

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.

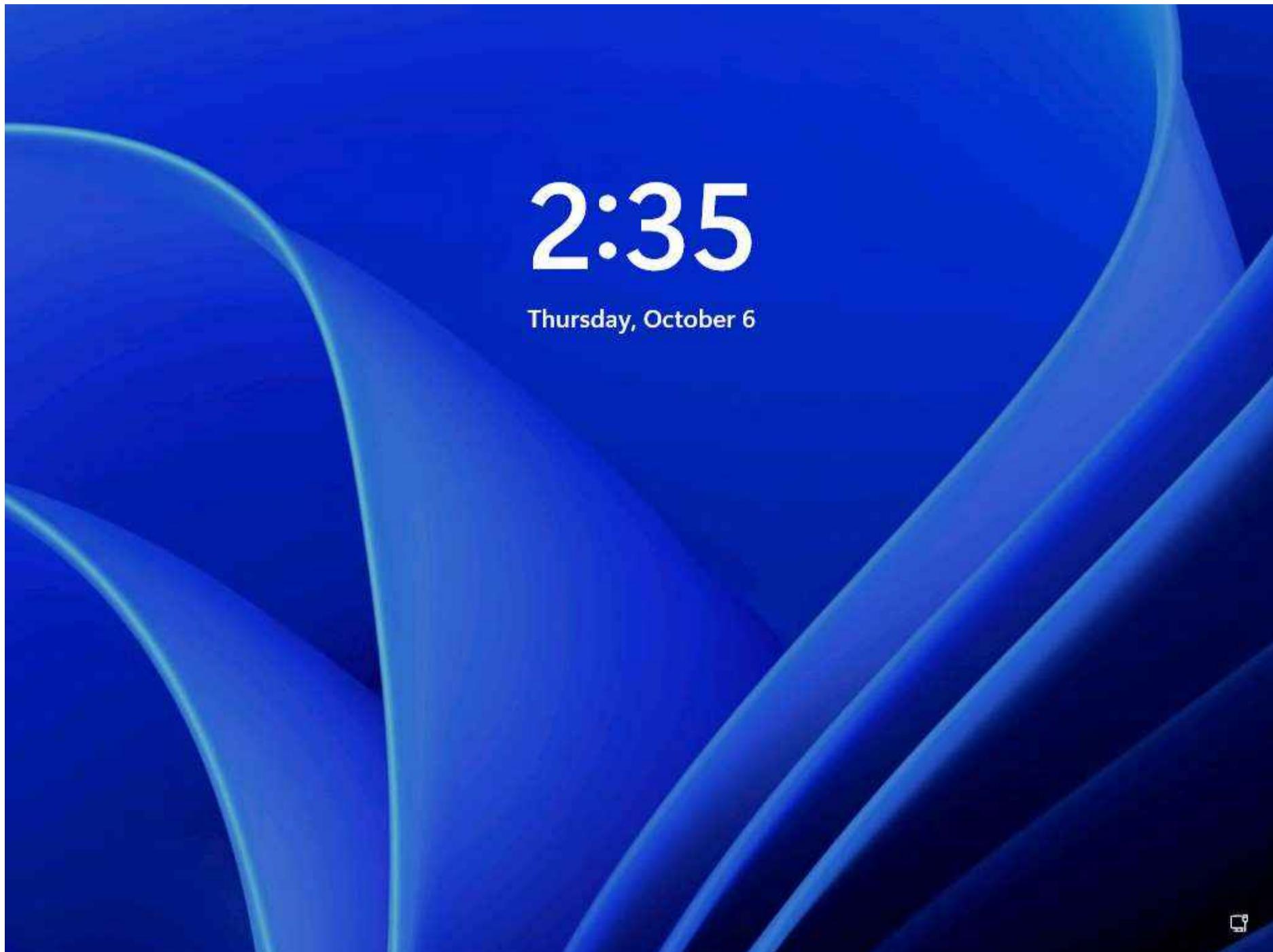


Task 1: Gather Information using Advanced Google Hacking Techniques

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**.

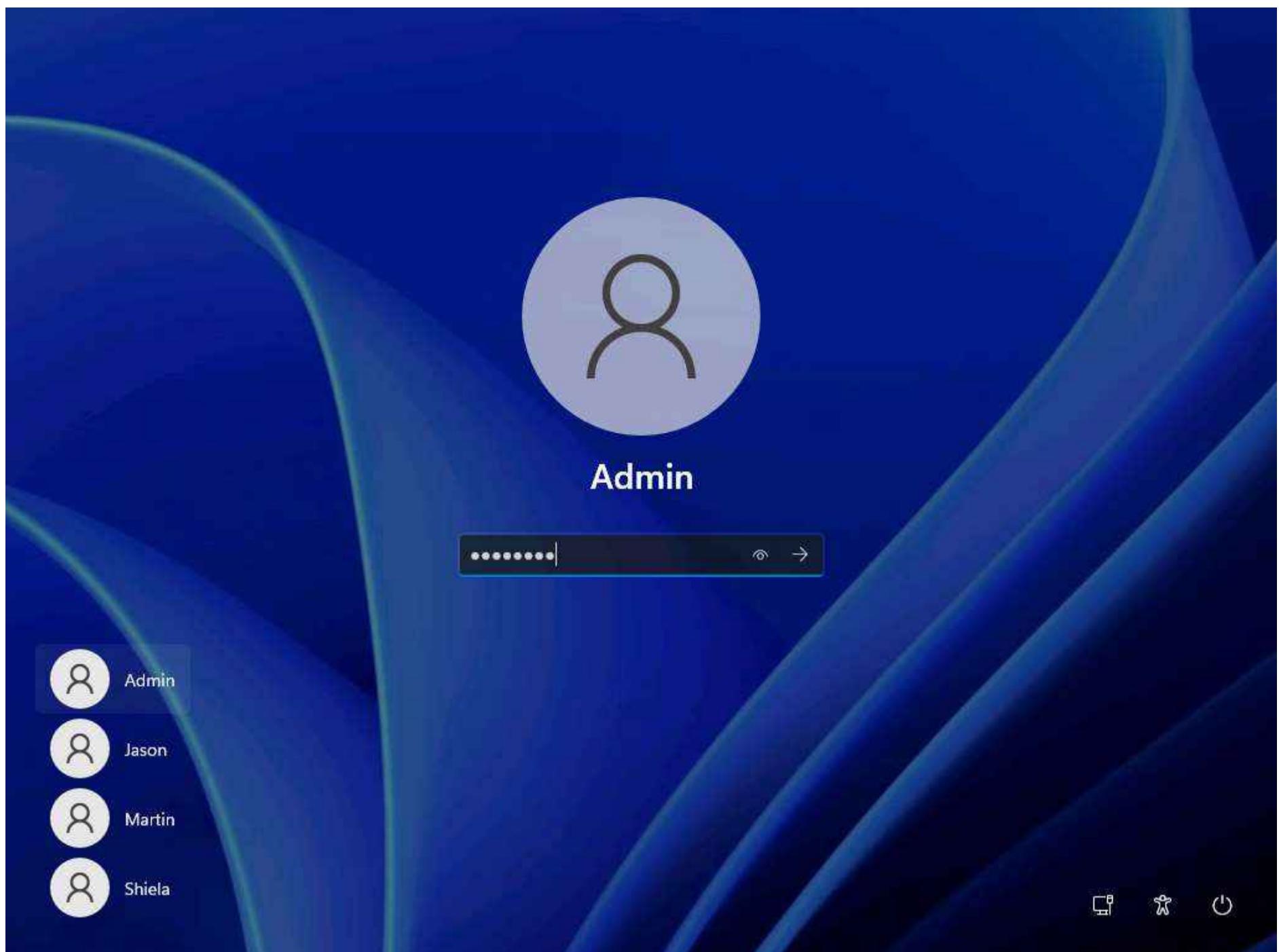


2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

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**.

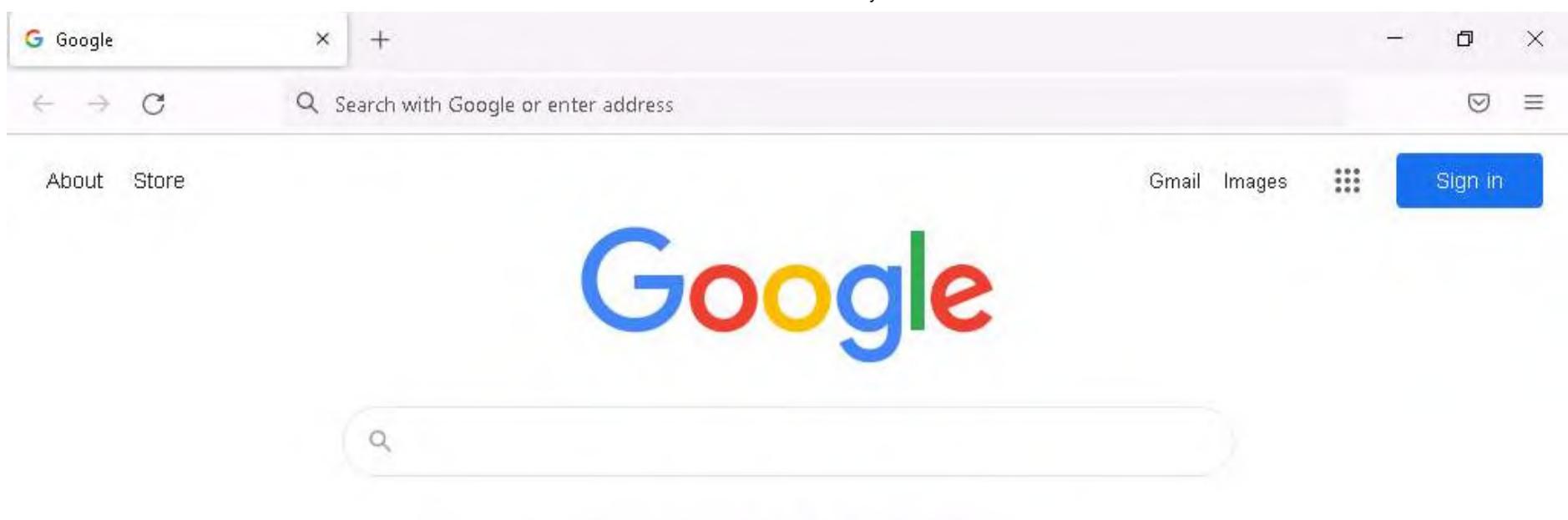
Note:

- 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**.





Singapore

[Advertising](#) [Business](#) [How Search works](#) [Privacy](#) [Terms](#) [Settings](#)2:45 AM
10/6/2022

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.



The screenshot shows a Google search results page. The search query is "intitle:login site:eccouncil.org". The results include links to the EC-Council login page and a thumbnail image for "Images for intitle:login site:eccouncil.org". The image shows two people and text related to EC-Council University.

- https://aspen.eccouncil.org > Account > Login ::
Login - ASPEN – EC-Council
 Type your username and password. Login. Username * Password *
- https://ilabs.eccouncil.org > login ::
Login to iLabs

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

The screenshot shows a Google search results page with the same search query and results as the previous screenshot. It includes the EC-Council login page and the iLabs login page.

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.

EC-Council filetype:pdf ceh - Go +

google.com/search?q=EC-Council+filetype%3Apdf+ceh&lz=1C1VDKB_enUS990US990&ei=mKg-Y9_tKsac3LU... 🔍 ⭐ 📁 🌐 ⚙️ ⋮

Google EC-Council filetype:pdf ceh X ⚙️ ⋮

All Images News Videos Shopping More Tools

About 79,900 results (0.34 seconds)

Ad · https://www.eccu.edu/

Eccu.edu - EC-Council University - 2Yr Masters in Cyber Security

Transform from a professional into a Leader with ECCU's Master's Degree in Cyber Security. DEAC Accredited, 100% Online with Industry Leaders as Faculty. Admissions Open. Apply...

<https://www.eccouncil.org/uploads/2022/09/CEH-brochure.pdf> PDF

CEH-brochure.pdf - EC-Council

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

24 pages

People also search for

- ec-council ceh practice test
- ceh v12 release date
- ec-council ceh v11 book
- ceh syllabus
- ceh v11 blueprint pdf
- ceh ec-council book pdf

People also ask :

Windows Taskbar: 3:09 AM 10/6/2022

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

About 79,900 results (0.34 seconds)

Ad • https://www.eccu.edu/

Eccu.edu - EC-Council University - 2Yr Masters in Cyber Security

Transform from a professional into a Leader with ECCU's Master's Degree in Cyber Security.
DEAC Accredited, 100% Online with Industry Leaders as Faculty. Admissions Open. Apply...

<https://www.eccouncil.org/uploads/2022/09/CEH-brochure.pdf>

CEH-brochure.pdf - EC-Council

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

24 pages

People also search for

- ec-council ceh practice test
- ceh v12 release date
- ec-council ceh v11 book
- ceh syllabus
- ceh v11 blueprint pdf
- ceh ec-council book pdf

People also ask

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

CEH-brochure.indd

1 / 24

88%

EC-Council

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

3:08 AM 10/6/2022

3:10 AM 10/6/2022

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**.

The screenshot shows a YouTube search results page for 'ec-council'. The main video thumbnail is for 'Mr. Sudershan Singh | CISSP, CCSP, CCEH Career Success Story | Canada'. A context menu is open over this video, with 'Copy Link' highlighted.

EC Council
30.3K subscribers • 463 videos
The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in ...
SUBSCRIBE

Latest from EC Council

- Mr. Sudershan Singh | CISSP, CCSP, CCEH Career Success Story | Canada**
8 views • 21 minutes ago
EC Council
In this video, Sudershan discusses how it has helped him in his career. He also shares his experience with the CISSP certification program, and
- Osaze Ehizojie, Kingdom recom**
27 views • 1 hour ago
EC Council
In this video, Osaze Ehizojie shares his experience with the CISSP certification program, and

https://www.youtube.com/shorts/mm8VYizXN_8

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.

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

Submit a link to a video, playlist, or channel

Accepted formats

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

Export & Share

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

Contains file(s)

11:51 PM 6/1/2022

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.

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

Submit a link to a video, playlist, or channel

Accepted formats

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

Export & Share

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

Contains file(s)

11:51 PM 6/1/2022

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.

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

✓ Snippet

```
{  
  "publishedAt": "2022-06-02T06:27:31Z",  
  "channelId": "UCHf4HMh2W5S1Shi1N442-cA",  
  "title": "Mr. Sudershan Singh | CEH Career Success Story | Canada",  
  "description": "In this video, Sudershan, shares his experience with the C|EH certification program, and discuss  
  "thumbnails": {  
    "default": {  
      "url": "https://i.ytimg.com/vi/mm8VYizXN_8/default.jpg",  
    }  
  }  
}
```

EC-Council **CEH**
"I strongly suggest C|EH Certification, Its One of the best industry certification"

MR. SUDERSHAN SINGH

CEH CAREER SUCCESS STORIES

Mr. Sudershan Singh | CEH Career Success Story | Canada

Published by EC Council

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

The video id is mm8VYizXN_8

01 Inspect the metadata for the rest of this channel's videos

Statistics

```
{
  "viewCount": "10",
  "likeCount": "1",
  "favoriteCount": "0",
  "commentCount": "0"
}
```

YouTube no longer provides the `dislikeCount` since 2021-12-13 (see more here).

Want dislikes back? Check out the [return-youtube-dislike](#) project!

Geolocation

```
{}
```

The video does not have recordingDetails.

Status

```
{
  "uploadStatus": "processed",
  "privacyStatus": "public",
  "license": "youtube",
  "embeddable": true,
```

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.

• Knowledge

thumbnails

Reverse image search all four thumbnail images.

Click to reverse image search

More

Check other resources for details or archival.

- Archive.org (details) - youtube-mm8VYizXN_8
- Archive.org (direct video 1) - mm8VYizXN_8
- Archive.org (direct video 2) - mm8VYizXN_8
- Archive.org (search) - Mr. Sudershan Singh | CEH Career Success Story | Canada
- Archive.org (web) - https://www.youtube.com/watch?v=mm8VYizXN_8
- Filmot.com - https://filmot.com/video/mm8VYizXN_8
- Google - "Mr. Sudershan Singh | CEH Career Success Story | Canada"
- Google - "mm8VYizXN_8"

https://www.google.com/searchbyimage?image_url=https://img.youtube.com/vi/mm8VYizXN_8/0.jpg

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

About 2 results (1.46 seconds)

Image size:
480 x 360
No other sizes of this image found.

Possible related search: [language](#)

<https://en.wikipedia.org/wiki/Language>

Language - Wikipedia

A **language** is a structured system of communication. The structure of a **language** is its grammar and the free components are its vocabulary.

<https://www.britannica.com/>

language | Definition, Types, Characteristics, Development ...

language, a system of conventional spoken, manual (signed), or written symbols by means of which human beings, as members of a social group and participants ...



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.

NAPALM
FTP indexer

With all the words ▾

Searching 381,136,327 files (4775.43 TB) in 2,325 FTP servers

Updated: 3/15/2022

NAPALM FTP Indexer lets you search and download files located on public FTP servers.
The most advanced FTP Search Engine service maintained by members.

[Donate Bitcoin](#) 13CaChceoDTfgtcyfmhUB28XdCA7djZHcn <<>

About | Faq | Contact Us | Terms of Use | Privacy Policy
Copyright © 2002-2022 NAPALM Indexer

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

microsoft

With all the words ▾

Searching 381,136,327 files (4775.43 TB) in 2,325 FTP servers

Updated: 3/15/2022

NAPALM FTP Indexer lets you search and download files located on public FTP servers.
The most advanced FTP Search Engine service maintained by members.

[Donate Bitcoin](#) 13CaChceoDTfgtcyfmhUB28XdCA7djZHcn <<>

About | Faq | Contact Us | Terms of Use | Privacy Policy
Copyright © 2002-2022 NAPALM Indexer

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

The screenshot shows a browser window with the title "NAPALM FTP Indexer". The address bar contains "https://www.searchftps.net". The search query "microsoft" is entered in the search bar. Below the search bar, there is a "Related keywords" section with a grid of links. The main content area displays search results for "microsoft", listing several RPM packages with their file sizes and download buttons.

File Path	File Size	Action
/linux/fedora-secondary/updates/32/Everything/ppc64le/Packages/p/ php-microsoft-tolerant-php-parser-0.0.23-1.fc32.noarch.rpm	85.6 KB	DOWNLOAD
/.../linux-fedora-buffet/fedora-secondary/development/35/Everything/s/ 390x/os/Packages/p/ php-microsoft-tolerant-php-parser-0.1.1-1.fc35.noarch.rpm	85.0 KB	DOWNLOAD
/pub/RedHat/fedora/linux/releases/35/Everything/x86_64/os/Packages/ p/ php-microsoft-tolerant-php-parser-0.1.1-1.fc35.noarch.rpm	85.0 KB	DOWNLOAD
/pub/RedHat/fedora/linux/releases/35/Everything/x86_64/os/Packages/a/ l/ ansible-collection-microsoft-sql-1.1.0-2.fc35.noarch.rpm	43.9 KB	DOWNLOAD

At the bottom right of the browser window, the system tray shows the date as Tuesday, March 15, 2022, and the time as 1:52 AM, 3/15/2022.

5. This concludes the demonstration of gathering information from the FTP search engine.

6. You can also use FTP search engines such as **FreewareWeb FTP File Search** (<https://www.freewareweb.com>) to gather crucial FTP information about the target organization.

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

Task 4: Gather Information from IoT Search Engines

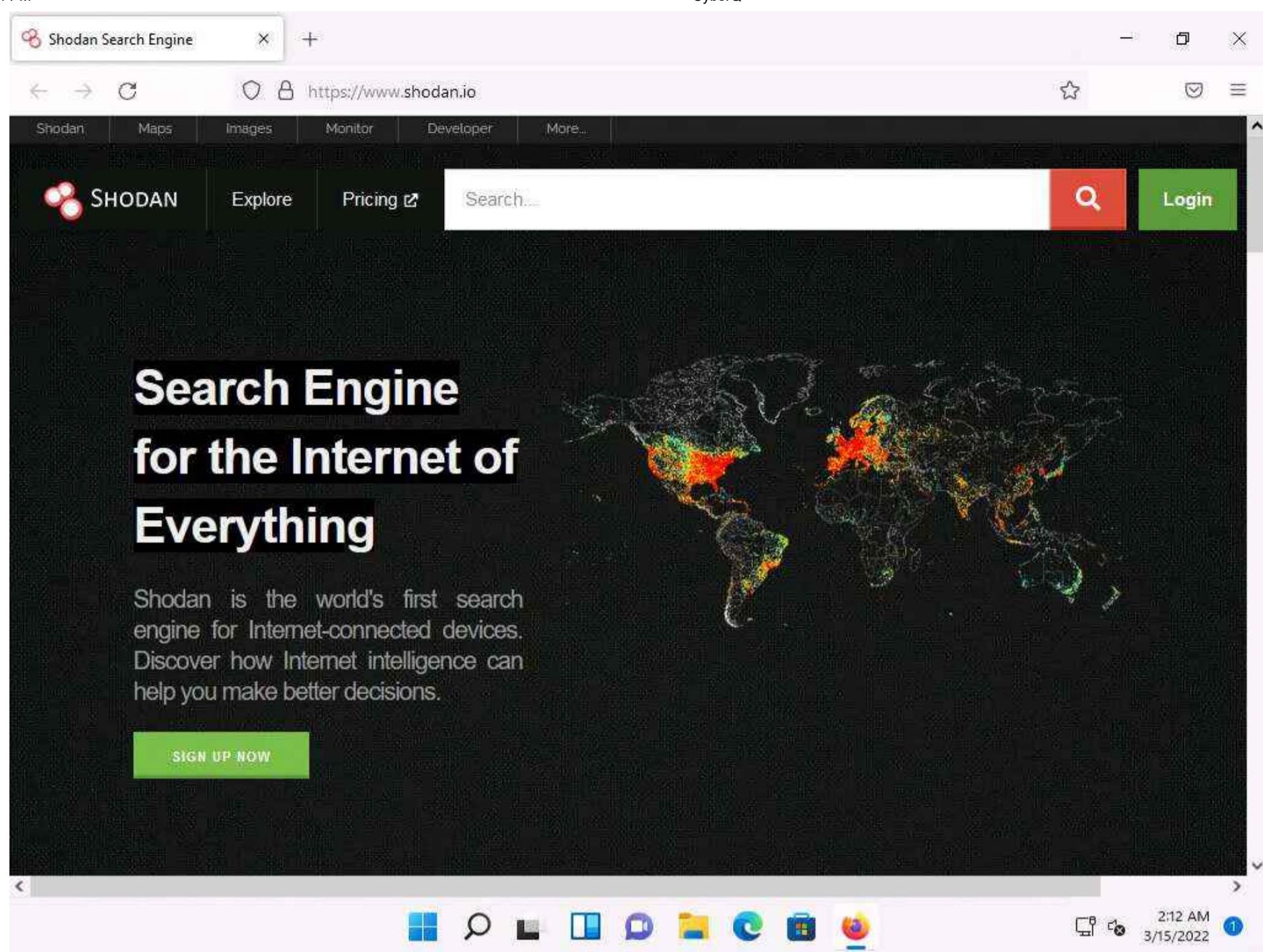
IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances,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

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

1. 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.

TOTAL RESULTS
1,613,565

TOP COUNTRIES

Country	Count
United States	446,136
Japan	175,004
Ireland	89,416
Germany	76,378
Singapore	76,325
More...	

TOP PORTS

Port	Count
80	163,703
443	103,589
21	35,389
8200	7,054
50000	6,710
More...	

SSL Certificate for 23.21.47.223

Issued By: I-Common Name: ip-10-236-69-171
Issued To: I-Common Name: ip-10-236-69-171
Organization: SomeOrganization

HTTP/1.1 200 OK
Date: Tue, 15 Mar 2022 09:09:52 GMT
Server: Apache/2.2.34 (Amazon)
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

301 Moved Permanently

Issued By: Entrust Certification Authority - L1K
Issued To: I-Common Name:

HTTP/1.1 301 Moved Permanently
Date: Tue, 15 Mar 2022 09:07:14 GMT
Server: Apache/2.4.52 (Amazon)
Location: http://www.fourpointsshonyc.com/
Content-Length: 241
Content-Type: text/html; charset=iso-8859-1

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.

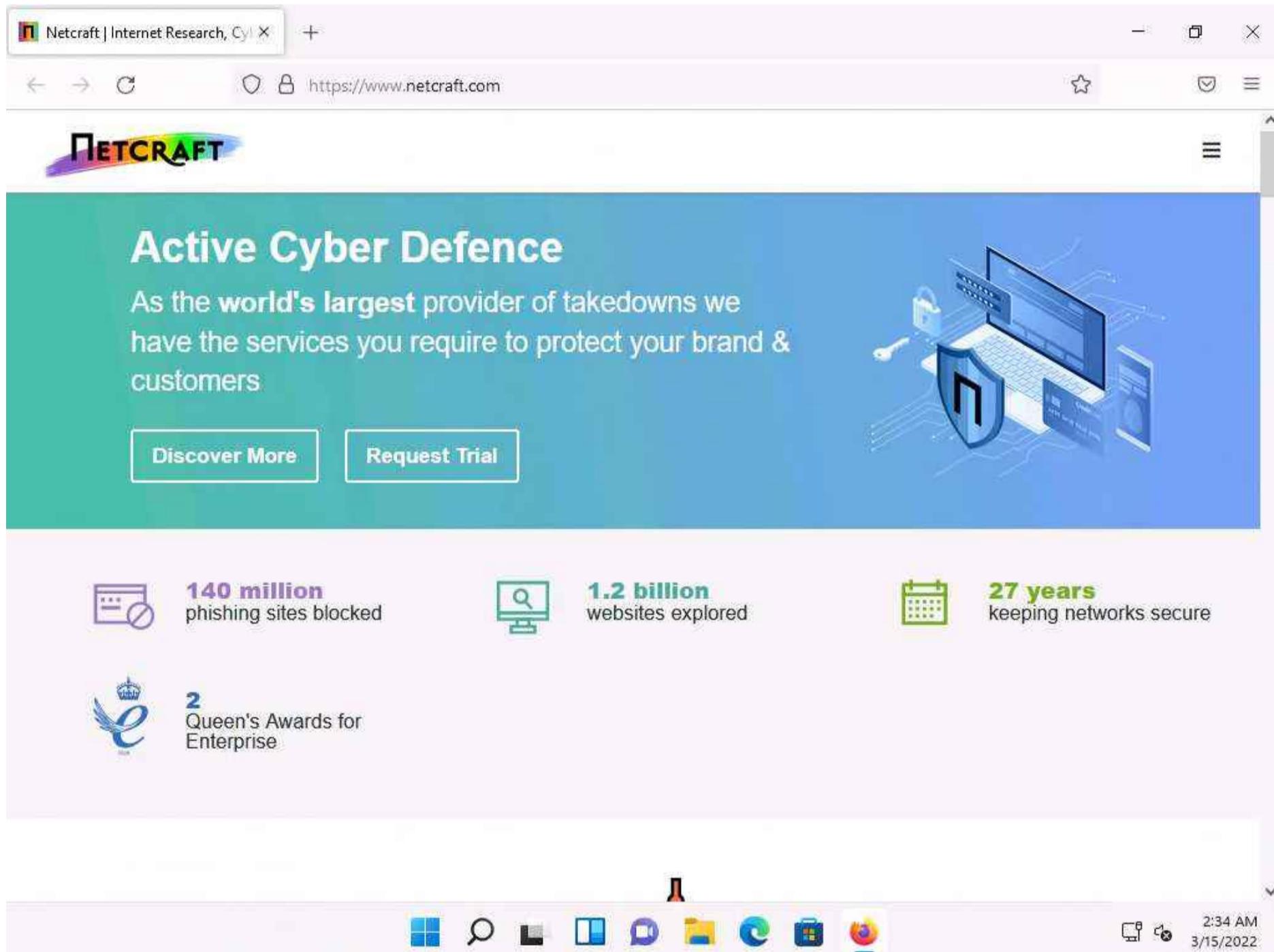
Here, we will extract the company's domains and sub-domains using the Netcraft web service.

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.

Commercial Services

Cybercrime Disruption
Security Testing

Resources

Protection Apps & Extensions
Site Report

Company

About Us
Contact Us

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.

The screenshot shows a browser window displaying the Netcraft Site Report for <https://www.eccouncil.org>. The page has a green header bar with the title "Site report for https://www.eccouncil.org". Below the header, there's a search bar with the placeholder "Look up another site?". The main content area is divided into sections:

- Background:** Includes fields for Site title (Certified Ethical Hacker | InfoSec Cyber Security Certification | EC-Council), Date first seen (March 2003), Site rank (1719), Netcraft Risk Rating (0/10), Description (EC-Council is a global leader in InfoSec Cyber Security certification programs like Certified Ethical Hacker and Computer Hacking Forensic Investigator.), and Primary language (English).
- Network:** Lists details about the website's infrastructure:
 - Site: <https://www.eccouncil.org> (Domain: eccouncil.org)
 - Netblock Owner: Cloudflare, Inc. (Nameserver: henry.ns.cloudflare.com)
 - Hosting company: Cloudflare (Domain registrar: pir.org)
 - Hosting country: US (Nameserver organisation: whois.cloudflare.com)
- Transferring data from static.netcraft.com...**: Shows the IP address 104.18.21.251 and a VirusTotal link.
- Icons:** A row of small icons representing various services or tools.
- Bottom right:** Shows the date and time (2:42 AM, 3/15/2022) and a circular arrow icon.

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

Site report for https://www.ecc... X +

https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.eccouncil.org 90% ⭐ 🌐 🔍

NETCRAFT Services Solutions News Company Resources Report Fraud Request Trial

Background

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

Network

Site	https://www.eccouncil.org ↗	Domain	eccouncil.org
Netblock Owner	Cloudflare, Inc.	Nameserver	henry.ns.cloudflare.com
Hosting company	Cloudflare	Domain registrar	pir.org
Hosting country	US	Nameserver organisation	whois.cloudflare.com
IPv4 address	104.18.21.251 (VirusTotal ↗)	Organisation	US
IPv4 autonomous systems	AS13335 ↗	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:0:0:0:6812:15fb	Top Level Domain	Organization entities (.org)
IPv6 autonomous systems	AS13335 ↗	DNS Security Extensions	Enabled
Reverse DNS	unknown		

2:43 AM 3/15/2022

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

Hostnames matching *.eccouncil.org X +

https://searchdns.netcraft.com/?host=*.eccouncil.org 90% ⭐ 🌐 🔍

NETCRAFT Services Solutions News Company Resources Report Fraud Request Trial

Hostnames matching *.eccouncil.org

▶ 🔎 Search with another pattern?

17 results

Rank	Site	First seen	Netblock	OS	Site Report
838	aspen.eccouncil.org ↗	June 2010	Cloudflare, Inc.	Linux	🔗
1179	iklass.eccouncil.org ↗	October 2009	Cloudflare, Inc.	unknown	🔗
1356	codered.eccouncil.org ↗	January 2020	Cloudflare, Inc.	Linux	🔗
1487	cyberq.eccouncil.org ↗	October 2018	Cloudflare, Inc.	Linux	🔗
1724	www.eccouncil.org ↗	February 2002	Cloudflare, Inc.	Linux	🔗
8978	cert.eccouncil.org ↗	March 2012	Cloudflare, Inc.	Linux	🔗
11579	store.eccouncil.org ↗	July 2013	Cloudflare, Inc.	Linux	🔗 Tuesday, March 15, 2022

2:43 AM 3/15/2022

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.

The screenshot shows a web browser window for the website [peekyou.com](https://www.peekyou.com). The page title is "PeekYou - People Search Made Easy". Below the title, a sub-header reads "Find friends, relatives and colleagues across the Web." A black and white photograph of a diverse group of people looking at a screen together serves as the background for the search form. The search form itself has three input fields: "Name" containing "Satya", "Username" containing "Nadella", and "Location" containing "Washington, DC". A blue button with a magnifying glass icon is positioned to the right of the location field. The browser's address bar shows the URL <https://www.peekyou.com>.

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

The screenshot shows a web browser window for the website https://www.peekyou.com/usa/district_of_columbia/satya_nadella. The search bar at the top has 'Name' selected, with 'Satya' in the first field and 'Nadella' in the second. A green 'START' button is prominent on the left. To its right is a 'Search Tools' section with an 'Easy Search Tool' button. Below these are links for Public Records, Facebook, Instagram, Twitter, Email, and Images. The main content area is titled 'Public Records & Background Search' and lists three results for 'Satya Nadella' (age 53), each with a 'View Full Report' link. Below this is an 'Arrest Records & Driving Infractions' section with a 'VIEW ARRESTS' button. At the bottom is a 'Phonebook' section with various icons. The status bar at the bottom right shows the date and time: 3/15/2022, 3:42 AM.

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.

We Found Satya Nadella

Phonebook

- 1) Satya Nadella's Phone & Current Address [Search Details](#)
- 2) Social Media Profiles & More [Search Details](#)
- Satya Nadella's Phone #, Address & More [Search Details](#)
- Satya Nadella's Contact Info, Social Profiles & More [Search Details](#)

Email Addresses

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

Contact Information & Address History

Satya Nadella [SEARCH DETAILS](#)

Facebook

Satya Nadella - satya.nadella.942

3:43 AM 3/15/2022

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

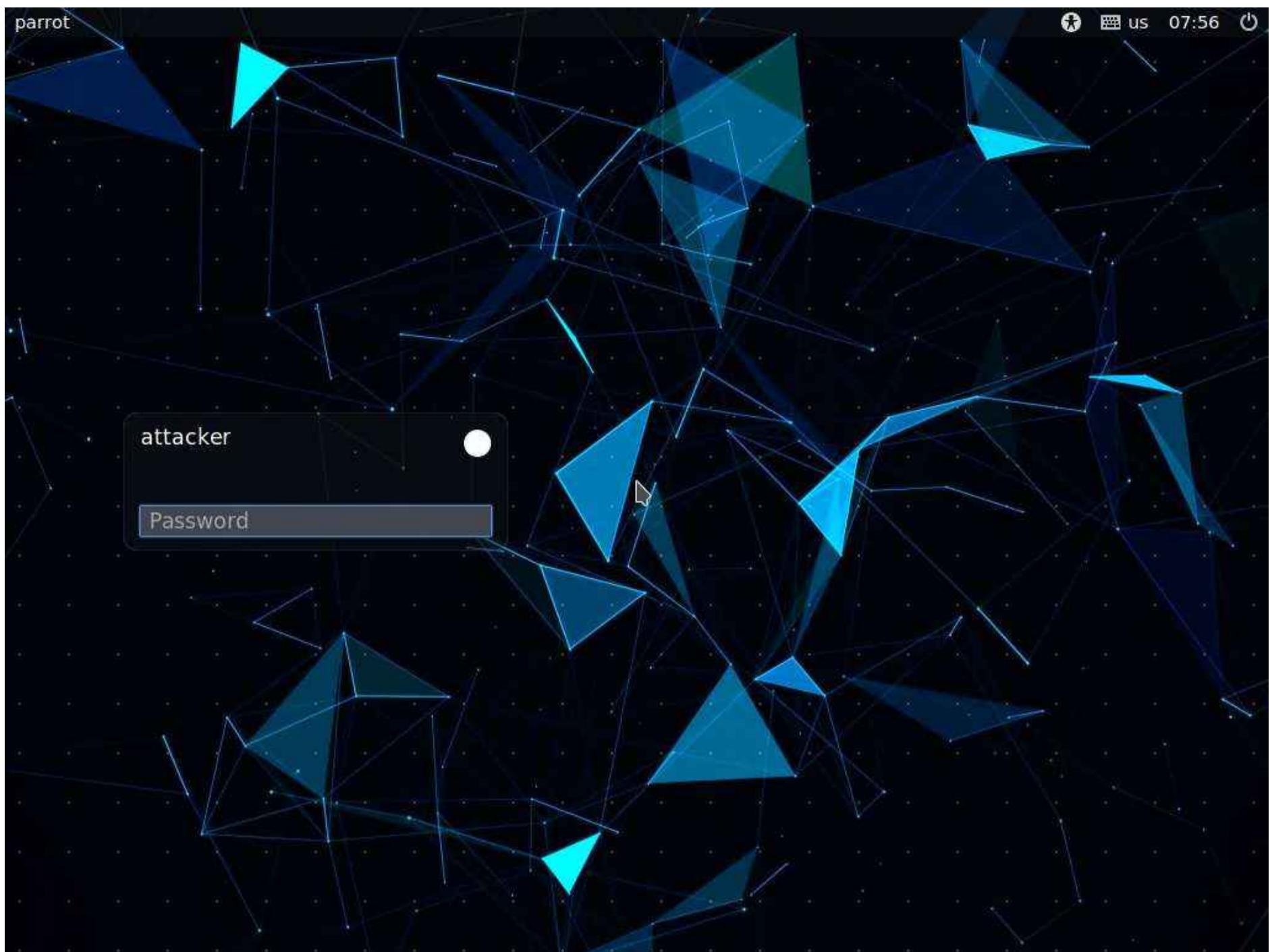
Emails are messaging sources that are crucial for performing information exchange. Email ID is considered by most people as the personal identification of employees or organizations. Thus, gathering the email IDs of critical personnel is one of the key tasks of ethical hackers.

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**.

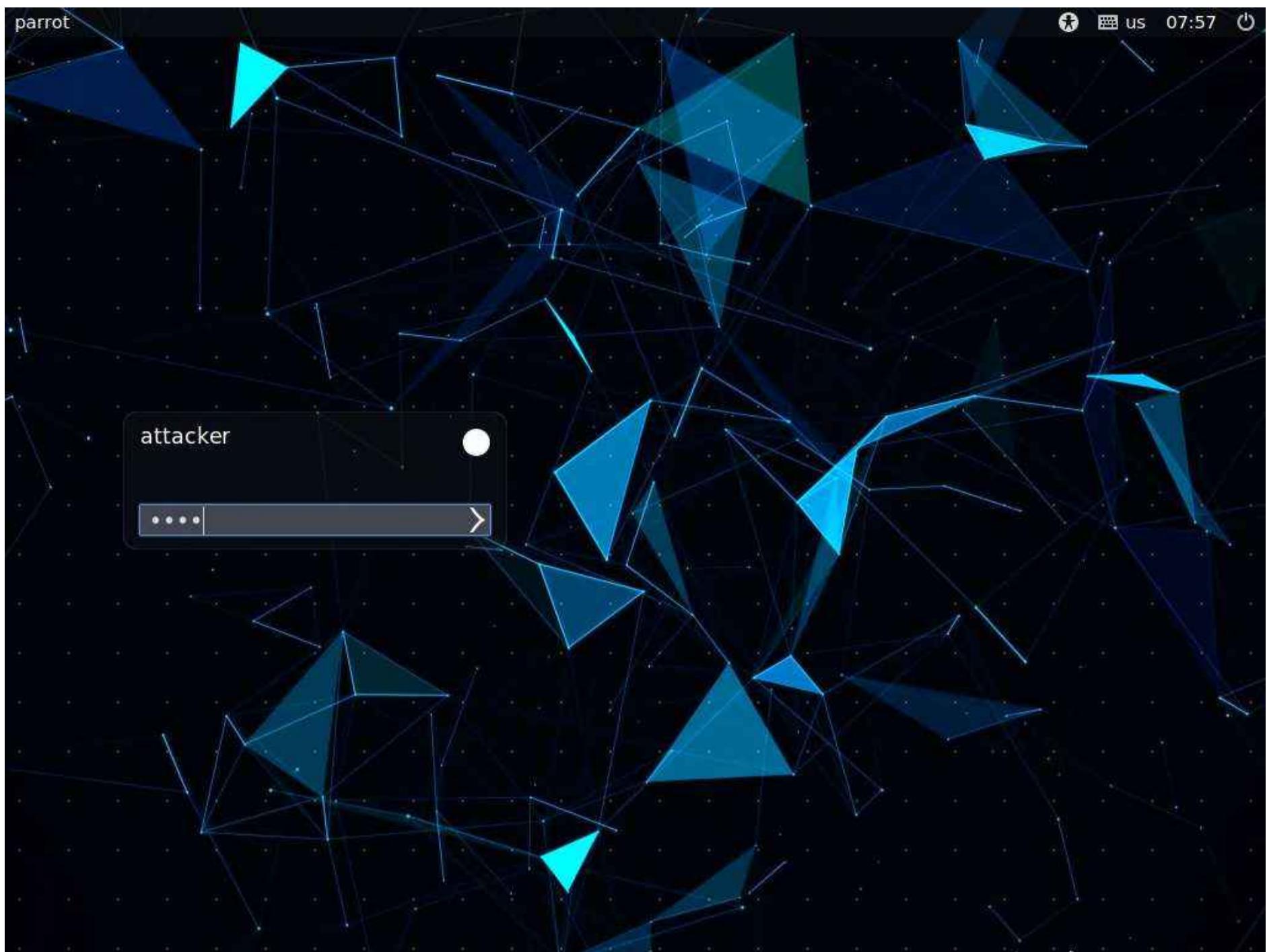


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

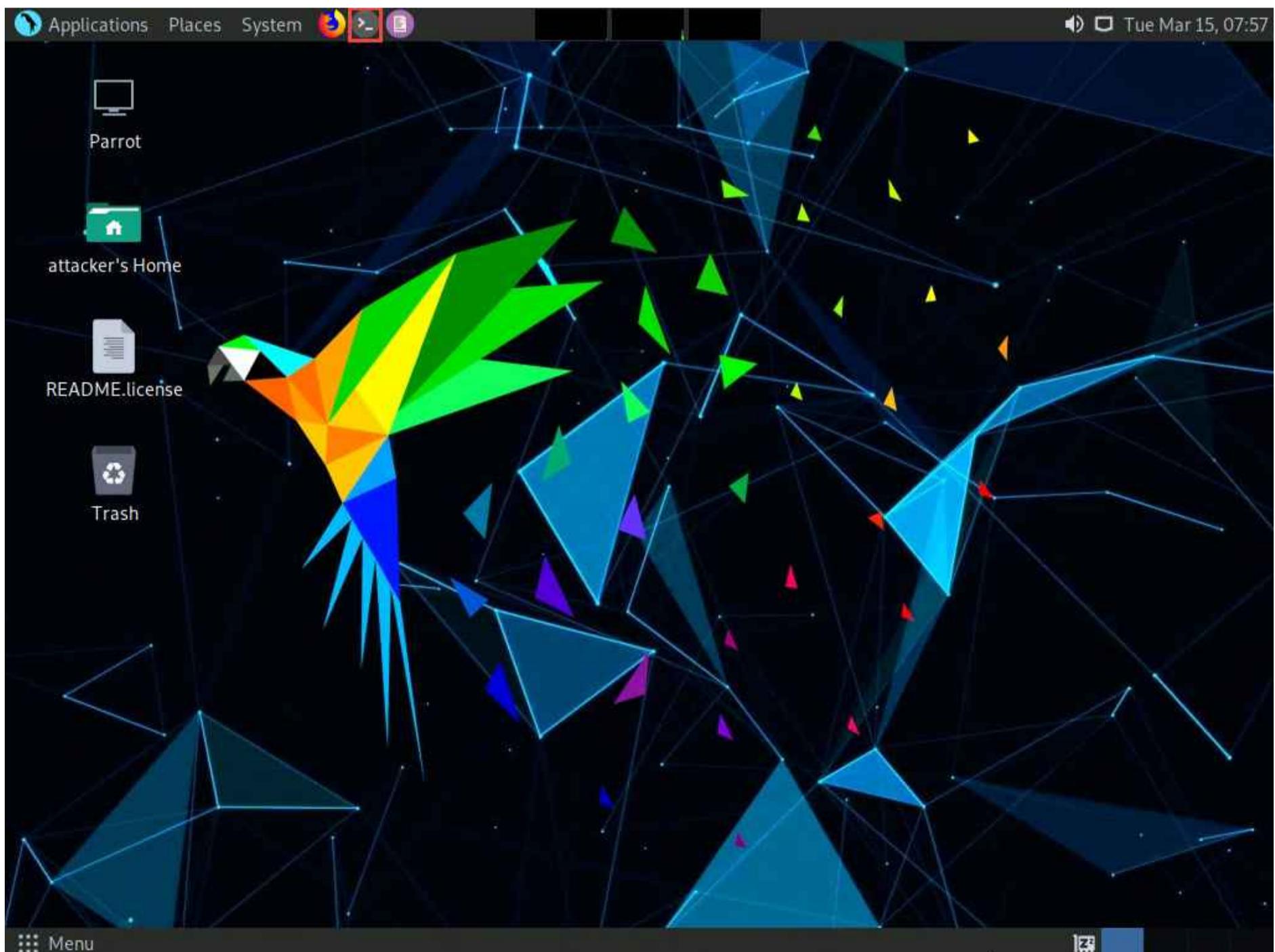
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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.

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

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.



```
[*] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] No emails found.
```

8. theHarvester starts extracting the details and displays them on the screen.

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

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

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

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

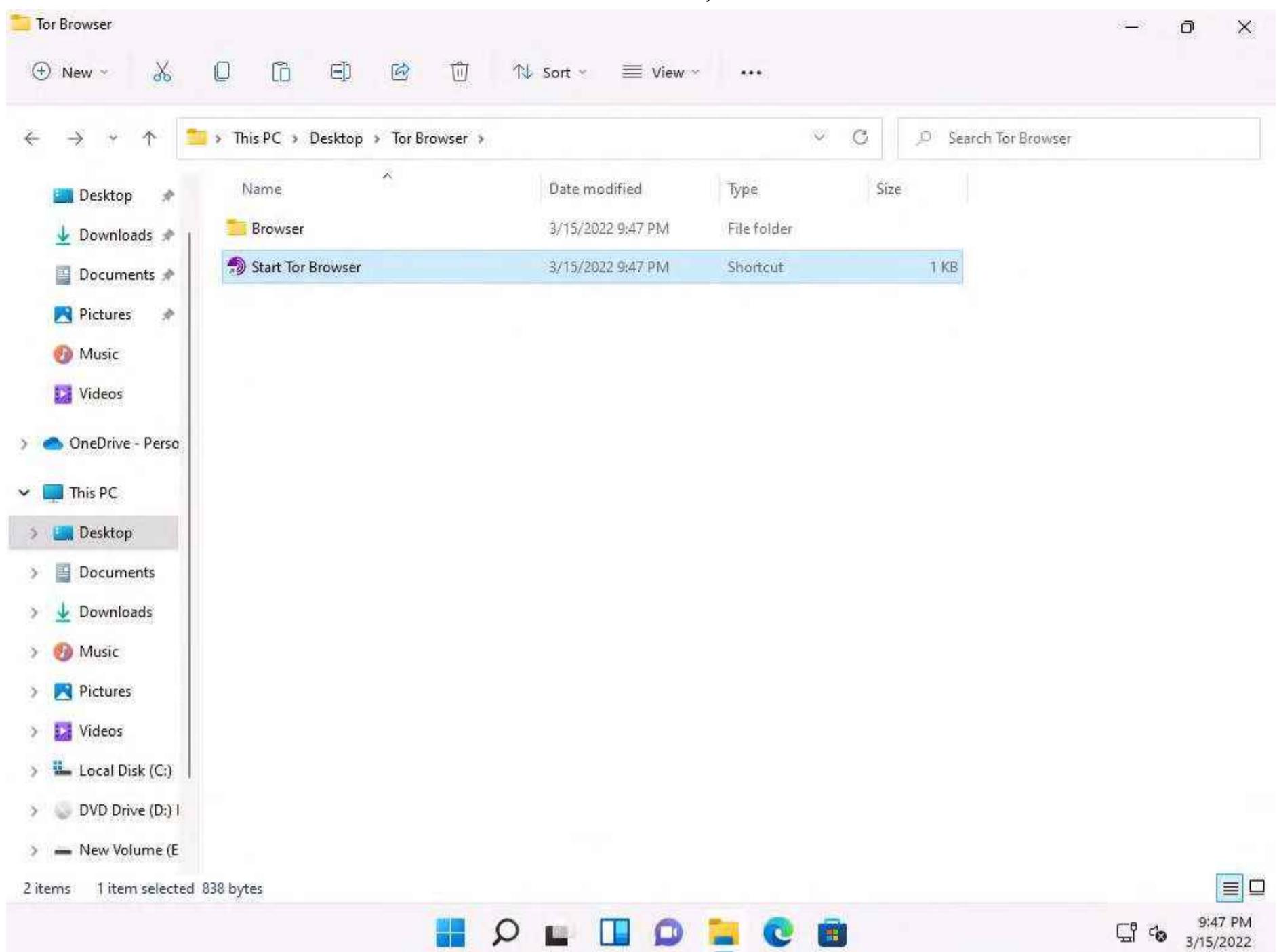
11. Close all open windows and document all the acquired information

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.

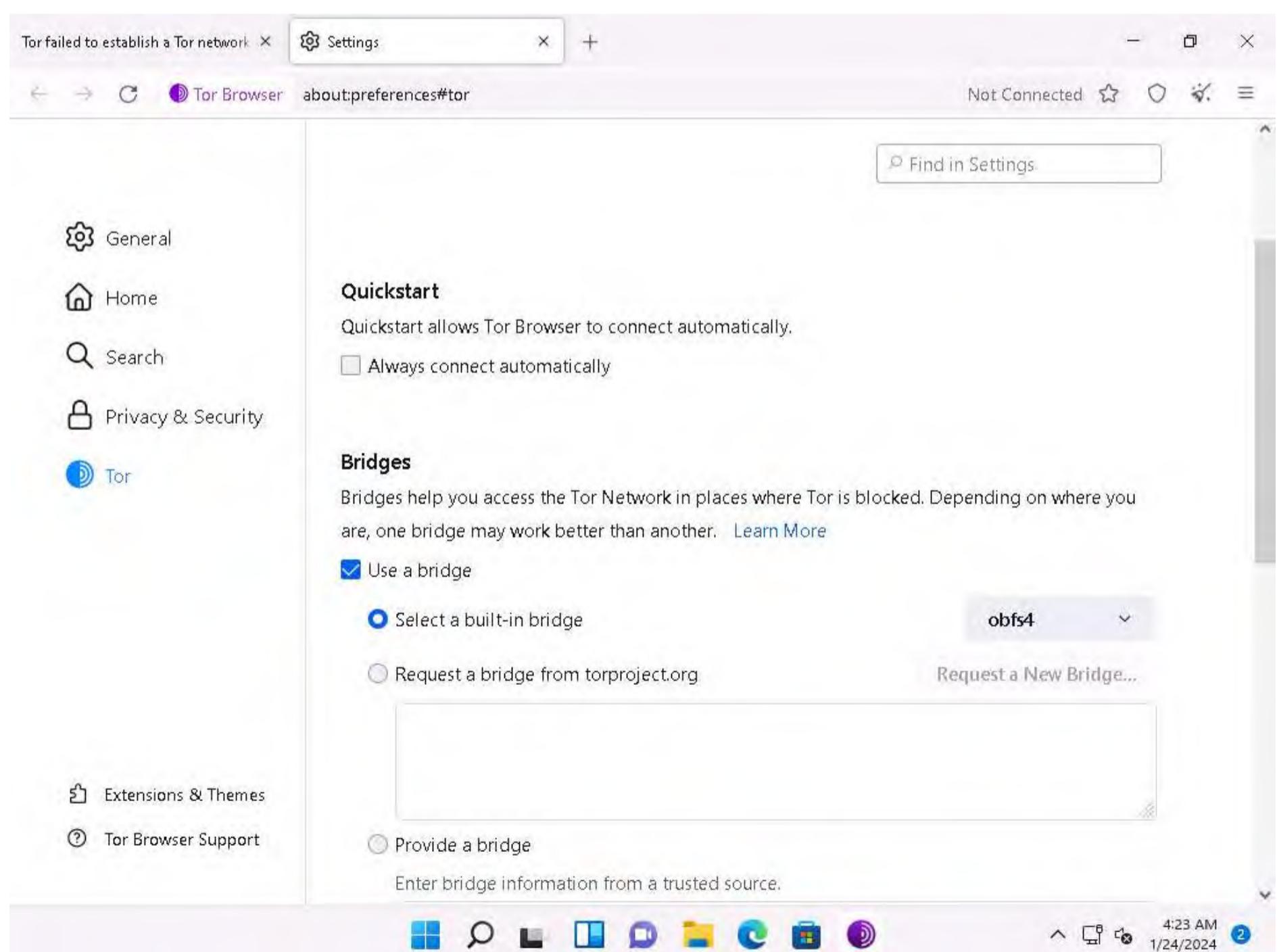
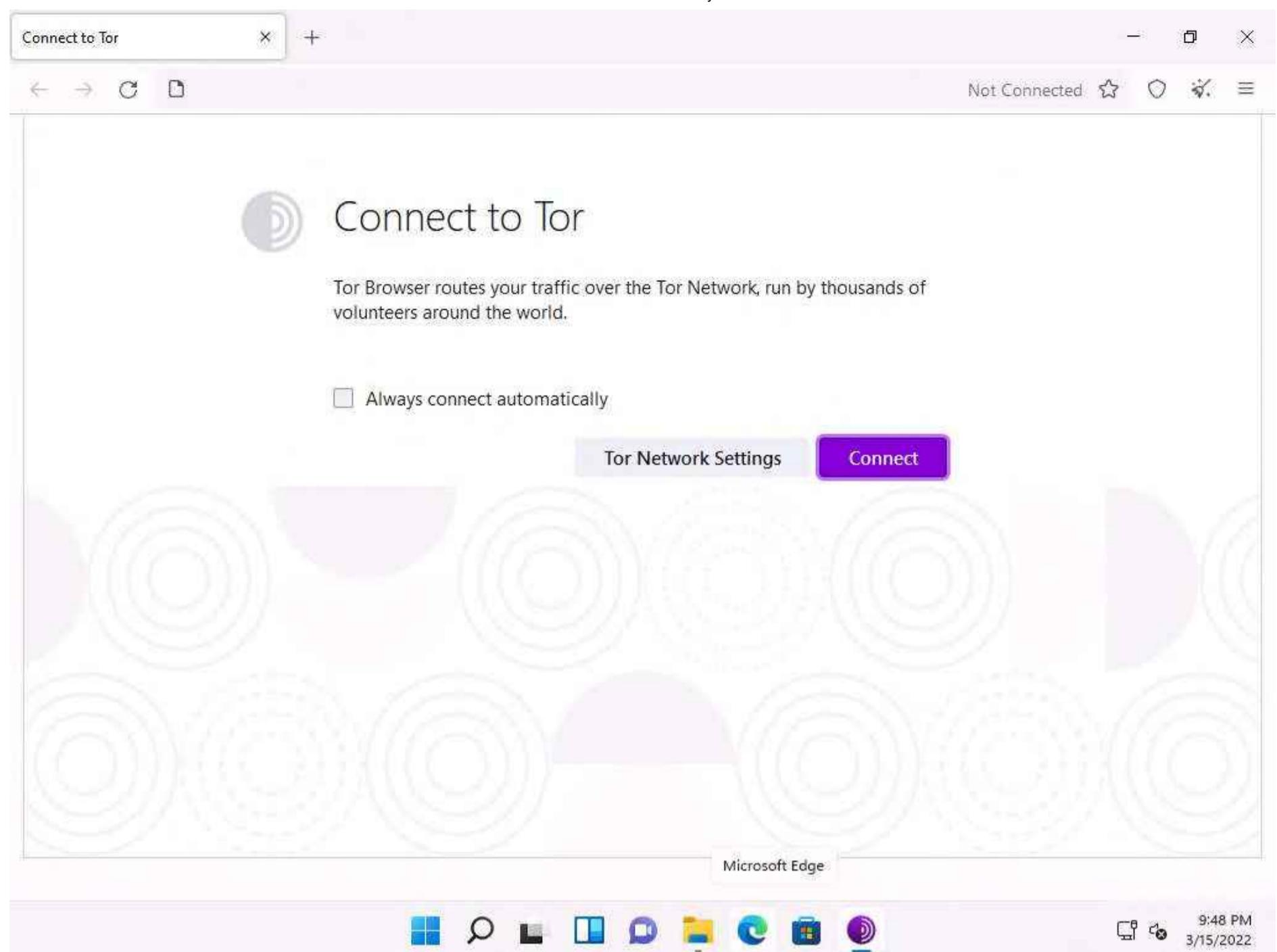
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
 2. Open a **File Explorer**, navigate to **C:\Users\Admin\Desktop\Tor Browser**, and double-click **Start Tor Browser**.

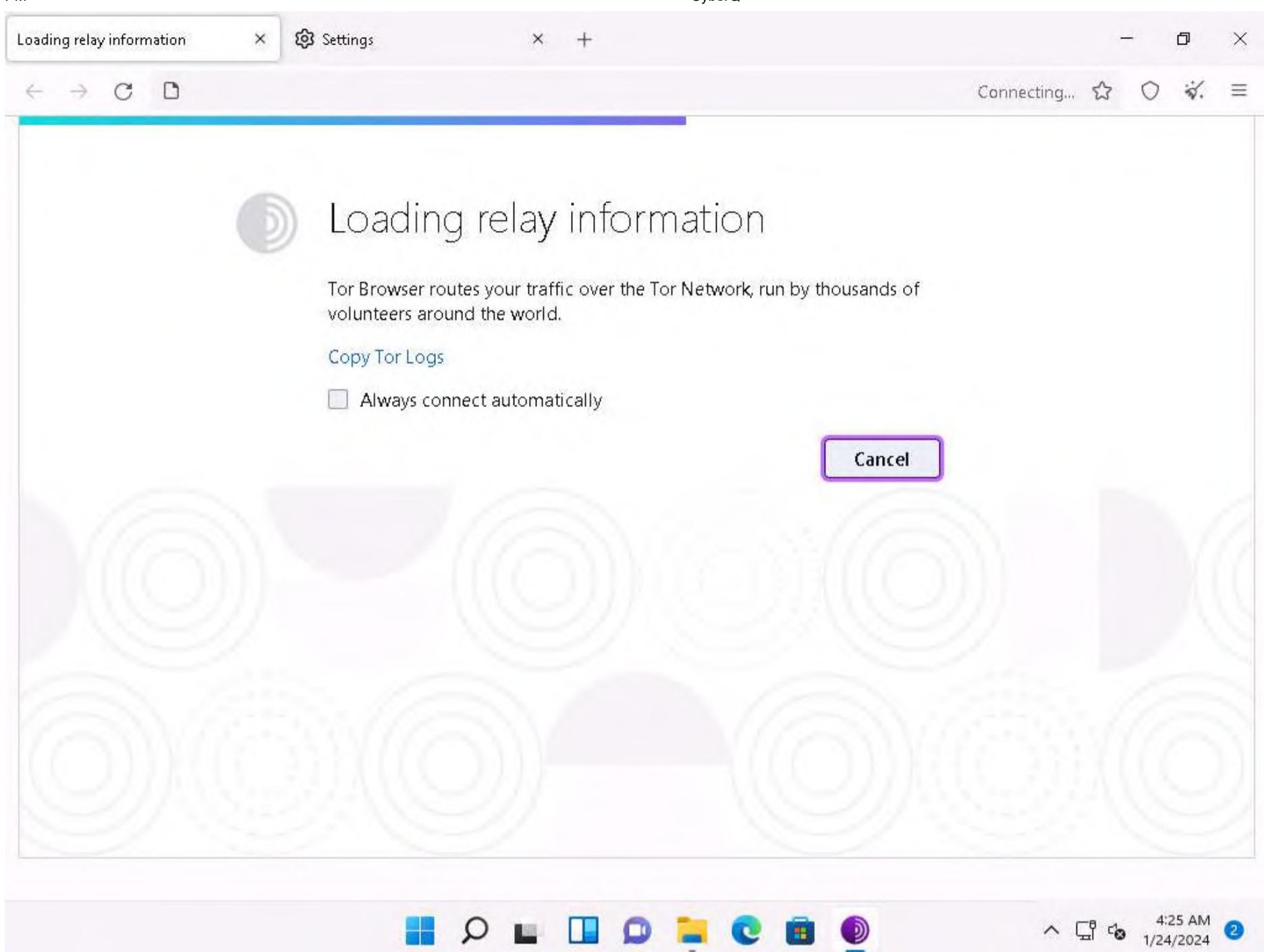


3. The **Connect to Tor** page appears. Click the **Connect** button to directly browse through Tor Browser's default settings.

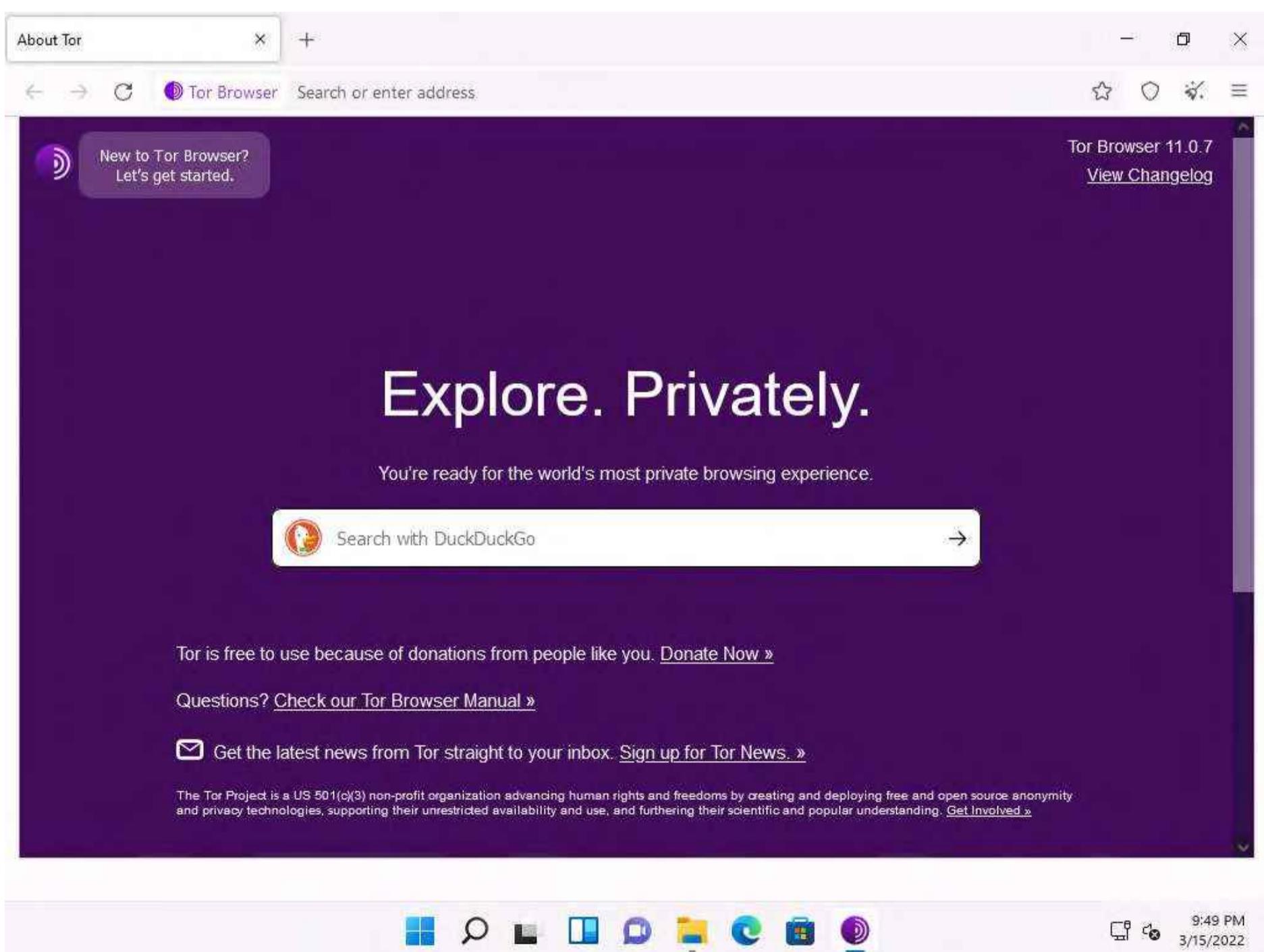
Note: If Tor is censored in your country or if you want to connect through Proxy, click the Tor Network Settings button and select any default built-in bridge as shown in the screenshot below and continue.







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.

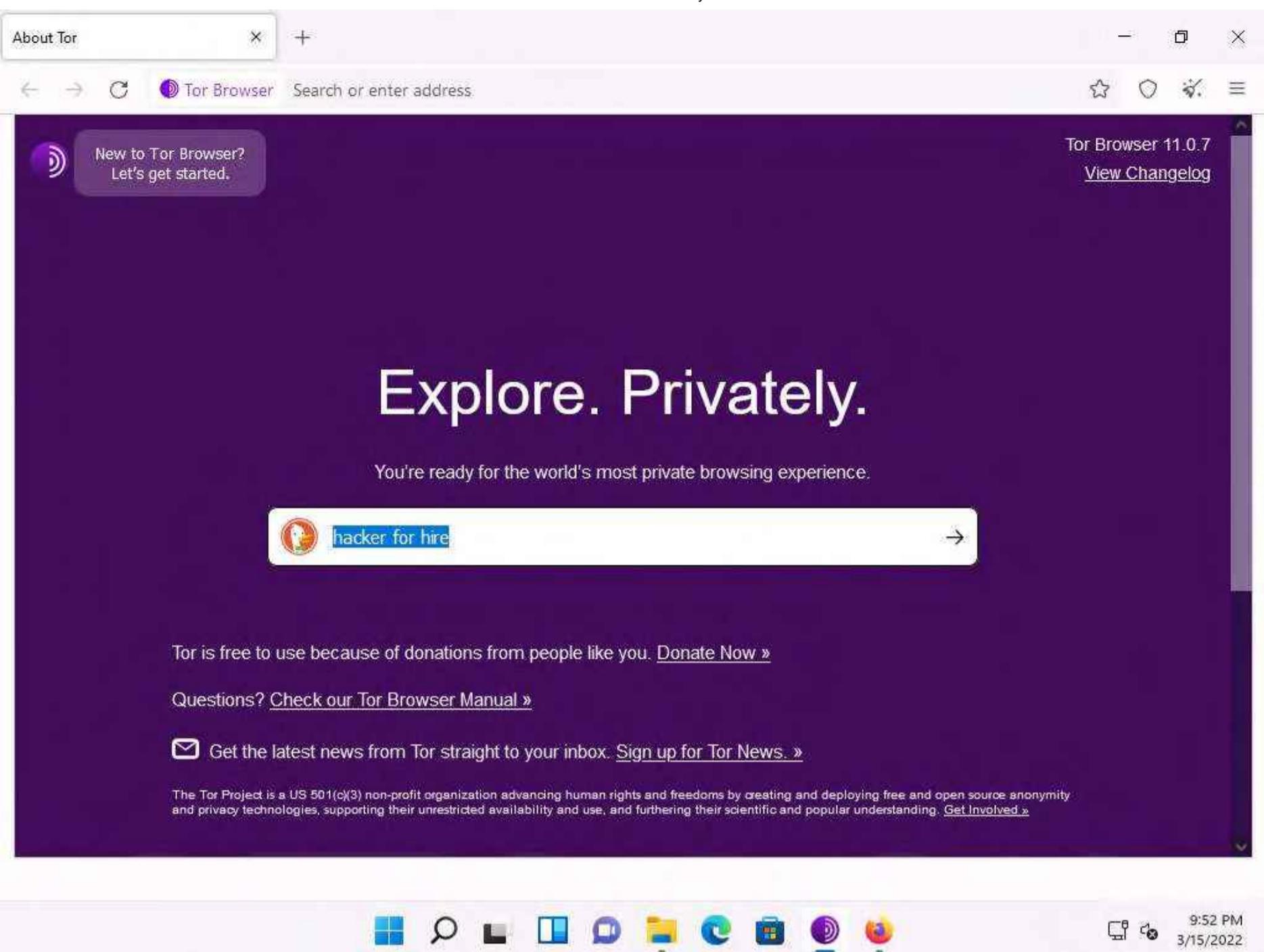
The screenshot shows a Mozilla Firefox window with the title bar "hacker for hire - Google Search". The address bar displays the URL "https://www.google.com/search?q=hacker+for+hire&source=hp&ei=jmwxySjQawqoigCA". The search bar also contains "hacker for hire". Below the search bar are navigation buttons (Back, Forward, Stop, Refresh) and a search icon. The main content area shows a Google search results page for "hacker for hire". The results include:

- 27 Best Freelance Hackers For Hire In March 2022 - Upwork™**
3 days ago — **Hire the best Hackers** : Razvan N. - (84 jobs) · Kali Linux; Security Testing; Security Analysis ; Esteban V. - (73 jobs) - Python; Firewall; Amazon ...
★★★★★ Rating: 4.7 - 1,807 reviews
- Hire the best Certified Ethical Hackers - Upwork**
Upwork is the leading online workplace, home to thousands of top-rated Certified Ethical Hackers. It's simple to post your job and get personalized bids, ...
★★★★★ Rating: 4.7 - 1,807 reviews
- Home - Hire A Hacker #1 Hackers for hire**
We have hired the best **hackers** in the industry from around the world to make sure all our customer's **hacking** needs are met so all our clients are satisfied. 15 ...
Phone Hackers for Hire · Whatsapp Hacker for Hire · Instagram Hacker for Hire

The taskbar at the bottom of the screen shows various pinned icons, and the system tray indicates the date and time as 9:50 PM on 3/15/2022.

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.

The screenshot shows a web browser window with the DuckDuckGo search engine. The search bar contains the query "hacker for hire". Below the search bar, there are filters for "All", "Images", "Videos", "News", and "Maps". The main search results area displays three entries:

- Hire a Professional Hacker - Certified Ethical Hackers ...**
https://evolutionhackers.com
Hire Hackers/Shop hacking tools today! Being an organization that's fully committed to solving everyday problems in the hacking community, we offer all kinds of hacking services. Furthermore, once you've successfully signed up with one of our hackers for any project, we'll give direct and unlimited access to our online store to shop for...
- 27 Best Freelance Hackers For Hire In March 2022 - Upwork™**
https://www.upwork.com/hire/hackers
Hire the best Hackers. Get to know top Hackers. And say hello to the newest member of your team. Get Started. Clients rate Hackers. Rating is 4.7 out of 5. 4.7/5. based on 1,807 client reviews. \$50/hr.
- Hacker For Hire. Hire the #1 Hire a Hacker Cyber Service ...**
https://www.hackerforhire.net
We are a US Based Service 3001 W Indian School Rd. Phoenix, AZ 85017 480-400-4600

To the right of the search results, there is a "Related Searches" sidebar with the following suggestions:

- hire a hacker for free
- illegal hackers for hire
- I need a hackers help
- best hackers for hire
- hackers for hire cheap
- hire a hacker for gmail
- find a hacker

The browser interface includes standard navigation buttons (back, forward, search) and a toolbar at the bottom. The status bar at the bottom right shows the time as 9:56 PM and the date as 3/15/2022.

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.

The screenshot shows the homepage of the [Hacker For Hire](https://www.hackerforhire.net) website. The page features a dark background with a stylized illustration of a person's face and hands interacting with a keyboard. The title "Hacker For Hire" is prominently displayed in white text. Below it is a red button labeled "HIRE A HACKER HOME". A large green banner at the bottom asks "Need a Hacker?". A quote in green text reads: "By now you've been to dozens of websites, all promising the world for cheap. Not us. We do not promise the world, nor are we cheap." At the bottom, another quote in green text says: "Everyone needs a good hacker, even other hackers. Even the best hackers in the world need to call on someone for a little help."

