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.

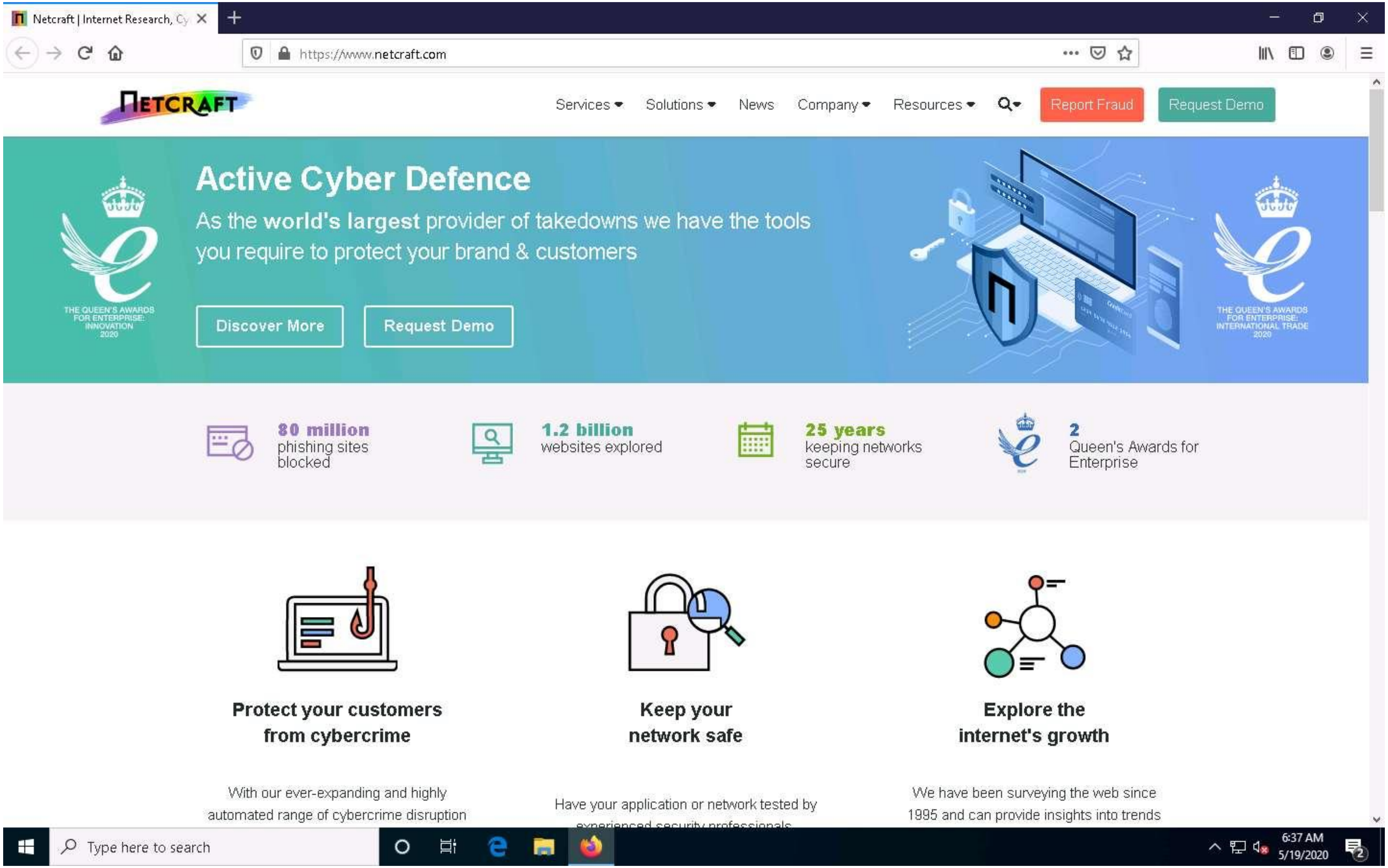
Here, we will extract the company's domains and sub-domains using the Netcraft web service.

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

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

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

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



Active Cyber Defence

As the **world's largest** provider of takedowns we have the tools you require to protect your brand & customers

80 million phishing sites blocked

1.2 billion websites explored

25 years keeping networks secure

2 Queen's Awards for Enterprise

Protect your customers from cybercrime

With our ever-expanding and highly automated range of cybercrime disruption

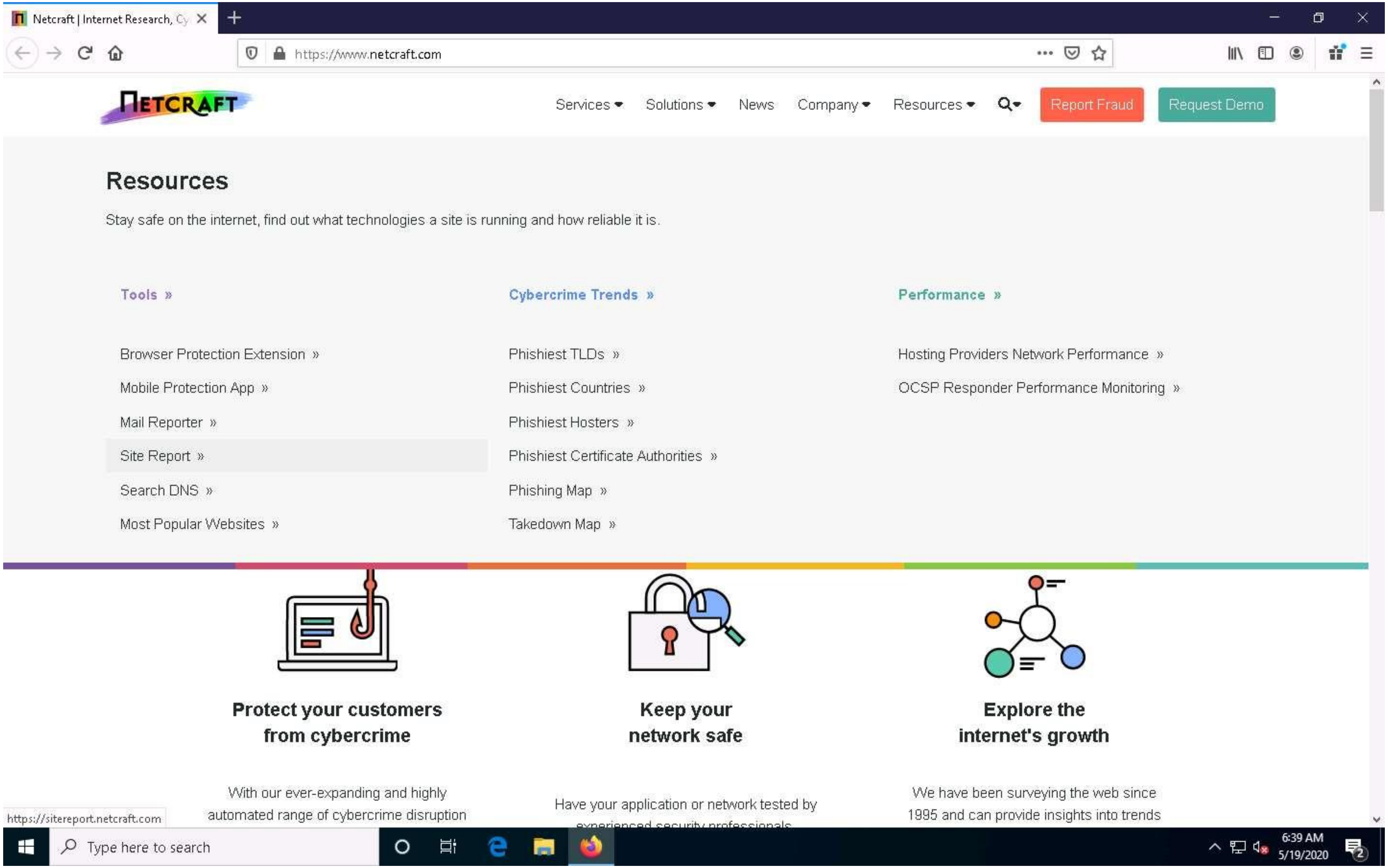
Keep your network safe

Have your application or network tested by experienced security professionals

Explore the internet's growth

We have been surveying the web since 1995 and can provide insights into trends

3. □ Click the **Resources** tab from the menu bar and click on the **Site Report** link under the Tools section.



Resources

Stay safe on the internet, find out what technologies a site is running and how reliable it is.

Tools »

Browser Protection Extension »

Mobile Protection App »

Mail Reporter »

Site Report »

Search DNS »

Most Popular Websites »

Cybercrime Trends »

Phishiest TLDs »

Phishiest Countries »

Phishiest Hosters »

Phishiest Certificate Authorities »

Phishing Map »

Takedown Map »

Performance »

Hosting Providers Network Performance »

OCSP Responder Performance Monitoring »

Protect your customers from cybercrime

With our ever-expanding and highly automated range of cybercrime disruption

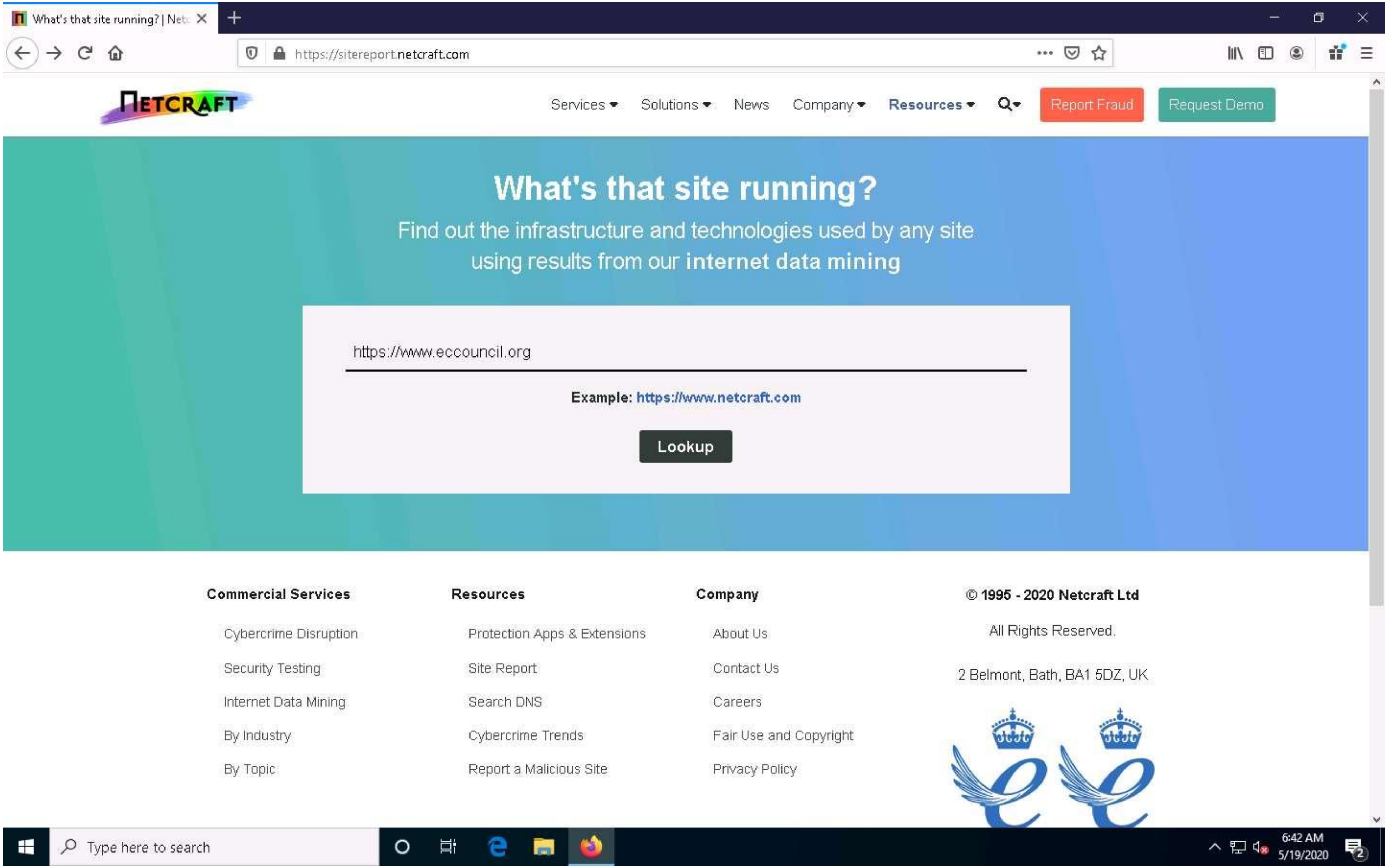
Keep your network safe

Have your application or network tested by experienced security professionals

Explore the internet's growth

We have been surveying the web since 1995 and can provide insights into trends

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 **Lookup** button, as shown in the screenshot.



What's that site running?

