Network Penetration Testing Methodology-Internal

6 Hr 39 Min Remaining

Instructions Resources Help  100%

Exercise 13: Performing Man-in-the-Middle Attack using Cain & Abel

Scenario

Unlike capturing network traffic in a hub-based network, it is not possible to capture traffic in a switch based network. Since most of the networks today are implemented on switch-based networks, it is not possible to capture traffic flowing between two hosts.

At this point, attackers implement techniques such as arp poisoning/MITM to capture clear-text traffic flowing between two machines in a network. MITM is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. MITM attacks come in many variations and can be carried out on a switched LAN. As a penetration tester, you need to know how to capture plain text traffic in a switch-based network.

In this lab, you will learn how to:

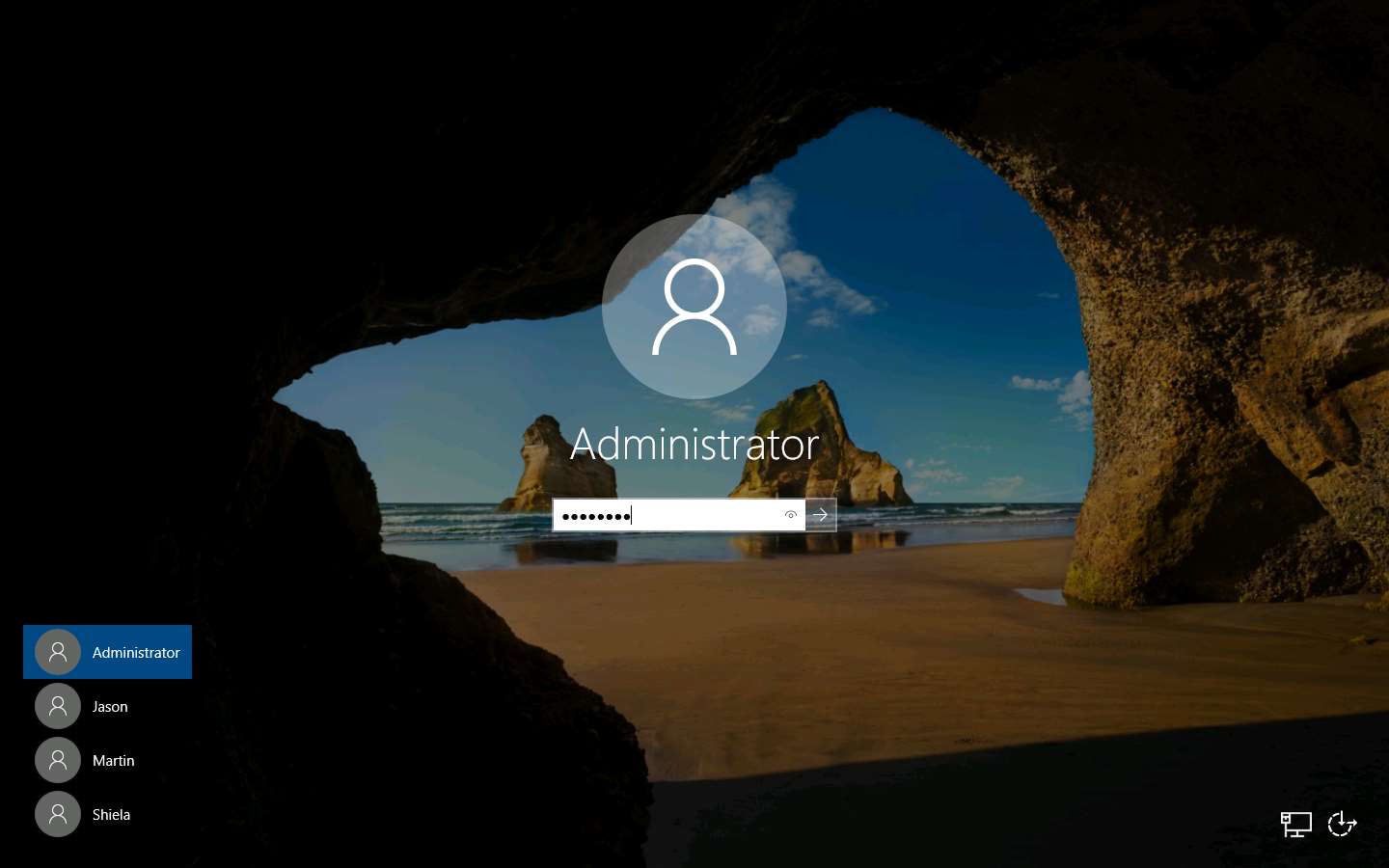
1. Perform ARP Poisoning
2. Launch a Man-in-the-Middle attack
3. Sniff a network for password

**Lab Duration**: **25** Minutes

1. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10) link and then click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10).



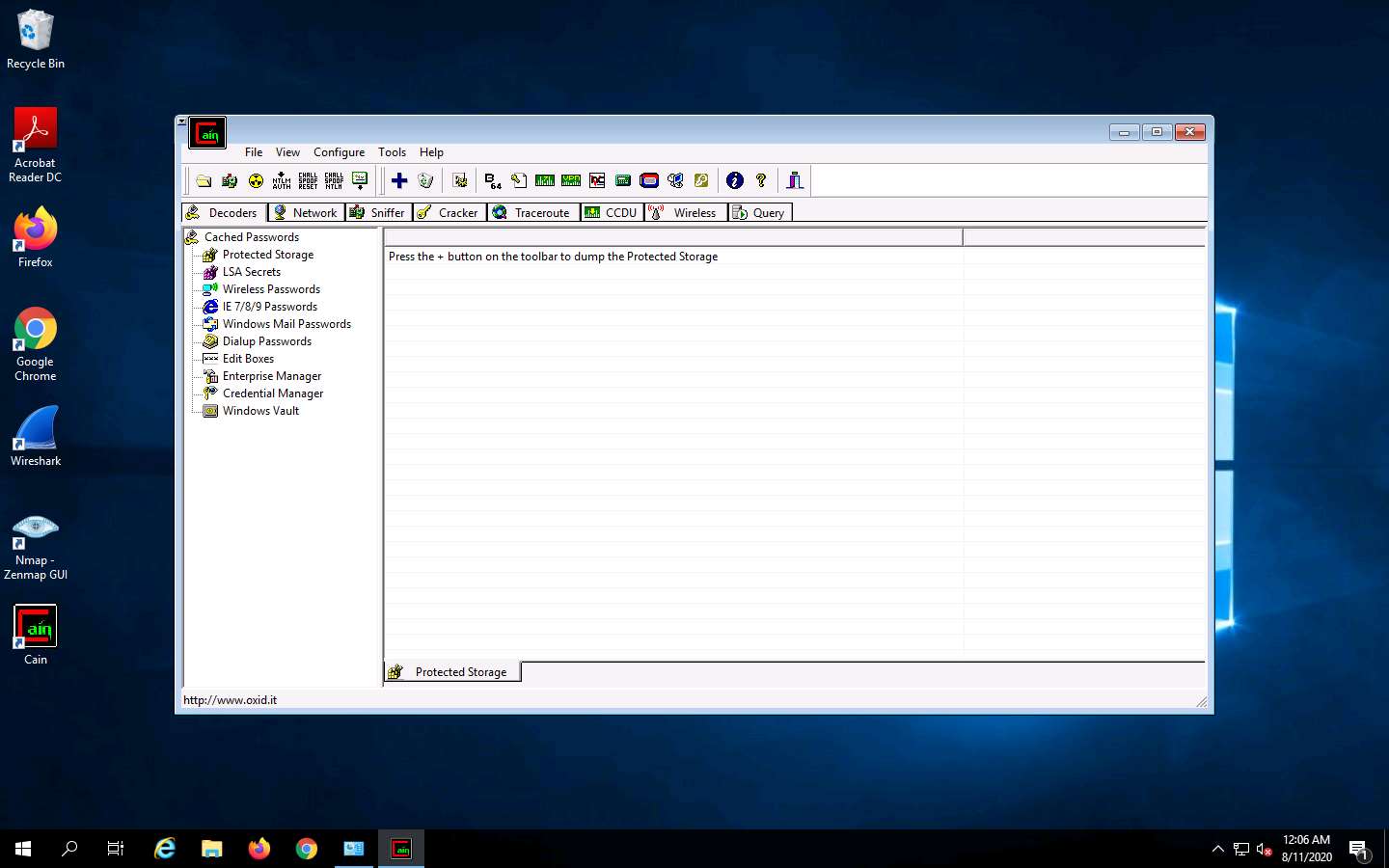
1. Click Pa$$w0rd and press **Enter** to login.



