Module 16: Hacking Wireless Networks

Lab 1: Perform Wireless Traffic Analysis

Lab Scenario

As a professional ethical hacker or pen tester, your next step in hacking wireless networks is to capture and analyze the traffic of the target wireless network.

This wireless traffic analysis will help you to determine the weaknesses and vulnerable devices in the target network. In the process, you will determine the network's broadcasted SSID, the presence of multiple access points, the possibility of recovering SSIDs, the authentication method used, WLAN encryption algorithms, etc.

The labs in this exercise demonstrate how to use various tools and techniques to capture and analyze the traffic of the target wireless network.

Lab Objectives

- Wi-Fi packet analysis using Wireshark

Overview of Wireless Traffic Analysis

Wireless traffic analysis helps in determining the appropriate strategy for a successful attack. Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets. You can use various Wi-Fi packet-sniffing tools to capture and analyze the traffic of a target wireless network.

Task 1: Wi-Fi Packet Analysis using Wireshark

Wireshark is a network protocol sniffer and analyzer. It lets you capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting. Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

Here, we will use Wireshark to analyze captured Wi-Fi packets.

In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (**WEPcrack-01.cap**) to analyze wireless packets.

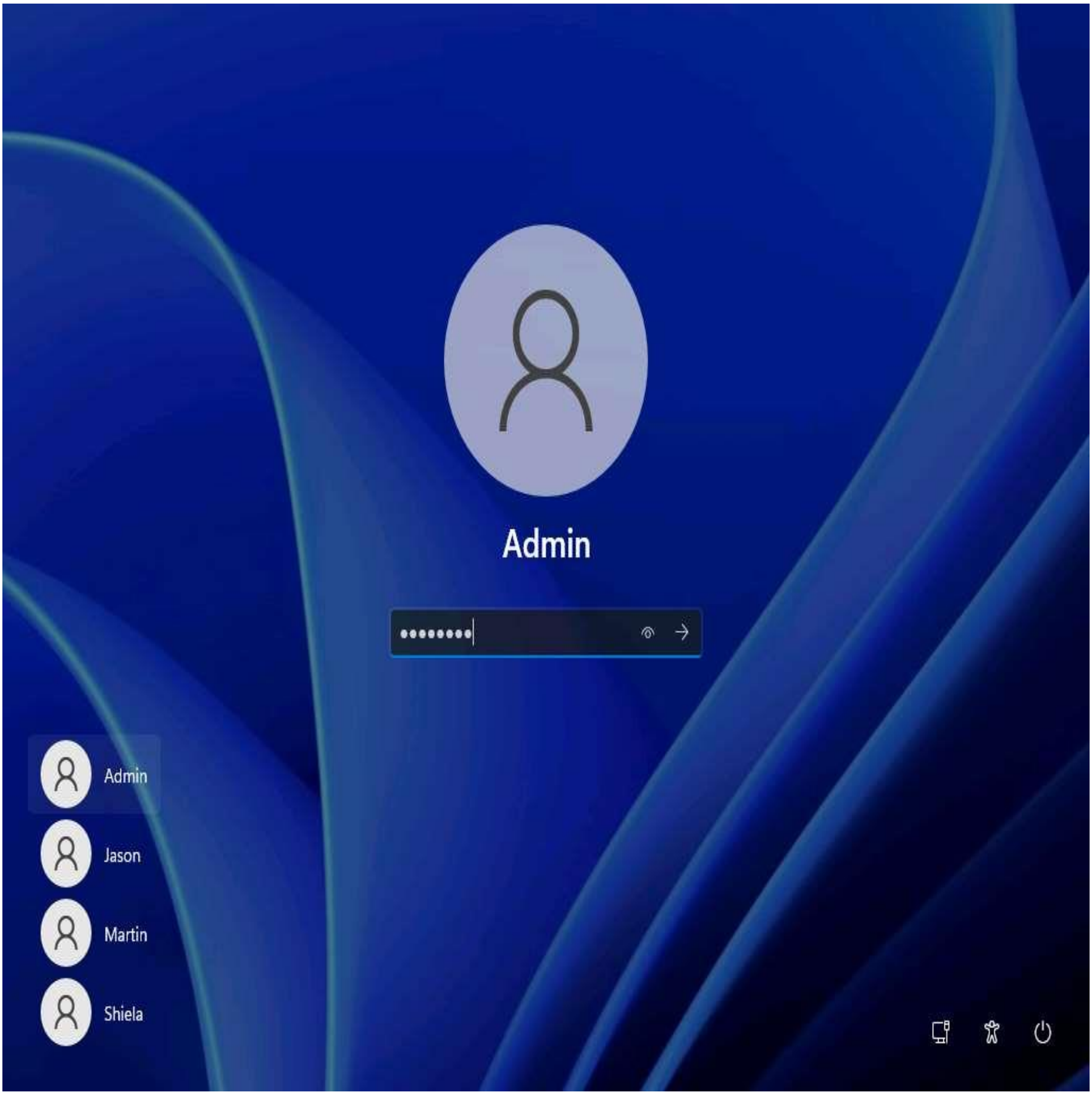
1. □ By default, **Windows 11** machine selected, click Ctrl+Alt+Delete.

   Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

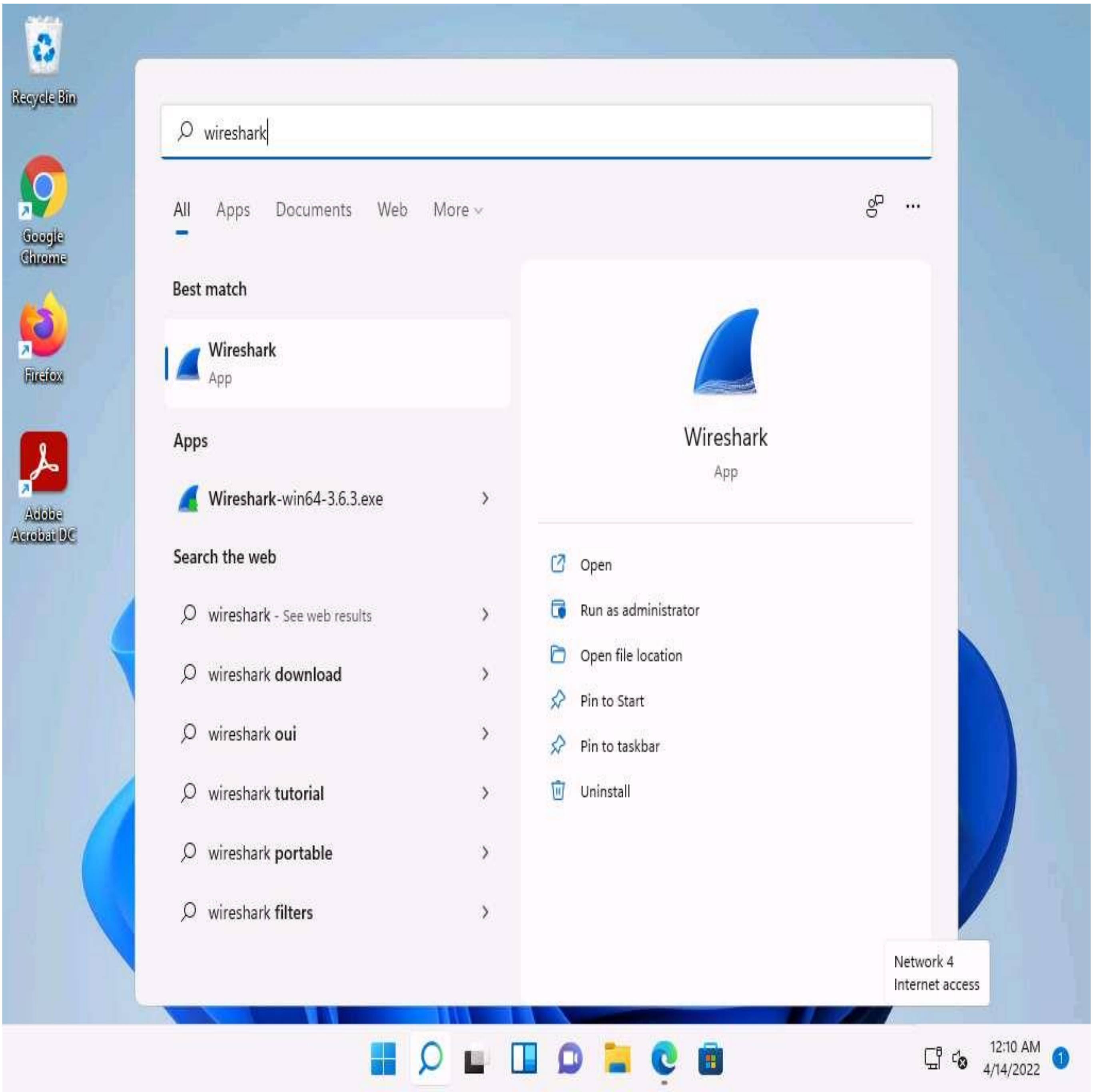
2. □ By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.
If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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

