Practice Labs - Ethical Hacker v10

Denial of Service

- **Introduction**
- **Lab Topology**
- **Exercise 1 - Perform Denial-of-Service (DoS) Attacks**
- **Exercise 2 - Know About DoS/DDoS Prevention**
- **Review**

Introduction

Denial of Service
DoS
Distributed Denial of Service
DDoS
Wireshark
SYN Flooding
ICMP Flood Attack
Ping of Death Attack
SYN Floor Attack
Metasploit Framework
Ethical Hacking

Welcome to the **Denial of Service** Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Perform Denial-of-Service (DoS) Attacks
- Exercise 2 - Know About DoS/DDoS Prevention

After completing this lab, you will be able to:

- Install Wireshark
- Perform SYN Flooding Attack
- Switch Off the Windows Firewall on PLABWIN10
- Perform an ICMP Flood Attack
- Perform the Ping of Death Attack
- Perform an SYN Floor Attack Using Metasploit Framework
- Know about DoS/DDoS Prevention Methods

Exam Objectives

The following exam objectives are covered in this lab:

- **3.2** Information Security Attack Detection
- **3.3** Information Security Attack Prevention

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **1 hour** to complete this lab.

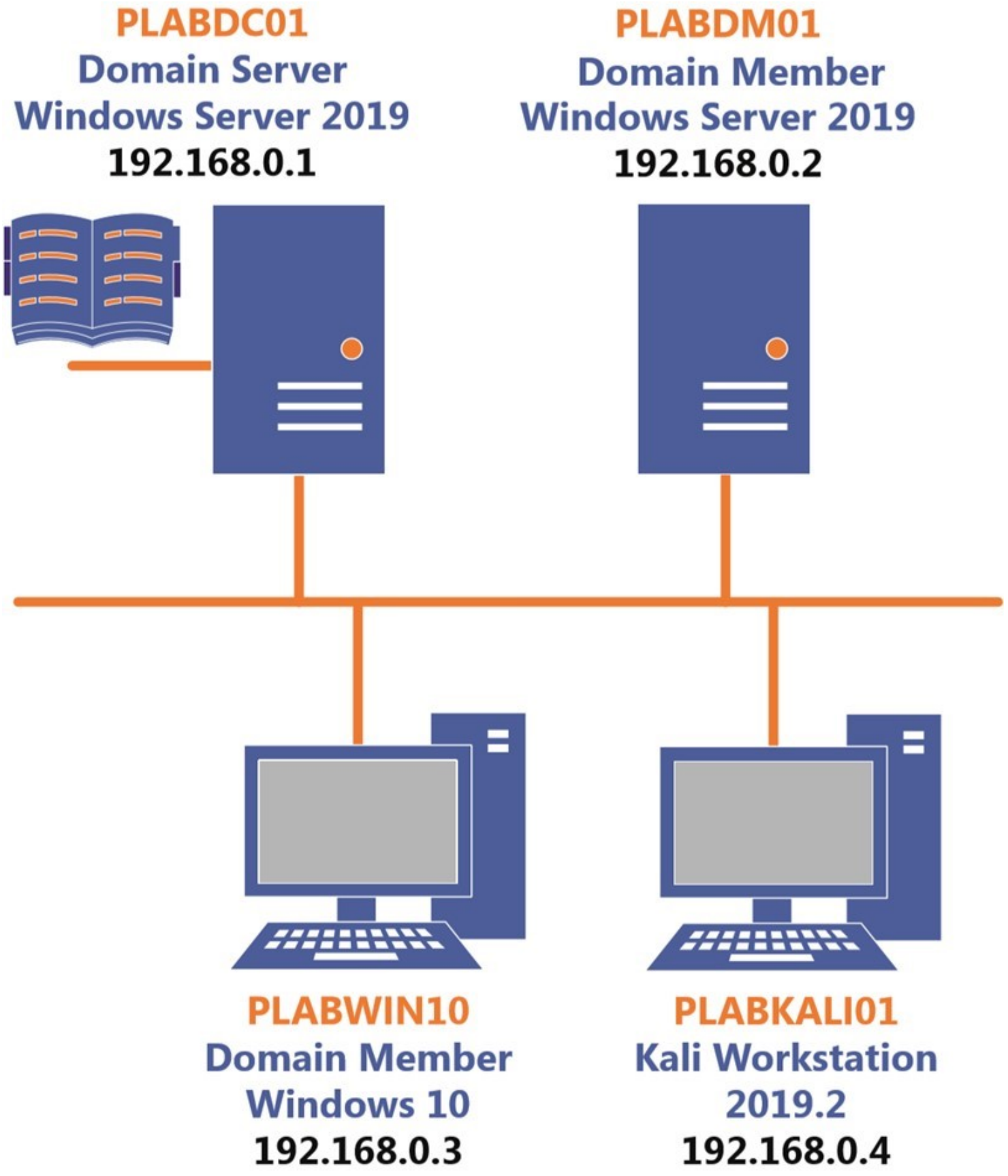
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

> Click **Next** to view the Lab topology used in this module.

Lab Topology

During your session, you will have access to the following lab configuration.



Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Member)
- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)

Click **Next** to proceed to the first exercise.

Exercise 1 - Perform Denial-of-Service (DoS) Attacks

A Denial of Service (DoS) attack is conducted using one system, which sends a high amount of traffic to the target system. The DoS attack is one to one kind of attack in which a single system, used by the attacker, targets another system, which is usually a server. When this attack is launched on a target, it drains out the system of its resources. Eventually, when the target runs out of system resources, it becomes unavailable to provide services to legitimate users.

Distributed Denial of Service (DDoS) has the same intent, but its method of execution is slightly different. Instead of using a single system, it may use hundreds or thousands (or even more) systems, which are known as zombies or bots, to attack one or more target systems. This type of attack sometimes becomes slightly difficult to detect as the traffic originates from different systems, which obviously have different IP addresses.

Key tools used for DoS/DDoS attack:

- Low Orbit Ion Cannon (LOIC)
- HOIC
- XOIC
- HTTP Unbearable Load King (HULK)

- UDP Flooder
- R-U-Dead-Yet (RUDY)
- Nemesy
- ToR's Hammer
- Pyloris
- OWASP Switchblade
- DAVOSET

In this exercise, you will learn to perform DoS attacks within the lab environment.

Learning Outcomes

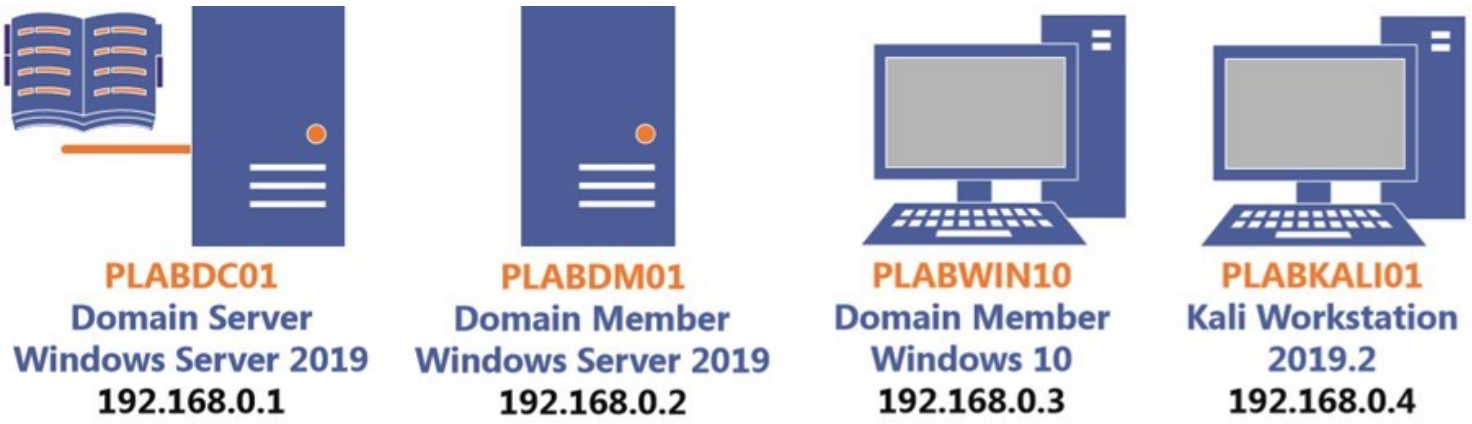
After completing this exercise, you will be able to:

- Install Wireshark
- Perform SYN Flooding Attack
- Switch Off the Windows Firewall on PLABWIN10
- Perform an ICMP Flood Attack
- Perform the Ping of Death Attack
- Perform an SYN Floor Attack Using Metasploit Framework

Your Devices

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Member)
- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)



Task 1 - Install Wireshark

Wireshark is a packet capturing tool. It can capture packets that traverse through the network. You can use Wireshark for also sniffing the network traffic.

In this task, you will learn to install Wireshark. To do this, perform the following steps:

Step 1

Ensure you have powered the required devices. Connect to **PLABWIN10**.

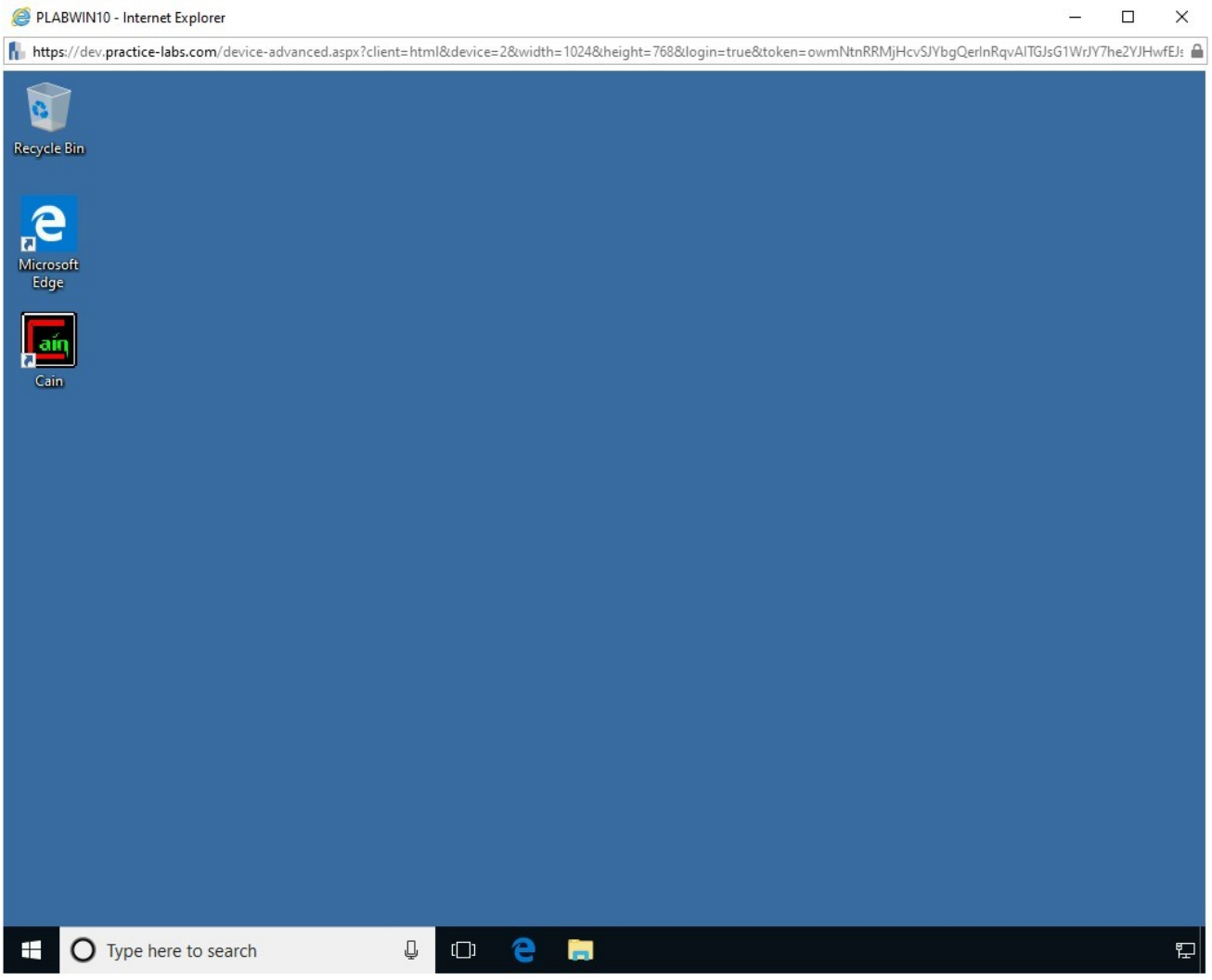


Figure 1.1 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Step 2

In the **Type here to search** text box, type the following:

```
Internet Explorer
```

From the search results, select **Internet Explorer**.

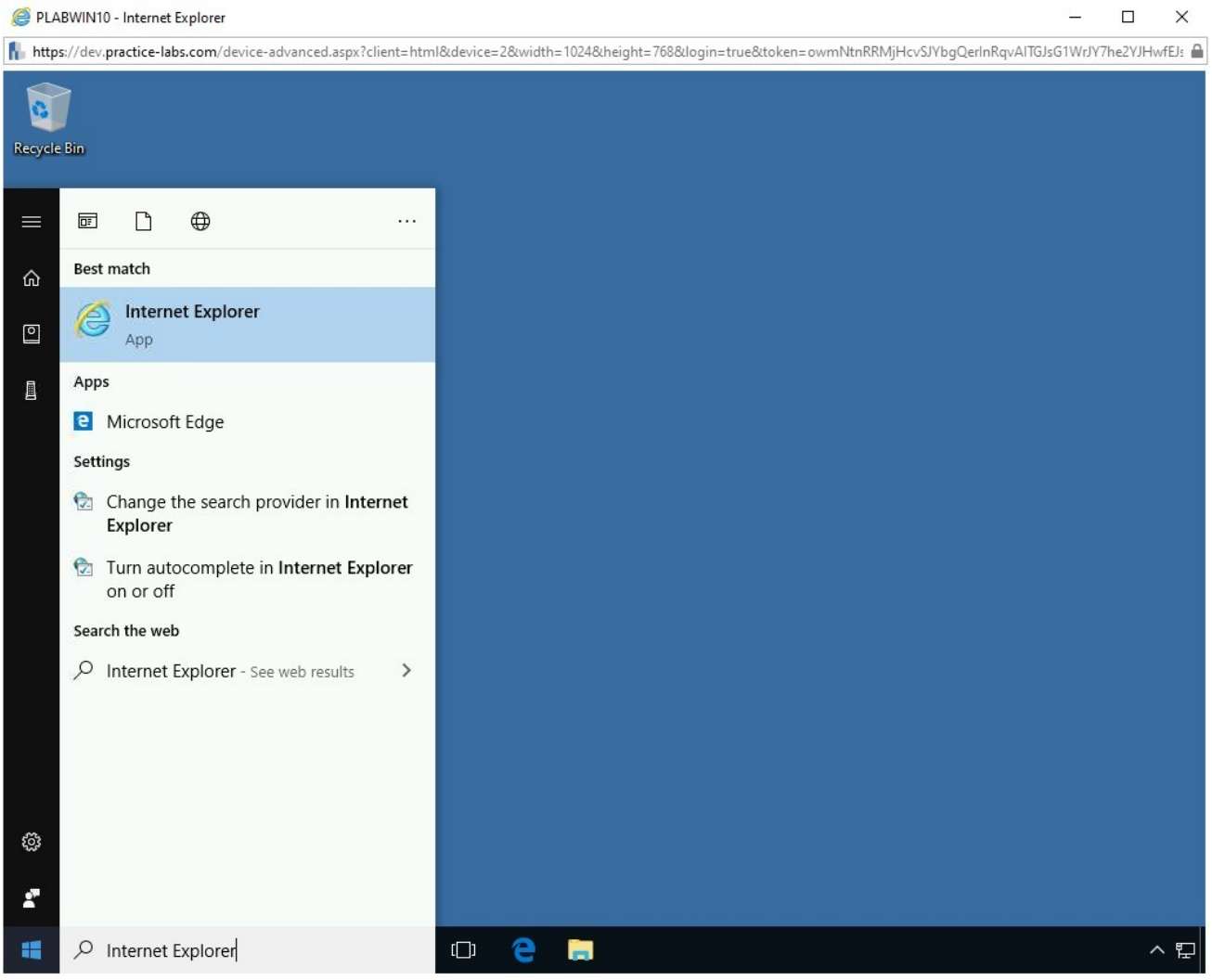


Figure 1.2 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

Step 3

The Intranet Website is displayed. On the **Intranet** homepage, click **Tools**.

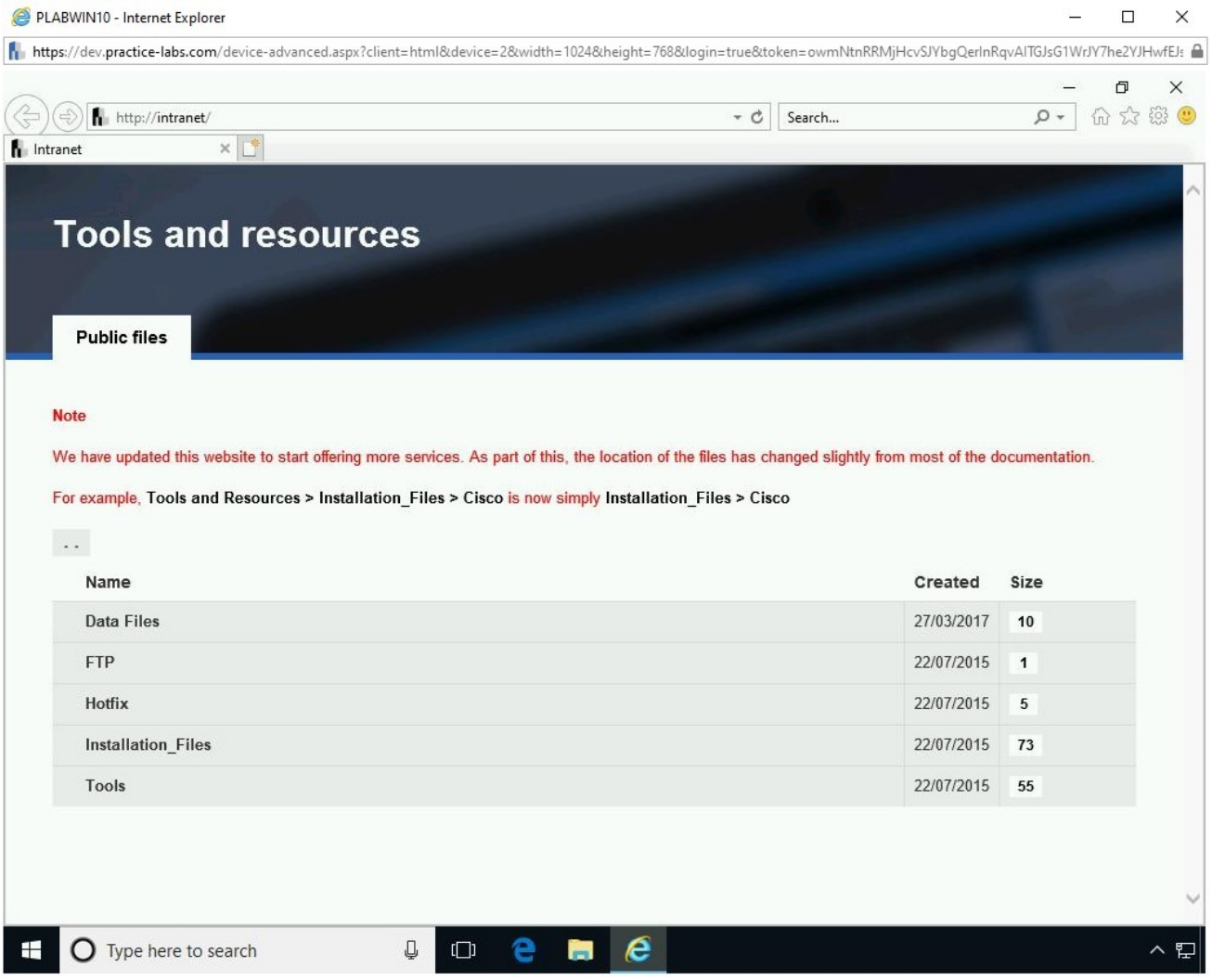


Figure 1.3 Screenshot of PLABWIN10: Clicking Tools on the Intranet homepage.

Step 4

On the **Tools** Webpage, click **Hacking Tools**.

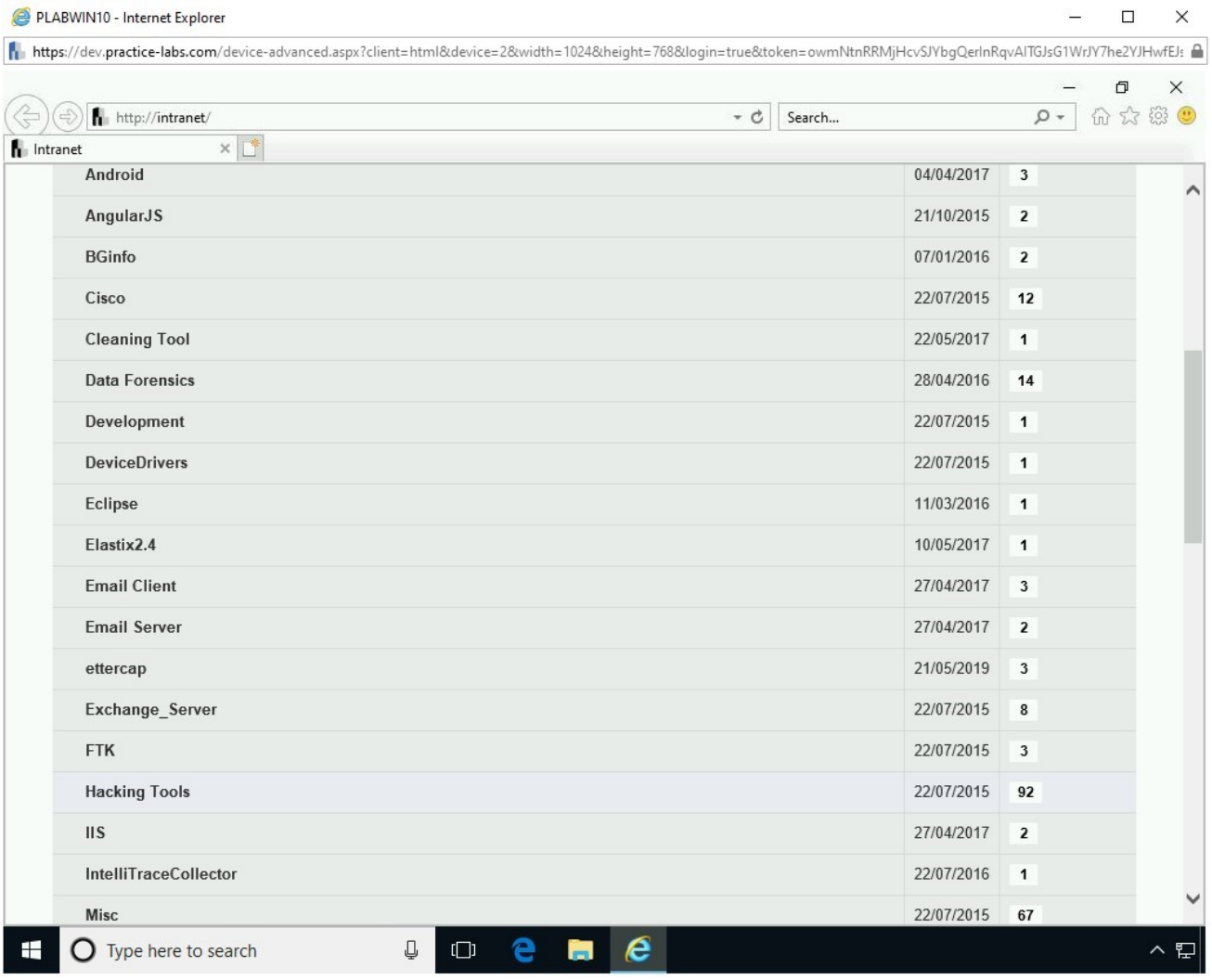


Figure 1.4 Screenshot of PLABWIN10: Clicking Hacking Tools on the Intranet homepage.

Step 5

Locate and click **Wireshark-win32-1.12.3.exe**.

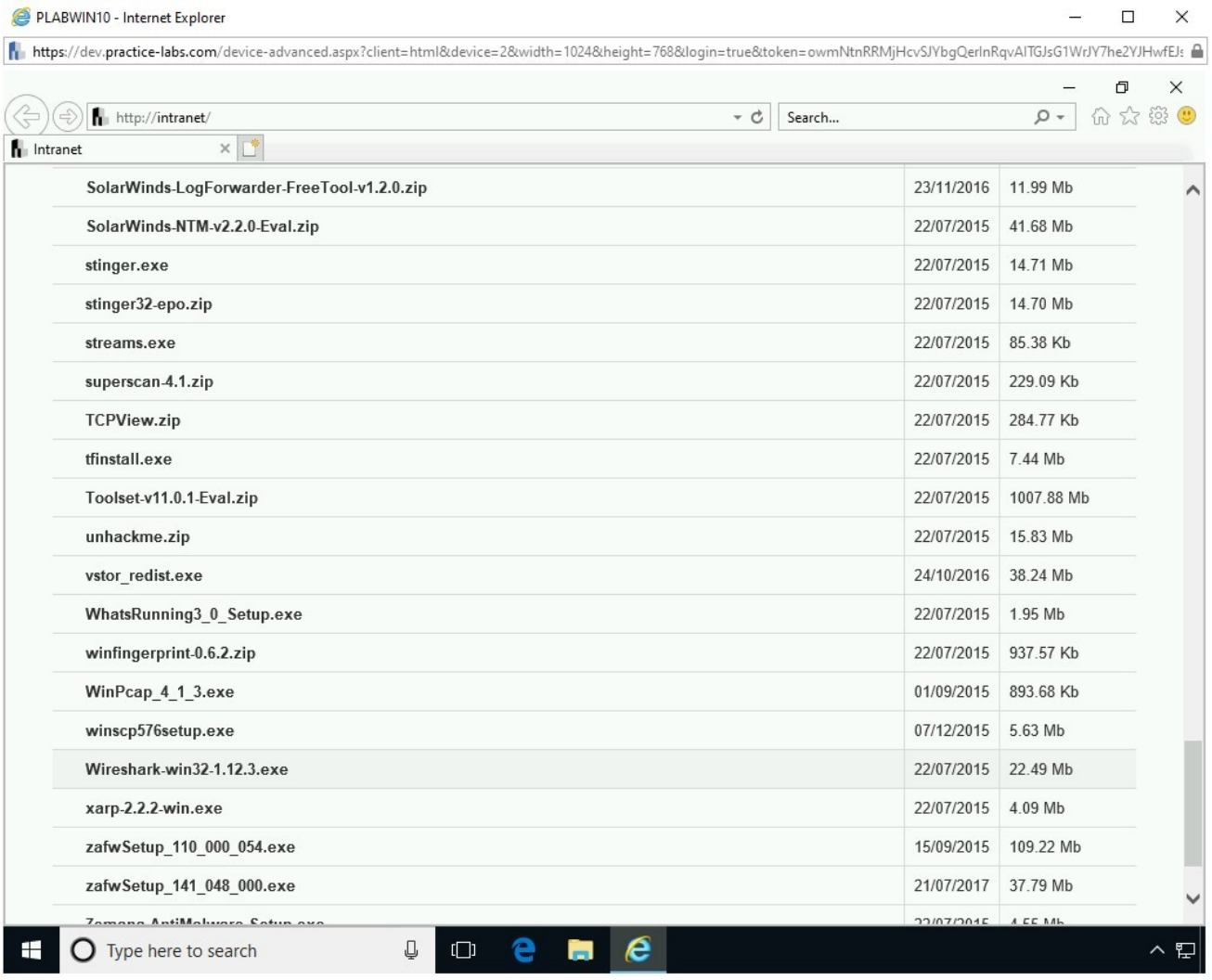


Figure 1.5 Screenshot of PLABWIN10: Clicking Wireshark-win32-1.12.3.exe on the Intranet homepage.

Step 6

In the notification bar, click **Save**.

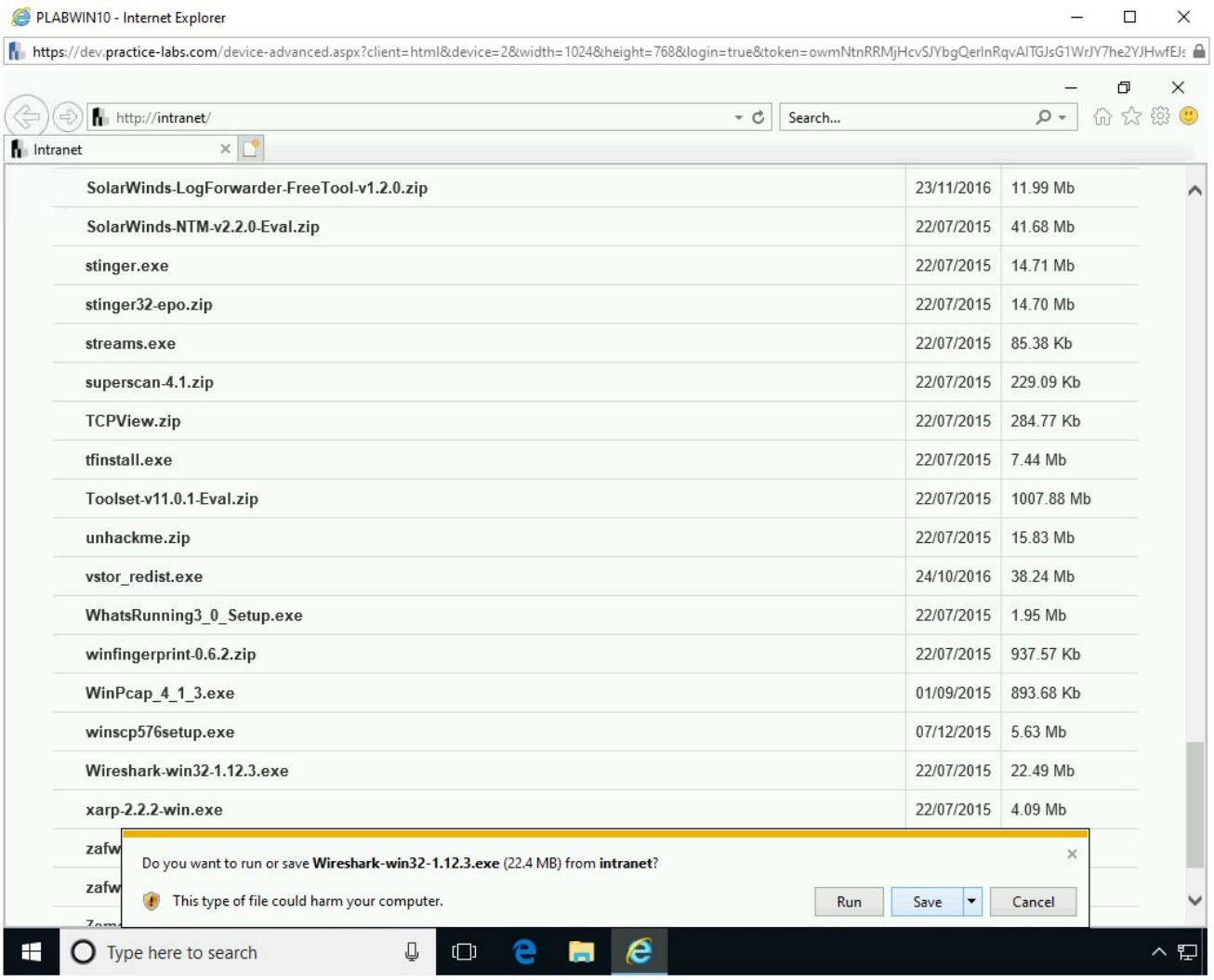


Figure 1.6 Screenshot of PLABWIN10: Clicking the Save option in the notification bar.

Step 7

In the notification bar, click **Open folder**.

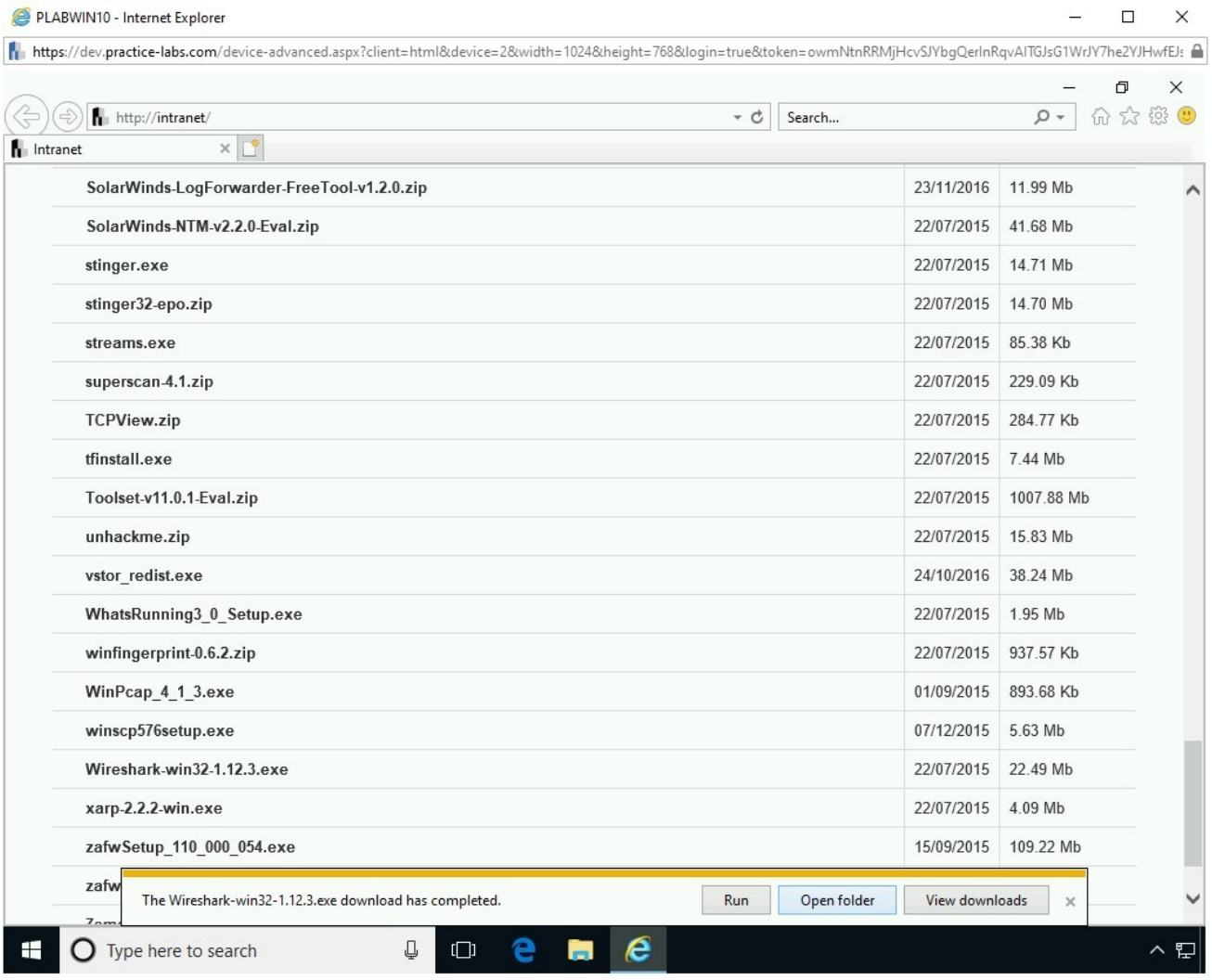


Figure 1.7 Screenshot of PLABWIN10: Clicking the Open folder option in the notification bar.

Step 8

The **File Explorer** window is now open. Double-click the **Wireshark-win32-1.12.3.exe** file.

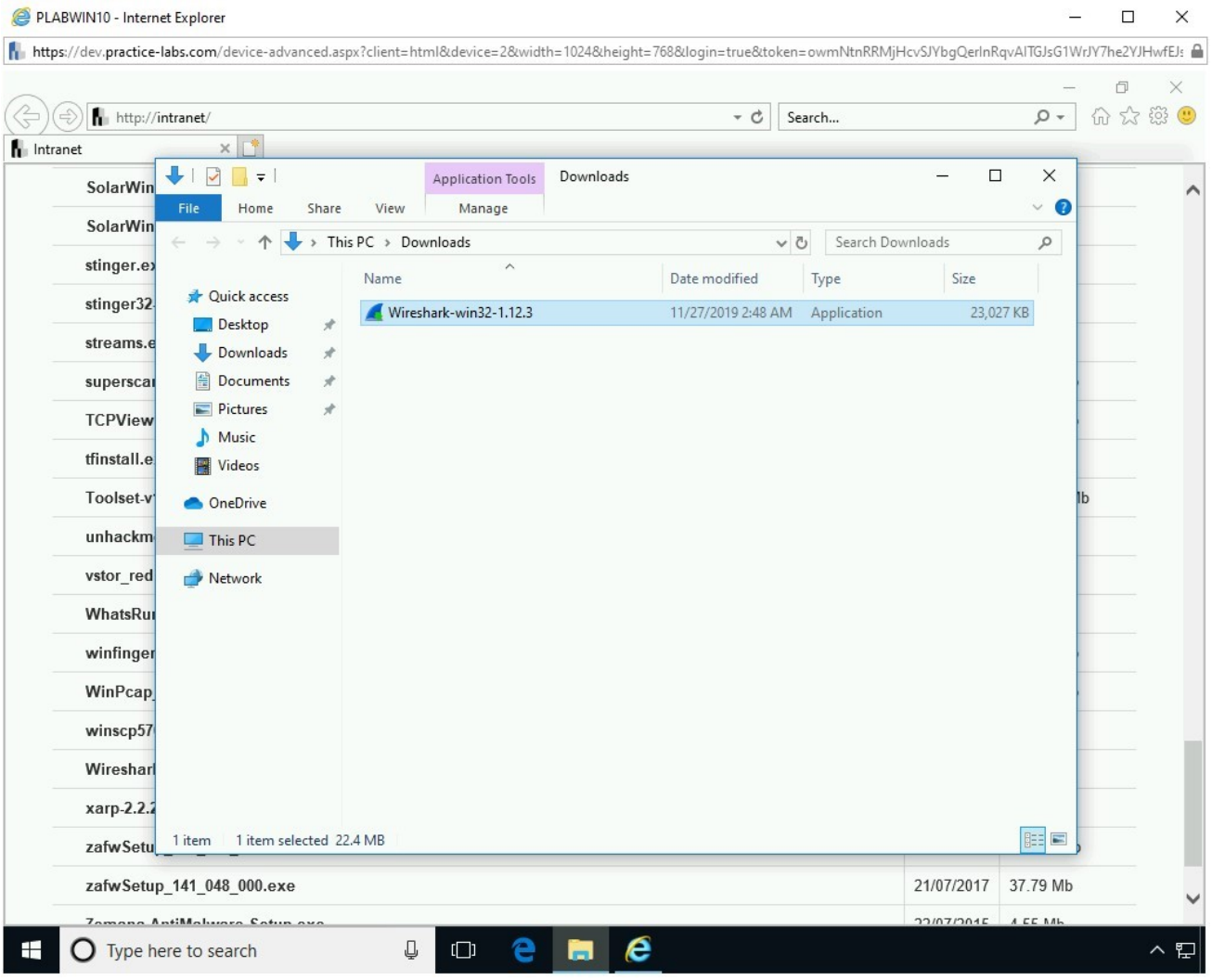


Figure 1.8 Screenshot of PLABWIN10: Double-clicking the Wireshark-win32-1.12.3.exe file.