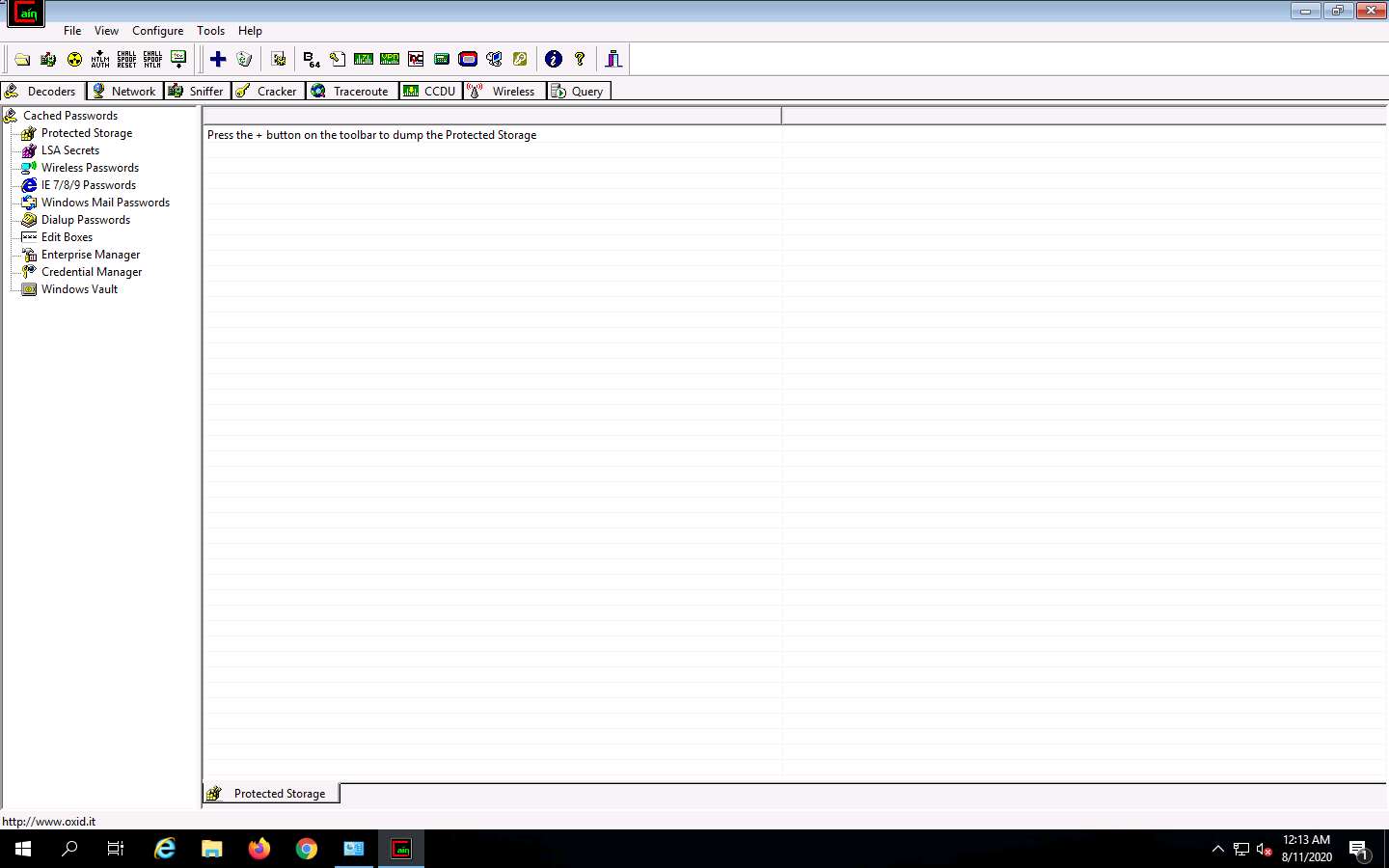
1. Launch Cain & Abel application by double-clicking the shortcut icon of **Cain** on the desktop.



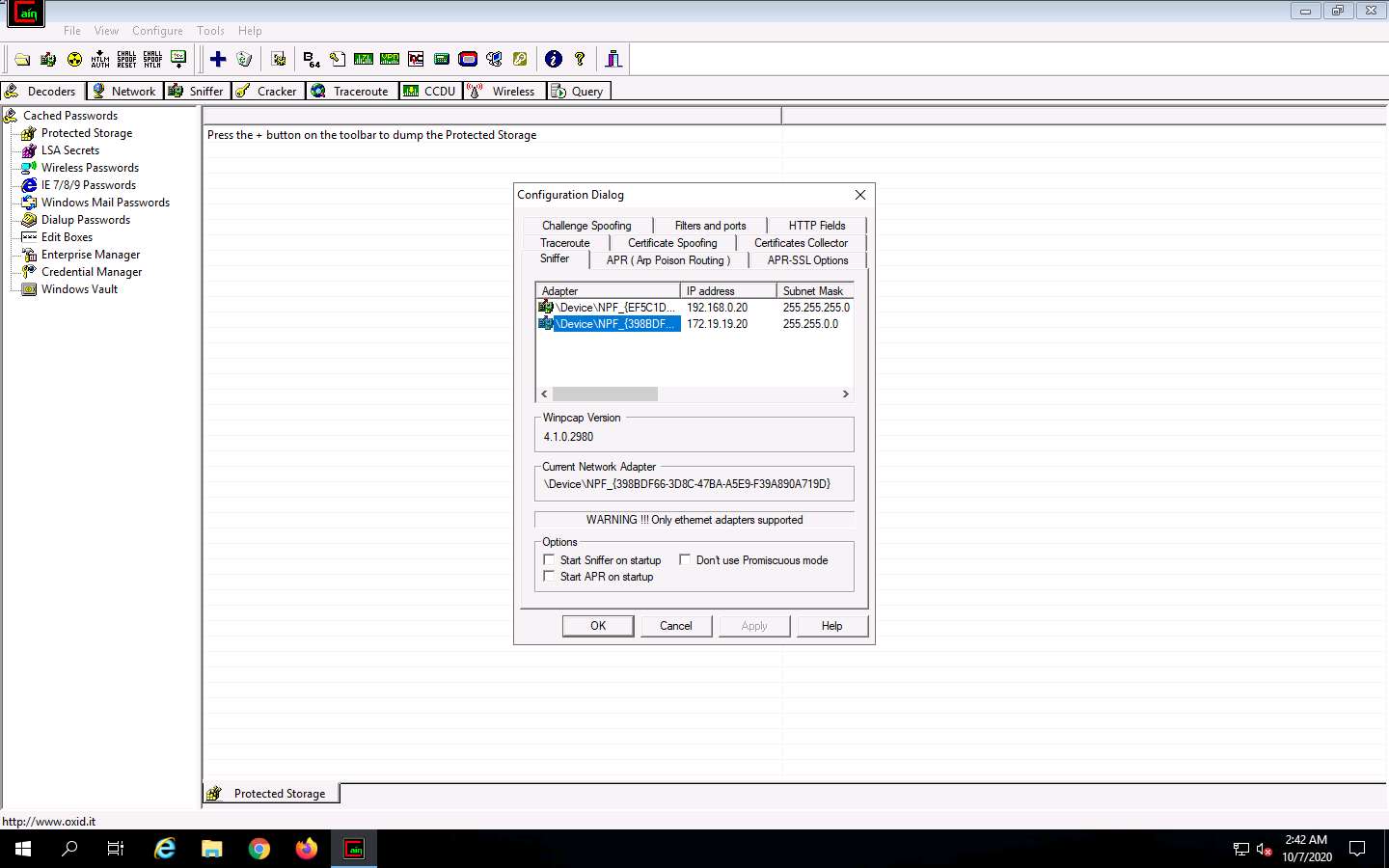
1. The main window of Cain & Abel appears as shown in the screenshot.



