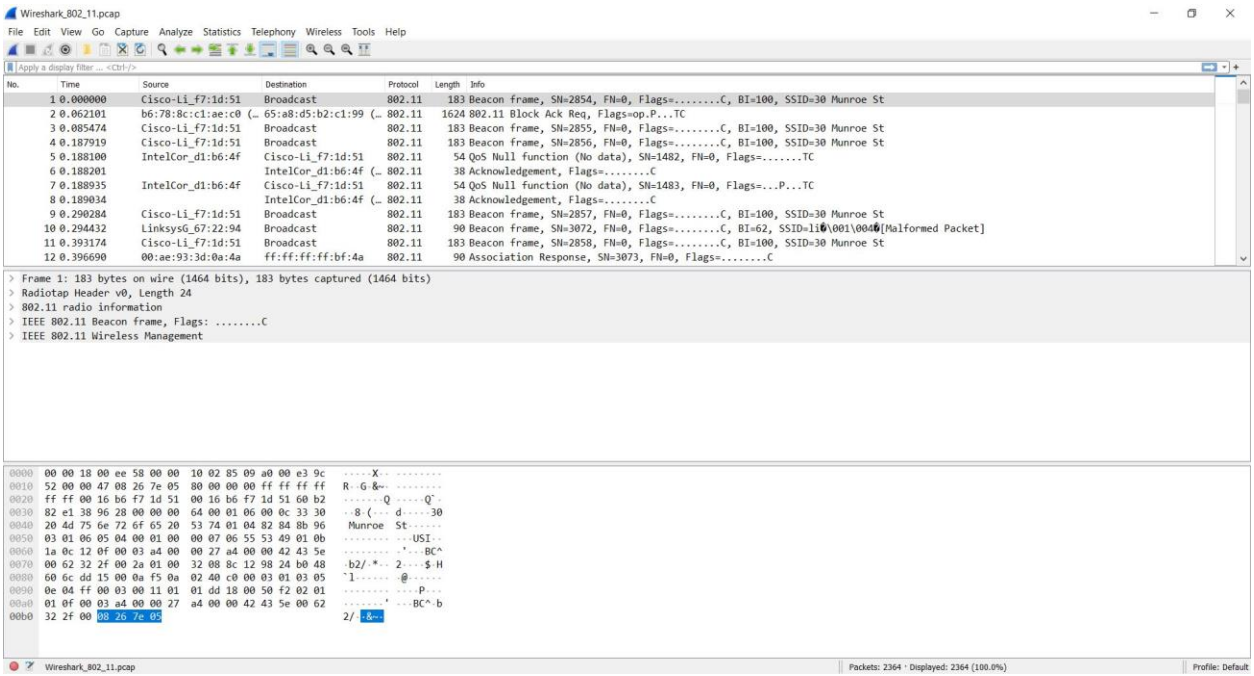
CO513 - Lab 07

Wireless Wireshark Lab - 802.1

E/16/039

Balasuriya B.M.N.U



Bacon Files

Exercise 1

1. **What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?**

   SSID = 30 Munroe st and SSID = Linksys 12

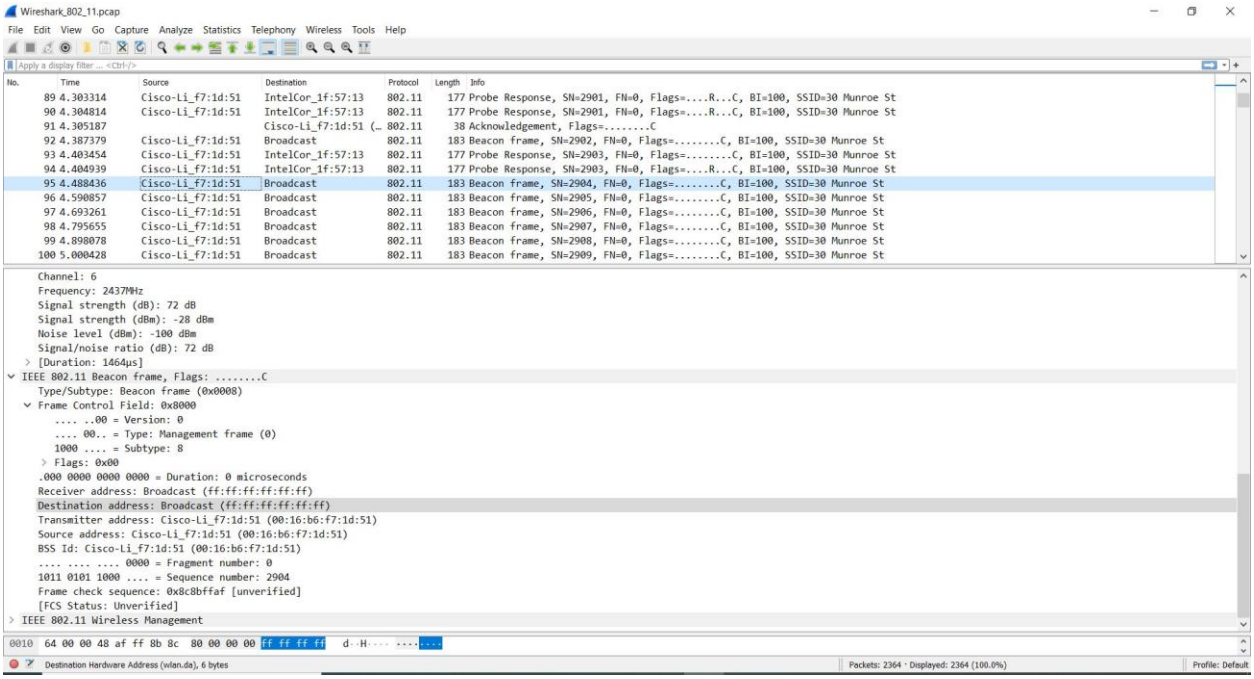
No.	Time	Source	Destination	Protocol	Length	Info
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
17	0.699847	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
18	0.802226	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2862, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID=linksys12
22	1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
23	1.113691	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=,inksys
24	1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
25	1.211992	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1484, FN=0, Flags=.....TC
26	1.212089		IntelCor_d1:b6:4f (…	802.11	38	Acknowledgement, Flags=.....C
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

2. **What are the intervals of time between the transmissions of the beacon frames and the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).**

They both are **0.1024 seconds.**

3. **What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St?**

The source MAC on the beacon feacom frame from 30 Munroe is **00:16:b6:f7:1d:51.**



4. **What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??**

The destination MAC shown here as broadcast. Therefore the destination mac address is **ff.ff.ff.ff.ff.ff**

5. **What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?**

The MAC BSS id on the beacon frame from 30 Munroe St is **00:16:b6:f7:1d:51.**

6. **The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional "extended supported rates." What are these rates?**

Four data rates are,
1.0Mb/s, 2.0Mb/s, 5.5Mb/s, 11.0Mb/s.