Step 9

The **Welcome to the Wireshark 1.12.3 (32-bit) Setup Wizard** is displayed. Click **Next** to continue.

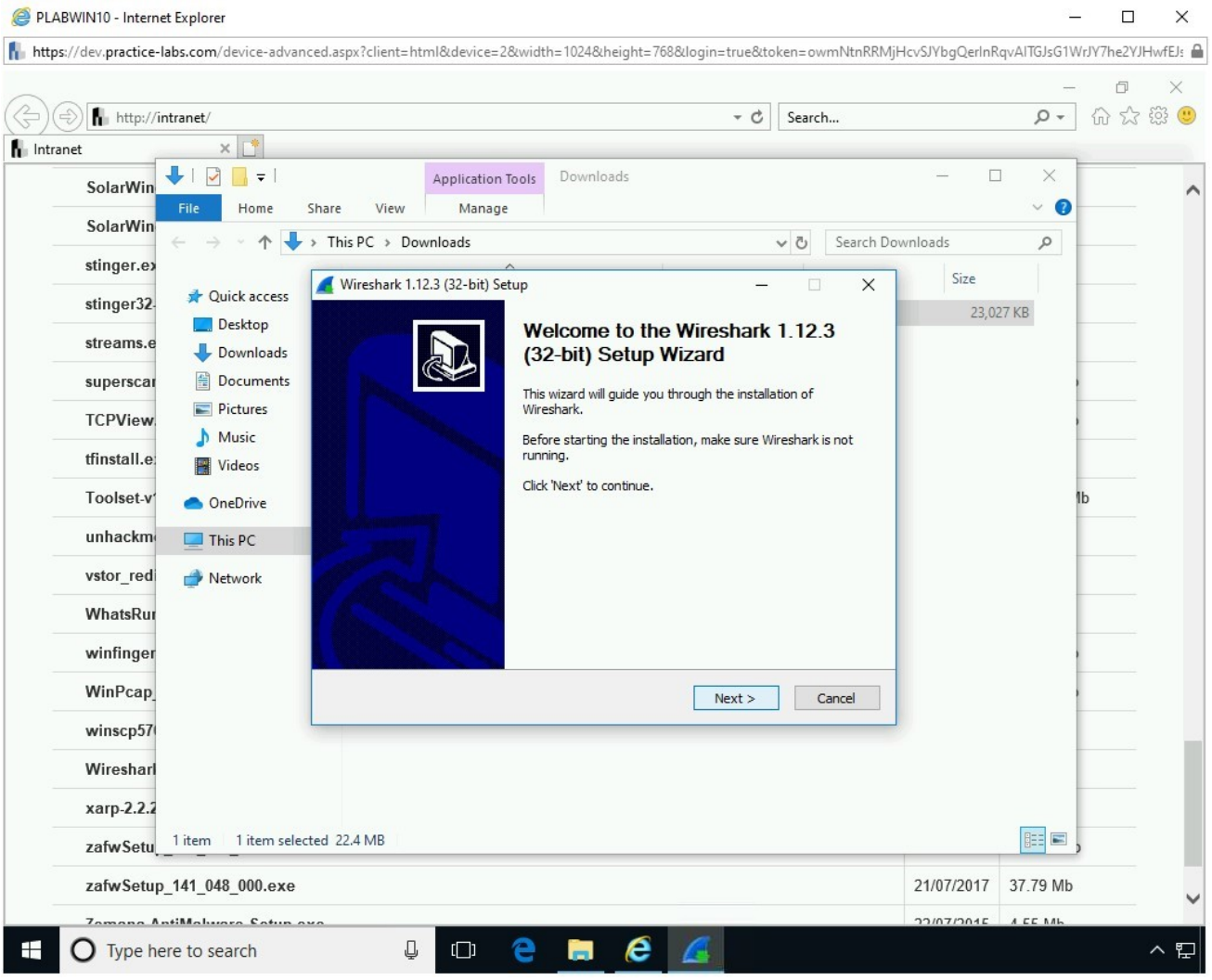


Figure 1.9 Screenshot of PLABWIN10: Clicking Next on the Welcome to the Wireshark 1.12.3 (32-bit) Setup Wizard page.

Step 10

On the **License Agreement** page, click **I Agree**.

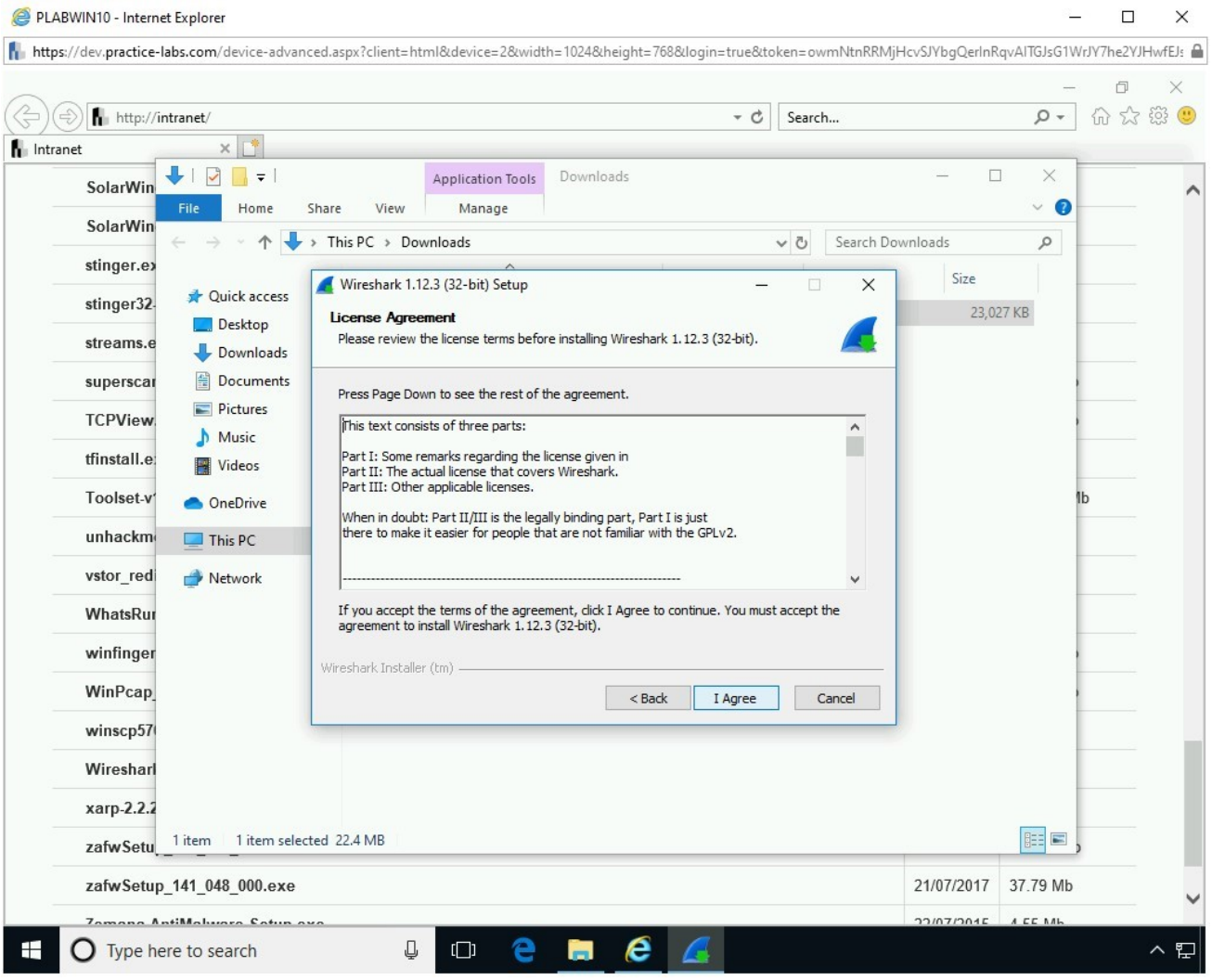


Figure 1.10 Screenshot of PLABWIN10: Clicking I Agree on the License Agreement page.

Step 11

On the **Choose Components** page, keep the default selection and click **Next**.

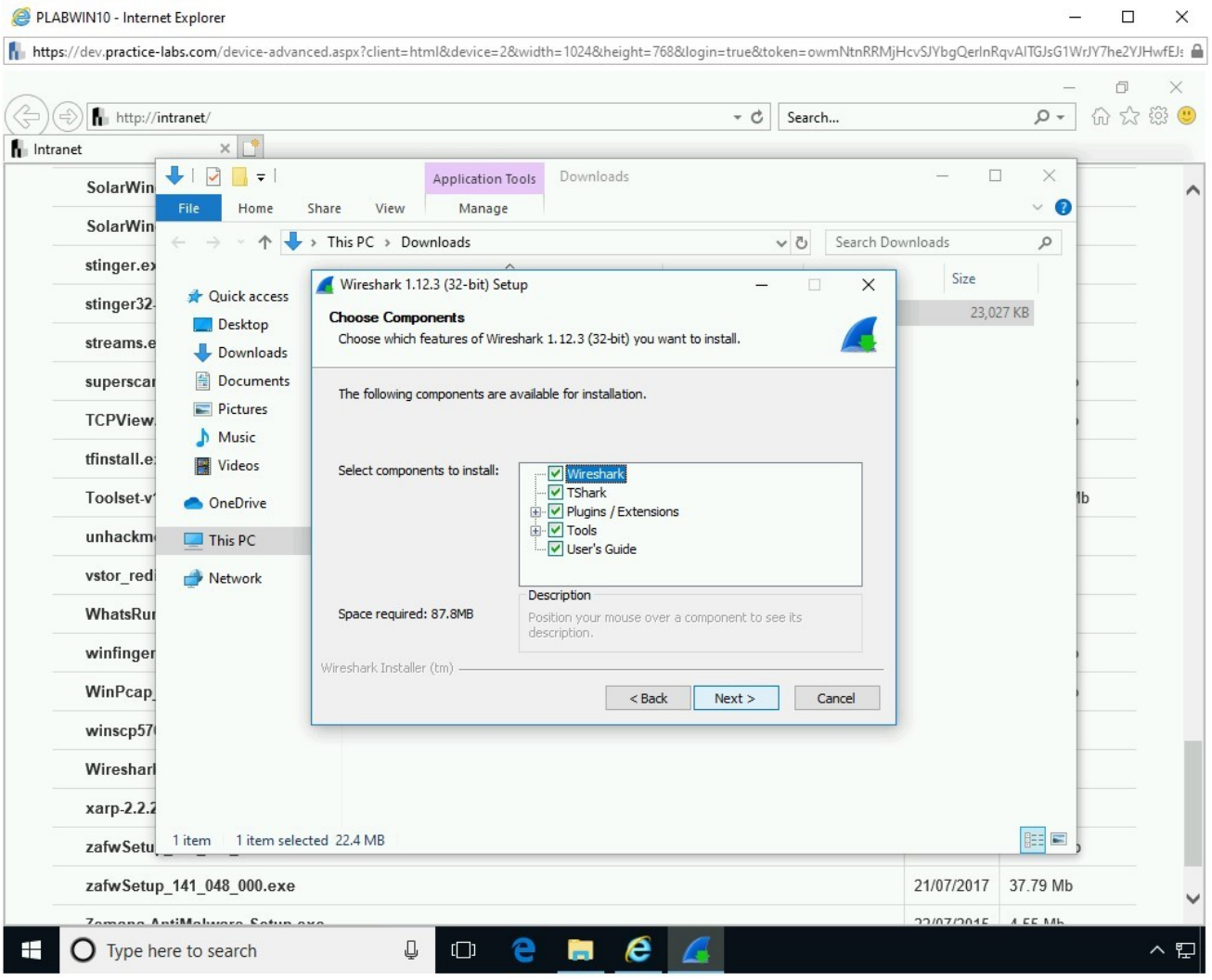


Figure 1.11 Screenshot of PLABWIN10: Keeping the default options on the Choose Components page.

Step 12

On the **Select Additional Tasks** page, select **Desktop** Icon.

Notice that the **Start Menu Item** and **Quick Launch Icons** options are already selected. Keep the option in the **File Extensions** section selected and click **Next**.

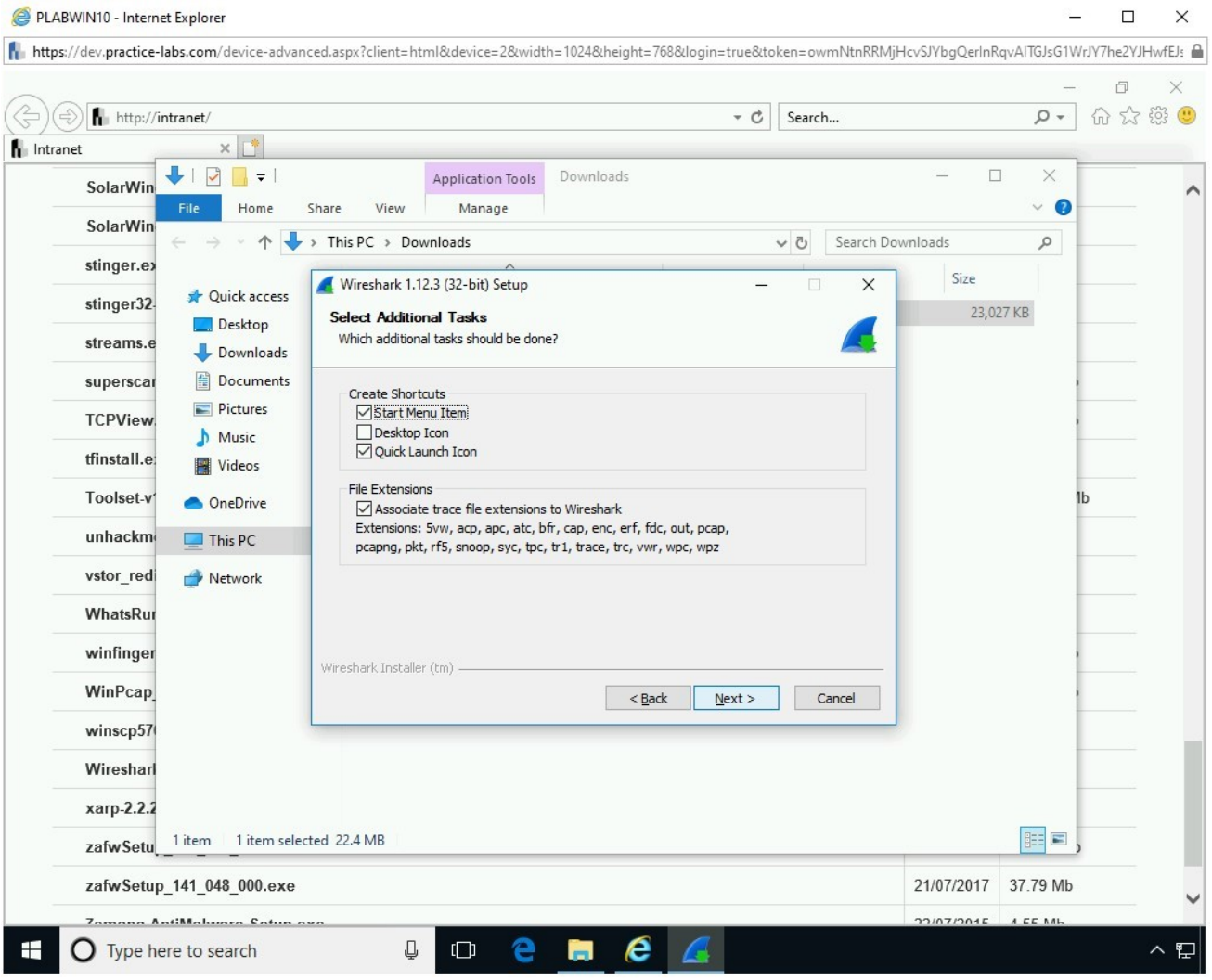


Figure 1.12 Screenshot of PLABWIN10: Selecting the Desktop Icon option on the Select Additional Tasks page.

Step 13

On the **Choose Install Location** page, keep the default location and click **Next**.

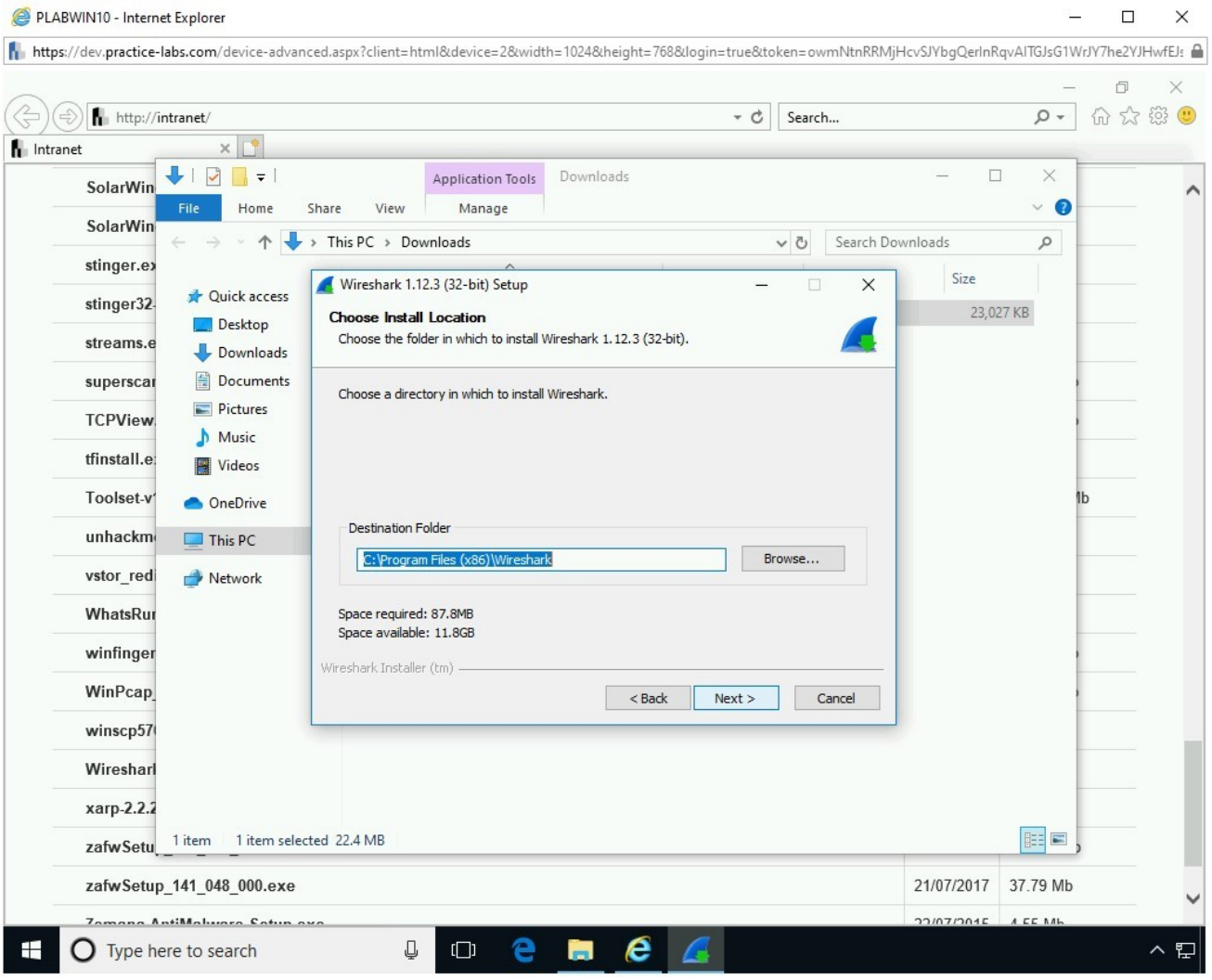


Figure 1.13 Screenshot of PLABWIN10: Keeping the default installation path on the Choose Install Location page.

Step 14

On the **Install WinPcap?** page, keep the default selection and click **Install**.

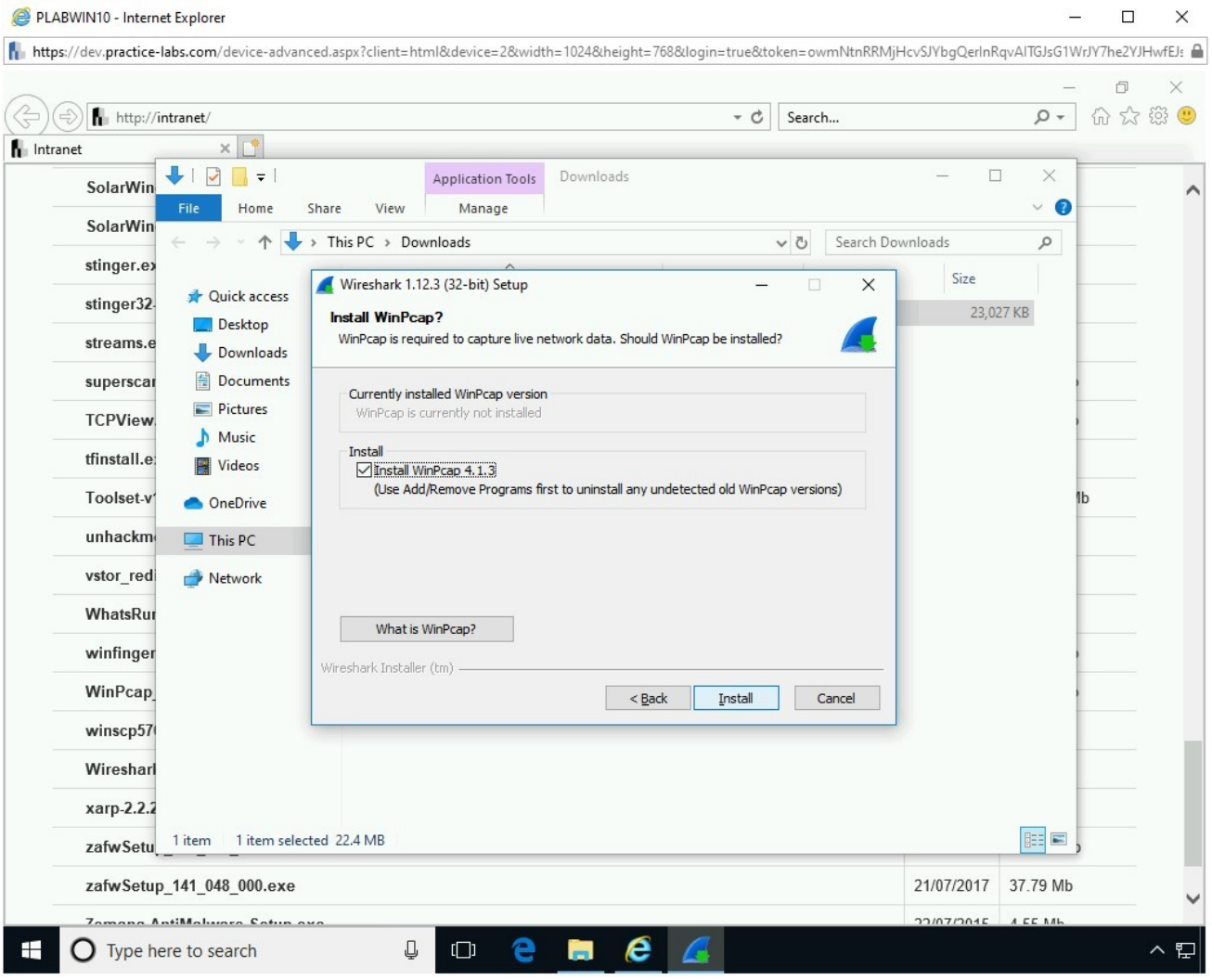


Figure 1.14 Screenshot of PLABWIN10: Keeping the default installation option on the Install WinPcap? page.

Step 15

On the **Installing** page, the installation process will start.

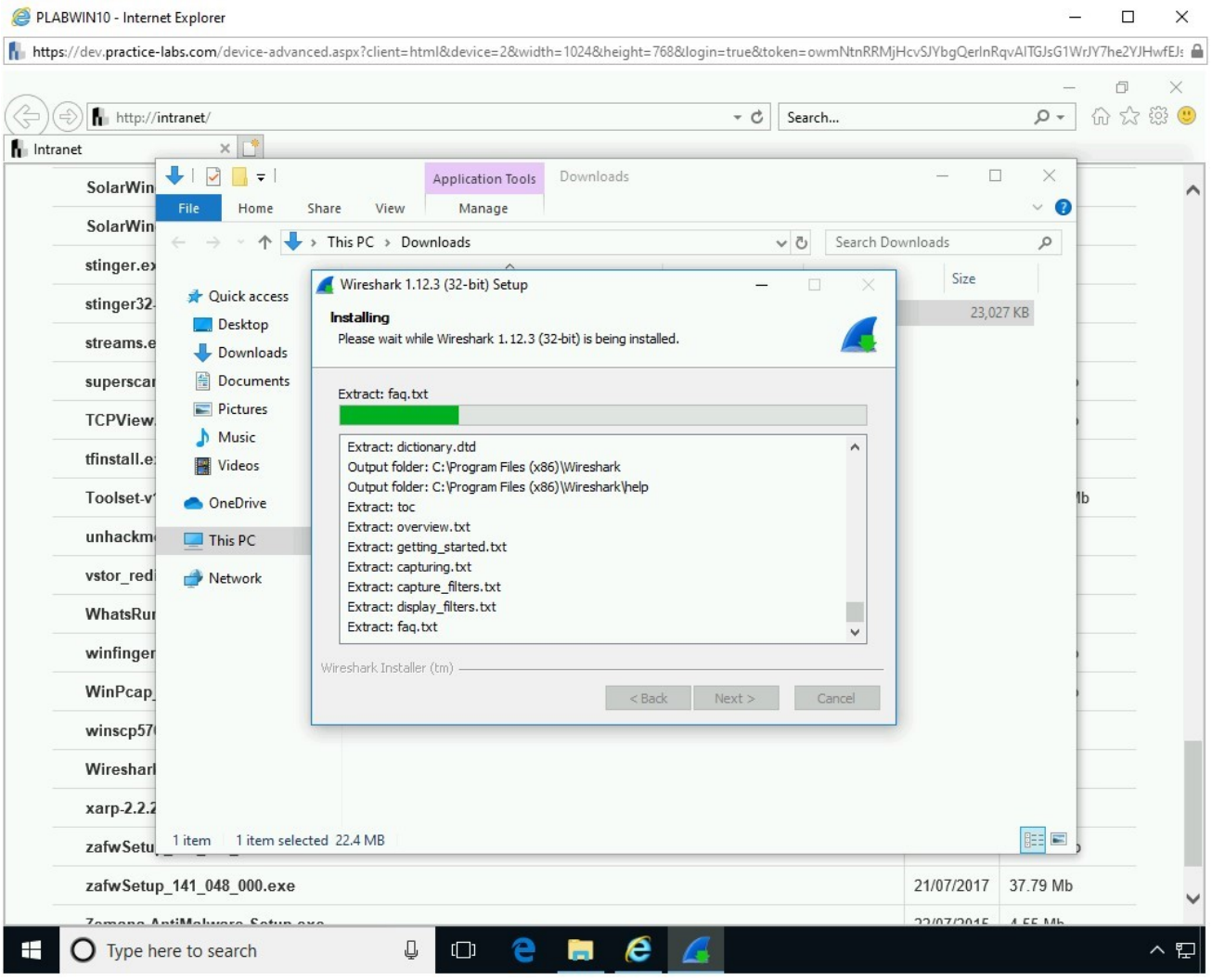


Figure 1.15 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 16

On the **Welcome to the WinPcap 4.1.3 Setup Wizard** page, click **Next**.

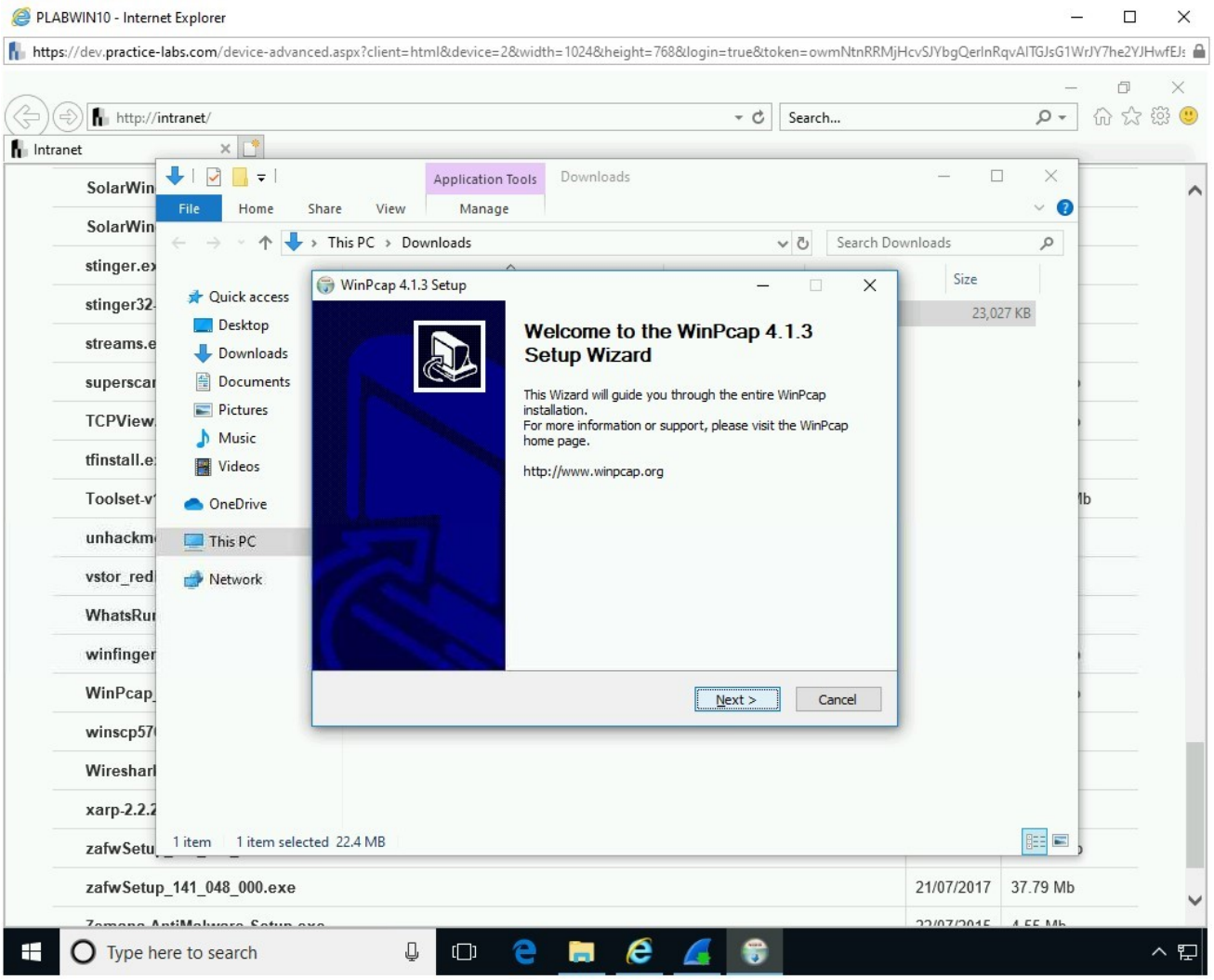


Figure 1.16 Screenshot of PLABWIN10: Clicking Next on the Welcome to the WinPcap 4.1.3 Setup Wizard page.

Step 17

On the **License Agreement** page, click **I Agree**.

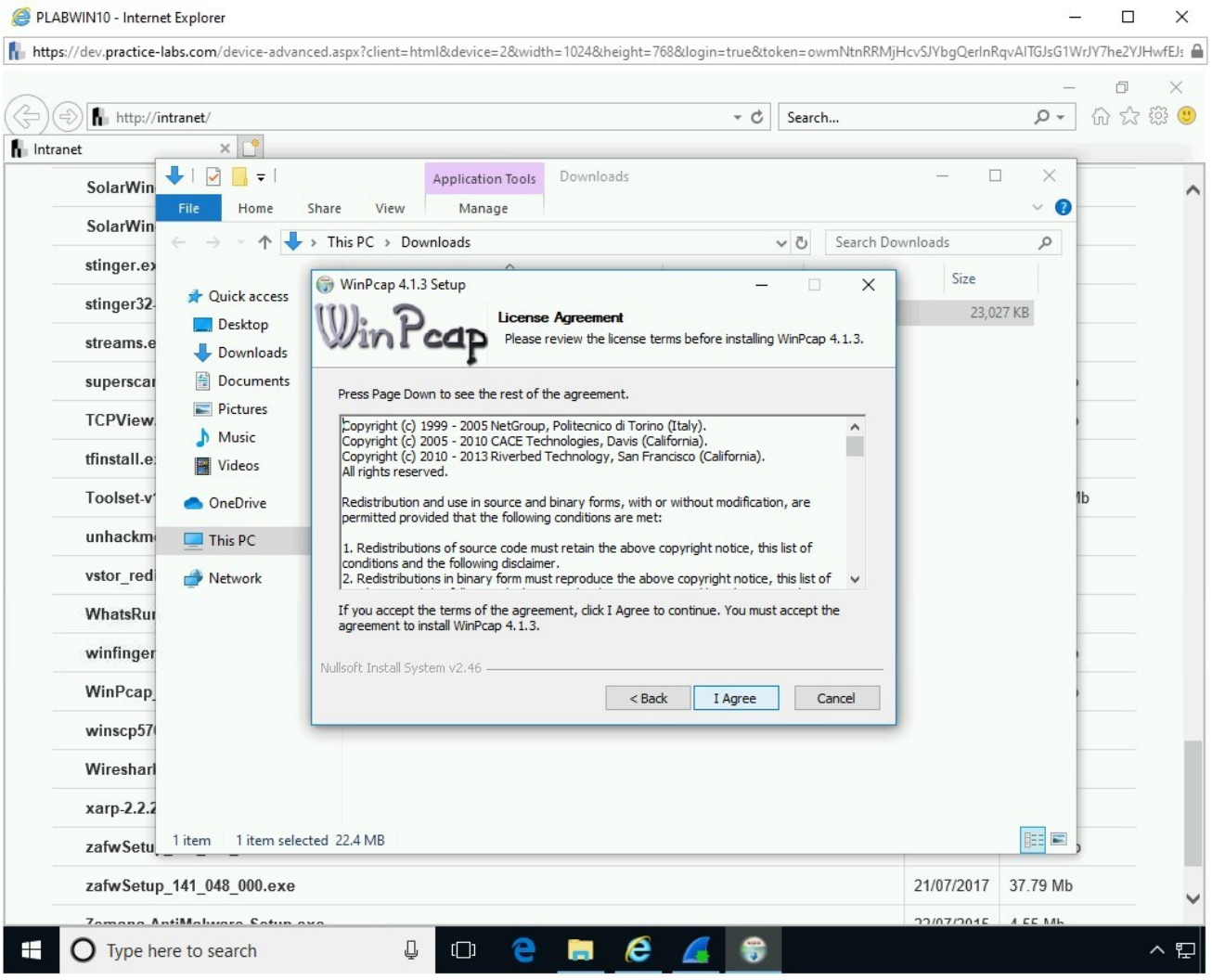


Figure 1.17 Screenshot of PLABWIN10: Clicking I Agree on the License Agreement page.

Step 18

On the **Installation options** page, keep the default selection and click **Install**.

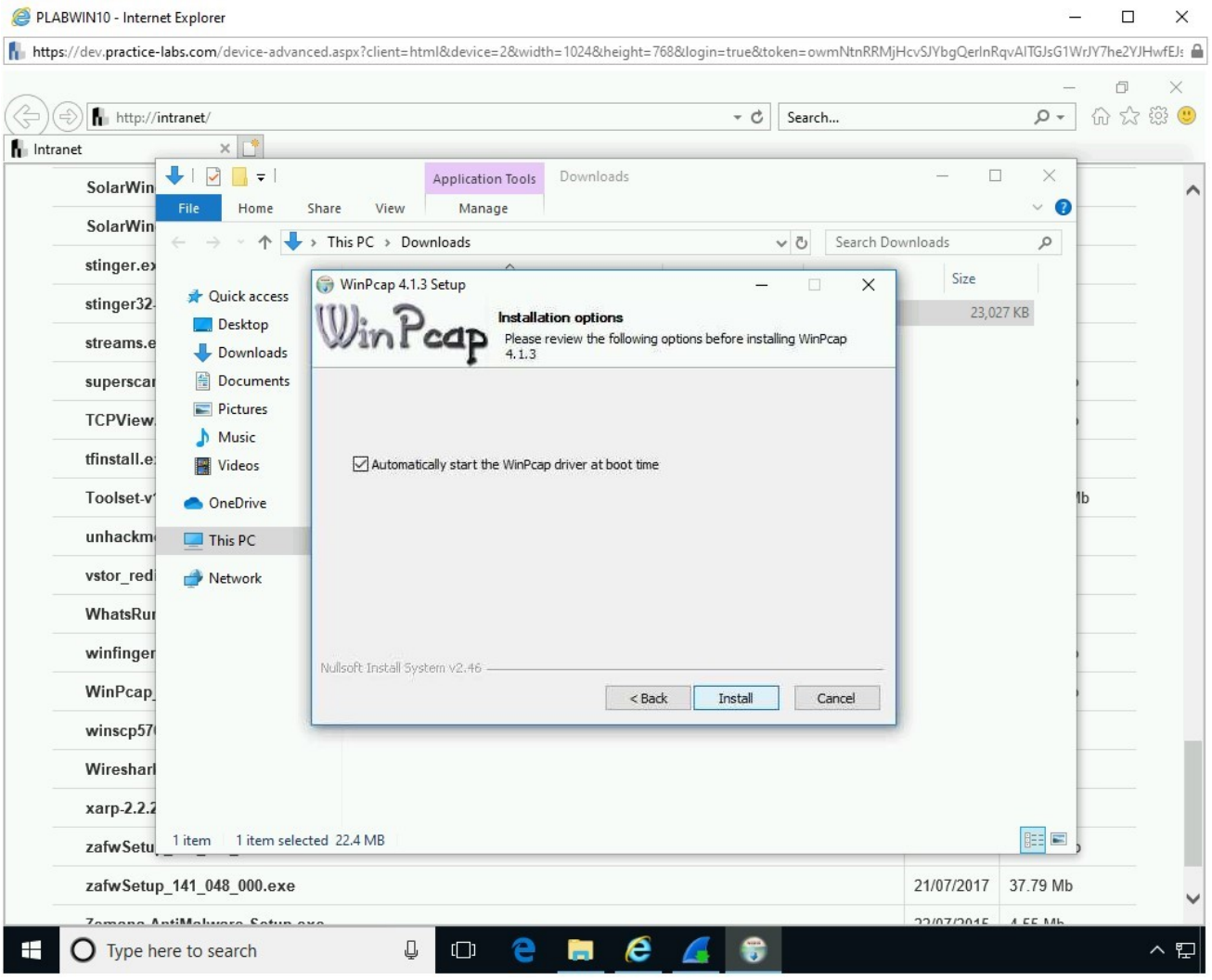


Figure 1.18 Screenshot of PLABWIN10: Keeping the default installation option on the Installation options page.

