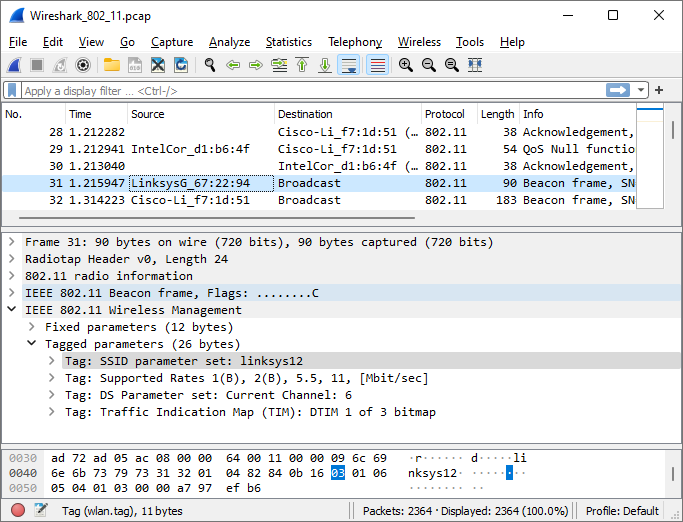
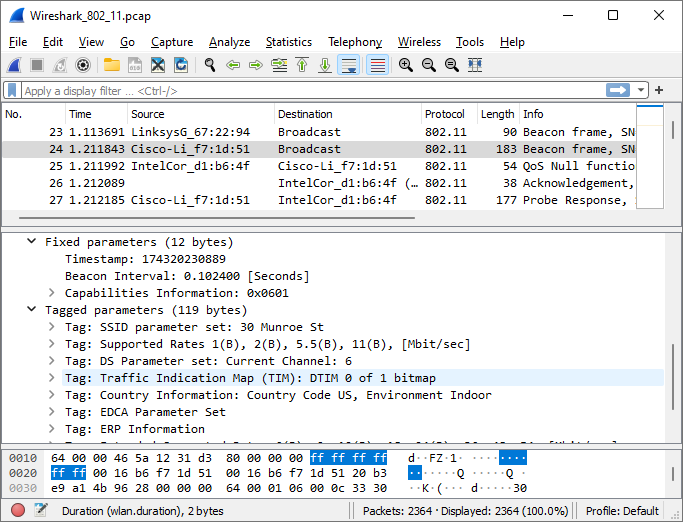
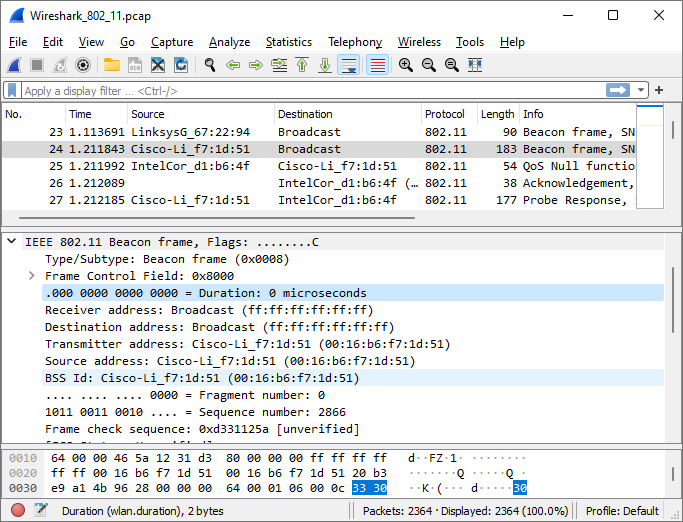
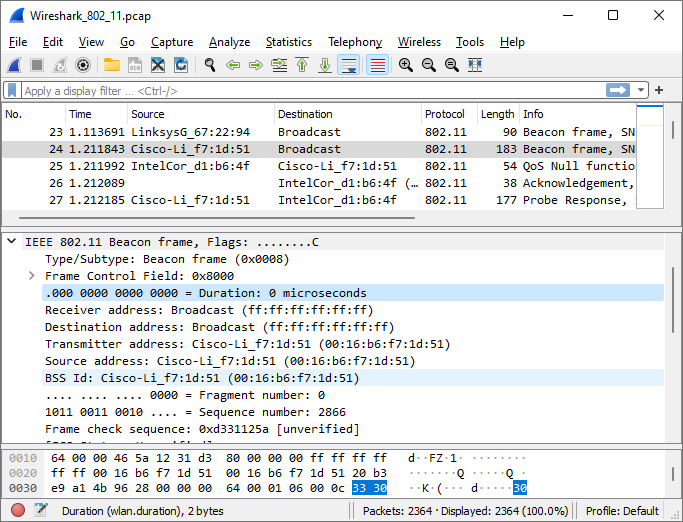
