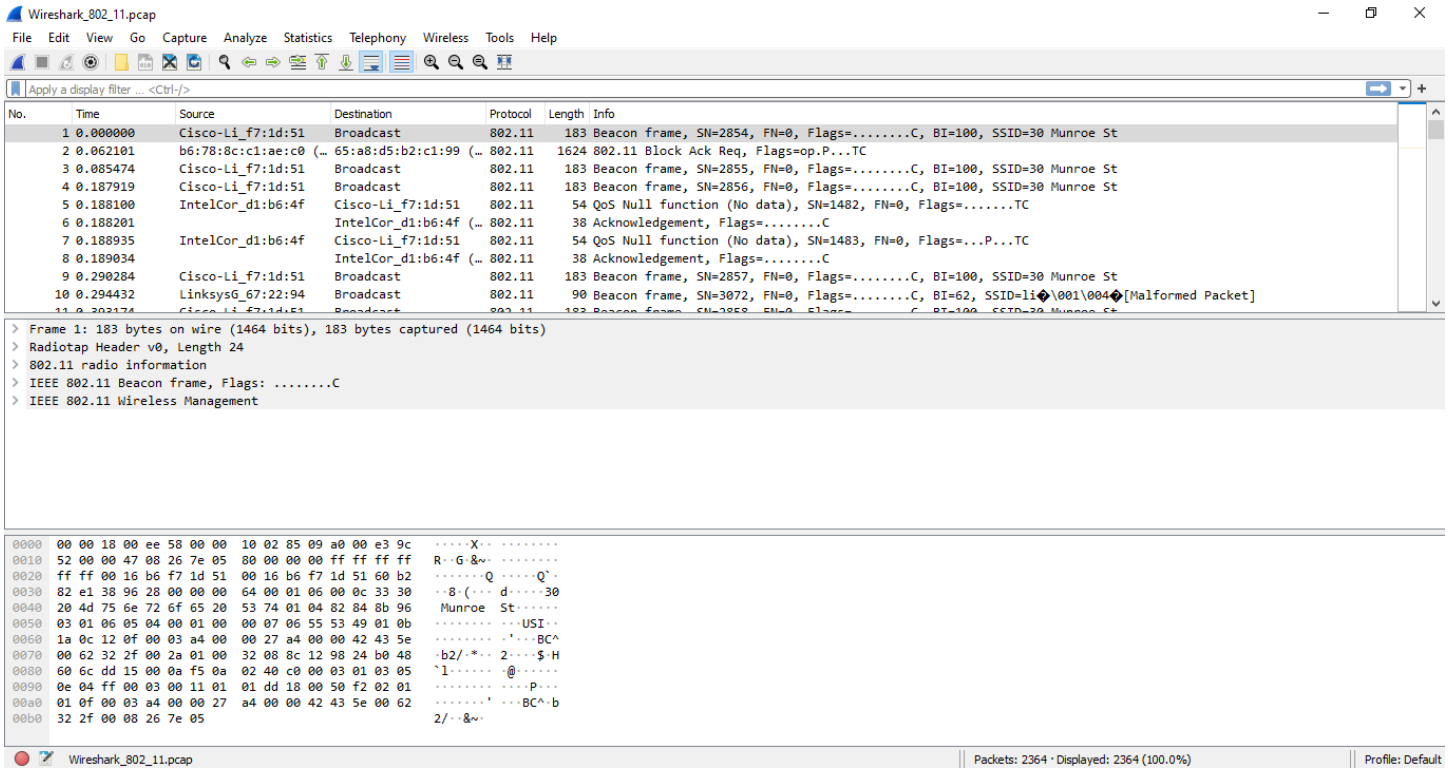
Jayathilaka H.A.D.T.T.