Extended supported rates are,
6.0Mb/s, 9.0Mb/s, 12.0Mb/s, 18.0Mb/s, 24.0Mb/s, 36.0Mb/s, 48.0Mb/s, 54.0Mb/s

```
> Capabilities Information: 0x0601
v Tagged parameters (119 bytes)
  > Tag: SSID parameter set: 30 Munroe St
  > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
  > Tag: DS Parameter set: Current Channel: 6
  > Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
  > Tag: Country Information: Country Code US, Environment Indoor
  > Tag: EDCA Parameter Set
  > Tag: ERP Information
  > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  > Tag: Vendor Specific: Airgo Networks, Inc.
  > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Data Transfer

Exercise 2

7. **Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt).**
   - **7.1. What are three MAC address fields in the 802.11 frame?**
     BSS Id, source address and destination address
   - **7.2. Which MAC address in this frame corresponds to the wireless host(in Hexadecimal Representation)?**
     00:13:02:d1:b6:4f
   - **7.3. Which MAC address in this frame corresponds to the access point ?**
     00:16:b6:f4:eb:a8
   - **7.4. Which MAC address in this frame corresponds to the first-hop router?**
     00:16:b6:j7:1d:51
   - **7.5. What is the IP address of the wireless host sending this TCP segment?**
     192.168.1.109
   - **7.6. What is the destination IP address?**
     128.199.245.12.
   - **7.7. Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.**

     The destination MAC address of the frame, is different from the destination IP address of the IP packet contained within this frame.

8. **Find the 802.11 frame containing the SYNACK segment for this TCP session.**