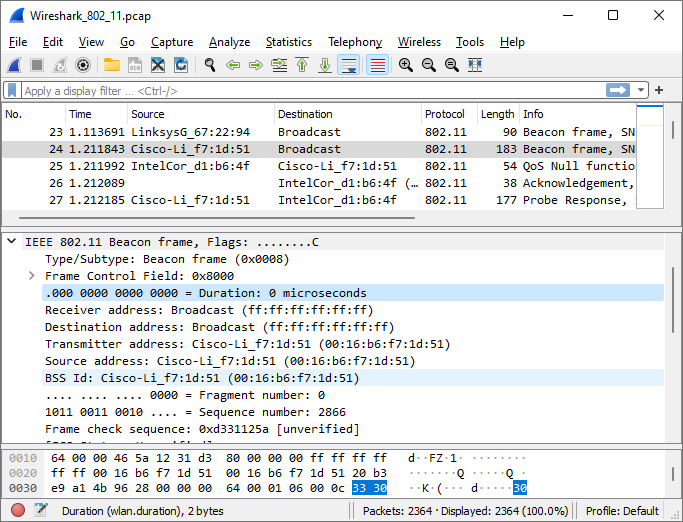
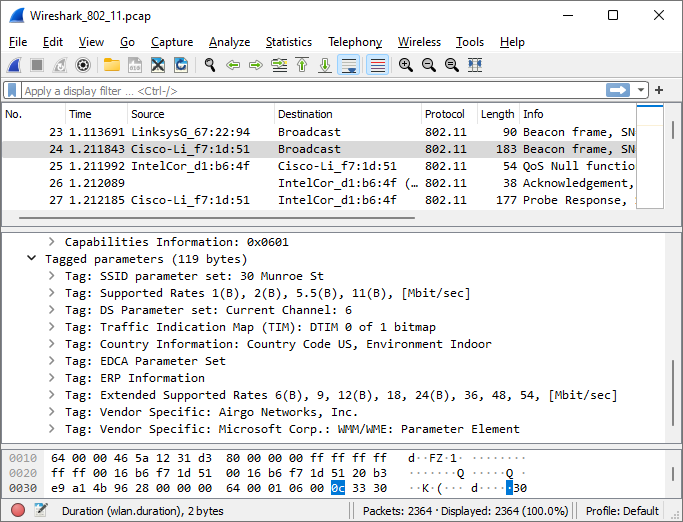
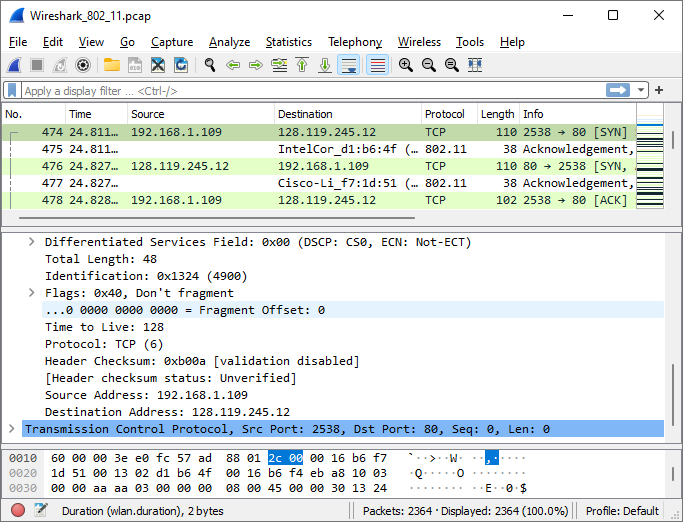
