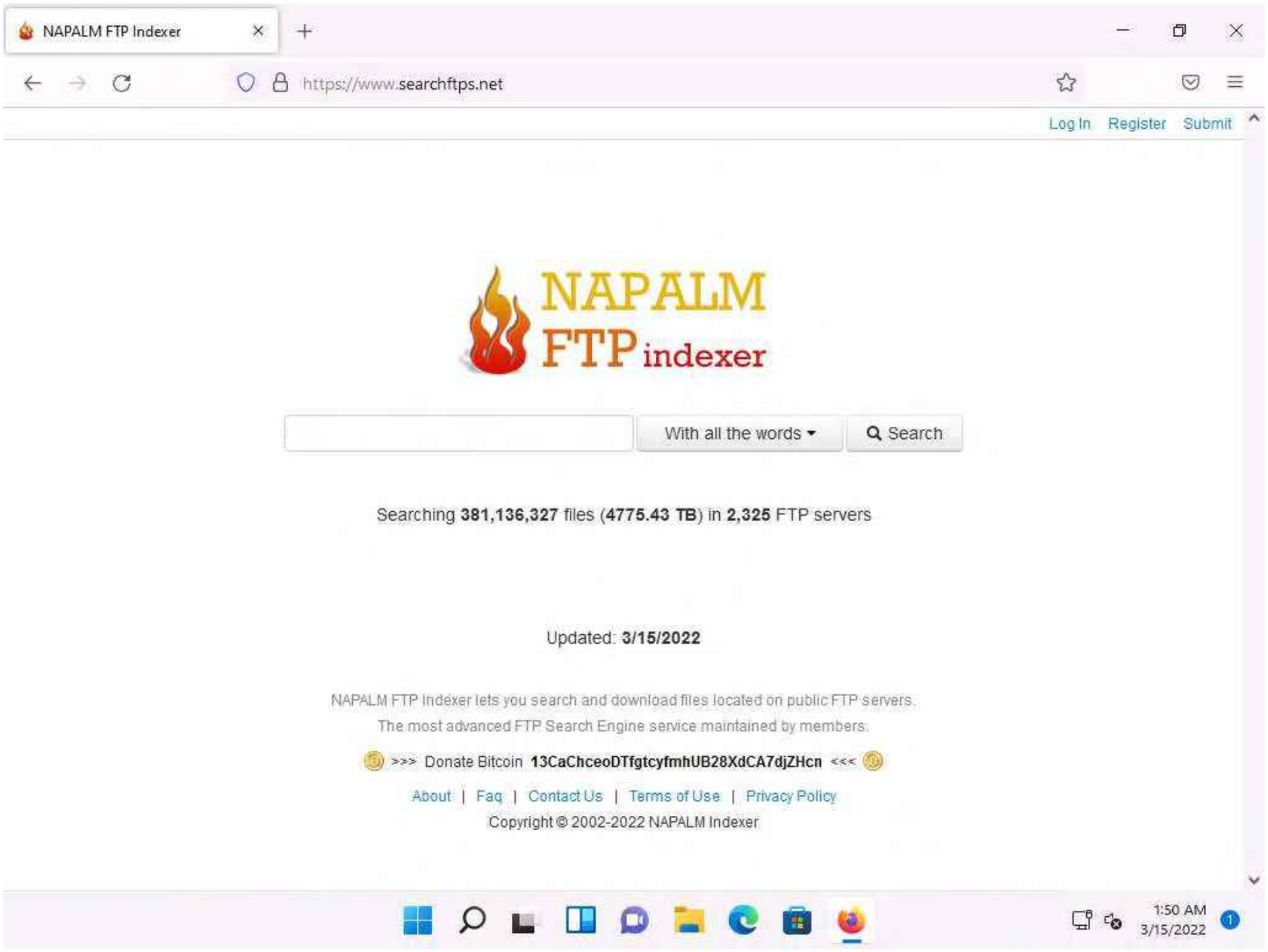
File Transfer Protocol (FTP) search engines are used to search for files located on the FTP servers; these files may hold valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to keep large file archives and other software that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

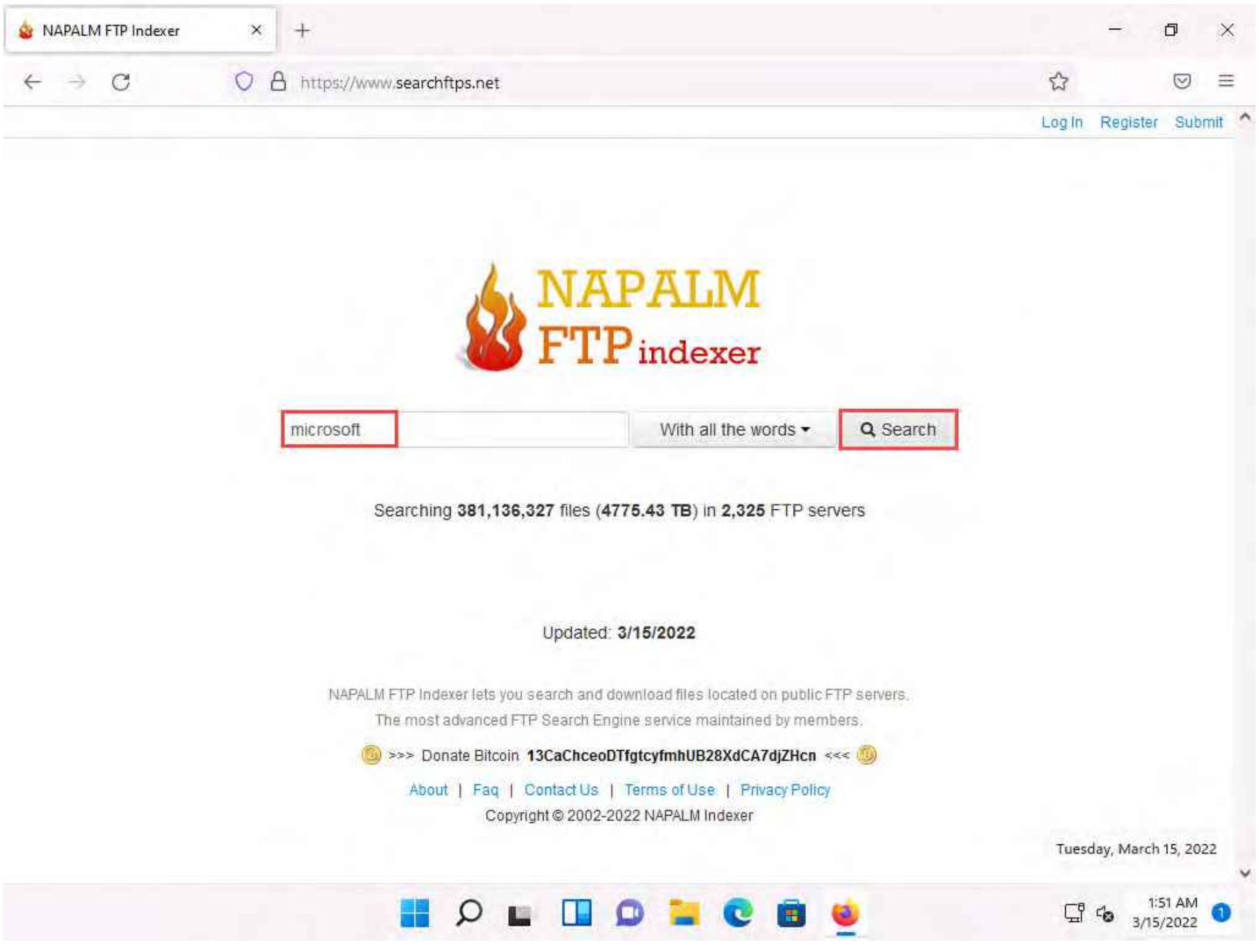
1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.searchftps.net/** and press **Enter**.

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

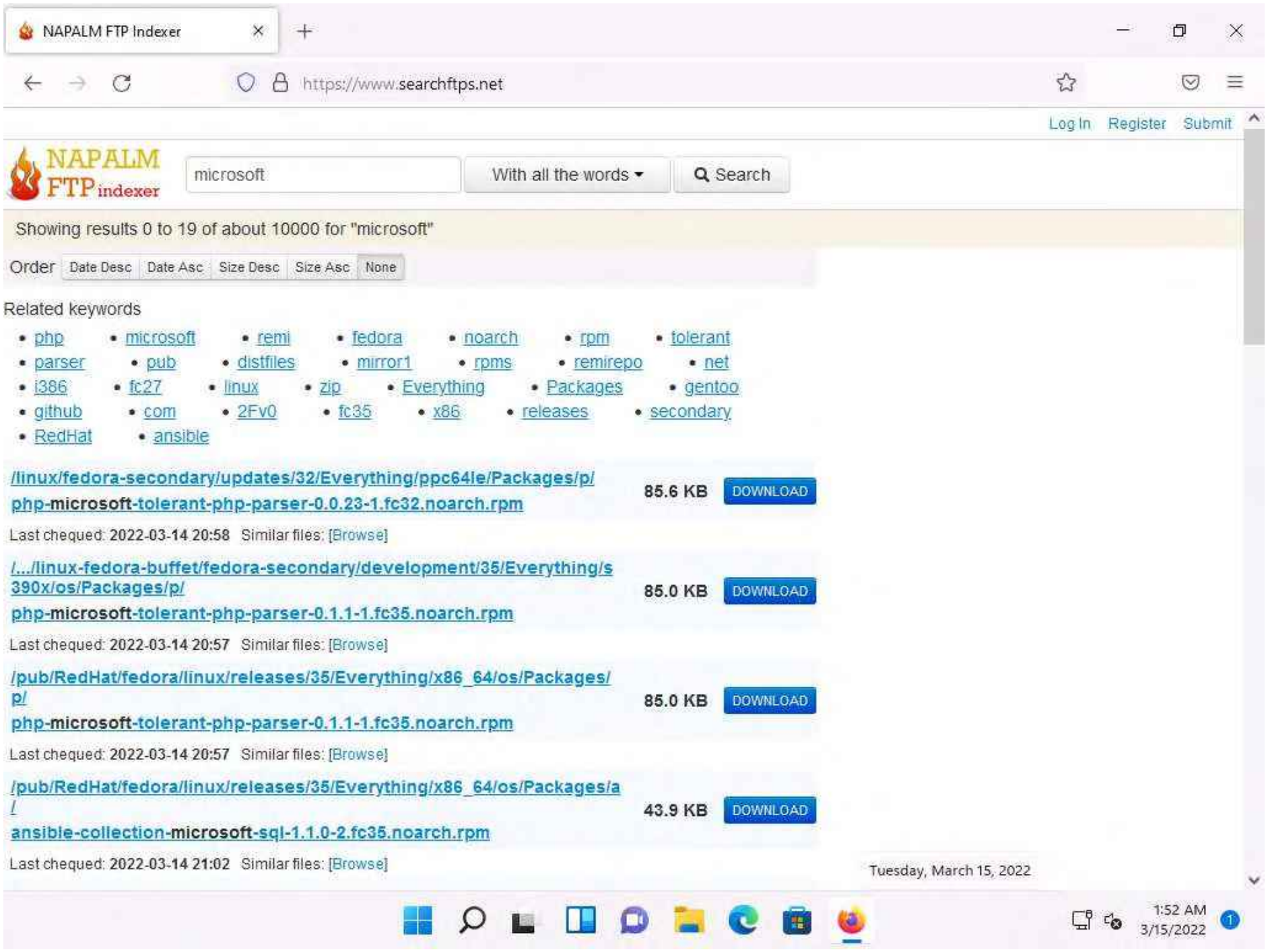
2. NAPALM FTP indexer website appears, as shown in the screenshot.



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.



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

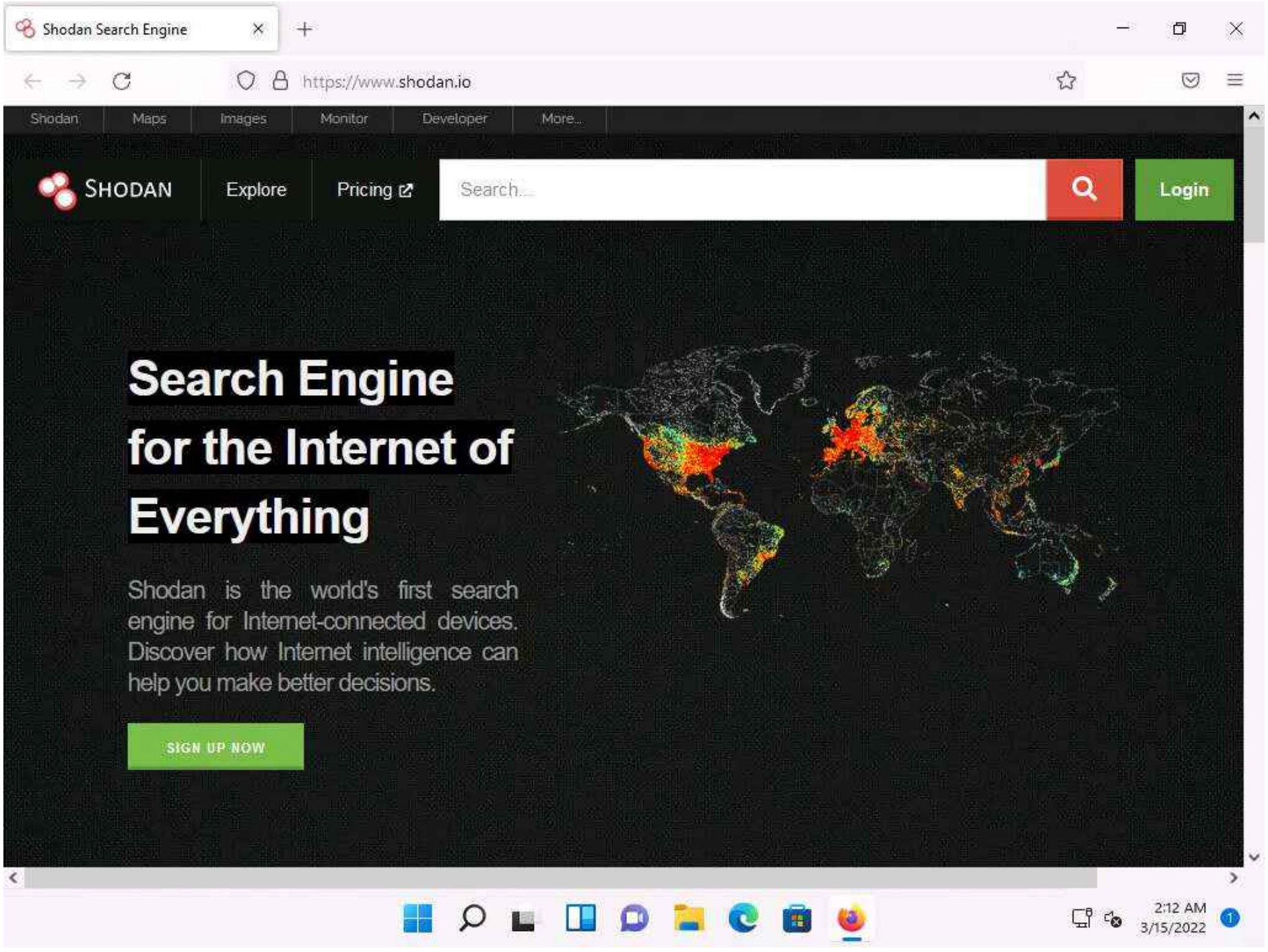
IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances,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

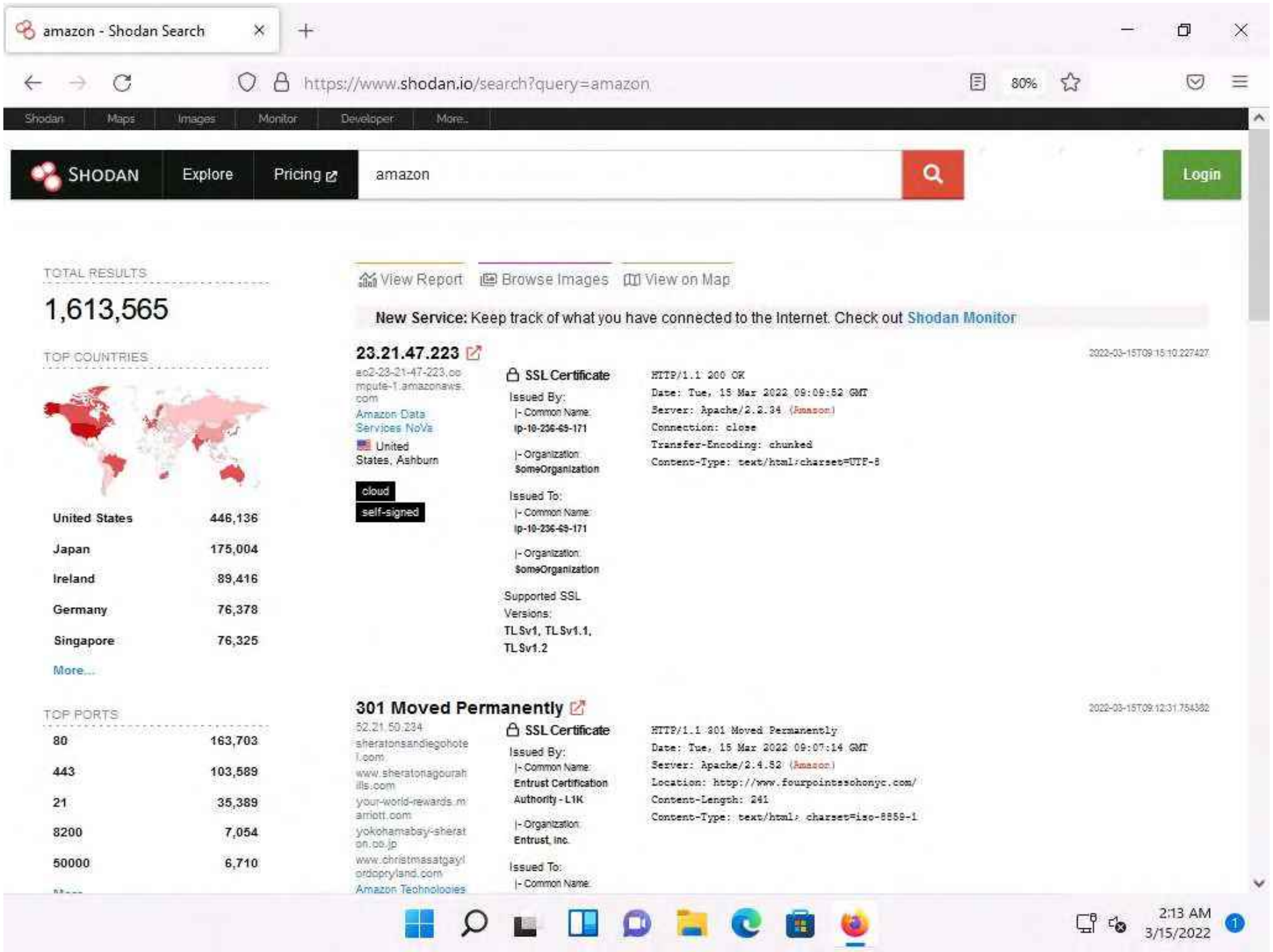
2. **Shodan** page appears, as shown in the screenshot.



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

> Note: Here, we are searching 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.



5. This concludes the demonstration of gathering vulnerable IoT information using the Shodan search engine.
6. You can also use **Censys** (https://censys.io), which is an 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.

Lab 2: Perform Footprinting Through Web Services

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

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).

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.

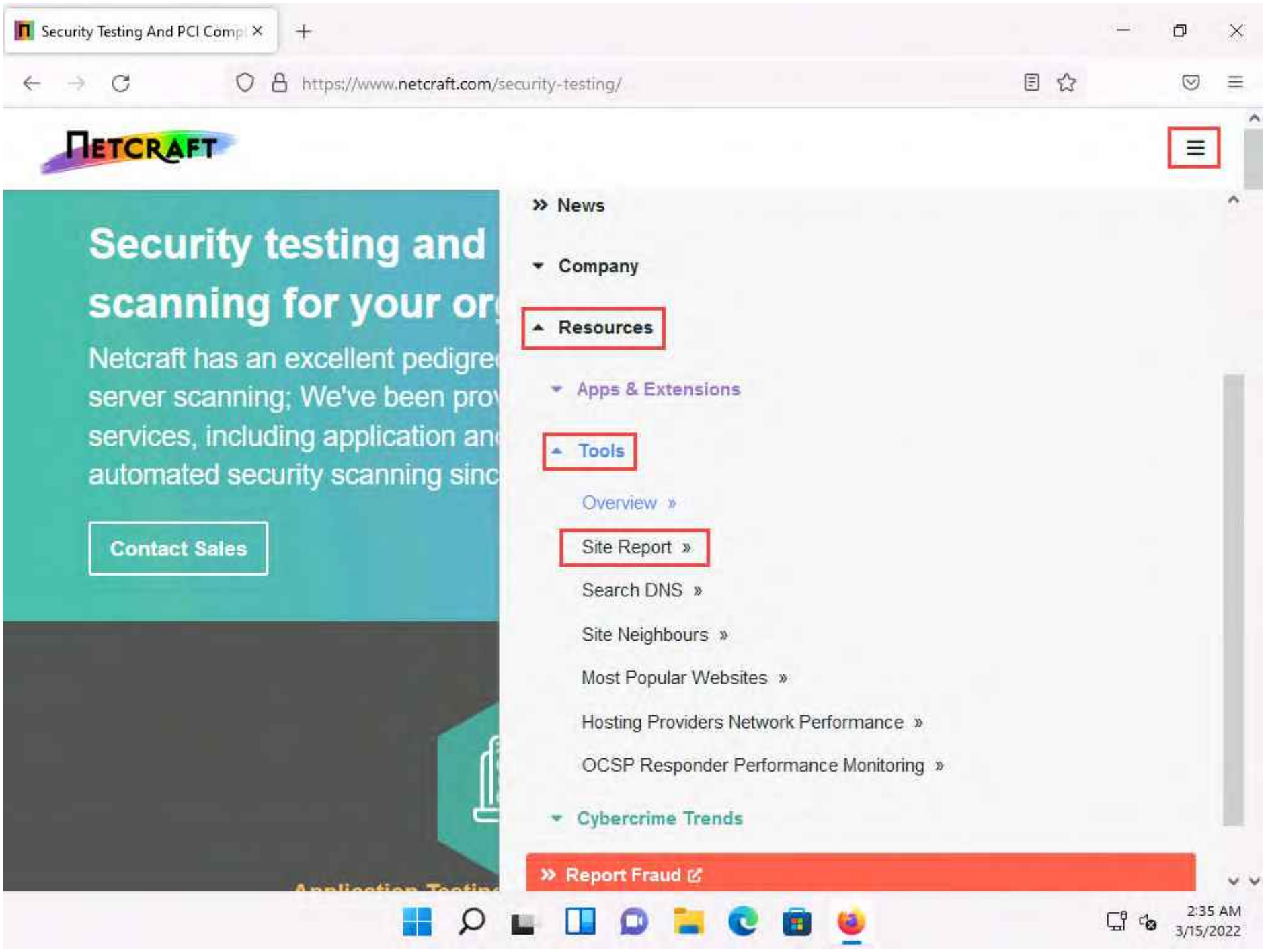
1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.netcraft.com** and press **Enter**.

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

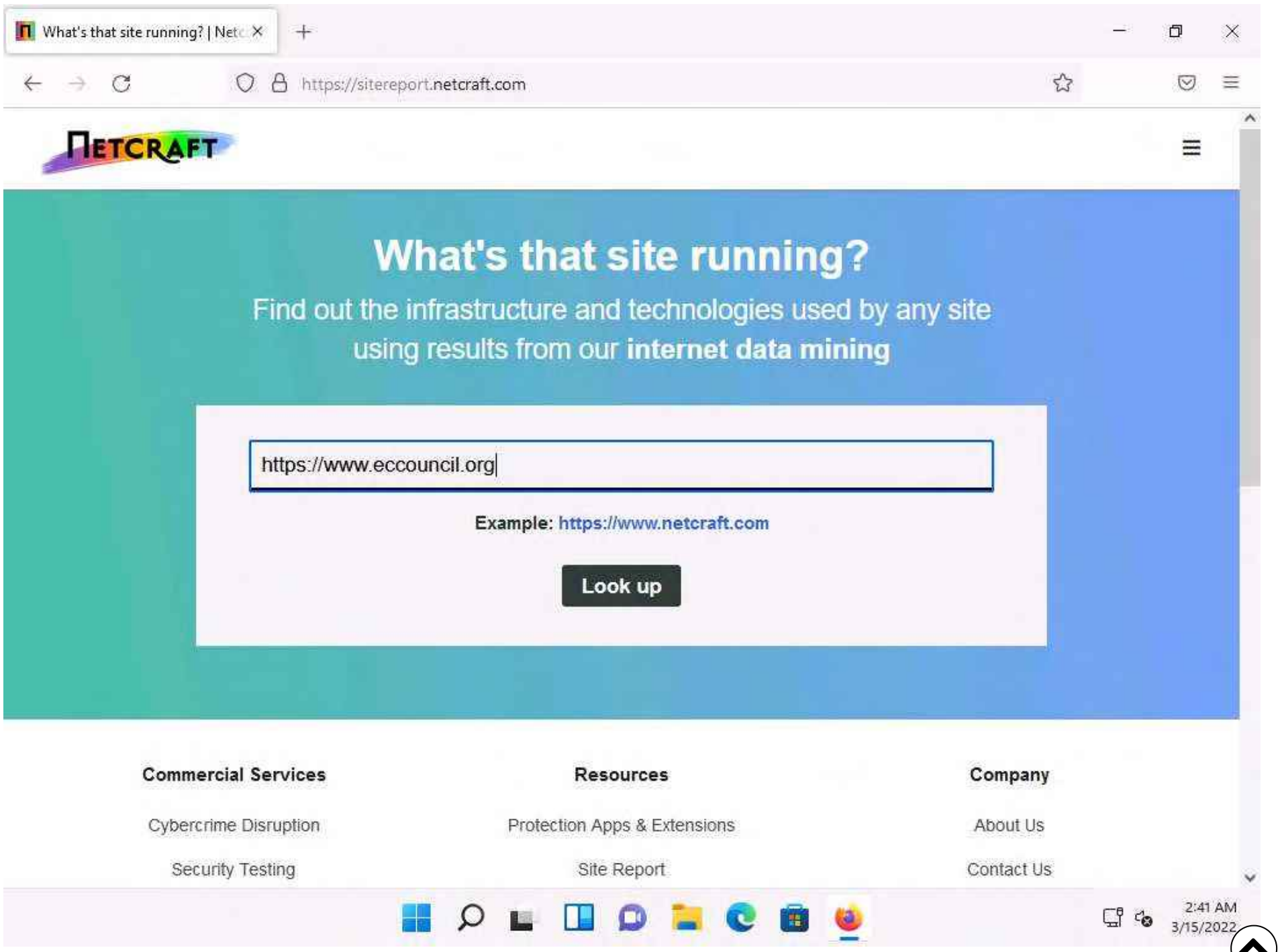
2. **Netcraft** page appears, as shown in the screenshot.

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

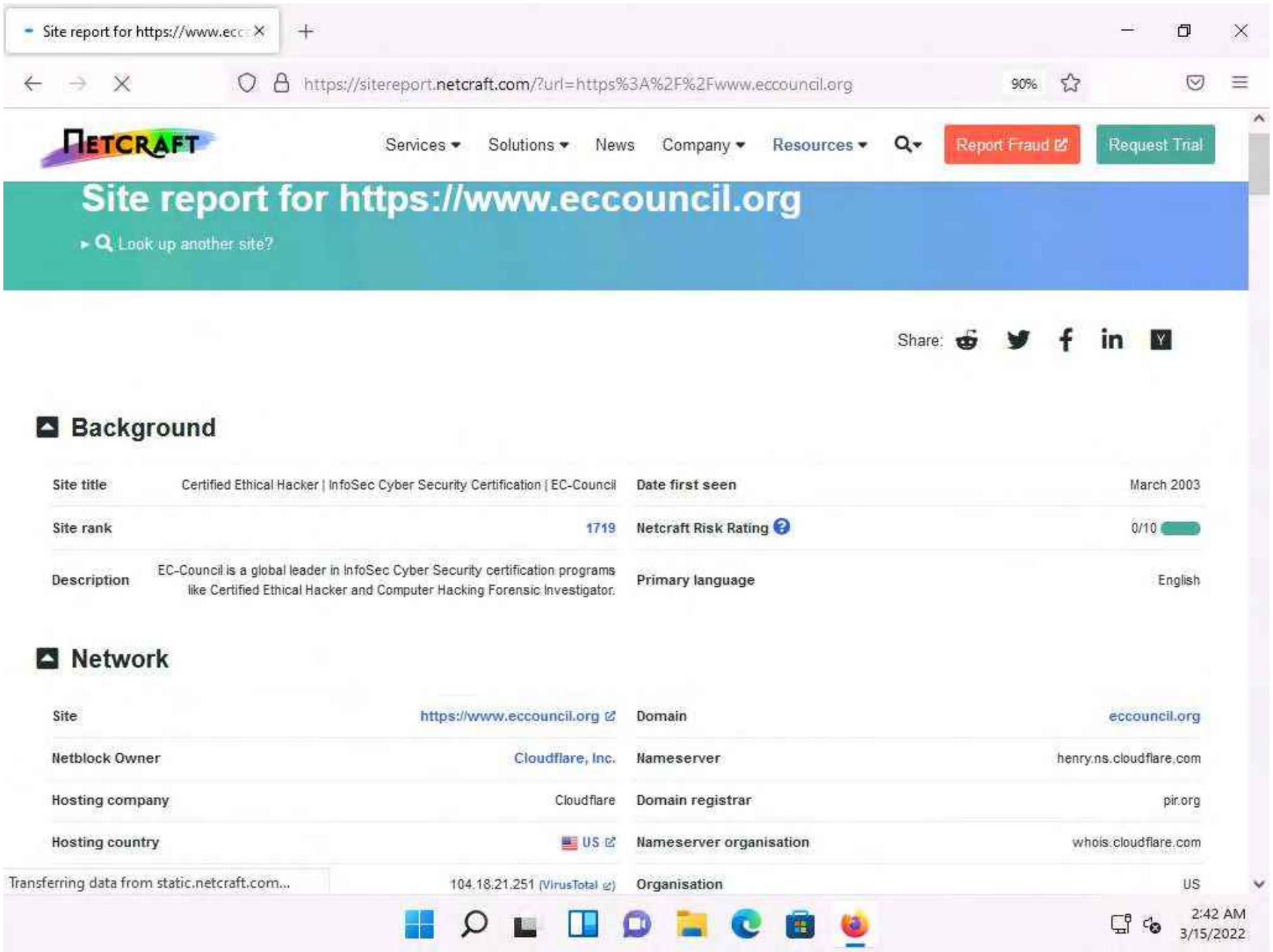
3. Click on menu icon from the top-right corner of the page and navigate to the **Resources** -> **Tools** -> **Site Report**.



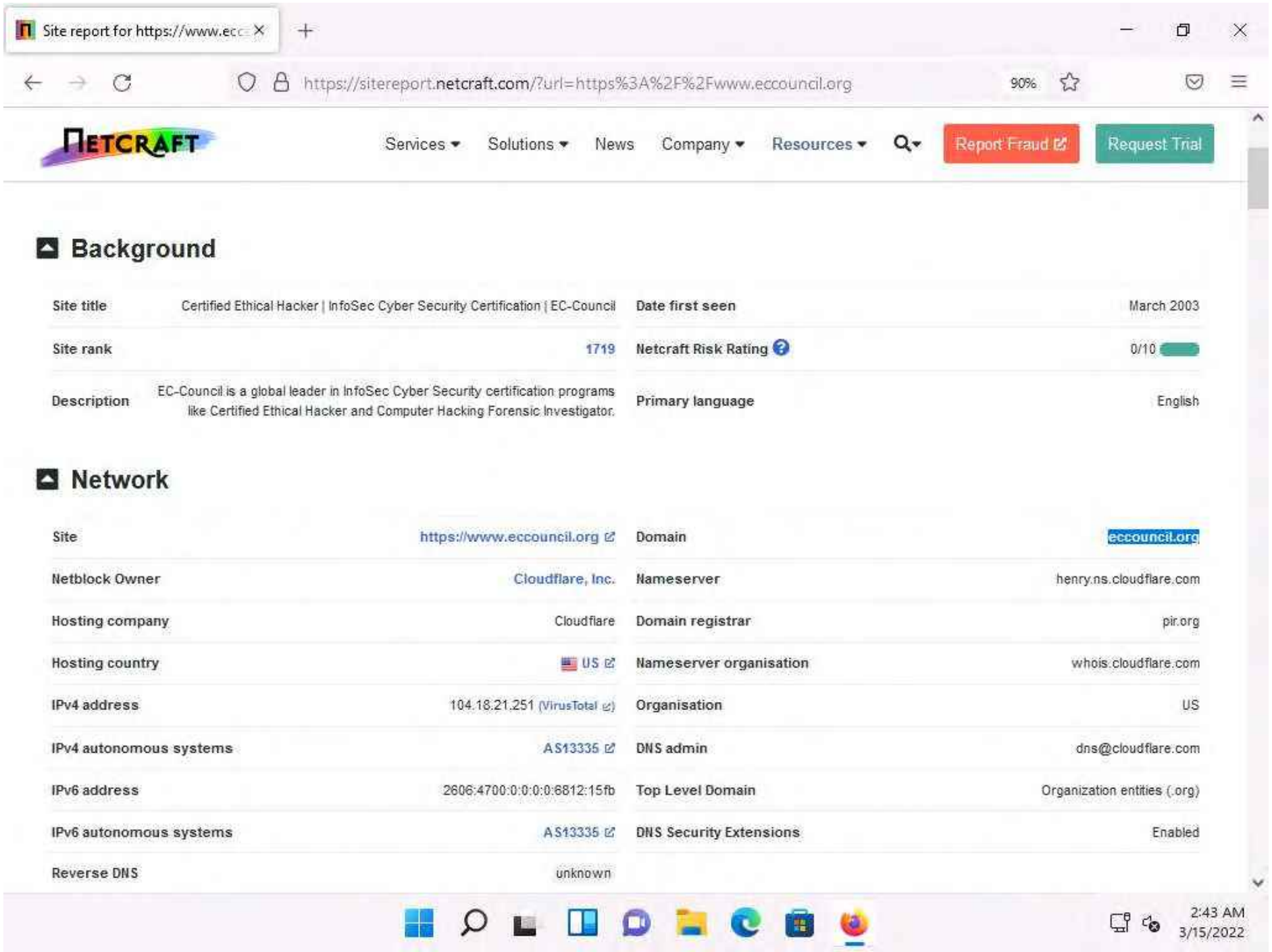
4. The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.eccouncil.org**) in the text field, and then click the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



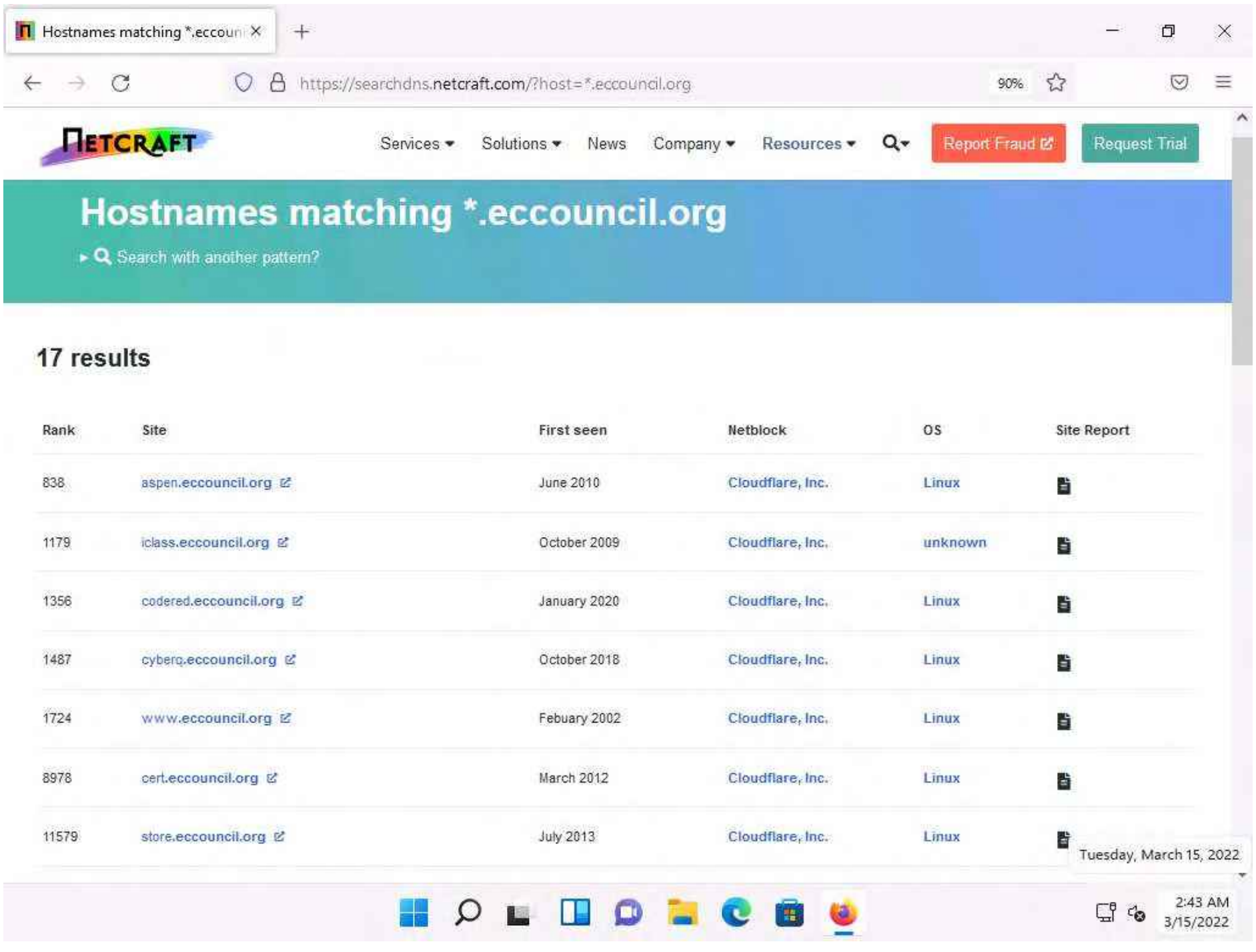
5. The **Site report for https://www.eccouncil.org** page appears, containing information related to **Background**, **Network**, **Hosting History**, etc., as shown in the screenshot.



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



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



8. 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 attack and Denial-of-Service (DoS) attacks.

9. 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.

10. 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. 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.

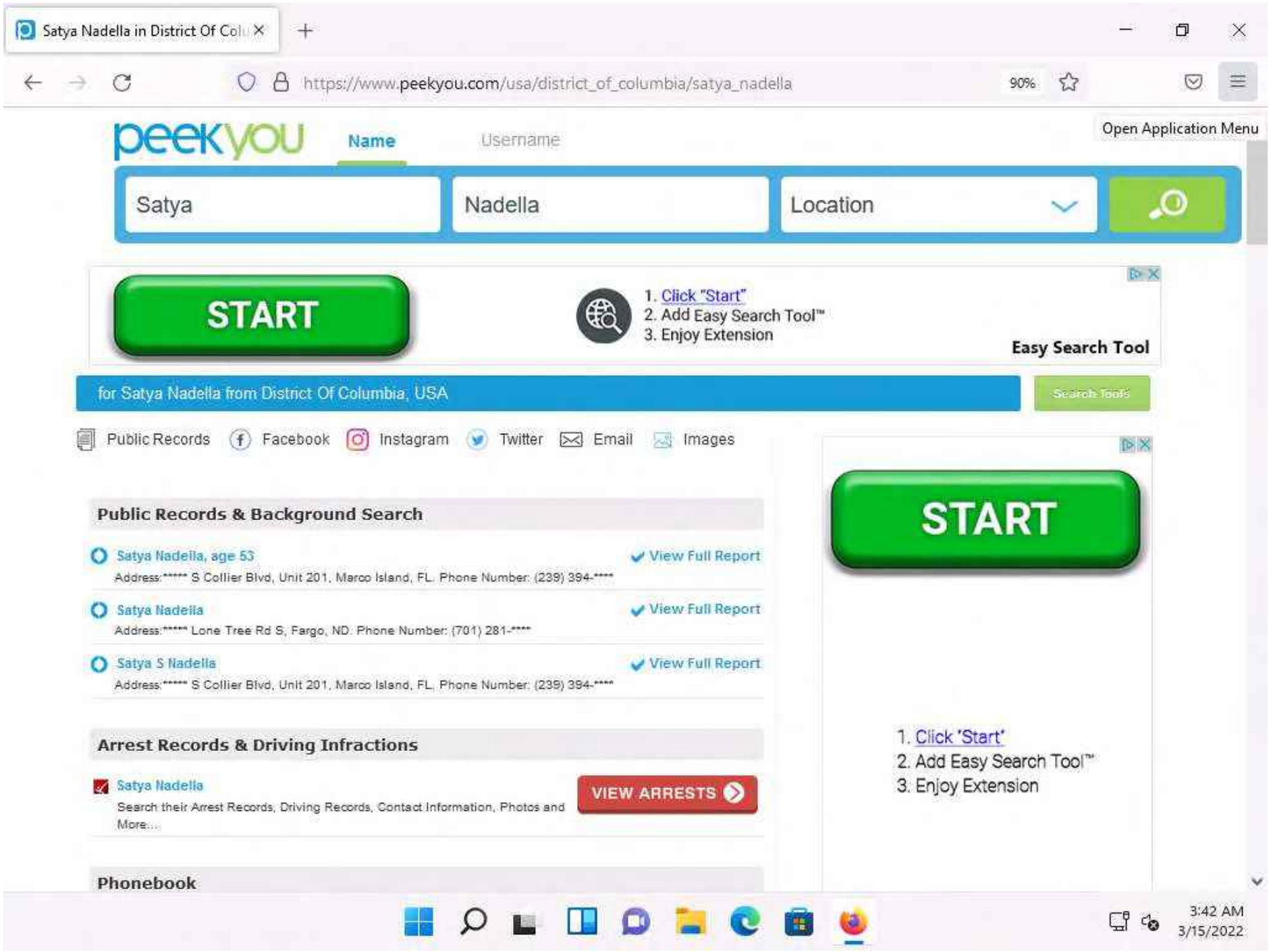
> Note: If cookie pop-up appears at the lower section of the browser, click **I agree**.

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.

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

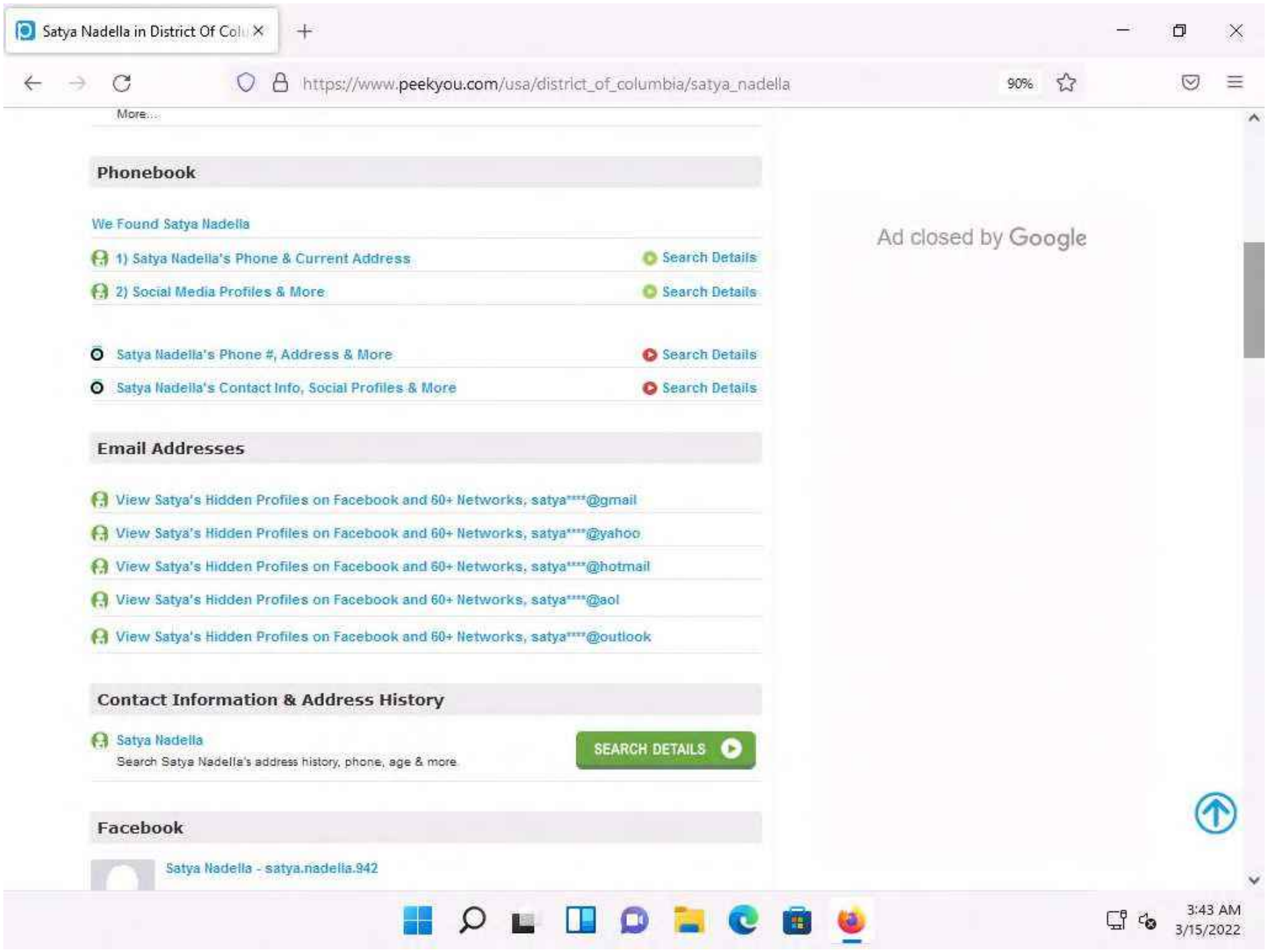
5. The result shows information such as public records, background details, email addresses, contact information, address history, etc. This information helps attackers to perform phishing, social engineering, and other types of attacks.



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.



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

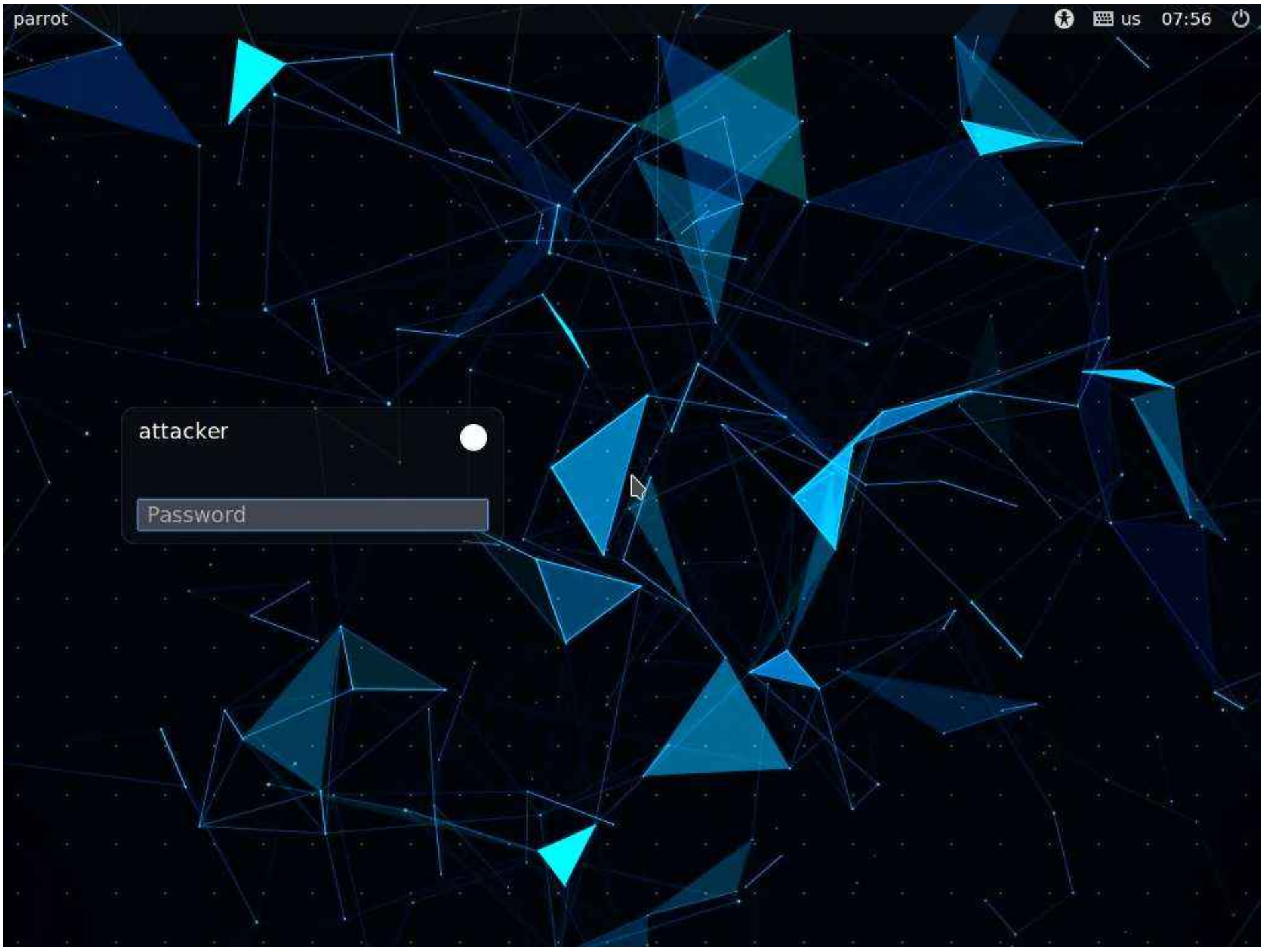
Emails are messaging sources that are crucial for performing information exchange. Email ID is considered by most people as the personal identification of employees or organizations. Thus, gathering the email IDs of critical personnel is one of the key tasks of ethical hackers.

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

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.

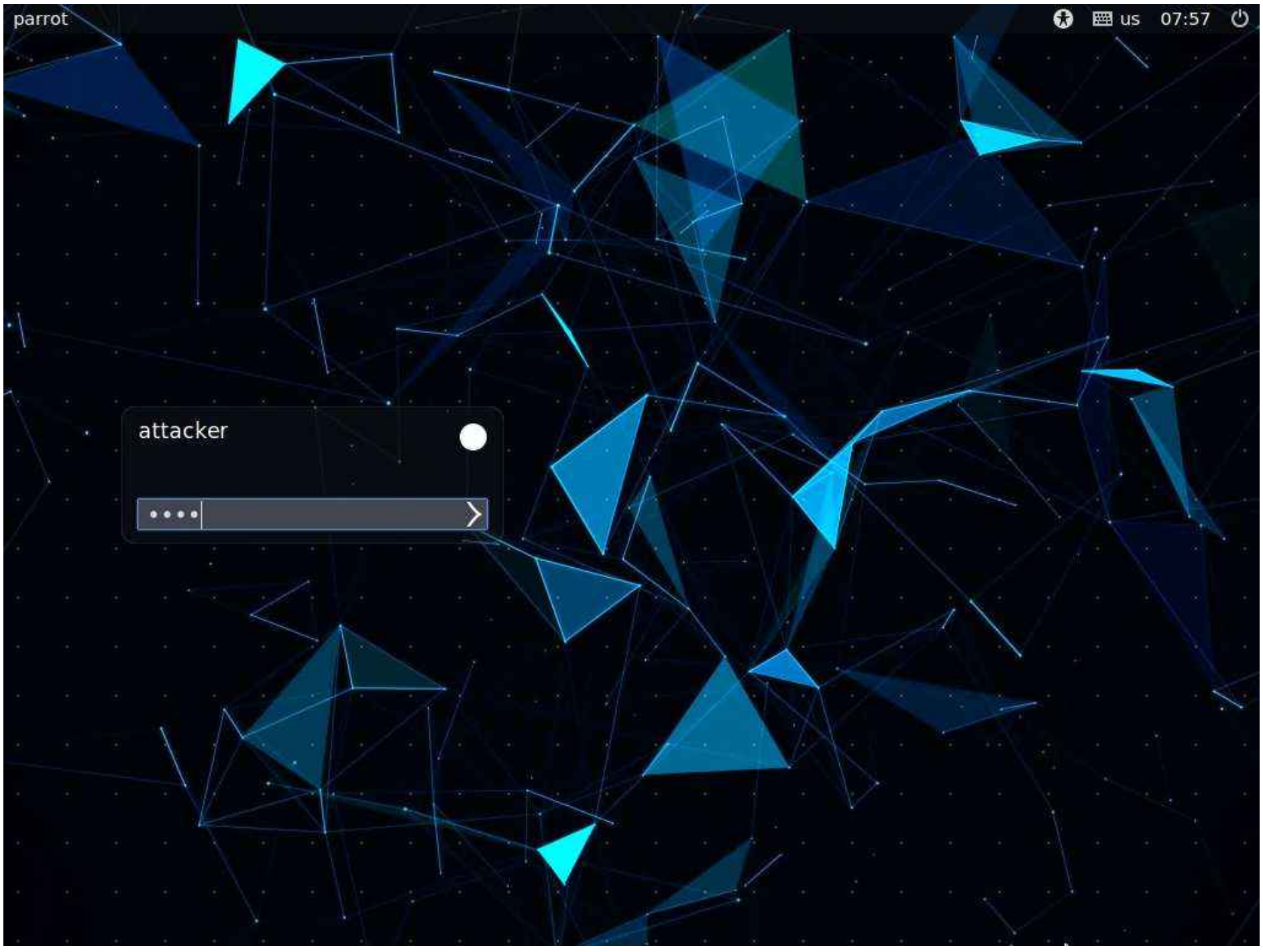
Note: Here, we will consider **Microsoft** as a target organization. However, you can select a target organization of your choice.

1. To launch **Parrot Security** machine, click **CEHv12 Parrot Security**.

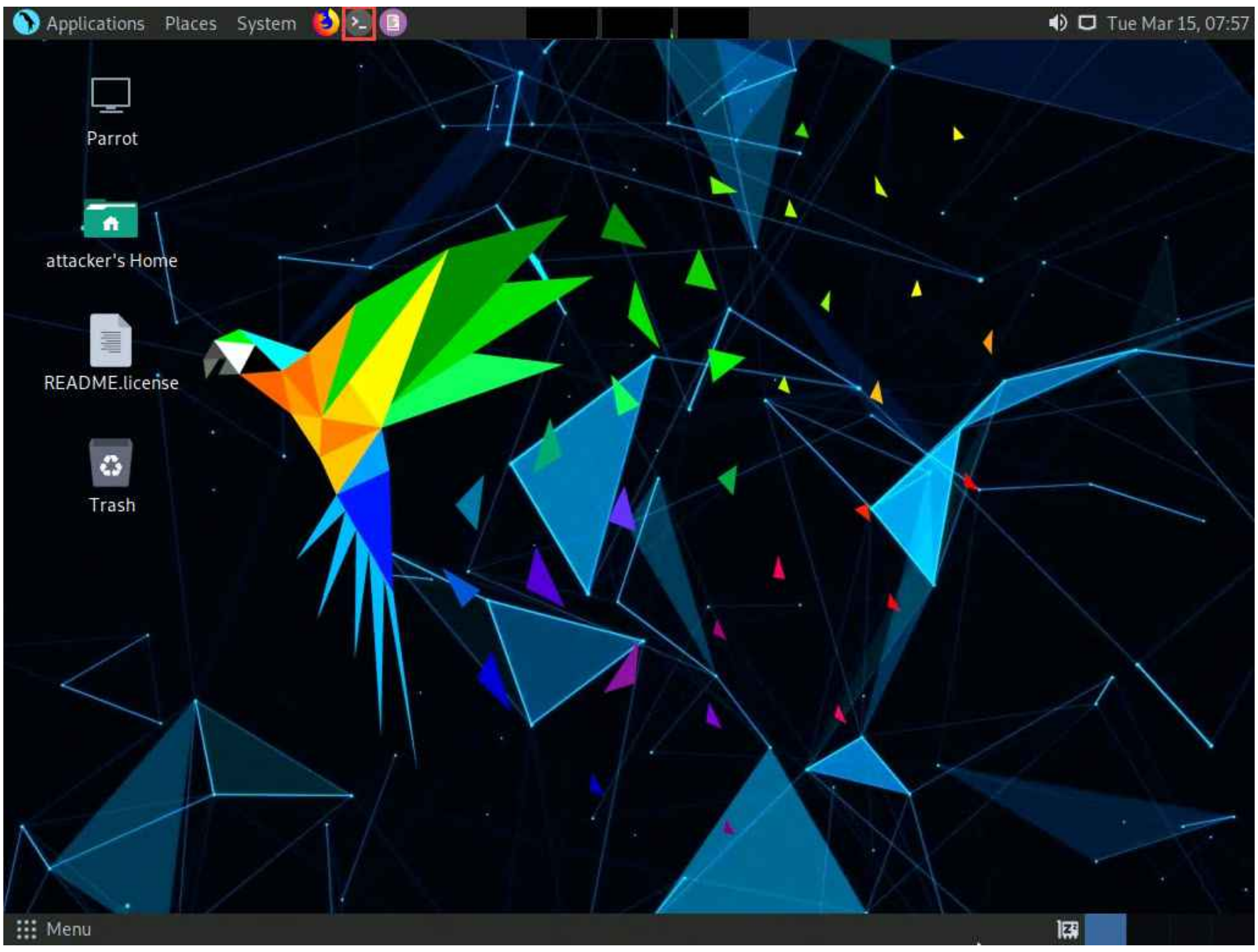


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

> 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.

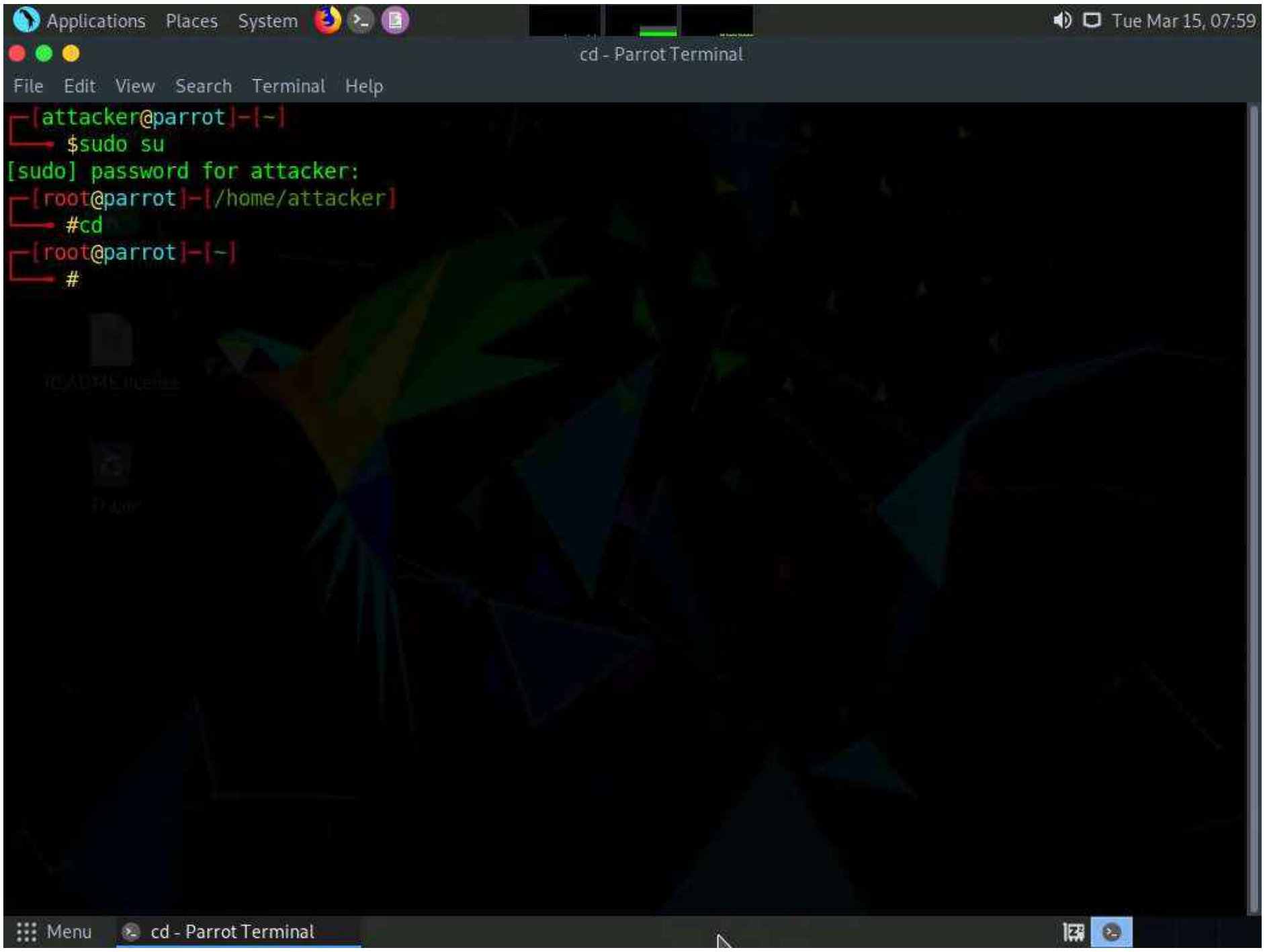


4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

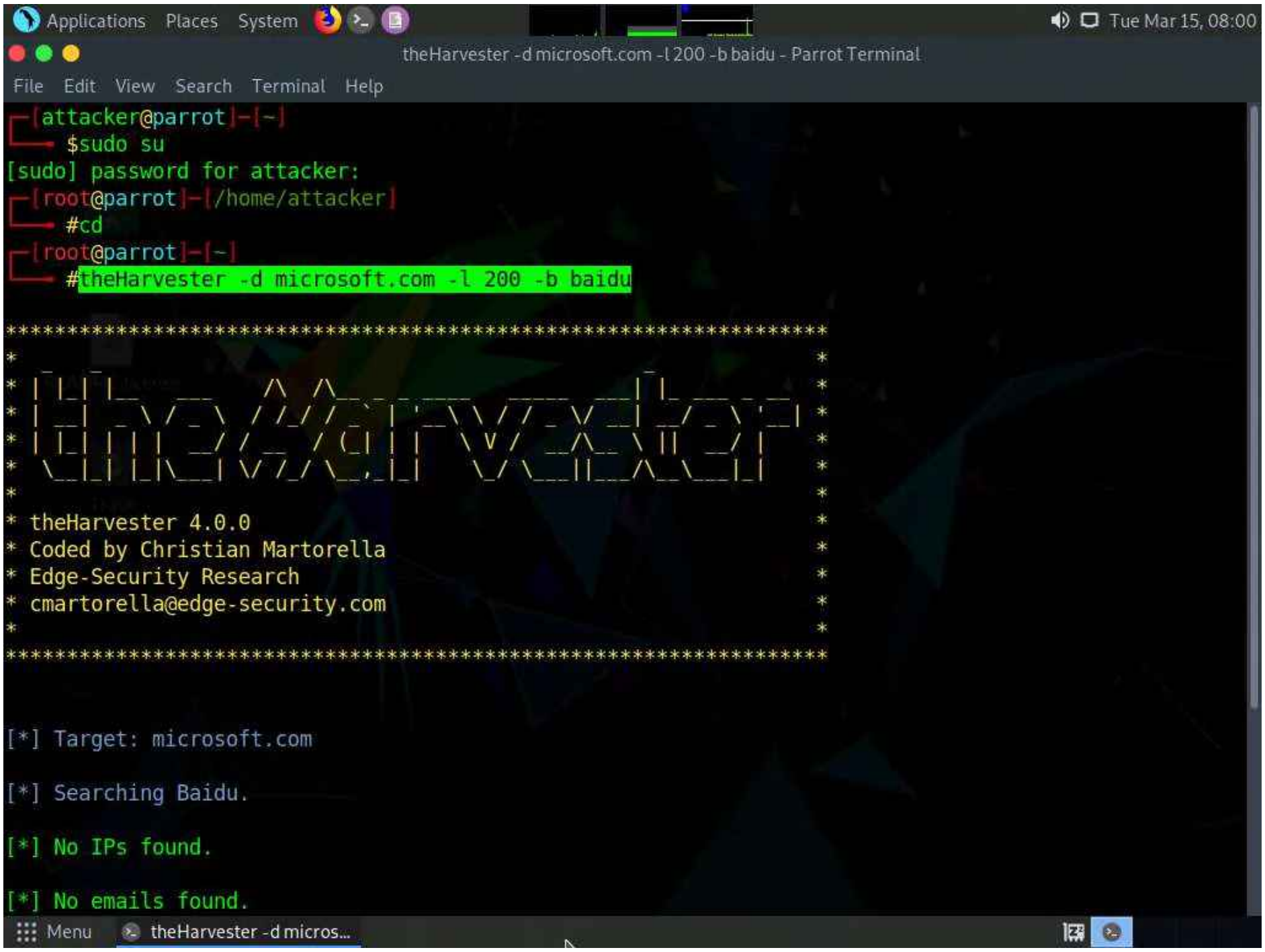
> Note: The password that you type will not be visible.

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



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

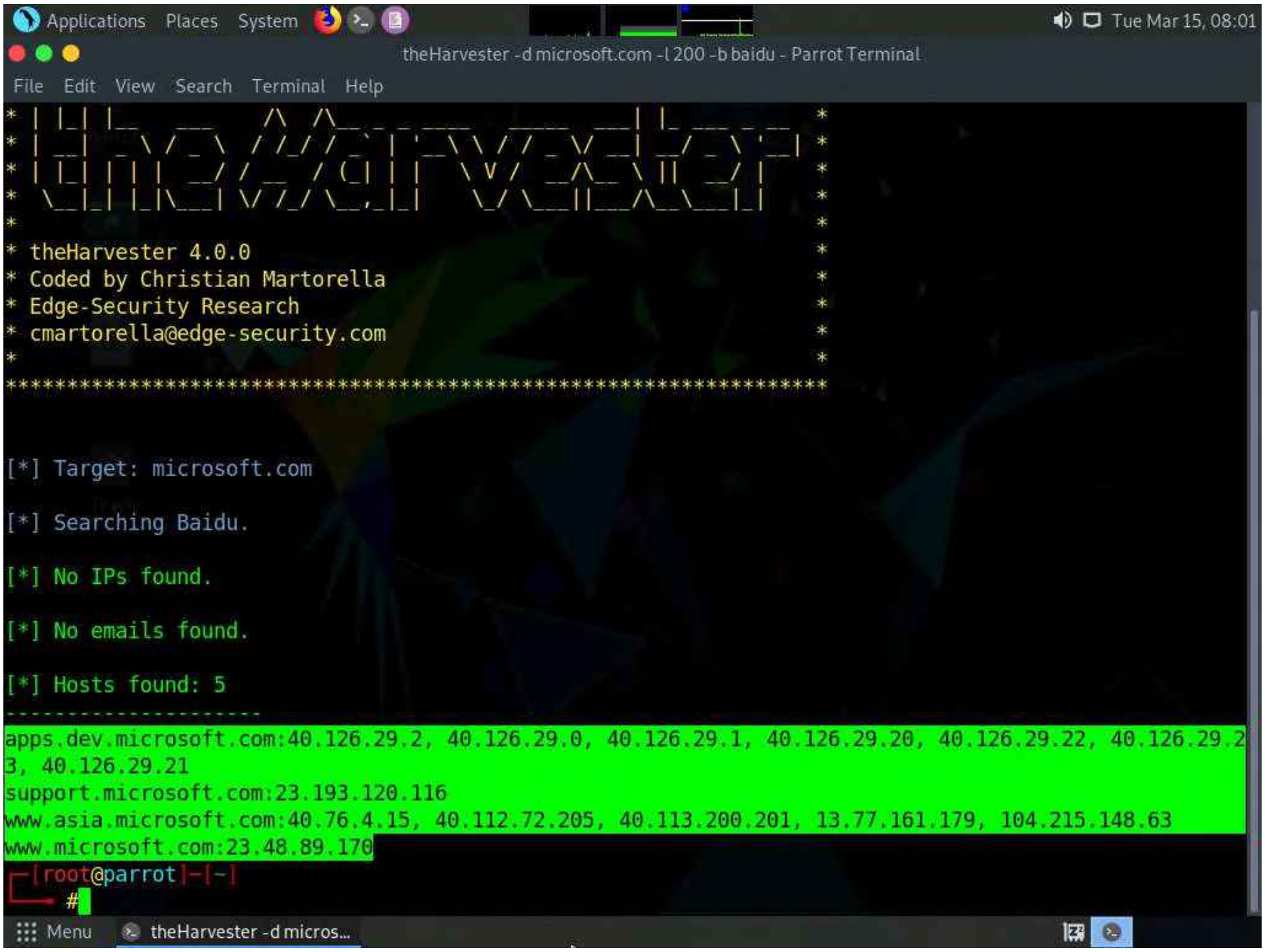
> Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source.



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.



10. This concludes the demonstration of gathering an email list using theHarvester.

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

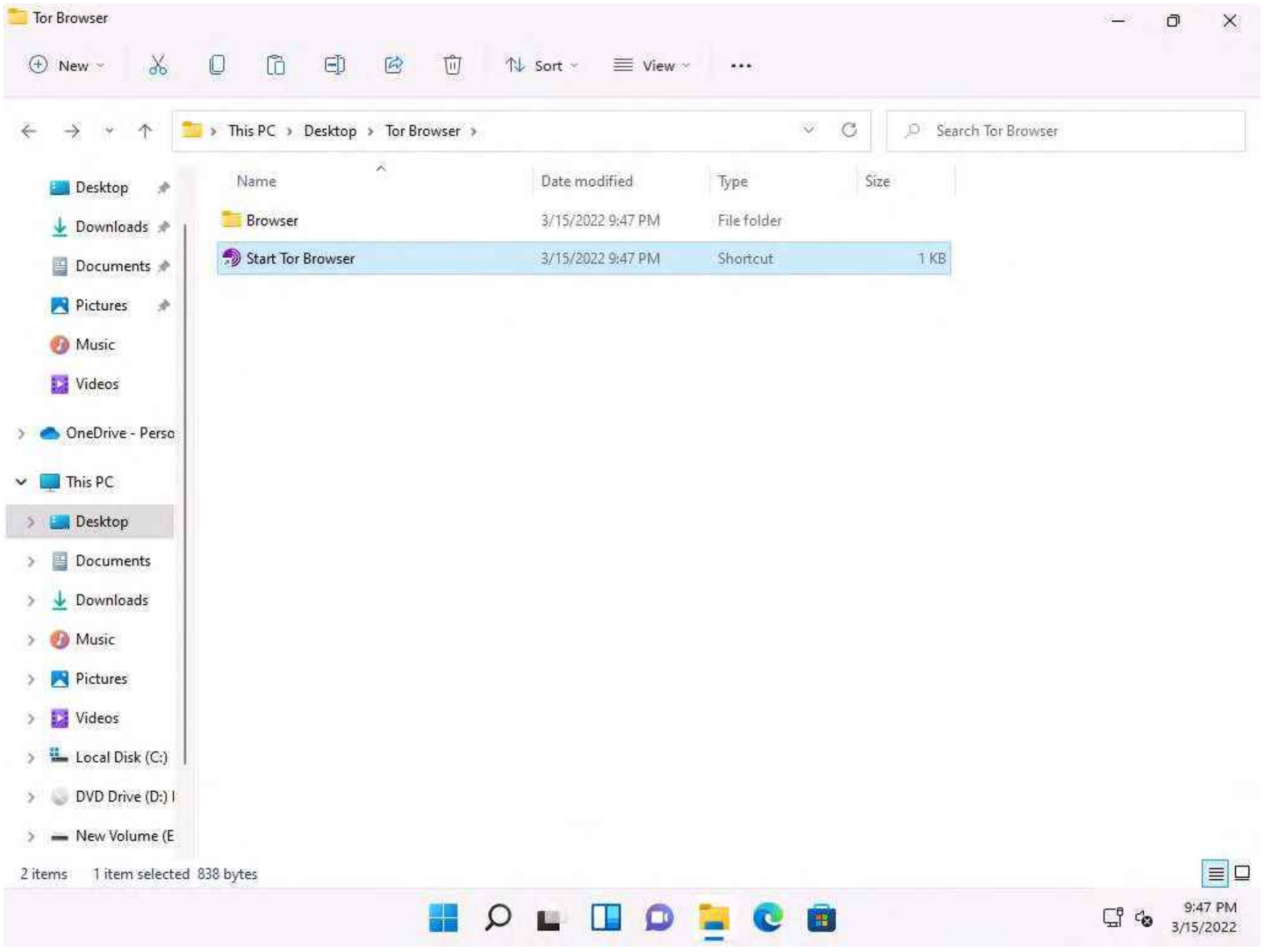
Task 4: Gather Information using Deep and Dark Web Searching

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.

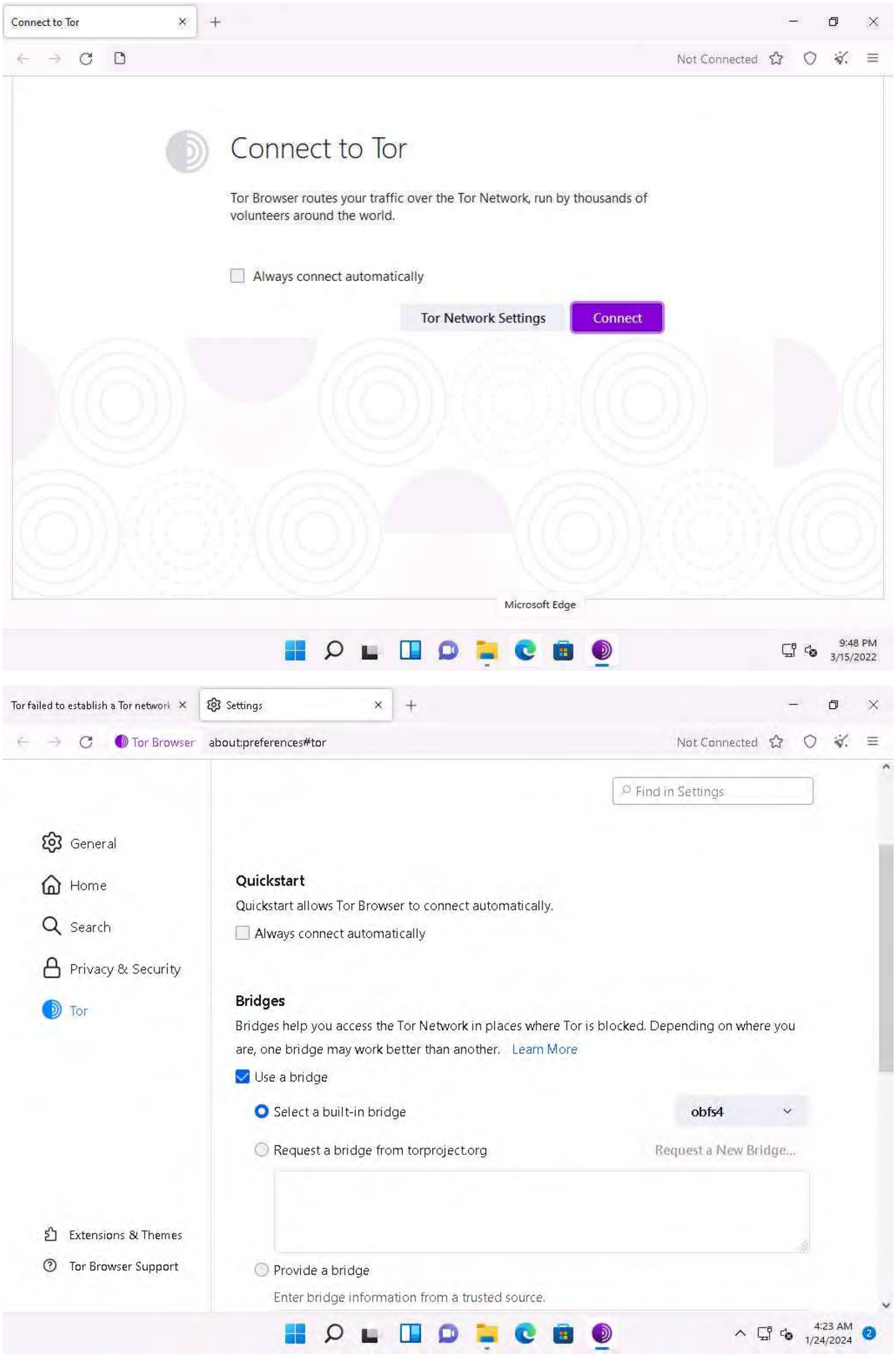
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

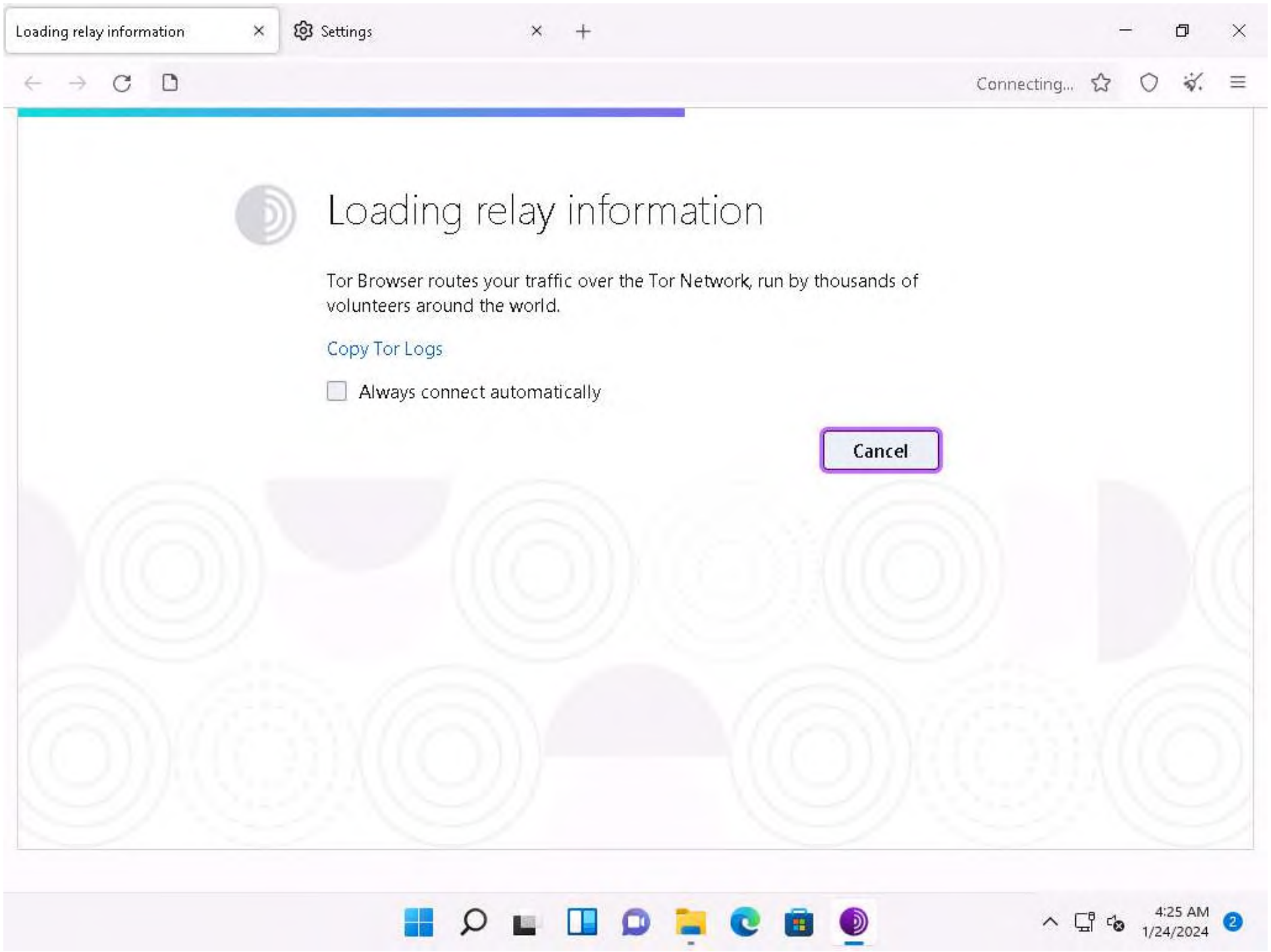
2. Open a **File Explorer**, navigate to **C:\Users\Admin\Desktop\Tor Browser**, and double-click **Start Tor Browser**.



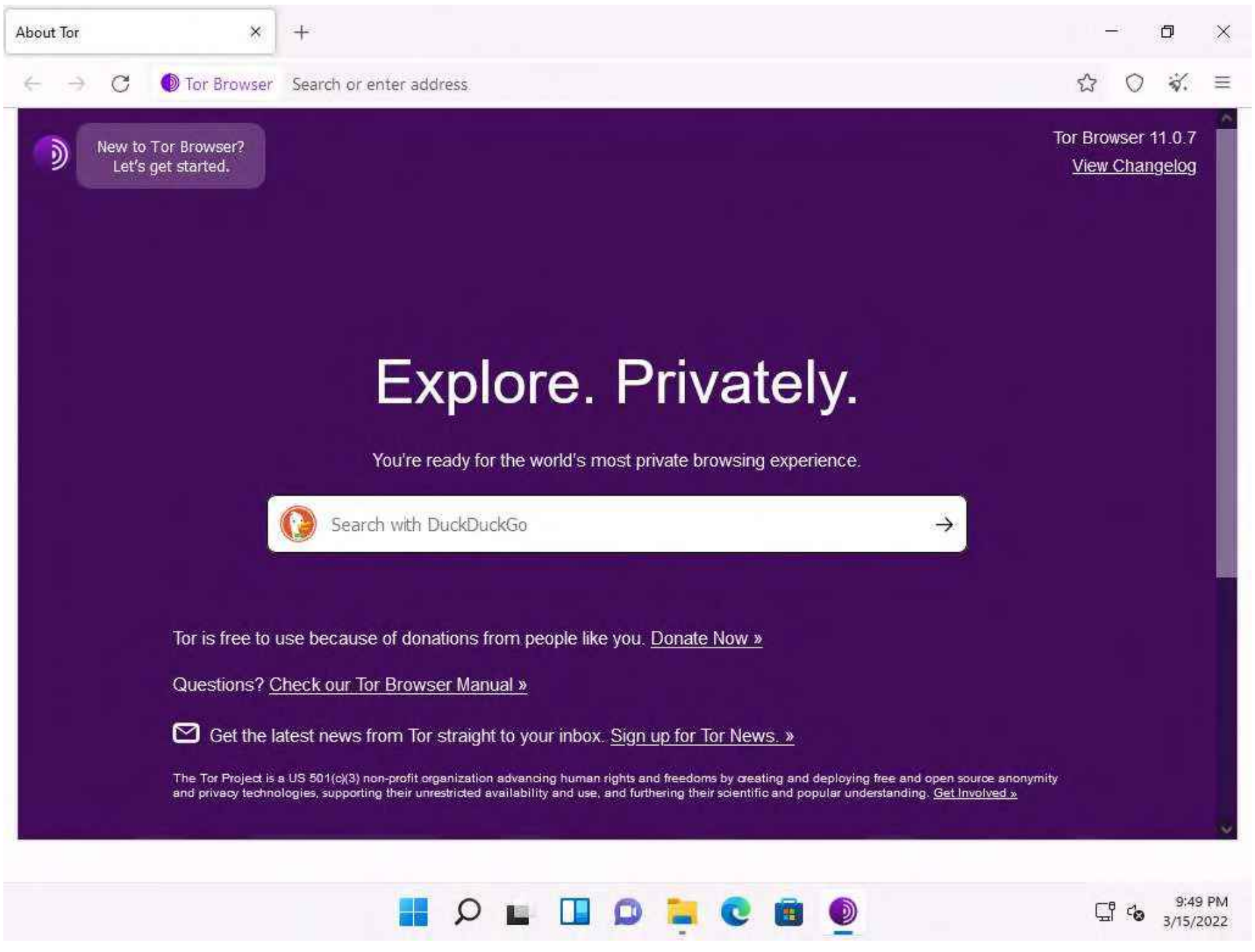
3. The **Connect to Tor** page appears. Click the **Connect** button to directly browse through Tor Browser's default settings.

Note: If Tor is censored in your country or if you want to connect through Proxy, click the Tor Network Settings button and select any default built-in bridge as shown in the screenshot below and continue.


Connect to Tor
Not Connected
Connect to Tor
Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.
Always connect automatically
Tor Network Settings
Connect
Microsoft Edge
9:48 PM
3/15/2022
Tor failed to establish a Tor network
Settings
Tor Browser
about:preferences#tor
Not Connected
Find in Settings
General
Home
Search
Privacy & Security
Tor
Extensions & Themes
Tor Browser Support
Quickstart
Quickstart allows Tor Browser to connect automatically.
Always connect automatically
Bridges
Bridges help you access the Tor Network in places where Tor is blocked. Depending on where you are, one bridge may work better than another. Learn More
Use a bridge
Select a built-in bridge
obfs4
Request a bridge from torproject.org
Request a New Bridge...
Provide a bridge
Enter bridge information from a trusted source.
4:23 AM
1/24/2024

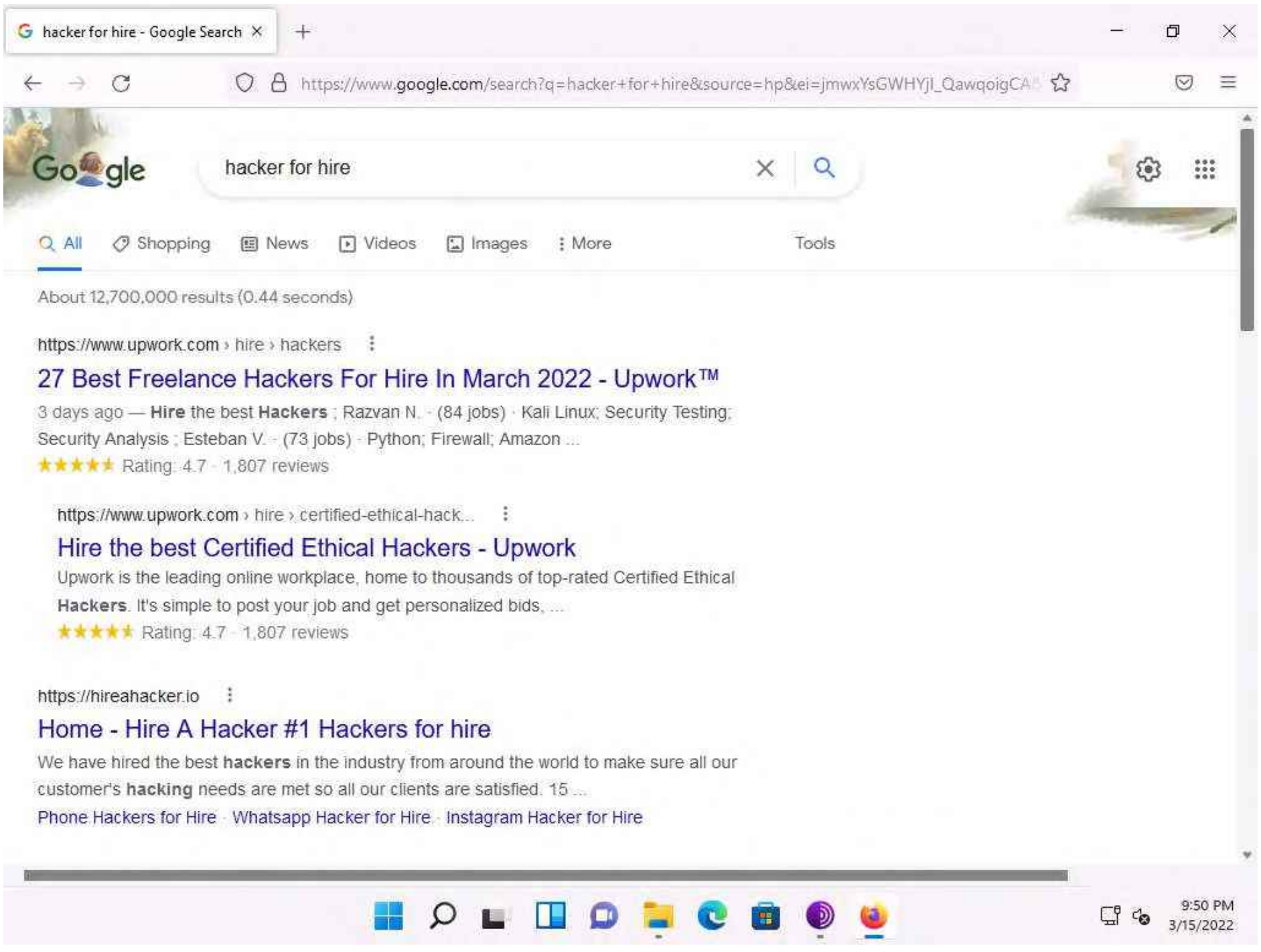


4. After a few seconds, the Tor Browser home page appears. The main advantage of Tor Browser is that it maintains the anonymity of the user throughout the session.



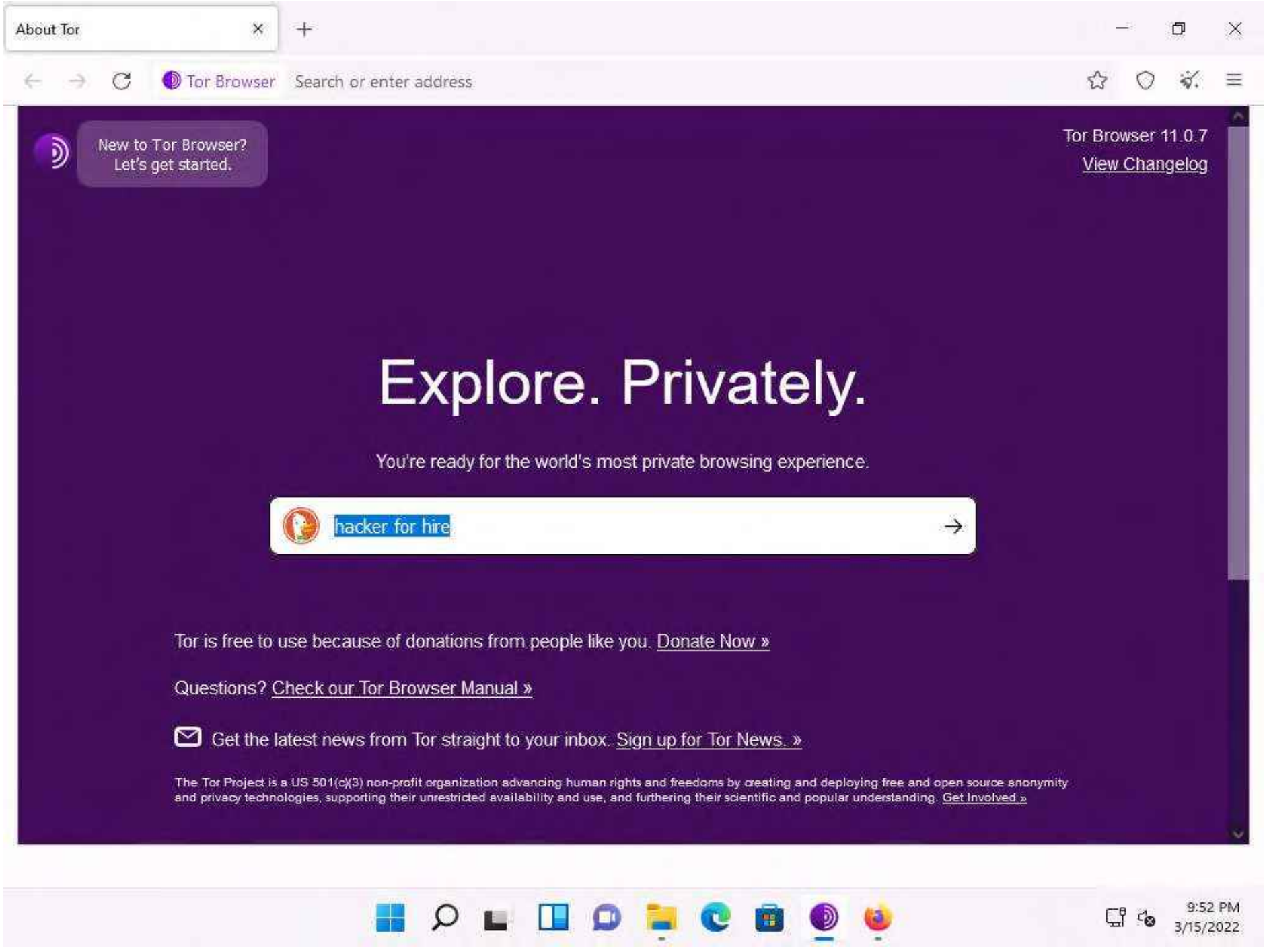
5. As an ethical hacker, you need to collect all possible information related to the target organization from the dark web. Before doing so, you must know the difference between surface web searching and dark web searching.

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.

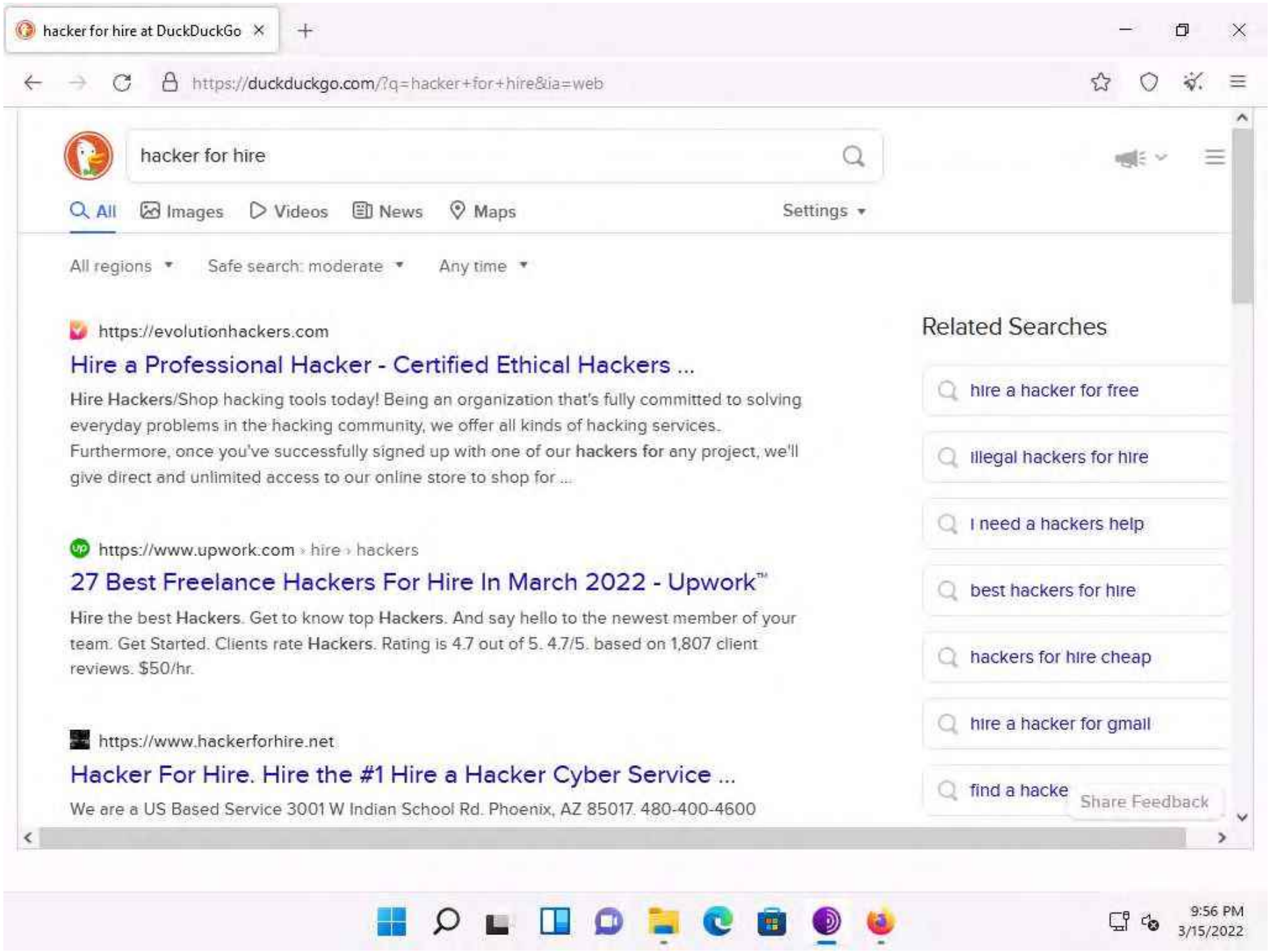
Note: Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.



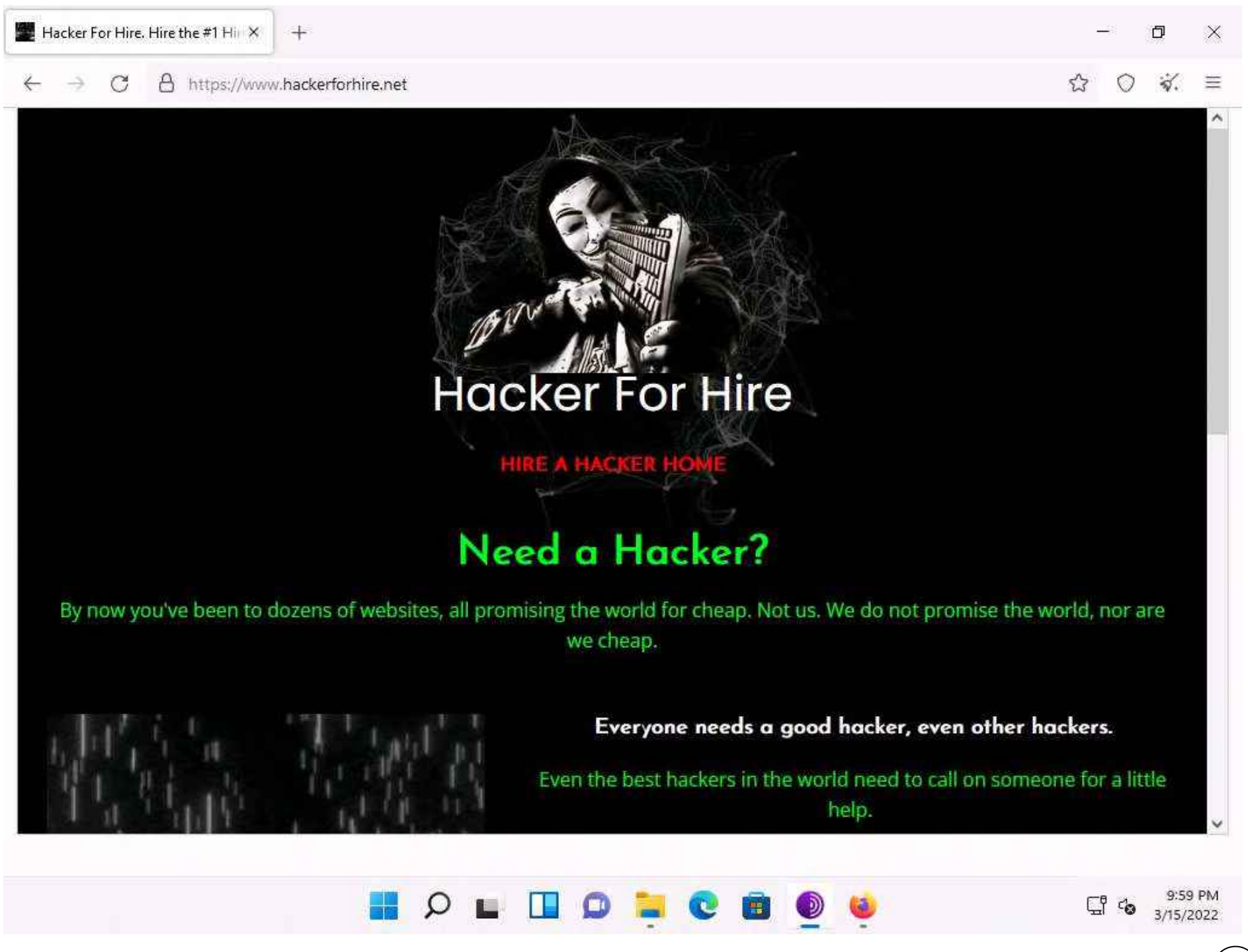
8. By default, **All regions** search parameter is selected. However, you can click the down arrow to view the drop-down options and select a region of your choice, this specifies the country of VPN/Proxy.

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://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.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

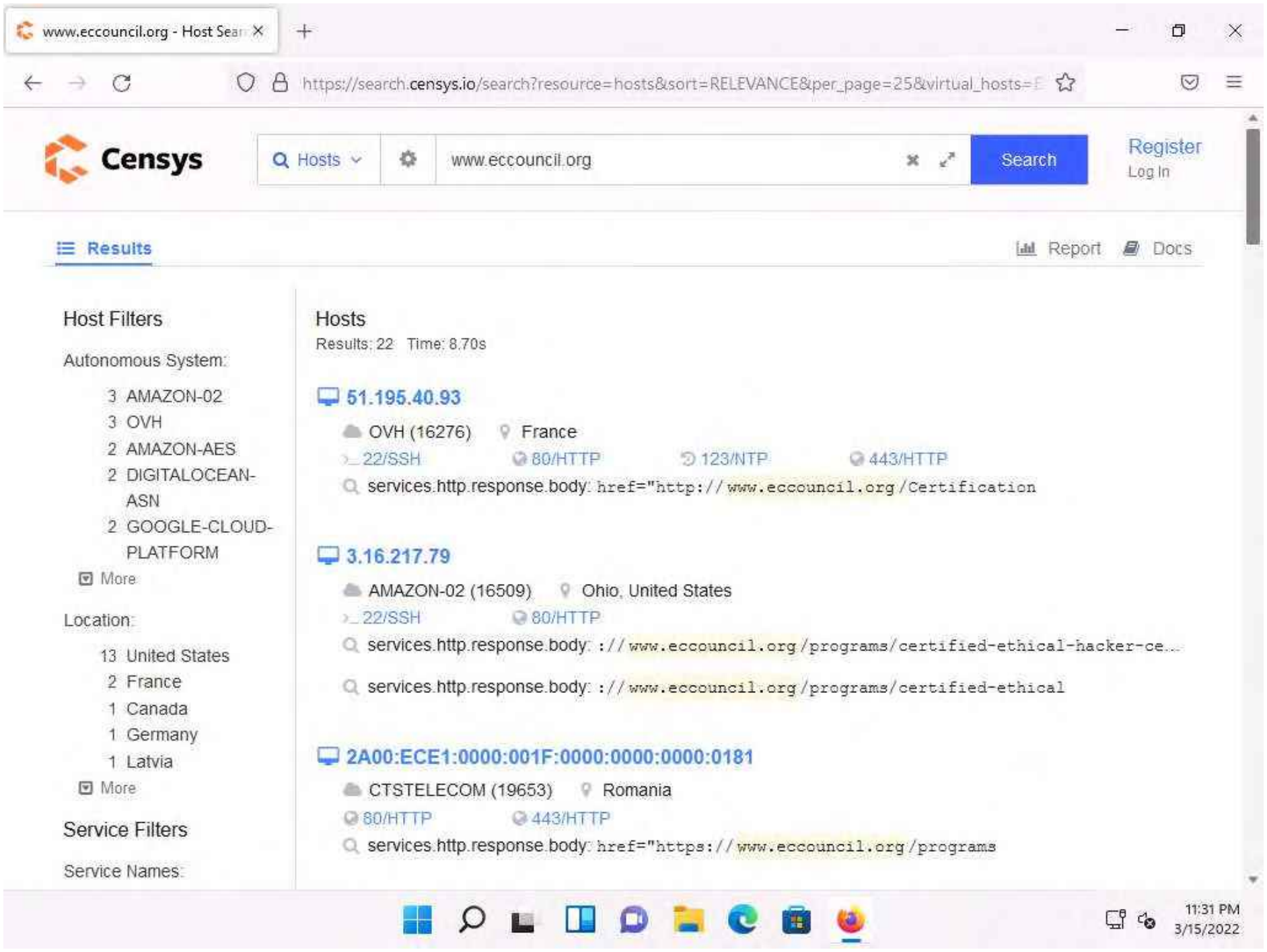
Operating system information is crucial for every ethical hacker. Ethical hackers can acquire details of the operating system running on the target machine by performing various passive footprinting techniques and obtain other information such as the city, country, latitude/longitude, hostname, operating system, and IP address of the target organization.

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

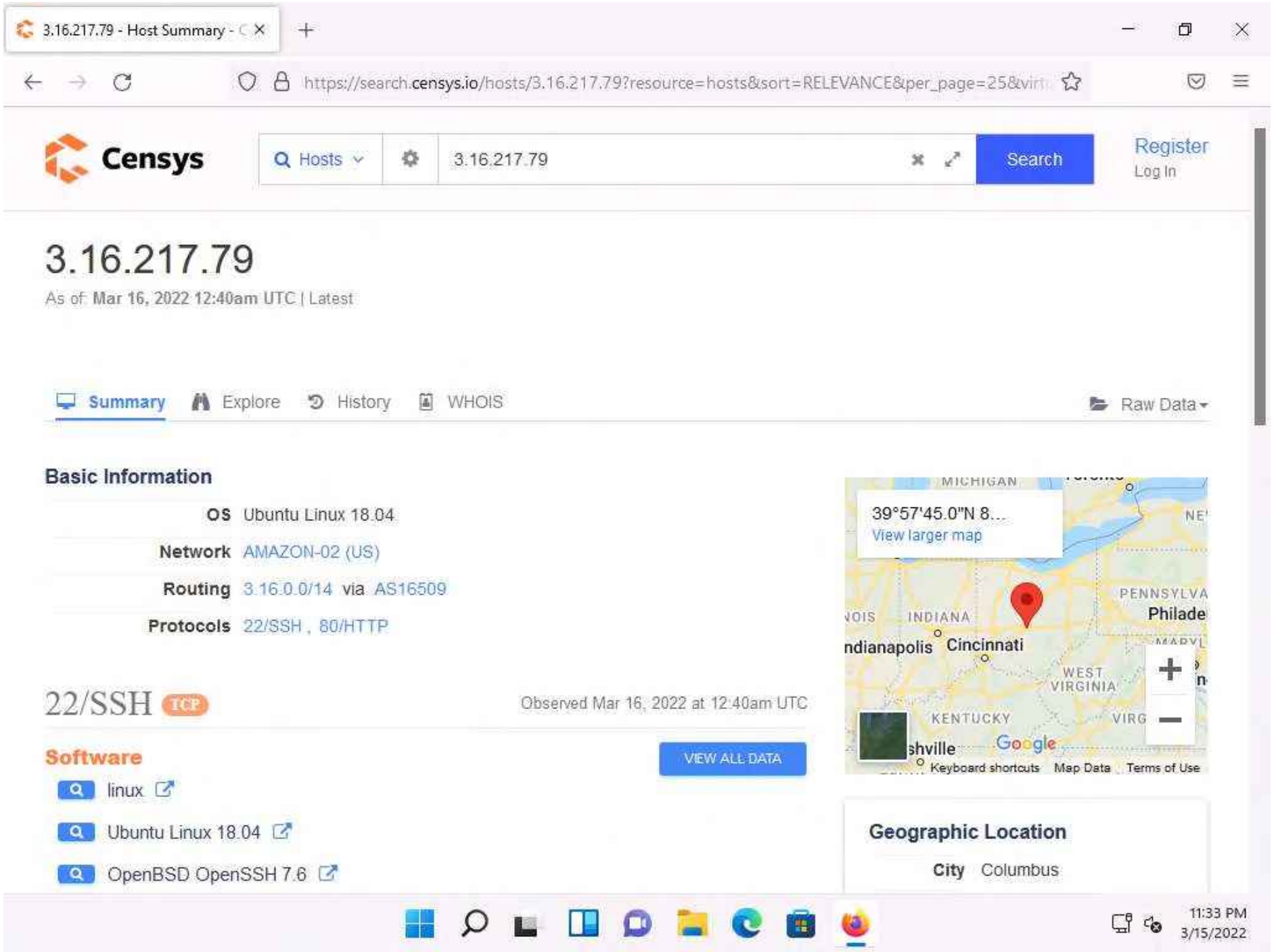
> Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. 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**) 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.



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.



4. This concludes the demonstration of gathering OS information through passive footprinting using the Censys web service.
5. You can also use webservices 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.

Lab 3: Perform Footprinting Through Social Networking Sites

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

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.

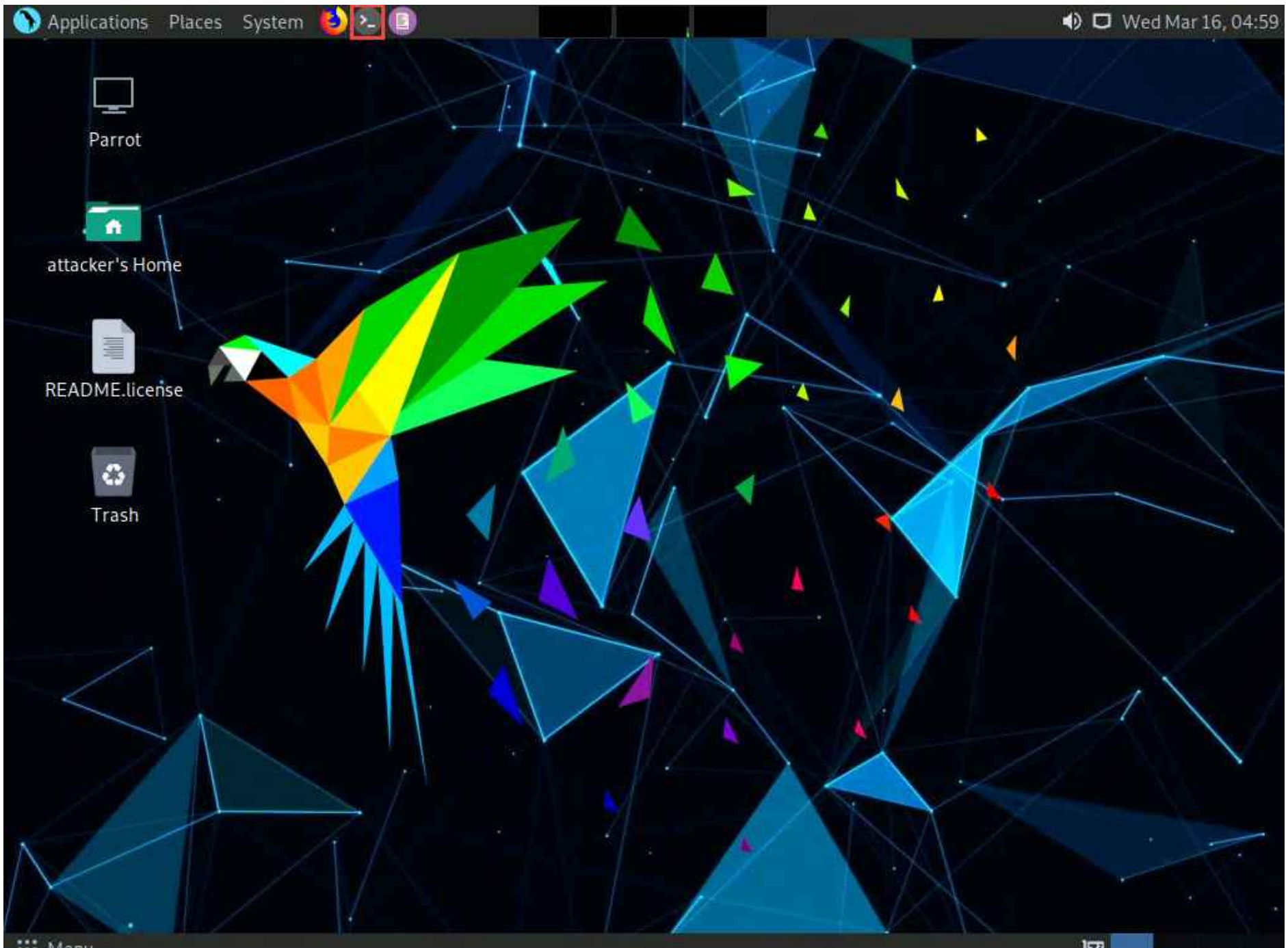
Task 1: Gather Employees' Information from LinkedIn using theHarvester

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.

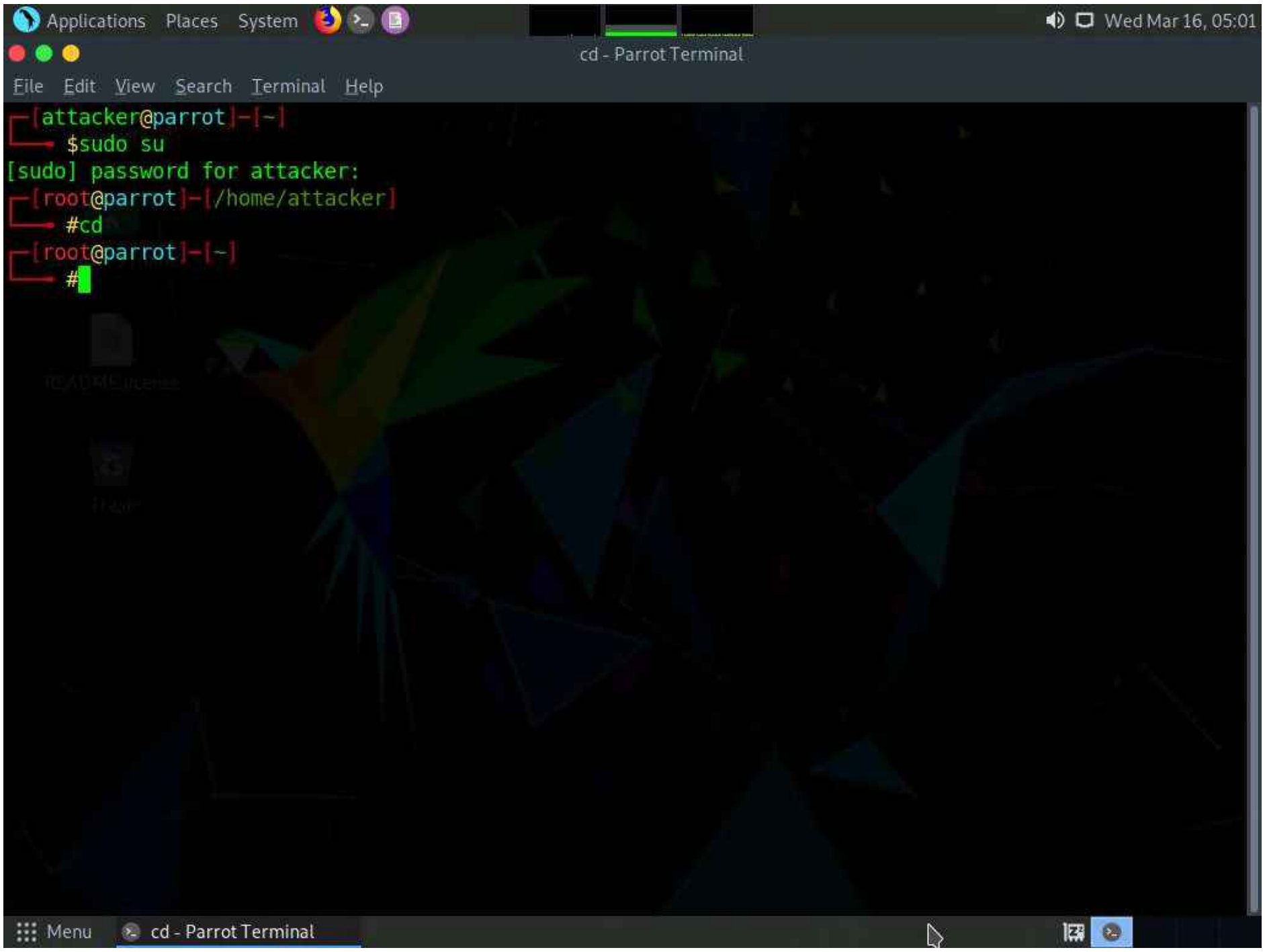
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



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.