Step 19

On the **Completing the WinPcap 4.1.3 Setup Wizard** page, click **Finish**.

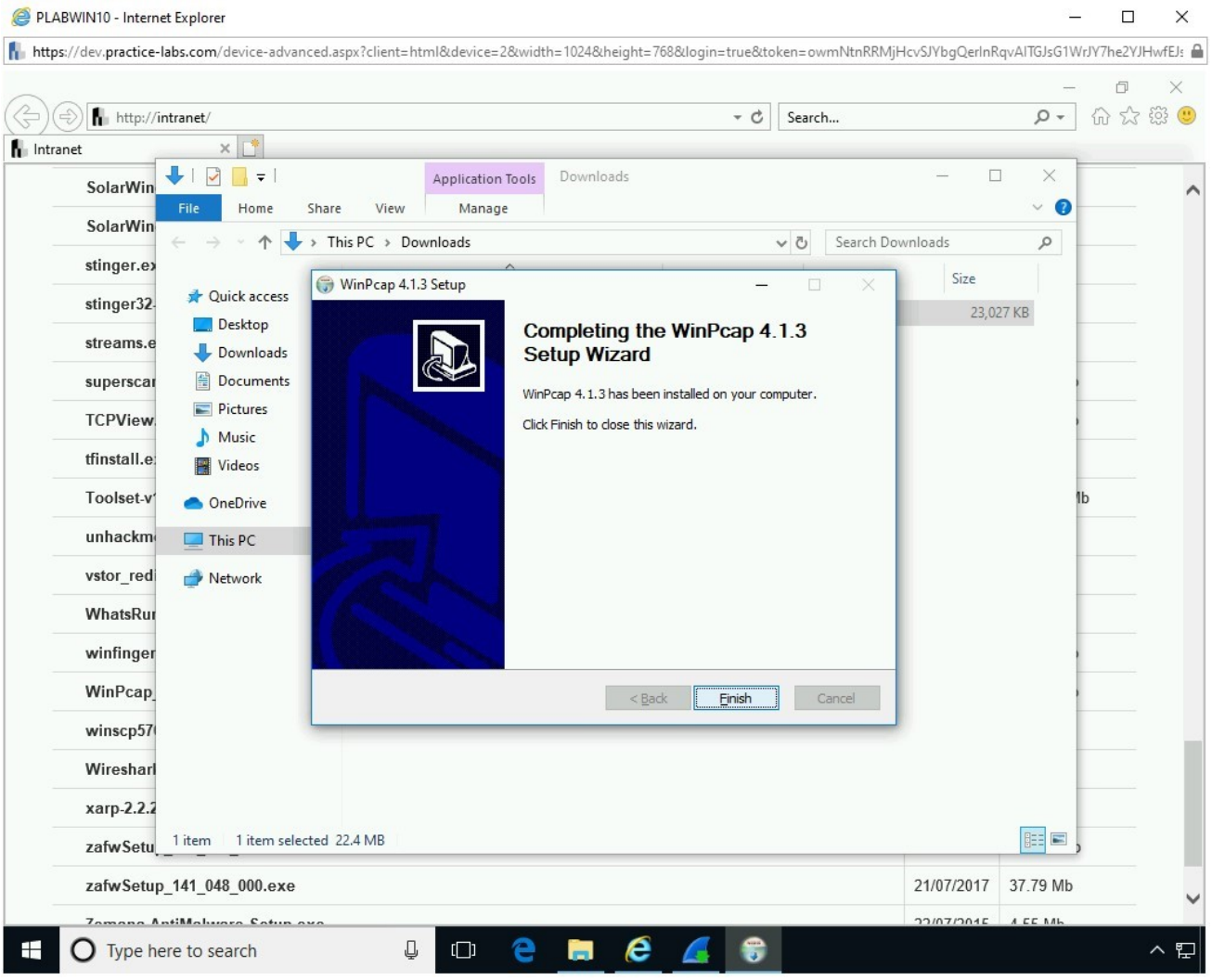


Figure 1.19 Screenshot of PLABWIN10: Clicking Finish on the Completing the WinPcap 4.1.3 Setup Wizard page.

Step 20

On the **Installing** page, the installation progress is displayed.

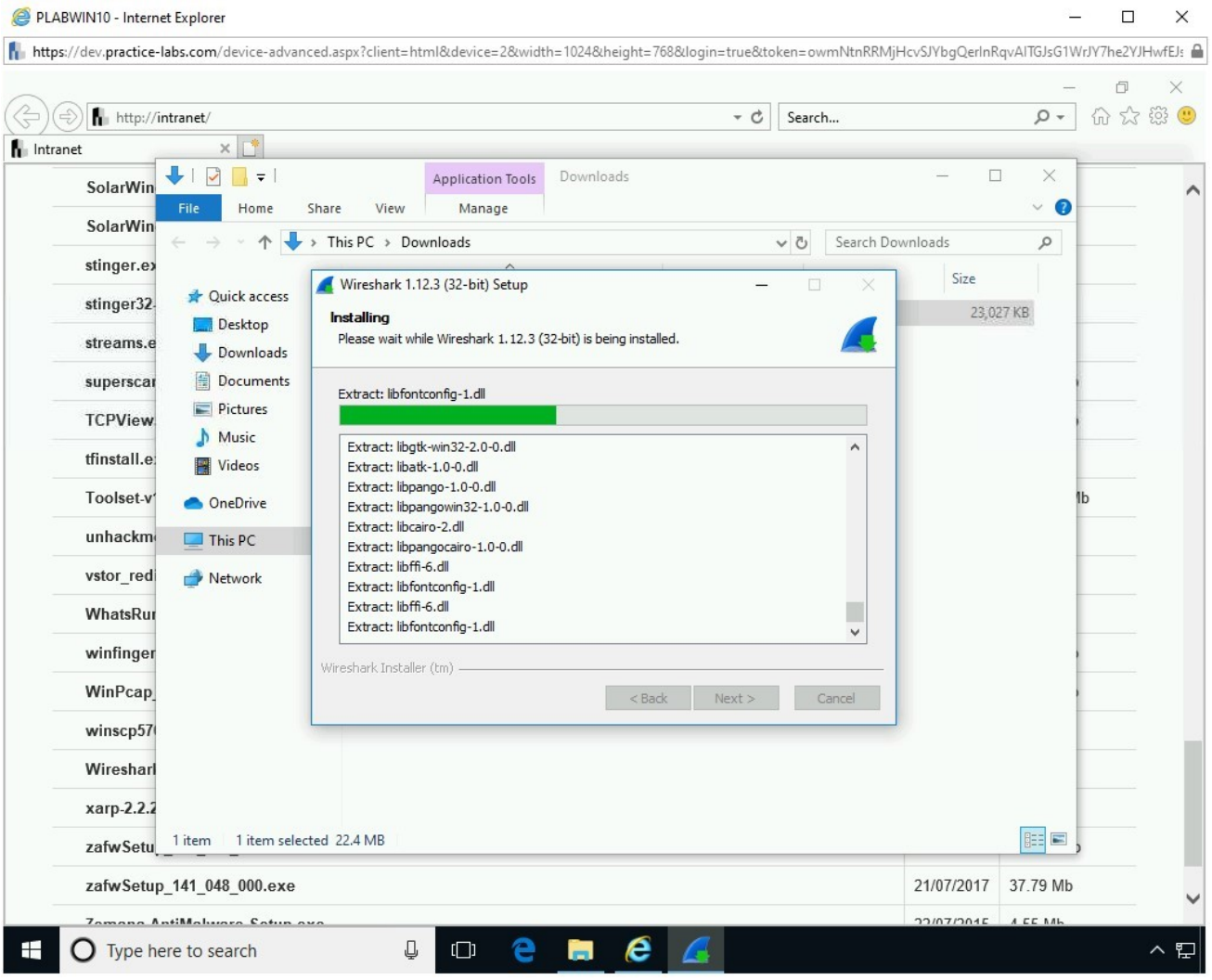


Figure 1.20 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 21

On the **Installation Complete** page, click **Next**.

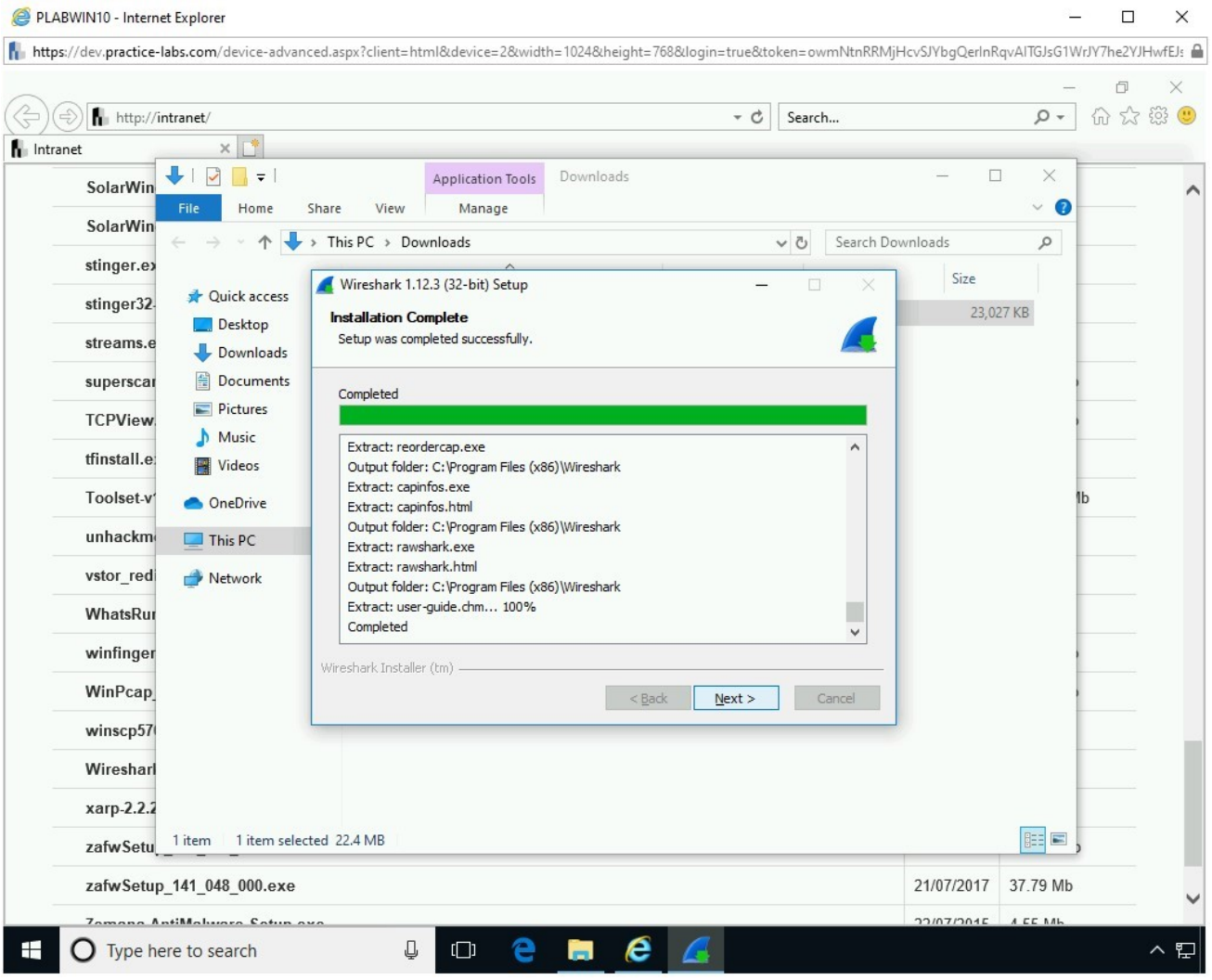


Figure 1.21 Screenshot of PLABWIN10: Clicking Next on the Installation Complete page.

Step 22

On the **Completing the Wireshark 1.12.3 (32-bit) Setup Wizard** page, **select Run Wireshark 1.12.3 (32-bit)** and click **Finish**.

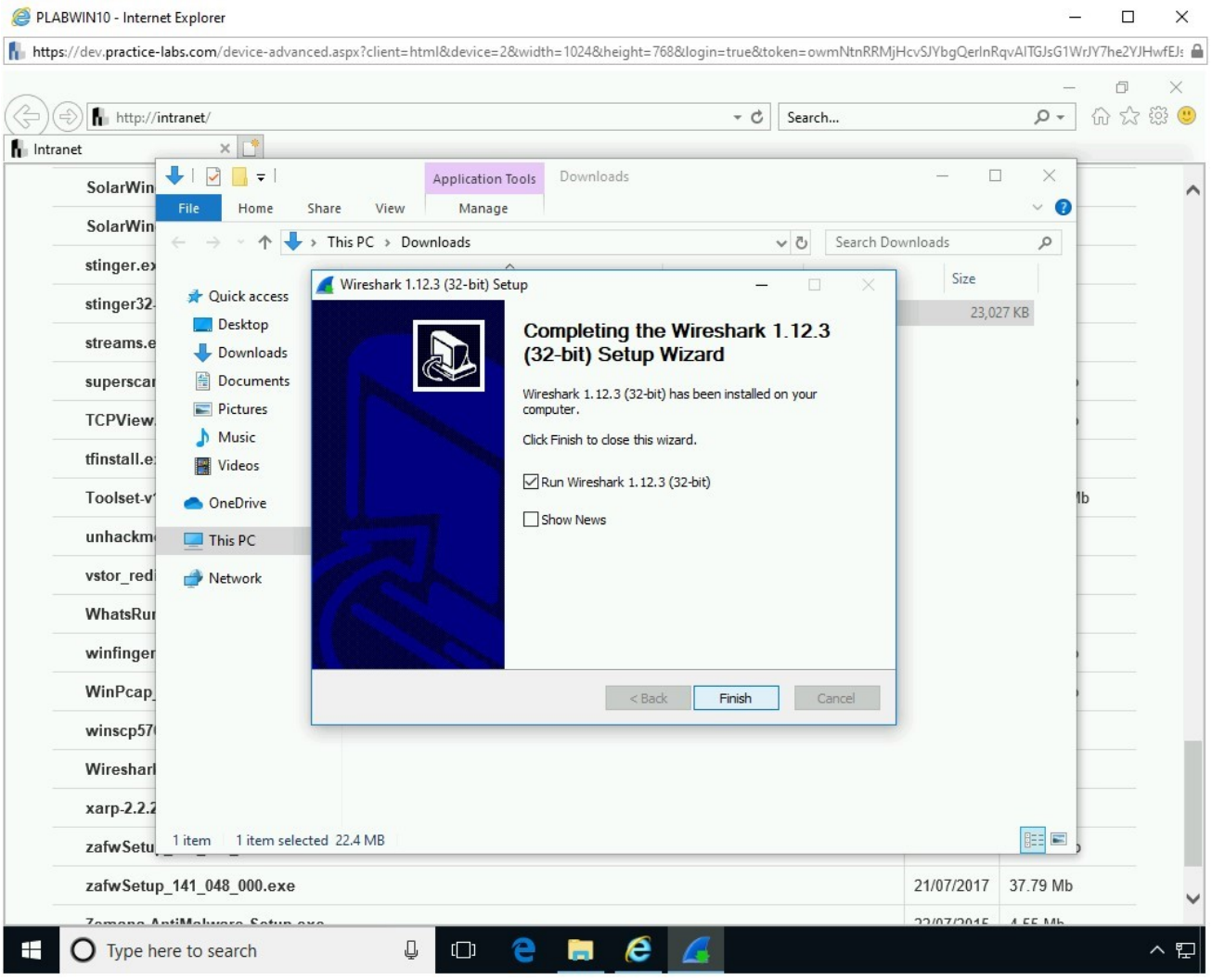


Figure 1.22 Screenshot of PLABWIN10: Clicking Finish on the Completing the Wireshark 1.12.3 (32-bit) Setup Wizard page.

Step 23

The **Wireshark** window is displayed. The **Software Update** dialog box is also displayed. Click **Remind me later**.

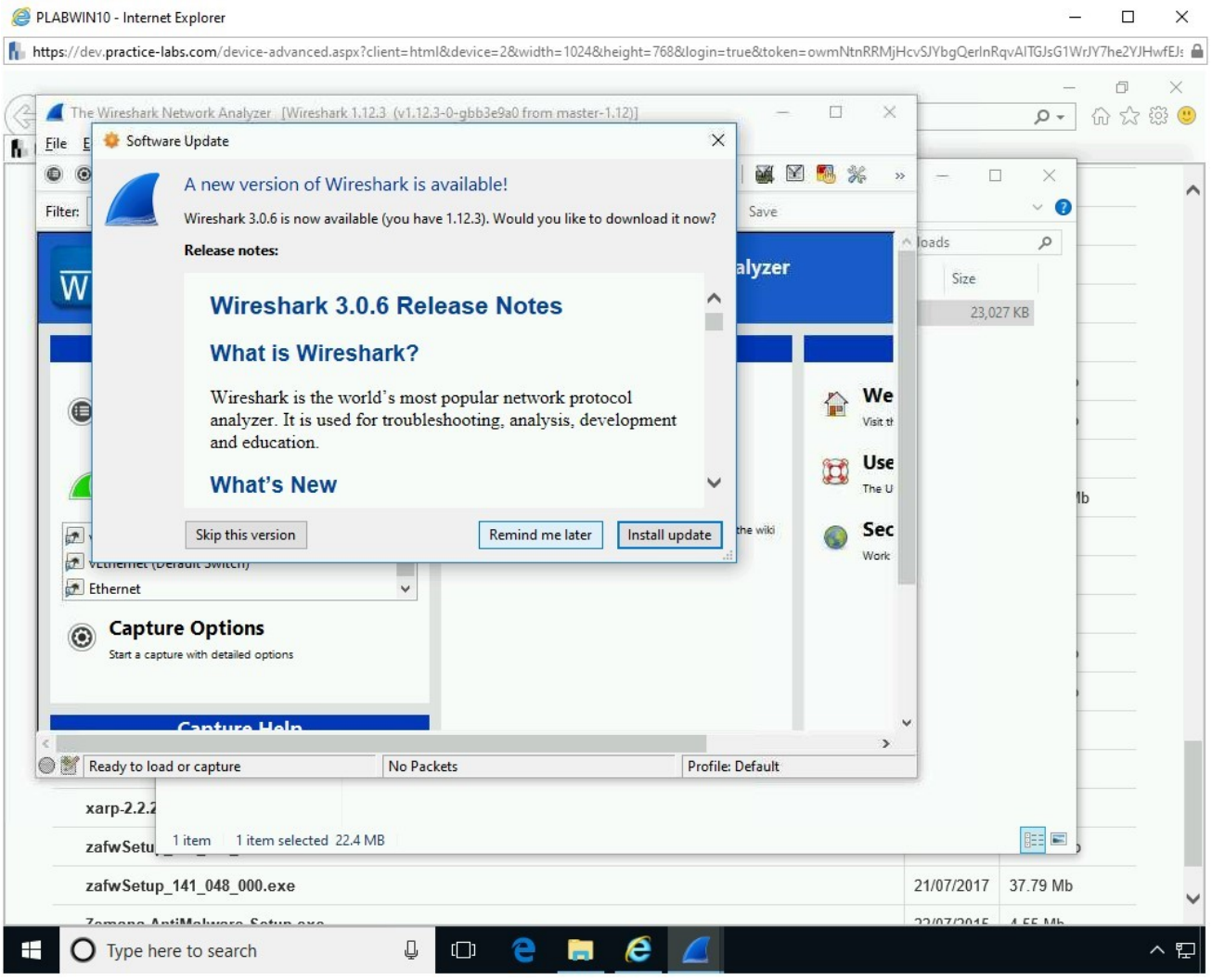


Figure 1.23 Screenshot of PLABWIN10: Clicking Remind me later on the Software Update dialog box.

Step 24

You are now on the Wireshark window.

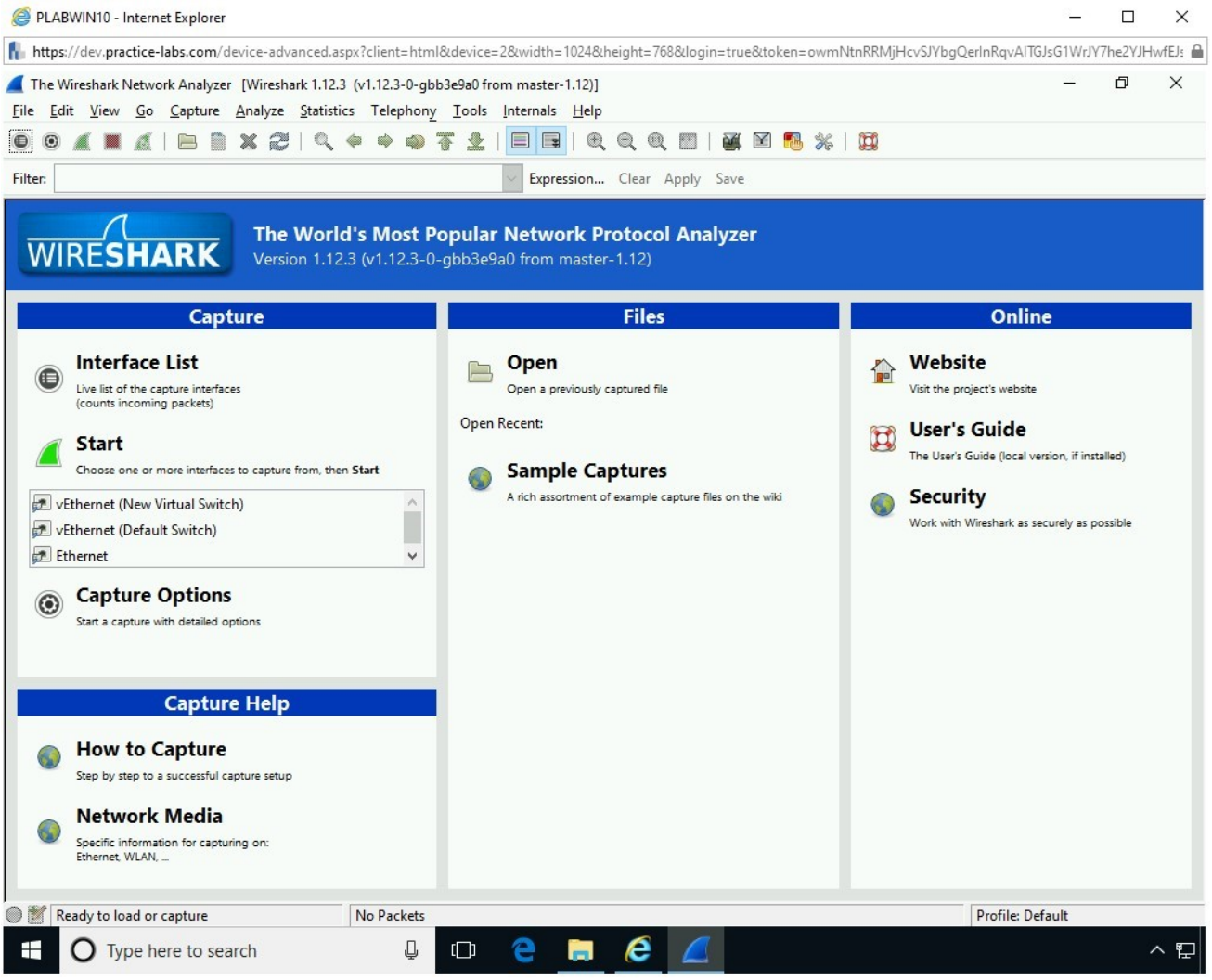


Figure 1.24 Screenshot of PLABWIN10: Showing the Wireshark window.

Step 25

Just below the **Start** option in the left pane, you have a list of network interfaces listed in a list box. Select **Ethernet** and click **Start**.

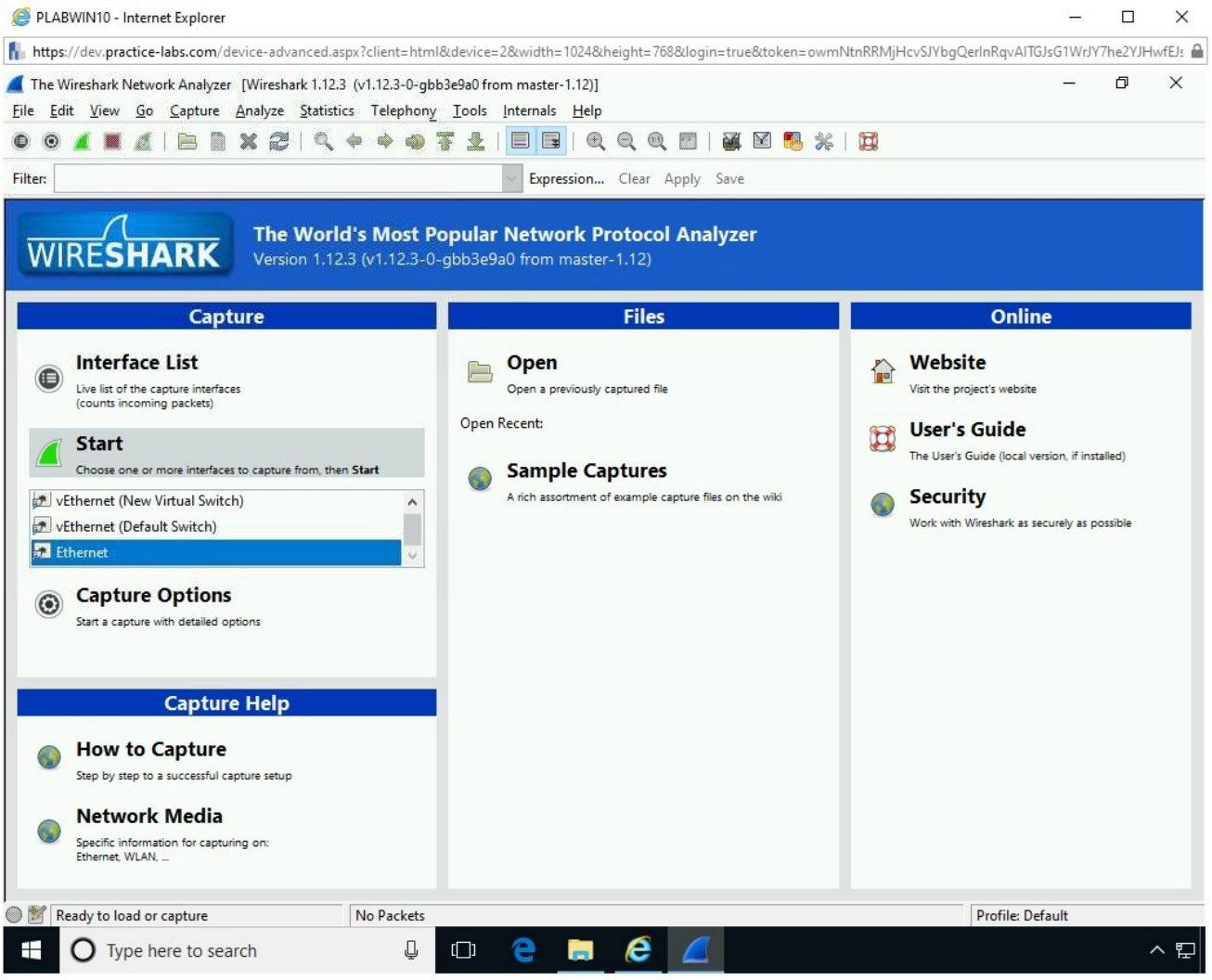


Figure 1.25 Screenshot of PLABWIN10: Selecting Ethernet and clicking Start.

Step 26

Notice that packet capturing starts.

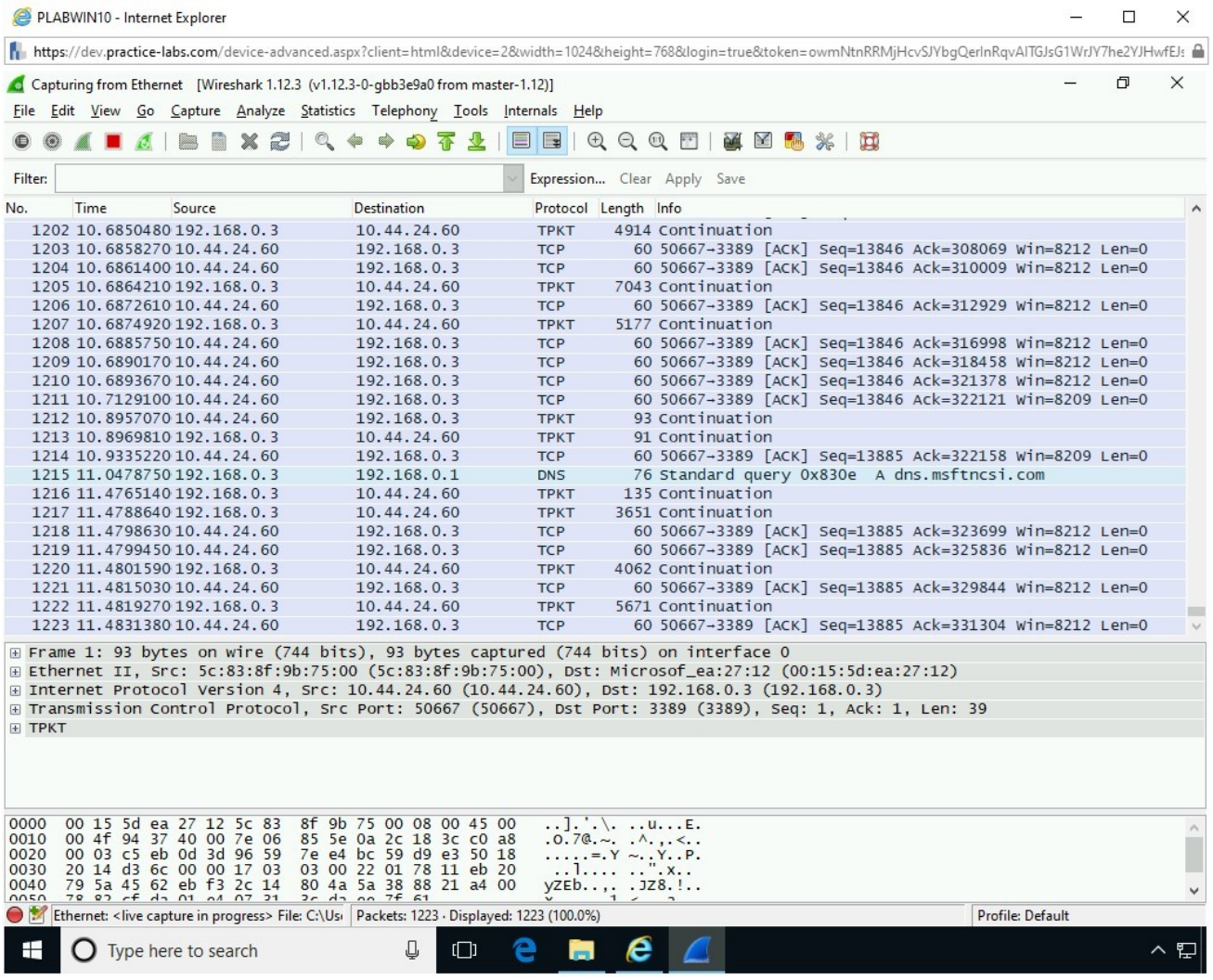


Figure 1.26 Screenshot of PLABWIN10: Showing the packet capture progress in Wireshark.

Keep the **Wireshark** window open.

Task 2 - Perform SYN Flooding Attack

SYN flooding, a type of denial-of-service (DoS) attack, is conducted by an attacker to send a flood of SYN packets to a target. With the flood of a large number of SYN packets, the target is unable to respond to them. In the process of responding to these SYN packets, the target system starts consuming all its resources and, therefore, exhausts them eventually. As a consequence of running out of system resources, the target becomes non-responsive or hangs. In some cases, the target also crashes.

To conduct SYN flooding, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALI01**.

Credentials are:

Username:

```
root
```

Password:

```
Passw0rd
```

The desktop of **PLABKALI01** is displayed.

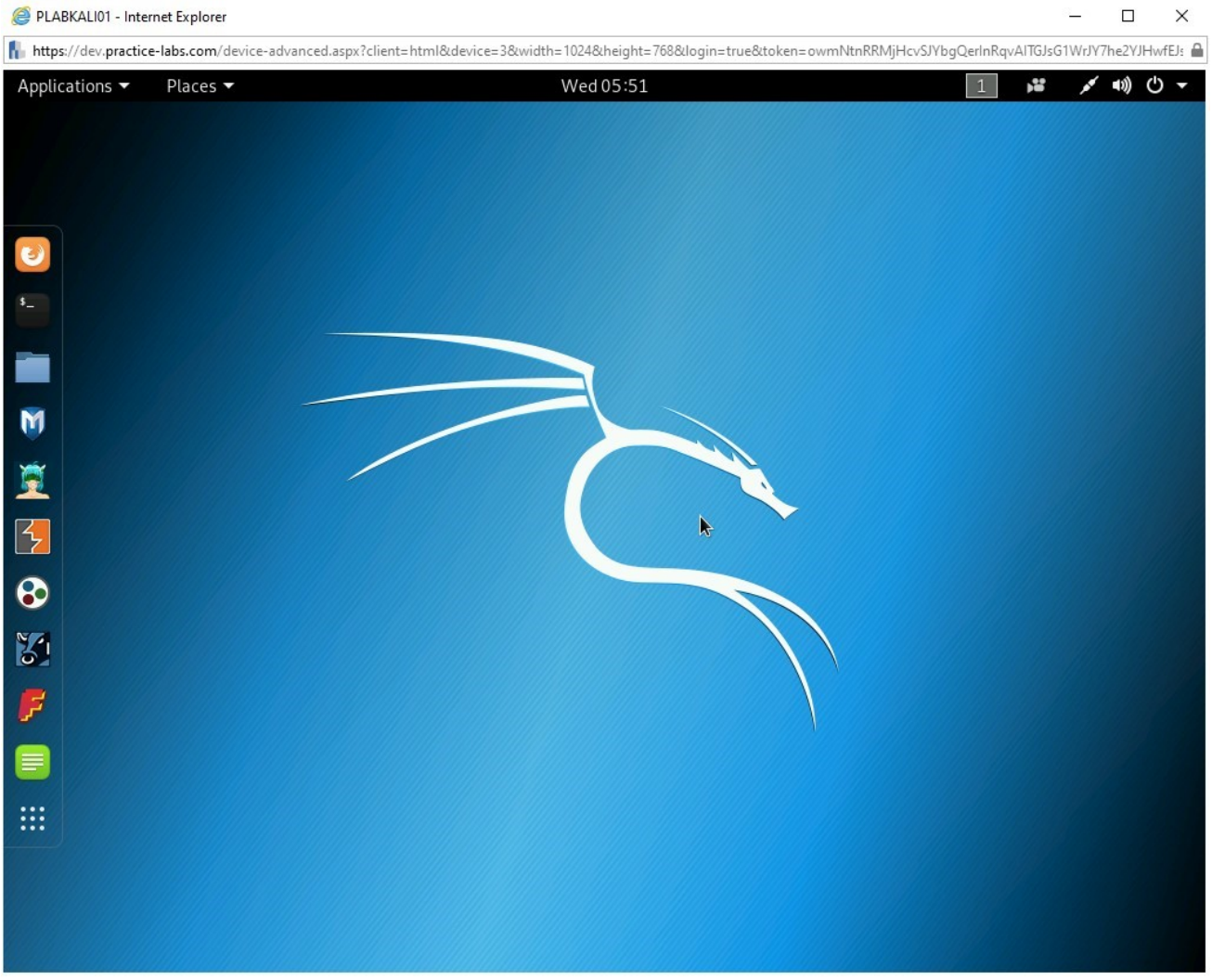


Figure 1.27 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01.

Step 2

On the desktop, in the left pane, click the **Terminal** icon.

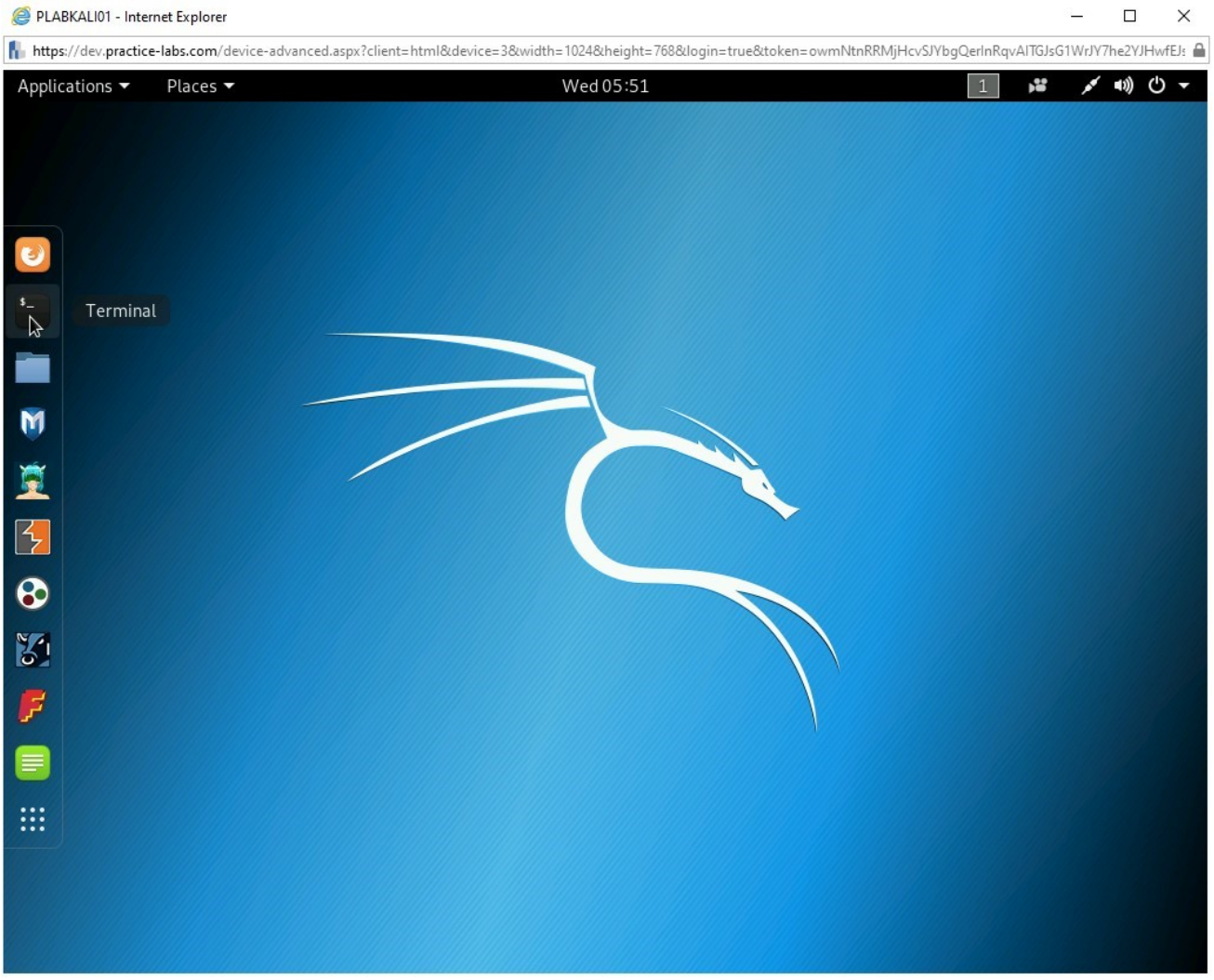


Figure 1.28 Screenshot of PLABKALI01: Clicking the Terminal icon in the left pane.

