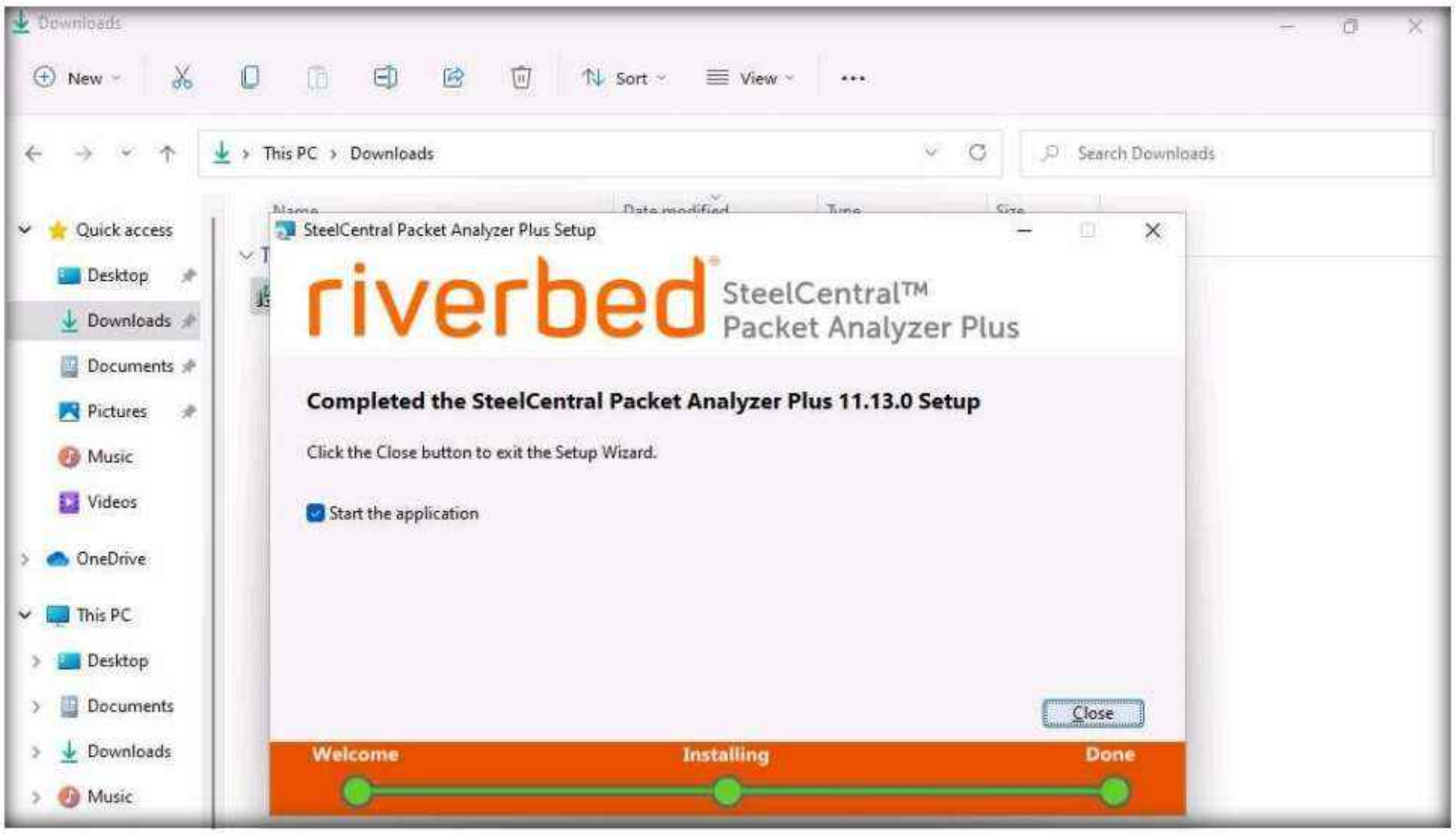
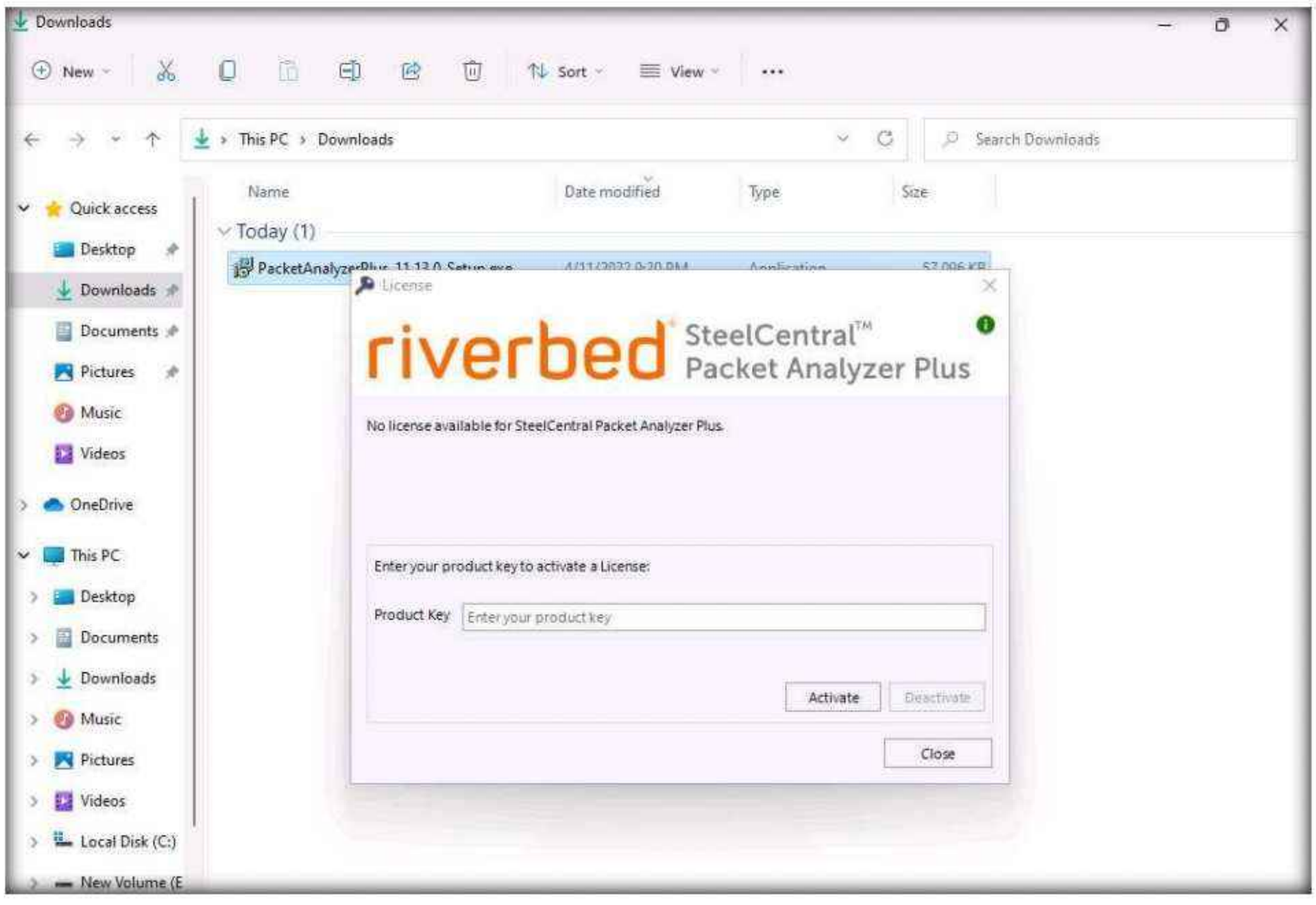
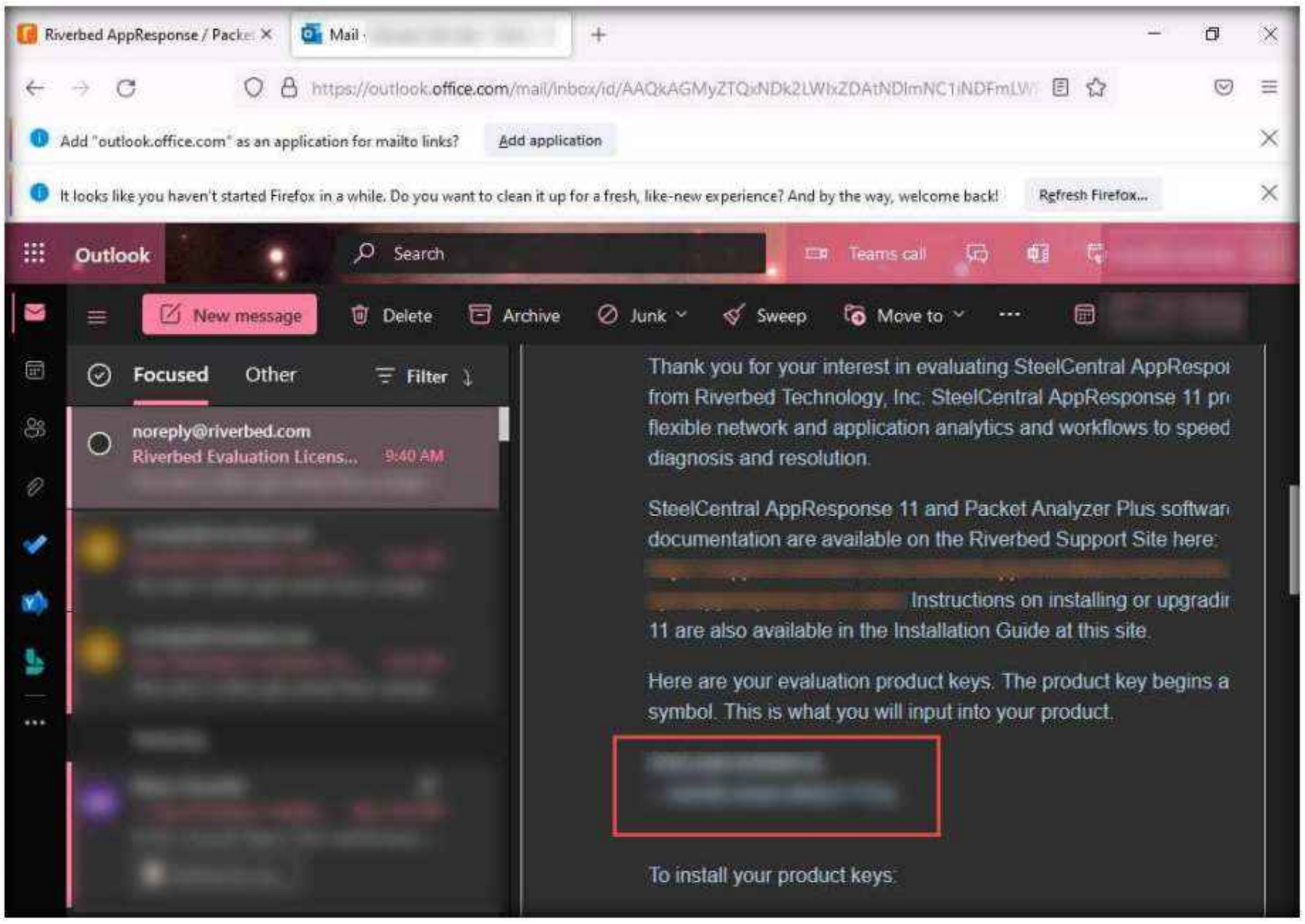
10. SteelCentral Packet Analyzer starts installing, and after the completion of the installation, the **Completed the SteelCentral Packet Analyzer Plus Setup** wizard appears. Ensure that the **Start the application** checkbox is selected and click **Close**.



11. The **License** window appears. Leave this window running.



12. Switch to your browser (here, **Mozilla Firefox**). Navigate to the tab where the **Riverbed Evaluation License Request for SteelCentral AppResponse Virtual** email is open and copy the **License Key** provided in the email.

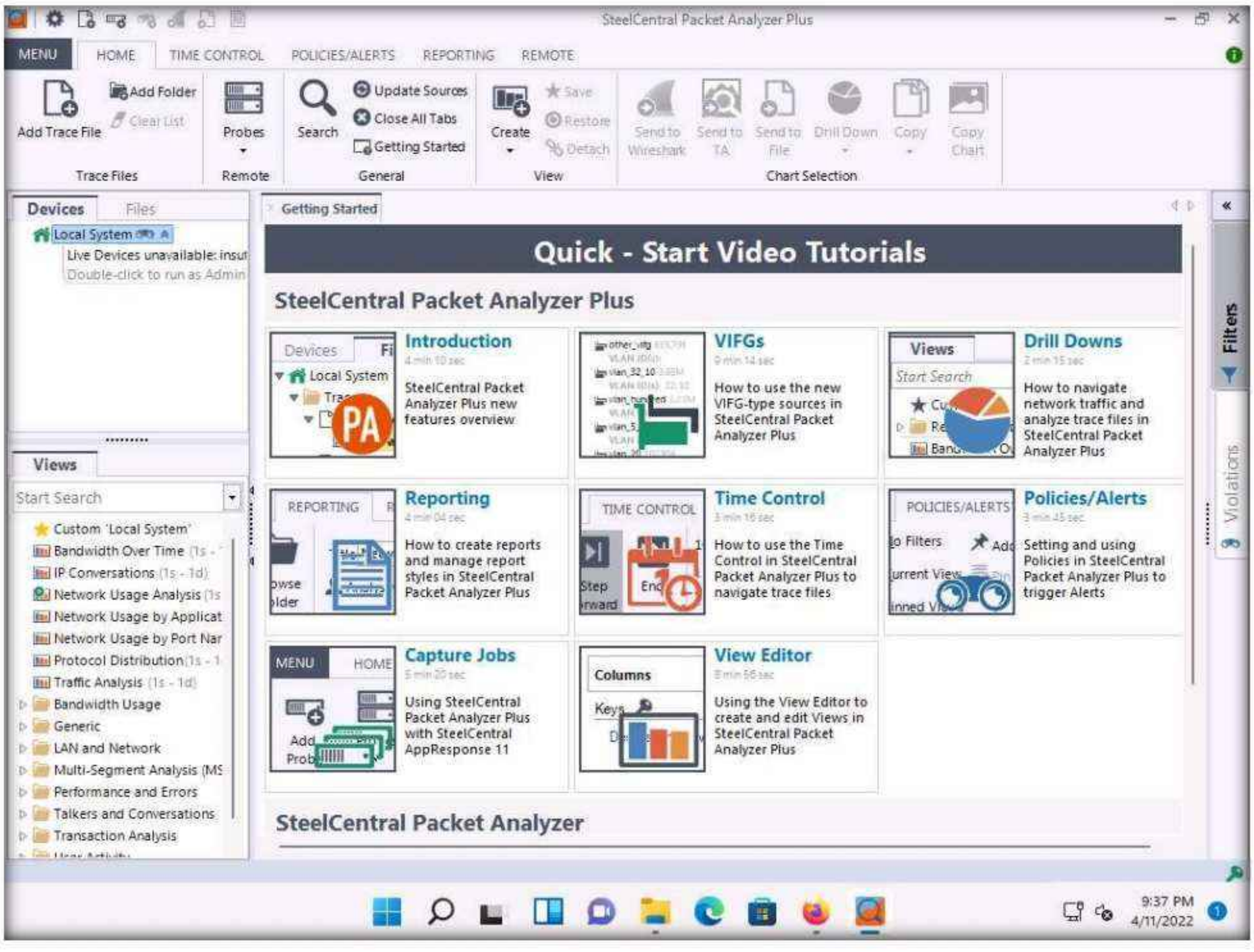


13. Switch back to **License** window and paste the **License Key** in the **Product Key** field. Click the **Activate** button.

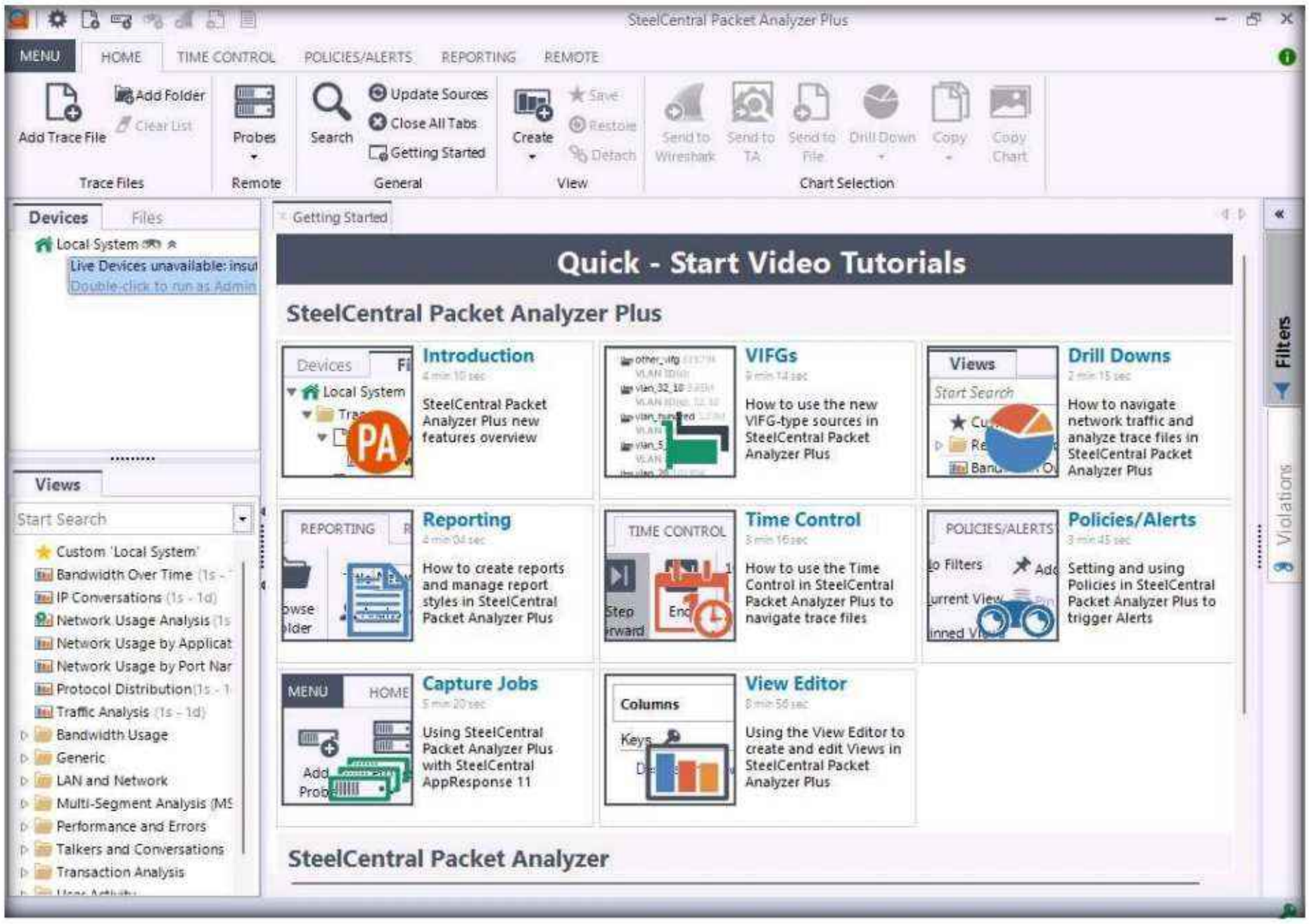
Note: If a **User Account Control** pop-up appears, click **Yes**.

14. The **SteelCentral Packet Analyzer Plus license activated** notification appears; click the **Start** button to start the application.

15. The **SteelCentral Packet Analyzer Plus** main window appears, displaying the **Getting Started** tab options, as shown in the screenshot.

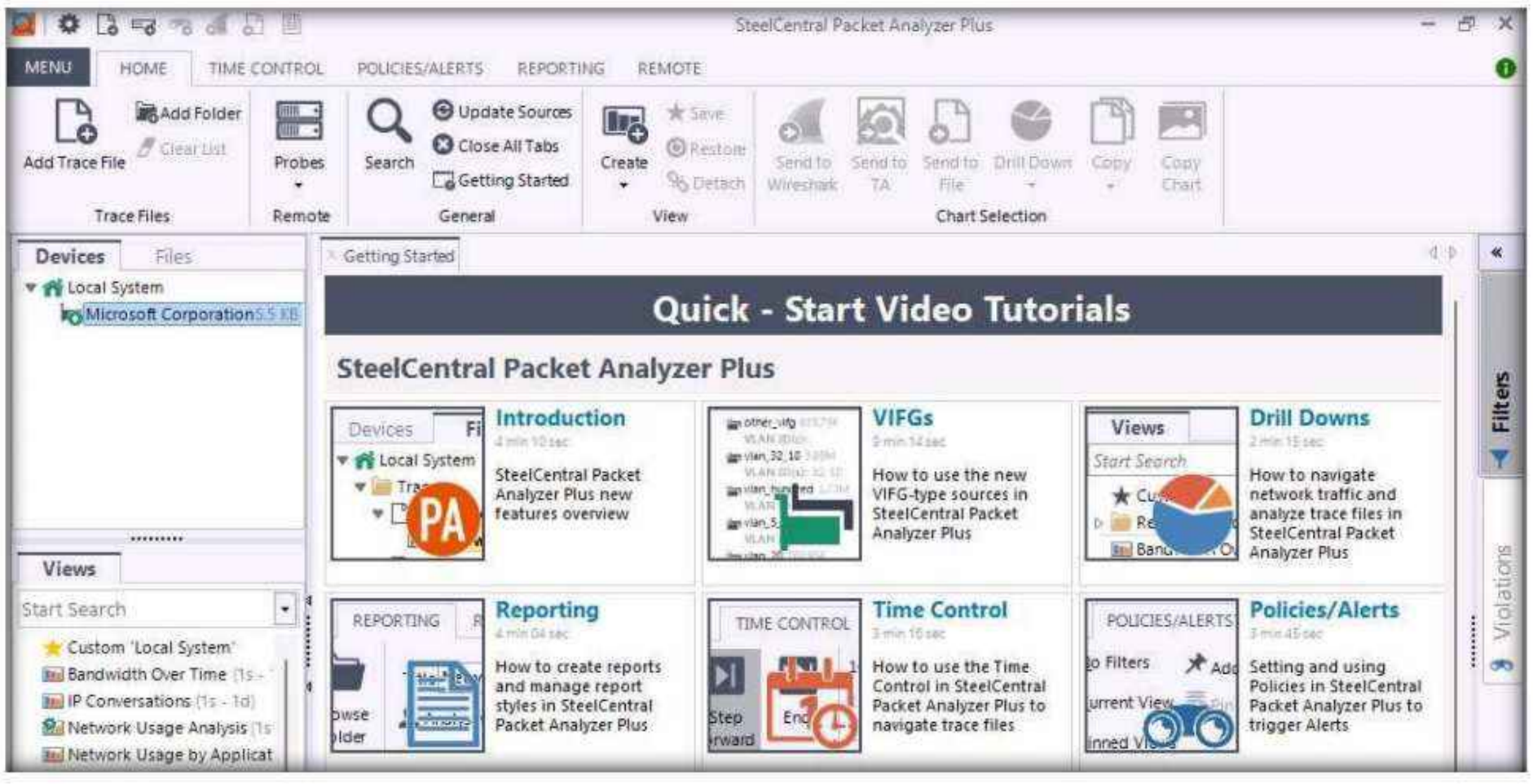


16. Observe that under the **Devices** tab in the left-hand pane, the application is unable to detect any **Local System** as it requires admin privileges. Therefore, double-click **Live Devices unavailable: Insufficient privileges** to run the application as an **Administrator**.

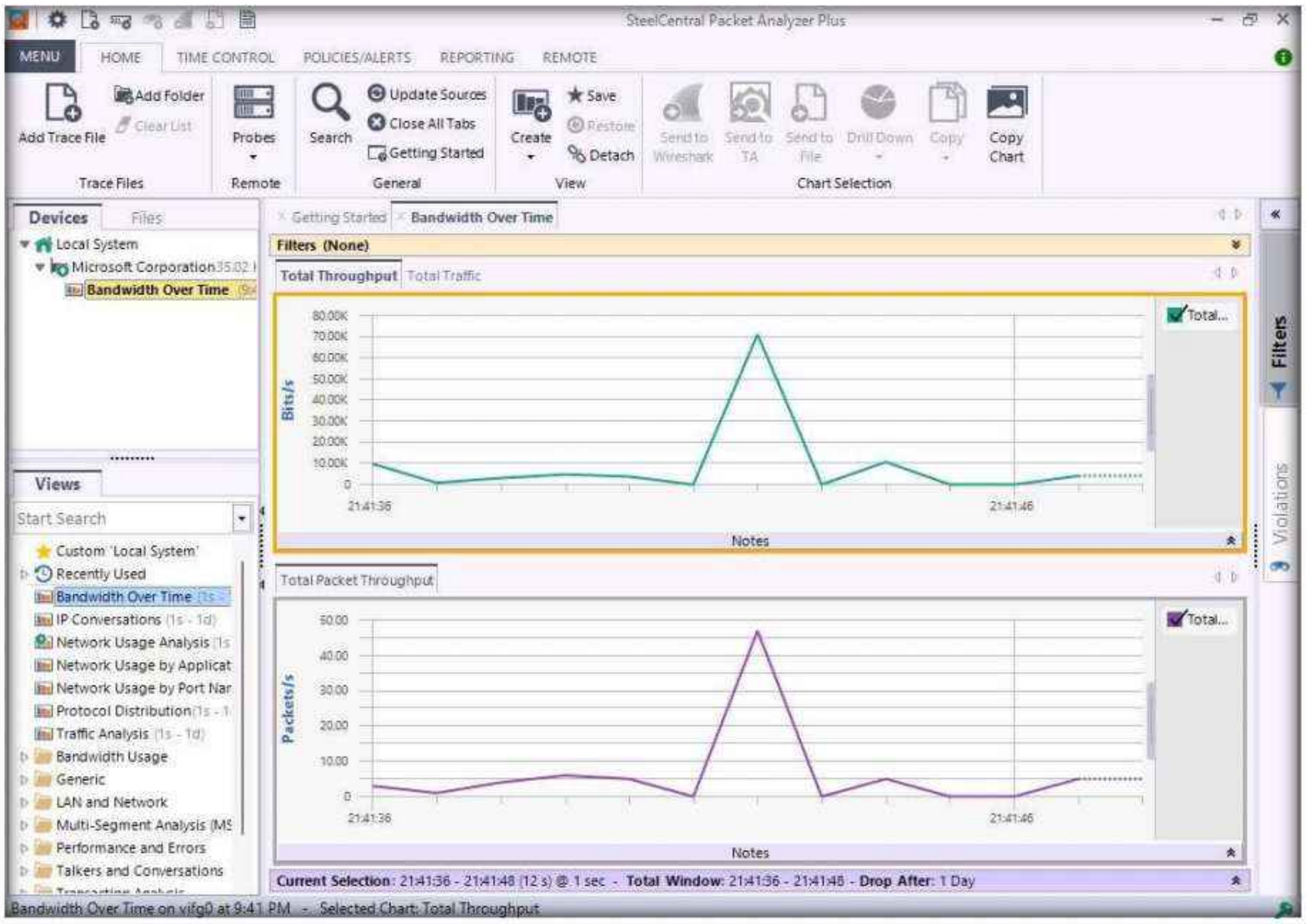


17. A **User Account Control** pop-up appears; click **Yes**.

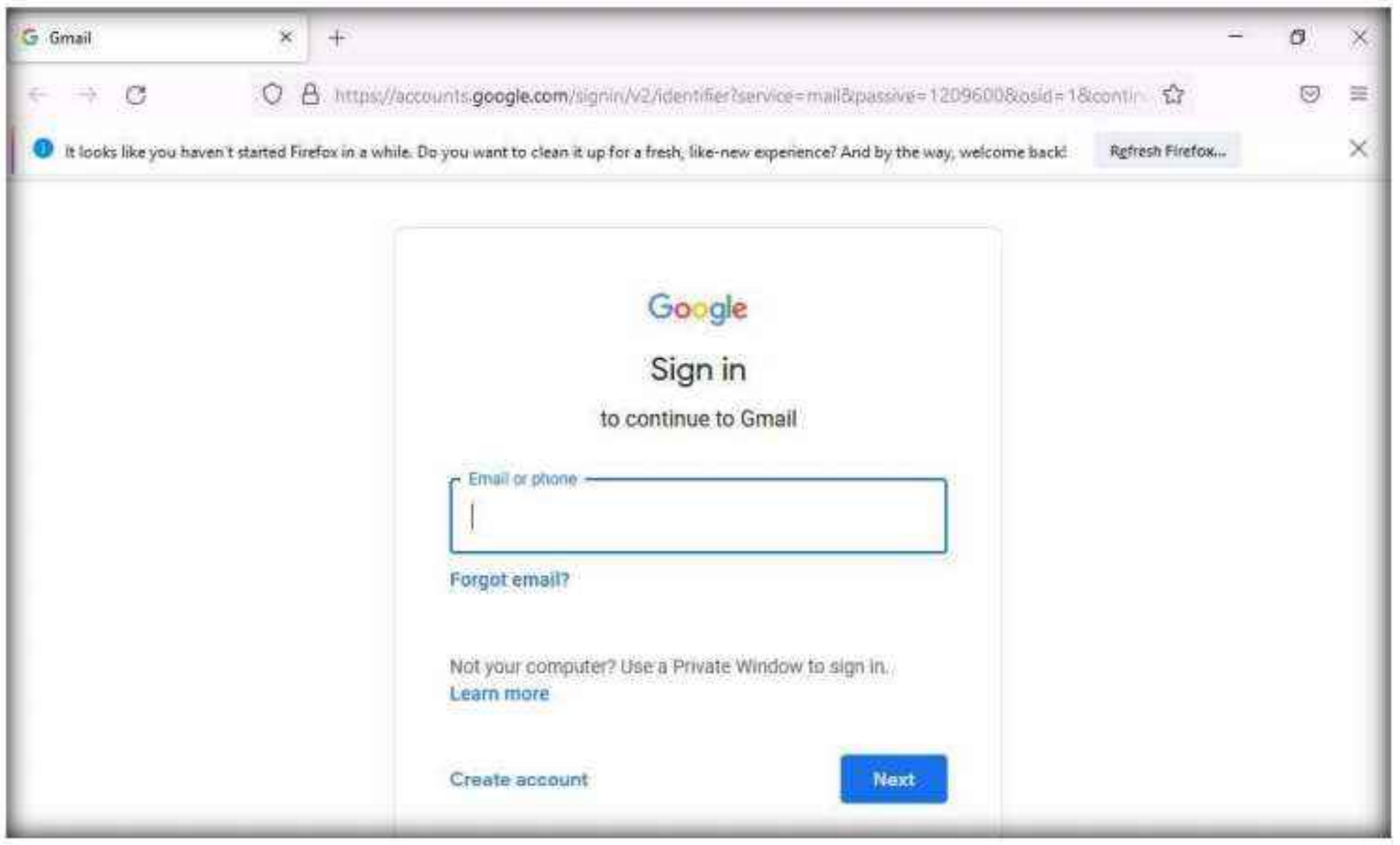
18. Ethernet adapter appear under **Local System** in the left-hand pane. Click the **Microsoft Corporation** adapter.



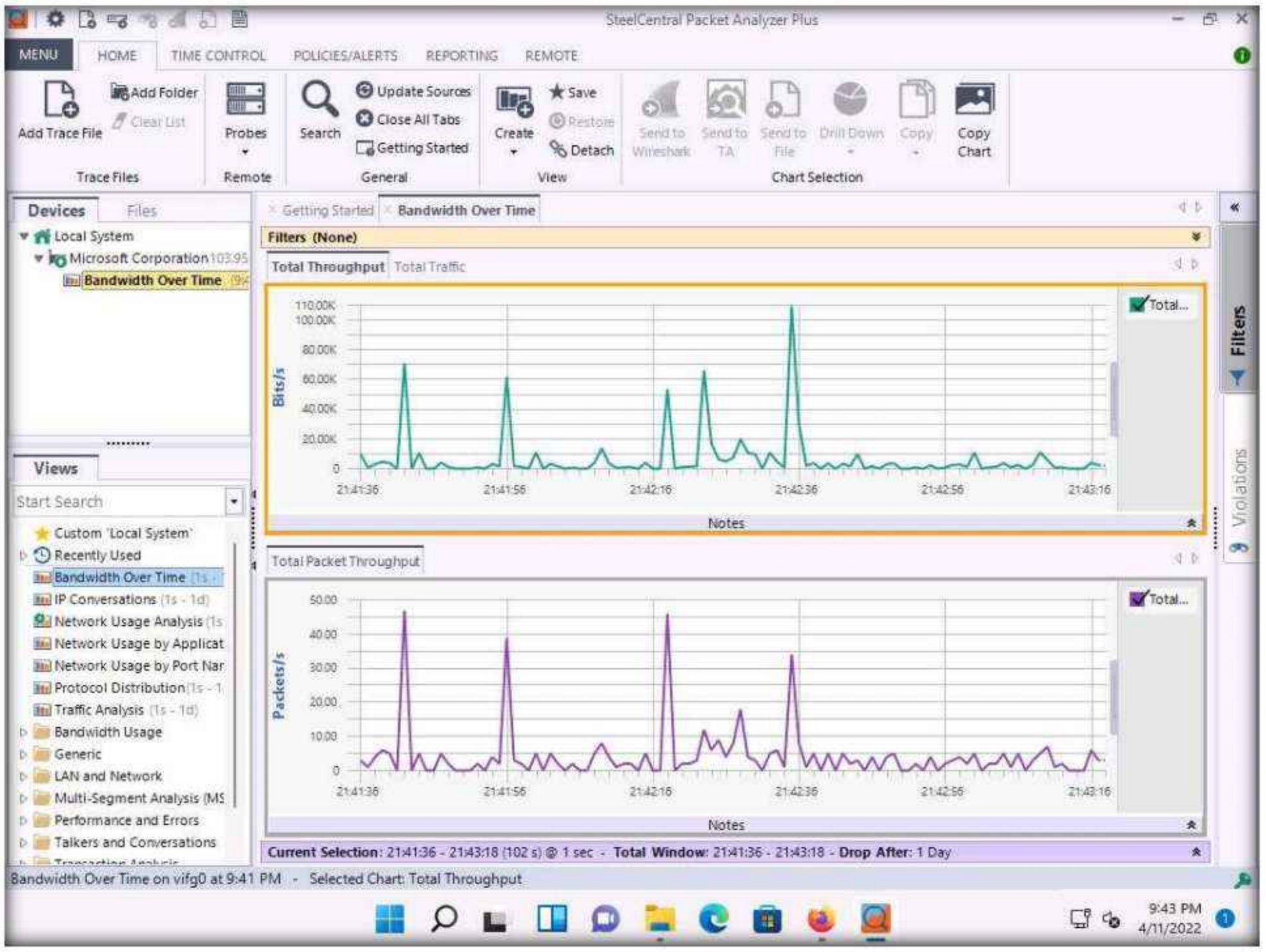
19. Double-click the **Bandwidth Over Time** option under the **Recently Used** node in the left-hand pane under the **Views** section.
20. A new **Bandwidth Over Time** tab appears, and SteelCentral Packet Analyzer Plus starts capturing the network traffic, as shown in the screenshot.



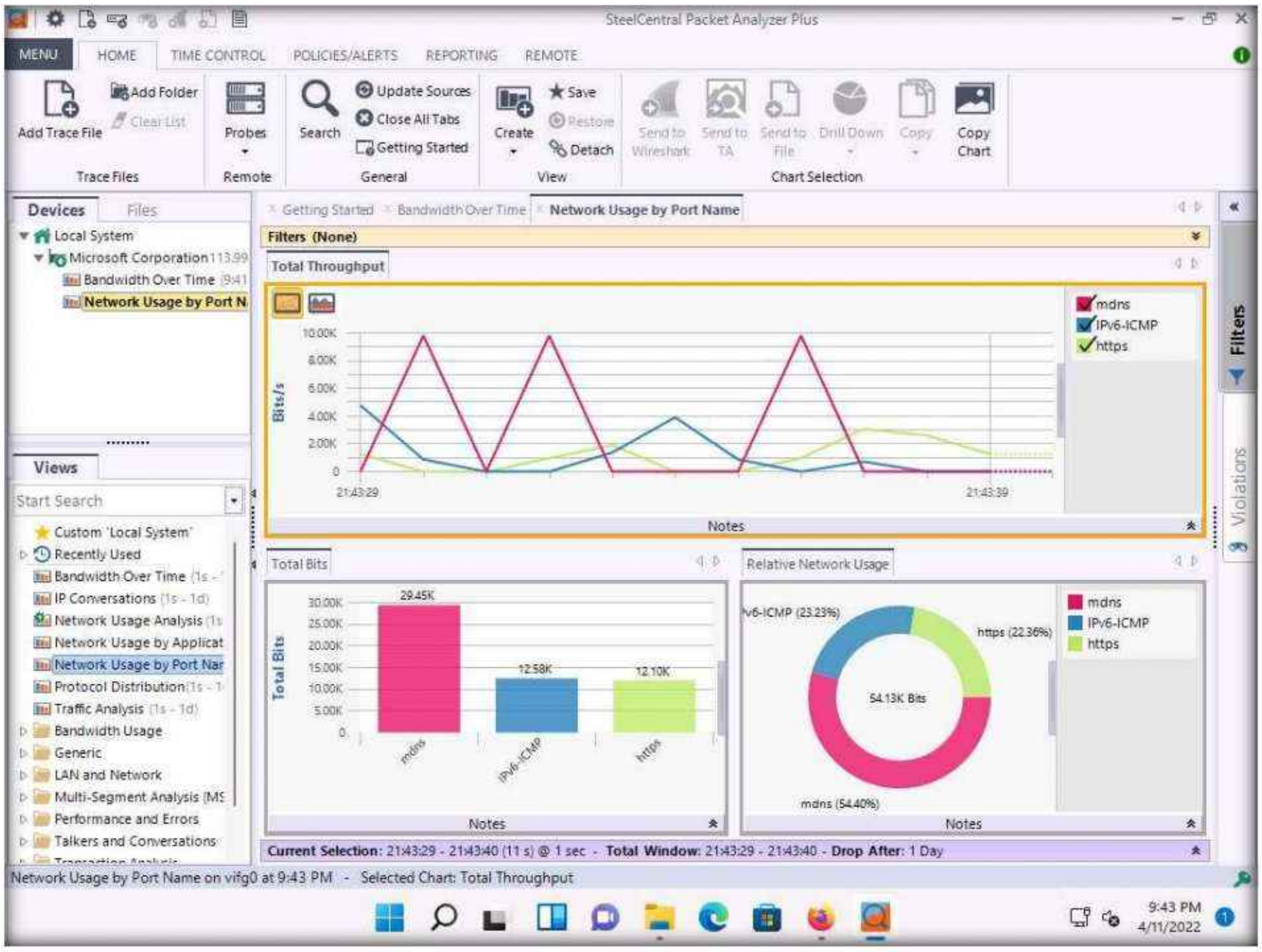
21. Now, switch to the **Windows Server 2019** virtual machine.
22. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.gmail.com**).



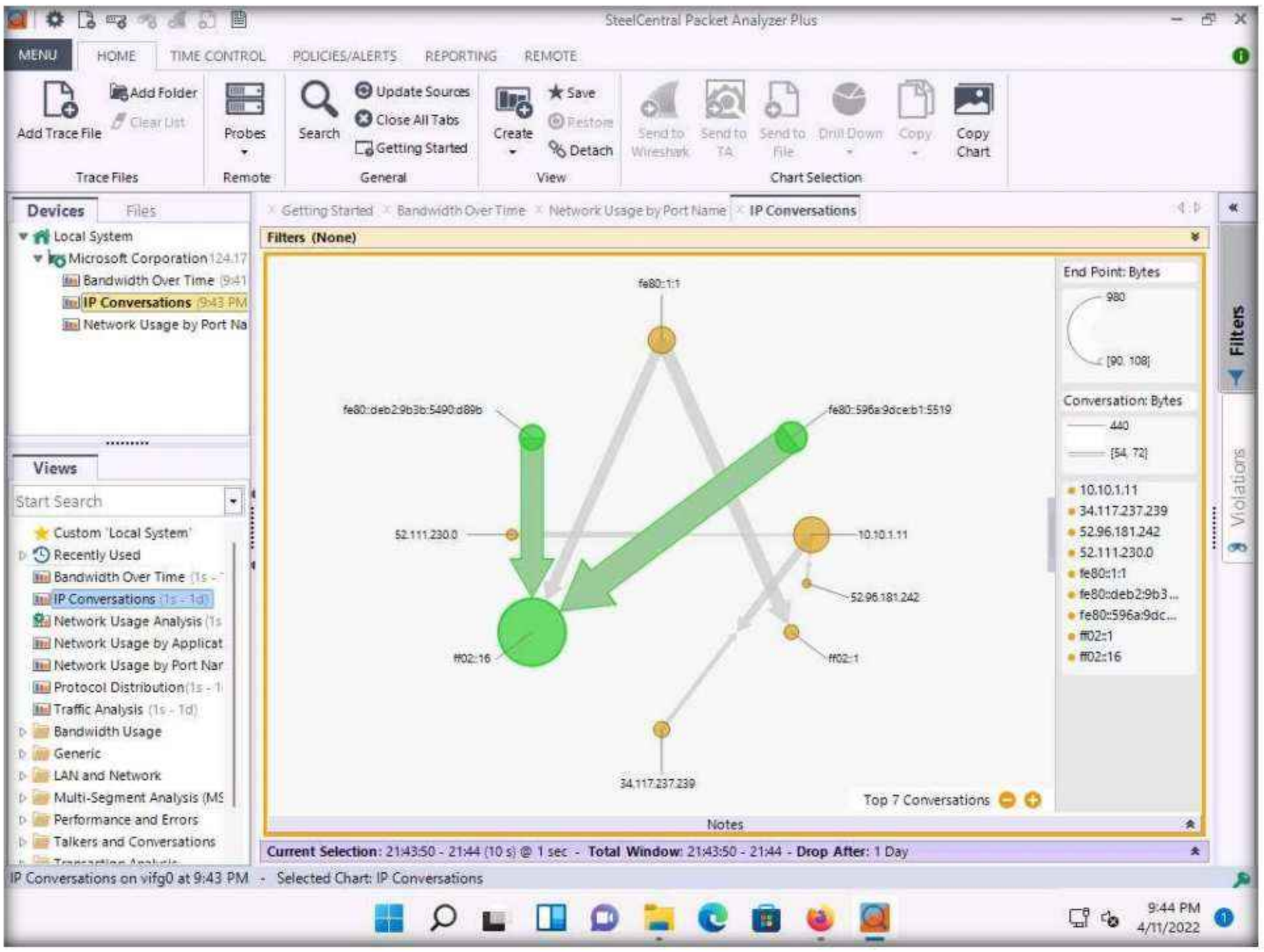
23. Switch back to the **Windows 11** virtual machine and observe the network traffic captured by **SteelCentral Packet Analyzer**, as shown in the screenshot.



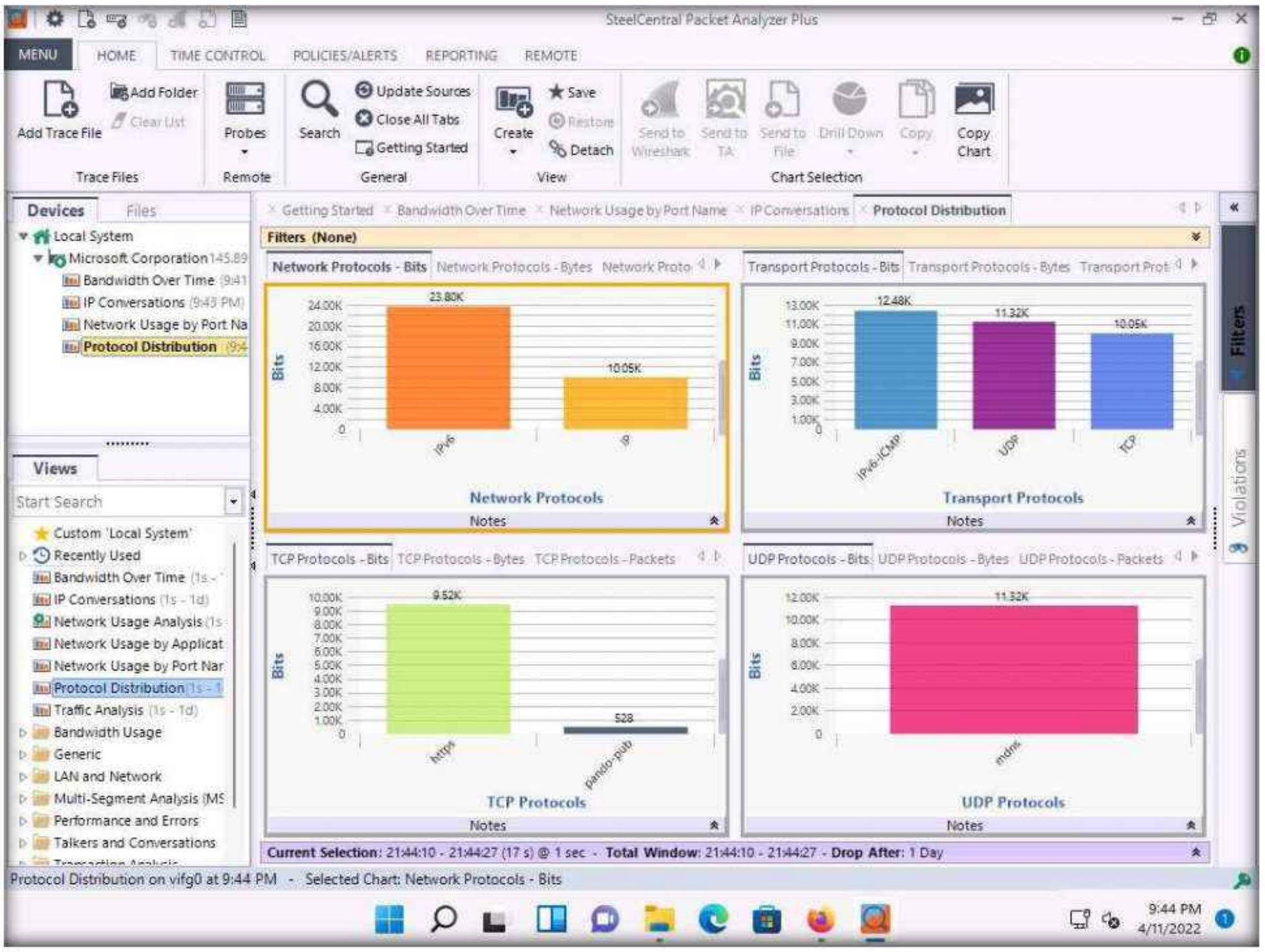
24. Double-click the **Network Usage by Port Name** option under the **Recently Used** node in the left-hand pane under the **Views** section.
25. A new **Network Usage by Port Name** tab appears, and **SteelCentral Packet Analyzer Plus** displays the captured network traffic.



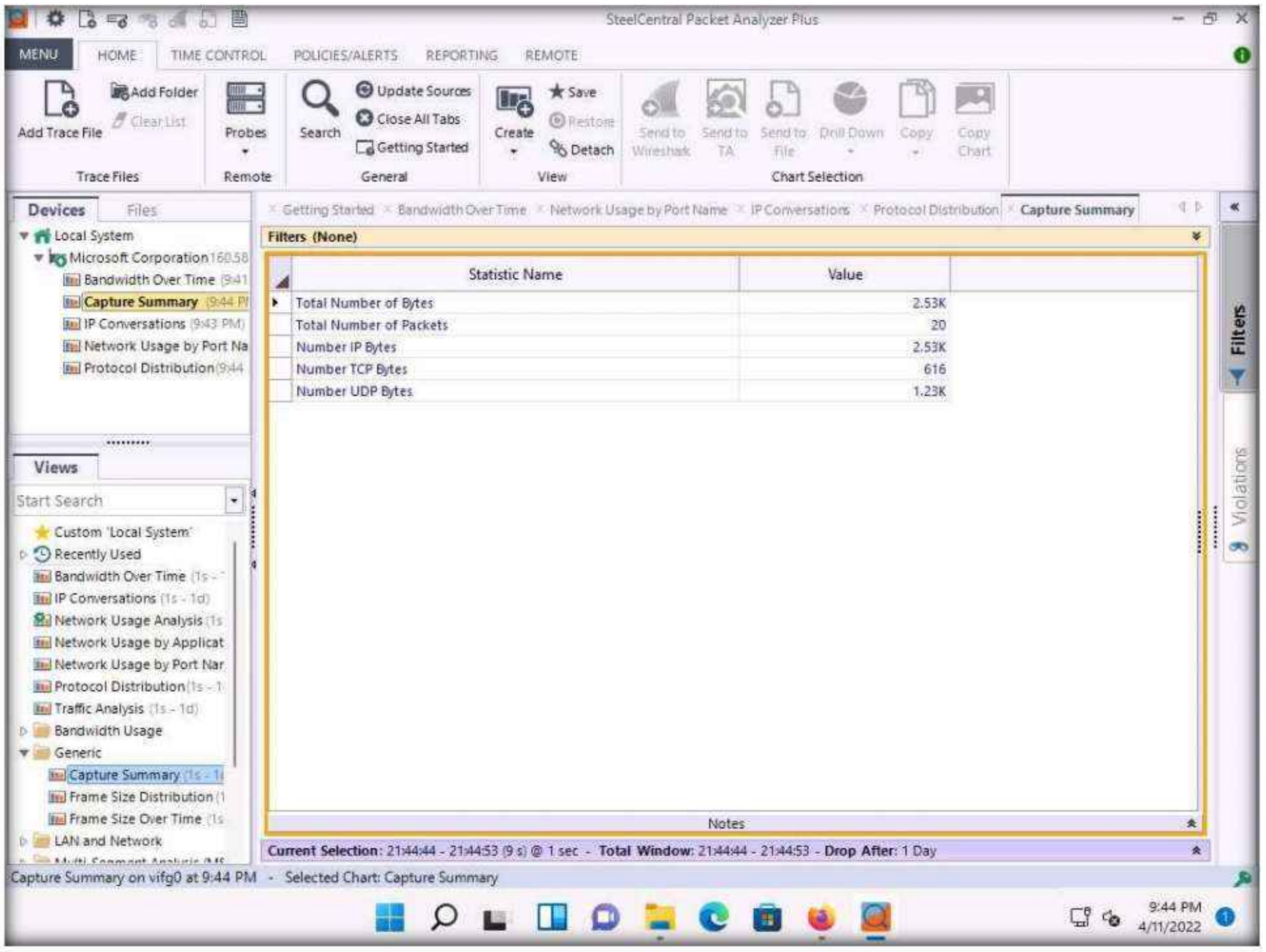
26. Double-click the **IP Conversations** option under the **Recently Used** node in the left-hand pane under the **Views** section.
27. A new **IP Conversations** tab appears, displaying conversations between different IP addresses in a map view.



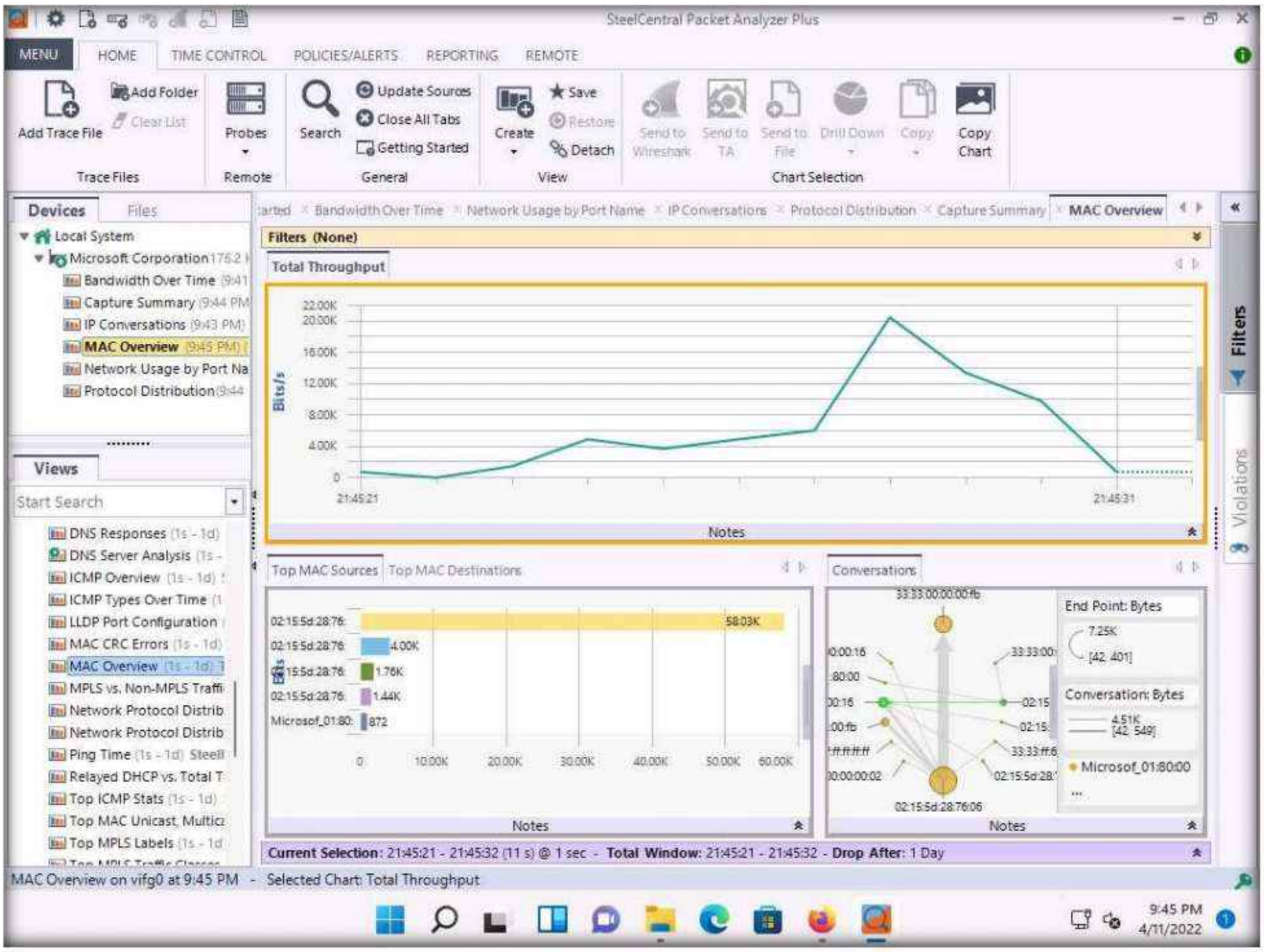
28. Double-click the **Protocol Distribution** option under the **Recently Used** node in the left-hand pane under the **Views** section.
29. A new **Protocol Distribution** tab appears, displaying **Network Protocols**, **Transport Protocols**, **TCP Protocols**, **UDP Protocols**, and other information, as shown in the screenshot.



30. Now, expand the **Generic** node and double-click the **Capture Summary** option in the left-hand pane.
31. A new **Capture Summary** tab appears, displaying information about the captured network traffic packets.

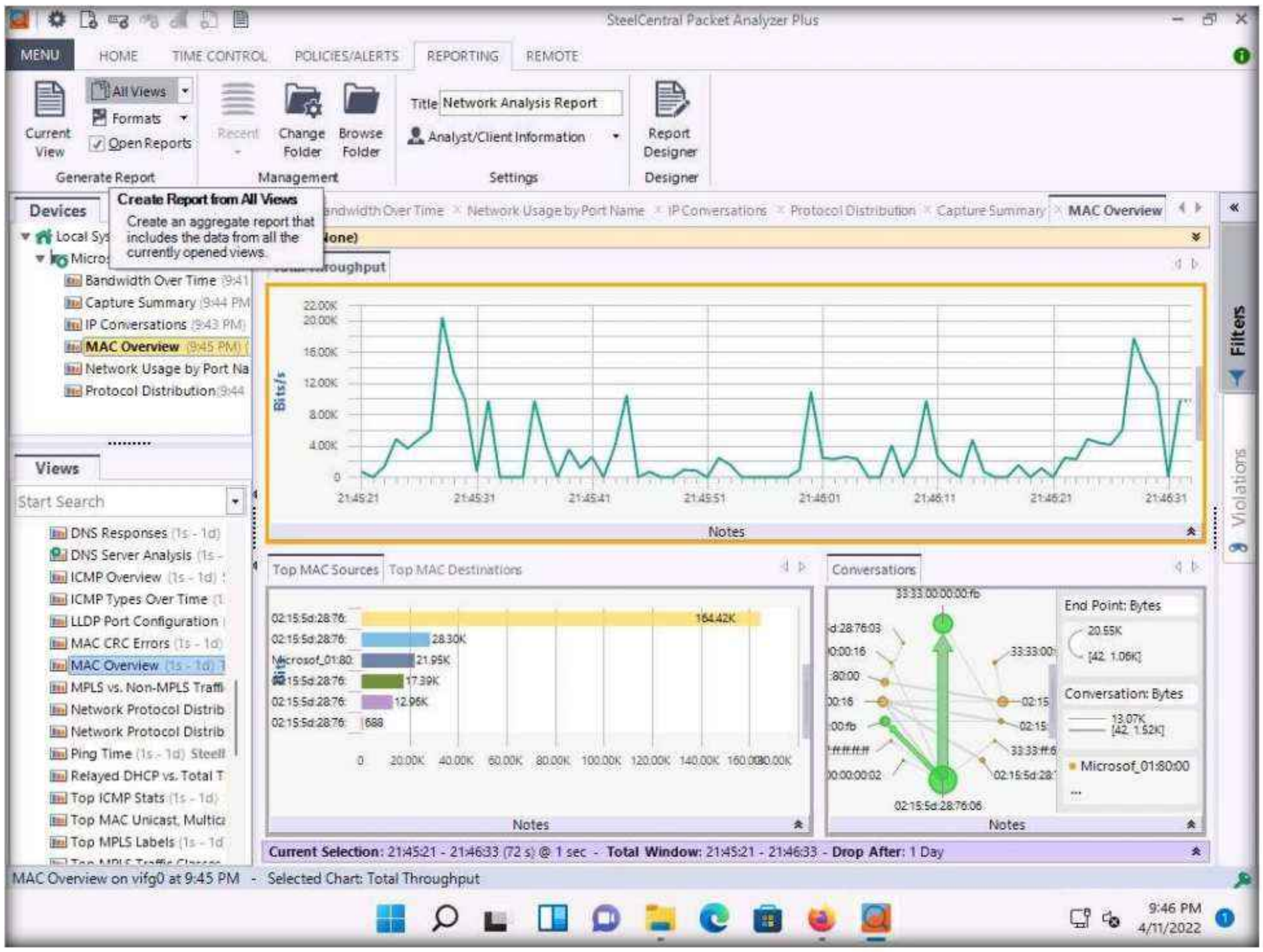


32. Expand the **LAN and Network** node and double-click the **MAC Overview** option in the left-hand pane.
33. A new **MAC Overview** tab appears, displaying information about MAC sources and destinations and MAC conversations.

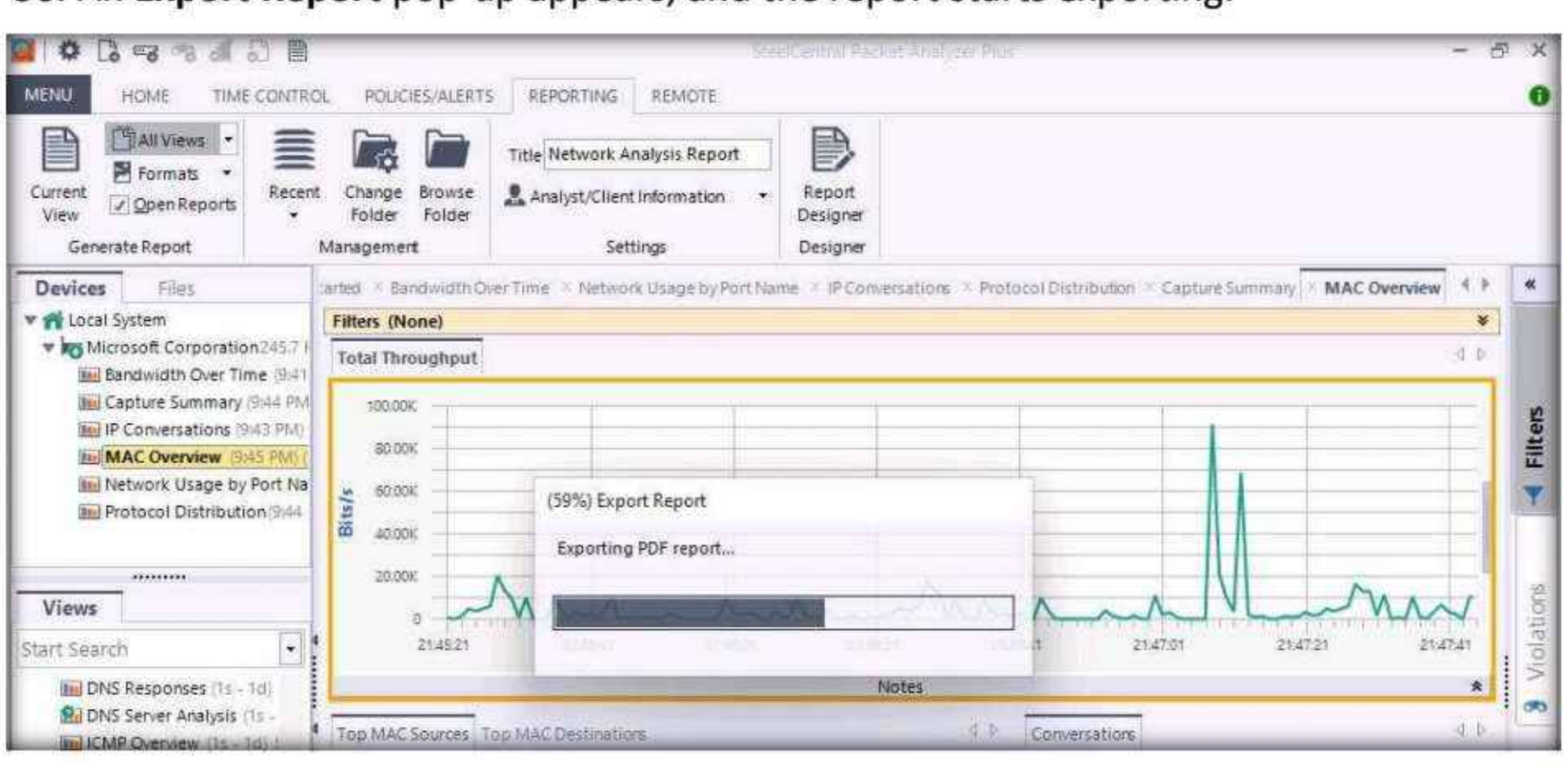


34. Similarly, you can explore various options in other nodes such as VLAN, MPLS, ARP, ICMP, and DHCP.

35. Click **Reporting** from the menu bar. Click on the **All Views** option to generate a report that includes all views.

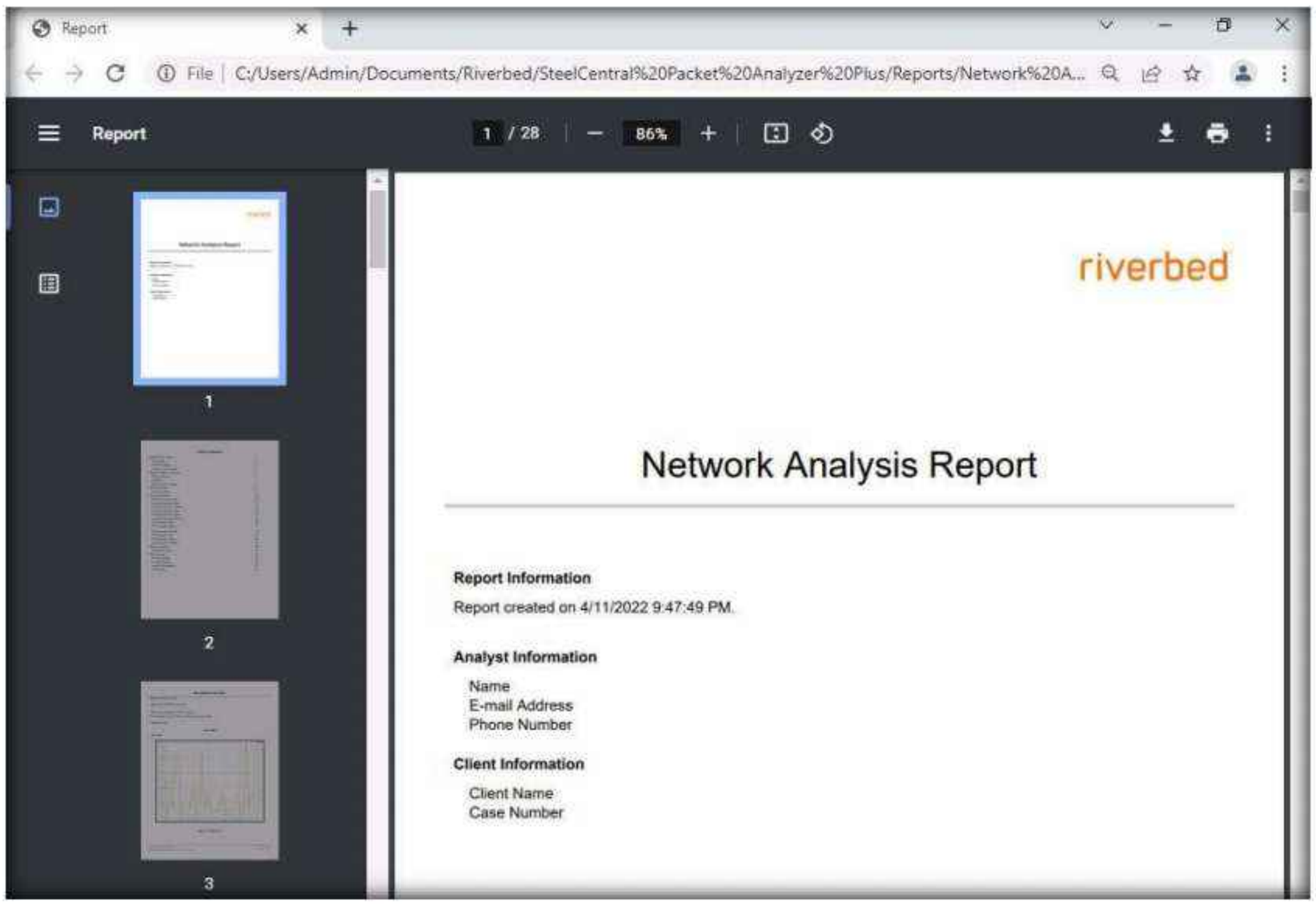


36. An **Export Report** pop-up appears, and the report starts exporting.

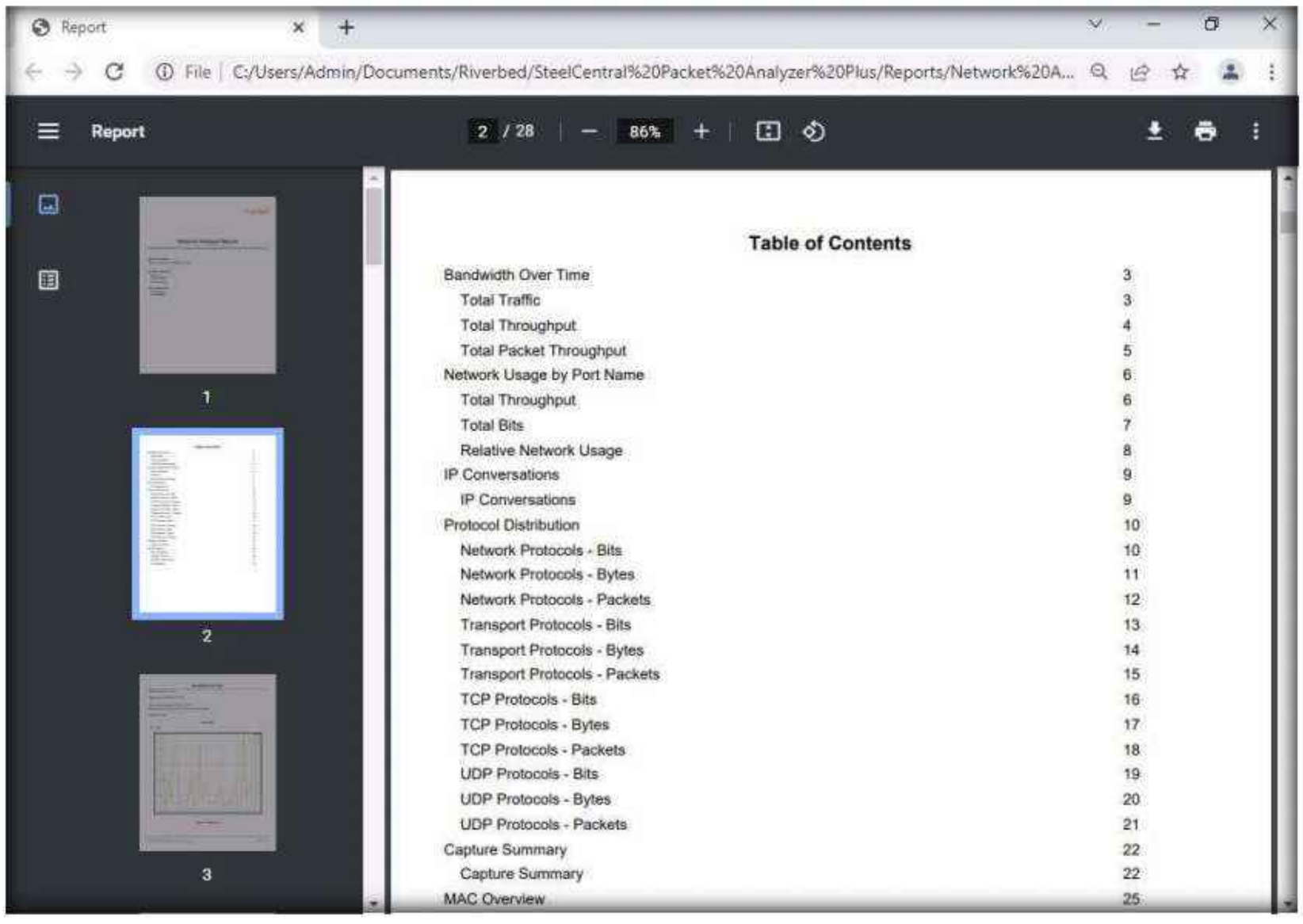


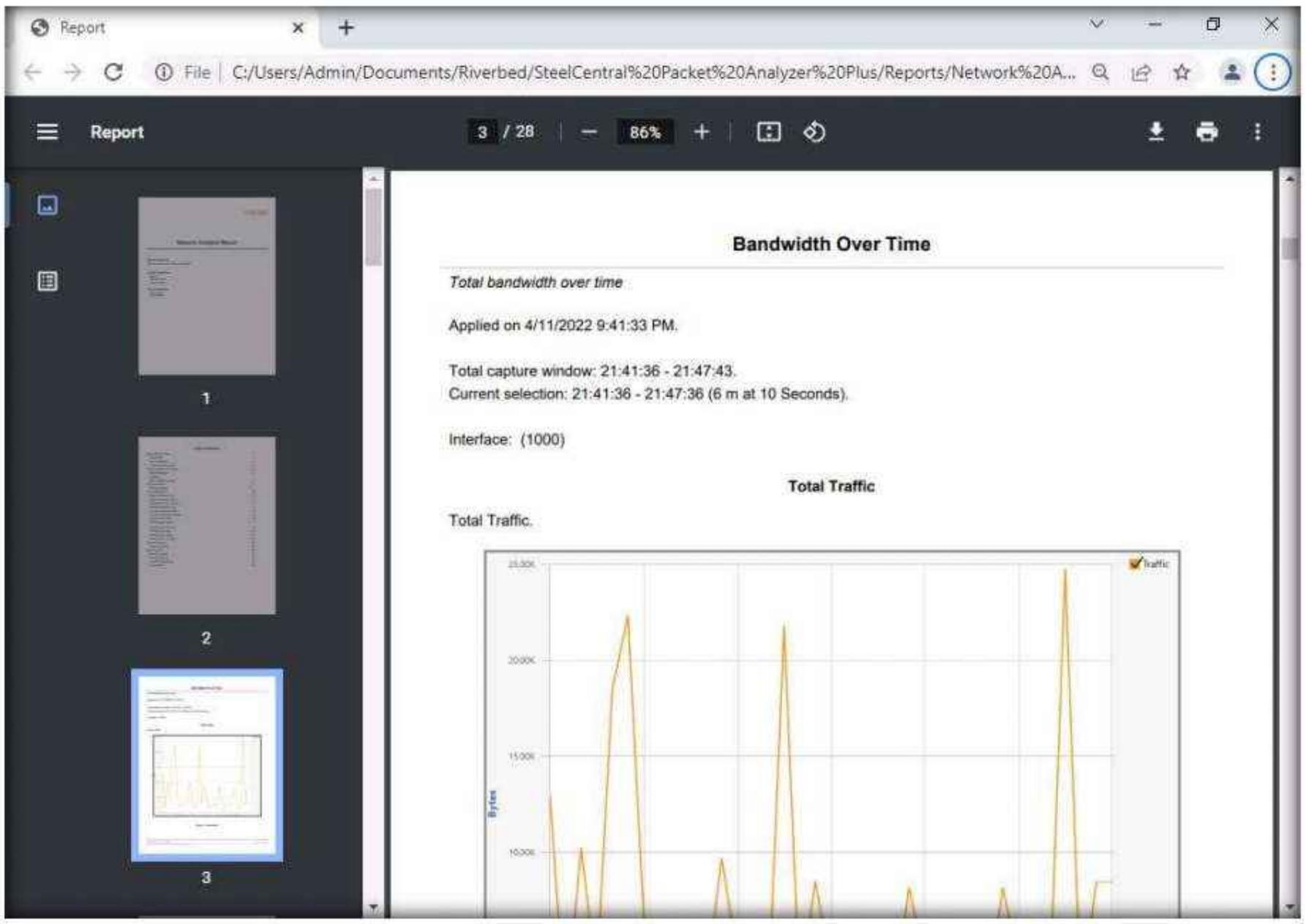
37. After completing the extraction, the generated report appears, as shown in the screenshot.

    Note: If a **How do you want to open this file?** pop up appears, click on **Google Chrome** and press **OK**



38. Scroll down to view detailed information on each option shown in **Table of Contents**.





39. This concludes the demonstration of analyzing a network using SteelCentral Packet Analyzer.
40. Close all open windows and document all the acquired information.
41. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 3

Detect Network Sniffing

Ethical hackers and pen testers are aided in the detection of network sniffing by various tools that make its detection an easy task.

Lab Scenario

The previous labs demonstrated how an attacker carries out sniffing with different techniques and tools. This lab helps you understand possible defensive techniques used to defend a target network against sniffing attacks.

A professional ethical hacker or pen tester should be able to detect network sniffing in the network. A sniffer on a network only captures data and runs in promiscuous mode, so it is not easy to detect. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace, since it does not transmit data. Therefore, to detect sniffing attempts, you must use the various network sniffing detection techniques and tools discussed in this lab.

Lab Objectives

- Detect ARP poisoning and promiscuous mode in a switch-based network
- Detect ARP poisoning using the Capsa Network Analyzer

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Detecting Network Sniffing

Network sniffing involves using sniffer tools that enable the real-time monitoring and analysis of data packets flowing over computer networks. These network sniffers can be detected by using various techniques such as:

- **Ping Method**: Identifies if a system on the network is running in promiscuous mode
- **DNS Method**: Identifies sniffers in the network by analyzing the increase in network traffic
- **ARP Method**: Sends a non-broadcast ARP to all nodes in the network; a node on the network running in promiscuous mode will cache the local ARP address

Lab Tasks

Task 1: Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network

ARP poisoning involves forging many ARP request and reply packets to overload a switch. ARP cache poisoning is the method of attacking a LAN network by updating the target computer's ARP cache with both forged ARP request and reply packets designed to change the Layer 2 Ethernet MAC address (that of the network card) to one that the attacker can monitor. Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

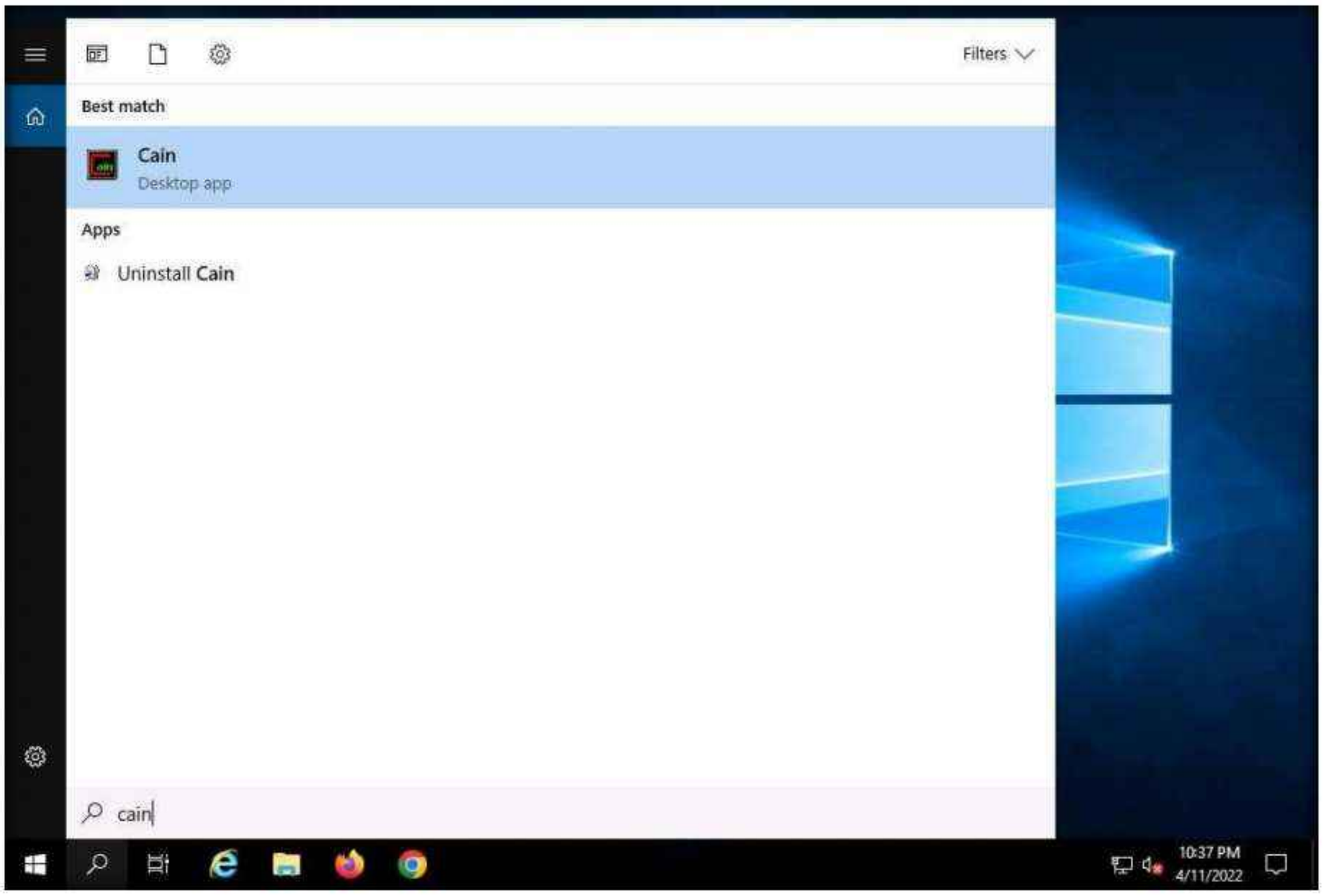
Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer toggles the NIC of a system to promiscuous mode, so that it listens to all data transmitted on its segment. A sniffer can constantly monitor all network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Promiscuous mode in the network can be detected using various tools.

The ethical hacker and pen tester must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

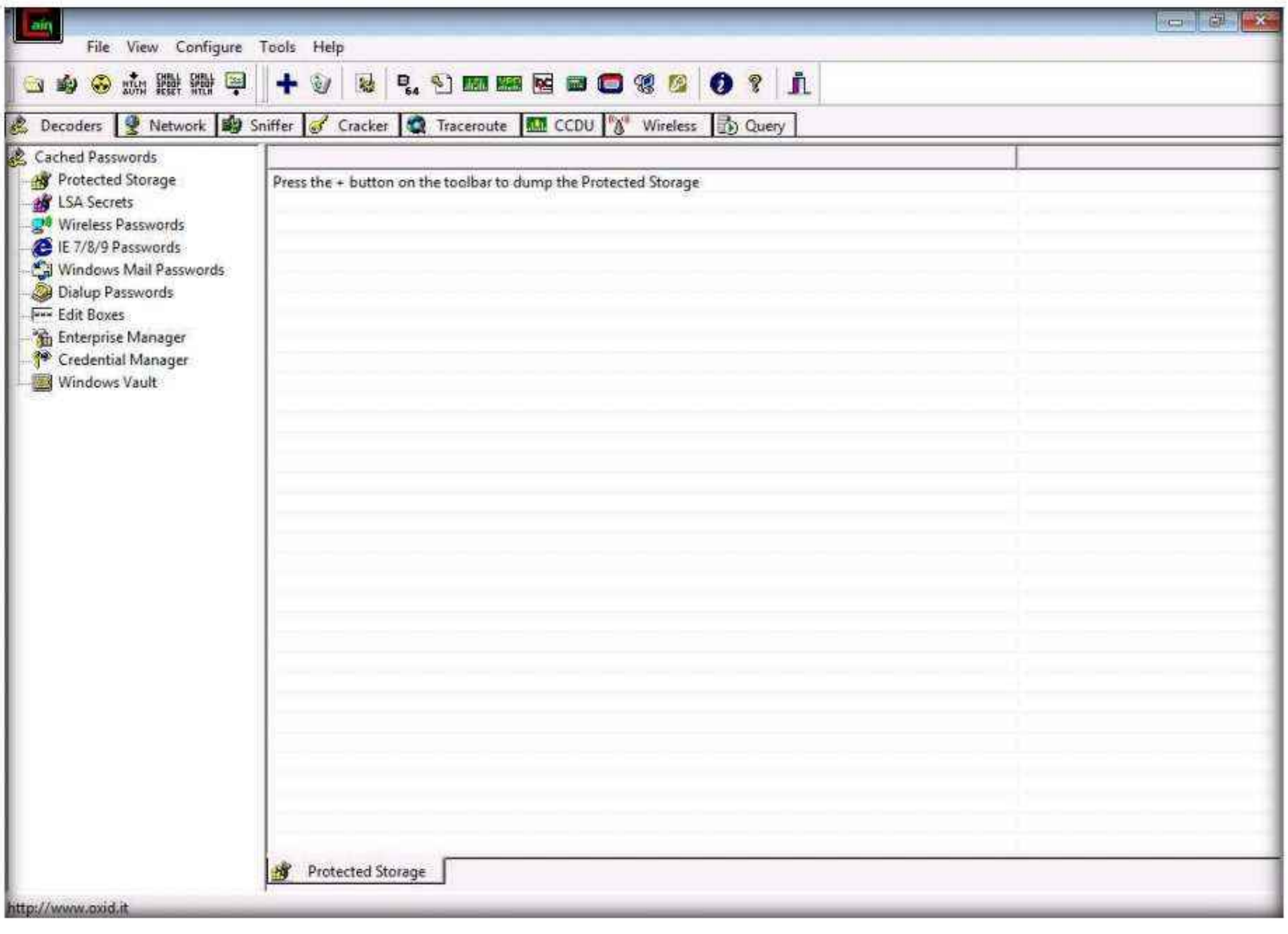
Here, we will detect ARP poisoning in a switch-based network using Wireshark and we will use the Nmap Scripting Engine (NSE) to check if a system on a local Ethernet has its network card in promiscuous mode.

Note: In this task, we will use the **Windows Server 2019** machine as the host machine to perform ARP poisoning and will sniff traffic flowing between the **Windows 11** and **Parrot Security** machines. We will use the same machine (**Windows Server 2019**) to detect ARP poisoning and use the Windows 11 machine to detect promiscuous mode in the in the network.

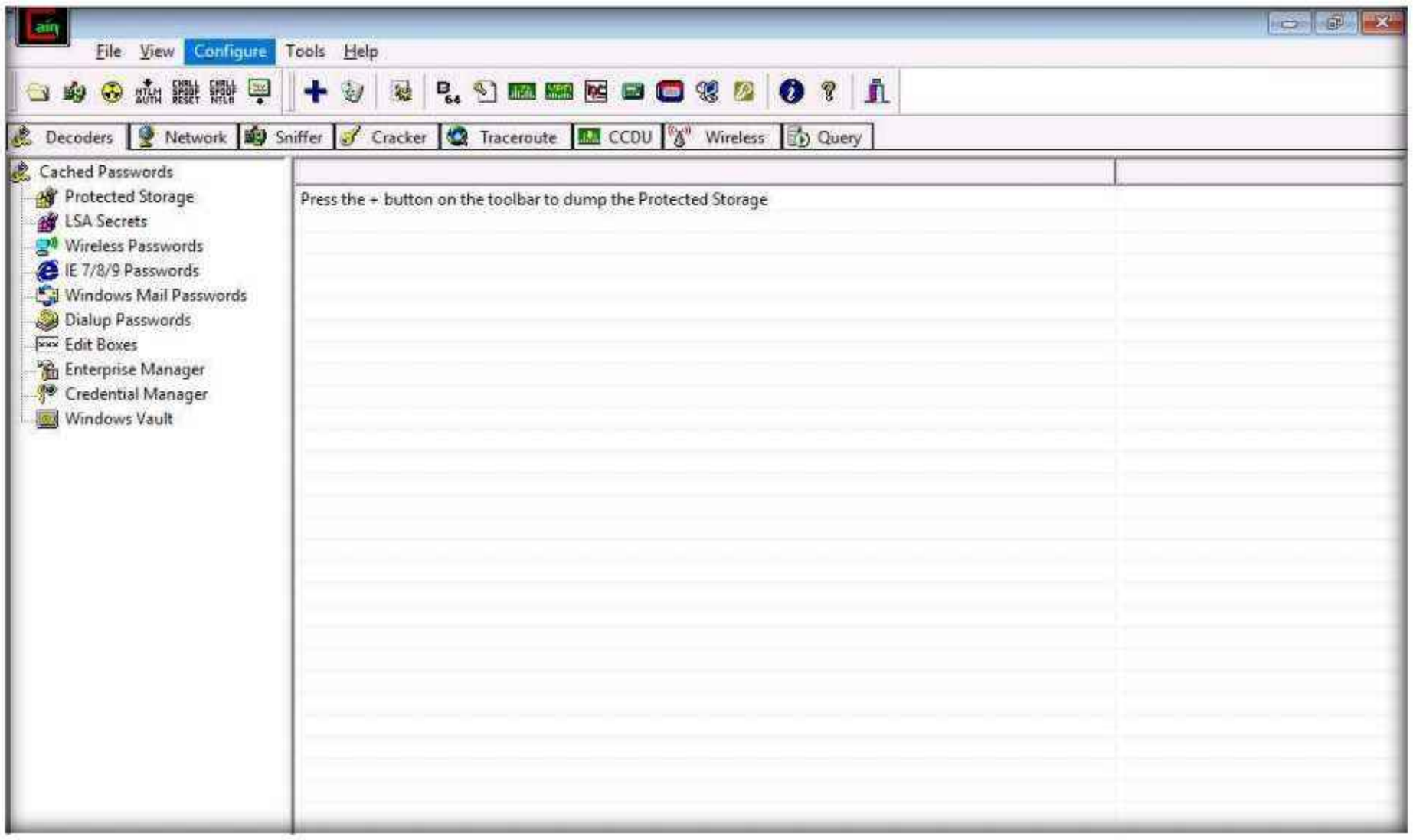
1. Turn on the **Windows 11**, **Windows Server 2019** and **Parrot Security** virtual machines.
2. Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.



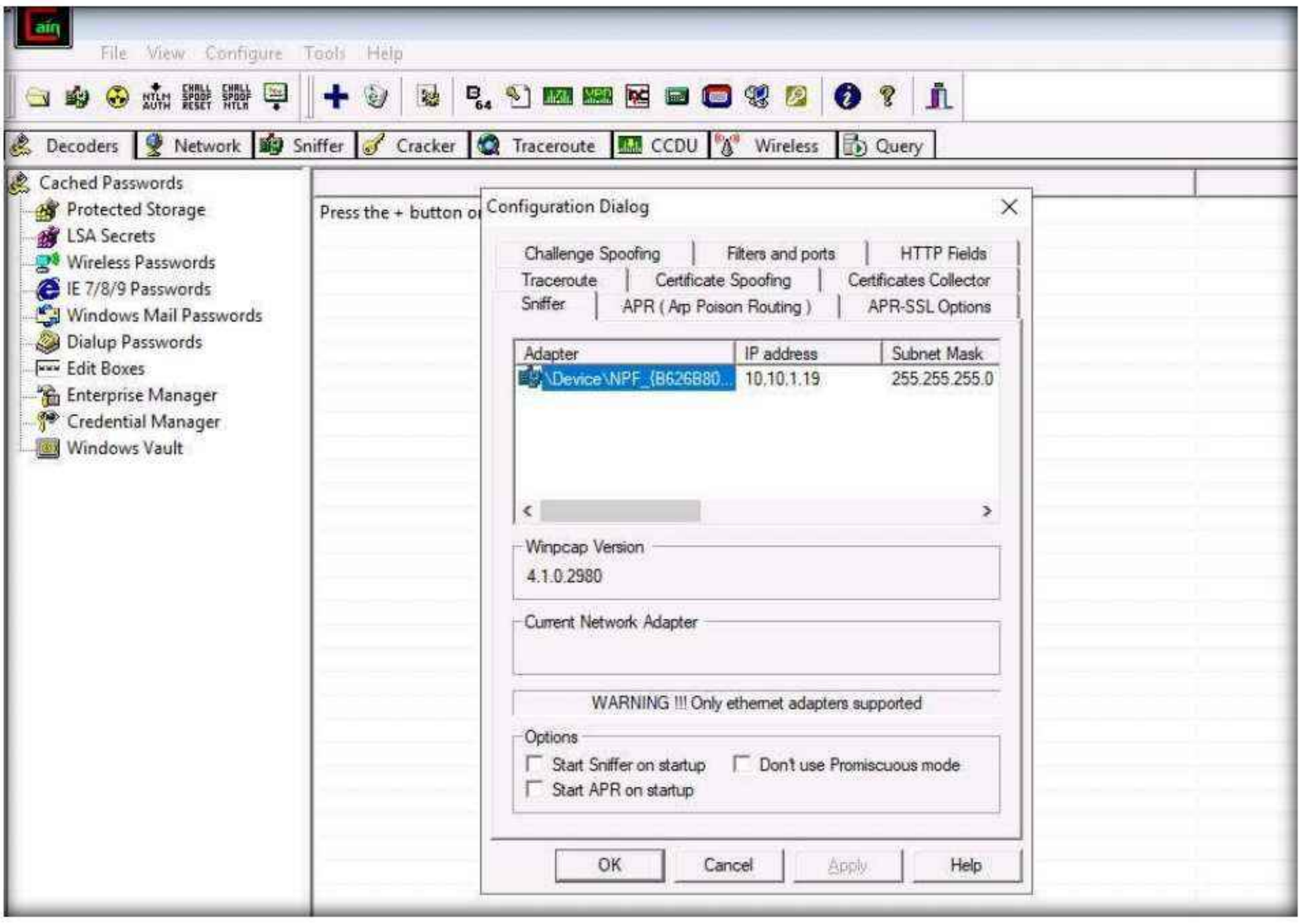
3. The **Cain & Abel** main window appears, as shown in the screenshot.



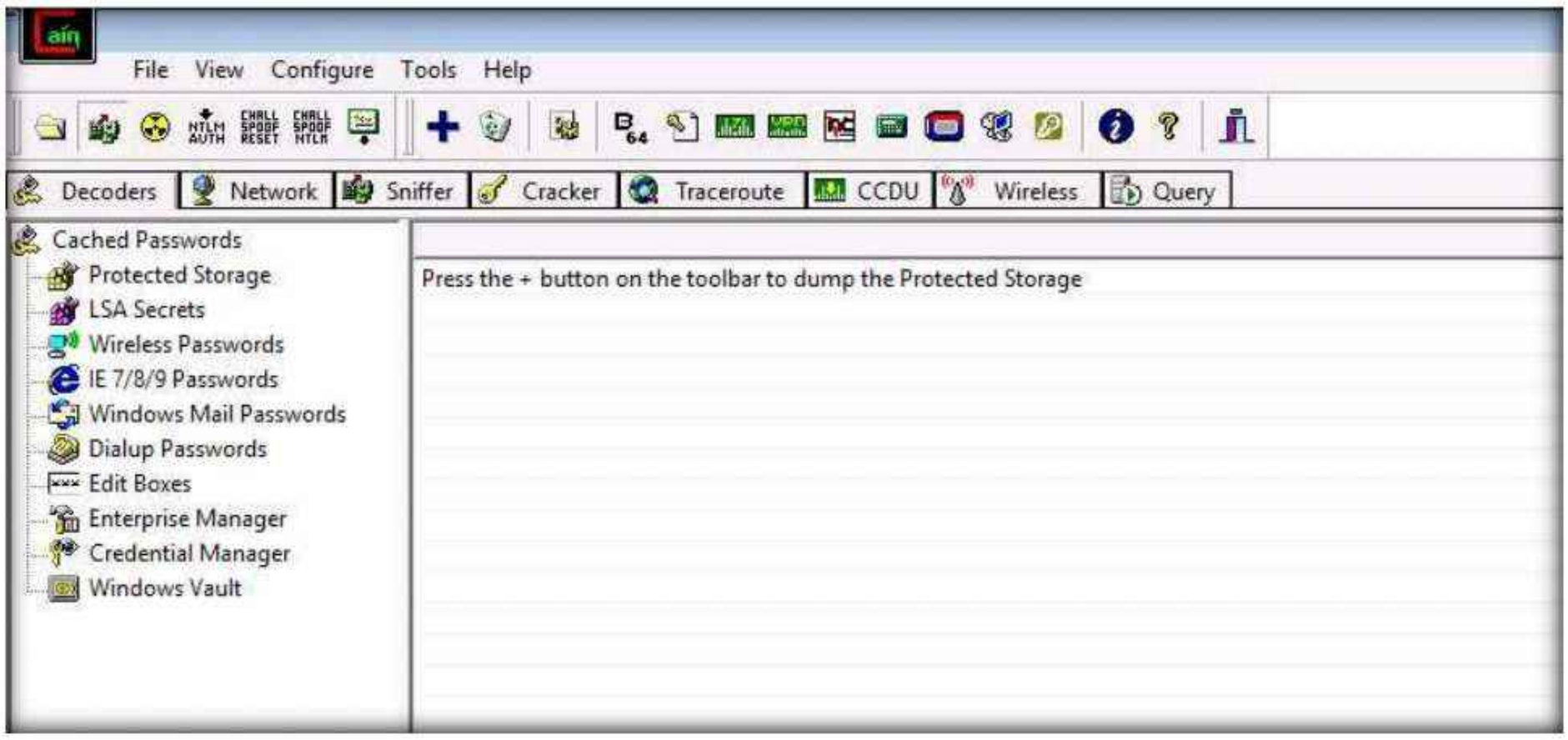
4. Click **Configure** from the menu bar to configure an ethernet card.



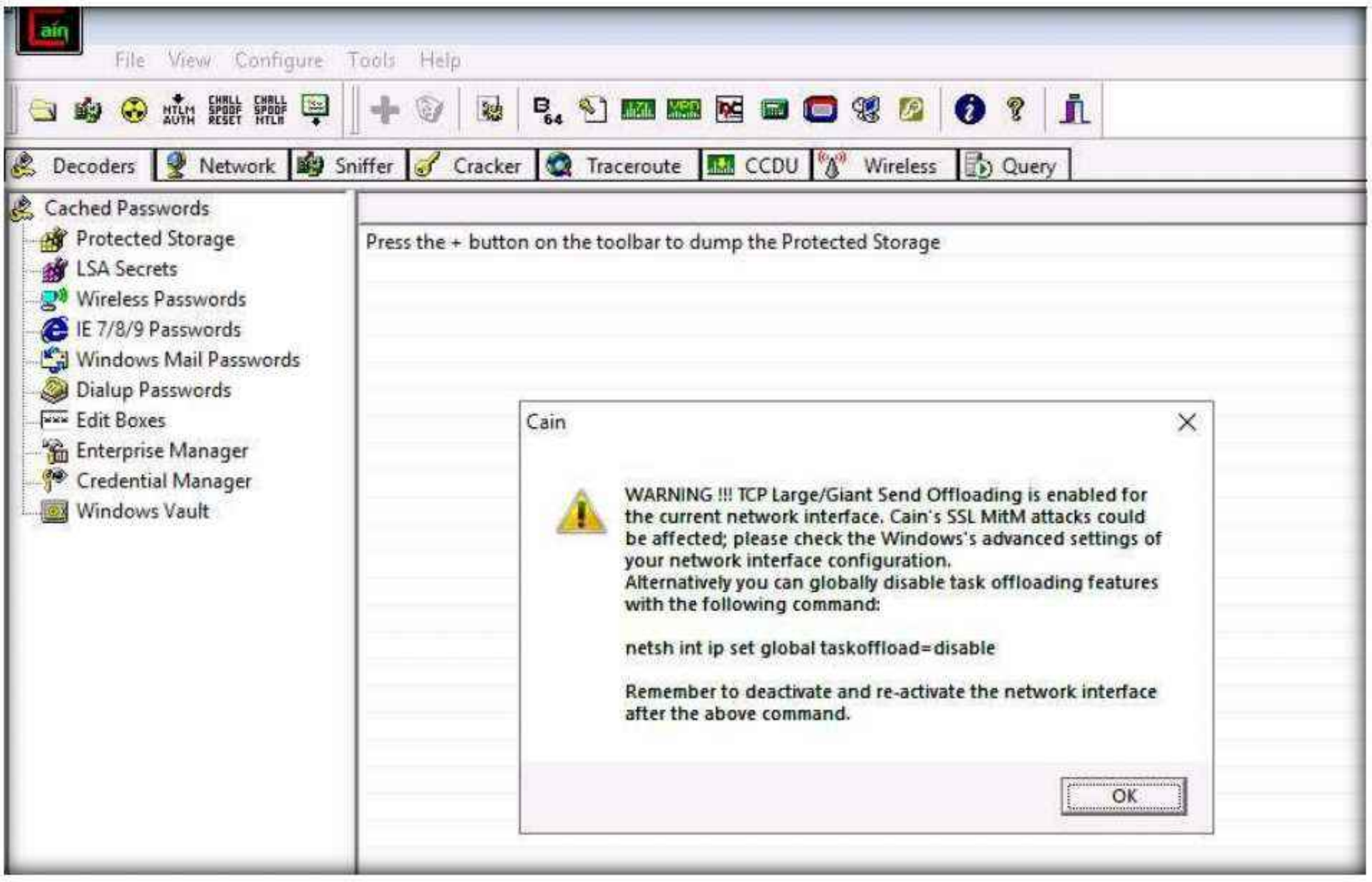
5. The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.



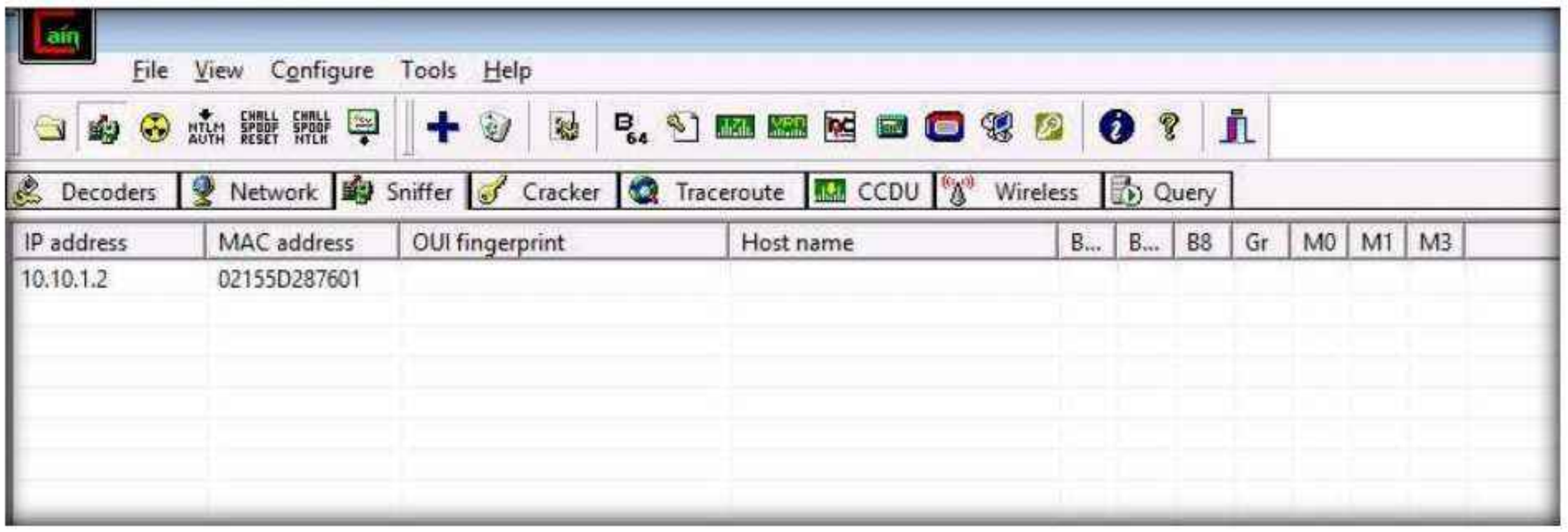
6. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



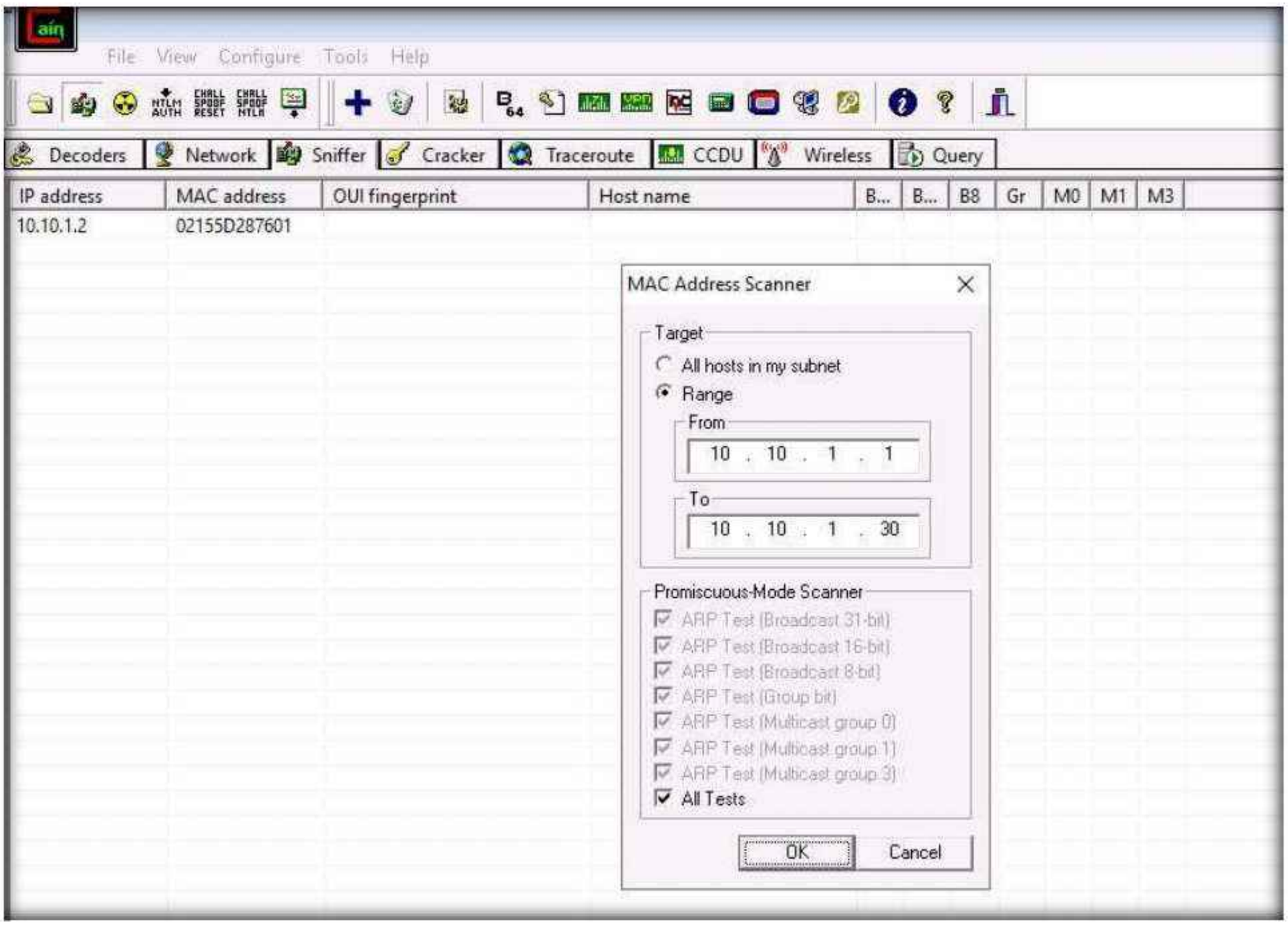
7. The **Cain** pop-up appears with a **Warning** message, click **OK**.



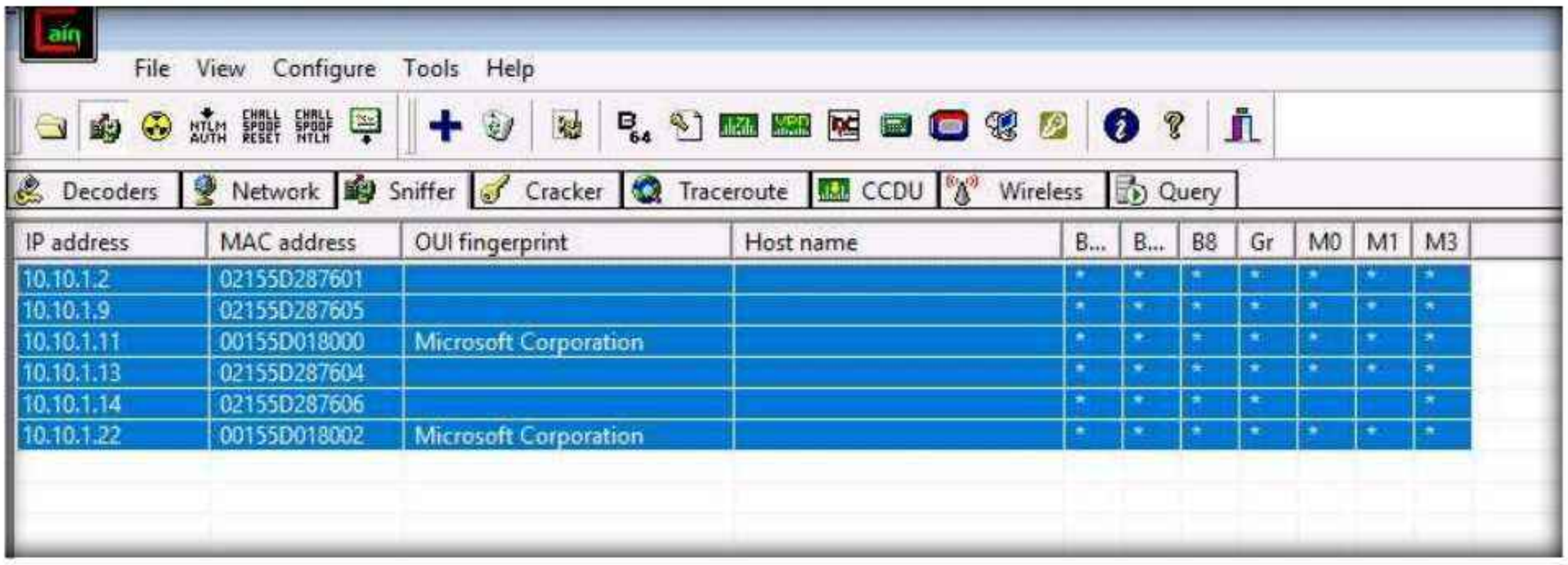
8. Now, click the **Sniffer** tab.



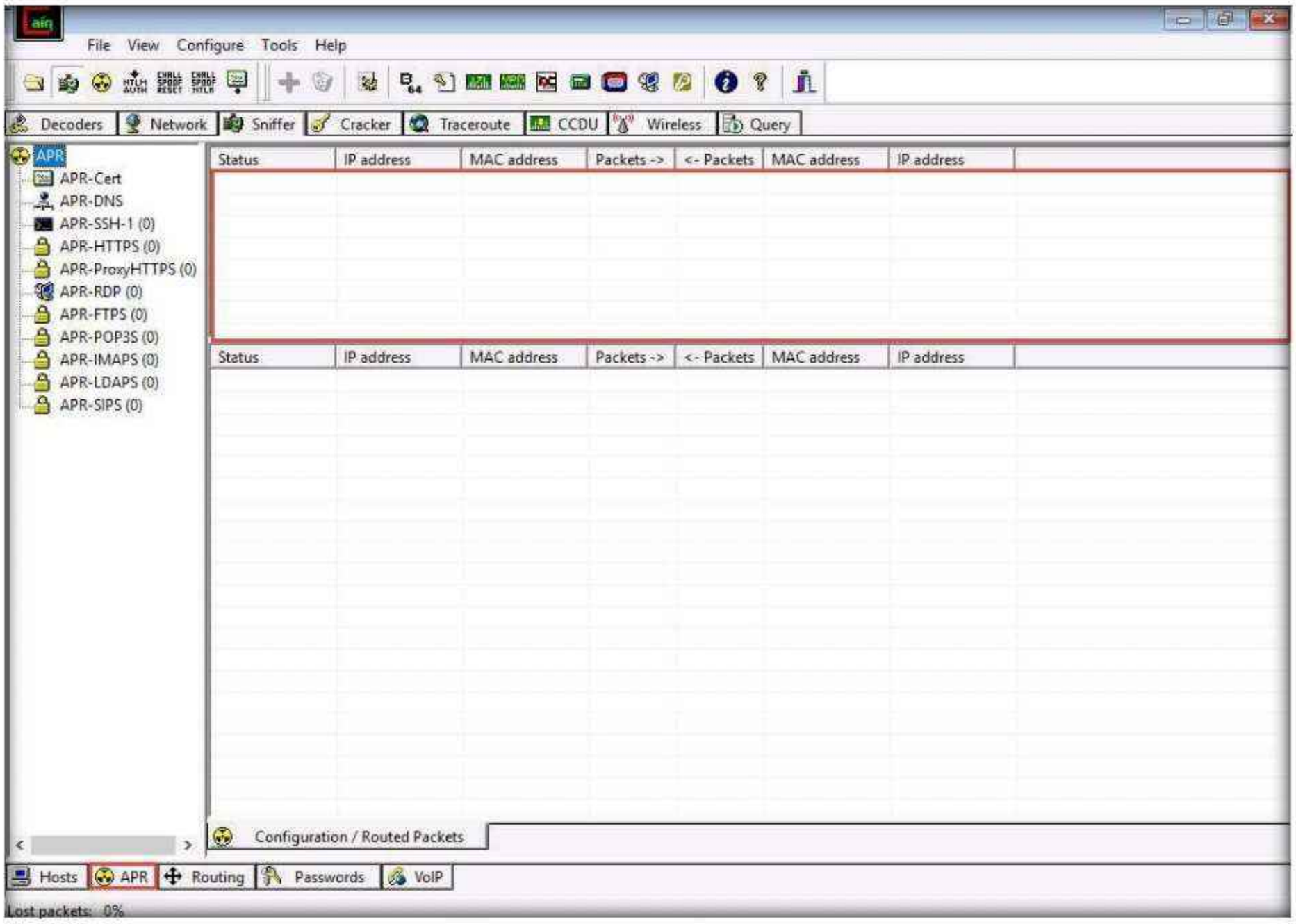
9. Click the plus (**+**) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
10. The **MAC Address Scanner** window appears. Check **the Range** radio button and specify the IP address range as **10.10.1.1-10.10.1.30**. Select the **All Tests** checkbox; then, click **OK**.



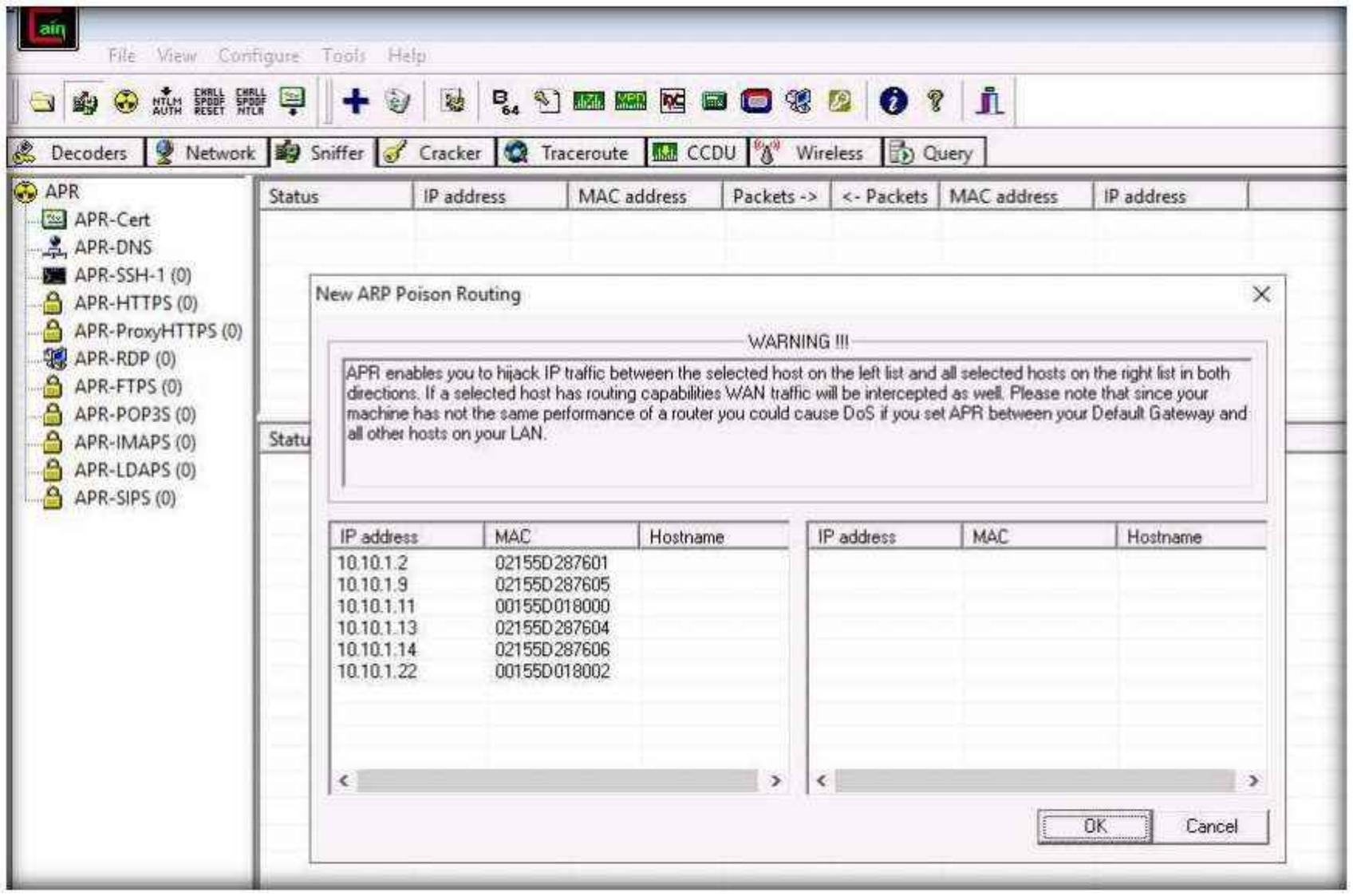
11. Cain & Abel starts scanning for MAC addresses and lists all those found.
12. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.



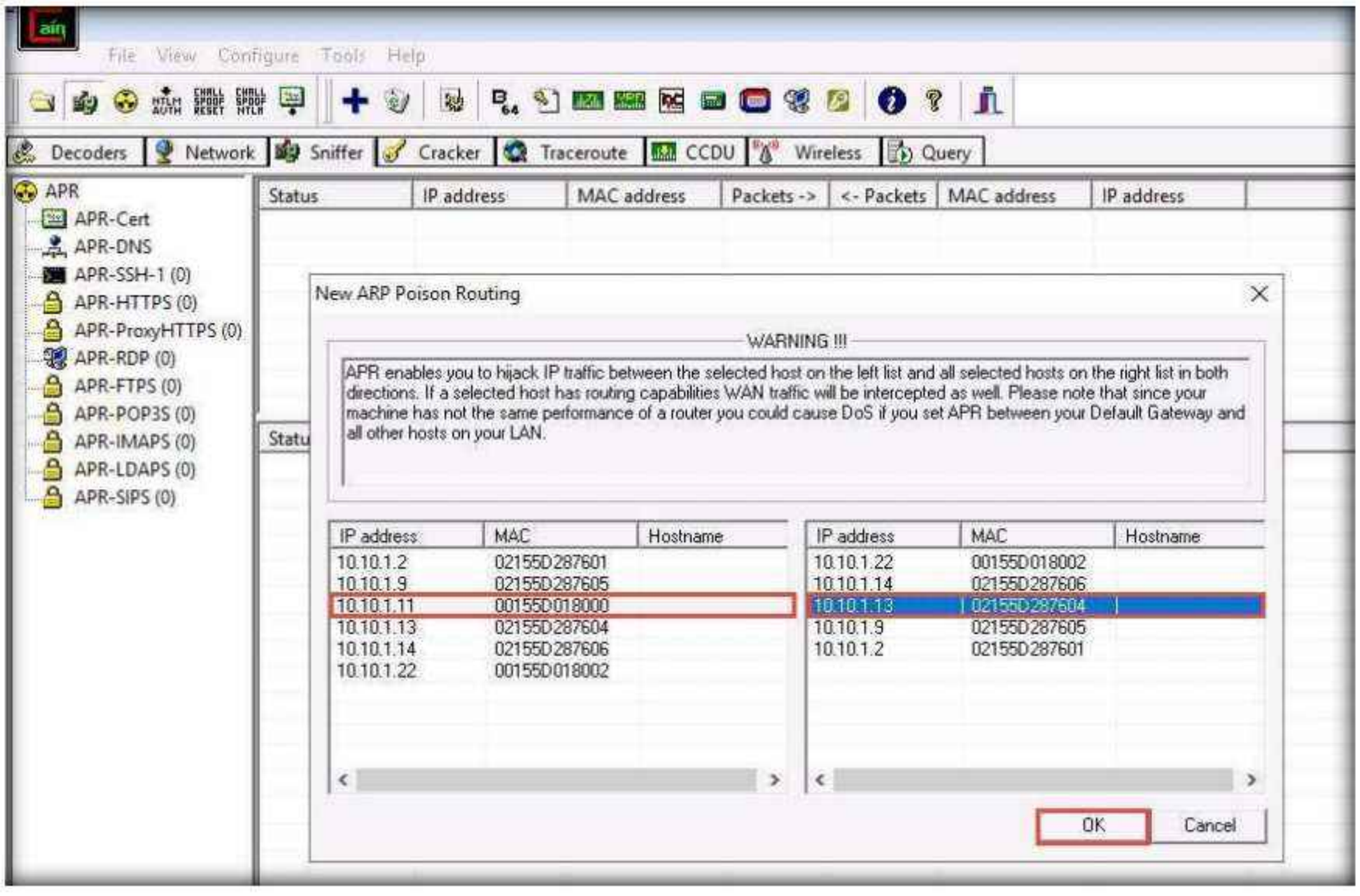
13. Now, click the **APR** tab at the bottom of the window.
14. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.



