|  |  |
| --- | --- |
| Course | Wireless Network Security |
| Lab | Lab 5- WLAN Traffic Analysis |
| Student ID | 100899259 |
| Student Name | Maisha Khatoon |

# **LAB: 05**

**WLAN traffic analysis**

**Objective:**

In this lab students will explore ways to perform wireless capture and understand WiFi packets.

**Activities:**

Download and install Kali Linux

Configure ALFA network WiFi USB adapter

Configure WiFi AP

**Leaning Activities:**

At the end of these activities, you should understand:

* How to capture wireless packets
* How to inspect management, control and data wireless packets
* How run applications on Kali Linux

*Note: The following chipset and driver of the wireless cards are recommended for the following tasks.*

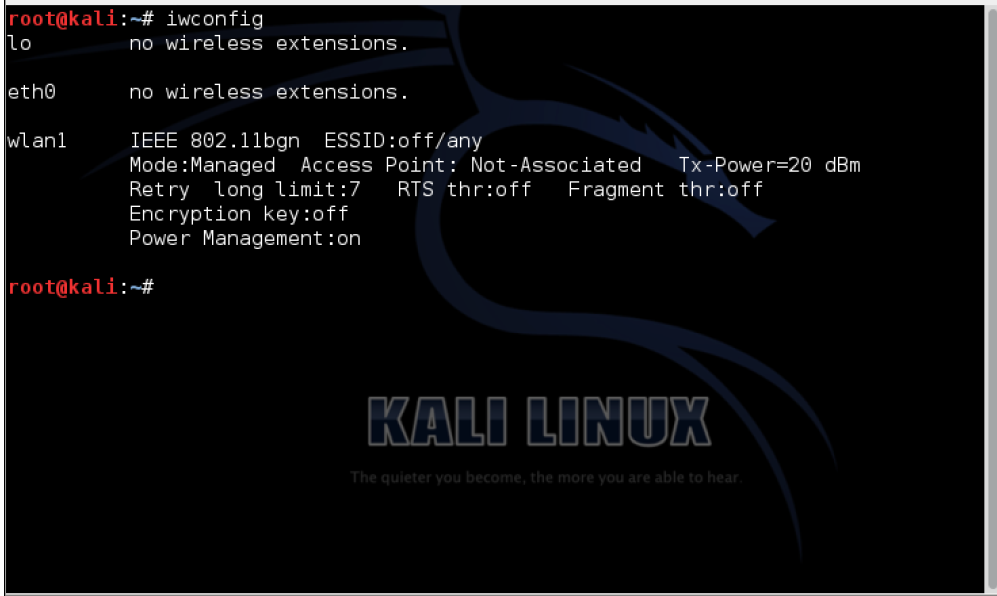
[*https://www.aircrack-ng.org/doku.php?id=compatibility\_drivers*](https://www.aircrack-ng.org/doku.php?id=compatibility_drivers)

*!!Your built-in WiFi card may not work for packet injection and capture!!*

**Task-1**

**Creating a monitor mode interface**

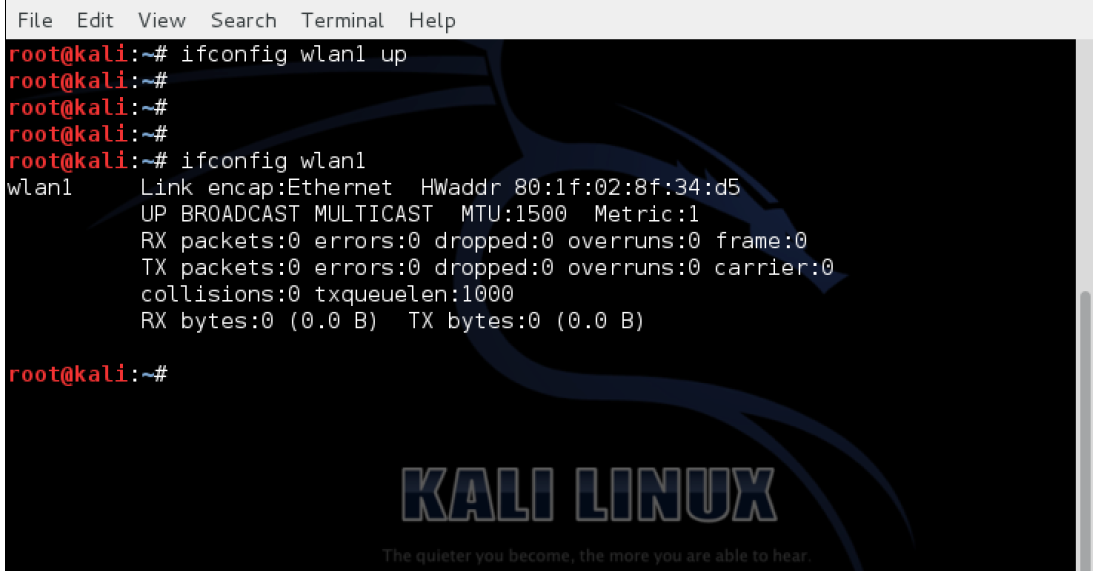
1. Boot Kali with your adapter connected. Once you are within the console, enter **iwconfig** to confirm that your card has been detected and the driver has been loaded properly.