Step 3

In the terminal window, type the following command:

```
hping3 -S 192.168.0.3 -a 192.168.0.4 -p 22 --flood
```

In this command, the target system is **192.168.0.3,** and the attacker is **192.168.0.4**.

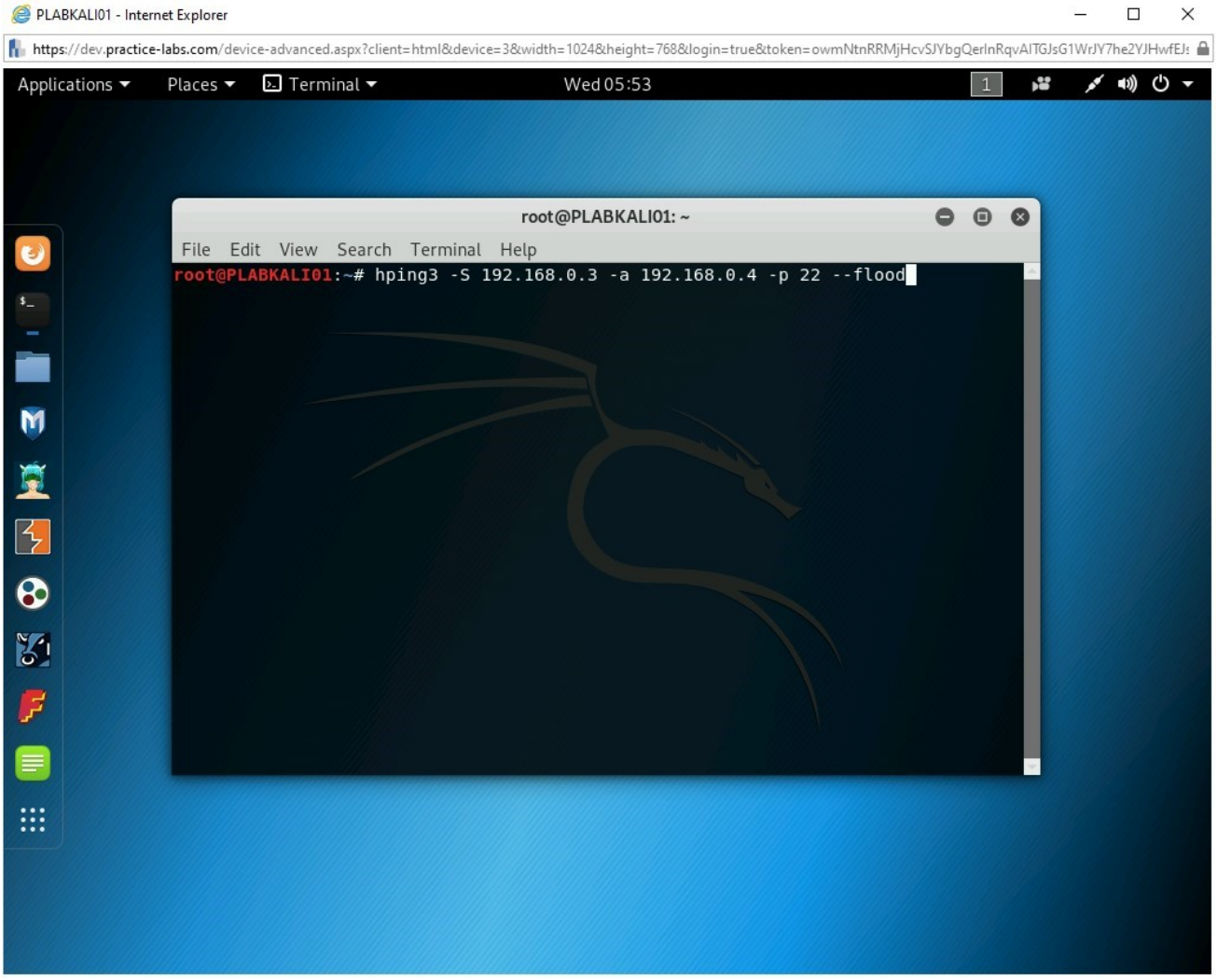


Figure 1.29 Screenshot of PLABKALI01: Entering the hping3 command in the terminal window.

Step 4

The hping3 command starts.

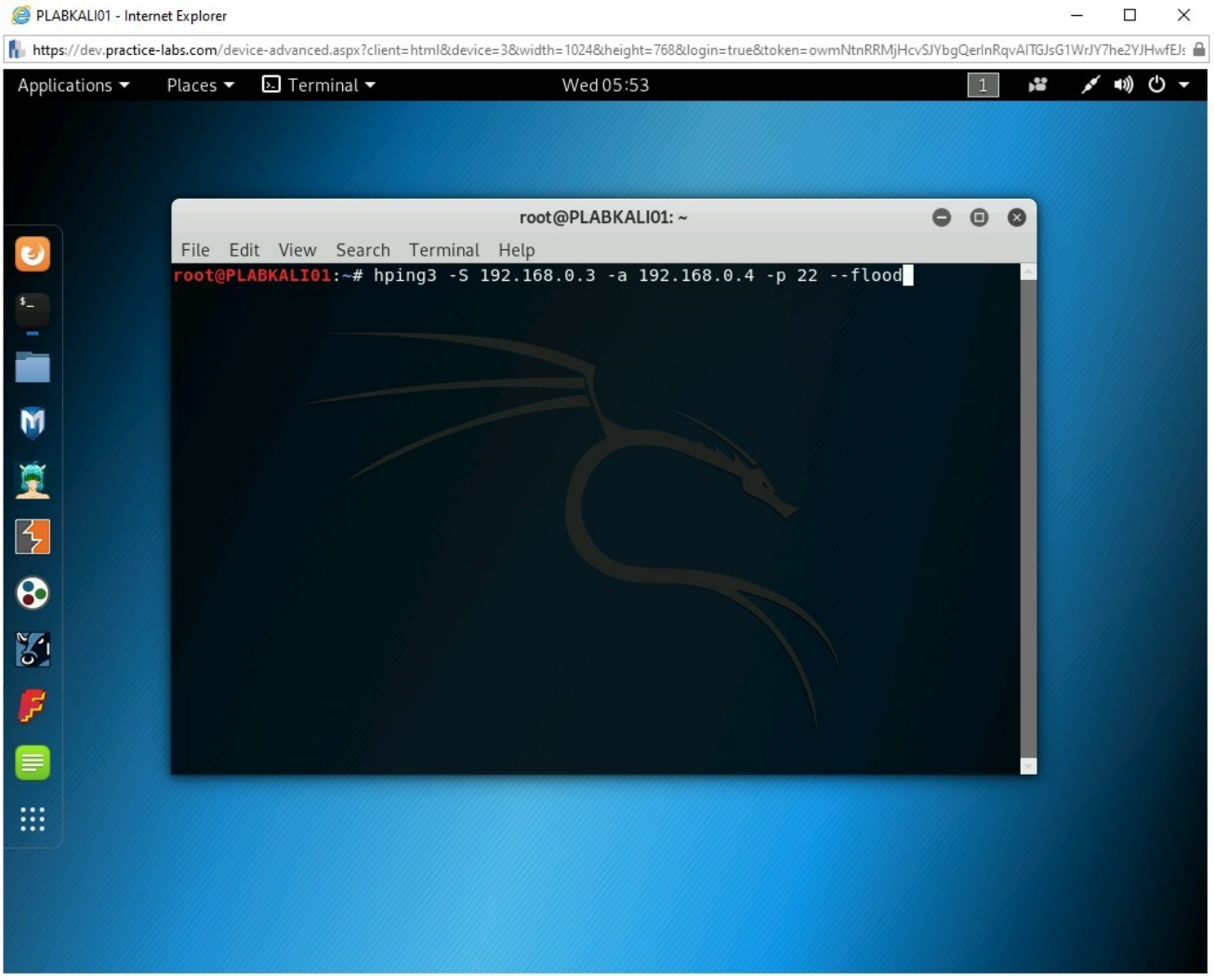


Figure 1.30 Screenshot of PLABKALI01: Showing the execution of the hping3 command.

Step 5

Connect to **PLABWIN10**. Ensure that the Wireshark window is open.

> ***Note:*** *Since you have attacked* ***PLABWIN10****, there will be a bit of a system lag on the computer.*

> **Alert:** If the PLABWIN10 console is unresponsive please continue on to the next step.

PLABWIN10 is now running out of system resources. The system will most likely become unresponsive. Attempt to click inside the Wireshark window or on the Start

charm. You will notice that the **PLABWIN10** system does not respond.

> ***Note:*** *You may get to see the out of memory error. However, the error may or may not occur, depending on your system resources and applications running at the time of packet capture. You might see other symptoms, such as the* ***PLABWIN10*** *window closing abruptly.*

The **SYN** packets are now being captured.

Note that there is a flood of SYN packets that are sent to **192.168.0.3**, which is **PLABWIN10**.

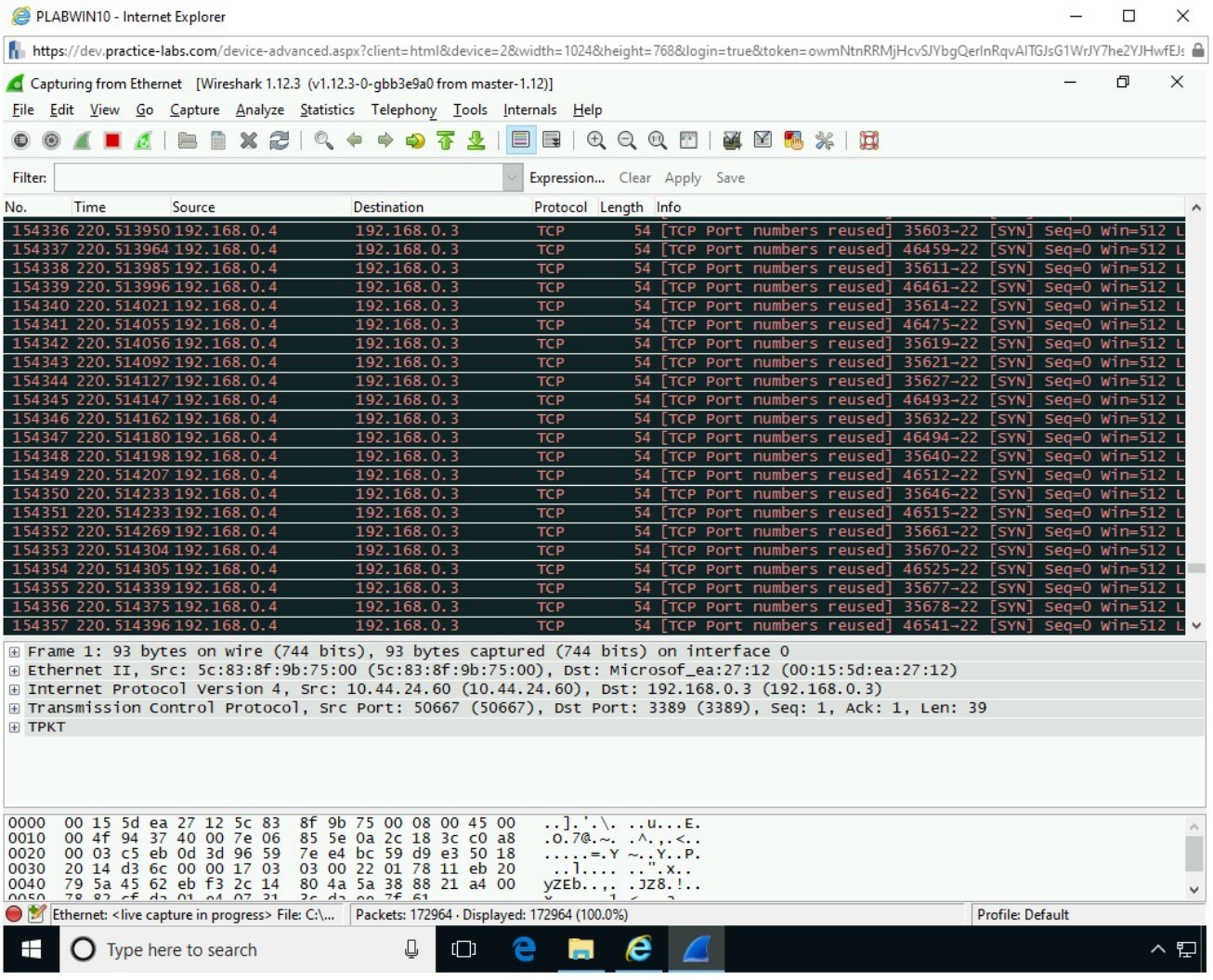


Figure 1.31 Screenshot of PLABWIN10: Showing the SYN packets in the Wireshark window.

Step 6

Switch to **PLABKALI01**. SYN flooding is still in progress.

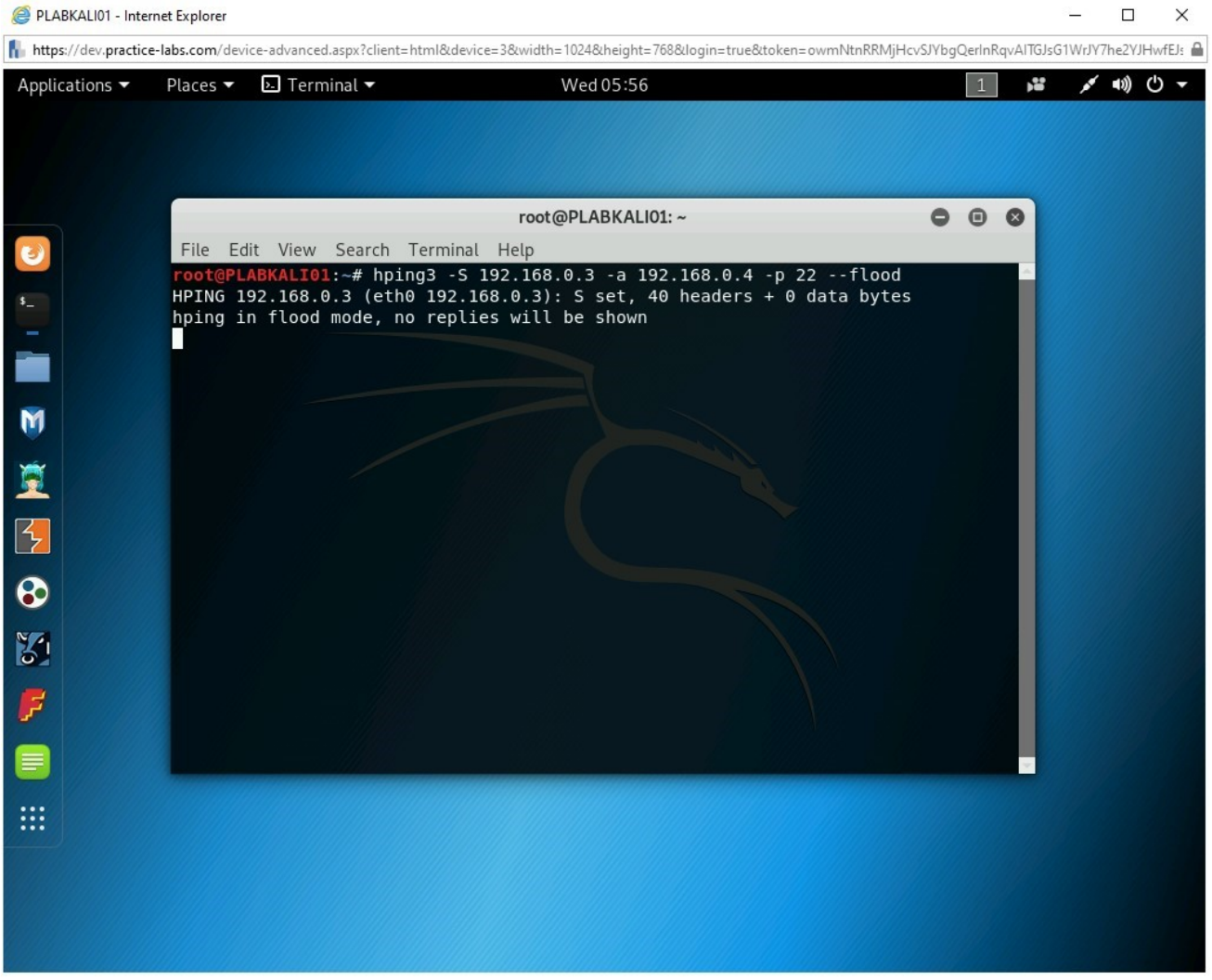


Figure 1.32 Screenshot of PLABKALI01: Showing the SYN flood attack in progress.

Step 7

Enter **CTRL + c** to kill the command.

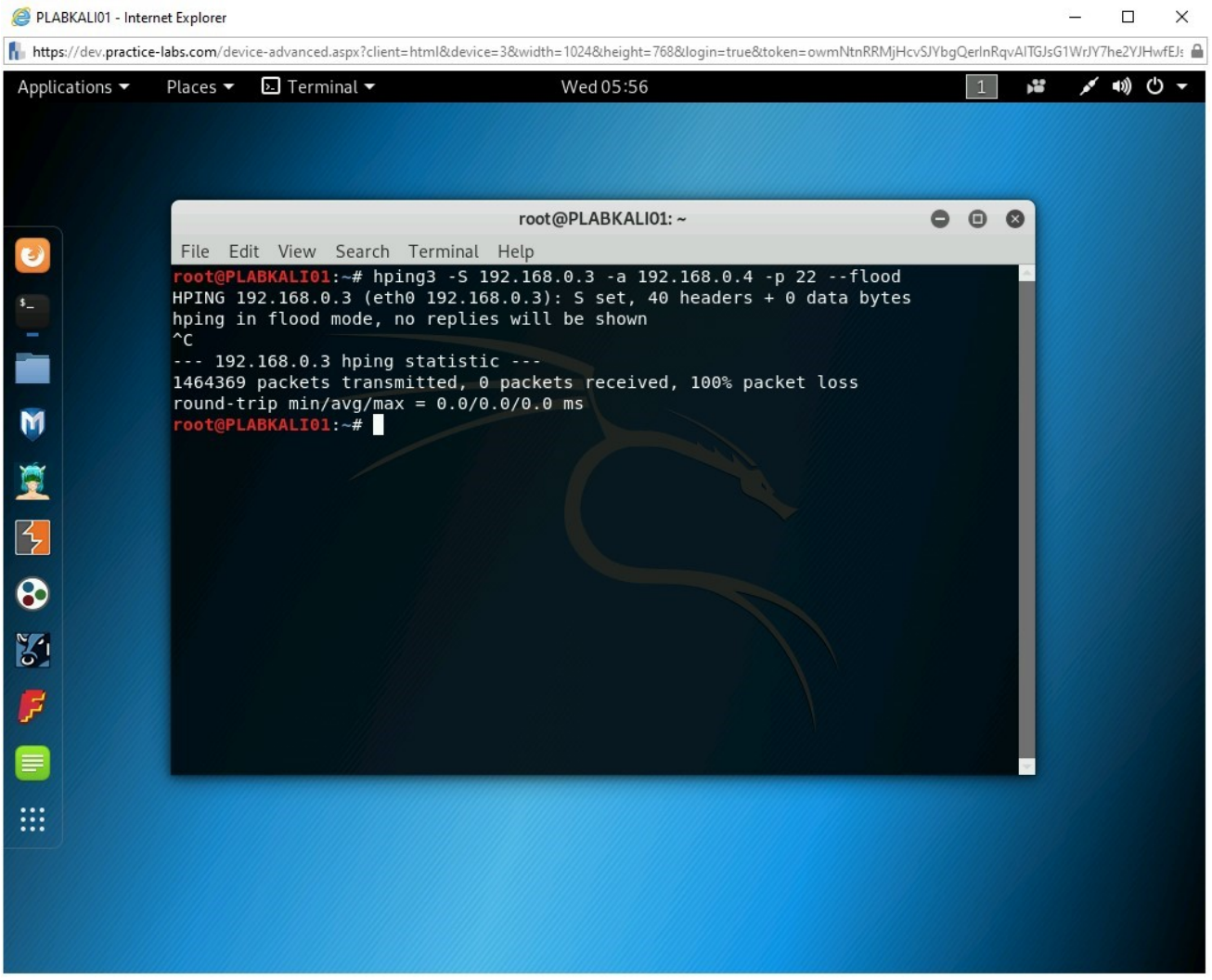


Figure 1.33 Screenshot of PLABKALI01: Terminating the hping3 command.

Step 8

Switch back to **PLABWIN10**. Close all open windows. You should now be on the desktop.

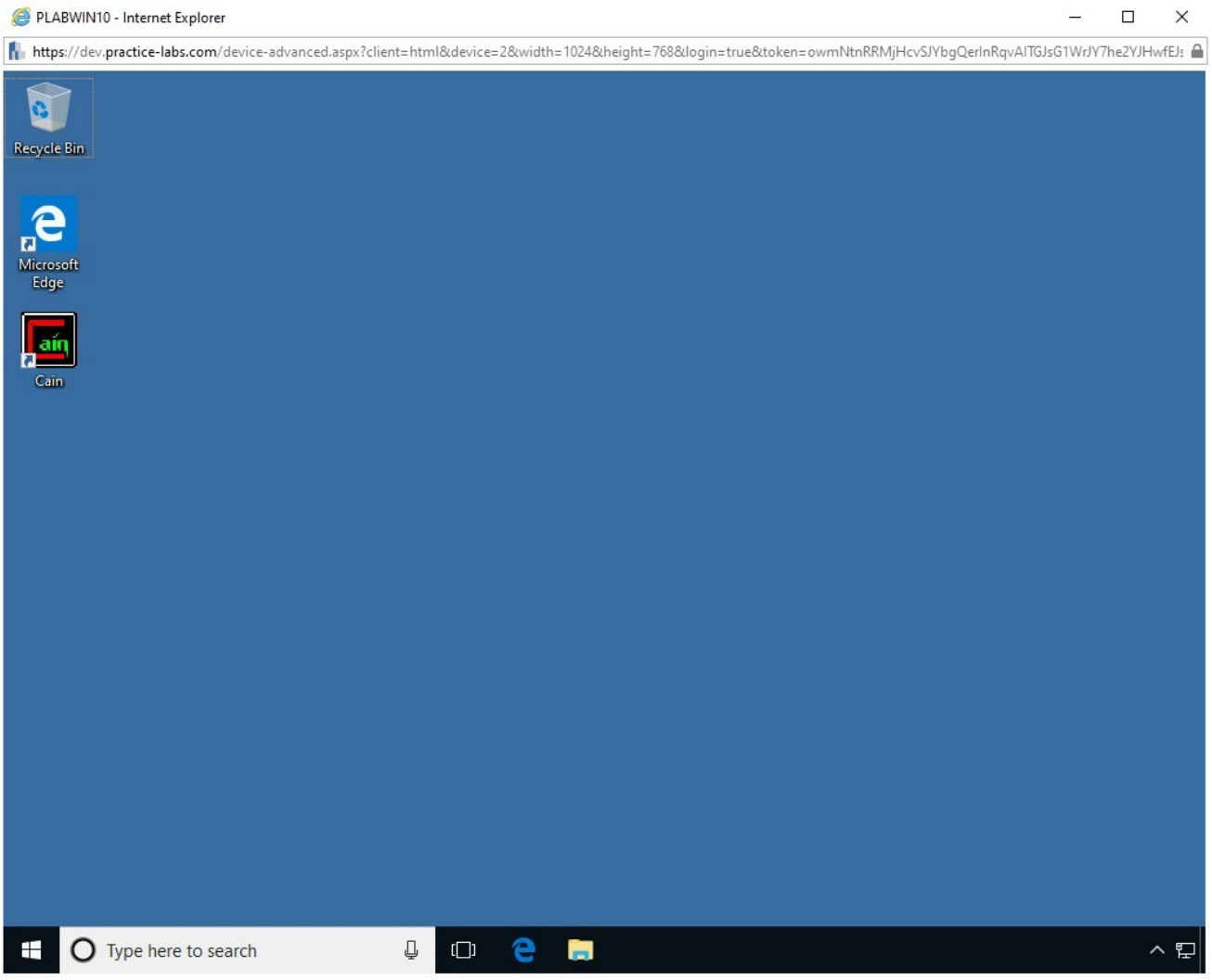


Figure 1.34 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Task 3 - Switch Off the Windows Firewall on PLABWIN10

You will need to switch off the Windows Firewall to perform an attack on **PLABWIN10**. There are attacking methods that you can use to bypass the Windows or any other firewall running on the target. However, for the sake of this module, you will switch off the Windows Firewall and proceed with the remaining tasks.

To switch off the Windows Firewall on **PLABWIN10**, perform the following steps:

Step 1

Ensure that you have connected to **PLABWIN10** and logged into the system.

Note that the **PLABWIN10** desktop is displayed.

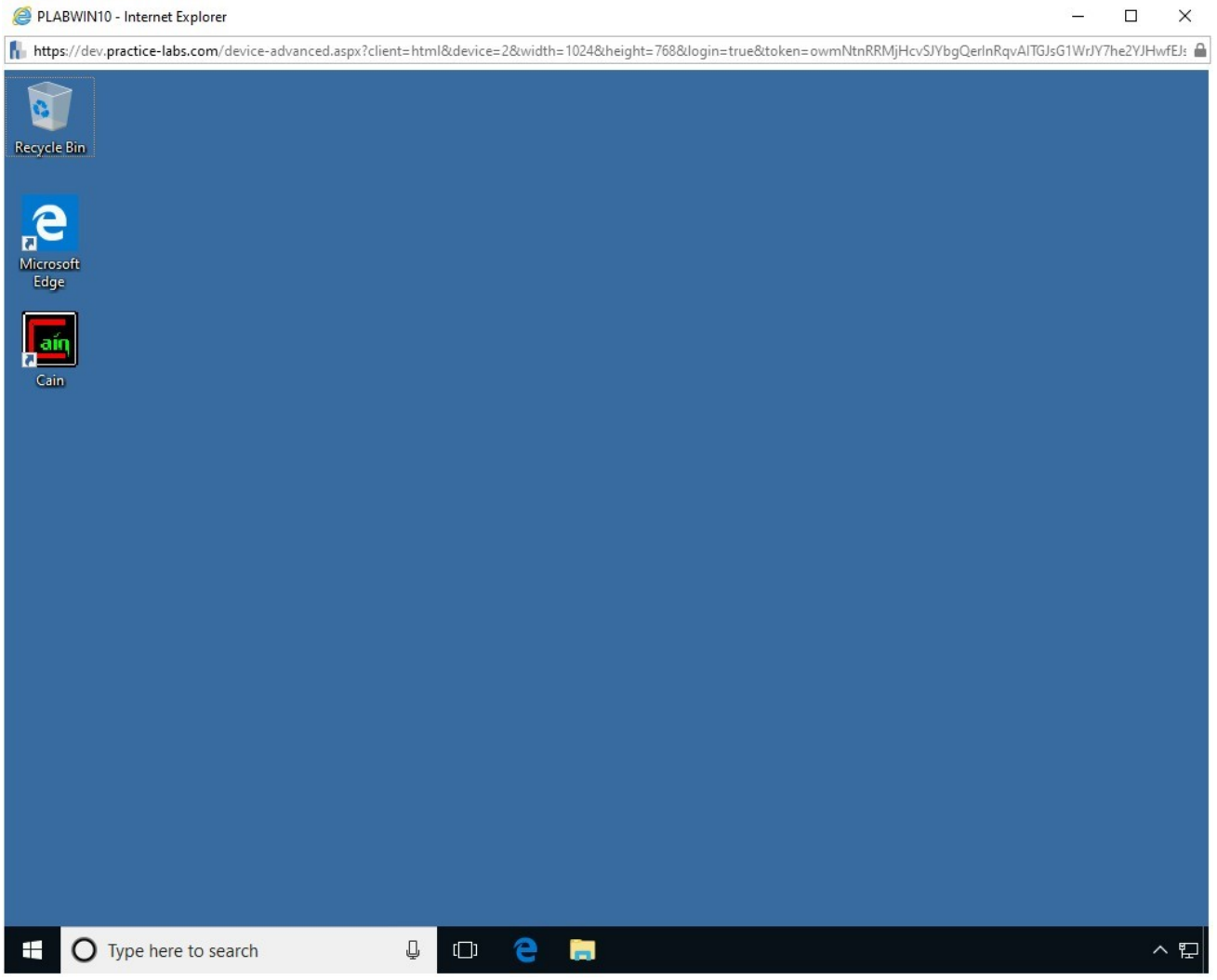


Figure 1.35 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Step 2

In the **Type here to search** text box, type the following:

```
windows firewall
```

From the search results, select the **Windows Defender Firewall**.

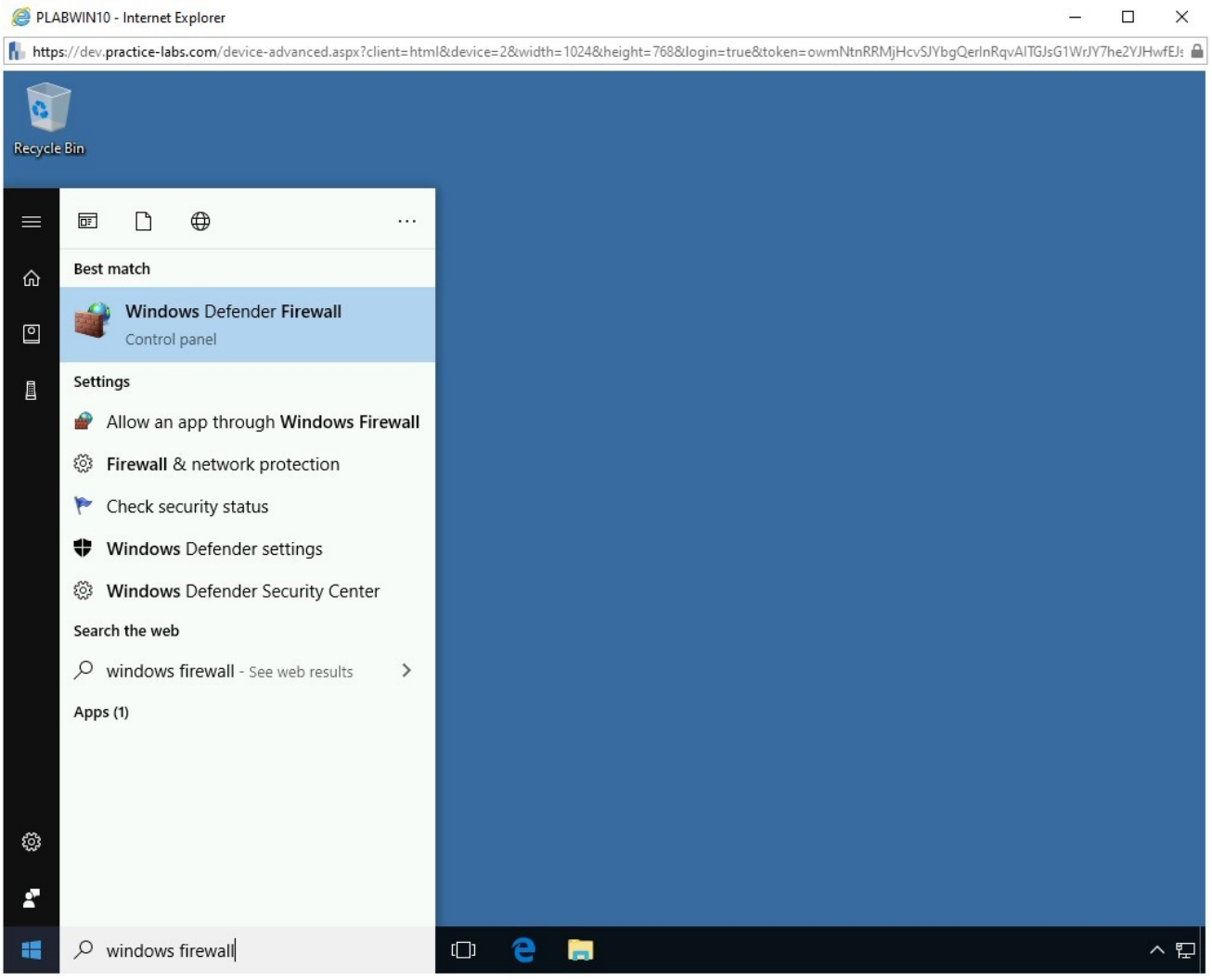


Figure 1.36 Screenshot of PLABWIN10: Right-clicking the Windows Charm and selecting Control Panel.

Step 3

The **Windows Defender Firewall** window is displayed. On the **Help protect your PC with Windows Defender Firewall** page, click **Turn Windows Defender Firewall on or off** in the left pane.

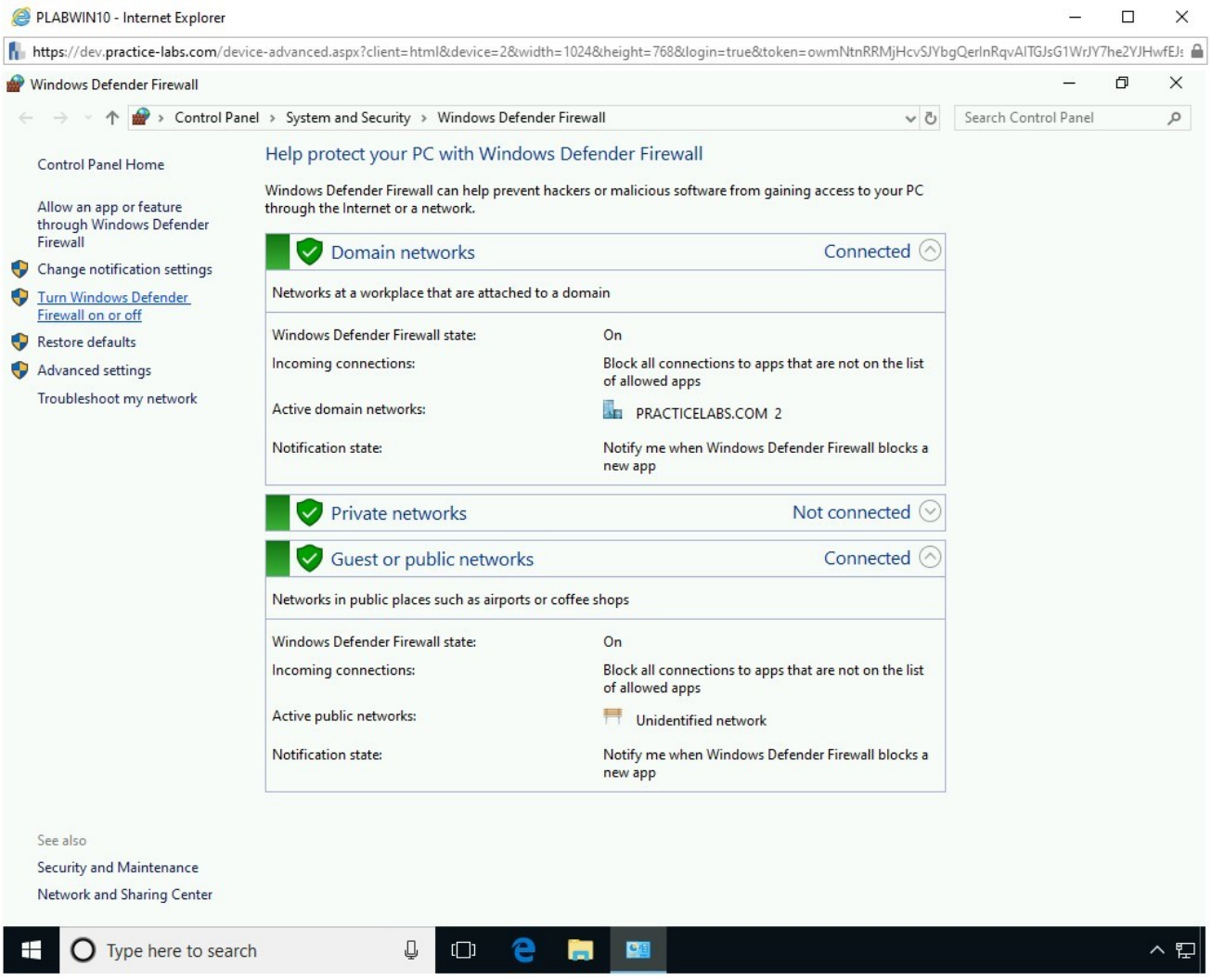


Figure 1.37 Screenshot of PLABWIN10: Clicking Turn Windows Firewall on or off in the left pane.

Step 4

On the **Customize settings for each type of network** page, select **Turn off Windows Defender Firewall (not recommended)** for **Domain**, **Private**, and **Public** network.

Click **OK**.

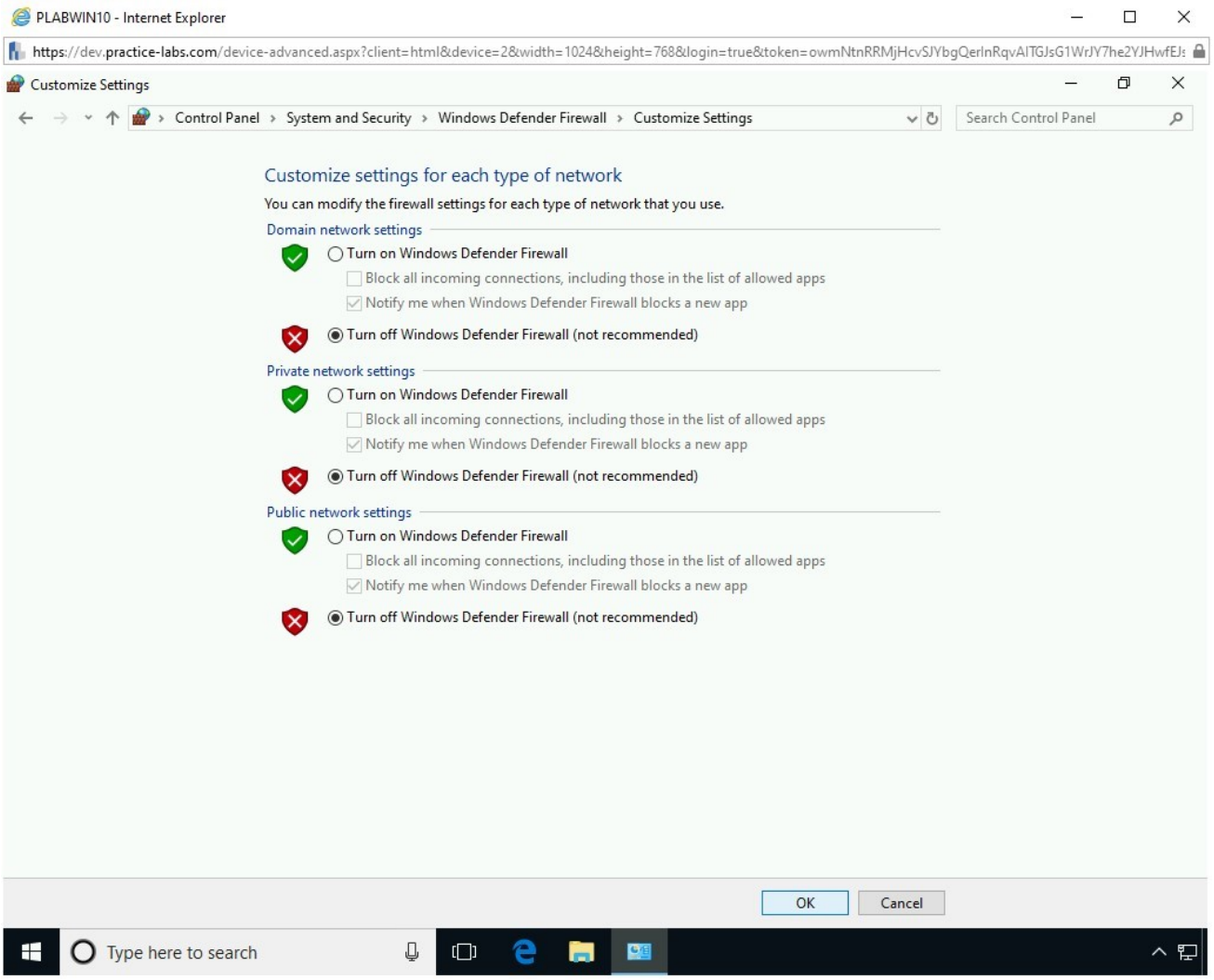


Figure 1.38 Screenshot of PLABWIN10: Selecting Turn off Windows Firewall (not recommended) for Domain, Private, and Public network.