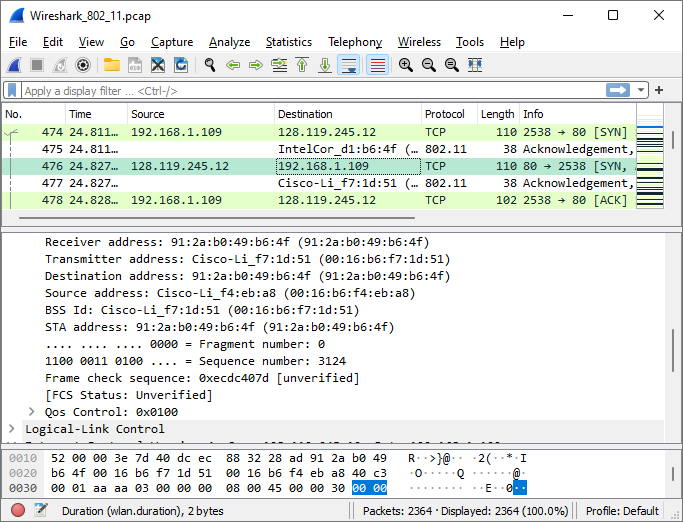
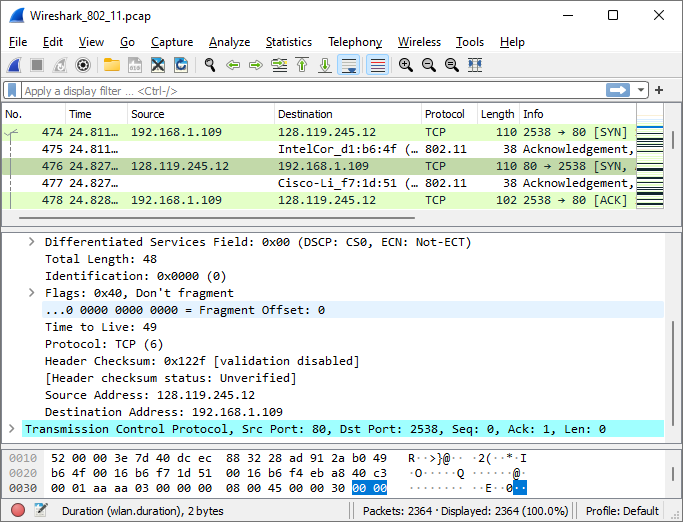
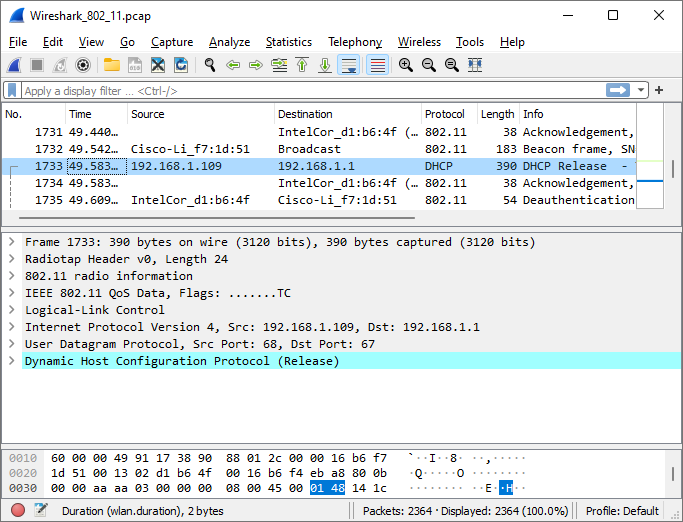
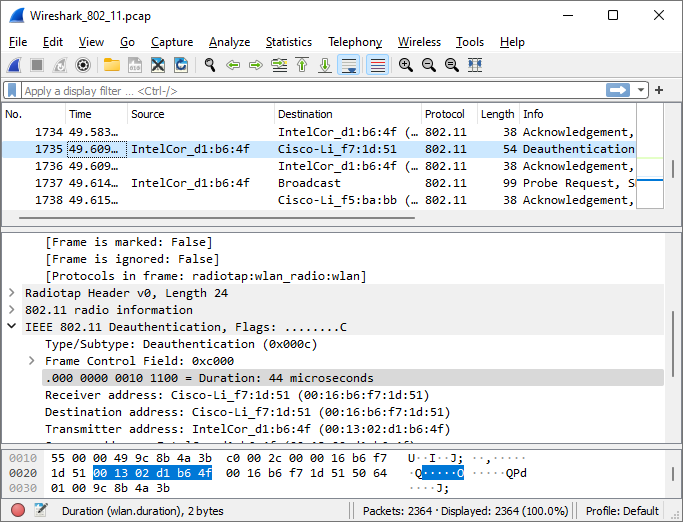
