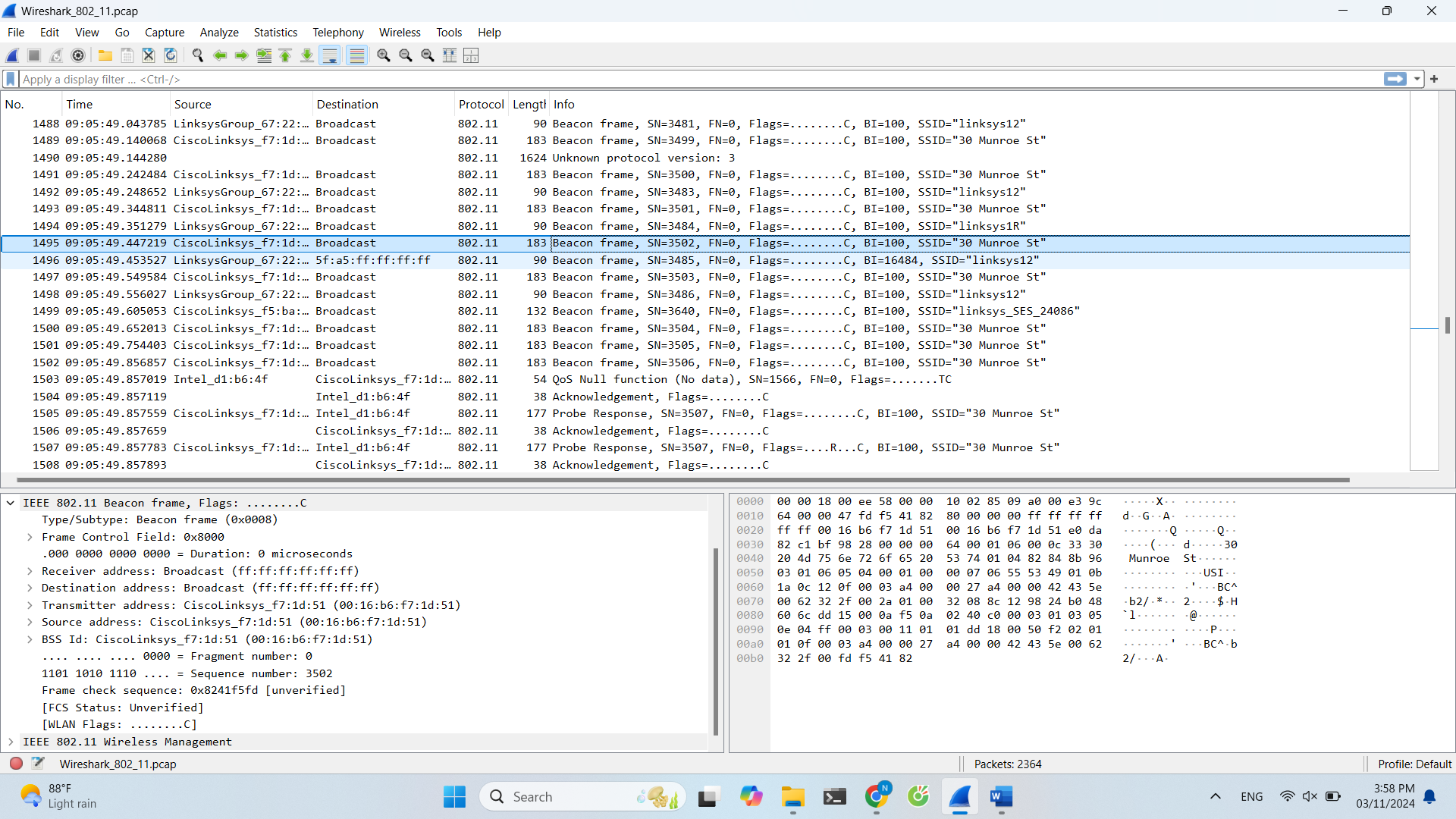
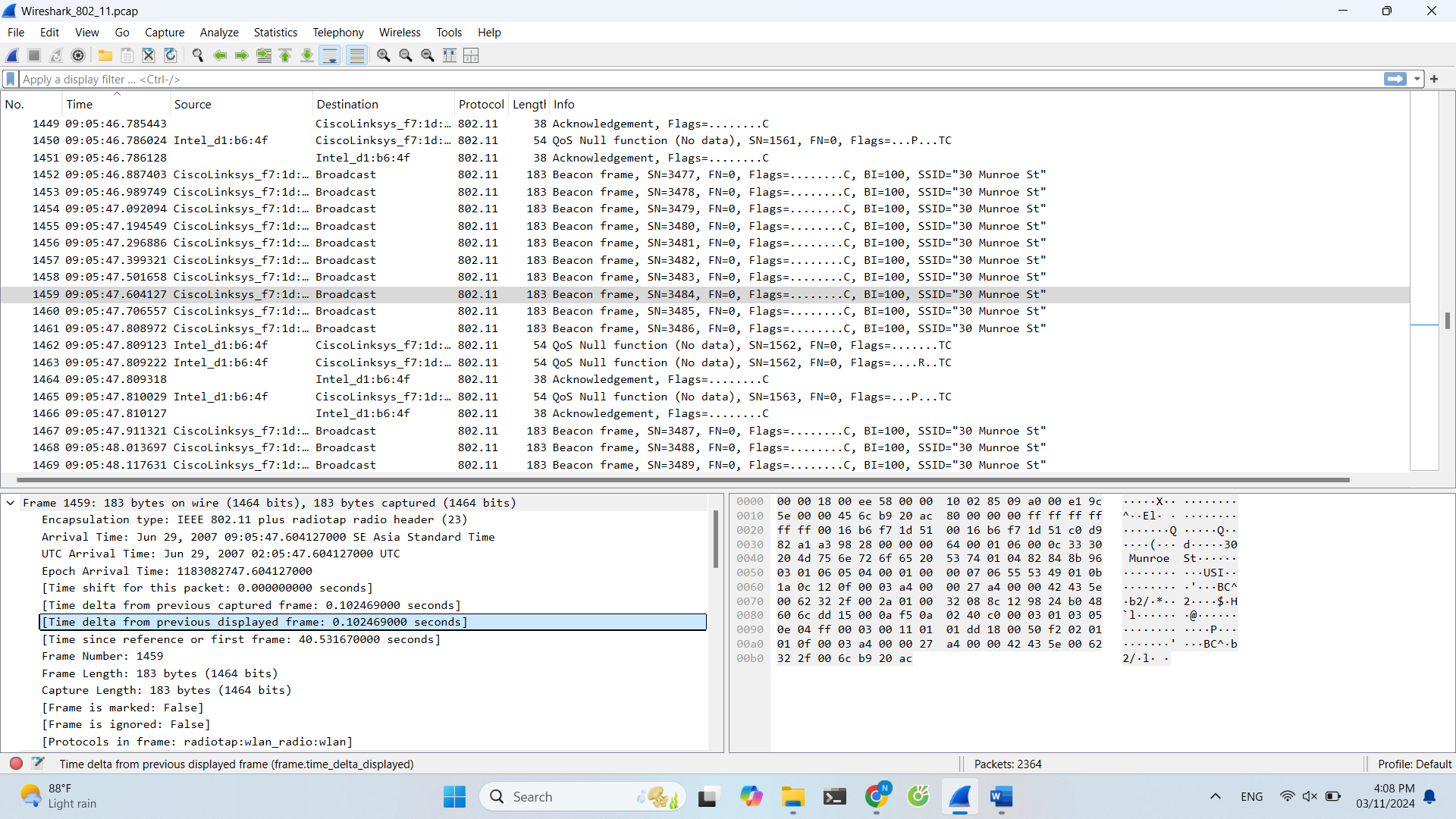
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