Find out the infrastructure and technologies used by any site using results from our **internet data mining**

https://www.eccouncil.org

Example: https://www.netcraft.com

Lookup

Commercial Services

Cybercrime Disruption

Security Testing

Internet Data Mining

By Industry

By Topic

Resources

Protection Apps & Extensions

Site Report

Search DNS

Cybercrime Trends

Report a Malicious Site

Company

About Us

Contact Us

Careers

Fair Use and Copyright

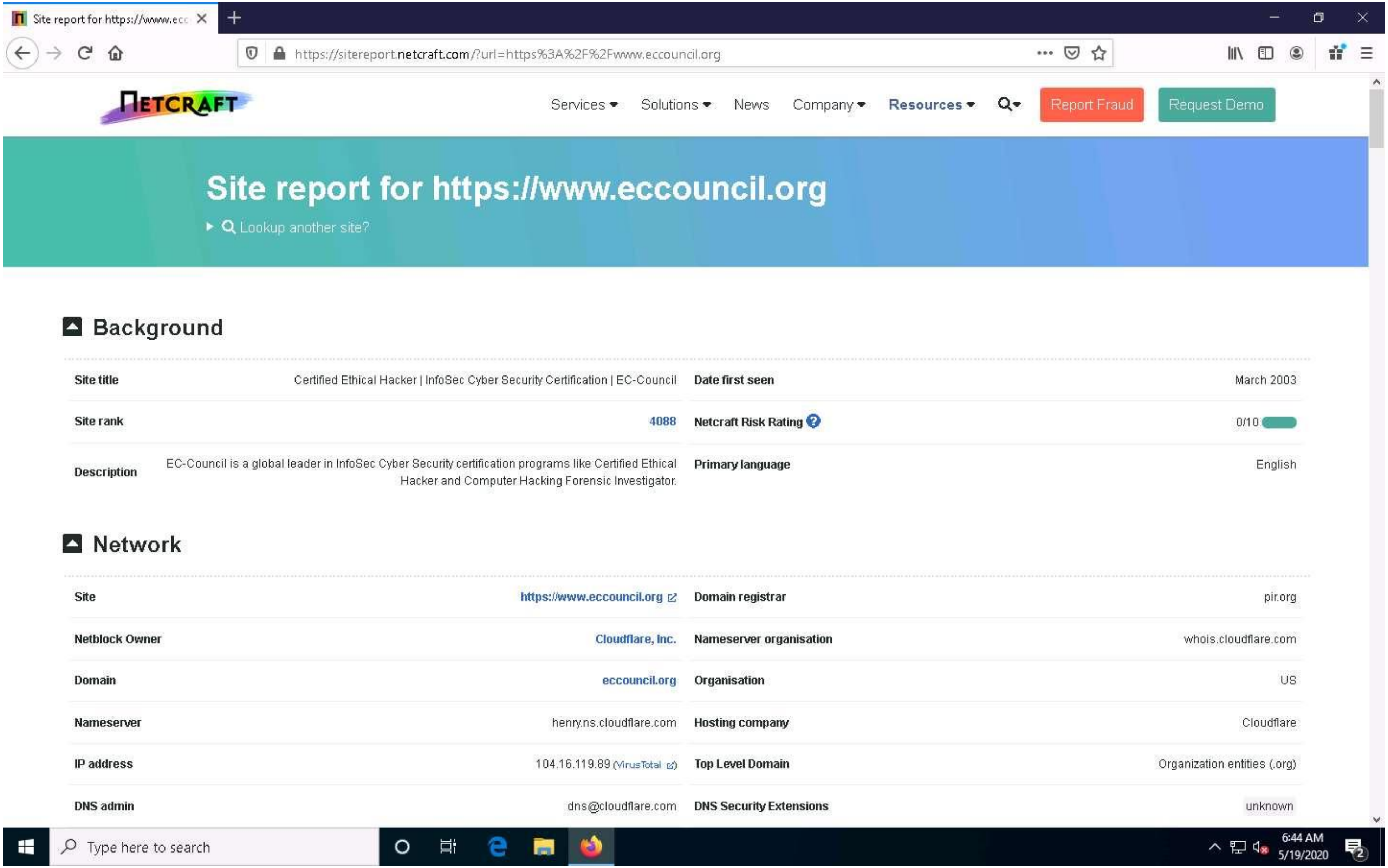
Privacy Policy

© 1995 - 2020 Netcraft Ltd

All Rights Reserved.

2 Belmont, Bath, BA1 5DZ, UK

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.



Site report for https://www.eccouncil.org

Lookup another site?

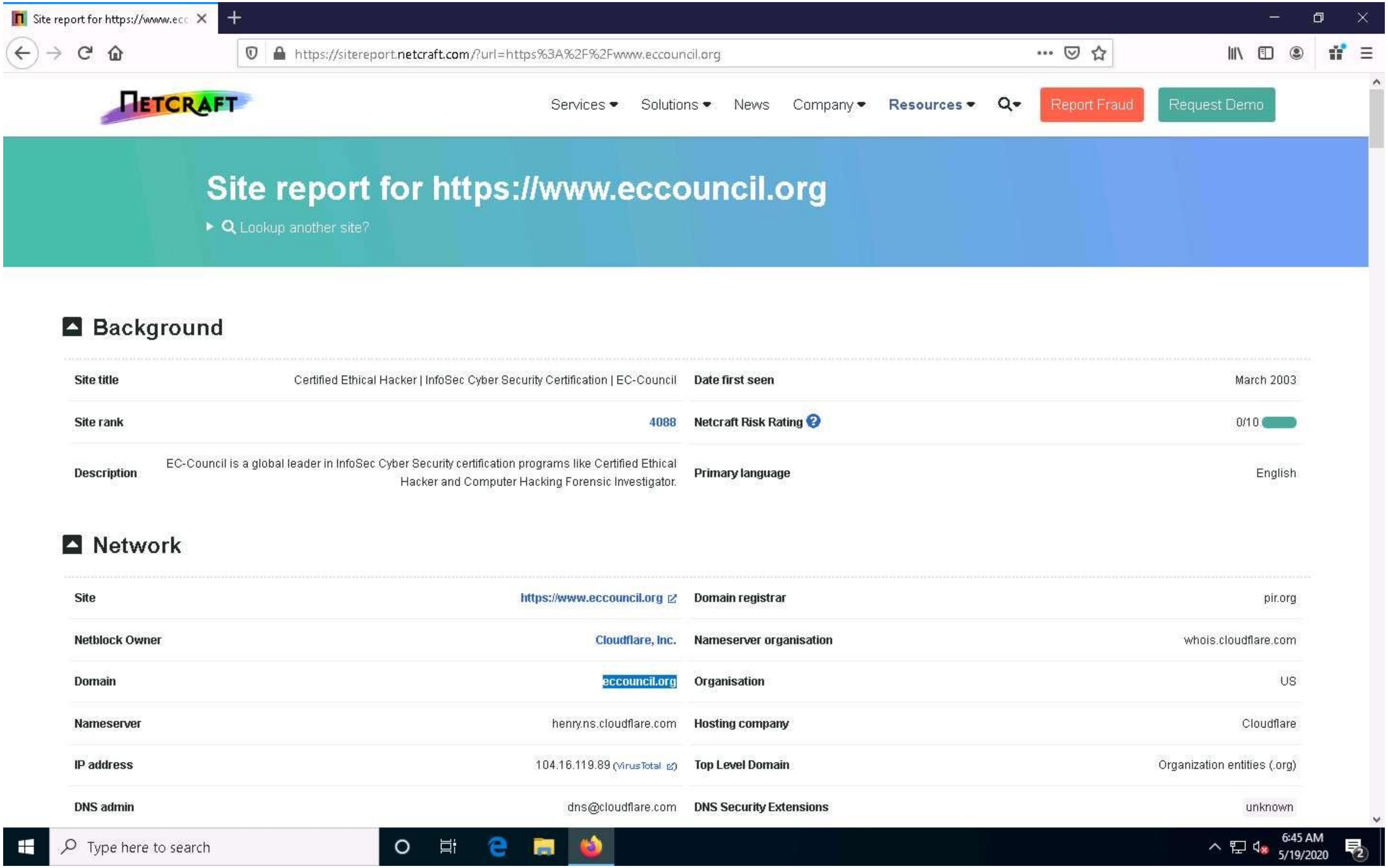
Background

Site title	Certified Ethical Hacker | InfoSec Cyber Security Certification | EC-Council	Date first seen	March 2003
Site rank	4088	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 registrar	pir.org
Netblock Owner	Cloudflare, Inc.	Nameserver organisation	whois.cloudflare.com
Domain	eccouncil.org	Organisation	US
Nameserver	henry.ns.cloudflare.com	Hosting company	Cloudflare
IP address	104.16.119.89 (VirusTotal)	Top Level Domain	Organization entities (.org)
DNS admin	dns@cloudflare.com	DNS Security Extensions	unknown

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.eccouncil.org

▸ Lookup another site?

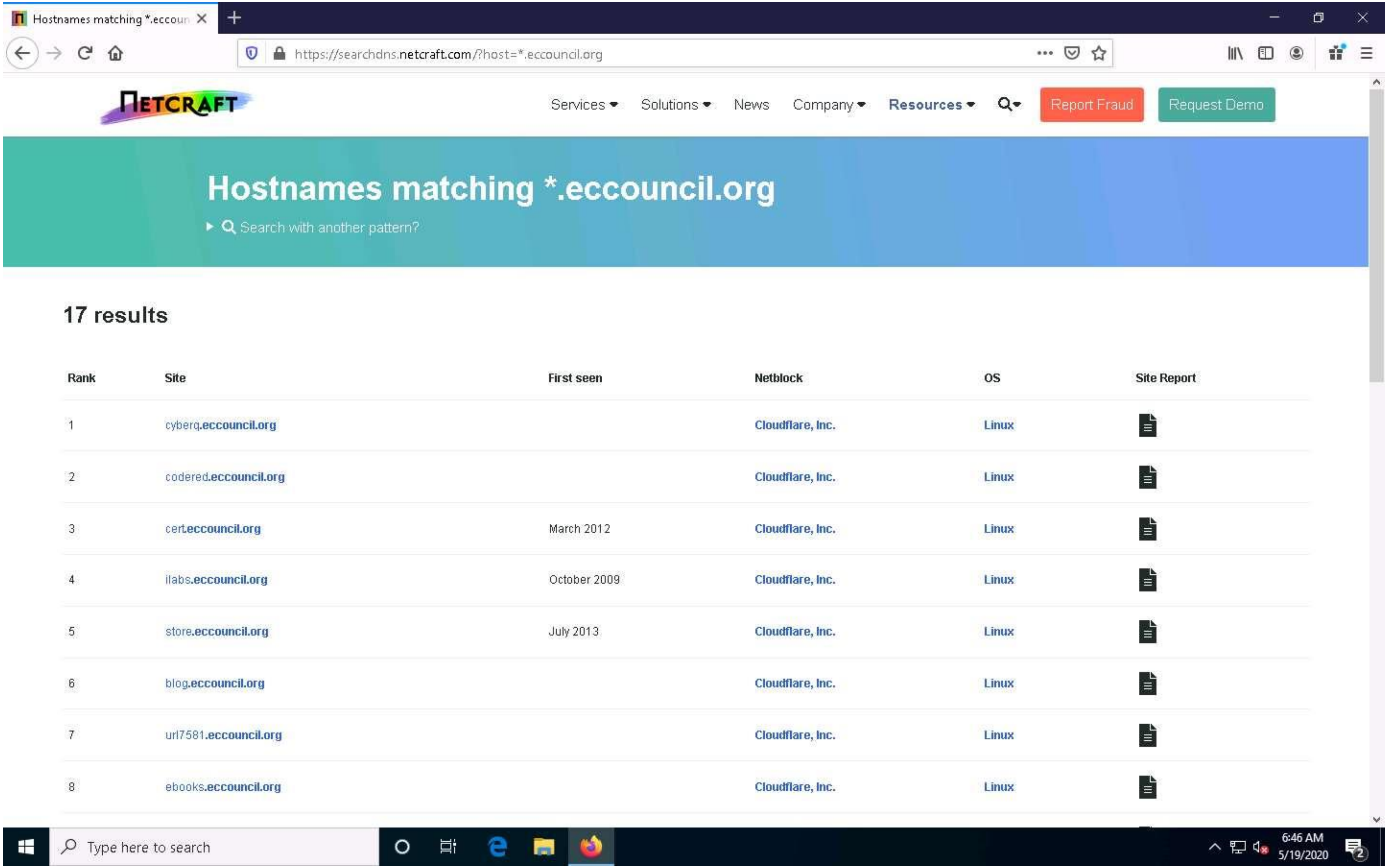
Background

Site title	Certified Ethical Hacker | InfoSec Cyber Security Certification | EC-Council	**Date first seen**	March 2003
Site rank	4088	**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 registrar**	pir.org
Netblock Owner	Cloudflare, Inc.	**Nameserver organisation**	whois.cloudflare.com
Domain	eccouncil.org	**Organisation**	US
Nameserver	henry.ns.cloudflare.com	**Hosting company**	Cloudflare
IP address	104.16.119.89 (VirusTotal)	**Top Level Domain**	Organization entities (.org)
DNS admin	dns@cloudflare.com	**DNS Security Extensions**	unknown

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



https://searchdns.netcraft.com/?host=*.eccouncil.org

Hostnames matching *.eccouncil.org

17 results

Rank	Site	First seen	Netblock	OS	Site Report
1	cyberq.eccouncil.org		Cloudflare, Inc.	Linux	
2	codered.eccouncil.org		Cloudflare, Inc.	Linux	
3	cert.eccouncil.org	March 2012	Cloudflare, Inc.	Linux	
4	ilabs.eccouncil.org	October 2009	Cloudflare, Inc.	Linux	
5	store.eccouncil.org	July 2013	Cloudflare, Inc.	Linux	
6	blog.eccouncil.org		Cloudflare, Inc.	Linux	
7	url7581.eccouncil.org		Cloudflare, Inc.	Linux	
8	ebooks.eccouncil.org		Cloudflare, Inc.	Linux	

8. □ This concludes the demonstration of finding the company's domains and sub-domains using the Netcraft tool.