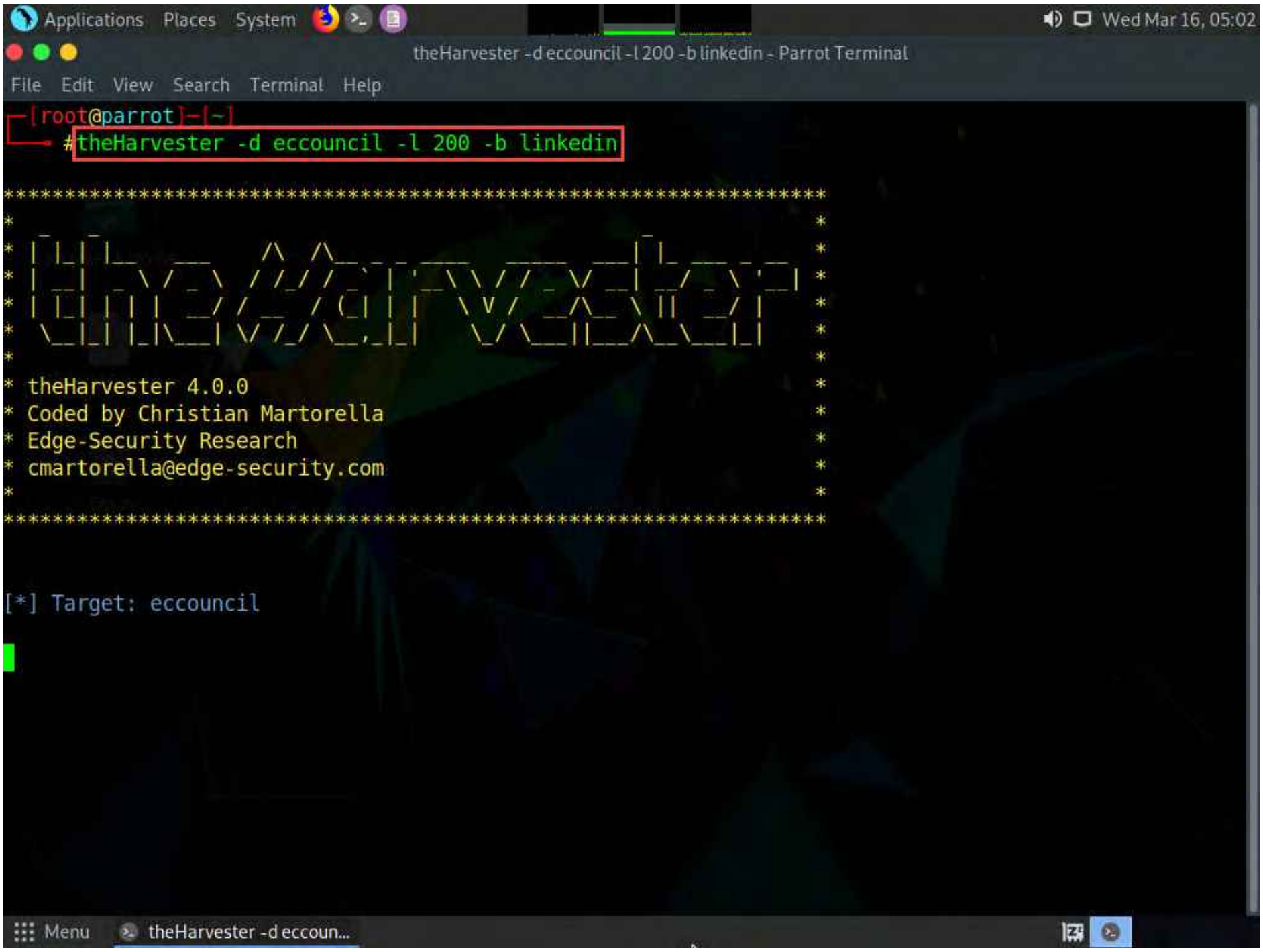
5. Now, type **cd** and press **Enter** to jump to the root directory.



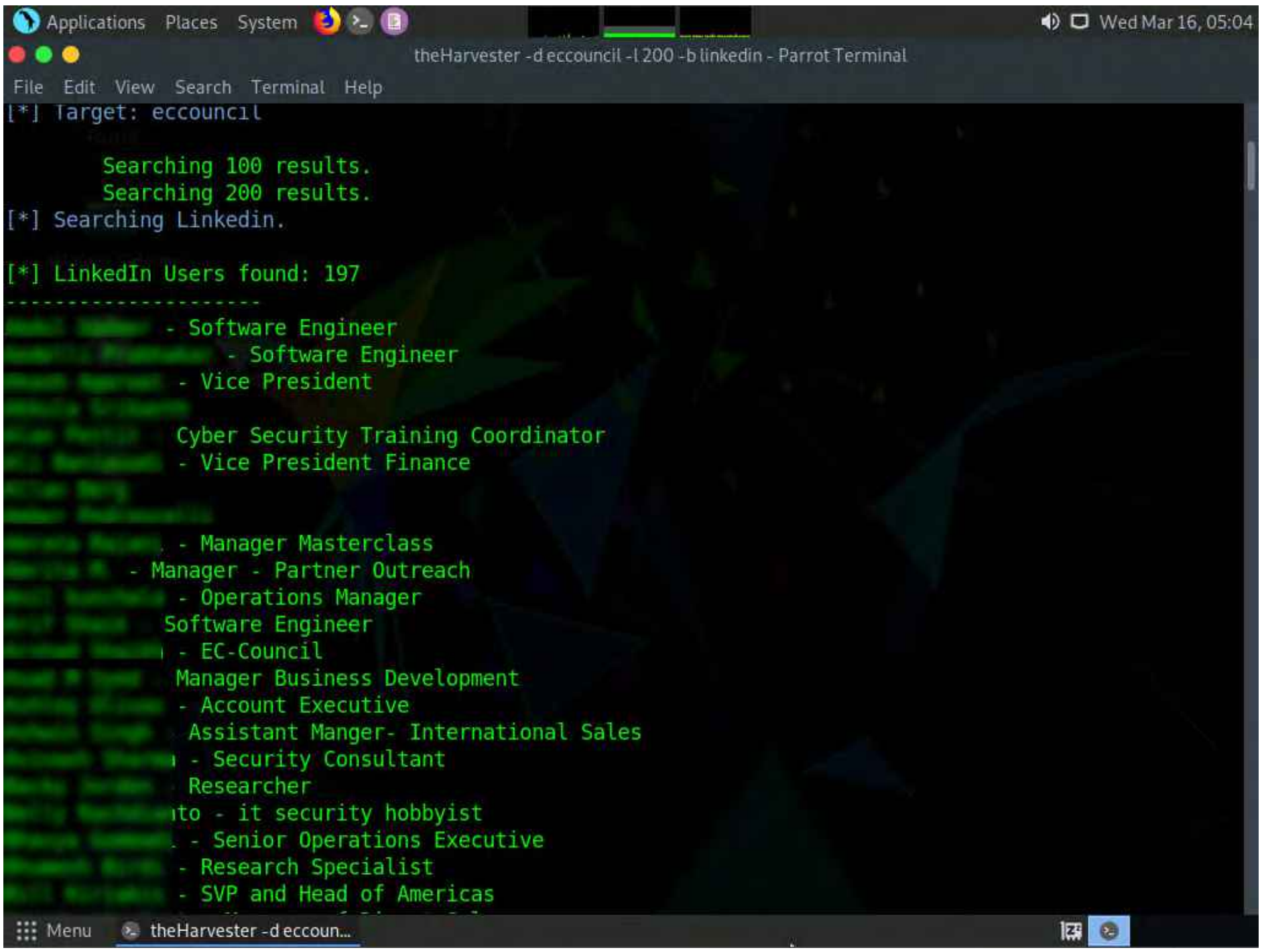
6. In the terminal window, type **theHarvester -d eccouncil -l 200 -b linkedin** and press **Enter** to see 200 results of EC-Council from the LinkedIn source.

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**.



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.



8. This concludes the demonstration of gathering employees' information from LinkedIn using theHarvester.

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

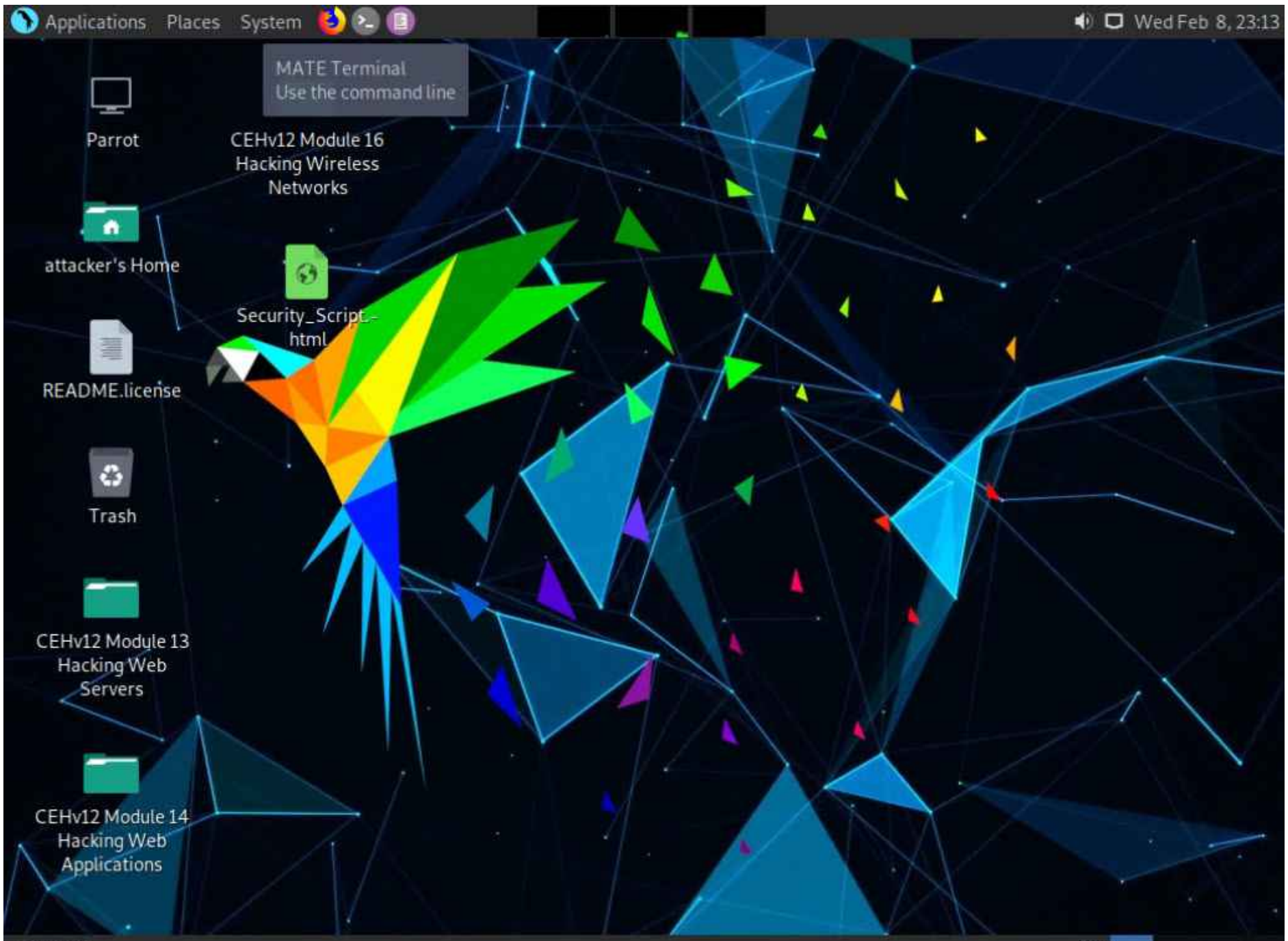
Task 2: Gather Personal Information from Various Social Networking Sites using Sherlock

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.

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

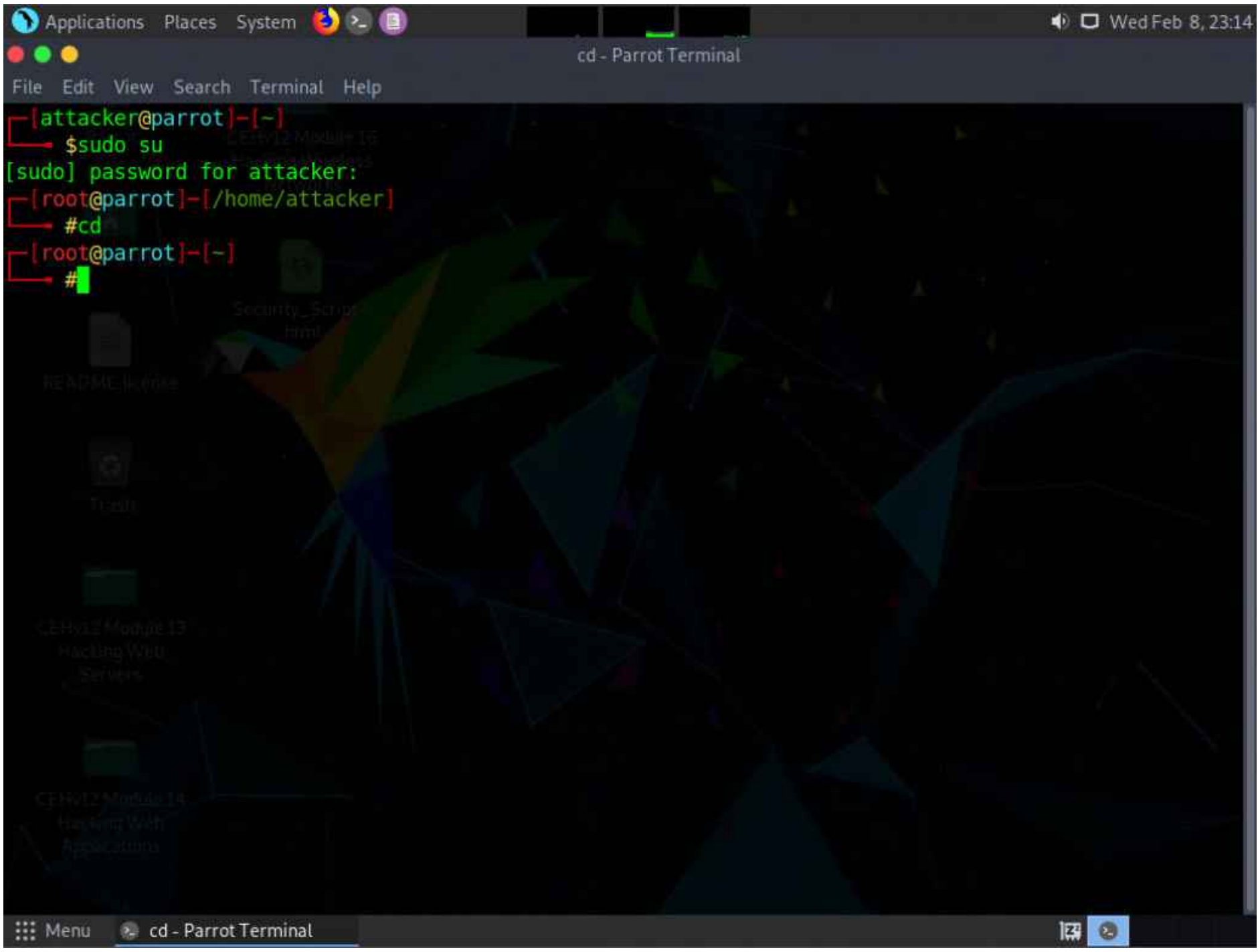


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

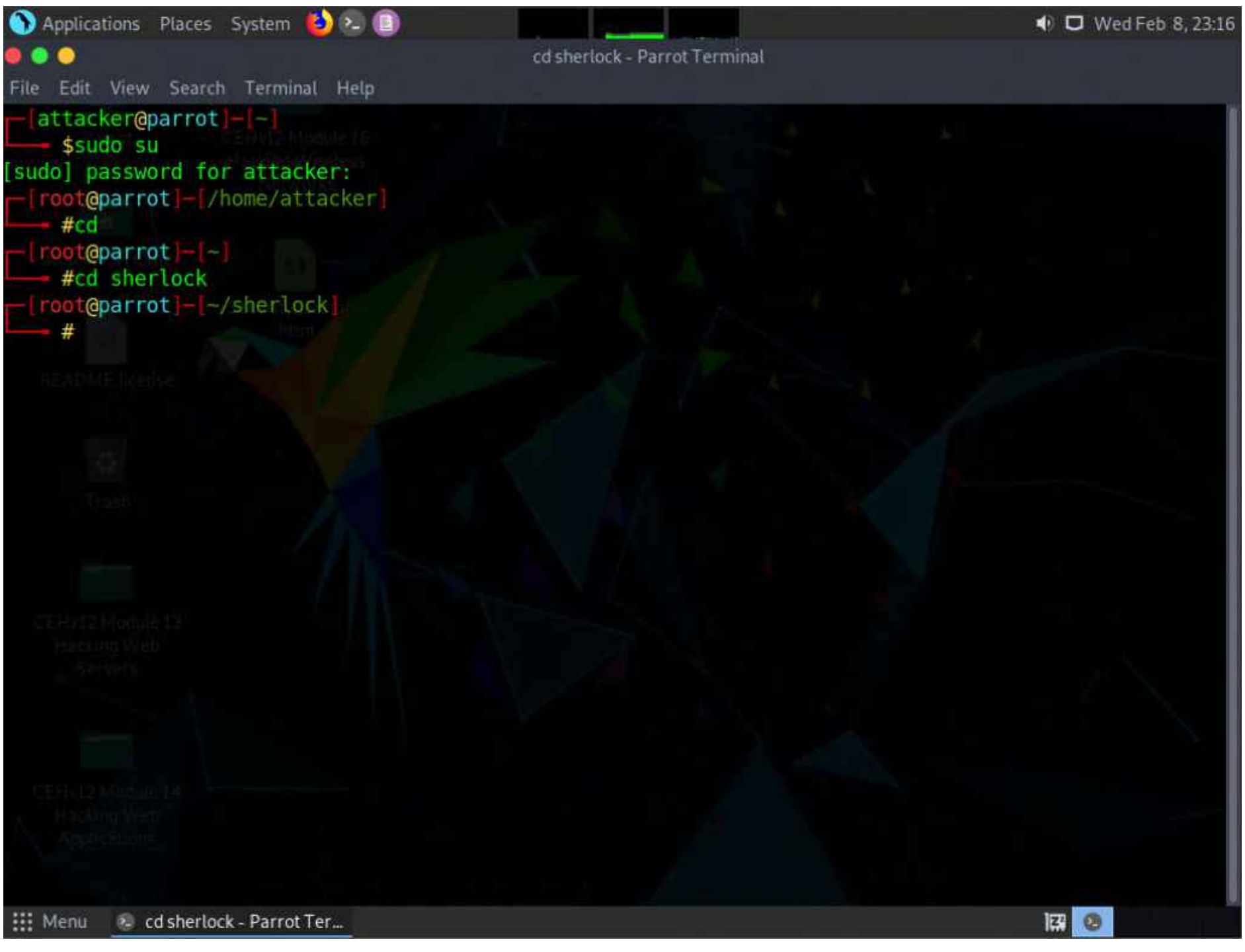
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

4. Type **cd** and press **Enter** to navigate to the root directory.

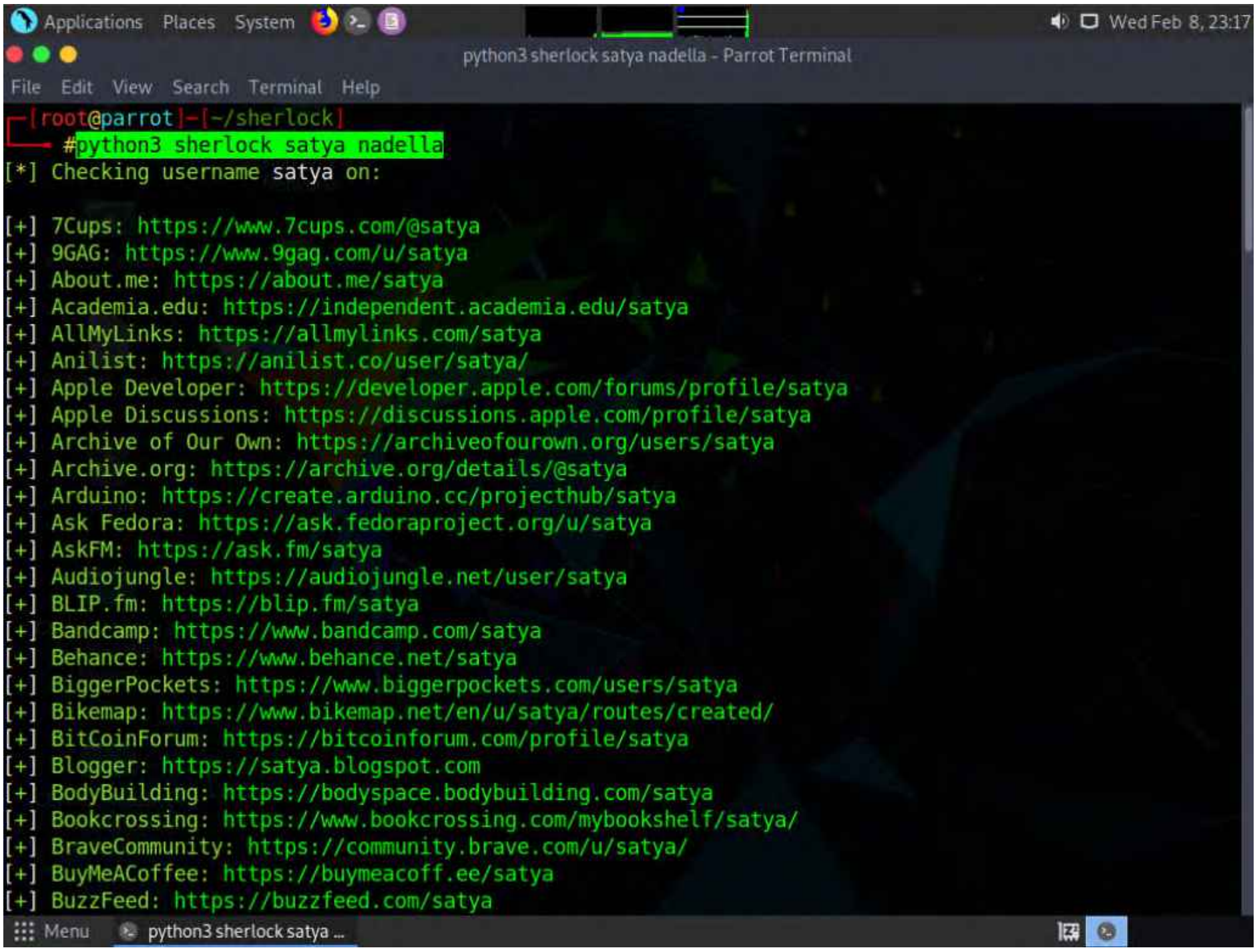


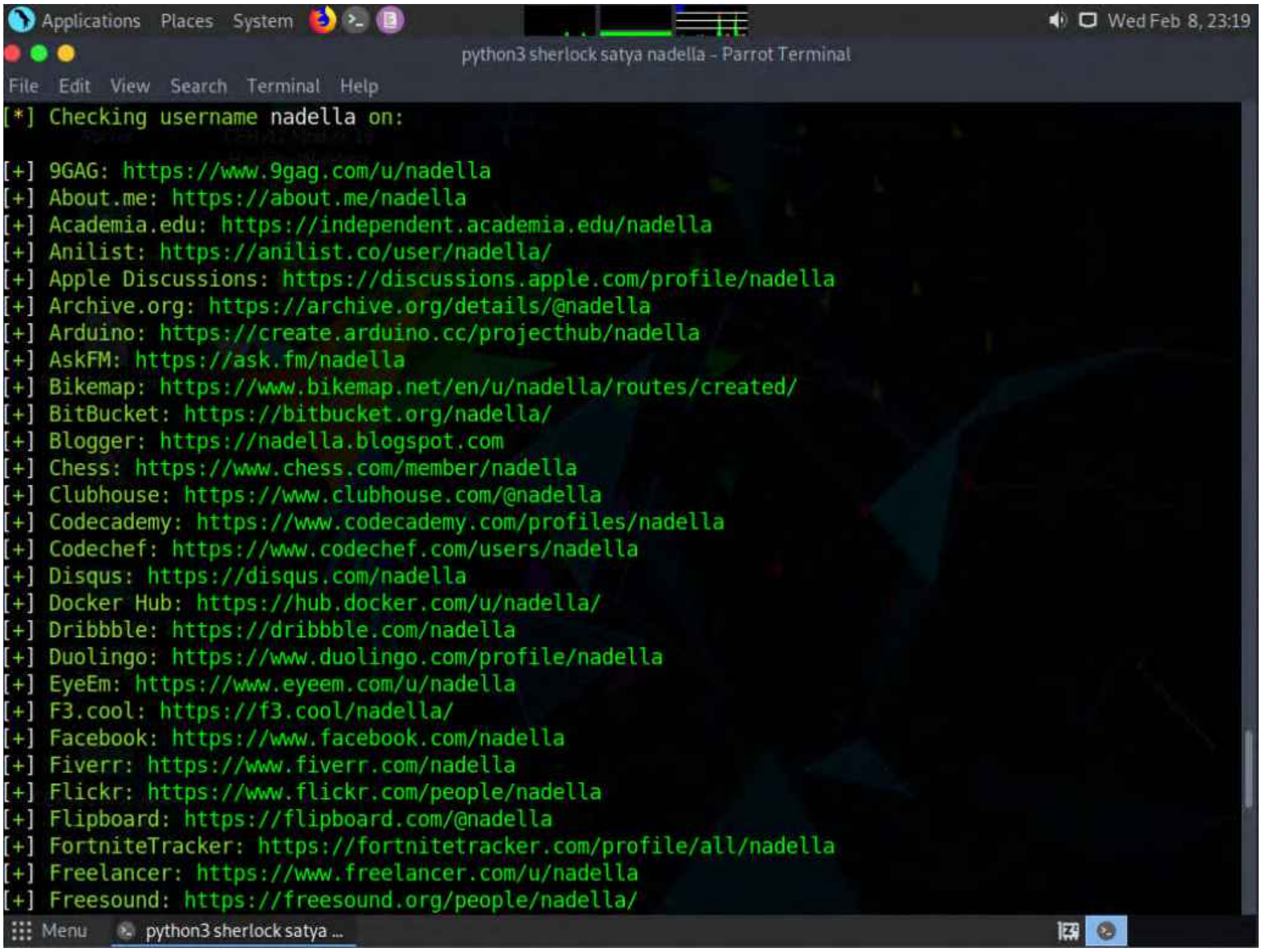
5. Type **cd sherlock** and press **Enter** to navigate to the sherlock folder.



6. Type **python3 sherlock 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.





7. 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.
8. This concludes the demonstration of gathering person information from various social networking sites using Sherlock.
9. 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.
10. Close all open windows and document all the acquired information.

Lab 4: Perform Website Footprinting

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

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.

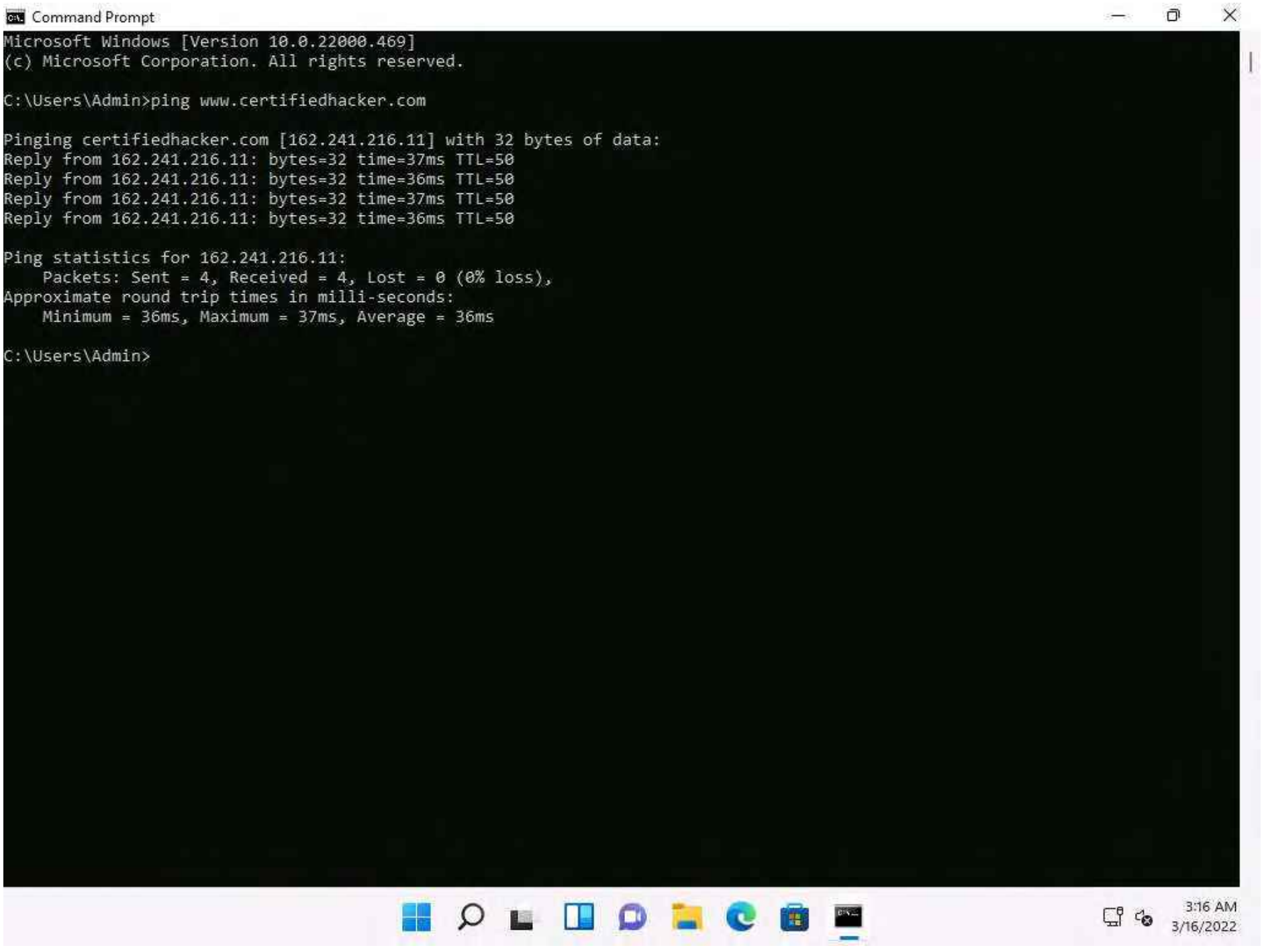
Task 1: Gather Information About a Target Website using Ping Command Line Utility

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.

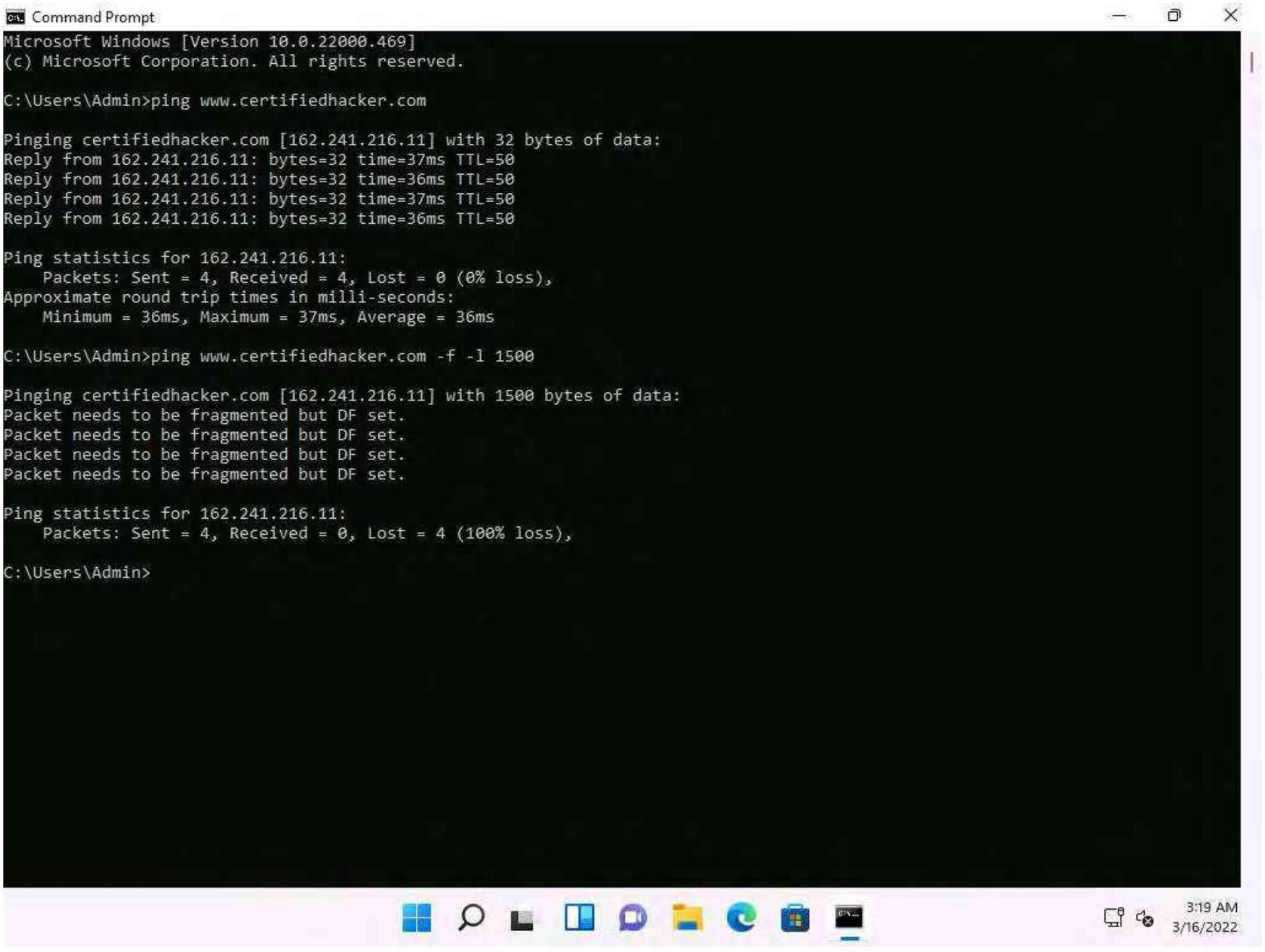
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Open the **Command Prompt** window. Type **ping www.certifiedhacker.com** and press **Enter** to find its IP address. The displayed response should be similar to the one shown in the screenshot.

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



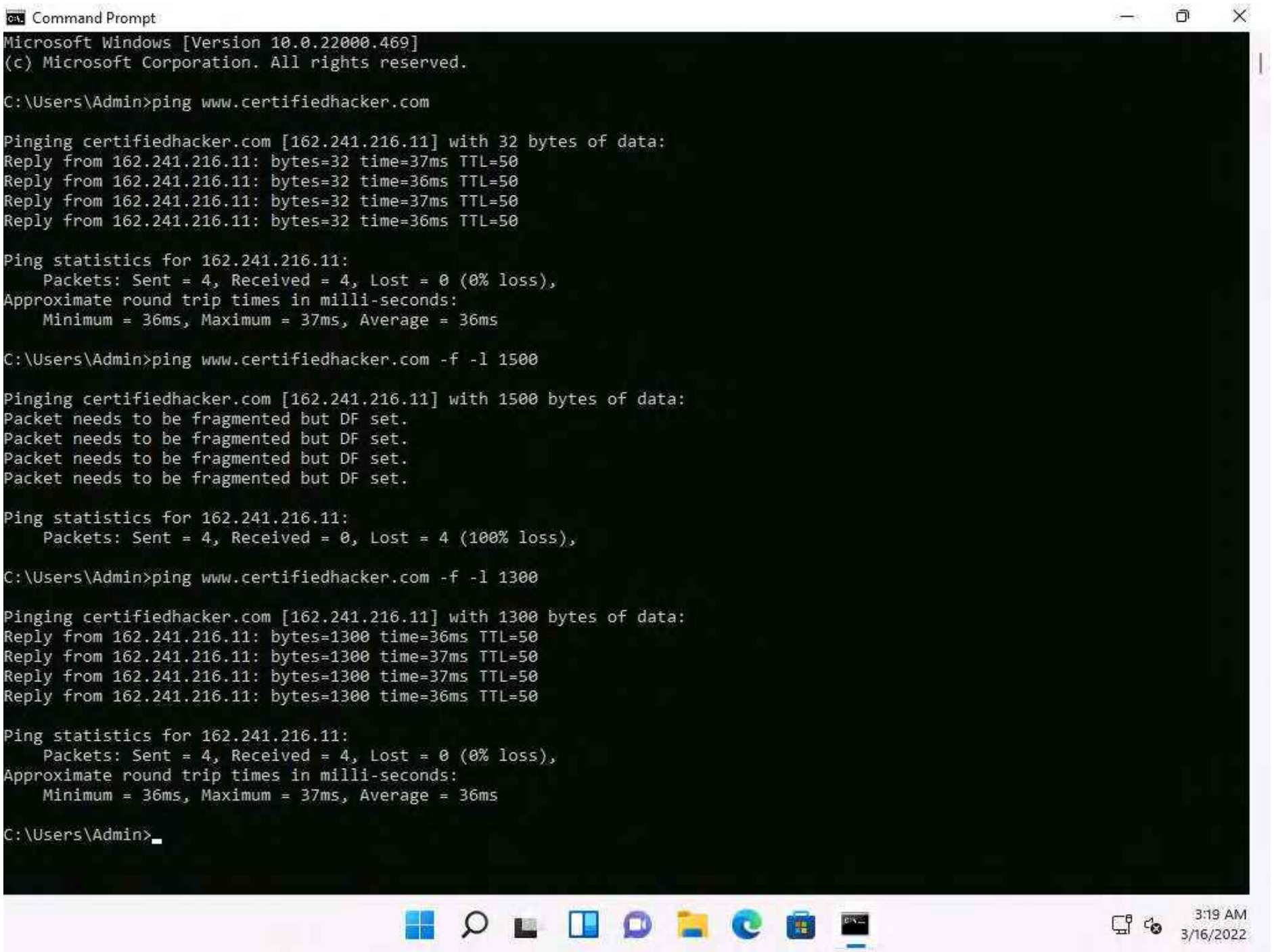
3. Note the target domain's IP address in the result above (here, **162.241.216.11**). You also obtain information on Ping Statistics such as packets sent, packets received, packets lost, and approximate round-trip time.
4. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1500** and press **Enter**.

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



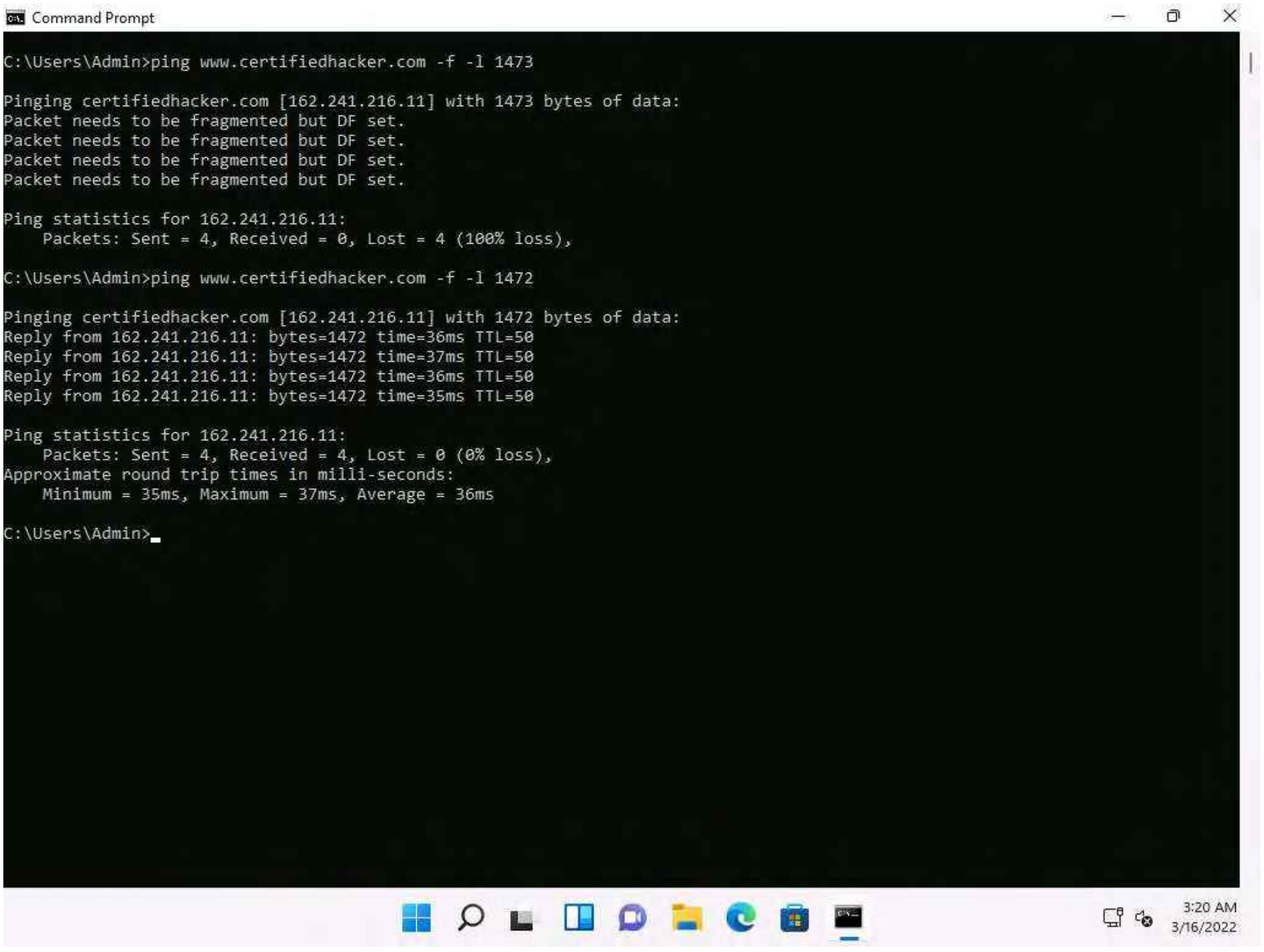
5. The response, **Packet needs to be fragmented but DF set**, means that the frame is too large to be on the network and needs to be fragmented. The packet was not sent as we used the **-f ** switch with the ping command, and the ping command returned this error.

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



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

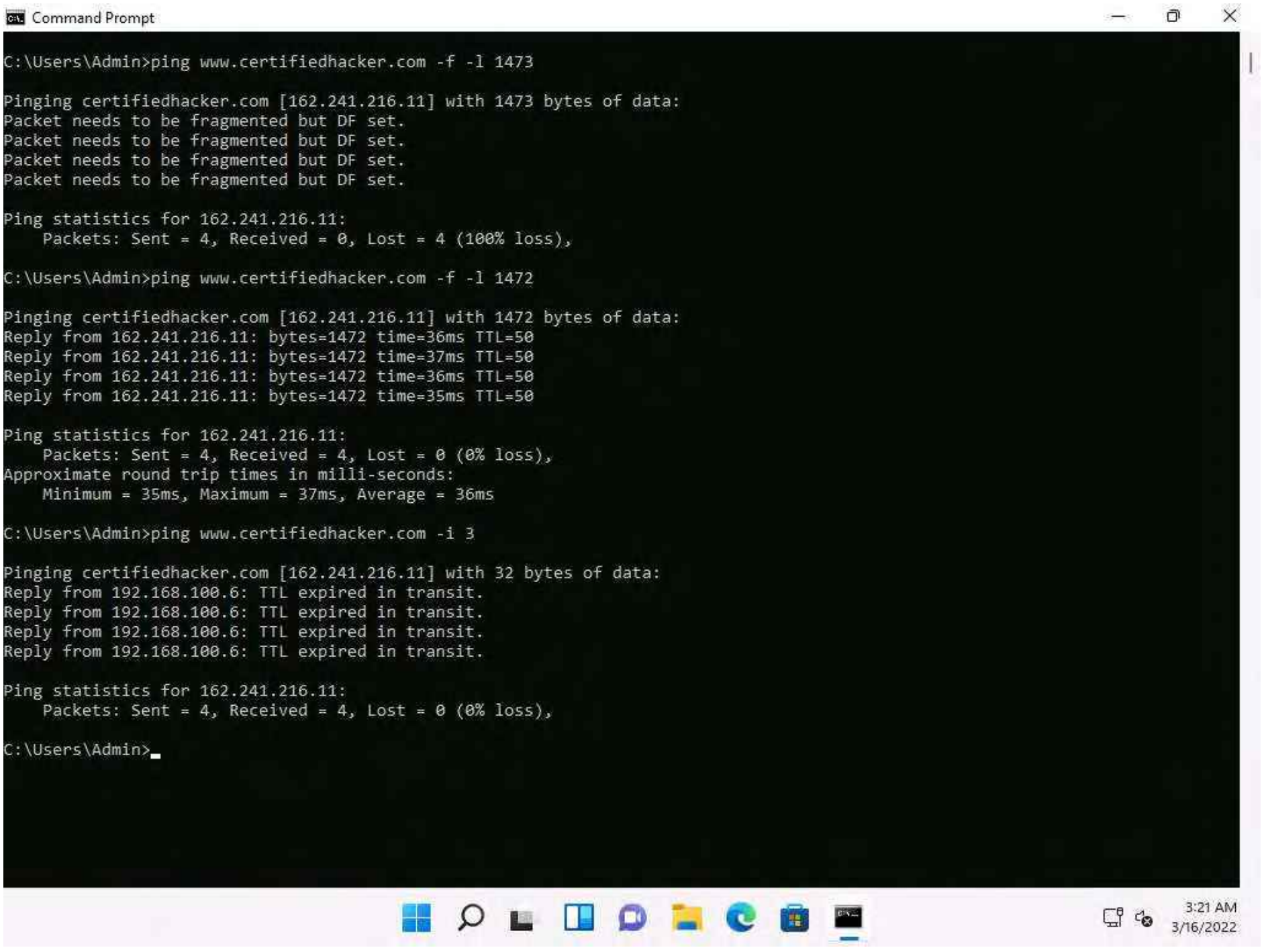
8. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com -f -l 1473** replies with **Packet needs to be fragmented but DF set**, and **ping www.certifiedhacker.com -f -l 1472** replies with a successful ping. It indicates that **1472** bytes are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



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.

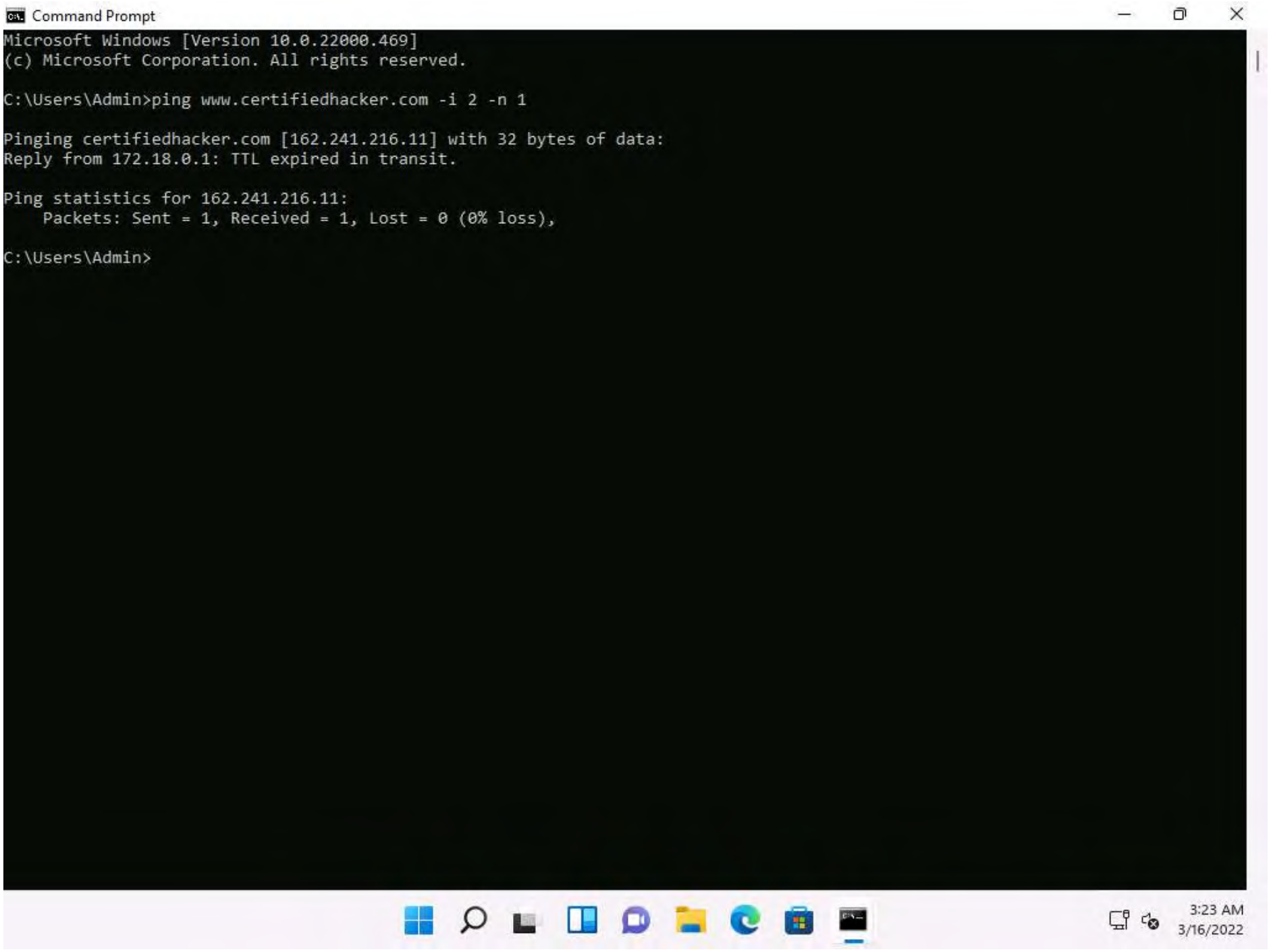


11. Reply from **192.168.100.6**: **TTL expired in transit** means that the router (192.168.100.6, you will have some other IP address) discarded the frame because its TTL has expired (reached 0).

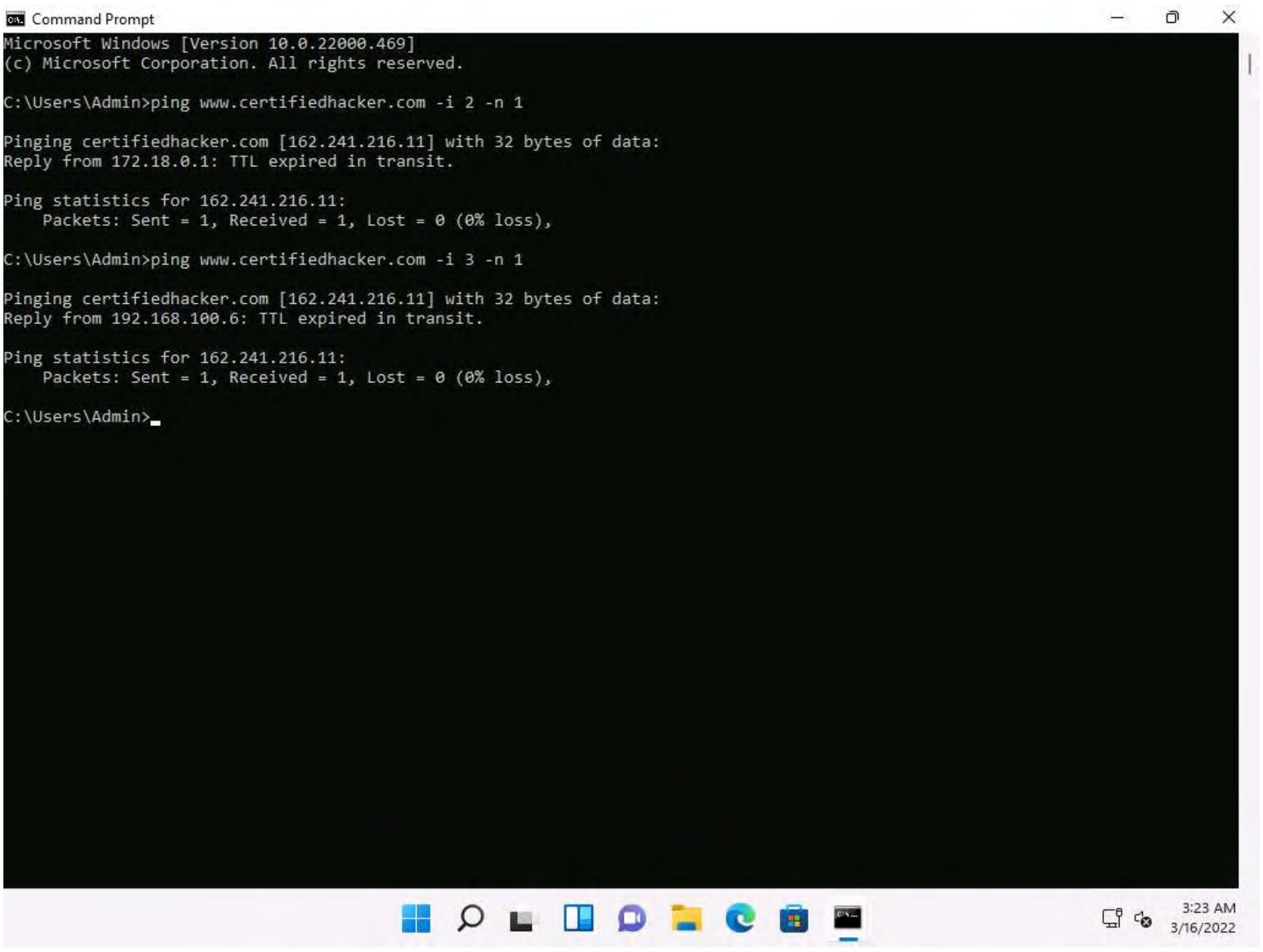
> Note: The IP address 192.168.100.6 might vary when you perform this task.

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.

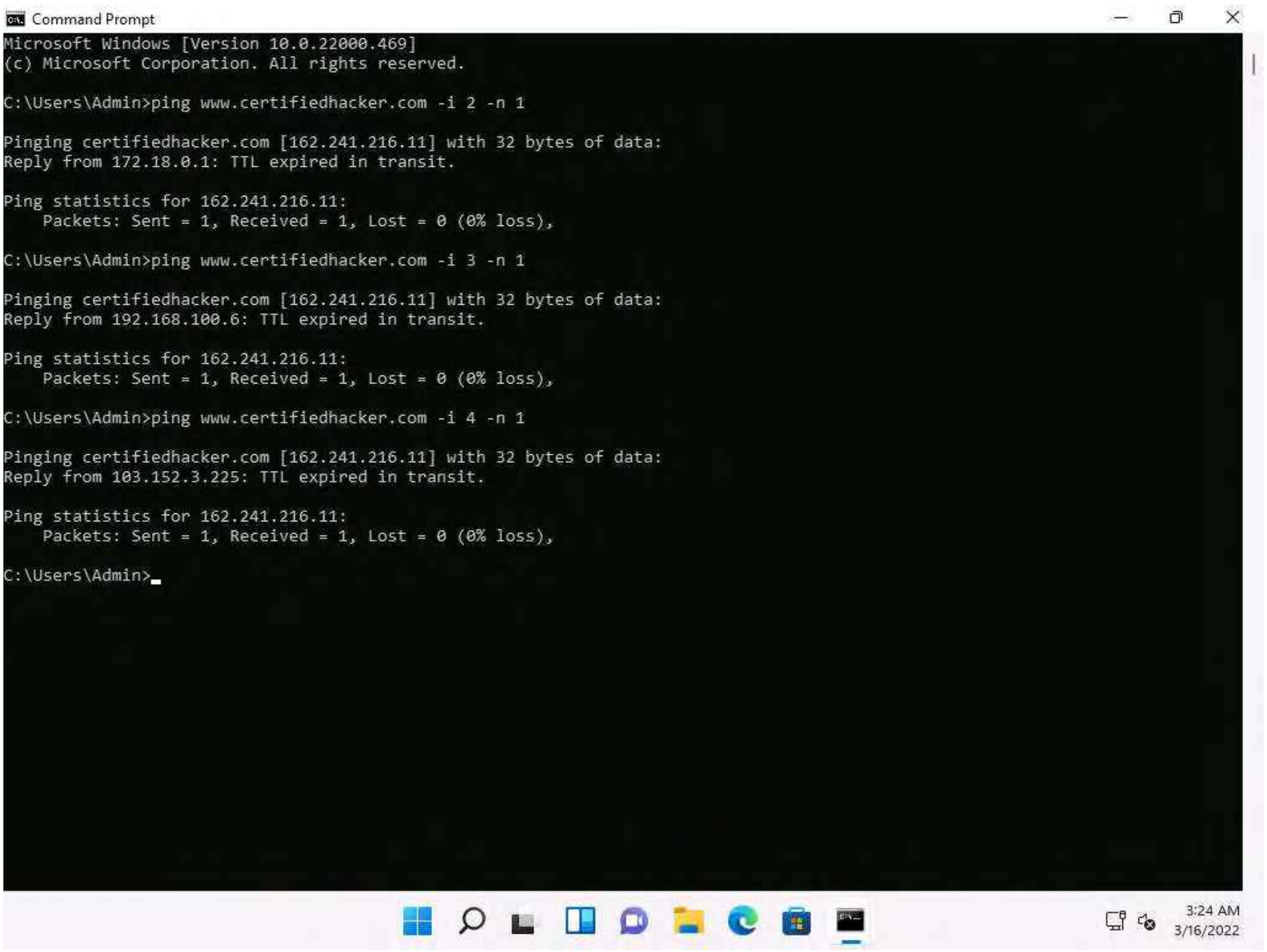


13. Type **ping www.certifiedhacker.com -i 3 -n 1**. This sets the TTL value to **3**.



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**.



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.

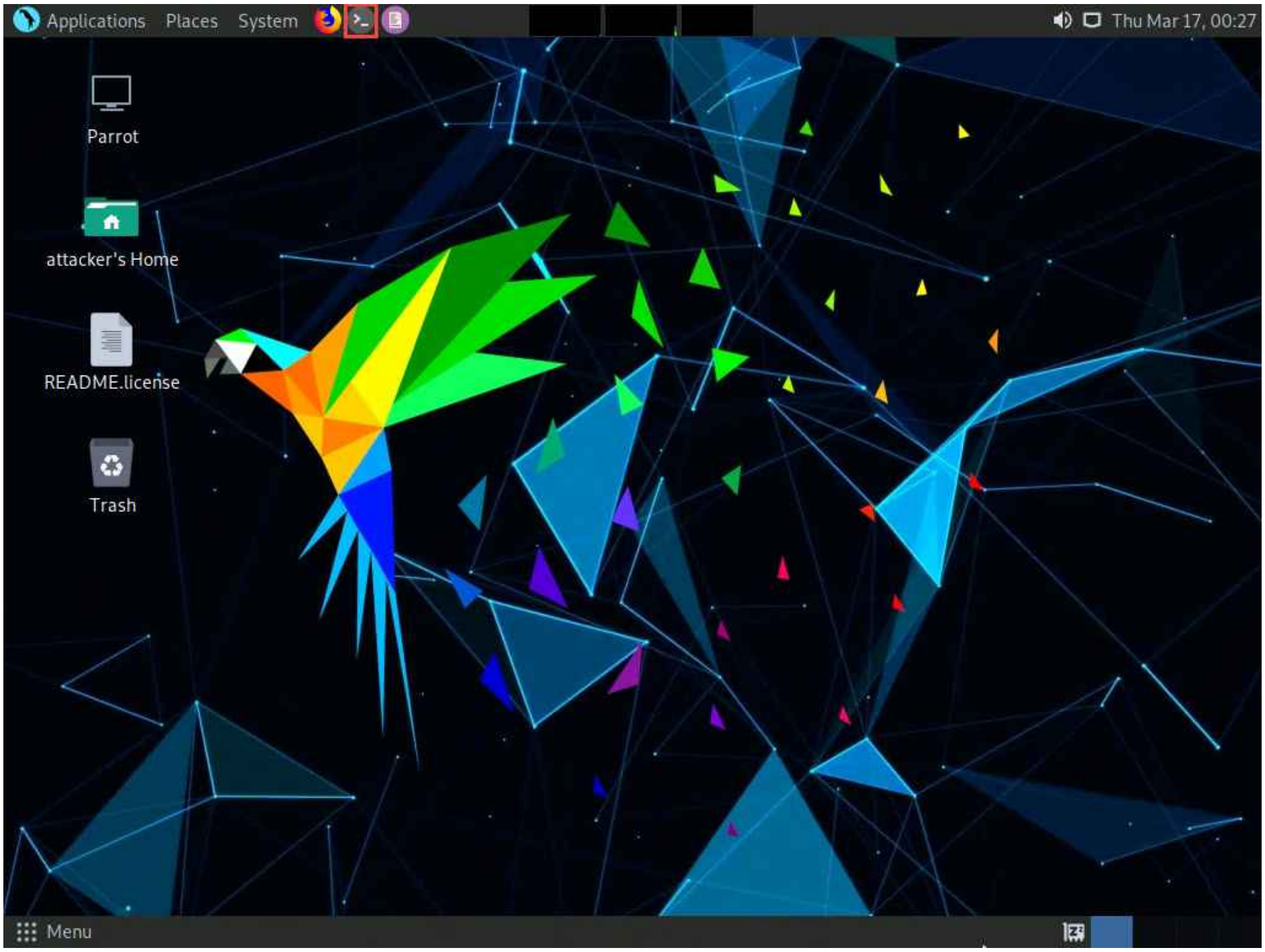
18. On successfully finding the TTL value it will imply that the reply is received from the destination host (**162.241.216.11**).
19. This concludes the demonstration of gathering information about a target website using Ping command-line utility (such as the IP address of the target website, hop count 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** as the target website. However, you can select a target domain of your choice.

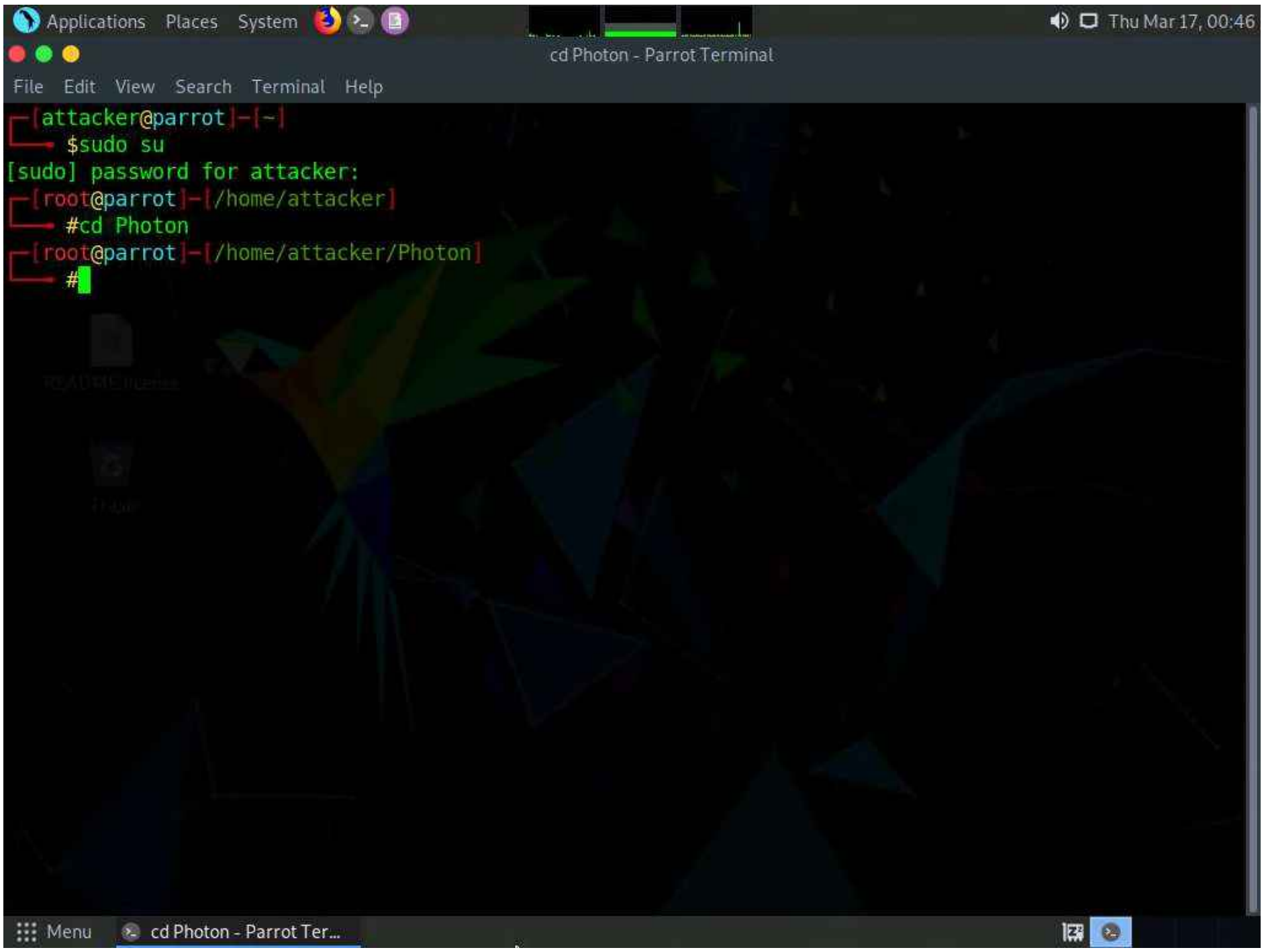
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



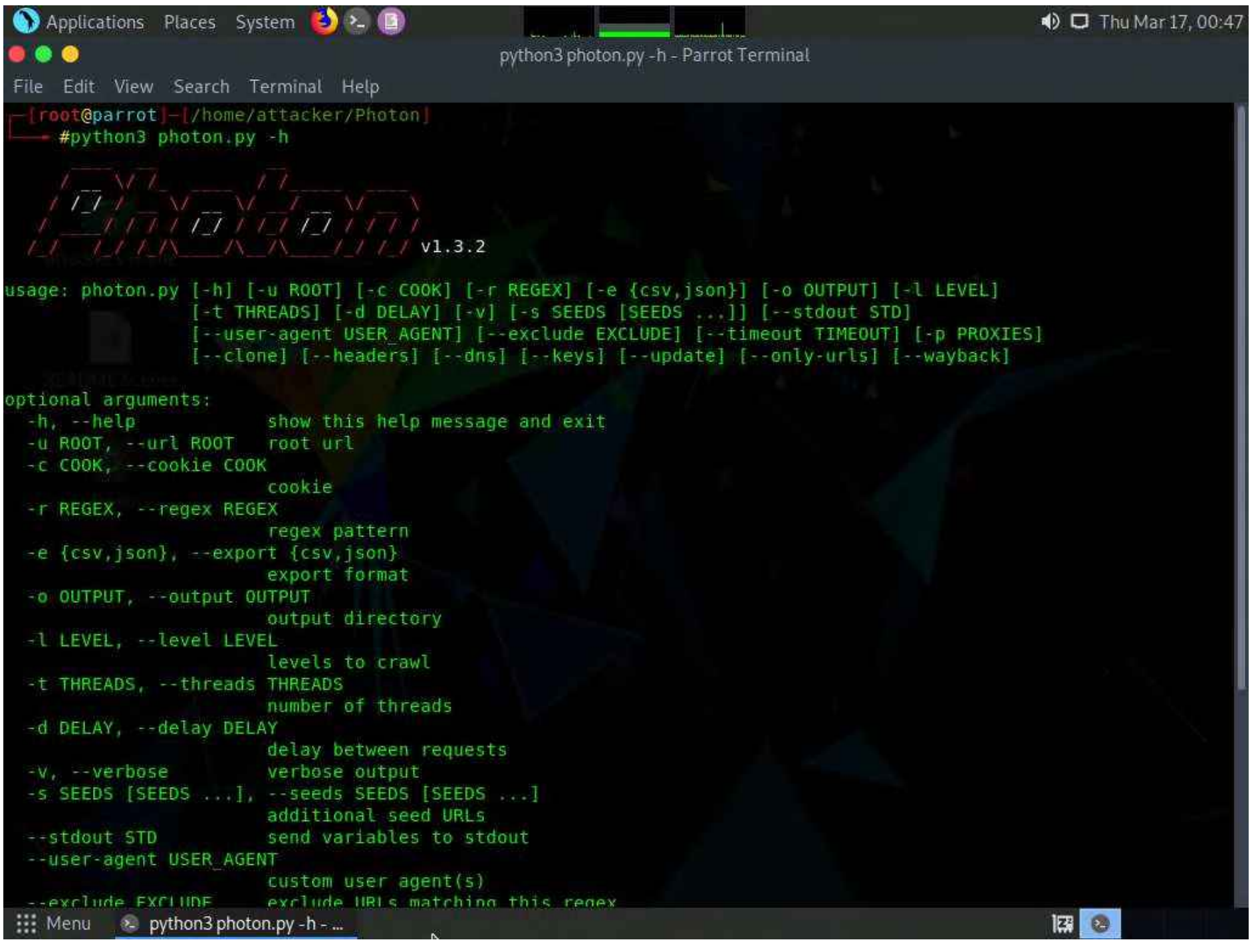
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> 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.



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

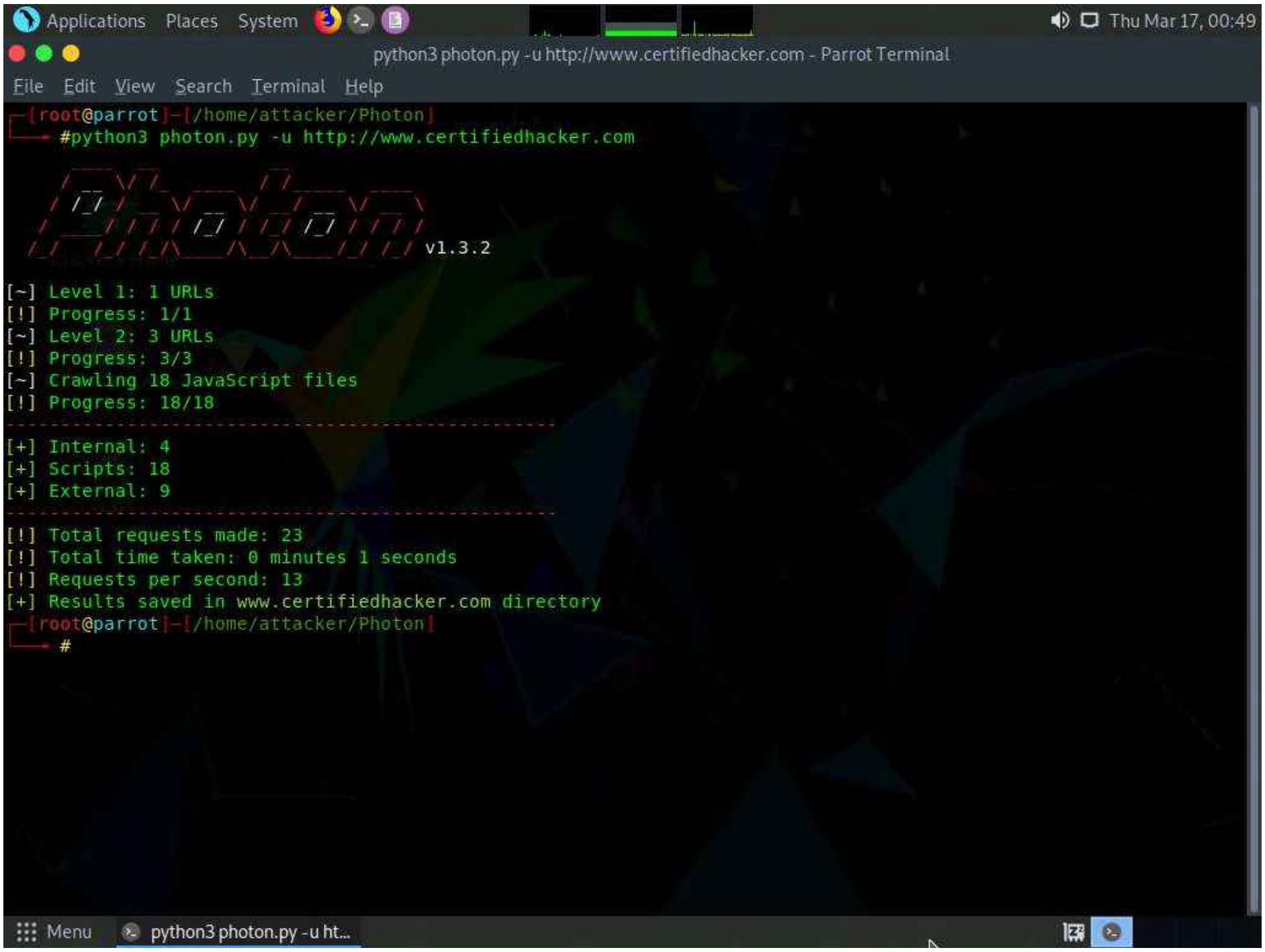


7. Type **python3 photon.py -u http://www.certifiedhacker.com** and press **Enter** to crawl the target website for internal, external and scripts URLs.

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

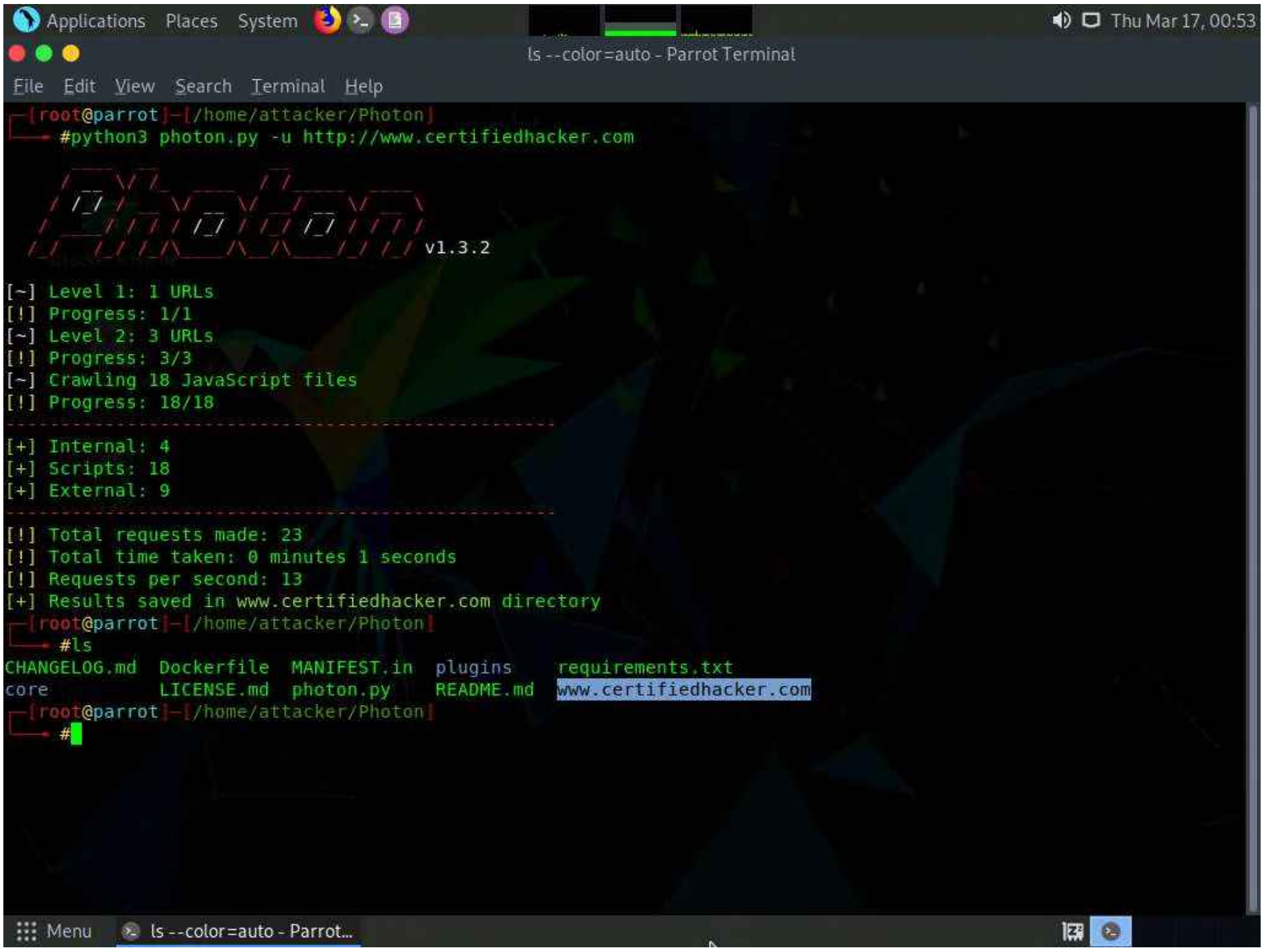
8. The results obtained are saved in **www.certifiedhacker.com** directory under Photon folder.

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

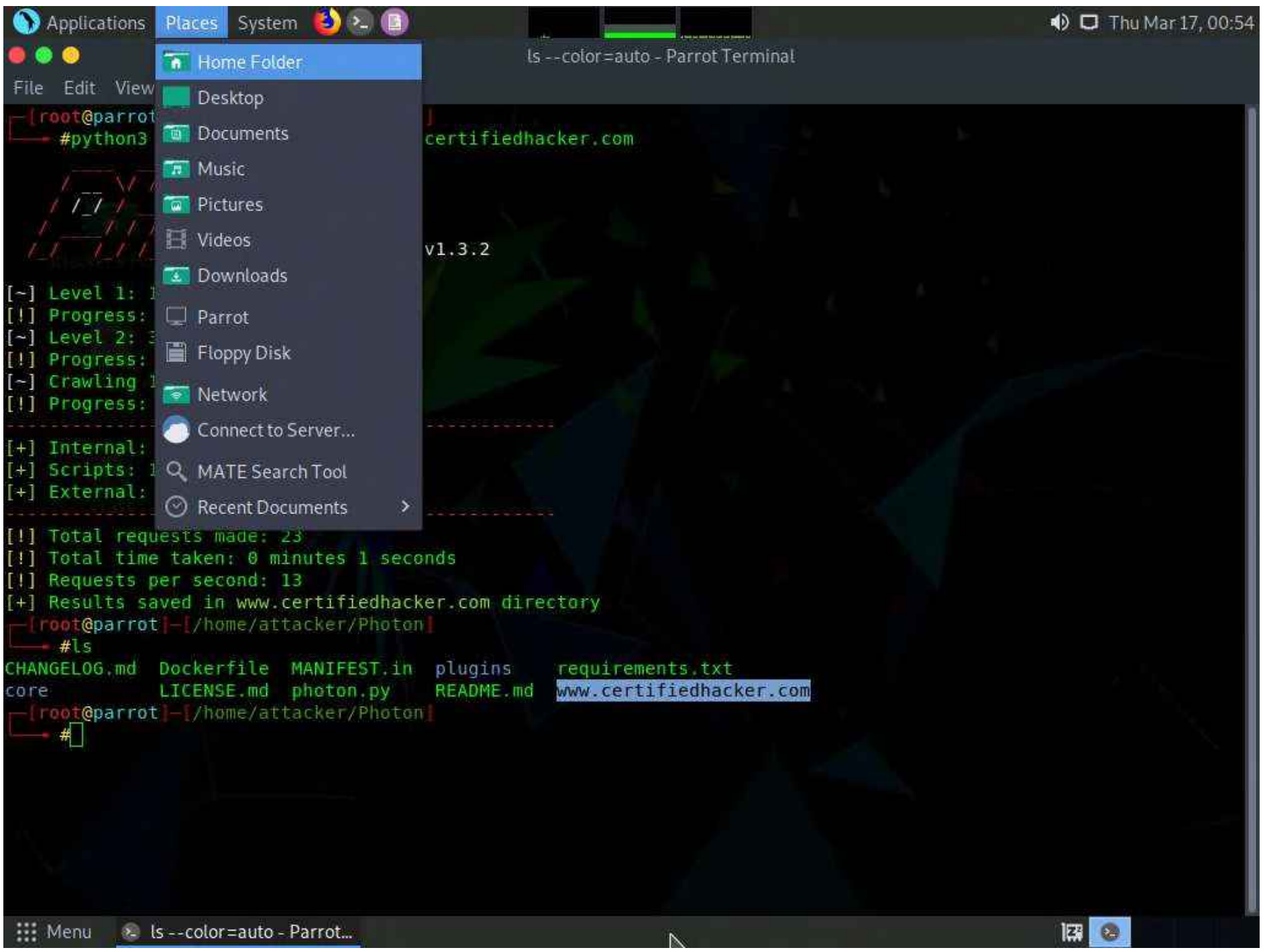


9. Type **ls** and press **Enter** to view the folder content.

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

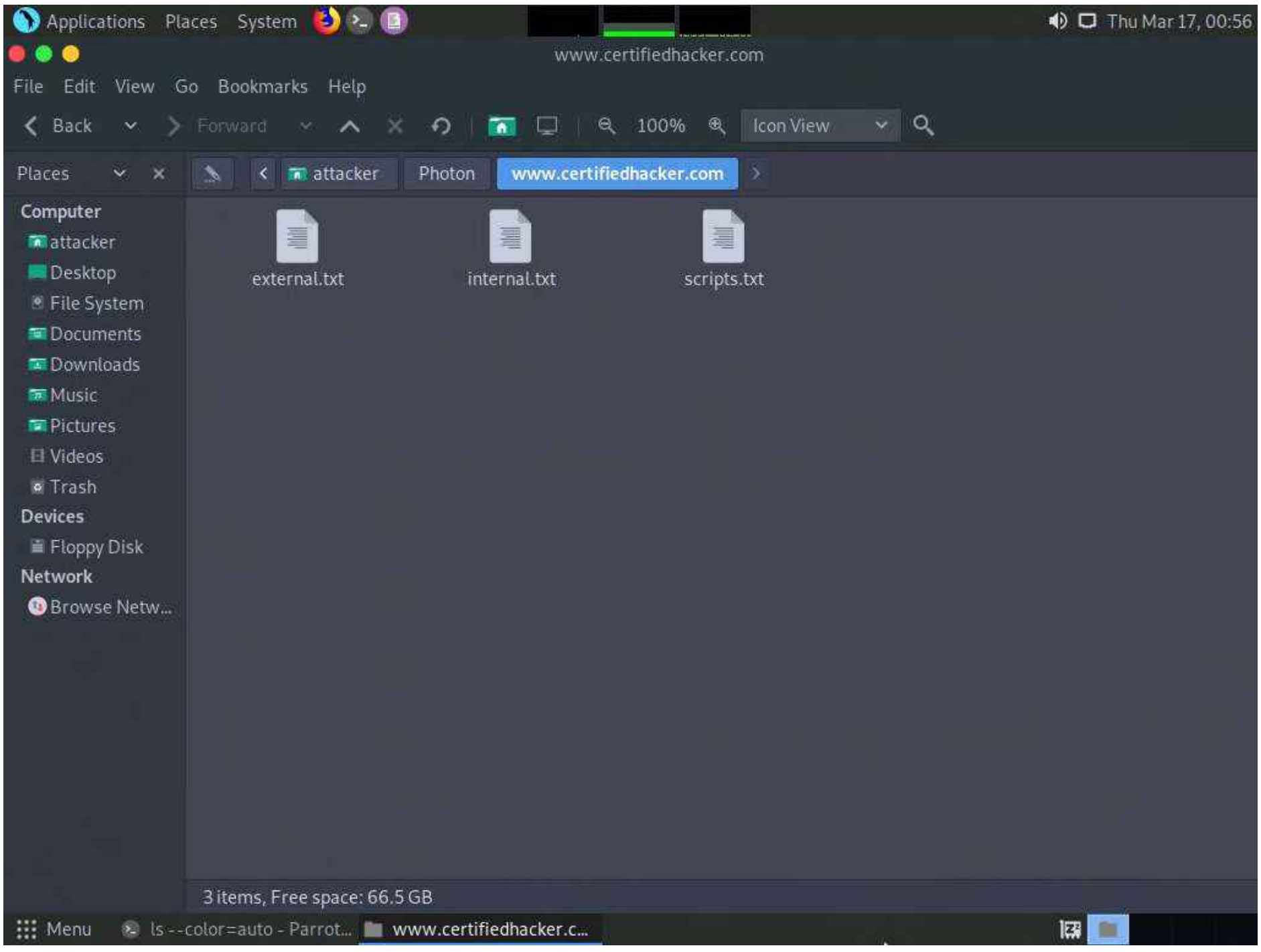


11. Now, click **Places** from the top-section of the **Desktop** and select **Home Folder**.



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

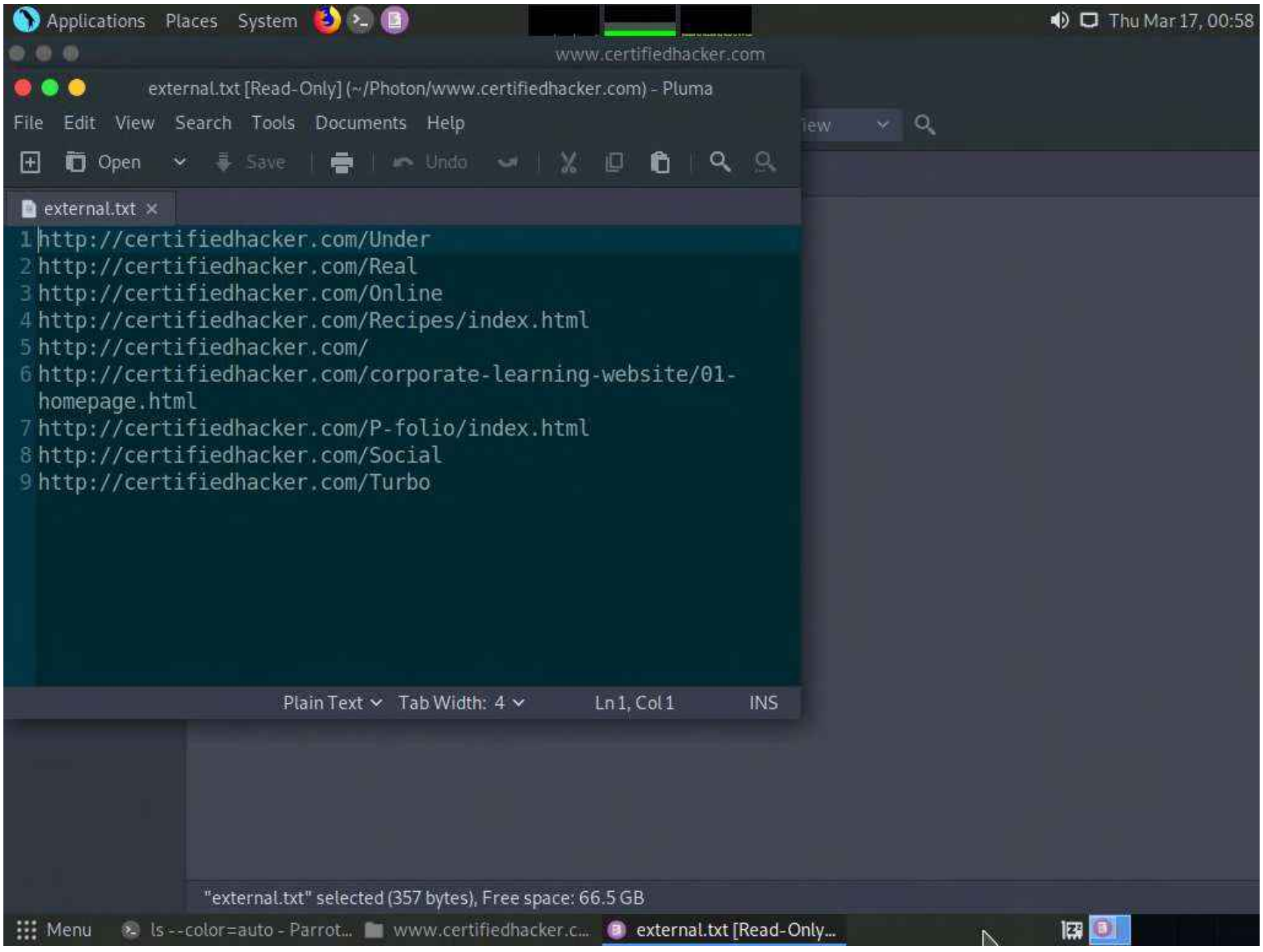
13. You can observe three text files in this folder: external, internal and scripts.



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.



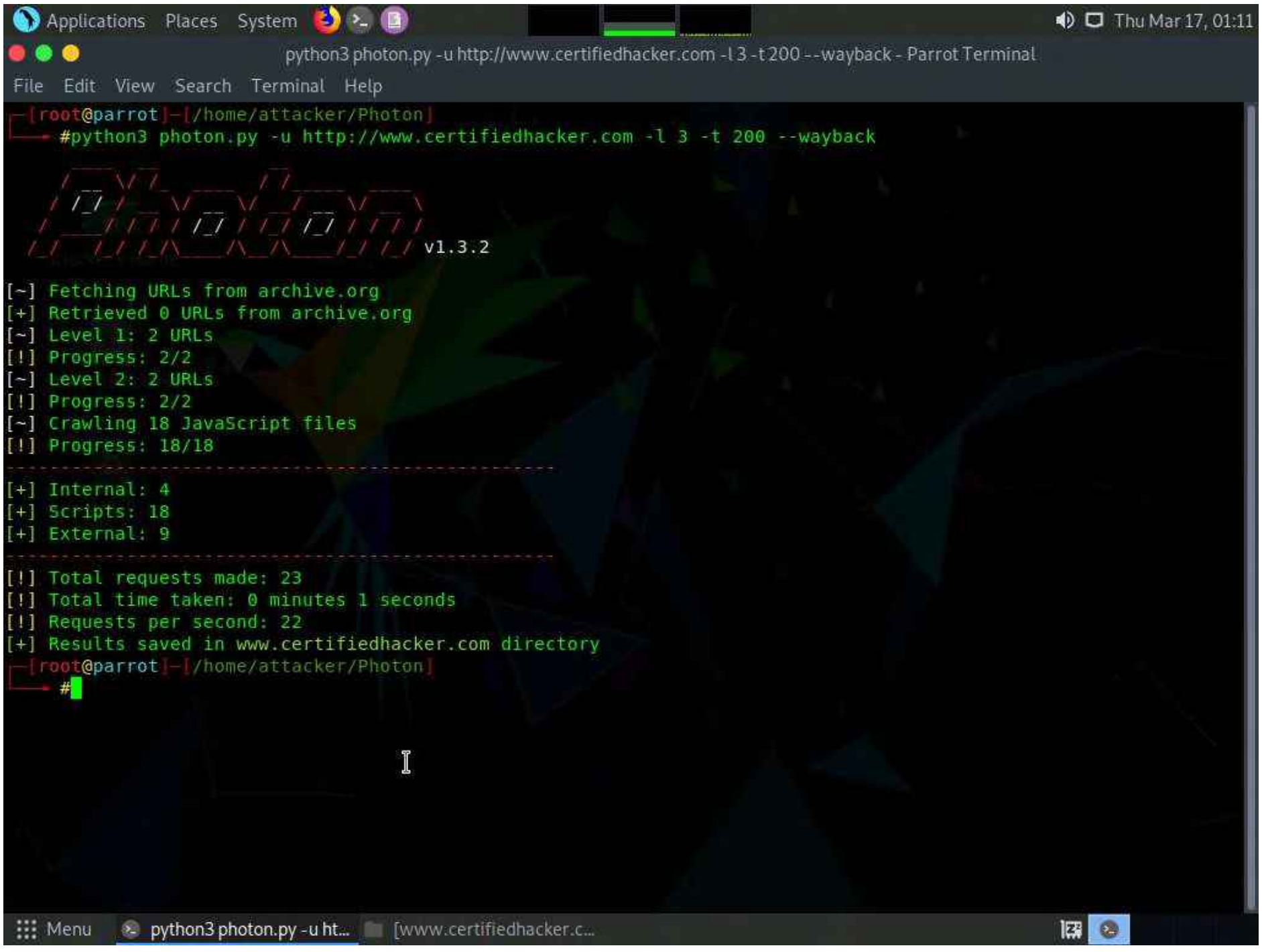
16. Similarly, you can view internal and scripts text files containing URLs that are crawled by Photon tool.

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.



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.

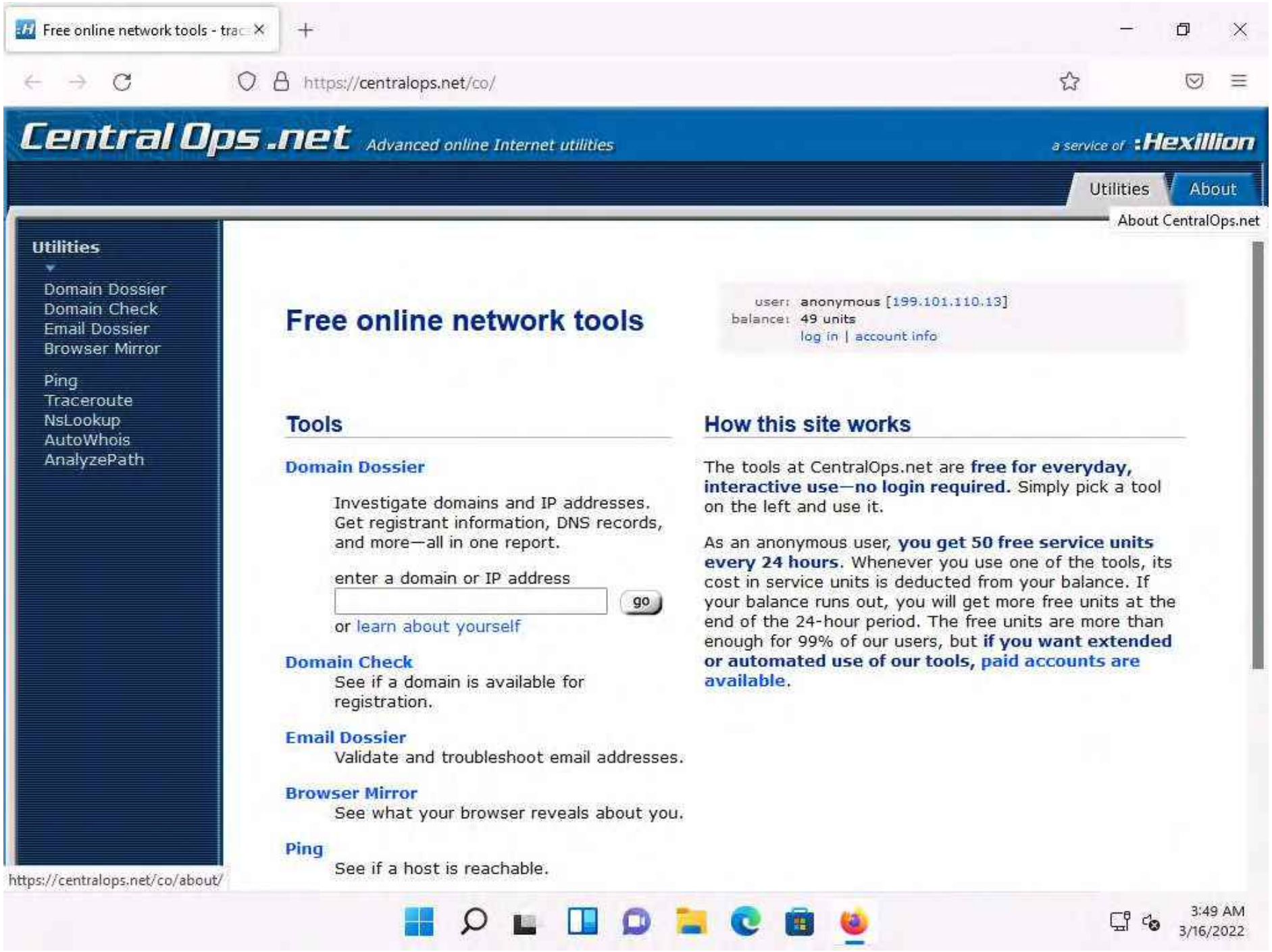
22. Close all open windows and document all the acquired information

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

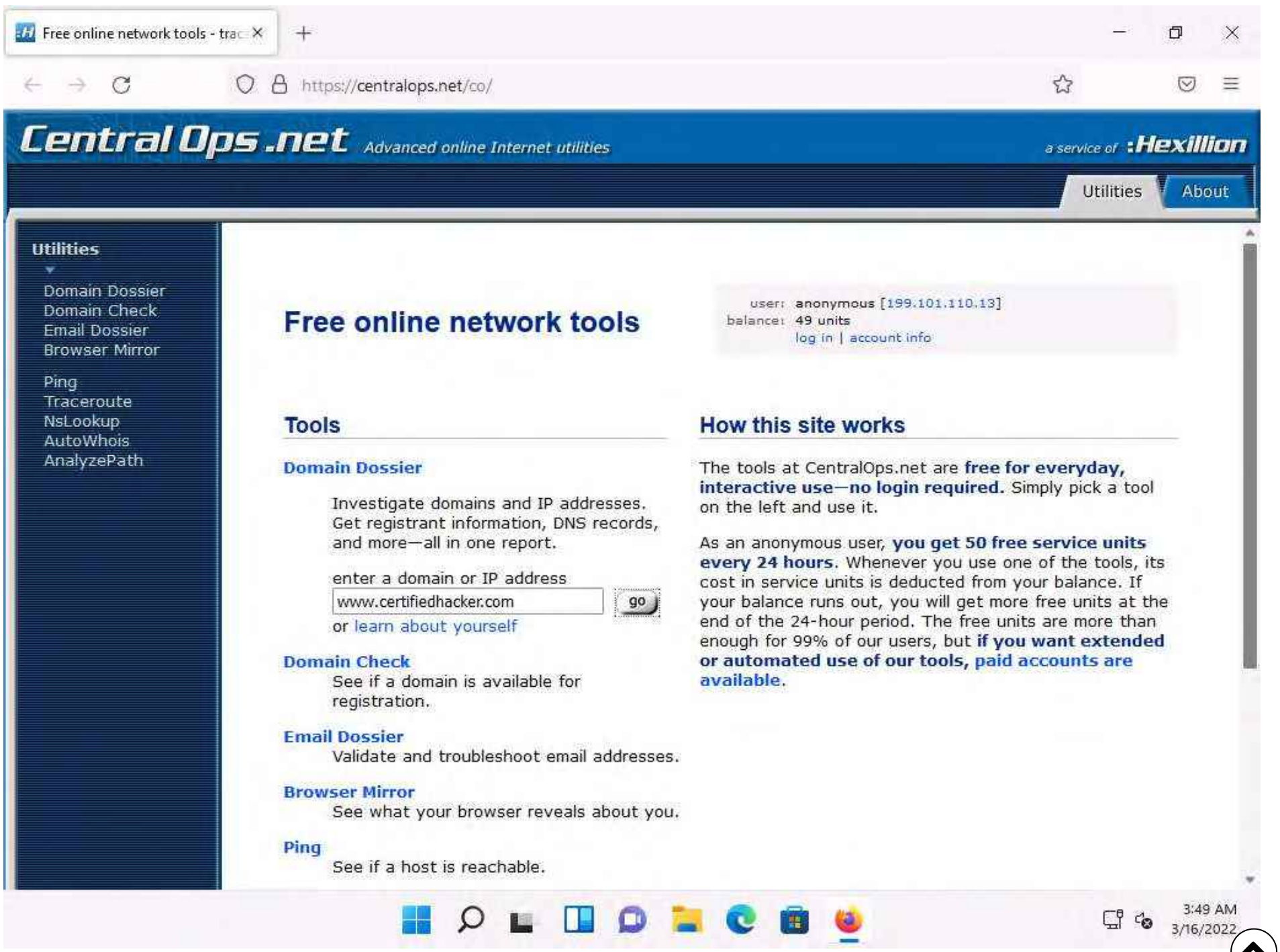
CentralOps (centralops.net) is a free online network scanner that investigates domains and IP addresses, DNS records, traceroute, nslookup, whois searches, etc.

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

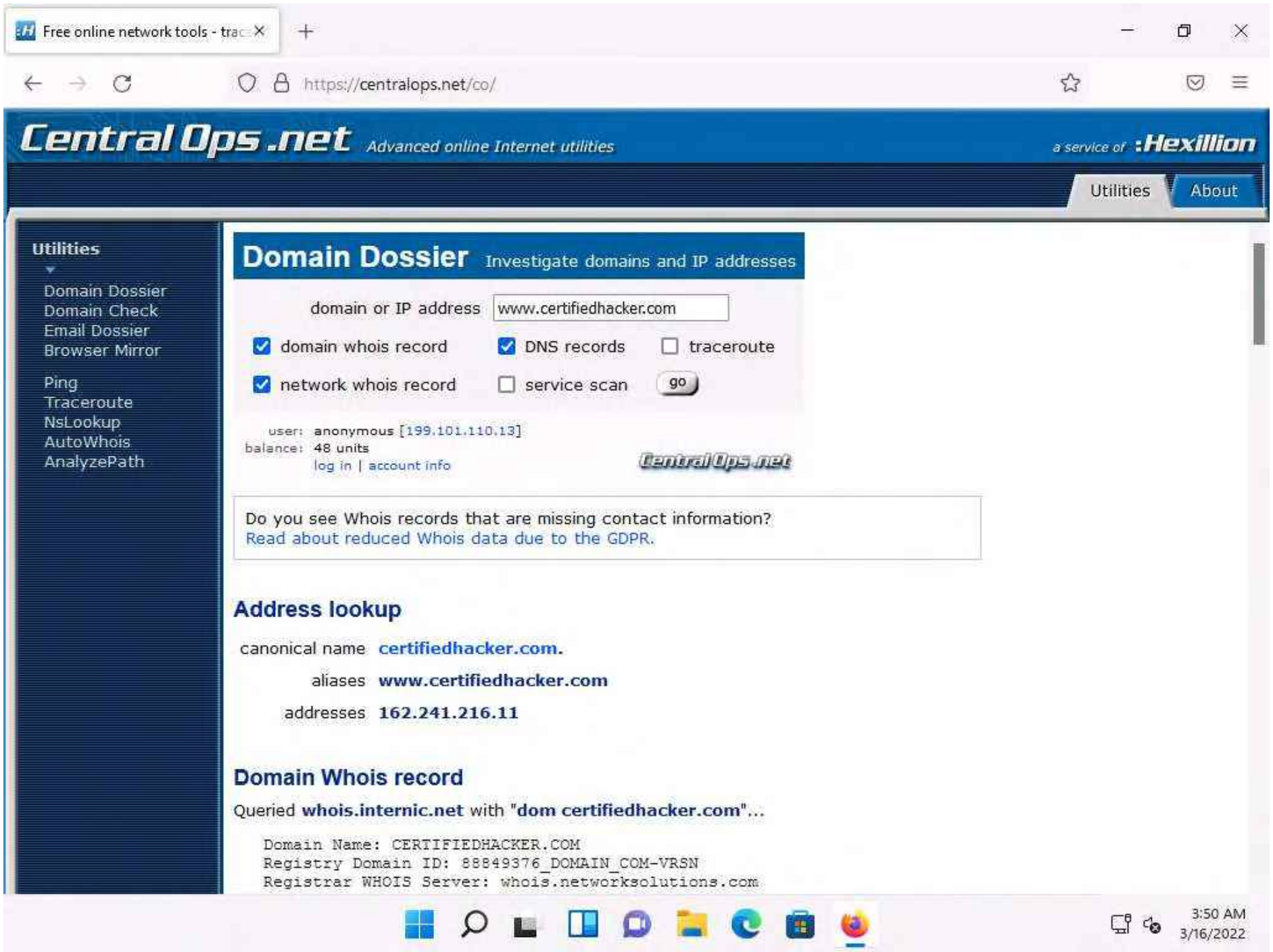
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://centralops.net** and press **Enter**. The Central Ops website appears, as shown in the screenshot.



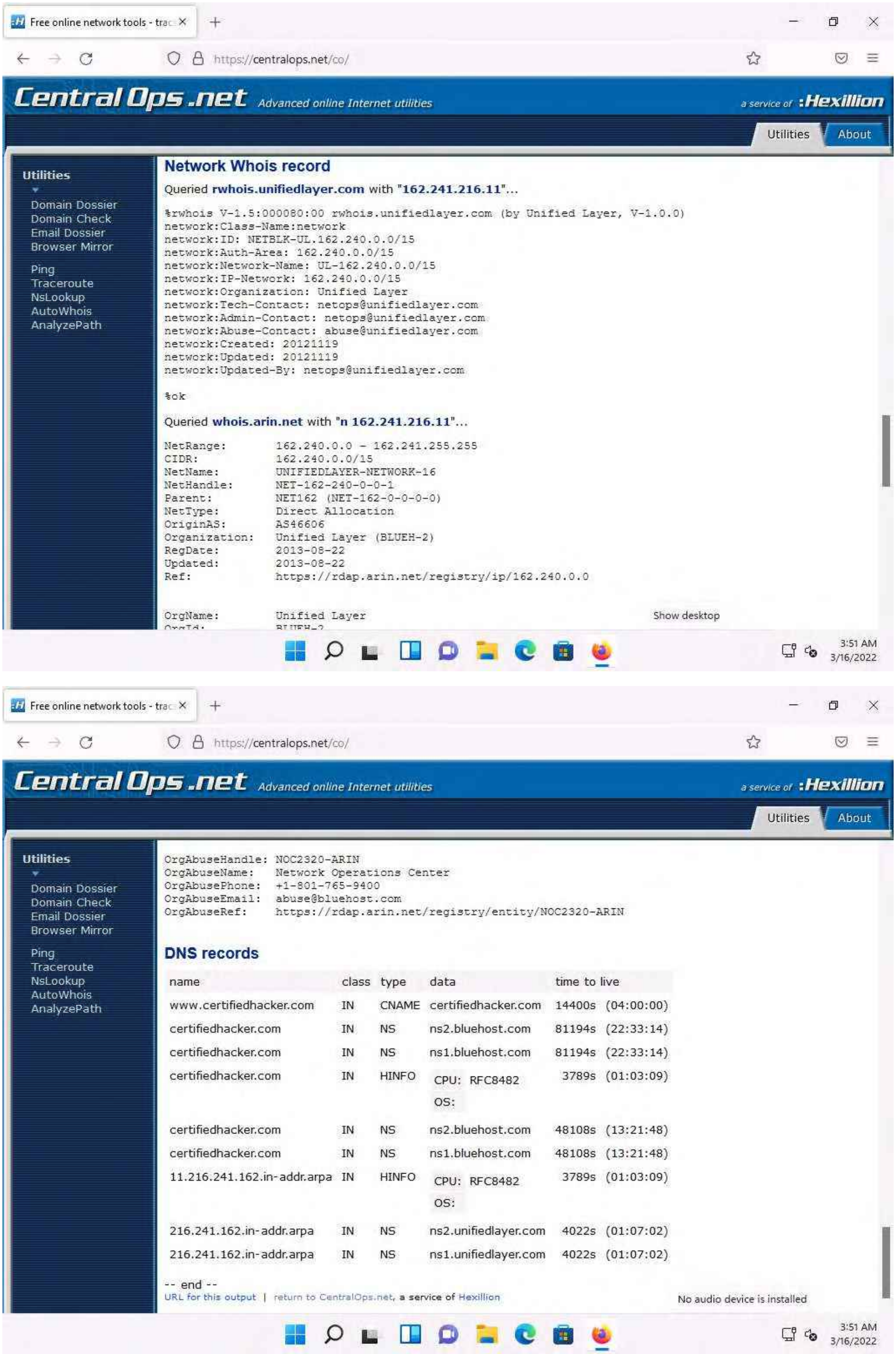
2. To extract information associated with the target organization website, type the target website's URL (here, **www.certifiedhacker.com**) in the **enter a domain or IP address** field, and then click on the **go** button, as shown in the screenshot below.



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



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.



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.

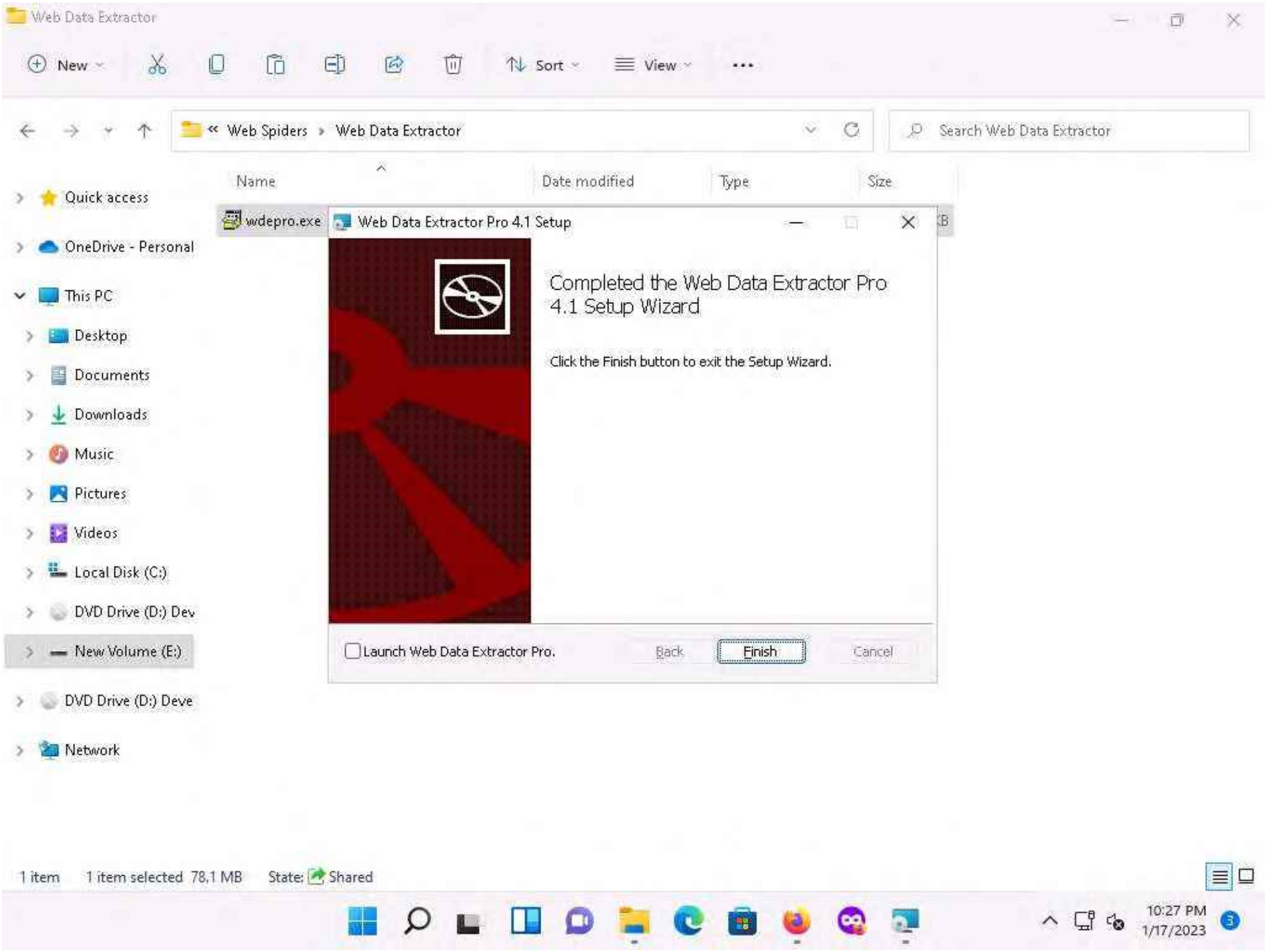
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wdepro.exe**.

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

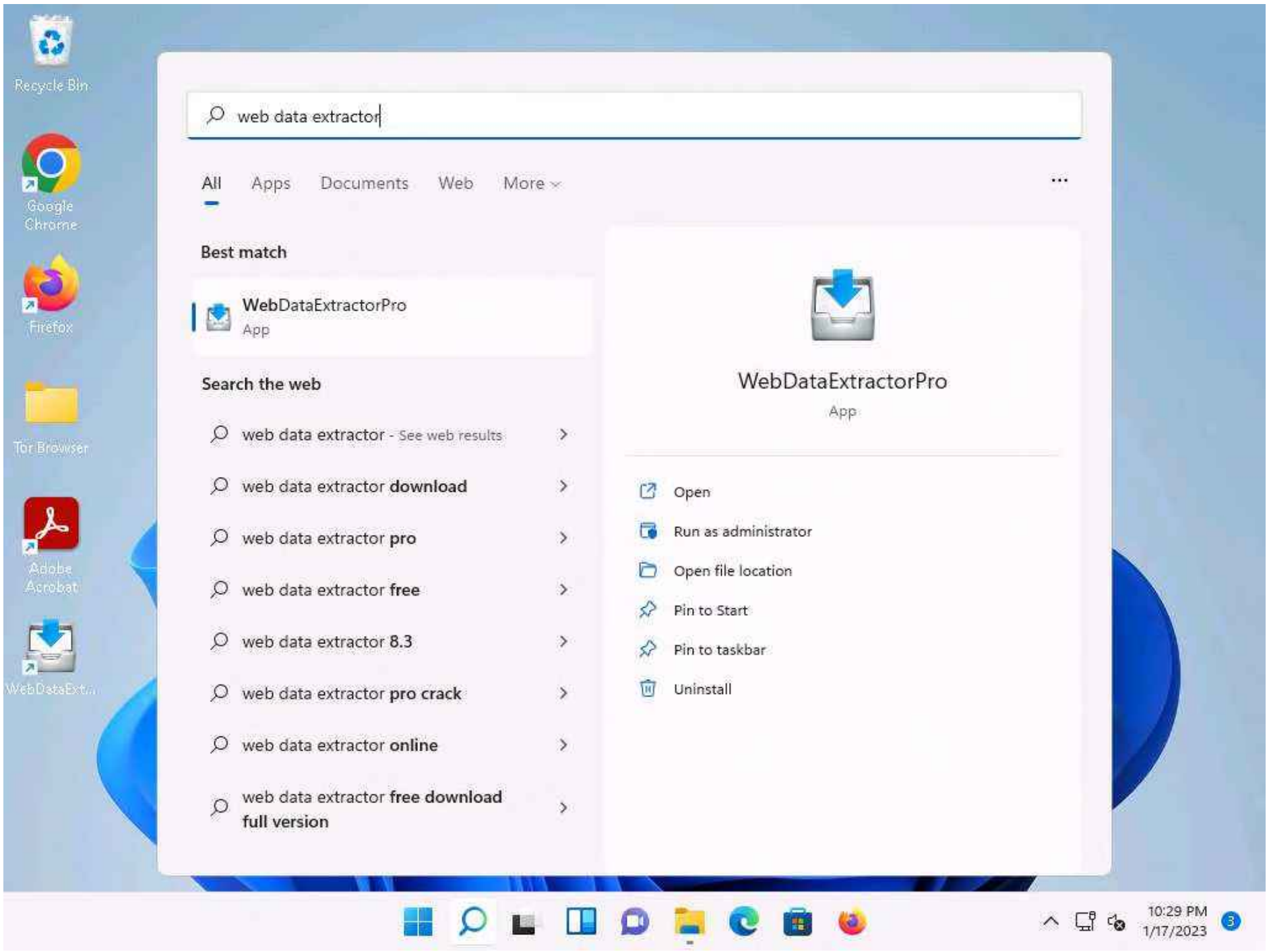
2. If the **User Account Control** pop-up appears, click **Yes**.

