Lab 4: Scan beyond IDS and Firewall

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the OS of the target IP address(es) is to perform network scanning without being detected by the network security perimeters such as the firewall and IDS. IDSs and firewalls are efficient security mechanisms; however, they still have some security limitations. You may be required to launch attacks to exploit these limitations using various IDS/firewall evasion techniques such as packet fragmentation, source routing, IP address spoofing, etc. Scanning beyond the IDS and firewall allows you to evaluate the target network's IDS and firewall security.

Lab Objectives

- Scan beyond IDS/firewall using various evasion techniques
- Create custom packets using Colasoft Packet Builder to scan beyond the IDS/firewall
- Create custom UDP and TCP packets using Hping3 to scan beyond the IDS/firewall
- Create custom packets using Nmap to scan beyond the IDS/firewall

Overview of Scanning beyond IDS and Firewall

An Intrusion Detection System (IDS) and firewall are the security mechanisms intended to prevent an unauthorized person from accessing a network. However, even IDSs and firewalls have some security limitations. Firewalls and IDSs intend to avoid malicious traffic (packets) from entering into a network, but certain techniques can be used to send intended packets to the target and evade IDSs/firewalls.

Techniques to evade IDS/firewall:

- **Packet Fragmentation**: Send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments
- **Source Routing**: Specifies the routing path for the malformed packet to reach the intended target
- **Source Port Manipulation**: Manipulate the actual source port with the common source port to evade IDS/firewall
- **IP Address Decoy**: Generate or manually specify IP addresses of the decoys so that the IDS/firewall cannot determine the actual IP address
- **IP Address Spoofing**: Change source IP addresses so that the attack appears to be coming in as someone else
- **Creating Custom Packets**: Send custom packets to scan the intended target beyond the firewalls
- **Randomizing Host Order**: Scan the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall
- **Sending Bad Checksums**: Send the packets with bad or bogus TCP/UPD checksums to the intended target
- **Proxy Servers**: Use a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions

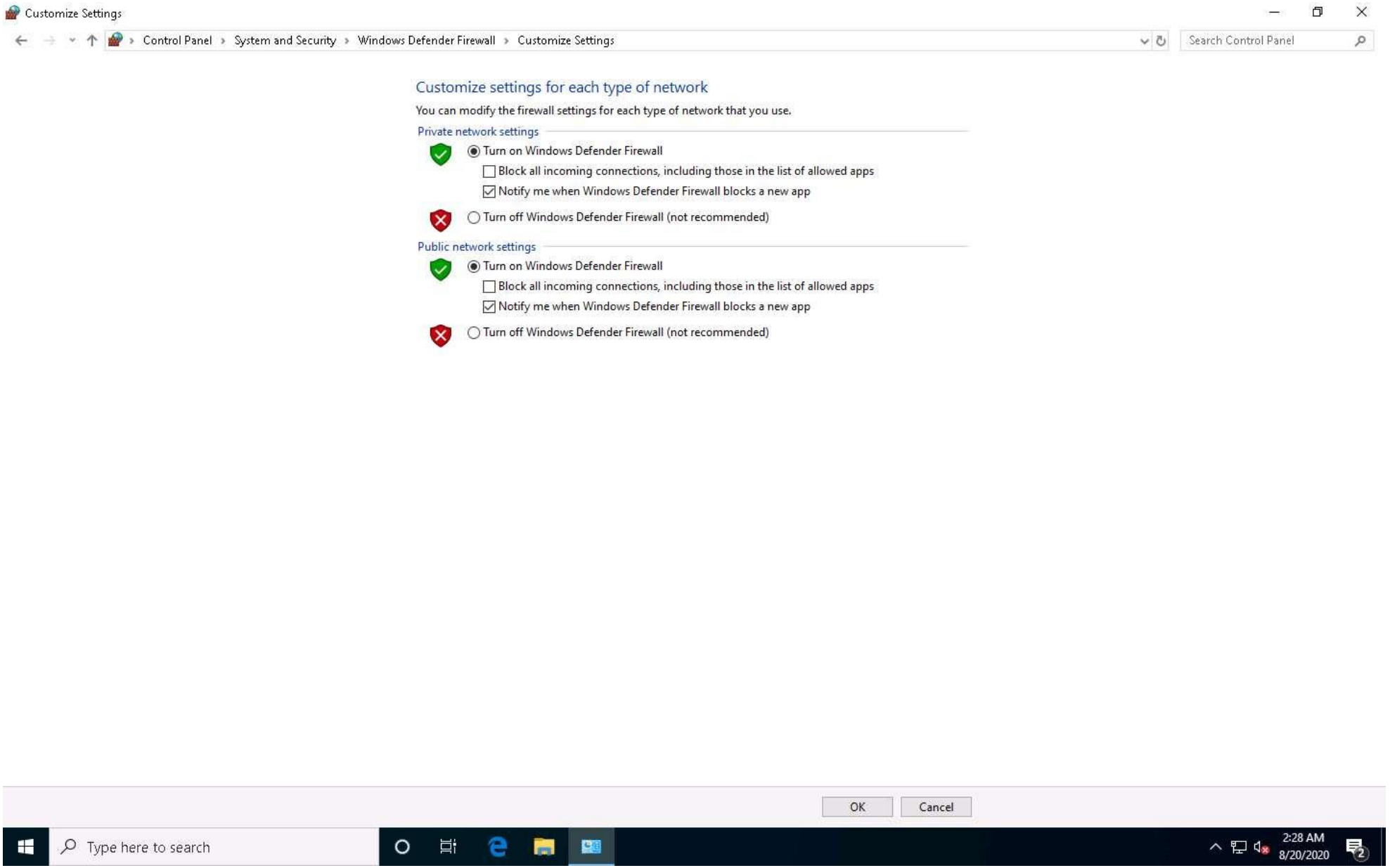
- **Anonymizers**: Use anonymizers that allow them to bypass Internet censors and evade certain IDS and firewall rules

Task 1: Scan beyond IDS/Firewall using various Evasion Techniques

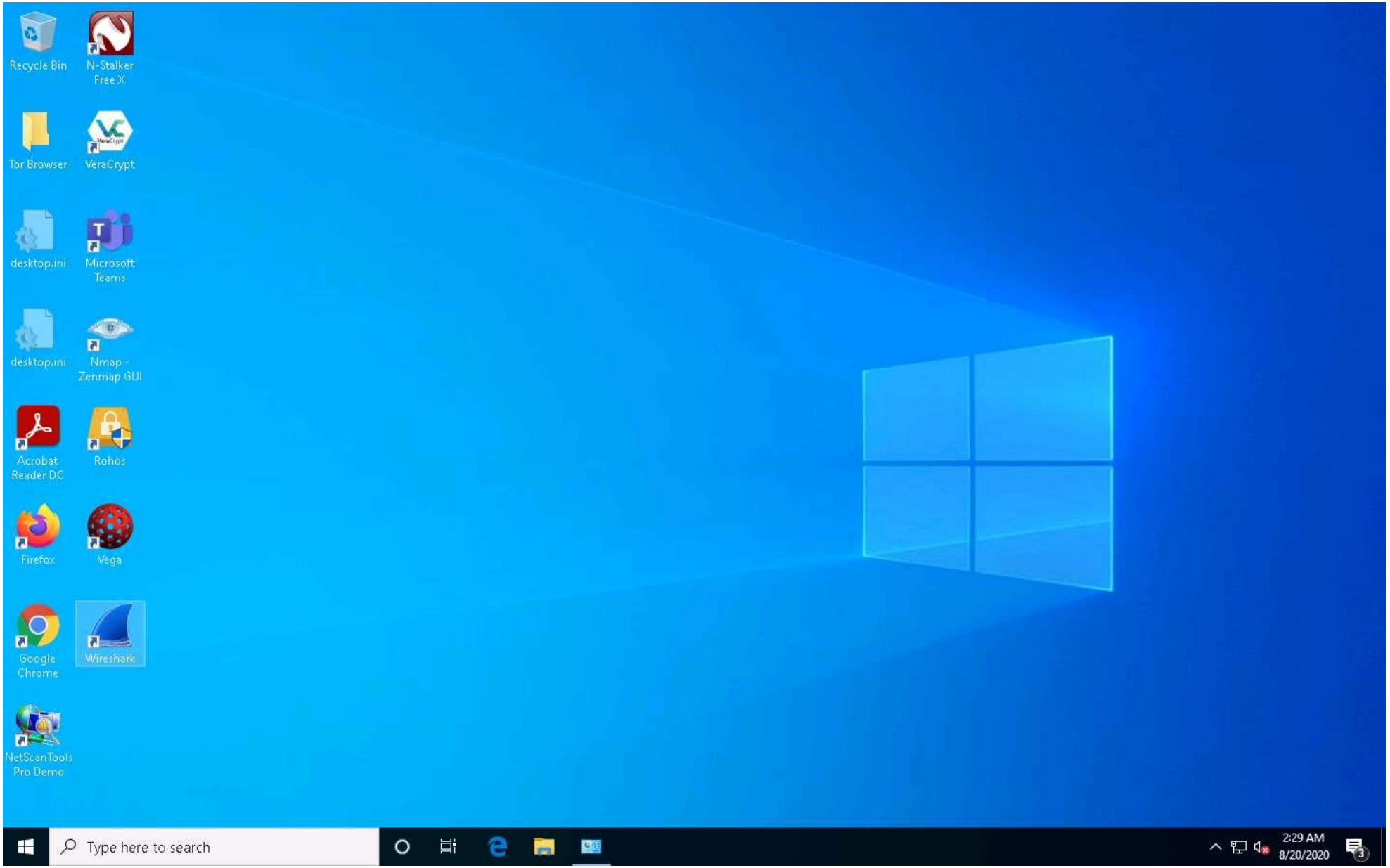
Nmap offers many features to help understand complex networks with enabled security mechanisms and supports mechanisms for bypassing poorly implemented defenses. Using Nmap, various techniques can be implemented, which can bypass the IDS/firewall security mechanisms.

Here, we will use Nmap to evade IDS/firewall using various techniques such as packet fragmentation, source port manipulation, MTU, and IP address decoy.

1. Click Windows 10 to switch to the **Windows 10** machine.
2. Navigate to **Control Panel** --> **System and Security** --> **Windows Defender Firewall** --> **Turn Windows Defender Firewall on or off**, enable Windows Defender Firewall and click **OK**, as shown in the screenshot.

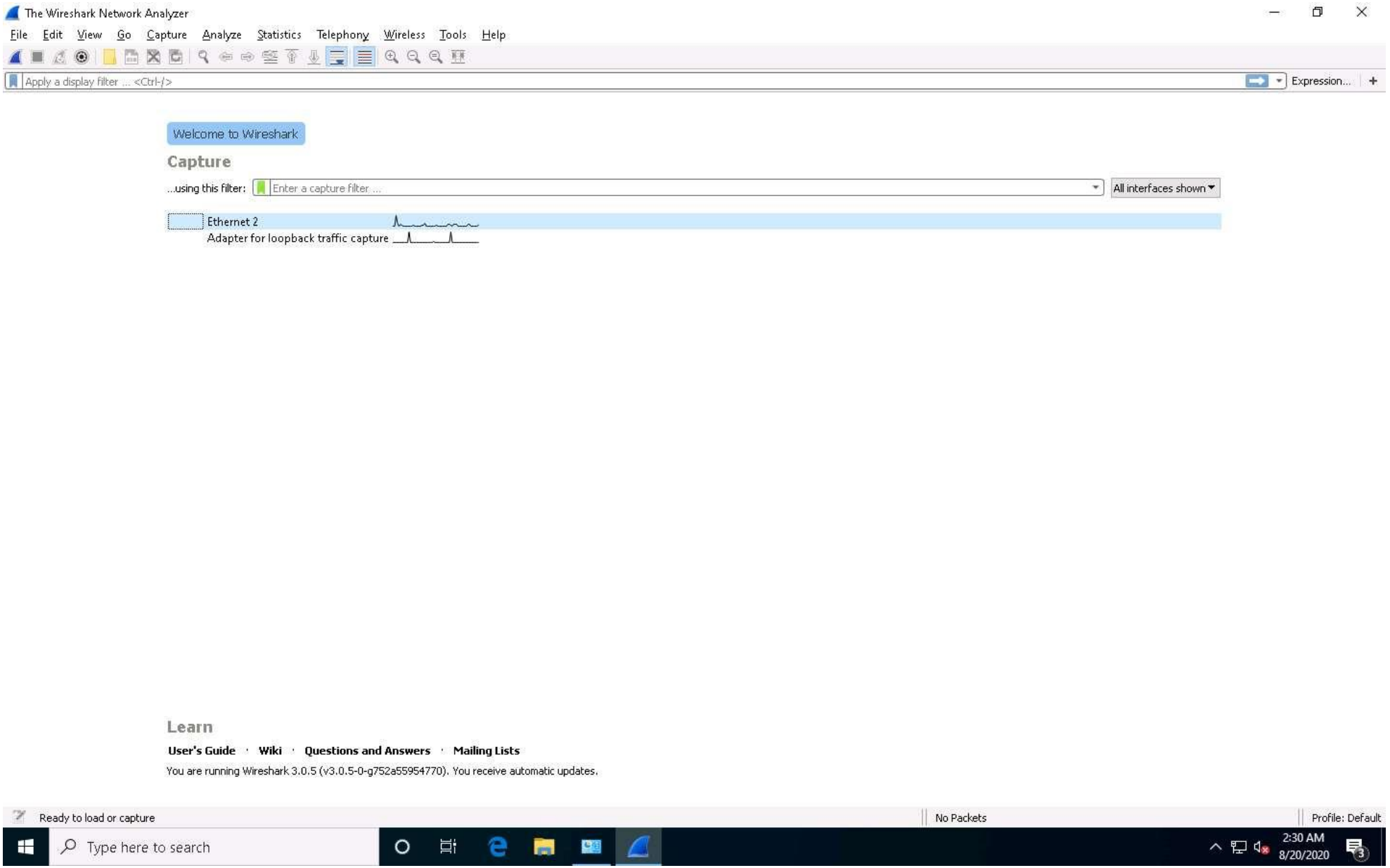


3. ☐ Minimize the **Control Panel** window, navigate to the **Desktop** and double-click **Wireshark** shortcut.

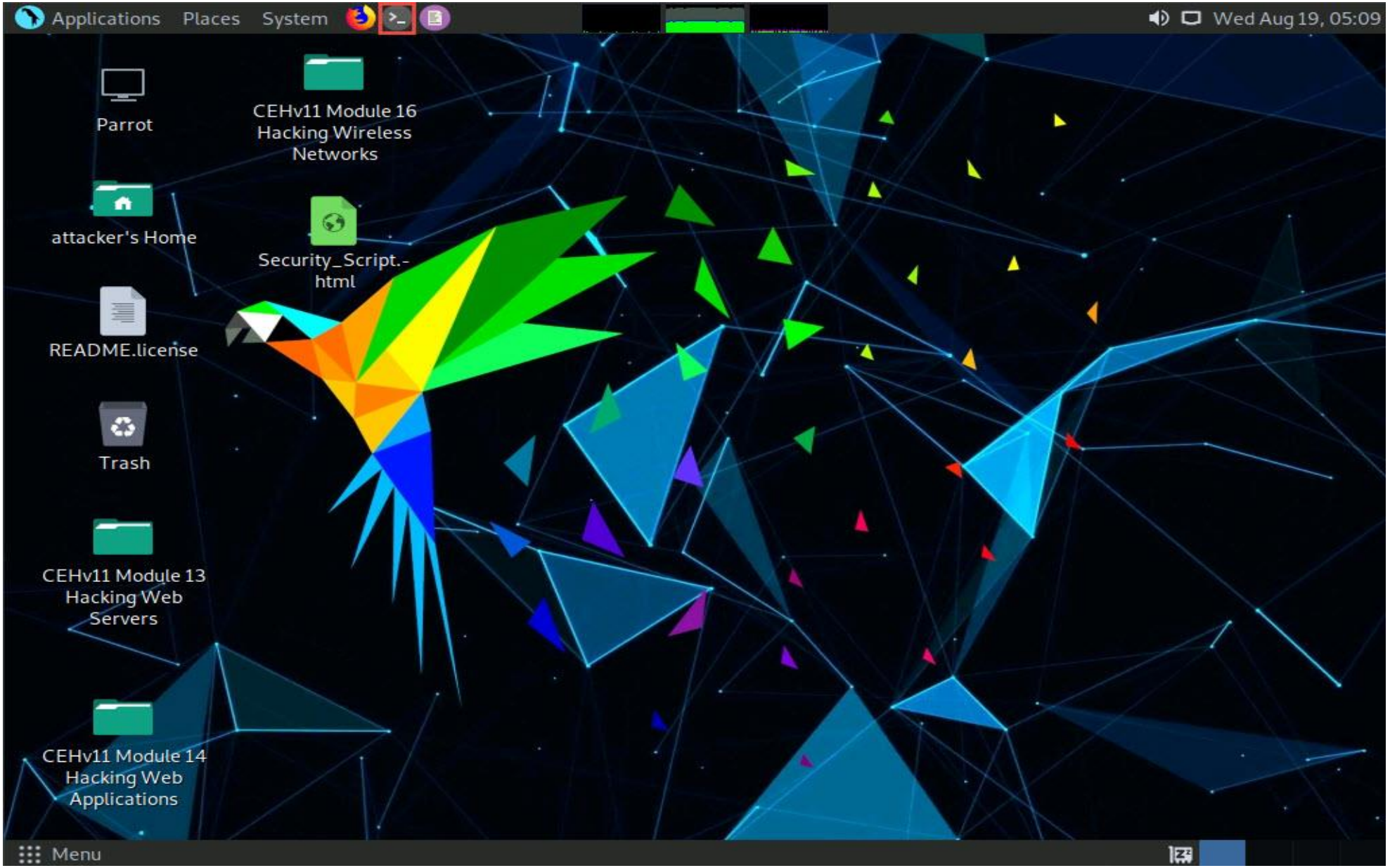


4. ☐ The **Wireshark Network Analyzer** window appears, Start capturing packets by double-clicking the available ethernet or interface (here, **Ethernet2**).

If **Software Update** window appears, click **Remind me later**.



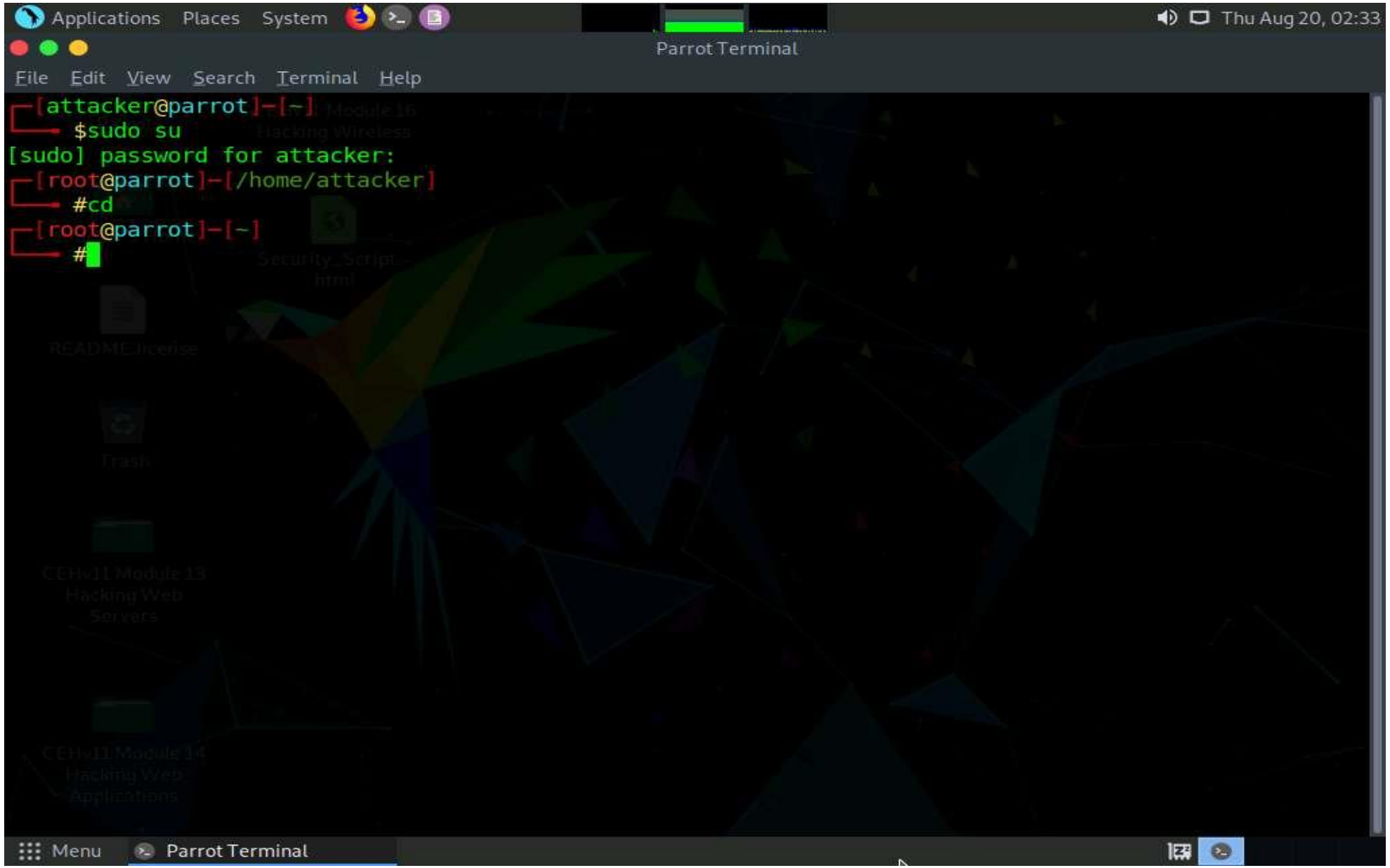
5. ☐ Click Parrot Security to switch to the **Parrot Security** machine.
6. ☐ Click the **MATE Terminal** icon in the top-left corner of the **Desktop** window to open a **Terminal** window.



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

The password that you type will not be visible.