Step 5

On the **Help protect your PC with Windows Defender Firewall** page, notice that **Windows Defender Firewall** is now turned off for **Domain**, **Private**, and **Public** network.

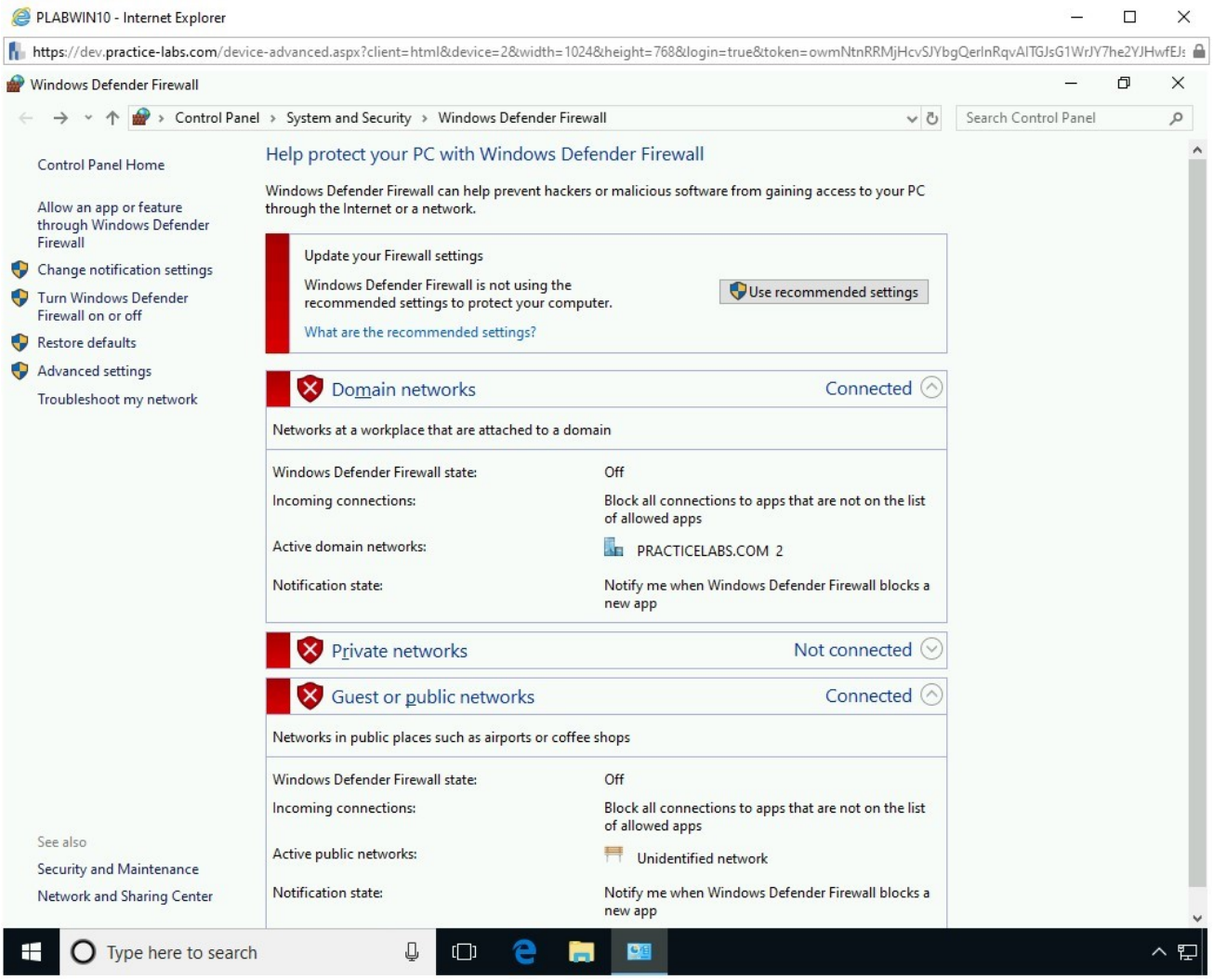


Figure 1.39 Screenshot of PLABWIN10: Verifying the Windows Firewall status and closing the Control Panel.

Step 6

Close the **Windows Defender Firewall** window.

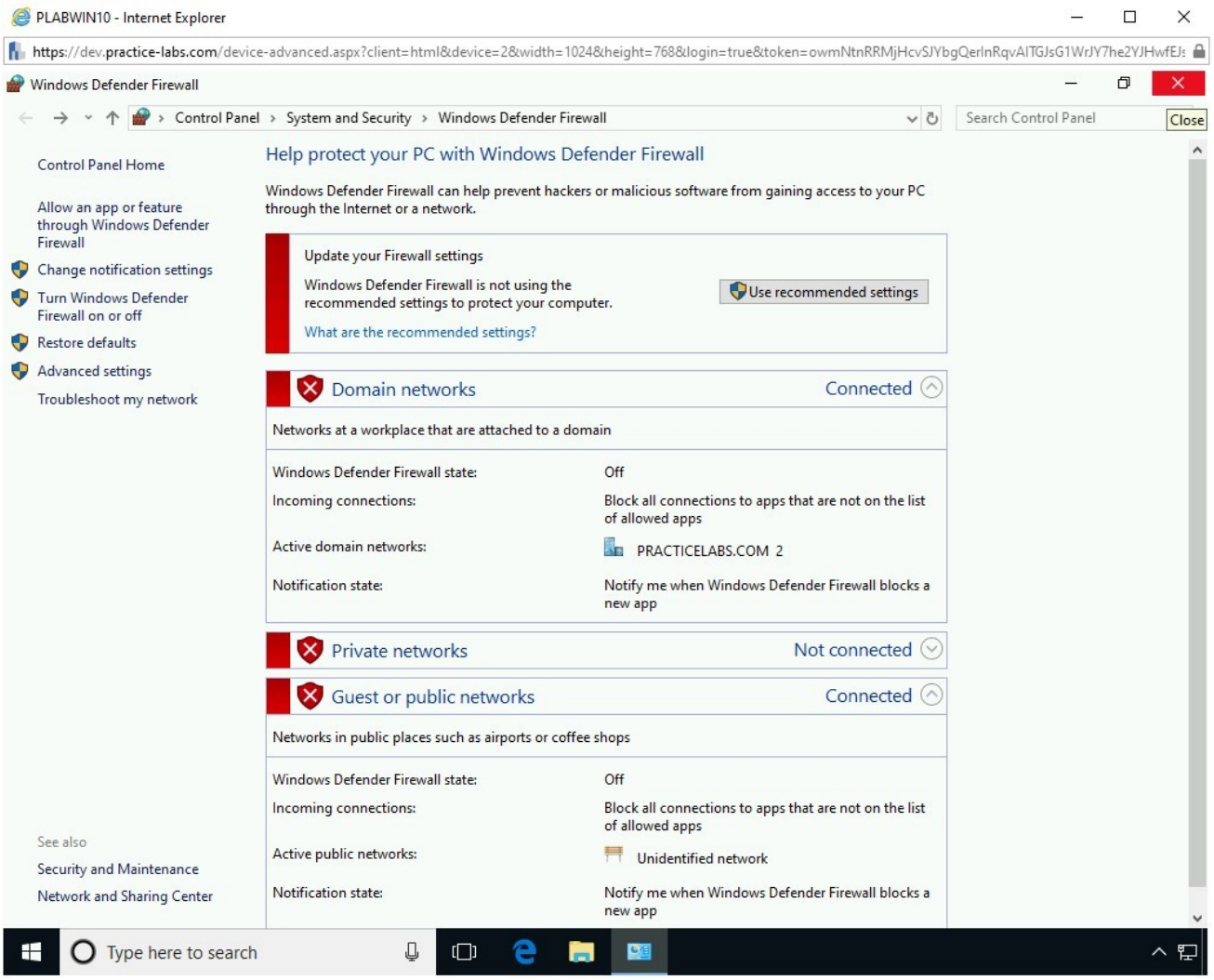


Figure 1.40 Screenshot of PLABWIN10: Verifying the Windows Firewall status and closing the Control Panel window.

Step 7

You should now be back on the desktop.

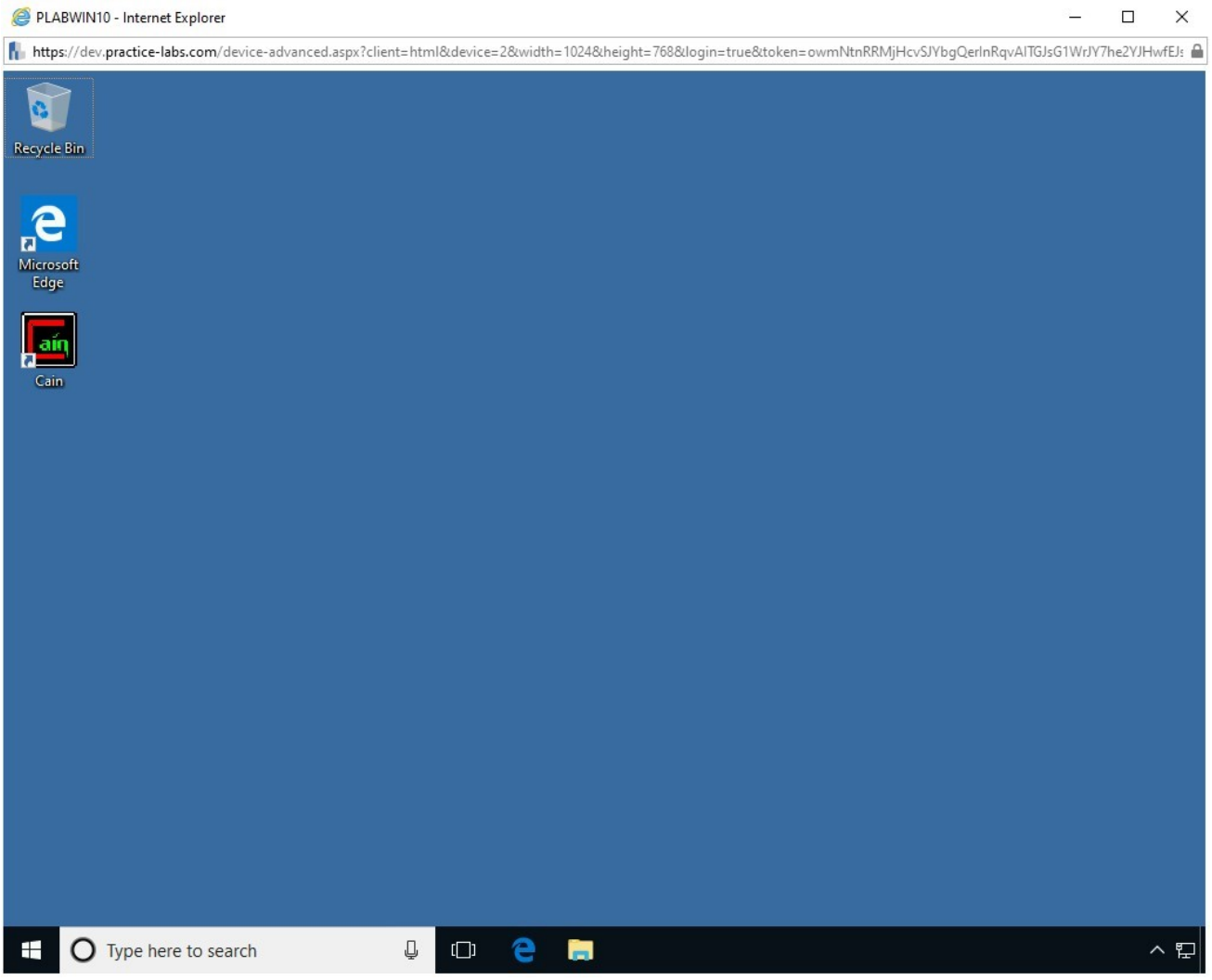


Figure 1.41 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Task 4 - Perform an ICMP Flood Attack

Similar to the SYN flood attack, there is another type of flood attack known as ICMP flooding, which is also a denial-of-service (DoS) attack. In this type of attack, instead of sending SYN packets, the attacker sends a flood of ICMP packets to a target system.

In this task, you will learn to conduct ICMP flooding.

To conduct ICMP flooding, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**.

In the **Type here to search** text box, type the following:

```
Wireshark
```

From the search results, select **Wireshark**.

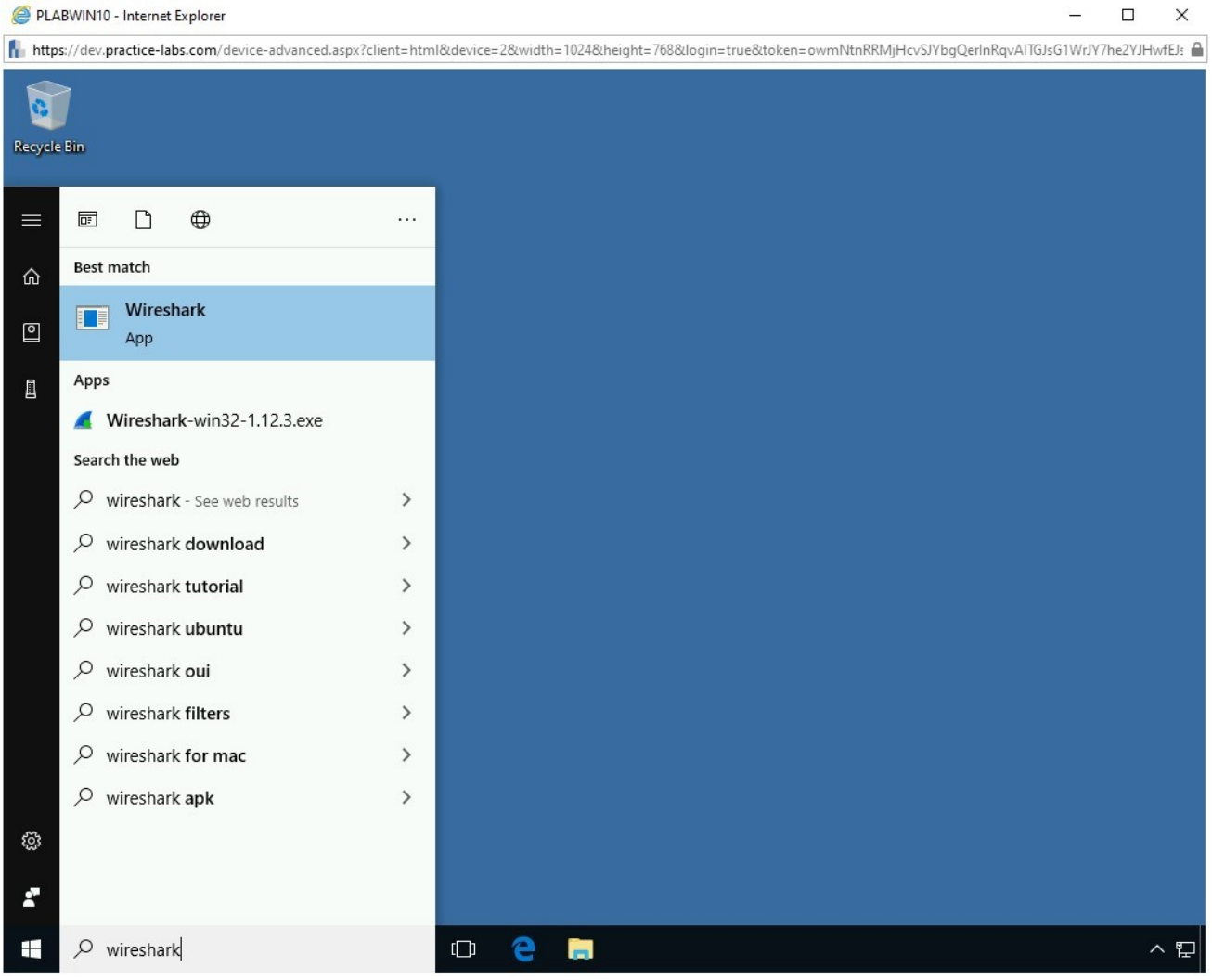


Figure 1.42 Screenshot of PLABWIN10: Double-clicking the Wireshark icon.

Step 2

The **Wireshark Network Analyzer** window is displayed.

Select **Ethernet** and click **Start**.

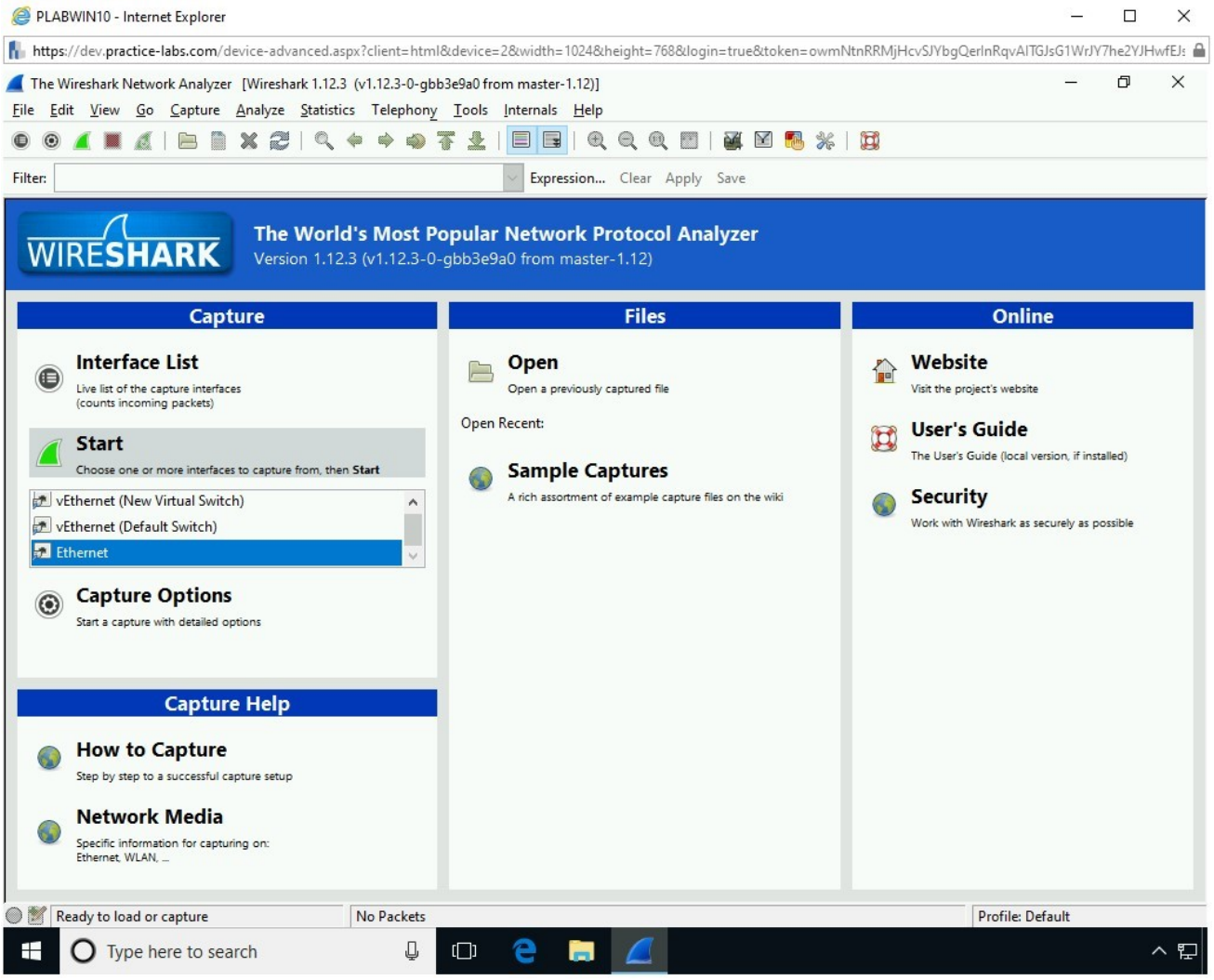


Figure 1.43 Screenshot of PLABWIN10: Selecting Ethernet and clicking Start.

Step 3

The packet capturing is in progress.

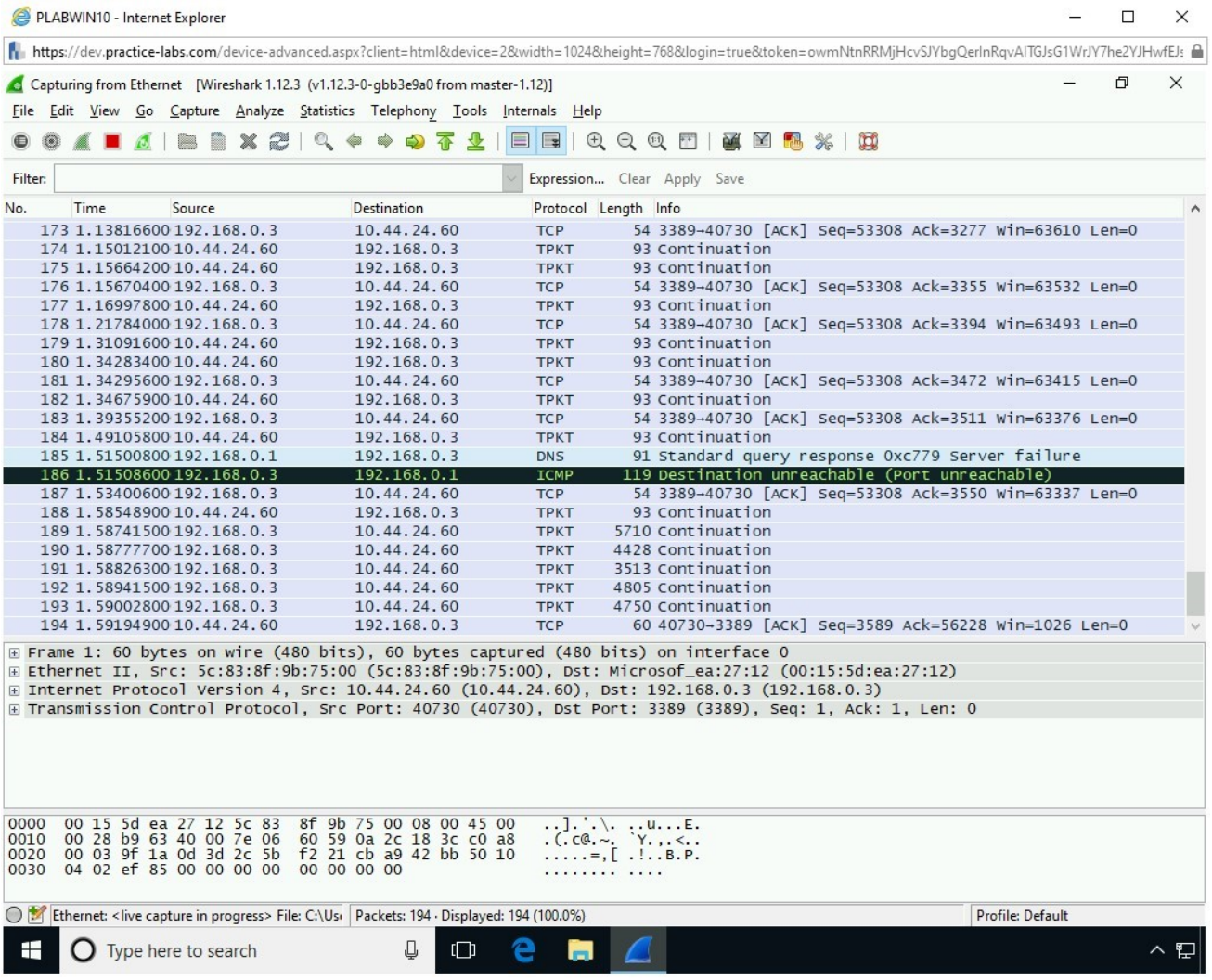


Figure 1.44 Screenshot of PLABWIN10: Showing the packet capturing in progress.

Step 4

Switch to **PLABKALI01**. The terminal window should be open.

Clear the screen by entering the following command:

```
clear
```

Type the following command:

```
hping3 -c 100 --icmp 192.168.0.3
```

Press **Enter**.

You will be sending **100 ICMP** packets to the target system, **192.168.0.3**.

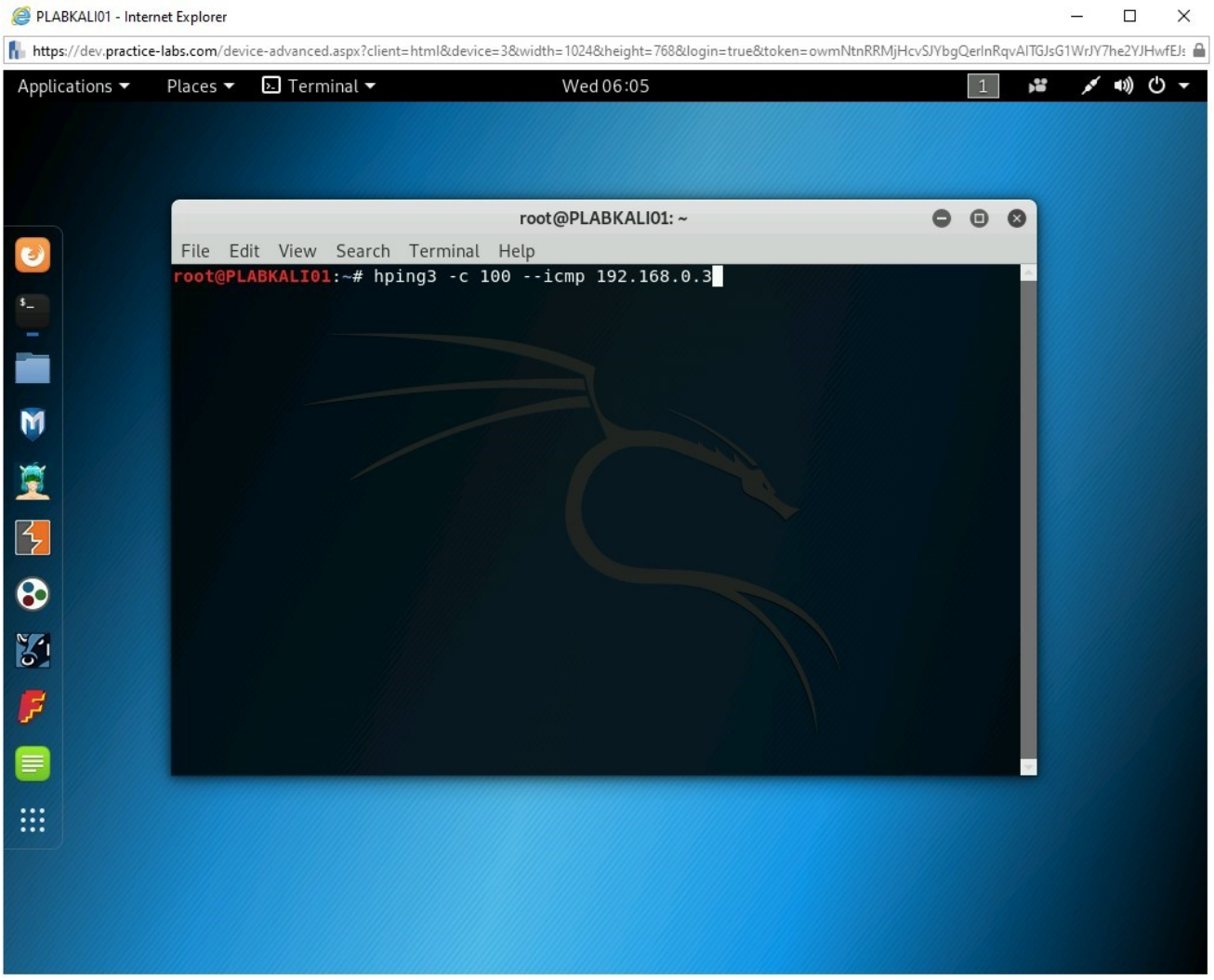


Figure 1.45 Screenshot of PLABKALI01: Entering the hping3 command in the terminal window.

Step 5

The ICMP packets are now sent to the target system.

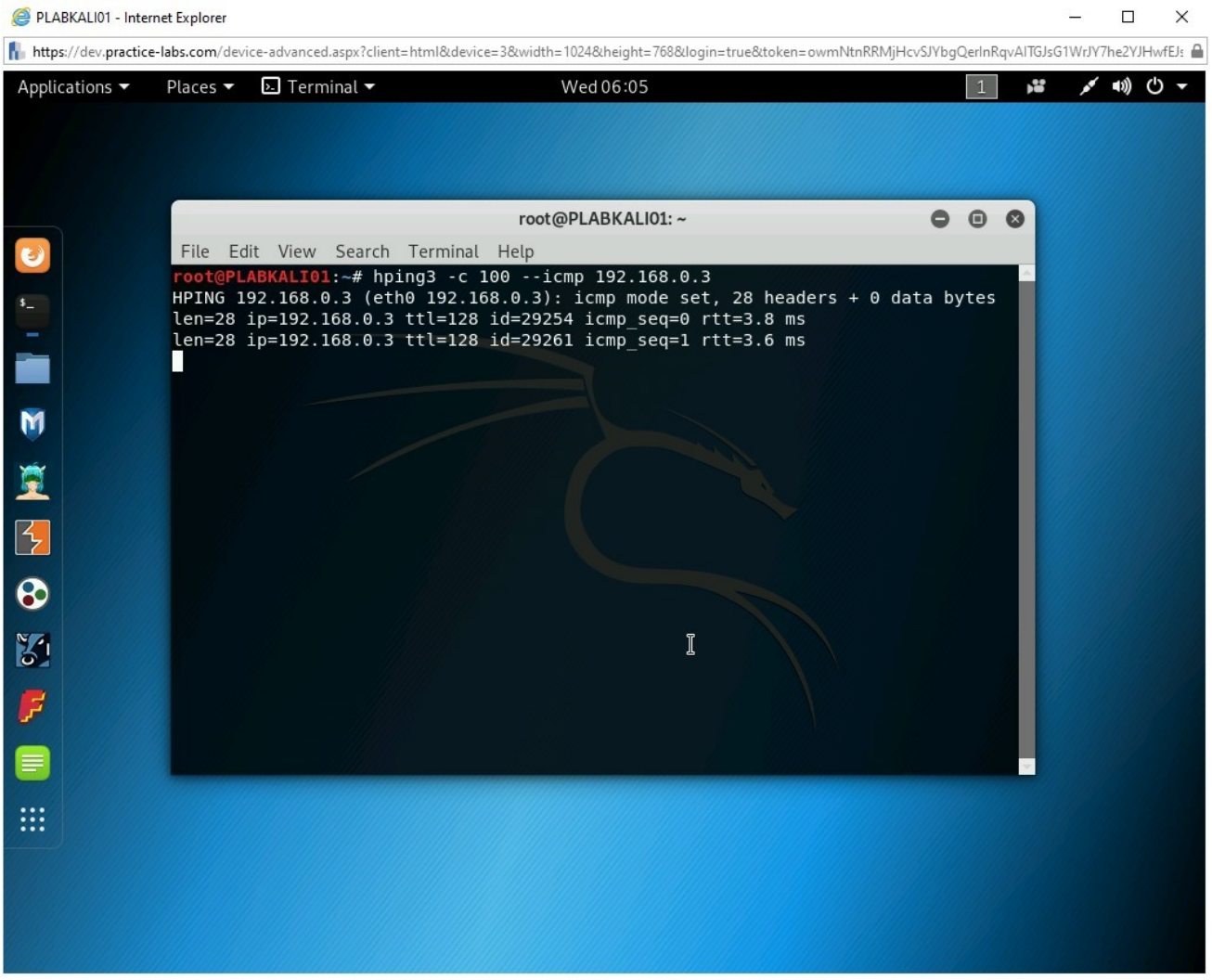


Figure 1.46 Screenshot of PLABKALI01: Showing the execution of the hping3 command.

Step 6

Switch to **PLABWIN10**. Notice the packet capture highlighted in blue color.

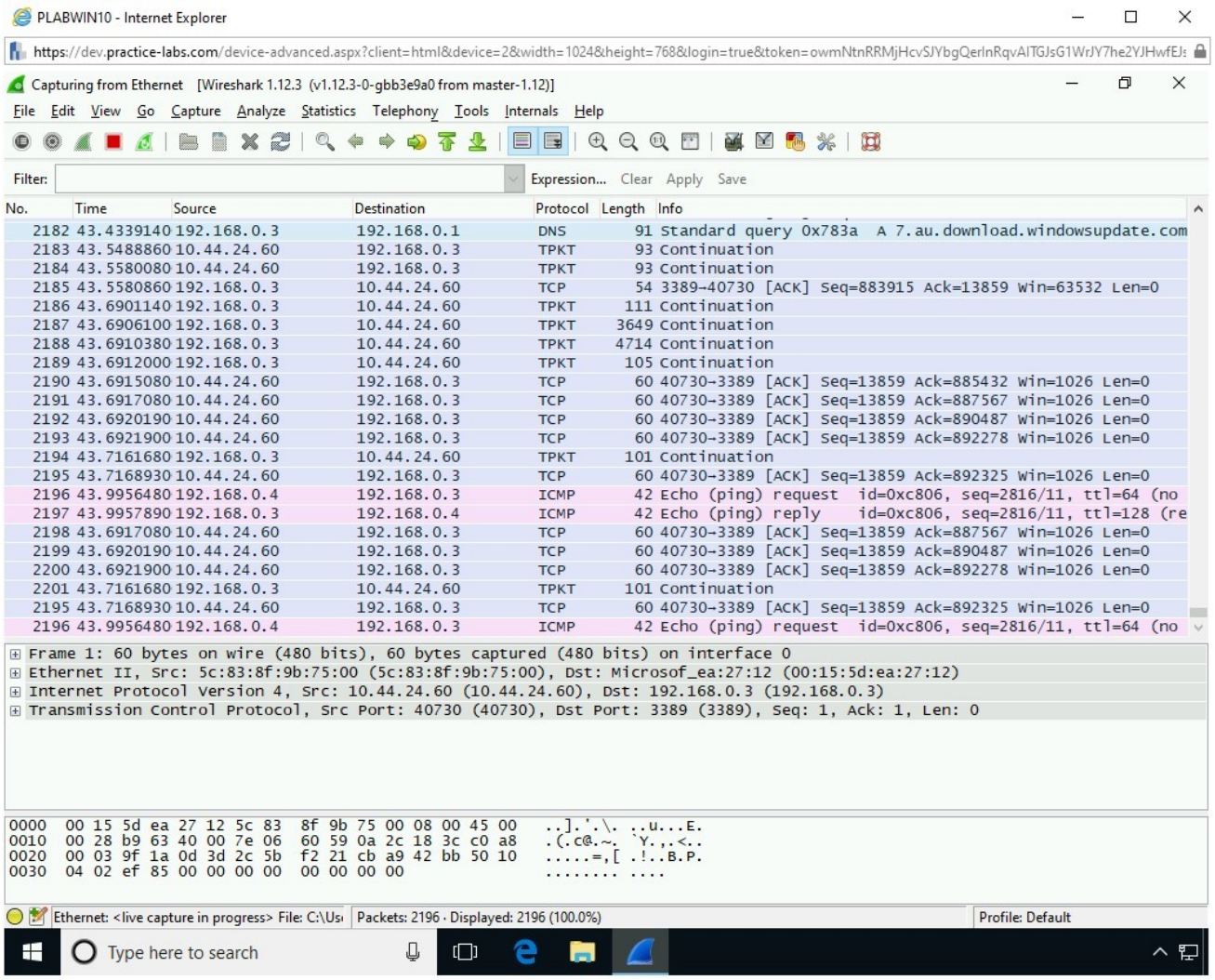


Figure 1.47 Screenshot of PLABWIN10: Showing the captured packets in the Wireshark window.

Step 7

Switch to **PLABKALI01**. Note that **100** packets have been successfully transmitted.

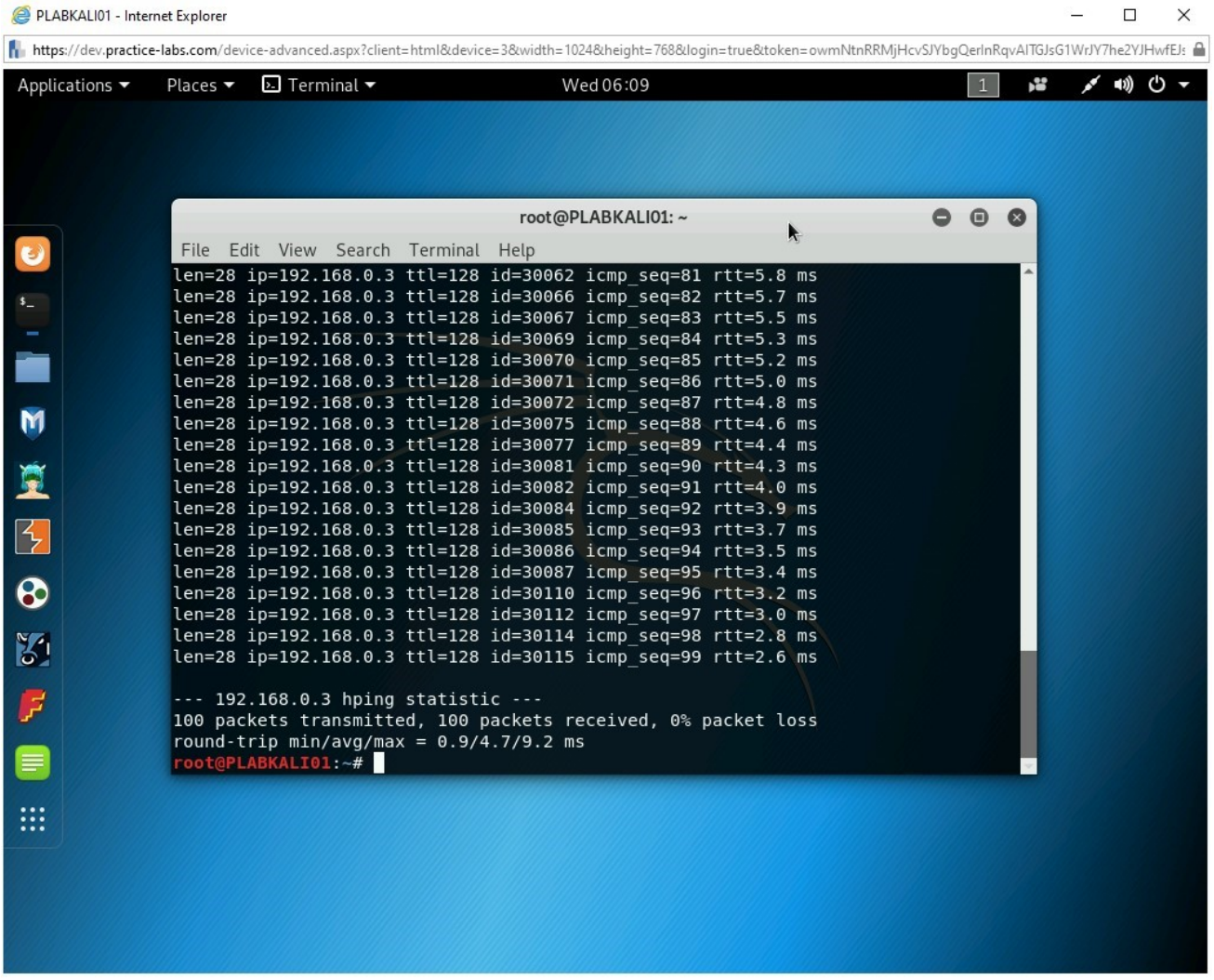


Figure 1.48 Screenshot of PLABKALI01: Showing the completion of the hping3 command.

