



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

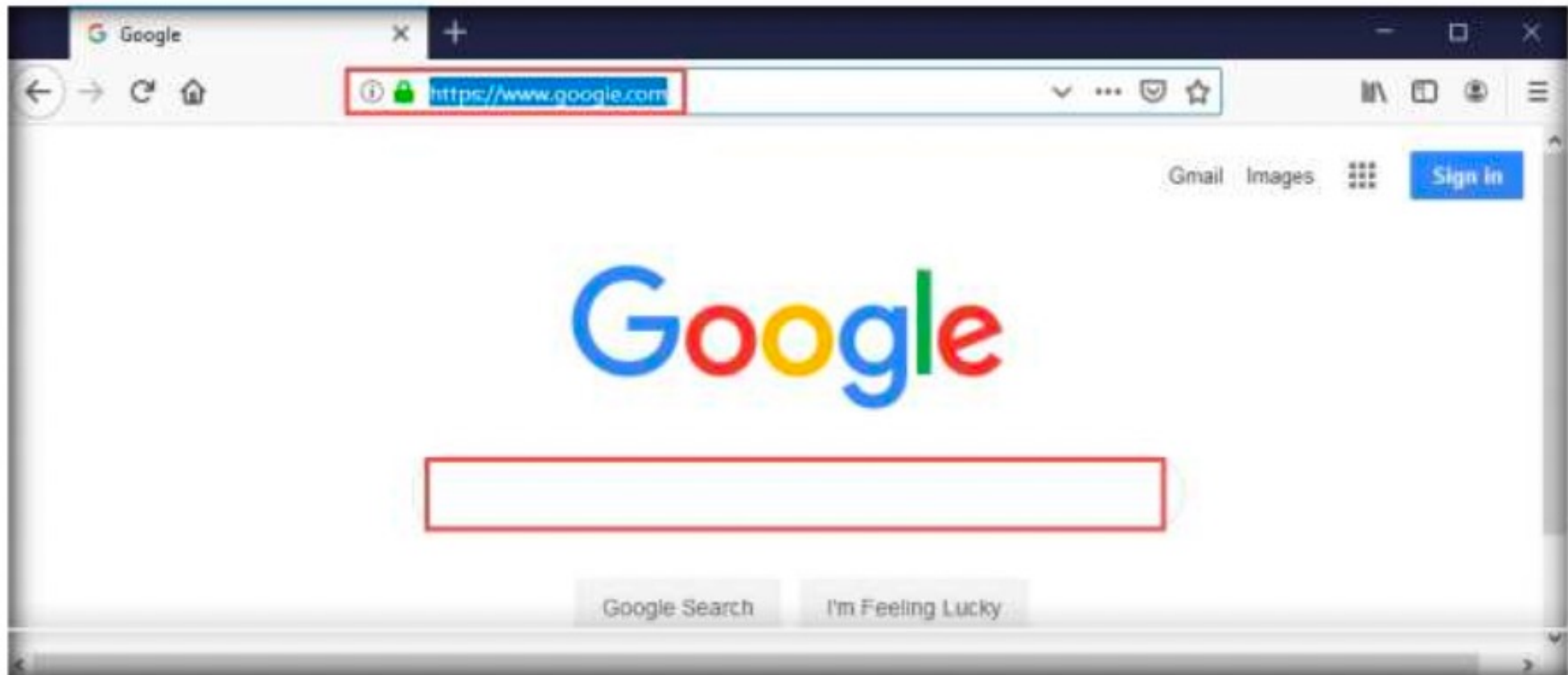
2- Footprinting is the first step of any attack, the attacker collects information about a target network.

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>.

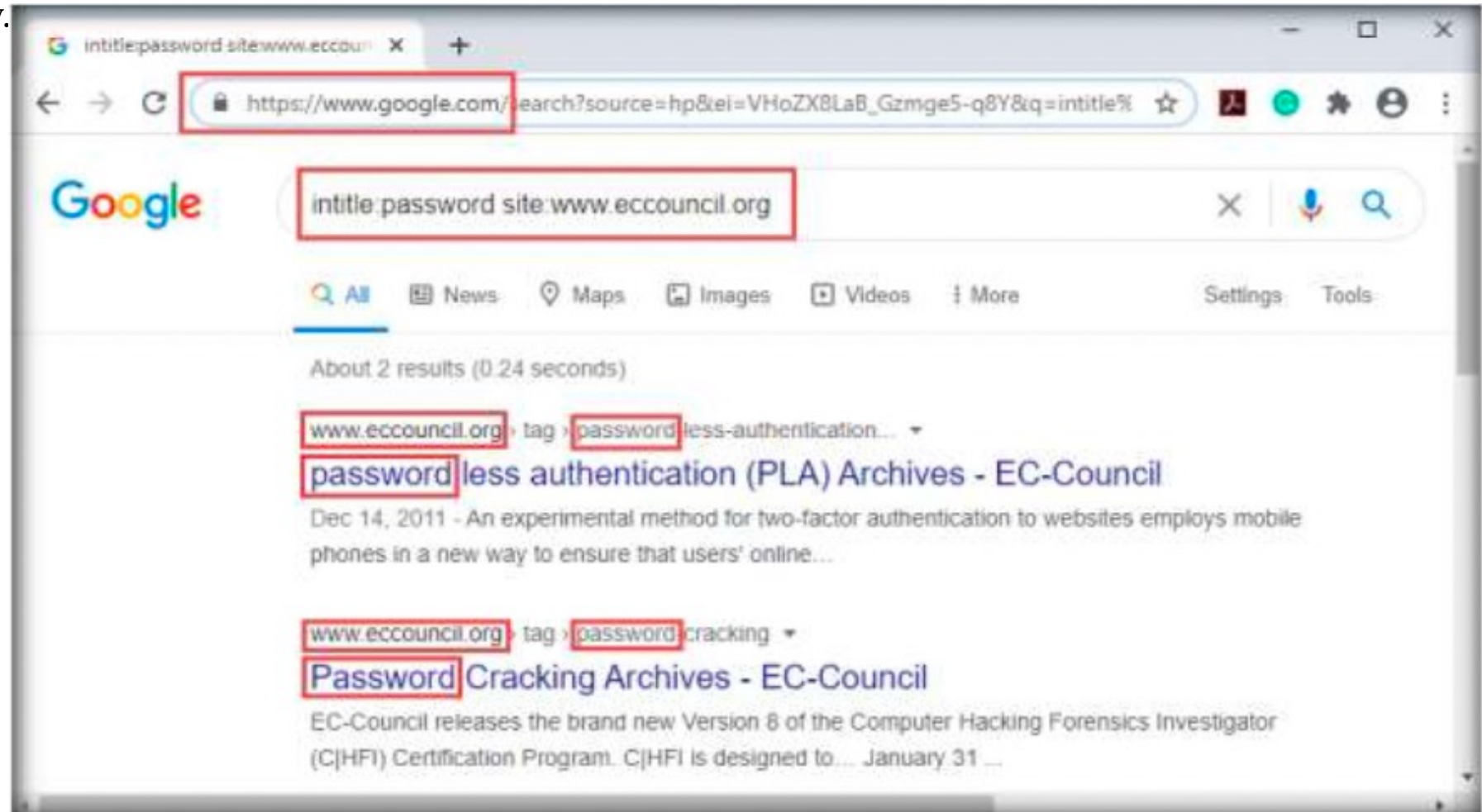


1

Gather Information using Advanced Google Hacking Techniques

Perform
Footprinting
Through
Search Engines

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.

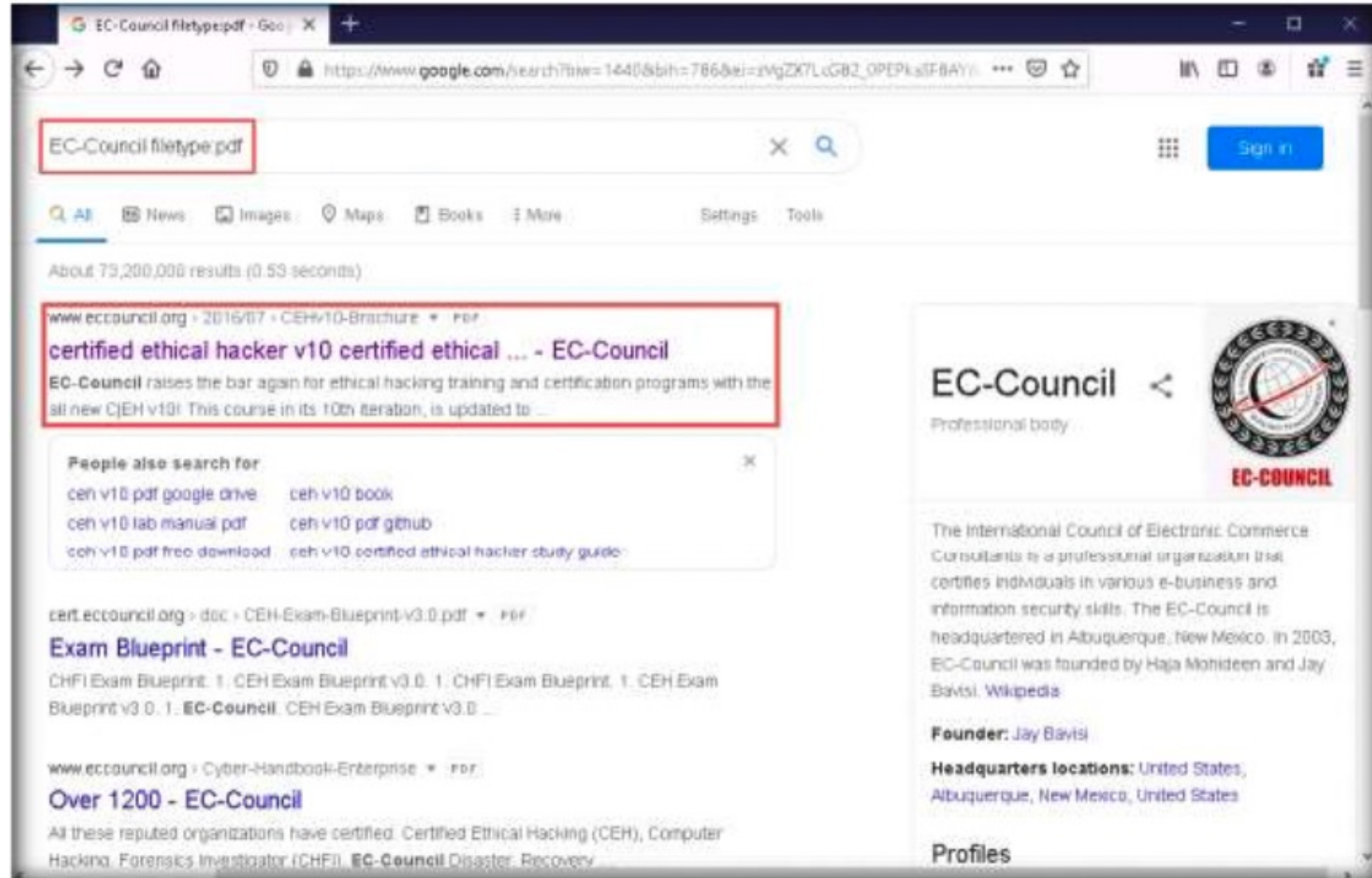


1

Gather Information using Advanced Google Hacking Techniques

Perform
Footprinting
Through
Search Engines

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..



1

Gather Information using Advanced Google Hacking Techniques

Perform
Footprinting
Through
Search Engines

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

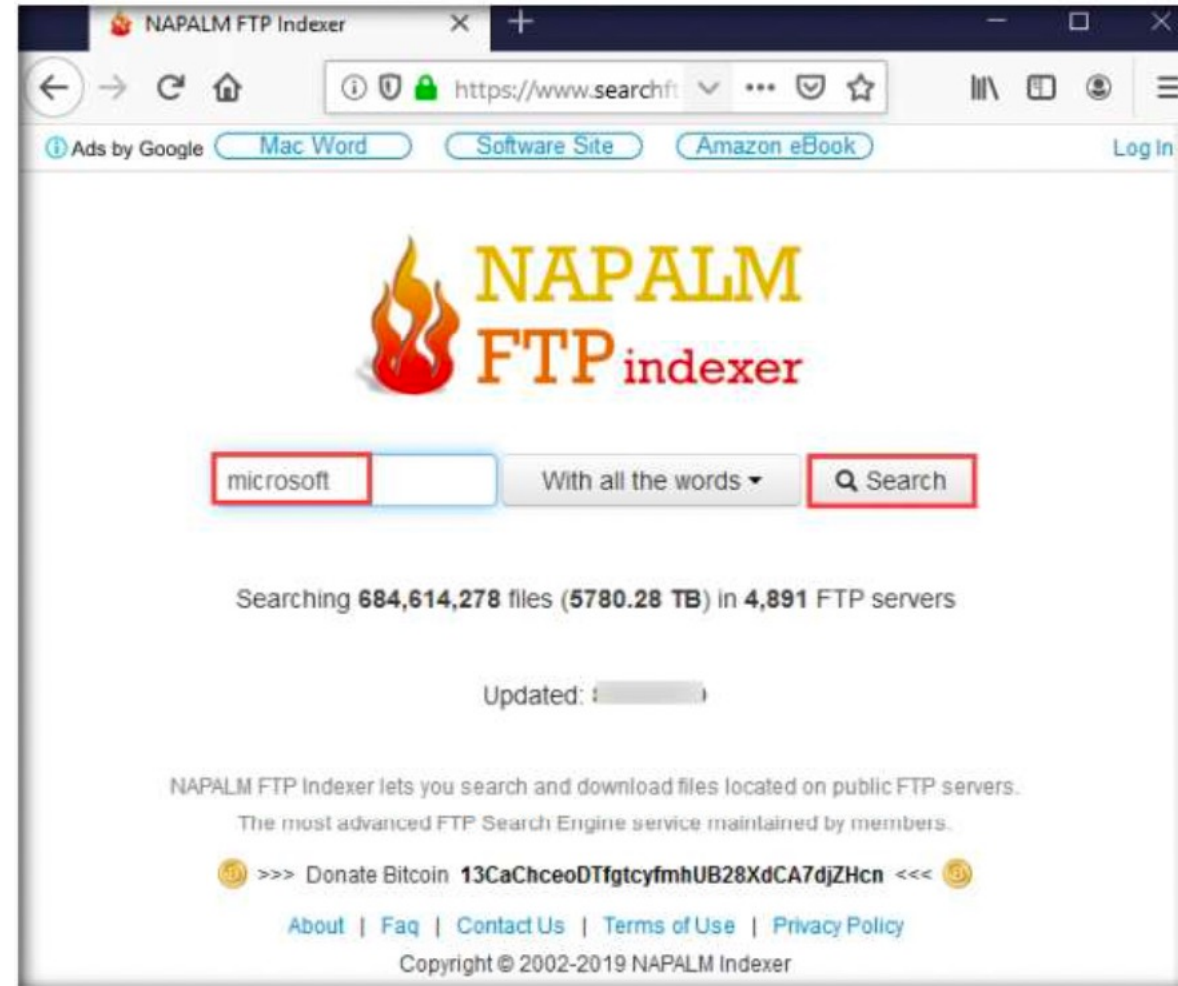


2

Gather Information from FTP Search Engines

Perform
Footprinting
Through
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**