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.

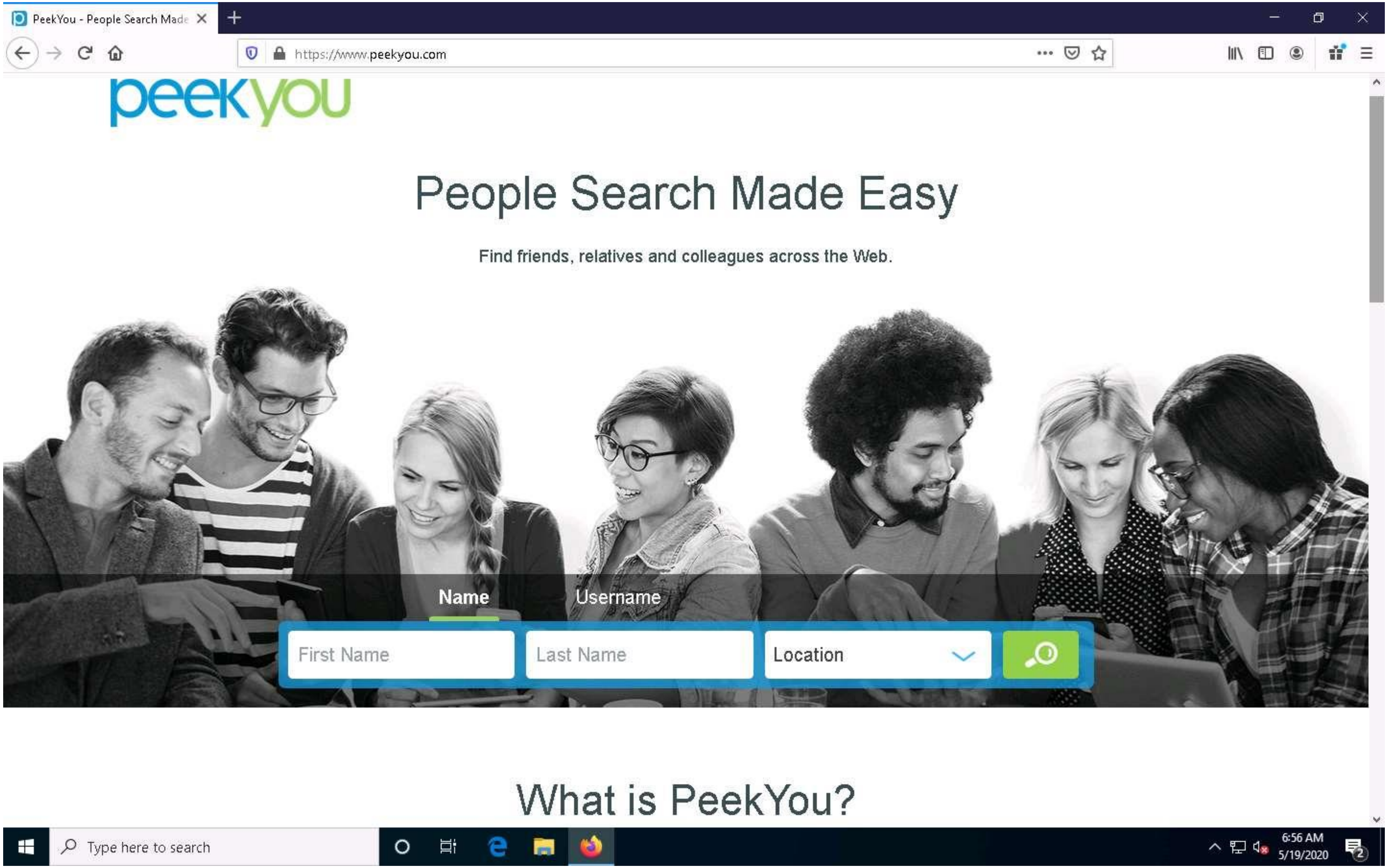
Here, we will gather information about a person from the target organization by performing people search using the PeekYou online people search service.

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

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

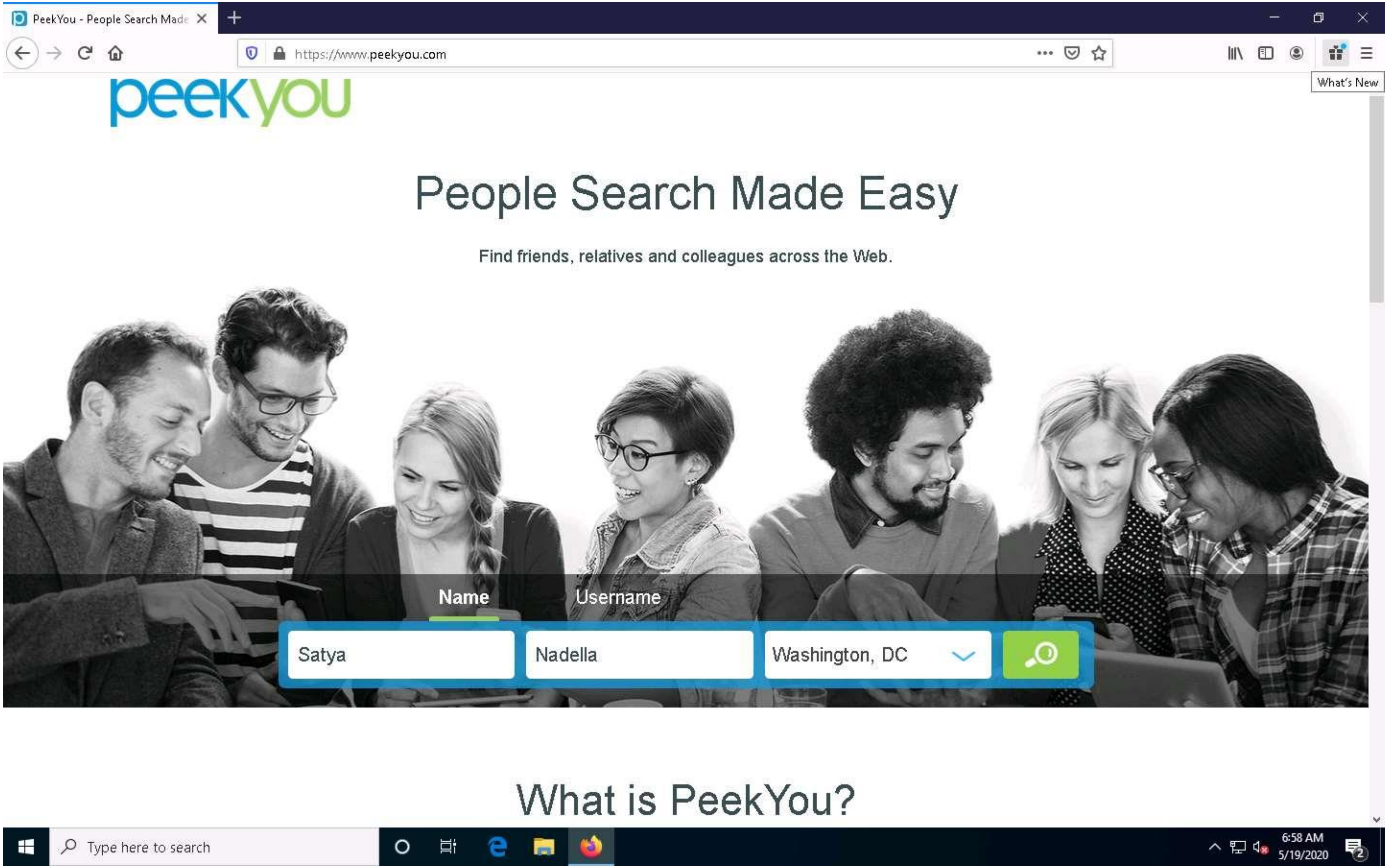
2. □ **PeekYou** page appears, as shown in the screenshot.

   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.

The list of location might differ in your lab environment.



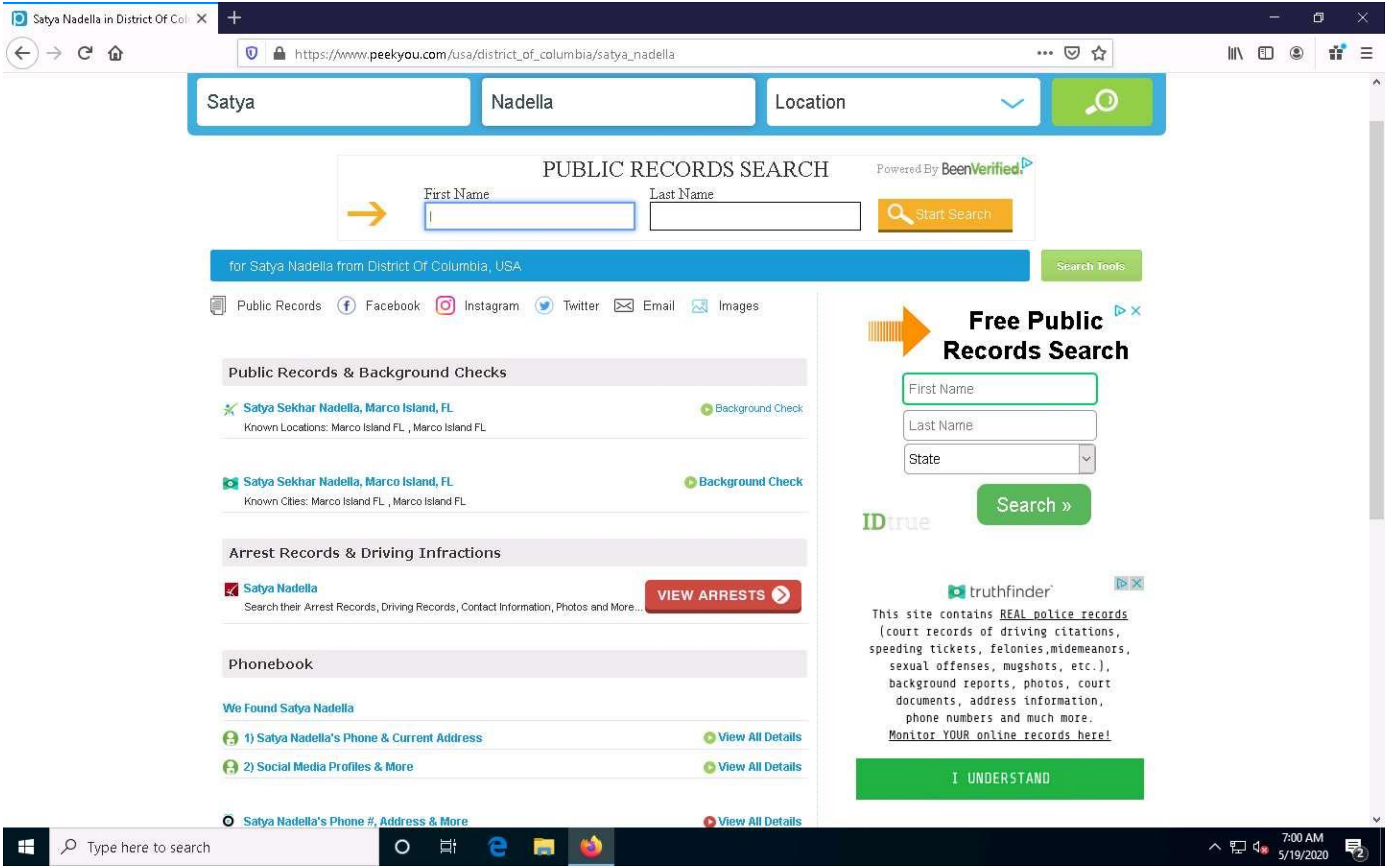
Satya

Nadella

Washington, DC

What is PeekYou?

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



Satya Nadella in District Of Col
https://www.peekyou.com/usa/district_of_columbia/satya_nadella
Satya
Nadella
Location

PUBLIC RECORDS SEARCH

Powered By BeenVerified

First Name

Last Name

Start Search

for Satya Nadella from District Of Columbia, USA

Search Tools
Public Records
Facebook
Instagram
Twitter
Email
Images

Public Records & Background Checks

Satya Sekhar Nadella, Marco Island, FL — Background Check

Known Locations: Marco Island FL , Marco Island FL

Satya Sekhar Nadella, Marco Island, FL — Background Check

Known Cities: Marco Island FL , Marco Island FL

Arrest Records & Driving Infractions

Satya Nadella — VIEW ARRESTS

Search their Arrest Records, Driving Records, Contact Information, Photos and More...