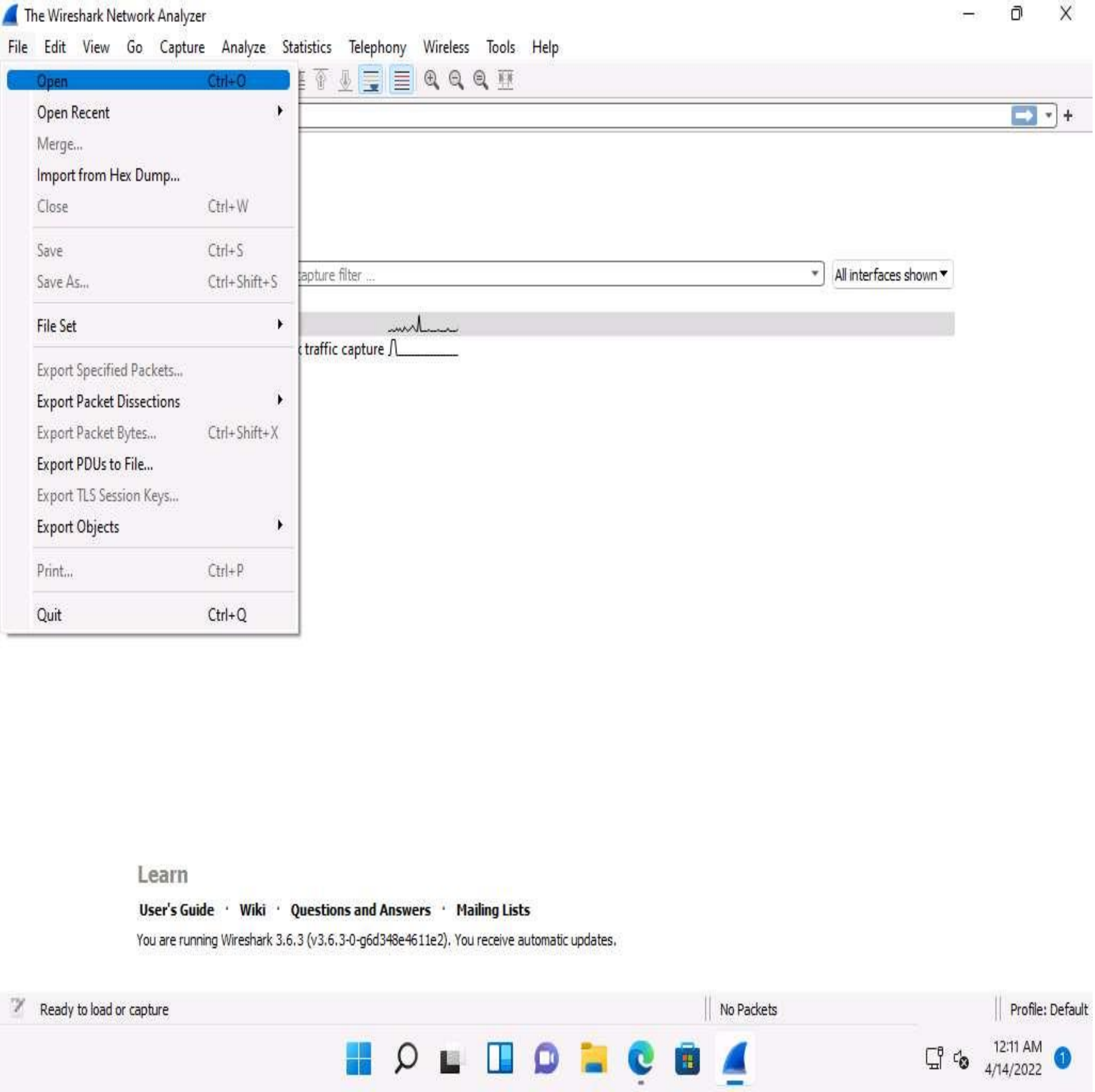


3. □ Click **search** icon 🔍 on the **Desktop**. Type **wire** in the search field,the **Wireshark** appears in the results, click **open** to lanch it.