E/16/156

CO513 - Lab 07

Wireless Wireshark Lab - 802.11

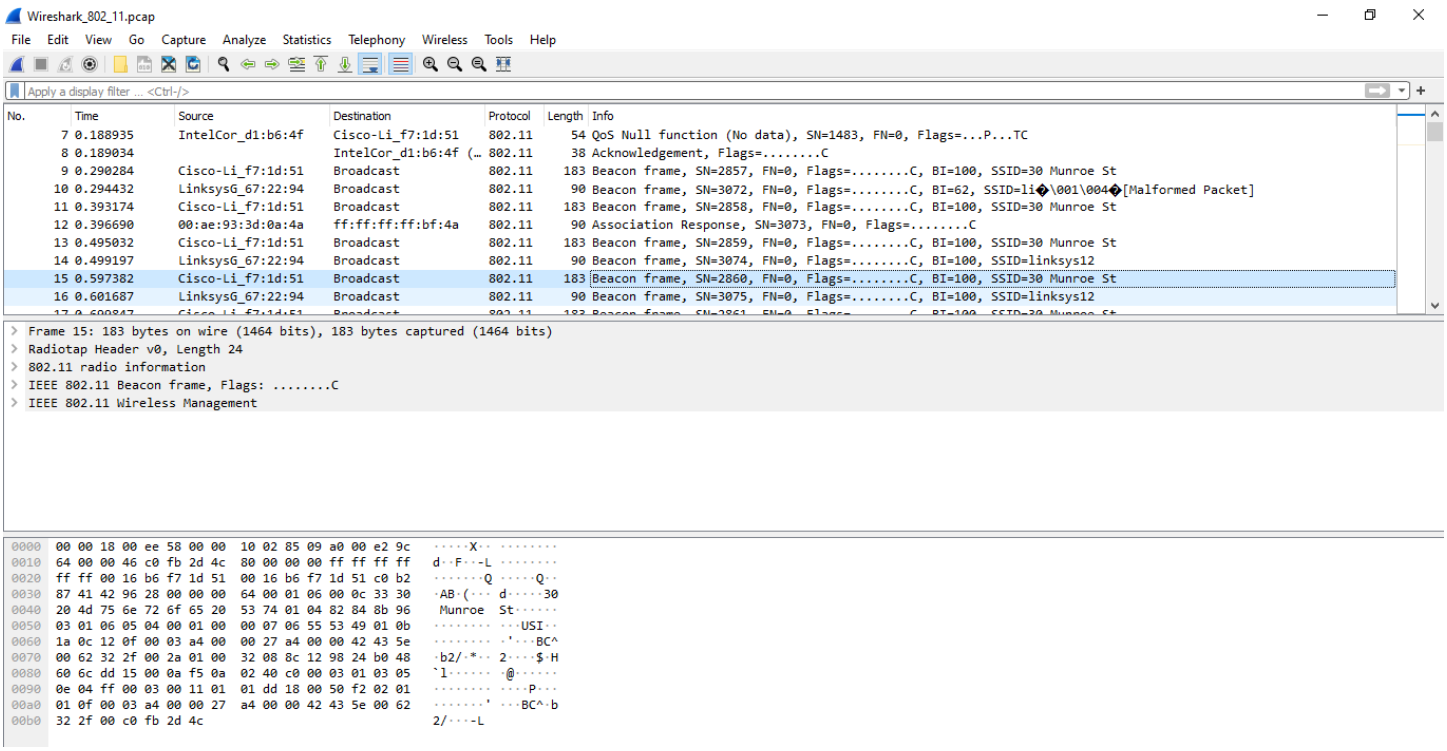


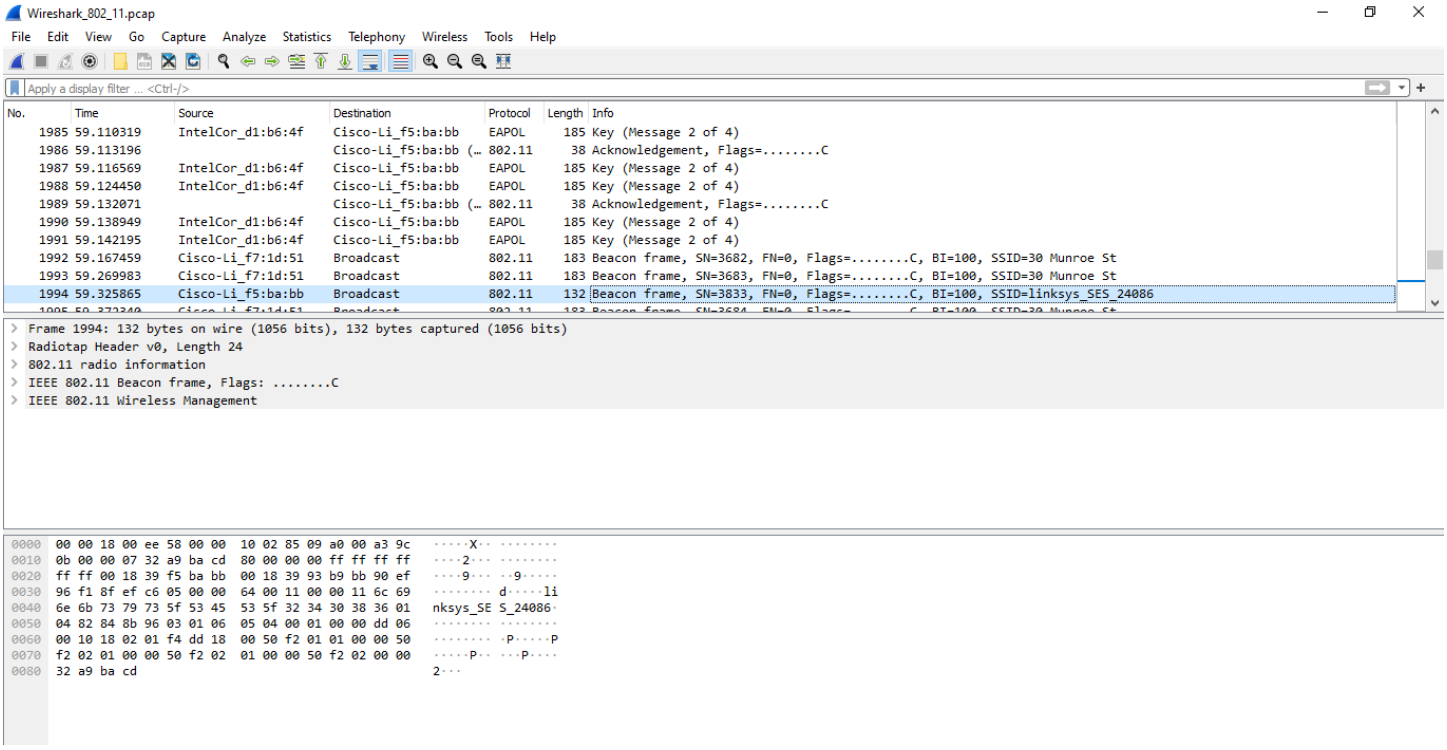
Exercise 1

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

   SSID : linksys_SES_24086





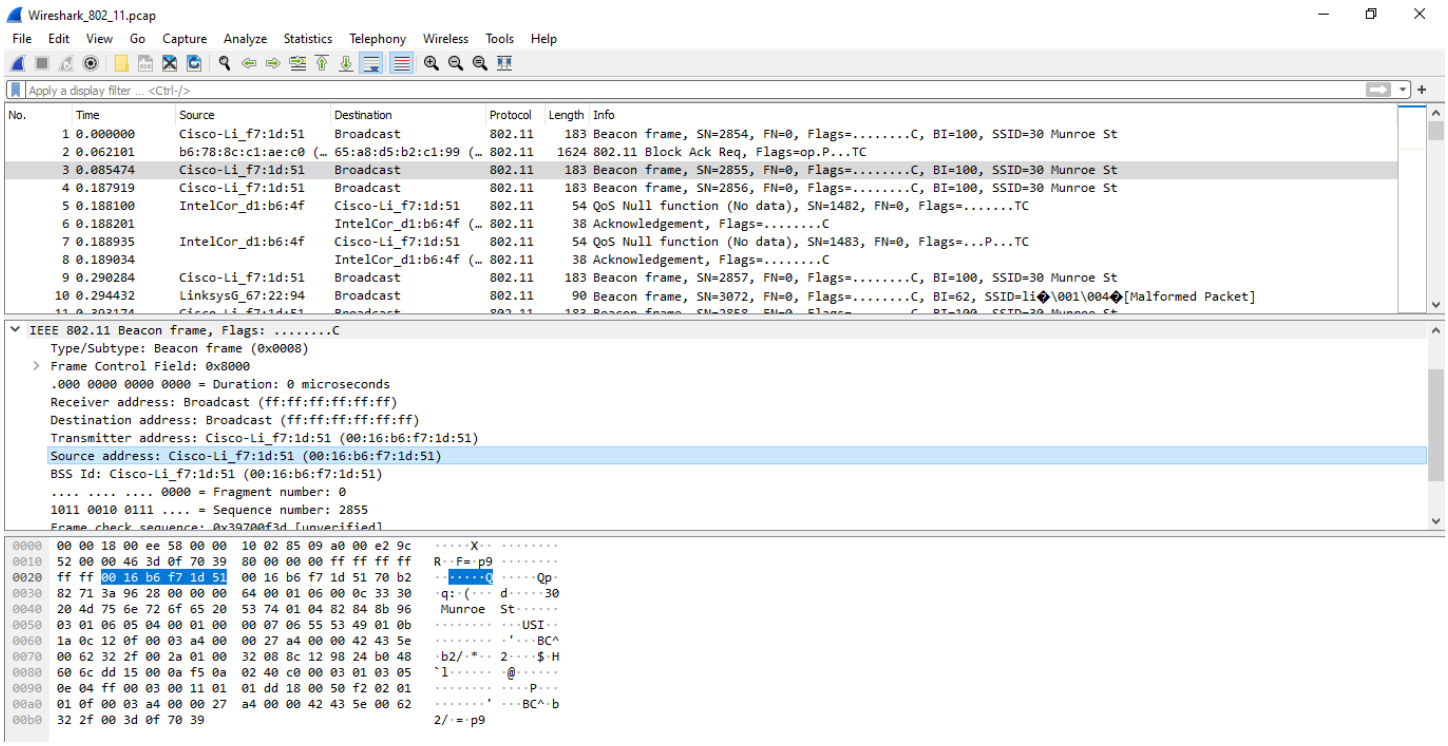
2. What are the intervals of time between the transmissions of the beacon frames and the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

From the 30 Munroe St. access point : 0.1024 s

From linksys_ses_24086 access point : 0.1024 s

3. **What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).**

The source MAC address on the beacon frame from 30 Munroe St 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 address on the beacon frame from 30 Munroe St is ff:ff:ff:ff:ff:ff.