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://zqktlwiauvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.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.



Host Filters

Autonomous System:

- 3 AMAZON-02
- 3 OVH
- 2 AMAZON-AES
- 2 DIGITALOCEAN-ASN
- 2 GOOGLE-CLOUD-PLATFORM
- More

Location:

- 13 United States
- 2 France
- 1 Canada
- 1 Germany
- 1 Latvia
- More

Service Filters

Service Names:

Hosts
Results: 22 Time: 8.70s

51.195.40.93
 OVH (16276) France
 22/SSH 80/HTTP 123/NTP 443/HTTP
 services.http.response.body: href="http://www.eccouncil.org/Certification"

3.16.217.79
 AMAZON-02 (16509) Ohio, United States
 22/SSH 80/HTTP
 services.http.response.body: //www.eccouncil.org/programs/certified-ethical-hacker-ce...
 services.http.response.body: //www.eccouncil.org/programs/certified-ethical

2A00:ECE1:0000:001F:0000:0000:0181
 CTSTELECOM (19653) Romania
 80/HTTP 443/HTTP
 services.http.response.body: href="https://www.eccouncil.org/programs"

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

3.16.217.79

As of Mar 16, 2022 12:40am UTC | Latest

Summary **Explore** **History** **WHOIS** **Raw Data**

Basic Information

- OS** Ubuntu Linux 18.04
- Network** AMAZON-02 (US)
- Routing** 3.16.0.0/14 via AS16509
- Protocols** 22/SSH , 80/HTTP

22/SSH **TCP** Observed Mar 16, 2022 at 12:40am UTC **VIEW ALL DATA**

Software

- linux
- Ubuntu Linux 18.04
- OpenBSD OpenSSH 7.6

Geographic Location

City Columbus

39°57'45.0"N 80°00'00.0"W

View larger map

Keyboard shortcuts Map Data Terms of Use

11:33 PM 3/15/2022

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.

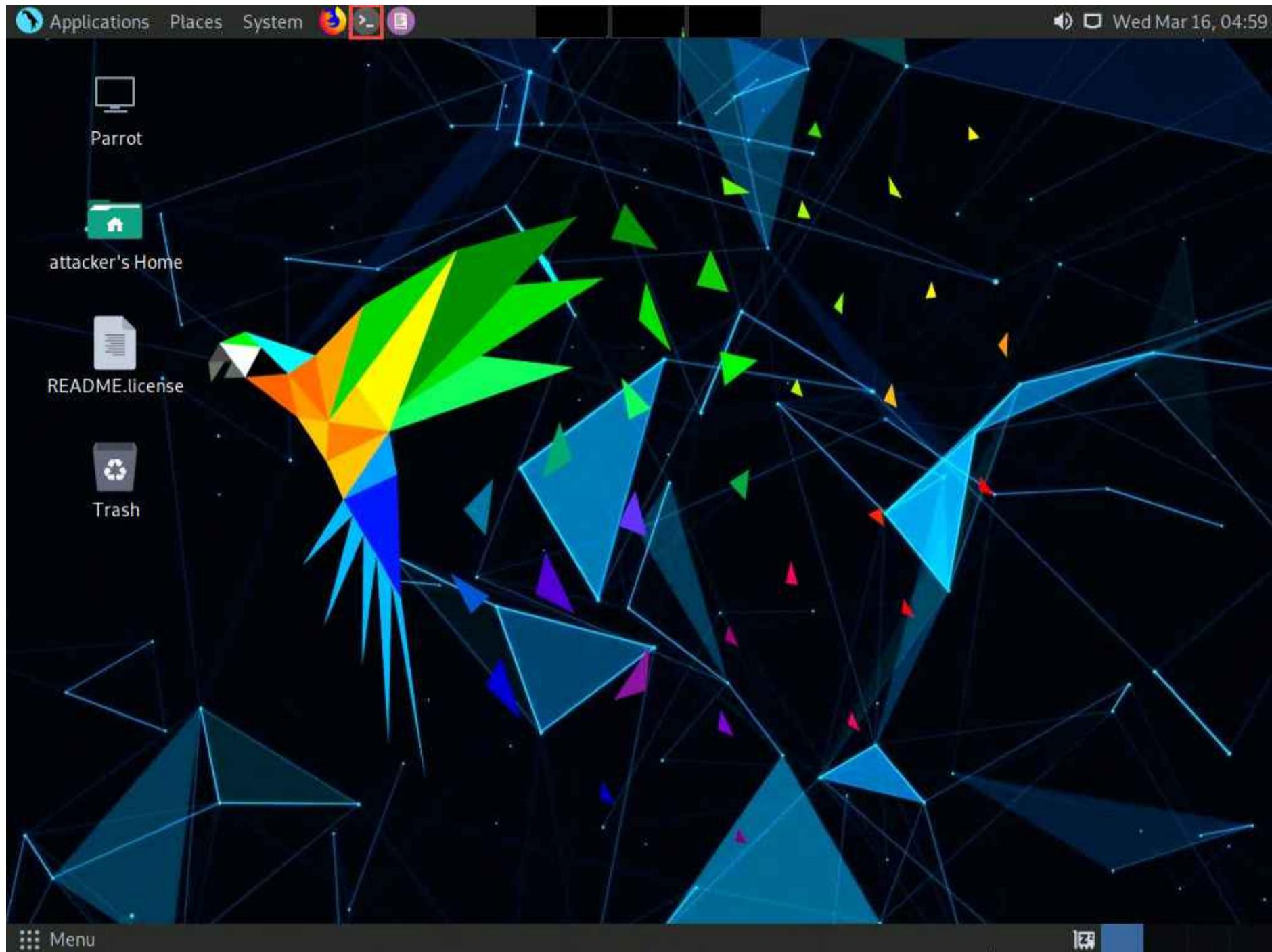
Task 1: Gather Employees' Information from LinkedIn using theHarvester

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.



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

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.

```
Applications Places System theHarvester -deccouncil -l200 -b linkedin - Parrot Terminal
File Edit View Search Terminal Help
[*] Target: eccouncil

        Searching 100 results.
        Searching 200 results.
[*] Searching Linkedin.

[*] LinkedIn Users found: 197
-----
    - Software Engineer
        - Software Engineer
    - Vice President

    Cyber Security Training Coordinator
    - Vice President Finance

    - Manager Masterclass
    - Manager - Partner Outreach
        - Operations Manager
    Software Engineer
        - EC-Council
    Manager Business Development
        - Account Executive
        Assistant Manger- International Sales
        - Security Consultant
        Researcher
        ito - it security hobbyist
        - Senior Operations Executive
        - Research Specialist
        - SVP and Head of Americas
```

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

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

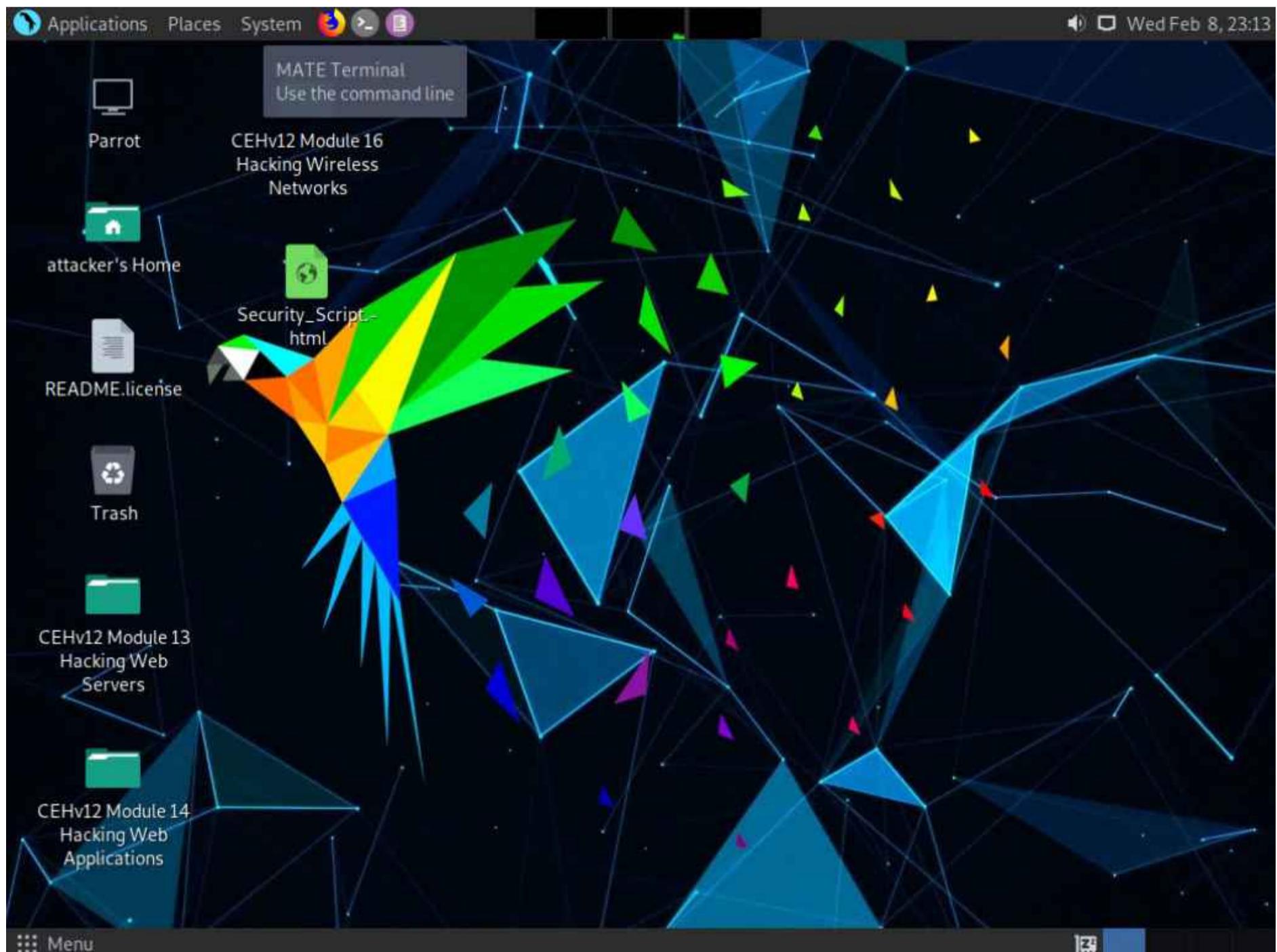
Task 2: Gather Personal Information from Various Social Networking Sites using Sherlock

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

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

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

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.

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

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

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

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.

The screenshot shows a terminal window titled "python3 sherlock satya nadella - Parrot Terminal". The terminal is running as root on a Parrot OS system. The command "#python3 sherlock satya nadella" has been entered and executed. The output lists numerous URLs found for the username "satya" across various platforms, including 7Cups, 9GAG, About.me, Academia.edu, AllMyLinks, Anilist, Apple Developer, Apple Discussions, Archive of Our Own, Archive.org, Arduino, Ask Fedora, AskFM, Audiojungle, BLIP.fm, Bandcamp, Behance, BiggerPockets, Bikemap, BitCoinForum, Blogger, BodyBuilding, Bookcrossing, BraveCommunity, BuyMeACoffee, and BuzzFeed. The terminal interface includes a menu bar with "Applications", "Places", "System", and "File" options, along with standard window control buttons (minimize, maximize, close) at the top and bottom.

```
[root@parrot]~/.sherlock
#python3 sherlock satya nadella
[*] Checking username satya on:

[+] 7Cups: https://www.7cups.com/@satya
[+] 9GAG: https://www.9gag.com/u/satya
[+] About.me: https://about.me/satya
[+] Academia.edu: https://independent.academia.edu/satya
[+] AllMyLinks: https://allmylinks.com/satya
[+] Anilist: https://anilist.co/user/satya/
[+] Apple Developer: https://developer.apple.com/forums/profile/satya
[+] Apple Discussions: https://discussions.apple.com/profile/satya
[+] Archive of Our Own: https://archiveofourown.org/users/satya
[+] Archive.org: https://archive.org/details/@satya
[+] Arduino: https://create.arduino.cc/projecthub/satya
[+] Ask Fedora: https://ask.fedoraproject.org/u/satya
[+] AskFM: https://ask.fm/satya
[+] Audiojungle: https://audiojungle.net/user/satya
[+] BLIP.fm: https://blip.fm/satya
[+] Bandcamp: https://www.bandcamp.com/satya
[+] Behance: https://www.behance.net/satya
[+] BiggerPockets: https://www.biggerpockets.com/users/satya
[+] Bikemap: https://www.bikemap.net/en/u/satya/routes/created/
[+] BitCoinForum: https://bitcoinaforum.com/profile/satya
[+] Blogger: https://satya.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/satya
[+] Bookcrossing: https://www.bookcrossing.com/mybookshelf/satya/
[+] BraveCommunity: https://community.brave.com/u/satya/
[+] BuyMeACoffee: https://buymeacoff.ee/satya
[+] BuzzFeed: https://buzzfeed.com/satya
```

```

Applications Places System python3 sherlock satya nadella - Parrot Terminal
File Edit View Search Terminal Help
[*] Checking username nadella on:

[+] 9GAG: https://www.9gag.com/u/nadella
[+] About.me: https://about.me/nadella
[+] Academia.edu: https://independent.academia.edu/nadella
[+] Anilist: https://anilist.co/user/nadella/
[+] Apple Discussions: https://discussions.apple.com/profile/nadella
[+] Archive.org: https://archive.org/details/@nadella
[+] Arduino: https://create.arduino.cc/projecthub/nadella
[+] AskFM: https://ask.fm/nadella
[+] Bikemap: https://www.bikemap.net/en/u/nadella/routes/created/
[+] BitBucket: https://bitbucket.org/nadella/
[+] Blogger: https://nadella.blogspot.com
[+] Chess: https://www.chess.com/member/nadella
[+] Clubhouse: https://www.clubhouse.com/@nadella
[+] Codecademy: https://www.codecademy.com/profiles/nadella
[+] Codechef: https://www.codechef.com/users/nadella
[+] Disqus: https://disqus.com/nadella
[+] Docker Hub: https://hub.docker.com/u/nadella/
[+] Dribbble: https://dribbble.com/nadella
[+] Duolingo: https://www.duolingo.com/profile/nadella
[+] EyeEm: https://www.eyeem.com/u/nadella
[+] F3.cool: https://f3.cool/nadella/
[+] Facebook: https://www.facebook.com/nadella
[+] Fiverr: https://www.fiverr.com/nadella
[+] Flickr: https://www.flickr.com/people/nadella
[+] Flipboard: https://flipboard.com/@nadella
[+] FortniteTracker: https://fortnitetracker.com/profile/all/nadella
[+] Freelancer: https://www.freelancer.com/u/nadella
[+] Freesound: https://freesound.org/people/nadella/

```

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.

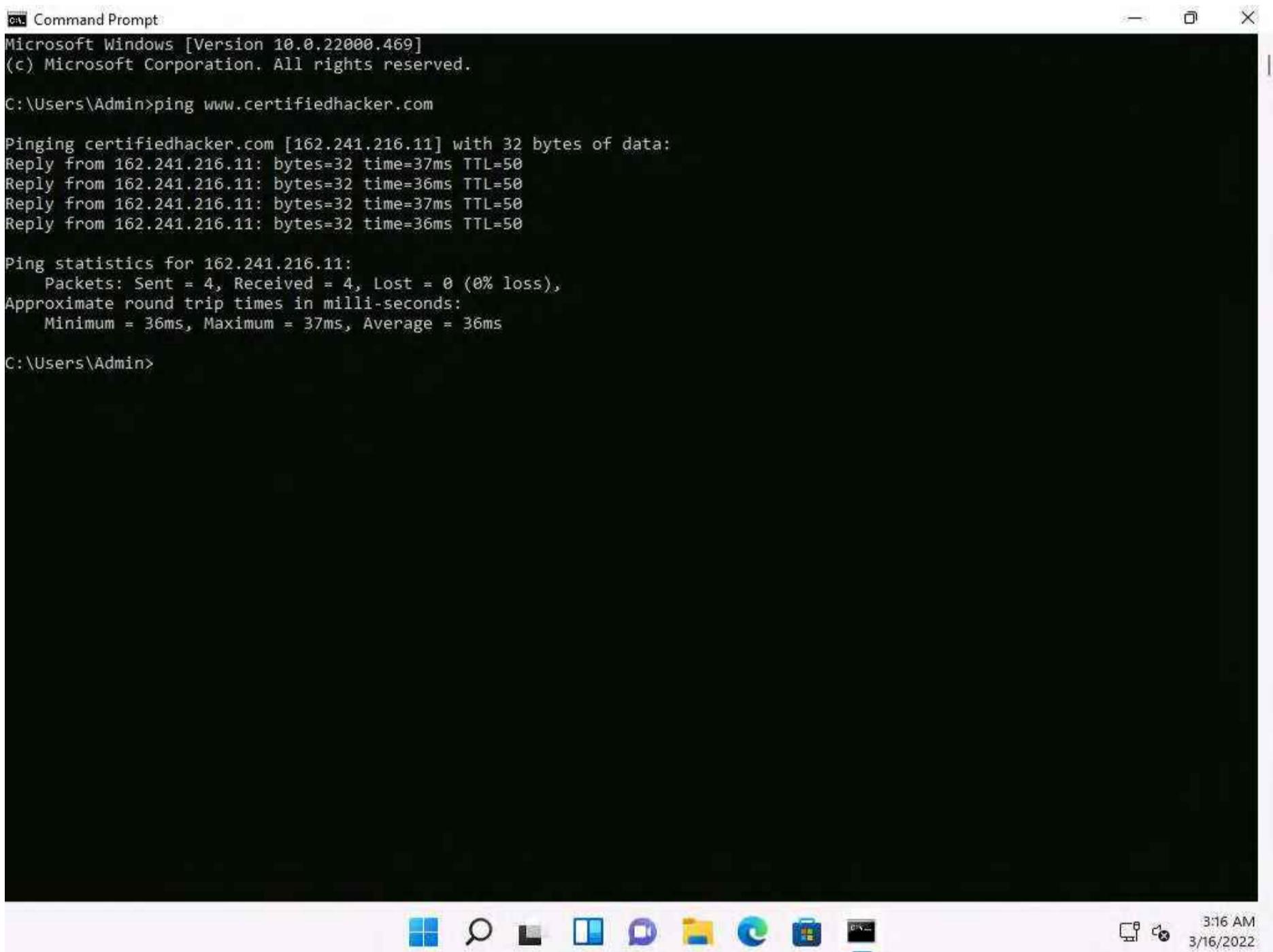
Task 1: Gather Information About a Target Website using Ping Command Line Utility

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.



```

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

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

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

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

C:\Users\Admin>

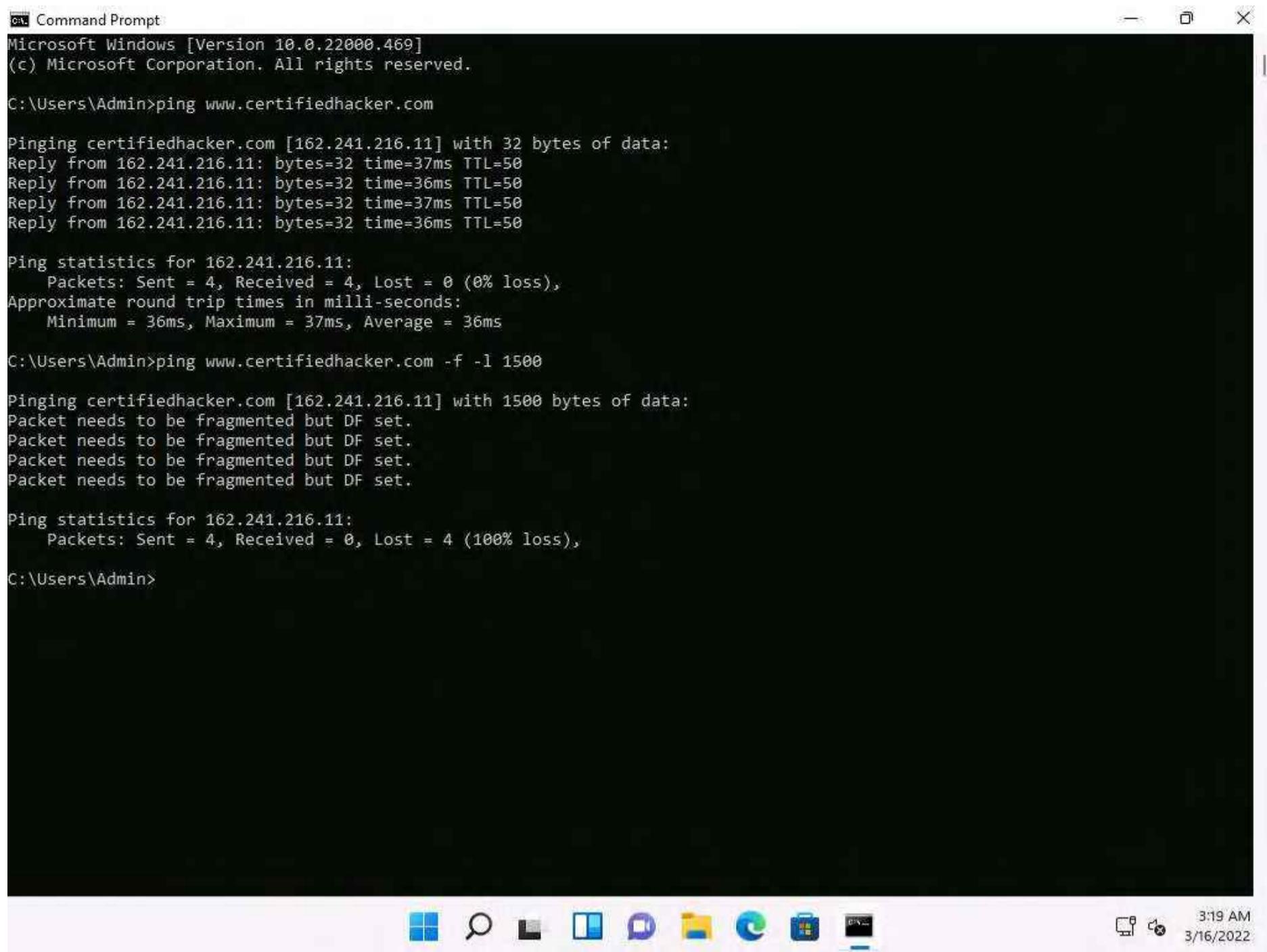
```

The screenshot shows a Windows 11 desktop environment. A Command Prompt window is open in the foreground, displaying the output of a ping command to the website www.certifiedhacker.com. The window title is "Command Prompt". The output shows four successful replies from the target IP address 162.241.216.11, with round-trip times ranging from 36ms to 37ms. Below the window, the Windows taskbar is visible with icons for File Explorer, Task View, Start, Search, and Edge browser. The system tray shows the date and time as 3/16/2022 at 3:16 AM.

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.





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

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

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

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

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

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

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

C:\Users\Admin>
```

3:19 AM
3/16/2022

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**.



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

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

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

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

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

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

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

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

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

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

C:\Users\Admin>
```

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

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



```
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1473
Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472
Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=35ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 37ms, Average = 36ms
C:\Users\Admin>
```

3:20 AM
3/16/2022

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

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

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



```
C:\Users\Admin>ping www.certifiedhacker.com -f -l 1473

Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:
Packet needs to be fragmented but DF set.

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

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472

Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=35ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 37ms, Average = 36ms

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

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

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

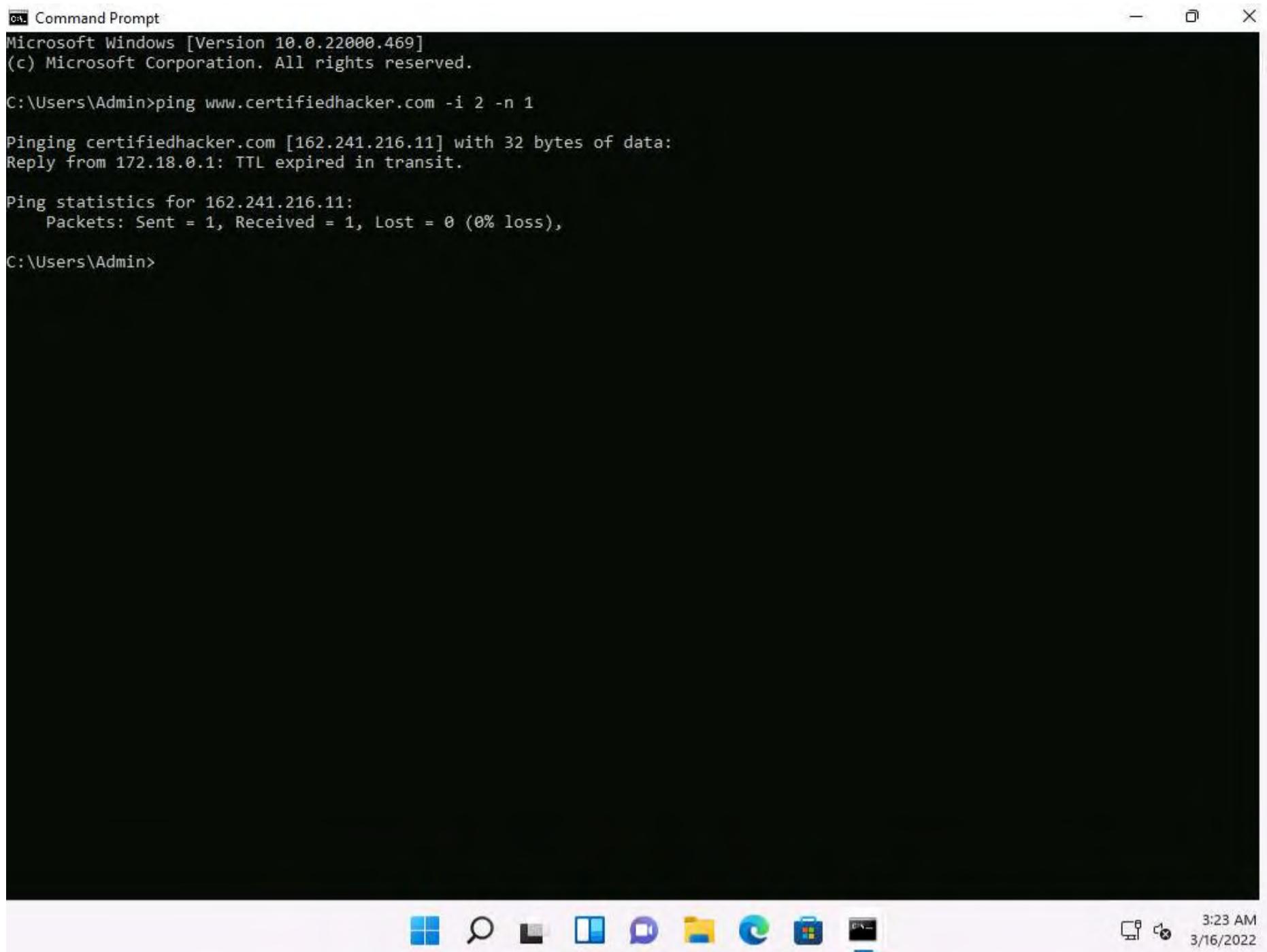
11. Reply from **192.168.100.6: TTL expired in transit** means that the router (192.168.100.6, you will have some other IP address) discarded the frame because its TTL has expired (reached 0).

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.





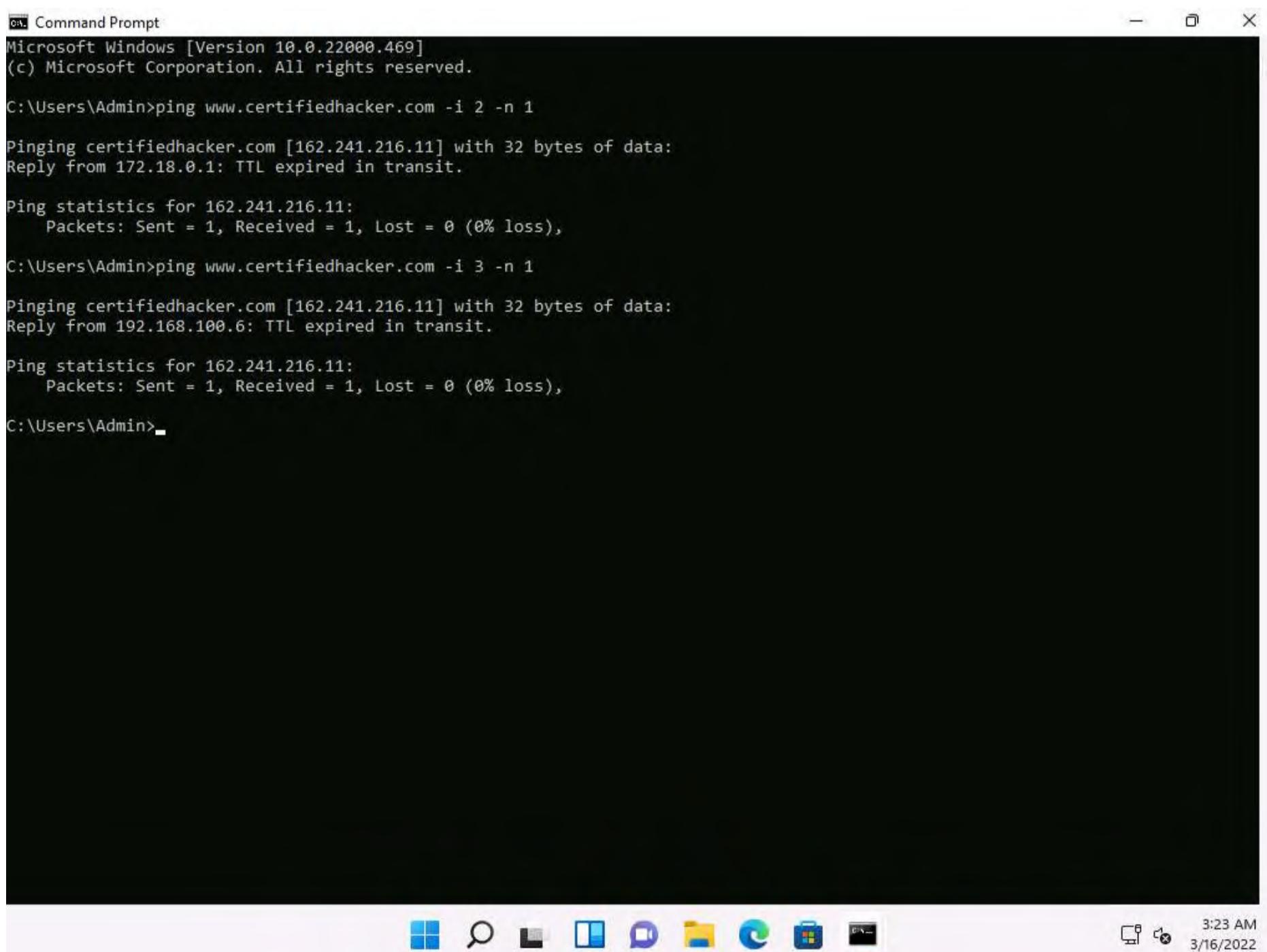
```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

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

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

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

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



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

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

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

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

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

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

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

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**.

```

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

C:\Users\Admin>ping www.certifiedhacker.com -i 2 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.18.0.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\Users\Admin>ping www.certifiedhacker.com -i 3 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 192.168.100.6: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\Users\Admin>ping www.certifiedhacker.com -i 4 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 103.152.3.225: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\Users\Admin>

```

3:24 AM
3/16/2022

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

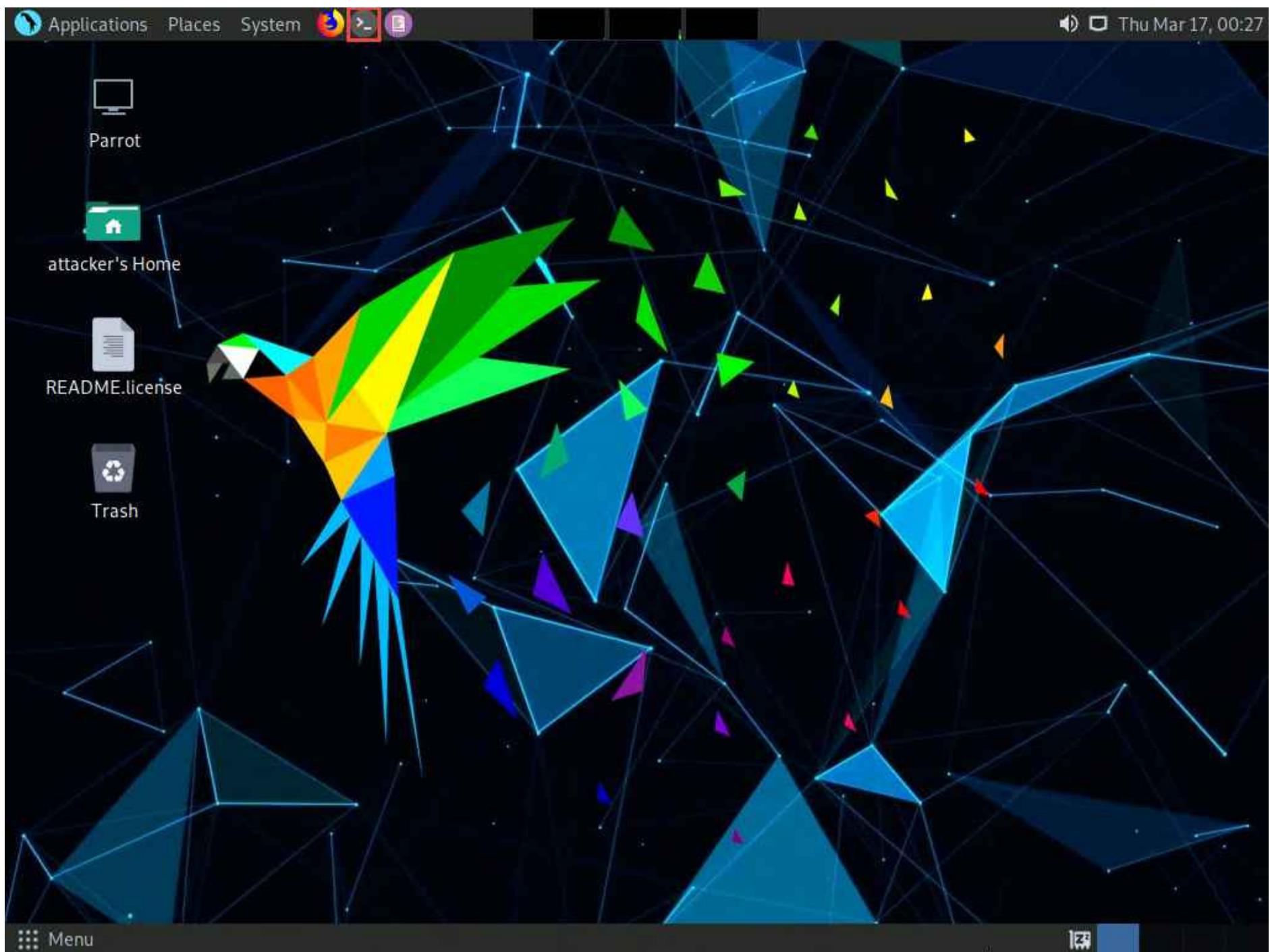
Photon is a Python script used to crawl a given target URL to obtain information such as URLs (in-scope and out-of-scope), URLs with parameters, email, social media accounts, files, secret keys and subdomains. The extracted information can further be exported in JSON format.

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.





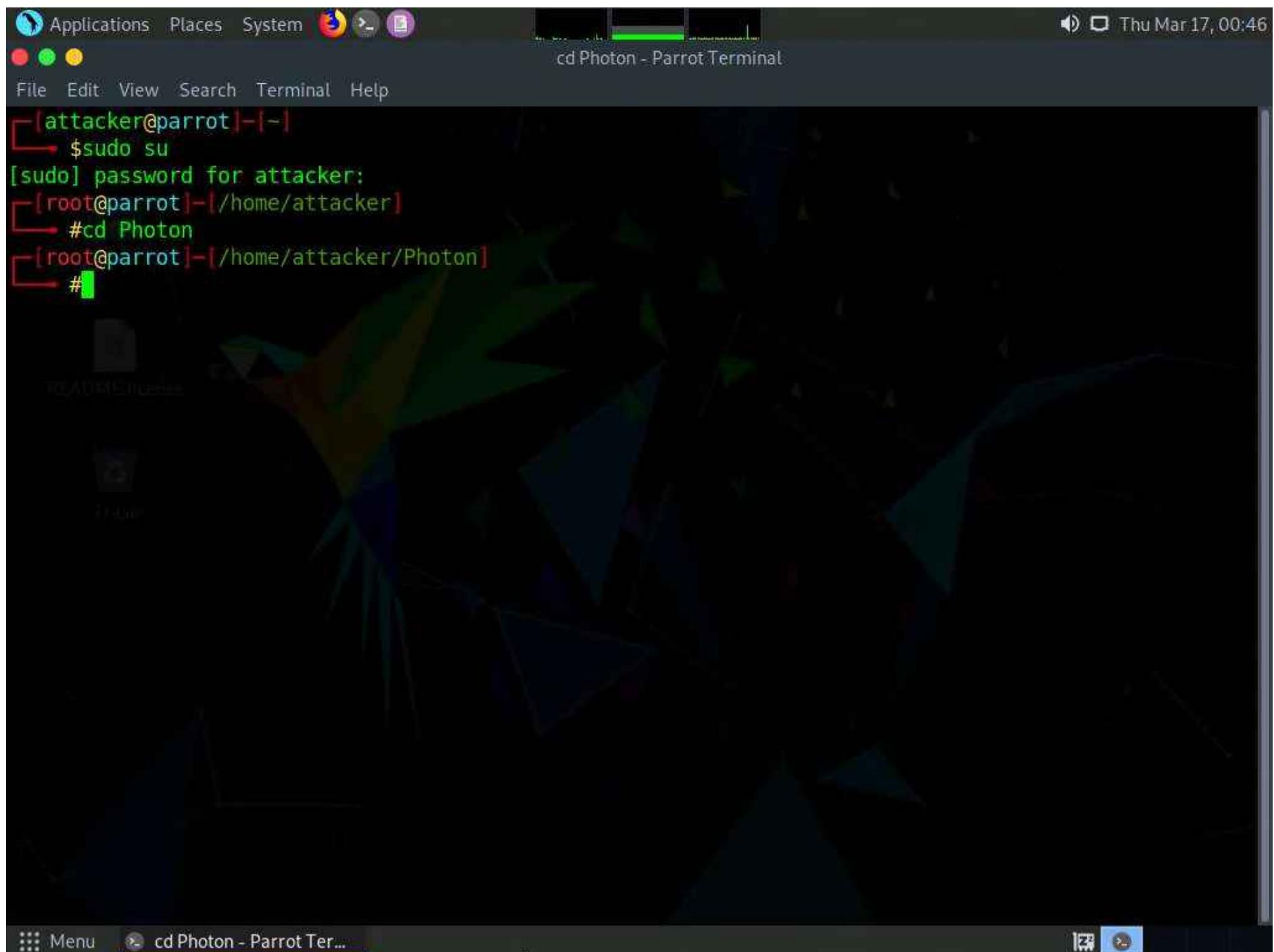
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

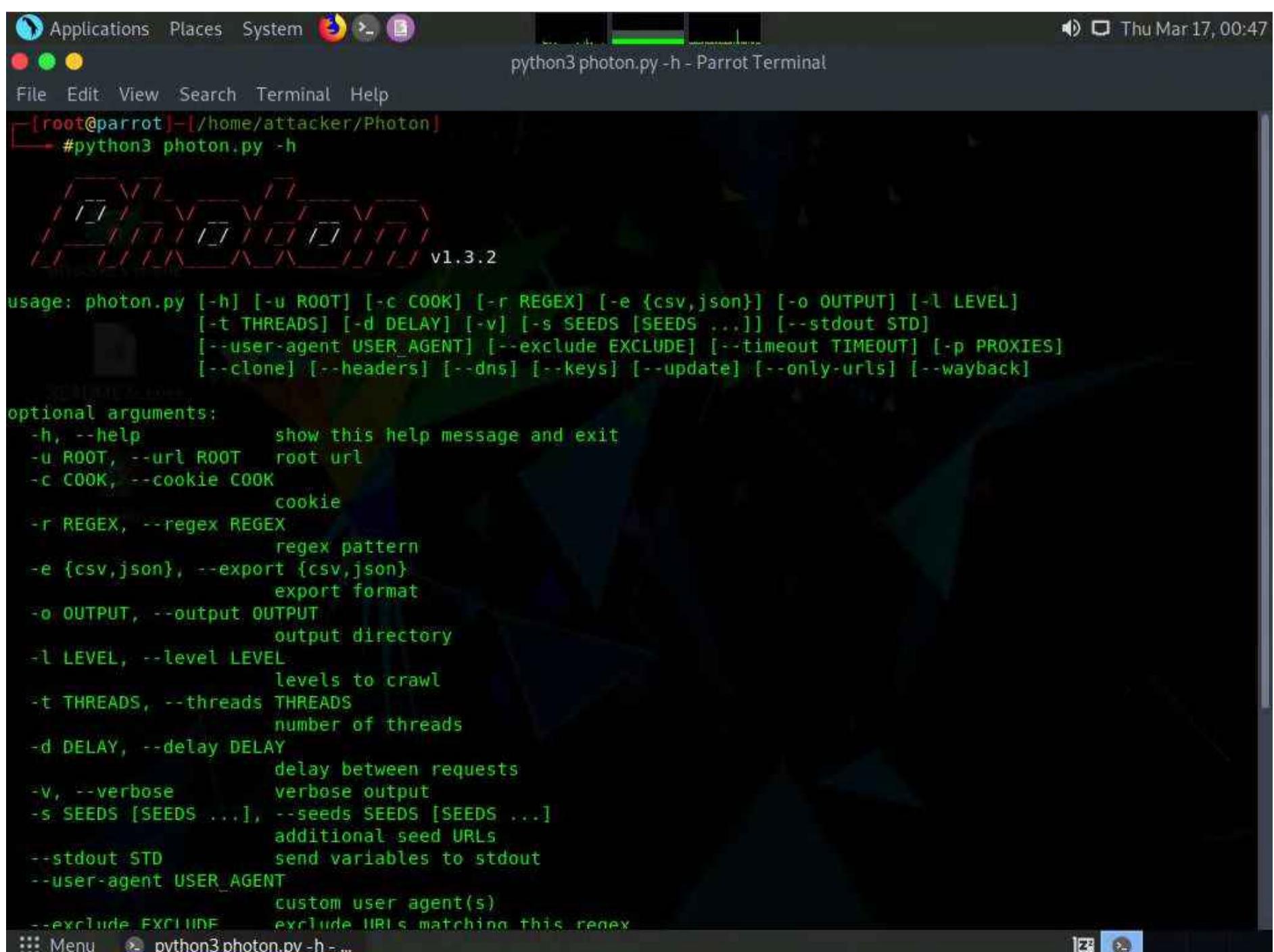
Note: The password that you type will not be visible.

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.

```
python3 photon.py -u http://www.certifiedhacker.com - Parrot Terminal
[~] Level 1: 1 URLs
[!] Progress: 1/1
[~] Level 2: 3 URLs
[!] Progress: 3/3
[~] Crawling 18 JavaScript files
[!] Progress: 18/18
[+] Internal: 4
[+] Scripts: 18
[+] External: 9
[!] Total requests made: 23
[!] Total time taken: 0 minutes 1 seconds
[!] Requests per second: 13
[+] Results saved in www.certifiedhacker.com directory
[root@parrot]~[/home/attacker/Photon]
#
```

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

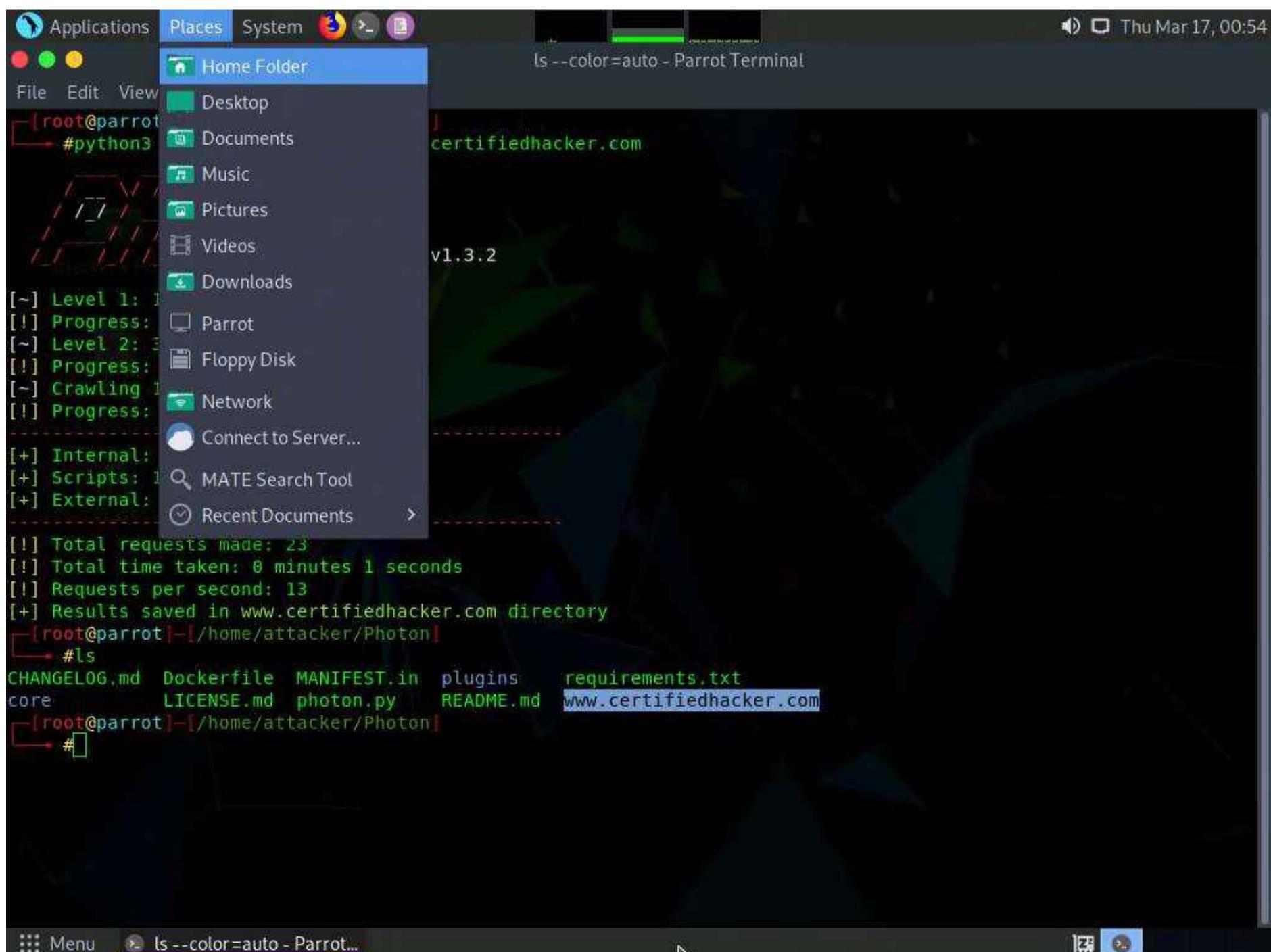
10. You can observe that a directory named **www.certifiedhacker.com** is created, as shown in the screenshot.



```

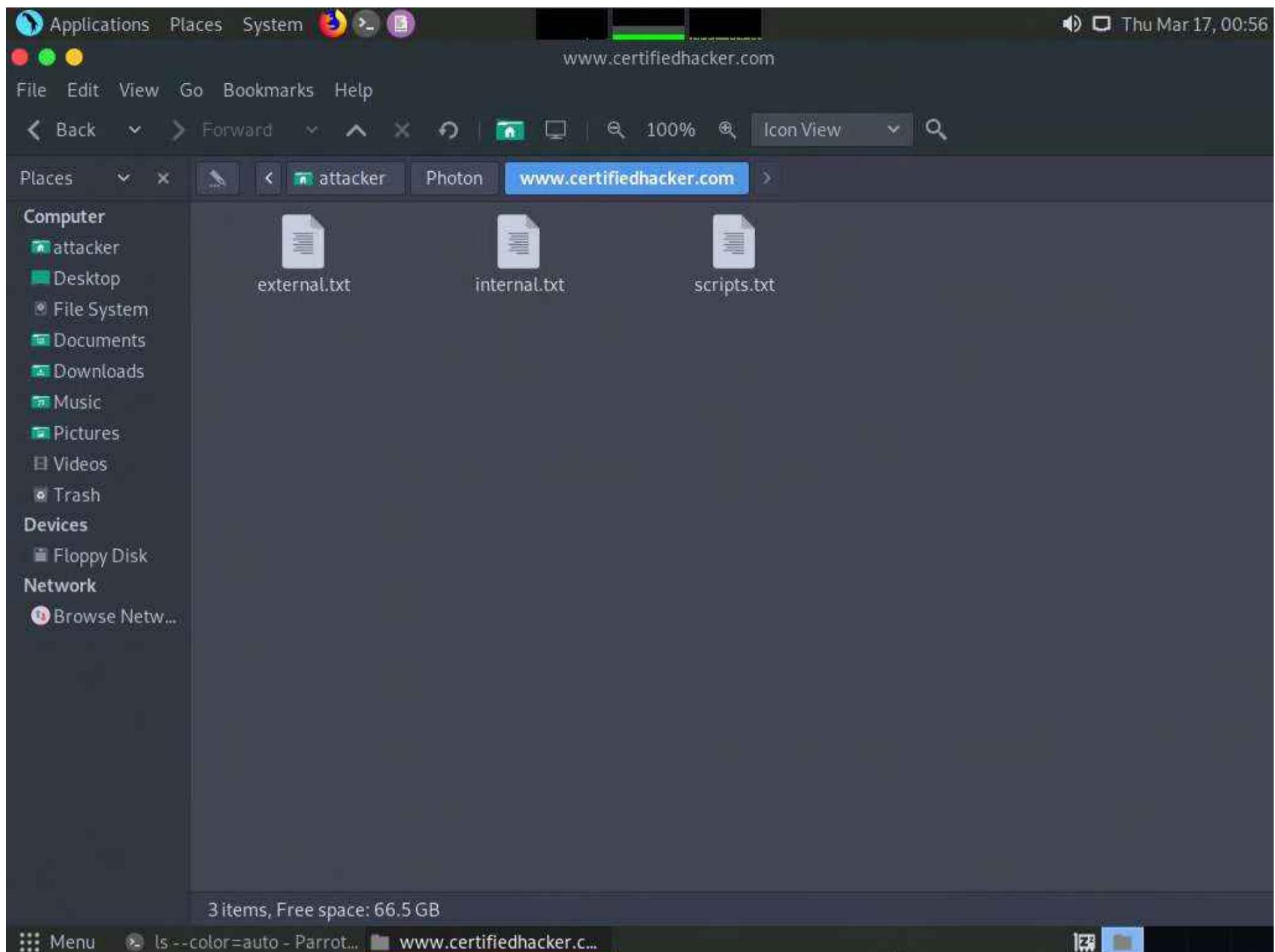
ls --color=auto - Parrot Terminal
[~] Level 1: 1 URLs
[!] Progress: 1/1
[~] Level 2: 3 URLs
[!] Progress: 3/3
[~] Crawling 18 JavaScript files
[!] Progress: 18/18
[+] Internal: 4
[+] Scripts: 18
[+] External: 9
[!] Total requests made: 23
[!] Total time taken: 0 minutes 1 seconds
[!] Requests per second: 13
[+] Results saved in www.certifiedhacker.com directory
[root@parrot]~/home/attacker/Photon]
#ls
CHANGELOG.md Dockerfile MANIFEST.in plugins requirements.txt
core LICENSE.md photon.py README.md www.certifiedhacker.com
[root@parrot]~/home/attacker/Photon]
#
```

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



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

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

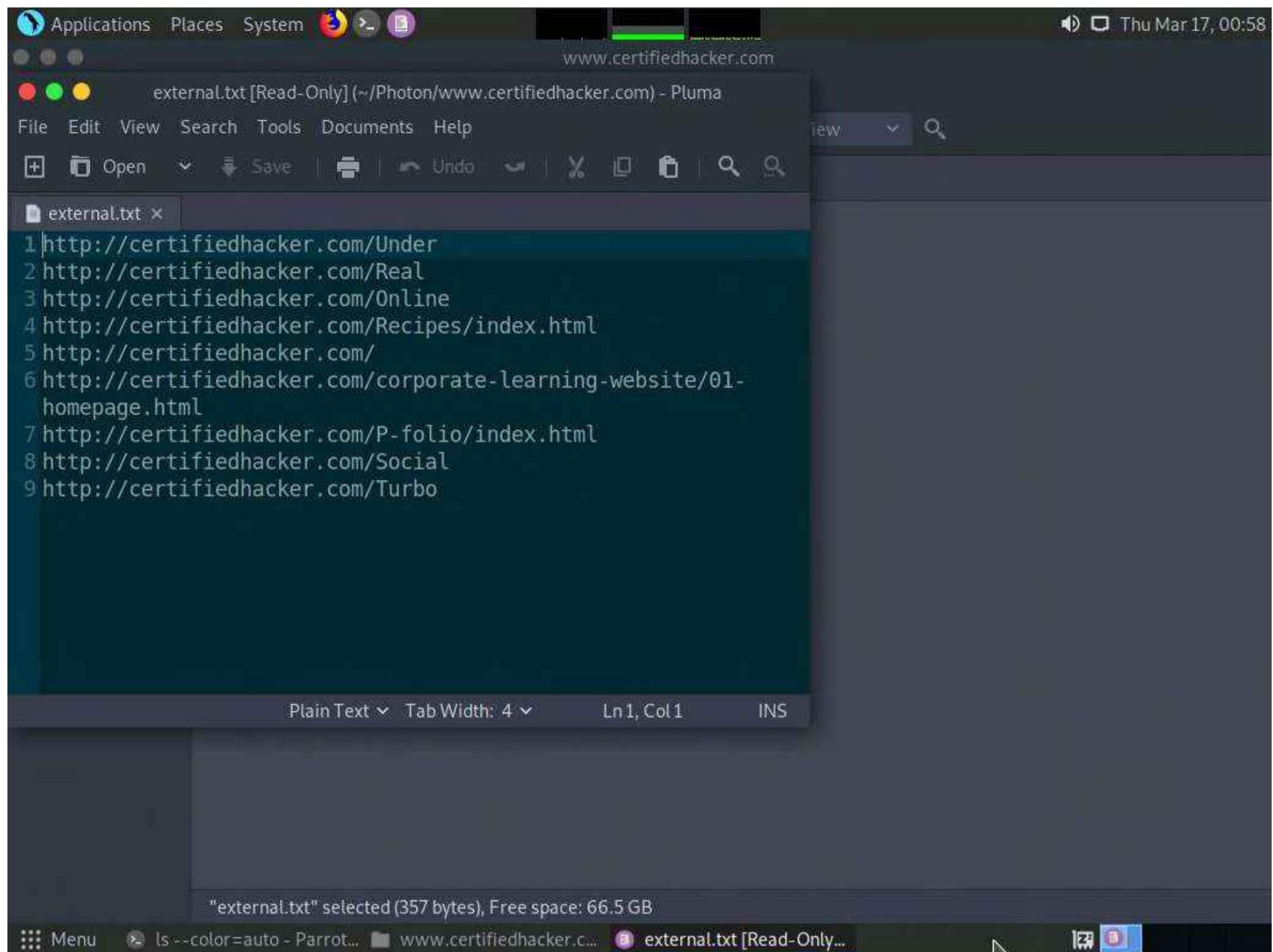


14. Double-click **external.txt** file to view the file content.

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

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





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

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

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

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

-l: specifies level to crawl (here, 3)

-t: specifies number of threads (here, 200)

--wayback: specifies using URLs from archive.org as seeds

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

```

Applications Places System python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 --wayback - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Photon]
#python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 --wayback
v1.3.2

[~] Fetching URLs from archive.org
[+] Retrieved 0 URLs from archive.org
[~] Level 1: 2 URLs
[!] Progress: 2/2
[~] Level 2: 2 URLs
[!] Progress: 2/2
[~] Crawling 18 JavaScript files
[!] Progress: 18/18

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

[!] Total requests made: 23
[!] Total time taken: 0 minutes 1 seconds
[!] Requests per second: 22
[+] Results saved in www.certifiedhacker.com directory
[root@parrot]~/home/attacker/Photon]
#

```

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.



The screenshot shows the CentralOps.net website with a blue header bar. The header includes the site's name, "Advanced online Internet utilities", and a note "a service of :Hexillion". On the right side of the header are links for "Utilities" and "About". Below the header is a sidebar titled "Utilities" containing links to various tools: Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup, AutoWhois, and AnalyzePath.

The main content area features a section titled "Free online network tools" with a sub-section titled "Tools". Under "Tools", there are five items: "Domain Dossier", "Domain Check", "Email Dossier", "Browser Mirror", and "Ping". Each tool has a brief description and a form field for entering a domain or IP address, followed by a "go" button.

In the top right corner of the main content area, there is a user status box showing "user: anonymous [199.101.110.13]" and "balance: 49 units", with links for "log in" and "account info".

The bottom of the page features a toolbar with icons for Windows, search, file operations, and other browser functions. The status bar at the bottom right shows the time as 3:49 AM and the date as 3/16/2022.

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.

This screenshot is identical to the one above, but the "Domain Dossier" tool's input field contains the URL "www.certifiedhacker.com". The "go" button is visible next to the input field.

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

The screenshot shows a web browser window for 'Central Ops .net' with the URL <https://centralops.net/co/>. The page title is 'Domain Dossier' with the subtitle 'Investigate domains and IP addresses'. On the left, a sidebar titled 'Utilities' lists various tools: Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup, AutoWhois, and AnalyzePath. The main content area has a form where 'domain or IP address' is set to 'www.certifiedhacker.com'. Underneath, several checkboxes are checked: 'domain whois record', 'DNS records', 'network whois record', and 'traceroute'. There is also an unchecked checkbox for 'service scan' and a 'go!' button. Below the form, it says 'user: anonymous [199.101.110.13]' and 'balance: 48 units'. A link to 'log in | account info' is present. A note at the bottom encourages users to 'Read about reduced Whois data due to the GDPR.' The right side of the page features the 'CentralOps.net' logo and navigation links for 'Utilities' and 'About'. The status bar at the bottom right shows the date and time: '3/16/2022 3:50 AM'.

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

The screenshot shows a Microsoft Windows desktop environment. A browser window is open to <https://centralops.net/>. The page displays network whois records for the IP address 162.241.216.11. The results show details from rwhois unifiedlayer.com and whois.arin.net. The Windows taskbar at the bottom includes icons for File Explorer, Task View, Start, Search, Taskbar settings, and a system tray with a battery icon.

Network Whois record

Queried **rwhois.unifiedlayer.com** with "162.241.216.11"...

```

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

```

%ok

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

```

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

```

OrgName: Unified Layer

Show desktop

3:51 AM 3/16/2022

The screenshot shows a Microsoft Windows desktop environment. A browser window is open to <https://centralops.net/>. The page displays DNS records for the domain www.certifiedhacker.com. The results include CNAME, NS, and HINFO records. The Windows taskbar at the bottom includes icons for File Explorer, Task View, Start, Search, Taskbar settings, and a system tray with a battery icon.

DNS records

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

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

No audio device is installed

3:51 AM 3/16/2022

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.

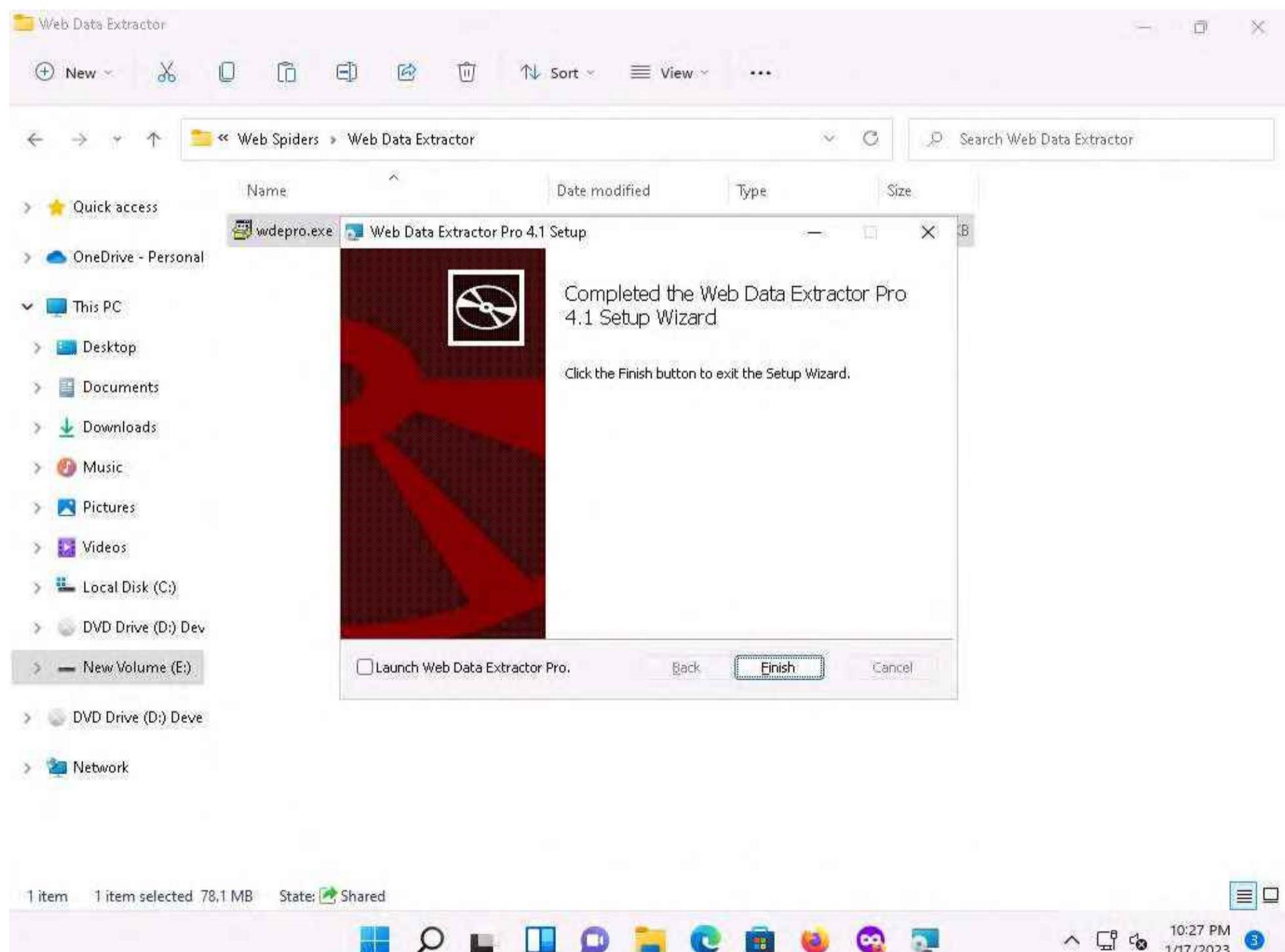
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wdepro.exe**.

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

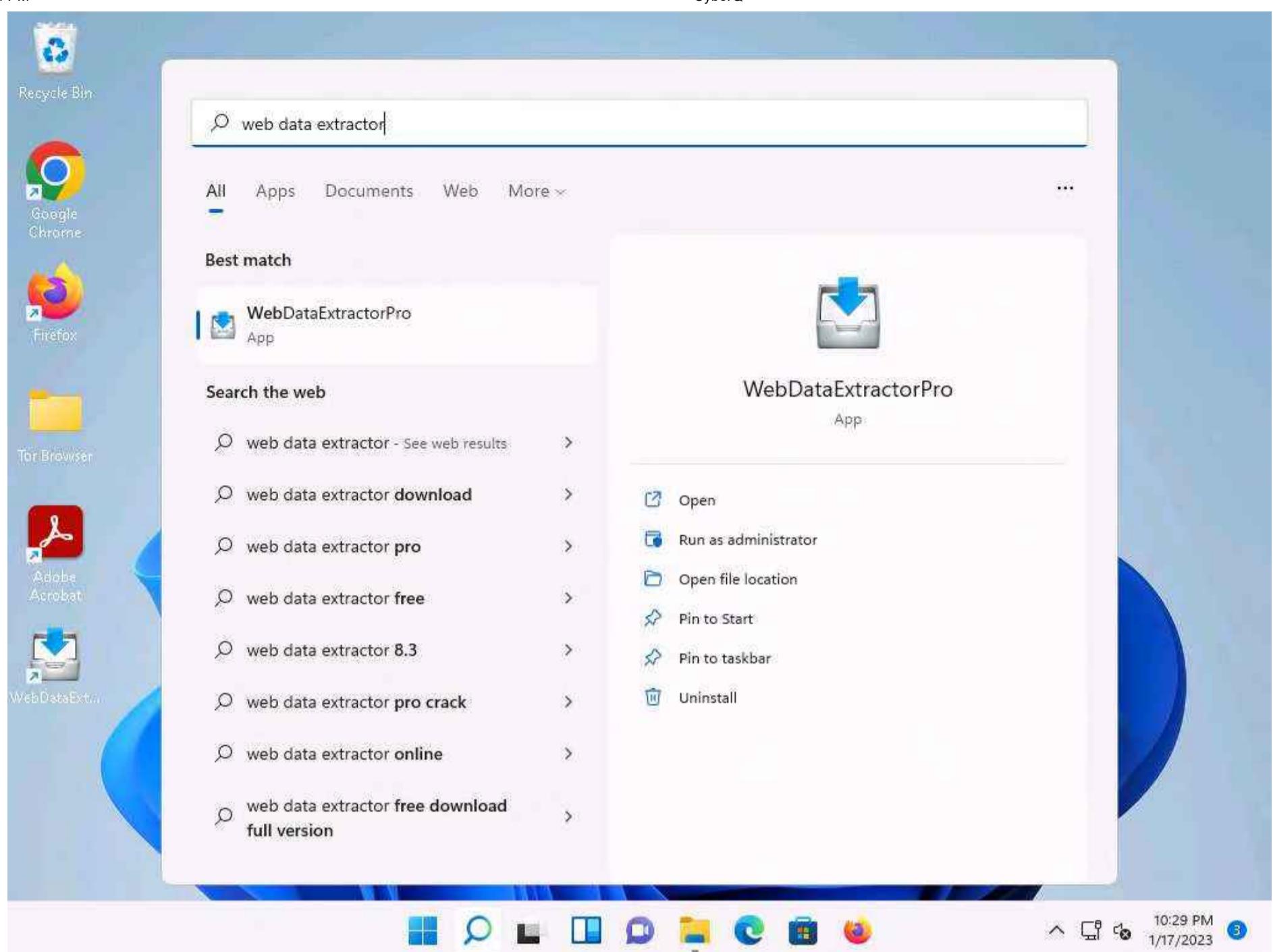
2. If the **User Account Control** pop-up appears, click **Yes**.

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

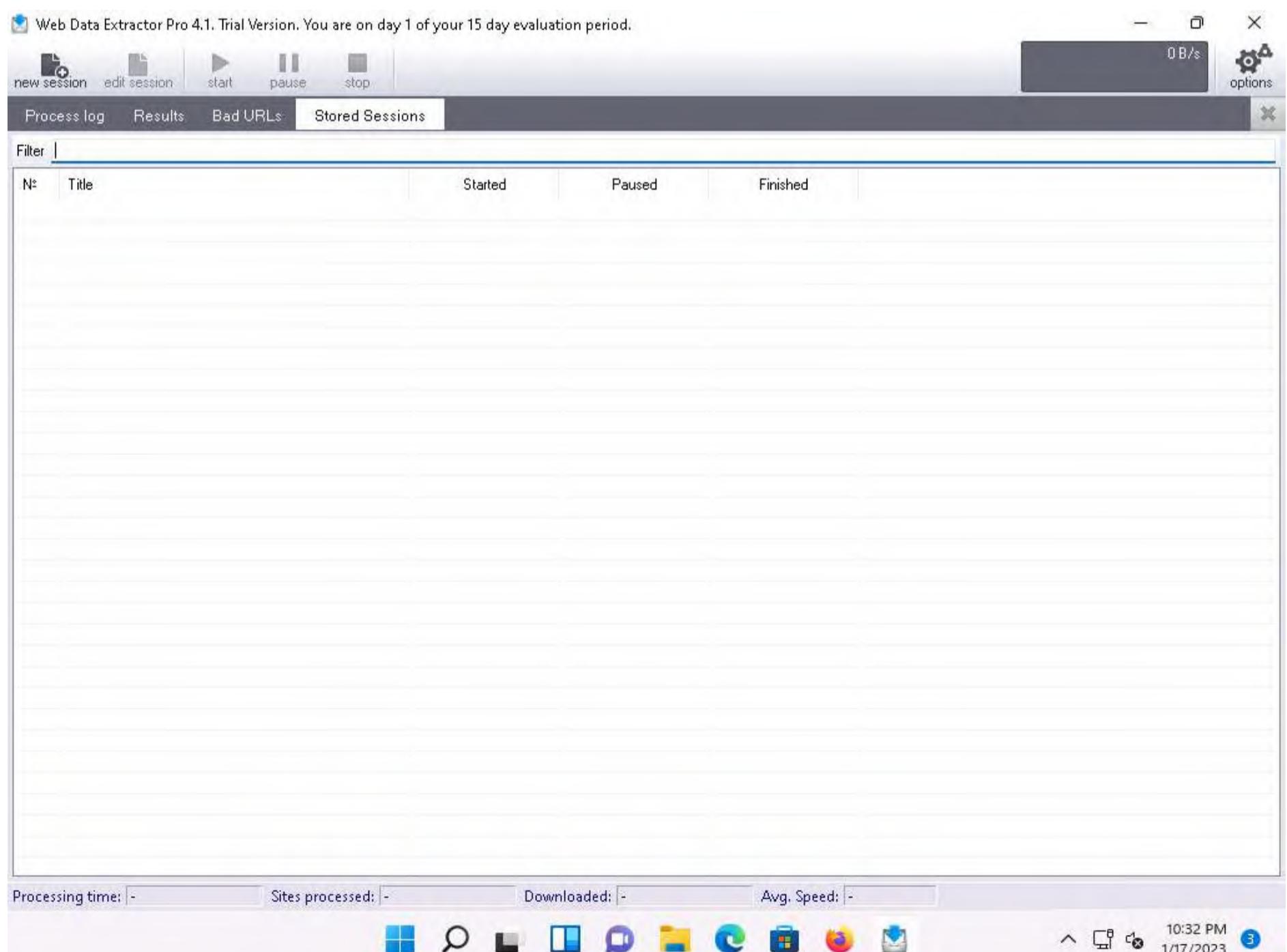
Note: Ensure that **Launch Web Data Extractor** checkbox is unchecked.