Cisco-Li’s SSID is “30 Munroe St”, and LinksysG\_67:22:94’s SSID is “linksys12”

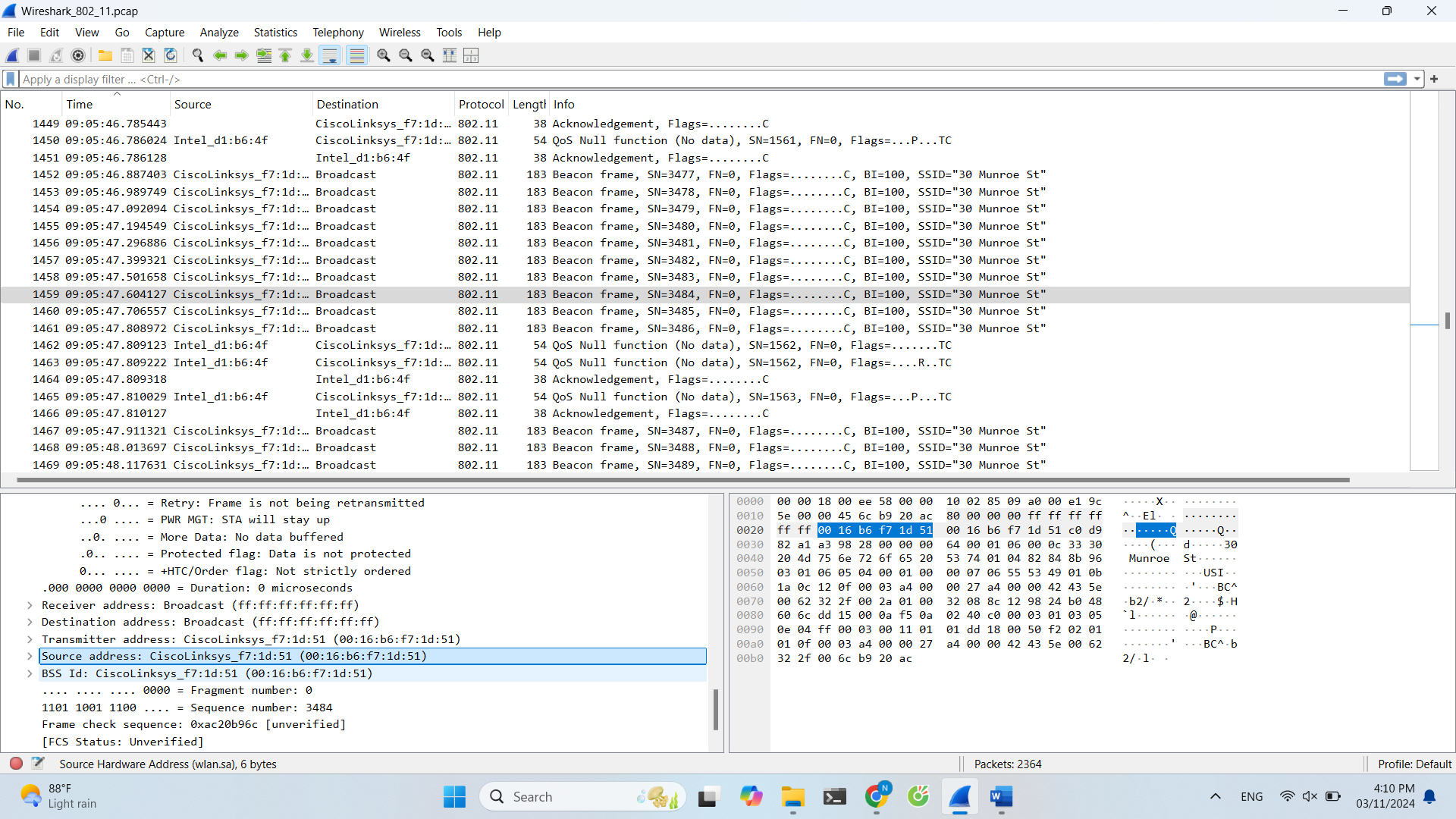


2. What are the intervals of time between the transmissions of the beacon frames the linksys\_ses\_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

Approximately 0.1024 seconds.