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



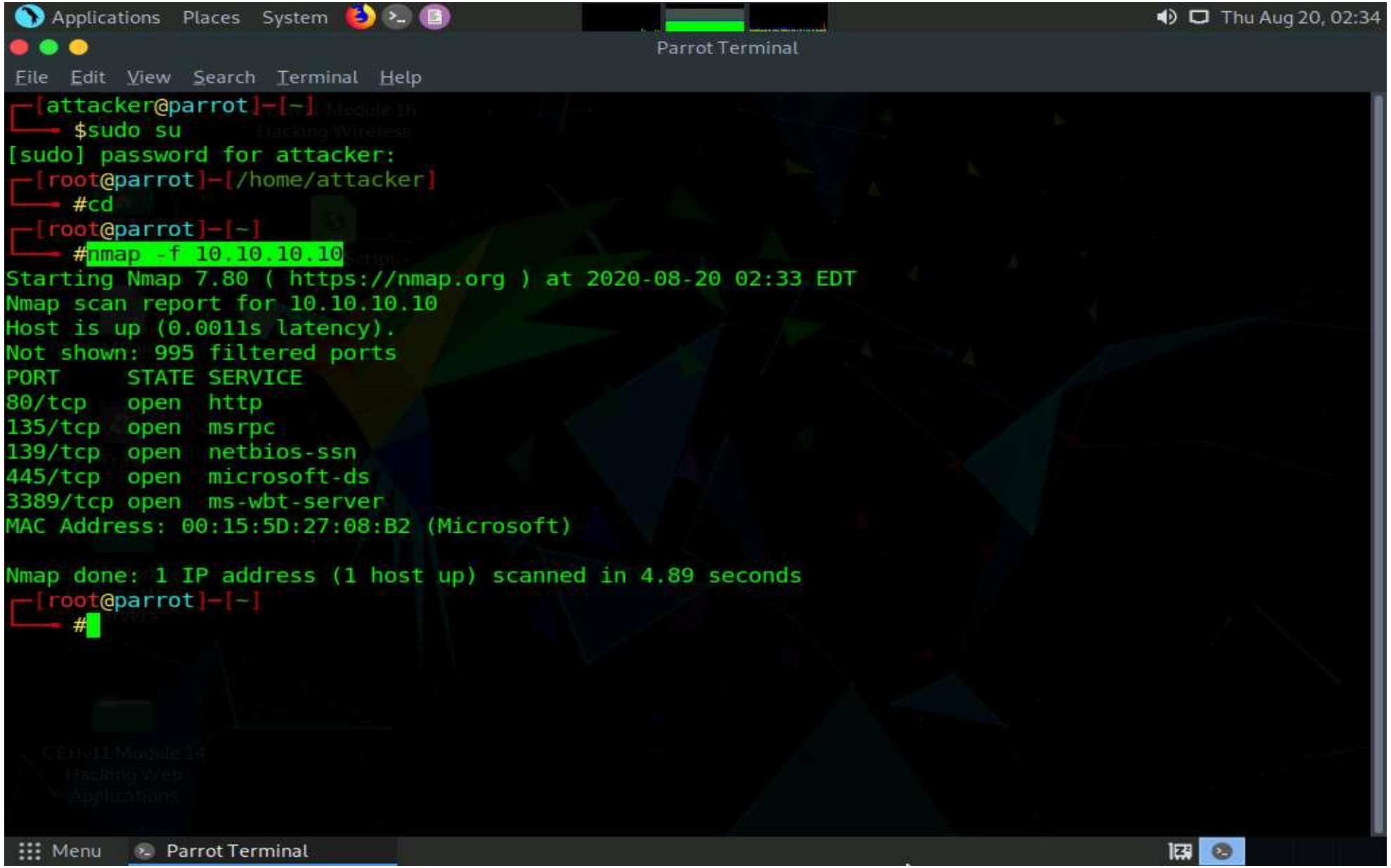
10. A **Parrot Terminal** window appears. In the terminal window, type **nmap -f [Target IP Address]**, (here, the target machine is **Windows 10** [**10.10.10.10**]) and press **Enter**.

-f switch is used to split the IP packet into tiny fragment packets.

Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.

more...

11. Although **Windows Defender Firewall** is turned on in the target system (here, **Windows 10**), you can still obtain the results displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

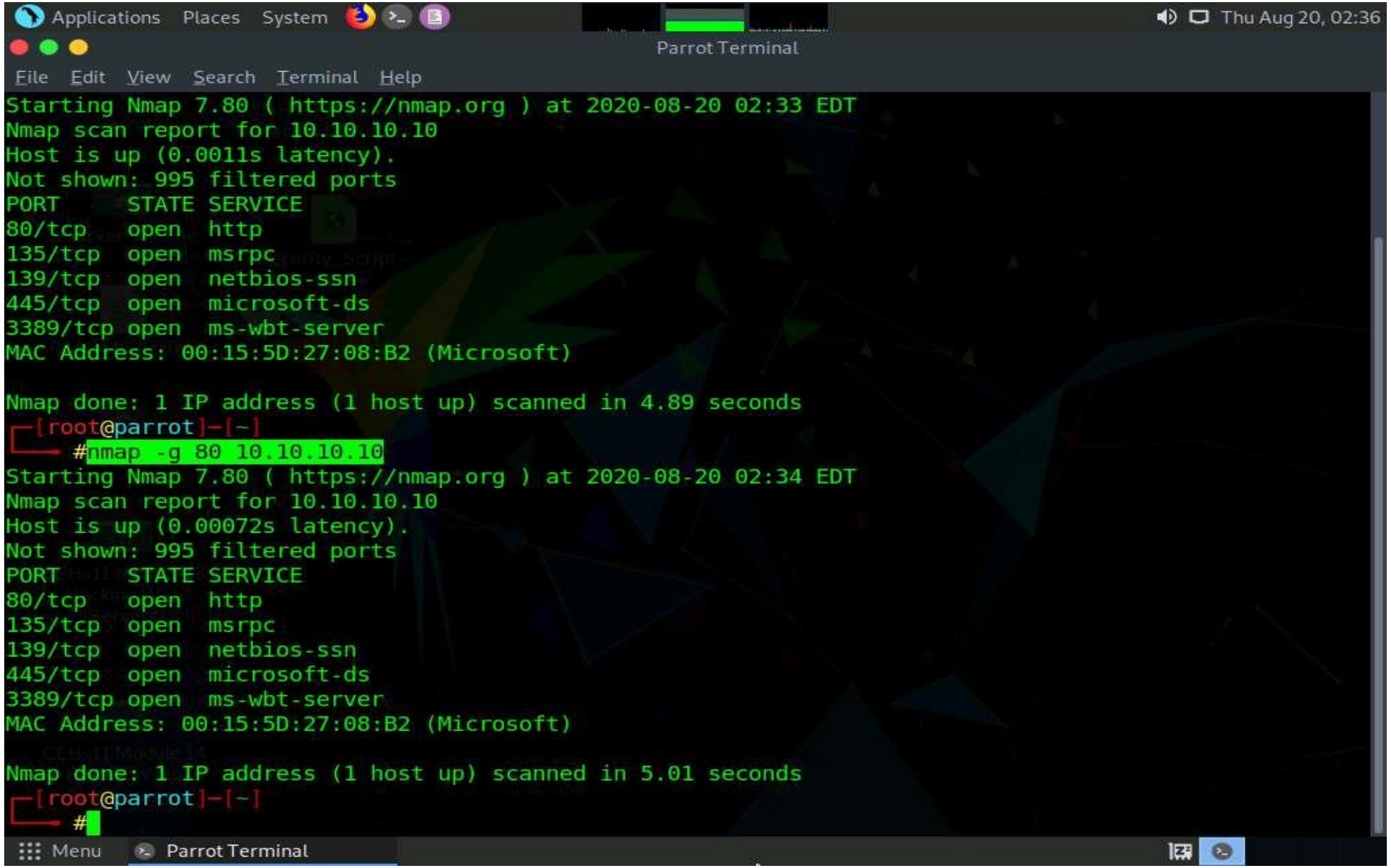


12. ☐ In the **Parrot Terminal** window, type **nmap -g 80 [Target IP Address]**, (here, target IP address is **10.10.10.10**) and press **Enter**.

In this command, you can use the **-g** or **--source-port** option to perform source port manipulation.

Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall: this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.

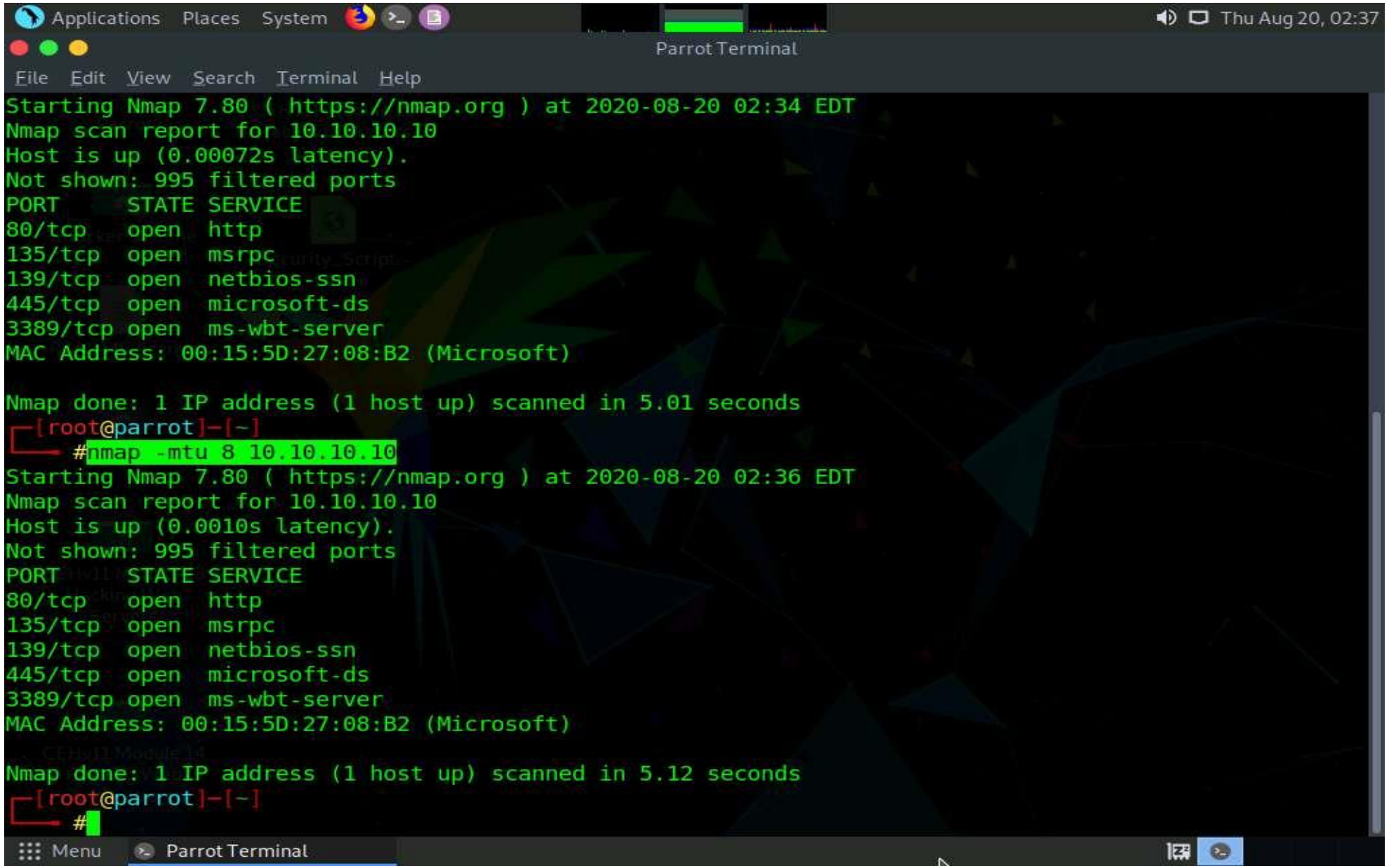
13. The results appear, displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.



14. ☐ Now, type **nmap -mtu 8 [Target IP Address]** (here, target IP address is **10.10.10.10**) and press **Enter**.

In this command, **-mtu**: specifies the number of Maximum Transmission Unit (MTU) (here, **8** bytes of packets).

Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.

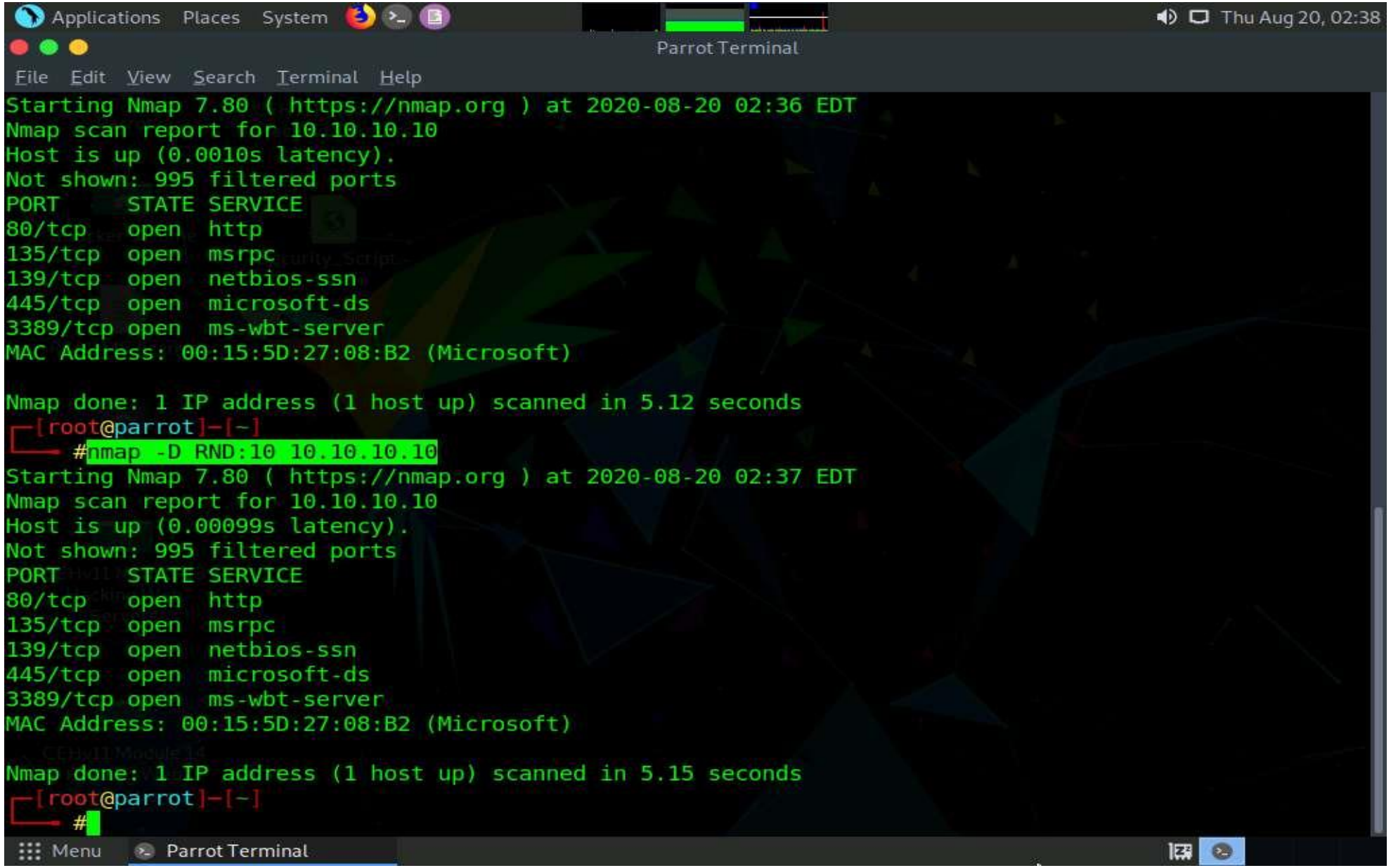


15. Now, type **nmap -D RND:10 [Target IP Address]** (here, target IP address is **10.10.10.10**) and press **Enter**.

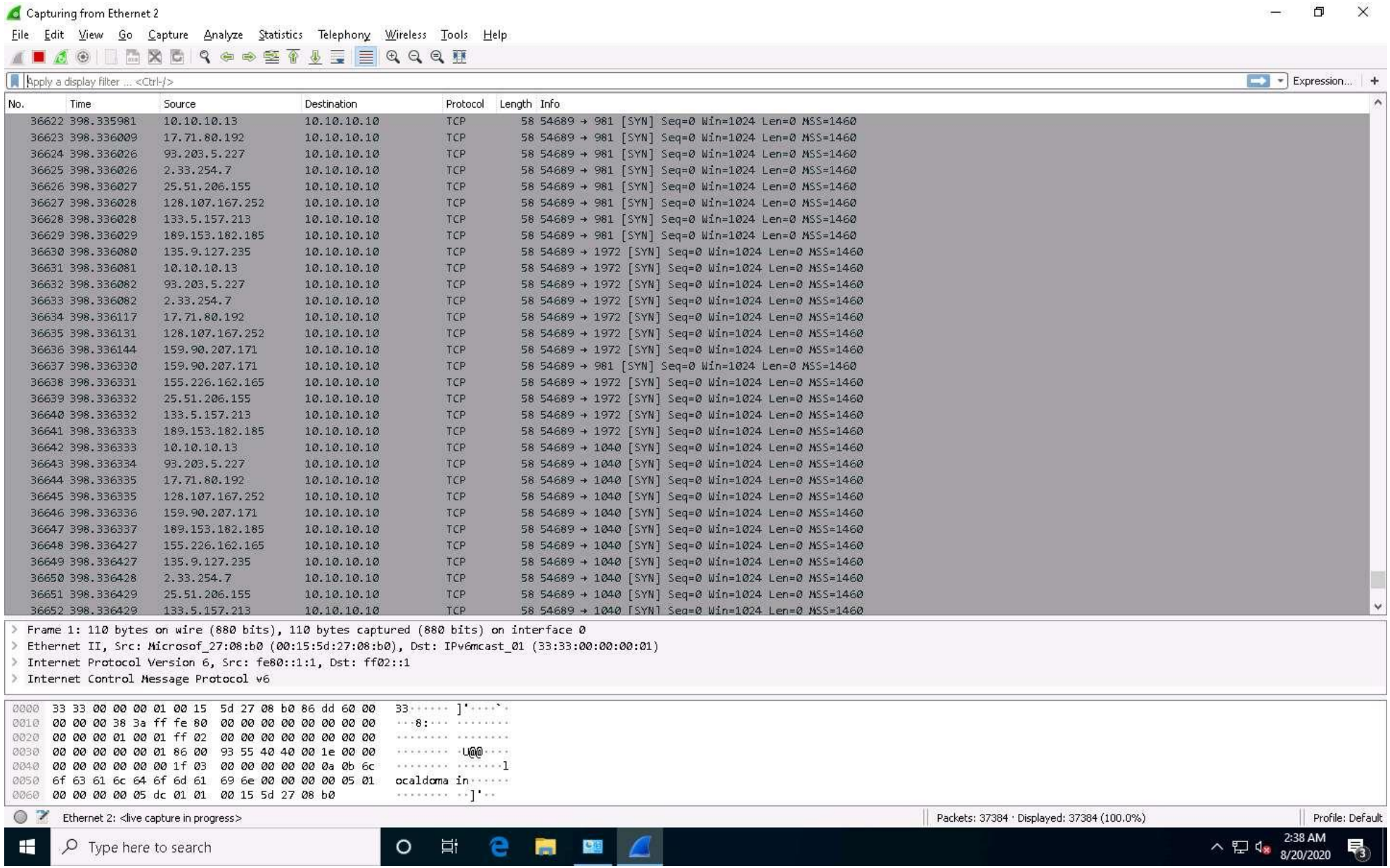
In this command, **-D**: performs a decoy scan and **RND**: generates a random and non-reserved IP addresses.

The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys. By using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.

more...



16. ☐ Now, click Windows 10 to switch to the **Windows 10** machine (target machine) and observe packets captured by Wireshark, which displays the multiple IP addresses in the source section, as shown in the screenshot.



17. ☐ This concludes the demonstration of evading IDS and firewall using various evasion techniques in Nmap.
18. ☐ Close all open windows and document all the acquired information.

Task 2: Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall

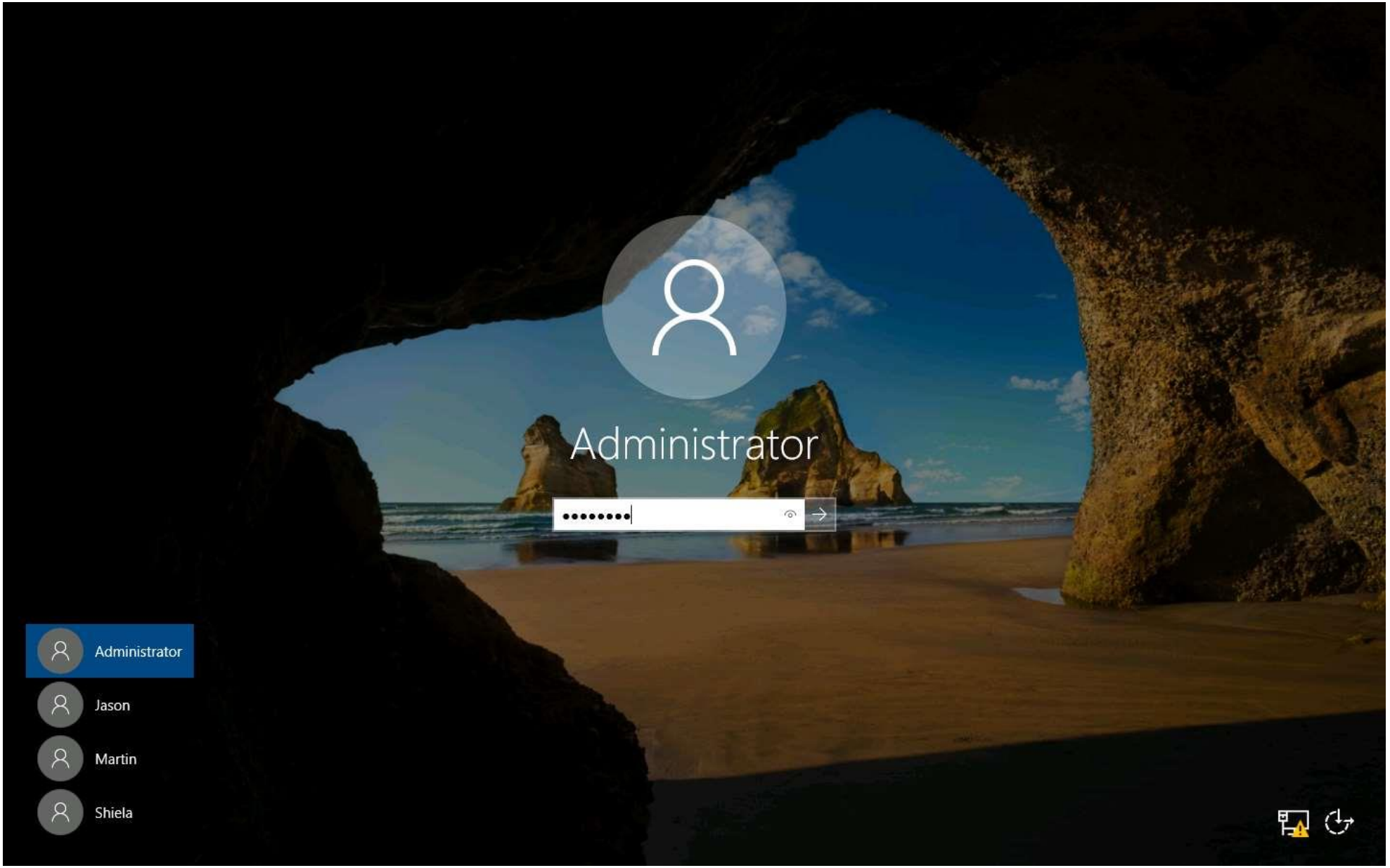
Colasoft Packet Builder is a tool that allows you to create custom network packets to assess network security. You can also select a TCP packet from the provided templates and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet. In addition to building packets, the Colasoft Packet Builder supports saving packets to packet files and sending packets to the network.