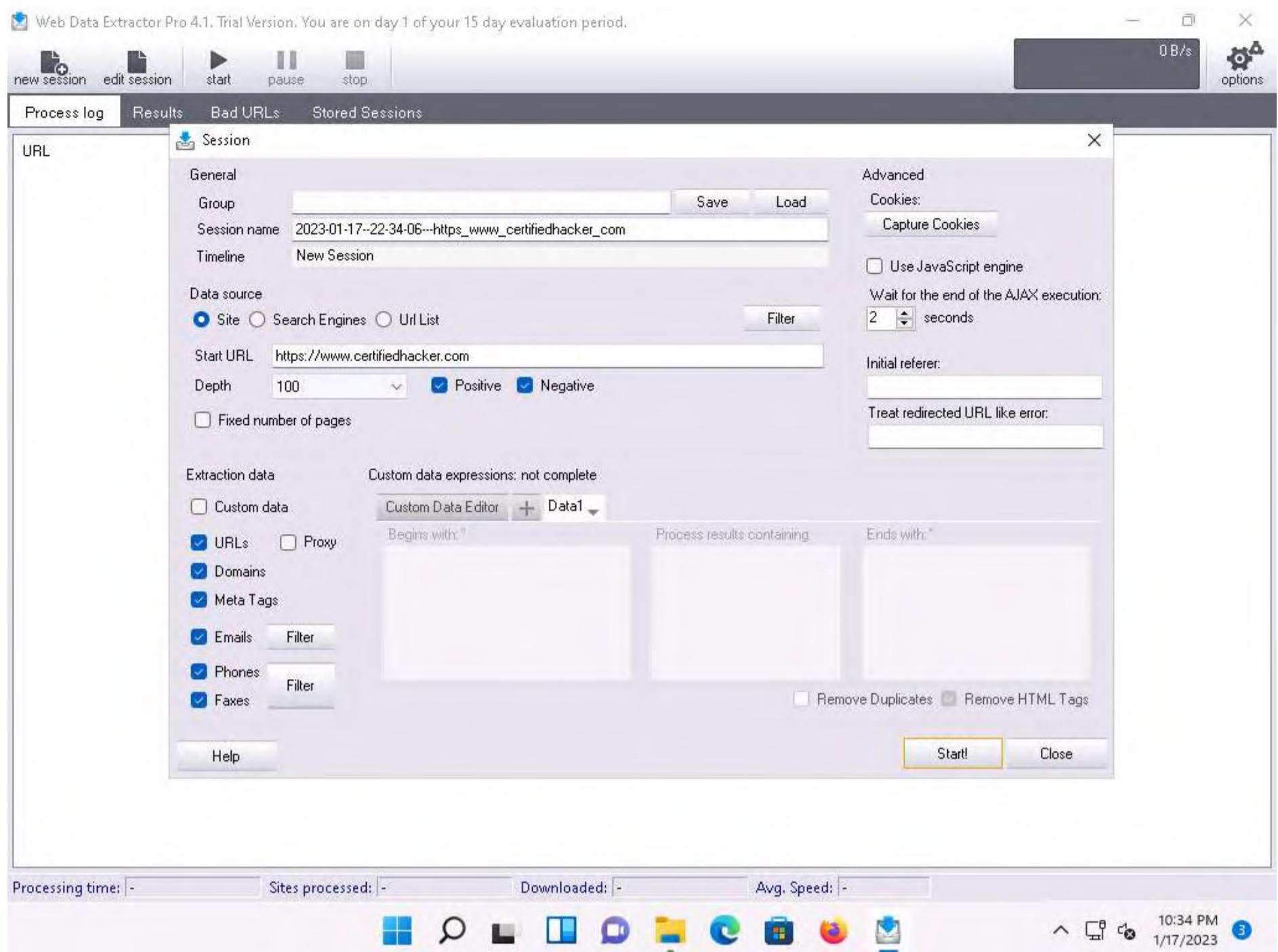
4. Click **Search** icon () on the **Desktop** and type **web data extractor** in the search field. The **Web Data Extractor Pro** appears in the results, click **Open** to launch it.



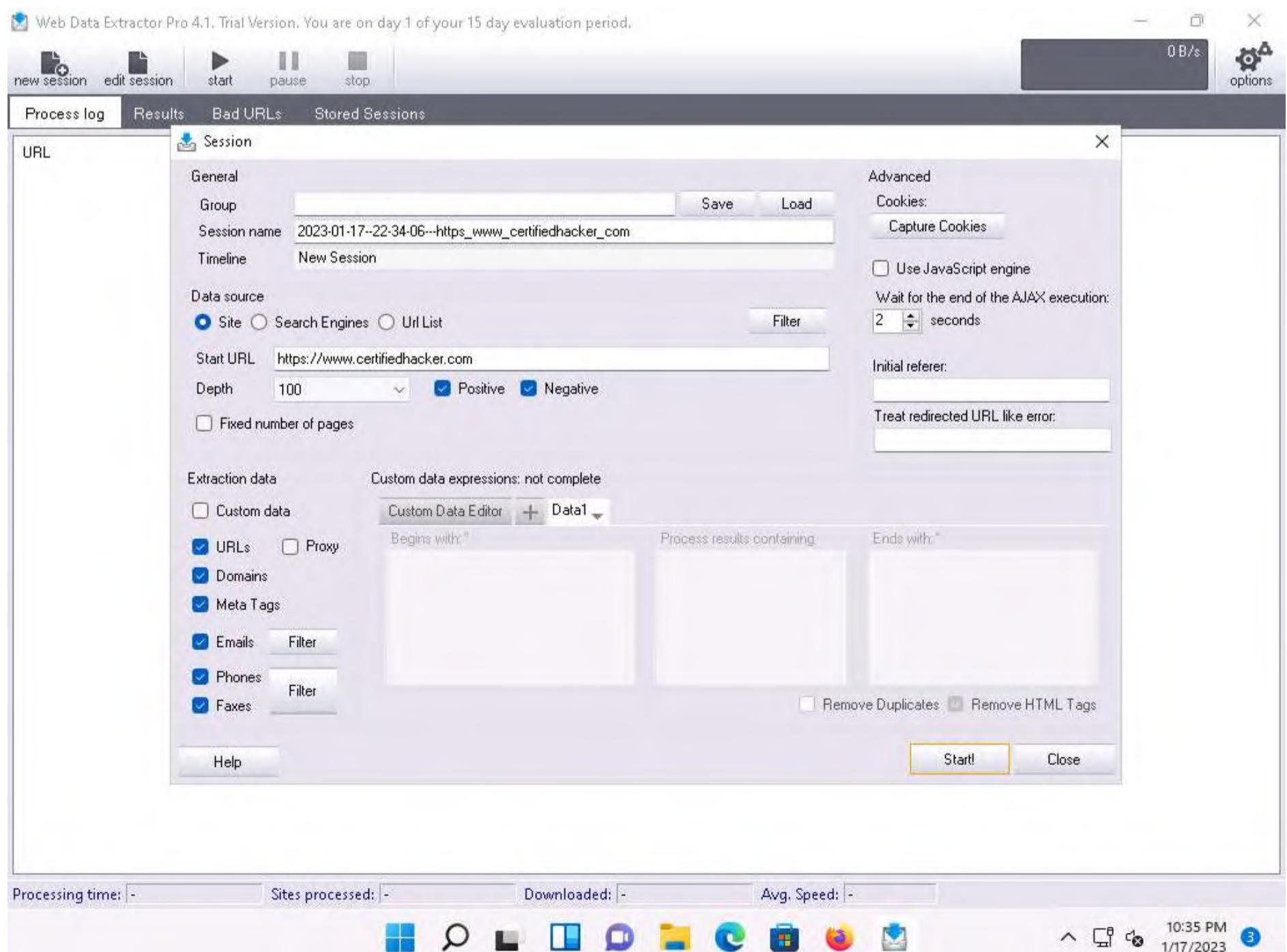
5. The **Web Data Extractor** main window appears. Click **new session** to start a new session.



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).

Web Data Extractor Pro 4.1. Trial Version. You are on day 1 of your 15 day evaluation period.

new session edit session start pause stop

Process log *Results Bad URLs (11) Stored Sessions

URL	Title	State	Size	Downloaded
https://certifiedhacker.com/docs/NIST.SP.800-63a.pdf		Parse	836,298	836,298
https://certifiedhacker.com/docs/NIST.SP.800-63-3.pdf		Parse	2,512,126	2,512,126

Processing time: 00:00:09.984 Sites processed: 75 / 82 Downloaded: 7,490 KB Avg. Speed: 891 KB/s

10:35 PM 1/17/2023

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

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

Web Data Extractor Pro 4.1. Trial Version. You are on day 1 of your 15 day evaluation period.

new session edit session start pause stop

Process log *Results Bad URLs (12) Stored Sessions

MetaTag (26)	Email (11)	Phone (147)	Fax (143)	Link (61)	Domain (1)	Description	Keywords	Title	Url	Host	Domain	Page size	Page last modified
A brief description of this we...	keywords, or phrases, asso...	Certified Hacker				https://www.certifiedhacker.com/	certifiedhacker.com	com	9660	2011-02-10			
Professional Real Estate Se...	real estate, real estate listin...	Professional Real Estate S...				https://certifiedhacker.com/Real%20...	certifiedhacker.com	com	5845	2011-02-10			
A short description of your c...	Some keywords that best d...	Clear Construction				https://certifiedhacker.com/Under%2...	certifiedhacker.com	com	5381	2011-02-10			
Turbo max powerfull one pa...	Turbo max , owltemplates.c...	Your company - Homepage				https://certifiedhacker.com/Recipes/...	certifiedhacker.com	com	5151	2017-12-27			
A brief description of this we...	keywords, or phrases, asso...	Under the Trees				https://certifiedhacker.com/Under%2...	certifiedhacker.com	com	5899	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	P-Folio				https://certifiedhacker.com/P-folio/in...	certifiedhacker.com	com	3653	2017-12-27			
A short description of your c...	Some keywords that best d...	Turbo Max Theme - OwlTe...				https://certifiedhacker.com/Turbo%2...	certifiedhacker.com	com	11606	2017-12-27			
A brief description of this we...	keywords, or phrases, asso...	Unite - Together is Better (...				https://certifiedhacker.com/Social%2...	certifiedhacker.com	com	12125	2017-12-27			
Online Booking	booking, hotel, hotels, rese...	Online Booking				https://certifiedhacker.com/Online%2...	certifiedhacker.com	com	15094	2017-12-27			
A short description of your c...	Some keywords that best d...	Your company - Recipes d...				https://certifiedhacker.com/Online%2...	certifiedhacker.com	com	20280	2017-12-27			
A short description of your c...	Some keywords that best d...	Your company - About us				https://certifiedhacker.com/Recipes/...	certifiedhacker.com	com	9635	2011-02-10			
A short description of your c...	Some keywords that best d...	Your company - Menu				https://certifiedhacker.com/About%2...	certifiedhacker.com	com	5762	2011-02-10			
A short description of your c...	Some keywords that best d...	Your company - Contact us				https://certifiedhacker.com/Menu/...	certifiedhacker.com	com	7909	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	Online Booking: Checkout				https://certifiedhacker.com/Contact%2...	certifiedhacker.com	com	5828	2011-02-10			
A short description of your c...	Some keywords that best d...	Your company - Recipes				https://certifiedhacker.com/Checkout/...	certifiedhacker.com	com	12968	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	Online Booking: Browse D...				https://certifiedhacker.com/Recipes/...	certifiedhacker.com	com	12716	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	Online Booking: Sitemap				https://certifiedhacker.com/Browse%2...	certifiedhacker.com	com	16031	2011-02-10			
A short description of your c...	Some keywords that best d...	Online Booking: Typography				https://certifiedhacker.com/Sitemap/...	certifiedhacker.com	com	11689	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	Your company - Menu cate...				https://certifiedhacker.com/Typography/...	certifiedhacker.com	com	12661	2011-02-10			
A short description of your c...	Some keywords that best d...	Online Booking: Search				https://certifiedhacker.com/Menu/...	certifiedhacker.com	com	11584	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	Online Booking: Contact Us				https://certifiedhacker.com/Search/...	certifiedhacker.com	com	27877	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	Online Booking: FAQ				https://certifiedhacker.com/Contact%2...	certifiedhacker.com	com	14163	2011-02-10			
A short description of your c...	Some keywords that best d...	Your company - Recipes c...				https://certifiedhacker.com/FAQ/...	certifiedhacker.com	com	14047	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	Online Booking: Print Previ...				https://certifiedhacker.com/Recipes/...	certifiedhacker.com	com	12451	2011-02-10			
Online Booking	booking, hotel, hotels, rese...	Online Booking: Hotel Info				https://certifiedhacker.com/Print%2...	certifiedhacker.com	com	5693	2011-02-10			
						https://certifiedhacker.com/Hotel%2...	certifiedhacker.com	com	39498	2011-02-10			

Processing time: 00:03:02,874 Sites processed: 78 / 82 Downloaded: 4,220 KB Avg. Speed: 710 KB/s

10:38 PM 1/17/2023

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.

The screenshot shows the 'Results' tab selected in the top navigation bar. Below it is a table with columns: Description, Keywords, Title, Url, Host, Domain, Page size, and Page last modified. The table contains 26 rows of meta-tag data. At the bottom of the window, there is a status bar displaying processing time, sites processed, download statistics, and average speed. The status bar also shows the date and time (10:39 PM, 1/17/2023) and has icons for various applications like File Explorer, Task Manager, and Mail.

Description	Keywords	Title	Url	Host	Domain	Page size	Page last modified
A brief description of this we...	keywords, or phrases, asso...	Certified Hacker	https://www.certifiedhacker.com/	certifiedhacker.com	.com	9660	2011-02-10
Professional Real Estate Se...	real estate, real estate listin...	Professional Real Estate S...	https://certifiedhacker.com/Real%20...	certifiedhacker.com	.com	5845	2011-02-10
A short description of your c...	Some keywords that best d...	Clear Construction	https://certifiedhacker.com/Under%2...	certifiedhacker.com	.com	5381	2011-02-10
Turbo max powerfull one pa...	Turbo max , owltemplates.c...	Turbo Max Theme - OwlTe...	https://certifiedhacker.com/Turbo%2...	certifiedhacker.com	.com	12125	2017-12-27
A brief description of this we...	keywords, or phrases, asso...	Unite - Together is Better (...)	https://certifiedhacker.com/Social%2...	certifiedhacker.com	.com	15094	2017-12-27
Online Booking	booking, hotel, hotels, rese...	Online Booking	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	20280	2017-12-27
A short description of your c...	Some keywords that best d...	Your company - Recipes d...	https://certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	9635	2011-02-10
A short description of your c...	Some keywords that best d...	Your company - About us	https://certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	5762	2011-02-10
A short description of your c...	Some keywords that best d...	Your company - Menu	https://certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	7909	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Your company - Contact us	https://certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	5828	2011-02-10
A short description of your c...	Some keywords that best d...	Online Booking: Checkout	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	12968	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Your company - Recipes	https://certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	12716	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Online Booking: Browse D...	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	16031	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Online Booking: Sitemap	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	11689	2011-02-10
A short description of your c...	Some keywords that best d...	Online Booking: Typography	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	12661	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Your company - Menu cate...	https://certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	11584	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Online Booking: Search	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	27877	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Online Booking: Contact Us	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	14163	2011-02-10
A short description of your c...	Some keywords that best d...	Online Booking: FAQ	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	14047	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Your company - Recipes c...	https://certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	12451	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Online Booking: Print Previ...	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	5693	2011-02-10
Online Booking	booking, hotel, hotels, rese...	Online Booking: Hotel Info	https://certifiedhacker.com/Online%2...	certifiedhacker.com	.com	39498	2011-02-10

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

Processing time: 00:04:04.875 Sites processed: 78 / 82 Downloaded: 4,220 KB Avg. Speed: 710 KB/s

10:39 PM 1/17/2023

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

Processing time: 00:05:27.138 Sites processed: 78 / 82 Downloaded: 4,220 KB Avg. Speed: 710 KB/s

10:40 PM 1/17/2023

14. Check for more information under the **Fax**, **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

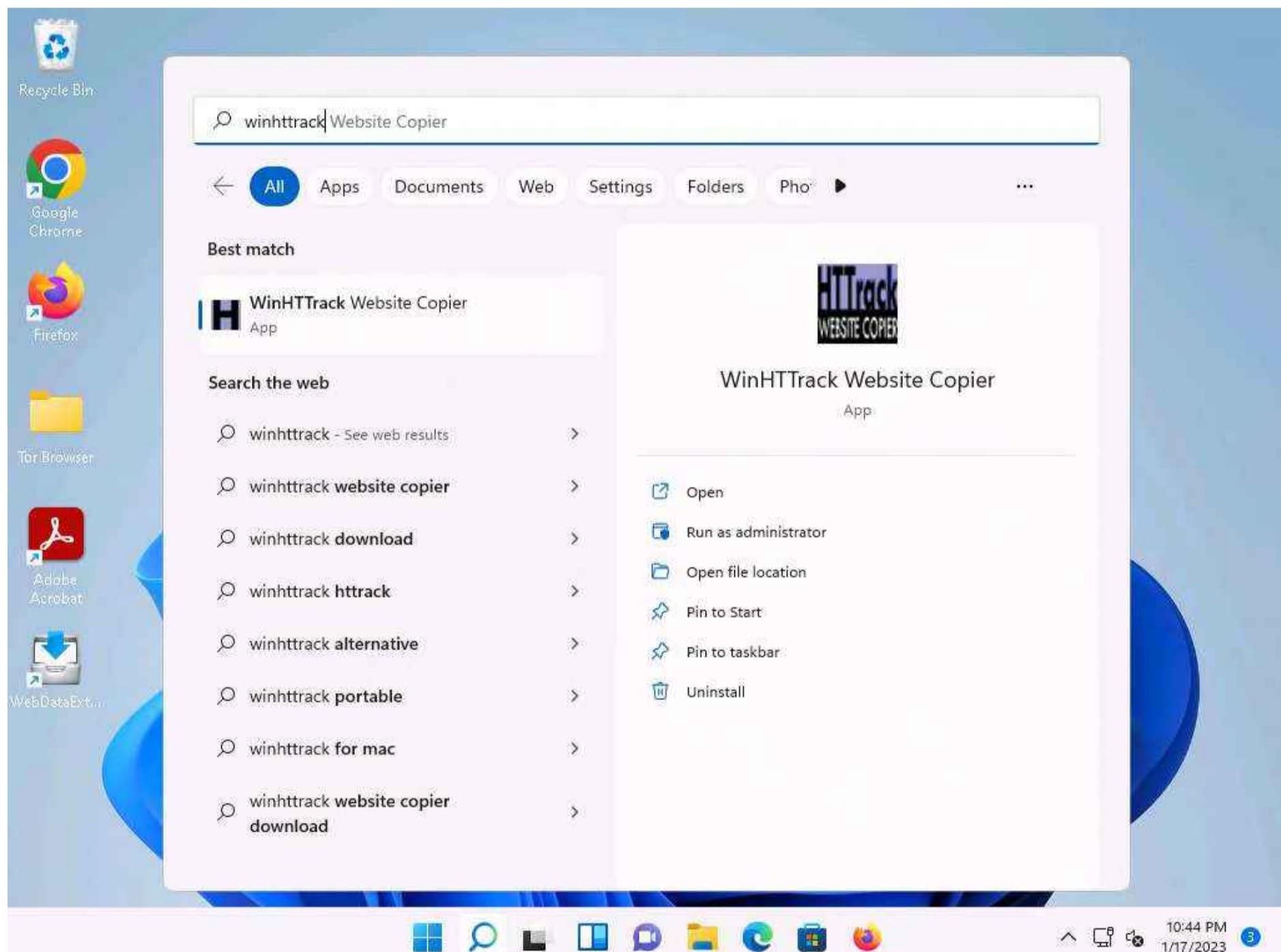
Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos,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

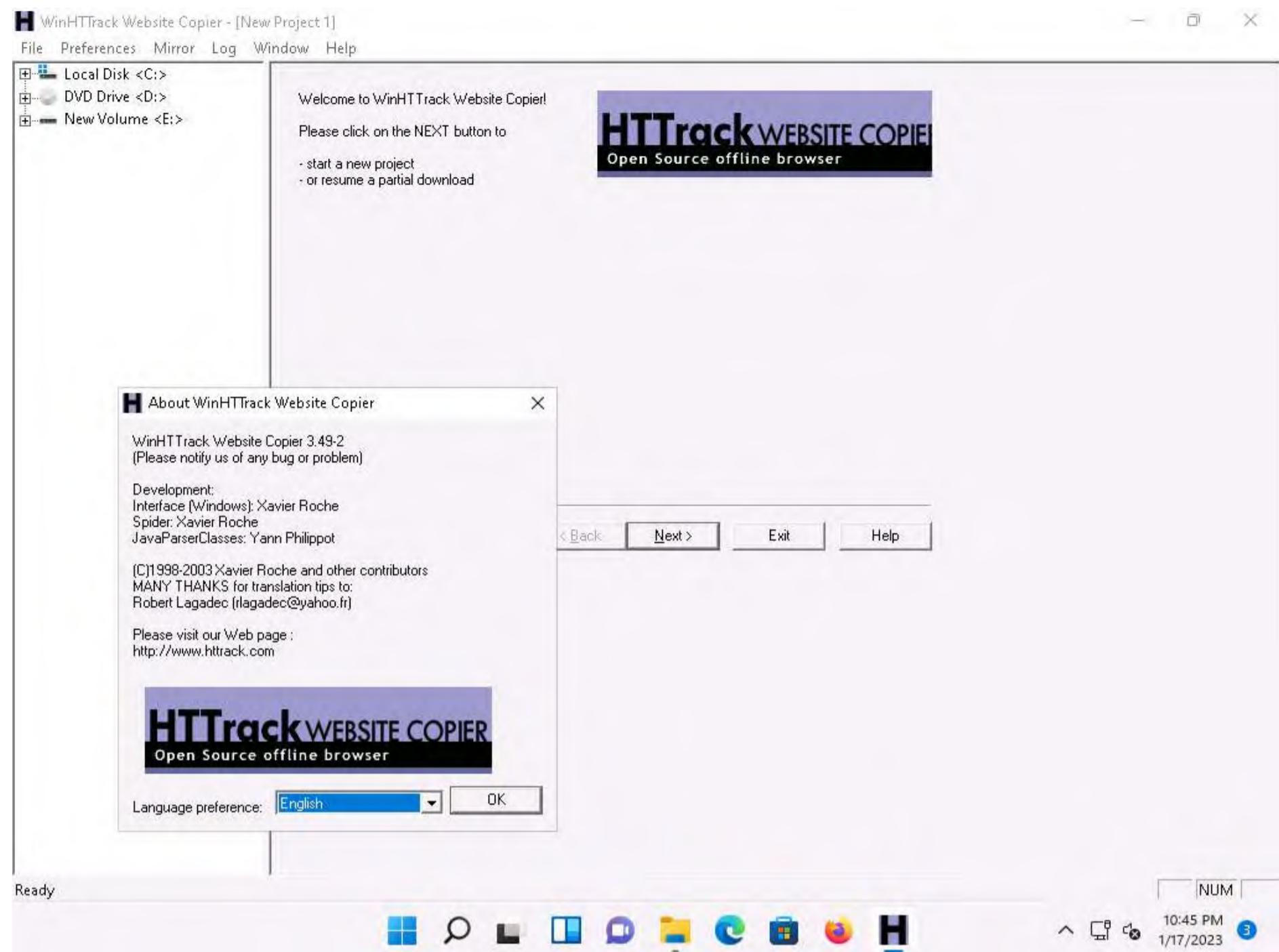
Here, we will use the HTTrack Web Site Copier tool to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

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

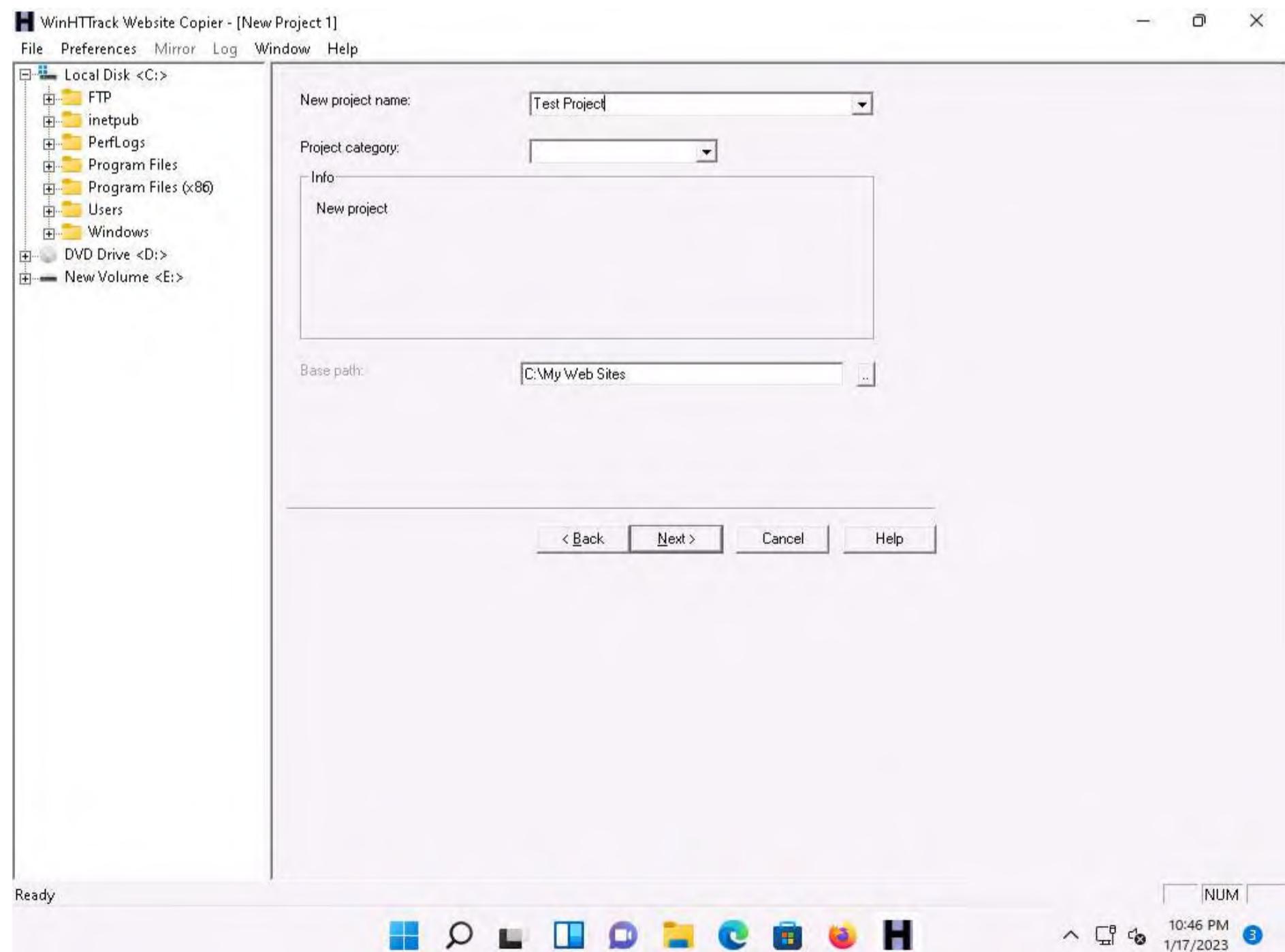
1. In the **Windows 11** machine, click **Search** icon () on the **Desktop** and type **winhtrack** in the search field. The **WinHTTrack Website Copier** appears in the results, click **Open** to launch it.



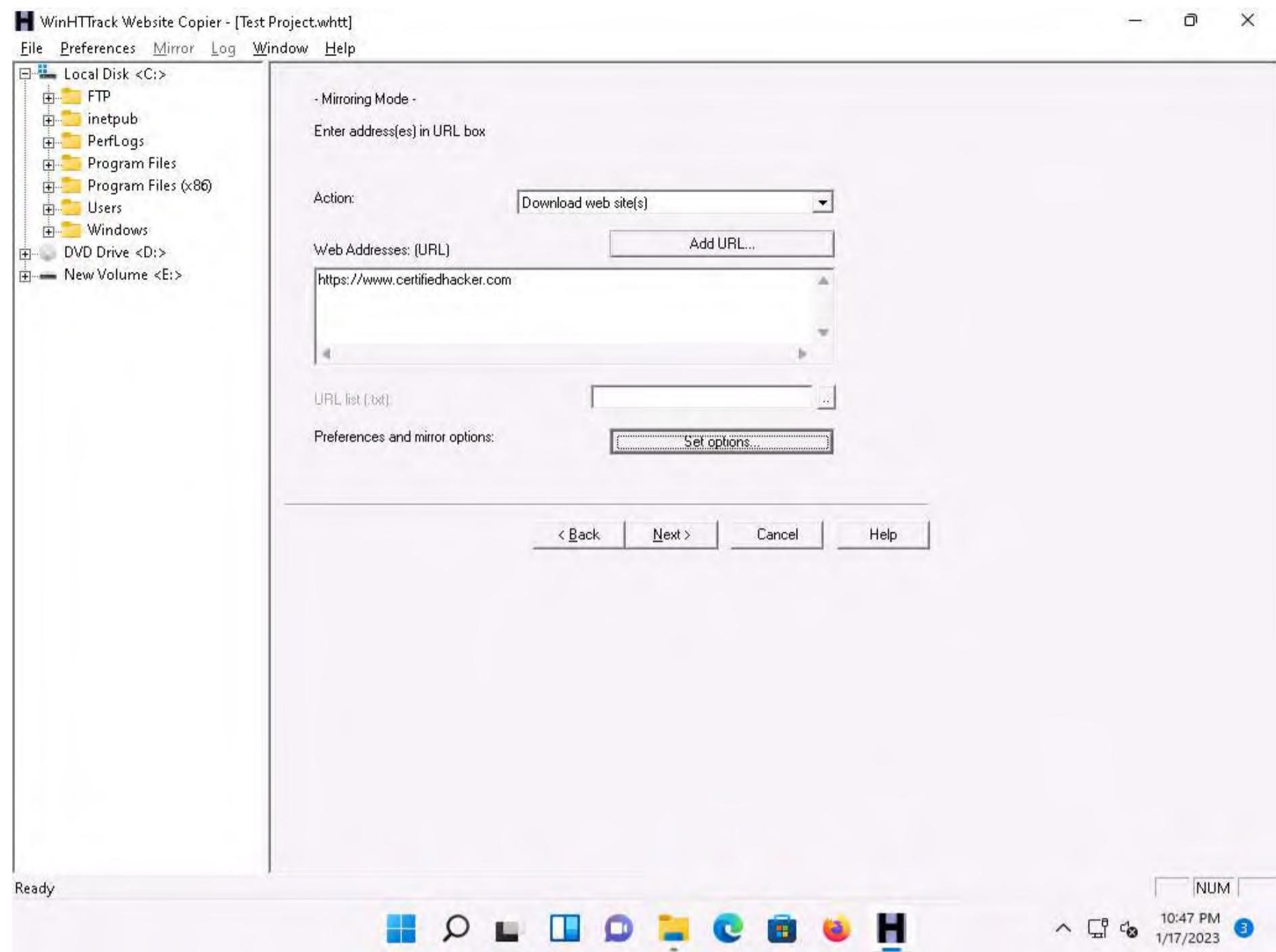
2. The **About WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.



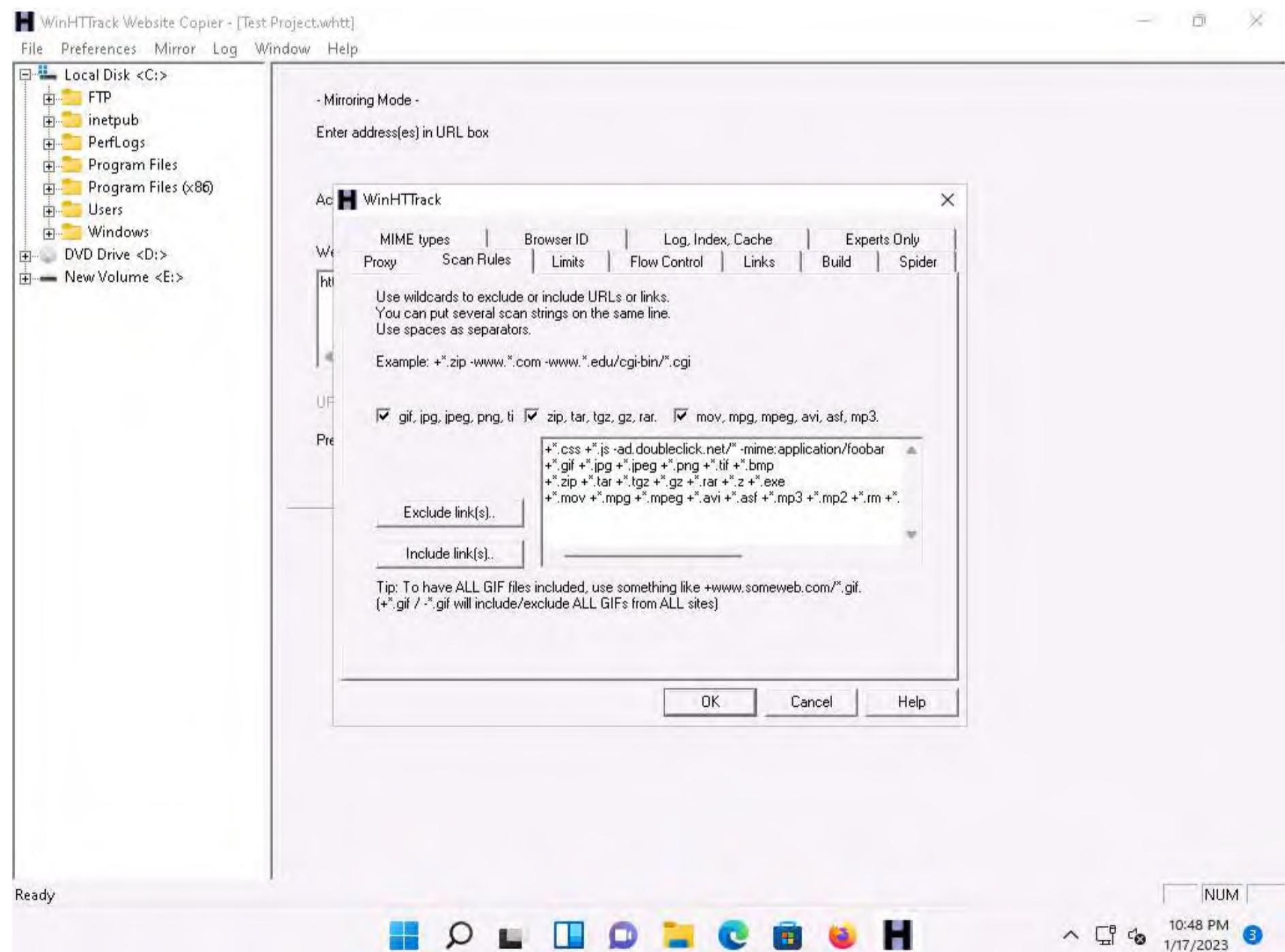
3. Enter the name of the project (here, **Test Project**) in the **New project name:** field. Select the **Base path:** to store the copied files; click **Next >**.



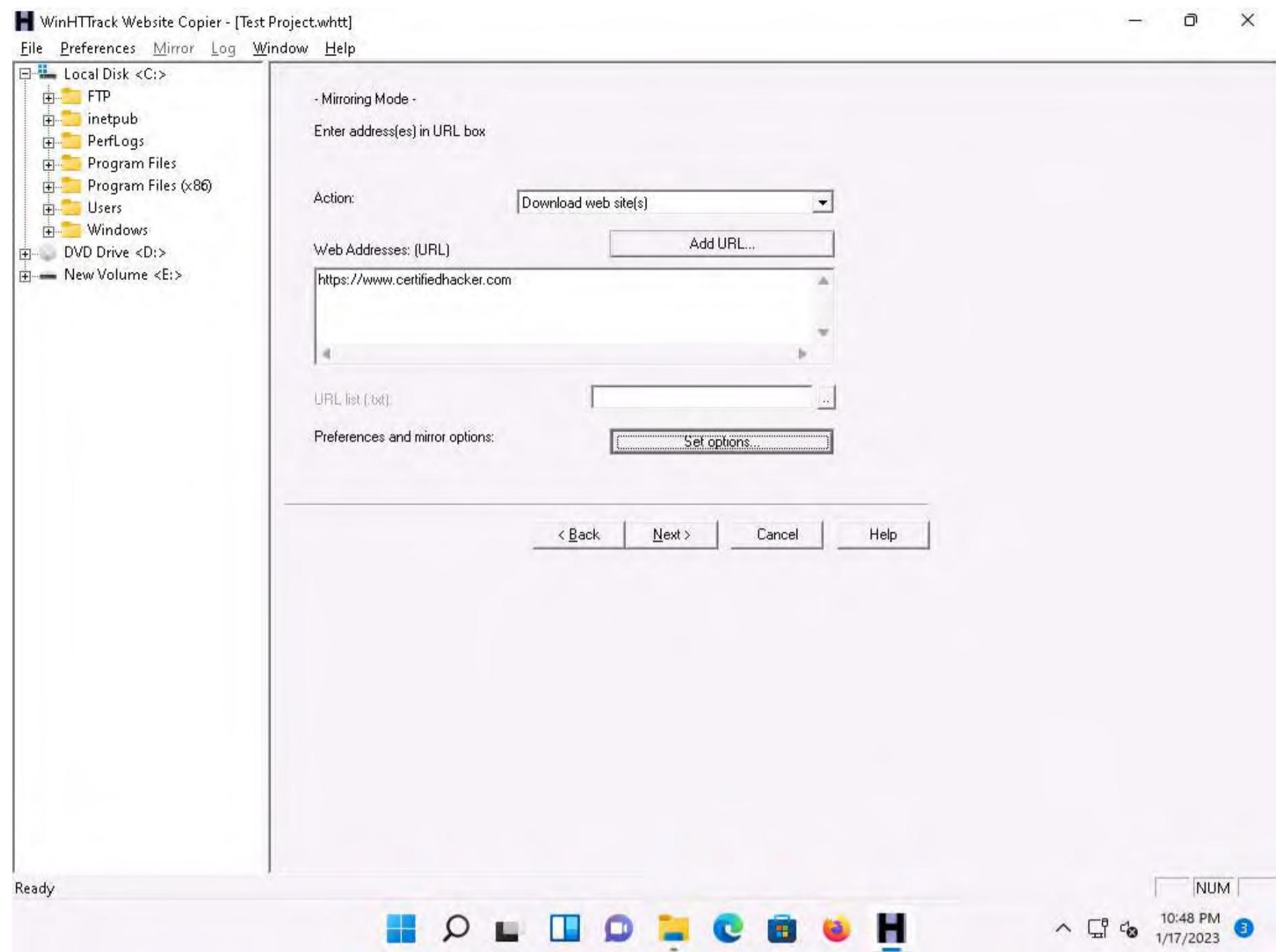
4. Enter a target URL (here, <https://www.certifiedhacker.com>) in the **Web Addresses: (URL)** field and click **Set options...**



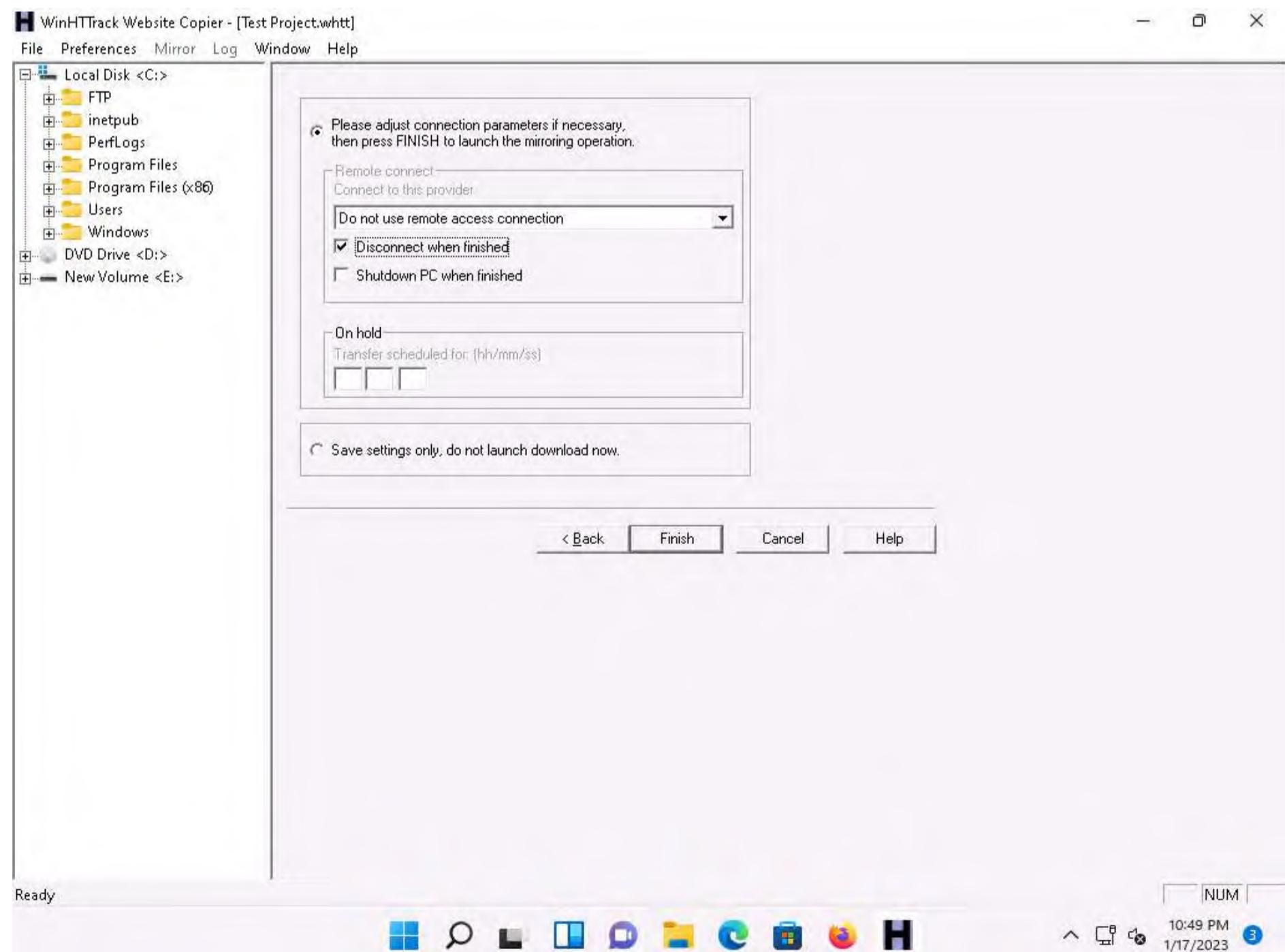
5. WinHTTTrack window appears, click the **Scan Rules** tab and select the checkboxes for the file types as shown in the following screenshot; click **OK**.



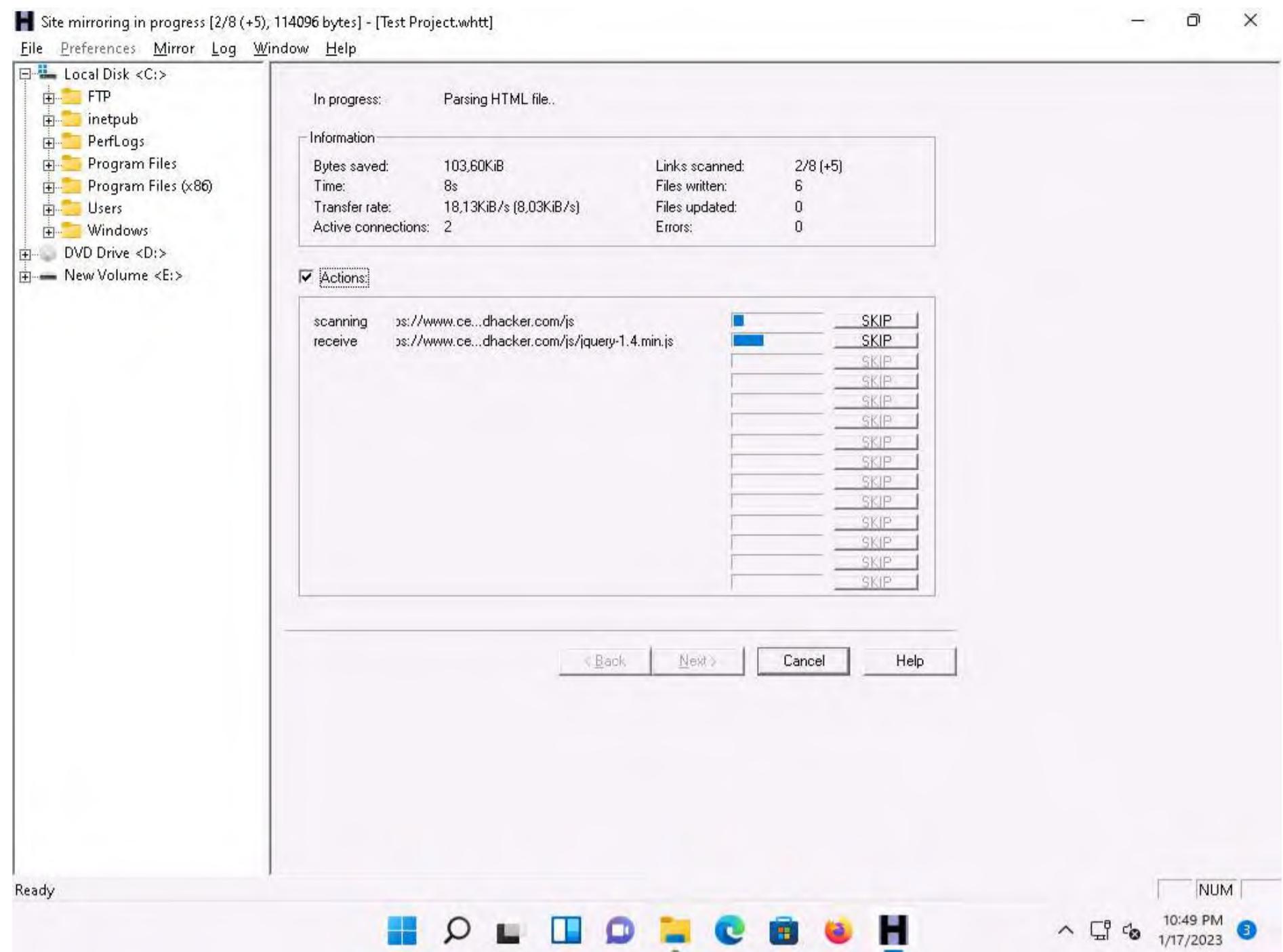
6. Click the **Next >** button.



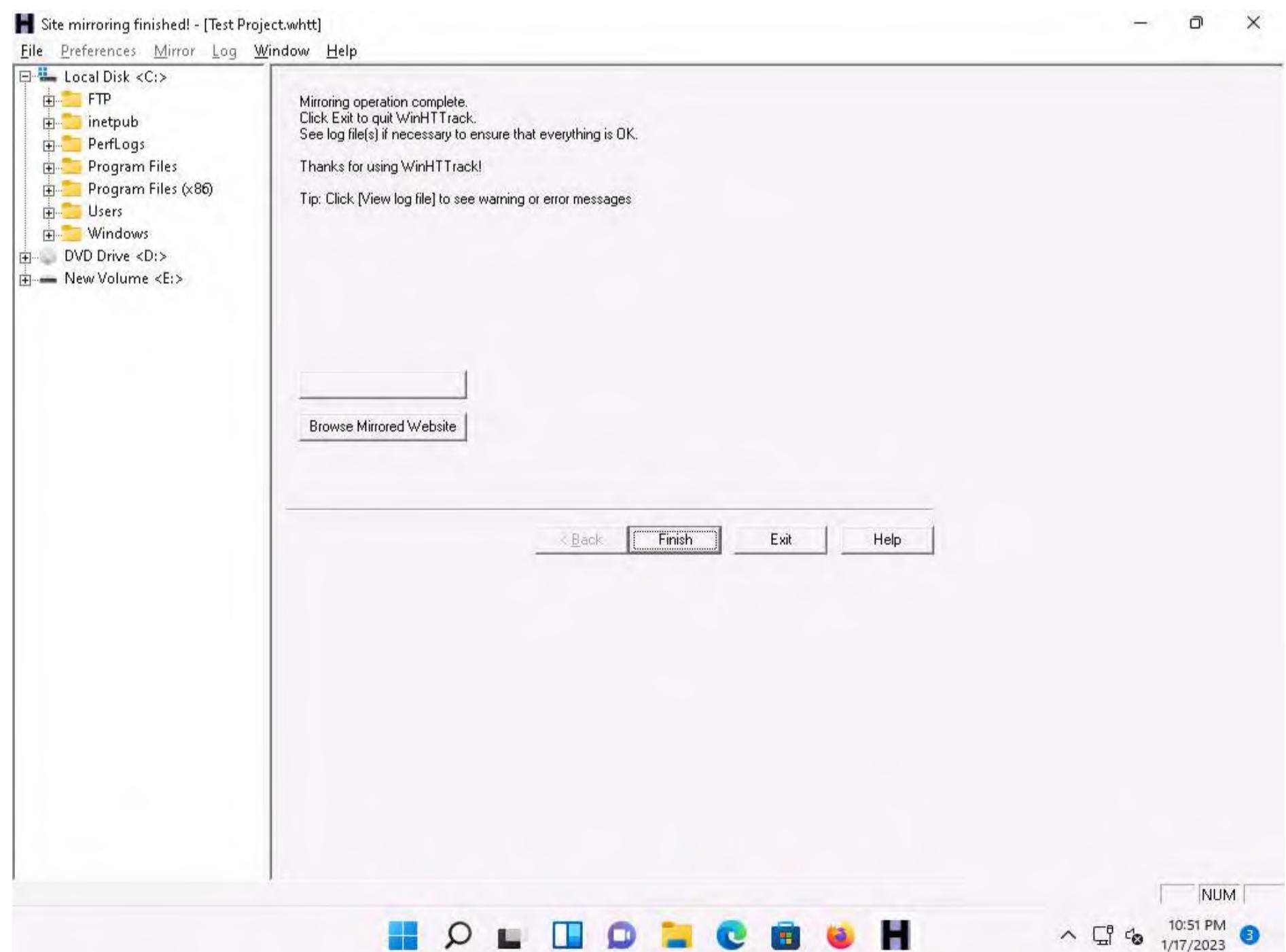
7. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.** Check **Disconnect when finished** and click **Finish** to start mirroring the website.



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

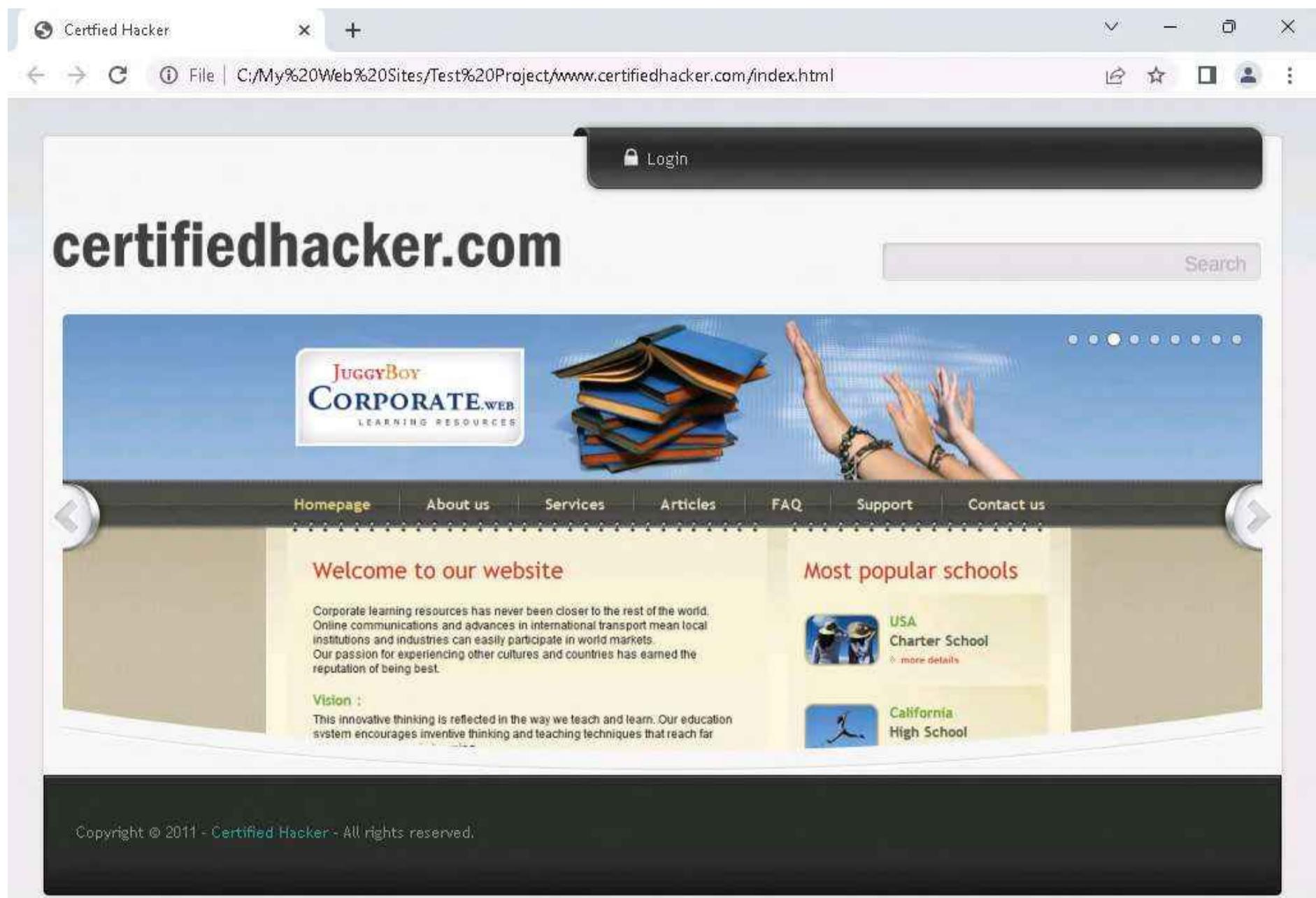


- Once the site mirroring is completed, WinHTTrack displays the message **Mirroring operation complete**; click on **Browse Mirrored Website**.



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

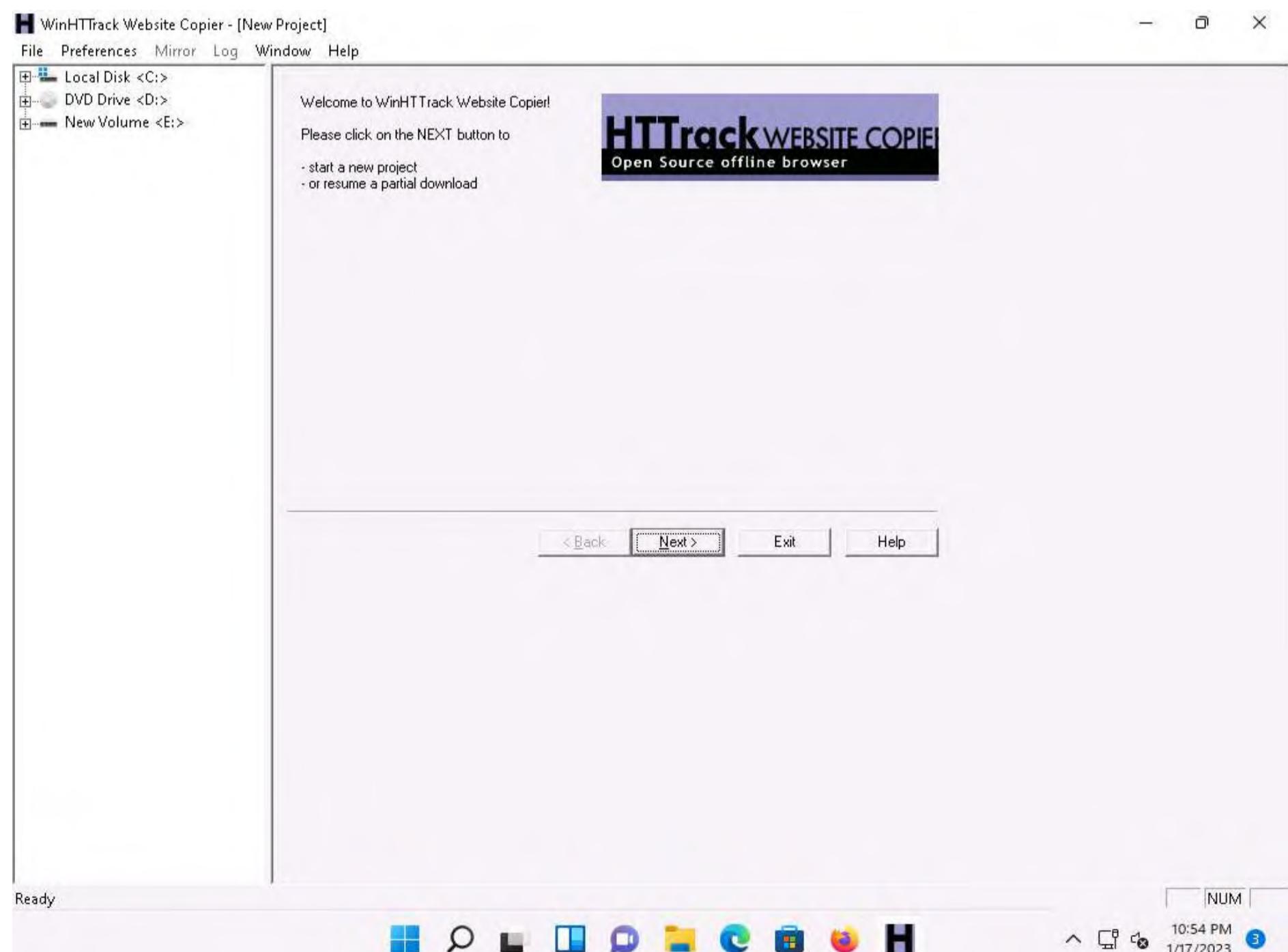
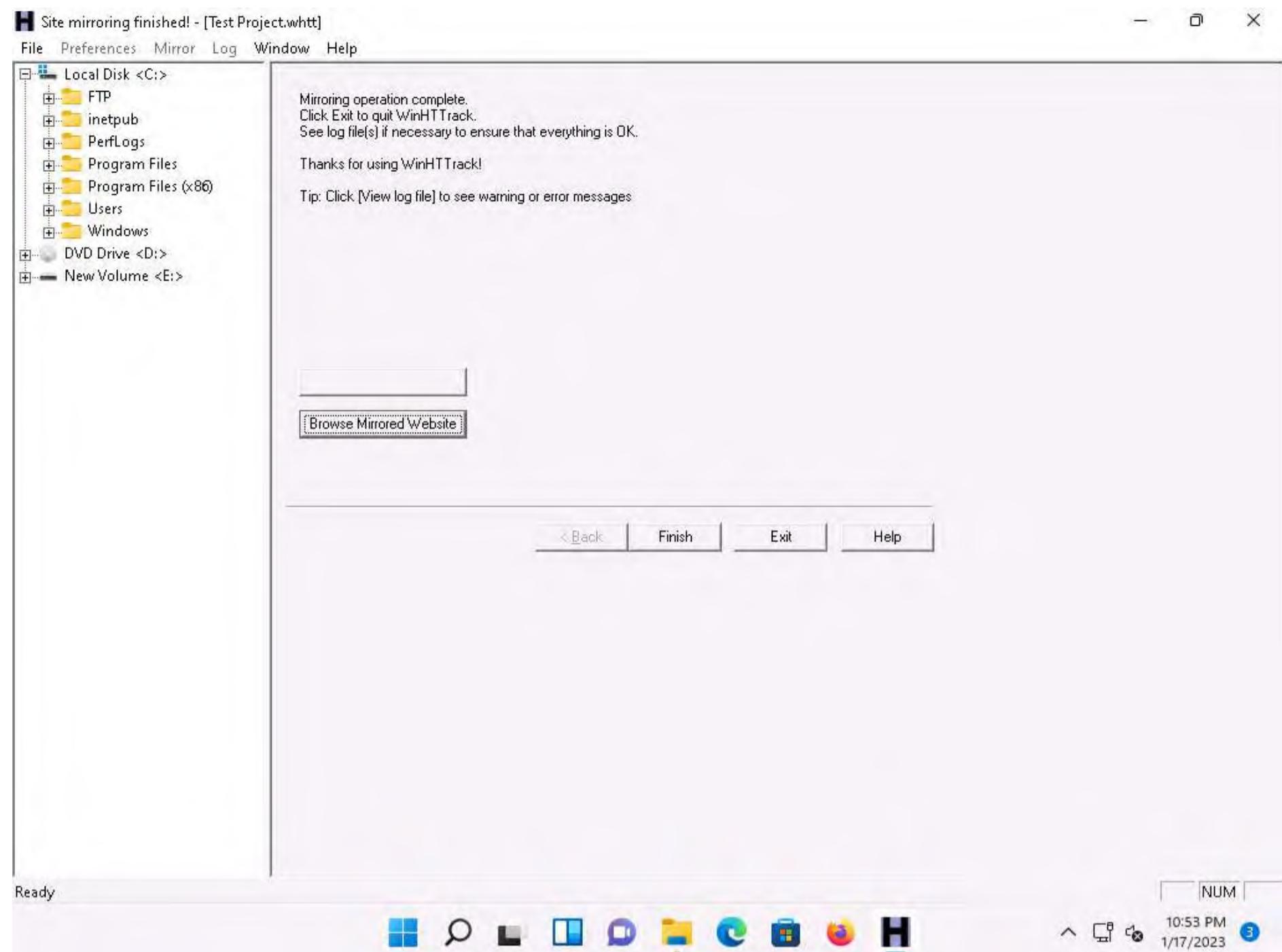
11. The mirrored website for <https://www.certifiedhacker.com> launches. The URL displayed in the address bar indicates that the website's image is stored on the local machine.



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.

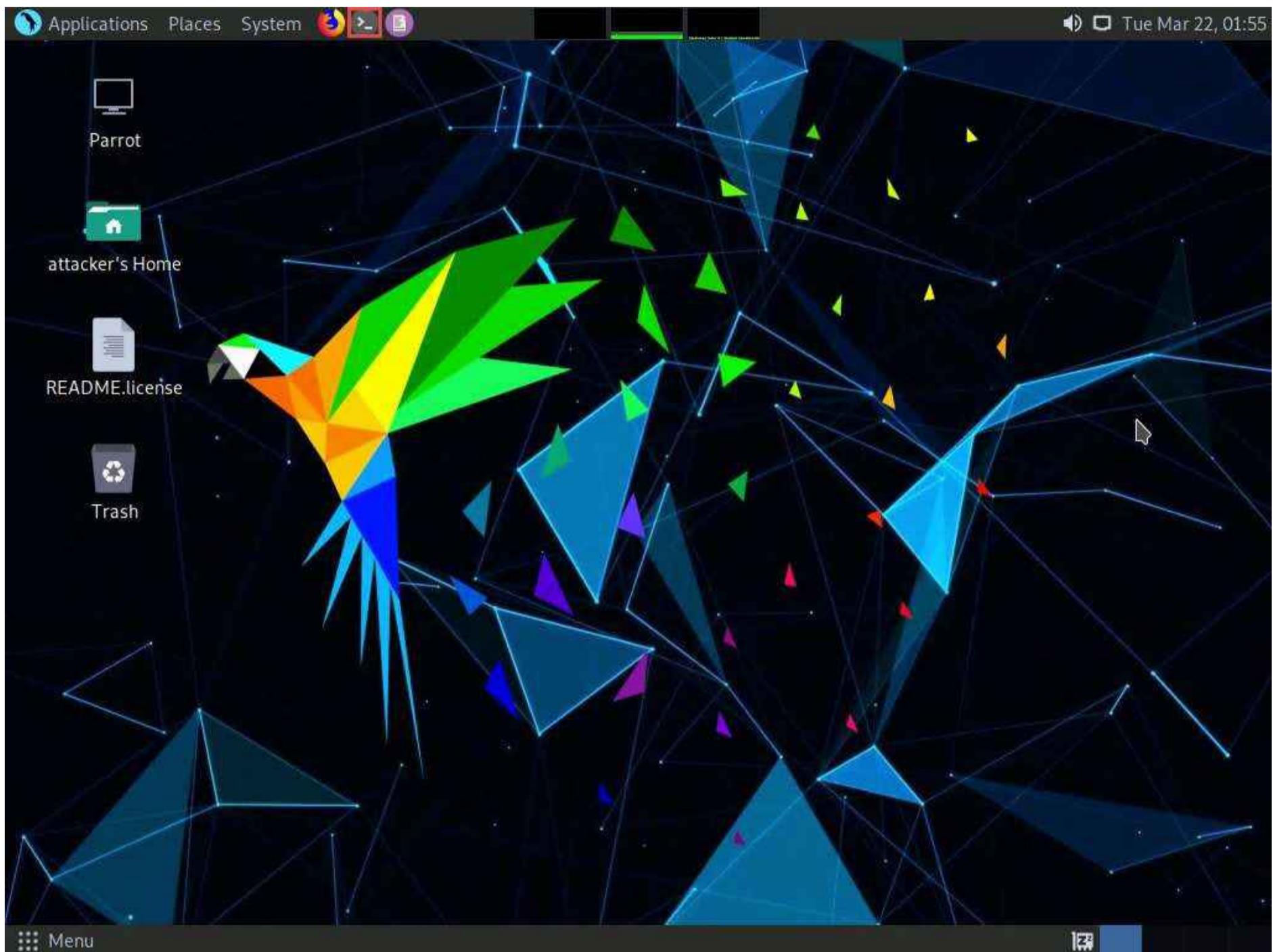
15. The attackers can further use the vulnerabilities identified through **HTTrack Website Copier** to launch various web application attacks on target organization's website.

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.

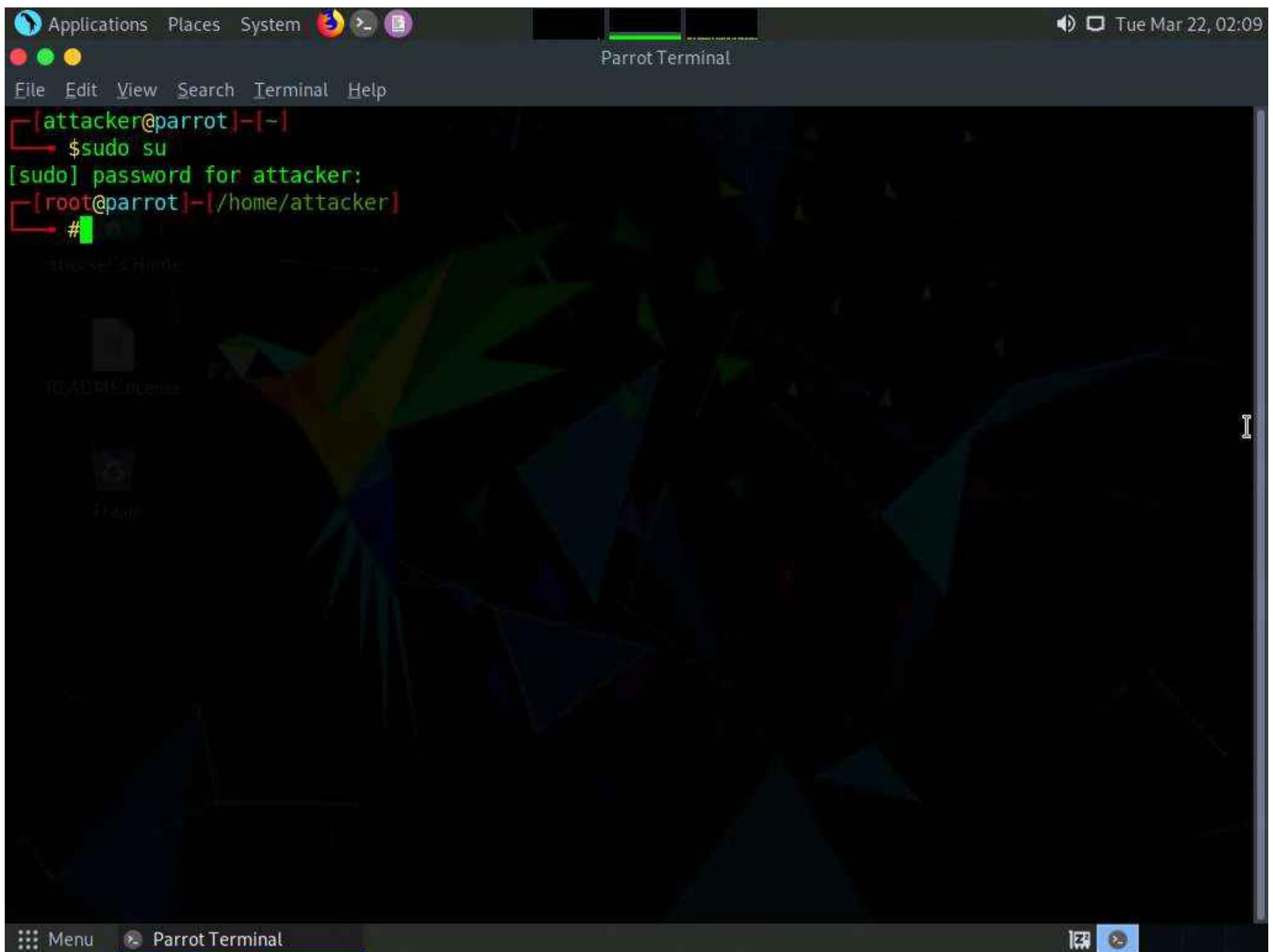
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



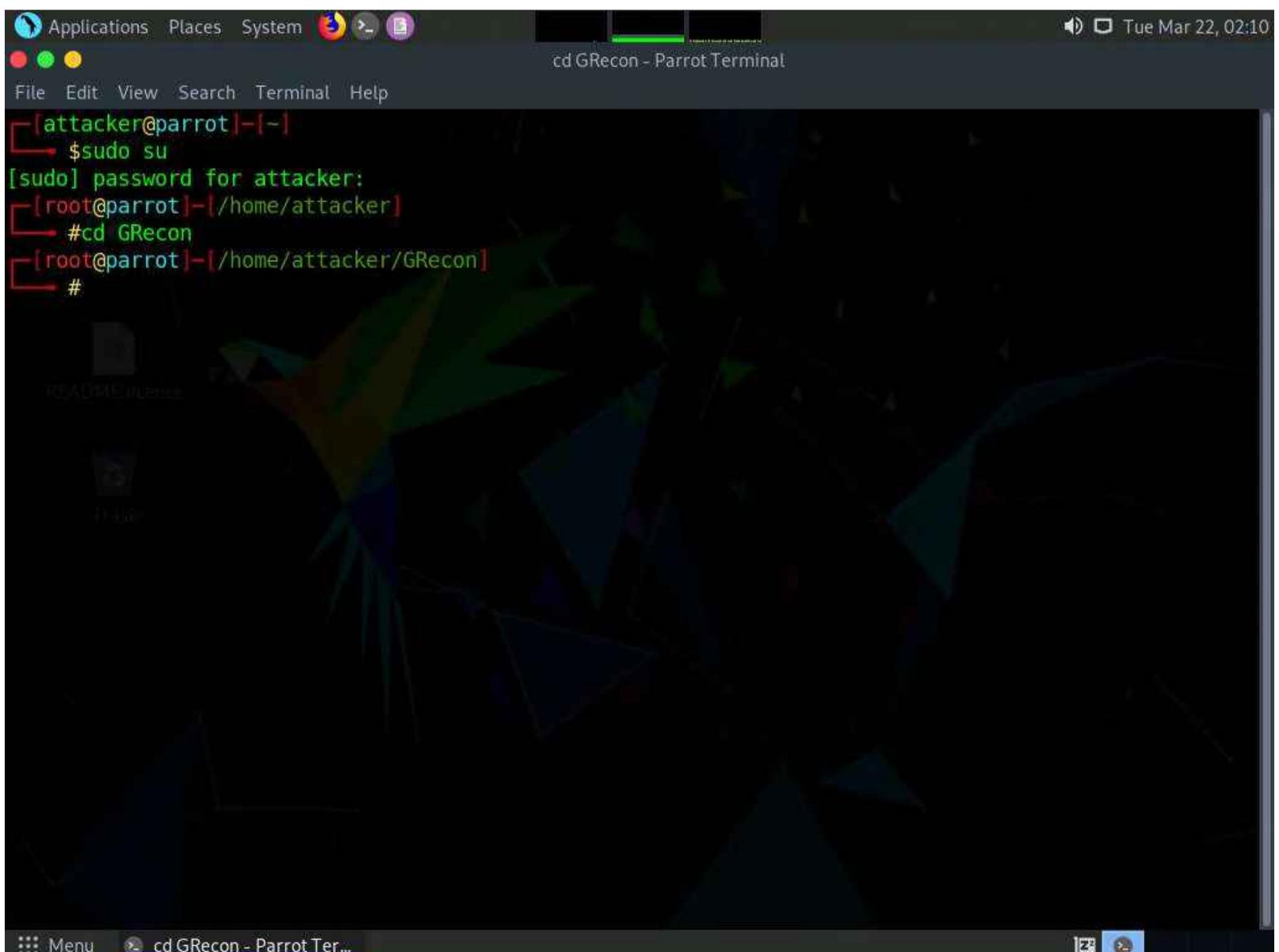
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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**.