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



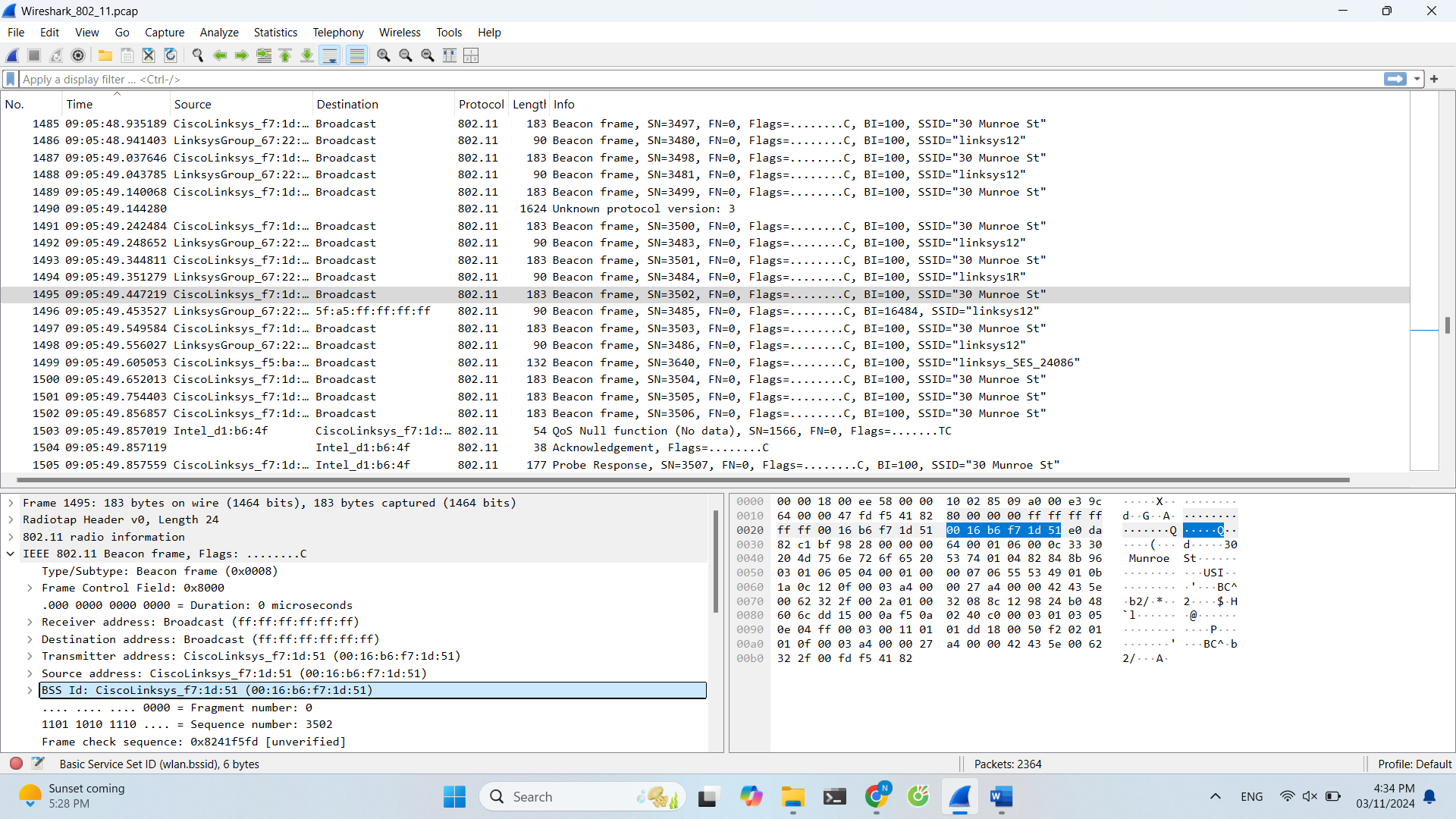
00:16:b6:f7:1d:51

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

Since it is a probing broadcast, it is addressed to ff:ff:ff:ff:ff:ff