Here, we will use the Colasoft Packet Builder tool to create custom TCP packets to scan the target host by bypassing the IDS/firewall.

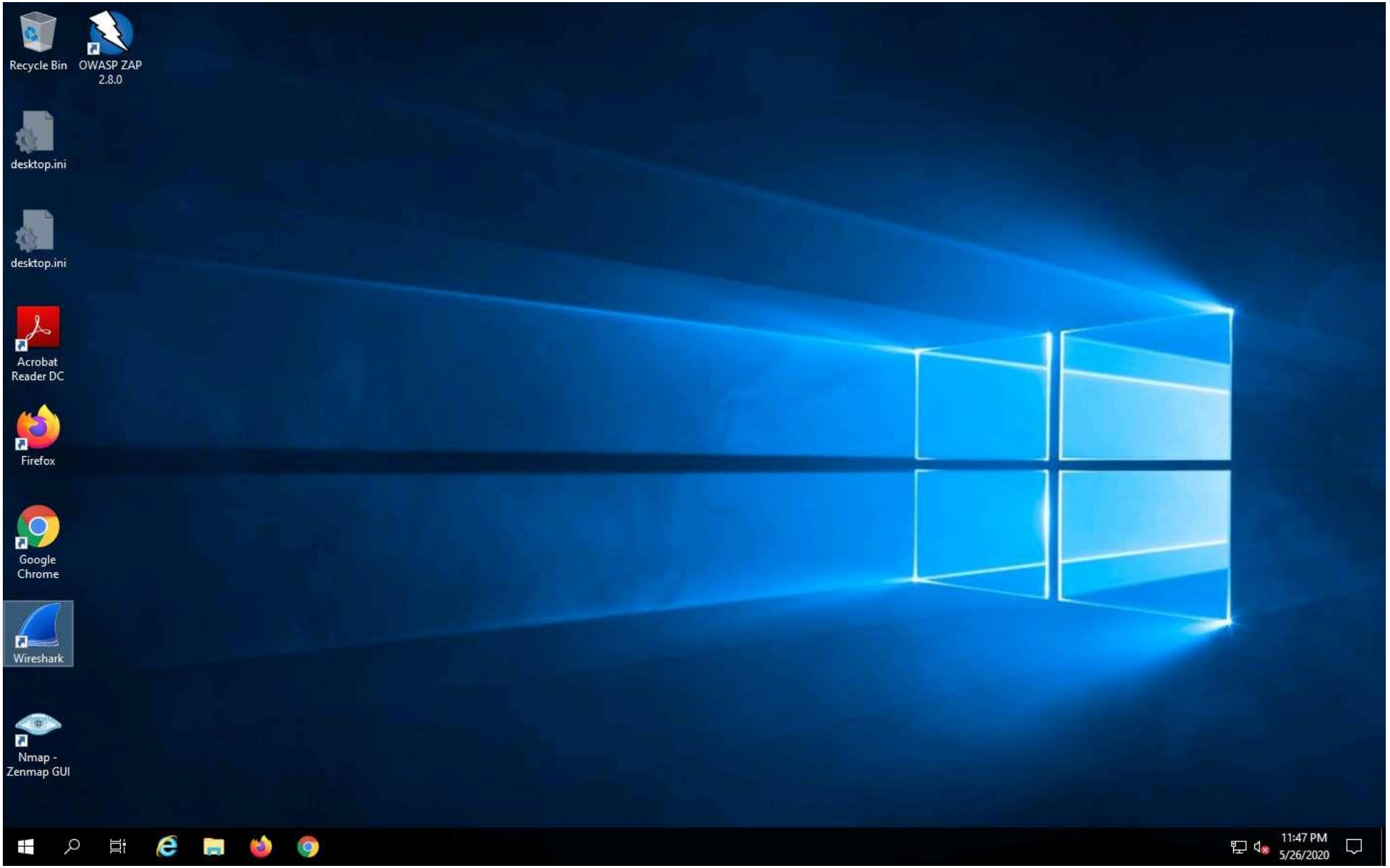
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
2. Click Ctrl+Alt+Delete to activate the machine. By default, **Administration** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2019** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

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

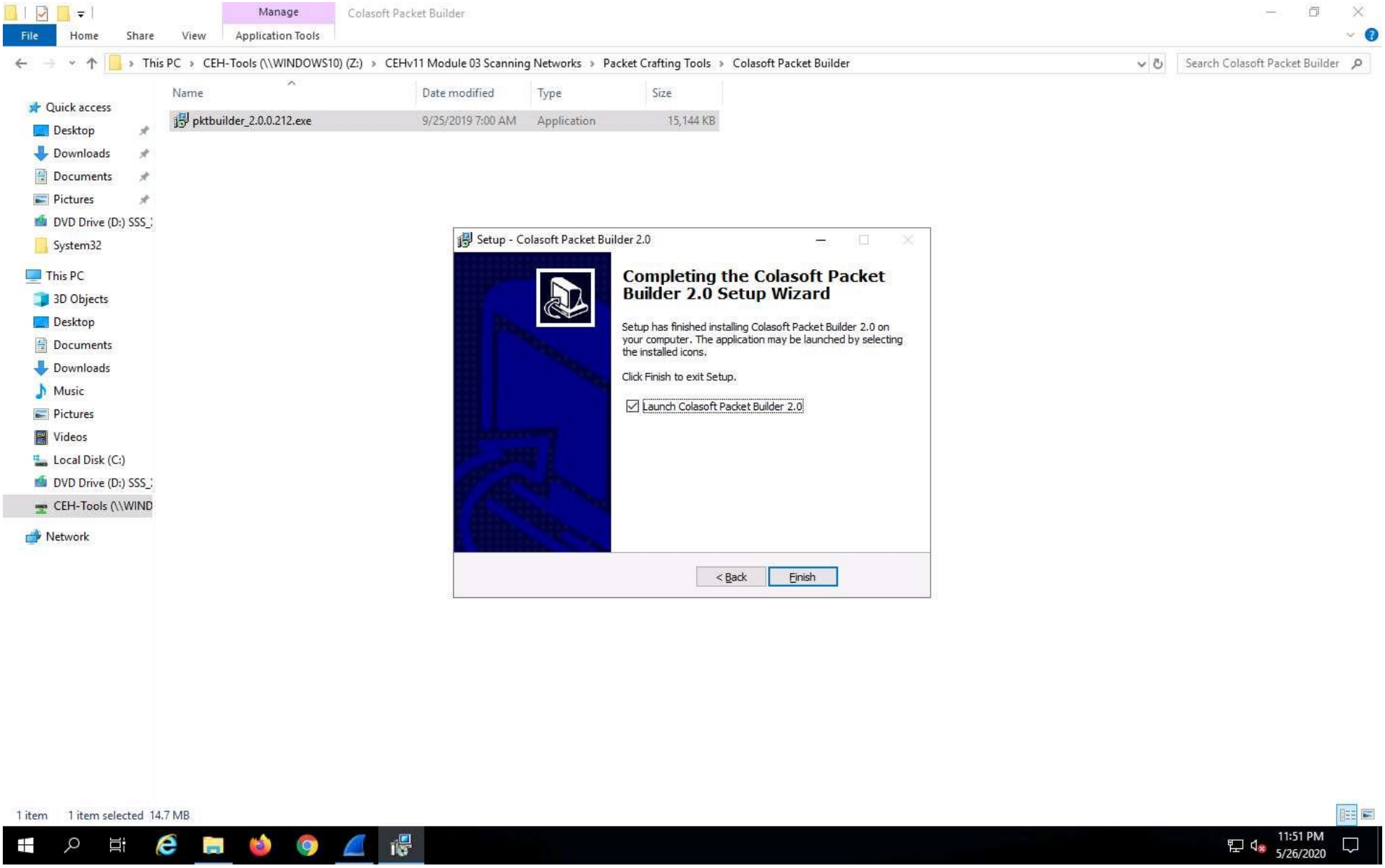


3. ☐ In the **Desktop**, double-click **Wireshark** shortcut.



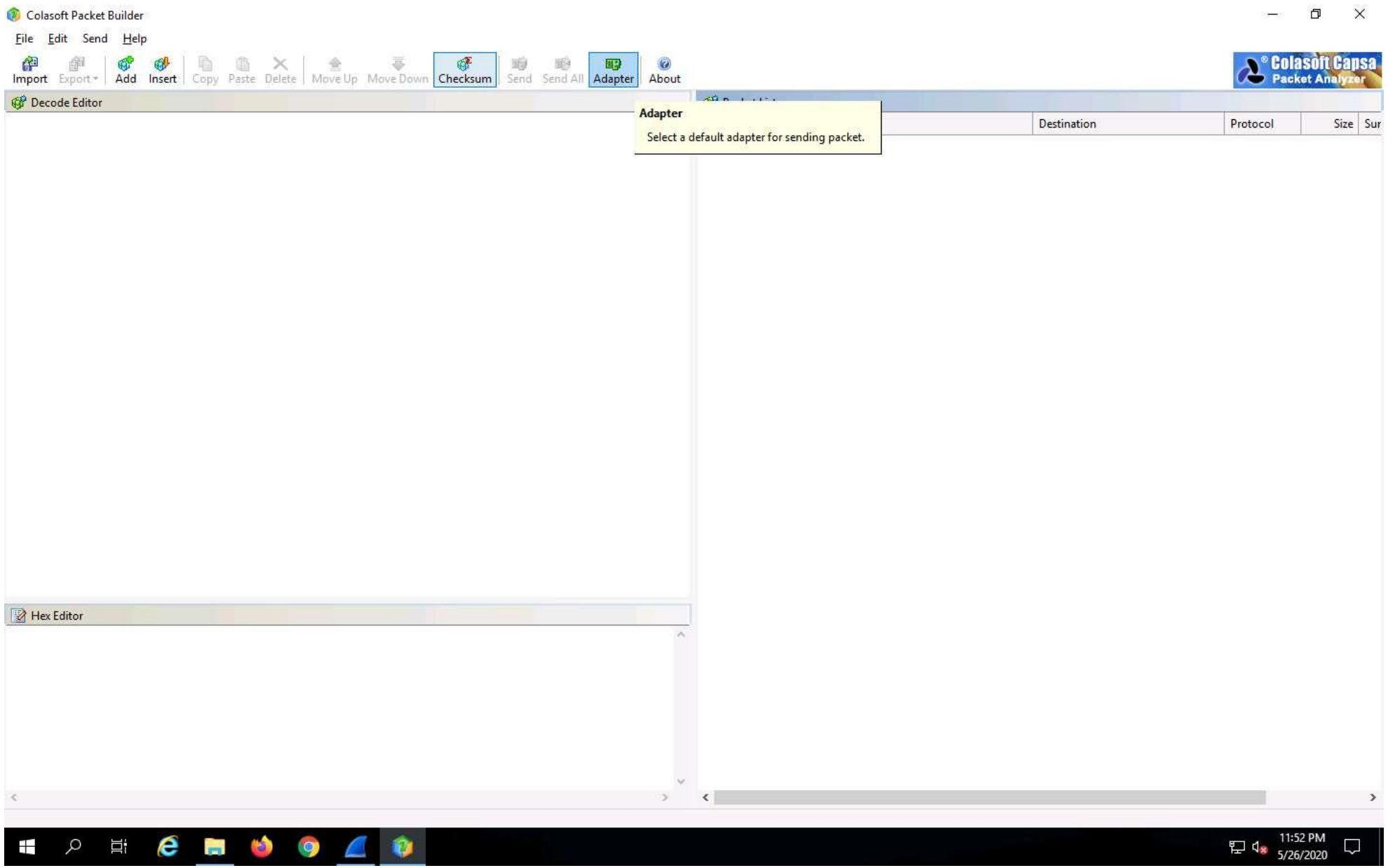
4. ☐ The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture.
5. ☐ Navigate to **Z:\CEHv11 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder** and double-click **pktbuilder_2.0.0.212.exe**.

6. Follow the wizard-driven installation steps to install **Colasoft Packet Builder**.
7. After the completion of the installation, click on the **Launch Colasoft Packet Builder 2.0** checkbox and click **Finish**.

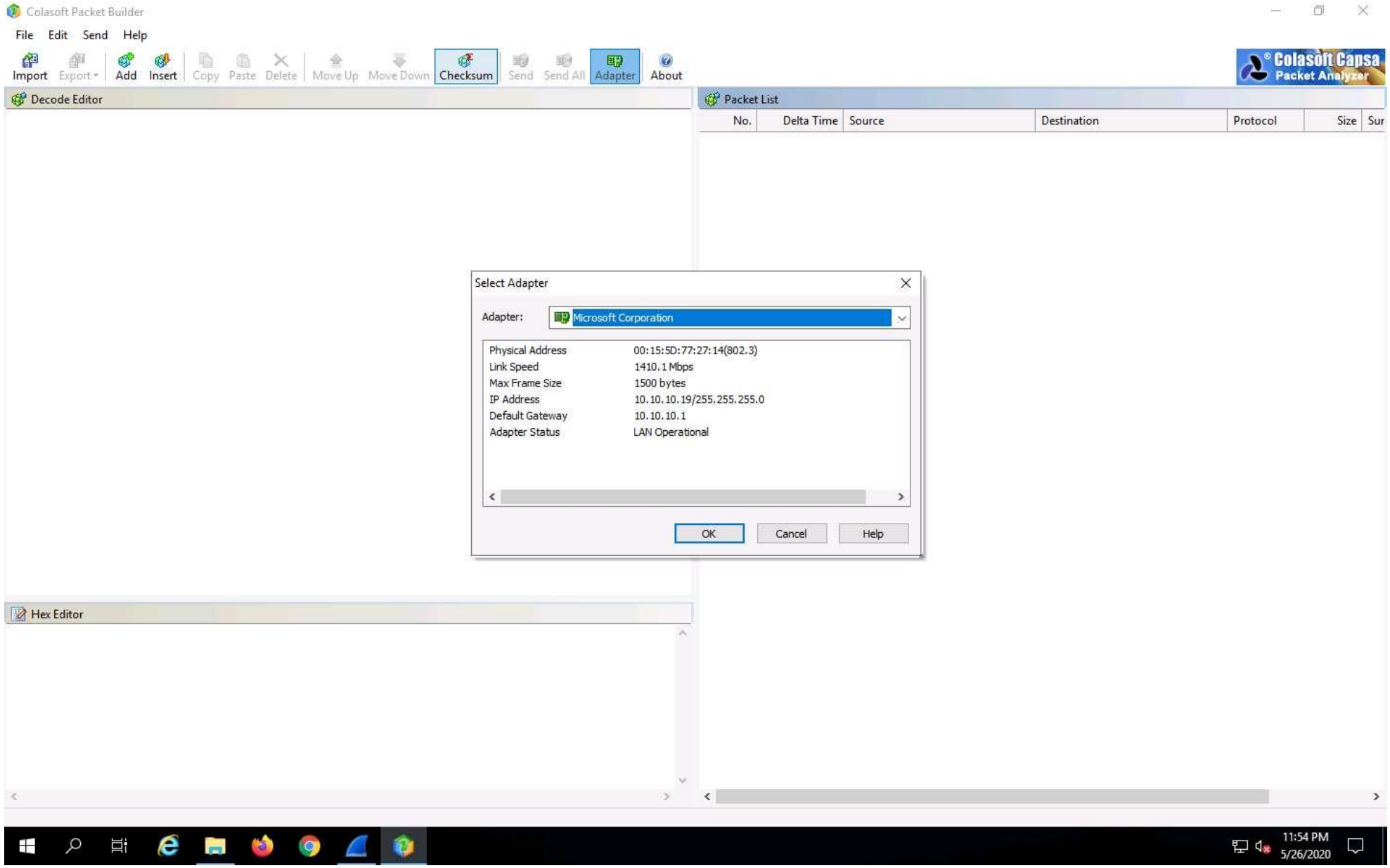


8. ☐ The **Colasoft Packet Builder** GUI appears; click on the **Adapter** icon, as shown in the screenshot.

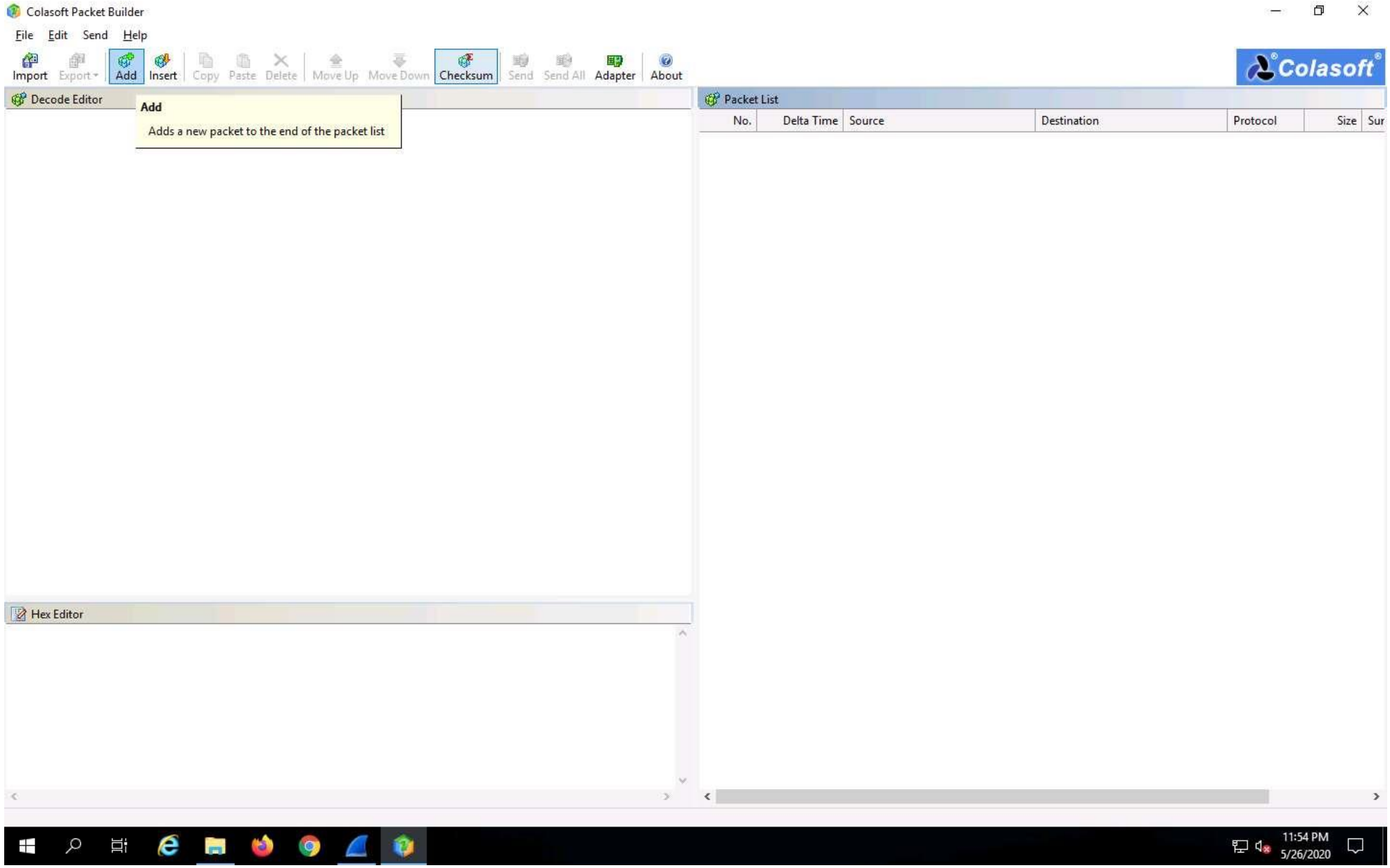
If a pop-up appears, close the window.