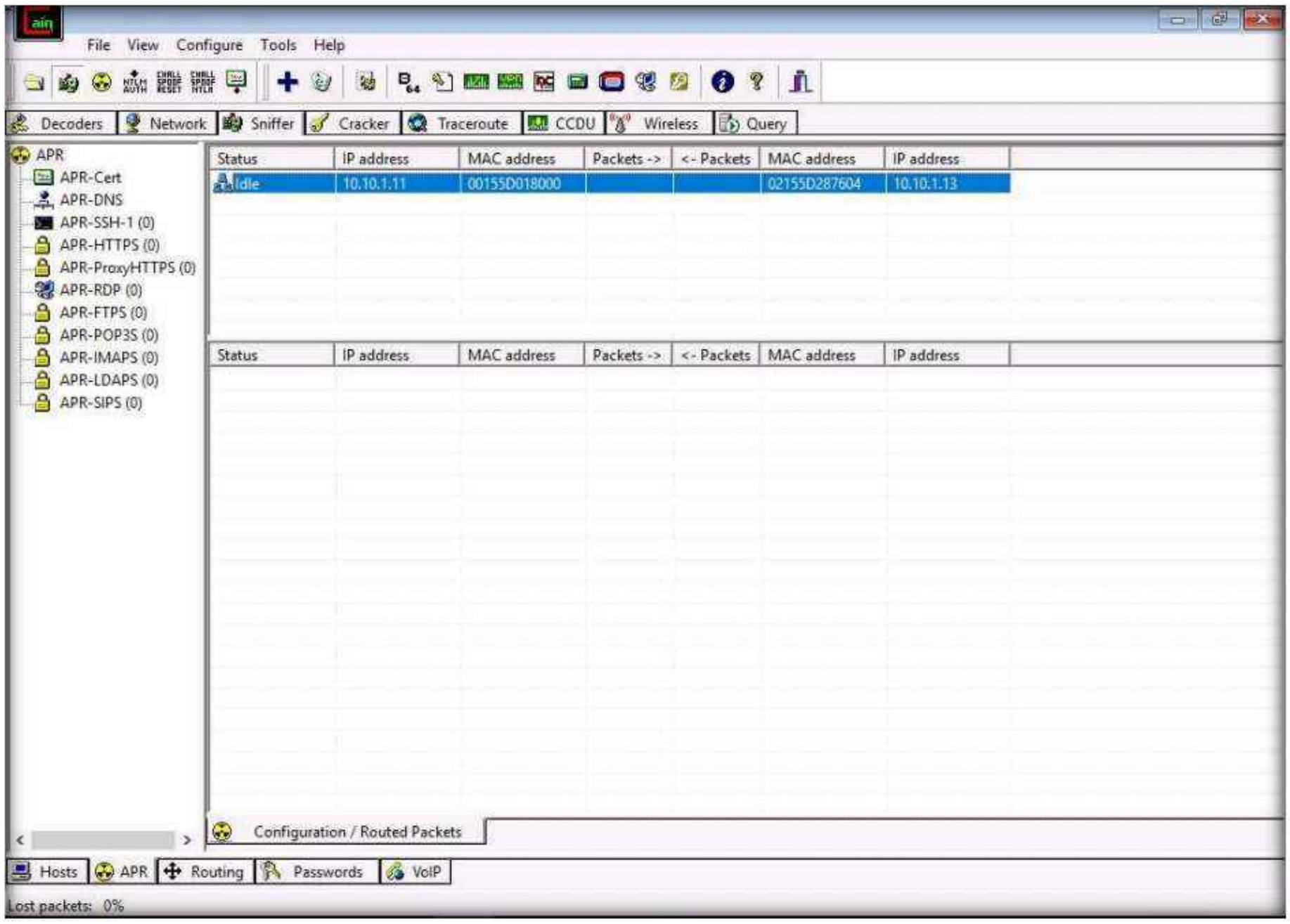
15. Click the plus (**+**) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.



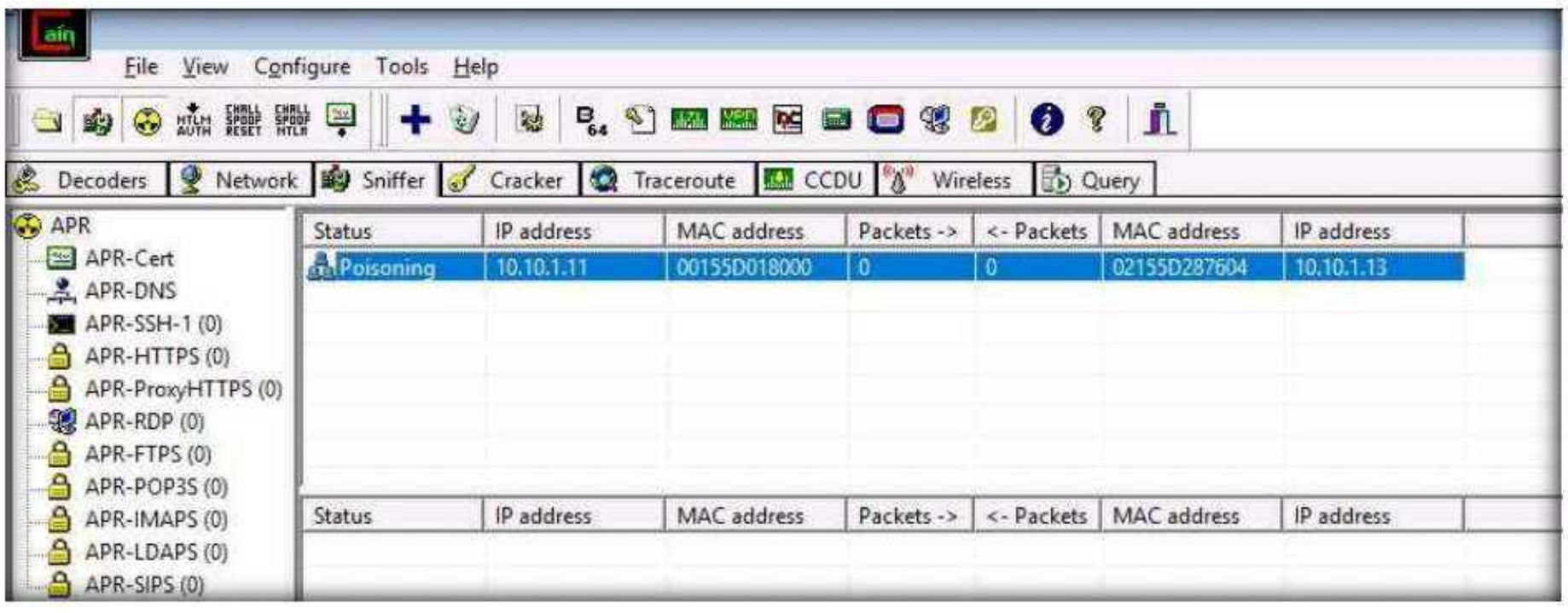
16. To monitor the traffic between two systems (here, **Windows 11** and **Parrot Security**), from the left-hand pane, click to select **10.10.1.11** (**Windows 11**) and from the right-hand pane, click **10.10.1.13** (**Parrot Security**); click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.



17. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.
18. Click on the **Start/Stop APR** icon to start capturing ARP packets.



19. After clicking on the **Start/Stop APR** icon, Cain & Abel starts ARP **poisoning** and the status of the scan changes to Poisoning, as shown in the screenshot.



20. Cain & Abel intercepts the traffic traversing between these two machines.
21. To generate traffic between the machines, you need to ping one target machine using the other.
22. Switch to the **Parrot Security** virtual machine.

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

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

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

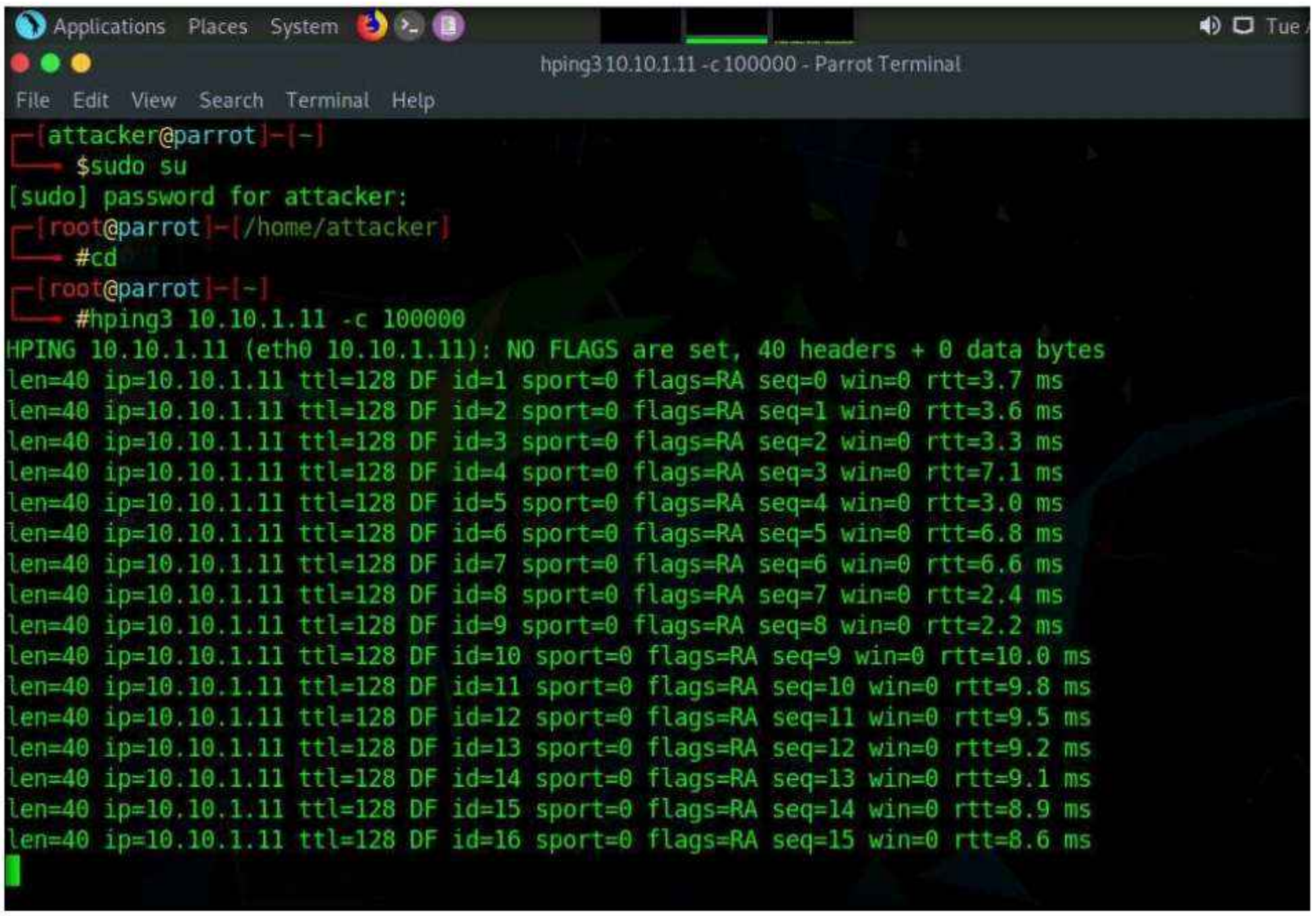
24. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
25. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
26. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

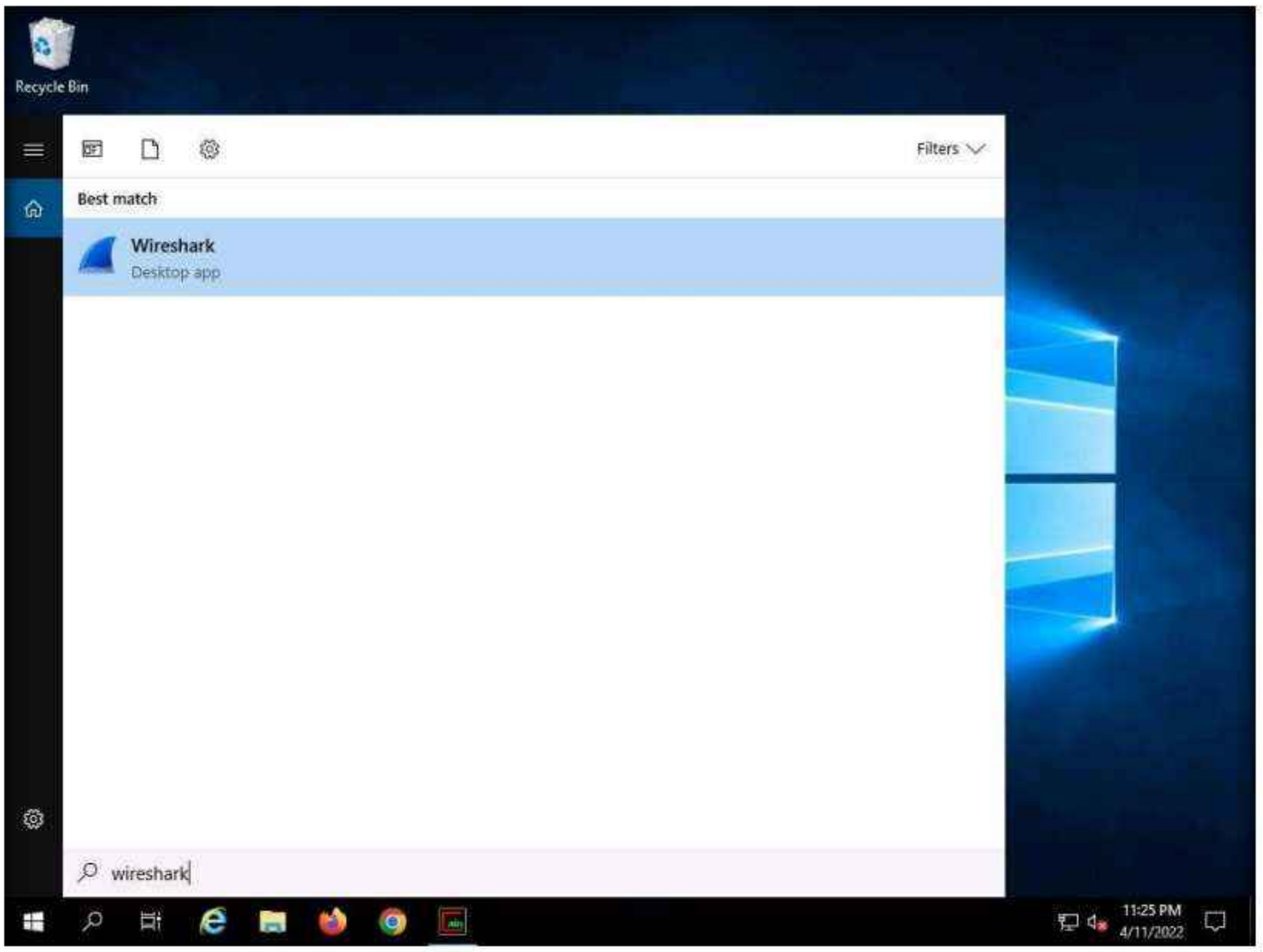
27. Now, type **cd** and press **Enter** to jump to the root directory.
28. A **Parrot Terminal** window appears; type **hping3 [Target IP Address] -c 100000** (here, target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

    Note: **-c**: specifies the packet count.

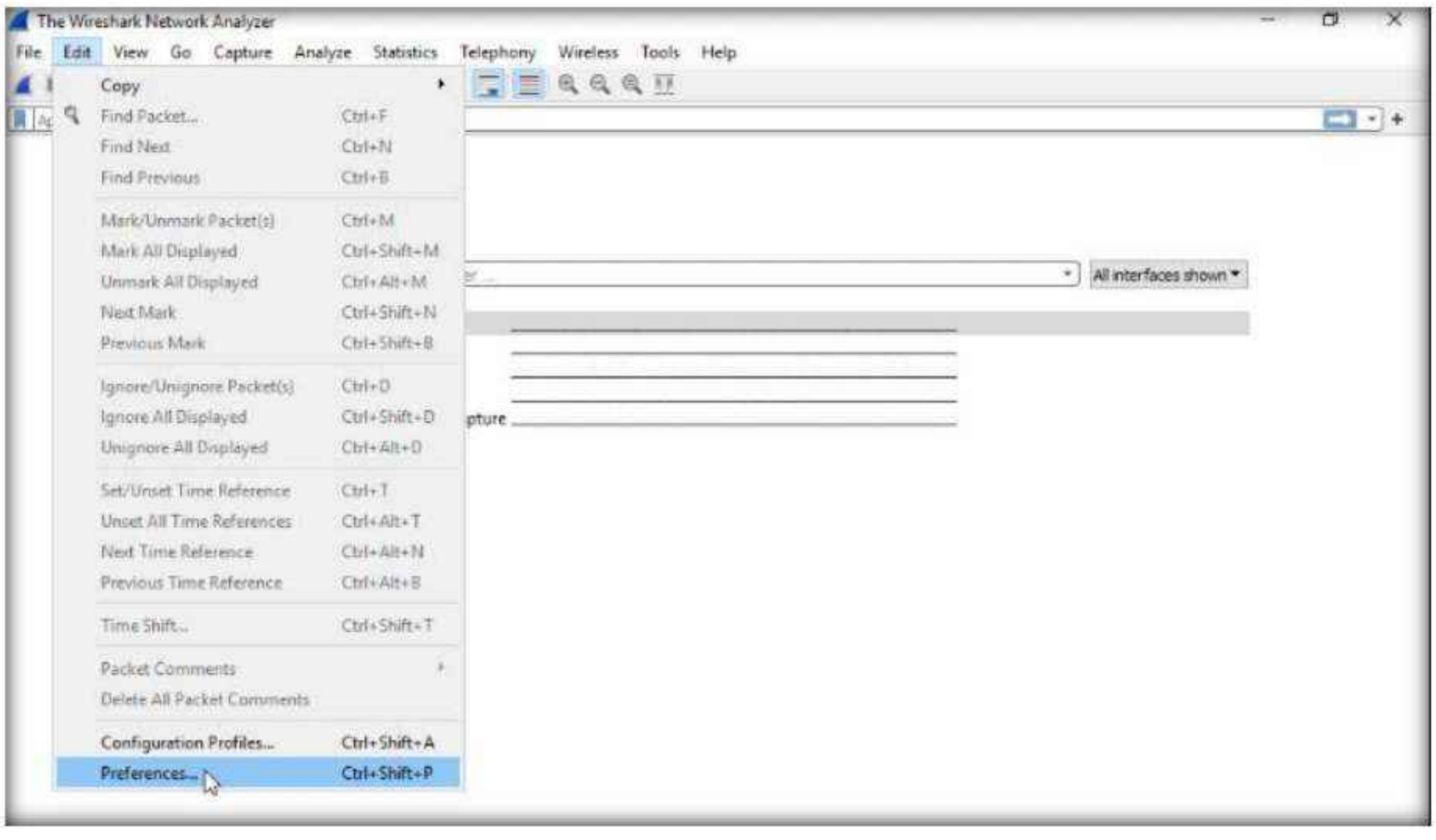
29. This command will start pinging the target machine (**Windows 11**) with 100,000 packets.



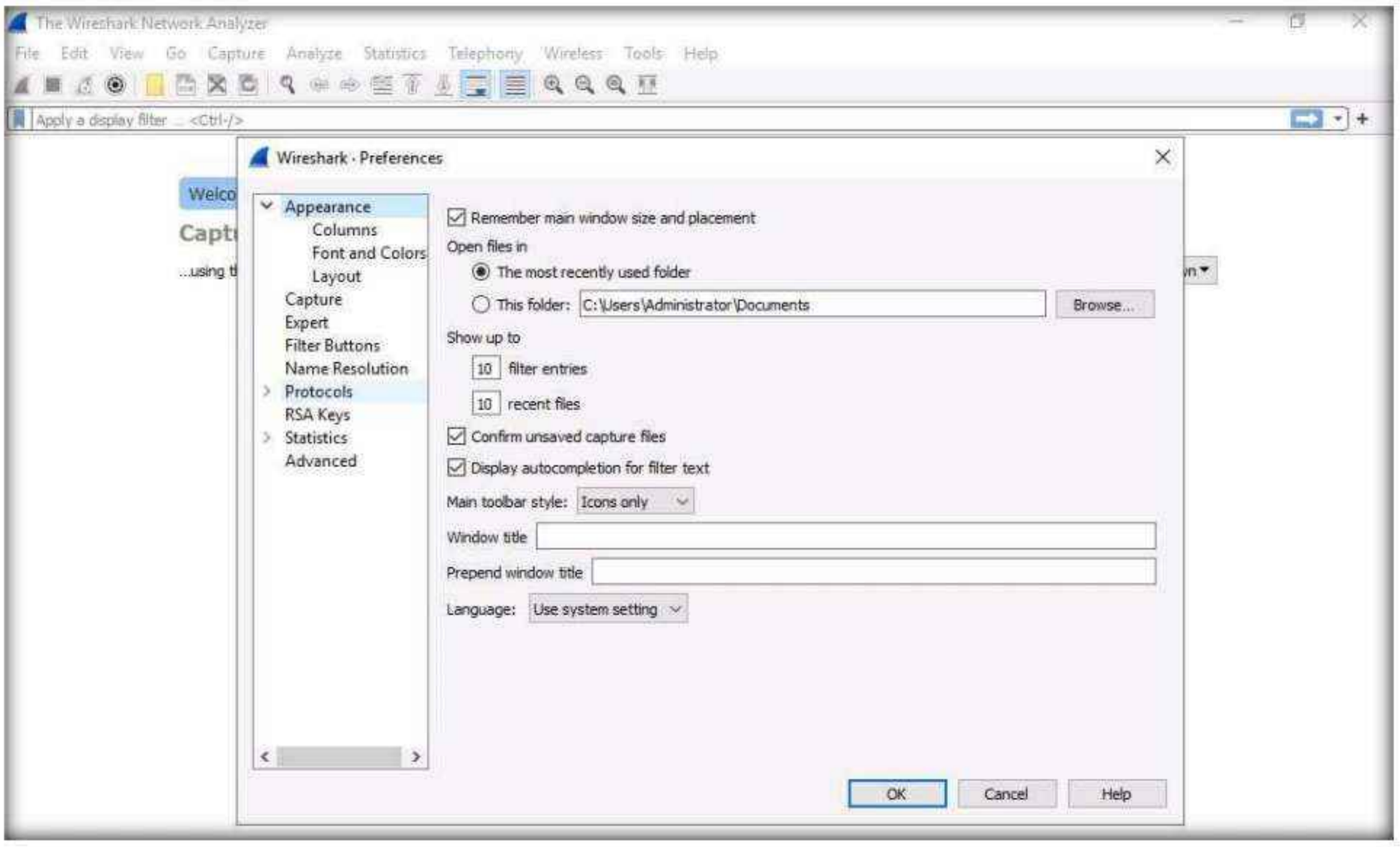
30. Leave the command running and immediately switch to the **Windows Server 2019** virtual machine.
31. Click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.



32. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences…**.

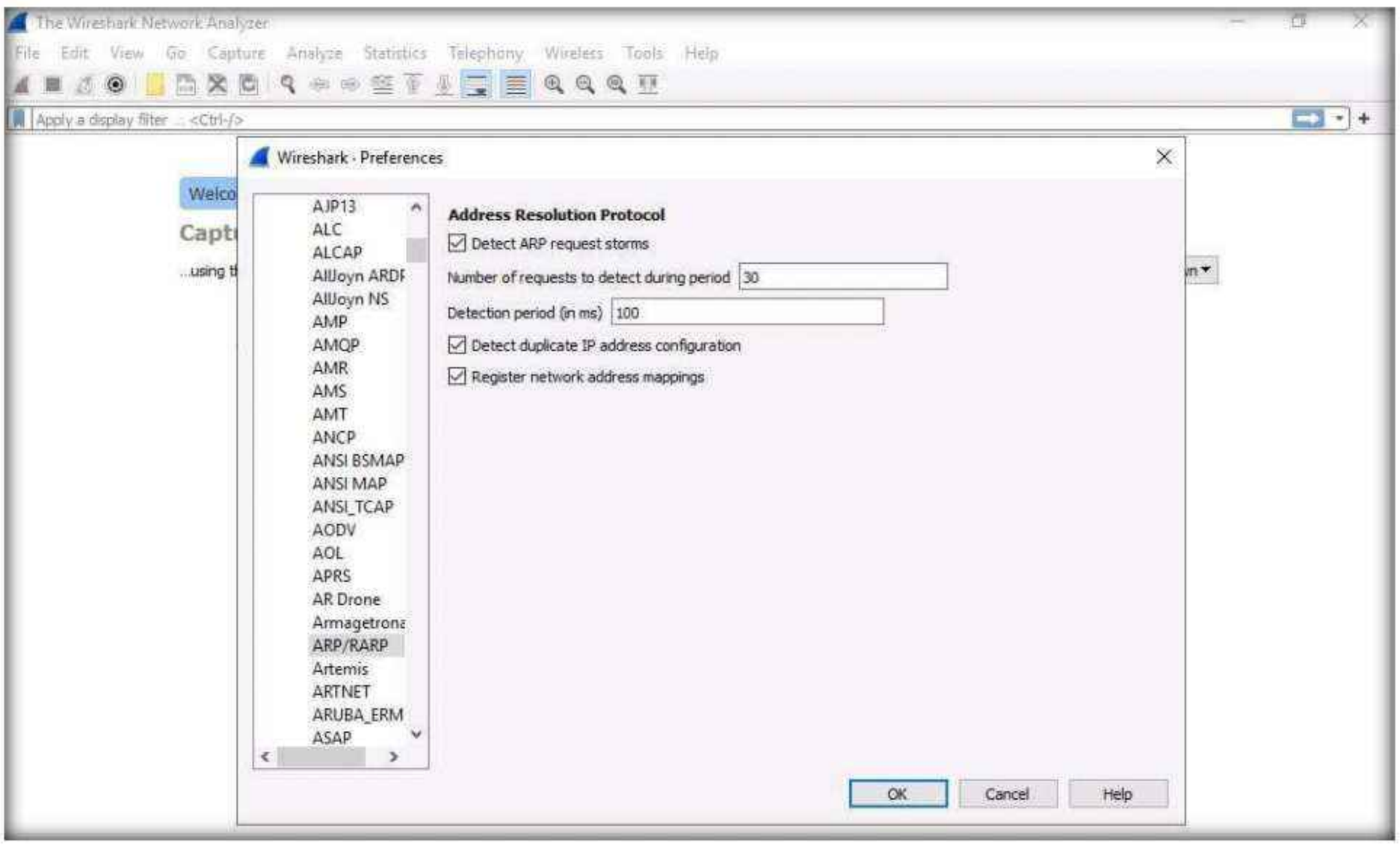


33. The **Wireshark . Preferences** window appears; expand the **Protocols** node.

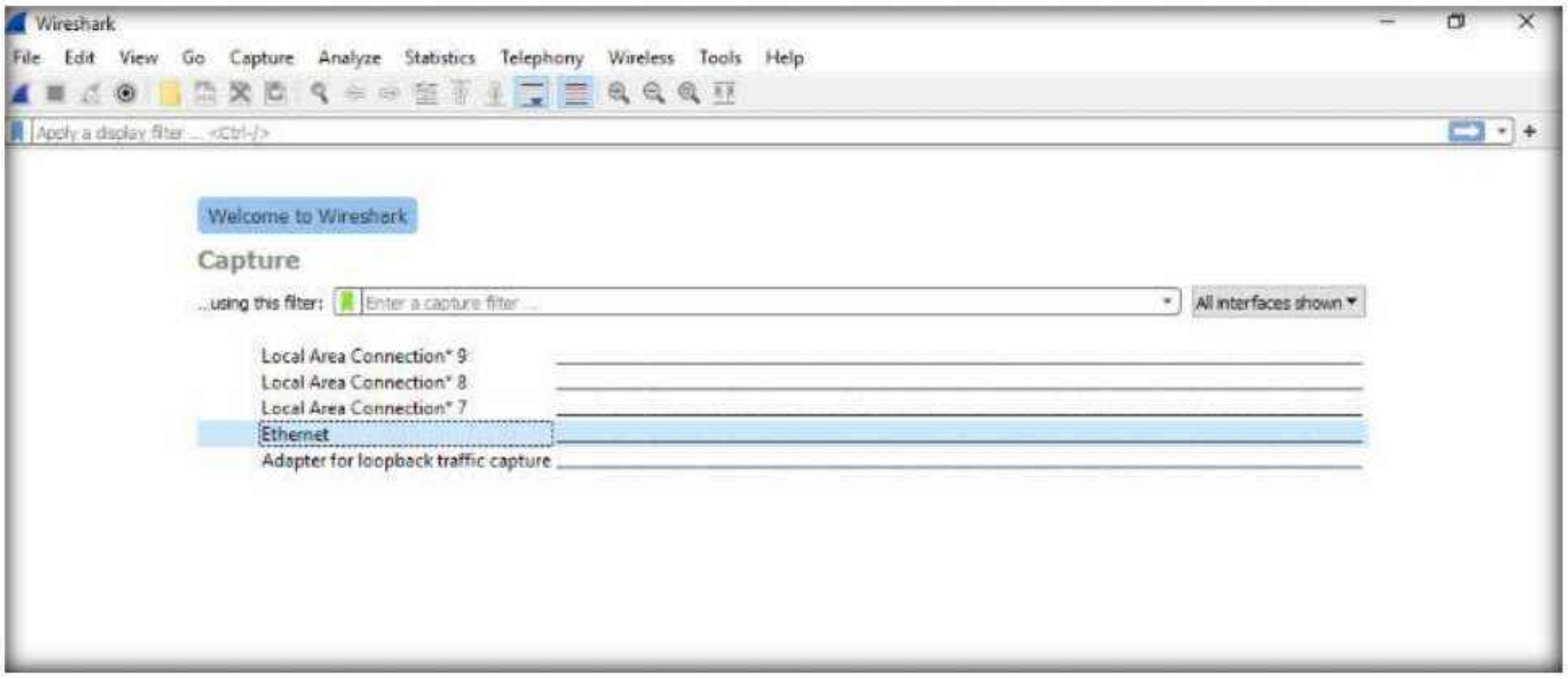


34. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.

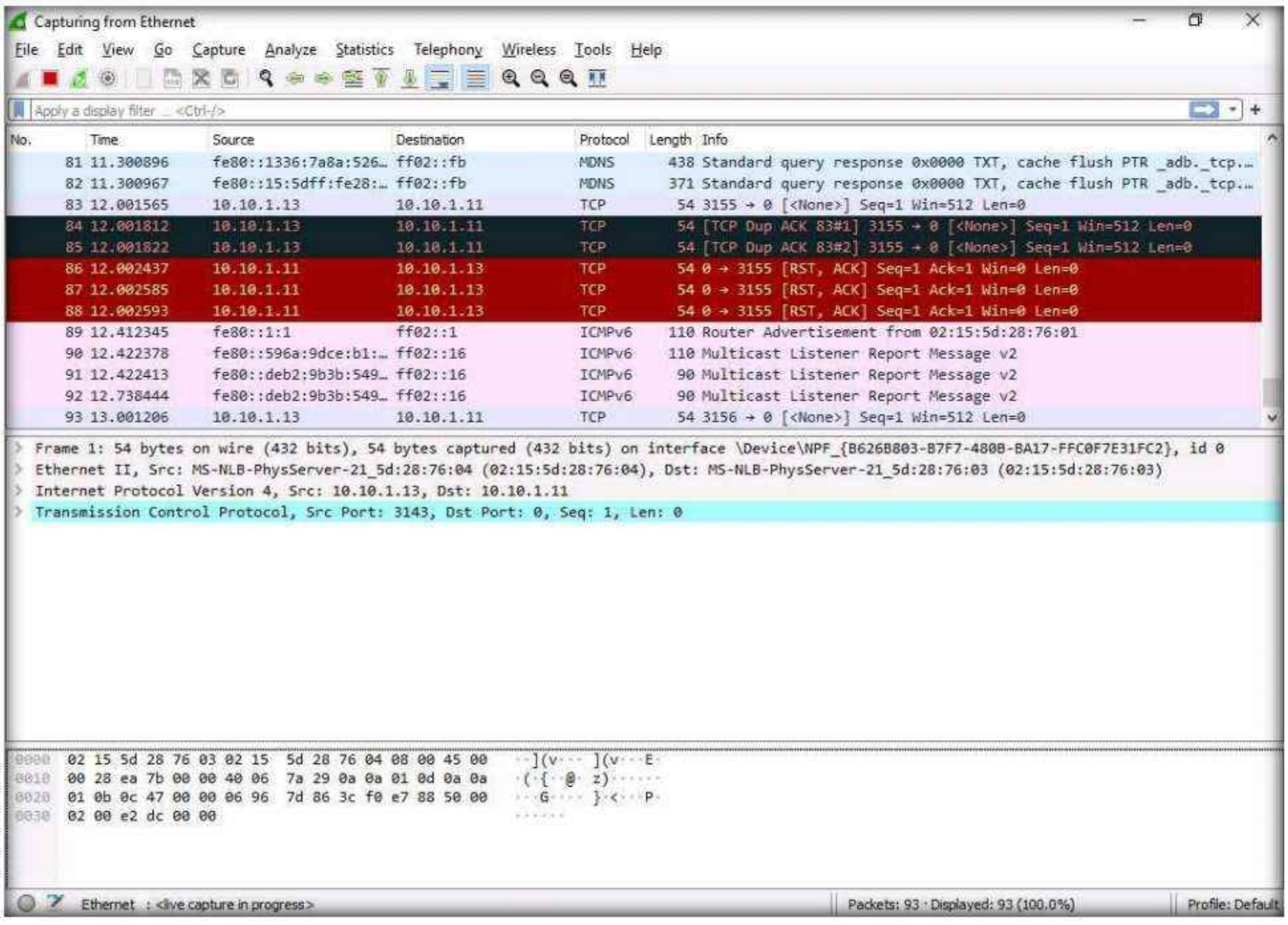
35. From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.



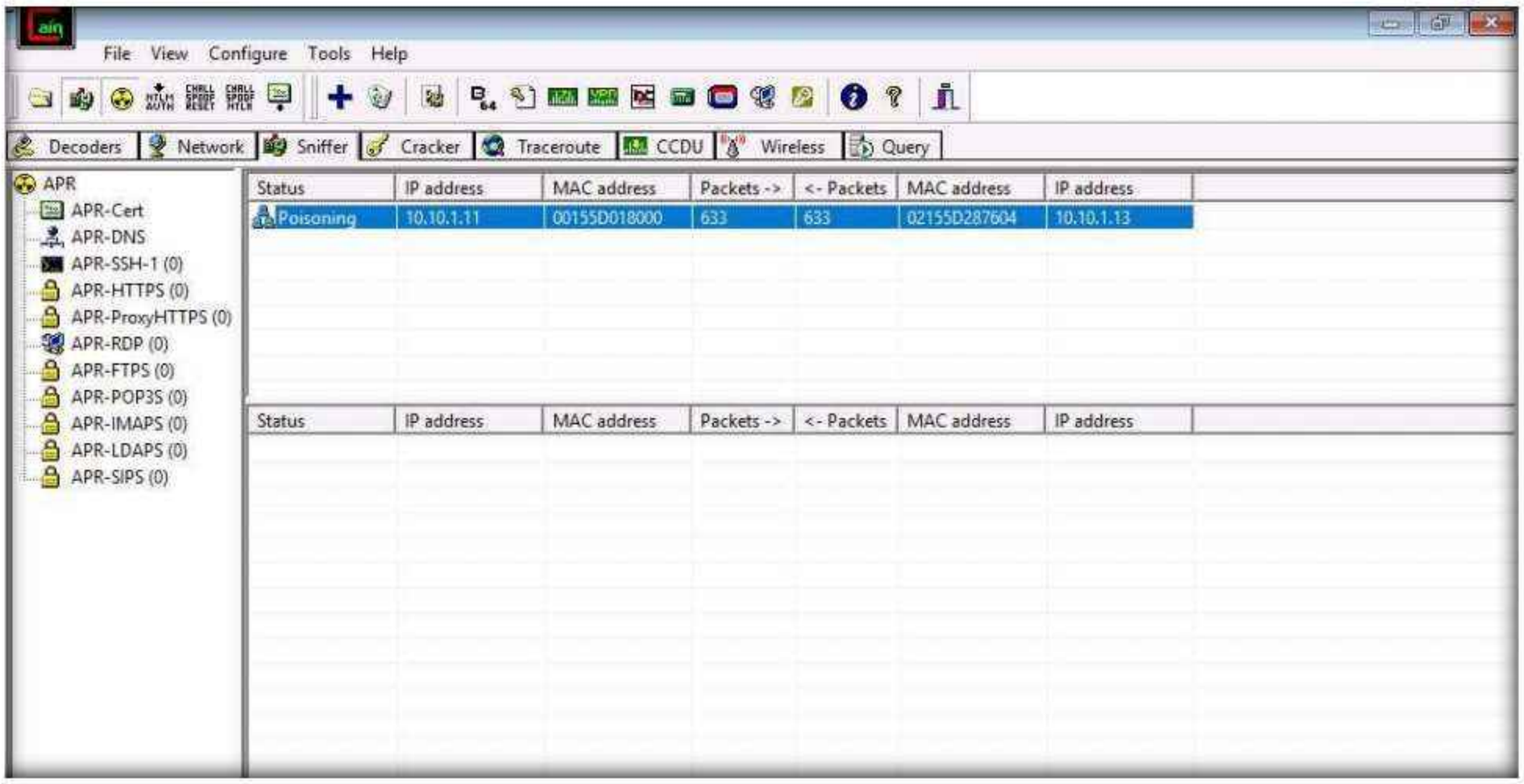
36. Now, double-click on the adapter associated with your network (here, **Ethernet**) to start capturing the network packets.



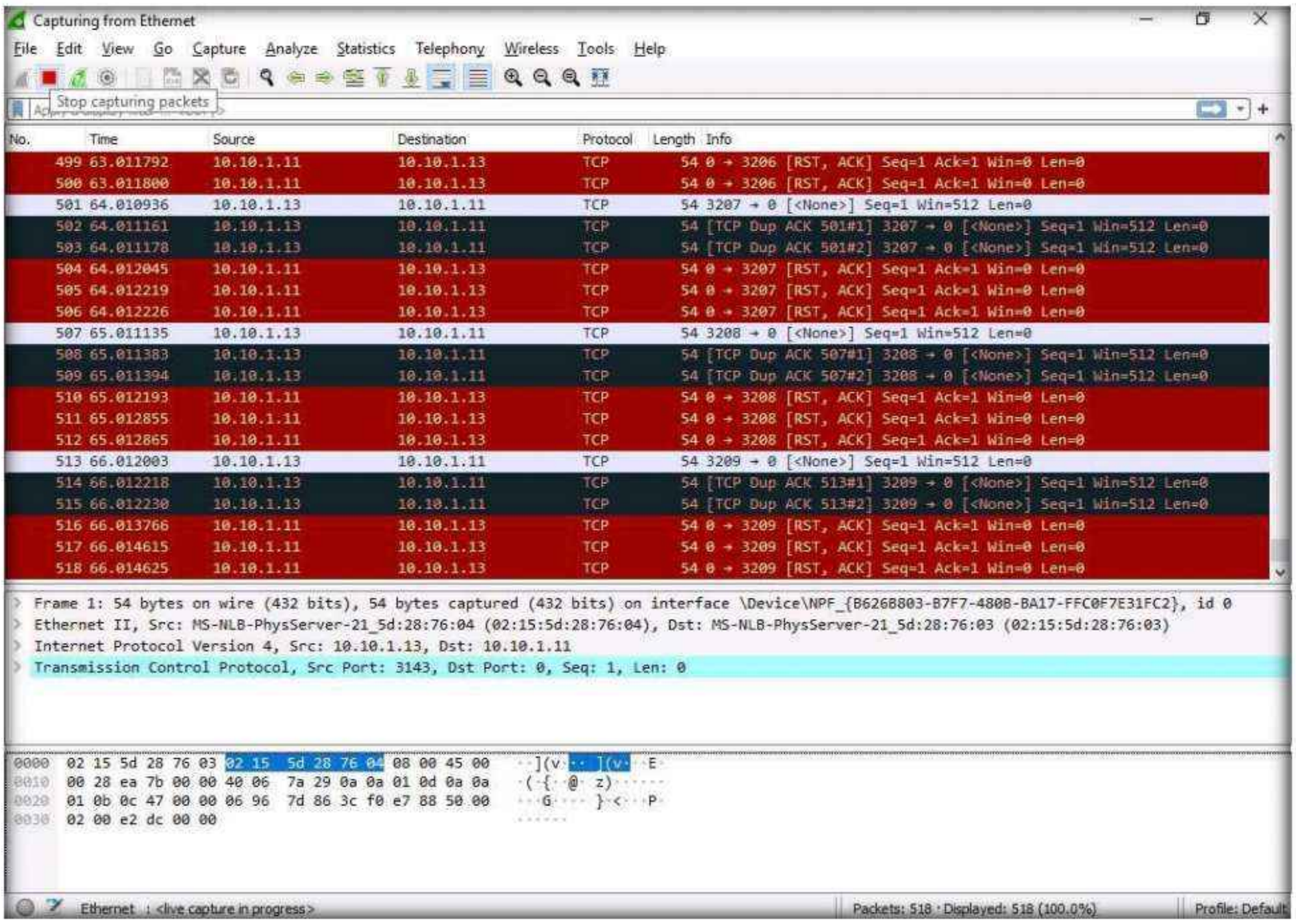
37. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.



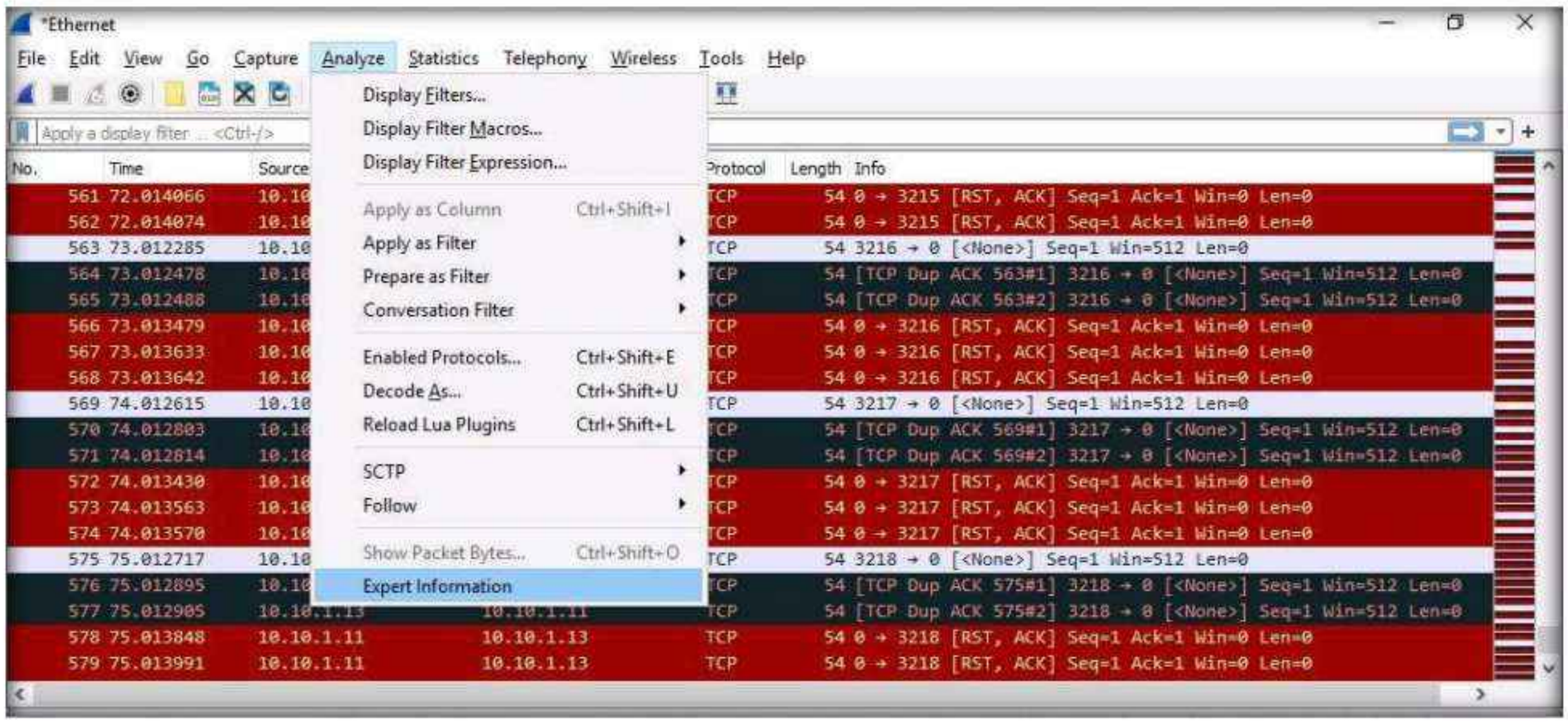
38. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.



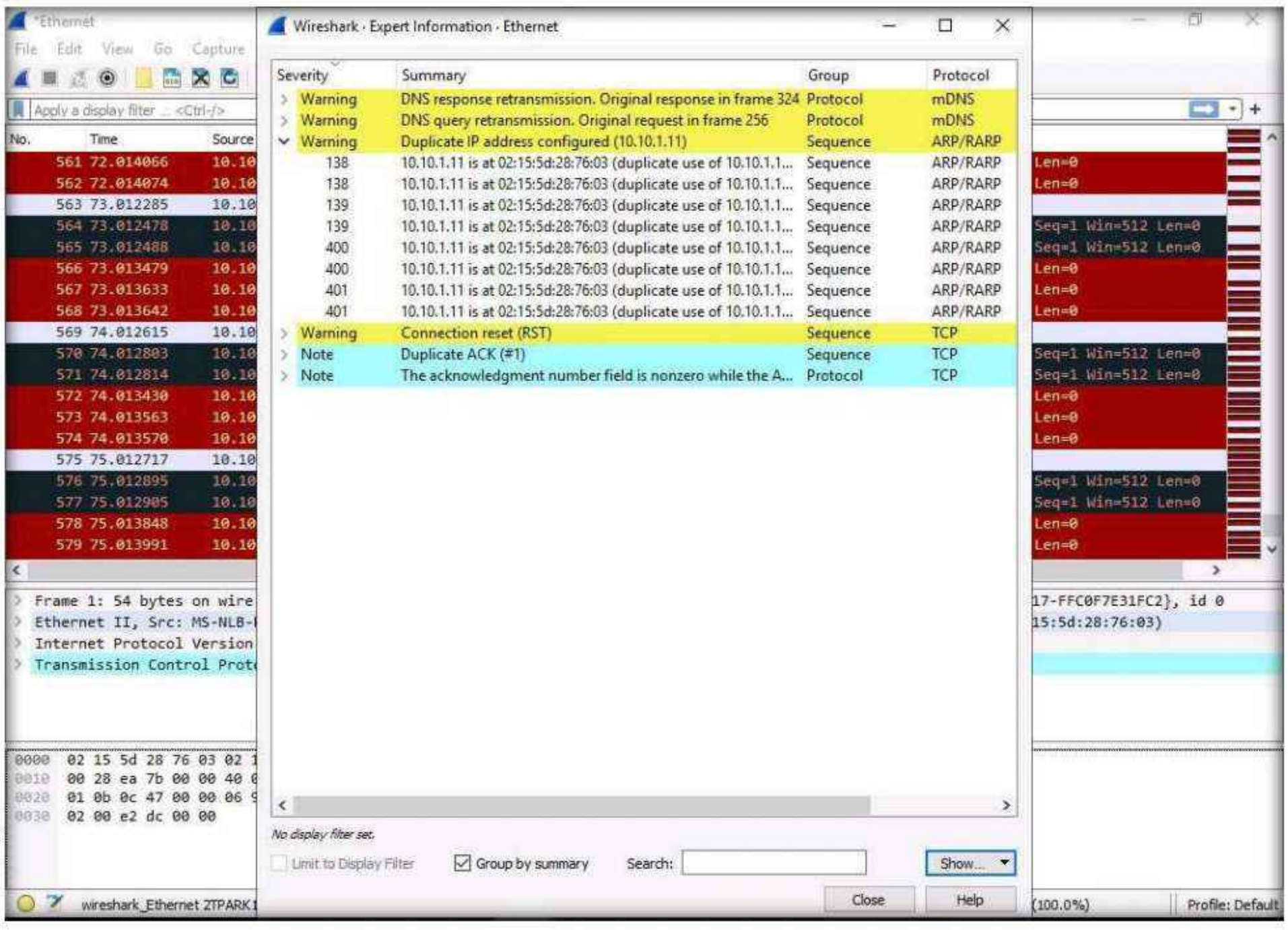
39. Now, switch to **Wireshark** and click the **Stop packet capturing** icon to stop the packet capturing.



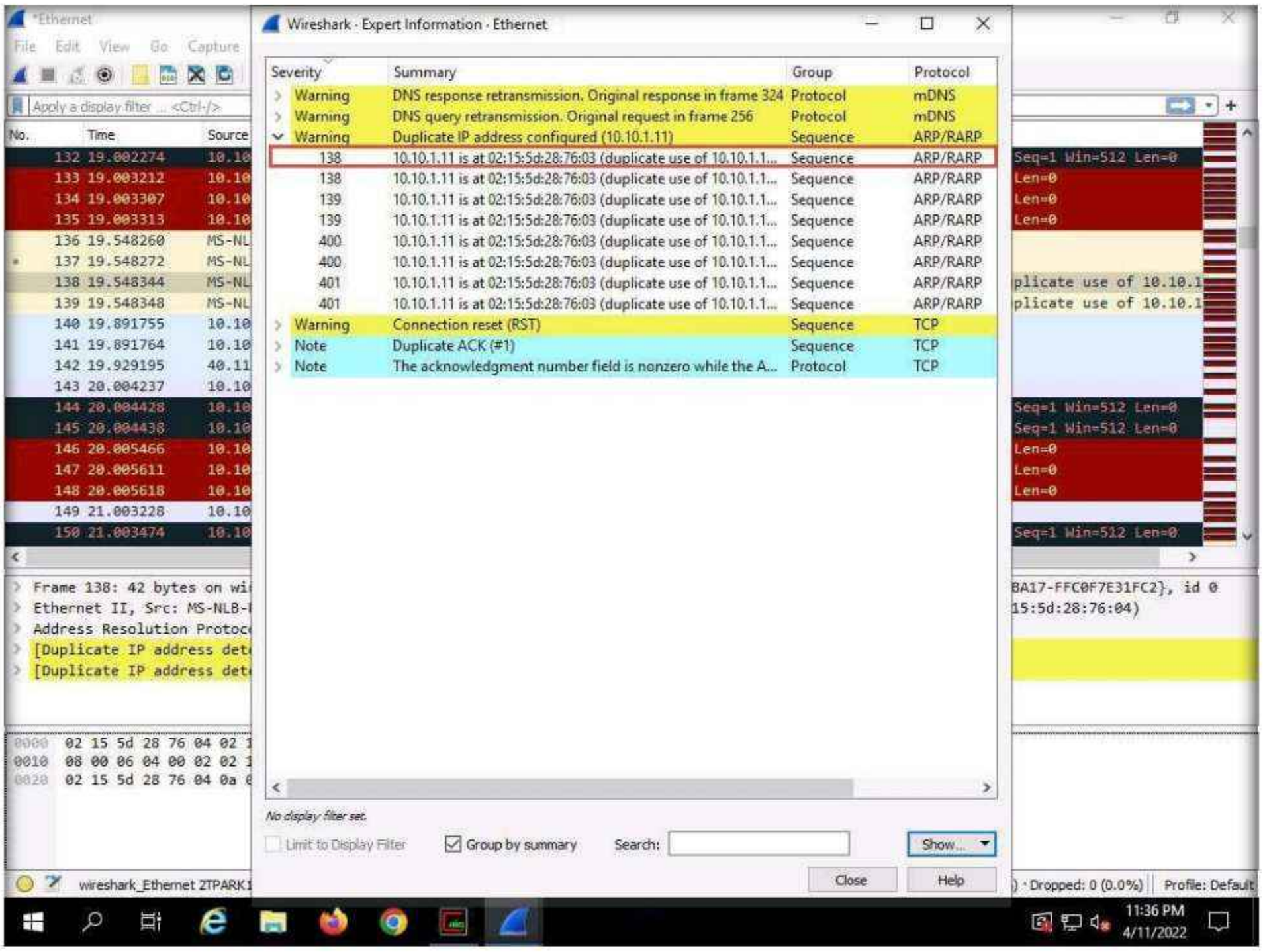
40. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.



41. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.1.11)**, running on the **ARP/RARP** protocol.

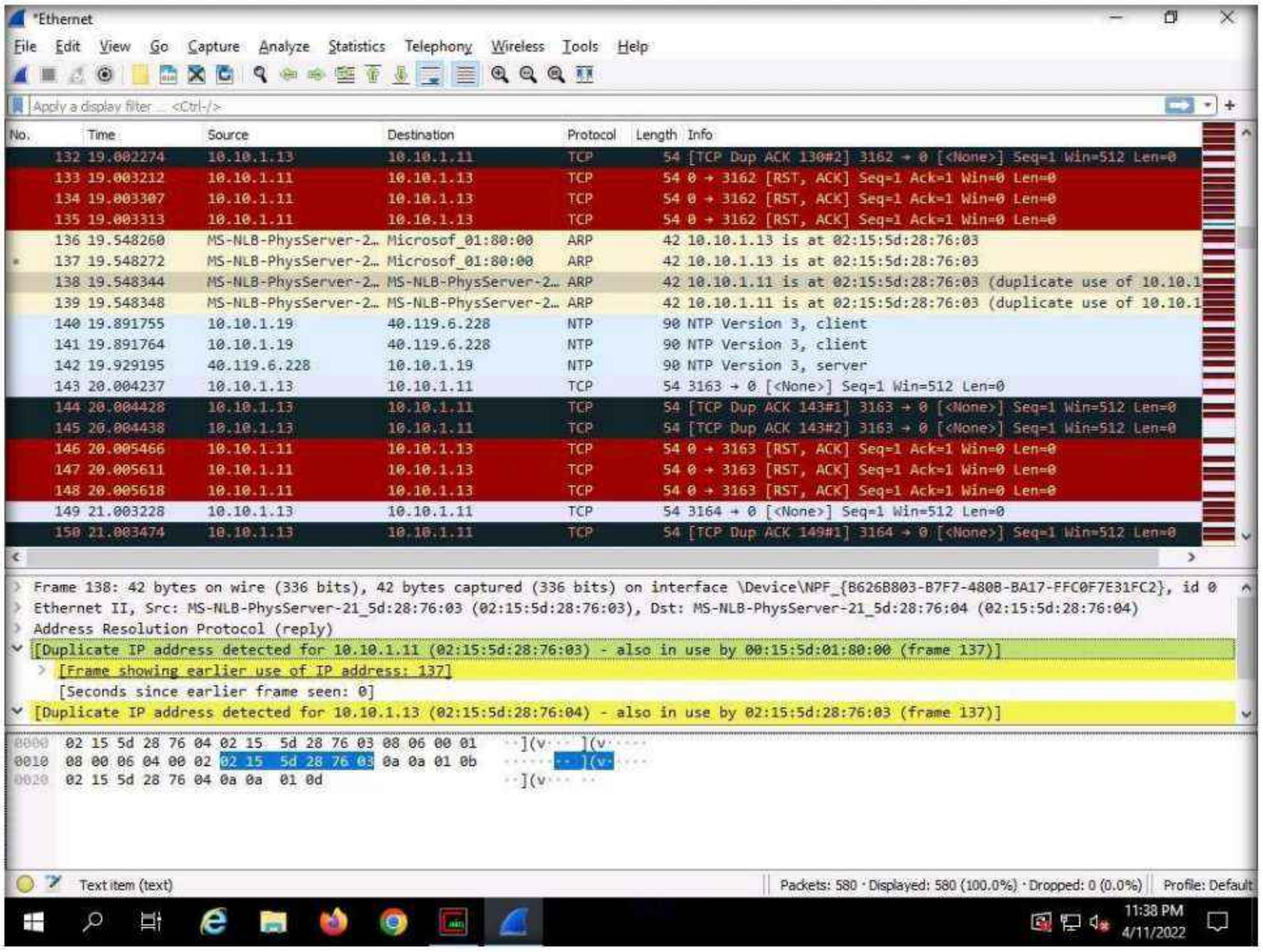


42. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.
43. In the **Wireshark . Expert Information** window, click any packet (here, **138**).



44. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section. Close the **Wireshark . Expert Information** window.

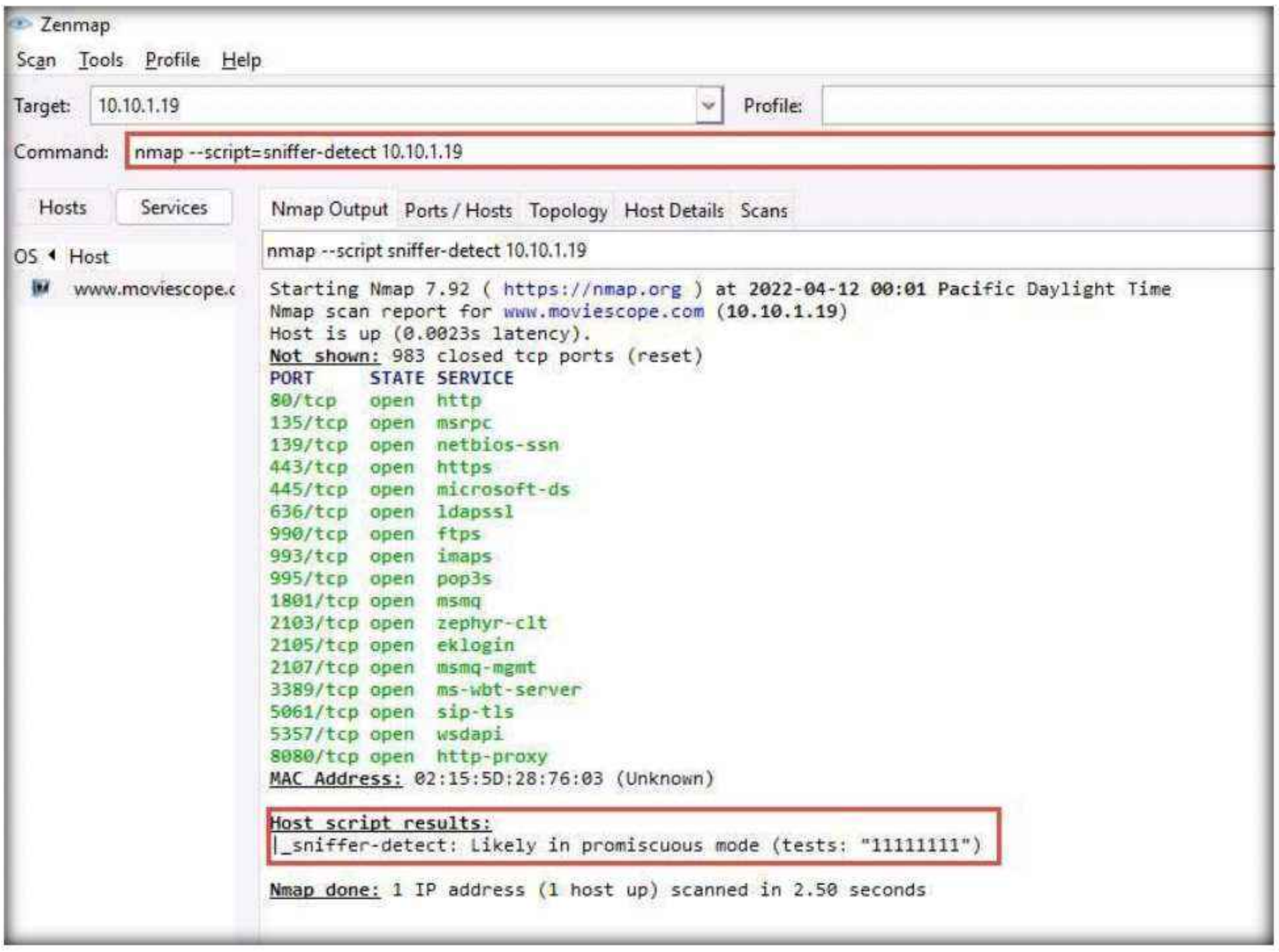
45. The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot.



Note: ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. At this point, the attacker can launch a DoS attack by associating a non-existent MAC address with the IP address of the gateway or may passively sniff the traffic, and then forward it to the target destination.

46. This concludes the demonstration of detecting ARP poisoning in a switch-based network.
47. Close the **Wireshark** window and leave all other windows running.
48. Now, we shall perform promiscuous mode detection using **Nmap**.
49. Now, switch to the **Windows 11** virtual machine. Click **Search** icon () on the **Desktop**. Type **zenmap** in the search field, the **Nmap - Zenmap GUI** appears in the results, click **Open** to launch it.

50. The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect [Target IP Address/ IP Address Range]** (here, target IP address is **10.10.1.19 [Windows Server 2019]**) and click **Scan**.
51. The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. This indicates that the target system is in promiscuous mode.



52. Close the **Nmap** tool window and document all the acquired information.
53. Close all open windows in all machines (ensure that ARP poisoning is not running in **Windows Server 2019**), and document all the acquired information.

Task 2: Detect ARP Poisoning using the Capsa Network Analyzer

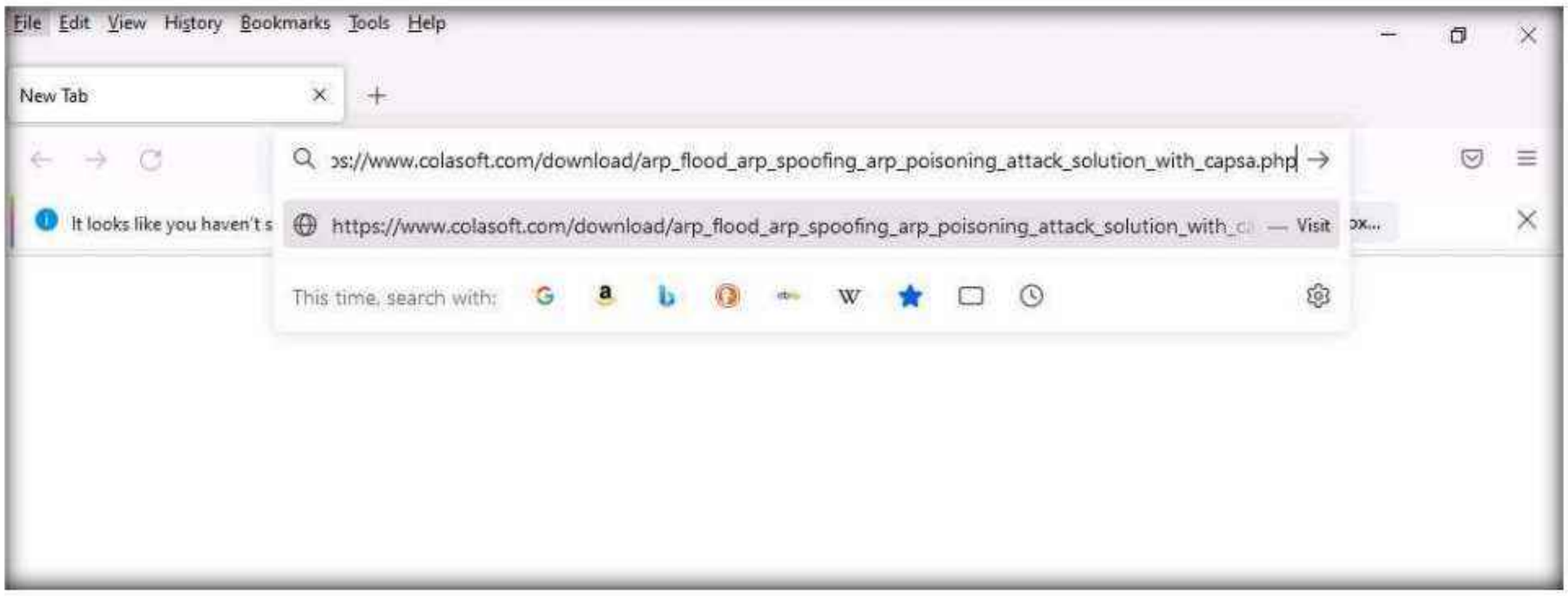
Capsa Network Analyzer

Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis capabilities with an easy-to-use interface that allows users to protect and monitor networks in a critical business environment. It helps ethical hackers or pen testers in quickly detecting ARP poisoning and ARP flooding attack and in locating attack source.

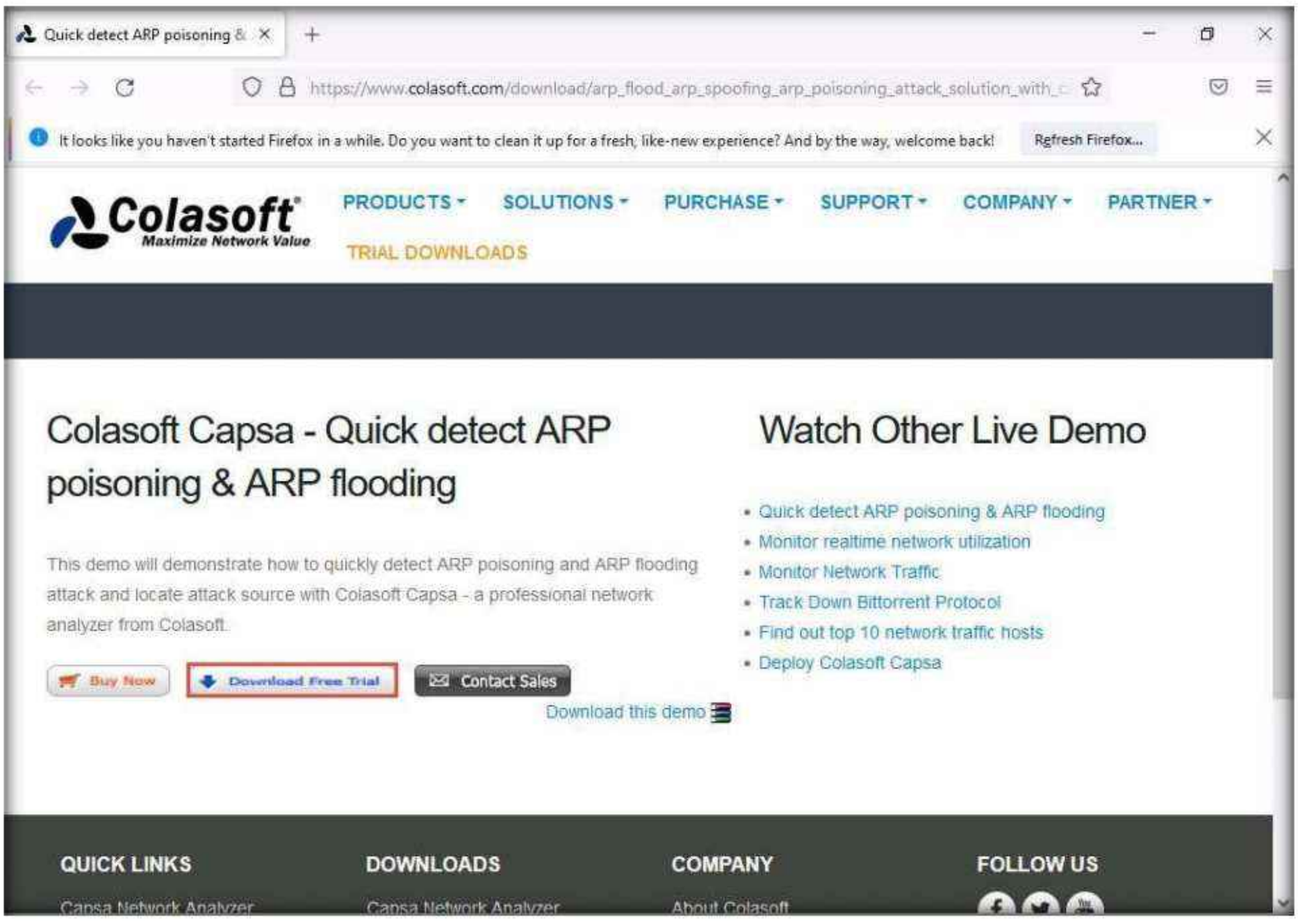
Habu: Habu is an open-source penetration testing toolkit that can perform various tasks such as ARP poisoning, ARP sniffing, DHCP starvation and DHCP discovers.

Here, we will use Habu tool to perform ARP poisoning attack on the target system and use Capsa Network Analyzer to detect the attack.

1. Switch to the **Windows 11** virtual machine.
2. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar, type **https://www.colasoft.com/download/arp_flood_arp_spoofing_arp_poisoning_attack_solution_with_capsa.php** in the address bar, and press **Enter**.

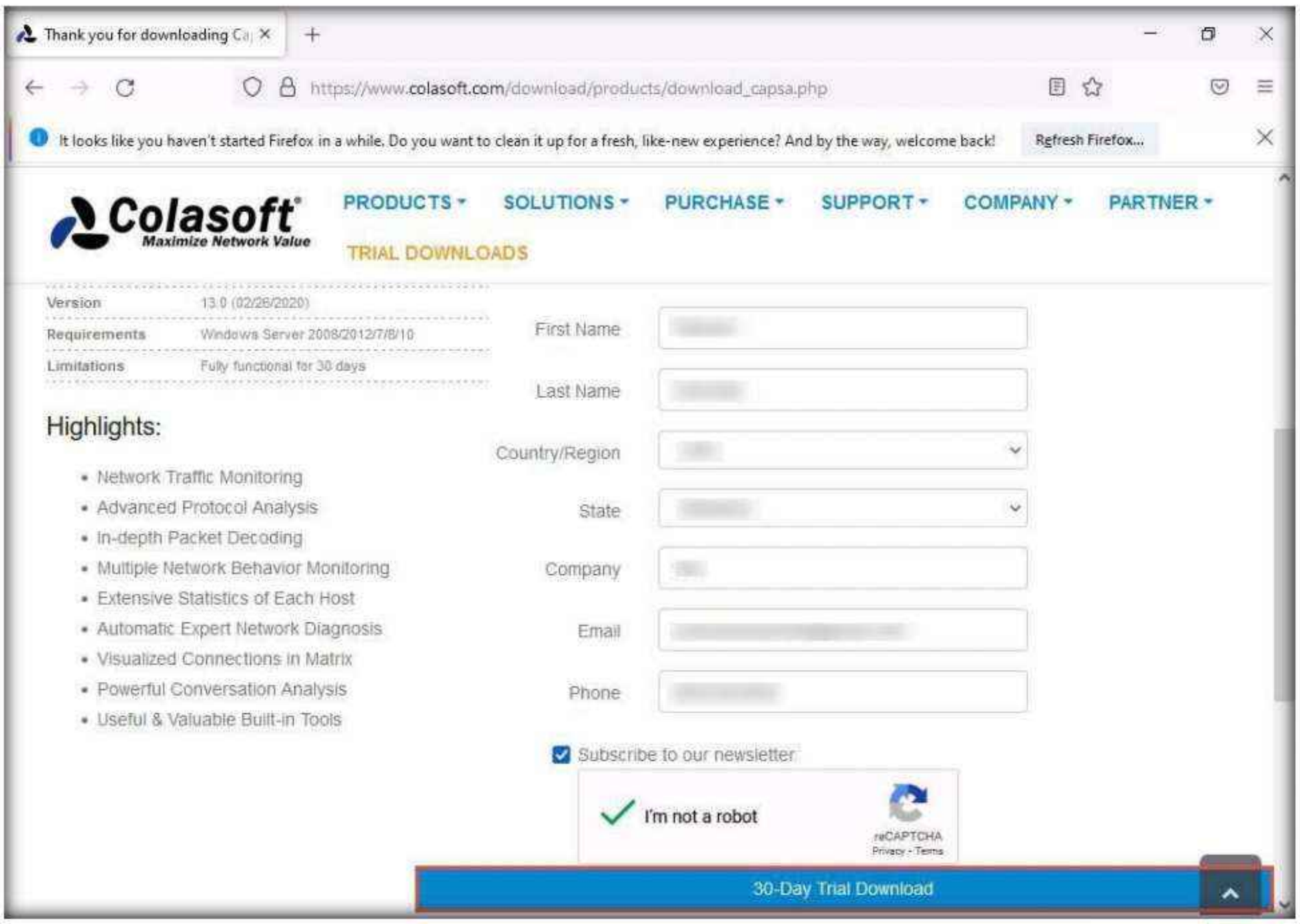


3. In the **Colasoft Capsa - Quick detect ARP poisoning & ARP flooding** window, click on **Download Free Trial** button.

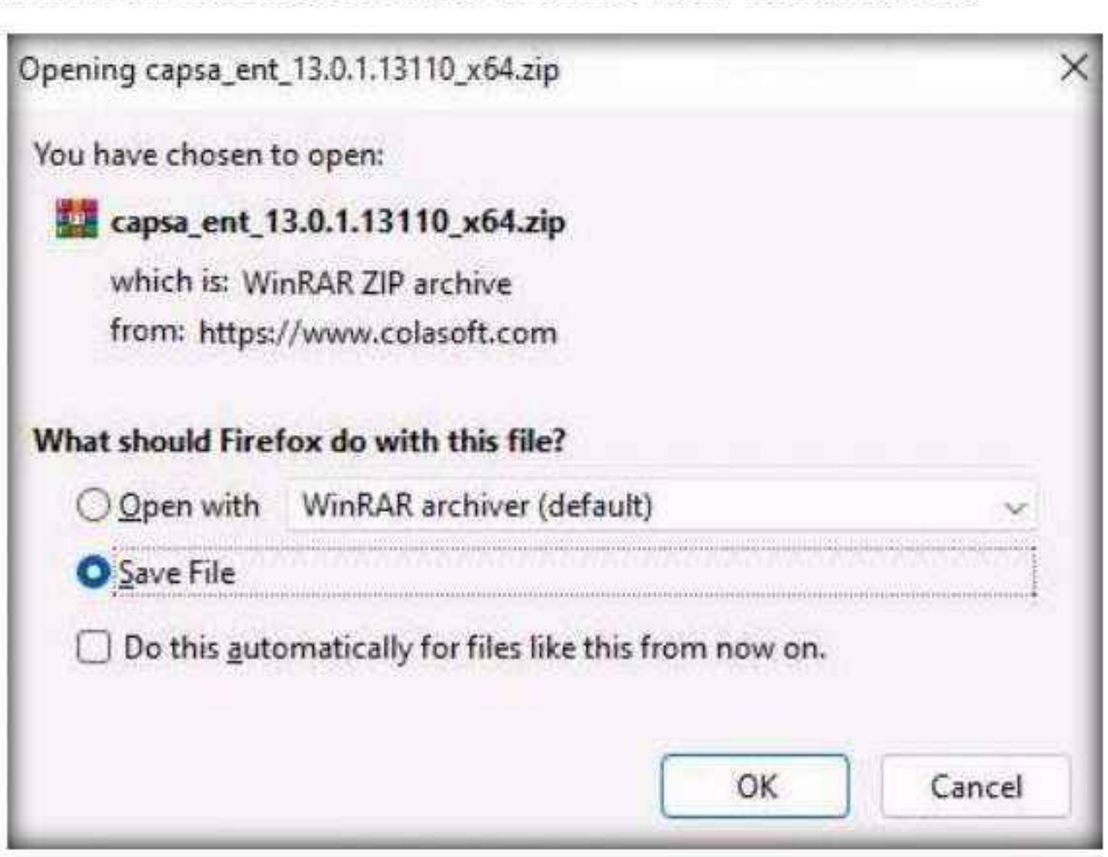


4. You will be redirected to **Download Capsa Enterprise Trial** window, scroll-down and fill all the required personal details and click on **30-Day Trial Download**.

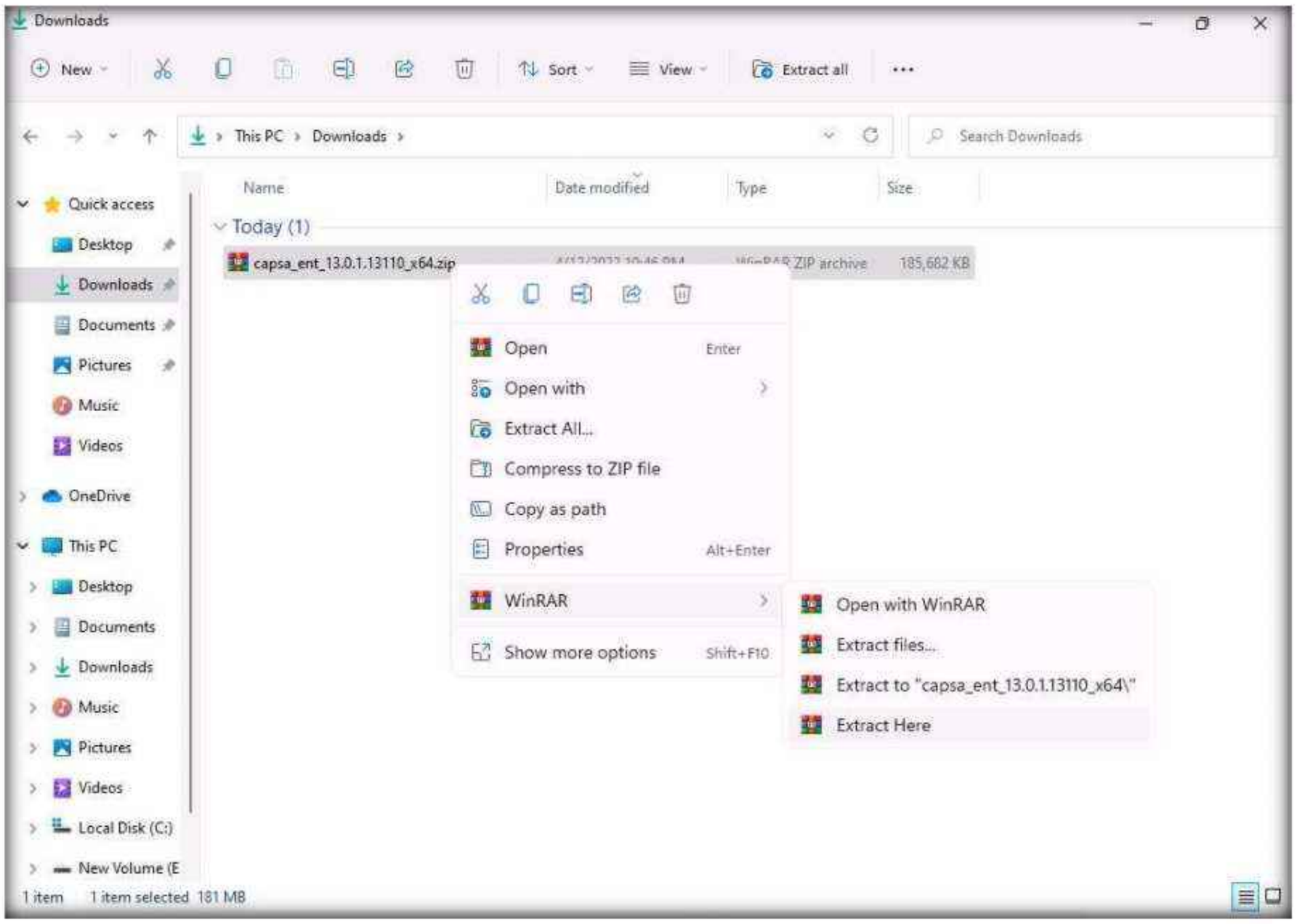
   Note: Here, you must provide your professional **EMAIL ADDRESS** (work or school accounts).



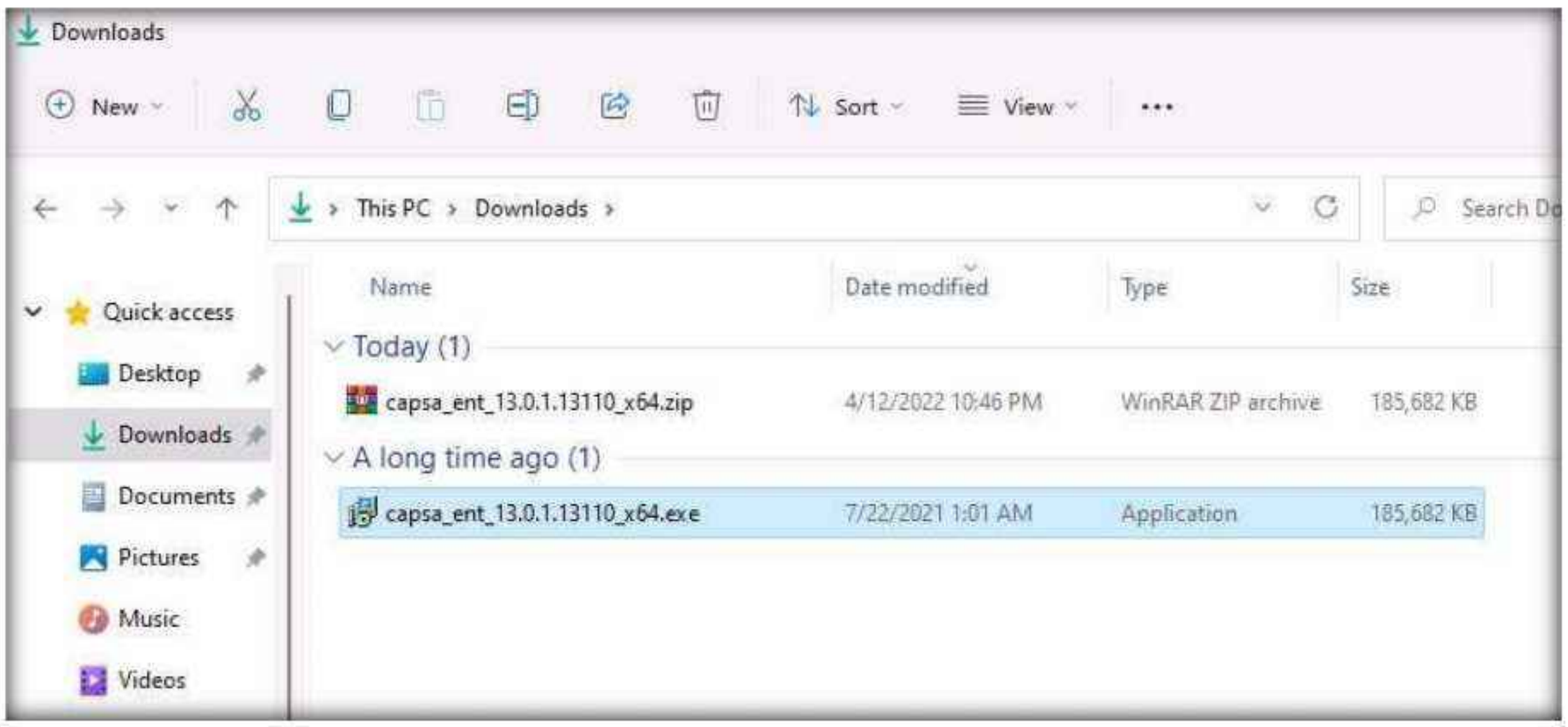
5. You will be redirected to download page, if **Opening capsa_ent_13.0.1.13110_x64.zip** pop-up appears select **Save File** radio button and click on **OK**.



6. The **capsa_ent_13.0.1.13110_x64.zip** file starts downloading, it will take approximately **5** minutes for the download.
7. Once the download completes, navigate to the **Downloads** folder and right-click on **capsa_ent_13.0.1.13110_x64.zip** file and hover the cursor over **WinRAR** and select **Extract Here** option from the list.



8. Once the extraction is completed, double-click the **capsa_ent_13.0.1.13110_x64.exe** file.

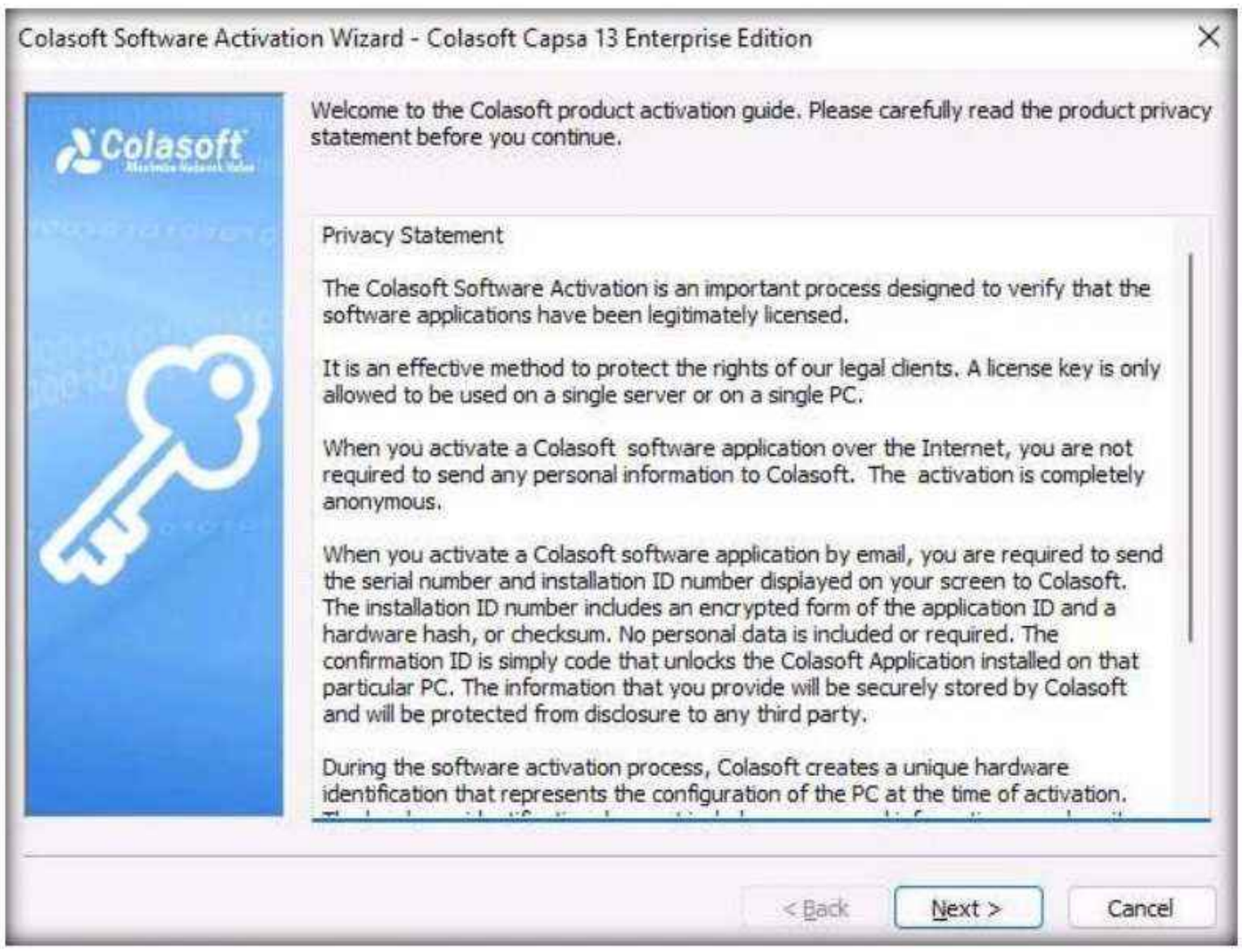


9. A **User Account Control** pop-up appears; click **Yes**.

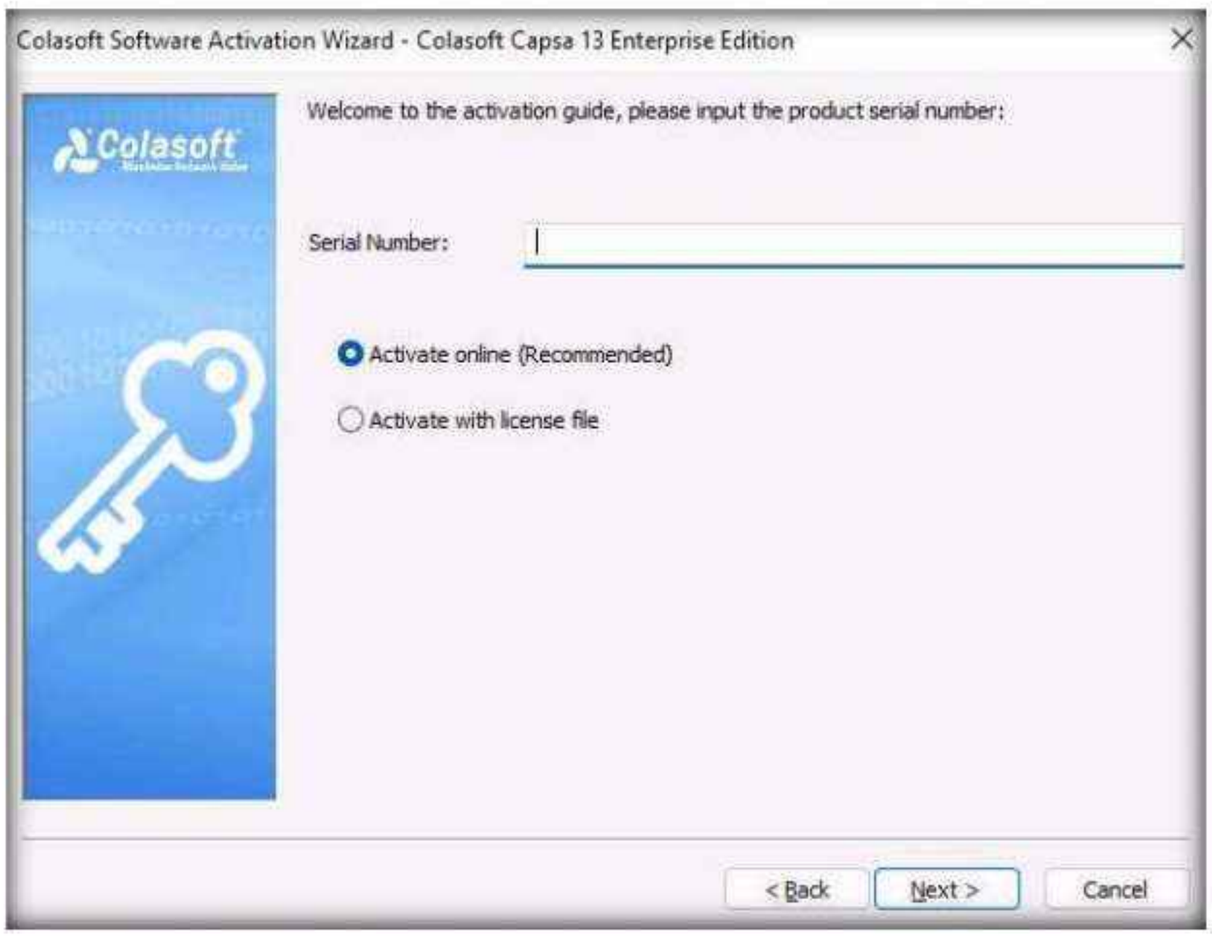
10. **Setup - Colasoft Capsa 13 Enterprise** window appears, click **Next** and follow the wizard driven steps to install **Colasoft Capsa 13 Enterprise** tool.

11. In the **Completing the Colasoft Capsa 13 Enterprise Setup** Wizard, ensure that **Launch Program** checkbox is checked and click on **Finish**.

12. In the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window, click **Next**.

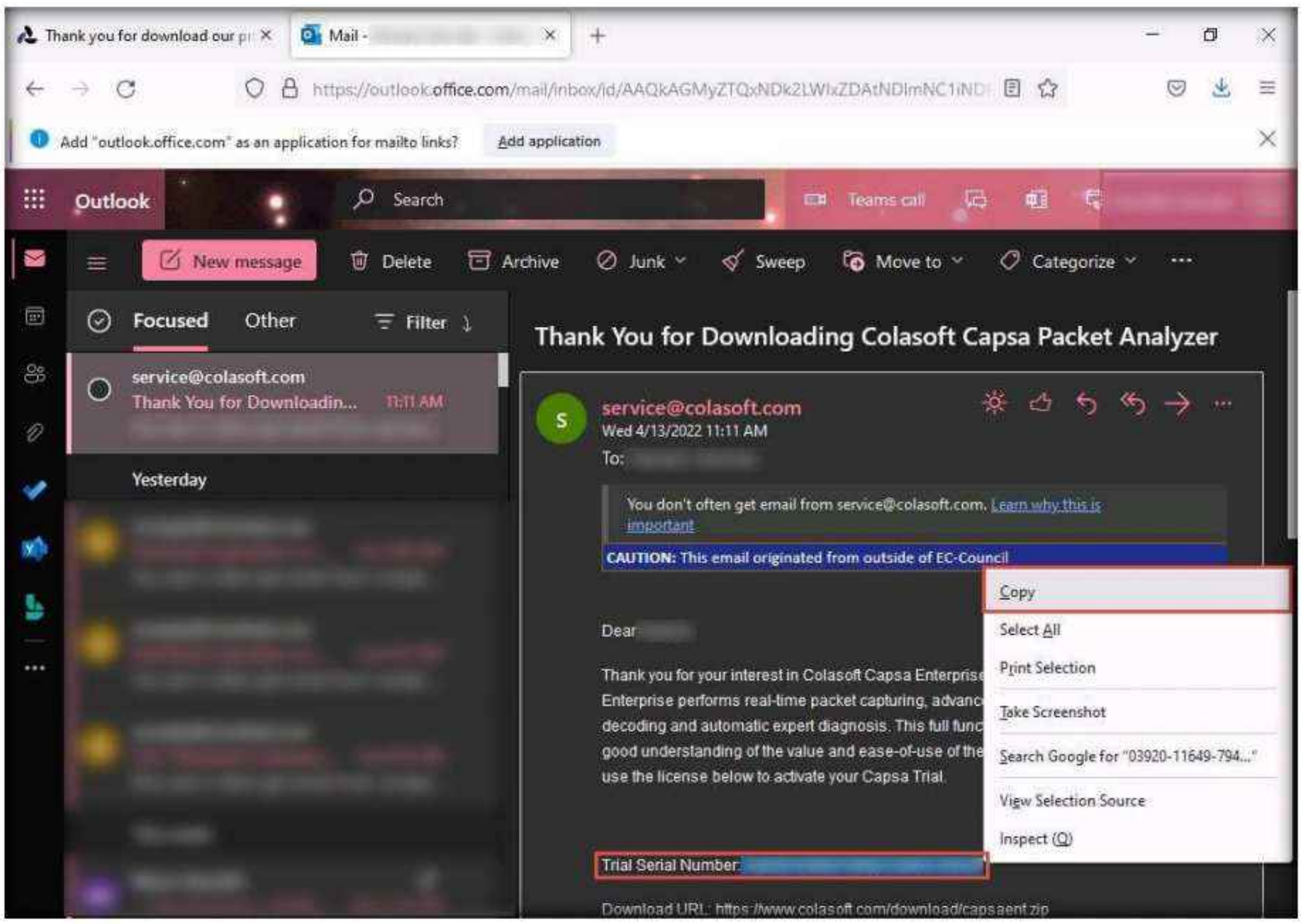


13. In the next window we need to enter the serial number to activate the licence.



14. Leave the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** as it is and switch to the browser.

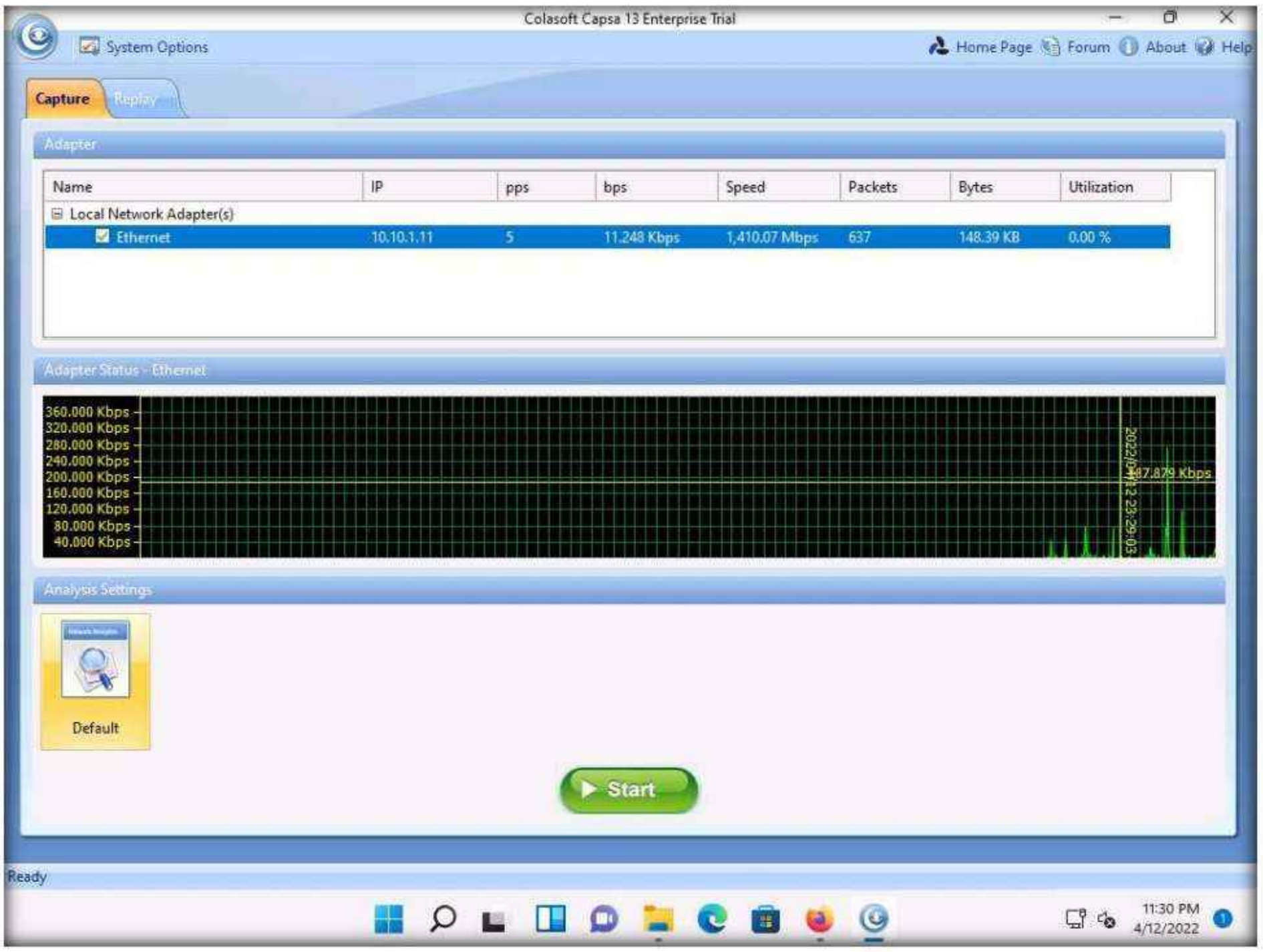
15. Open a new tab in the browser and log in to the email account you provided during registration. Open the email from **service@colasoft.com** and copy the **Trial Serial Number** as shown in the screenshot.



16. Now, minimize the browser window and switch to the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window and paste the copied serial number in the **Serial Number** field. Ensure that **Activate online (Recommended)** radio button is selected and click on **Next**.

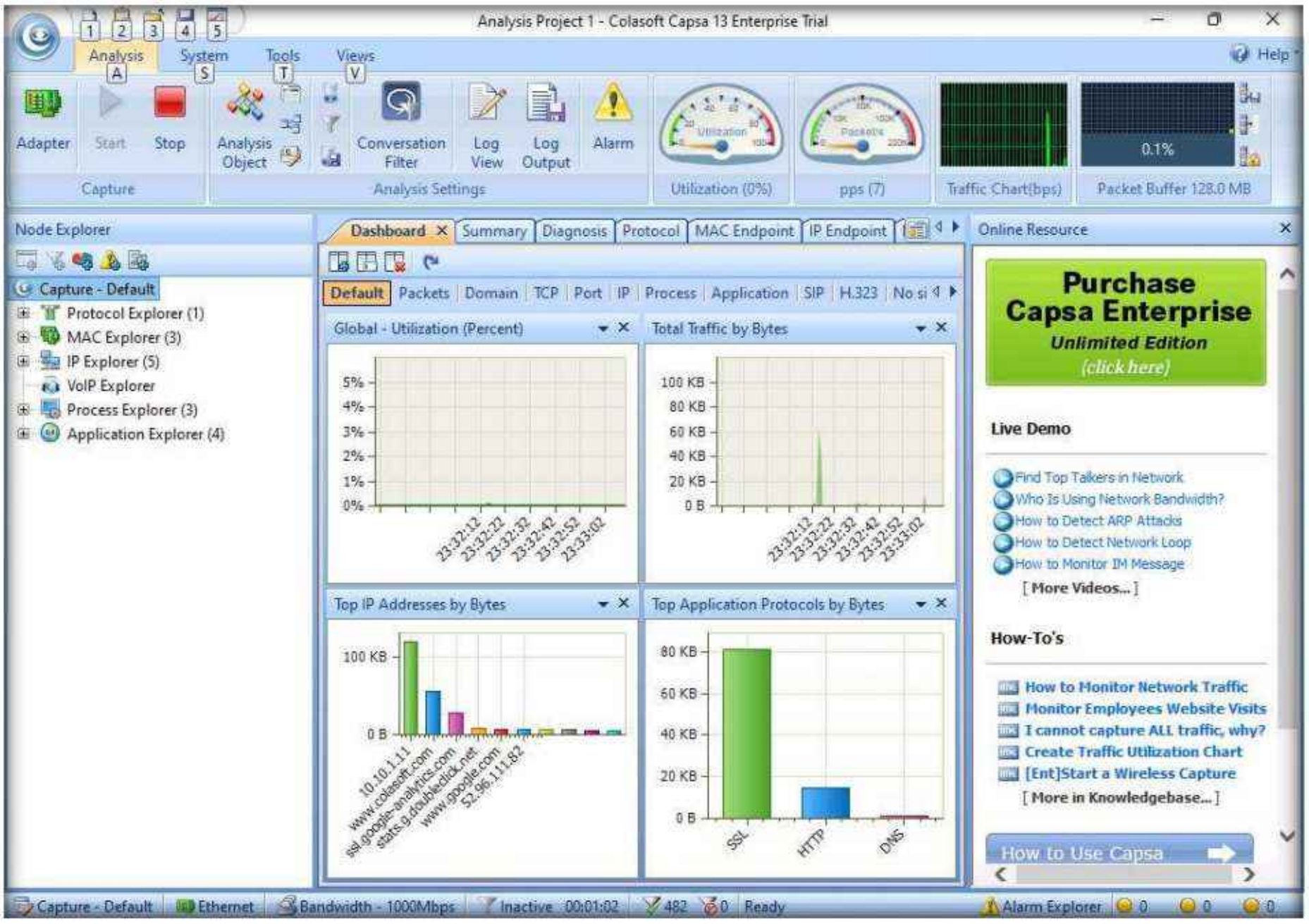
17. A **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window appears, showing that the software has been successfully activated, click on **Finish**.

18. After successful installation, A **Colasoft Capsa 13 Enterprise Trial** window appears.
19. In the **Colasoft Capsa 13 Enterprise Trial** window, check the checkbox beside the available adapter (here, **Ethernet**) and click on **Start**.

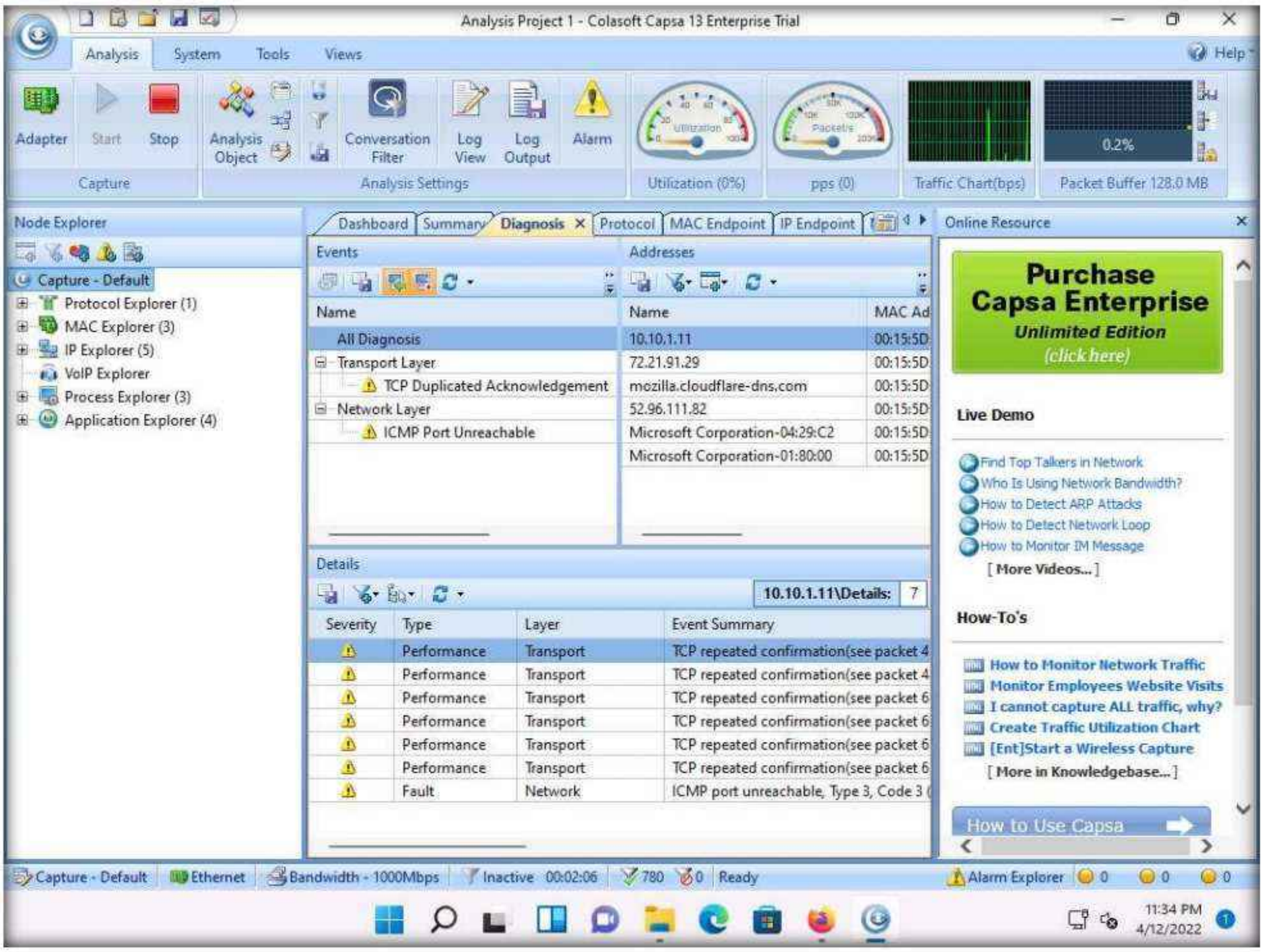


20. If a **Colasoft Capsa 13 Enterprise Trial** pop-up appears, select **Don't show this again** checkbox and click on **OK**.

21. The **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window appears, as shown in the screenshot.



22. Navigate to the **Diagnosis** tab in the **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window.

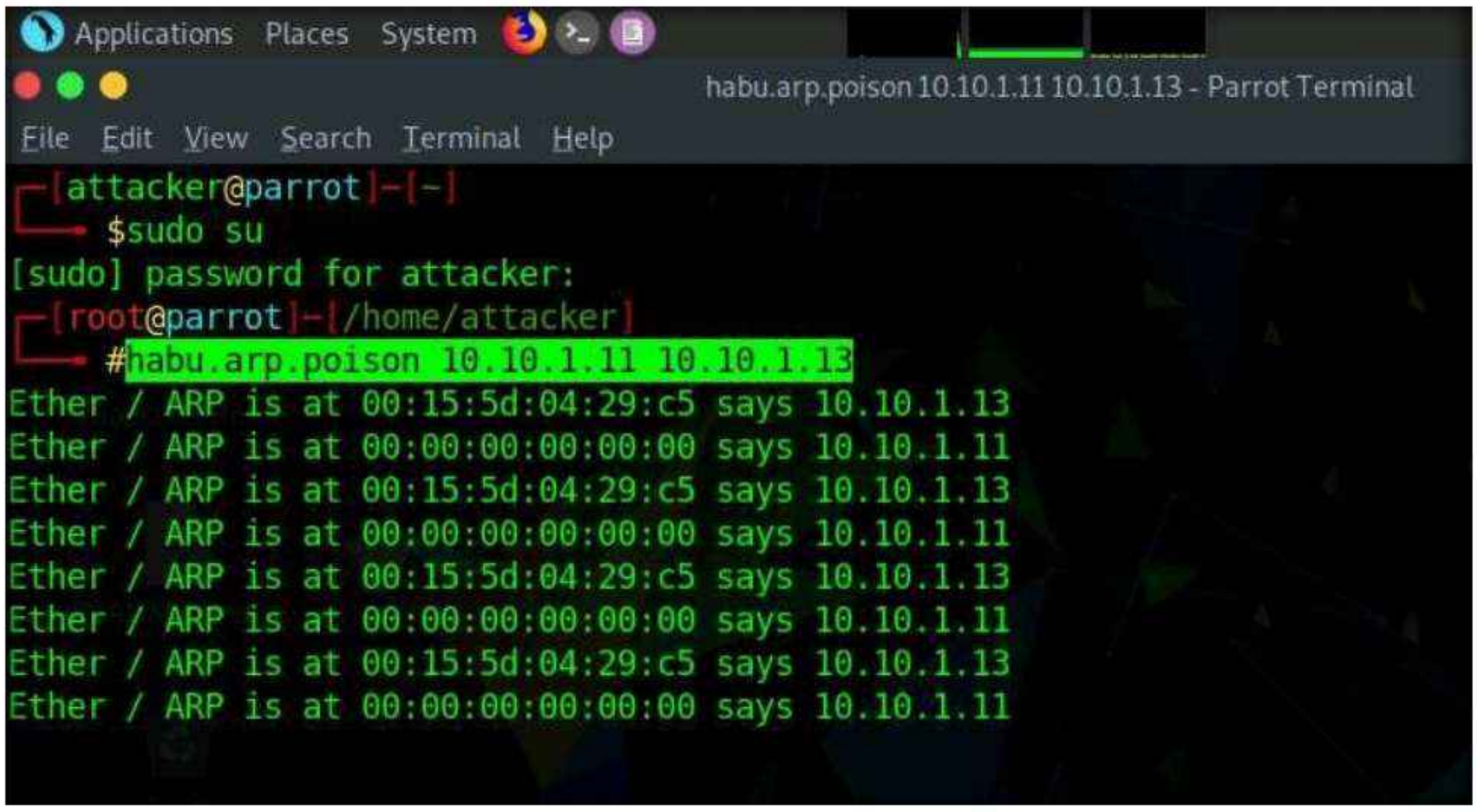


23. Switch to **Parrot Security** virtual machine.
24. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
25. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
26. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

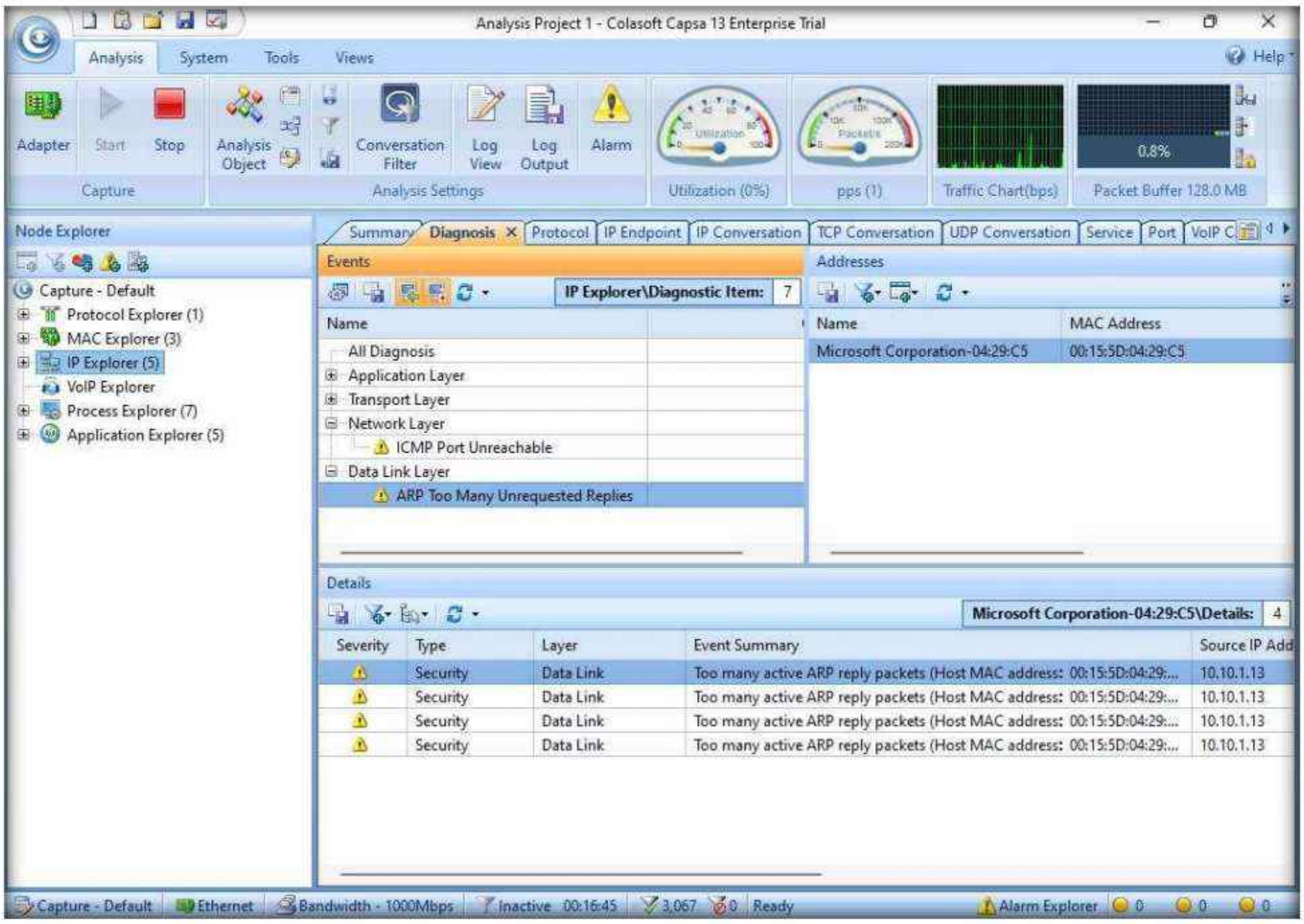
    Note: The password that you type will not be visible.
27. In the terminal window, type **habu.arp.poison 10.10.1.11 10.10.1.13** and press **Enter**, to start ARP poisoning on **Windows 11** machine.

    Note: The above command sends ARP **'is-at'** packets to the specified victim(s), poisoning their ARP tables to send their traffic to the attacker system.

    Note: If you receive any error while running the command ignore it.

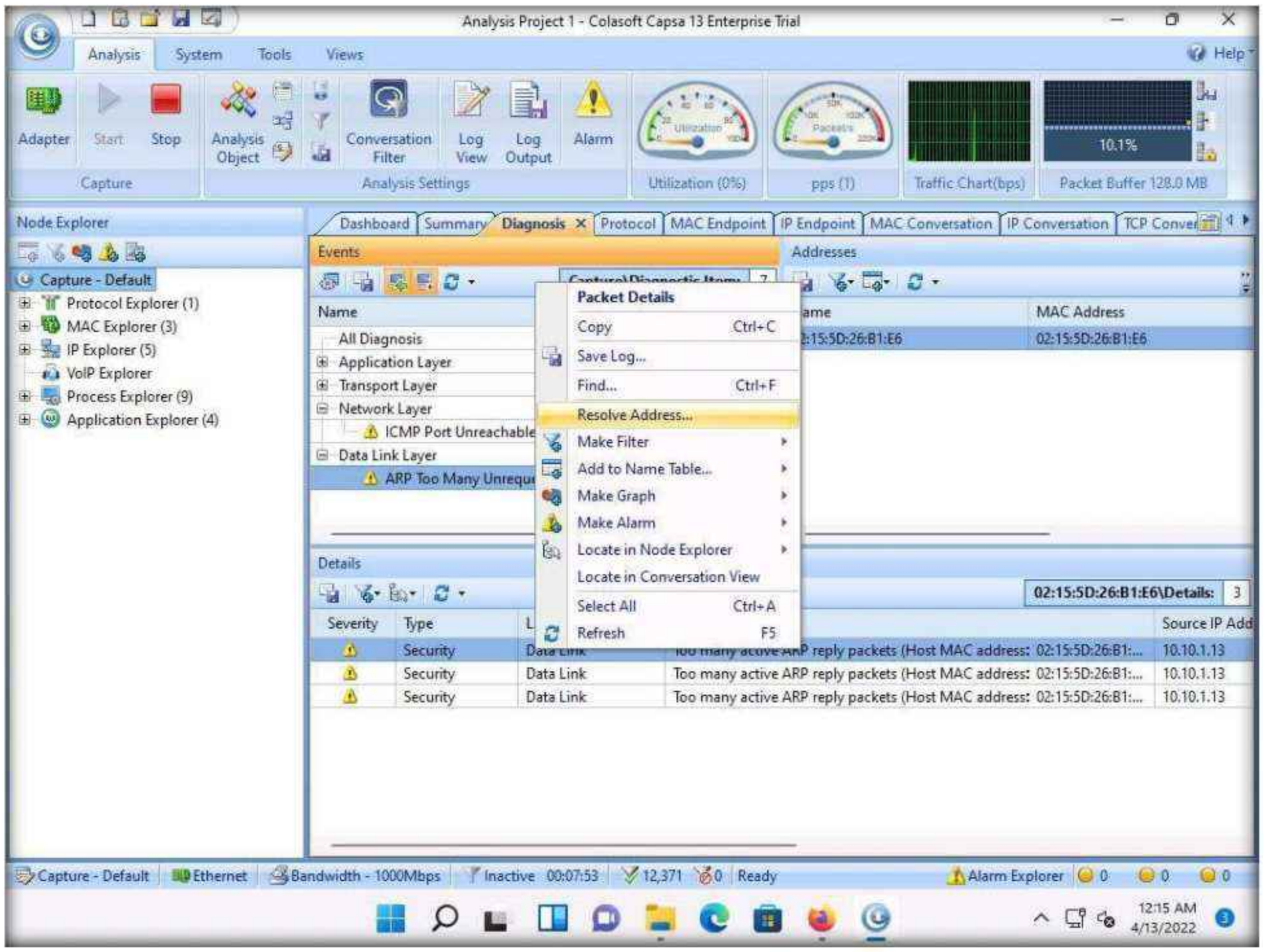


28. Switch to **Windows 11** virtual machine.
29. In the **Diagnosis** tab, expand the **Data Link Layer** node to see the **ARP Too Many Unrequested Replies** warning.

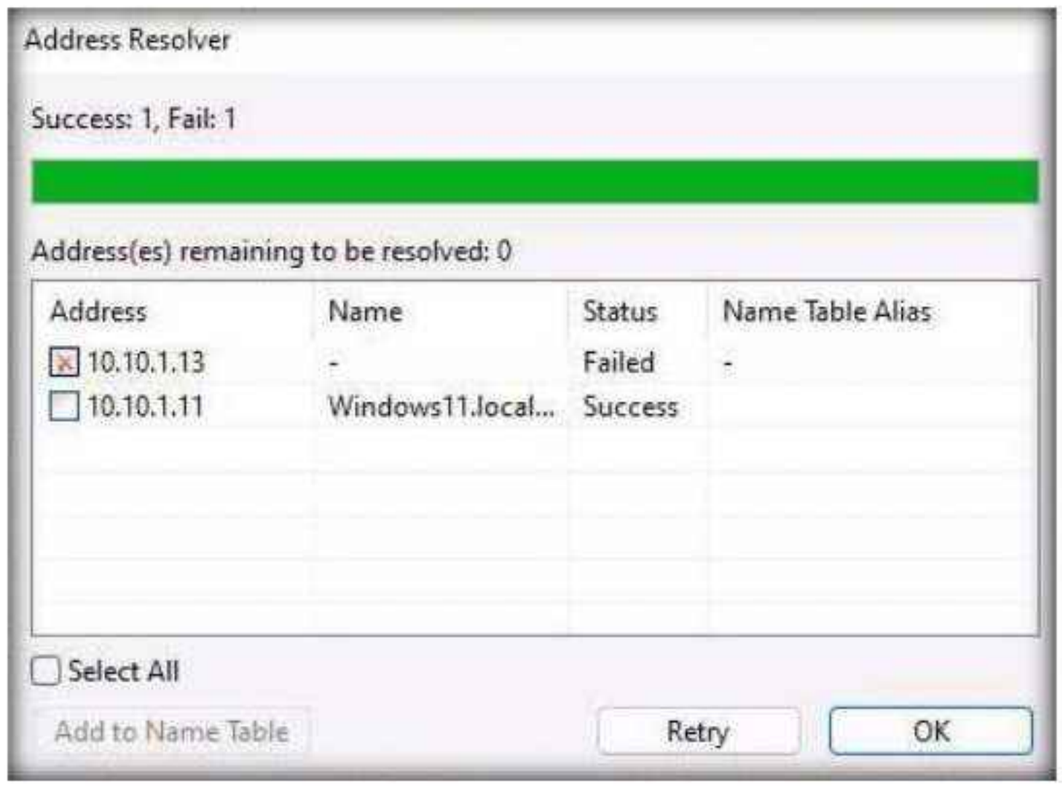


Note: It will take approximately **10** minutes for the tool to capture the **ARP** requests.