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

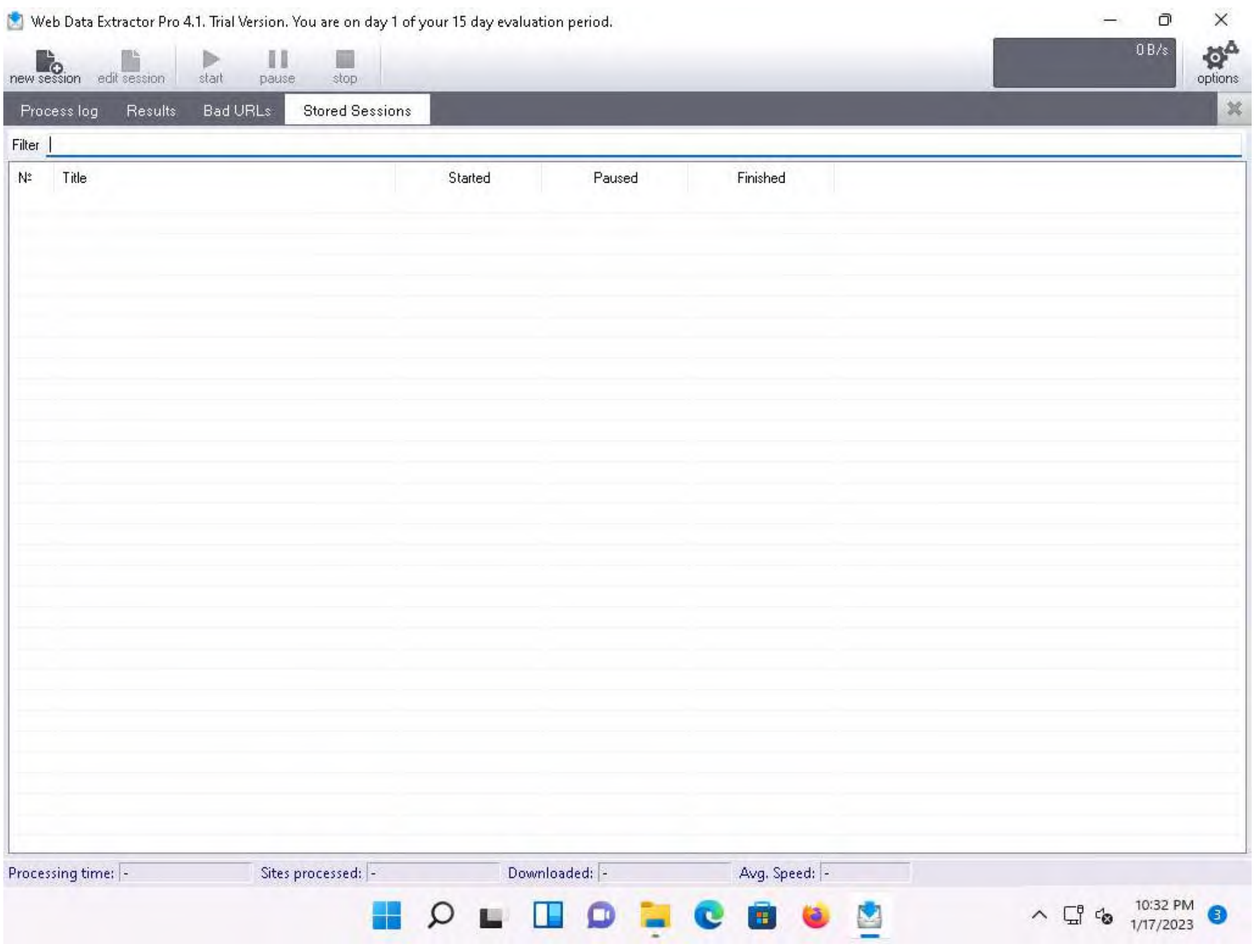
Note: Ensure that **Launch Web Data Extractor** checkbox is unchecked.



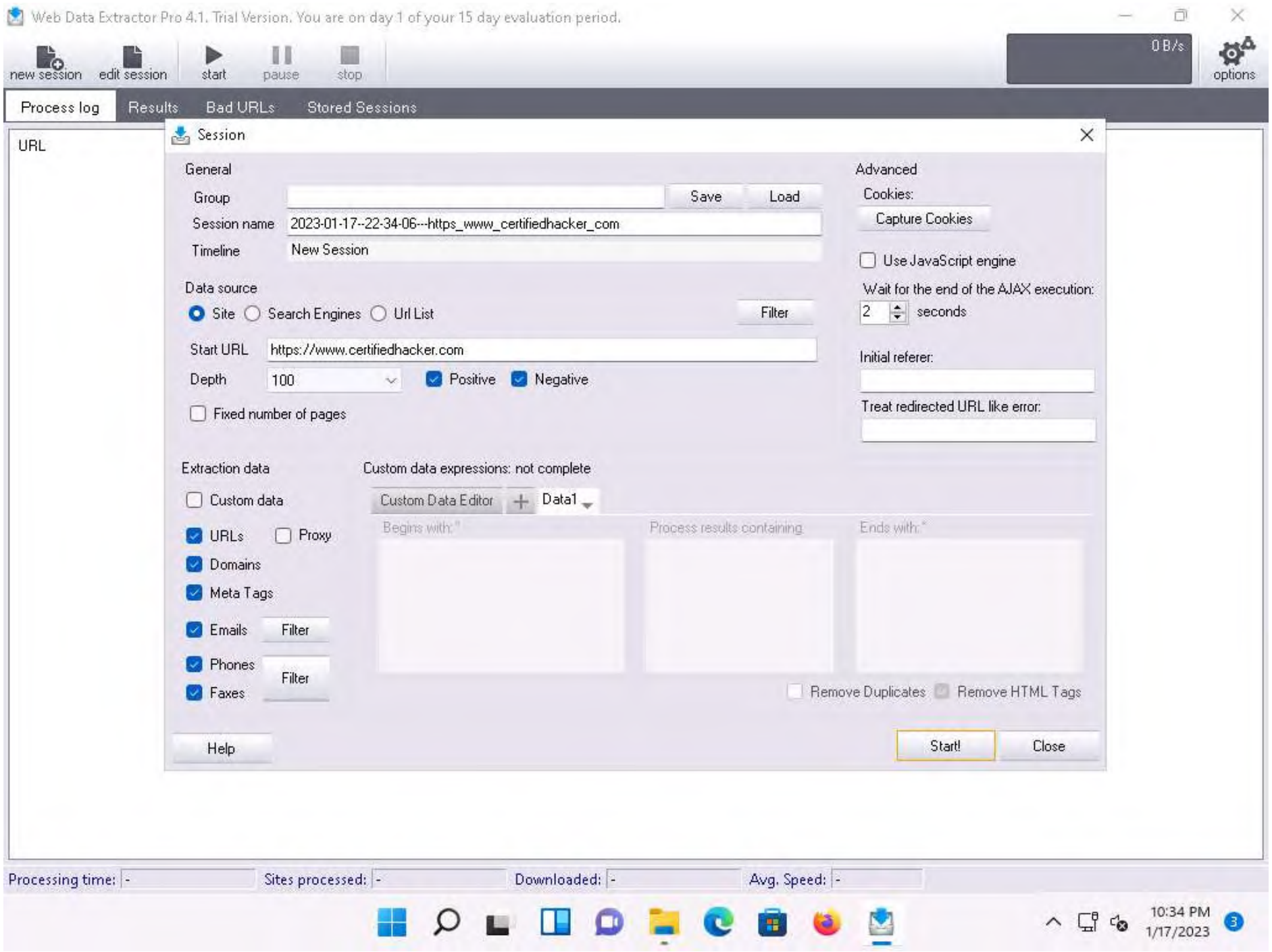
4. Click **Search** icon ( ) on the **Desktop** and type **web data extractor** in the search field. The **Web Data Extractor Pro** appears in the results, click **Open** to launch it.



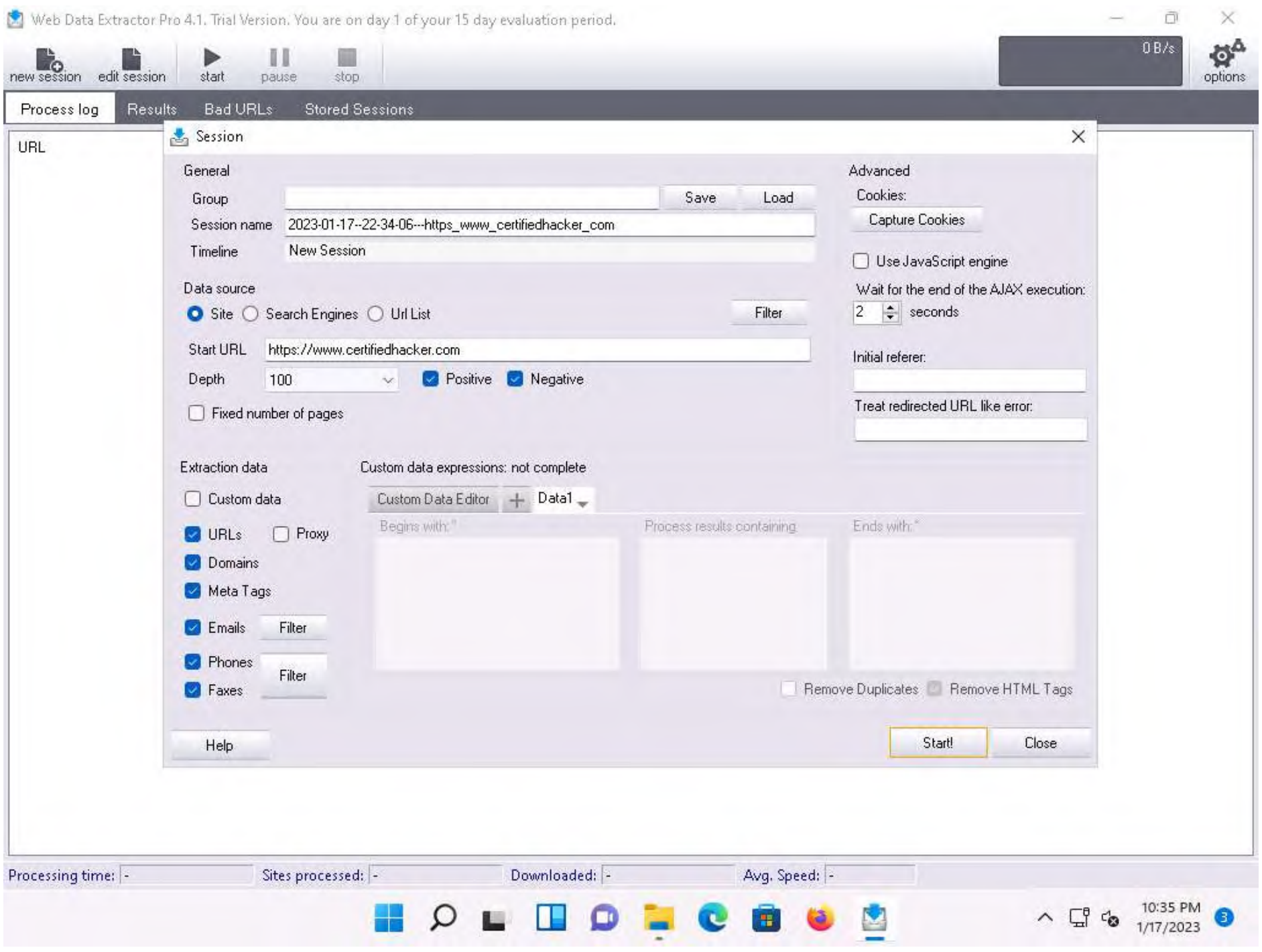
5. The **Web Data Extractor** main window appears. Click **new session** to start a new session.



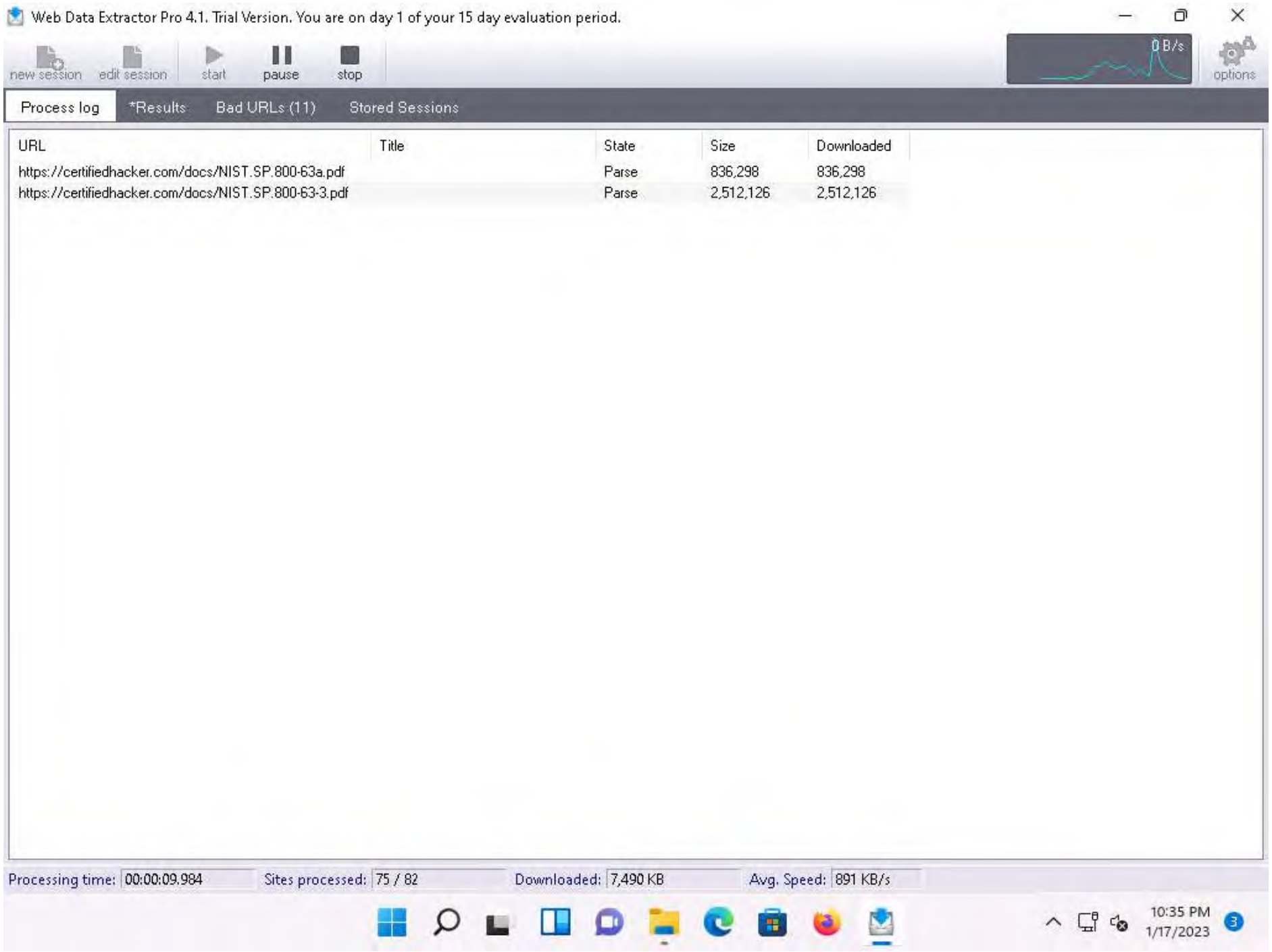
6. The **Session settings** window appears; type a URL (here, **https://www.certifiedhacker.com**) in the **Start URL** field. Check all the options, as shown in the screenshot.



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



8. **Web Data Extractor** will start collecting information (**Session**, **Meta tags**, **Emails**, **Phones**, **Faxes**, **Links** and **Domains**).

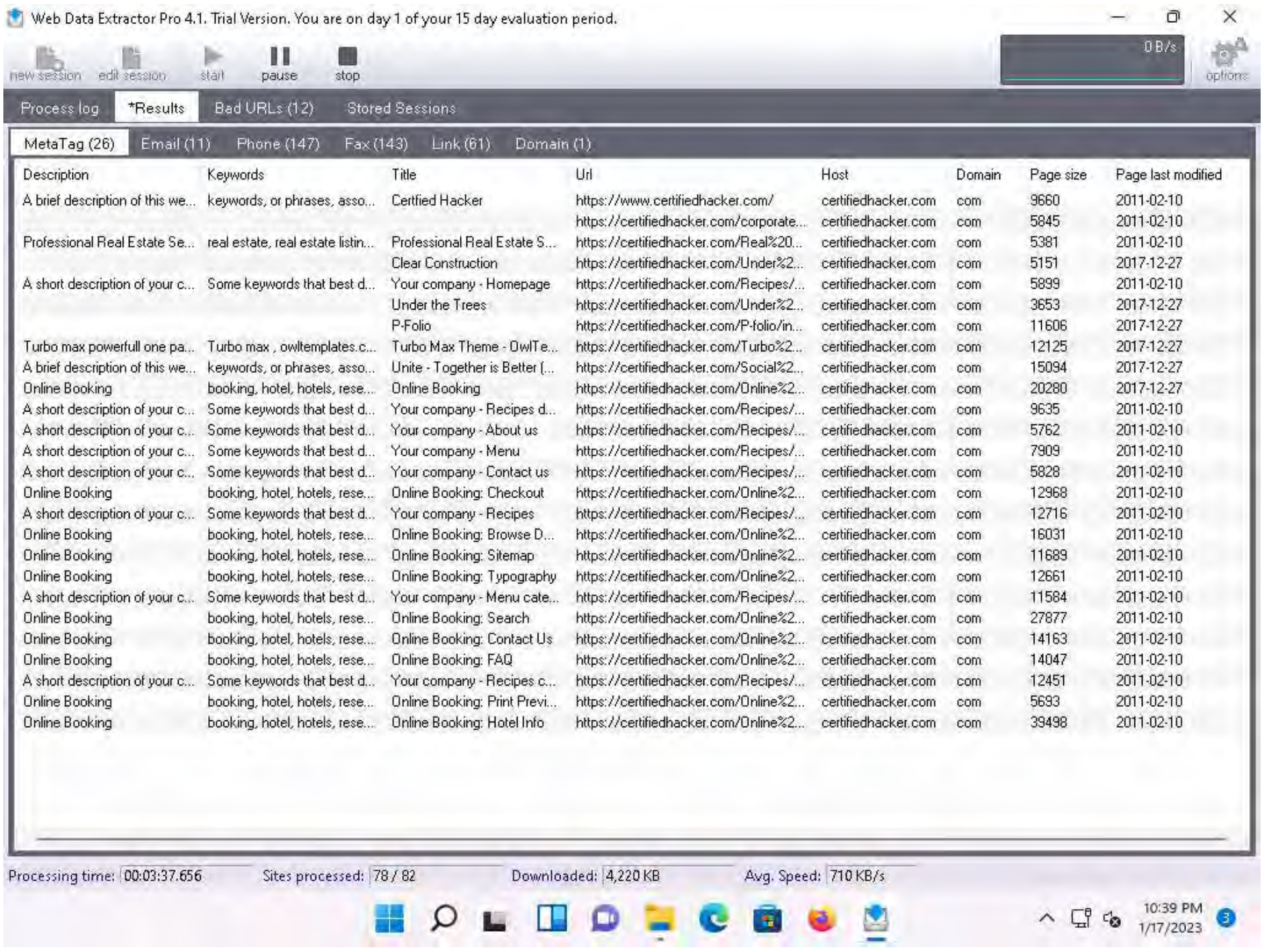


9. Click on **Results** tab to view the collected information about the website.

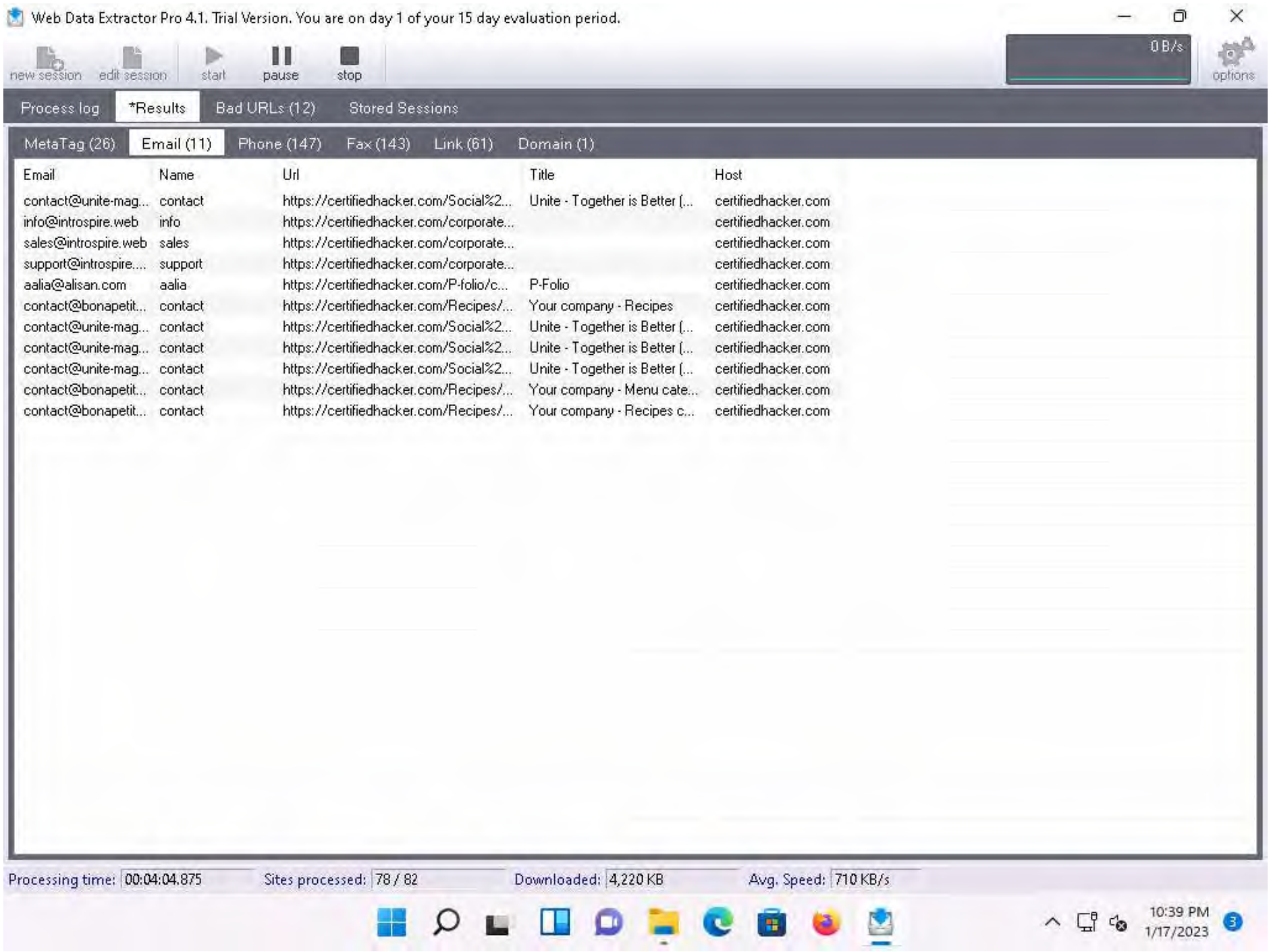
Note: The results might vary when you perform the task.

10. View the extracted information by clicking the tabs.

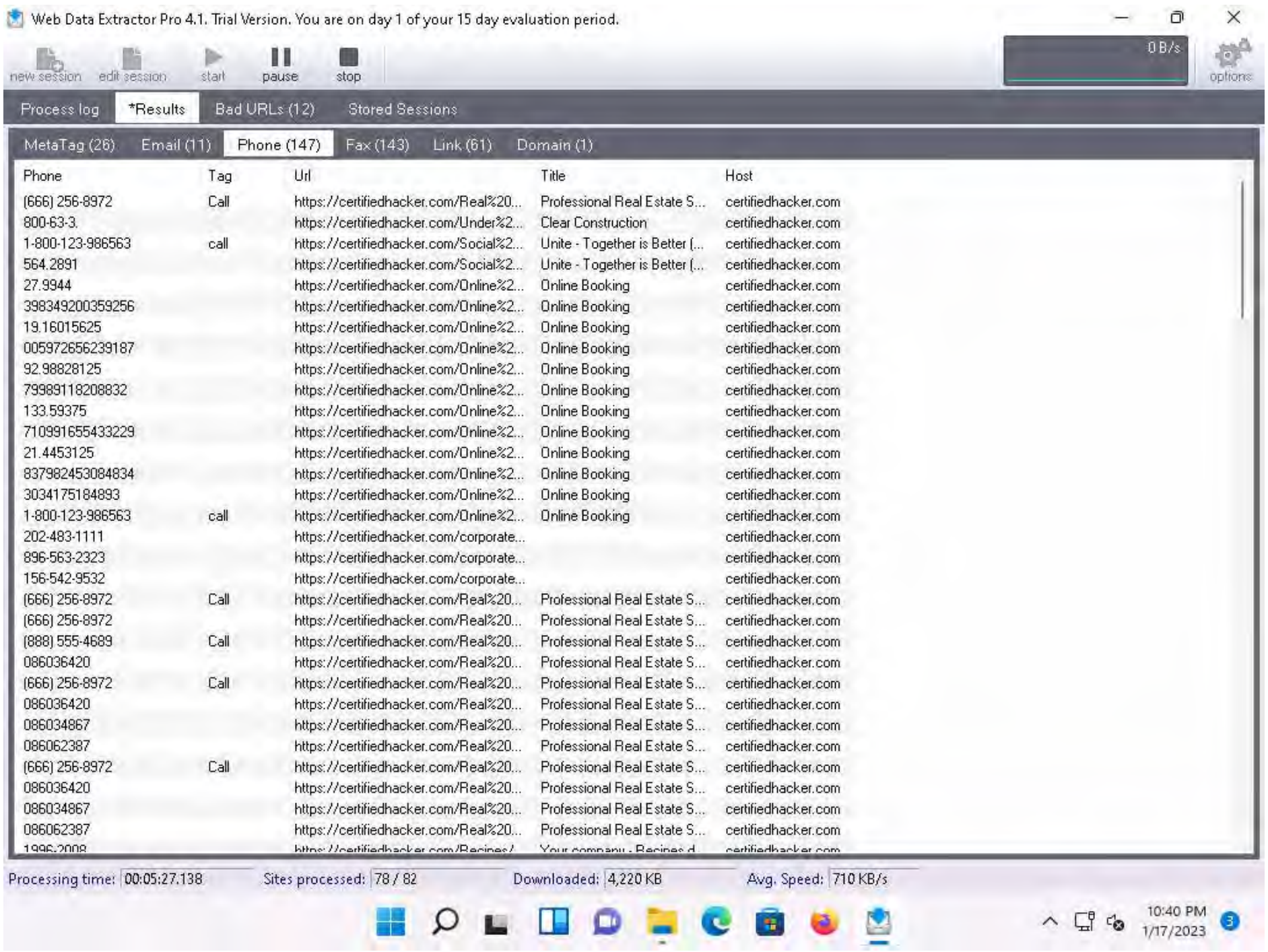
11. Select the **Meta tag** tab to view the URL, Title, Keywords, Description, Host, Domain, page size, etc.



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



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



14. Check for more information under the **Faxe**, **Link**, and **Domain** tabs.

15. This concludes the demonstration of extracting a company's data using the Web Data Extractor Pro tool.
16. 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.
17. Close all open windows and document all the acquired information.

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

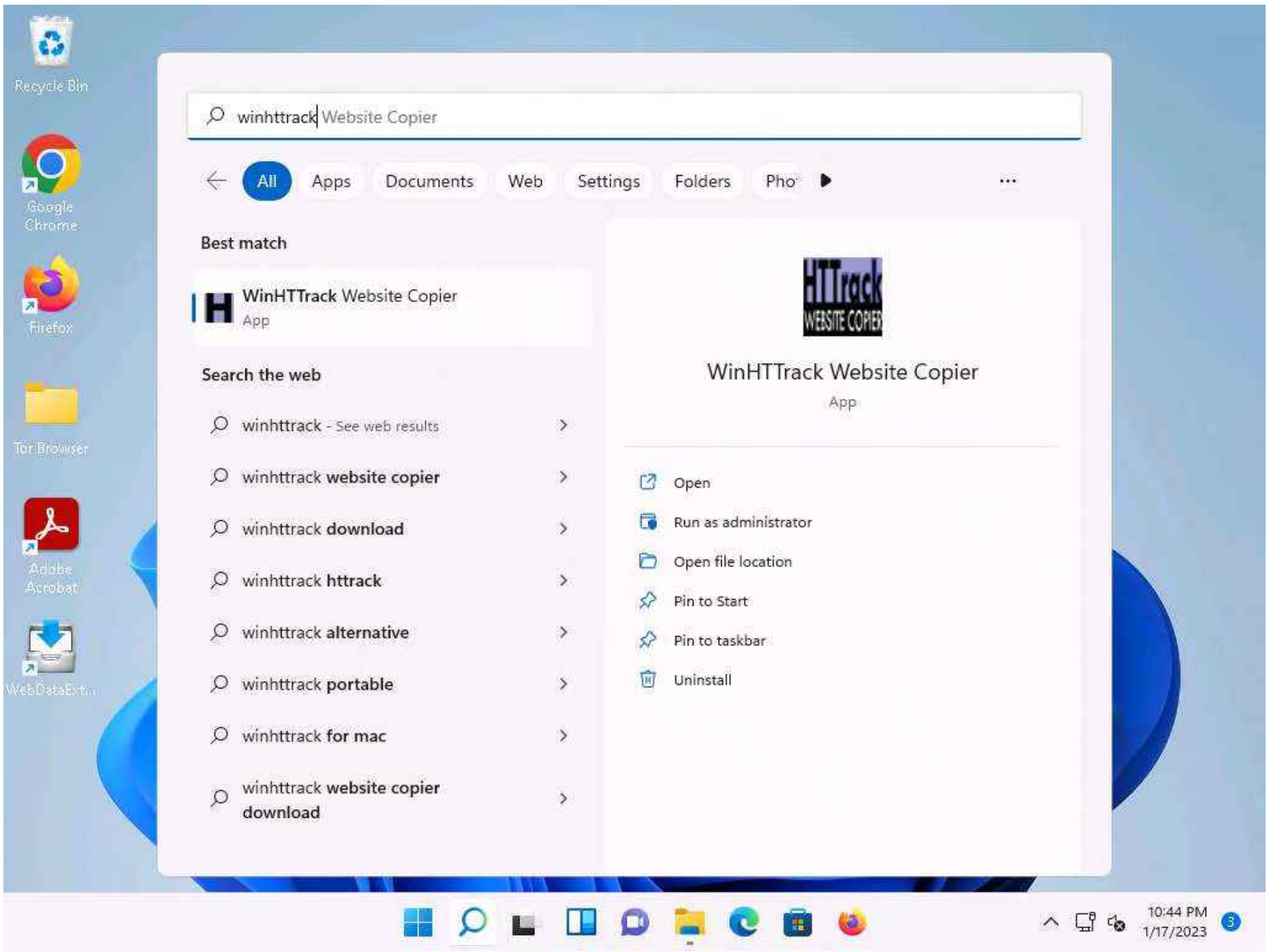
Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos,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

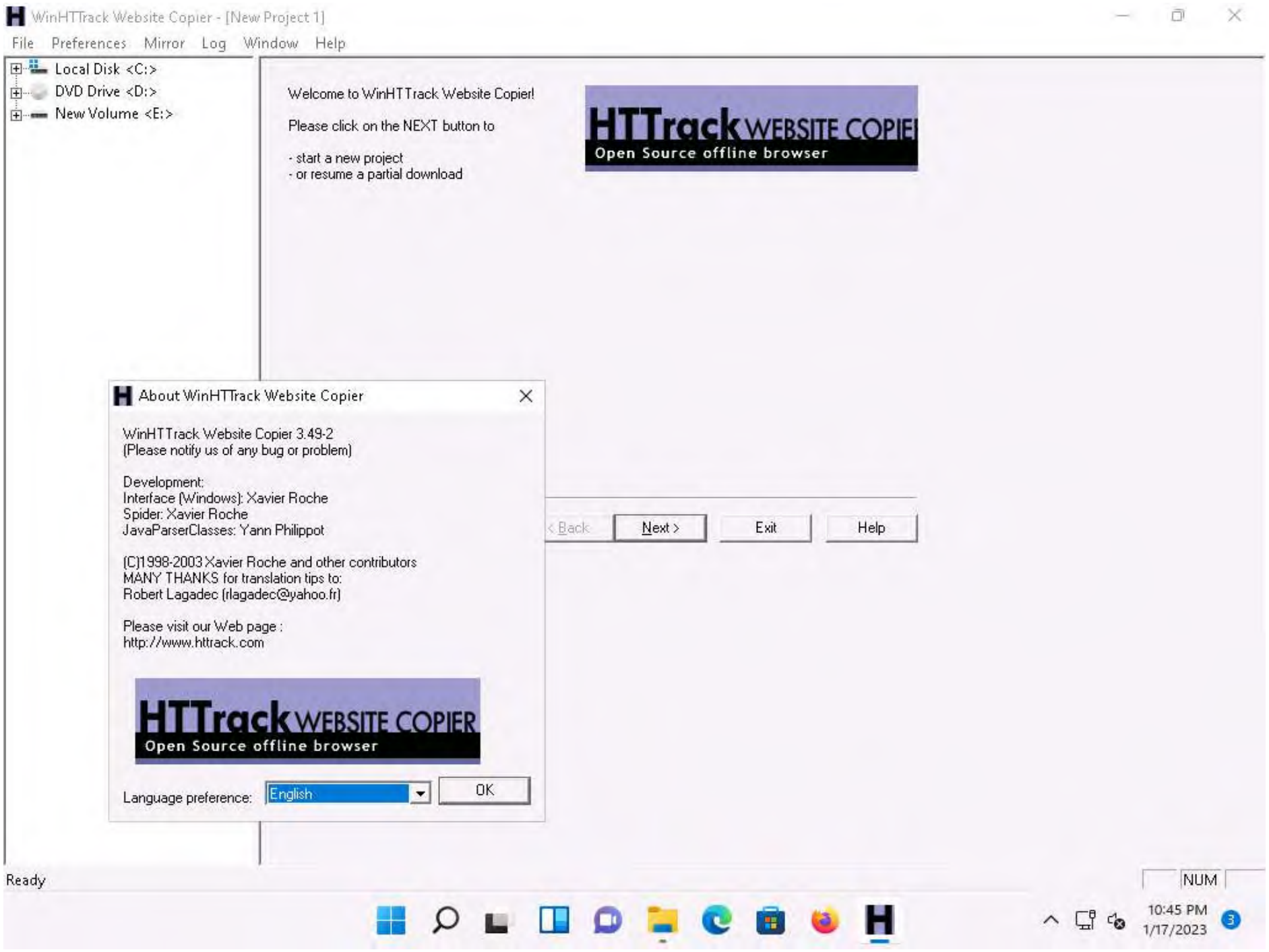
Here, we will use the HTTrack Web Site Copier tool to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

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

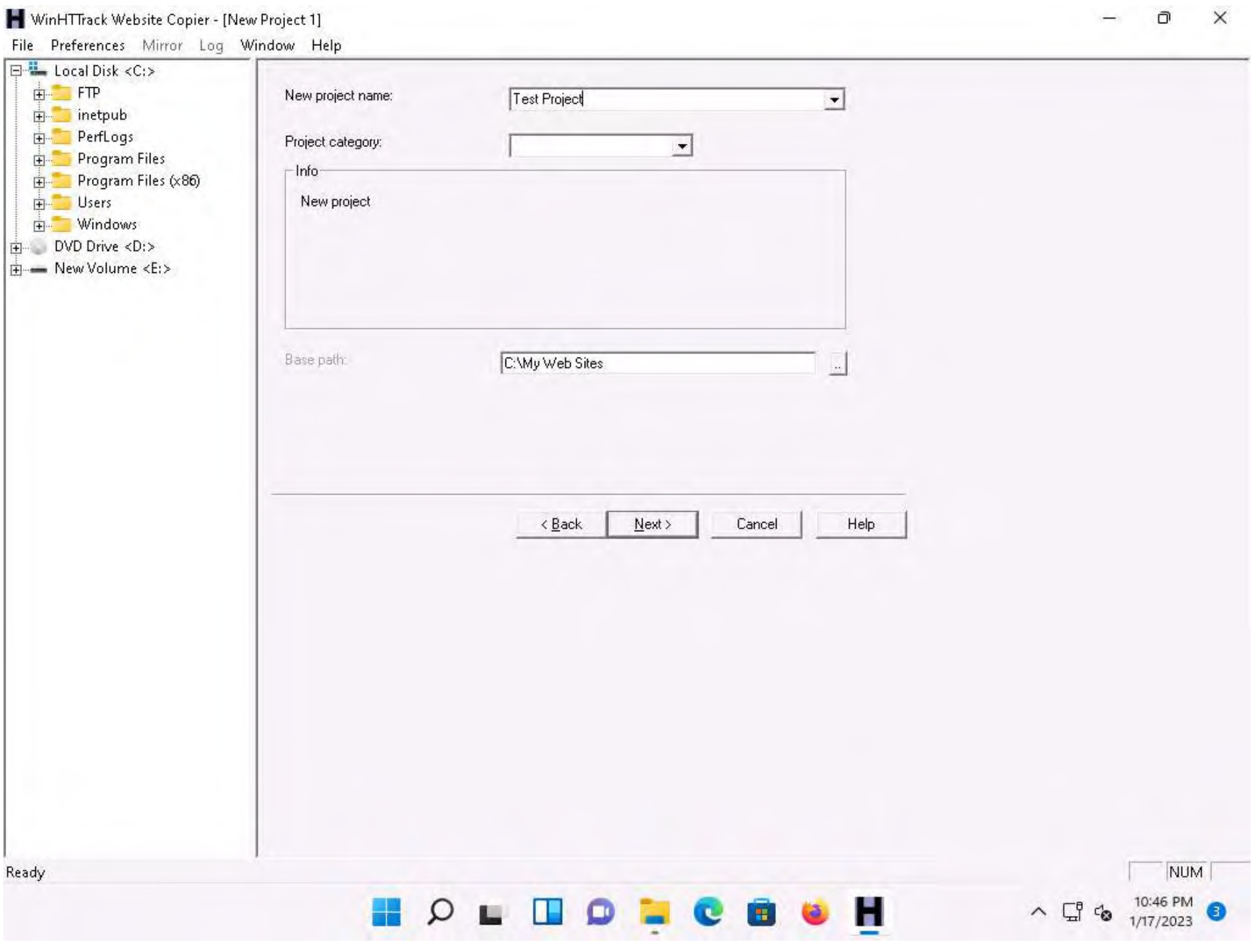
1. In the **Windows 11** machine, click **Search** icon ( ) on the **Desktop** and type **winhttrack** in the search field. The **WinHTTrack Website Copier** appears in the results, click **Open** to launch it.



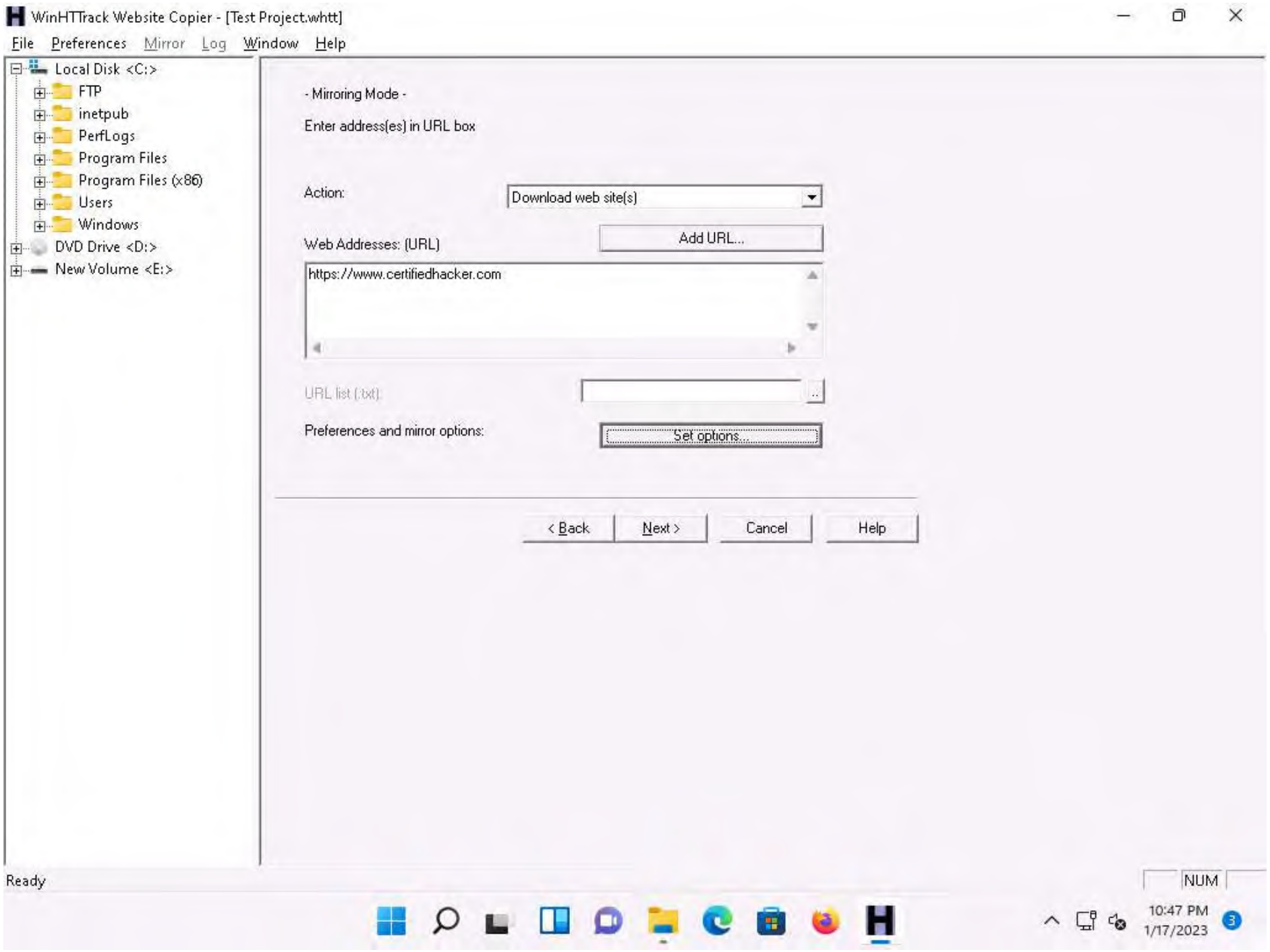
2. The **About WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.



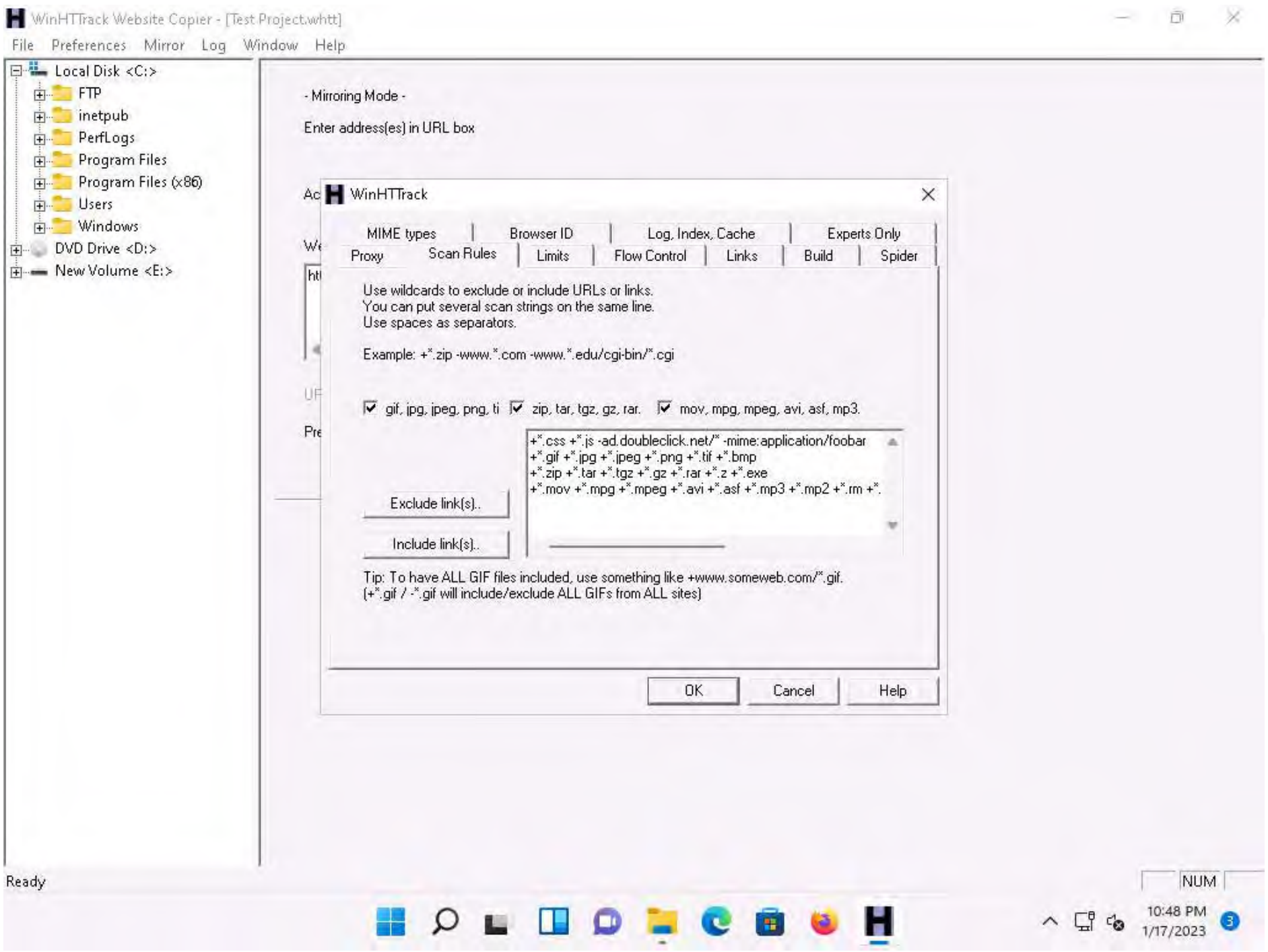
3. Enter the name of the project (here, **Test Project**) in the **New project name:** field. Select the **Base path:** to store the copied files; click **Next >**.



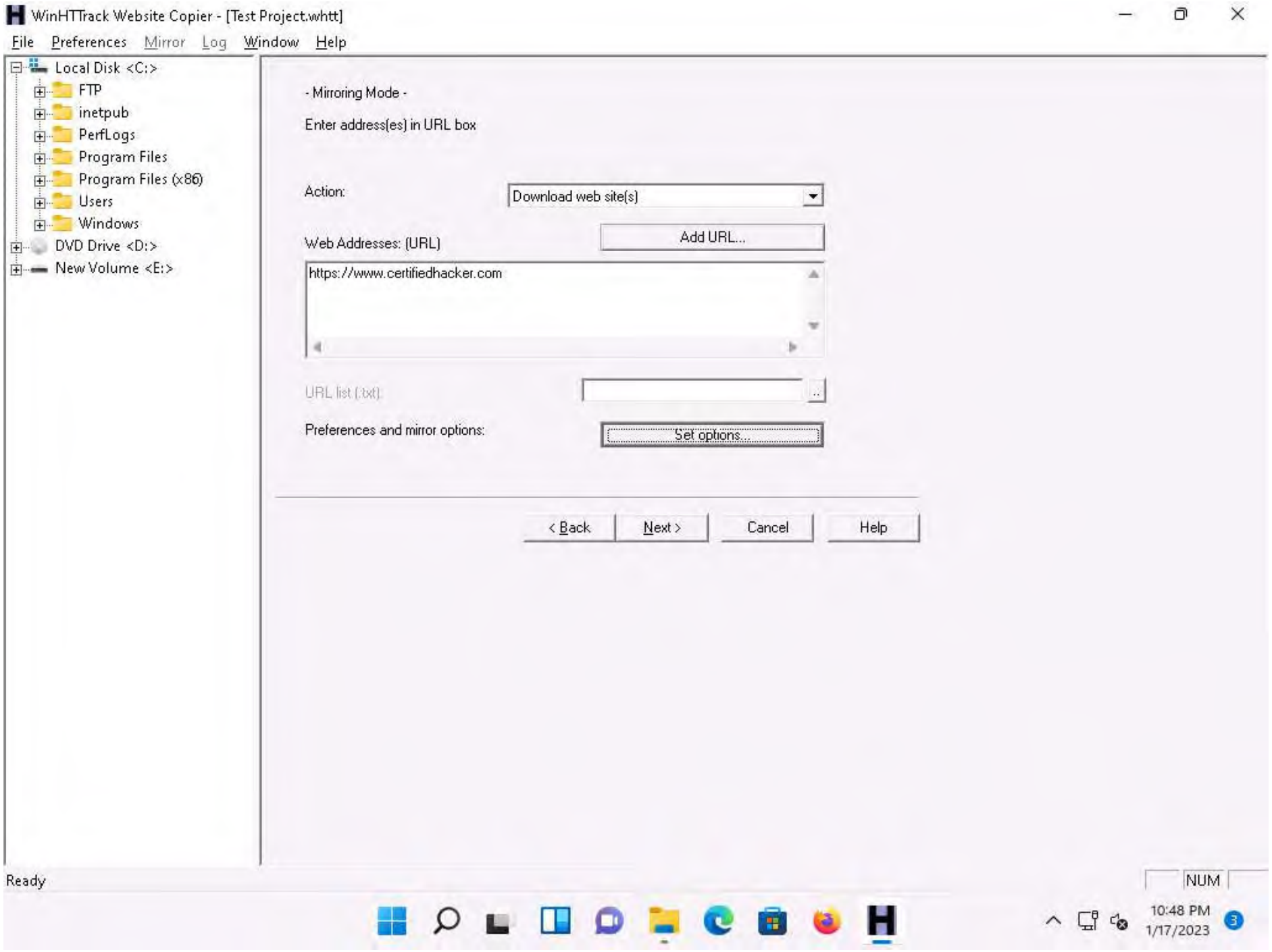
4. Enter a target URL (here, **https://www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options...**.



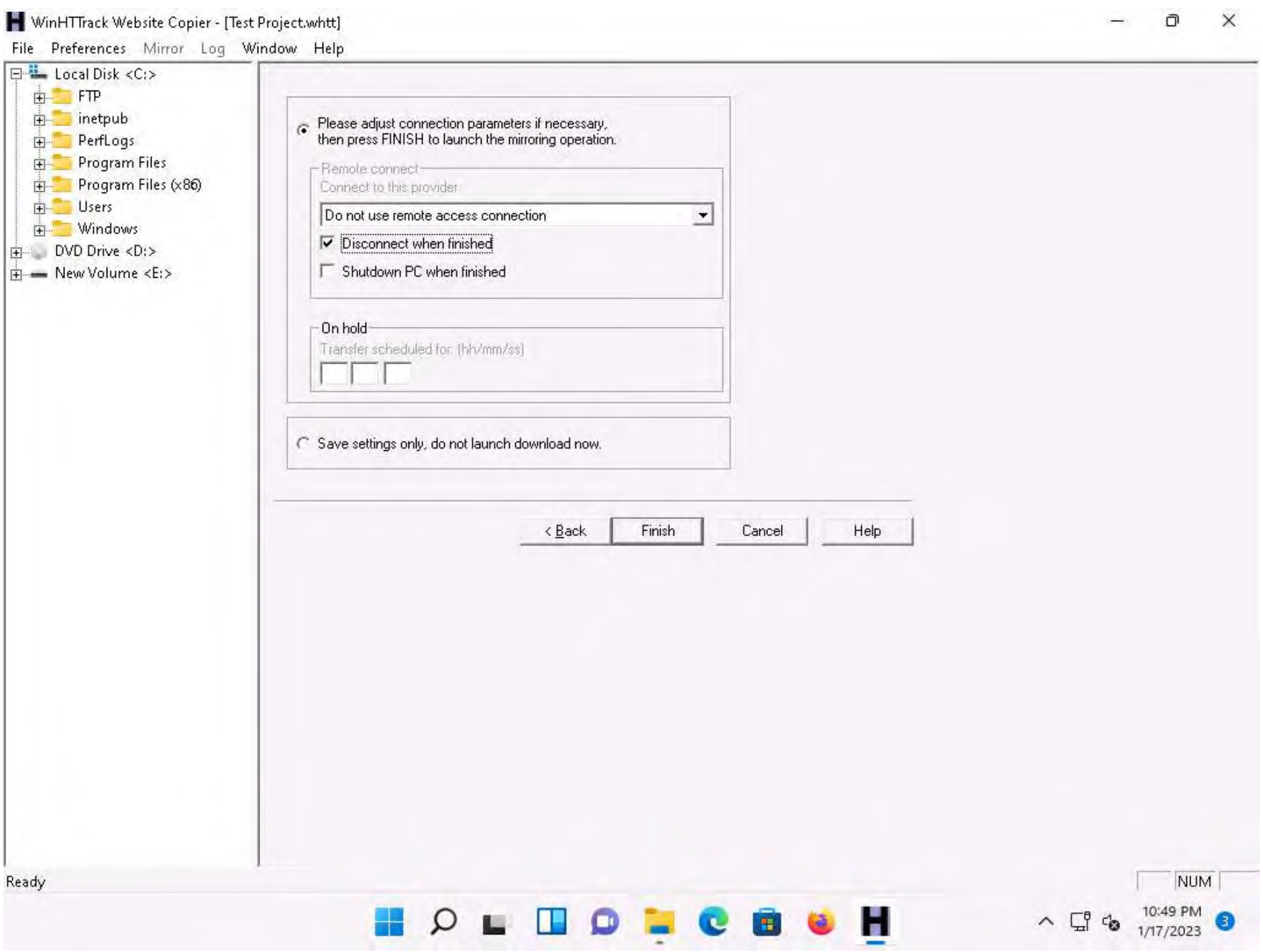
5. **WinHTTrack** window appears, click the **Scan Rules** tab and select the checkboxes for the file types as shown in the following screenshot; click **OK**.



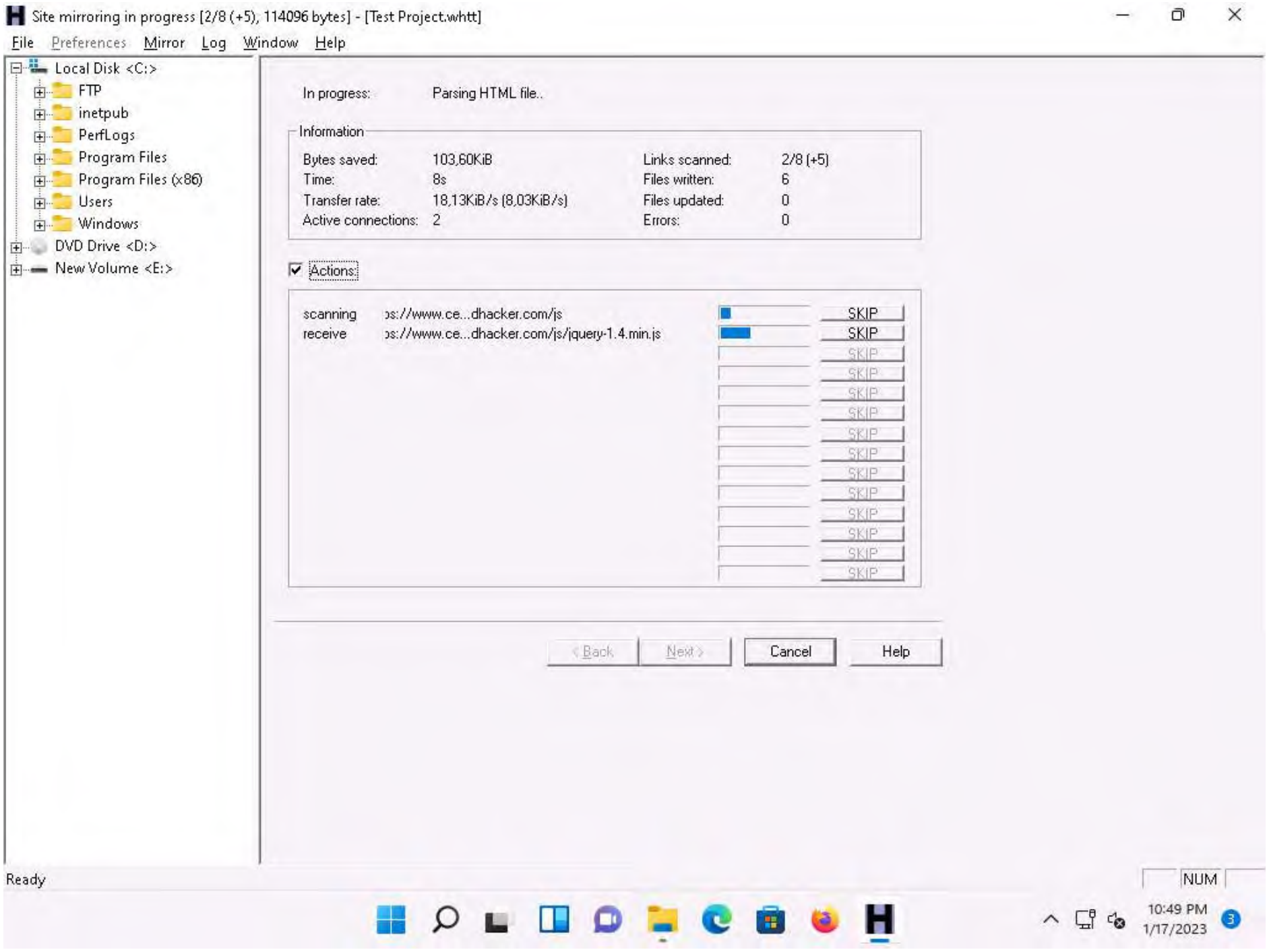
6. Click the **Next >** button.



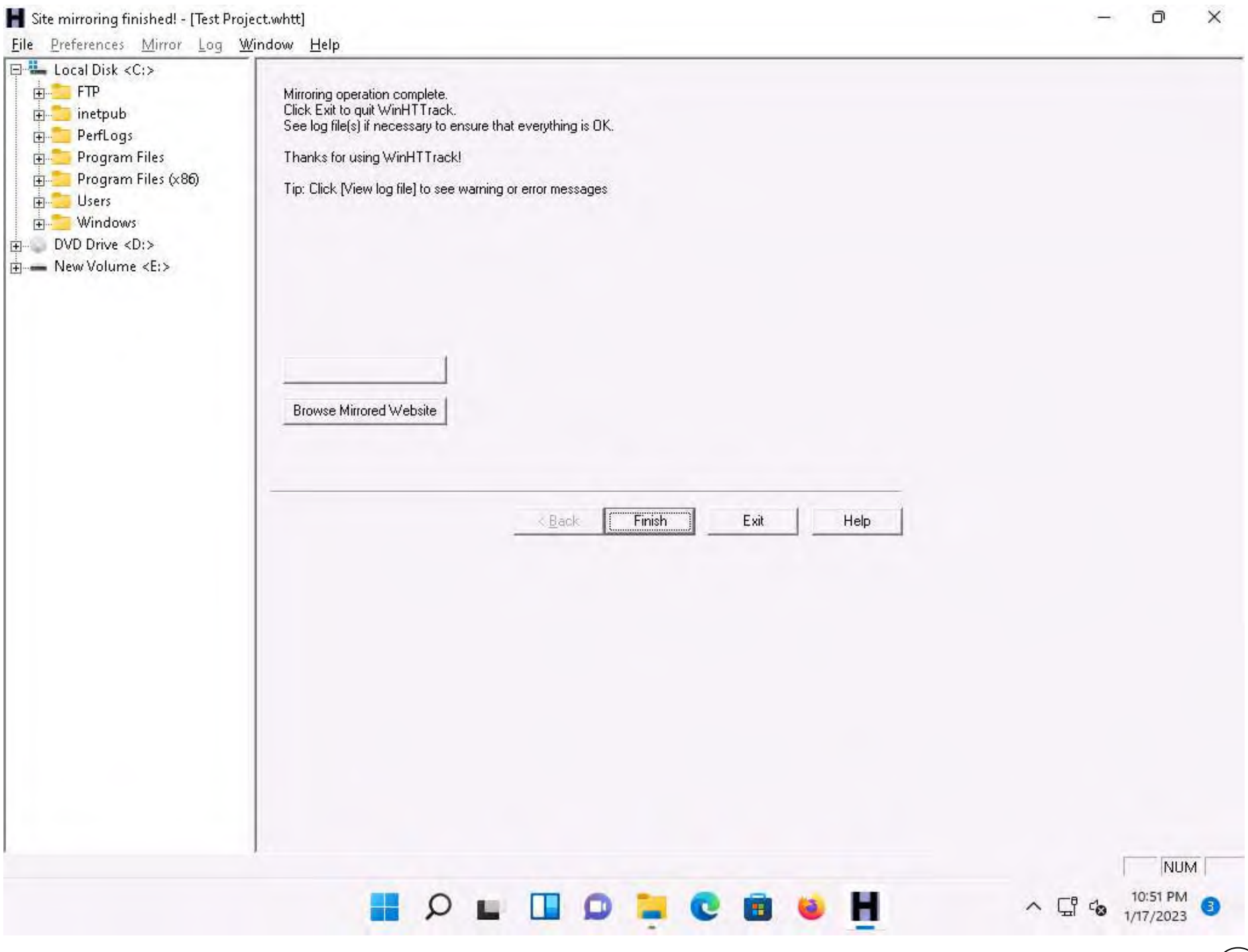
7. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation**. Check **Disconnect when finished** and click **Finish** to start mirroring the website.



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

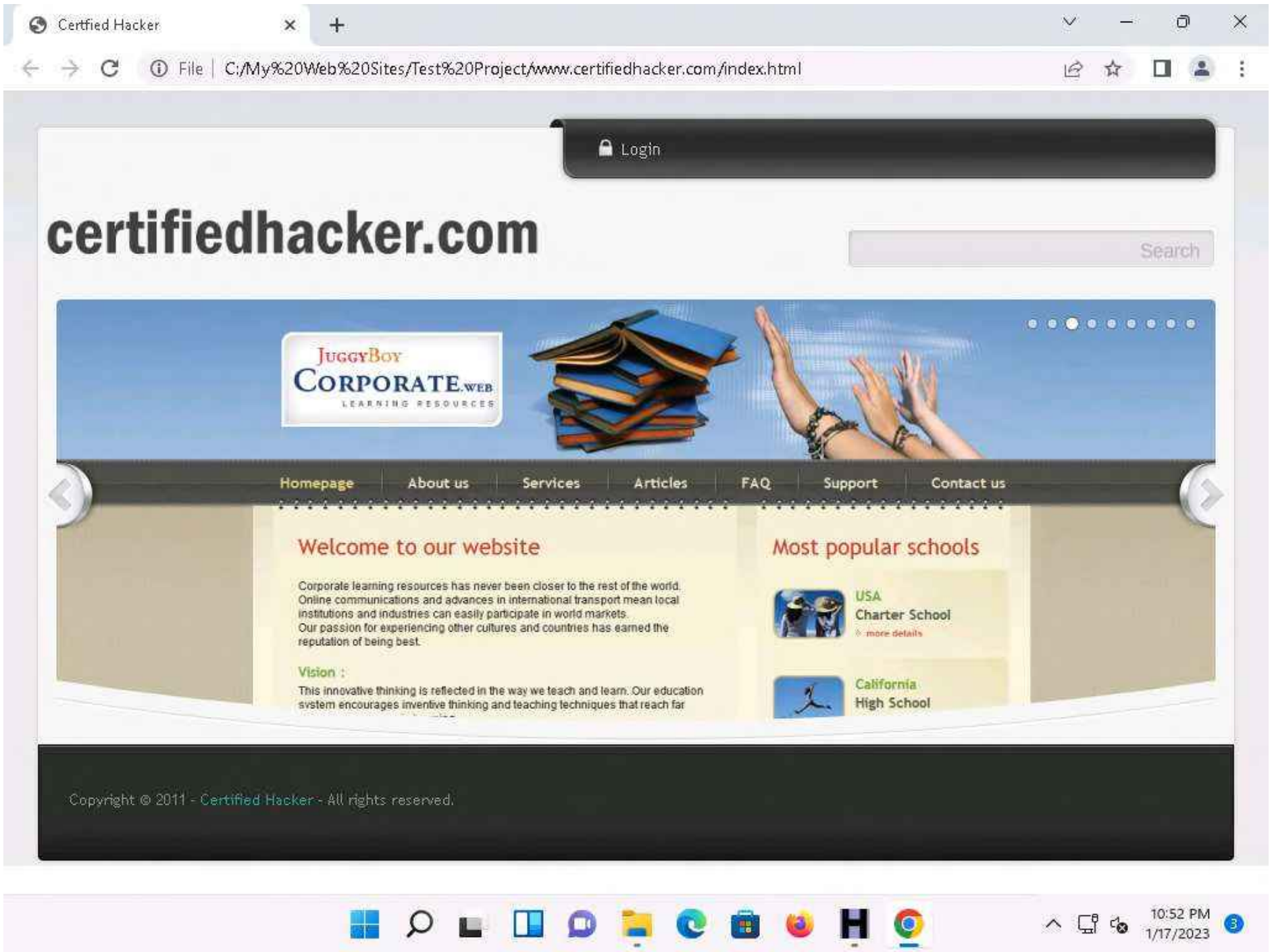


9. Once the site mirroring is completed, WinHTTrack displays the message **Mirroring operation complete**; click on **Browse Mirrored Website**.



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

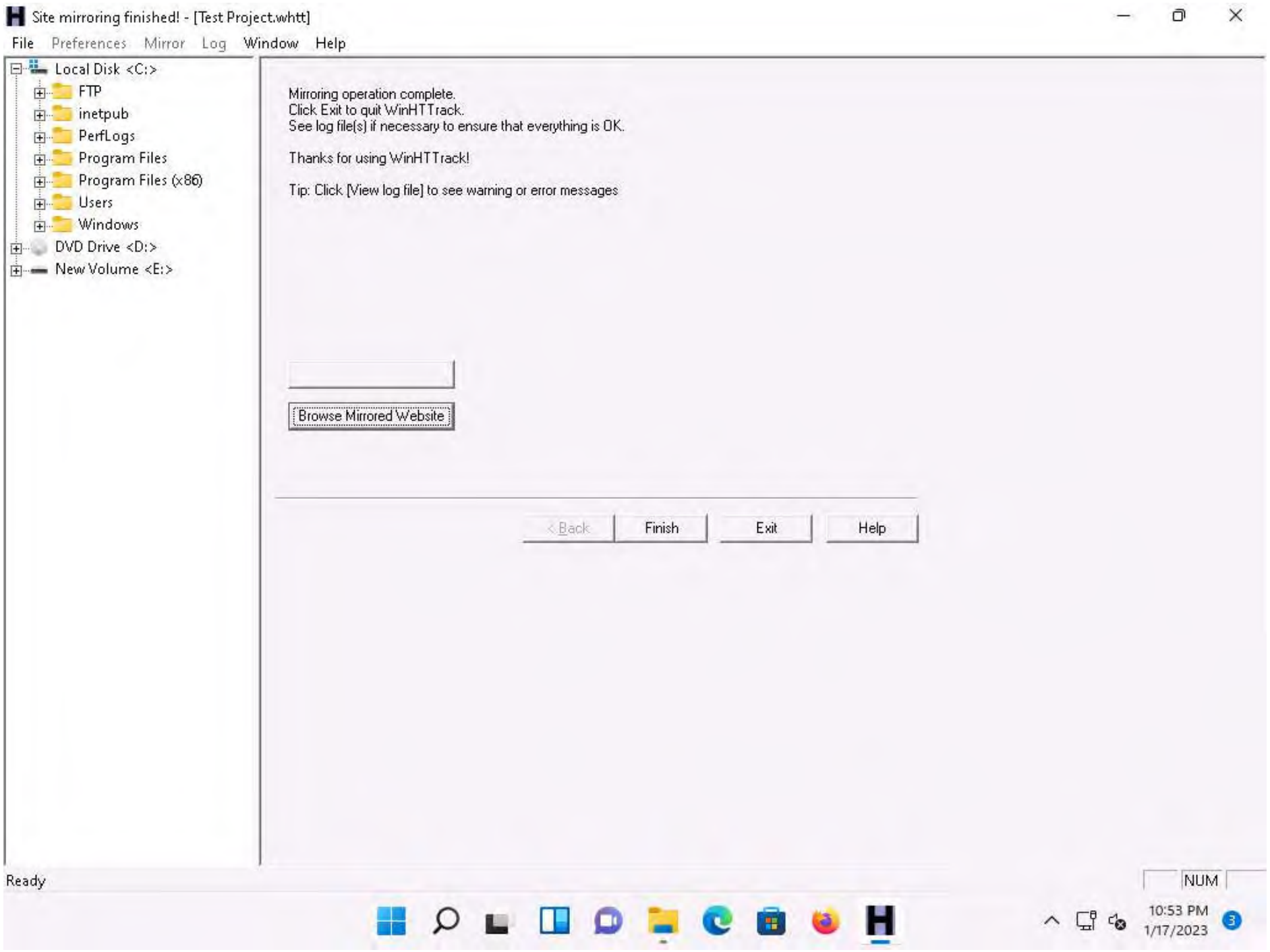
11. The mirrored website for **https://www.certifiedhacker.com** launches. The URL displayed in the address bar indicates that the website's image is stored on the local machine.

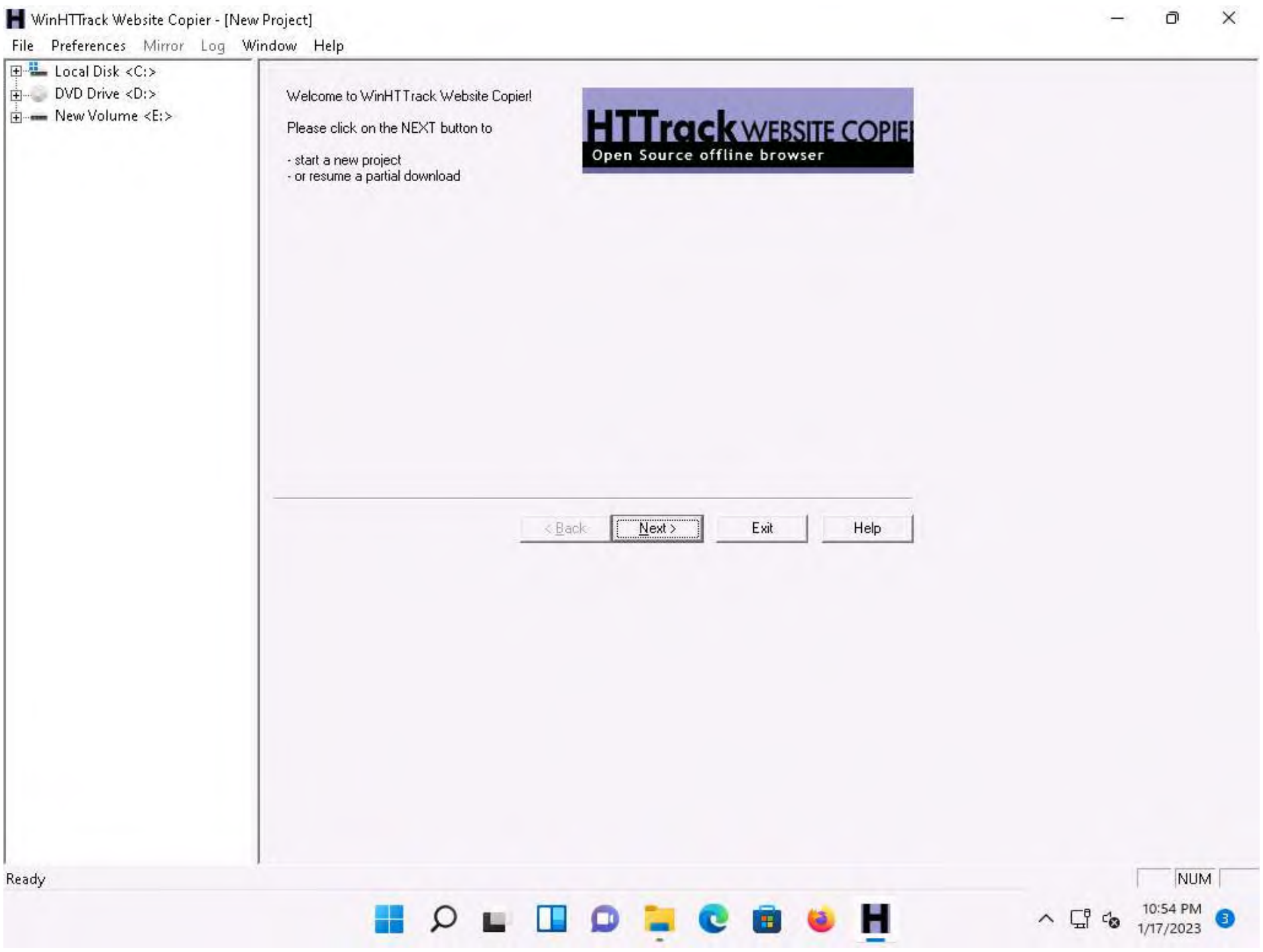


12. Analyze all directories, HTML, images, flash, videos, and other files available on the mirrored target website. You can also check for possible exploits and vulnerabilities. The site will work like a live hosted website.

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

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





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

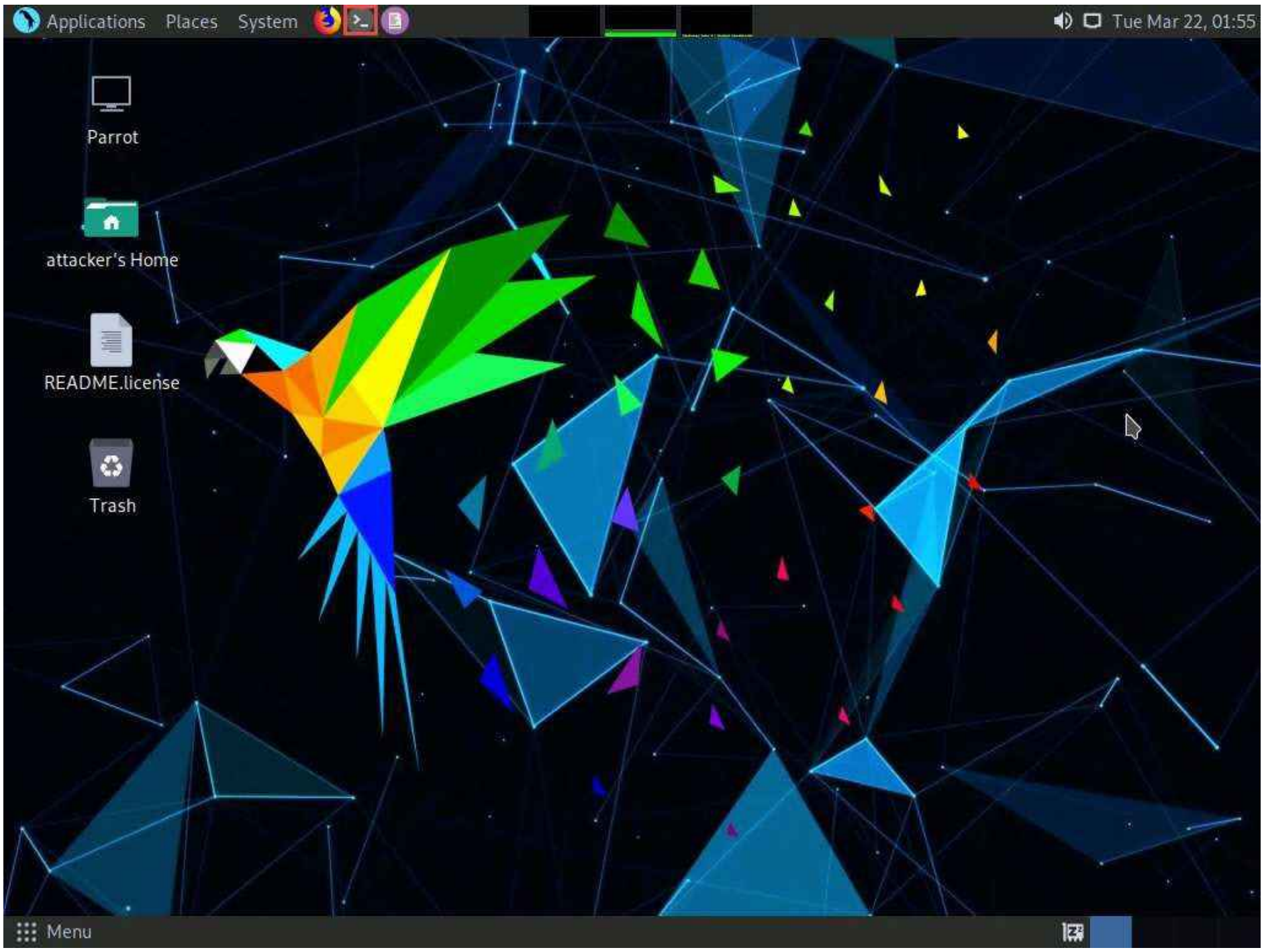
15. The attackers can further use the vulnerabilities identified through **HTTrack Website Copier** to launch various web application attacks on target organization's website.

16. This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.
17. You can also use other mirroring tools such as **Cyotek WebCopy** (https://www.cyotek.com), etc. to mirror a target website.
18. Close all open windows and document all the acquired information.

Task 6: Gather Information About a Target Website using GRecon

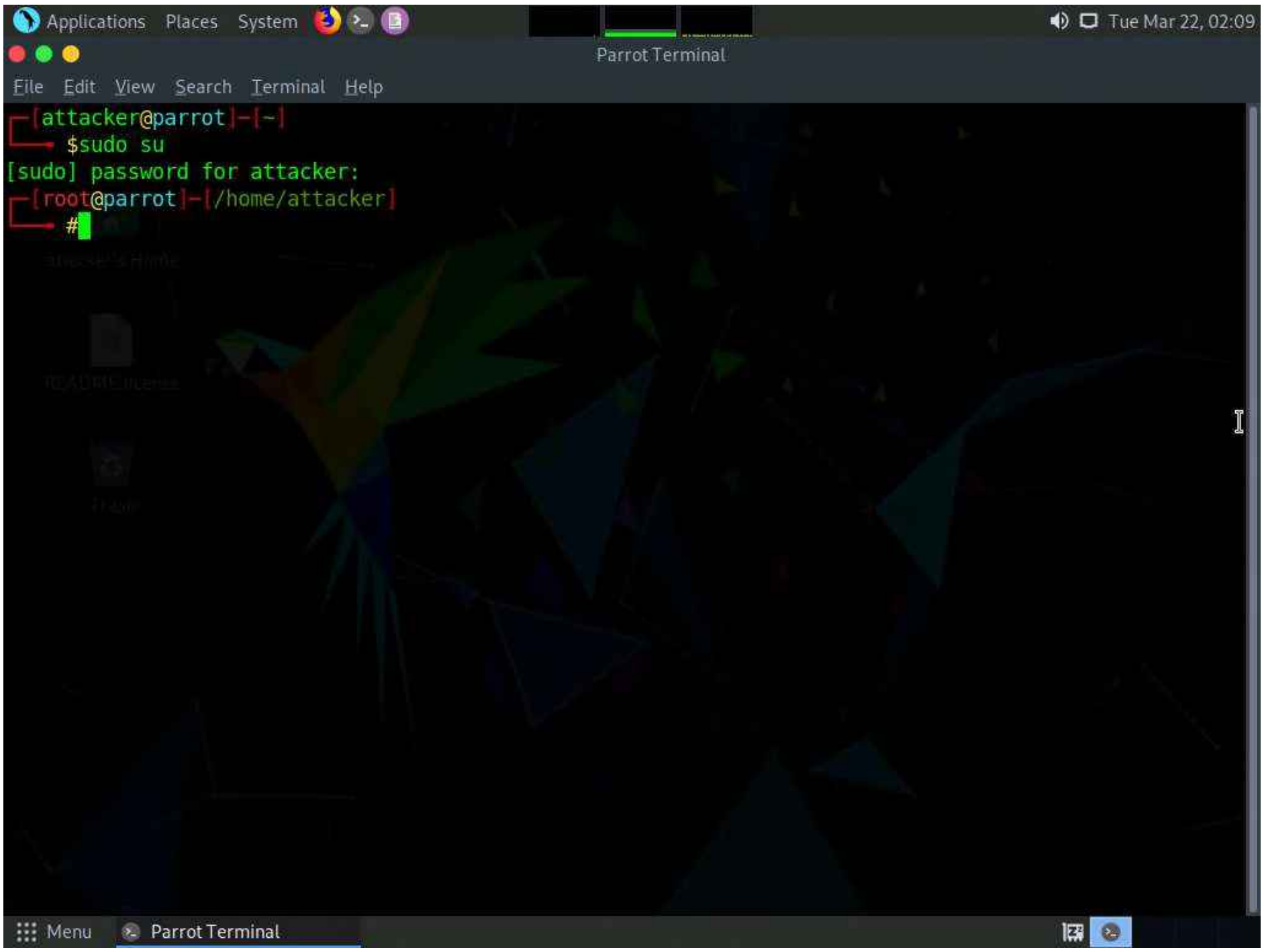
GRecon is a Python tool that can be used to run Google search queries to perform reconnaissance on a target to find subdomains, sub-subdomains, login pages, directory listings, exposed documents, and WordPress entries.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.

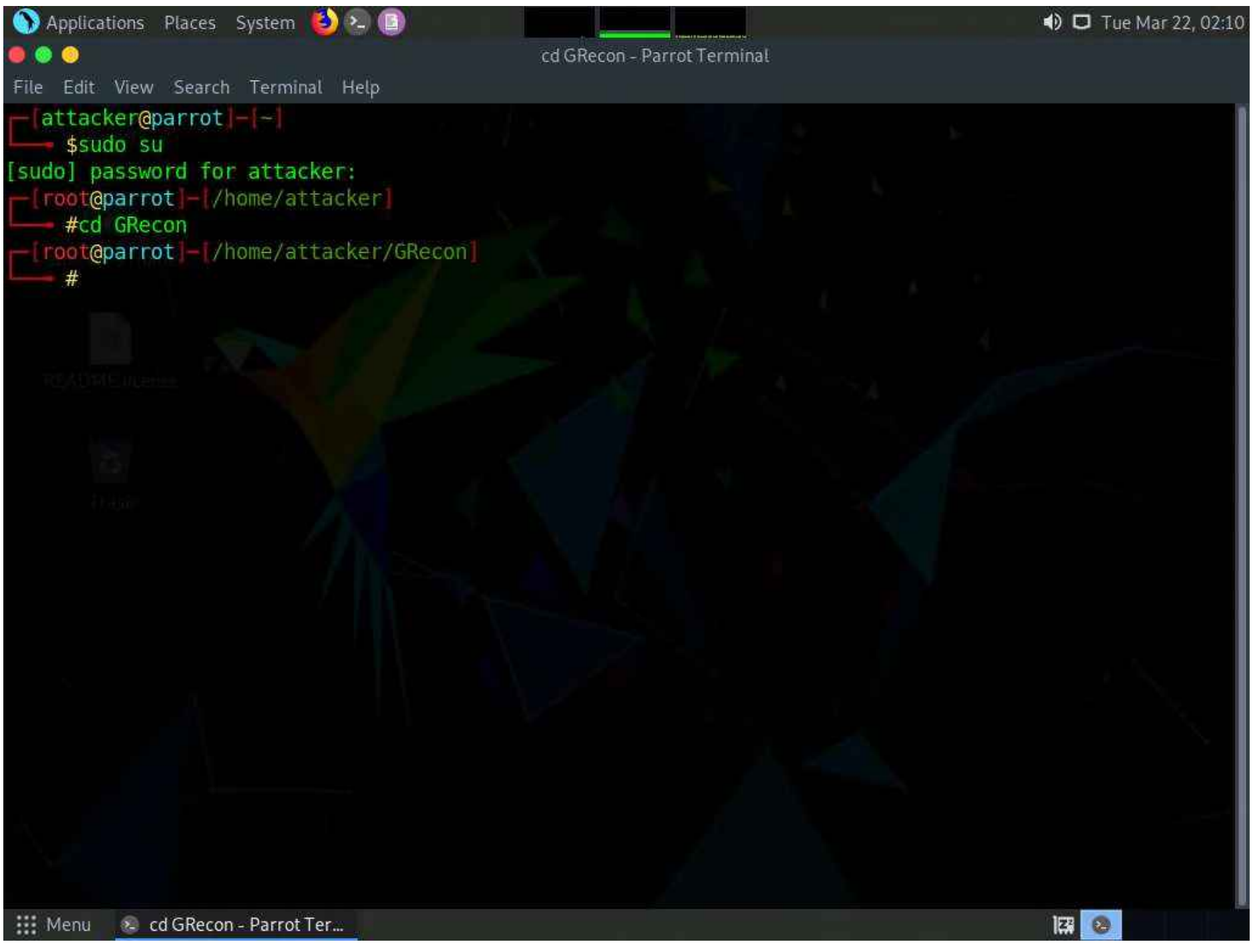


3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

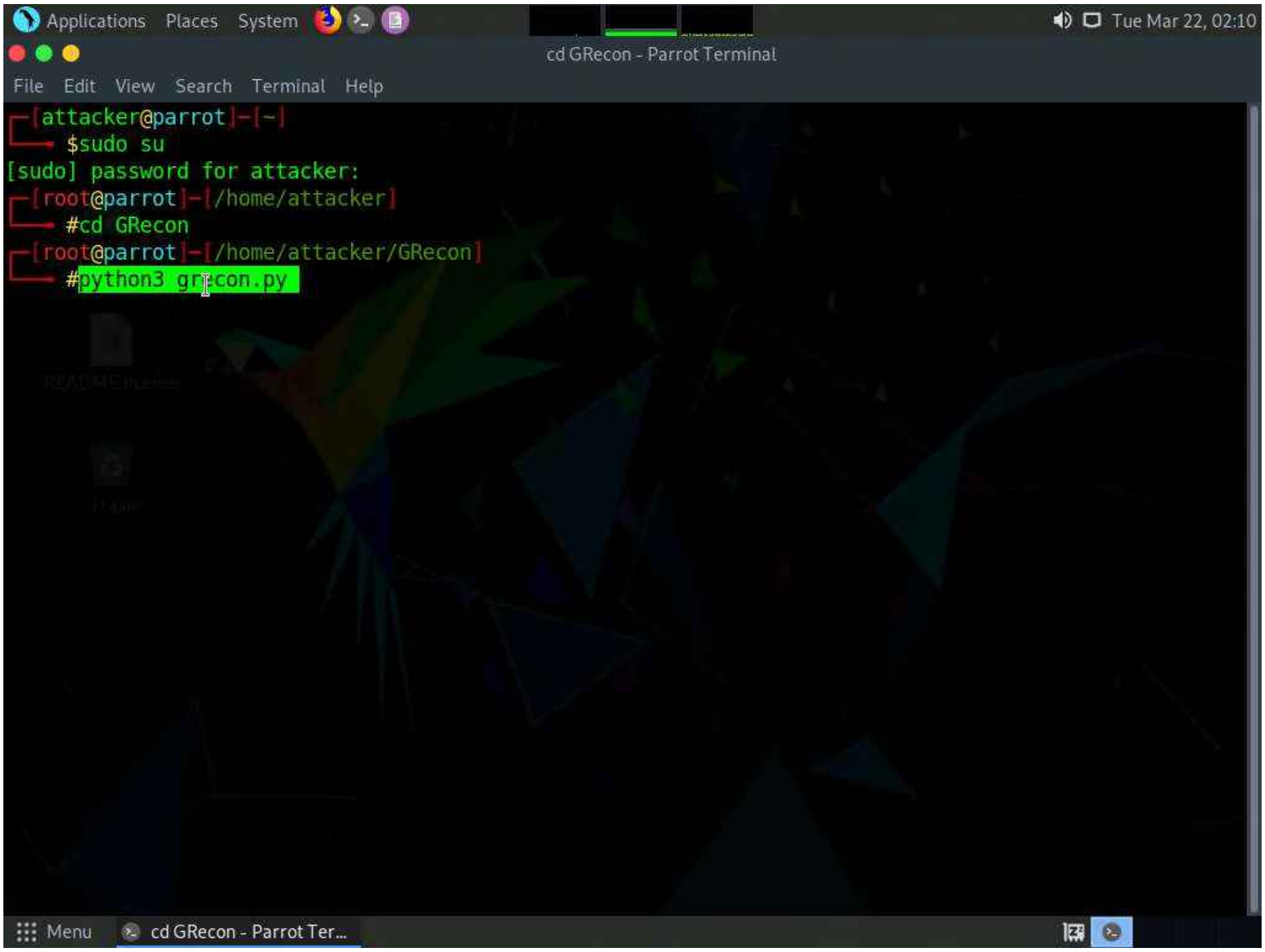
> Note: The password that you type will not be visible.



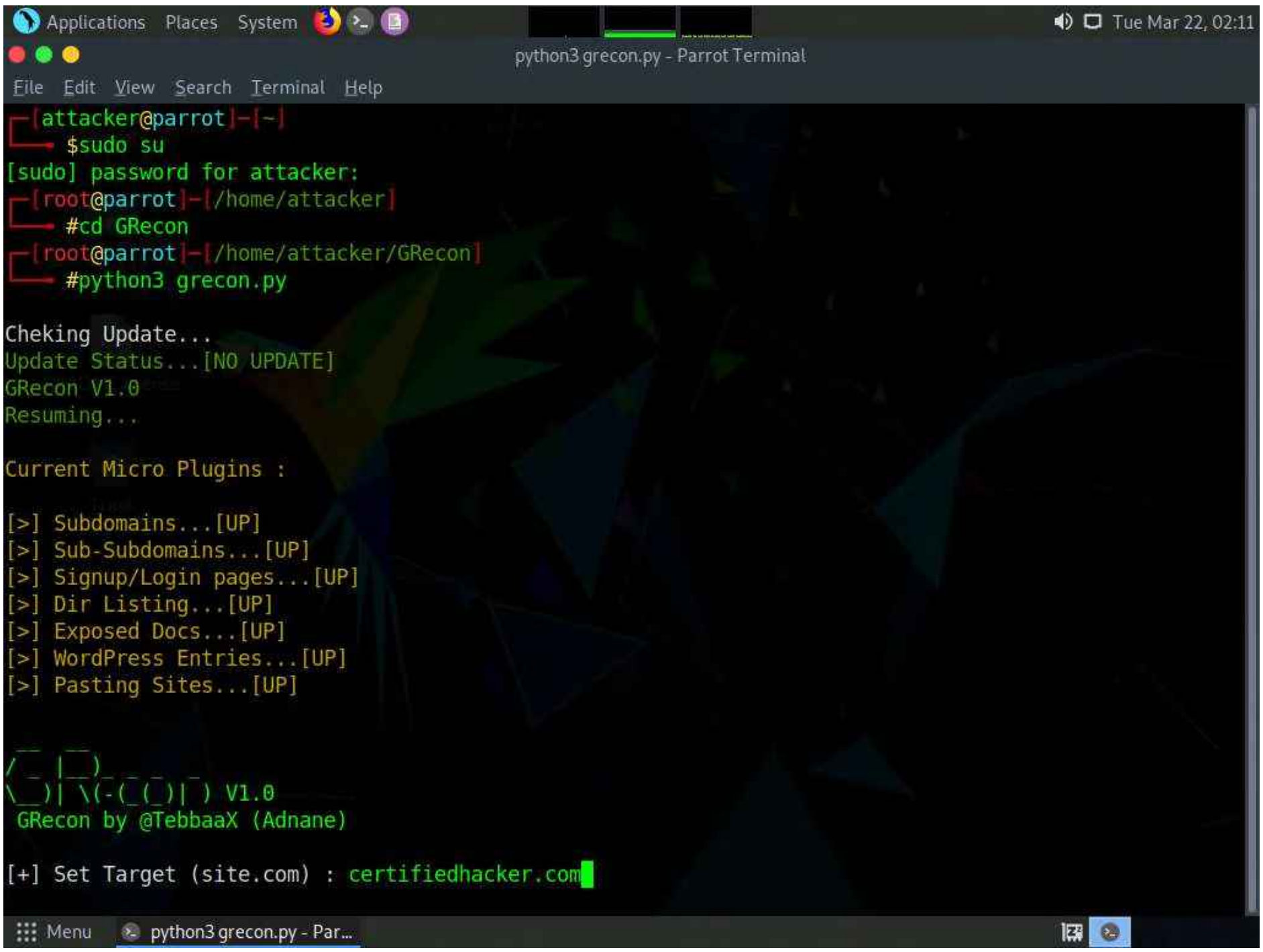
5. Now type **cd GRecon** and press **Enter** to navigate to GRecon directory.



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

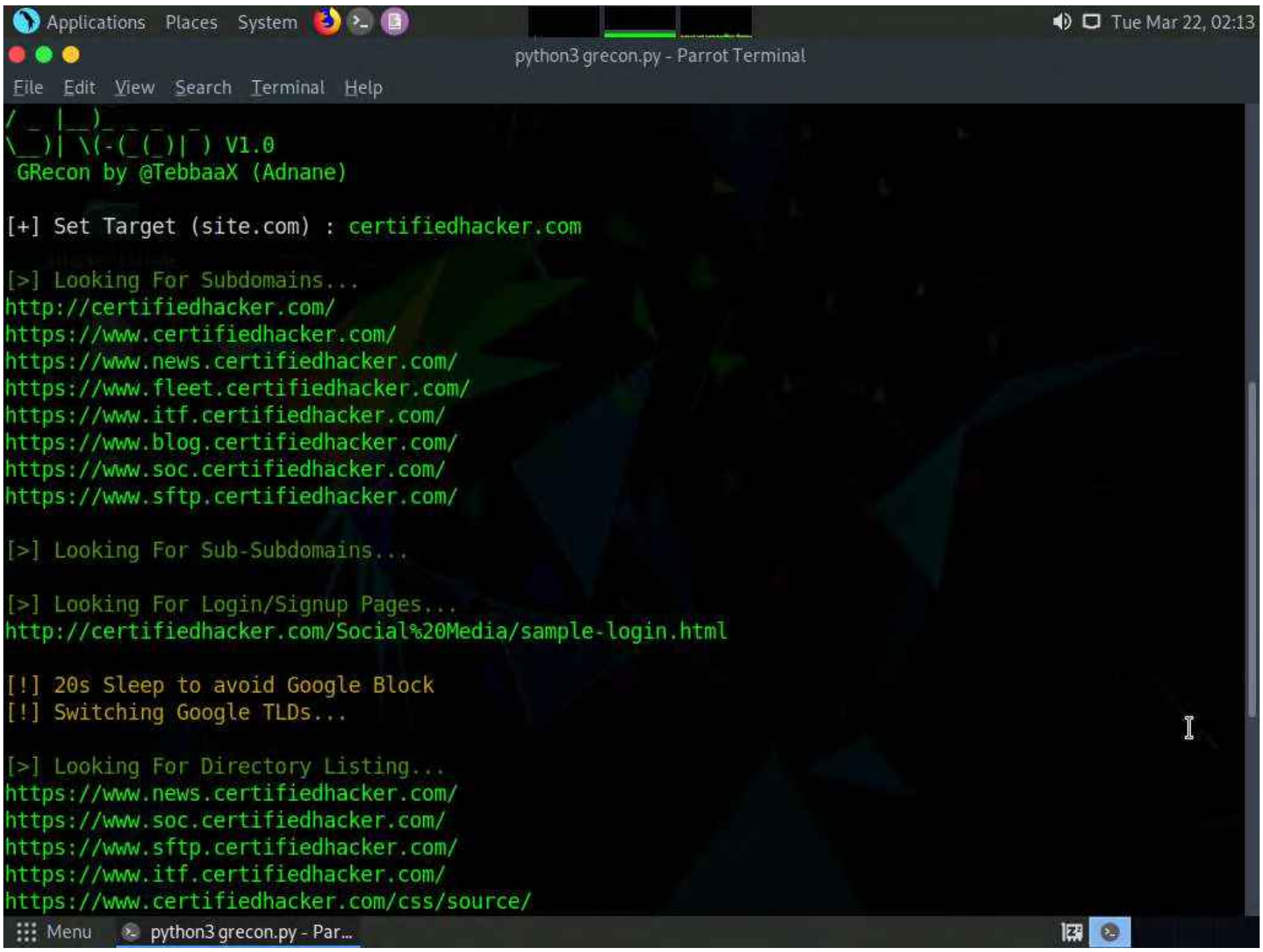


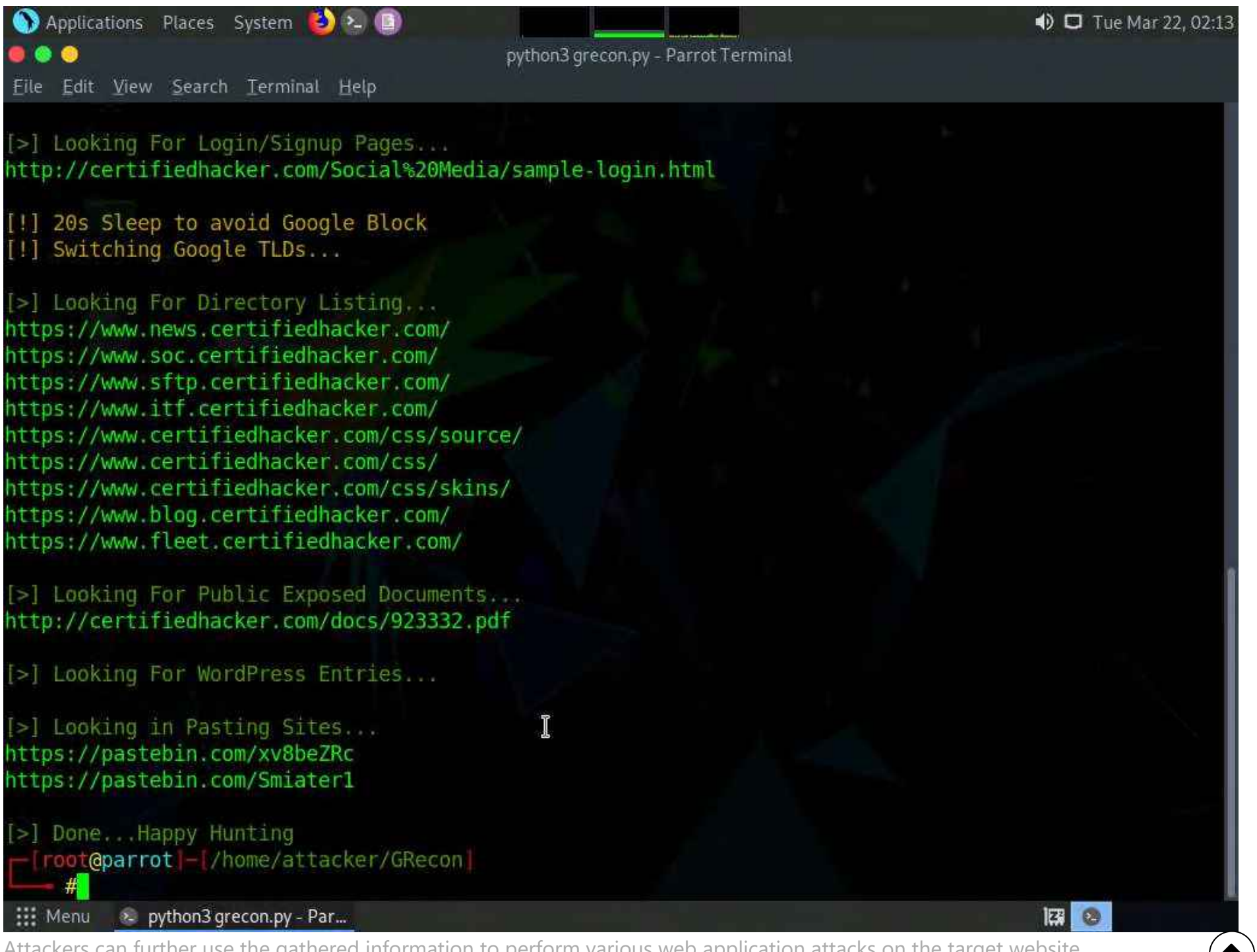
7. **GRecon** initializes, in the **Set Target (site.com):** field type **certifiedhacker.com** and press **Enter**.



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.





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.

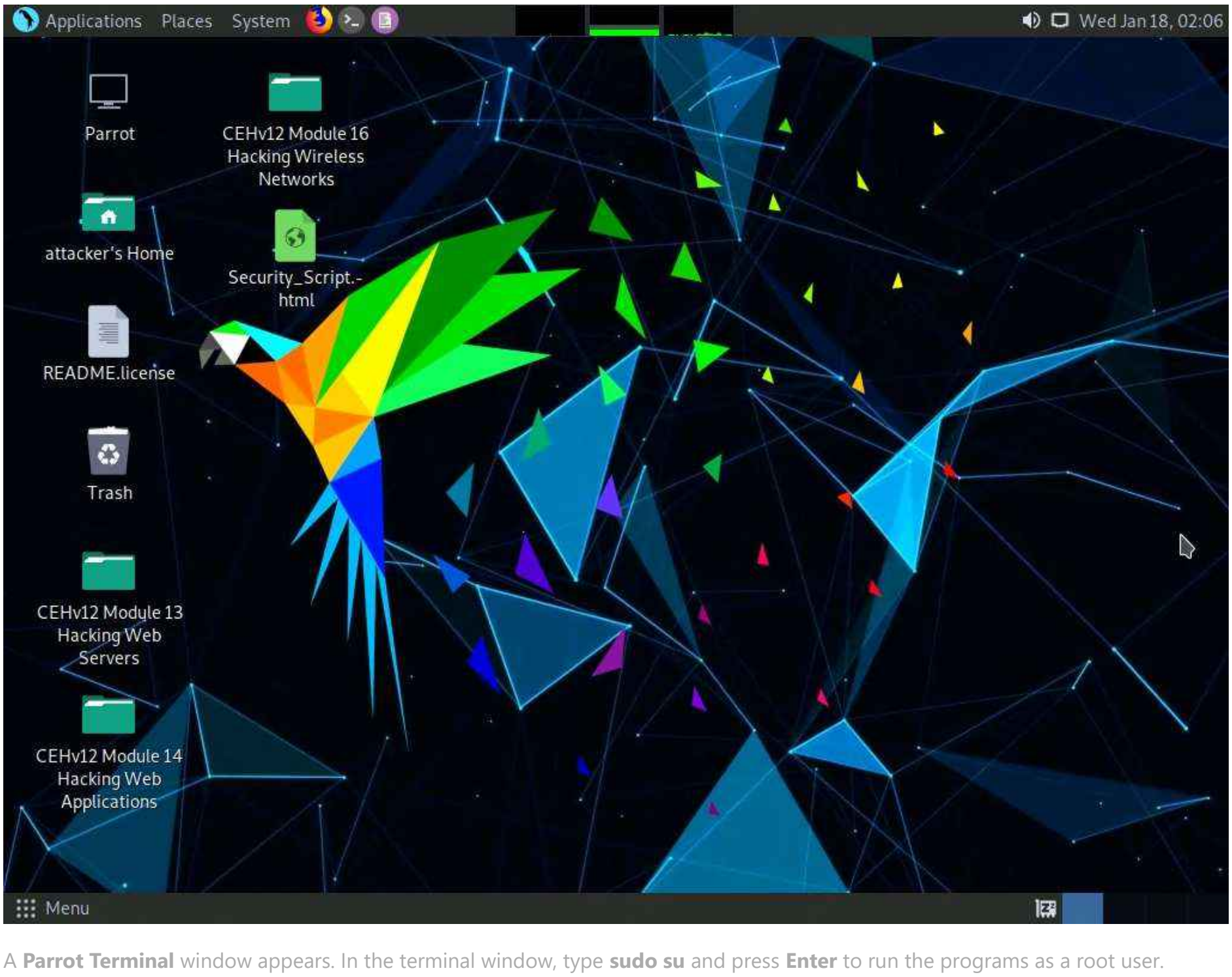
11. Close all open windows and document all the acquired information.

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

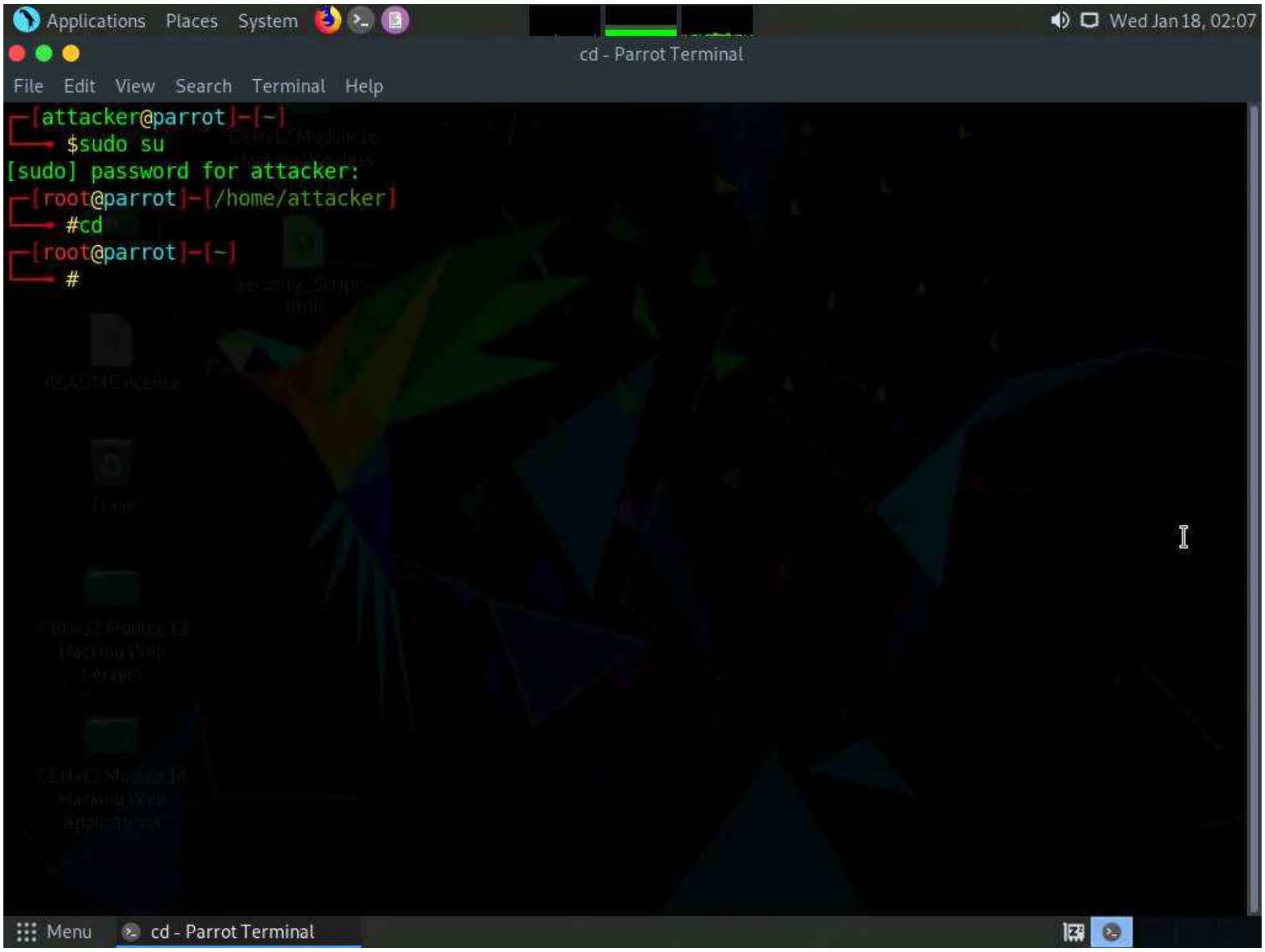


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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.

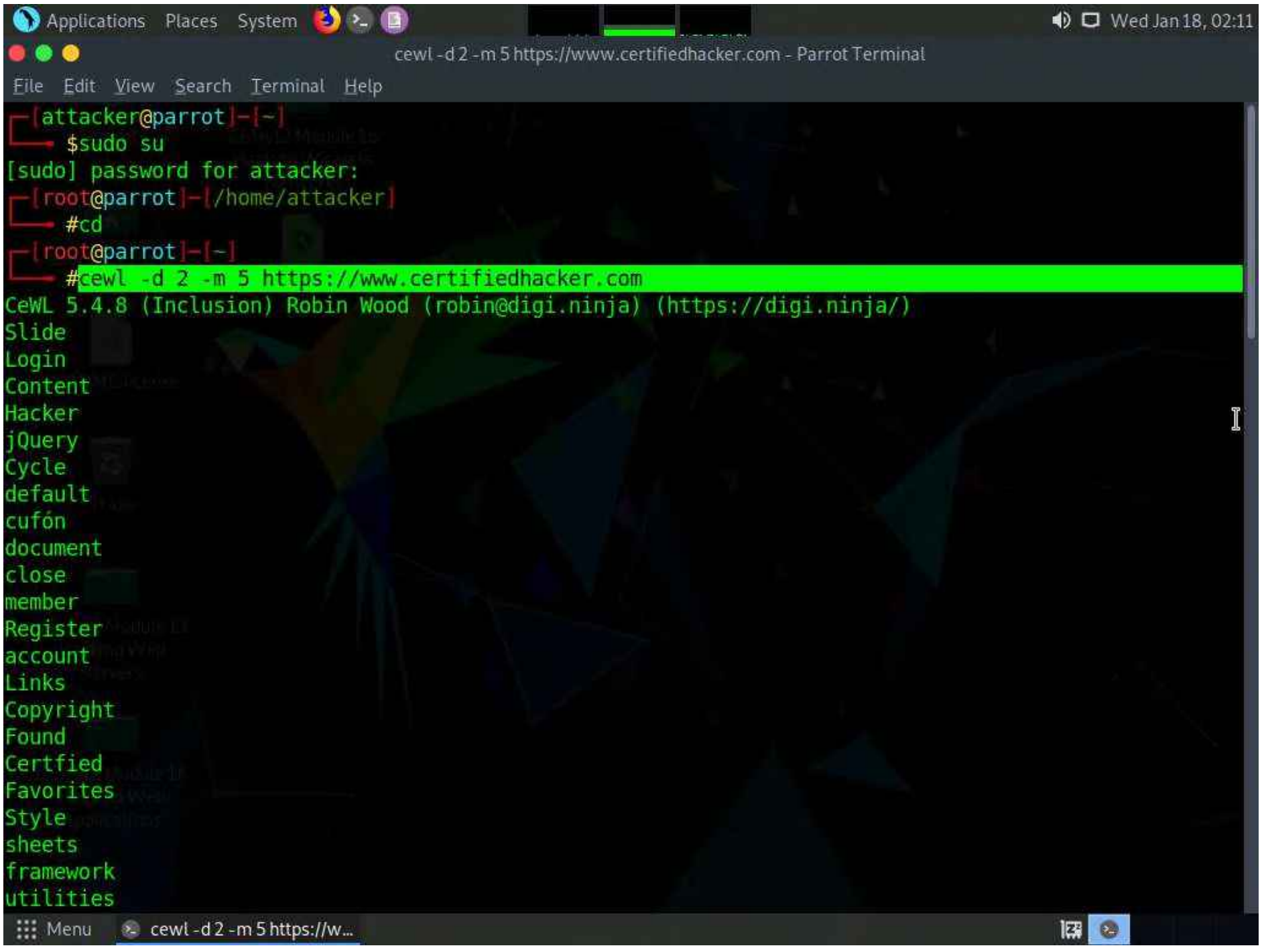


5. In the terminal window, type **cewl -d 2 -m 5 https://www.certifiedhacker.com** and press **Enter**.

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

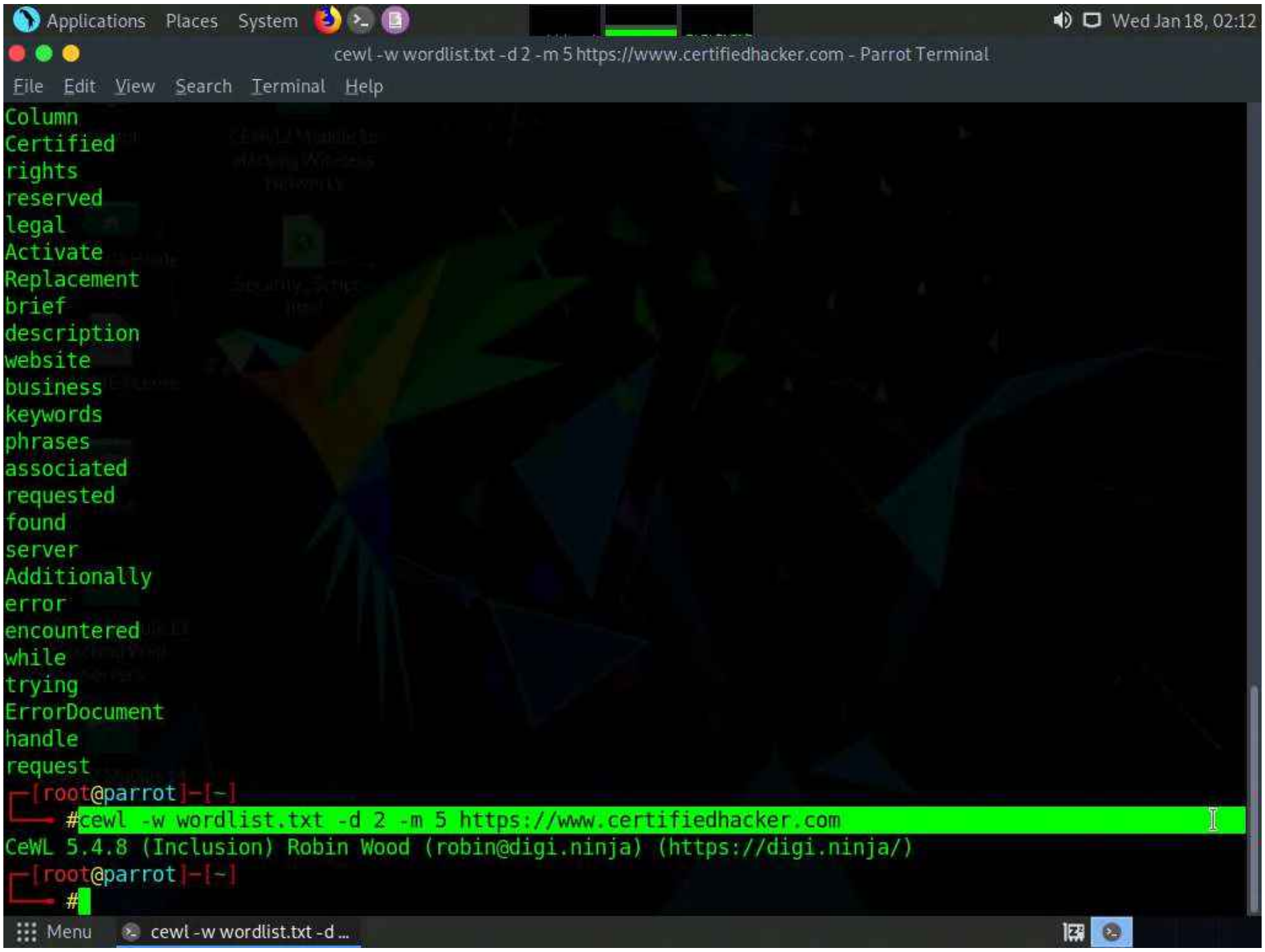
6. A unique wordlist from the target website is gathered, as shown in the screenshot.

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

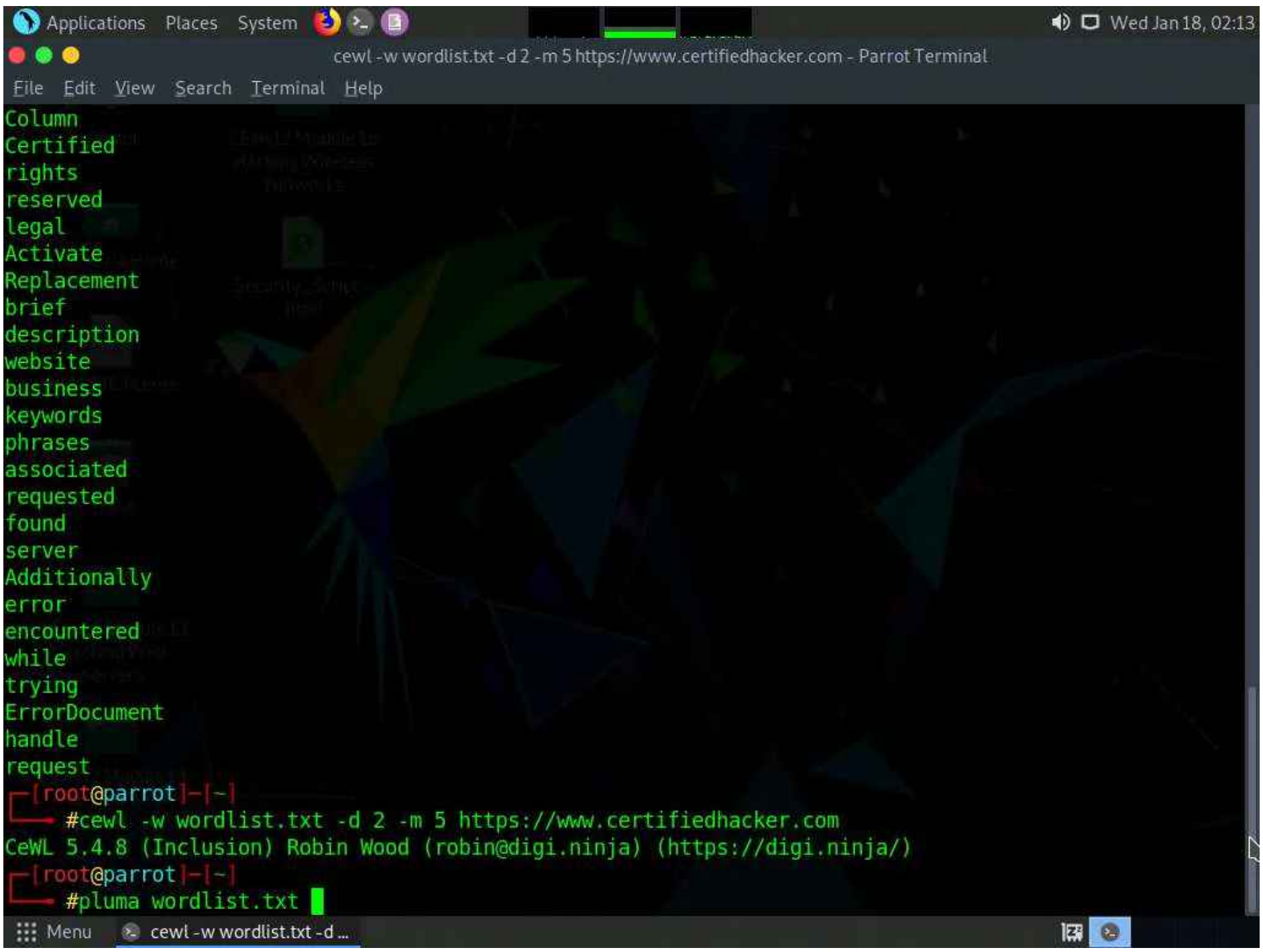


7. Alternatively, this unique wordlist can be written directly to a text file. To do so, type **cewl -w wordlist.txt -d 2 -m 5 https://www.certifiedhacker.com** and press **Enter**.