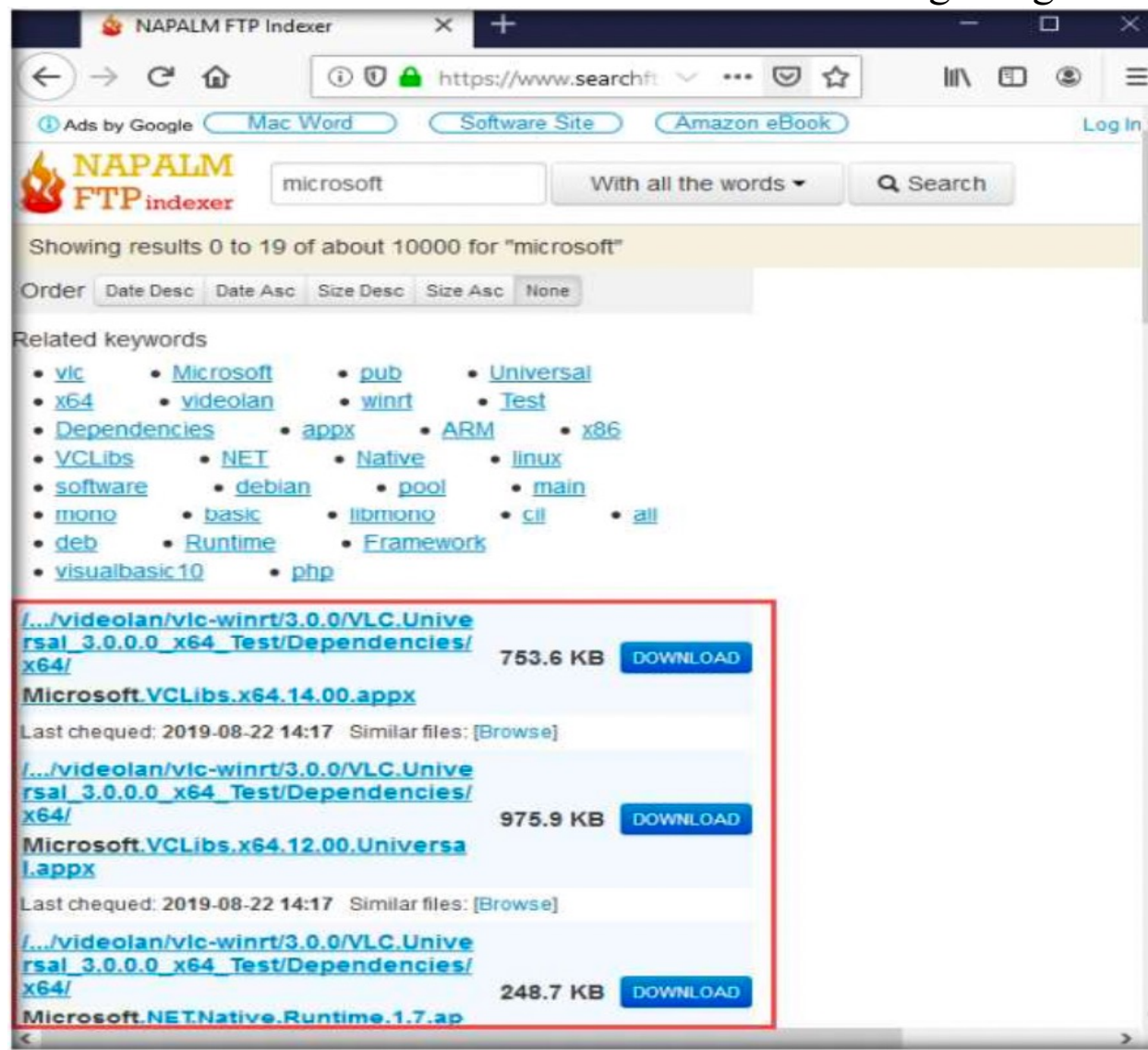


2

Gather Information from FTP Search Engines

Perform
Footprinting
Through
Search Engines

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



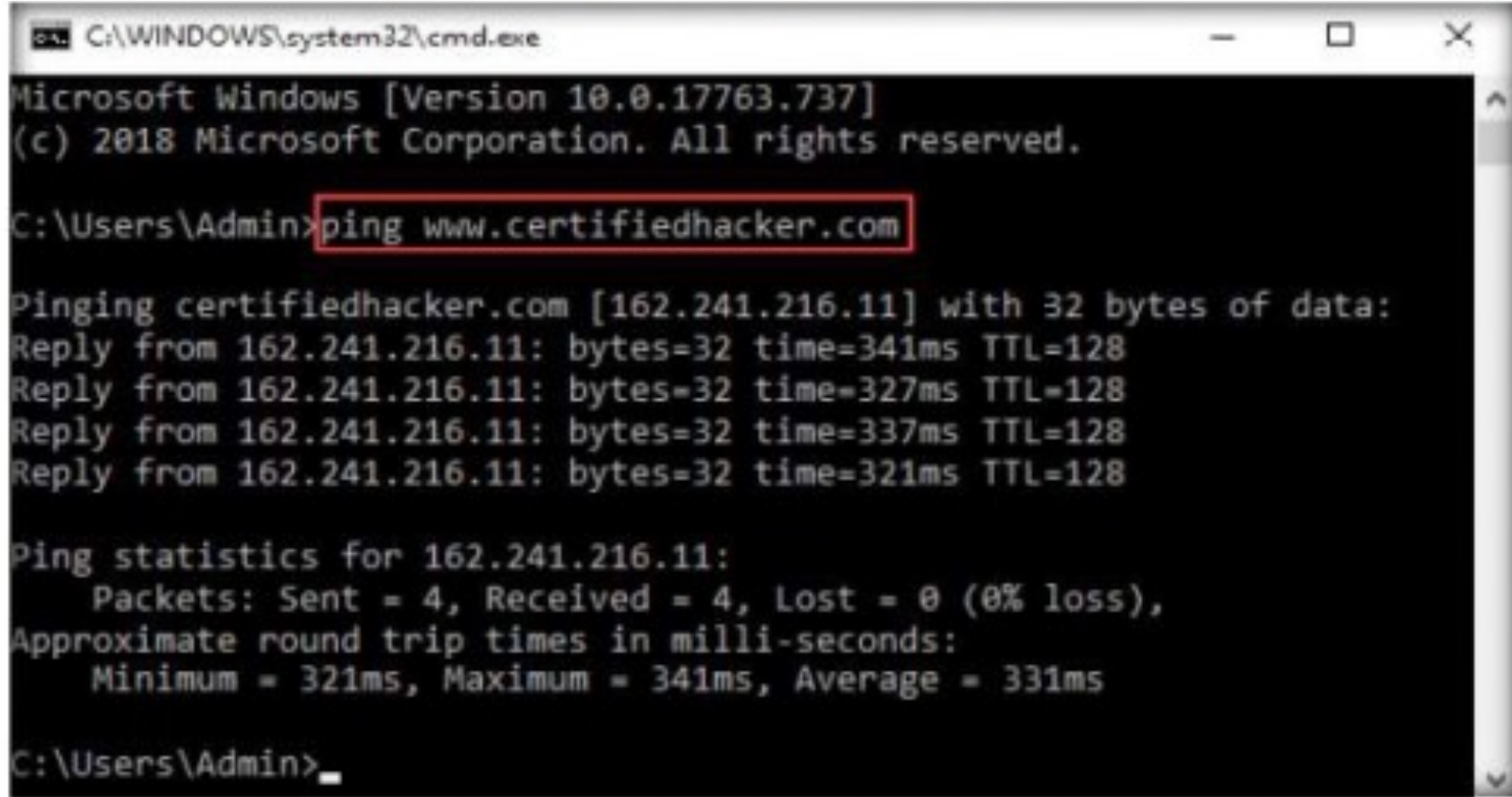
3

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.

A screenshot of a Windows Command Prompt window. The title bar shows 'C:\WINDOWS\system32\cmd.exe'. The window contains the following text: 'Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Users\Admin>ping www.certifiedhacker.com'. The command is highlighted with a red rectangular box. Below the command, the output shows four successful ping replies from IP address 162.241.216.11, each with 32 bytes of data, varying round-trip times (341ms, 327ms, 337ms, 321ms), and a TTL of 128. Finally, it displays ping statistics: 4 packets sent, 4 received, 0% loss, with minimum, maximum, and average round-trip times of 321ms, 341ms, and 331ms respectively. The prompt ends with 'C:\Users\Admin>_'.

```
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>_
```

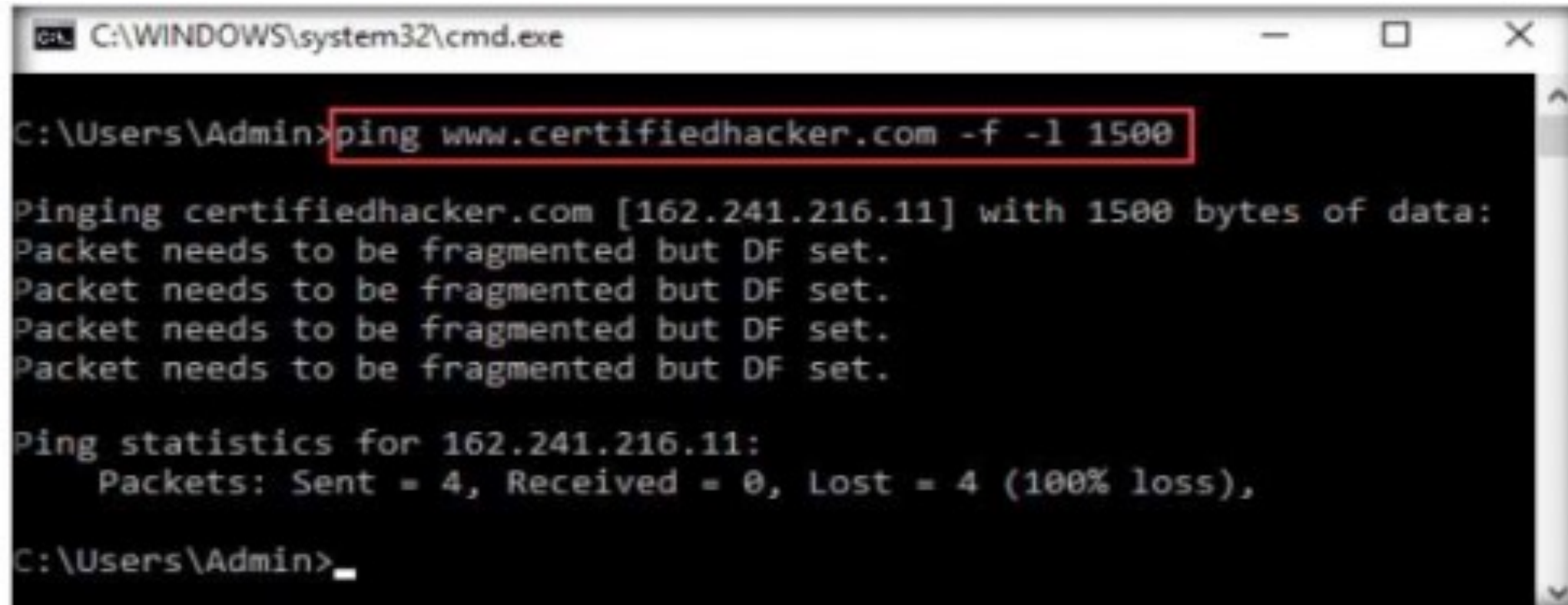
3

Website Footprinting

3.1

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

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**.



```
C:\WINDOWS\system32\cmd.exe

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.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
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>
```

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

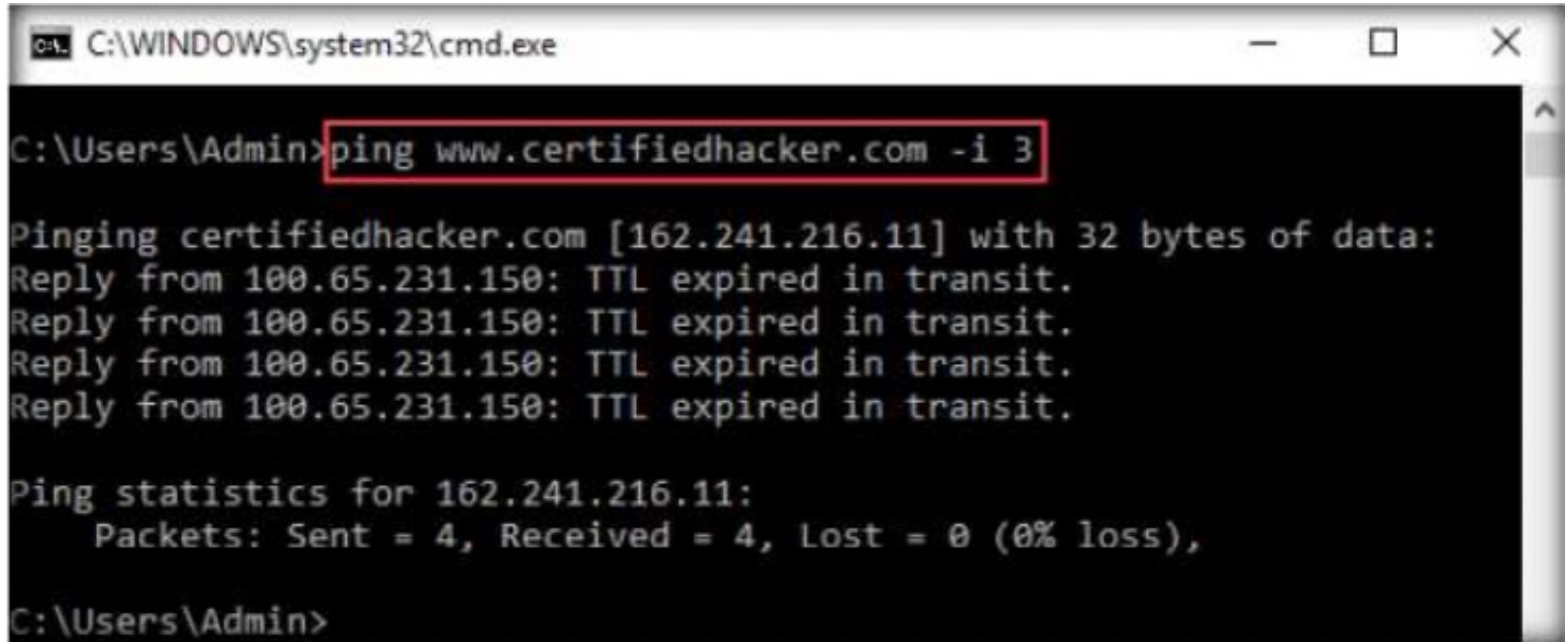
3

Website Footprinting

3.1

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

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



```
C:\WINDOWS\system32\cmd.exe

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

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 100.65.231.150: TTL expired in transit.
Reply from 100.65.231.150: TTL expired in transit.
Reply from 100.65.231.150: TTL expired in transit.
Reply from 100.65.231.150: TTL expired in transit.

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

C:\Users\Admin>
```