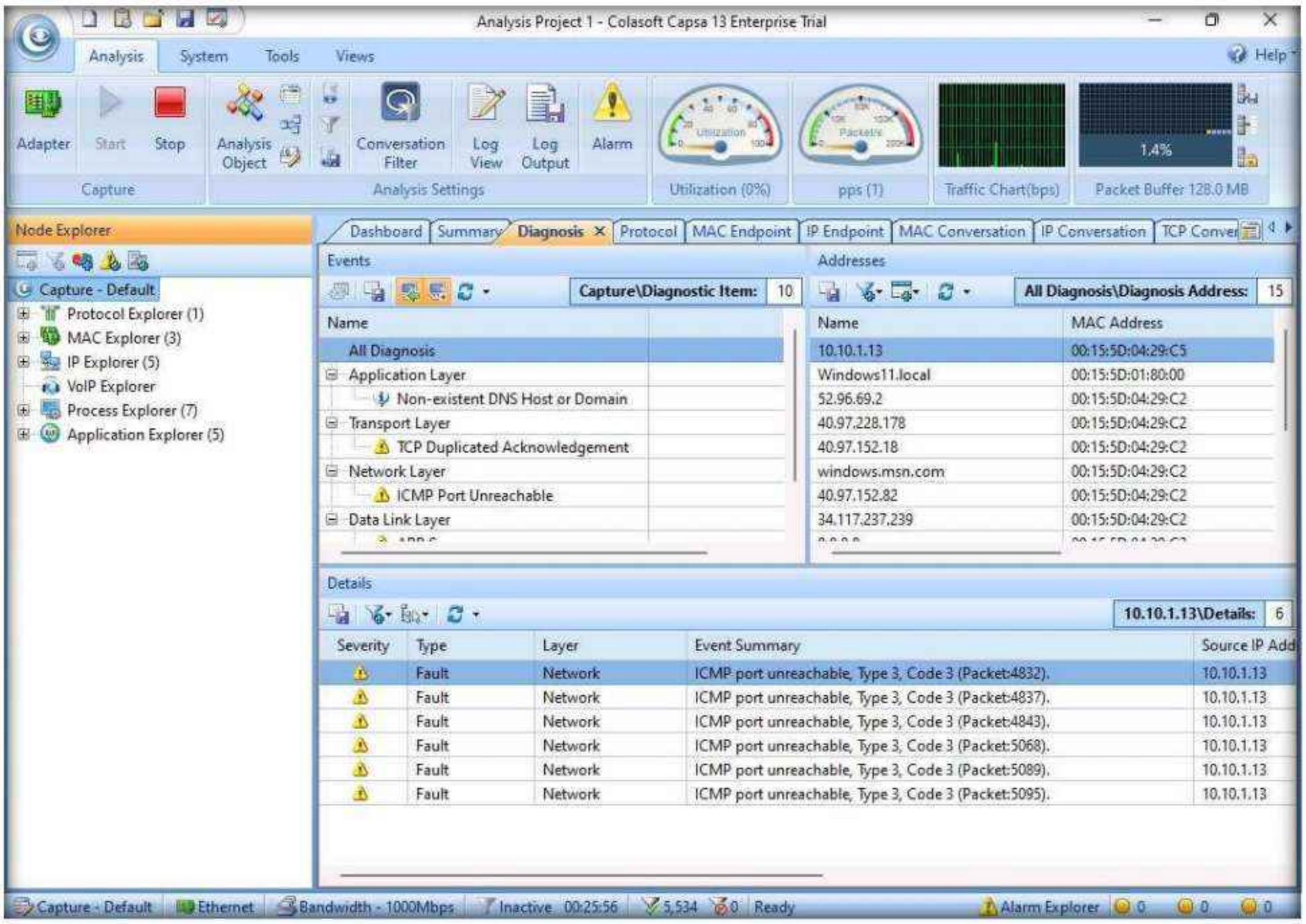
30. Click on **ARP Too Many Unrequested Replies** warning under **Data Link Layer** node.
31. Right-click on **Security** warning under **Details** section and select **Resolve Address...** from the context menu.



32. An **Address Resolver** pop-up appears, once the address resolving completes click on **OK**.

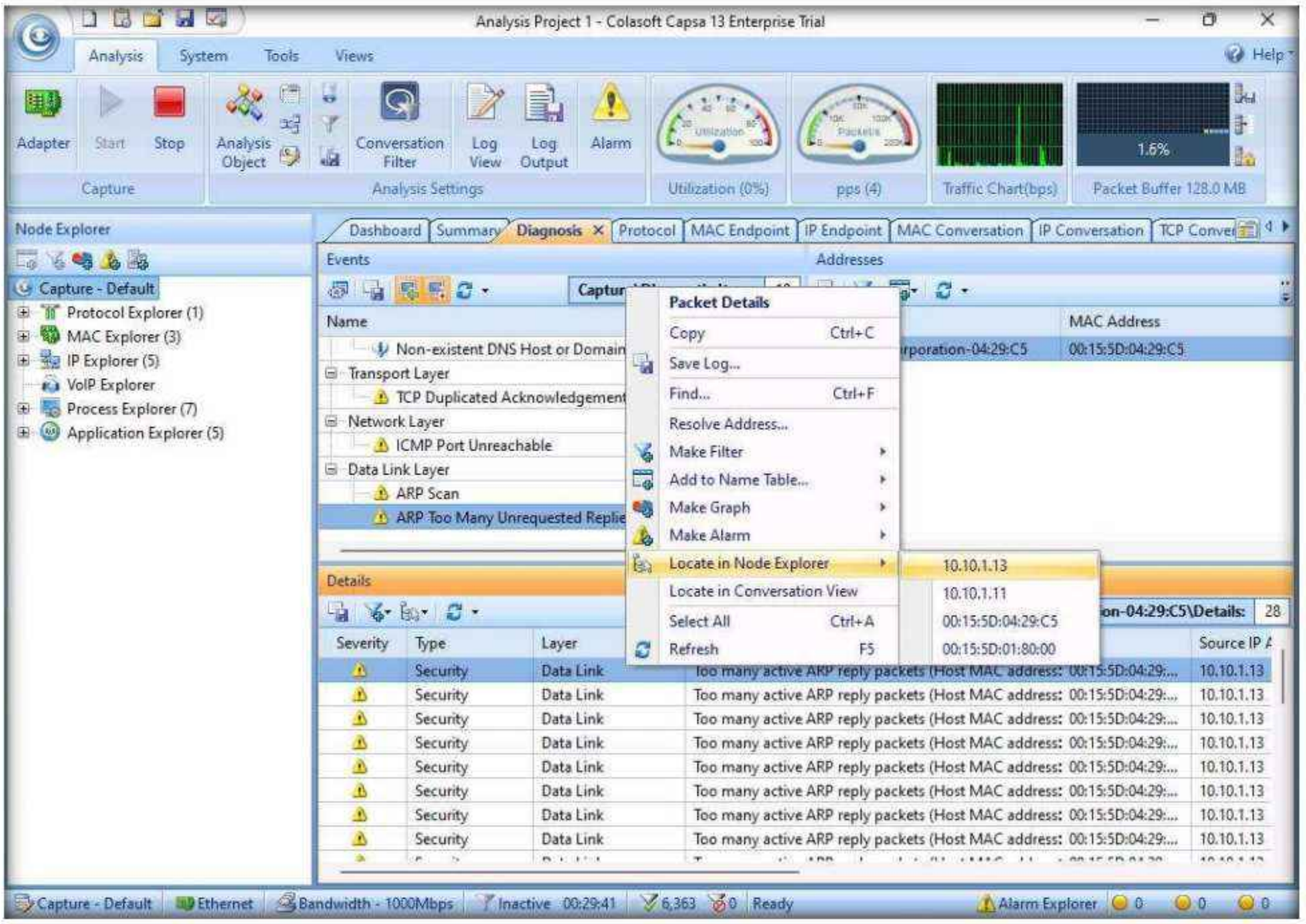


33. Now to locate the Parrot Machine's IP address click on **Capture Default** option under **Node Explorer** section in the left-pane.

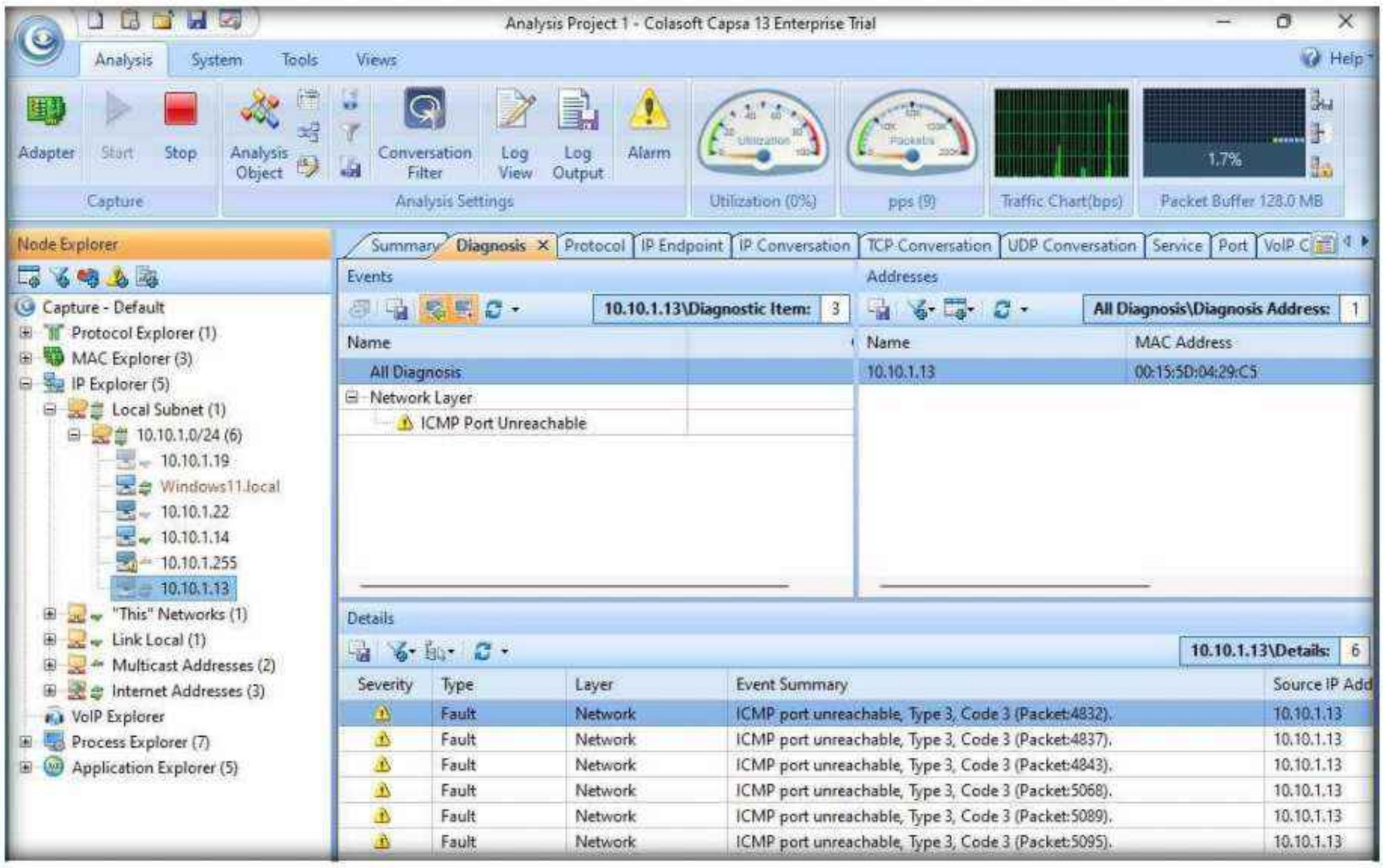


34. Click on **ARP Too Many Unrequested Replies** warning under **Data Link Layer** node.
35. Now right click any warning in the **Details** tab and click on **Locate in Node Explorer** and select **Parrot Security** machine's IP address from the list (here, **10.10.1.13**).

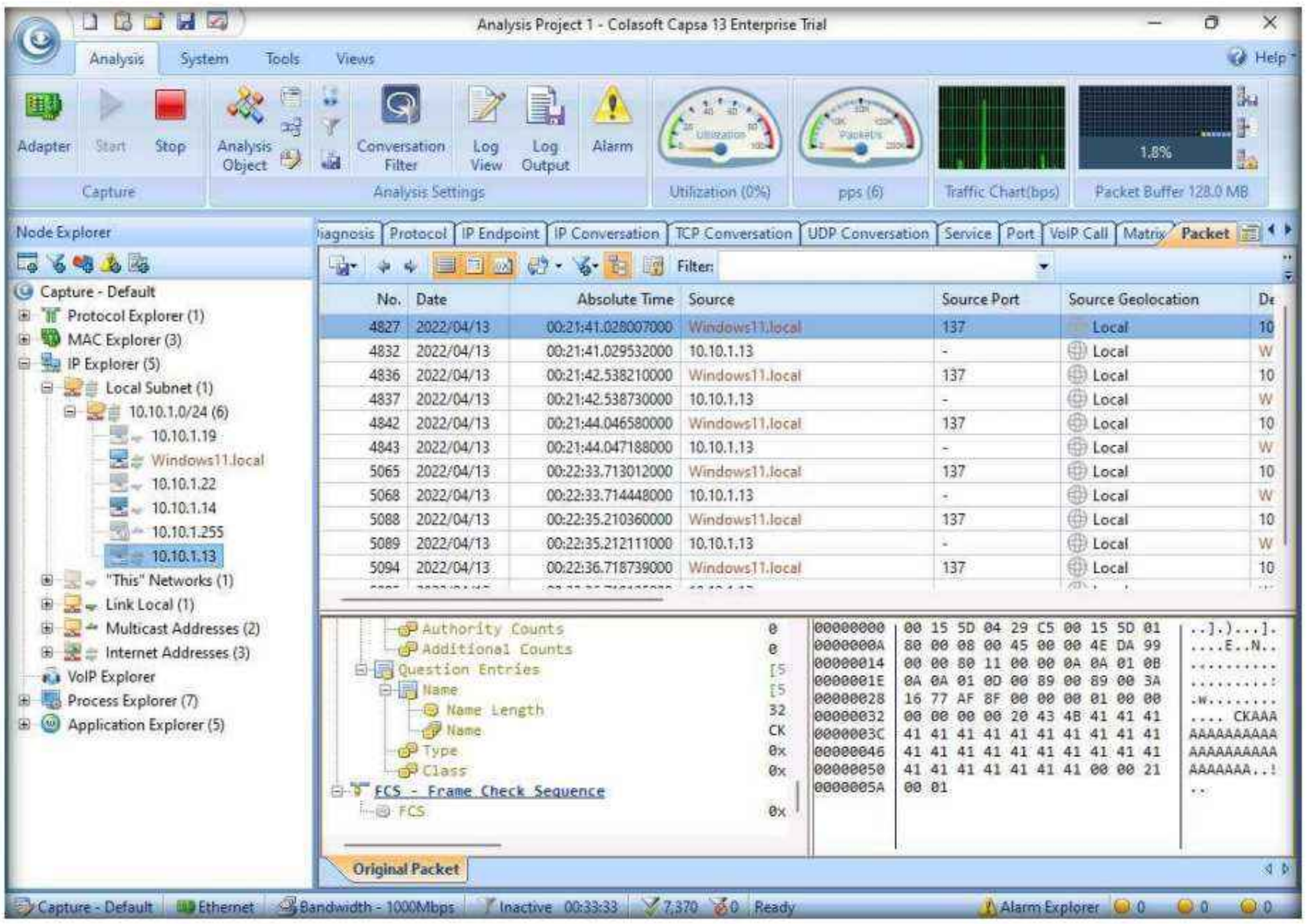
    Note: Here, the IP address of the Parrot Security machine is the attacker's IP address.



36. The IP address of the Parrot Security machine is displayed under **Node Explorer** section in the left-pane.

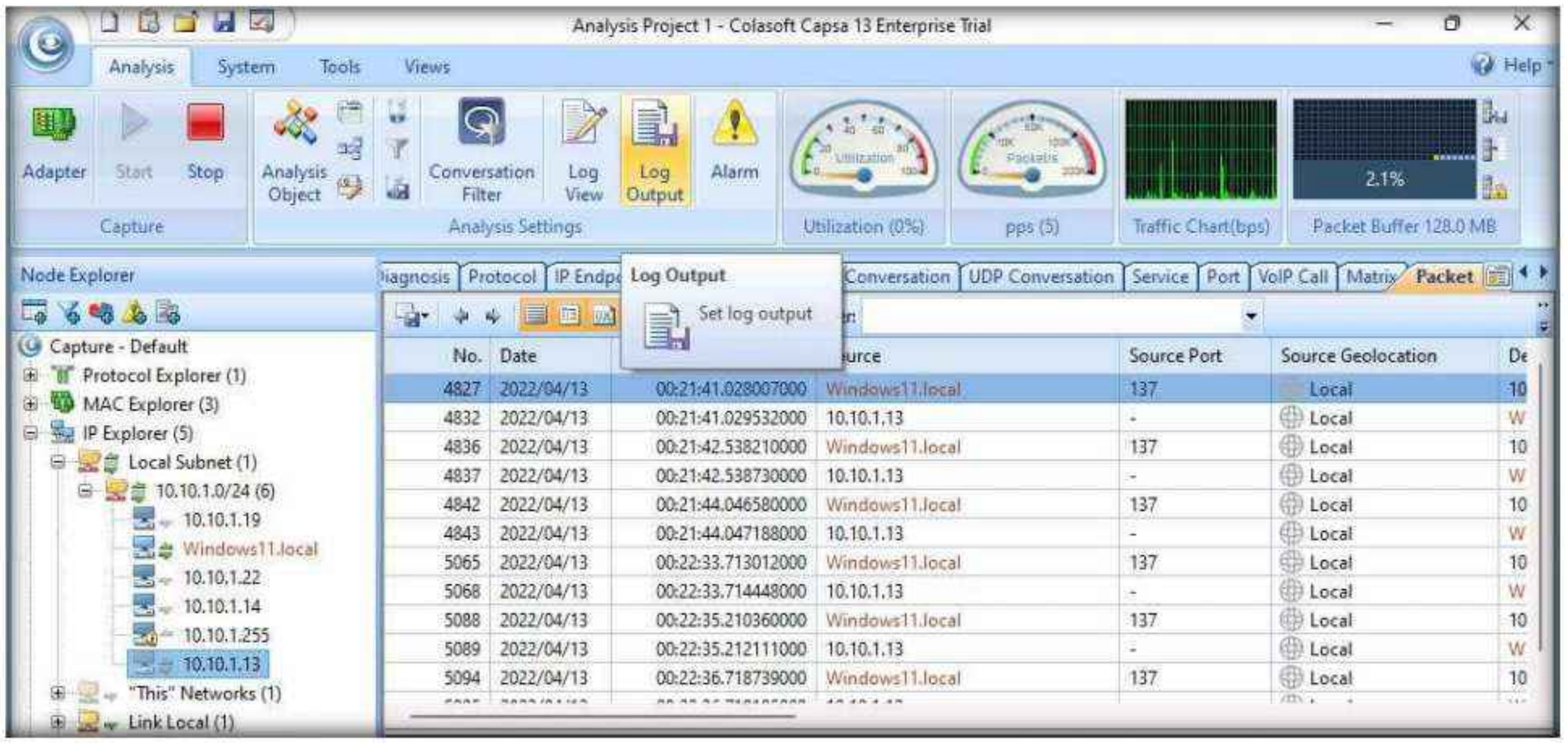


37. Now click on **Packet** tab in the **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window, to check the packets transferred by the **Parrot Security** machine.

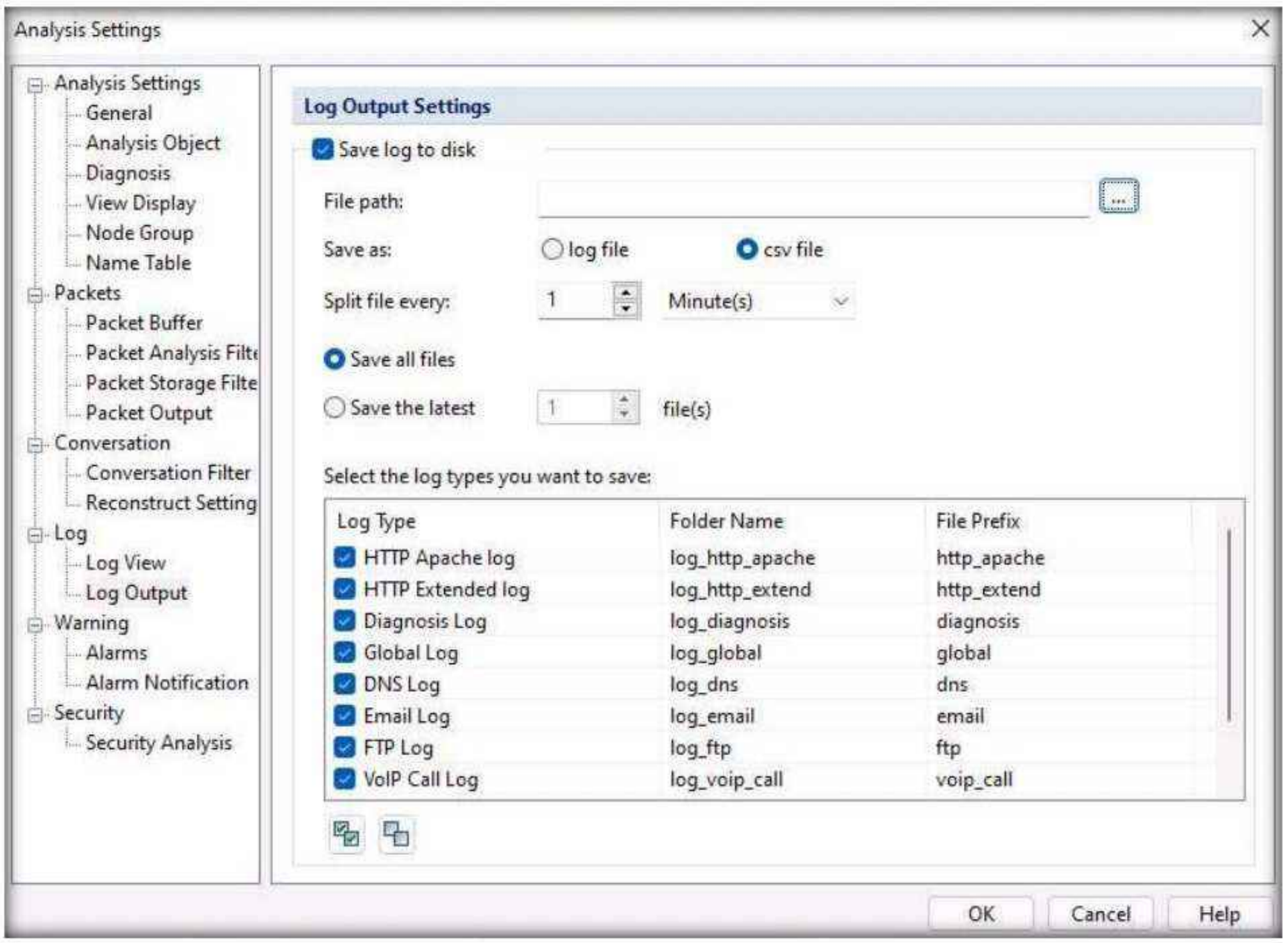


38. Similarly, you can navigate to all the available tabs such as **Protocol**, **MAC Endpoint**, **IP Endpoint**, **MAC Conversation**, **IP Conversation** etc.

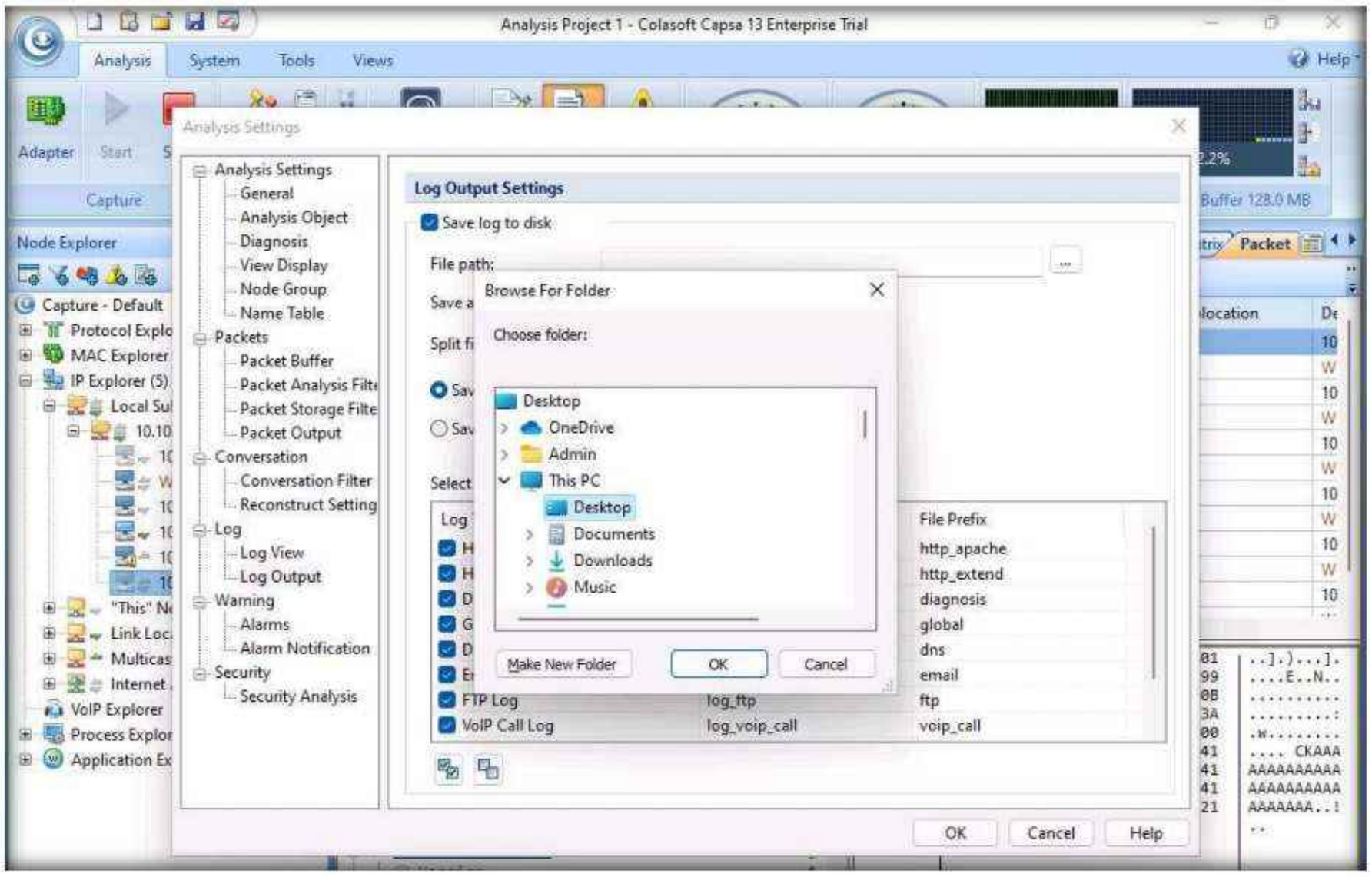
39. After completing the analysis click on **Log Output** option from the menu bar.



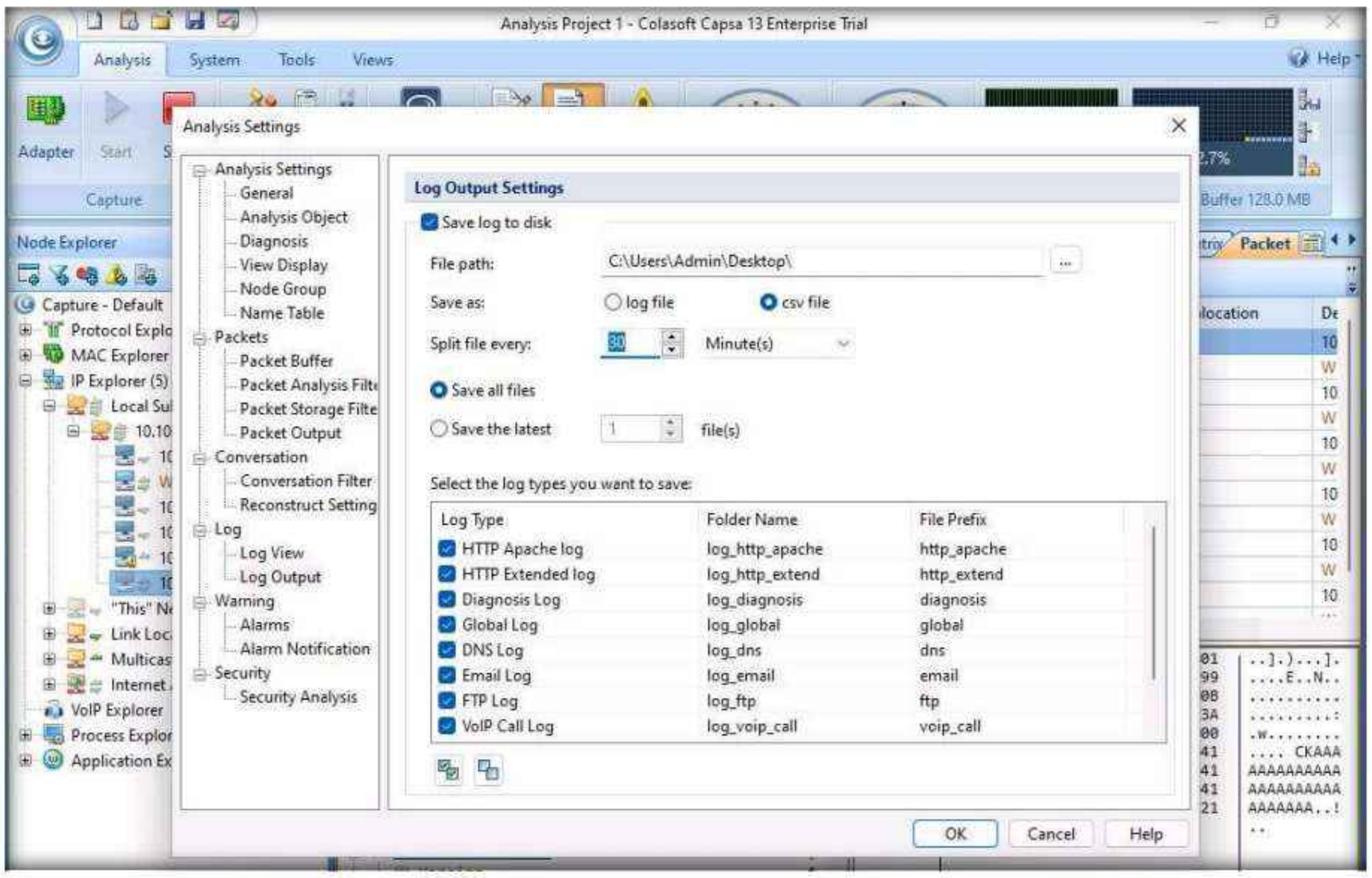
40. In the **Analysis Settings window**, check the **Save log to disk** checkbox and click the ellipsis button under **File path** option.



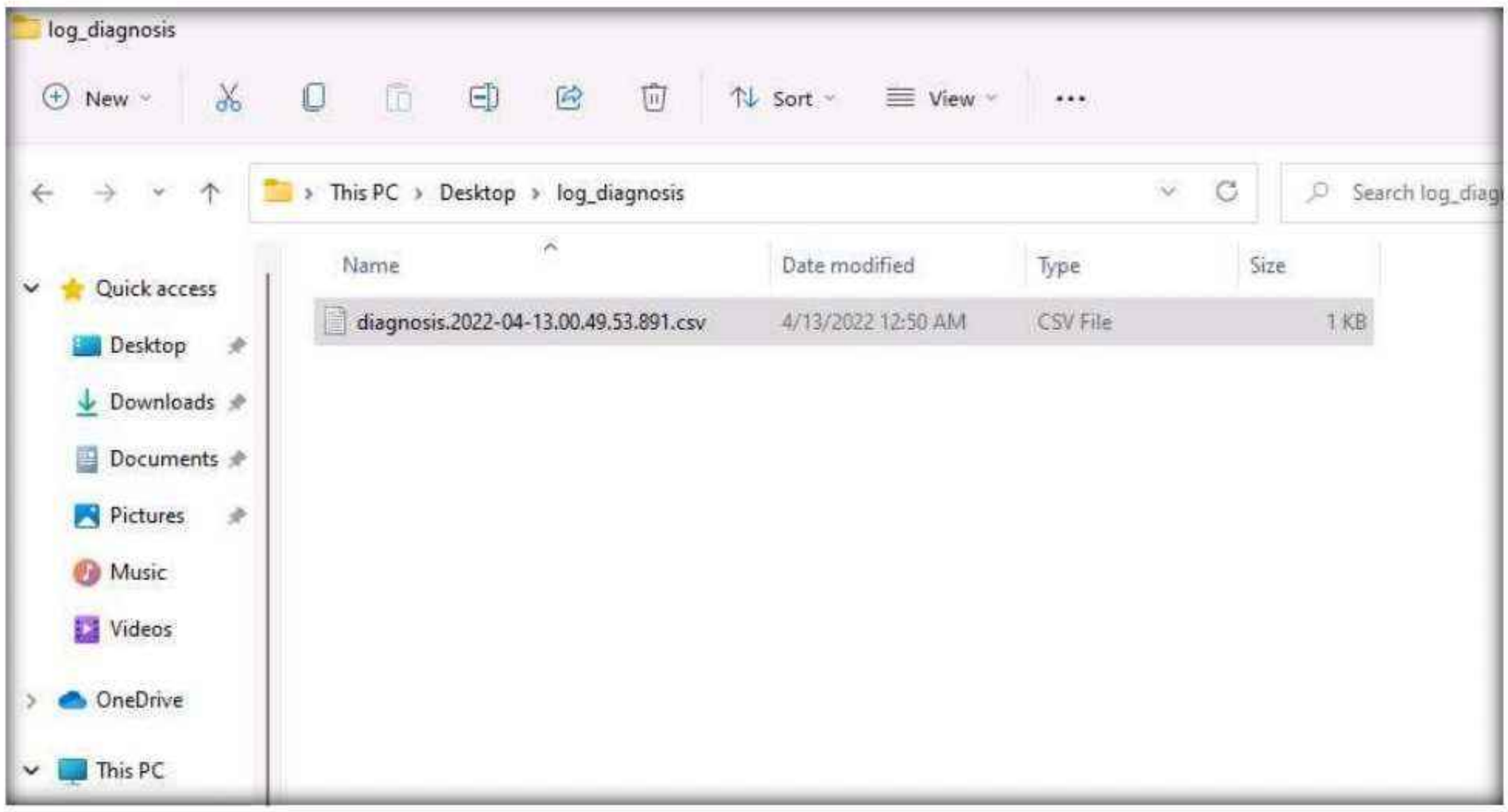
41. In the **Browse For Folder** window, select **Desktop** and click on **OK**.



42. Ensure that **csv** file radio button is selected under **Save As** section and select **30** seconds under **Split file every:** section (this option directly saves a new log file in the specified location for every 30 seconds), leave all the other settings as default and click **OK**.



43. We can see that the csv log file is created in **Desktop → log_diagnosis** location.



44. This concludes the demonstration of detecting ARP poisoning using the Capsa Network Analyzer.
45. Close all open windows and document all the acquired information.
46. Turn off the **Windows 11**, **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

Social Engineering

Module 09

Social Engineering

Social engineering is the art of convincing users to reveal confidential information.

Lab Scenario

Organizations fall victim to social engineering tactics despite having strong security policies and solutions in place. This is because social engineering exploits the most vulnerable link in information system security—employees. Cybercriminals are increasingly using social engineering techniques to target people's weaknesses or play on their good natures.

Social engineering can take many forms, including phishing emails, fake sites, and impersonation. If the features of these techniques make them an art, the psychological insights that inform them make them a science.

While non-existent or inadequate defense mechanisms in an organization can encourage attackers to use various social engineering techniques to target its employees, the bottom line is that there is no technological defense against social engineering. Organizations must educate employees on how to recognize and respond to these attacks, but only constant vigilance will minimize attackers' chances of success.

As an expert ethical hacker and penetration tester, you need to assess the preparedness of your organization or the target of evaluation against social engineering attacks. It is important to note, however, that social engineering primarily requires soft skills. The labs in this module therefore demonstrate several techniques that facilitate or automate certain facets of social engineering attacks.

Lab Objective

The objective of the lab is to use social engineering and related techniques to:

- Sniff user/employee credentials such as employee IDs, names, and email addresses
- Obtain employees' basic personal details and organizational information
- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of Social Engineering

Social engineering is the art of manipulating people to divulge sensitive information that will be used to perform some kind of malicious action. Because social engineering targets human weakness, even organizations with strong security policies are vulnerable to being compromised by attackers. The impact of social engineering attacks on organizations can include economic losses, damage to goodwill, loss of privacy, risk of terrorism, lawsuits and arbitration, and temporary or permanent closure.

There are many ways in which companies may be vulnerable to social engineering attacks. These include:

- Insufficient security training
- Unregulated access to information
- An organizational structure consisting of several units
- Non-existent or lacking security policies

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform social engineering tests. The recommended labs that will assist you in learning various social engineering techniques are:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform Social Engineering using Various Techniques	√	√	√
	1.1 Sniff Credentials using the Social-Engineer Toolkit (SET)	√		√
2	Detect a Phishing Attack	√	√	√
	2.1 Detect Phishing using Netcraft	√		√
	2.2 Detect Phishing using PhishTank		√	√
3	Audit Organization's Security for Phishing Attacks	√		√
	3.1 Audit Organization's Security for Phishing Attacks using OhPhish	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

***CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Perform Social Engineering using Various Techniques

Social engineering techniques are used to gather sensitive information from people or organizations in order to commit fraud or carry out other criminal activities.

Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees.

In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system

Lab Objectives

- Sniff credentials using the Social-Engineer Toolkit (SET)

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Social Engineering Techniques

There are three types of social engineering attacks: human-, computer-, and mobile-based.

- **Human-based social engineering** uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping

- **Computer-based social engineering** uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging
- **Mobile-based social engineering** uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

Lab Tasks

Task 1: Sniff Credentials using the Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks. For example, it allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

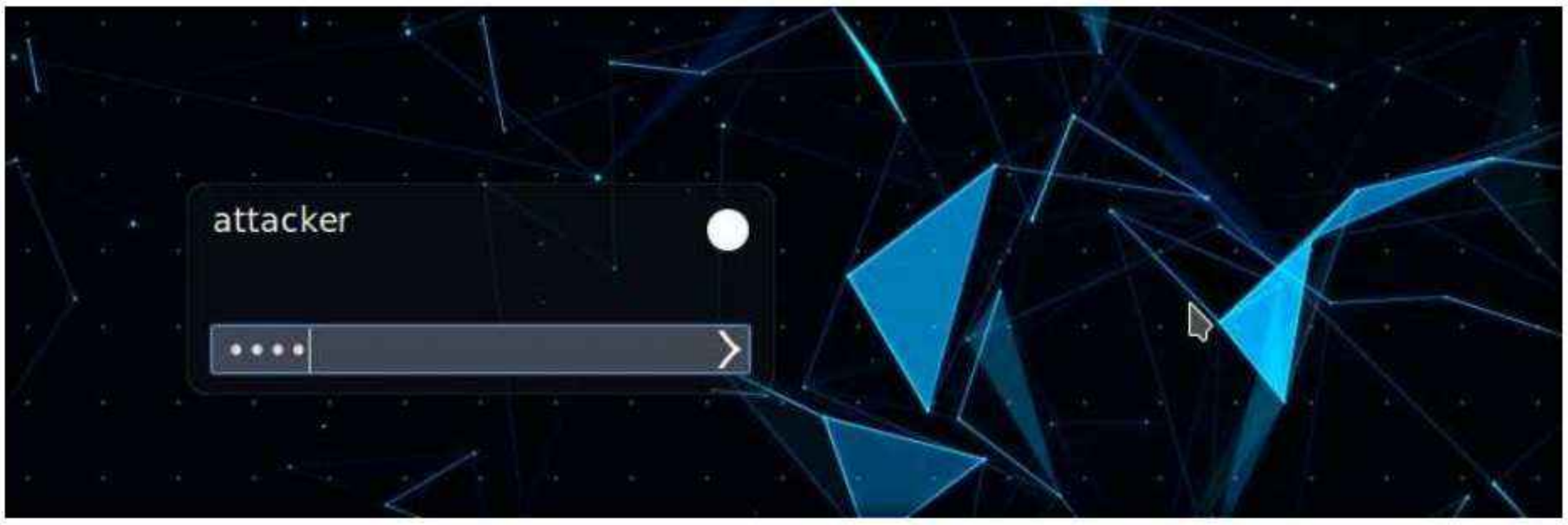
Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

As an ethical hacker, penetration tester, or security administrator, you should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

Here, we will sniff user credentials using the SET.

1. Turn on the **Windows 11** and **Parrot Security** virtual machine.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press Enter to log in to the machine.

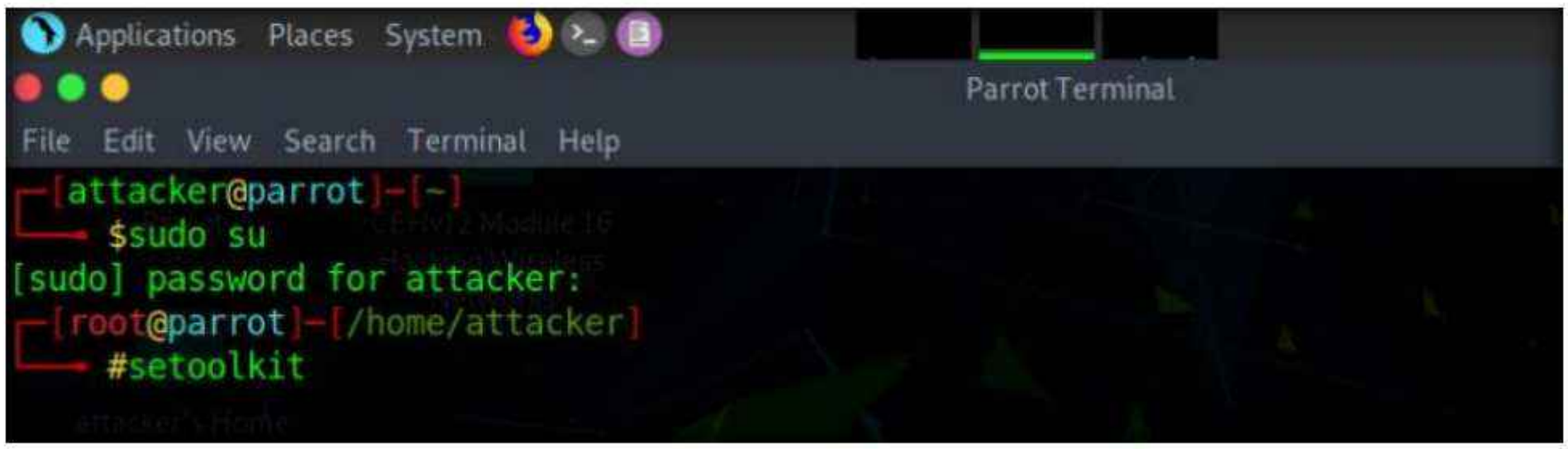
   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



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

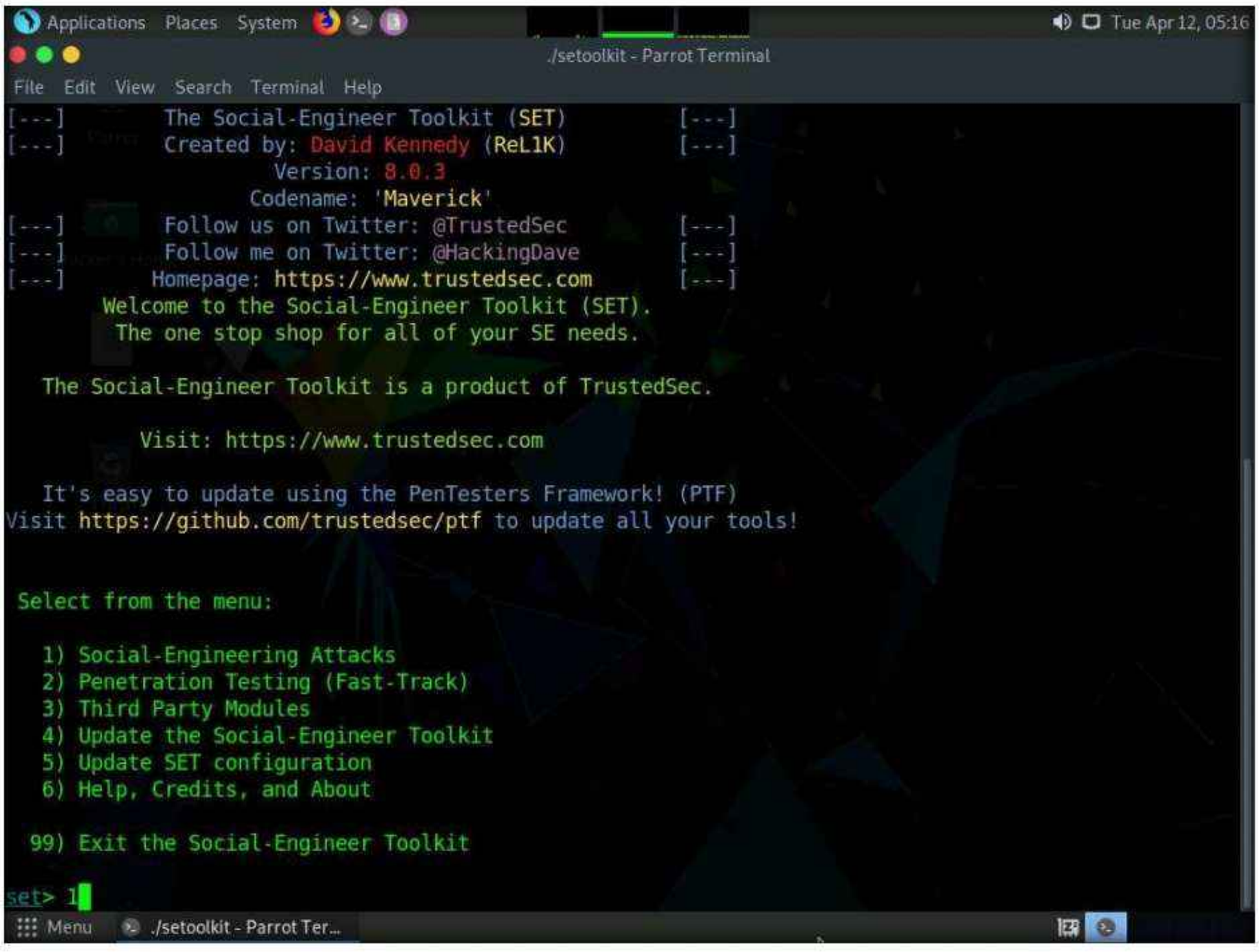
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
6. Type **setoolkit** and press **Enter** to launch Social-Engineer Toolkit (SET).

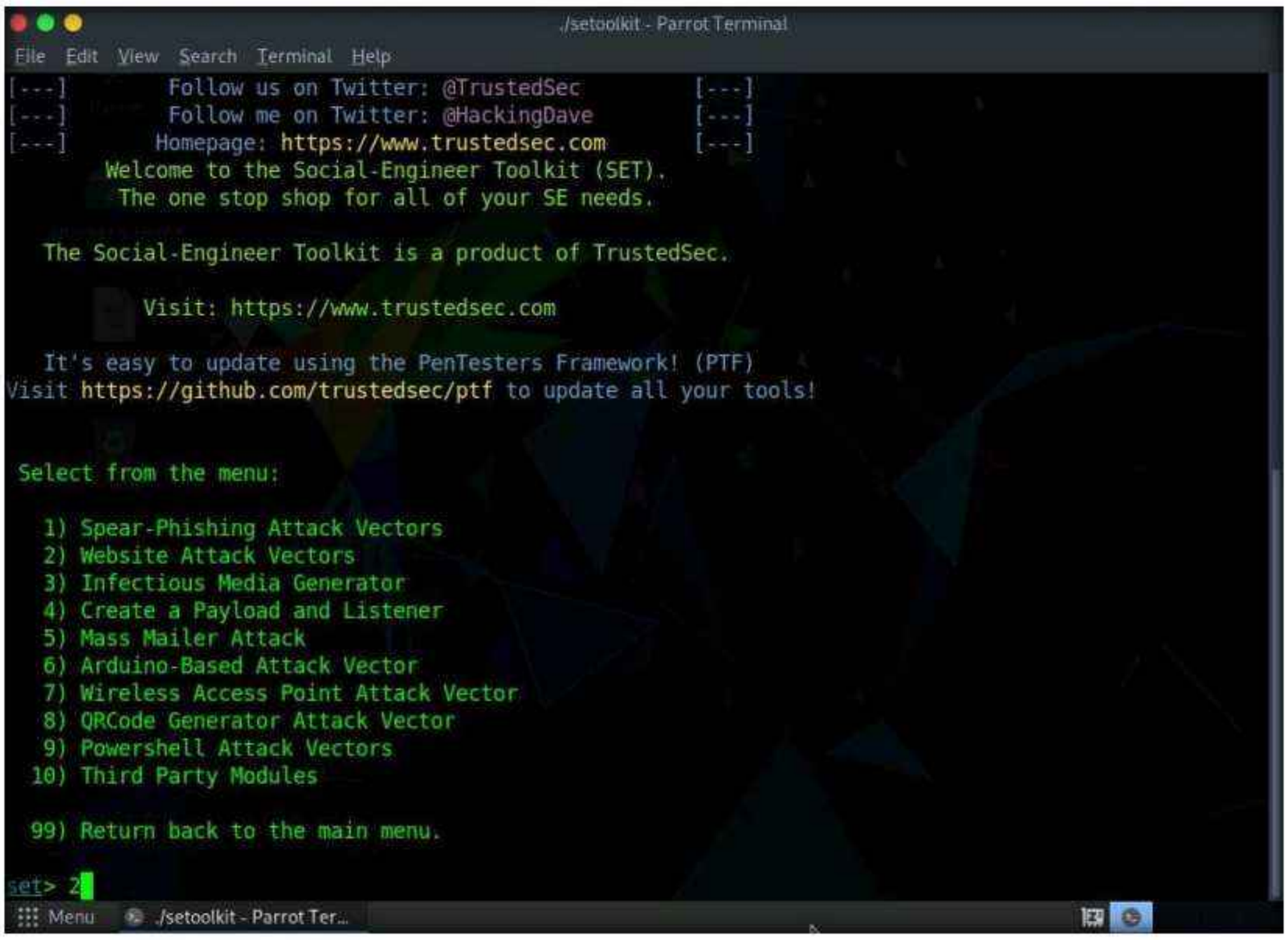


7. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.

   Note: If a **Do you agree to the terms of service [y/n]** question appears, enter **y** and press **Enter**.

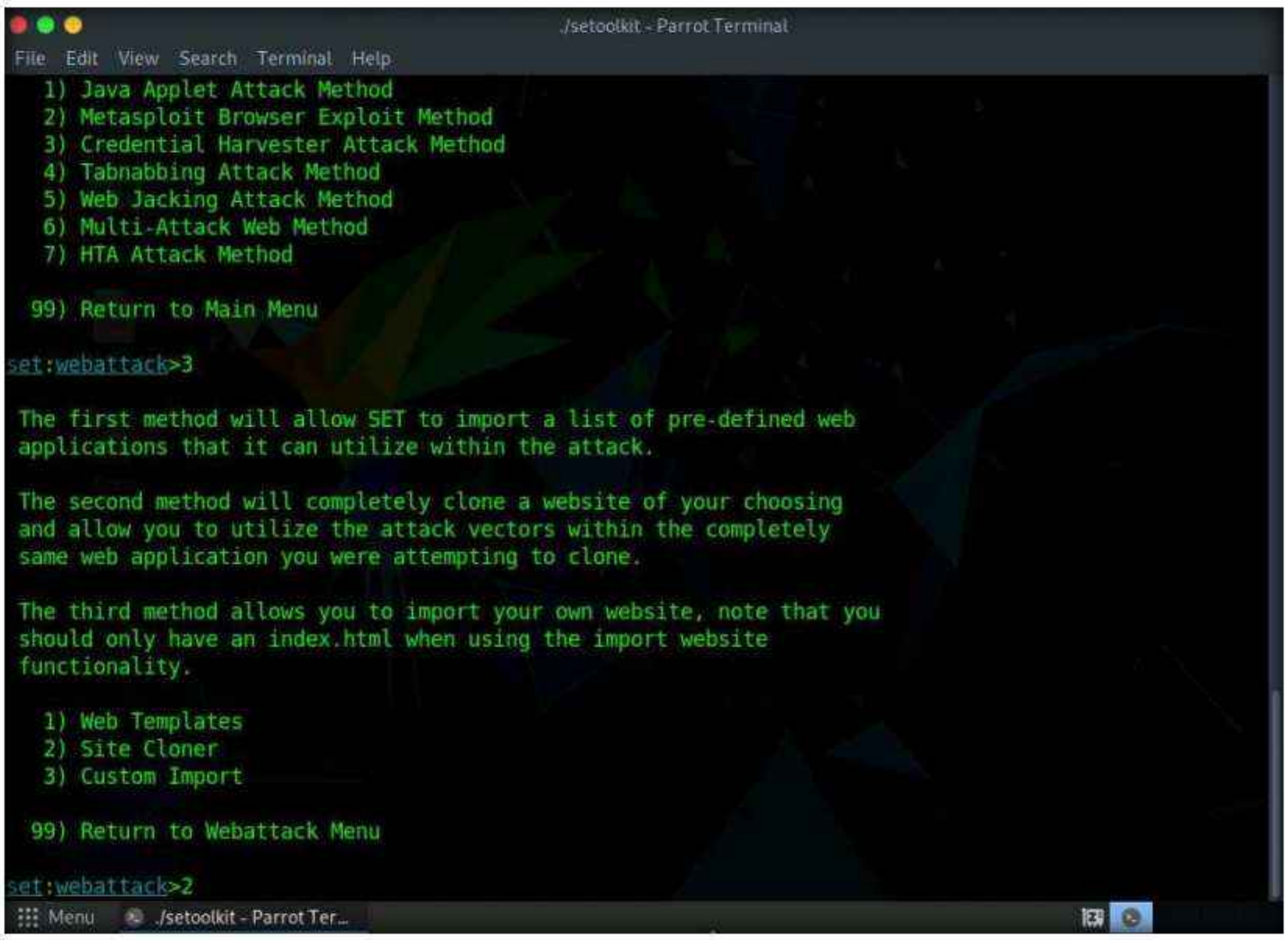


8. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.



9. A list of options in **Website Attack Vectors** appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.

10. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

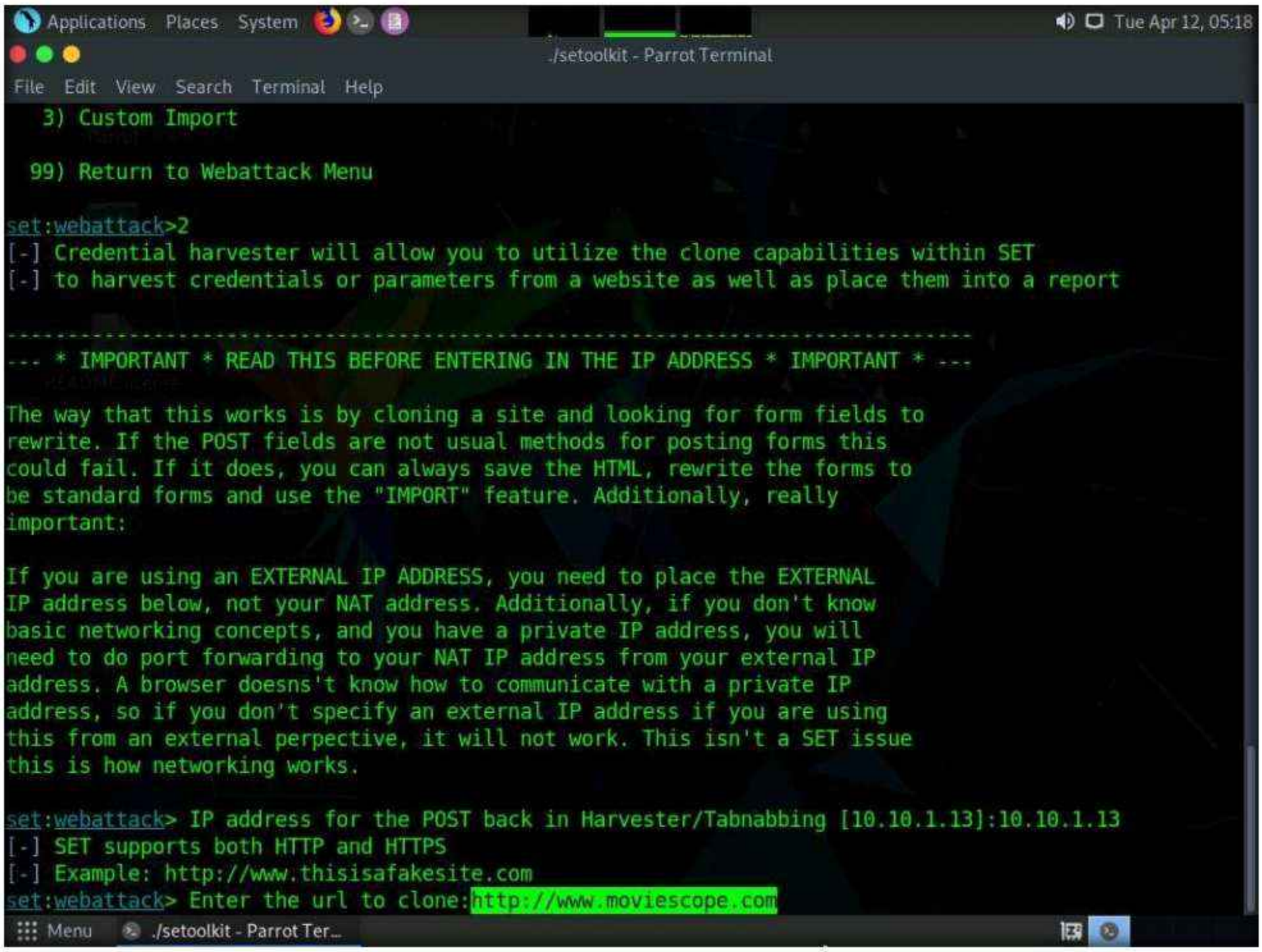


11. Type the IP address of the local machine (**10.10.1.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.

    Note: In this case, we are targeting the **Parrot Security** machine (IP address: **10.10.1.13**).

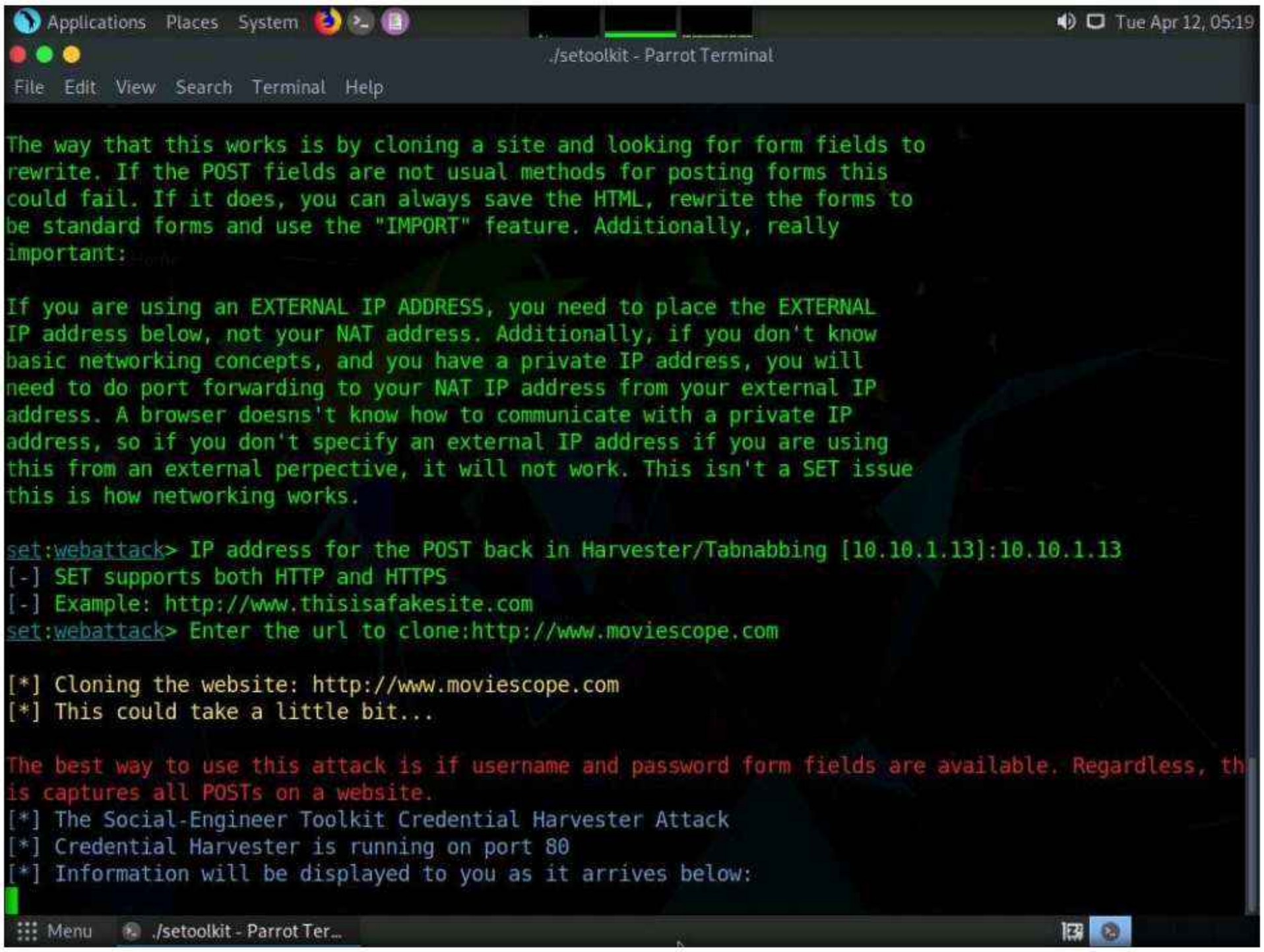
12. Now, you will be prompted for the URL to be cloned; type the desired URL in "**Enter the url to clone**" and press **Enter**. In this task, we will clone the URL **http://www.moviescope.com**.

    Note: You can clone any URL of your choice.



13. If a message appears that reads **Press {return} if you understand what we're saying here**, press **Enter**.

14. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.

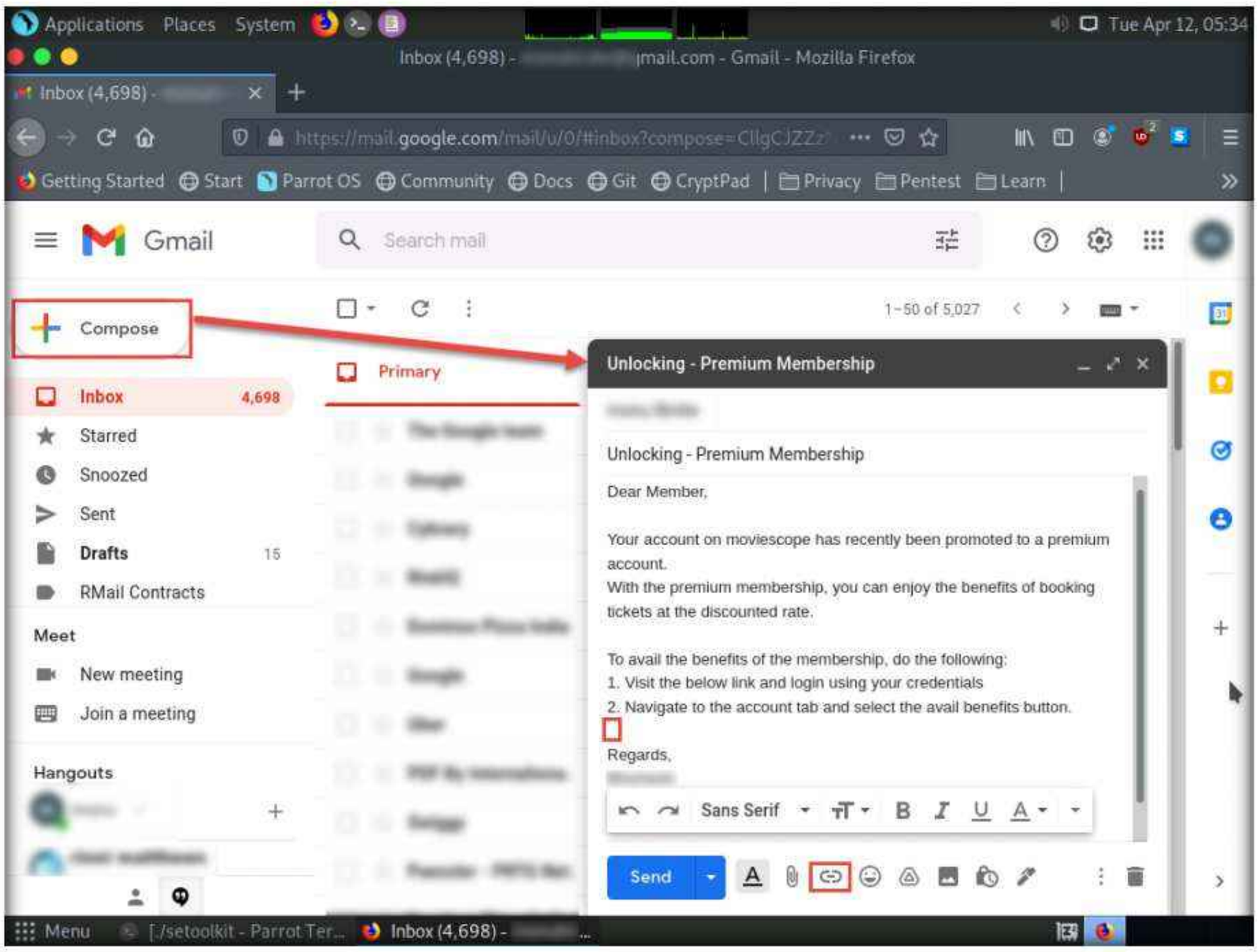


15. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.
16. Click **Firefox** icon from the top-section of the **Desktop** to launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

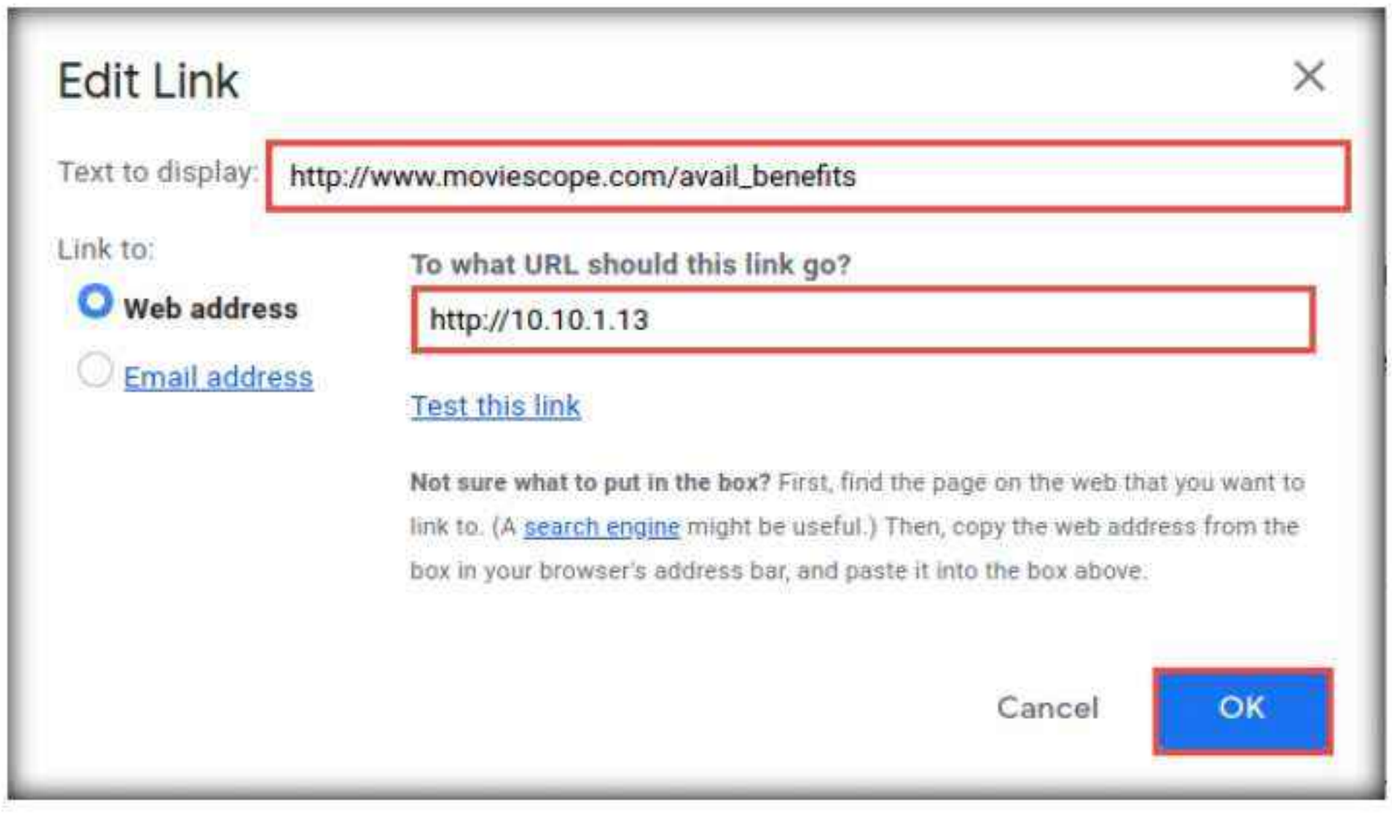
    Note: You can log in to any email account of your choice.
17. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

    Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate MovieScope URL (in this case), but that actually links to your malicious cloned MovieScope page.

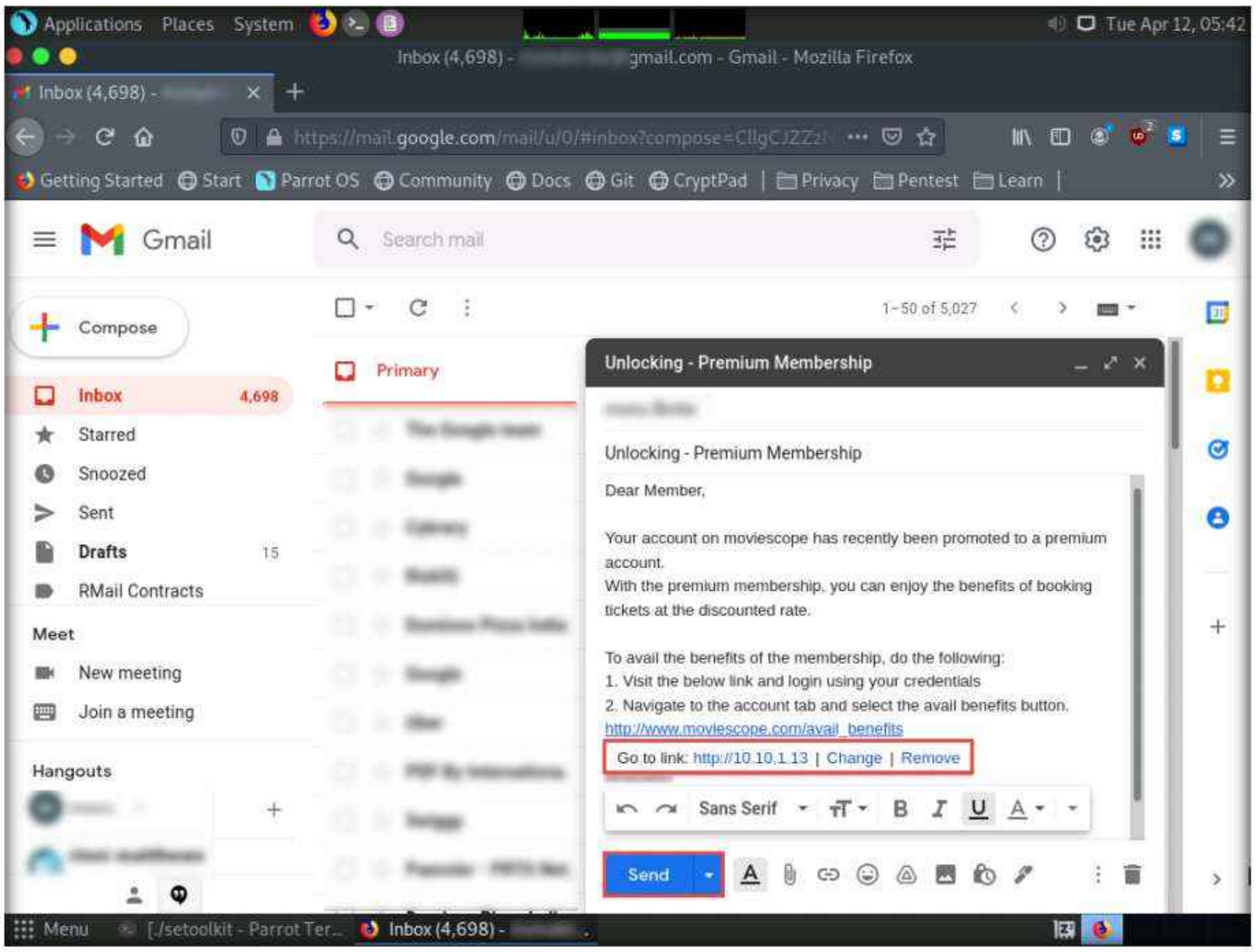
18. Position the cursor just above Regards to place the fake URL, then click the **Insert link** icon.



19. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned MovieScope site is **http://10.10.1.13**, and the text that will be displayed in the message is **http://www.moviescope.com/avail_benefits**; click **OK**.



20. The fake URL should appear in the message body, as shown in the screenshot.
21. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.

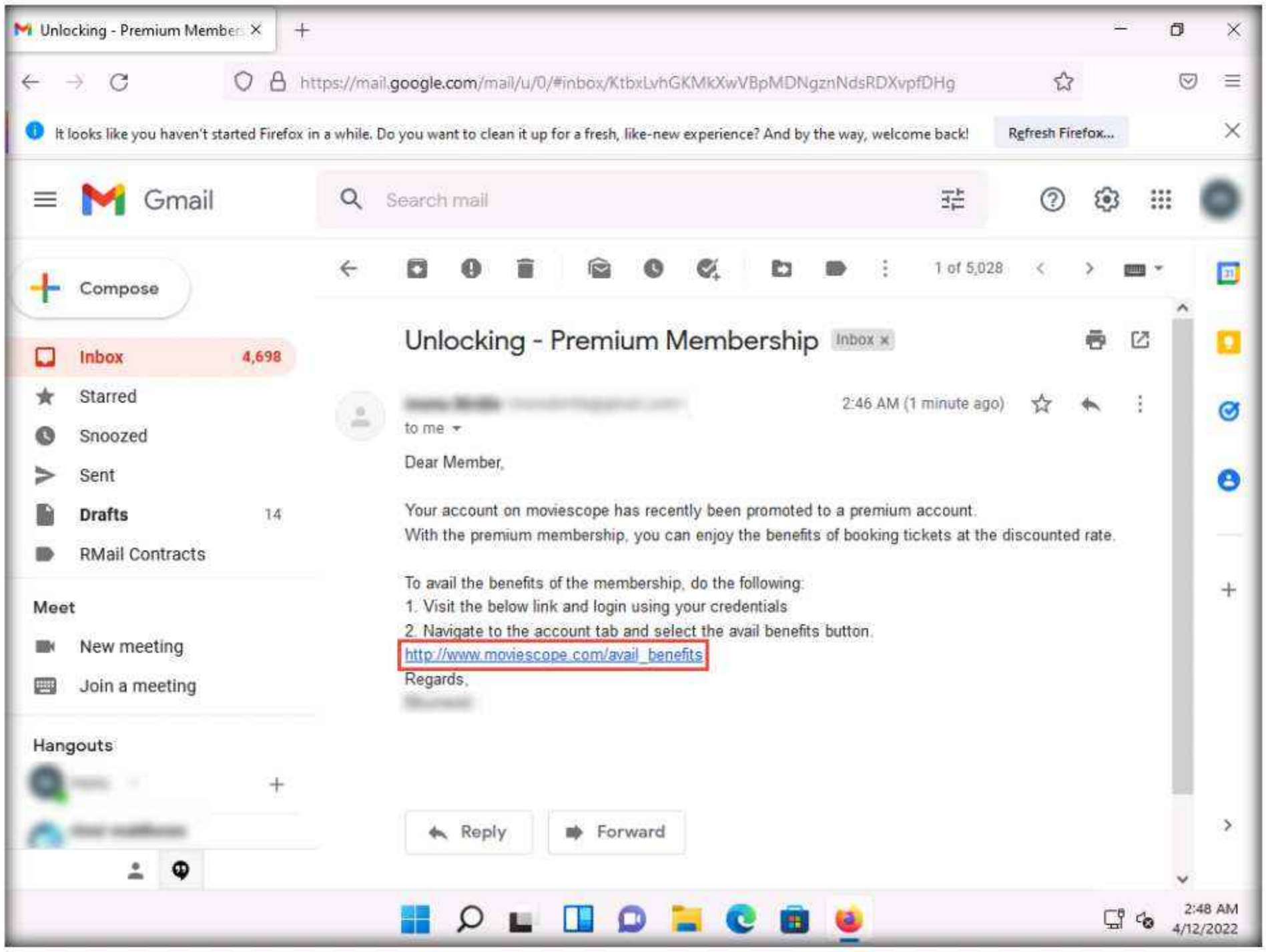


22. Switch to the **Windows 11** virtual machine and click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

    Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

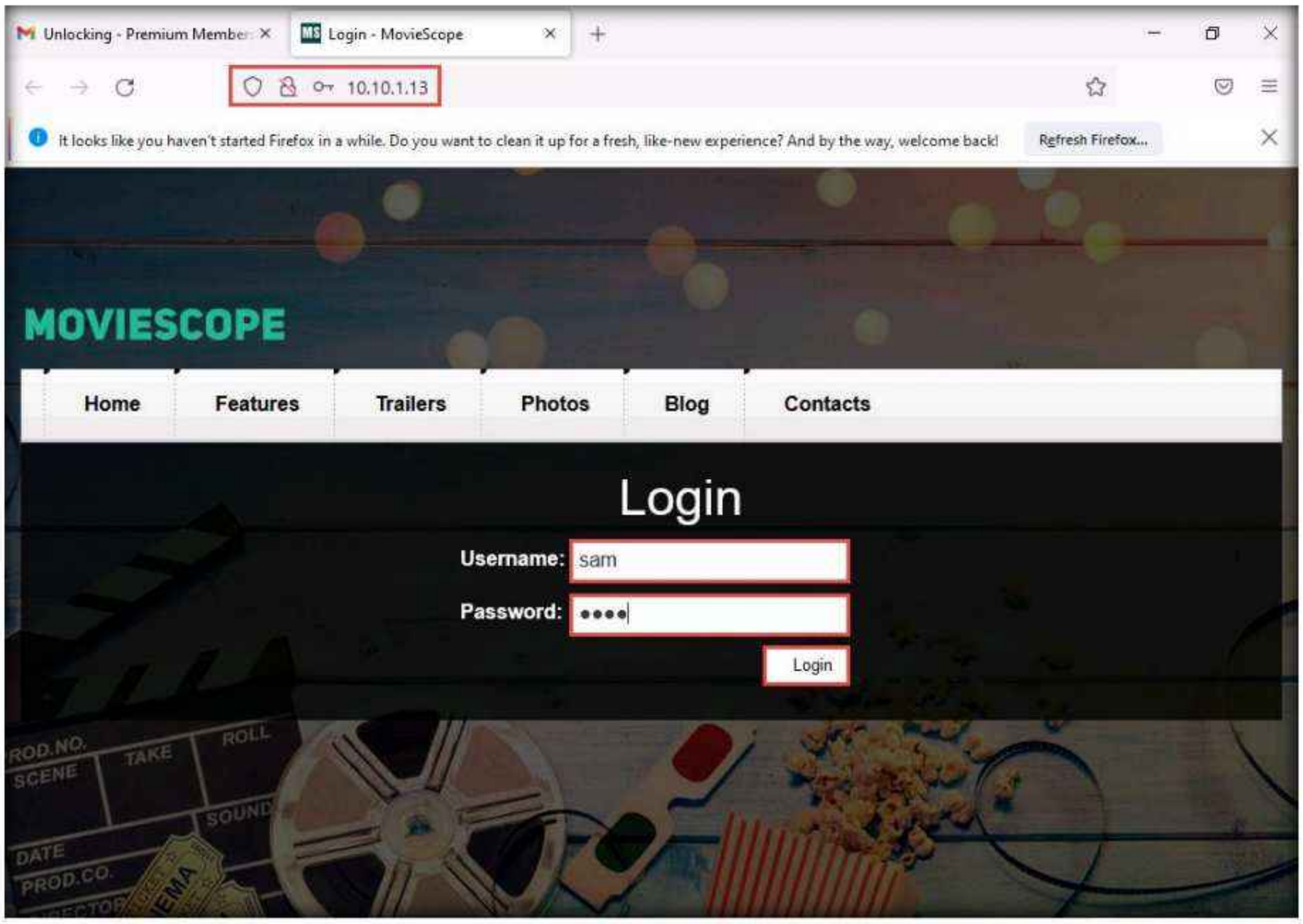
    Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

23. Open any web browser (here, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

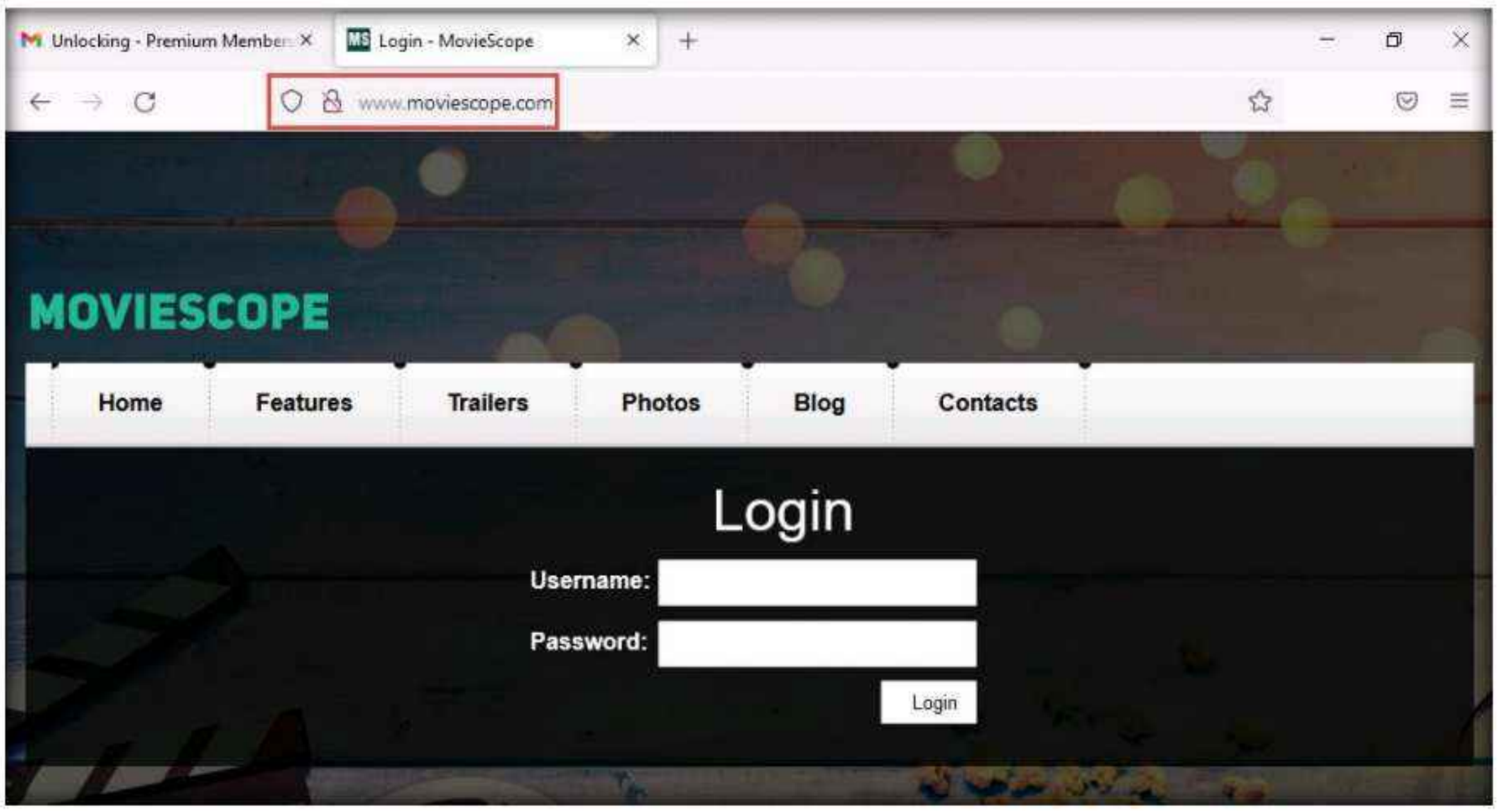


24. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.moviescope.com**.

25. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.

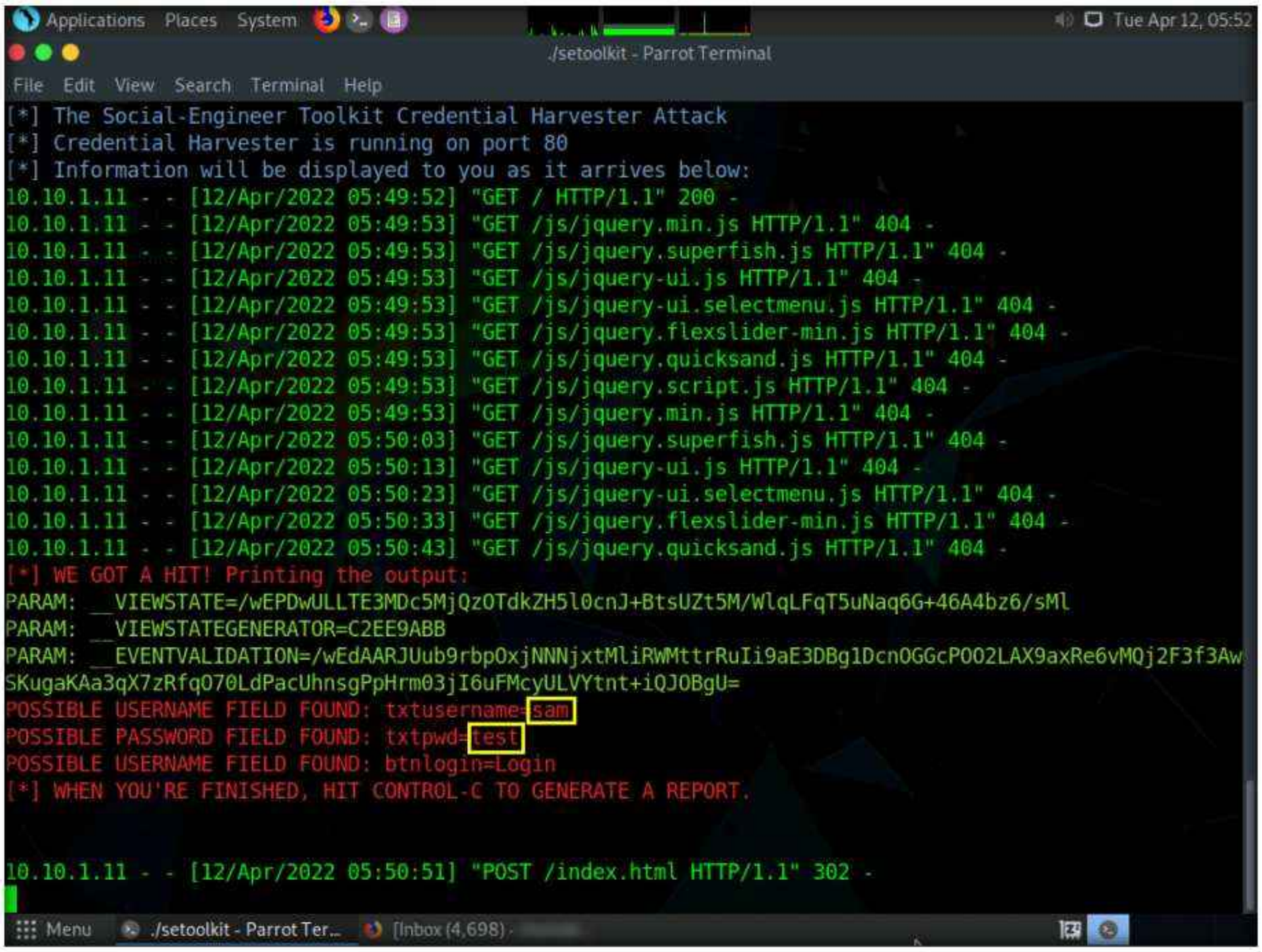


Note: If save credentials notification appears, click **Don't Save**.



26. Now, switch back to the **Parrot Security** virtual machine and switch to the **terminal** window.
27. As soon as the victim types in his/her **Username** and **Password** and clicks **Login**, **SET** extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.

28. Scroll down to find **Username** and **Password** displayed in plain text, as shown in the screenshot.



29. This concludes the demonstration of phishing user credentials using the SET.
30. Close all open windows and document all the acquired information.
31. Turn off the **Windows 11** and **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 2

Detect a Phishing Attack

Phishing is the practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information.

Lab Scenario

With the tremendous increase in the use of online banking, online shares trading, and e-commerce, there has been a corresponding growth in incidents of phishing being used to carry out financial fraud.

As a professional ethical hacker or penetration tester, you must be aware of any phishing attacks that occur on the network and implement anti-phishing measures. Be warned, however, that even if you employ the most sophisticated and expensive technological solutions, these can all be bypassed and compromised if employees fall for simple social engineering scams.

The success of phishing scams is often due to users' lack of knowledge, being visually deceived, and not paying attention to security indicators. It is therefore imperative that all people in your organization are properly trained to recognize and respond to phishing attacks. It is your responsibility to educate employees about best practices for protecting systems and information. In this lab, you will learn how to detect phishing attempts using various phishing detection tools.

Lab Objectives

- Detect phishing using Netcraft
- Detect phishing using PhishTank

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Detecting Phishing Attempts

Phishing attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against phishing attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

Lab Tasks

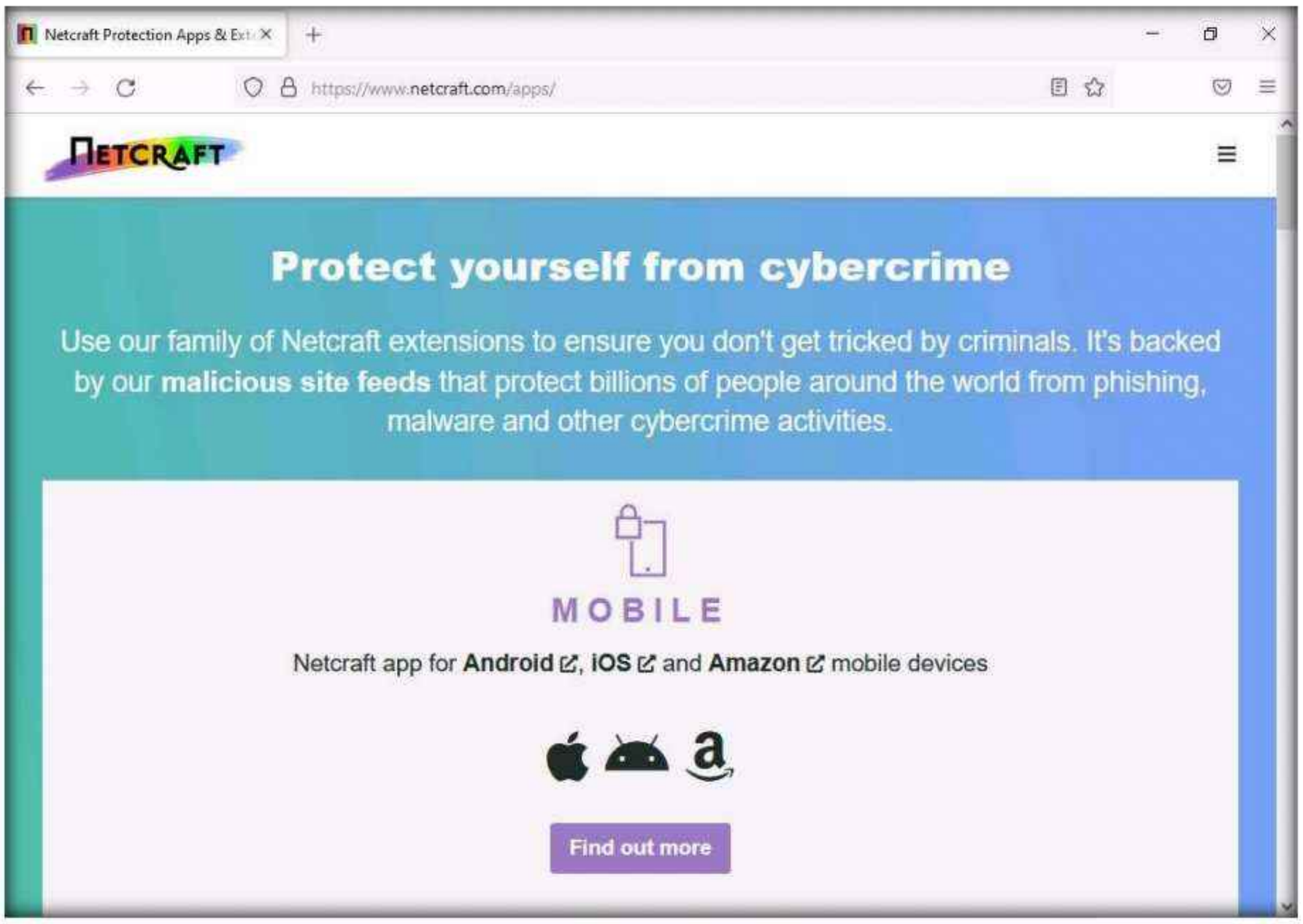
Task 1: Detect Phishing using Netcraft

The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

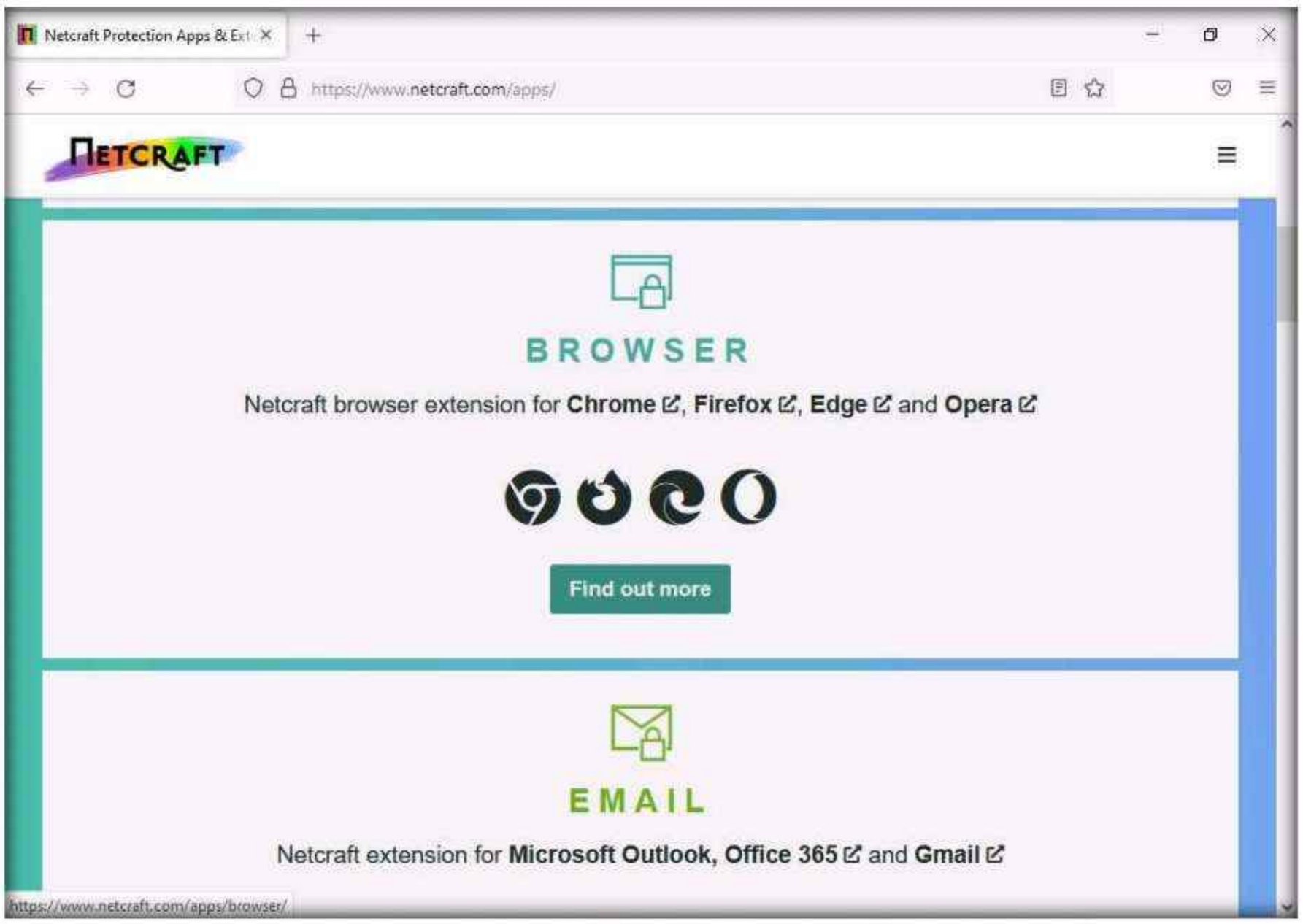
Here, we will use the Netcraft Extension to detect phishing sites.

1. Turn on the **Windows 11** virtual machine.
2. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. First, it is necessary to install the Netcraft extension. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **https://www.netcraft.com/apps/** and press **Enter**.
4. The **Netcraft** website appears, as shown in the screenshot.

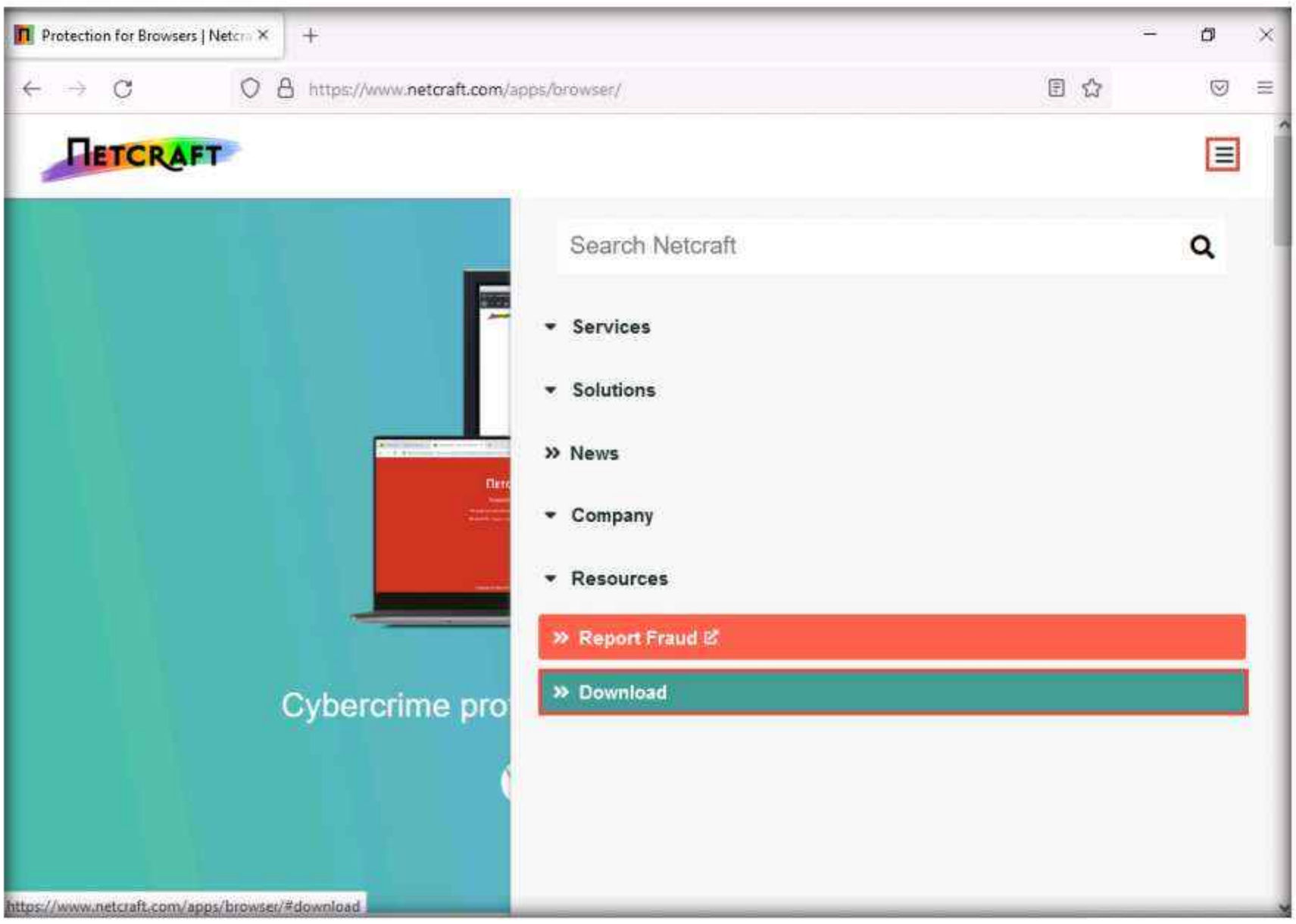
   Note: Click **Accept** in the cookie notification in the lower section of the browser.



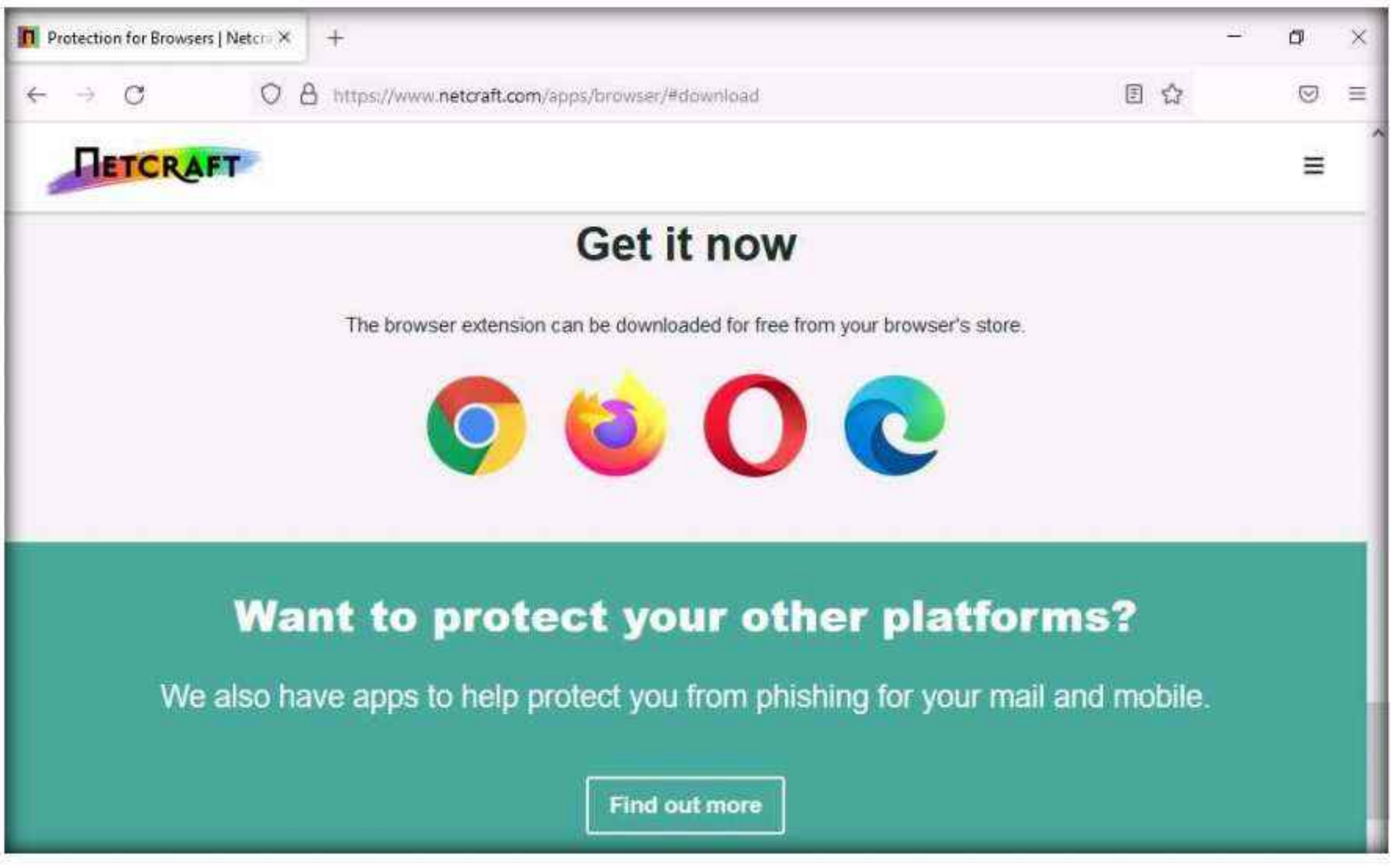
5. Scroll-down and click **Find out more** button under **BROWSER** option on the webpage.



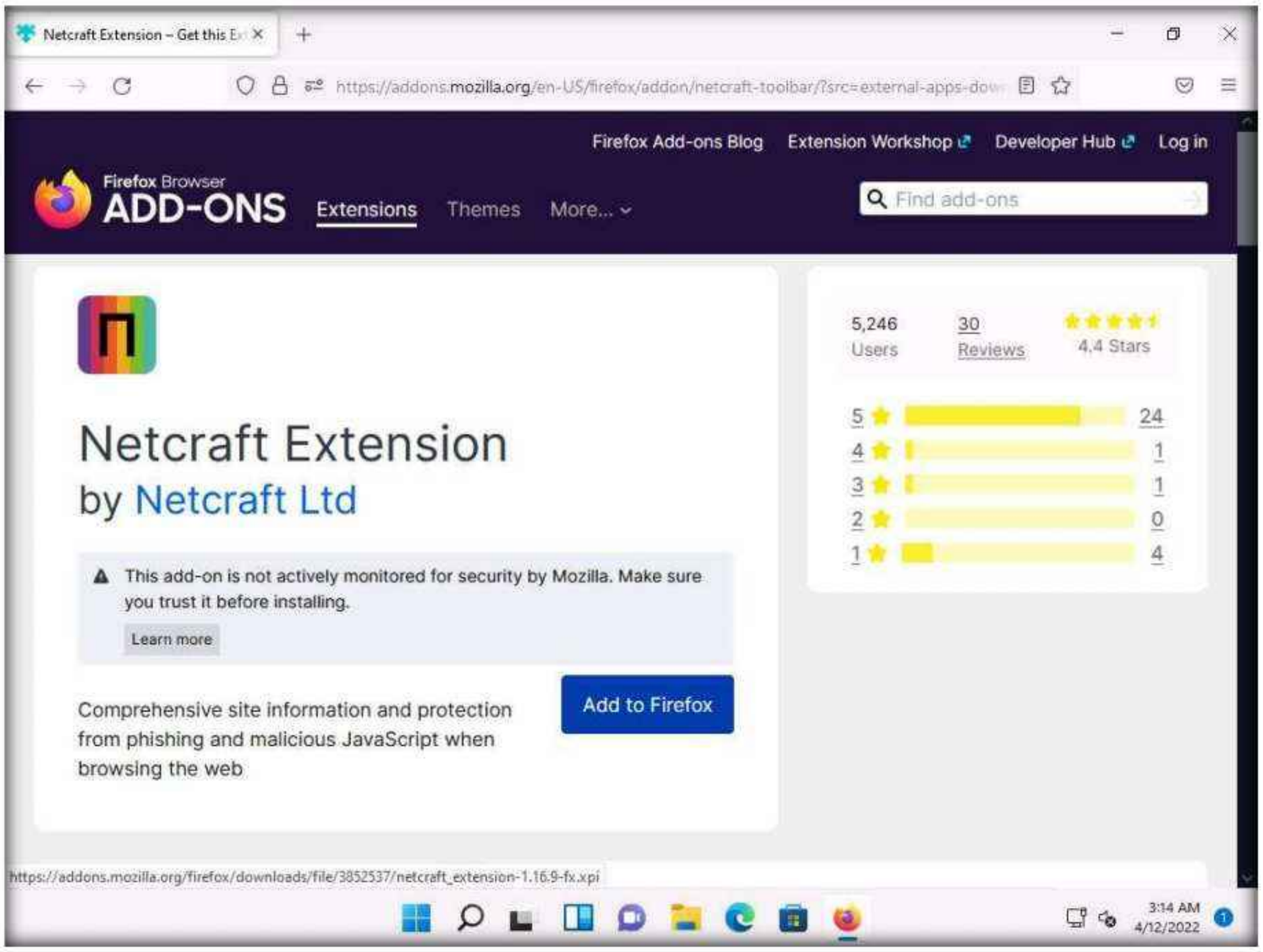
6. Click ellipses icon ( ) from the top-right corner of the webpage and click **Download** button.



7. Click ellipses icon ( ) again to close the menu.
8. You will be directed to the **Get it now** section; click the **Firefox** browser icon.

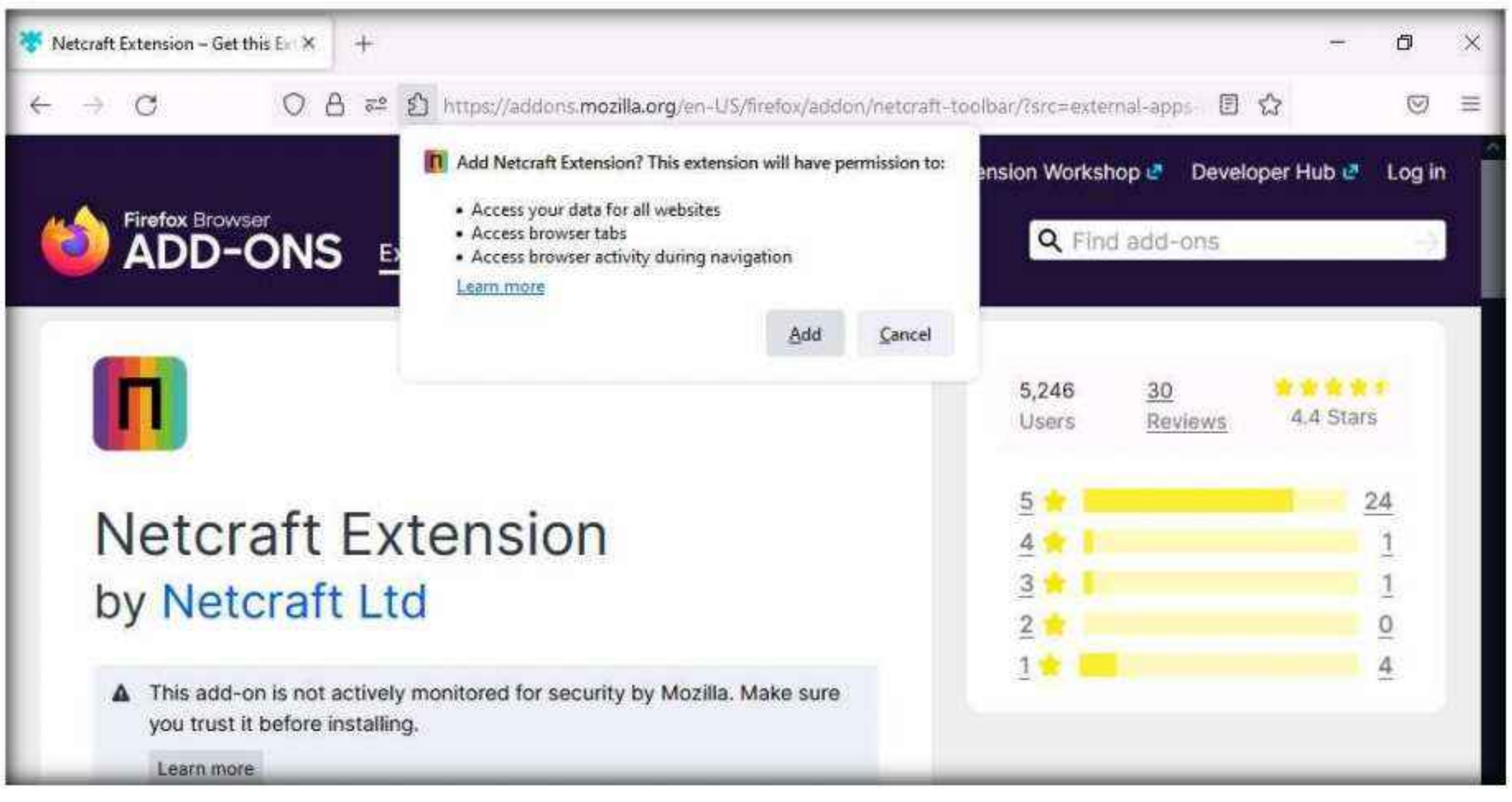


9. On the next page, click the **Add to Firefox** button to install the Netcraft extension.



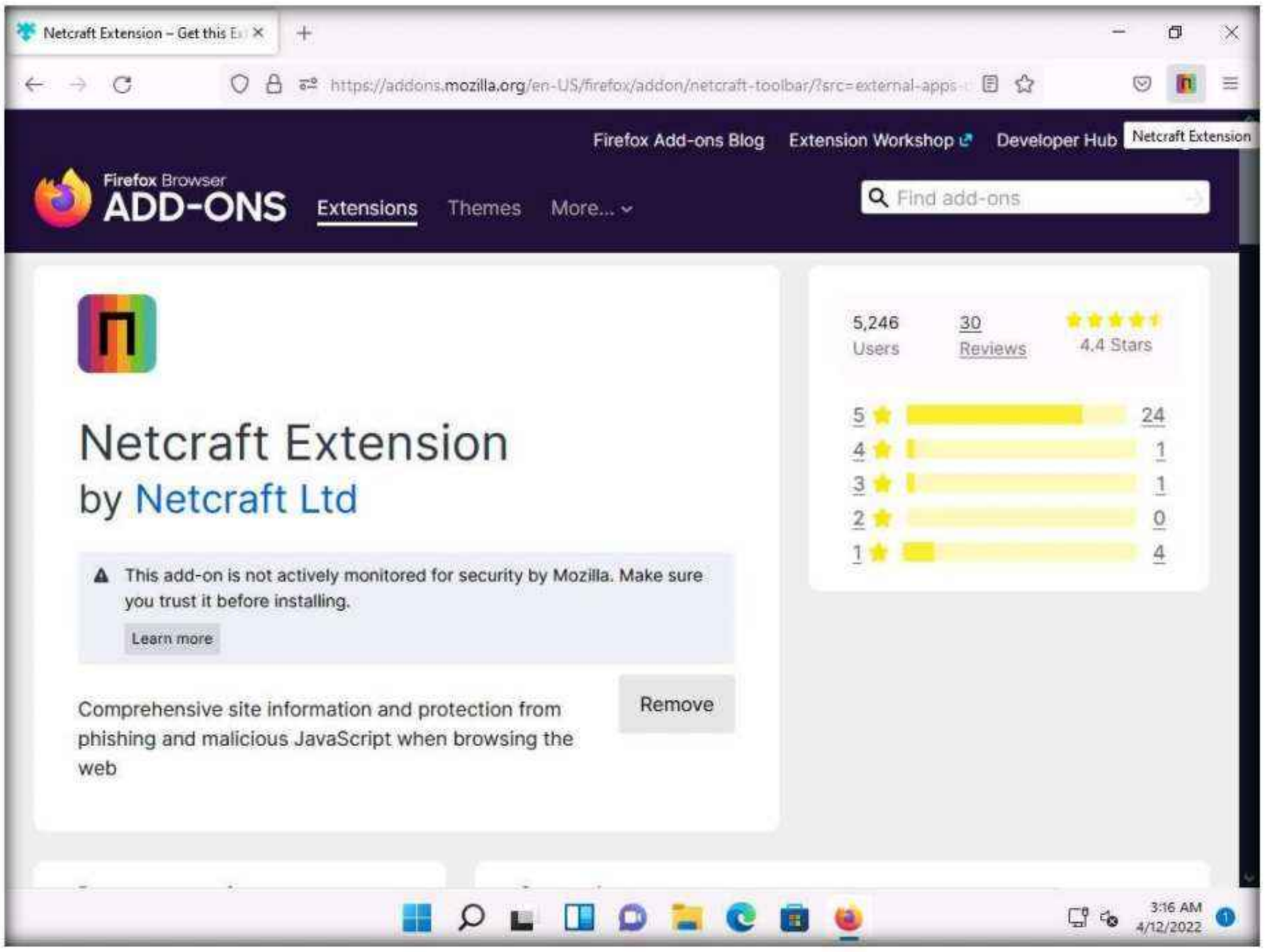
10. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

    Note: If the **Netcraft Extension has been added to Firefox** pop-up appears in the top section of the browser, click **Okay**.

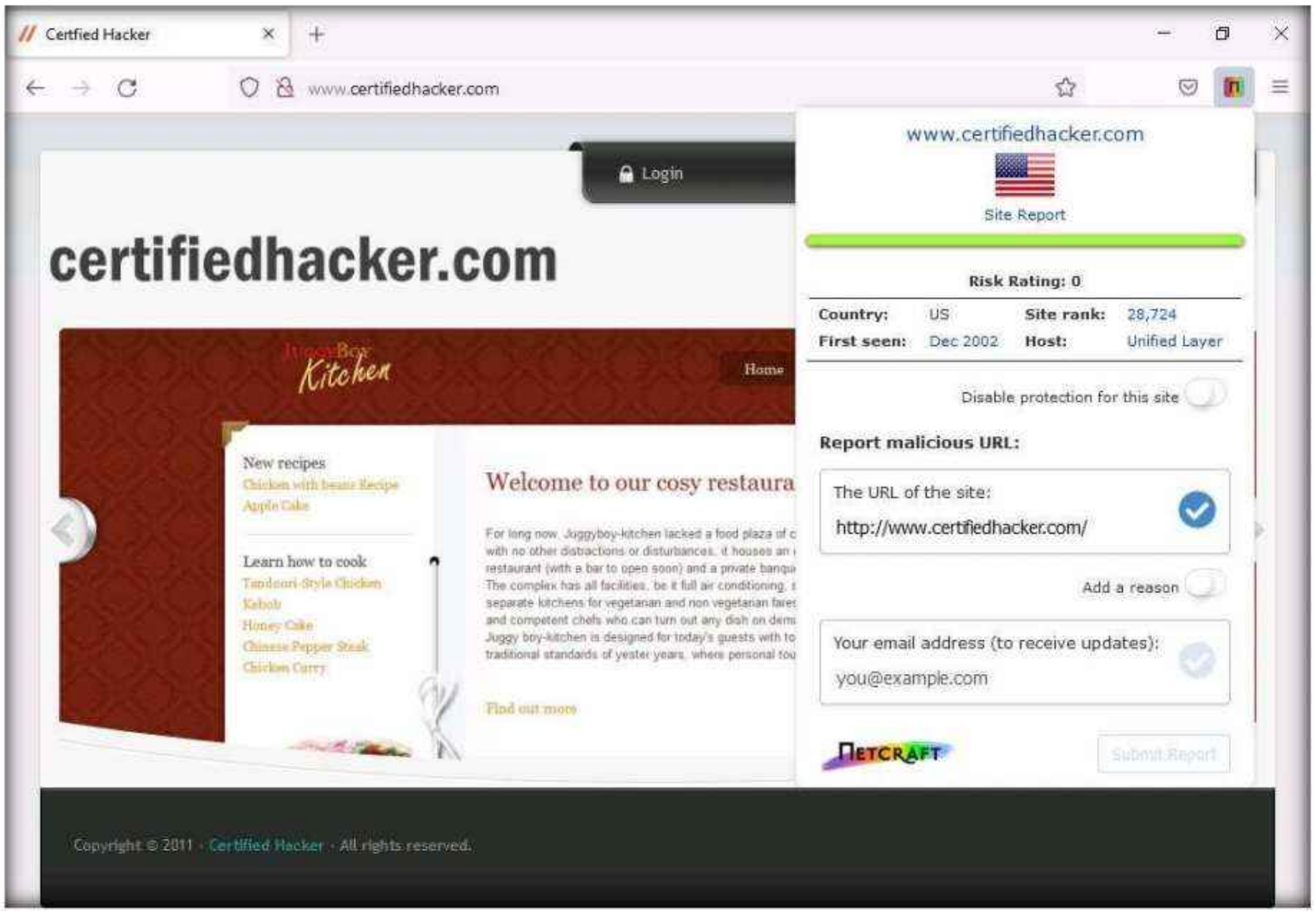


11. After the installation finishes, you may be asked to restart the browser. If so, click **Restart Now**.
12. If **Netcraft Extension has been added to Firefox** notification appears, click **Okay**, **Got it**.
13. The **Netcraft Extension** icon now appears on the top-right corner of the browser, as shown in the screenshot.