Note: The above command displays “wlan1”, your system may displays “wlan(n)” where n=0,1,2 …

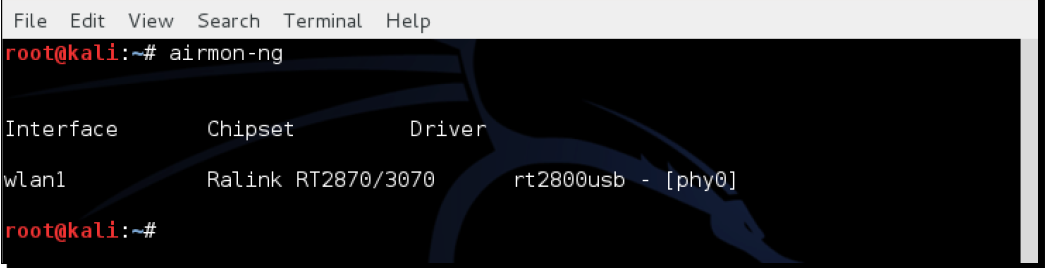
1. Use the **ifconfig wlan(n) up** command to bring the card up (where wlan1 is your adapter). Verify whether the card is up by running **ifconfig wlan(n)**. You should see the word **UP** in the second line of the output as shown in the following screenshot:

Ex:



1. To put our card into monitor mode, we will use the **airmon-ng** utility that is available by default on Kali. First type **airmon-ng** command to verify whether it detects the available cards. You should see the **wlan(n)** interface listed in the output:

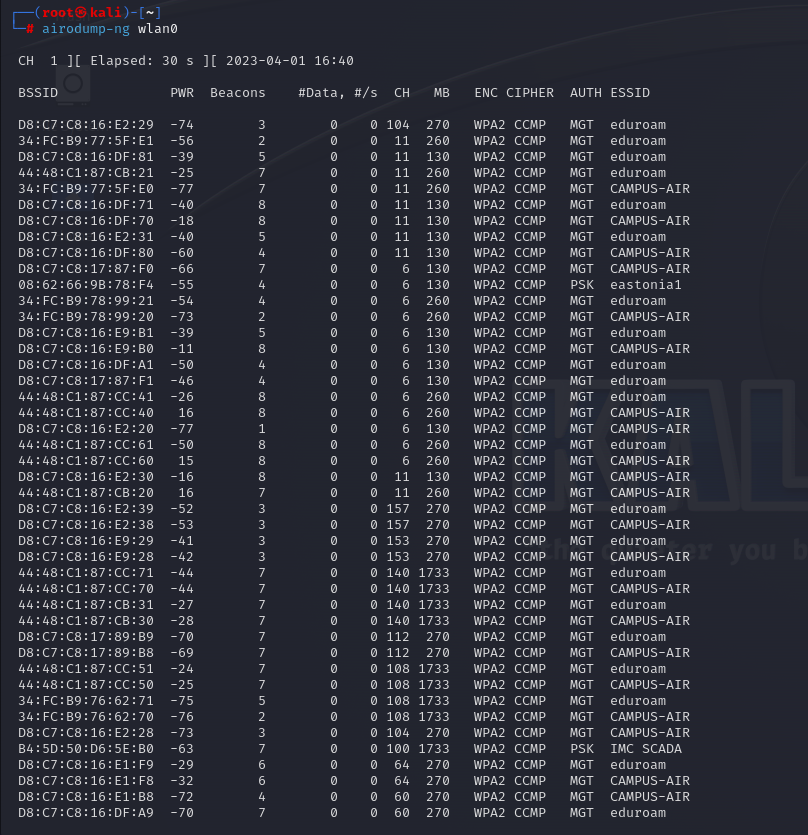
Ex:



1. Write the commands to active Alfa card to monitor mode.

airmon-ng start wlan0

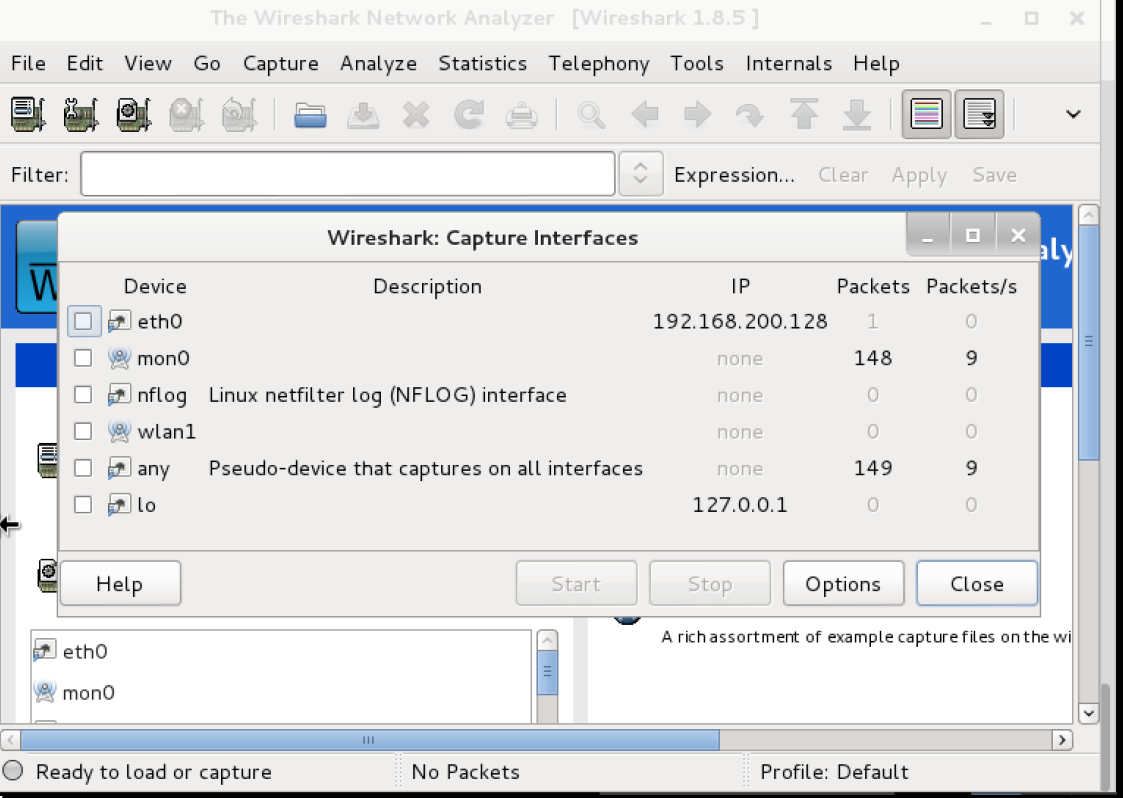
1. Does your Alfa card scan WiFi network? (screenshot)