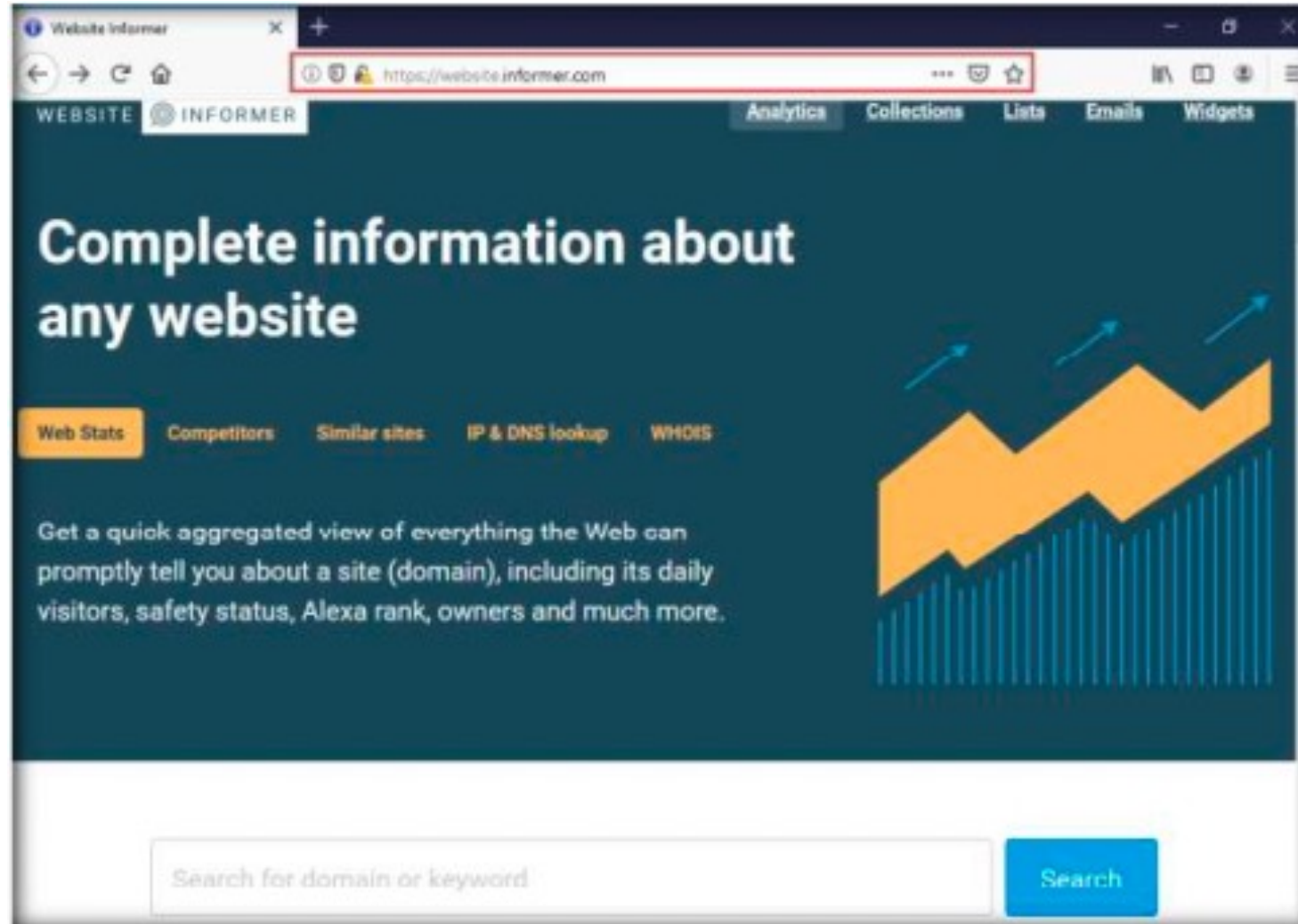
3

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.



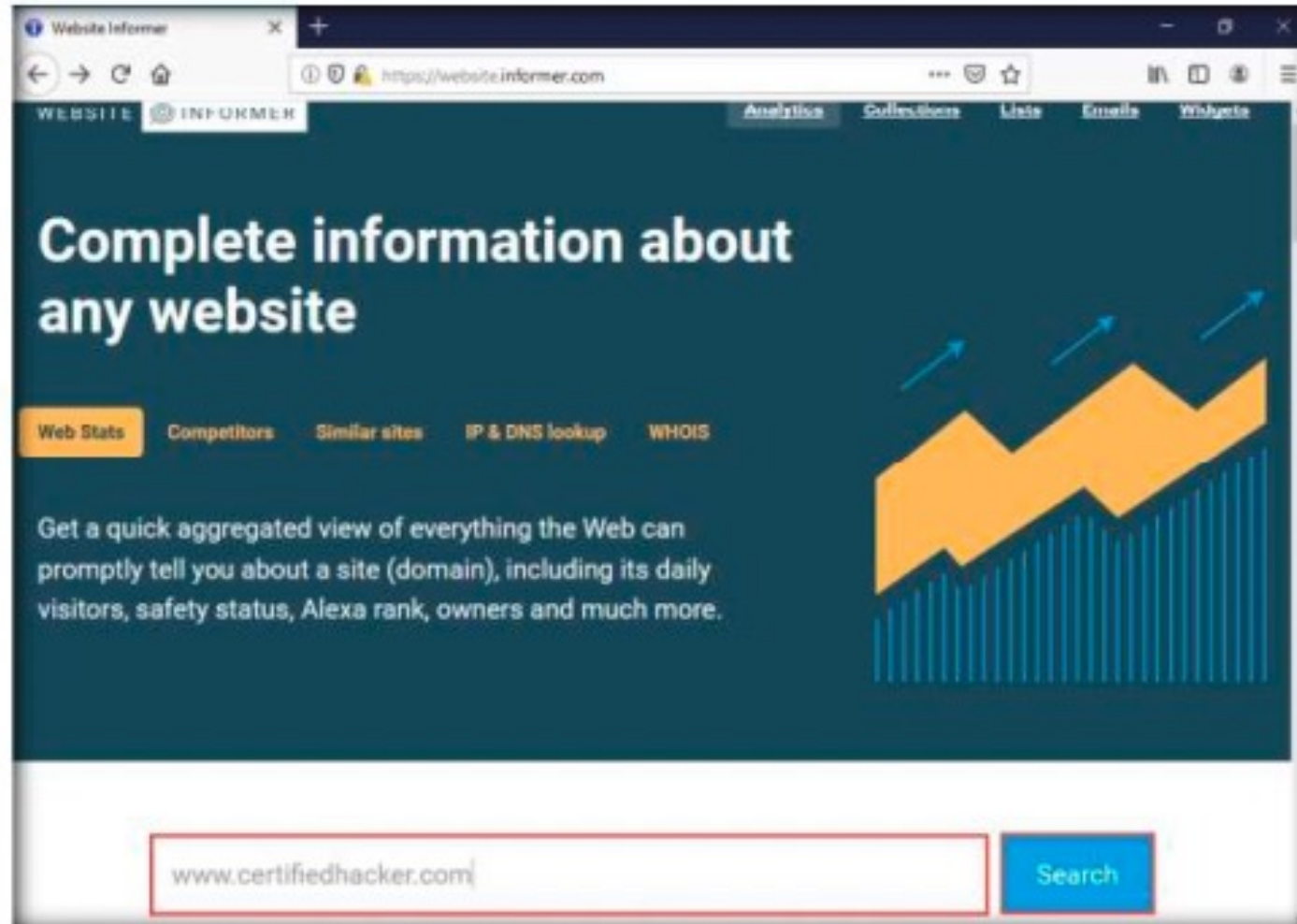
3

Website Footprinting

3.2

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

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

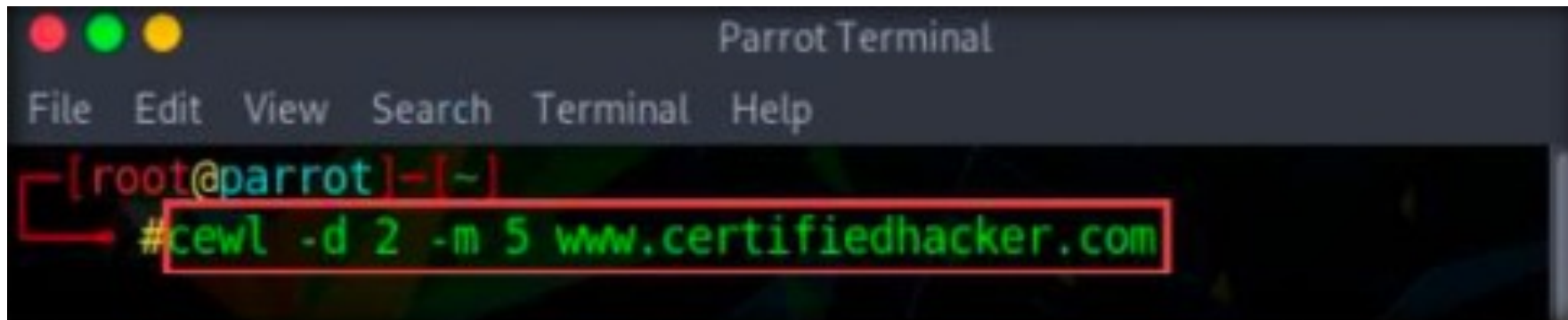
Gather a Wordlist from the Target Website using **CeWL**

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



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

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



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
# cewl -d 2 -m 5 www.certifiedhacker.com
```

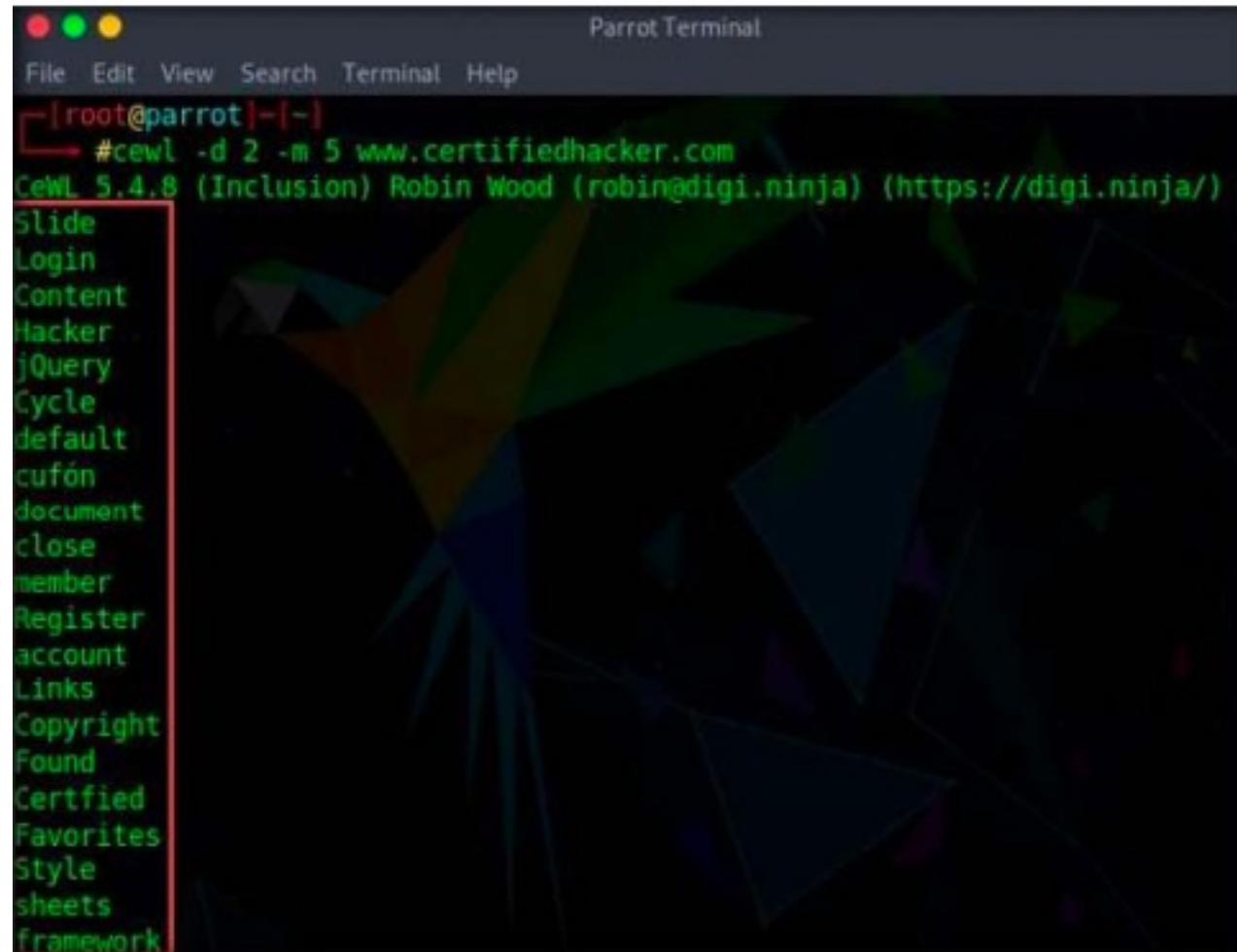
3

Website Footprinting

3.4

Gather a Wordlist from the Target Website
using **CeWL**

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.



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# #cewl -d 2 -m 5 www.certifiedhacker.com
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Slide
Login
Content
Hacker
jQuery
Cycle
default
cufón
document
close
member
Register
account
Links
Copyright
Found
Certfied
Favorites
Style
sheets
framework
```

