University of Babylon
College of information Technology
Department of Information Security

Ethical Hacking

Lab 3 & 4: Footprinting and Reconnaissance

Rasha Hussein, Shahad A. Hussein, Hasan Abdulameer, Duha Fadel

Footprinting and Reconnaissance

1. Gather Information using Advanced Google Hacking Techniques
2. Gather Information from FTP Search Engines
3. Website Footprinting
4. Email Footprinting
5. Whois Footprinting
6. DNS Footprinting
7. Network Footprinting

1- Search engines are the main information sources

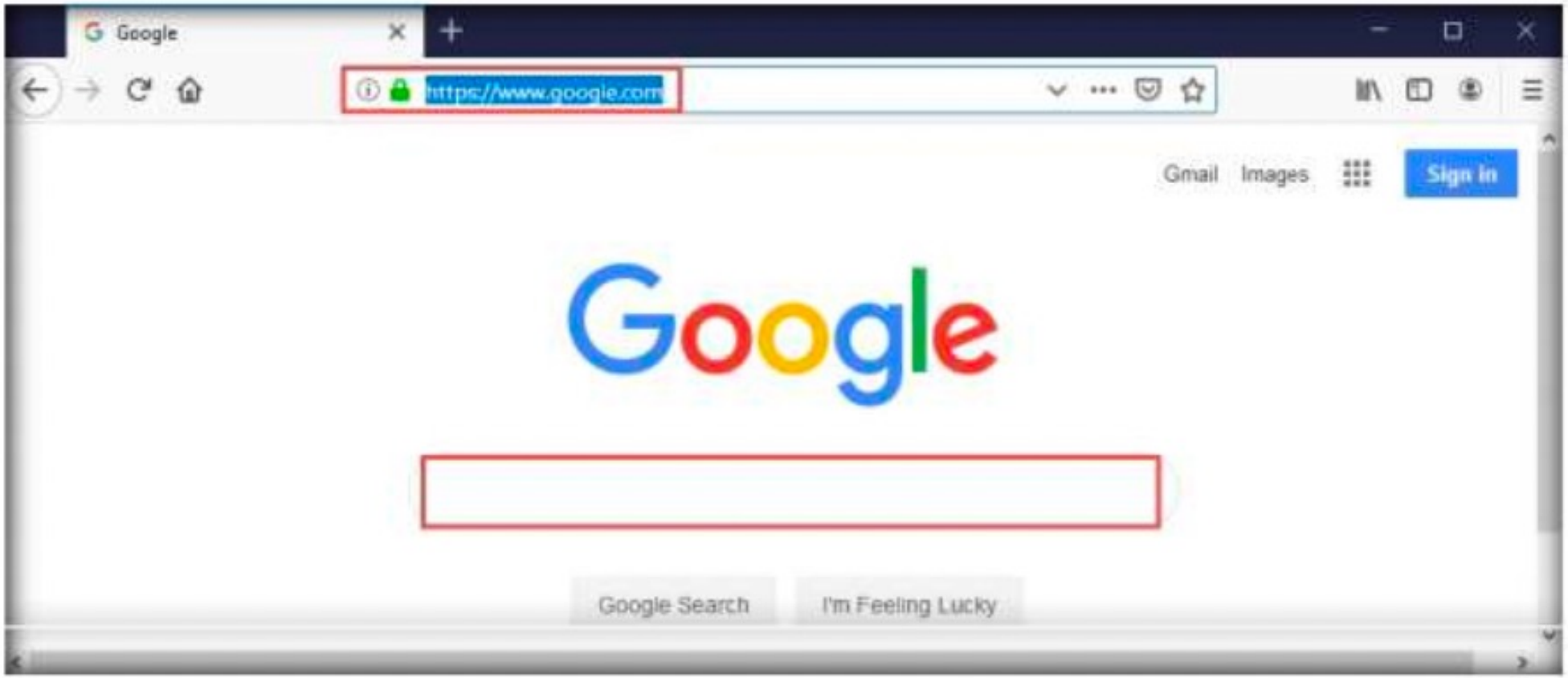
2- Footprinting is the first step of any attack, the attacker collects information about a target network.

1

Gather Information using Advanced Google Hacking Techniques

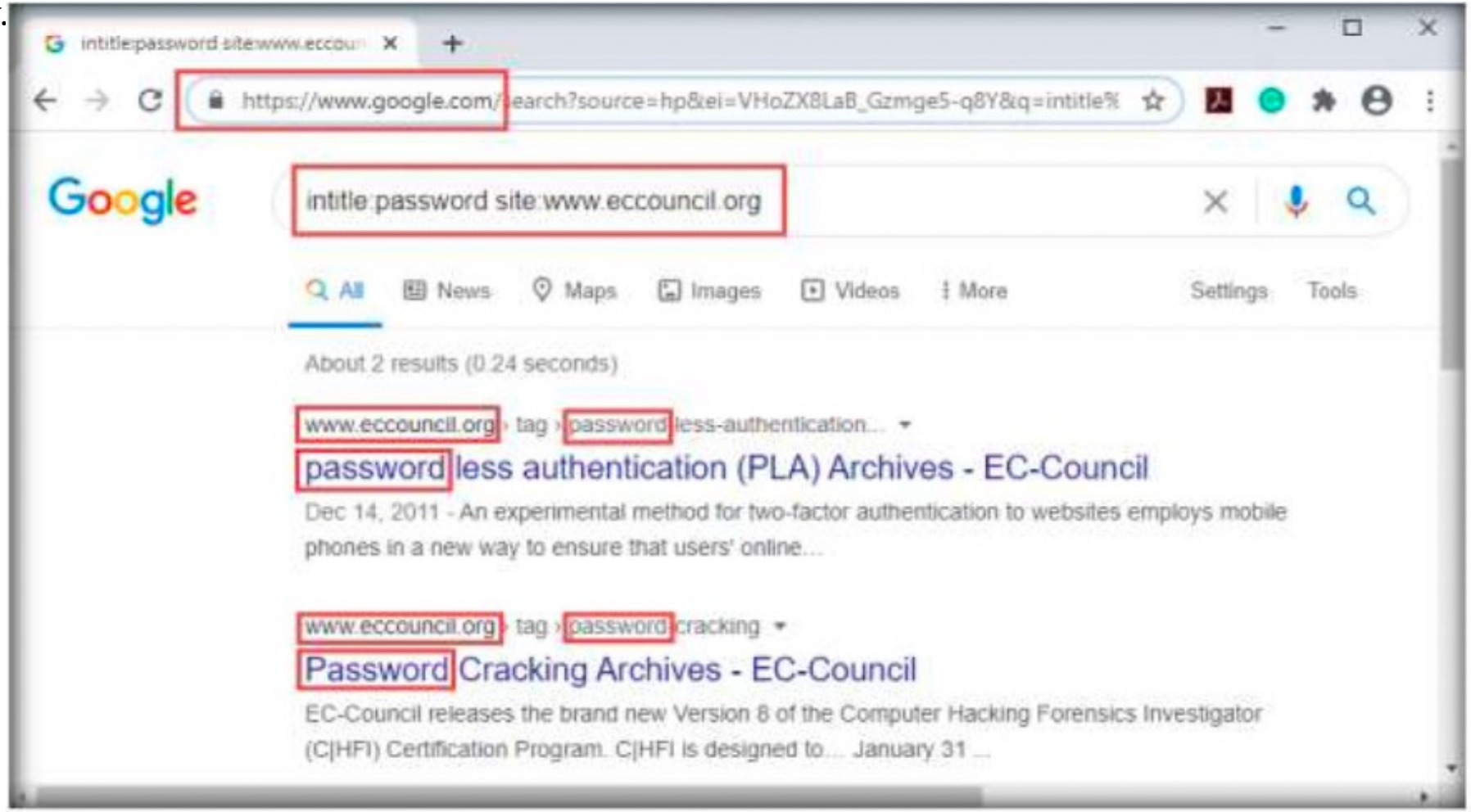
Perform Footprinting Through Search Engines

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



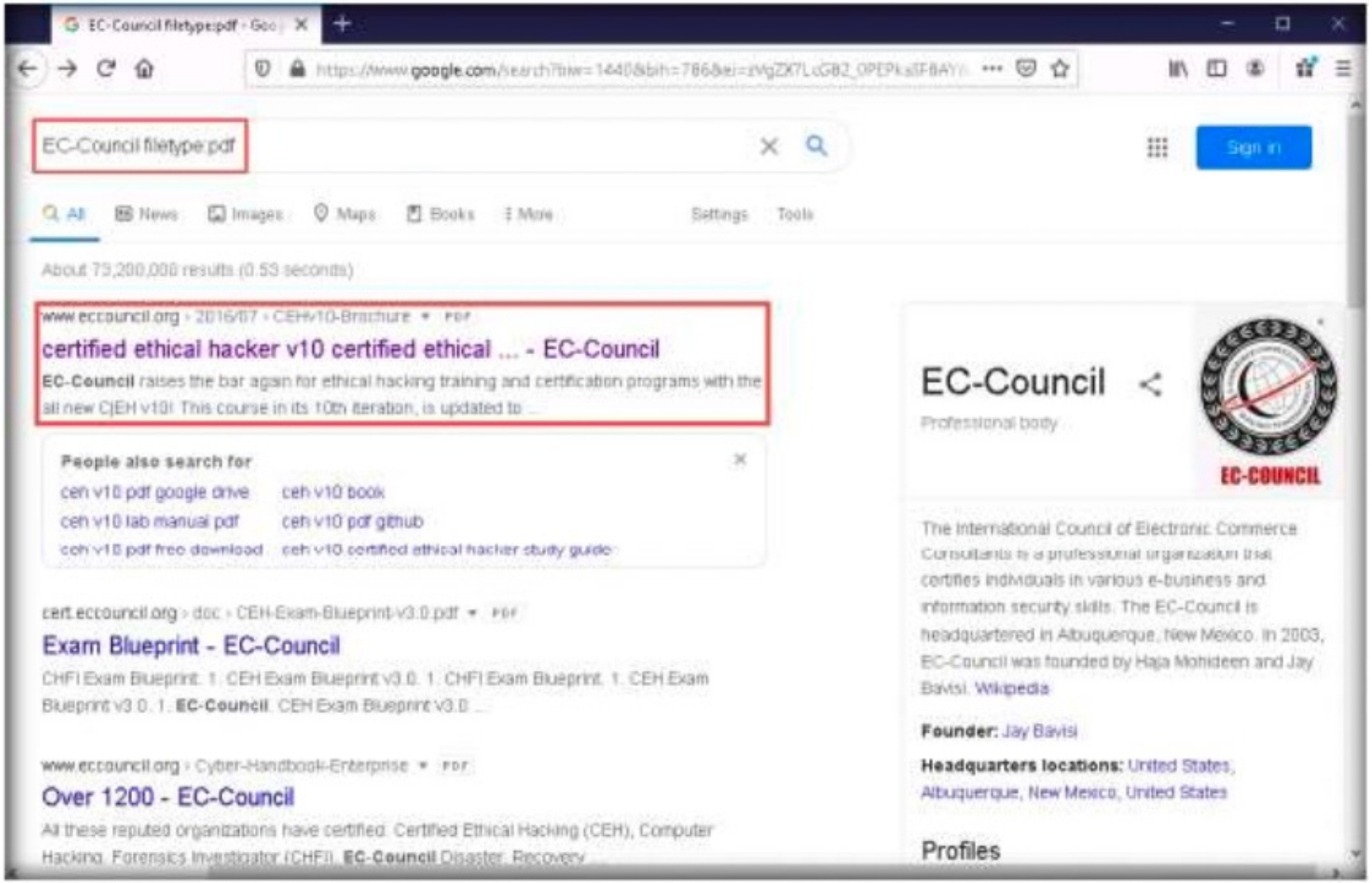
Gather Information using Advanced Google Hacking Techniques