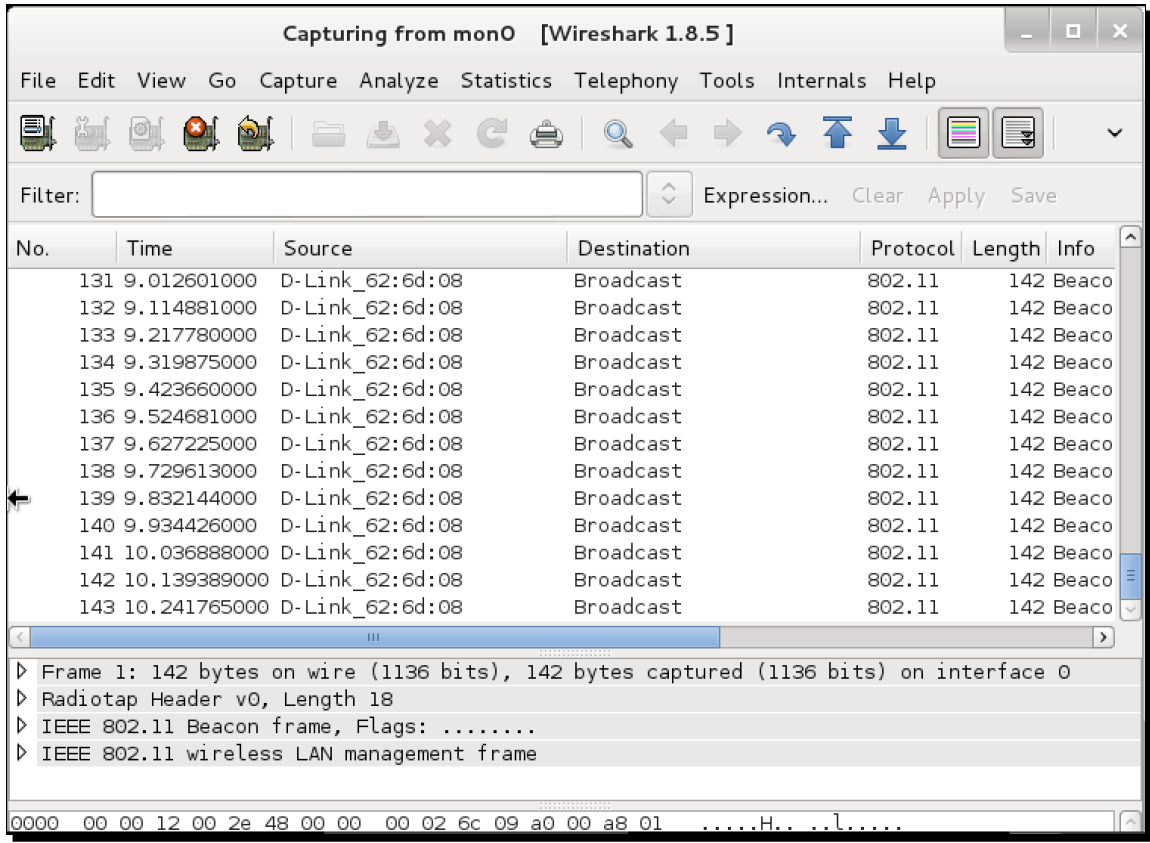
**Task-2**

**Sniffing wireless packets**

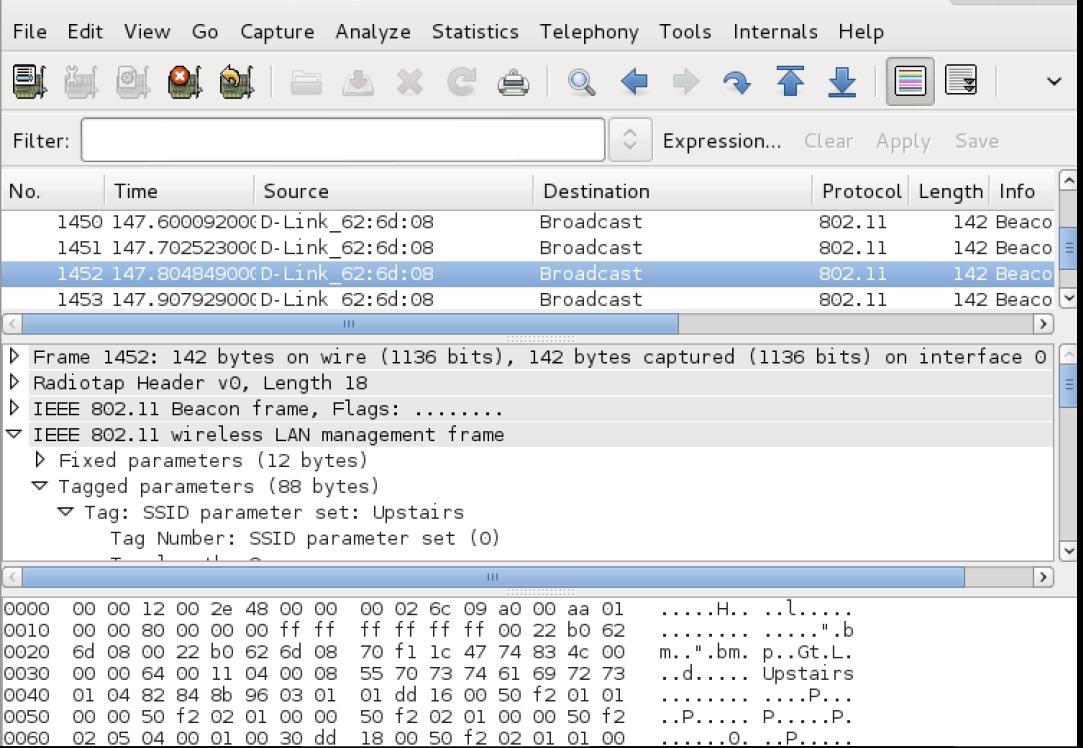
1. Start Wireshark by typing Wireshark & in the console. Once Wireshark is running, navigate to Capture | Interfaces.