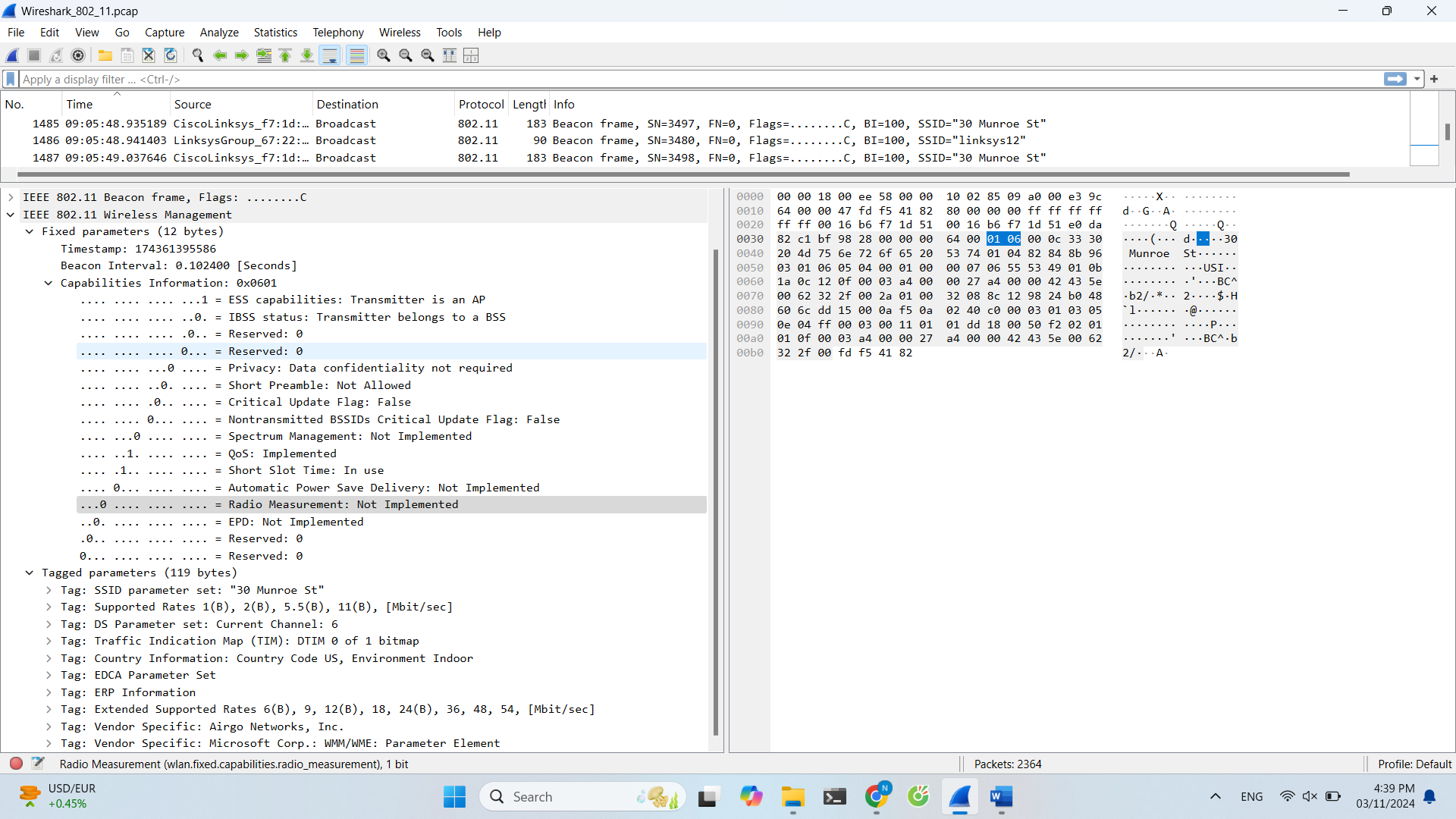
5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

The BSS Id for 30 Munroe is Cisco-LI-f7:1d:51 (00:16:b6:f7:1d:51) which is also the source address