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

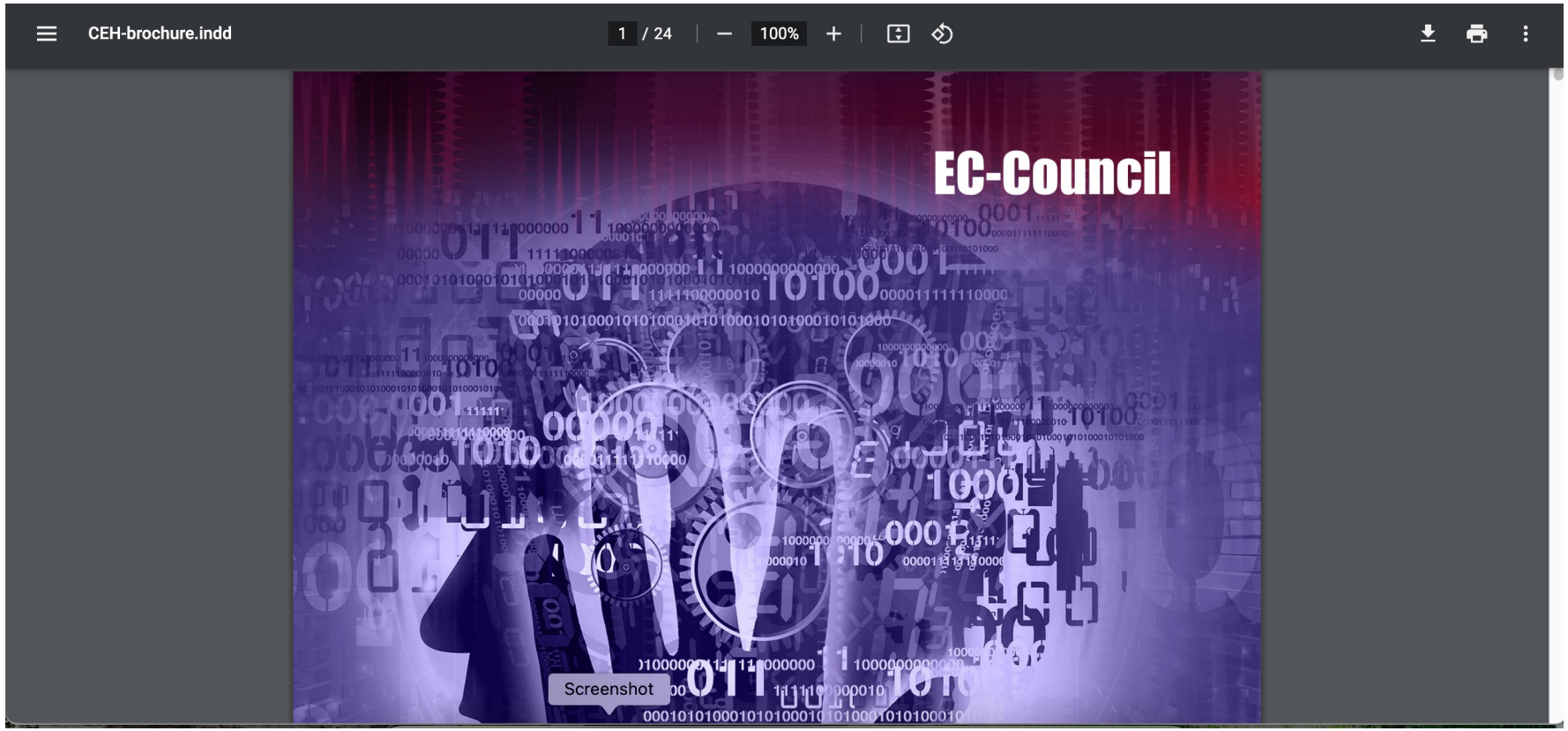


Gather Information using Advanced Google Hacking Techniques

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



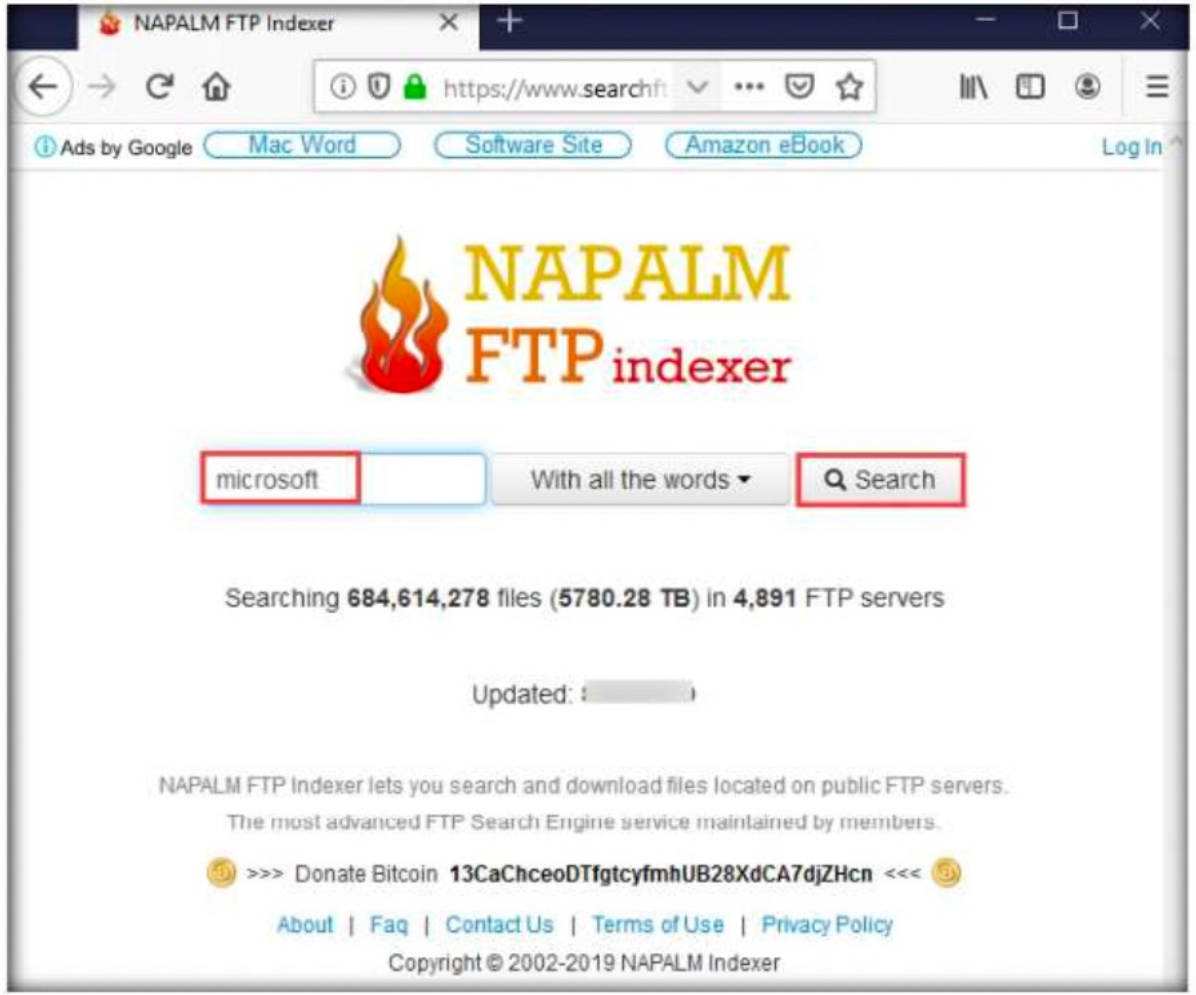
4. The page appears displaying the **PDF** file, as shown in the screenshot.



2

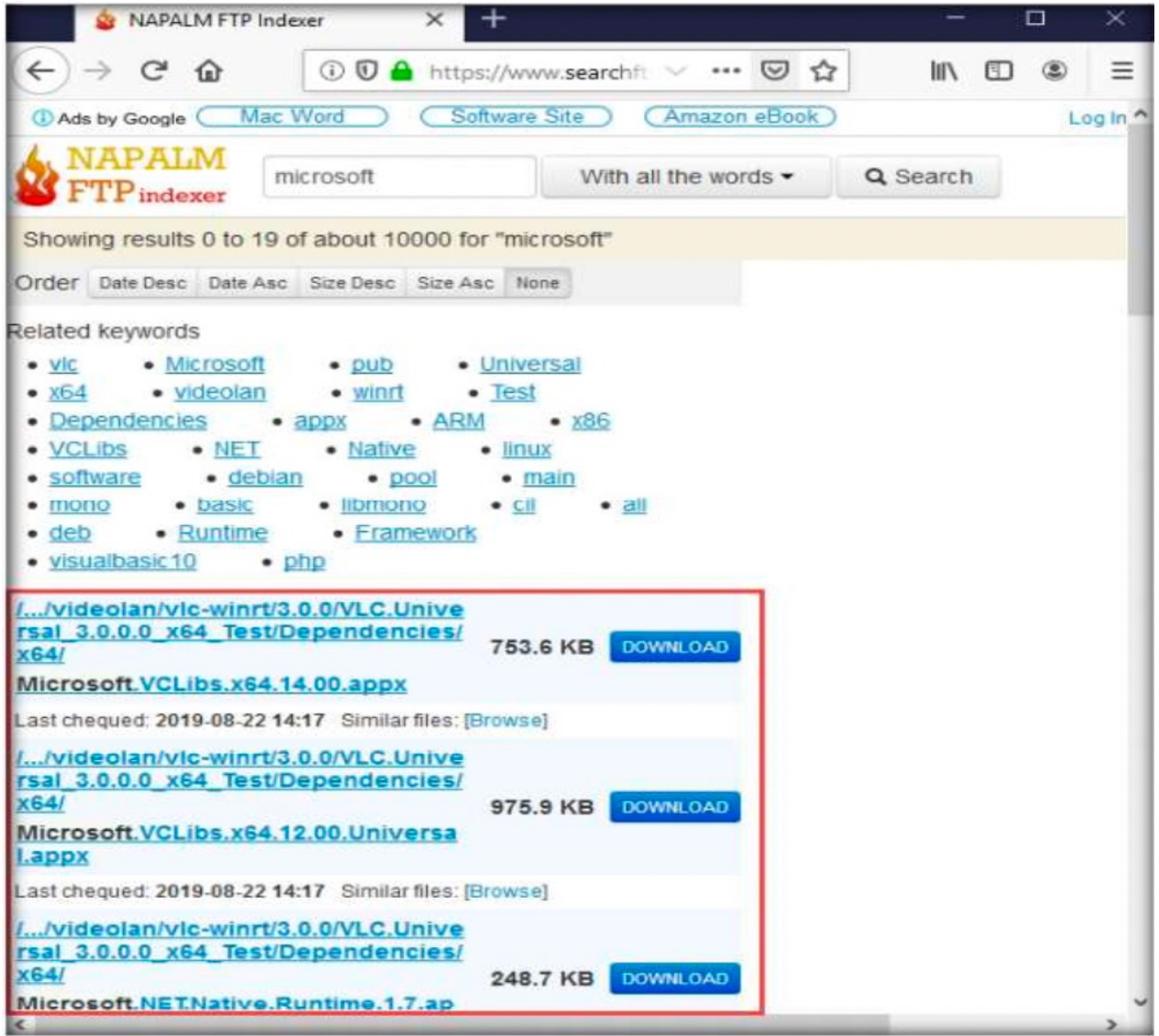
Gather Information from FTP Search Engines

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



Gather Information from FTP Search Engines

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



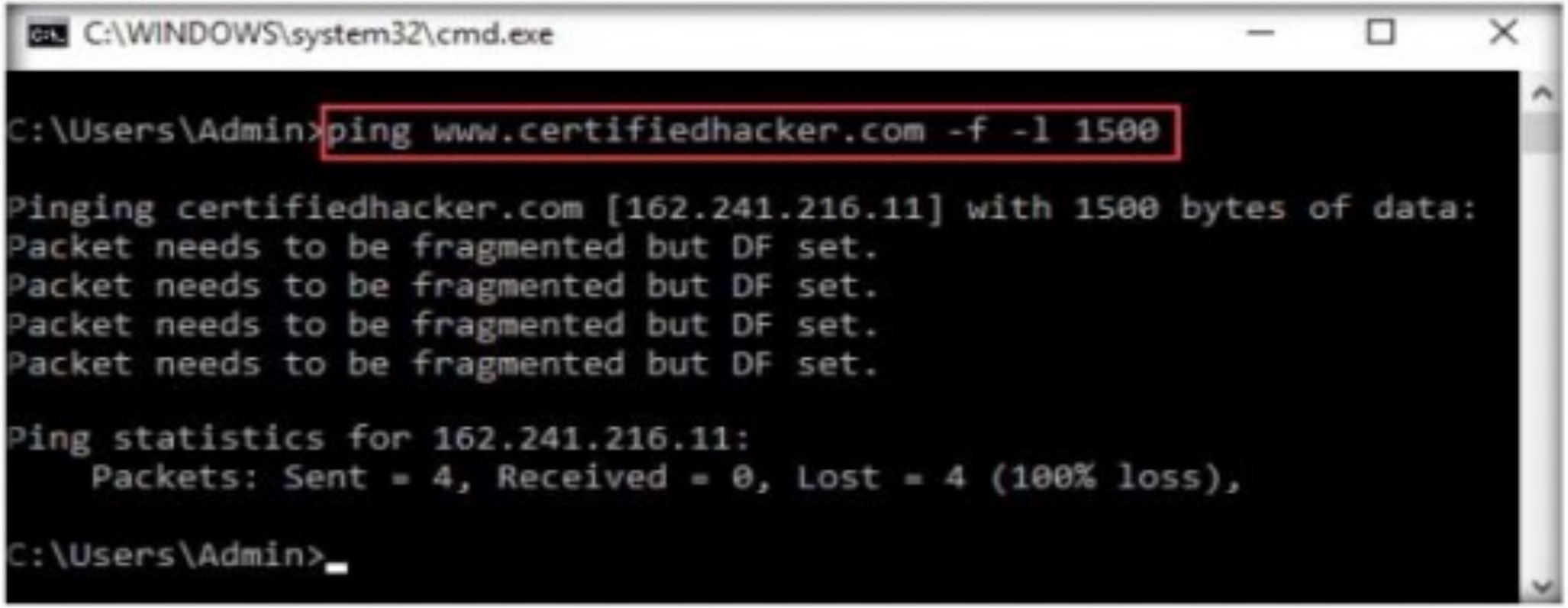
3 Website Footprinting

3.1 Gather Information About a Target Website using **Ping** Command Line Utility

1. Open the Command Prompt window. Type **ping www.certifiedhacker.com** and press **Enter** to find its IP address.

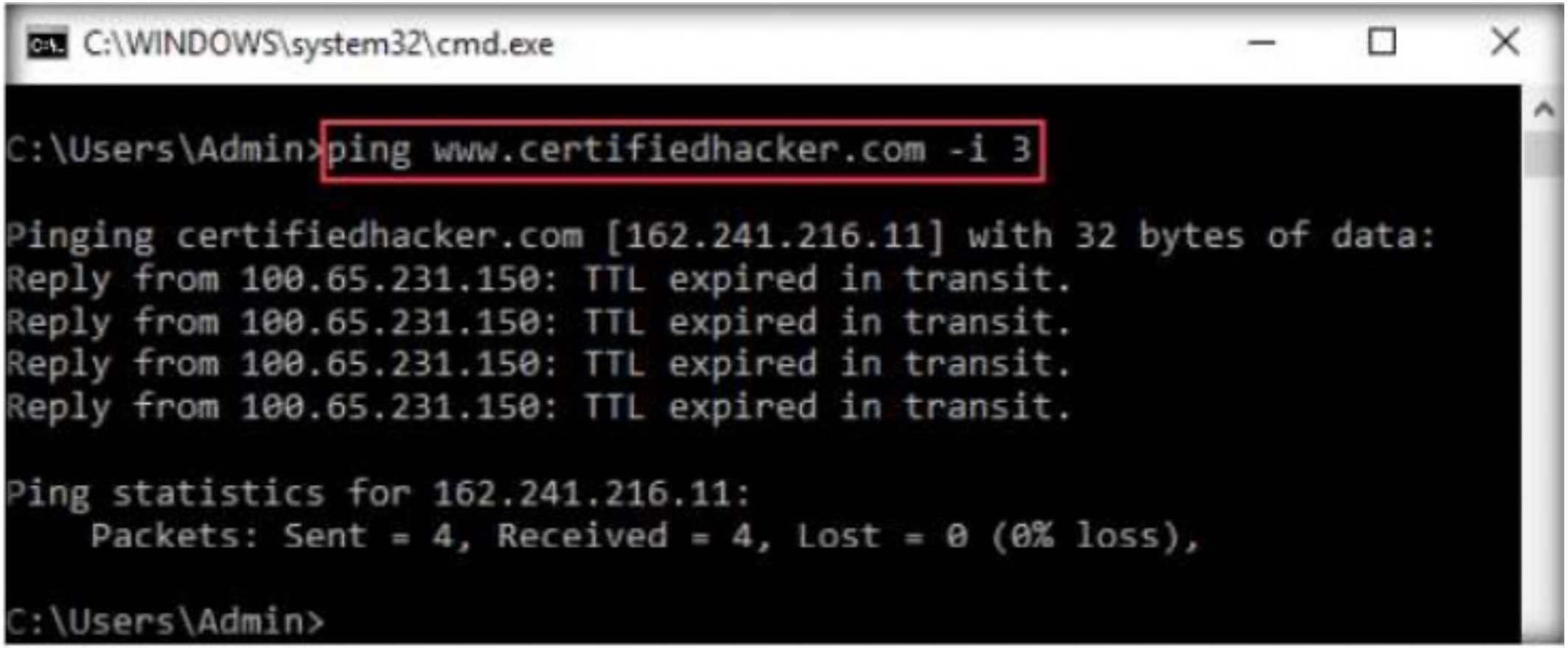
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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=341ms TTL=128
Reply from 162.241.216.11: bytes=32 time=327ms TTL=128
Reply from 162.241.216.11: bytes=32 time=337ms TTL=128
Reply from 162.241.216.11: bytes=32 time=321ms TTL=128

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 321ms, Maximum = 341ms, Average = 331ms