Phonebook

We Found Satya Nadella

1) Satya Nadella's Phone & Current Address — View All Details

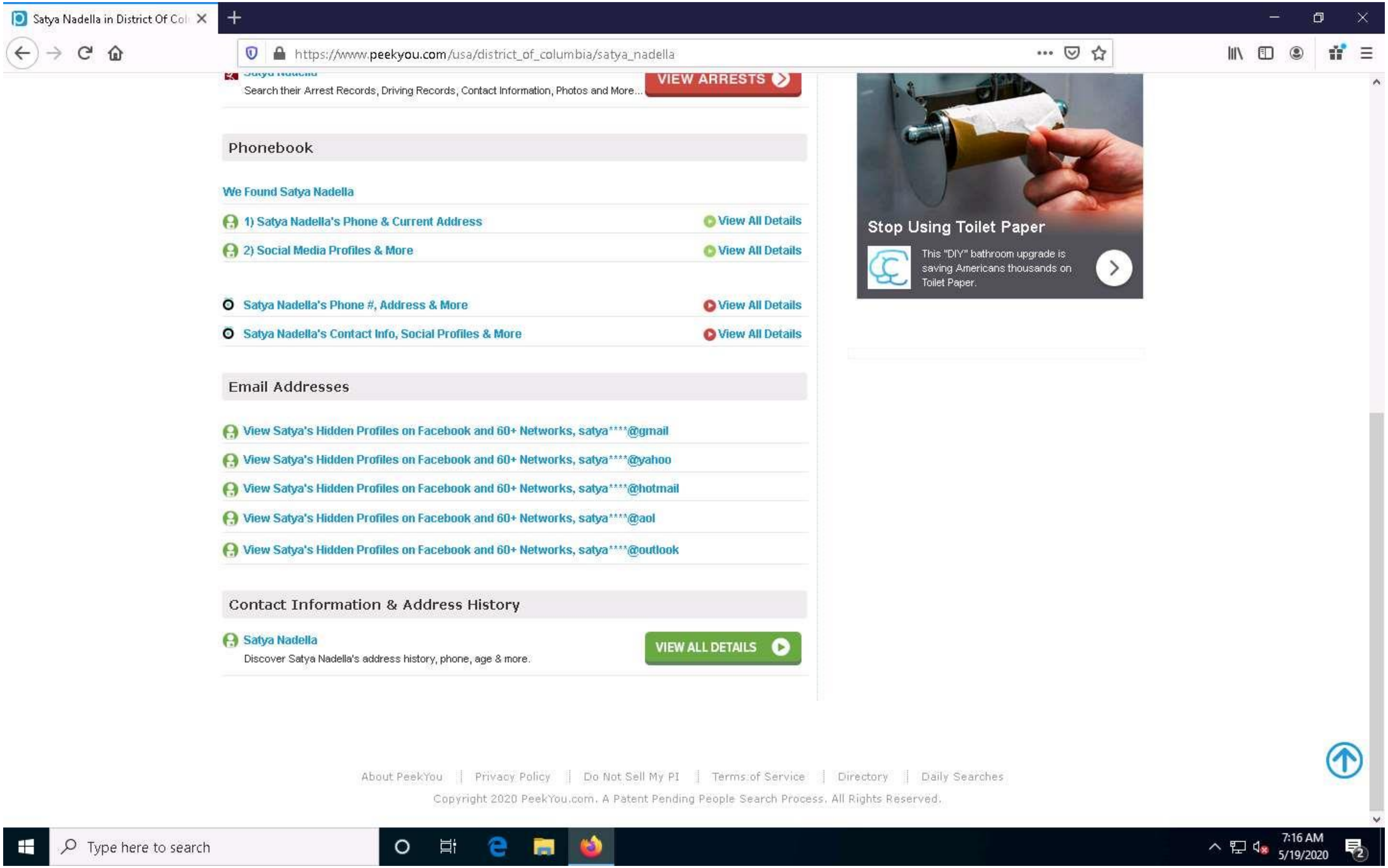
2) Social Media Profiles & More — View All Details

Satya Nadella's Phone #, Address & More — View All Details

5. □ You can further click on the appropriate result to view the detailed information about the target person to see a detailed information about the target person.

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 target.

6. □ Scroll down to view the entire information about the target person.



Satya Nadella in District Of Col
https://www.peekyou.com/usa/district_of_columbia/satya_nadella
VIEW ARRESTS

Search their Arrest Records, Driving Records, Contact Information, Photos and More...

Phonebook

We Found Satya Nadella

1) Satya Nadella's Phone & Current Address — View All Details

2) Social Media Profiles & More — View All Details

Satya Nadella's Phone #, Address & More — View All Details

Satya Nadella's Contact Info, Social Profiles & More — View All 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

Discover Satya Nadella's address history, phone, age & more.

VIEW ALL DETAILS
Stop Using Toilet Paper
This "DIY" bathroom upgrade is saving Americans thousands on Toilet Paper.
About PeekYou | Privacy Policy | Do Not Sell My PI | Terms of Service | Directory | Daily Searches
Copyright 2020 PeekYou.com. A Patent Pending People Search Process. All Rights Reserved.
Type here to search
7:16 AM
5/19/2020

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

---

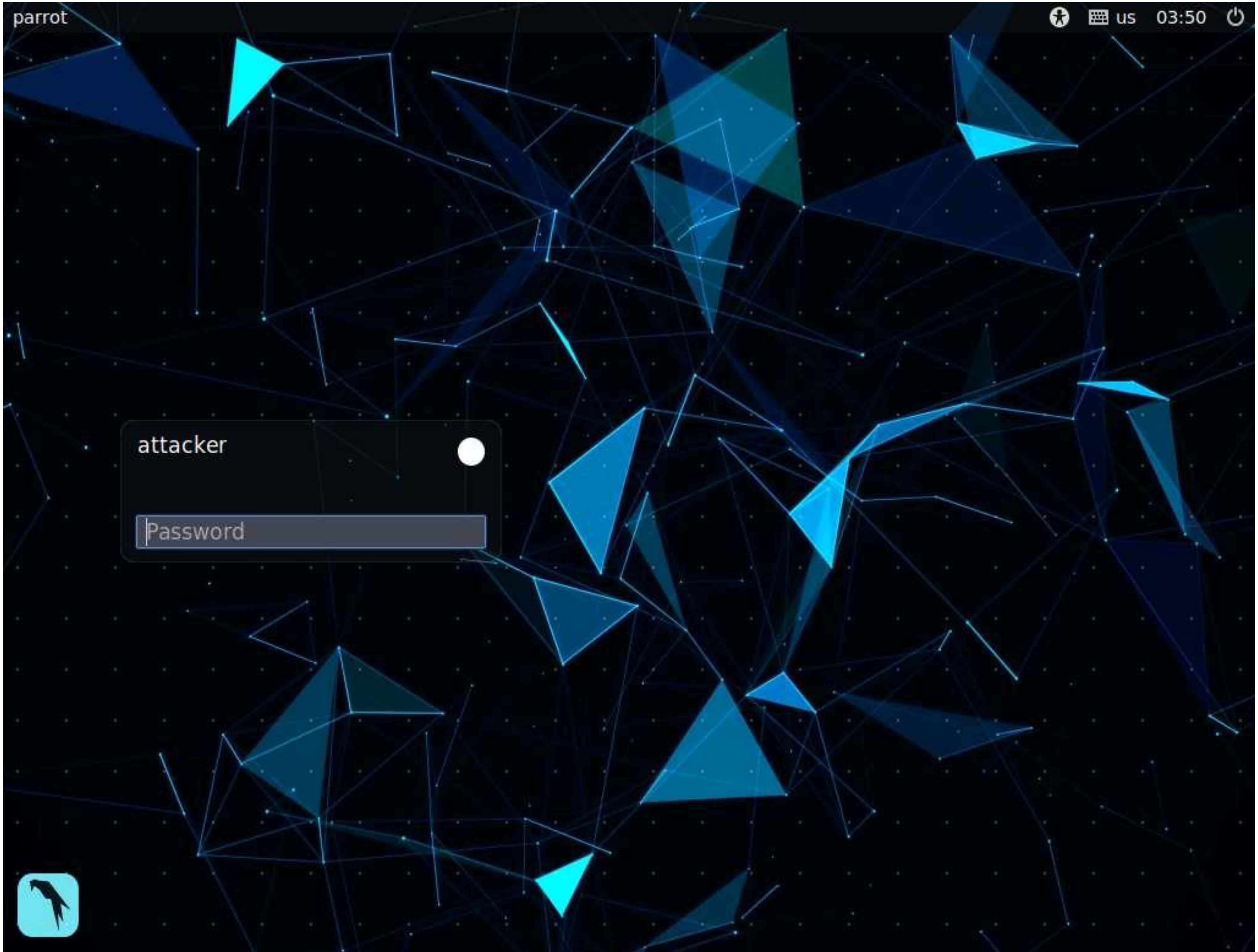
Task 3: Gather an Email List using theHarvester

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.

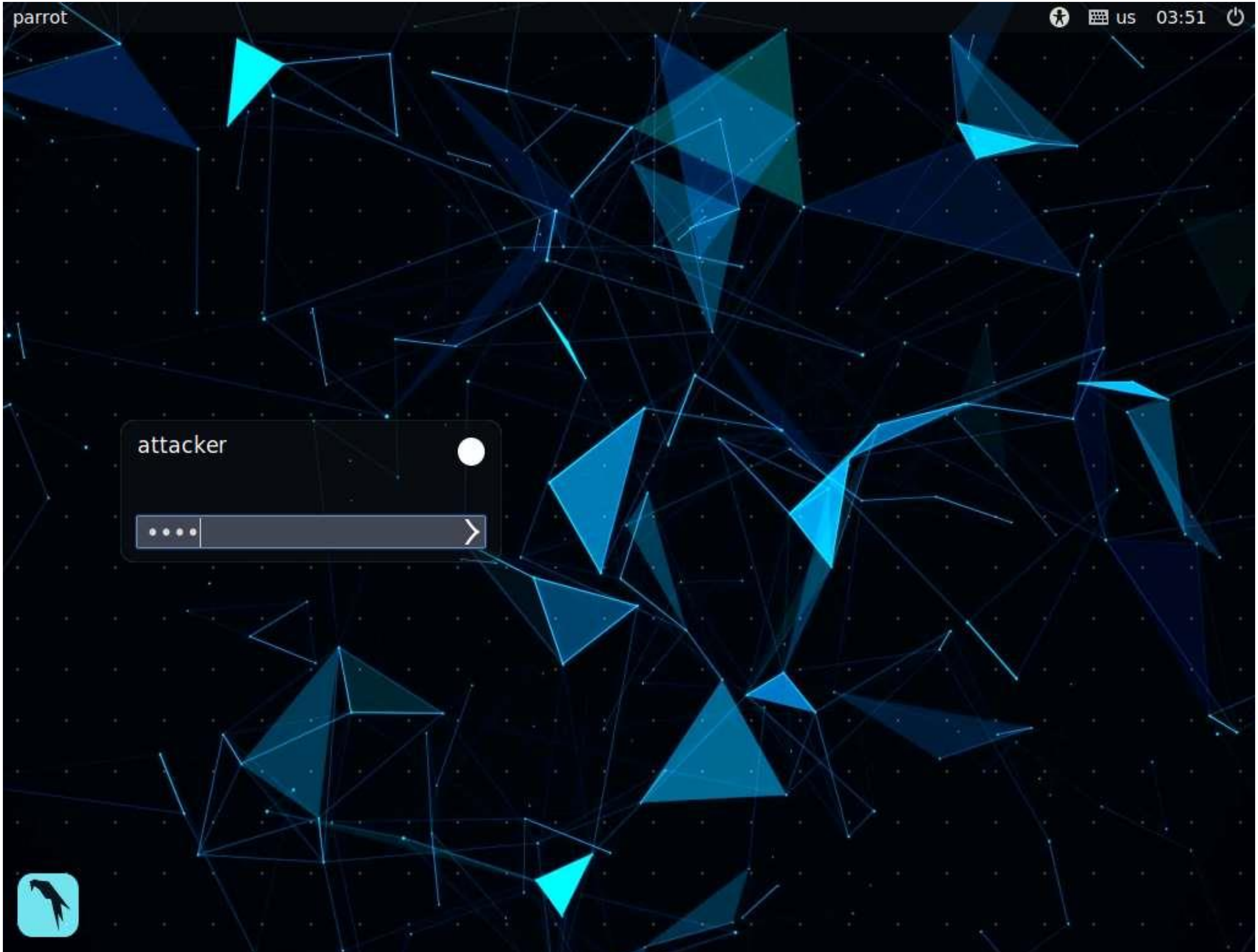
1. □ To launch **Parrot Security** machine, click Parrot Security.