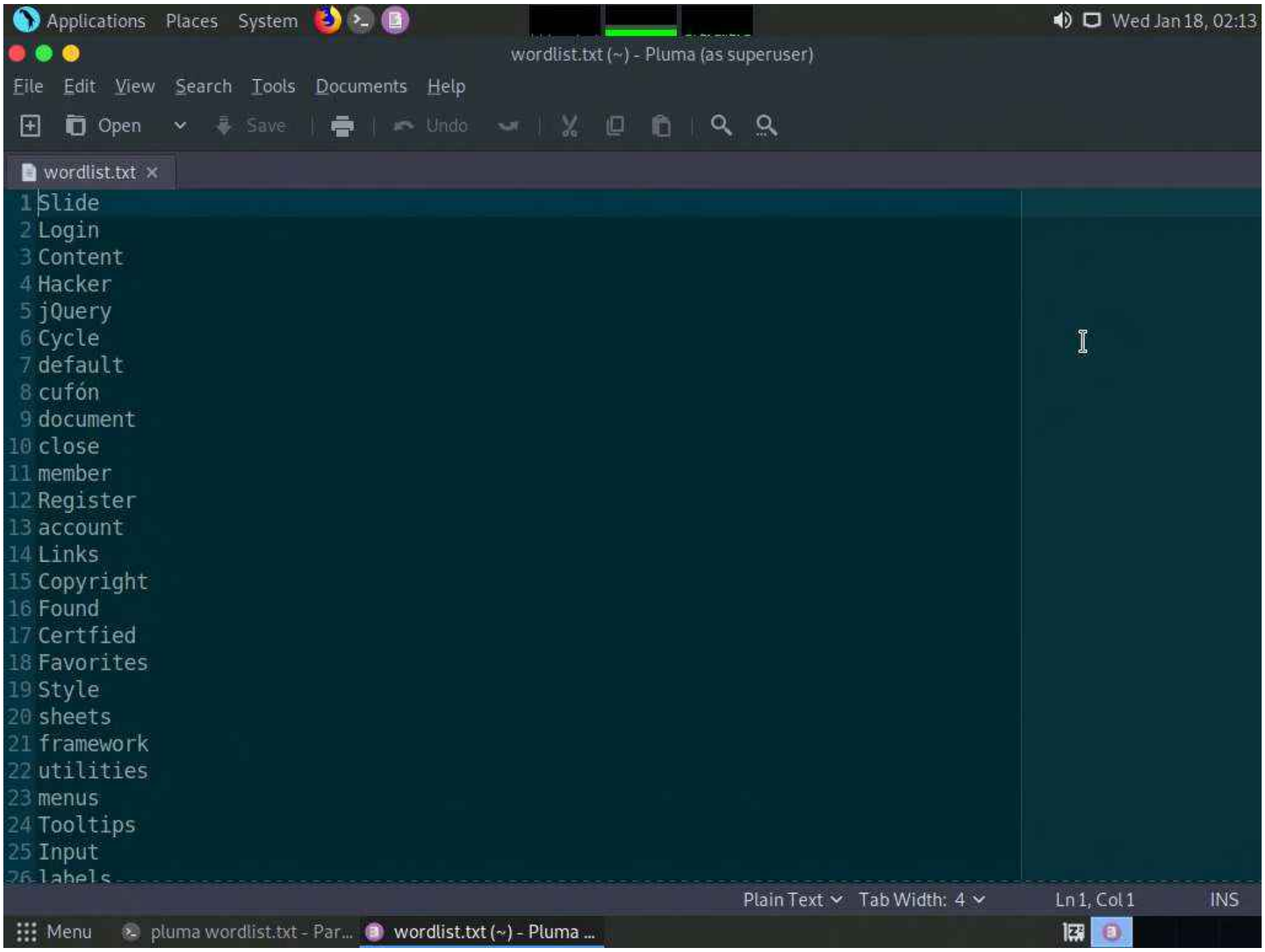
Note: **-w** - Write the output to the file (here, **wordlist.txt**)



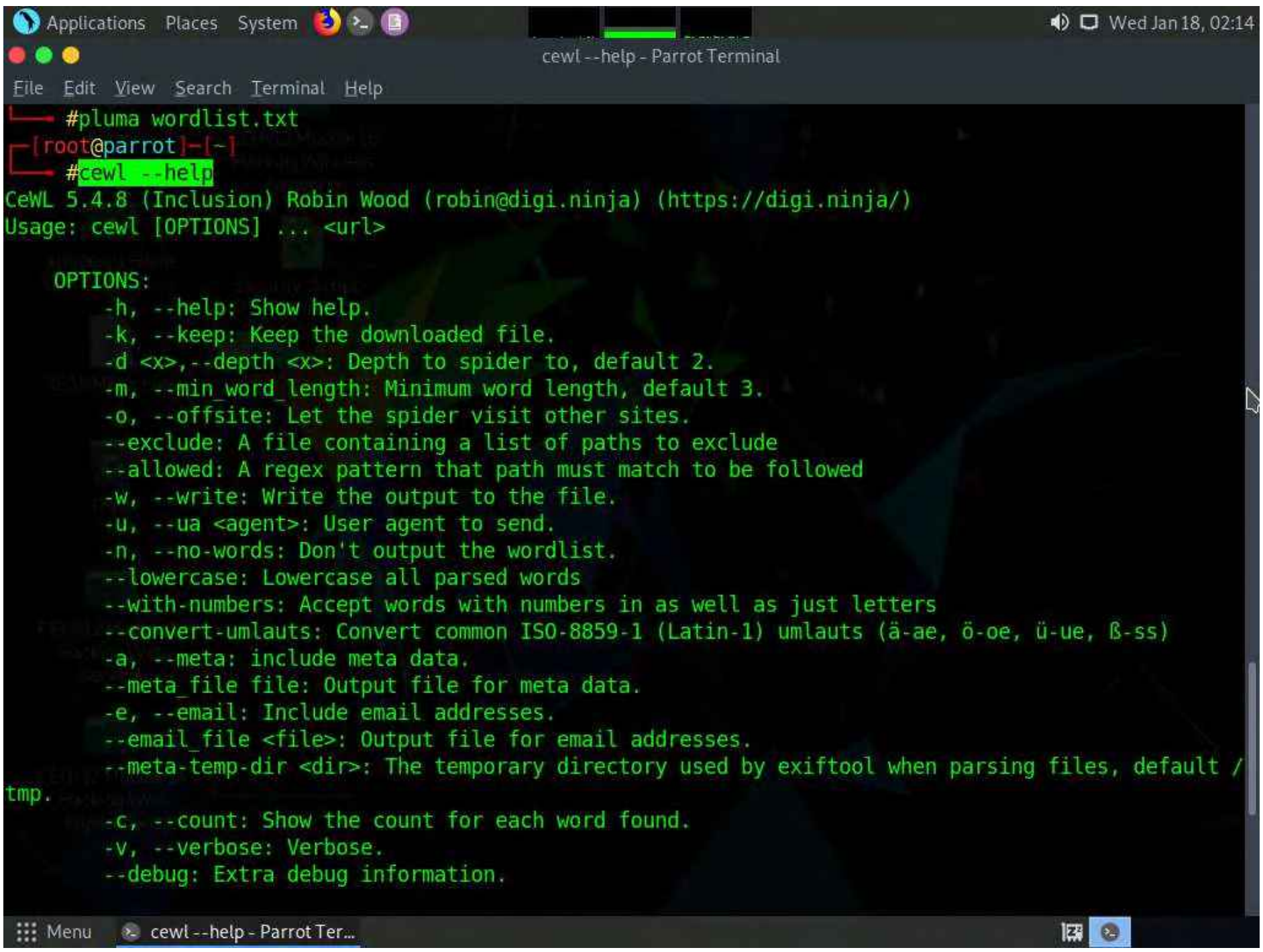
8. By default, the wordlist file gets saved in the **root** directory. Type **pluma wordlist.txt** and press **Enter** to view the extracted wordlist.



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



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



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.

Lab 5: Perform Email Footprinting

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

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:.

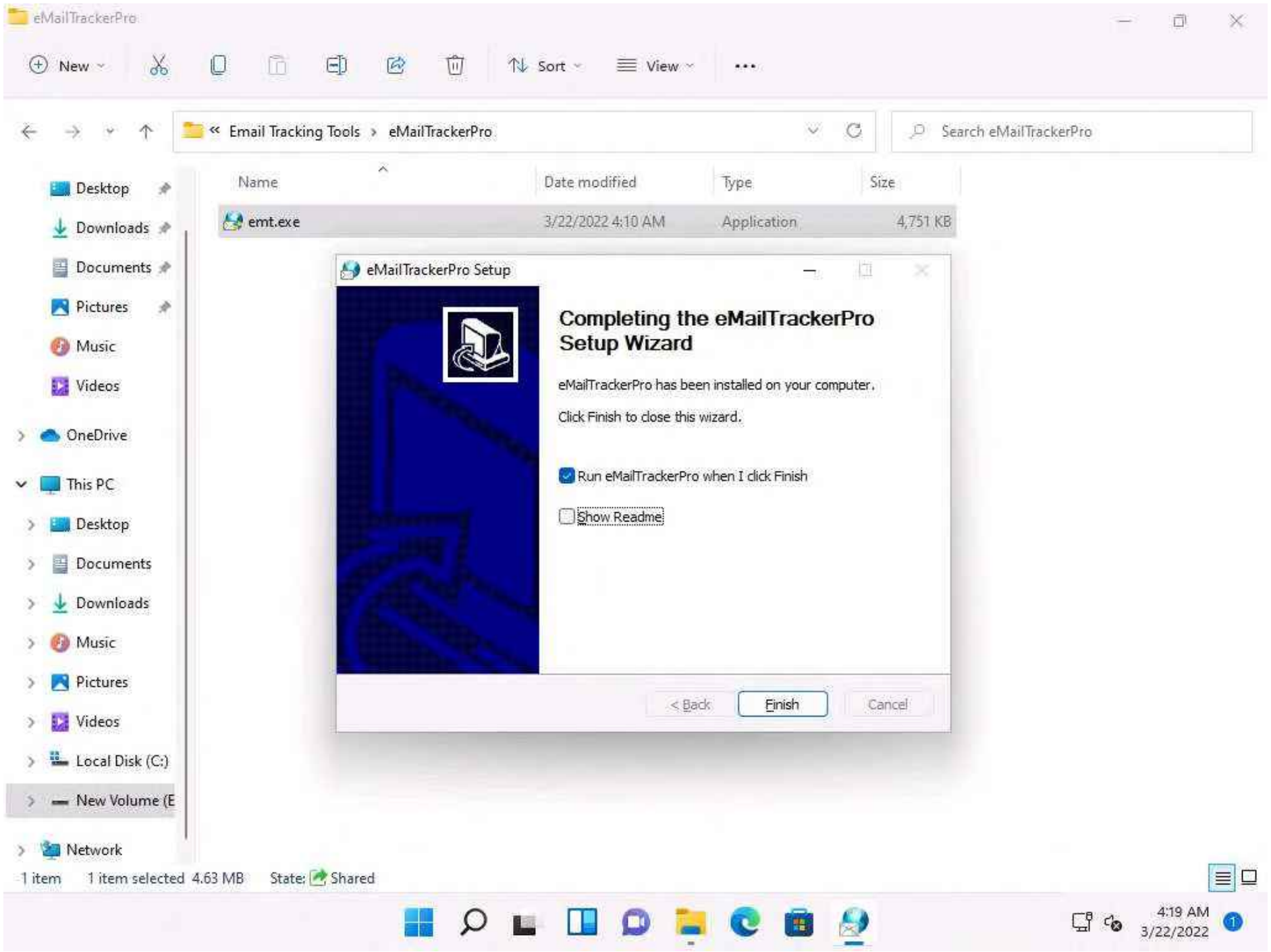
Recipient's system IP address
The GPS coordinates and map location of the recipient
When an email message was received and read
Type of server used by the recipient
Operating system and browser information
If a destructive email was sent
The time spent reading the email
Whether or not the recipient visited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

Task 1: Gather Information about a Target by Tracing Emails using eMailTrackerPro

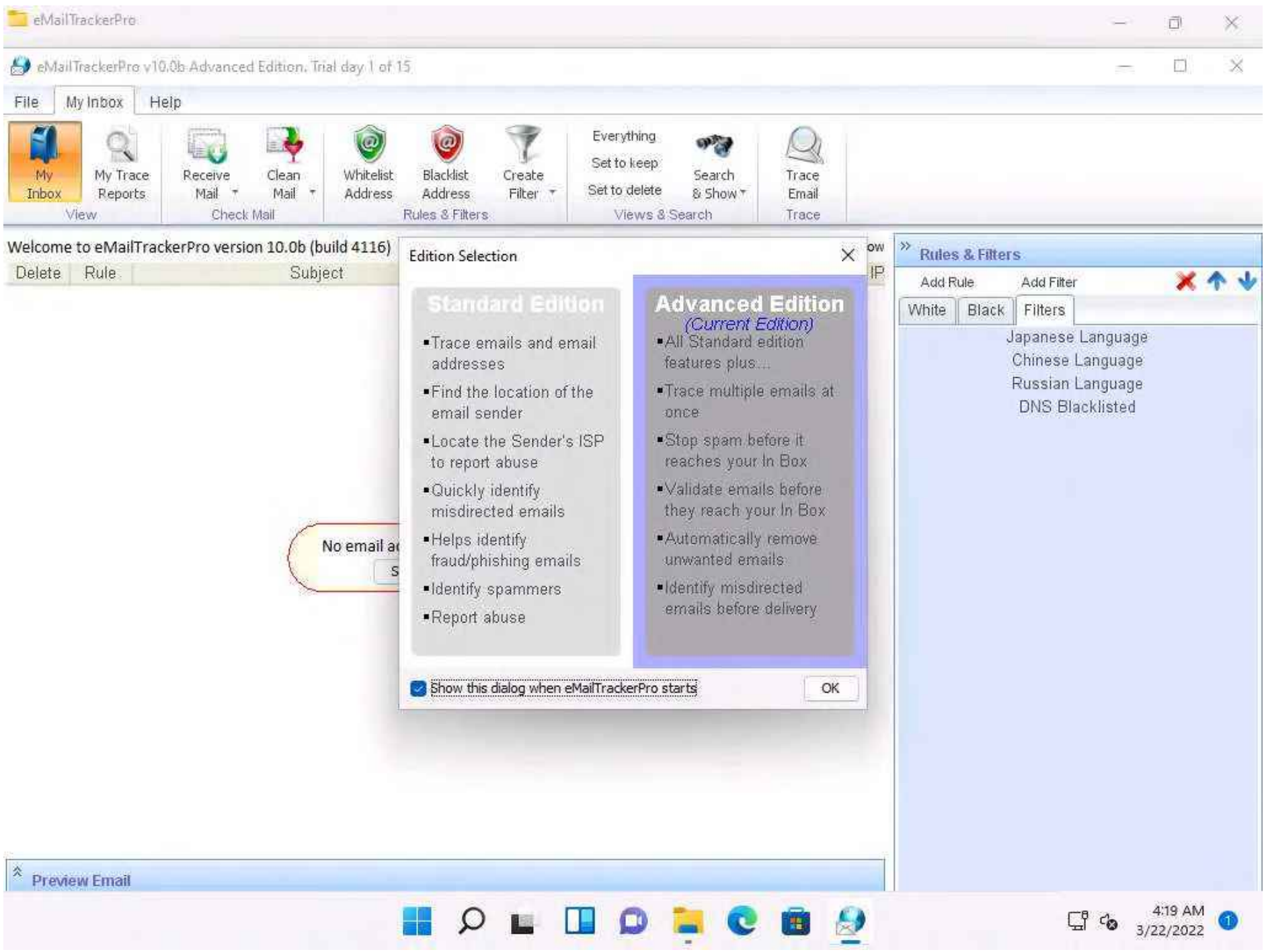
The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email 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.

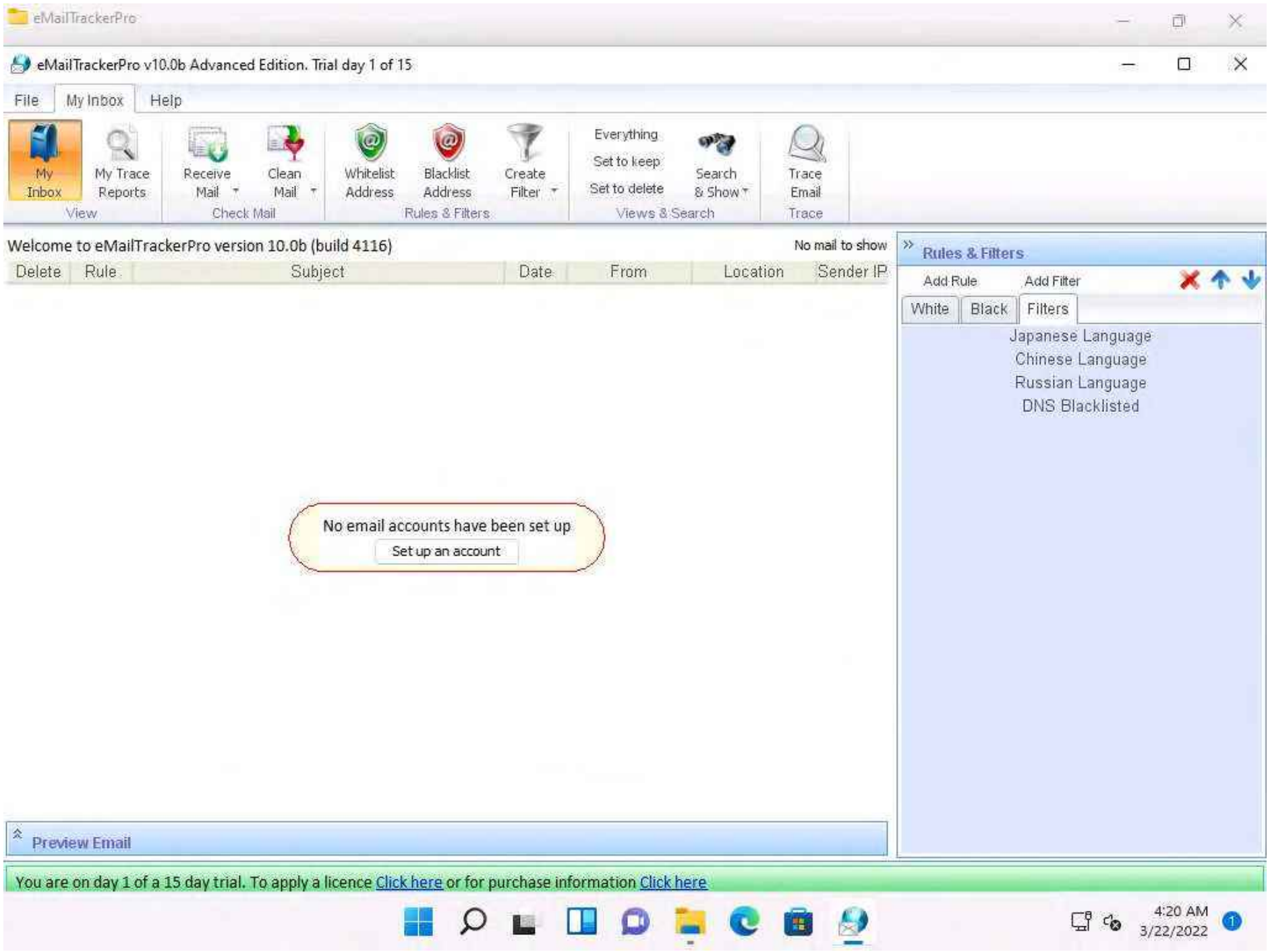
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. The **eMailTrackerPro 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.



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

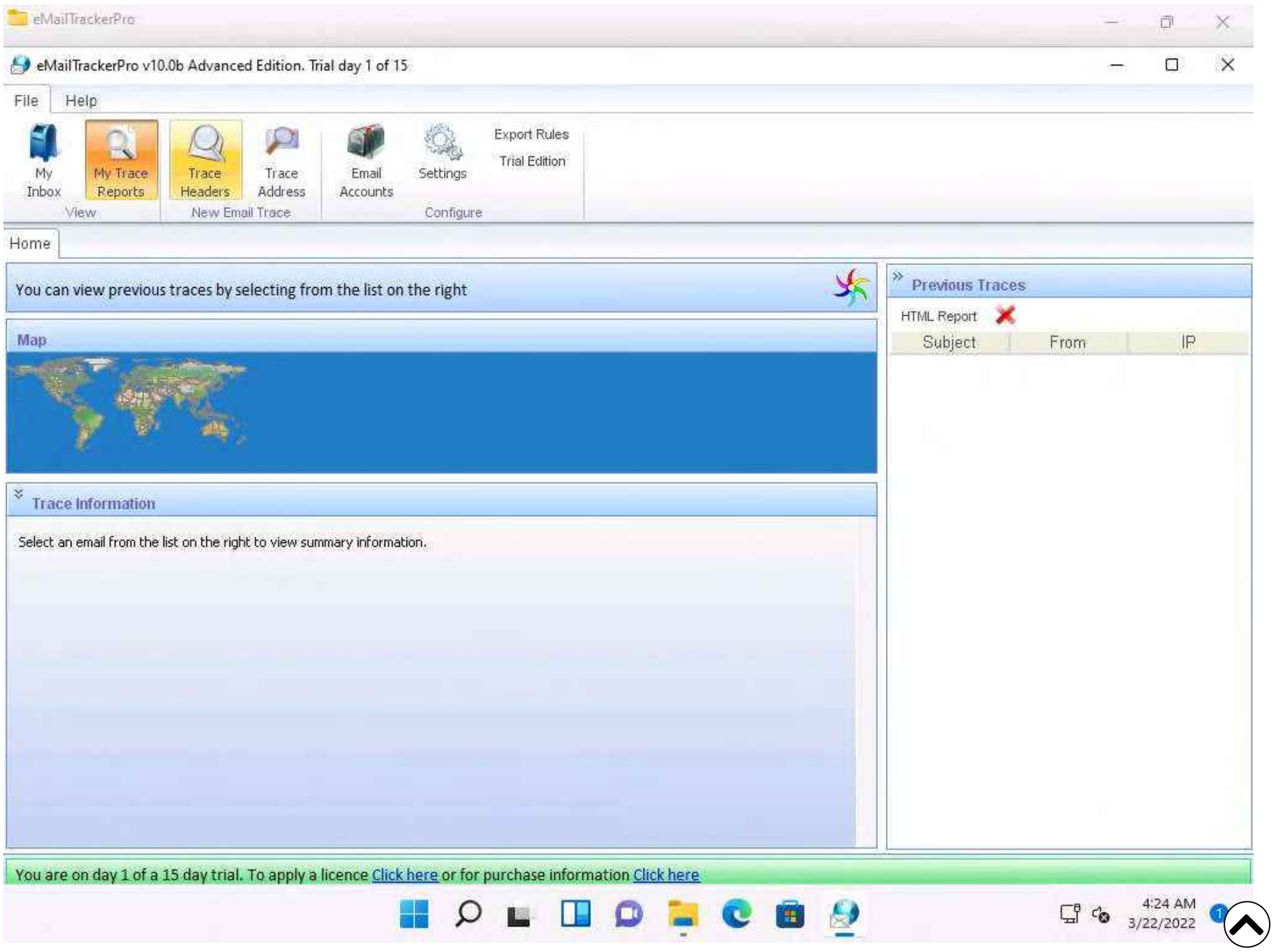


6. The **eMailTrackerPro** main window appears, as shown in the screenshot.

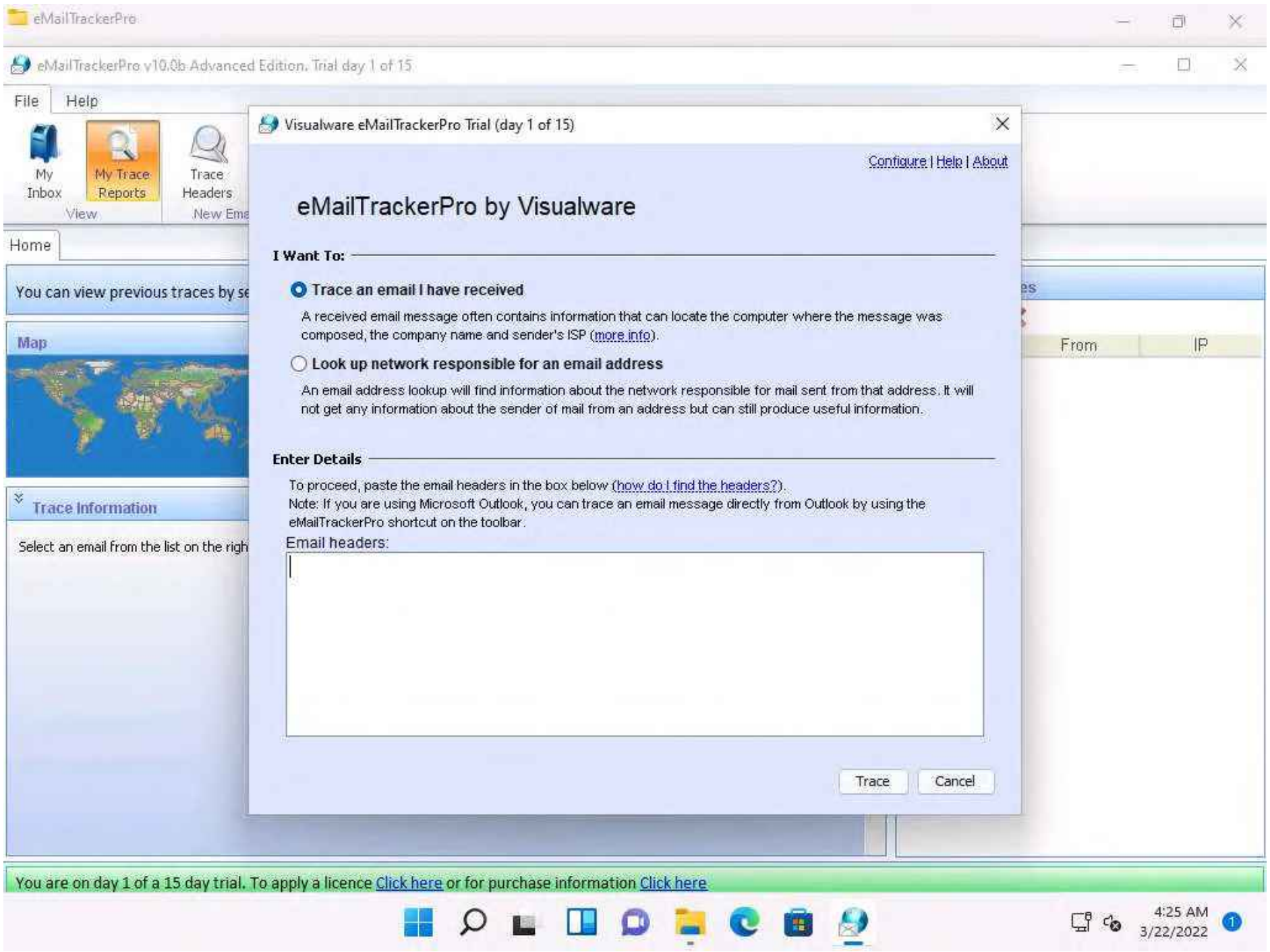


7. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header).

8. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.



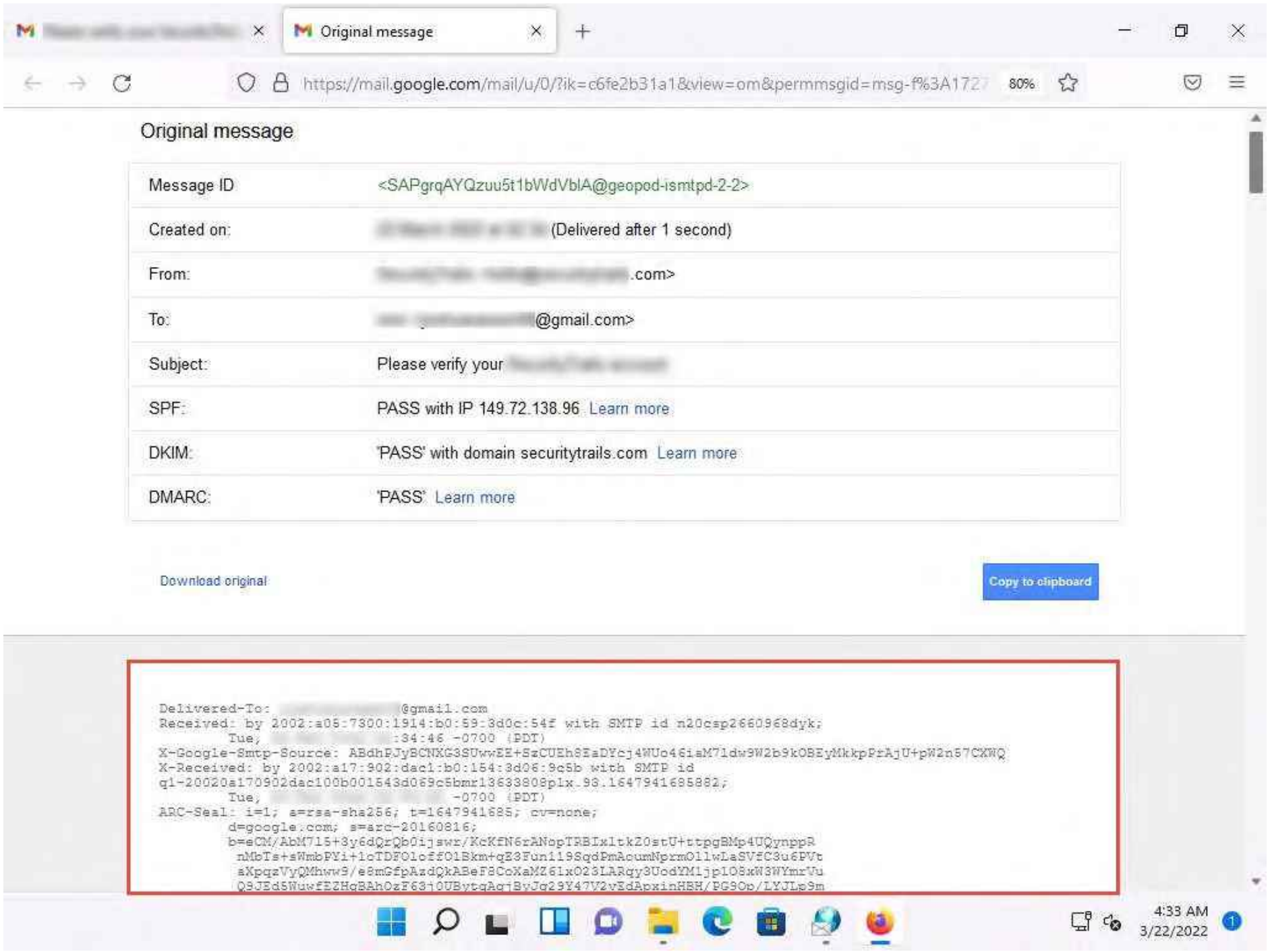
9. A pop-up window will appear; select **Trace an email I have received**. Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers**: field under **Enter Details** section.



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.

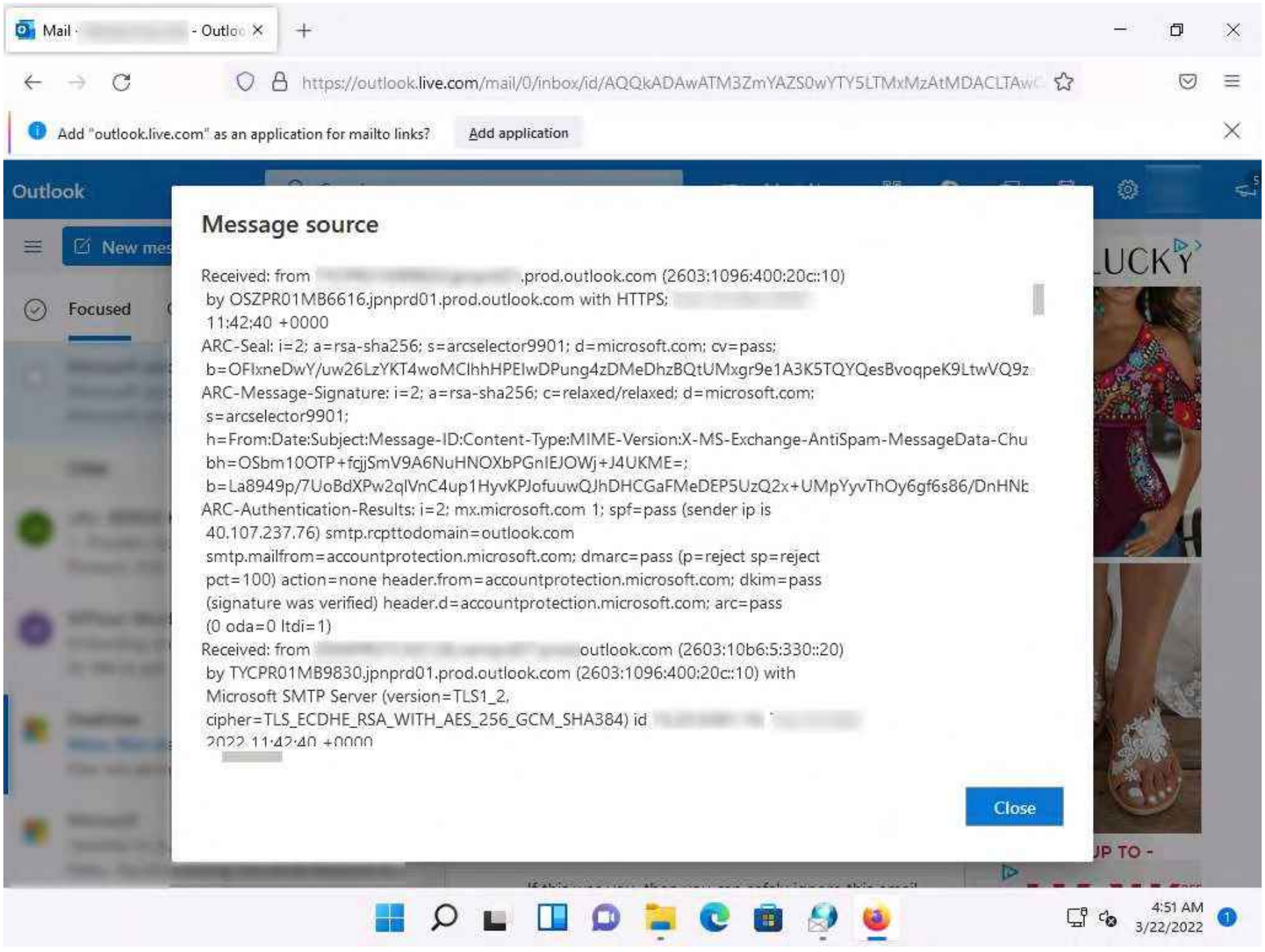
Note: In **Gmail**, find the email header by following the steps:

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



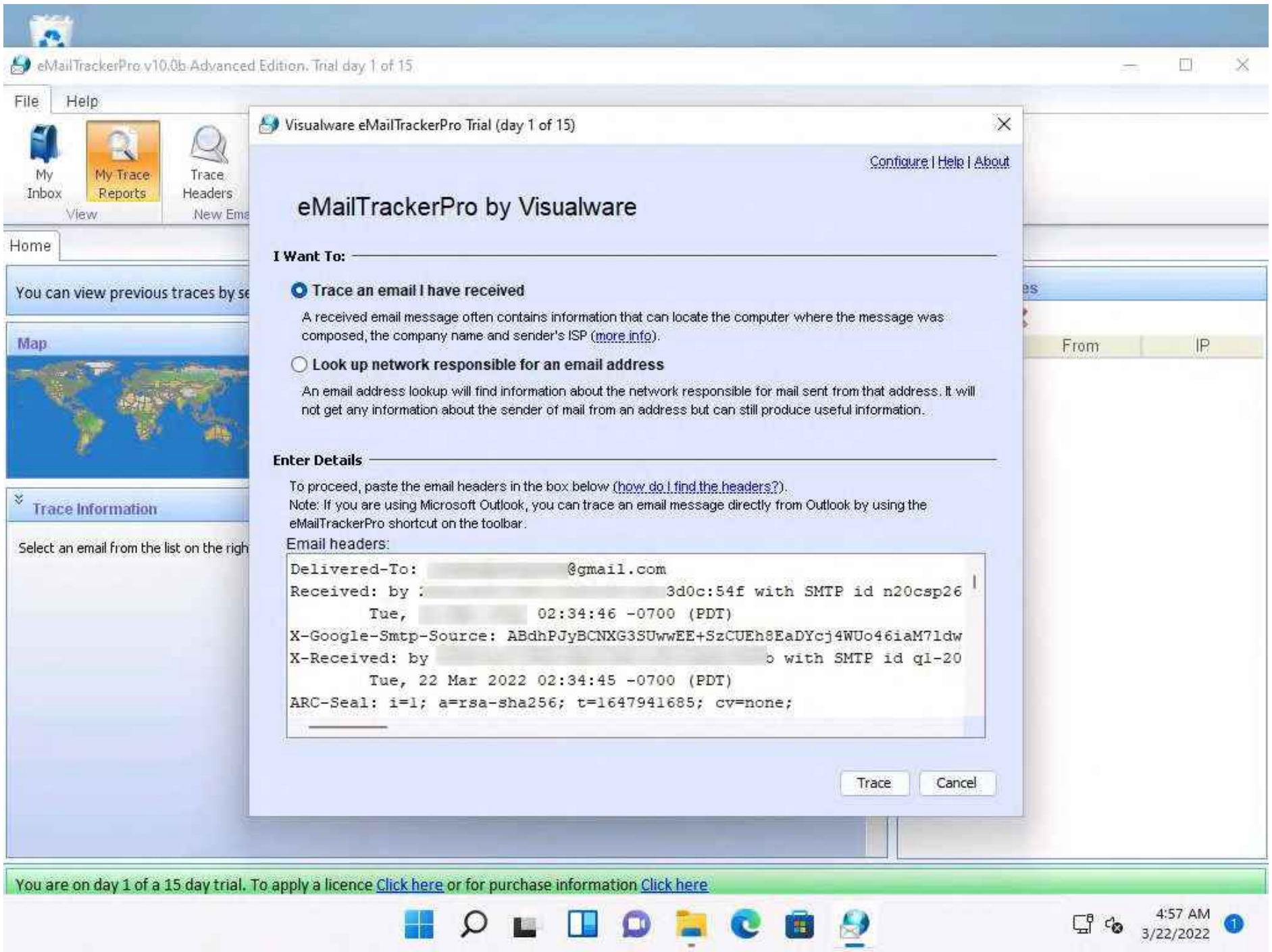
Note: In **Outlook**, find the email header by following the steps:

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



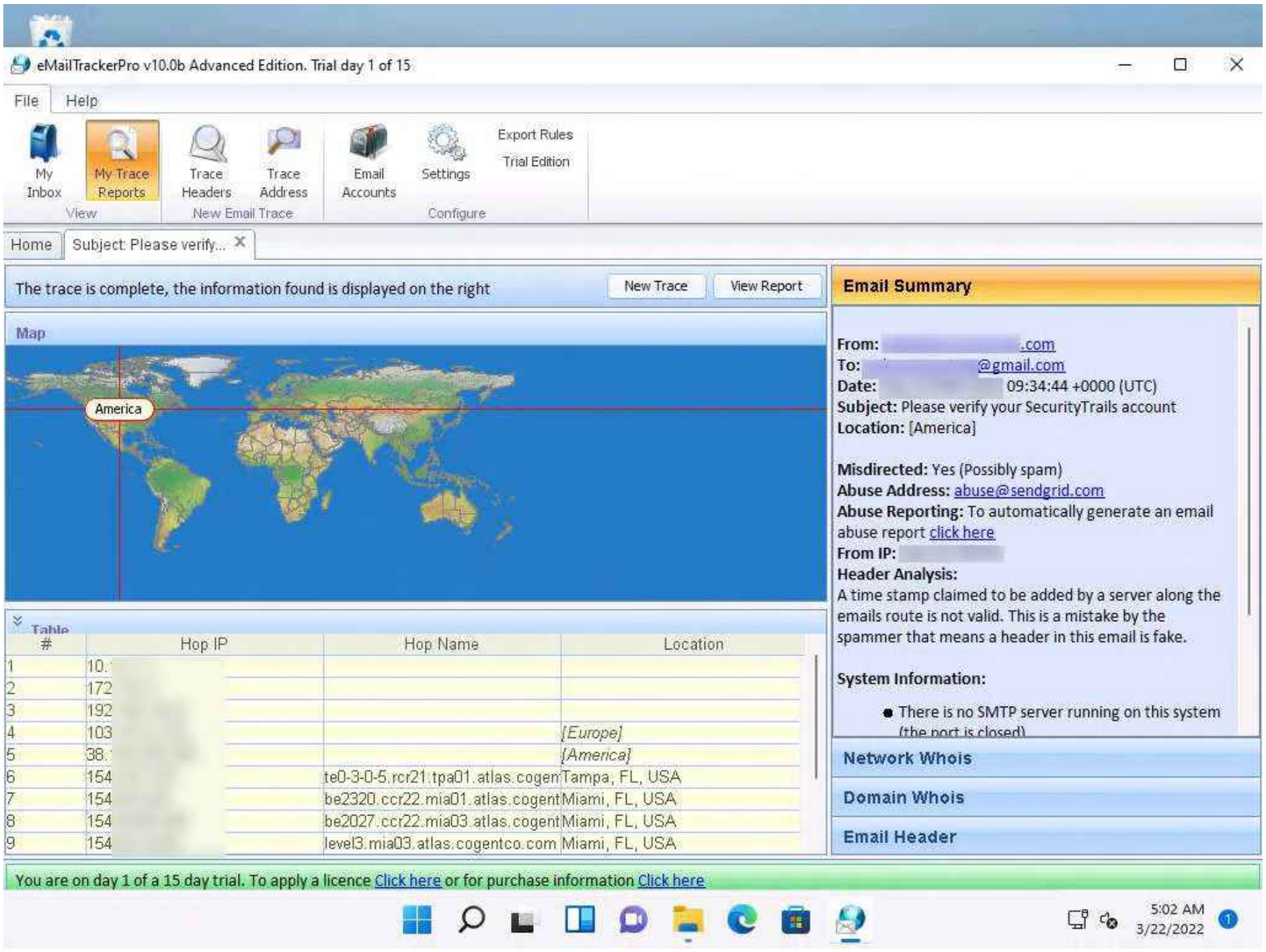
11. Copy the entire email header text and paste it into the **Email headers**: field of eMailTrackerPro, and click **Trace**.

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

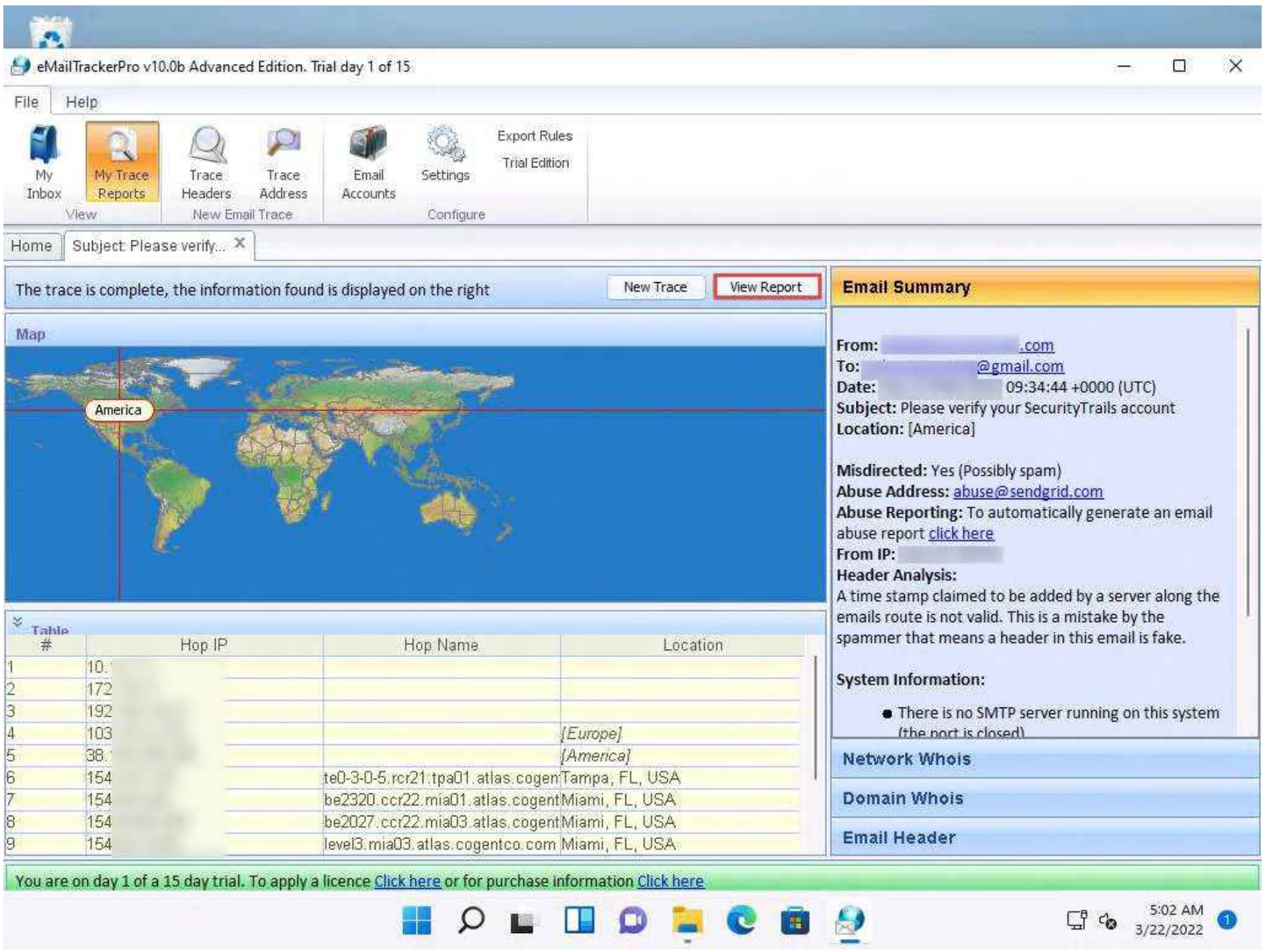


12. The **My Trace Reports** window opens.

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.



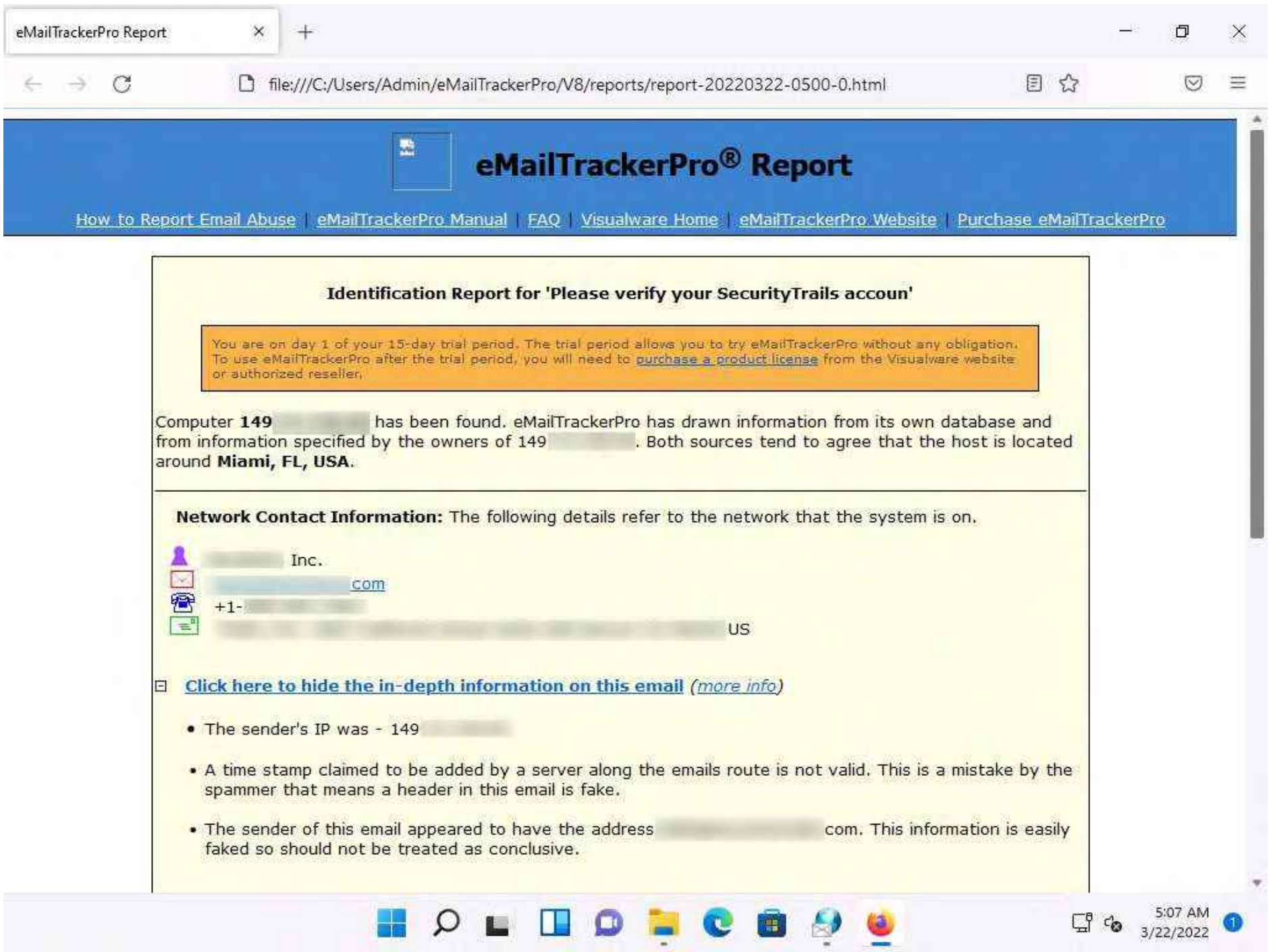
14. To examine the report, click the **View Report** button above **Map** to view the complete trace report.



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.



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.

Lab 6: Perform Whois Footprinting

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

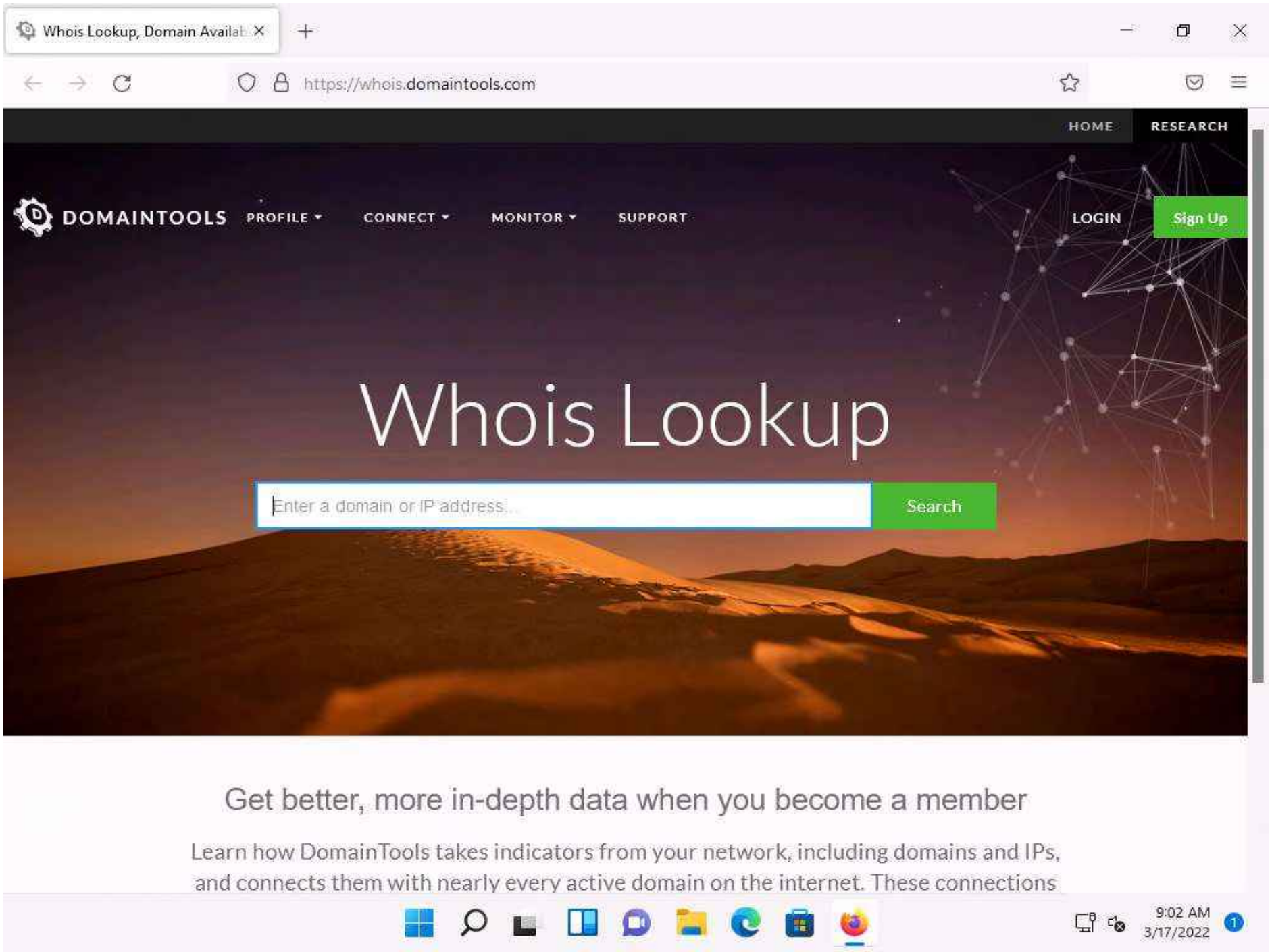
Overview of Whois Footprinting

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).

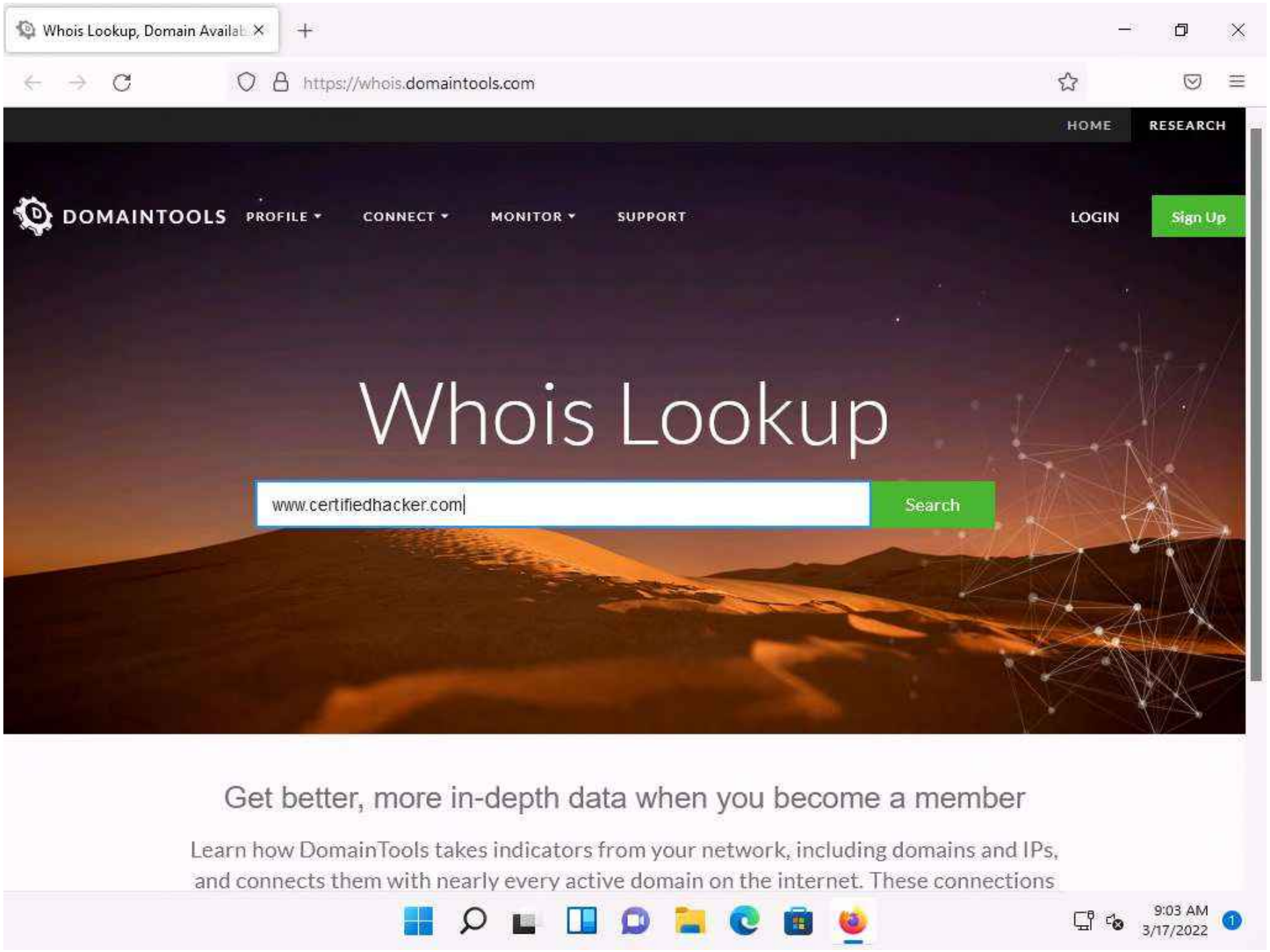
Task 1: Perform Whois Lookup using DomainTools

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

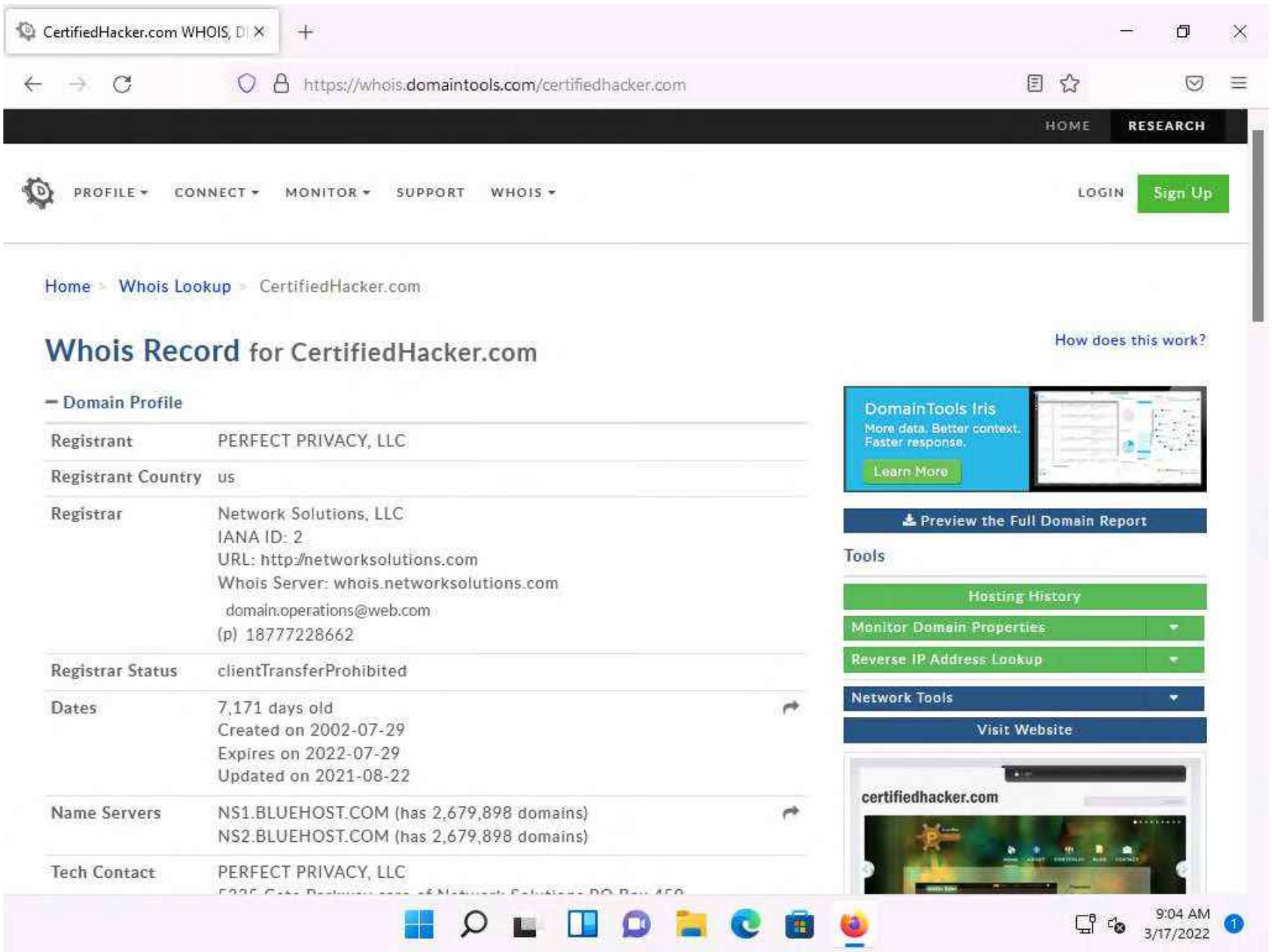
1. In the **Windows 11** machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **http://whois.domaintools.com** and press **Enter**. The Whois Lookup website appears, as shown in the screenshot.

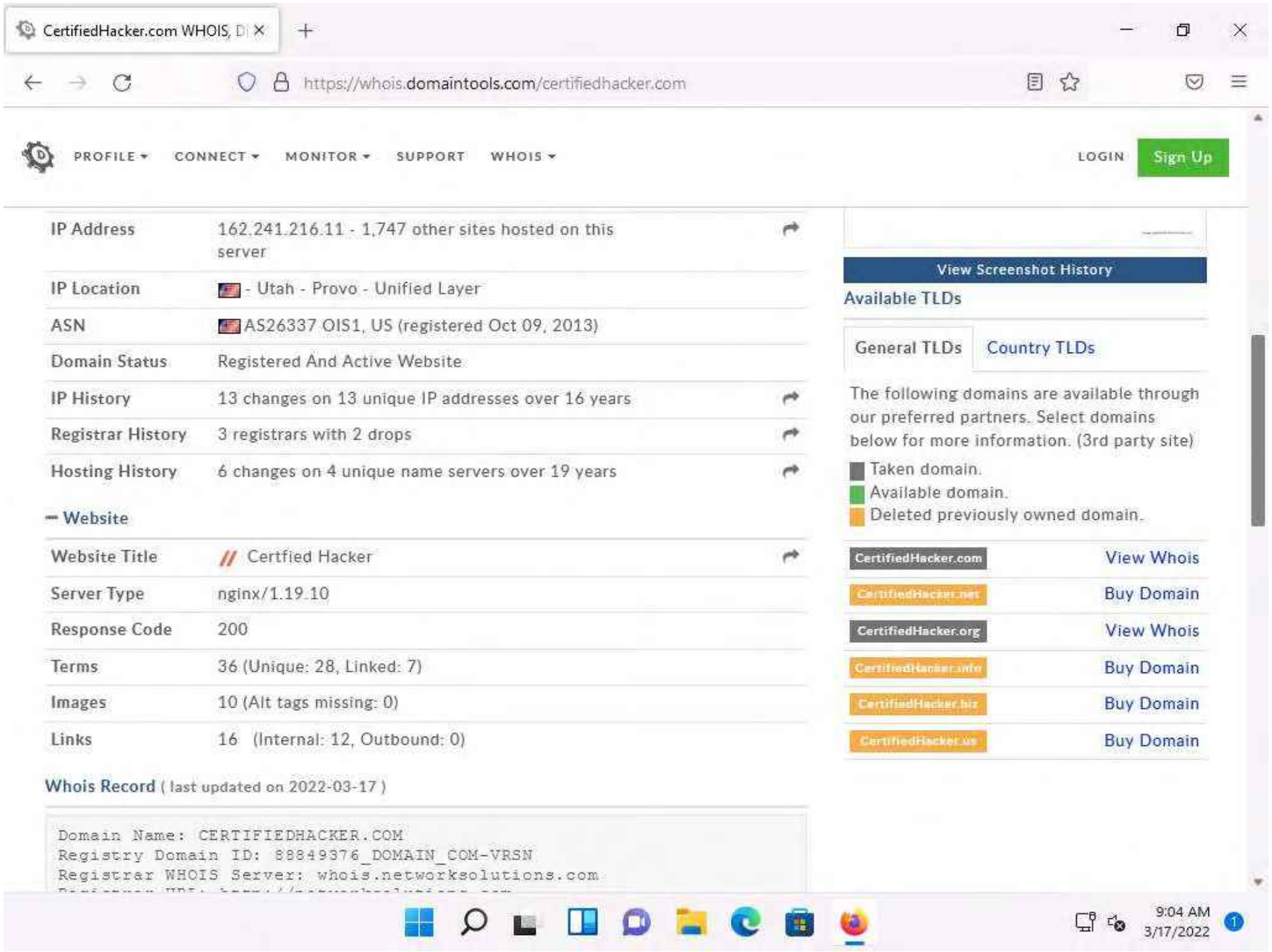


2. Now, in the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.



3. 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.





4. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
5. 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.
6. Close all open windows and document all the acquired information.

Lab 7: Perform DNS Footprinting

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

Overview of DNS

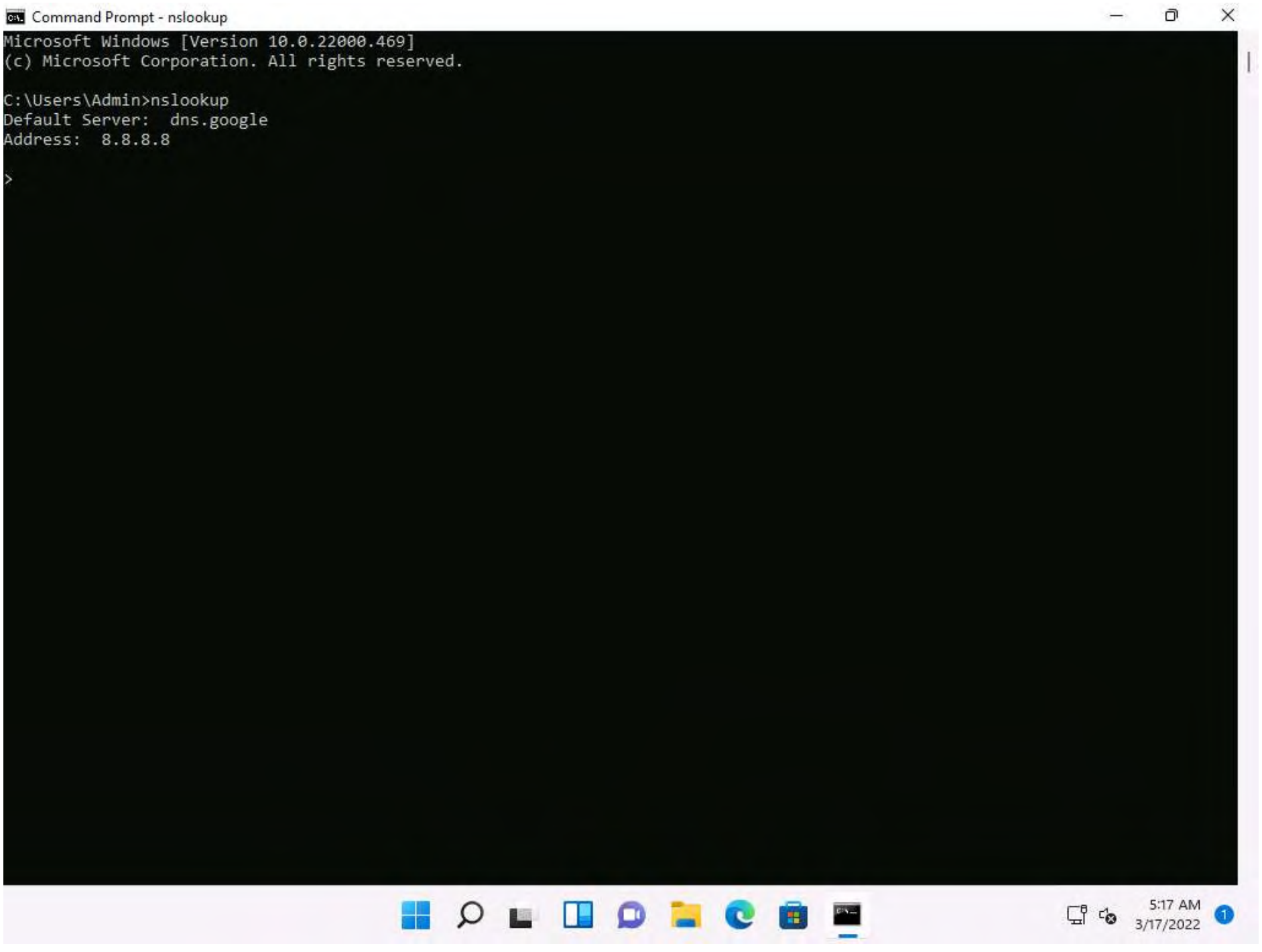
DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all 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.

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.

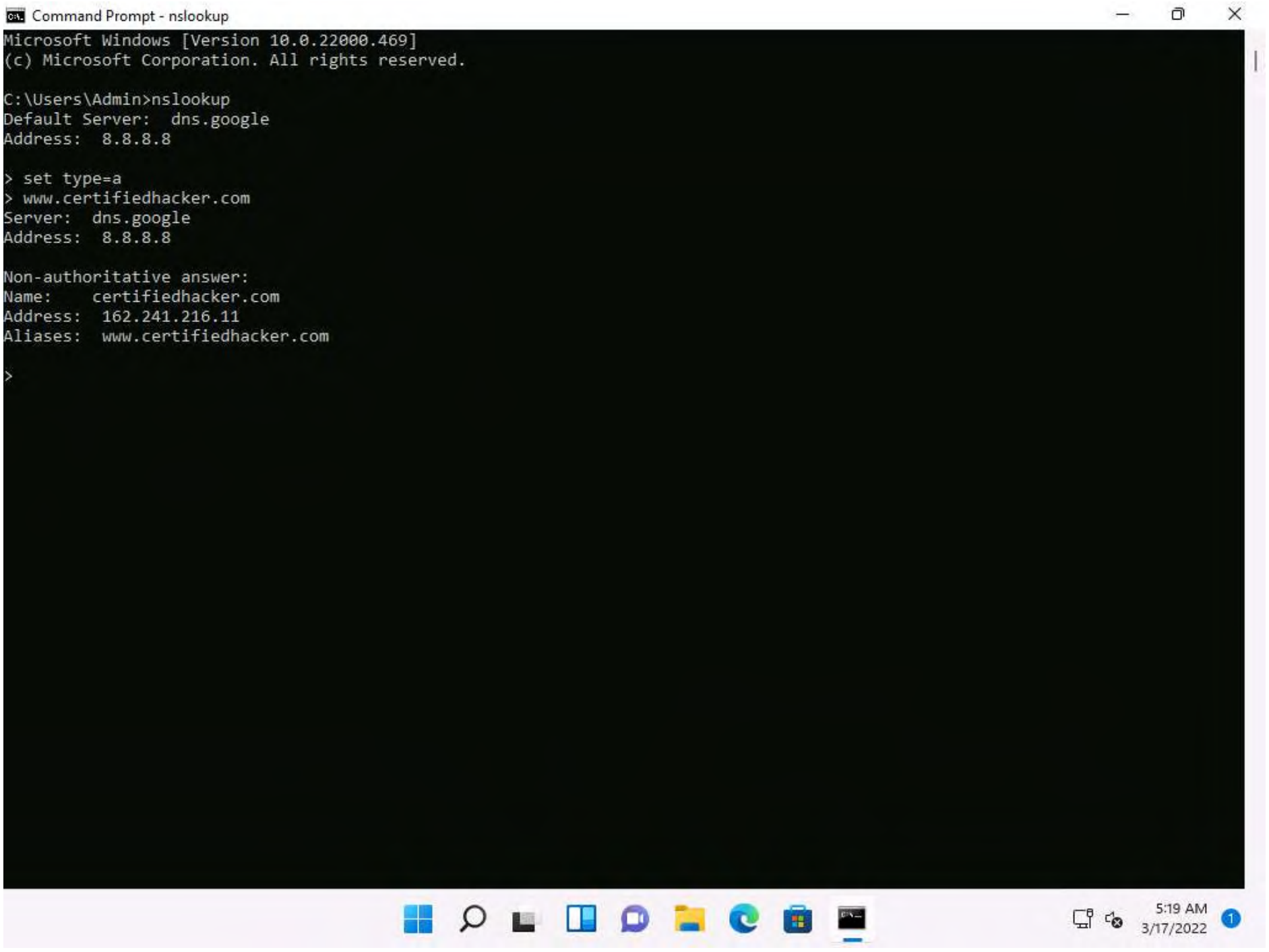
Here, we will perform DNS information gathering about target organizations using the nslookup command-line utility and NSLOOKUP web application.

1. In the **Windows 11** machine, launch a **Command Prompt**, type **nslookup** and press **Enter**. This displays the default server and its address assigned to the **Windows 11** machine.



2. 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.

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



4. 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.

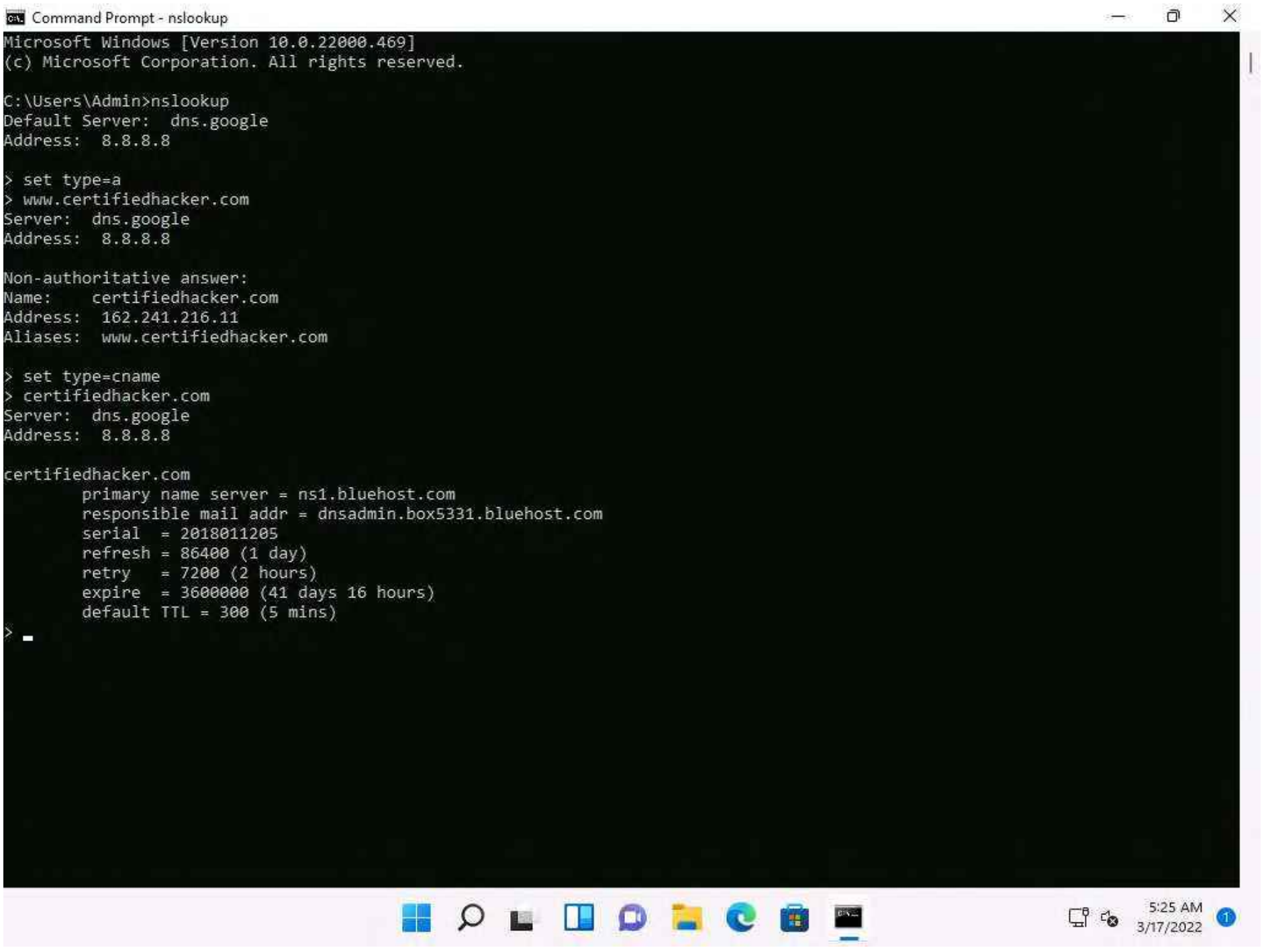
5. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**; it is considered to be a non-authoritative answer. Here, the IP address of the target domain **www.certifiedhacker.com** is **162.241.216.11**.

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

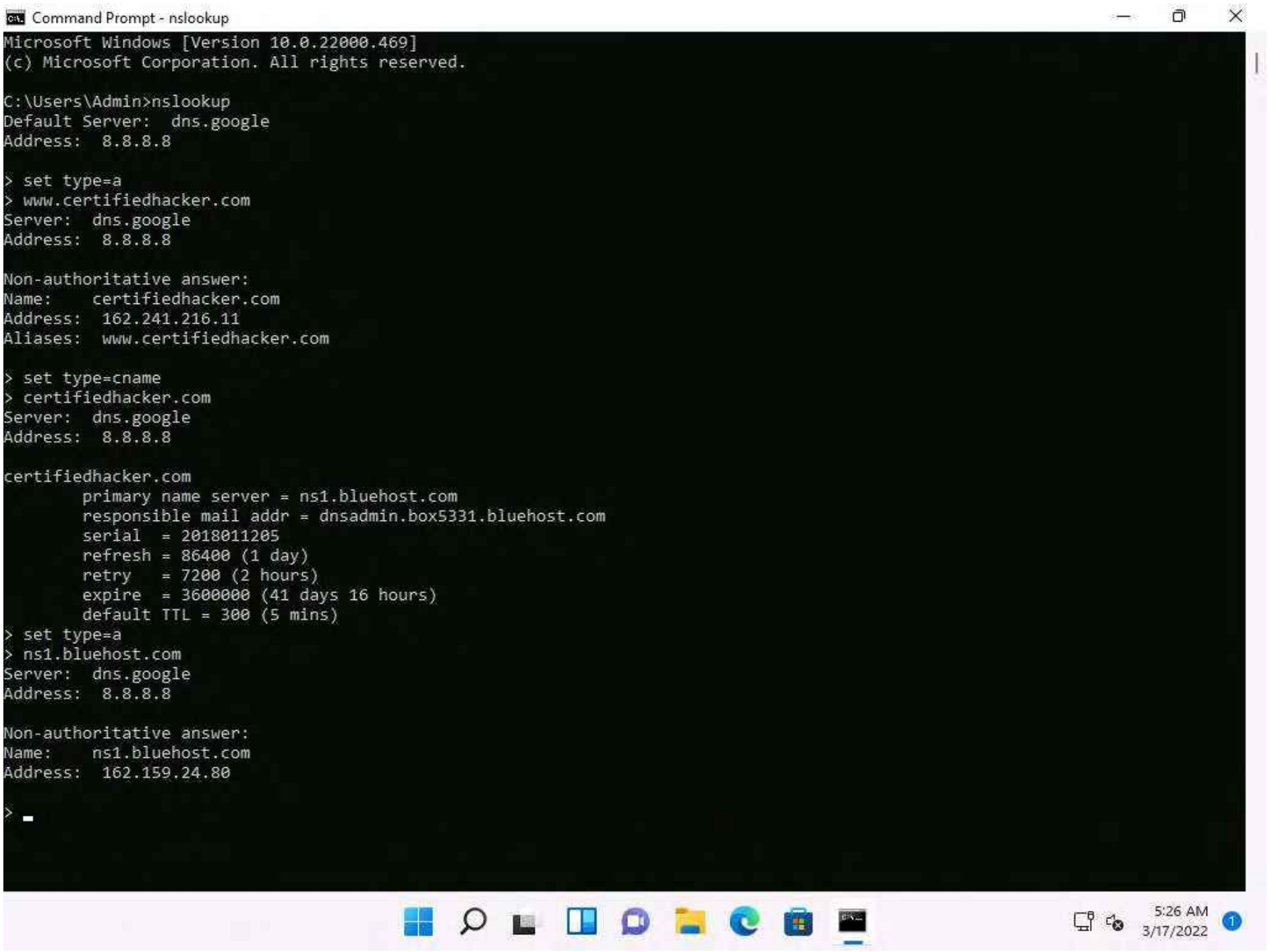
7. Type **set type=cname** and press **Enter**. The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.

8. Type **certifiedhacker.com** and press **Enter**.

9. 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.



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



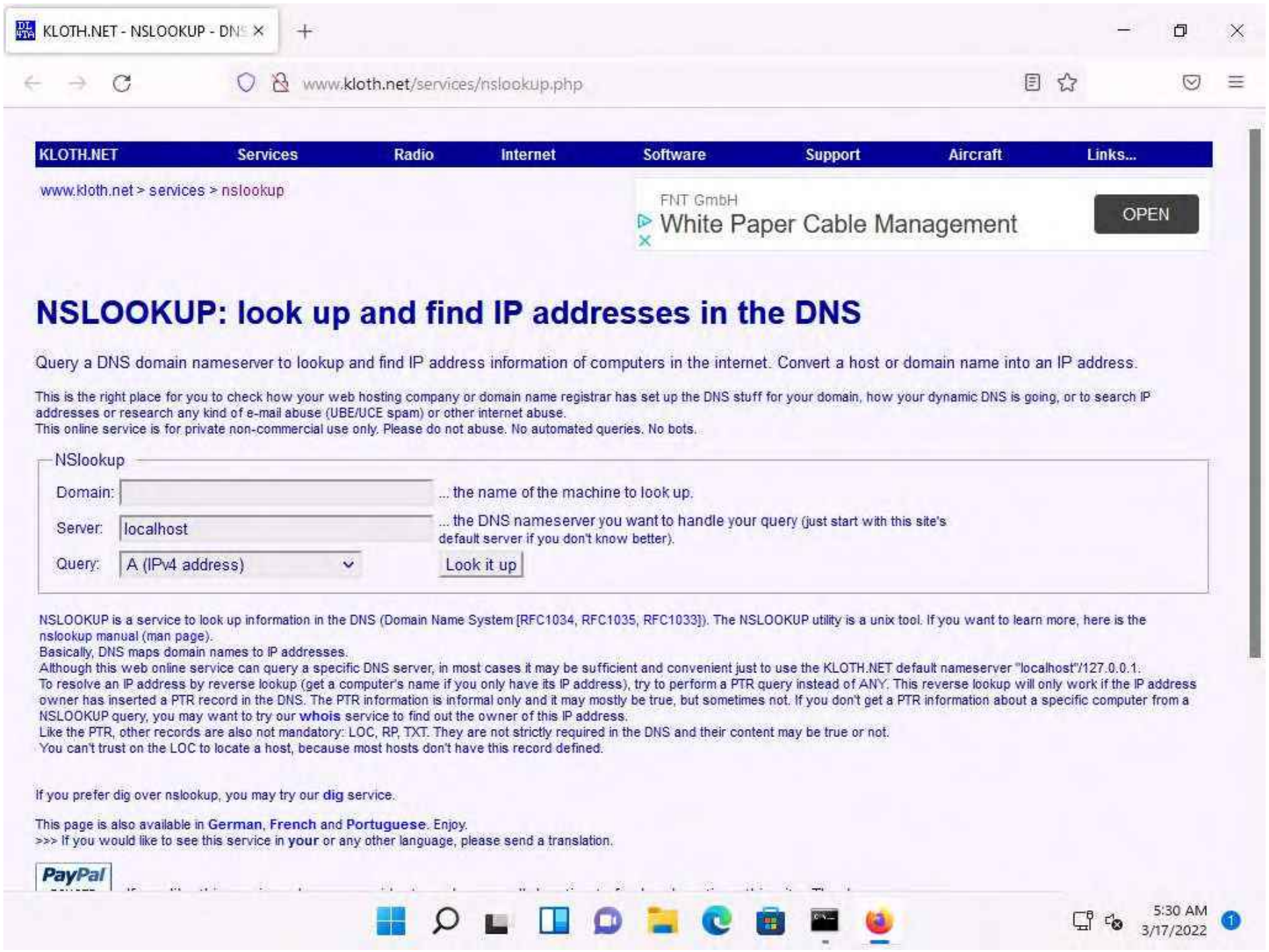
13. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.

14. 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.

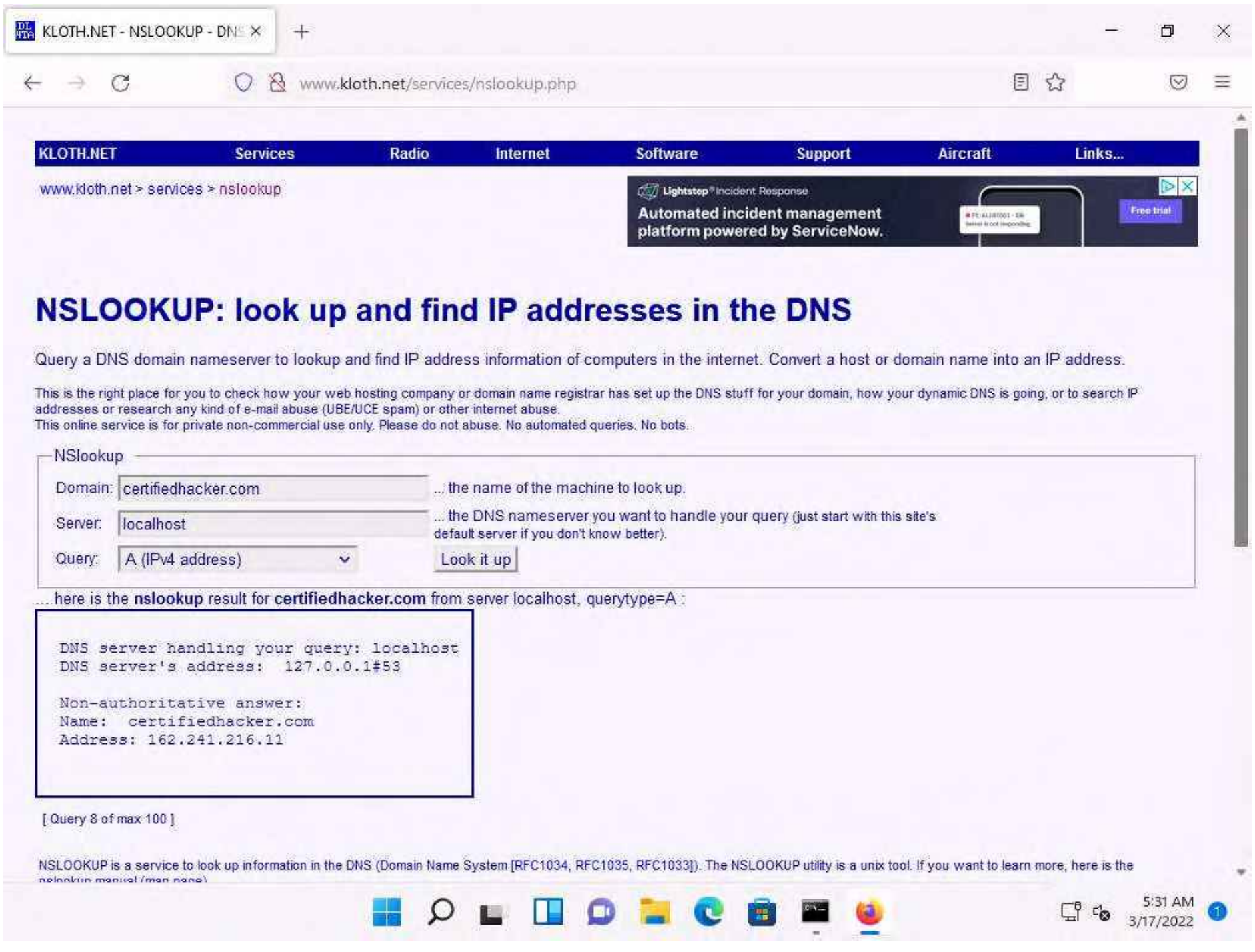
15. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.

16. 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**.

17. **NSLOOKUP** website appears, as shown in the screenshot.

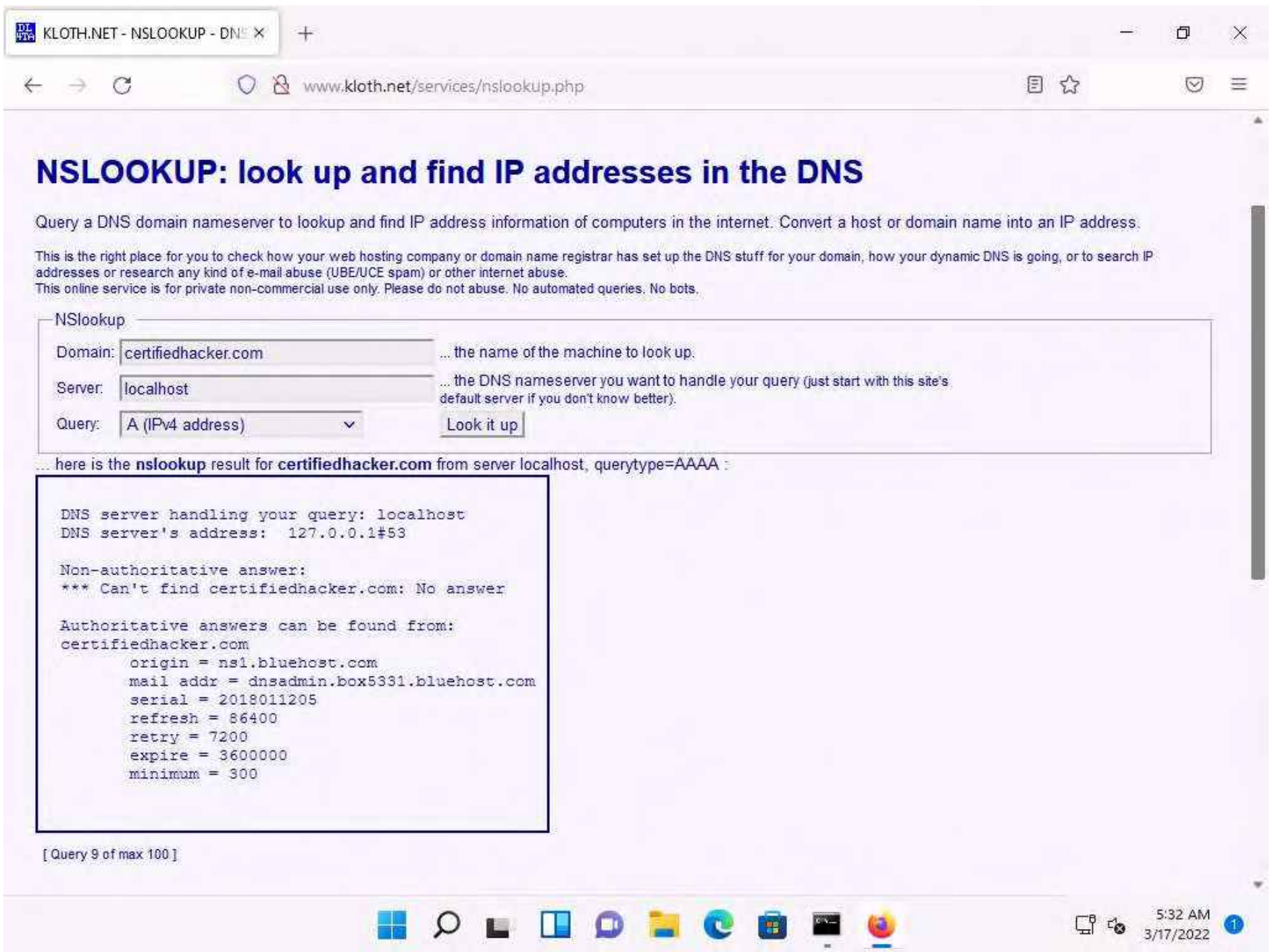


18. Once the site opens, in the **Domain:** field, enter **certifiedhacker.com**. Set the **Query:** field to default [**A (IPv4 address)**] and click the **Look it up** button to review the results that are displayed.



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

20. 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.



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

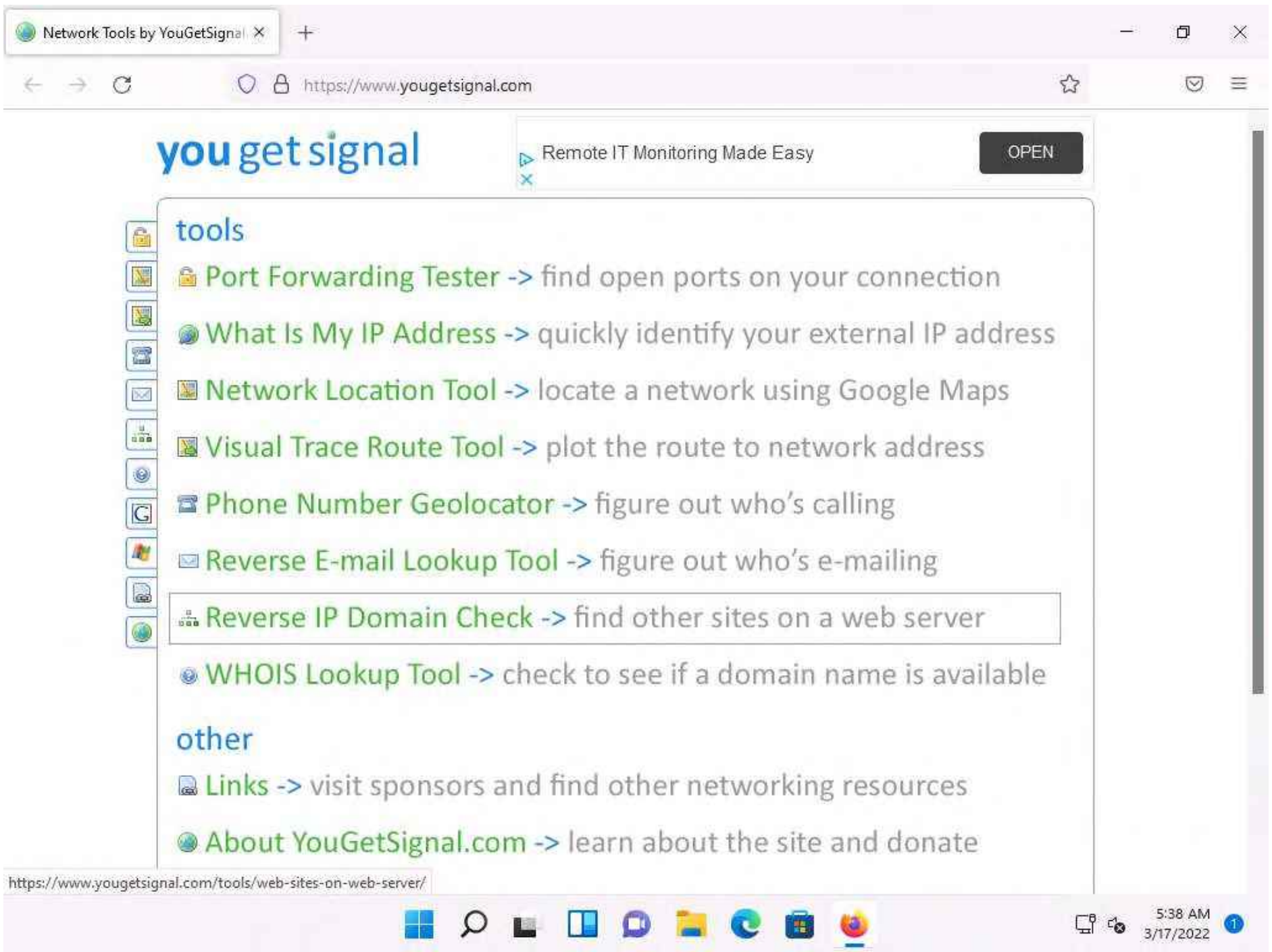
Task 2: Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

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

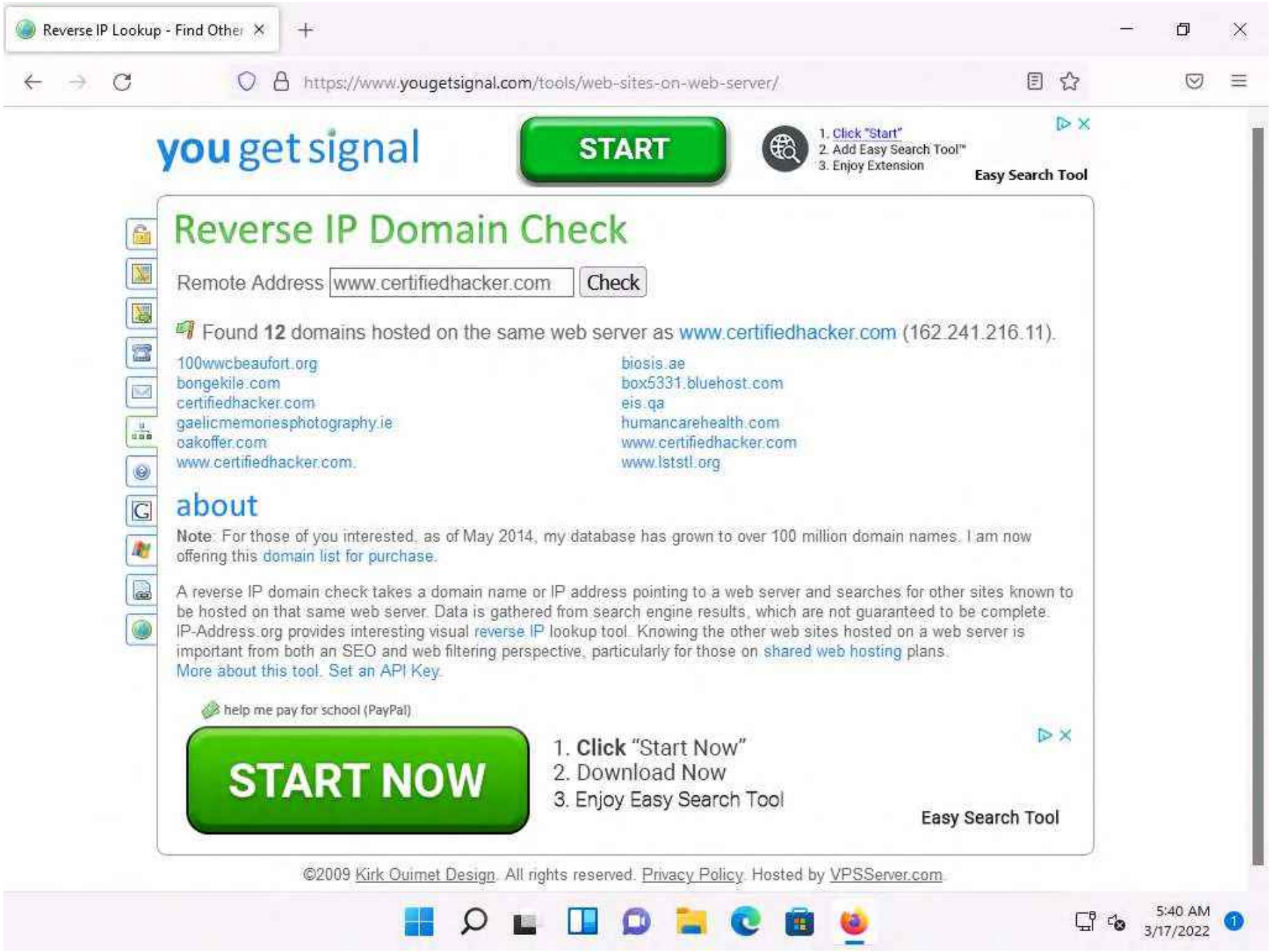
Here, we will perform reverse DNS lookup using you get signal's Reverse IP Domain Check tool to find the other domains/sites that share the same web server as our target server.

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

1. 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**.

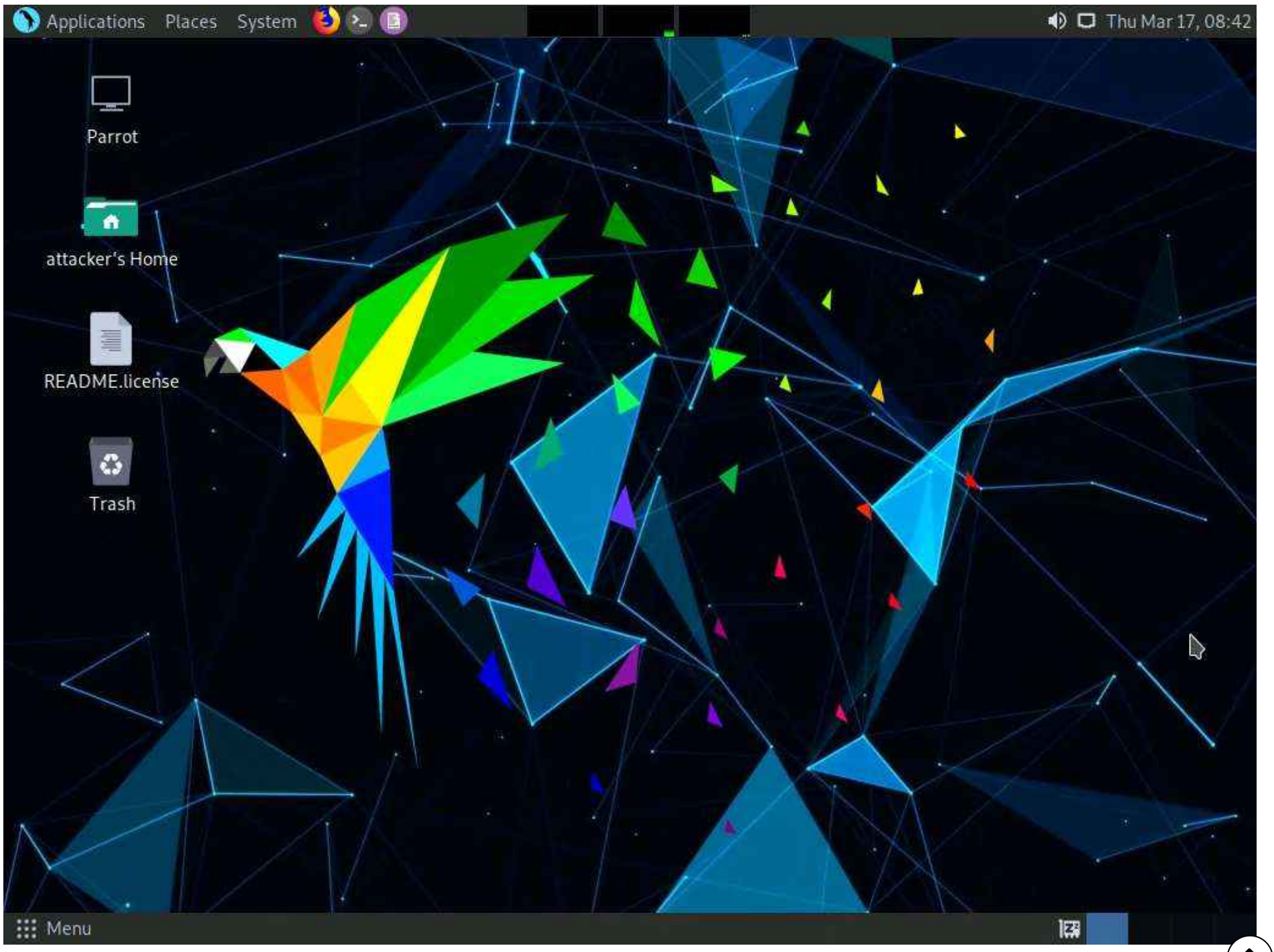


3. On the **Reverse IP Domain Check** page, enter **www.certifiedhacker.com** in the **Remote Address** field and click **Check** to find other domains/sites hosted on a certifiedhacker.com web server. You will get the list of domains/sites hosted on the same server as **www.certifiedhacker.com**, as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



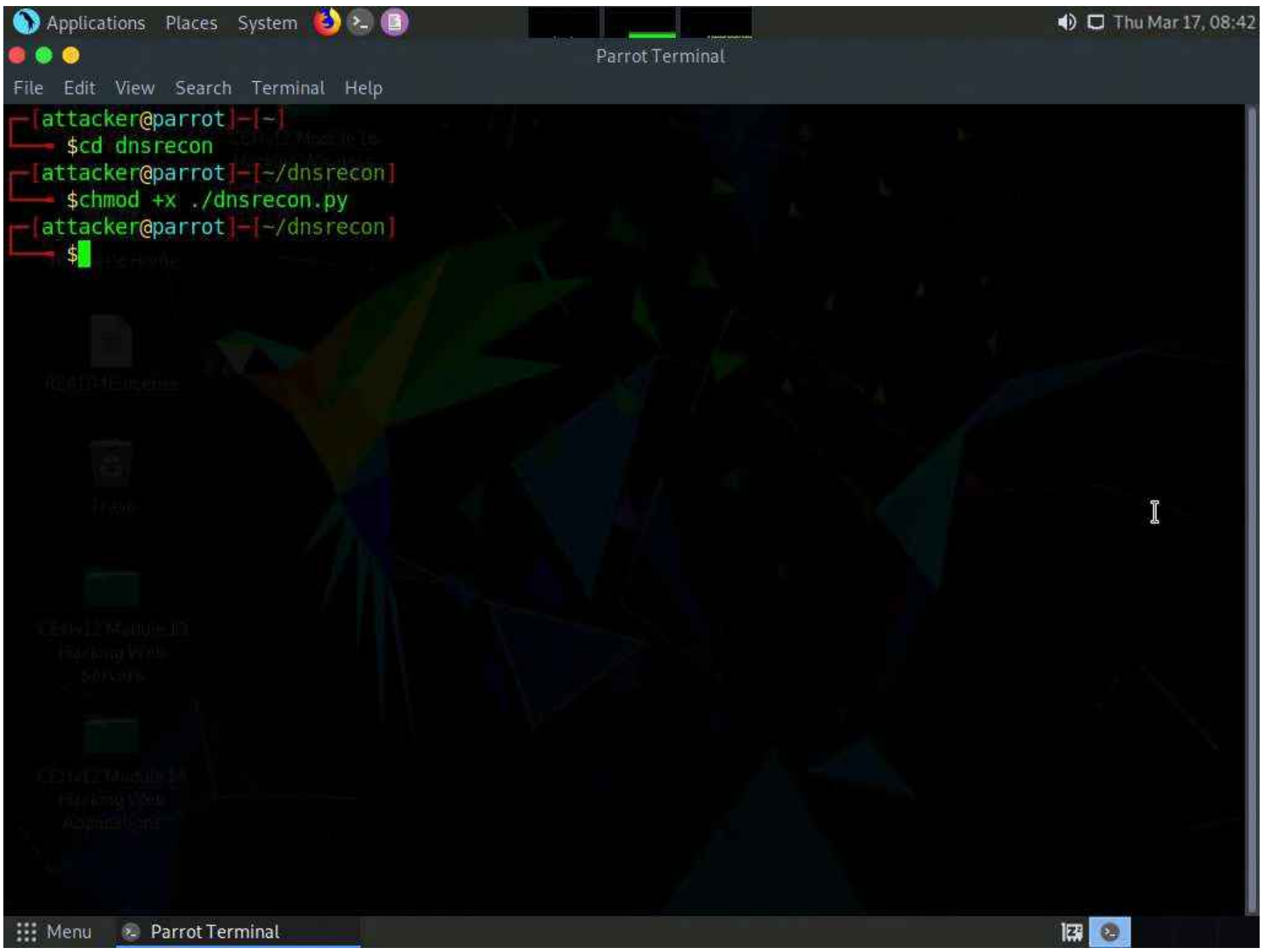
4. Now, click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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



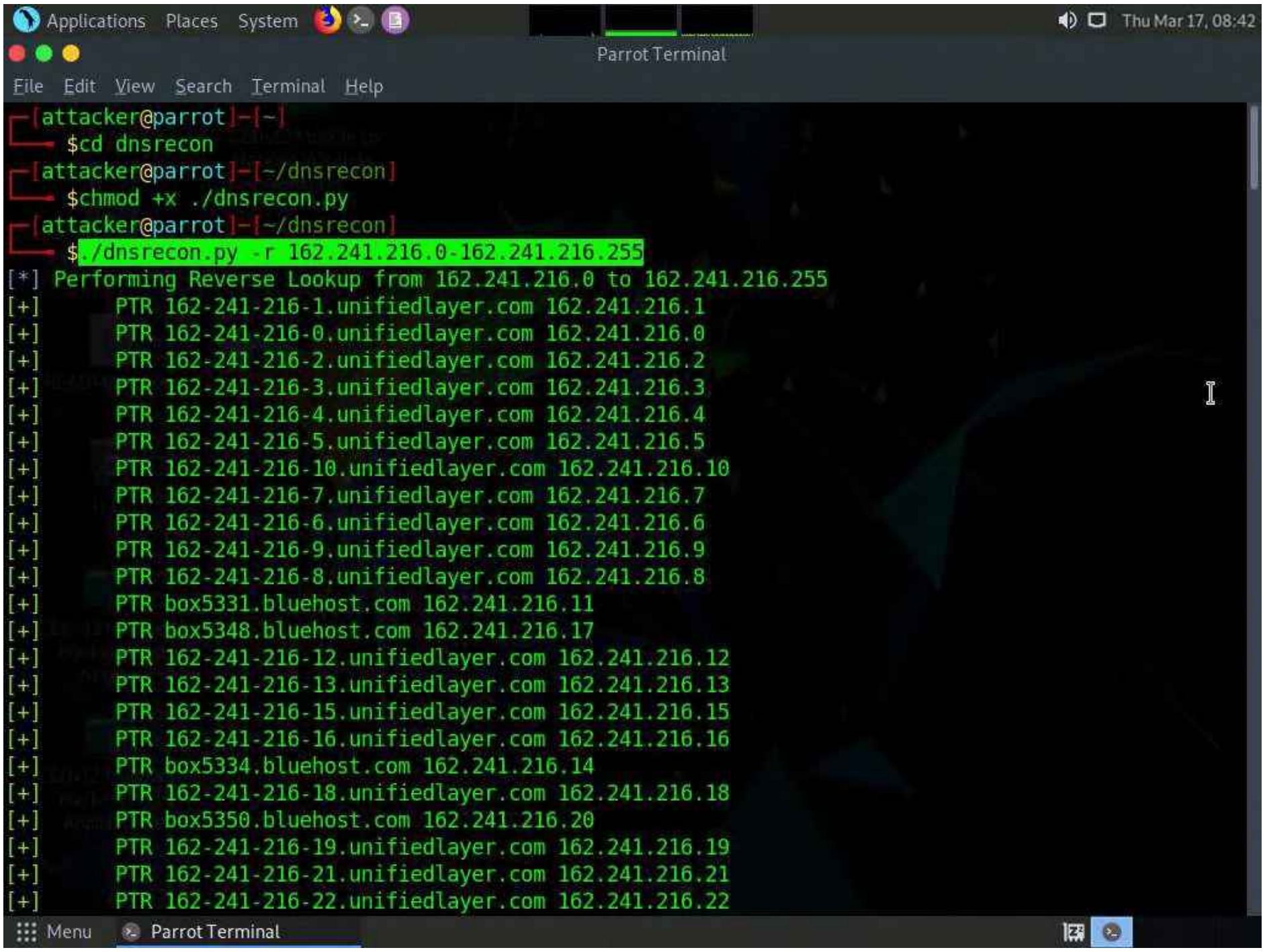
6. In the **Parrot Terminal** window, type **cd dnsrecon** and press **Enter** to enter into dnsrecon directory.

7. Type **chmod +x ./dnsrecon.py** and press **Enter**.



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.



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.

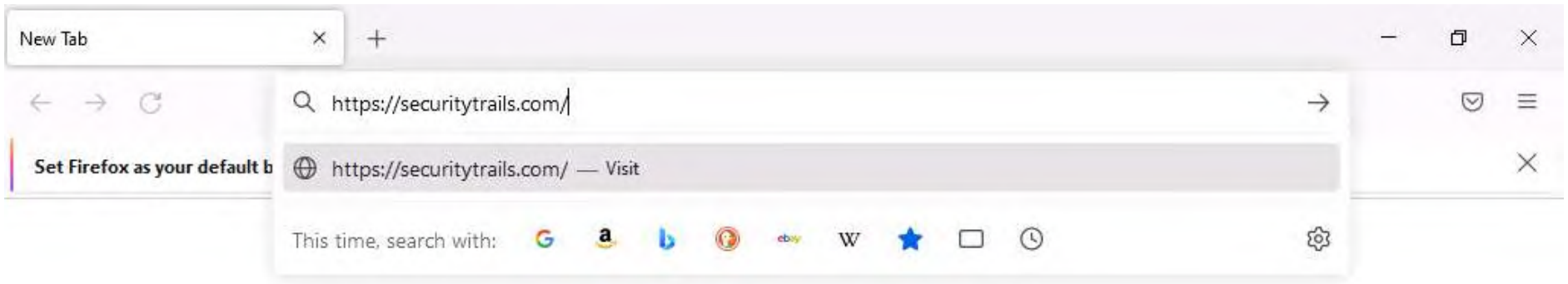
Task 3: Gather Information of Subdomain and DNS Records using SecurityTrails

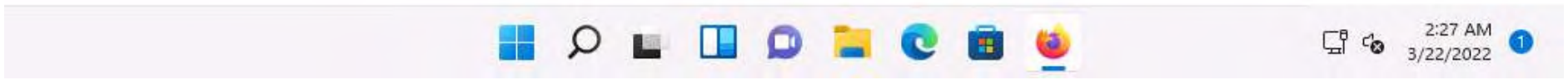
SecurityTrails is an advanced DNS enumeration tool that is capable of creating a DNS map of the target domain network. It can enumerate both current and historical DNS records such as A, AAAA, NS, MX, SOA, and TXT, which helps in building the DNS structure. It also enumerates all the existing subdomains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

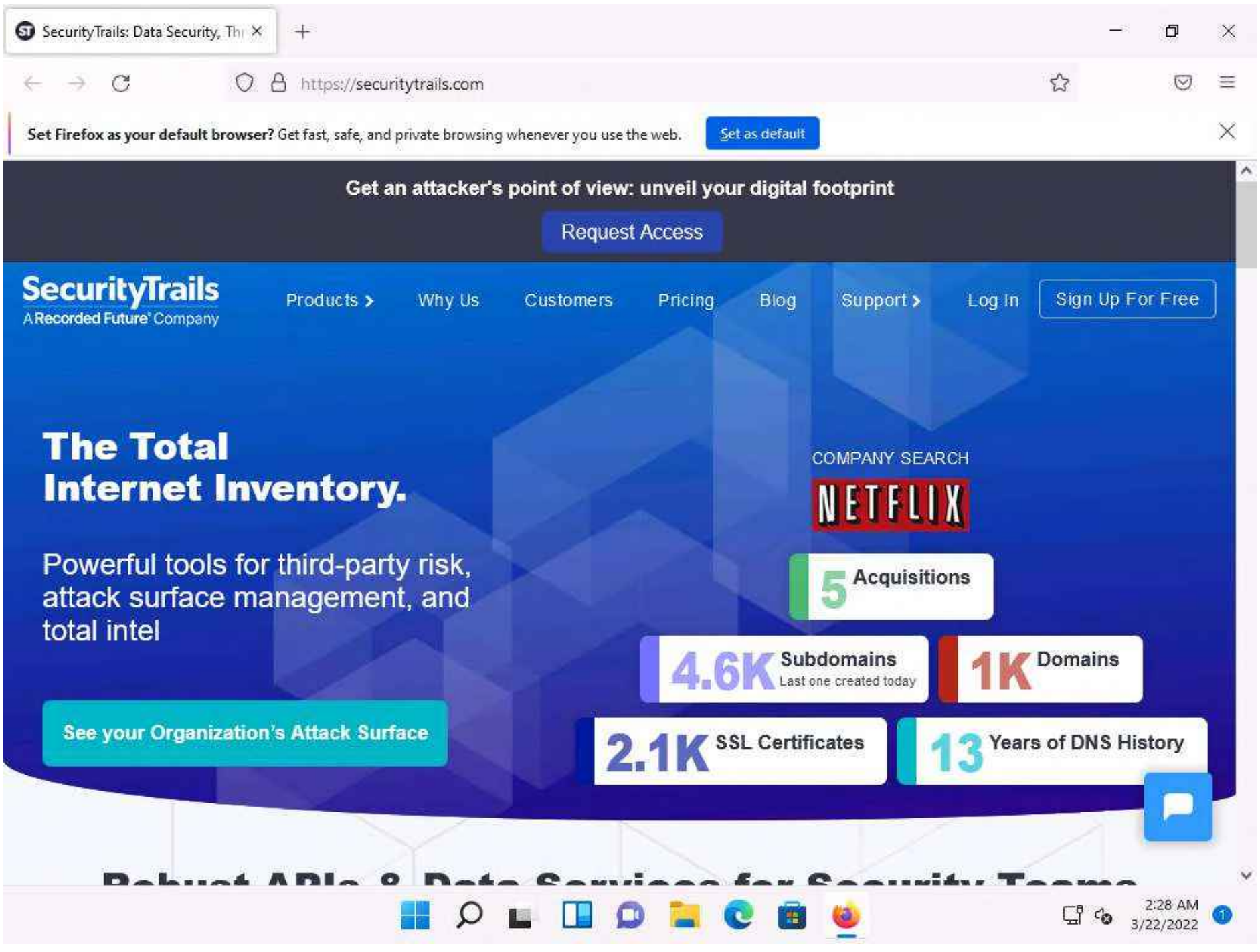
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

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**.