C:\Users\Admin>_
```

2. 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**.
3. In the Command Prompt window, type **ping www.certifiedhacker.com –f -l 1500** and press **Enter**.



4. The response, Packet needs to be **fragmented but DF set**

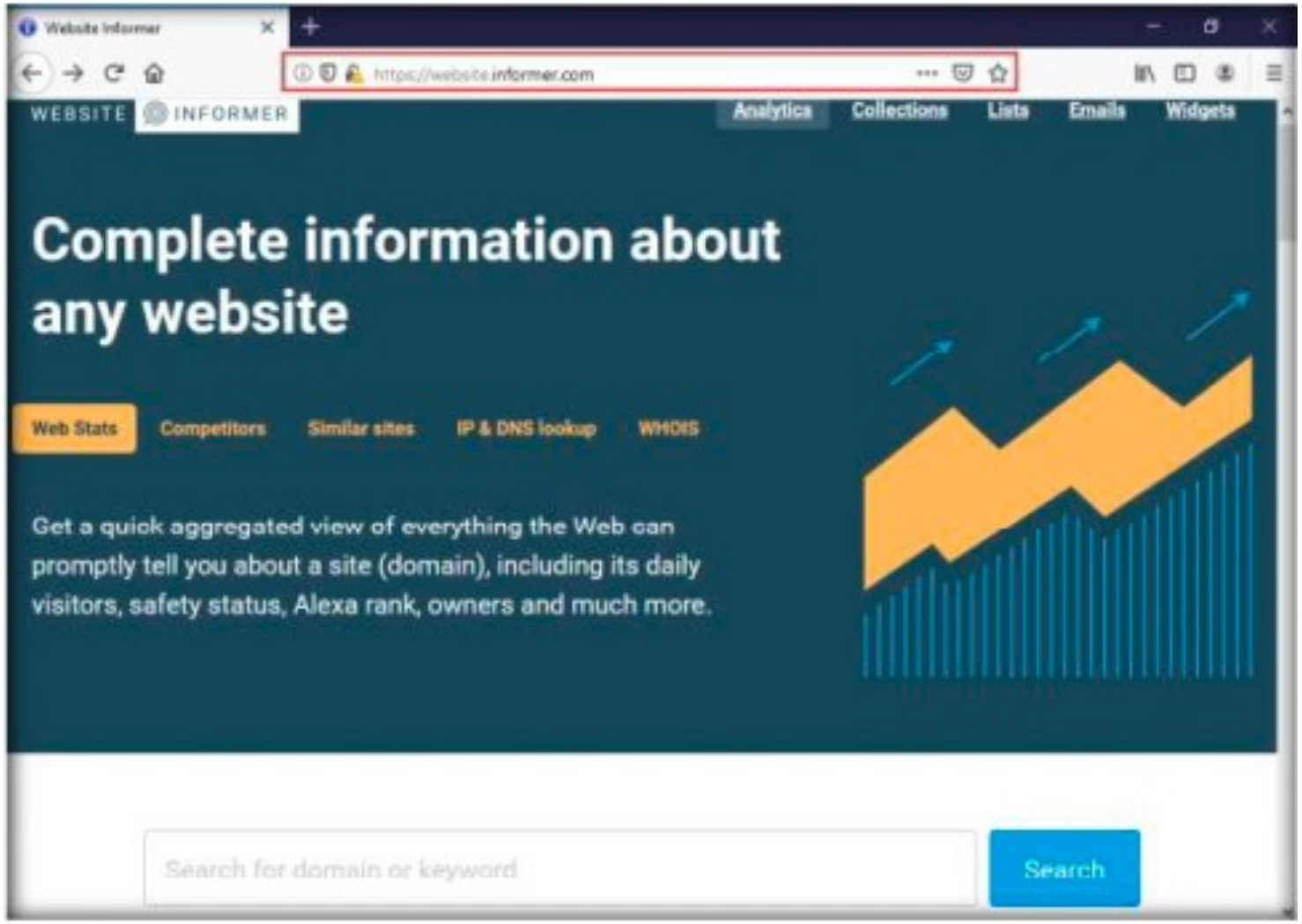
5. In Command Prompt, **type ping www.certifiedhacker.com -i 3** and press Enter.



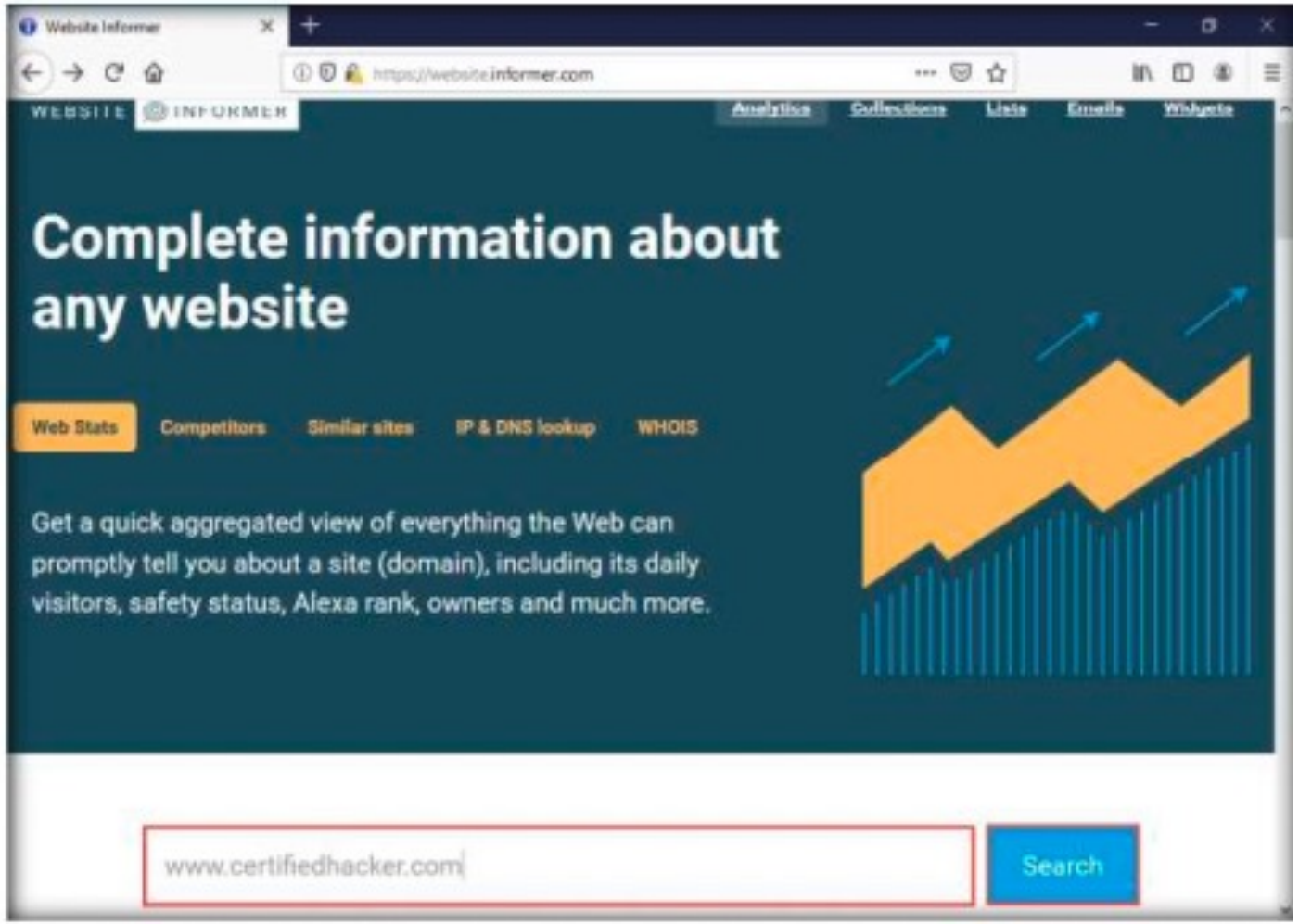
3 Website Footprinting

3.2 Gather Information About a Target Website using **Website Informer**

1. open a web browser (here, Mozilla Firefox), type **https://website.informer.com** in the address bar, and press **Enter** The Website Informer website appears.

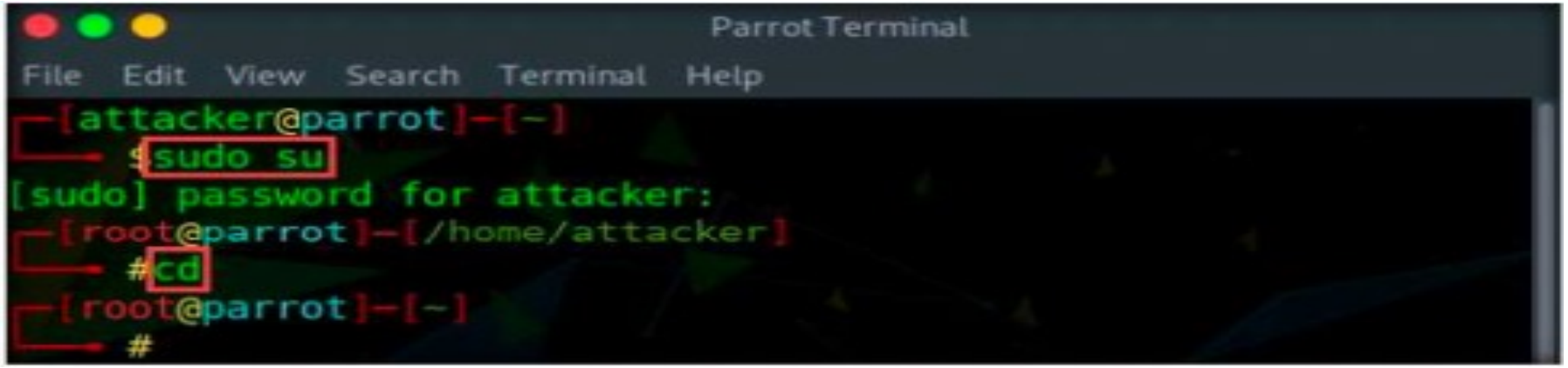


2. Type the target website's URI, (here**, www.certifiedhacker.com**) in the text field, and then click on the **Search** button. as shown in the screenshot below.



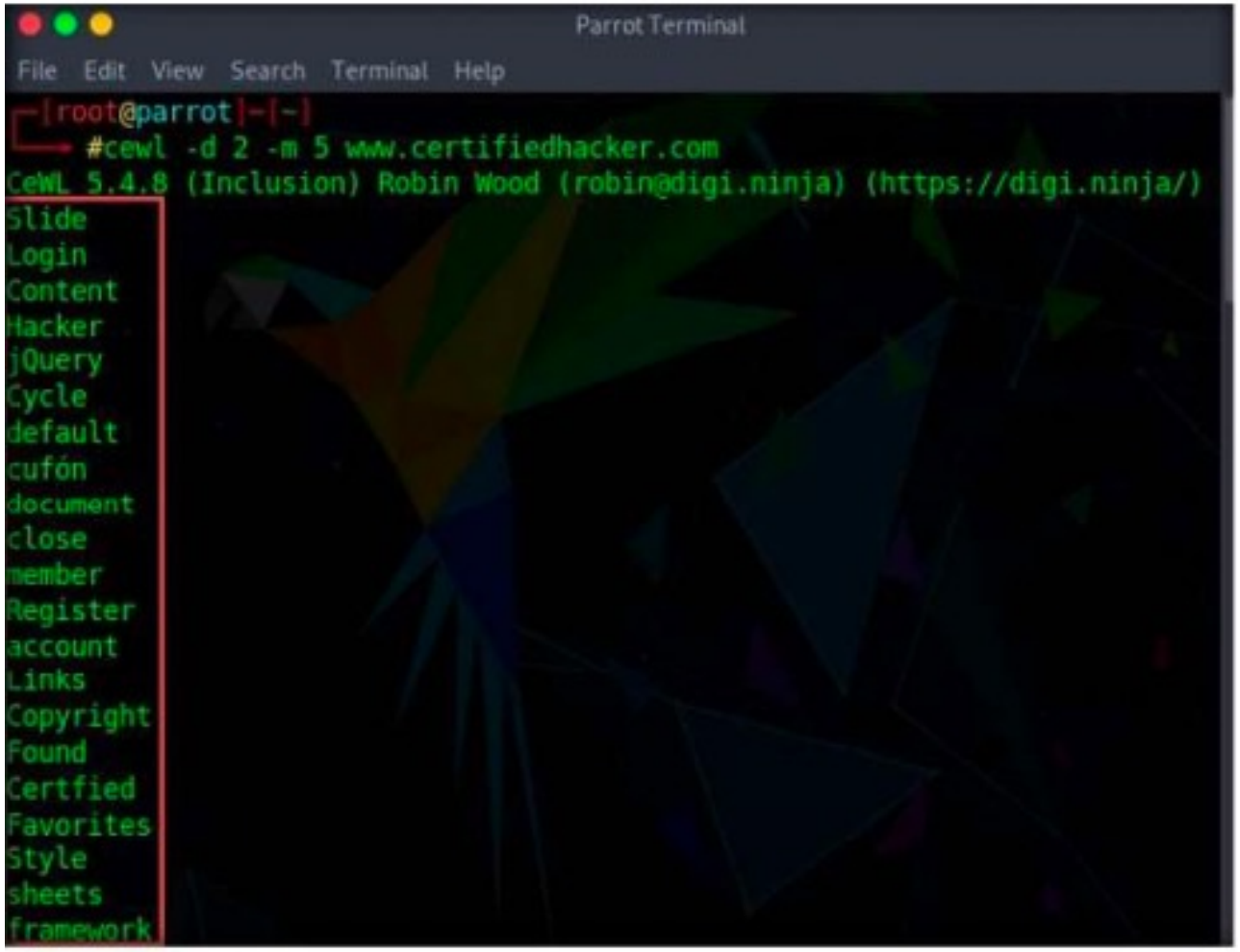
3 Website Footprinting 3.3 Gather a Wordlist from the Target Website using **CeWL**

1. Type **cd** and press **Enter** to jump to the **root** directory.

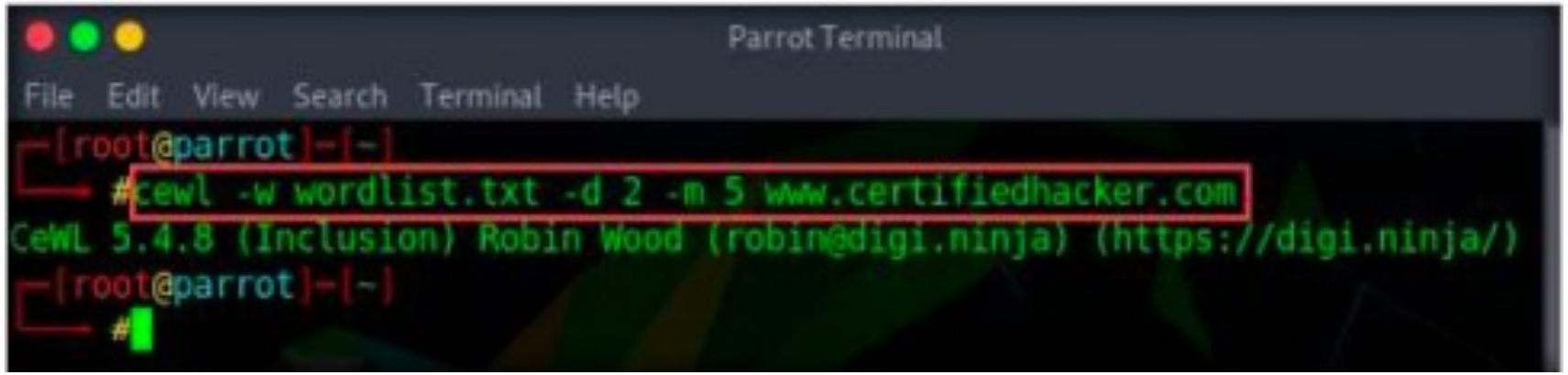


2. In the Terminal window, type **cewl –d 2 -m 5 www.certifiedhacker.com** and press **Enter**.

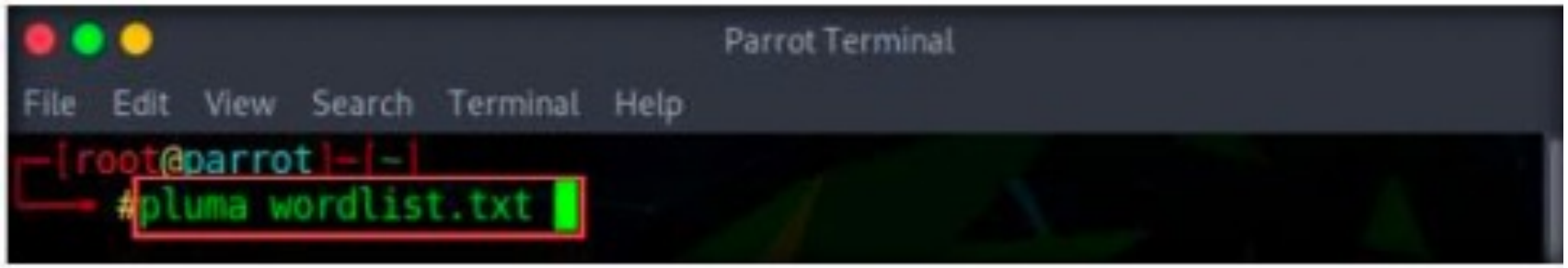
3. A unique wordlist from the target website is gathered. The minimum word length is 5, and the depth to spider the target website is 2.



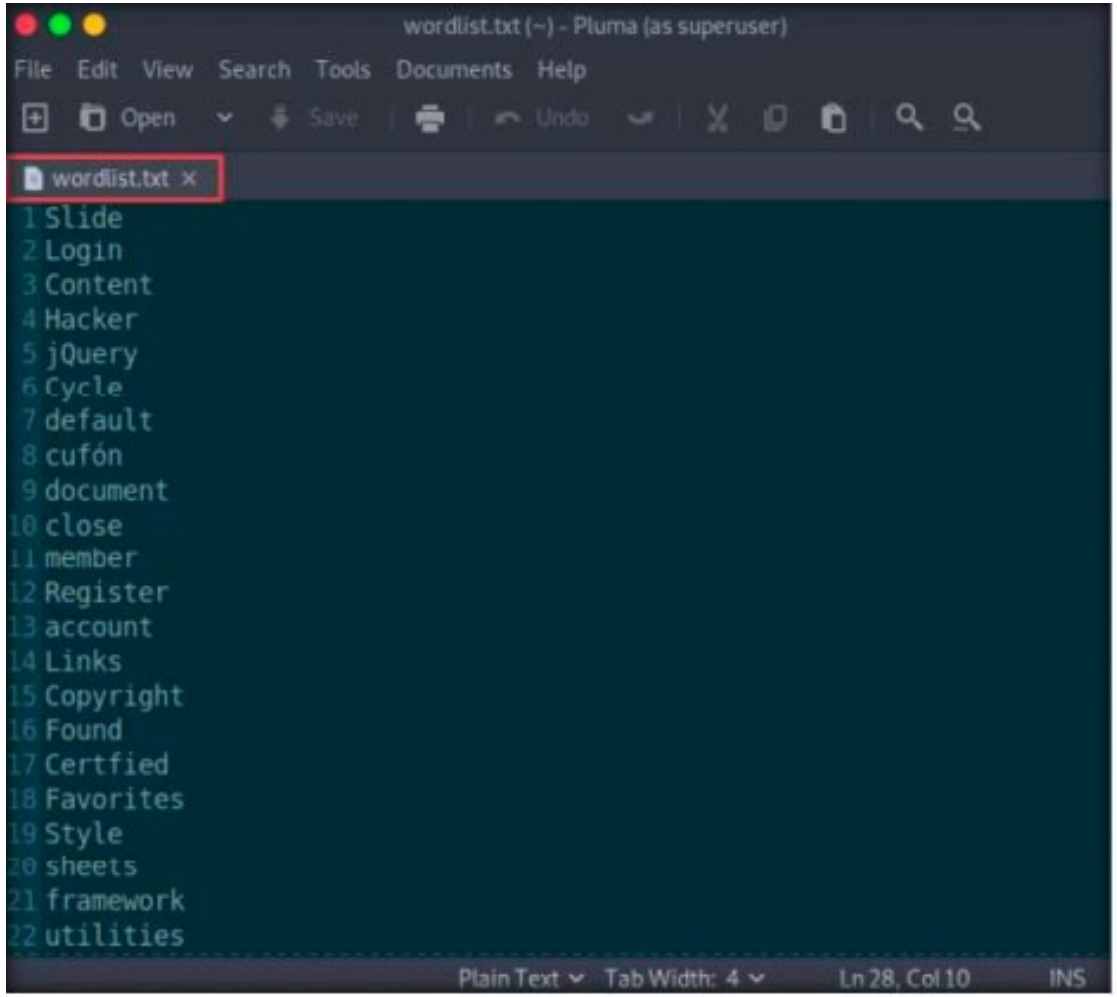
4. Alternatively, this unique wordlist can be written directly to a text file. To do so, type **cewl –w wordlist.txt -d 2 -m 5 www.certifiedhacker.com** and press **Enter**. **-w** . Write the output to the file (here, **wordlist.txt**)



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



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