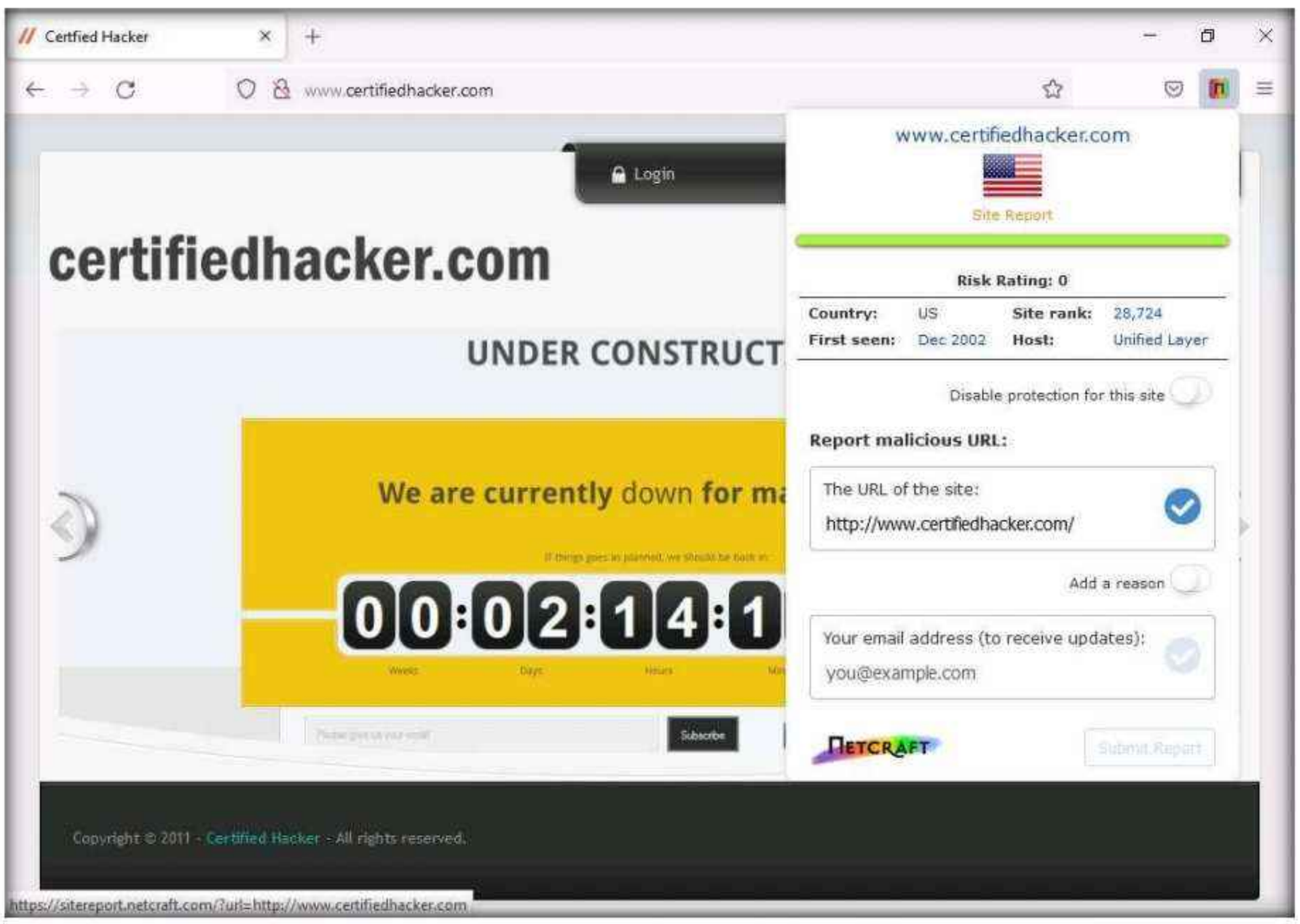
    Note: Screenshots may differ with newer versions of Firefox.



14. Now, in the address bar of the browser place your mouse cursor, type **http://www.certifiedhacker.com/** and press **Enter**.
15. The **certifiedhacker.com** webpage appears. Click the **Netcraft Extension** icon in the top-right corner of the browser. A dialog box appears, displaying a summary of information such as **Risk Rating**, **Site rank**, **First seen**, and **Host** about the searched website.

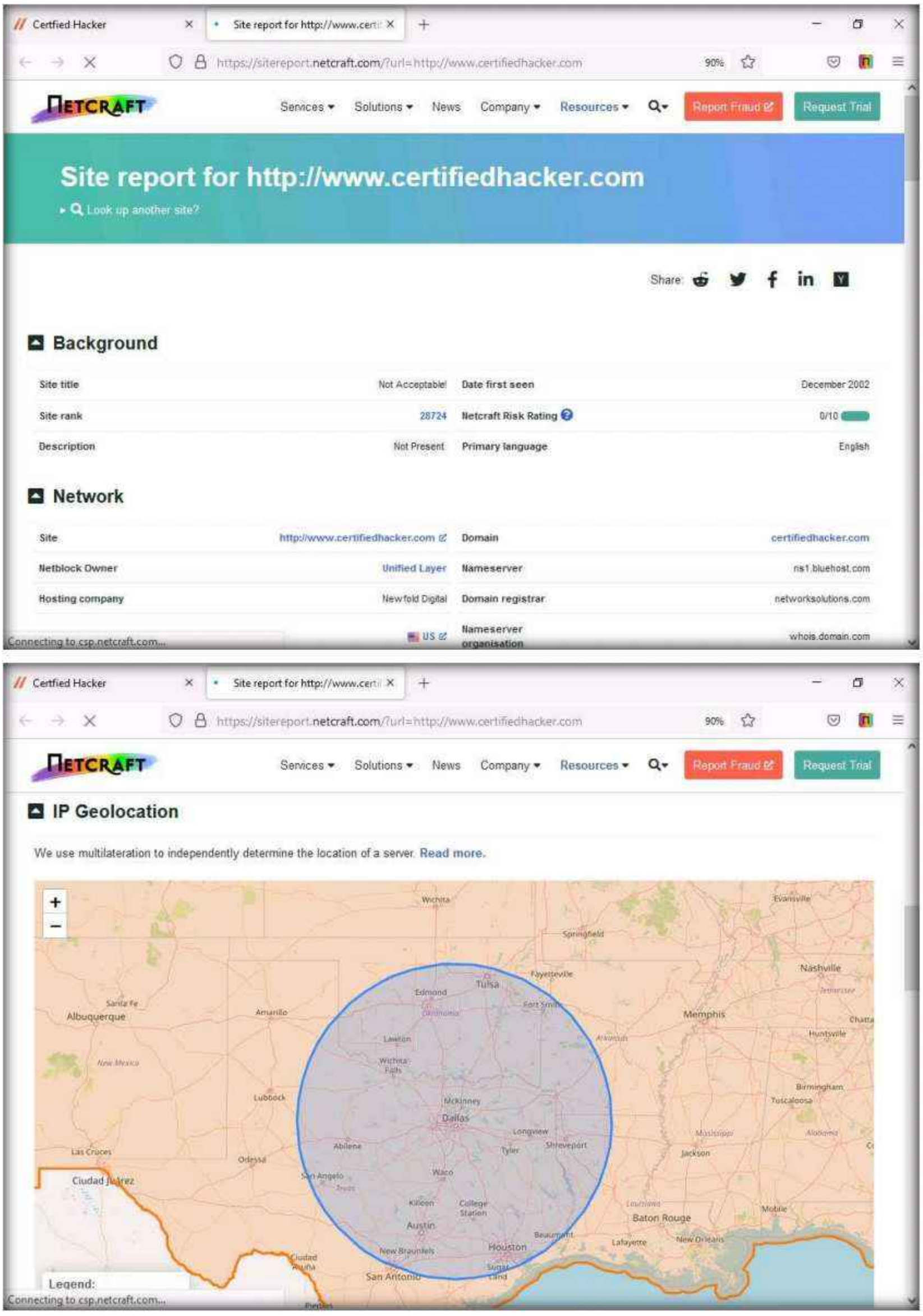


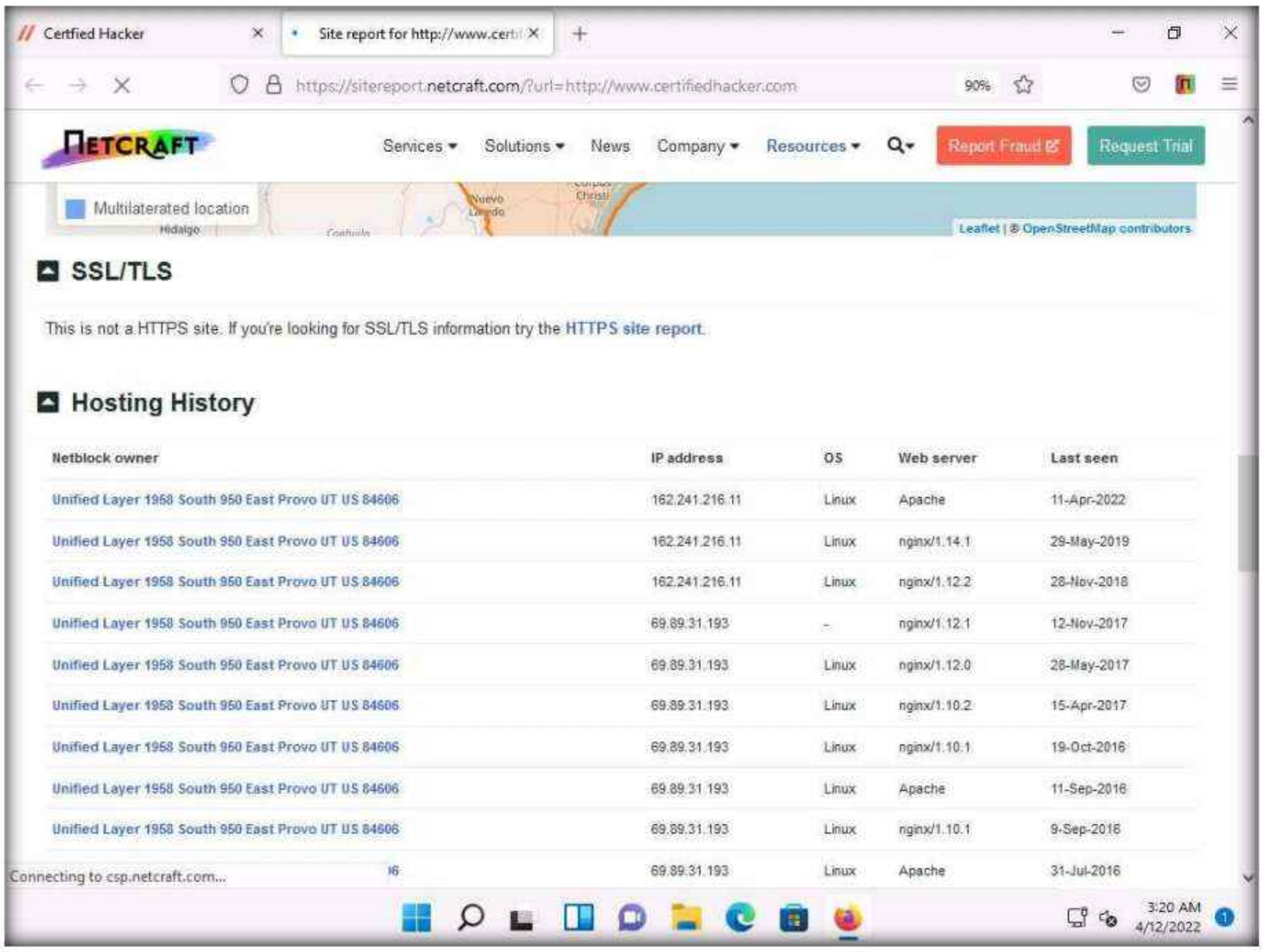
16. Now, click the **Site Report** link from the dialog-box to view a report of the site.



17. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background, Network**, **IP Geolocation**, **SSL/TLS** and **Hosting History**

    Note: If a **Site information not available** pop-up appears, ignore it.





18. If you attempt to visit a website that has been identified as a phishing site by the **Netcraft Extension**, you will see a pop-up alerting you to **Suspected Phishing**.
19. Now, in the browser window open a new tab, type **https://sfrclients.ml/** and press **Enter**.

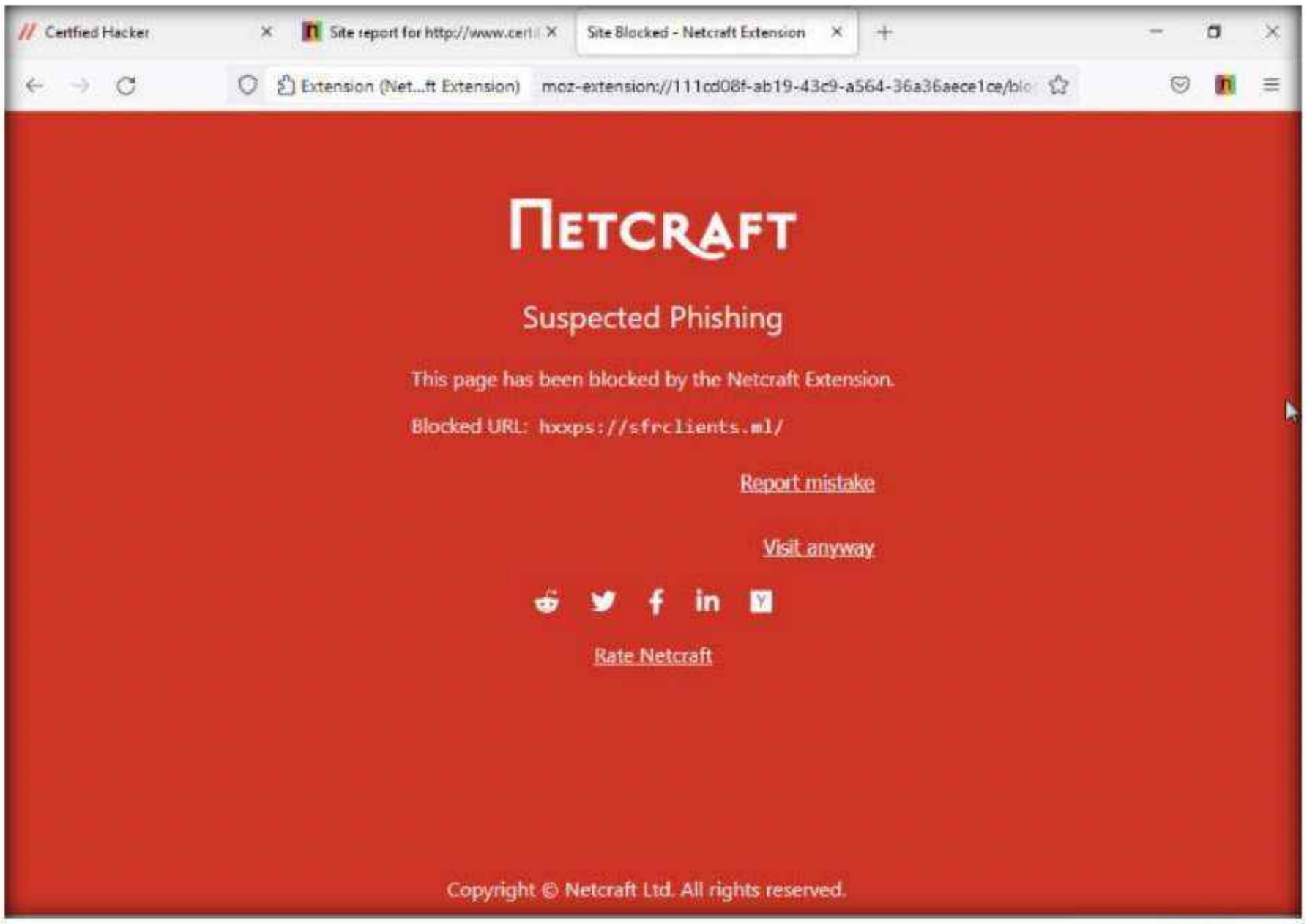
    Note: Here, for demonstration purposes, we are using **https://sfrclients.ml/** phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.
20. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

    Note: If you are getting an error in opening the website (**https://sfrclients.ml/**), try to open other phishing website.

    OR

    You will get a **Suspected Phishing** page in the **Firefox** browser.

    Note: If you get **Secure Connection Failed** webpage, then use some other phishing website to get the result, as shown in the screenshot.



21. This concludes the demonstration of detecting phishing using Netcraft Extension.
22. Close all open windows and document all the acquired information.

Task 2: Detect Phishing using PhishTank

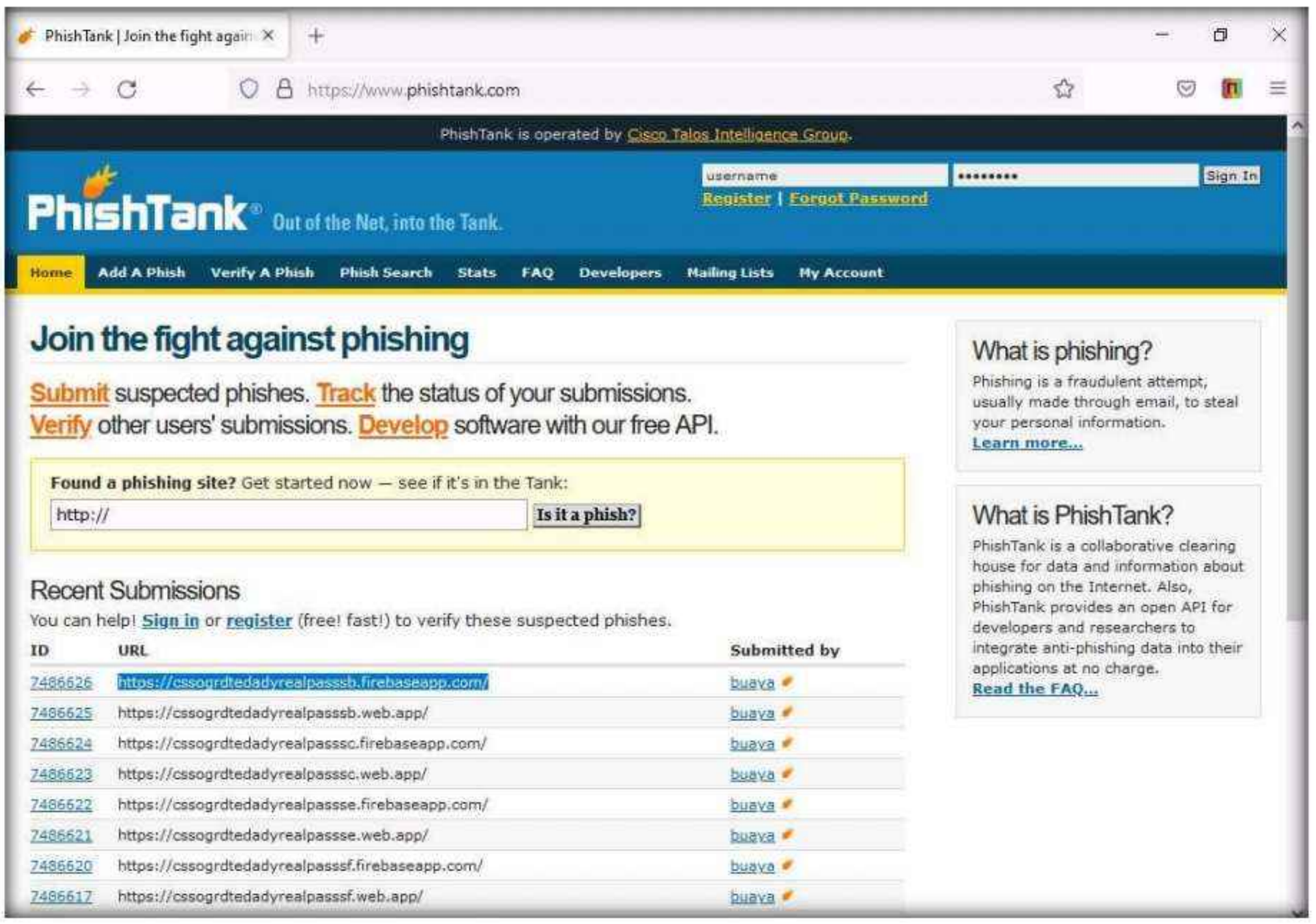
PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. As the official website notes, "it is a collaborative clearing house for data and information about phishing on the Internet." PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.

In this task, we will use PhishTank to detect phishing.

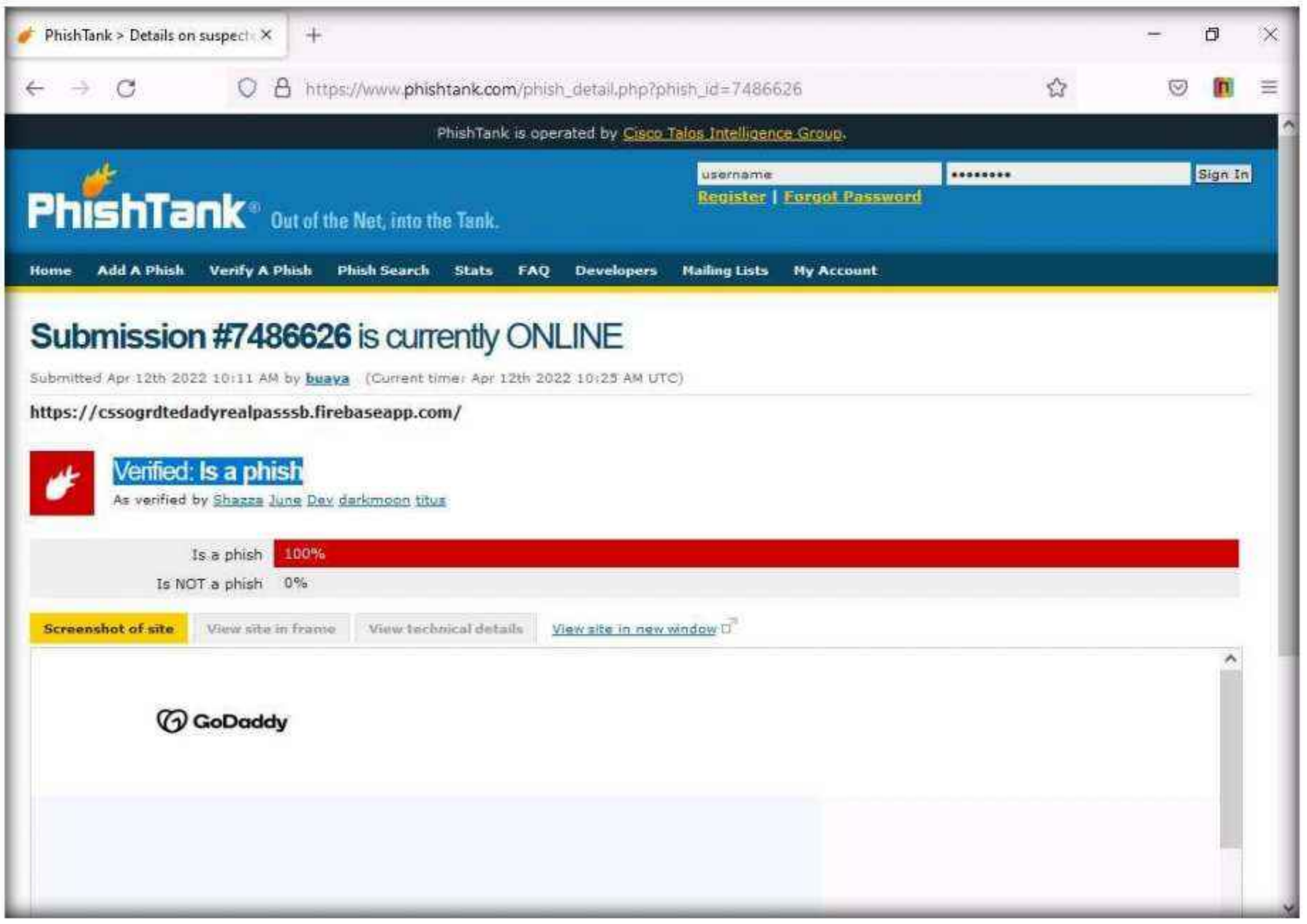
1. In the **Windows 11** machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **https://www.phishtank.com** and press **Enter**.
2. The **PhishTank** webpage appears, displaying a list of phishing websites under **Recent Submissions**.
3. Click on any phishing website **ID** in the **Recent Submissions** list (in this case, **7486626**) to view detailed information about it.

   Note: If a notification appears asking **Would you like Firefox to save this login for phishtank.com?**, click **Don't Save**.

   Note: If you are redirected to the page asking captcha, enter the captcha to proceed.



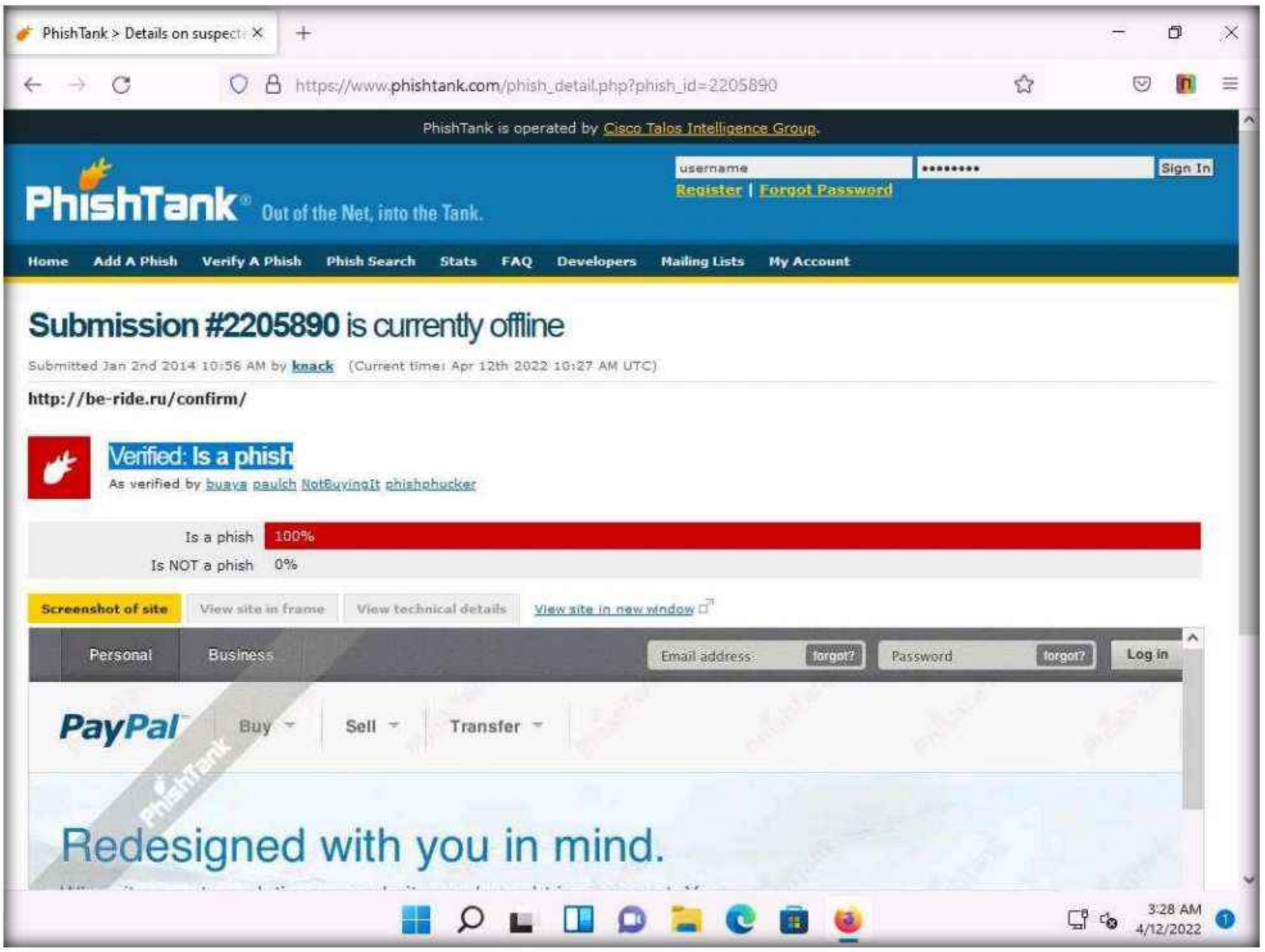
4. If the site is a phishing site, **PhishTank** returns a result stating that the website "**Is a phish**," as shown in the screenshot.



5. Navigate back to the **PhishTank** home page by clicking the **Back** button in the top-left corner of the browser.
6. In the **Found a phishing site?** text field, type a website URL to be checked for phishing (in this example, the URL entered is **be-ride.ru/confirm**). Click the **Is it a phish?** button.

Note: You can examine any website of your choice for phishing.

7. If the site is a phishing site, **PhishTank** returns a result stating that the website "**Is a phish**," as shown in the screenshot.



8. This concludes the demonstration of detecting phishing using PhishTank.
9. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 3

Audit Organization's Security for Phishing Attacks

Ethical hackers and penetration testers are aided in auditing an organization's security for phishing attacks by various tools that make security assessment an easy task.

Lab Scenario

Social engineers exploit human behavior (manners, enthusiasm toward work, laziness, innocence, etc.) to gain access to the information resources of the target company. This information is difficult to be guarded against social engineering attacks, as the victim may not be aware that he or she has been deceived. The attacks performed are similar to those used to extract a company's valuable data. To guard against social engineering attacks, a company must evaluate the risk of different types of attacks, estimate the possible losses, and spread awareness among its employees.

As a professional ethical hacker or pen tester, you must perform phishing attacks in the organization to assess the awareness of its employees.

As an administrator or penetration tester, you may have implemented highly sophisticated and expensive technology solutions; however, all these techniques can be bypassed if the employees fall prey to simple social engineering scams. Thus, employees must be educated about the best practices for protecting the organization's systems and information.

In this lab, you will learn how to audit an organization's security for phishing attacks within the organization.

Lab Objectives

- Audit organization's security for phishing attacks using OhPhish

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection

- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview

In phishing attacks, attackers implement social engineering techniques to trick employees into revealing confidential information of their organization. They use social engineering to commit fraud, identity theft, industrial espionage, and so on. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

To be truly effective in combating social engineering attacks, an organization should do the following:

- Disseminate policies among its employees and provide proper education and training.
- Provide specialized training benefits to employees who are at a high risk of social engineering attacks.
- Obtain signatures of employees on a statement acknowledging that they understand the policies.
- Define the consequences of policy violations.

Lab Tasks

Task 1: Audit Organization's Security for Phishing Attacks using OhPhish

---

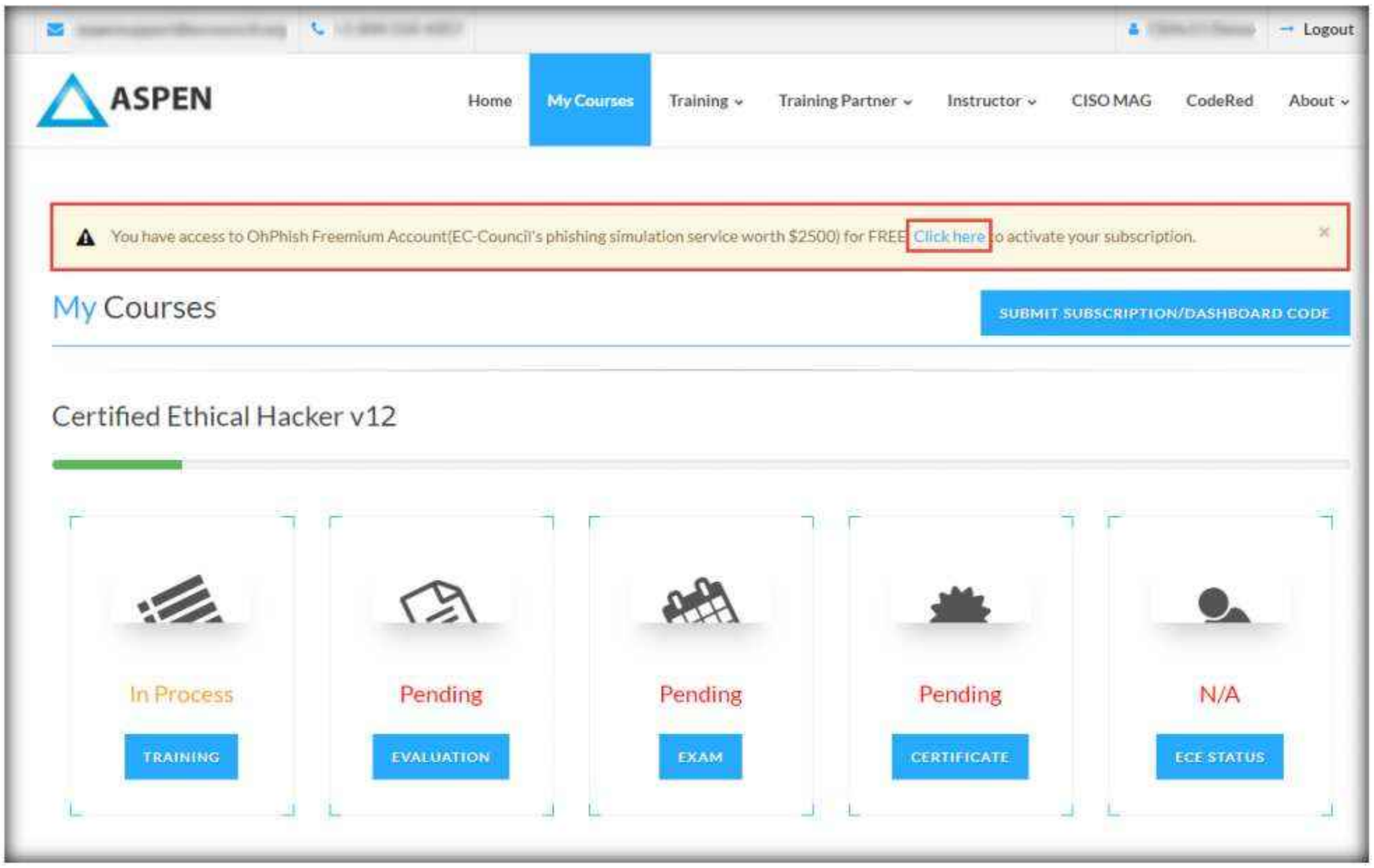
OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

Here, we will audit the organization's security infrastructure for phishing attacks using OhPhish.

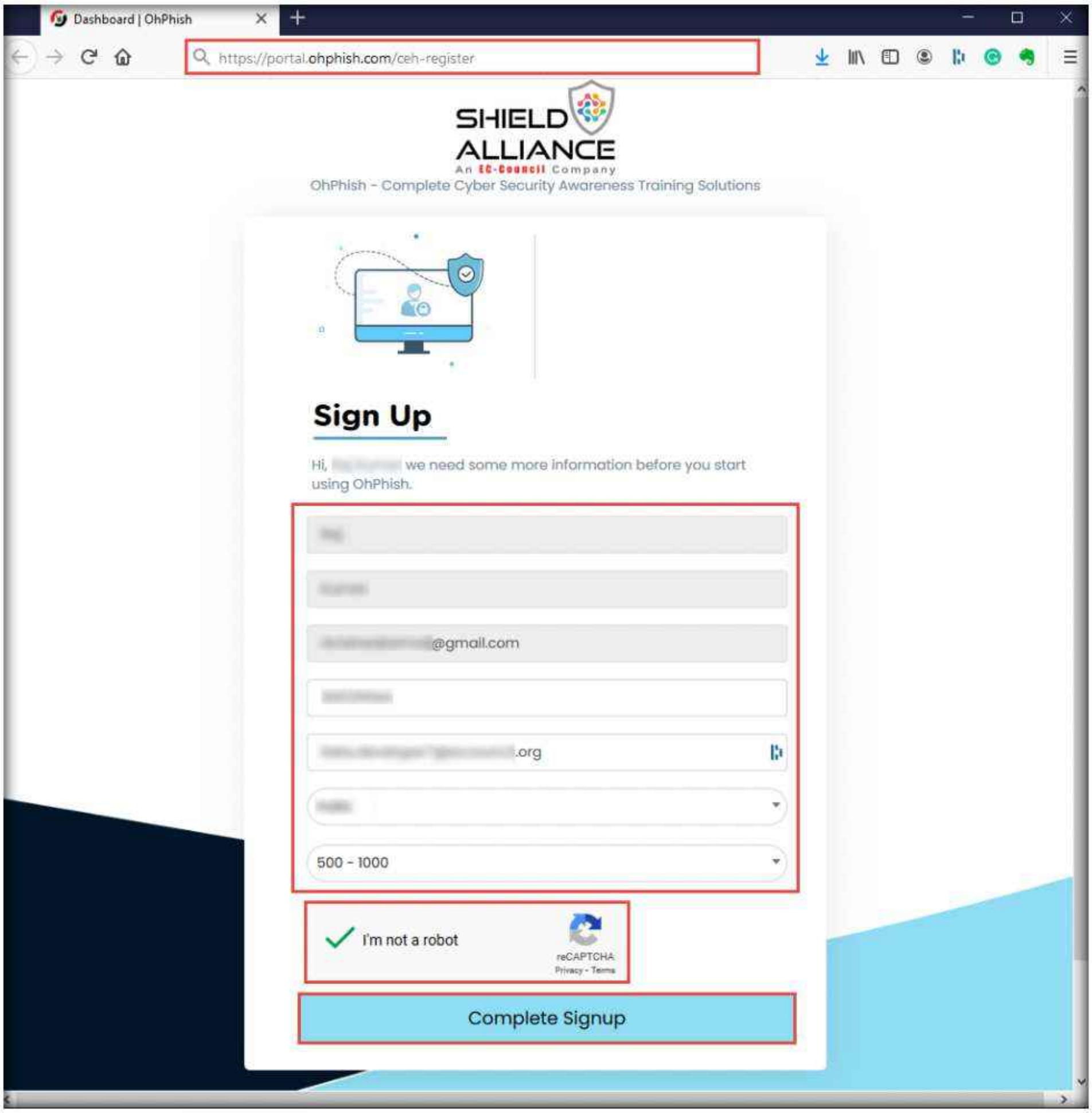
1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Before starting this task, you must activate your **OhPhish** account.
4. Open any web browser (here, **Mozilla Firefox**). Log in to your **ASPEN** account and navigate to **Certified Ethical Hacker v12** in the **My Courses** section.

Note: If you do not have an ASPEN account or access to CEHv12 program on ASPEN, please write to **support@eccouncil.org** for an OhPhish account. Once your account is setup, you will receive an email from **aware@eccouncil.org** with an account activation link. Upon activation, continue from **STEP 14**.

5. Click on **Click here** hyperlink in the **OhPhish** notification above **My Courses** section.

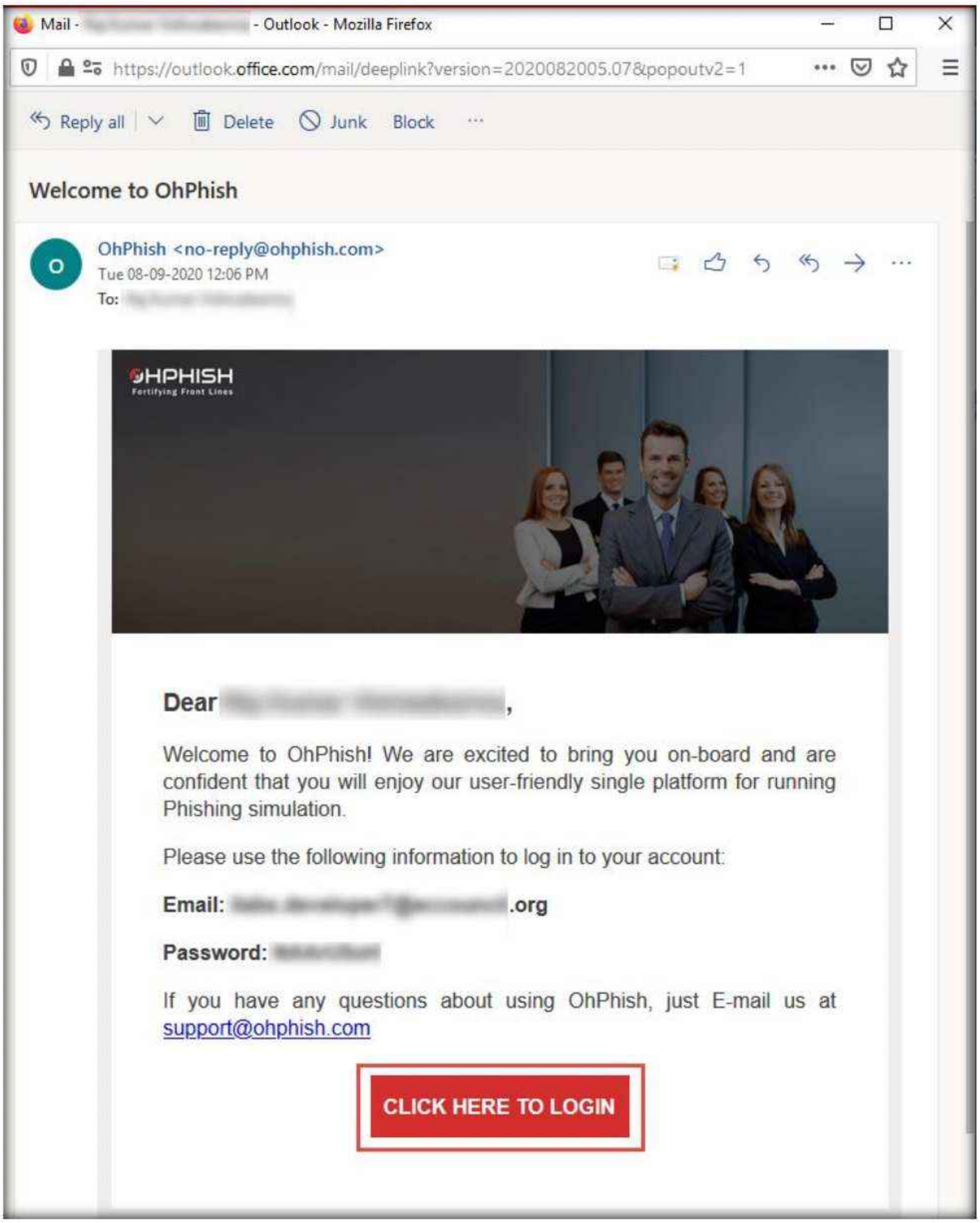


6. You will be redirected to the OhPhish **Sign Up** page. Enter the remaining personal details, check **I'm not a robot** checkbox and click **Complete Signup** button.



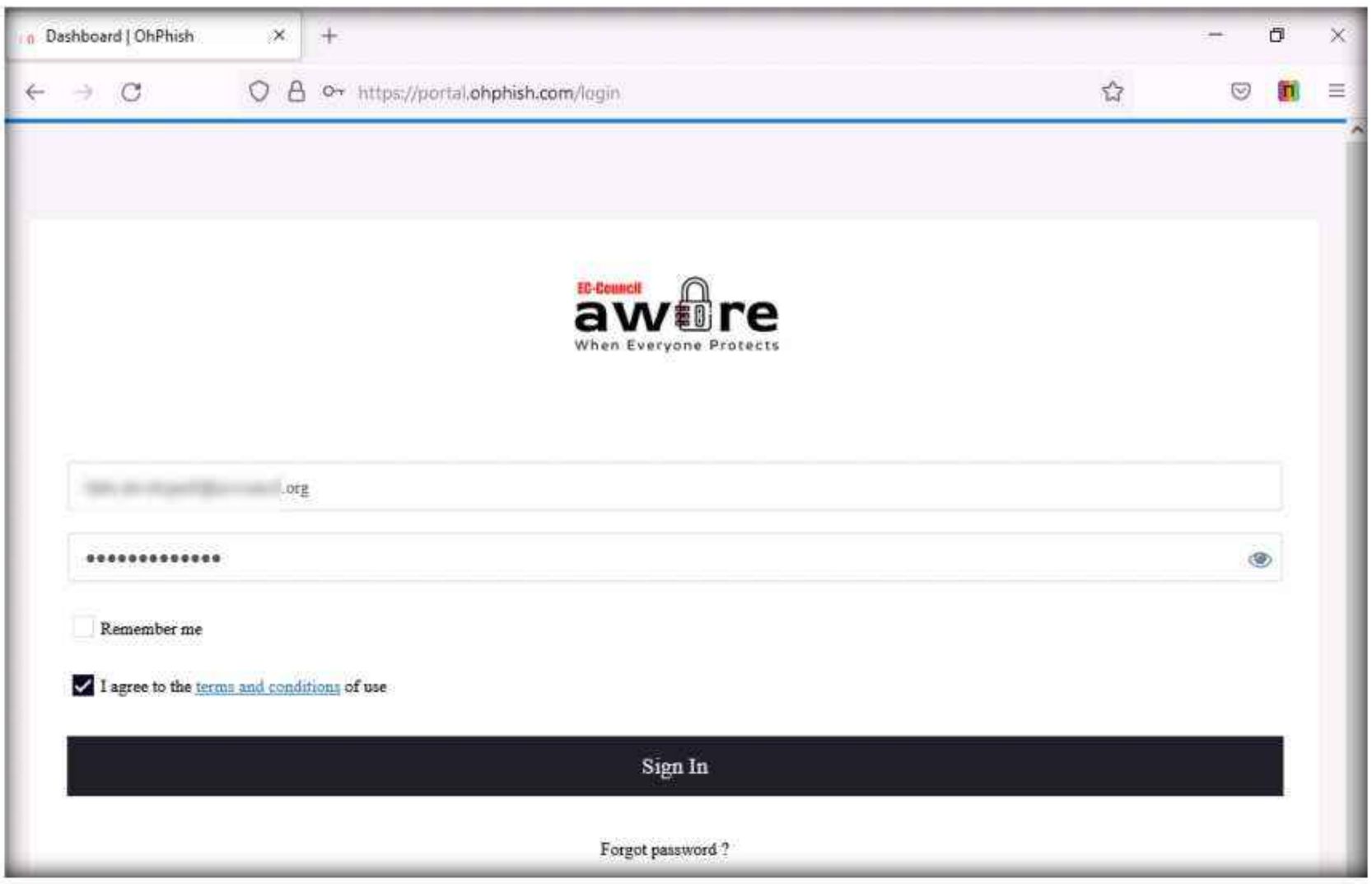
7. Account creation **Alert!** appears, click **OK**.

8. Now, open your email account given during registration process. Open an email from **OhPhish** and in the email, click **HERE TO LOGIN** button.

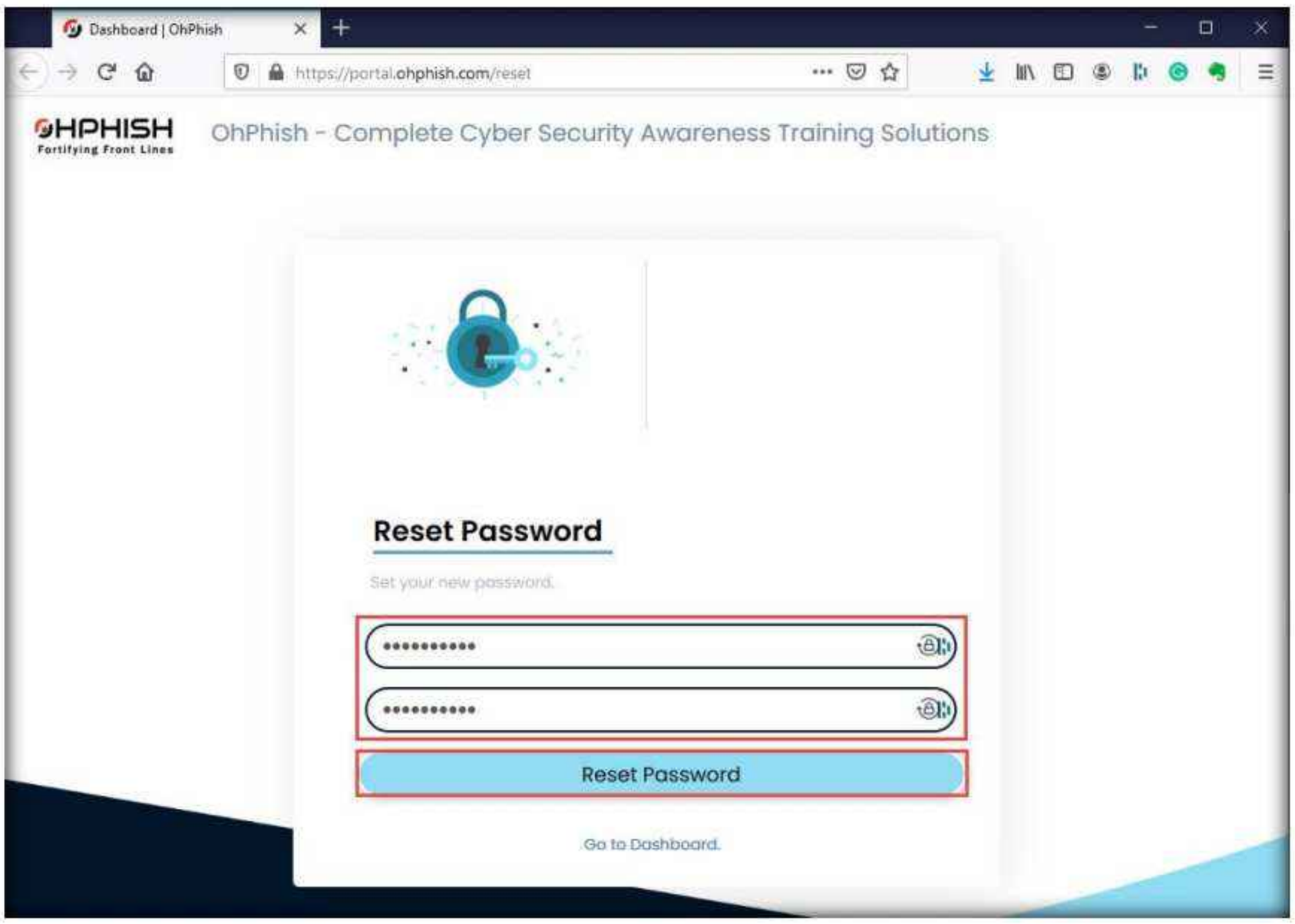


9. **EC-Council Aware** page appears, in the **Username** field enter your email address and click **Next**. In the next page, enter your password in the **Password** field and click **Sign In**.

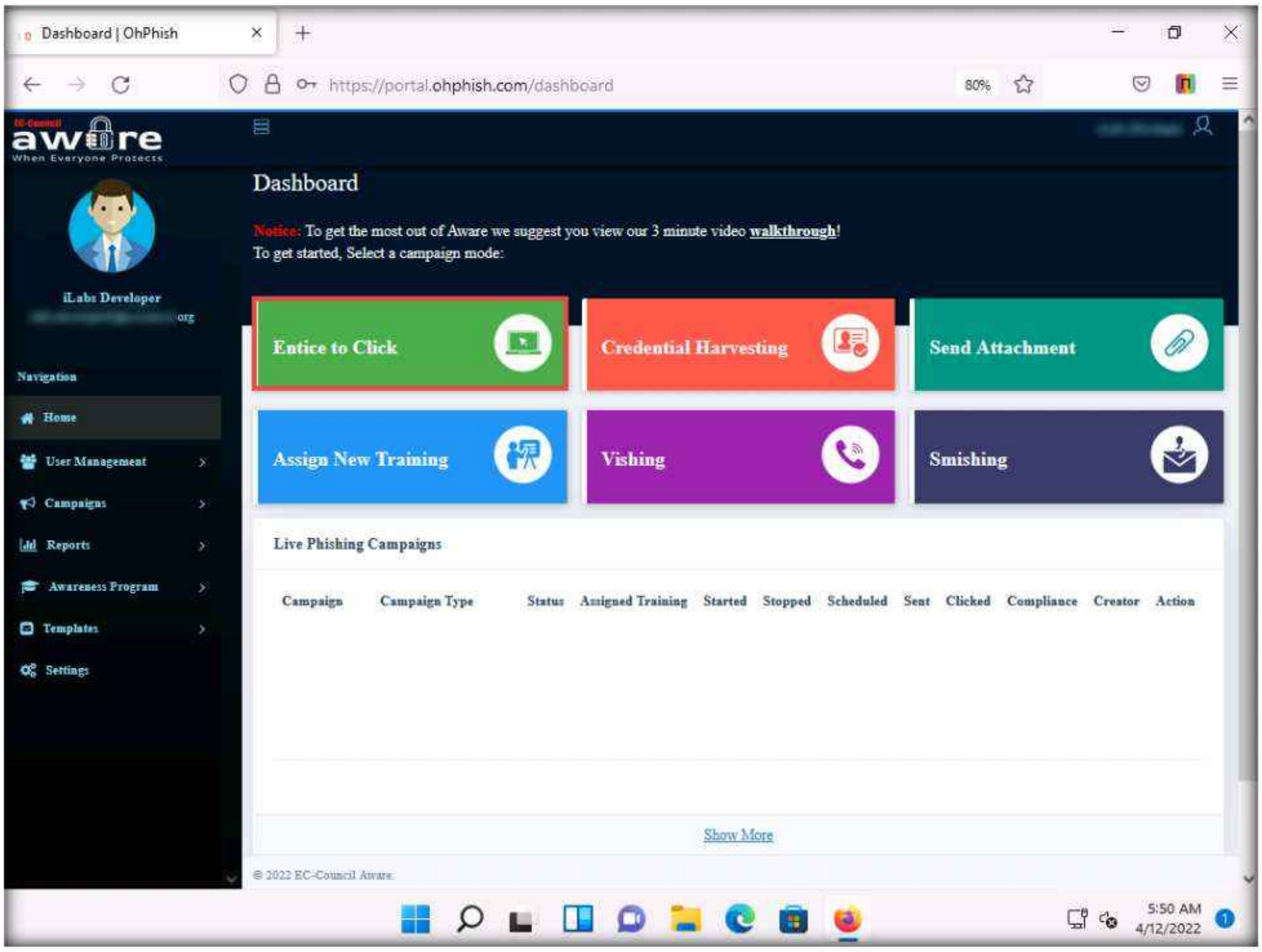
   Note: If **Save login for ohphish.com?** notification appears, click **Don't Save**.



10. You will be redirected to **Reset Password** page, enter the new password in both the fields and click **Reset Password** button to reset the password.



11. Your account password is changed successfully.
12. Now, you can login to your OhPhish account either by clicking on the **LOGIN TO OHPHISH PORTAL** button in your **ASPEN** account under **My Courses** section or you can navigate to the OhPhish website (**https://portal.ohphish.com/login**) and login using your credentials.
13. Once you login to your OhPhish account you will be redirected to the OhPhish **Dashboard**.
14. In the OhPhish **Dashboard**, click on the **Entice to Click** option.



15. The **Create New Email Phishing Campaign** form appears.

    Note: If the **OhPhish Helpdesk** notification appears in the right corner of the dashboard, close it.

    Note: **Almost Done** pop-up appears, click **DISCARD CHANGES**.

16. In the **Campaign Name** field, enter any name (here, **Test - Entice to Click**). In the **Select Template Category** field, select **Coronavirus/COVID-19** from the drop-down list.

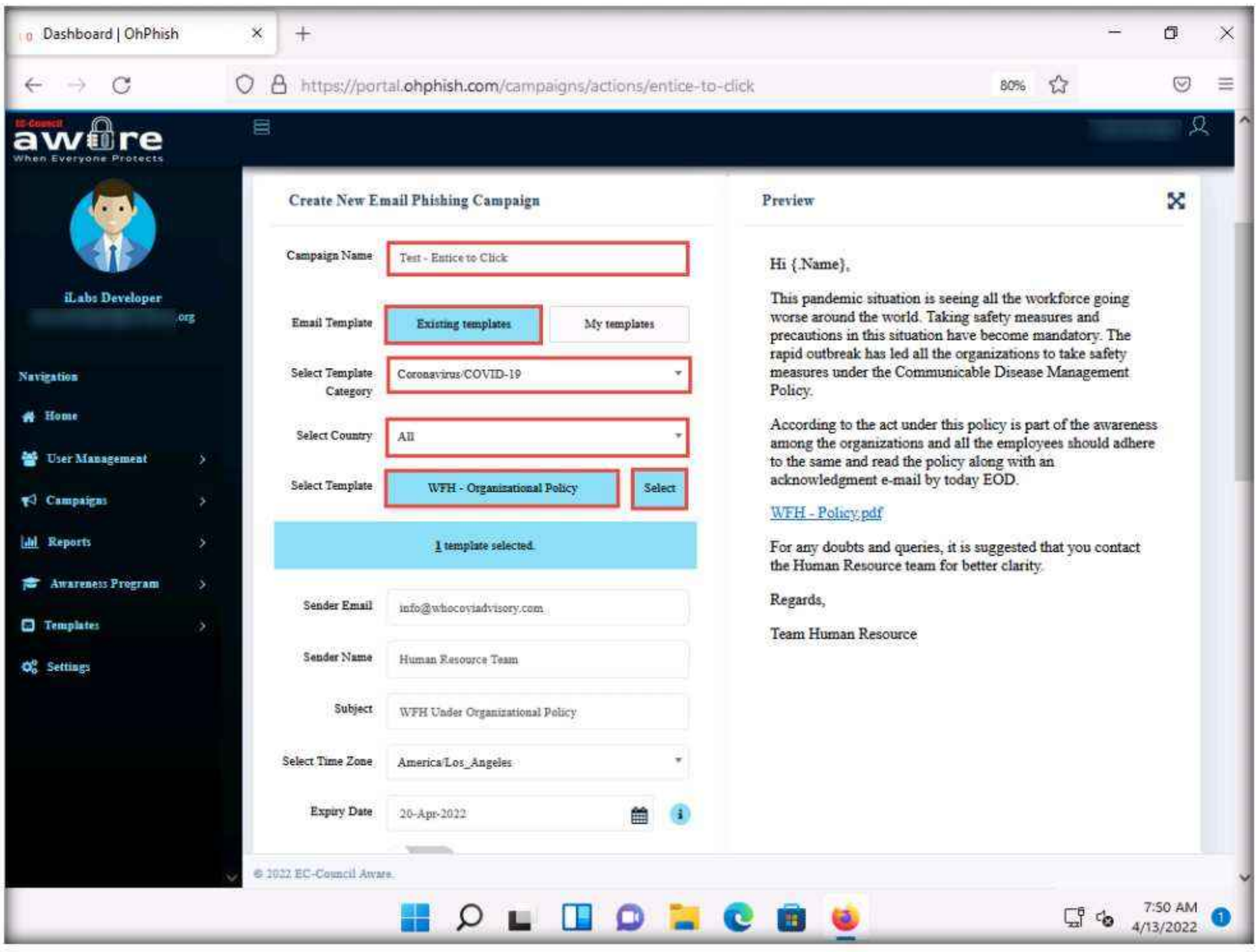
    Note: Ensure that the **Existing Template** is selected in the **Email Template** option.

17. In the **Select Country** field, leave the default option selected (**All**).

18. In the **Select Template** field, click the **Select Template** button and select **Work From Home: COVID-19** from the drop-down list.

19. Click the **Select** button in the **Select Template** field to select the template.

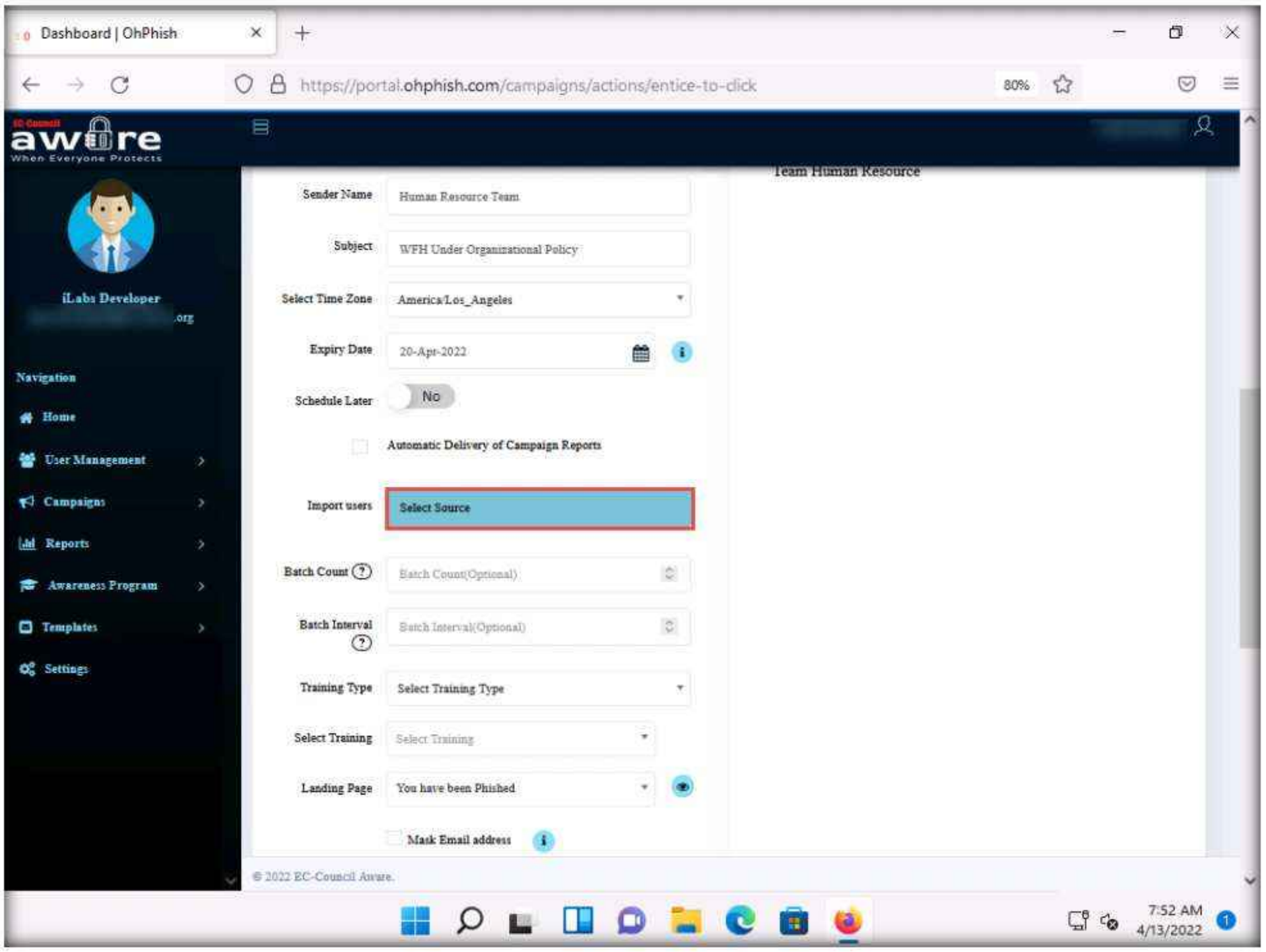
    Note: The **template selected** notification appears below the **Select Template** field.



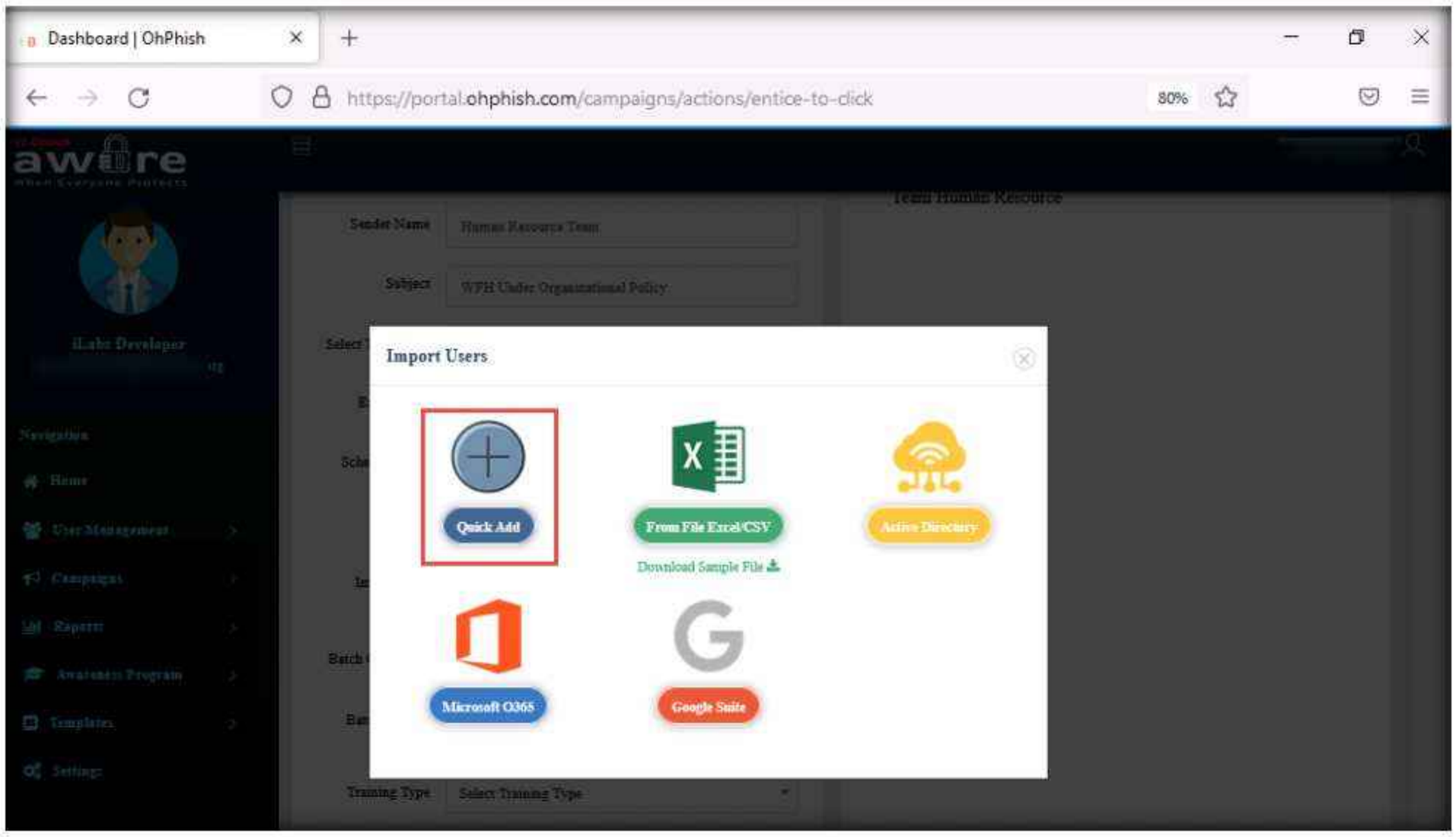
20. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

    Note: You can change the above-mentioned options if you want to.

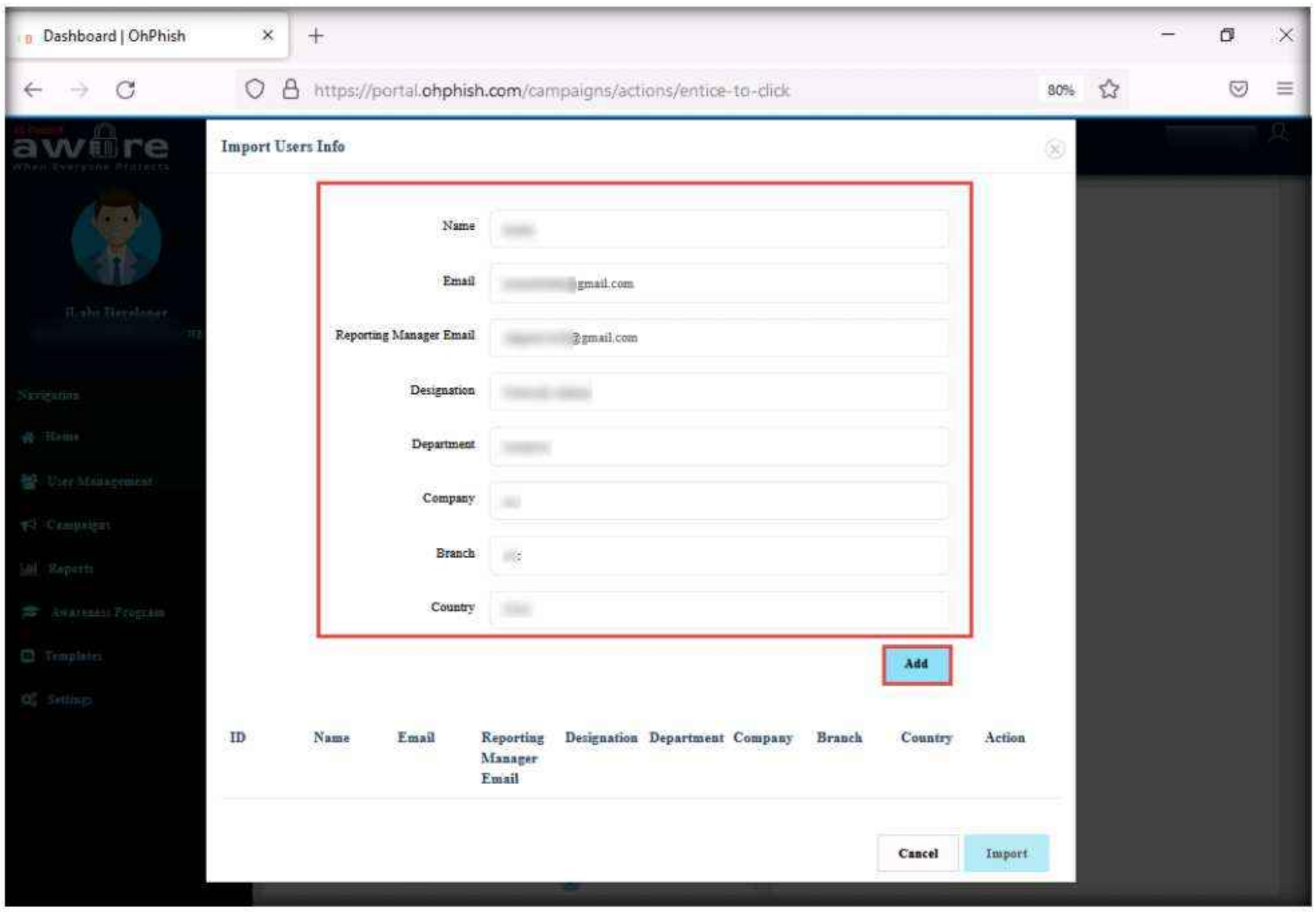
21. In the **Import users** field, click **Select Source**.



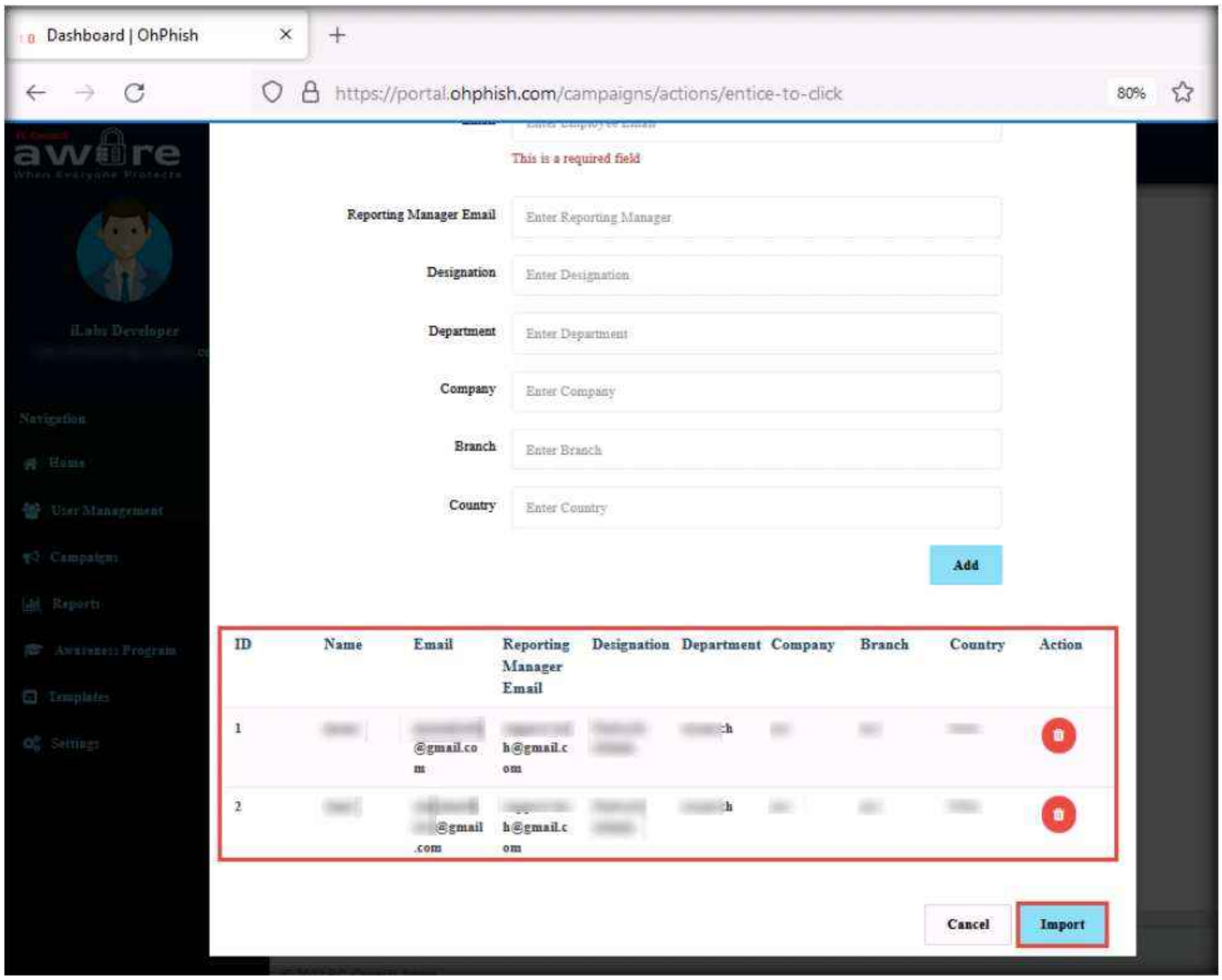
22. **Import Users** pop-up appears, click to select **Quick Add** option from the list of options.



23. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.



24. Similarly, you can add the details of multiple users. Here, we added two users.
25. After adding the users' details, click **Import**.

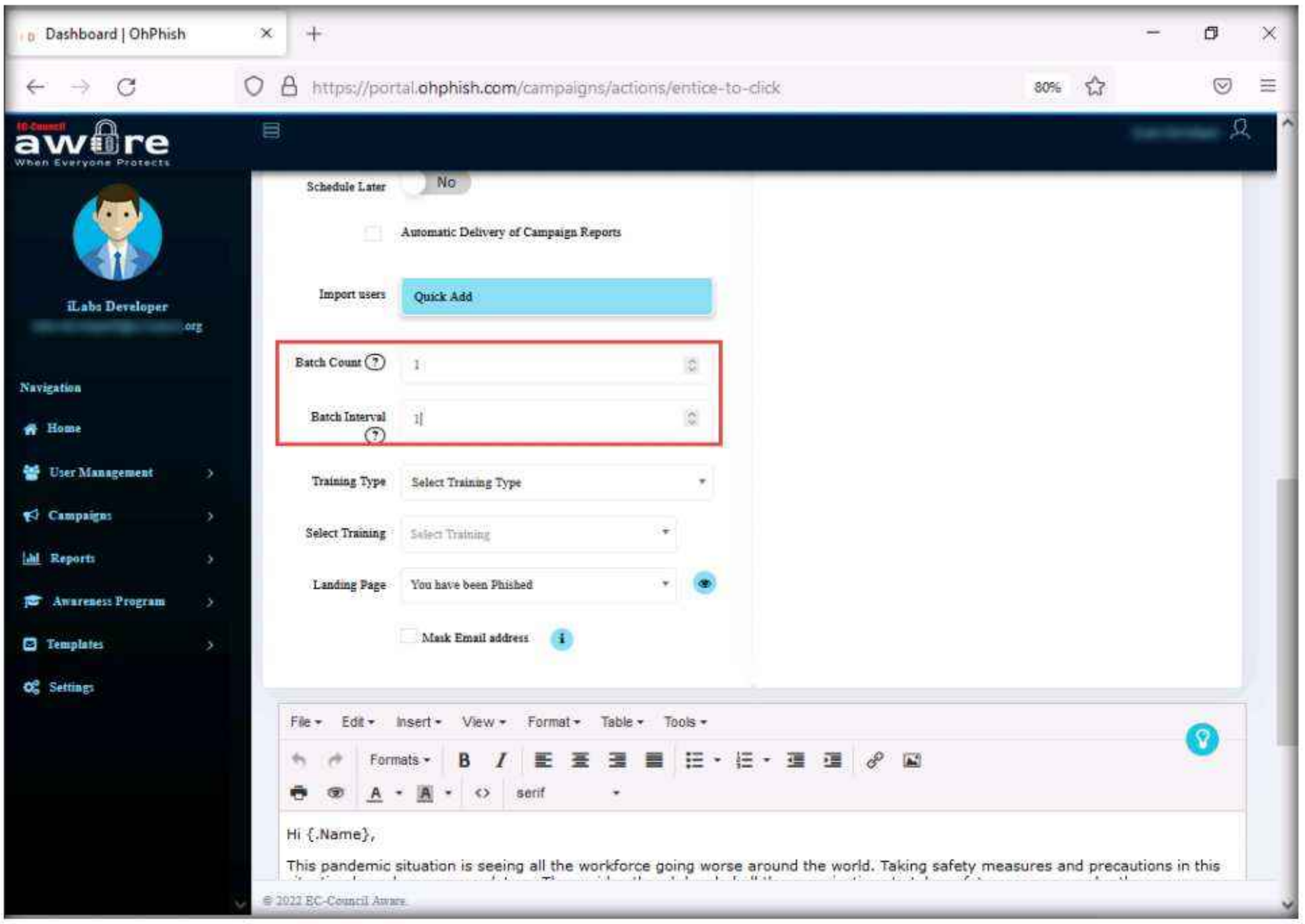


26. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

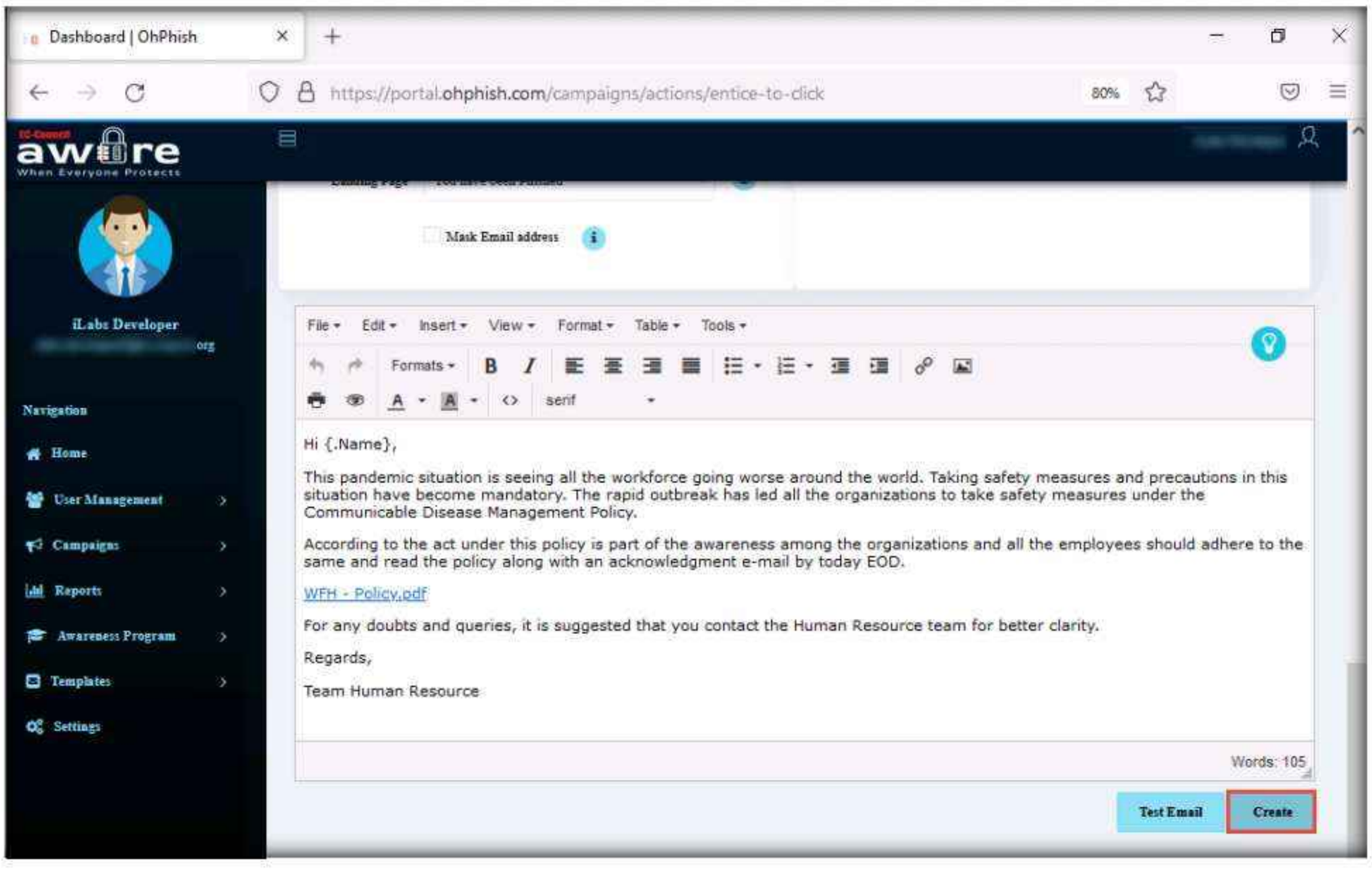
    Note: **Batch Count**: indicates how many you want to send emails to at one time; **Batch Interval**: indicates at what interval (in minutes) you want to send emails to a batch of users.

    Note: The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.

27. Leave the **Landing Page** field set to its default value.

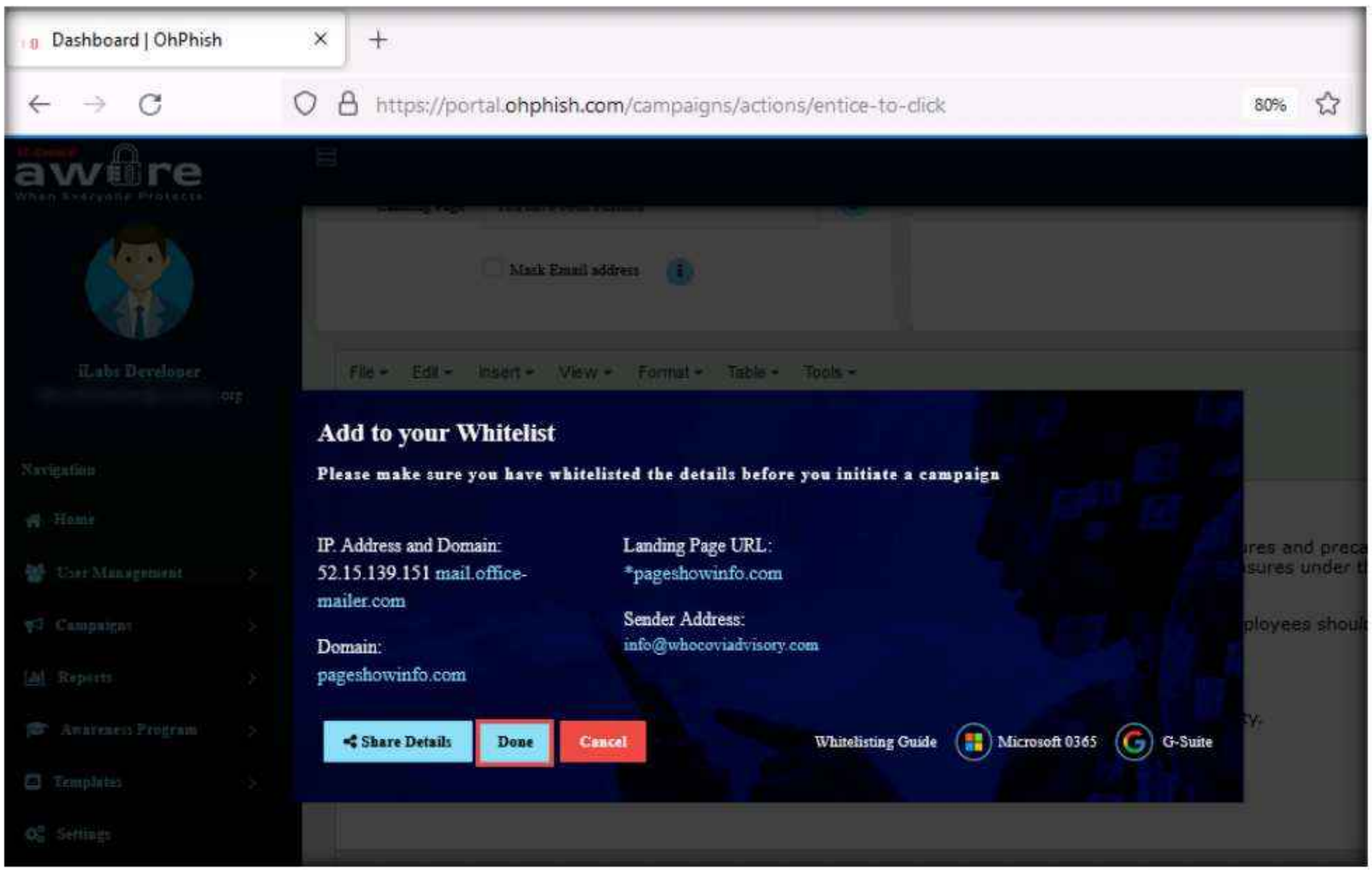


28. Now, scroll down to the end of the page and click **Create** to create the phishing campaign.

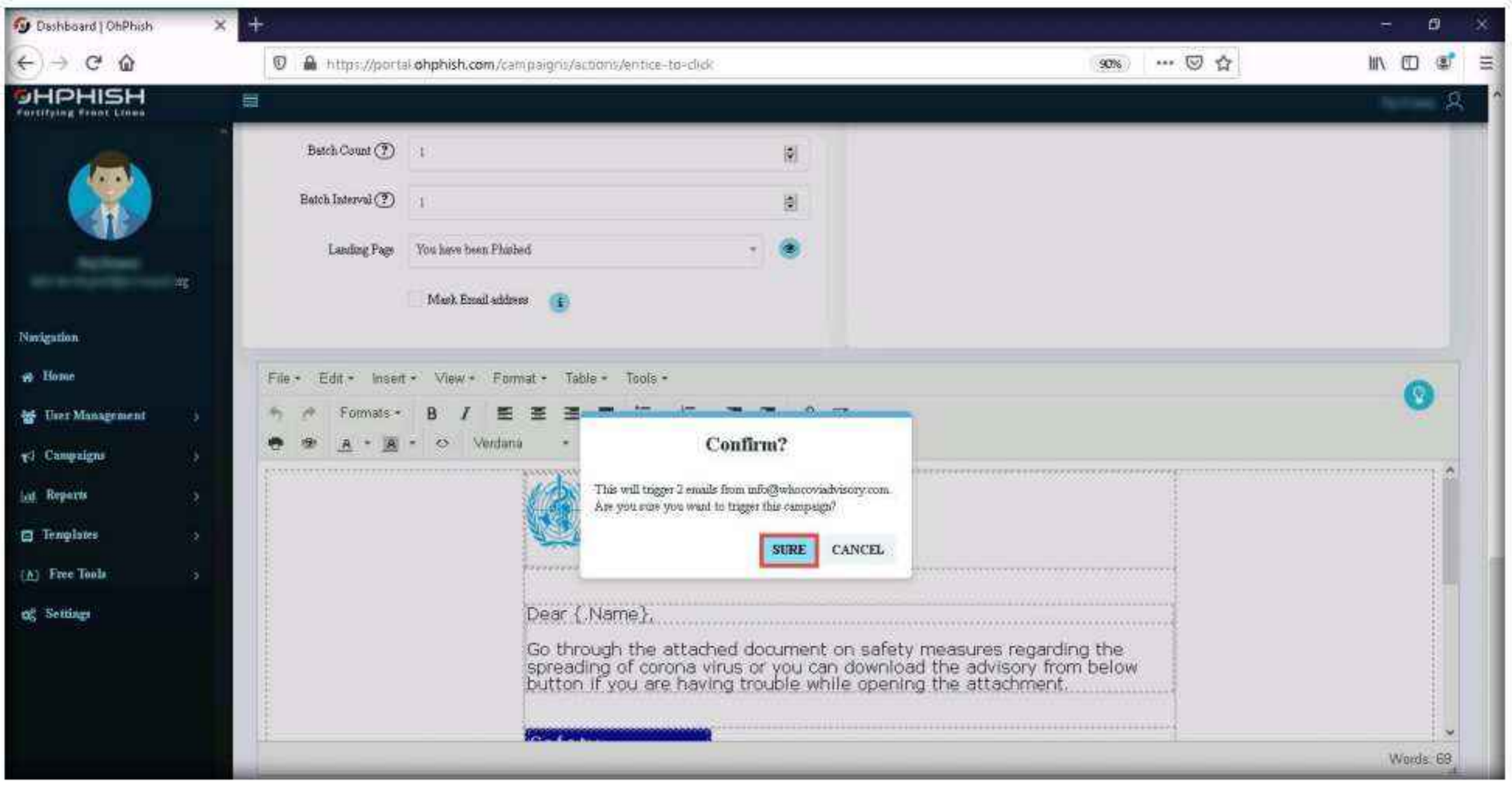


29. **Add to your Whitelist** pop-up appears, click **Done**.

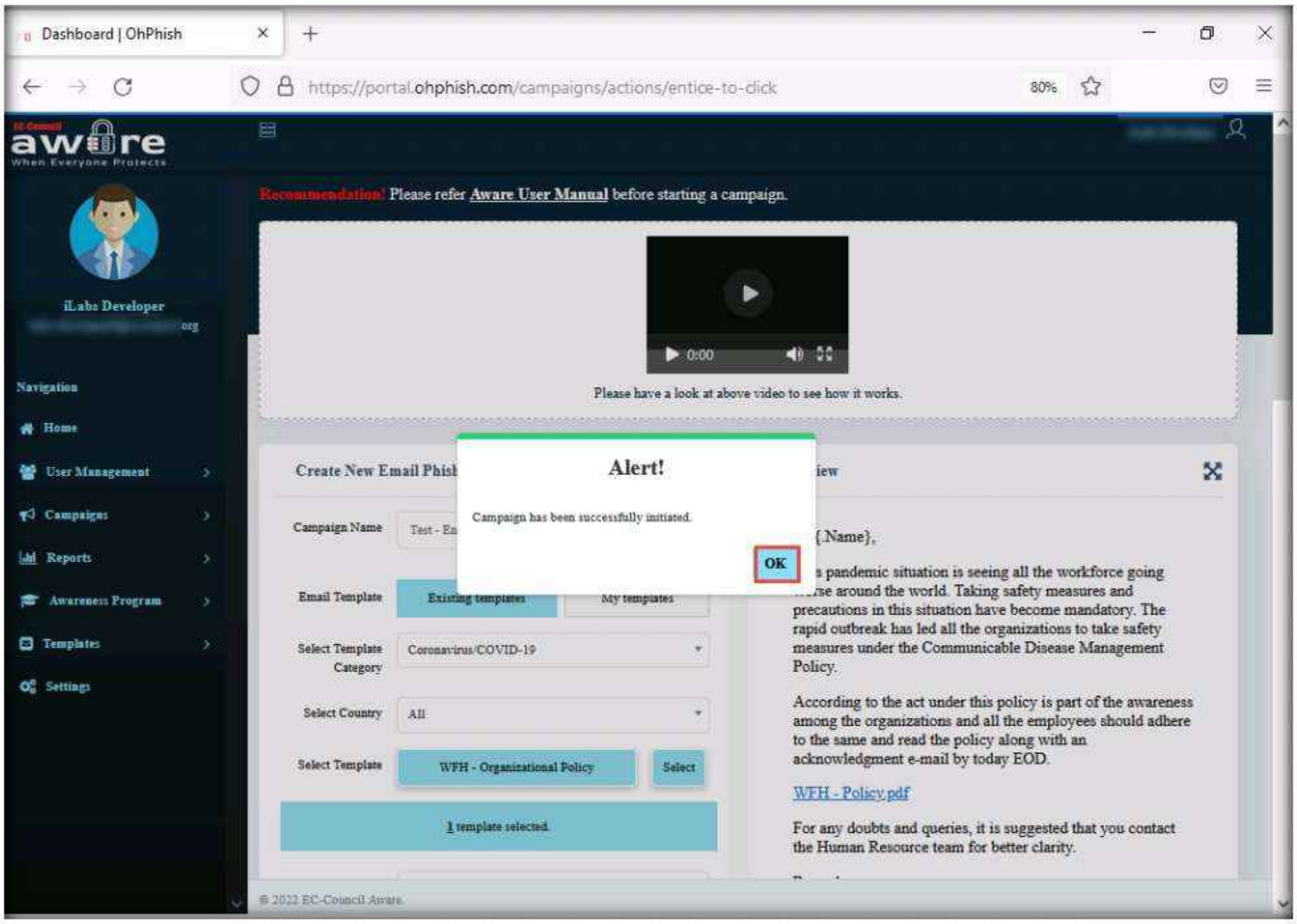
Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.



30. The **Confirm?** pop-up appears; click **SURE**.



31. A count down timer appears and phishing campaign initiates in ten seconds.
32. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.



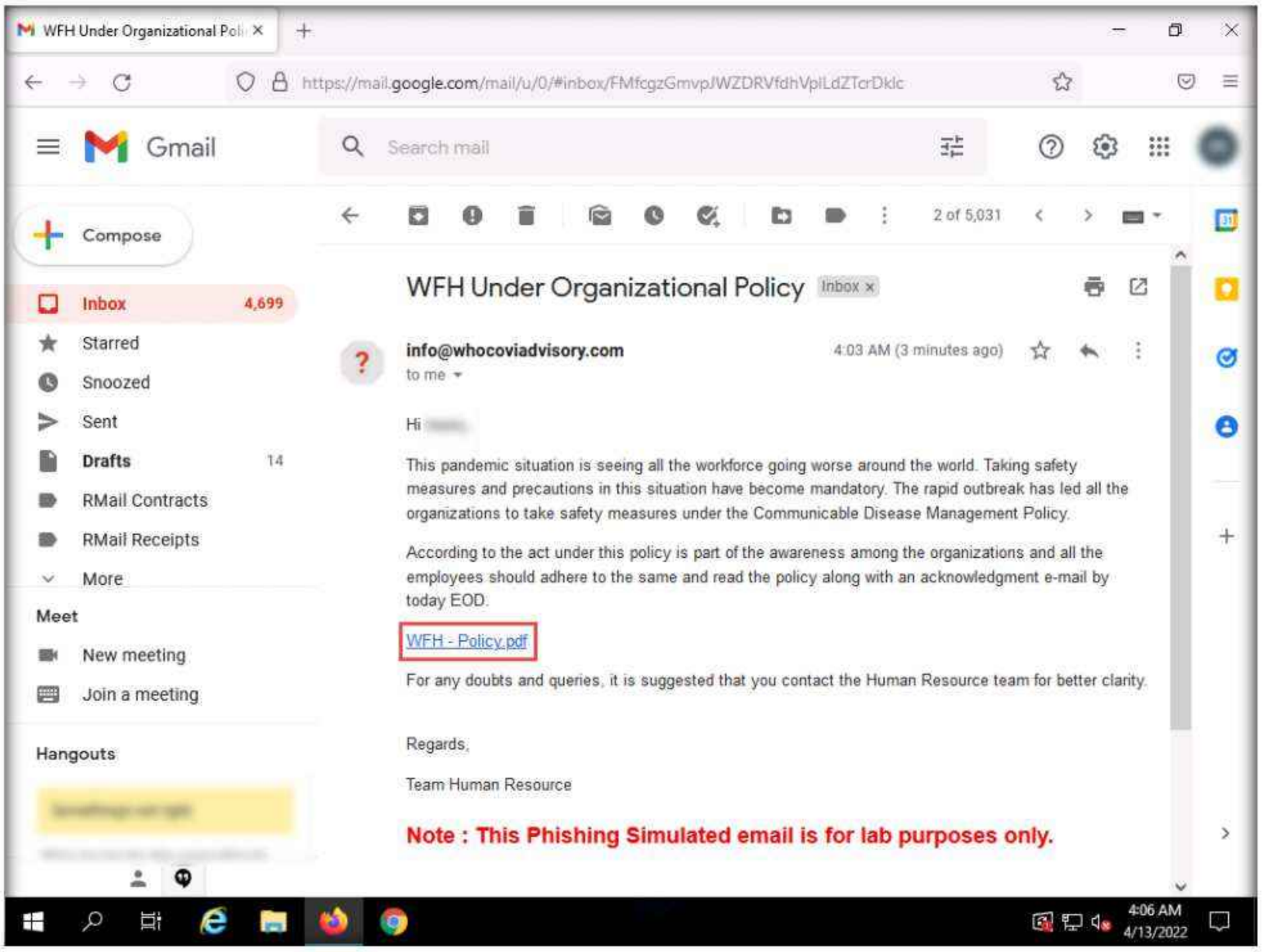
33. Now, we must open the phishing email as a victim (here, an employee of the organization). To do so, switch to the **Windows Server 2019** virtual machine.
34. Click on **Ctrl+Alt+Del** to activate it, by default, **Administrator** profile is selected type **Pa$$w0rd** in the Password field and press **Enter** to login.

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

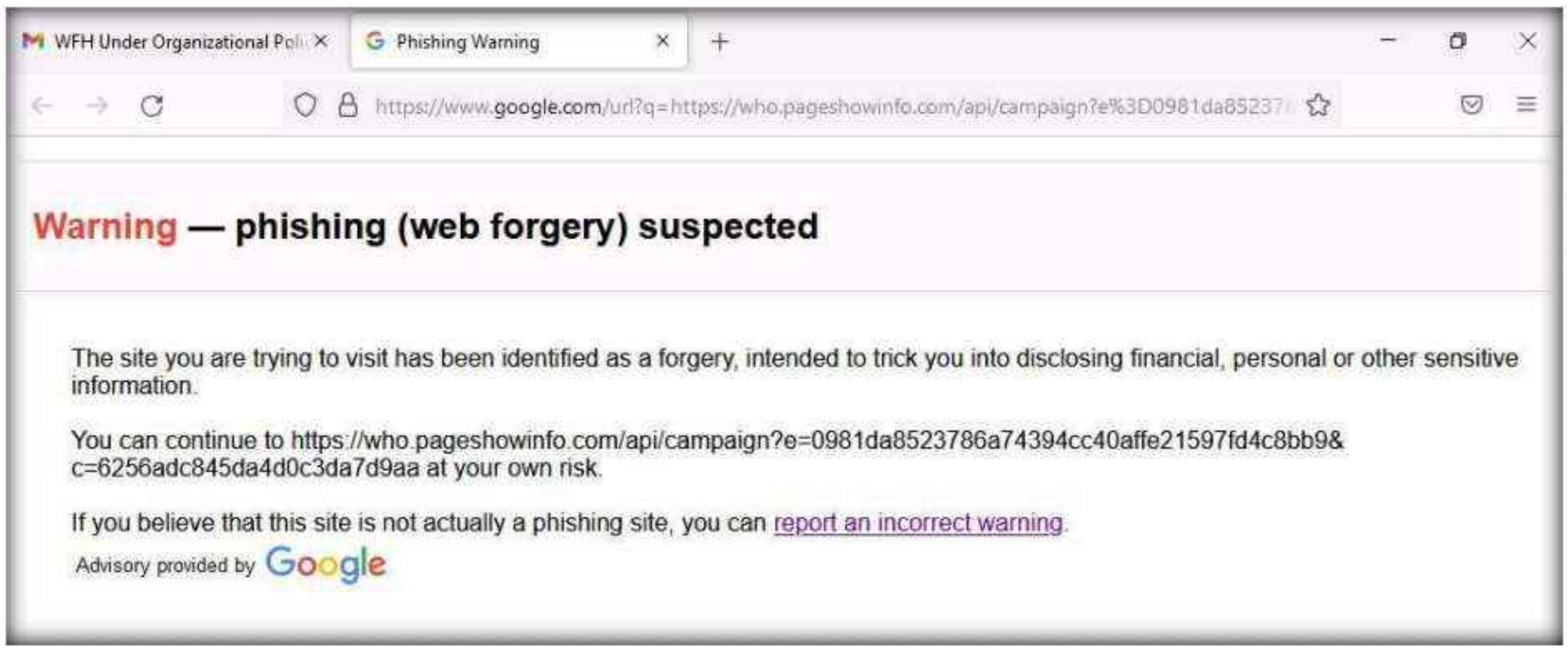
35. Open any web browser (here, **Mozilla Firefox**) and then open the email client provided while creating the phishing campaign (here, **Gmail**).
36. After you login to your **Gmail** account, search for an email with the subject **WFH Under Organizational Policy** in the **Inbox**.

    Note: Depending on the security implementations of your organization, for example, if proper spam filters are enabled, this phishing email will end up in the **Spam** folder.

    Note: If the email is not present in the **Inbox** folder, then check your **Spam** folder.
37. Click on the **WFH - Policy.pdf** link in the email.

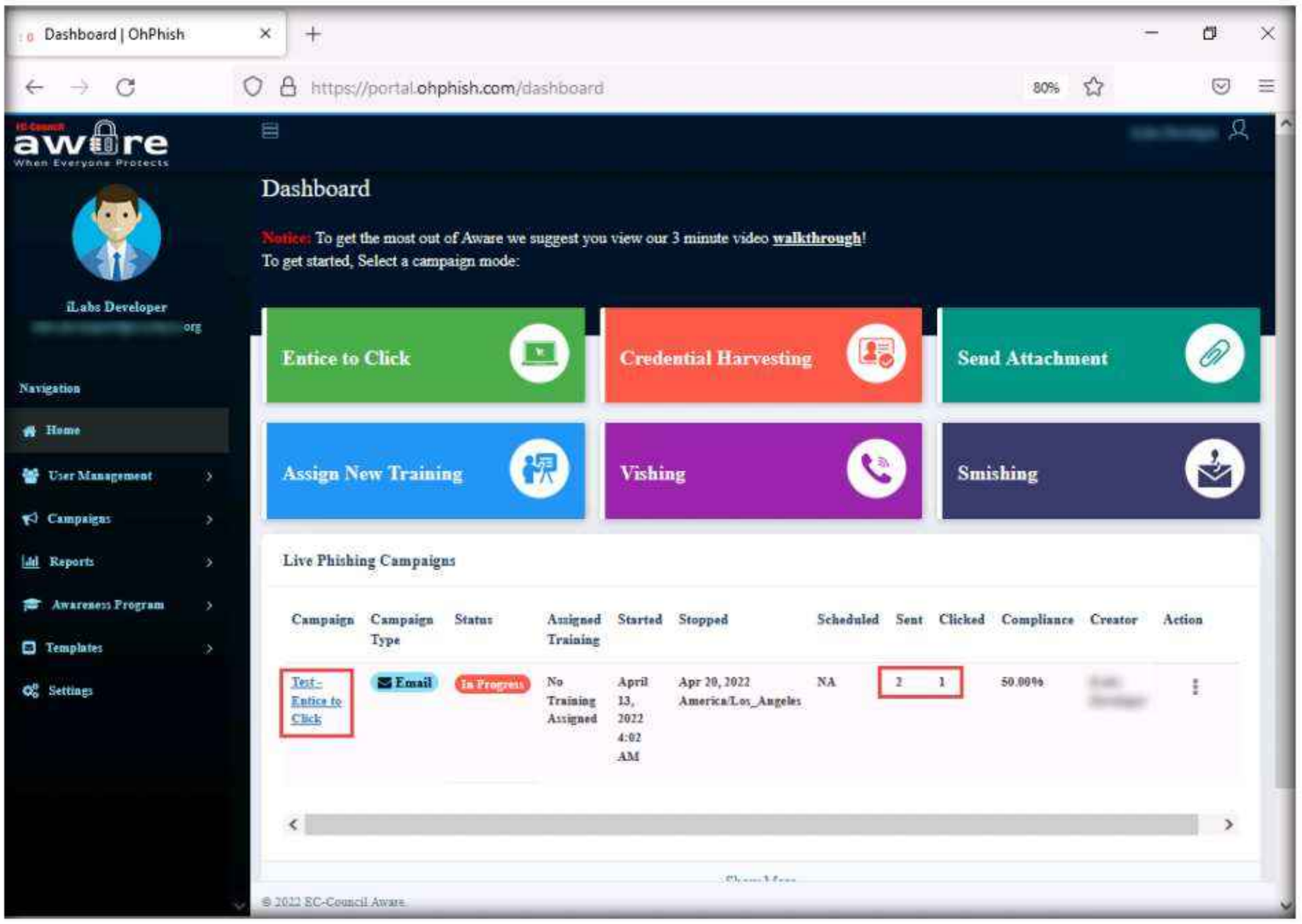


38. A **Warning - phishing suspected** page appears, as shown in the screenshot.
39. You can further click **report an incorrect warning** link to whitelist the link.

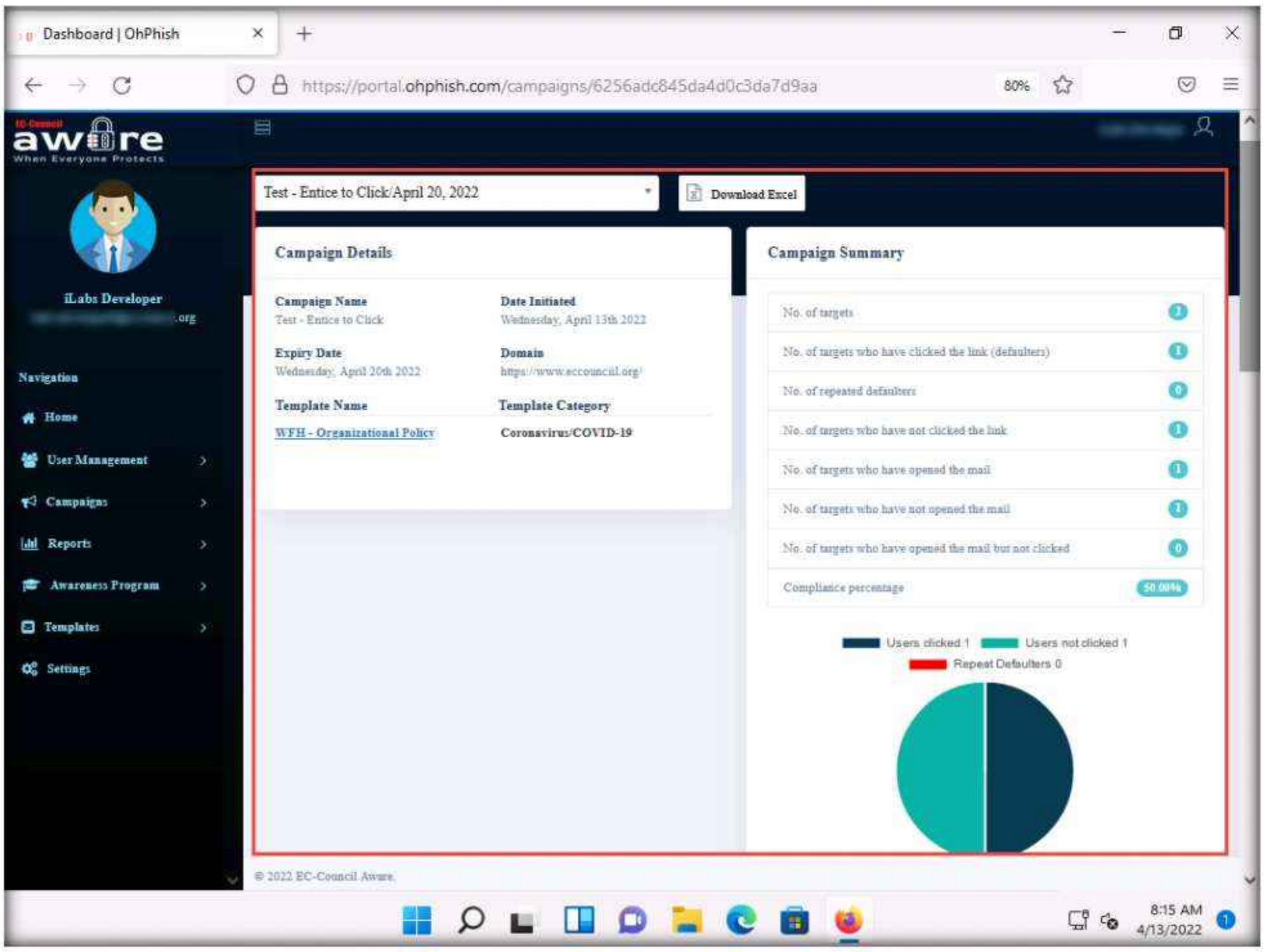


40. Close the current tab.
41. Now, click switch back to the **Windows 11** virtual machine.
42. Click on the **Test – Entice to Click** campaign present on the **OhPhish Dashboard**. You can observe that one person has clicked the link.

    Note: Refresh the Ohphish dashboard page, if the clicked value is still 0.

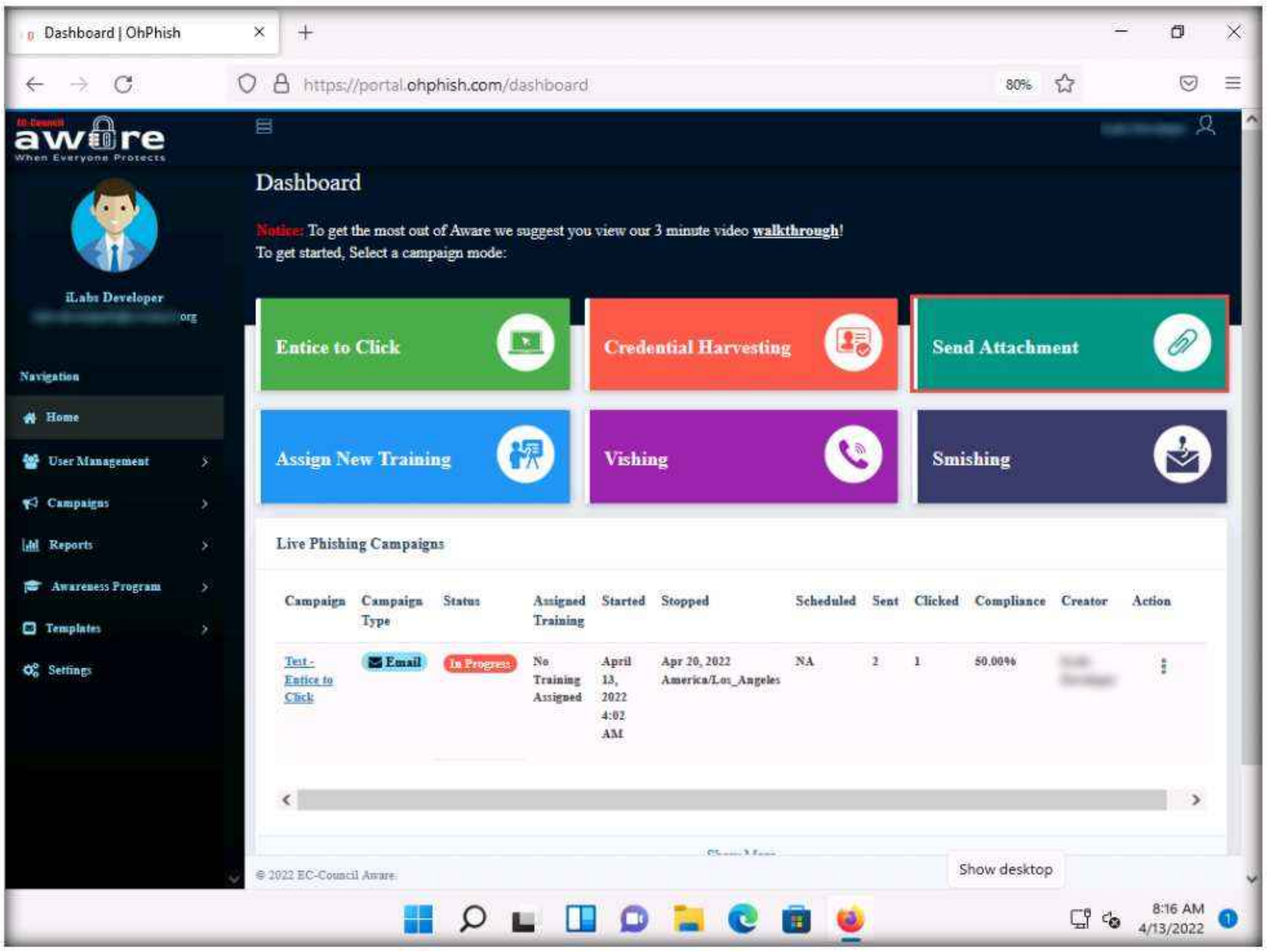


43. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.
44. In the **Campaign Summary** section, you can observe that the values of **No. of targets who have clicked the link (defaulters)** and **No. of Targets who have opened the mail** are both **1** (here, we have opened only one email account).



45. Now, click **Home** in the left pane to navigate back to the OhPhish **Dashboard**.

46. In the OhPhish **Dashboard**, click on the **Send Attachment** option.



47. The **Create New Email Phishing Campaign** form appears.

    Note: **Almost Done** pop-up appears, click **DISCARD CHANGES**.

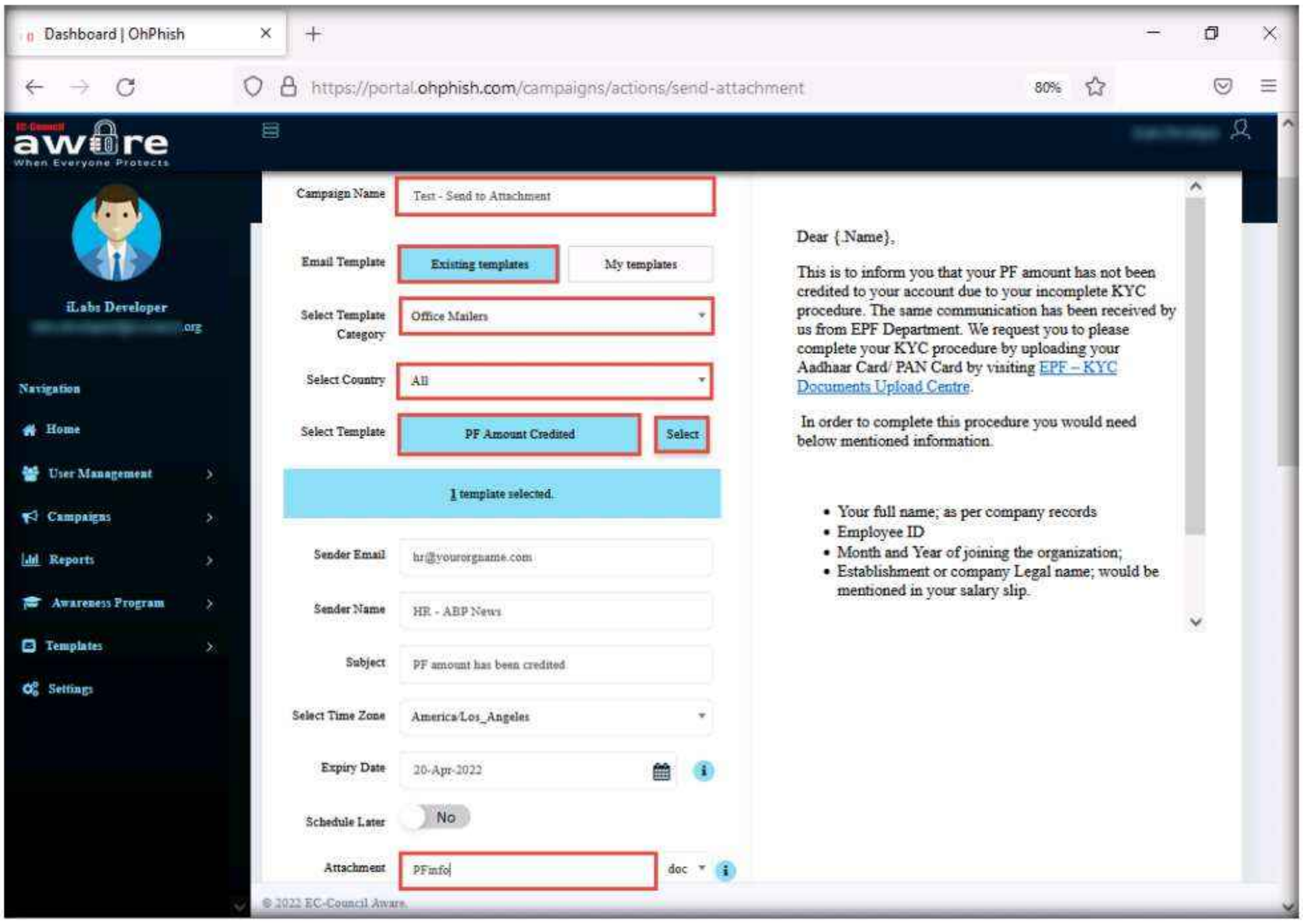
48. In the **Campaign Name** field, enter any name (here, **Test – Send to Attachment**). In the **Select Template Category** field, select **Office Mailers** from the drop-down list.

    Note: Ensure that the **Existing templates** button is selected in the **Email Template** field.

49. In the **Select Country** field, leave the default option selected (**All**).
50. In the **Select Template** field, select the **PF Amount Credited** option from the drop-down list and then click the **Select** button.
51. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

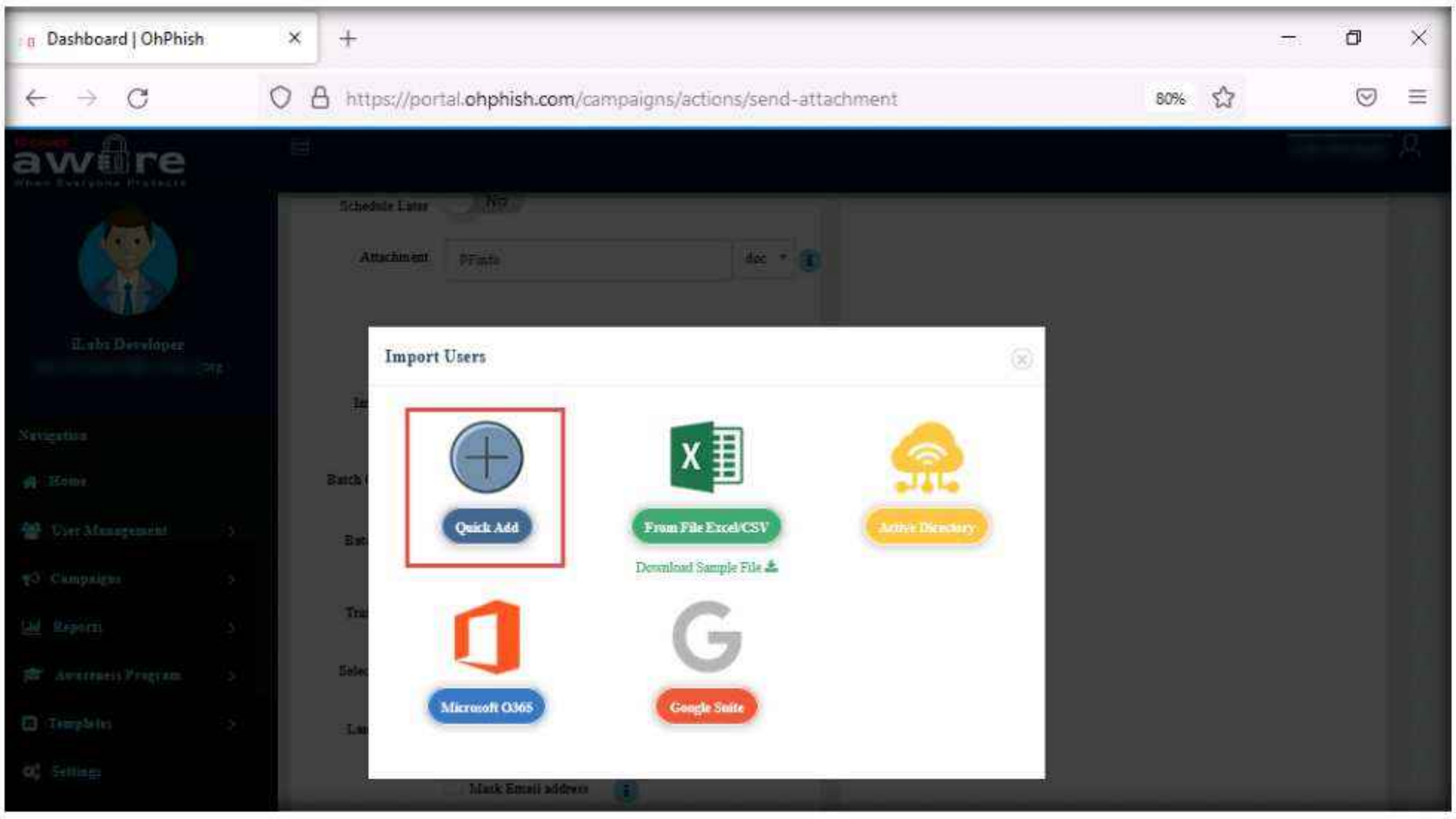
    Note: You can change the above-mentioned options if you want to.