1. To configure the **Ethernet** card, click **Configure** from the menu bar.

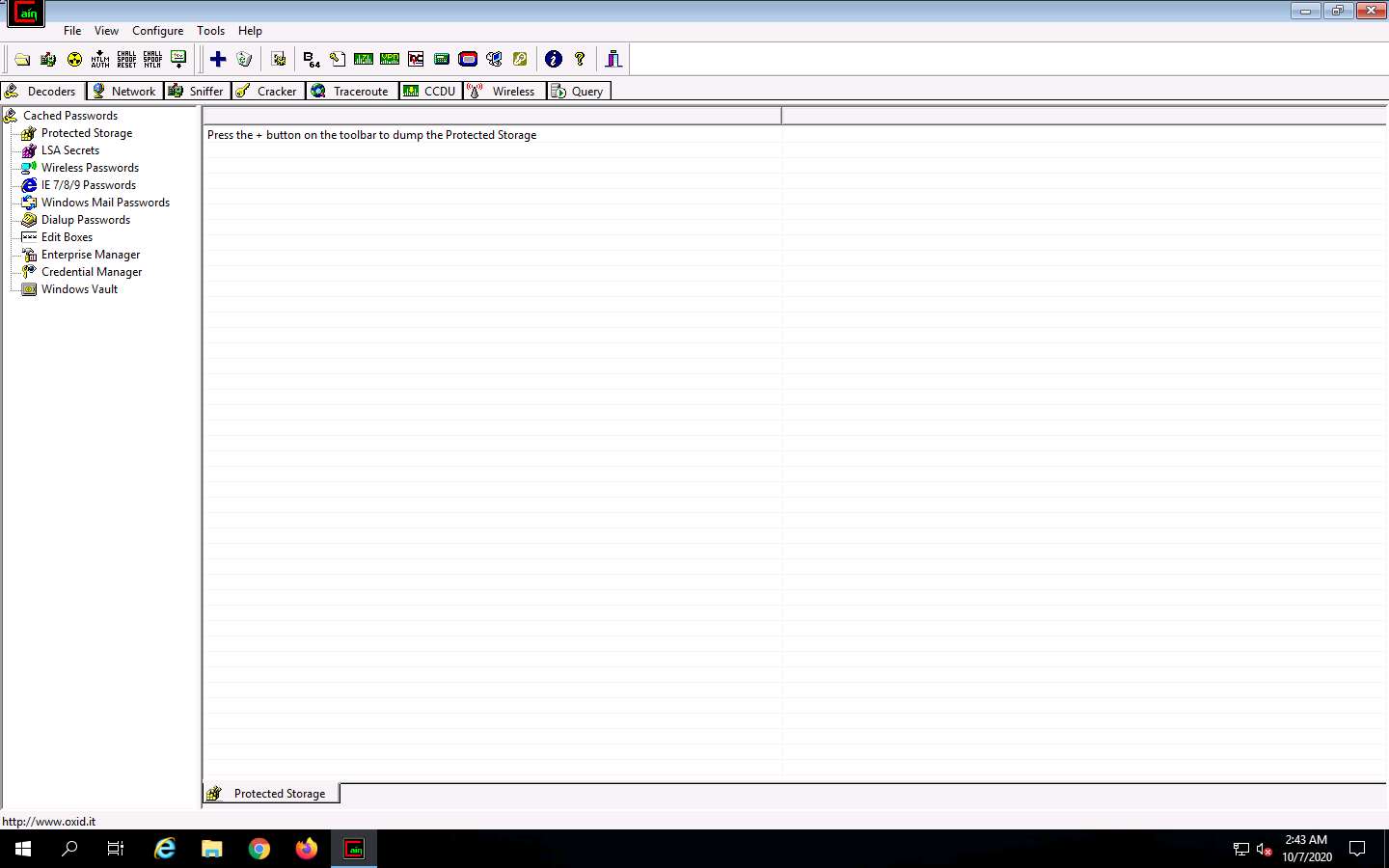


1. The **Configuration** Dialog window appears. The window consists of several tabs. Click **Sniffer** tab to select sniffing adapter. Select the Adapter associated with the IP address **172.19.19.20**, click **Apply** and **OK**.