1. Select packet capture from the wlan(n) interface by clicking on the Start button to the right of the wlan(n) interface as shown in the previous screenshot. Wireshark will begin the capture, and now you should see packets within the Wireshark window.

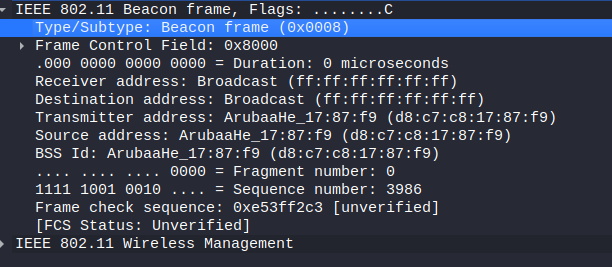


1. These are wireless packets that your wireless adapter is sniffing off the air. In order to view any packet, select it in the top window and the entire packet will be displayed in the middle window.



1. Click on the triangle in front of IEEE 802.11 Wireless LAN management frame to expand and view additional information.

4.1 Identify beacon frames (screenshot)



4.2 What is the filter in wireshark filter to identify beacon frames?

wlan.fc.type\_subtype ==8

(Ref: <https://semfionetworks.com/wp-content/uploads/2021/04/wireshark_802.11_filters_-_reference_sheet.pdf>)

* 1. What is the filter in wireshark to identify probe frames?

wlan.fc.type\_subtype ==4

* 1. What are the SSIDs? (List 3)