52. In the **Attachment** field, enter any name (here, **PFinfo**).

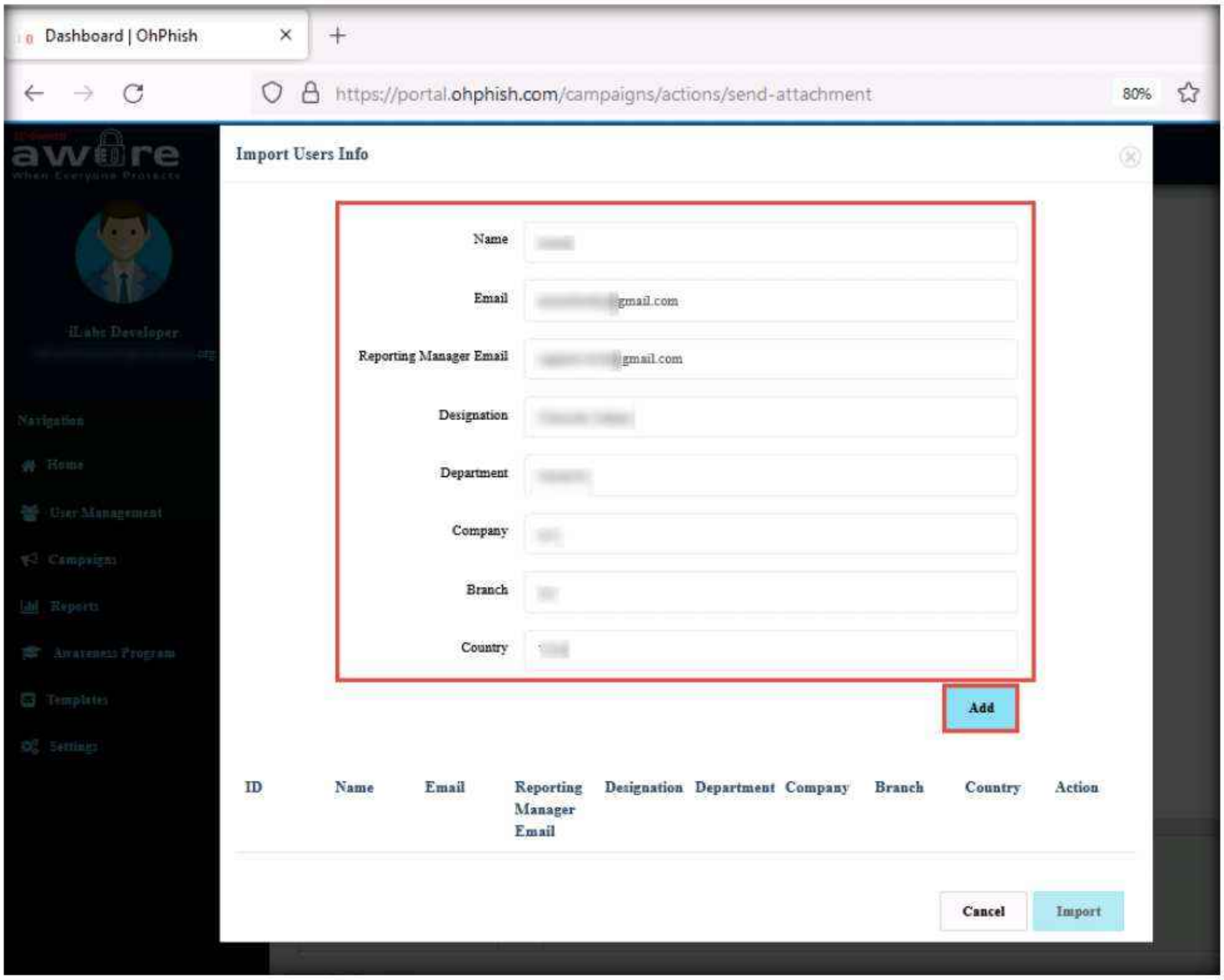


53. Click **Select Source** button under **Import user's** field.

Import Users pop-up appears, click to select the **Quick Add** option from the list of options.



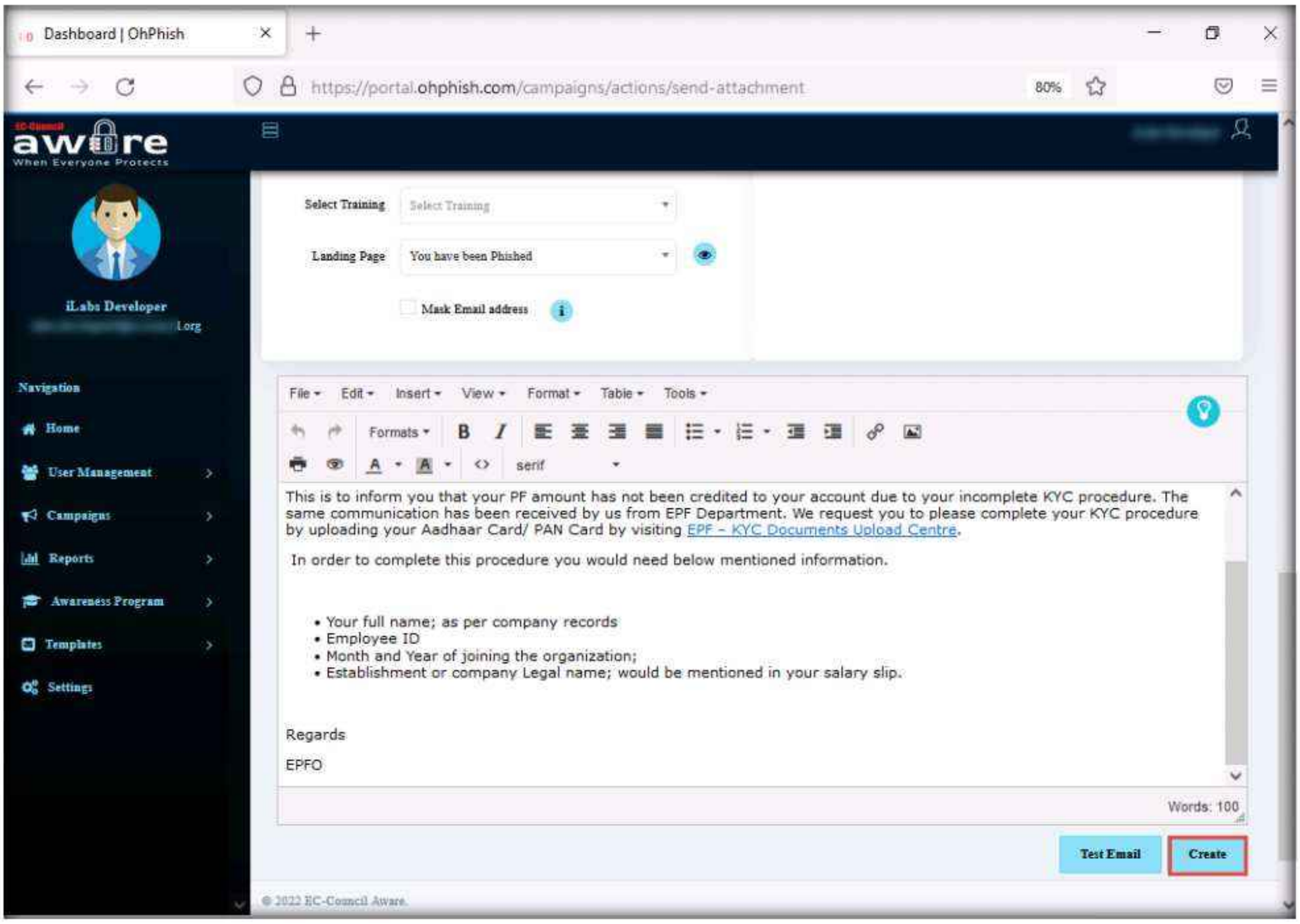
54. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.



55. Similarly, you can add the details of multiple users. Here, we added two users.
56. After adding the users' details, click **Import**.
57. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

    Note: The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.

58. Leave the **Landing Page** field set to its default value.
59. Scroll down to the end of the page and click **Create** to create the phishing campaign.



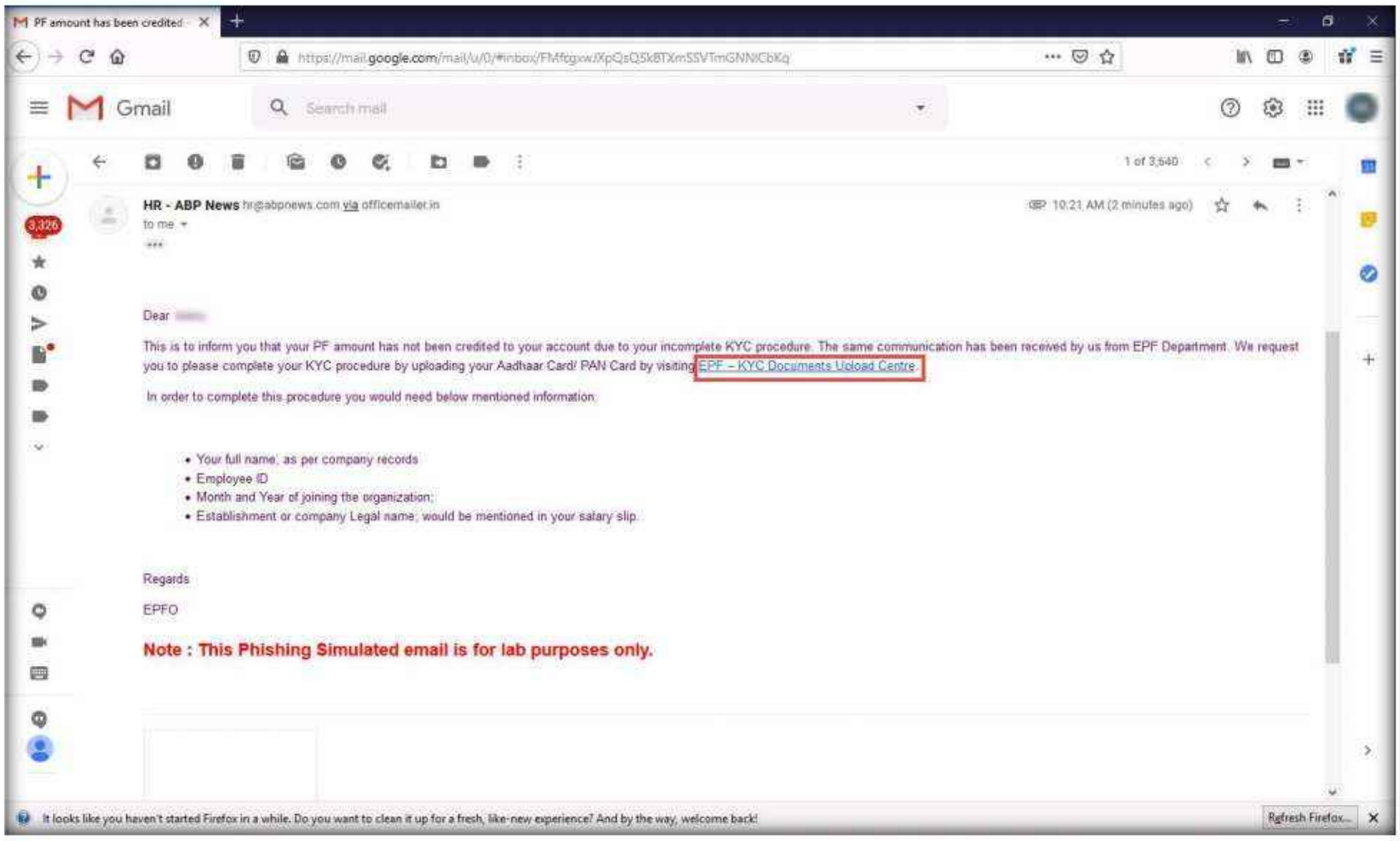
60. **Add to your Whitelist** pop-up appears, click **Done**.

    Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.

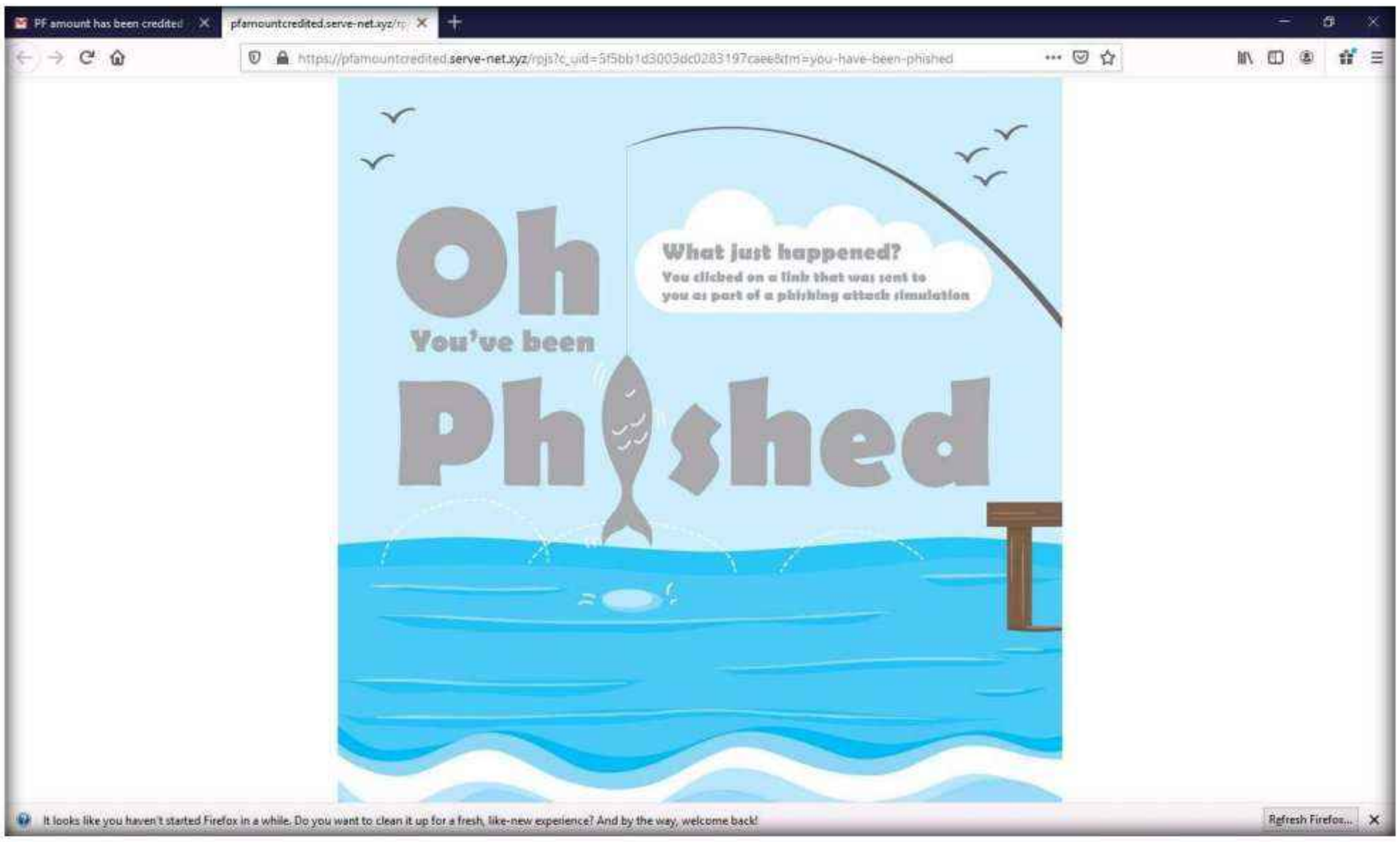
61. The **Confirm?** pop-up appears; click **SURE**.
62. A count down timer appears and phishing campaign initiates in ten seconds.
63. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.
64. Now, switch to the **Windows Server 2019** virtual machine.

    Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

65. In the **Gmail** account opened previously, navigate to the **Inbox** folder.
66. You will find an email from **HR – ABP News**, as shown in the screenshot.
67. Click on the **EPF – KYC Documents Upload Centre** hyperlink present in the email.

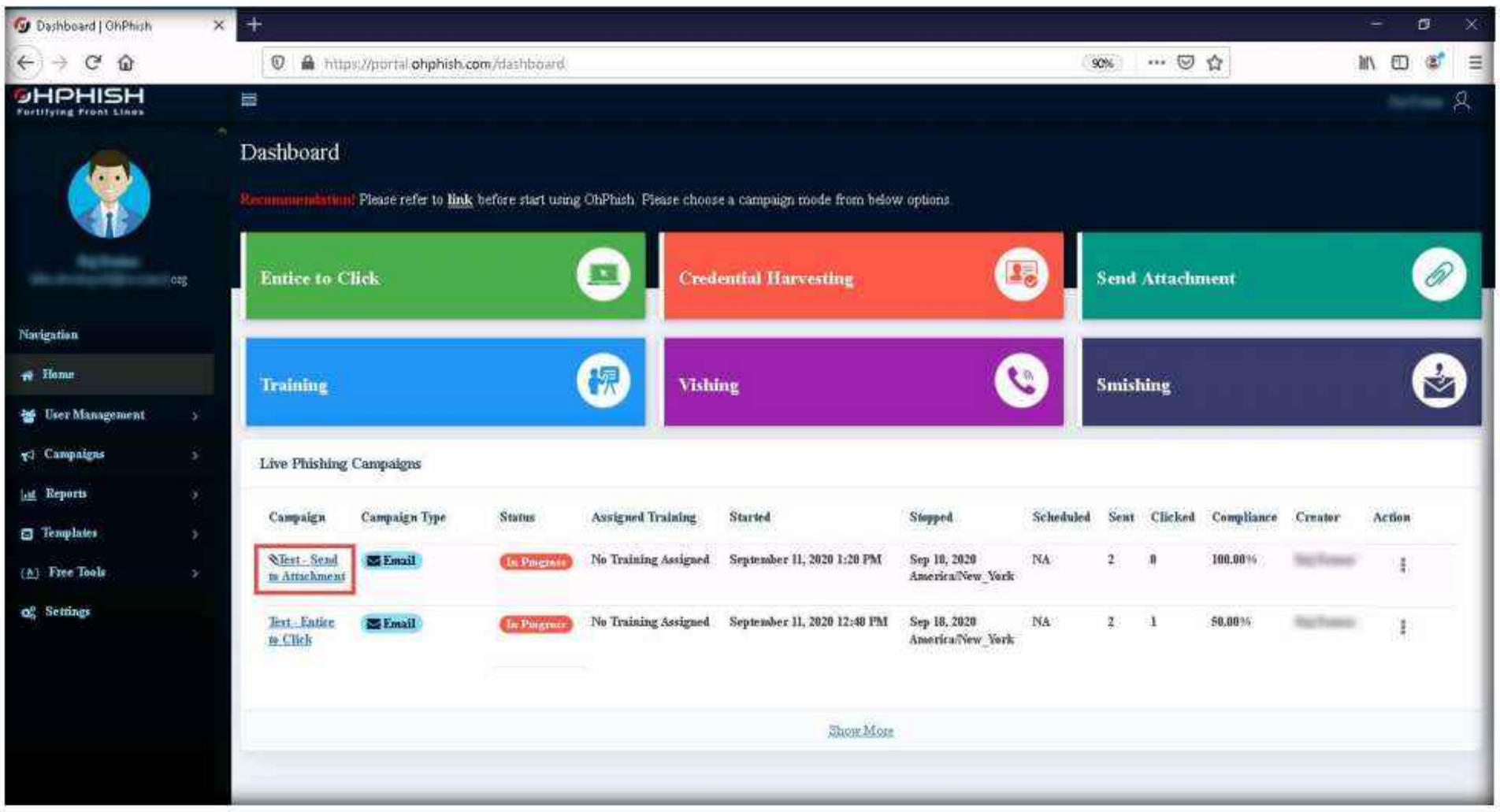


68. If a **Suspicious** link pop-up appears, click **Proceed**.
69. You will be re-directed to the **Oh You've been Phished** landing page, as shown in the screenshot.



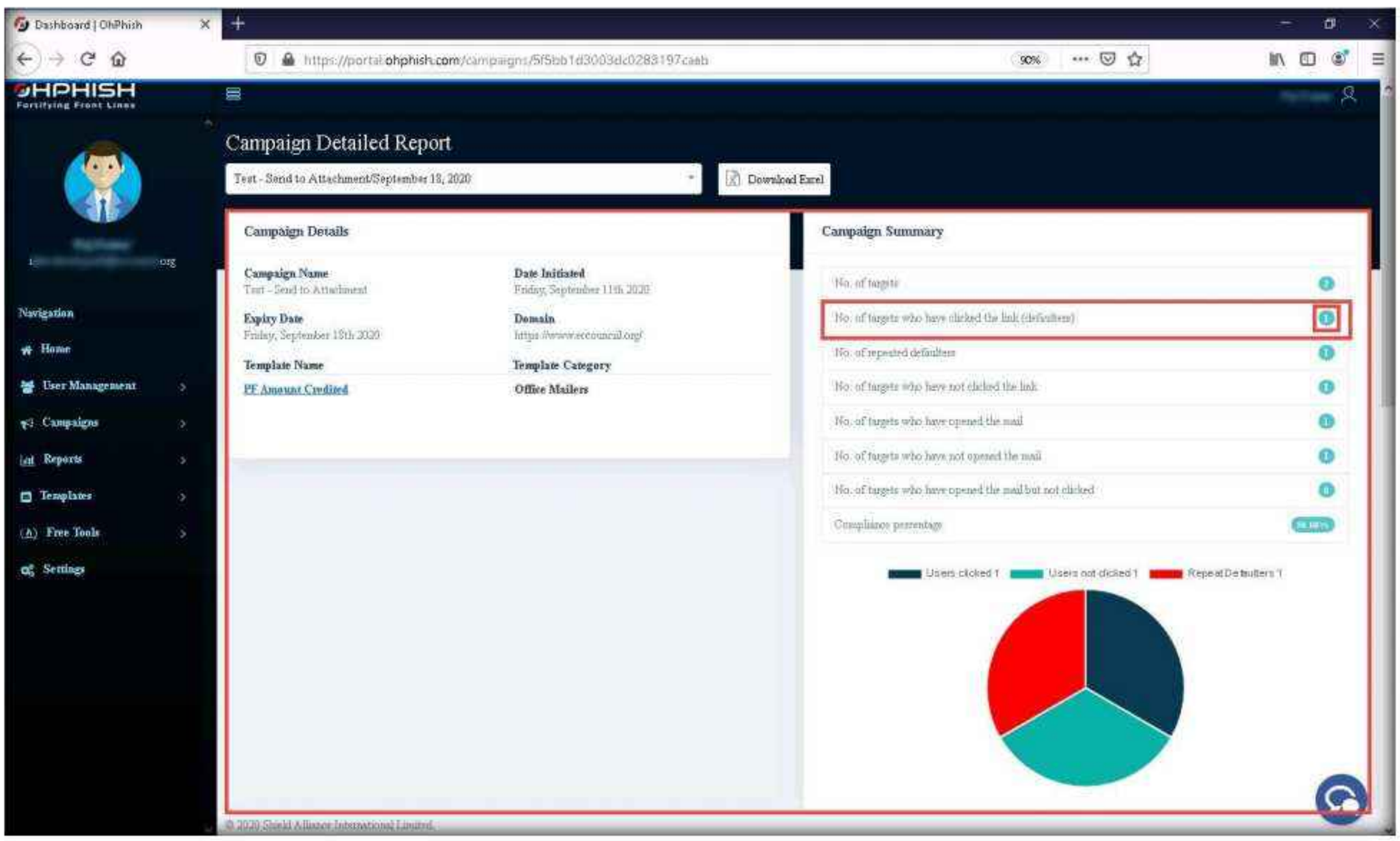
70. Now, switch back to the **Windows 11** virtual machine.

71. Click on the **Test – Send to Attachment** campaign present on the **OhPhish Dashboard**.

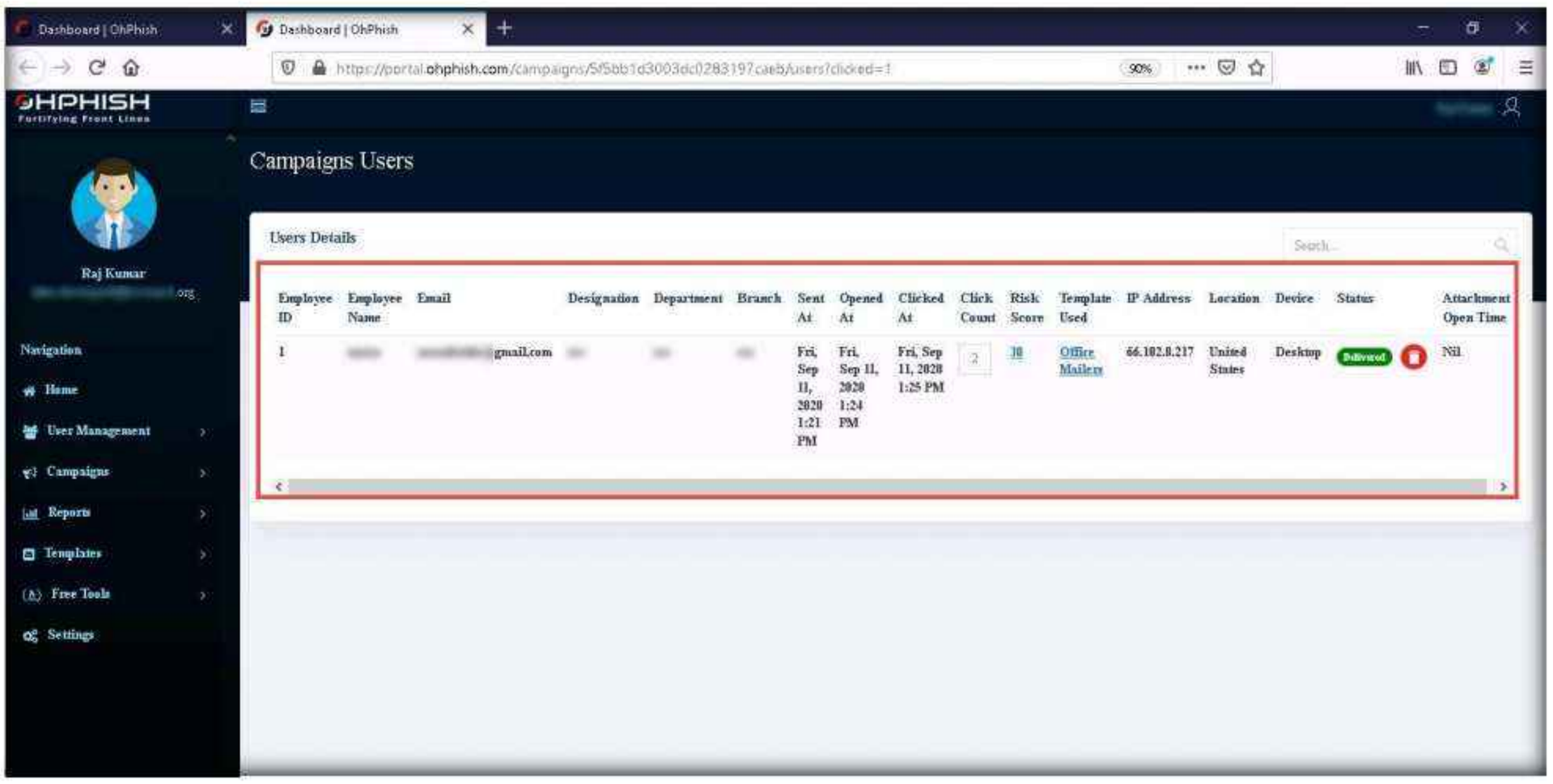


72. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.

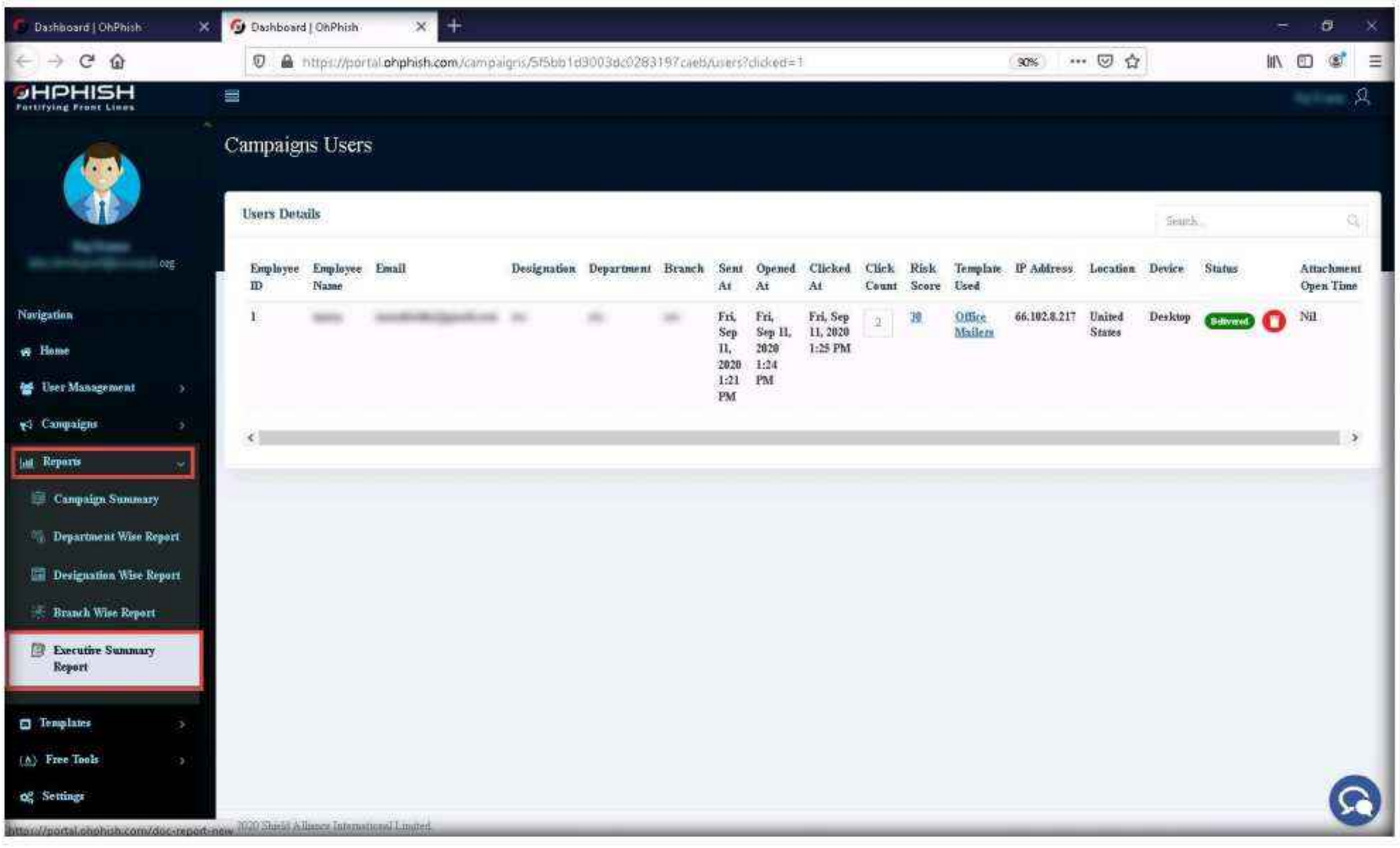
73. In the **Campaign Summary** section, you can observe that the value of **No. of targets who have clicked the link (defaulters)** is **1**. Click on **1** icon to see the defaulter.



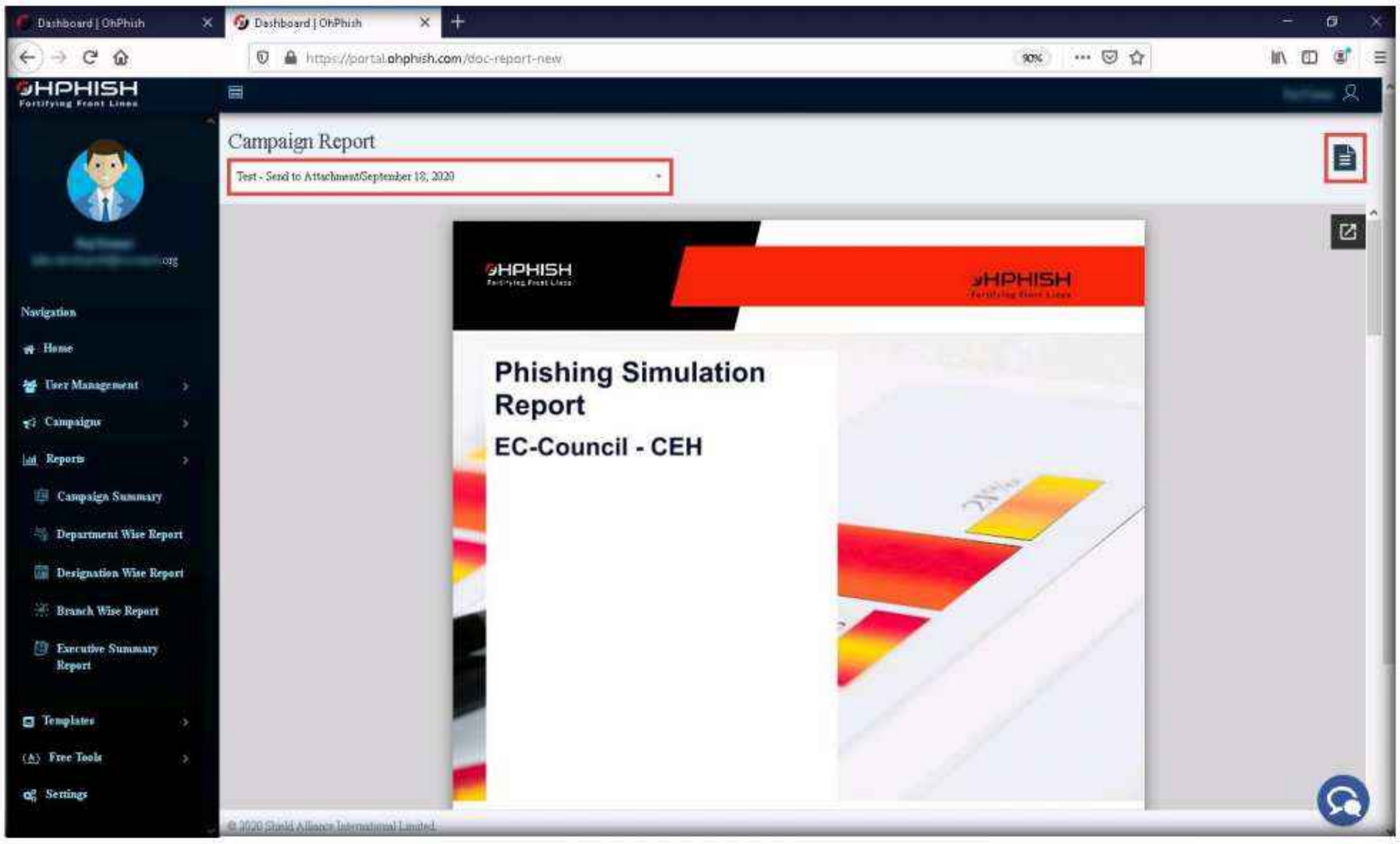
74. The **Campaigns Users** page appears, displaying the details of the defaulter, such as **Risk Score**, **Credentials**, **IP Address**, **Location**, etc., as shown in the screenshot.



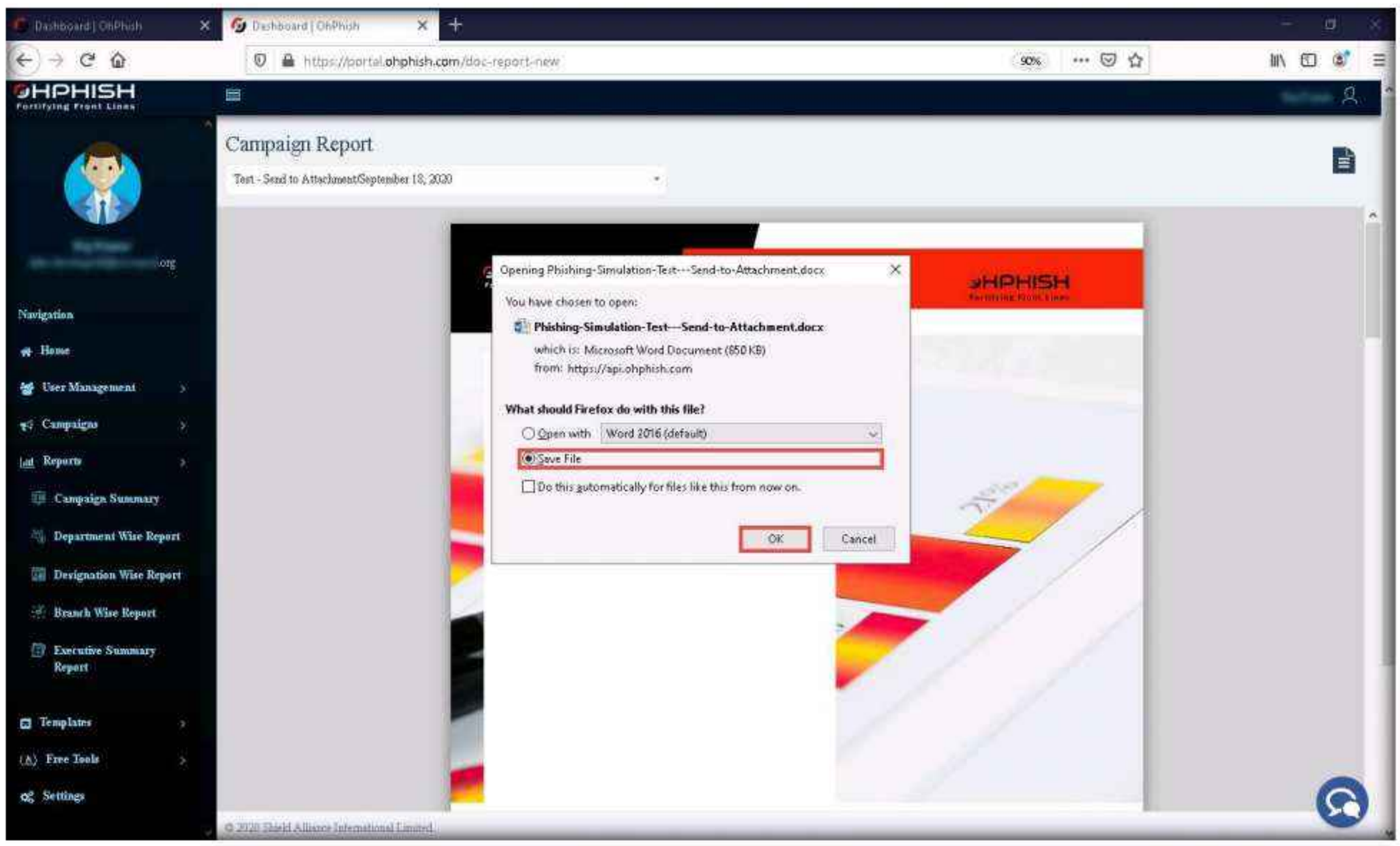
75. Now, click to expand the **Reports** section in the left pane and select the **Executive Summary Report** option.



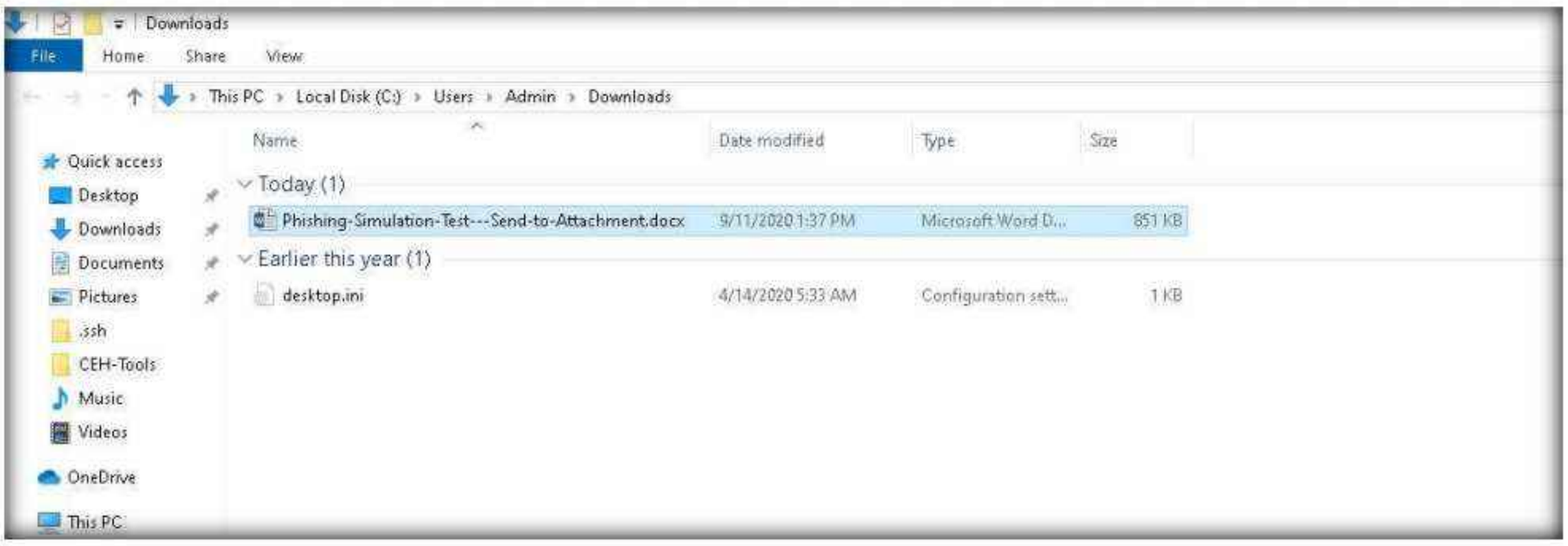
76. The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send to Attachment**) and click on the **Export** icon to export the report.



77. The **Opening Phishing-Simulation-Test** window appears; select the **Save File** radio button and click **OK**.



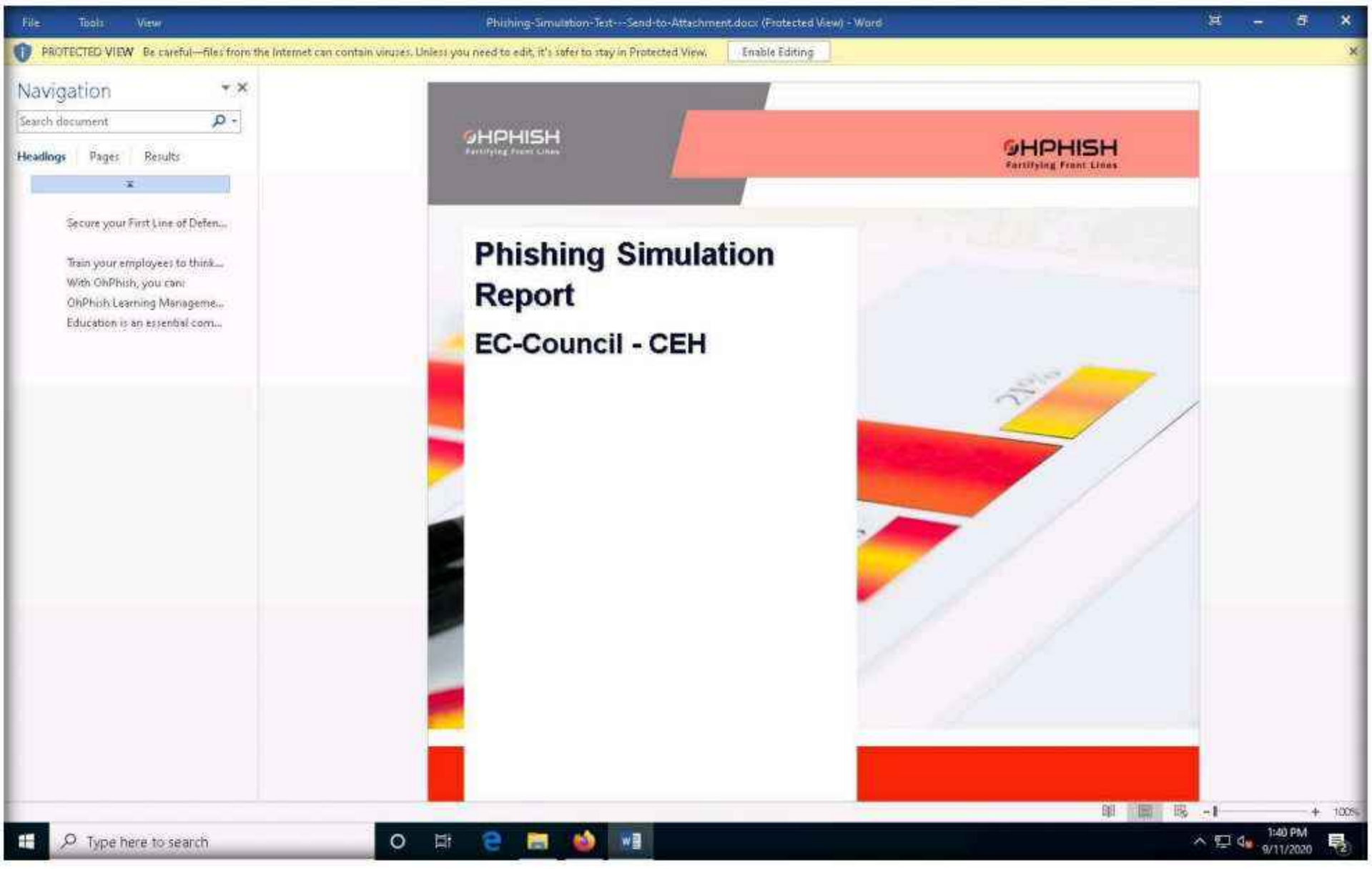
78. The file is downloaded to the default location (here, **Downloads**). Navigate to the download location and double-click the **Phishing-Simulation-Test---Send-Attachment** file to open it.

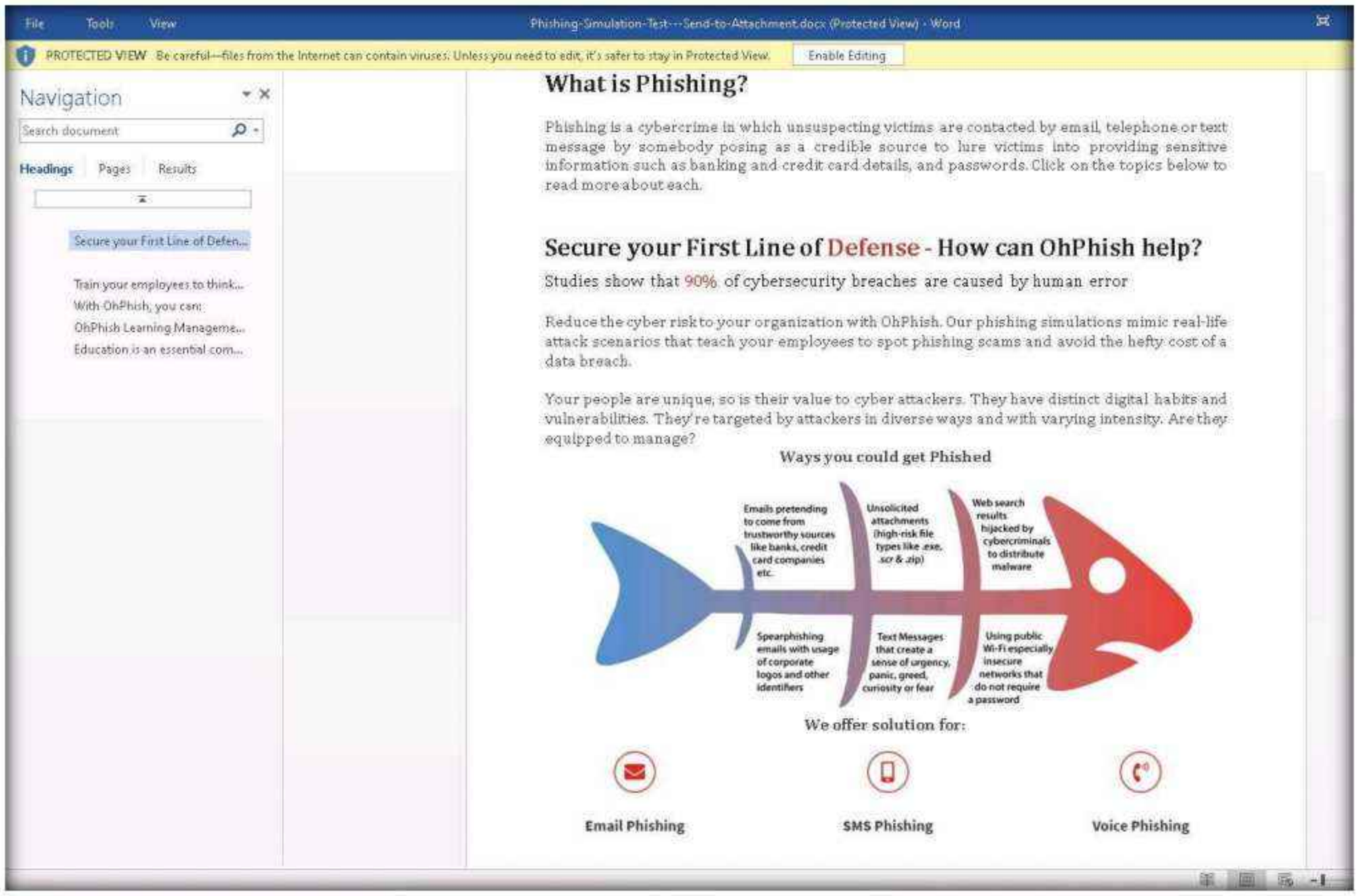


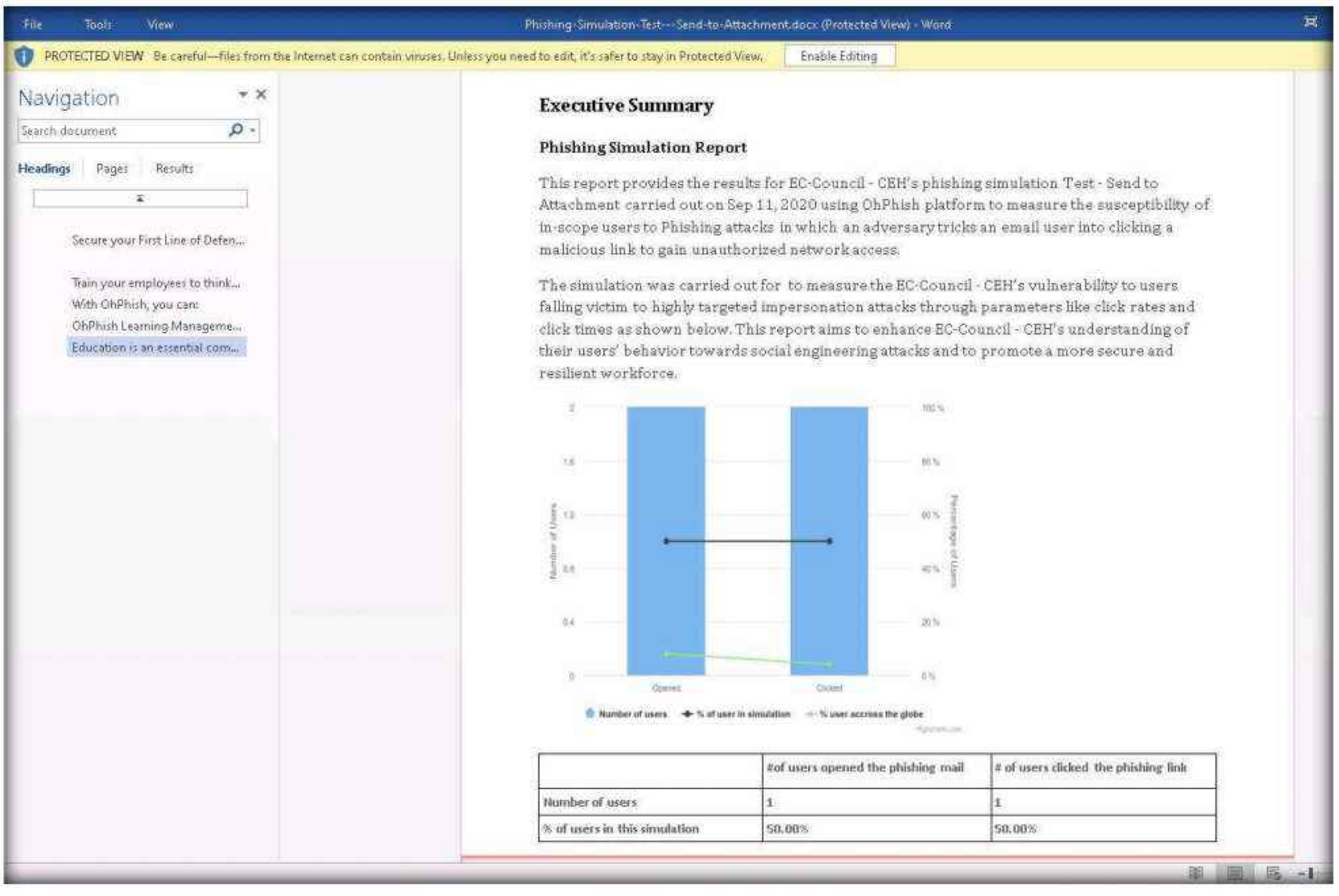
79. The executive phishing report appears in the document, as shown in the screenshot.

Note: If **Microsoft Word** pop-up appears, click **OK**. In the second **Microsoft Word** pop-up, click **Yes**.

Note: You can also explore other report options such as **Department Wise Report**, **Designation Wise Report**, and **Branch Wise Report**.







	#of users opened the phishing mail	# of users clicked the phishing link
Number of users	1	1
% of users in this simulation	50.00%	50.00%

80. If you have an upgraded OhPhish account you can also explore other phishing methods such as **Credential Harvesting**, **Training**, **Vishing** and **Smishing**.
81. This concludes the demonstration of auditing an organization's security for phishing attacks using OhPhish.
82. Close all the open windows and document all the acquired information.
83. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

CEH Lab Manual

Denial-of-Service

Module 10

Denial-of-Service

Denial-of-Service is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.

Lab Scenario

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks have become a major threat to computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually, DoS and DDoS attacks exploit vulnerabilities in the implementation of TCP/IP model protocol or bugs in a specific OS.

In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources, bringing the system down and leading to the unavailability of the victim's website—or at least significantly slowing the victim's system or network performance. The goal of a DoS attack is not to gain unauthorized access to a system or corrupt data, but to keep legitimate users from using the system.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus depriving legitimate users of these resources. Connectivity attacks overflow a computer with a flood of connection requests, consuming all available OS resources, so that the computer cannot process legitimate users' requests.

As an expert ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of DoS and DDoS attacks to detect and neutralize attack handlers, and mitigate such attacks.

The labs in this module give hands-on experience in auditing a network against DoS and DDoS attacks.

Lab Objective

The objective of the lab is to perform DoS attack and other tasks that include, but is not limited to:

- Perform a DoS attack by continuously sending a large number of SYN packets
- Perform a DoS attack (SYN Flooding, Ping of Death (PoD), and UDP application layer flood) on a target host
- Perform a DDoS attack
- Detect and analyze DoS attack traffic
- Detect and protect against a DDoS attack

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

Overview of Denial of Service

A DoS attack is a type of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. Further, failure to protect against such attacks might mean the loss of a service such as email. In a worst-case scenario, a DoS attack can mean the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of the attack.

Some examples of types of DoS attacks:

- Flooding the victim's system with more traffic than it can handle
- Flooding a service (such as an internet relay chat (IRC)) with more events than it can handle
- Crashing a transmission control protocol (TCP)/internet protocol (IP) stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected way
- Hanging a system by causing it to go into an infinite loop

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform DoS and DDoS attacks on the target network. Recommended labs that will assist you in learning various DoS attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform DoS and DDoS Attacks using Various Techniques	√	√	√
	1.1 Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit		√	√

	1.2 Perform a DoS Attack on a Target Host using hping3		√	√
	1.3 Perform a DoS Attack using Raven-storm	√		√
	1.4 Perform a DDoS Attack using HOIC	√		√
	1.5 Perform a DDoS Attack using LOIC		√	√
2	Detect and Protect Against DoS and DDoS Attacks	√		√
	2.1 Detect and Protect against DDoS Attack using Anti DDoS Guardian	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Perform DoS and DDoS Attacks using Various Techniques

As an expert hacker and pen tester, you must implement various techniques to launch DoS or DDoS attacks on target computers or networks.

Lab Scenario

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations.

In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

As an expert ethical hacker or pen tester, you must have the required knowledge to perform DoS and DDoS attacks to be able to test systems in the target network.

In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

Lab Objectives

- Perform a DoS attack (SYN flooding) on a target host using Metasploit
- Perform a DoS attack on a target host using hping3

- Perform a DoS attack using Raven-storm
- Perform a DDoS attack using HOIC
- Perform a DDoS attack using LOIC

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 45 Minutes

Overview of DoS and DDoS Attacks

DDoS attacks mainly aim at the network bandwidth; they exhaust network, application, or service resources, and thereby restrict legitimate users from accessing their system or network resources.

In general, the following are categories of DoS/DDoS attack vectors:

- **Volumetric Attacks**: Consume the bandwidth of the target network or service
  Attack techniques:
  - UDP flood attack
  - ICMP flood attack
  - Ping of Death and smurf attack
  - Pulse wave and zero-day attack
- **Protocol Attacks**: Consume resources like connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers

  Attack techniques:
  - SYN flood attack
  - Fragmentation attack
  - Spoofed session flood attack
  - ACK flood attack

- **Application Layer Attacks**: Consume application resources or services, thereby making them unavailable to other legitimate users

  Attack techniques:

  - HTTP GET/POST attack
  - Slowloris attack
  - UDP application layer flood attack
  - DDoS extortion attack

Lab Tasks

Tasks 1: Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit

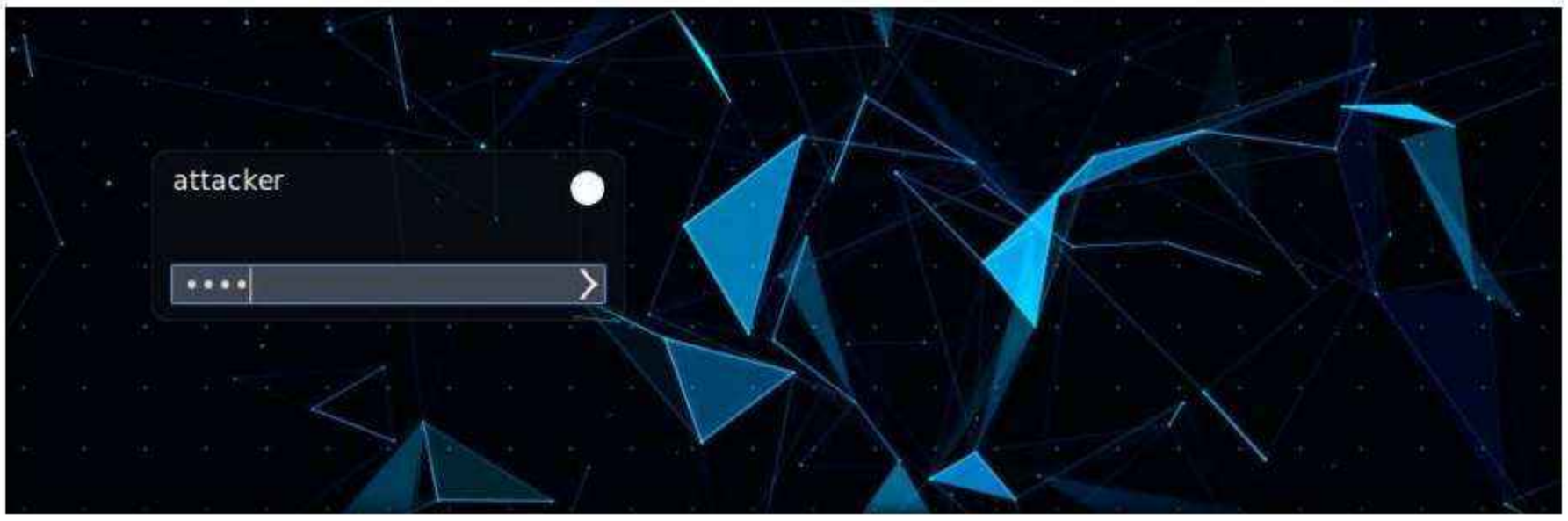
SYN flooding takes advantage of a flaw with regard to how most hosts implement the TCP three-way handshake. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle. Normally, the connection establishes with the TCP three-way handshake, and the host keeps track of the partially open connections while waiting in a listening queue for response ACK packets.

Metasploit is a penetration testing platform that allows a user to find, exploit, and validate vulnerabilities. Also, it provides the infrastructure, content, and tools to conduct penetration tests and comprehensive security auditing. The Metasploit framework has numerous auxiliary module scripts that can be used to perform DoS attacks.

Here, we will use the Metasploit tool to perform a DoS attack (SYN flooding) on a target host.

Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine to perform SYN flooding on the **Windows 11 (10.10.1.11)** machine through **port 21**.

1. Turn on the **Windows 11**, **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. 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.



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

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

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

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

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

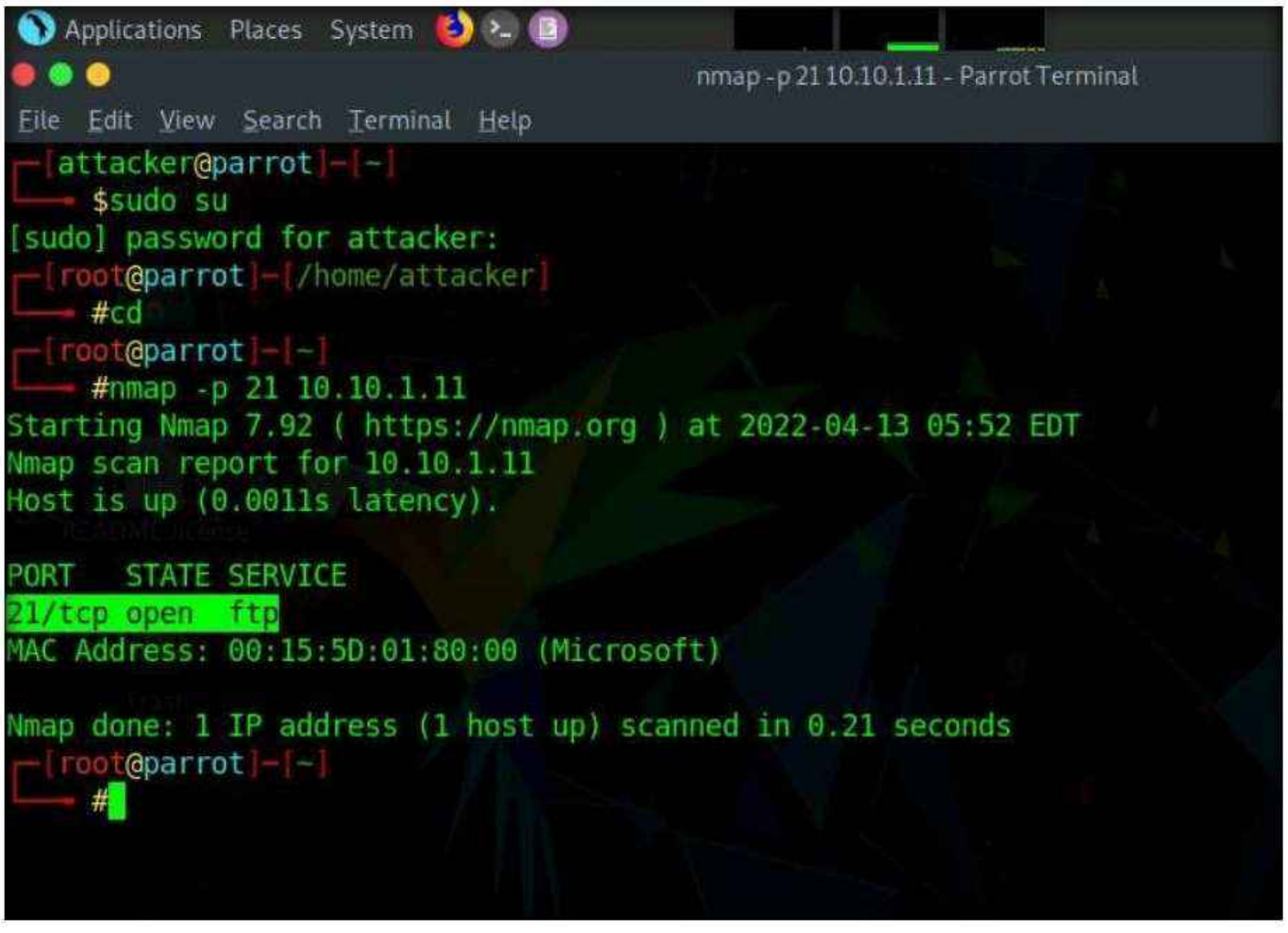
6. Now, type **cd** and press **Enter** to jump to the root directory.

7. First, determine whether port 21 is open or not. This involves using Nmap to determine the state of the port.

8. On the **Parrot Terminal** window, type **nmap -p 21 (Target IP address)** (here, target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

   Note: **-p**: specifies the port to be scanned.

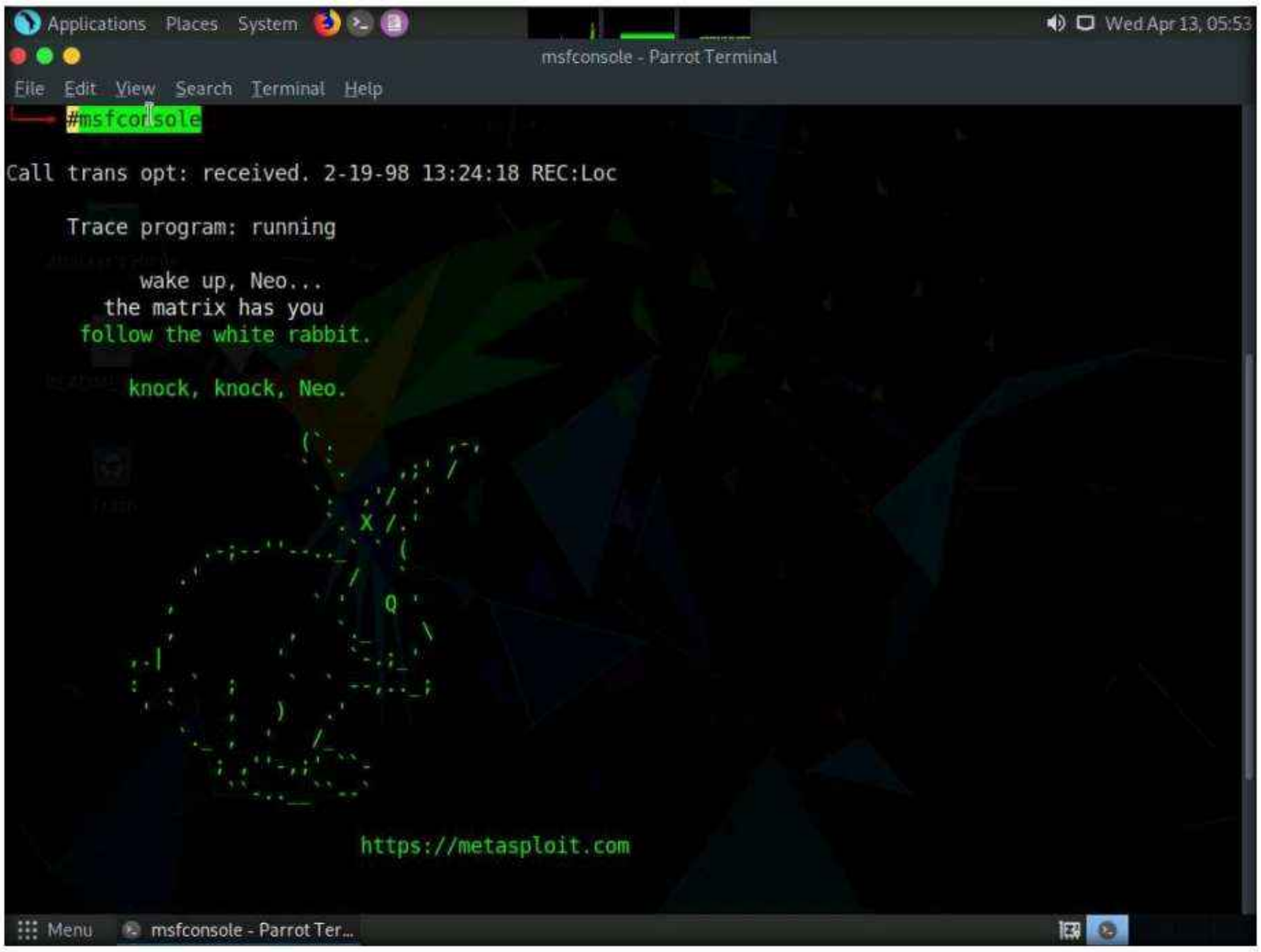
9. The result appears, displaying the port status as open, as shown in the screenshot.



10. Now, we will perform SYN flooding on the target machine (**Windows 11**) using port 21.

11. In this task, we will use an auxiliary module of Metasploit called **synflood** to perform a DoS attack on the target machine.

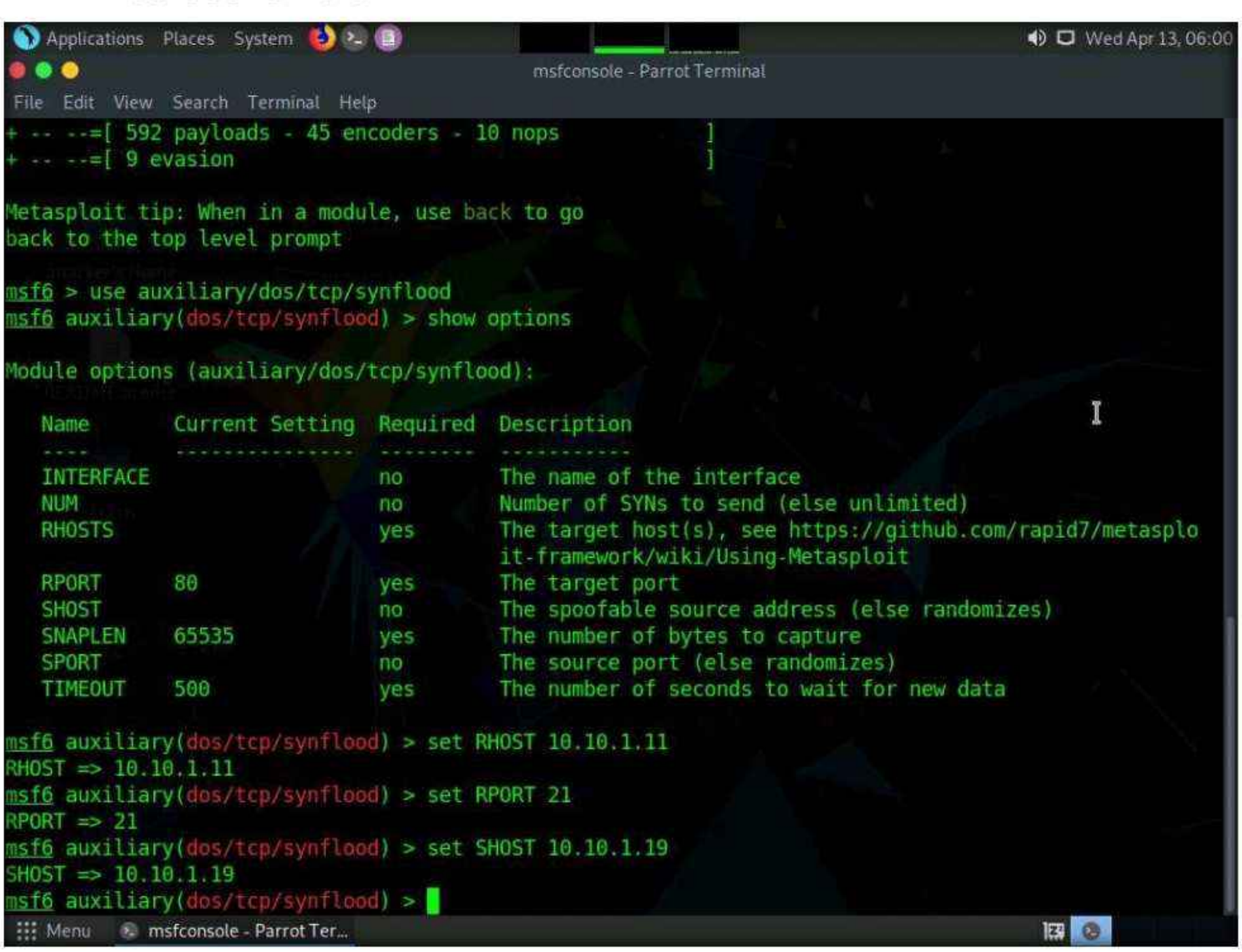
12. Type **msfconsole** from a command-line terminal and press **Enter** to launch msfconsole.



13. In the **msf** command line, type **use auxiliary/dos/tcp/synflood** and press **Enter** to launch a SYN flood module.
14. Now, determine which module options need to be configured to begin the DoS attack.
15. Type **show options** and press **Enter**. This displays all the options associated with the auxiliary module.

16. Here, we will perform SYN flooding on port **21** of the **Windows 11** machine by spoofing the IP address of the **Parrot Security** machine with that of the **Windows Server 2019 (10.10.1.19)** machine.
17. Issue the following commands:
    - **set RHOST (Target IP Address)** (here, **10.10.1.11**)
    - **set RPORT 21**
    - **set SHOST (Spoofable IP Address)** (here, **10.10.1.19**)

    Note: By setting the SHOST option to the IP address of the Windows Server 2019 machine, you are spoofing the IP address of the Parrot Security machine with that of Windows Server 2019.



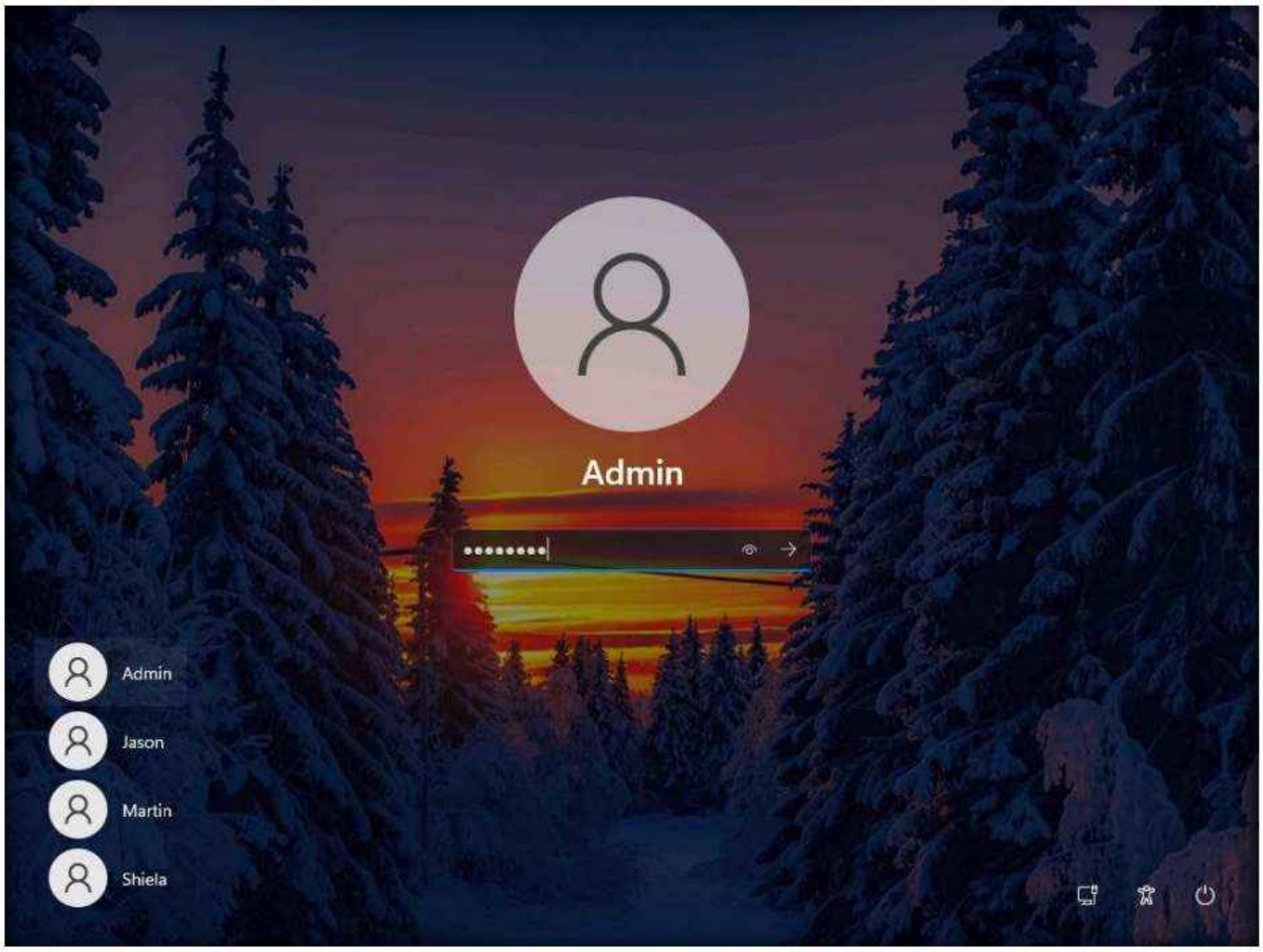
18. Once the auxiliary module is configured with the required options, start the DoS attack on the **Windows 11** machine.

19. To do so, type **exploit** and press **Enter**. This begins SYN flooding the **Windows 11** machine.

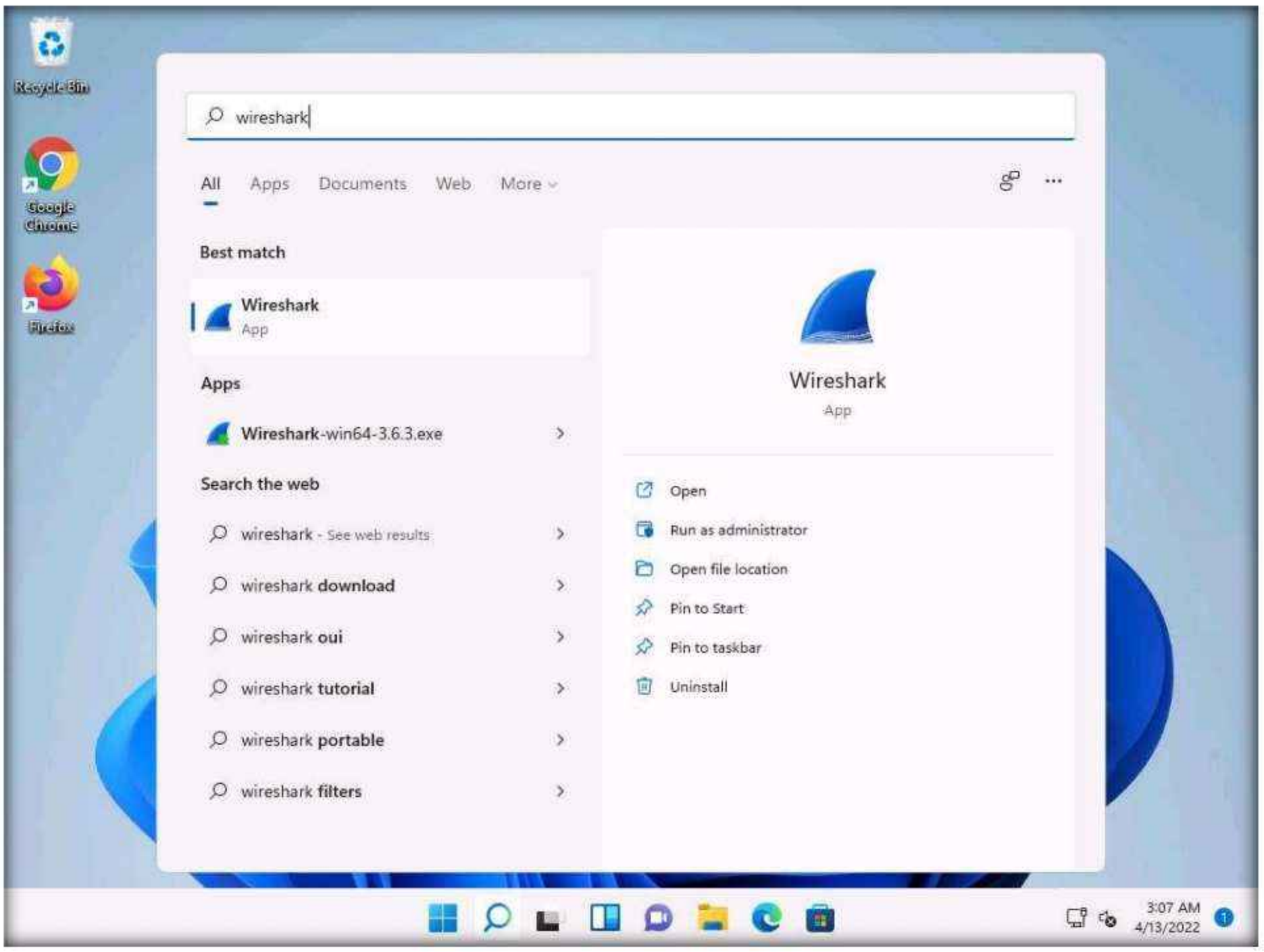
20. To confirm, switch to the **Windows 11** virtual machine and click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

    Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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



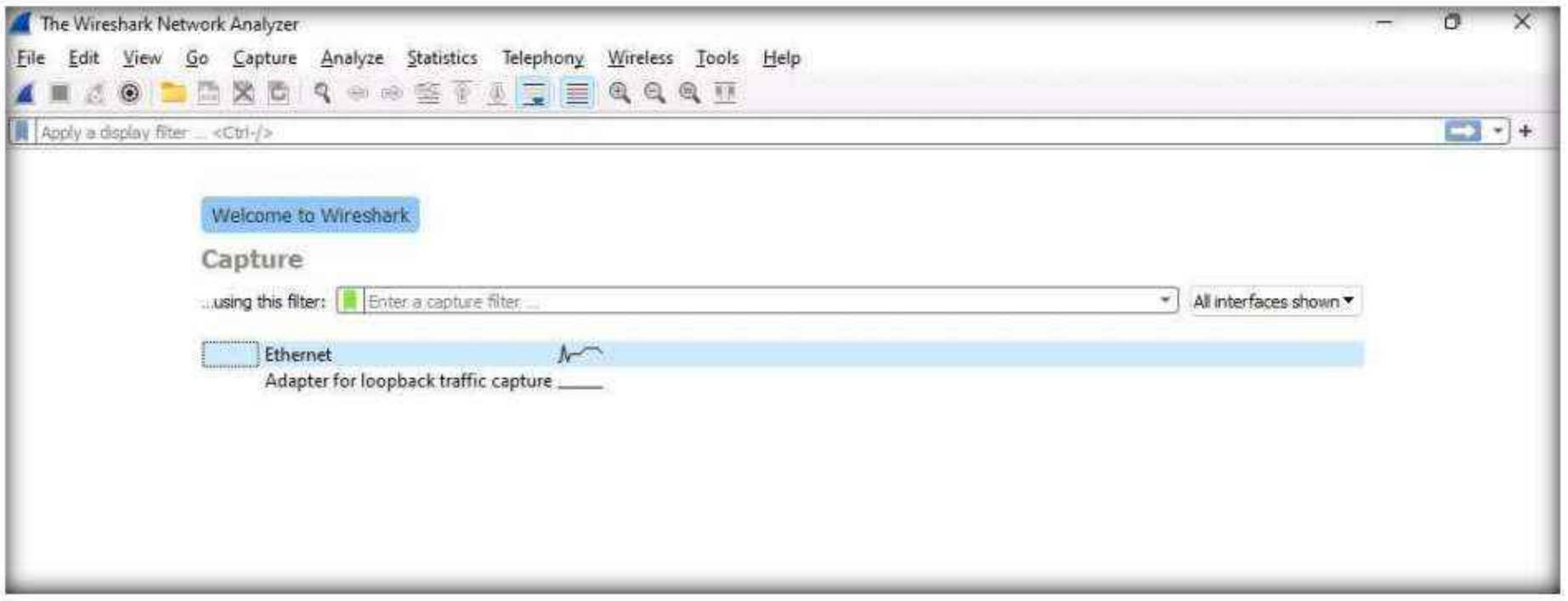
21. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



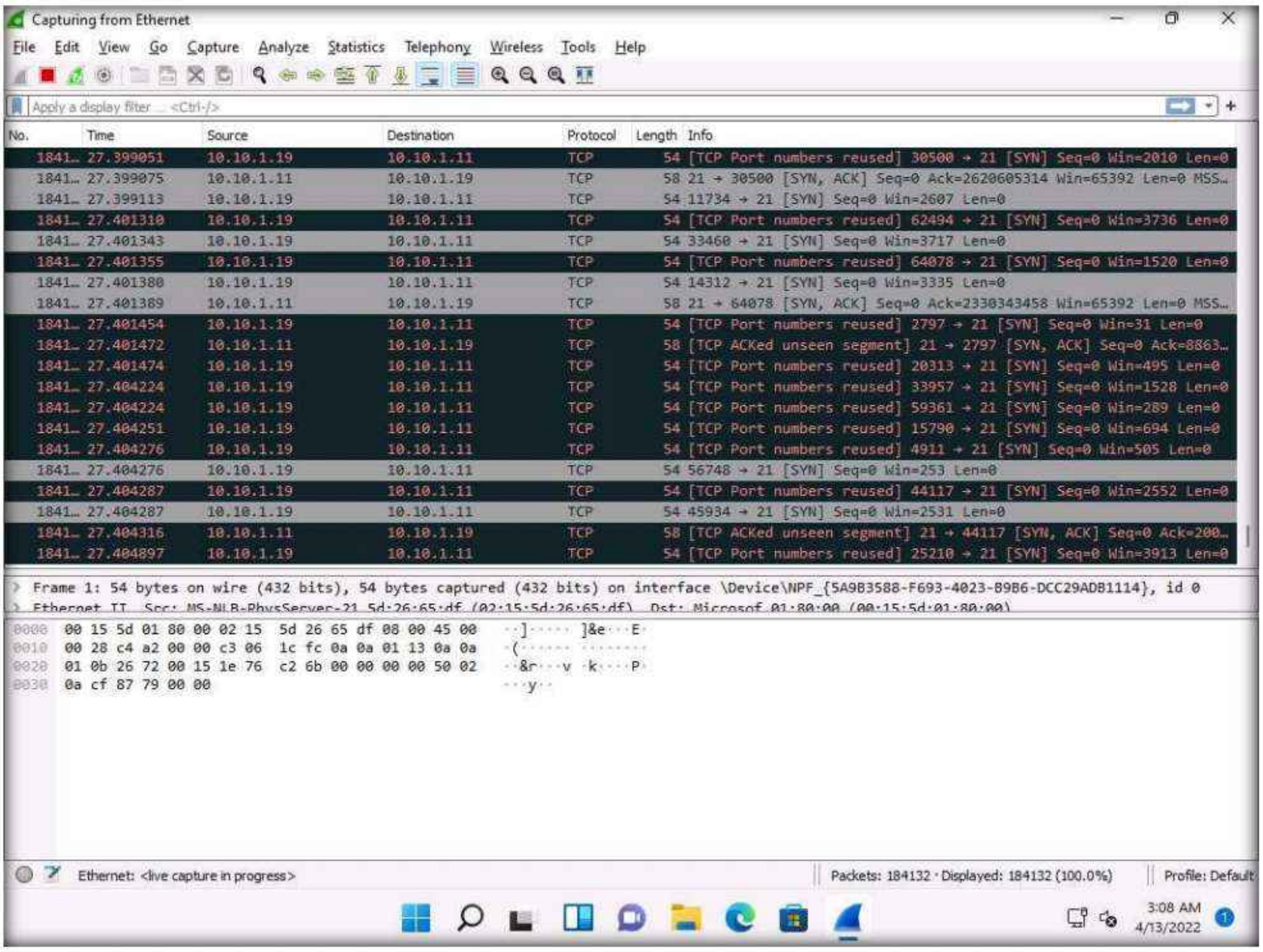
22. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: The network interface might differ when you perform the task.

Note: If a **Software Update** pop-up appears click on **Remind me later**.

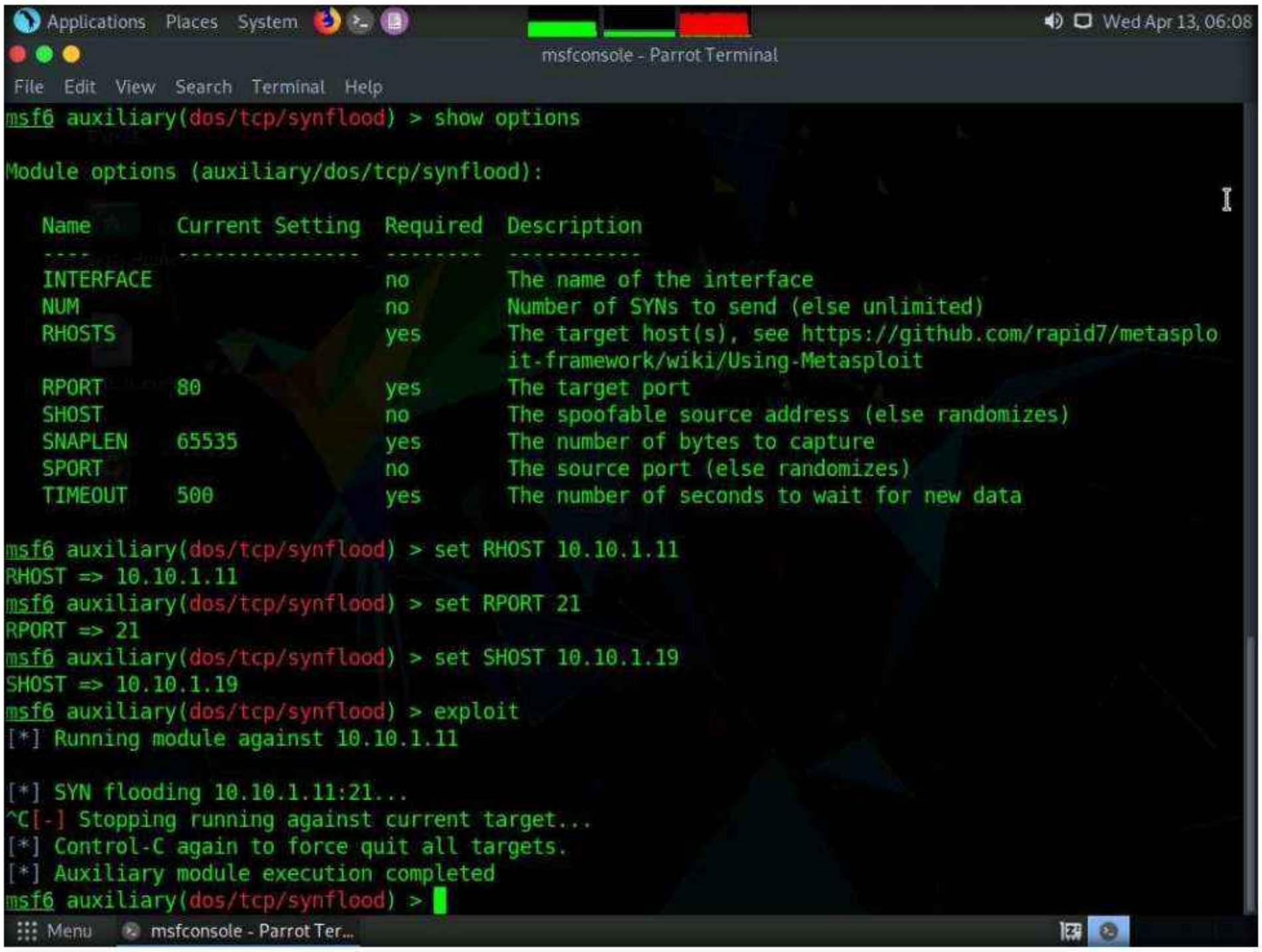


23. **Wireshark** displays the traffic coming from the machine. Here, you can observe that the **Source IP** address is that of the **Windows Server 2019** (10.10.1.19) machine. This implies that the IP address of the **Parrot Security** machine has been spoofed.



24. Observe that the target machine (**Windows 11**) has drastically slowed, implying that the DoS attack is in progress on the machine. If the attack is continued for some time, the machine's resources will eventually be completely exhausted, causing it to stop responding.

25. Once the performance analysis of the machine is complete, switch to the **Parrot Security** machine and press **Ctrl+C** to terminate the attack.



26. This concludes the demonstration of how to perform SYN flooding on a target host using Metasploit.
27. Close all open windows and document all the acquired information.

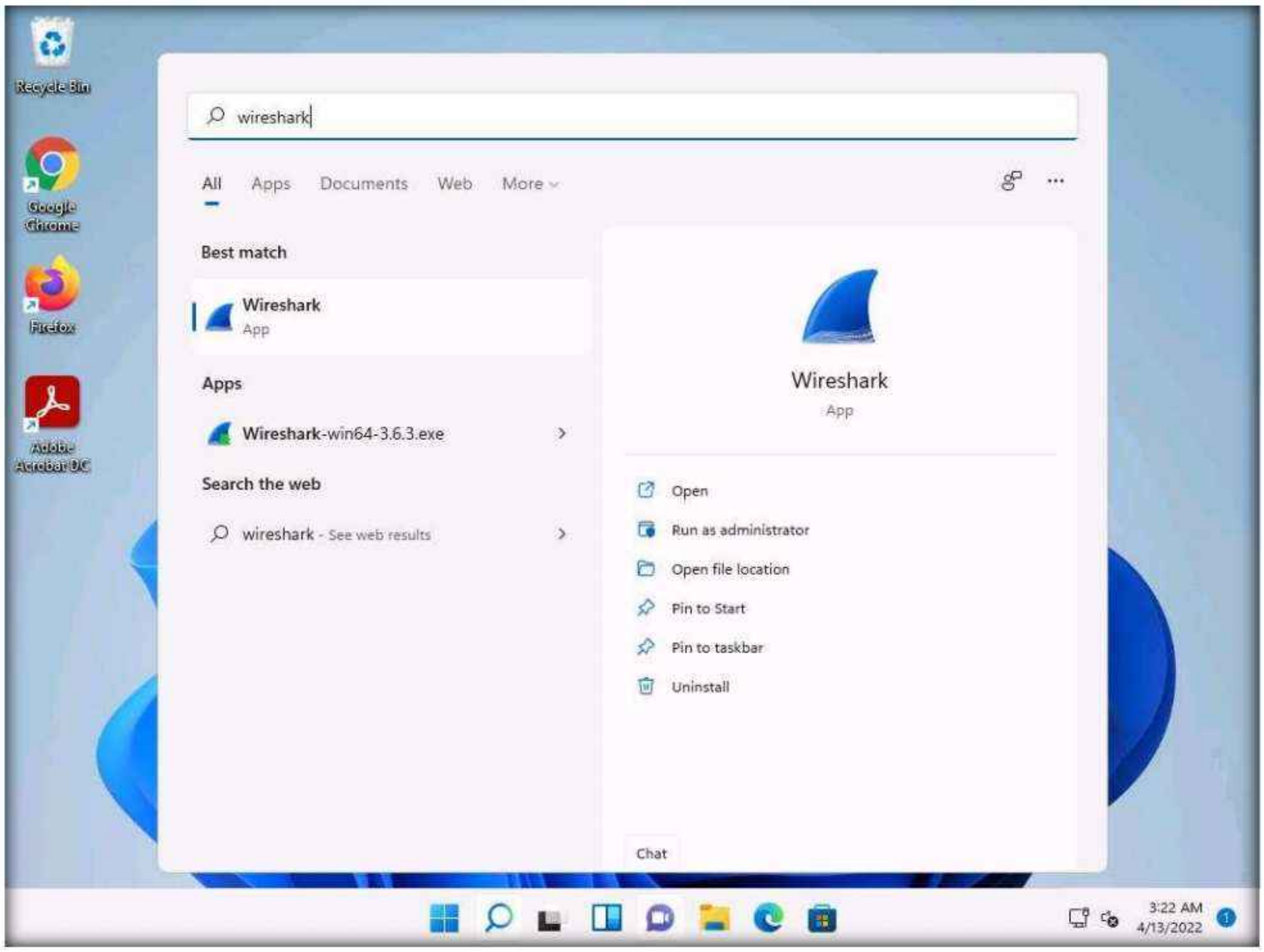
Task 2: Perform a DoS Attack on a Target Host using hping3

hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

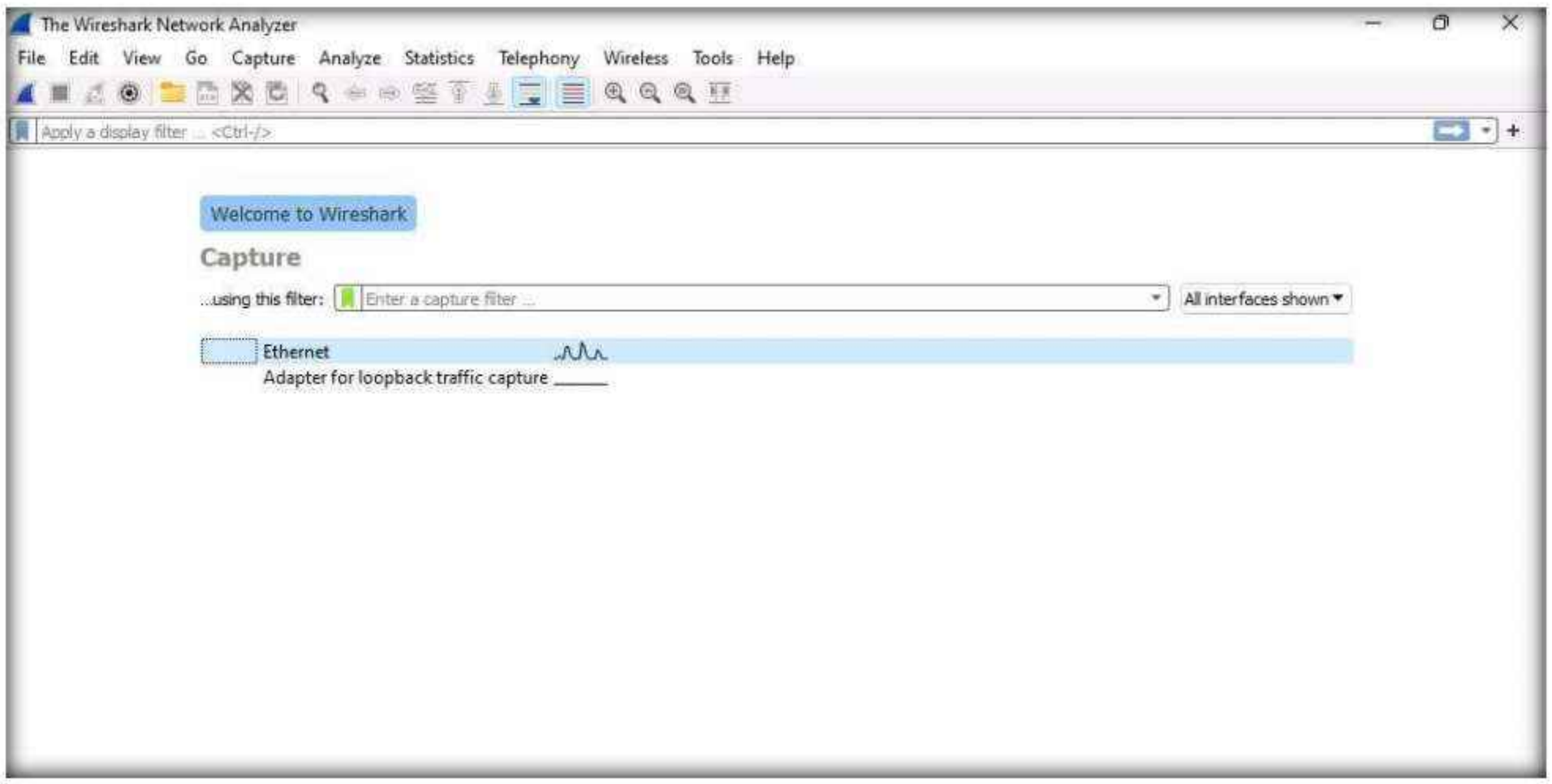
Here, we will use the hping3 tool to perform DoS attacks such as SYN flooding, Ping of Death (PoD) attacks, and UDP application layer flood attacks on a target host.

1. Switch to the **Windows 11** virtual machine. On the **Windows 11** machine, Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.

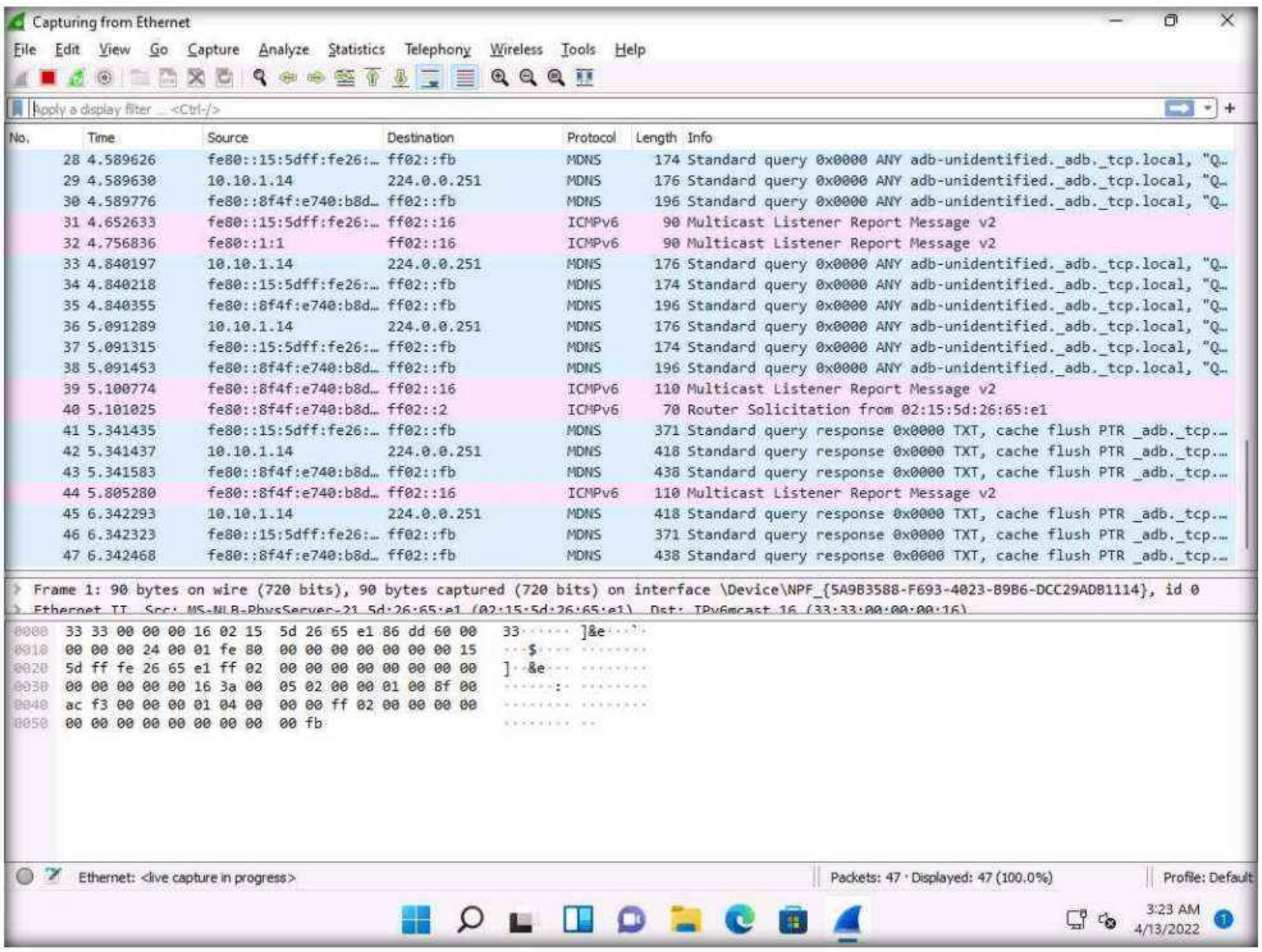


2. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

   Note: If a **Software Update** pop-up appears click on **Remind me later**.



3. **Wireshark** starts capturing the packets; leave it running.

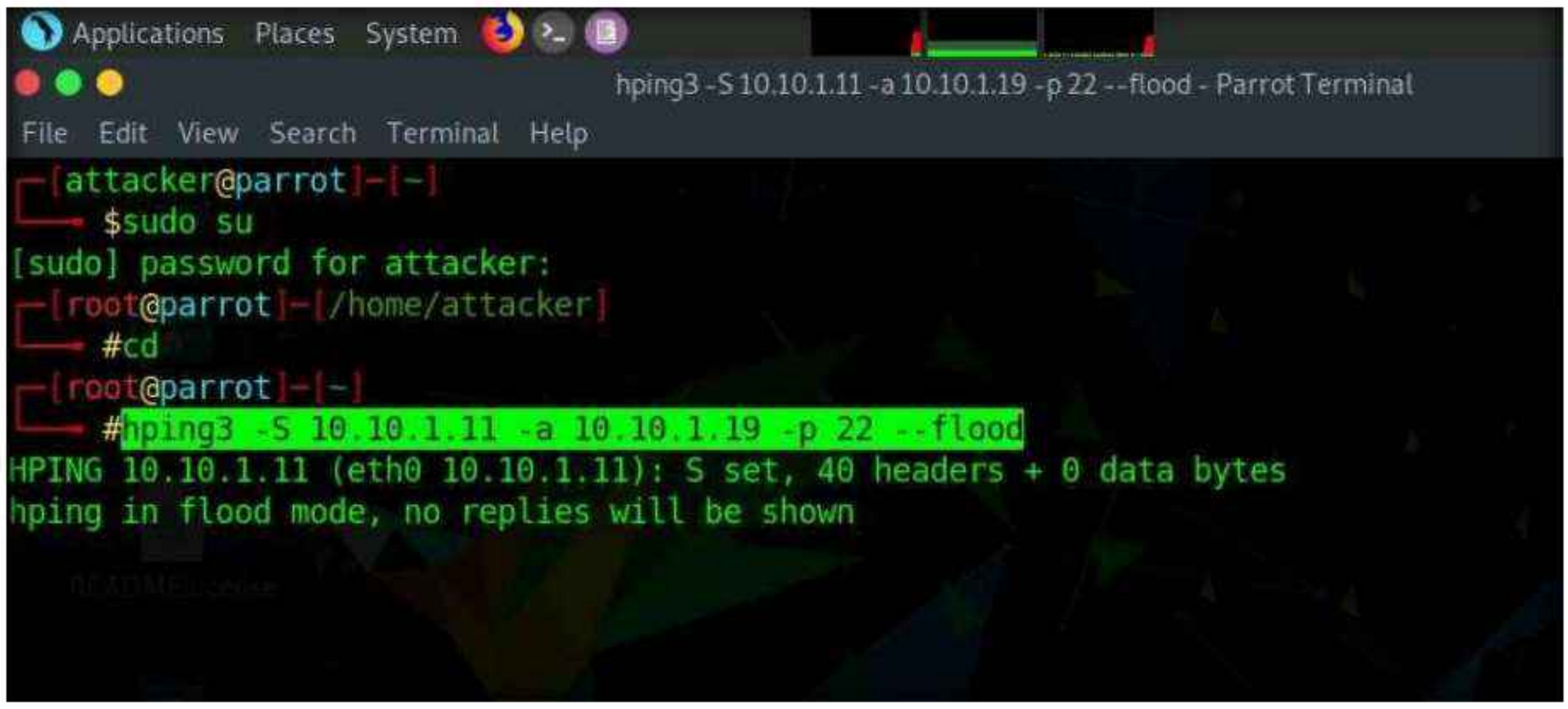


4. Switch to the **Parrot Security** virtual machine.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. The **Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
8. Now, type **cd** and press **Enter** to jump to the root directory.
9. A **Parrot Terminal** window appears; type **hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood** and press **Enter**.

   Note: Here, the target IP address is **10.10.1.11 [Windows 11]**, and the spoofable IP address is **10.10.1.19 [Windows Server 2019]**.

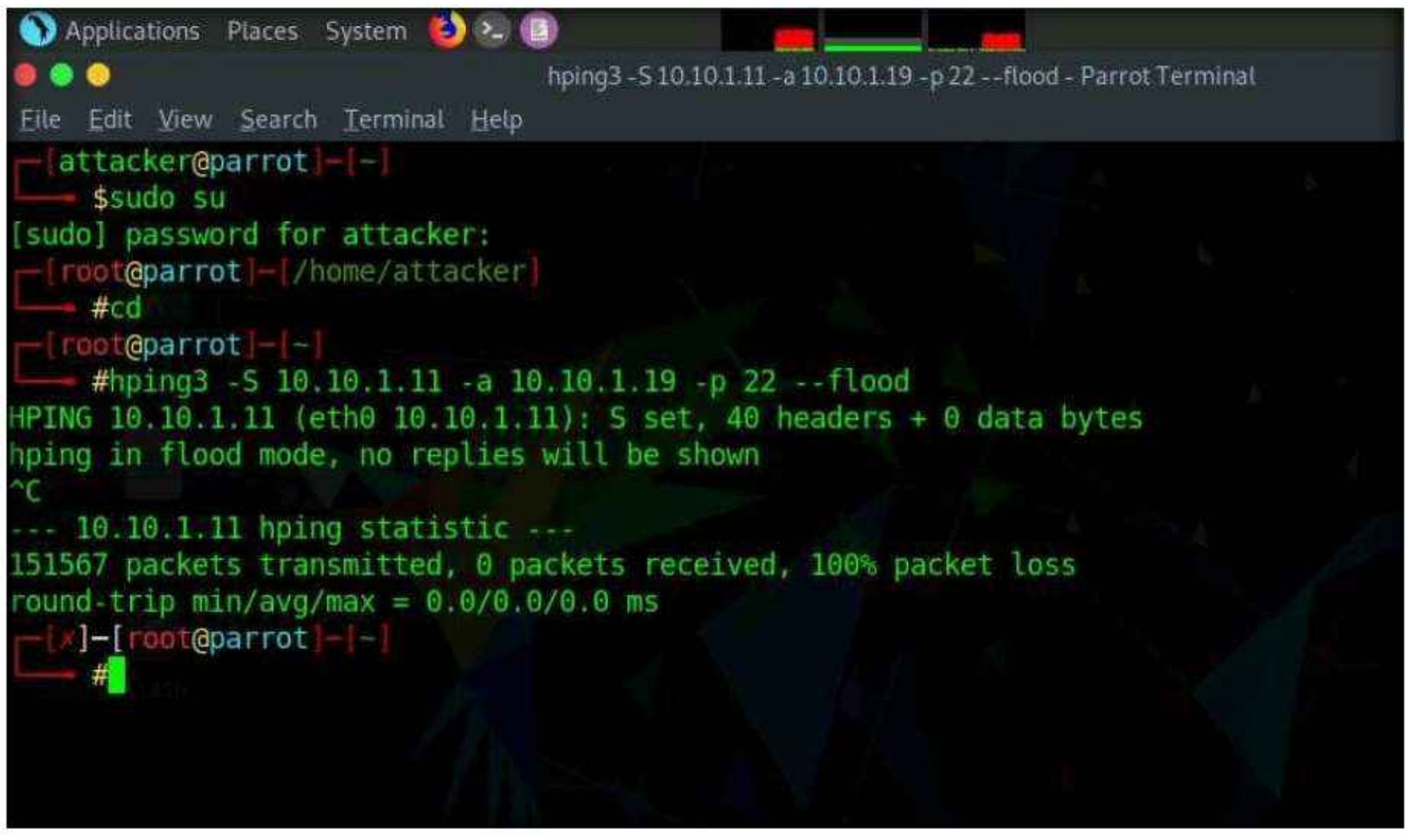
   Note: **-S**: sets the SYN flag; **-a**: spoofs the IP address; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.



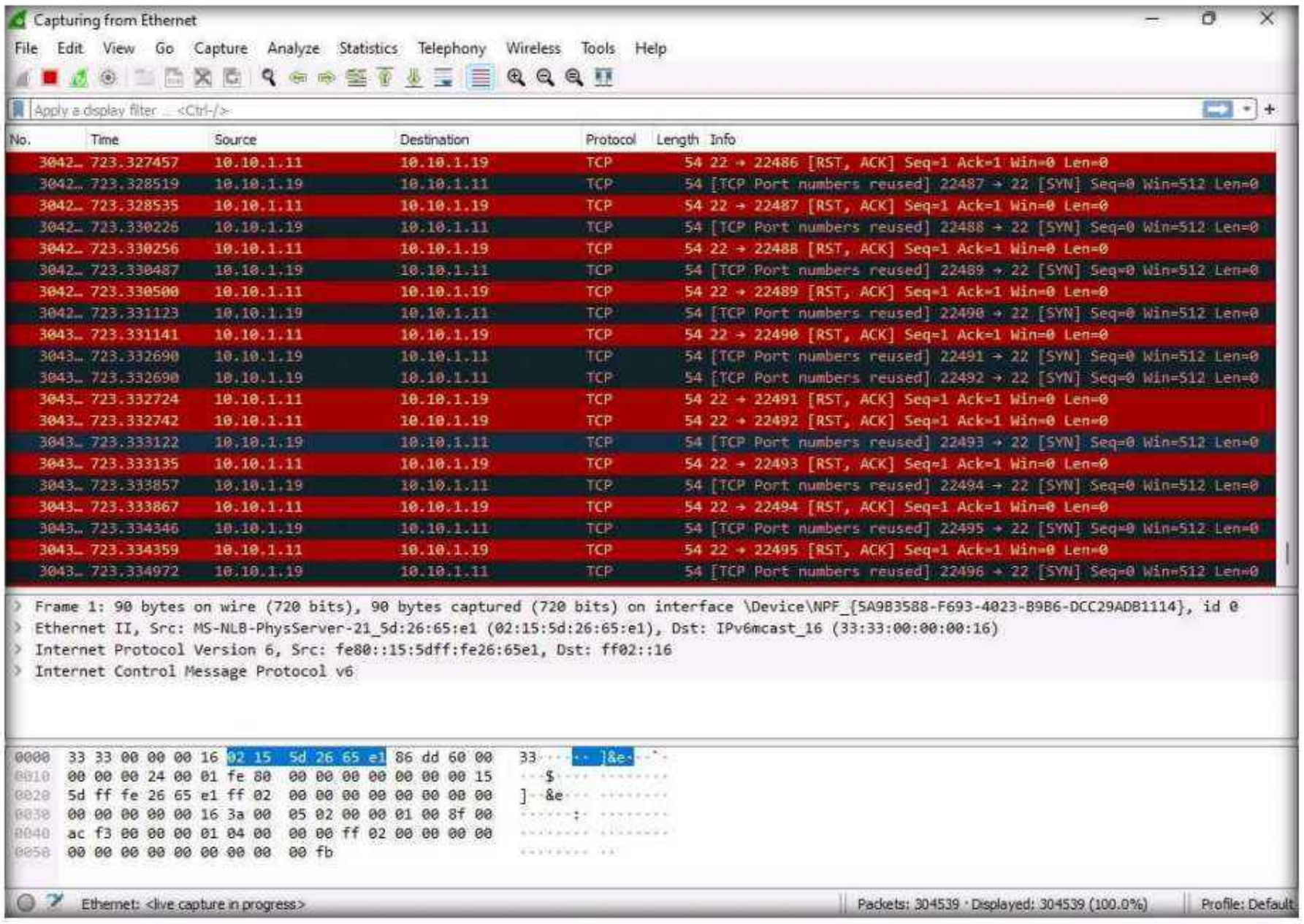
10. This command initiates the SYN flooding attack on the **Windows 11** machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

    Note: If you send the SYN packets for a long period, then the target system may crash.

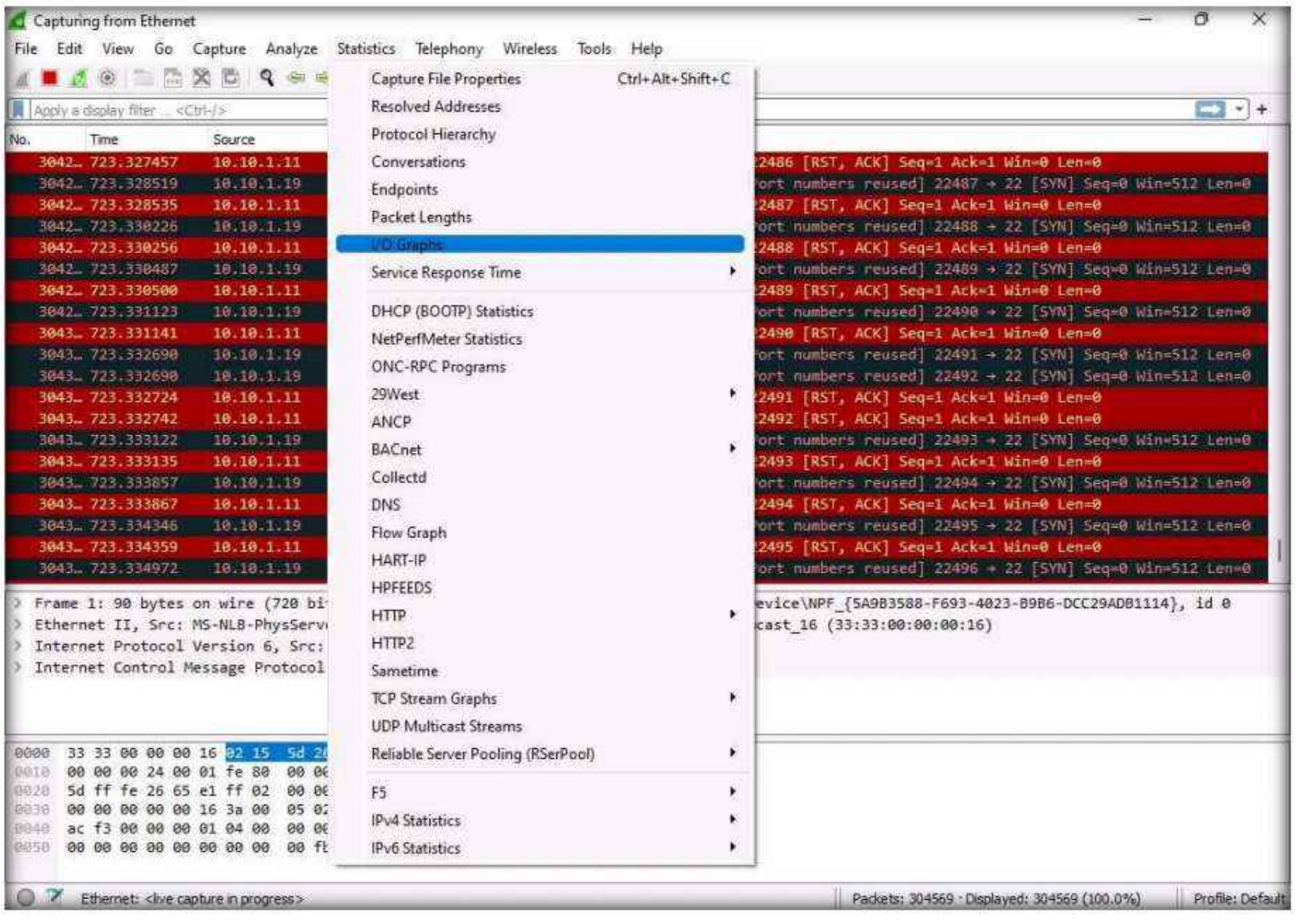
11. Observe how, in very little time, the huge number of packets are sent to the target machine.