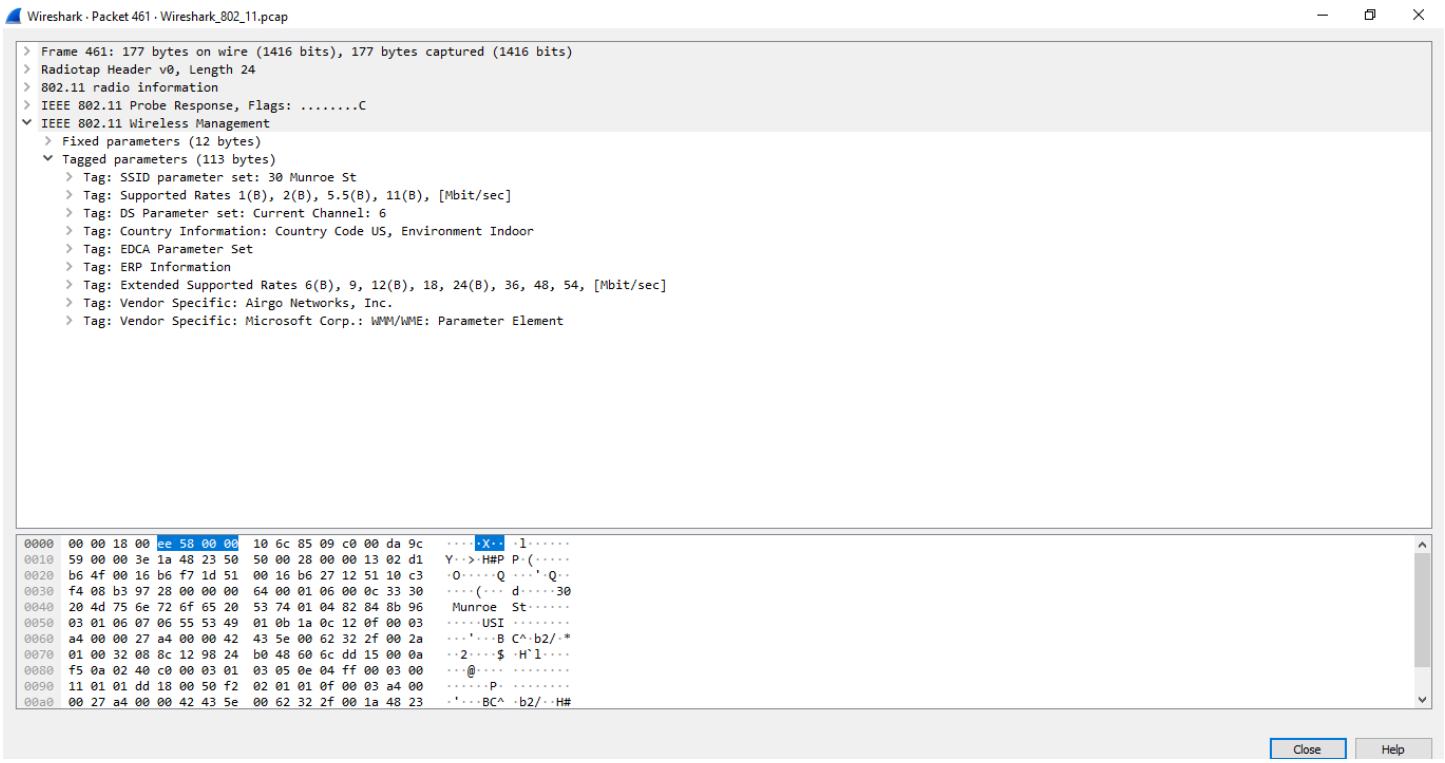
5. **What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?**