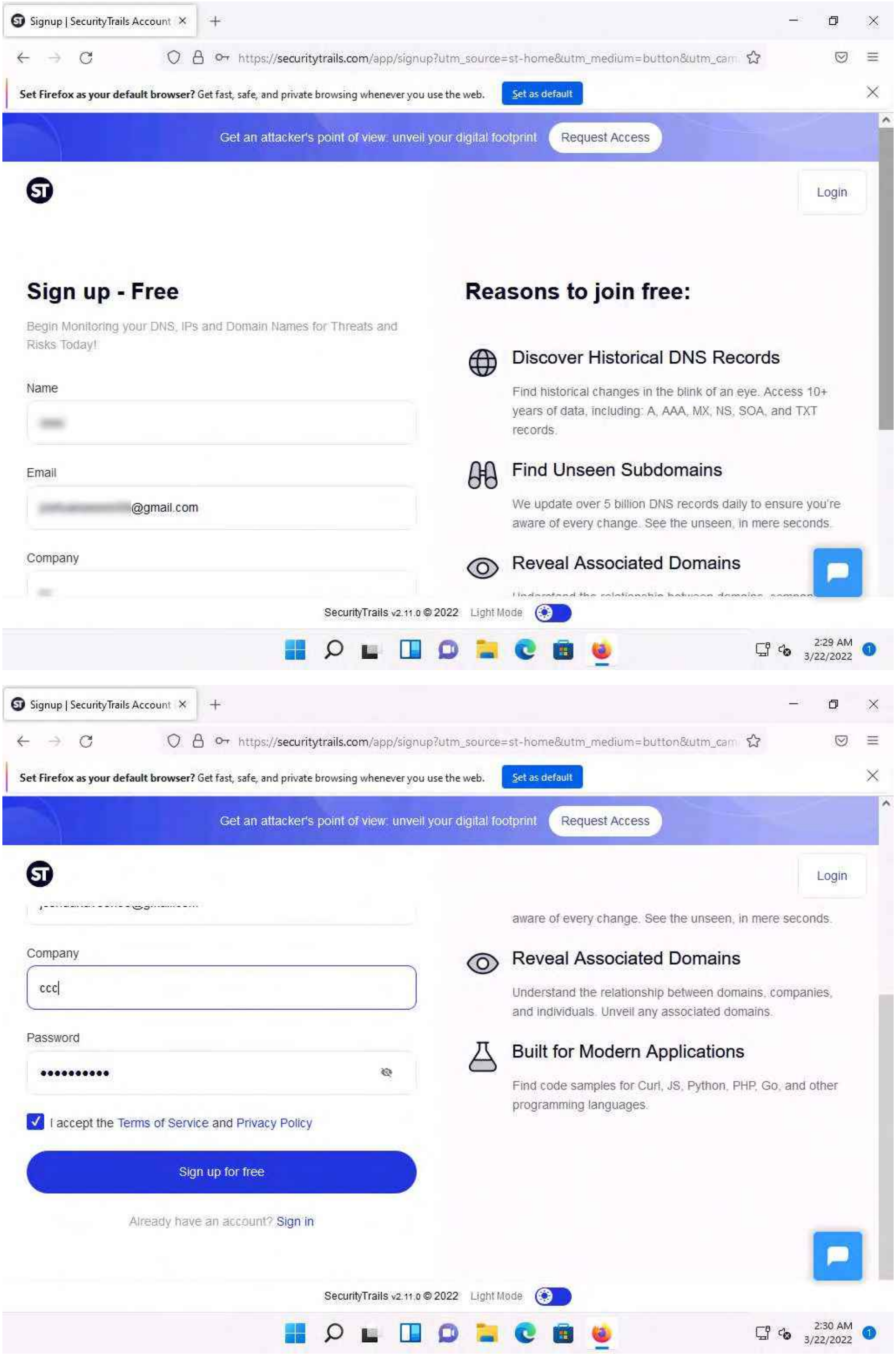




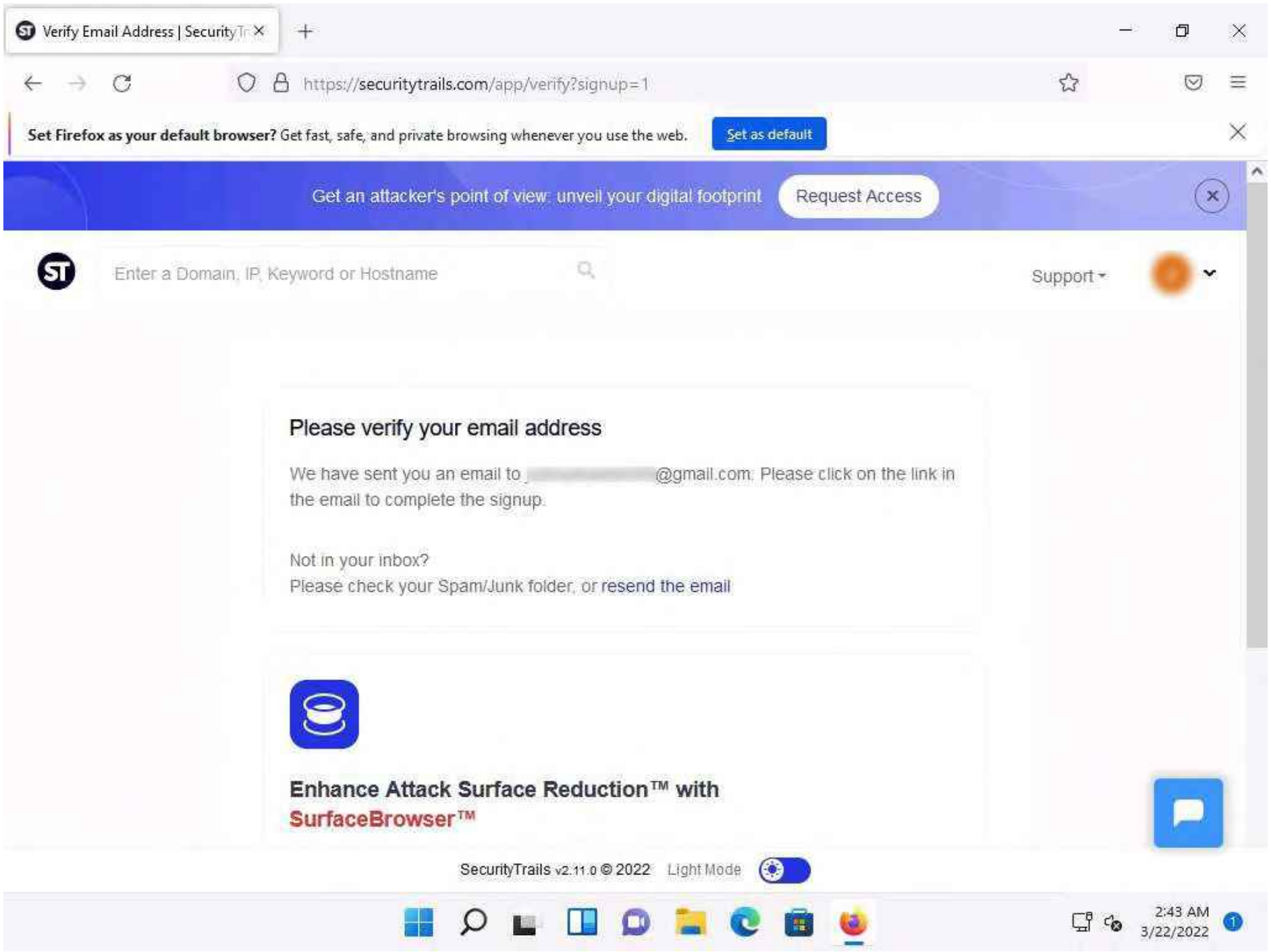
3. **SecurityTrails** website appears, In the website click on **Sign Up For Free** button at the top right corner of the page.



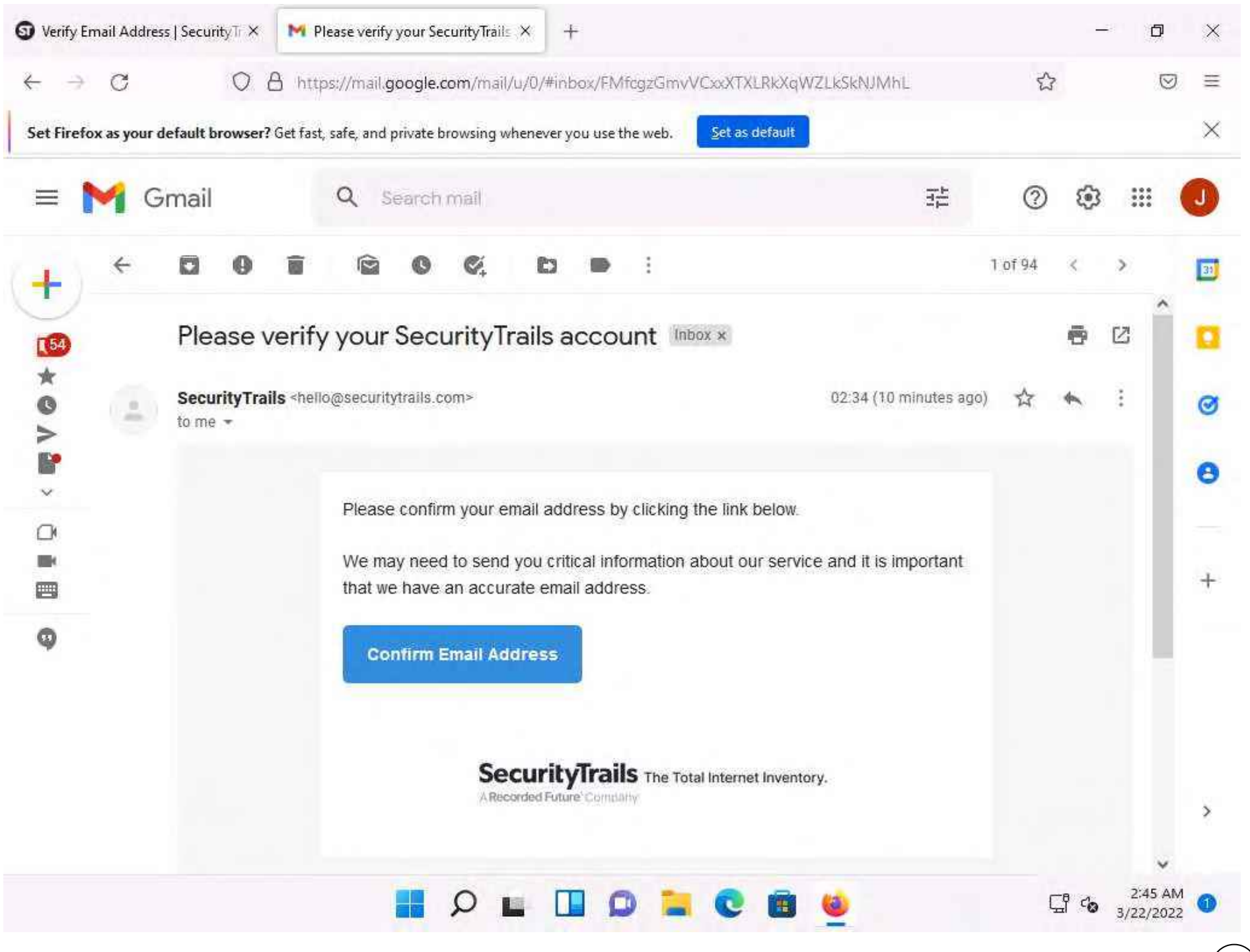
4. **Sign up-Free** page appears, enter the required details and check the terms and conditions check box. Click **Sign up for free**.



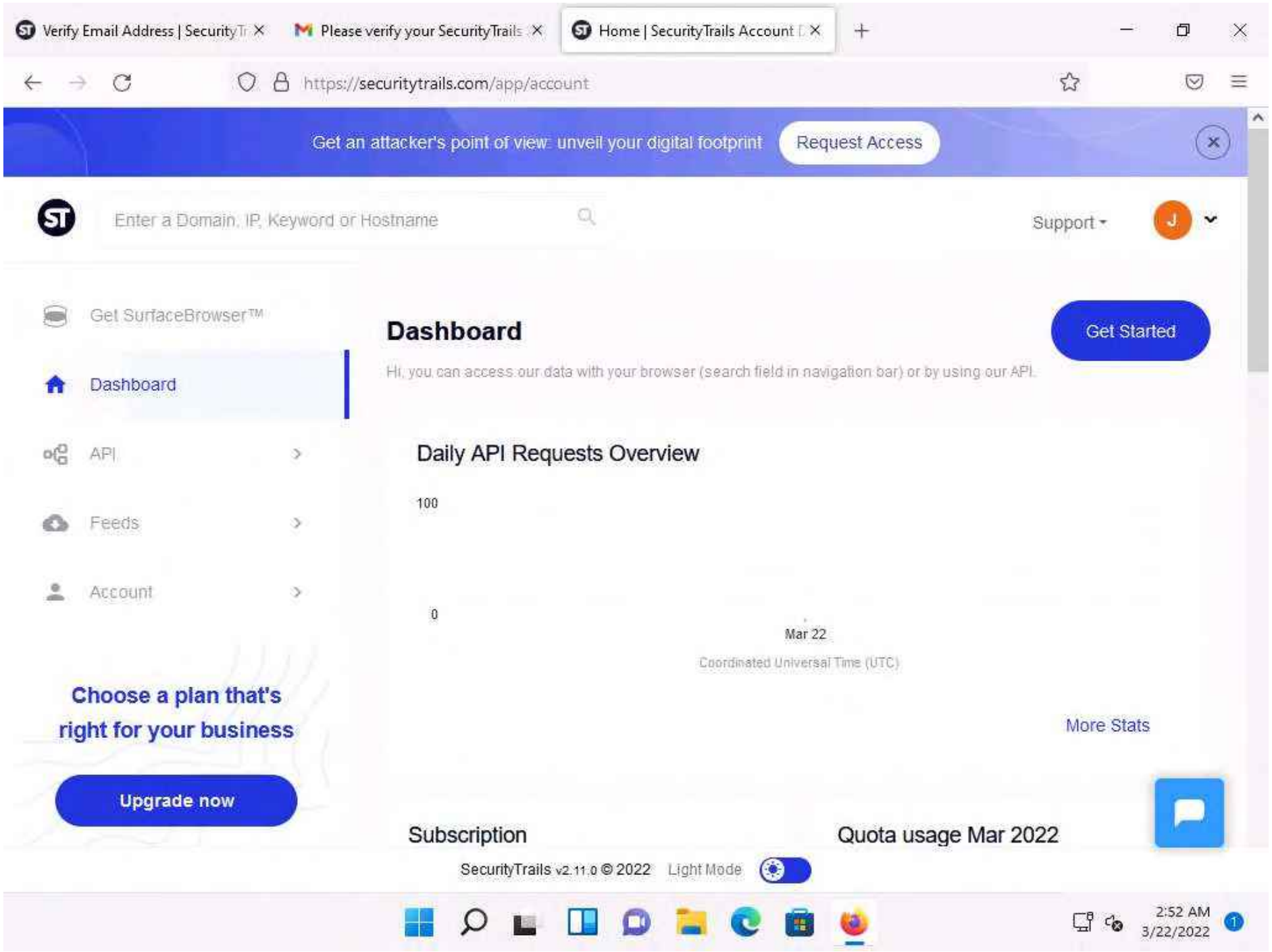
5. A verification email will be sent to the email address.



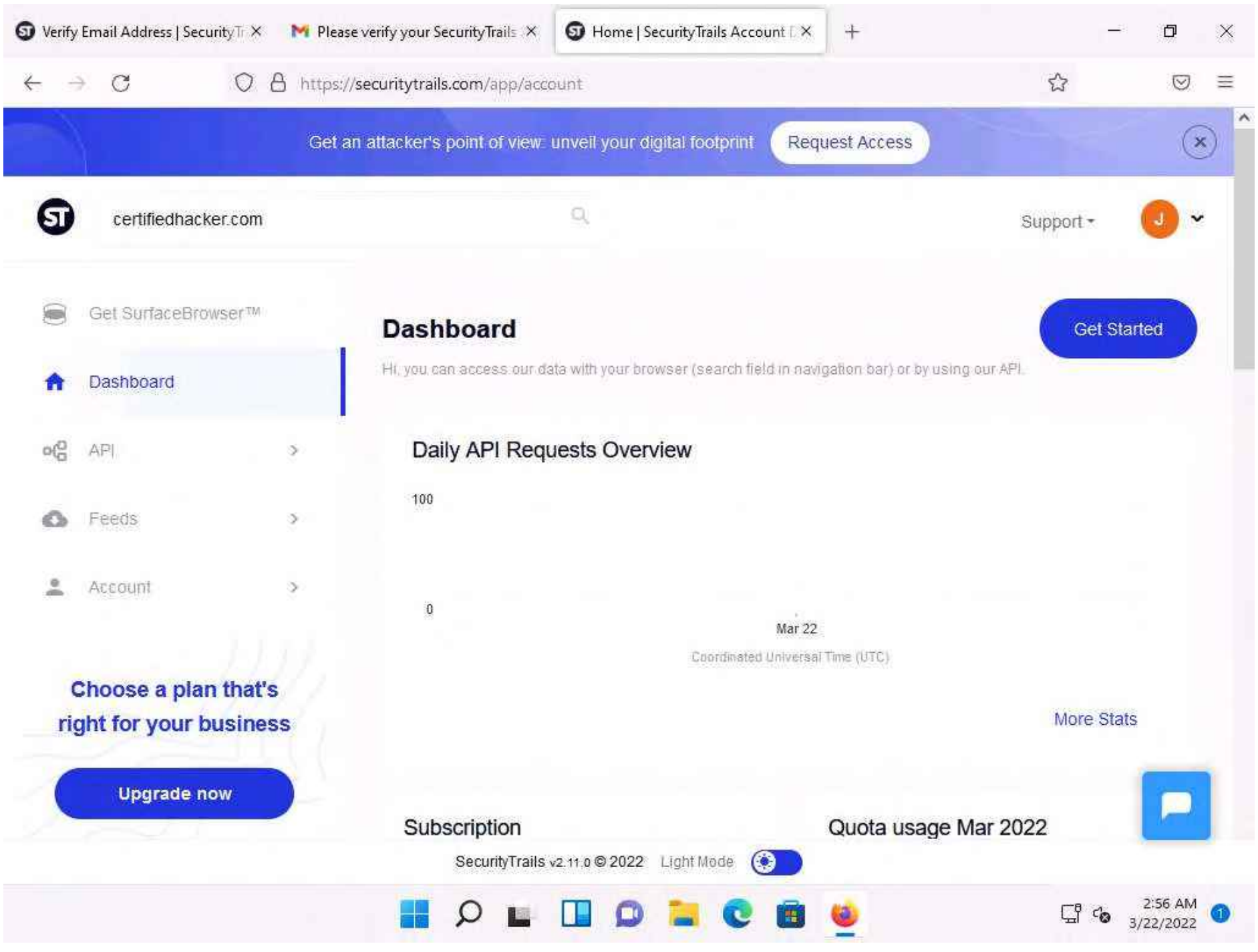
6. Open a new tab in the browser and login to the email account provided during sign up. Open the mail received from SecurityTrails and click on **Confirm Email Address**.



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



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



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.

Verify Email Address | SecurityTr ✕ | Please verify your SecurityTrails ✕ | certifiedhacker.com - Current D ✕

https://securitytrails.com/domain/certifiedhacker.com/dns

SecurityTrails
A Recorded Future Company

certifiedhacker.com

DOMAIN

DNS Records

Historical Data

Subdomains 89

certifiedhacker.com DNS records as of Mar 22, 2022

A records

Unified Layer

162.241.216.11 35,942

AAAA records

NO RECORDS

MX records

3:00 AM
3/22/2022

Verify Email Address | SecurityTr ✕ | Please verify your SecurityTrails ✕ | certifiedhacker.com - Current D ✕

https://securitytrails.com/domain/certifiedhacker.com/dns

Get an attacker's point of view: unveil your digital footprint Request Access

SecurityTrails
A Recorded Future Company

certifiedhacker.com

DOMAIN

MX records

Unified Layer

0 mail.certifiedhacker.com 1

DNS Records

Historical Data

Subdomains 89

NS records

Cloudflare, Inc.

ns2.bluehost.com 2,069,456

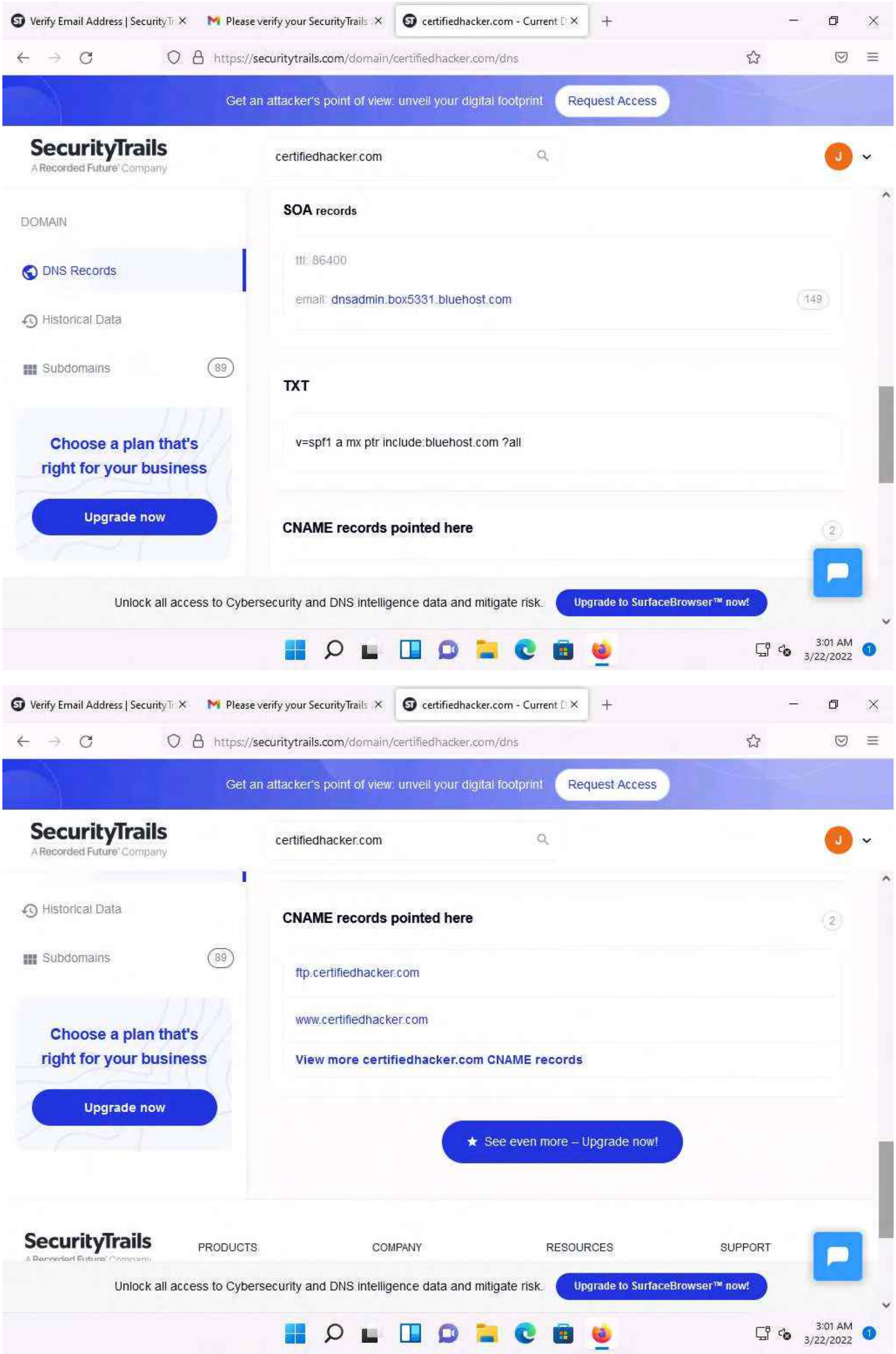
ns1.bluehost.com 2,069,544

Choose a plan that's right for your business

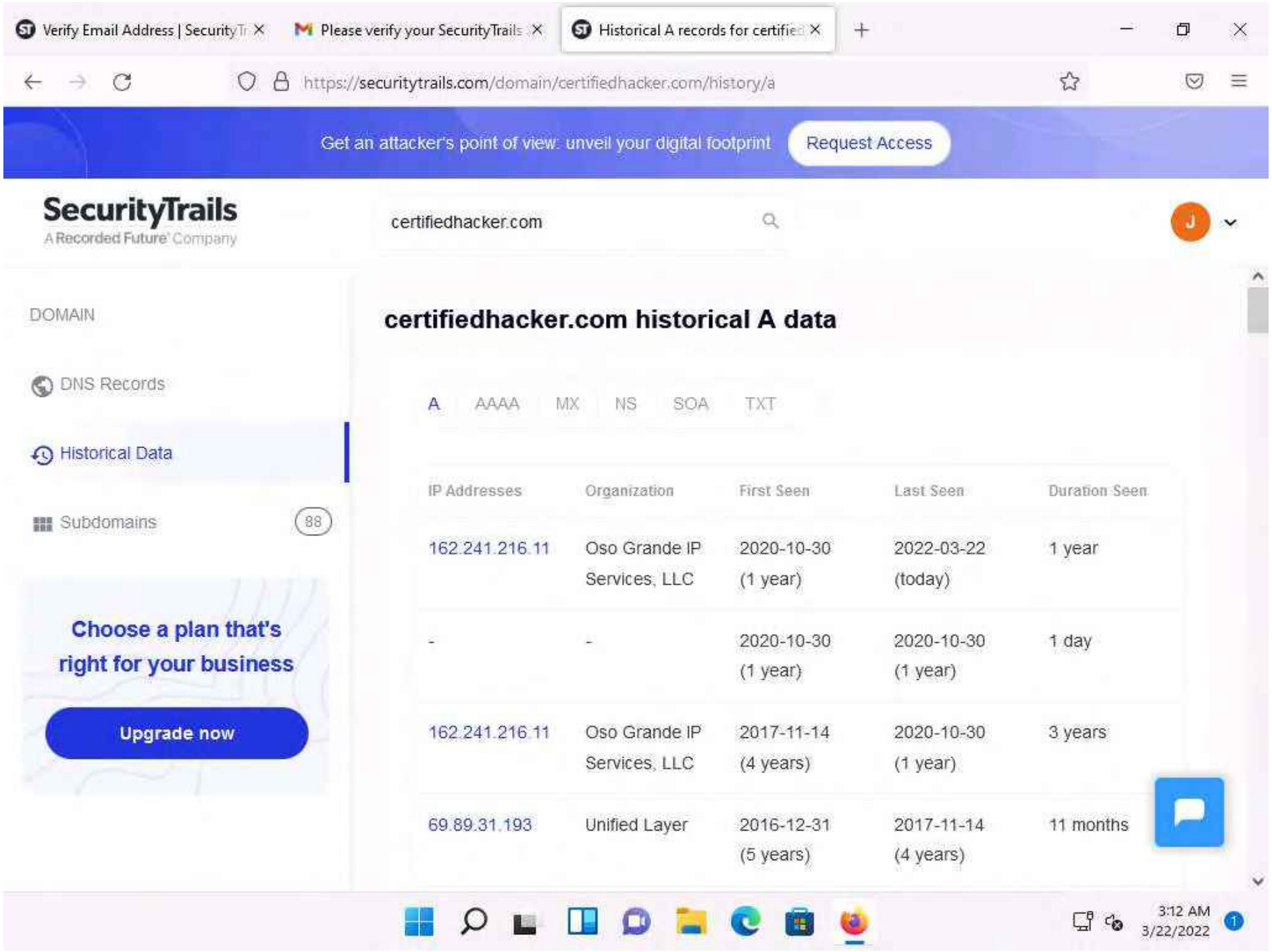
Upgrade now

Unlock all access to Cybersecurity and DNS intelligence data and mitigate risk. Upgrade to SurfaceBrowser™ now!

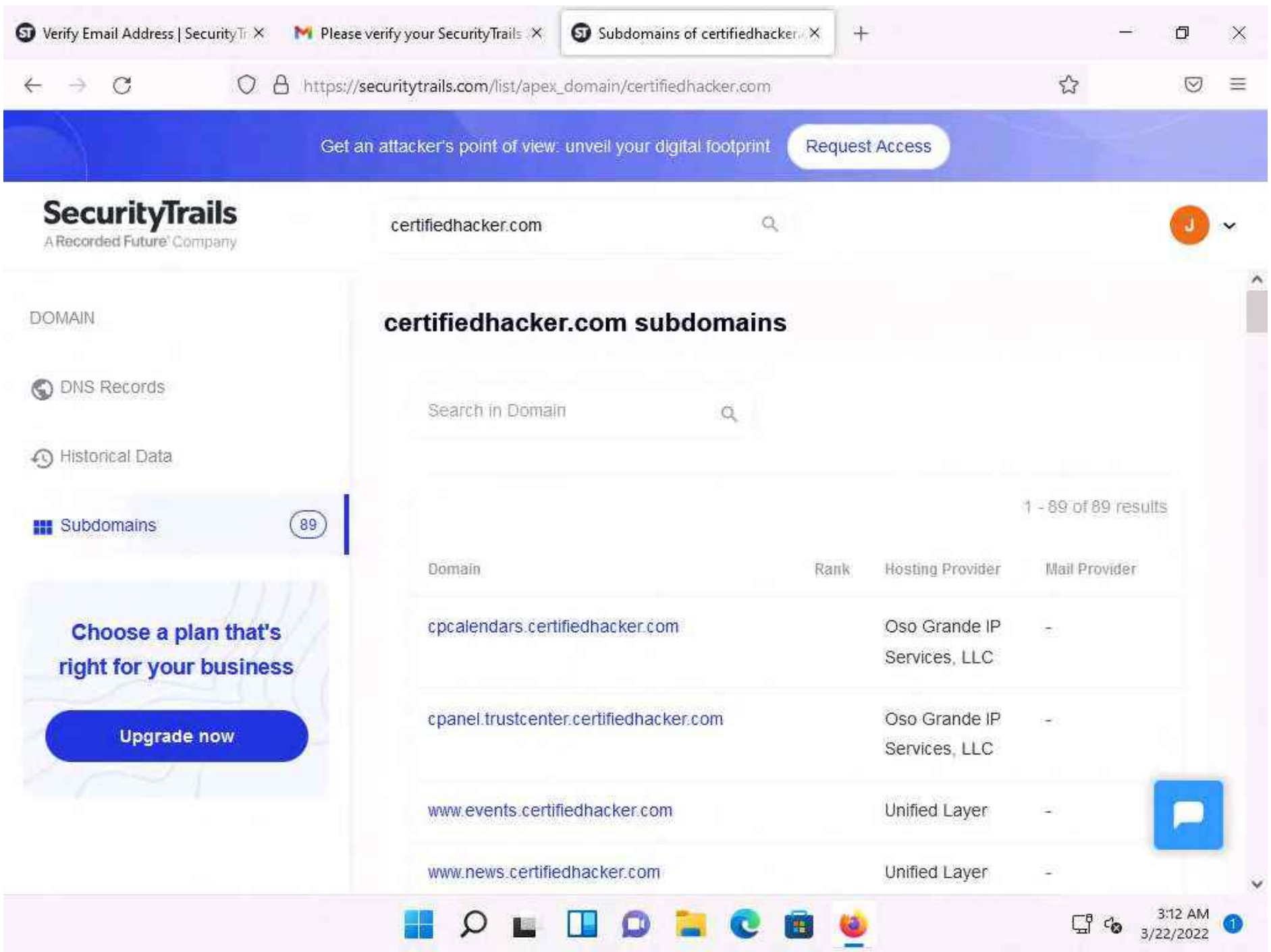
3:01 AM
3/22/2022



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.



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



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.

Lab 8: Perform Network Footprinting

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

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.

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.

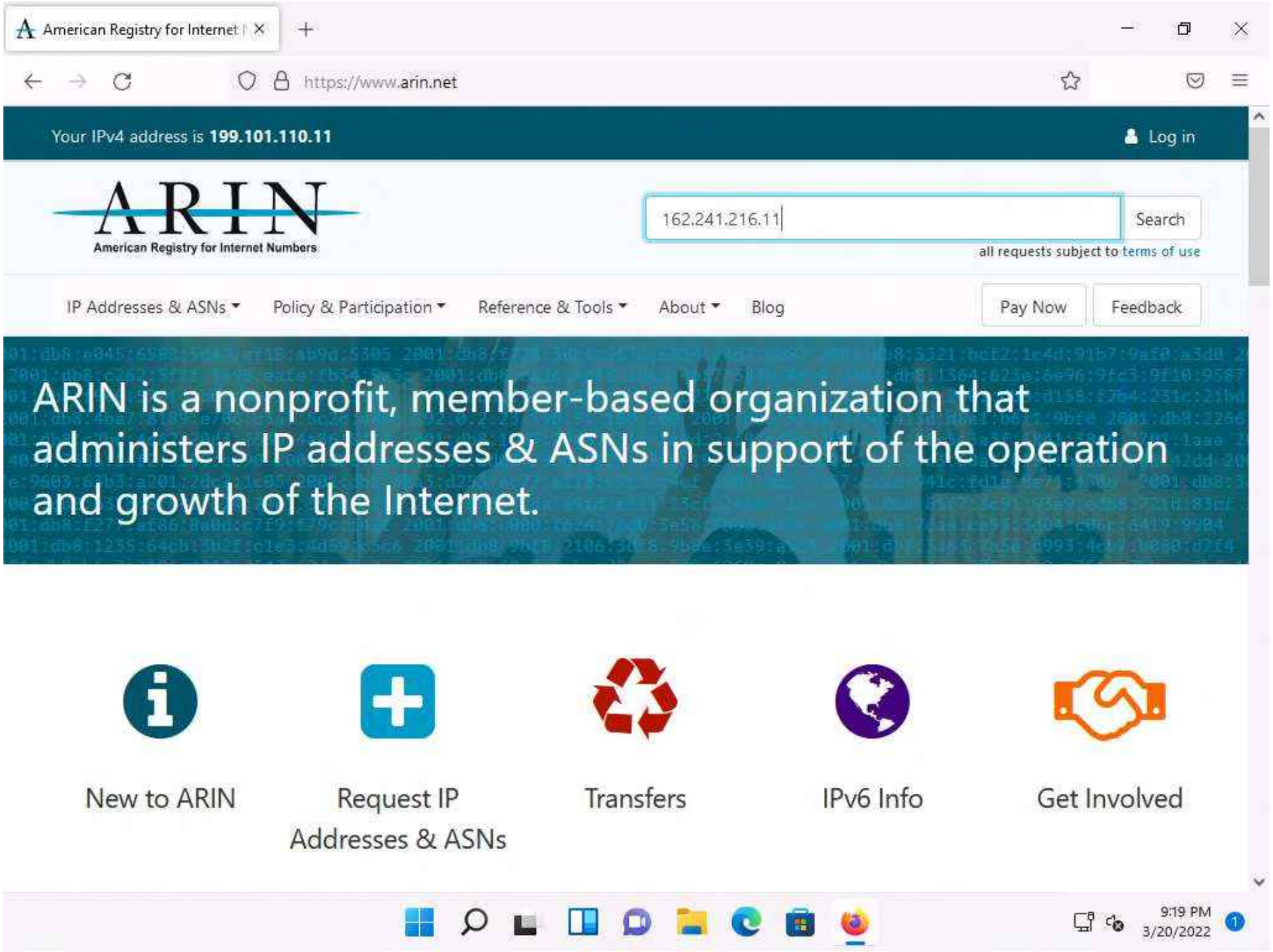
Here, we will locate the network range using the ARIN Whois database search tool.

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

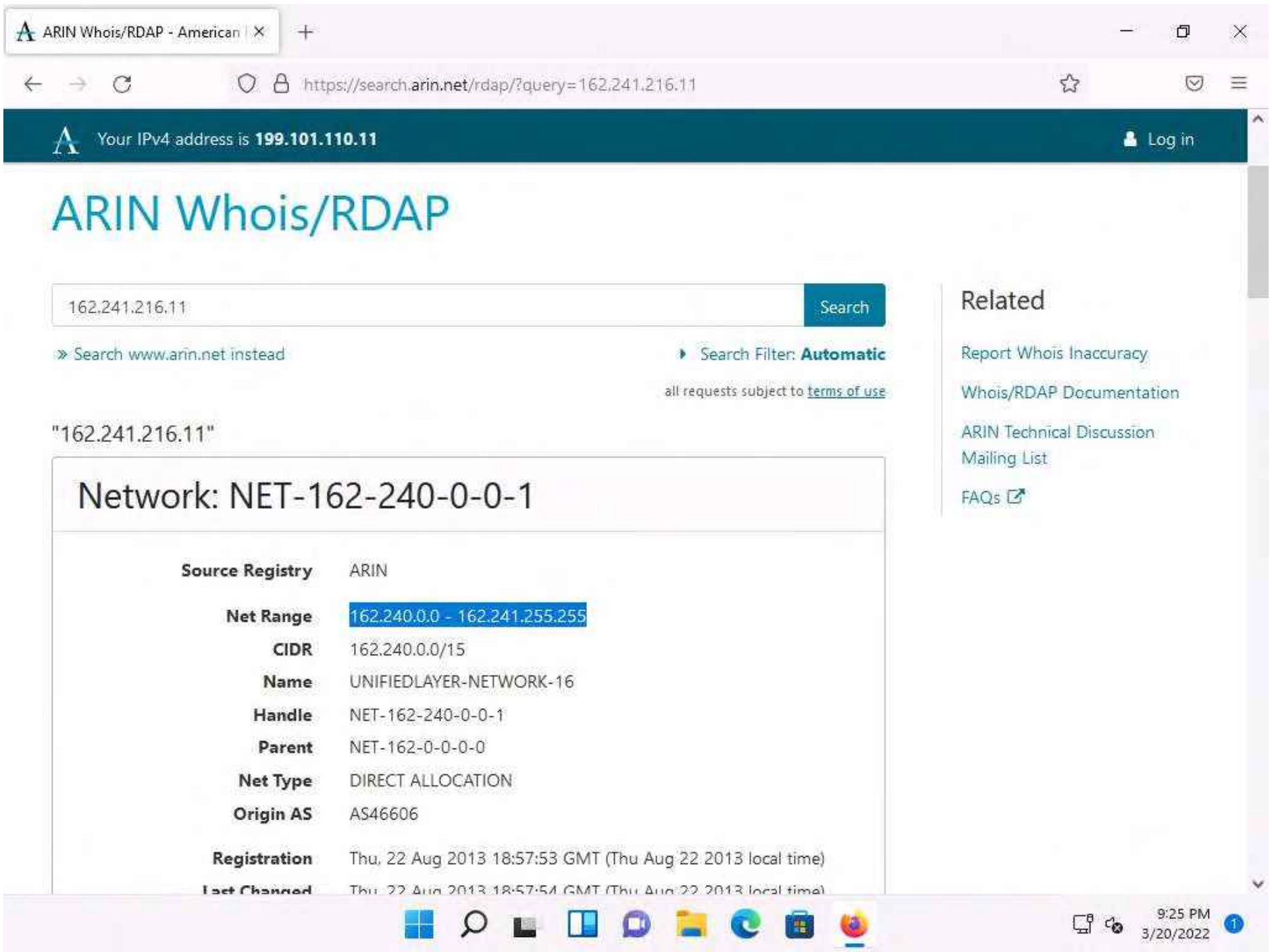
1. In the **Windows 11** machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://www.arin.net/about/welcome/region** and press **Enter**.

   > Note: If **More secure, encrypted DNS lookups** notification appears at the top section of browser, click **Disable**.

2. 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.



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



4. This concludes the demonstration of locating network range using the ARIN Whois database search tool.

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

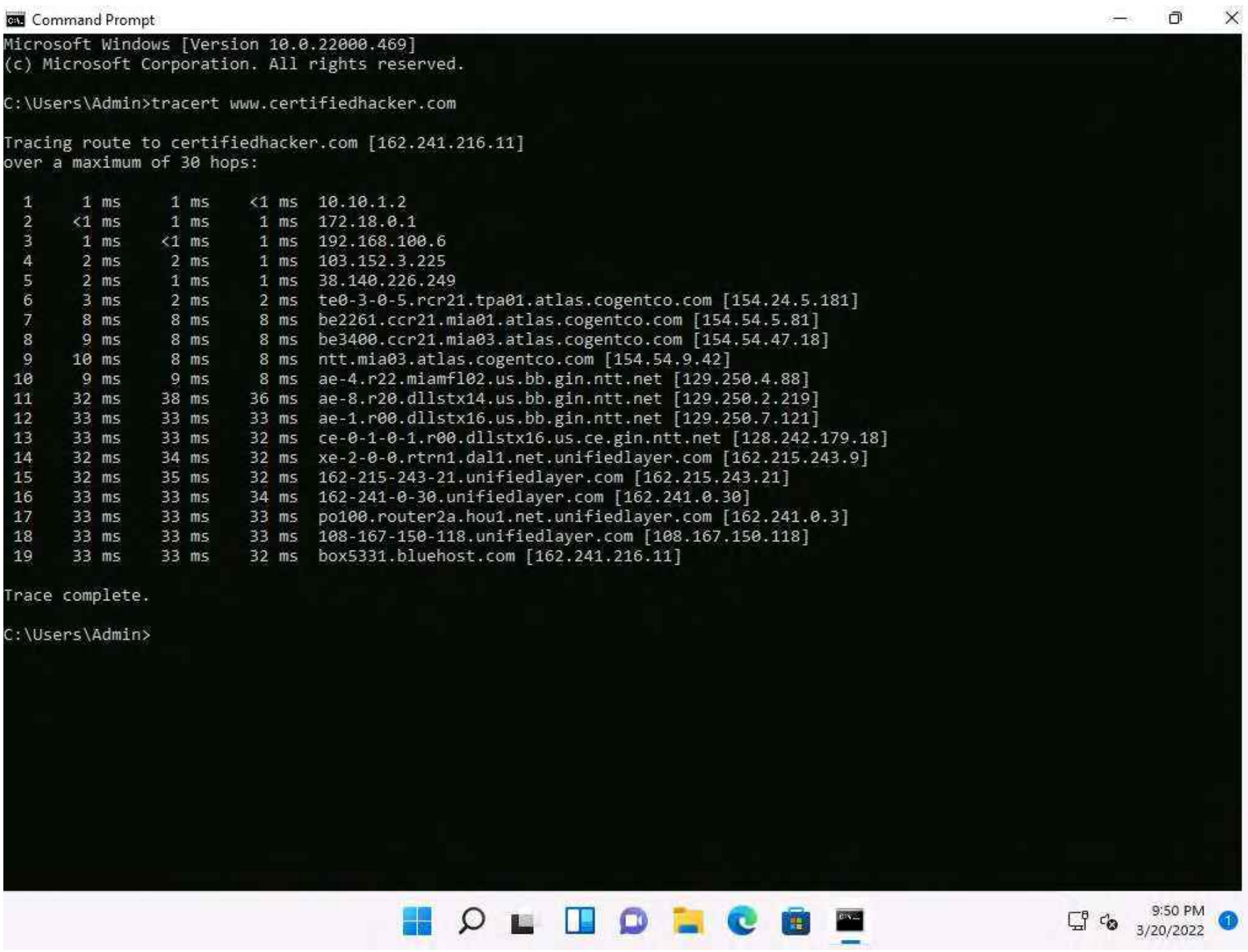
Task 2: Perform Network Tracerouting in Windows and Linux Machines

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** as a target website. However, you can select a target domain of your choice.

1. In the **Windows 11** 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.

```
Command Prompt
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.

C:\Users\Admin>
```

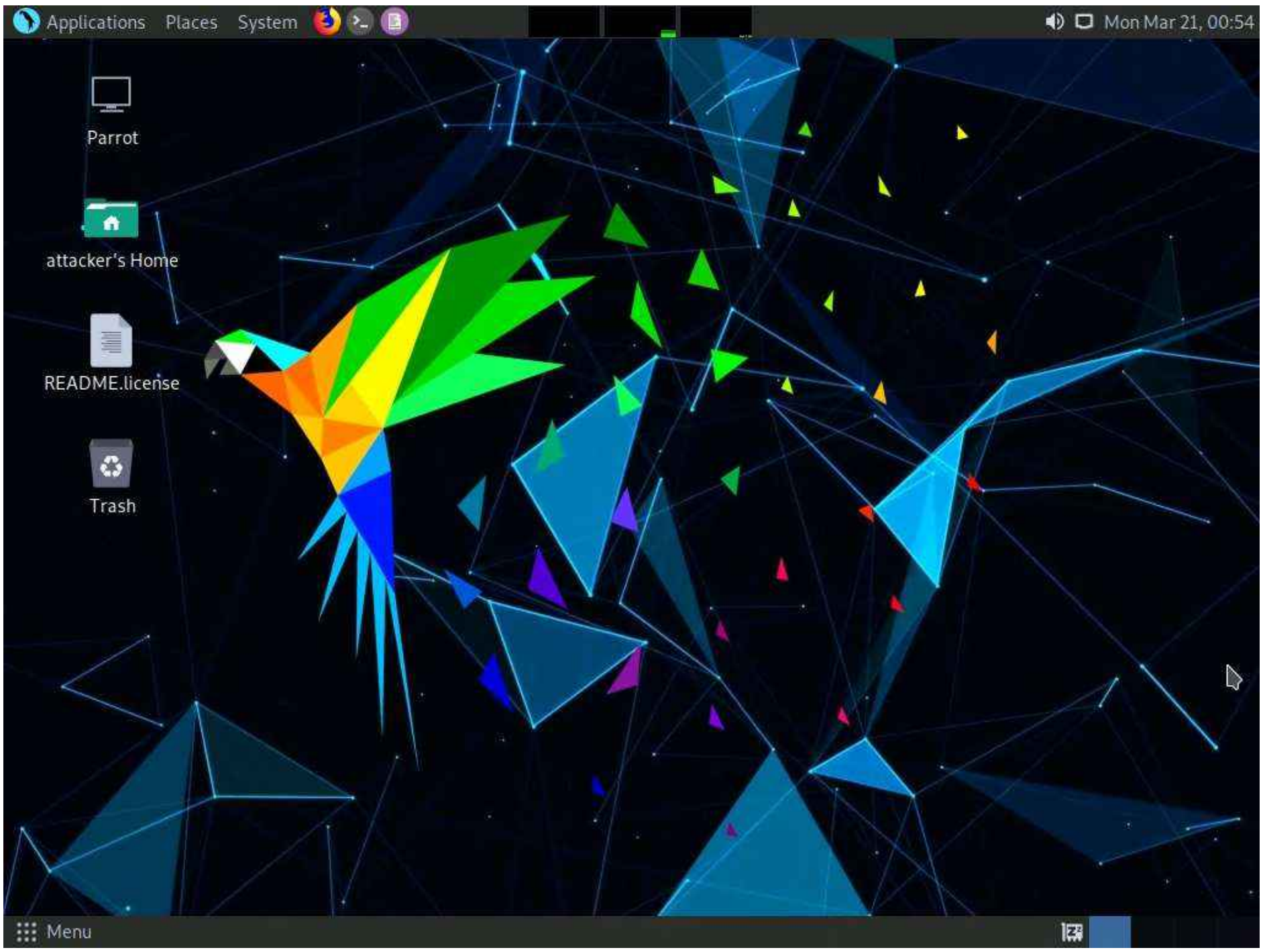
3. Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

```
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.

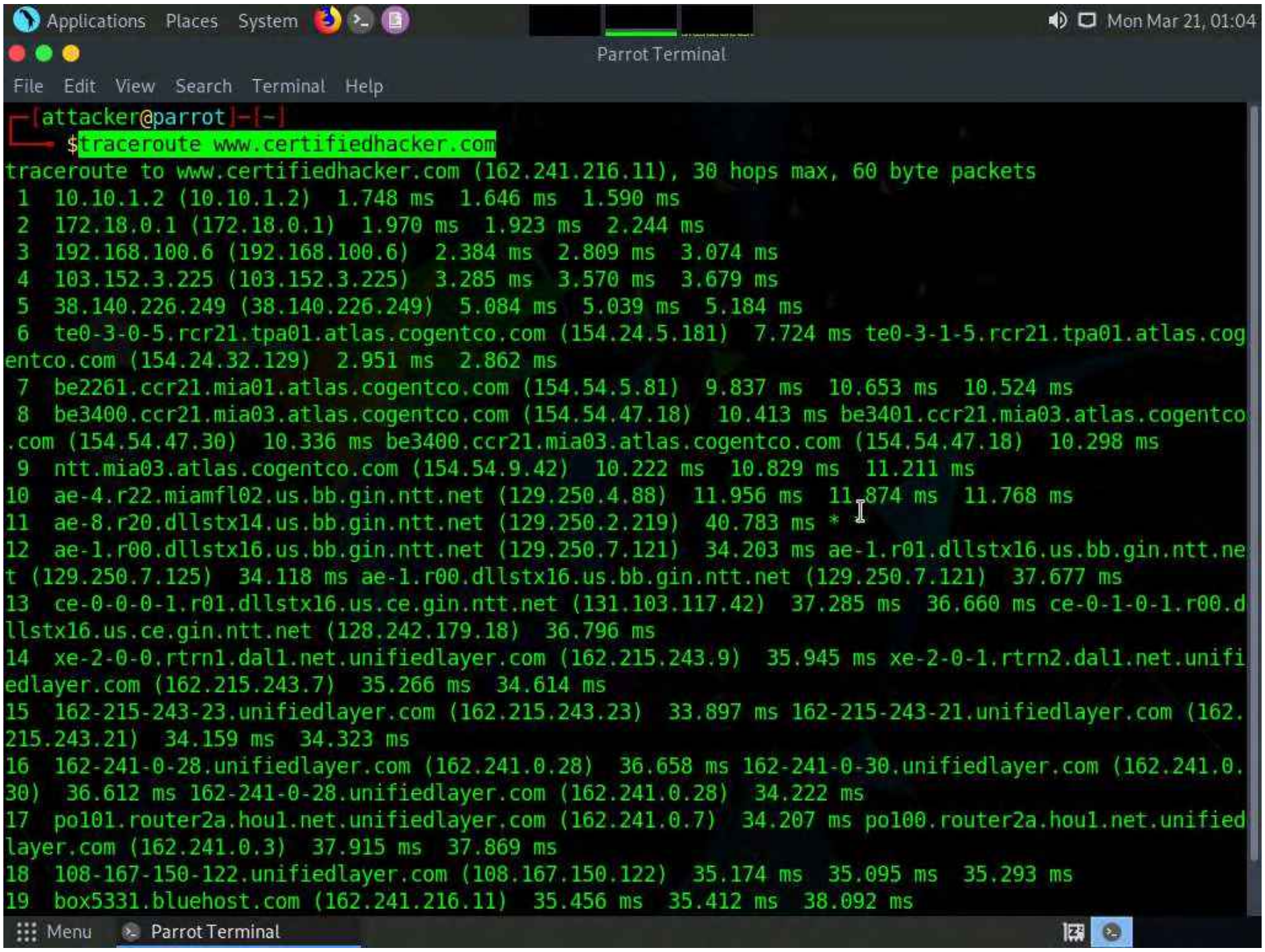
5. Now, click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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.



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.

Lab 9: Perform Footprinting using Various Footprinting Tools

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

Overview of Footprinting Tools

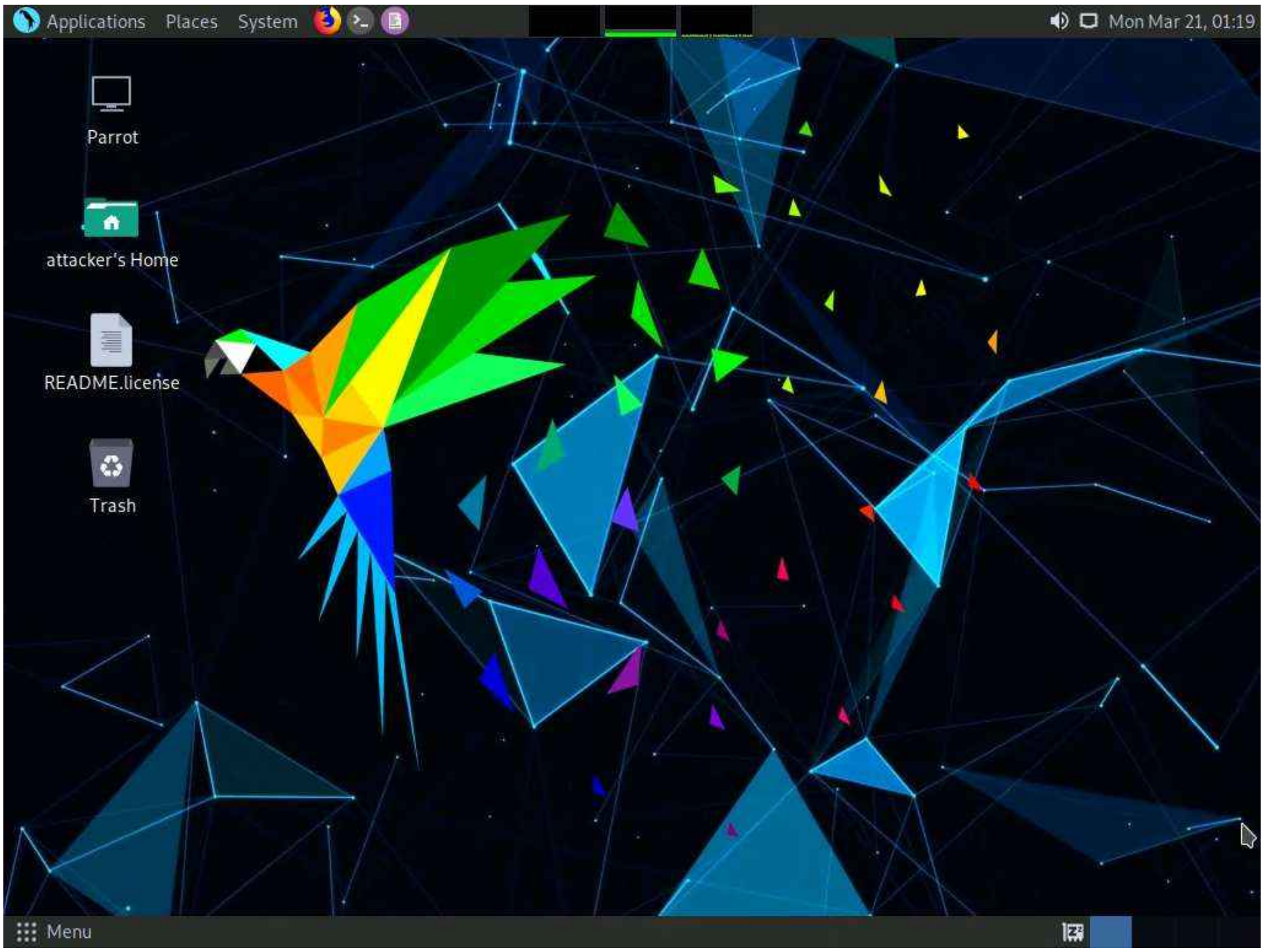
Footprinting tools are used to collect basic information about the target systems in order to exploit them. Information collected by the footprinting tools contains the target's IP location information, routing information, business information, address, phone number and social security number, details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

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** 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.

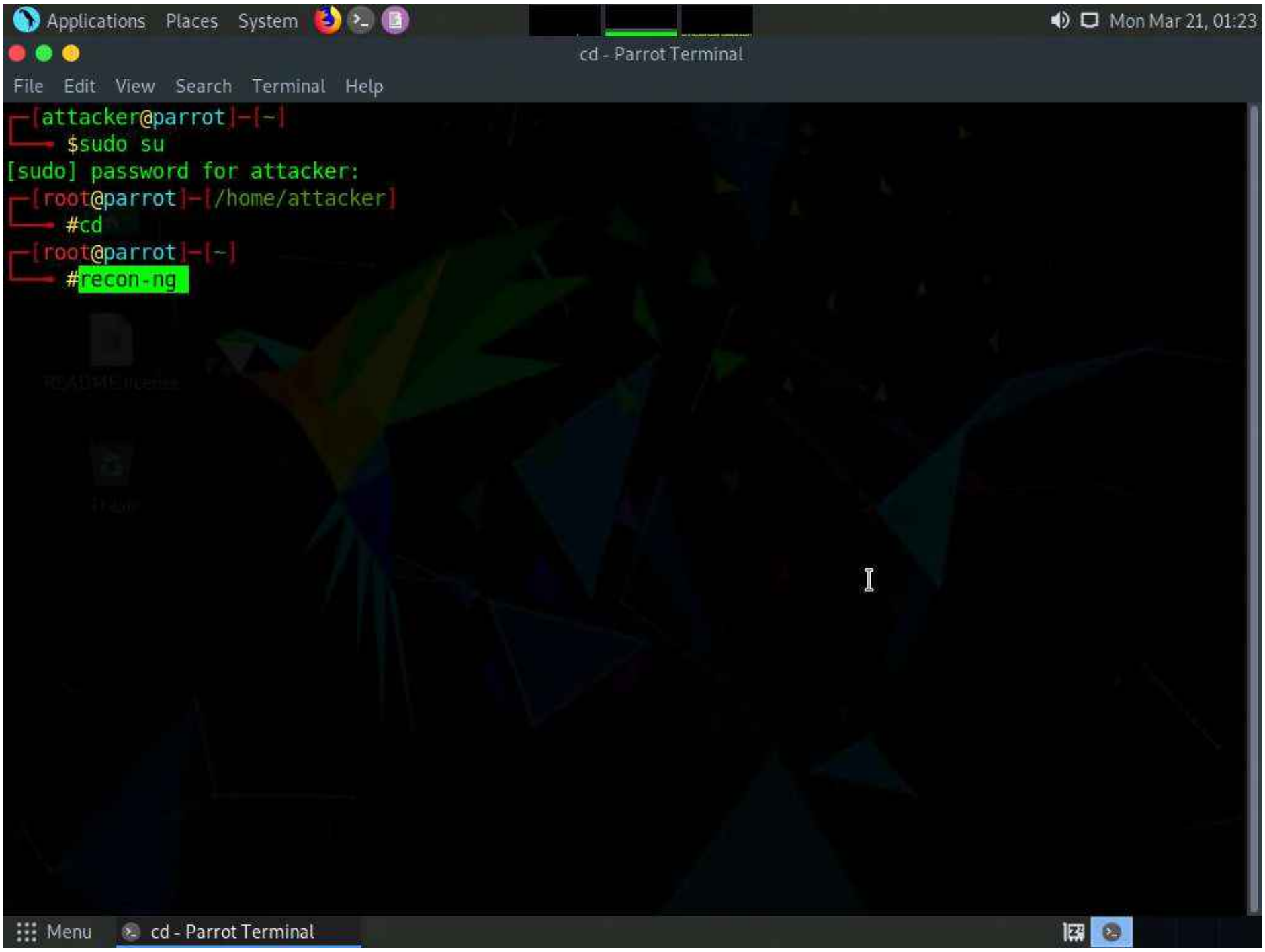
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



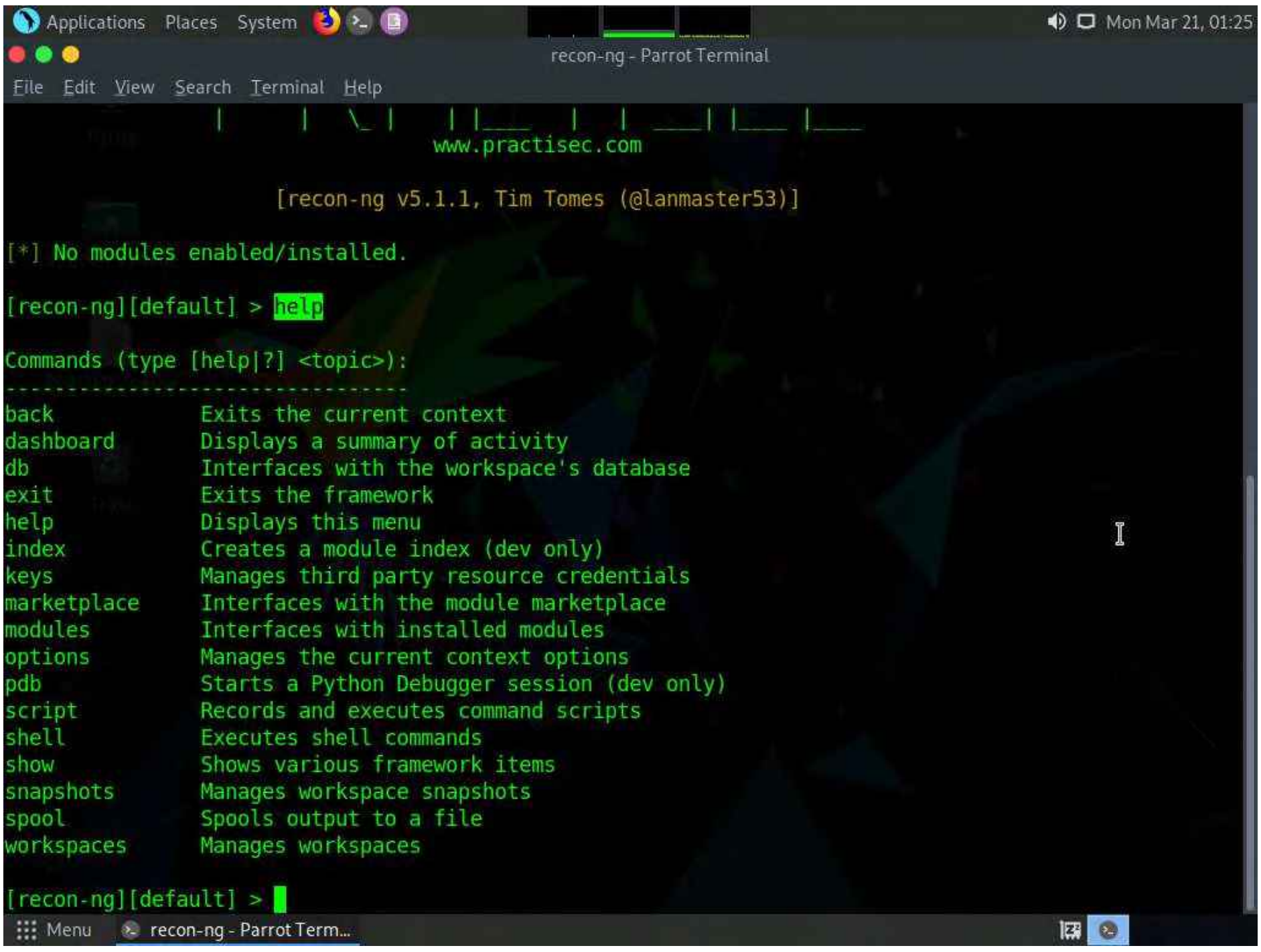
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

5. Now, type **cd** and press **Enter** to jump to the root directory.
6. In the **Terminal** window, type the command **recon-ng** and press **Enter** to launch the application.

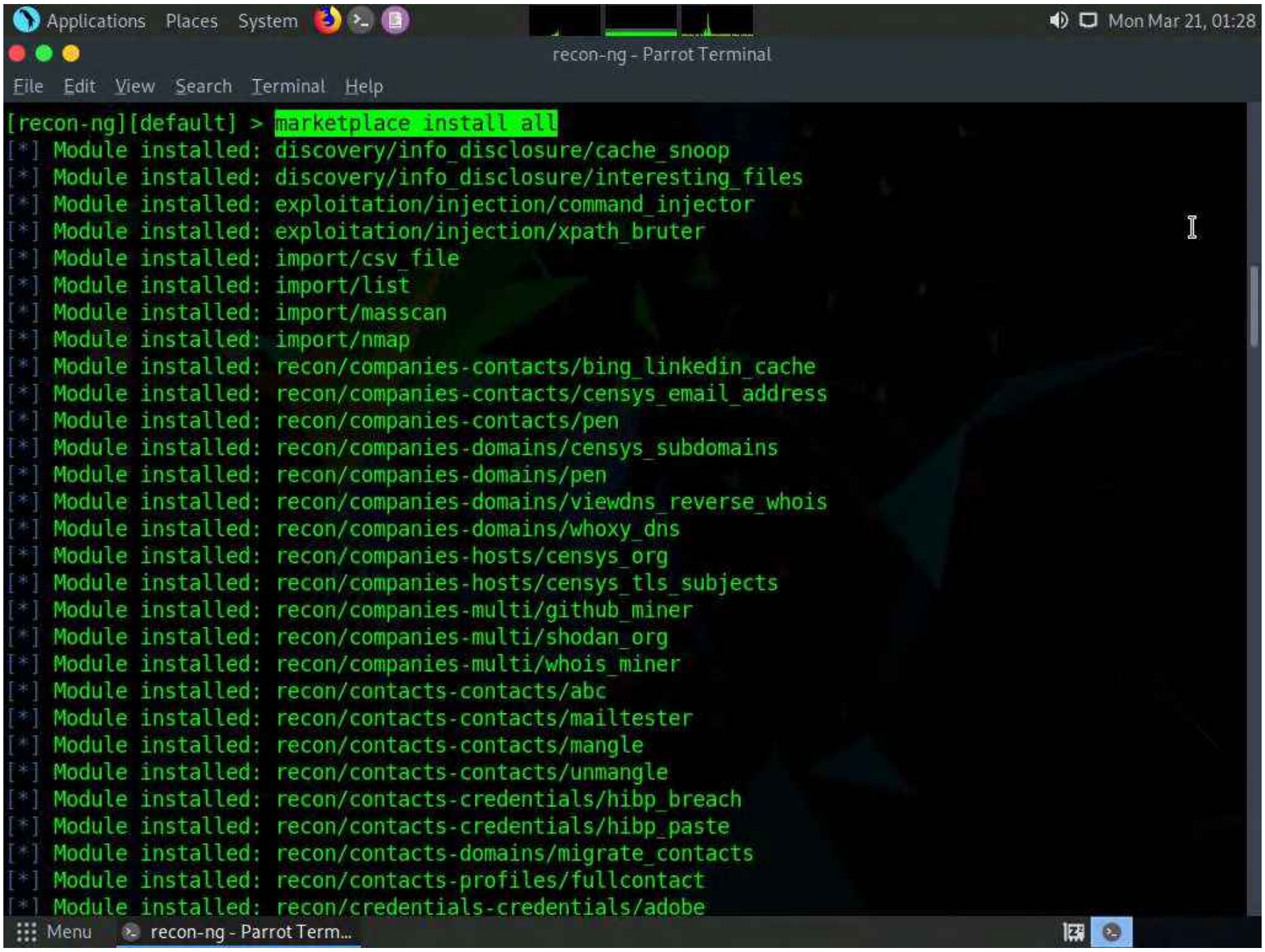


7. Type **help** and press **Enter** to view all the commands that allow you to add/delete records to a database, query a database, etc.

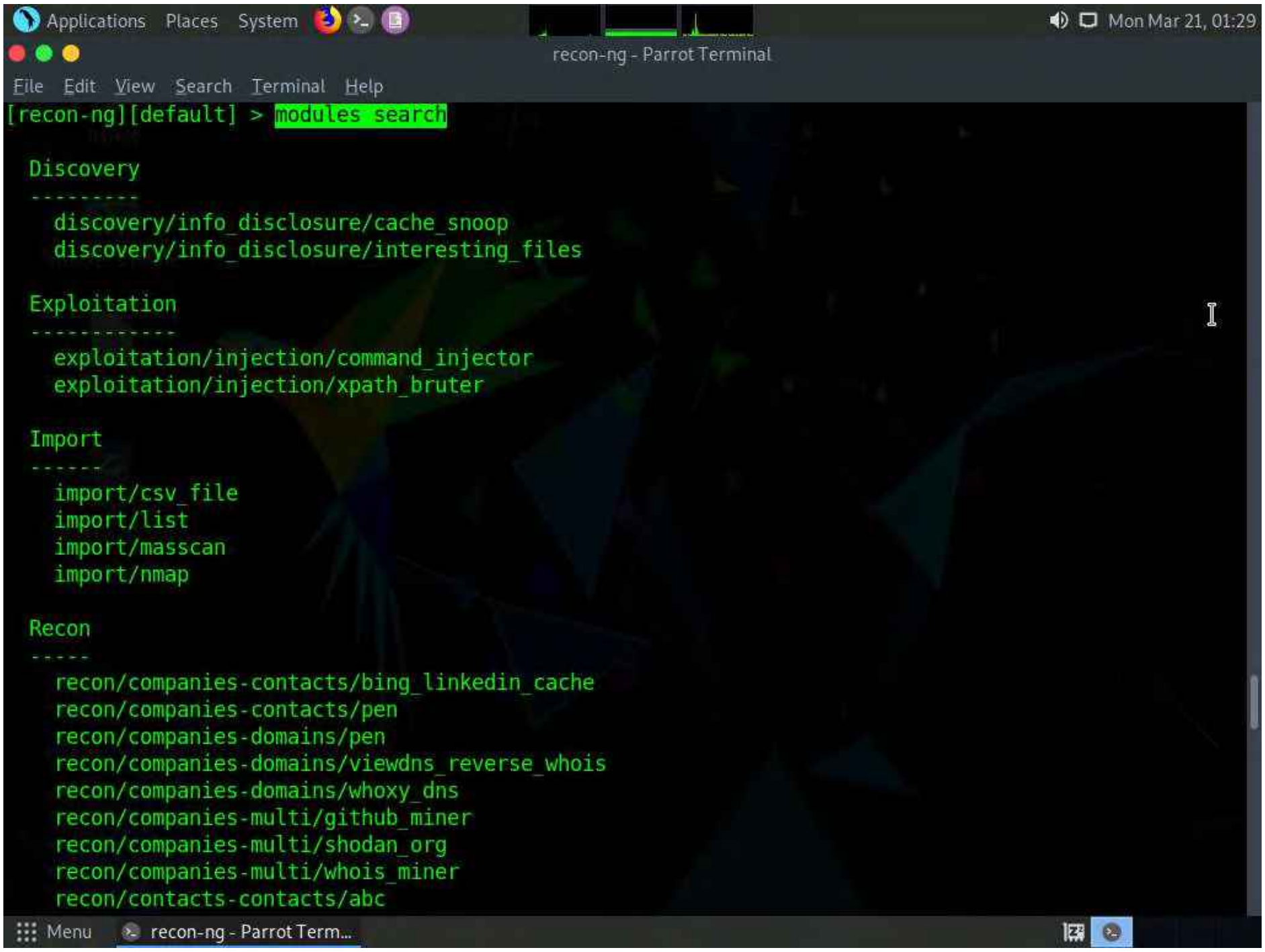


8. Type **marketplace install all** and press **Enter** to install all the modules available in recon-ng.

Note: Ignore the errors while running the command.

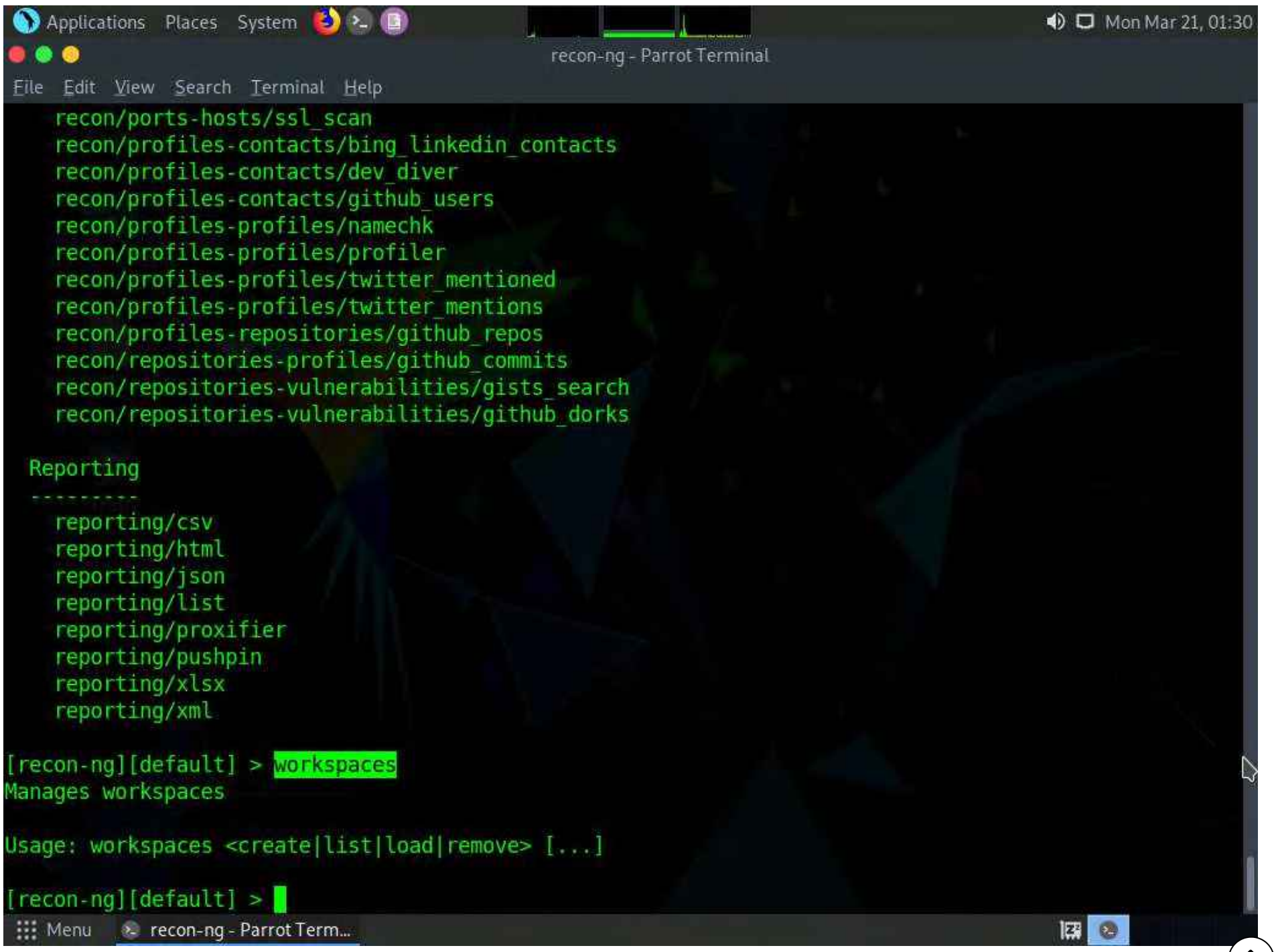


9. After the installation of modules, type the **modules search** command and press **Enter**. This displays all the modules available in recon-ng.



10. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.

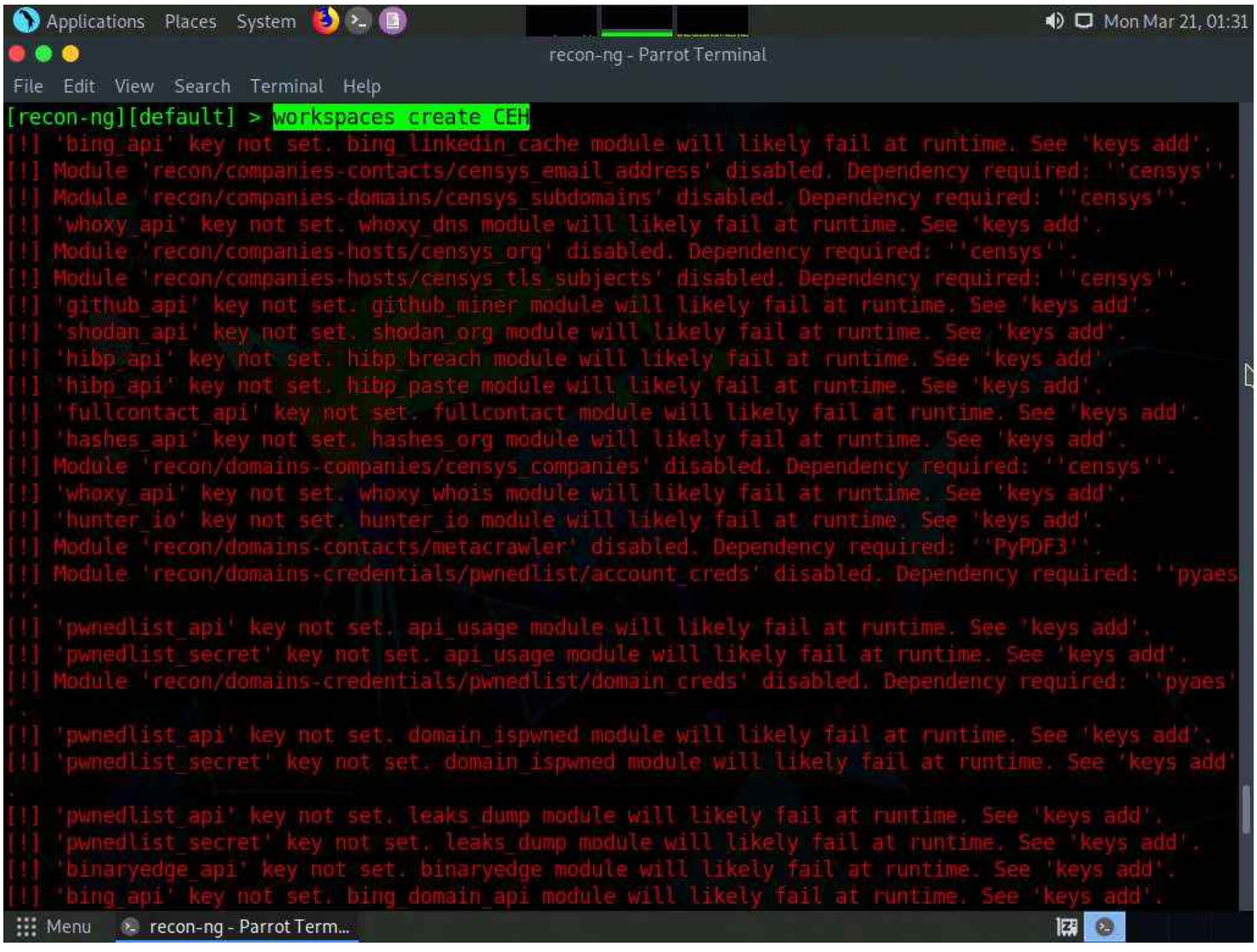
11. Type the **workspaces** command and press **Enter**. This displays the commands related to the workspaces.



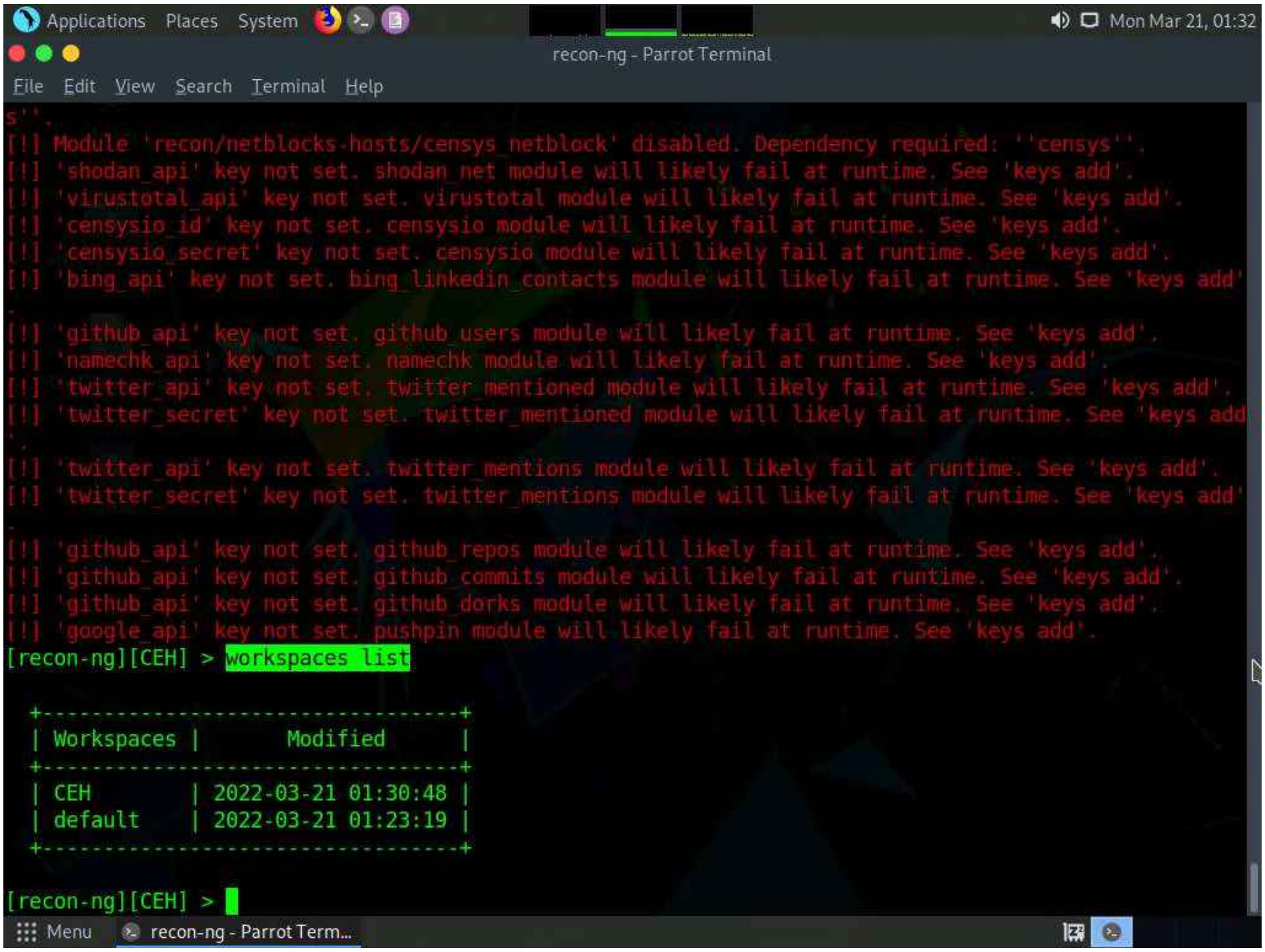
12. Create a workspace in which to perform network reconnaissance. In this task, we shall be creating a workspace named **CEH**.

13. To create the workspace, type the command **workspaces create CEH** and press **Enter**. This creates a workspace named CEH.

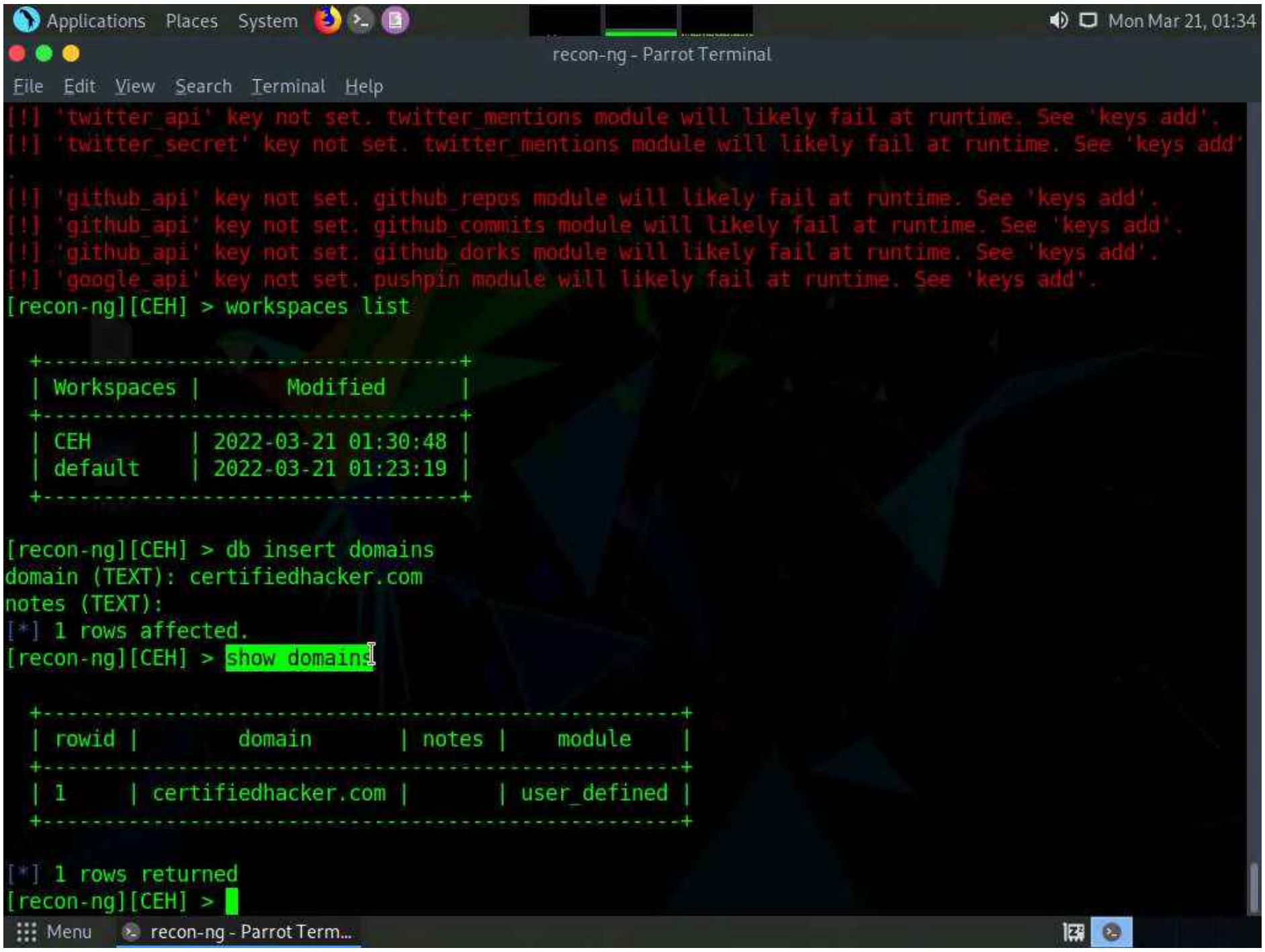
> Note: You can alternatively issue the command workspaces select CEH to create a workspace named CEH. Ignore the errors while running the commands



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.

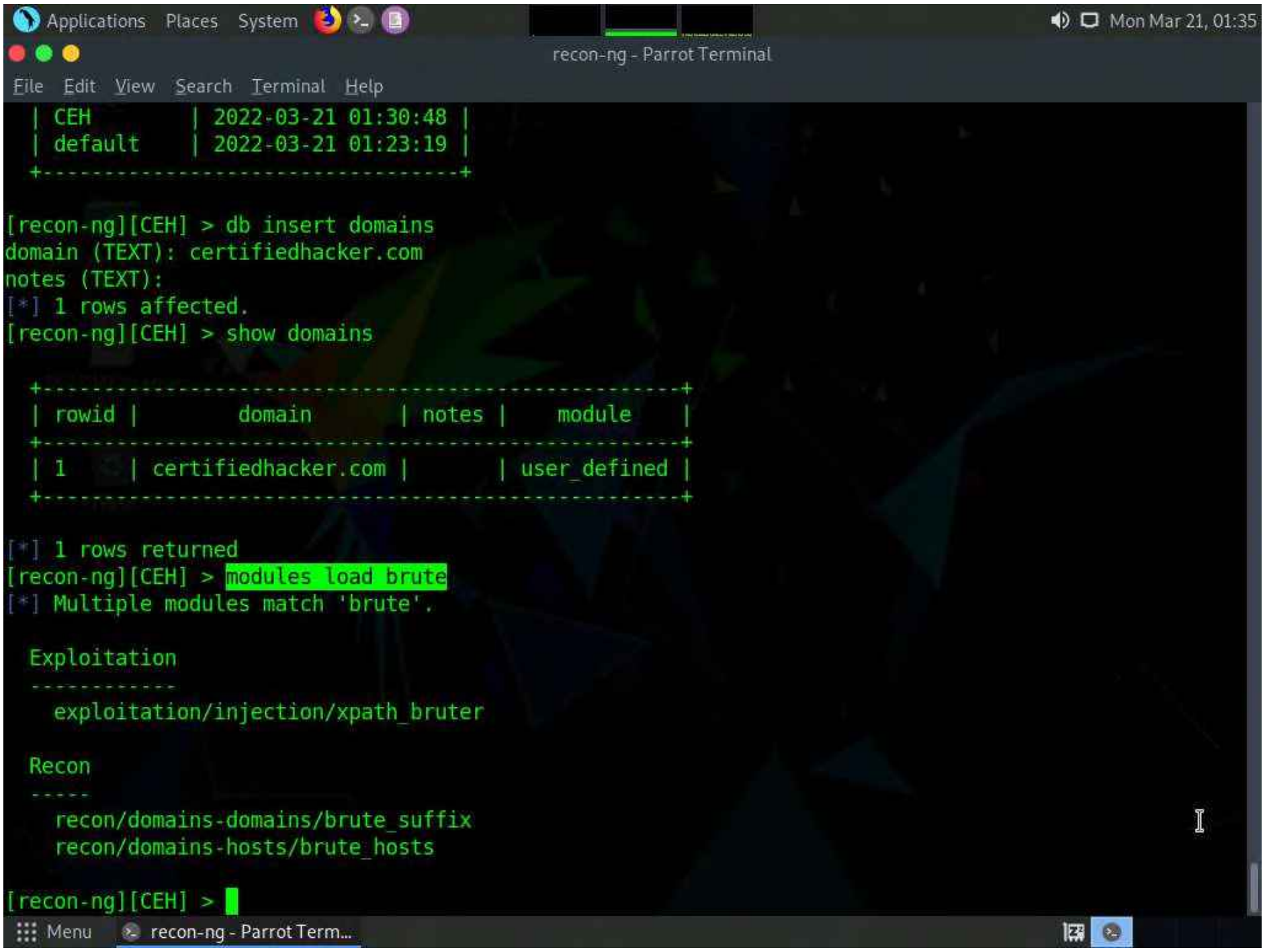


15. Add a domain in which you want to perform network reconnaissance.
16. Type the command **db insert domains** and press **Enter**.
17. In the **domain (TEXT)** option type **certifiedhacker.com** and press **Enter**. In the **notes (TEXT)** option press **Enter**. This adds certifiedhacker.com to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

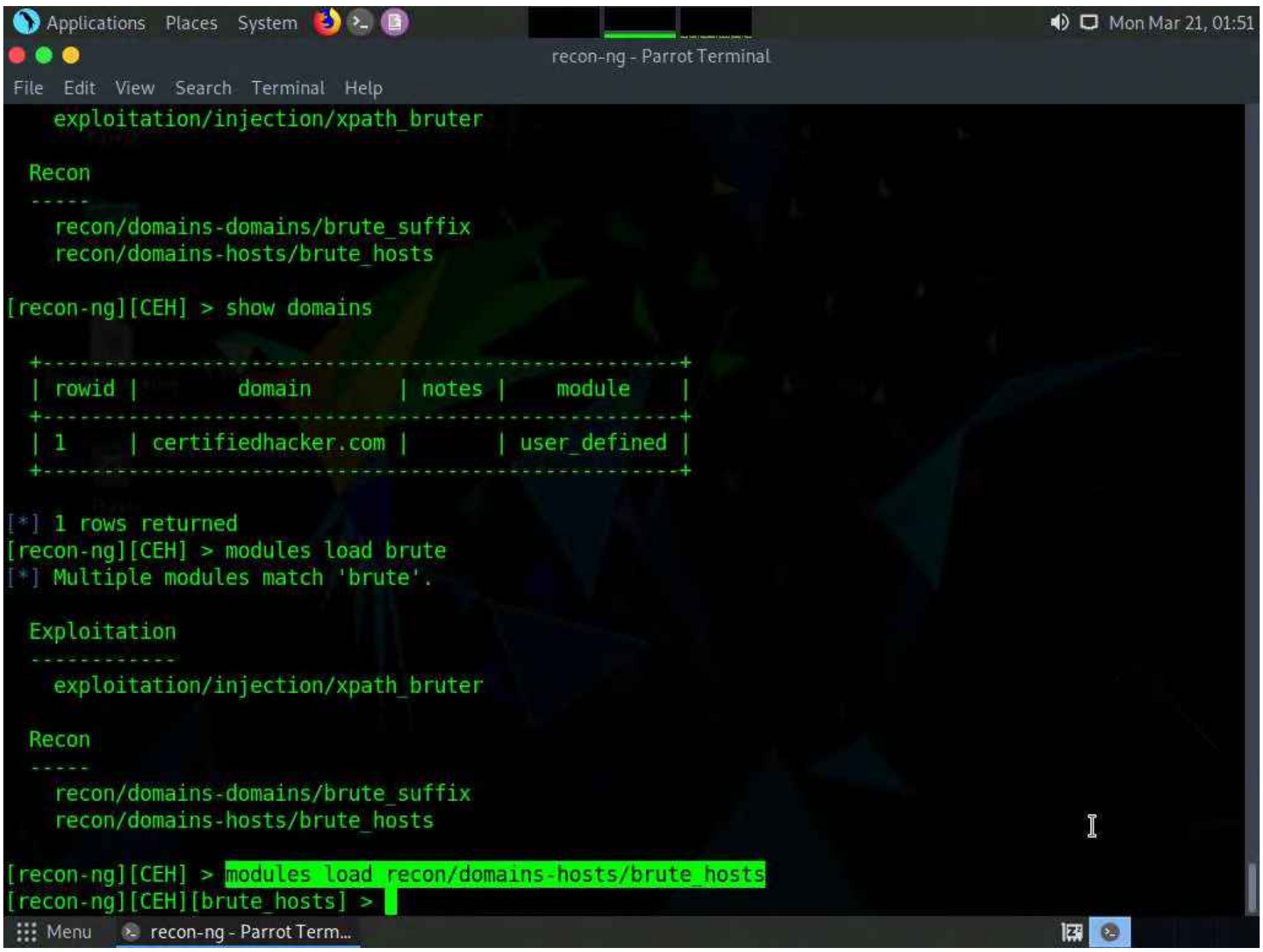


19. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as brute_hosts, Netcraft, and Bing.

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.



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



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

```
Applications  Places  System                                   Mon Mar 21, 01:53
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.
Menu  recon-ng - Parrot Term...
```

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