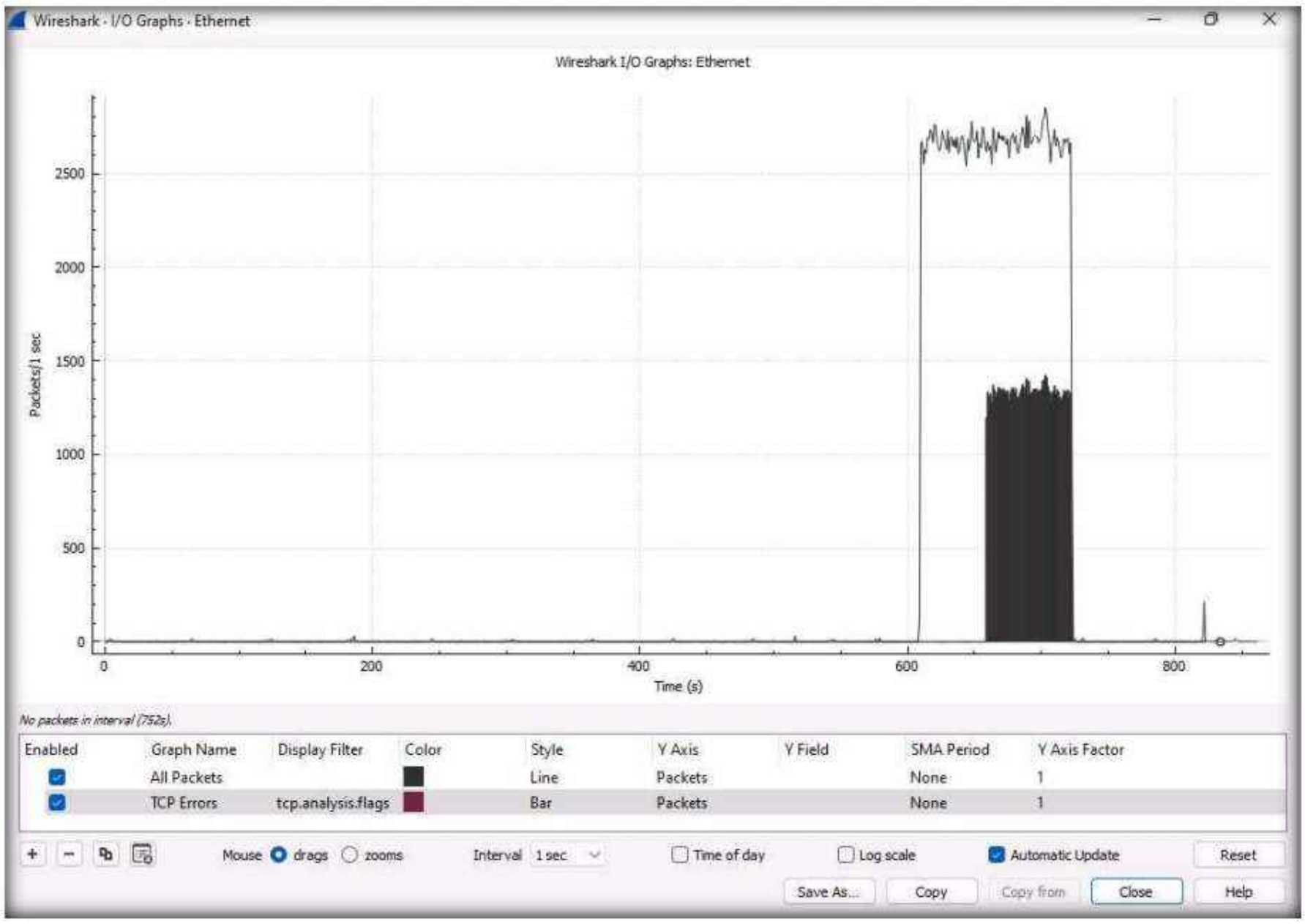
12. **hping3** floods the victim machine by sending bulk **SYN packets** and **overloading** the victim's resources.
13. Switch to the **Windows 11** virtual machine and observe the TCP-SYN packets captured by **Wireshark**.



14. Now, observe the graphical view of the captured packets. To do so, click **Statistics** from the menu bar, and then click the **I/O Graph** option from the drop-down list.

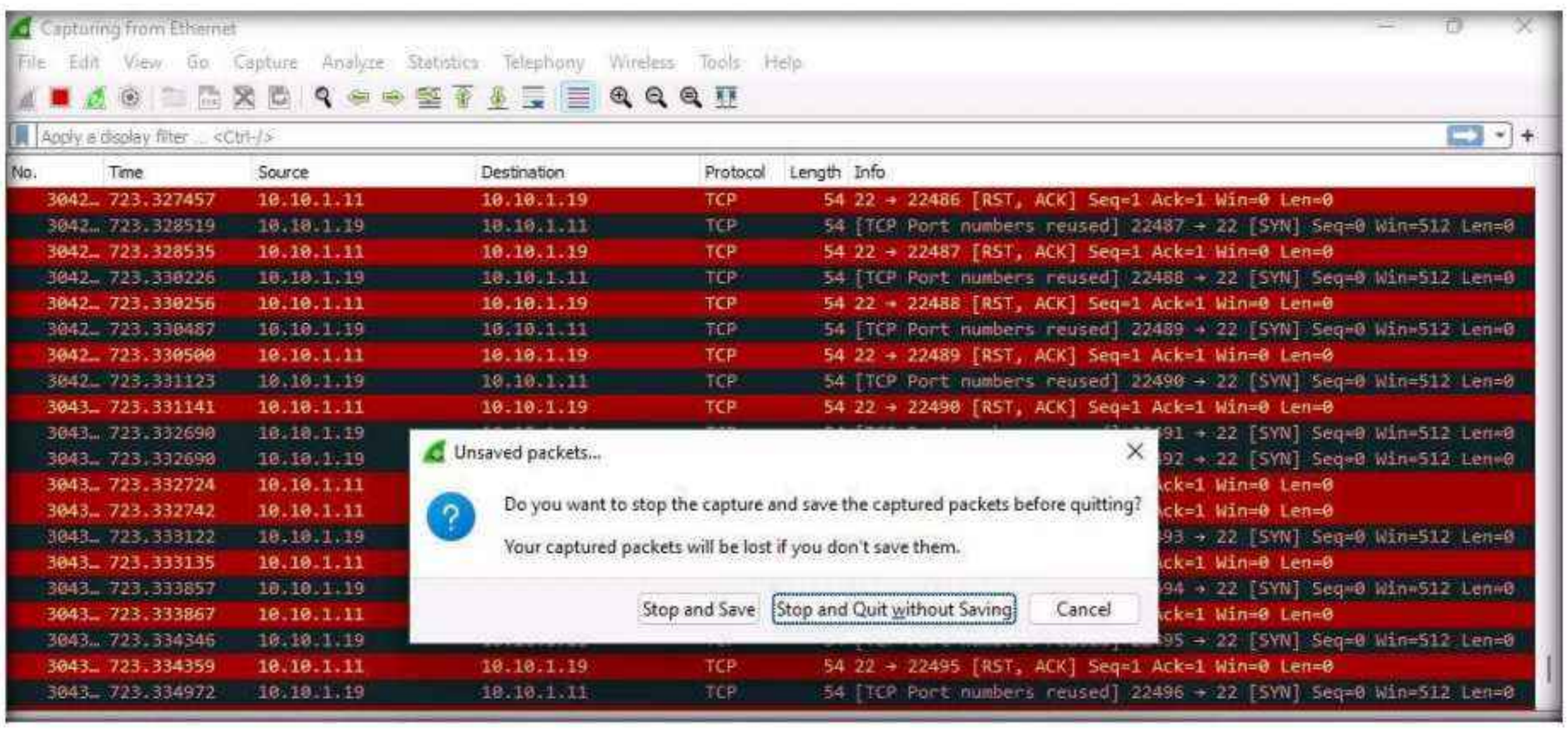


15. The **Wireshark** . **IO Graphs** . **Ethernet** window appears, displaying the graphical view of the captured packets. Observe the huge number of TCP packets captured by Wireshark, as shown in the screenshot.



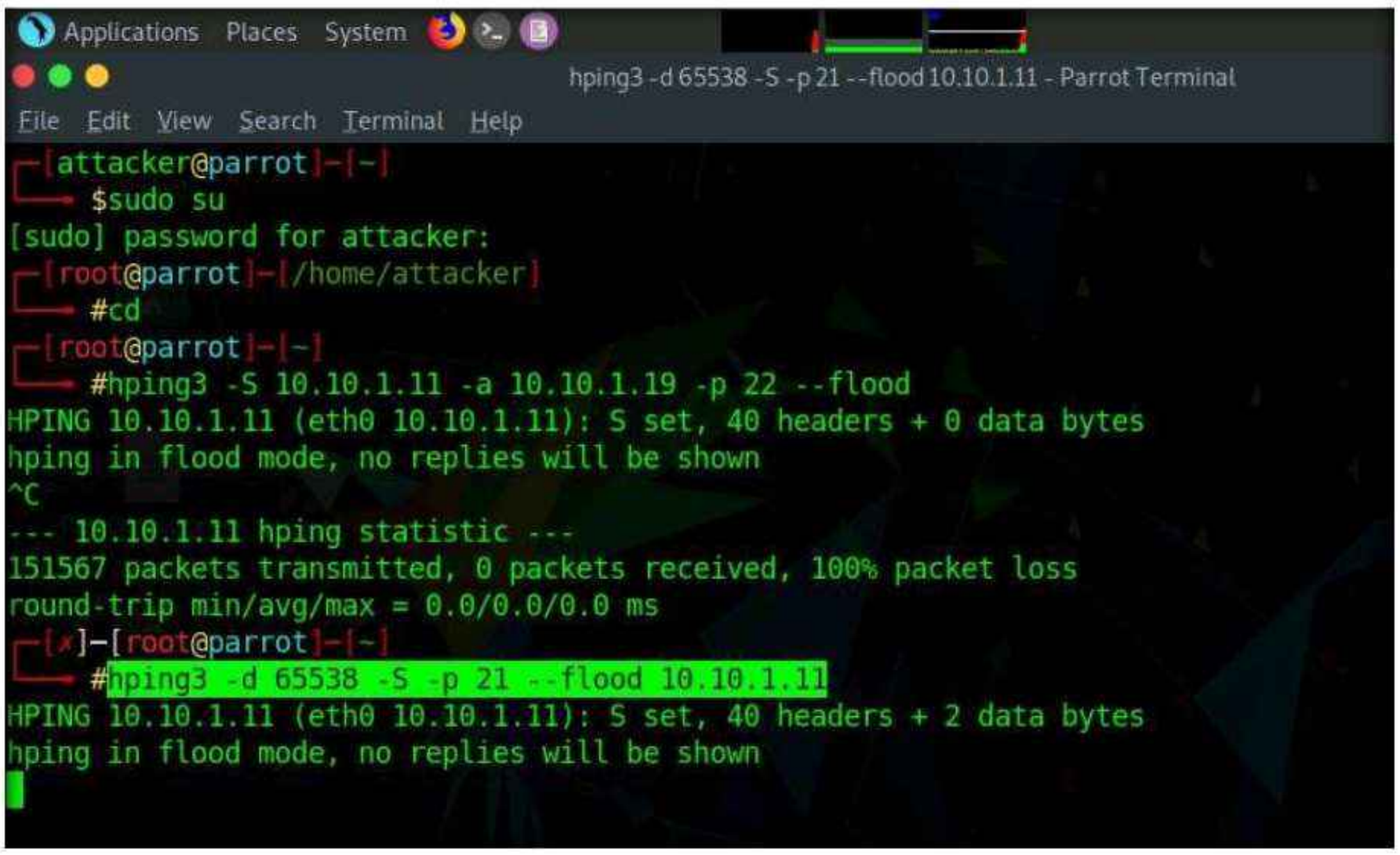
16. After analyzing the **I/O Graph**, click **Close** to close the **Wireshark** . **IO Graphs** . **Ethernet** window.

17. Close the **Wireshark** main window. If an **Unsaved packets…** pop-up appears, click **Stop and Quit without Saving**.



18. Now, we shall perform a PoD attack on the target system.
19. Now, switch to the **Parrot Security** virtual machine. In the **Terminal** window, type **hping3 -d 65538 -S -p 21 --flood (Target IP Address)** (here, the target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

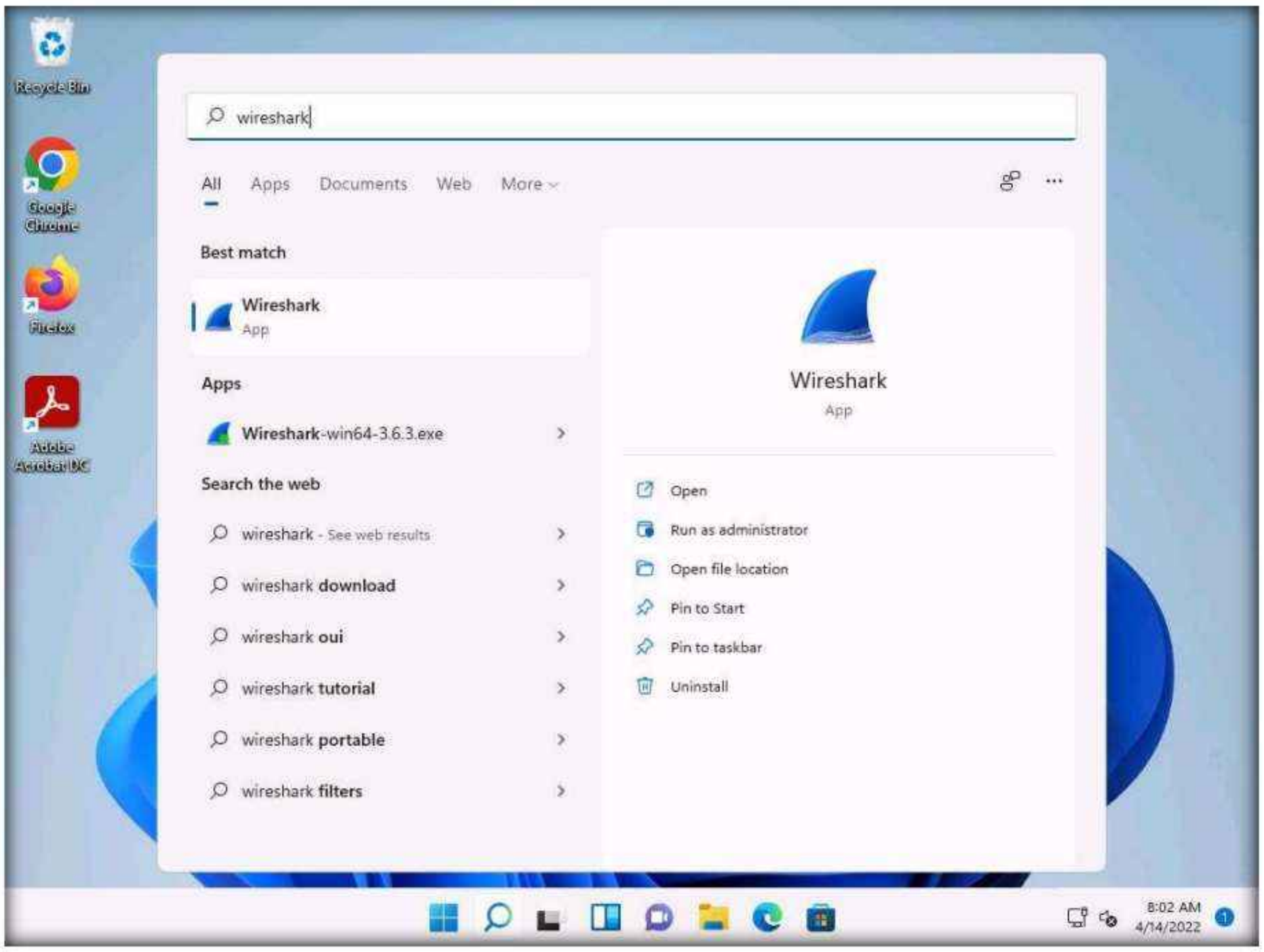
    Note: **-d**: specifies data size; **-S**: sets the SYN flag; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.



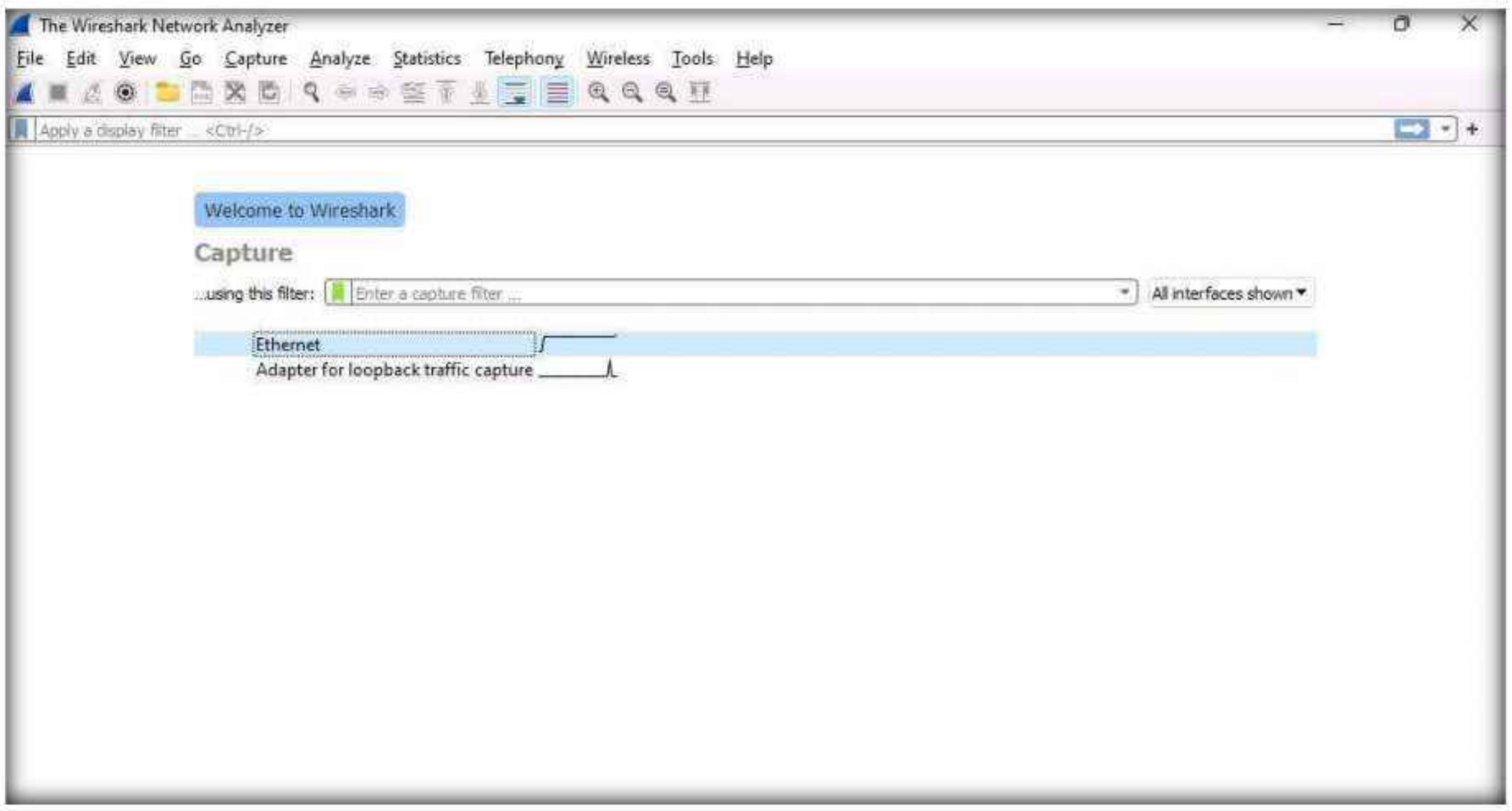
20. This command initiates the PoD attack on the **Windows 11** machine.

    Note: In a PoD attack, the attacker tries to crash, freeze, or destabilize the targeted system or service by sending malformed or oversized packets using a simple ping command.

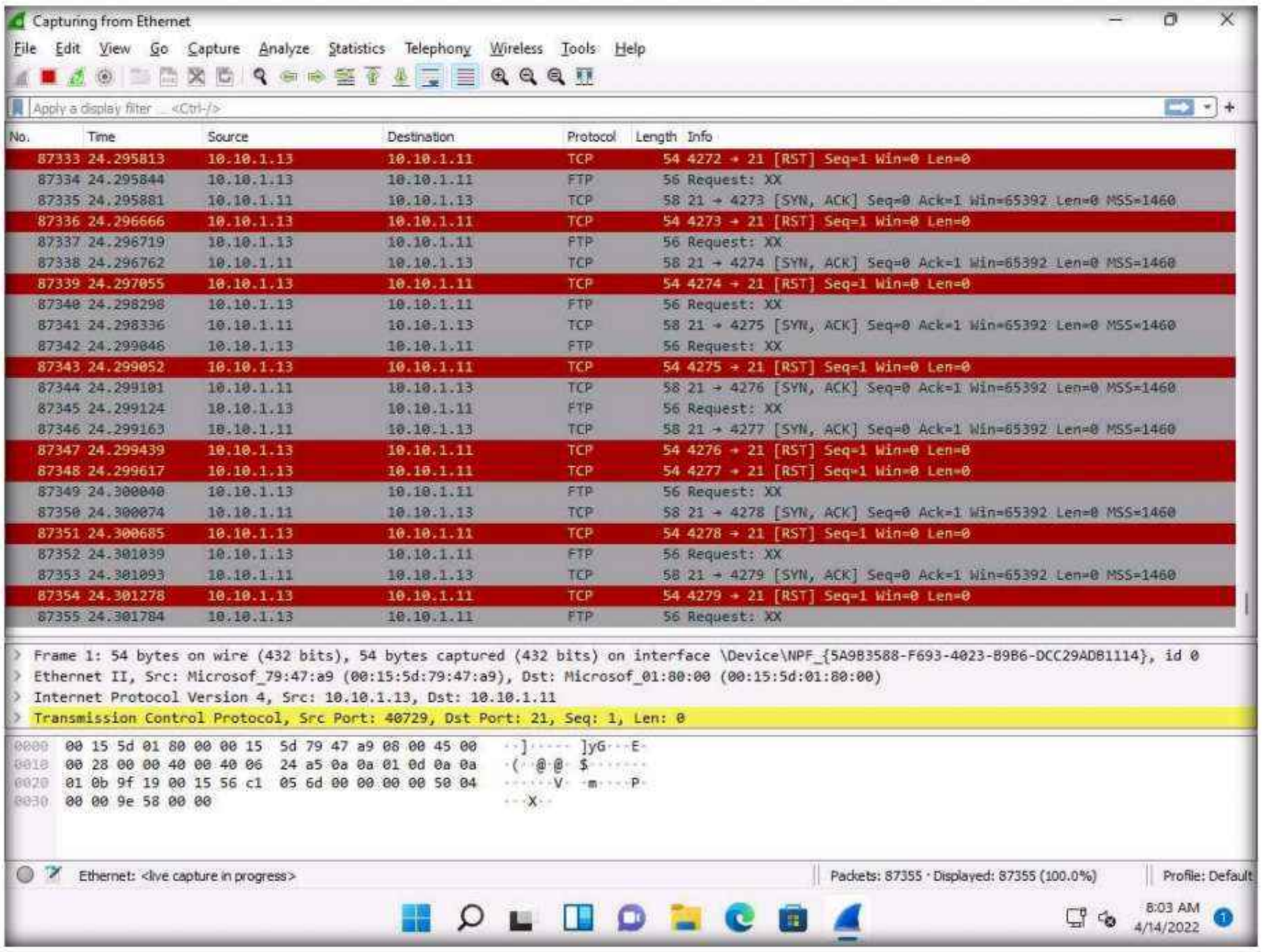
    Note: For example, the attacker sends a packet that has a size of 65,538 bytes to the target web server. This packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The receiving system's reassembly process might cause the system to crash.
21. **hping3** floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.
22. Switch to the **Windows 11** virtual machine.
23. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



24. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.



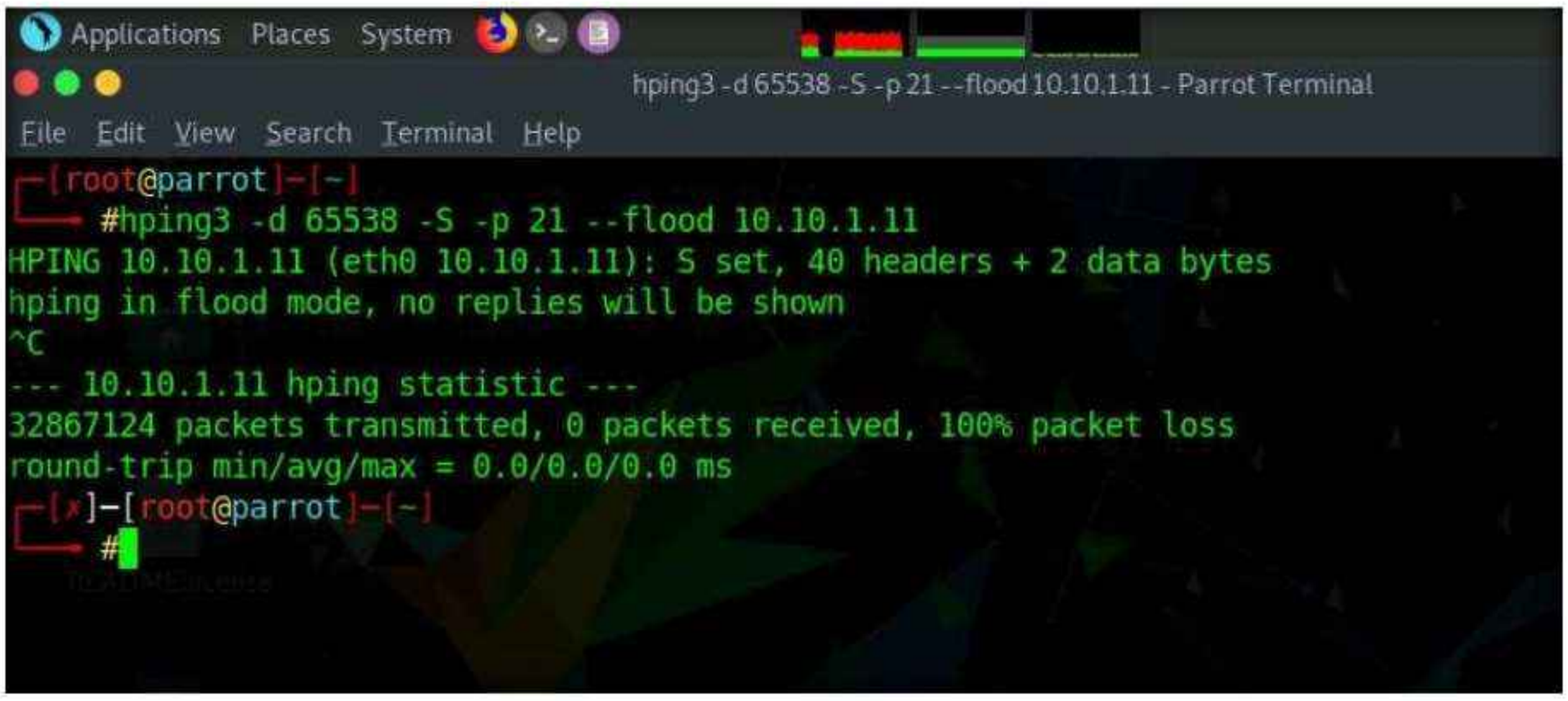
25. Observe the large number of packets captured by **Wireshark**.



26. You can observe the degradation in the performance of the system.

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

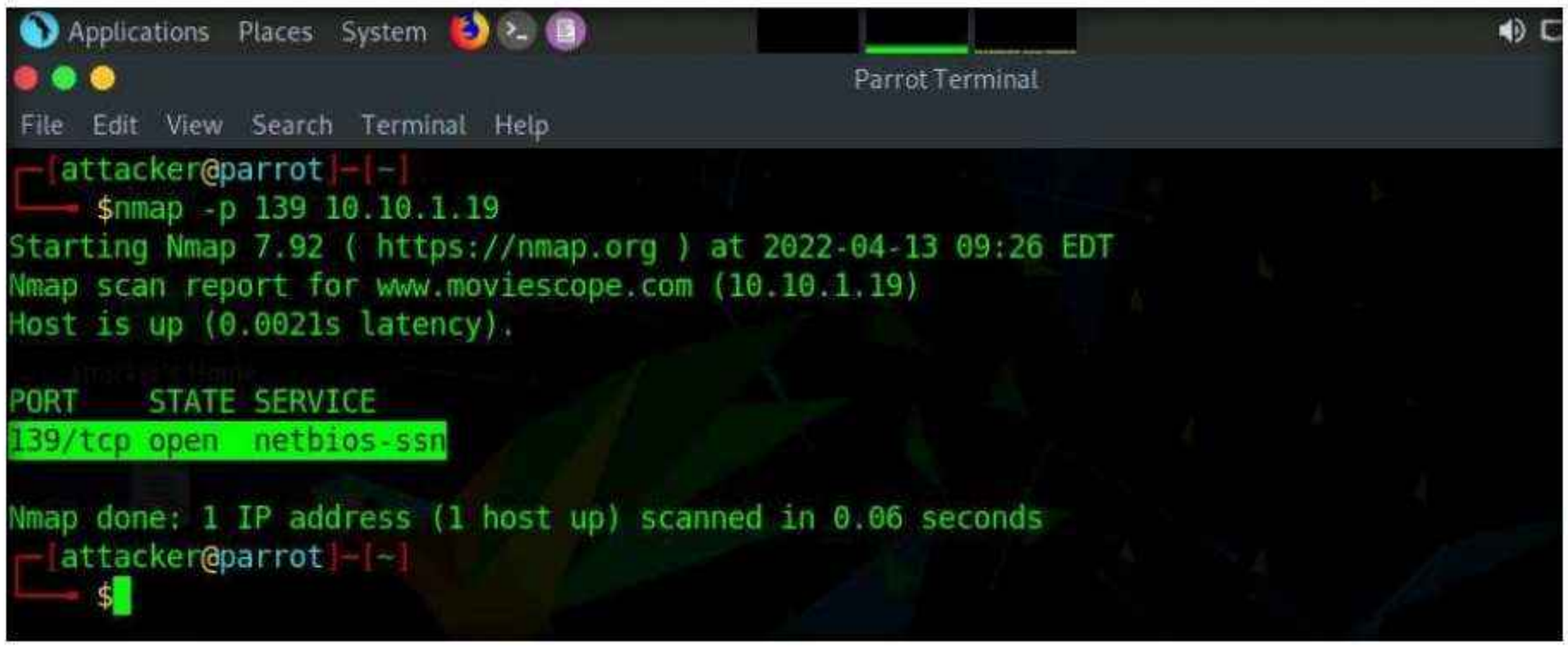
27. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the PoD attack using hping3.



28. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.

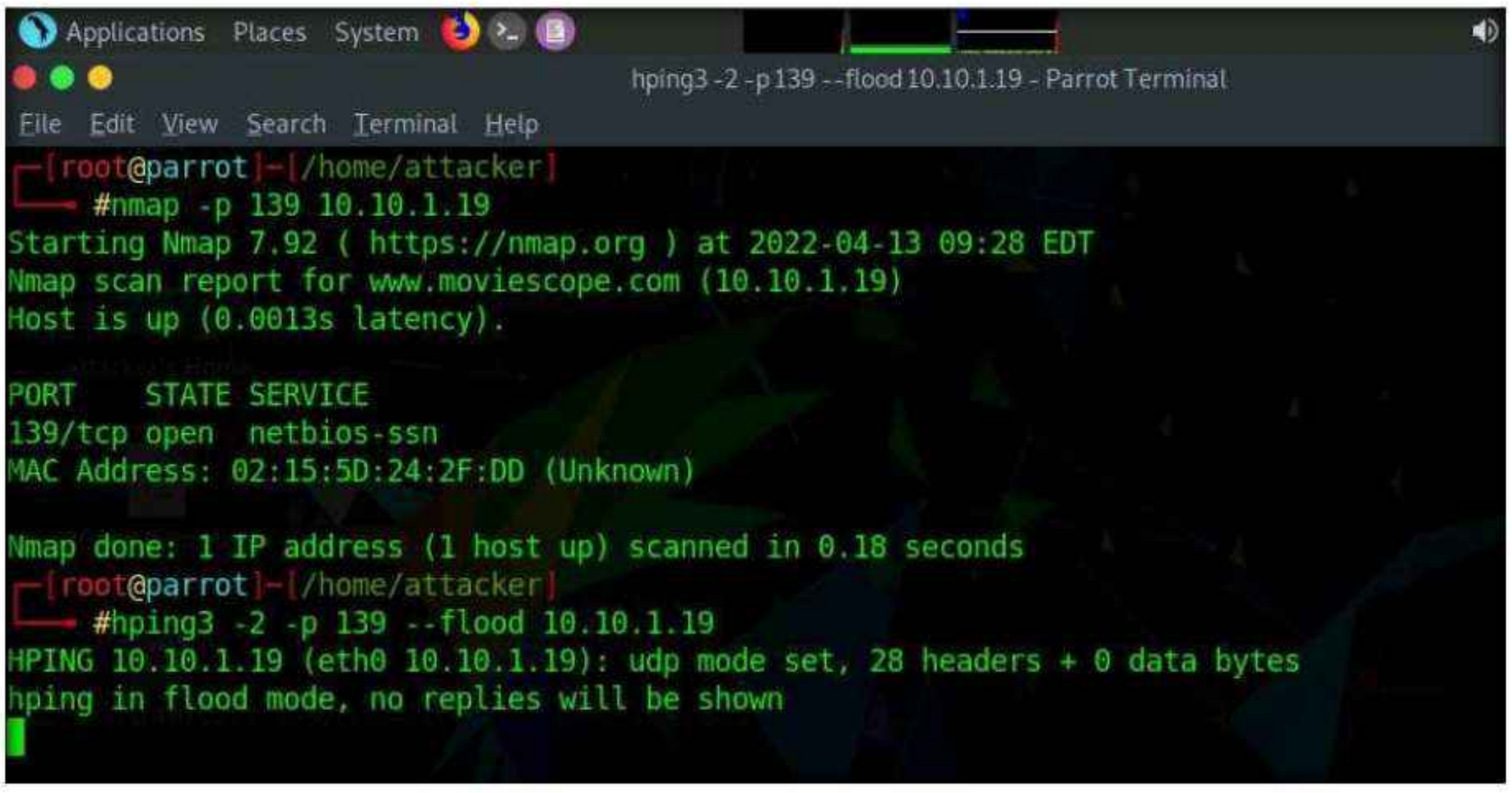
29. In the terminal window, type **nmap -p 139 (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.

    Note: Here, we will use NetBIOS port 139 to perform a UDP application layer flood attack.



30. Now, type **hping3 -2 -p 139 --flood (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.

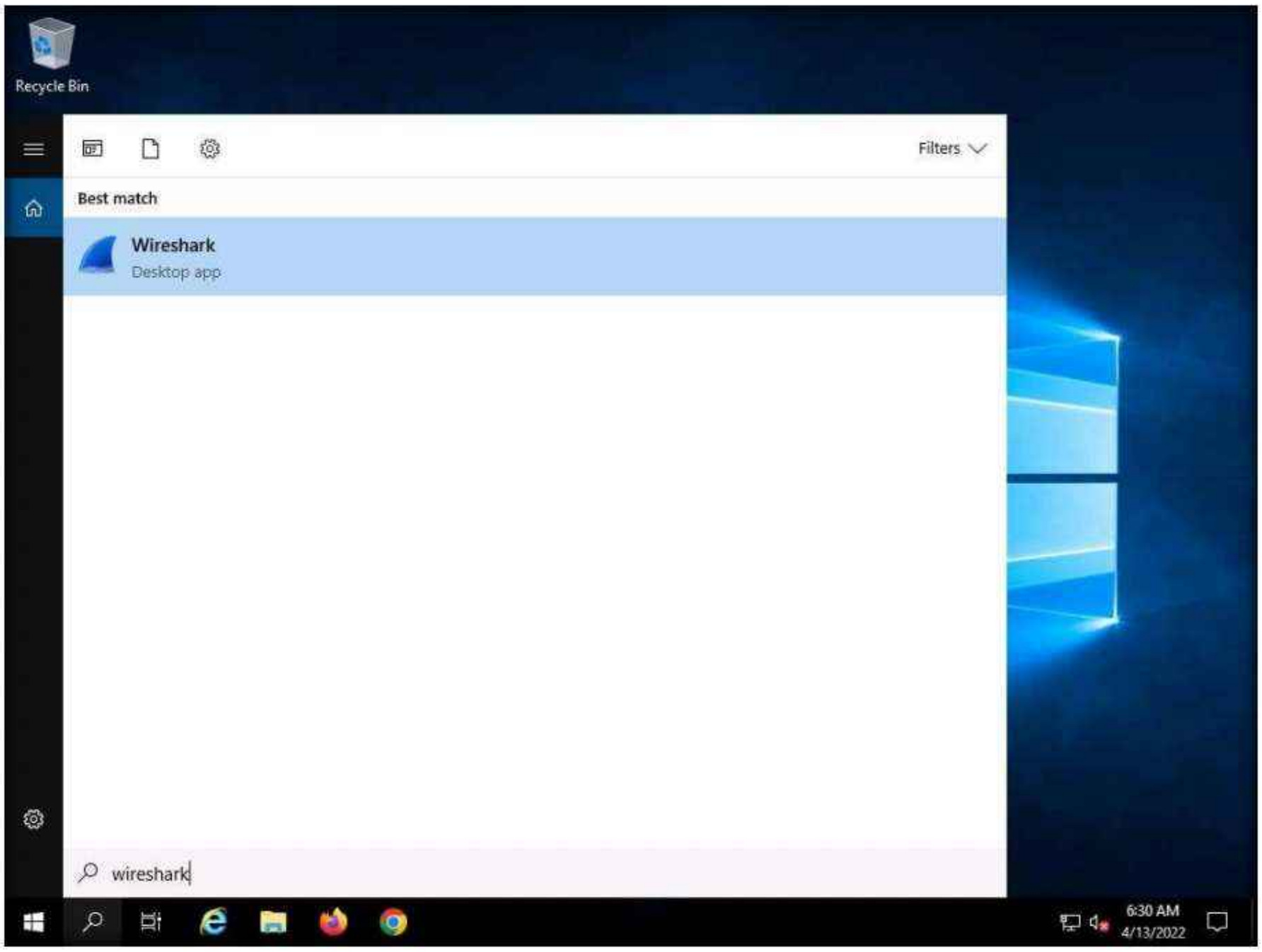
    Note: **-2**: specifies the UDP mode; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.



31. Switch to the **Windows Server 2019** machine, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to log in.

32. In the **Type here to search** field on the **Desktop**, type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.

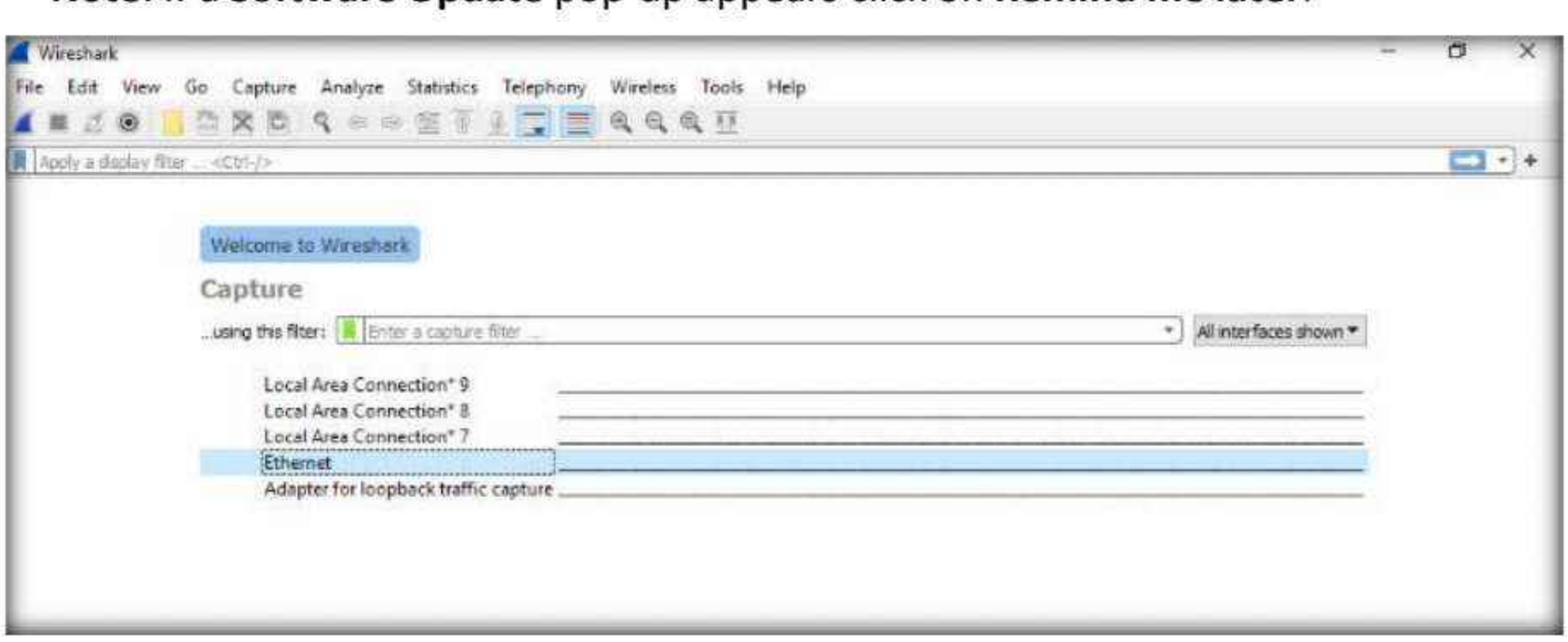
    Note: You might experience degradation in the **Window Server 2019** machine's performance.



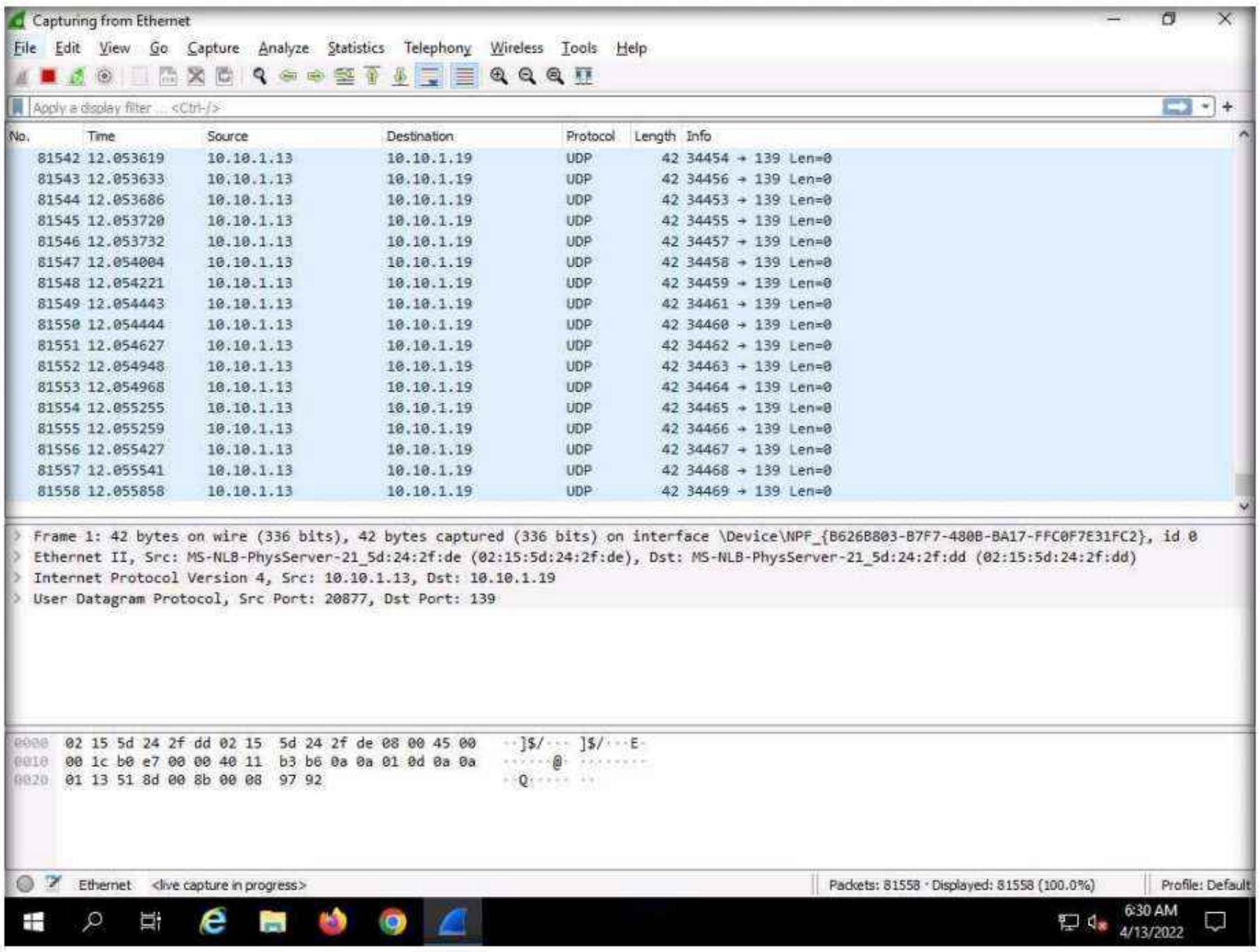
33. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

    Note: The network interface might differ when you perform the task.

    Note: If a **Software Update** pop-up appears click on **Remind me later**.



34. **Wireshark** displays the network's flow of traffic. Here, observe the huge number of **UDP** packets coming from the **Source** IP address **10.10.1.13** via port **139**.



35. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the DoS attack.

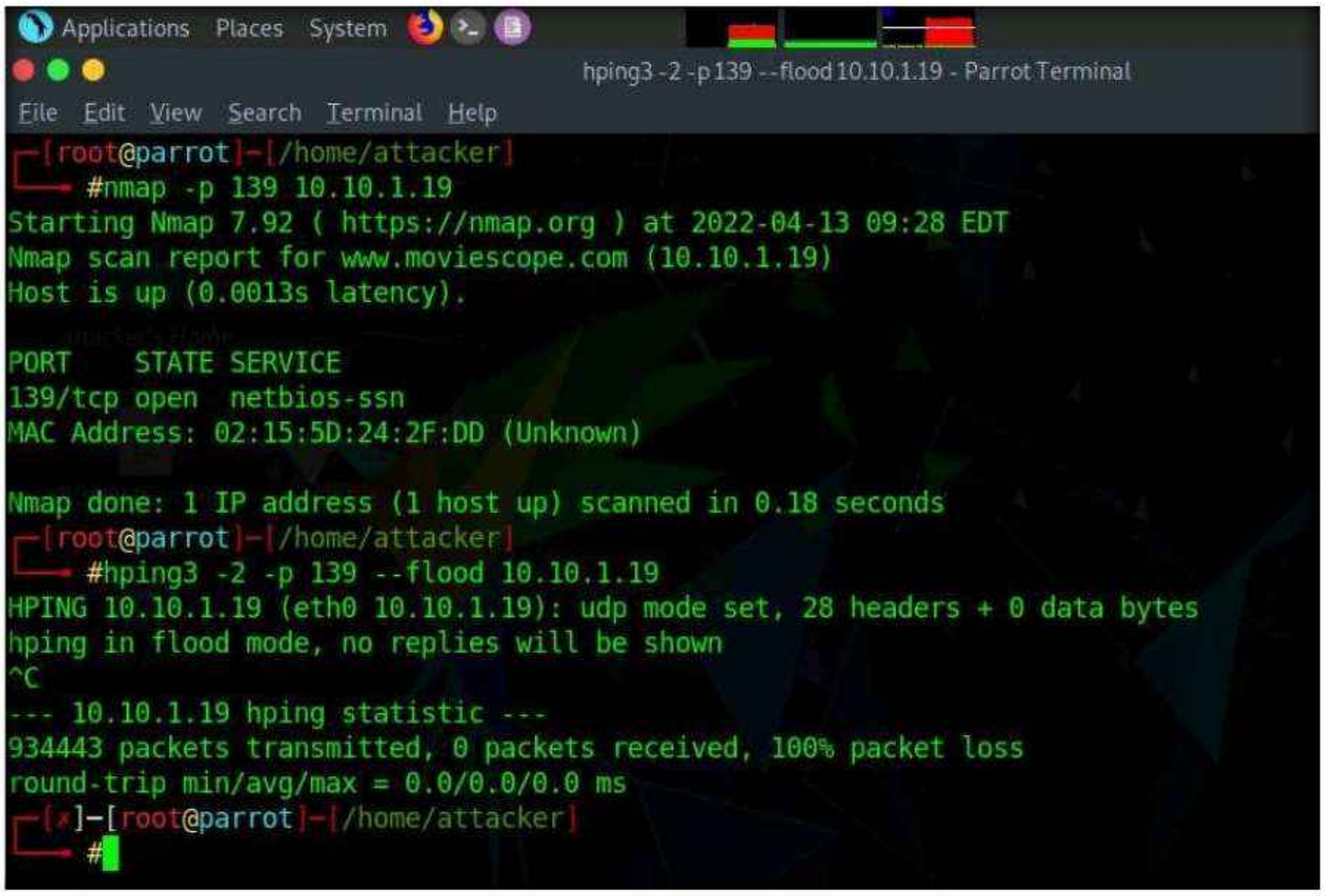
    Note: Here, we have used NetBIOS port 139 to perform a UDP application layer flood attack. Similarly, you can employ other application layer protocols to perform a UDP application layer flood attack on a target network.

    Note: Some of the UDP based application layer protocols that attackers can employ to flood target networks include:

    Note:

    - **CharGEN** (Port 19)
    - **SNMPv2** (Port 161)
    - **QOTD** (Port 17)
    - **RPC** (Port 135)
    - **SSDP** (Port 1900)
    - **CLDAP** (Port 389)
    - **TFTP** (Port 69)

- **NetBIOS** (Port 137,138,139)
- **NTP** (Port 123)
- **Quake Network Protocol** (Port 26000)
- **VoIP** (Port 5060)



36. This concludes the demonstration of how to perform DoS attacks (SYN flooding, PoD attacks, and UDP Application Layer Flood Attacks) on a target host using hping3.
37. Close all open windows and document all the acquired information.

Task 3: Perform a DoS Attack using Raven-storm

Raven-Storm is a DDoS tool for penetration testing that features Layer 3, Layer 4, and Layer 7 attacks. It is written in python3 and is effective and powerful in shutting down hosts and servers. It can be used to perform strong attacks and can be optimized for non typical targets.

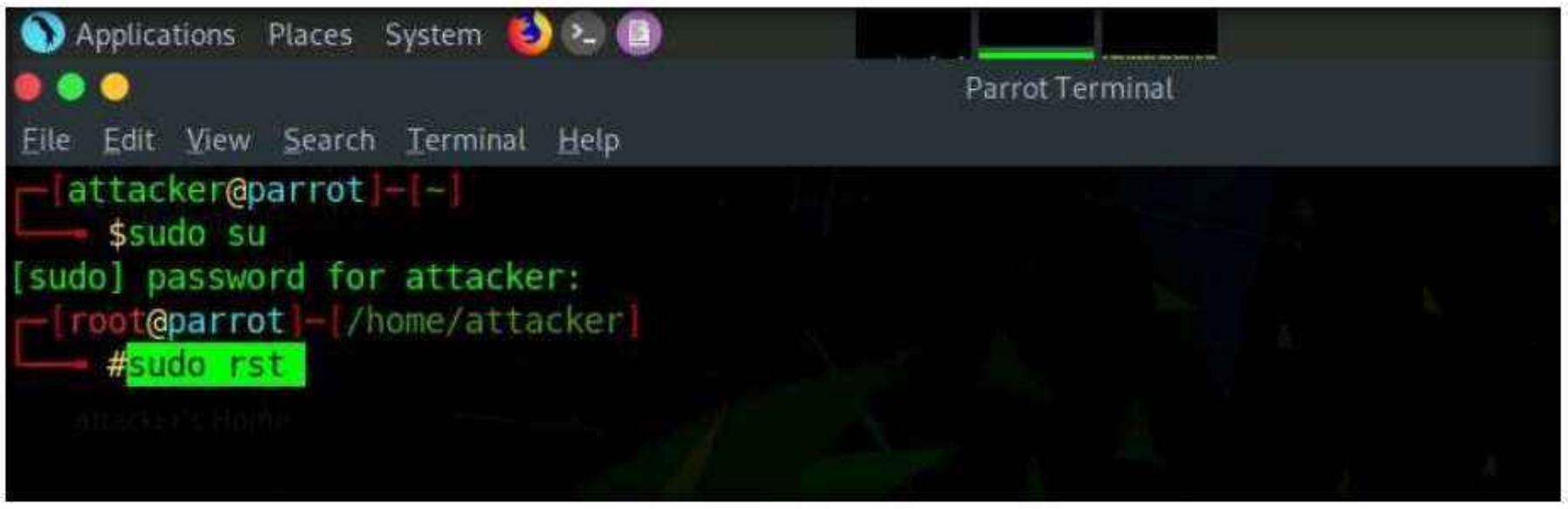
Here, we will use Raven-storm tool to perform a DoS attack.

1. Switch to the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

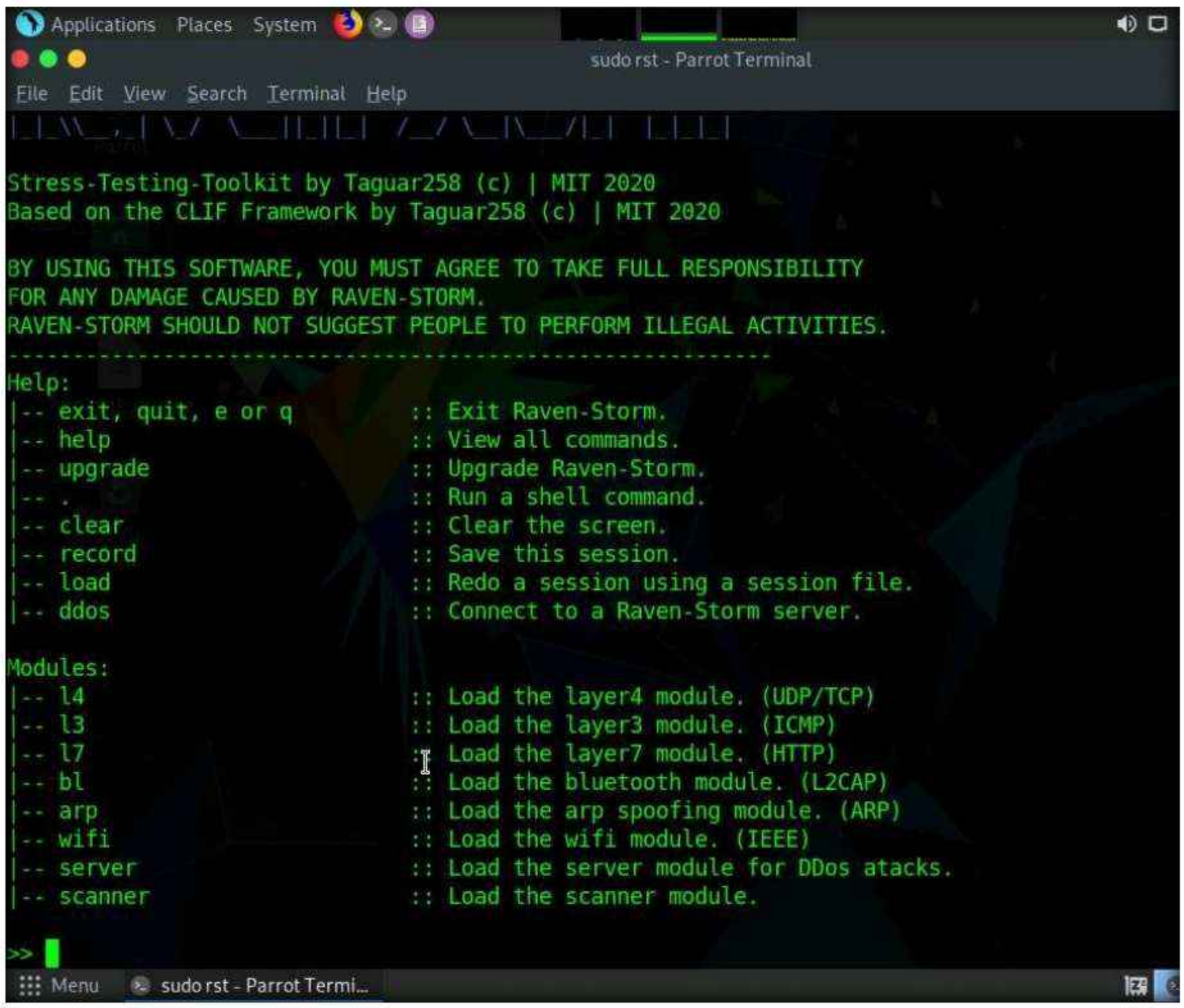
   Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

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

   Note: The password that you type will not be visible.
5. Type **sudo rst** and press **Enter** to start Raven-storm tool.



6. Raven-storm tool initializes, as shown in the screenshot.

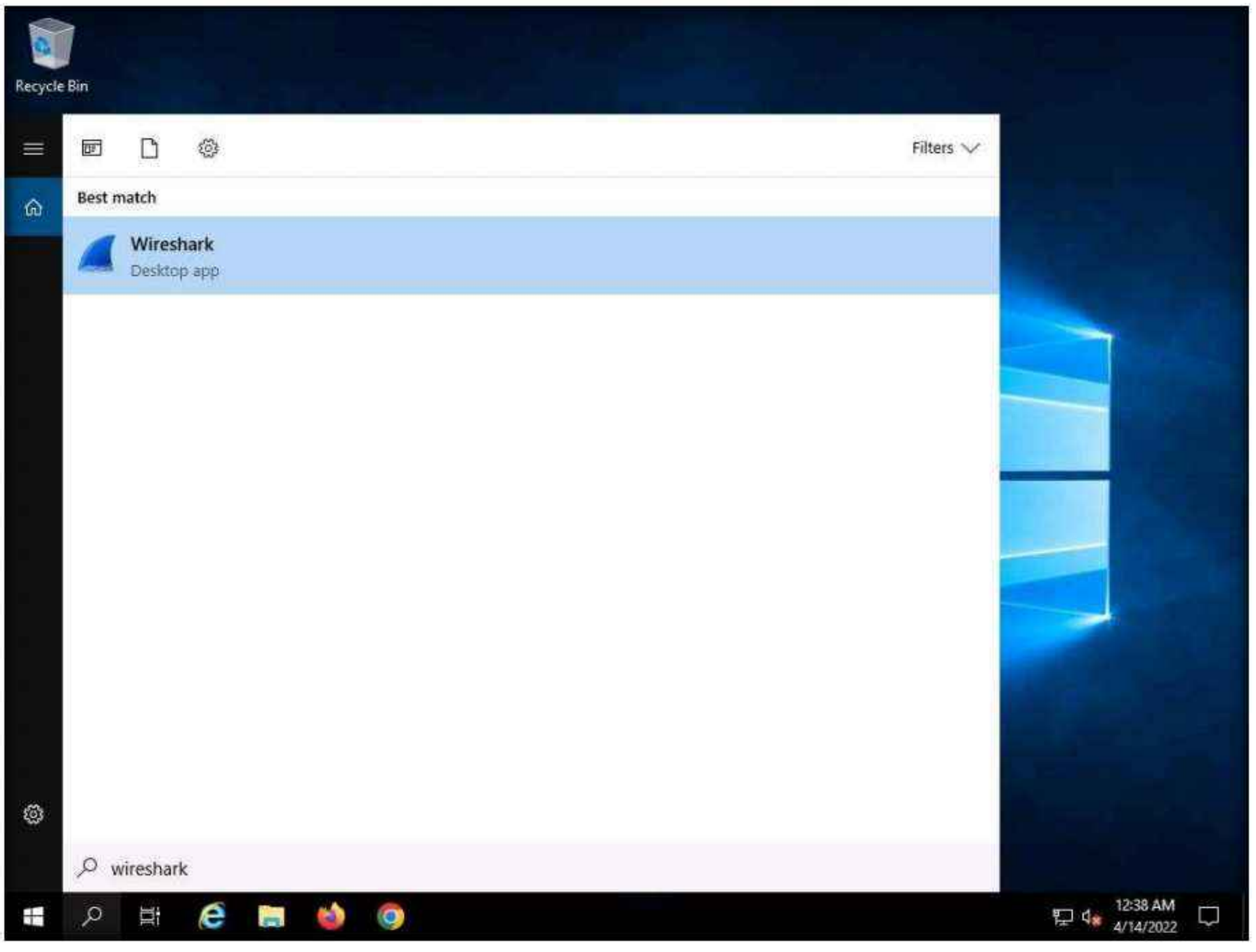


7. Type **l4** and press **Enter** to load **layer4** module (UDP/TCP).

8. Now, switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

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

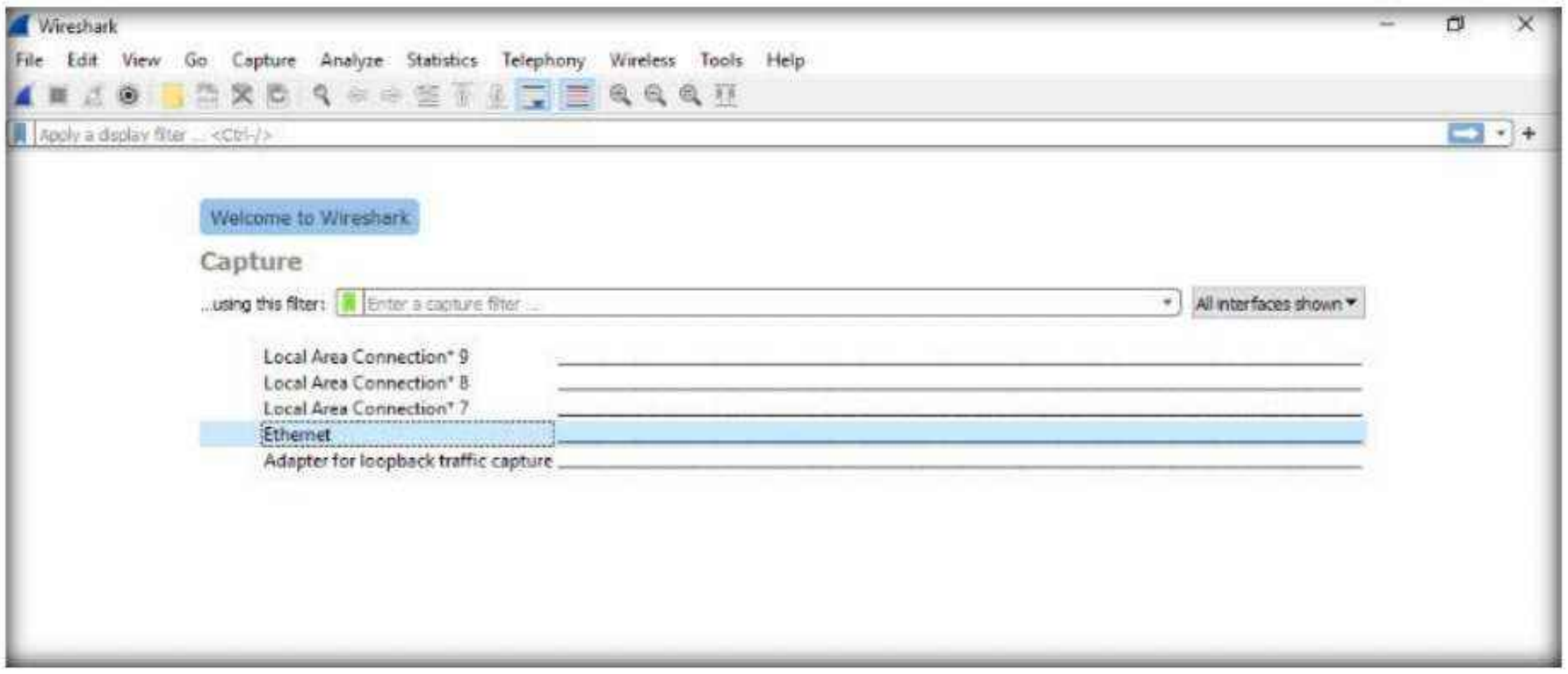
9. In the **Type here to search** field on the **Desktop**, type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.



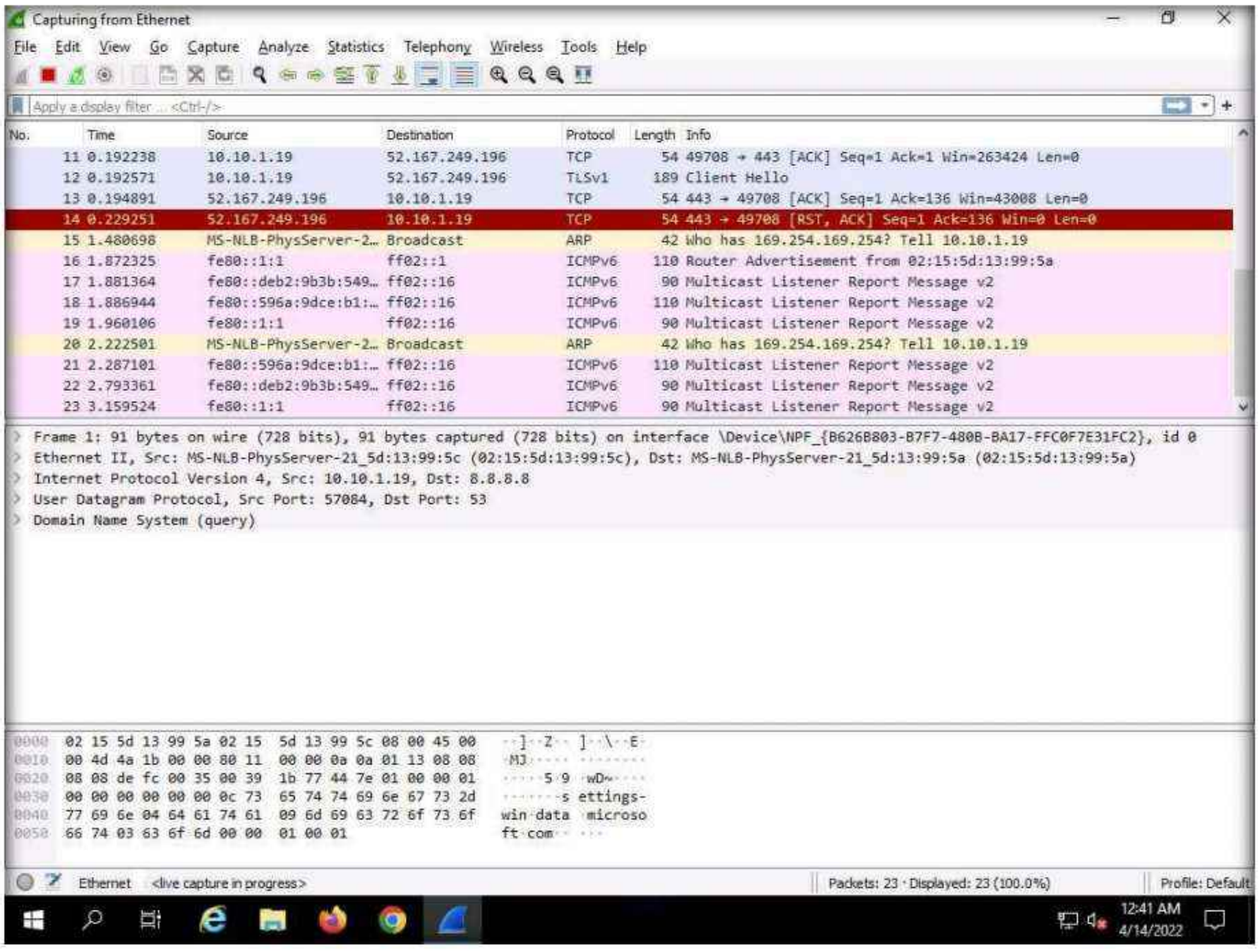
10. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

    Note: The network interface might differ when you perform the task.

Note: If a **Software Update** pop-up appears click on **Remind me later**.

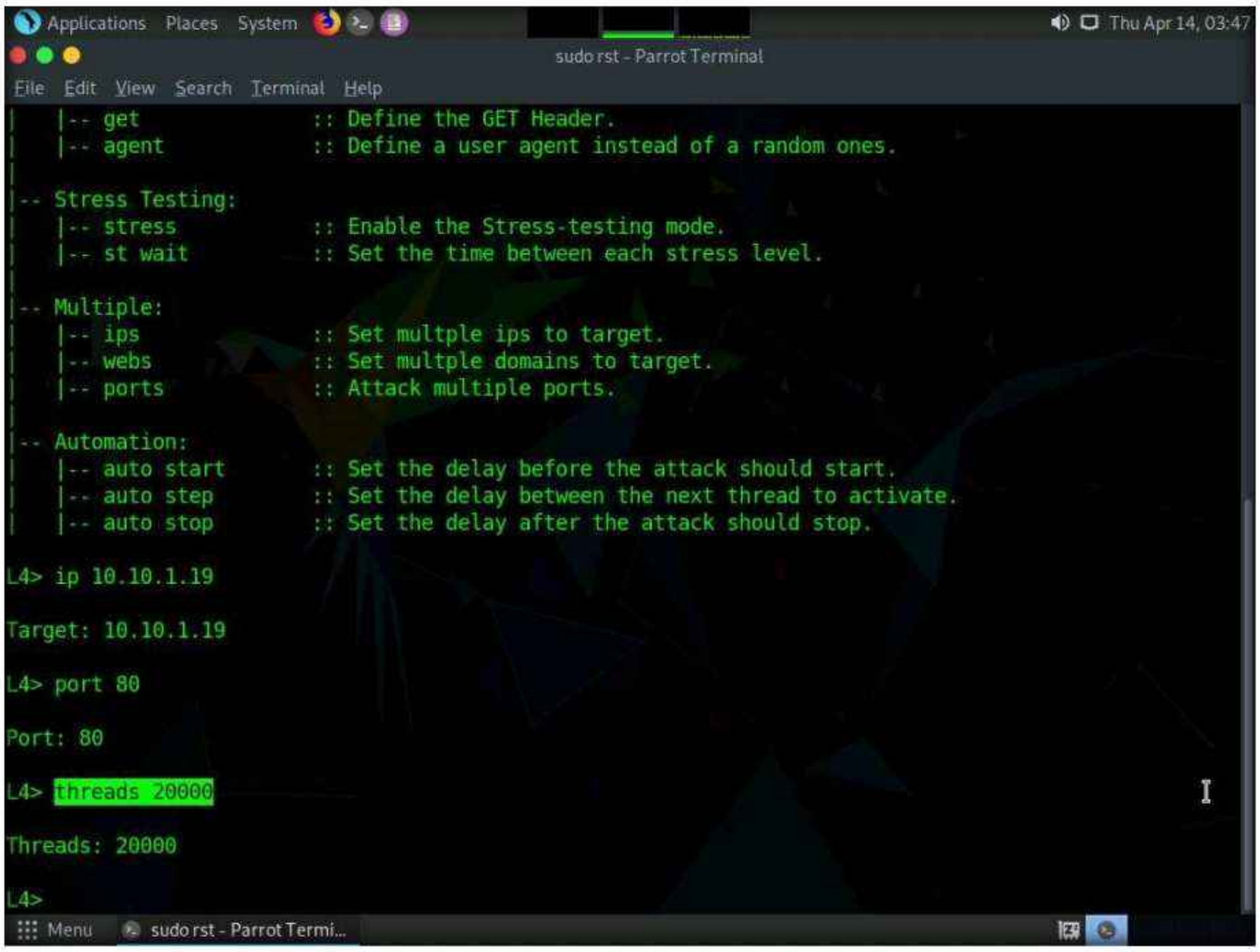


11. **Wireshark** starts capturing the packets; leave it running.



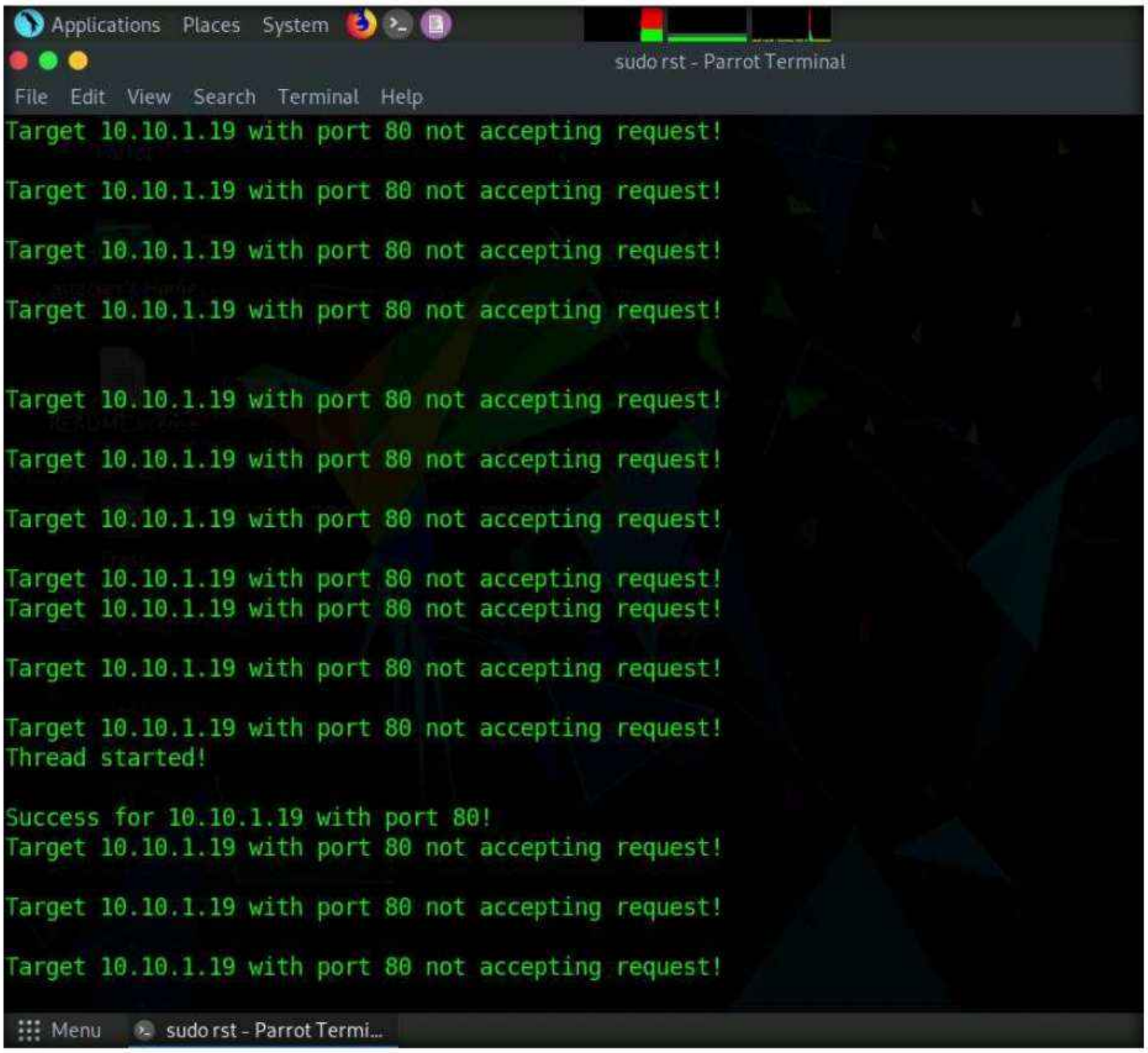
12. Switch to **Parrot Security** virtual machine.

13. In the terminal window, type **ip 10.10.1.19** and press **Enter** to specify the target IP address.
14. Type **port 80** and press **Enter**, to specify the target port.
15. Type **threads 20000** and press **Enter**, to specify number of threads.

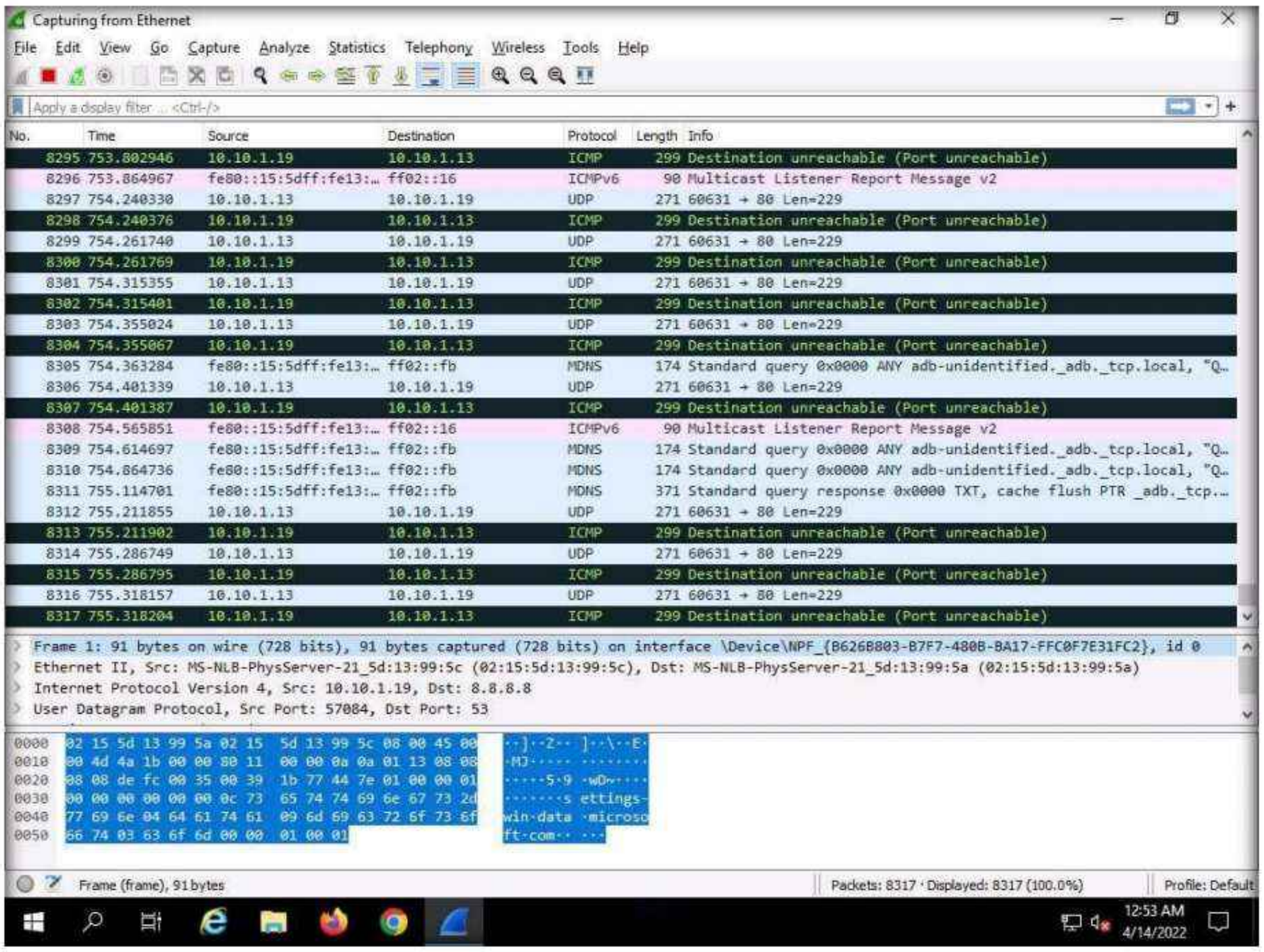


16. Now, in the terminal type **run** and press **Enter**, to start the DoS attack on the target machine.
17. In the **Do you agree to the terms of use? (Y/N)** field, type **Y** and press **Enter**.

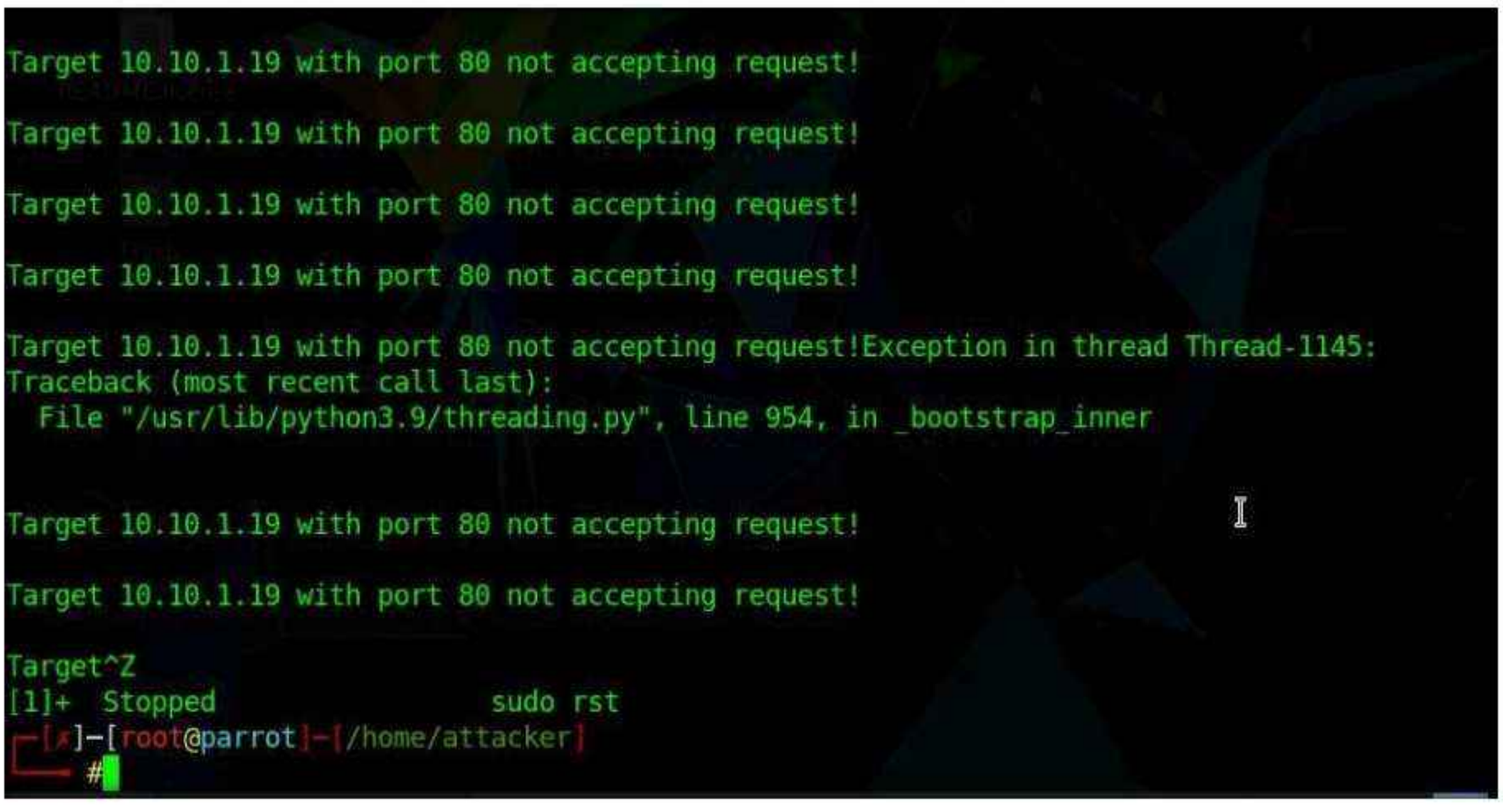
18. Raven-storm starts DoS attack on the target machine (here, **Windows Server 2019**).



19. Switch to **Windows Server 2019** virtual machine.
20. You can observe a large number of packets received from **Parrot Security** machine (**10.10.1.13**).



21. Switch to **Parrot Security** virtual machine and press **ctrl+z** to stop the attack.



22. This concludes the demonstration of a DoS attack using Raven-storm.

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

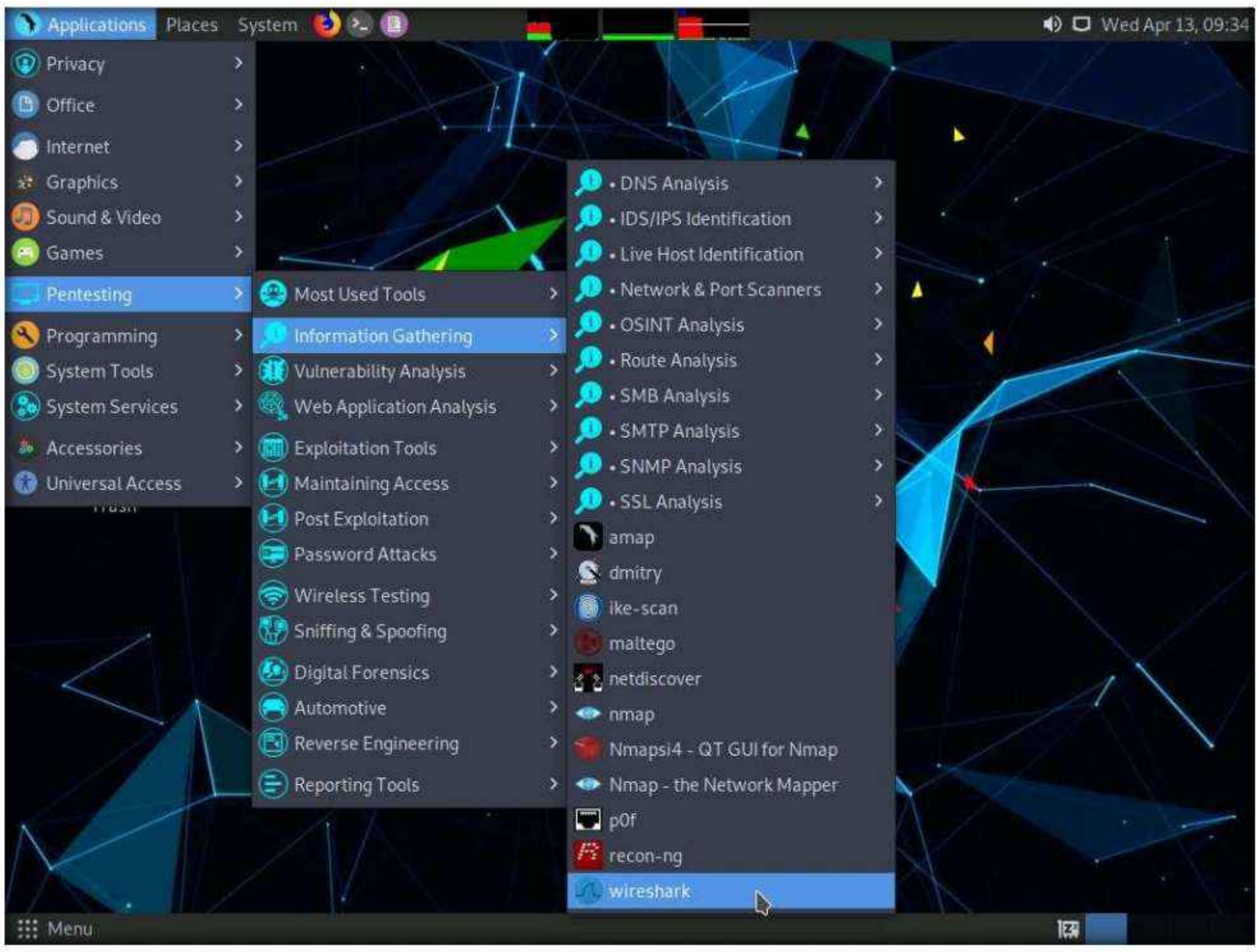
Task 4: Perform a DDoS Attack using HOIC

HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs. It offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of "boosters," which are scripts designed to thwart DDoS countermeasures and increase DoS output.

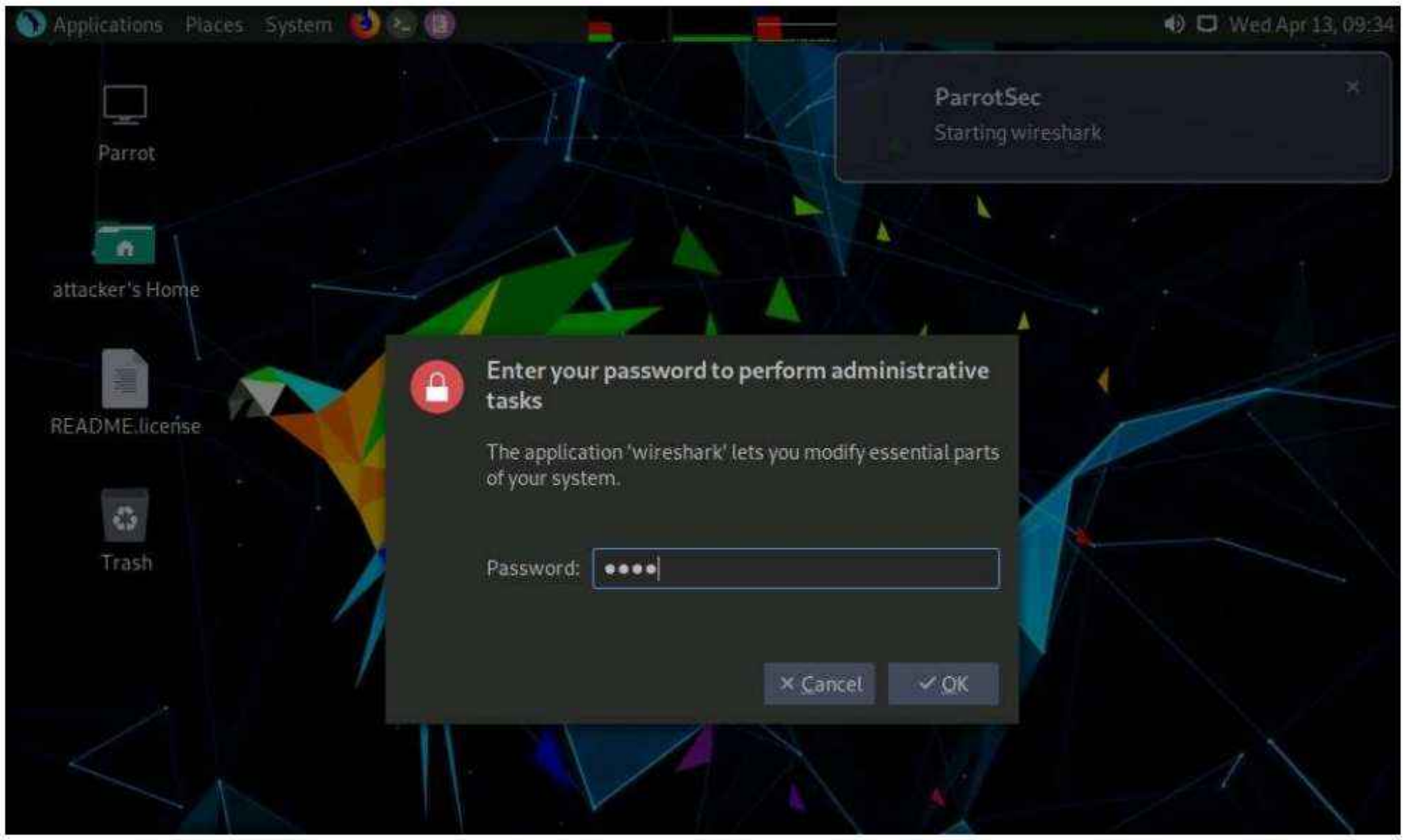
Here, we will use the HOIC tool to perform a DDoS attack on the target machine.

Note: In this task, we will use the **Windows 11**, **Windows Server 2019** and **Windows Server 2022** machines to launch a DDoS attack on the **Parrot Security** machine.

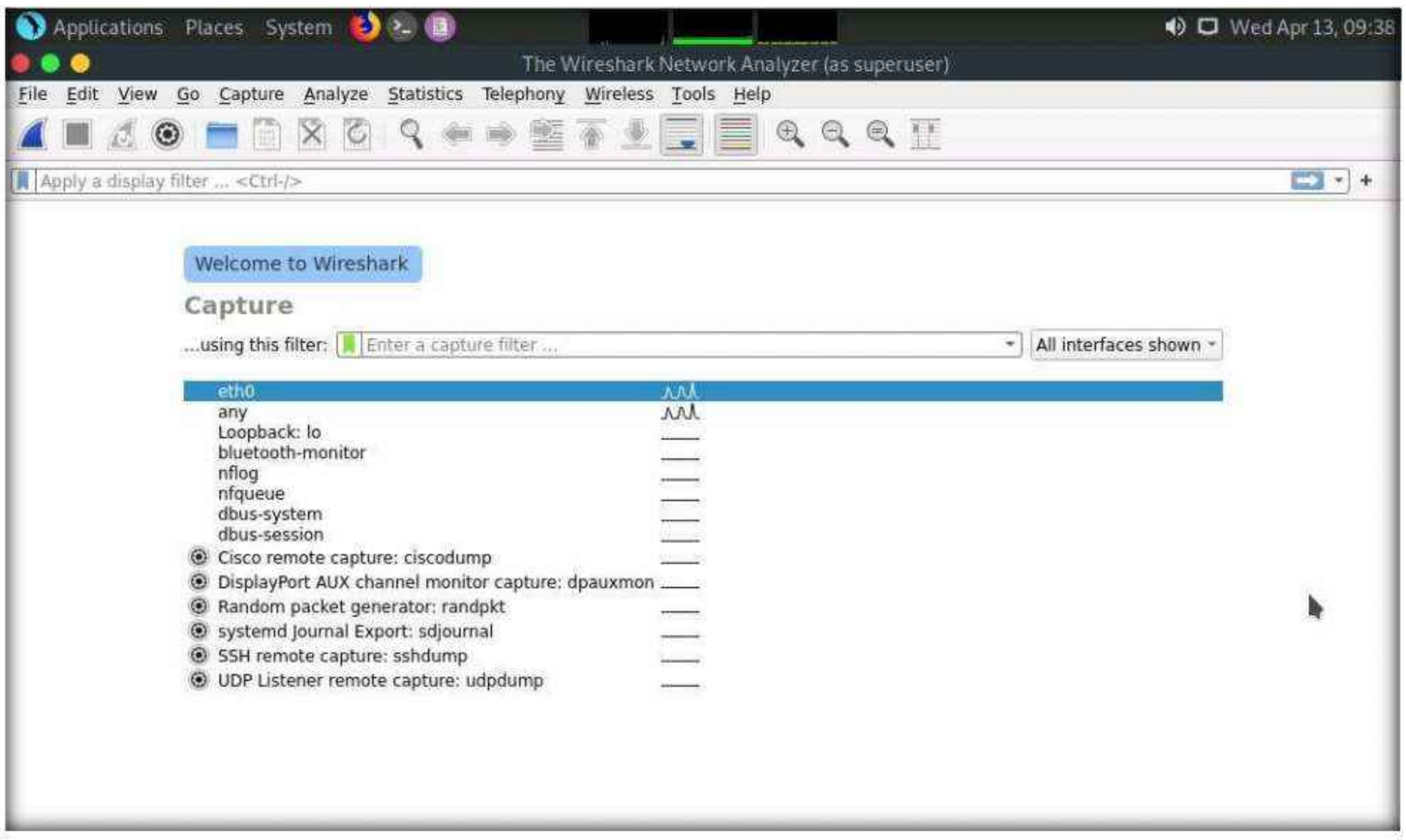
1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.



3. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

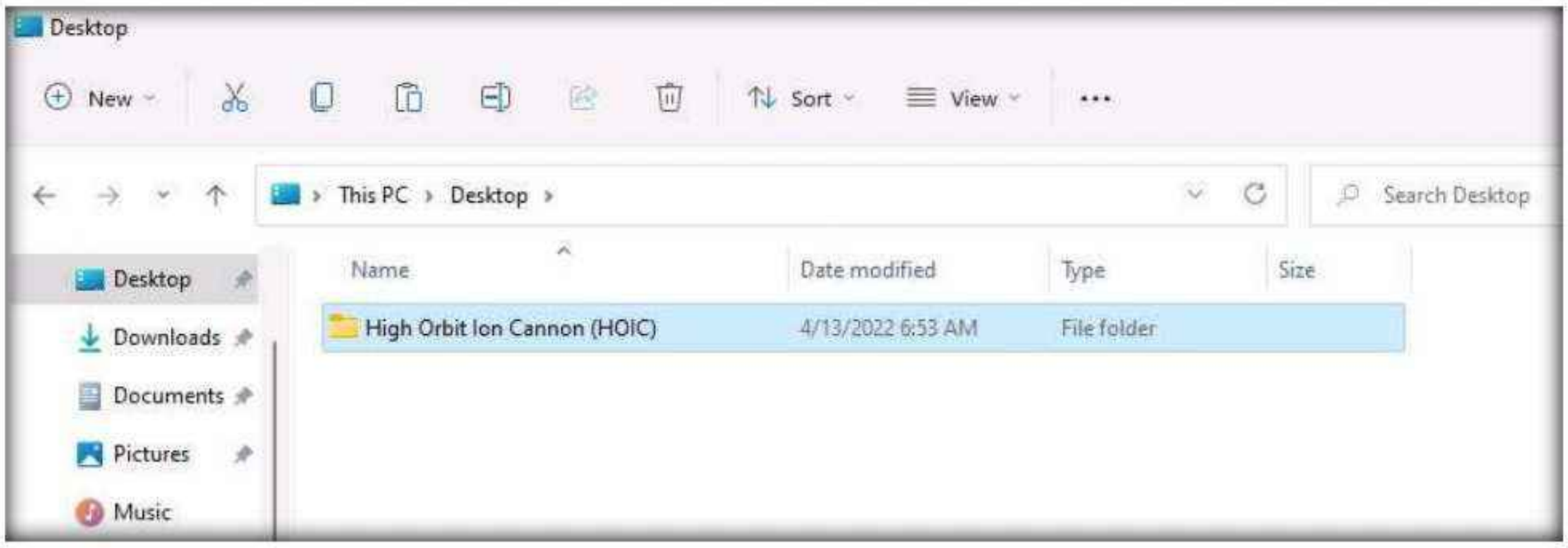


4. The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.



5. Switch to the **Windows 11** virtual machine.
6. Navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.

   Note: To perform the DDoS attack, run this tool from various machines at once. If you run the tool directly from the shared drive in the machines one at a time, errors might occur. To avoid errors, copy the folder **High Orbit Ion Cannon (HOIC)** individually to each machine's **Desktop**, and then run the tool.

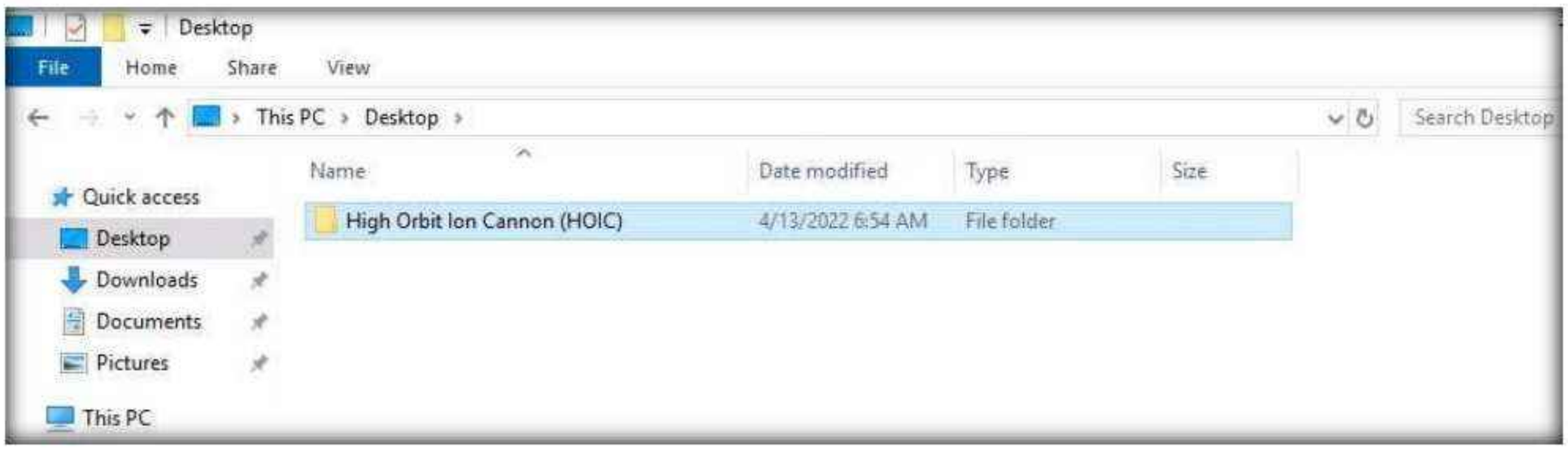


7. Similarly, follow the previous step (**Step #6**) on the **Windows Server 2019** and **Windows Server 2022** virtual machines.

   Note: In **Windows Server 2019**, click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to log in.

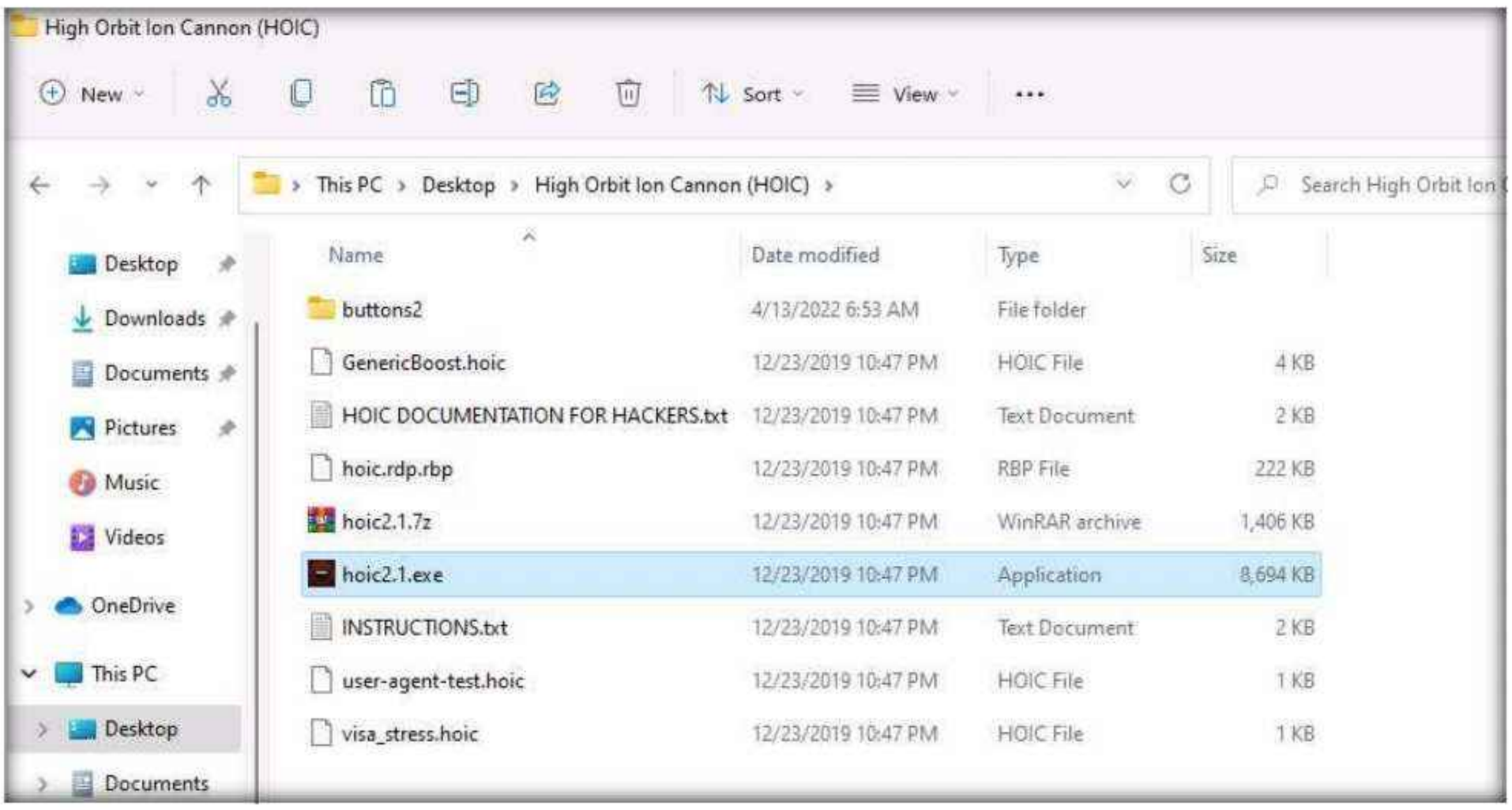
   Note: In **Windows Server 2022**, click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to log in.

   Note: On the **Windows Server 2019** and **Windows Server 2022** machines, the **High Orbit Ion Cannon (HOIC)** folder is located at **Z:\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools.**



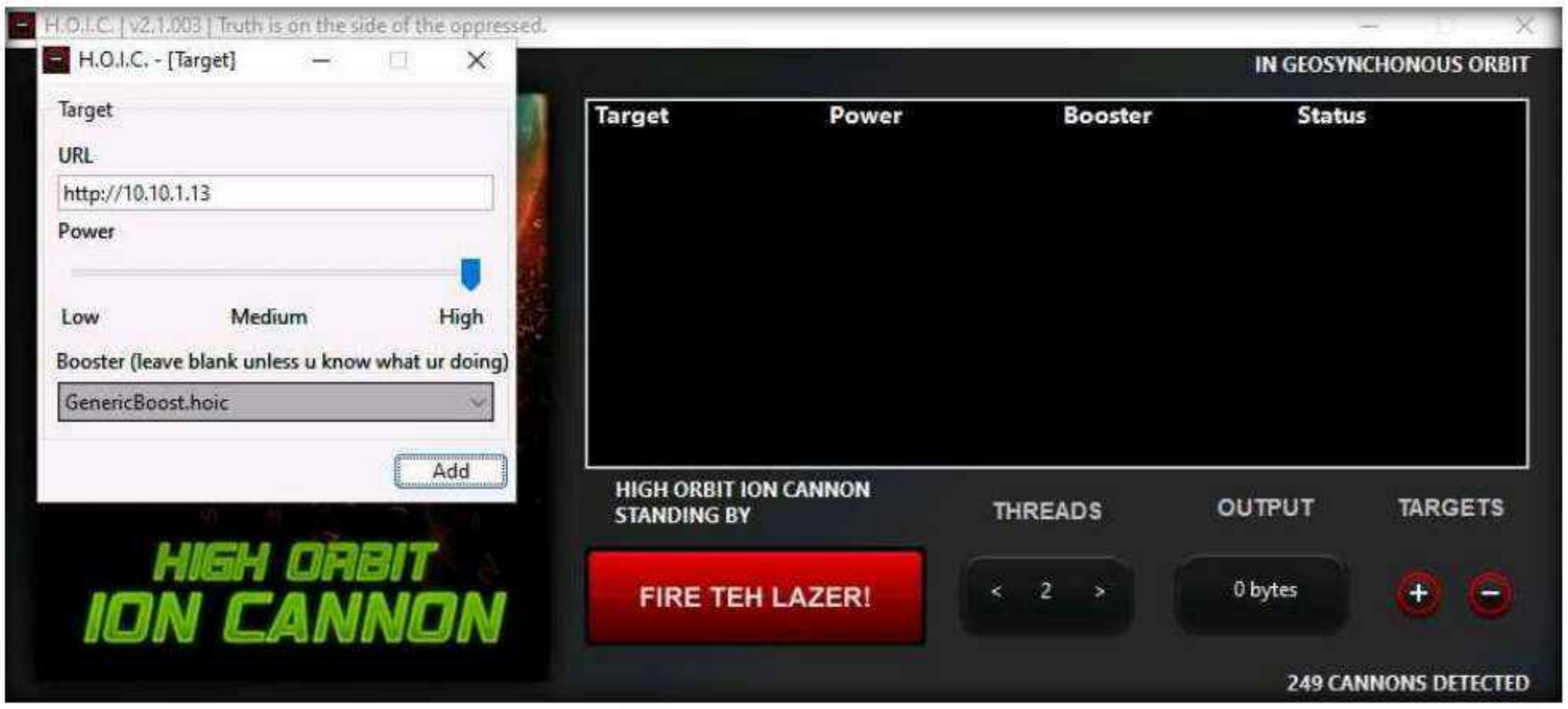
8. Now, switch to the **Window 11** virtual machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**.

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



9. The **HOIC** GUI main window appears; click the "**+**" button below the **TARGETS** section.

10. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.1.13 [Parrot Security]**) in the URL field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list, and click **Add**.

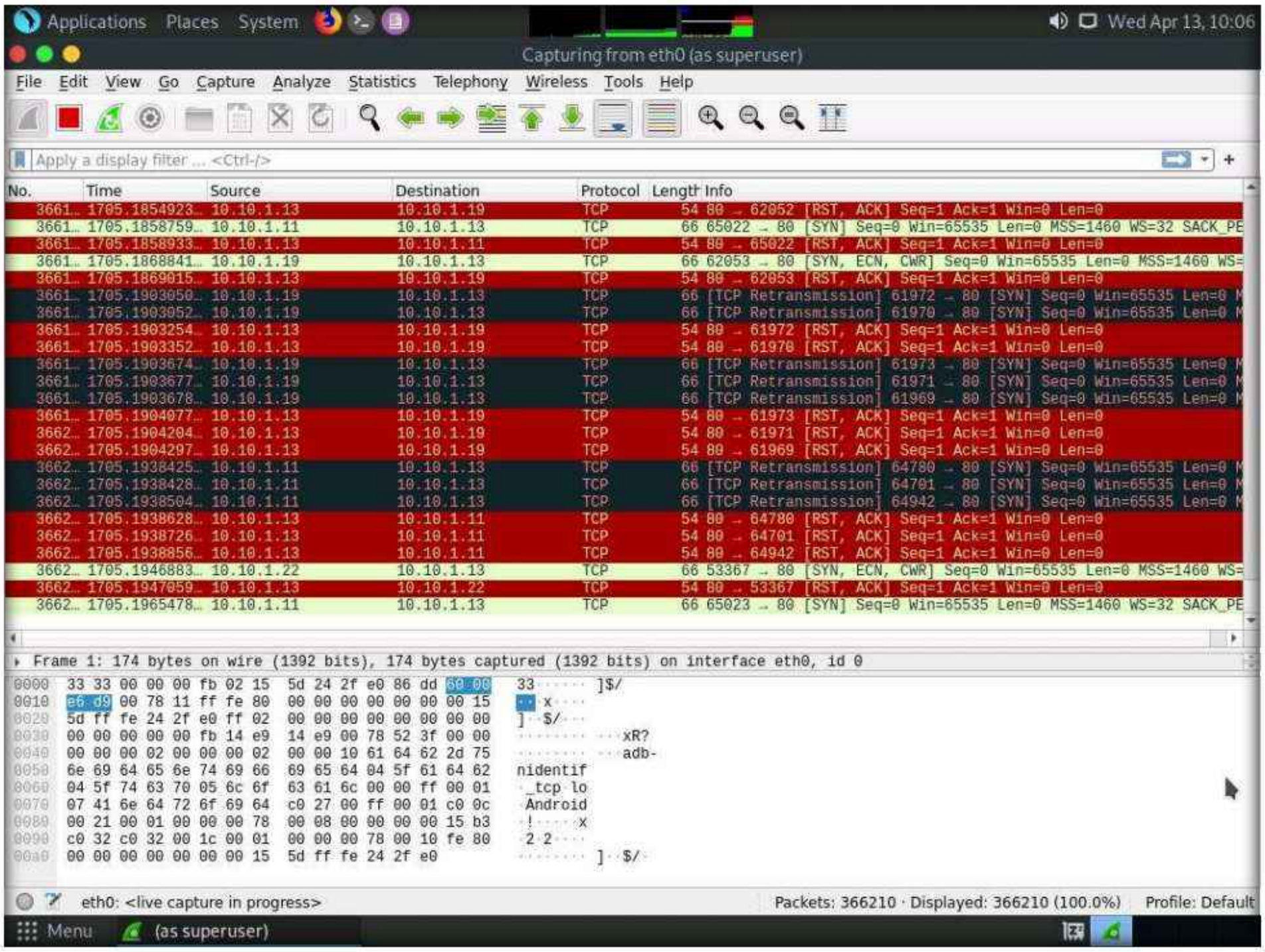


11. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

12. Now, switch to the **Windows Server 2019** and **Windows Server 2022** virtual machines and follow **Steps 8-11** to configure HOIC.
13. Once **HOIC** is configured on all machines, switch to each machine (**Windows 11**, **Windows Server 2019**, and **Windows Server 2022**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target the **Parrot Security** virtual machine.

14. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.

15. Switch to the **Parrot Security** virtual machine.
16. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 11, Windows Server 2019**, and **Windows Server 2022** machines.



17. You can observe that the performance of the machine is slightly affected and that its response is slowing down.

18. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, **Parrot Security**) resources are completely consumed, and the machine is overwhelmed.

    Note: In real-time, a group of hackers operating hundreds or thousands of machines configure this tool on their machines, communicate with each other through IRCs, and simulate the DDoS attack by flooding a target machine or website at the same time. The target is overwhelmed and stops responding to user requests or starts dropping packets coming from legitimate users. The larger the number of attacker machines, the higher the impact of the attack on the target machine or website.

19. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all the attacker machines. Also, close the **Wireshark** window on the **Parrot Security** machine.

20. This concludes the demonstration of how to perform a DDoS attack using HOIC.
21. Close all open windows and document all the acquired information.

Task 5: Perform a DDoS Attack using LOIC

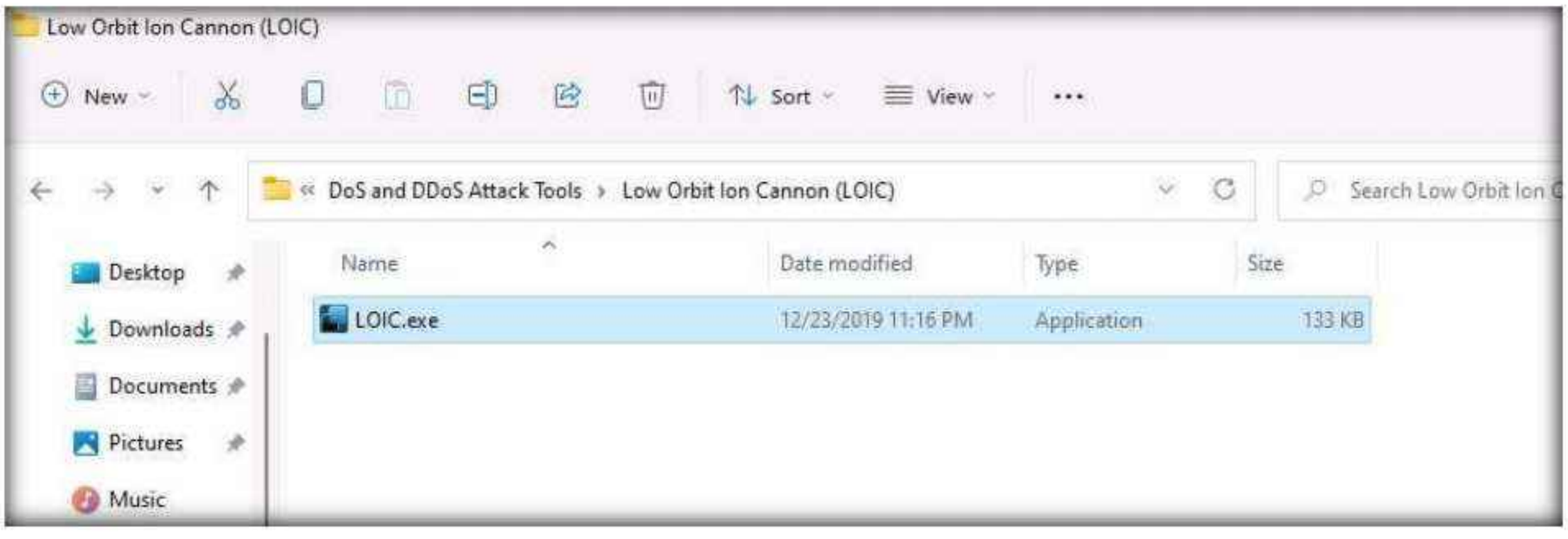
LOIC (Low Orbit Ion Cannon) is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

Here, we will use the LOIC tool to perform a DDoS attack on the target system.

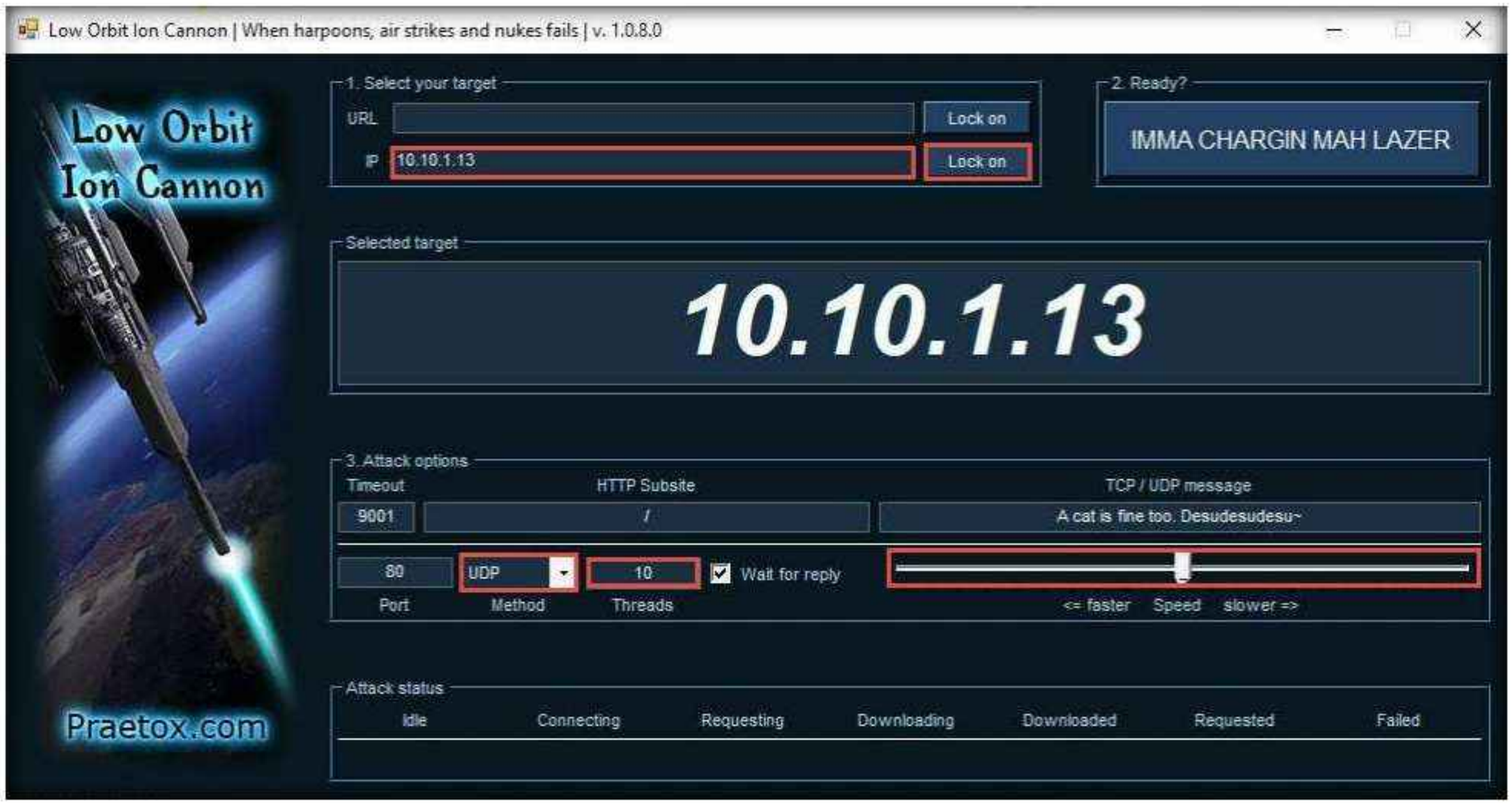
Note: In this task, we will use the **Windows 11**, **Windows Server 2019**, and **Windows Server 2022** machines to launch a DDoS attack on the **Parrot Security** machine.