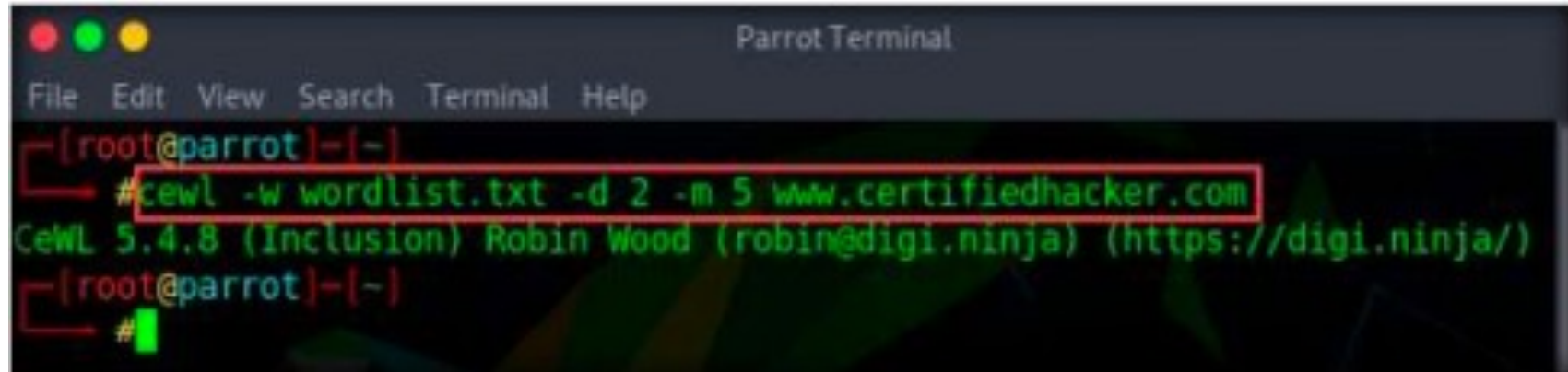
3

Website Footprinting

3.5

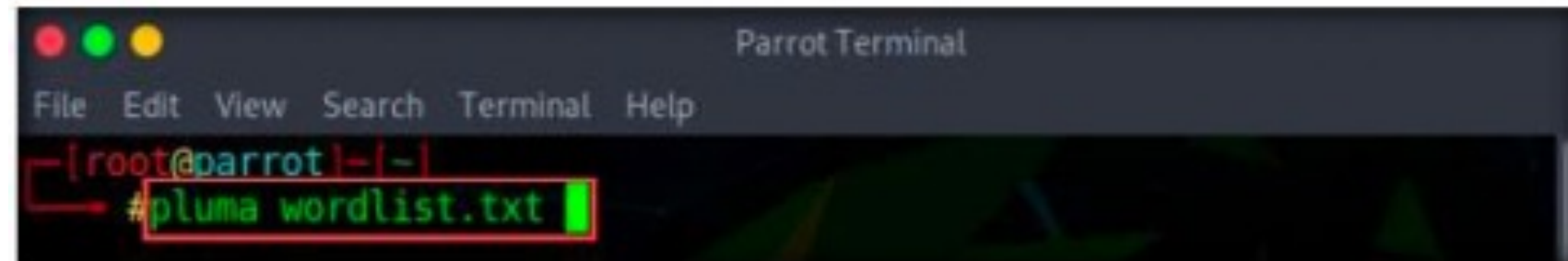
Gather a Wordlist from the Target Website
using **CeWL**

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**)



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
[root@parrot]-[~]
#
```

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



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#pluma wordlist.txt
```

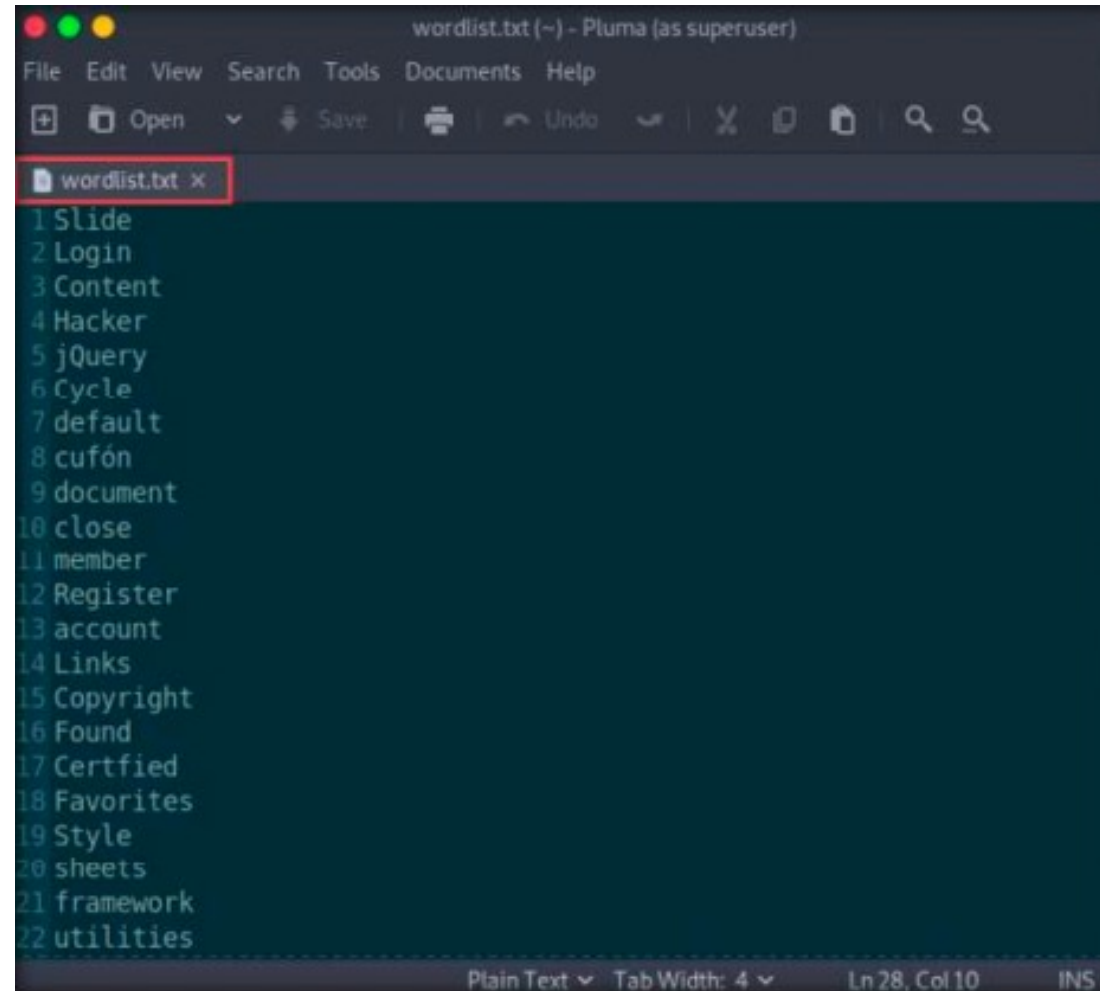
3

Website Footprinting

3.5

Gather a Wordlist from the Target Website
using **CeWL**

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



The screenshot shows a text editor window titled "wordlist.txt (~) - Pluma (as superuser)". The window contains a list of words extracted from a target website, numbered 1 through 22. The words are: Slide, Login, Content, Hacker, jQuery, Cycle, default, cufón, document, close, member, Register, account, Links, Copyright, Found, Certfied, Favorites, Style, sheets, framework, and utilities. The text is displayed in a dark-themed editor with a light blue background. The status bar at the bottom indicates "Plain Text", "Tab Width: 4", "Ln 28, Col 10", and "INS".

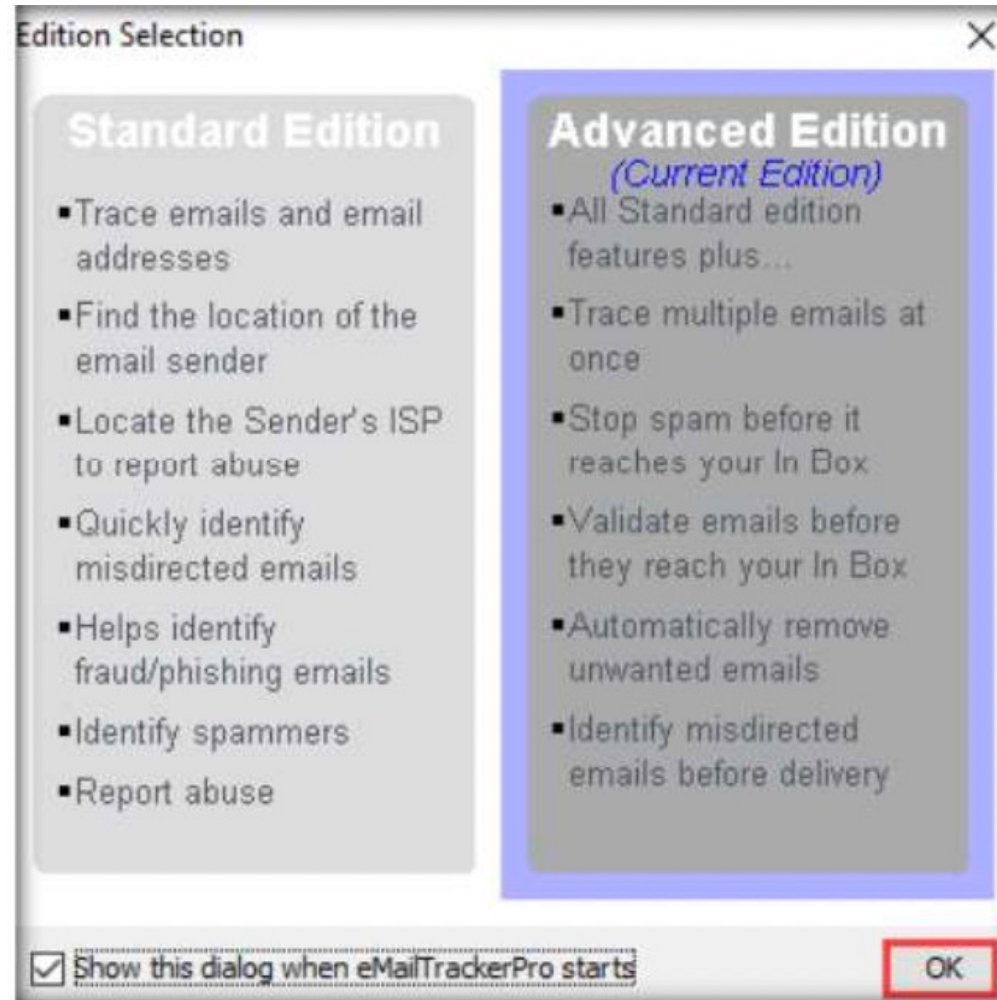
```
wordlist.txt (~) - Pluma (as superuser)
File Edit View Search Tools Documents Help
+ Open Save Undo
wordlist.txt x
1 Slide
2 Login
3 Content
4 Hacker
5 jQuery
6 Cycle
7 default
8 cufón
9 document
10 close
11 member
12 Register
13 account
14 Links
15 Copyright
16 Found
17 Certfied
18 Favorites
19 Style
20 sheets
21 framework
22 utilities
Plain Text Tab Width: 4 Ln 28, Col 10 INS
```

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**.