Task 5 - Perform the Ping of Death Attack

Using the ping command, you can perform a Ping of Death attack. You can send data packets of size 65500 indefinitely to a target system. While it may not bring down the system, it will impact the performance of the target system. You can use a DDoS attack on a target system to bring it down.

In this task, you will perform the Ping of Death attack. To do this, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABDM01**.

The **Server Manager** window is displayed. You can close this window.

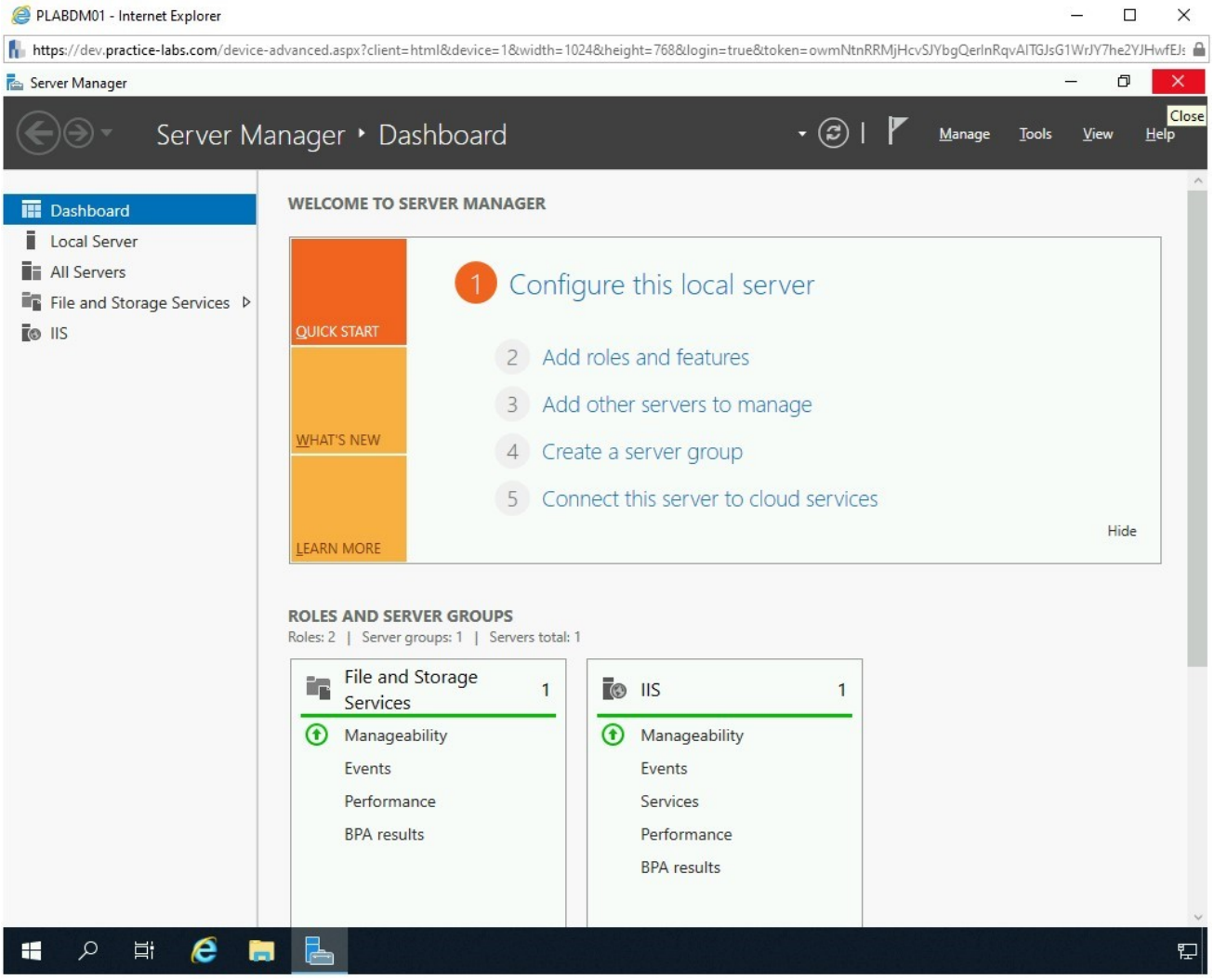


Figure 1.49 Screenshot of PLABDM01: Showing the desktop of PLABDM01.

Step 2

Right-click the **Windows Charm** and select **Run**.

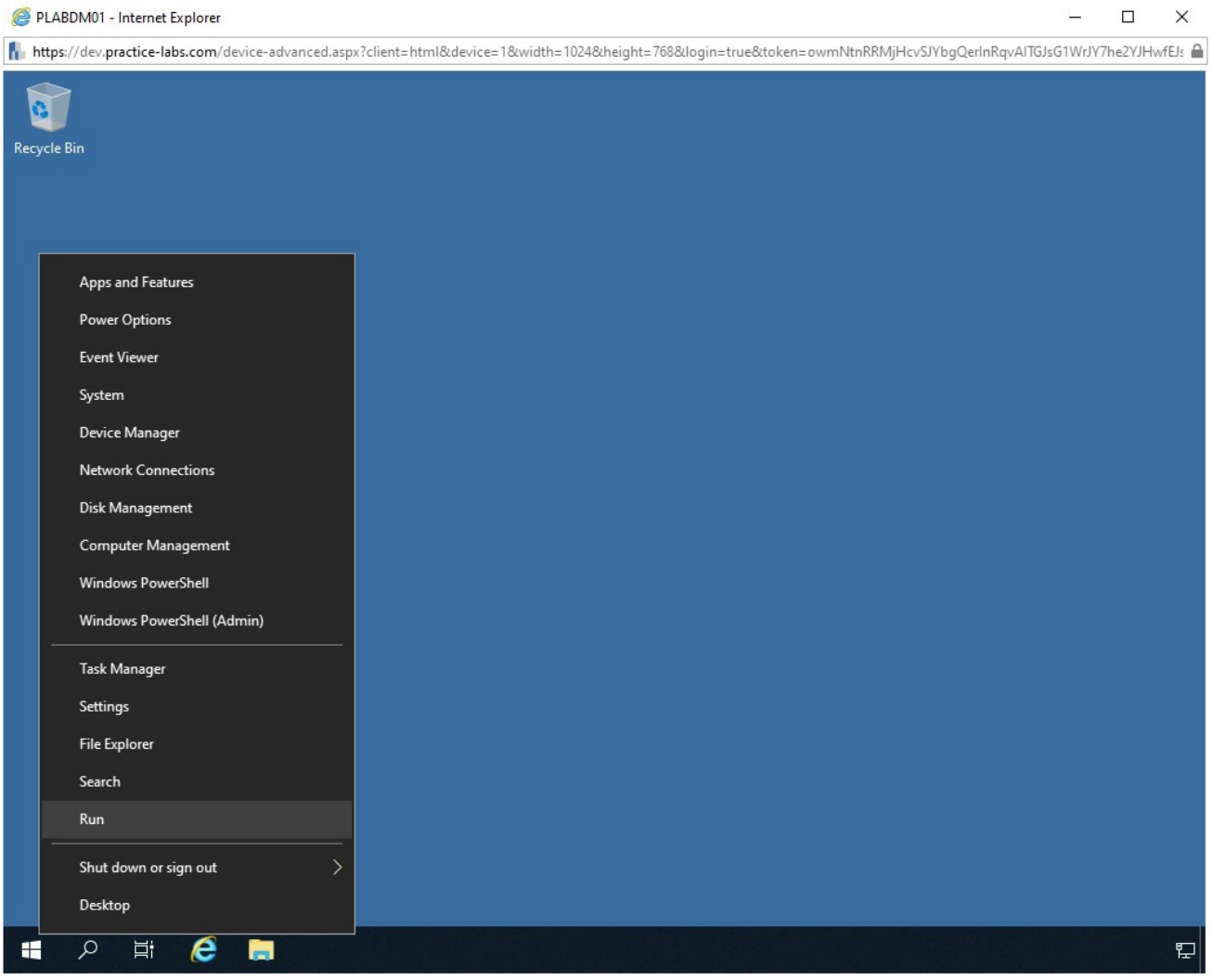


Figure 1.50 Screenshot of PLABDM01: Right-clicking the Windows charm and selecting Run.

Step 3

In the **Open** textbox of the **Run** dialog box, type the following command:

```
cmd
```

Click **OK**.

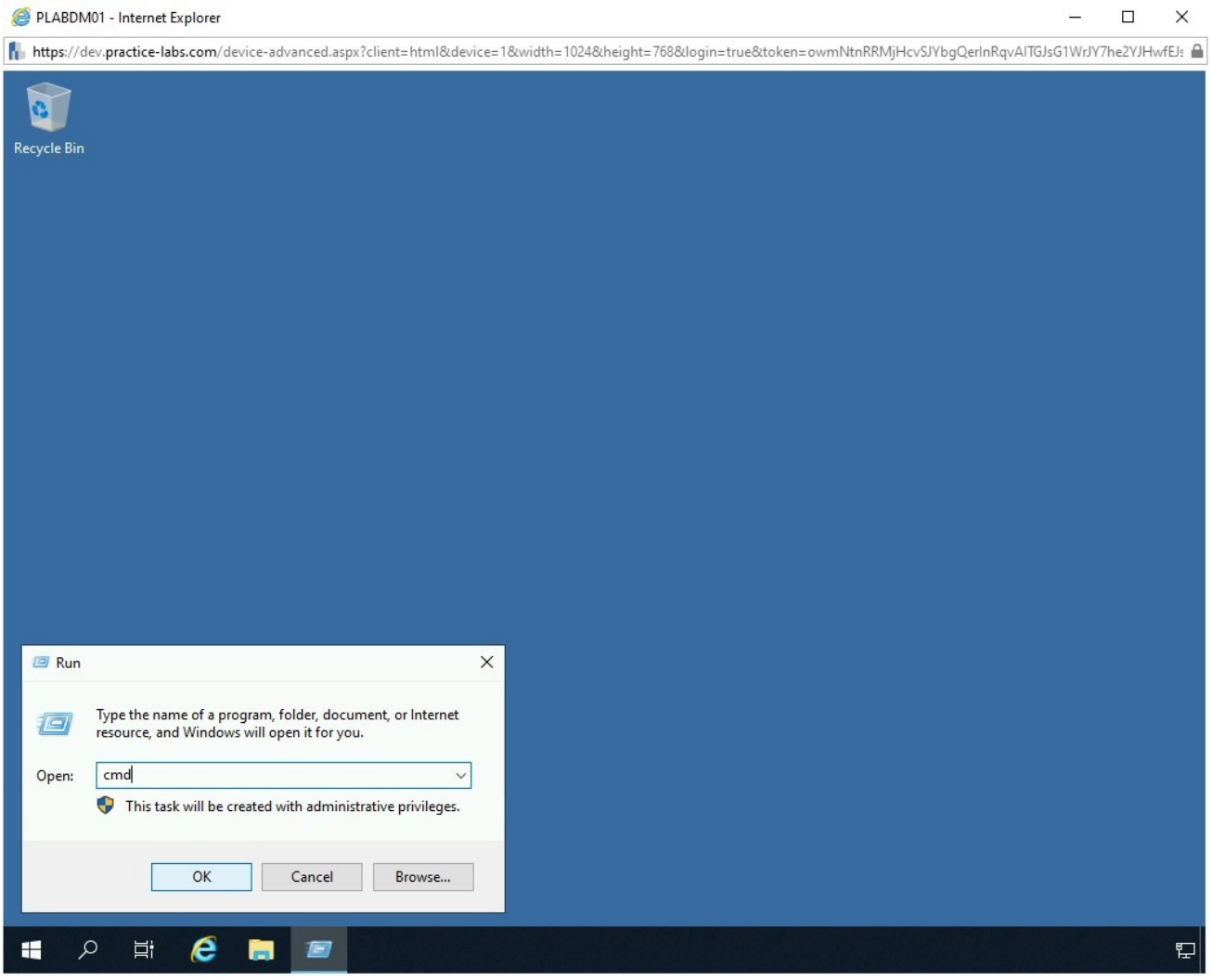


Figure 1.51 Screenshot of PLABDM01: Entering the cmd command and clicking OK on the Run dialog box.

Step 4

The command prompt window is displayed. Type the following command:

```
ping 192.168.0.3 -t -l 65500
```

Press **Enter**.

Note: *192.168.0.3 is the IP address of the target system, which is* ***PLABWIN10****. The* ***-t*** *parameter will send the data packets indefinitely until*

you terminate the command. The ***-l*** *parameter defines the size of the data packet.*

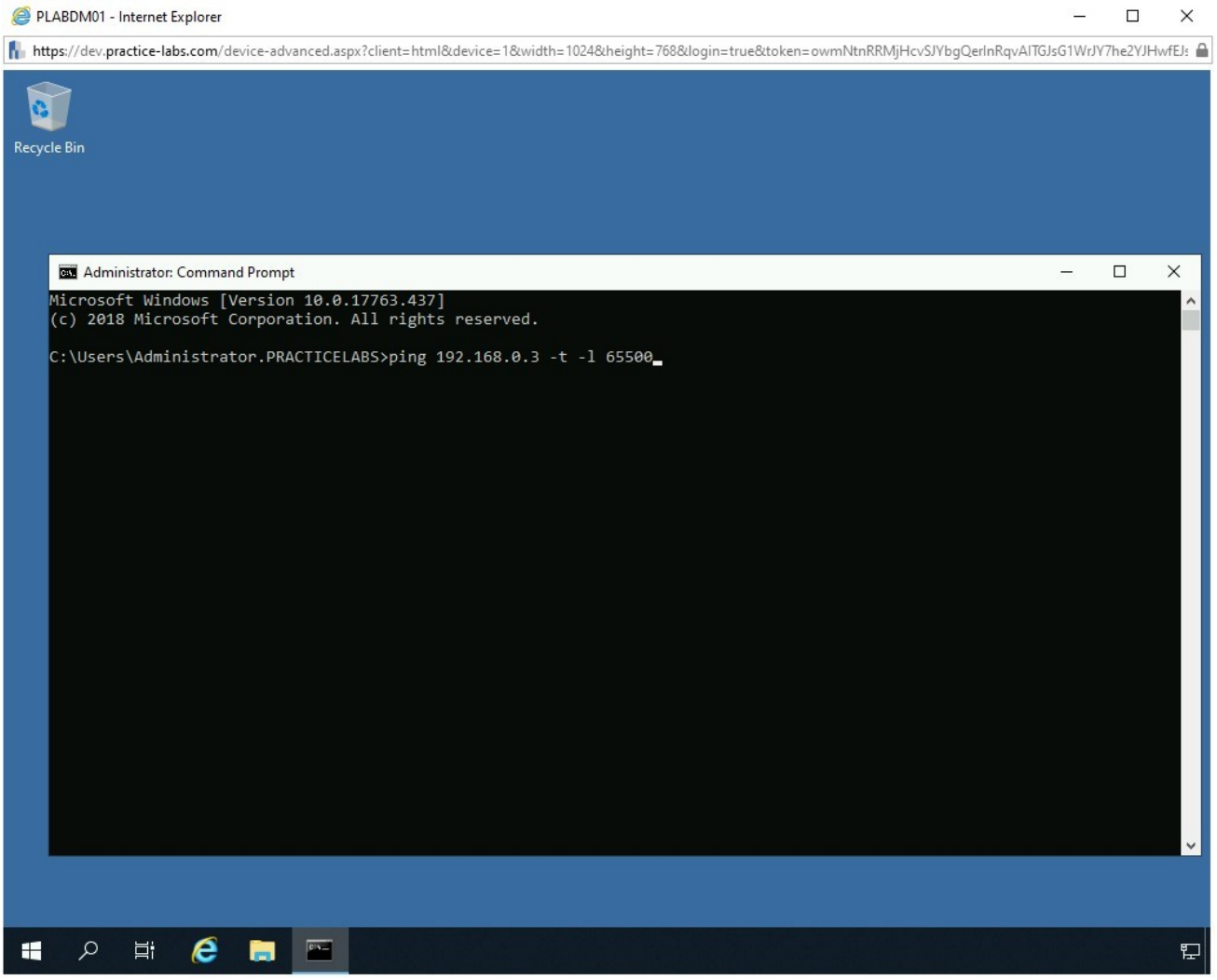


Figure 1.52 Screenshot of PLABDM01: Entering the ping command on the command line.

Step 5

The ping command starts to send packets to the target system, which is **PLABWIN10**.

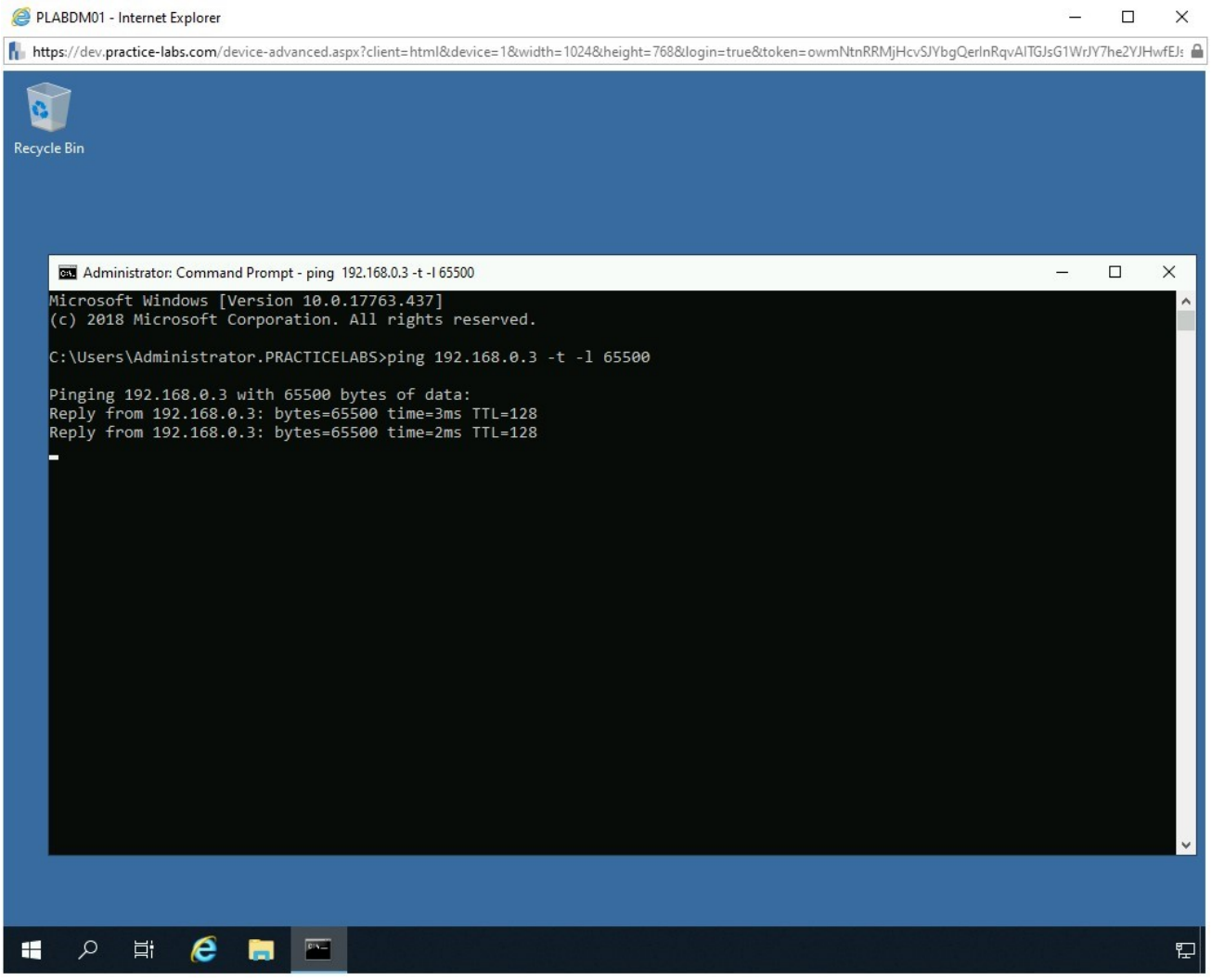


Figure 1.53 Screenshot of PLABDM01: Showing the execution of the ping command.

Step 6

Switch to **PLABWIN10**. And close Wireshark.

You should be on the desktop. Right-click the taskbar and select **Task Manager**.

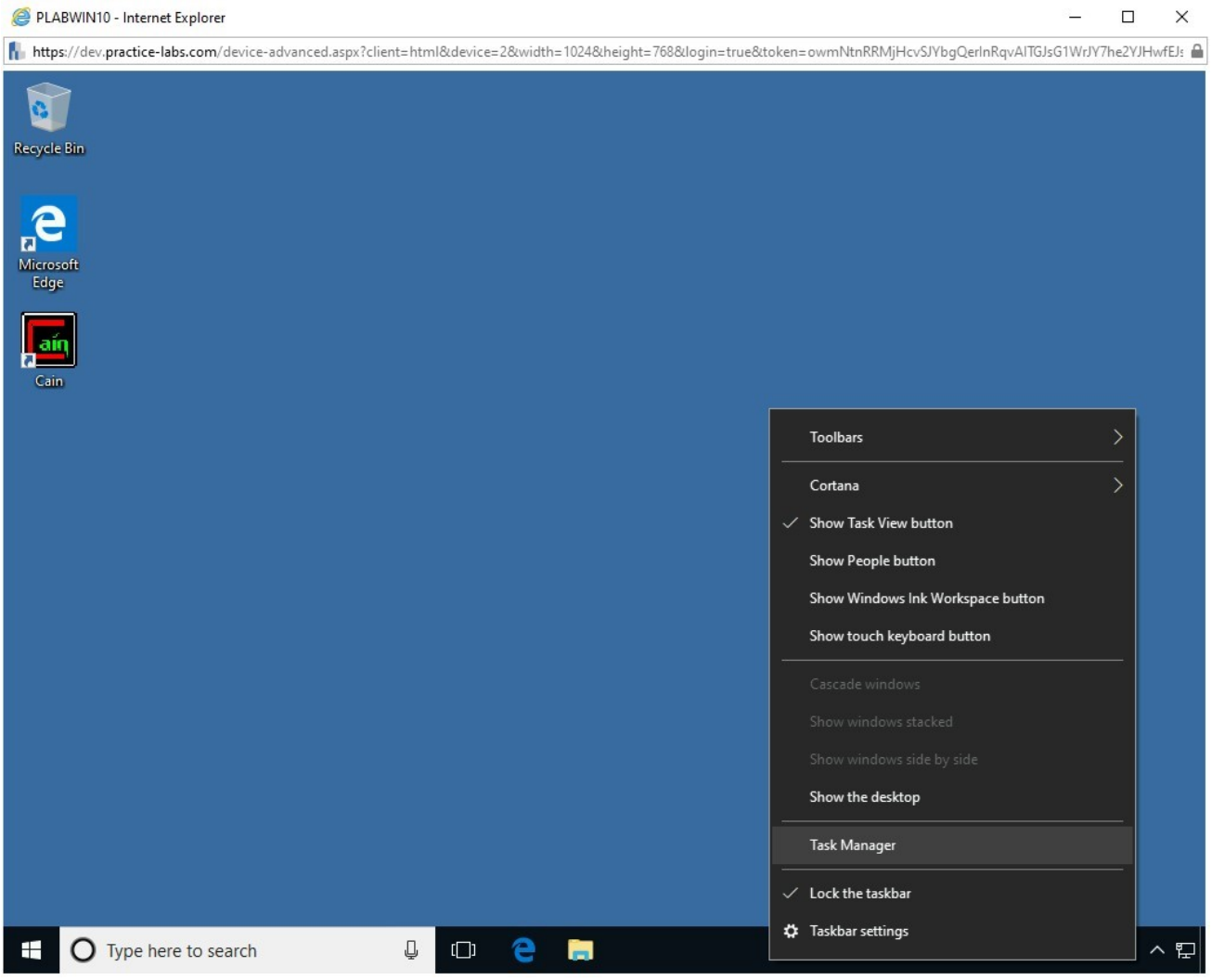


Figure 1.54 Screenshot of PLABWIN10: Right-clicking the taskbar and selecting Task Manager.

Step 7

Click the **More details** down arrow.

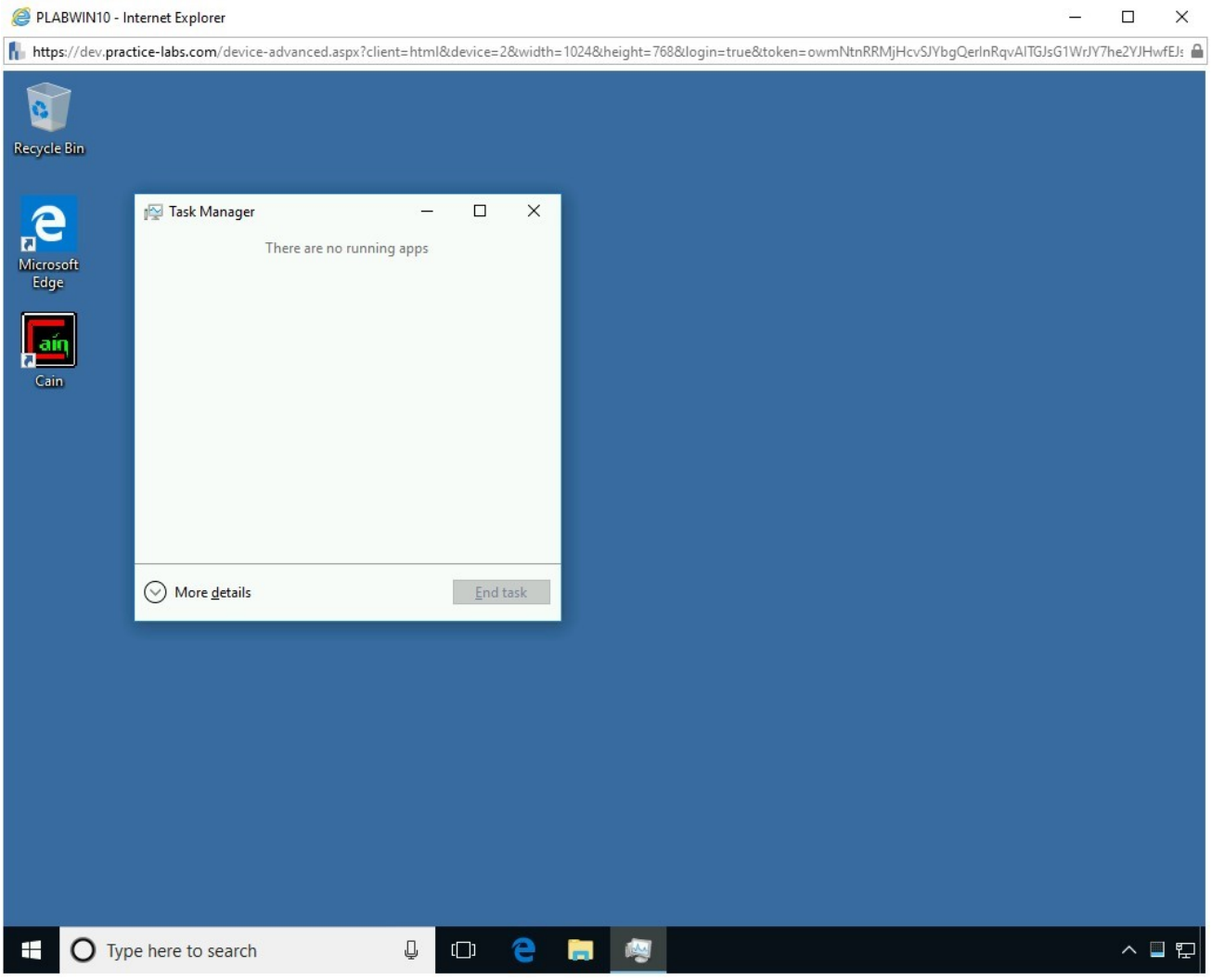


Figure 1.55 Screenshot of PLABWIN10: Clicking the More details arrow on the Task Manager dialog box.

Step 8

Notice that multiple tabs in the **Task Manager** window appear. Click the **Performance** tab.

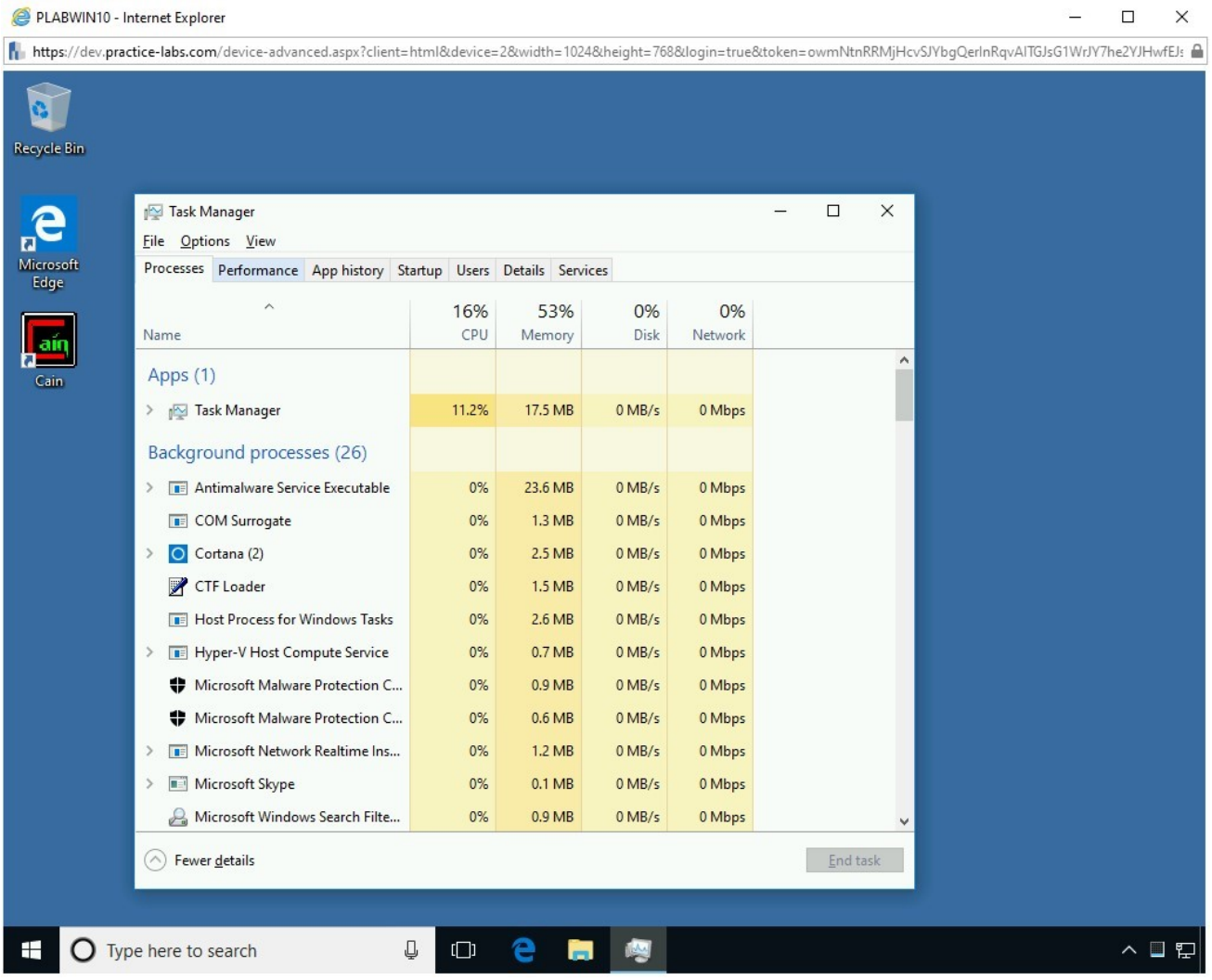


Figure 1.56 Screenshot of PLABWIN10: Clicking the Performance tab in Task Manager.

Step 9

On the **Performance** tab, **CPU** is selected by default. Click **Ethernet**.

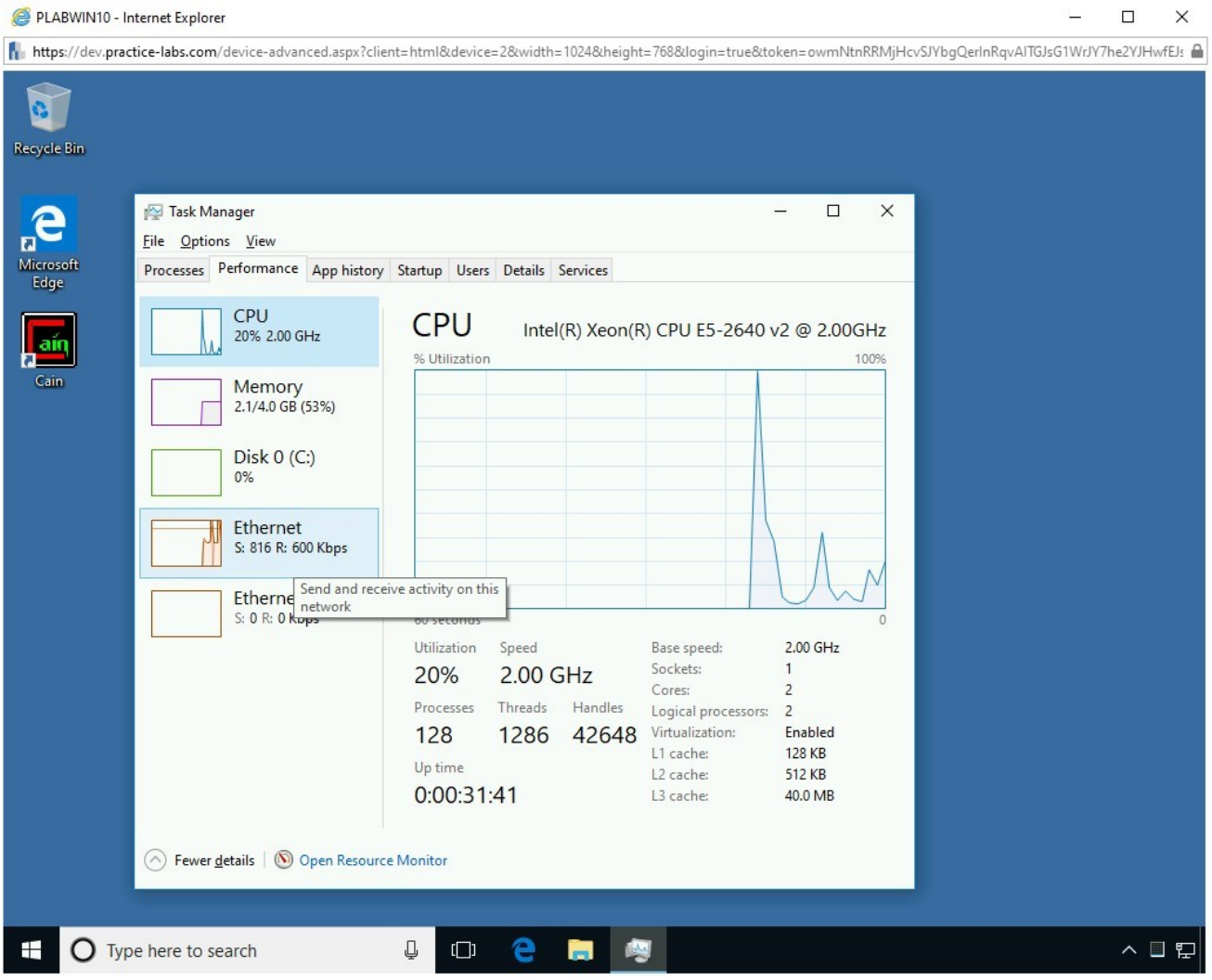


Figure 1.57 Screenshot of PLABWIN10: Selecting Ethernet on the Performance tab in Task Manager.

Step 10

Notice that there is an increased network activity on the **PLABWIN10** system.

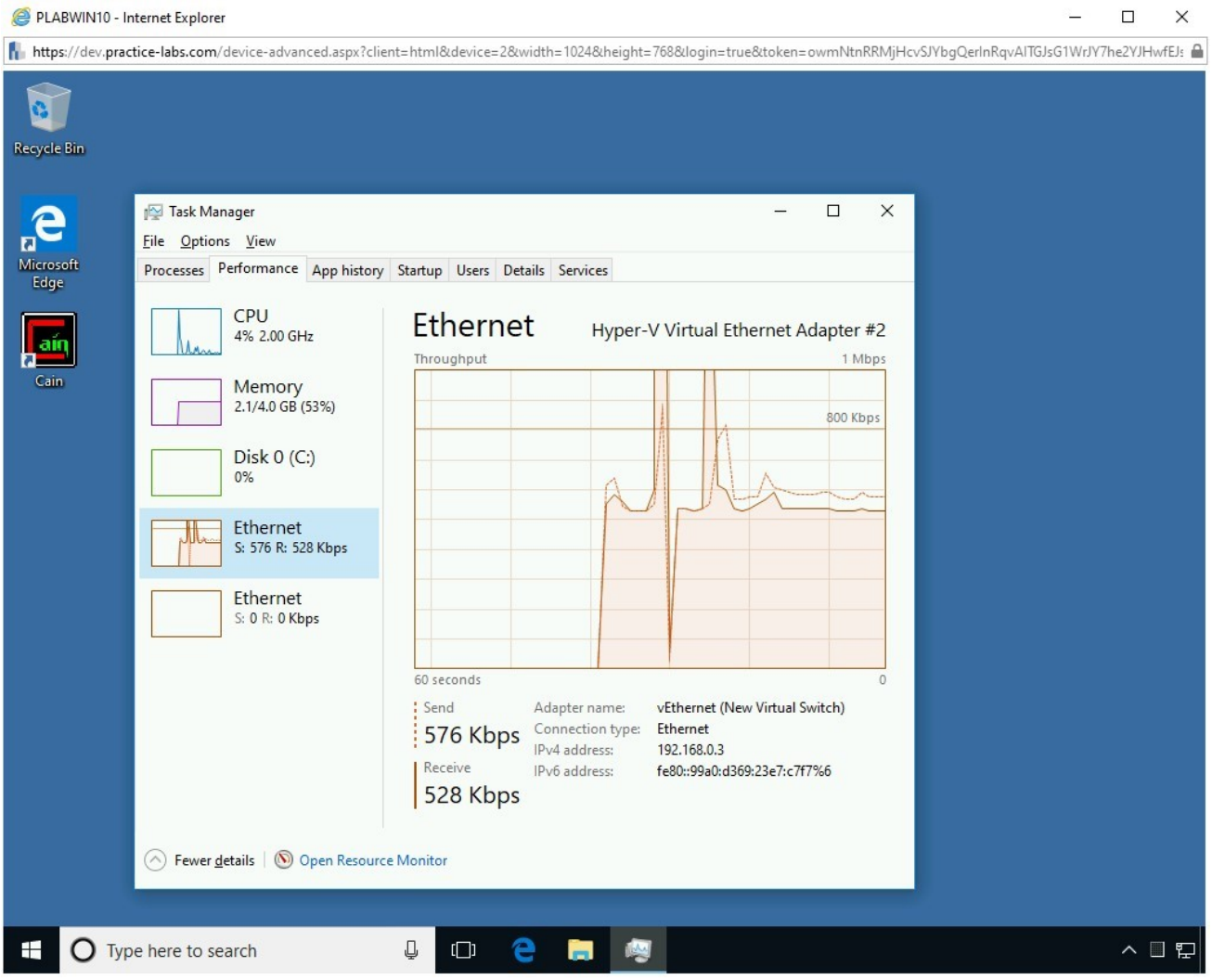


Figure 1.58 Screenshot of PLABWIN10: Showing the increased traffic activity in PLABWIN10.