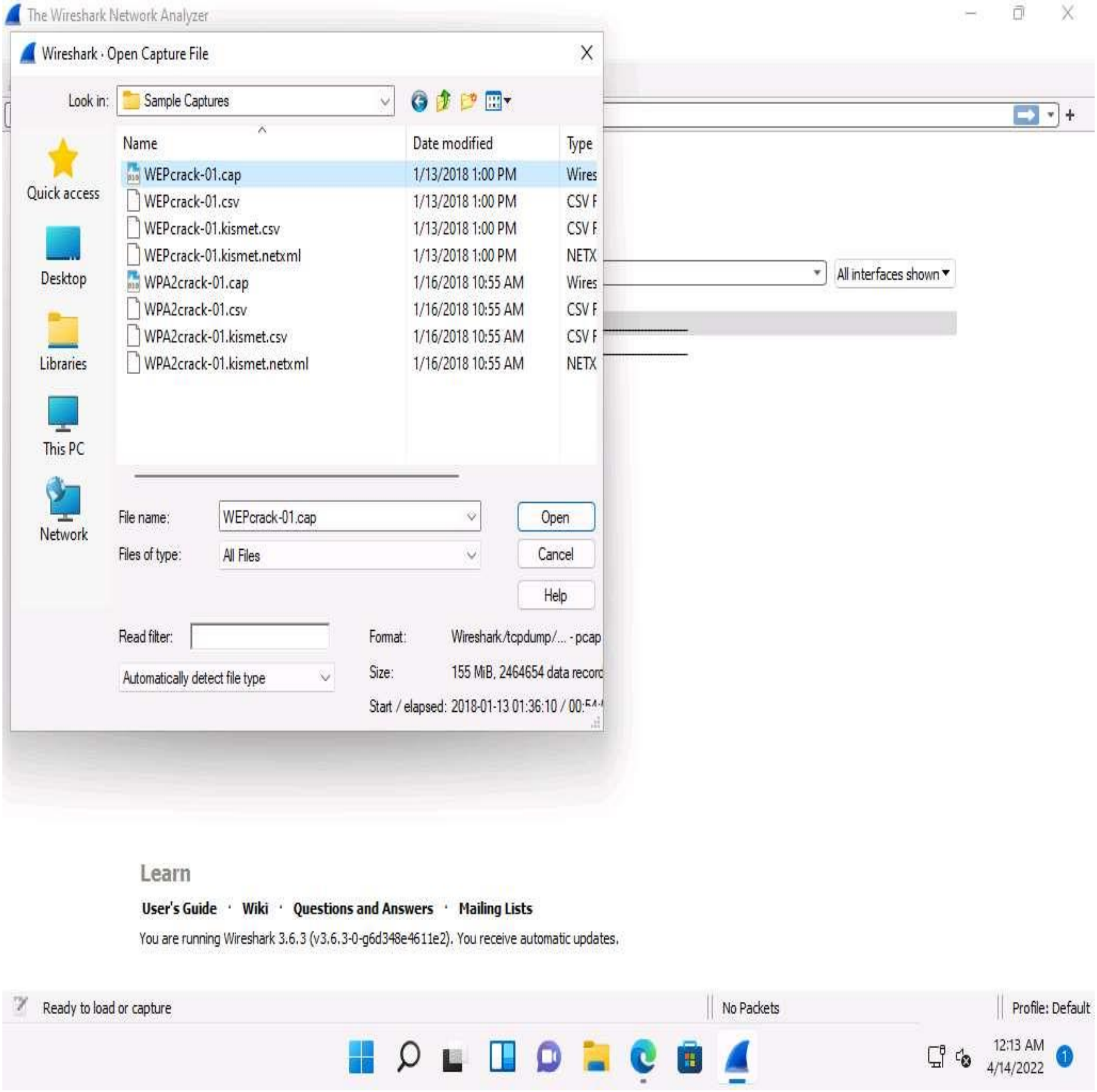


wireshark

4. □ The **Wireshark Network Analyzer** window appears.
5. □ In the menu bar, click **File** and click **Open** option from the drop-down list.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
apture filter ...
All interfaces shown
traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.6.3 (v3.6.3-0-g6d348e4611e2). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
12:11 AM
4/14/2022

6. □ **Wireshark: Open Capture File** window appears, navigate to **E:\CEH-Tools\CEHv12 Module 16 Hacking Wireless Networks\Sample Captures**, select **WEPcrack-01.cap** and click **Open**.