   - **8.1. What are three MAC address fields in the 802.11 frame?**
     BSS id: 00:16:b6:f7:1d:51
     Destination: 00:13:02:d1:b6:4f
     source address: 00:16:b6:f4:eb:a8.
   - **8.2. Which MAC address in this frame corresponds to the host?**

The destination address, 00:13:02:d1:b6:4f

8.3. Which MAC address in this frame corresponds to the access point?
00:16:b6:f4:eb:a8

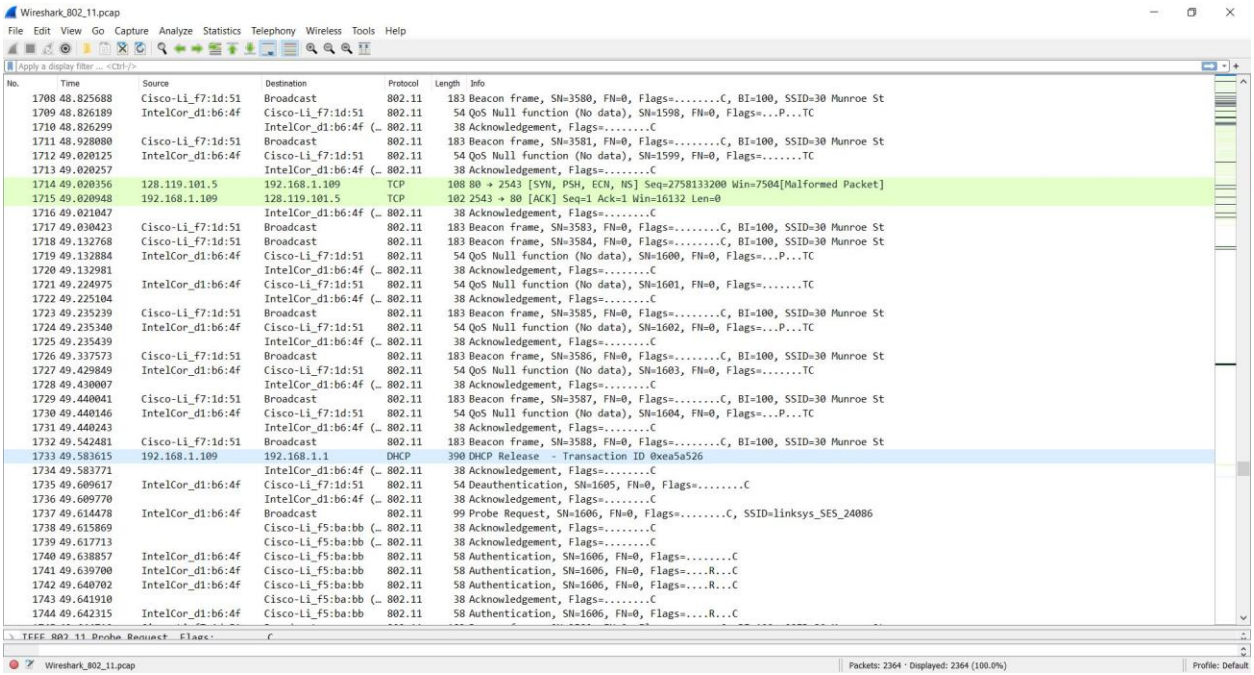
8.4. Which MAC address in this frame corresponds to the first-hop router?
00:16:b6:f4:eb:a8

8.5. Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram?
the IP address of the device that sent the TCP segment is different from the MAC address of the host used in the frame that sends the TCP SYN. The host wireless interface is behaving as if it has two interface addresses

Association and Disassociation

Exercise 3

9. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?
At t = 49.583615 a DHCP release is sent by the host to the DHCP server (whose IP address is 192.168.1.1) in the network that the host is leaving. At t = 49.609617, the host sends a DEAUTHENTICATION frame



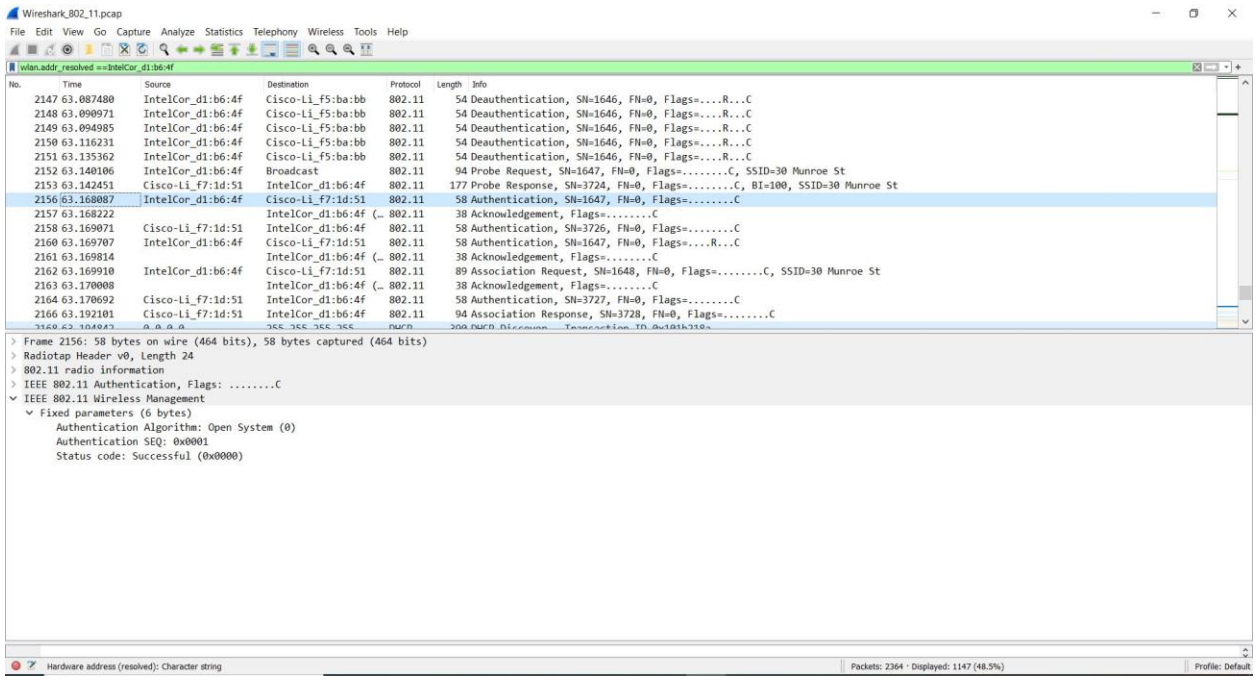
10. **Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49? .**

    There are 17 AUTHENTICATION messages from the wireless host to the linksys_ses_24086 AP.

11. **Does the host want the authentication to require a key or be open?**
    Yes

12. **Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?**
    NO, we cannot see any reply authentication.