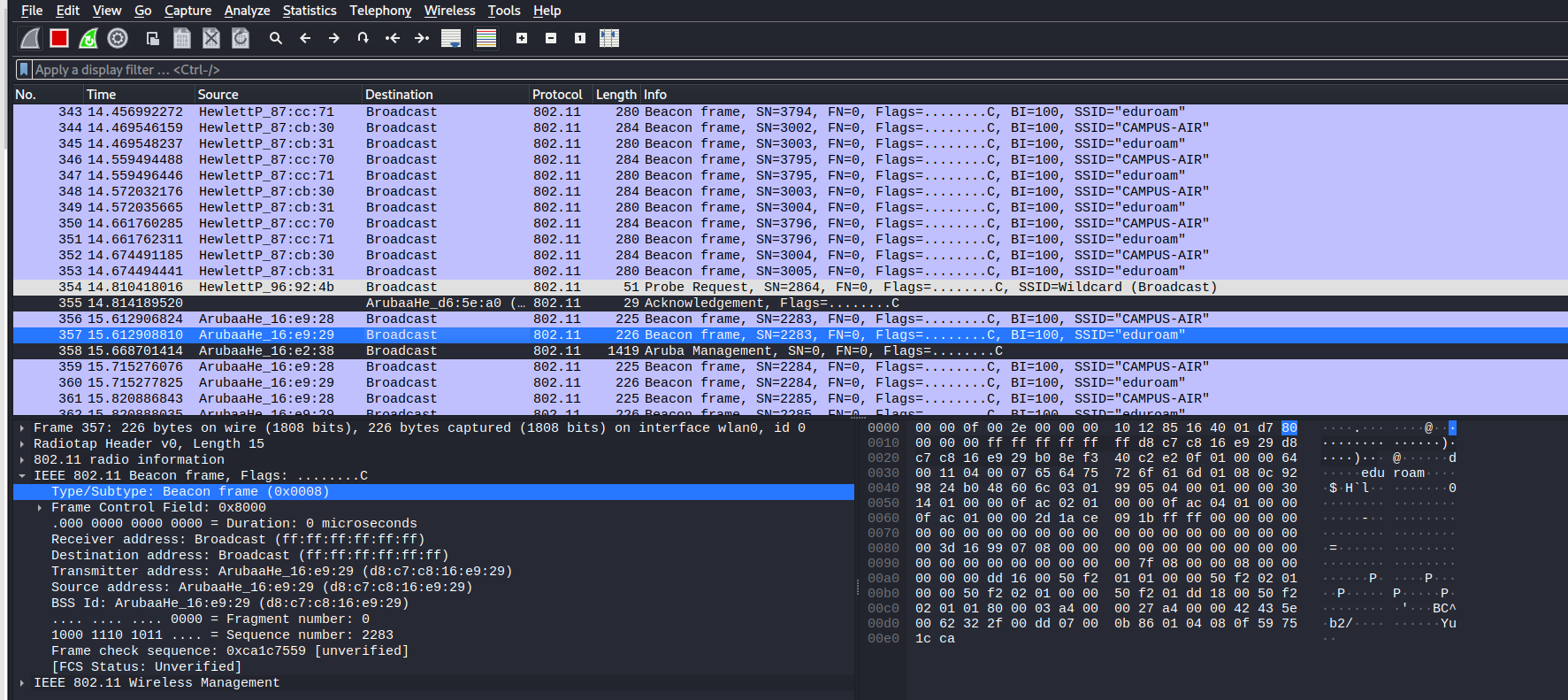
wlan.fc.type\_subtype == 0x0004

wlan.fc.type\_subtype == 0x0005

**Apply colour filters**

* 1. We can apply some colour filters captured packet in wireshark. So whenever we apply this filter in future the specific colour filters will also get applied. It makes it a lot easier to visually isolate the packets which we want to see.

Apply colour filters for beacon and probe frames. (screen shoot)

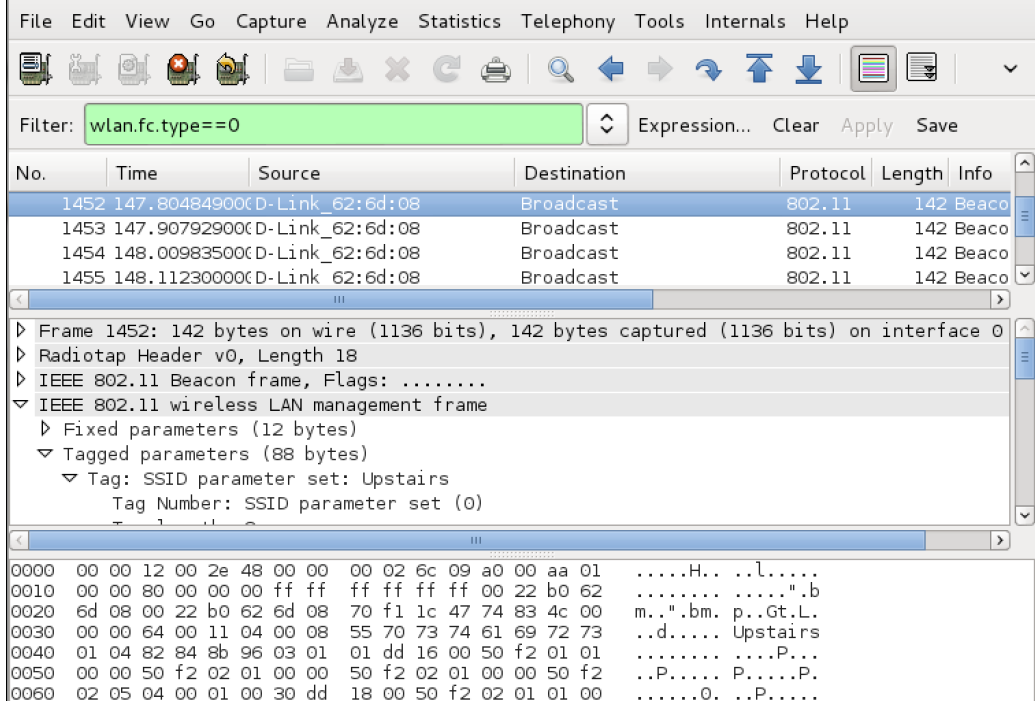


(Ref: <https://www.wireshark.org/docs/wsug_html_chunked/ChCustColorizationSection.html>)