```
Applications  Places  System                                   Mon Mar 21, 01:54
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] >
Menu  recon-ng - Parrot Term...
```

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.

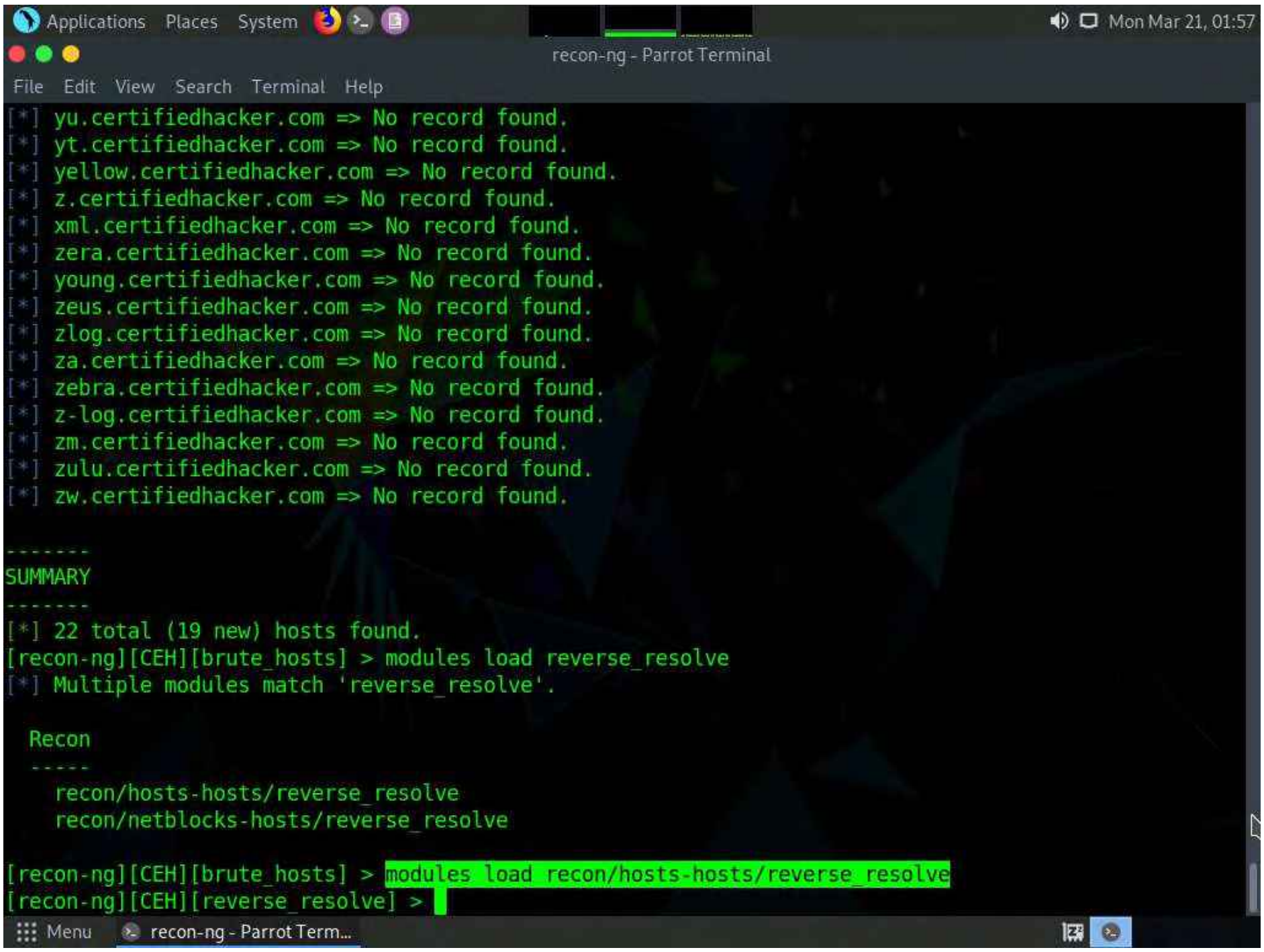
Note: To resolve hosts using the Bing module, use the following commands:

back
modules load recon/domains-hosts/bing_domain_web
run

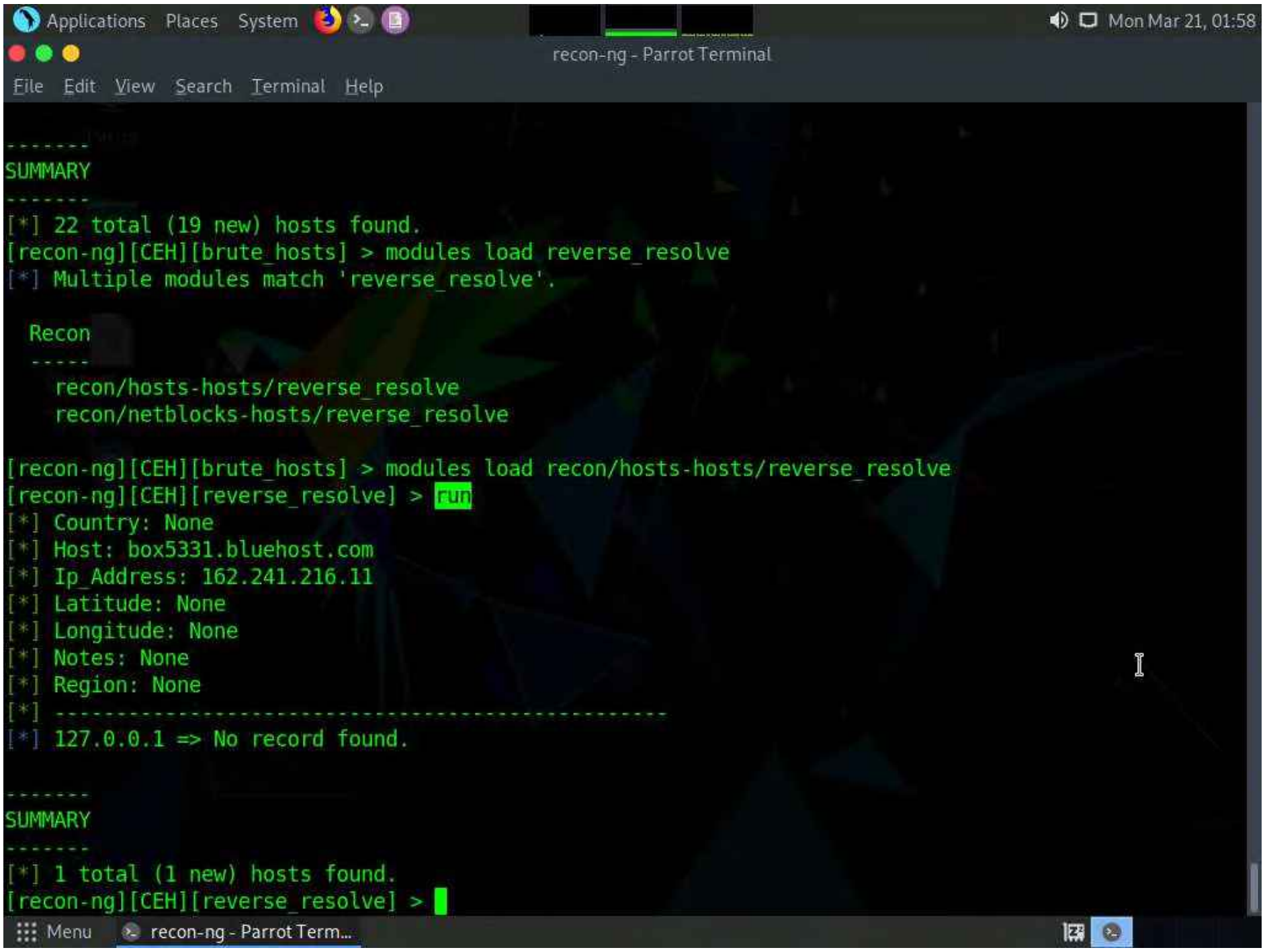
25. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

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.

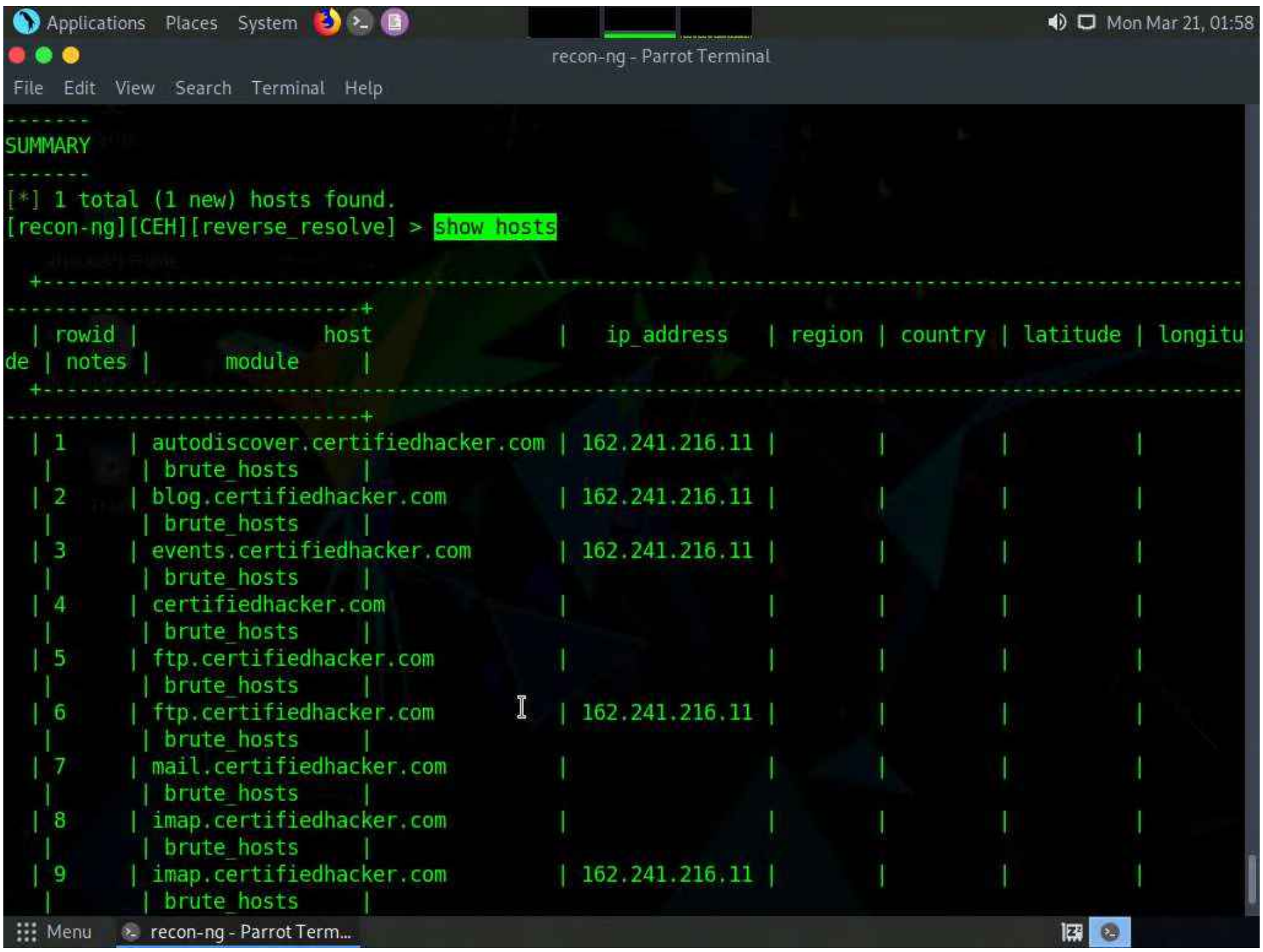
27. Type the **modules load recon/hosts-hosts/reverse_resolve** command and press **Enter** to load the module.



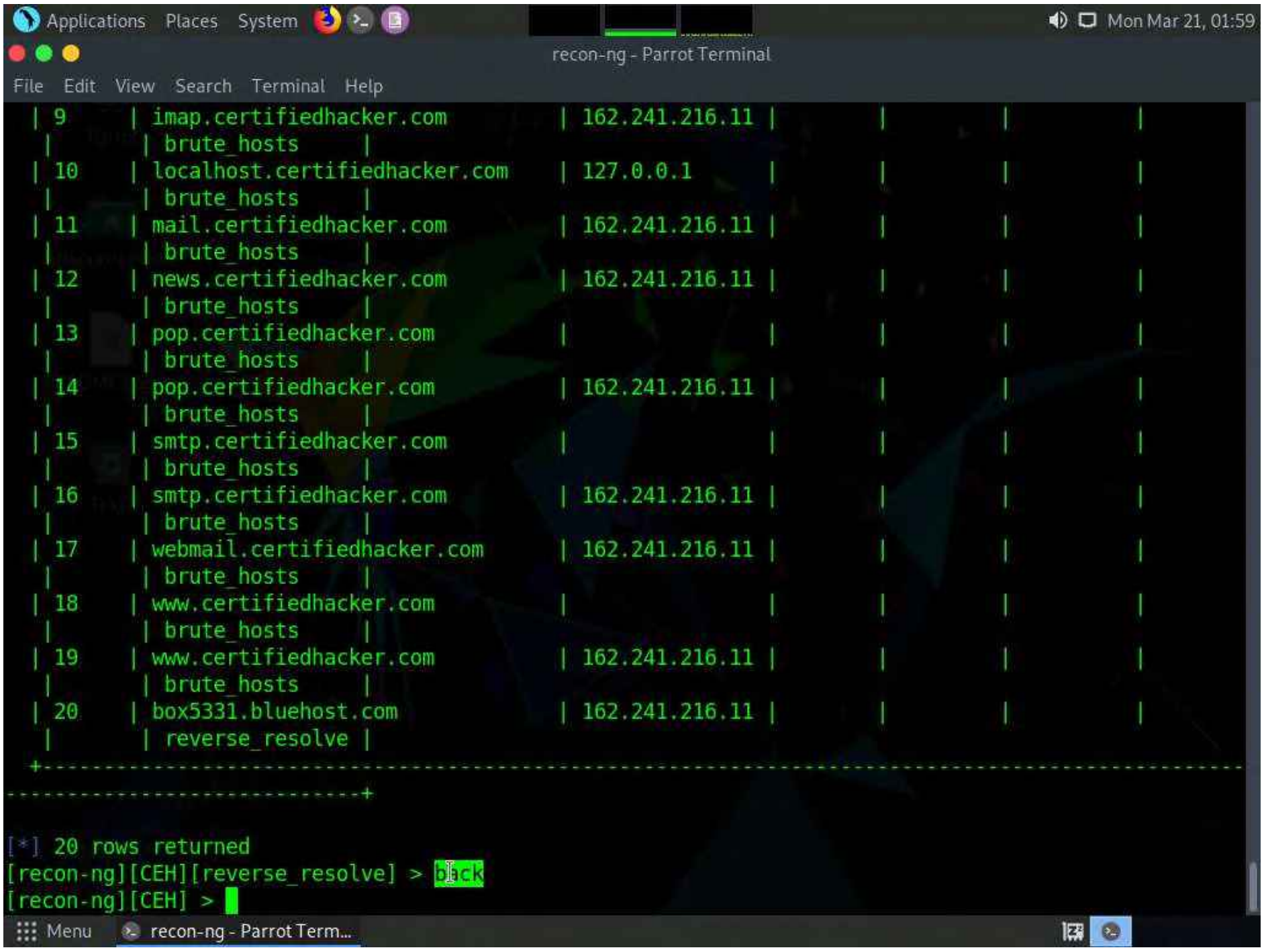
28. Issue the **run** command to begin the reverse lookup.



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.

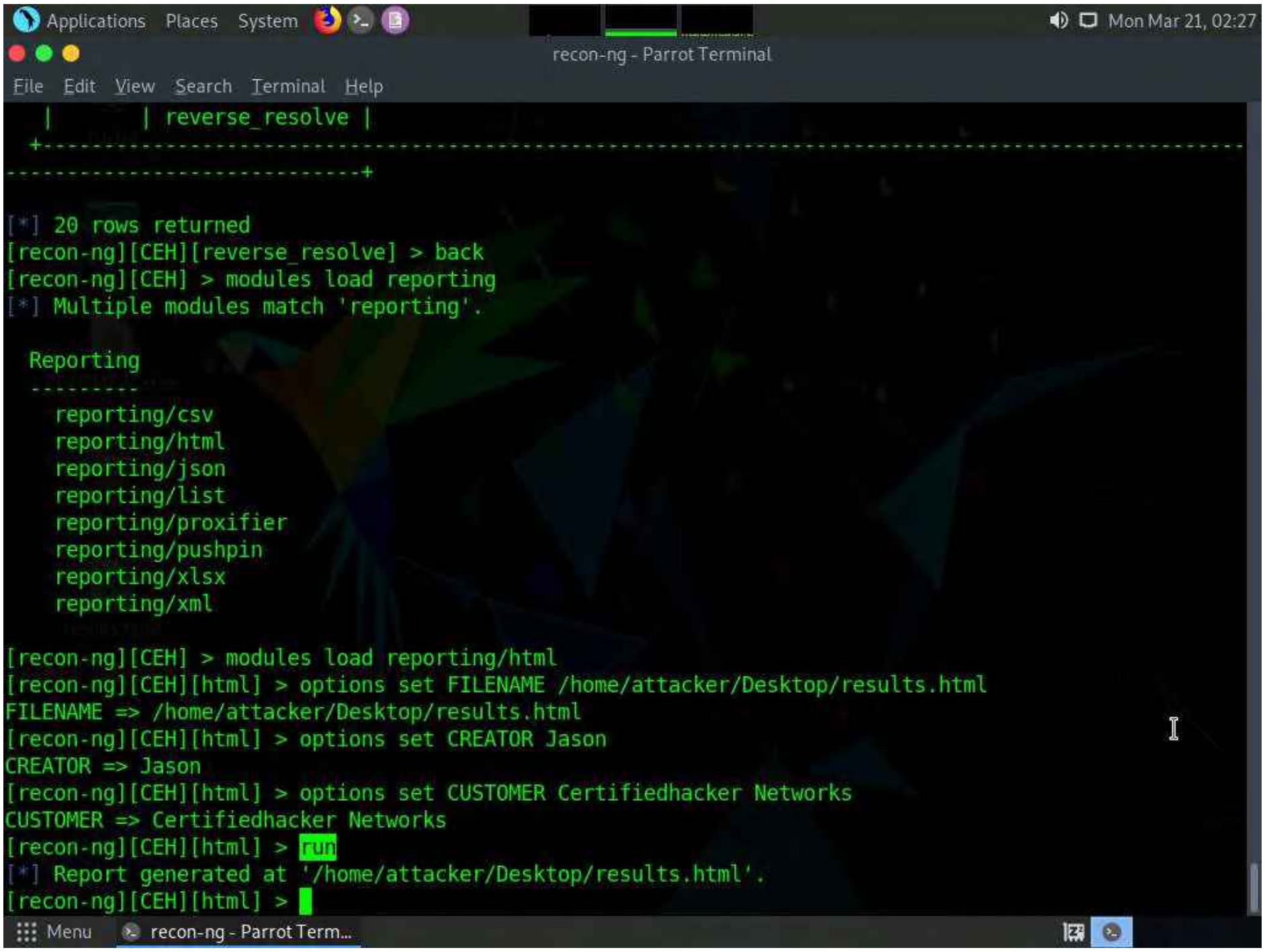


30. Now, type the **back** command and press **Enter** to go back to the CEH attributes terminal.



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:

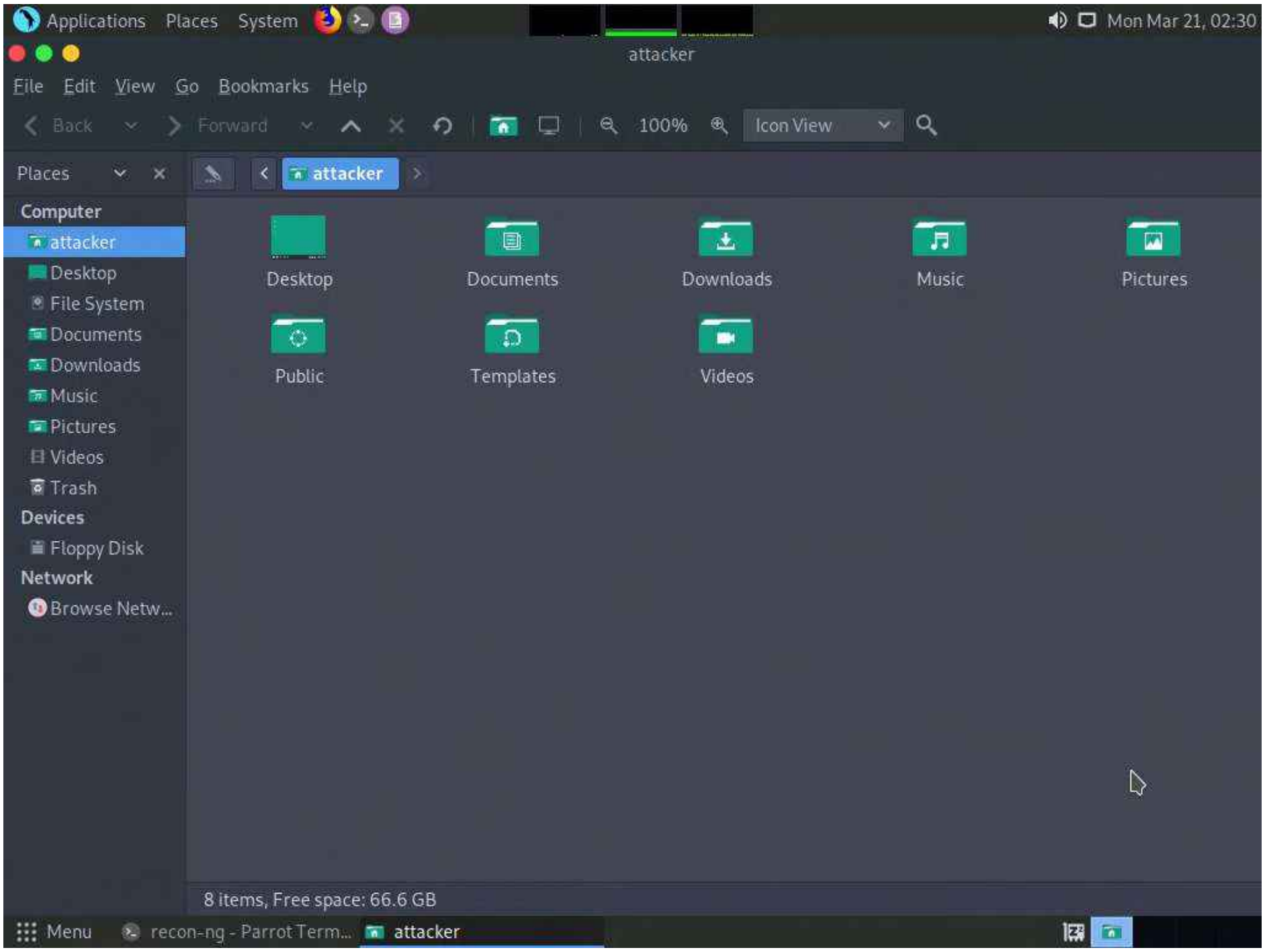
    options set FILENAME /home/attacker/Desktop/results.html and press **Enter**. By issuing this command, you are setting the report name as **results.html** and the path to store the file as **Desktop**.
    options set CREATOR [your name] (here, **Jason**) and press **Enter**.
    options set CUSTOMER 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.



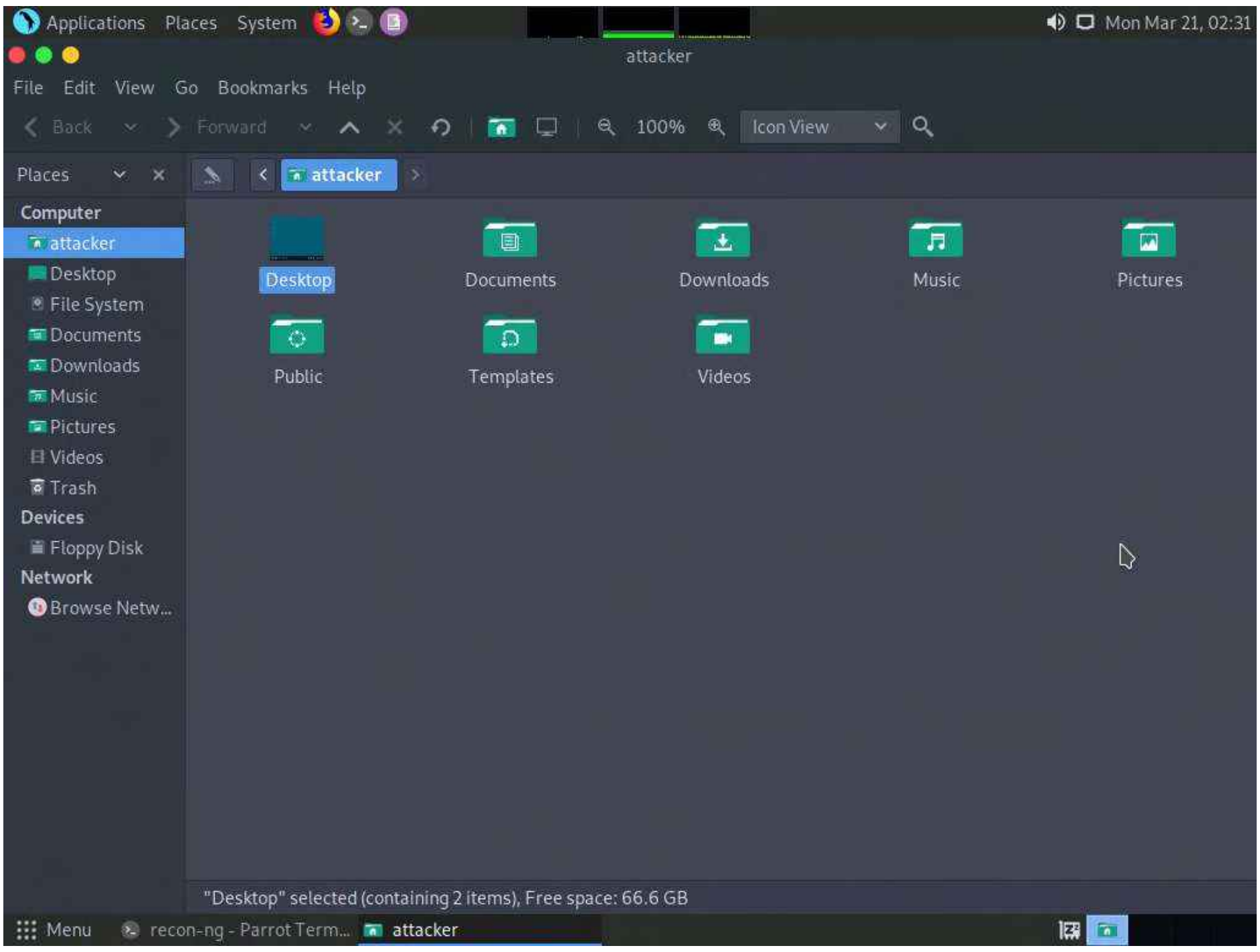
37. The generated report is saved to **/home/attacker/Desktop/**.

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

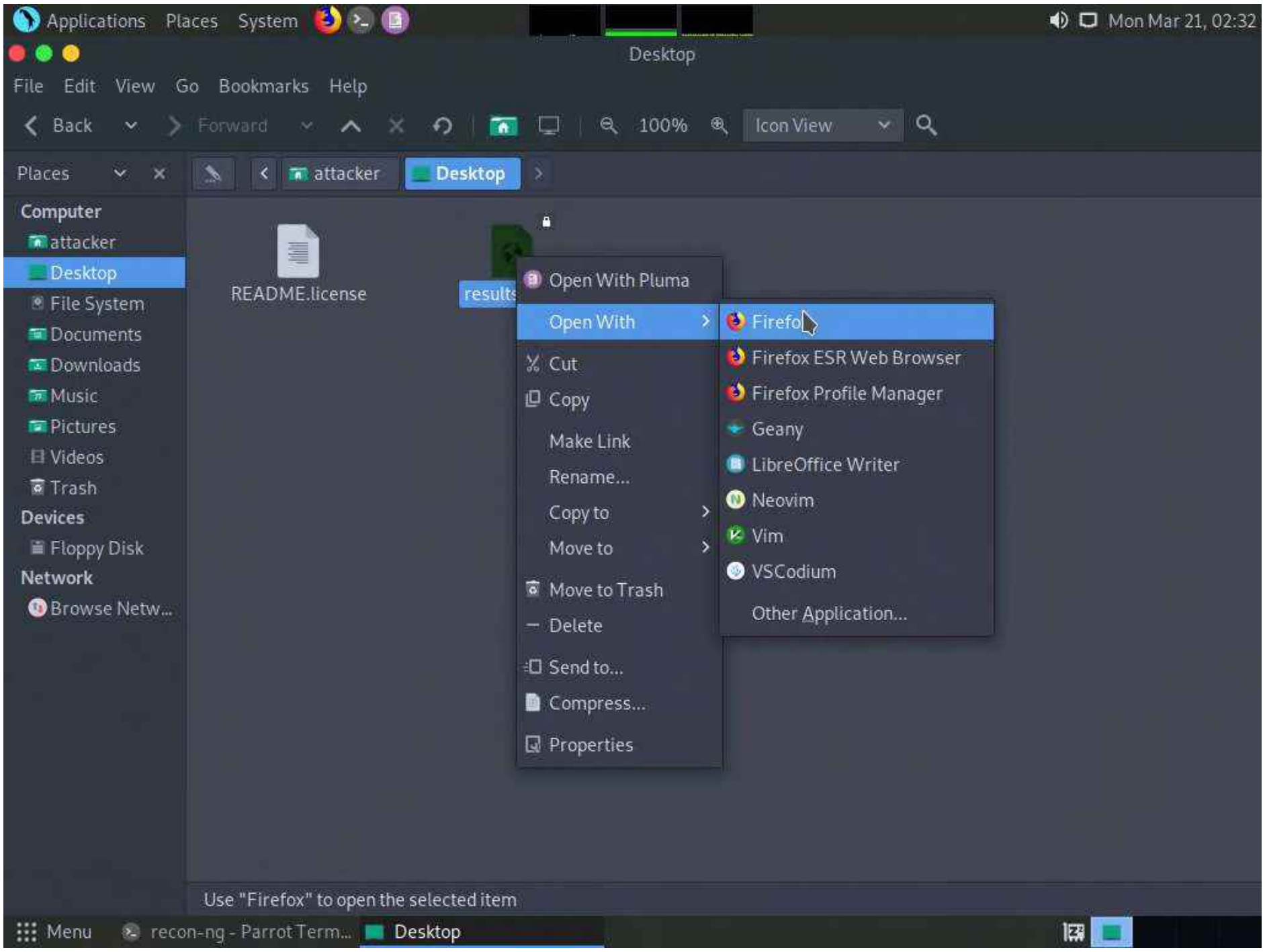
39. The **attacker** window appears.



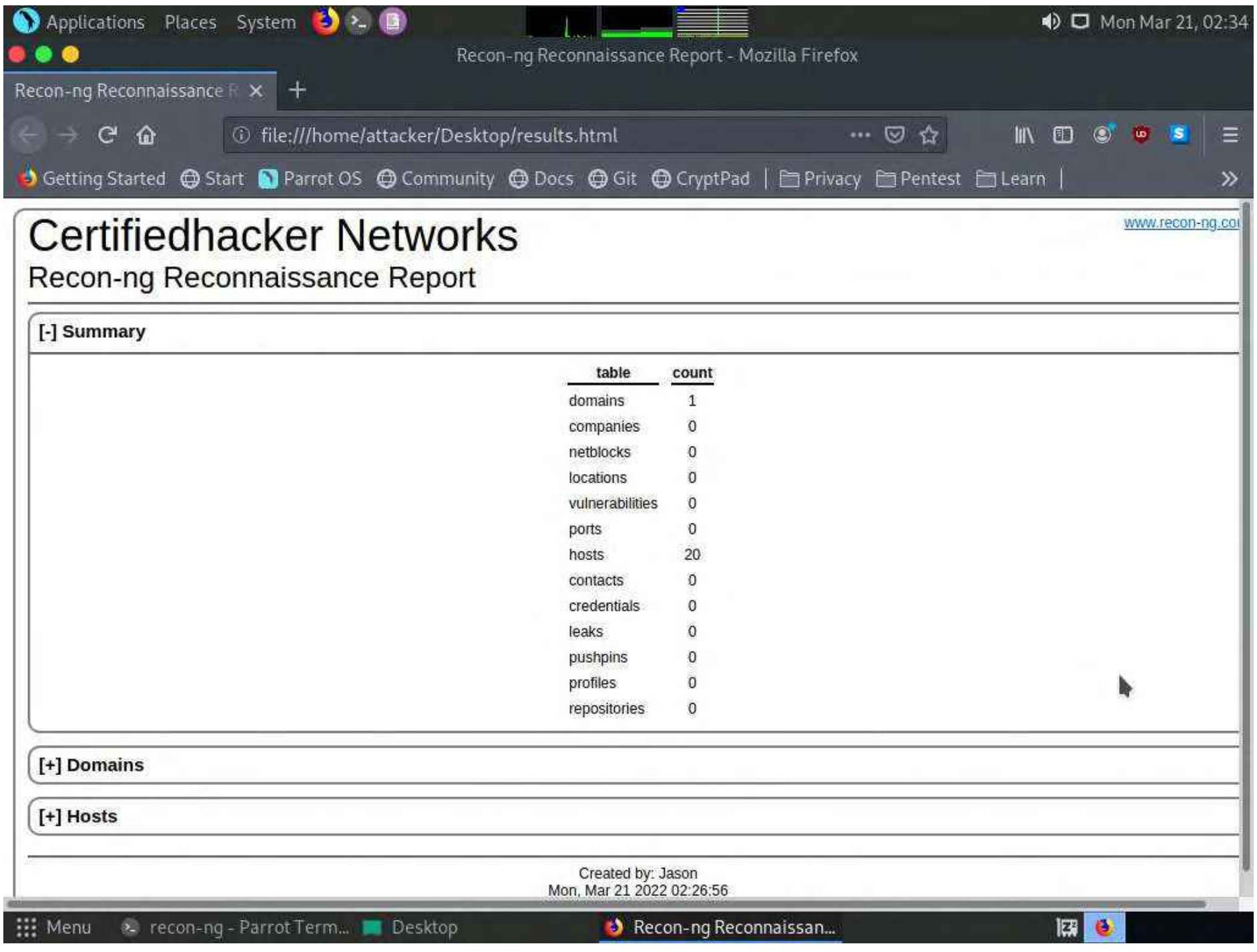
40. In the **attacker** window, double-click **Desktop**.



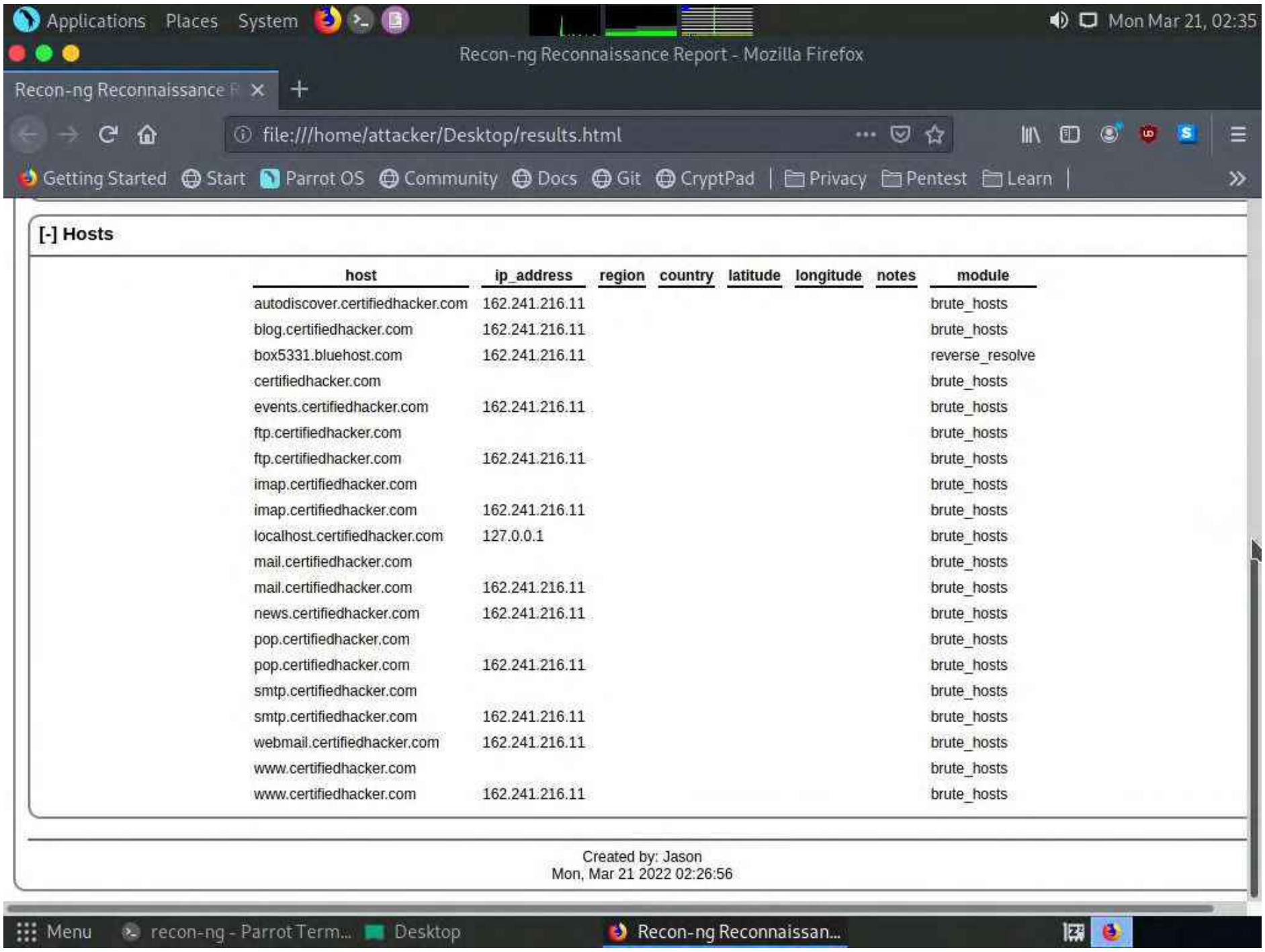
41. **Desktop** window appears, right-click on the **results.html** file, click on **Open With**, and select the **Firefox** browser from the available options.



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



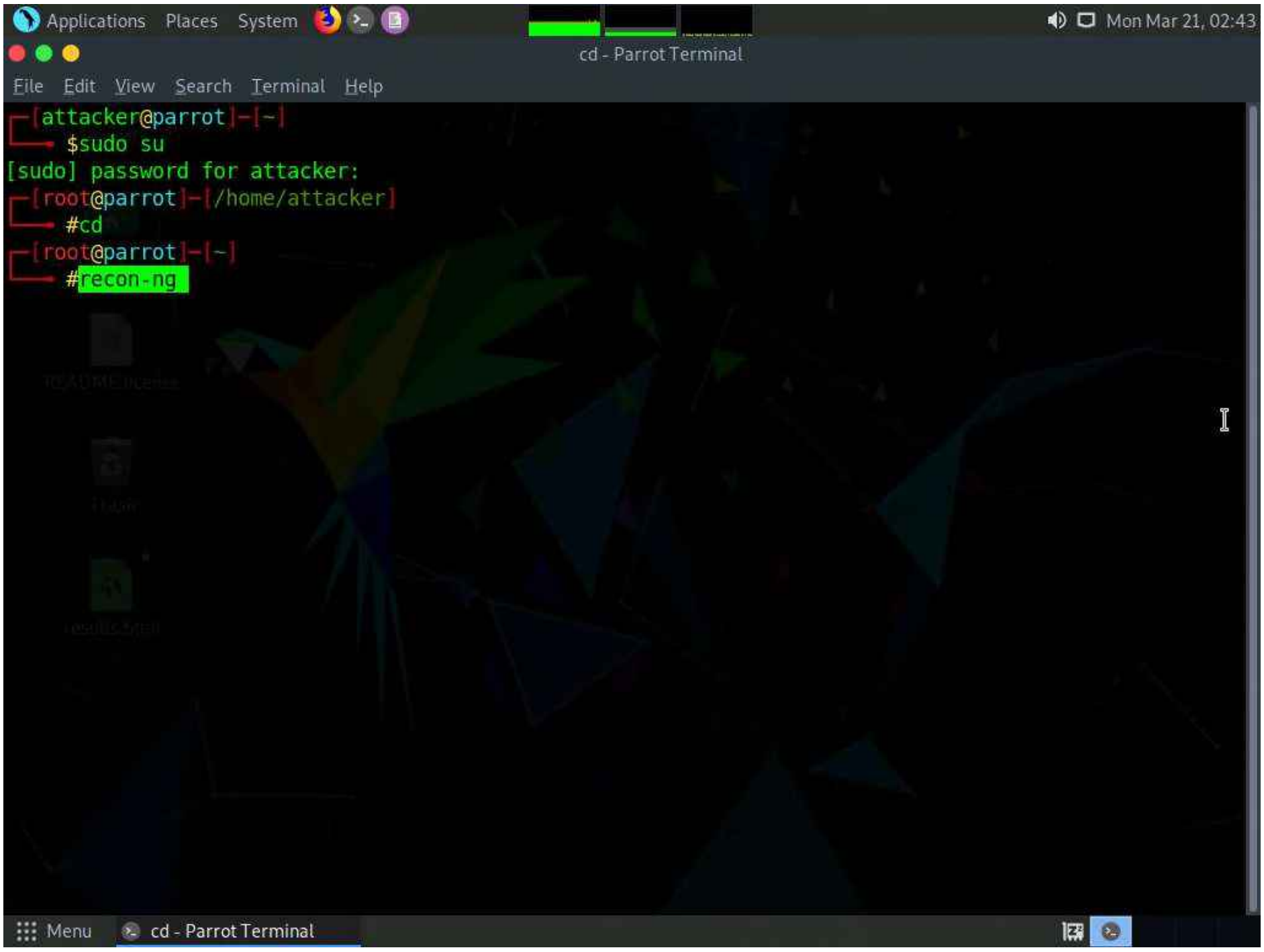
43. You can expand the **Hosts** node to view all the harvested hosts, as shown in the screenshot.



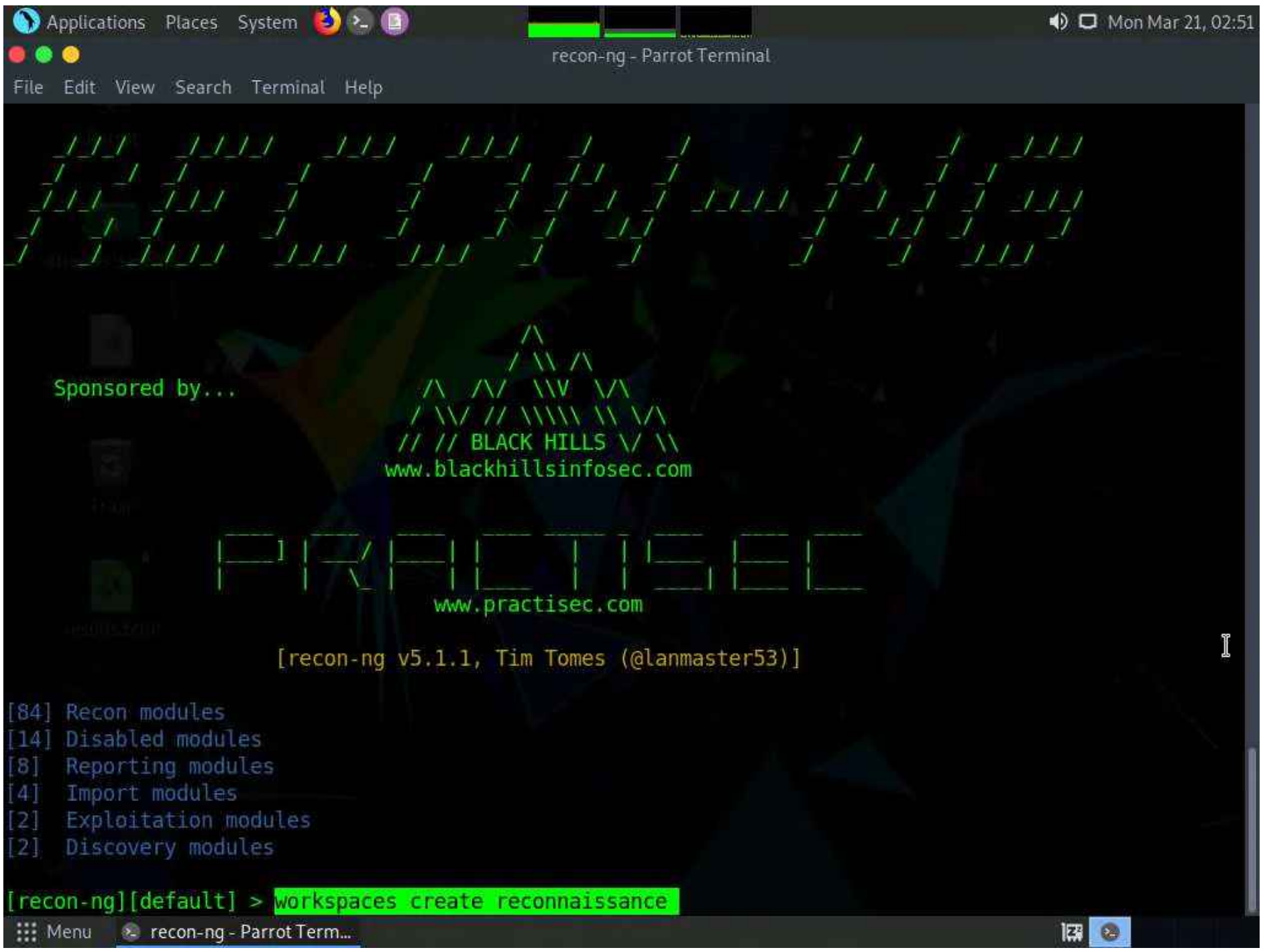
44. Close all open windows.
45. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain
46. Now, we will use Recon-ng to gather personnel information.
47. Open a new **Parrot Terminal** window, In the terminal window, type **sudo su** and press **Enter** to run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



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



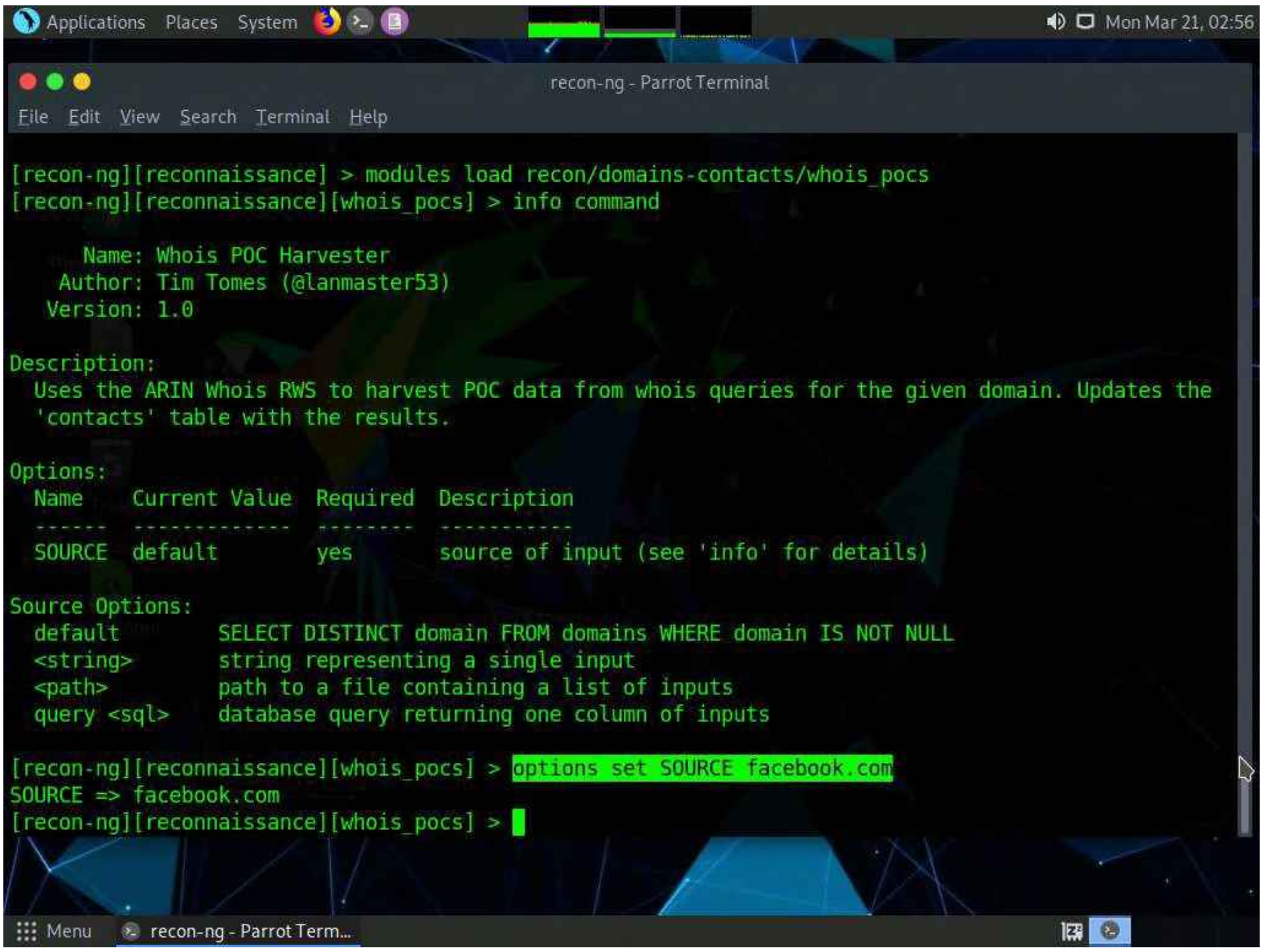
52. Set a domain and perform footprinting on it to extract contacts available in the domain.

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.

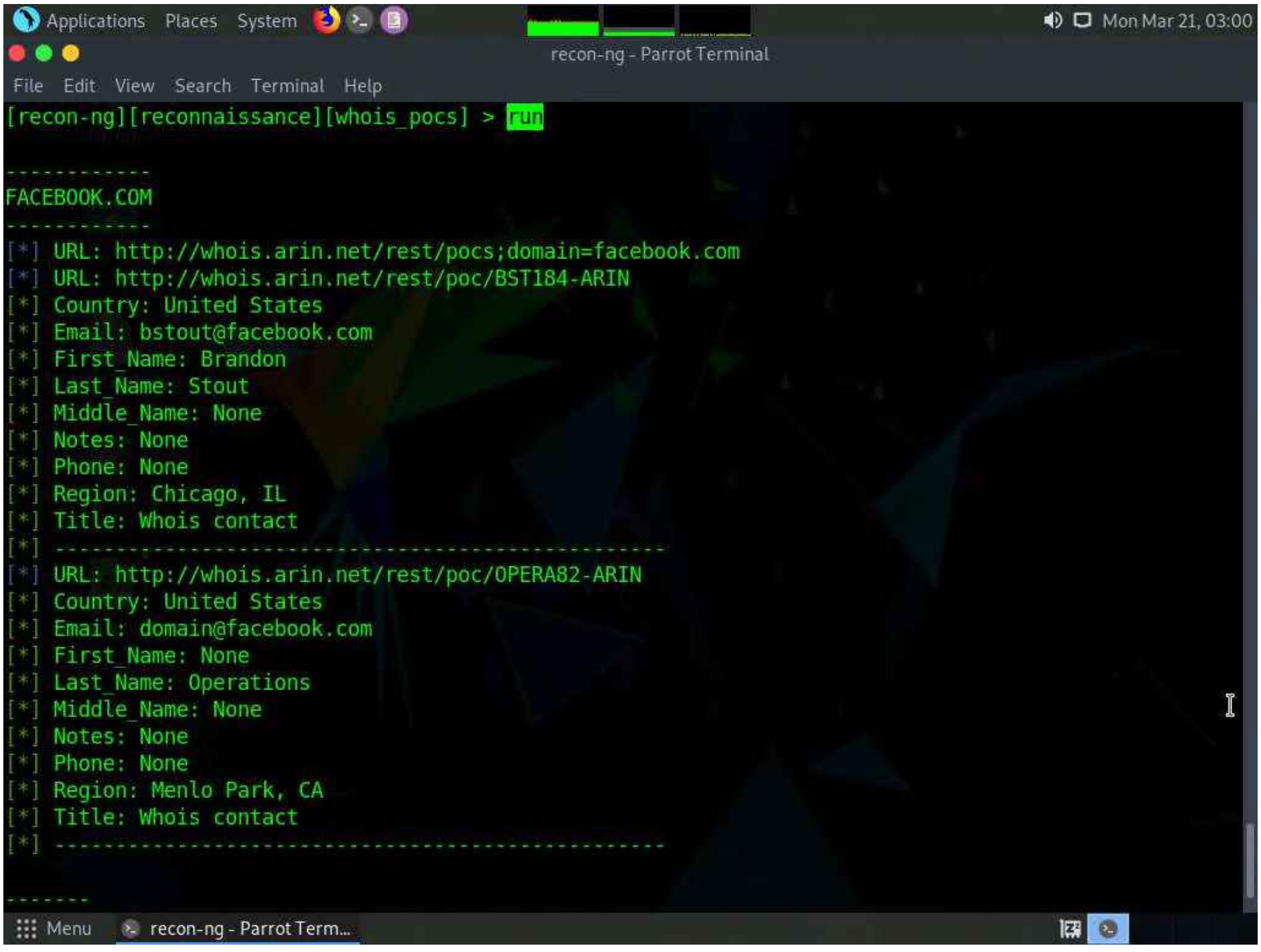
55. Type **options set SOURCE facebook.com** and press **Enter** to add facebook.com as a target domain.

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



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

> Note: Results might differ when you perform the lab.



57. Until now, we have obtained contacts related to the domains. Note down these contacts' names. Close all the open windows.

58. Now, we will use Recon-ng to extract a list of subdomains and IP addresses associated with the target URL.

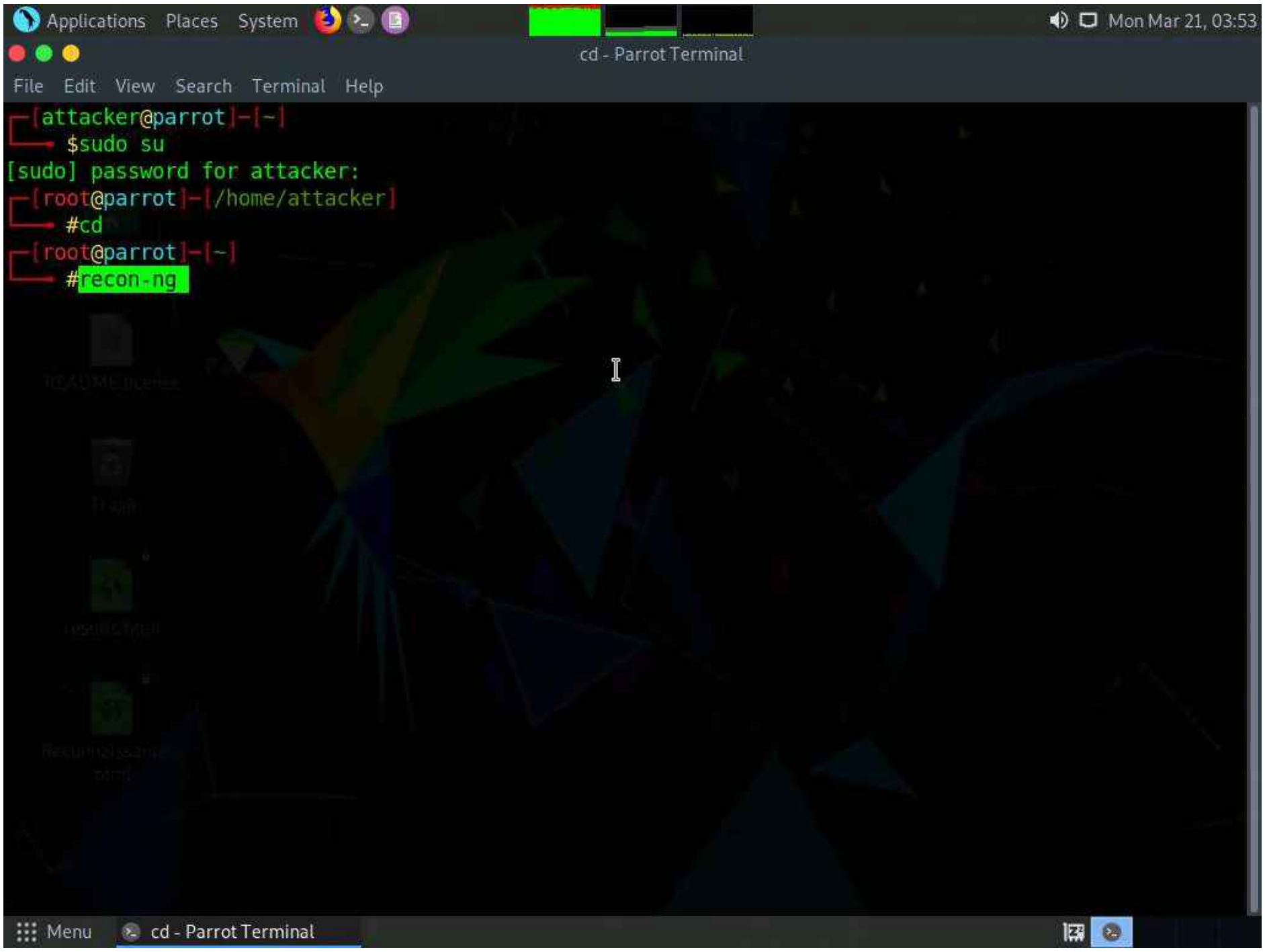
59. Open a new **Parrot Terminal** window, In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

60. 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.

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

62. Type **recon-ng**, and press **Enter**.

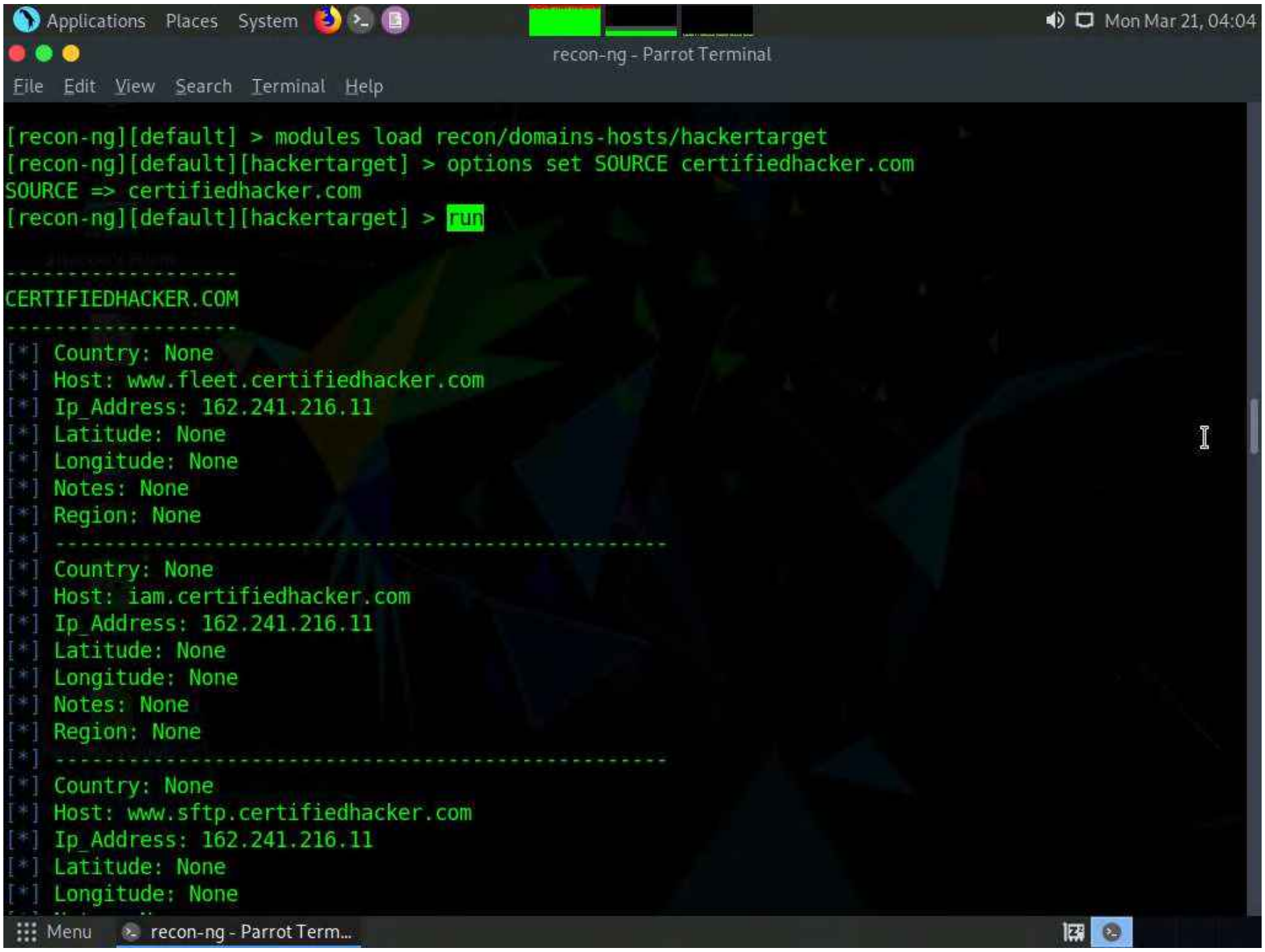


63. To extract a list of subdomains and IP addresses associated with the target URL, we need to load the **recon/domains-hosts/hackertarget** module.

64. Type the **modules load recon/domains-hosts/hackertarget** command and press **Enter**.

65. Type the **options set SOURCE certifiedhacker.com** command and press **Enter**.

66. 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.



67. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.

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

Task 2: Footprinting a Target using Maltego

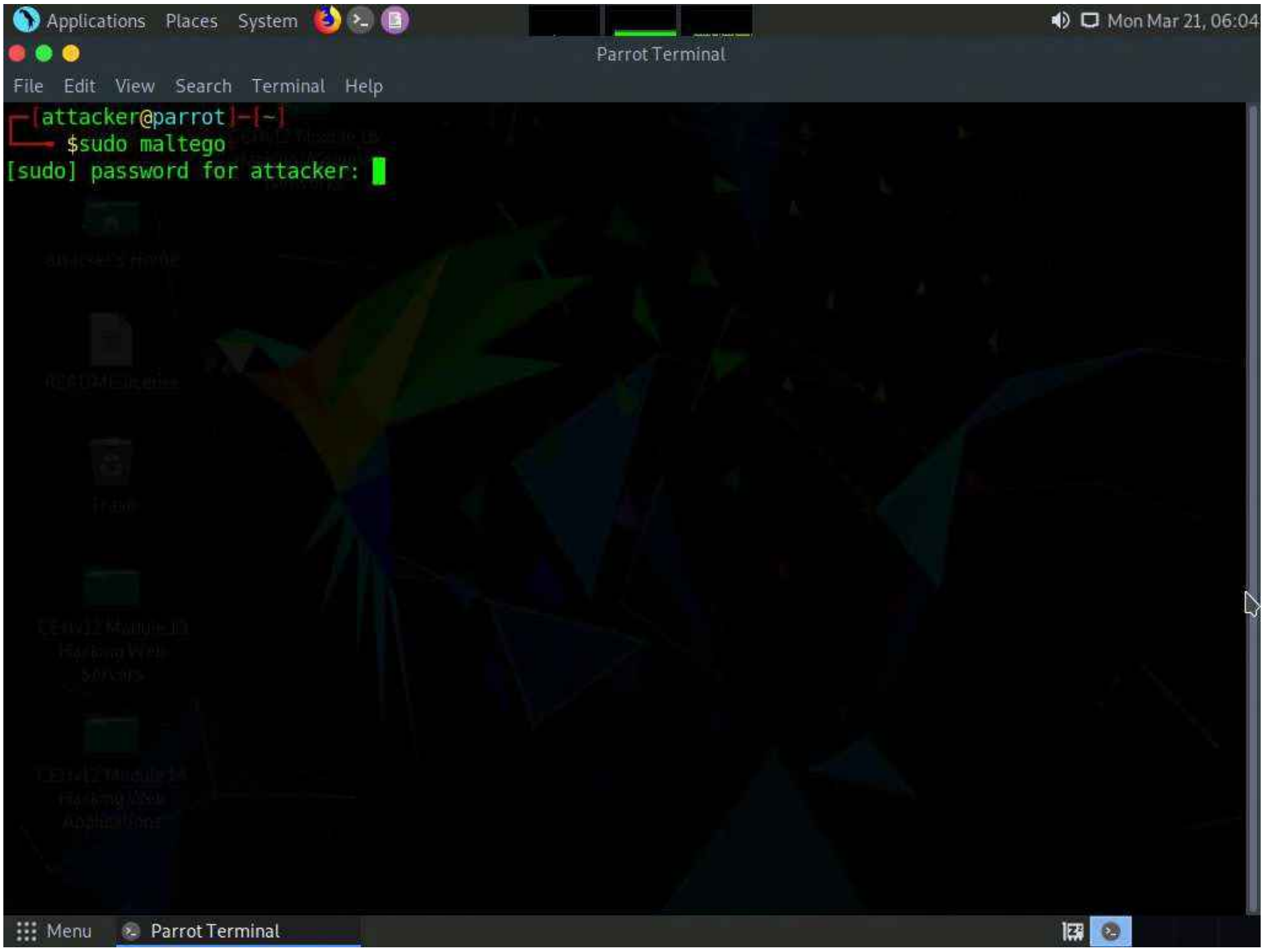
Maltego is a footprinting tool used to gather maximum information for the purpose of ethical hacking, computer forensics, and pentesting. It provides a library of transforms to discover data from open sources and visualizes that information in a graph format, suitable for link analysis and data mining. 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** as a target website. However, you can select a target domain of your choice.

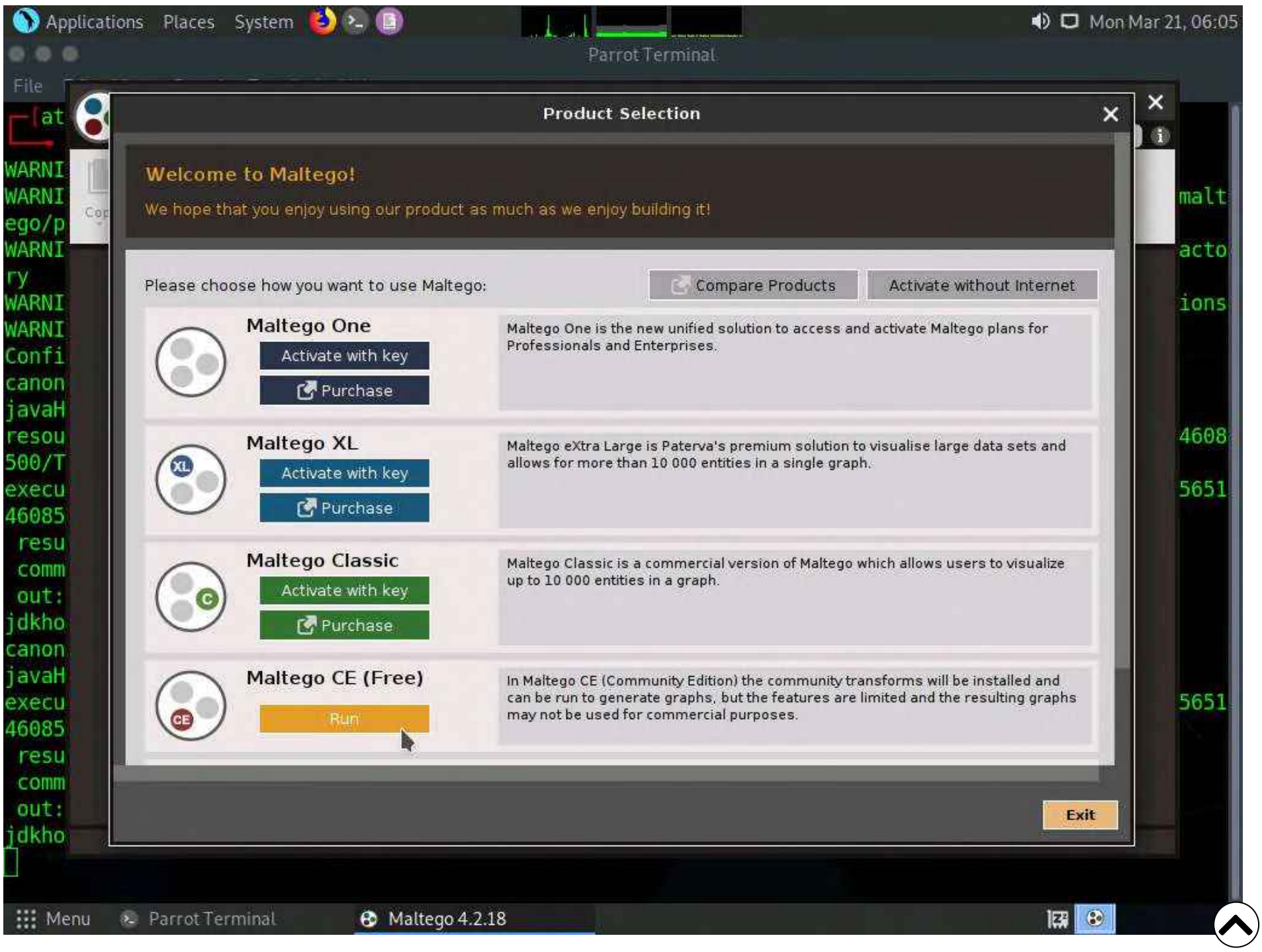
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine, open a terminal and type **sudo maltego** and press **Enter** to launch **Maltego**.

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

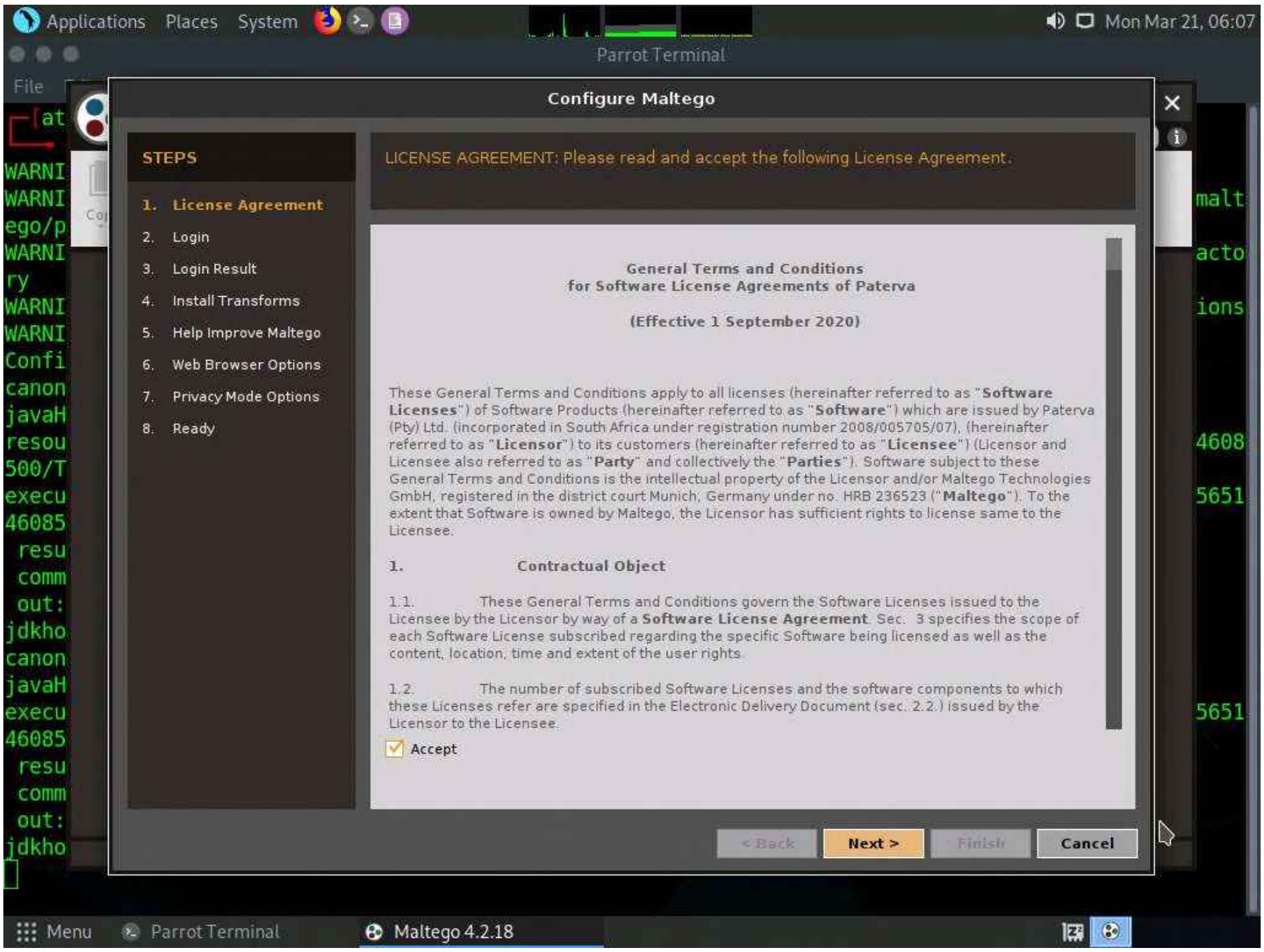


2. A **Product Selection** wizard appears on the Maltego GUI; click **Run** from **Maltego CE (Free)** option.

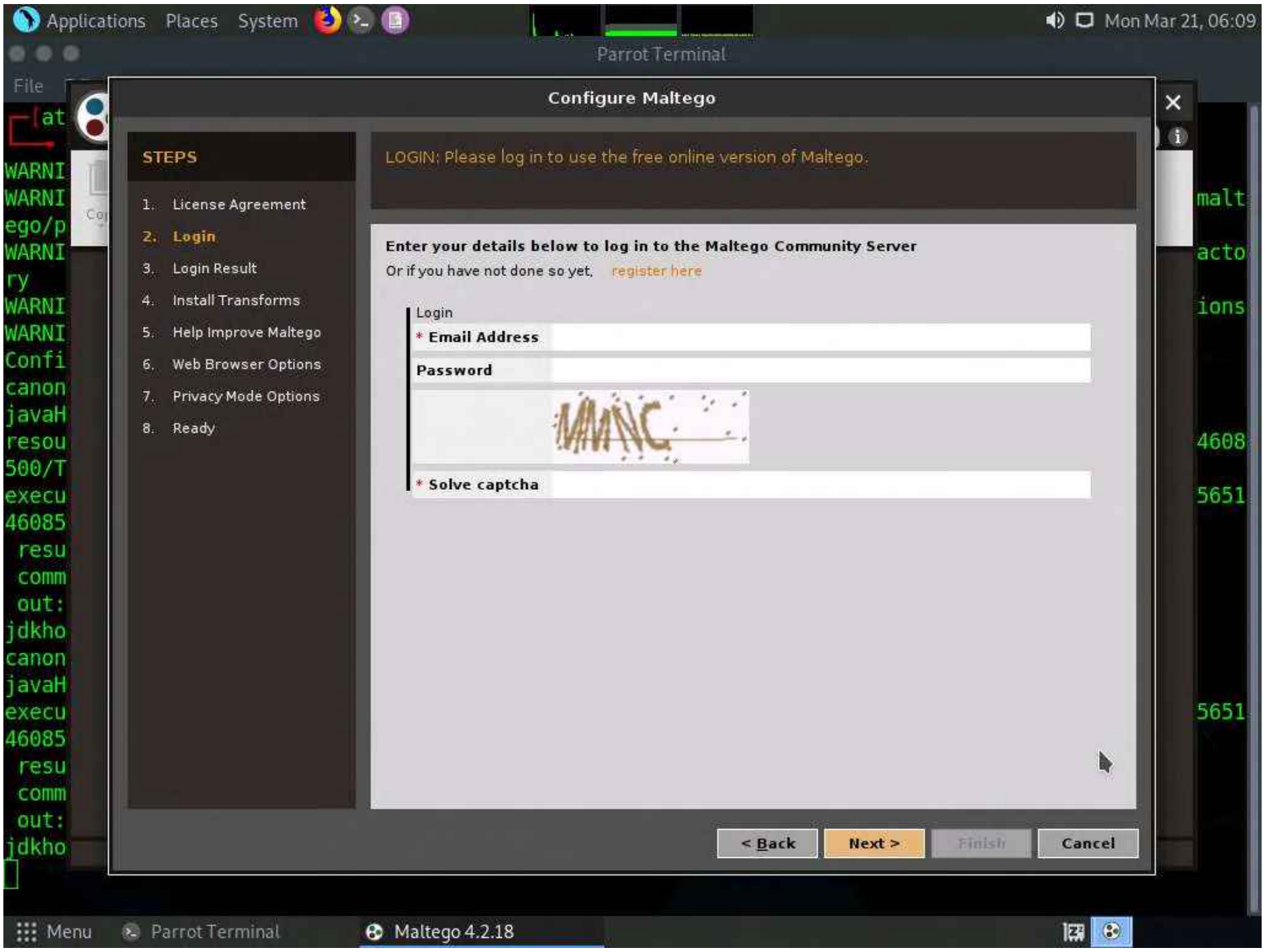
Note: If the **Memory Settings Optimized** pop-up appears, click **Restart Now**.



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



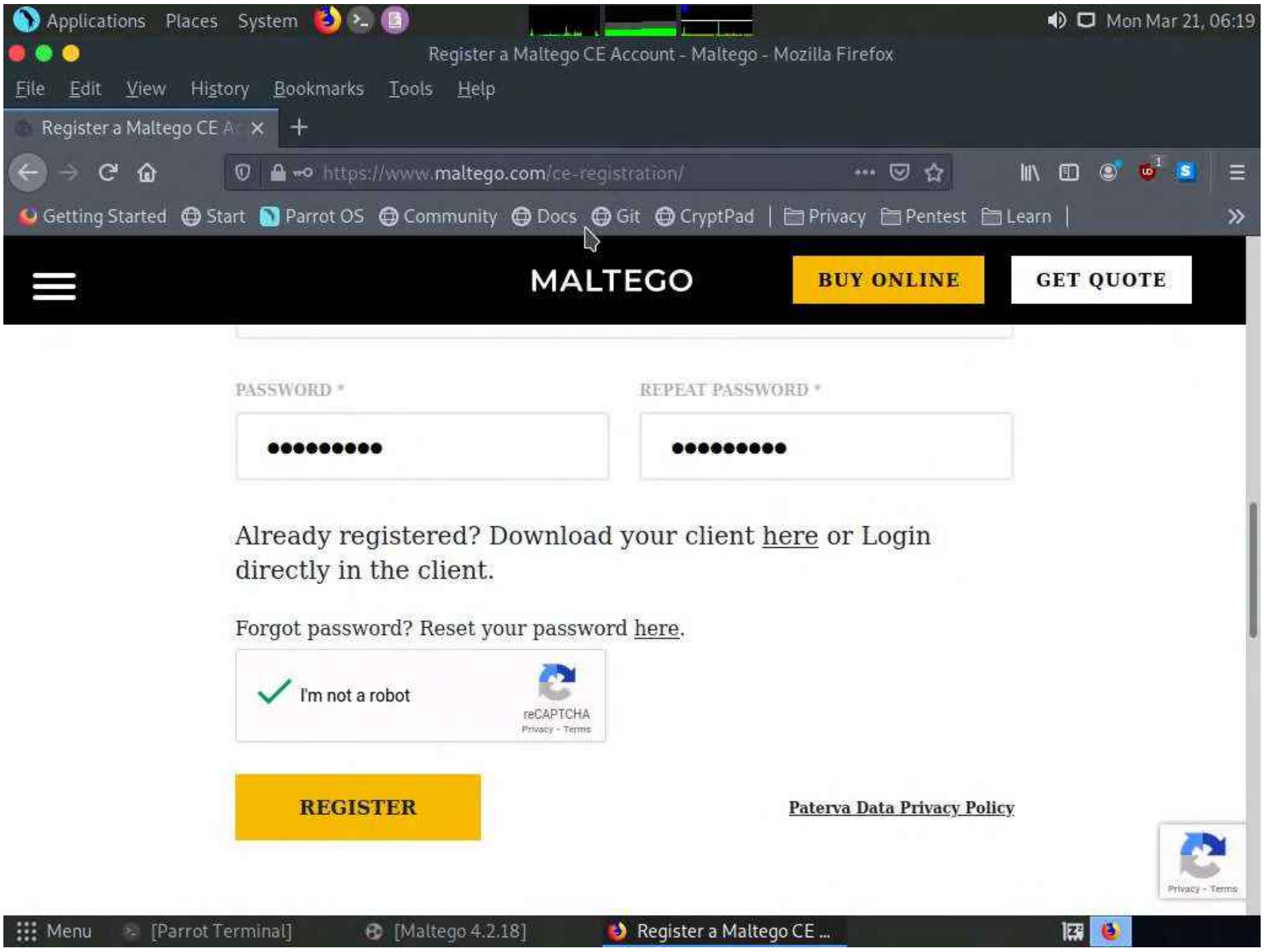
4. You will be redirected to the **Login** section; leave the **Maltego** window as it is and click **Firefox** icon from the top-section of the window to launch the Firefox browser.



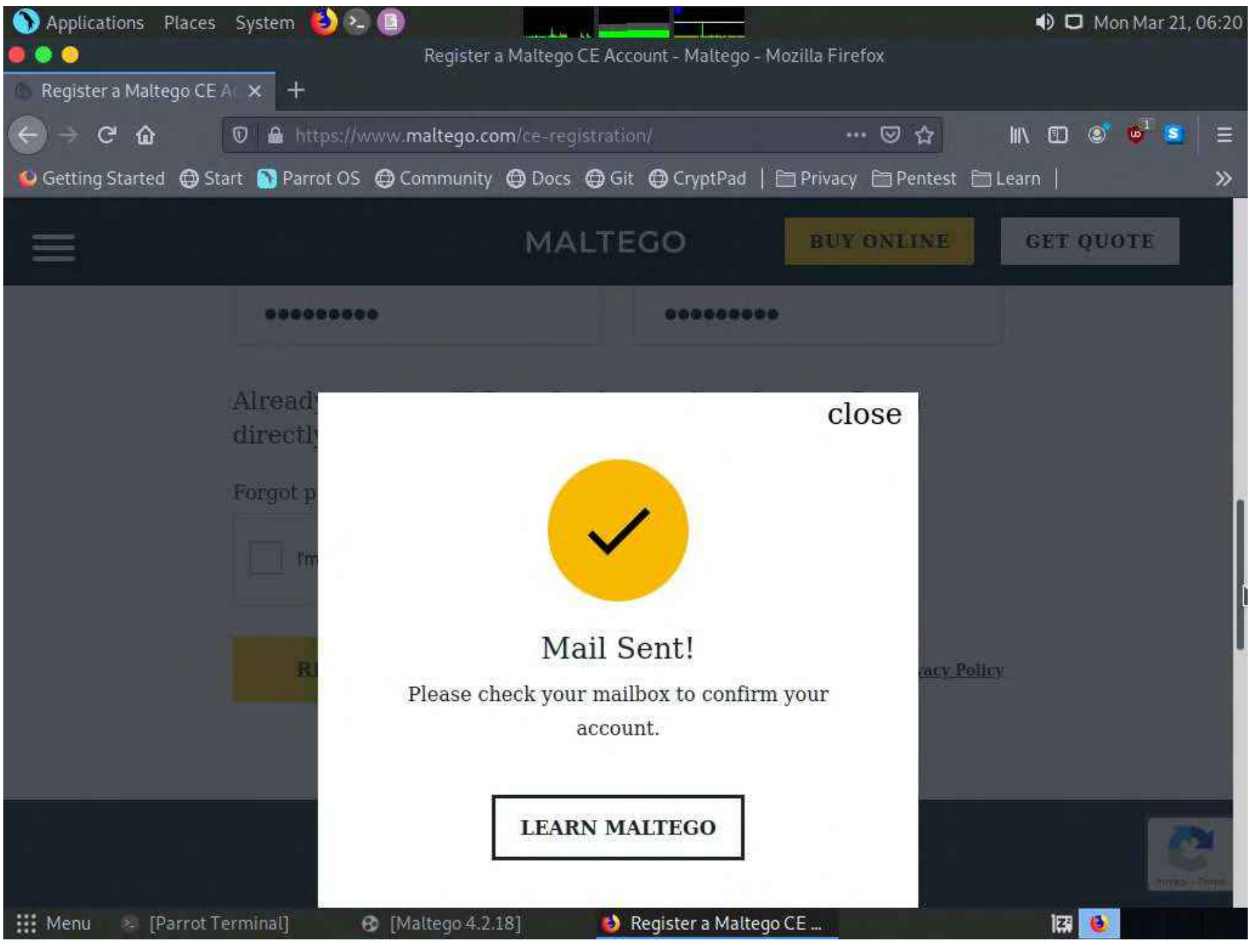
5. The **Firefox** window appears in the address type **https://www.maltego.com/ce-registration** and press **Enter**.

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.

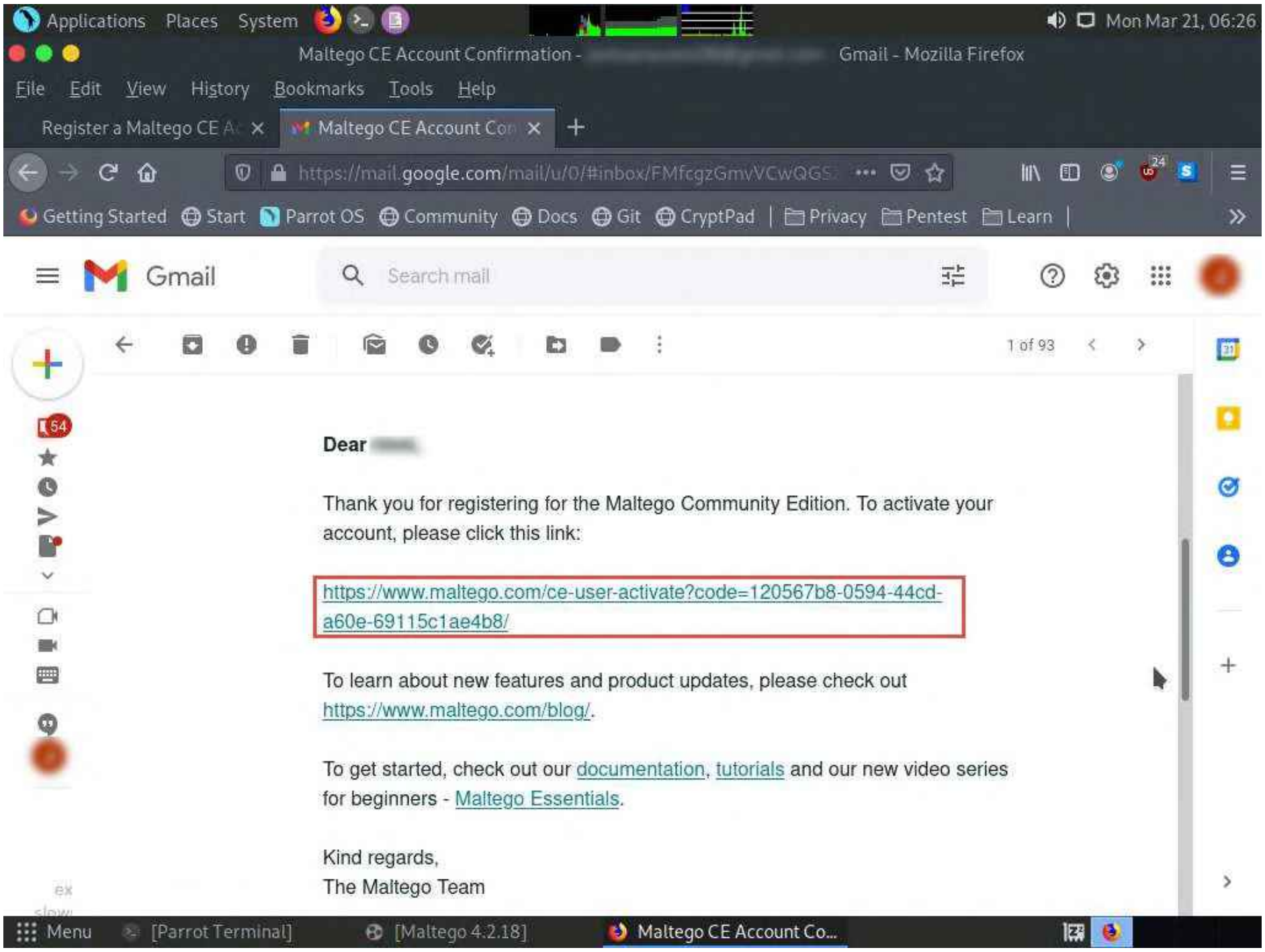
Note: If cookie notification appears in the lower section of the browser, click **Accept**.



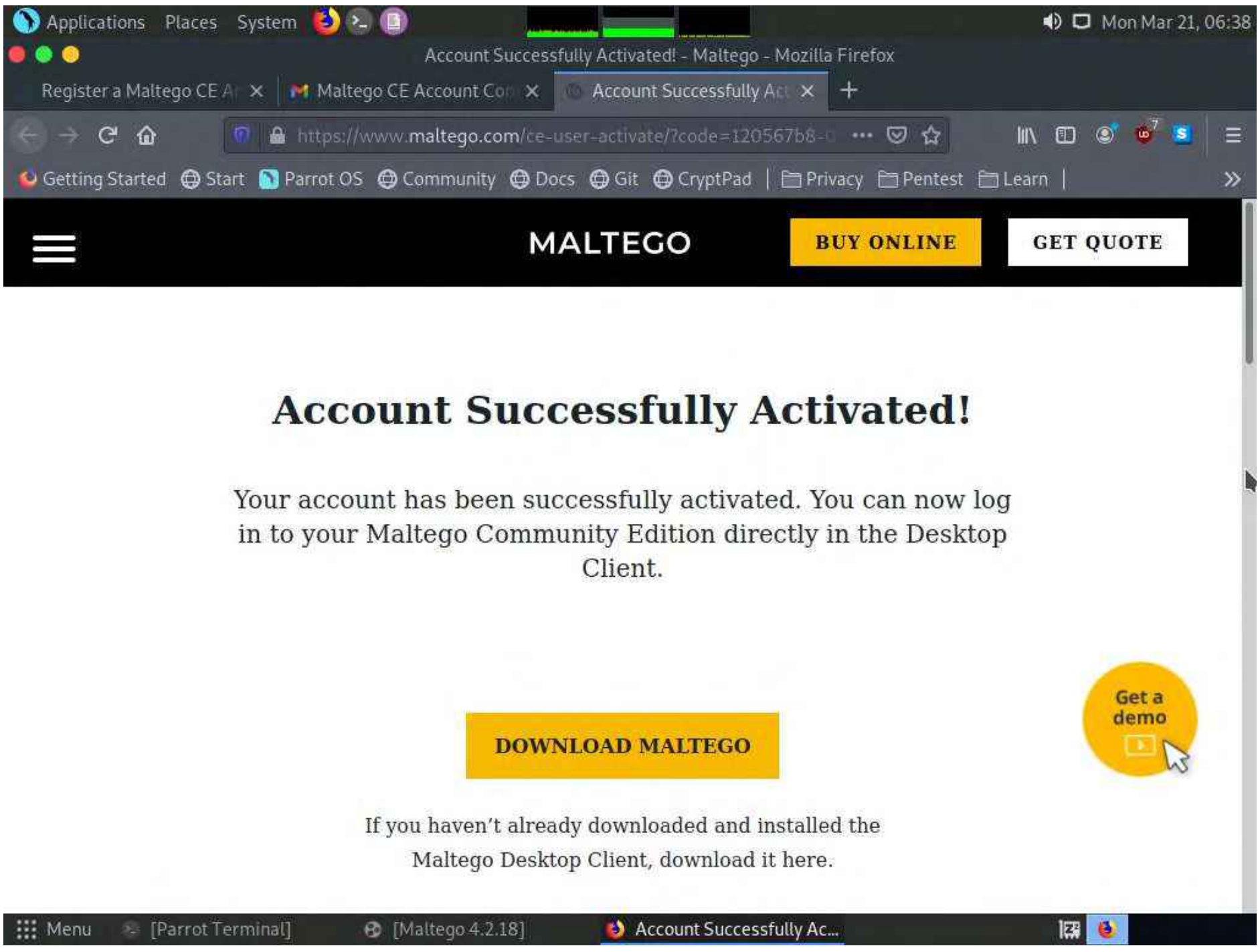
7. **Mail Sent!** notification appears, click **close** button.



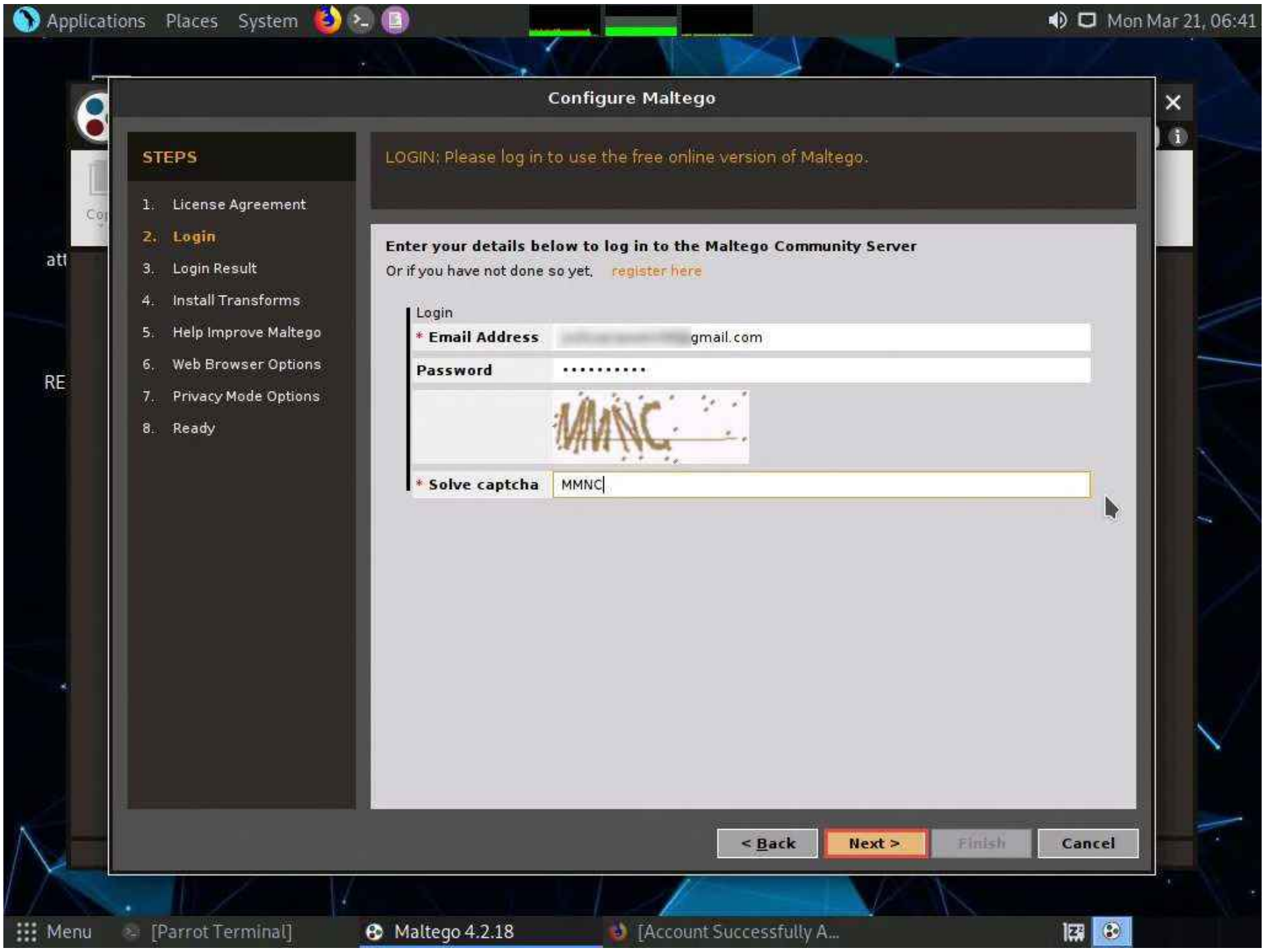
8. Now, in the browser window, click '**+**' icon to open a new tab. Open the email account given at the time of registration in **Step#6**. Open the mail from **Maltego** and click on the activation link.



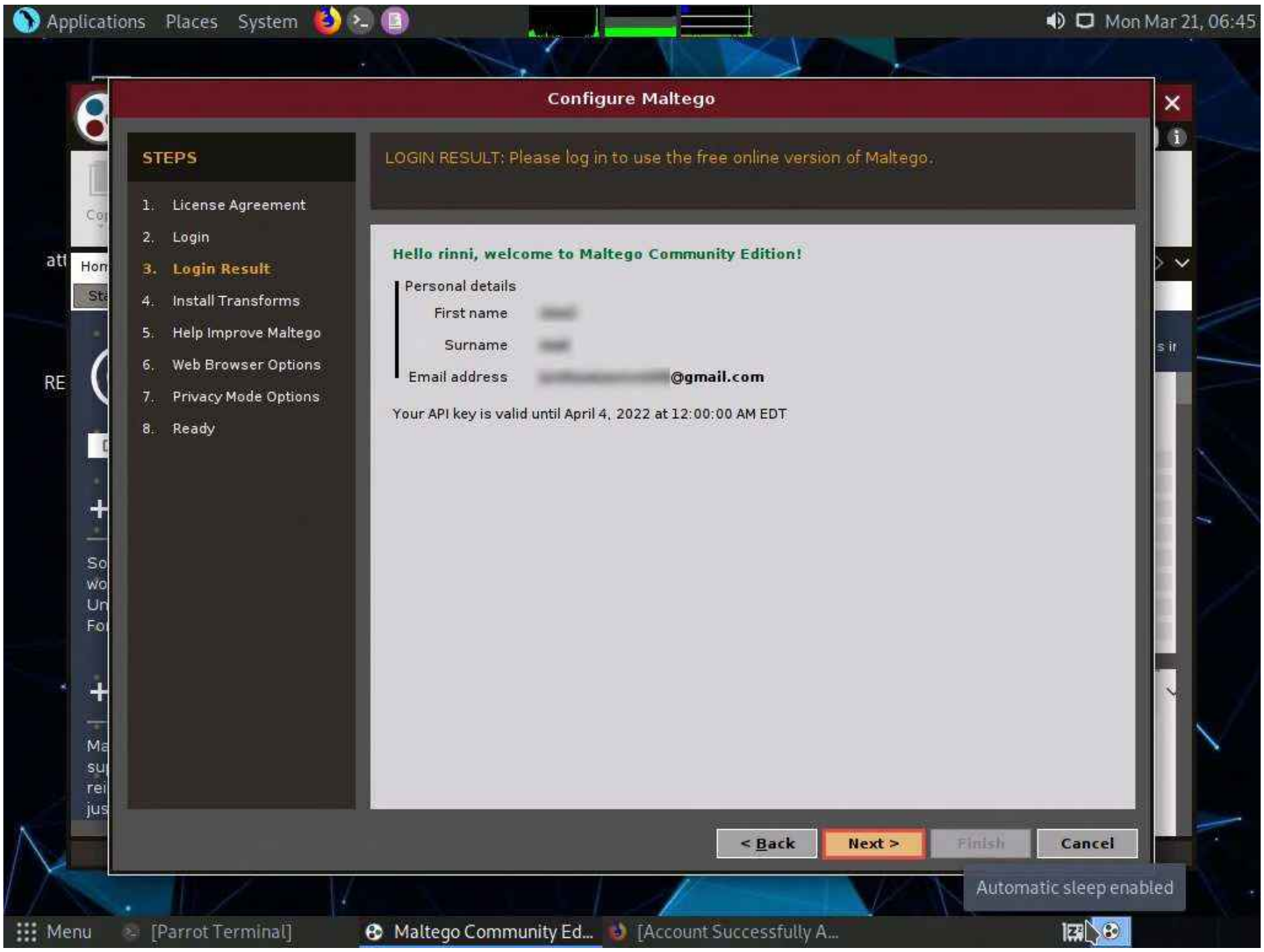
9. **Account Successfully Activated!** page appears, as shown in the screenshot.



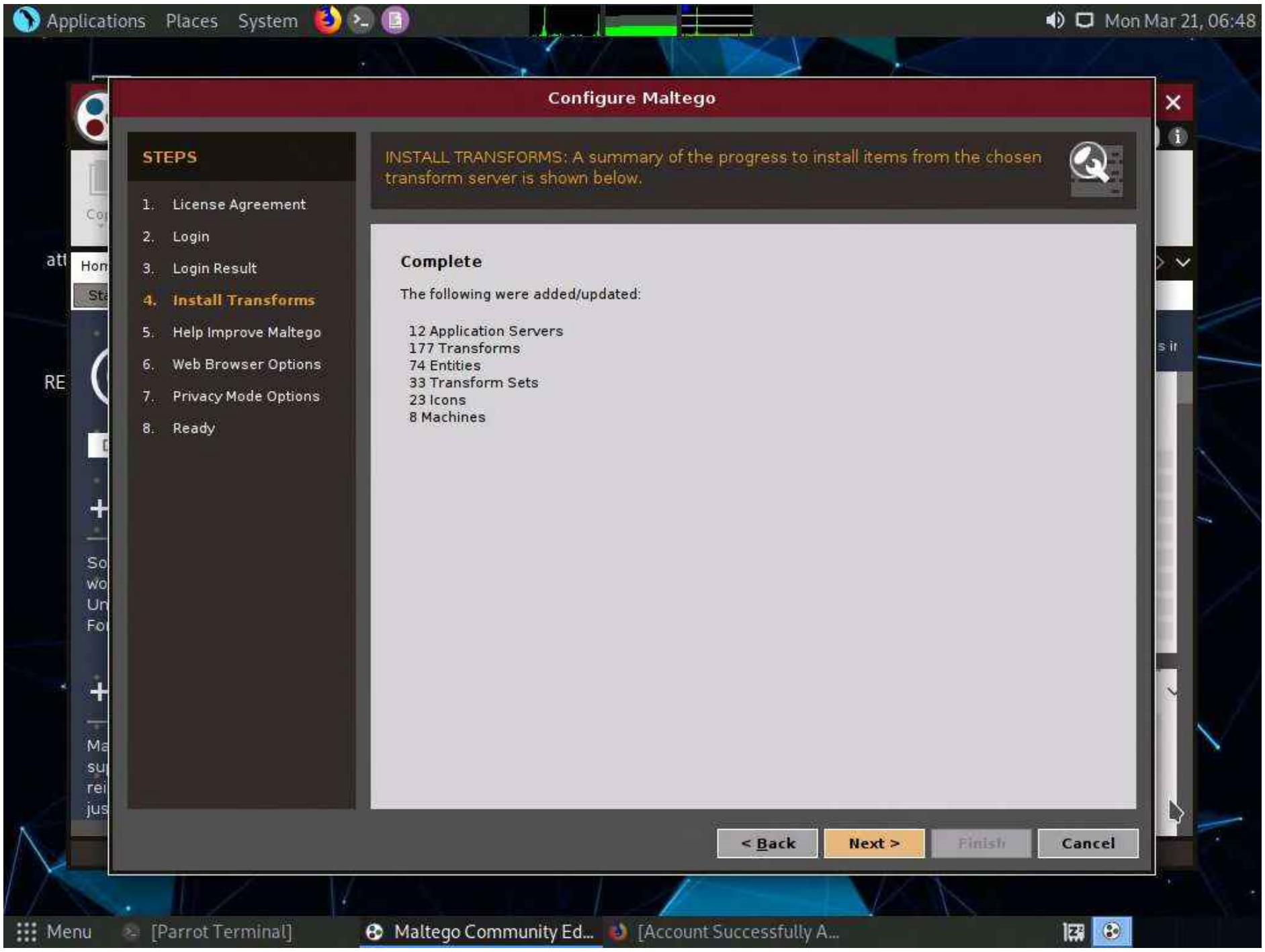
10. Minimize the web browser and go back to the setup wizard and enter the **Email Address** and **Password** specified at the time of registration; solve the captcha and click **Next**.



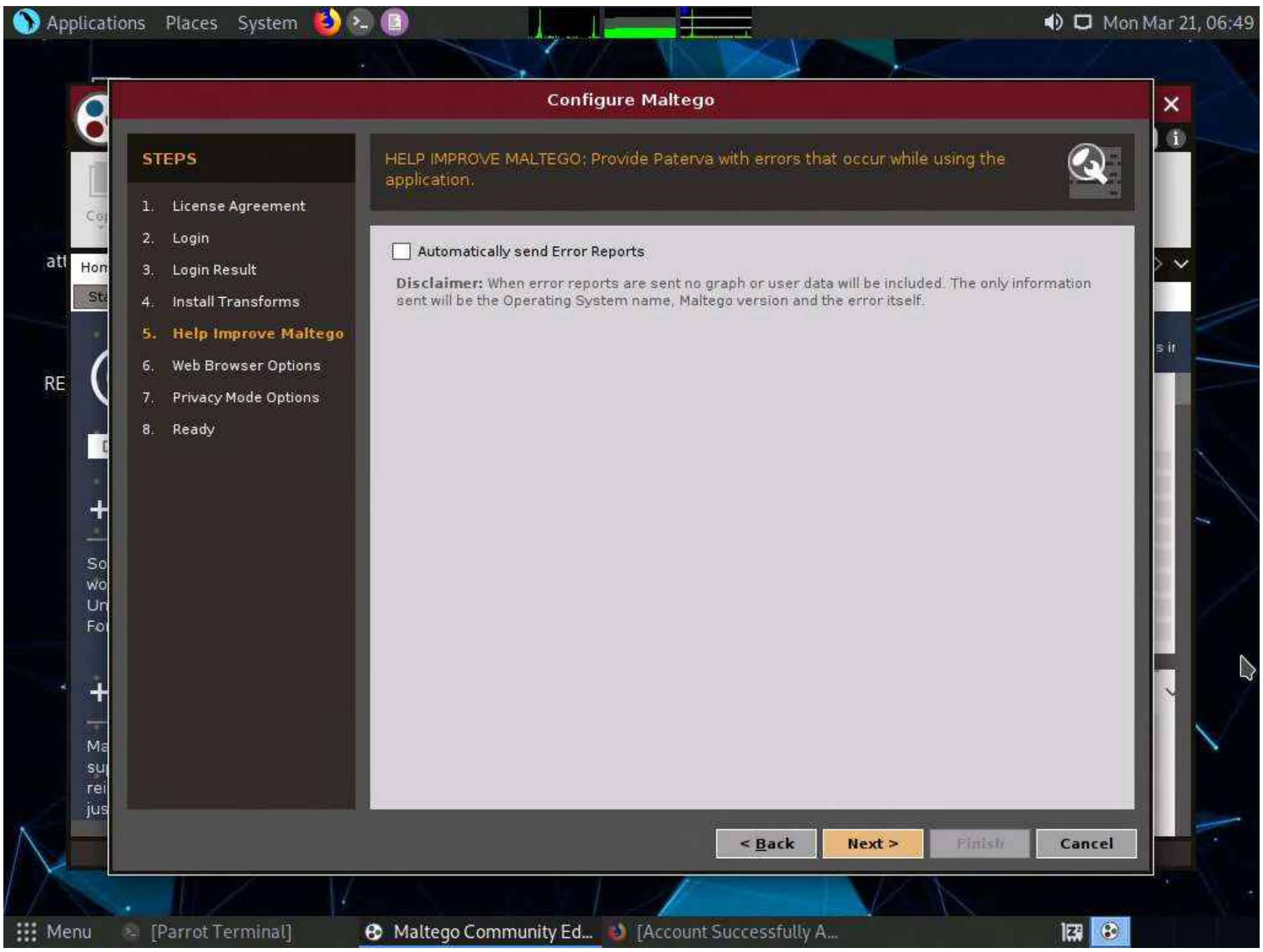
11. The **Login Result** section displays your personal details; click **Next**.



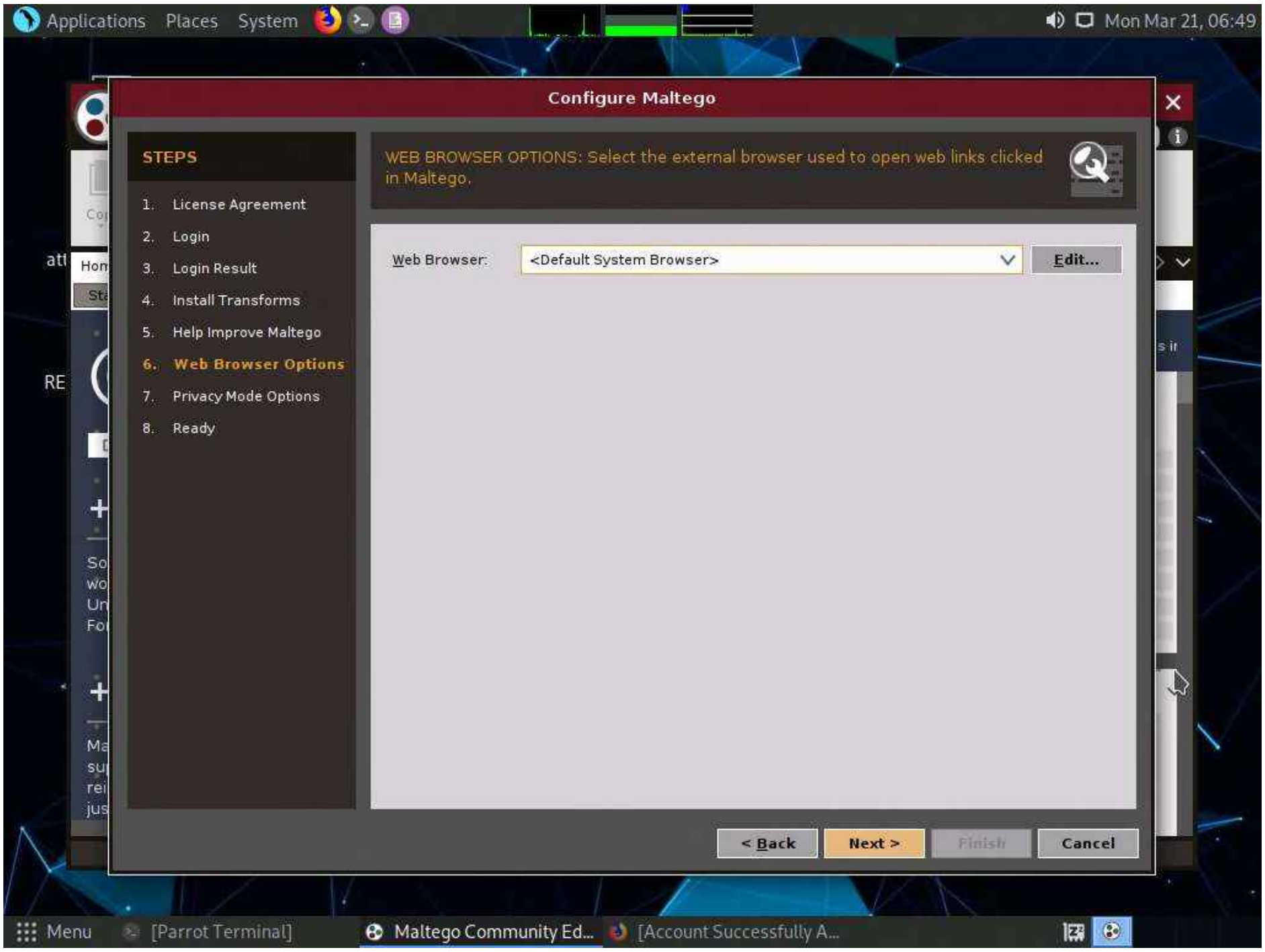
12. The **Install Transforms** section appears, which will install items from the chosen transform server. Leave the settings to default and click **Next**.



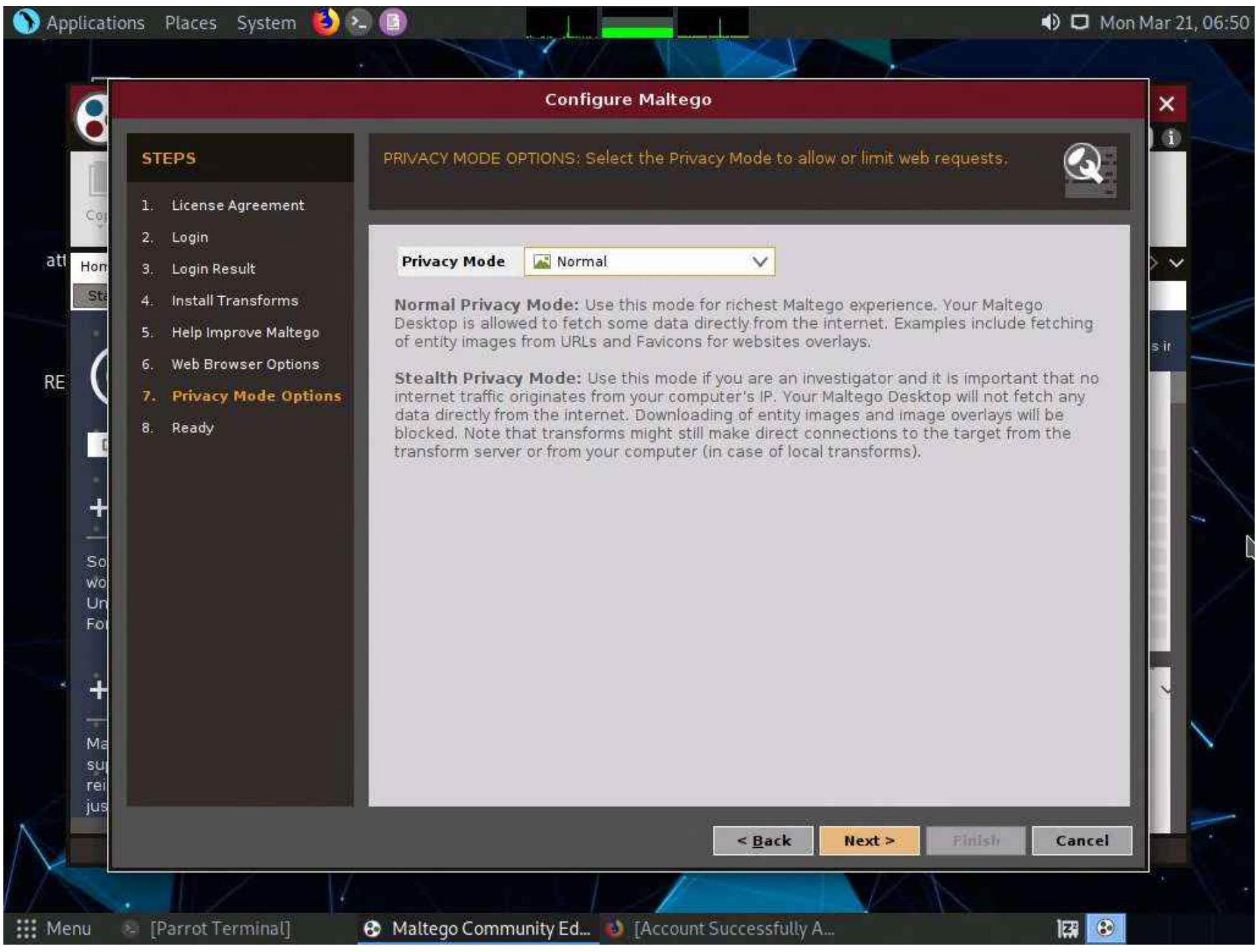
13. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.



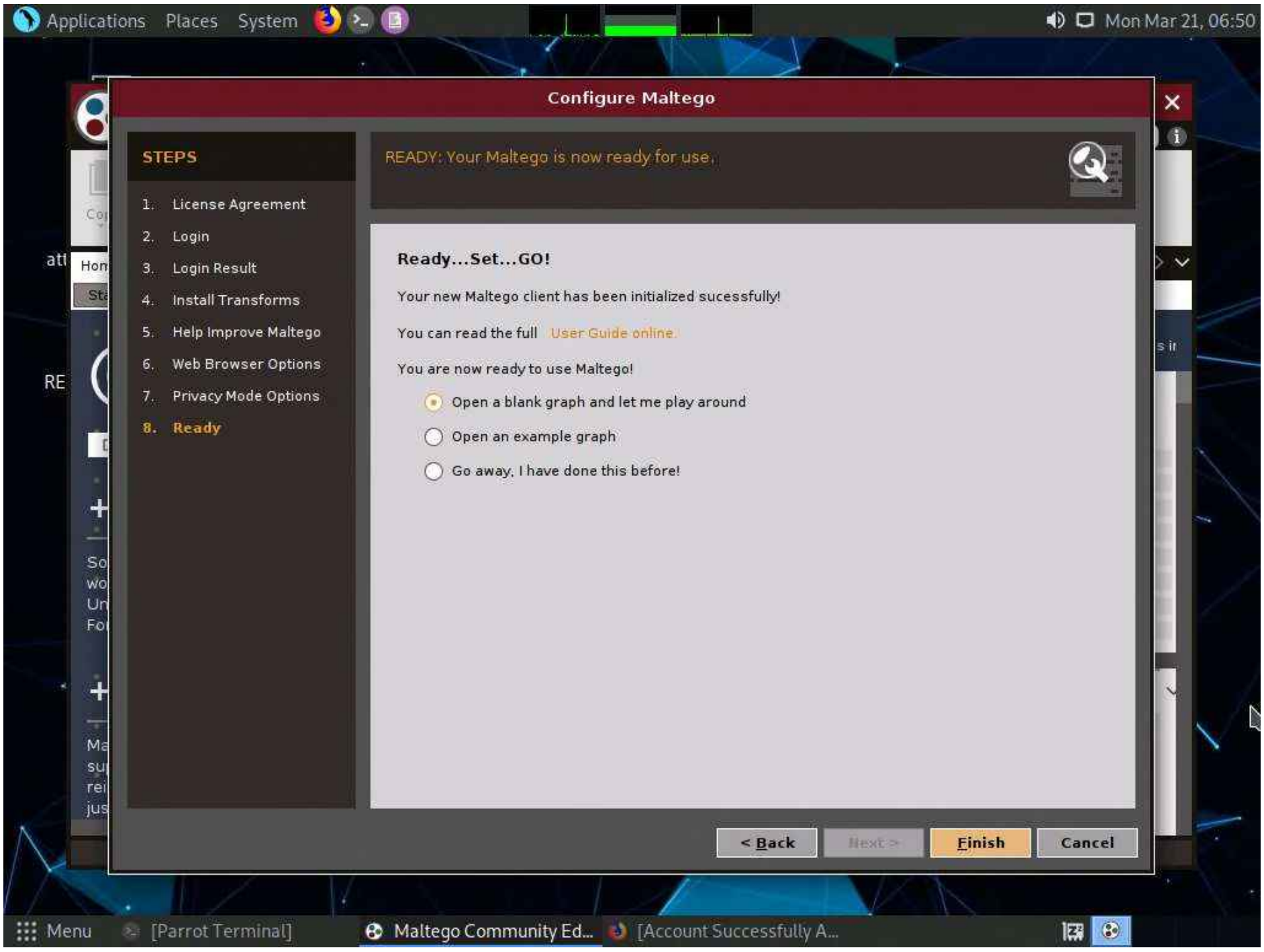
14. The **Web Browser Options** section appears. Leave the options set to default and click **Next**.



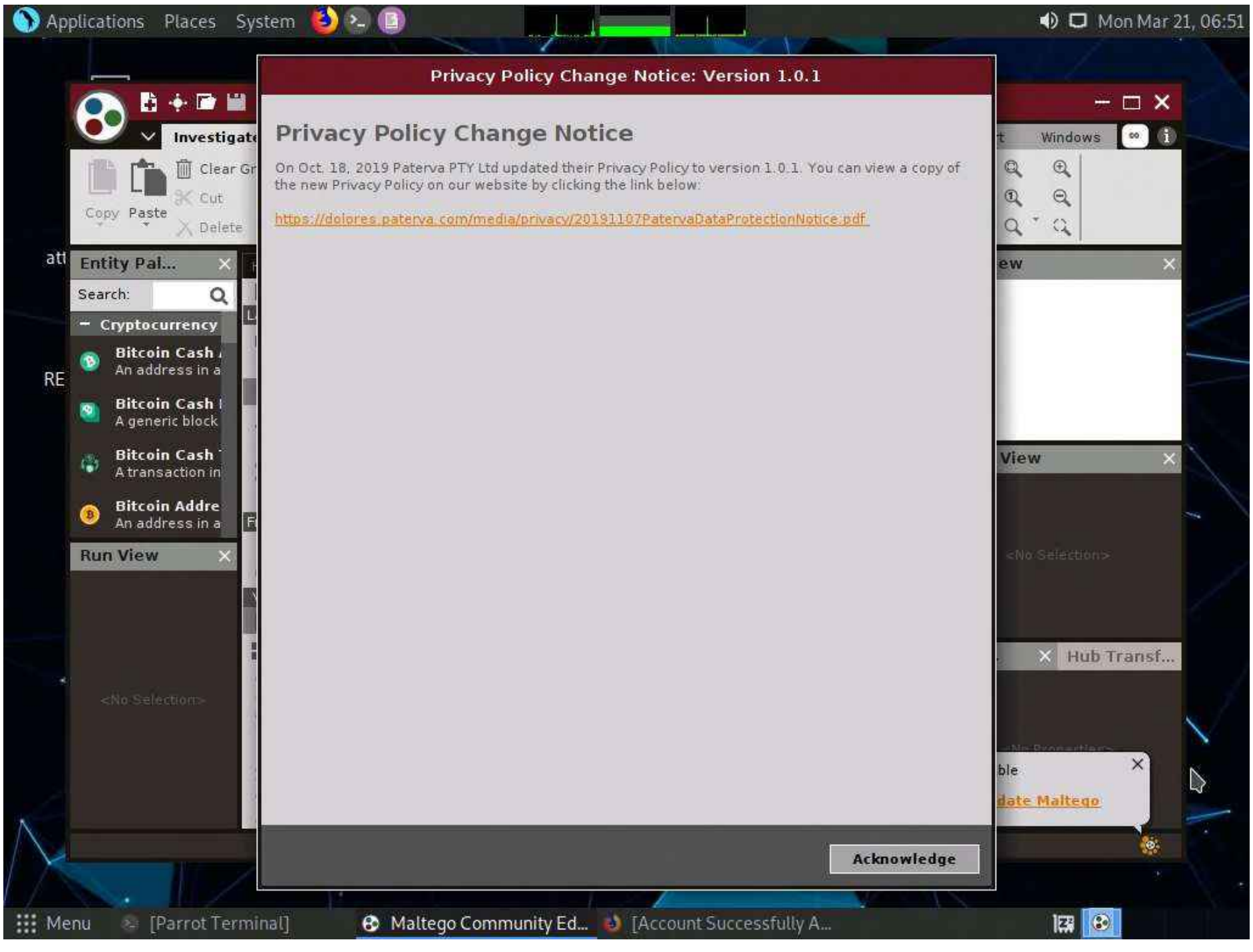
15. The **Privacy Mode Options** section appears. Leave the options set to default and click **Next**.



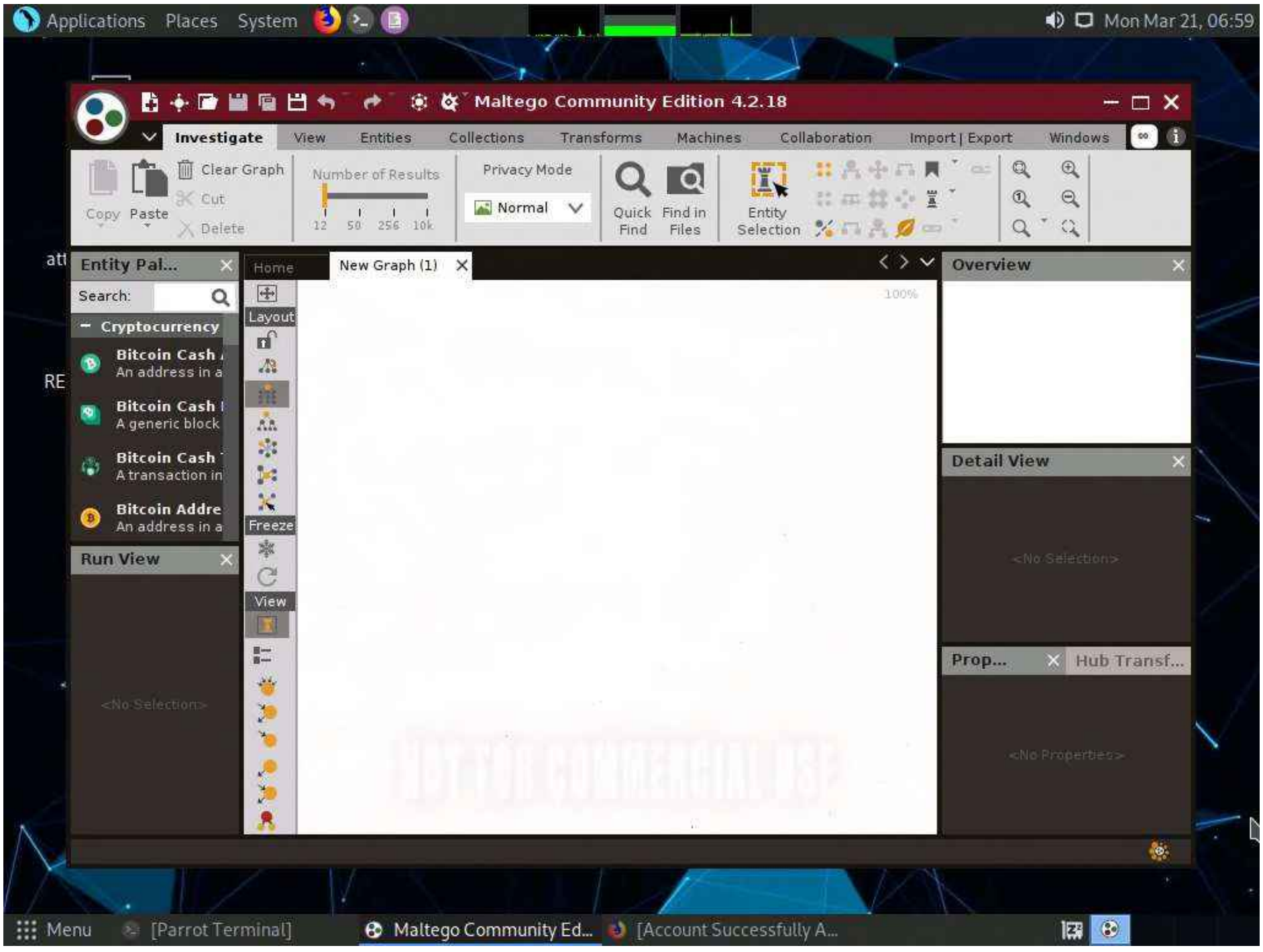
16. The **Ready** section appears, select **Open a blank graph and let me play around** option and click **Finish**.



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.

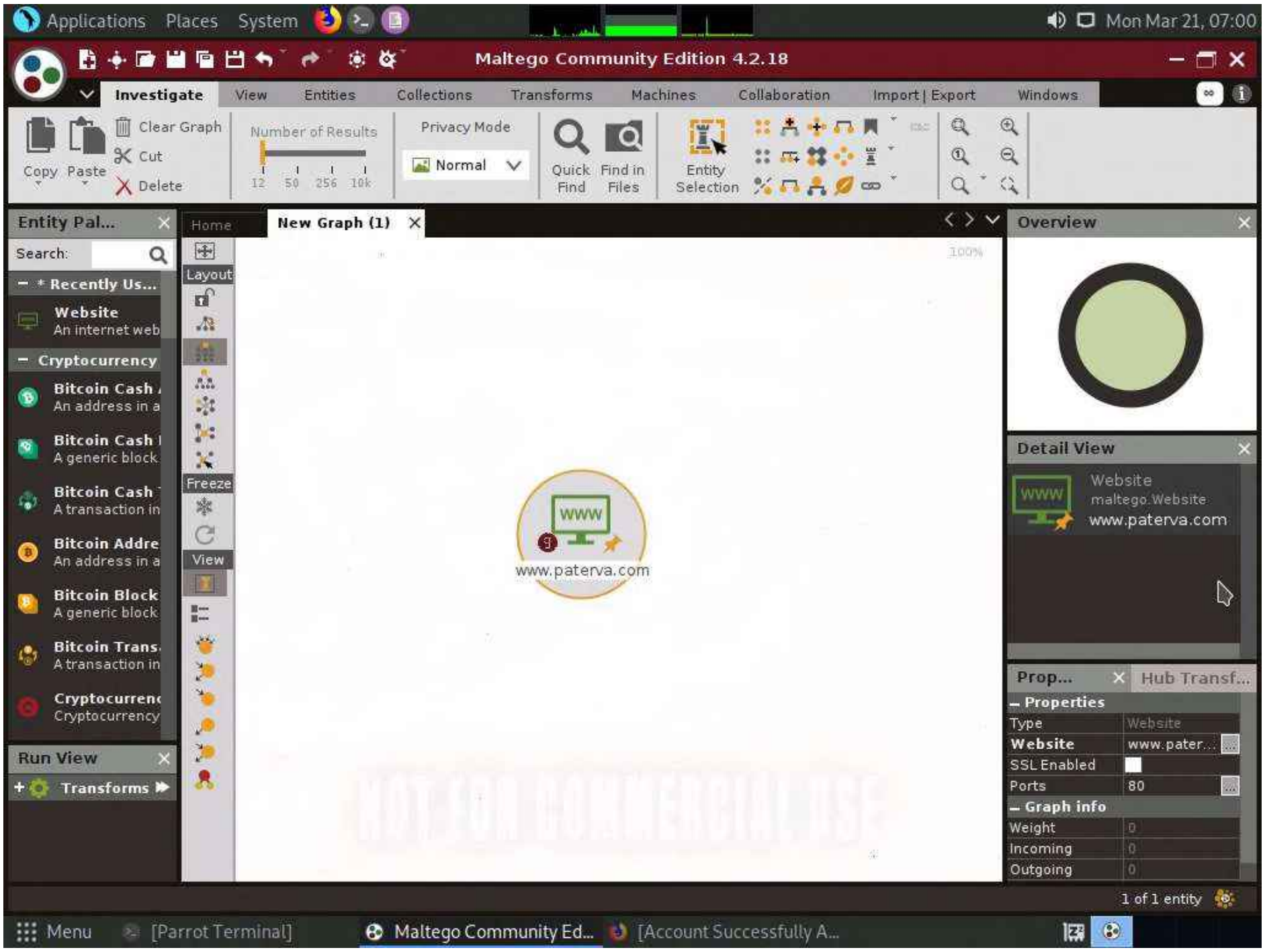


19. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS**, **DNS Name**, **Domain**, **IPv4 Address**, **URL**, **Website**,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

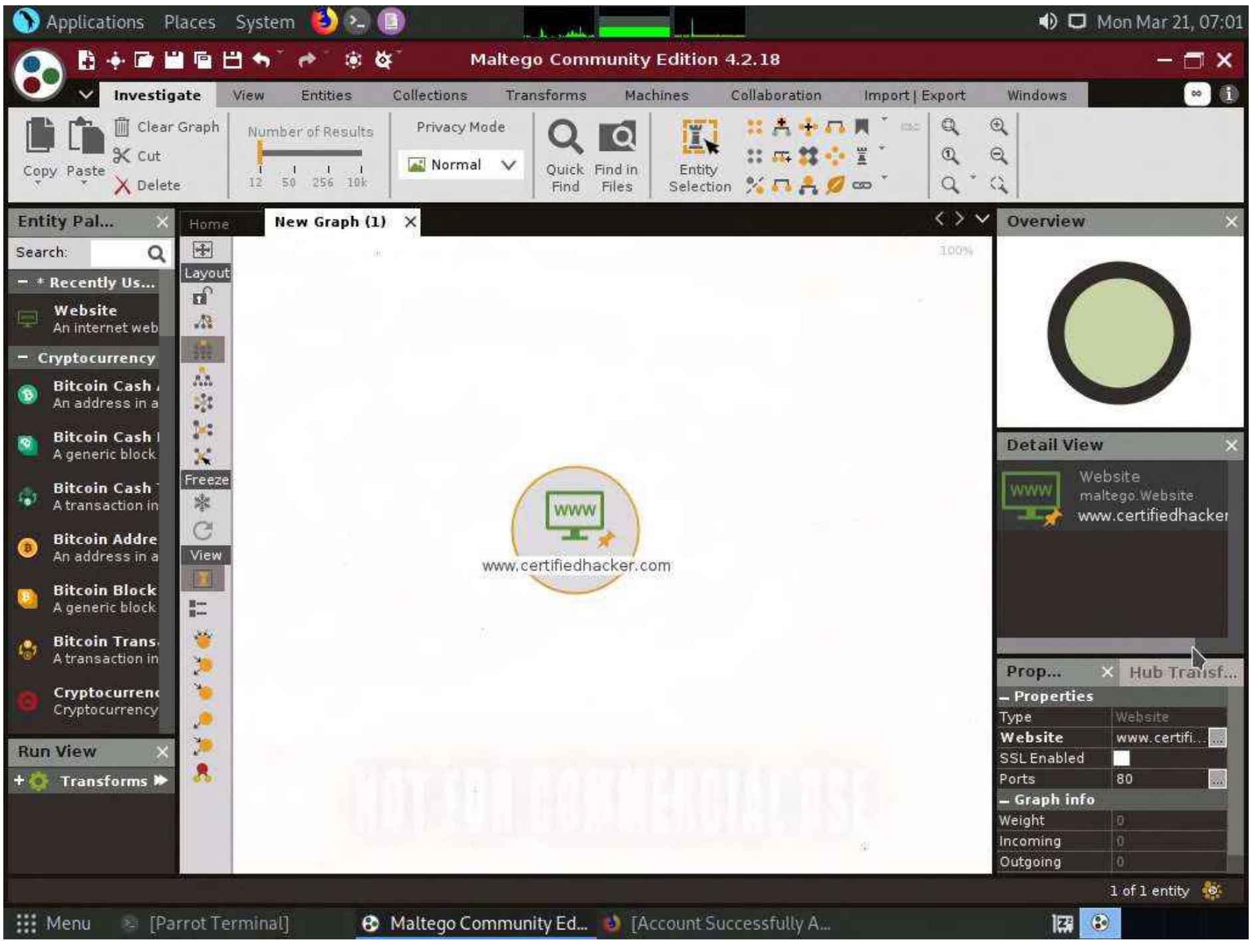
20. Drag the **Website** entity onto the **New Graph (1)** window.

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

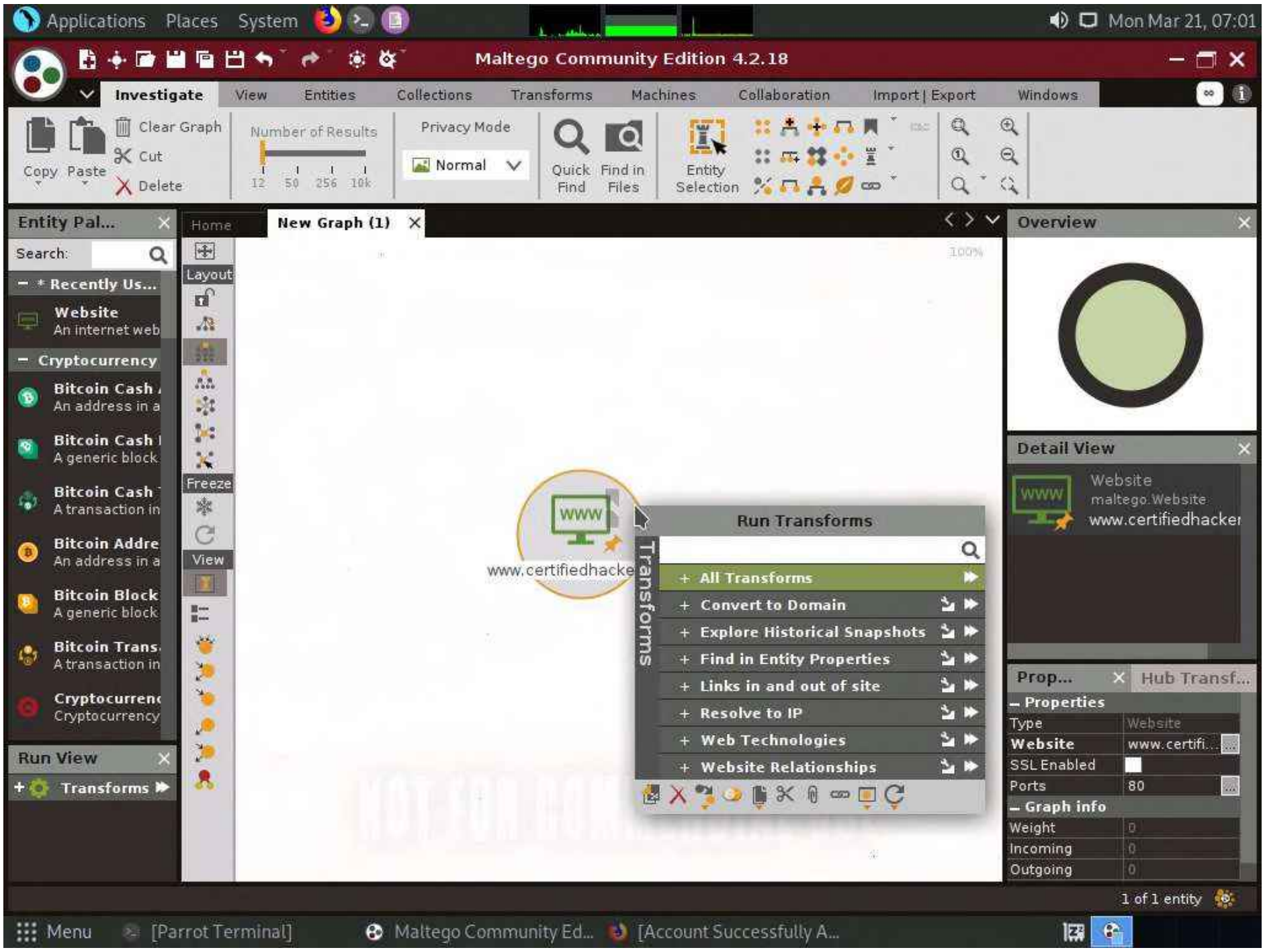
> Note: If you are not able to view the entity as shown in the screenshot, click in **the New Graph (1)** window and **scroll up**, which will increase the size of the entity.



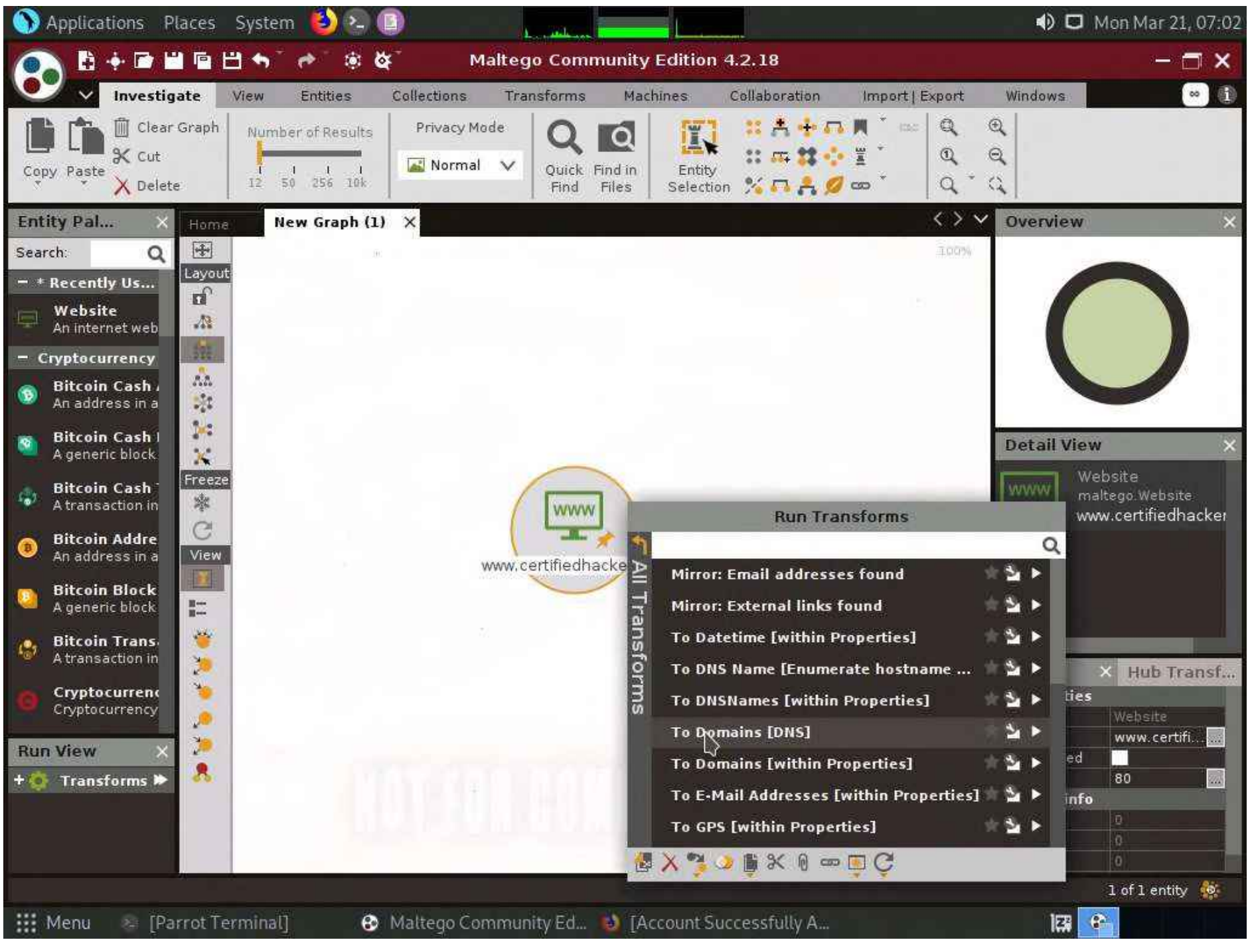
22. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press **Enter**.



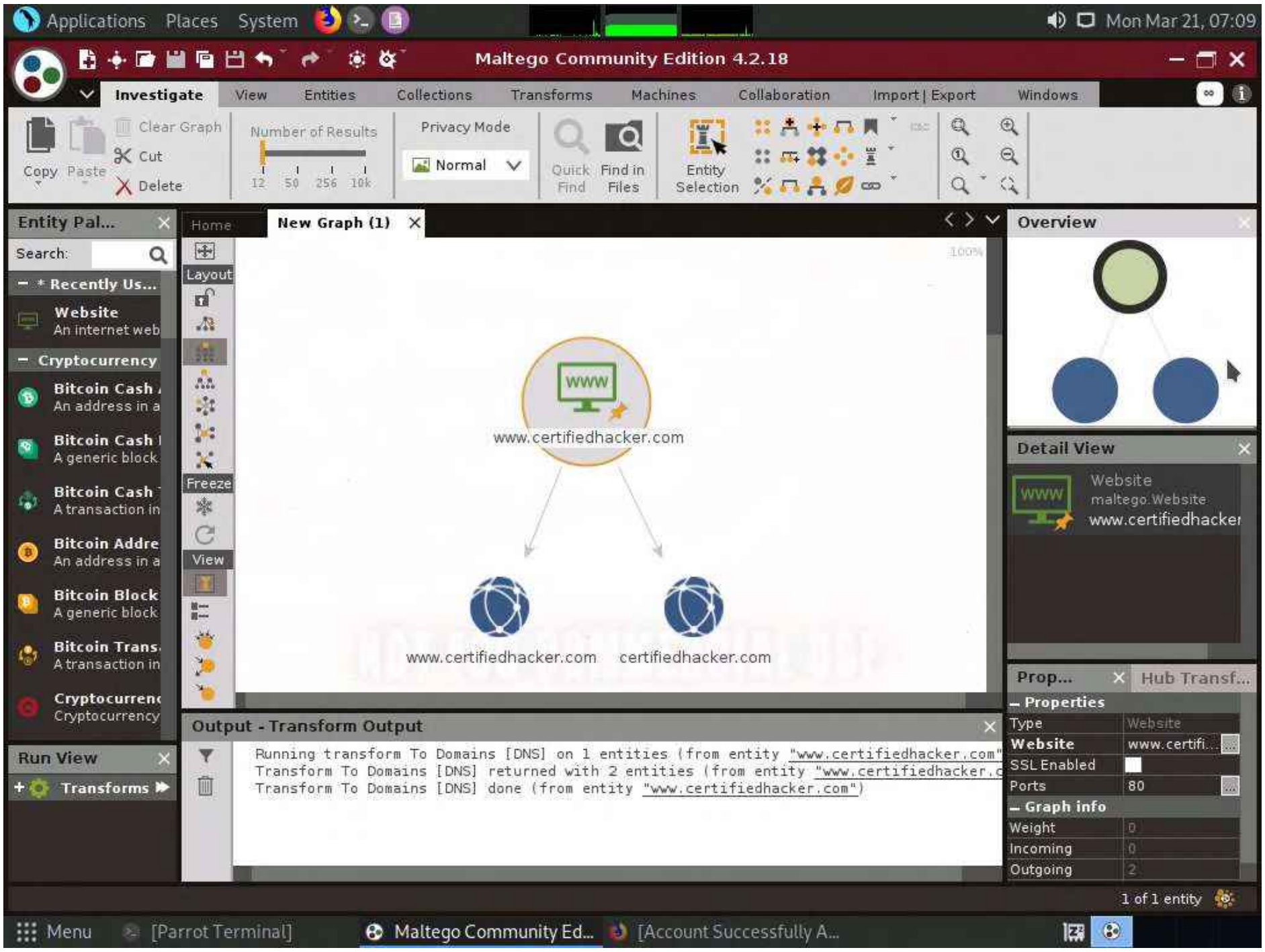
23. Right-click the entity and select **All Transforms**.



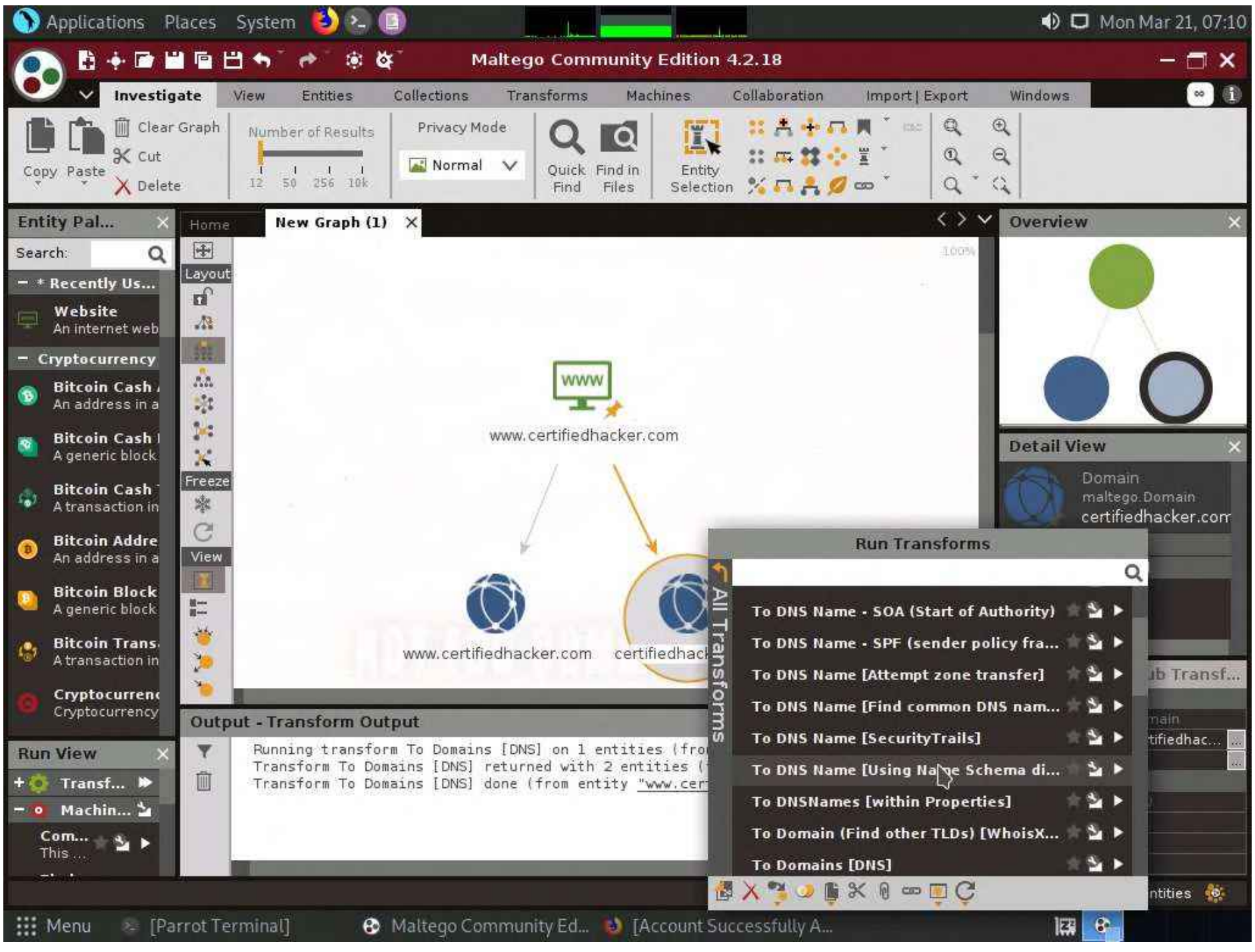
24. The **Run Transform(s)** list appears; click **To Domains [DNS]**.



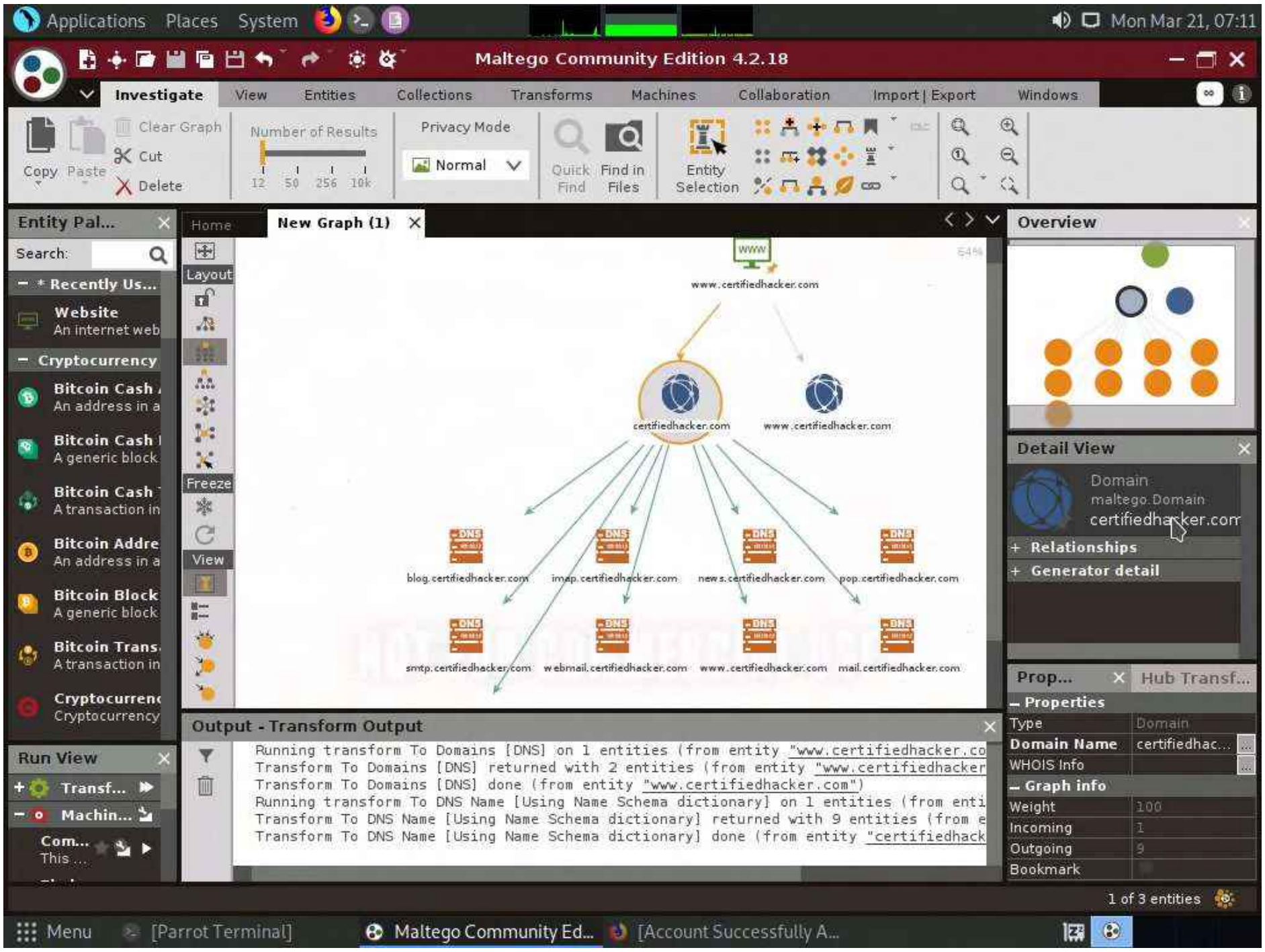
25. The domain corresponding to the website displays, as shown in the following screenshot.



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



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.

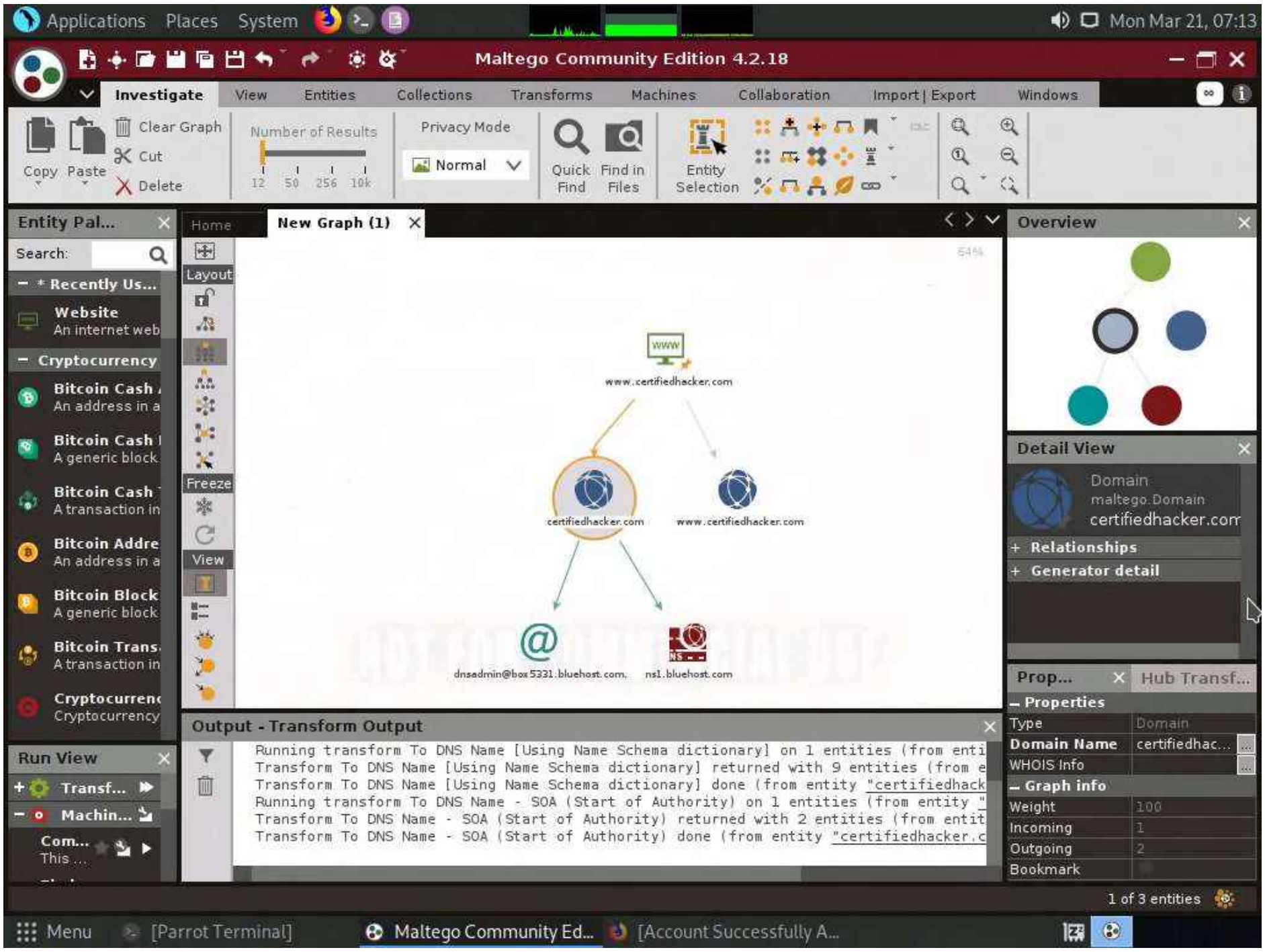


28. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential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

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

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

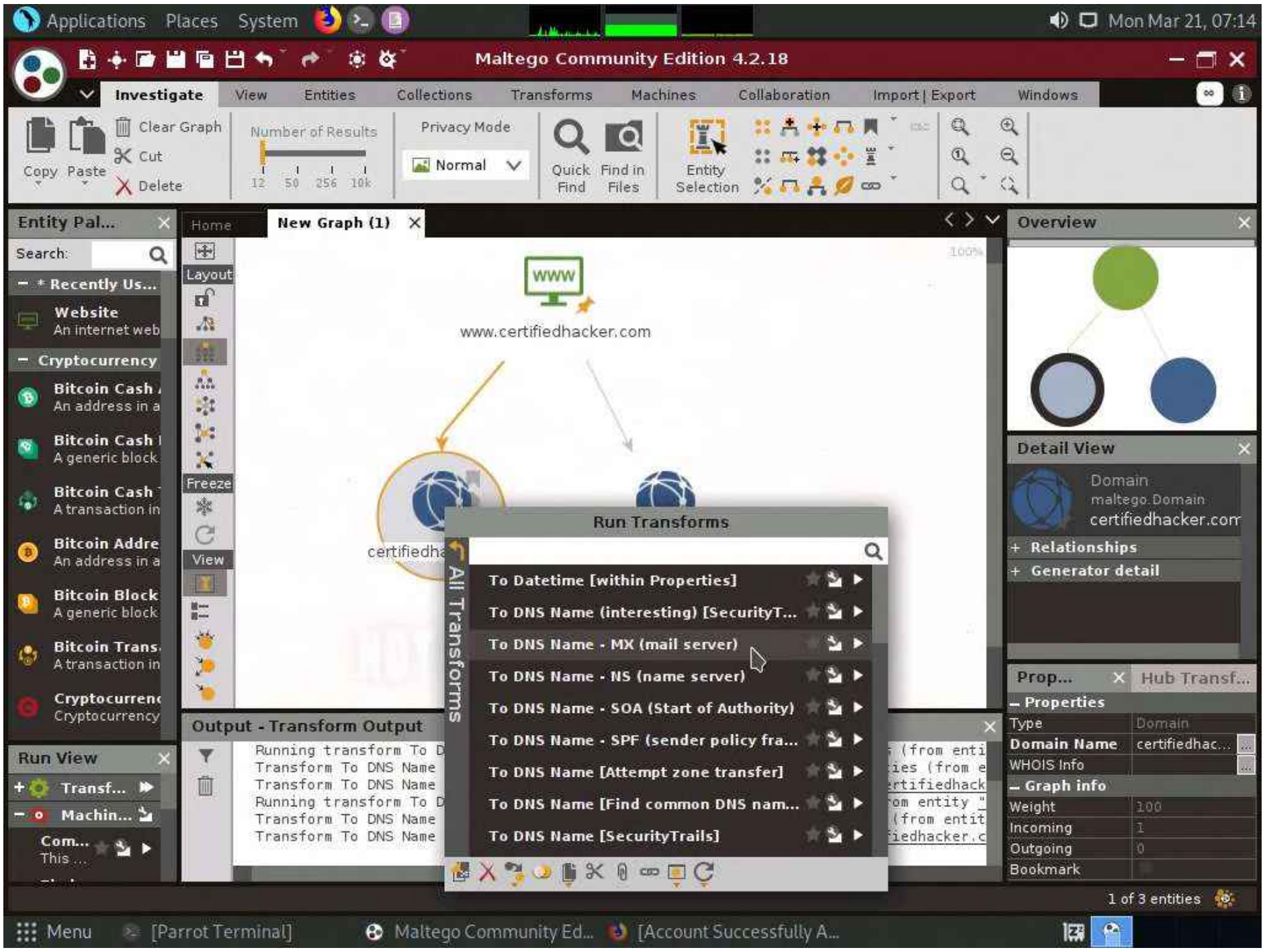
31. This returns the primary name server and the email of the domain administrator, as shown in the following screenshot.



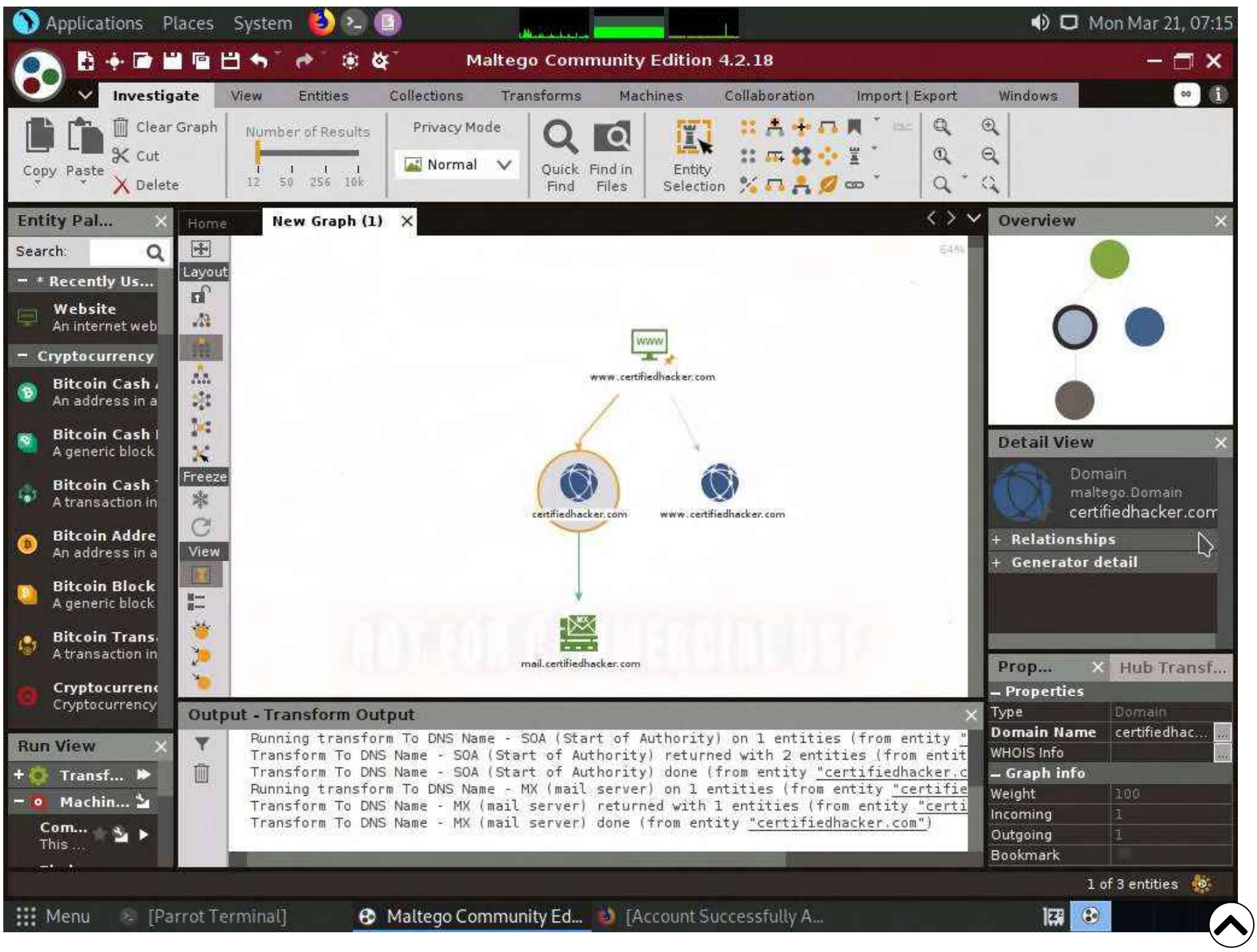
32. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.

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)**.

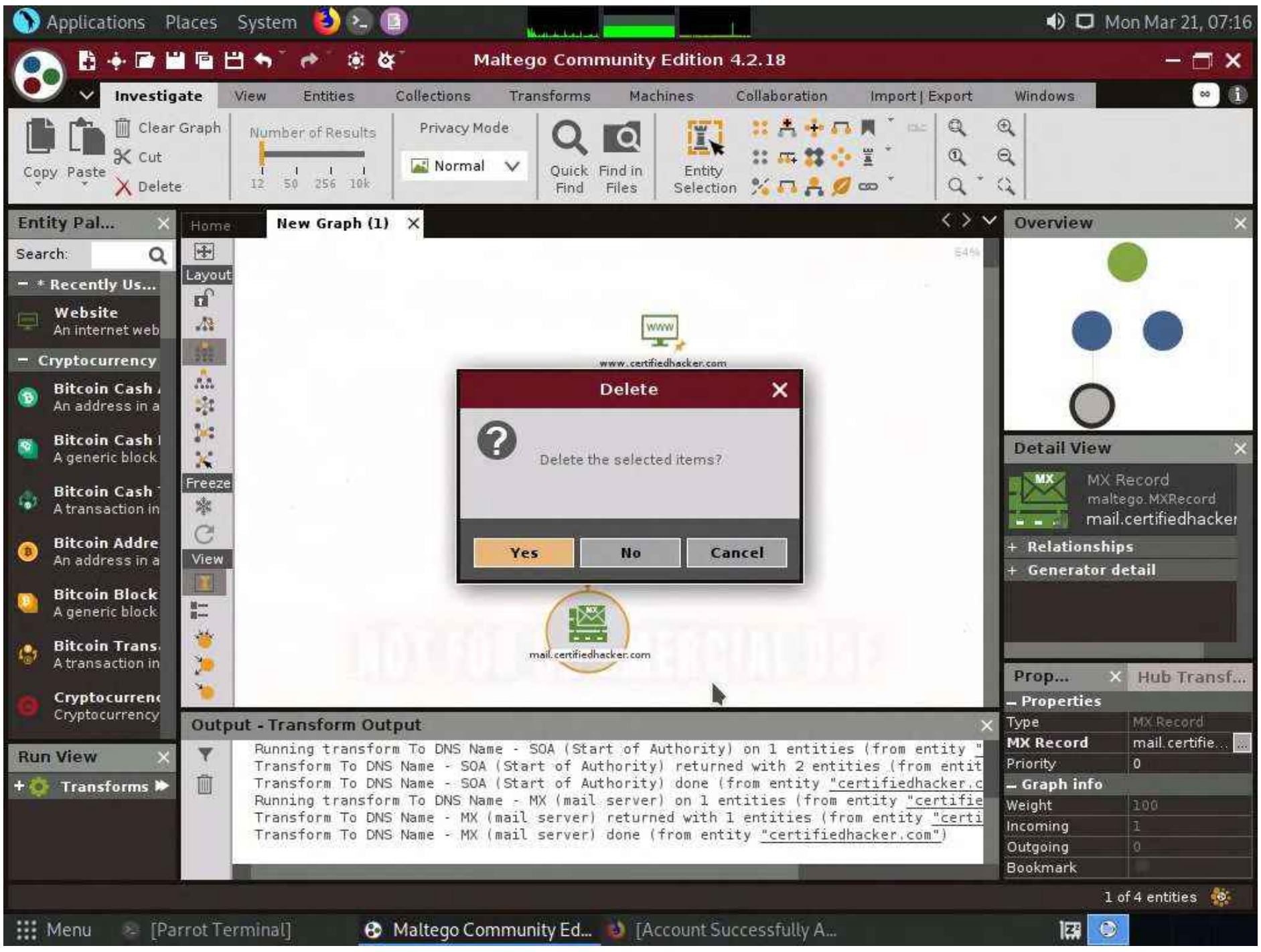