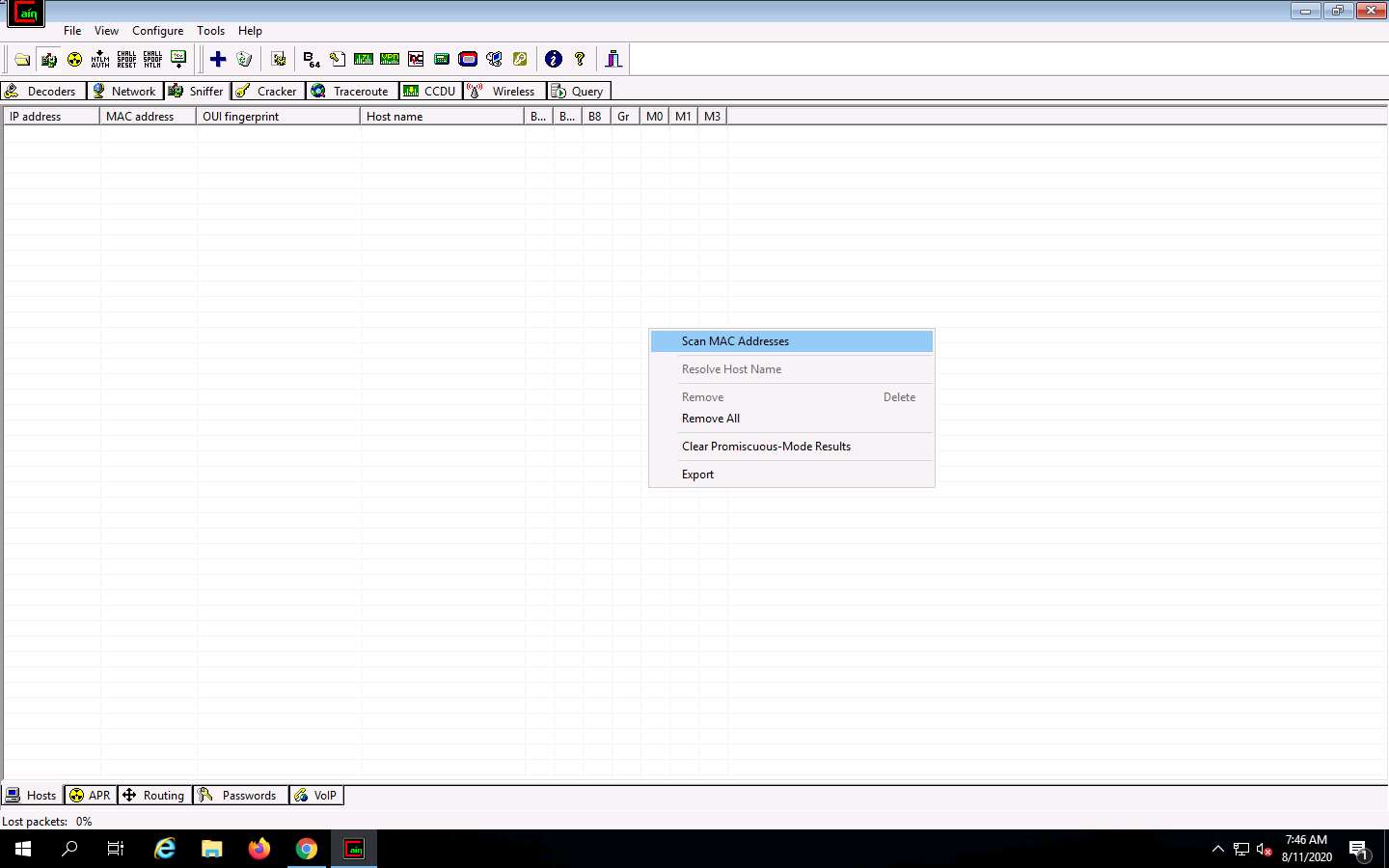


1. Click **Start/StopSniffer** (second icon from left) on the toolbar to begin sniffing.

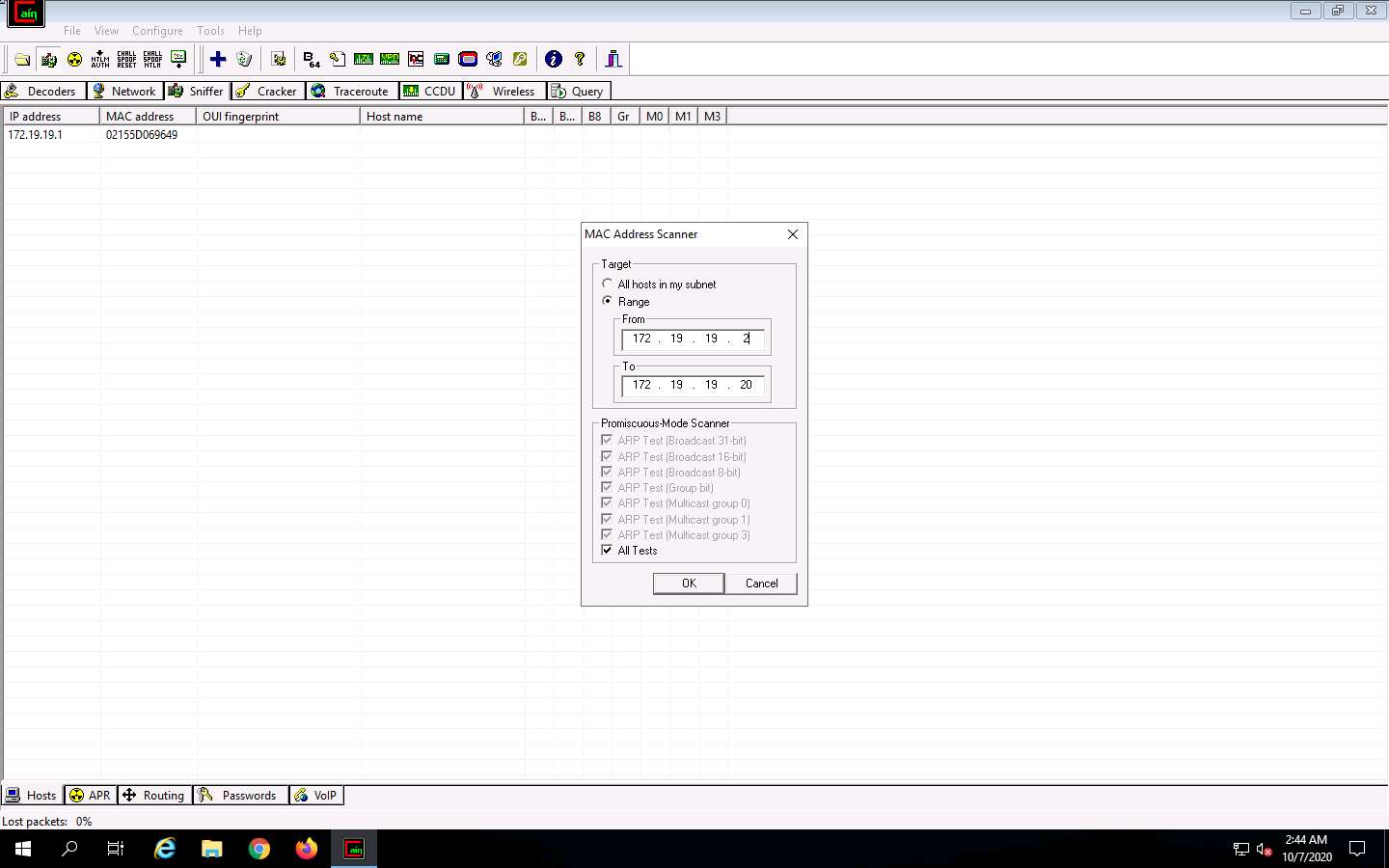
If a **Cain Warning** pop-up appears, click **OK**.



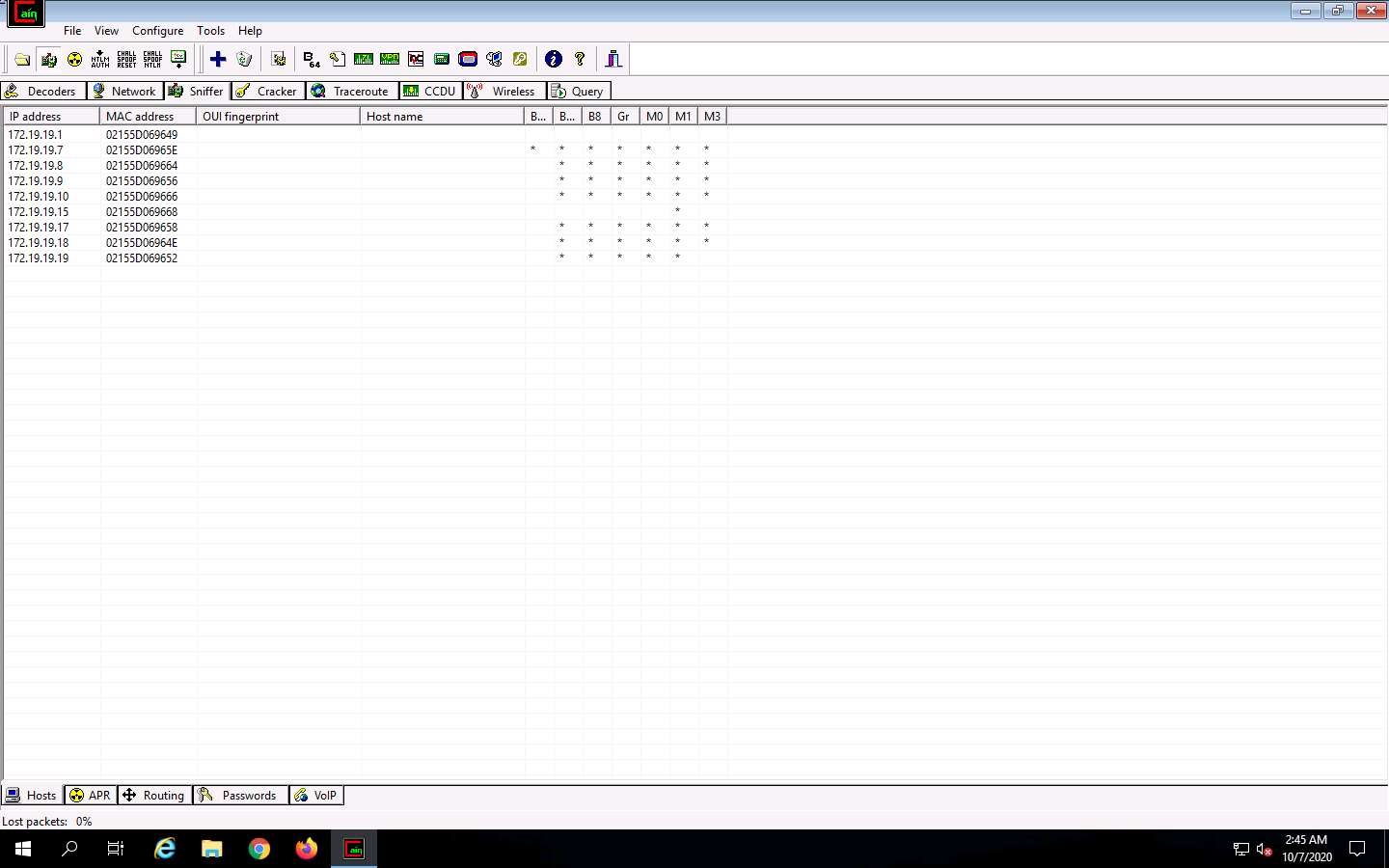
1. Now click the **Sniffer** tab and then, click the **Plus** (+) icon (or) right click in the window, and select **Scan MAC Addresses** to scan the network for hosts.



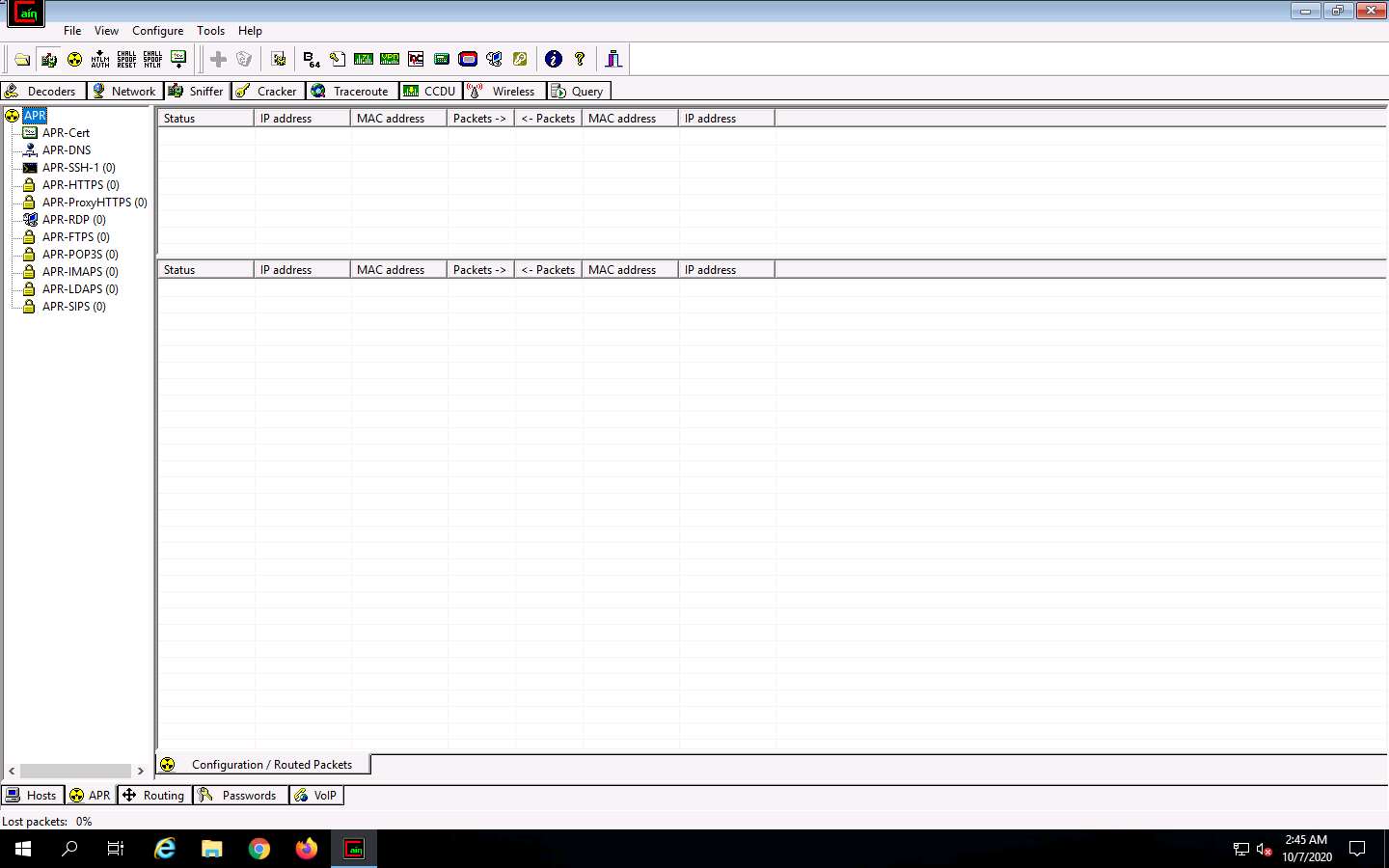
1. The MAC Address Scanner window appears. Click on the **Range** radio button, enter the range (**172.19.19.2** - **172.19.19.20**), check **All Tests** option and click **OK**. Cain & Abel starts scanning for MAC addresses and lists all those found.