The MAC BSS id is 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?**

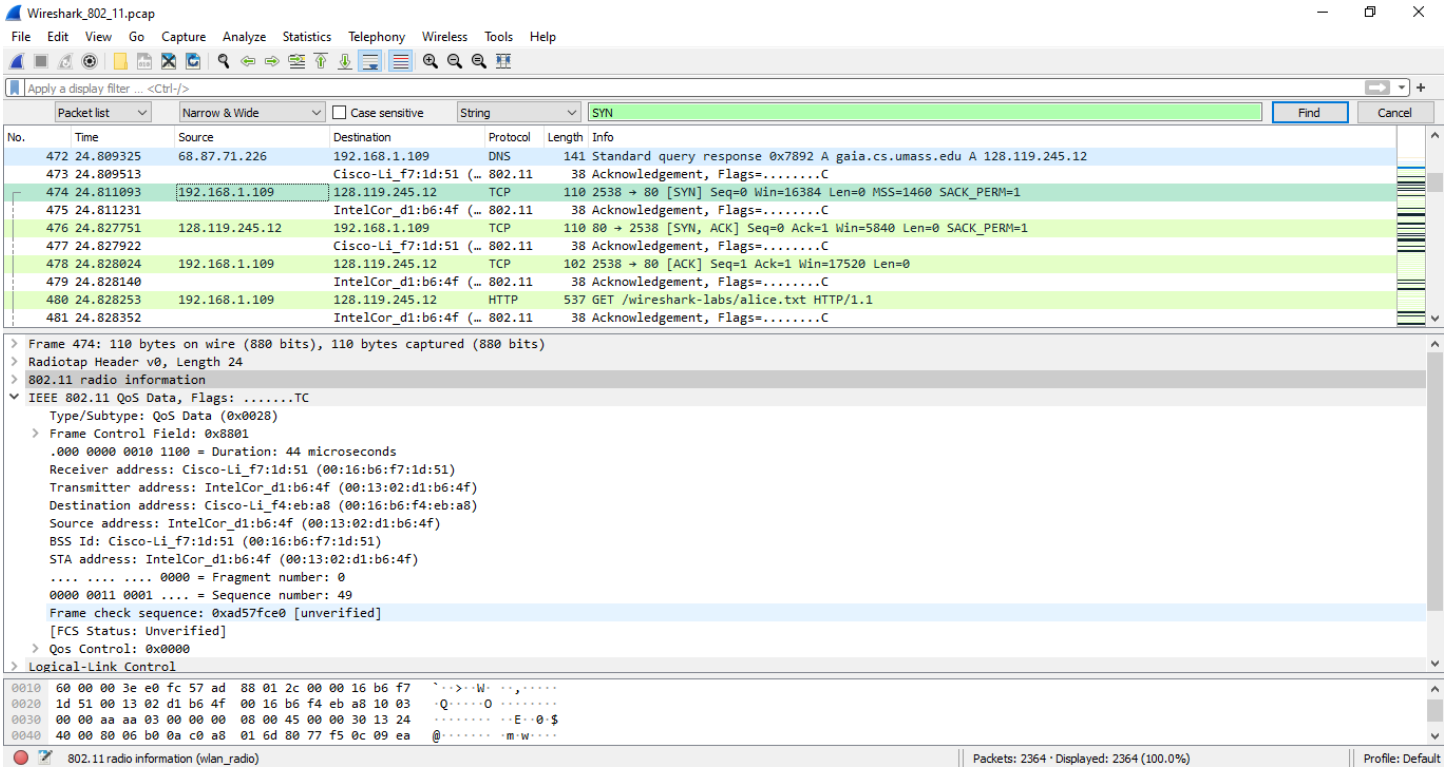
Four data rates : 1.0Mb/s, 2.0Mb/s, 5.5Mb/s, 11.0Mb/s

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



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
- Destination

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:f7:1d:51

7.5. What is the IP address of the wireless host sending this TCP segment?

192.168.1.109

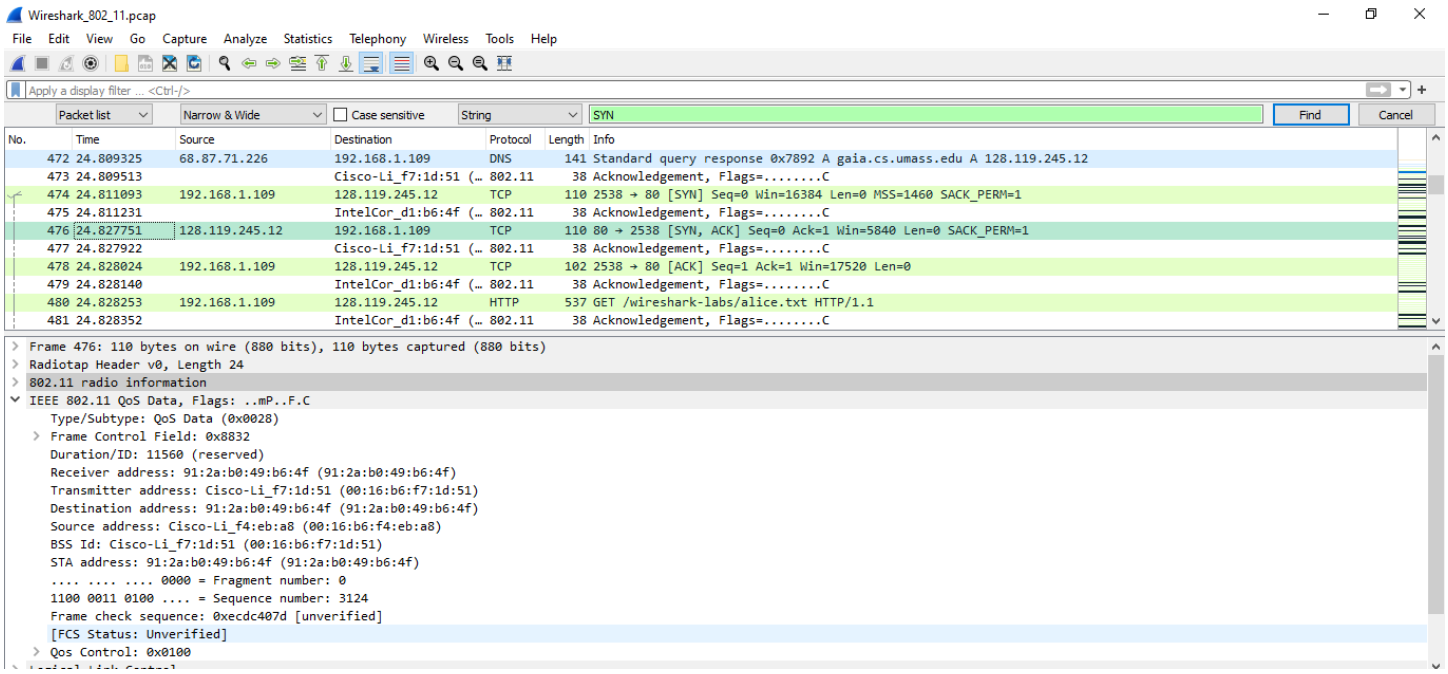
7.6. What is the destination IP address?