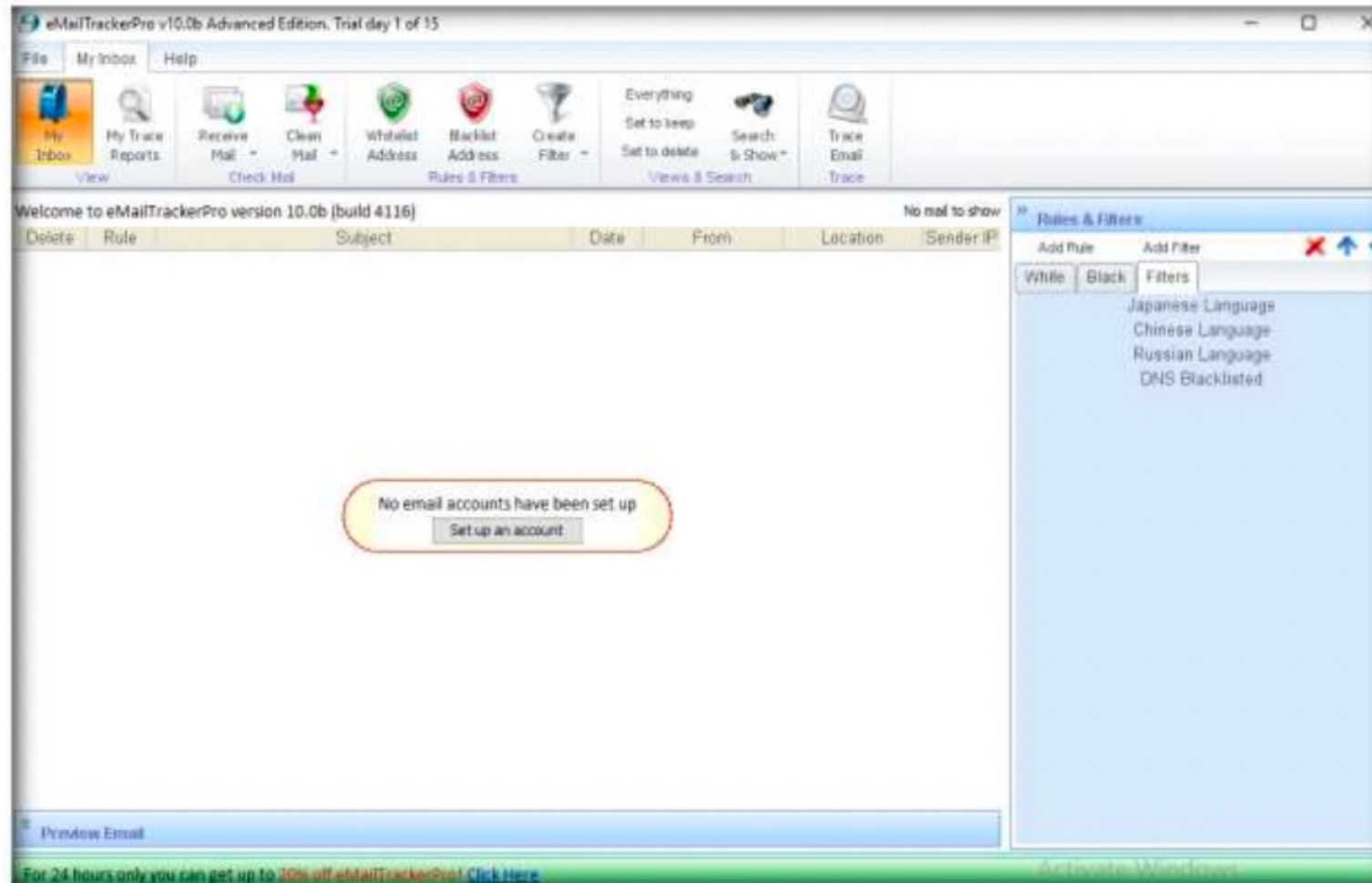


5

Email Footprinting

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

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

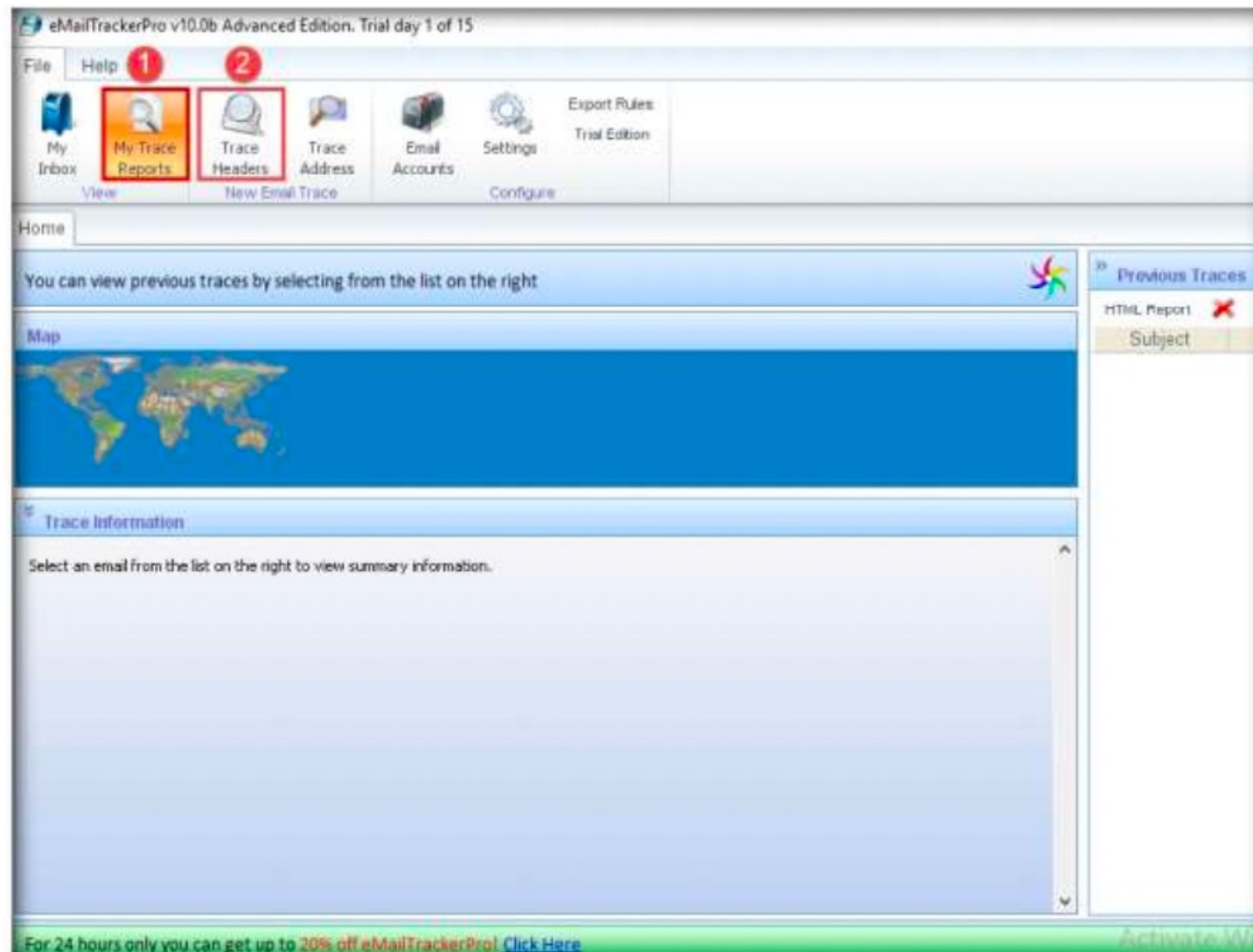


5

Email Footprinting

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

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.



5

Email Footprinting

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

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.

Visualware eMailTrackerPro Trial (day 1 of 15)

[Configure](#) | [Help](#) | [About](#)

eMailTrackerPro by Visualware

I Want To:

☒ **Trace an email I have received**

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP ([more info](#)).

☐ **Look up network responsible for an email address**

An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details

To proceed, paste the email headers in the box below ([how do I find the headers?](#)).

Note: If you are using Microsoft Outlook, you can trace an email message directly from Outlook by using the eMailTrackerPro shortcut on the toolbar.

Email headers:

Trace **Cancel**

5

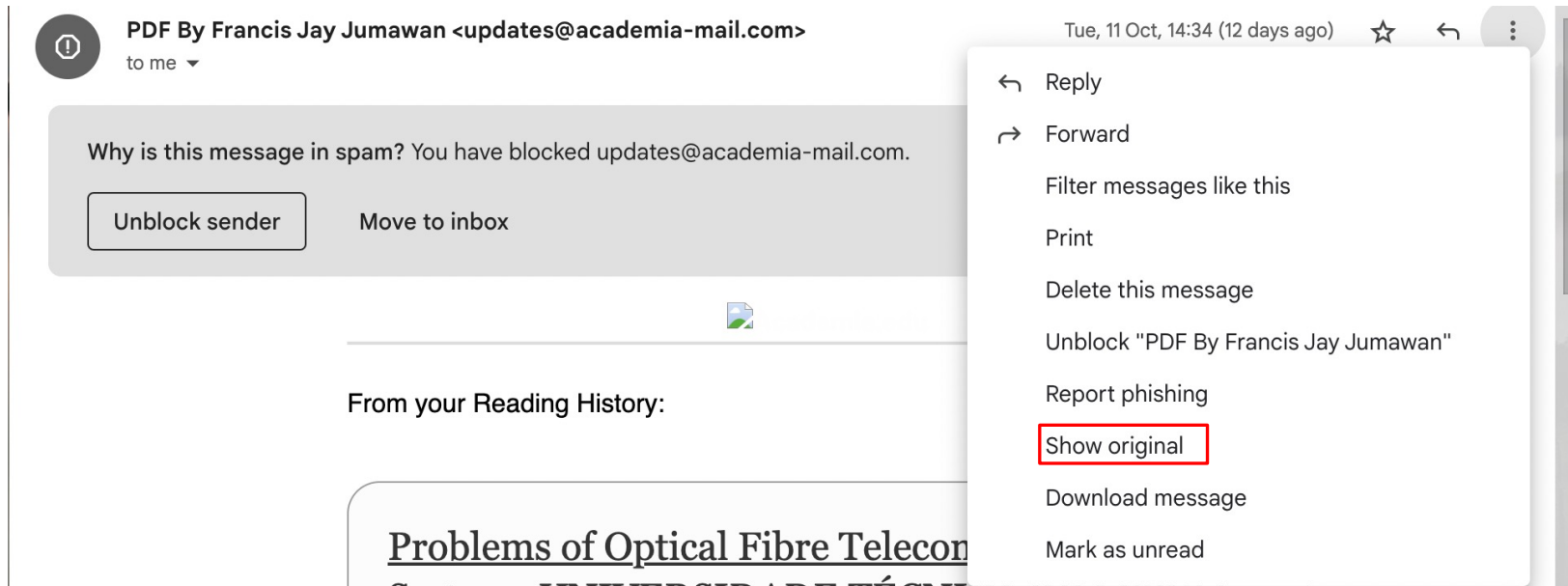
Email Footprinting

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

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.

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.



5

Email Footprinting

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

Original Message

Message ID: <c6a3ec45832af8bb2ab7416077b2af85@localhost.localdomain>
Created at: [REDACTED] at 2:48 PM (Delivered after 1 second)
From: TSVBNKCRD <[REDACTED]@[REDACTED].info> Using PHPMailer [version 1.73]
To: [REDACTED]@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](#)

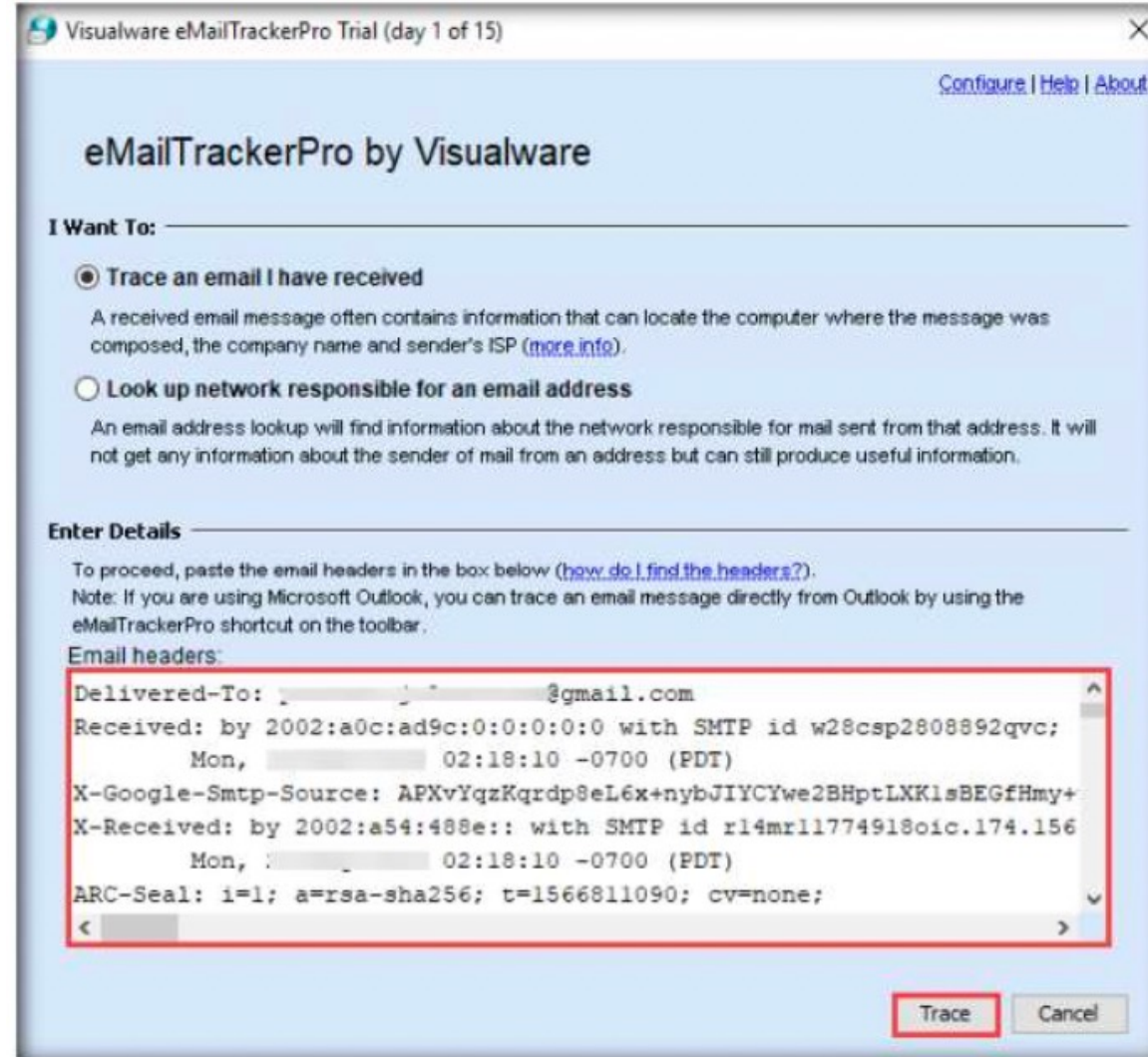
```
Delivered-To: [REDACTED]@gmail.com
Received: by 2002:a0c:ad9c:0:0:0:0 with SMTP id w28csp2808892qvc;
Mon, 02:18:10 -0700 (PDT)
X-Google-Smtp-Source: APXvYqzKqrdp8eL6x+nyb3IYCYwe2BHptLXX1sBEGfHmy+vC1VG4ybuN6dsWCgZ+4Zmulh3YTtPg
X-Received: by 2002:a54:488e:: with SMTP id r14mr11774918oic.174.1566811090471;
Mon, 02:18:10 -0700 (PDT)
ARC-Seal: 1=1; a=rsa-sha256; t=1566811090; cv=none;
d=google.com; s=arc-20160816;
b=D8E17aUKPGkvRo7nqaDxb301LqMdh/+5X1gLhXa07Q0bc0MoB48fcsT5n/876SeqX
BfVzgM/Su9o+piYnFaxXsDBAIAz9Me7DVA57dYtDxUeX9xQb8rIUg75xVISCLBUNQ61
XS1cH3i3Bb7T14GQ0doR81DH6nCOwVG2WTEHTR10EvM1KpUZ4FEXDFeRk6X2QvcpgL3
rrpYvLag2JCazyPqMY0B8x65XphkH1gv+vdF/L1UsFsHybCYpNsUtE+89ghwLTXPYOfW
```


5

Email Footprinting

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

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



Visualware eMailTrackerPro Trial (day 1 of 15)

[Configure](#) | [Help](#) | [About](#)

eMailTrackerPro by Visualware

I Want To: _____

☒ **Trace an email I have received**

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP ([more info](#)).

