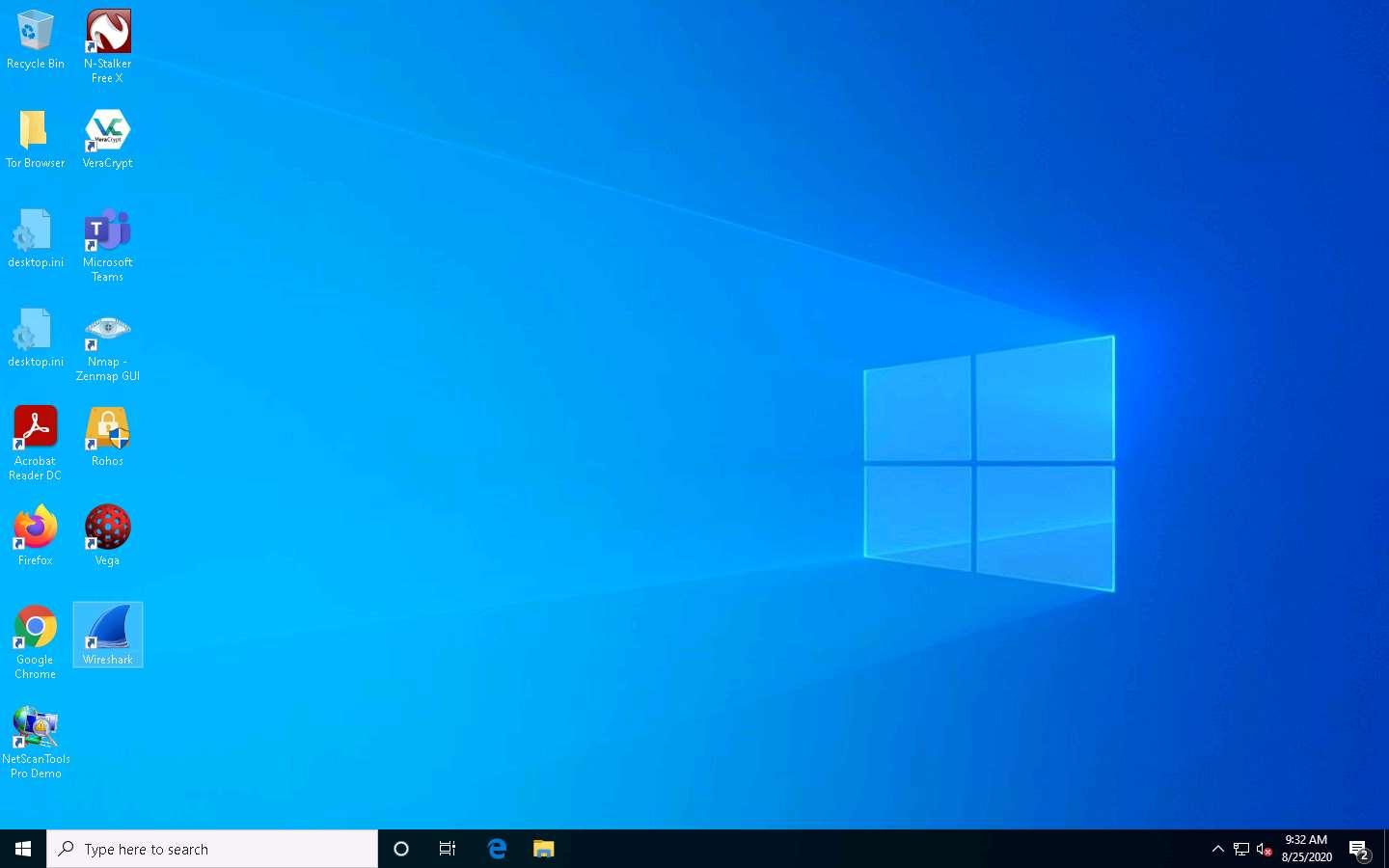
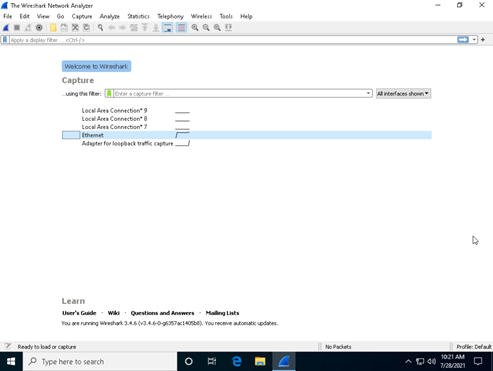
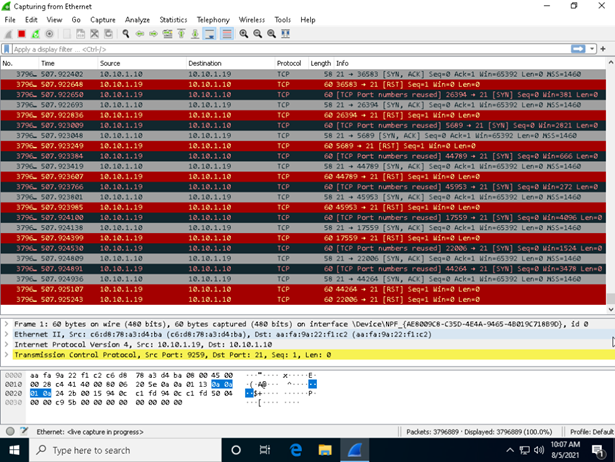
1. On the **Windows 10** machine, double-click **Wireshark** shortcut present on the **Desktop**.