1. Switch to the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

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



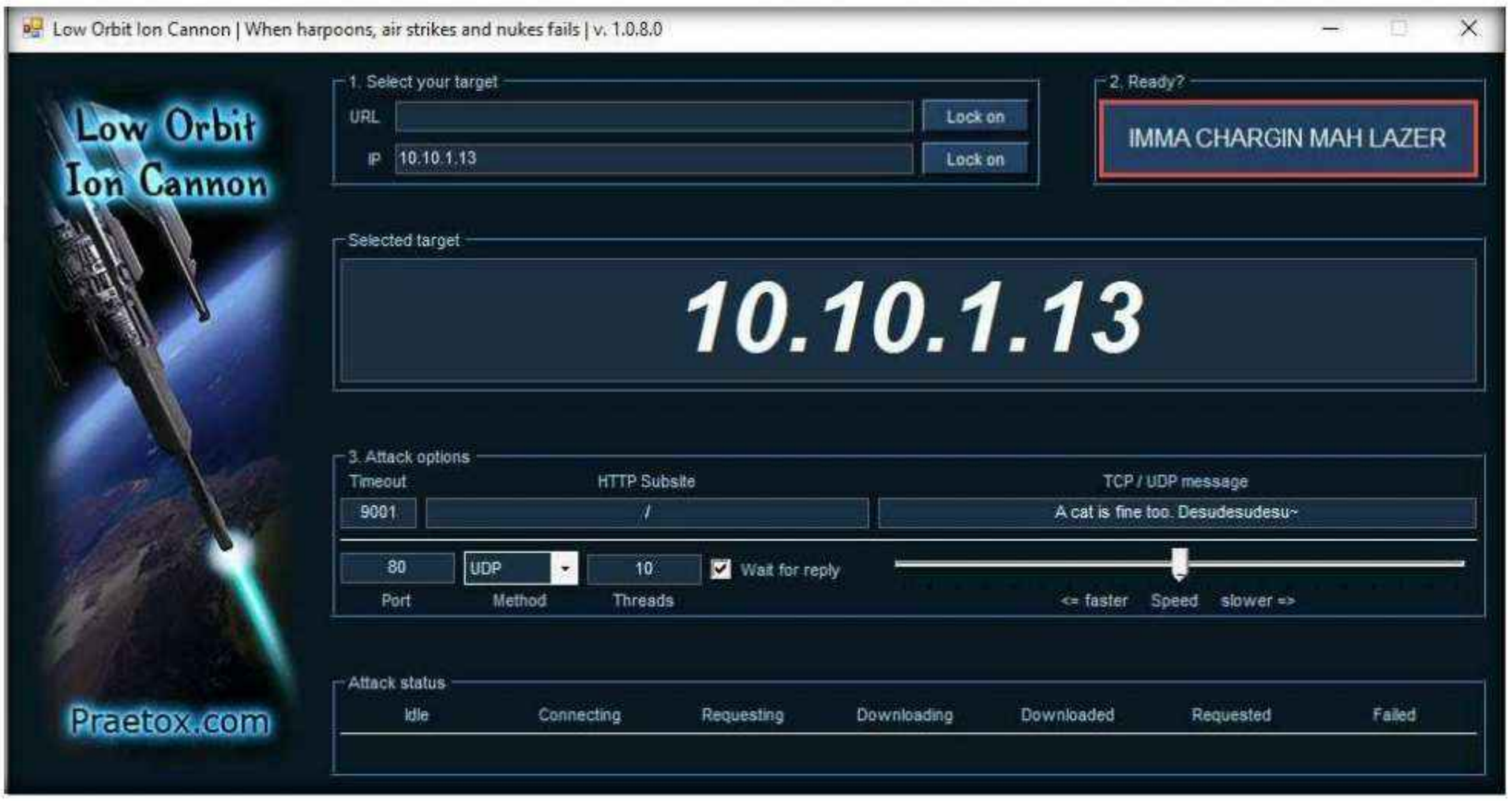
2. The **Low Orbit Ion Cannon** main window appears.
3. Perform the following settings:
   - Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.1.13**), and then click the **Lock on** button to add the target devices.
   - Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **10** under the **Threads** field. Slide the power bar to the middle.



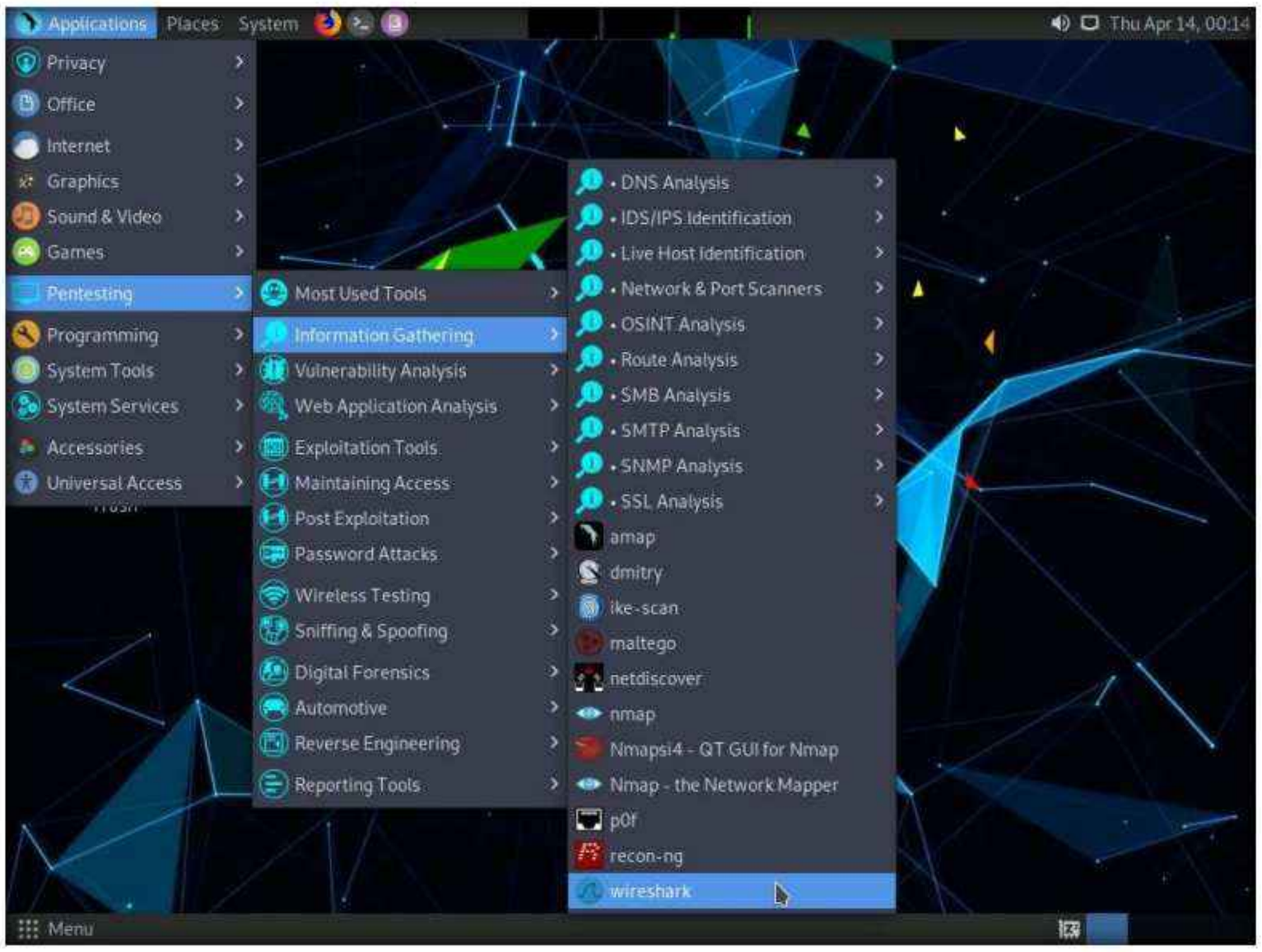
4. Now, switch to the **Windows Server 2019** and **Windows Server 2022** virtual machines and follow **Steps 1 - 3** to launch LOIC and configure it.

   Note: On the **Windows Server 2019** and **Windows Server 2022** virtual machines, LOIC is located at **Z:\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC).**

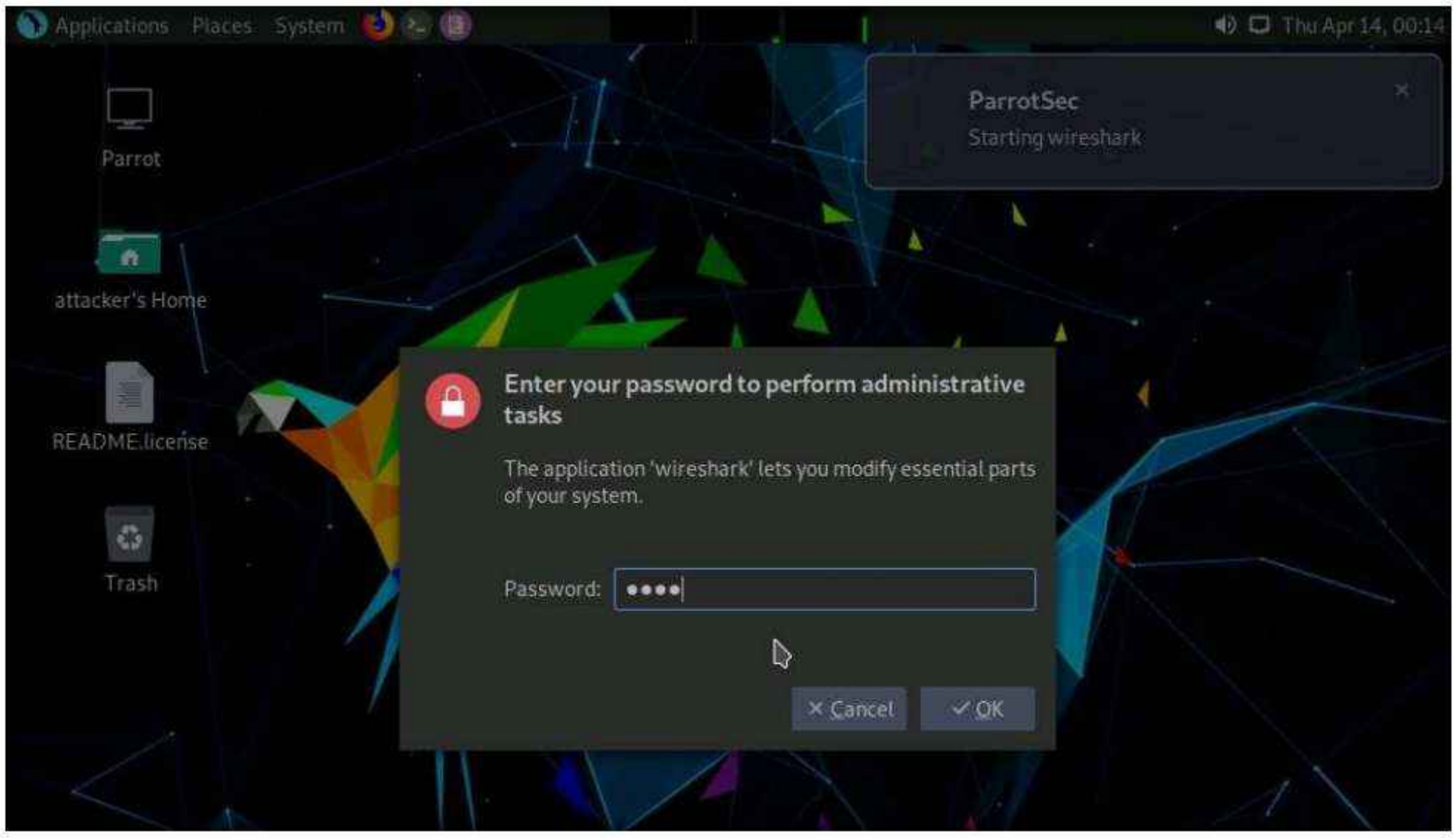
5. Once **LOIC** is configured on all machines, switch to each machine (**Windows 11, Windows Server 2019**, and **Windows Server 2022**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Parrot Security** machine.



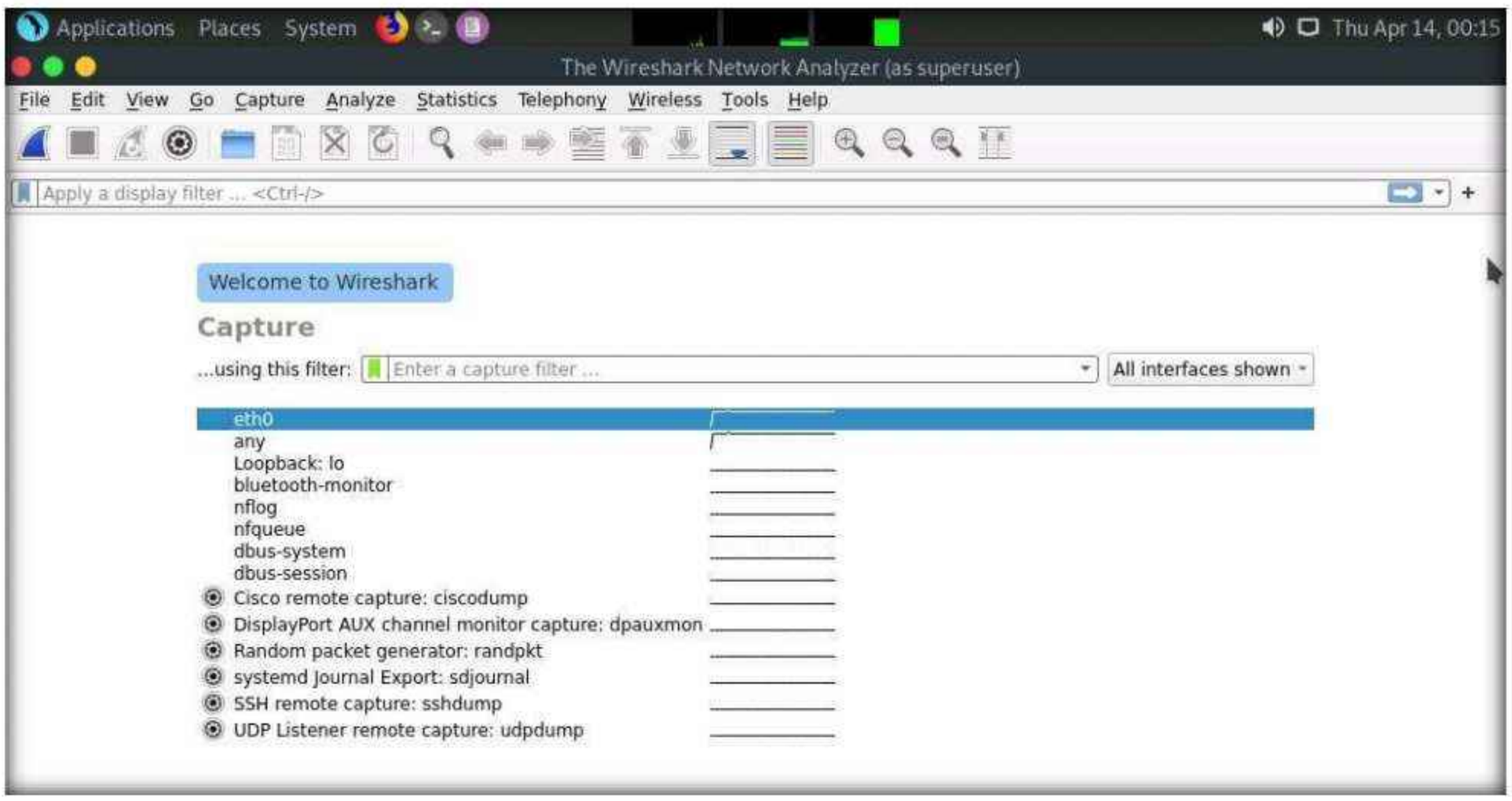
6. Switch to the **Parrot Security** virtual machine.
7. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



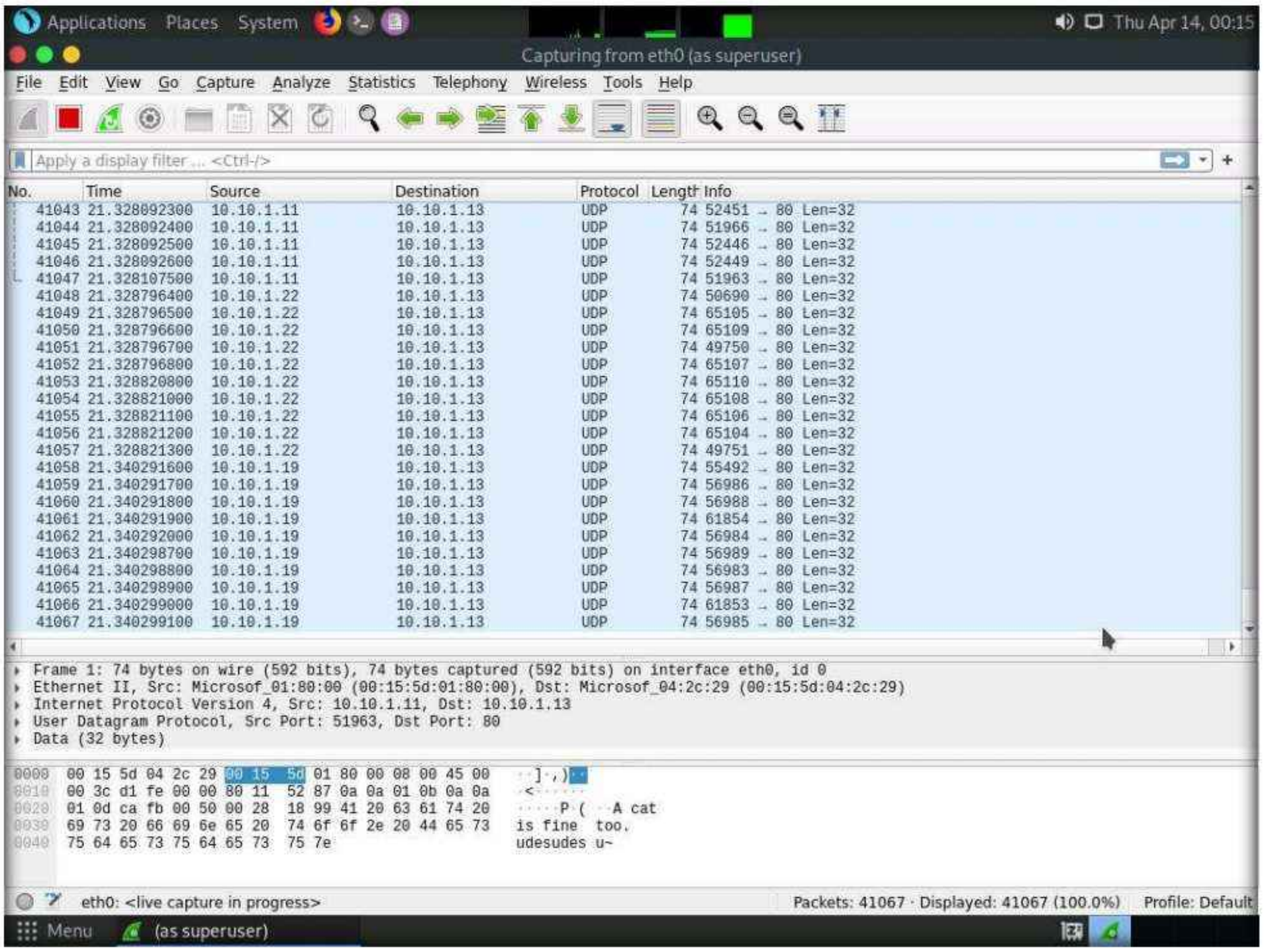
8. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



9. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.

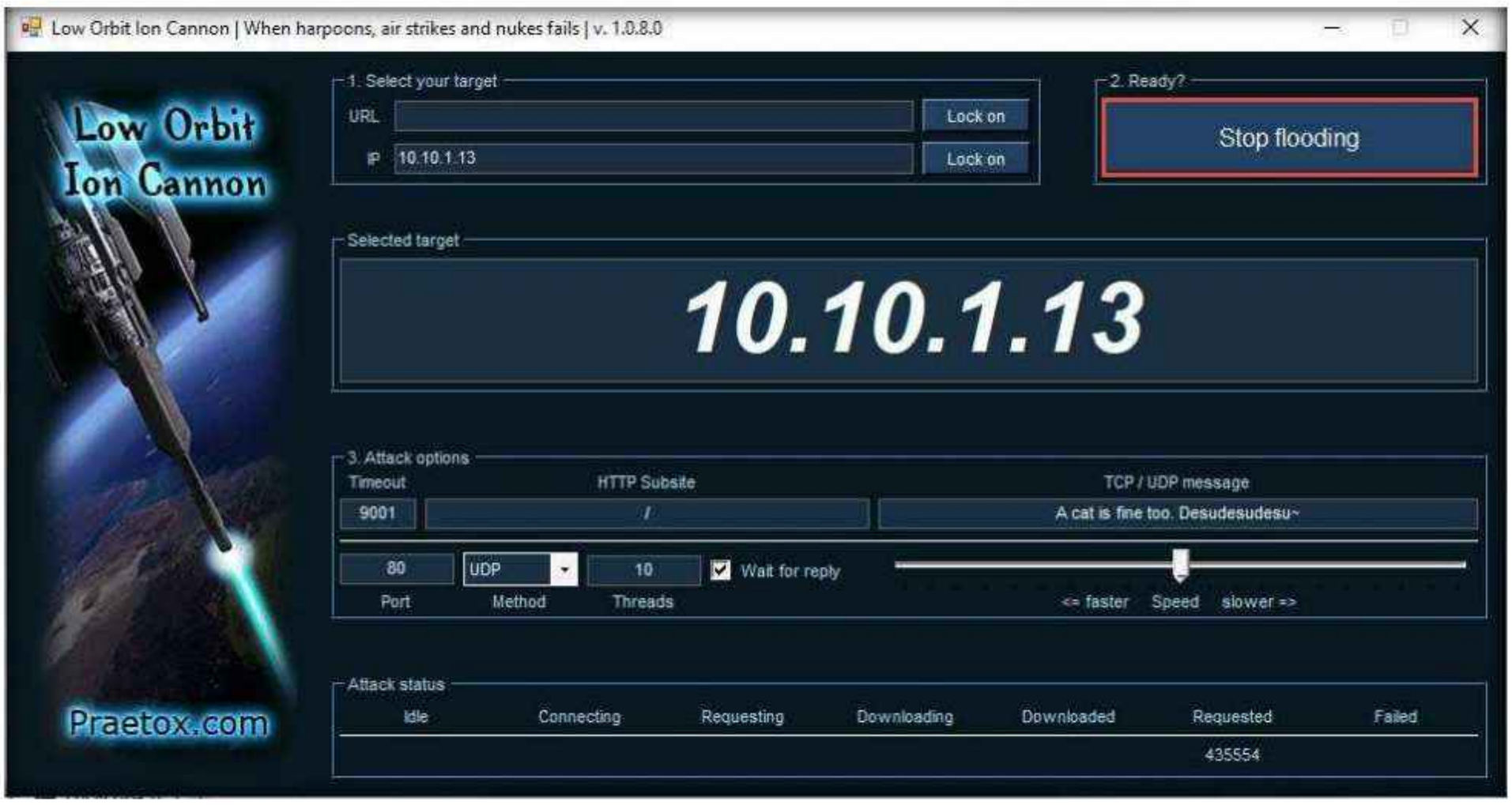


10. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 11, Windows Server 2019**, and **Windows Server 2022** machines.



11. Leave the machine intact for 5–10 minutes, and then open it again. You will observe that the performance of the machine is slightly affected and that its response is slowing down.

12. On completion of the task, click **Stop flooding**, and then close the LOIC window on all the attacker machines.



13. This concludes the demonstration of how to perform a DDoS attack using LOIC.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11**, **Windows Server 2019**, **Windows Server 2022** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 2

Detect and Protect Against DoS and DDoS Attacks

DoS and DDoS attack detection techniques are based on identifying and discriminating between illegitimate traffic increases and flash events from legitimate packet traffic.

Lab Scenario

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

As a professional ethical hacker or pen tester, you must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

Lab Objectives

- Detect and protect against DDoS attacks using Anti DDoS Guardian

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of DoS and DDoS Attack Detection

Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from the legitimate packet traffic.

The following are the three types of detection techniques:

- **Activity Profiling**: Profiles based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information
- **Sequential Change-point Detection**: Filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate over time
- **Wavelet-based Signal Analysis**: Analyzes network traffic in terms of spectral components

Lab Tasks

Task 1: Detect and Protect Against DDoS Attacks using Anti DDoS Guardian

---

Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

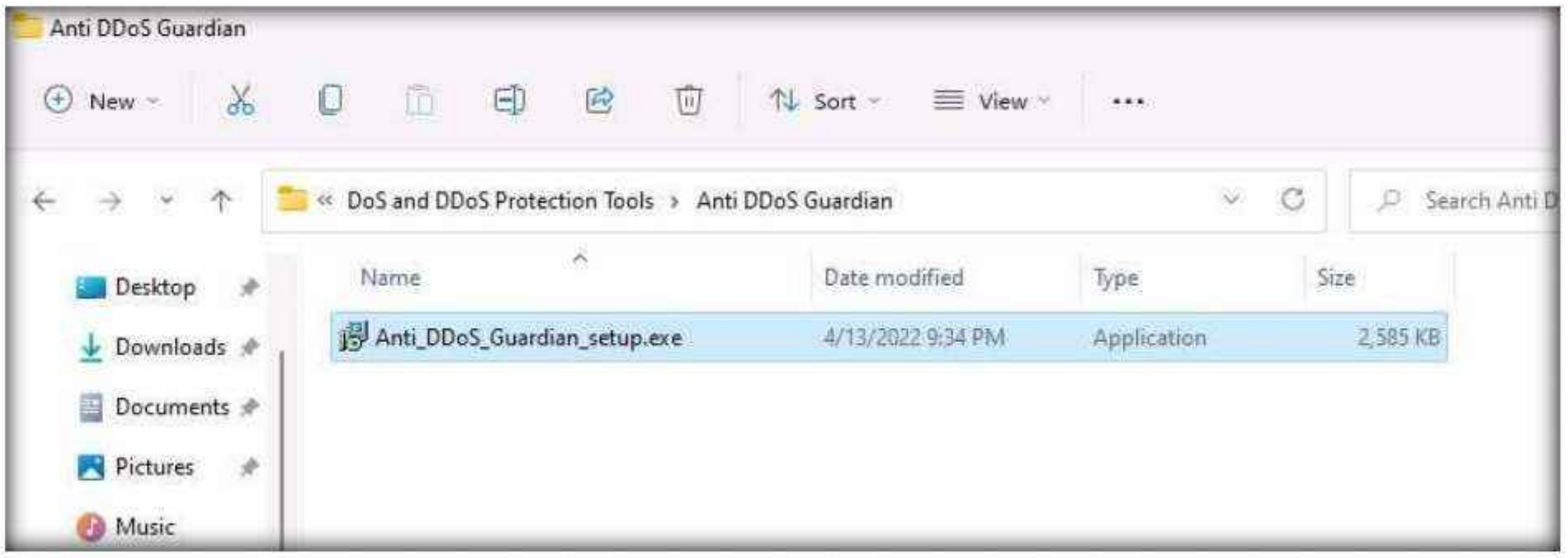
Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian.

Note: In this task, we will use the **Windows Server 2019** and **Windows Server 2022** machines to perform a DDoS attack on the target system, **Windows 11**.

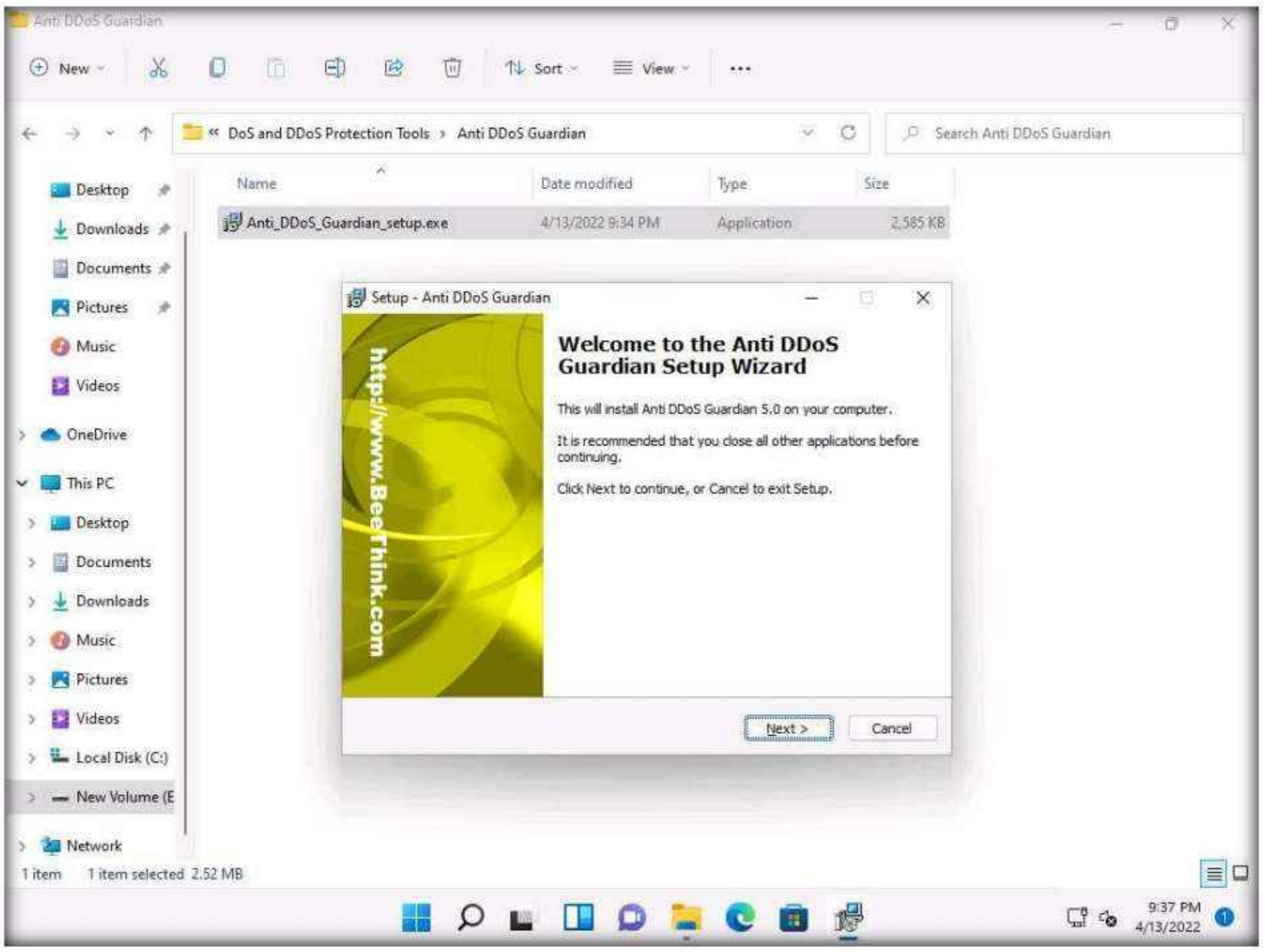
1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. Login with Username: **Admin** and Password: **Pa$$w0rd**.
3. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double click **Anti_DDoS_Guardian_setup.exe.**

Note: If a **User Account Control** pop-up appears, click **Yes**.

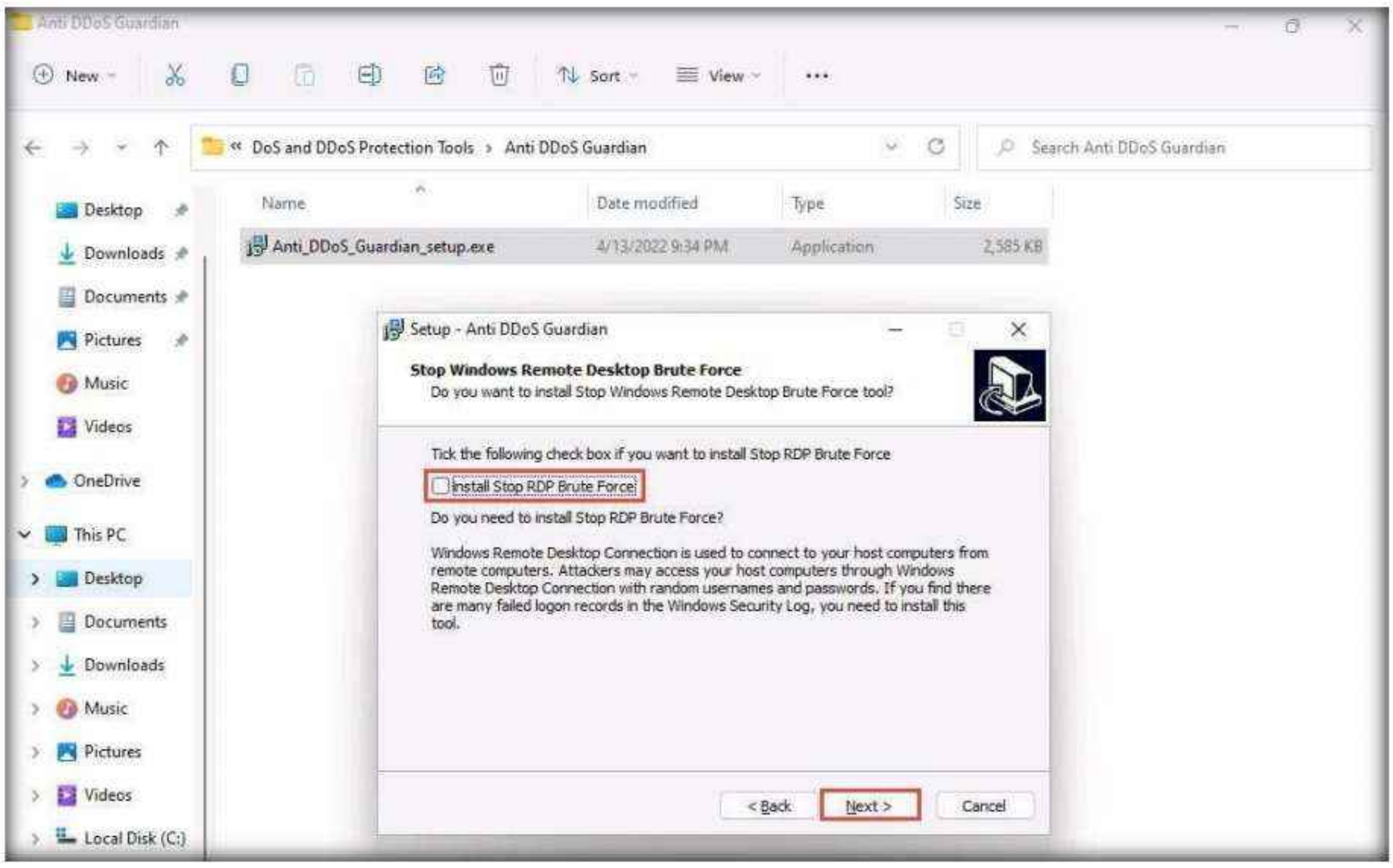
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



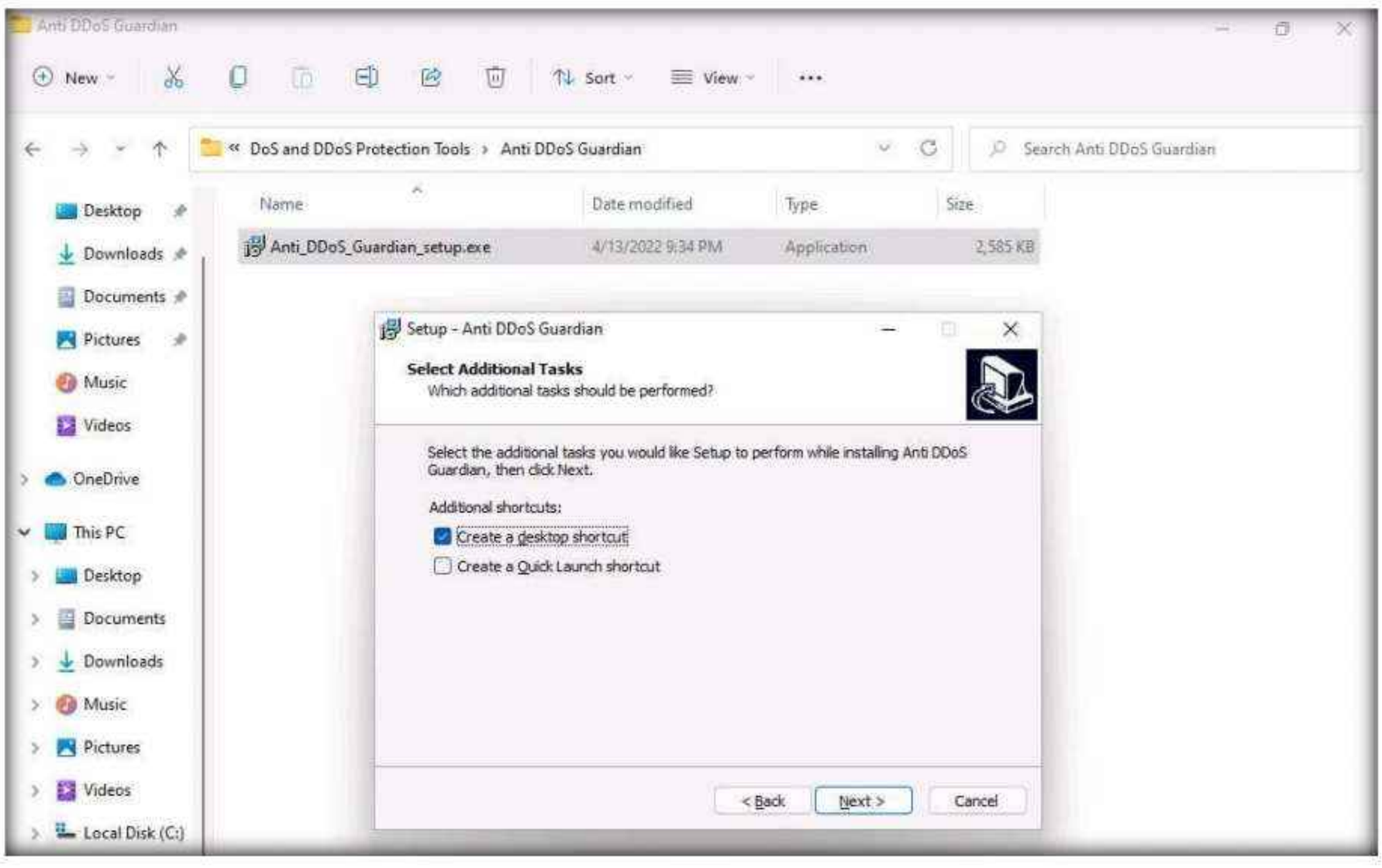
4. The **Setup - Anti DDoS Guardian window** appears; click **Next**. Follow the wizard-driven installation steps to install the application.



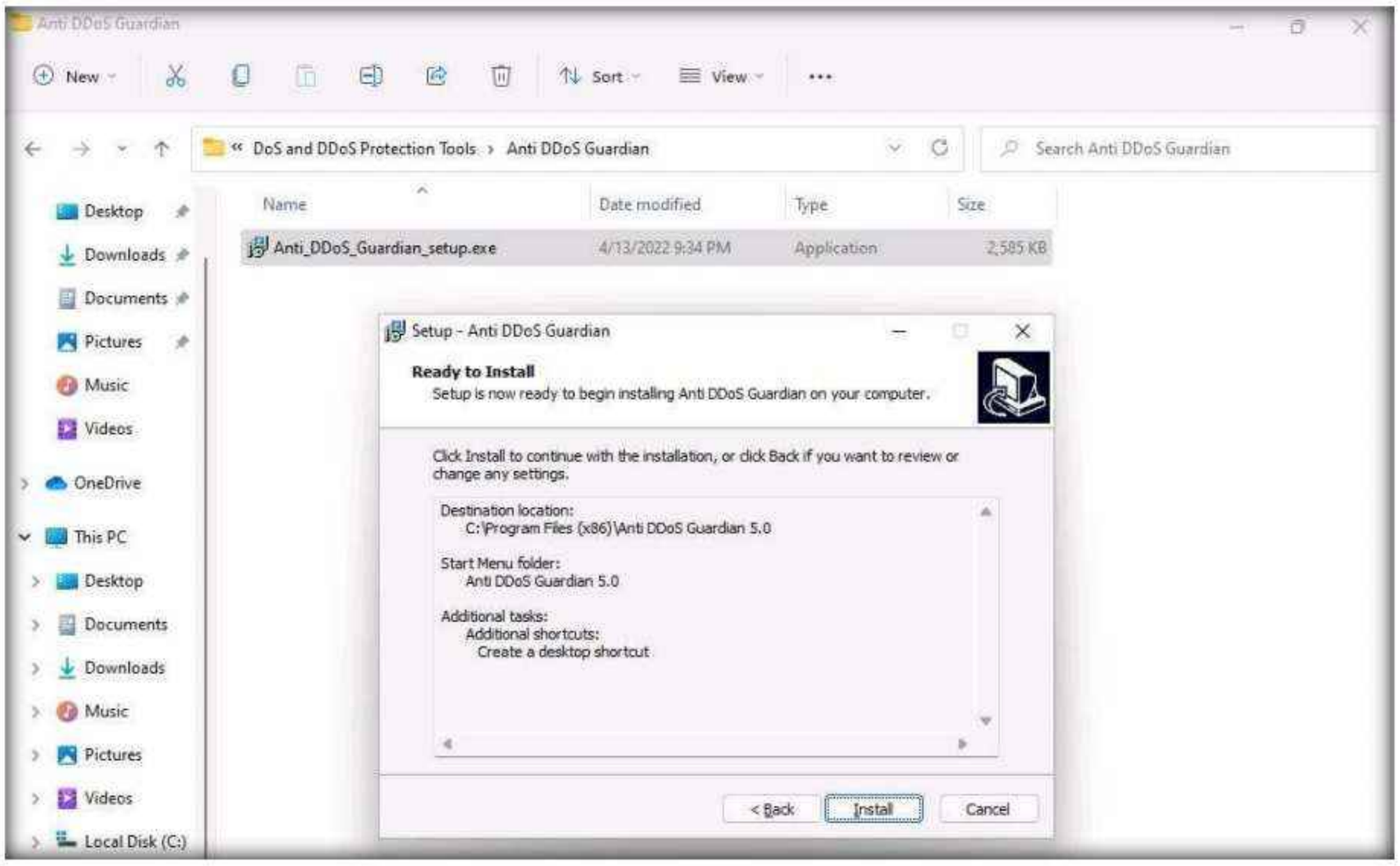
5. In the **Stop Windows Remote Desktop Brute Force** wizard, uncheck the **install Stop RDP Brute Force** option, and click **Next**.



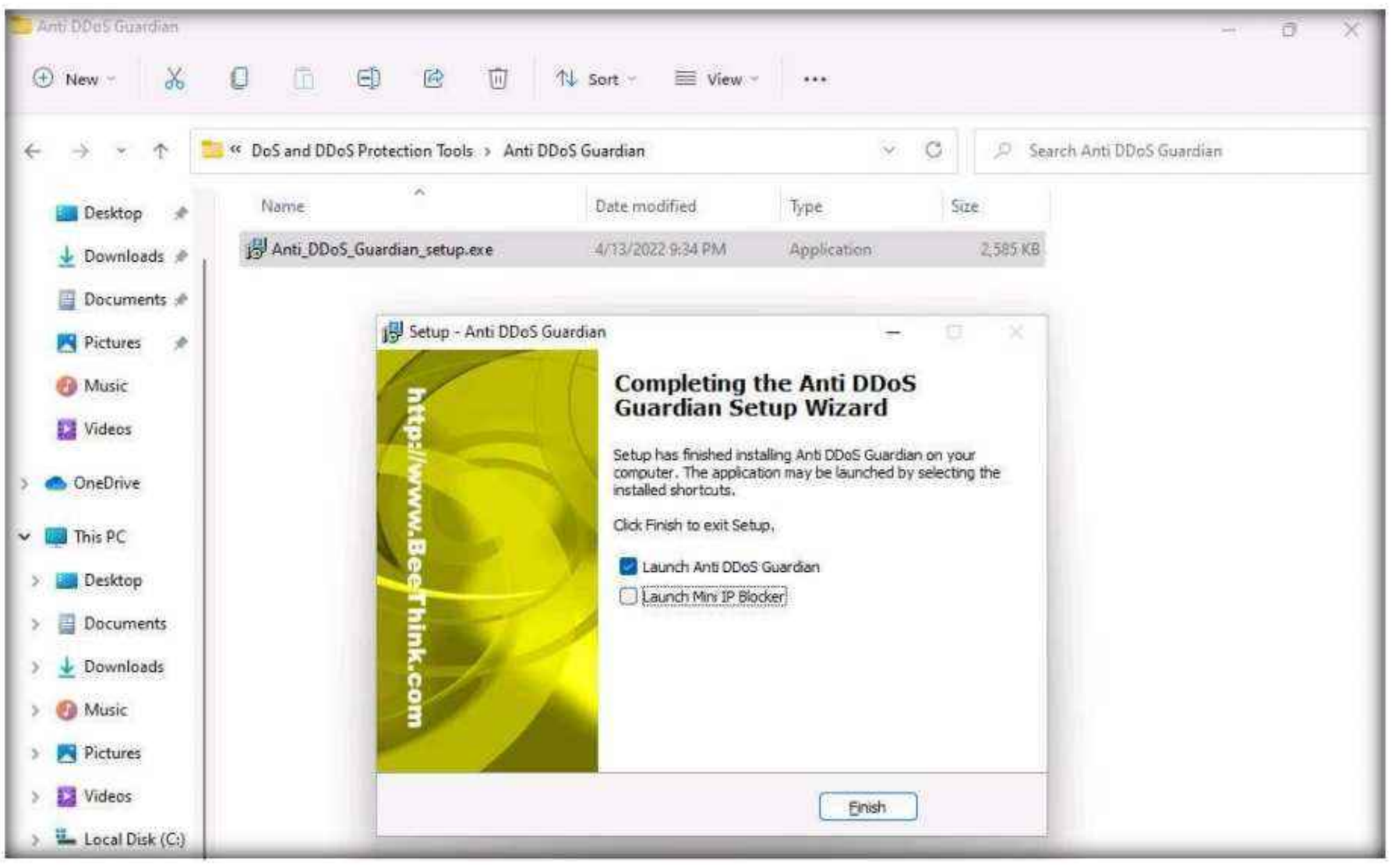
6. The **Select Additional Tasks** wizard appears; check the **Create a desktop shortcut** option, and click **Next**.



7. The **Ready to Install** wizard appears; click **Install**.

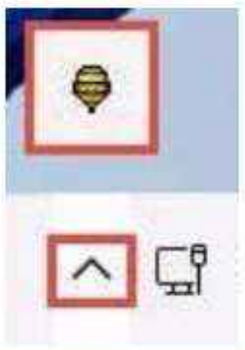


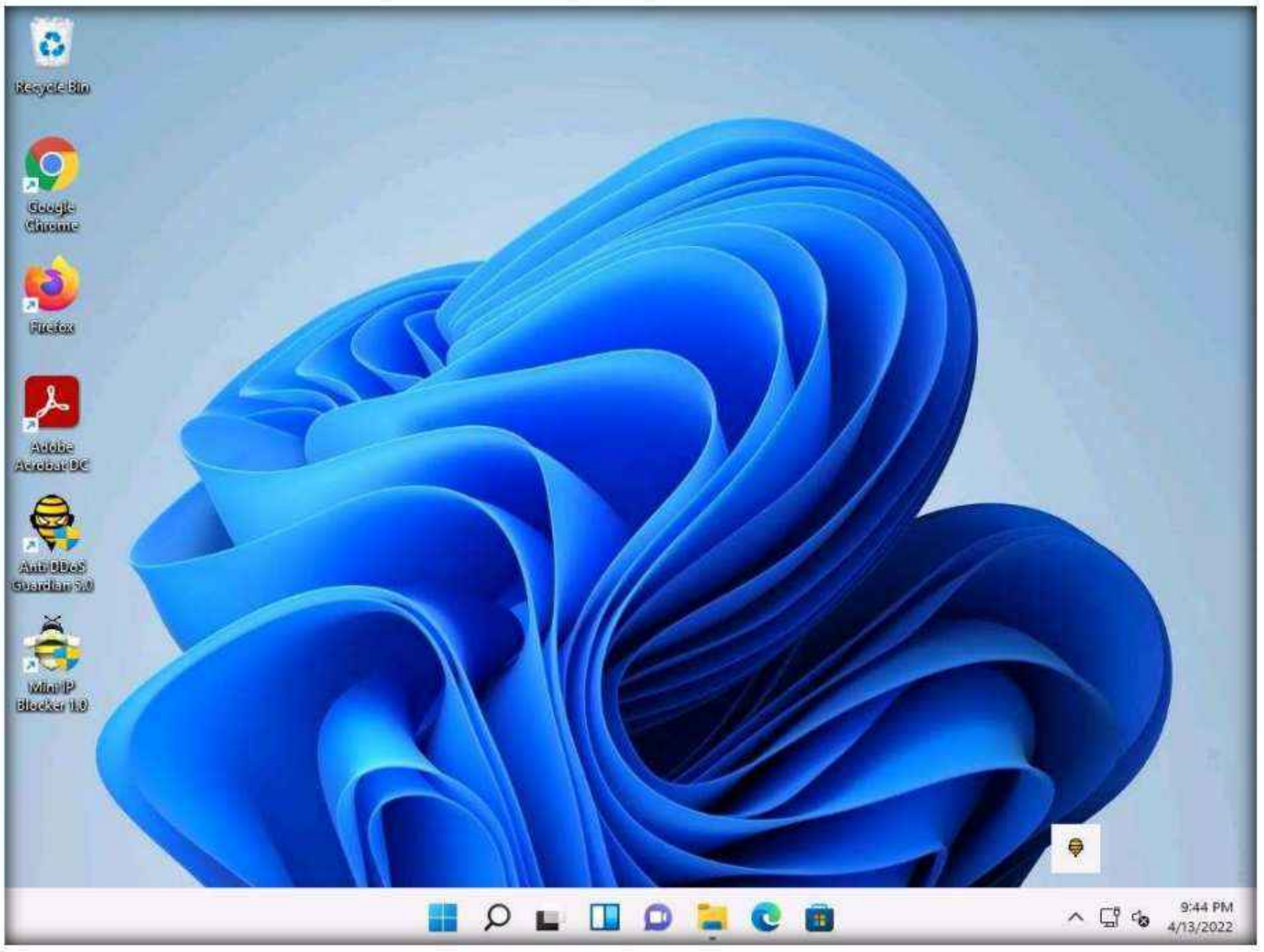
8. The **Completing the Anti DDoS Guardian Setup Wizard** window appears; uncheck the **Launch Mini IP Blocker** option and click **Finish**.



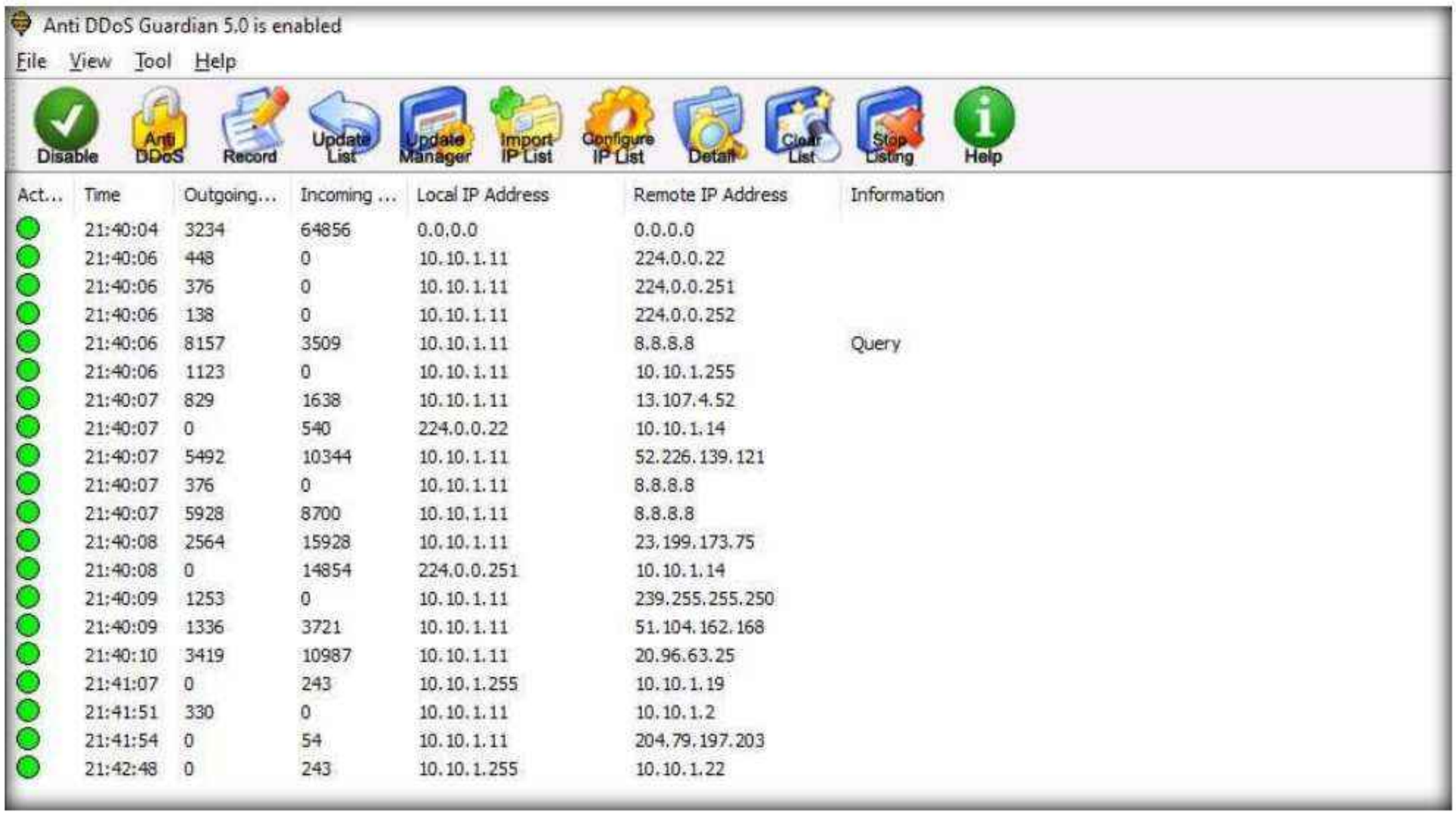
9. The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.

10. Click **Show hidden icons** from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon.





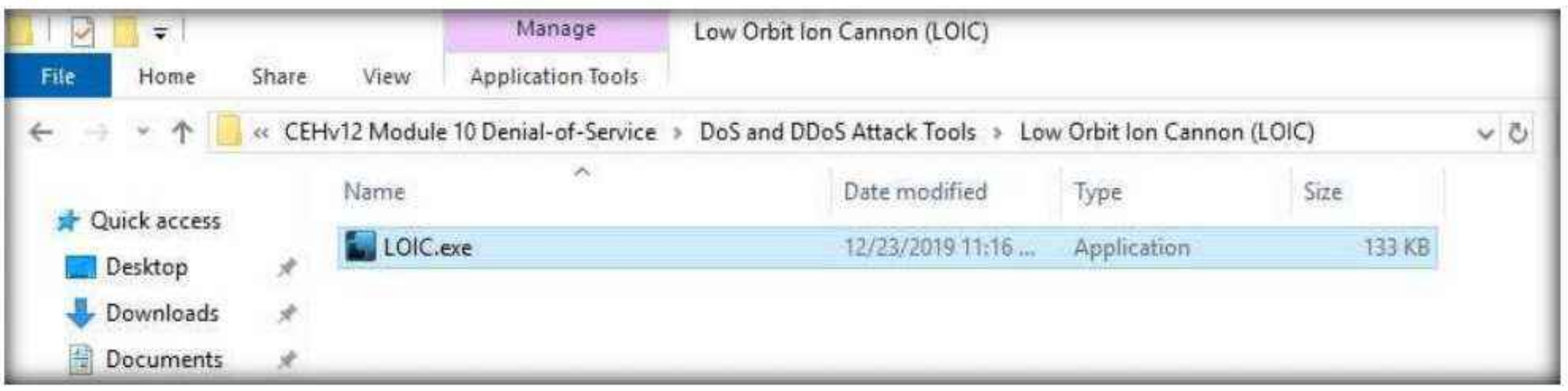
11. The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.



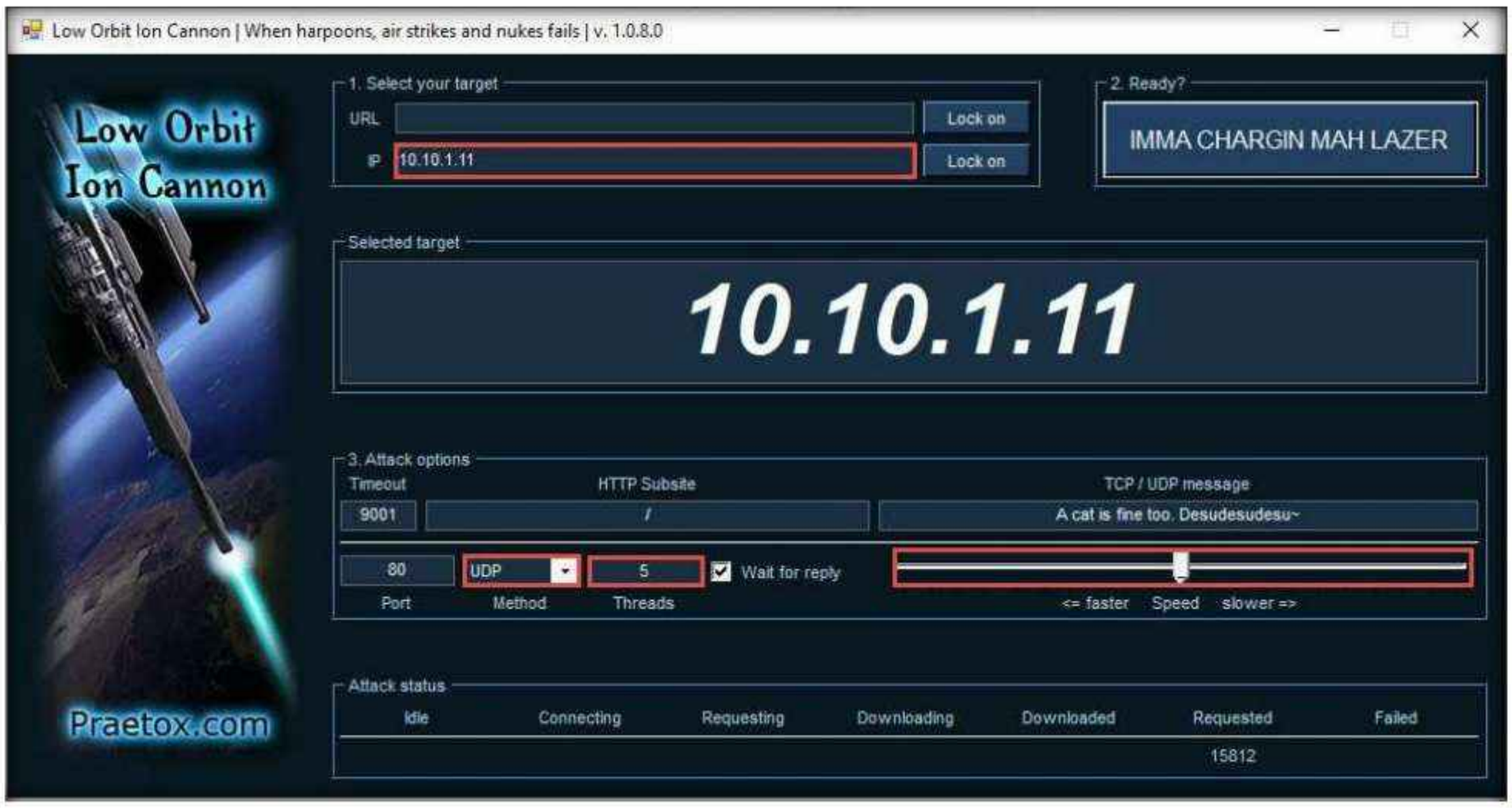
Act...	Time	Outgoing...	Incoming ...	Local IP Address	Remote IP Address	Information
	21:40:04	3234	64856	0.0.0.0	0.0.0.0	
	21:40:06	448	0	10.10.1.11	224.0.0.22	
	21:40:06	376	0	10.10.1.11	224.0.0.251	
	21:40:06	138	0	10.10.1.11	224.0.0.252	
	21:40:06	8157	3509	10.10.1.11	8.8.8.8	Query
	21:40:06	1123	0	10.10.1.11	10.10.1.255	
	21:40:07	829	1638	10.10.1.11	13.107.4.52	
	21:40:07	0	540	224.0.0.22	10.10.1.14	
	21:40:07	5492	10344	10.10.1.11	52.226.139.121	
	21:40:07	376	0	10.10.1.11	8.8.8.8	
	21:40:07	5928	8700	10.10.1.11	8.8.8.8	
	21:40:08	2564	15928	10.10.1.11	23.199.173.75	
	21:40:08	0	14854	224.0.0.251	10.10.1.14	
	21:40:09	1253	0	10.10.1.11	239.255.255.250	
	21:40:09	1336	3721	10.10.1.11	51.104.162.168	
	21:40:10	3419	10987	10.10.1.11	20.96.63.25	
	21:41:07	0	243	10.10.1.255	10.10.1.19	
	21:41:51	330	0	10.10.1.11	10.10.1.2	
	21:41:54	0	54	10.10.1.11	204.79.197.203	
	21:42:48	0	243	10.10.1.255	10.10.1.22	

12. Now, switch to the **Windows Server 2019** virtual machine and click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to log in.
13. Navigate to **Z:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

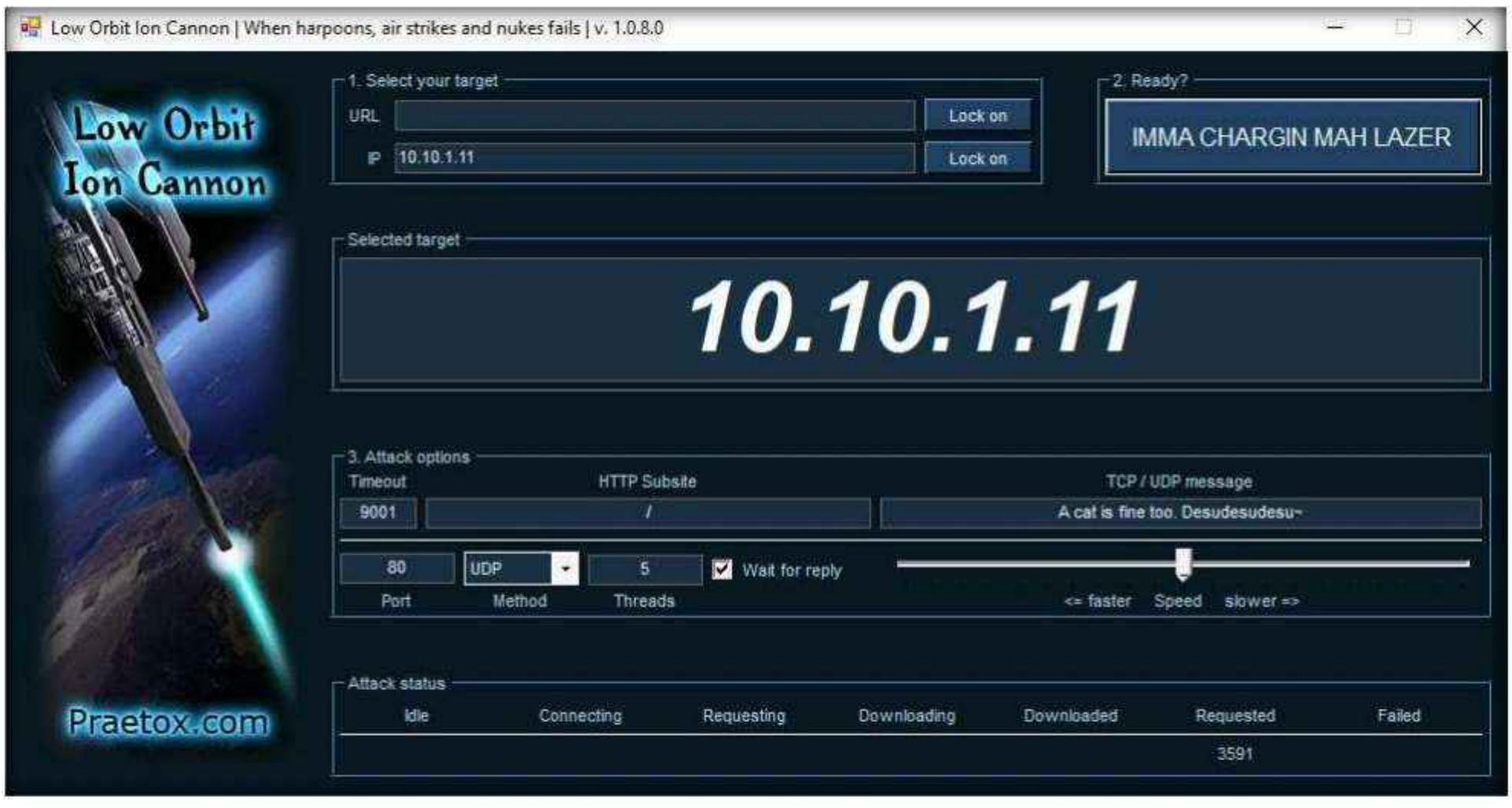
    Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



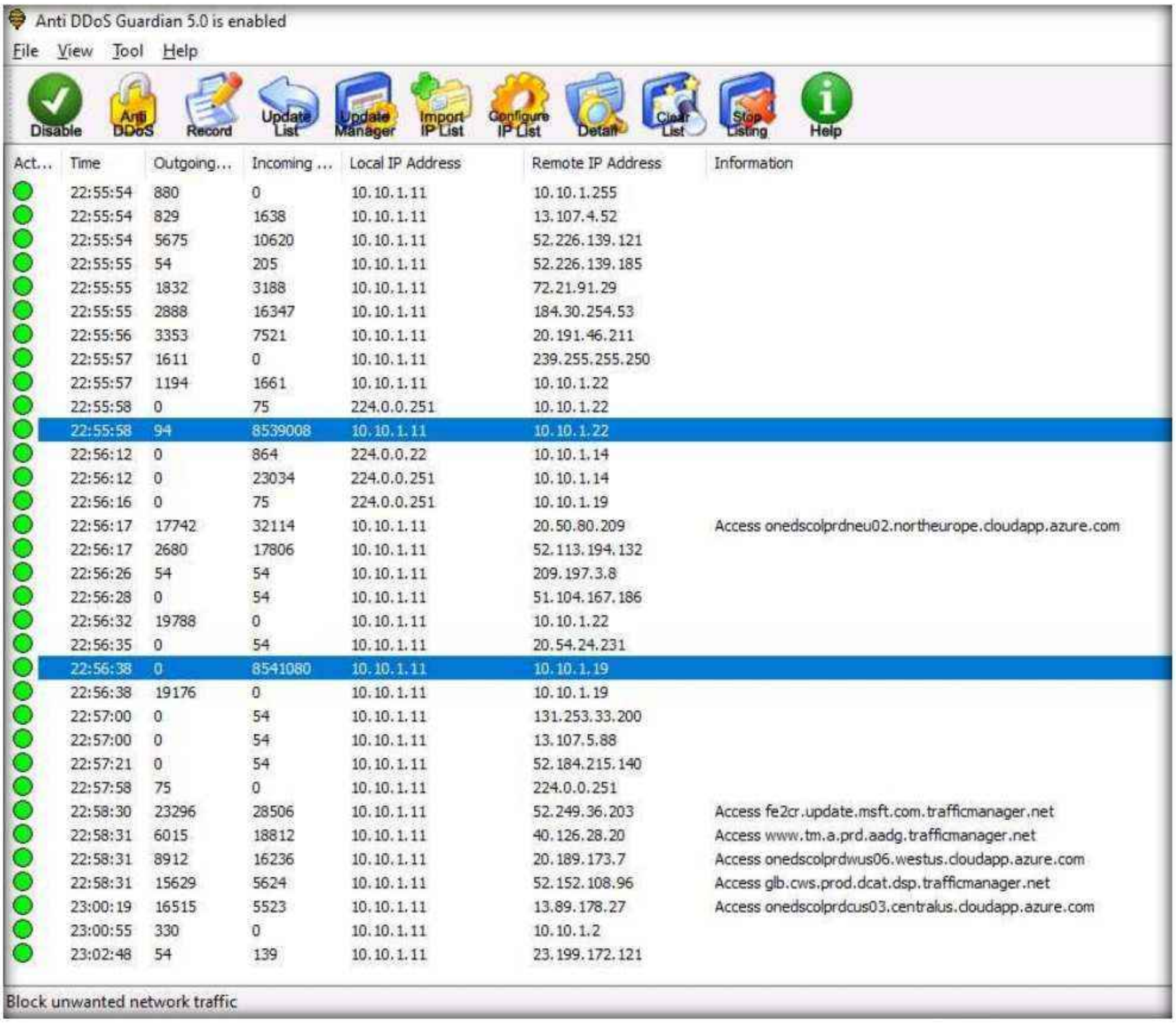
14. The **Low Orbit Ion Cannon** main window appears.
15. Perform the following settings:
    - Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.1.11**), and then click the **Lock on** button to add the target devices.
    - Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **5** under the **Threads** field. Slide the power bar to the middle.



16. Now, switch to the **Windows Server 2022** machine and follow **Steps 13 - 15** to launch LOIC and configure it.
17. Once **LOIC** is configured on all machines, switch to each machine (**Windows Server 2019**, and **Windows Server 2022**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Windows 11** machine.



18. Switch back to the **Windows 11** virtual machine and observe the packets captured by **Anti DDoS Guardian**.
19. Observe the huge number of packets coming from the host machines (**10.10.1.19 [Windows Server 2019]** and **10.10.1.22 [Windows Server 2022]**).



20. Double-click any of the sessions **10.10.1.19** or **10.10.1.22**.

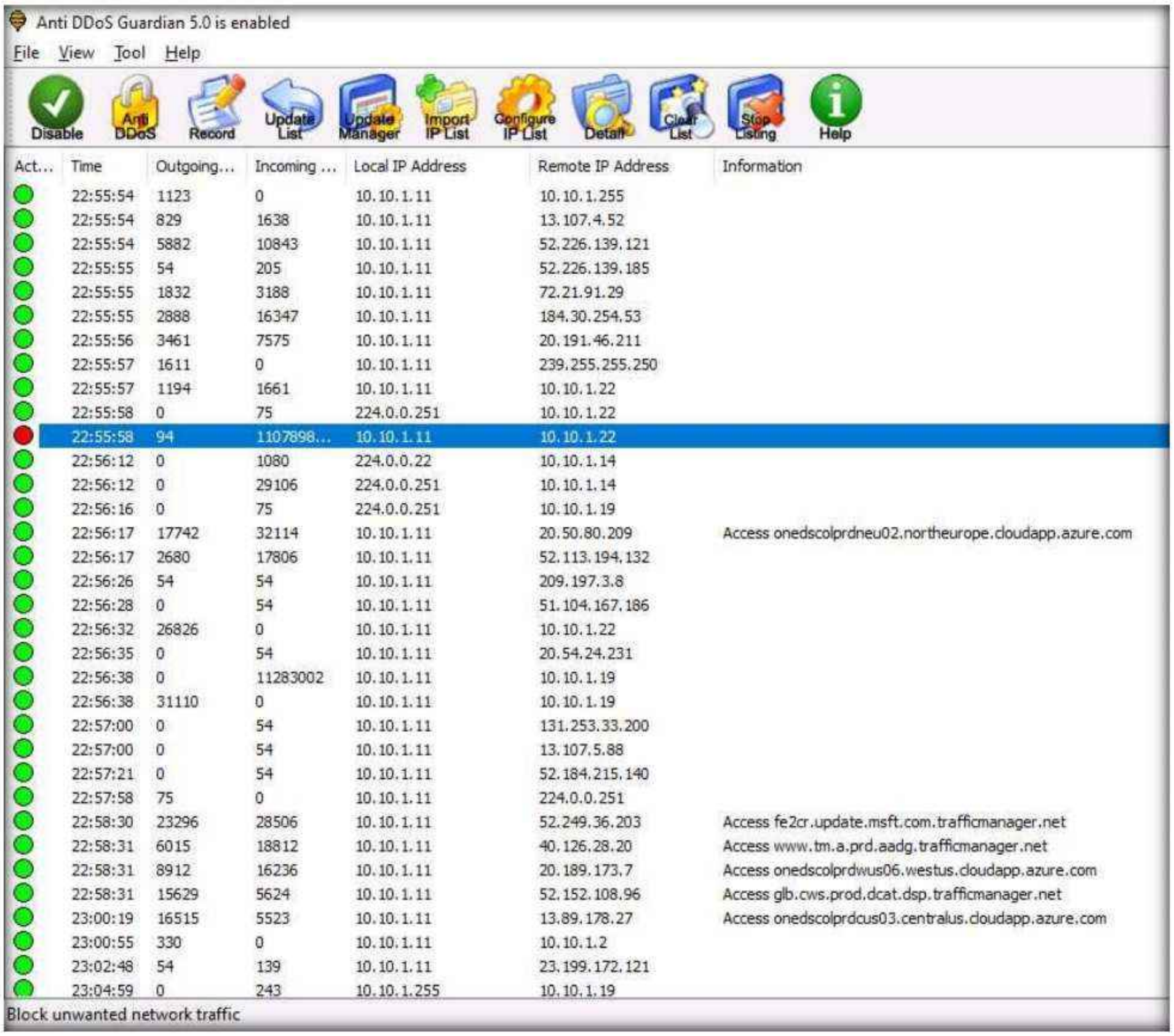
    Note: Here, we have selected 10.10.1.22. You can select either of them.

21. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.1.22**, as shown in the screenshot.

22. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the Block IP option blocks the IP address sending the huge number of packets.

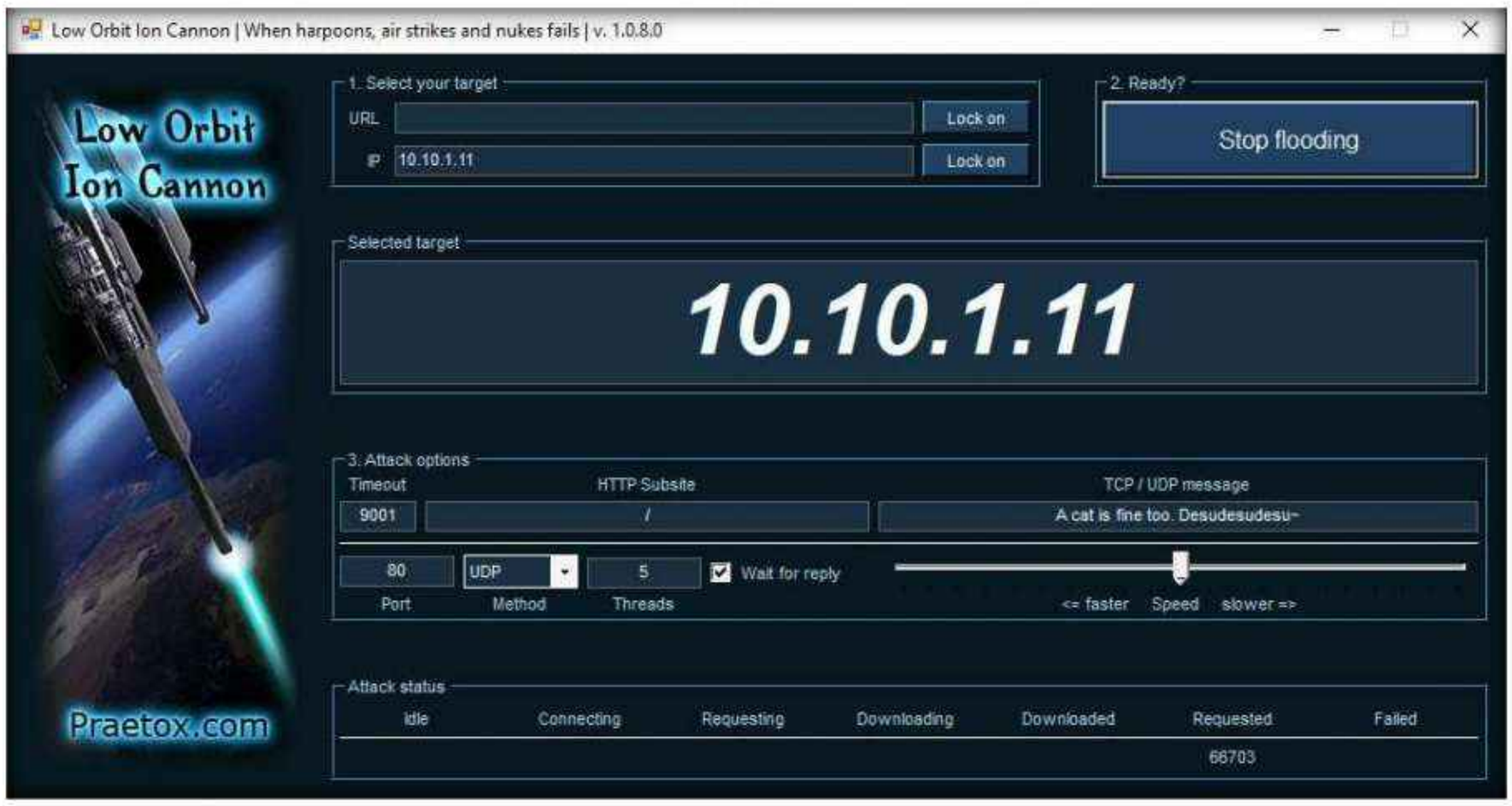
23. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.

24. Observe that the blocked IP session turns red in the **Action Taken** column.



25. Similarly, you can **Block IP** the address of the **10.10.1.19** session.

26. On completion of the task, click **Stop flooding**, and then close the LOIC window on all the attacker machines. (**Windows Server 2019** and **Windows Server 2022**).



27. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
28. Close all open windows and document all the acquired information.
29. You can also use other DoS and DDoS protection tools such as, **DOSarrest's DDoS protection service** (https://www.dosarrest.com), **DDoS-GUARD** (https://ddos-guard.net), and **Cloudflare** (https://www.cloudflare.com) to protect organization's systems and networks from DoS and DDoS attacks.
30. Switch to the **Windows 11** machine. Navigate to **Control Panel** → **Programs** → **Programs and Features** and uninstall **Anti DDoS Guardian**.
31. Turn off the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ CyberQ

Session Hijacking

Module 11

Session Hijacking

Session hijacking is when an attacker takes over either a valid TCP communication session between two computers or a valid user session in a web application.

Lab Scenario

A session hijacking attack refers to the exploitation of a session token-generation mechanism or token security controls that enables an attacker to establish an unauthorized connection with a target server. The attacker guesses or steals a valid session ID (which identifies authenticated users) and uses it to establish a session with the server.

As an ethical hacker or penetration tester, you should understand different session hijacking concepts, how attackers perform application- and network-level session hijacking, and the various tools used to launch this kind of attack. You should also be able to implement security measures at both the application and network levels to protect your network from session hijacking. Application-level hijacking involves gaining control over the Hypertext Transfer Protocol (HTTP) user session by obtaining the session IDs. Network-level hijacking is prevented by packet encryption, which can be achieved with protocols such as IPsec, SSL, and SSH.

Lab Objective

The objective of the lab is to perform session hijacking and other tasks that include, but are not limited to:

- Hijack a session by intercepting traffic between server and client
- Steal a user session ID by intercepting traffic
- Detect session hijacking attacks

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 50 Minutes

Overview of Session Hijacking

Session hijacking can be either active or passive, depending on the degree of involvement of the attacker:

- **Active session hijacking**: An attacker finds an active session and takes it over
- **Passive session hijacking**: An attacker hijacks a session, and, instead of taking over, monitors and records all the traffic in that session

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform session hijacking on the target systems. Recommended labs that will assist you in learning various session hijacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform Session Hijacking	√	√	√
	1.1 Hijack a Session using Zed Attack Proxy (ZAP)	√		√
	1.2 Intercept HTTP Traffic using bettercap		√	√
	1.3 Intercept HTTP Traffic using Hetty	√		√
2	Detect Session Hijacking	√		√
	2.1 Detect Session Hijacking using Wireshark	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Perform Session Hijacking

In a session hijacking attack, an attacker takes over (hijacks) a victim's valid user session in order to establish an unauthorized connection with a target server.

Lab Scenario

Session hijacking allows an attacker to take over an active session by bypassing the authentication process. It involves stealing or guessing a victim's valid session ID, which the server uses to identify authenticated users, and using it to establish a connection with the server. The server responds to the attacker's requests as though it were communicating with an authenticated user, after which the attacker is able to perform any action on that system.

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the-middle (MITM) and Denial-of-Service (DoS) attacks. A MITM attack occurs when an attacker places himself/herself between the authorized client and the server to intercept information flowing in either direction. A DoS attack happens when attackers sniff sensitive information and use it to make host or network resource unavailable to users, usually by flooding the target with requests until the system is overloaded.

As a professional ethical hacker or penetration tester, you must possess the required knowledge to hijack sessions in order to test the systems in the target network.

The labs in this exercise demonstrate how to hijack an active session between two endpoints.

Lab Objectives

- Hijack a session using Zed Attack Proxy (ZAP)
- Intercept HTTP traffic using bettercap
- Intercept HTTP traffic using Hetty

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2022 virtual machine

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of Session Hijacking

Session hijacking can be divided into three broad phases:

- **Tracking the Connection**: The attacker uses a network sniffer to track a victim and host, or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict
- **Desynchronizing the Connection**: A desynchronized state occurs when a connection between the target and host has been established, or is stable with no data transmission, or when the server's sequence number is not equal to the client's acknowledgment number (or vice versa)
- **Injecting the Attacker's Packet**: Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or actively participate as the man-in-the-middle, passing data between the target and server, while reading and injecting data at will

Lab Tasks

Task 1: Hijack a Session using Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

ZAP allows you to see all the requests you make to a web app and all the responses you receive from it. Among other things, it allows you to see AJAX calls that may not otherwise be outright visible. You can also set breakpoints, which allow you to change the requests and responses in real-time.

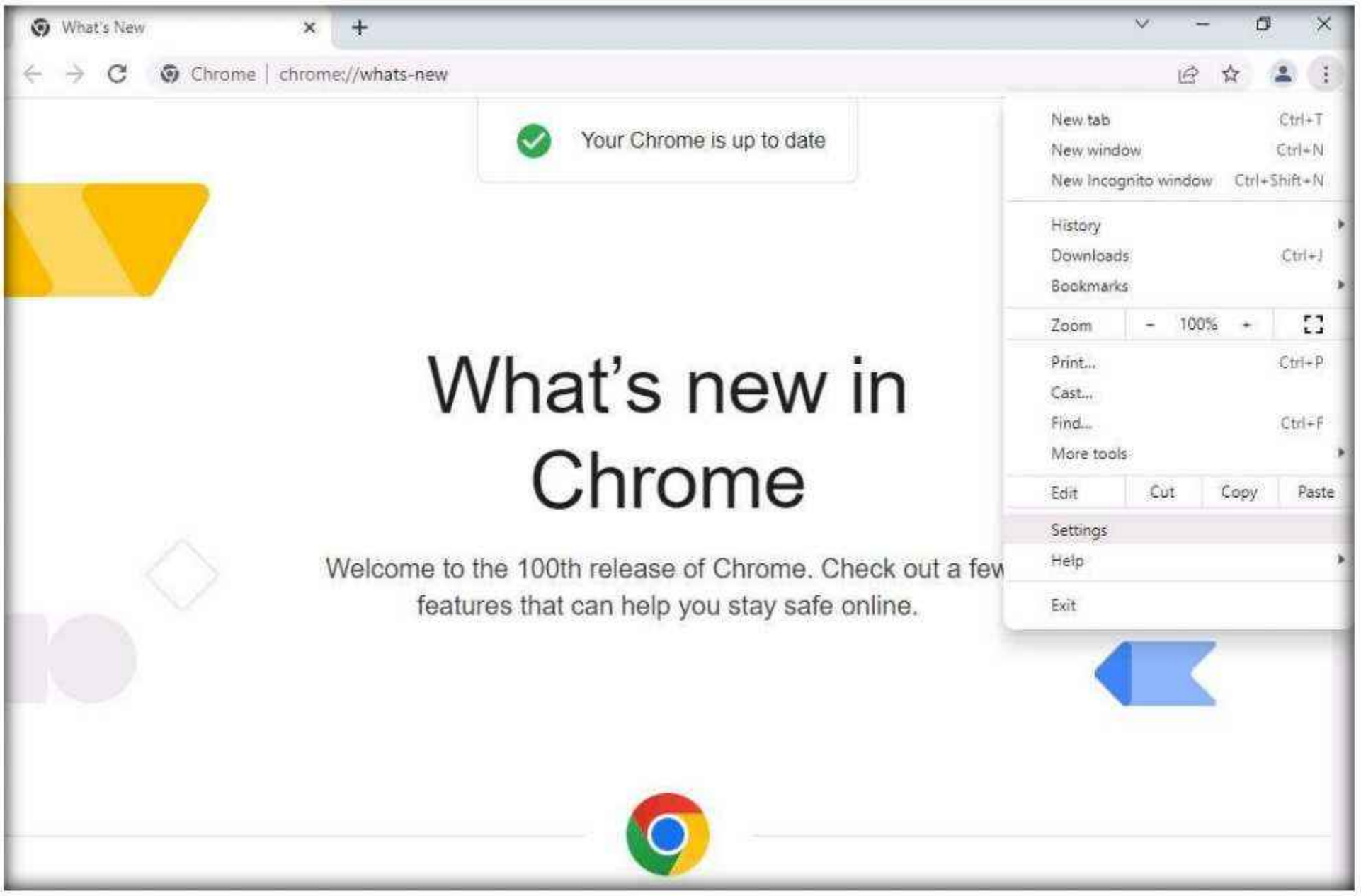
Here, we will hijack a session using ZAP. You will learn how to intercept the traffic of victims' machines with a proxy and how to view all the requests and responses from them.

Note: Before starting this task, we need to configure the proxy settings in the victim's machine, which in this task will be the **Windows 11** machine.

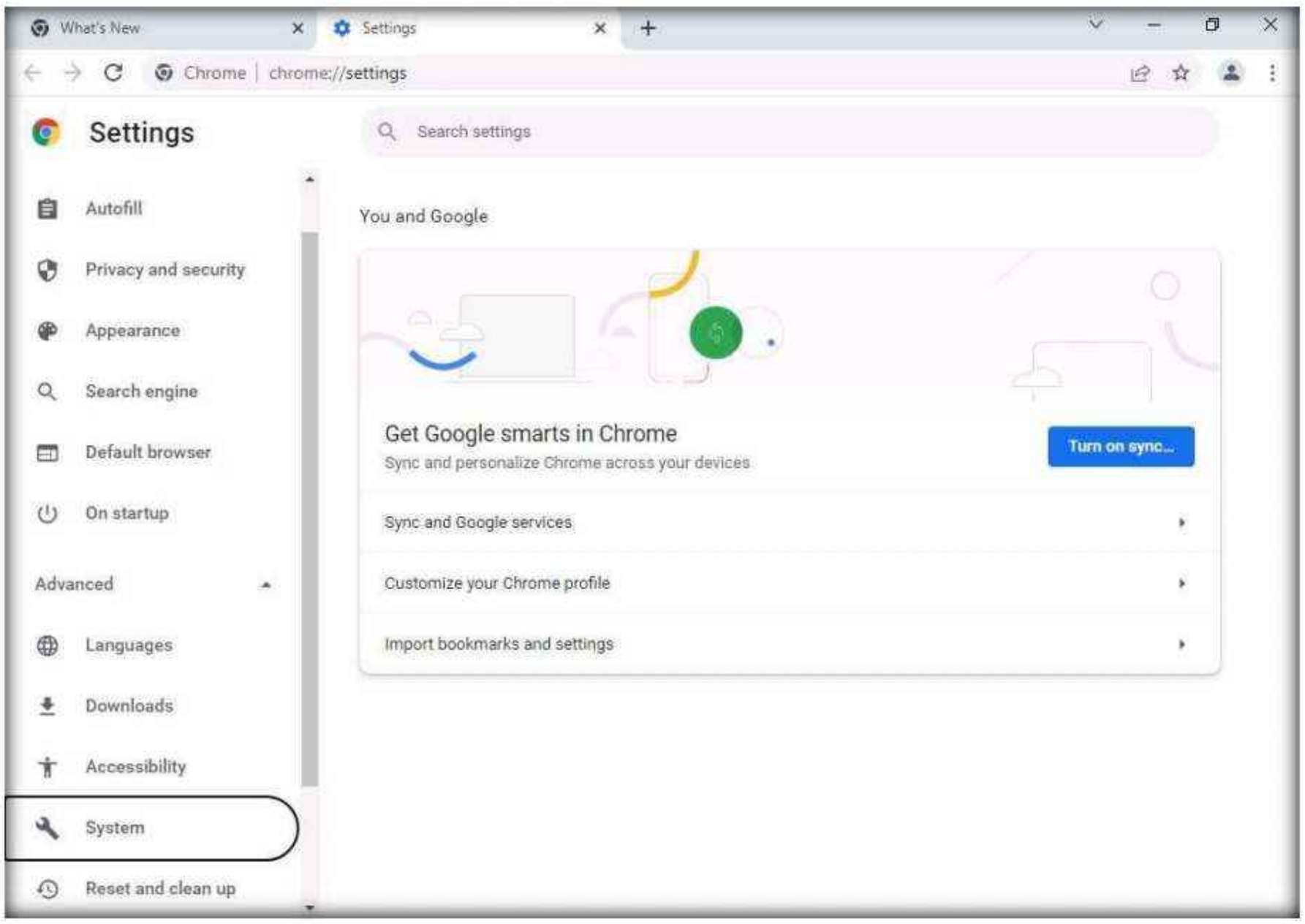
1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click Continue. In the **Sign in with Microsoft** wizard click **Cancel** to continue.

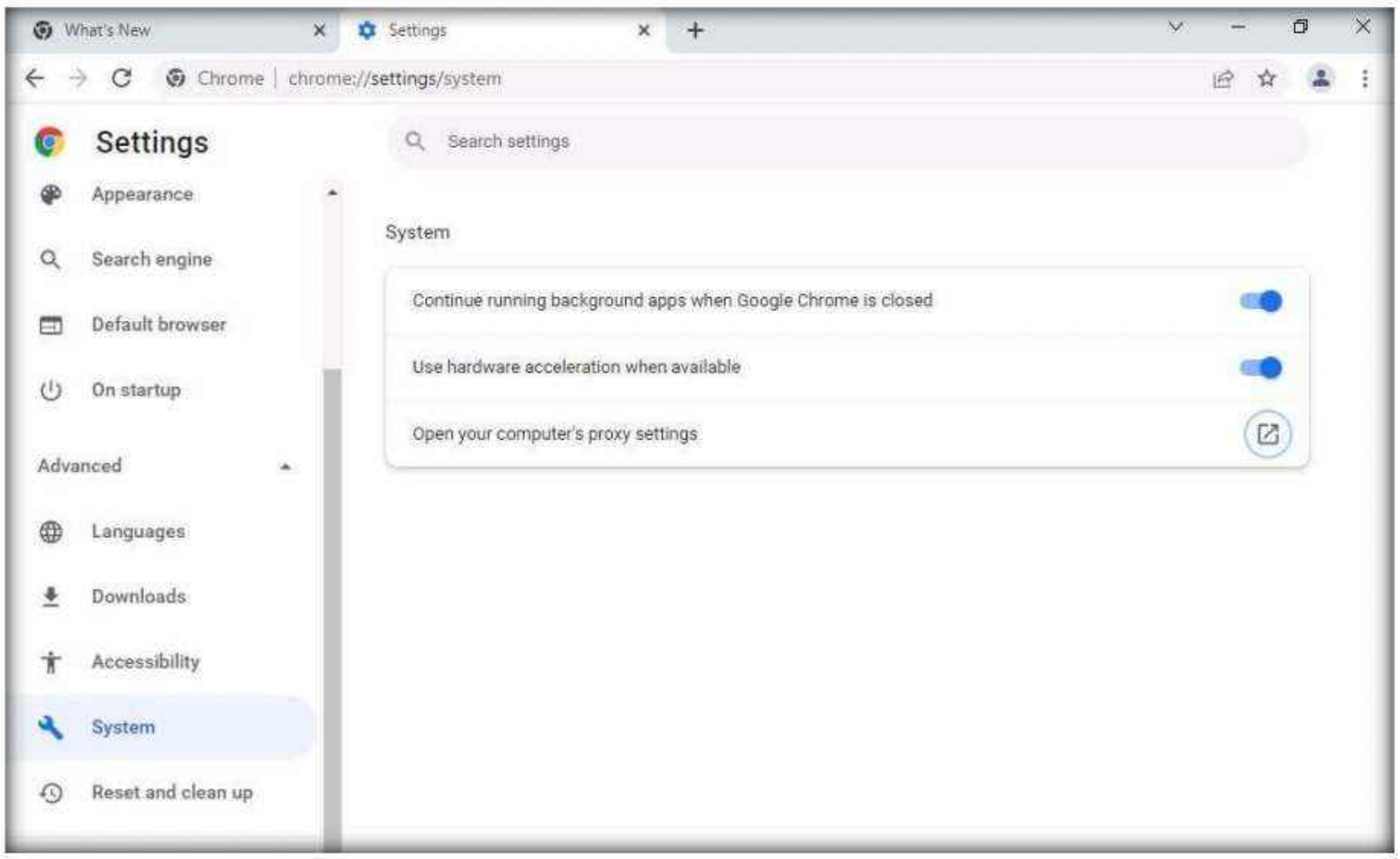
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Open any web browser (here, **Google Chrome**), click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.



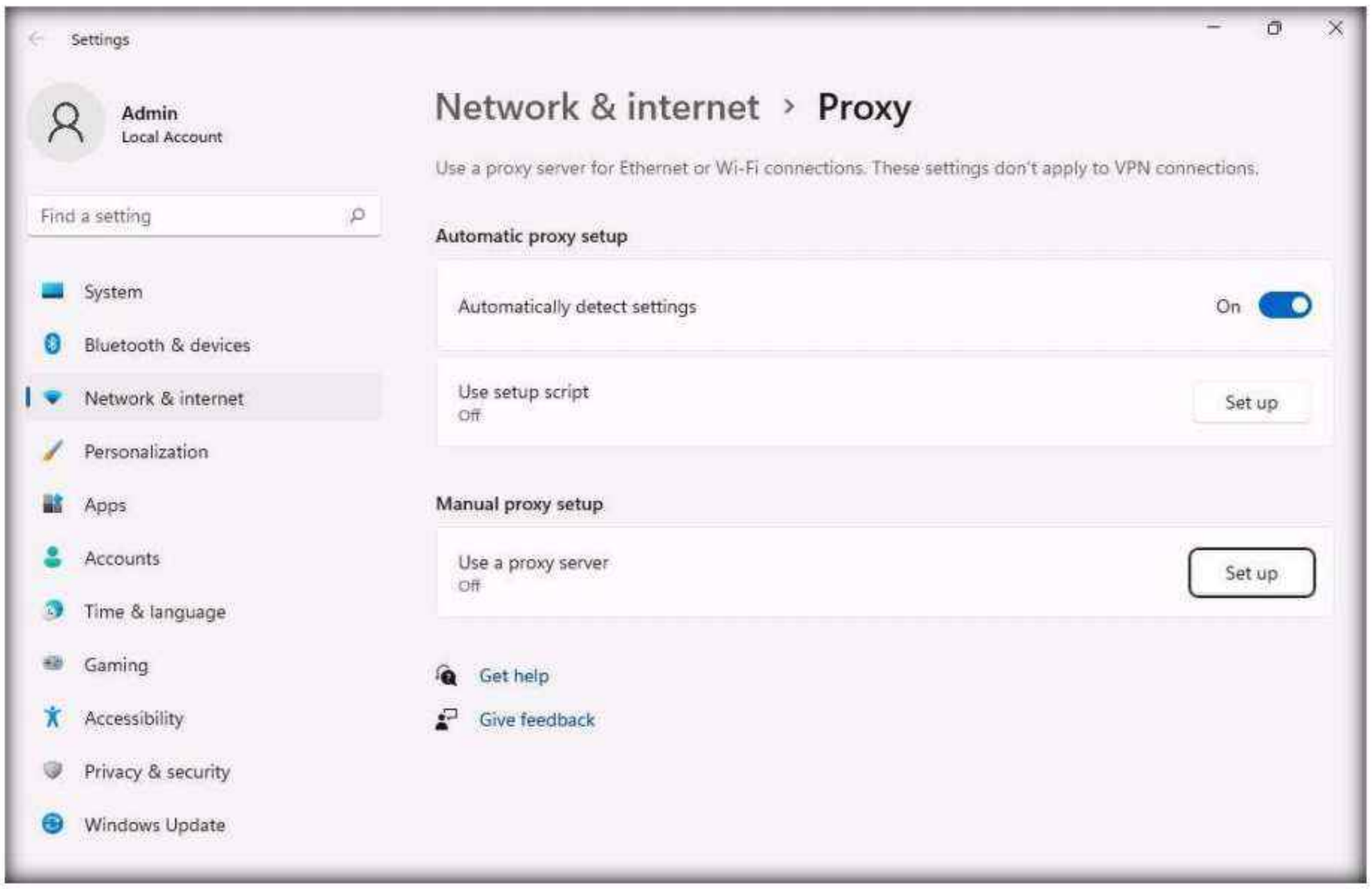
4. On the **Settings** page, scroll down, expand the **Advanced** settings and select **System** option from the left pane.



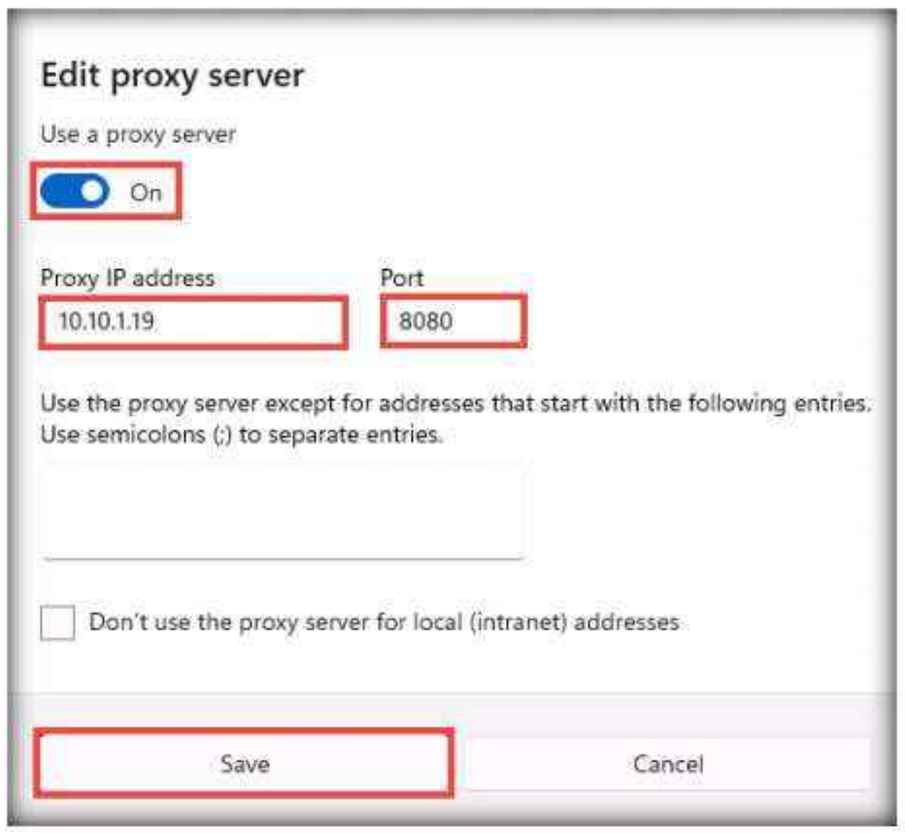
5. **System** page appears and click **Open your computer's proxy settings** to configure a proxy.



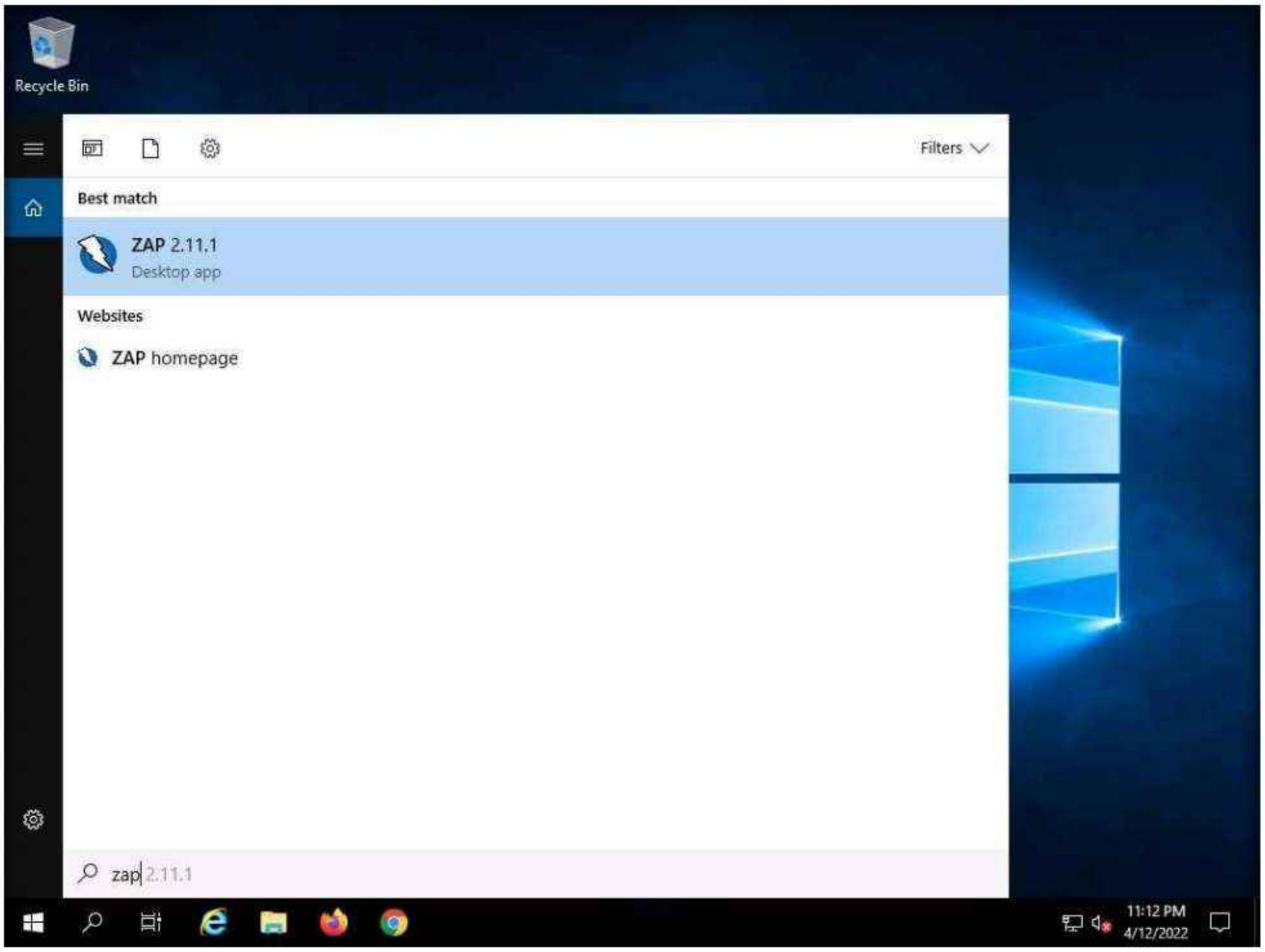
6. A **Settings** window opens, with the **Proxy** settings in the right pane.
7. Click **Set up** button under **Manual proxy setup** section.



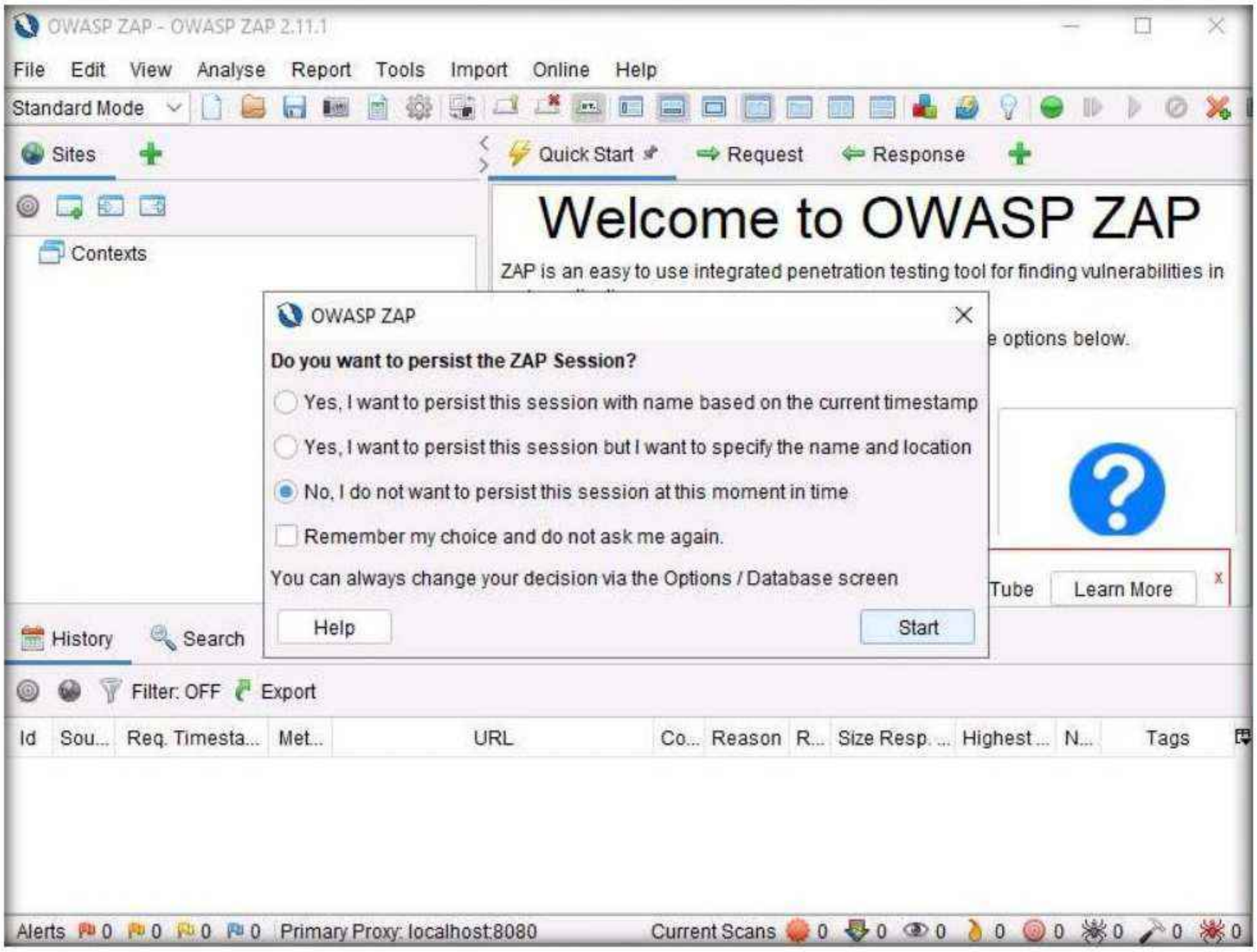
8. **Edit proxy server** window appears, make the following changes:
   - Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
   - In the **Proxy IP address** field, type **10.10.1.19** (the IP address of the attacker's machine).
   - In the **Port** field, type **8080**.
   - Click **Save**.



9. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.
10. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
11. Click **Type here to search** icon ( ) on the **Desktop**. Type **zap** in the search field, the **ZAP 2.11.1** appears in the result, press **Enter** to launch it.



12. **OWASP ZAP** initializes and a prompt that reads **Do you want to persist the ZAP Session?** appears. Select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

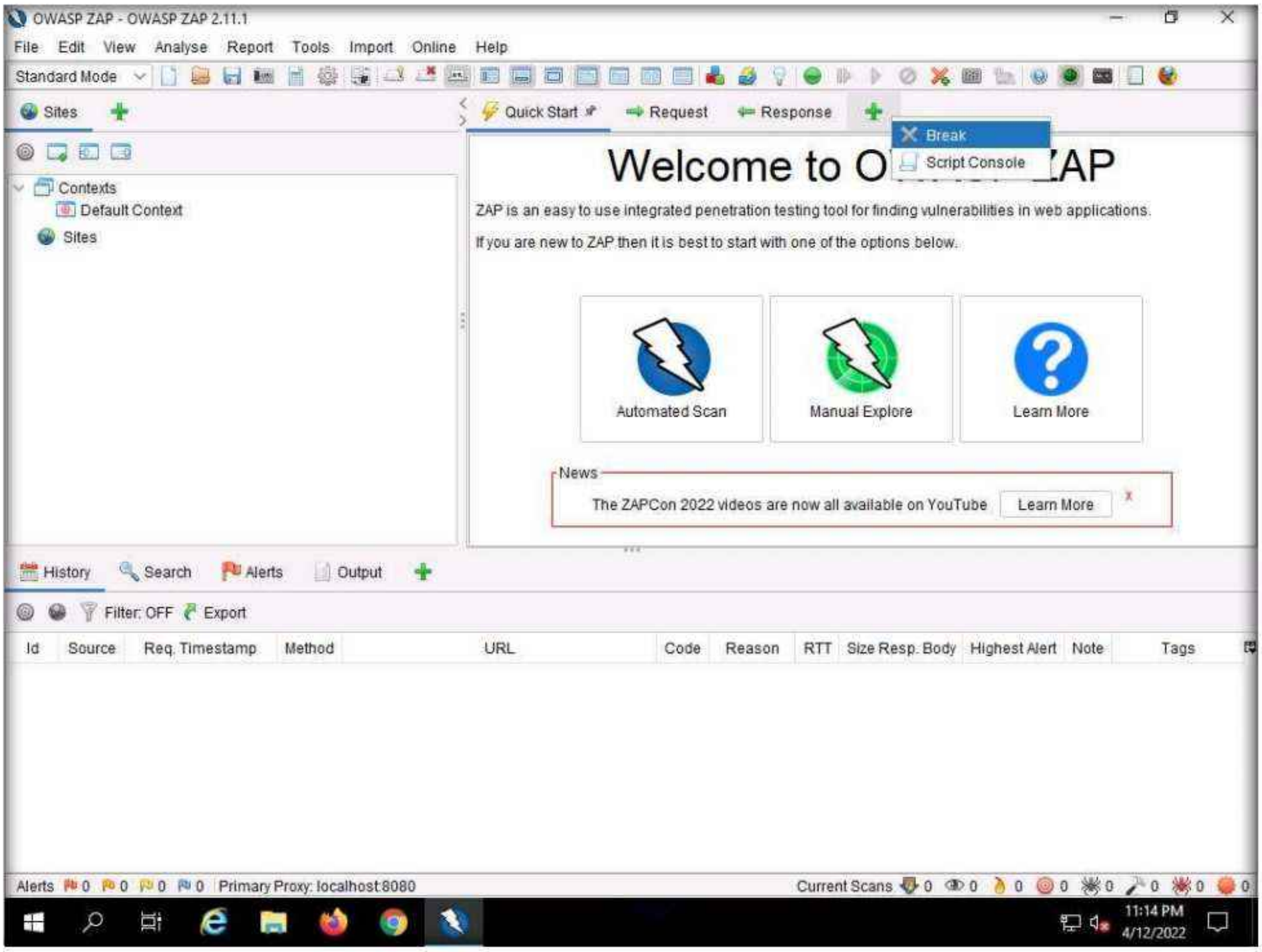


13. The **OWASP ZAP** main window appears. Click on the "**+**" icon in the right pane and select **Break** from the options.

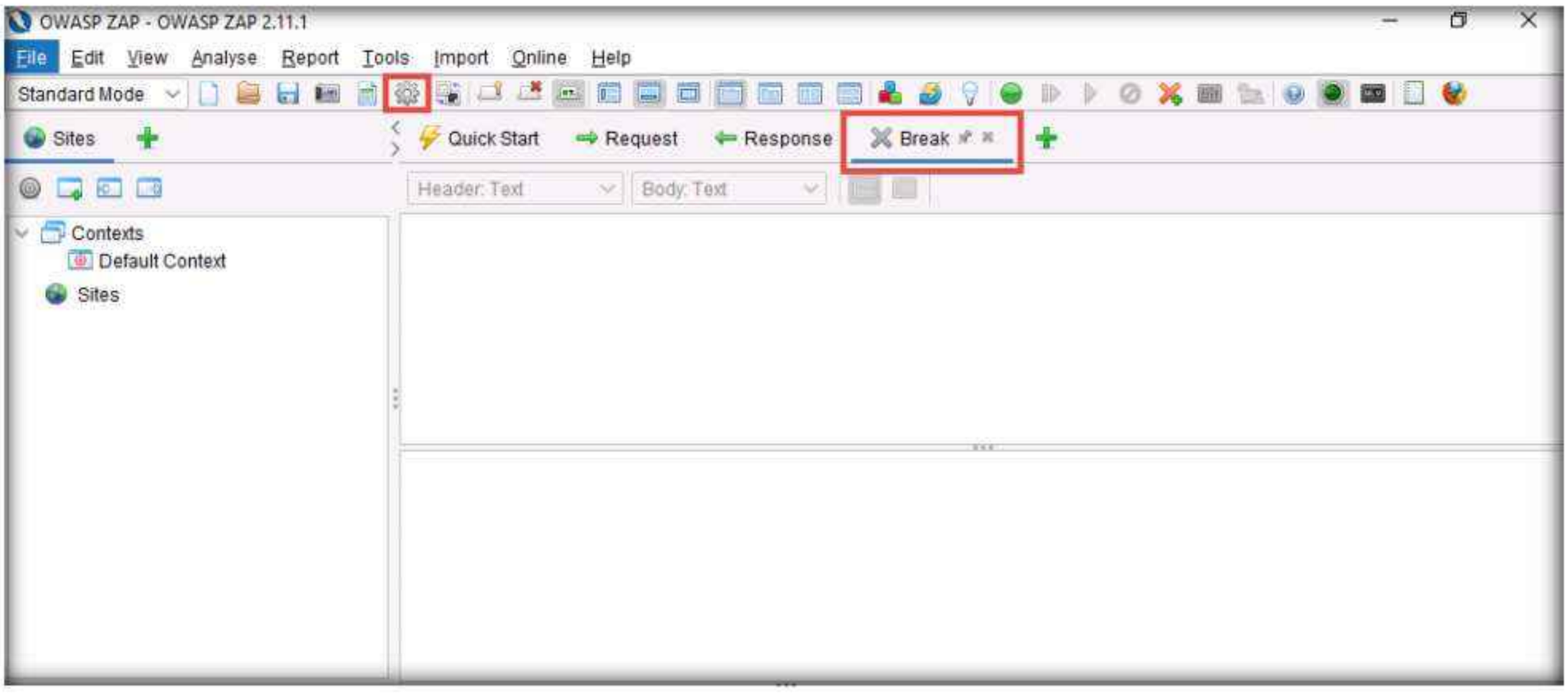
    Note: If a OWASP ZAP pop-up appears, click **OK** in all the pop-ups.

    Note: The **Break** tab allows you to modify a response or request when ZAP has caught it. It also allows you to modify certain elements that you cannot modify through your browser, including:

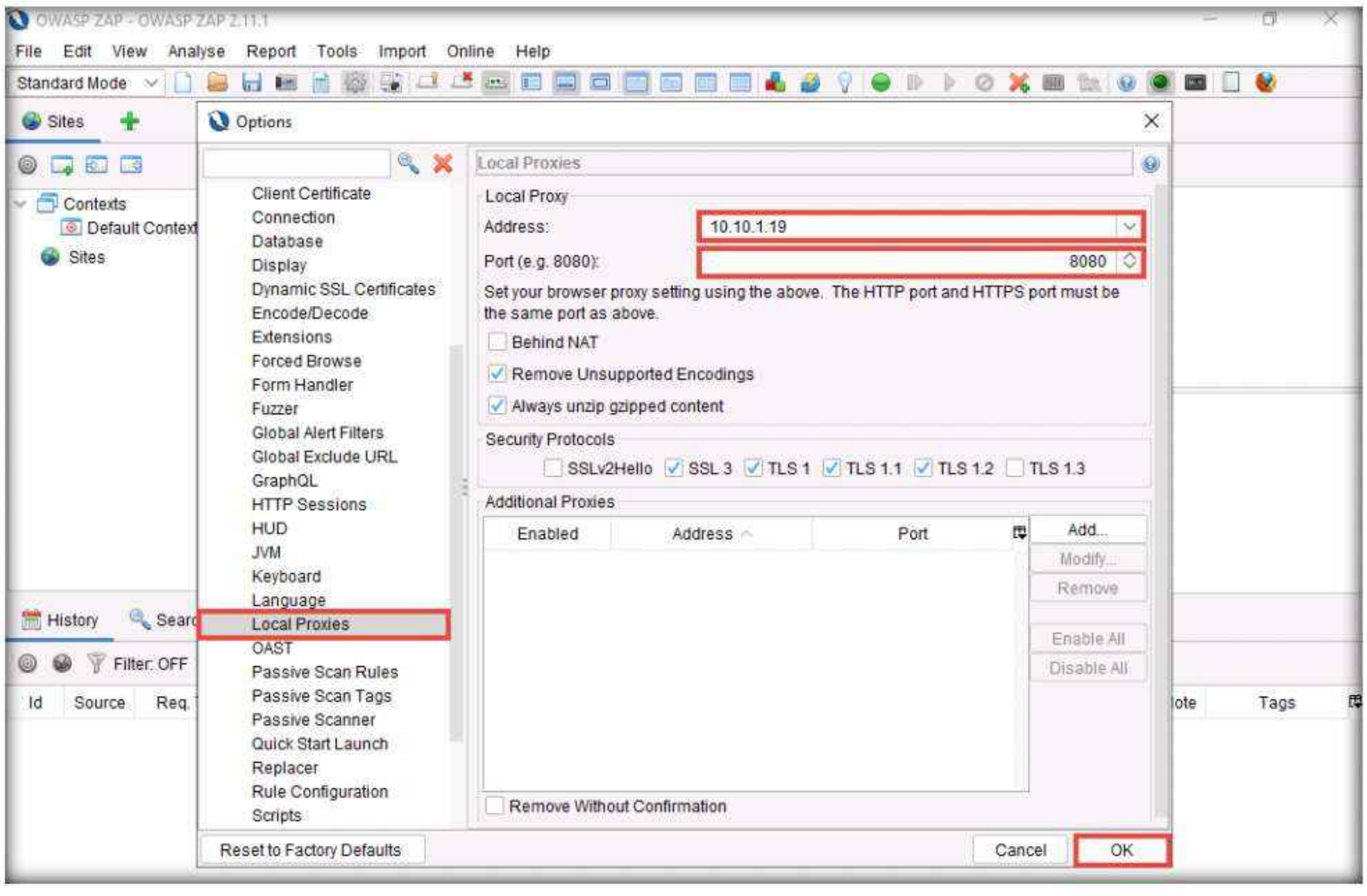
    - The header
    - Hidden fields
    - Disabled fields
    - Fields that use JavaScript to filter out illegal characters



14. The **Break** tab is added to your **OWASP ZAP** window.
15. To configure ZAP as a proxy, click the **Options...** icon from the toolbar.