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.

Yes, Destination IP address is corresponding to the host. The frame's destination MAC address is not the same as the destination IP address of the IP packet contained within it.

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?

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

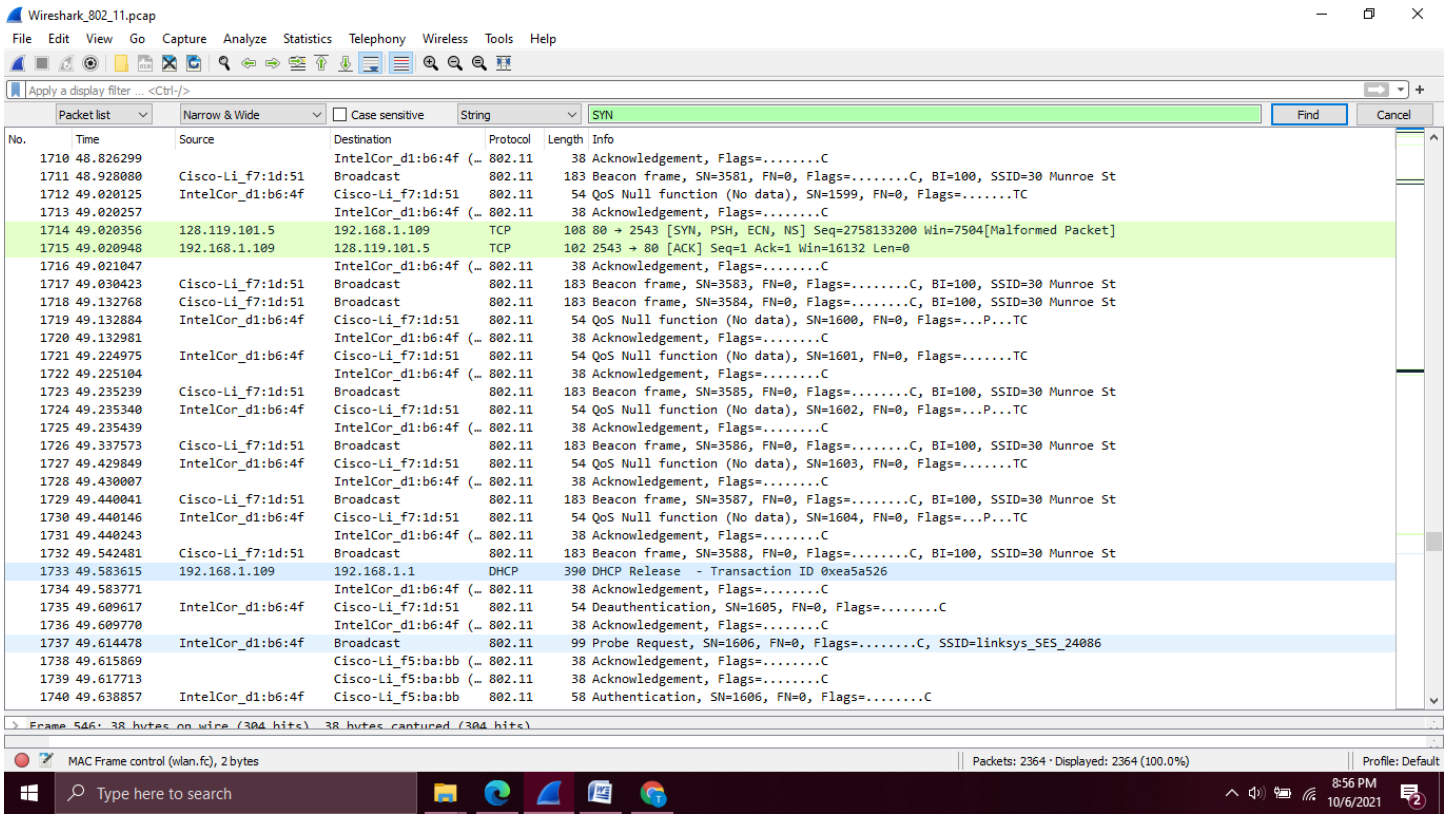
8.5. Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: refer text book in reference list if you are unsure of how to answer this question, or the corresponding part of the previous question).

Because the TCP SYNACK's IP address is 128:199:245:12 and the destination IP address is 192.168.1.109, the sender MAC address in the frame does not correspond to the IP address of the device that transmitted the TCP segment enclosed within this datagram.

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?

- A DHCP release is sent to 192.168.1.1 at t=49.583615
- The host sends a DEAUTHENTICATION frame at t=49.609617



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? .