Look in: Sample Captures

Name	Date modified	Type
WEPcrack-01.cap	1/13/2018 1:00 PM	Wires
WEPcrack-01.csv	1/13/2018 1:00 PM	CSV F
WEPcrack-01.kismet.csv	1/13/2018 1:00 PM	CSV F
WEPcrack-01.kismet.netxml	1/13/2018 1:00 PM	NETX
WPA2crack-01.cap	1/16/2018 10:55 AM	Wires
WPA2crack-01.csv	1/16/2018 10:55 AM	CSV F
WPA2crack-01.kismet.csv	1/16/2018 10:55 AM	CSV F
WPA2crack-01.kismet.netxml	1/16/2018 10:55 AM	NETX

File name: WEPcrack-01.cap

Files of type: All Files

Read filter:

Automatically detect file type

Format: Wireshark/tcpdump/... - pcap

Size: 155 MiB, 2464654 data record

Start / elapsed: 2018-01-13 01:36:10 / 00:54

You are running Wireshark 3.6.3 (v3.6.3-0-g6d348e4611e2). You receive automatic updates.

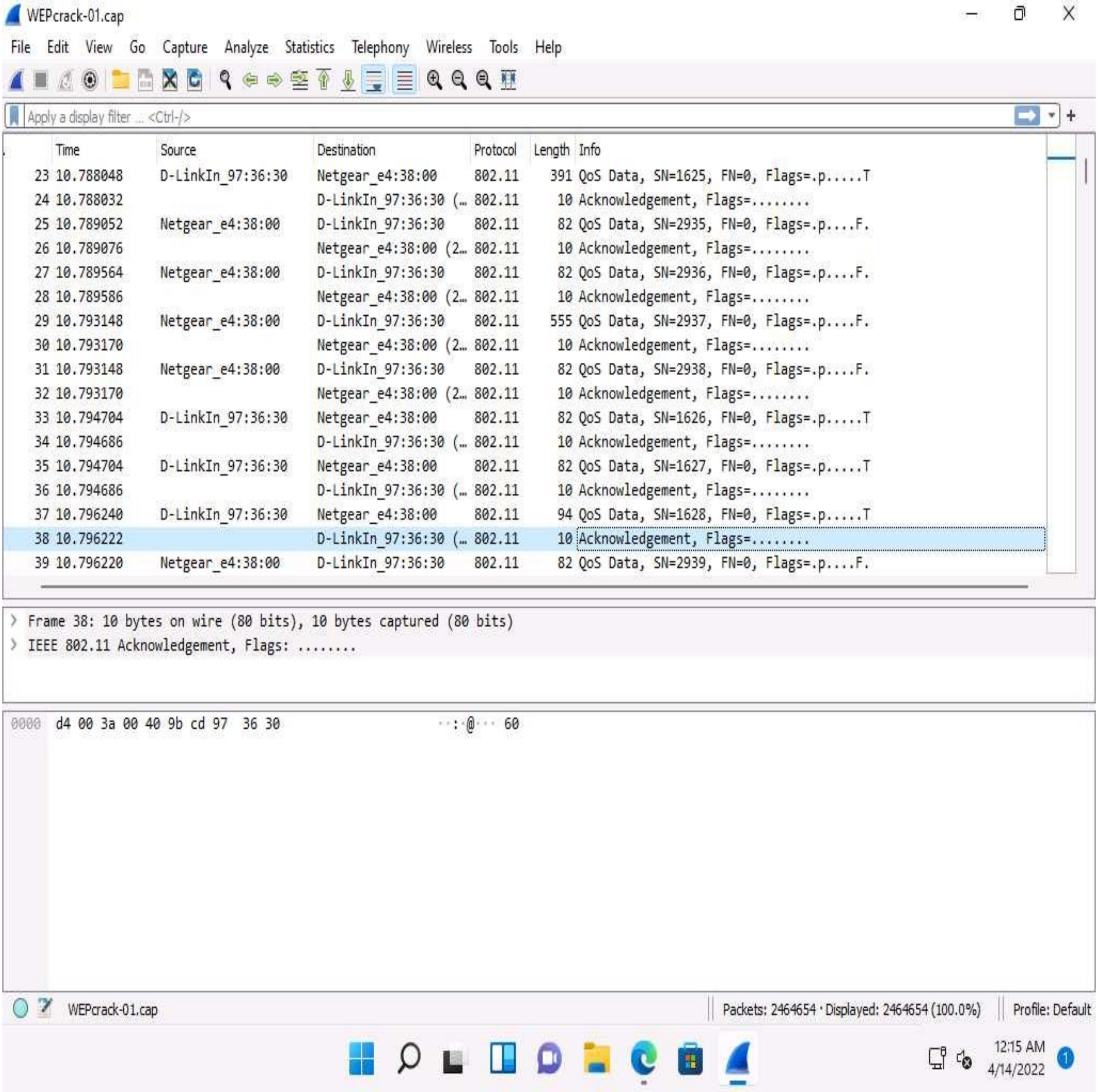
7. □ The **WEPcrack-01.cap** file opens in Wireshark window showing you the details of the packet for analysis. Here you can see the wireless packets captured which were otherwise masked to look like **ethernet** traffic.