parrot
us
03:50
attacker
Password

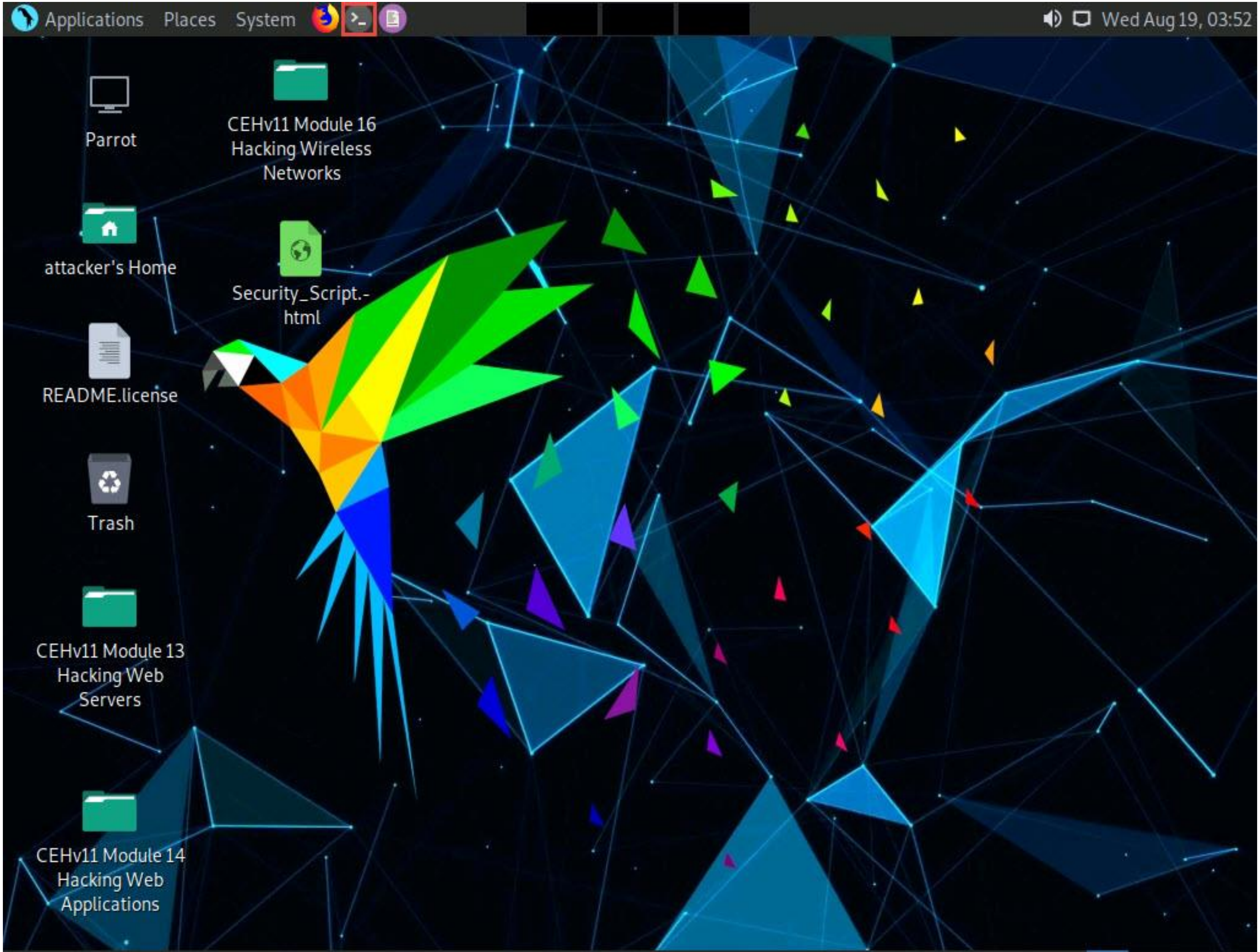
2. □ In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

   If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.


parrot
us
03:51
attacker
••••

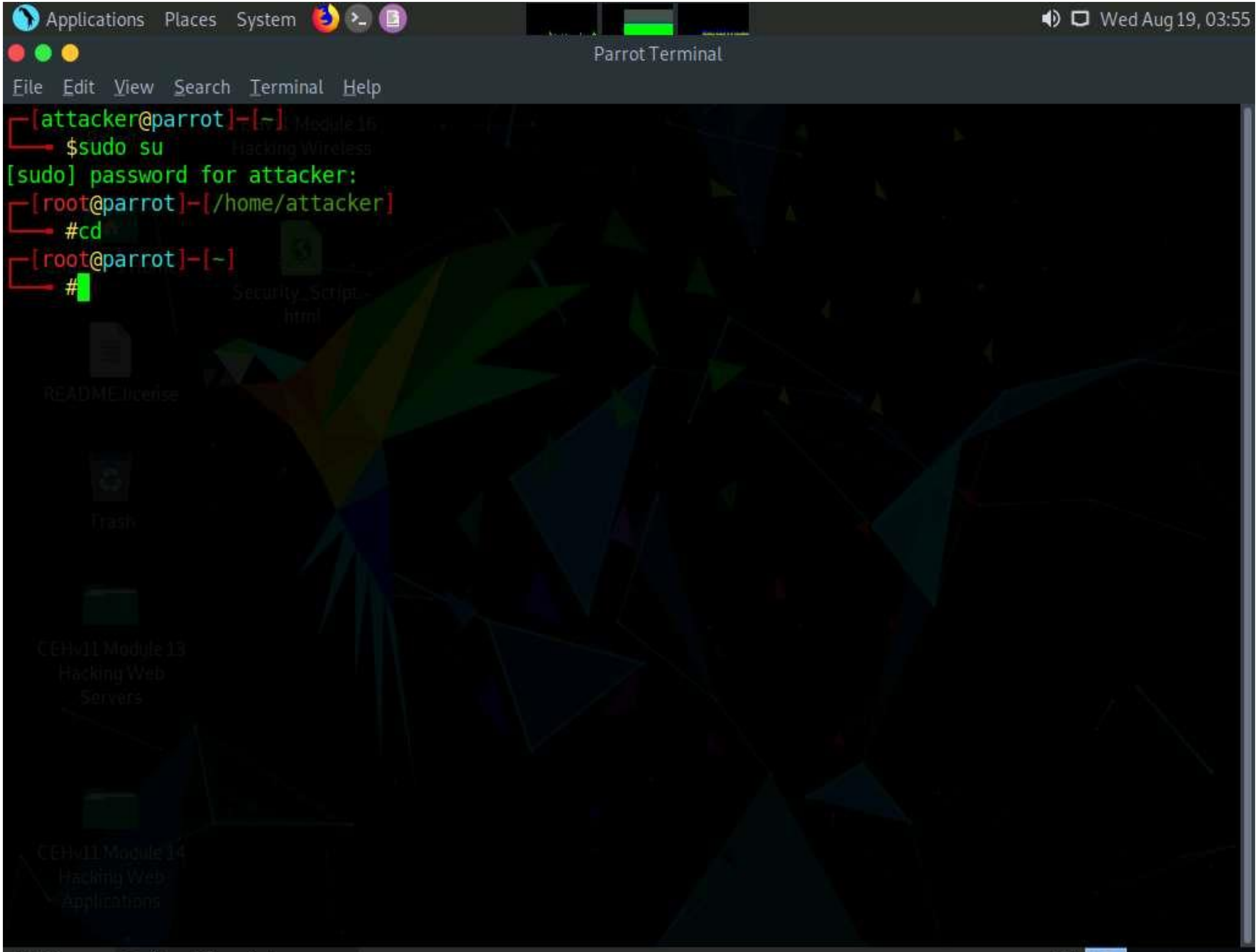
3. □ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.


Applications
Places
System
[redacted]
Wed Aug 19, 03:52
Parrot
CEHv11 Module 16 Hacking Wireless Networks
attacker's Home
Security_Script.-html
README.license
Trash
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications

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**.

The password that you type will not be visible.

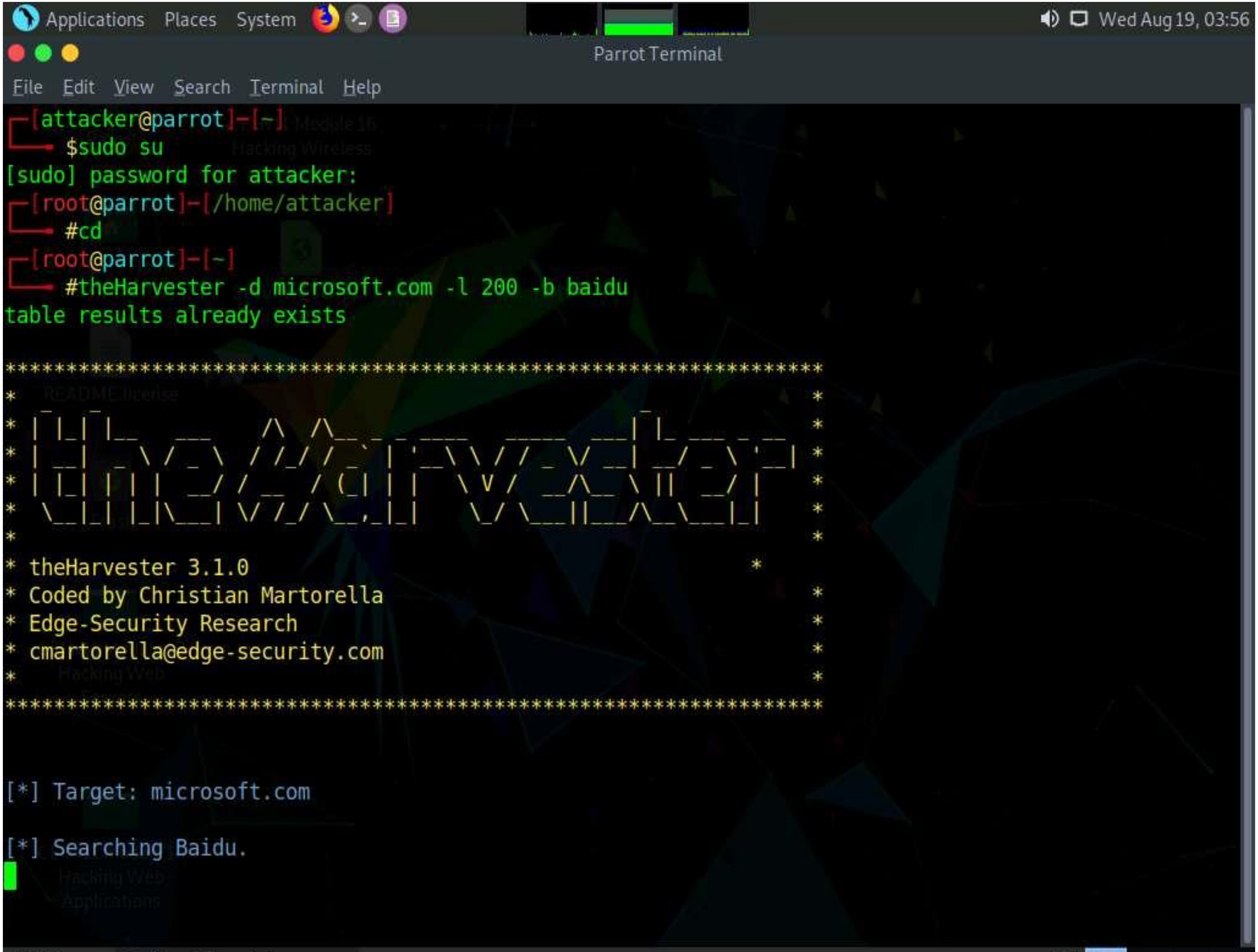
6. □ Now, type **cd** and press **Enter** to jump to the root directory.



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

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

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.

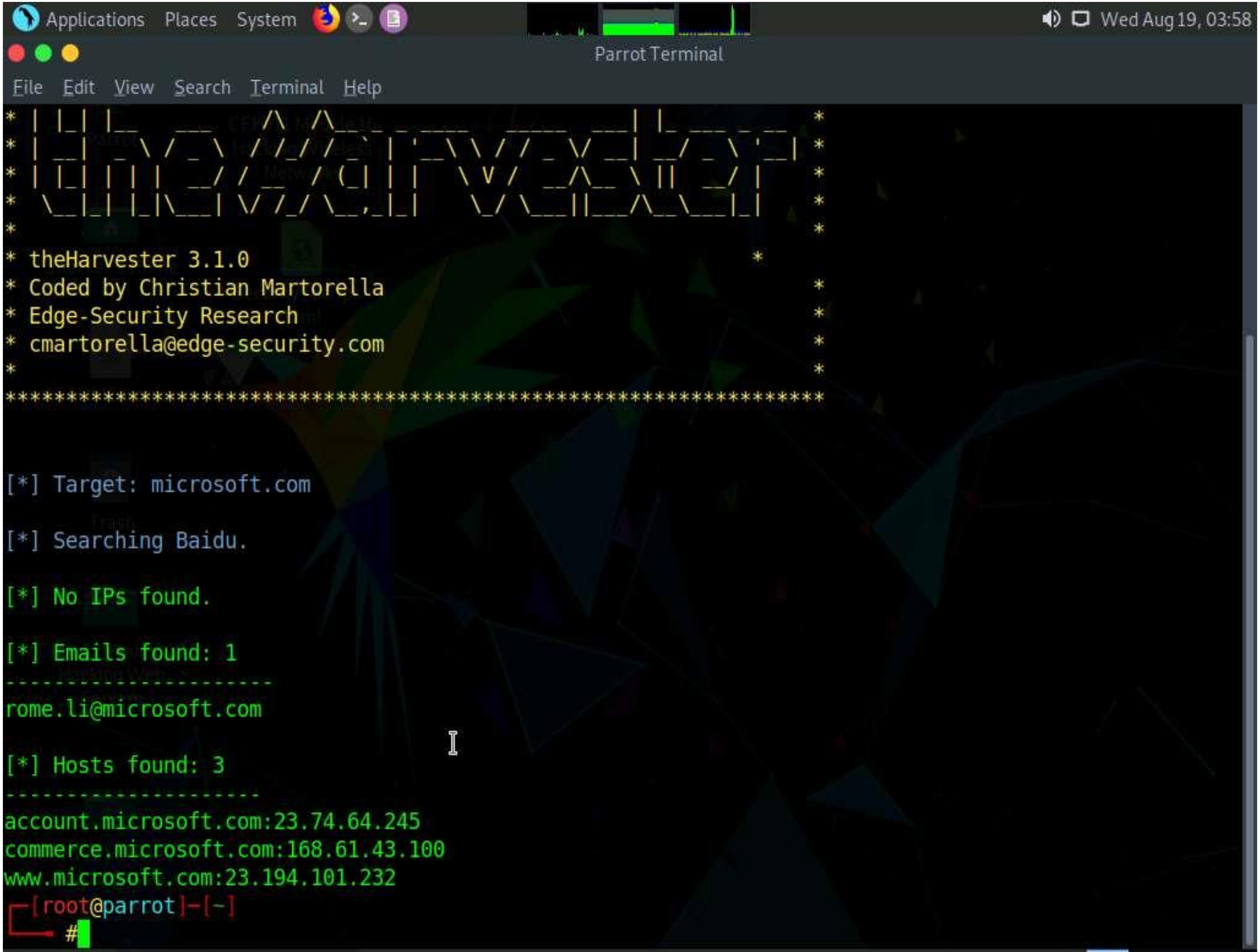


```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #theHarvester -d microsoft.com -l 200 -b baidu
table results already exists

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 3.1.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: microsoft.com

[*] Searching Baidu.
```

8. □ theHarvester starts extracting the details and displays them on the screen. 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 results might differ when you perform the lab.