17 AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP

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

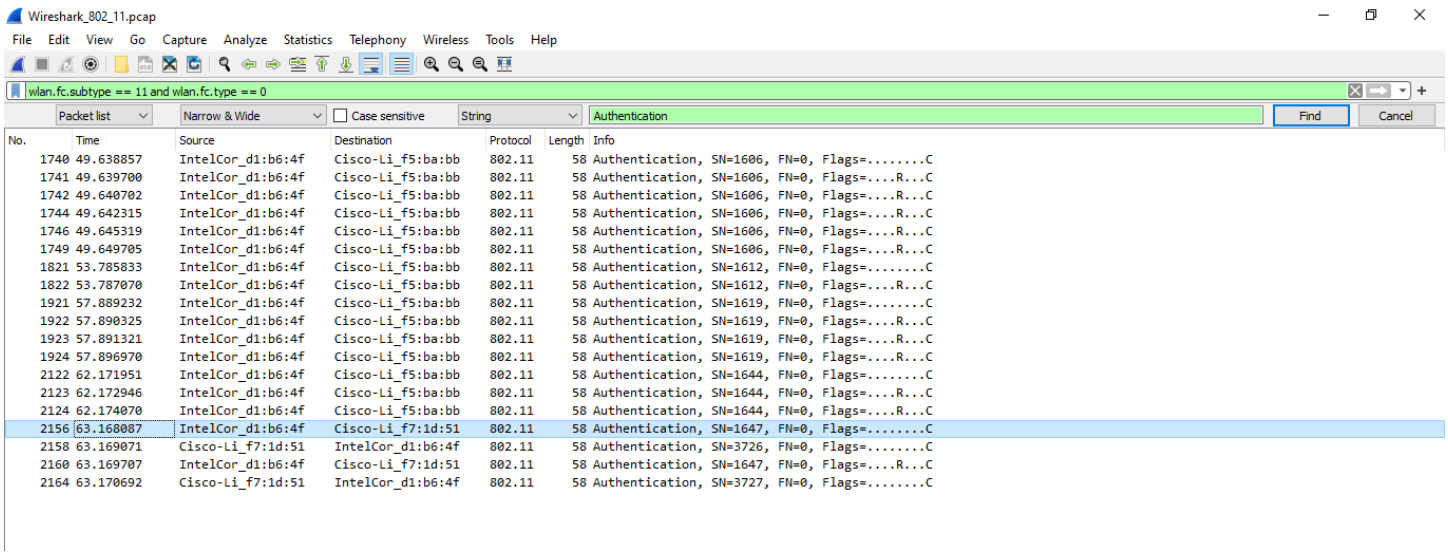
Yes

12. Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?

No

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.)

When t = 63.168087, there is an AUTHENTICATION frame starting at 00:13:02:d1:b6:4f and ending at 00:16:b7:f7:1d:51. At t = 63.169071, the AUTHENTICATION is returned.



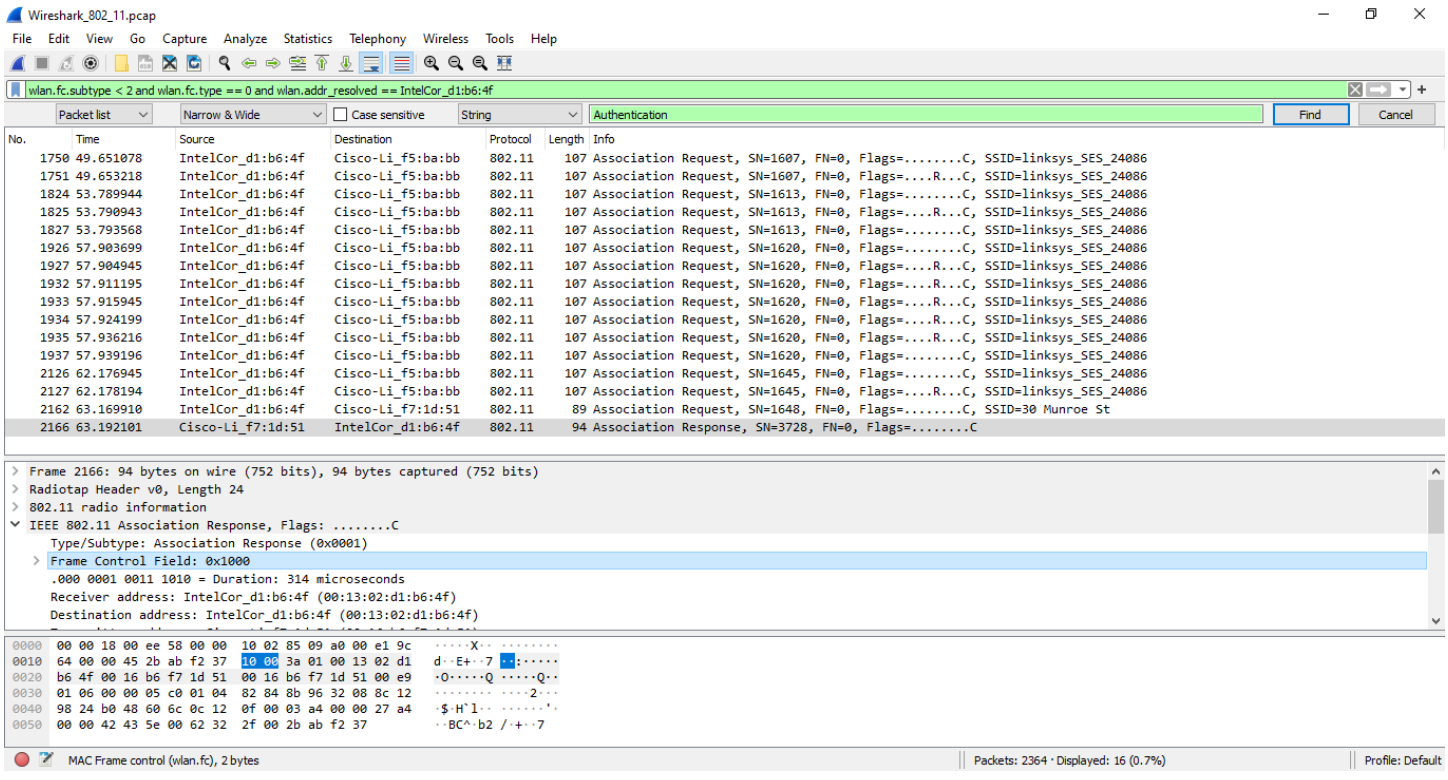
14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to be associated with an AP.