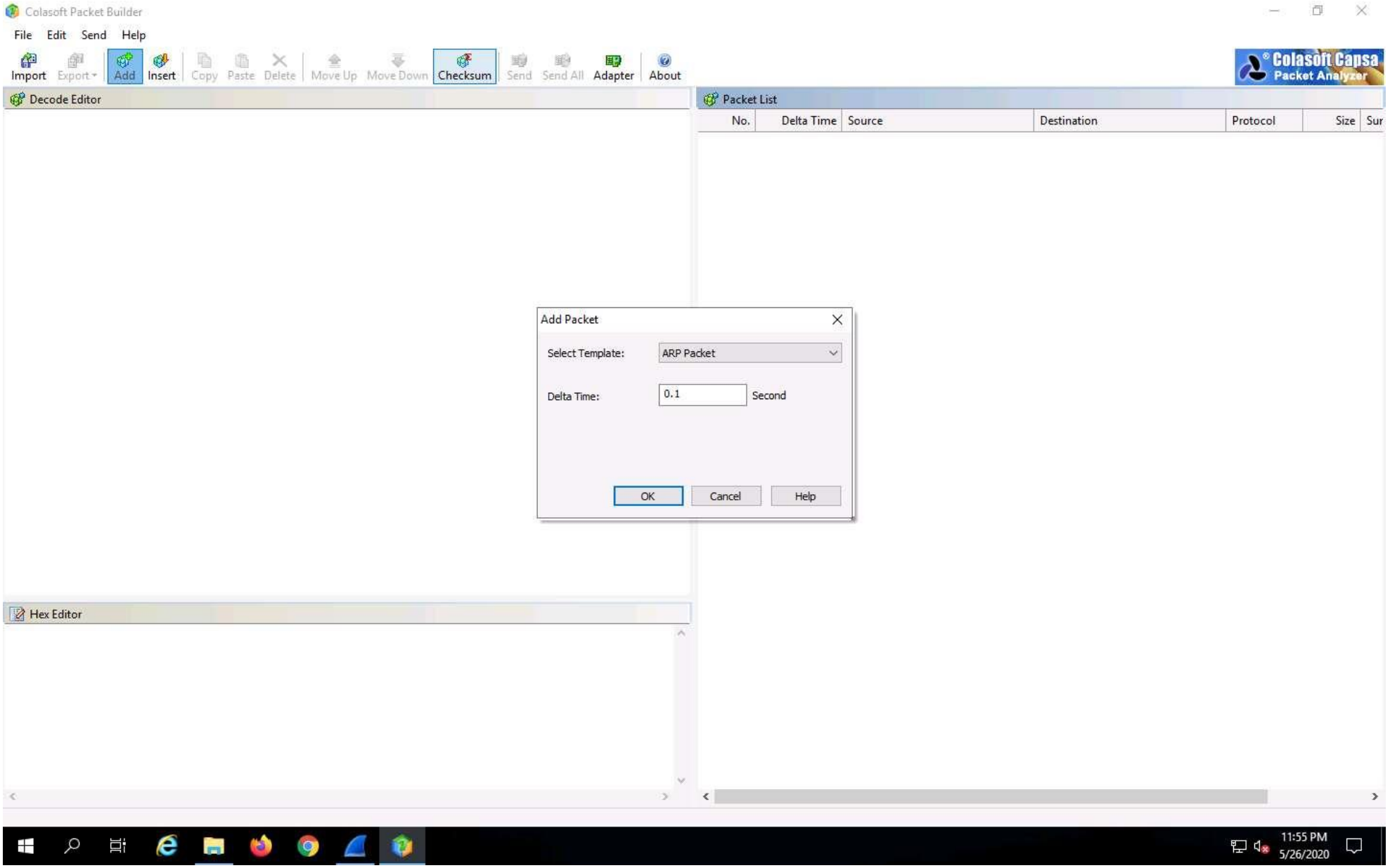
9. When the **Select Adapter** window appears, check the **Adapter** settings and click **OK**.



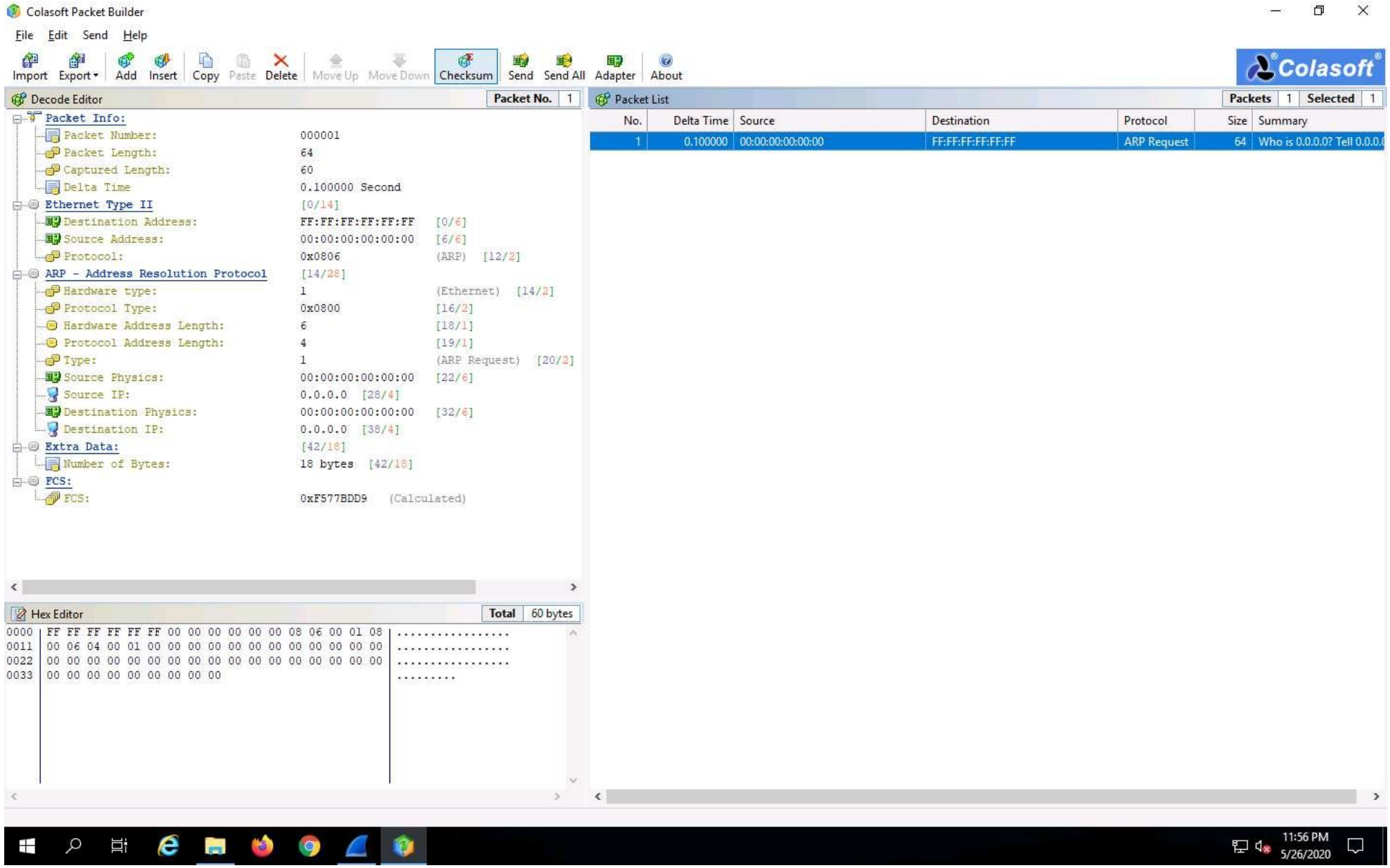
10. ☐ To add or create a packet, click the **Add** icon in the **Menu** bar.



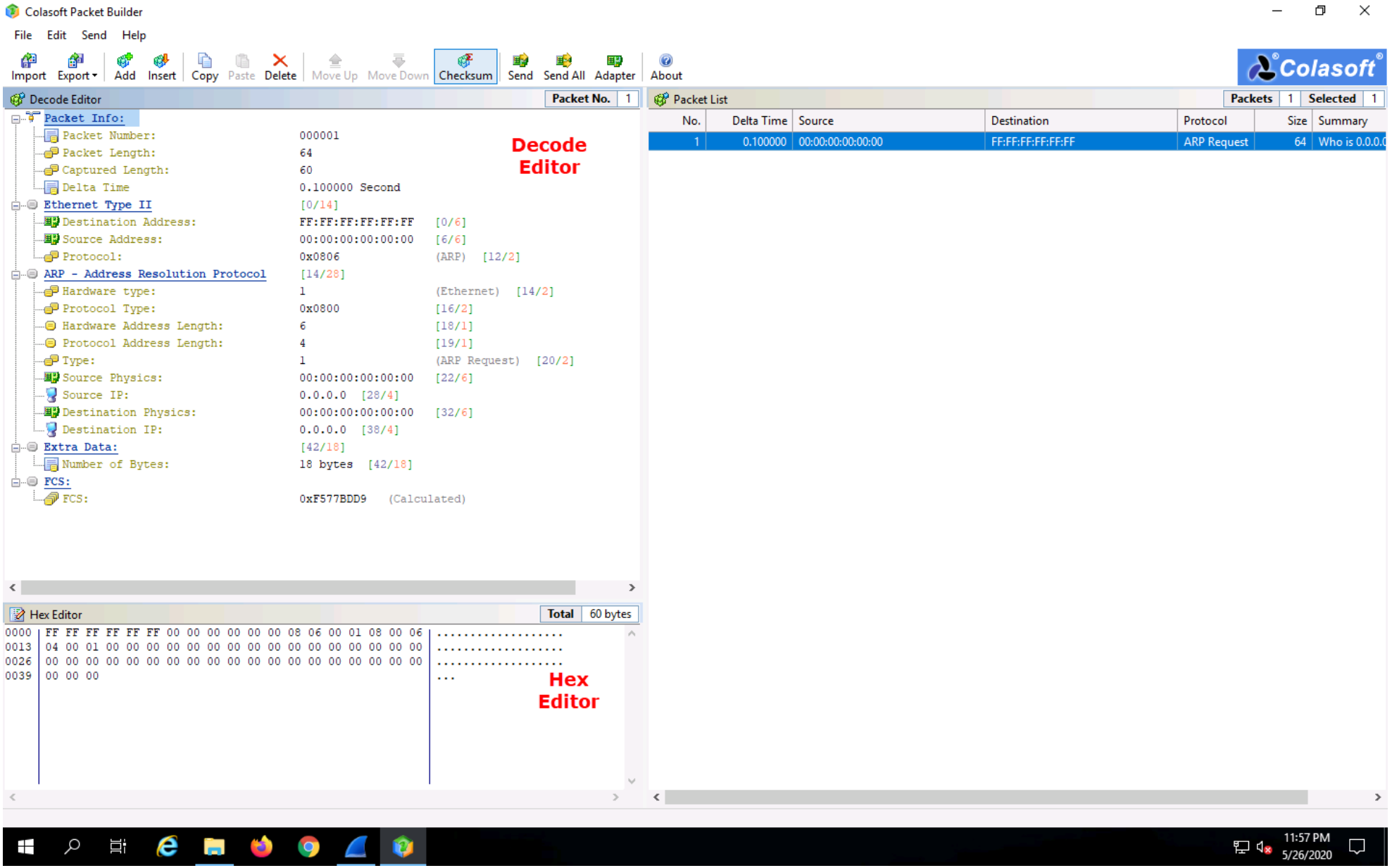
11. In the **Add Packet** dialog box, select the **ARP Packet** template, set **Delta Time** as **0.1** seconds, and click **OK**.



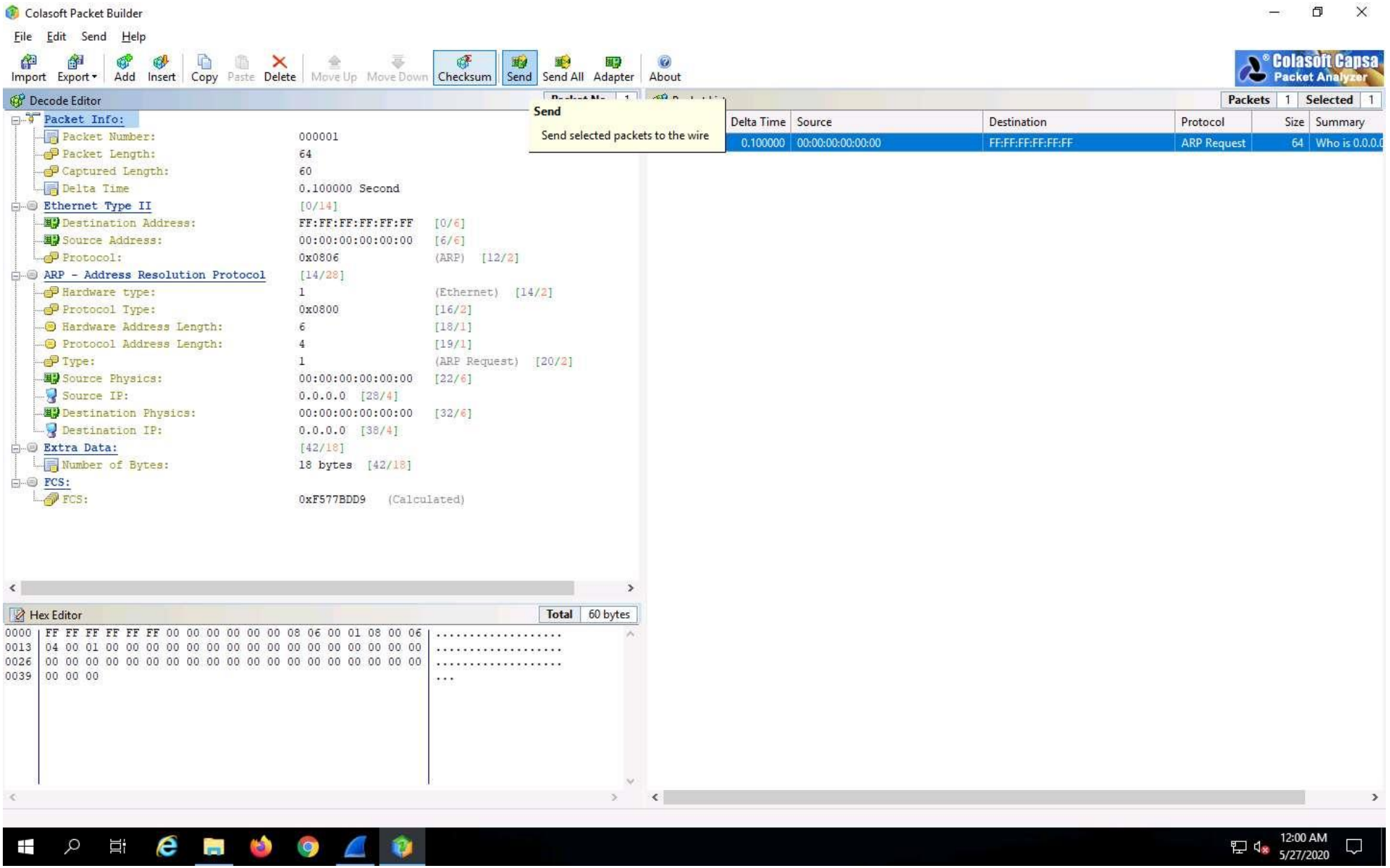
12. You can view the added packets list on the right-hand side of the window, under **Packet List**.



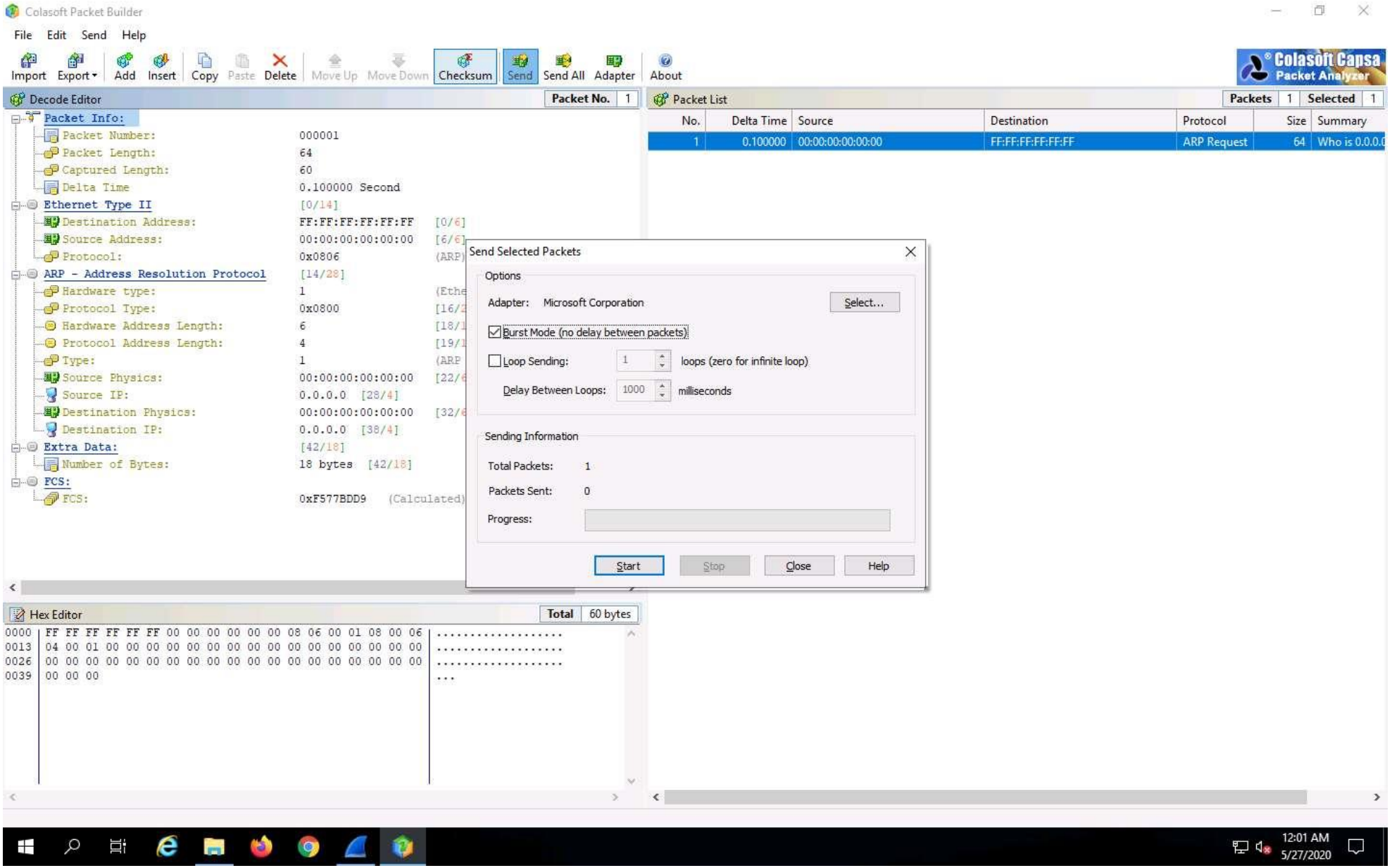
13. **Colasoft Packet Builder** allows you to edit the decoding information in the two editors, **Decode Editor** and **Hex Editor**, located in the left pane of the window.
    - The **Decode Editor** section allows you to edit the packet decoding information by double-clicking the item that you wish to decode.
    - **Hex Editor** displays the actual packet contents in raw hexadecimal value on the left and its ASCII equivalent on the right.



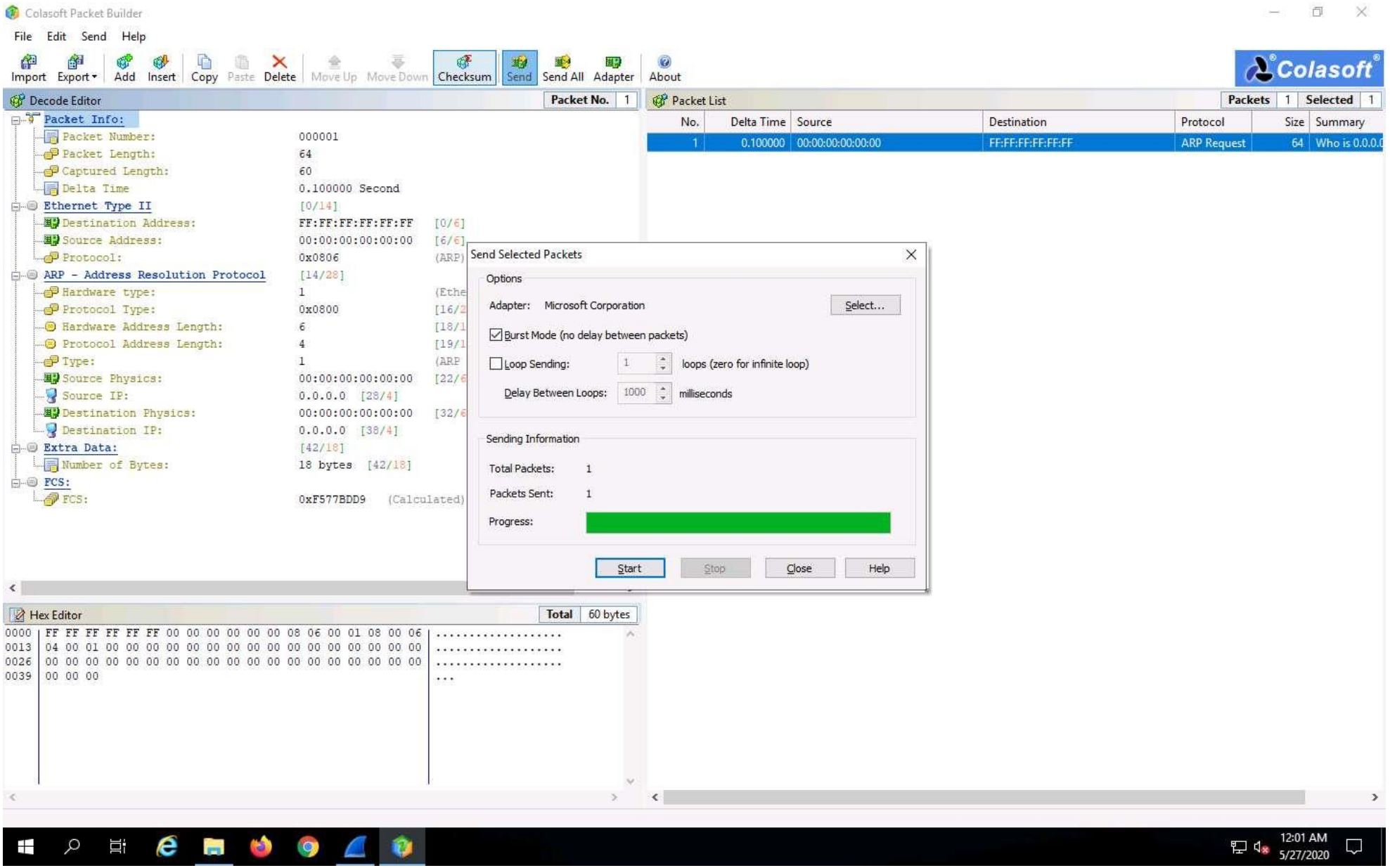
14. To send the packet, click **Send** from the **Menu** bar.



15. ☐ In the **Send Selected Packets** window, select the **Burst Mode (no delay between packets)** option, and then click **Start**.