Here, we specify Baidu search engine as a data source. You can specify different data sources (e.g., Baidu, bing, bingapi, dogpile, Google, GoogleCSE, Googleplus, Google-profiles, linkedin, pgp, twitter, vhost, virustotal, threatcrowd, crtsh, netcraft, yahoo, all) to gather information about the target.



```
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 3.1.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: microsoft.com

[*] Searching Baidu.

[*] No IPs found.

[*] Emails found: 1
----------------------
rome.li@microsoft.com

[*] Hosts found: 3
---------------------
account.microsoft.com:23.74.64.245
commerce.microsoft.com:168.61.43.100
www.microsoft.com:23.194.101.232
┌─[root@parrot]─[~]
└──╼ #
```

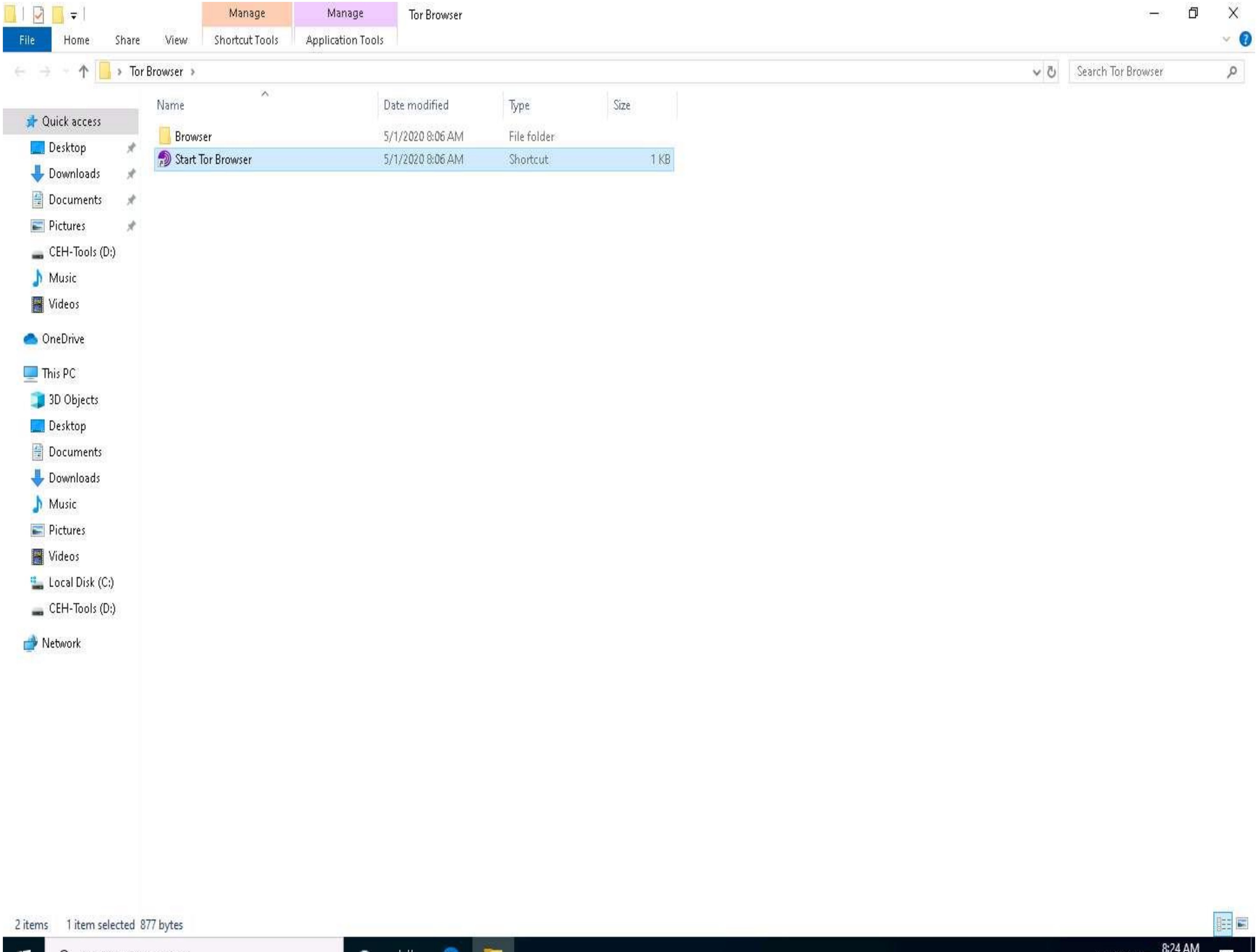
9. □ This concludes the demonstration of gathering an email list using theHarvester.
10. □ Close all open windows and document all the acquired information.

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 Windows 10 to switch to the **Windows 10** machine.
2. □ Open a **File Explorer**, navigate to **C:\Users\Admin\Desktop\Tor Browser**, and double-click **Start Tor Browser**.

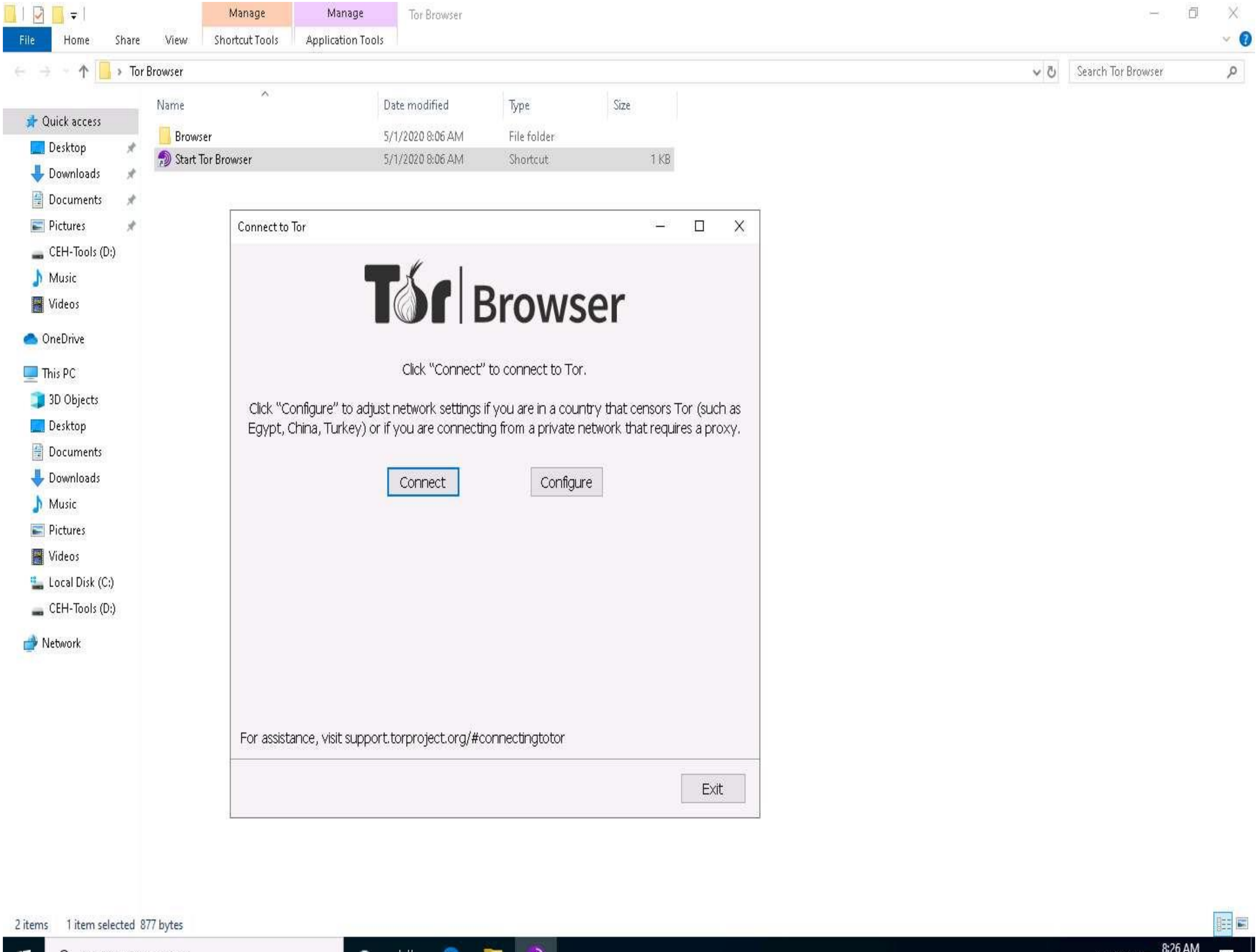


Name	Date modified	Type	Size
Browser	5/1/2020 8:06 AM	File folder	
Start Tor Browser	5/1/2020 8:06 AM	Shortcut	1 KB

2 items 1 item selected 877 bytes

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

If Tor is censored in your country or if you want to connect through Proxy, click the Configure button and continue.



Name	Date modified	Type	Size
Browser	5/1/2020 8:06 AM	File folder	
Start Tor Browser	5/1/2020 8:06 AM	Shortcut	1 KB

Connect to Tor

Tor Browser

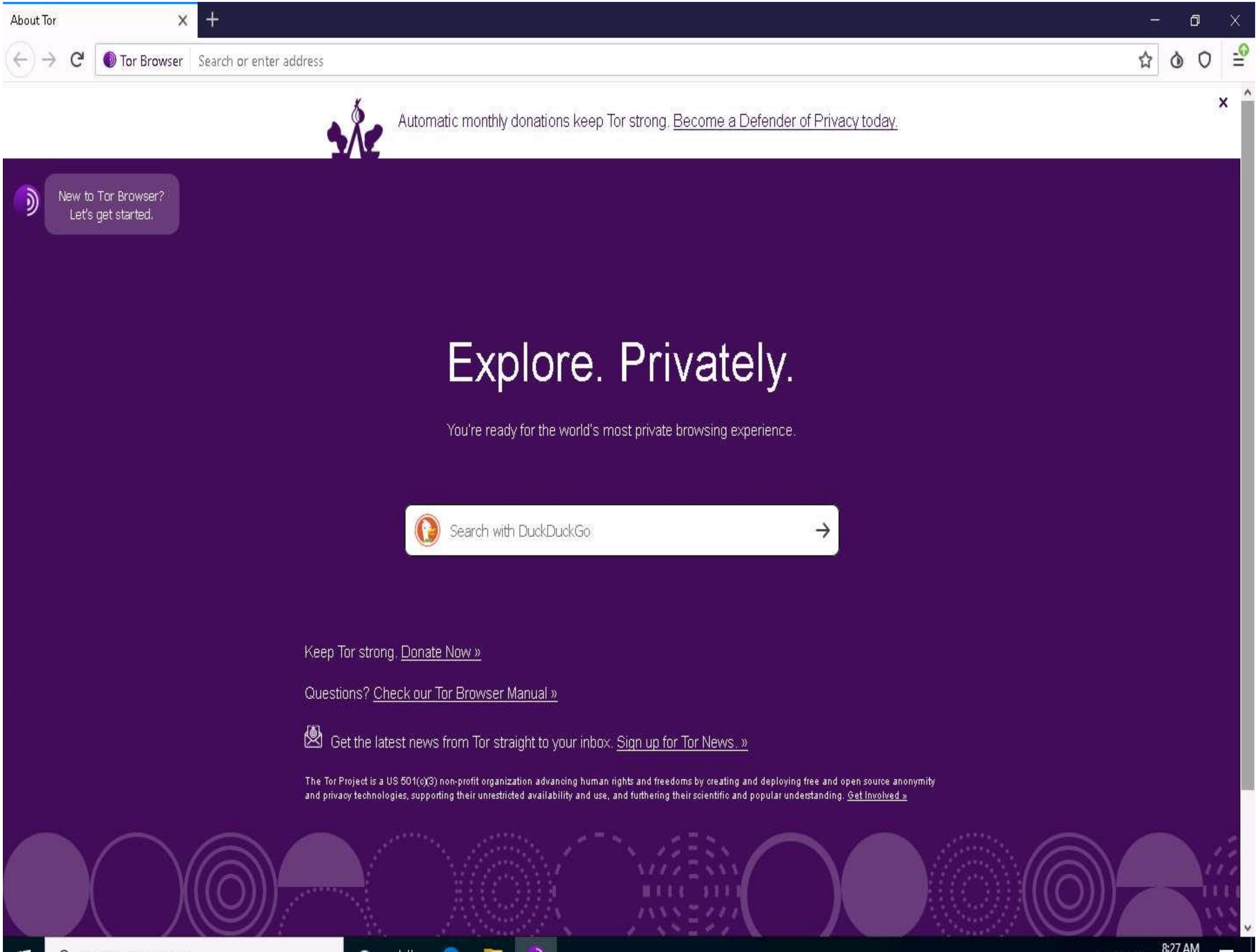
Click "Connect" to connect to Tor.