☐ **Look up network responsible for an email address**

An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details _____

To proceed, paste the email headers in the box below ([how do I find the headers?](#)).
Note: If you are using Microsoft Outlook, you can trace an email message directly from Outlook by using the eMailTrackerPro shortcut on the toolbar.

Email headers:

```
Delivered-To: [redacted]@gmail.com
Received: by 2002:a0c:ad9c:0:0:0:0:0 with SMTP id w28csp2808892qvc;
Mon, [redacted] 02:18:10 -0700 (PDT)
X-Google-Smtp-Source: APXvYqzKqrdp8eL6x+nybJIYCYwe2BHptLXK1sBEGfHmy+
X-Received: by 2002:a54:488e:: with SMTP id rl4mr11774918oic.174.156
Mon, [redacted] 02:18:10 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1566811090; cv=none;
```

Trace **Cancel**

5

Email Footprinting

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

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.

The screenshot displays the eMailTrackerPro v10.0b Advanced Edition interface. The main window shows a world map with a location marker in West Chester, Pennsylvania, USA. Below the map is a table showing the email trace hops.

Hop #	Hop IP	Hop Name	Location
End	208.78.224.20	server.economist.co.uk	West Chester, Pennsylvania, USA

The right-hand side of the window displays the **Email Summary** for the traced email. The summary includes the following information:

- From:** [Redacted]
- To:** [Redacted]@gmail.com
- Date:** Mon, 09:18:09 +0000
- Subject:** THYBNKCRD CREDIT CARD (XQ2S17) WILL BE DE
- Location:** West Chester, Pennsylvania, USA
- Misdirected:** No
- Abuse Address:** abuse@private-systems.net
- Abuse Reporting:** To automatically generate an email abi
- From IP:** 208.78.224.20

System Information:

- The system is running a mail server (ESMTP Exim - This means that this system can be used to send e
- The system is running a web server on port 80 (s.i) This means that this system serves web pages.
- The system is running a secure web server (Apache (link here to view it). This means that this system

At the bottom of the window, there are links for **Network Whois**, **Domain Whois**, and **Email Header**.

5

Email Footprinting

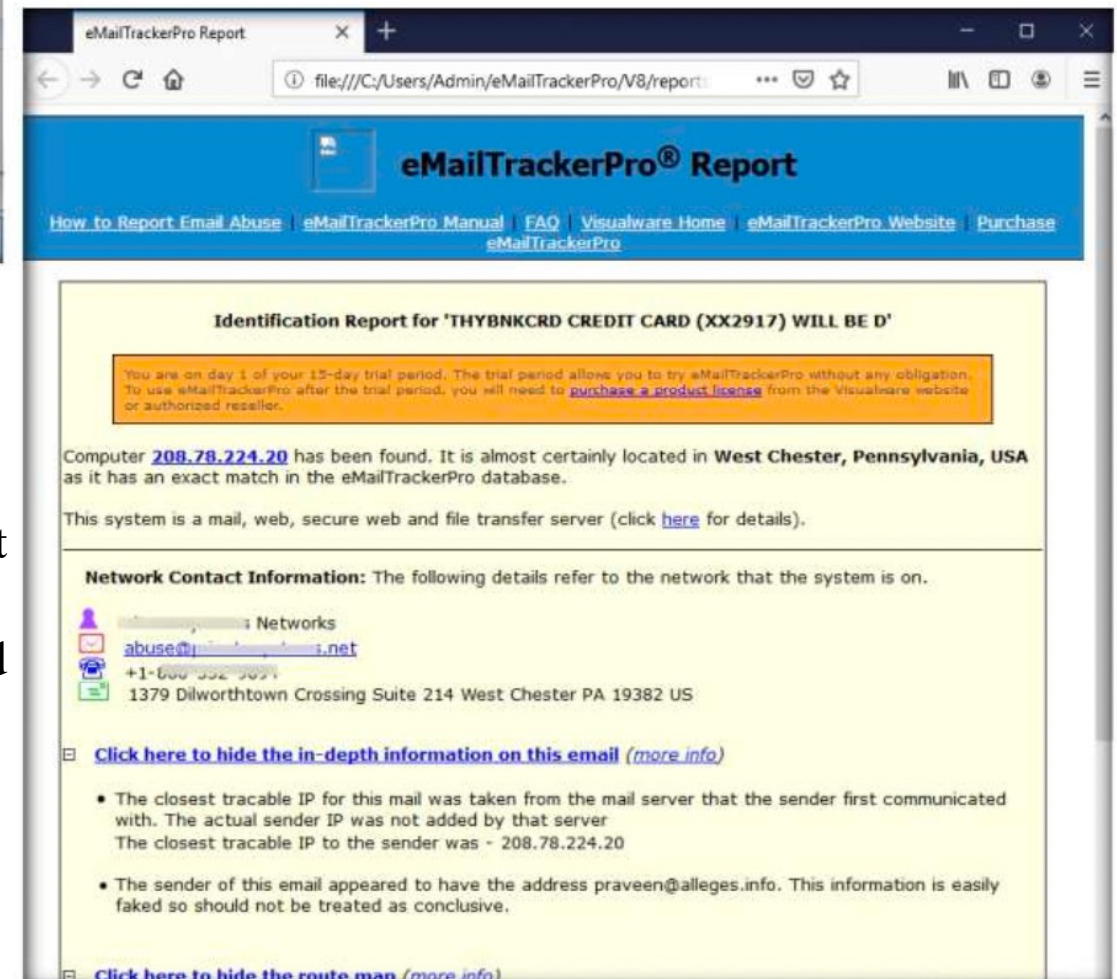
Gather Information about a Target by Tracing Emails using **eMailTrackerPro**

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.



5

Email Footprinting

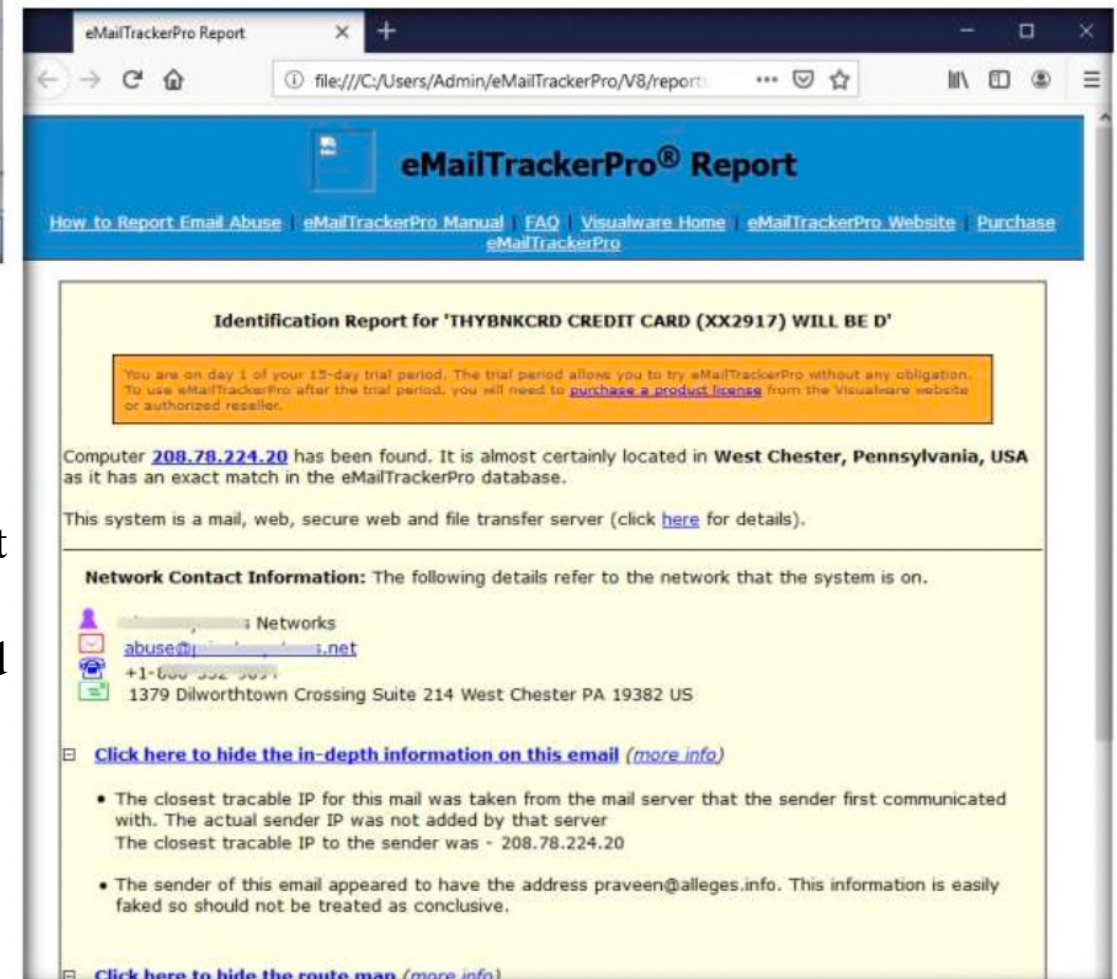
Gather Information about a Target by Tracing Emails using **eMailTrackerPro**

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.



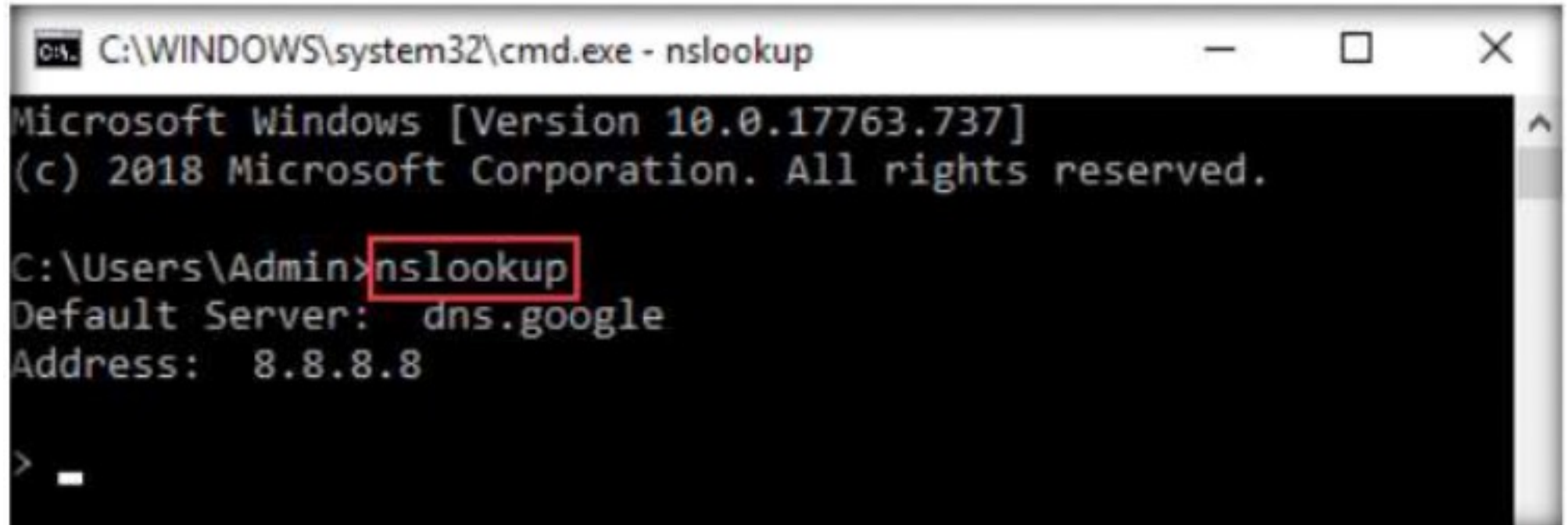
6

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**



```
C:\WINDOWS\system32\cmd.exe - nslookup

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

> _
```

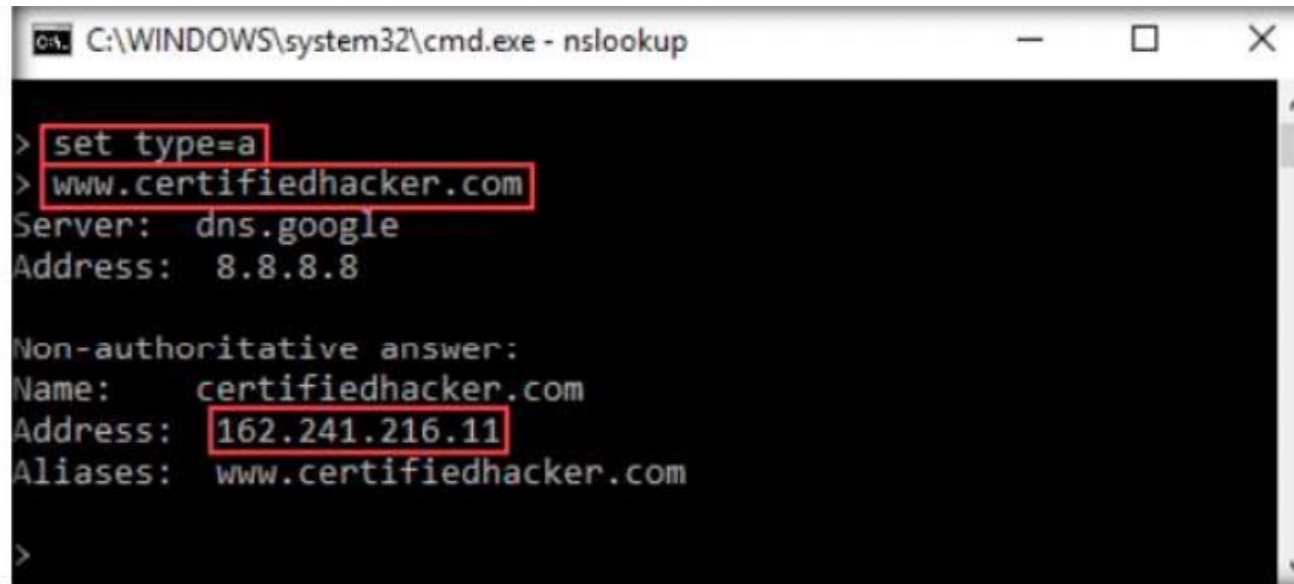

6

DNS Footprinting

6.1

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

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.



```
C:\WINDOWS\system32\cmd.exe - nslookup

> 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

>
```