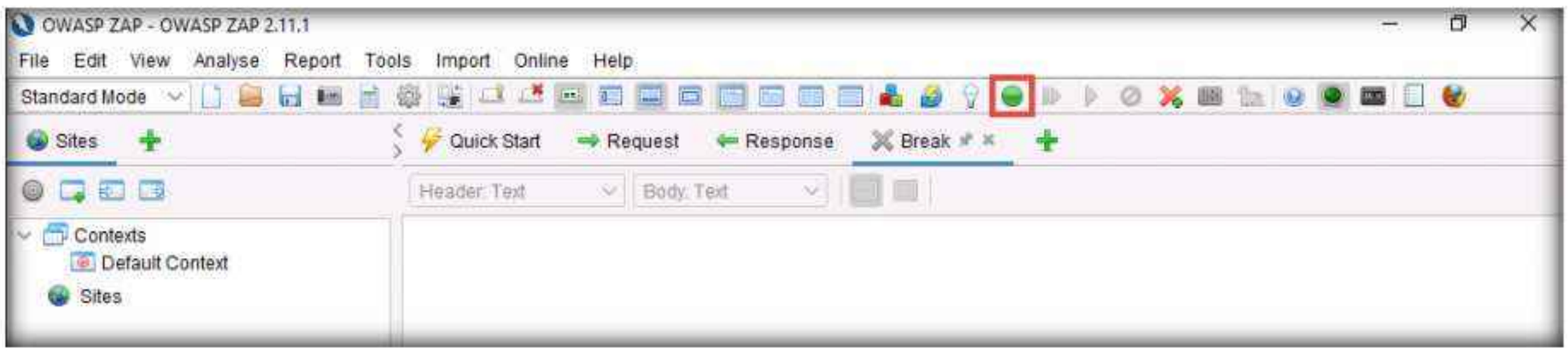


16. In the **Options** window, scroll-down in the left-pane and click **Local Proxies**. In the right pane, under the **Local Proxy** section, type **10.10.1.19** (the IP address of the **Windows Server 2019** machine) in the **Address** field and leave the **Port** value to the default, **8080**; click **OK**.

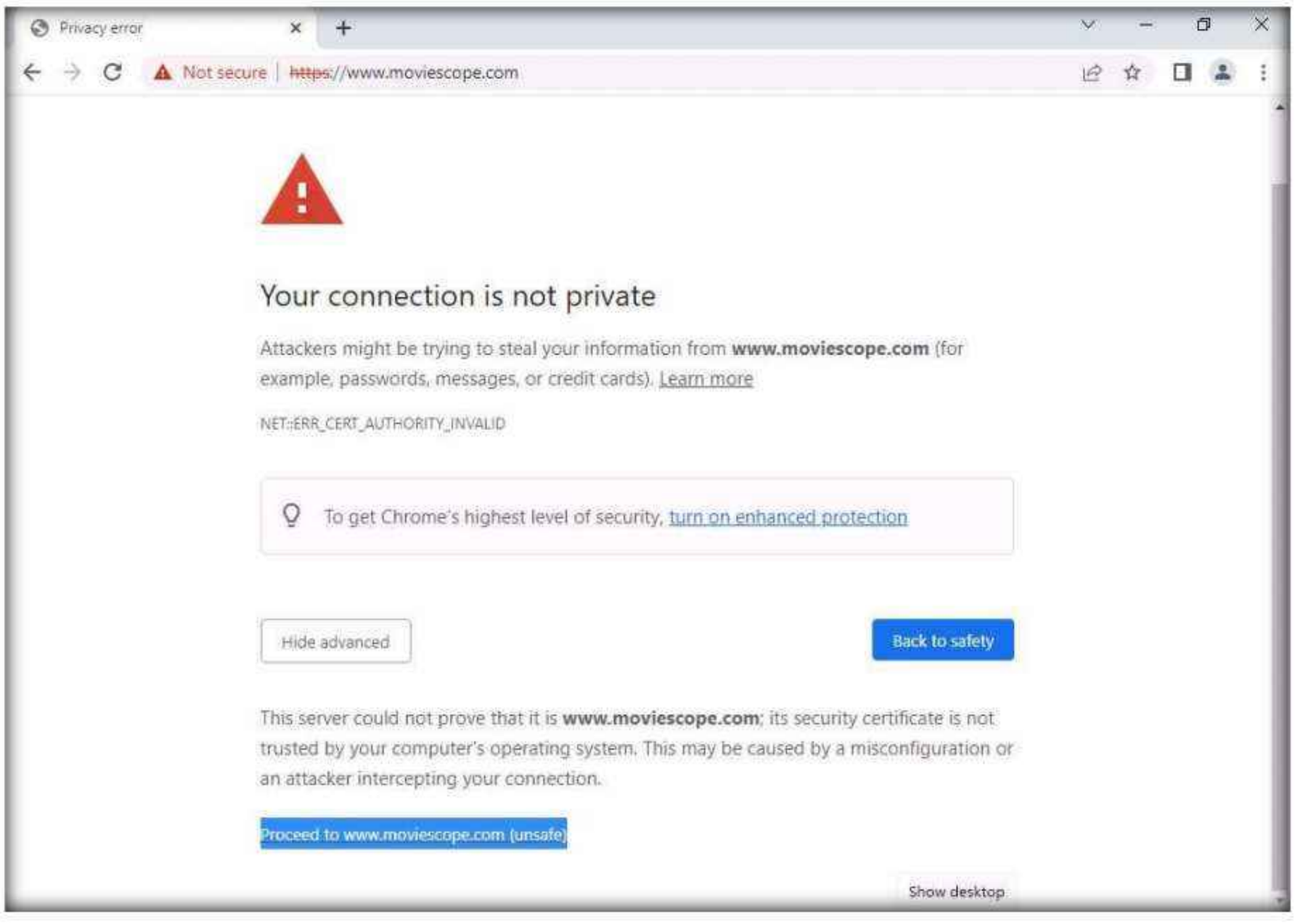


17. Click the **Set break on all requests and responses** icon on the main ZAP toolbar. This button sets and unsets a global breakpoint that will trap and display the next response or request from the victim's machine in the **Break** tab.

    Note: The **Set break on all requests and responses** icon turns **automatically** from green to red.

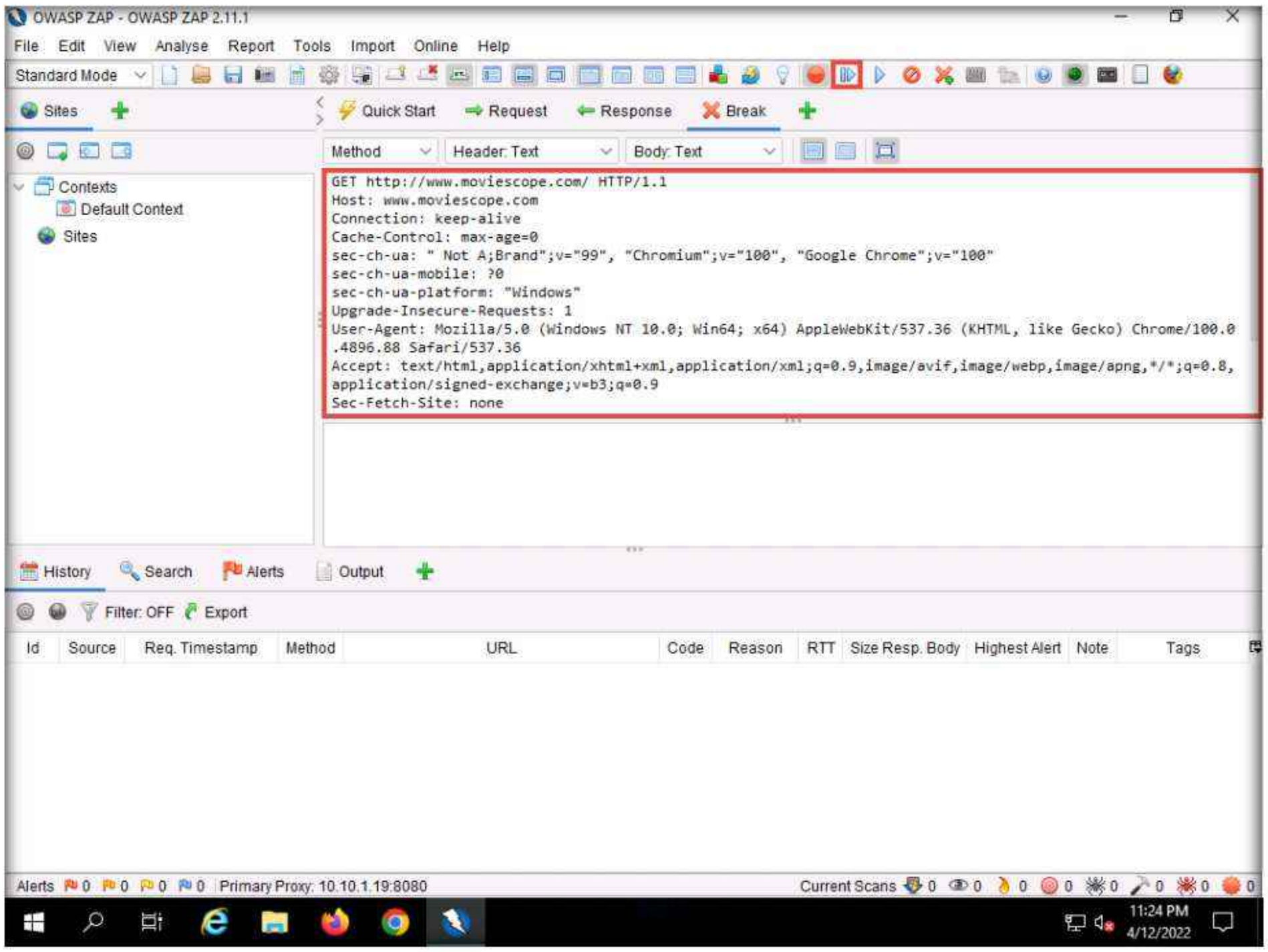


18. Now, switch back to the victim's machine (**Windows 11**) and launch the same browser in which you configured the proxy settings. In this task, we have configured the **Google Chrome** browser.
19. Place your mouse cursor in the address bar, type **www.moviescope.com** and press **Enter**.
20. A message appears, stating that **Your connection is not private**. Click the **Advanced** button.
21. On the next page, click **Proceed to www.moviescope.com (unsafe)** to open the website.

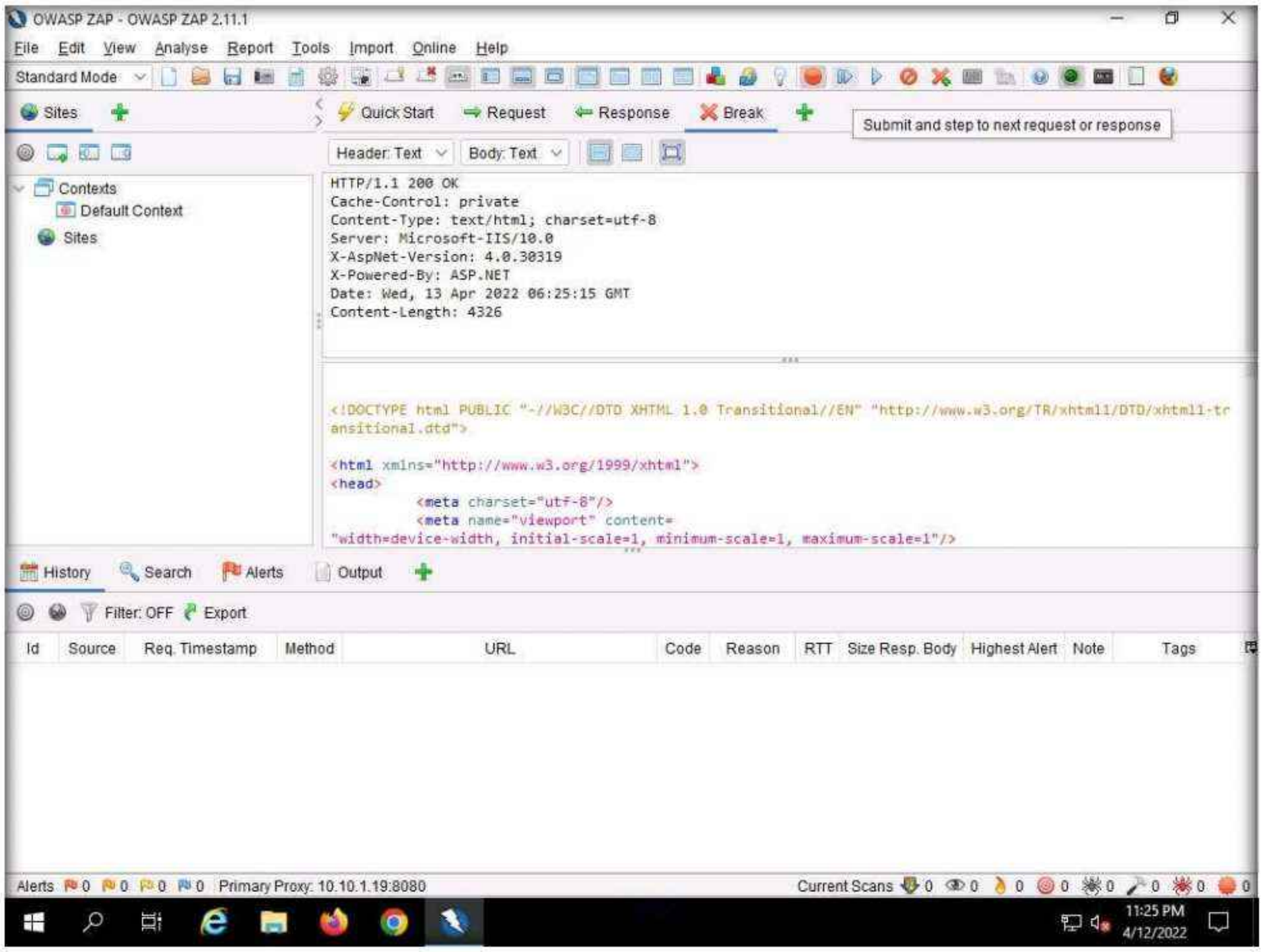


22. Now, switch back to the attacker machine (**Windows Server 2019**) and observe that **OWASP ZAP** has begun to capture the requests of the victim's machine.

23. In **Steps 19-21**, we have visited **www.moviescope.com** in the victim's browser. Look in the **Break** tab and click the **Submit and step to next request or response** icon on the toolbar to capture the **www.moviescope.com** request.



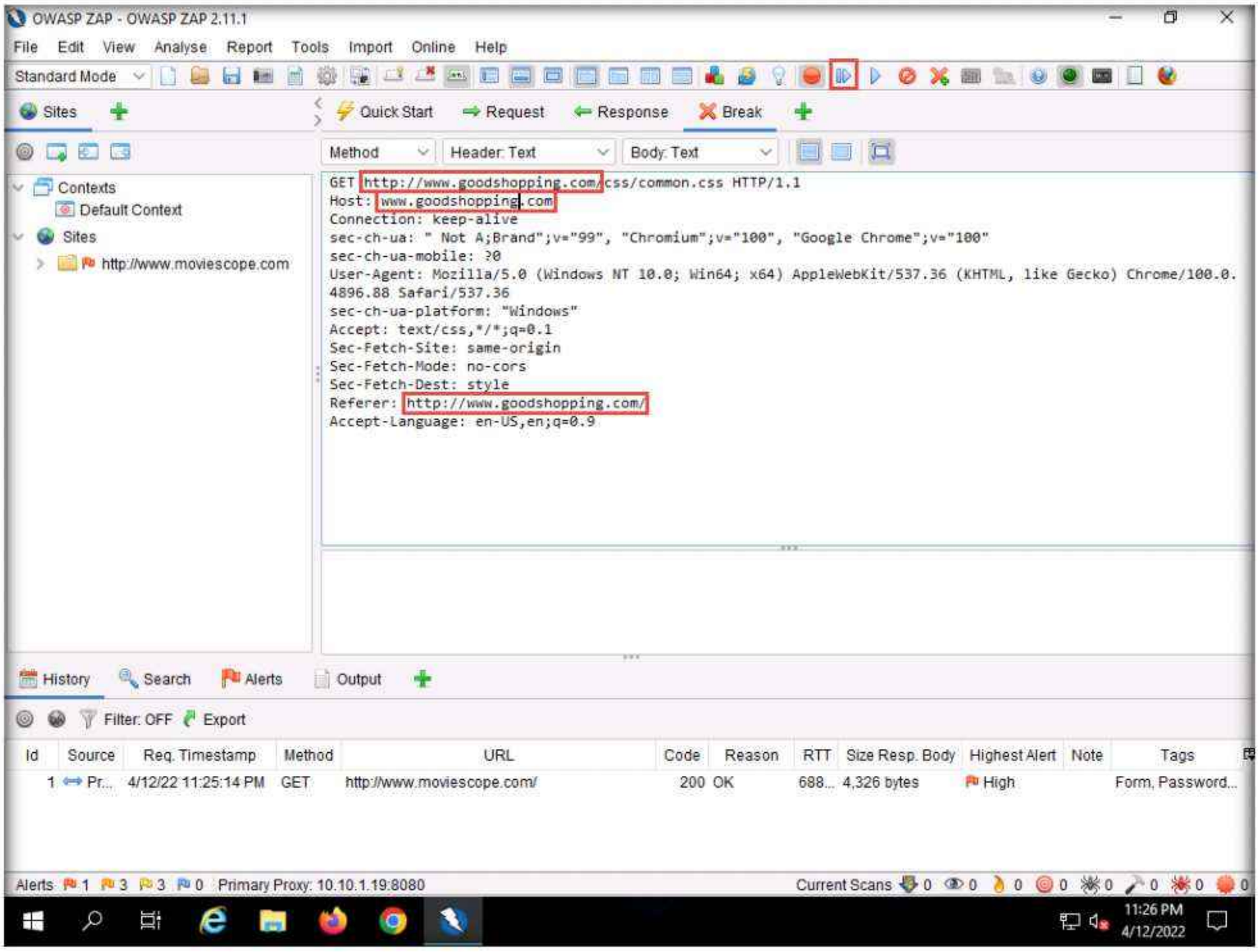
24. A **HTTP response** appears; click the **Submit and step to next request or response** icon again on the toolbar.



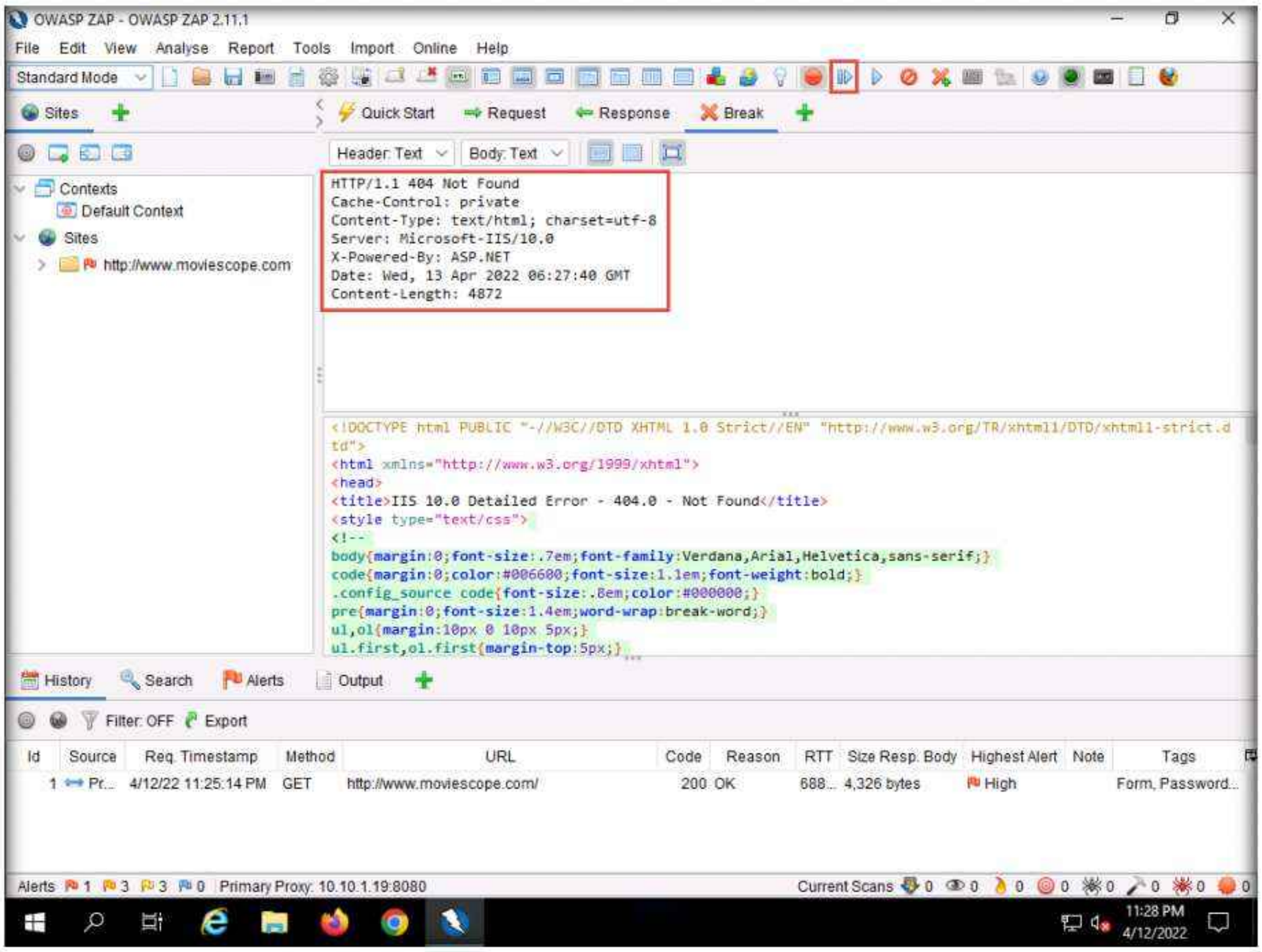
25. Now, in the **Break** tab, modify **www.moviescope.com** to **www.goodshopping.com** in all the captured GET requests.

    Note: If you find any URL starting with **https**, modify it to **http**.

26. Once you have modified the GET requests, click the **Submit and step to next request or response** icon on the toolbar to forward the traffic to the victim's machine.



27. In all the **HTTP Not Found** requests, click the **Submit and step to next request or response** icon on the toolbar to forward the traffic.



28. In a similar way, modify every **GET** request captured by **OWASP ZAP** until you see the **www.goodshopping.com** page in the victim's machine.

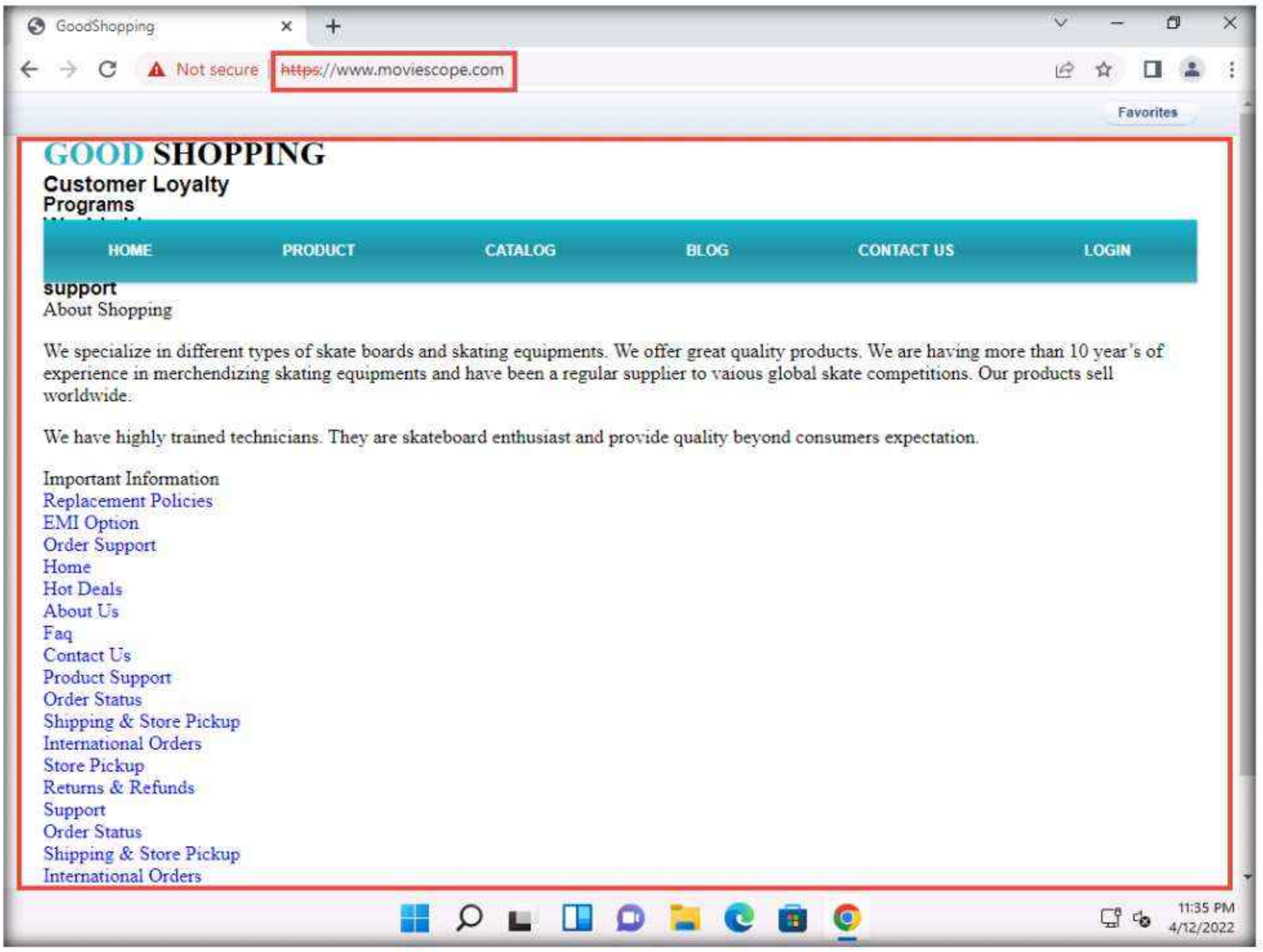
    Note: You will need to switch back and forth from the victim's machine to see the browser status while you do this.

    Note: If you do not receive any request or you see a blank break tab then switch to **Windows 11** machine and refresh the browser to capture the request again.

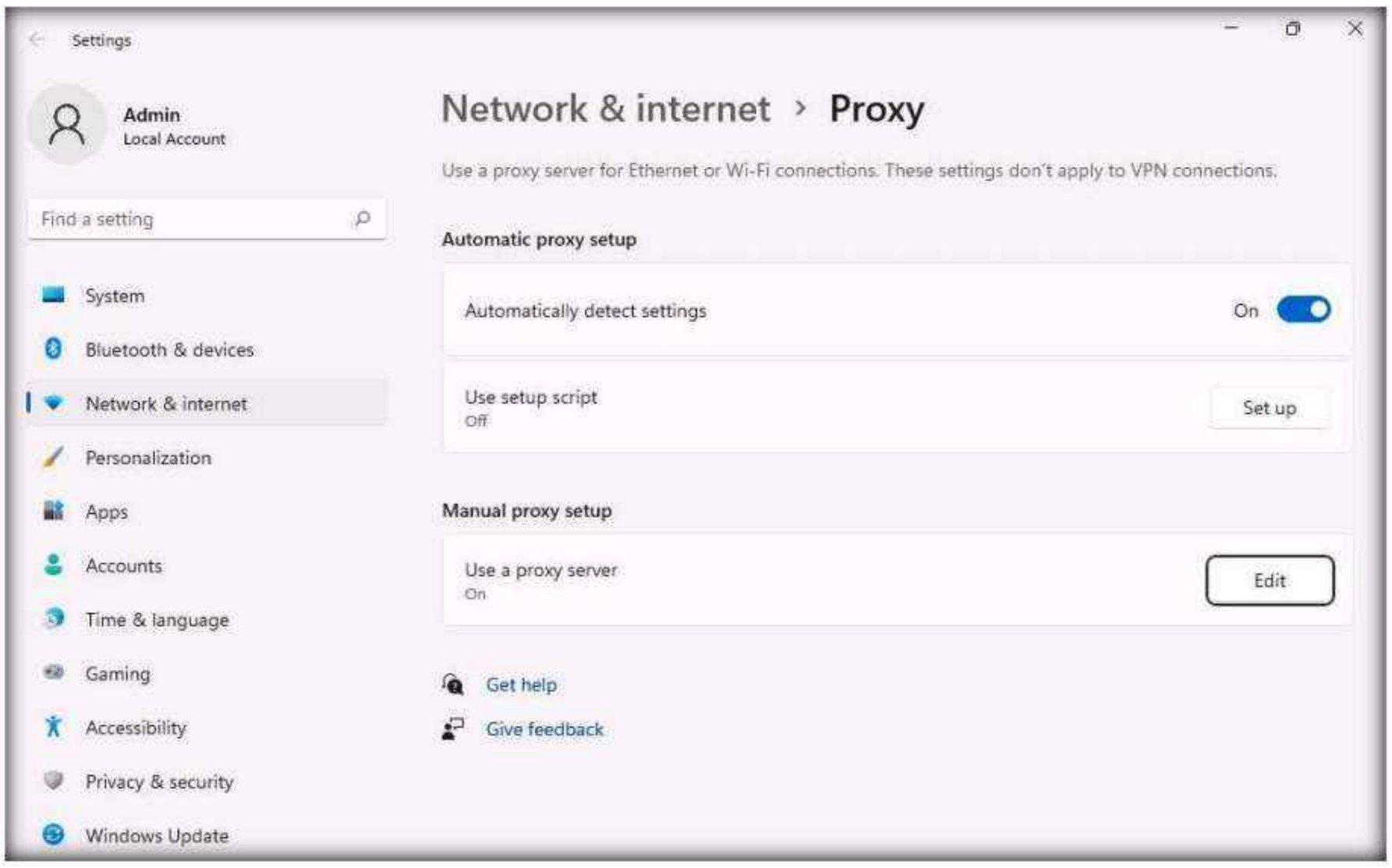
29. Now, switch to the victim's machine (**Windows 11**); the browser displays the website that the attacker wants the victim's machine to see (in this example, **www.goodshopping.com**).

    Note: It takes multiple iterations to open the Good Shopping site in the victim's machine.

30. The victim has navigated to **www.moviescope.com**, but now sees **www.goodshopping.com**; while the address bar displays **www. moviescope.com**, the window displays **www.goodshopping.com**.



31. Now, we shall change the proxy settings back to the default settings. To do so, perform **Steps 4-6** again.
32. In the **Settings** window, under the **Manual proxy setup** section in the right-pane, click the **Edit** button.



33. **Edit proxy server** window appears, under the **Use a proxy server** option, click the **On** button to switch it **Off** and click **Save**.

34. This concludes the demonstration of performing session hijacking using ZAP.
35. Close all open windows and document all the acquired information.
36. Turn off the **Windows Server 2019** virtual machine.

Task 2: Intercept HTTP Traffic using bettercap

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the middle (MITM) attacks. In an MITM attack, the attacker places himself/herself between the authorized client and the webserver so that all information traveling in either direction passes through them.

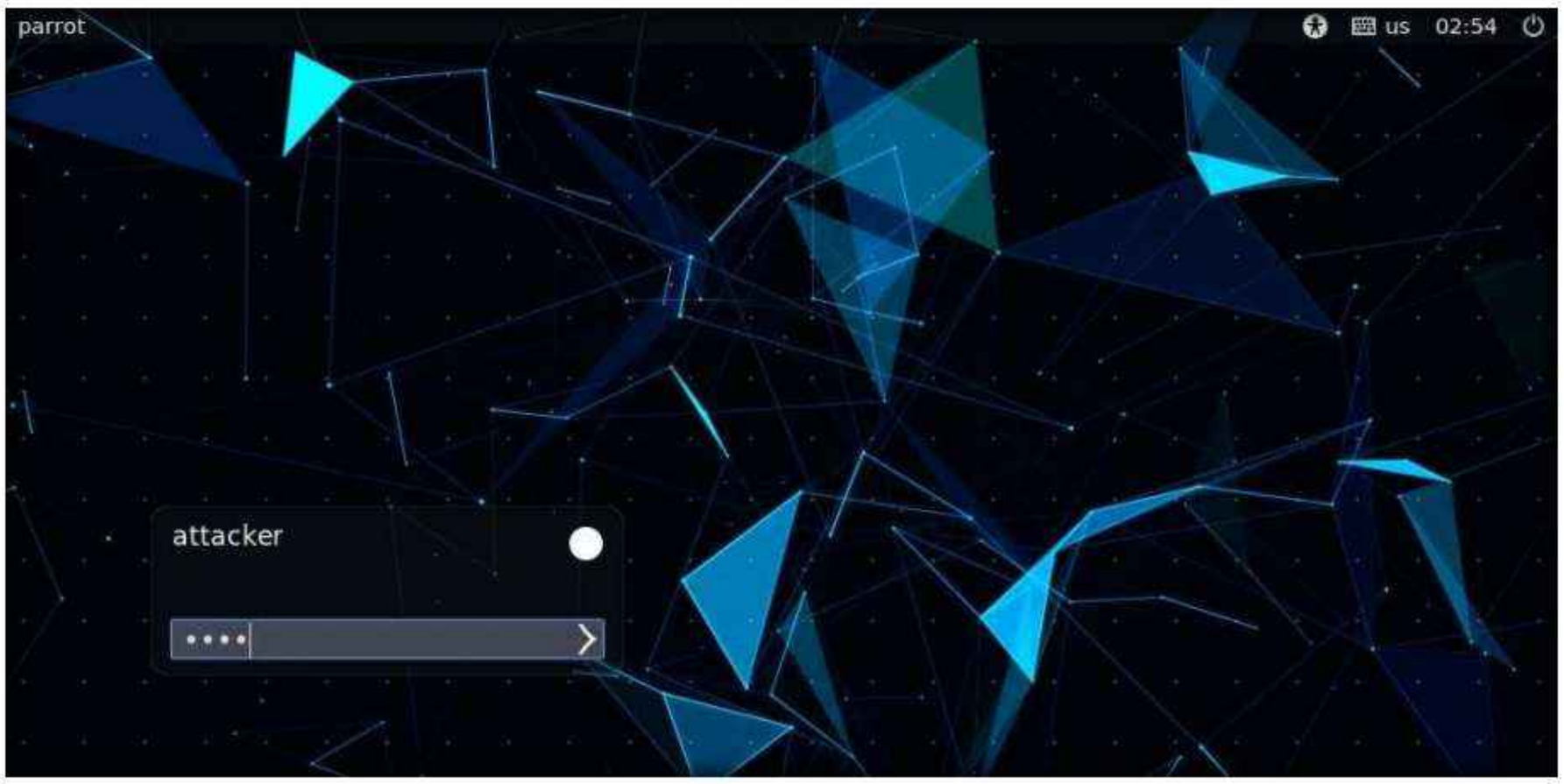
An ethical hacker or a penetration tester, you must know how MITM attacks work, so that you can protect your organization's sensitive information from them.

bettercap is a powerful, flexible, and portable tool created to perform various types of MITM attacks against a network; manipulate HTTP, HTTPS, and TCP traffic in real-time; sniff for credentials; etc.

Here, we will use the bettercap tool to intercept HTTP traffic on the target system.

Note: Ensure that the **Windows 11** virtual machine is running.

1. Turn on to the **Parrot Security** virtual machine.
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.



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

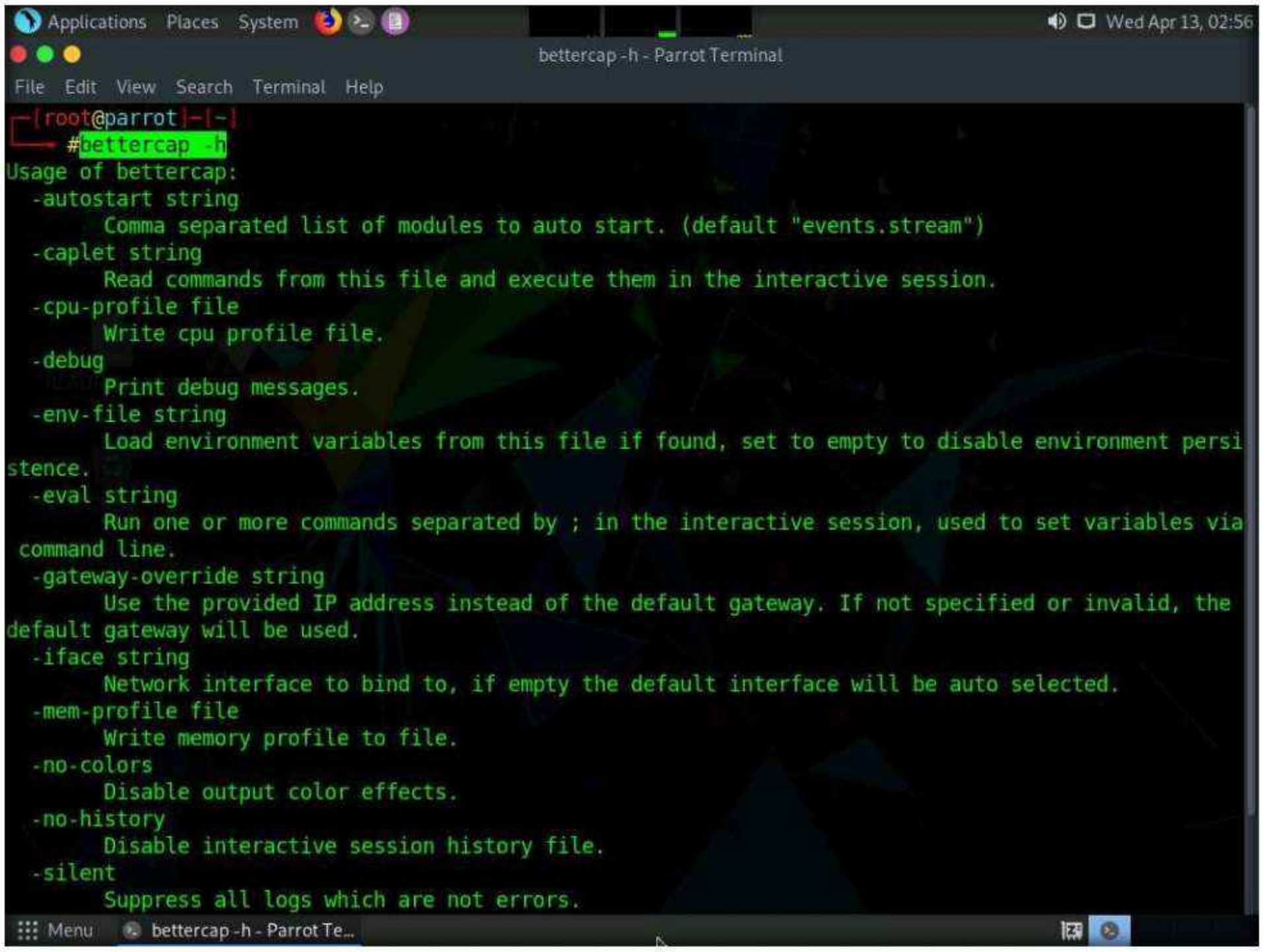
   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

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

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

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. In the terminal window; type **bettercap -h** and press **Enter**.

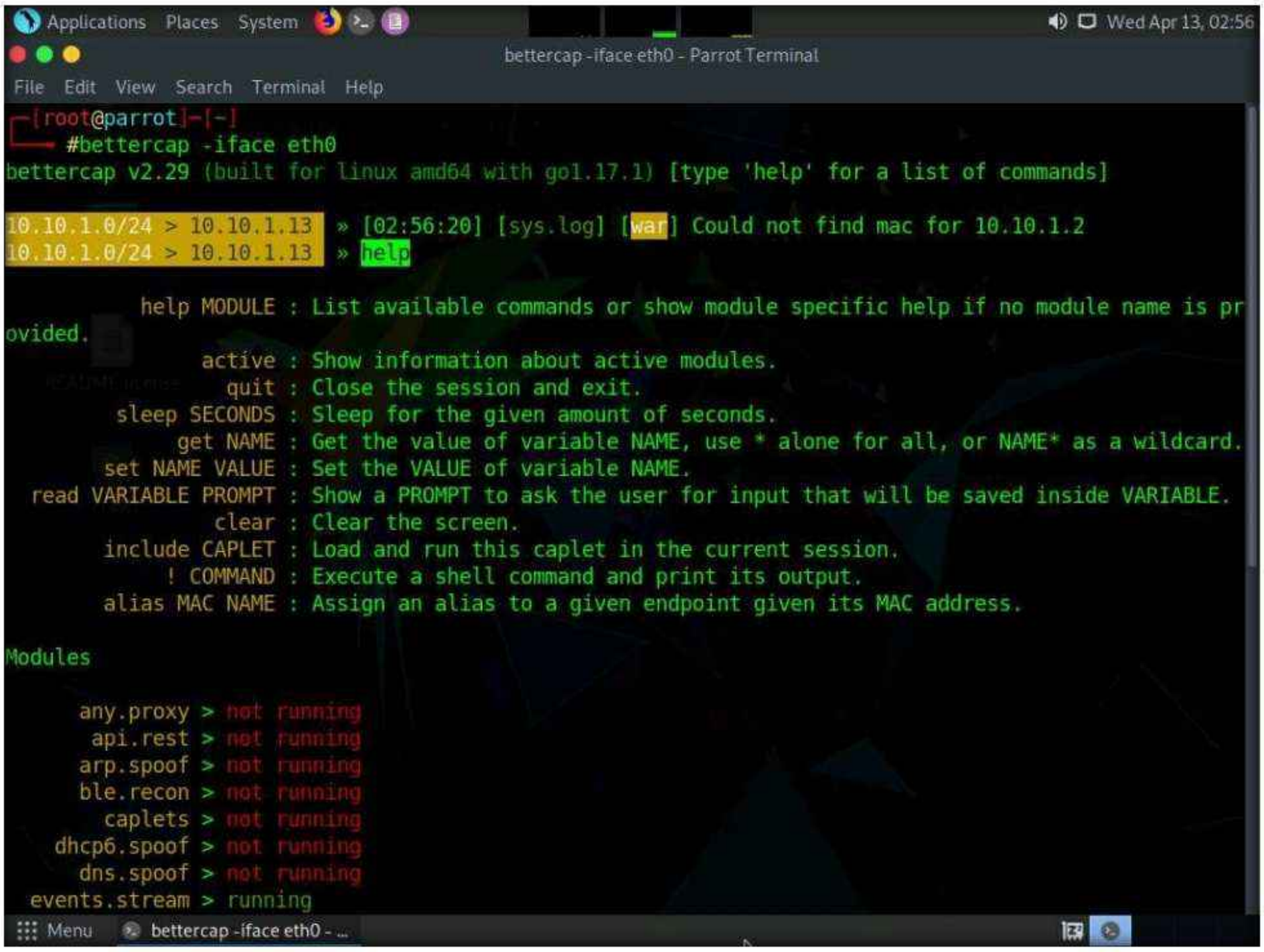
   Note: In this command, **-h**: requests a list of the available options.



8. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

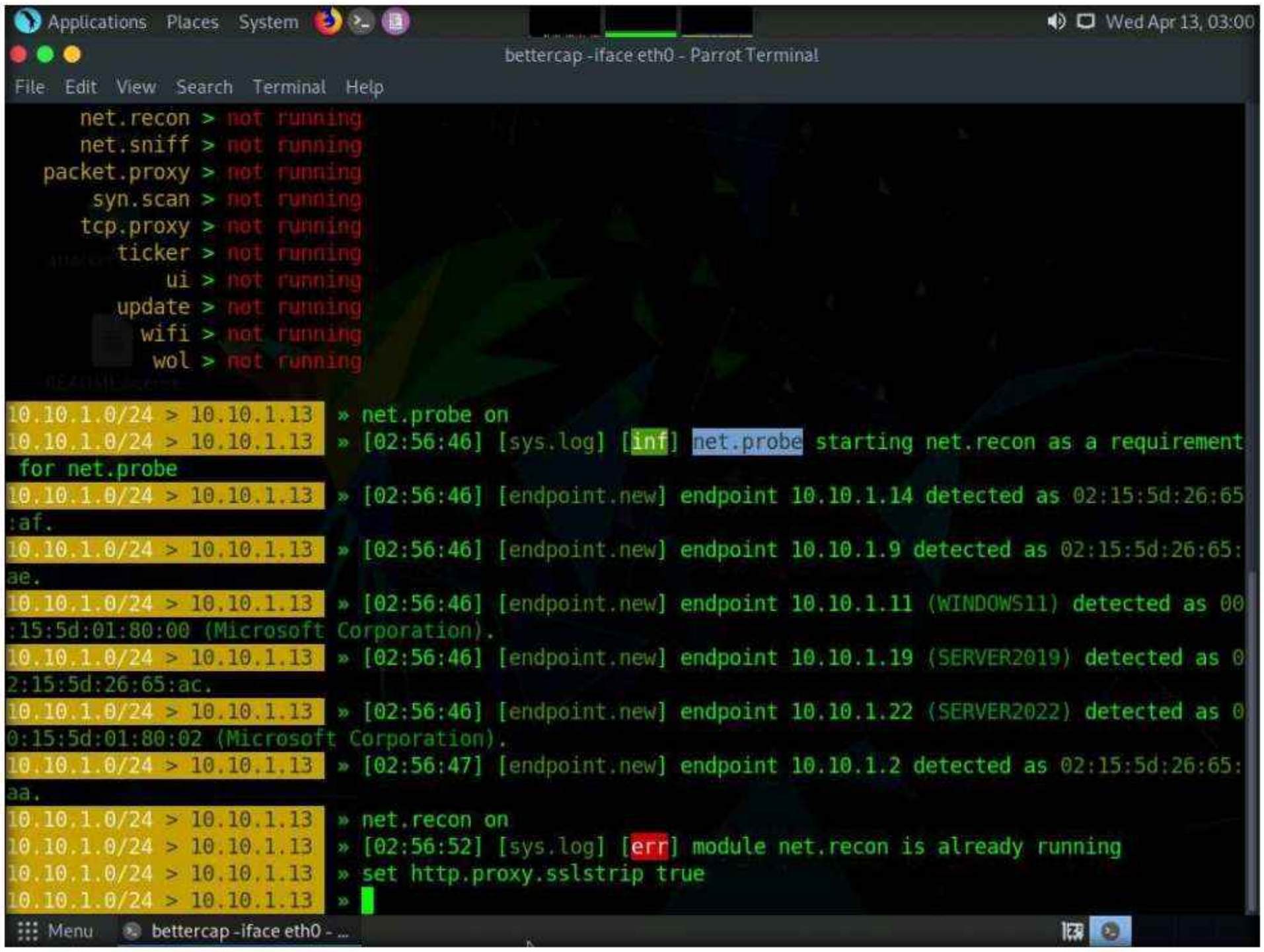
   Note: **-iface**: specifies the interface to bind to (in this example, **eth0**).

9. Type **help** and press **Enter** to view the list of available modules in bettercap.

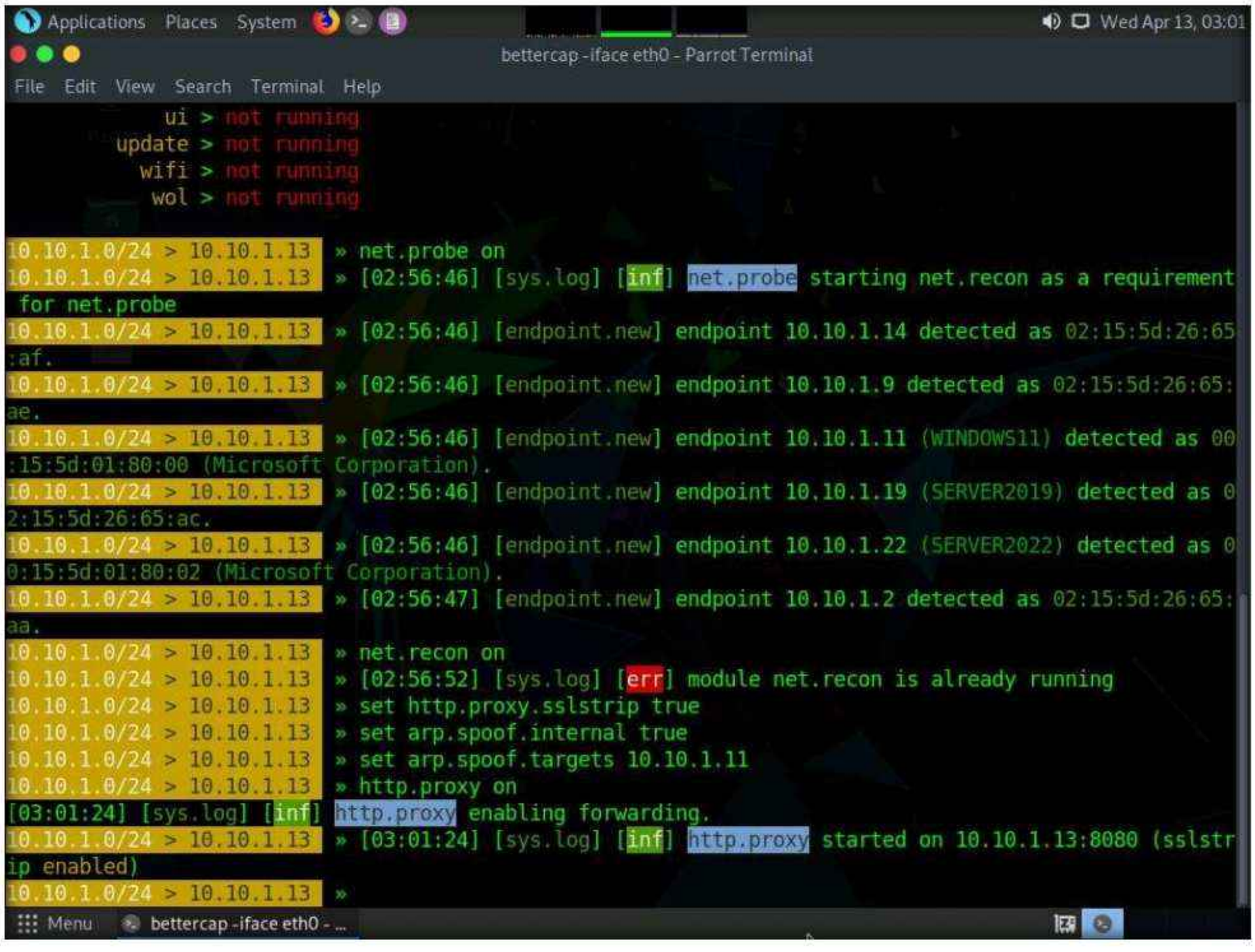


10. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.
11. Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

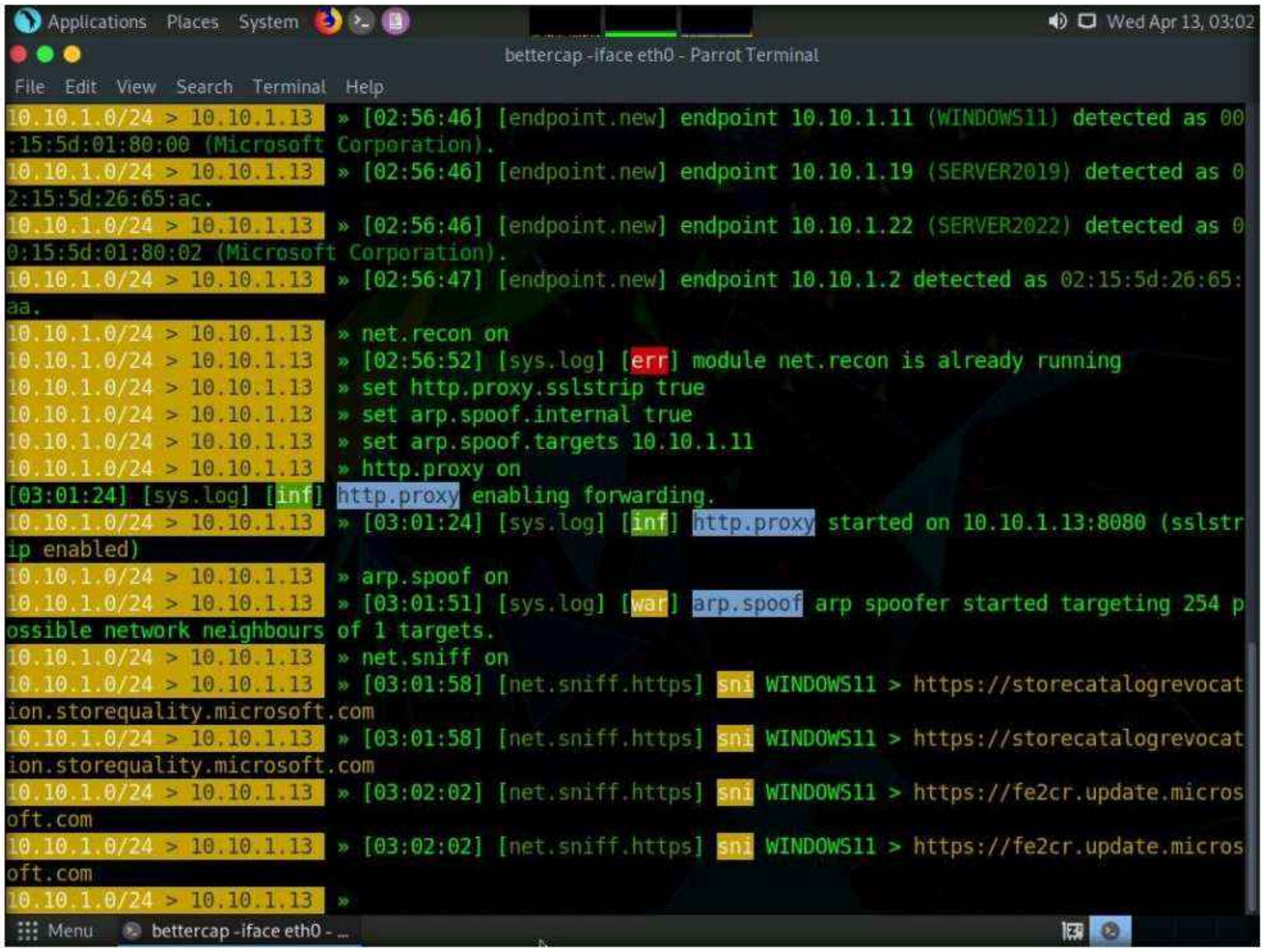
    Note: The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.
12. Type **set http.proxy.sslstrip true** and press **Enter**. This module enables SSL stripping.



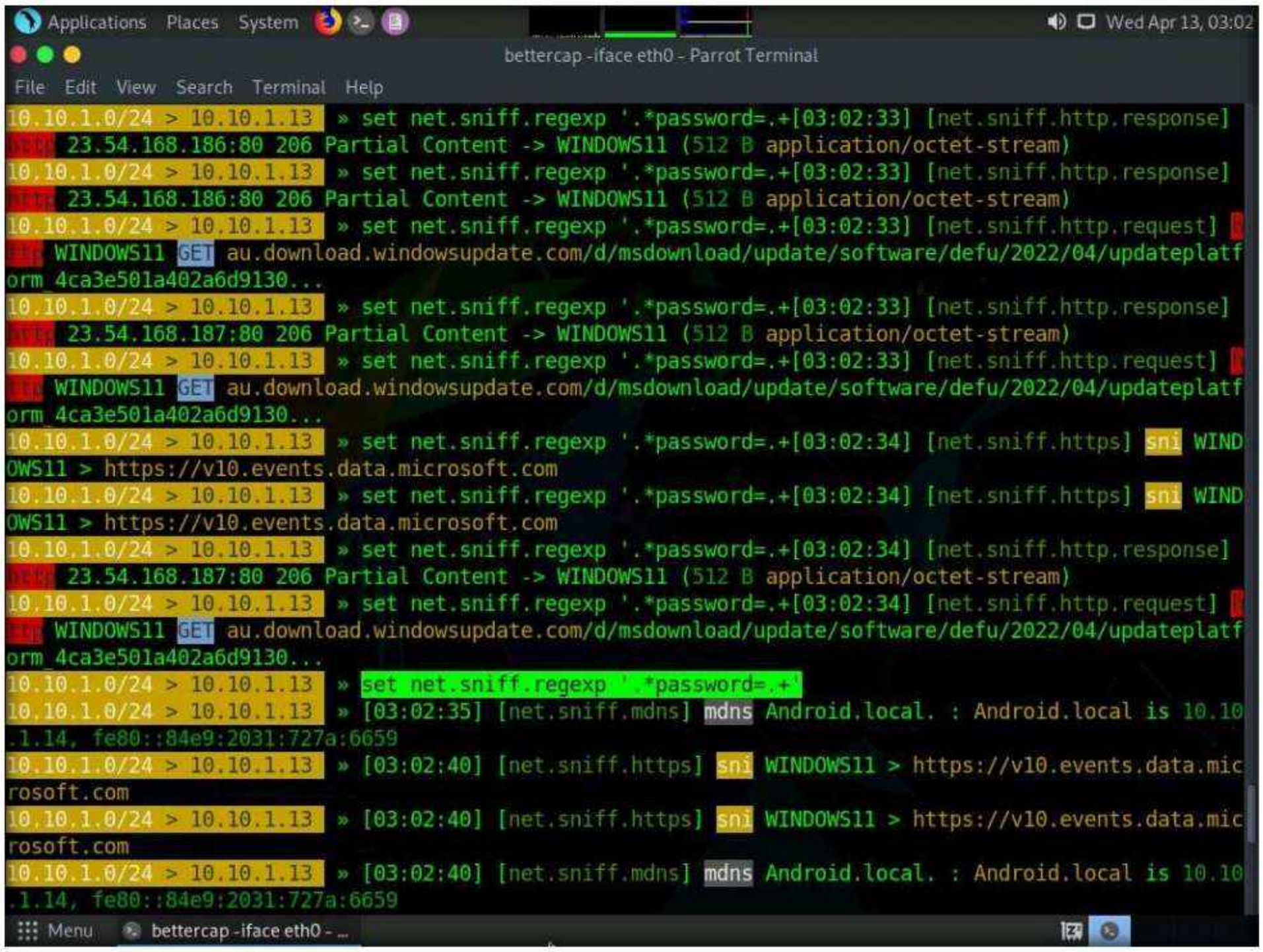
13. Type **set arp.spoof.internal true** and press **Enter**. This module spoofs the local connections among computers of the internal network.
14. Type **set arp.spoof.targets 10.10.1.11** and press **Enter**. This module spoofs the IP address of the target host.
15. Type **http.proxy on** and press **Enter**. This module initiates http proxy.



16. Type **arp.spoof on** and press **Enter**. This module initiates arp spoofing.
17. Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.

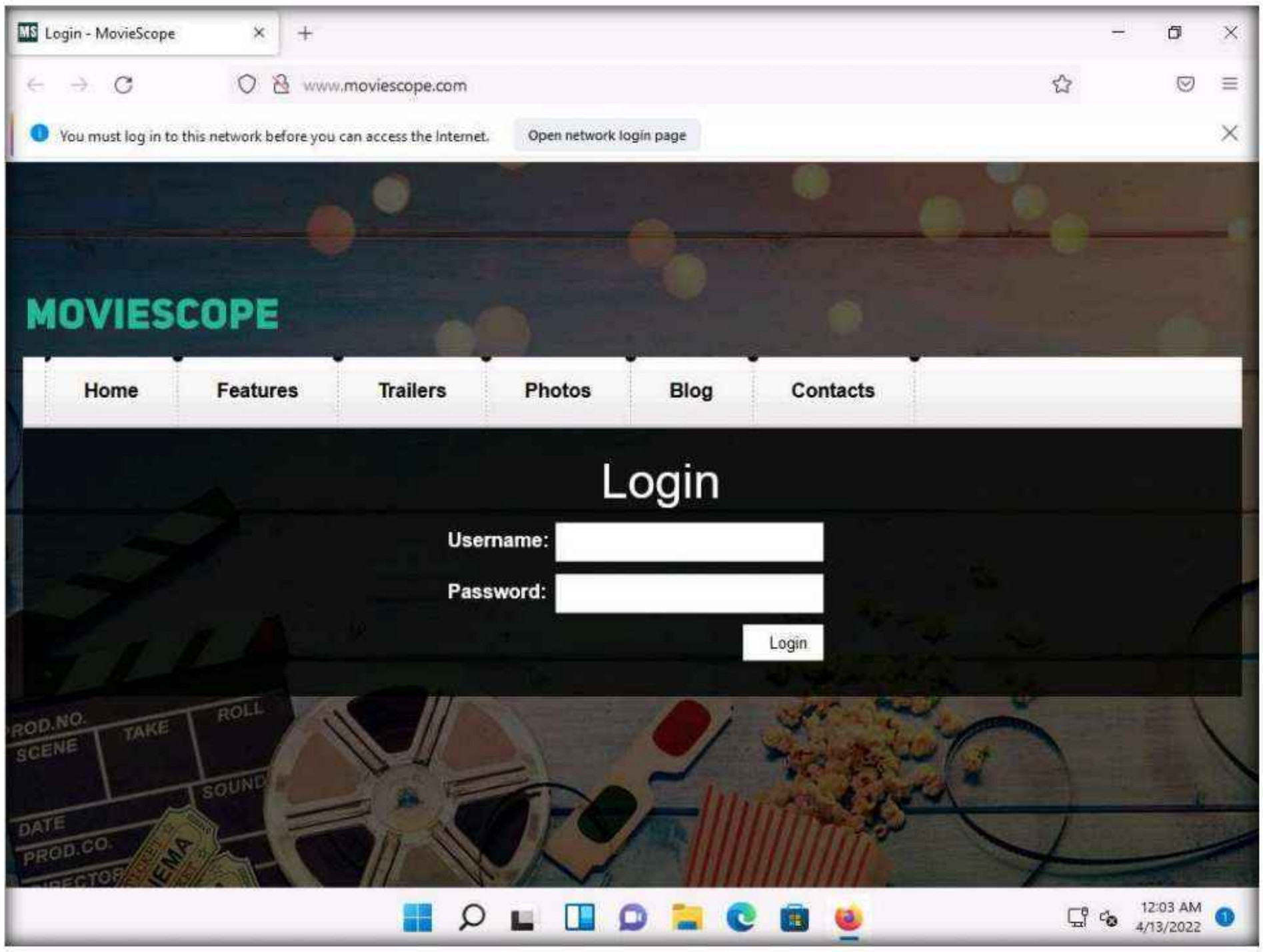


18. Type **set net.sniff.regexp '.*password=.+'** and press **Enter**. This module will only consider the packets sent with a payload matching the given regular expression (in this case, **'.*password=.+'**).

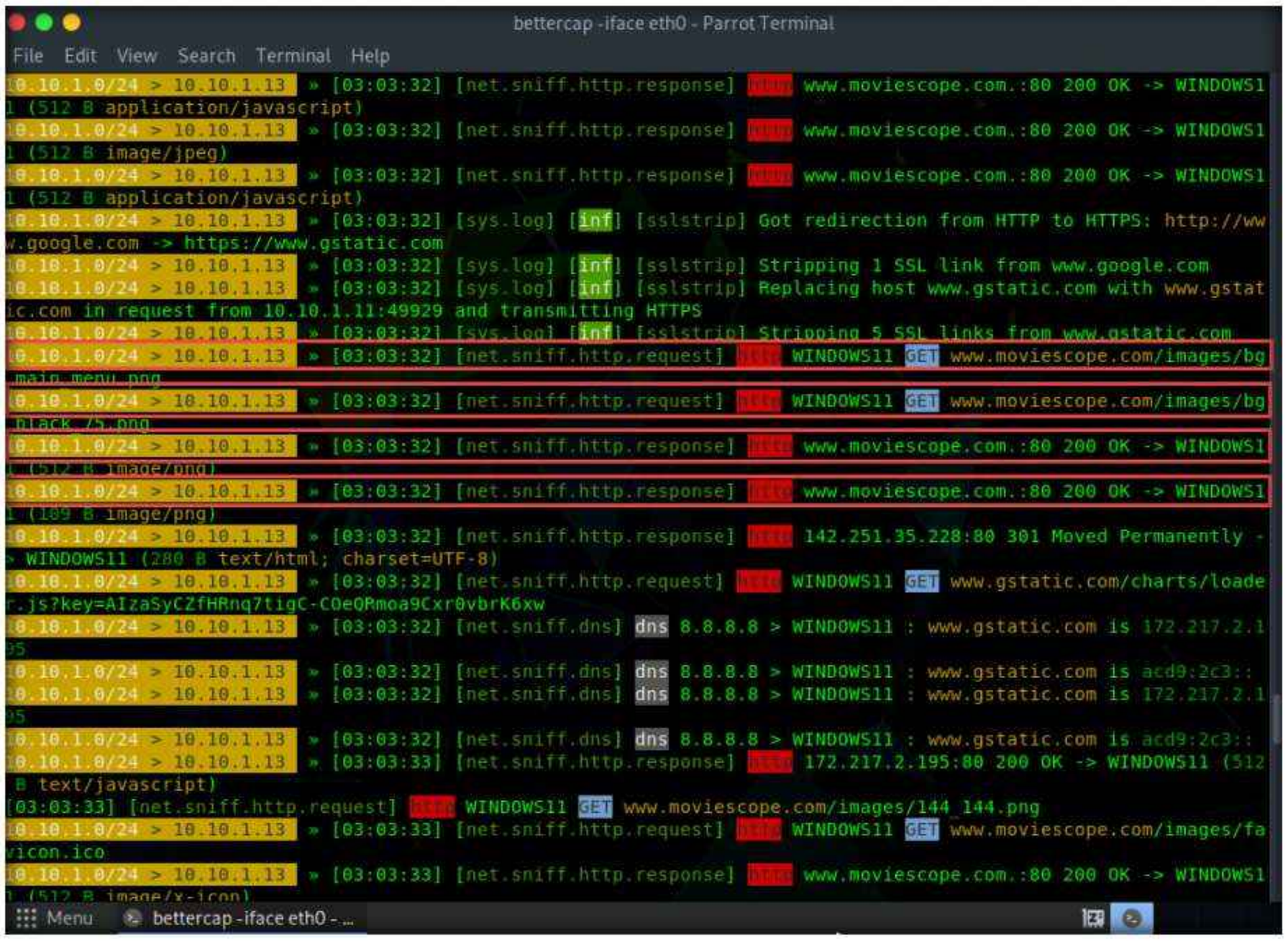


19. You can observe that bettercap starts sniffing network traffic on target machine **Windows 11**.

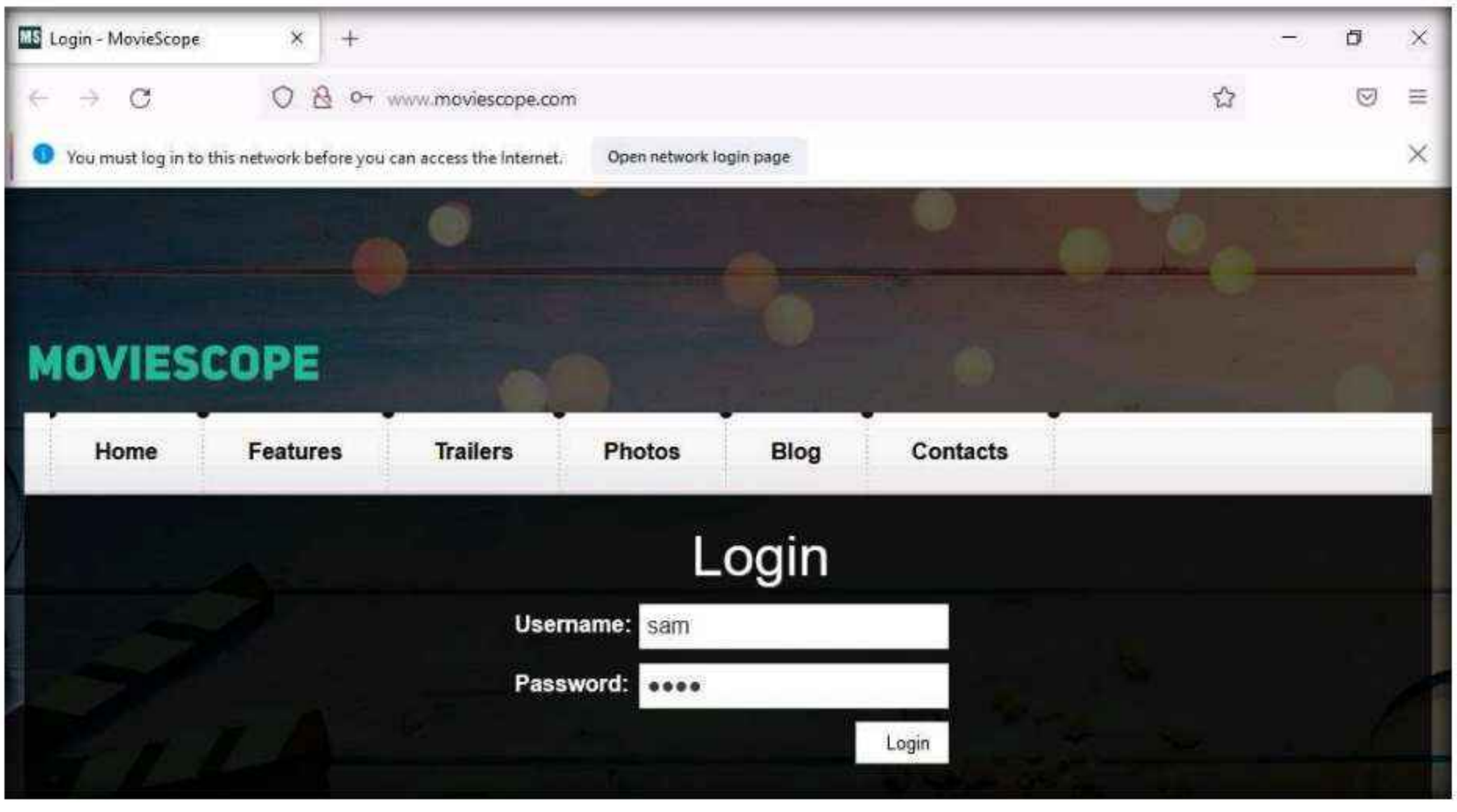
20. Now, switch to the **Windows 11** virtual machine. Open any web browser (in this case, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://www.moviescope.com** and press **Enter**.



21. Switch back to the **Parrot Security** virtual machine. You can observe that bettercap has sniffed the website browsed by the victim on the target system, as shown in the screenshot.

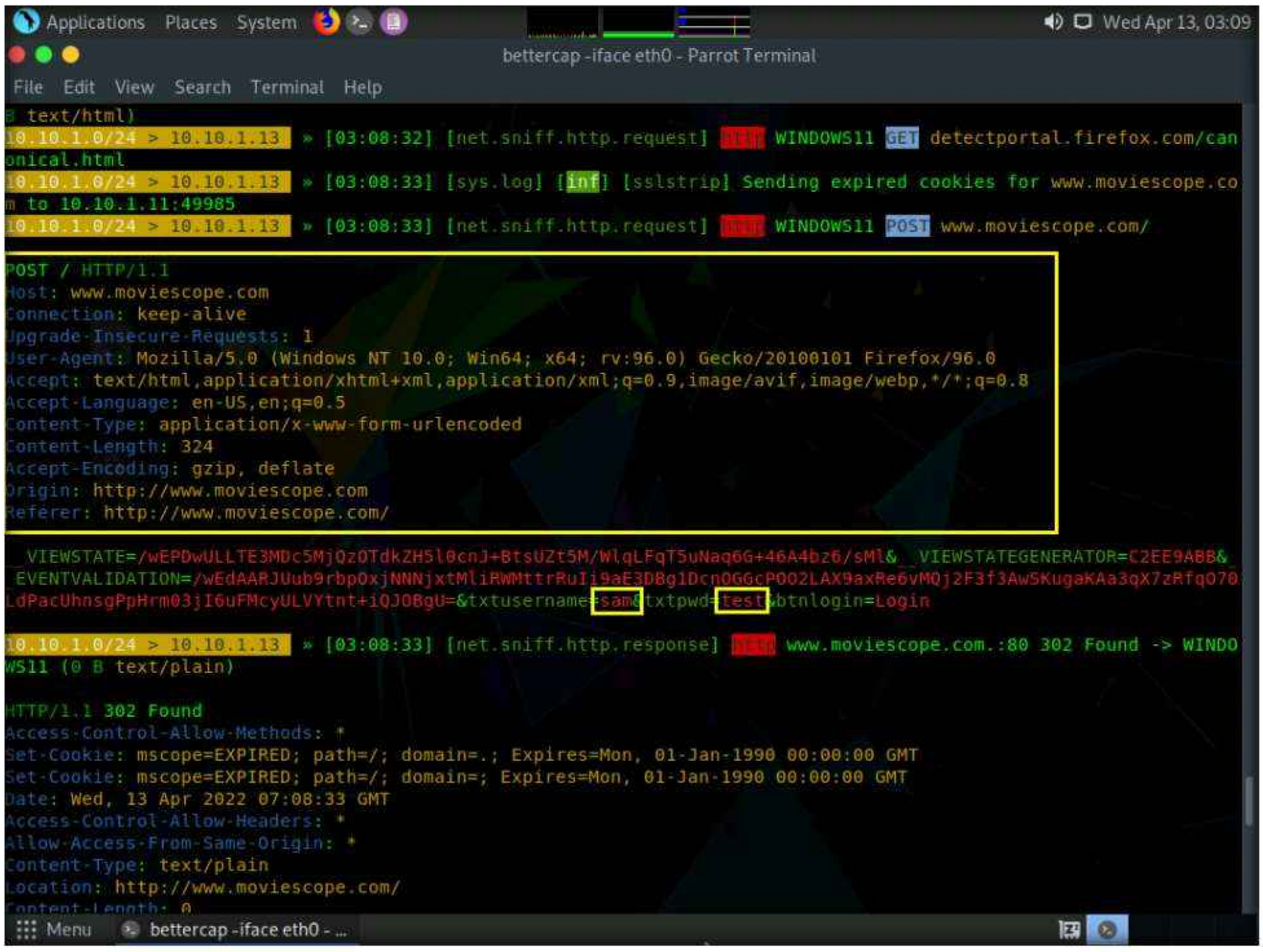


22. Switch to the **Windows 11** virtual machine. On the **MovieScope** website, enter any credentials (here, **sam/test**) and press **Enter** to log in.

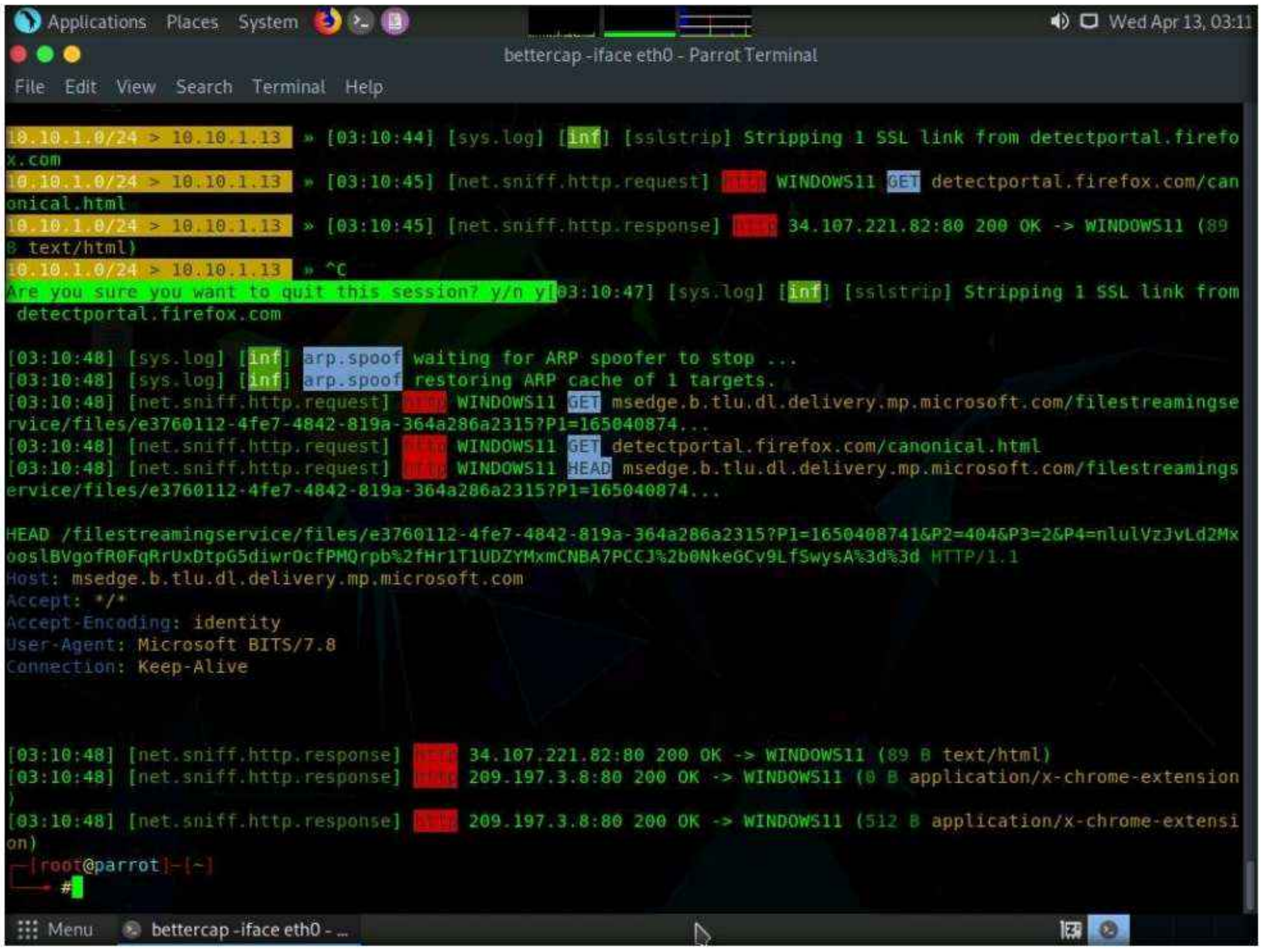


23. Switch to the **Parrot Security** virtual machine. You can observe the details of both the browsed website and the credentials obtained in plain text, as shown in the screenshot.

    Note: bettercap collects all http logins used by routers, servers, and websites that do not have SSL enabled. In this task, we are using **www.moviescope.com** for demonstration purposes, as it is http-based. To use bettercap to sniff network traffic from https-based websites, you must enable the SSL strip module by issuing the command **set http.proxy.sslstrip true**.



24. After obtaining the credentials, press **Ctrl+C** to terminate bettercap. The credentials can be used to log in to the target user's account and obtain further sensitive information.
25. When the **Are you sure you want to quit this session?** message appears, press **y**, and then **Enter**.



26. This concludes the demonstration of how to intercept HTTP traffic using bettercap.
27. Close all open windows and document all the acquired information.
28. Turn off the **Parrot Security** virtual machine.

Task 3: Intercept HTTP Traffic using Hetty

Hetty is an HTTP toolkit for security research. It aims to become an open-source alternative to commercial software such as Burp Suite Pro, with powerful features tailored to the needs of the InfoSec and bug bounty communities. Hetty can be used to perform Machine-in-the-middle (MITM) attack, manually create/edit requests, and replay proxied requests for HTTP clients and further intercept requests and responses for manual review.

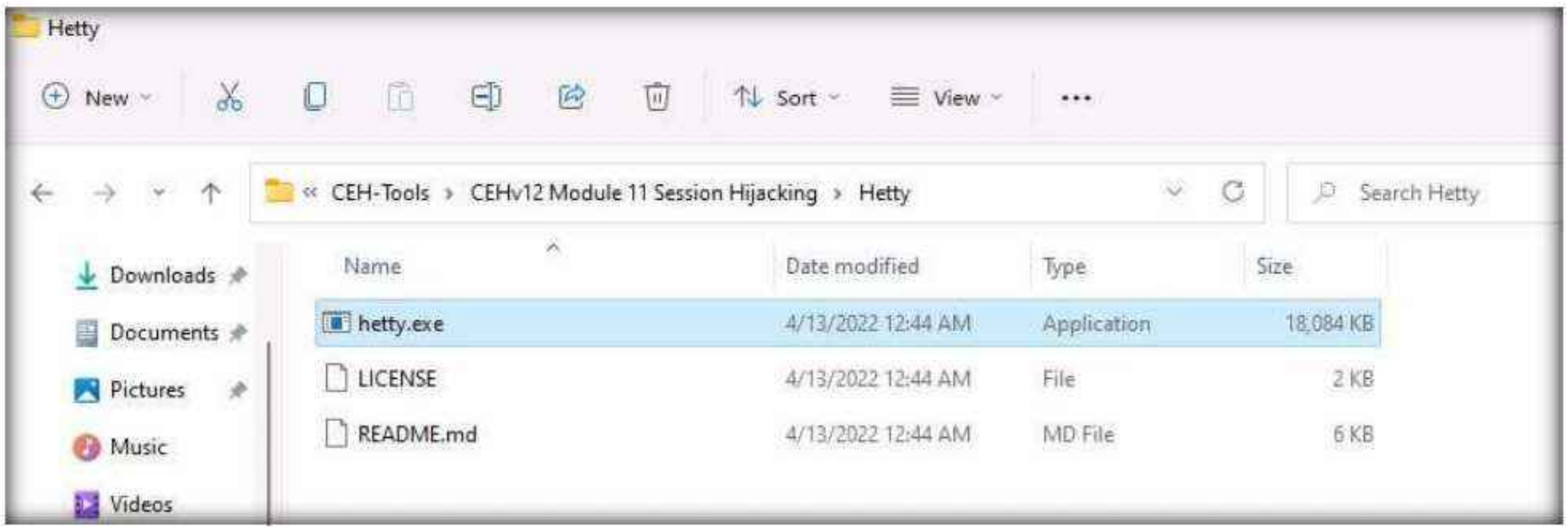
Here, we will use the Hetty tool to intercept HTTP traffic on the target system.

Note: Here, we will use **Windows 11** machine as an attacker machine and **Windows Server 2022** machine as a target machine.

1. Turn on the **Windows Server 2022** virtual machine.

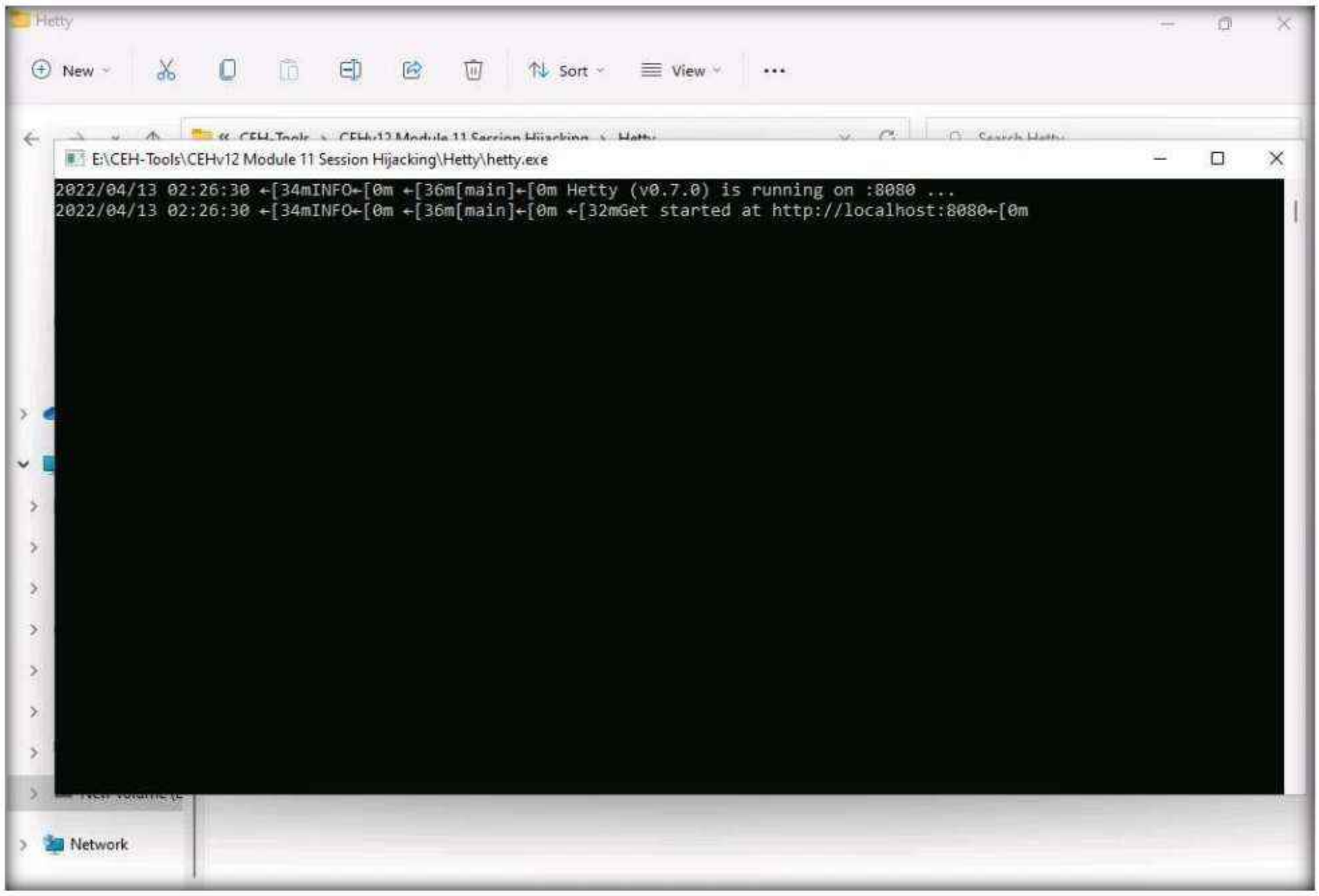
   Note: Ensure that the **Windows 11** virtual machine is running.

2. Switch to the **Windows 11** virtual machine. Navigate to **E:\CEH-Tools\CEHv12 Module 11 Session Hijacking\Hetty** and double-click **hetty.exe**.



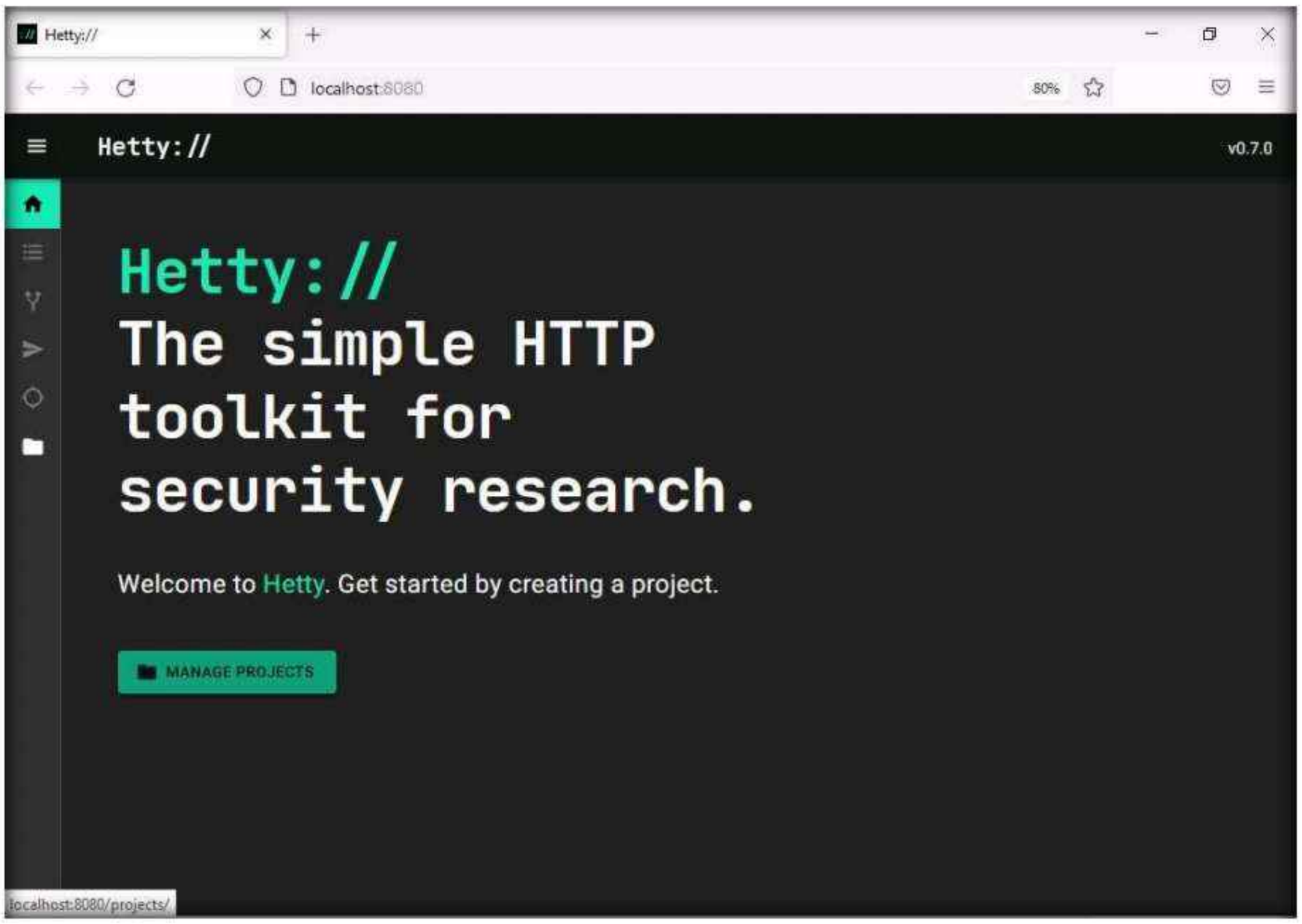
3. **Open File - Security Warning** window appears, click **Run**.

4. A **Command Prompt** window appears, and Hetty initializes.

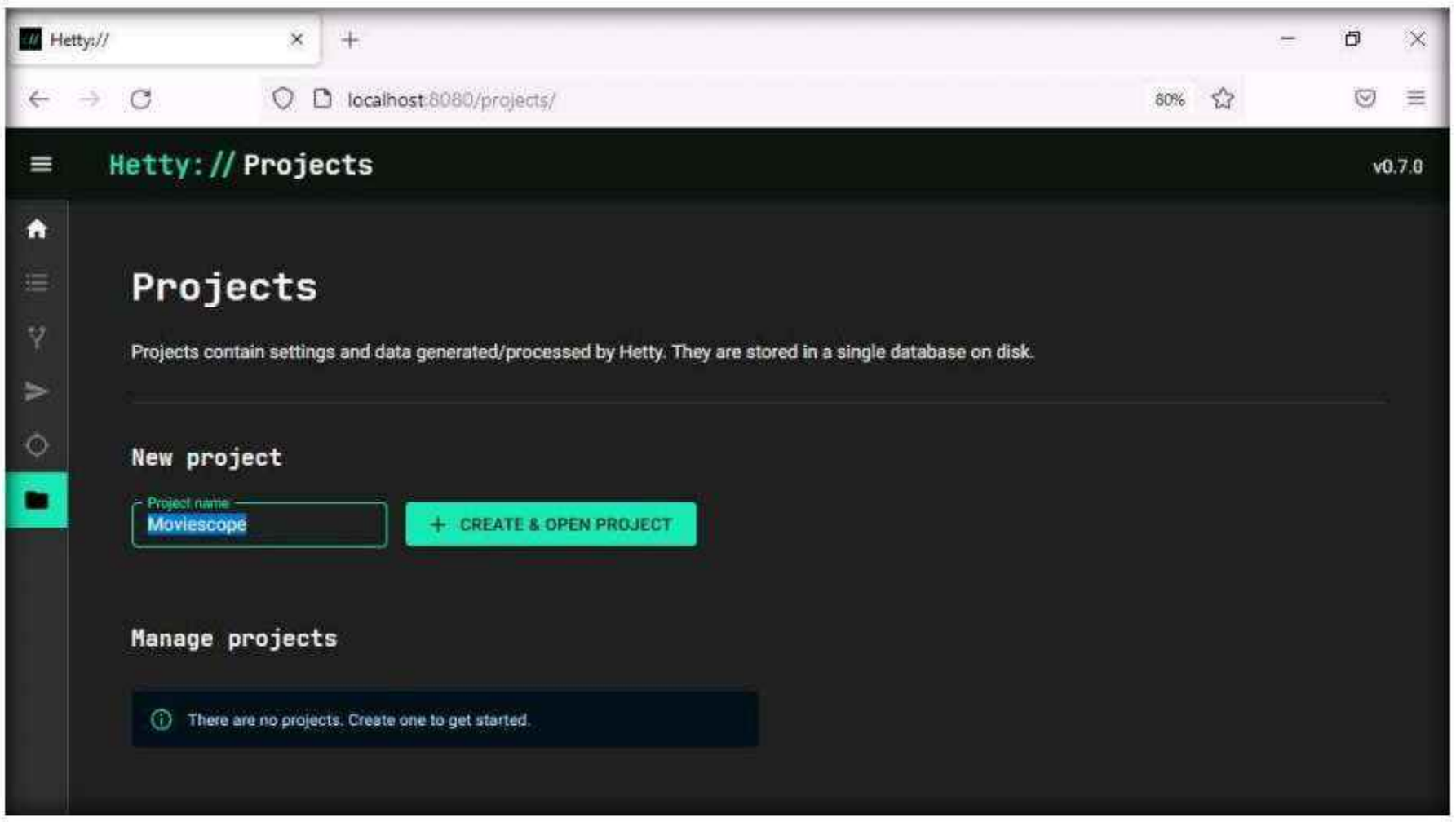


5. Now, minimize all the windows and launch any web browser (here, **Mozilla Firefox**).

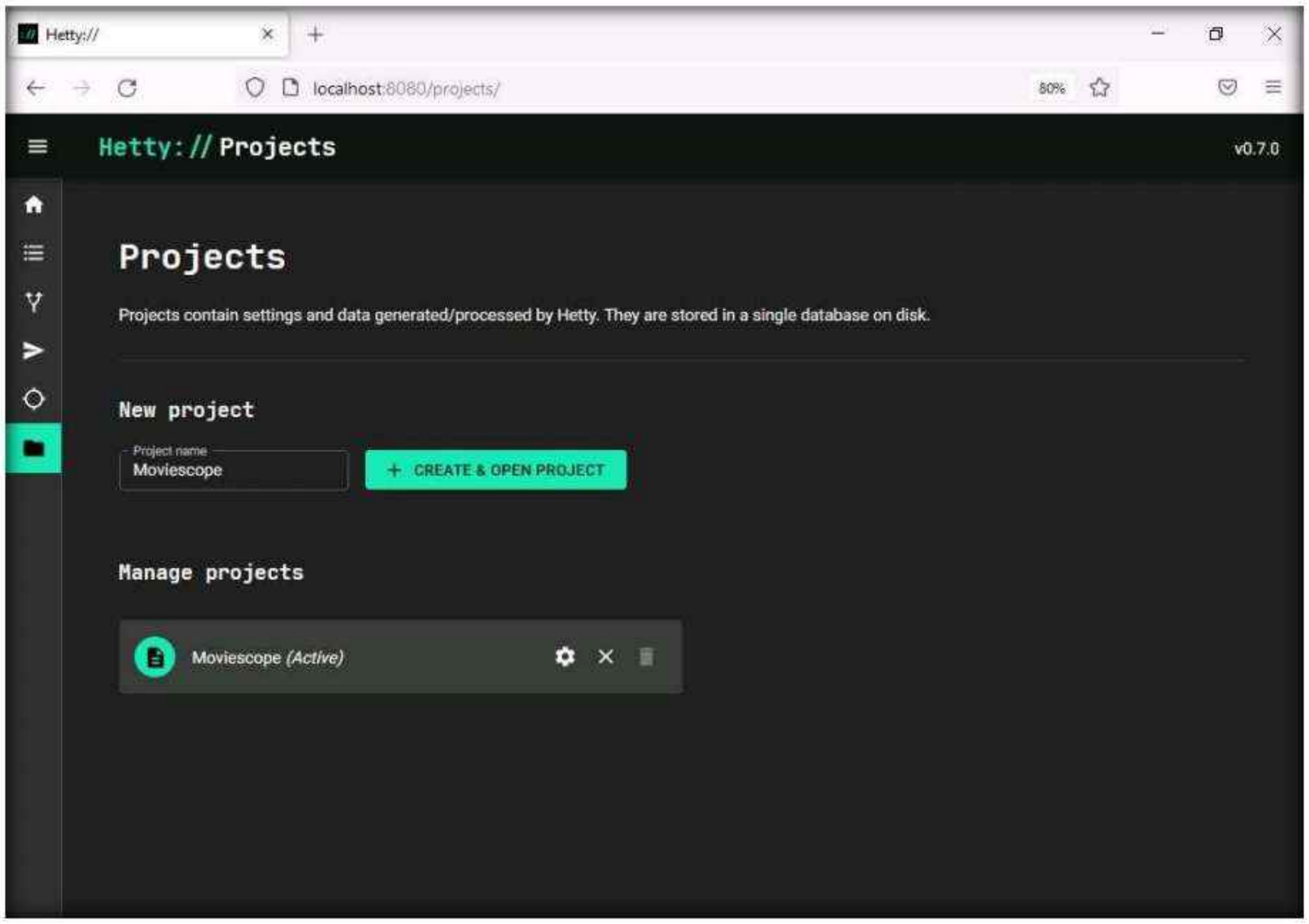
6. A browser window, in the address bar, type **http://localhost:8080** and press **Enter** to open Hetty dashboard.
7. In the Hetty dashboard, click **MANAGE PROJECTS** button.



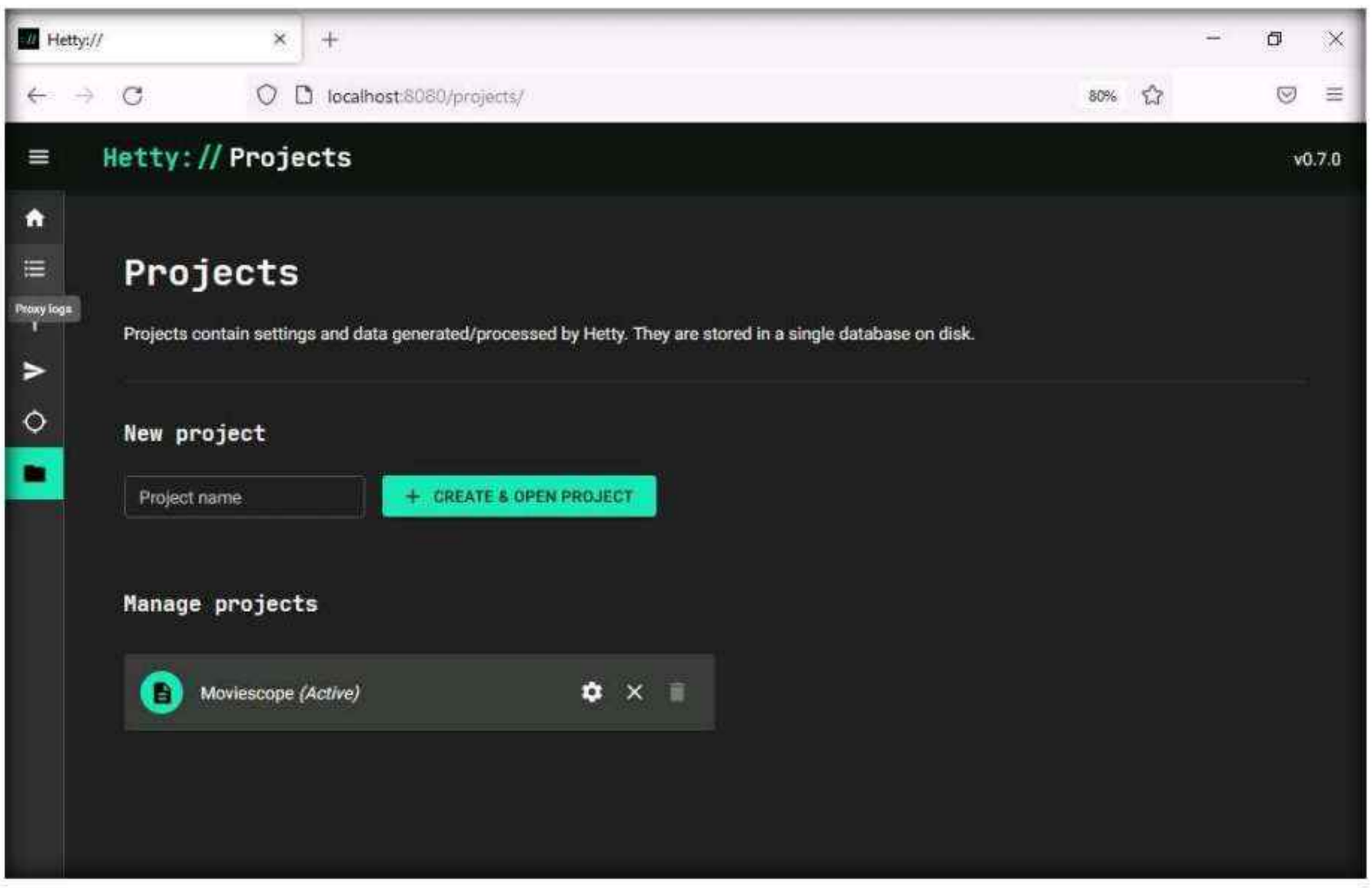
8. **Projects** page appears, type **Project name** as **Moviescope** under **New Project** section and click **+ CREATE & OPEN PROJECT** button.



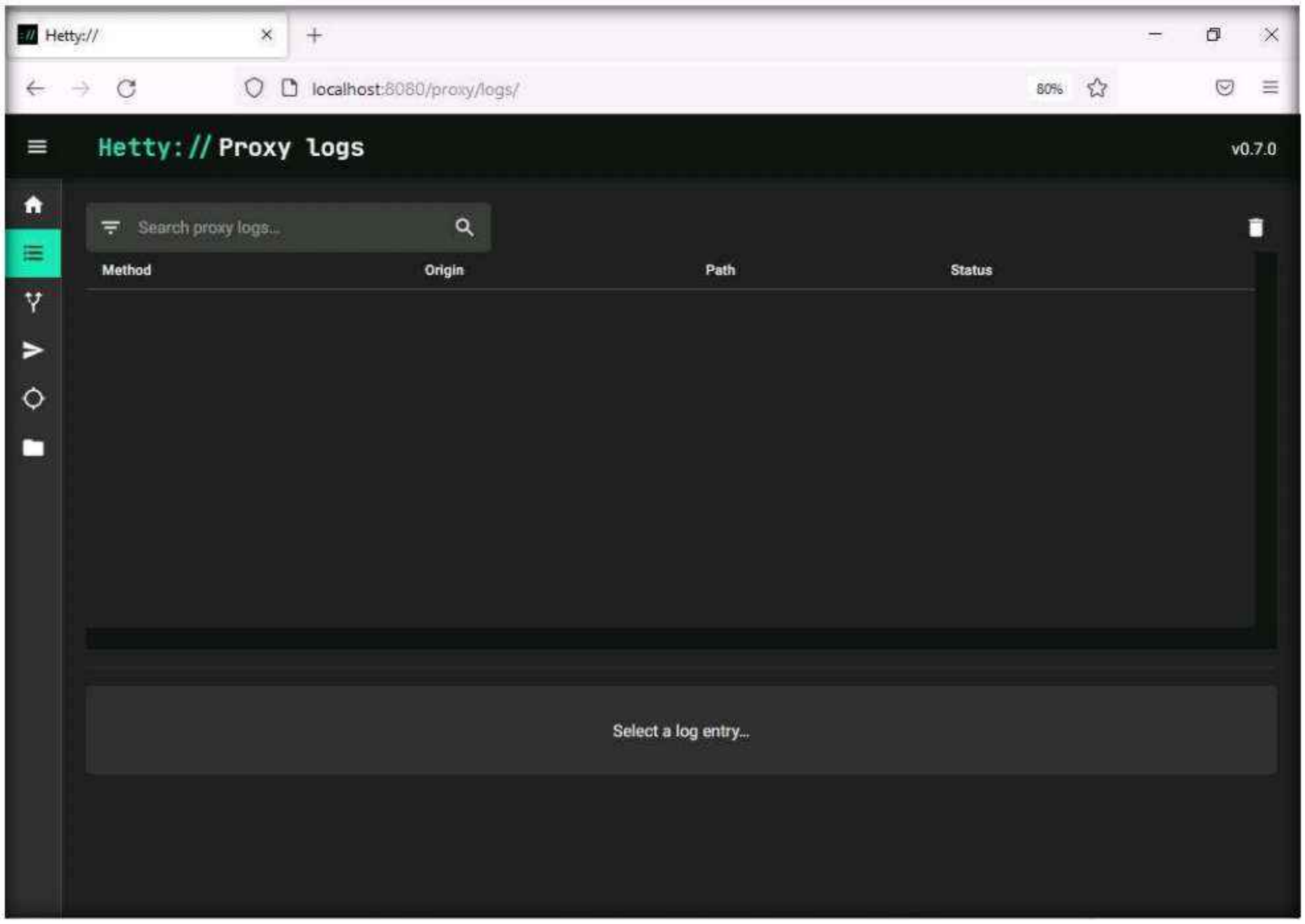
9. You can observe that a new project name **Moviescope** has been created under **Manage projects** section with a status as **Active**.



10. Click **Proxy logs** icon ( ) from the left-pane.



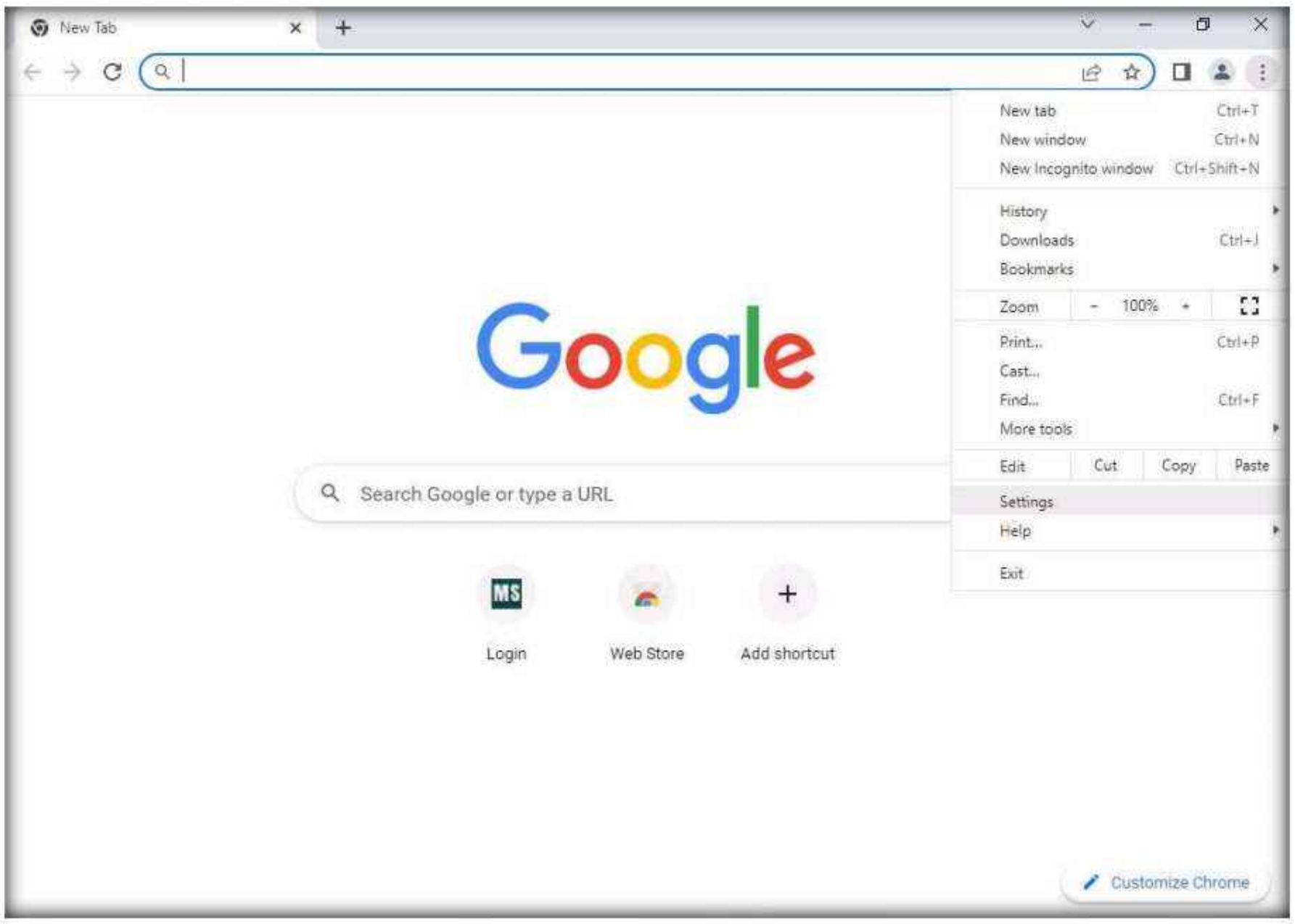
11. A **Proxy logs** page appears, as shown in the screenshot.



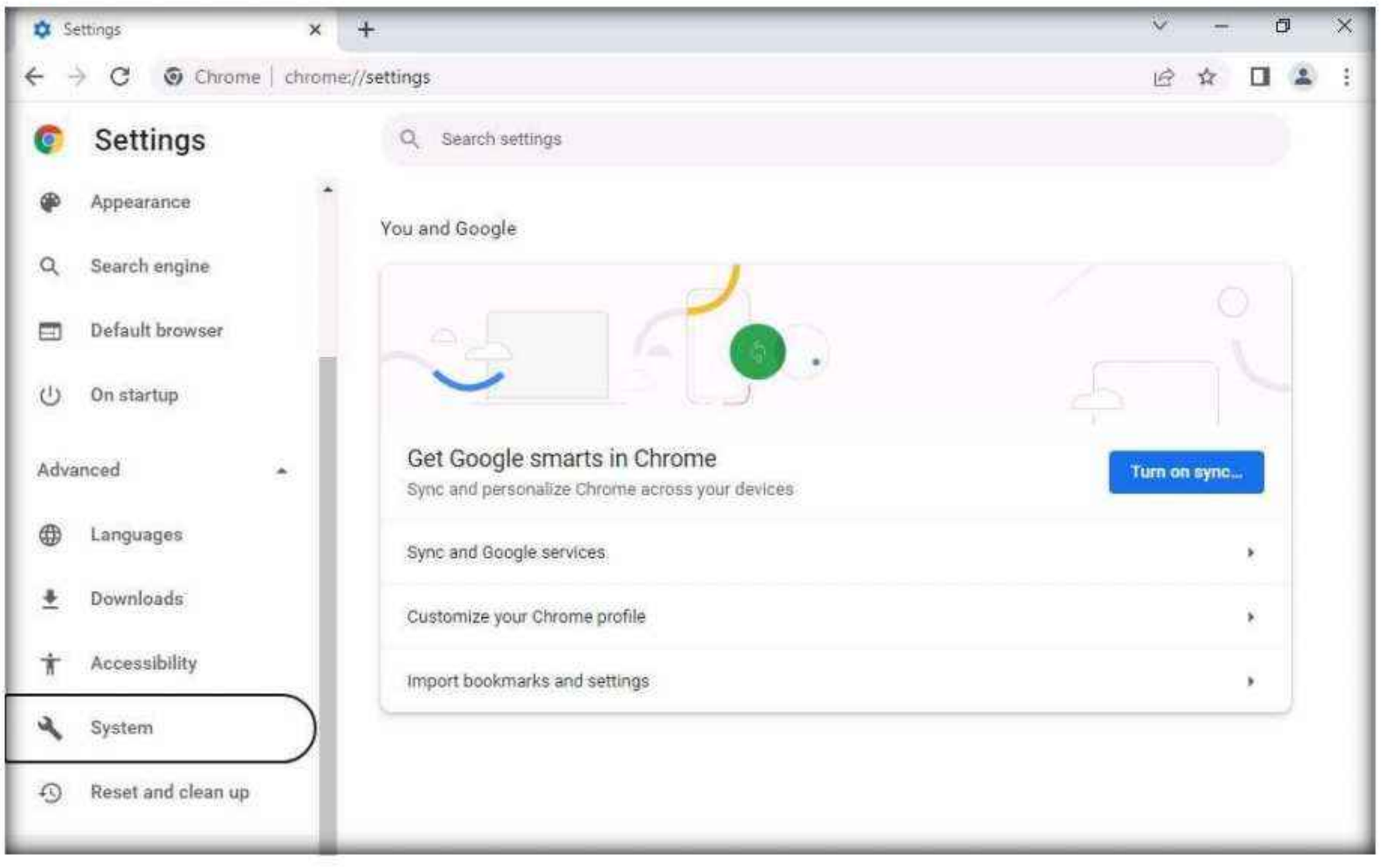
12. Now, switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

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

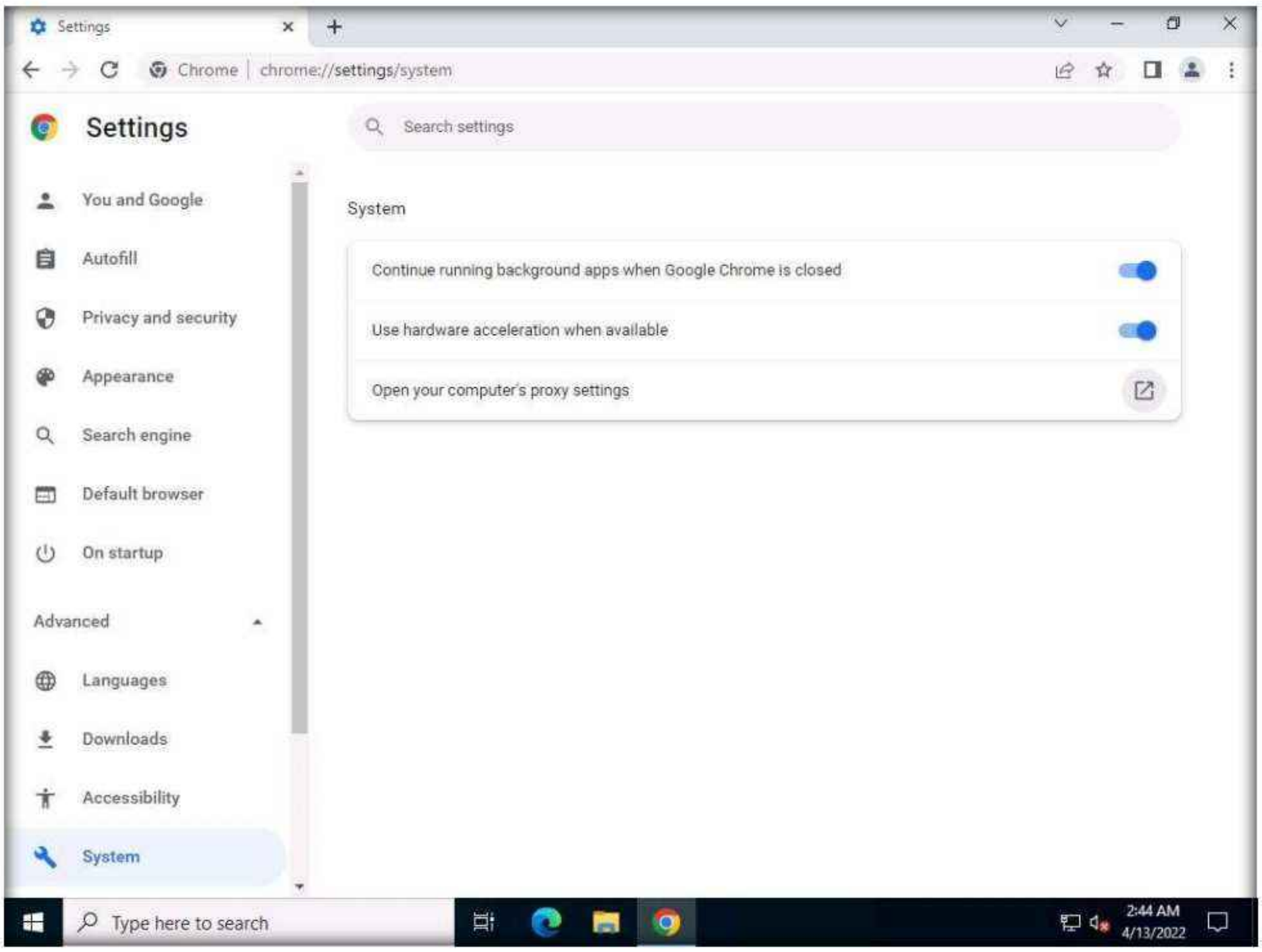
13. Open **Google Chrome** web browser, click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.



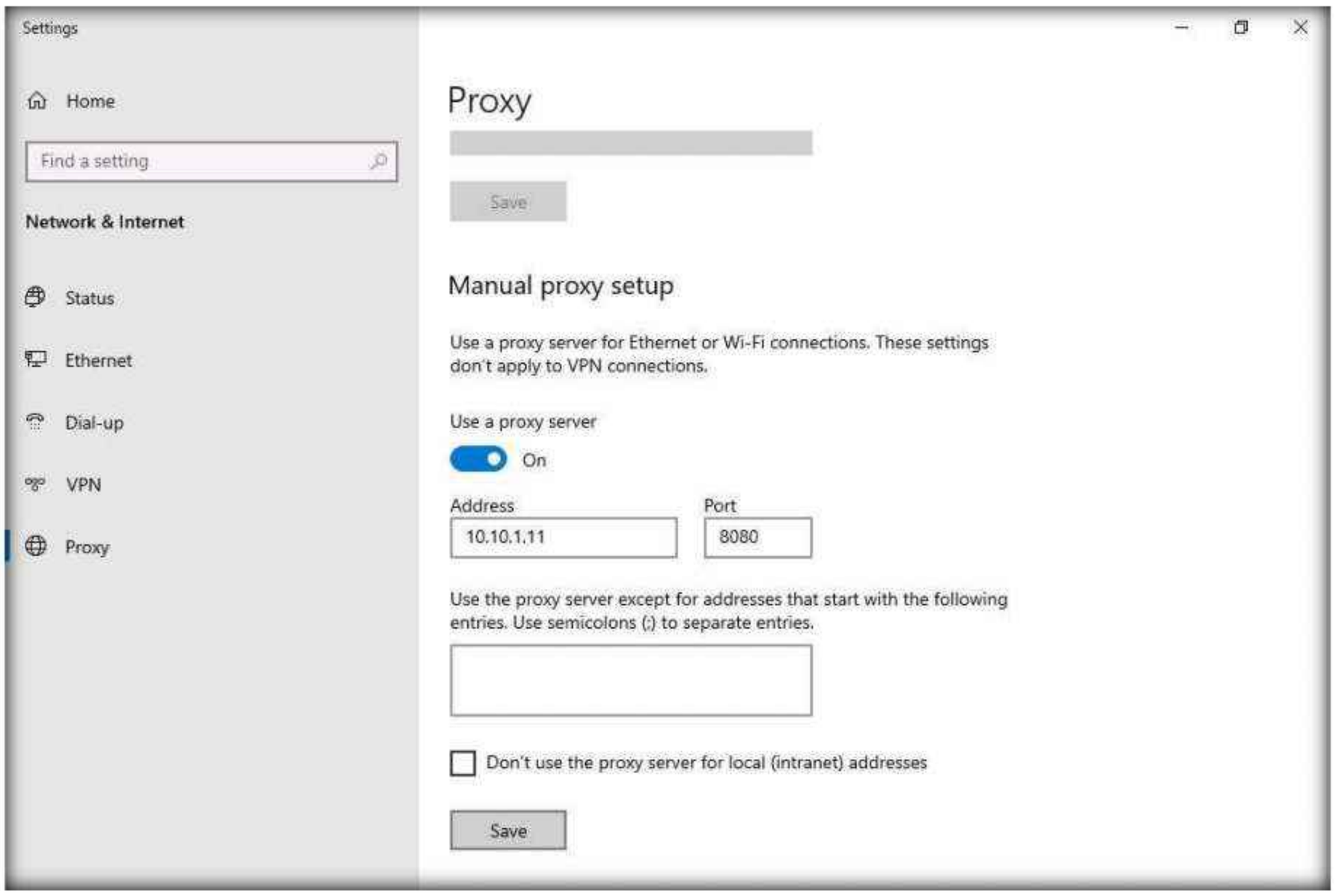
14. On the **Settings** page, expand **Advanced** settings and click **System** in the left-pane.



15. Scroll down to the **System** section and click **Open your computer's proxy settings** to configure a proxy.



16. A **Settings** window appears, with the **Proxy** settings in the right pane.
17. In the **Manual proxy setup** section, make the following changes:
    - Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
    - In the **Address** field, type **10.10.1.11** (the IP address of the attacker's machine, here, **Windows 11**).
    - In the **Port** field, type **8080**.
    - Click **Save**.



18. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.
19. Now, in the browser window open a new tab, in the address bar, type **http://www.moviescope.com** and press **Enter**.