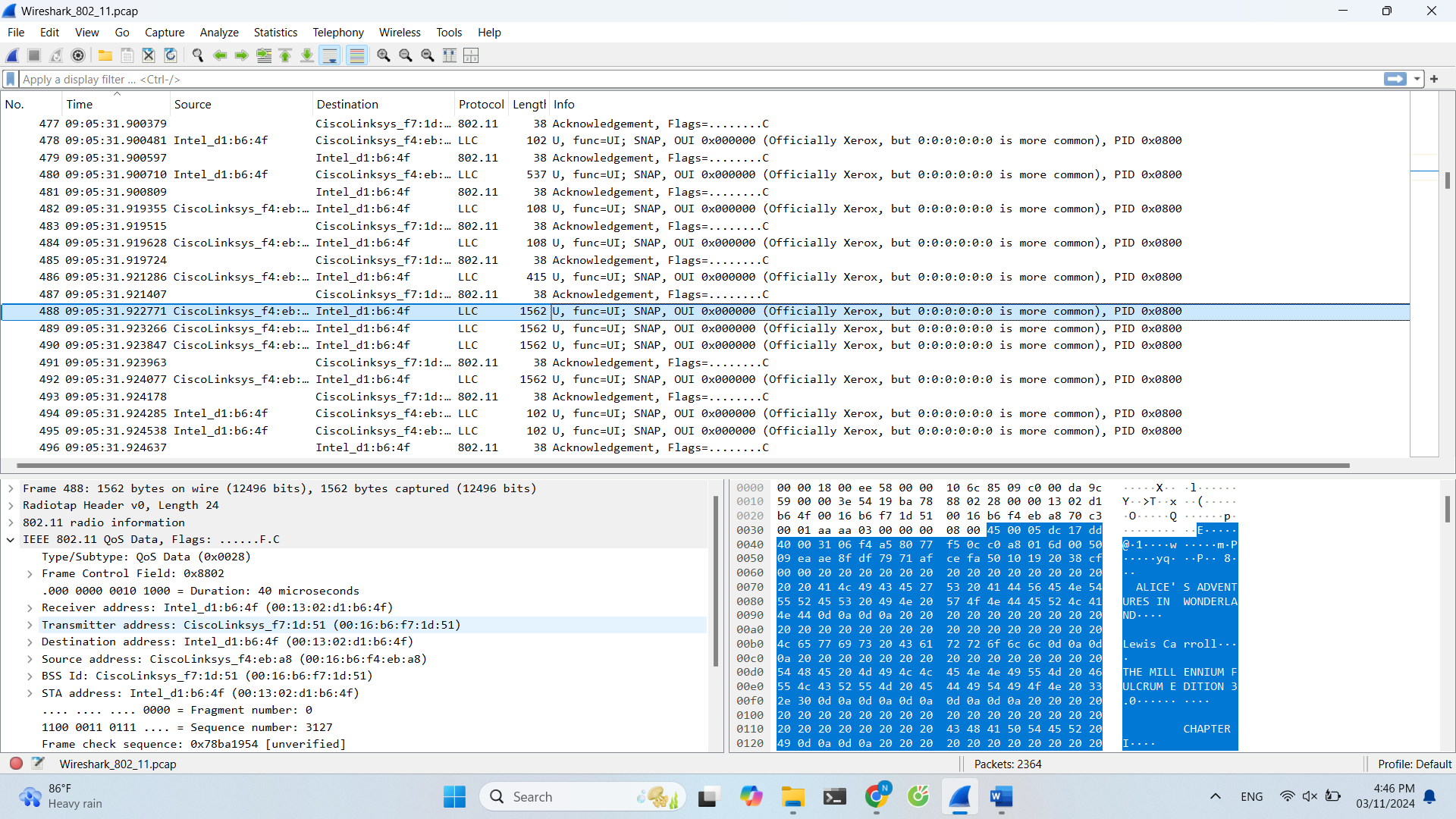
6. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

The four supported rates are 1(B), 2(B), 5.5(B) AND 11(B). The 8 Extended Unsupported Rates are 6(B), 9, 12(B), 18, 24(B), 36, 48 and 54. All these rates are measured in Mbit/sec.



7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session.

The frame that contains this is No. 488. The three MAC addresses are the Destination Address of 00:13:02:d1:b6:4f, as well as the Source Address & BSS Id, both having a value of 00:16:b6:f7:1d:51. The host is 00:13:02:d1:b6:4f. The access point is 00:16:b6:f7:1d:51, which is also the first hop router.



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?

To end the association with 30 Munroe a Deauthentication is sent out, and only after that is ACK’ed, does the probe request get sent out.