Step2: **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.



Step3: **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.

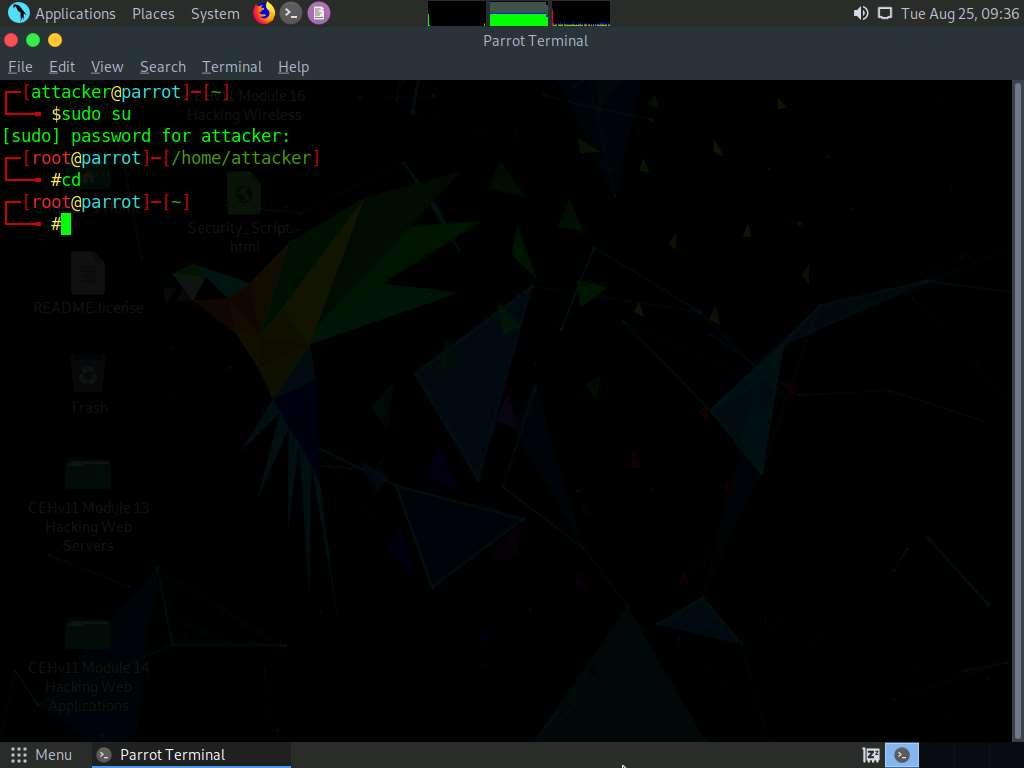


Step4:

1. The **terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
2. 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.

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



Step5: Hping 3 -s 10.10.1.10 -a 10.10.1.19 -p 22 - -



Step7:

1. ou can observe **TCP-SYN** packets captured by **Wireshark**, as shown in the screenshot.