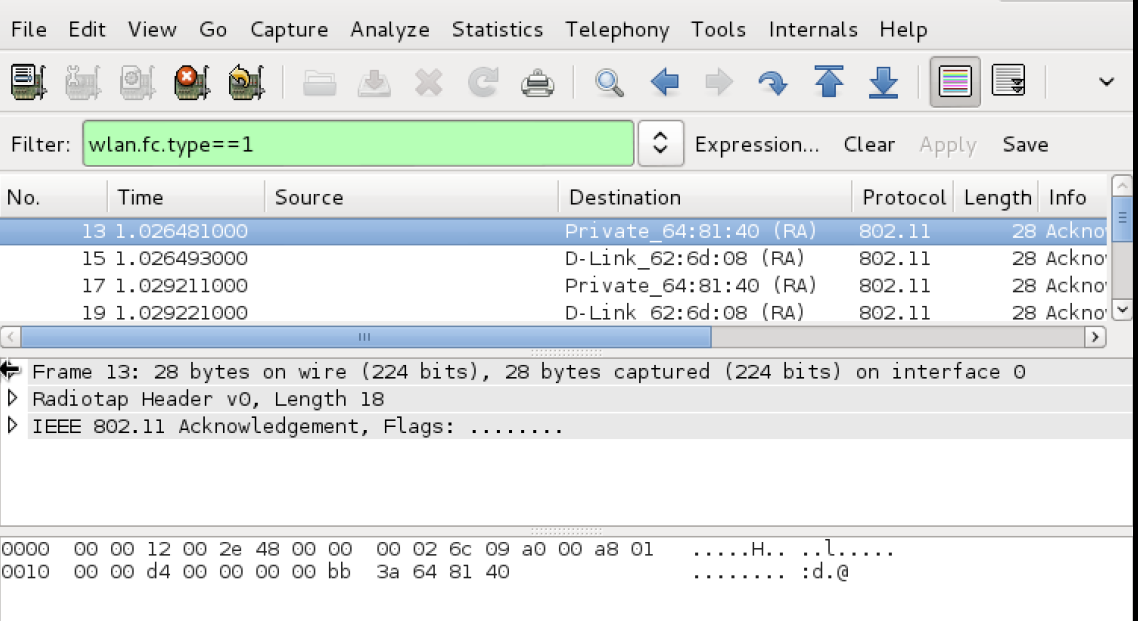
**Task-3**

**Viewing management, control, and data frames**

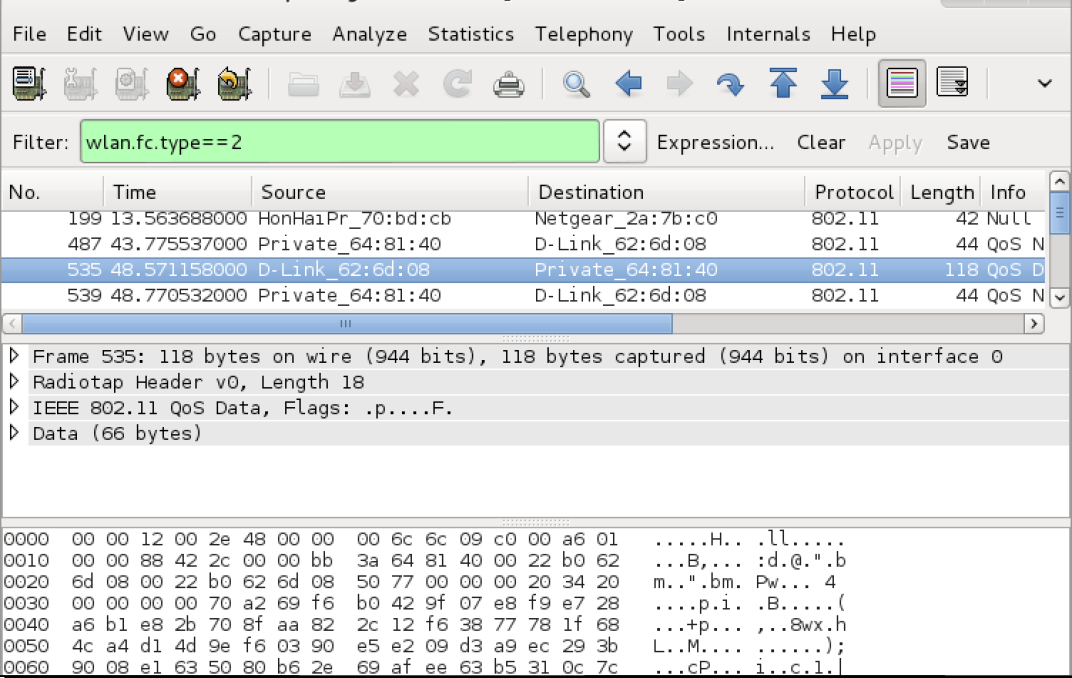
1. To view all the Management frames in the packets being captured, enter the filter **wlan.fc.type == 0** into the filter window and click Apply. You can stop the packet capture if you want to prevent the packets from scrolling down too fast.