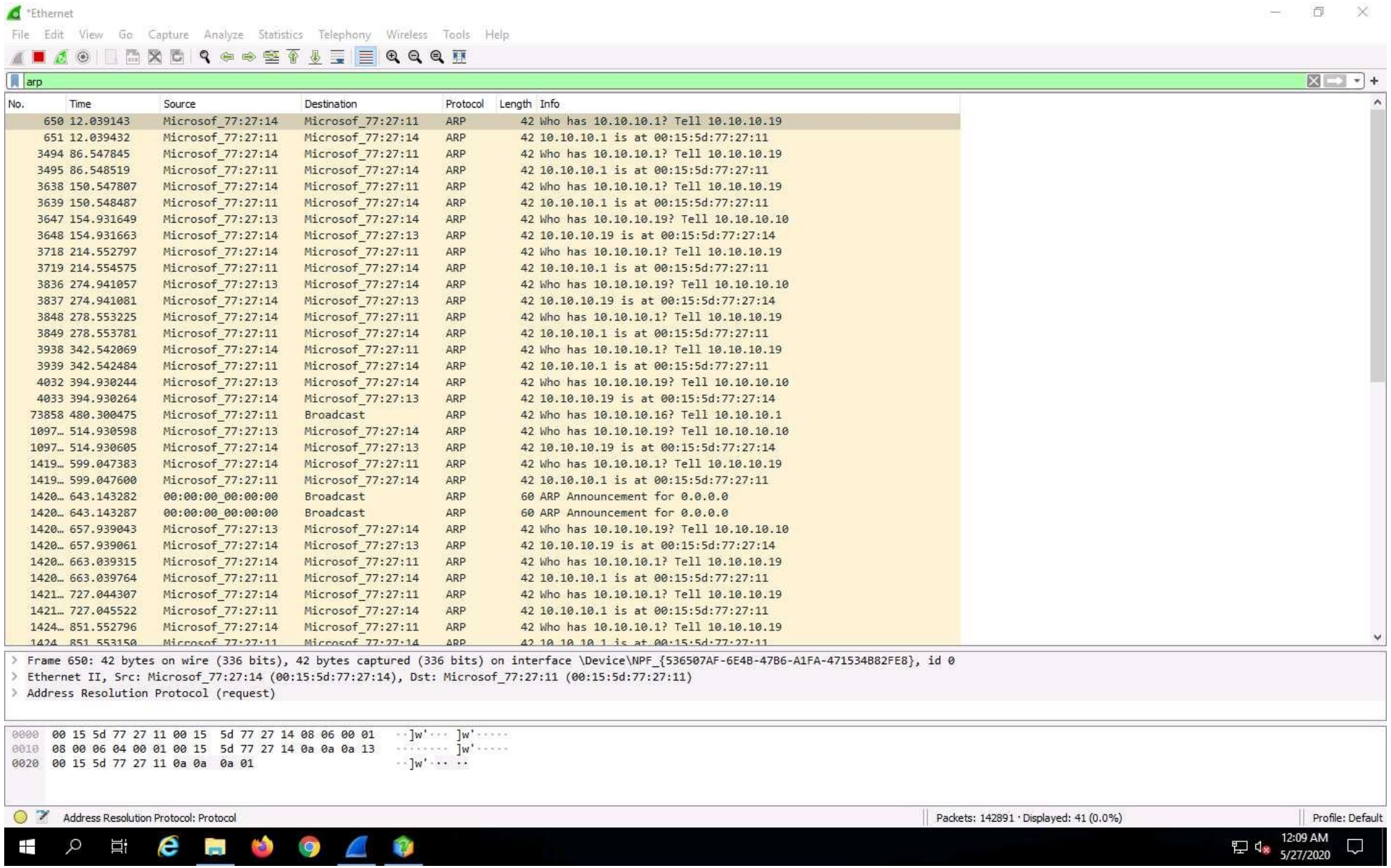
16. ☐ After the **Progress** bar completes, click **Close**.



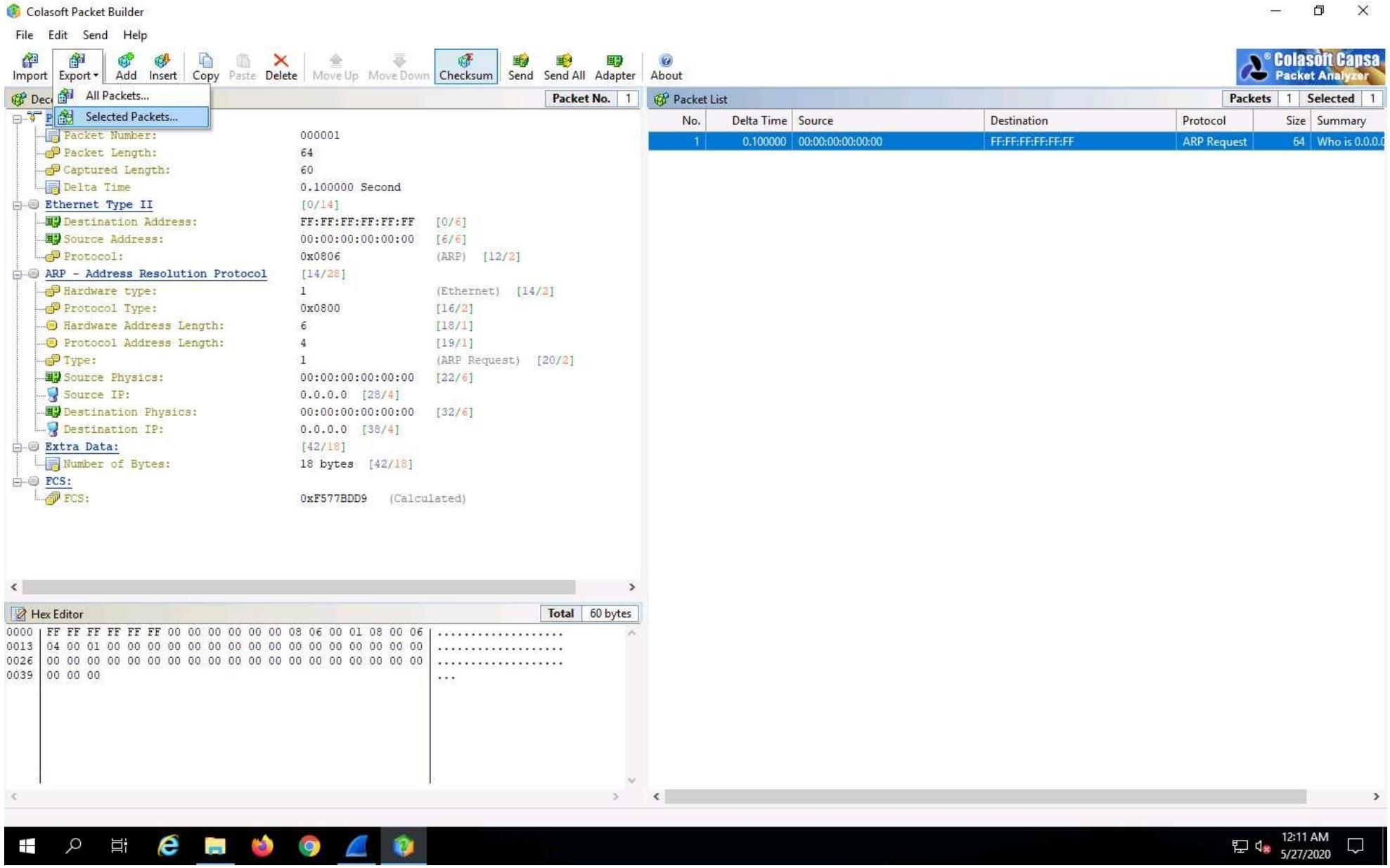
17. ☐ Now, when this ARP packet is broadcasted in the network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the **Wireshark** tool.

18. In the **Wireshark** window, click on the **Filter** field, type **arp** and press **Enter**. The ARP packets will be displayed, as shown in the screenshot.

Here, the host machine (**10.10.10.19**) is broadcasting ARP packets, prompting the target machines to reply to the message.



19. ☐ Switch back to the **Colasoft Packet Builder** window, to export the packet, click **Export** --> **Selected Packets...**.



20. In the **Save As** window, select a destination folder in the **Save in** field, specify **File name** and **Save as type**, and click **Save**.
21. This saved file can be used for future reference.
22. This concludes the demonstration of creating a custom TCP packets to scan the target host by bypassing the IDS/firewall.
23. Close all open windows and document all the acquired information.

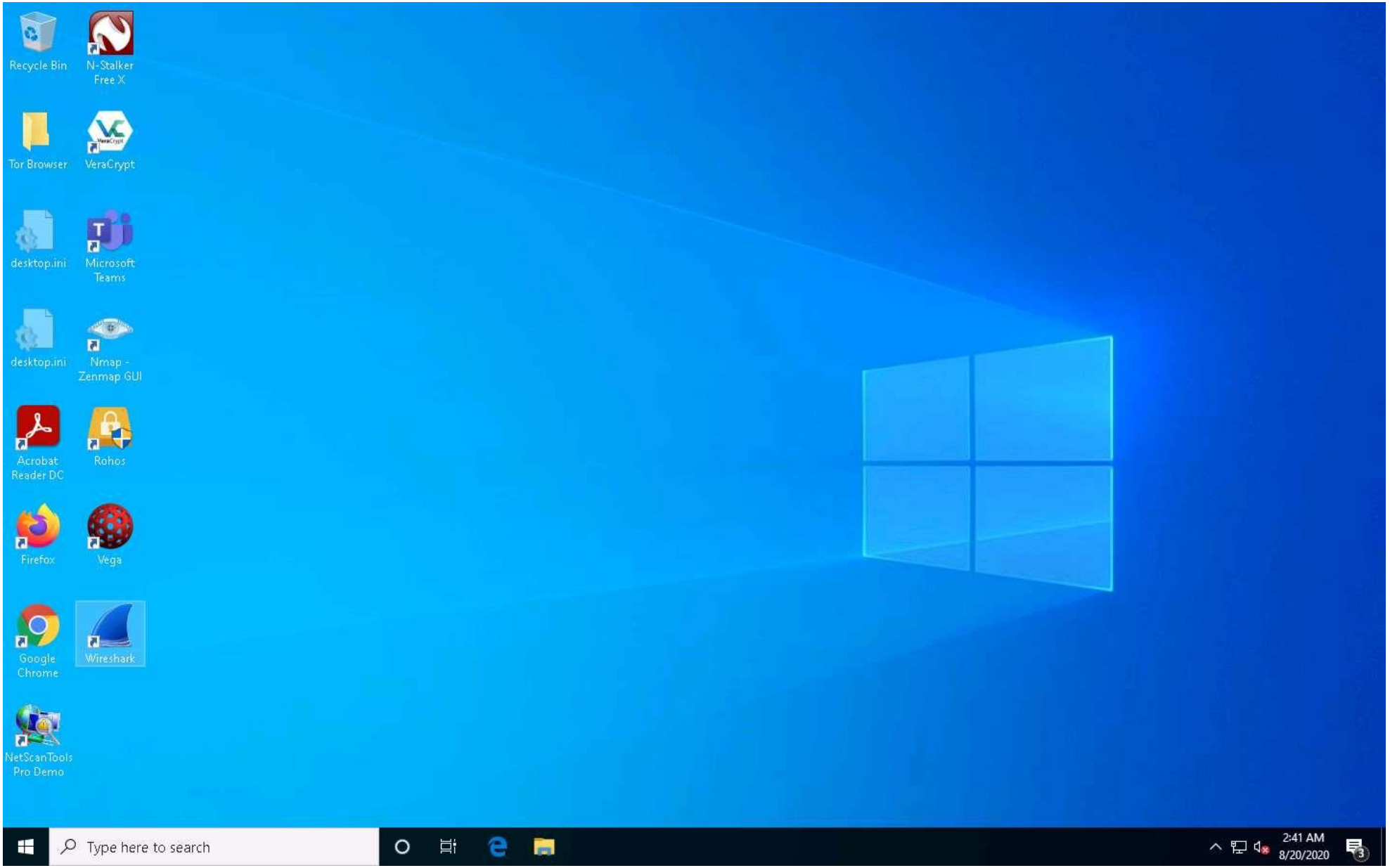
Task 3: Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall

Hping3 is a scriptable program that uses the TCL language, whereby packets can be received and sent via a binary or string representation describing the packets.

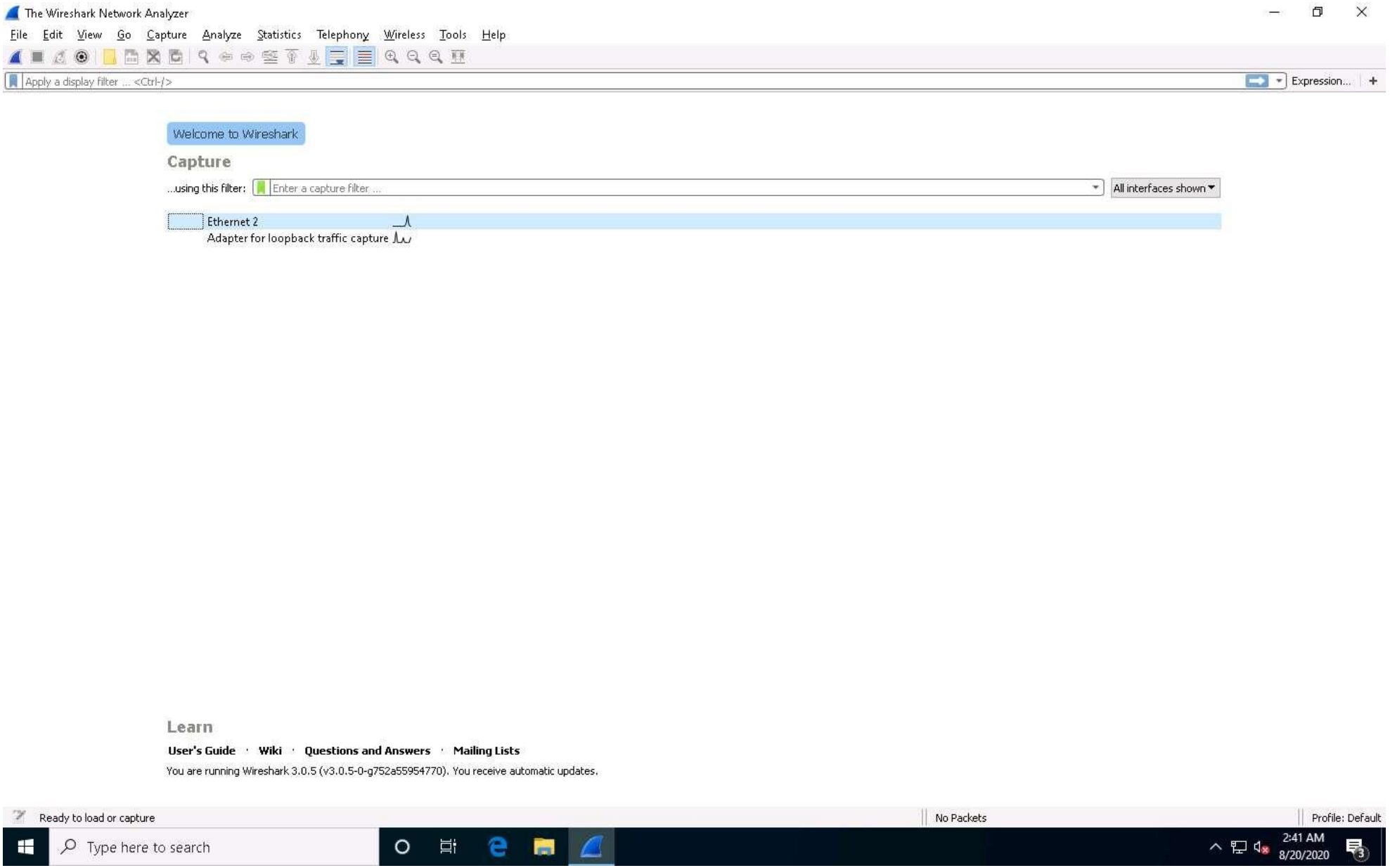
Here, we will use Hping3 to create custom UDP and TCP packets to evade the IDS/firewall in the target network.

Before beginning this task, ensure that the **Windows Defender Firewall** in the **Windows 10** machine is enabled.

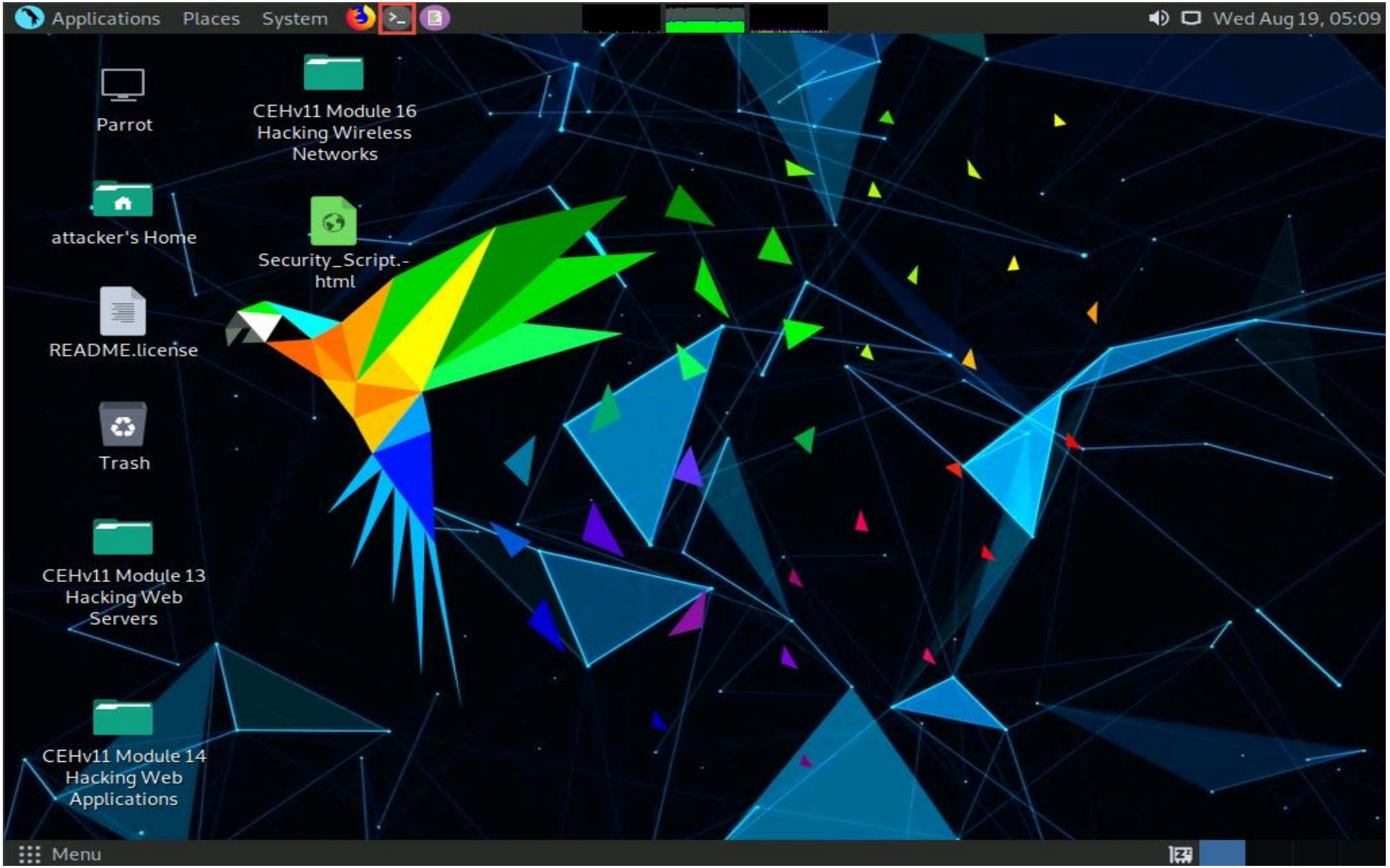
1. Click Windows 10 to switch to the **Windows 10** machine.
2. Navigate to the **Desktop**, double-click **Wireshark** shortcut.



3. ☐ The **Wireshark Network Analyzer** window appears, double-click the available ethernet or interface (here, **Ethernet2**) to start the packet capture.



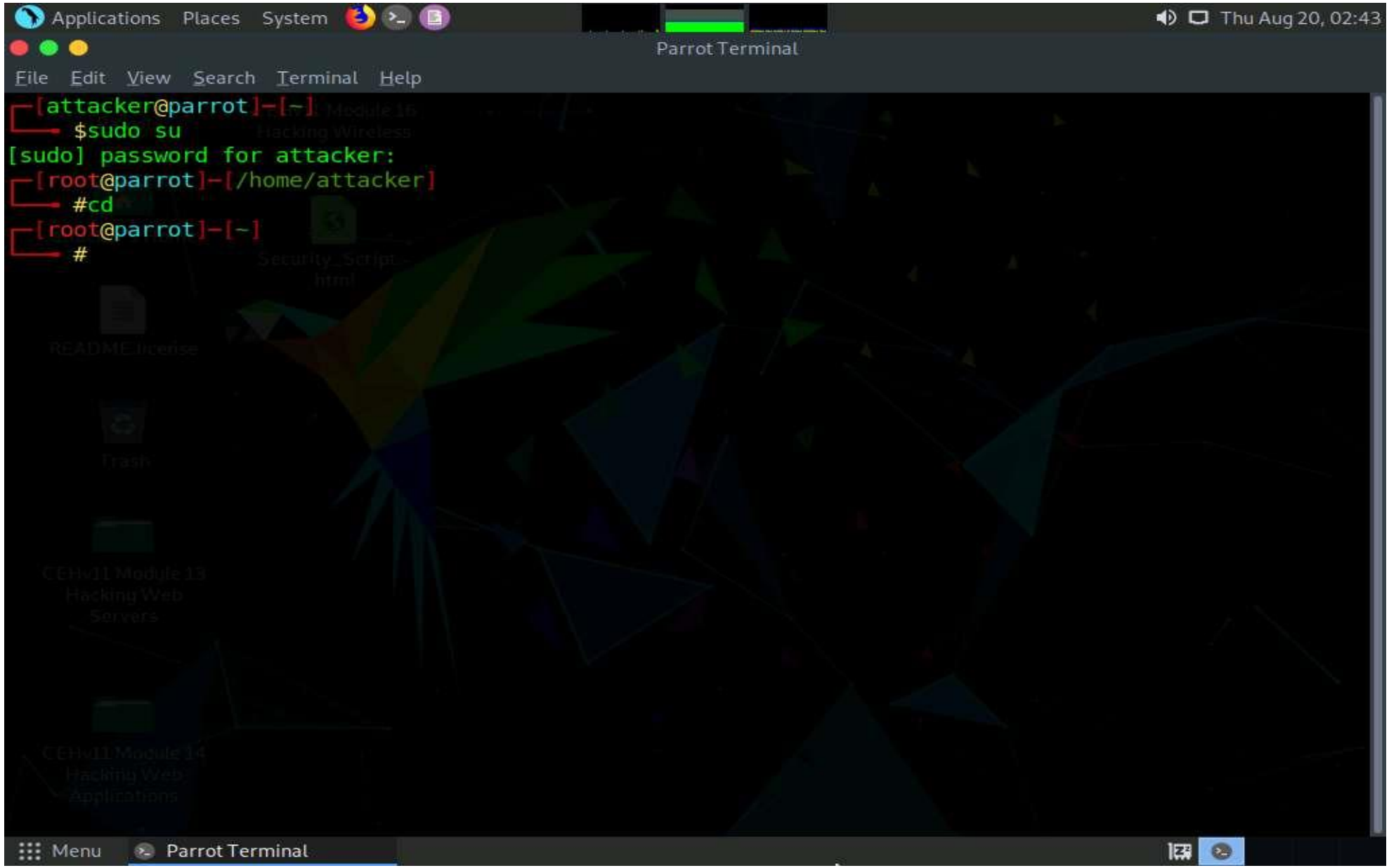
4. ☐ Click Parrot Security to switch to the **Parrot Security** machine.
5. ☐ Click the **MATE Terminal** icon in the top-left corner of the **Desktop** window to open a **Terminal** window.