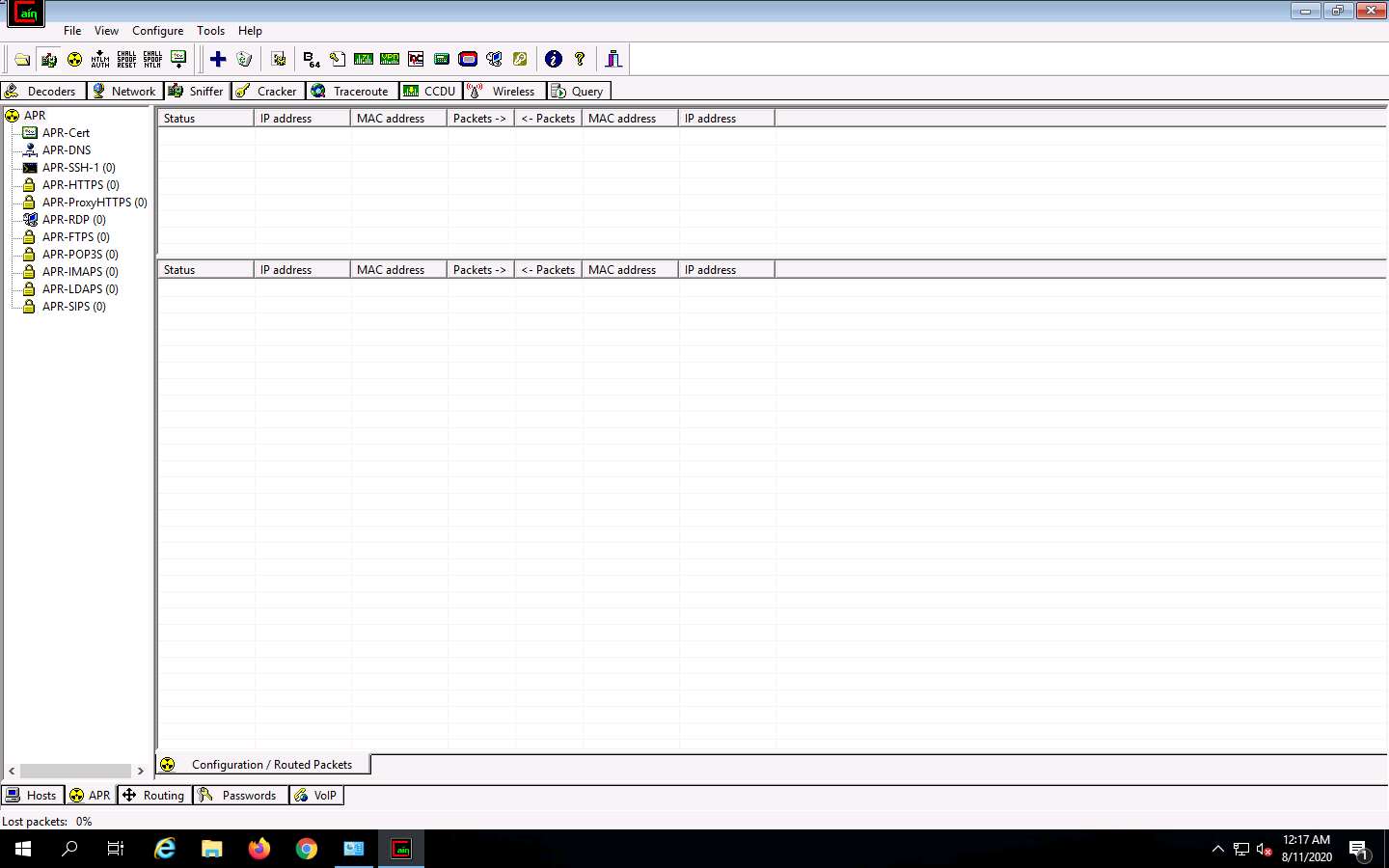
1. After scanning is completed, a list of detected MAC addresses is displayed as shown in the screenshot.



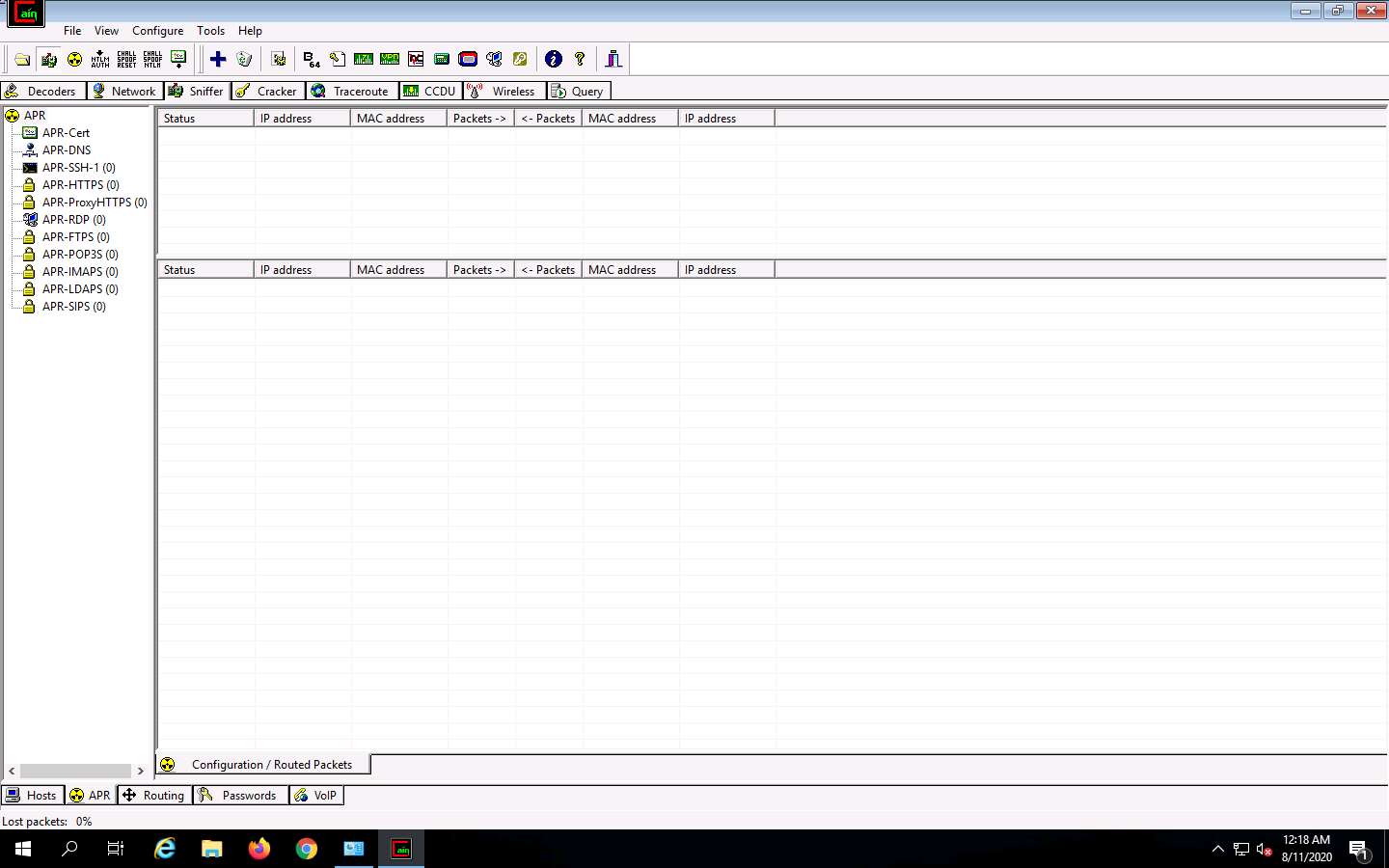
1. Click the **APR** tab at the lower end of the window.