1. To view Control Frames, modify the filter expression to read **wlan.fc.type == 1**.

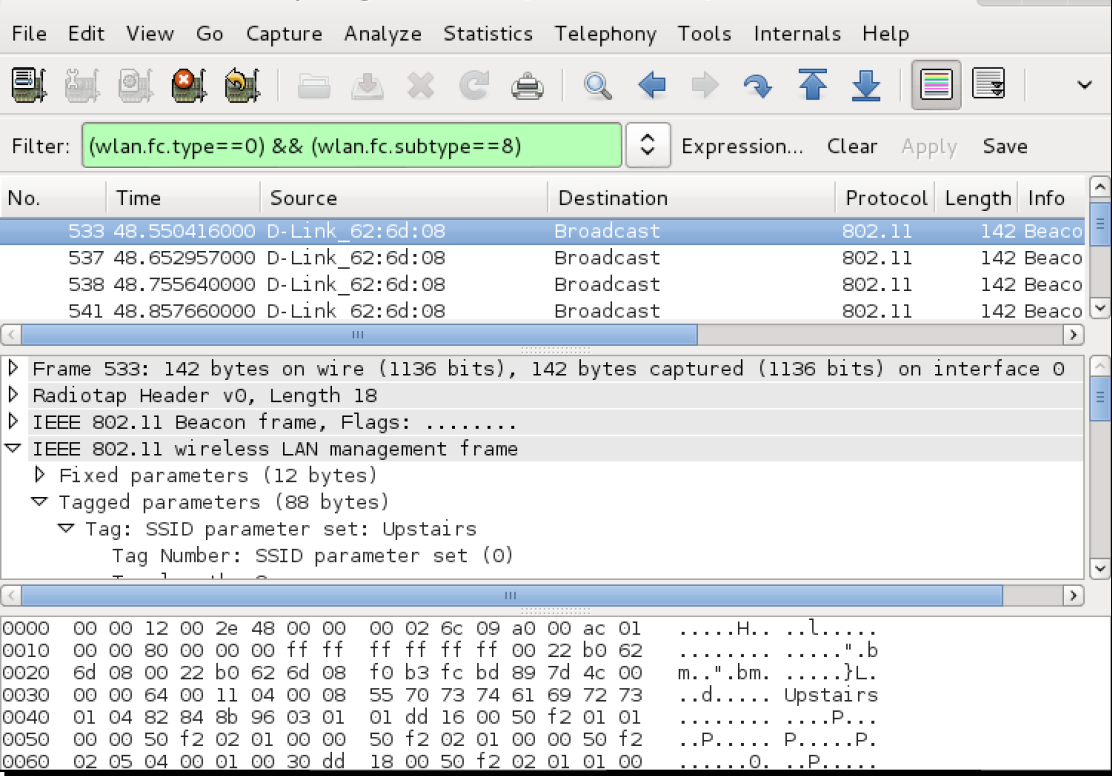


1. To view data frames, modify the filter expression to **wlan.fc.type == 2**.



1. To additionally select a sub-type, use the **wlan.fc.subtype** filter.

For example, to view all the Beacon frames among all Management frames, use the following filter:(wlan.fc.type == 0) && (wlan.fc.subtype == 8).



1. Alternately, you can right-click on any of the header fields in the middle window and then select Apply as Filter | Selected to add it as a filter.