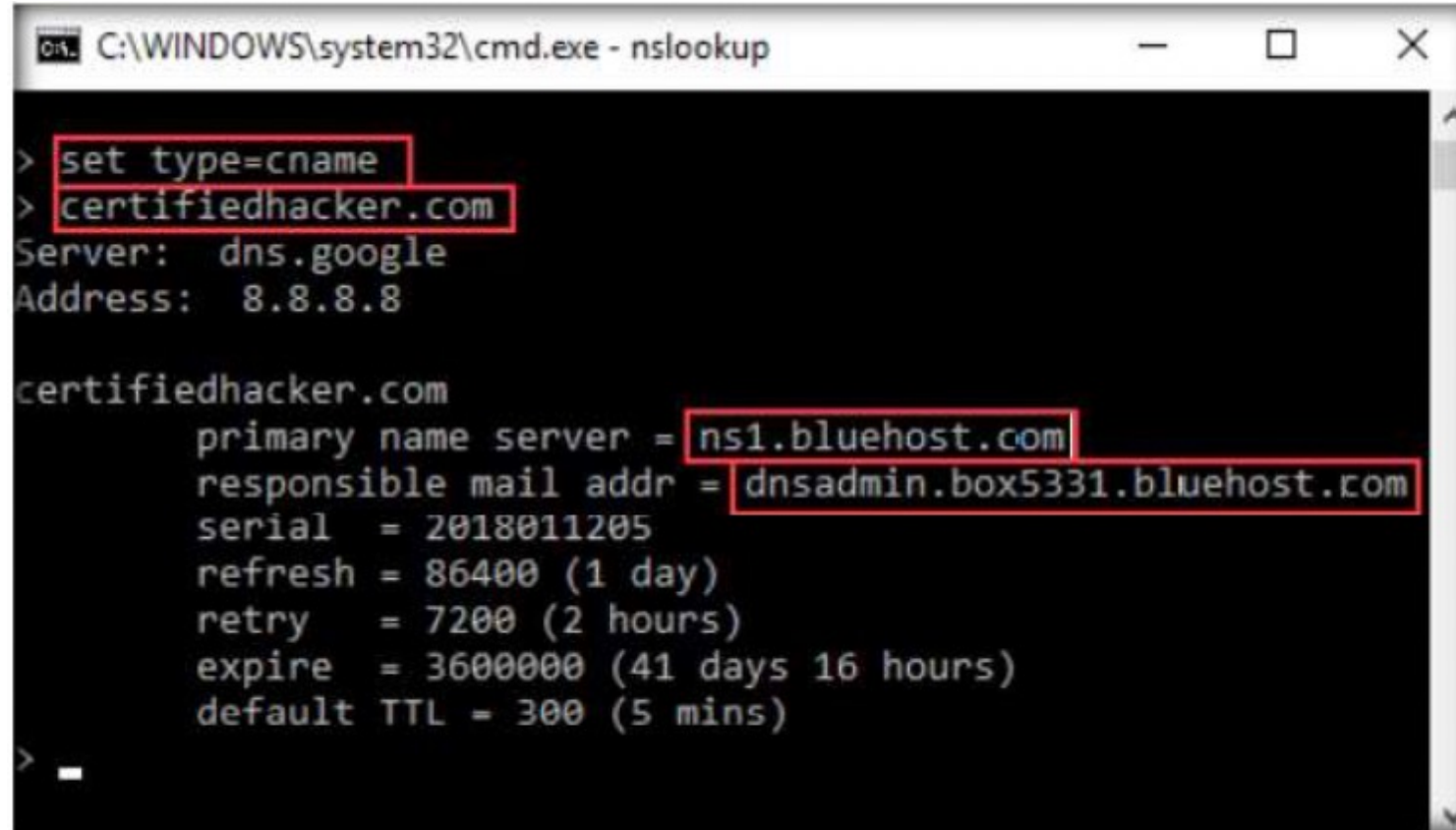
6

DNS Footprinting

6.1

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

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



```
C:\WINDOWS\system32\cmd.exe - nslookup

> 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)

> _
```

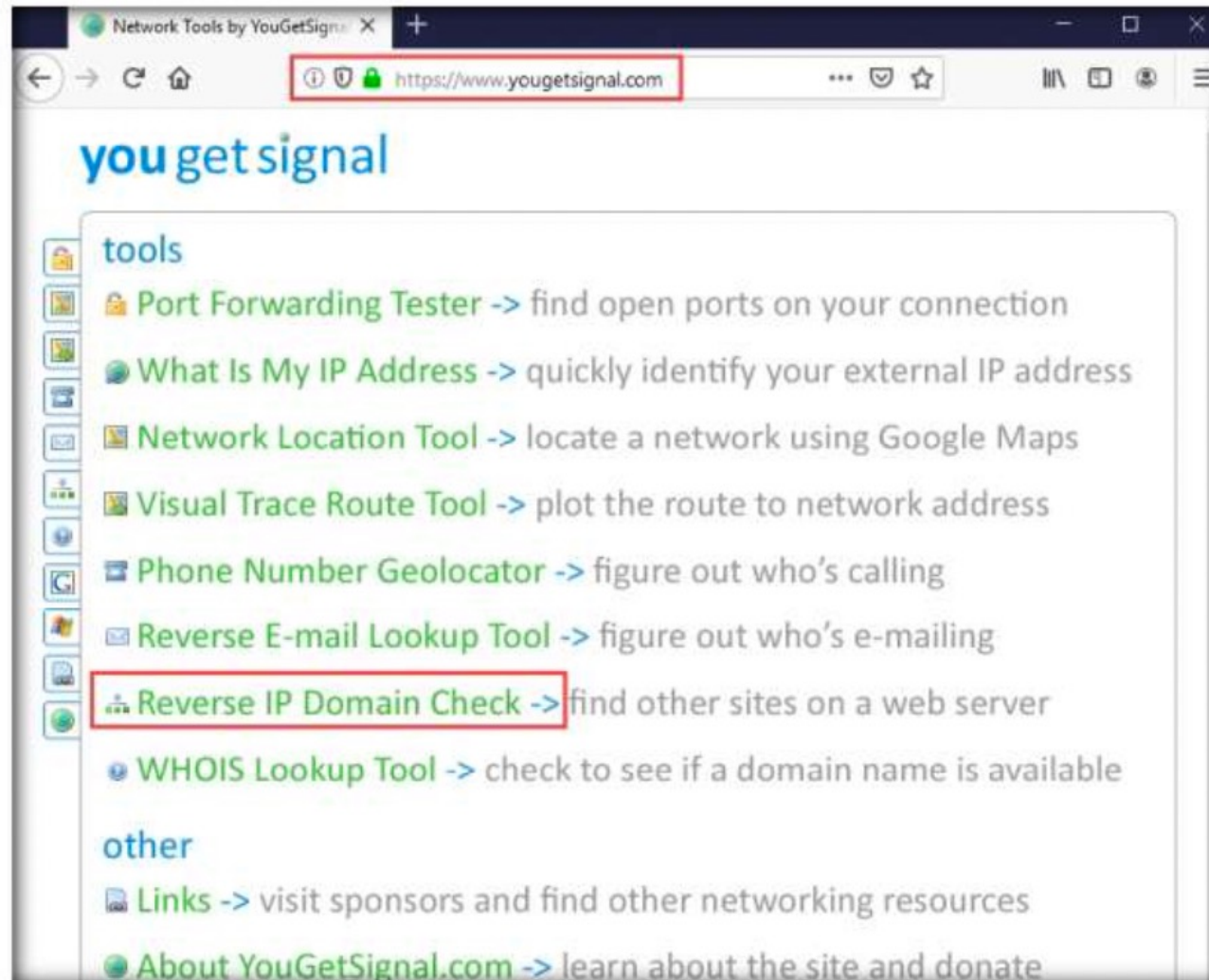
6

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**



6

DNS Footprinting

6.2

Perform Reverse DNS Lookup using
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**.



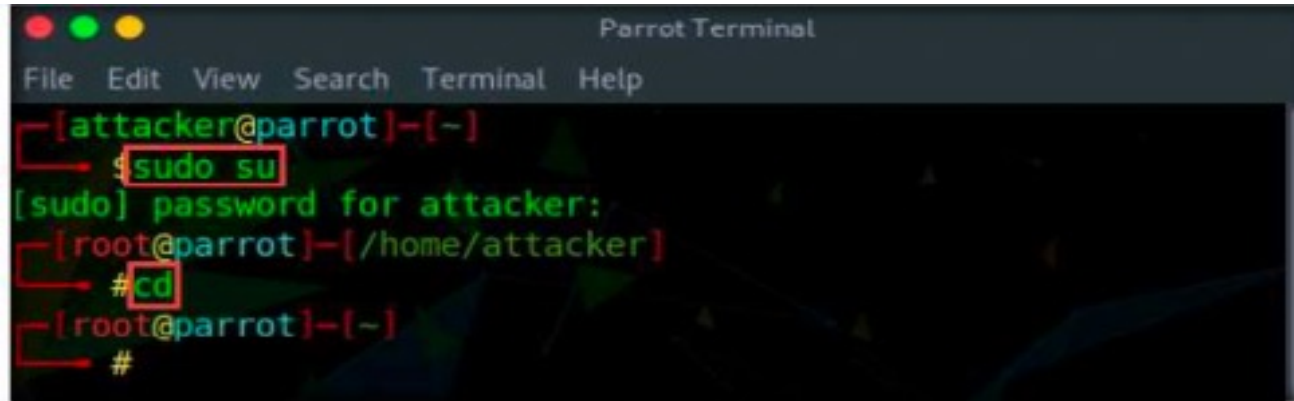
6

DNS Footprinting

6.3

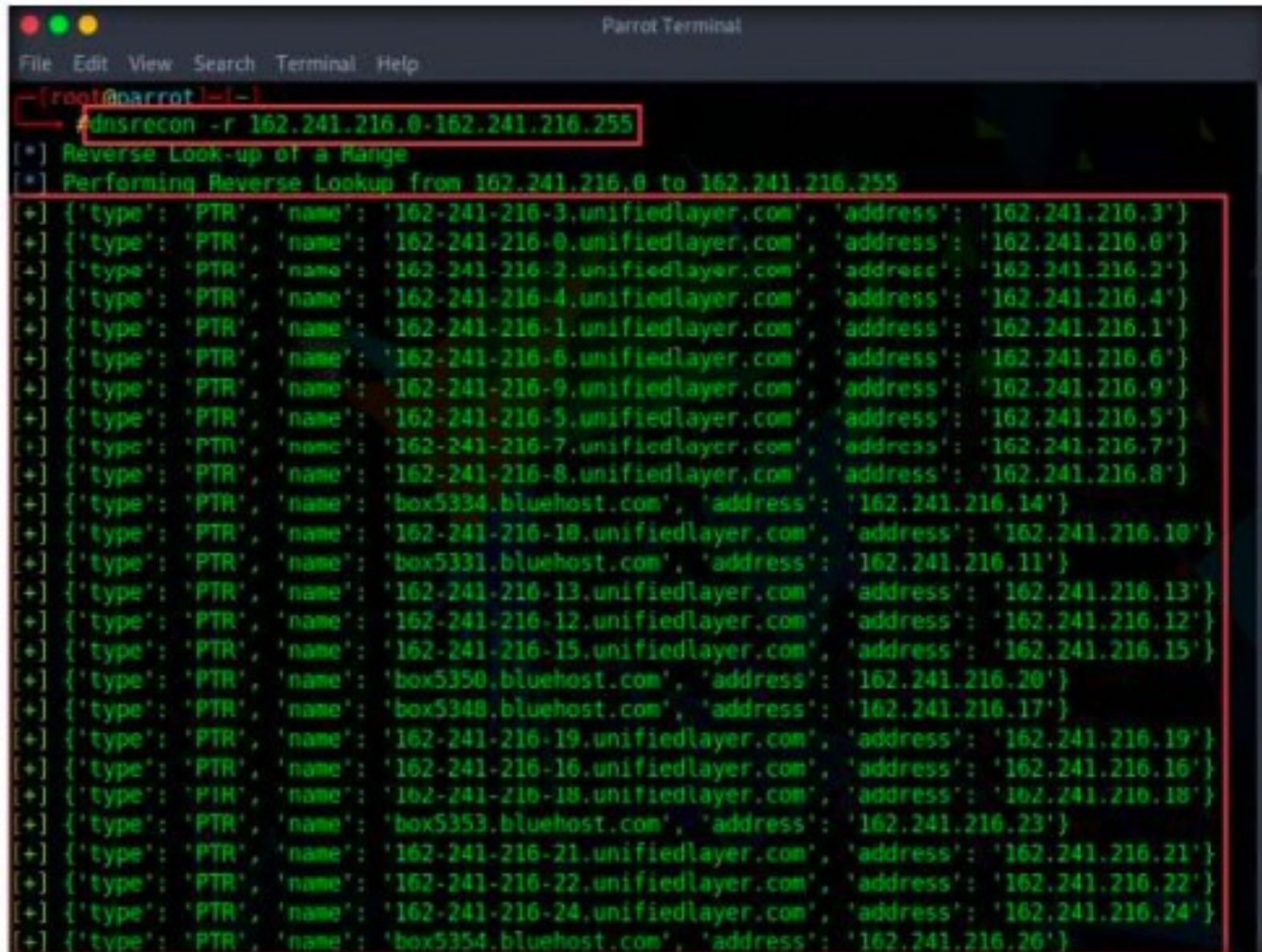
Perform Reverse DNS Lookup using DNSRecon

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



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

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.