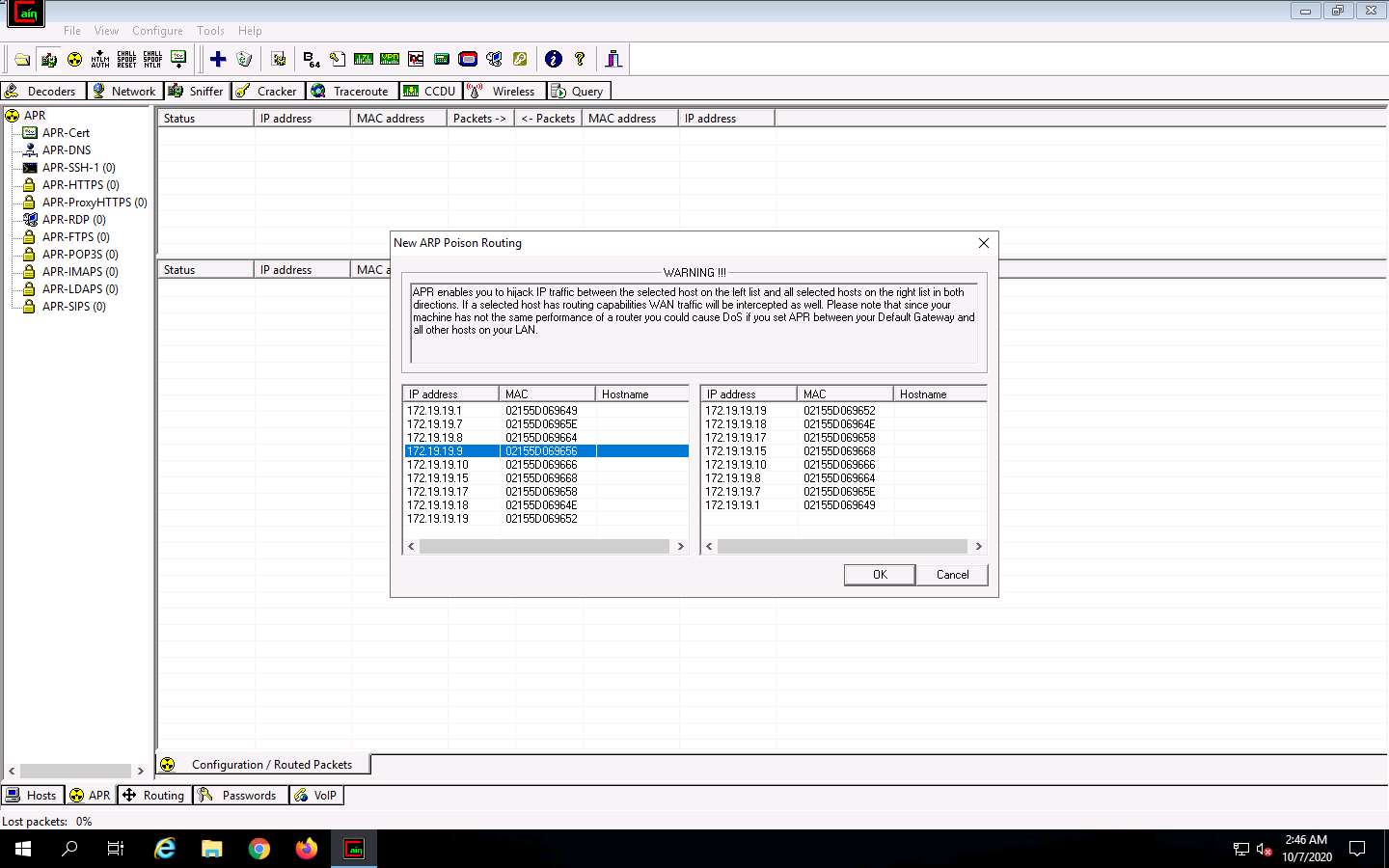
1. Click anywhere on the top most section in the right pane to activate the **+** icon.

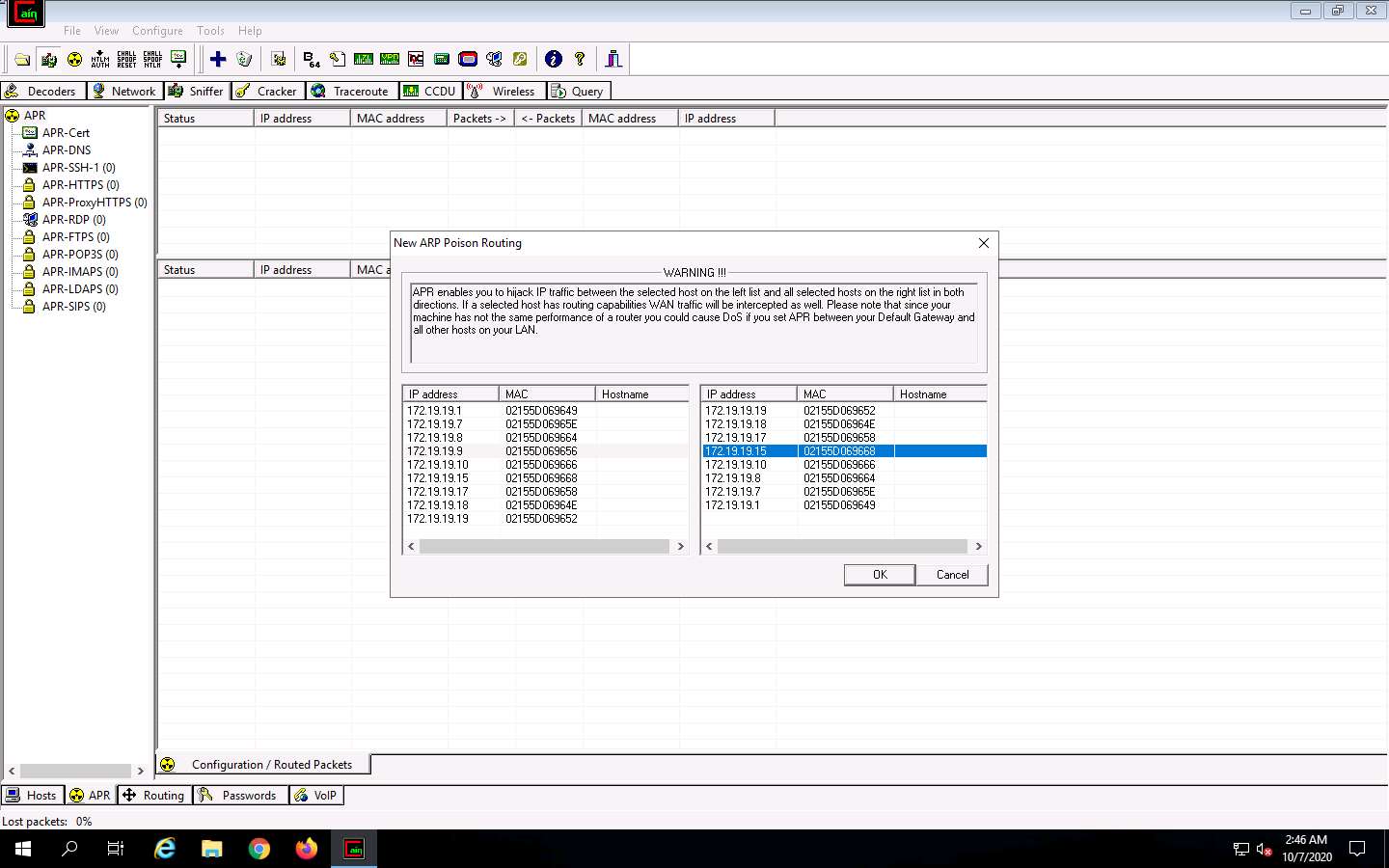


1. Click the Plus (+) icon; the **New ARP Poison Routing** window opens, from which we can add IP’s to listen to traffic.