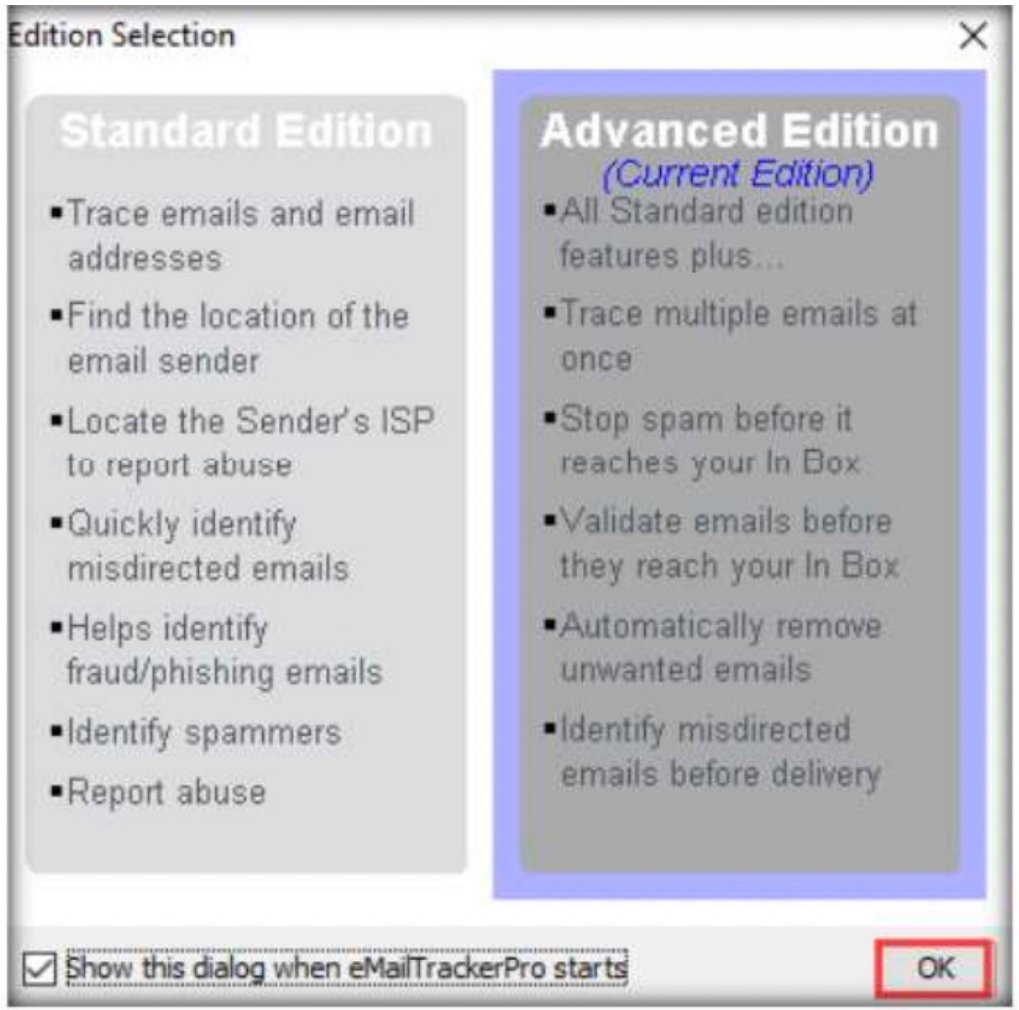


5

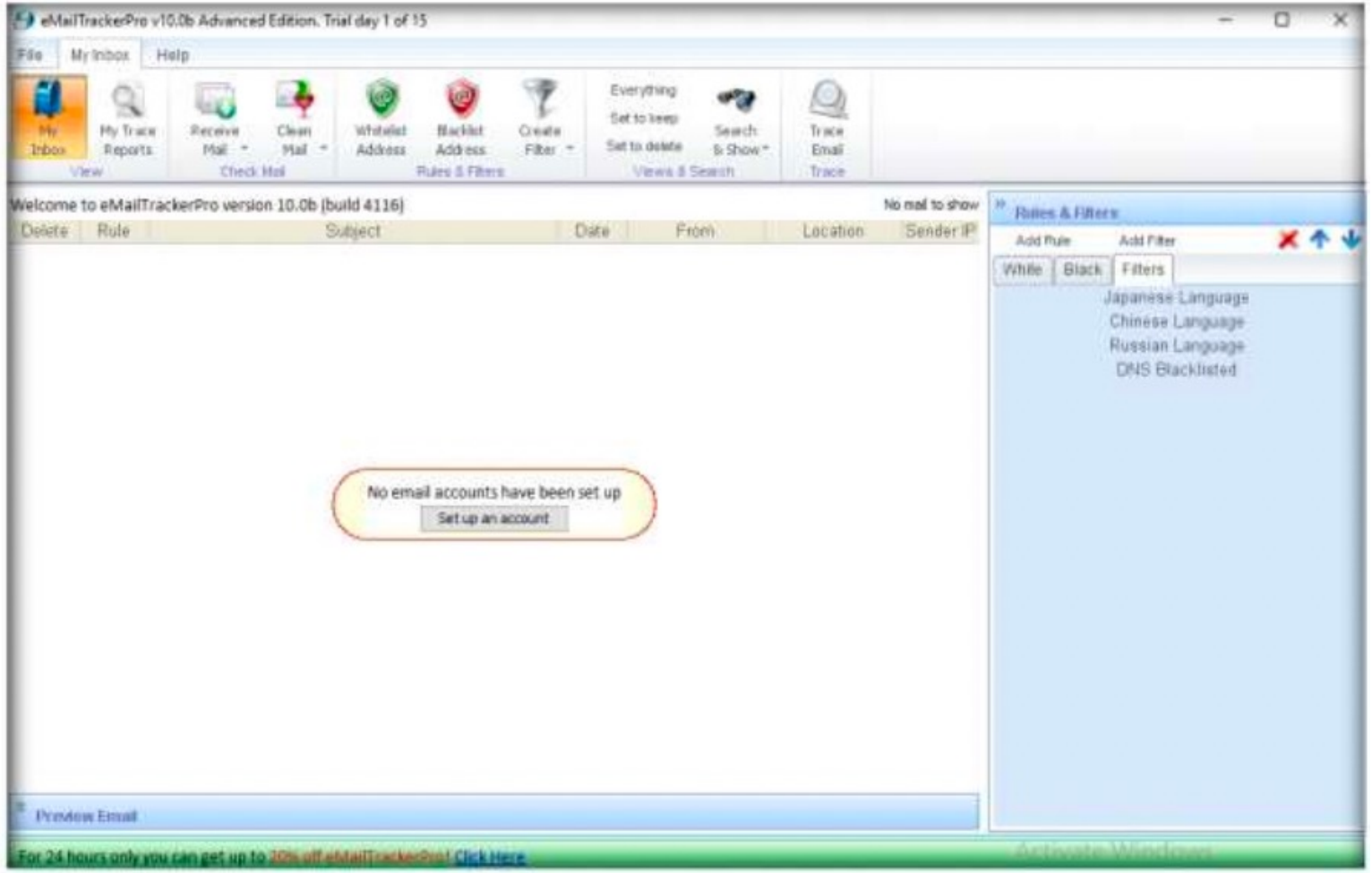
Email Footprinting

Gather Information about a Target by Tracing Emails using **eMailTrackerPro**

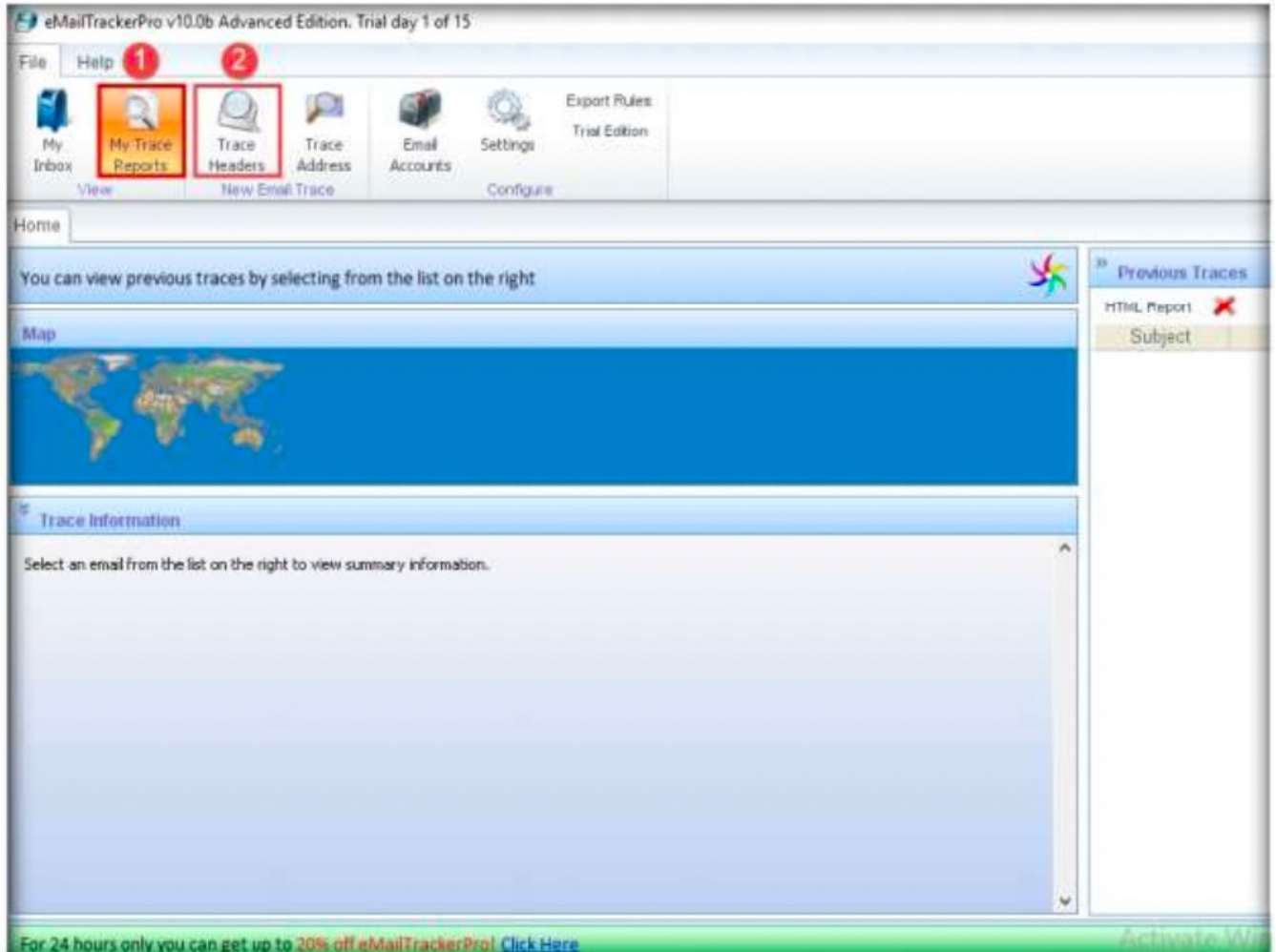
1. Install eMailTrackerPro, and After installation, **launch** the eMailTrackerPro.
2. The main window of **eMailTrackerPro** appears along with the **Edition** Selection pop-up; click **OK**.



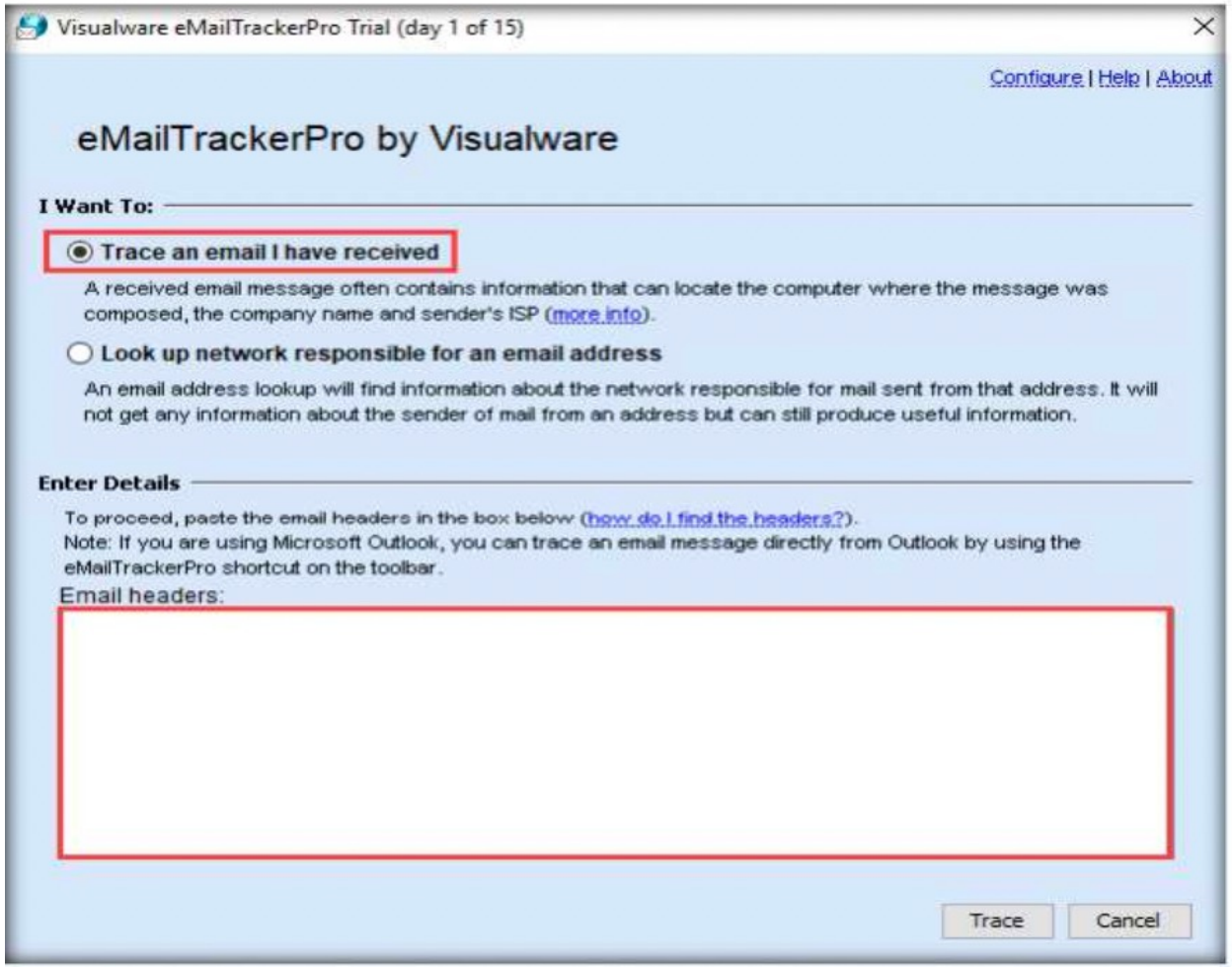
3. The **eMailTrackerPro** main window appears, as shown in the screenshot.



4. 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)
5. Click the **Trace Headers icon** from the **New Email Trace** section to start the trace.



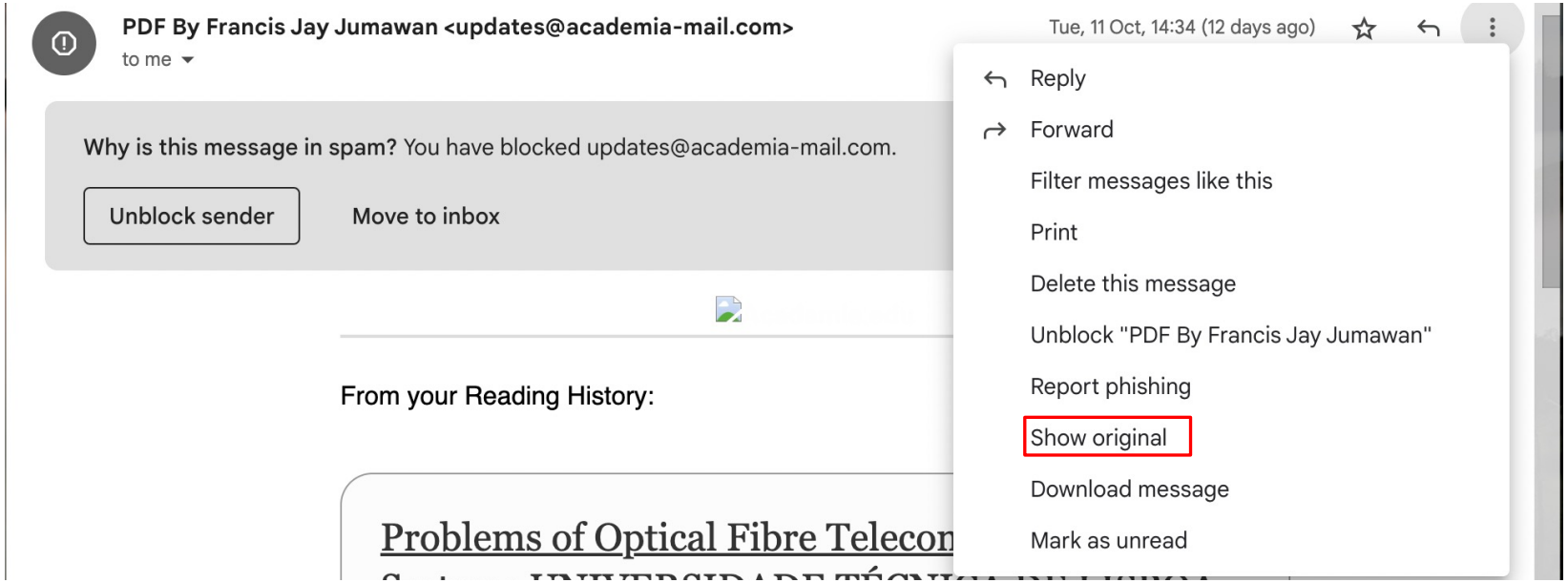
6. A pop-up window will appear; select **Trace an email I have received**. Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers**: field under **Enter Details section.**



7. 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.

<u>Note</u>: 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.



5

Email Footprinting

Gather Information about a Target by Tracing Emails using **eMailTrackerPro**

Original Message

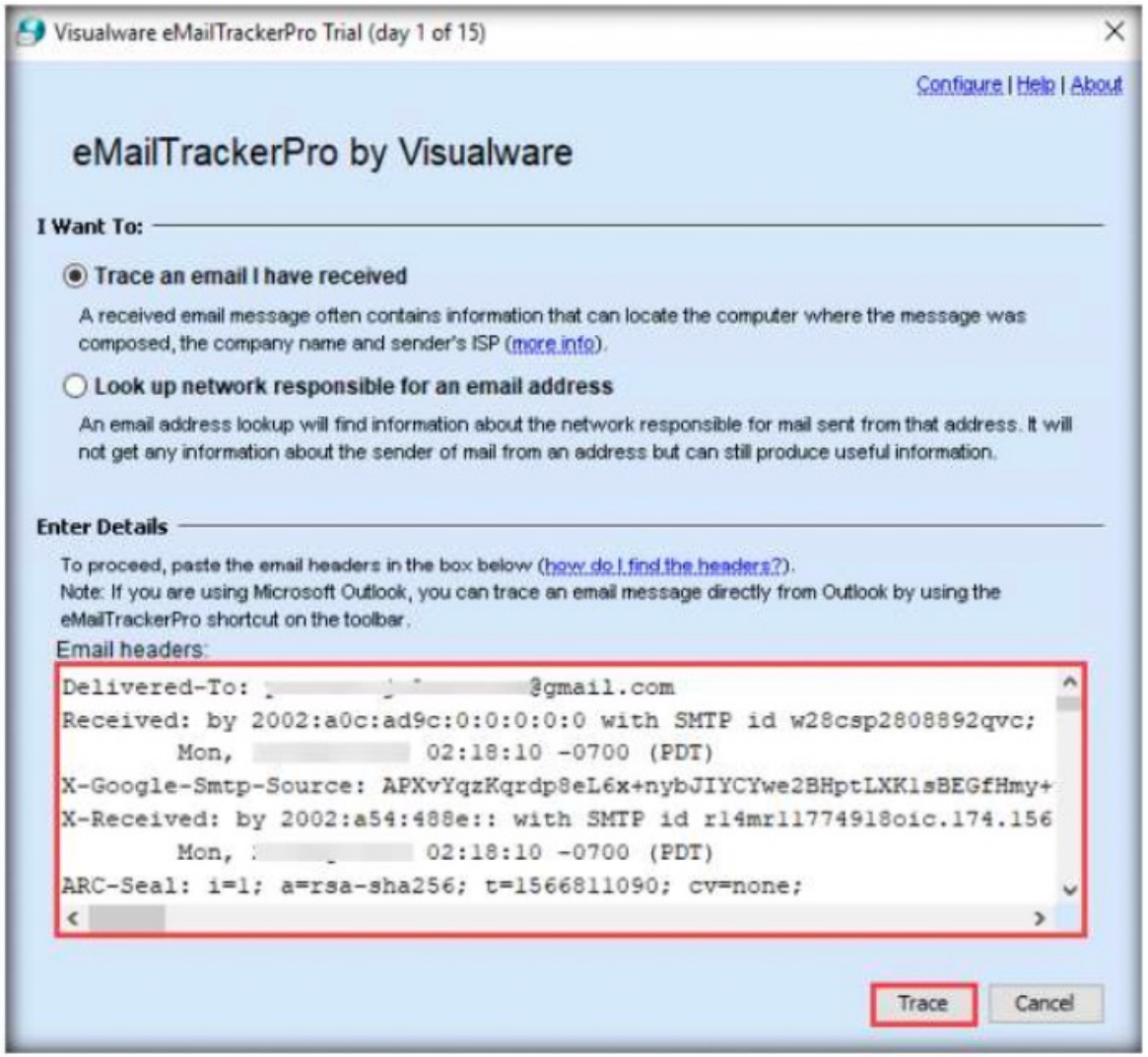
Message ID	<c6a3ec45832af8bb2ab7416077b2af85@localhost.localdomain>
Created at:	[illegible] at 2:48 PM (Delivered after 1 second)
From:	TSVBNKCRD <[illegible]@[illegible].info> Using PHPMailer [version 1.73]
To:	[illegible]@gmail.com
Subject:	THYBNKCRD CREDIT CARD (XX2917) WILL BE DELIVERED THIS WEEK
SPF:	NEUTRAL with IP 67.222.2.167 Learn more
DKIM:	'PASS' with domain alleges.info Learn more

Download Original

Copy to clipboard

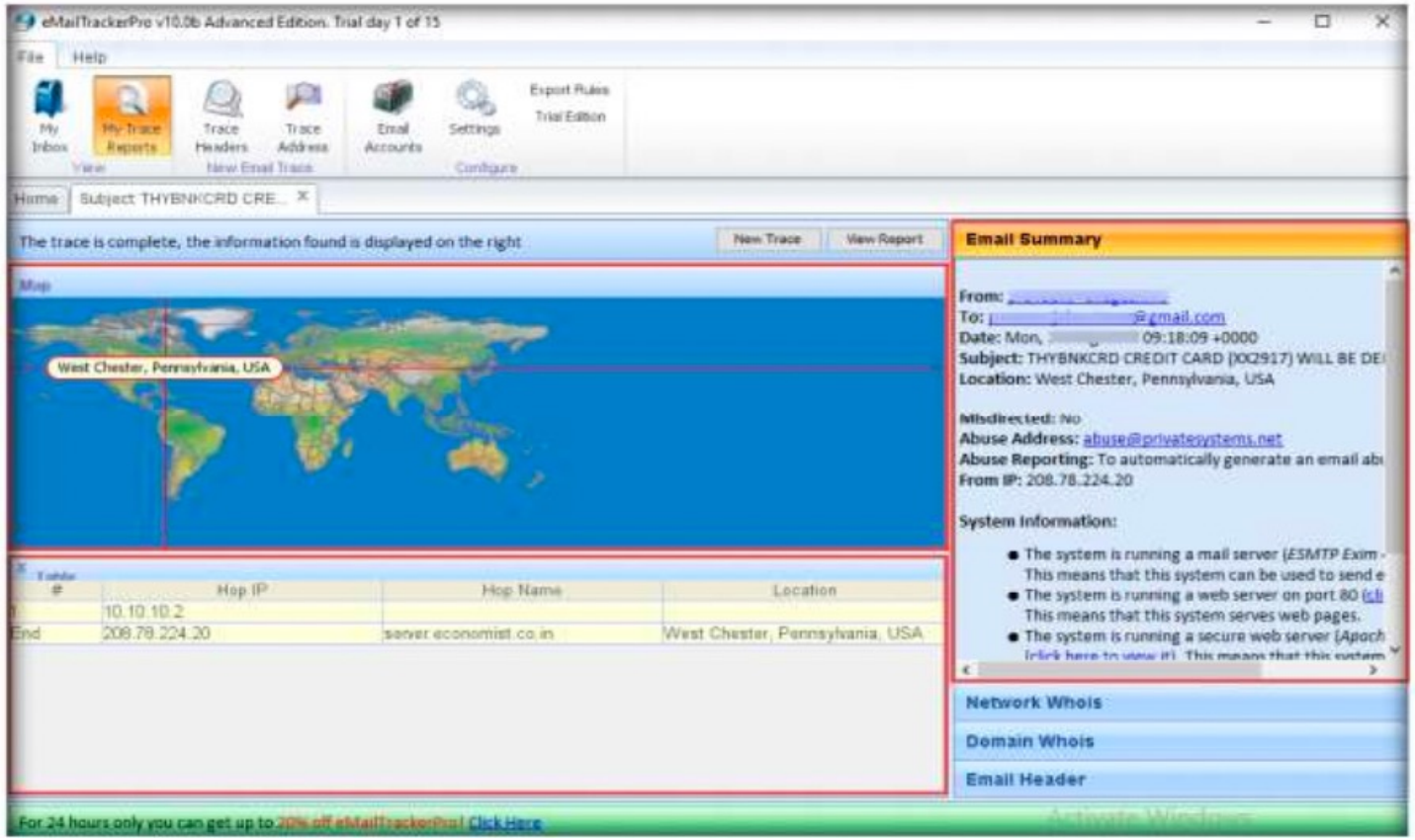
```
Delivered-To: [illegible]@gmail.com
Received: by 2002:a0c:ad9c:0:0:0:0:0 with SMTP id w28csp2808892qvc;