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

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

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

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

Current Micro Plugins :

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

GRecon by @TebbaaX (Adnane)

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

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

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

```

Applications Places System python3 grecon.py - Parrot Terminal
File Edit View Search Terminal Help
python3 grecon.py - Parrot Terminal
GRecon by @TebbaaX (Adnane)
[+] Set Target (site.com) : certifiedhacker.com
[>] Looking For Subdomains...
http://certifiedhacker.com/
https://www.certifiedhacker.com/
https://www.news.certifiedhacker.com/
https://www.fleet.certifiedhacker.com/
https://www.itf.certifiedhacker.com/
https://www.blog.certifiedhacker.com/
https://www.soc.certifiedhacker.com/
https://www.sftp.certifiedhacker.com/
[>] Looking For Sub-Subdomains...
[>] Looking For Login/Signup Pages...
http://certifiedhacker.com/Social%20Media/sample-login.html
[!] 20s Sleep to avoid Google Block
[!] Switching Google TLDs...
[>] Looking For Directory Listing...
https://www.news.certifiedhacker.com/
https://www.soc.certifiedhacker.com/
https://www.sftp.certifiedhacker.com/
https://www.itf.certifiedhacker.com/
https://www.certifiedhacker.com/css/source/

```

```

Applications Places System python3 grecon.py - Parrot Terminal
File Edit View Search Terminal Help
python3 grecon.py - Parrot Terminal
[>] Looking For Login/Signup Pages...
http://certifiedhacker.com/Social%20Media/sample-login.html
[!] 20s Sleep to avoid Google Block
[!] Switching Google TLDs...
[>] Looking For Directory Listing...
https://www.news.certifiedhacker.com/
https://www.soc.certifiedhacker.com/
https://www.sftp.certifiedhacker.com/
https://www.itf.certifiedhacker.com/
https://www.certifiedhacker.com/css/source/
https://www.certifiedhacker.com/css/
https://www.certifiedhacker.com/css/skins/
https://www.blog.certifiedhacker.com/
https://www.fleet.certifiedhacker.com/
[>] Looking For Public Exposed Documents...
http://certifiedhacker.com/docs/923332.pdf
[>] Looking For WordPress Entries...
[>] Looking in Pasting Sites...
https://pastebin.com/xv8beZRc
https://pastebin.com/Smiaterl
[>] Done...Happy Hunting
[root@parrot]# /home/attacker/GRecon

```

9. Attackers can further use the gathered information to perform various web application attacks on the target website.

10. This concludes the demonstration of gathering information about a target website using GRecon.

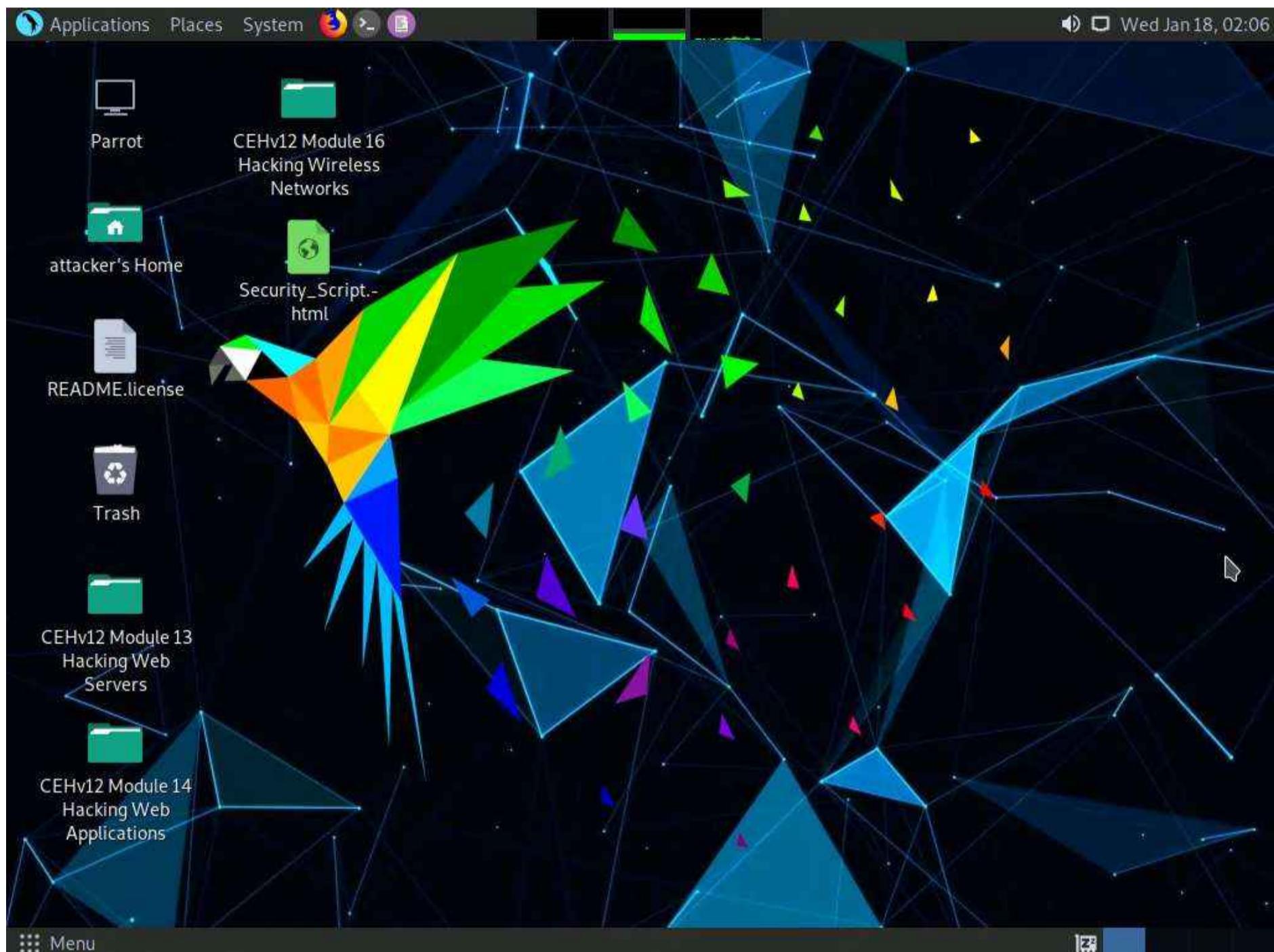
11. Close all open windows and document all the acquired information.

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

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

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

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

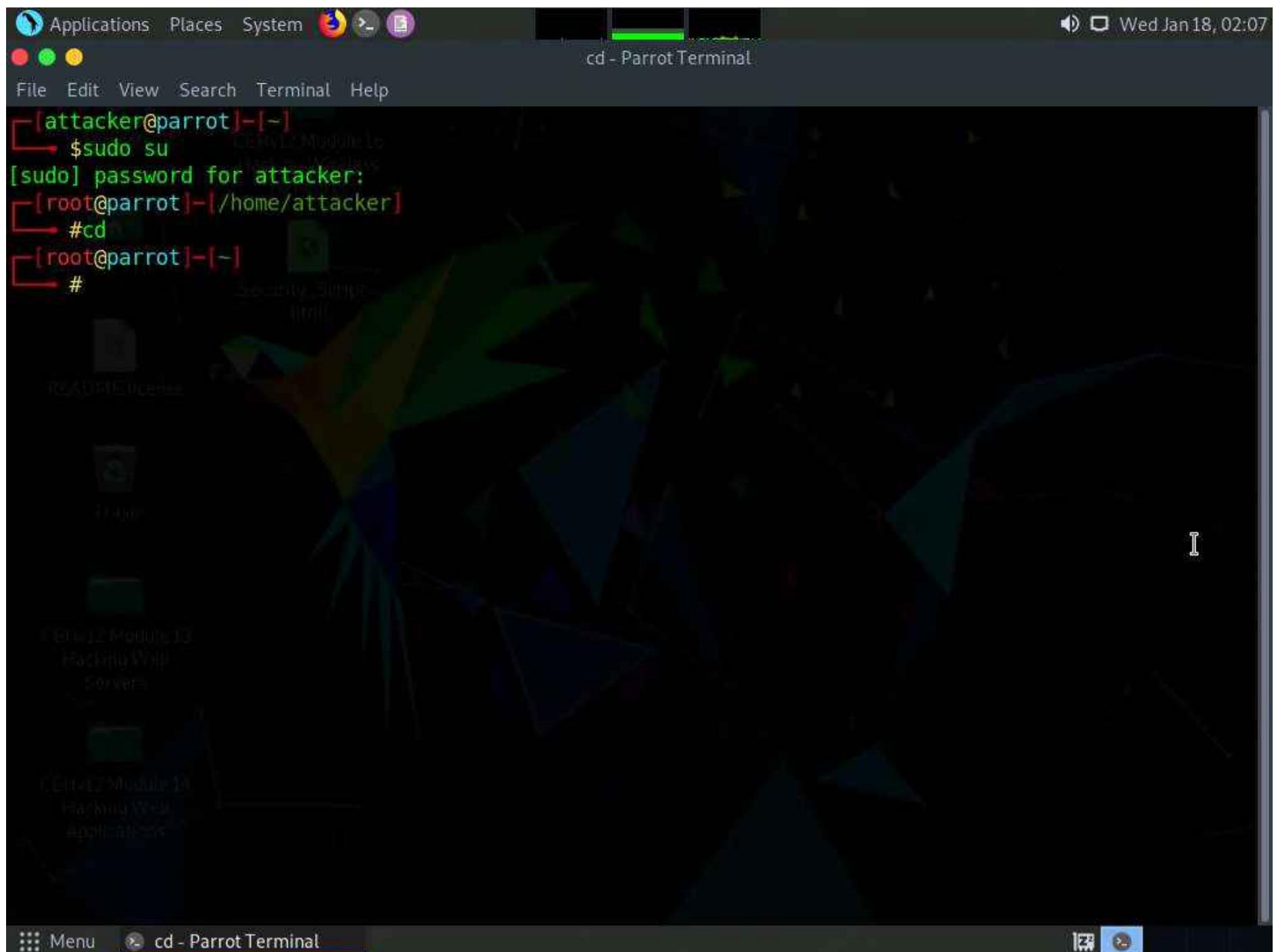


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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.

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
#cd
[root@parrot] ~
# cewl -d 2 -m 5 https://www.certifiedhacker.com
CewL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

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**)



```

cewl -w wordlist.txt -d 2 -m 5 https://www.certifiedhacker.com - Parrot Terminal
[...]
Column
Certified
rights
reserved
legal
Activate
Replacement
brief
description
website
business
keywords
phrases
associated
requested
found
server
Additionally
error
encountered
while
trying
ErrorDocument
handle
request
[root@parrot]~[-]
#cewl -w wordlist.txt -d 2 -m 5 https://www.certifiedhacker.com
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
[root@parrot]~[-]
#

```

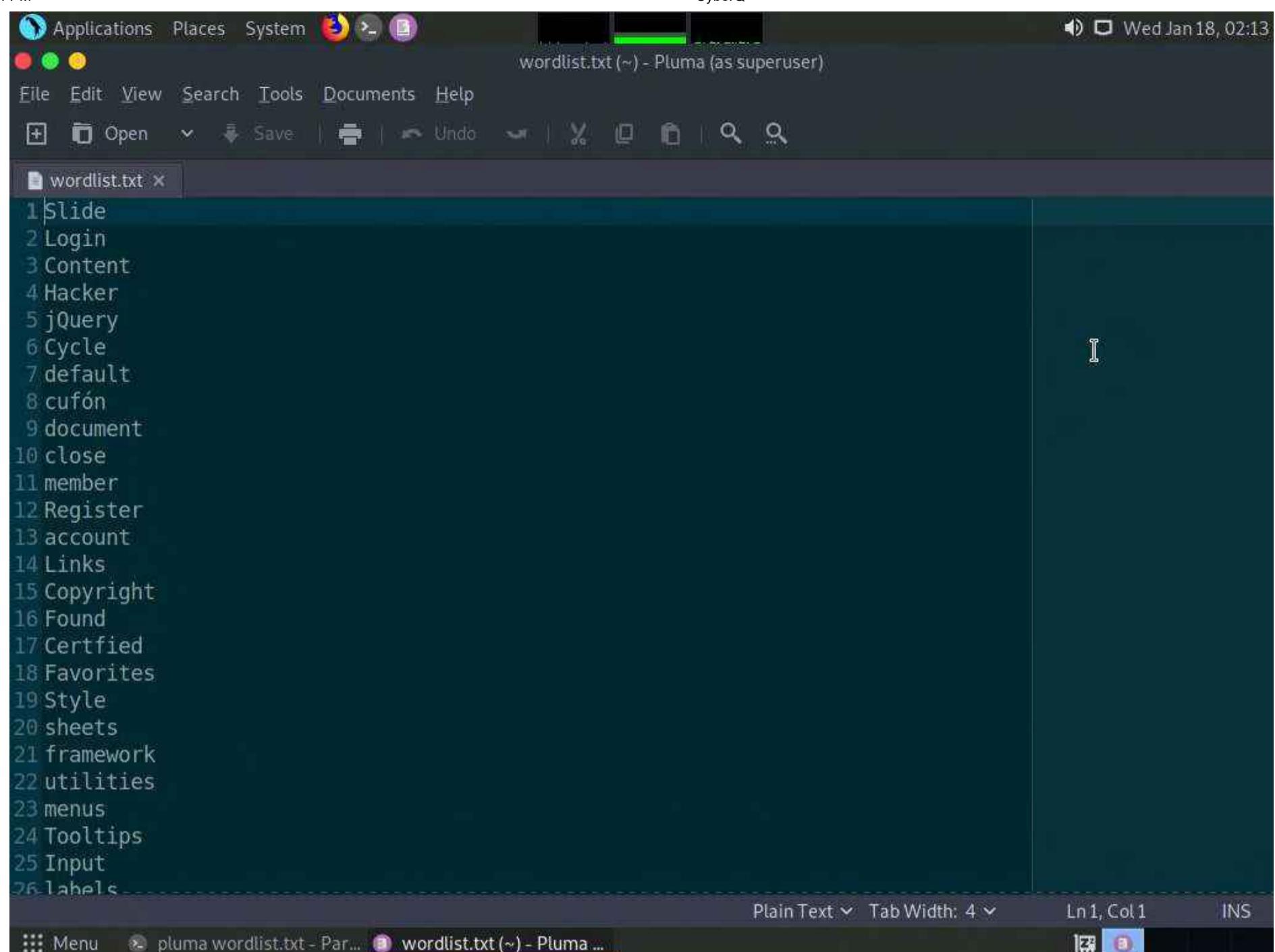
8. By default, the wordlist file gets saved in the **root** directory. Type **pluma wordlist.txt** and press **Enter** to view the extracted wordlist.

```

cewl -w wordlist.txt -d 2 -m 5 https://www.certifiedhacker.com - Parrot Terminal
[...]
Column
Certified
rights
reserved
legal
Activate
Replacement
brief
description
website
business
keywords
phrases
associated
requested
found
server
Additionally
error
encountered
while
trying
ErrorDocument
handle
request
[root@parrot]~[-]
#cewl -w wordlist.txt -d 2 -m 5 https://www.certifiedhacker.com
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
[root@parrot]~[-]
#pluma wordlist.txt

```

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



```

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

```

Plain Text ▾ Tab Width: 4 ▾

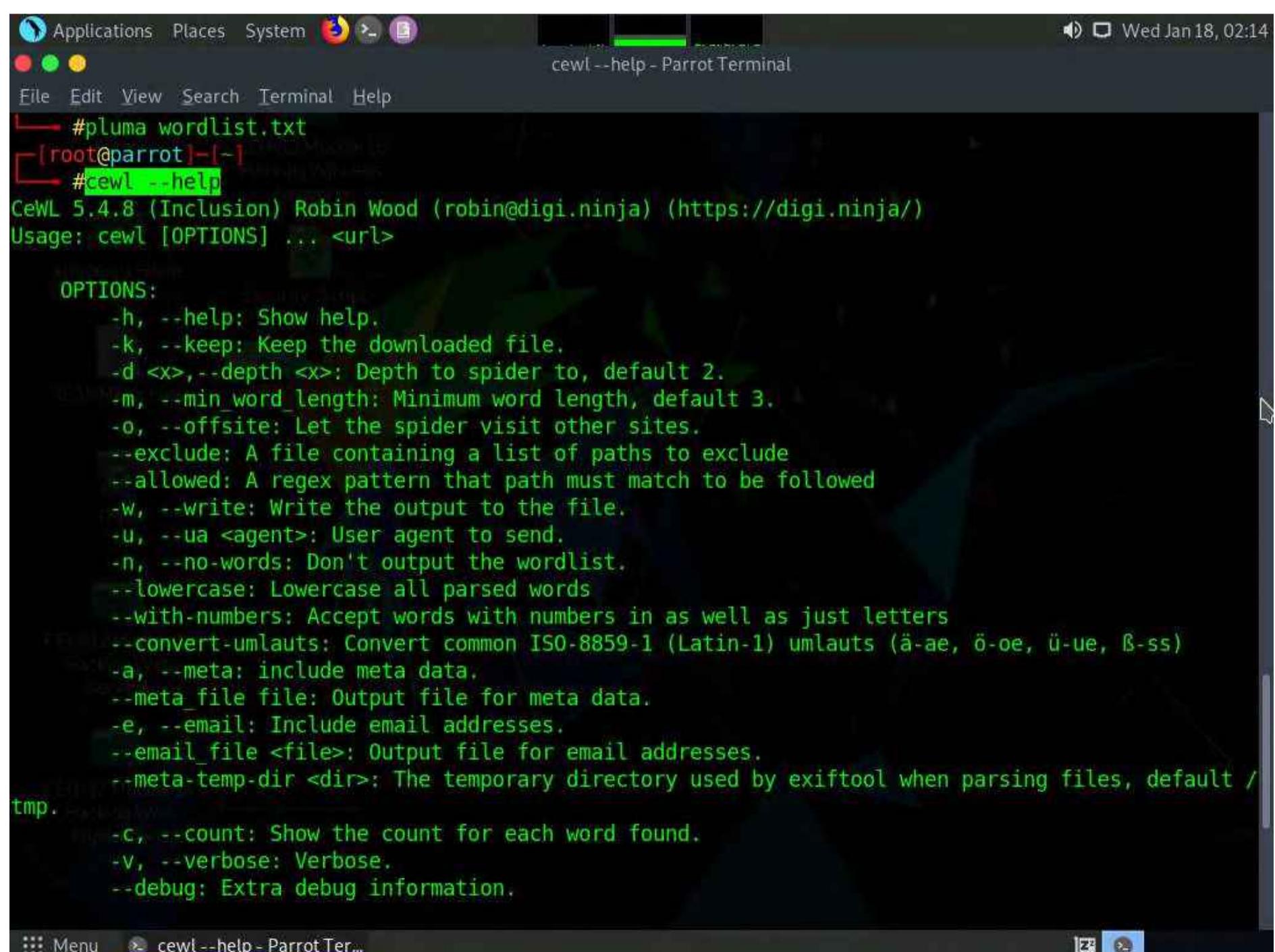
Ln 1, Col 1

INS

Menu pluma wordlist.txt - Par...



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



```

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

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

```

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

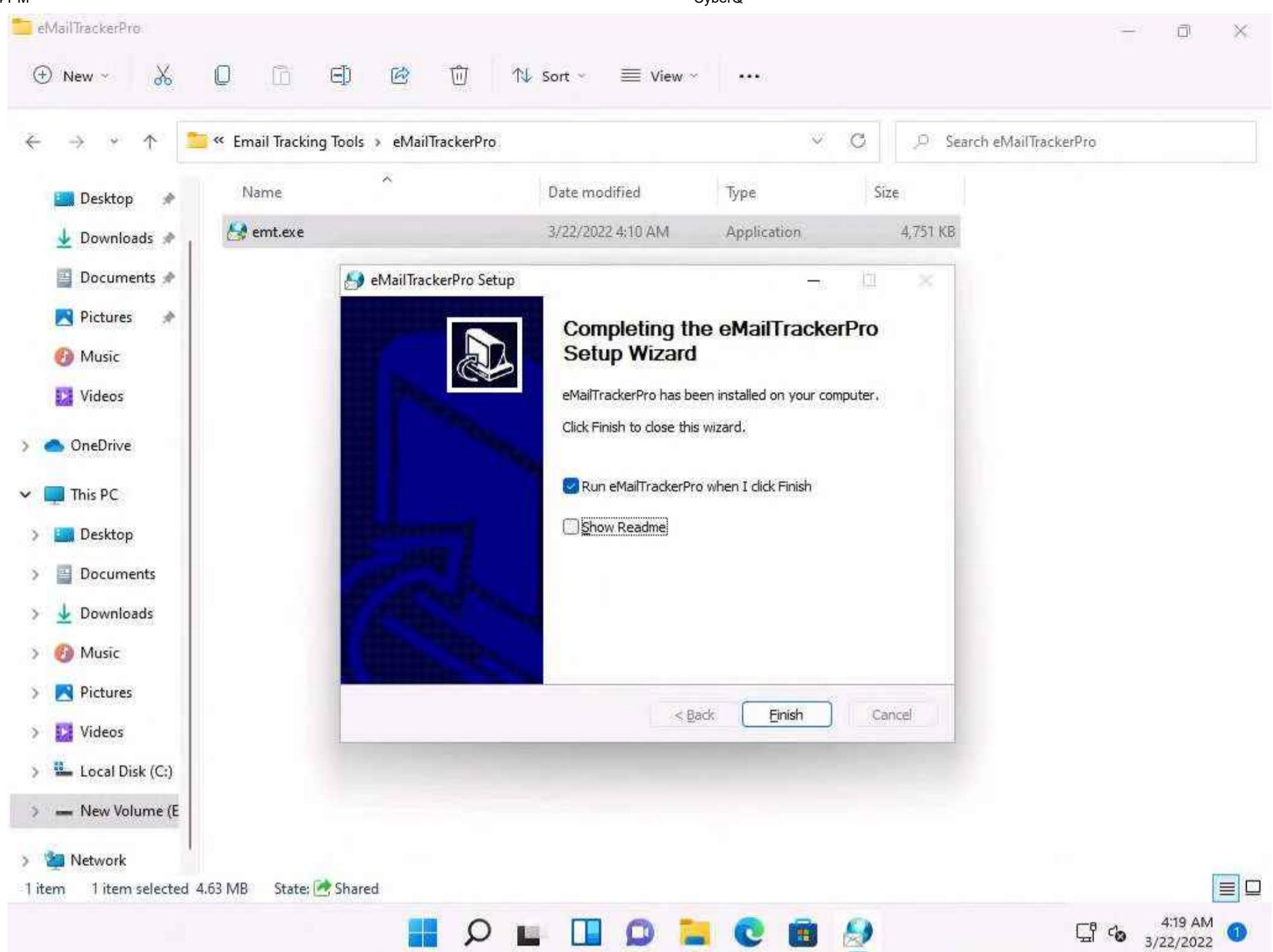
Task 1: Gather Information about a Target by Tracing Emails using eMailTrackerPro

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.

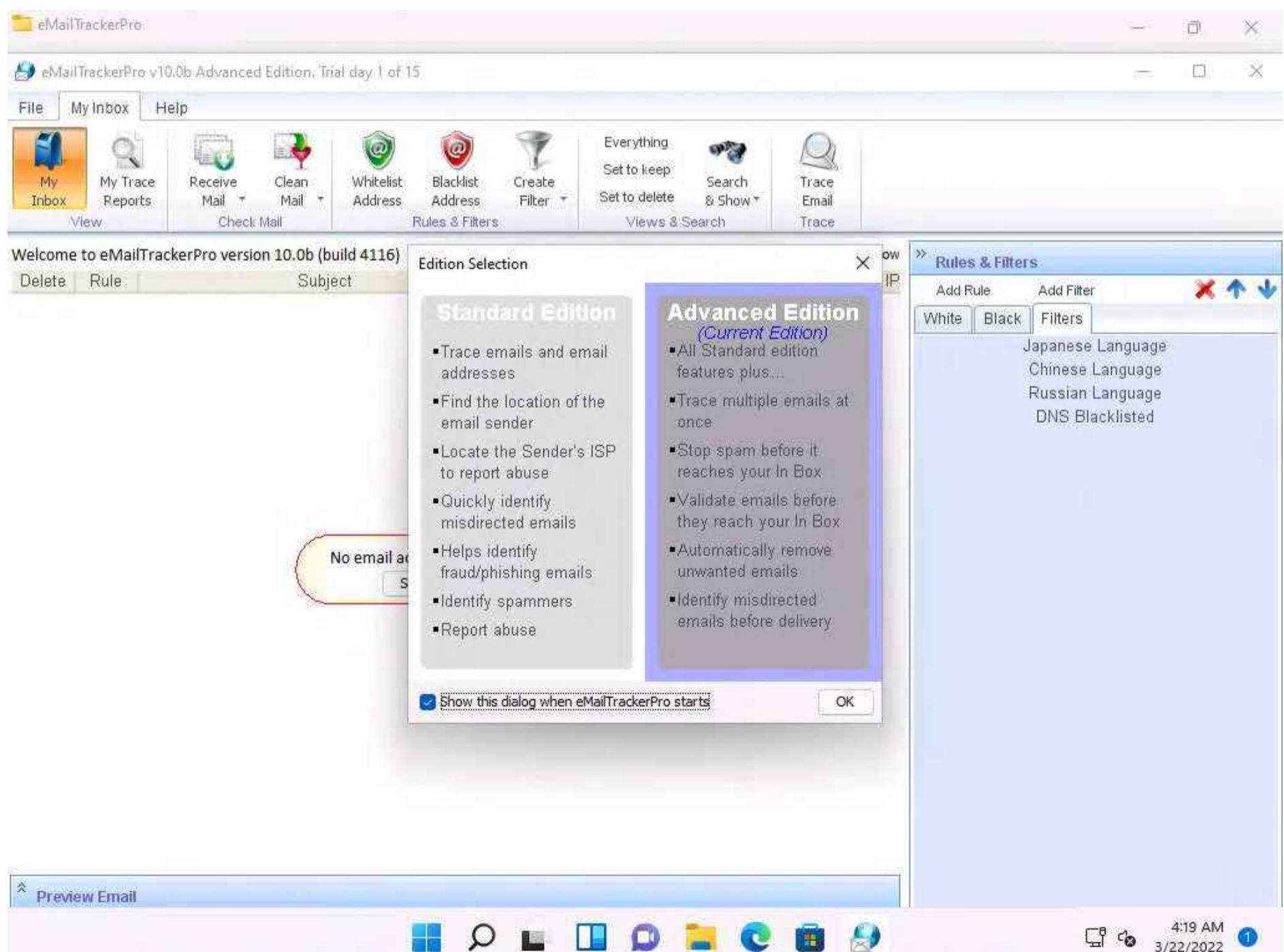
Here, we will gather information by analyzing the email header using eMailTrackerPro.

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.

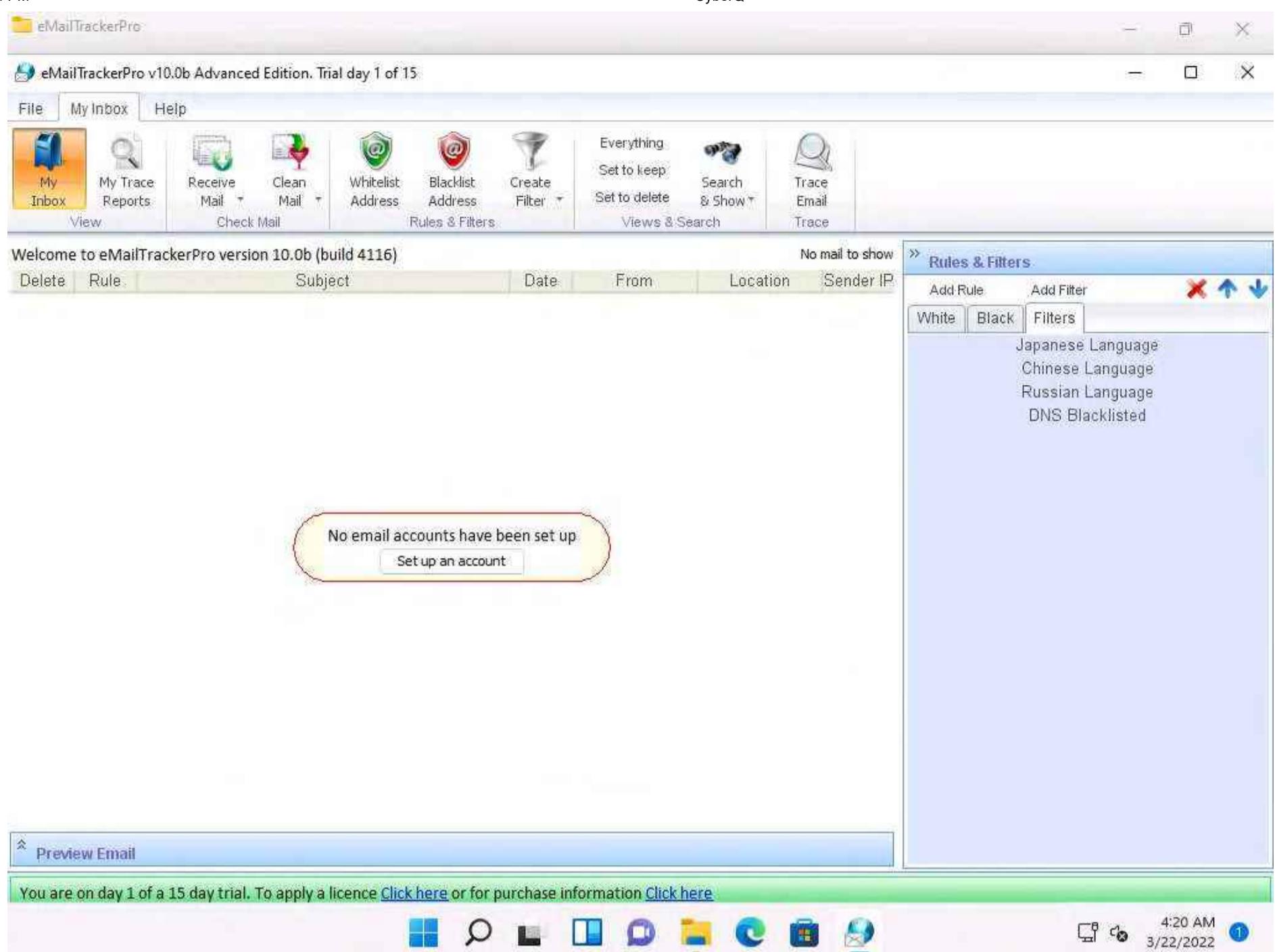




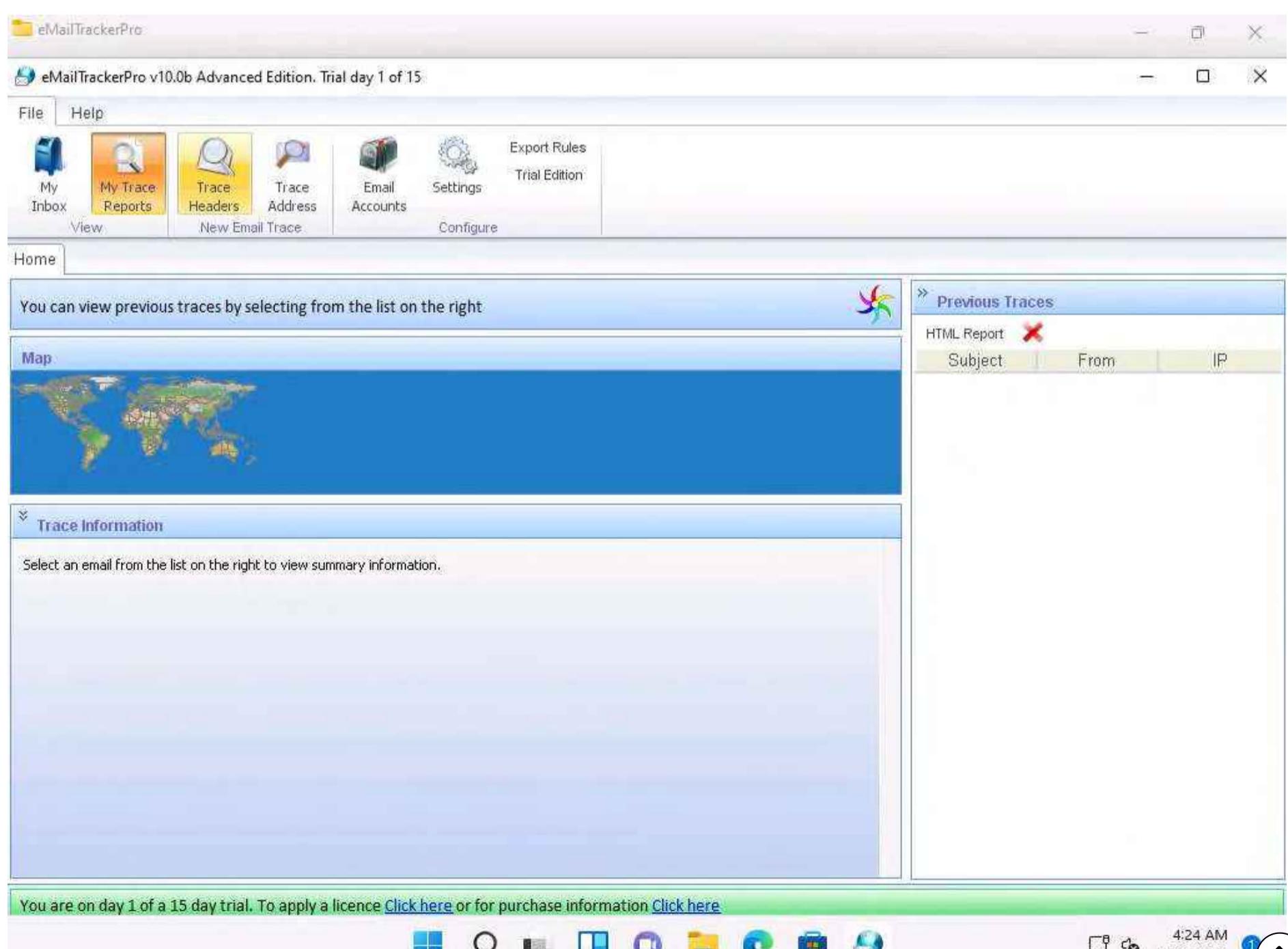
5. The main window of eMailTrackerPro appears along with the Edition Selection pop-up; click OK.



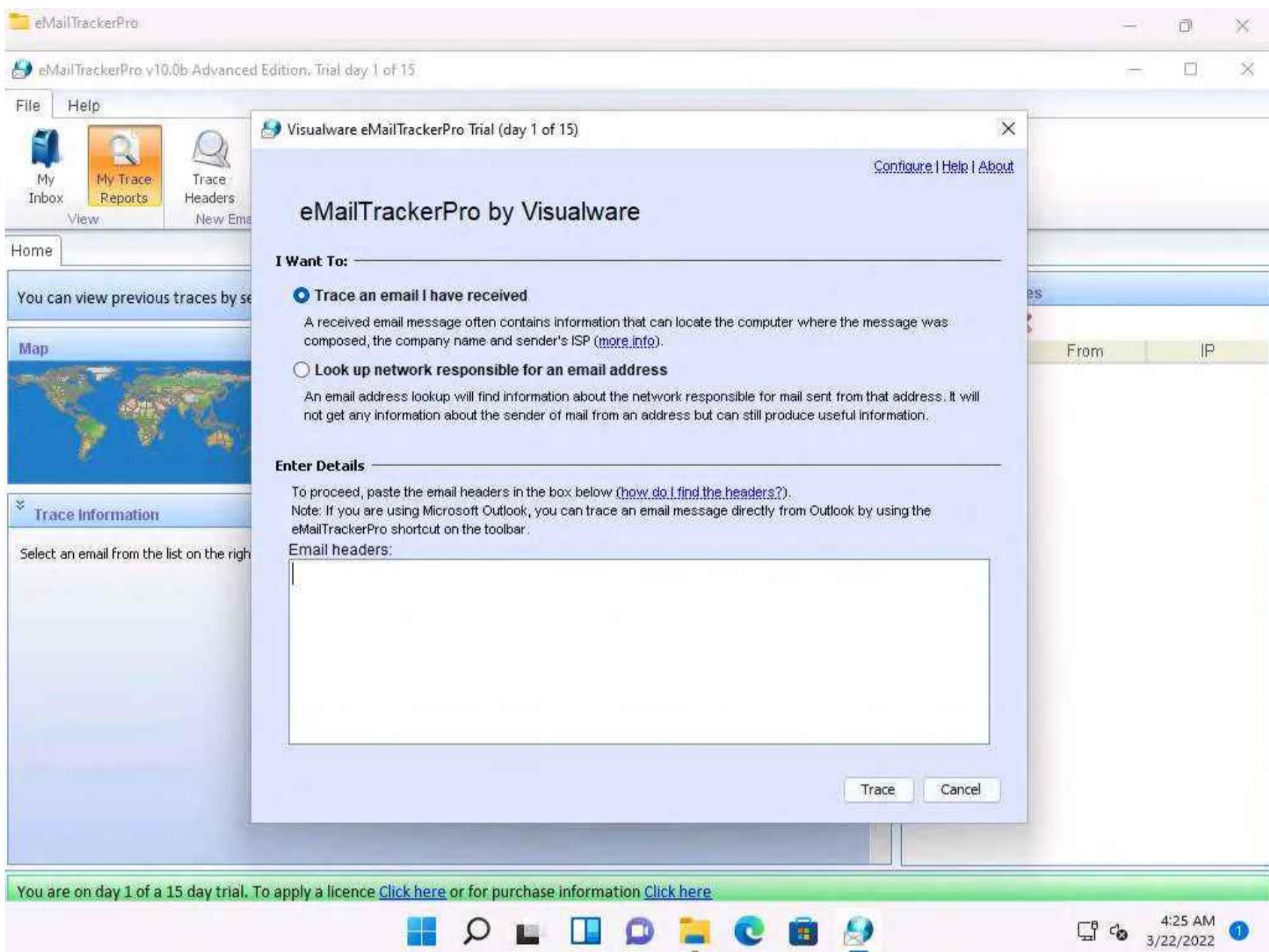
6. The eMailTrackerPro main window appears, as shown in the screenshot.



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

Message ID:	<SAPgrqAYQzuu5t1bWdVbIA@geopod-isnmpd-2-2>
Created on:	(Delivered after 1 second)
From:	[REDACTED].com>
To:	[REDACTED]@gmail.com>
Subject:	Please verify your [REDACTED]
SPF:	PASS with IP 149.72.138.96. Learn more
DKIM:	'PASS' with domain securitytrails.com. Learn more
DMARC:	'PASS' Learn more

[Download original](#) [Copy to clipboard](#)

```

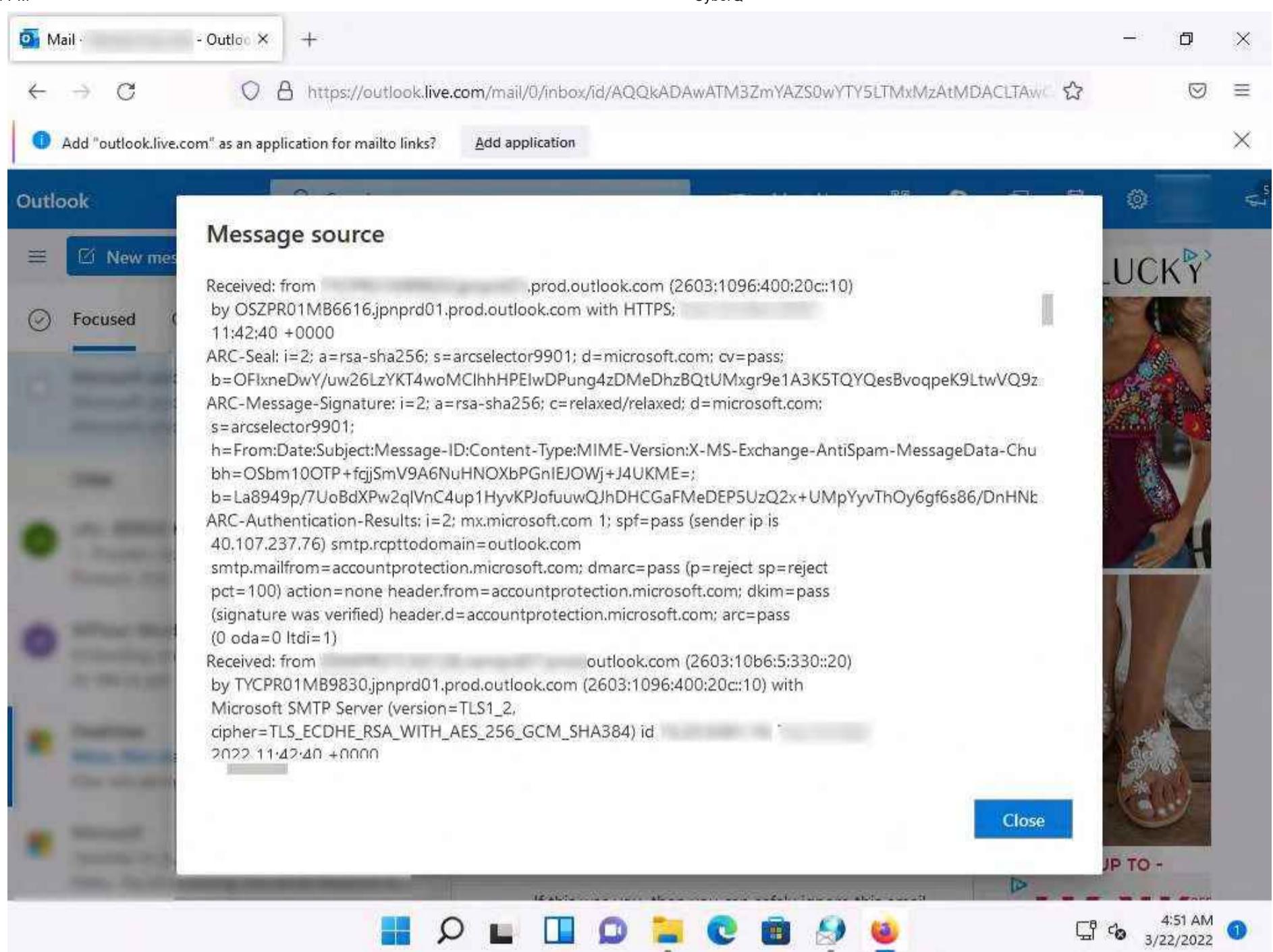
Delivered-To: [REDACTED]@gmail.com
Received: by 2002:a05:7300:1914:b0:59:3d0c:54f with SMTP id n20csp266096dyk;
      Tue, :34:46 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyBCNKG3SUwwEE+SzCUEhSEzDYcJ4WUo46iaM71dw9W2b9k0BEyMkkpPrAjU+pW2n57CXWQ
X-Received: by 2002:a17:902:dacl:b0:154:3d0e:9c5b with SMTP id q1-20020a170902dac100b001543d069c5bmr13633808pix.98.1647941685882;
      Tue, -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1647941685; cv=none;
d=google.com; s=arc-20160816;
b=eCM/AbM715+3y6dQrQb0ijswr/KcKfN6crBnopTRBLxltkZ0stU+ttppgEMp4UQynppR
nMbTs+sWmbPYi+1cTDFQlcff01Bkm+qE3Funil9SqdEmAcumNprmo1lwLaSVfc3u6PVt
sXpqzVyQMhww9/e8mGfpArdQkABeF8CoKaM261x023LARqy3UcdYMIjp1O8wW3WYmrVu
QSJE5NuwfEZHoBAhOzF63j0UBvtgAajByJg29Y47V2vEdApxinHEH/FG9Op/LYJLs9m

```

4:33 AM
3/22/2022

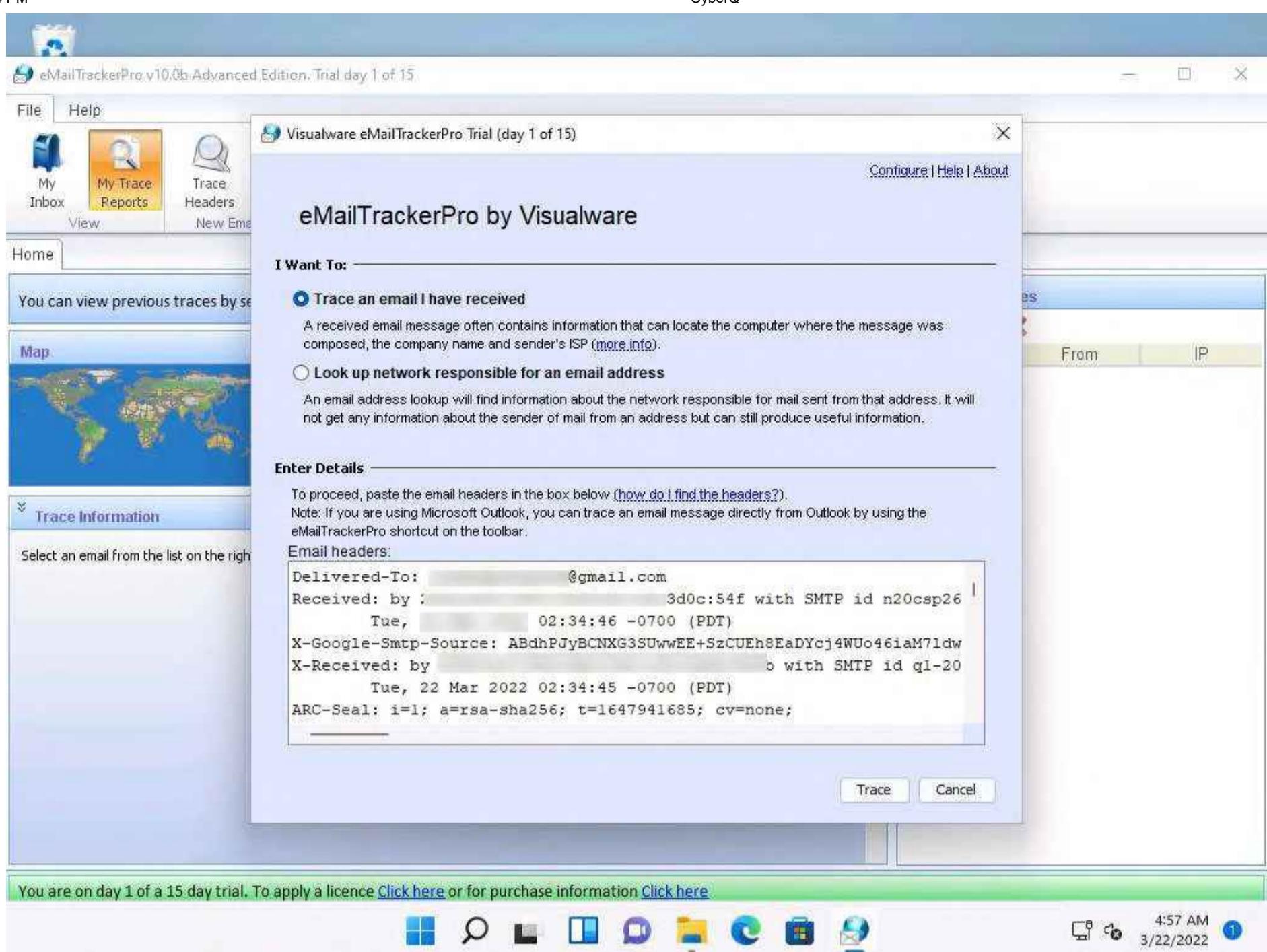
Note: In **Outlook**, find the email header by following the steps:

- 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.



The trace is complete, the information found is displayed on the right

Email Summary

From: [REDACTED].com
To: [REDACTED]@gmail.com
Date: 09:34:44 +0000 (UTC)
Subject: Please verify your SecurityTrails account
Location: [America]

Misdirected: Yes (Possibly spam)
Abuse Address: abuse@sendgrid.com
Abuse Reporting: To automatically generate an email abuse report [click here](#)
From IP: [REDACTED]
Header Analysis:
A time stamp claimed to be added by a server along the emails route is not valid. This is a mistake by the spammer that means a header in this email is fake.

System Information:
• There is no SMTP server running on this system (the port is closed)

Network Whois

Domain Whois

Email Header

#	Hop IP	Hop Name	Location
1	10.		
2	172		
3	192		
4	103		[Europe]
5	38		[America]
6	154	te0-3-0-5.rcr21.tpa01.atlas.cogen	Tampa, FL, USA
7	154	be2320.ccr22.mia01.atlas.cogent	Miami, FL, USA
8	154	be2027.ccr22.mia03.atlas.cogent	Miami, FL, USA
9	154	level3.mia03.atlas.cogentco.com	Miami, FL, USA

You are on day 1 of a 15 day trial. To apply a licence [Click here](#) or for purchase information [Click here](#)

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

The trace is complete, the information found is displayed on the right

Email Summary

From: [REDACTED].com
To: [REDACTED]@gmail.com
Date: 09:34:44 +0000 (UTC)
Subject: Please verify your SecurityTrails account
Location: [America]

Misdirected: Yes (Possibly spam)
Abuse Address: abuse@sendgrid.com
Abuse Reporting: To automatically generate an email abuse report [click here](#)
From IP: [REDACTED]
Header Analysis:
A time stamp claimed to be added by a server along the emails route is not valid. This is a mistake by the spammer that means a header in this email is fake.

System Information:
• There is no SMTP server running on this system (the port is closed)

Network Whois

Domain Whois

Email Header

#	Hop IP	Hop Name	Location
1	10.		
2	172		
3	192		
4	103		[Europe]
5	38		[America]
6	154	te0-3-0-5.rcr21.tpa01.atlas.cogen	Tampa, FL, USA
7	154	be2320.ccr22.mia01.atlas.cogent	Miami, FL, USA
8	154	be2027.ccr22.mia03.atlas.cogent	Miami, FL, USA
9	154	level3.mia03.atlas.cogentco.com	Miami, FL, USA

You are on day 1 of a 15 day trial. To apply a licence [Click here](#) or for purchase information [Click here](#)

15. The complete report appears in the default browser.

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

16. Expand each section to view detailed information.

The screenshot shows a web browser window titled "eMailTrackerPro Report". The address bar displays "file:///C:/Users/Admin/eMailTrackerPro/V8/reports/report-20220322-0500-0.html". The main content area is titled "Identification Report for 'Please verify your SecurityTrails account'". A message box states: "You are on day 1 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to purchase a product license from the Visualware website or authorized reseller." Below this, it says: "Computer 149 has been found. eMailTrackerPro has drawn information from its own database and from information specified by the owners of 149. Both sources tend to agree that the host is located around Miami, FL, USA." A section titled "Network Contact Information" shows the following details: "Inc.", "com", "+1-", and "US". There is a link to "Click here to hide the in-depth information on this email (more info)". A bulleted list follows: "• The sender's IP was - 149", "• A time stamp claimed to be added by a server along the emails route is not valid. This is a mistake by the spammer that means a header in this email is fake.", and "• The sender of this email appeared to have the address com. This information is easily faked so should not be treated as conclusive." The bottom of the window shows a taskbar with various icons and the system tray indicating the date and time as 5:07 AM on 3/22/2022.

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](https://whois.domaintools.com) and press **Enter**. The Whois Lookup website appears, as shown in the screenshot.

The screenshot shows a Mozilla Firefox browser window with the URL <https://whois.domaintools.com> in the address bar. The page itself is the DomainTools Whois Lookup interface. At the top, there's a navigation bar with links for HOME, PROFILE, CONNECT, MONITOR, SUPPORT, LOGIN, and Sign Up. Below the navigation is a large banner with the text "Whois Lookup" and a search bar containing "Enter a domain or IP address...". To the right of the search bar is a green "Search" button. The background of the page features a scenic landscape of hills under a sunset sky. A promotional message at the bottom left encourages users to become members for better data. The Firefox toolbar at the bottom includes icons for Back, Forward, Stop, Home, and Search, along with the date and time (9:02 AM, 3/17/2022).

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

The screenshot shows the DomainTools website with a search bar containing "www.certifiedhacker.com". Below the search bar, there's a large banner with a sunset background and a network graph. Text on the banner encourages becoming a member for better data. A message below the banner explains how DomainTools connects domains and IPs. The top navigation bar includes links for HOME, RESEARCH, LOGIN, and Sign Up.

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.

The screenshot shows the DomainTools Whois Record for CertifiedHacker.com. The left side displays a detailed table of domain registration information, including the registrant (PERFECT PRIVACY, LLC), registrar (Network Solutions, LLC), and various dates. The right side features promotional banners for "DomainTools Iris" and "Preview the Full Domain Report", along with a "Tools" sidebar containing links for Hosting History, Monitor Domain Properties, Reverse IP Address Lookup, Network Tools, and Visit Website. Below the tools is a preview of the domain's website content.

IP Address 162.241.216.11 - 1,747 other sites hosted on this server

IP Location 🇺🇸 - Utah - Provo - Unified Layer

ASN 🇺🇸 AS26337 OIS1, US (registered Oct 09, 2013)

Domain Status Registered And Active Website.

IP History 13 changes on 13 unique IP addresses over 16 years

Registrar History 3 registrars with 2 drops

Hosting History 6 changes on 4 unique name servers over 19 years

Website

Website Title // Certified Hacker

Server Type nginx/1.19.10

Response Code 200

Terms 36 (Unique: 28, Linked: 7)

Images 10 (Alt tags missing: 0)

Links 16 (Internal: 12, Outbound: 0)

Whois Record (last updated on 2022-03-17)

Domain Name:	CERTIFIEDHACKER.COM
Registry Domain ID:	88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server:	whois.networksolutions.com

General TLDs Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

- Taken domain.
- Available domain.
- Deleted previously owned domain.

CertifiedHacker.com	View Whois
CertifiedHacker.net	Buy Domain
CertifiedHacker.org	View Whois
CertifiedHacker.info	Buy Domain
CertifiedHacker.biz	Buy Domain
CertifiedHacker.us	Buy Domain

9:04 AM 3/17/2022

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

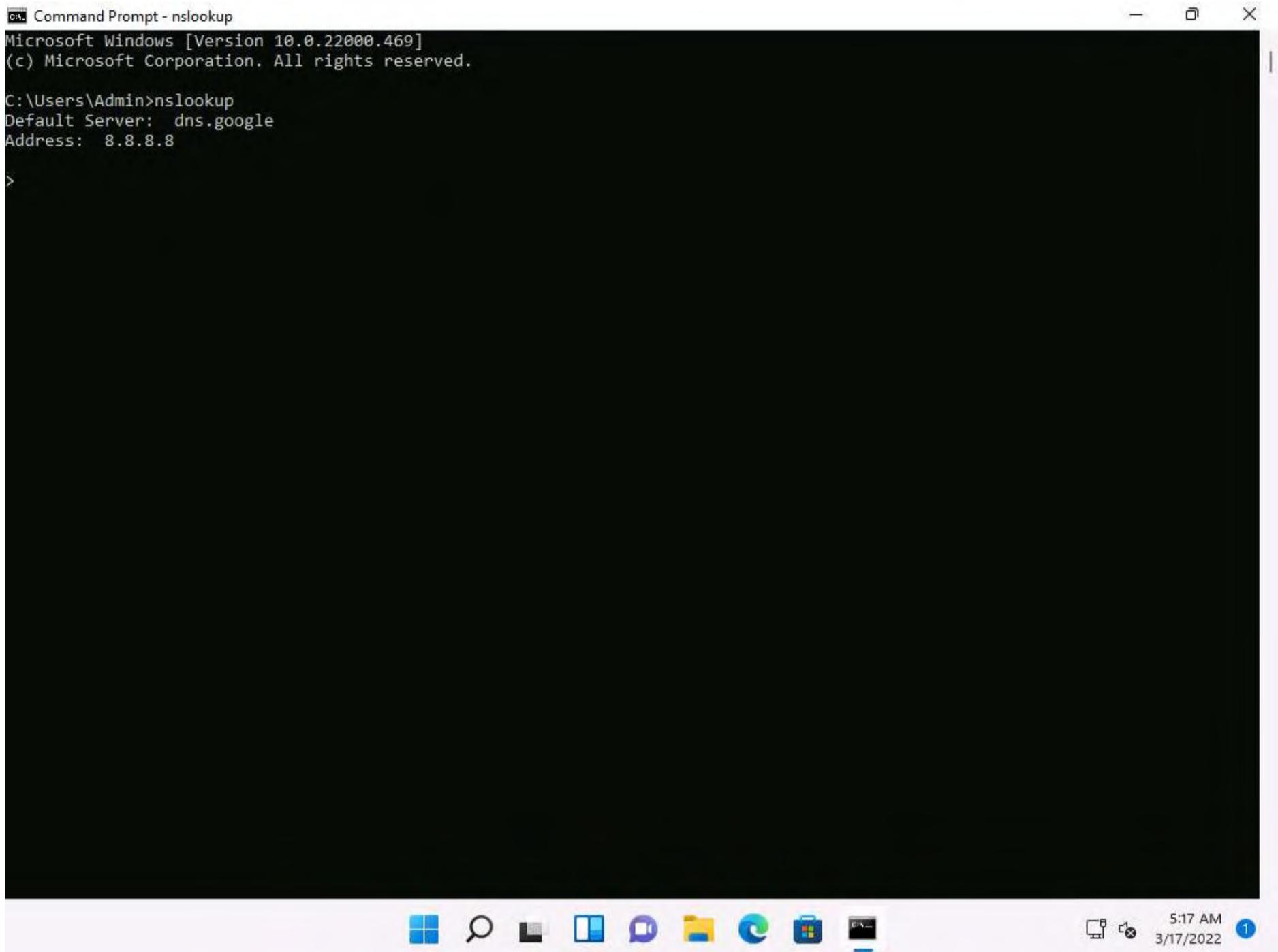
DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all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



The screenshot shows a Windows 11 Command Prompt window titled "Command Prompt - nslookup". The window displays the following text:

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

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

>
```

The taskbar at the bottom of the screen includes icons for Start, Search, Task View, File Explorer, Edge, File Explorer, and Task View. The system tray shows the date and time as 5:17 AM 3/17/2022, with a battery icon indicating 1% remaining.

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**.

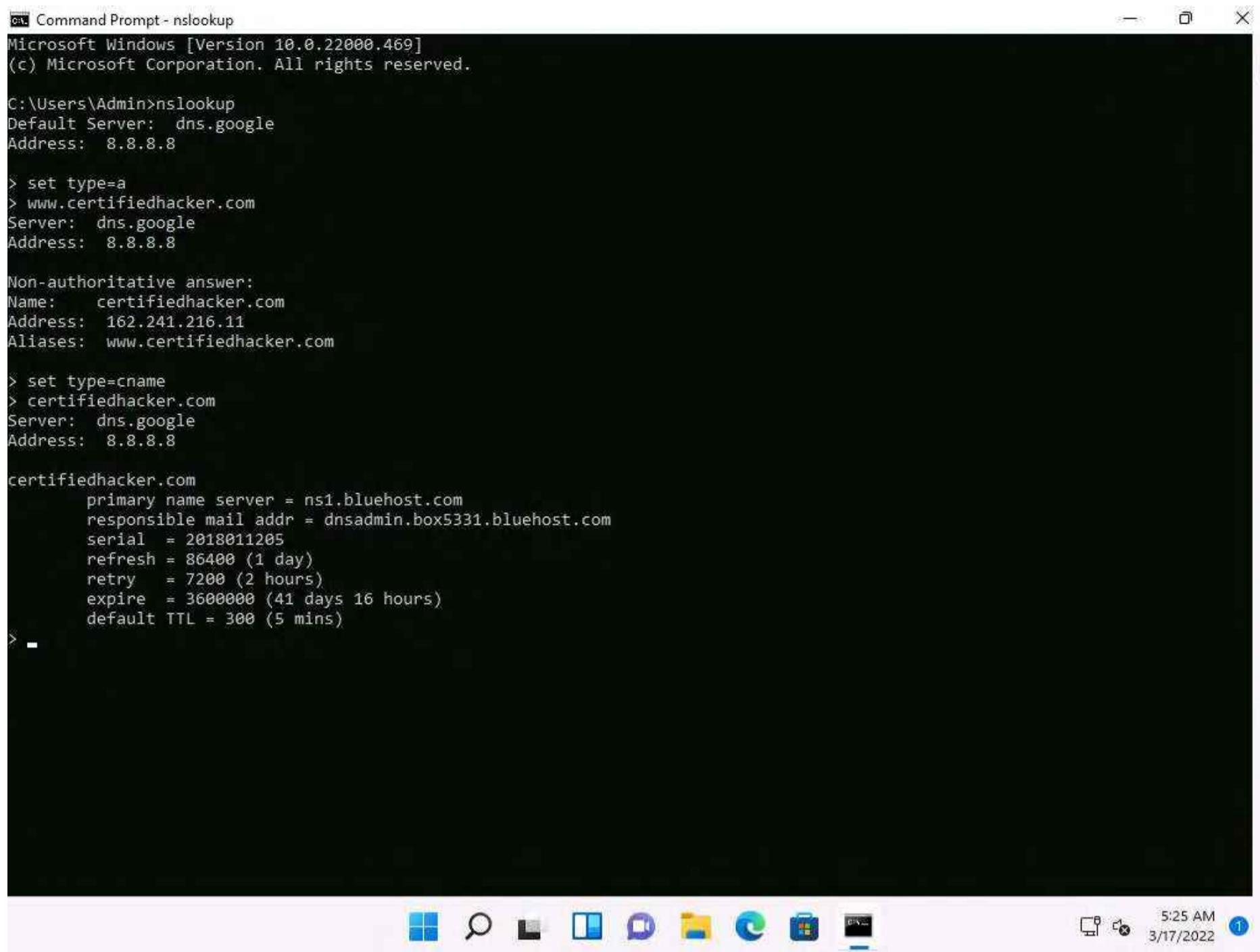
6. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.

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.





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

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

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

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

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

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

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.