Step 11

Switch back to **PLABDM01**.

Press **Ctrl + C** to terminate the ping command.

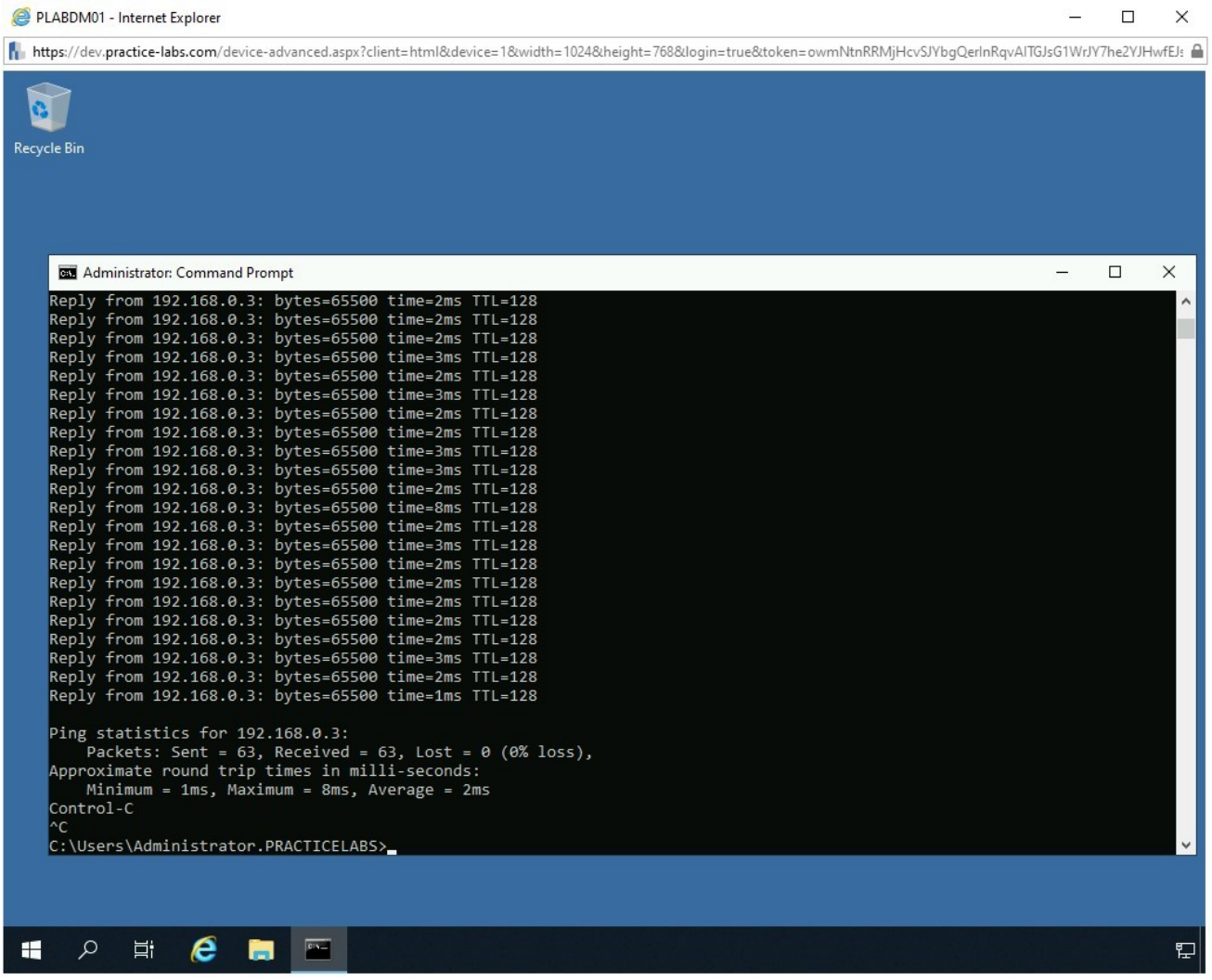


Figure 1.59 Screenshot of PLABDM01: Terminating the ping command.

Close the **command prompt** window.

Step 12

Switch back to **PLABWIN10**. Notice that the network activity has reduced greatly.

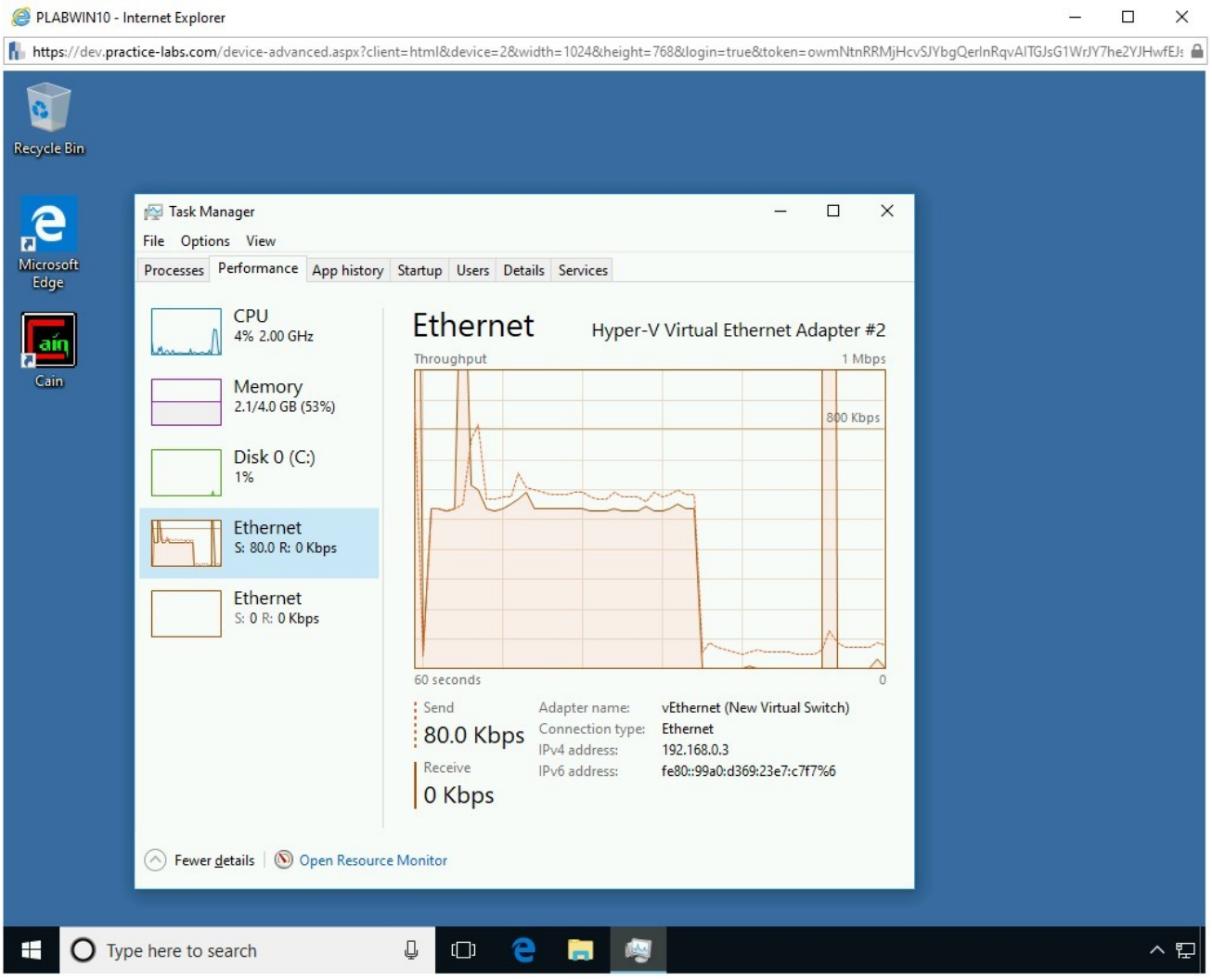


Figure 1.60 Screenshot of PLABWIN10: Showing the decreased network activity.

Close the **Task Manager** window.

Task 6 - Perform an SYN Floor Attack Using Metasploit Framework

Along with other types of attacks, you can also use the Metasploit Framework to perform a SYN attack on a target system. In this task, you will learn to perform a DoS attack using the Metasploit Framework. To do this, perform the following steps:

Step 1

Ensure that you have logged into the **PLABKALI01** system.

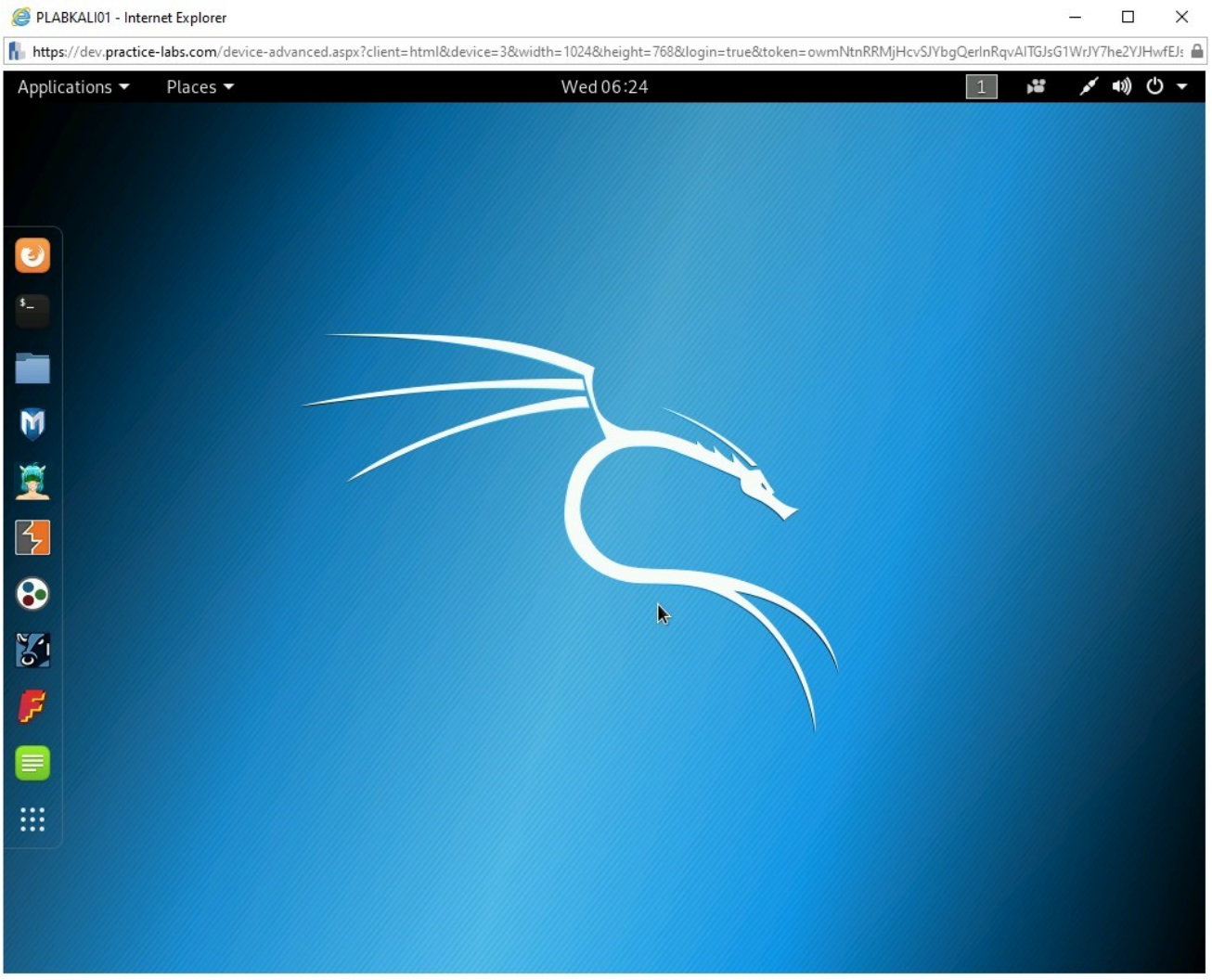


Figure 1.61 Screenshot of PLABKALI01: Showing the desktop of PLABKALI01.

Step 2

On the desktop, in the left pane, click the **Metasploit framework** icon.

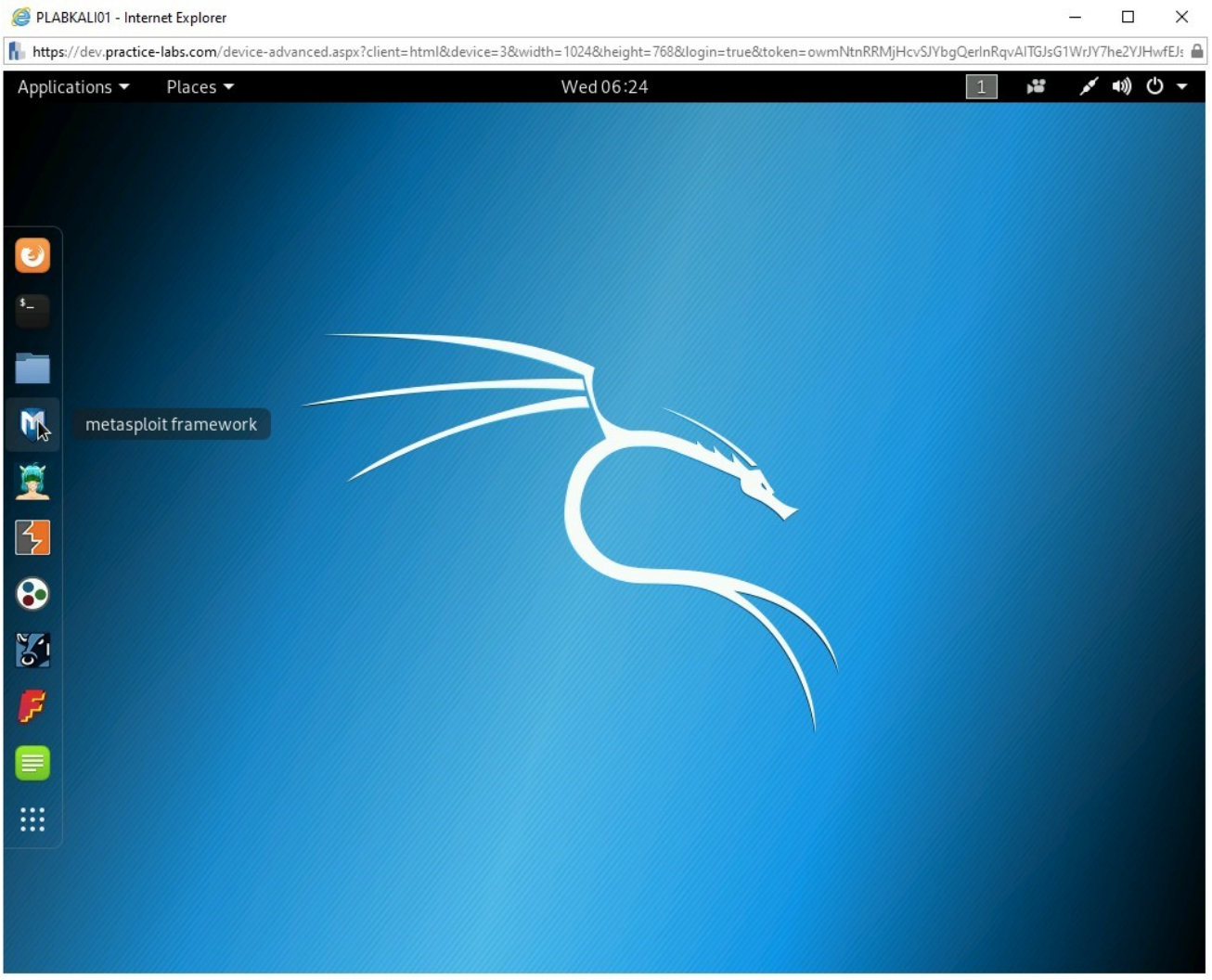
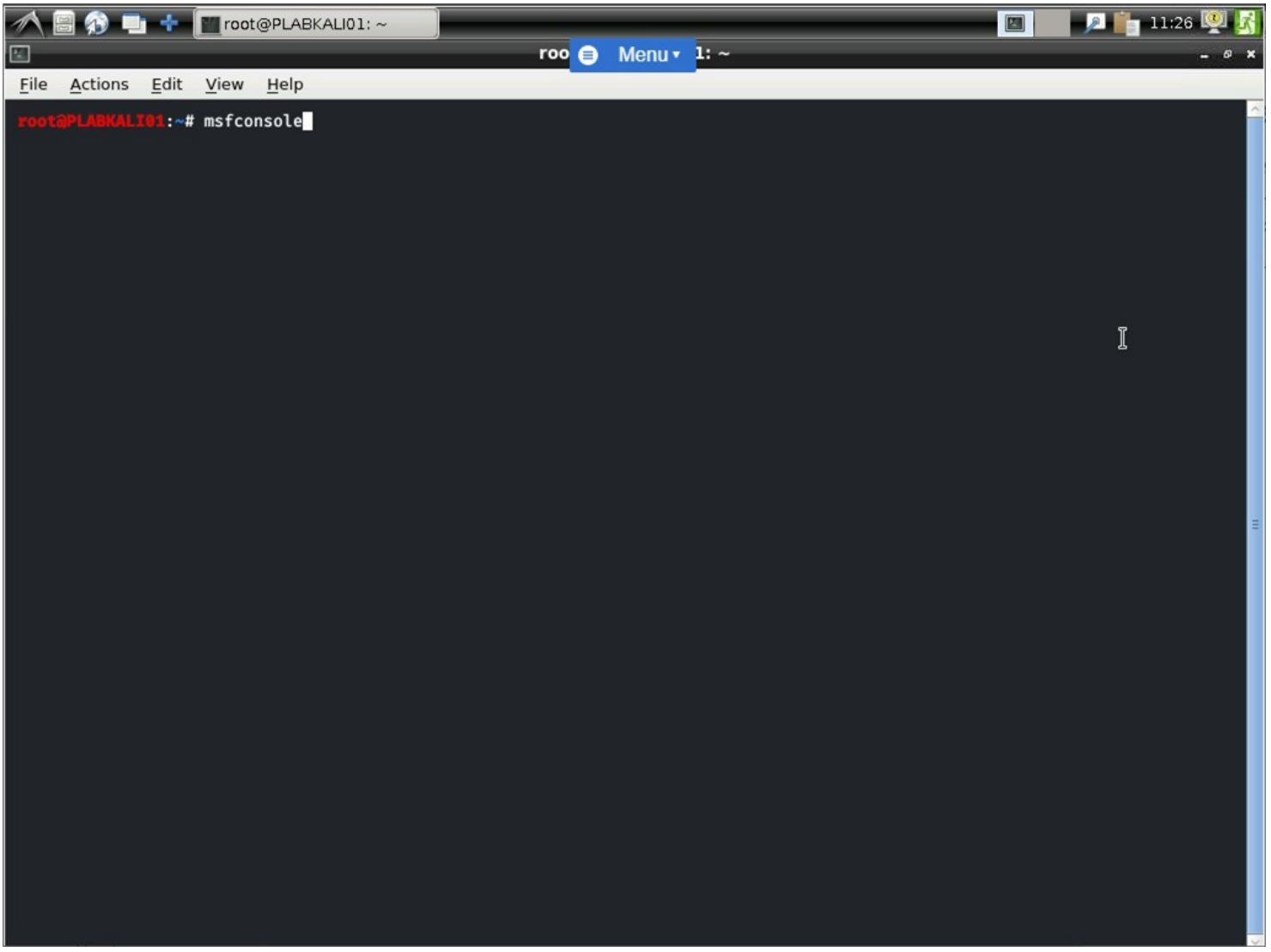


Figure 1.62 Screenshot of PLABKALI01: Clicking the Metasploit framework icon in the left pane.

Step 3

The terminal window is displayed. Type in

```
msfconsole
```



Step 4

The **metasploit framework** has started now.

> ***Note:*** *The number of exploits and payloads will change from time to time.*

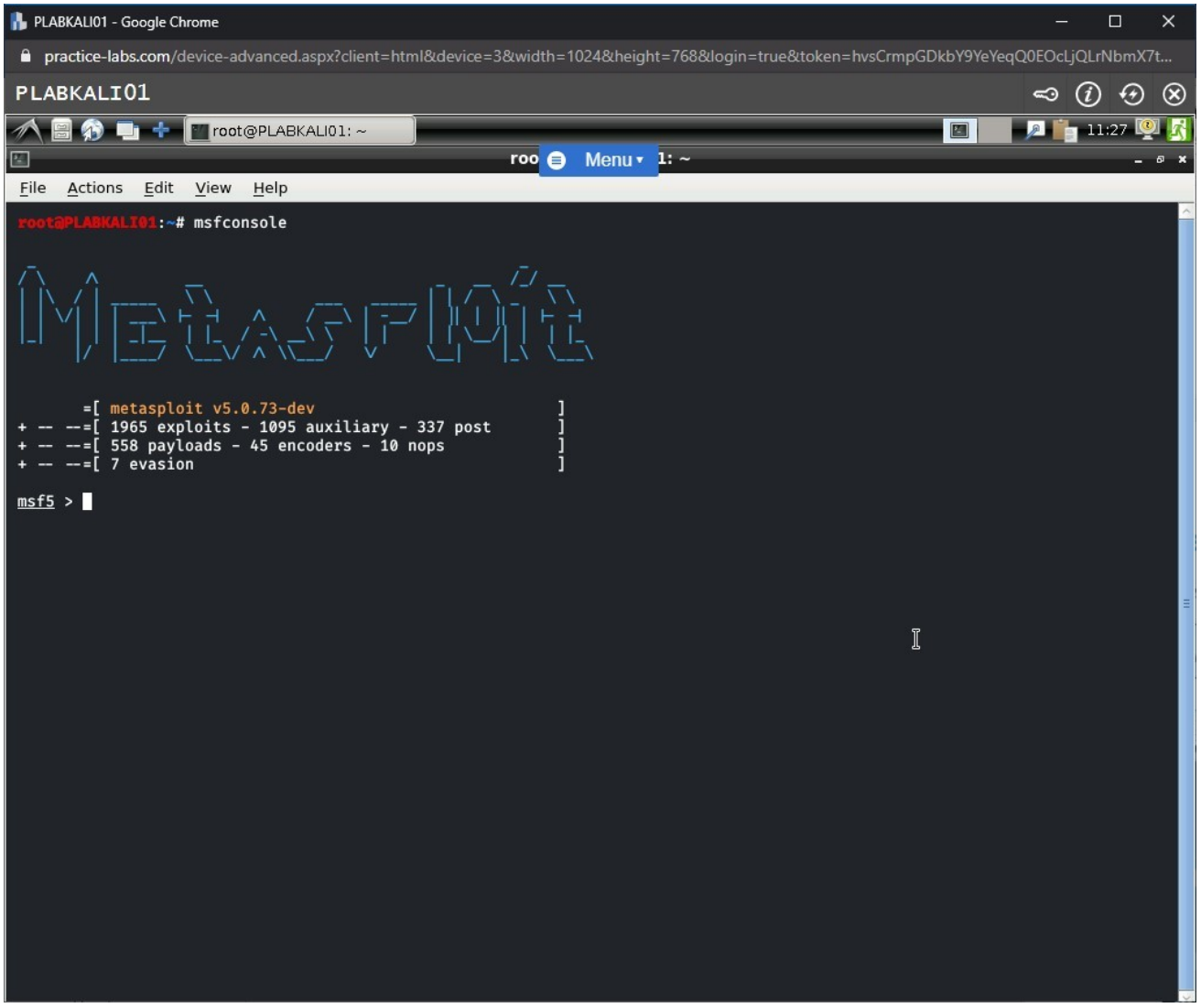


Figure 1.64 Screenshot of PLABKALI01: Showing the msf5 prompt after the Metasploit framework starts.

Step 5

You will now use the **synflood** module to target the **PLABWIN10** system. To do this, type the following command:

```
use auxiliary/dos/tcp/synflood
```

Press **Enter**.

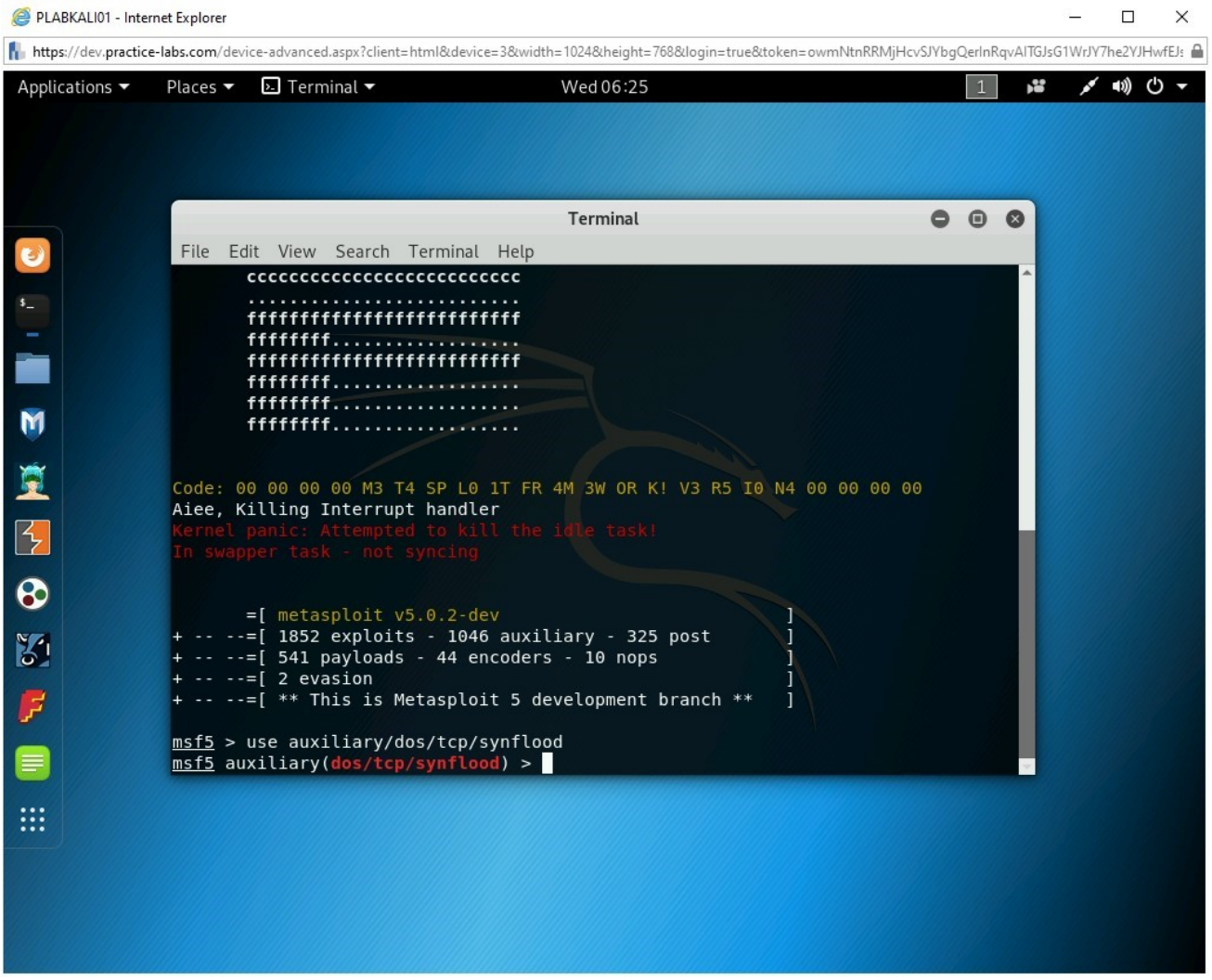


Figure 1.65 Screenshot of PLABKALI01: Entering the command to use the synflood module.

Step 6

Now, set the target system. Type the following command:

```
set RHOST 192.168.0.3
```

Press **Enter**.

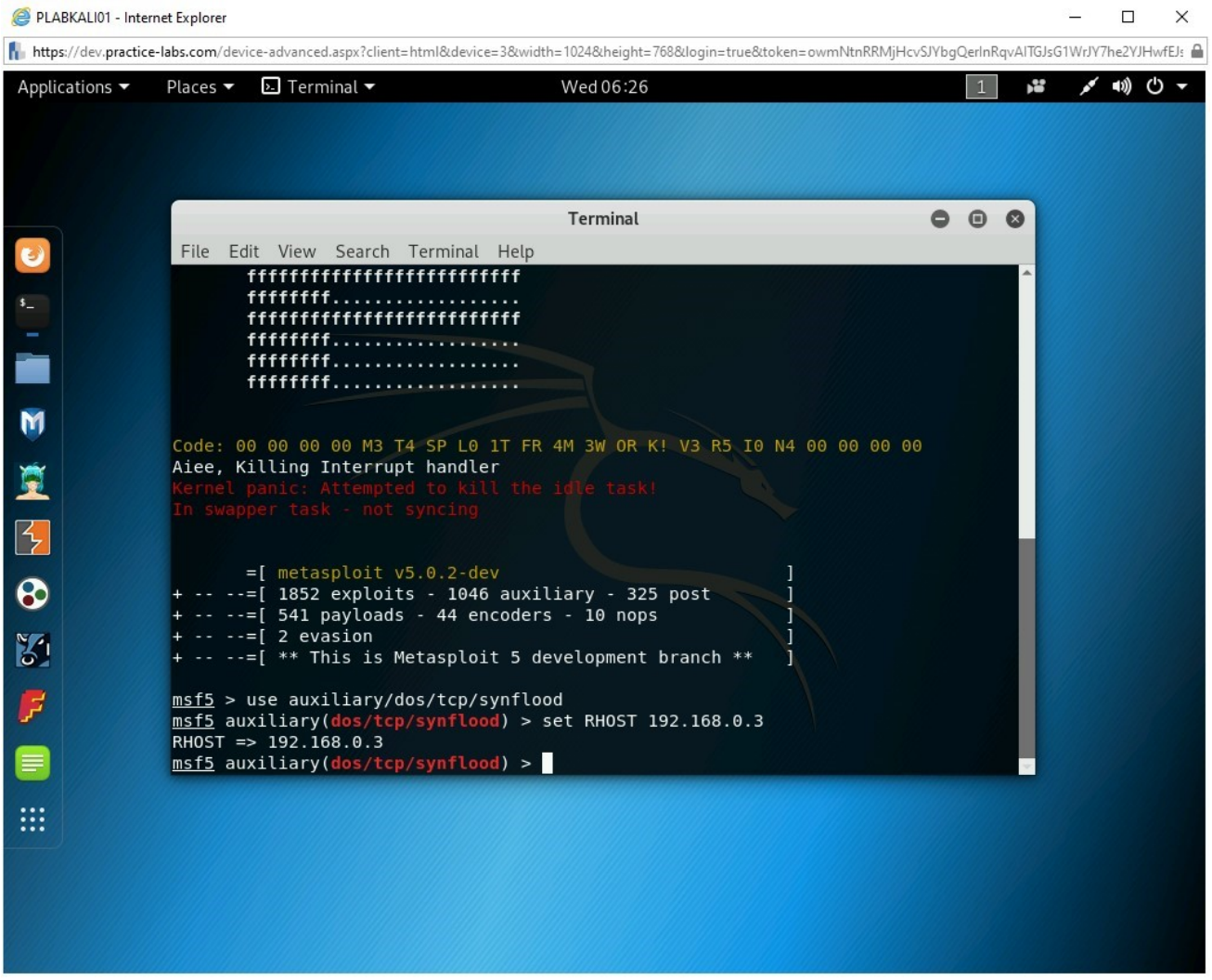


Figure 1.66 Screenshot of PLABKALI01: Setting the RHOST value.

Step 7

To configure the port, type the following command:

```
set RPORT 21
```

Press **Enter**.

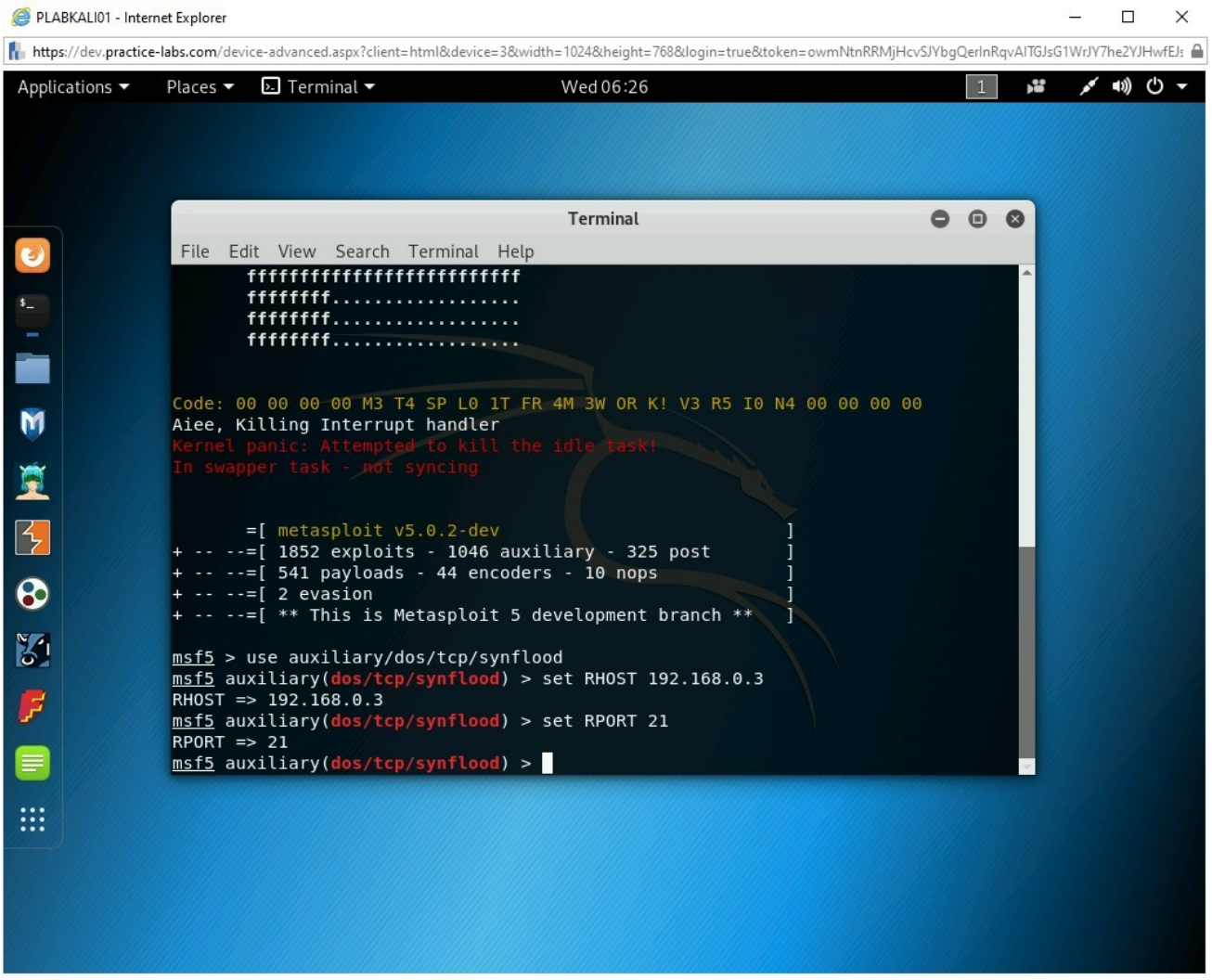


Figure 1.67 Screenshot of PLABKALI01: Setting the RPORT value.

Step 8

To set the spoofed IP address, type the following command:

```
set SHOST 192.168.0.10
```

Press **Enter**.

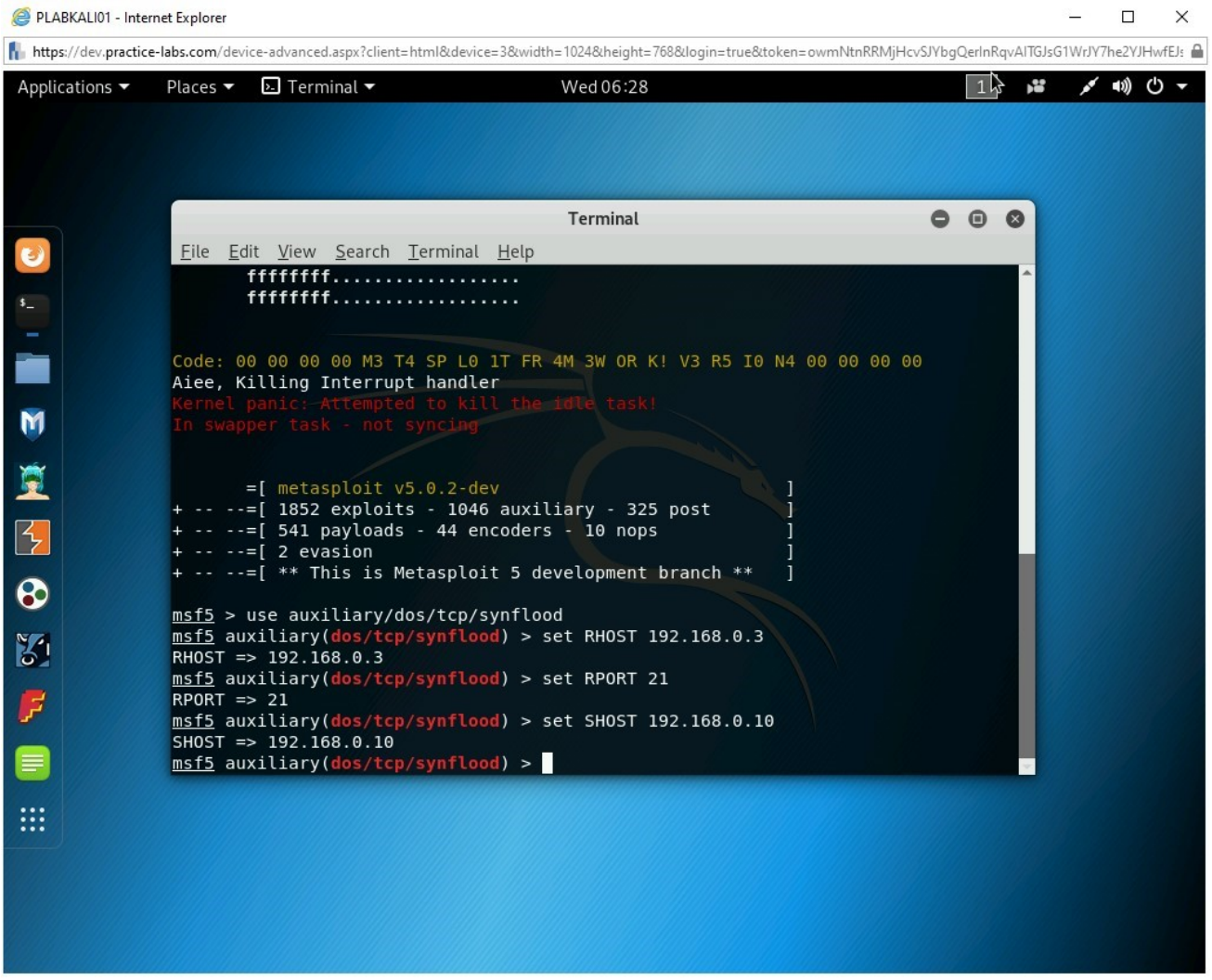


Figure 1.68 Screenshot of PLABKALI01: Setting the SHOST value.