        Mon, [illegible] 02:18:10 -0700 (PDT)
X-Google-Smtp-Source: APXvYqzKqrdp8eL6x+nybJIYCYwe2BHptLXK1sBEGfHmy+vC1VG4ybuN6dsWCgZ+4ZmuNh3YTtPg
X-Received: by 2002:a54:488e:: with SMTP id r14mr11774918oic.174.1566811090471;
        Mon, [illegible] 02:18:10 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1566811090; cv=none;
        d=google.com; s=arc-20160816;
        b=D8El7aUKPGkvRo7nqaDxb301LqMdhh/+5X1gLhXaO7Q0bcOMoB48fcsT5n/87GSeqX
         BfVzgM/Su9o+plYnFaxXxsDBAIAz9Me7DVaS7dYtDxUeX9xQb8rIUg7SxVI5CLBUMQ61
         X5IcH3i3Bb7T14GQ0doR81DH6nCOwVG2WTEHTR1OEvM1KpUZ4FEXDfeRKk6X2QvcpgL3
         rrpYvLag2JCazyPqMY0B8x65XphkH1gv+vdf/LlUsFsHybCYpNsUtE+B9qhwLtXPYOfW
```

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



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

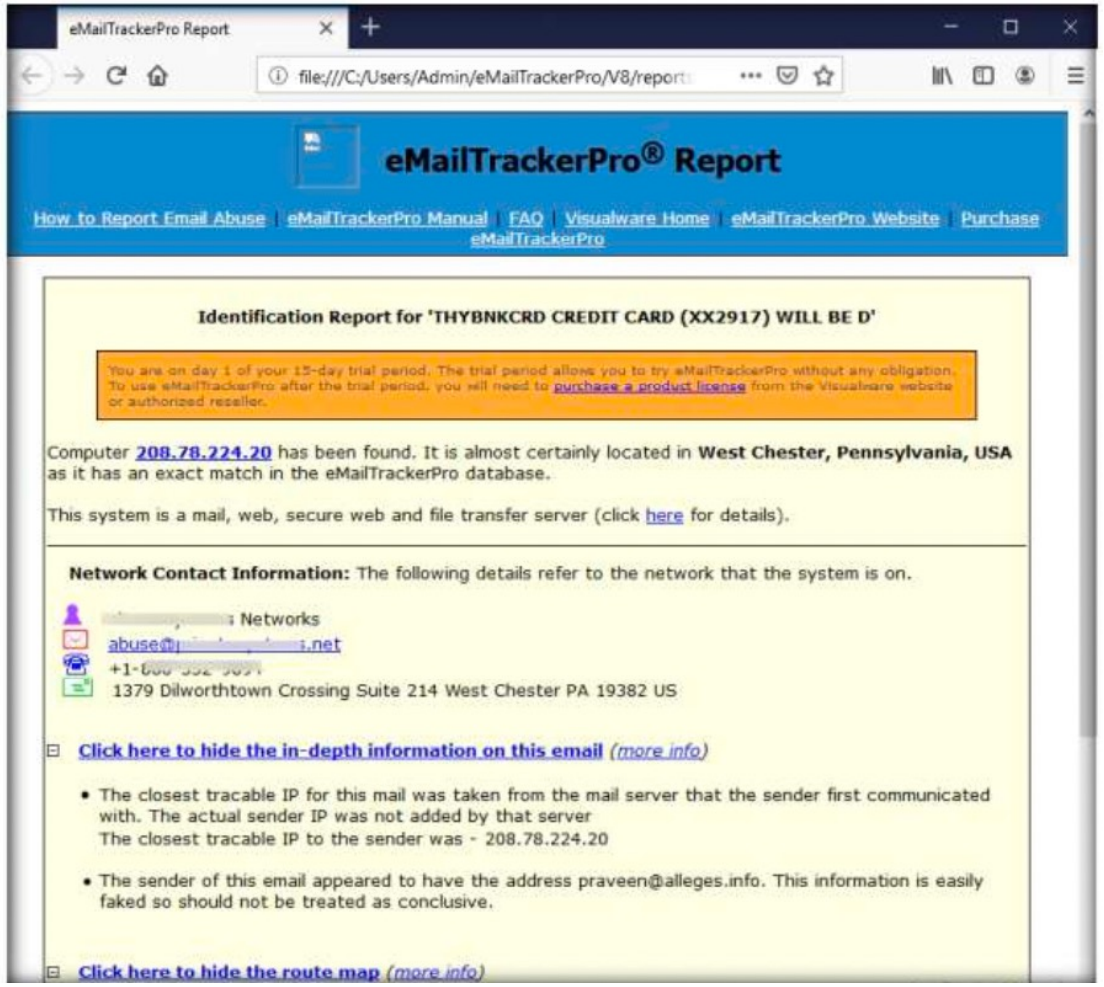
Note: The location and IP addresses may vary according to your email header.



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

10. The complete report appears in the default browser.

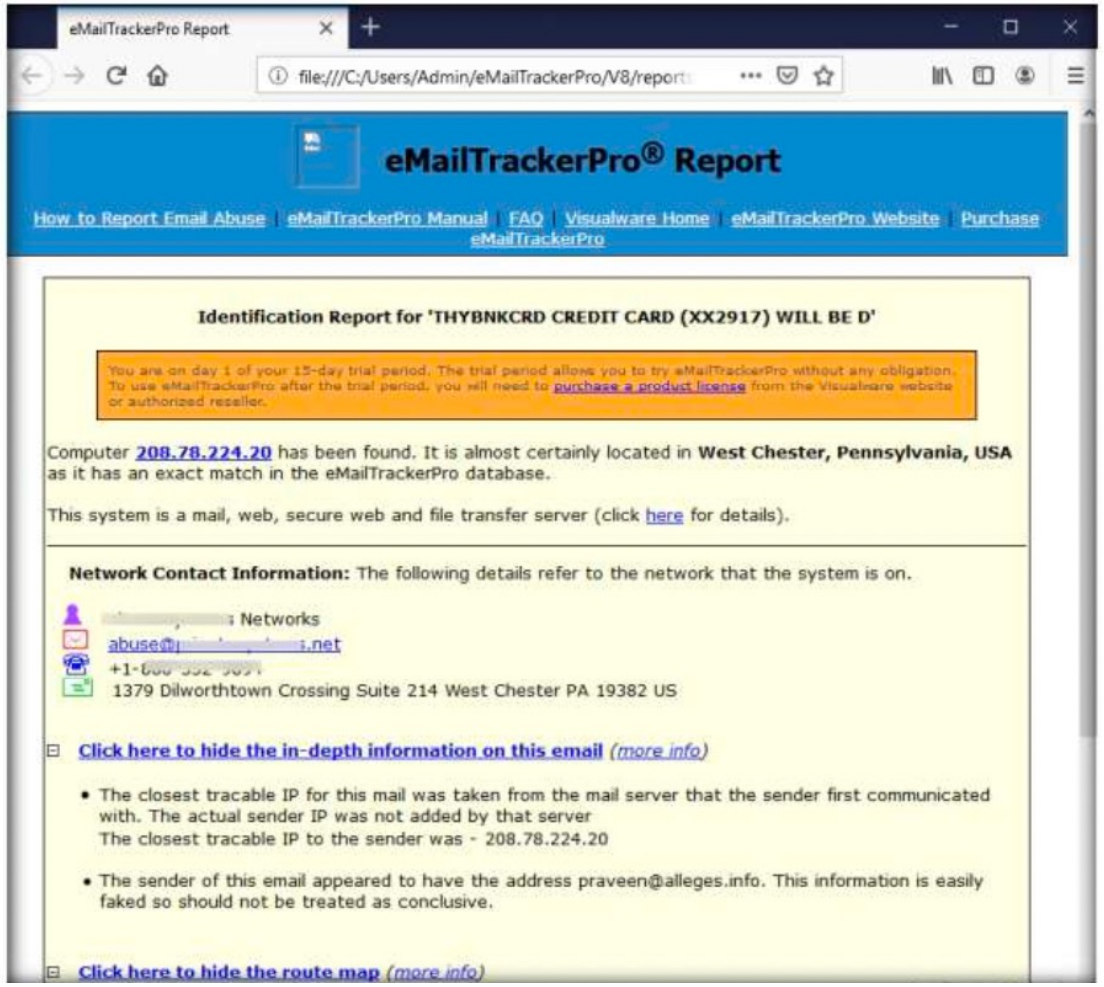
11. Expand each section to view detailed information.



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

10. The complete report appears in the default browser.

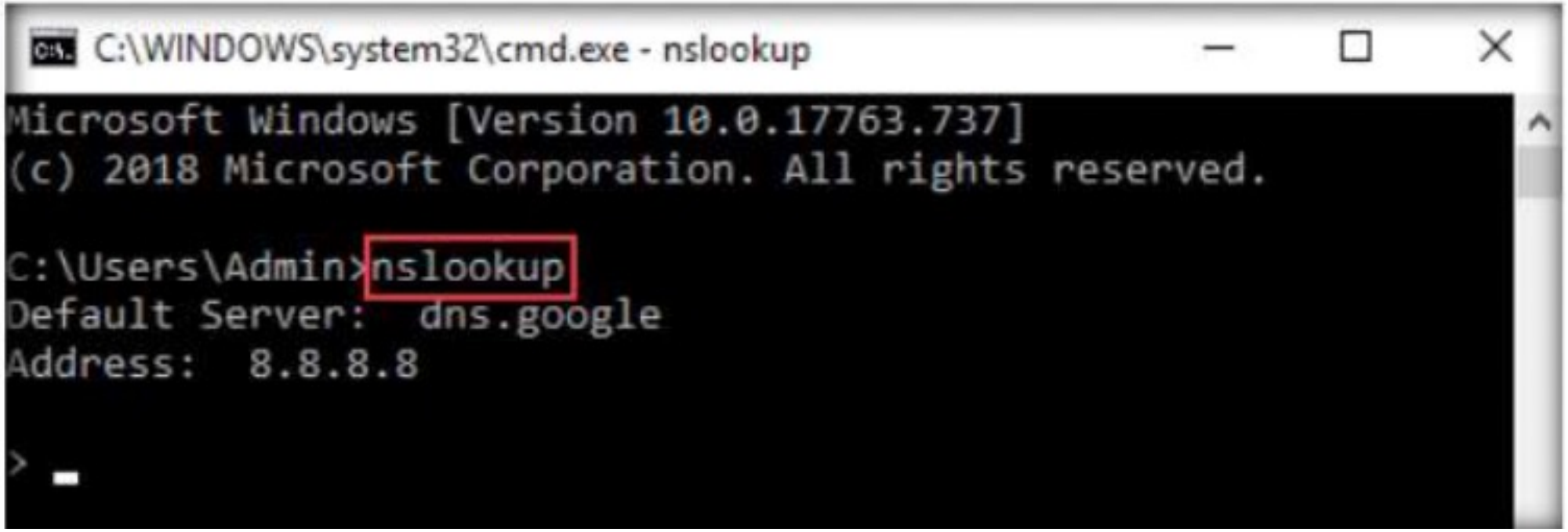
11. Expand each section to view detailed information.



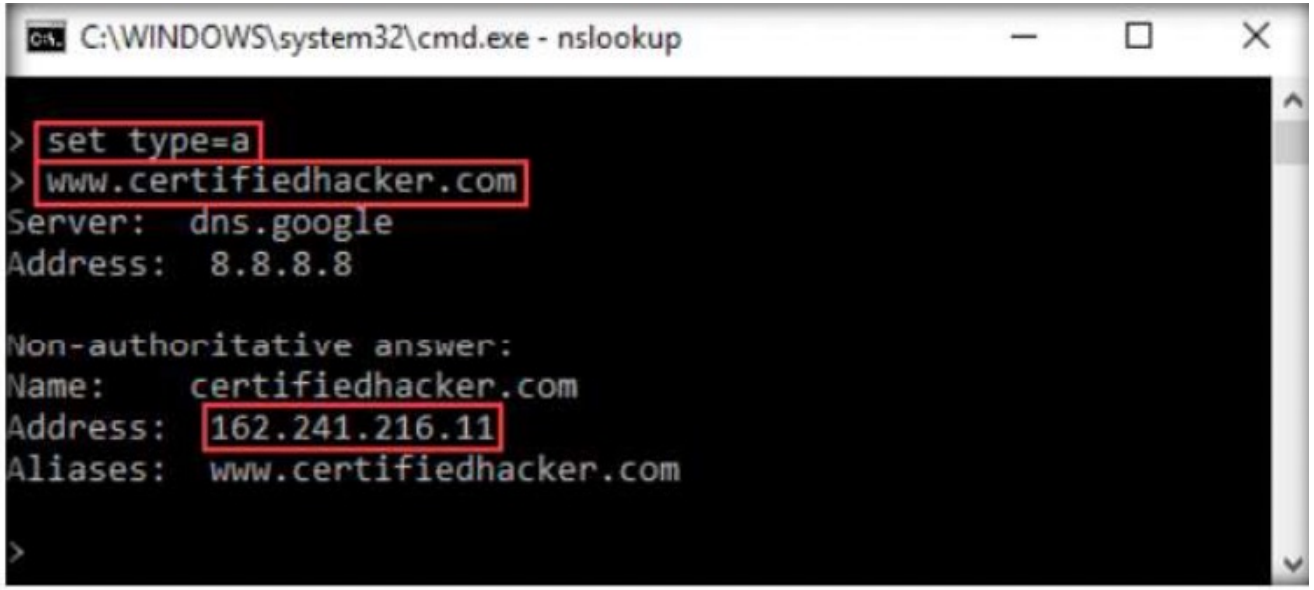
6 DNS Footprinting

6.1 Gather DNS Information using **nslookup** Command Line Utility and **Online** Tool

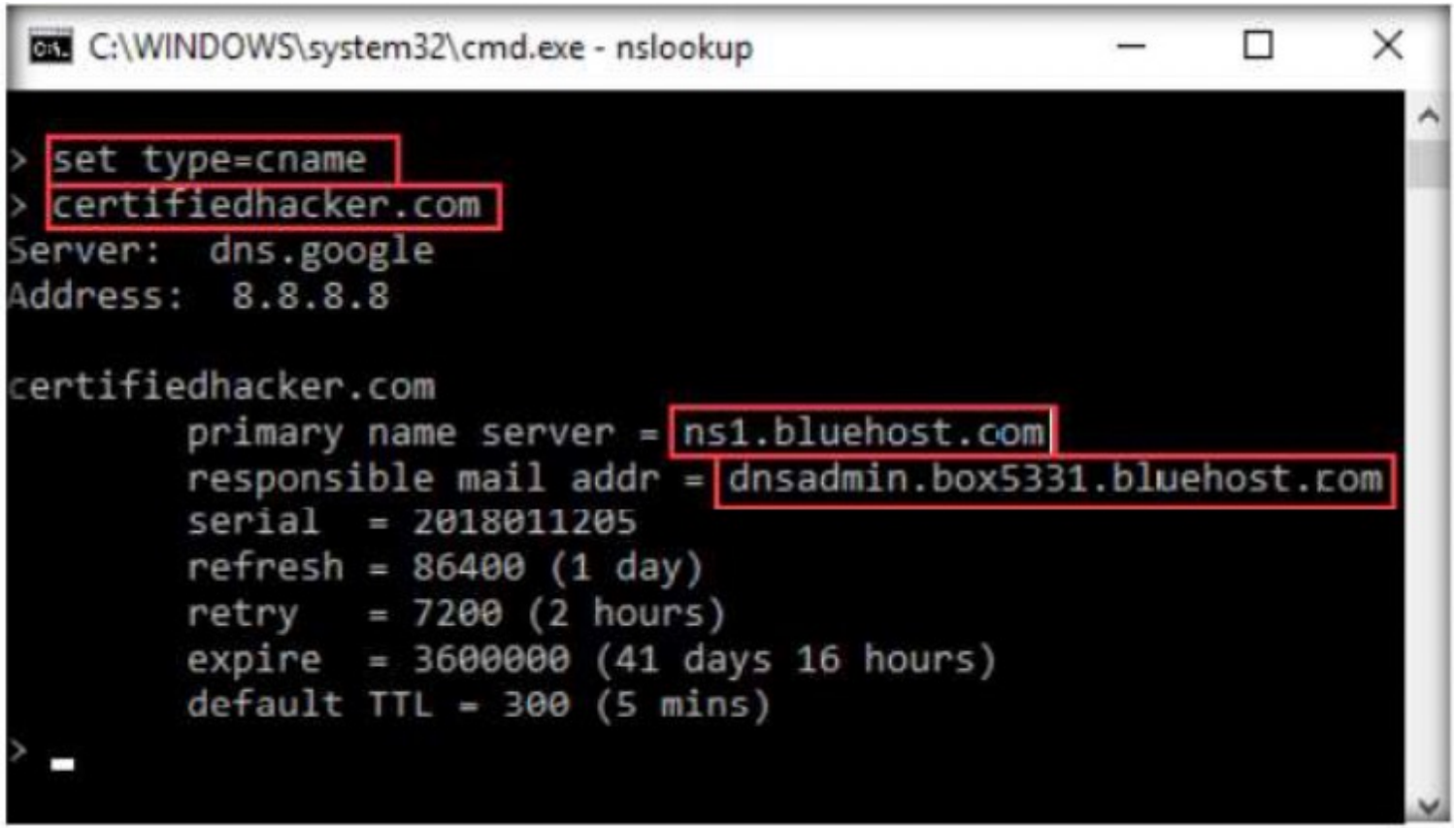
1. Launch a command prompt, type **nslookup**, and press **Enter**. This displays the **default** server and its address assigned to the **Windows 10**



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.



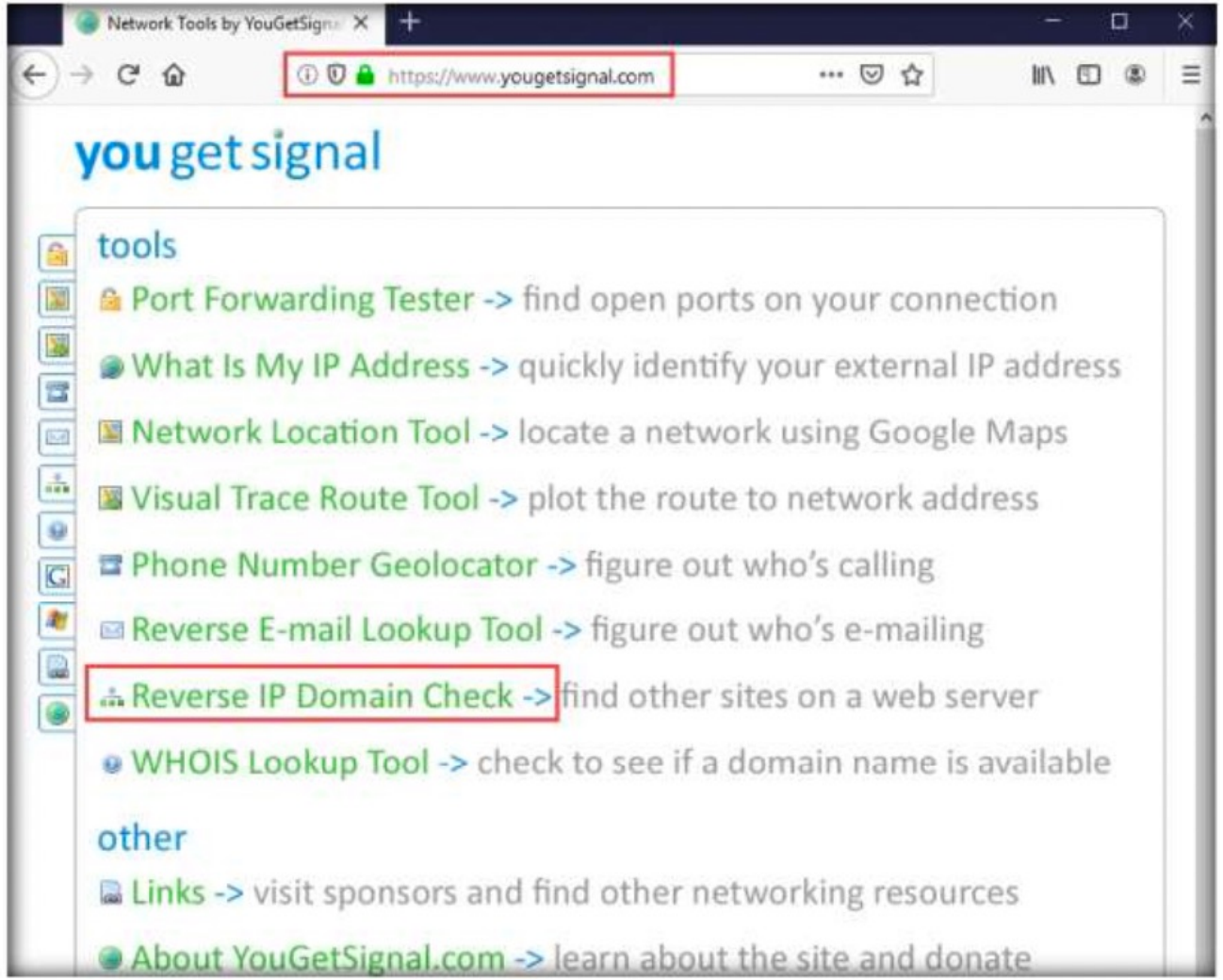