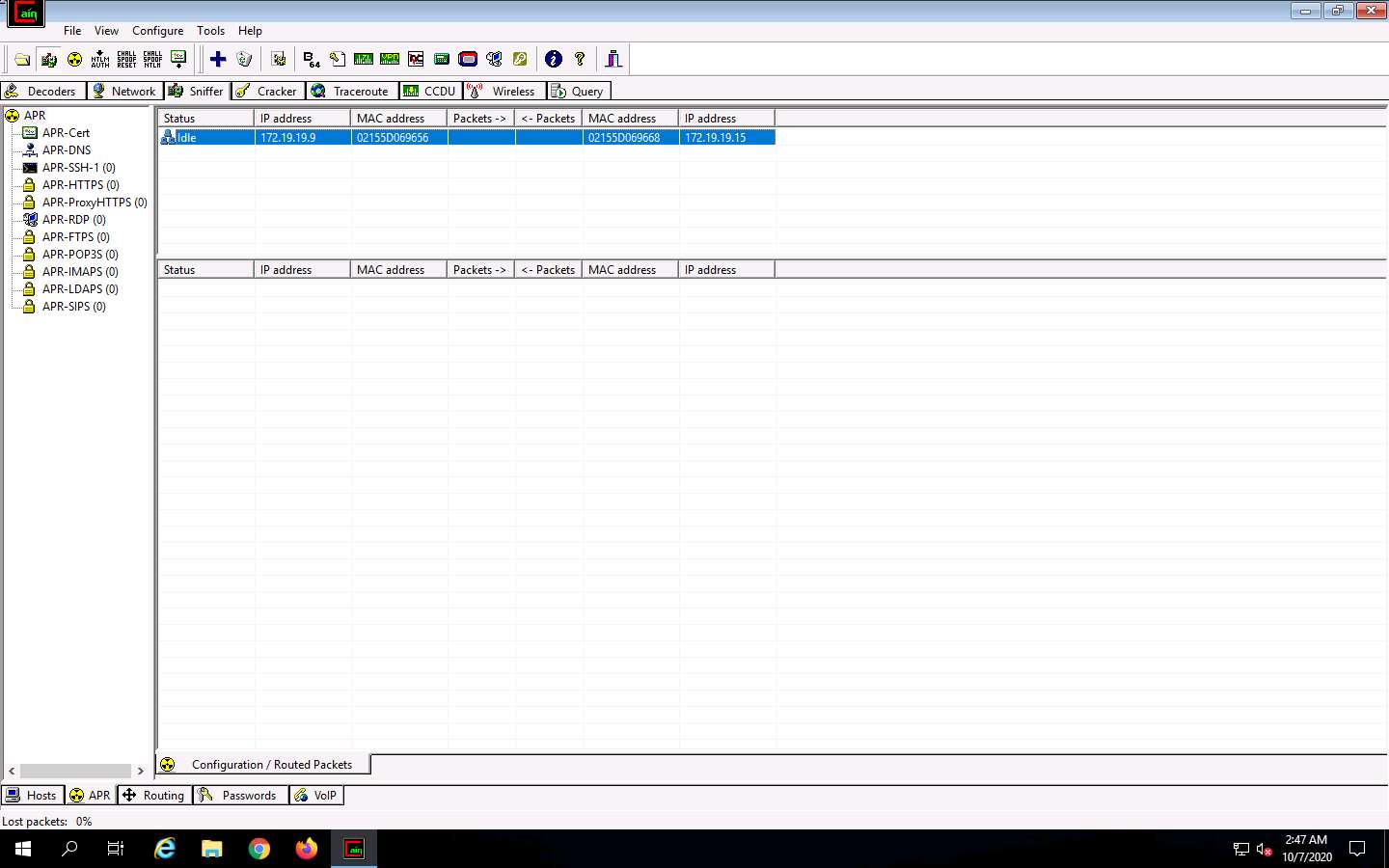


1. To monitor the traffic between two computers, select **172.19.19.9** (FTP Server) and **172.19.19.15** (Advertisement Dept). Click **OK**. In this lab, we are going to log in to FTP server from Advertisement Dept machine.





1. Select the added IP address in the **Configuration/Routed** packets, and click **Start/Stop APR** (third icon from left) icon. Cain begins ARP poisoning in between these machines.



1. Log on to **Advertisement Dept** and **Sign in** as **Administrator**. For doing this, select **Advertisement Dept** machine from the **Resources** pane. Go to **Commands** and click **Ctrl+Alt+Delete**.



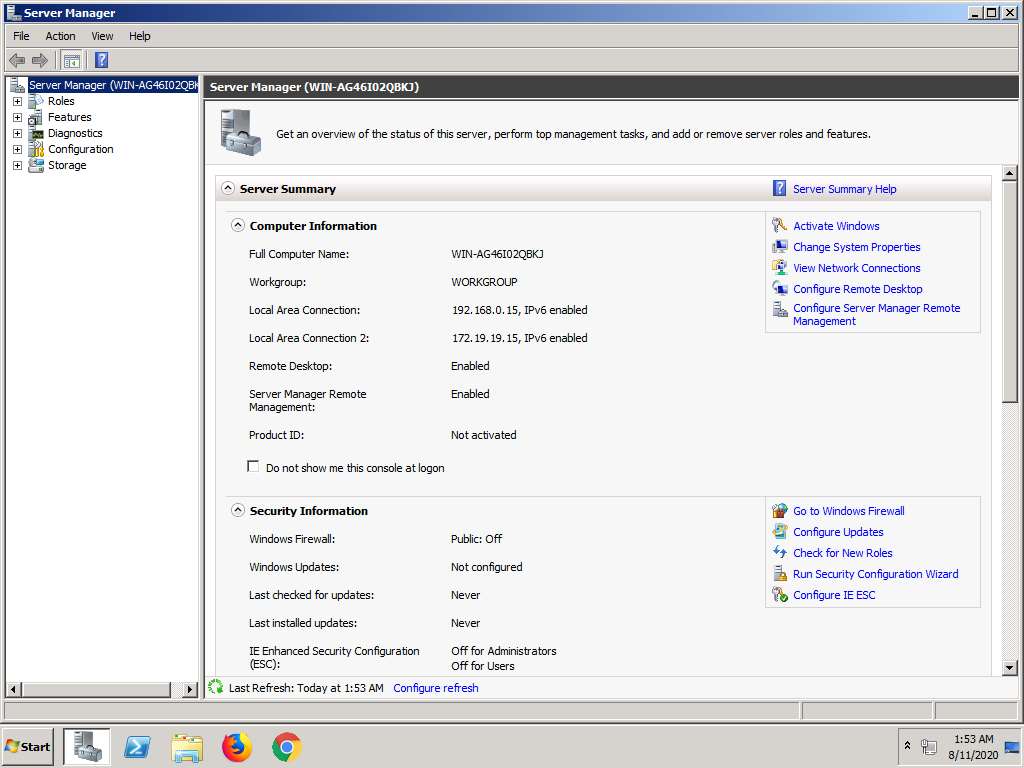
1. Select **Administrator** user in the login window.



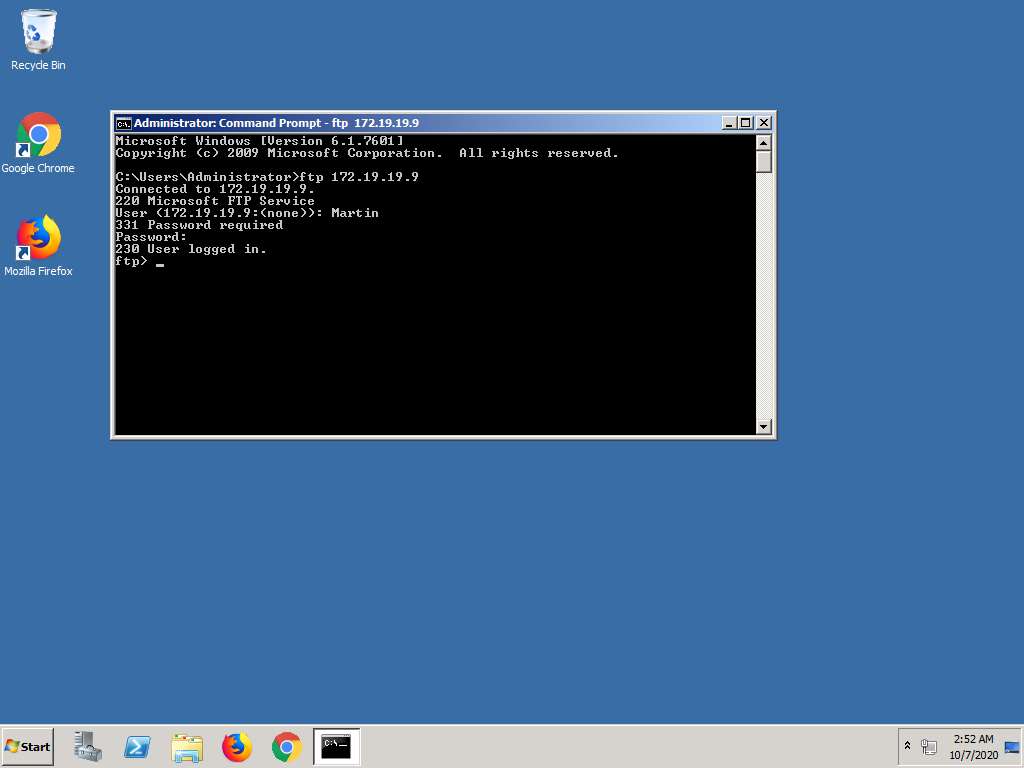
1. In the logon box enter the password **Pa$$w0rd** press **Enter**:



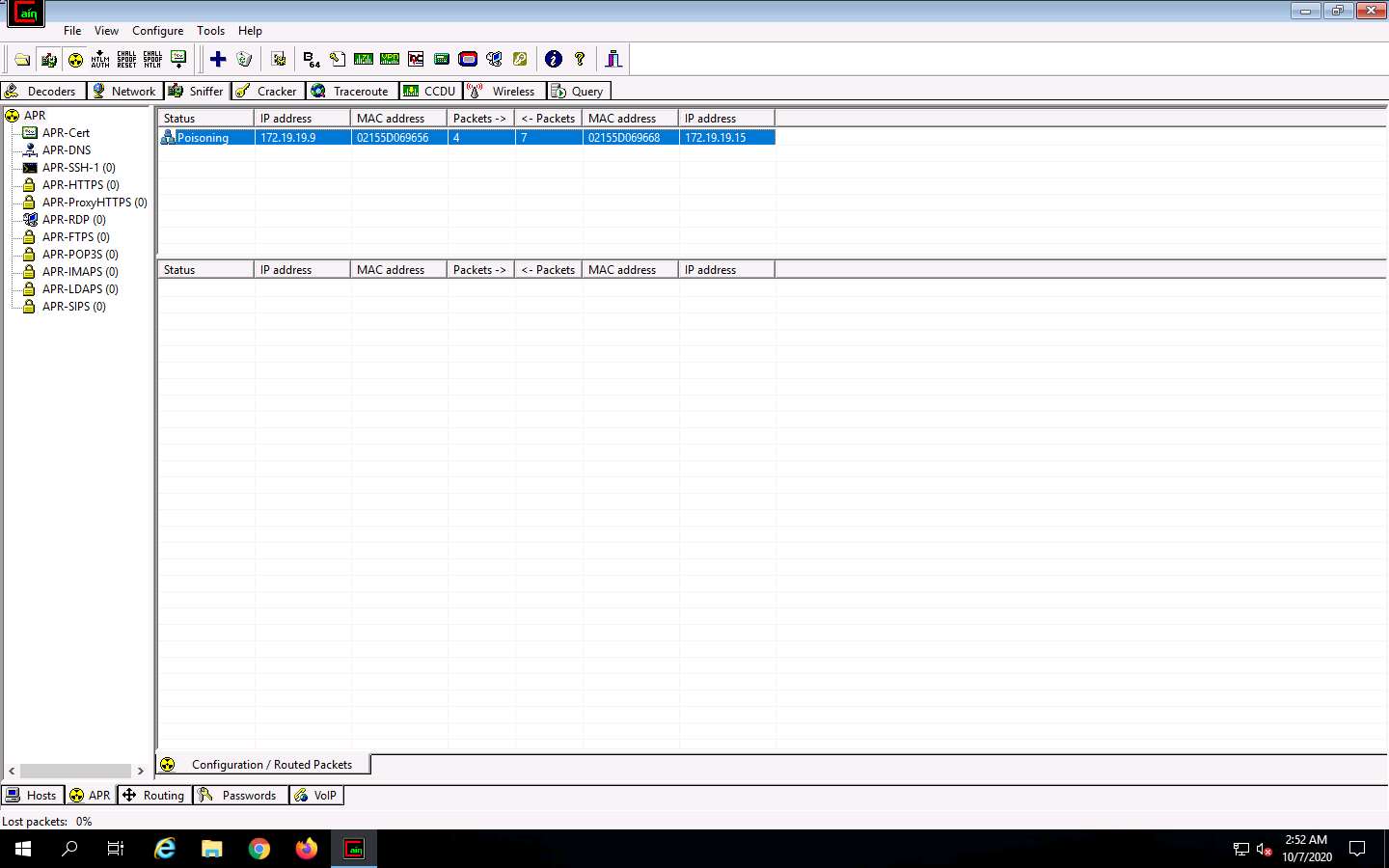
1. Click on the **Close** button at the top right corner of the **Server Manager** window.



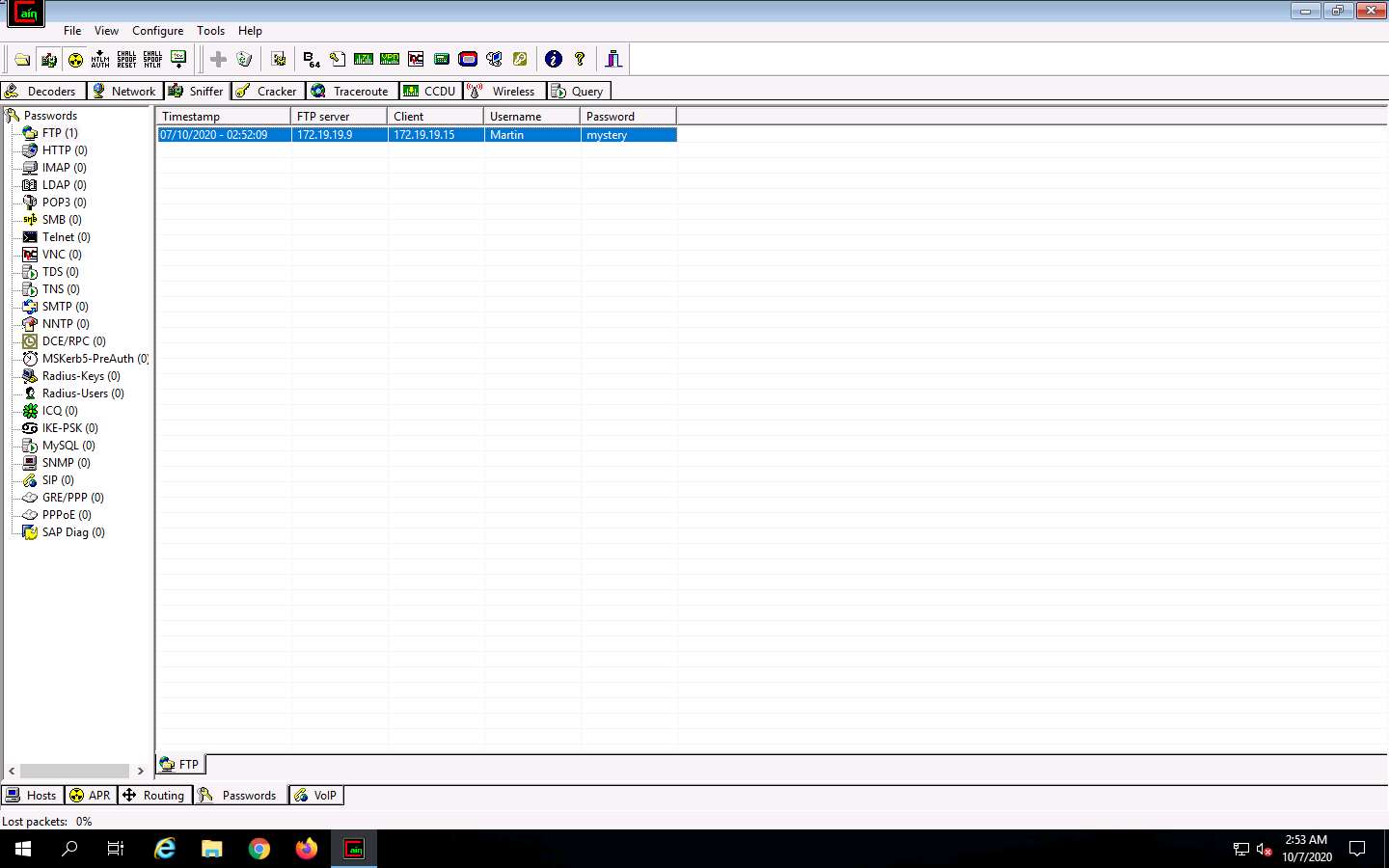
1. Now launch a command prompt in the machine, type **ftp 172.19.19.9** (IP address of **FTP Server** machine) and press **Enter**. When prompted for the Username, type "**Martin"** and press **Enter**. When prompted for the password, type "**mystery"** and press **Enter**.



1. Switch [Windows Server 2019](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10) machine. You will observe that Cain & Abel captured some packets which can be observed under the Packets field.



1. Click the **Passwords** tab in the **Cain & Abel** GUI. Select **FTP** from the left pane under the **Passwords** section. You will observe the credentials being captured by Cain & Abel as shown in the screenshot.



1. This way, you have successfully captured user credentials traversing in clear-text. In this lab, you have learned how to capture user credentials in a switch based network.