```

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

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

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

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

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

> set type=a
> ns1.bluehost.com
Server: dns.google
Address: 8.8.8.8

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

>

```

5:26 AM 3/17/2022

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.



NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.

This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSlookup

Domain: ... the name of the machine to look up.

Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query:

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).

Basically, DNS maps domain names to IP addresses.

Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"/127.0.0.1.

To resolve an IP address by reverse lookup (get a computer's name if you only have its IP address), try to perform a PTR query instead of ANY. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly be true, but sometimes not. If you don't get a PTR information about a specific computer from a NSLOOKUP query, you may want to try our whois service to find out the owner of this IP address.

Like the PTR, other records are also not mandatory: LOC, RP, TXT. They are not strictly required in the DNS and their content may be true or not.

You can't trust on the LOC to locate a host, because most hosts don't have this record defined.

If you prefer dig over nslookup, you may try our dig service.

This page is also available in [German](#), [French](#) and [Portuguese](#). Enjoy.

>>> If you would like to see this service in your or any other language, please send a translation.

5:30 AM 3/17/2022

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.

NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.

This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSlookup

Domain: certifiedhacker.com ... the name of the machine to look up.

Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query:

here is the nslookup result for certifiedhacker.com from server localhost, querytype=A:

```
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
```

[Query 8 of max 100]

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).

5:31 AM 3/17/2022

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

NSLOOKUP: look up and find IP addresses in the DNS

... here is the nslookup result for **certifiedhacker.com** from server localhost, querytype=A:

```
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
```

[Query 8 of max 100]

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the [nslookup manual \(man page\)](#).

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.

NSLOOKUP: look up and find IP addresses in the DNS

... here is the nslookup result for **certifiedhacker.com** from server localhost, querytype=AAAA:

```
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53

Non-authoritative answer:
*** Can't find certifiedhacker.com: No answer

Authoritative answers can be found from:
certifiedhacker.com
    origin = ns1.bluehost.com
    mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400
    retry = 7200
    expire = 3600000
    minimum = 300
```

[Query 9 of max 100]

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.

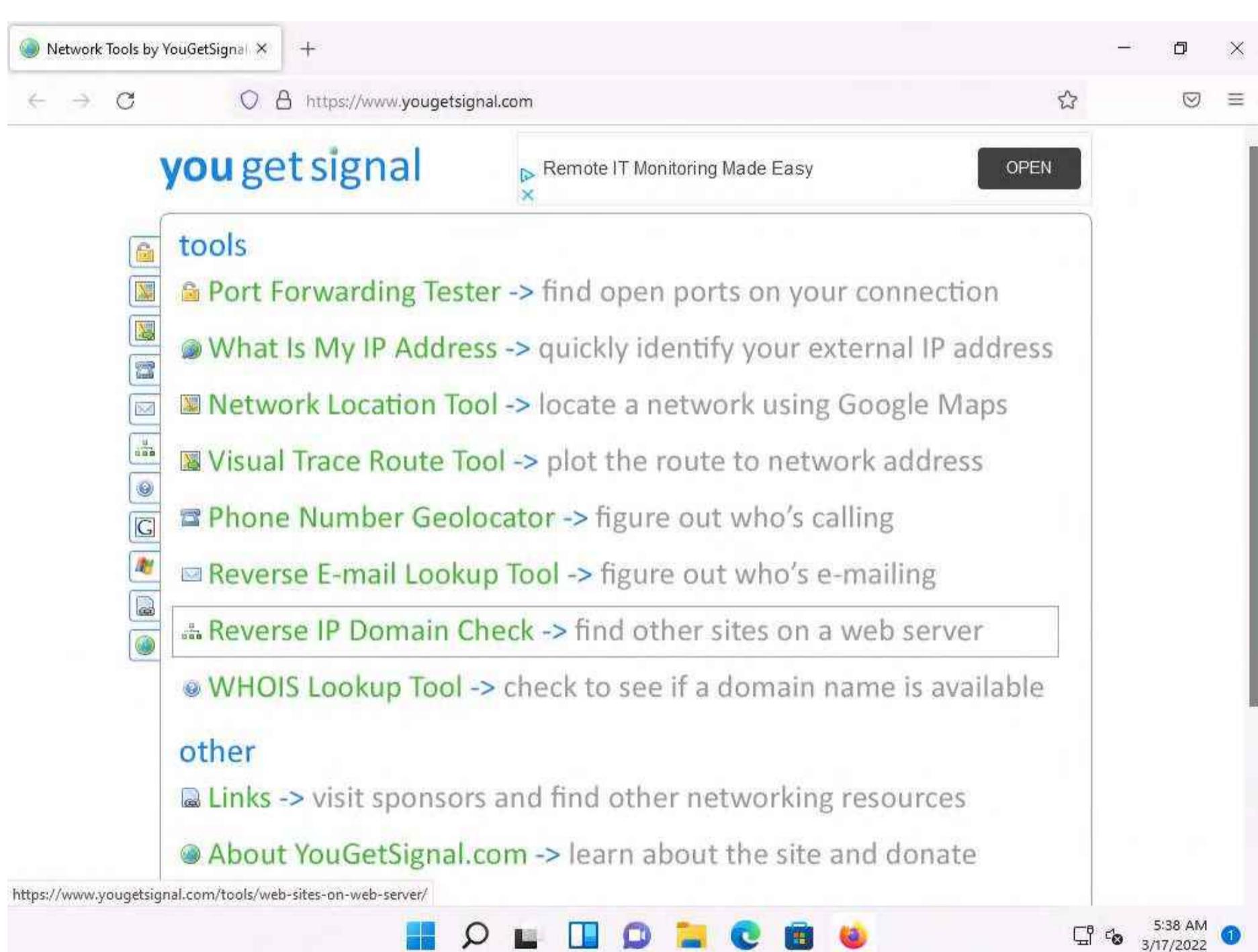
Task 2: Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

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.

Reverse IP Domain Check

Remote Address:

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

100wwcbeaufort.org	biosis.ae
bongekile.com	box5331.bluehost.com
certifiedhacker.com	eis.qa
gaelicmemoriesphotography.ie	humancarehealth.com
oakoffer.com	www.certifiedhacker.com
www.certifiedhacker.com.	www.lststl.org

about

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

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

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

[help me pay for school \(PayPal\)](#)

START NOW

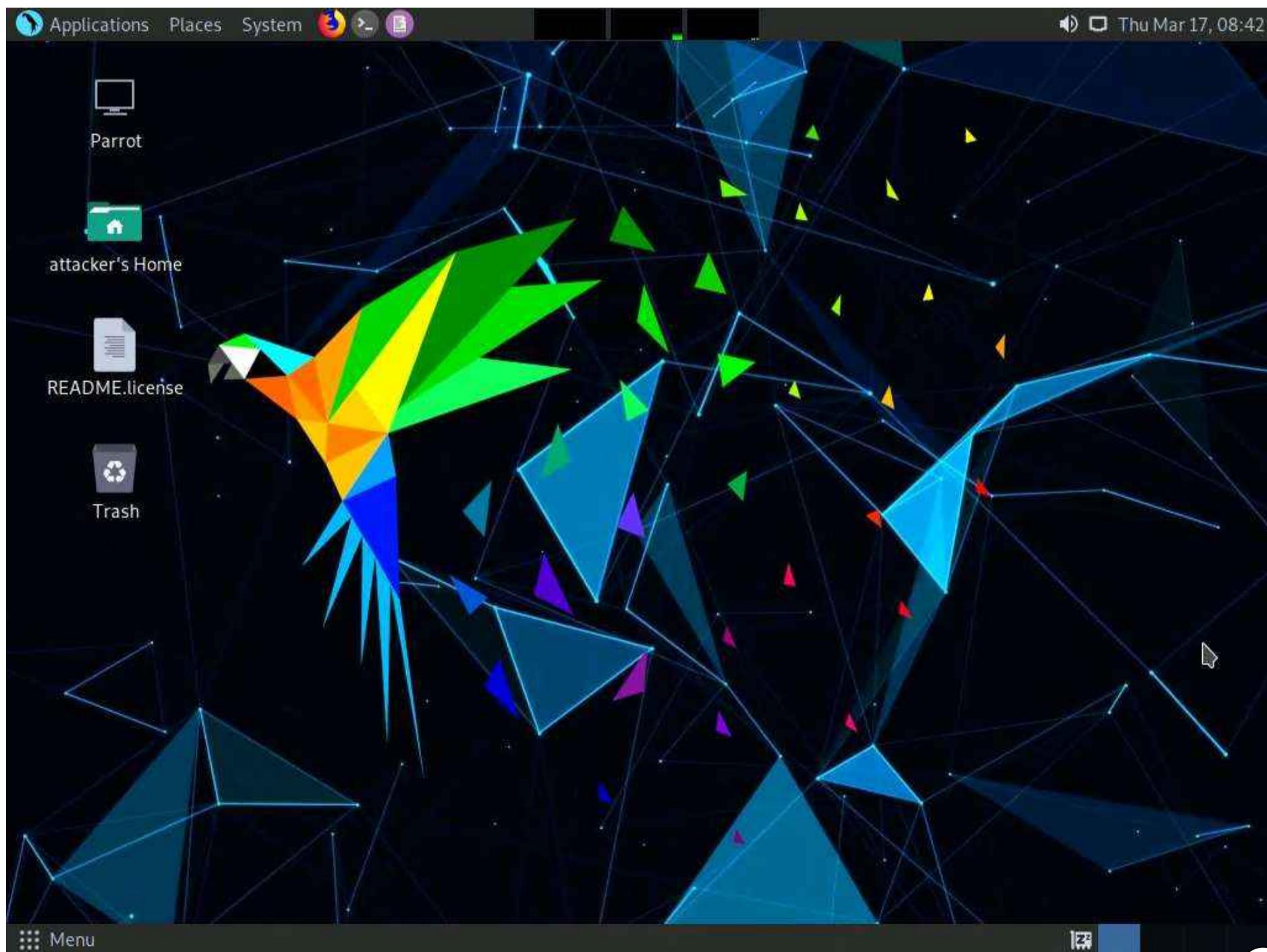
1. Click "Start Now"
2. Download Now
3. Enjoy Easy Search Tool

Easy Search Tool

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

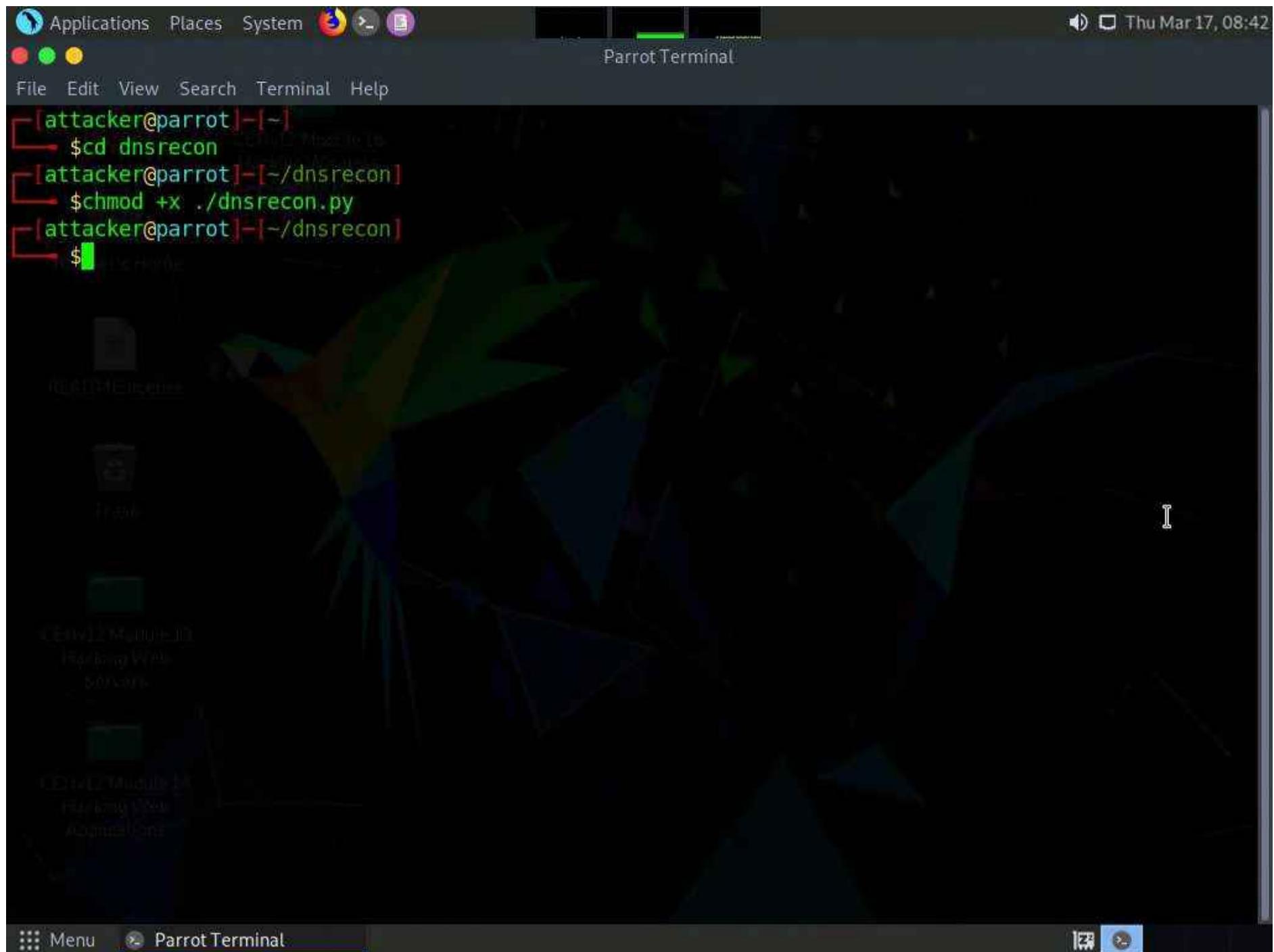
4. Now, click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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.



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

9. This concludes the demonstration of gathering information about a target organization by performing reverse DNS lookup using "you get signal's" Reverse IP Domain Check and DNSRecon tool.

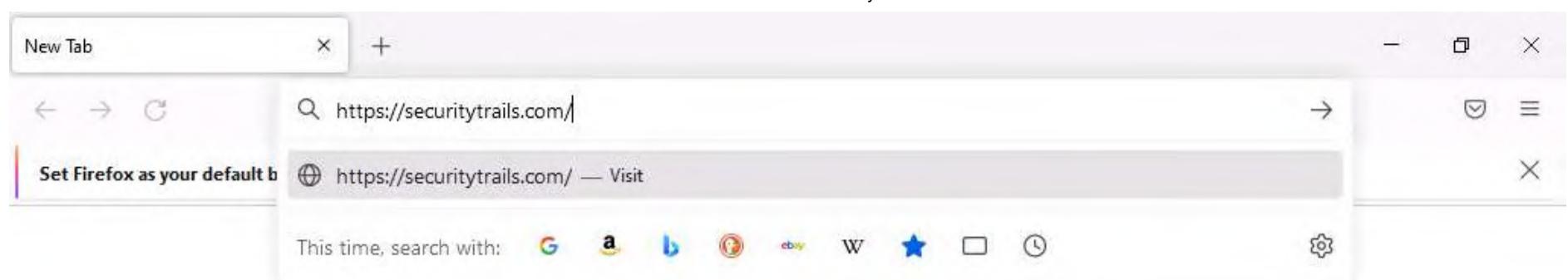
10. Close all open windows and document all the acquired information.

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.

A screenshot of a Firefox browser window displaying the SecurityTrails website. The URL 'https://securitytrails.com' is in the address bar. The page features a dark blue header with the text 'Get an attacker's point of view: unveil your digital footprint' and a 'Request Access' button. Below the header, the SecurityTrails logo is visible along with navigation links for Products, Why Us, Customers, Pricing, Blog, Support, Log In, and a prominent 'Sign Up For Free' button. The main content area has a blue background with white text. It includes a section titled 'The Total Internet Inventory.' with the subtext 'Powerful tools for third-party risk, attack surface management, and total intel'. To the right, there are several data points: 'NETFLIX' with a company search icon, '5 Acquisitions', '4.6K Subdomains' (with a note 'Last one created today'), '1K Domains', '2.1K SSL Certificates', and '13 Years of DNS History'. A large teal button at the bottom left says 'See your Organization's Attack Surface'. The browser's taskbar at the bottom shows various pinned icons.

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

The screenshot shows the Firefox browser window with the URL https://securitytrails.com/app/signup?utm_source=st-home&utm_medium=button&utm_campaign=button. The page title is "Signup | SecurityTrails Account". A banner at the top says "Get an attacker's point of view: unveil your digital footprint" with a "Request Access" button. On the left, there are fields for "Name" (redacted), "Email" (@gmail.com), and "Company" (redacted). On the right, under "Reasons to join free:", there are three sections: "Discover Historical DNS Records" (with a globe icon), "Find Unseen Subdomains" (with a magnifying glass icon), and "Reveal Associated Domains" (with an eye icon). The status bar at the bottom shows "SecurityTrails v2.11.0 © 2022" and "Light Mode". The taskbar at the bottom of the screen shows various pinned icons.

This screenshot is identical to the one above, but the "Company" field now contains the text "ccc". The rest of the interface, including the "Reasons to join free:" section and the system status bar, remains the same.

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

Please verify your email address

We have sent you an email to [REDACTED]@gmail.com. Please click on the link in the email to complete the signup.

Not in your inbox?
Please check your Spam/Junk folder, or resend the email

Enhance Attack Surface Reduction™ with SurfaceBrowser™

SecurityTrails v2.11.0 © 2022 Light Mode

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**.

Please verify your SecurityTrails account

SecurityTrails <hello@securitytrails.com>
to me

Please confirm your email address by clicking the link below.

We may need to send you critical information about our service and it is important that we have an accurate email address.

Confirm Email Address

SecurityTrails The Total Internet Inventory.
A Recorded Future® Company

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

The screenshot shows the SecurityTrails.com dashboard. At the top, there are three tabs: "Verify Email Address | SecurityTrails" (disabled), "Please verify your SecurityTrails" (disabled), and "Home | SecurityTrails Account". The "Home | SecurityTrails Account" tab is active. Below the tabs, the URL "https://securitytrails.com/app/account" is displayed. A banner at the top says "Get an attacker's point of view: unveil your digital footprint" and has a "Request Access" button. On the left, a sidebar lists "Get SurfaceBrowser™", "Dashboard" (selected), "API", "Feeds", and "Account". The main content area is titled "Dashboard" and displays a chart titled "Daily API Requests Overview" for March 22, 2022. The chart shows 100 API requests. Below the chart, a message says "Hi, you can access our data with your browser (search field in navigation bar) or by using our API." A blue button labeled "Get Started" is visible. On the right, there is a "Choose a plan that's right for your business" section with a "Upgrade now" button, a "Subscription" section, and a "Quota usage Mar 2022" section. The status bar at the bottom shows "SecurityTrails v2.11.0 © 2022 Light Mode".

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

The screenshot shows the SecurityTrails.com dashboard after searching for "certifiedhacker.com". The search results are not yet visible, but the search term is present in the search bar. The rest of the interface is identical to the previous screenshot, including the tabs, sidebar, and main dashboard content.

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 | SecurityTrails X Please verify your SecurityTrails X certifiedhacker.com - Current X +

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

certifiedhacker.com DNS records as of Mar 22, 2022

- DNS Records
- Historical Data
- Subdomains (89)

A records

Unified Layer

162.241.216.11 (35,942)

AAAA records

NO RECORDS

MX records

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

Windows Search File Mail Internet Explorer Task View Start 3:00 AM 3/22/2022 1

Verify Email Address | SecurityTrails X Please verify your SecurityTrails X certifiedhacker.com - Current X +

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

mail.certifiedhacker.com (1)

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!

Windows Search File Mail Internet Explorer Task View Start 3:01 AM 3/22/2022 1

SOA records

ttl: 86400

email: dnsadmin.box5331.bluehost.com

TXT

v=spf1 a mx ptr include:bluehost.com ?all

CNAME records pointed here

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

CNAME records pointed here

ftp.certifiedhacker.com

www.certifiedhacker.com

View more certifiedhacker.com CNAME records

★ See even more – Upgrade now!

SecurityTrails
A Recorded Future® Company

PRODUCTS COMPANY RESOURCES SUPPORT

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

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

The screenshot shows the SecurityTrails interface for the domain `certifiedhacker.com`. On the left sidebar, there are tabs for DNS Records, Historical Data, and Subdomains. The Subdomains tab is currently selected, indicated by a blue background and the number 89 in a badge. The main content area is titled "certifiedhacker.com historical A data". Below this, there is a table with columns: IP Addresses, Organization, First Seen, Last Seen, and Duration Seen. The table contains four rows of data. At the bottom of the page, there is a toolbar with various icons and a system tray showing the date and time as 3/22/2022 at 3:12 AM.

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

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

The screenshot shows the SecurityTrails interface for the domain `certifiedhacker.com`. The Subdomains tab is selected, indicated by a blue background and the number 89 in a badge. The main content area is titled "certifiedhacker.com subdomains". Below this, there is a table with columns: Domain, Rank, Hosting Provider, and Mail Provider. The table contains five rows of data. At the bottom of the page, there is a toolbar with various icons and a system tray showing the date and time as 3/22/2022 at 3:12 AM.

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

12. DNS records provide important information about the locations and types of servers which attackers can use to further launch web application attacks.

13. This concludes the demonstration of gathering information on the subdomain and DNS records of a target organization using SecurityTrails.
14. You can also use **DNSChecker** (<https://dnschecker.org>), and **DNSdumpster** (<https://dnsdumpster.com>), etc. to perform DNS footprinting on a target website.
15. Close all open windows and document all the acquired information.

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.



The screenshot shows the ARIN website homepage. At the top, it displays "Your IPv4 address is 199.101.110.11". A search bar contains the IP address "162.241.216.11" with a "Search" button. Below the search bar, a message reads "all requests subject to terms of use". The main banner features the text "ARIN is a nonprofit, member-based organization that administers IP addresses & ASNs in support of the operation and growth of the Internet." Below the banner are five icons: a blue circle with a white "i", a blue square with a white plus sign, a red recycling symbol, a purple globe, and an orange handshake. Below these icons are links: "New to ARIN", "Request IP Addresses & ASNs", "Transfers", "IPv6 Info", and "Get Involved". The taskbar at the bottom shows various pinned icons.

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

The screenshot shows the ARIN Whois/RDAP search results for the IP address 162.241.216.11. The search bar at the top also contains "162.241.216.11". The results are displayed in a table:

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

On the right side, there is a "Related" sidebar with links: "Report Whois Inaccuracy", "Whois/RDAP Documentation", "ARIN Technical Discussion", "Mailing List", and "FAQs". The taskbar at the bottom shows various pinned icons.

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.

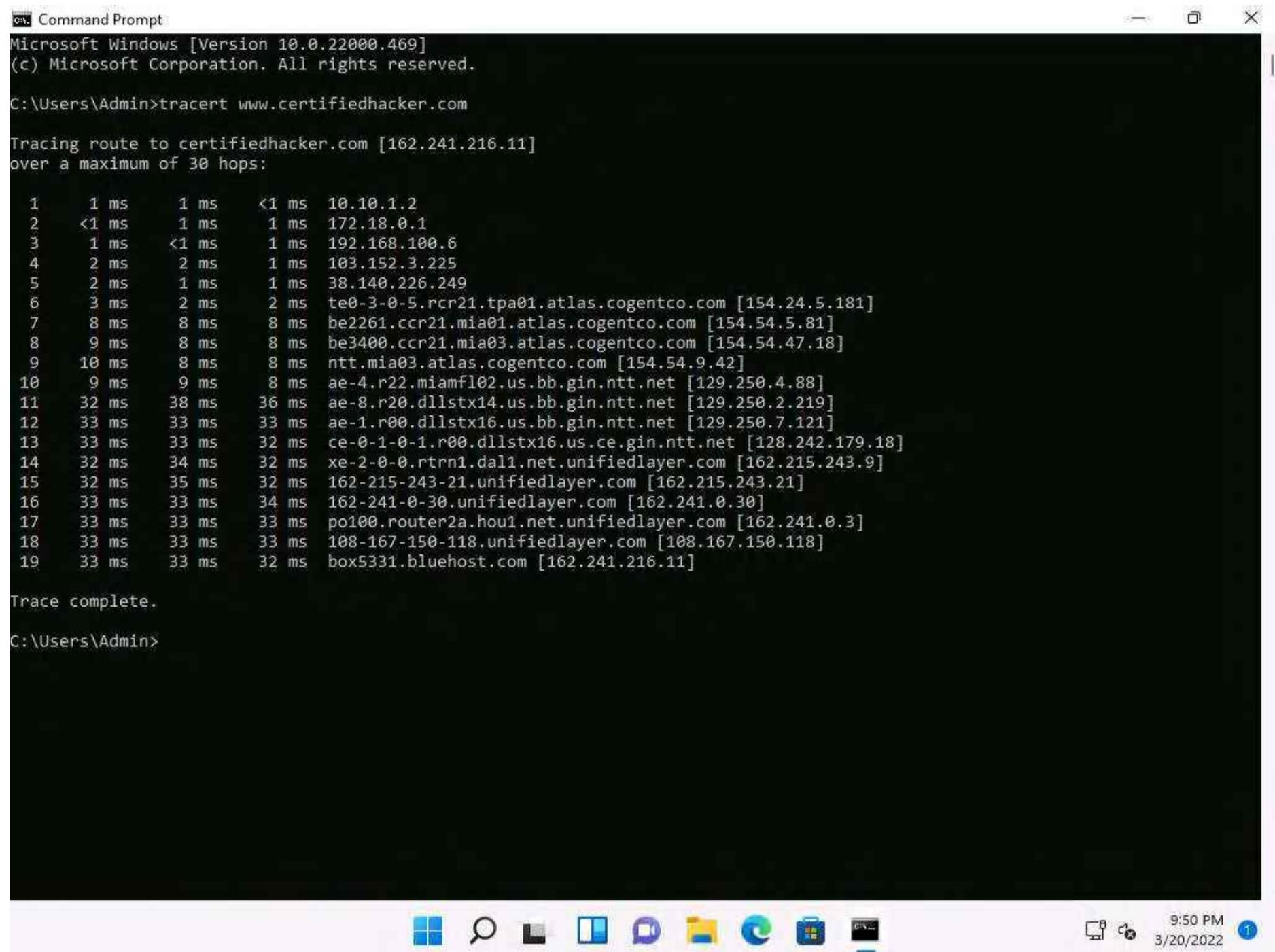
Task 2: Perform Network Tracerouting in Windows and Linux Machines

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.



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

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.rtrm1.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>
```

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



```
C:\ 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.

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

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

 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

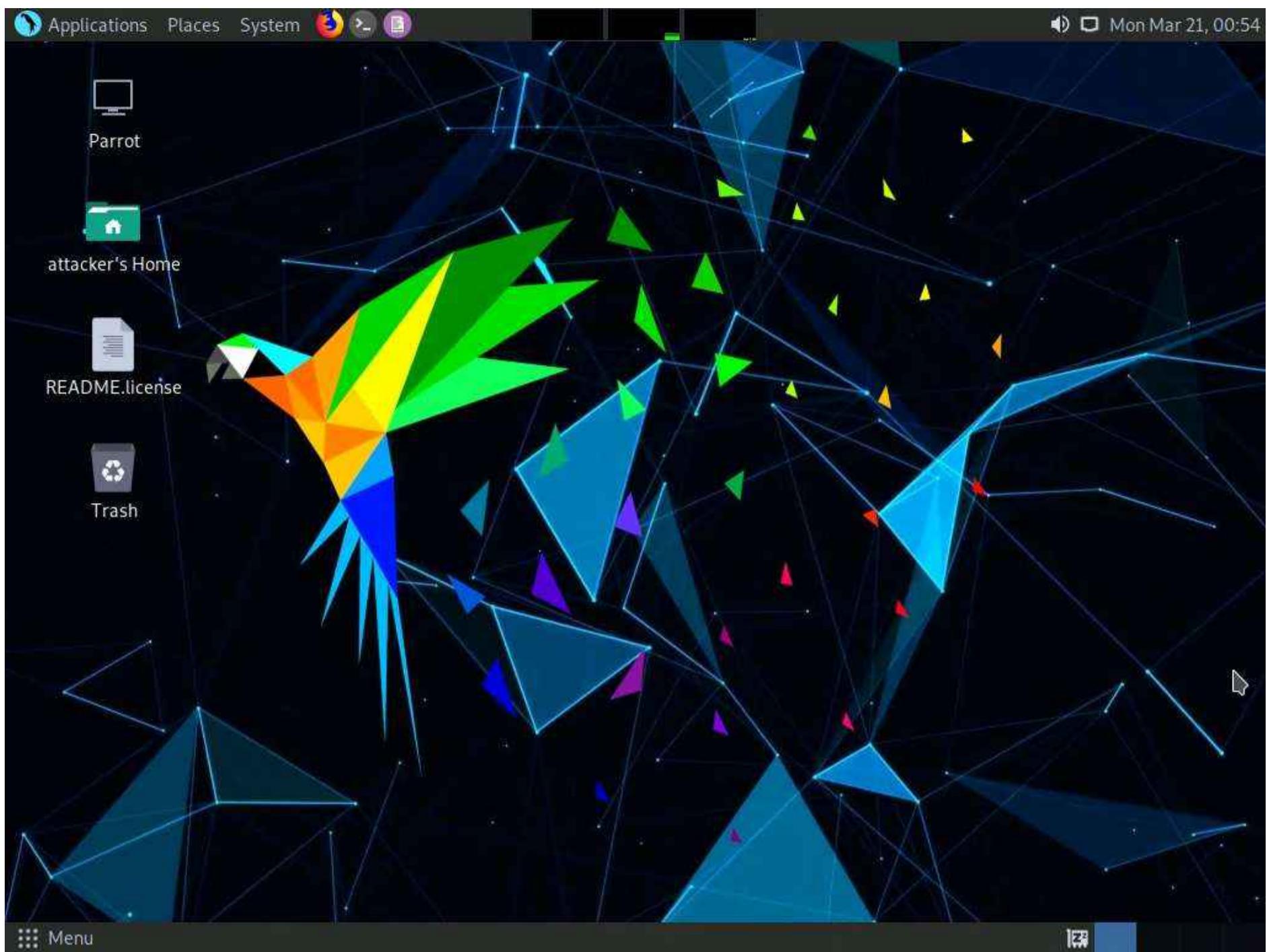
Trace complete.

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.



```
[attacker@parrot:~] $ traceroute www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  1.748 ms  1.646 ms  1.590 ms
 2  172.18.0.1 (172.18.0.1)  1.970 ms  1.923 ms  2.244 ms
 3  192.168.100.6 (192.168.100.6)  2.384 ms  2.809 ms  3.074 ms
 4  103.152.3.225 (103.152.3.225)  3.285 ms  3.570 ms  3.679 ms
 5  38.140.226.249 (38.140.226.249)  5.084 ms  5.039 ms  5.184 ms
 6  te0-3-0-5.rcr21.tpa01.atlas.cogentco.com (154.24.5.181)  7.724 ms te0-3-1-5.rcr21.tpa01.atlas.cogentco.com (154.24.32.129)  2.951 ms  2.862 ms
 7  be2261.ccr21.mia01.atlas.cogentco.com (154.54.5.81)  9.837 ms  10.653 ms  10.524 ms
 8  be3400.ccr21.mia03.atlas.cogentco.com (154.54.47.18)  10.413 ms be3401.ccr21.mia03.atlas.cogentco.com (154.54.47.30)  10.336 ms be3400.ccr21.mia03.atlas.cogentco.com (154.54.47.18)  10.298 ms
 9  ntt.mia03.atlas.cogentco.com (154.54.9.42)  10.222 ms  10.829 ms  11.211 ms
10  ae-4.r22.miamfl02.us.bb.gin.ntt.net (129.250.4.88)  11.956 ms  11.874 ms  11.768 ms
11  ae-8.r20.dllstx14.us.bb.gin.ntt.net (129.250.2.219)  40.783 ms *
12  ae-1.r00.dllstx16.us.bb.gin.ntt.net (129.250.7.121)  34.203 ms ae-1.r01.dllstx16.us.bb.gin.ntt.net (129.250.7.125)  34.118 ms ae-1.r00.dllstx16.us.bb.gin.ntt.net (129.250.7.121)  37.677 ms
13  ce-0-0-0-1.r01.dllstx16.us.ce.gin.ntt.net (131.103.117.42)  37.285 ms  36.660 ms ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net (128.242.179.18)  36.796 ms
14  xe-2-0-0.rtrn1.dall.net.unifiedlayer.com (162.215.243.9)  35.945 ms xe-2-0-1.rtrn2.dal1.net.unifiedlayer.com (162.215.243.7)  35.266 ms  34.614 ms
15  162-215-243-23.unifiedlayer.com (162.215.243.23)  33.897 ms 162-215-243-21.unifiedlayer.com (162.215.243.21)  34.159 ms  34.323 ms
16  162-241-0-28.unifiedlayer.com (162.241.0.28)  36.658 ms 162-241-0-30.unifiedlayer.com (162.241.0.30)  36.612 ms 162-241-0-28.unifiedlayer.com (162.241.0.28)  34.222 ms
17  po101.router2a.hou1.net.unifiedlayer.com (162.241.0.7)  34.207 ms po100.router2a.hou1.net.unifiedlayer.com (162.241.0.3)  37.915 ms  37.869 ms
18  108-167-150-122.unifiedlayer.com (108.167.150.122)  35.174 ms  35.095 ms  35.293 ms
19  box5331.bluehost.com (162.241.216.11)  35.456 ms  35.412 ms  38.092 ms
```

8. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.

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

10. Close all open windows and document all acquired information.

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.

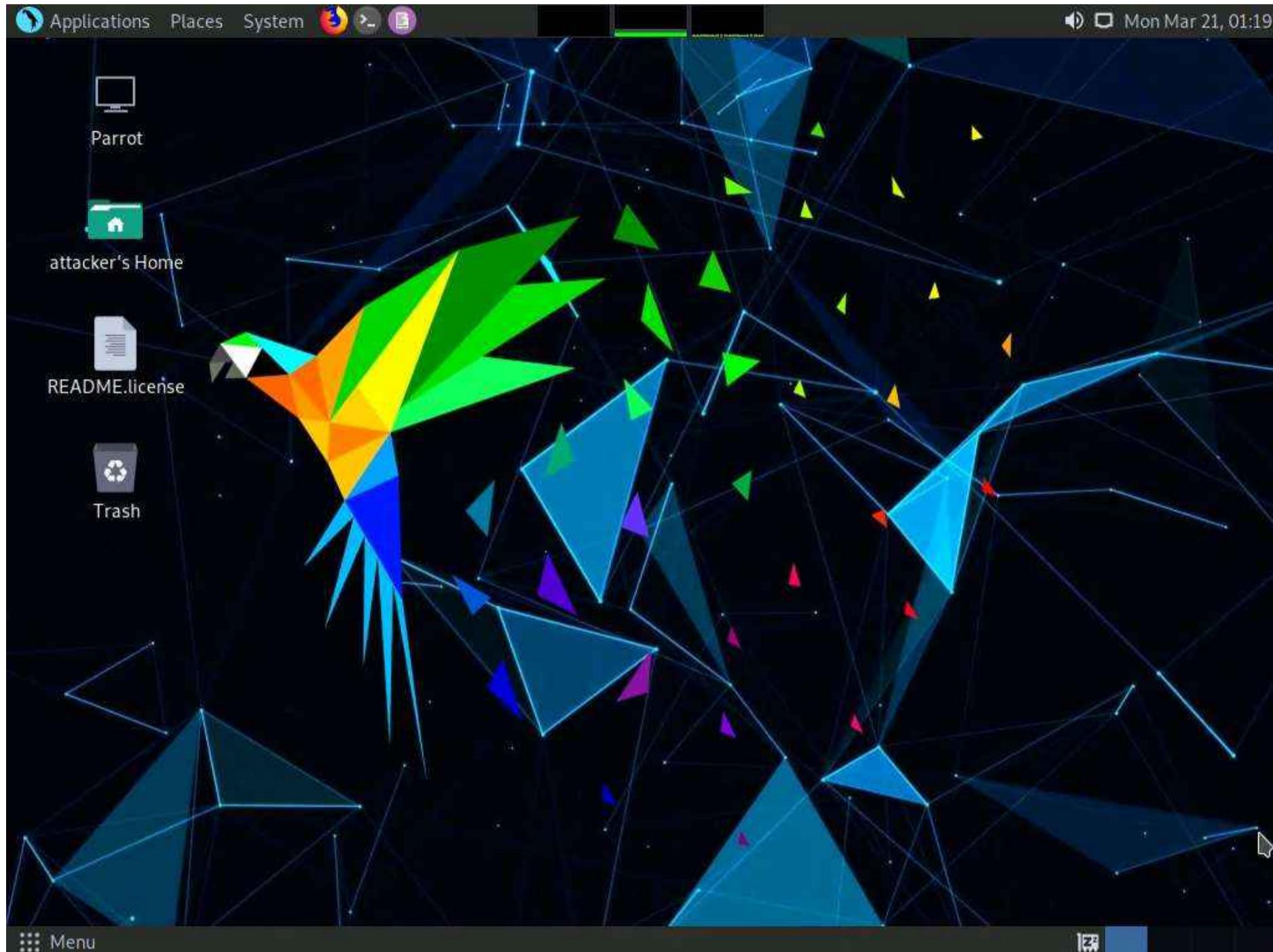
Task 1: Footprinting a Target using Recon-ng

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.



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

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

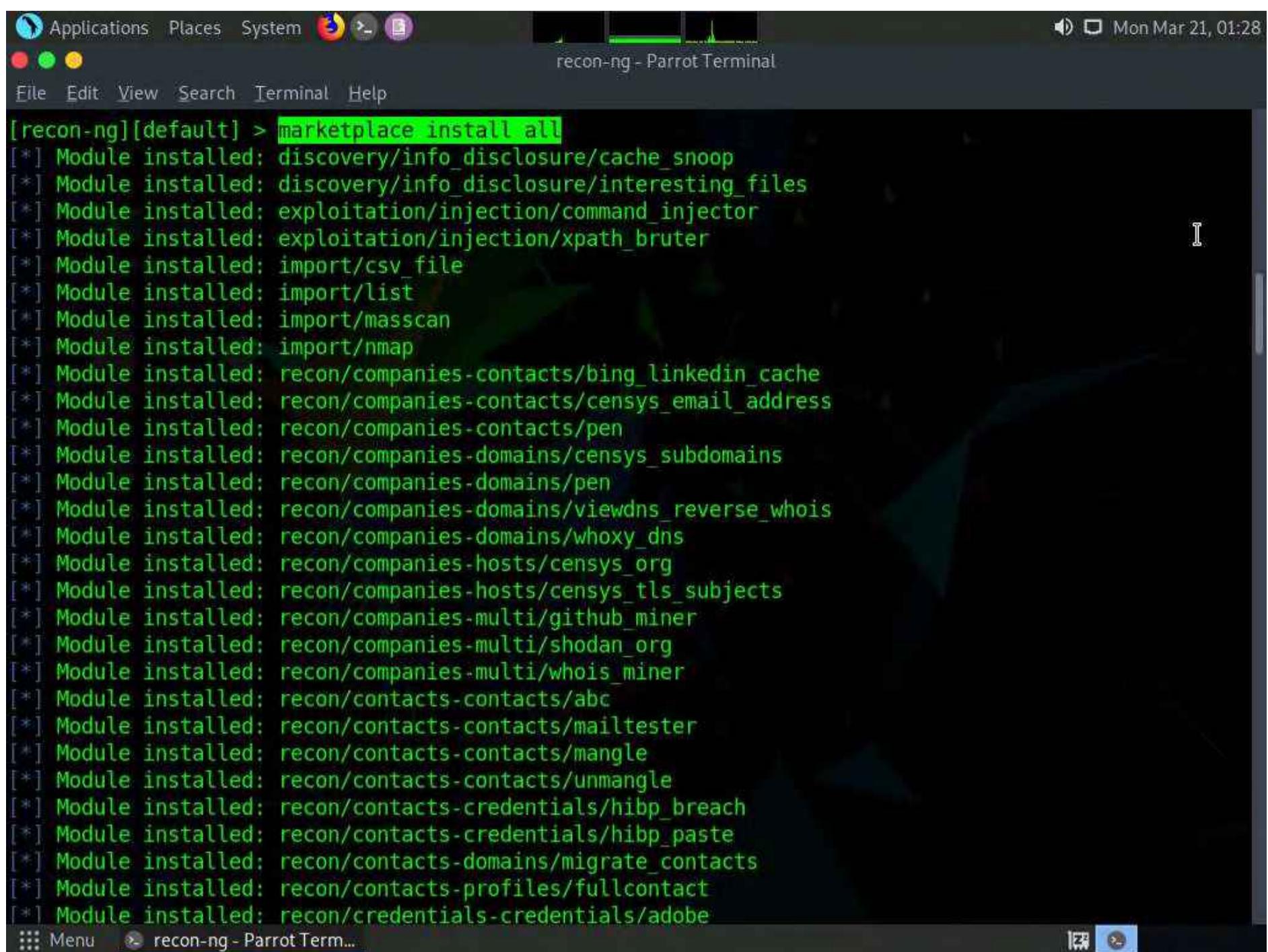
```
recon-ng - Parrot Terminal
[*] No modules enabled/installed.

[recon-ng][default] > help

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

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.



The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The window contains the command "[recon-ng][default] > marketplace install all" followed by a list of module installations. The modules listed are: discovery/info_disclosure/cache_snoop, discovery/info_disclosure/interesting_files, exploitation/injection/command_injector, exploitation/injection/xpath_bruter, import/csv_file, import/list, import/masscan, import/nmap, recon/companies-contacts/bing_linkedin_cache, recon/companies-contacts/censys_email_address, recon/companies-contacts/pen, recon/companies-domains/censys_subdomains, recon/companies-domains/pen, recon/companies-domains/viewdns_reverse_whois, recon/companies-domains/whoxy_dns, recon/companies-hosts/censys_org, recon/companies-hosts/censys_tls_subjects, recon/companies-multi/github_miner, recon/companies-multi/shodan_org, recon/companies-multi/whois_miner, recon/contacts-contacts/abc, recon/contacts-contacts/mailtester, recon/contacts-contacts/mangle, recon/contacts-contacts/unmangle, recon/contacts-credentials/hibp_breach, recon/contacts-credentials/hibp_paste, recon/contacts-domains/migrate_contacts, recon/contacts-profiles/fullcontact, recon/credentials-credentials/adobe. The terminal window has a dark theme with green text for success messages. The status bar at the bottom shows "recon-ng - Parrot Term...".

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

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

```

Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
[recon-ng][default] > modules search

Discovery
-----
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files

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

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

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

```

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

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

```

Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
[recon-ng][default] > workspaces
Manages workspaces

Usage: workspaces <create|list|load|remove> [...]
[recon-ng][default] >

```

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

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

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

```
[recon-ng][default] > workspaces create CEH
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email_address' disabled. Dependency required: "'censys'".
[!] Module 'recon/companies-domains/censys_subdomains' disabled. Dependency required: "'censys'".
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-hosts/censys_org' disabled. Dependency required: "'censys'".
[!] Module 'recon/companies-hosts/censys_tls_subjects' disabled. Dependency required: "'censys'".
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_paste module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-companies/censys_companies' disabled. Dependency required: "'censys'".
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: "'PyPDF3'".
[!] Module 'recon/domains-credentials/pwnedlist/account_creds' disabled. Dependency required: "'pyaes'".
[!] 'pwnedlist_api' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-credentials/pwnedlist/domain_creds' disabled. Dependency required: "'pyaes'".
[!] 'pwnedlist_api' key not set. domain_ispwned module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. domain_ispwned module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_api' key not set. leaks_dump module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. leaks_dump module will likely fail at runtime. See 'keys add'.
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_domain_api module will likely fail at runtime. See 'keys add'.
```

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

```
s$ .
[!] Module 'recon/netblocks-hosts/censys_netblock' disabled. Dependency required: 'censys'.
[!] 'shodan_api' key not set. shodan net module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin contacts module will likely fail at runtime. See 'keys add'

[!] 'github_api' key not set. github users module will likely fail at runtime. See 'keys add'.
[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'

[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'

[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[recon-ng][CEH] > workspaces list

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

15. Add a domain in which you want to perform network reconnaissance.

16. Type the command **db insert domains** and press **Enter**.

17. In the **domain (TEXT)** option type **certifiedhacker.com** and press **Enter**. In the **notes (TEXT)** option press **Enter**. This adds certifiedhacker.com to the present workspace.

18. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal displays several error messages about missing API keys for Twitter, GitHub, and Google modules. It then lists workspaces, inserts a domain into the database, and shows the inserted domain in the database table.

```
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.

[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.

[recon-ng][CEH] > workspaces list

+-----+
| Workspaces | Modified |
+-----+
| CEH        | 2022-03-21 01:30:48 |
| default    | 2022-03-21 01:23:19 |
+-----+

[recon-ng][CEH] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.

[recon-ng][CEH] > show domains

+-----+
| rowid | domain      | notes | module |
+-----+
| 1     | certifiedhacker.com |       | user_defined |
+-----+

[*] 1 rows returned
```

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

```

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

+-----+
| rowid | domain | notes | module |
+-----+
| 1 | certifiedhacker.com | user_defined |
+-----+

[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
-----
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][CEH] >

```

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

```

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

Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][CEH] > show domains

+-----+
| rowid | domain | notes | module |
+-----+
| 1 | certifiedhacker.com | user_defined |
+-----+

[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
-----
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

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

```

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

```

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

-----
SUMMARY
-----
[*] 22 total (19 new) hosts found.

[recon-ng][CEH][brute_hosts] >

```

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

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

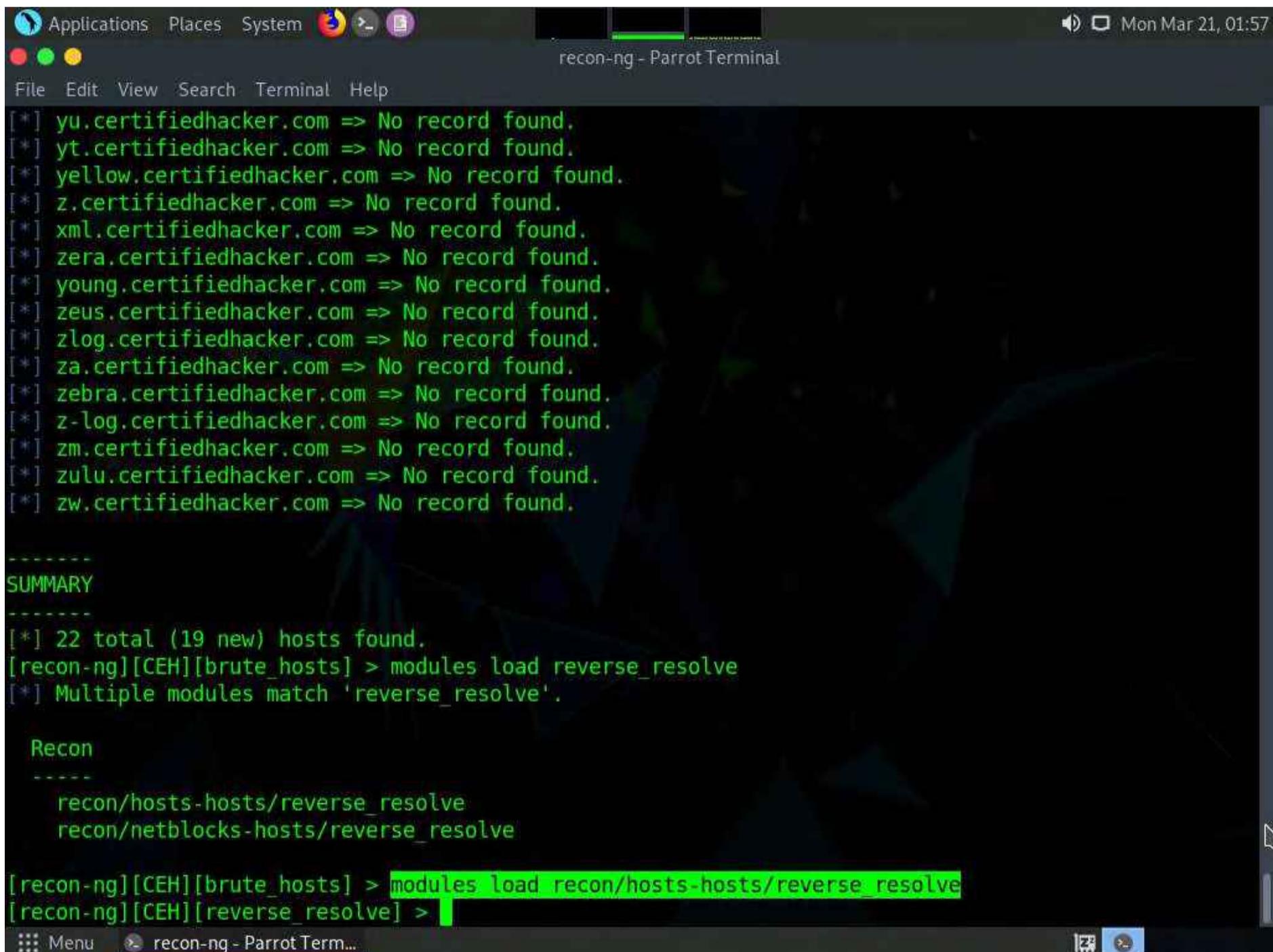
Note: To resolve hosts using the Bing module, use the following commands:

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

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

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

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



```
[*] yu.certifiedhacker.com => No record found.
[*] yt.certifiedhacker.com => No record found.
[*] yellow.certifiedhacker.com => No record found.
[*] z.certifiedhacker.com => No record found.
[*] xml.certifiedhacker.com => No record found.
[*] zera.certifiedhacker.com => No record found.
[*] young.certifiedhacker.com => No record found.
[*] zeus.certifiedhacker.com => No record found.
[*] zlog.certifiedhacker.com => No record found.
[*] za.certifiedhacker.com => No record found.
[*] zebra.certifiedhacker.com => No record found.
[*] z-log.certifiedhacker.com => No record found.
[*] zm.certifiedhacker.com => No record found.
[*] zulu.certifiedhacker.com => No record found.
[*] zw.certifiedhacker.com => No record found.

-----
SUMMARY

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

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

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

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

```

Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
-----  

SUMMARY  

-----  

[*] 22 total (19 new) hosts found.  

[recon-ng][CEH][brute_hosts] > modules load reverse_resolve  

[*] Multiple modules match 'reverse_resolve'.  

Recon  

-----  

recon/hosts-hosts/reverse_resolve  

recon/netblocks-hosts/reverse_resolve  

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

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

[*] Country: None  

[*] Host: box5331.bluehost.com  

[*] Ip_Address: 162.241.216.11  

[*] Latitude: None  

[*] Longitude: None  

[*] Notes: None  

[*] Region: None  

[*]  

[*] 127.0.0.1 => No record found.  

-----  

SUMMARY  

-----  

[*] 1 total (1 new) hosts found.  

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

```

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

```

Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
-----  

SUMMARY  

-----  

[*] 1 total (1 new) hosts found.  

[recon-ng][CEH][reverse_resolve] > show hosts  

+-----+
| rowid | module | host | ip_address | region | country | latitude | longitude |
| notes | | | | | | | |
+-----+
| 1 | brute_hosts | autodiscover.certifiedhacker.com | 162.241.216.11 | | | | |
| 2 | brute_hosts | blog.certifiedhacker.com | 162.241.216.11 | | | | |
| 3 | brute_hosts | events.certifiedhacker.com | 162.241.216.11 | | | | |
| 4 | brute_hosts | certifiedhacker.com | | | | | |
| 5 | brute_hosts | ftp.certifiedhacker.com | | | | | |
| 6 | brute_hosts | mail.certifiedhacker.com | | | | | |
| 7 | brute_hosts | imap.certifiedhacker.com | | | | | |
| 8 | brute_hosts | imap.certifiedhacker.com | | | | | |
| 9 | brute_hosts | | | | | | |

```

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

```

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

```

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

32. Type the **modules load reporting** command and press **Enter** to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is **reporting/html**.

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

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

35. Type:

options set FILENAME /home/attacker/Desktop/results.html and press **Enter**. By issuing this command, you are setting the report name as **results.html** and the path to store the file as **Desktop**.

options set CREATOR [your name] (here, **Jason**) and press **Enter**.

options set CUSTOMER Certifiedhacker Networks (since you have performed network reconnaissance on **certifiedhacker.com** domain) and press **Enter**.

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

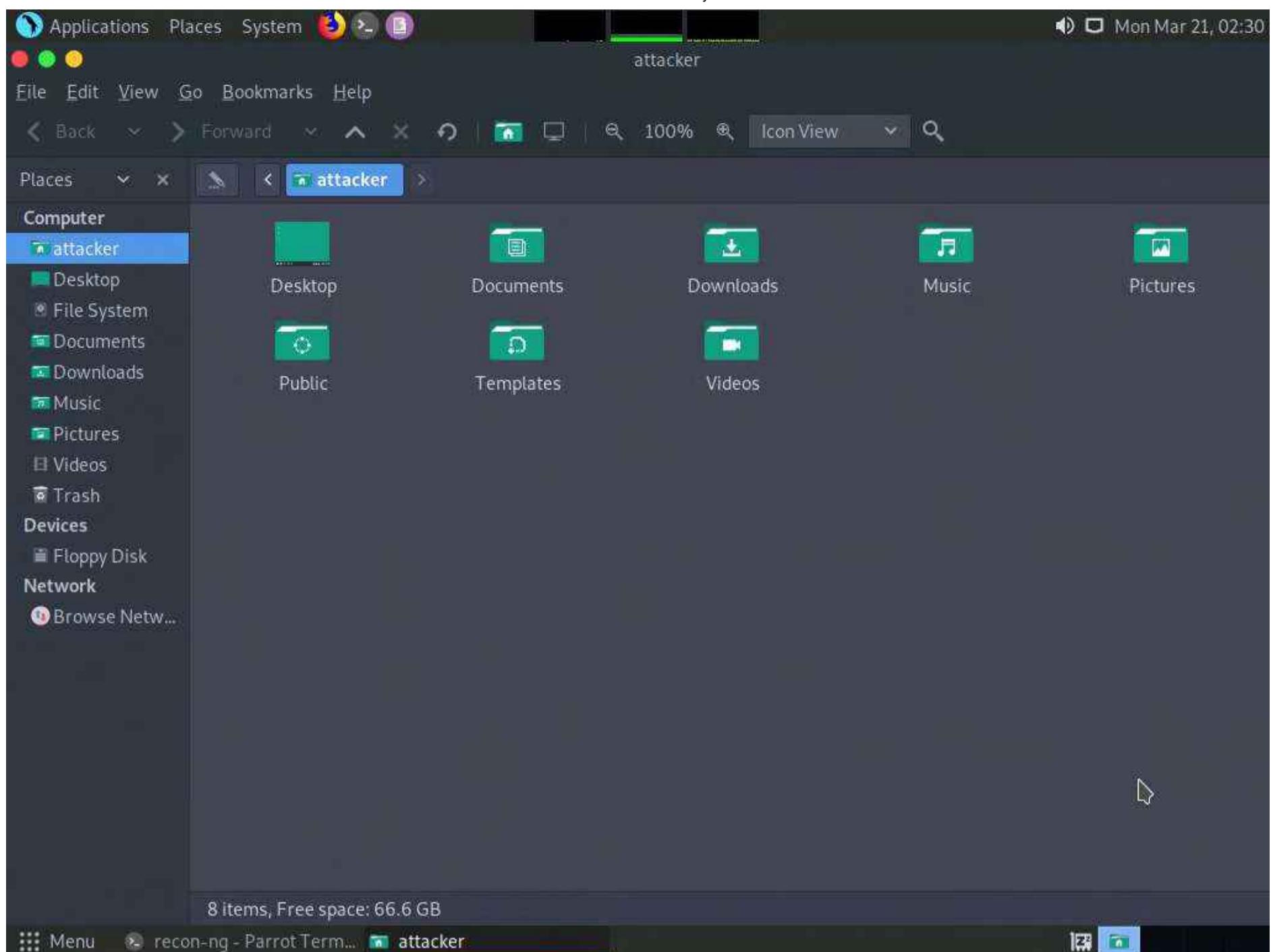
```
| reverse_resolve |  
----+  
[*] 20 rows returned  
[recon-ng][CEH][reverse_resolve] > back  
[recon-ng][CEH] > modules load reporting  
[*] Multiple modules match 'reporting'.  
  
Reporting  
----  
reporting/csv  
reporting/html  
reporting/json  
reporting/list  
reporting/proxifier  
reporting/pushpin  
reporting/xlsx  
reporting/xml  
  
[recon-ng][CEH] > modules load reporting/html  
[recon-ng][CEH][html] > options set FILENAME /home/attacker/Desktop/results.html  
FILENAME => /home/attacker/Desktop/results.html  
[recon-ng][CEH][html] > options set CREATOR Jason  
CREATOR => Jason  
[recon-ng][CEH][html] > options set CUSTOMER Certifiedhacker Networks  
CUSTOMER => Certifiedhacker Networks  
[recon-ng][CEH][html] > run  
[*] Report generated at '/home/attacker/Desktop/results.html'.  
[recon-ng][CEH][html] > |  
Menu  reconn...  reconn- Parrot Term...  Help
```

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

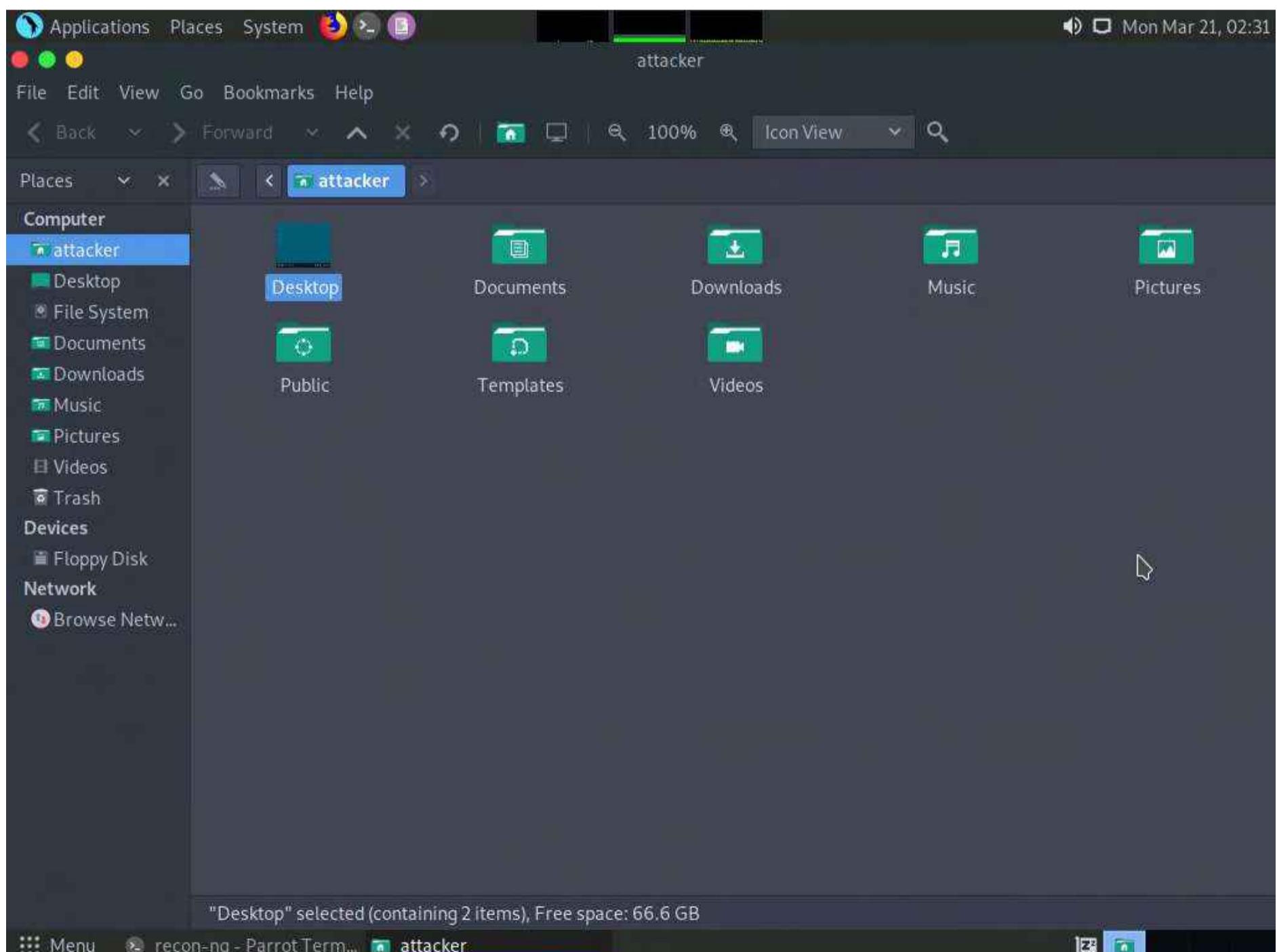
38. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

39. The **attacker** window appears.

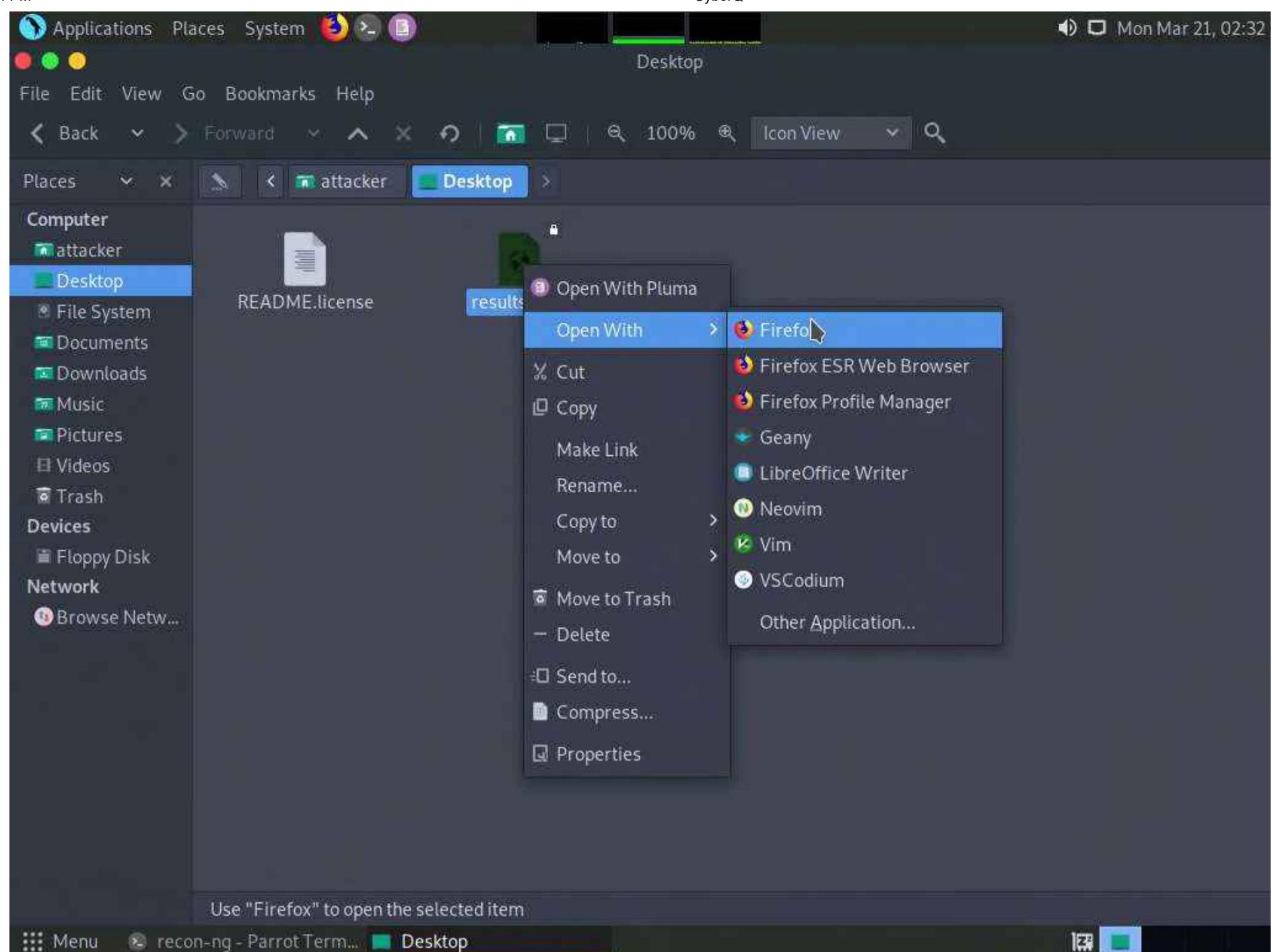




40. In the **attacker** window, double-click **Desktop**.



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.

The screenshot shows a Mozilla Firefox browser window with the title 'Recon-ng Reconnaissance Report - Mozilla Firefox'. The address bar shows the URL 'file:///home/attacker/Desktop/results.html'. The main content area displays a 'Certifiedhacker Networks Recon-ng Reconnaissance Report'. Below the title, there is a section titled '[+] Summary' containing a table:

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

Below the summary, there are two expandable sections: '[+] Domains' and '[+] Hosts'. At the bottom of the page, it says 'Created by: Jason Mon, Mar 21 2022 02:26:56'. The browser's toolbar and status bar are visible at the bottom of the screen.

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

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

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

44. Close all open windows.

45. Until now, we have used the Recon-NG tool to perform network reconnaissance on a target domain

46. Now, we will use Recon-NG to gather personnel information.

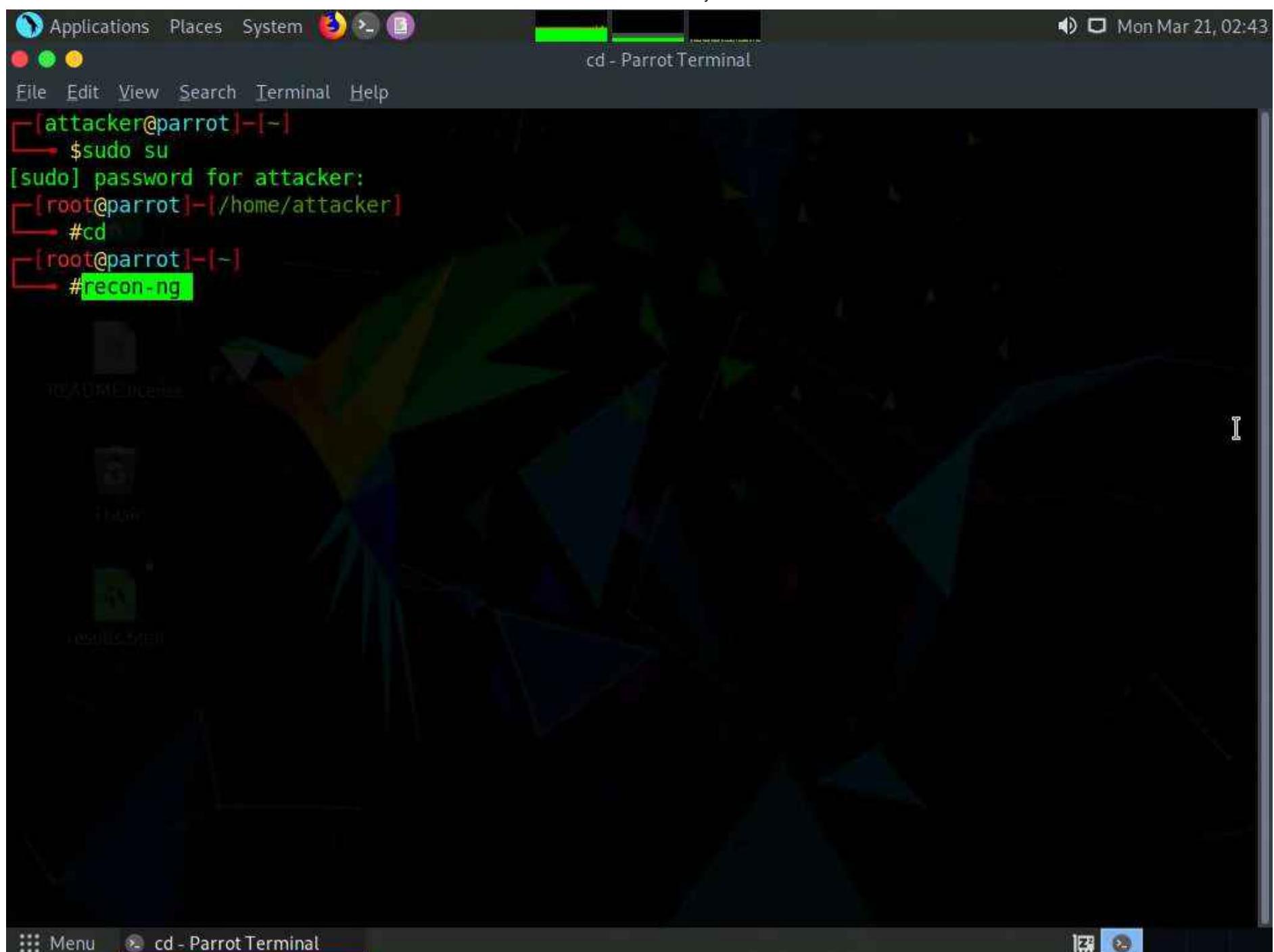
47. Open a new **Parrot Terminal** window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

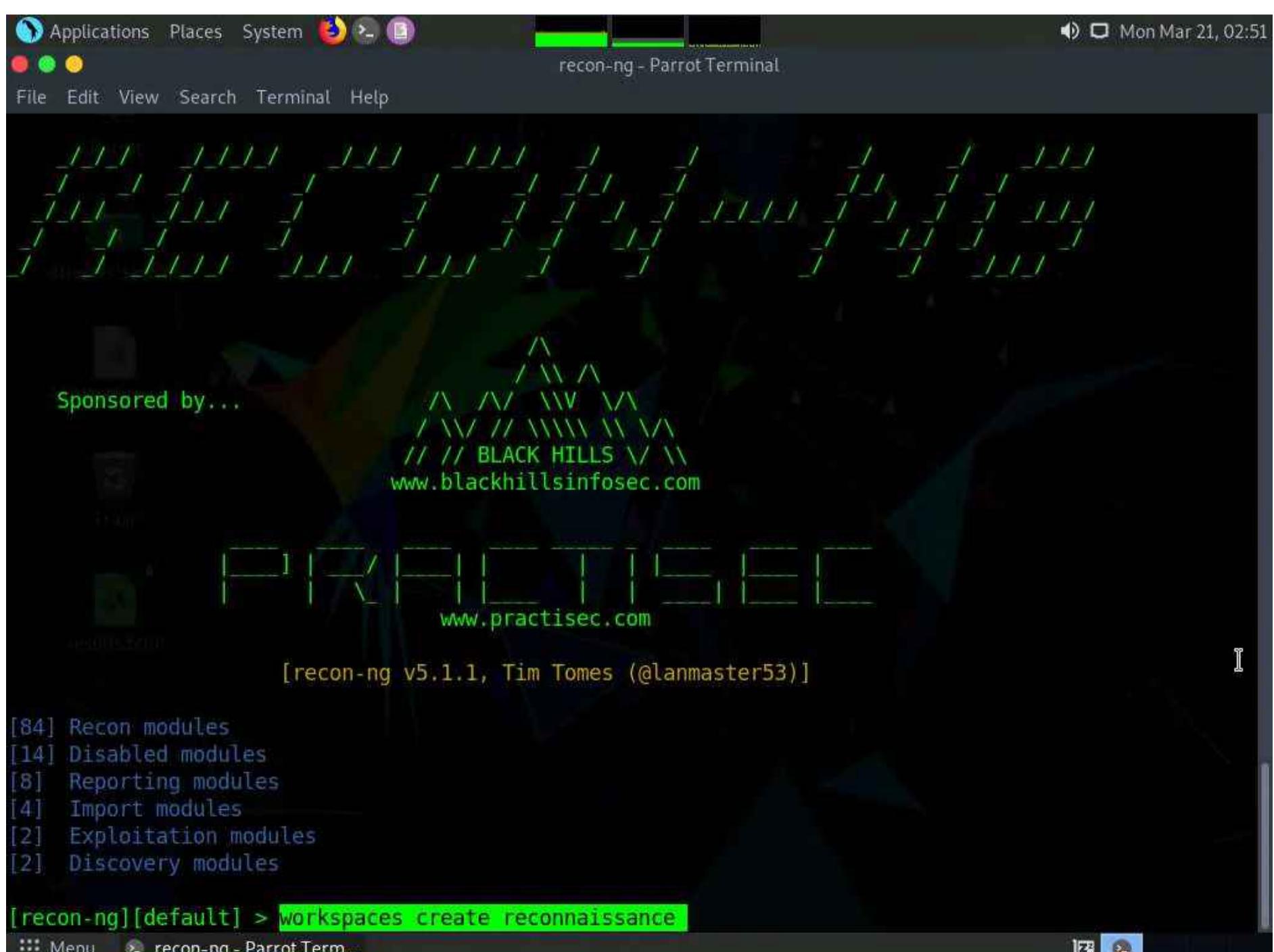
Note: The password that you type will not be visible.

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

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



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.

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

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

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

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

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

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

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

Note: Results might differ when you perform the lab.

```
[recon-ng][reconnaissance][whois_pocs] > run
-----
FACEBOOK.COM
-----
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First Name: Brandon
[*] Last Name: Stout
[*] Middle Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First Name: None
[*] Last Name: Operations
[*] Middle Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
[*] Title: Whois contact
[*]
-----
```

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**.

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

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.



```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][hackertarget] > run

-----[REDACTED]-----
CERTIFIEDHACKER.COM
-----
[*] Country: None
[*] Host: www.fleet.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
-----
[*] Country: None
[*] Host: iam.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
-----
[*] Country: None
[*] Host: www.sftp.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
-----[REDACTED]-----
```

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.

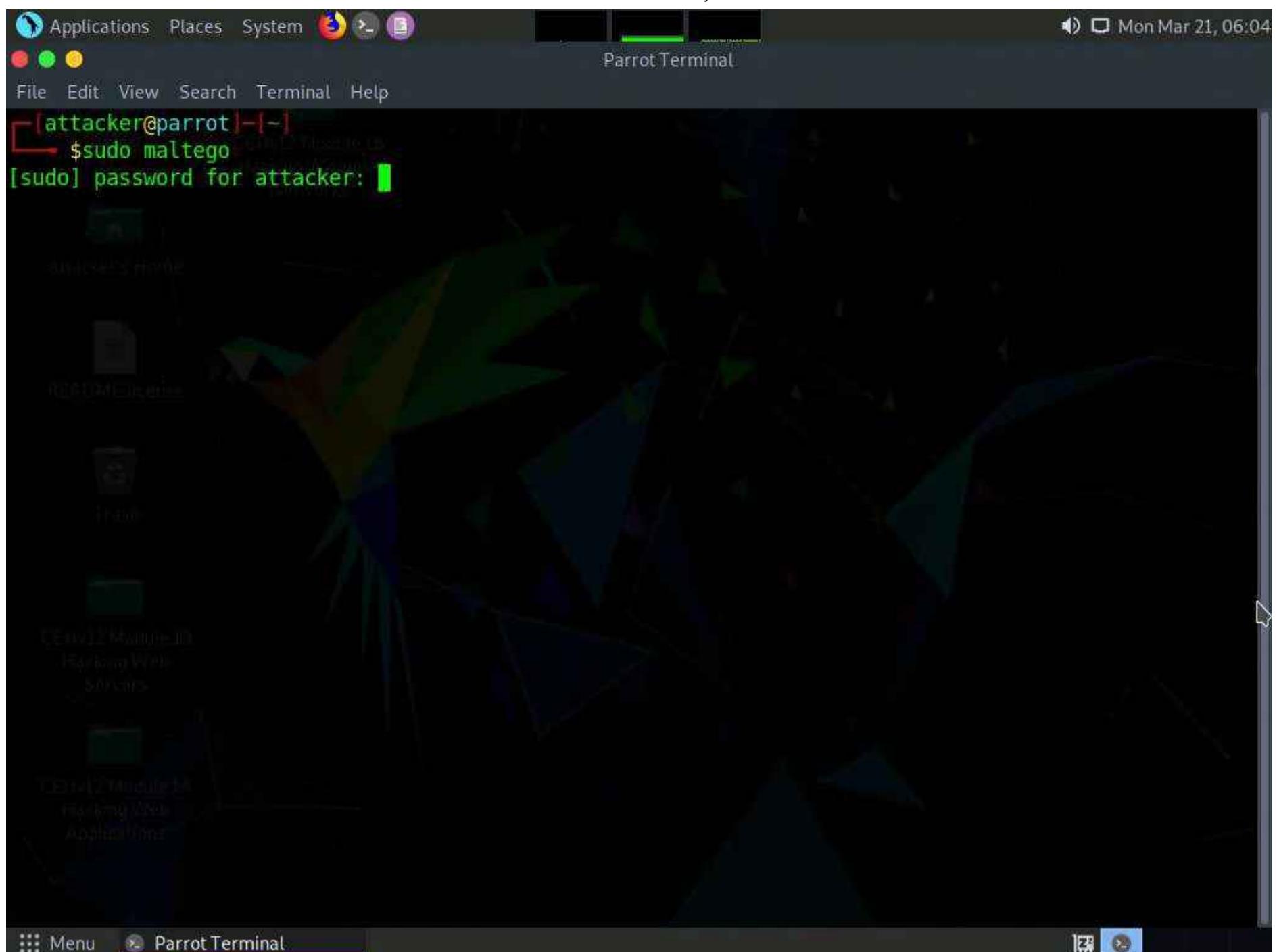
Here, we will gather a variety of information about the target organization using Maltego.

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**.