35. This transform returns the mail server associated with the certifiedhacker.com domain, as shown in the following screenshot.

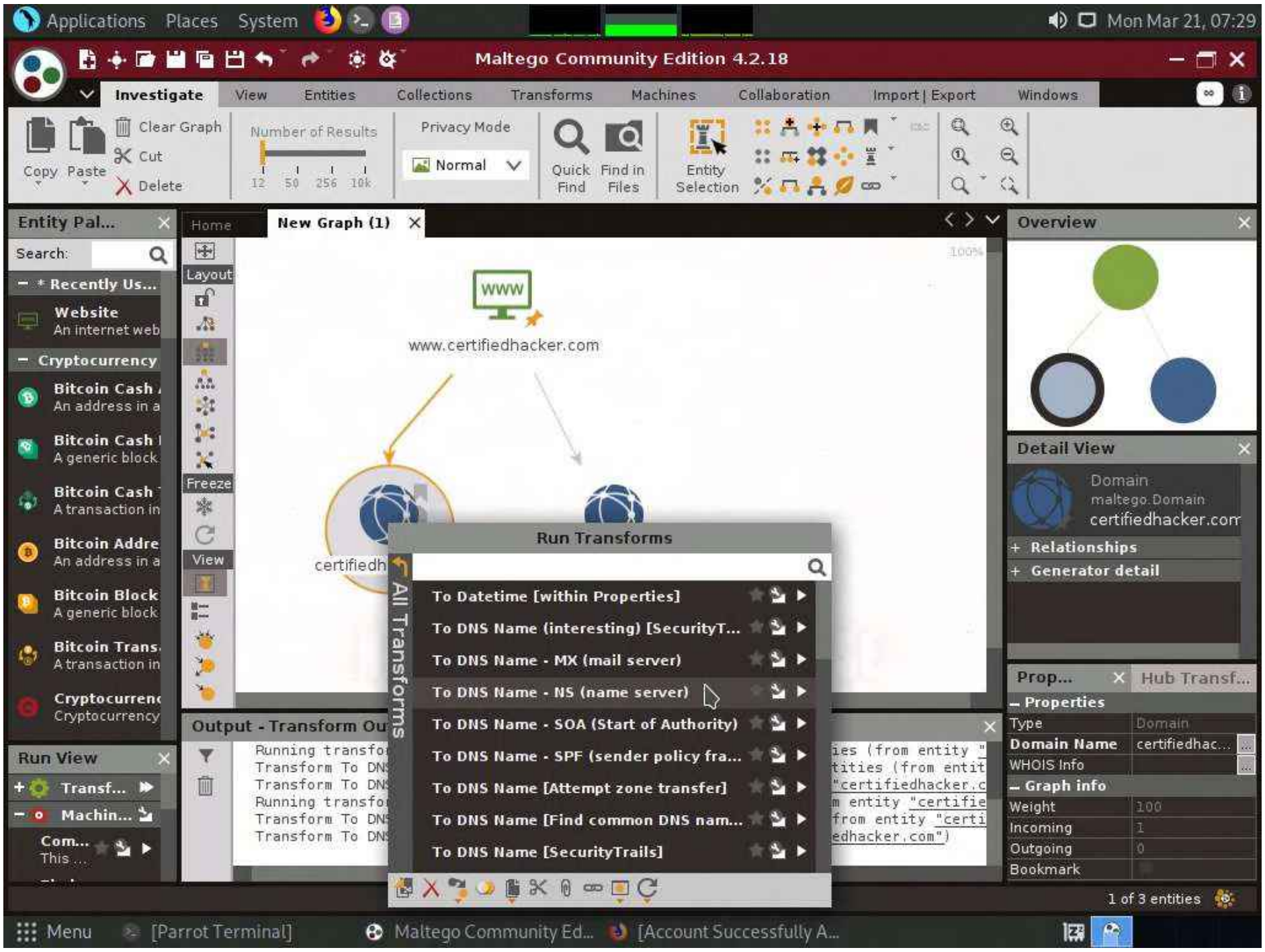


36. By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and, thereby, use it to perform malicious activities such as sending spam e-mails.

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



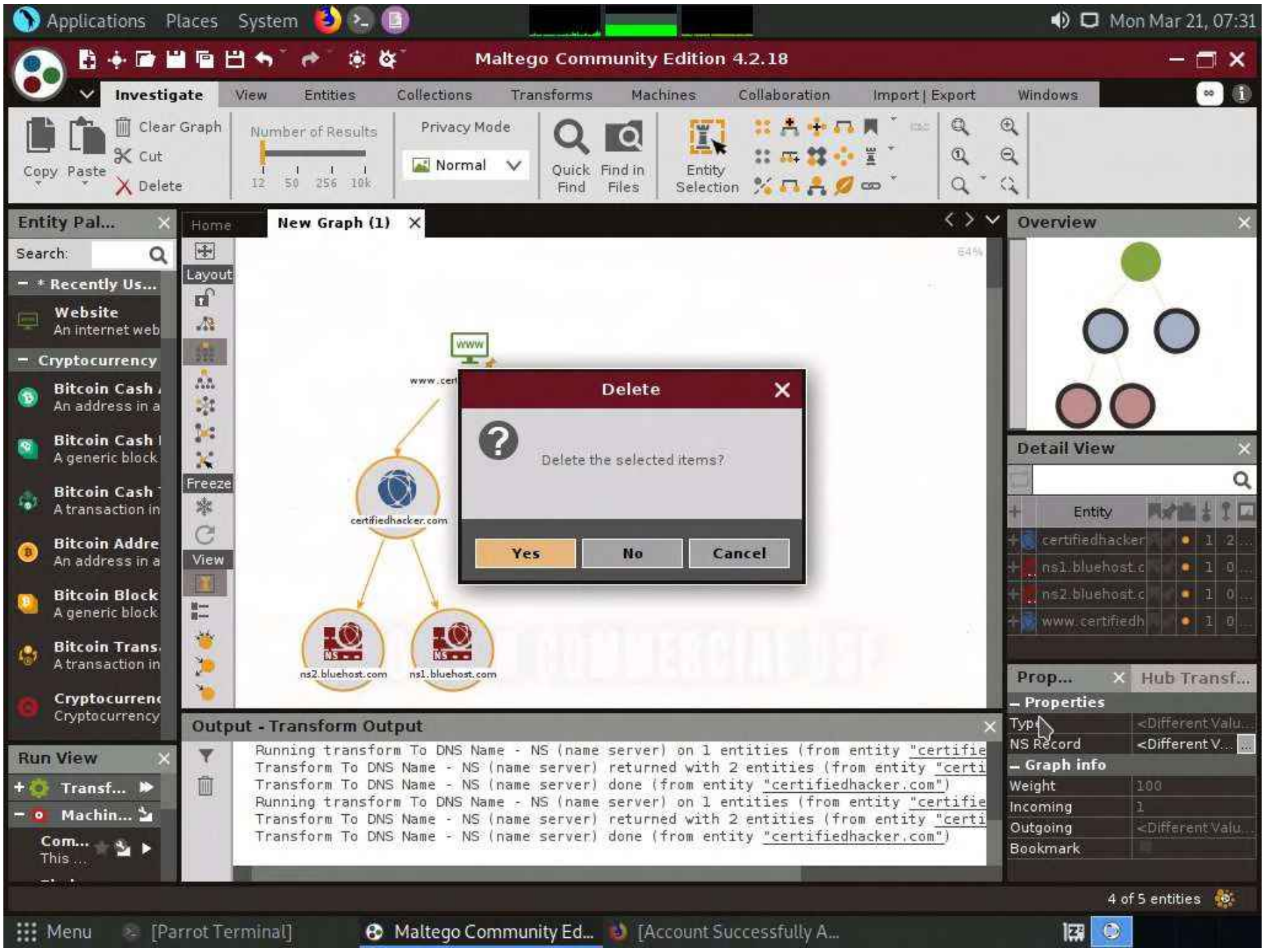
38. Right-click the **certifiedhacker.com** entity and select **All Transforms** --> **To DNS Name - NS (name server)**.



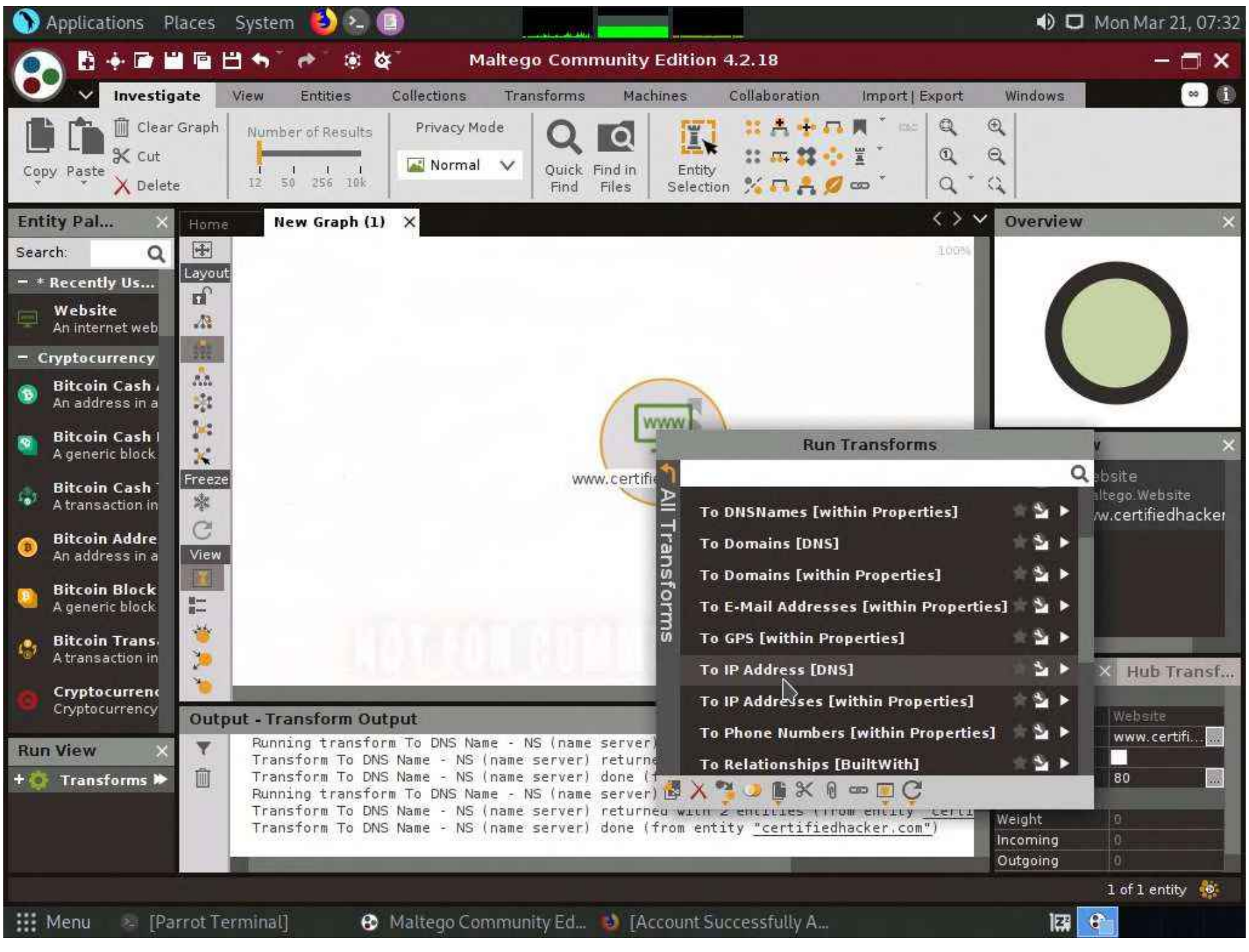
39. This returns the name servers associated with the domain, as shown in the following screenshot.

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.

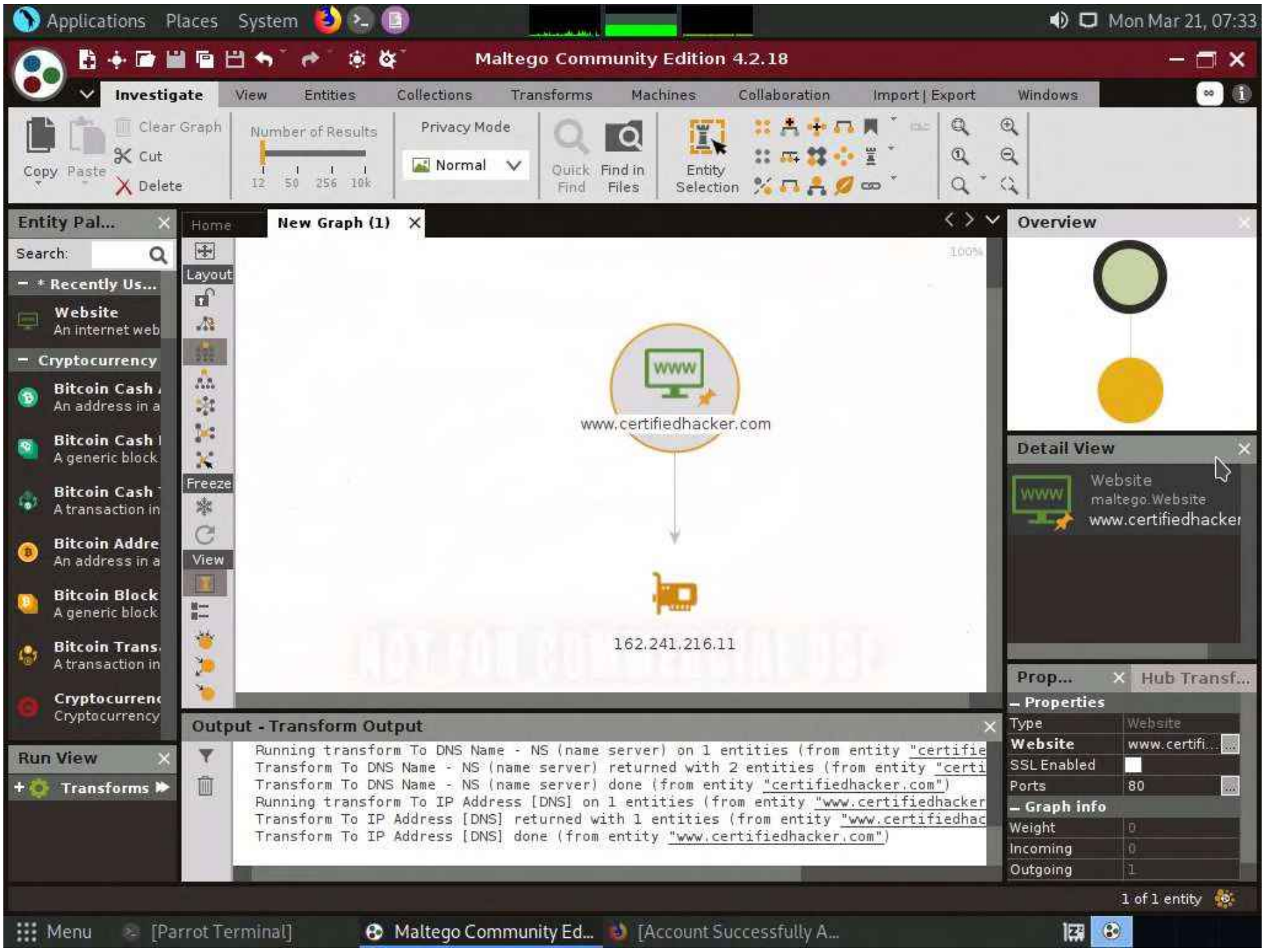
41. Select both the domain and the name server by dragging and deleting them.



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

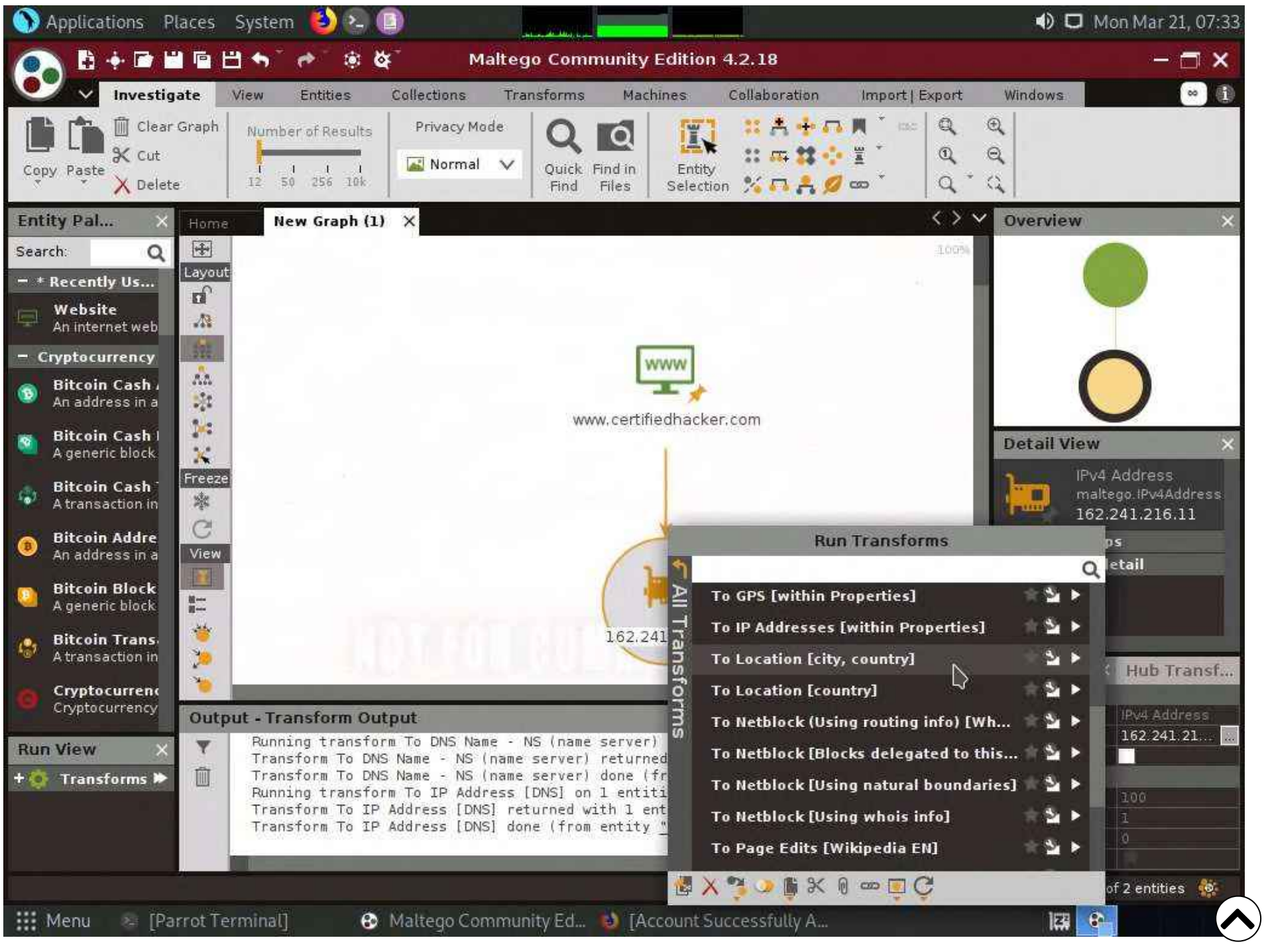


43. This displays the IP address of the website, as shown in the following screenshot.

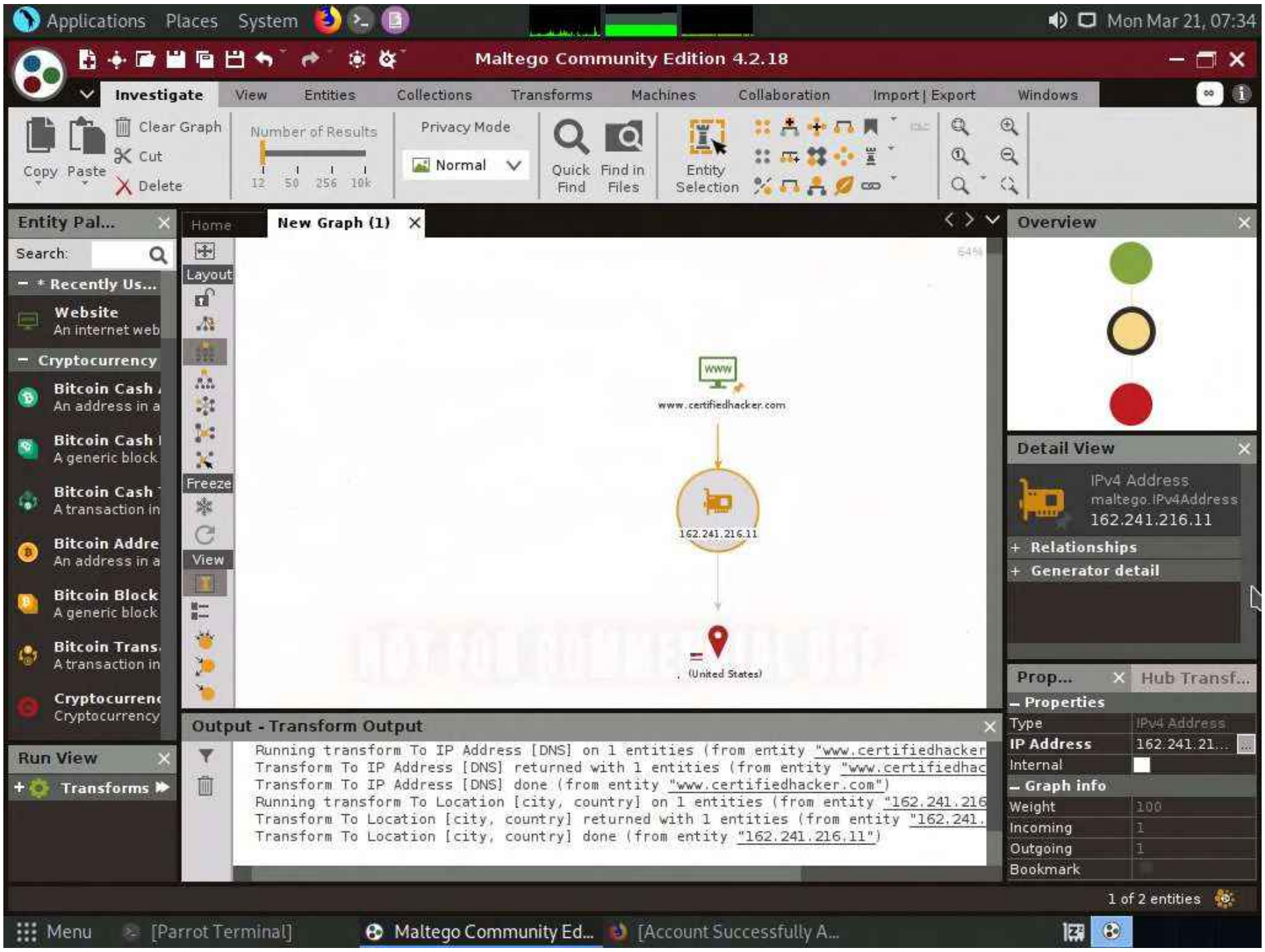


44. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

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

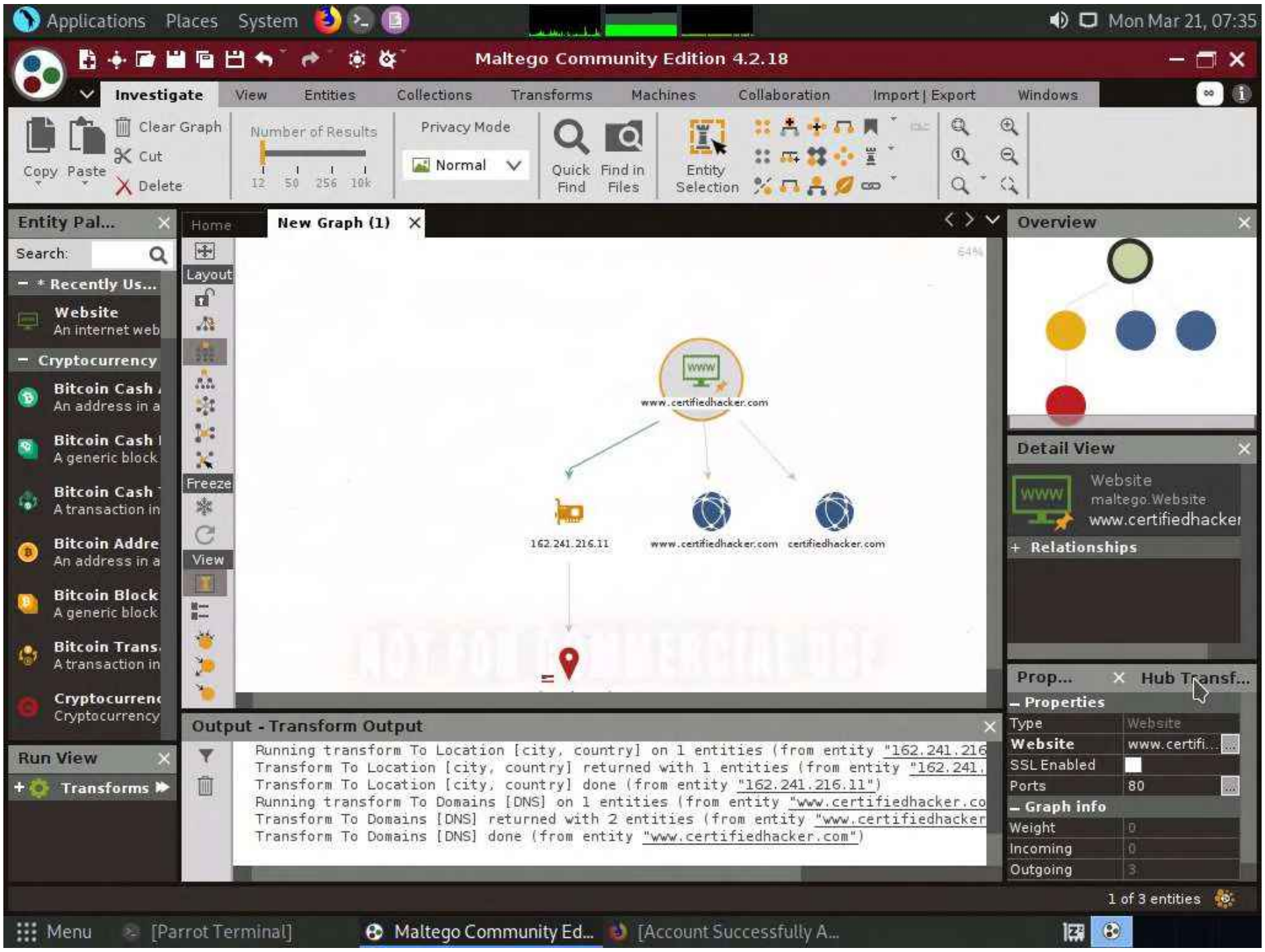


46. This transform identifies the geographical location of the IP address, as shown in the following screenshot.

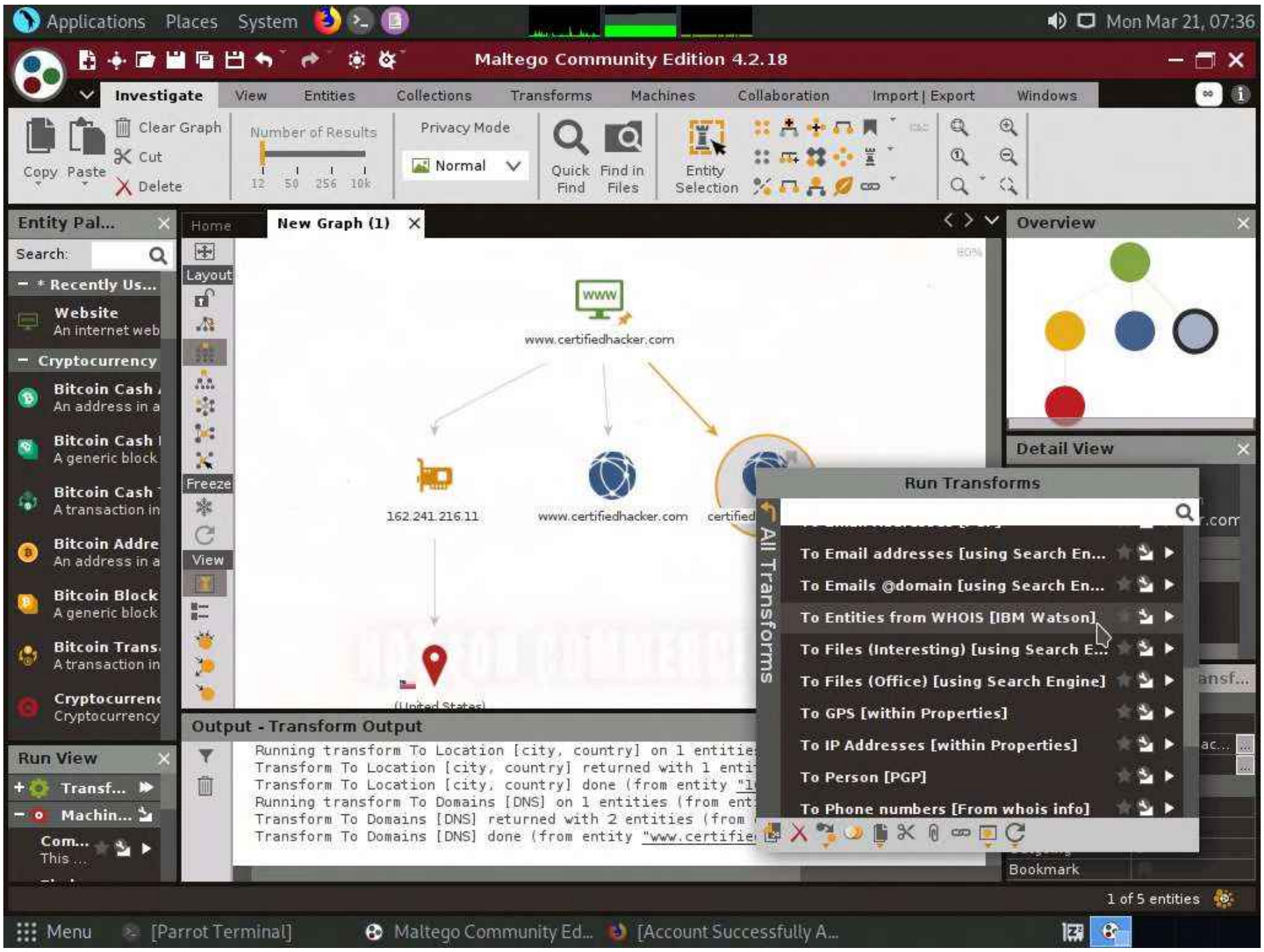


47. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

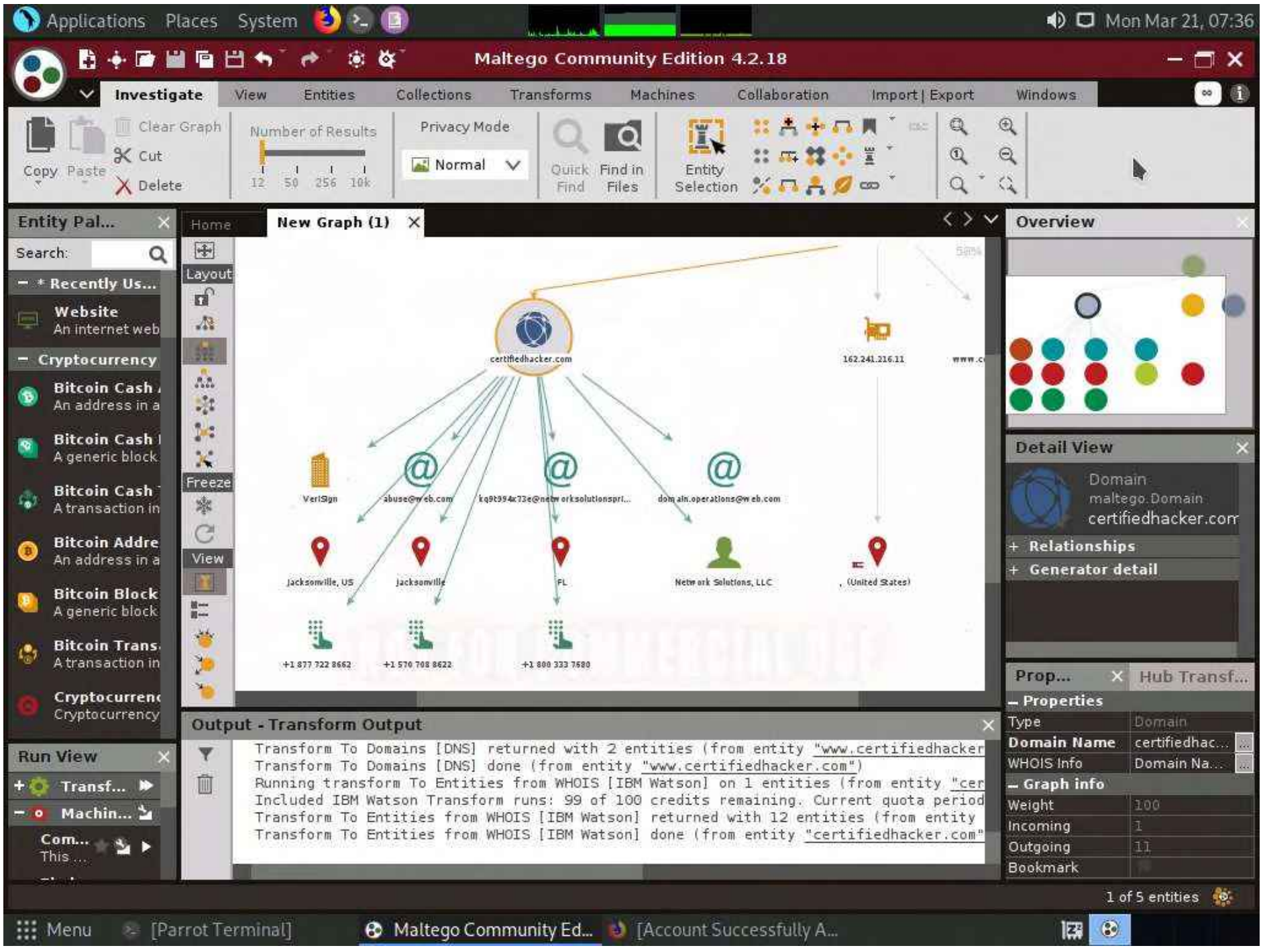
48. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms** --> **To Domains [DNS]**. The domains corresponding to the website display, as shown in the screenshot.



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



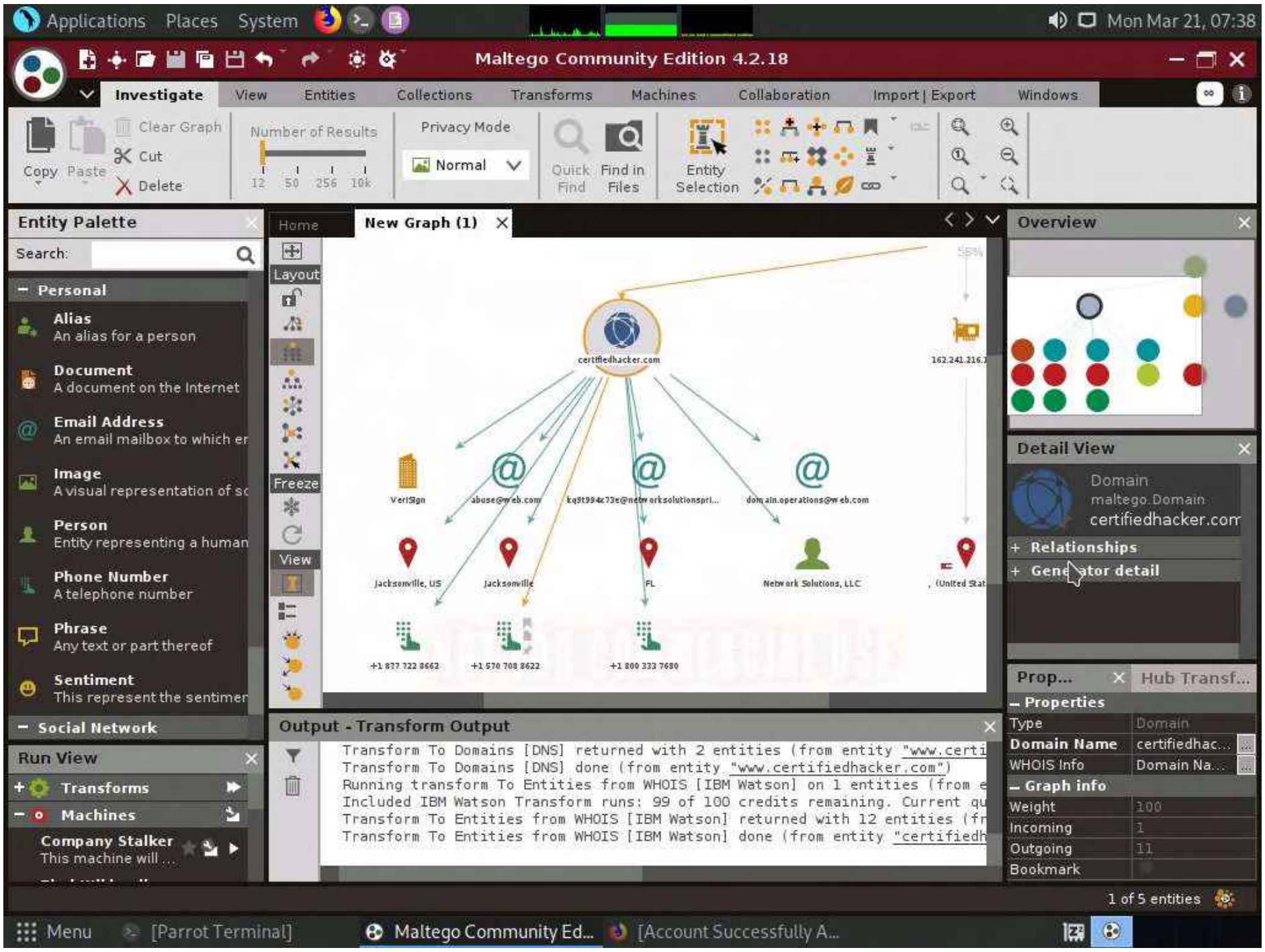
50. This transform returns the entities pertaining to the owner of the domain, as shown in the following screenshot.



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.

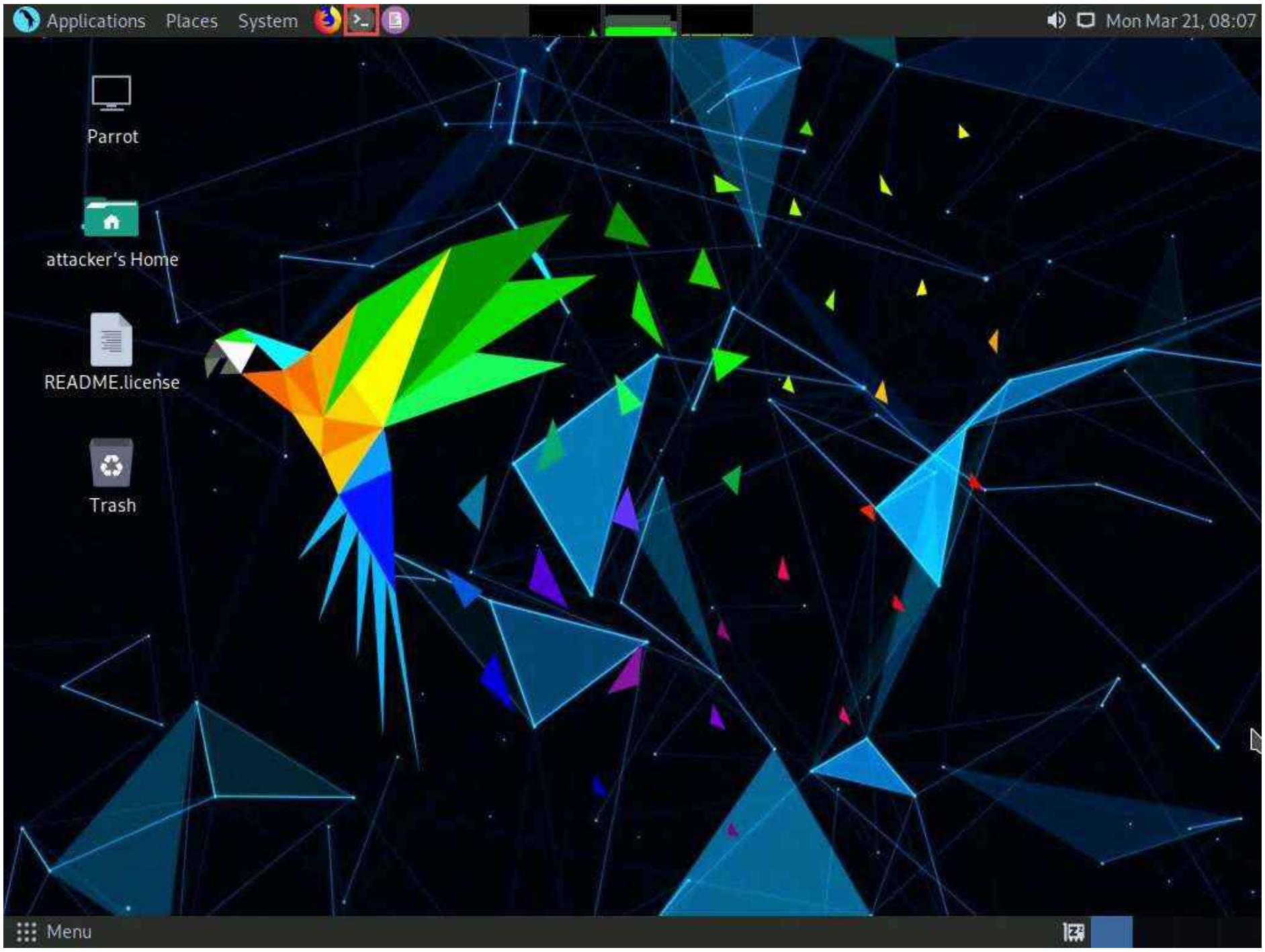
56. This concludes the demonstration of footprinting a target using Maltego.

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. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.

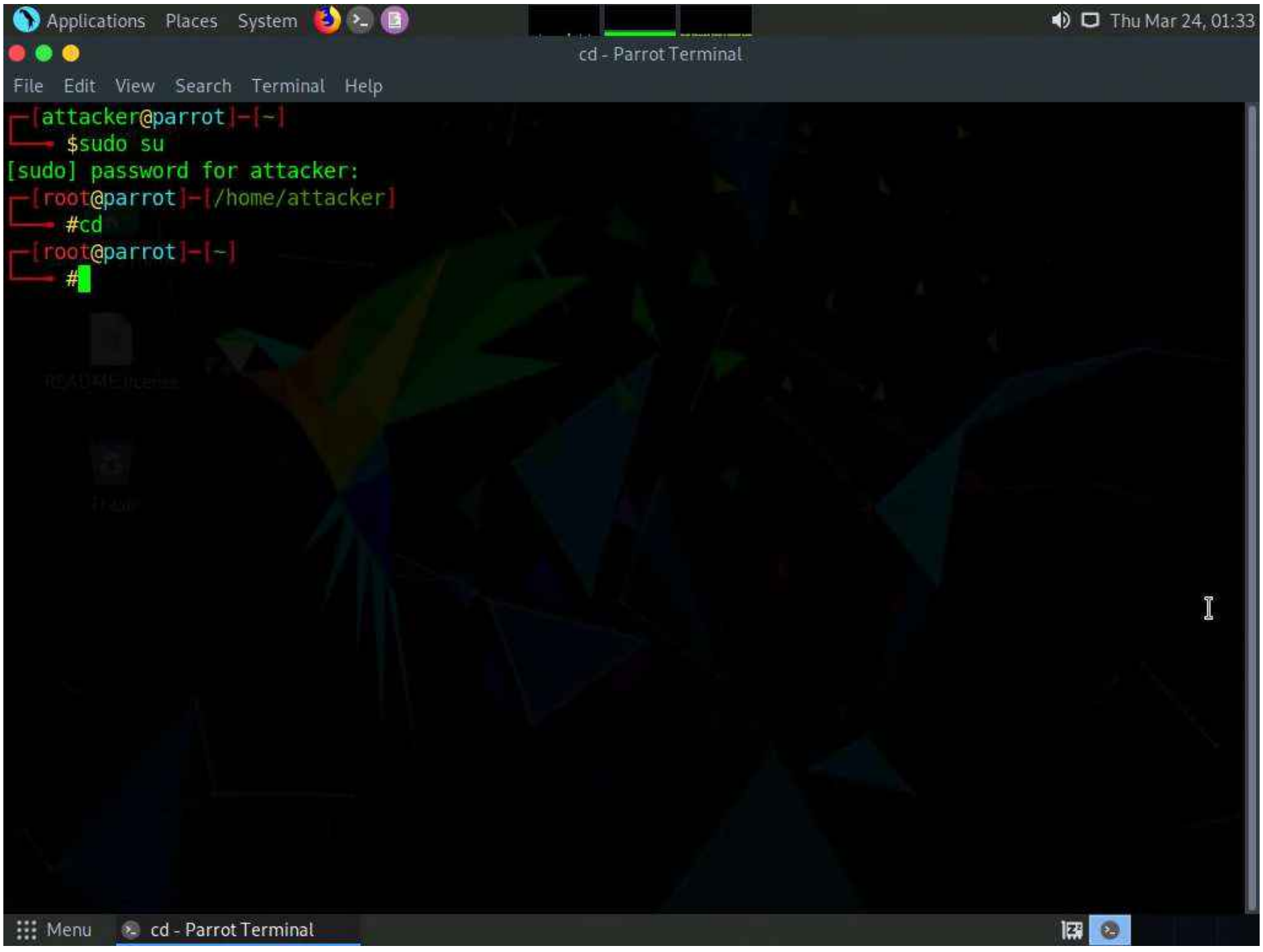


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

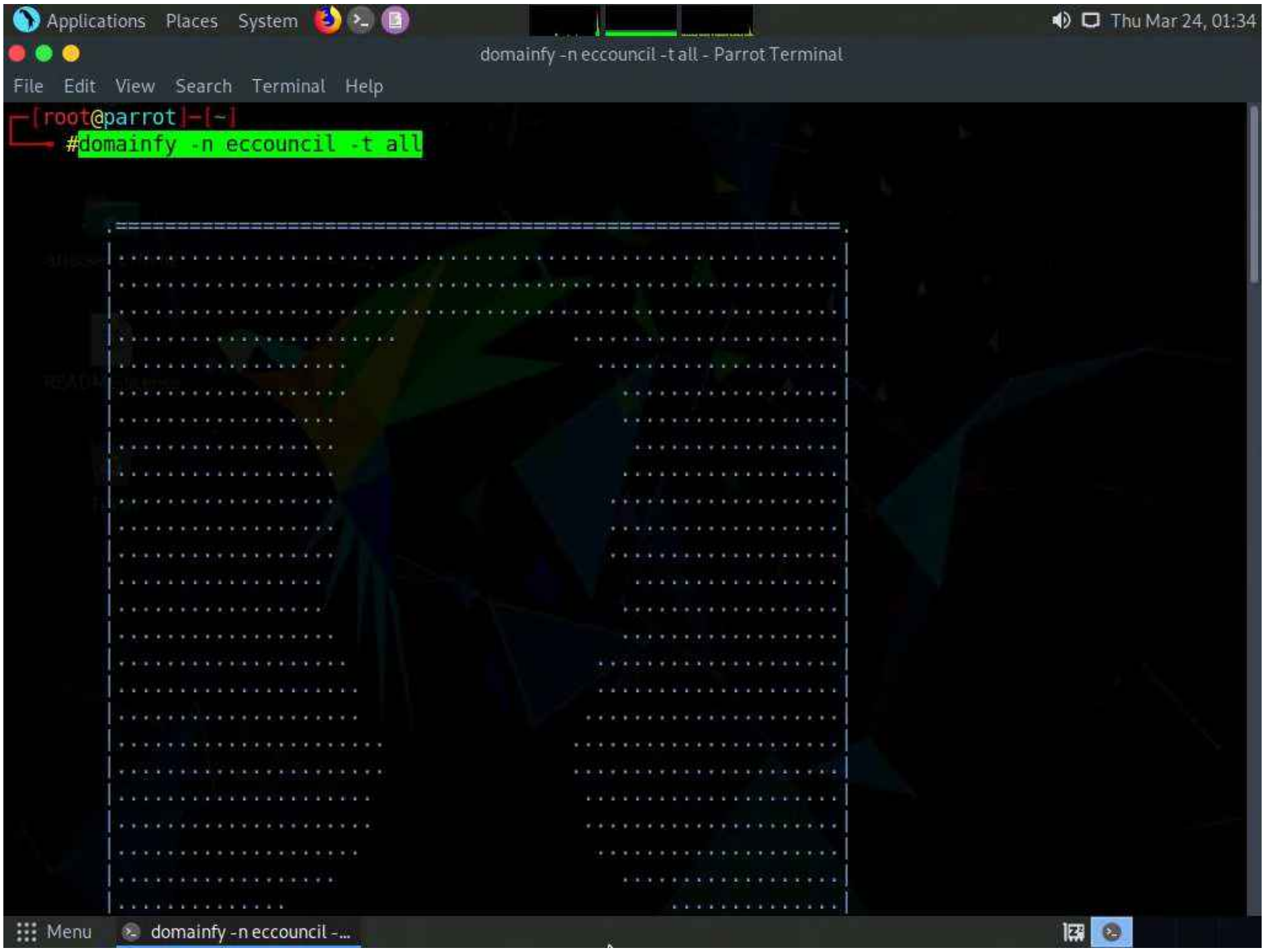
> Note: The password that you type will not be visible.

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

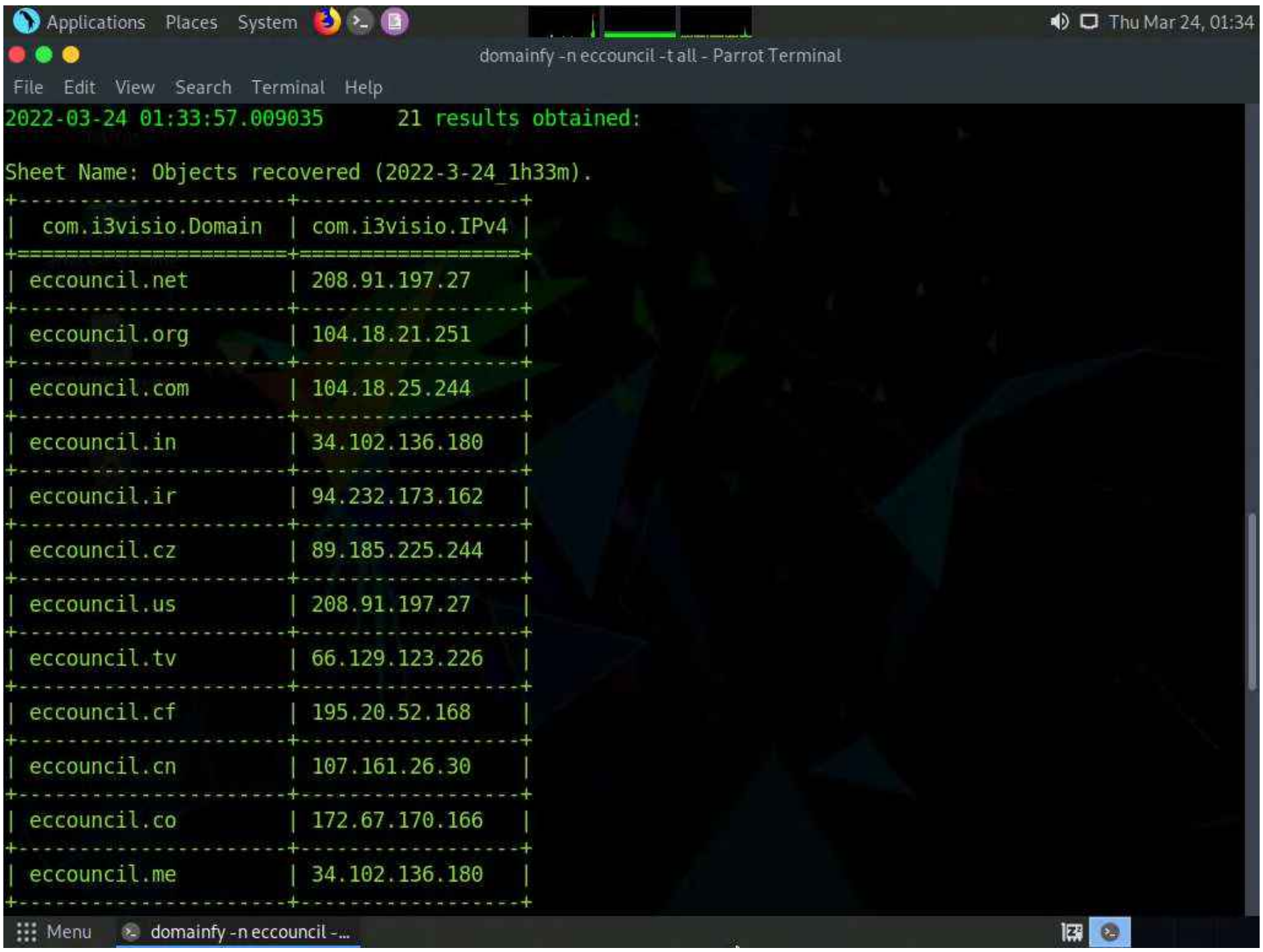


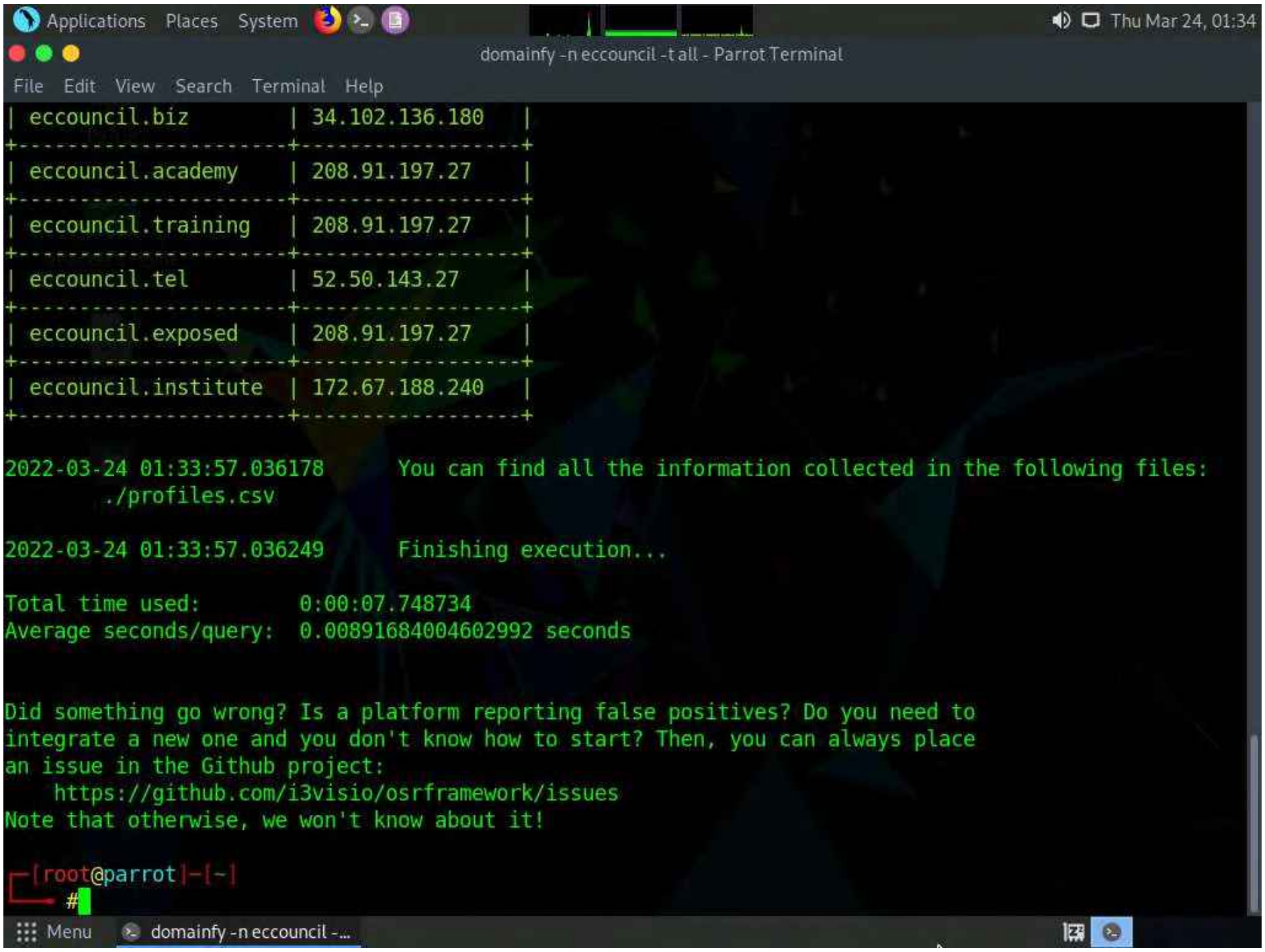
5. Use **domainfy** to check with the existing domains using words and nicknames. Type **domainfy -n [Domain Name] -t all** (here, the target domain name is **ECCOUNCIL**) and press **Enter**.

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.



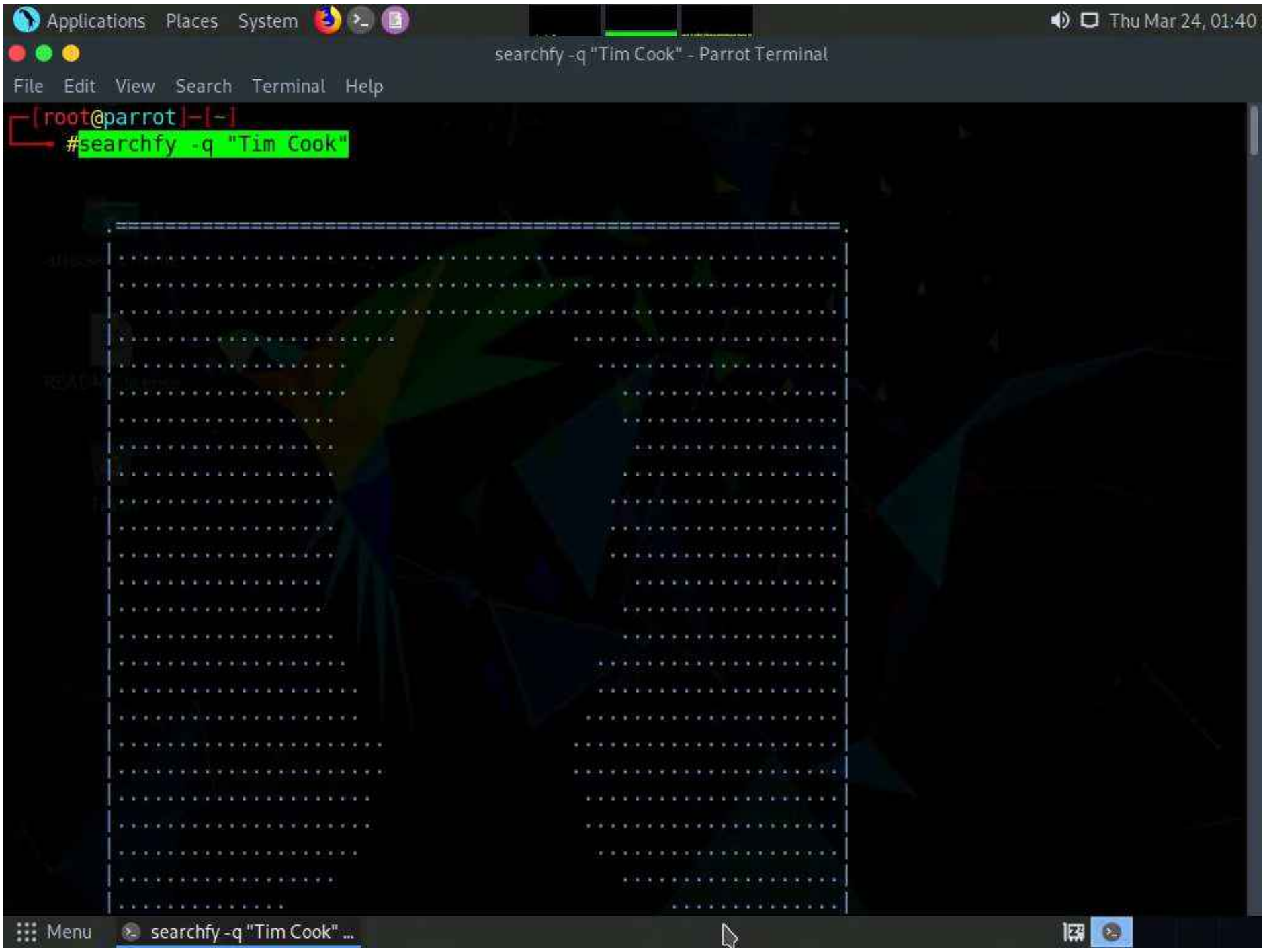
6. The tool will retrieve all the domains along with their IP addresses related to the target domain. Using this information, attackers can further find vulnerabilities in the subdomains of the target website and launch web application attacks.



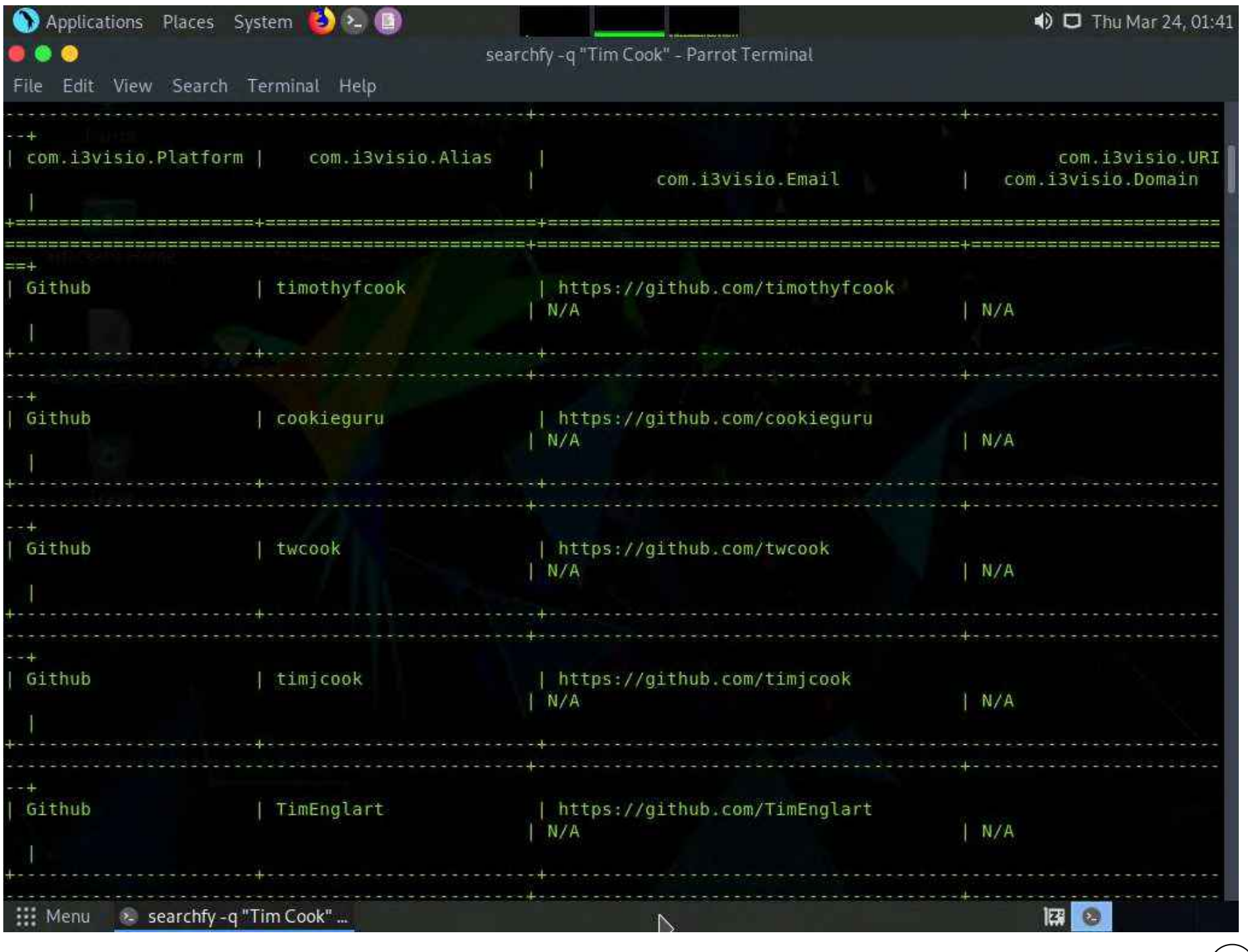


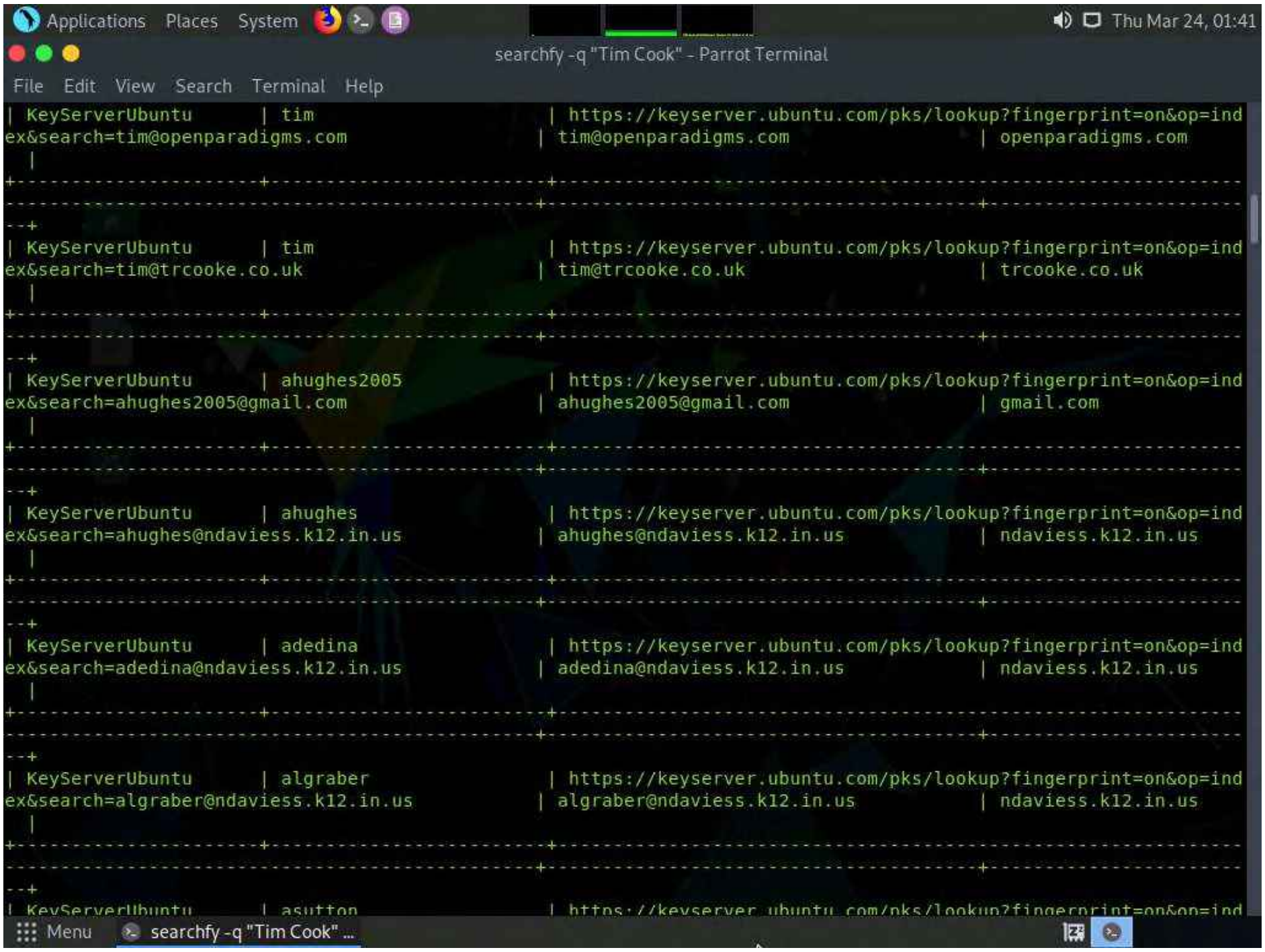
7. Use **searchfy** to check for the existence of a given user details on different social networking platforms such as Github, Instagram and Keyserverubuntu. Type **searchfy -q "target user name or profile name"** (here, the target user name or profile is **Tim Cook** and it is searched in all the social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

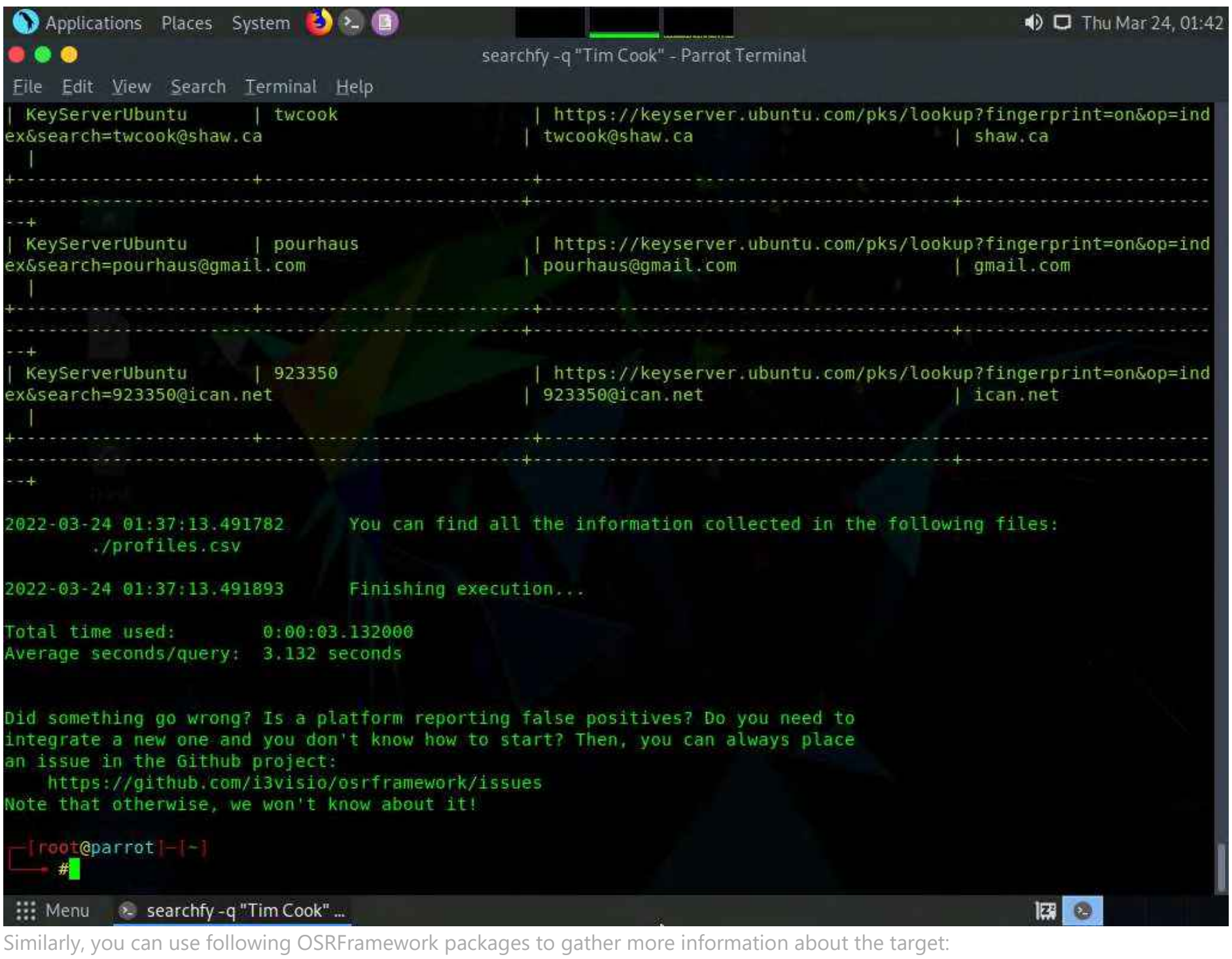
Note: **-q**: specifies the query or list of queries to be performed.



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.







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.

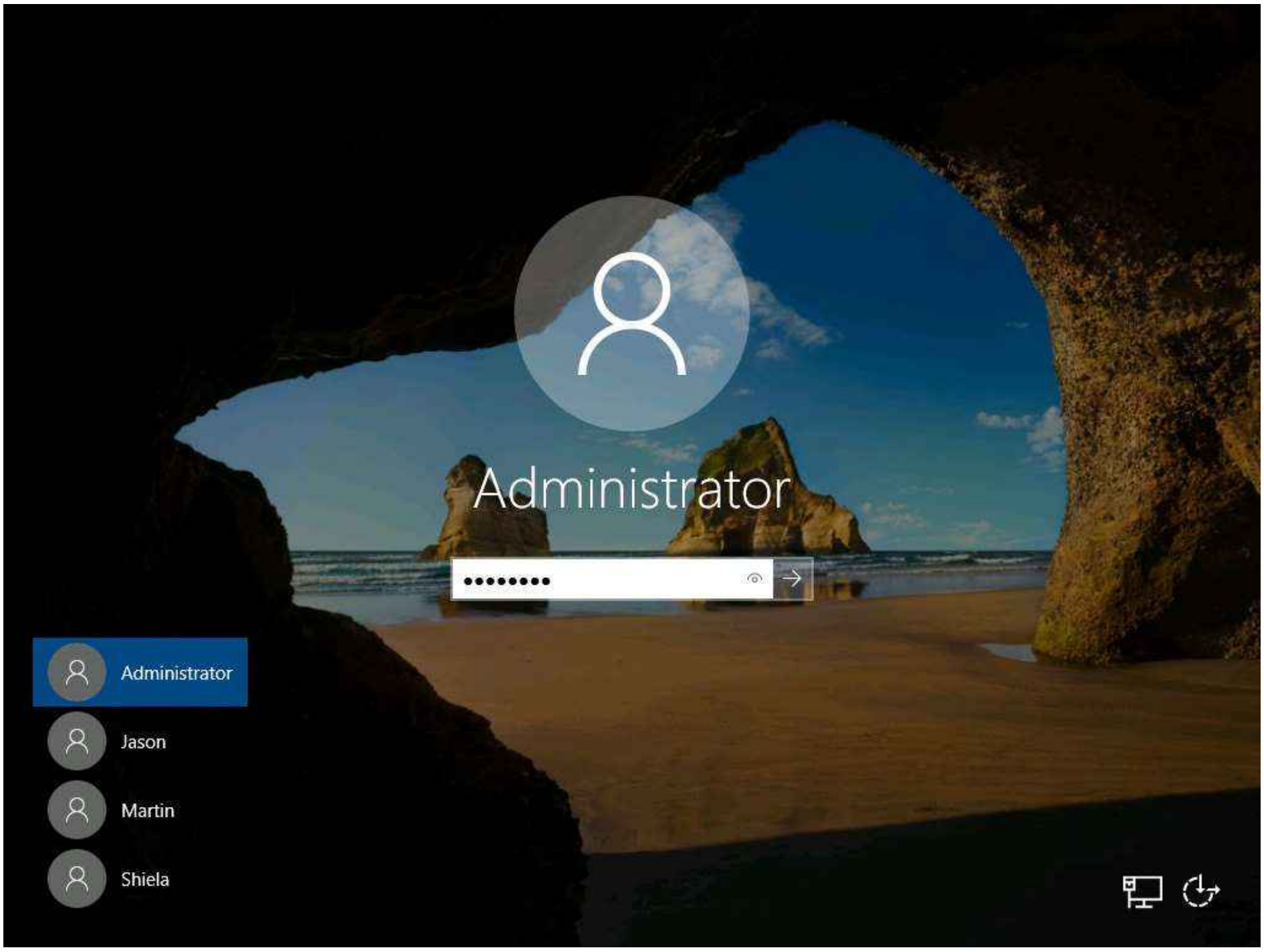
Task 4: Footprinting a Target using FOCA

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.

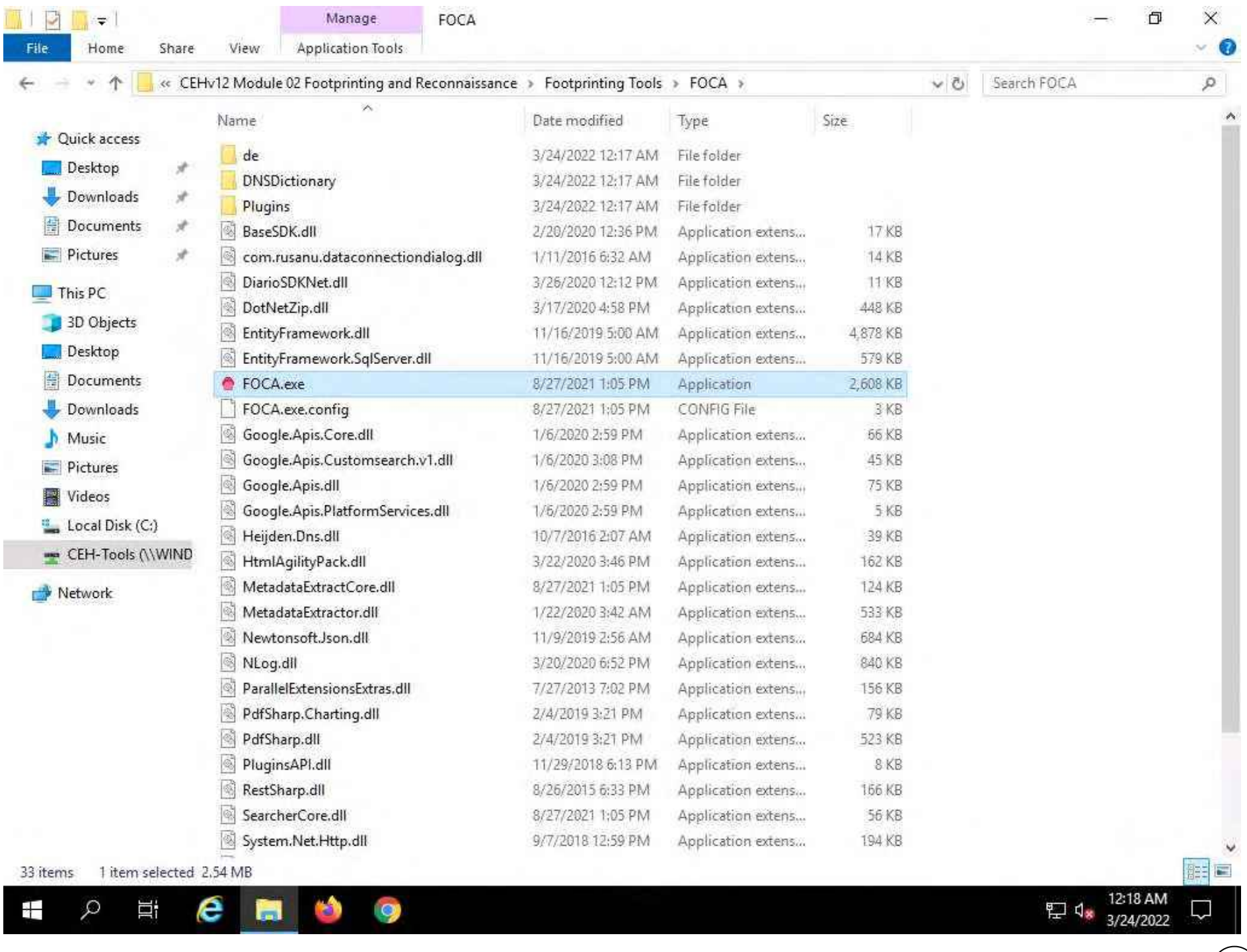
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

2. 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.

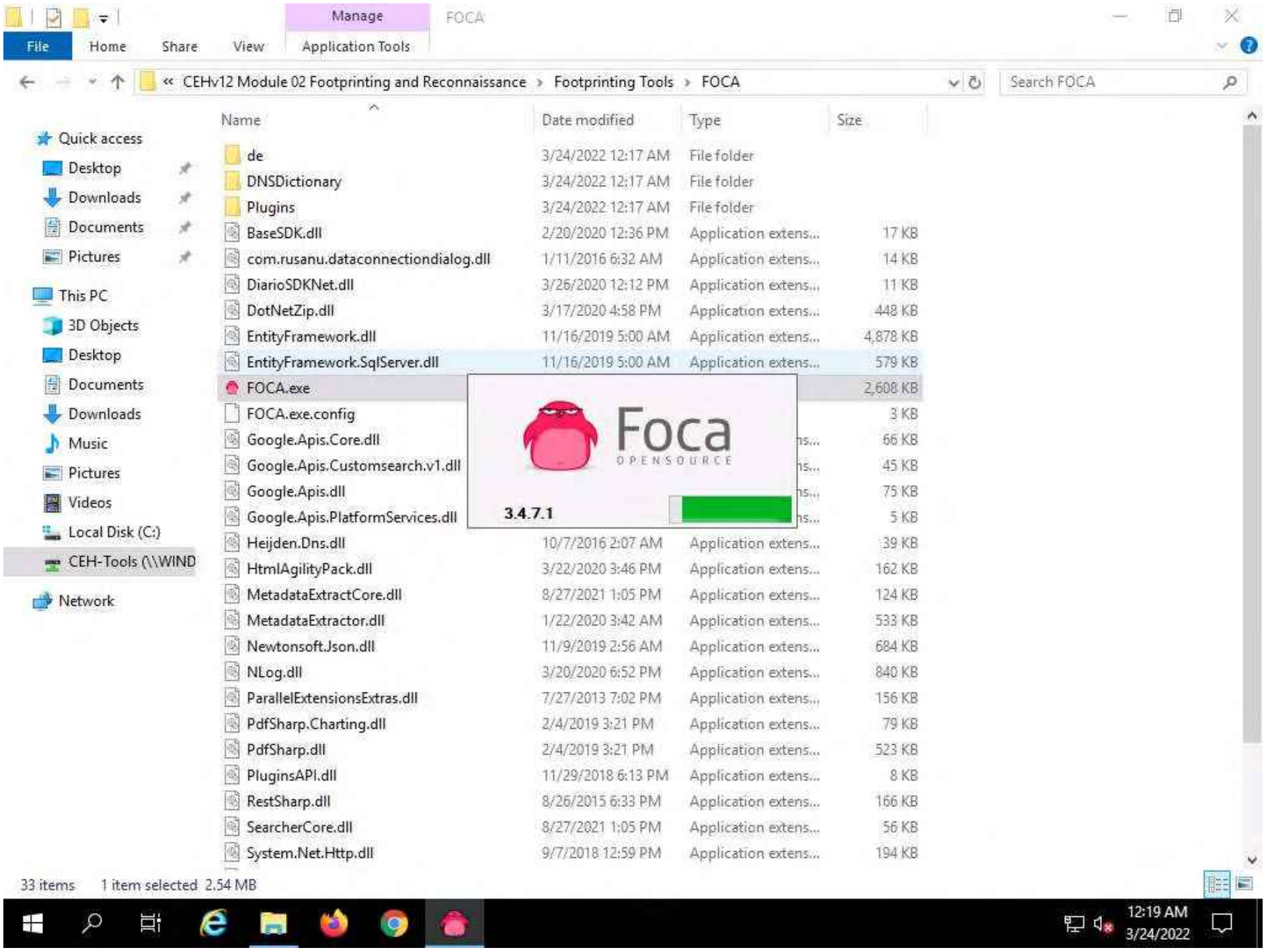
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



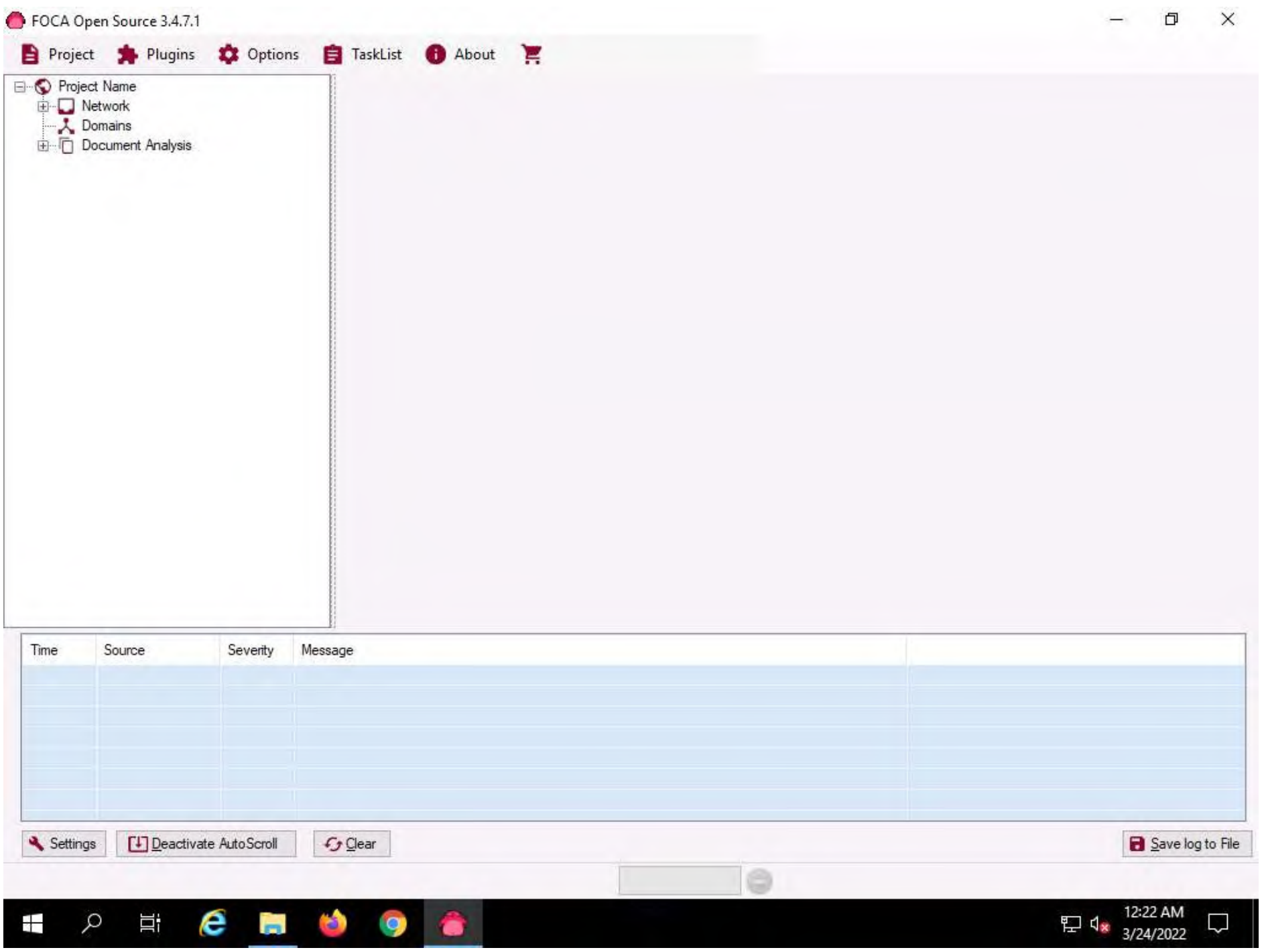
3. To launch FOCA, navigate to **Z:\CEHv12 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA** and double-click **FOCA.exe**.



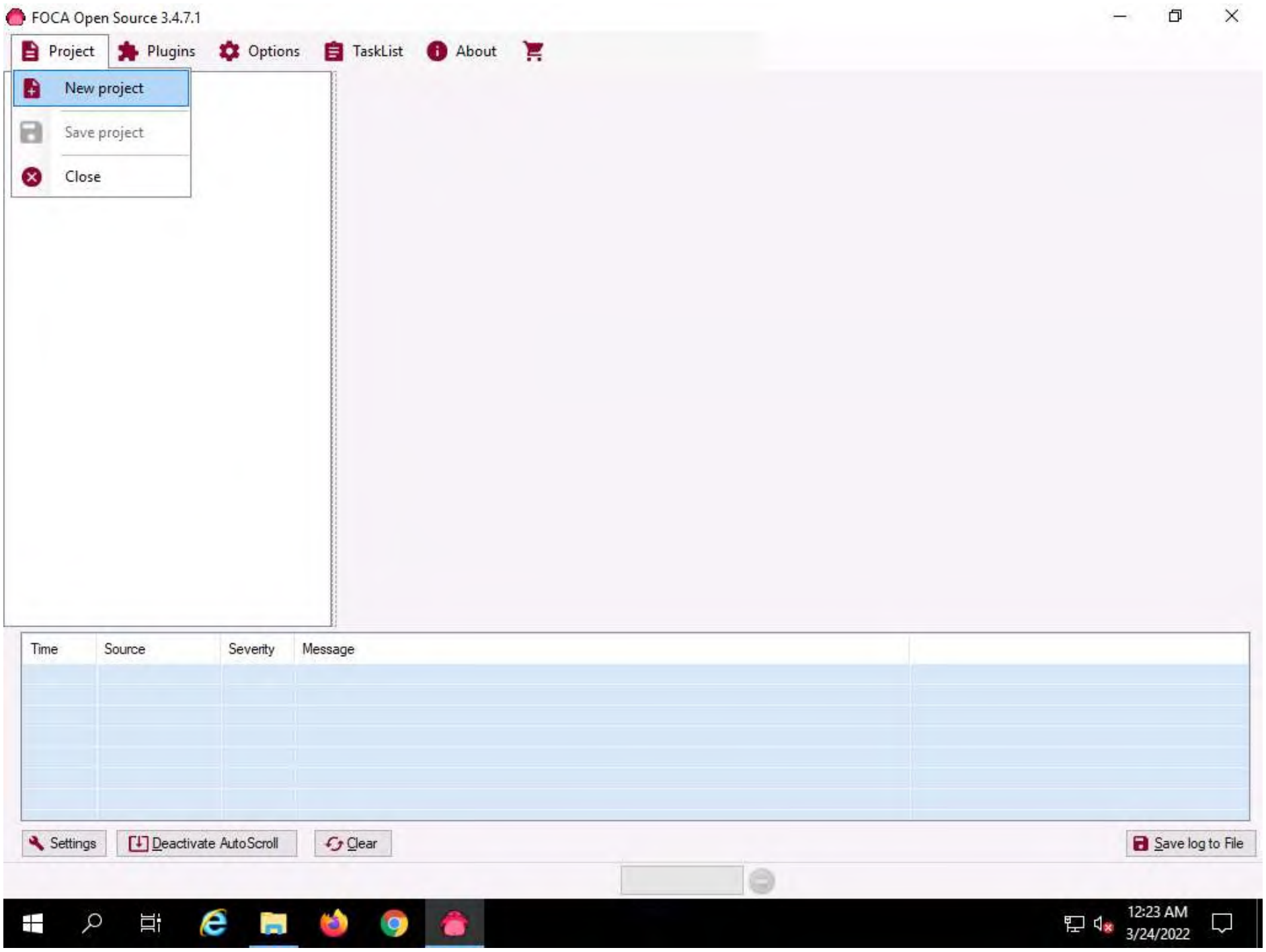
4. The FOCA dialog-box appears, wait for the initialization to complete.



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

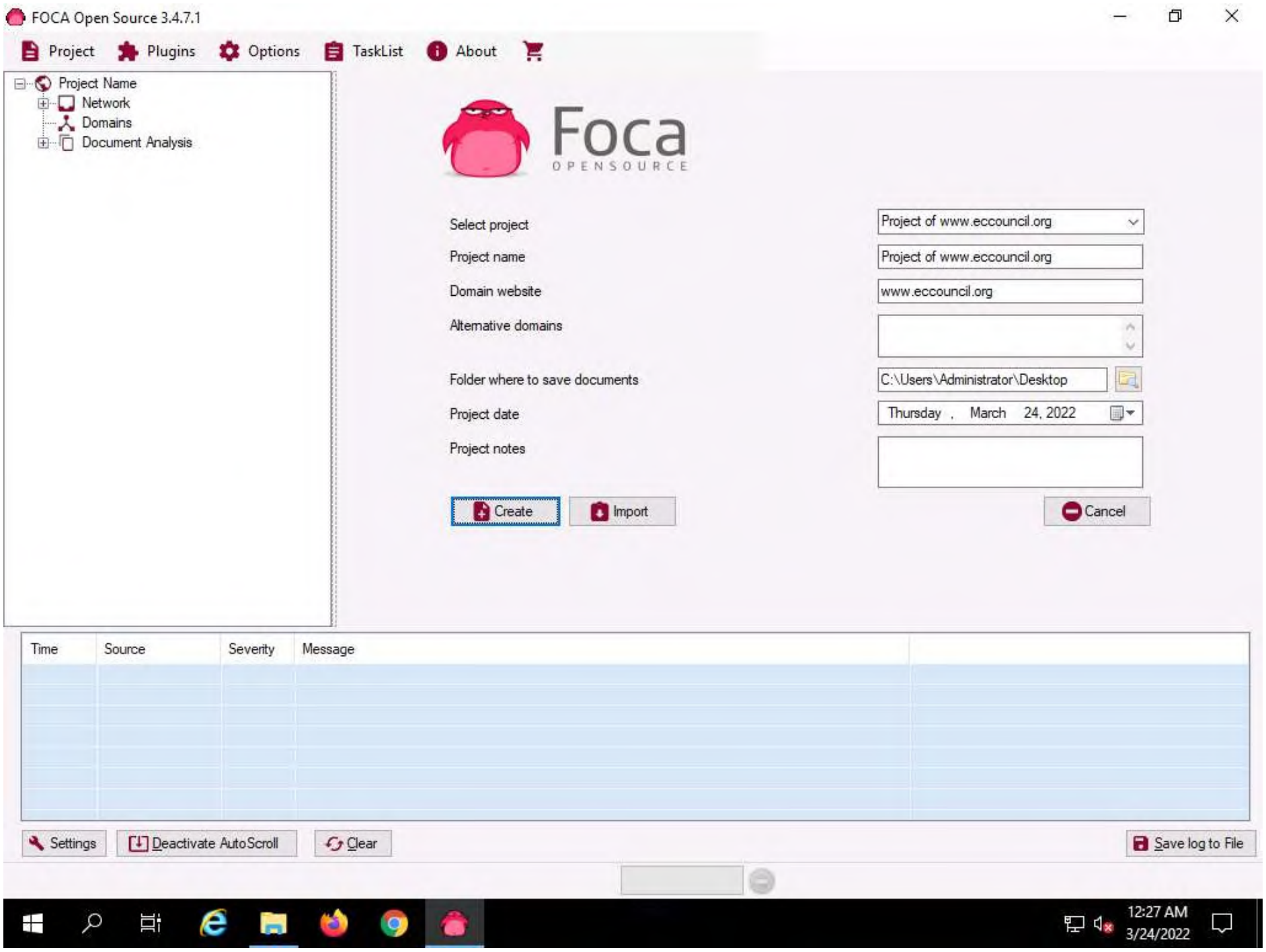


6. Create a new project by navigating to **Project** and click **New project** on the menu bar.

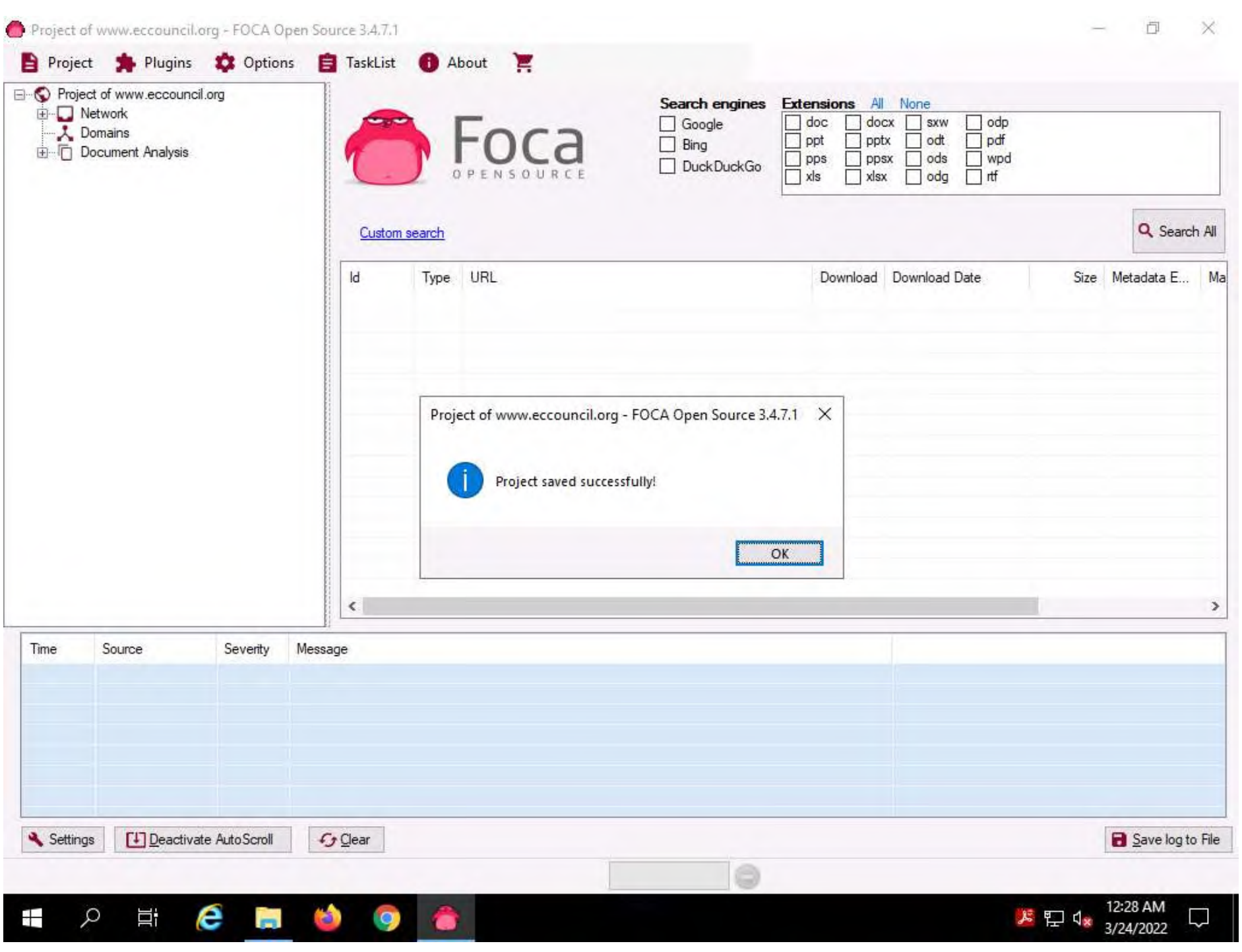


7. The FOCA new project wizard appears, follow the steps below:

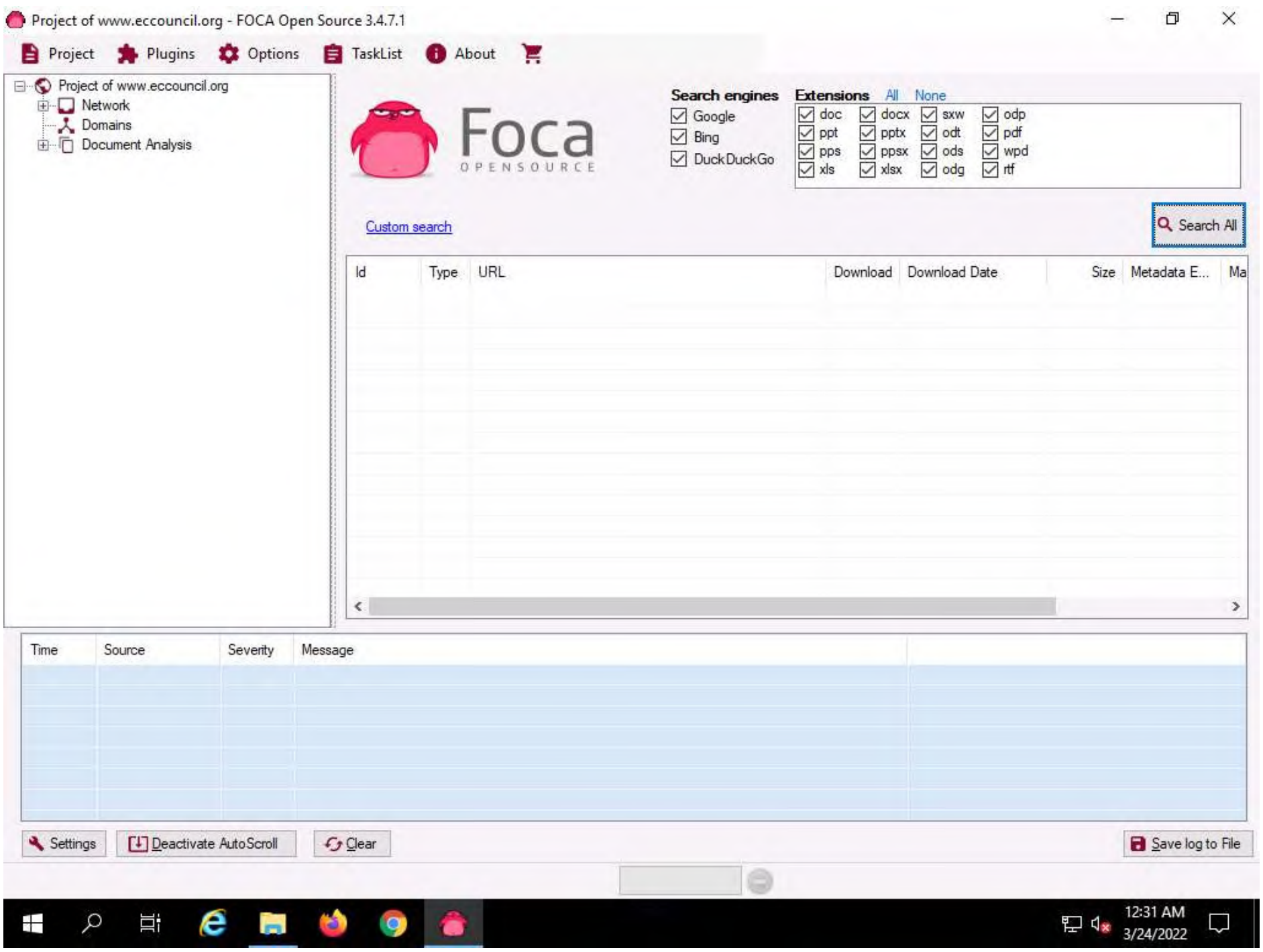
Enter a project name in the **Project name** field (here, **Project of www.eccouncil.org**).
Enter the domain website in the **Domain website** field (here, **www.eccouncil.org**).
You can leave the optional **Alternative domains** field empty.
Under the **Folder where to save documents** field, click 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.



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

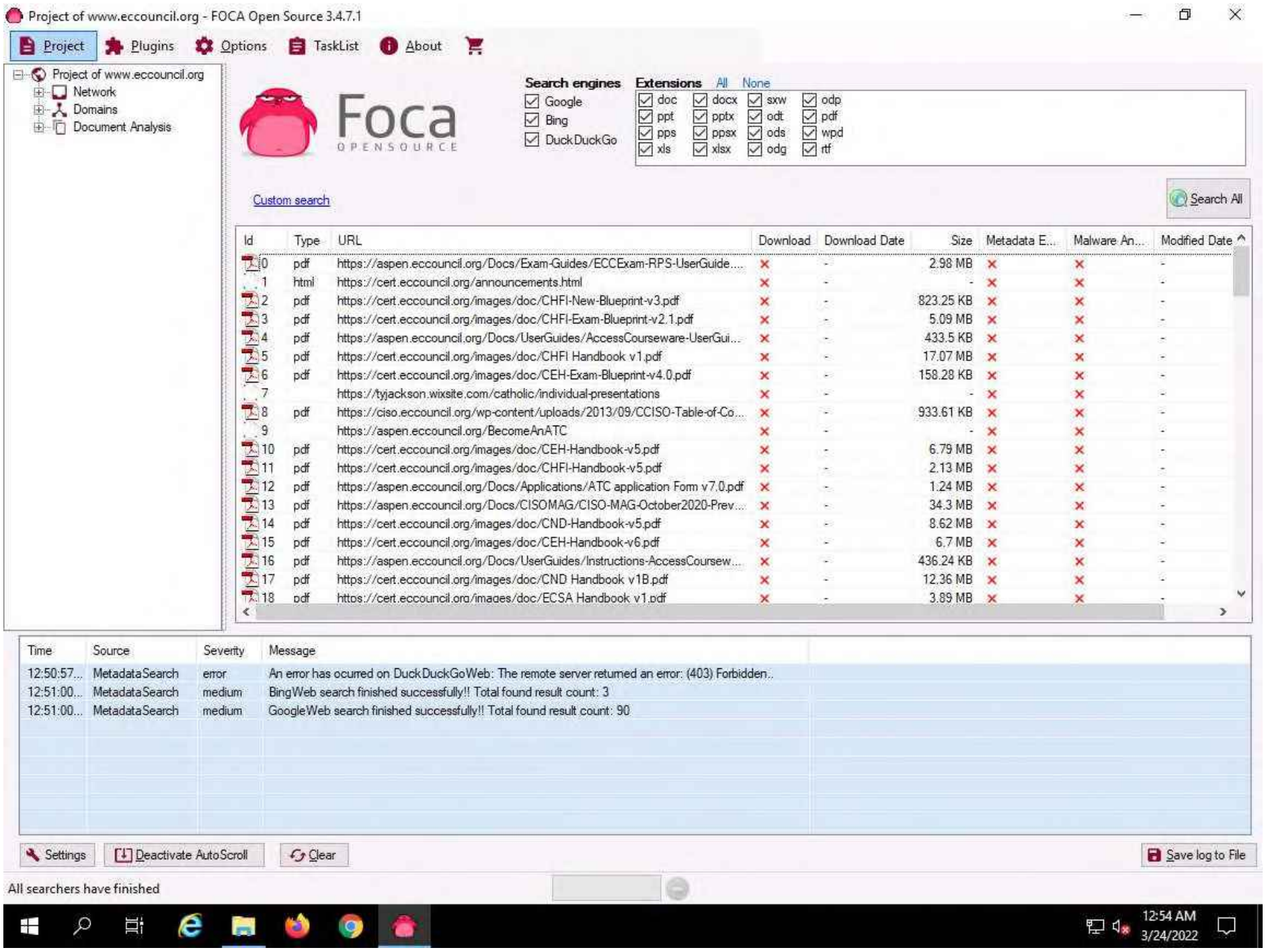


9. To extract the information of the targeted domain, select all three search engines (**Google**, **Bing**, and **DuckDuckGo**) present under **Search engines** section. Similarly, under **Extensions** section, click **All** option to choose all the given extensions and then click the **Search All**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



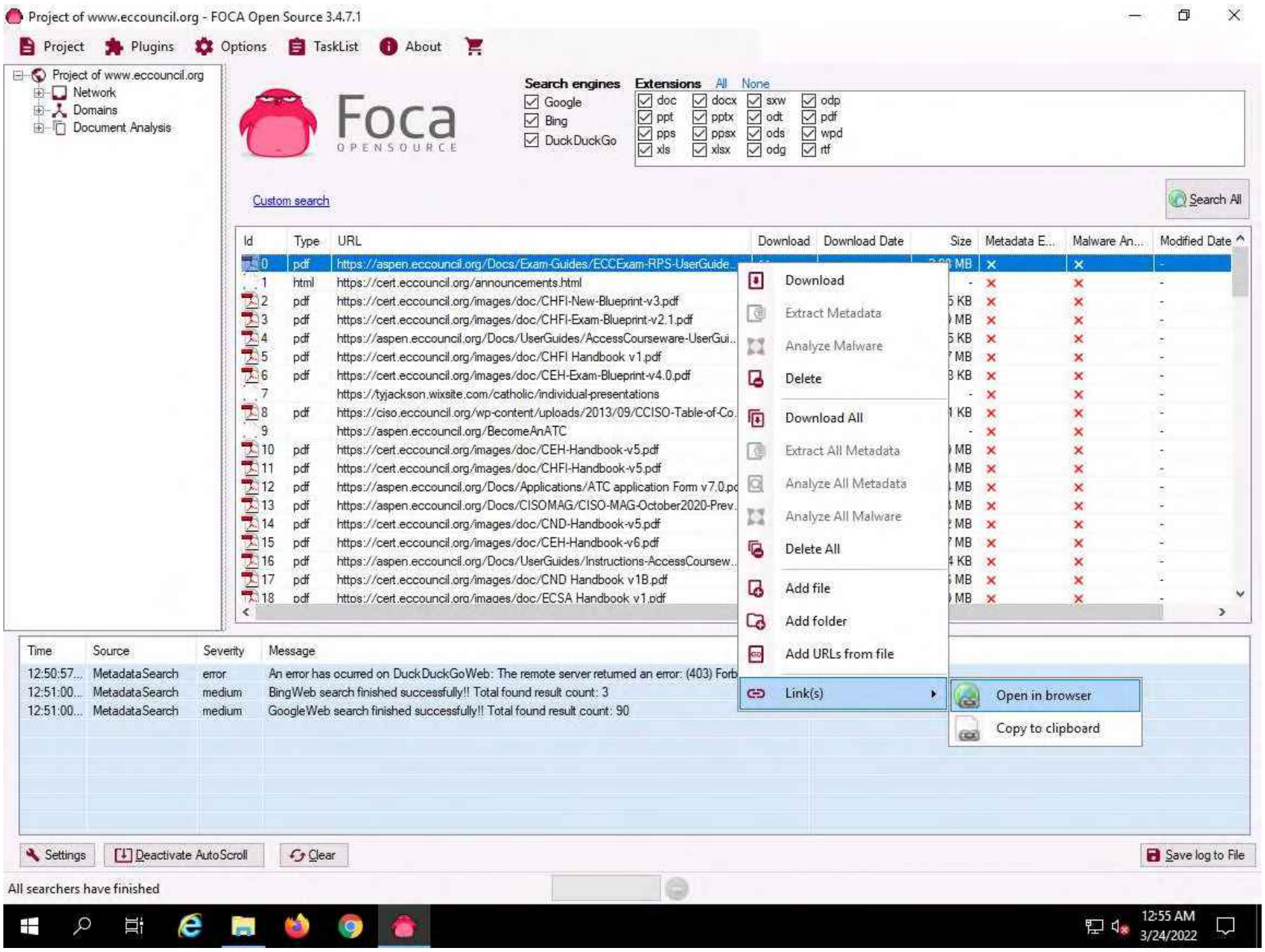
10. The **Search All** button automatically toggles the **Stop** button, and begins gathering information on the target domain in the middle pane.

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



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**.

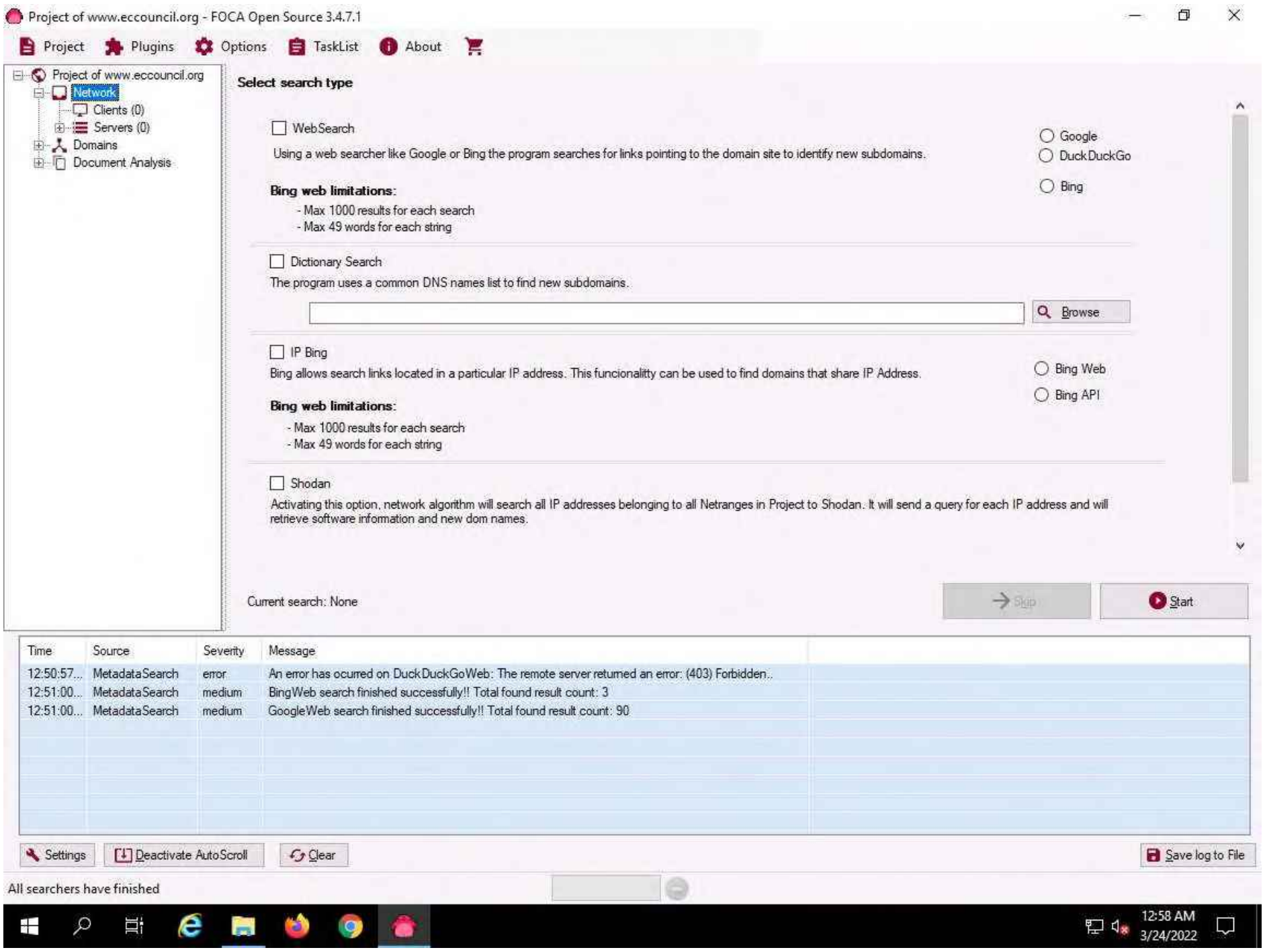


13. The extracted file from the domain by using FOCA appears on the web browser, as shown in the screenshot.

14. Close the web browser.

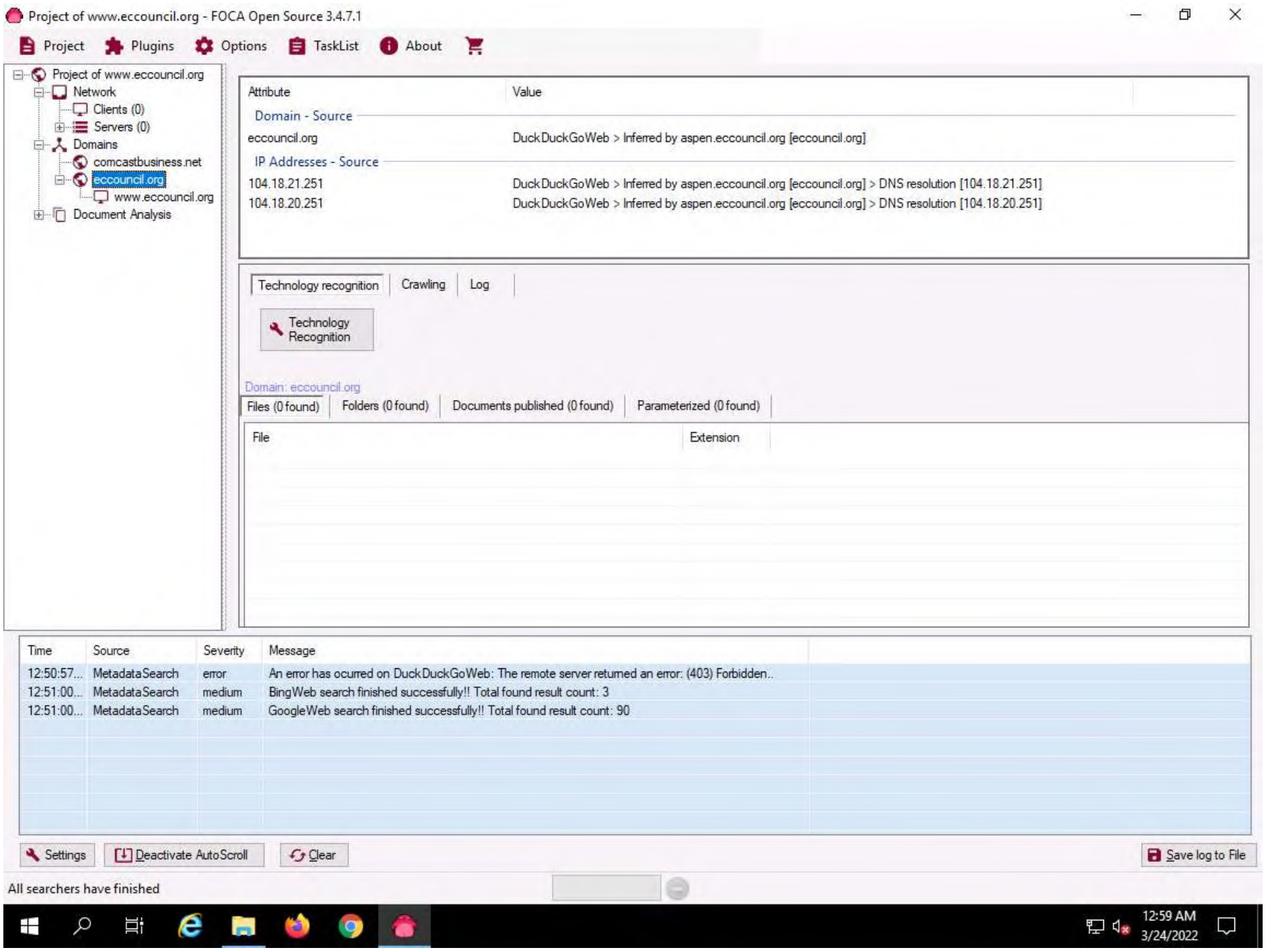
15. Navigate back to the FOCA window and click the **Network** node to expand the node in the left pane of the window to view the network structure.

> Note: The domain we used does not have associated clients or servers.

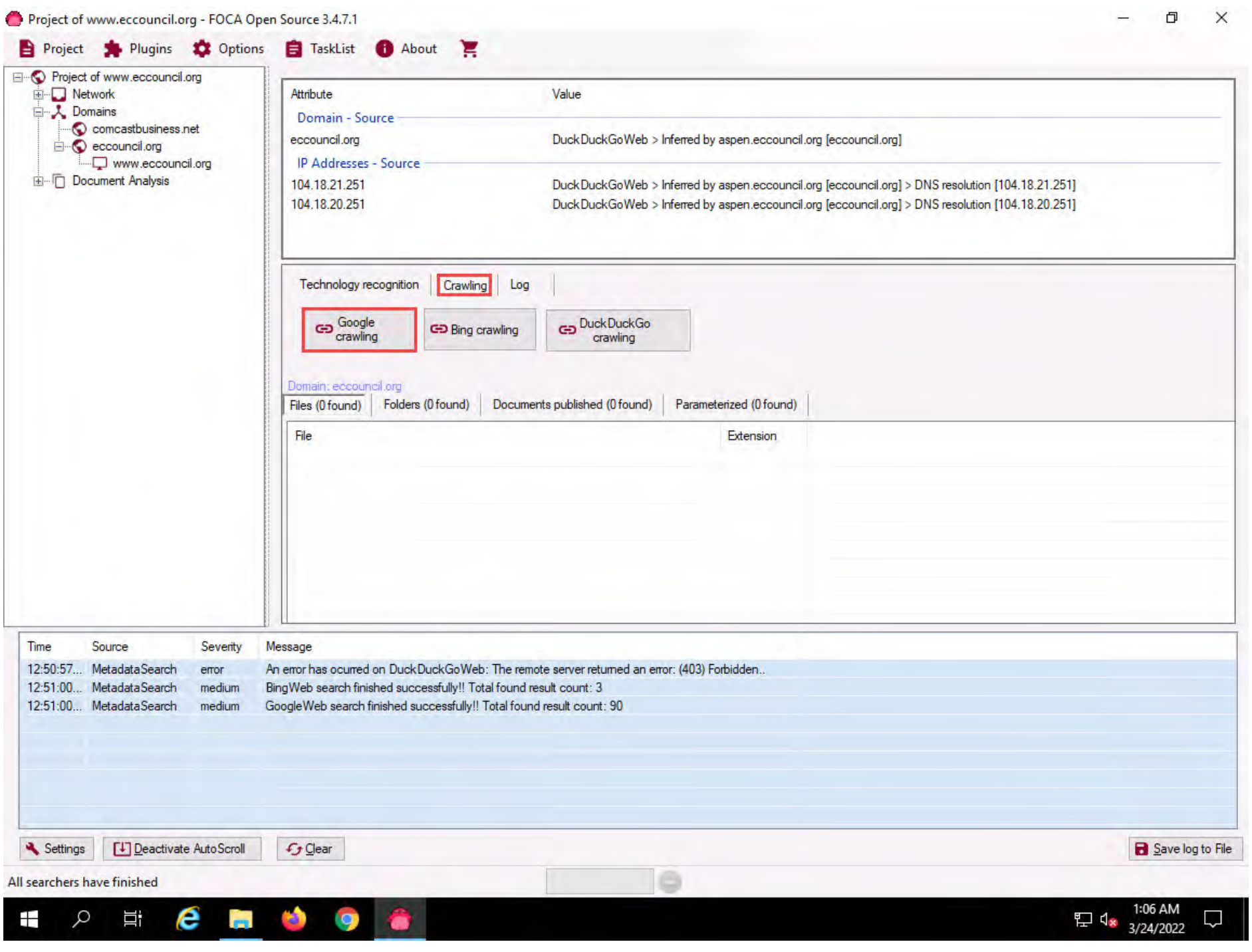


16. If the domain has any of the associated **Clients** or **Servers**, it displays the related information.

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

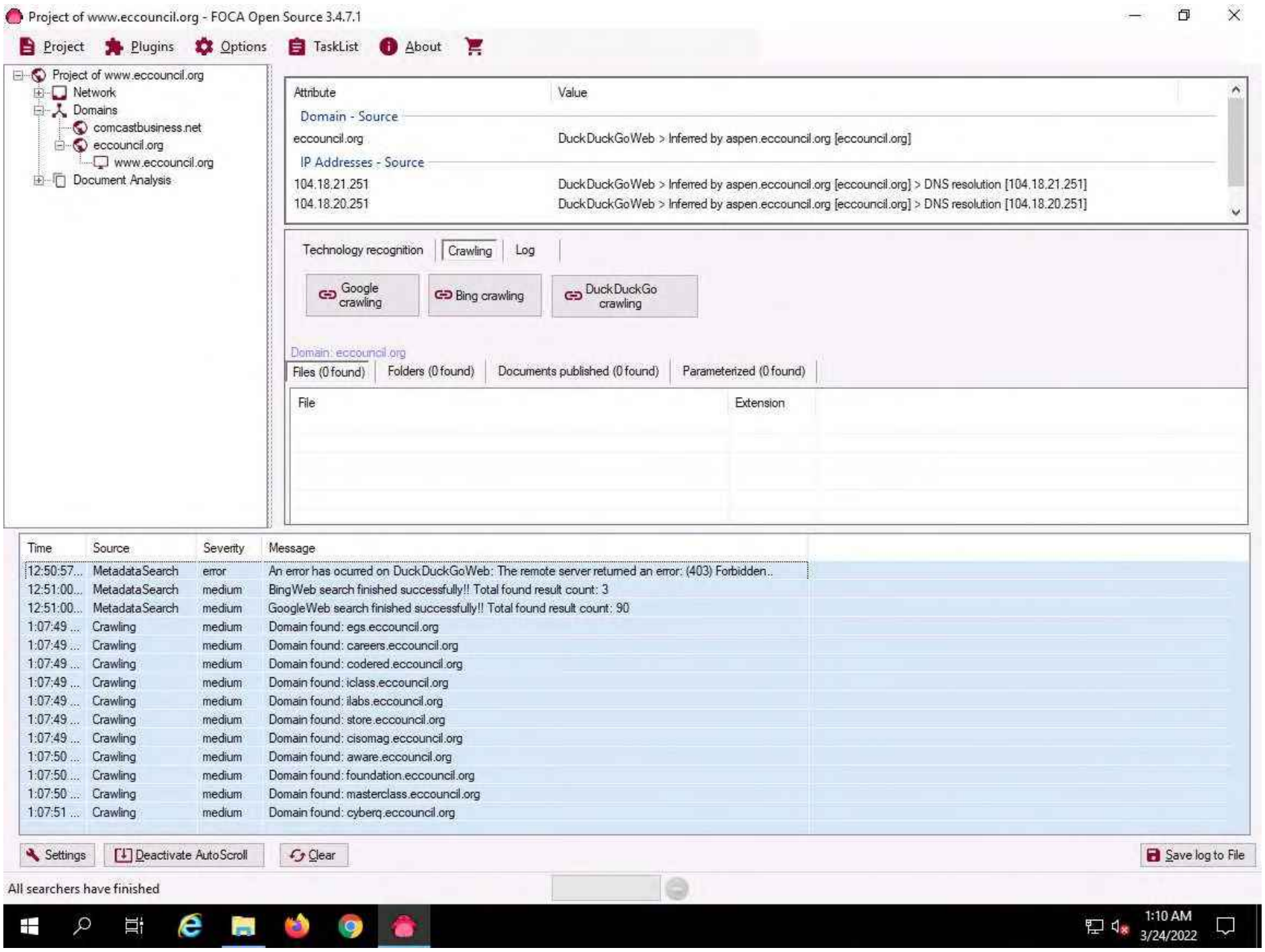


18. In the right-pane, click **Crawling** tab and then click **Google crawling** button.



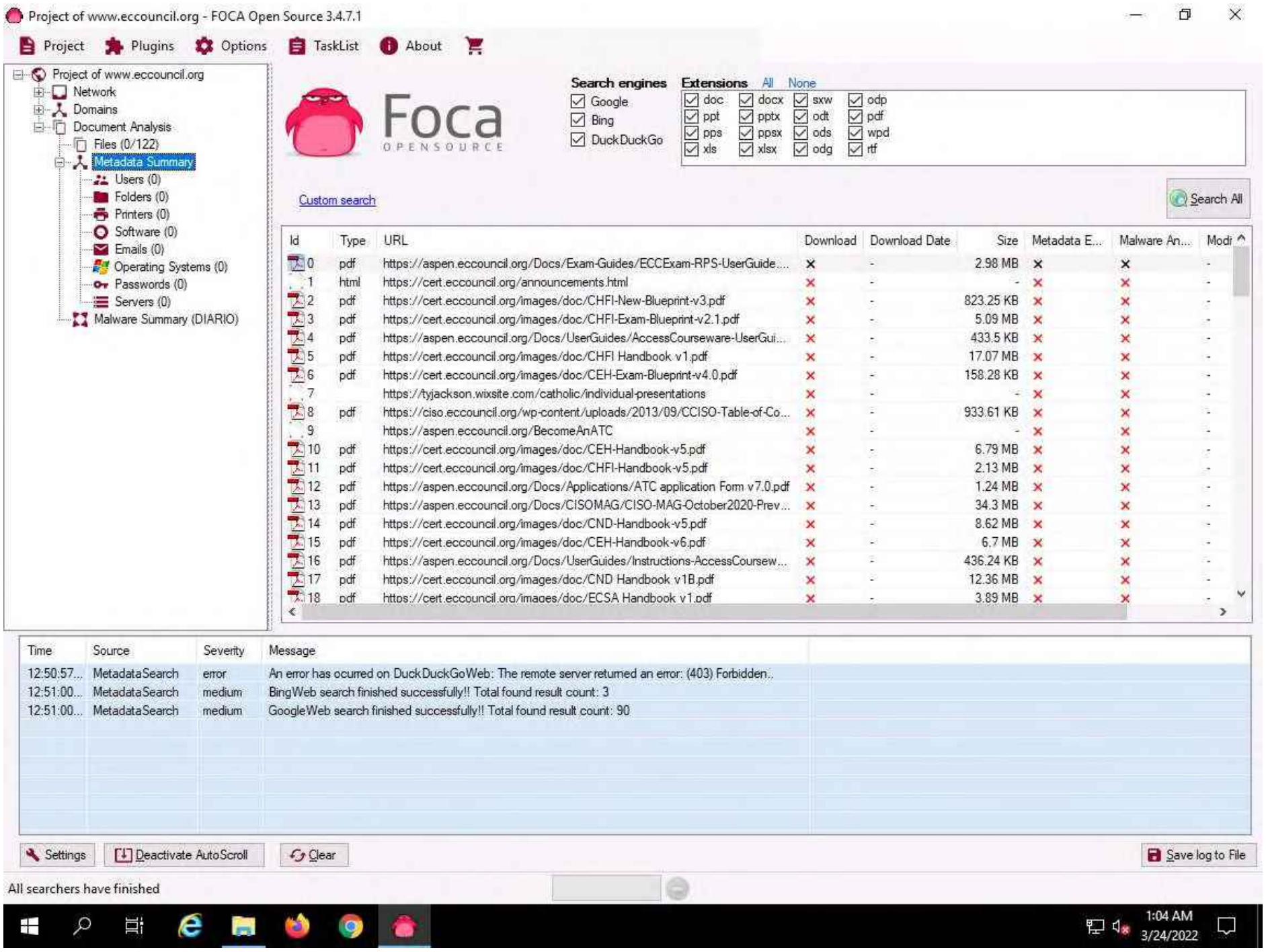
19. Google's crawling functionality begins crawling the target website. Once the crawling is completed, results appear in the lower pane.

20. The results include the domains obtained through scanning along with their severity as low, medium or high is displayed, as shown in the screenshot. Using this information, attackers can further find vulnerabilities in the target domain and exploit them to launch web application attacks.



21. Now, expand the **Document Analysis** node; further expand the **Metadata Summary** node. Here, information regarding users, folders, printers, software, etc. is displayed.

Note: The domain we used does not have information associated with metadata summary.



22. This concludes the demonstration of gathering useful information about the target organization using the FOCA tool.

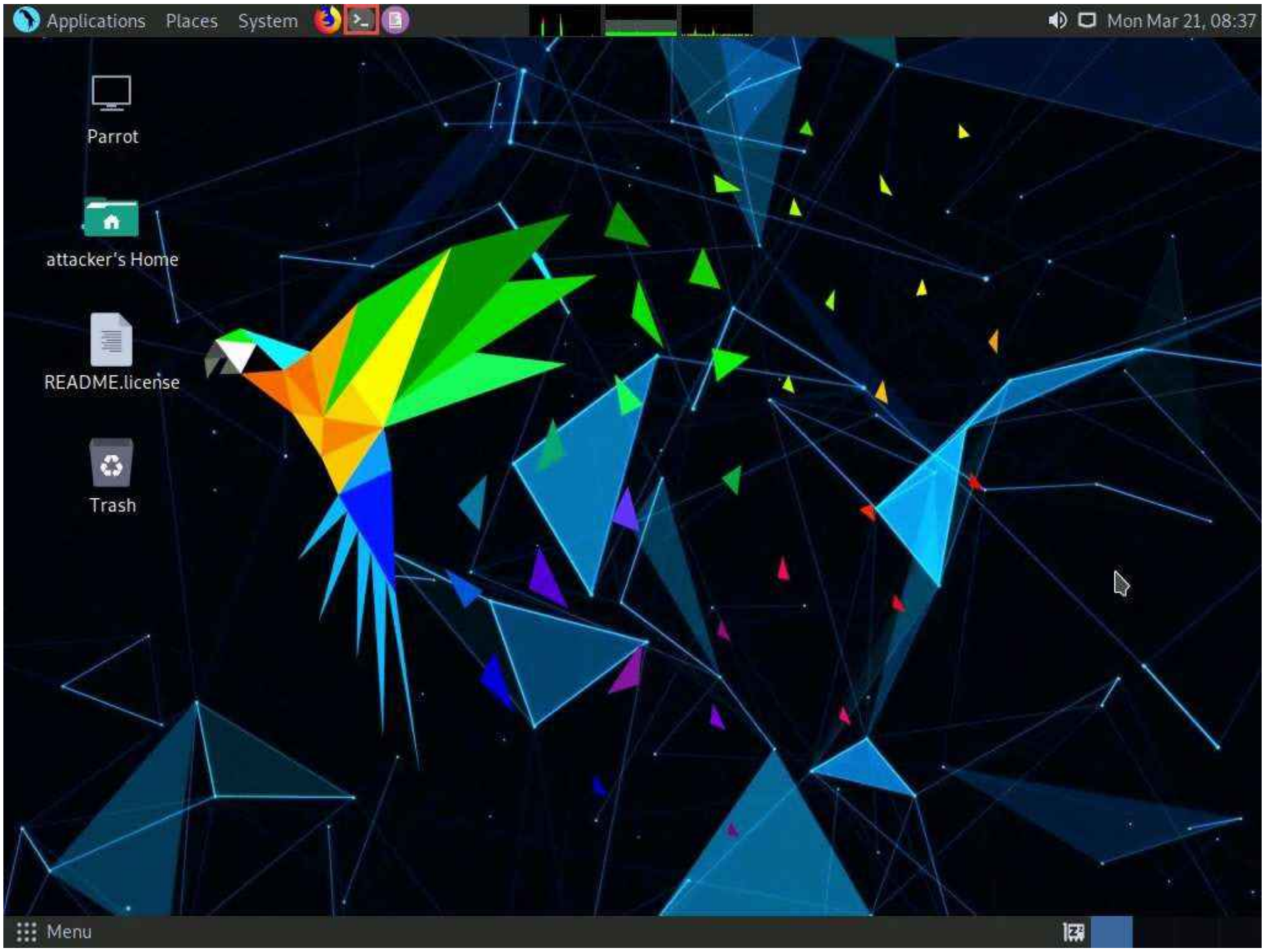
23. Close all open windows and document all the acquired information.

Task 5: Footprinting a Target using BillCipher

BillCipher is an information gathering tool for a Website or IP address. Using this tool, you can gather information such as DNS Lookup, Whois lookup, GeoIP Lookup, Subnet Lookup, Port Scanner, Page Links, Zone Transfer, HTTP Header, etc. Here, we will use the BillCipher tool to footprint a target website URL.

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

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.

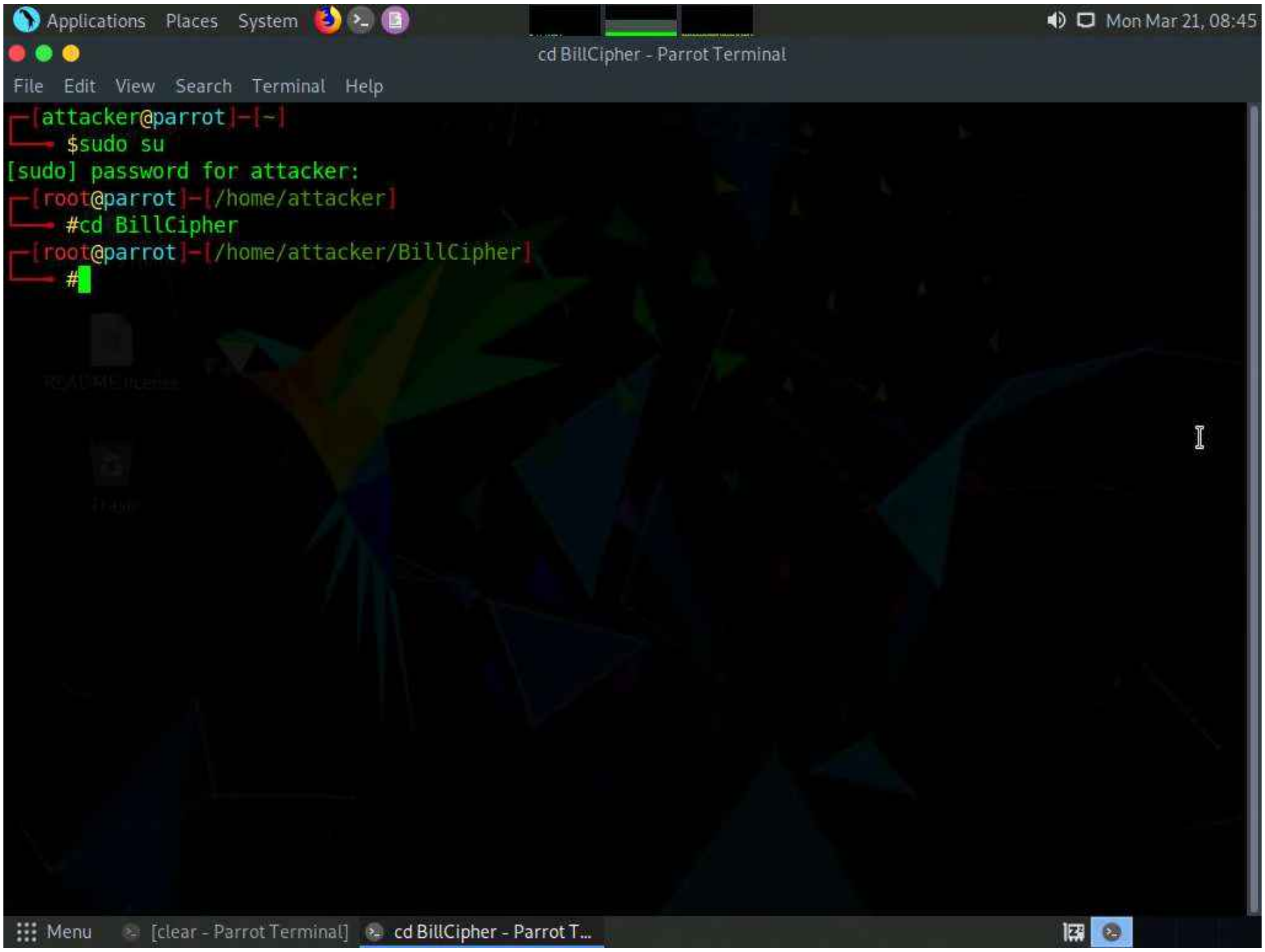


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

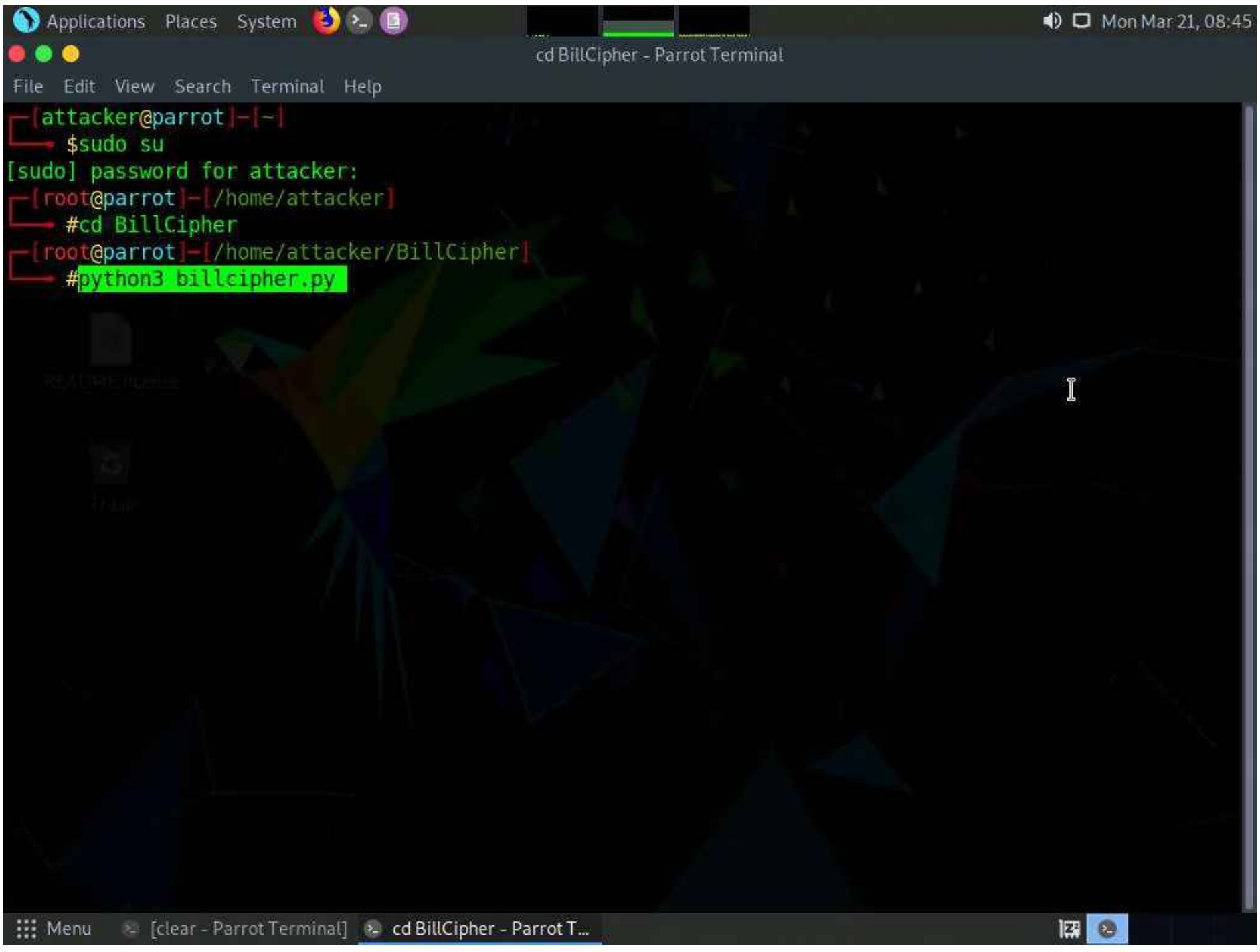
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

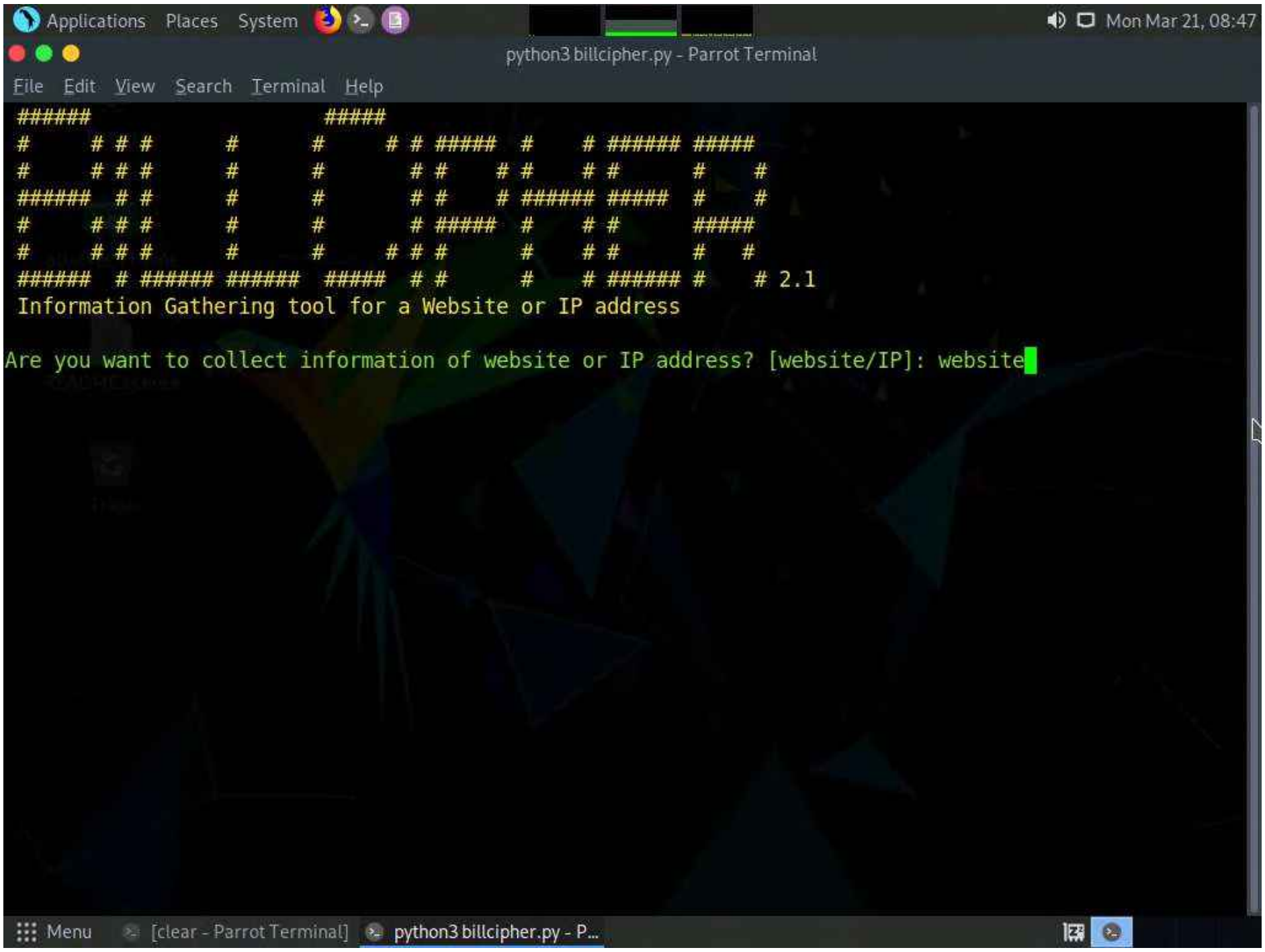
4. In the **Parrot Terminal** window, type **cd BillCipher** and press **Enter** to navigate to the BillCipher directory.



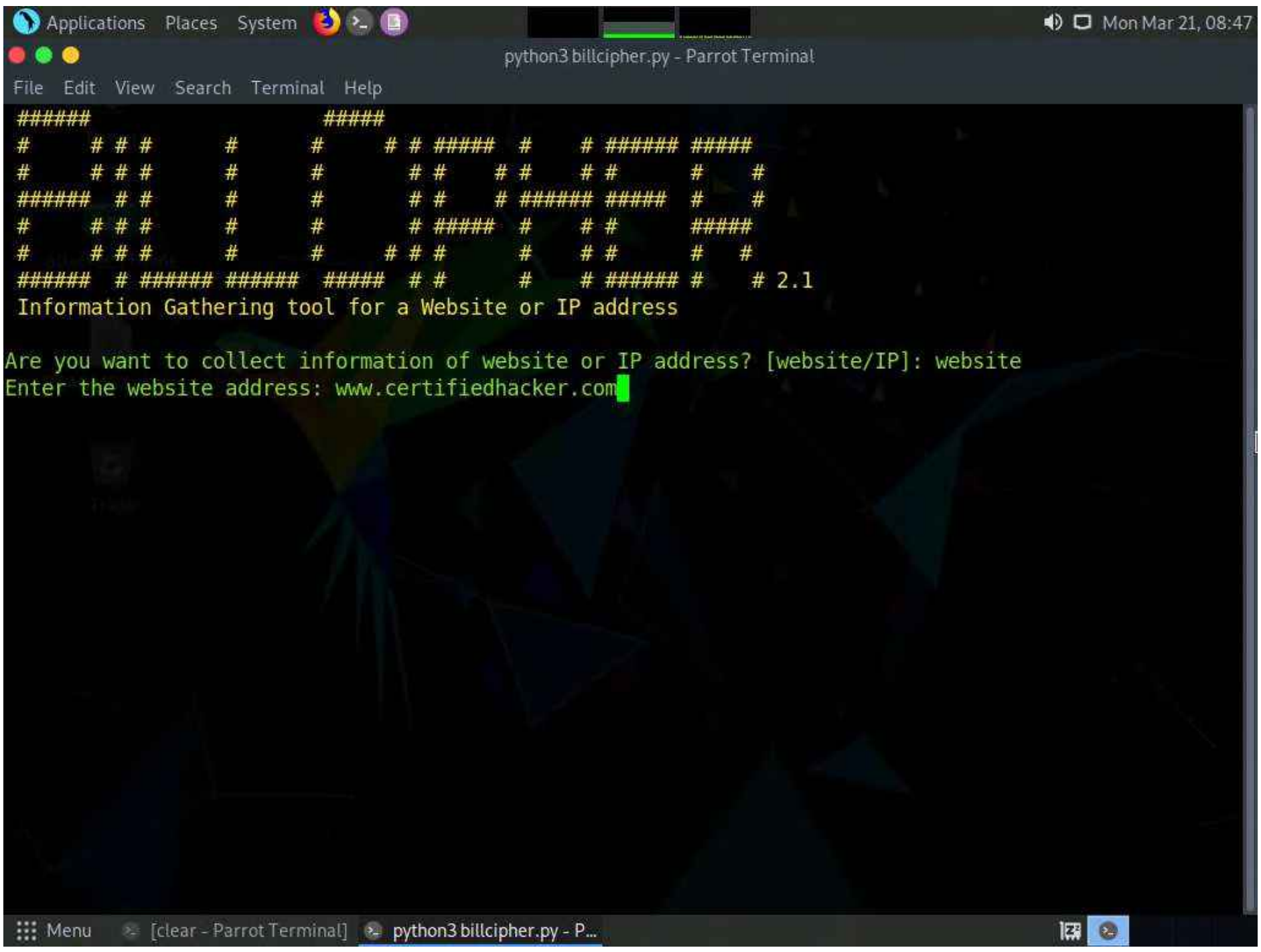
5. Now, type **python3 billcipher.py** and press **Enter** to launch the application.



6. BillCipher application initializes. In the **Are you want to collect information of a website or IP address?** option, type **website** and press **Enter**.



7. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

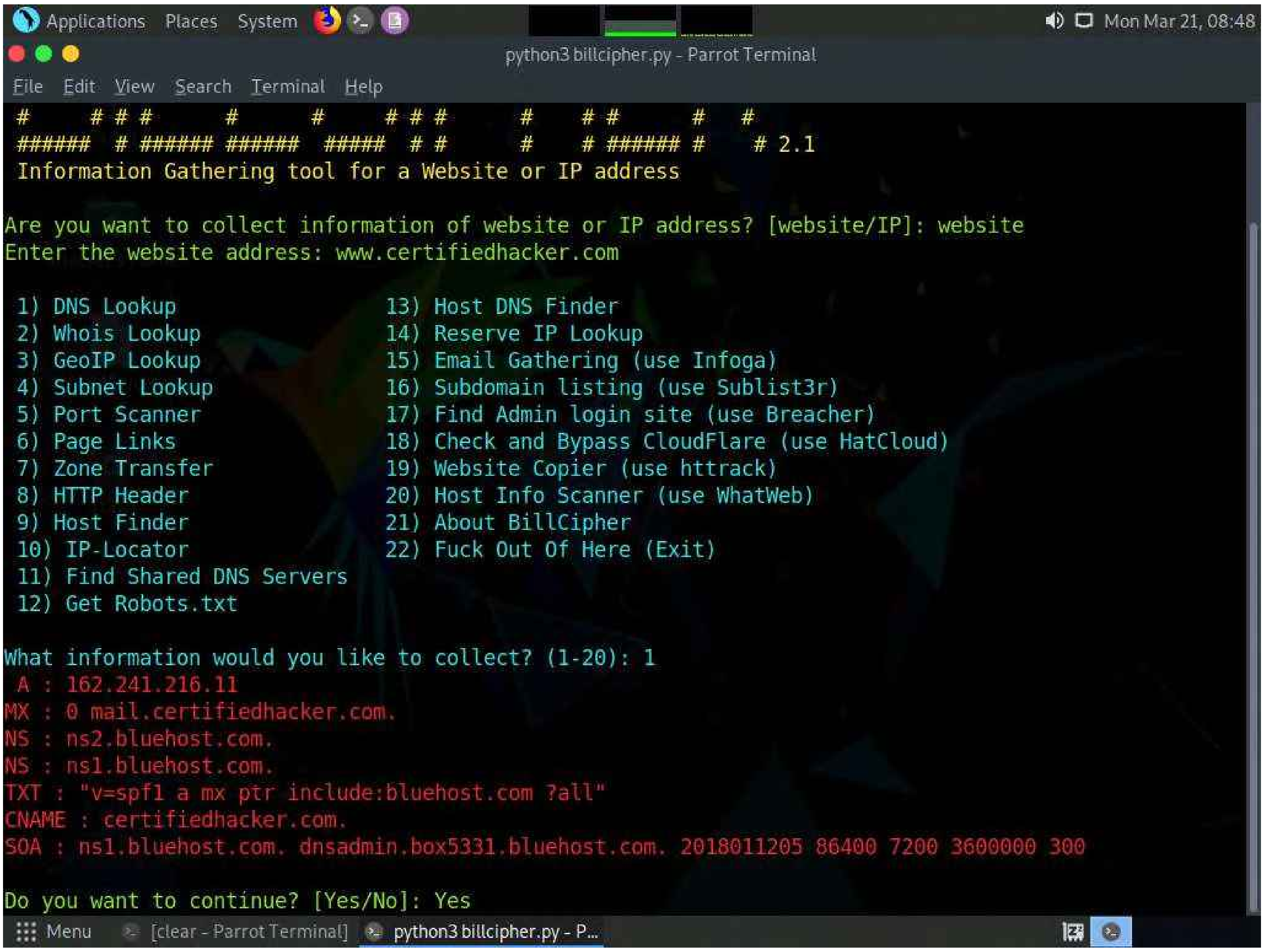


8. BillCipher displays various available options that you can use to gather information regarding a target website.

9. In the **What information would you like to collect?** option, type **1** to choose the **DNS Lookup** option and press **Enter**.

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

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



12. **Are you want to collect information of a website or IP address?** option appears, type **website** and press **Enter**.

13. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

14. Now, type **3** and press **Enter** to choose the **GeoIP Lookup** option from the available information gathering options.