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

At t=63.169910 s

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.)

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?

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

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

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

Exercise 4

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

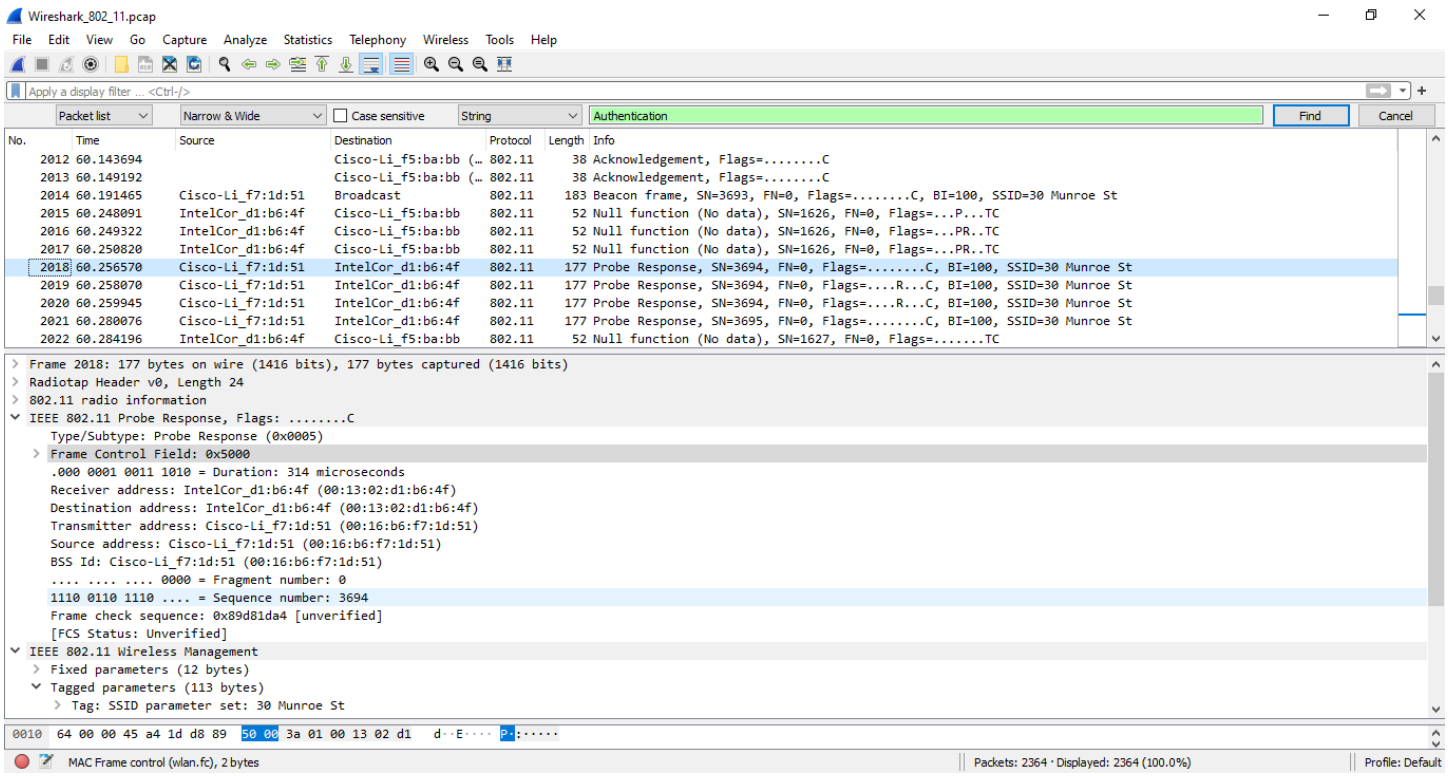
16.1. What are the sender, receiver and BSS ID MAC addresses in these frames?

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? (To answer this last question, you'll need to dig into the online references cited at the end of this lab sheet).

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