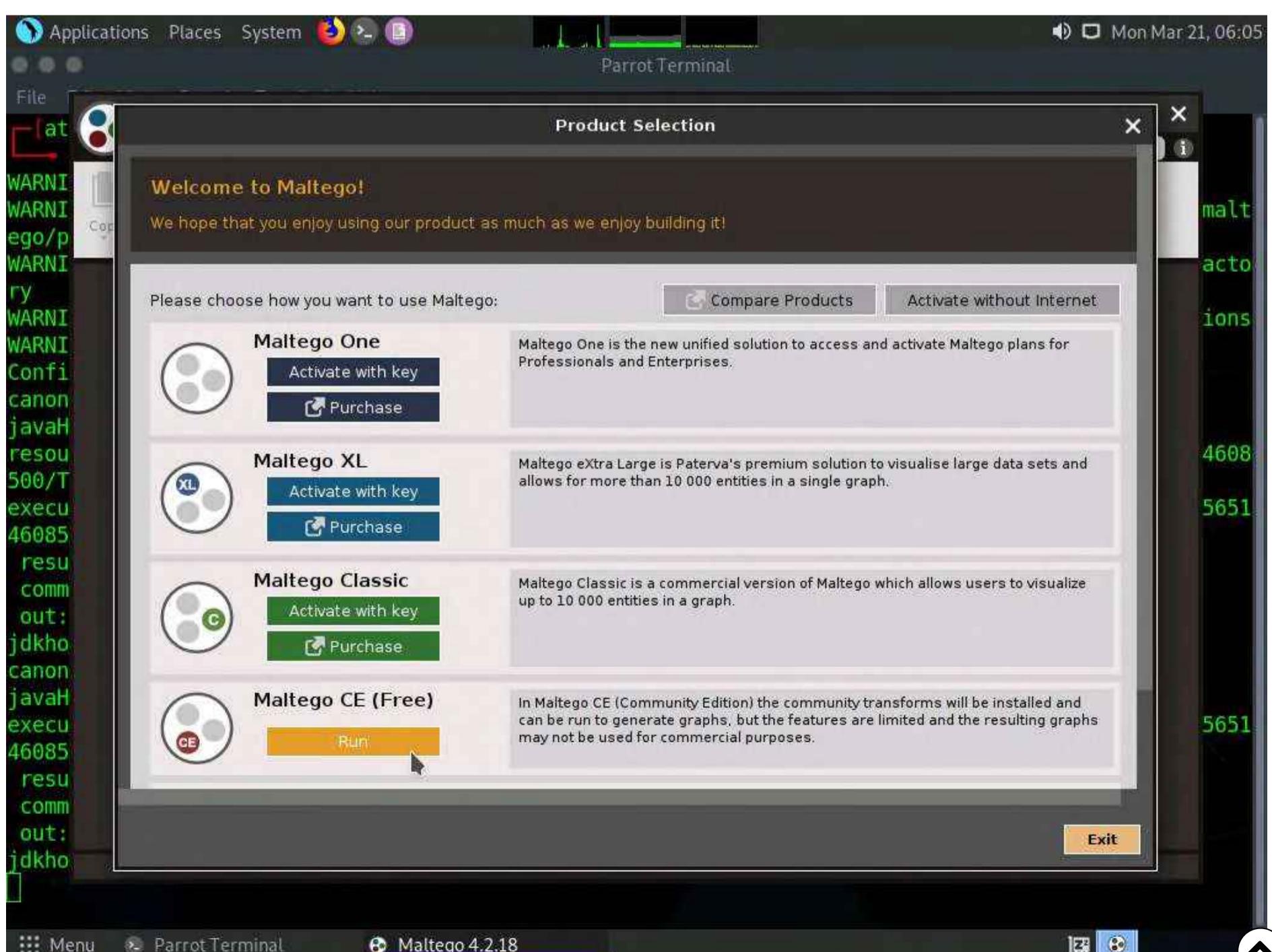
Note: In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.



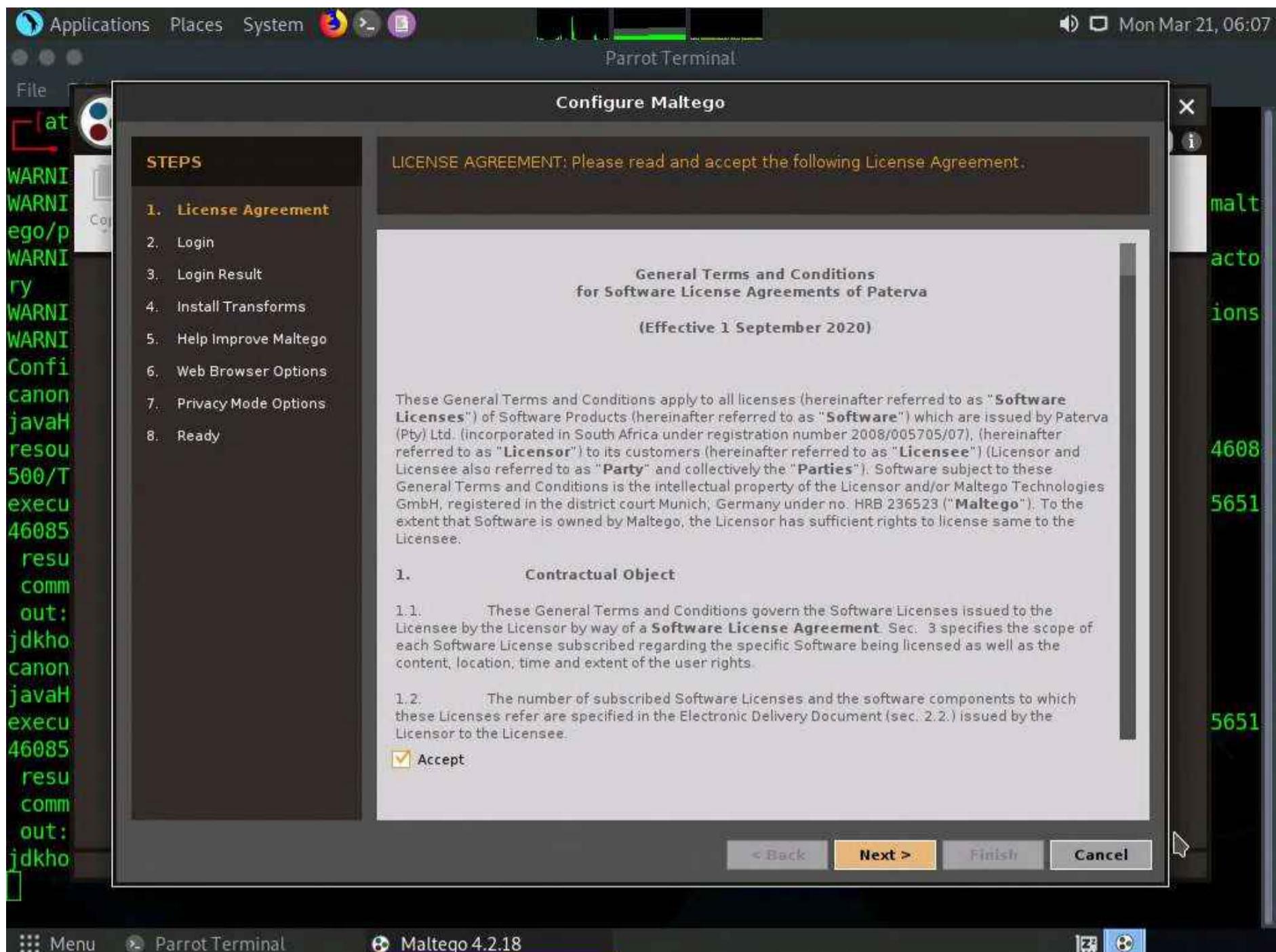


2. A Product Selection wizard appears on the Maltego GUI; click **Run** from **Maltego CE (Free)** option.

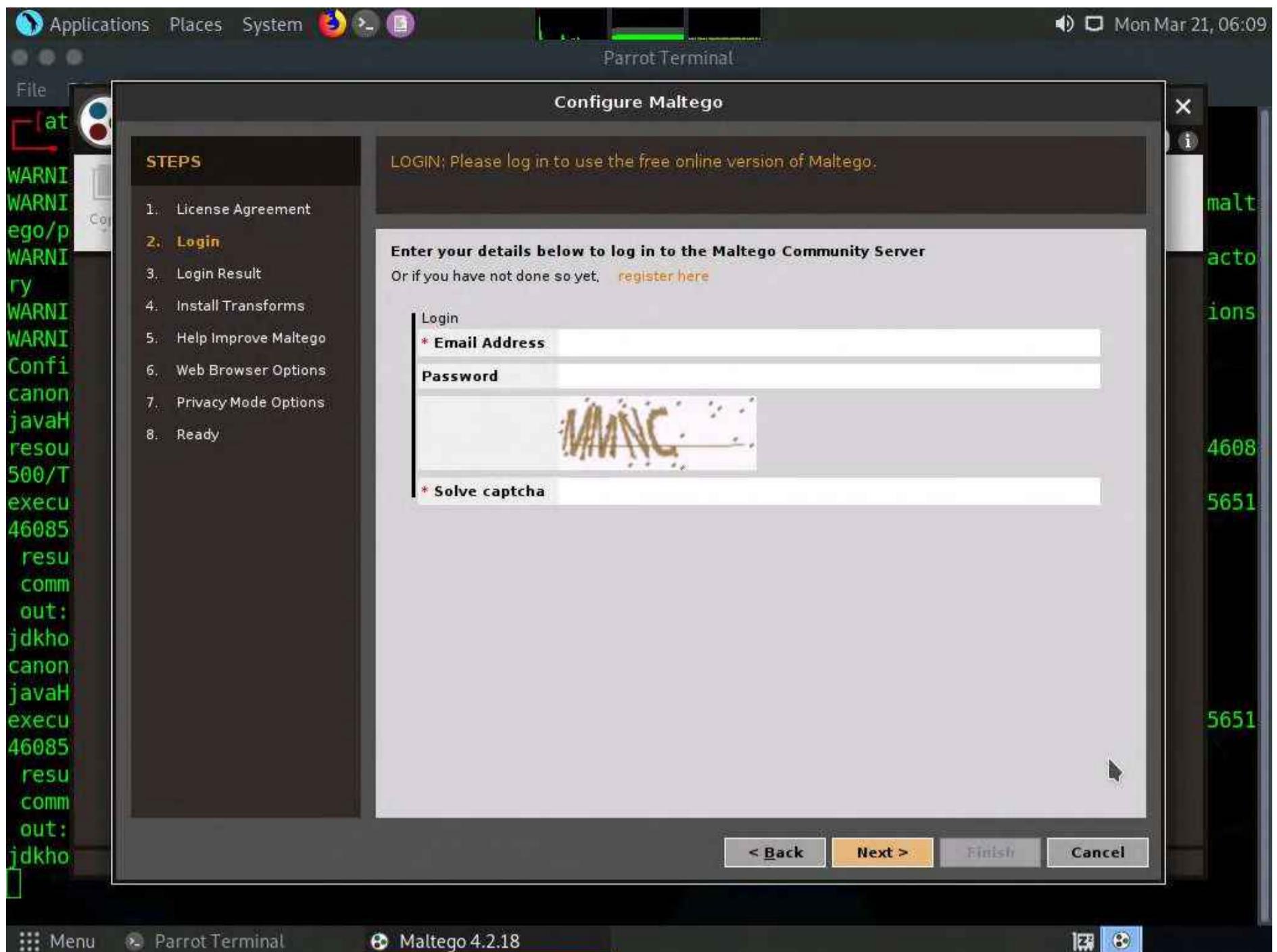
Note: If the **Memory Settings Optimized** pop-up appears, click **Restart Now**.



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.

PASSWORD *

REPEAT PASSWORD *

I'm not a robot

REGISTER

[Paterva Data Privacy Policy](#)

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

close

Mail Sent!

Please check your mailbox to confirm your account.

LEARN MALTEGO

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.

The screenshot shows a Gmail inbox with 54 unread messages. An email from "Maltego CE Account Confirmation" is selected, with the subject "Maltego CE Account Confirmation" visible in the header. The email body contains a message to the recipient, a link to activate the account, and links to learn about new features and documentation.

Subject: Maltego CE Account Confirmation

Message Preview:

Dear [REDACTED]

Thank you for registering for the Maltego Community Edition. To activate your account, please click this link:

<https://www.maltego.com/ce-user-activate?code=120567b8-0594-44cd-a60e-69115c1ae4b8/>

To learn about new features and product updates, please check out <https://www.maltego.com/blog/>.

To get started, check out our [documentation](#), [tutorials](#) and our new video series for beginners - [Maltego Essentials](#).

Kind regards,
The Maltego Team

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

The screenshot shows the Maltego website with the title "Account Successfully Activated! - Maltego - Mozilla Firefox". The main content area displays a large heading "Account Successfully Activated!" and a message stating that the account has been successfully activated and can now be logged into directly. It includes a yellow "BUY ONLINE" button and a yellow "GET QUOTE" button. A yellow "DOWNLOAD MALTEGO" button is also present. A circular button labeled "Get a demo" with a cursor icon is visible on the right.

Page Title: Account Successfully Activated! - Maltego - Mozilla Firefox

Content:

MALTEGO

BUY ONLINE

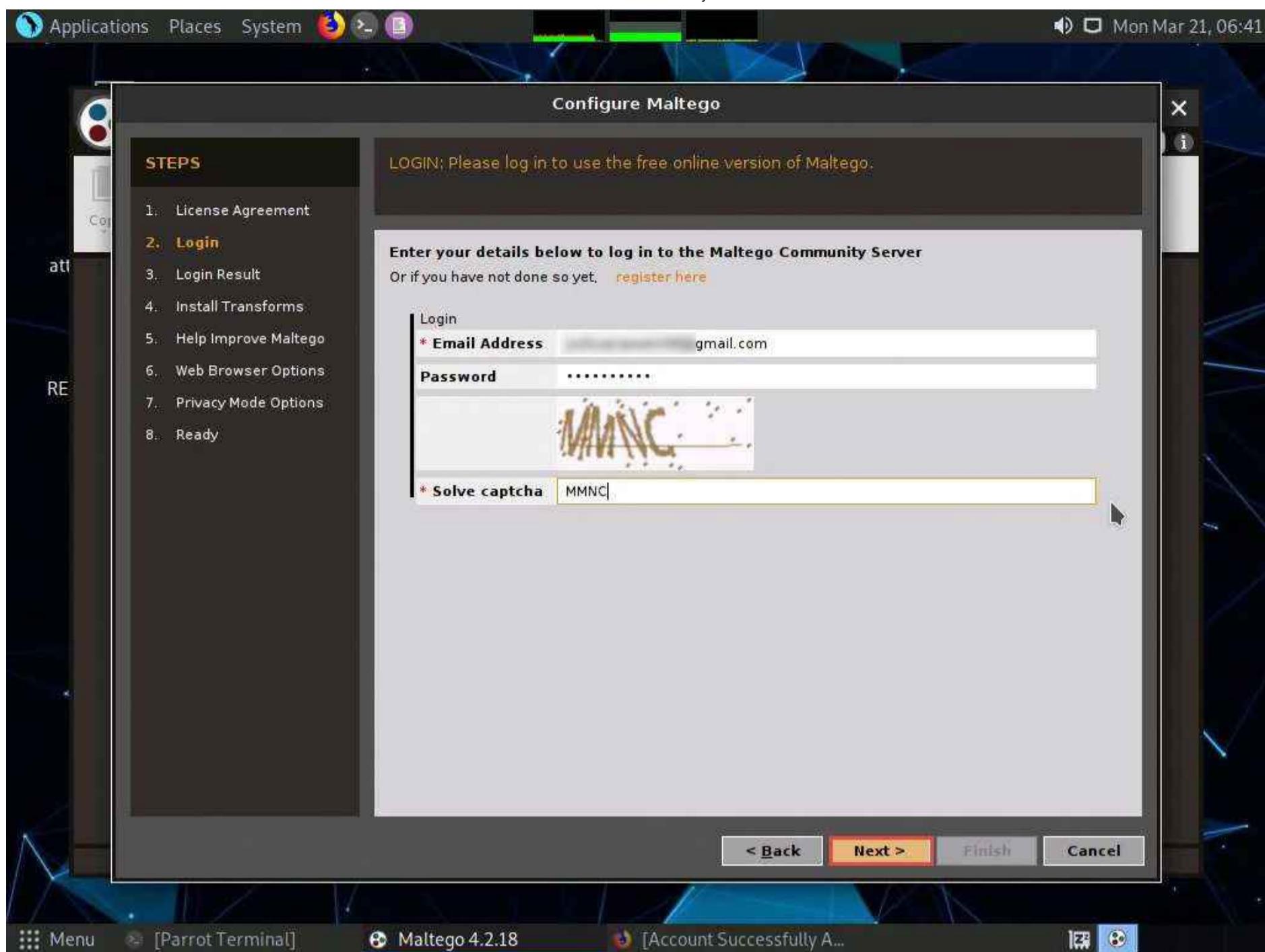
GET QUOTE

DOWNLOAD MALTEGO

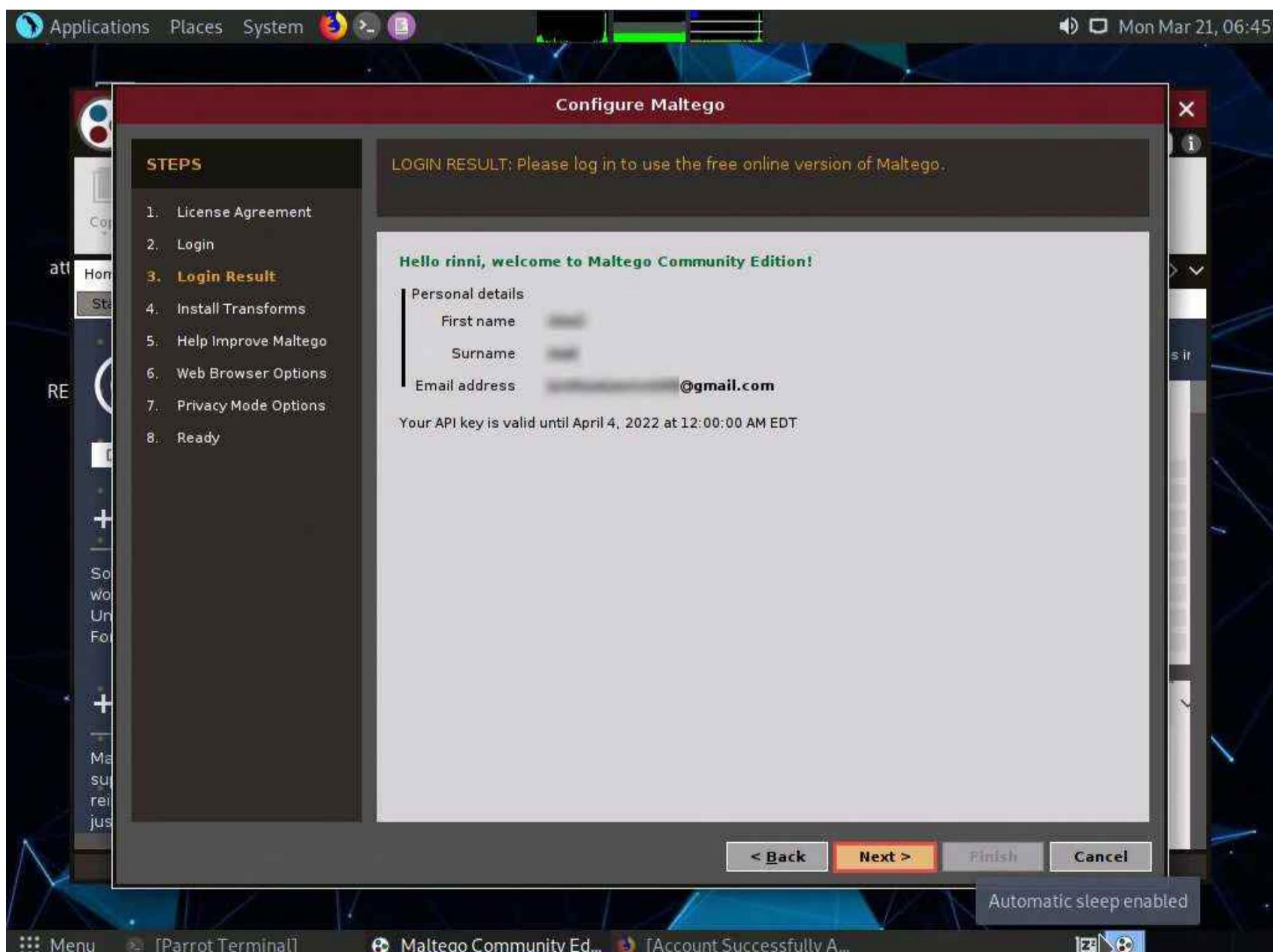
Get a demo

If you haven't already downloaded and installed the Maltego Desktop Client, download it here.

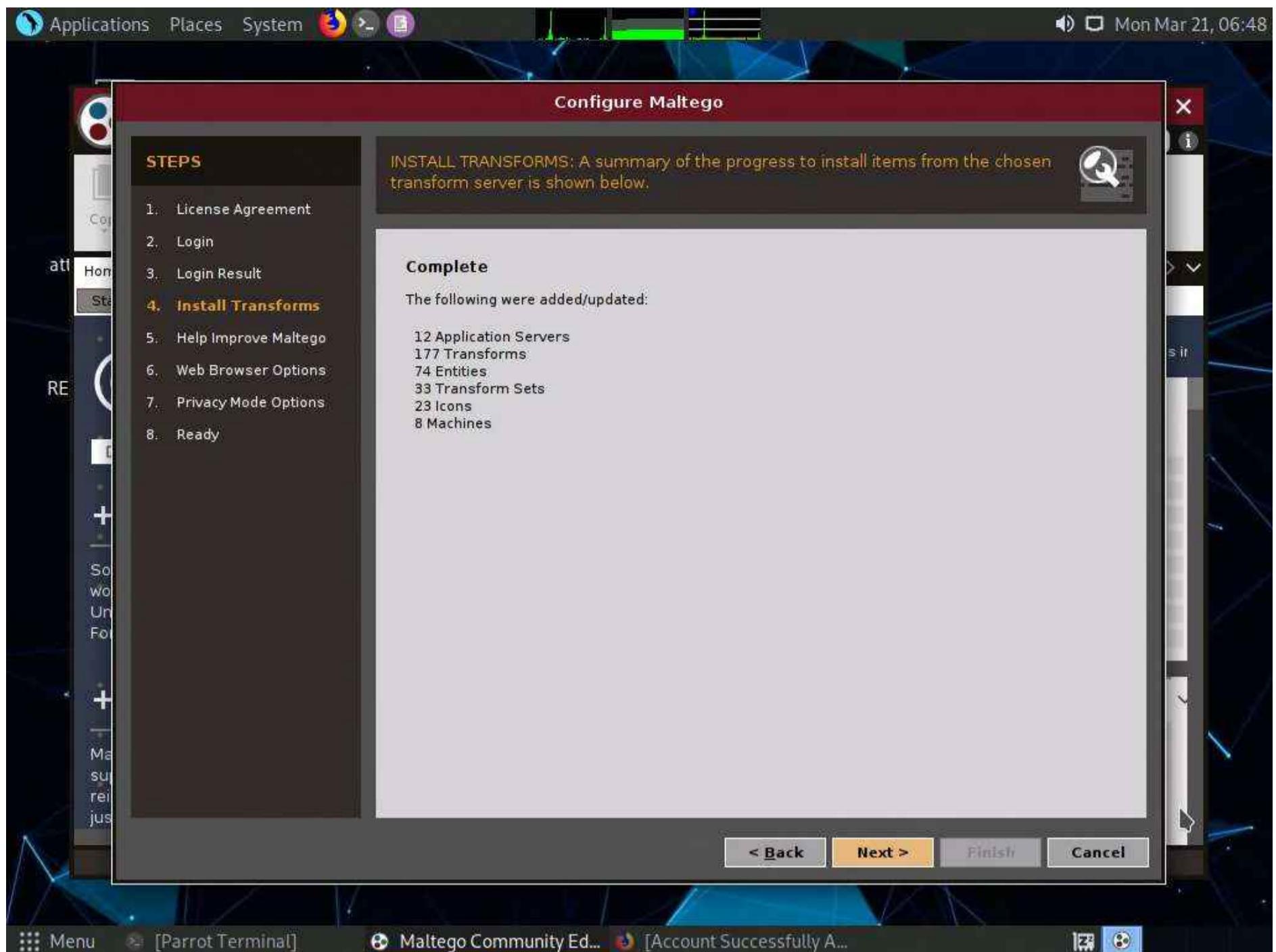
10. Minimize the web browser and go back to the setup wizard and enter the **Email Address** and **Password** specified at the time of registration; solve the captcha and click **Next**.



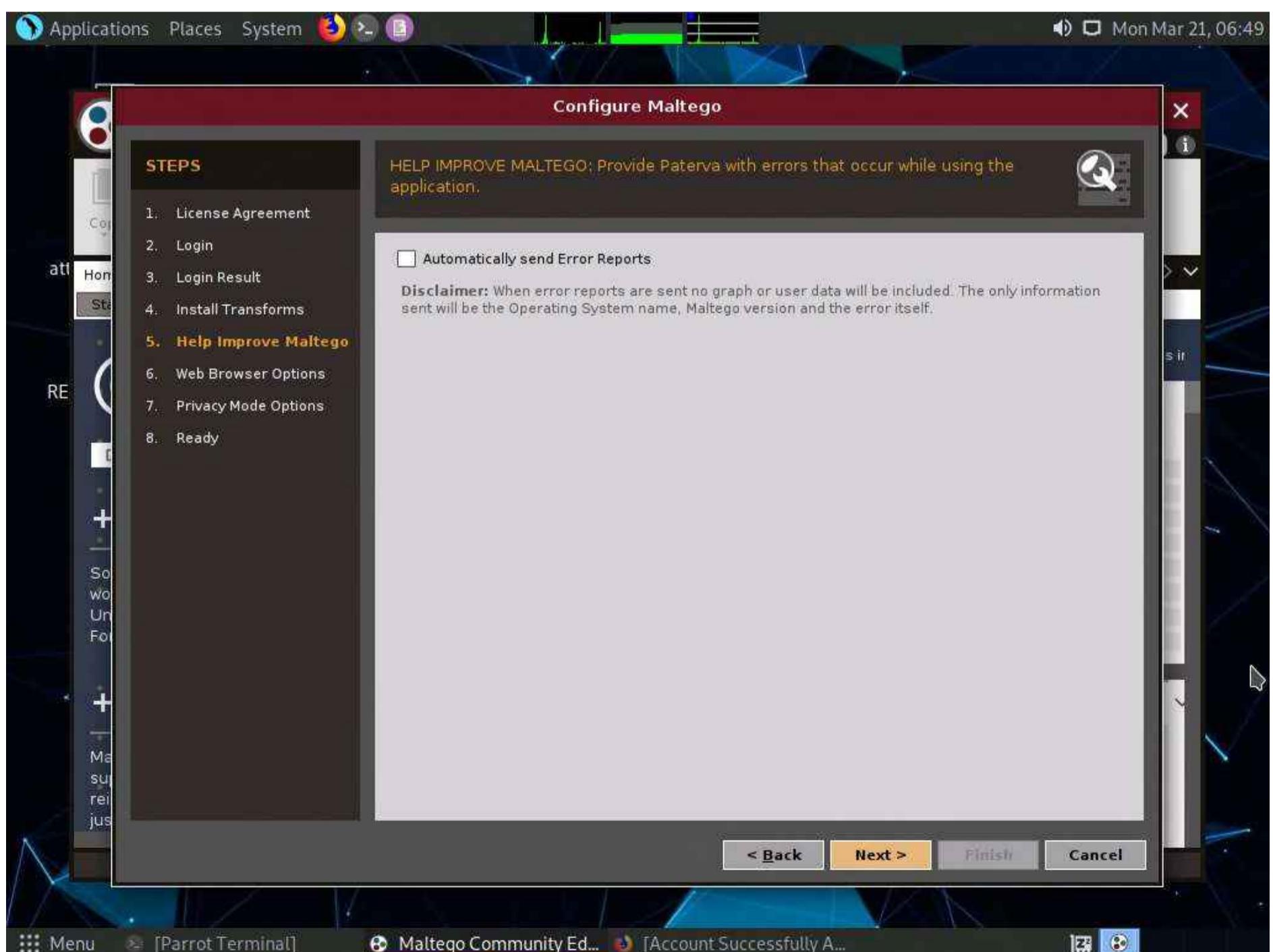
11. The **Login Result** section displays your personal details; click **Next**.



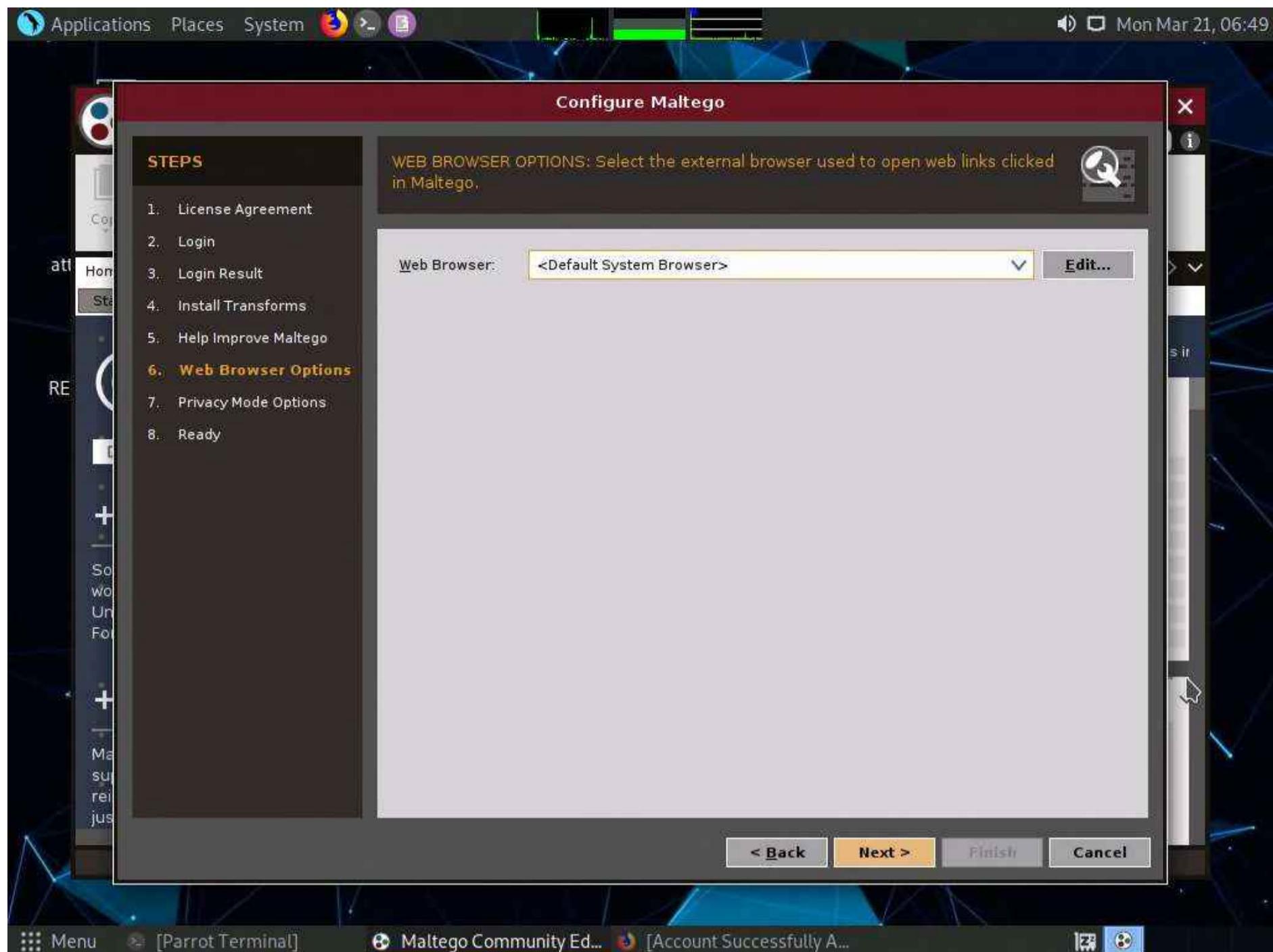
12. The **Install Transforms** section appears, which will install items from the chosen transform server. Leave the settings to default and click **Next**.



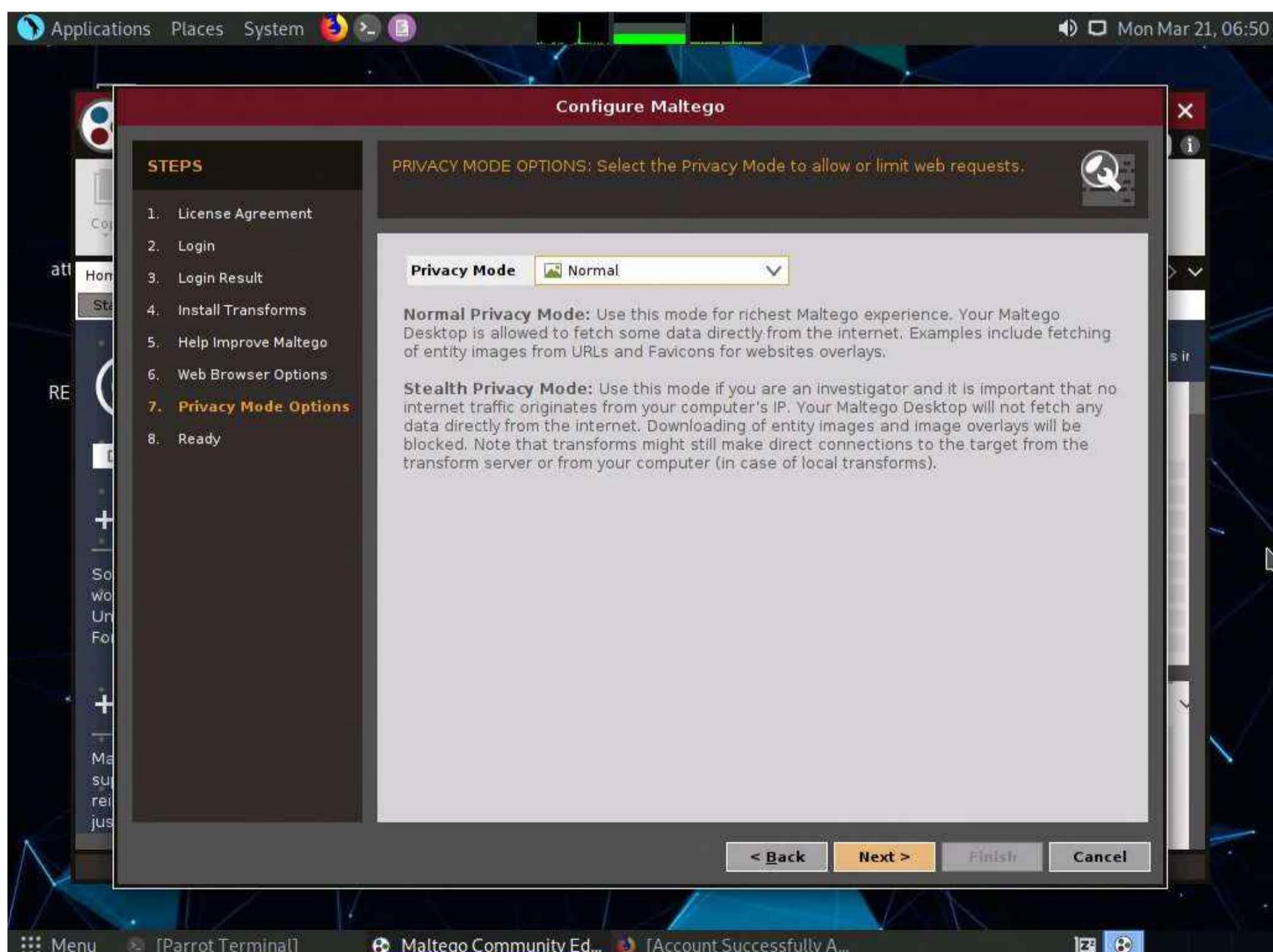
13. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.



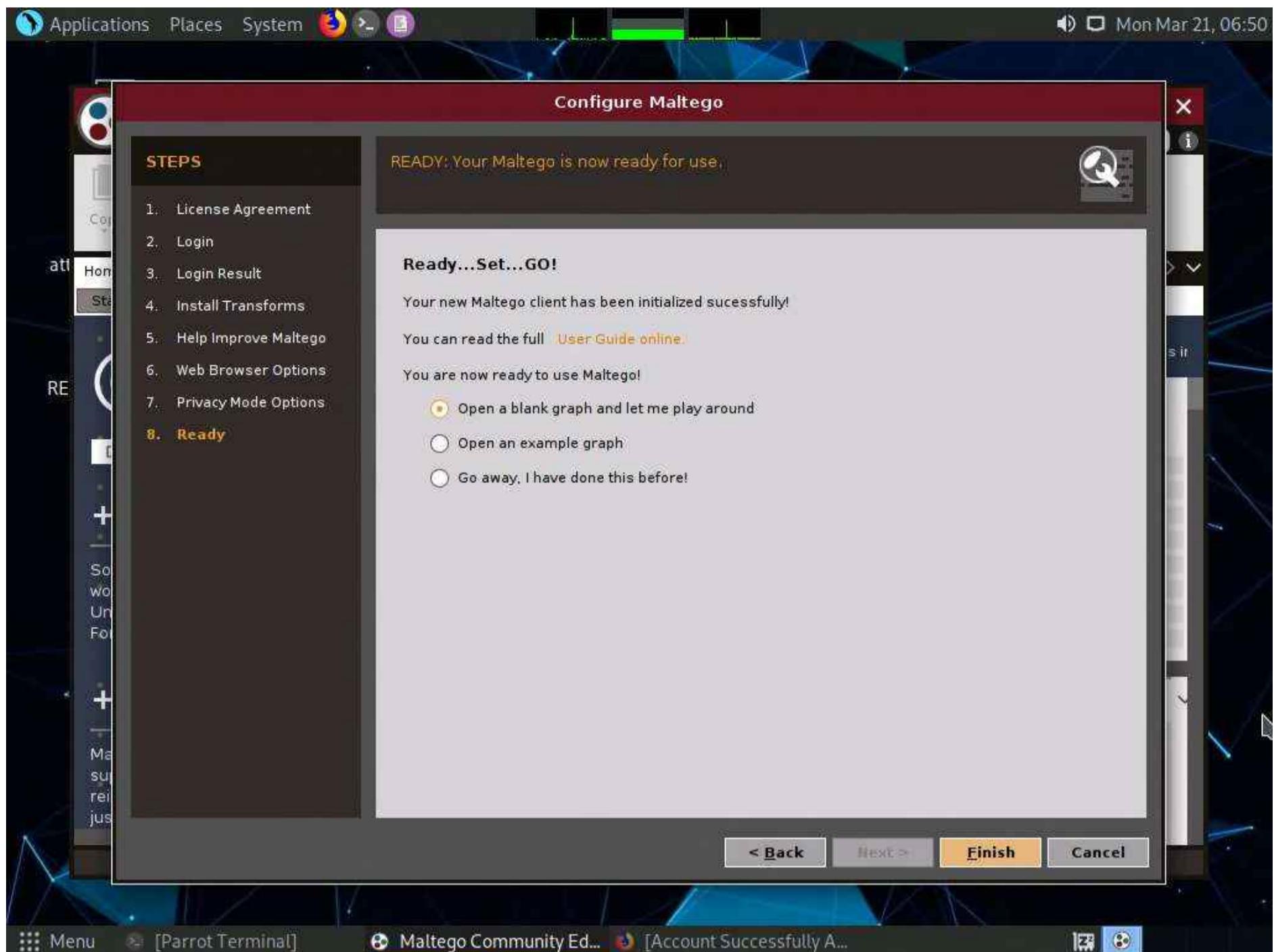
14. The **Web Browser Options** section appears. Leave the options set to default and click **Next**.



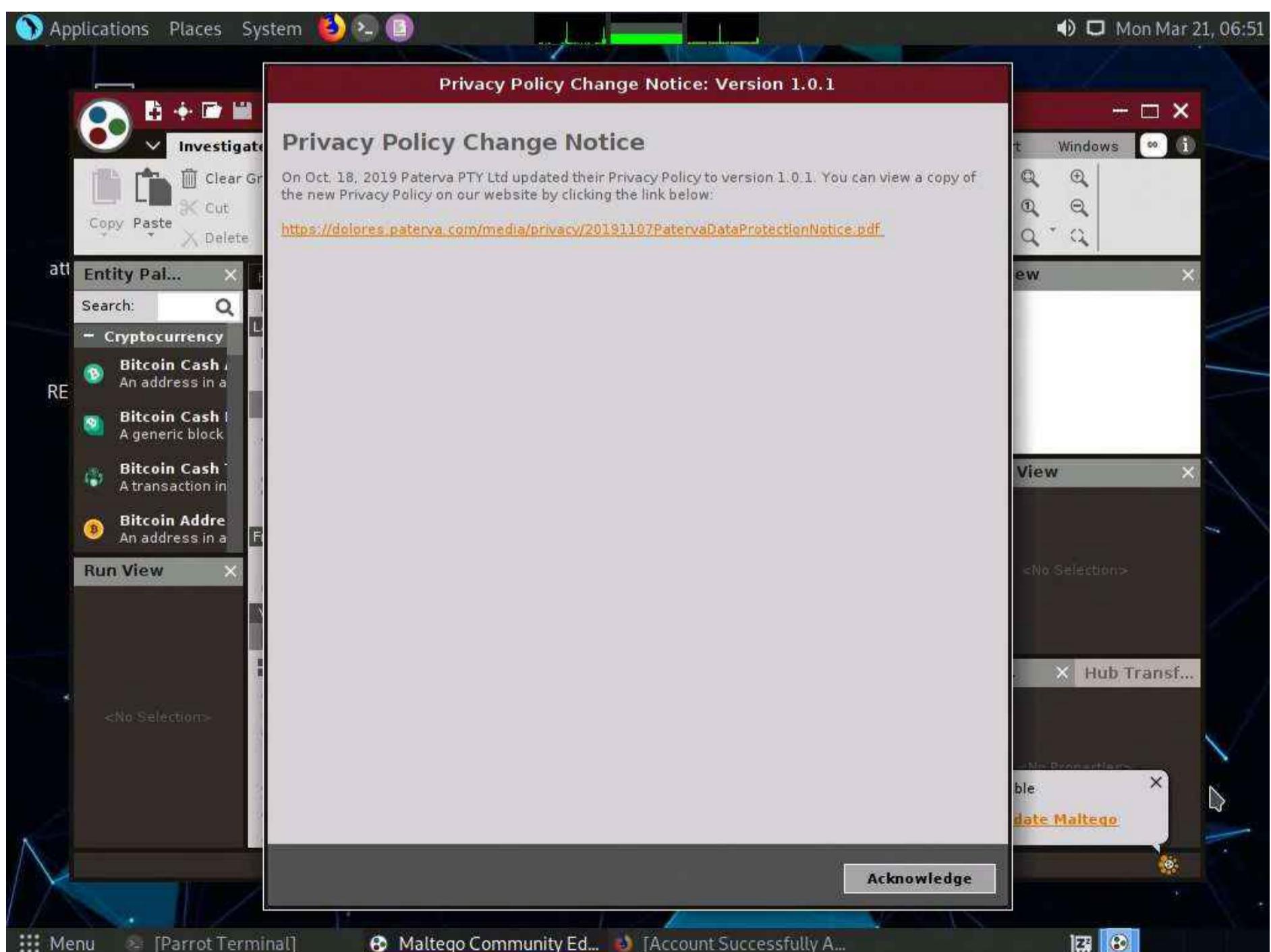
15. The **Privacy Mode Options** section appears. Leave the options set to default and click **Next**.



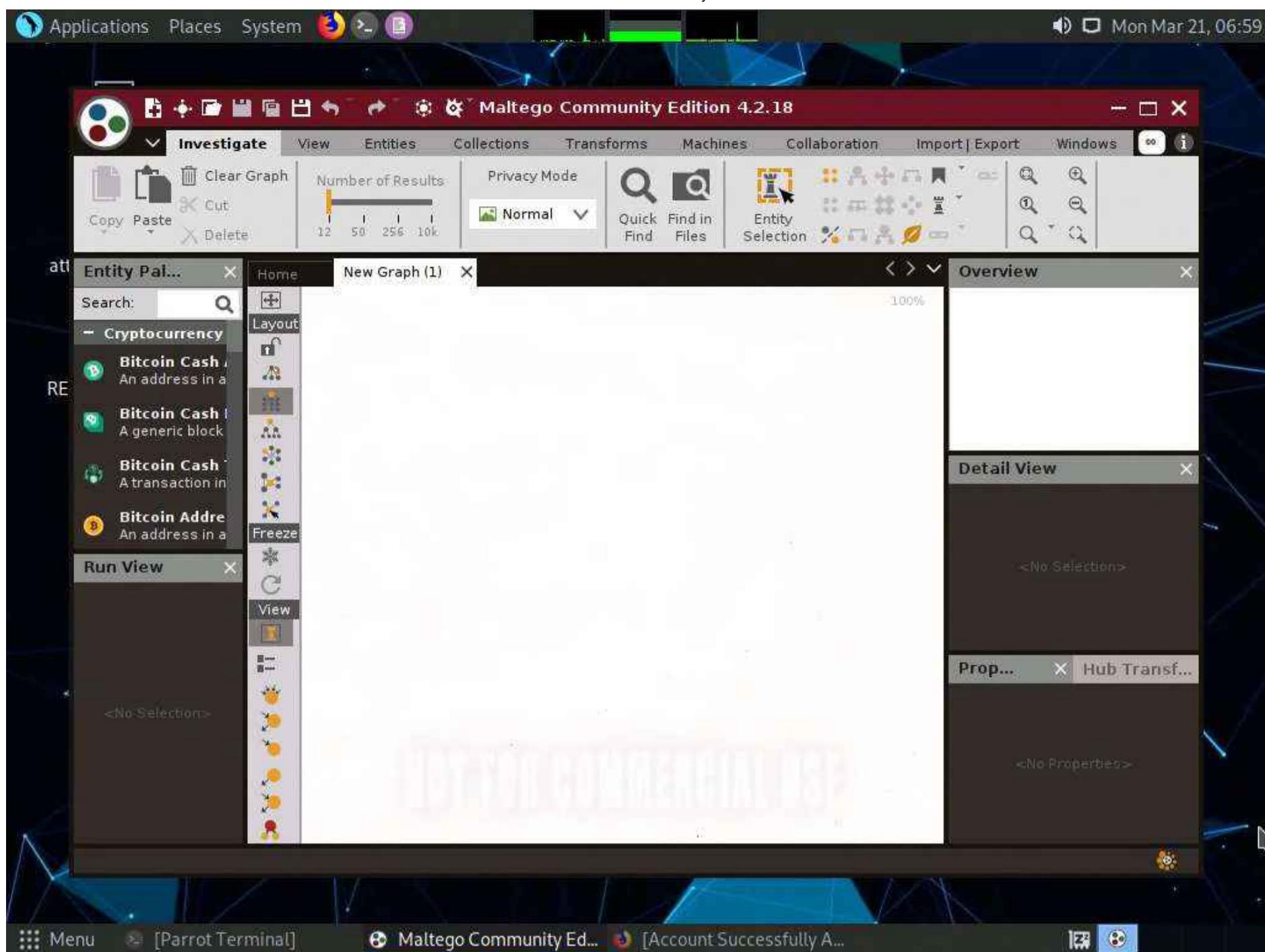
16. The **Ready** section appears, select **Open a blank graph and let me play around** option and click **Finish**.



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.

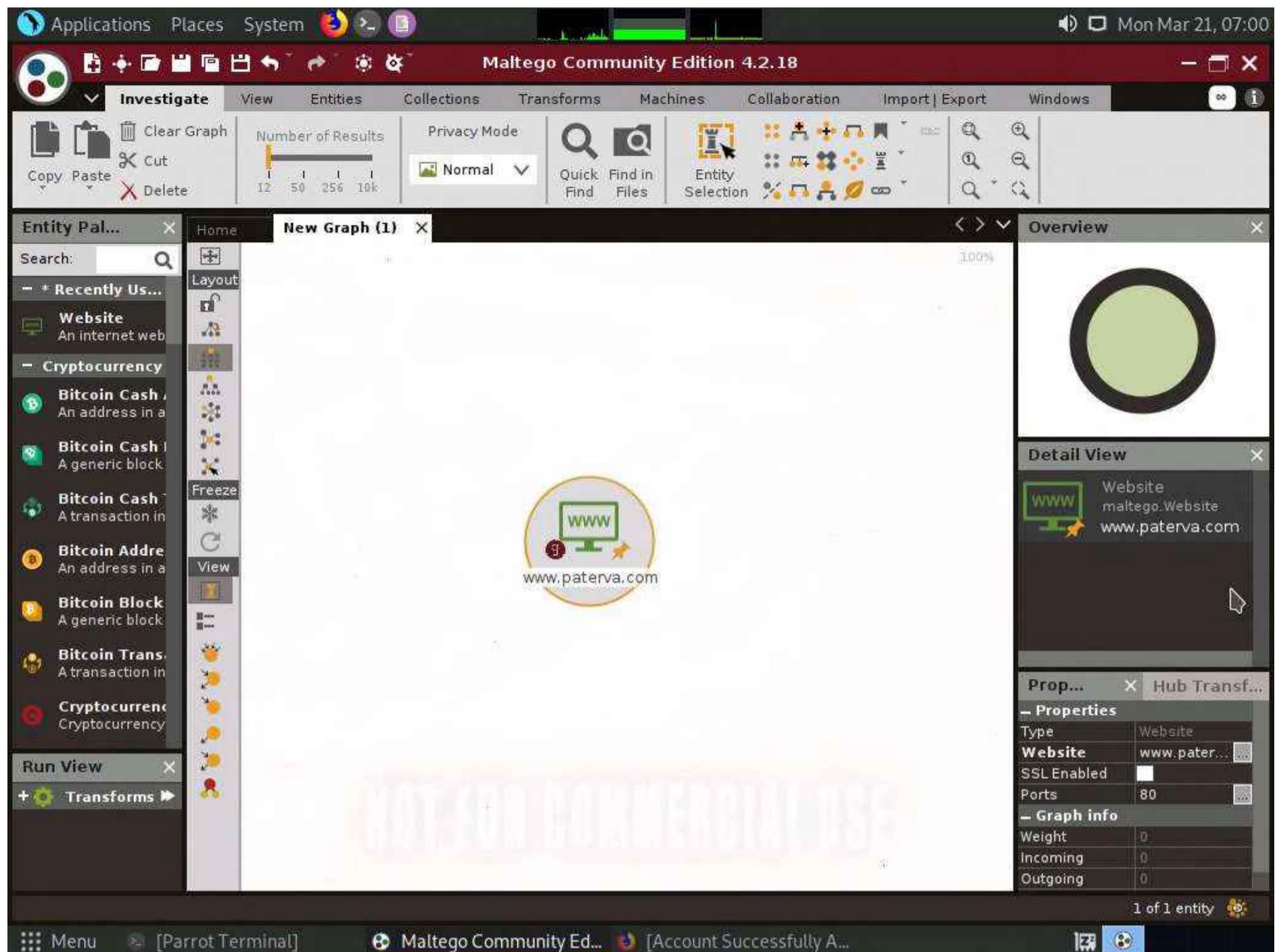


19. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS**, **DNS Name**, **Domain**, **IPv4 Address**, **URL**, **Website**,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

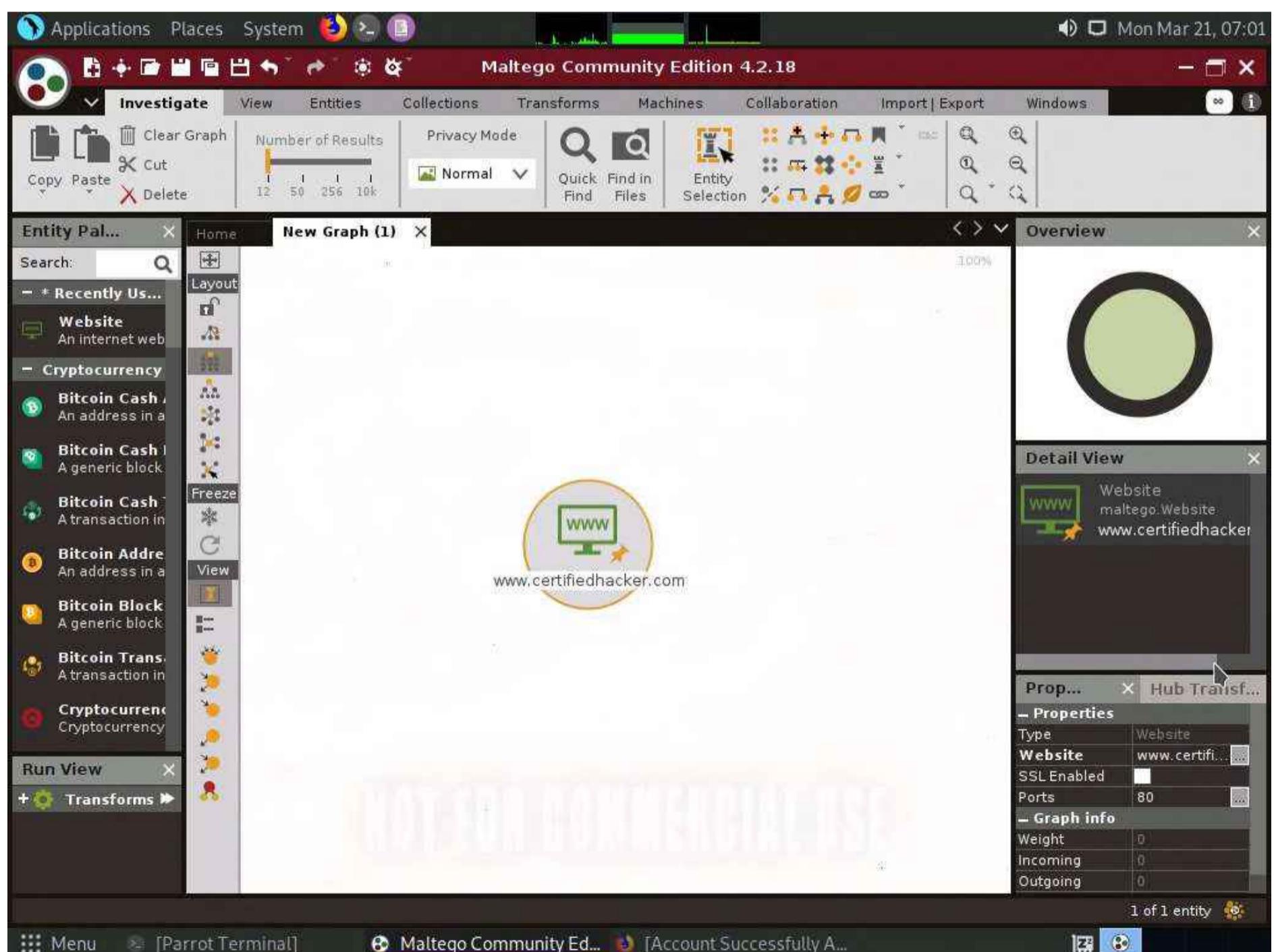
20. Drag the **Website** entity onto the **New Graph (1)** window.

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

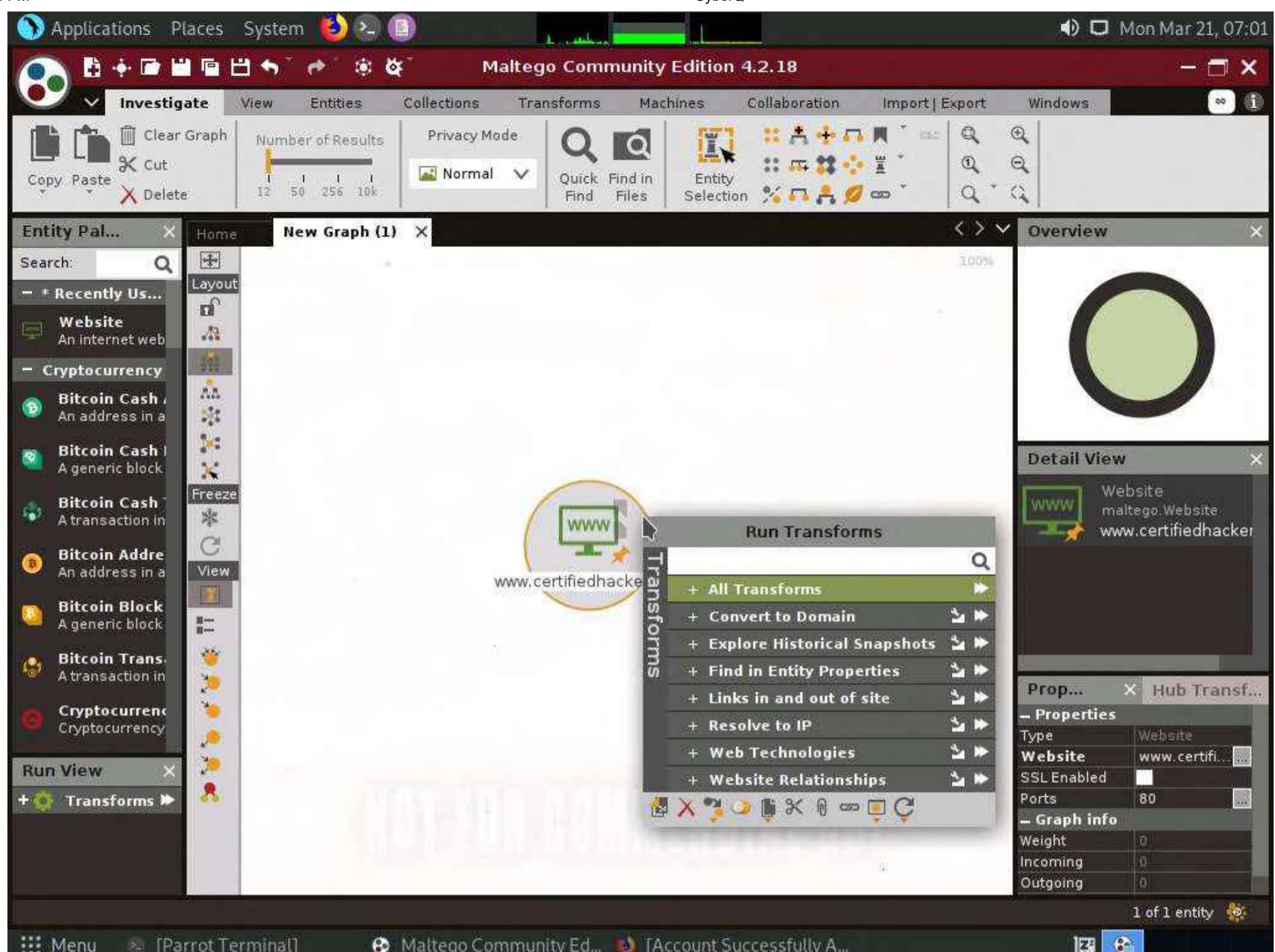
Note: If you are not able to view the entity as shown in the screenshot, click in **the New Graph (1)** window and **scroll up**, which will increase the size of the entity.



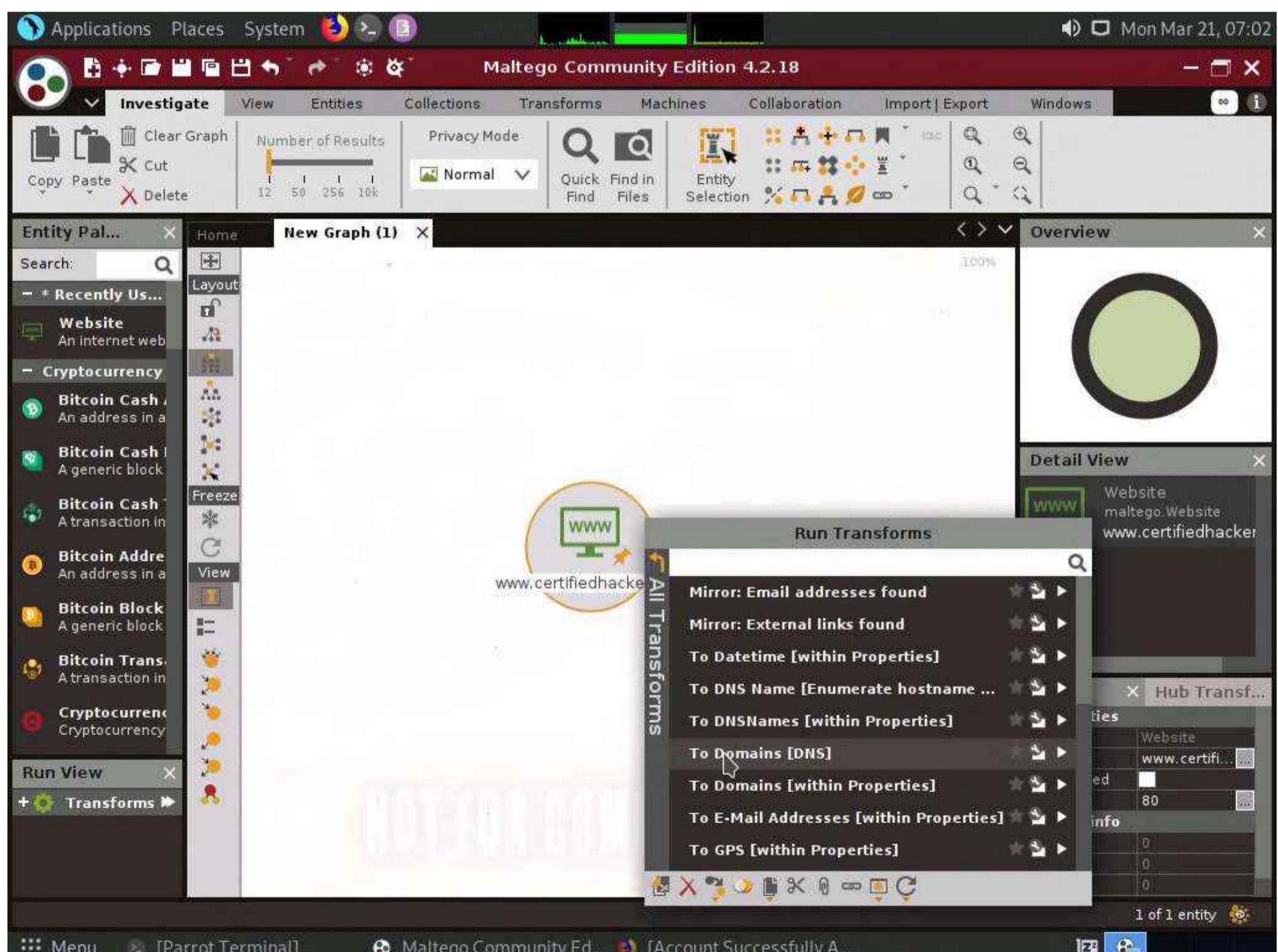
22. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press **Enter**.



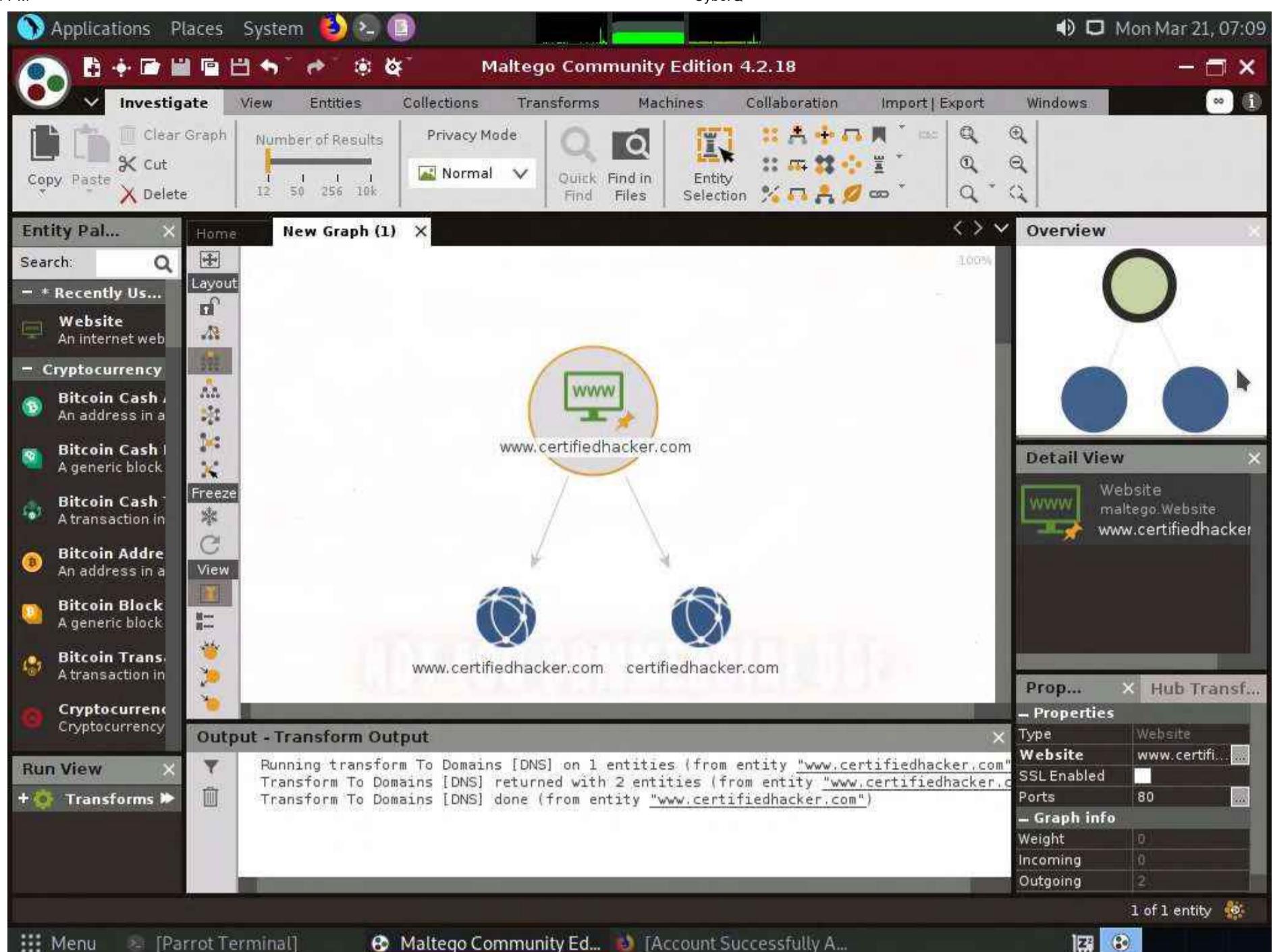
23. Right-click the entity and select **All Transforms**.



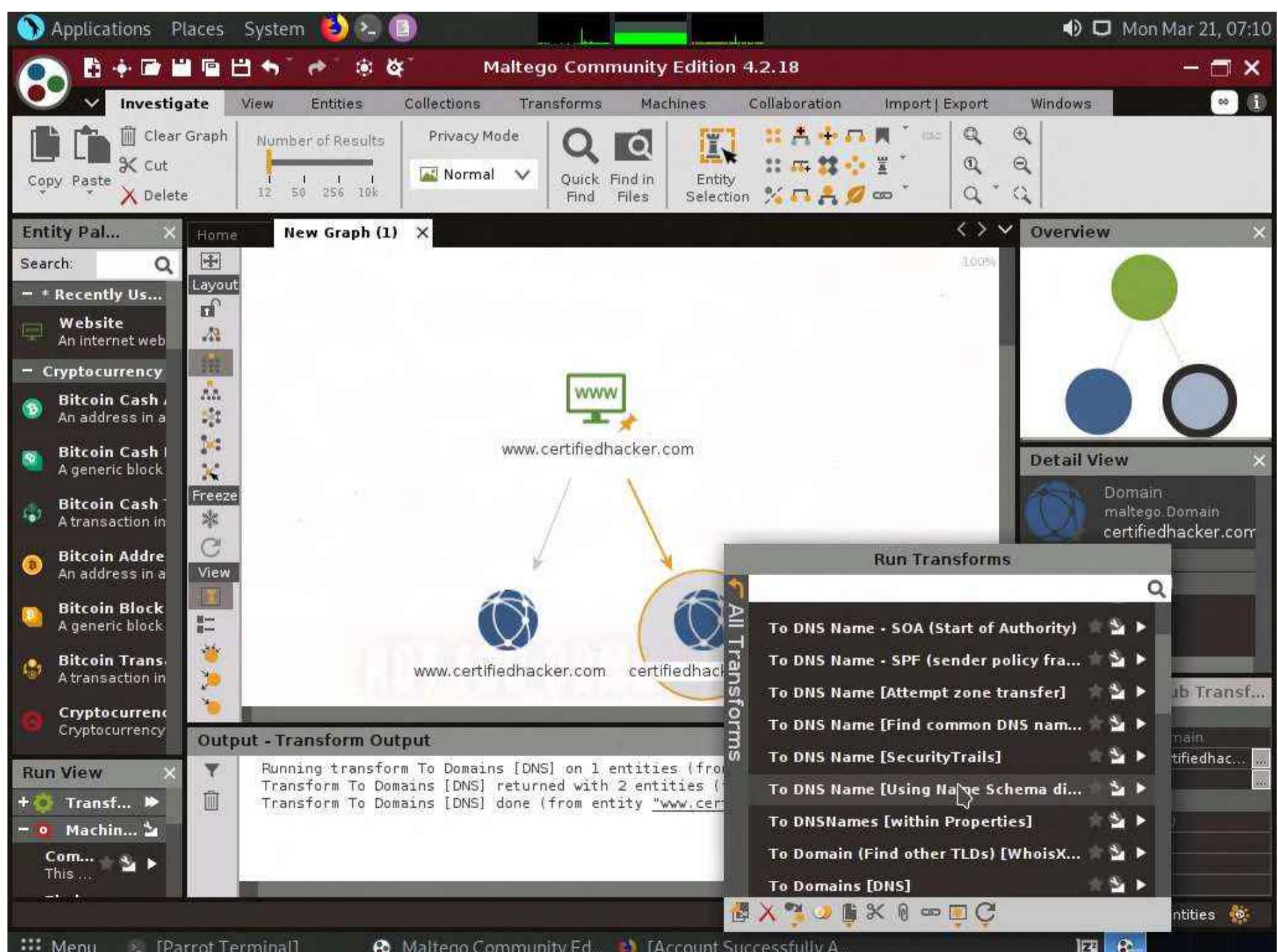
24. The Run Transform(s) list appears; click To Domains [DNS].