Click "Configure" to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.

For assistance, visit support.torproject.org/#connectingtotor

2 items 1 item selected 877 bytes

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.



Automatic monthly donations keep Tor strong. Become a Defender of Privacy today.

Explore. Privately.

You're ready for the world's most private browsing experience.

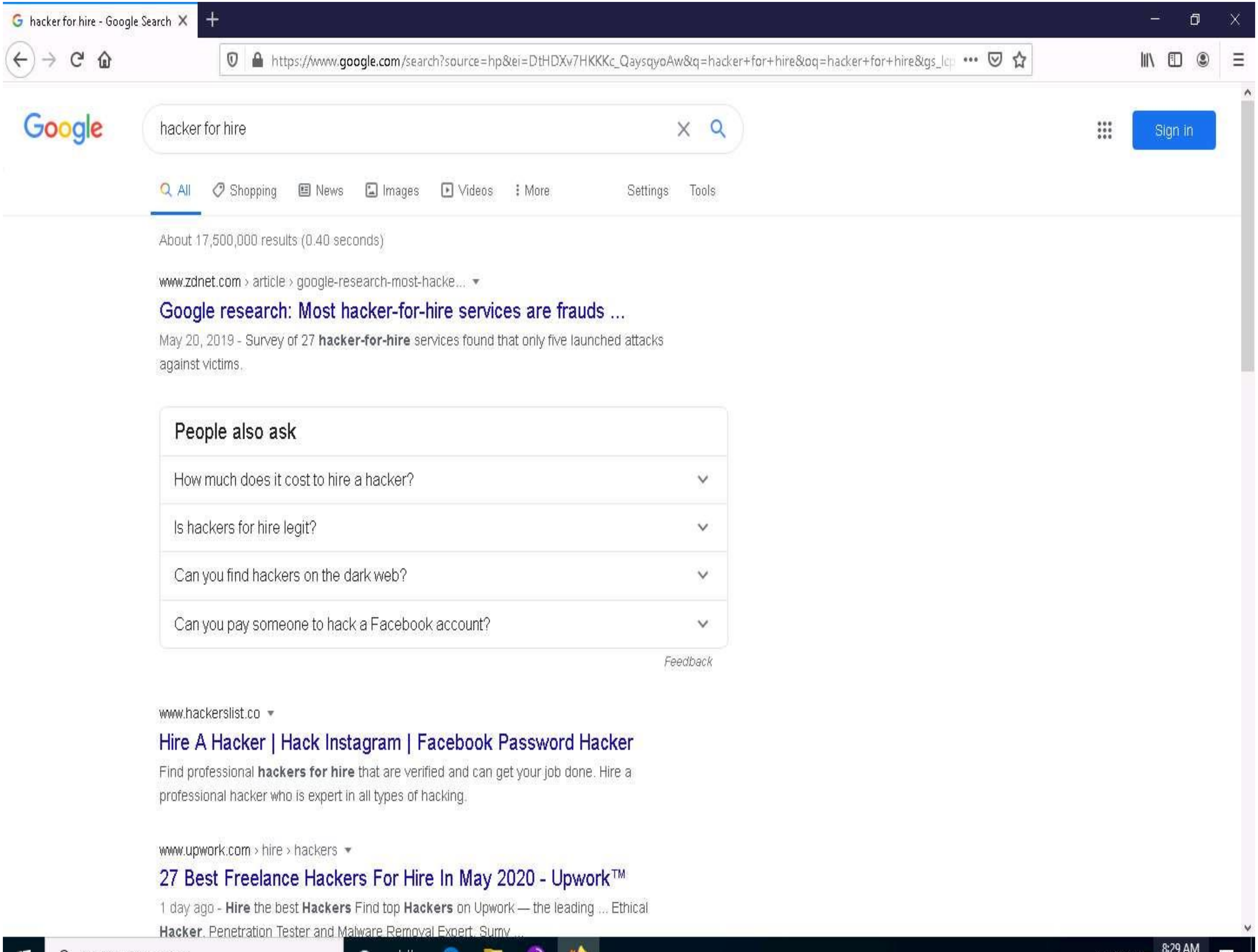
Keep Tor strong. Donate Now »

Questions? Check our Tor Browser Manual »

Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

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.


hacker for hire - Google Search
https://www.google.com/search?source=hp&ei=DtHDXv7HKKKc_QaysqyoAw&q=hacker+for+hire&oq=hacker+for+hire&gs_lcp
Google
hacker for hire
Sign in
All
Shopping
News
Images
Videos
More
Settings
Tools
Feedback
8:29 AM

About 17,500,000 results (0.40 seconds)

www.zdnet.com › article › google-research-most-hacke... ▾

Google research: Most hacker-for-hire services are frauds ...

May 20, 2019 - Survey of 27 **hacker-for-hire** services found that only five launched attacks against victims.

People also ask

How much does it cost to hire a hacker?

Is hackers for hire legit?

Can you find hackers on the dark web?

Can you pay someone to hack a Facebook account?

www.hackerslist.co ▾

Hire A Hacker | Hack Instagram | Facebook Password Hacker

Find professional **hackers for hire** that are verified and can get your job done. Hire a professional hacker who is expert in all types of hacking.

www.upwork.com › hire › hackers ▾

27 Best Freelance Hackers For Hire In May 2020 - Upwork™

1 day ago - **Hire** the best **Hackers** Find top **Hackers** on Upwork — the leading ... Ethical **Hacker**, Penetration Tester and Malware Removal Expert. Sumy ...

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.

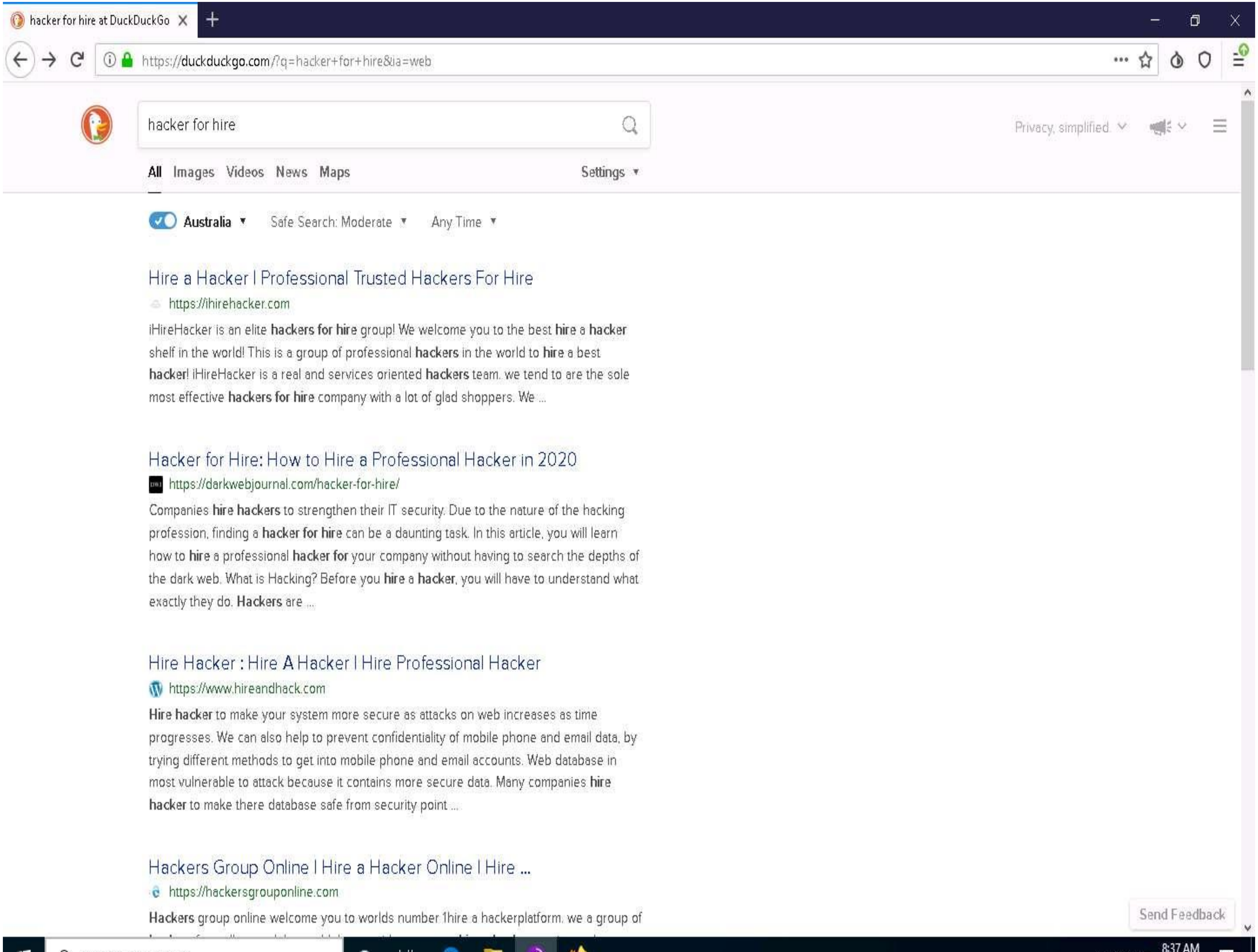
   Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.

8. □ Now, click on the toggle button that specifies the country of VPN/Proxy (here, by default, **Germany** is selected) and select a relevant country (here, **Australia**).

   Here, country might differ in your lab environment.

9. □ Search results for **hacker for hire** will be loaded, as shown in the screenshot. Click to open any of the search results (here, **https://ihirehacker.com**).

   The search results will be different in your lab environment.



Hire a Hacker l Professional Trusted Hackers For Hire

https://ihirehacker.com

iHireHacker is an elite **hackers for hire** group! We welcome you to the best **hire** a **hacker** shelf in the world! This is a group of professional **hackers** in the world to **hire** a best **hacker**! iHireHacker is a real and services oriented **hackers** team. we tend to are the sole most effective **hackers for hire** company with a lot of glad shoppers. We ...

Hacker for Hire: How to Hire a Professional Hacker in 2020

https://darkwebjournal.com/hacker-for-hire/

Companies **hire hackers** to strengthen their IT security. Due to the nature of the hacking profession, finding a **hacker for hire** can be a daunting task. In this article, you will learn how to **hire** a professional **hacker for** your company without having to search the depths of the dark web. What is Hacking? Before you **hire** a **hacker**, you will have to understand what exactly they do. **Hackers** are ...