6. ☐ A **Parrot 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**.

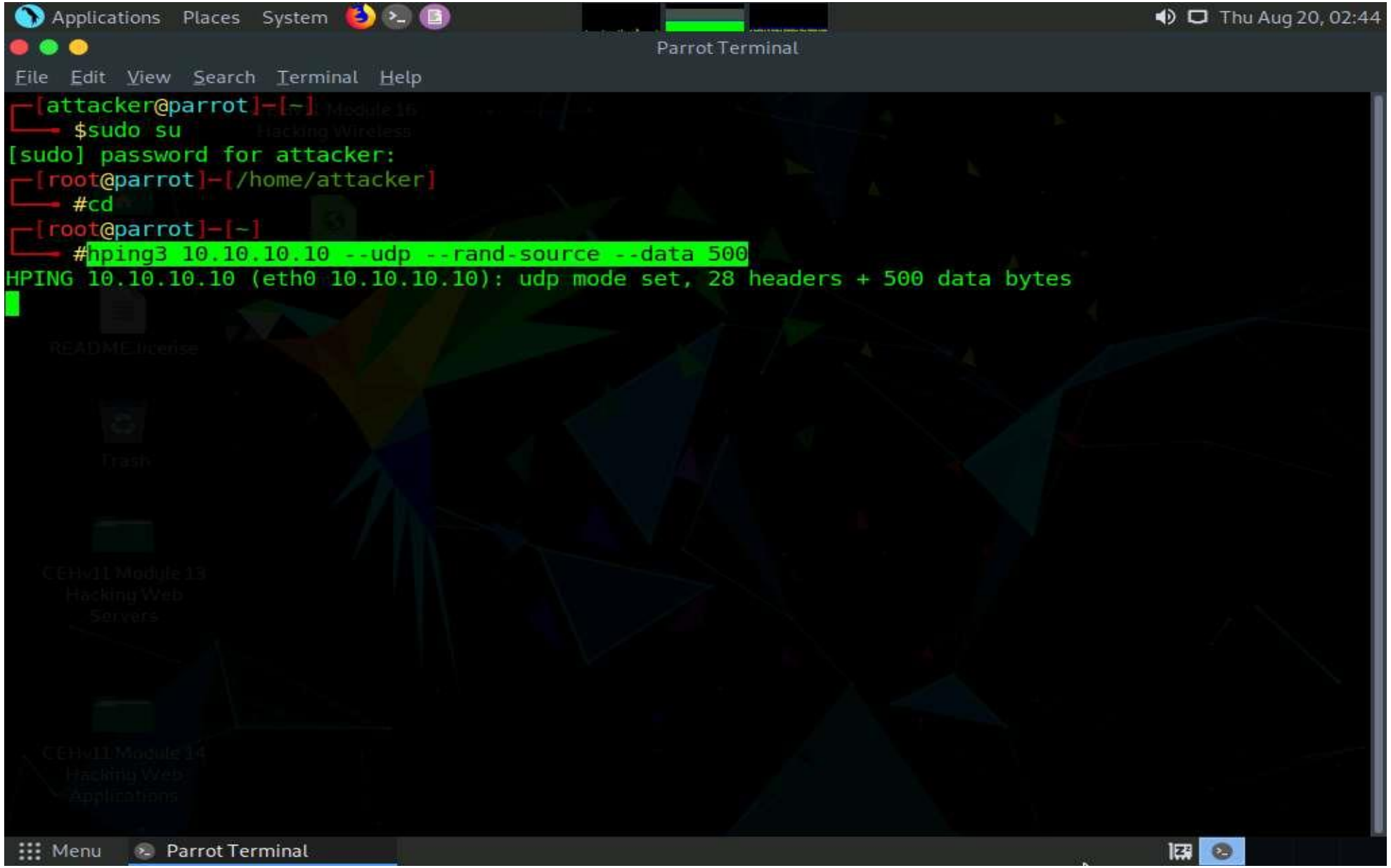
The password that you type will not be visible.

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



9. A **Parrot Terminal** window appears, type **hping3 [Target IP Address] --udp --rand-source --data 500** (here, the target machine is **Windows 10** [**10.10.10.10**]) and press **Enter**.

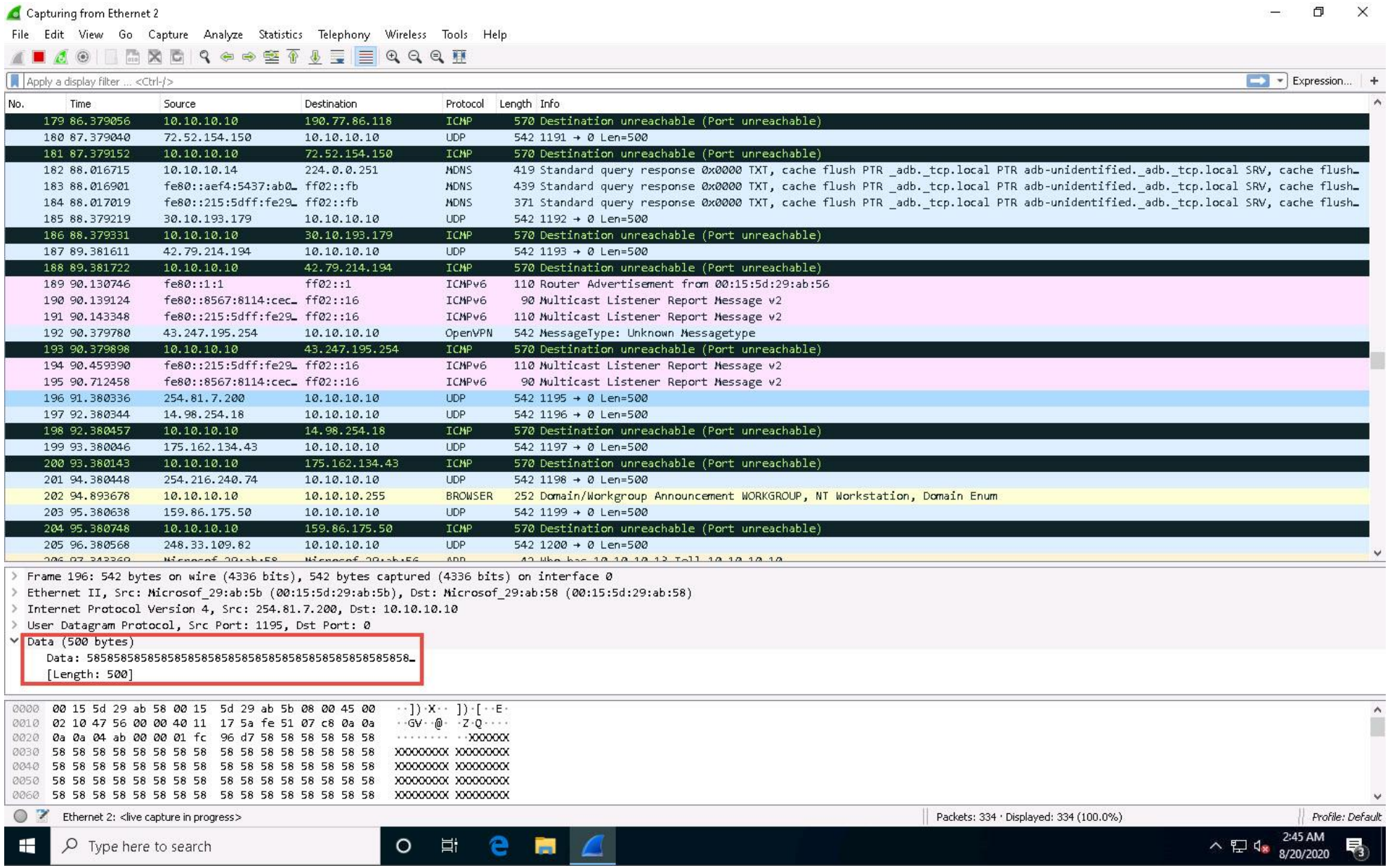
Here, **--udp** specifies sending the UDP packets to the target host, **--rand-source** enables the random source mode and **--data** specifies the packet body size.



10. ☐ Now, click Windows 10 to switch to the **Windows 10** machine and observe the random UDP packets captured by **Wireshark**.

You can double-click any UDP packet and observe the detail.

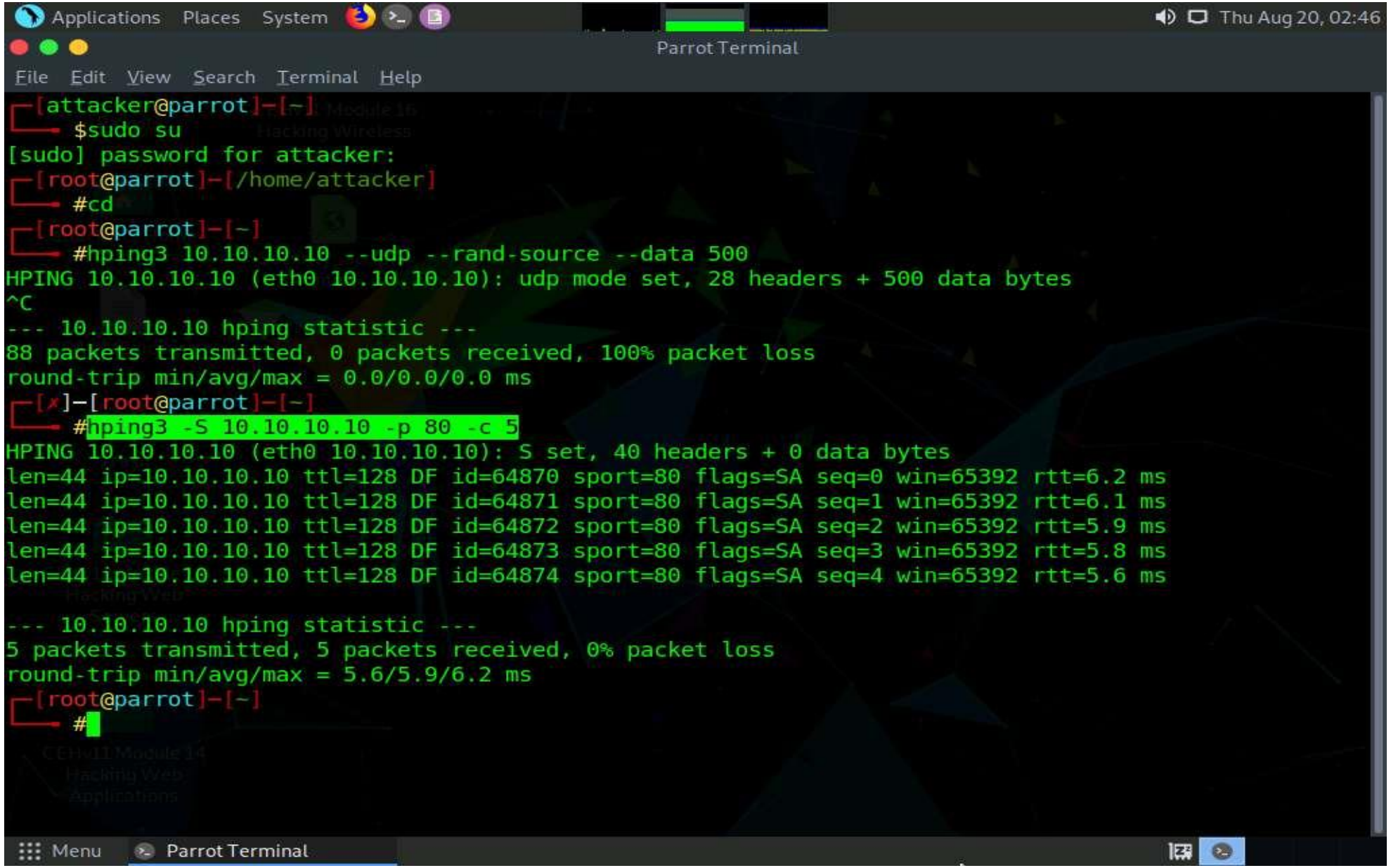
11. Expand the **Data** node in the **Packet Details** pane and observe the size of **Data** and its **Length** (the length is the same as the size of the packet body that we specified in Hping3 command, i.e., **500**).



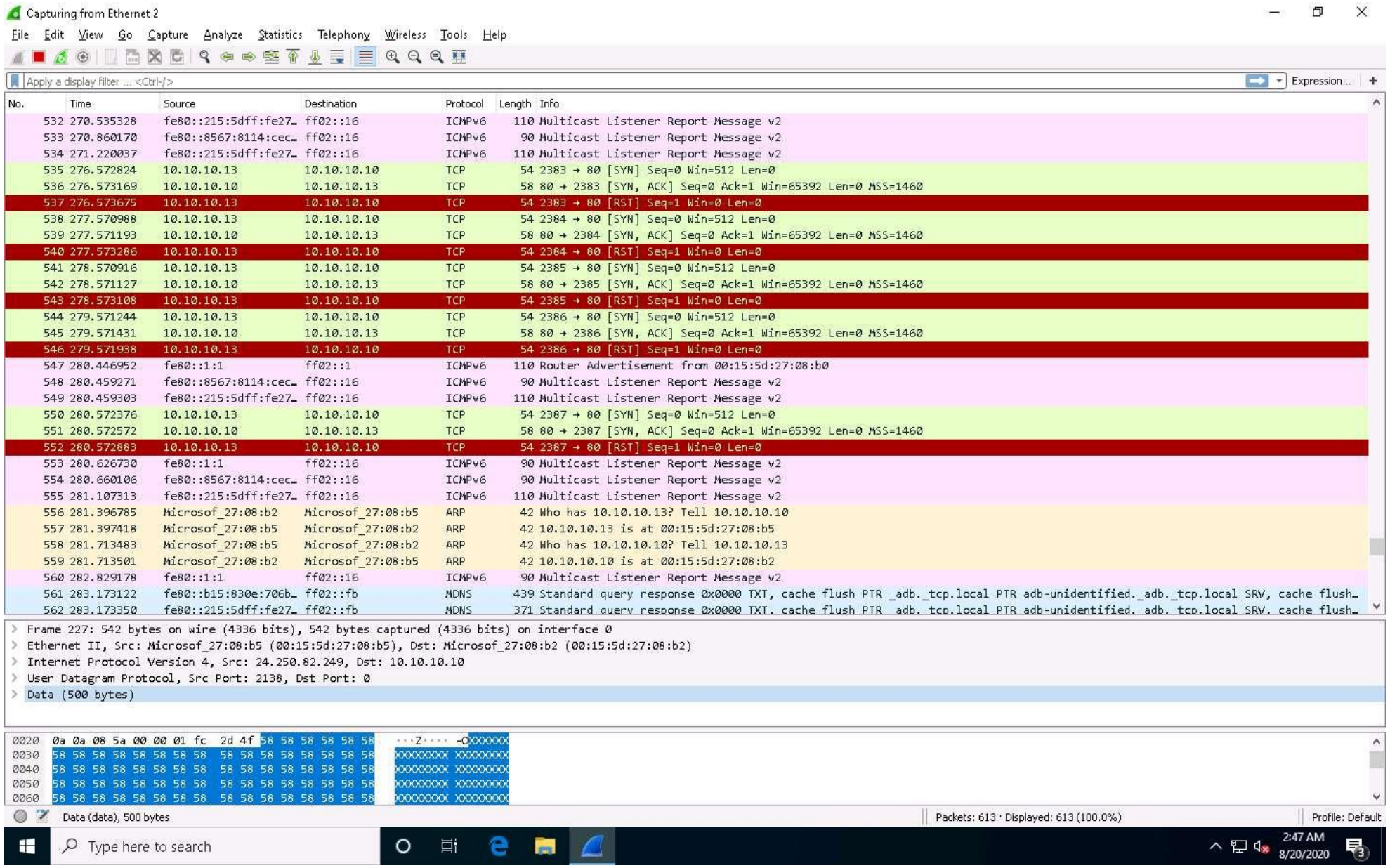
12. Click Parrot Security to switch to the **Parrot Security** machine. In the **Parrot Terminal** window, first press **Control+C** and type **hping3 -S [Target IP Address] -p 80 -c 5** (here, target IP address is **10.10.10.10**), and then press **Enter**.

    Here, **-S** specifies the TCP SYN request on the target machine, **-p** specifies assigning the port to send the traffic, and **-c** is the count of the packets sent to the target machine.

13. In the result, it is indicated that five packets were sent and received through port 80.



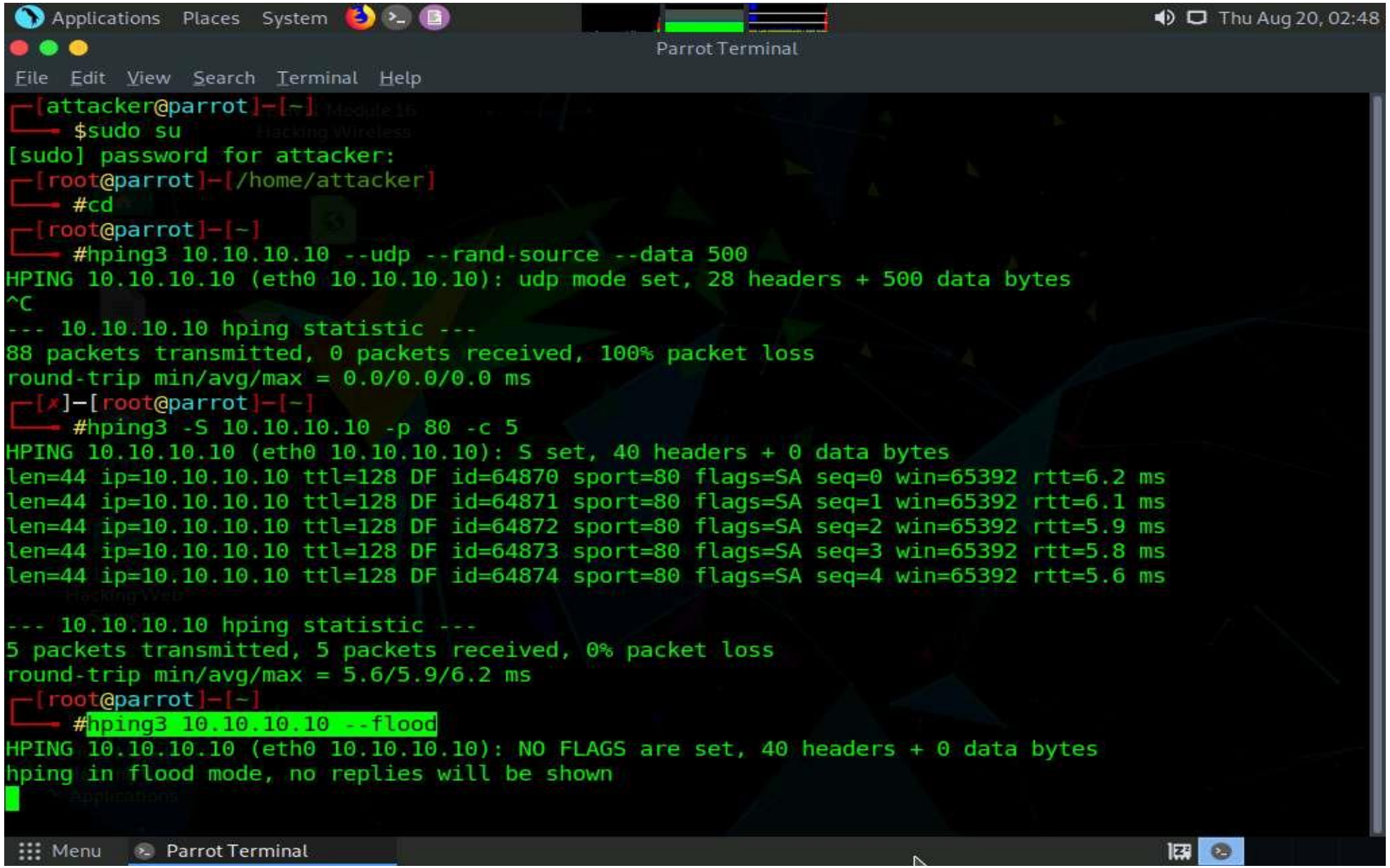
14. ☐ Now, click Windows 10 to switch to the target machine (i.e., **Windows 10**) and observe the TCP packets captured via **Wireshark**.



15. ☐ Click Parrot Security to switch to the **Parrot Security** machine and try to flood the target machine (here, **Windows 10**) with TCP packets.
16. ☐ In the **Parrot Terminal** window, type **hping3 [Target IP Address] --flood** (here, target IP address is **10.10.10.10**) and press **Enter**.