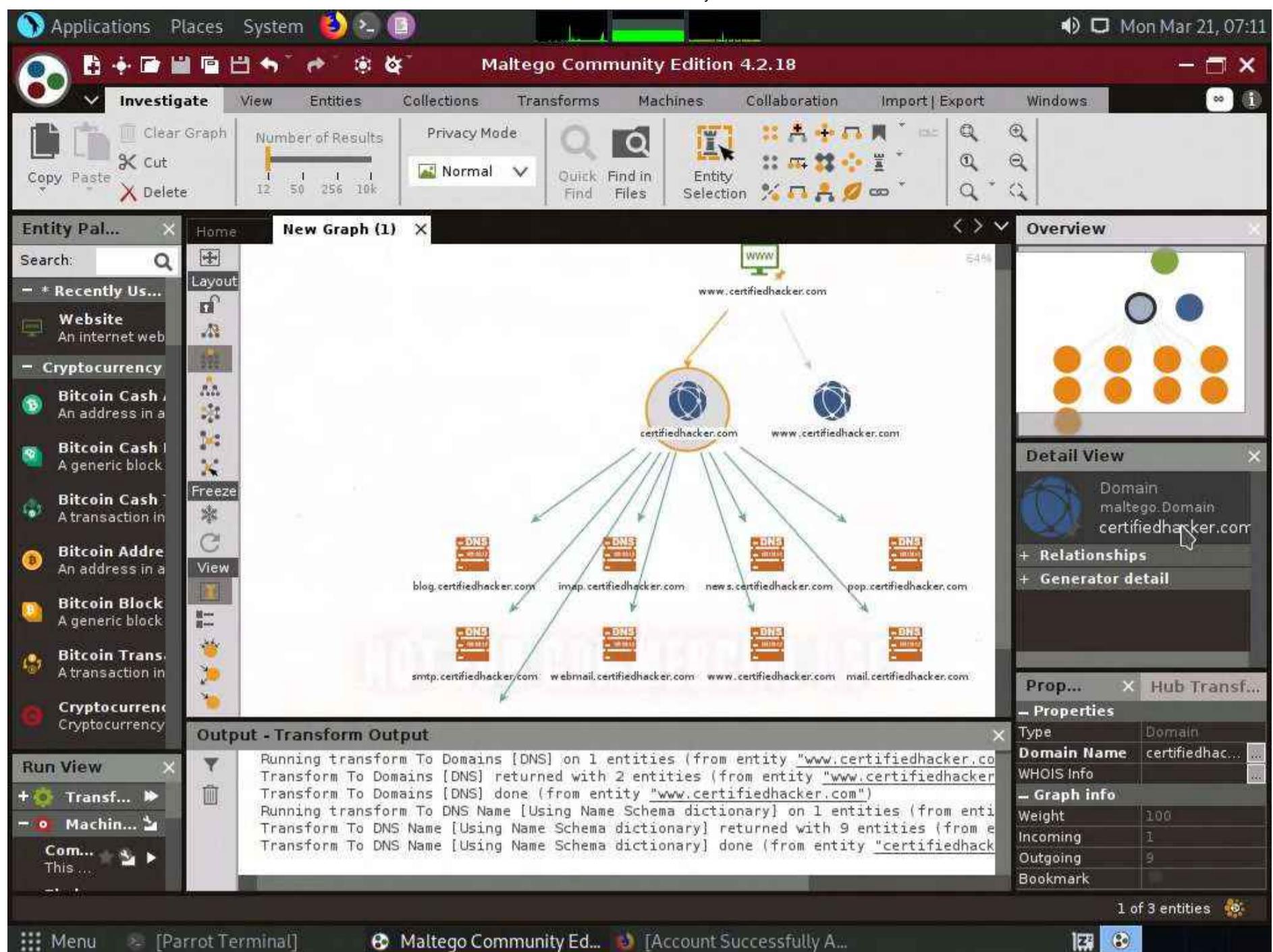
25. The domain corresponding to the website displays, as shown in the following screenshot.



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.

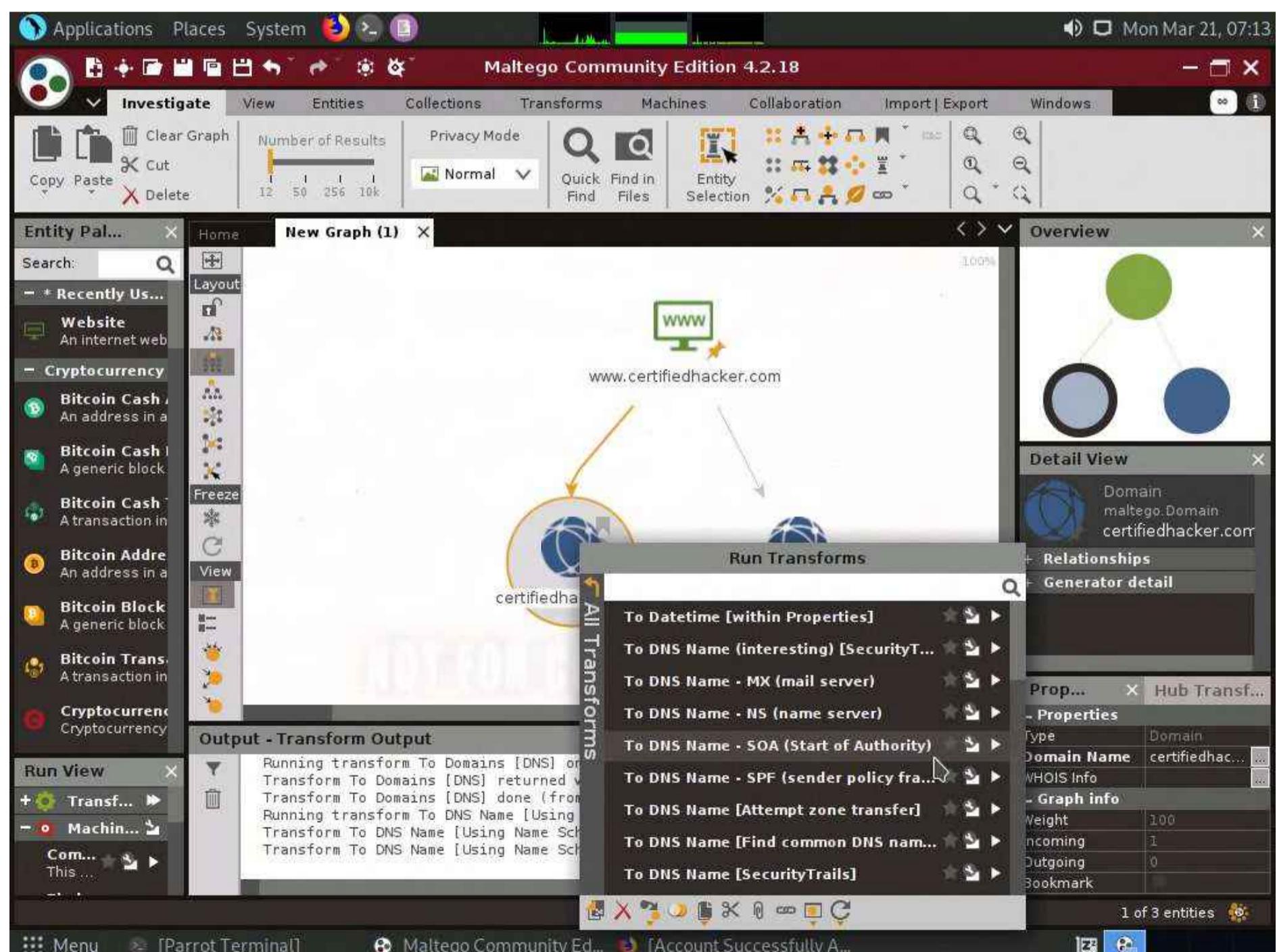


28. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential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

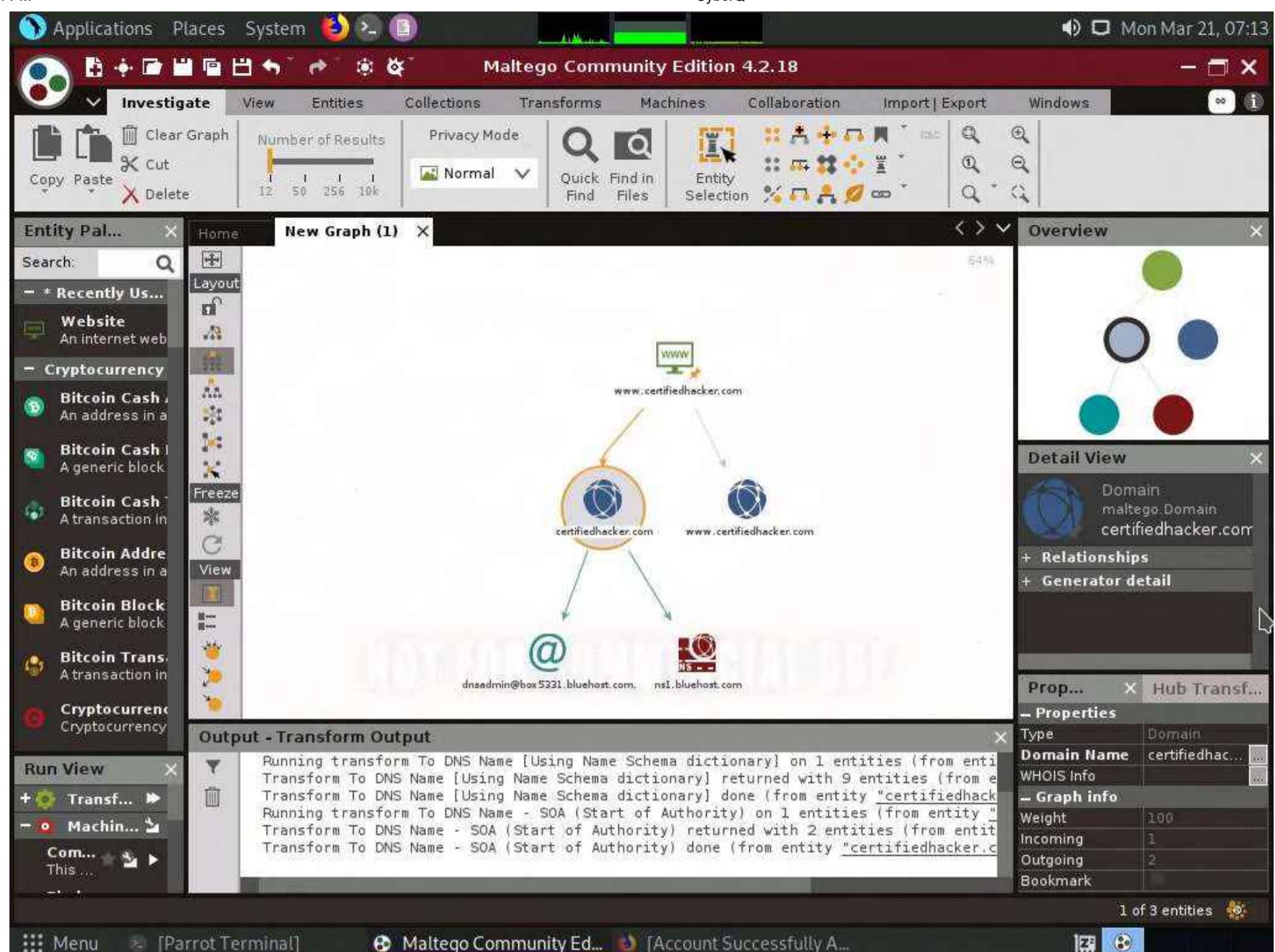
29. Select only the name schemas by dragging and deleting them.



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

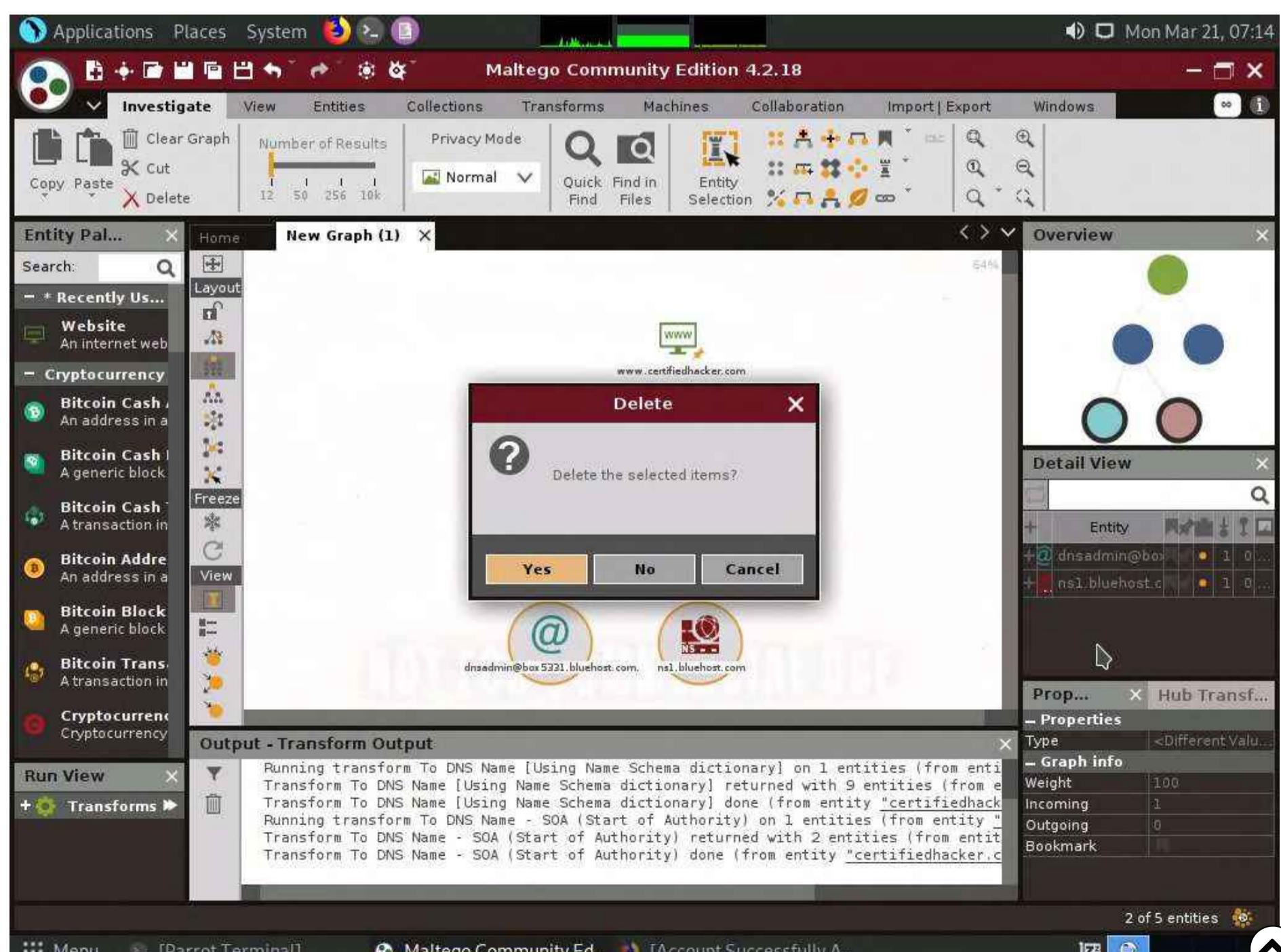


31. This returns the primary name server and the email of the domain administrator, as shown in the following screenshot.

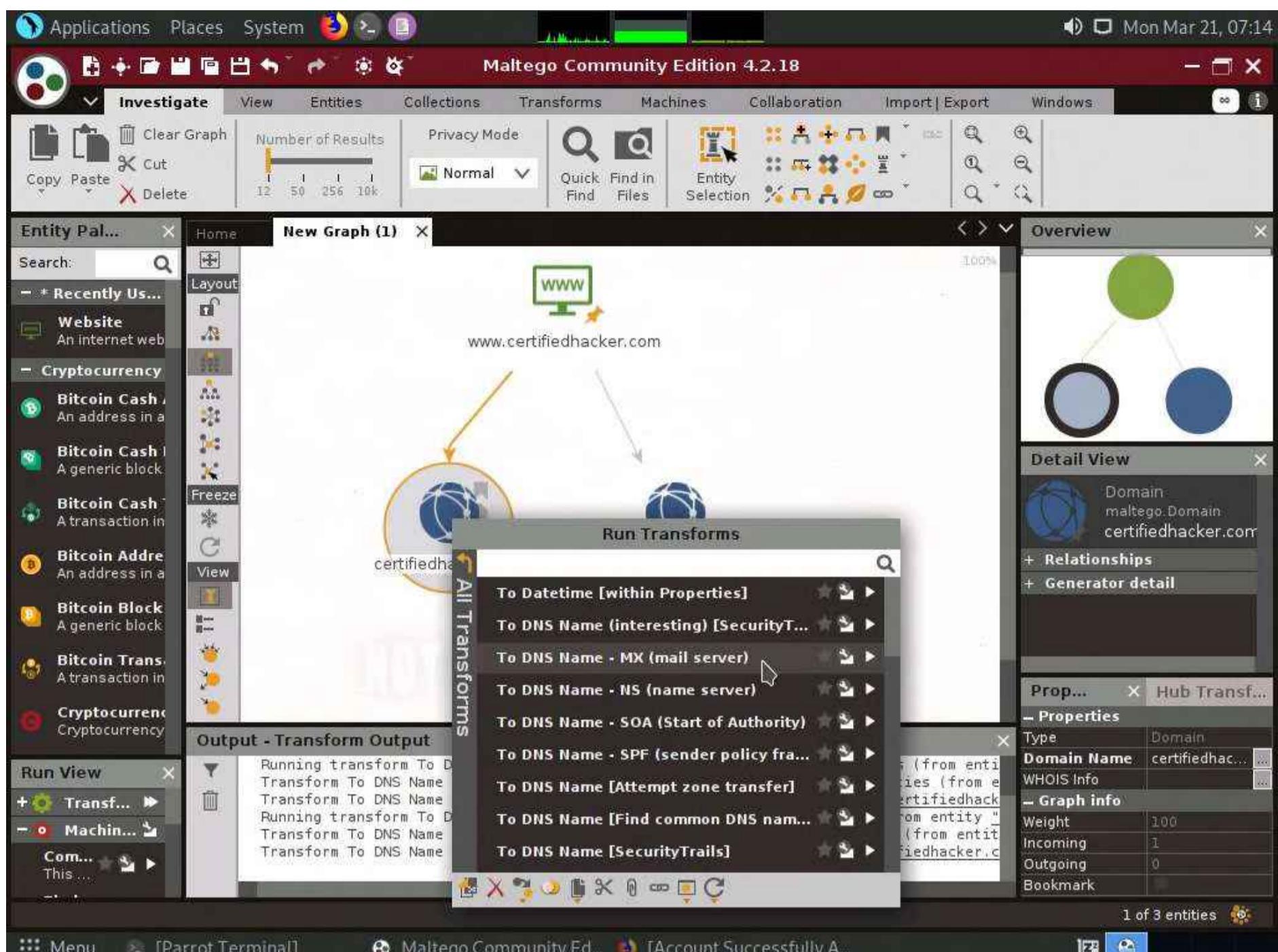


32. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.

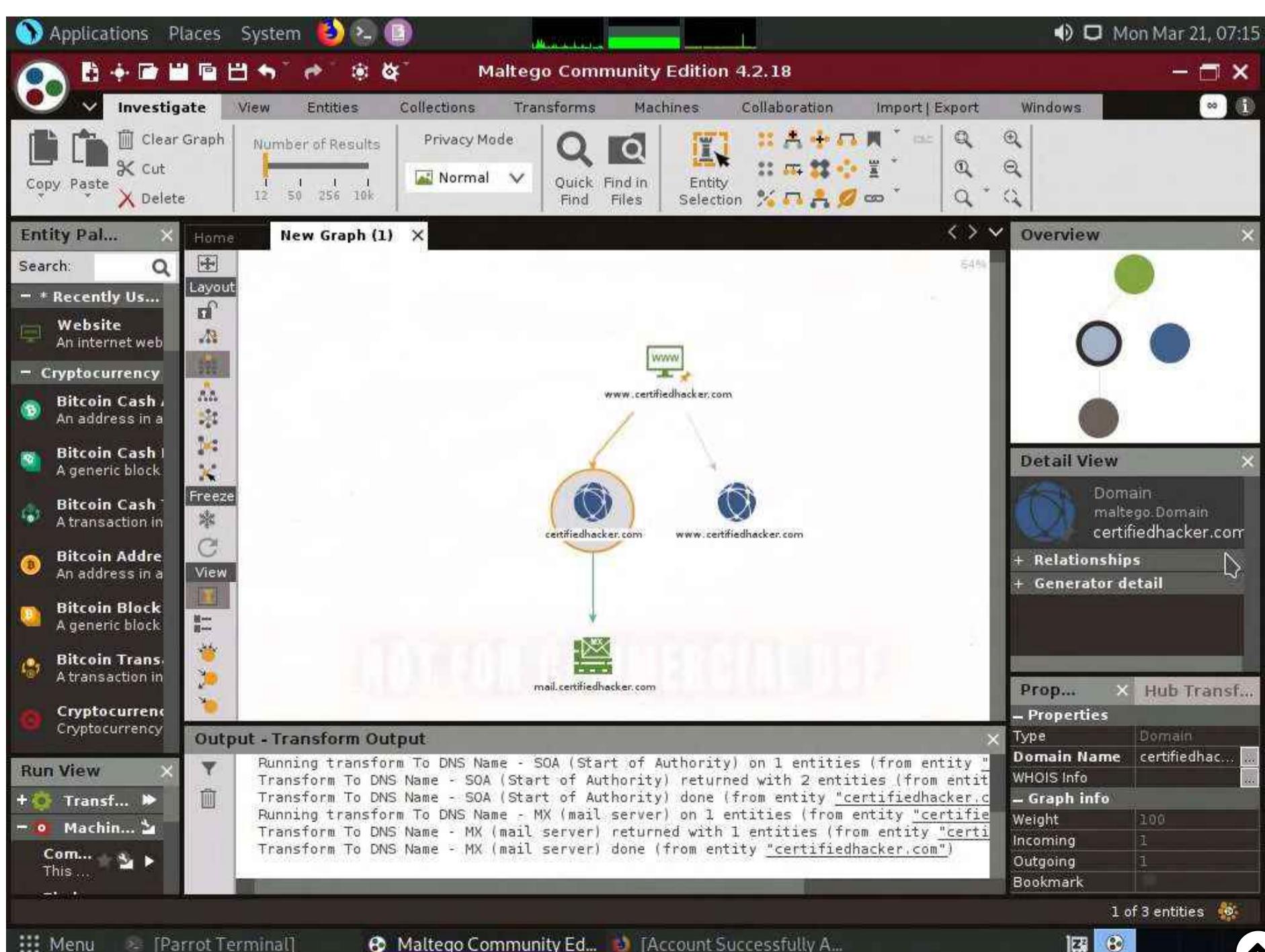
33. Select both the name server and the email by dragging and deleting them.



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

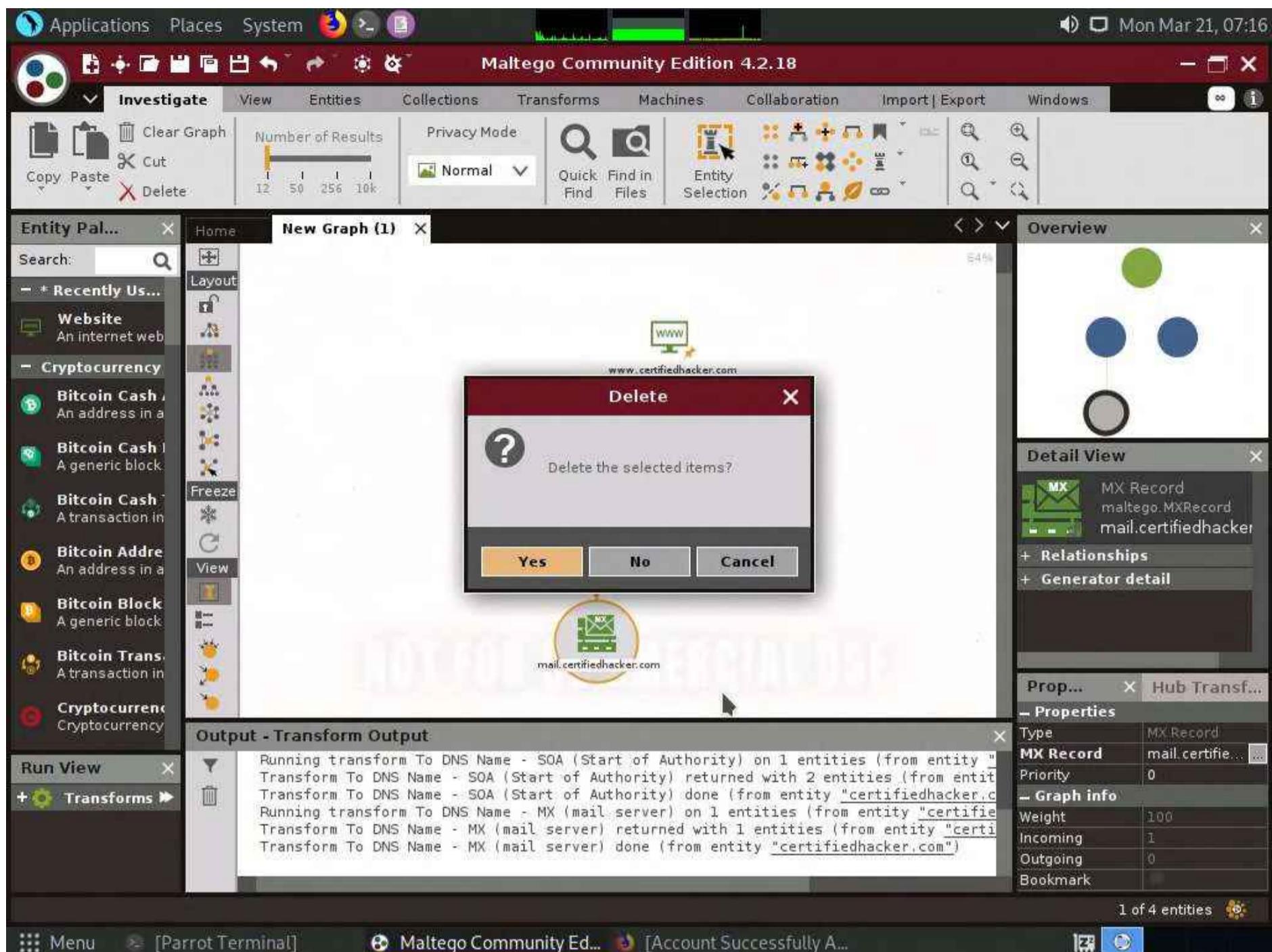


35. This transform returns the mail server associated with the certifiedhacker.com domain, as shown in the following screenshot.

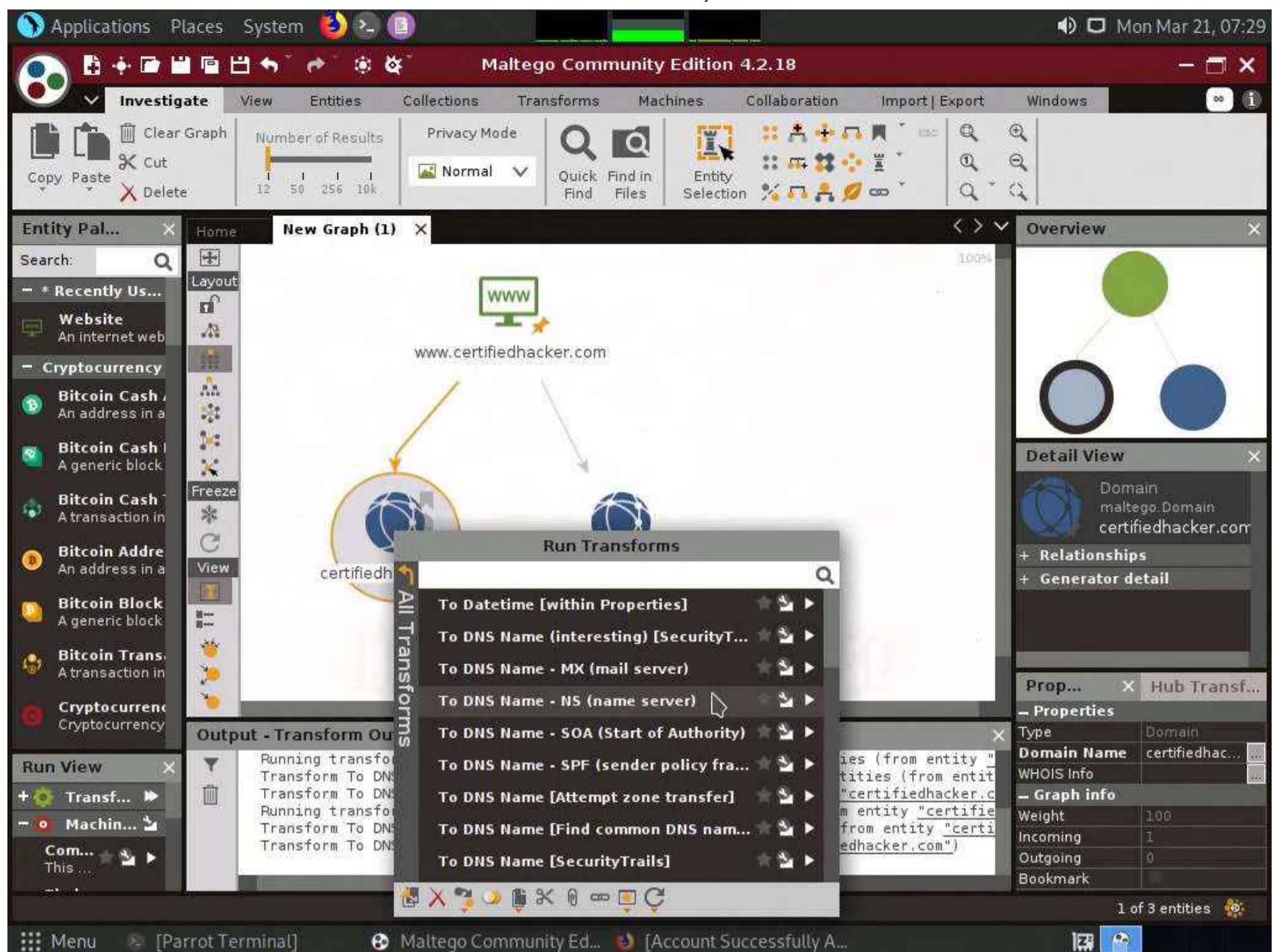


36. By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and, thereby, use it to perform malicious activities such as sending spam e-mails.

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



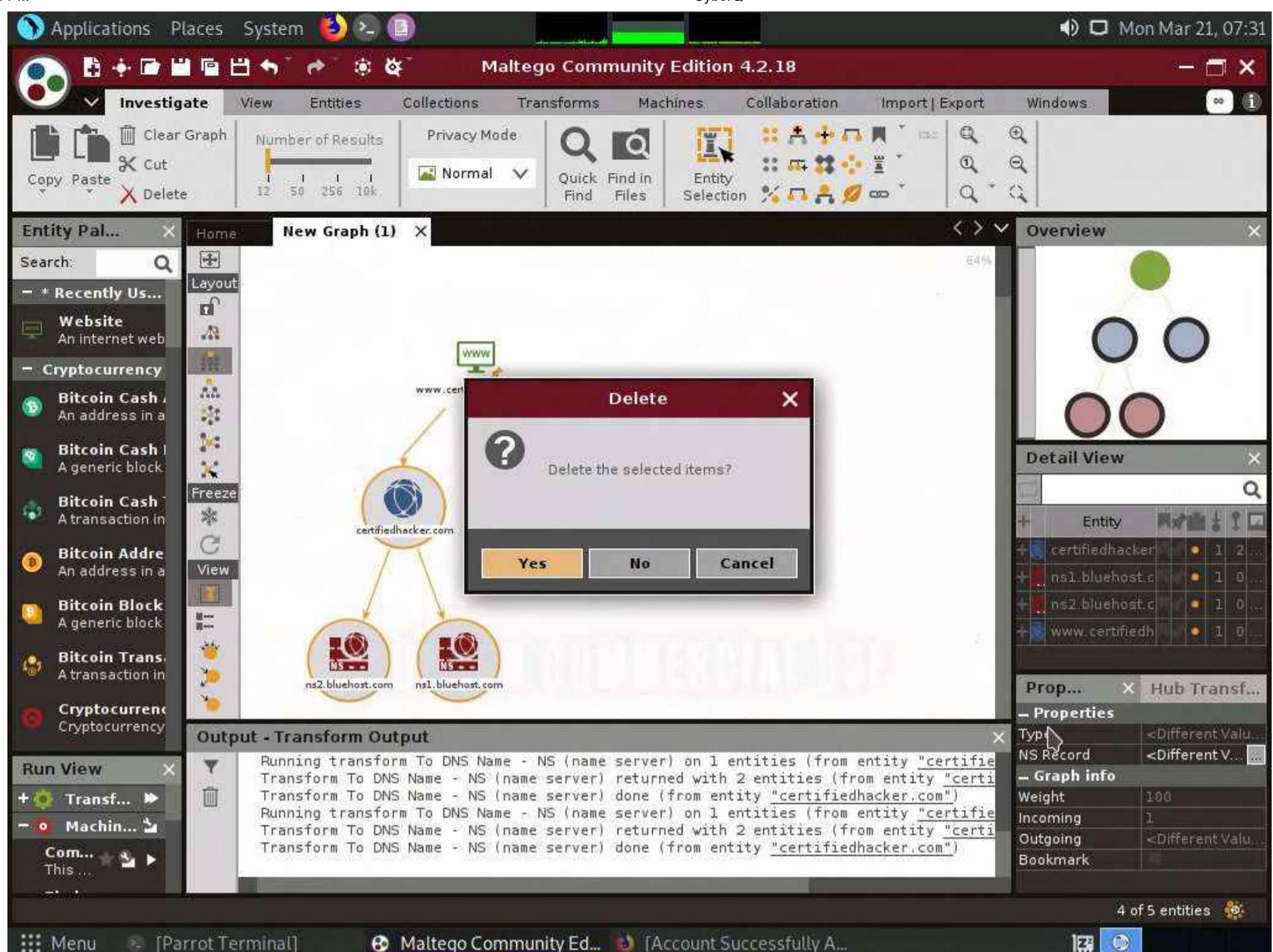
38. Right-click the **certifiedhacker.com** entity and select All Transforms --> To DNS Name - NS (name server).



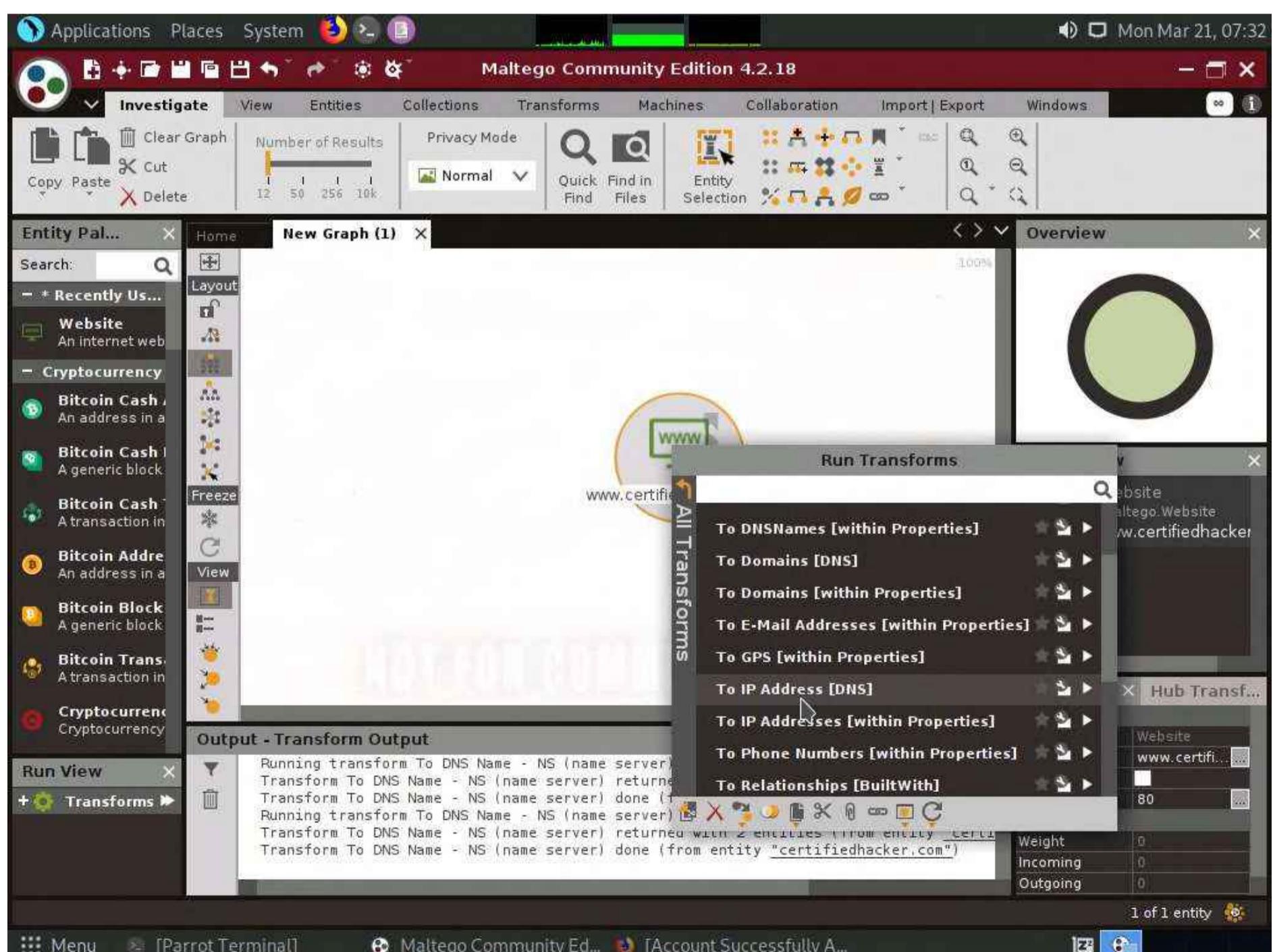
39. This returns the name servers associated with the domain, as shown in the following screenshot.

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.

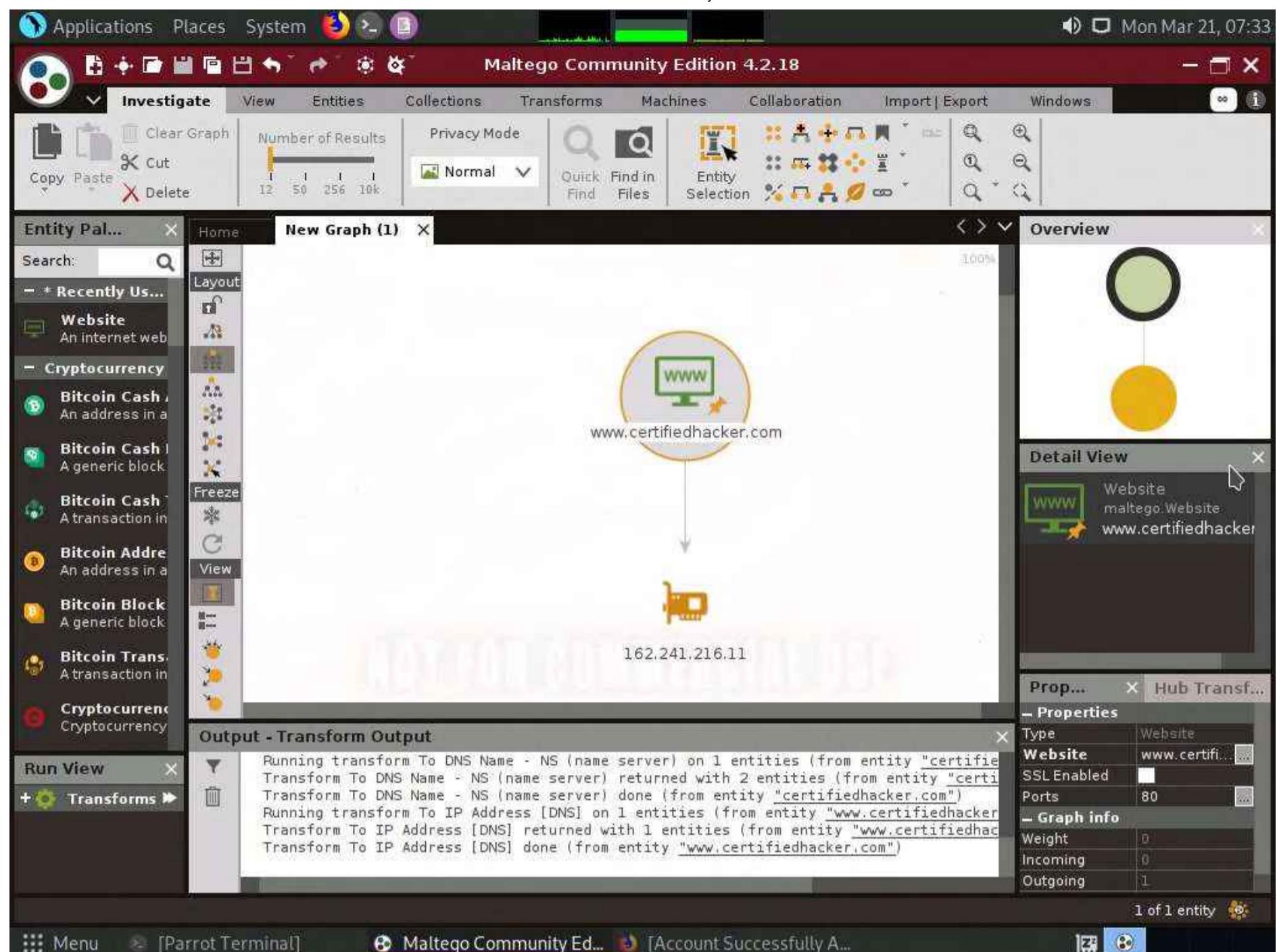
41. Select both the domain and the name server by dragging and deleting them.



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

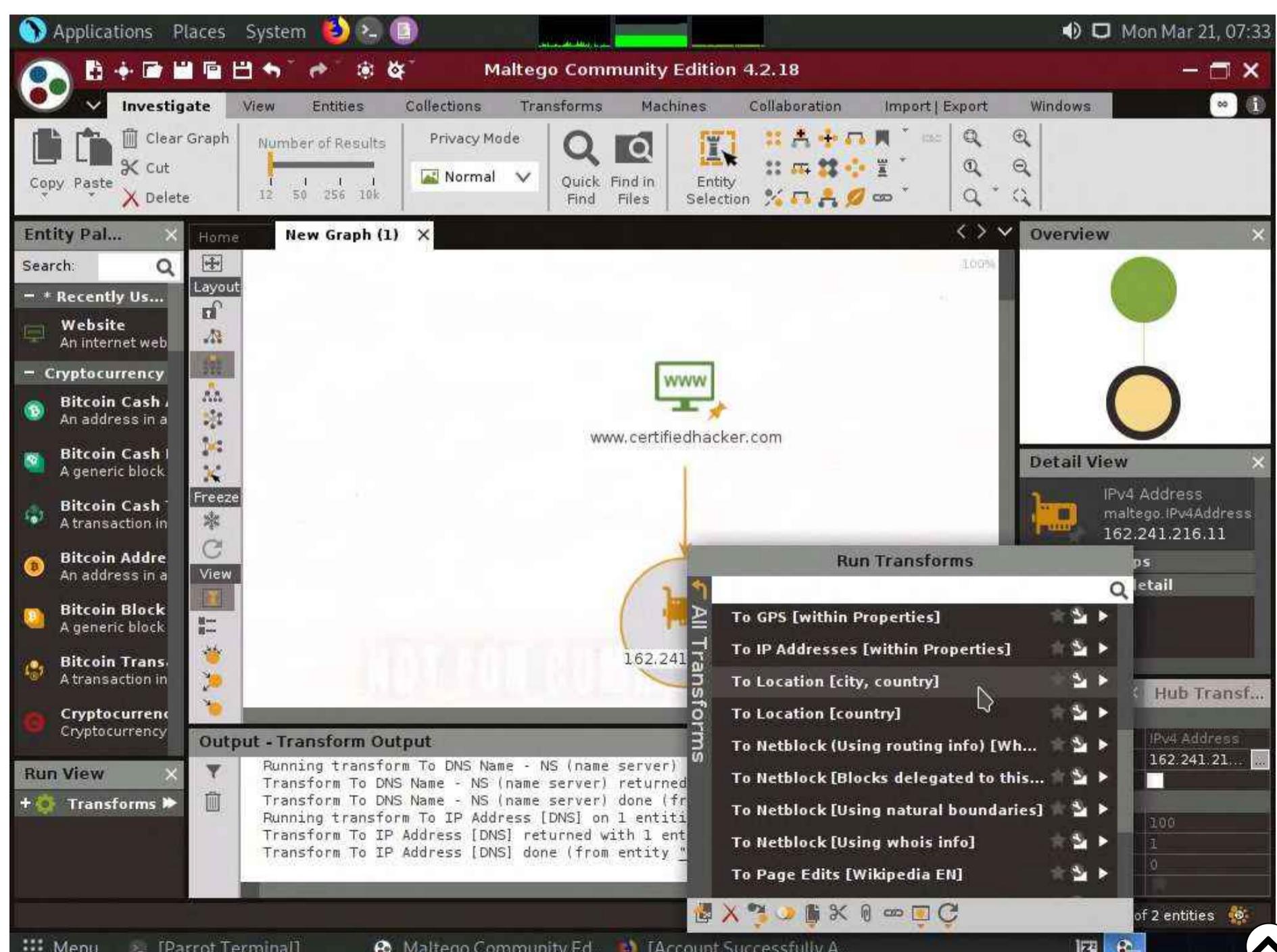


43. This displays the IP address of the website, as shown in the following screenshot.

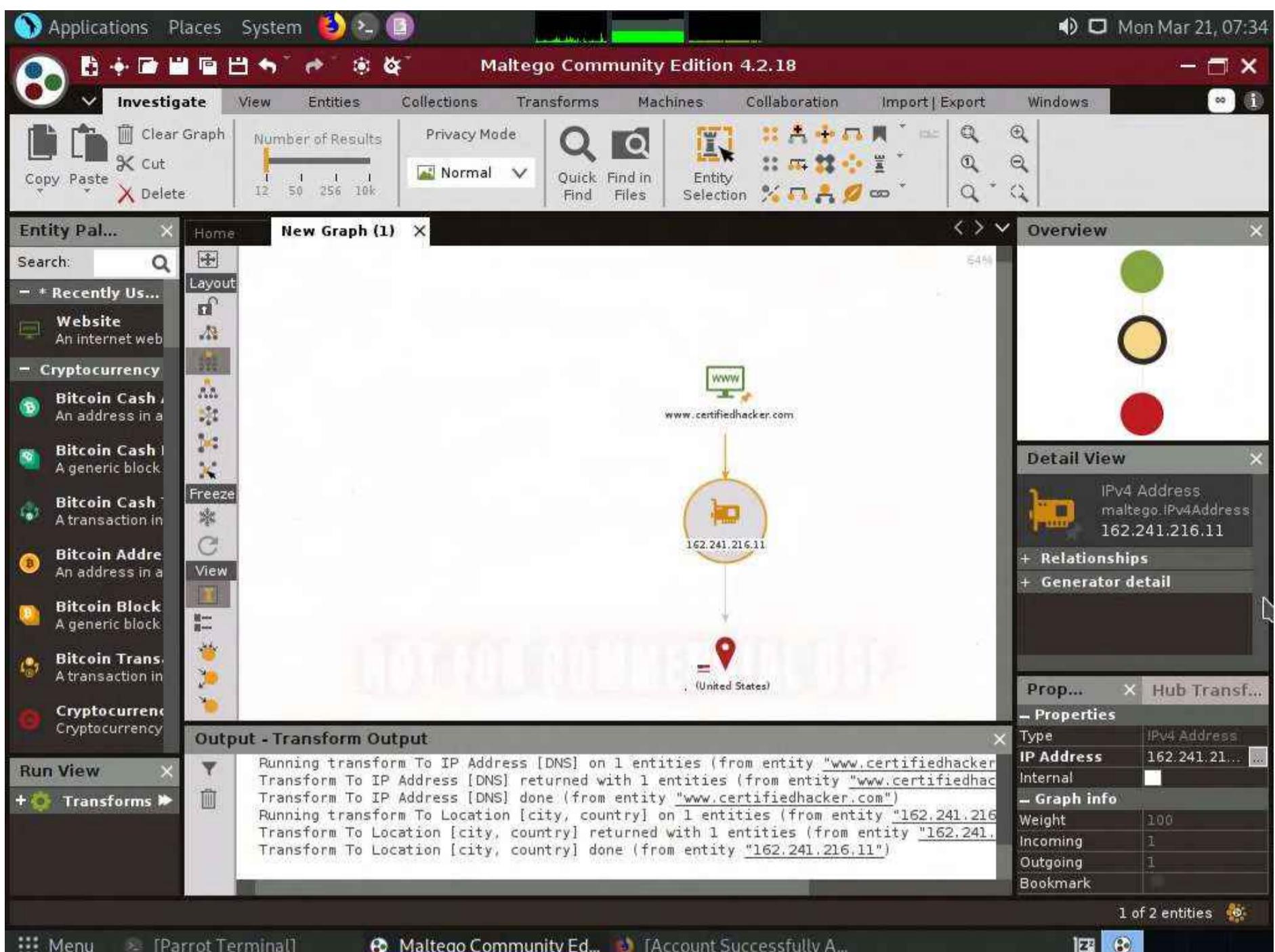


44. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

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

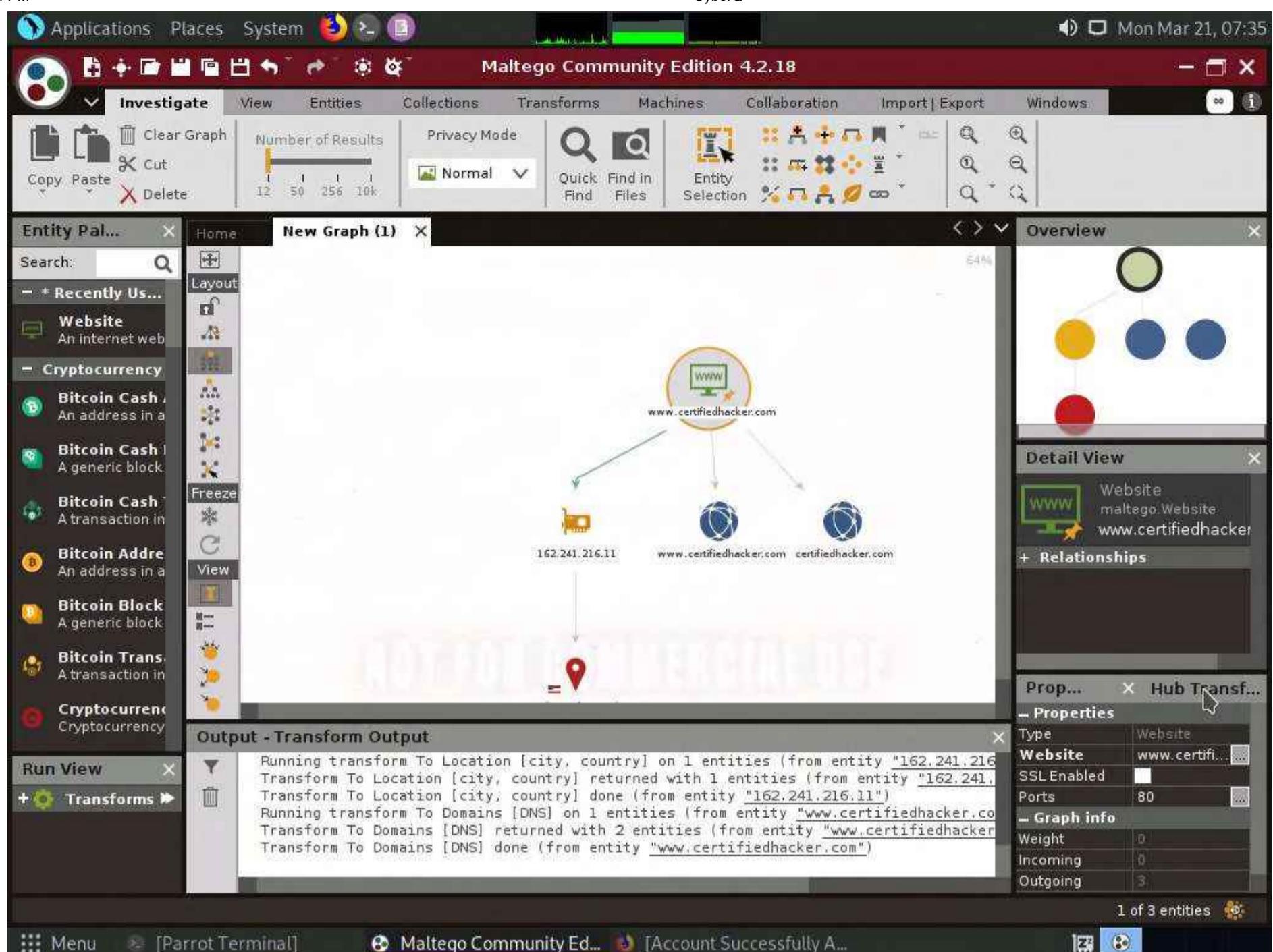


46. This transform identifies the geographical location of the IP address, as shown in the following screenshot.

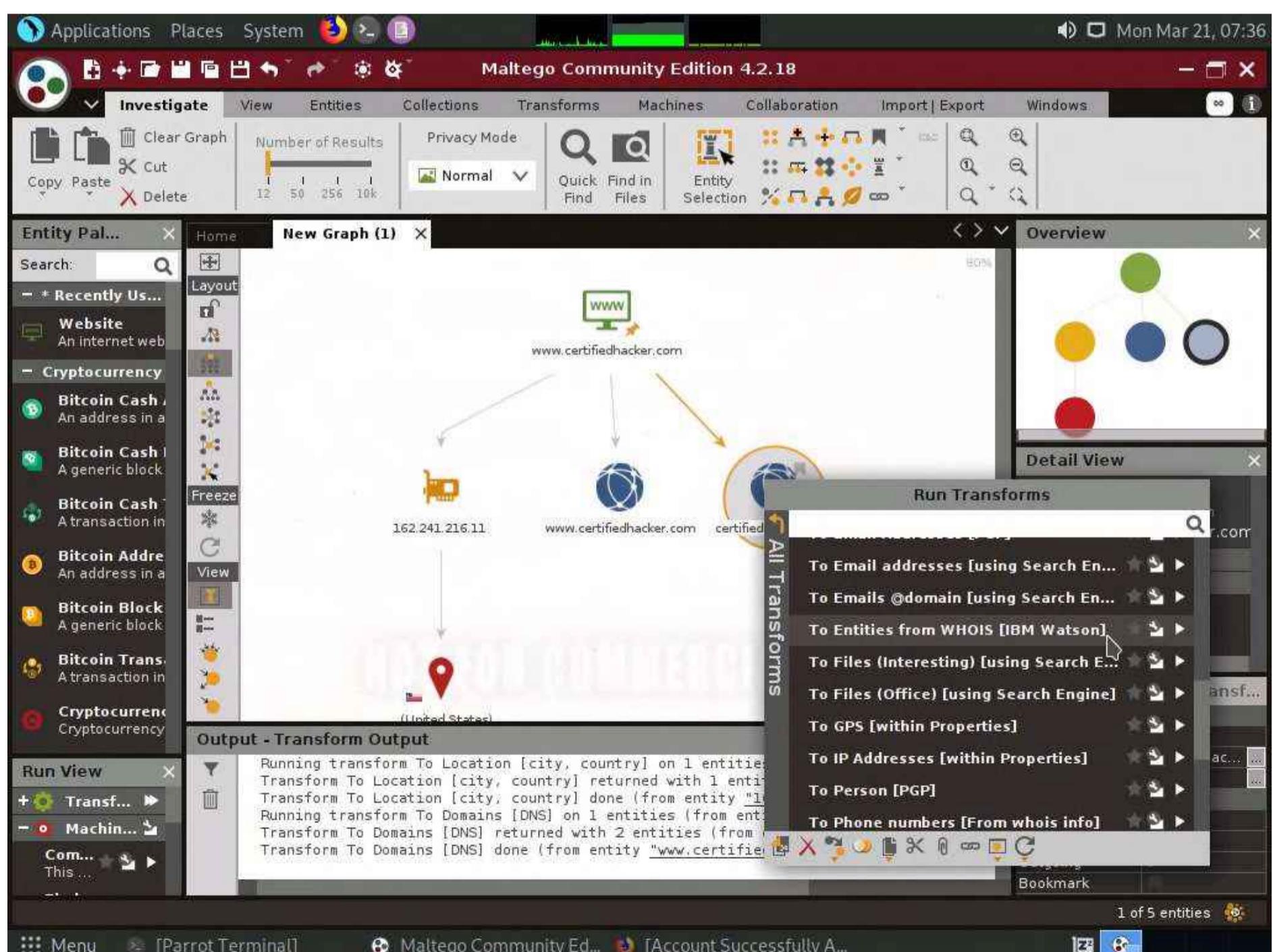


47. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

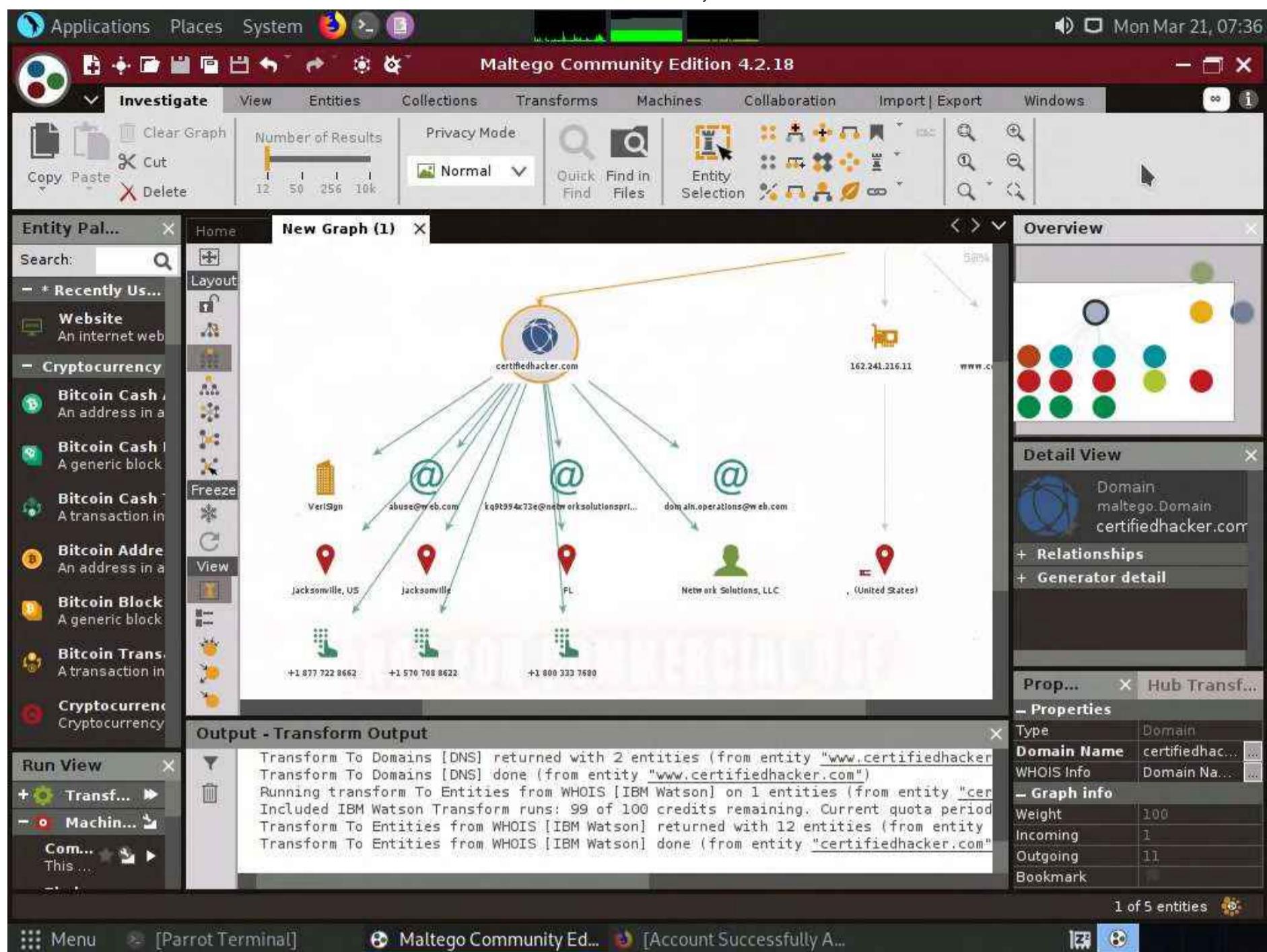
48. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms --> To Domains [DNS]**. The domains corresponding to the website display, as shown in the screenshot.



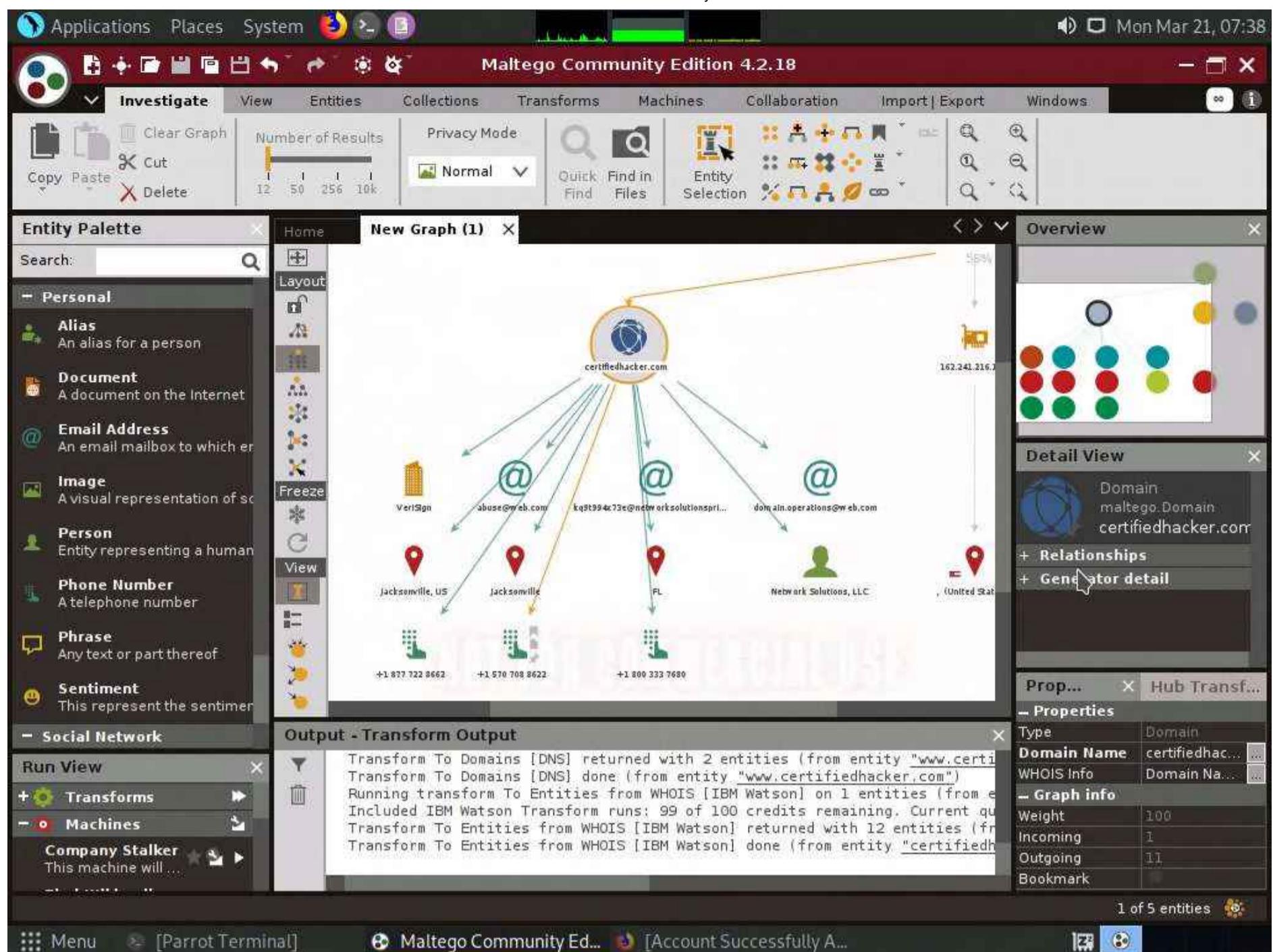
49. Right-click the domain entity (certifiedhacker.com) and select All Transform --> To Entities from WHOIS [IBM Watson].



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.

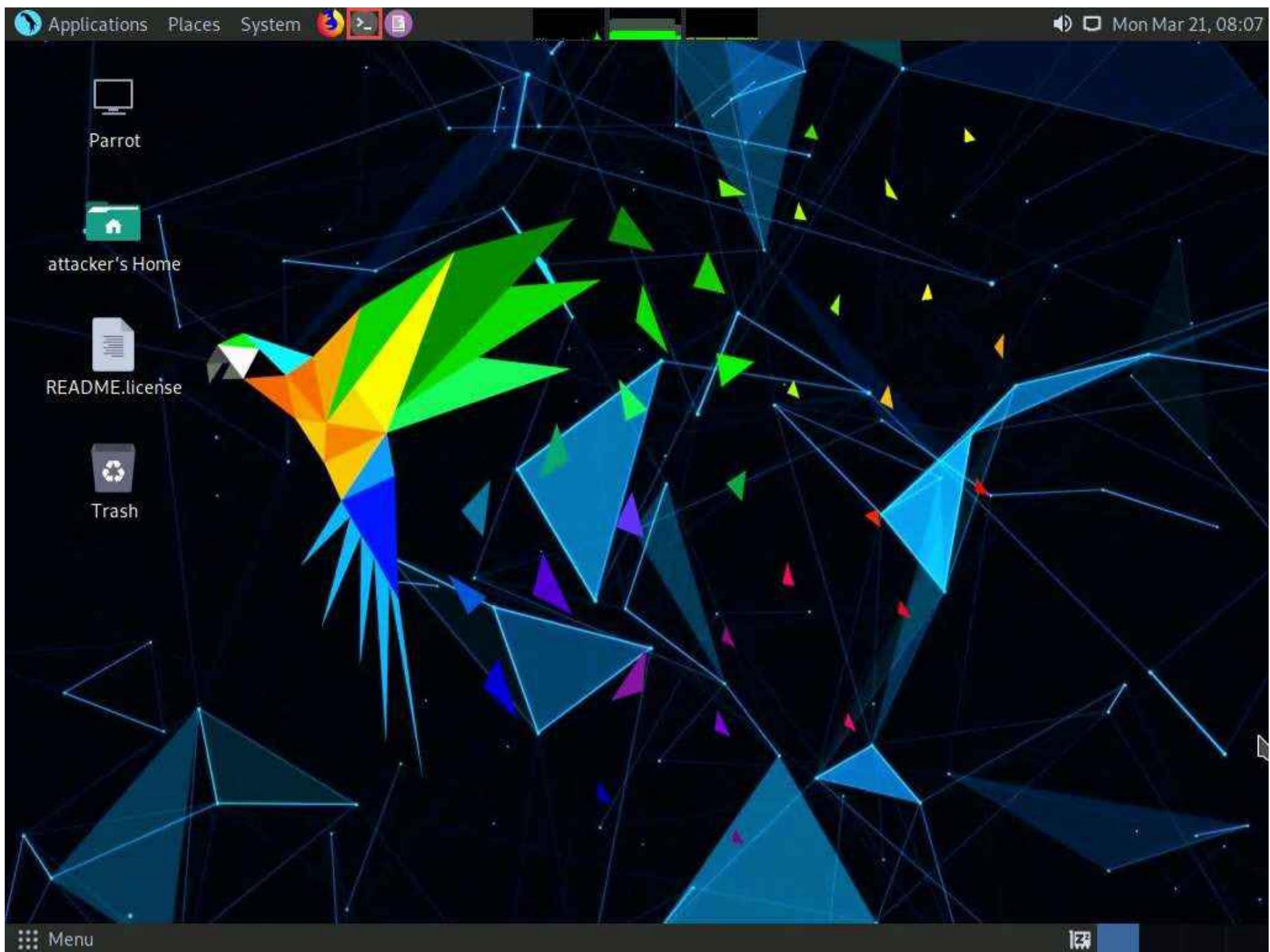
56. This concludes the demonstration of footprinting a target using Maltego.

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.



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

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

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



The screenshot shows a terminal window titled "domainfy -n eccouncil -t all - Parrot Terminal". The command "#domainfy -n eccouncil -t all" is entered at the root prompt. The terminal has a dark background with a green progress bar at the top.

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.

The screenshot shows a terminal window titled "domainfy -n eccouncil -t all - Parrot Terminal". The output of the command is displayed, showing 21 results obtained. The results are listed in a table format:

Sheet Name: Objects recovered (2022-3-24_1h33m).
+-----+-----+
com.i3visio.Domain com.i3visio.IPV4
+=====+=====+
eccouncil.net 208.91.197.27
+-----+-----+
eccouncil.org 104.18.21.251
+-----+-----+
eccouncil.com 104.18.25.244
+-----+-----+
eccouncil.in 34.102.136.180
+-----+-----+
eccouncil.ir 94.232.173.162
+-----+-----+
eccouncil.cz 89.185.225.244
+-----+-----+
eccouncil.us 208.91.197.27
+-----+-----+
eccouncil.tv 66.129.123.226
+-----+-----+
eccouncil.cf 195.20.52.168
+-----+-----+
eccouncil.cn 107.161.26.30
+-----+-----+
eccouncil.co 172.67.170.166
+-----+-----+
eccouncil.me 34.102.136.180
+-----+-----+

```

Applications Places System domainfy -n eccouncil -t all - Parrot Terminal
File Edit View Search Terminal Help
| eccouncil.biz | 34.102.136.180 |
+-----+-----+
| eccouncil.academy | 208.91.197.27 |
+-----+-----+
| eccouncil.training | 208.91.197.27 |
+-----+-----+
| eccouncil.tel | 52.50.143.27 |
+-----+-----+
| eccouncil.exposed | 208.91.197.27 |
+-----+-----+
| eccouncil.institute | 172.67.188.240 |
+-----+-----+

2022-03-24 01:33:57.036178      You can find all the information collected in the following files:
./profiles.csv

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

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

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

```

[root@parrot] ~ #

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.



A screenshot of a terminal window titled "searchfy -q "Tim Cook" - Parrot Terminal". The terminal is running on a Linux desktop environment with a dark theme. The command "#searchfy -q \"Tim Cook\"" is visible at the bottom of the terminal window.

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.