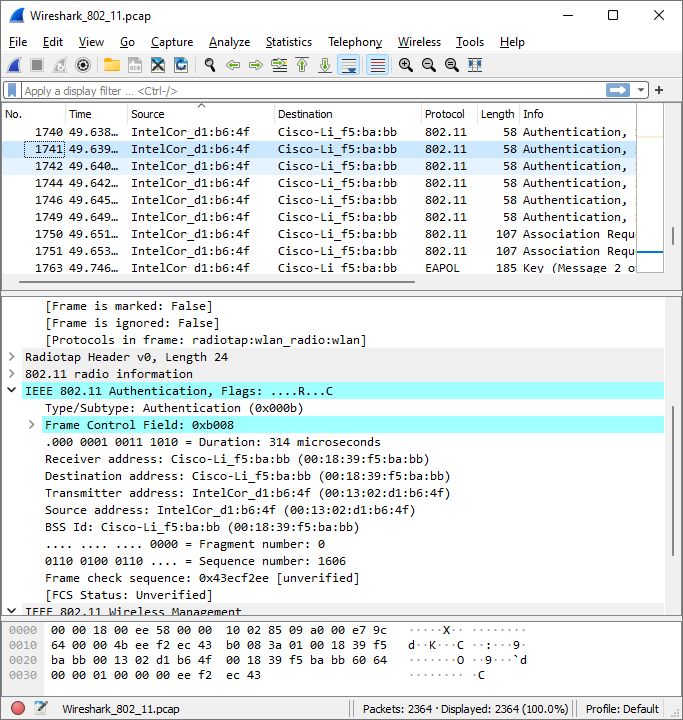
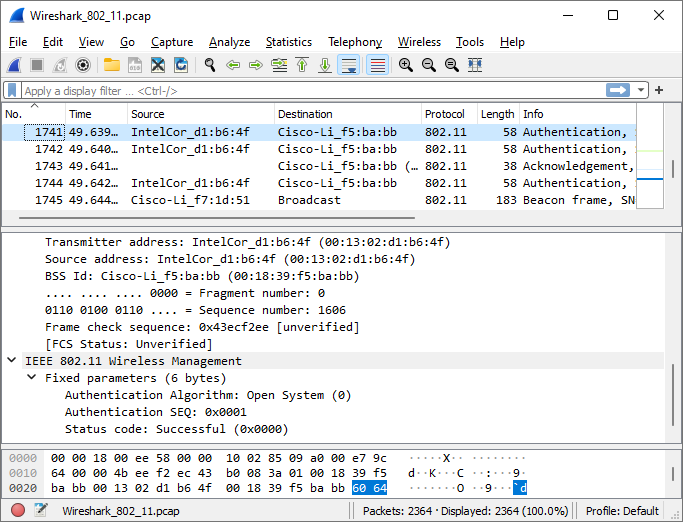
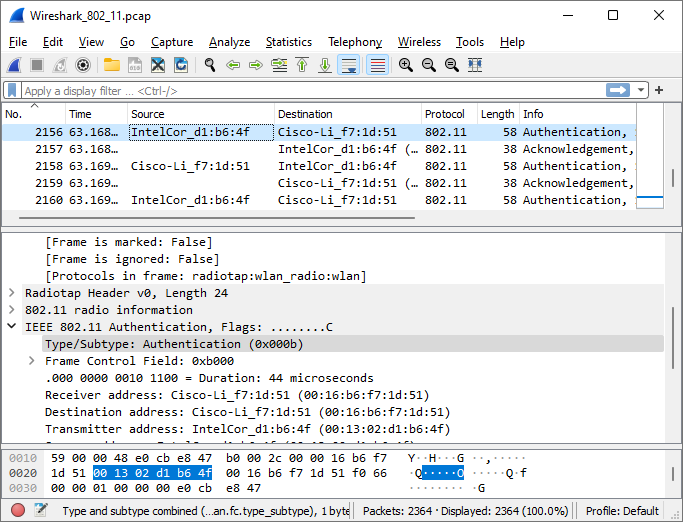
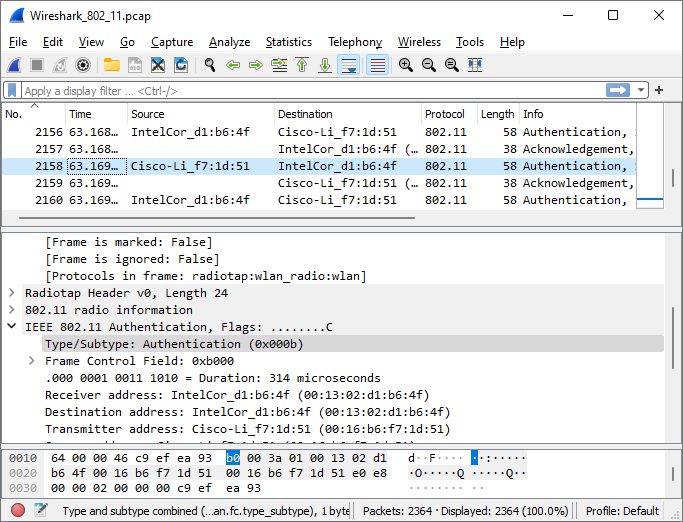