Step 9

To set the timeout, type the following command:

```
set TIMEOUT 50000
```

Press **Enter**.

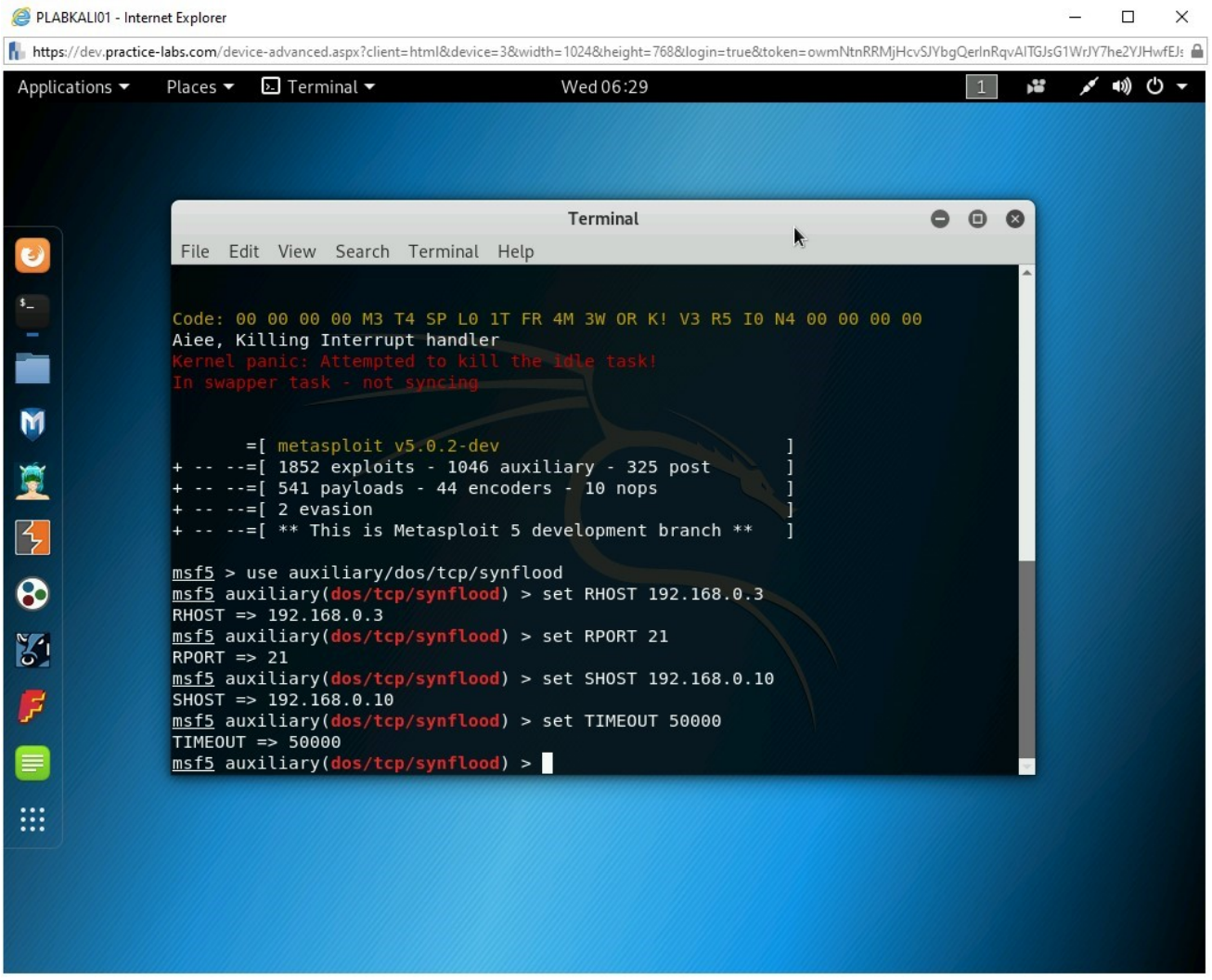


Figure 1.69 Screenshot of PLABKALI01: Setting the TIMEOUT value.

Step 10

To trigger the module, type the following command:

```
exploit
```

Press **Enter**.

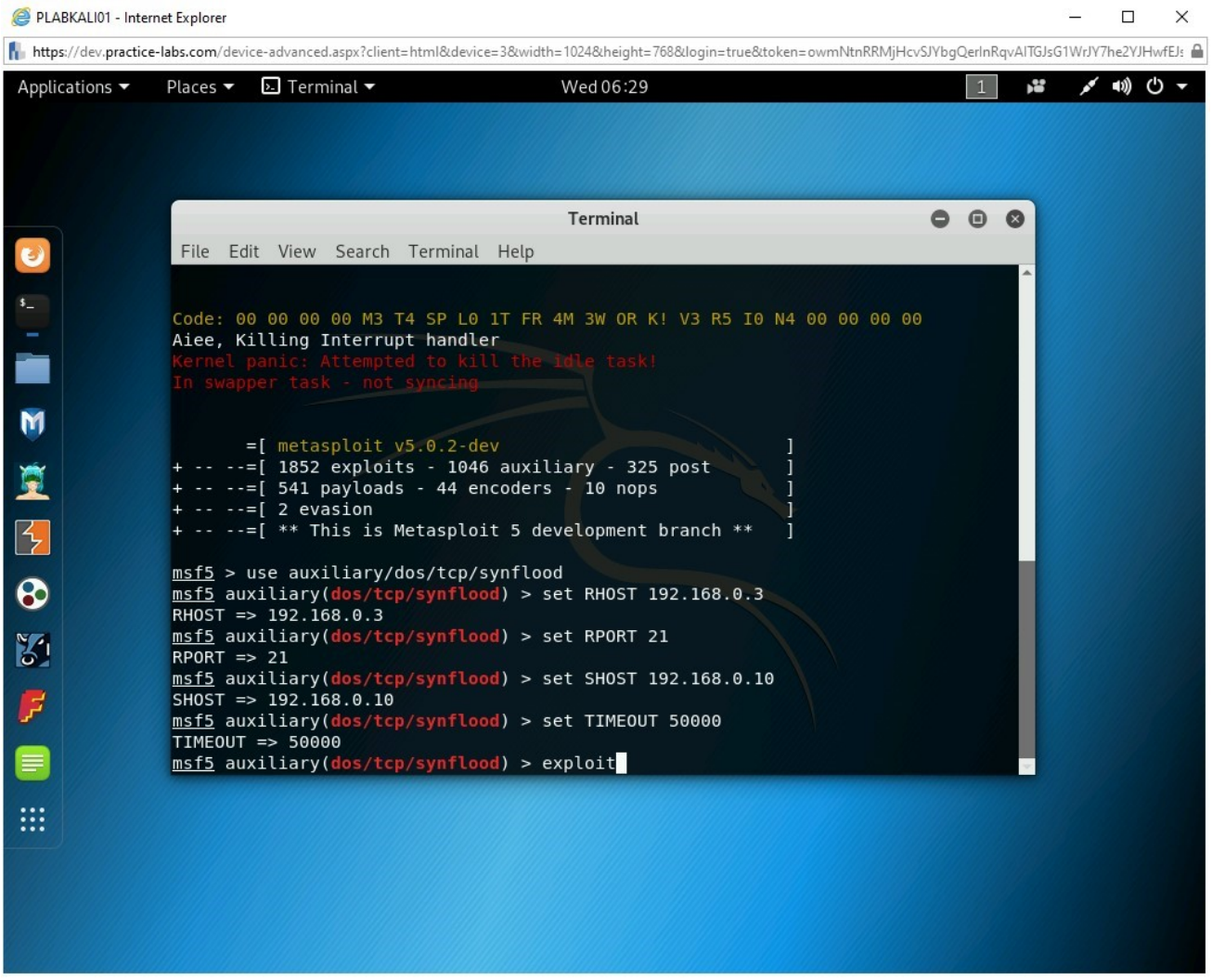


Figure 1.70 Screenshot of PLABKALI01: Entering the exploit command.

Step 11

The **SYN** flood attack starts.

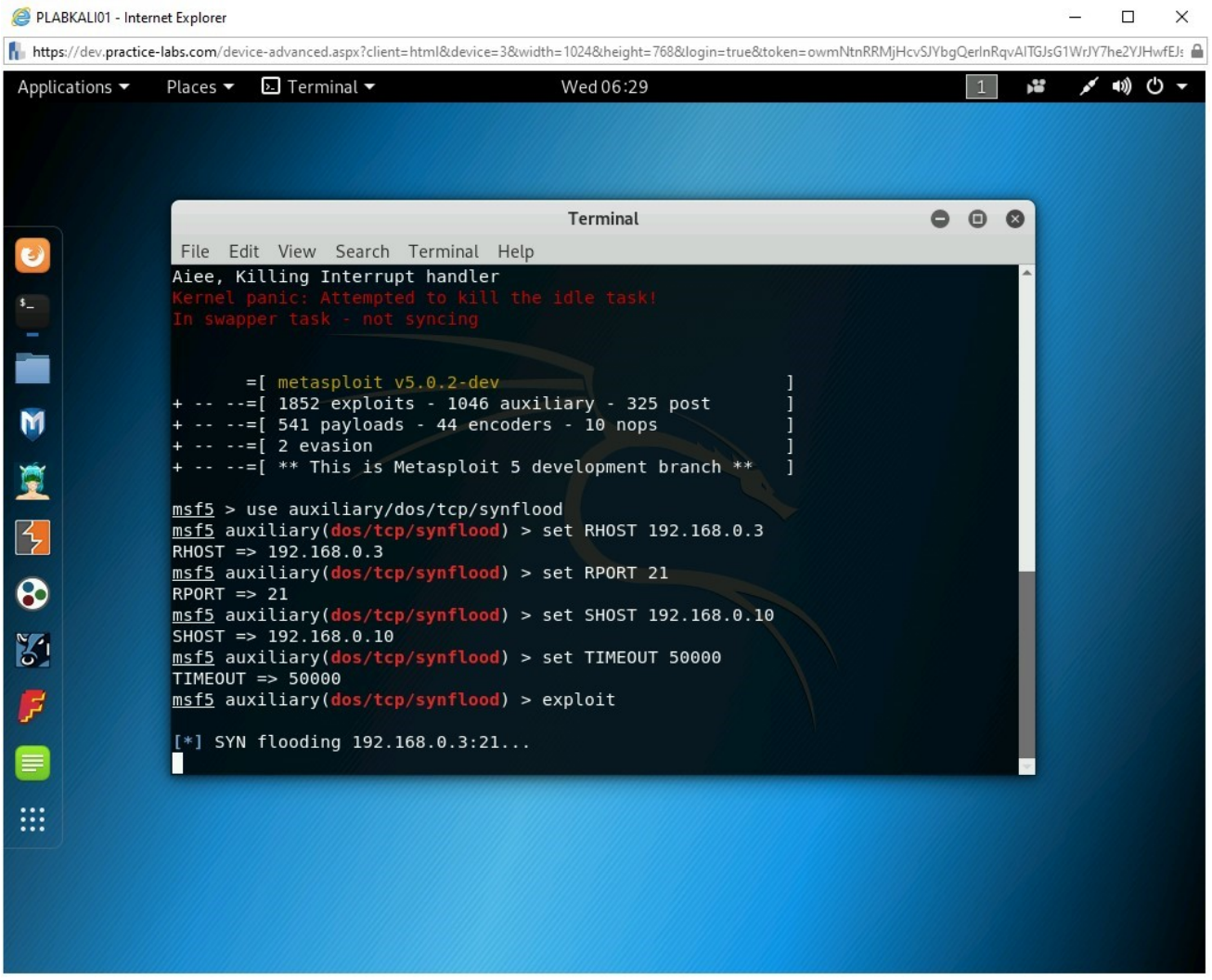


Figure 1.71 Screenshot of PLABKALI01: Showing the SYN flood attack in progress.

Step 12

Switch to **PLABWIN10**. You should be on the desktop. Right-click the taskbar and select **Task Manager**.

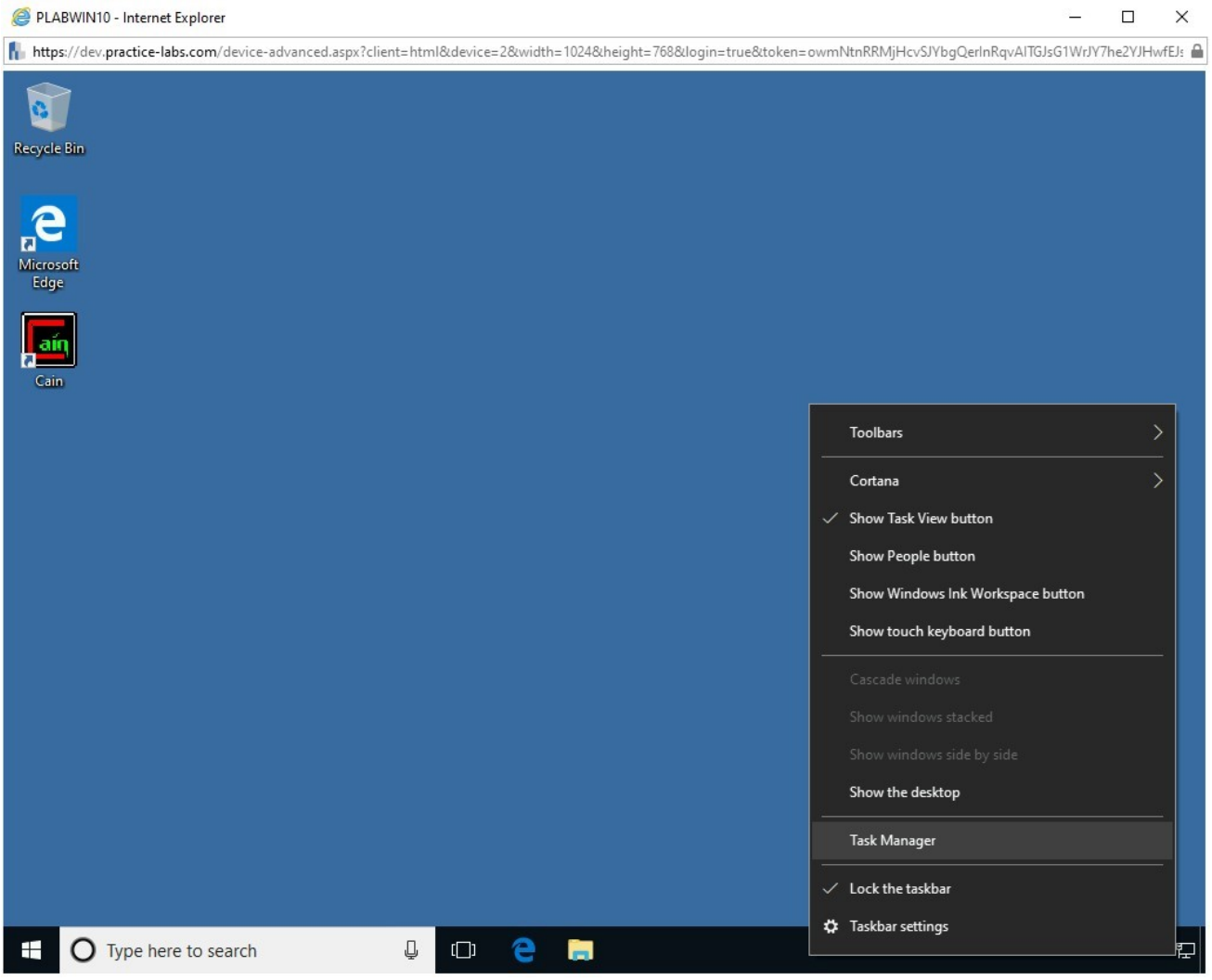


Figure 1.72 Screenshot of PLABWIN10: Right-clicking the taskbar and selecting Task Manager.

Step 13

Notice that multiple tabs in the **Task Manager** window appear. Click the **Performance** tab.

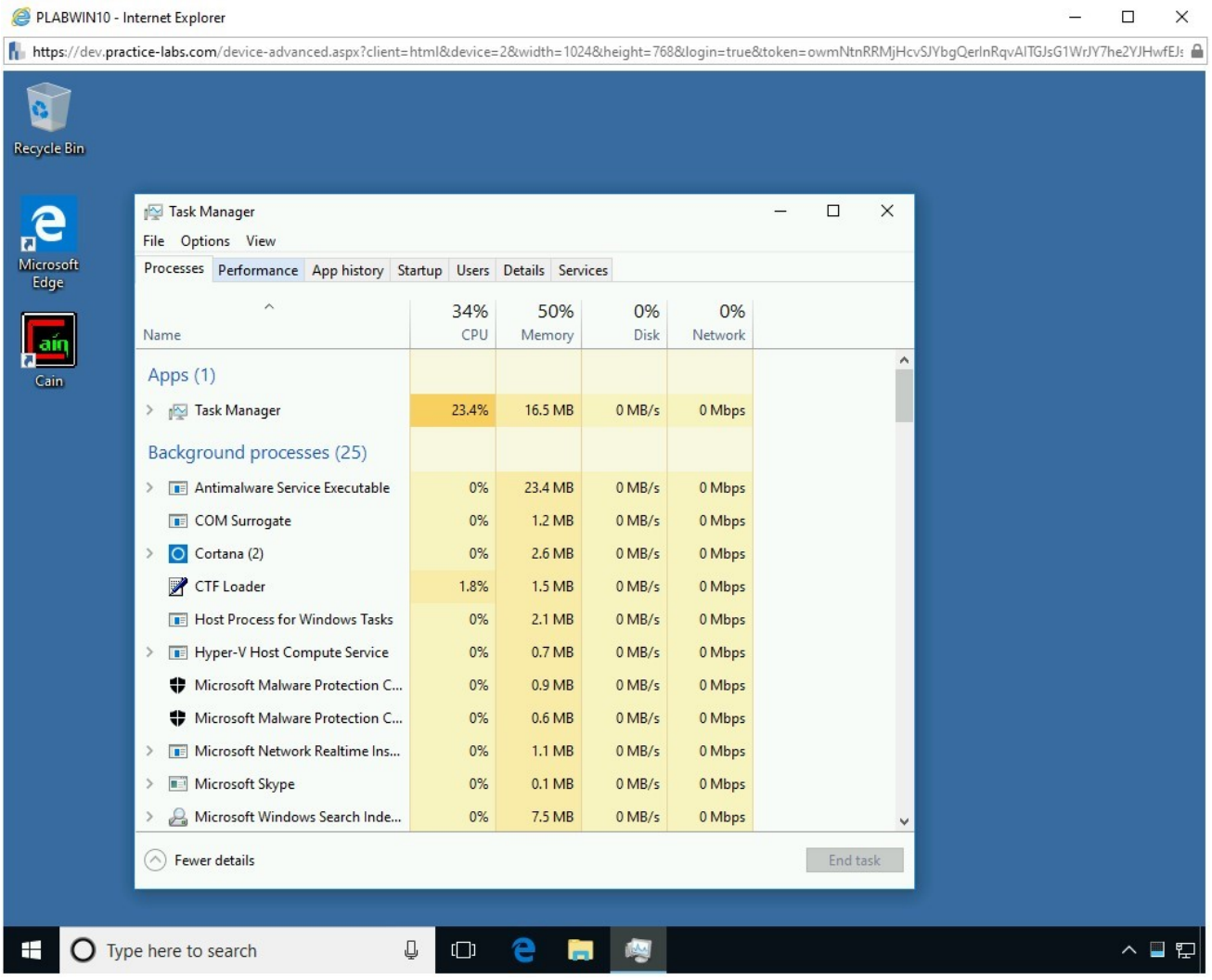


Figure 1.73 Screenshot of PLABWIN10: Clicking the Performance tab in Task Manager.

Step 14

On the **Performance** tab, CPU is selected by default. Click **Ethernet**.

> ***Note: Ethernet*** *might already be selected as it was selected in Task 5.*

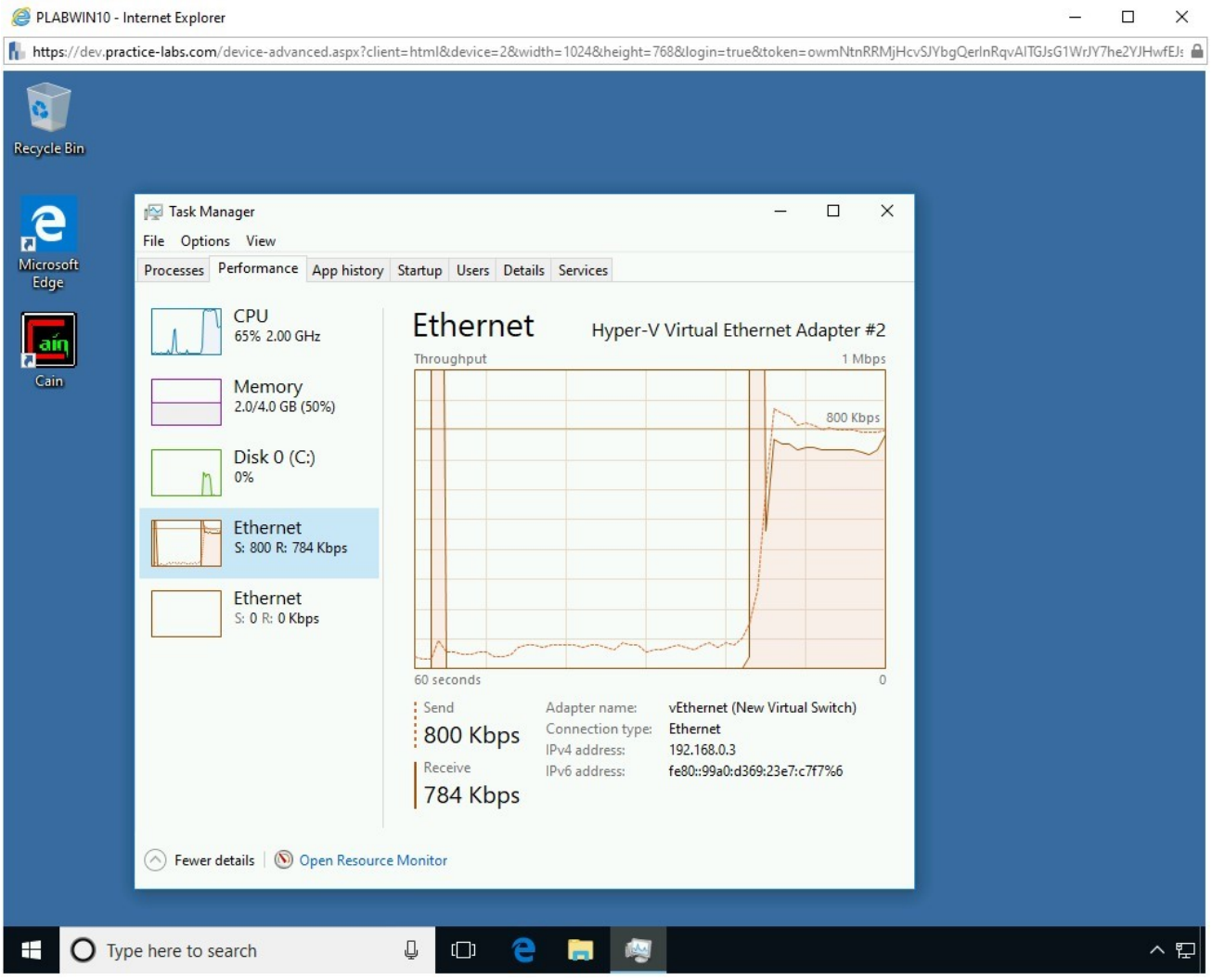


Figure 1.74 Screenshot of PLABWIN10: Clicking Ethernet on the Performance tab in Task Manager.

Step 15

Notice that there is an increased network activity on the **PLABWIN10** system.

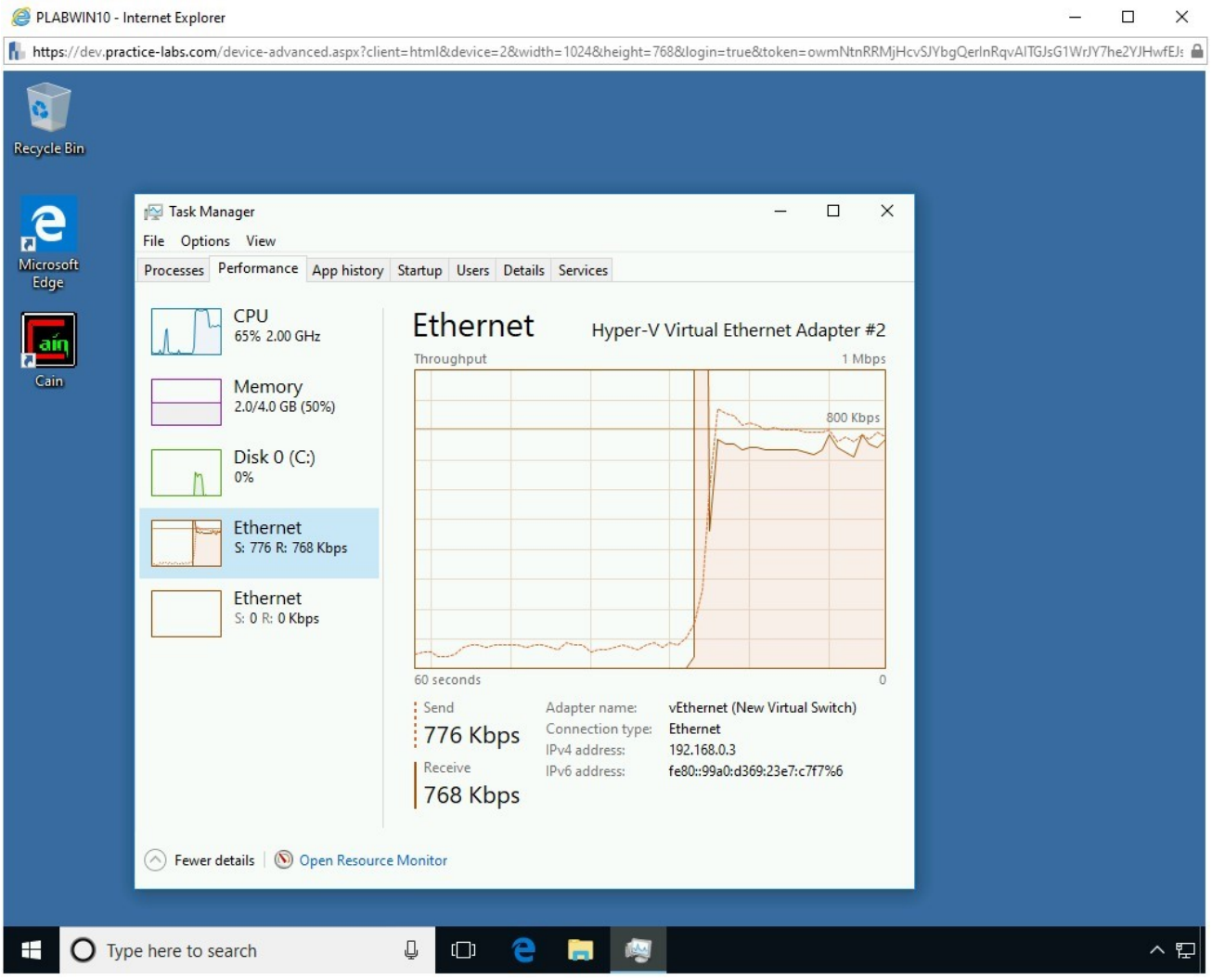


Figure 1.75 Screenshot of PLABWIN10: Showing the increased network traffic on the Performance tab.

Step 16

Switch back to **PLABKALI01**. Press **Ctrl + C** to terminate the SYN flood attack.

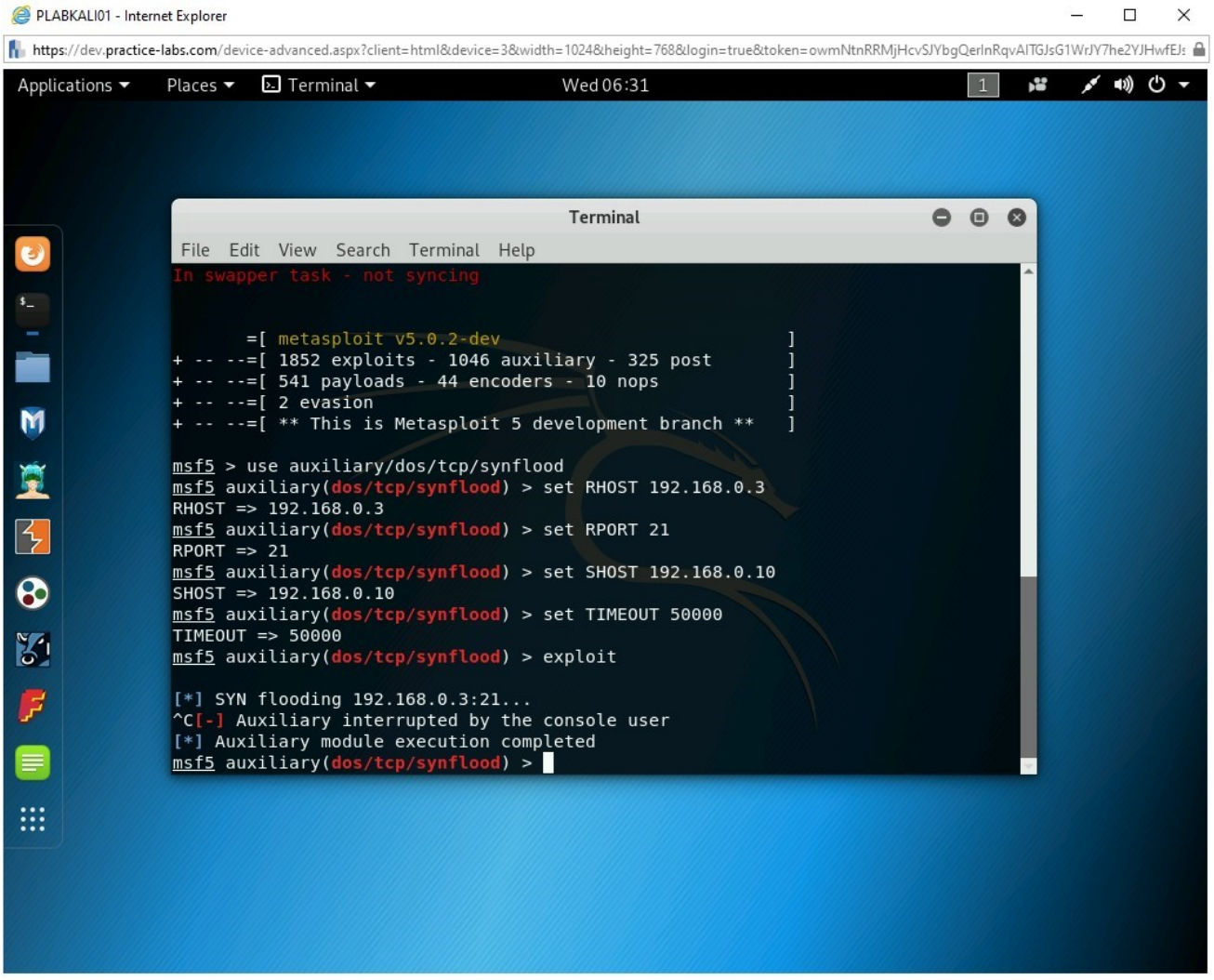


Figure 1.76 Screenshot of PLABKALI01: Terminating the SYN flood attack.

Close the **terminal** window.

Exercise 2 - Know About DoS/DDoS Prevention

When a system is attacked with a DoS or DDoS attack, the symptoms are usually visible. For example, some of the symptoms can be:

- Extremely slow performance
- Unavailability of system resources
- Network utilization extremely high

There are a few methods that can be used to prevent DoS/DDoS attacks. In this exercise, you will learn about the DoS/DDoS prevention methods.

Learning Outcomes

After completing this exercise, you will be able to:

- Know about DoS/DDoS Prevention Methods

Your Devices

This exercise contains supporting materials for Certified Ethical Hacker v10.

Know about DoS/DDoS Prevention Methods

You need to first detect and then prevent the DoS/DDoS attacks. You can use some of the following methods:

Detection

Detection of unusual traffic can be done by using a simple packet capturing tool, such as Wireshark. The SYN flood can be detected and marked by the Wireshark tool. In the exhibit below, the SYN flood packets are clearly distinguished and marked.

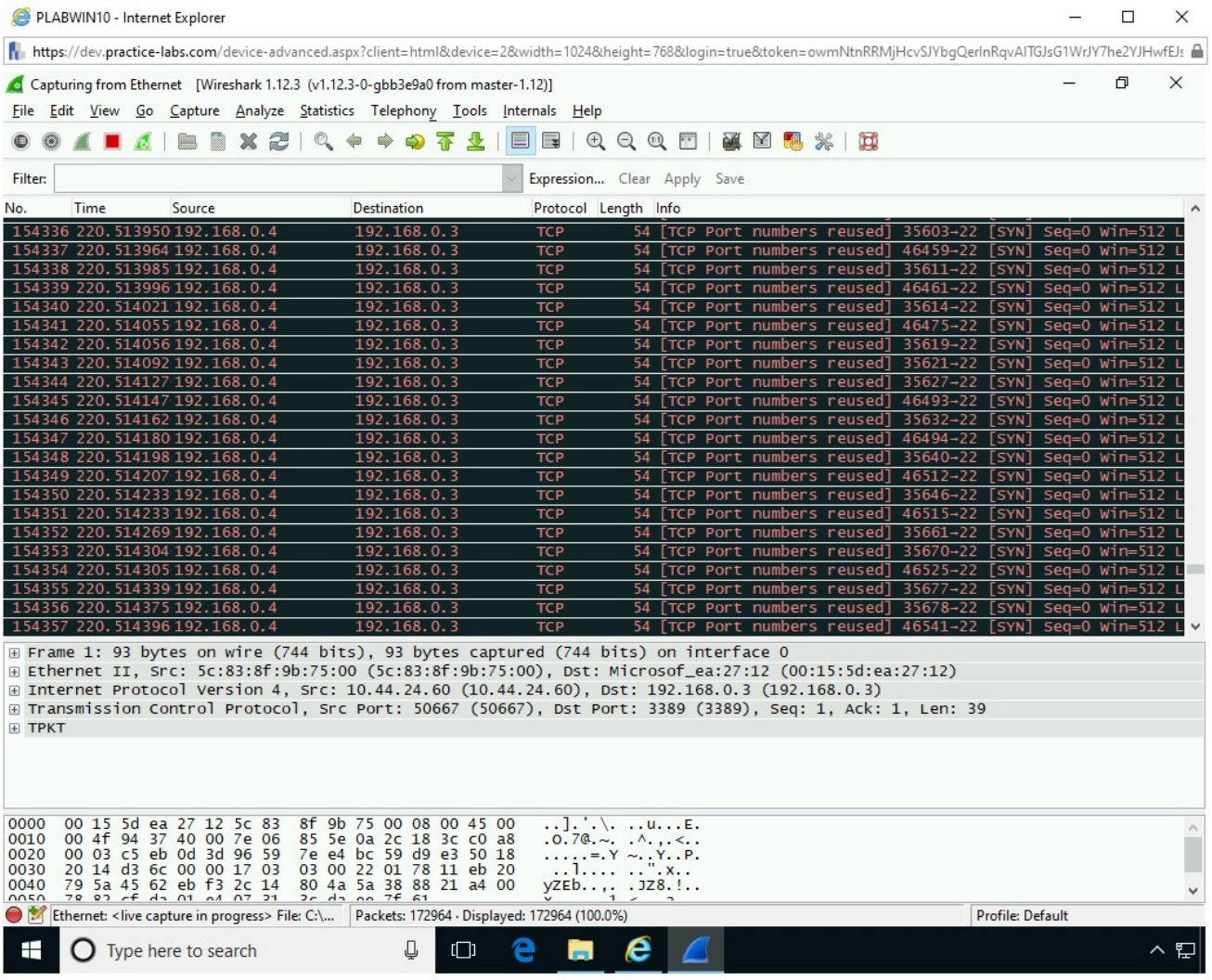


Figure 2.1 Screenshot of PLABWIN10: Showing the SYN flood attack in Wireshark.

There are other methods that can be used in detecting a DoS/DDoS attack. Some of these methods are:

Activity System and Network Profiling

You need to monitor what is happening on your system and network. You must monitor the traffic flow using a tool such as Wireshark and observe for the data packets. In the activity profiling, you need to benchmark the network traffic with the average network traffic that exists on the network at any given point of time.

Wavelet Analysis

Using this method, you observe the volume-based anomalies. Using an adaptive filtering method, it will filter any large volume of traffic.

Sequential Change-Point Detection

This method observes the traffic patterns to detect the DoS/DDoS attacks.

Prevention

You can use various methods to prevent your infrastructure from DoS/DDoS attacks. Some of these methods are:

- Use a firewall to filter incoming traffic
- Use anti-malware on systems and servers
- Have ample bandwidth available
- Use WAF for Web application protection
- Enable router throttling
- Disable unnecessary services
- Filter unwanted E-mails
- Use reverse proxy
- Monitor and audit servers and network regularly

This is not an exhaustive list, but it can surely minimize the chances of a DoS or DDoS attack. For example, if you enable the firewall on a Windows system and attempt an ICMP attack, the firewall will block the ICMP packets. Most organizations prevent incoming ICMP packets to protect themselves from the Dos or DDoS attacks.

Review

Well done, you have completed the **Denial of Service** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Perform Denial-of-Service (DoS) Attacks
- Exercise 2 - Know About DoS/DDoS Prevention

You should now be able to:

- Install Wireshark
- Perform SYN Flooding Attack
- Switch Off the Windows Firewall on PLABWIN10
- Perform an ICMP Flood Attack
- Perform the Ping of Death Attack
- Perform an SYN Floor Attack Using Metasploit Framework
- Know about DoS/DDoS Prevention Methods

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.