A screenshot of a terminal window titled "searchfy -q "Tim Cook" - Parrot Terminal". The terminal displays the results of the searchfy command, which includes user profiles from GitHub. The output is organized into columns: Platform, Alias, Email, and URI. The profiles listed are:

Platform	Alias	Email	URI
Github	timothyfcook	N/A	https://github.com/timothyfcook
Github	cookieguru	N/A	https://github.com/cookieguru
Github	twcook	N/A	https://github.com/twcook
Github	timjcook	N/A	https://github.com/timjcook
Github	TimEnglart	N/A	https://github.com/TimEnglart

```
searchfy -q "Tim Cook" - Parrot Terminal
[...]
| KeyServerUbuntu | tim
ex&search=tim@openparadigms.com
|
+-----+
| KeyServerUbuntu | tim
ex&search=tim@trcooke.co.uk
|
+-----+
| KeyServerUbuntu | ahughes2005
ex&search=ahughes2005@gmail.com
|
+-----+
| KeyServerUbuntu | ahughes
ex&search=ahughes@ndaviess.k12.in.us
|
+-----+
| KeyServerUbuntu | adedina
ex&search=adedina@ndaviess.k12.in.us
|
+-----+
| KeyServerUbuntu | algraber
ex&search=algraber@ndaviess.k12.in.us
|
+-----+
| KeyServerUbuntu | lasutton
ex&search=lasutton@ndaviess.k12.in.us
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
tim@openparadigms.com | openparadigms.com
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
tim@trcooke.co.uk | trcooke.co.uk
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ahughes2005@gmail.com | gmail.com
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ahughes@ndaviess.k12.in.us | ndaviess.k12.in.us
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
adedina@ndaviess.k12.in.us | ndaviess.k12.in.us
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
algraber@ndaviess.k12.in.us | ndaviess.k12.in.us
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
lasutton@ndaviess.k12.in.us | ndaviess.k12.in.us
|
+-----+
[...]
Menu > searchfy -q "Tim Cook" ...
```

```
searchfy -q "Tim Cook" - Parrot Terminal
[...]
| KeyServerUbuntu | twcook
ex&search=twcook@shaw.ca
|
+-----+
| KeyServerUbuntu | pourhaus
ex&search=pourhaus@gmail.com
|
+-----+
| KeyServerUbuntu | 923350
ex&search=923350@ican.net
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
twcook@shaw.ca | shaw.ca
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
pourhaus@gmail.com | gmail.com
|
+-----+
| https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
923350@ican.net | ican.net
|
+-----+
2022-03-24 01:37:13.491782 You can find all the information collected in the following files:
./profiles.csv
2022-03-24 01:37:13.491893 Finishing execution...
Total time used: 0:00:03.132000
Average seconds/query: 3.132 seconds

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

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.

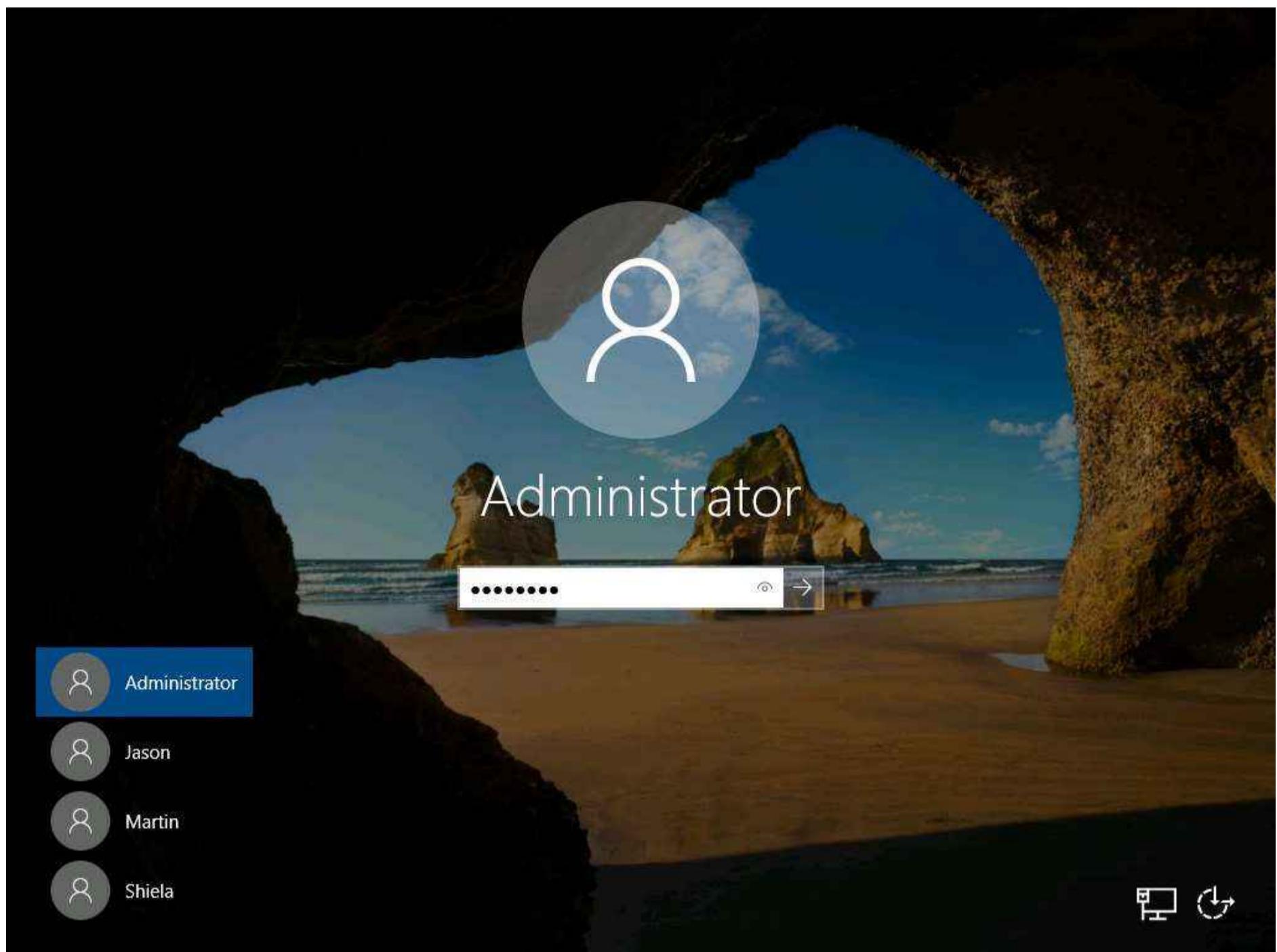
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.



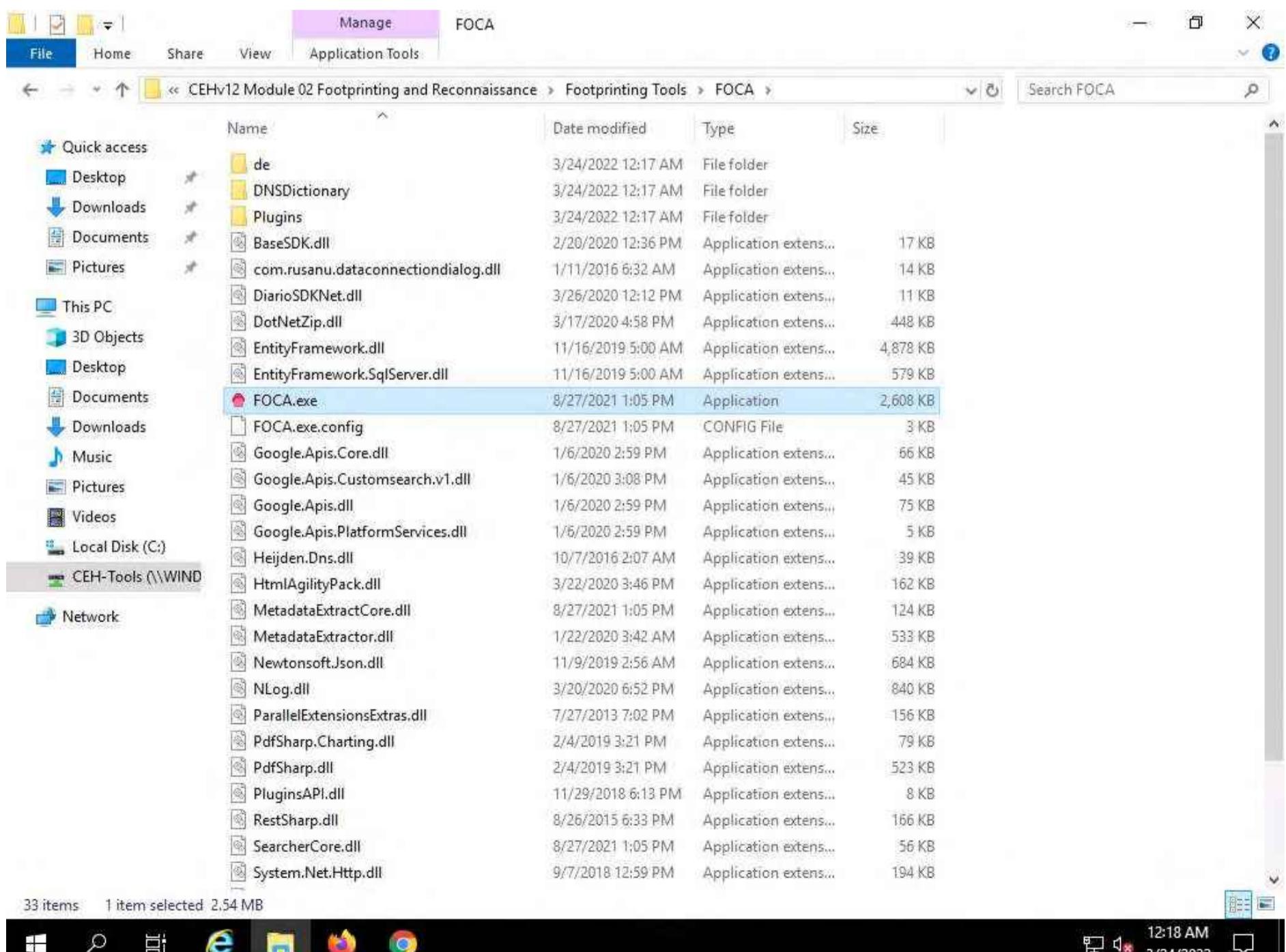
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type ****Pa\$\$w0rd ****in the Password field and press **Enter** to login.

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

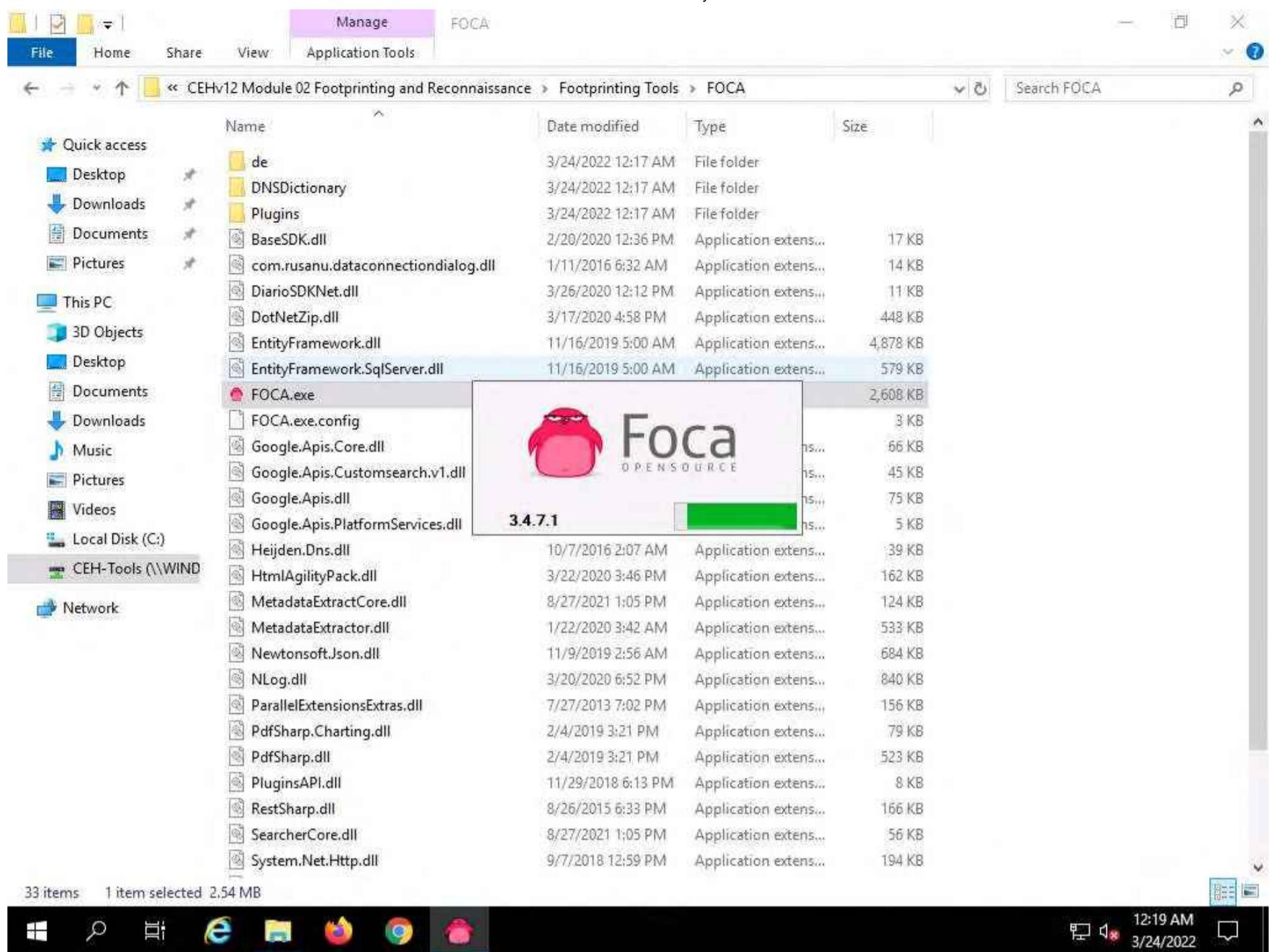




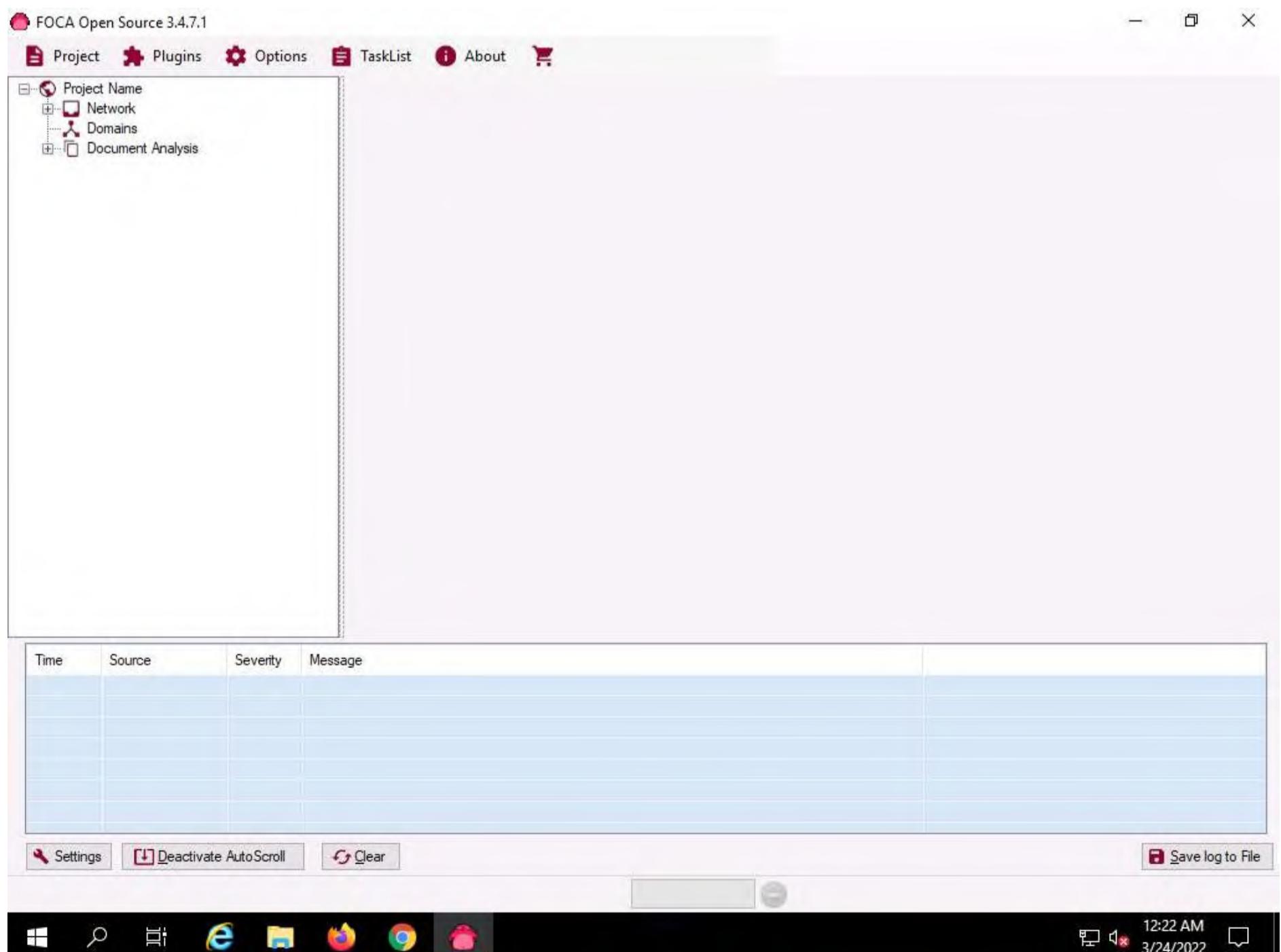
3. To launch FOCA, navigate to Z:\CEHv12 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA and double-click **FOCA.exe**.



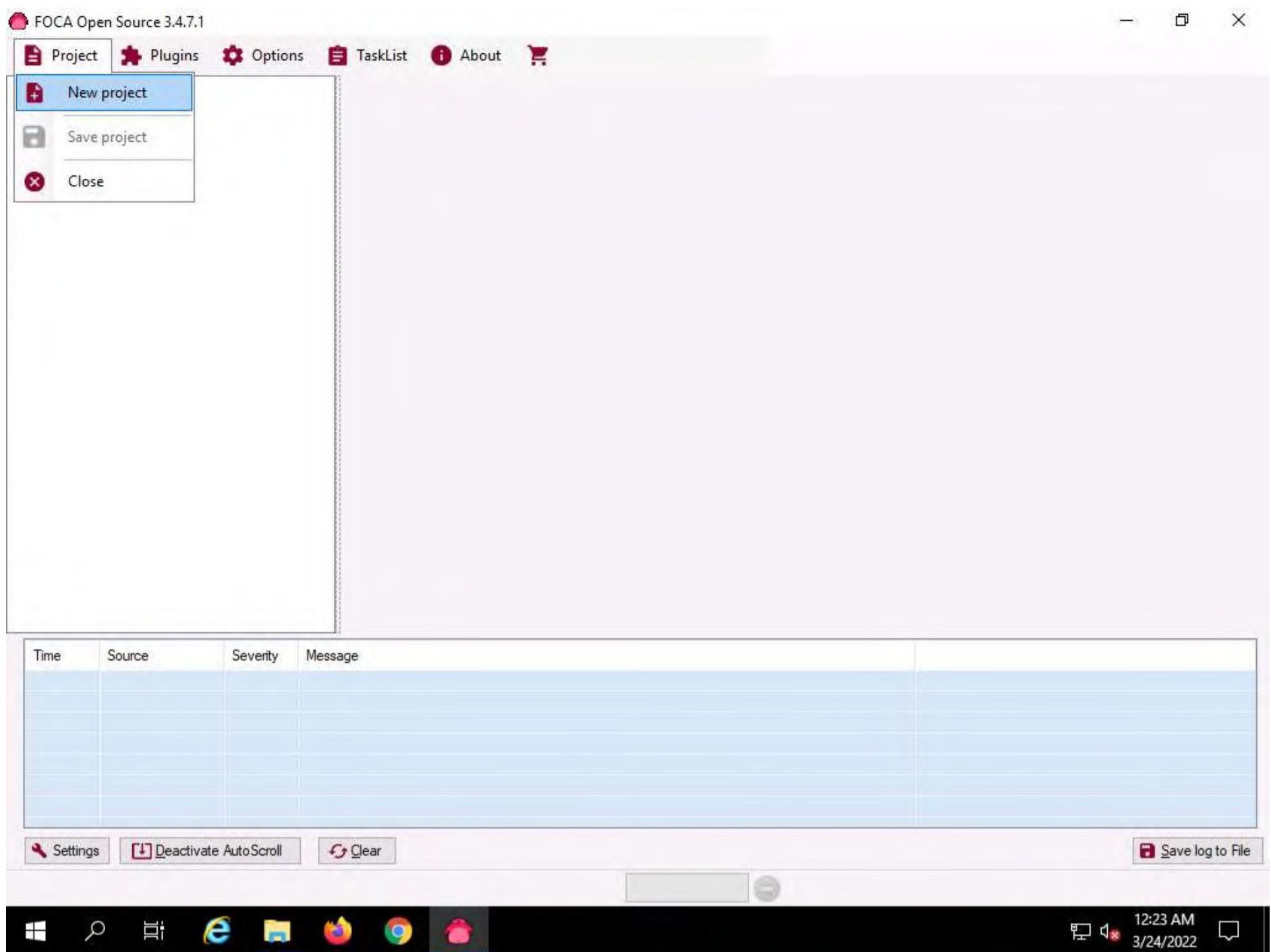
4. The FOCA dialog-box appears, wait for the initialization to complete.



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**).

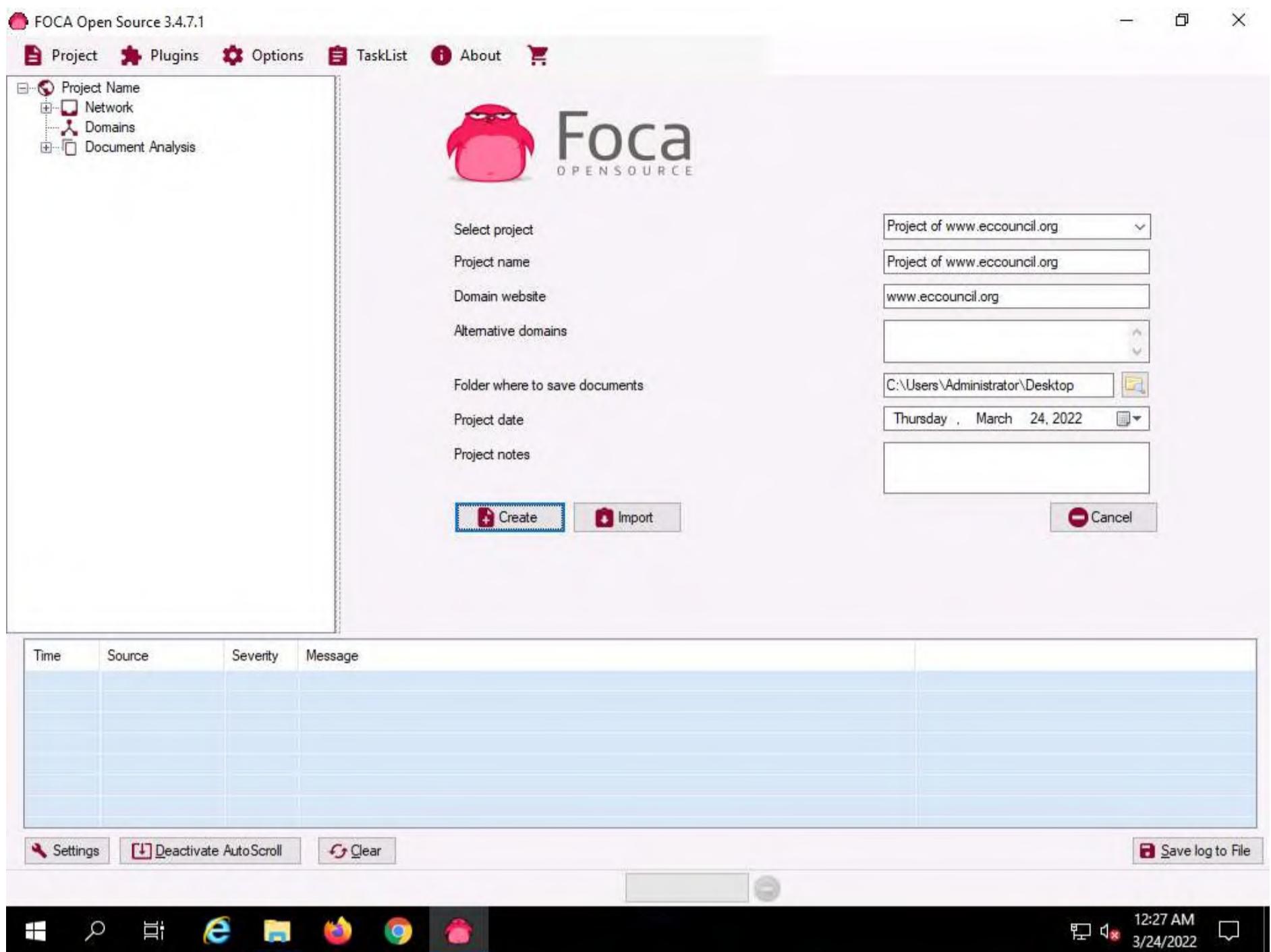
Enter the domain website in the **Domain website** field (here, **www.eccouncil.org**).

You can leave the optional **Alternative domains** field empty.

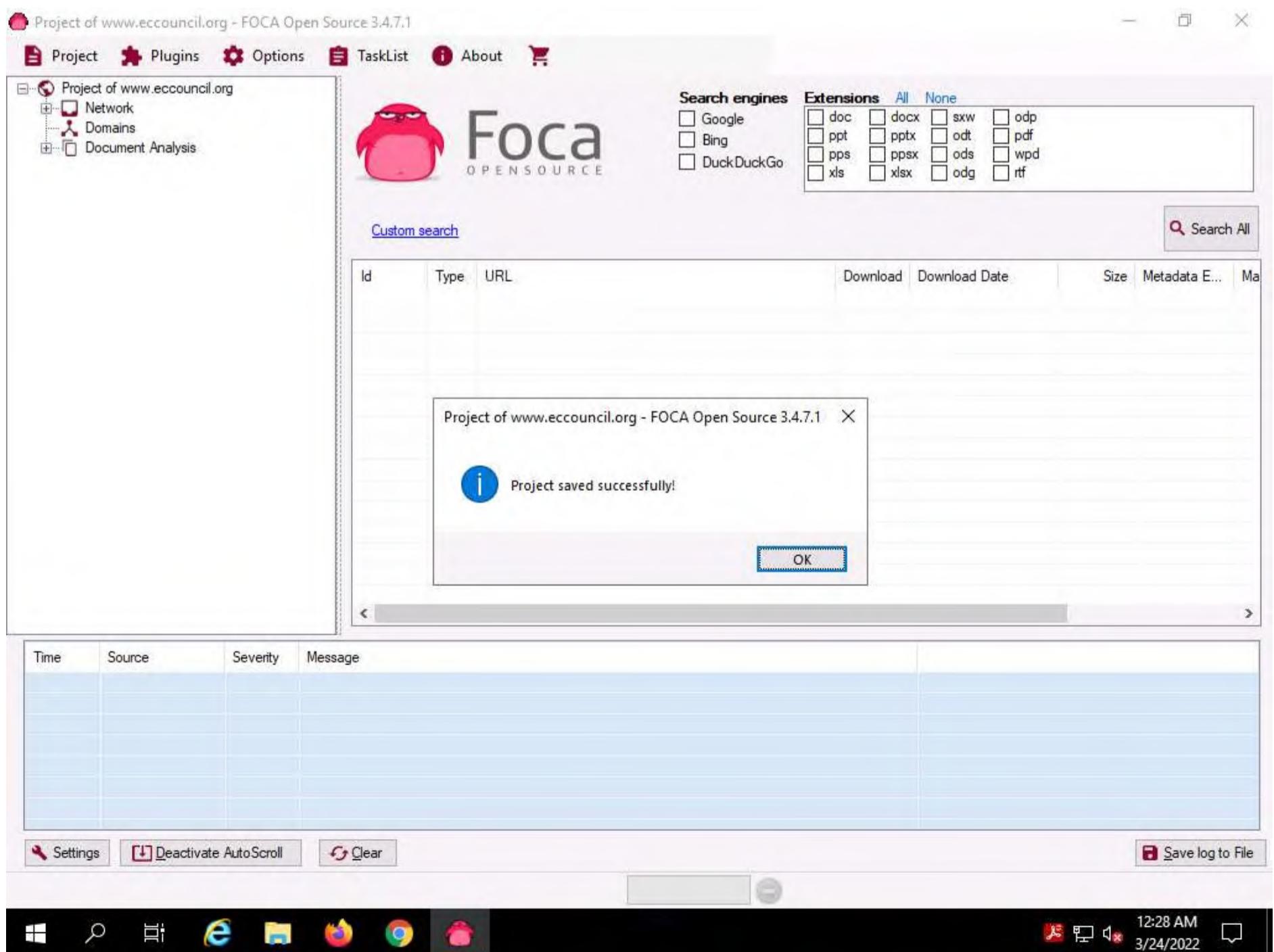
Under the **Folder where to save documents** field, click on the **Folder** icon. When the **Browse For Folder** pop up window appears, select the location to save the document that is extracted by FOCA (here, **Desktop**) and click **OK**.

Leave the other settings to default and click the **Create** button.

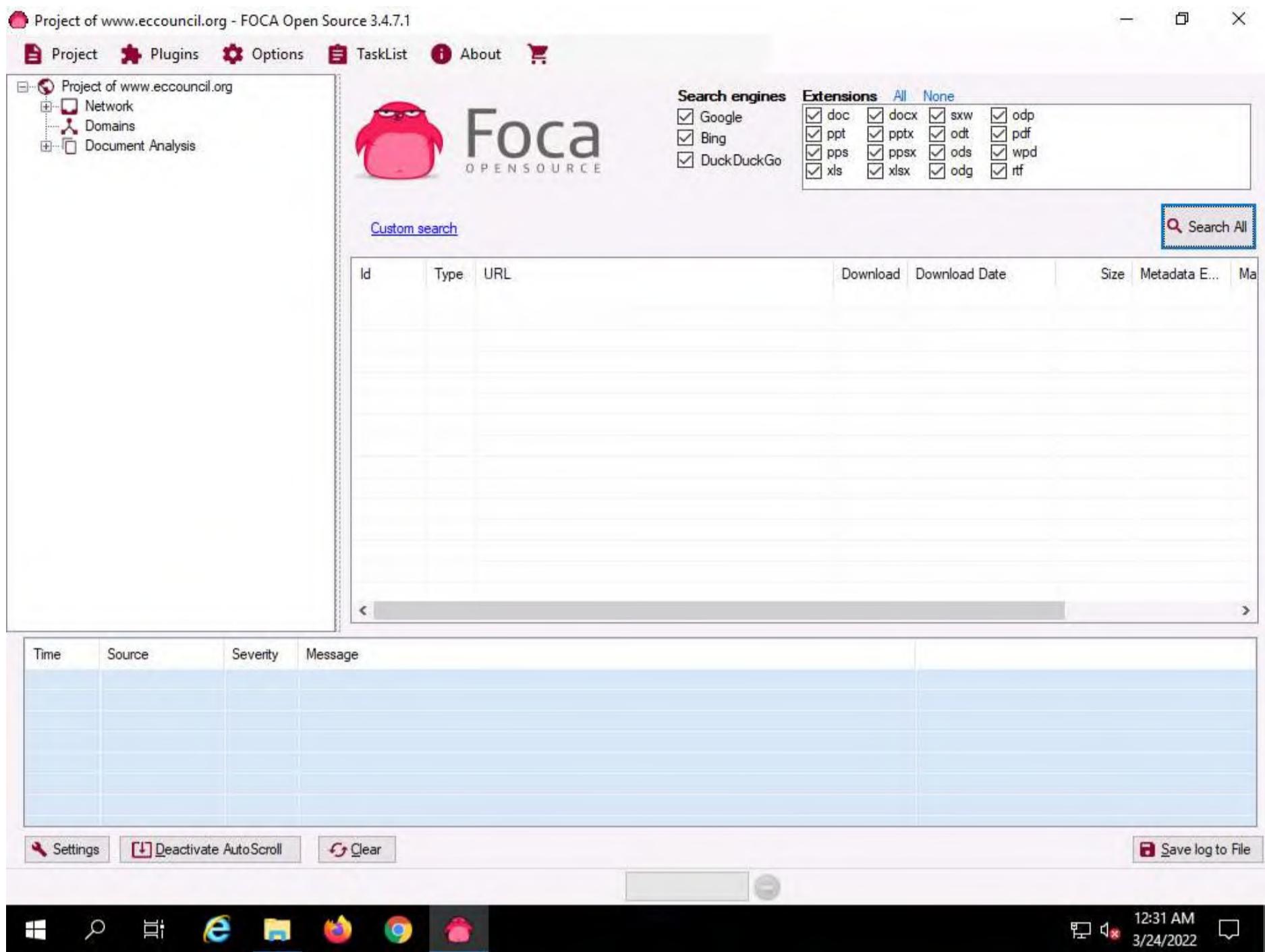




8. The Project saved successfully pop-up appears, click OK to close it.



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



ID	Type	URL	Download	Download Date	Size	Metadata E...	Malware An...	Modified Date
10	pdf	https://aspen.eccouncil.org/Docs/Exam-Guides/ECCExam-RPS-UserGuide...	X	-	2.98 MB	X	X	-
11	html	https://cert.eccouncil.org/announcements.html	X	-	-	X	X	-
12	pdf	https://cert.eccouncil.org/images/doc/CHFI-New-Blueprint-v3.pdf	X	-	823.25 KB	X	X	-
13	pdf	https://cert.eccouncil.org/images/doc/CHFI-Exam-Blueprint-v2.1.pdf	X	-	5.09 MB	X	X	-
14	pdf	https://aspen.eccouncil.org/Docs/UserGuides/AccessCourseware-UserGu...	X	-	433.5 KB	X	X	-
15	pdf	https://cert.eccouncil.org/images/doc/CHFI Handbook v1.pdf	X	-	17.07 MB	X	X	-
16	pdf	https://cert.eccouncil.org/images/doc/CEH-Exam-Blueprint-v4.0.pdf	X	-	158.28 KB	X	X	-
17	pdf	https://tyjackson.wiksite.com/catholic/individual-presentations	X	-	-	X	X	-
18	pdf	https://ciso.eccouncil.org/wp-content/uploads/2013/09/CCISO-Table-of-Co...	X	-	933.61 KB	X	X	-
19	pdf	https://aspen.eccouncil.org/BecomeAnATC	X	-	-	X	X	-
20	pdf	https://cert.eccouncil.org/images/doc/CEH-Handbook-v5.pdf	X	-	6.79 MB	X	X	-
21	pdf	https://cert.eccouncil.org/Images/doc/CHFI-Handbook-v5.pdf	X	-	2.13 MB	X	X	-
22	pdf	https://aspen.eccouncil.org/Docs/Applications/ATC application Form v7.0.pdf	X	-	1.24 MB	X	X	-
23	pdf	https://aspen.eccouncil.org/Docs/CISOMAG/CISO-MAG-October2020-Prev...	X	-	34.3 MB	X	X	-
24	pdf	https://cert.eccouncil.org/images/doc/CND-Handbook-v5.pdf	X	-	8.62 MB	X	X	-
25	pdf	https://cert.eccouncil.org/images/doc/CEH-Handbook-v6.pdf	X	-	6.7 MB	X	X	-
26	pdf	https://aspen.eccouncil.org/Docs/UserGuides/Instructions-AccessCourse...	X	-	436.24 KB	X	X	-
27	pdf	https://cert.eccouncil.org/images/doc/CND Handbook v1B.pdf	X	-	12.36 MB	X	X	-
28	pdf	https://cert.eccouncil.org/images/doc/ECSA Handbook v1.pdf	X	-	3.89 MB	X	X	-

Time	Source	Severity	Message
12:50:57...	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: The remote server returned an error: (403) Forbidden..
12:51:00...	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 3
12:51:00...	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 90

All searchers have finished

Save log to File

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**.

Project of www.eccouncil.org - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Foca OPEN SOURCE

Search engines: Google, Bing, DuckDuckGo

Extensions: All, None

Extension	doc	docx	sxw	odp
ppt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
pps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
xls	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
pdf				
odt				
ods				
wpd				
rtf				

Custom search

Search All

ID	Type	URL	Download	Download Date	Size	Metadata E...	Malware An...	Modified Date
1	pdf	https://aspen.eccouncil.org/Docs/Exam-Guides/ECCExam-RPS-UserGuide.pdf	-	-	2.20 MB	X	X	-
2	html	https://cert.eccouncil.org/announcements.html	-	-	5 KB	X	X	-
3	pdf	https://cert.eccouncil.org/images/doc/CHFI-New-Blueprint-v3.pdf	-	-	0 MB	X	X	-
4	pdf	https://cert.eccouncil.org/images/doc/CHFI-Exam-Blueprint-v2.1.pdf	-	-	5 KB	X	X	-
5	pdf	https://aspen.eccouncil.org/Docs/UserGuides/AccessCourseware-UserGu...	-	-	7 MB	X	X	-
6	pdf	https://cert.eccouncil.org/images/doc/CHFI Handbook v1.pdf	-	-	3 KB	X	X	-
7	pdf	https://tyjackson.wiksite.com/catholic/individual-presentations	-	-	1 KB	X	X	-
8	pdf	https://ciso.eccouncil.org/wp-content/uploads/2013/09/CCISO-Table-of-Co...	-	-	1 MB	X	X	-
9	pdf	https://aspen.eccouncil.org/BecomeAnATC	-	-	0 MB	X	X	-
10	pdf	https://cert.eccouncil.org/images/doc/CEH-Handbook-v5.pdf	-	-	0 MB	X	X	-
11	pdf	https://cert.eccouncil.org/Images/doc/CHFI-Handbook-v5.pdf	-	-	0 MB	X	X	-
12	pdf	https://aspen.eccouncil.org/Docs/Applications/ATC application Form v7.0.p...	-	-	0 MB	X	X	-
13	pdf	https://aspen.eccouncil.org/Docs/CISOMAG/CISO-MAG-October2020-Prev...	-	-	0 MB	X	X	-
14	pdf	https://cert.eccouncil.org/images/doc/CND-Handbook-v5.pdf	-	-	0 MB	X	X	-
15	pdf	https://cert.eccouncil.org/images/doc/CEH-Handbook-v6.pdf	-	-	0 MB	X	X	-
16	pdf	https://aspen.eccouncil.org/Docs/UserGuides/Instructions-AccessCourse...	-	-	4 KB	X	X	-
17	pdf	https://cert.eccouncil.org/images/doc/CND Handbook v1B.pdf	-	-	6 MB	X	X	-
18	pdf	https://cert.eccouncil.org/Images/doc/ECSA Handbook v1.pdf	-	-	0 MB	X	X	-

Download, Extract Metadata, Analyze Malware, Delete, Download All, Extract All Metadata, Analyze All Metadata, Analyze All Malware, Delete All, Add file, Add folder, Add URLs from file

Link(s), Open in browser, Copy to clipboard

Settings, Deactivate AutoScroll, Clear, Save log to File

All searchers have finished

12:50:57... MetadataSearch error An error has occurred on DuckDuckGoWeb: The remote server returned an error: (403) Forbidden

12:51:00... MetadataSearch medium BingWeb search finished successfully!! Total found result count: 3

12:51:00... MetadataSearch medium GoogleWeb search finished successfully!! Total found result count: 90

12:55 AM 3/24/2022

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

ECC Exam Online Proctoring Services User Guide 201...

1 / 46 80%

EC-Council

ECC EXAM CENTER & REMOTE PROCTORING SERVICES USER GUIDE

Welcome to EC-Council

The EC-Council Exam Center is the leading provider of IT certification and training services.

1. Introduction to EC-Council

2. Remote Proctoring Services

3. User Guide

4. Frequently Asked Questions

12:55 AM 3/24/2022

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.

The screenshot shows the FOCA interface with the following details:

- Project of www.eccouncil.org - FOCA Open Source 3.4.7.1**
- Project**, **Plugins**, **Options**, **TaskList**, **About**, **Cart** buttons.
- Network** node expanded in the left sidebar, showing **Clients (0)** and **Servers (0)**.
- Select search type** section:
 - WebSearch**: Using a web searcher like Google or Bing the program searches for links pointing to the domain site to identify new subdomains. Options: Google, DuckDuckGo, Bing.
 - Bing web limitations:**
 - Max 1000 results for each search
 - Max 49 words for each string
 - Dictionary Search**: The program uses a common DNS names list to find new subdomains.
 - IP Bing**: Bing allows search links located in a particular IP address. This functionality can be used to find domains that share IP Address. Options: Bing Web, Bing API.
 - Bing web limitations:**
 - Max 1000 results for each search
 - Max 49 words for each string
 - Shodan**: Activating this option, network algorithm will search all IP addresses belonging to all Netranges in Project to Shodan. It will send a query for each IP address and will retrieve software information and new dom names.
- Current search: None** button.
- Log Table** (Time, Source, Severity, Message):

Time	Source	Severity	Message
12:50:57...	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: The remote server returned an error: (403) Forbidden..
12:51:00...	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 3
12:51:00...	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 90
- Buttons**: , , , .
- System Tray**: All searchers have finished, 12:58 AM, 3/24/2022.

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.



Project of www.eccouncil.org - FOCA Open Source 3.4.7.1

Attribute Value

Domain - Source
eccouncil.org DuckDuckGoWeb > Inferred by aspen.eccouncil.org [eccouncil.org]

IP Addresses - Source
104.18.21.251 DuckDuckGoWeb > Inferred by aspen.eccouncil.org [eccouncil.org] > DNS resolution [104.18.21.251]
104.18.20.251 DuckDuckGoWeb > Inferred by aspen.eccouncil.org [eccouncil.org] > DNS resolution [104.18.20.251]

Technology recognition | Crawling | Log |

Technology Recognition

Domain: eccouncil.org

Files (0 found) | Folders (0 found) | Documents published (0 found) | Parameterized (0 found)

File	Extension

Time Source Severity Message

12:50:57... MetadataSearch error An error has occurred on DuckDuckGoWeb: The remote server returned an error: (403) Forbidden..
12:51:00... MetadataSearch medium BingWeb search finished successfully!! Total found result count: 3
12:51:00... MetadataSearch medium GoogleWeb search finished successfully!! Total found result count: 90

Settings | Deactivate AutoScroll | Clear | Save log to File

All searchers have finished

12:59 AM 3/24/2022

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

Project of www.eccouncil.org - FOCA Open Source 3.4.7.1

Attribute Value

Domain - Source
eccouncil.org DuckDuckGoWeb > Inferred by aspen.eccouncil.org [eccouncil.org]

IP Addresses - Source
104.18.21.251 DuckDuckGoWeb > Inferred by aspen.eccouncil.org [eccouncil.org] > DNS resolution [104.18.21.251]
104.18.20.251 DuckDuckGoWeb > Inferred by aspen.eccouncil.org [eccouncil.org] > DNS resolution [104.18.20.251]

Technology recognition | **Crawling** | Log |

Google crawling | **Bing crawling** | **DuckDuckGo crawling**

Domain: eccouncil.org

Files (0 found) | Folders (0 found) | Documents published (0 found) | Parameterized (0 found)

File	Extension

Time Source Severity Message

12:50:57... MetadataSearch error An error has occurred on DuckDuckGoWeb: The remote server returned an error: (403) Forbidden..
12:51:00... MetadataSearch medium BingWeb search finished successfully!! Total found result count: 3
12:51:00... MetadataSearch medium GoogleWeb search finished successfully!! Total found result count: 90

Settings | Deactivate AutoScroll | Clear | Save log to File

All searchers have finished

1:06 AM 3/24/2022

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.

The screenshot shows the FOCA Open Source 3.4.7.1 interface. The left sidebar displays a tree view of the project structure under "Project of www.eccouncil.org". The "Domains" node is expanded, showing "comcastbusiness.net", "eccouncil.org", and "www.eccouncil.org". The "Document Analysis" node is also present. The main pane contains several sections: "Attribute" and "Value" for "Domain - Source" (eccouncil.org) and "IP Addresses - Source" (104.18.21.251, 104.18.20.251); "Technology recognition" with tabs for "Crawling" (selected), "Log", "Google crawling", "Bing crawling", and "DuckDuckGo crawling"; a search bar for "Domain: eccouncil.org" with filters for "Files (0 found)", "Folders (0 found)", "Documents published (0 found)", and "Parameterized (0 found)"; and a log table with columns "Time", "Source", "Severity", and "Message". The log table entries show various search activities and errors. At the bottom, there are buttons for "Settings", "Deactivate AutoScroll", "Clear", and "Save log to File". The taskbar at the bottom of the window shows the Windows Start button, a search icon, a file icon, a browser icon, a Google Chrome icon, and the CyberQ icon. The system tray shows the date and time as 1:10 AM on 3/24/2022.

Time	Source	Severity	Message
12:50:57 ...	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: The remote server returned an error: (403) Forbidden..
12:51:00 ...	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 3
12:51:00 ...	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 90
1:07:49 ...	Crawling	medium	Domain found: egs.eccouncil.org
1:07:49 ...	Crawling	medium	Domain found: careers.eccouncil.org
1:07:49 ...	Crawling	medium	Domain found: codered.eccouncil.org
1:07:49 ...	Crawling	medium	Domain found: iclass.eccouncil.org
1:07:49 ...	Crawling	medium	Domain found: ilabs.eccouncil.org
1:07:49 ...	Crawling	medium	Domain found: store.eccouncil.org
1:07:49 ...	Crawling	medium	Domain found: cismag.eccouncil.org
1:07:50 ...	Crawling	medium	Domain found: aware.eccouncil.org
1:07:50 ...	Crawling	medium	Domain found: foundation.eccouncil.org
1:07:50 ...	Crawling	medium	Domain found: masterclass.eccouncil.org
1:07:51 ...	Crawling	medium	Domain found: cyberq.eccouncil.org

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.



The screenshot shows the FOCA Open Source 3.4.7.1 application window. At the top, there's a navigation bar with Project, Plugins, Options, TaskList, About, and a shopping cart icon. Below the navigation is a sidebar with a tree view of a project named "Project of www.eccouncil.org". The "Document Analysis" section is expanded, showing "Files (0/122)" and "Metadata Summary". The "Metadata Summary" section is selected and expanded, listing categories like Users (0), Folders (0), Printers (0), Software (0), Emails (0), Operating Systems (0), Passwords (0), Servers (0), and Malware Summary (DIARIO). To the right of the sidebar is a search configuration panel with tabs for "Search engines" (Google, Bing, DuckDuckGo) and "Extensions" (doc, docx, sxw, odp, ppt, pptx, odt, pdf, pps, ppsx, ods, wpd, xls,xlsx, odg, rtf). Below this is a "Custom search" table with columns: Id, Type, URL, Download, Download Date, Size, Metadata E..., Malware An..., and Mod. The table contains 18 rows of search results. At the bottom of the search panel is a log table with columns: Time, Source, Severity, and Message. The log shows three entries: an error from DuckDuckGoWeb, a medium severity message from BingWeb, and a medium severity message from GoogleWeb. Below the log are buttons for Settings, Deactivate AutoScroll, Clear, and Save log to File. The system tray at the bottom right shows the date and time as 1:04 AM 3/24/2022.

Time	Source	Severity	Message
12:50:57...	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: The remote server returned an error: (403) Forbidden..
12:51:00...	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 3
12:51:00...	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 90

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

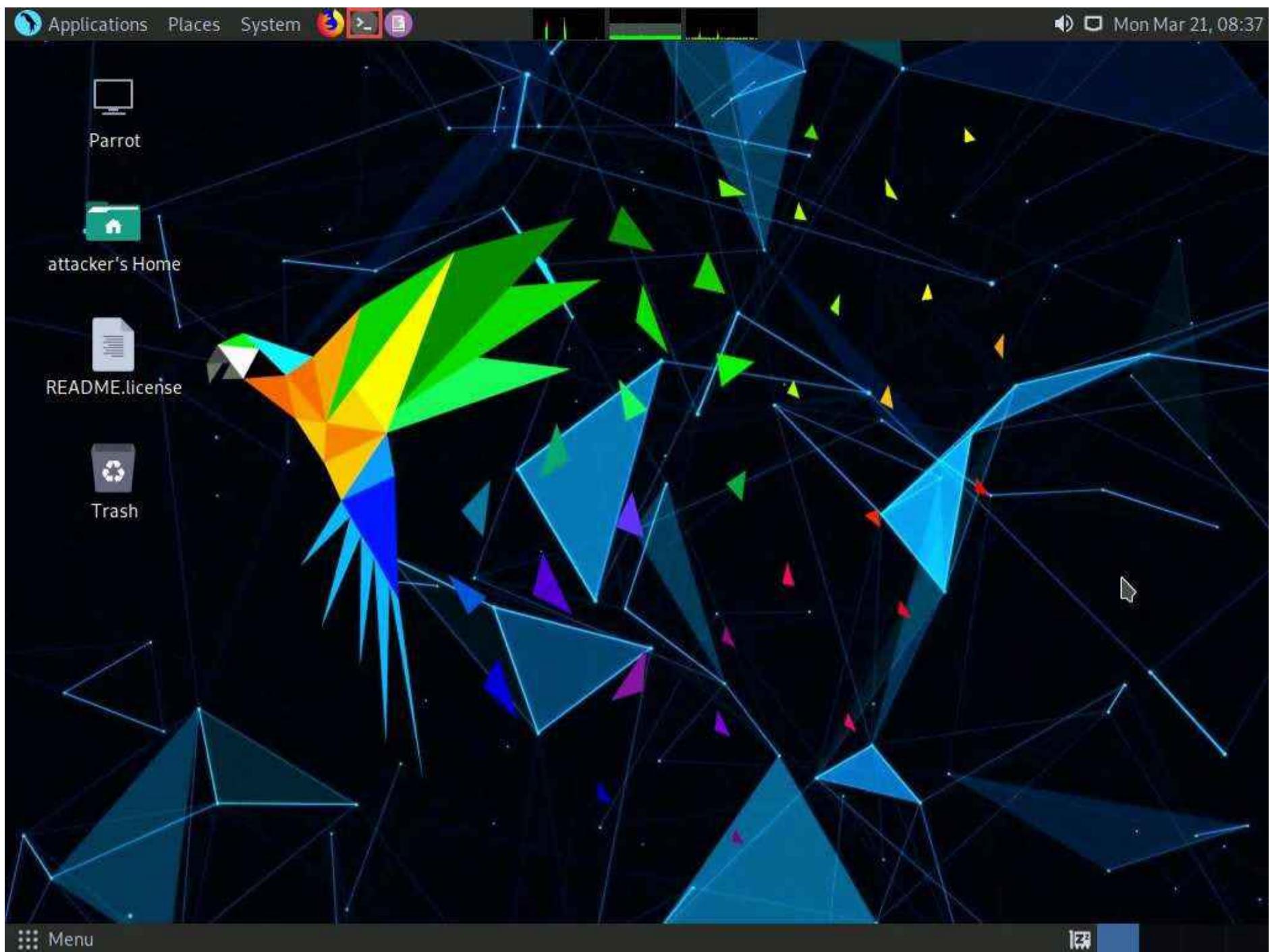
23. Close all open windows and document all the acquired information.

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.



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

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

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd BillCipher
[root@parrot] ~
# python3 billcipher.py
```

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

```
python3 bllcipher.py - Parrot Terminal  
File Edit View Search Terminal Help  
##### # #####  
# # # # # # # # # # # # # # # # # # # # # #  
# # # # # # # # # # # # # # # # # # # # # #  
##### # # # # # # # # # # # # # # # # # # # #  
# # # # # # # # # # # # # # # # # # # # # #  
# # # # # # # # # # # # # # # # # # # # # #  
##### # ##### ##### ##### # # # # # ##### # # 2.1  
Information Gathering tool for a Website or IP address
```

Are you want to collect information of website or IP address? [website/IP]: website

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

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

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.



The terminal window shows the following text:

```
#      # # #      #      # # #      #      # #      #      #
##### # ##### ##### ##### # #      #      # ##### #      # 2.1
Information Gathering tool for a Website or IP address

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)

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
```

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



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

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. When the option "Are you want to collect information of a website or IP address?" 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.

```

Applications Places System python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
python3 billcipher.py - Parrot Terminal
Mon Mar 21, 08:50

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

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

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

What information would you like to collect? (1-20): 4

```

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.

The screenshot shows a terminal window with the following content:

```

Applications Places System python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
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): 4
Address      = 162.241.216.11
Network      = 162.241.216.11 / 32
Netmask      = 255.255.255.255
Broadcast    = not needed on Point-to-Point links
Wildcard Mask = 0.0.0.0
Hosts Bits   = 0
Max. Hosts   = 1 (2^0 - 0)
Host Range   = { 162.241.216.11 - 162.241.216.11 }

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

```

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.



```
python3 billcipher.py - Parrot Terminal
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)

What information would you like to collect? (1-20): 6
http://certifiedhacker.com/P-folio/index.html
http://certifiedhacker.com/Online Booking/index.htm
http://certifiedhacker.com/corporate-learning-website/01-homepage.html
http://certifiedhacker.com/Real Estates/index.html
http://certifiedhacker.com/Recipes/index.html
http://certifiedhacker.com/Social Media/index.html
http://certifiedhacker.com/Turbo Max/index.htm
http://certifiedhacker.com/Under Construction/index.html
http://certifiedhacker.com/Under the trees/index.html
http://certifiedhacker.com/

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

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.

```
Applications Places System python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help

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)

What information would you like to collect? (1-20): 8
HTTP/1.1 200 OK
Date: Mon, 21 Mar 2022 12:52:46 GMT
Server: nginx/1.19.10
Content-Type: text/html
Content-Length: 3228
Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
host-header: c2hhcmVkLmJsdWob3N0LmNvbQ==
X-Server-Cache: true
X-Proxy-Cache: HIT
Accept-Ranges: bytes

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

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.

The terminal window shows the following output:

```

Applications Places System python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
Content-Encoding: gzip
host-header: c2hhcmVkLmJsdWob3N0LmNvbQ==
X-Server-Cache: true
X-Proxy-Cache: HIT
Accept-Ranges: bytes

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

What information would you like to collect? (1-20): 9
www.certifiedhacker.com, 162.241.216.11

```

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.

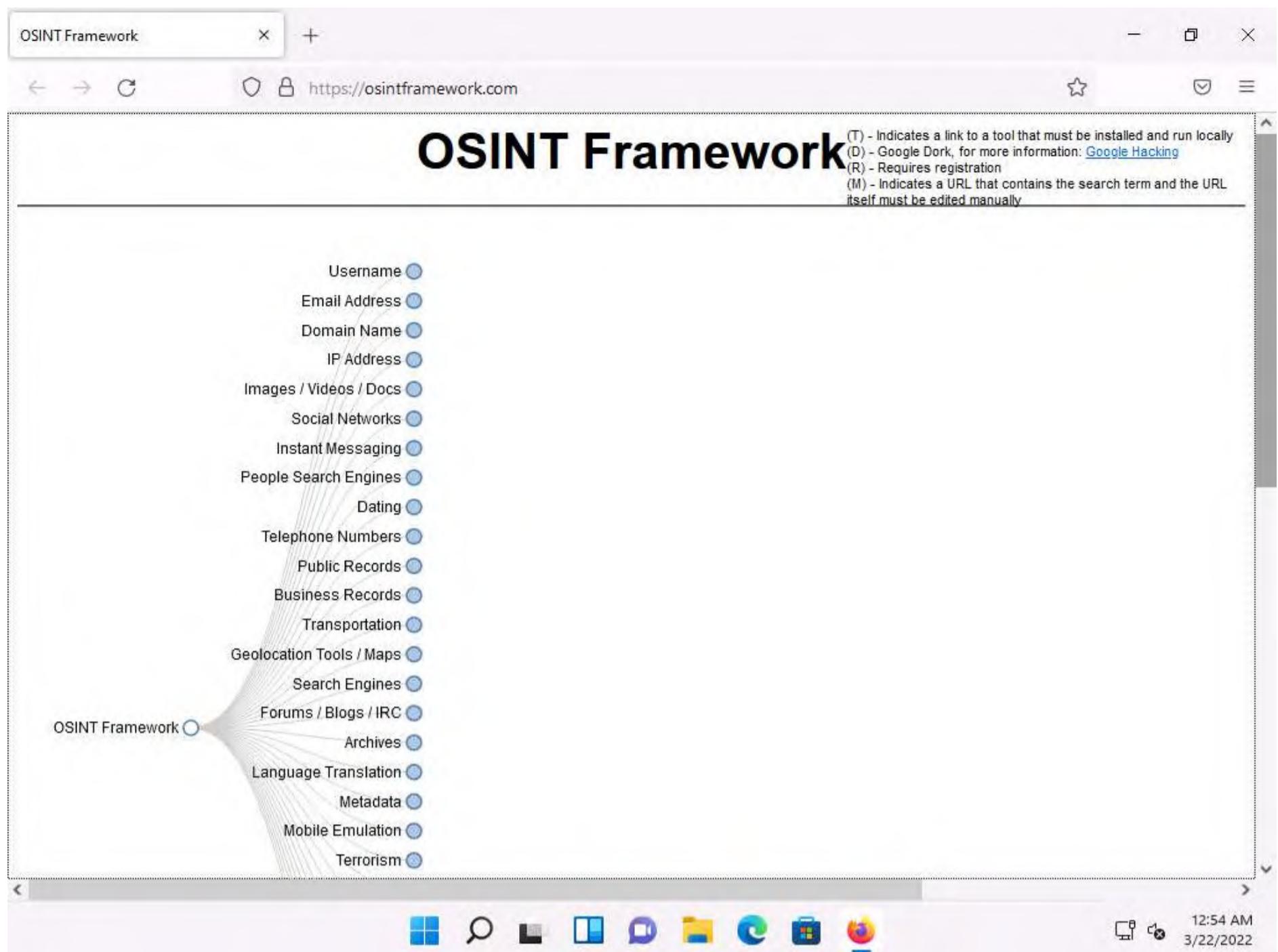
The OSINT Framework includes the following indicators with the available tools:

- (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

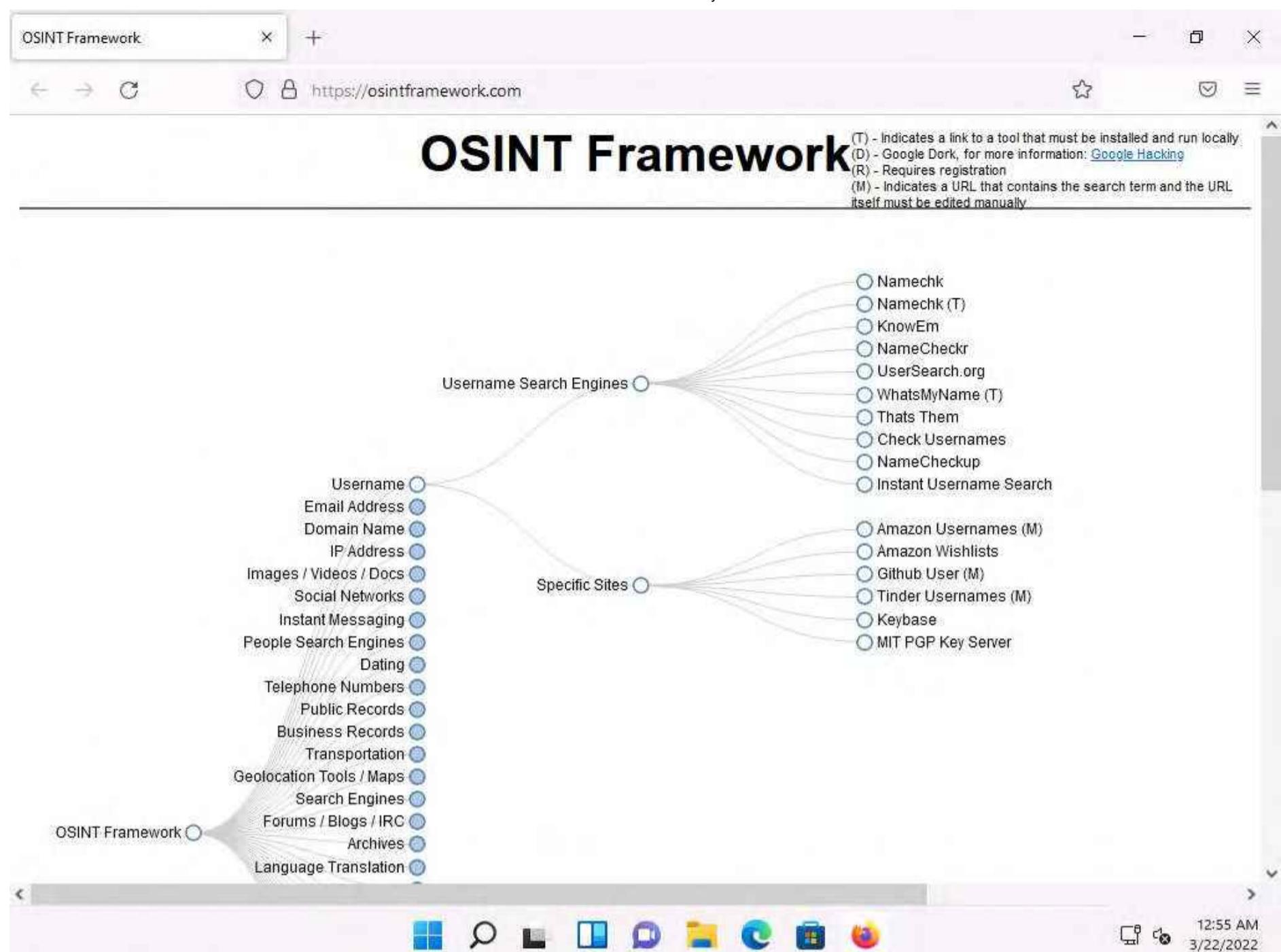
Here, we will use the OSINT Framework to explore footprinting categories and associated tools.

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.

The screenshot shows the NameCheckr website interface. At the top, there is a navigation bar with links for "Home", "Domains", and "Help". Below the navigation bar, a banner features the text "Identify 'high intent' buyers, close deals & scale faster" and "SLINTEL". On the left, there is a search bar with the placeholder "Enter your brand name to begin..". To the right of the search bar is a "Free Demo" button. The main content area displays a grid of icons and labels representing various platforms and domains. The grid is organized into rows:

- Row 1:** .com (Ready...), Facebook (Ready...), Twitter (Ready...), Tumblr (Ready...), Reddit (Ready...).
- Row 2:** Slack (Ready...), Twitch (Ready...), .net (Ready...), myspace (Ready...), YouTube (Ready...).
- Row 3:** Meetup (Ready...), Pinterest (Ready...), Dribbble (Ready...), .org (Ready...), Github (Ready...).
- Row 4:** Vimeo (Ready...), ello (Ready...), Feedburner (Ready...), Foursquare (Ready...), lastfm (Ready...).
- Row 5:** .co (Ready...), aboutme (Ready...), flickr (Ready...), Wordpress (Ready...), Blogger (Ready...).

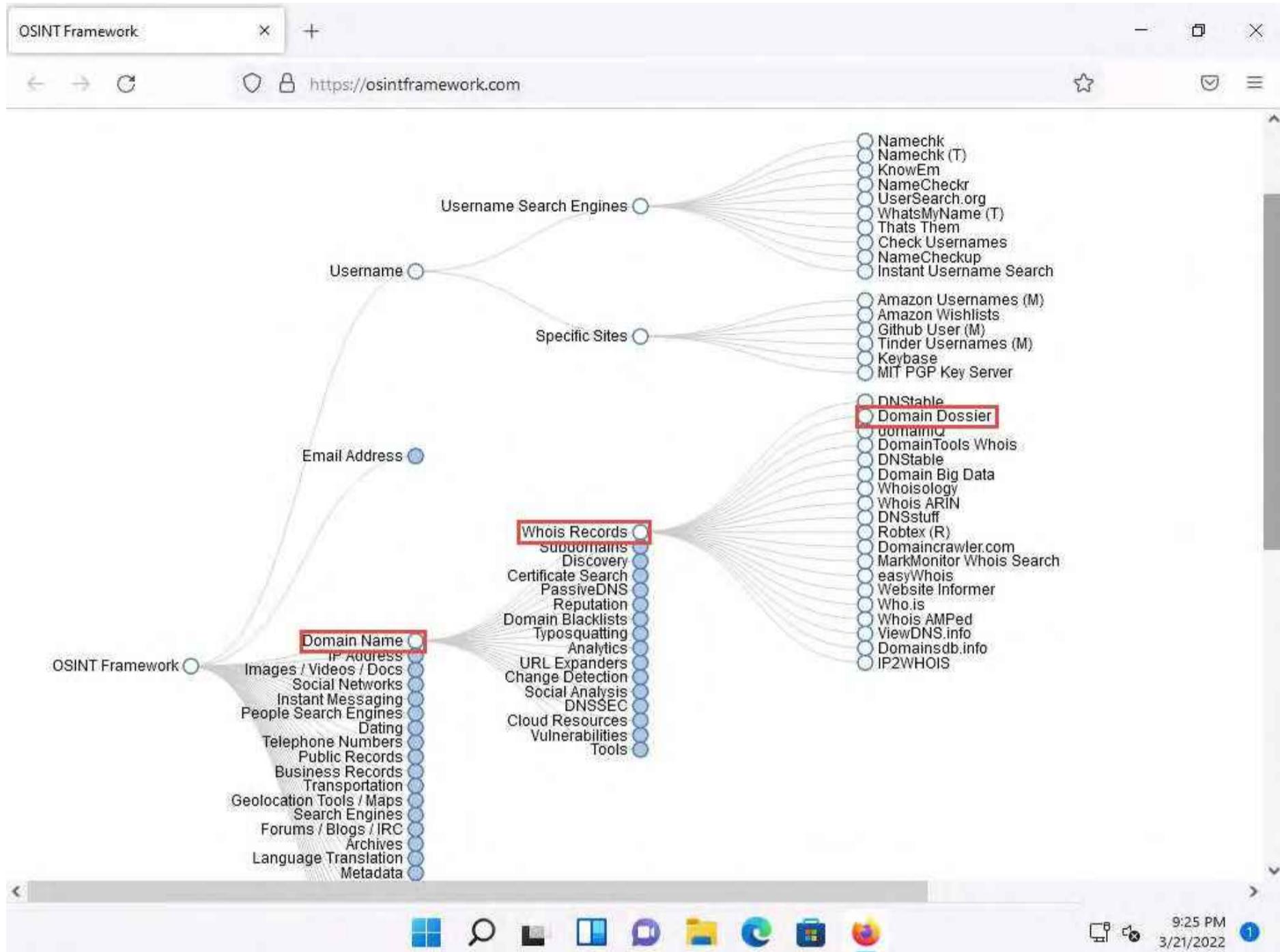
At the bottom of the page, there is a standard Windows taskbar with icons for File Explorer, Task View, Start, and others. The status bar at the bottom right shows the time as 9:24 PM and the date as 3/21/2022.

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

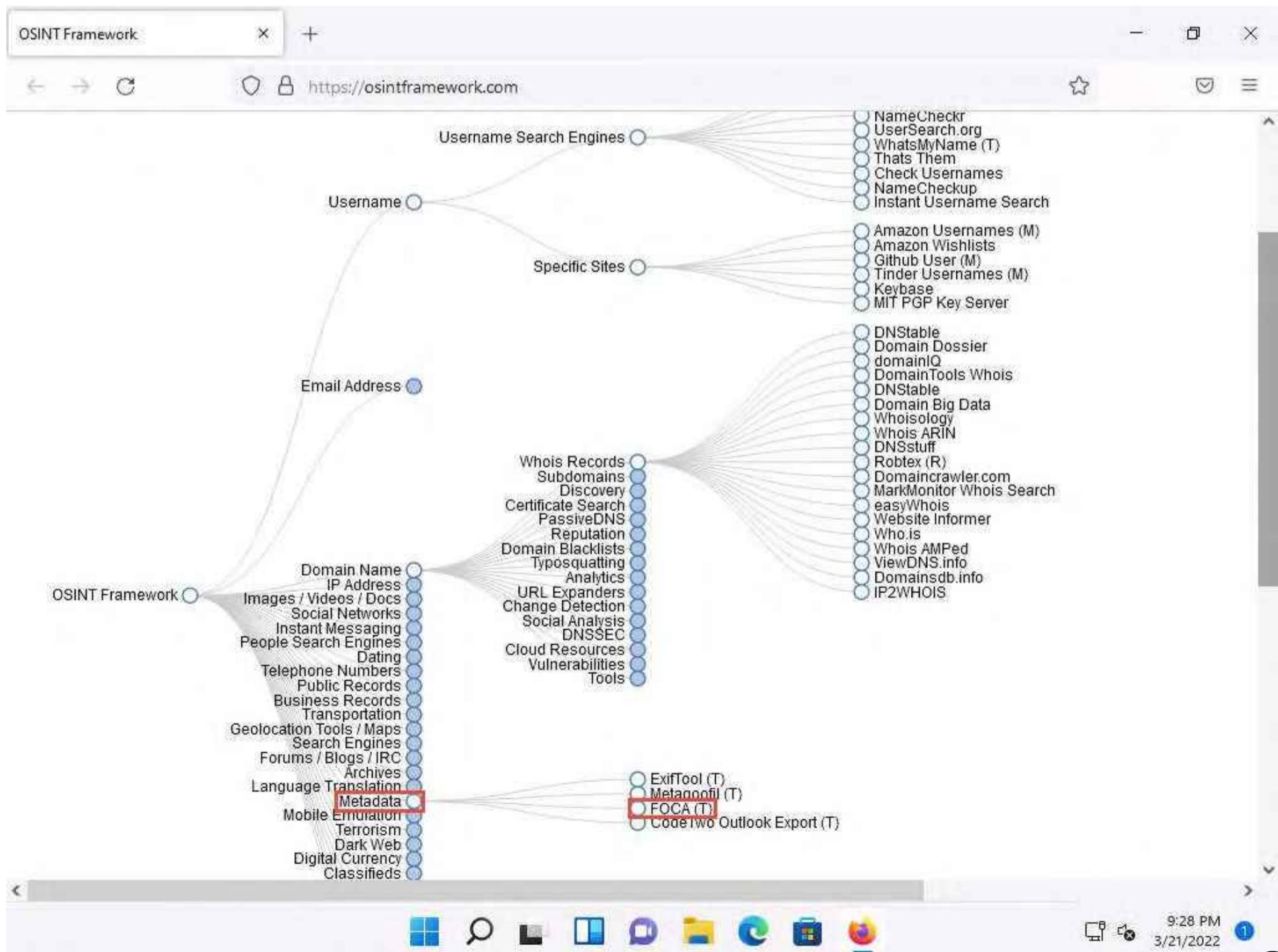
The Domain Dossier tool generates **reports from public records** about domain names and IP addresses to help solve problems, investigate cybercrime, or just better understand how things are set up. These reports may show you:

- 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.

OSINT Framework X Foca | Innovation and Lab | Telefónica Tech Cyber Security https://www.elevenpaths.com/innovation-labs/technologies/foca

HOME / INNOVATION AND LABS / TECHNOLOGIES / FOCA

FOCA

THREAT INTELLIGENCE

FOCA is a tool used mainly to find metadata and hidden information in the documents

Foca
OPENSOURCE

Windows Taskbar: 9:30 PM 3/21/2022

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.