4. To obtain the domain's **authoritative** name server. Type **set type=came** and press **Enter**.
5. Type **certifiedhacker.com** and press **Enter**.



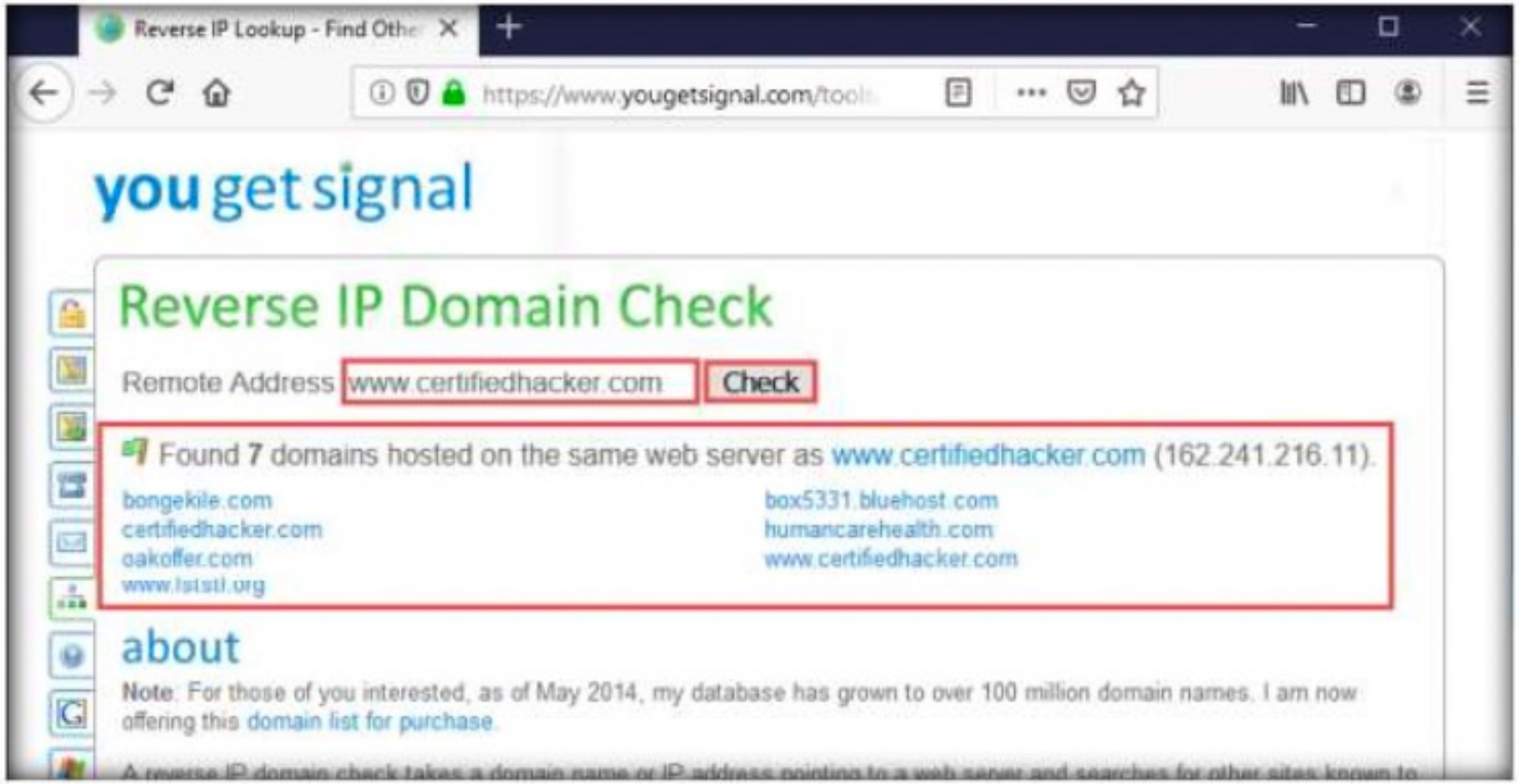
6 DNS Footprinting

6.2 Perform Reverse DNS Lookup using **Reverse IP Domain Check**

1. Open any web browser (here, Mozilla Firefox and navigate to **https:/www.yougetsignal.com**. On the website, click **Reverse IP Domain Check**



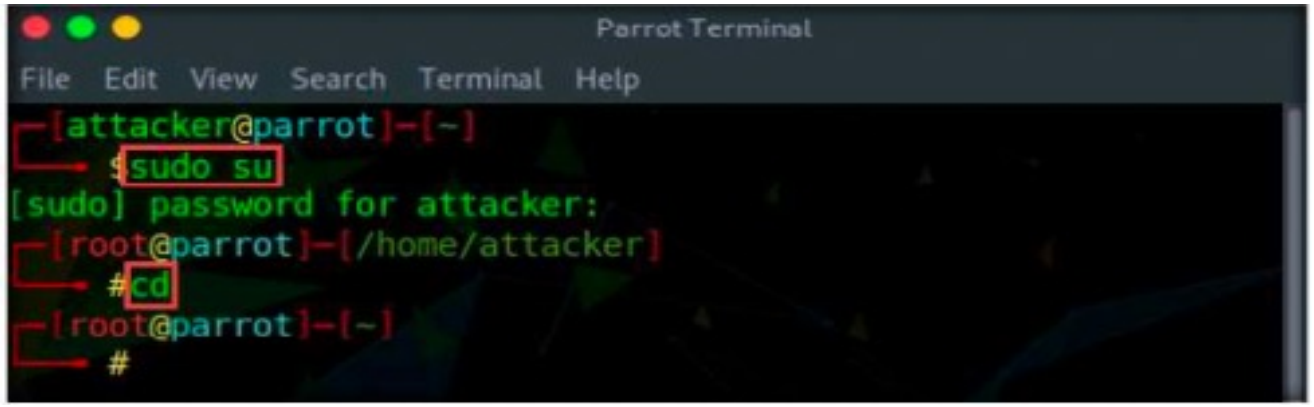
2. On **the Reverse IP Domain Check** page, enter **www.certifiedhacker**.com in **the Remote Address** field and click **Check** to find other domains/ sites hosted on a **certifiedhacker.com** web server. You will get the list of domans/sites hosted on the same server as **wwwcertifiedhacker.com.**



6 DNS Footprinting

6.3 Perform Reverse DNS Lookup using **DNSRecon**

1. Type **cd** and press **Enter** to jump to the **root** directory.



2. Type **dnsrocon -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.

6

DNS Footprinting

6.3

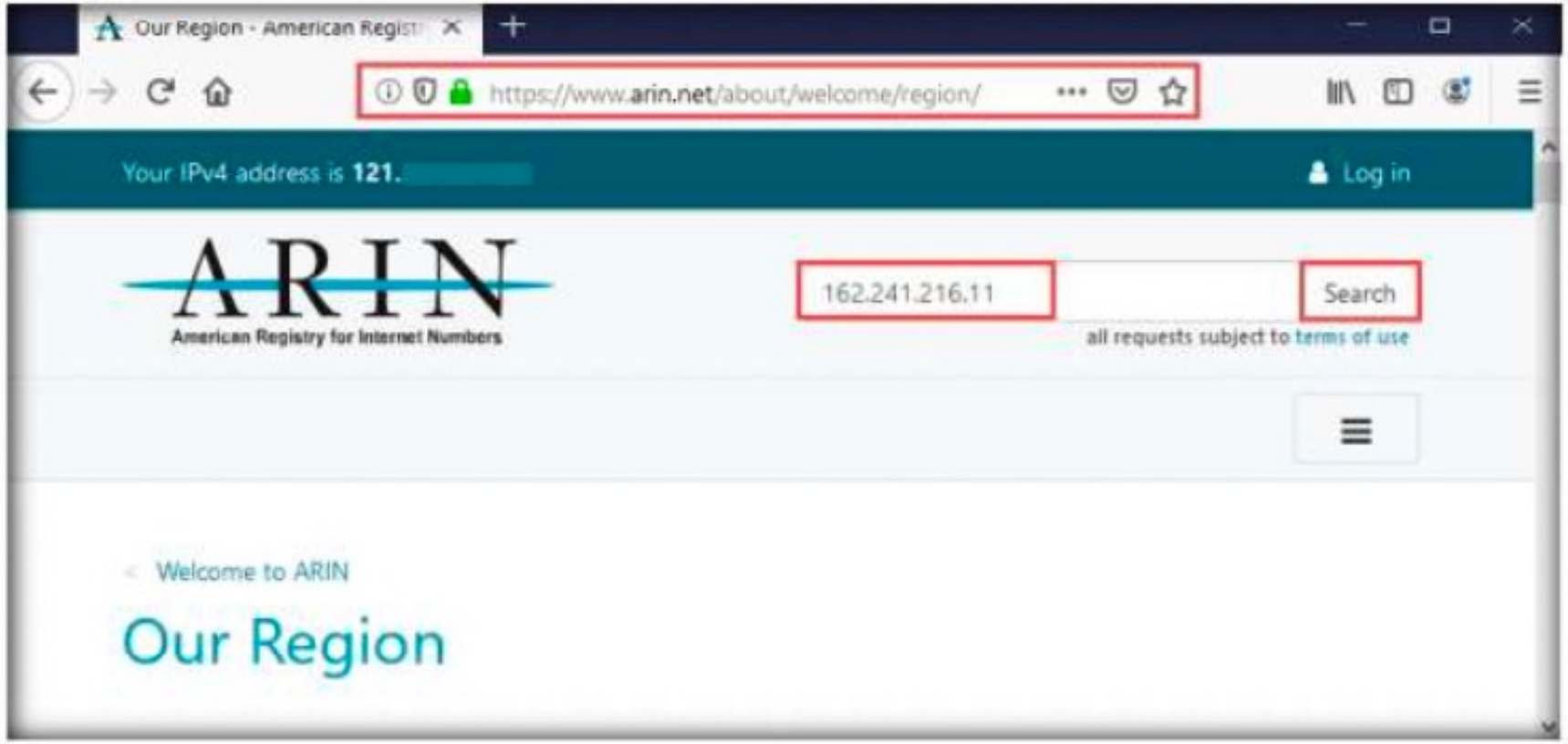
Perform Reverse DNS Lookup using **DNSRecon**

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[~]
└──╼ #dnsrecon -r 162.241.216.0-162.241.216.255
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[+] {'type': 'PTR', 'name': '162-241-216-3.unifiedlayer.com', 'address': '162.241.216.3'}
[+] {'type': 'PTR', 'name': '162-241-216-0.unifiedlayer.com', 'address': '162.241.216.0'}
[+] {'type': 'PTR', 'name': '162-241-216-2.unifiedlayer.com', 'address': '162.241.216.2'}
[+] {'type': 'PTR', 'name': '162-241-216-4.unifiedlayer.com', 'address': '162.241.216.4'}
[+] {'type': 'PTR', 'name': '162-241-216-1.unifiedlayer.com', 'address': '162.241.216.1'}
[+] {'type': 'PTR', 'name': '162-241-216-6.unifiedlayer.com', 'address': '162.241.216.6'}