Hire Hacker : Hire A Hacker l Hire Professional Hacker

https://www.hireandhack.com

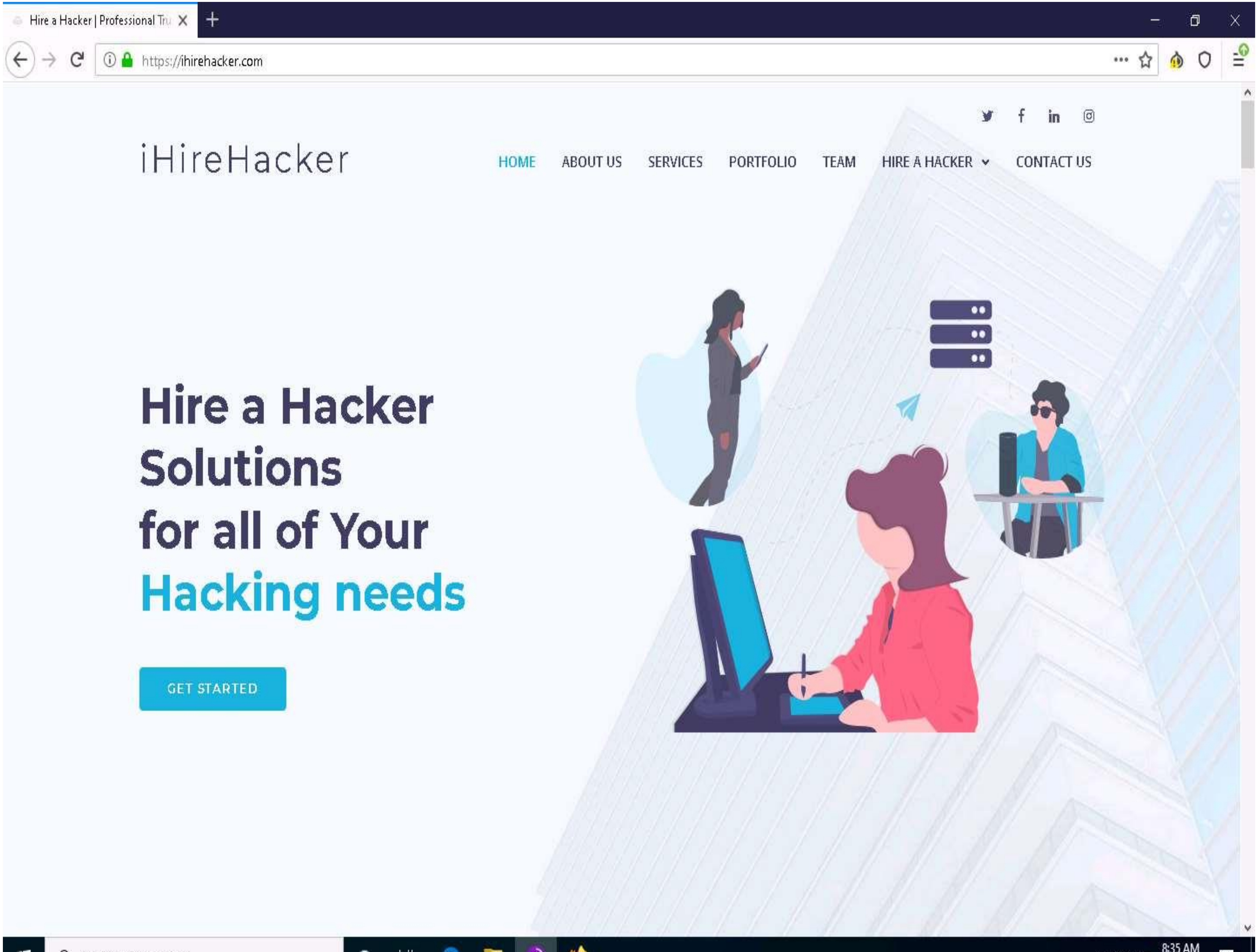
Hire hacker to make your system more secure as attacks on web increases as time progresses. We can also help to prevent confidentiality of mobile phone and email data, by trying different methods to get into mobile phone and email accounts. Web database in most vulnerable to attack because it contains more secure data. Many companies **hire hacker** to make there database safe from security point ...

Hackers Group Online l Hire a Hacker Online l Hire ...

https://hackersgrouponline.com

Hackers group online welcome you to worlds number 1hire a hackerplatform. we a group of

10. The **https://ihirehacker.com** webpage opens up, as shown in the screenshot. You can see that the site belongs to professional hackers who operate underground.



Hire a Hacker | Professional Tru

https://ihirehacker.com

iHireHacker

HOME ABOUT US SERVICES PORTFOLIO TEAM HIRE A HACKER CONTACT US

Hire a Hacker Solutions for all of Your Hacking needs

GET STARTED

11. □ ihirehacker 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://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page)
    - **FakeID** is an onion site for creating fake passports (http://fakeidskhfik46ux.onion/)
    - **The Paypal Cent** is an onion site that sells PayPal accounts with good balances (http://nare7pqnmnojs2pg.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.

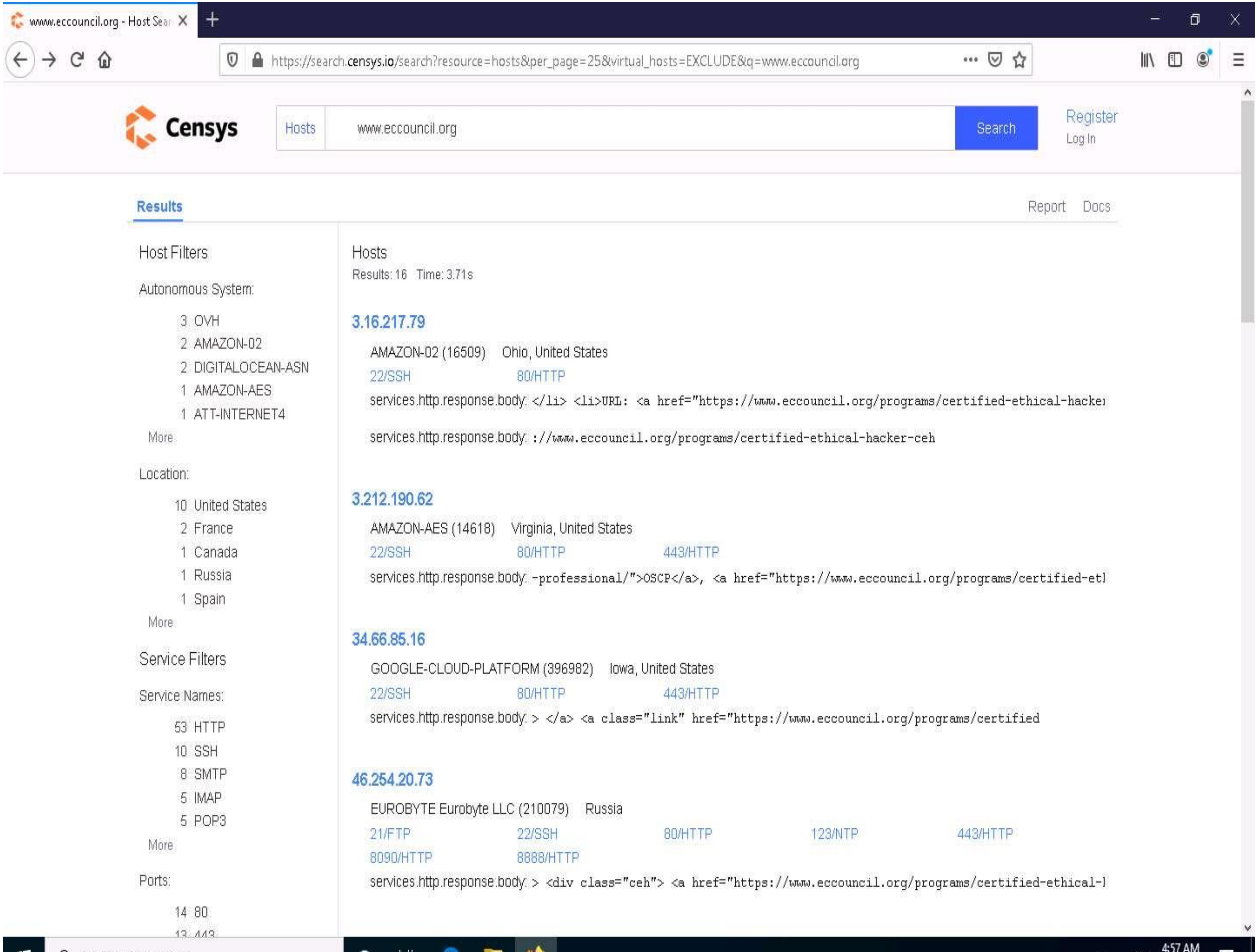
Task 5: Determine Target OS Through Passive Footprinting

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.

Here, we will gather target OS information through passive footprinting using the Censys 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 click https://censys.io/domain?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.

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



https://search.censys.io/search?resource=hosts&per_page=25&virtual_hosts=EXCLUDE&q=www.eccouncil.org

www.eccouncil.org

Host Filters

Autonomous System:

3	OVH
2	AMAZON-02
2	DIGITALOCEAN-ASN
1	AMAZON-AES
1	ATT-INTERNET4

More

Location:

10	United States
2	France
1	Canada
1	Russia
1	Spain

More

Service Filters

Service Names:

53	HTTP
10	SSH
8	SMTP
5	IMAP
5	POP3

More

Ports:

14	80
13	443

Hosts

Results: 16 Time: 3.71s

3.16.217.79

AMAZON-02 (16509) Ohio, United States

22/SSH 80/HTTP

services.http.response.body: `</li> <li>URL: <a href="https://www.eccouncil.org/programs/certified-ethical-hacke`

services.http.response.body: `://www.eccouncil.org/programs/certified-ethical-hacker-ceh`

3.212.190.62

AMAZON-AES (14618) Virginia, United States

22/SSH 80/HTTP 443/HTTP

services.http.response.body: `-professional/">OSCP</a>, <a href="https://www.eccouncil.org/programs/certified-et`

34.66.85.16

GOOGLE-CLOUD-PLATFORM (396982) Iowa, United States

22/SSH 80/HTTP 443/HTTP

services.http.response.body: `> </a> <a class="link" href="https://www.eccouncil.org/programs/certified`

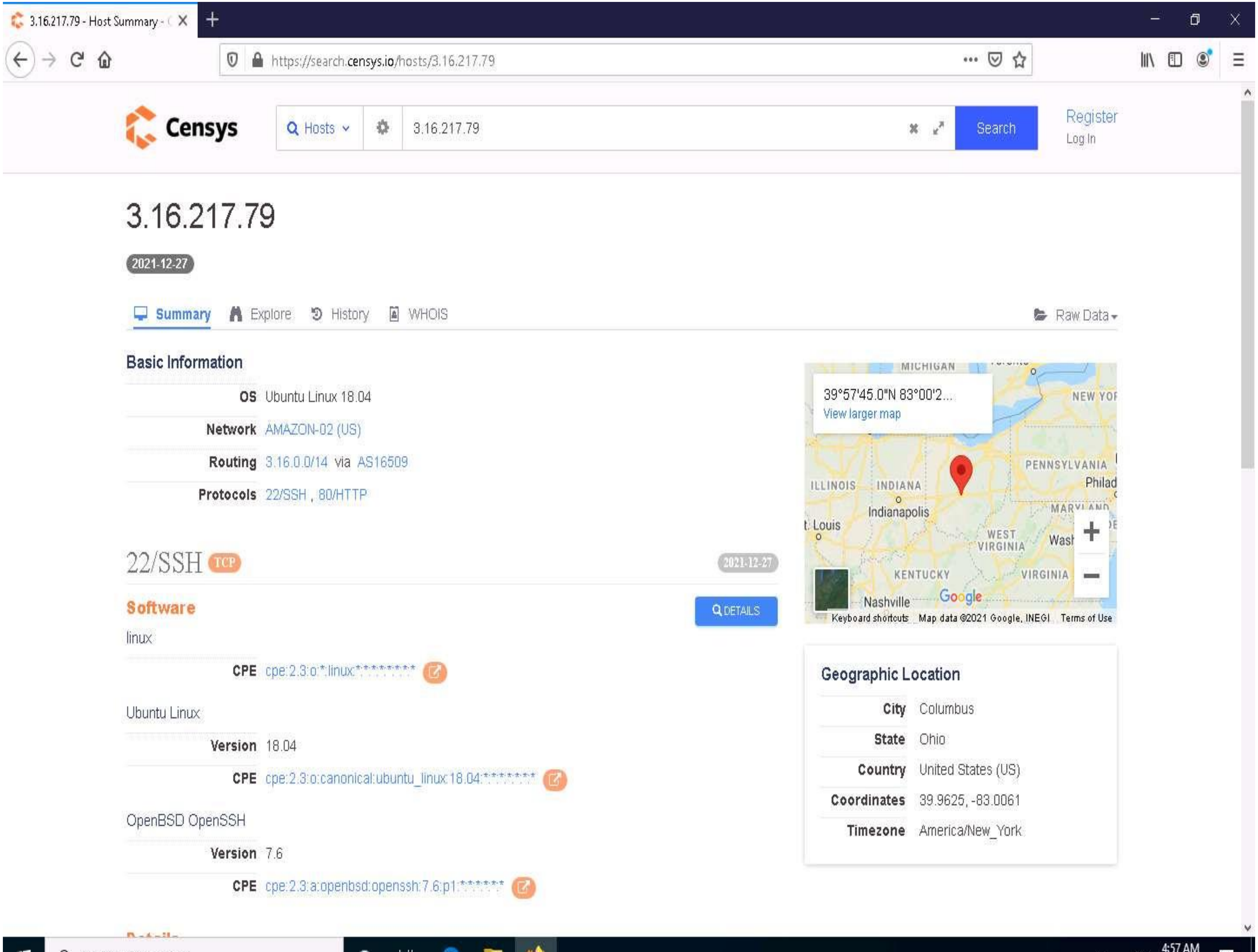
46.254.20.73

EUROBYTE Eurobyte LLC (210079) Russia

21/FTP 22/SSH 80/HTTP 123/NTP 443/HTTP
8090/HTTP 8888/HTTP

services.http.response.body: `> <div class="ceh"> <a href="https://www.eccouncil.org/programs/certified-ethical-`

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, host keys, etc.



3.16.217.79 - Host Summary - (
https://search.censys.io/hosts/3.16.217.79
Censys
Hosts
3.16.217.79
Search
Register
Log In

3.16.217.79

2021-12-27

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

2021-12-27

Software

linux

CPE	cpe:2.3:o:*:linux:*:*:*:*:*:*:*:*

Ubuntu Linux

Version	18.04
CPE	cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:*:*:*:*

OpenBSD OpenSSH

Version	7.6
CPE	cpe:2.3:a:openbsd:openssh:7.6:p1:*:*:*:*:*:*

Geographic Location

City	Columbus
State	Ohio
Country	United States (US)
Coordinates	39.9625, -83.0061
Timezone	America/New_York

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.