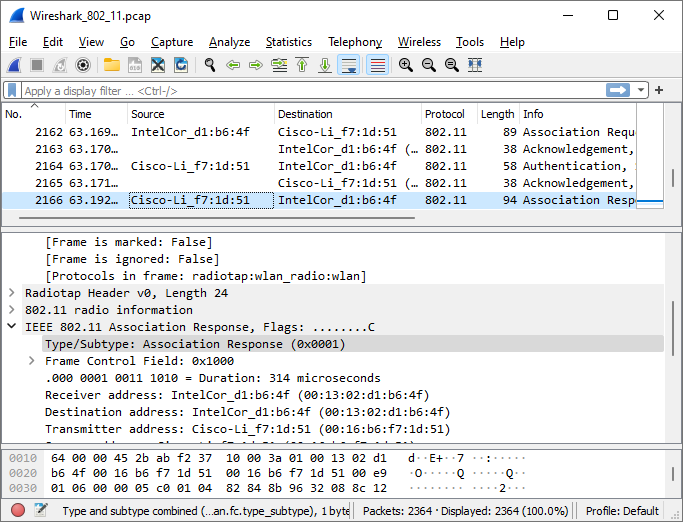
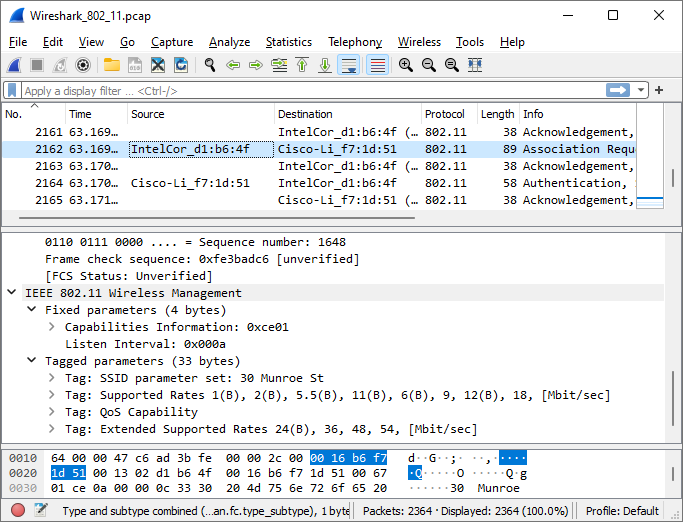
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?