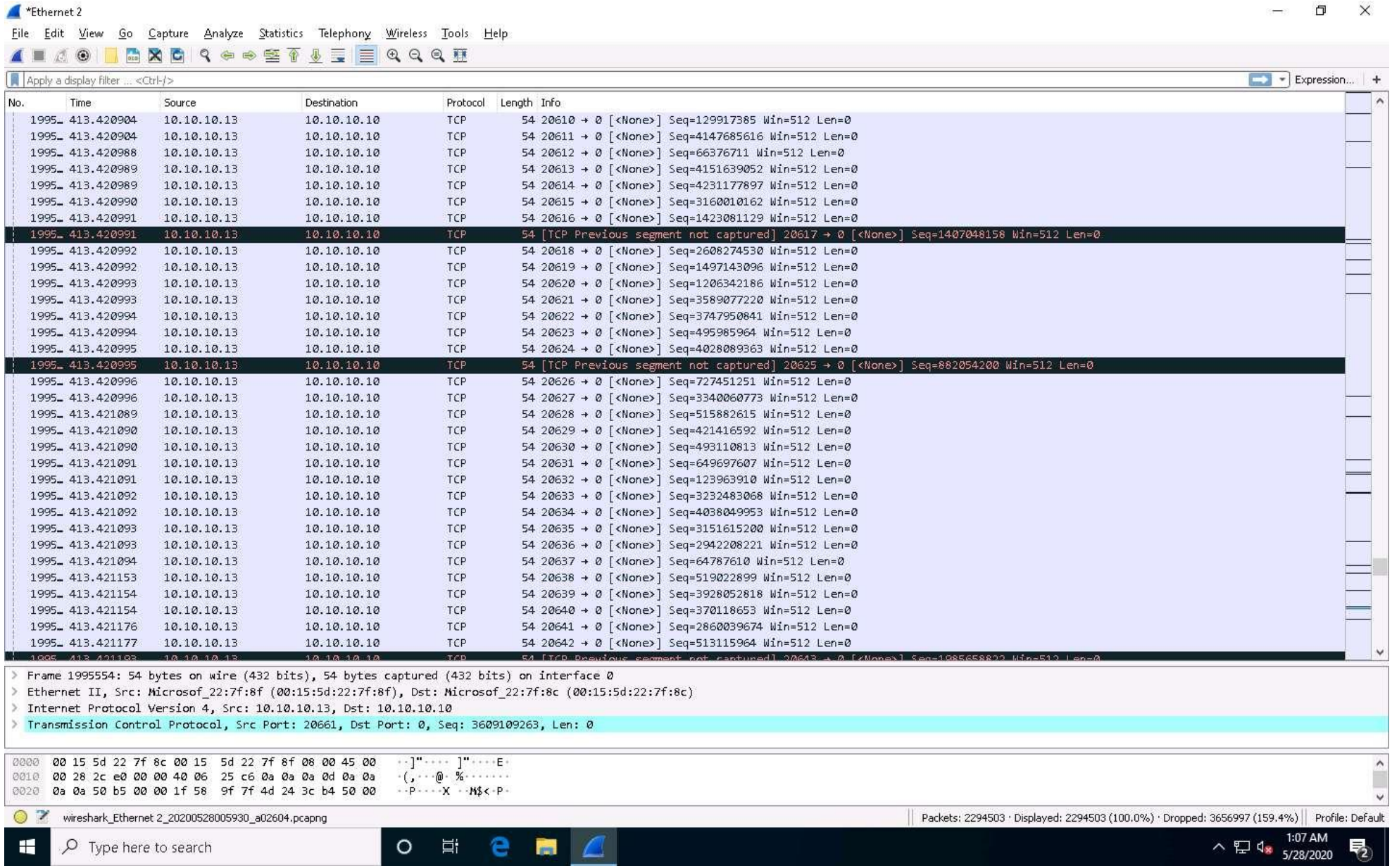
--flood: performs the TCP flooding.

17. Once you flood traffic to the target machine, it will respond in the hping3 terminal.

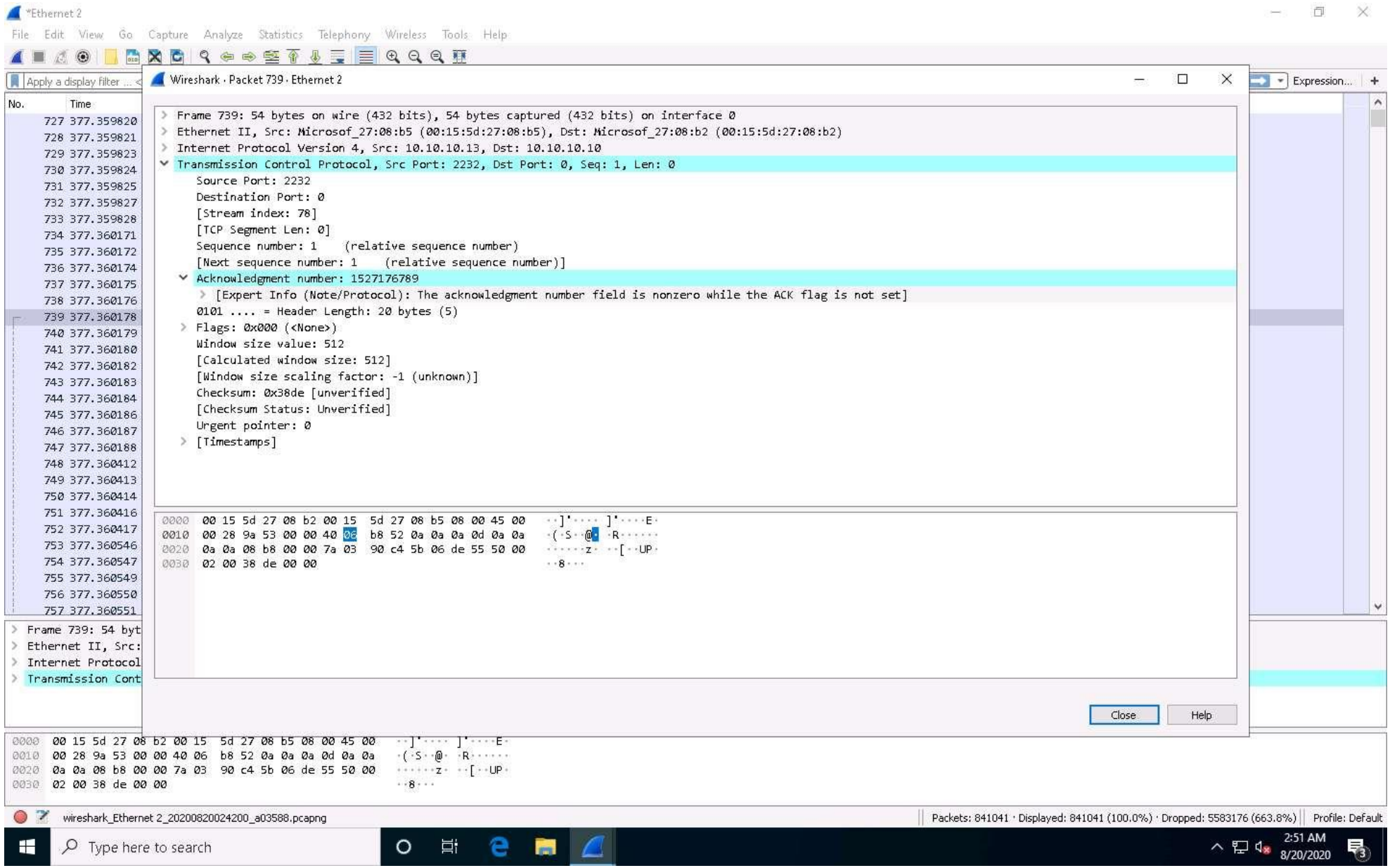


18. Click Windows 10 to switch to the **Windows 10** (target machine) and stop the packet capture in the **Wireshark** window after a while by click **Stop Capturing Packets** icon in the toolbar.
19. Observe the **Wireshark** window, which displays the TCP packet flooding from the host machine.

You can double-click the TCP packet stream to observe the TCP packet information.



20. ☐ The TCP packet stream displays the complete information of TCP packets such as the source and destination of the captured packet, source port, destination port, etc.



21. ☐ This concludes the demonstration of evading the IDS and firewall using various evasion techniques in Hping3.
22. ☐ Close all open windows and document all the acquired information.

Task 4: Create Custom Packets using Nmap to Scan beyond IDS/Firewall

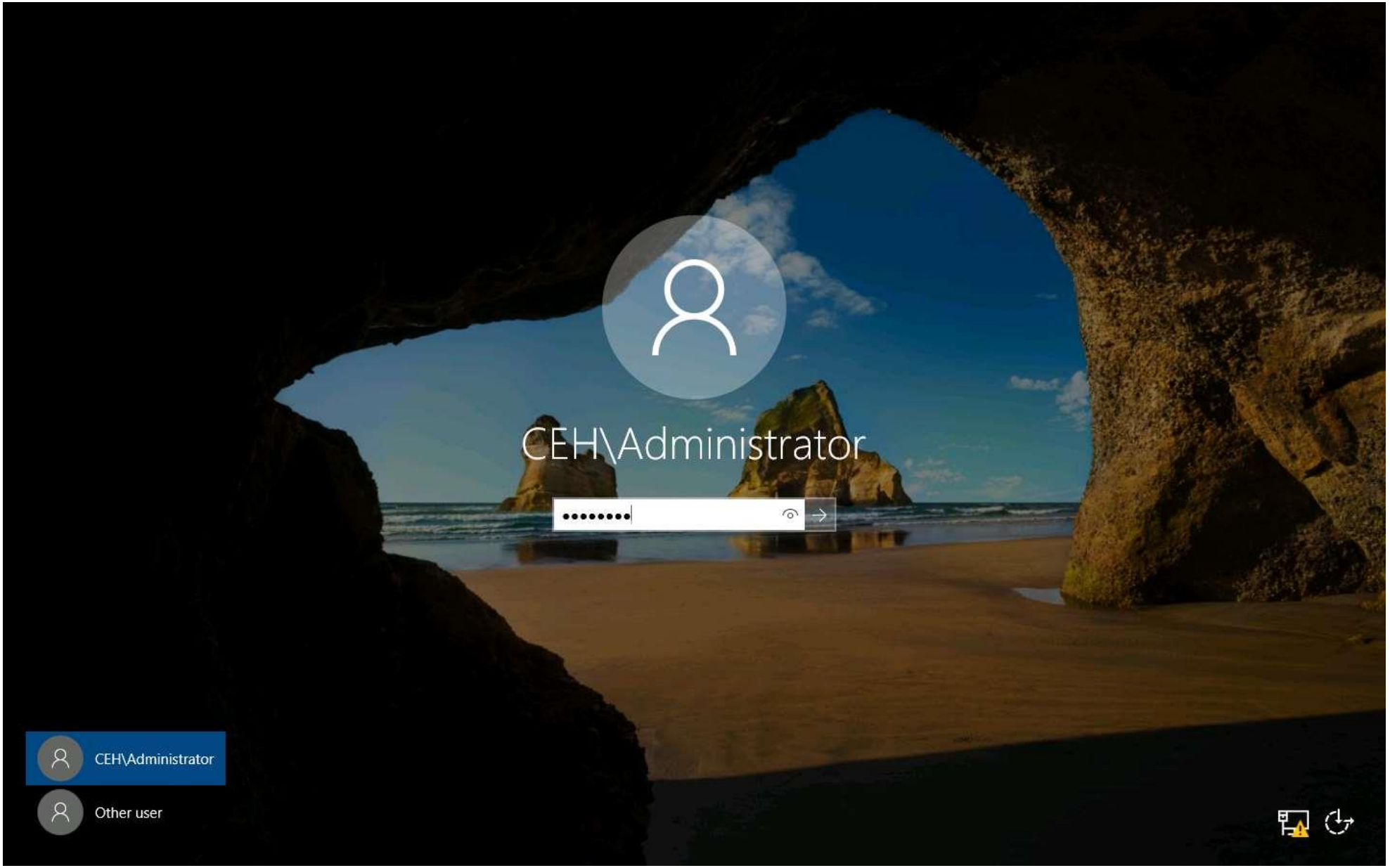
Nmap is a network scanning tool that can be used for sending customized data packets to scan the target host, thus bypassing various security mechanisms such as the IDS/firewall.

Here, we will use Nmap to perform various scanning techniques such as appending custom binary data, appending a custom string, appending random data, randomizing host order, and sending bad checksums to scan the target host beyond the IDS/firewall.

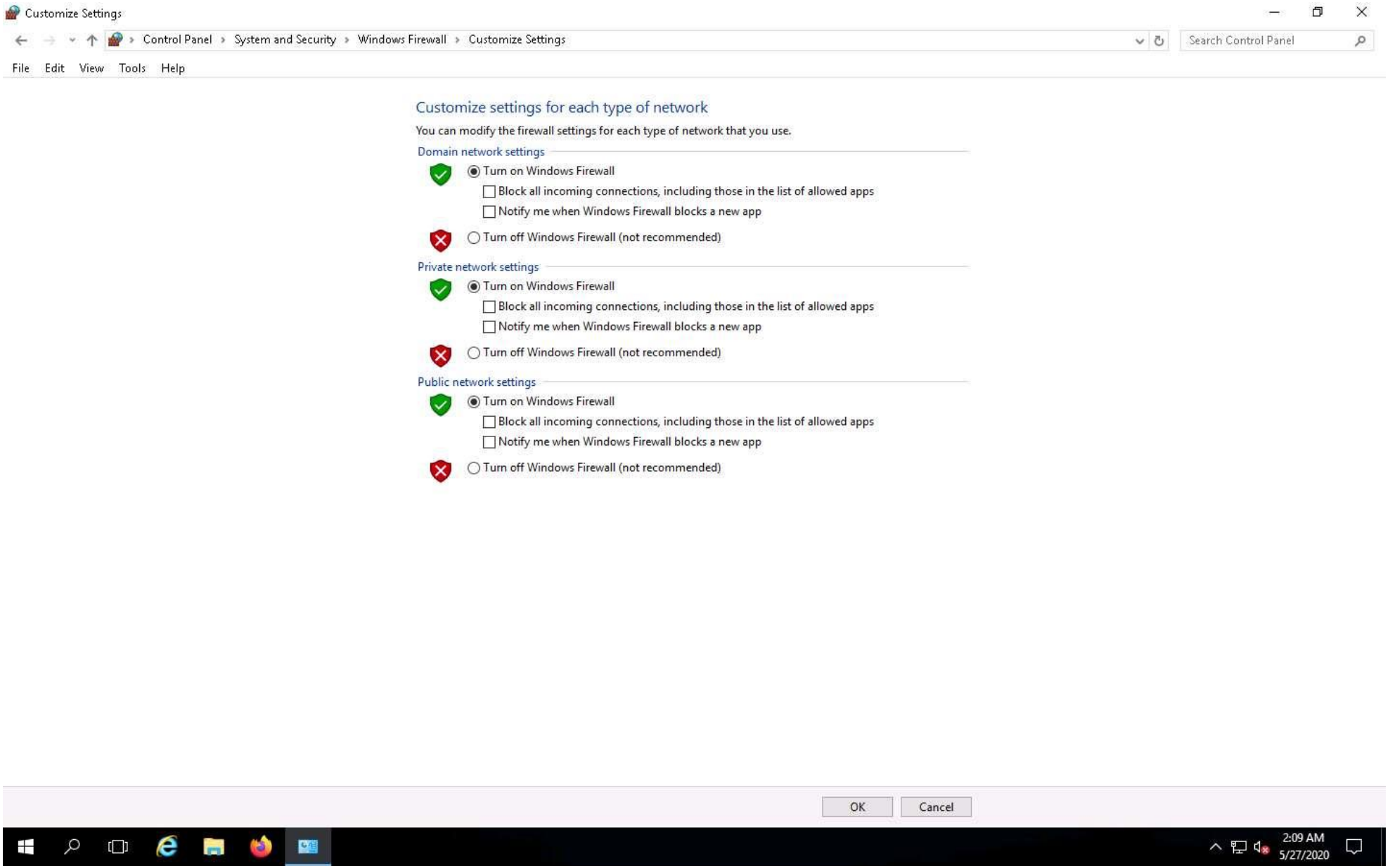
In this task, we are using the **Windows 10** (**10.10.10.10**) machine as a host machine and the **Windows Server 2016** (**10.10.10.16**) machine as a target machine.

1. Click Windows Server 2016 to switch to the **Windows Server 2016** machine.
2. Click Ctrl+Alt+Delete to activate the machine. By default, **Administration** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

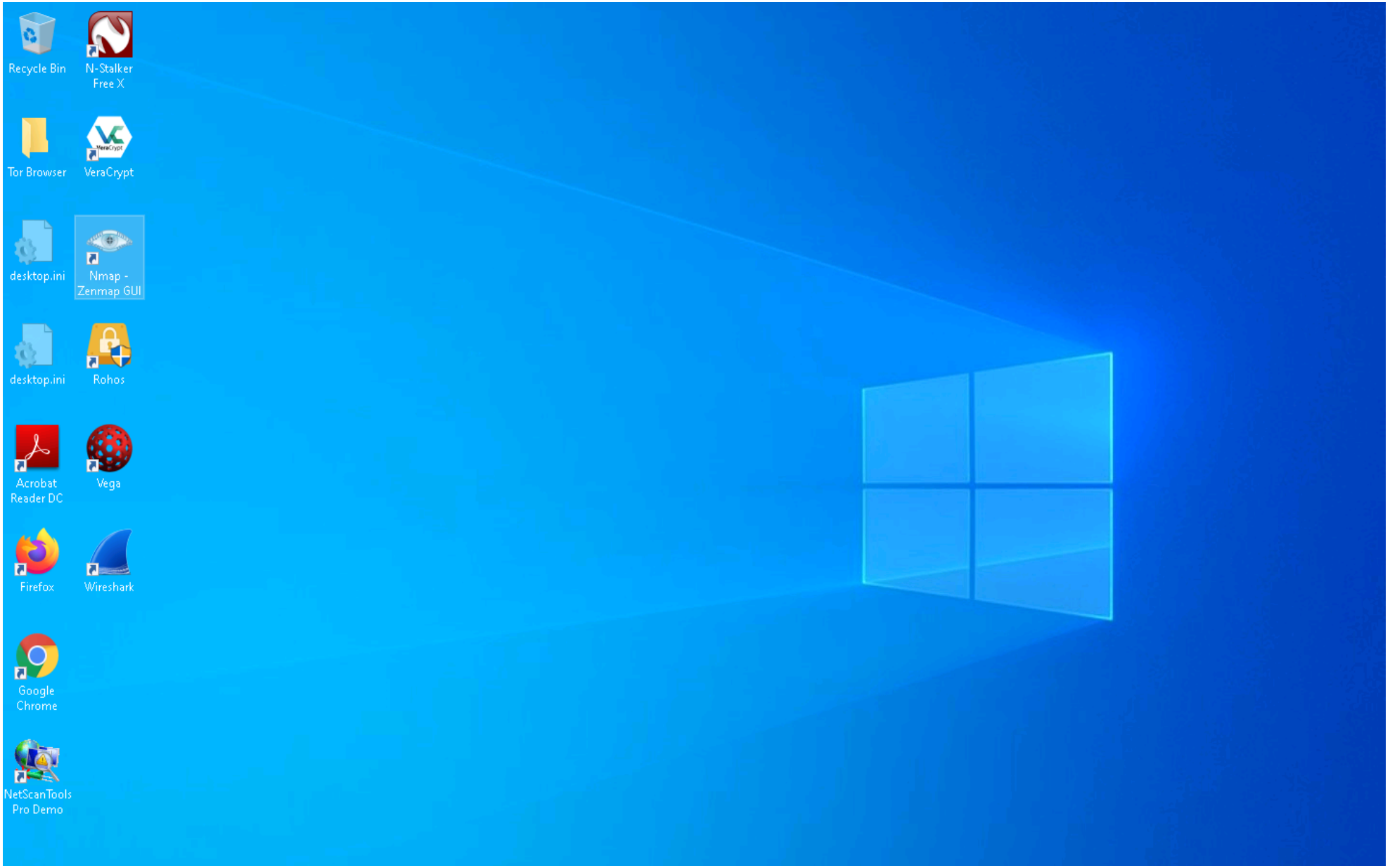
   Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2016** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.



3. Navigate to **Control Panel** --> **System and Security** --> **Windows Firewall** --> **Turn Windows Firewall on or off**, enable Windows Firewall and click **OK**, as shown in the screenshot.



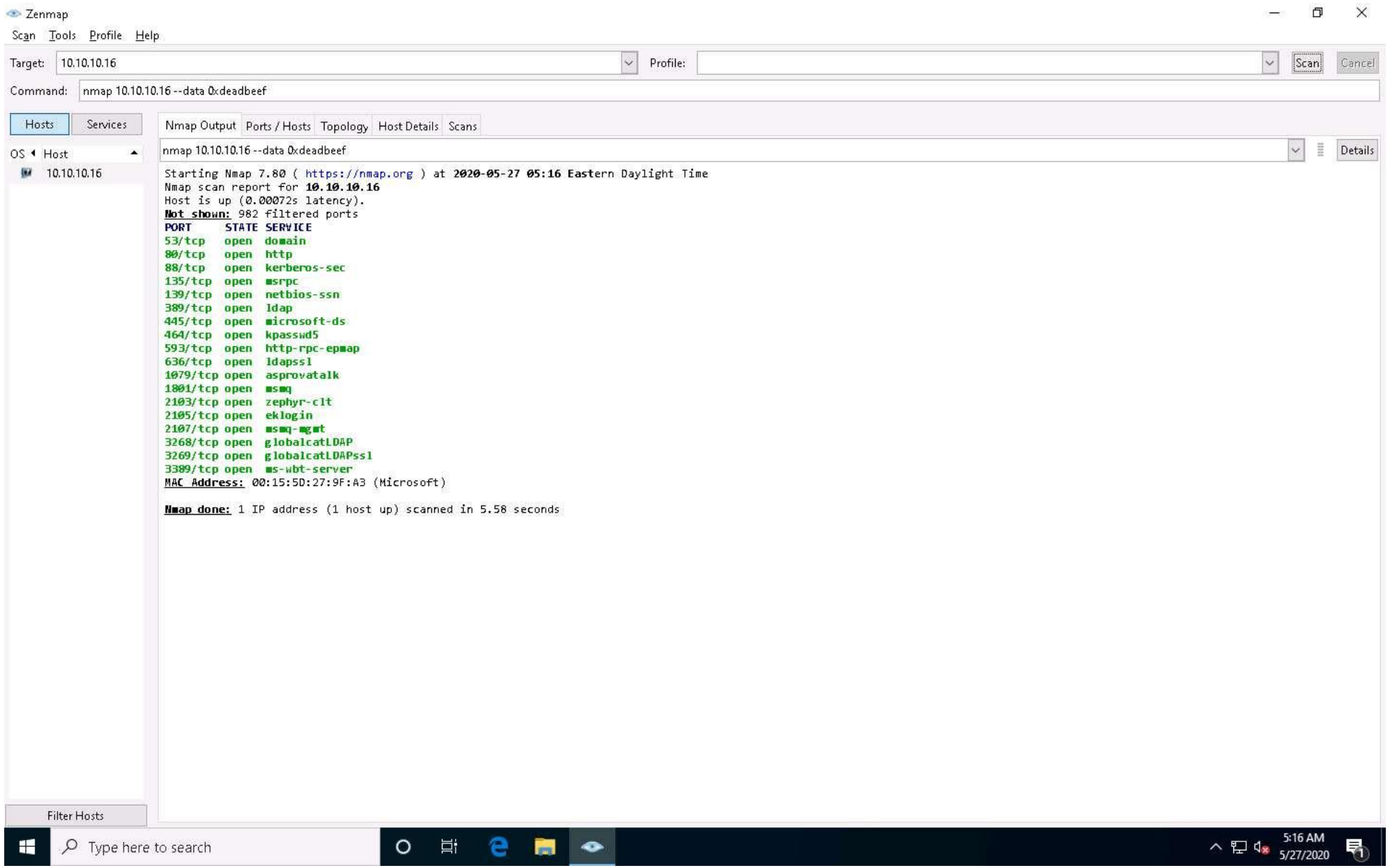
4. Click Windows 10 to switch to the **Windows 10** machine and launch **Nmap** by double-clicking on the **Nmap - Zenmap GUI** shortcut available on the **Desktop**.