Here 802.11 protocol indicates wireless packets.

You can access the saved packet capture file anytime, and by issuing packet filtering commands in the Filter field, you can narrow down the packet search in an attempt to find packets containing sensible information.

In real time, attackers enforce packet capture and packet filtering techniques to capture packets containing passwords (only for websites implemented on HTTP channel), perform attacks such as session hijacking, and so on.

Similarly you can also analyze the **WPA2crack-01.cap** file for WPA packets.


WEPcrack-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
   Time        Source             Destination          Protocol  Length Info
23 10.788048   D-LinkIn_97:36:30  Netgear_e4:38:00     802.11    391 QoS Data, SN=1625, FN=0, Flags=.p.....T
24 10.788032                      D-LinkIn_97:36:30 (… 802.11     10 Acknowledgement, Flags=........
25 10.789052   Netgear_e4:38:00   D-LinkIn_97:36:30    802.11     82 QoS Data, SN=2935, FN=0, Flags=.p....F.
26 10.789076                      Netgear_e4:38:00 (2… 802.11     10 Acknowledgement, Flags=........
27 10.789564   Netgear_e4:38:00   D-LinkIn_97:36:30    802.11     82 QoS Data, SN=2936, FN=0, Flags=.p....F.
28 10.789586                      Netgear_e4:38:00 (2… 802.11     10 Acknowledgement, Flags=........
29 10.793148   Netgear_e4:38:00   D-LinkIn_97:36:30    802.11    555 QoS Data, SN=2937, FN=0, Flags=.p....F.
30 10.793170                      Netgear_e4:38:00 (2… 802.11     10 Acknowledgement, Flags=........
31 10.793148   Netgear_e4:38:00   D-LinkIn_97:36:30    802.11     82 QoS Data, SN=2938, FN=0, Flags=.p....F.
32 10.793170                      Netgear_e4:38:00 (2… 802.11     10 Acknowledgement, Flags=........
33 10.794704   D-LinkIn_97:36:30  Netgear_e4:38:00     802.11     82 QoS Data, SN=1626, FN=0, Flags=.p.....T
34 10.794686                      D-LinkIn_97:36:30 (… 802.11     10 Acknowledgement, Flags=........
35 10.794704   D-LinkIn_97:36:30  Netgear_e4:38:00     802.11     82 QoS Data, SN=1627, FN=0, Flags=.p.....T
36 10.794686                      D-LinkIn_97:36:30 (… 802.11     10 Acknowledgement, Flags=........
37 10.796240   D-LinkIn_97:36:30  Netgear_e4:38:00     802.11     94 QoS Data, SN=1628, FN=0, Flags=.p.....T
38 10.796222                      D-LinkIn_97:36:30 (… 802.11     10 Acknowledgement, Flags=........
39 10.796220   Netgear_e4:38:00   D-LinkIn_97:36:30    802.11     82 QoS Data, SN=2939, FN=0, Flags=.p....F.
```

```
> Frame 38: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
> IEEE 802.11 Acknowledgement, Flags: ........
```

```
0000  d4 00 3a 00 40 9b cd 97  36 30                  ··:·@··· 60
```

8. □ This concludes the demonstration of how to analyze Wi-Fi packets using Wireshark.

9. □ Close all open windows and document all the acquired information.

10. □ You can also use other wireless traffic analyzers such as **AirMagnet WiFi Analyzer PRO** (https://www.netally.com), **SteelCentral Packet Analyzer** (https://www.riverbed.com), **Omnipeek Network Protocol Analyzer** (https://www.liveaction.com), **CommView for Wi-Fi** (https://www.tamos.com), and **Capsa Portable Network Analyzer** (https://www.colasoft.com) to analyze Wi-Fi traffic.