A screenshot of a Parrot Terminal window showing a reverse DNS lookup performed using the `dnsrecon` tool. The terminal title is "Parrot Terminal". The command `dnsrecon -r 162.241.216.0-162.241.216.255` is entered and executed. The output shows a list of PTR records for the specified IP range, including domains like `unifiedlayer.com` and `bluehost.com`. The output is highlighted with a red box.

```
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'}
```

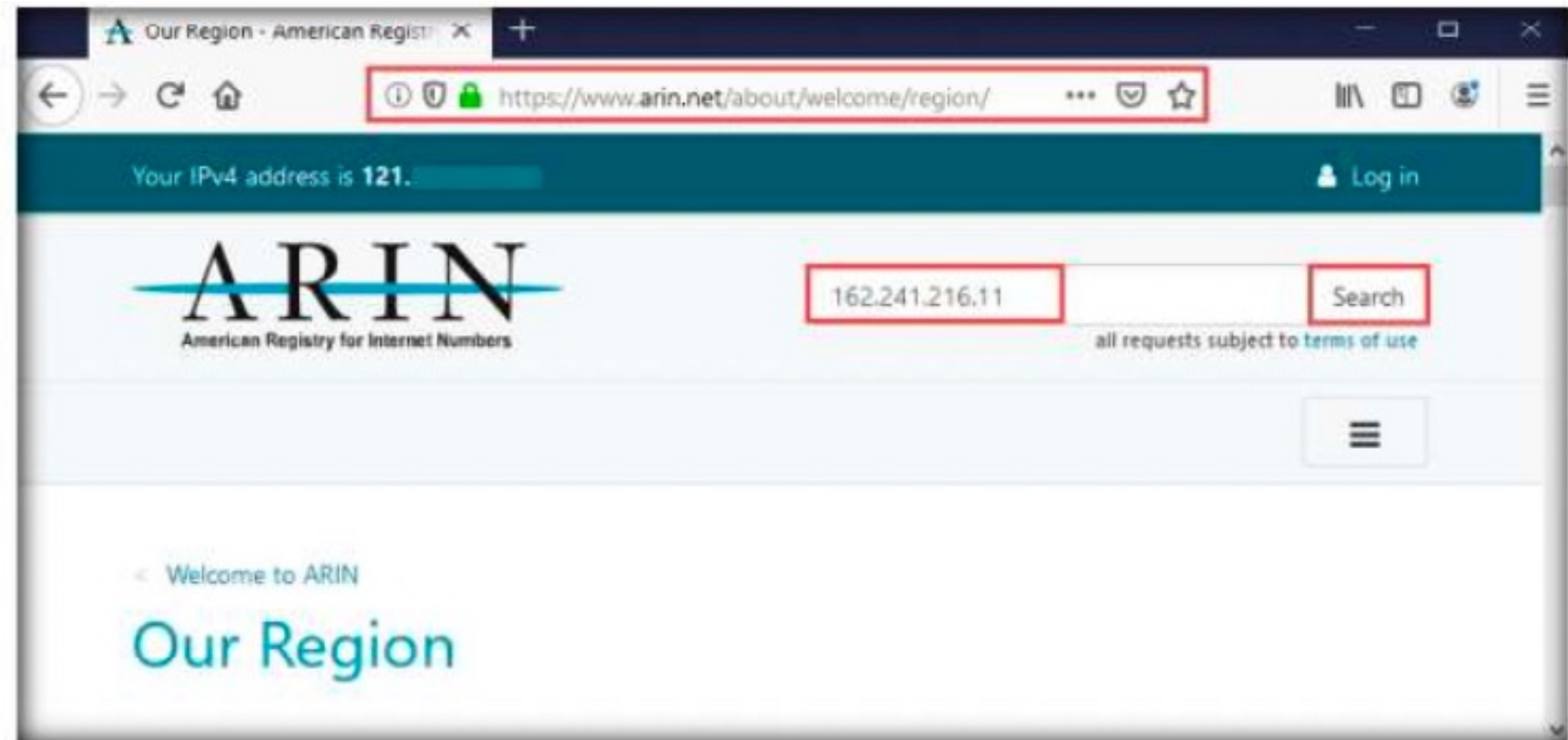
7

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.



7

Network Footprinting

7.1

Locate the Network Range

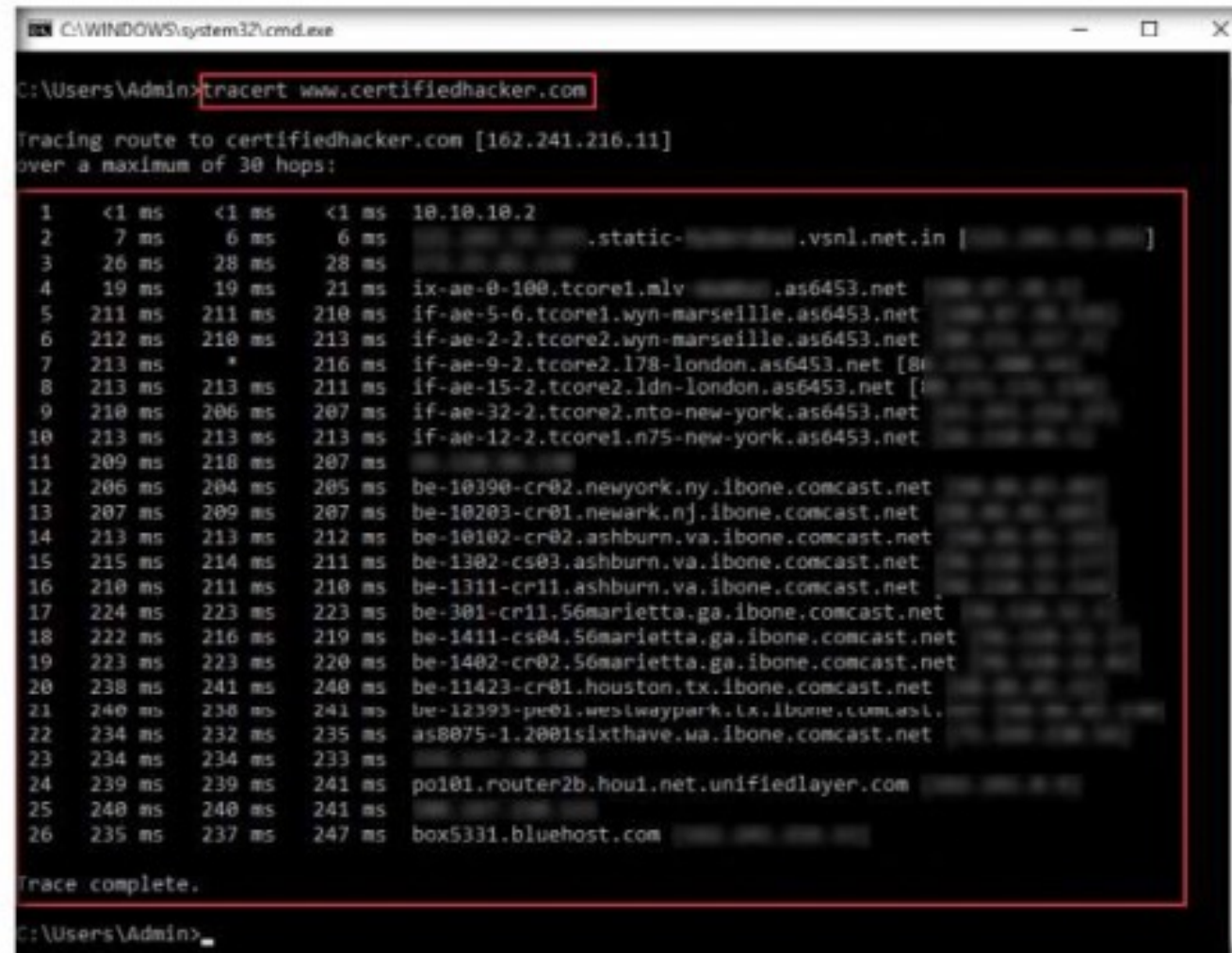
3. You will get the information about the network range along with the other information such as network type, registration information, etc.

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.

The screenshot shows the ARIN Whois/RDAP website interface. The search bar contains the IP address 162.241.216.11, and the search button is highlighted. Below the search bar, the results for the network 162.241.216.11 are displayed. The network is identified as NET-162-240-0-0-1. The source registry is ARIN. The net range is 162.240.0.0 - 162.241.255.255, which is highlighted with a red box. Other details include 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 17:57:53 GMT), and Last Changed (Thu, 22 Aug 2013 17:57:54 GMT).

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 17:57:53 GMT (Thu Aug 22 2013 local time)
Last Changed	Thu, 22 Aug 2013 17:57:54 GMT (Thu Aug 22 2013 local time)

1. 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.



```
CA\WINDOWS\system32\cmd.exe

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

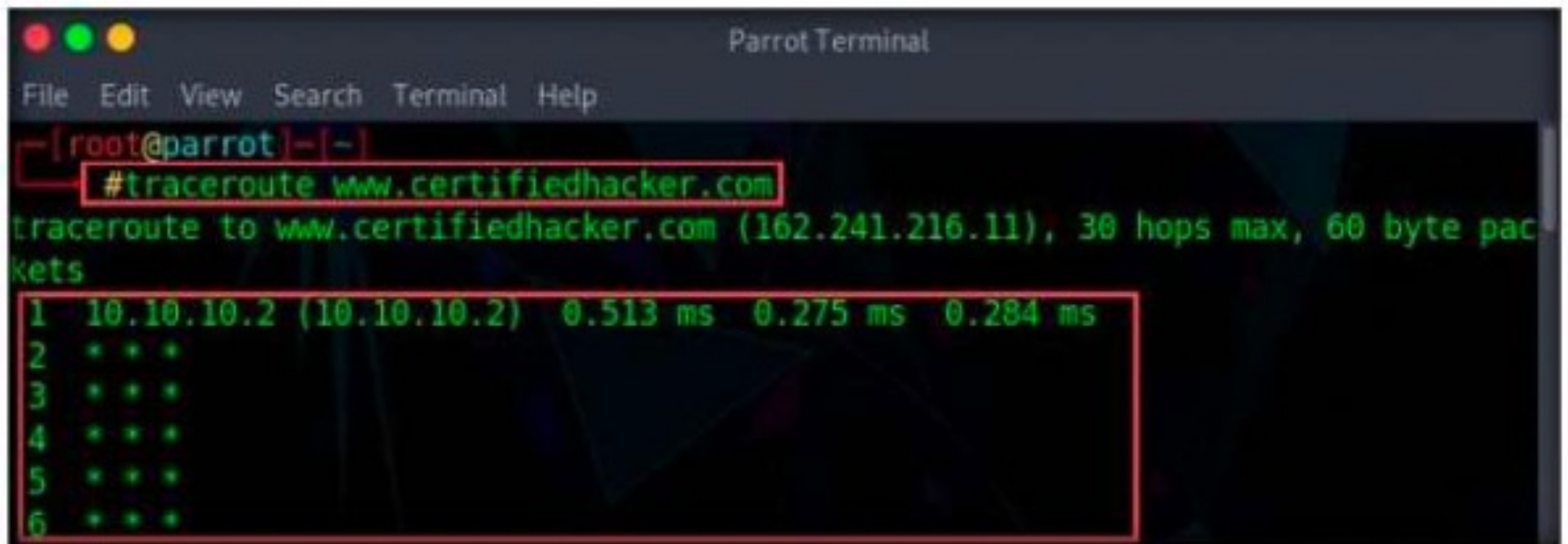
Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    10.10.10.2
  1  7 ms     6 ms     6 ms     [REDACTED].static-[REDACTED].vsnl.net.in [REDACTED]
  2  26 ms    28 ms    28 ms    [REDACTED]
  3  19 ms    19 ms    21 ms    ix-ae-0-100.tcore1.mlv[REDACTED].as6453.net [REDACTED]
  4  211 ms   211 ms   210 ms   if-ae-5-6.tcore1.wyn-marseille.as6453.net [REDACTED]
  5  212 ms   210 ms   213 ms   if-ae-2-2.tcore2.wyn-marseille.as6453.net [REDACTED]
  6  213 ms   *        216 ms   if-ae-9-2.tcore2.l78-london.as6453.net [REDACTED]
  7  213 ms   213 ms   211 ms   if-ae-15-2.tcore2.ldn-london.as6453.net [REDACTED]
  8  210 ms   206 ms   207 ms   if-ae-32-2.tcore2.nto-new-york.as6453.net [REDACTED]
  9  213 ms   213 ms   213 ms   if-ae-12-2.tcore1.n75-new-york.as6453.net [REDACTED]
 10  209 ms   218 ms   207 ms   [REDACTED]
 11  206 ms   204 ms   205 ms   be-10390-cr02.newyork.ny.ibone.comcast.net [REDACTED]
 12  207 ms   209 ms   207 ms   be-10203-cr01.newark.nj.ibone.comcast.net [REDACTED]
 13  213 ms   213 ms   212 ms   be-10102-cr02.ashburn.va.ibone.comcast.net [REDACTED]
 14  215 ms   214 ms   211 ms   be-1302-cs03.ashburn.va.ibone.comcast.net [REDACTED]
 15  210 ms   211 ms   210 ms   be-1311-cr11.ashburn.va.ibone.comcast.net [REDACTED]
 16  224 ms   223 ms   223 ms   be-301-cr11.56marietta.ga.ibone.comcast.net [REDACTED]
 17  222 ms   216 ms   219 ms   be-1411-cs04.56marietta.ga.ibone.comcast.net [REDACTED]
 18  223 ms   223 ms   220 ms   be-1402-cr02.56marietta.ga.ibone.comcast.net [REDACTED]
 19  238 ms   241 ms   240 ms   be-11423-cr01.houston.tx.ibone.comcast.net [REDACTED]
 20  240 ms   238 ms   241 ms   be-12393-pe01.westwaypark.tx.ibone.comcast.net [REDACTED]
 21  234 ms   232 ms   235 ms   as8075-1.2001sixthave.wa.ibone.comcast.net [REDACTED]
 22  234 ms   234 ms   233 ms   [REDACTED]
 23  239 ms   239 ms   241 ms   po101.router2b.hou1.net.unifiedlayer.com [REDACTED]
 24  240 ms   240 ms   241 ms   [REDACTED]
 25  235 ms   237 ms   247 ms   box5331.bluehost.com [REDACTED]

Trace complete.

C:\Users\Admin>
```

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



The screenshot shows a Parrot Terminal window with a dark background and green text. The terminal title bar reads "Parrot Terminal". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The prompt is "[root@parrot]-[~]". The command "#tracert www.certifiedhacker.com" is entered and highlighted with a red box. Below it, the output of the command is displayed: "tracert to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets". This output line is also highlighted with a red box. The traceroute results are shown in a table-like format, with the first line highlighted by a red box:

Hop	IP Address	Source IP	RTT1	RTT2	RTT3
1	10.10.10.2	(10.10.10.2)	0.513 ms	0.275 ms	0.284 ms
2	*	*	*		
3	*	*	*		
4	*	*	*		
5	*	*	*		
6	*	*	*		

Perform
Footprinting
Through
Search Engines

Home
work

Implement an Email Footprinting

Home
work

Perform Footprinting Through Web Services

Hint: Web series 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>

Thank
You