5. ☐ The **Nmap - Zenmap GUI** appears. In the **Command** field, type the command **nmap [Target IP Address] --data 0xdeadbeef** (here, target IP address is **10.10.10.16**) and click **Scan**.

Nmap uses **--data [hex string]** (here, **0xdeadbeef**) to send the binary data (o's and 1's) as payloads in the sent packets to scan beyond firewalls.

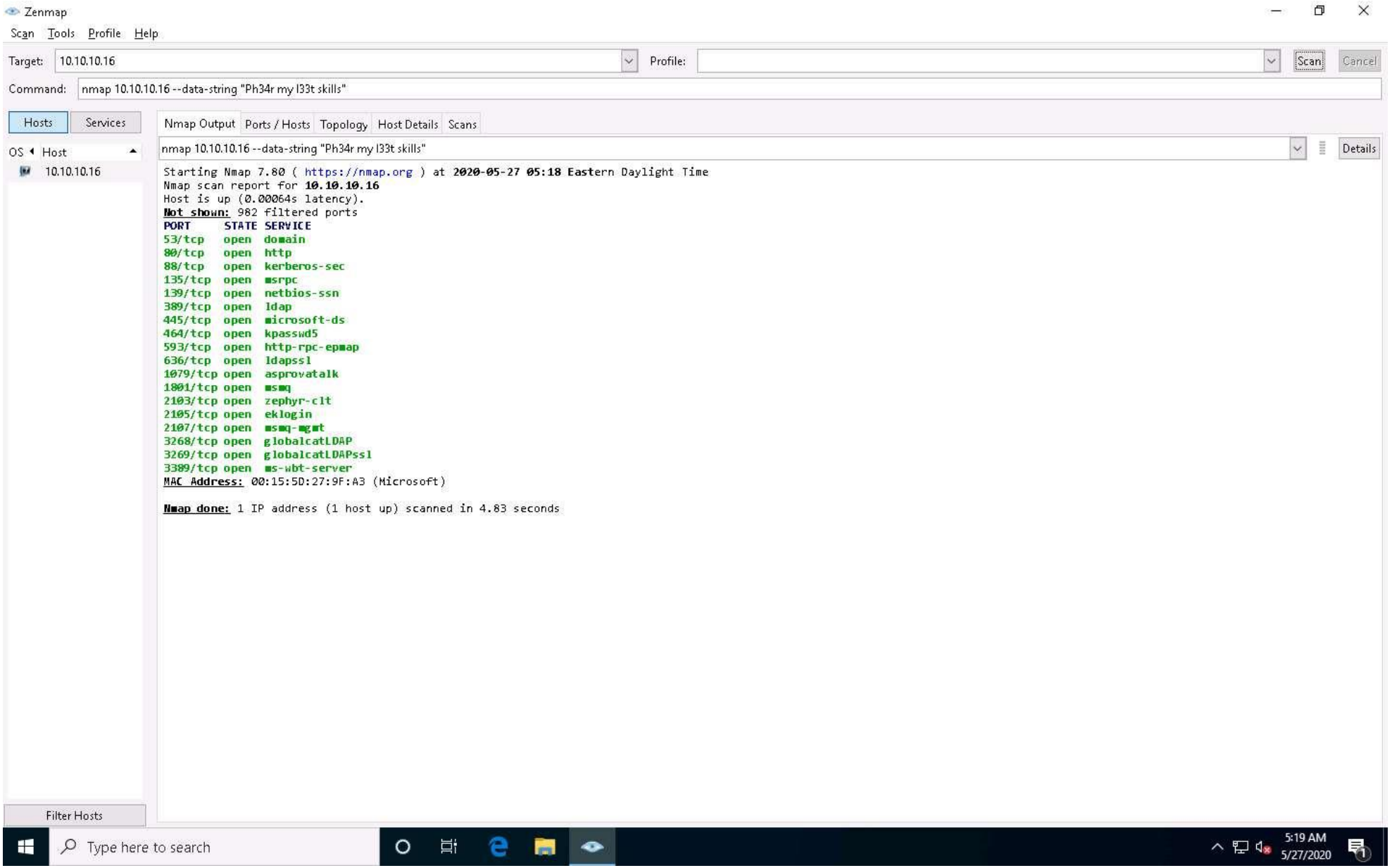
6. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.



7. In the **Command** field, type the command **nmap [Target IP Address] --data-string "Ph34r my l33t skills"** (here, target IP address is **10.10.10.16**) and click **Scan**.

   Nmap uses **--data-string [string]** (here, "**Ph34r my l33t skills**") to send a regular string as payloads in the sent packets to the target machine for scanning beyond the firewall.

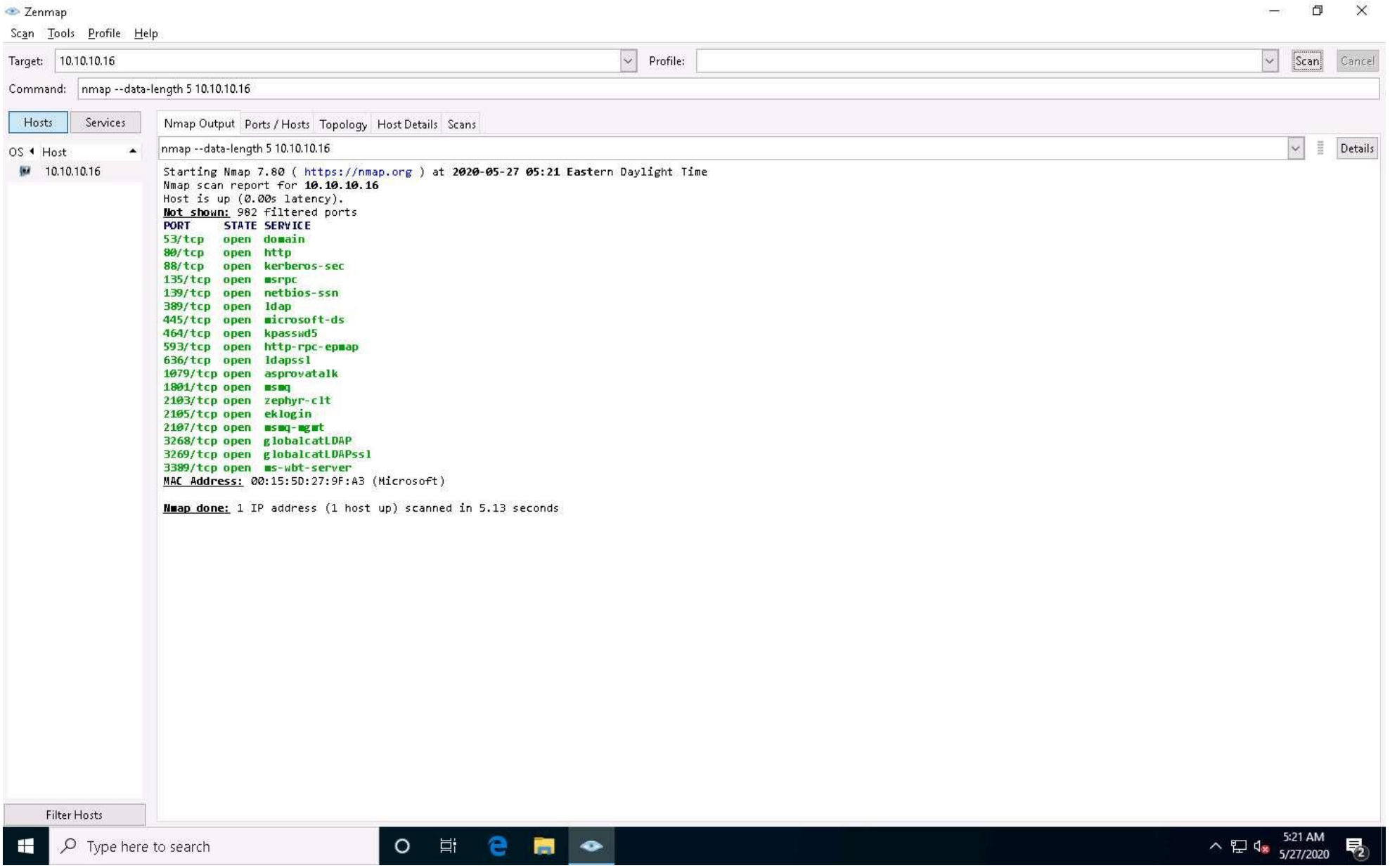
8. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.



9. ☐ In the **Command** field, type the command **nmap --data-length 5 [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Nmap uses **--data-length [len]** (here, **5**) to append the number of random data bytes to most of the packets sent without any protocol-specific payloads.

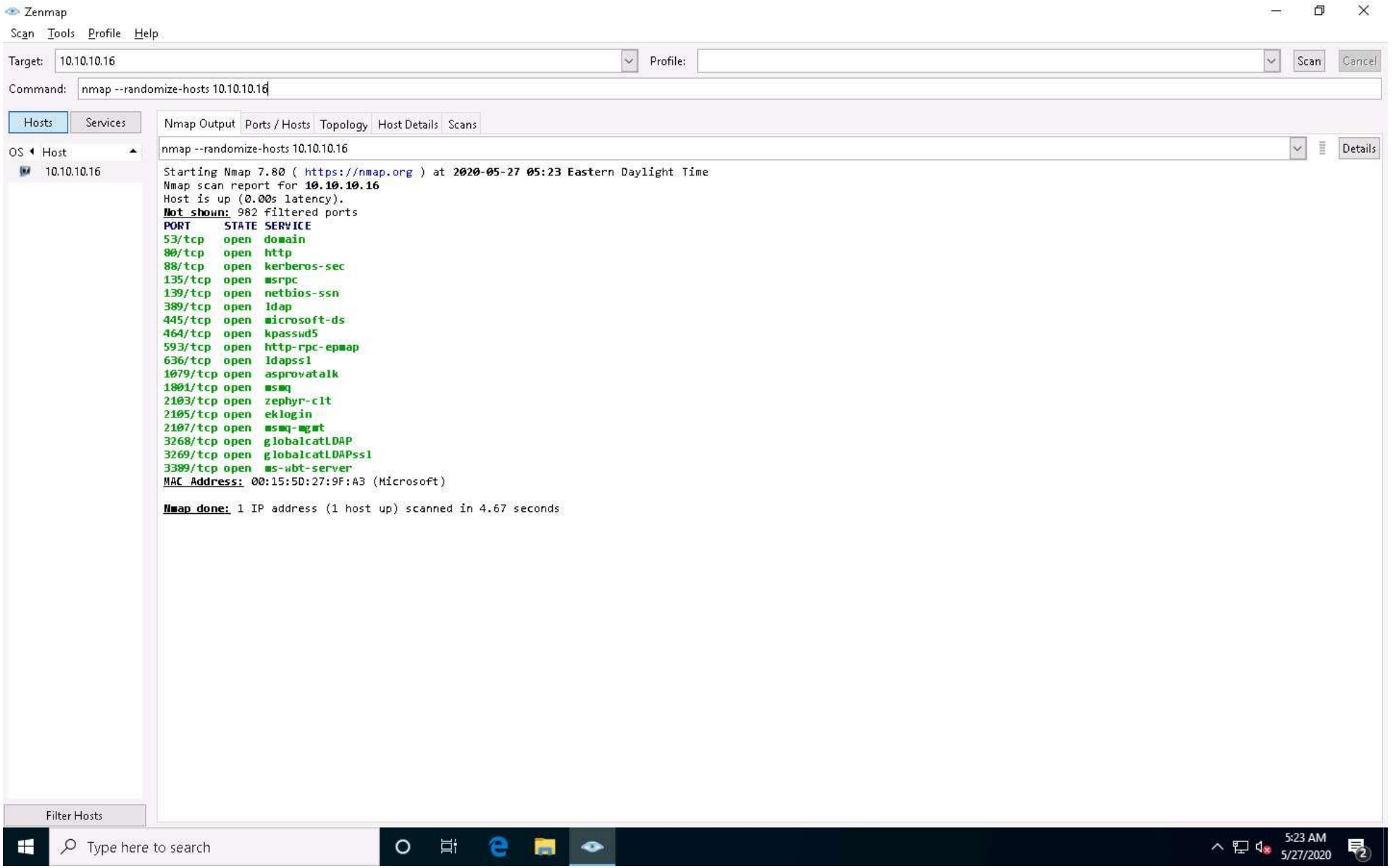
10. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.



11. In the **Command** field, type the command **nmap --randomize-hosts [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Nmap uses **--randomize-hosts** to scan the number of hosts in the target network in random order to scan the intended target that is beyond the firewall.

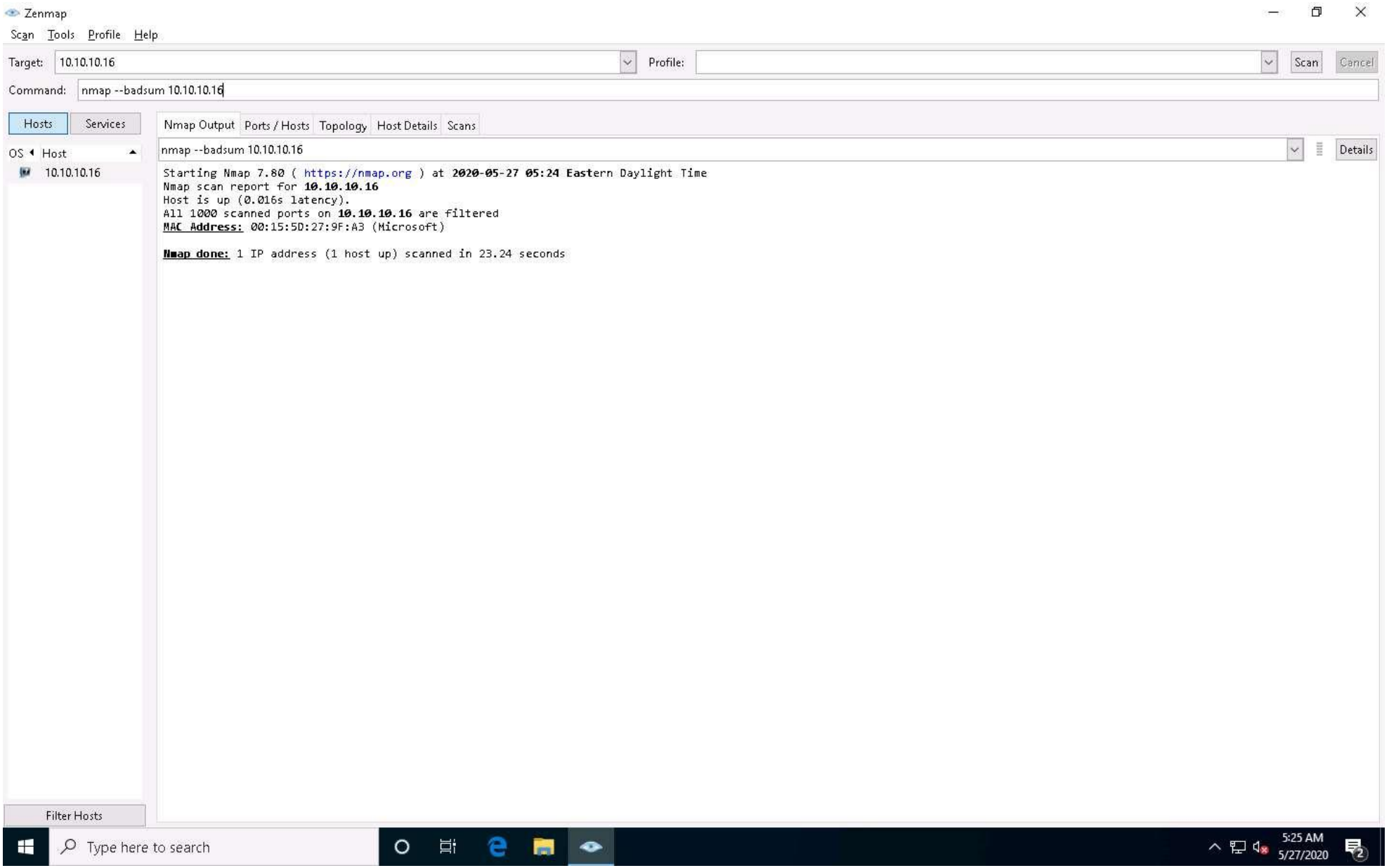
12. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.



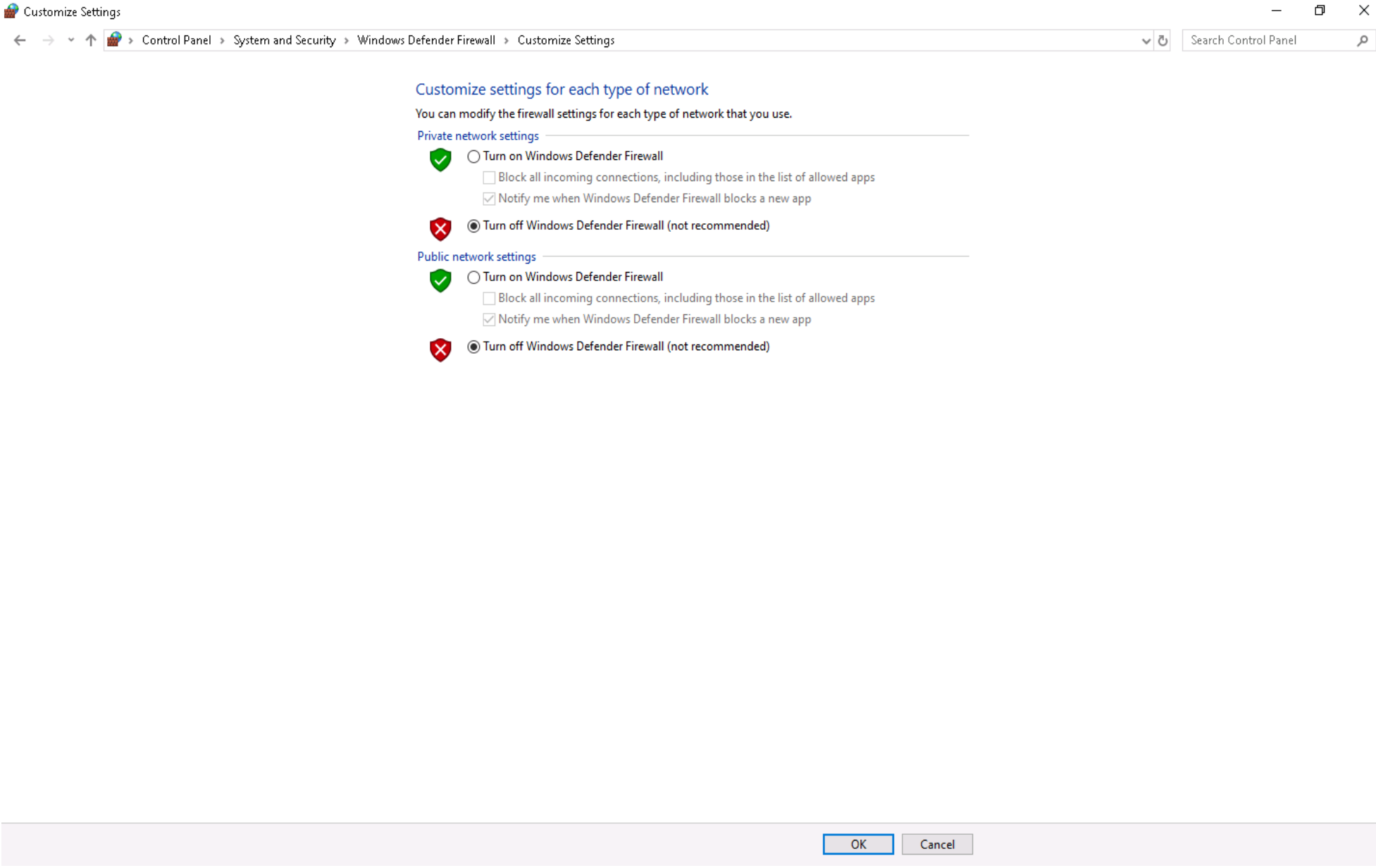
13. ☐ In the **Command** field, type the command **nmap --badsum [Target IP Address]** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Nmap uses **--badsum** to send the packets with bad or bogus TCP/UPD checksums to the intended target to avoid certain firewall rulesets.

14. The scan results appear, demonstrating that all ports are filtered, indicating that there is no response or the packets are dropped, and thus it can be inferred that the system is configured.



15. ☐ This concludes the demonstration of creating custom packets using Nmap to scan beyond the IDS and firewall.
16. ☐ You can also use other packet crafting tools such as **NetScanTools Pro** (https://www.netscantools.com), **Ostinato** (https://www.ostinato.org), and **WAN Killer** (https://www.solarwinds.com) to build custom packets to evade security mechanisms.
17. ☐ Close all open windows and document all the acquired information.
18. ☐ Turn off the **Windows Firewall** in the **Windows 10** and **Windows Server 2016** machines by navigating to **Control Panel** --> **System and Security** --> **Windows Defender Firewall** --> **Turn Windows Defender Firewall on or off**.


Customize Settings
Control Panel › System and Security › Windows Defender Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Public network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
OK
Cancel