13. **Now let's consider what happens as the host gives up trying to associate with the linksys_ses_24086 AP and now tries to associate with the 30 Munroe St AP. Look for AUTHENTICATION frames sent from the host to and AP and vice versa. At what times is there an AUTHENTICATION frame from the host to 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)**



There is an AUTHENTICATION frame from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51 when t = 63.168087. The AUTHENTICATION sent back at t = 63.169071.

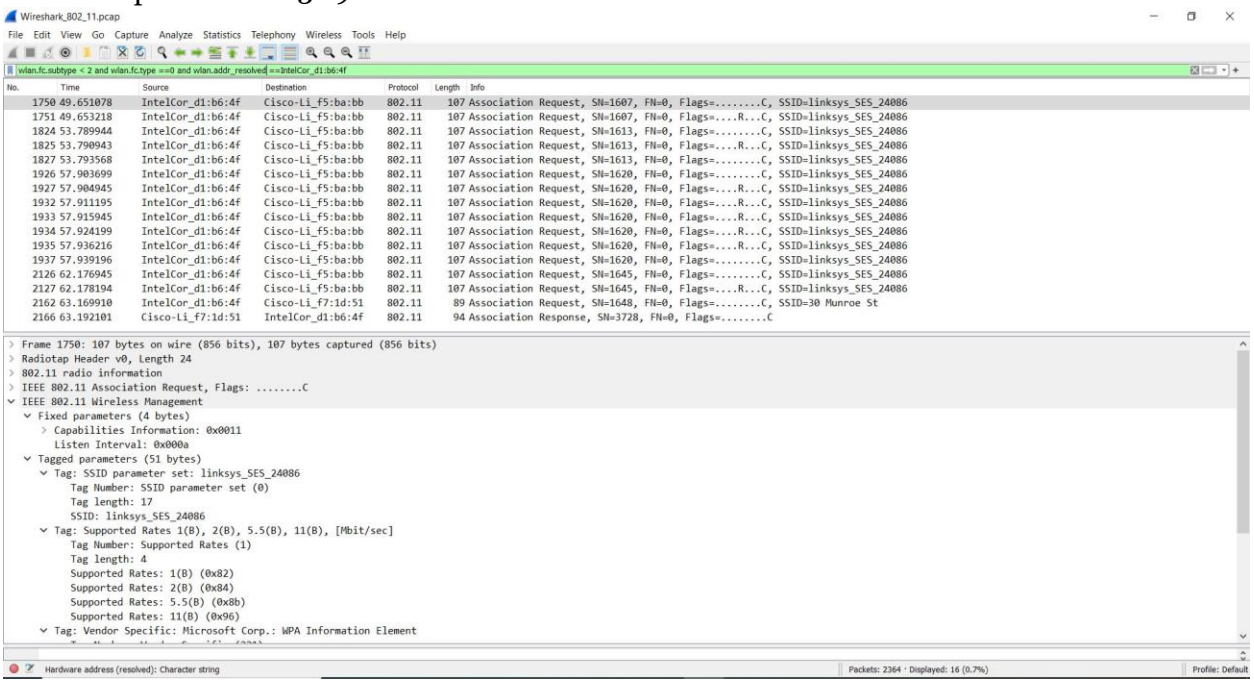
14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to be associated with an AP.

14.1. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP?

At t = 63.169910 seconds

14.2. When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

Replied at t = 63.192101 s



15. To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

15.1. What transmission rates is the host willing to use?

15.2. What transmission rates is the AP willing to use?

The possible rates that willing to use both host and AP are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, 54 Mbps.

Other Frame types

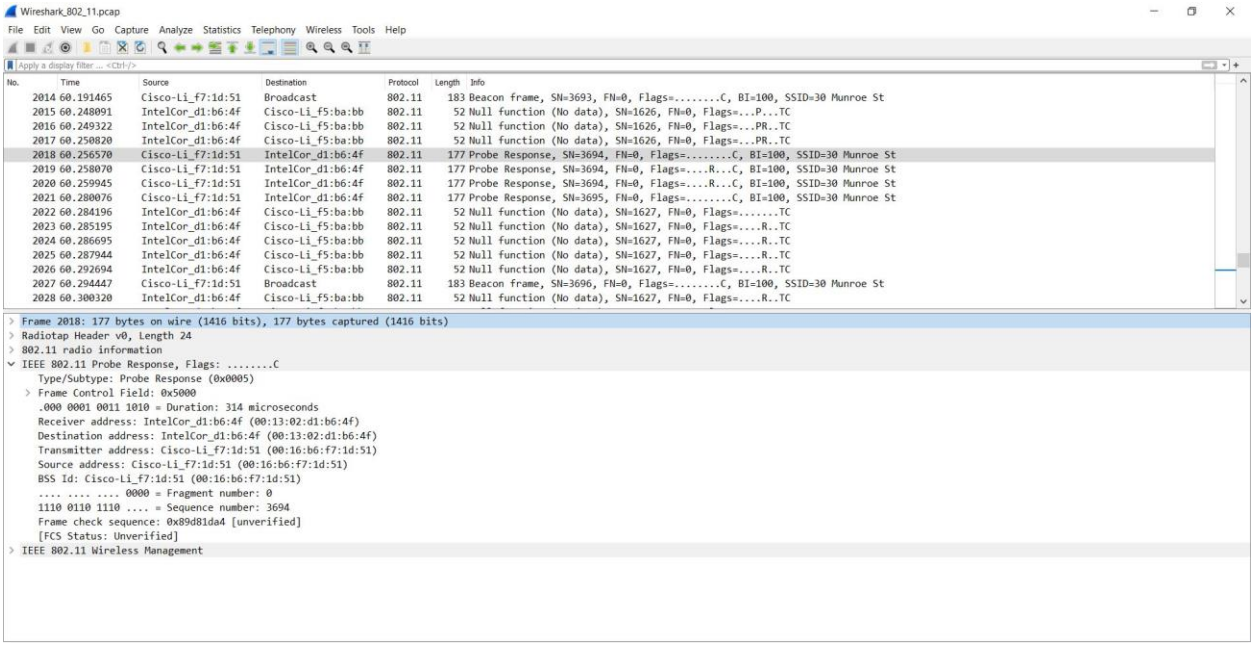
Exercise 4

16. Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.

16.1. What are the sender, receiver and BSS ID MAC addresses in these frames?

Probe request:

Source: 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, BSSID: ff:ff:ff:ff:ff:ff
Probe response:
Source: 00:16:b6:f7:1d:51, destination: 00:16:b6:f7:1d:51, BSSID: 00:16:b6:f7:1d:51



16.2. What is the purpose of these two types of frames?

The probe request is a broadcast to scan for an access point from the host. The probe response is used to response the host from the access point