[+] {'type': 'PTR', 'name': '162-241-216-9.unifiedlayer.com', 'address': '162.241.216.9'}
[+] {'type': 'PTR', 'name': '162-241-216-5.unifiedlayer.com', 'address': '162.241.216.5'}
[+] {'type': 'PTR', 'name': '162-241-216-7.unifiedlayer.com', 'address': '162.241.216.7'}
[+] {'type': 'PTR', 'name': '162-241-216-8.unifiedlayer.com', 'address': '162.241.216.8'}
[+] {'type': 'PTR', 'name': 'box5334.bluehost.com', 'address': '162.241.216.14'}
[+] {'type': 'PTR', 'name': '162-241-216-10.unifiedlayer.com', 'address': '162.241.216.10'}
[+] {'type': 'PTR', 'name': 'box5331.bluehost.com', 'address': '162.241.216.11'}
[+] {'type': 'PTR', 'name': '162-241-216-13.unifiedlayer.com', 'address': '162.241.216.13'}
[+] {'type': 'PTR', 'name': '162-241-216-12.unifiedlayer.com', 'address': '162.241.216.12'}
[+] {'type': 'PTR', 'name': '162-241-216-15.unifiedlayer.com', 'address': '162.241.216.15'}
[+] {'type': 'PTR', 'name': 'box5350.bluehost.com', 'address': '162.241.216.20'}
[+] {'type': 'PTR', 'name': 'box5348.bluehost.com', 'address': '162.241.216.17'}
[+] {'type': 'PTR', 'name': '162-241-216-19.unifiedlayer.com', 'address': '162.241.216.19'}
[+] {'type': 'PTR', 'name': '162-241-216-16.unifiedlayer.com', 'address': '162.241.216.16'}
[+] {'type': 'PTR', 'name': '162-241-216-18.unifiedlayer.com', 'address': '162.241.216.18'}
[+] {'type': 'PTR', 'name': box5353.bluehost.com', 'address': '162.241.216.23'}
[+] {'type': 'PTR', 'name': '162-241-216-21.unifiedlayer.com', 'address': '162.241.216.21'}
[+] {'type': 'PTR', 'name': '162-241-216-22.unifiedlayer.com', 'address': '162.241.216.22'}
[+] {'type': 'PTR', 'name': '162-241-216-24.unifiedlayer.com', 'address': '162.241.216.24'}
[+] {'type': 'PTR', 'name': box5354.bluehost.com', 'address': '162.241.216.26'}
```