```
Applications  Places  System                                   Mon Mar 21, 08:49
                          python3 billcipher.py - Parrot Terminal
File  Edit  View  Search  Terminal  Help
 12) Get Robots.txt

What information would you like to collect? (1-20): 1
 A : 162.241.216.11
MX : 0 mail.certifiedhacker.com.
NS : ns2.bluehost.com.
NS : ns1.bluehost.com.
TXT : "v=spf1 a mx ptr include:bluehost.com ?all"
CNAME : certifiedhacker.com.
SOA : ns1.bluehost.com. dnsadmin.box5331.bluehost.com. 2018011205 86400 7200 3600000 300

Do you want to continue? [Yes/No]: Yes

Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

 1) DNS Lookup                    13) Host DNS Finder
 2) Whois Lookup                  14) Reserve IP Lookup
 3) GeoIP Lookup                  15) Email Gathering (use Infoga)
 4) Subnet Lookup                 16) Subdomain listing (use Sublist3r)
 5) Port Scanner                  17) Find Admin login site (use Breacher)
 6) Page Links                    18) Check and Bypass CloudFlare (use HatCloud)
 7) Zone Transfer                 19) Website Copier (use httrack)
 8) HTTP Header                   20) Host Info Scanner (use WhatWeb)
 9) Host Finder                   21) About BillCipher
 10) IP-Locator                   22) Fuck Out Of Here (Exit)
 11) Find Shared DNS Servers
 12) Get Robots.txt

What information would you like to collect? (1-20): 3
Menu  [clear - Parrot Terminal]  python3 billcipher.py - P...
```

15. The result appears, displaying the **GeoIP Lookup** information of the target website, as shown in the screenshot.

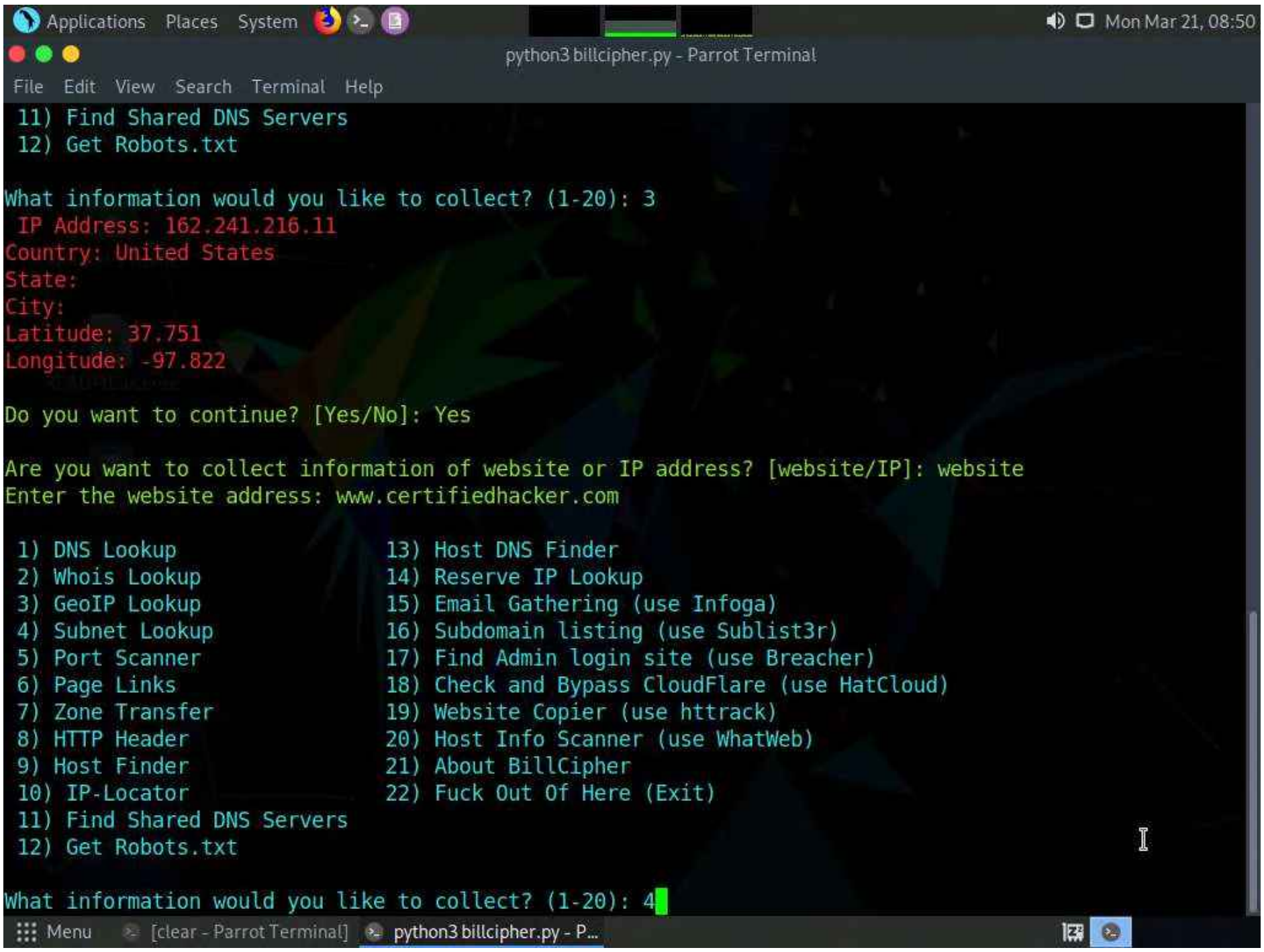
16. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

```
Applications  Places  System                                   Mon Mar 21, 08:49
                          python3 billcipher.py - Parrot Terminal
File  Edit  View  Search  Terminal  Help
CNAME : certifiedhacker.com.
SOA : ns1.bluehost.com. dnsadmin.box5331.bluehost.com. 2018011205 86400 7200 3600000 300

Do you want to continue? [Yes/No]: Yes

Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

 1) DNS Lookup                    13) Host DNS Finder
 2) Whois Lookup                  14) Reserve IP Lookup
 3) GeoIP Lookup                  15) Email Gathering (use Infoga)
 4) Subnet Lookup                 16) Subdomain listing (use Sublist3r)
 5) Port Scanner                  17) Find Admin login site (use Breacher)
 6) Page Links                    18) Check and Bypass CloudFlare (use HatCloud)
 7) Zone Transfer                 19) Website Copier (use httrack)
 8) HTTP Header                   20) Host Info Scanner (use WhatWeb)
 9) Host Finder                   21) About BillCipher
 10) IP-Locator                   22) Fuck Out Of Here (Exit)
 11) Find Shared DNS Servers
 12) Get Robots.txt

What information would you like to collect? (1-20): 3
 IP Address: 162.241.216.11
Country: United States
State:
City:
Latitude: 37.751
Longitude: -97.822

Do you want to continue? [Yes/No]: Yes
Menu  [clear - Parrot Terminal]  python3 billcipher.py - P...
```

17. **Are you want to collect information of a website or IP address?** option appears, type **website** and press **Enter**.

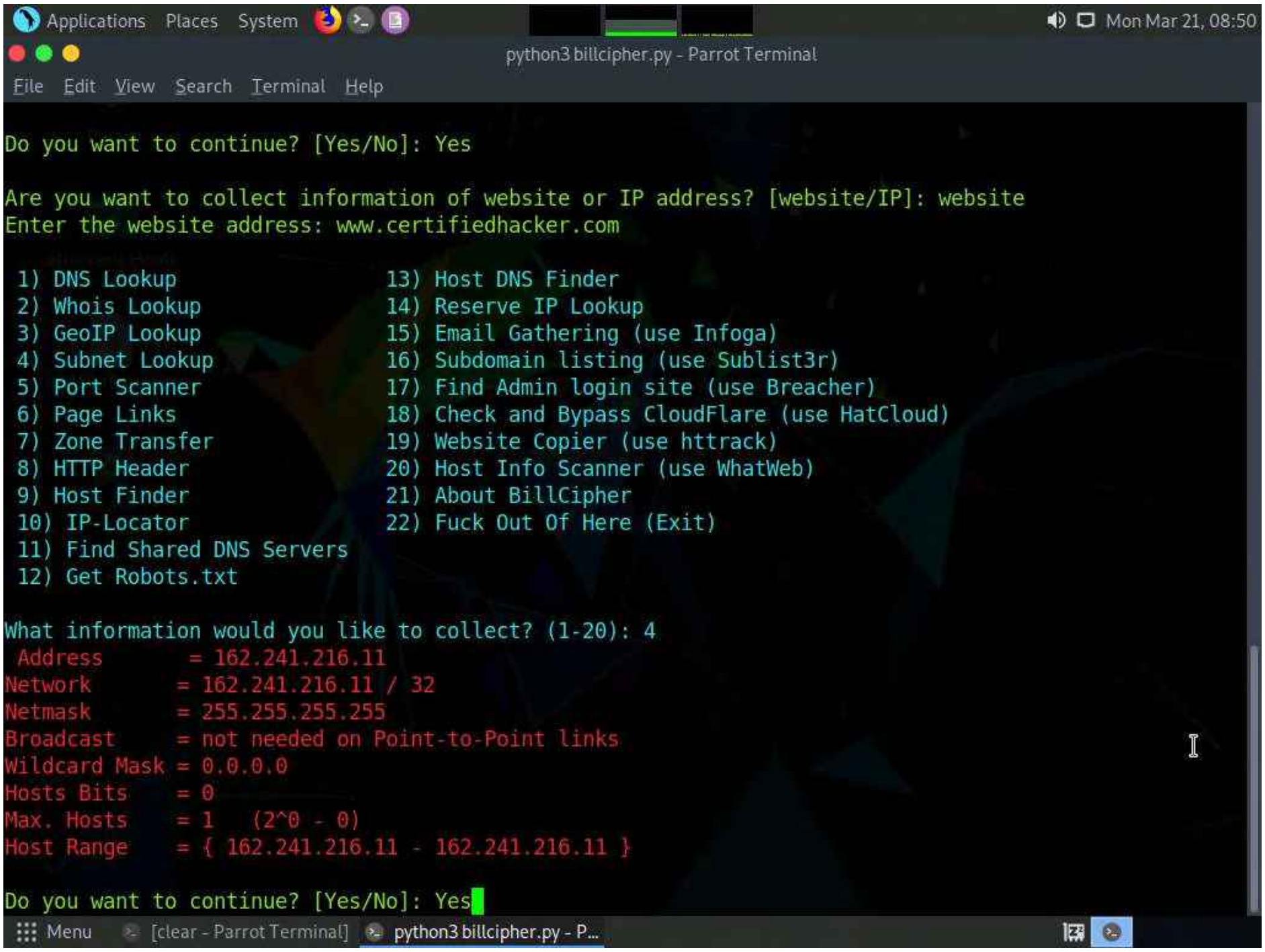
18. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

19. Now, type **4** and press **Enter** to choose the **Subnet Lookup** option from the available information gathering options.



20. The result appears, displaying the **Subnet Lookup** information of the target website.

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



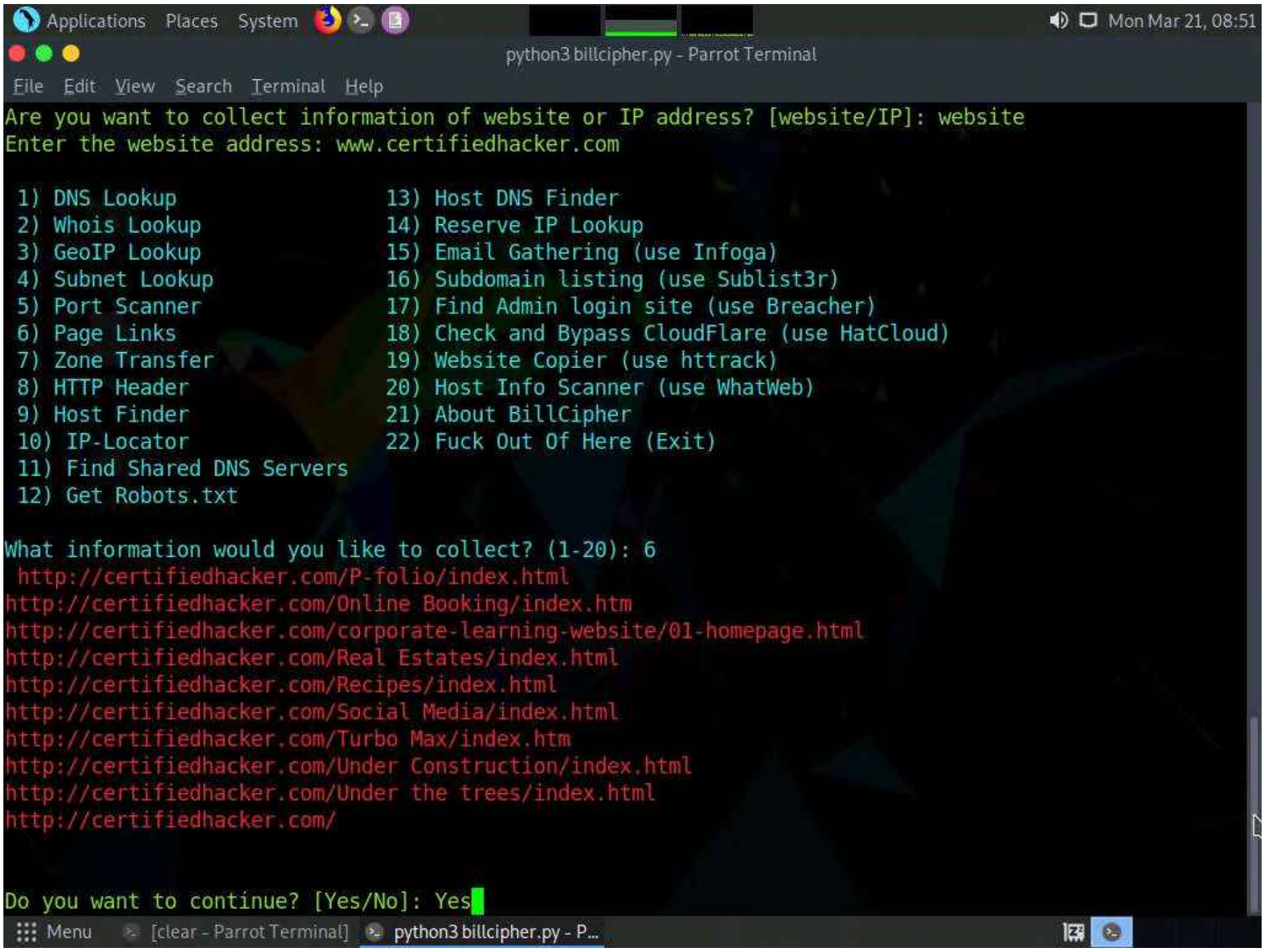
22. **Are you want to collect information of a website or IP address?** option appears, type **website** and press **Enter**.

23. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

24. Now, type **6** and press **Enter** to choose the **Page Links** option from the available information gathering options.

25. The result appears, displaying a list of **Visible links** and **Hidden links** of the target website, as shown in the screenshot.

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



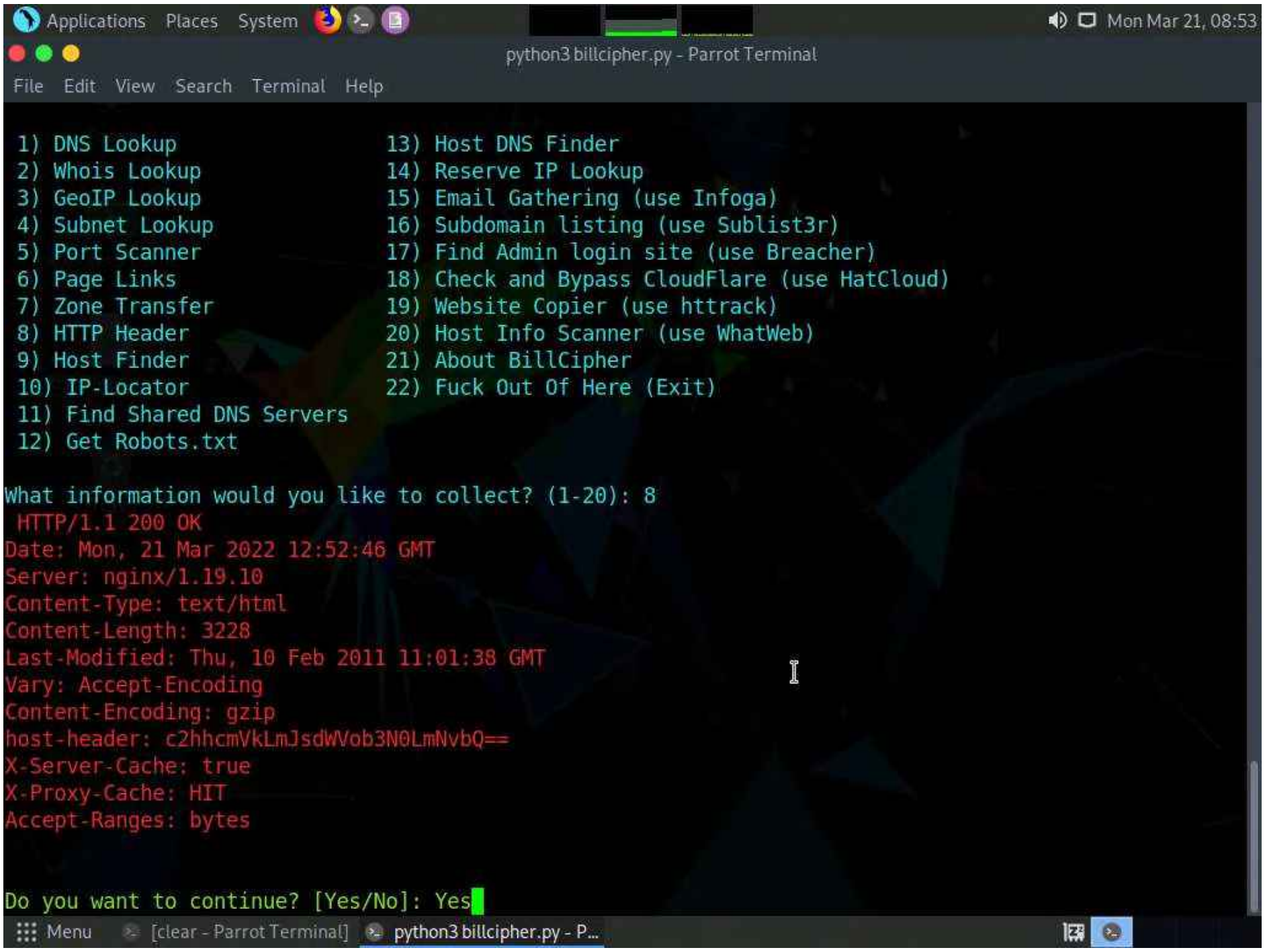
27. **Are you want to collect information of a website or IP address?** option appears, type **website** and press **Enter**.

28. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

29. Now, type **8** and press **Enter** to choose the **HTTP Header** option from the available information gathering options.

30. The result appears, displaying information regarding the HTTP header of the target website, as shown in the screenshot.

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

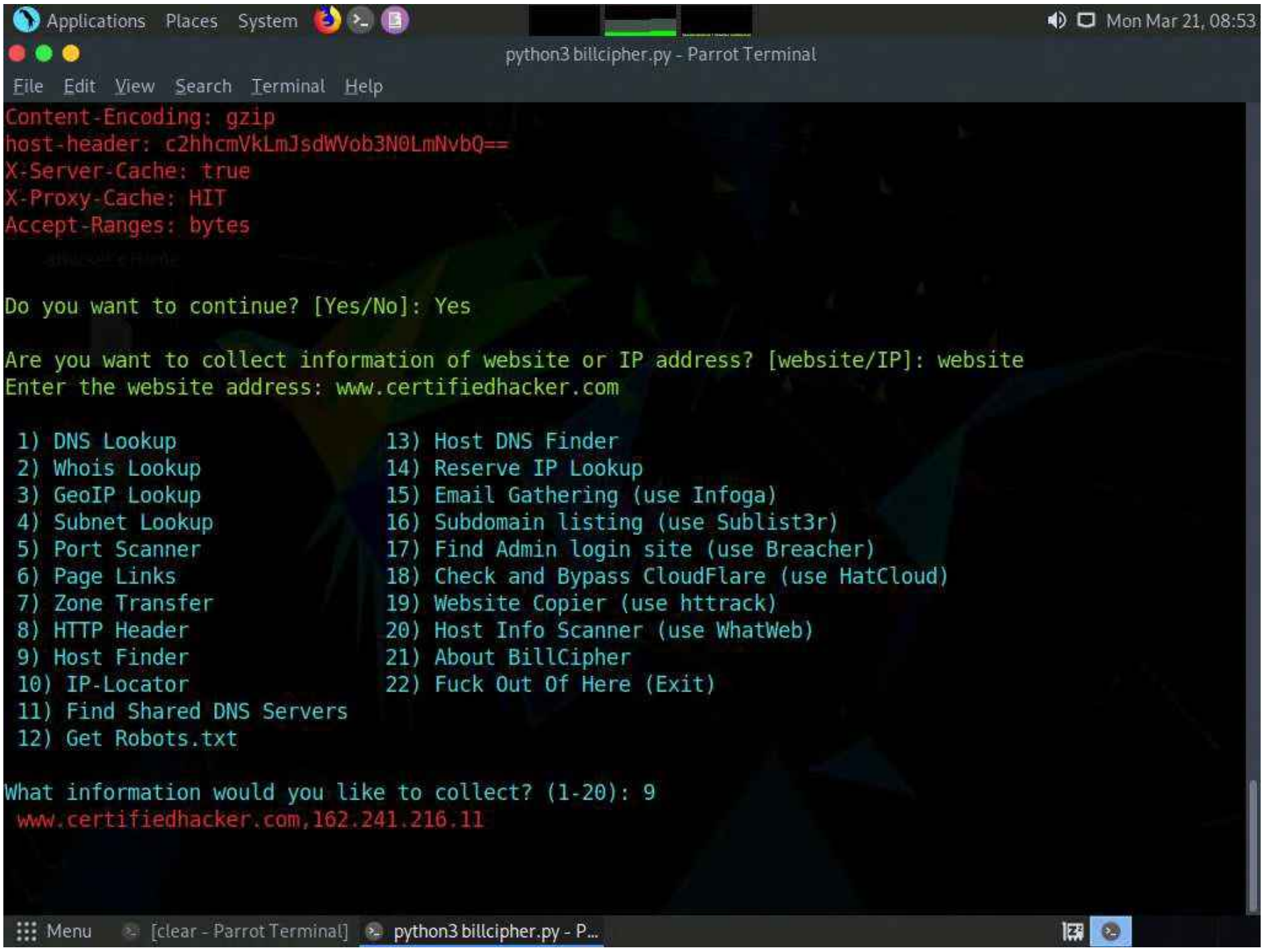


32. **Are you want to collect information of a website or IP address?** option appears, type **website** and press **Enter**.

33. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

34. Now, type **9** and press **Enter** to choose **Host Finder** option from the available information gathering option.

35. The result appears, displaying information regarding the IP address of the target website, as shown in the screenshot.



36. Similarly, you can use other information gathering options to gather information about the target.

37. This concludes the demonstration of footprinting the target website URL using BillCipher.

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

Task 6: Footprinting a Target using OSINT Framework

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

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

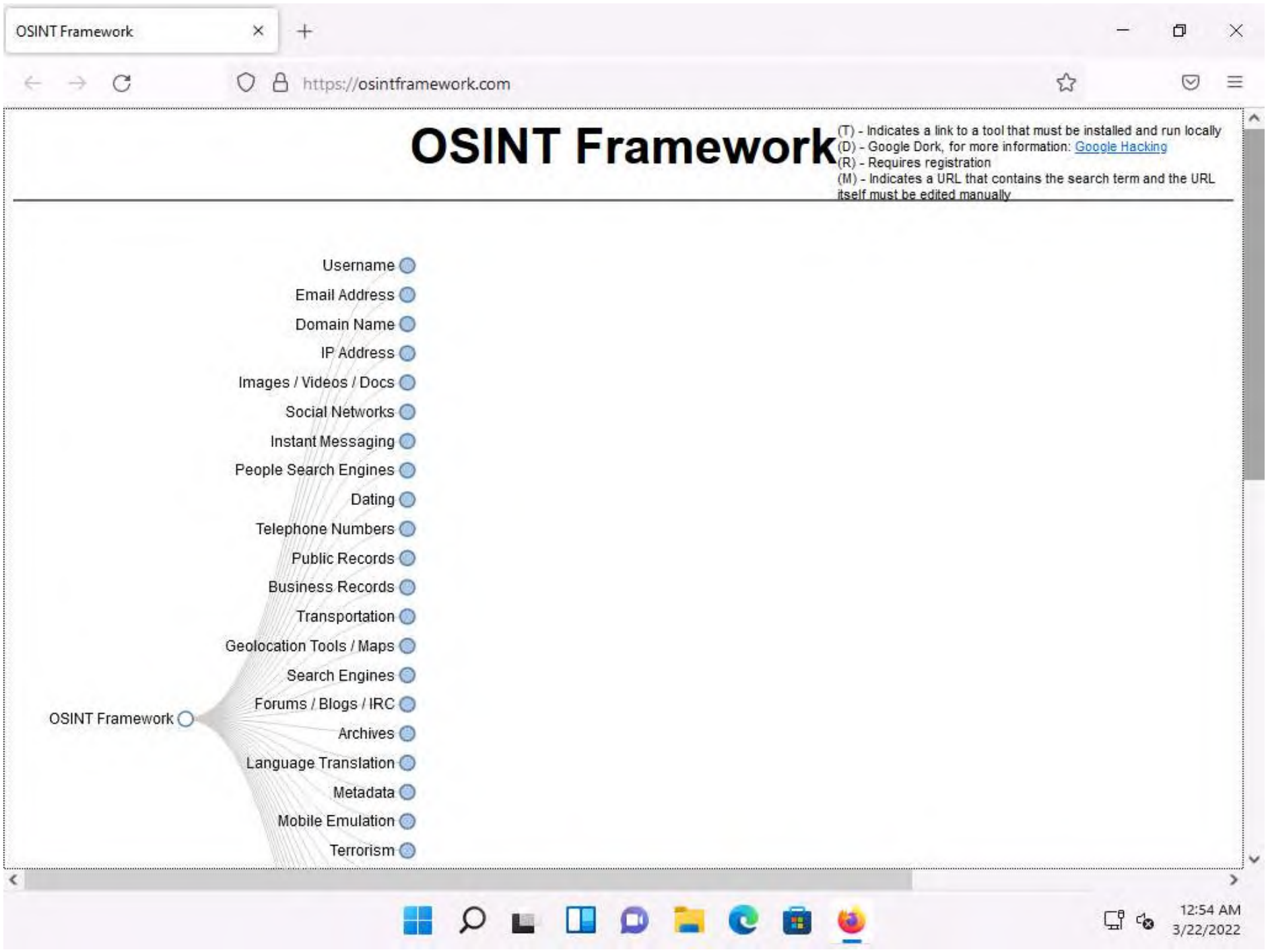
(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually

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

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://osintframework.com/** and press **Enter**.

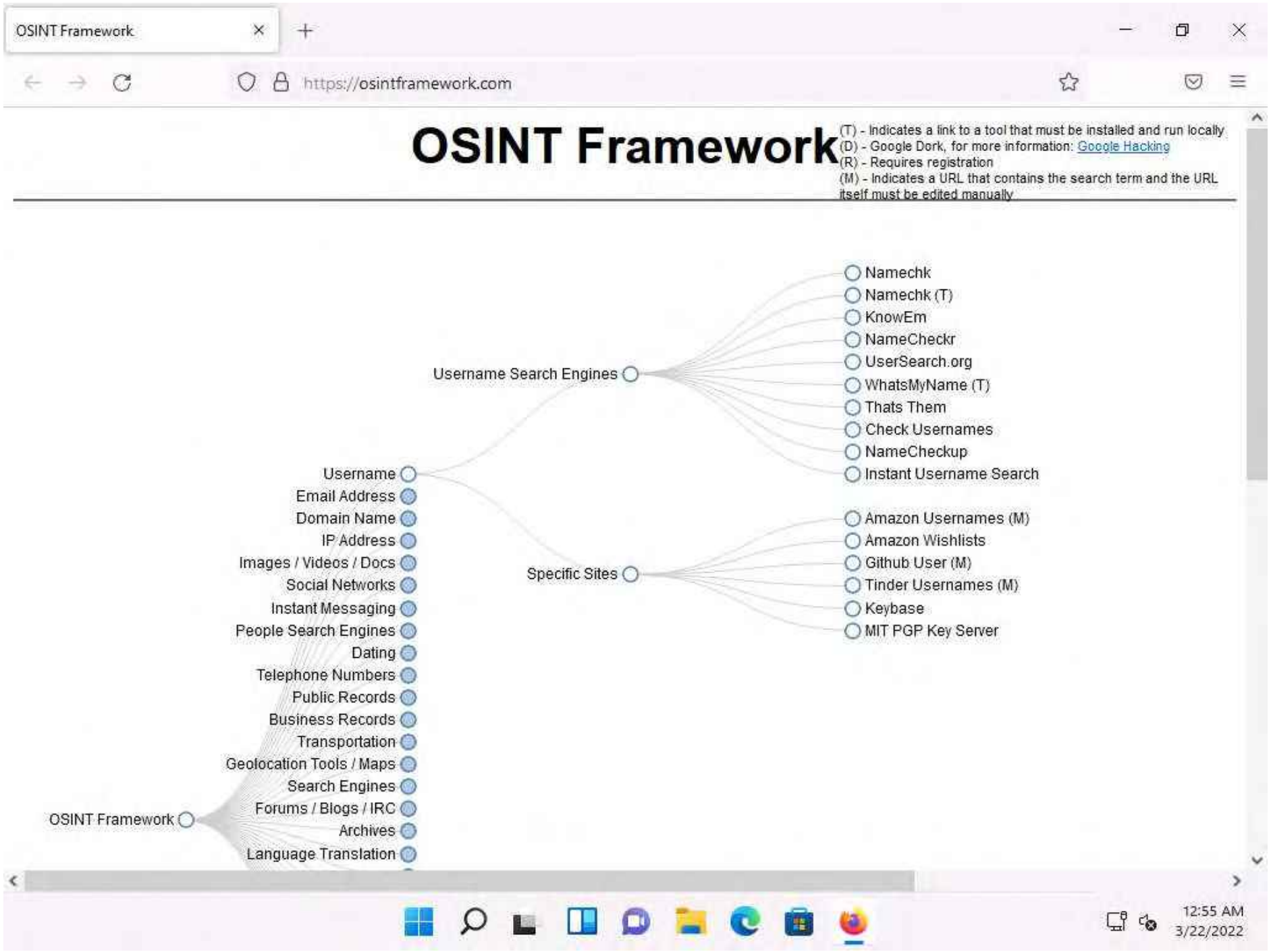
3. **OSINT Framework** website appears; you can observe the OSINT tree on the left side of screen, as shown in the screenshot.



4. Clicking on any of the categories such as **Username**, **Email Address**, or **Domain Name** will make many useful resources appear on the screen in the form of a sub-tree.

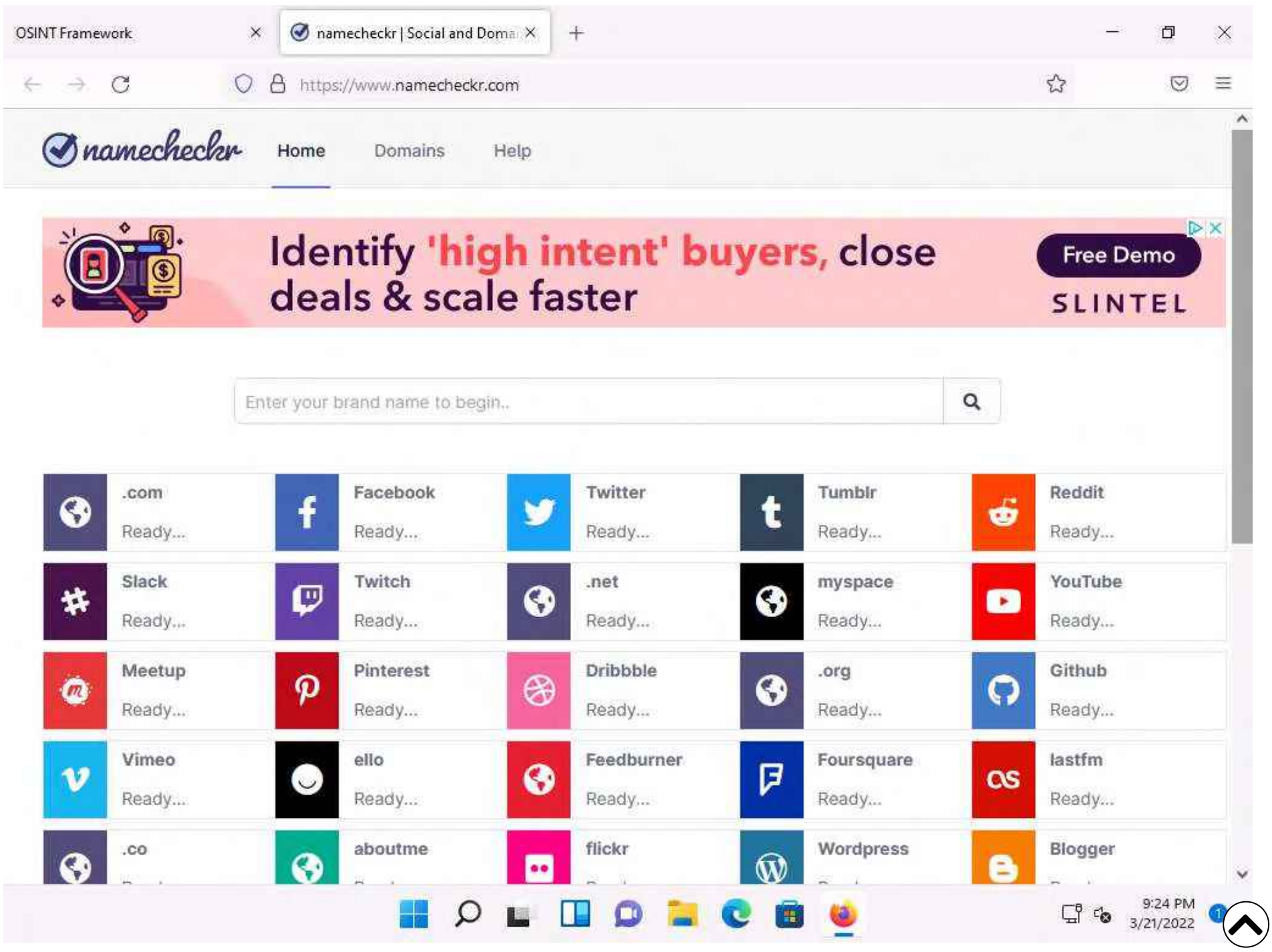
5. Click the **Username** category and click to expand the **Username Search Engines** and **Specific Sites** sub-categories.

6. You can observe a list of OSINT tools filtered by sub-categories (**Username Search Engines** and **Specific Sites** sub-categories).

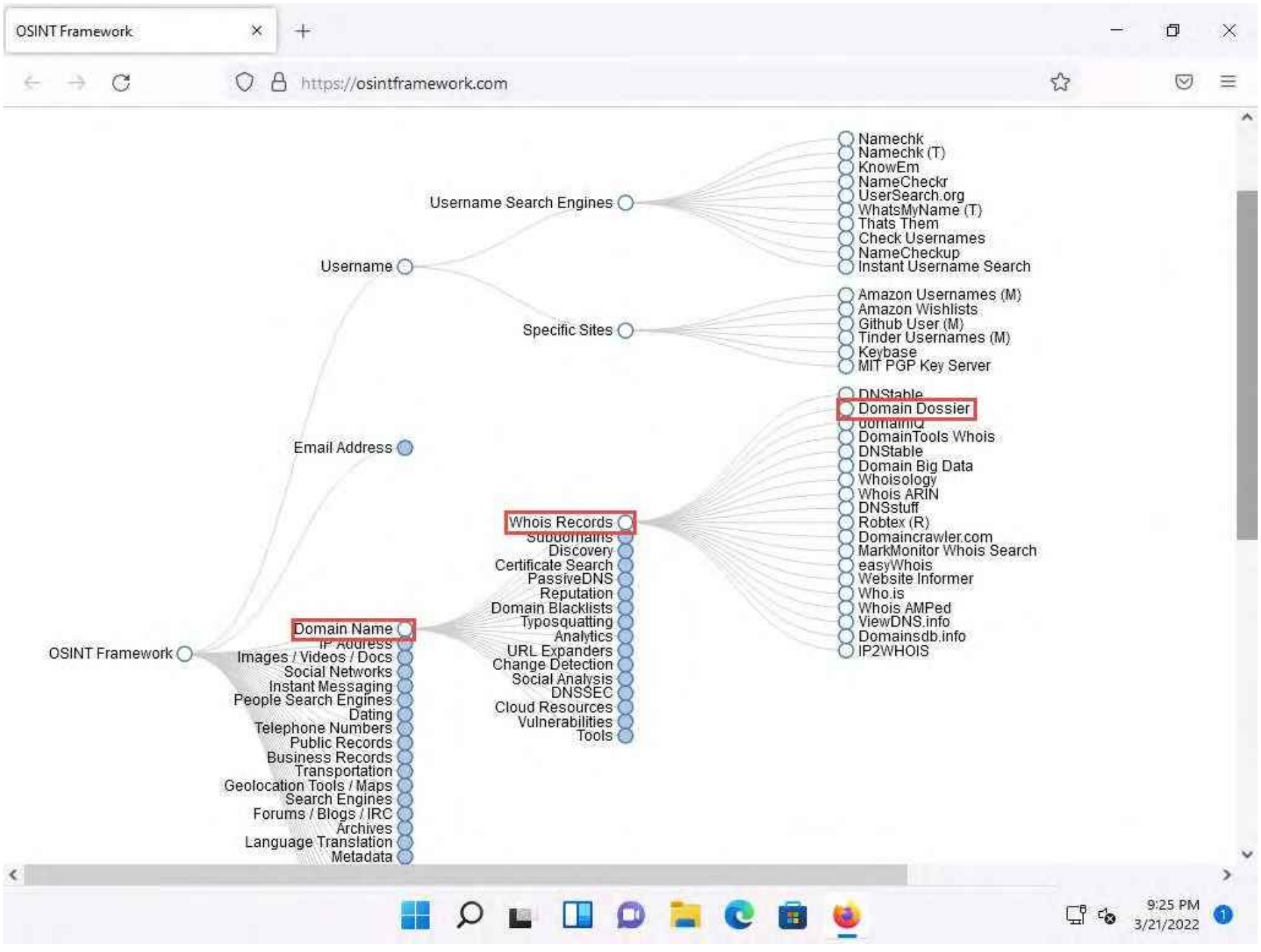


7. From the list of available tools under the **Username Search Engines** category, click on the **NameCheckr** tool to navigate to the **NameCheckr** website.

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

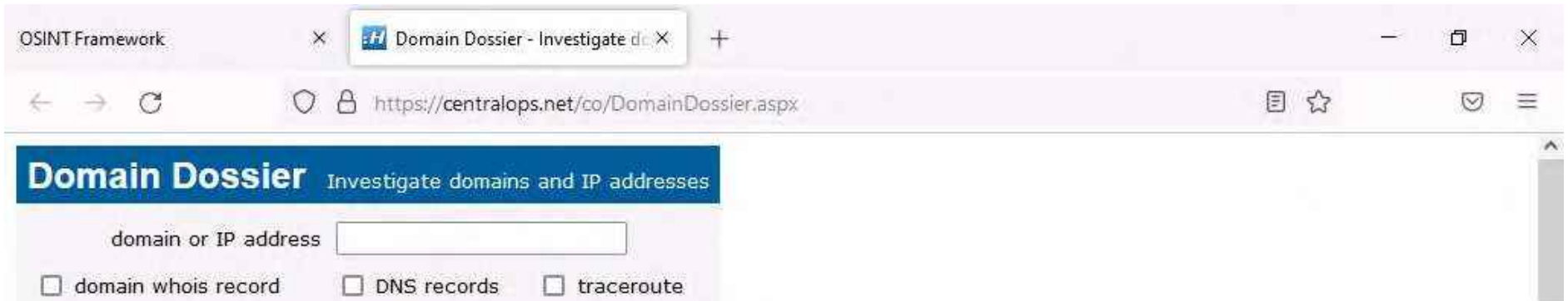


9. Close the current tab to navigate back to the OSINT Framework webpage.
10. Similarly, you can explore other tools from the list of mentioned tools under the **Username Search Engines** and **Specific Sites** sub-categories.
11. Now, click the **Domain Name** category, and its sub-categories appear. Click to expand the **Whois Records** sub-category.
12. A list of tools under the **Whois Records** sub-category appears; click the **Domain Dossier** tool.



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

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



About Domain Dossier

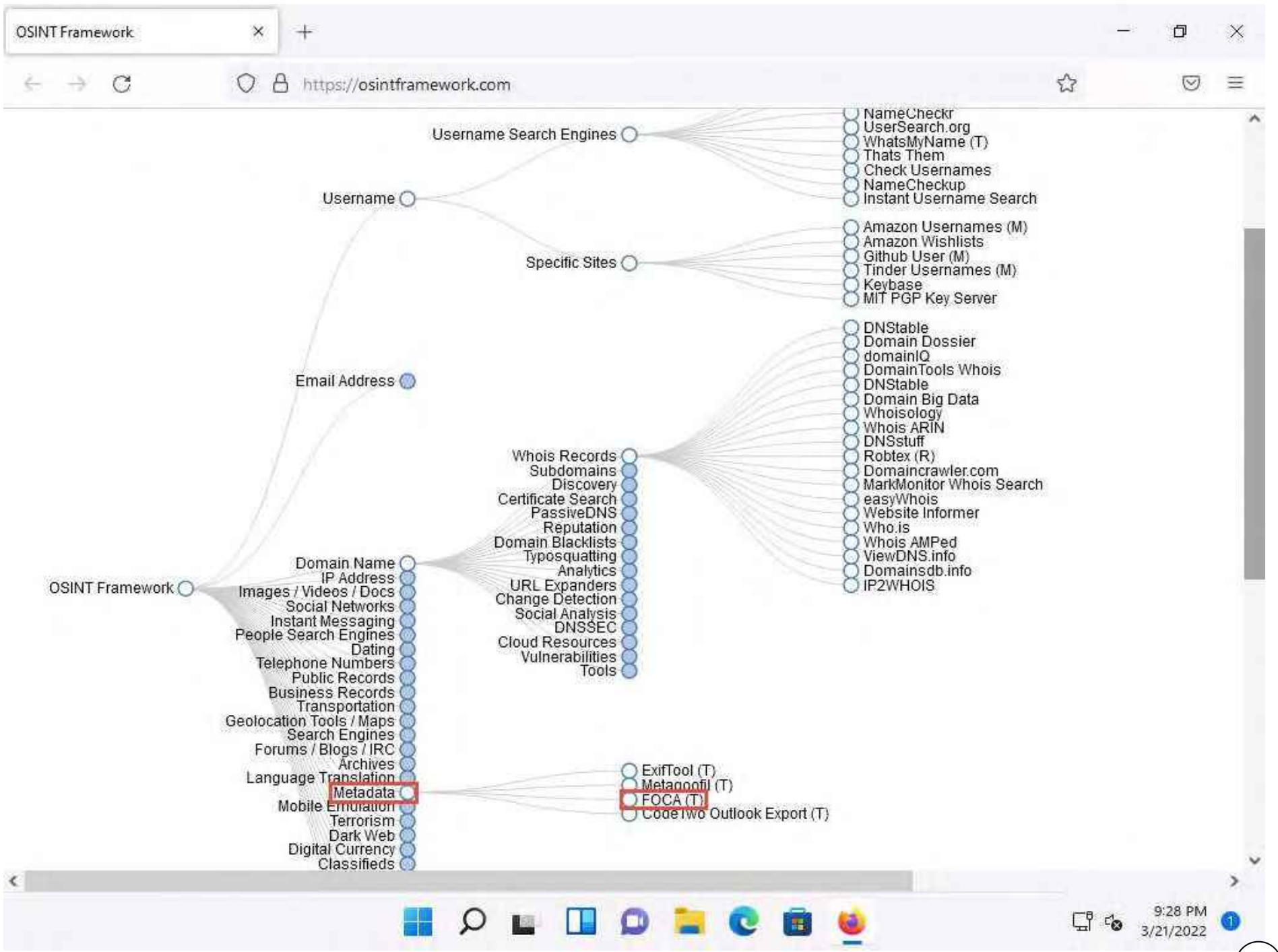
The Domain Dossier tool generates **reports from public records** about domain names and IP addresses to help solve problems, investigate cybercrime, or just better understand how things are set up. These reports may show you:

- Owner's contact information
- Registrar and registry information
- The company that is hosting a Web site
- Where an IP address is geographically located
- What type of server is at the address
- The upstream networks of a site
- and much more

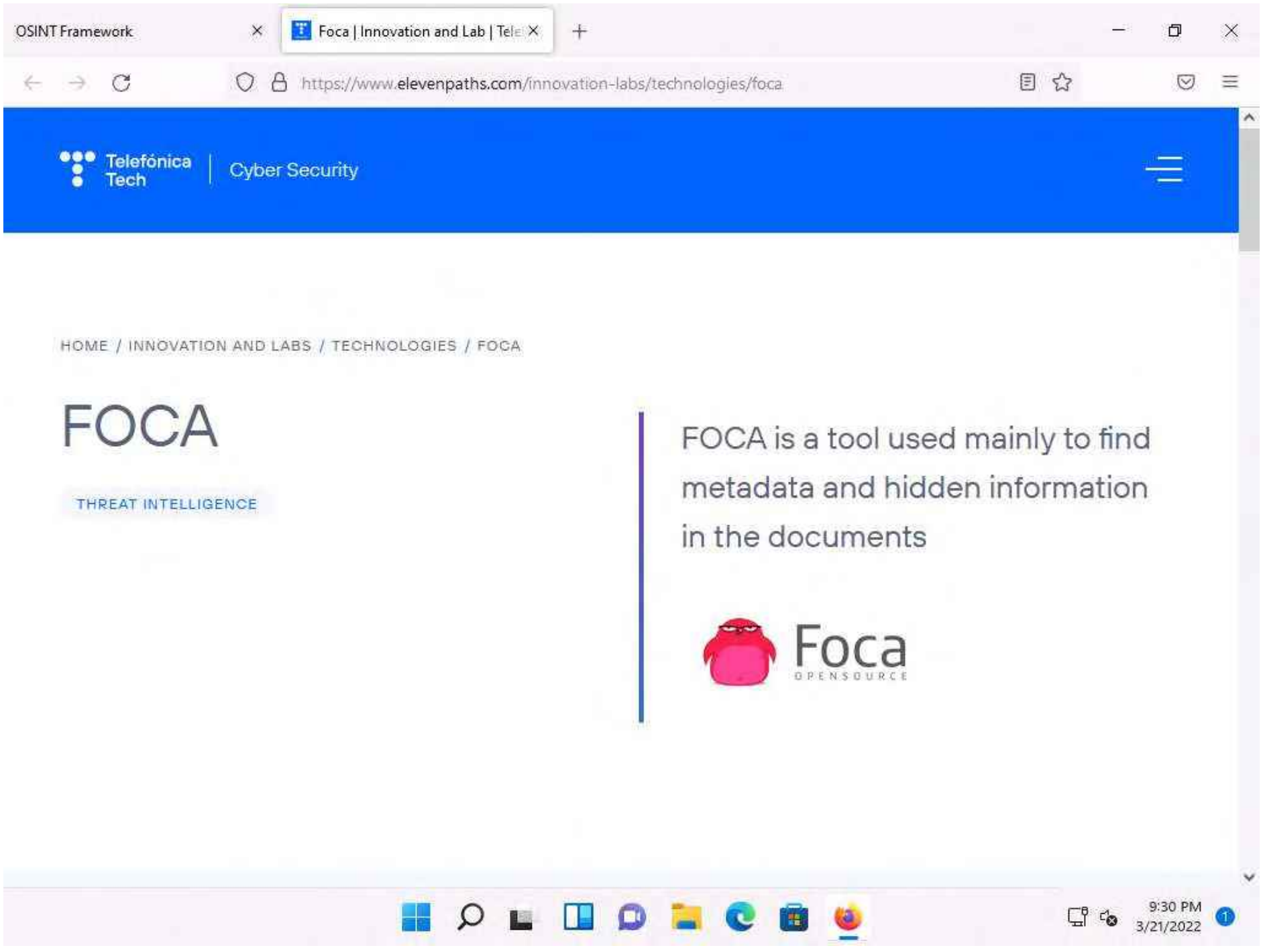
Domain Dossier normally gets records from their original sources *at the time you request them*, but it does keep copies in memory for up to 24 hours. Thus, if someone has already requested a particular Dossier, the records shown *could be up to a day old*.

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

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



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



17. Similarly, you can explore other available categories such as **Email Address**, **IP Address**, **Social Networks**, **Instant Messaging**, etc. and the tools associated with each category. Using these tools, you can perform footprinting on the target organization.

18. This concludes the demonstration of performing footprinting using the OSINT Framework.

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

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