   1. The two most used access points are 30 Munroe St, and linksys12.
   2. Graphical user interface, text, application, email

      Description automatically generated
   3. 
2. What are the intervals of time between the transmissions of the beacon frames 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).
   1. The beacon interval is 0.102400.
   2. 
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).
   1. The source address for 30 Munroe St is 00:16:b6:f7:1d:51
   2. 
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??
   1. The destination address is ff:ff:ff:ff:ff:ff
   2. 
5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?
   1. The BSS ID is 00:16:b6:f7:1d:51
   2. 
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?
   1. The support rates are 1, 2, 5.5, and 11 Mbps. The extended rates are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
   2. 
7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.
   1. The frame containing the SYN segment is frame 474 at time 24.811093. The three MAC address fields are the transmitter, the destination, and the BSS. The MAC address hex value for the transmitter(host) is 00:13:02:d1:b6:4f. The MAC address hex value for the first-hop router (destination) is 00:16:b6:f4:be:a8. The MAC address hex value for the BSS is 00:16:b6:f7:1d:51. The IP address for the host is 192.168.1.109. The IP address for the destination is 128.199.245.12. The destination IP address corresponds to the server.
   2. Graphical user interface, text, application

      Description automatically generated
   3. 
8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? 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: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It’s particularly important that you understand this).
   1. The TCP SYNACK is received on frame 476, or at time 24.827751. The three MAC address fields are the transmitter, the destination, and the BSS. The MAC address hex value for the transmitter(host) is 00:16:b6:f4:eb:a8. The MAC address hex value for the first-hop router (destination) is 91:2a:b0:49:b6:4f. The MAC address hex value for the BSS is 00:16:b6:f7:1d:51. The IP address for the host is 128.199.245.12. The IP address for the destination is 192.168.1.109. The destination IP address corresponds to our computer.
   2. 
   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?
   1. At frame 1733 or at time t=49.583615 a Release action is taken. At frame 1735 or at time t=49.60917 a Deauthentication action is taken. Another action we might have expected to see, but don’t is a Dissociation request.
   2. 
   3. 
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? .
    1. 6 Authentication frames are sent to and from the host, in frame numbers 1740, 1741, 1742, 1744, 1746, and 1749.
    2. 
11. Does the host want the authentication to require a key or be open?
    1. The host wants the authentication to be open, by saying it wants an open system
    2. 
12. Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?
    1. No, I don’t see an Authentication reply in the trace.
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 AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 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.)
    1. One Authentication frame is frame number 2156 and was sent at time 63.168087, and a reply is sent in frame 2158 and was sent at time 63.169071.
    2. 
    3. 
14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? 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.)
    1. The Associate request was sent in frame 2162 at time 63.16991, and the Associate Response is sent in frame 2166 at time 63.192101.
    2. Graphical user interface, text, application

       Description automatically generated
    3. 
15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.
    1. The supported transmission rates the host is willing to use are 1, 2, 5.5, 11, 6, 9, 12, and 18 Mbps. The extended transmission rates the host is willing to use are 24, 32, 48, and 54 Mbps. The supported transmission rates the AP is willing to use are 1, 2, 5.5, 11, 6, 9, 12, and 18 Mbps. The extended transmission rates the AP is willing to use are 24, 32, 48, and 54 Mbps.
    2. 
    3. Graphical user interface, text, application, email

       Description automatically generated
16. What are the sender, receiver and BSS ID MAC addresses in these frames? 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 earlier in this lab).
    1. The sender address in the Probe request frame, frame number 50, is 00:12:f0:1f:57:13. The receiver address is ff:ff:ff:ff:ff:ff. The BSS ID is ff:ff:ff:ff:ff:ff. The sender address in the Probe response frame, frame number 51, is 00:16:b6:f7:1d:51. The receiver address is 00:12:f0:1f:57:13. The BSS ID is 00:16:b6:f7:1d:51. A probe request is used to find an Access Point, and A probe response is sent by the access point to the host.
    2. Graphical user interface, text, application, email

       Description automatically generated
    3. 