7 Network Footprinting

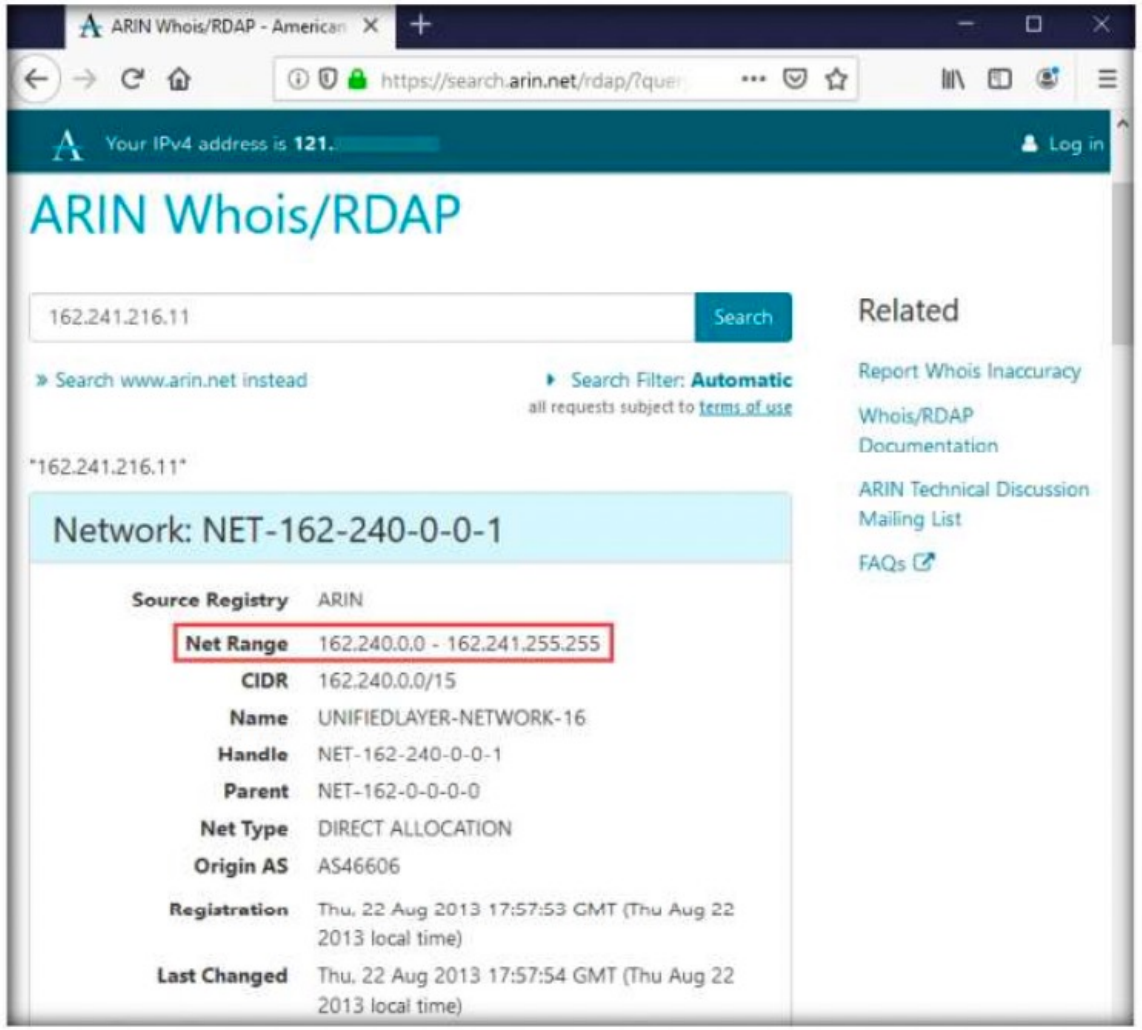
7.1 Locate the Network Range

1. Open any web browser (here, Mozilla Firefox) and navigate to **https://www.arin.net/about/welcome/region**.
2. In the search bar, enter the IP address of the target organization (here, the target organization is **certifiedhacker.com**, whose IP is **162.241.216.11**), and then click the **Search** button.

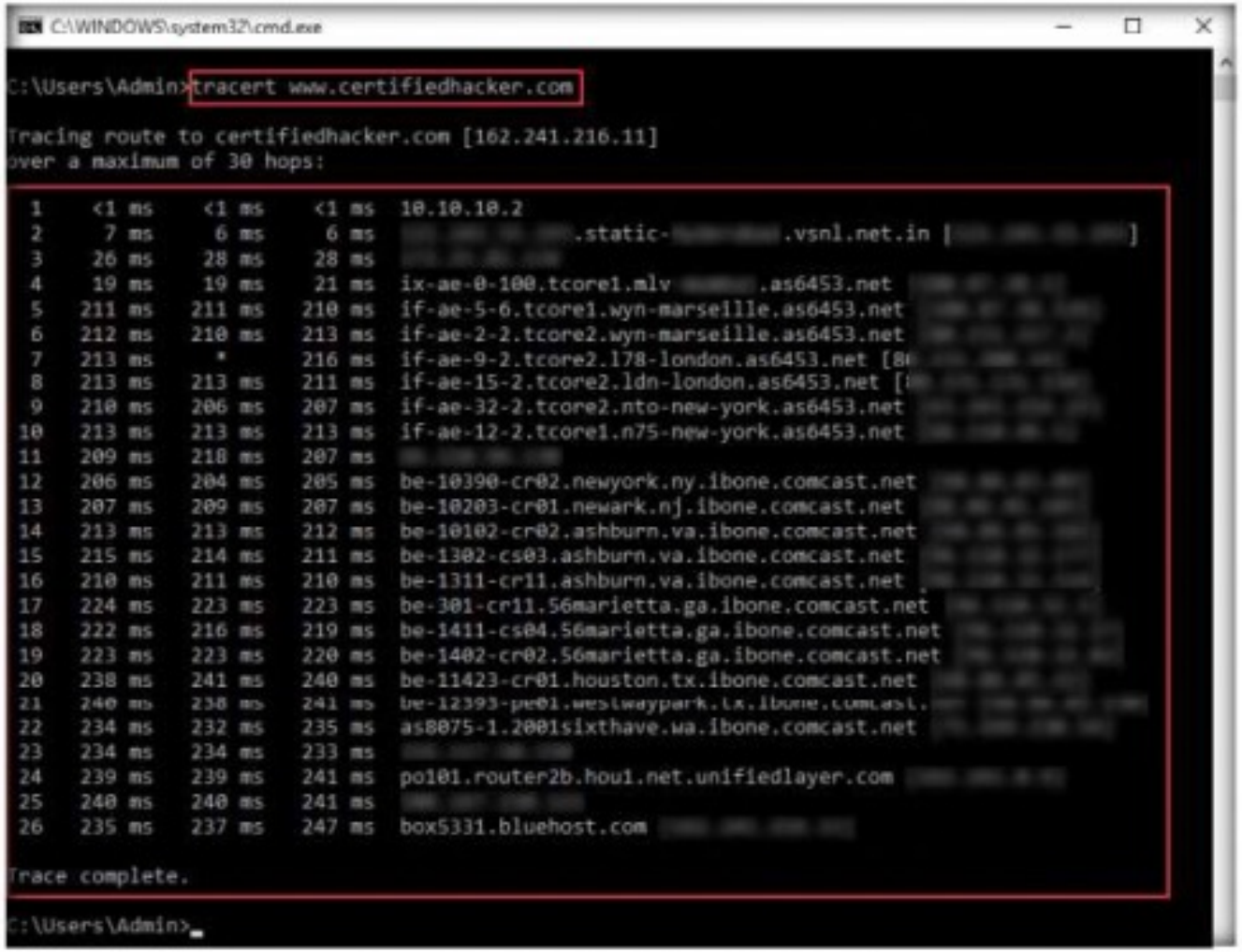


3. You will get the information about the network range along with the other information such as network type, registration information, etc.

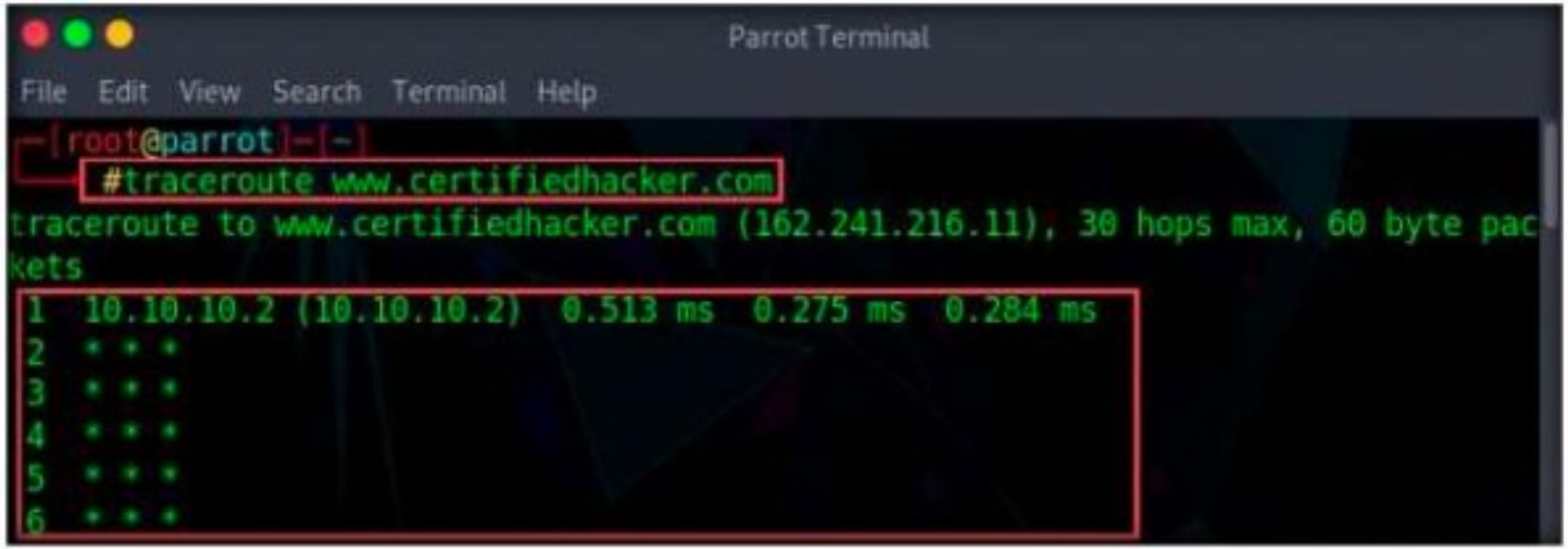
Network range information assists in creating a **map** of the target network. you can gather information about how the network is **structured**. Further, it also helps to **identify** the network **topology** and **access** the **control device** and **operating system** used in the target network.



1.Open the **Command Prompt** window. Tvpe **tracert www.certifiedhacker.com** and press **Enter** to view the **hops** that the packets made **before reaching** the destination.



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



Home work

Implement an Email Footprinting

Home work

Perform Footprinting Through Web Services

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

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

Target: https:/www.eccouncil.org