Each frame consists of the following basic components:

a) A MAC header, which comprises frame control, duration, address, and sequence control information;

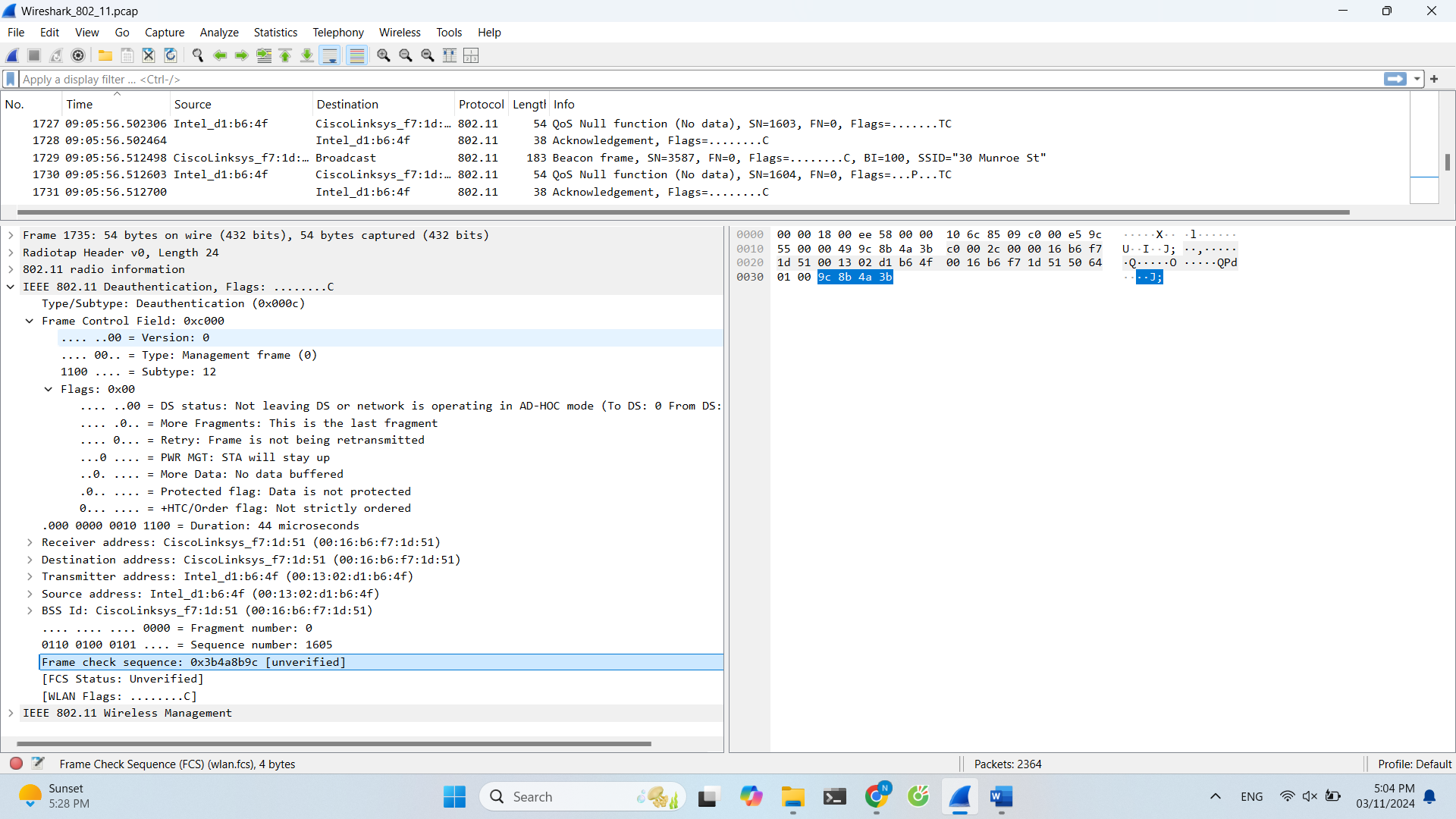
b) A variable length frame body, which contains information specific to the frame type;

c) A frame check sequence (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

I saw a MAC header, specifically, frame control = 0xc000(Normal), duration = 44 microseconds, address: = (destination addr = Cisco-Li\_f7:1d:51 & source addr = InterCor\_d1:b6:4f), and sequence control information(Fragment number = 0, Sequence number = 1605).

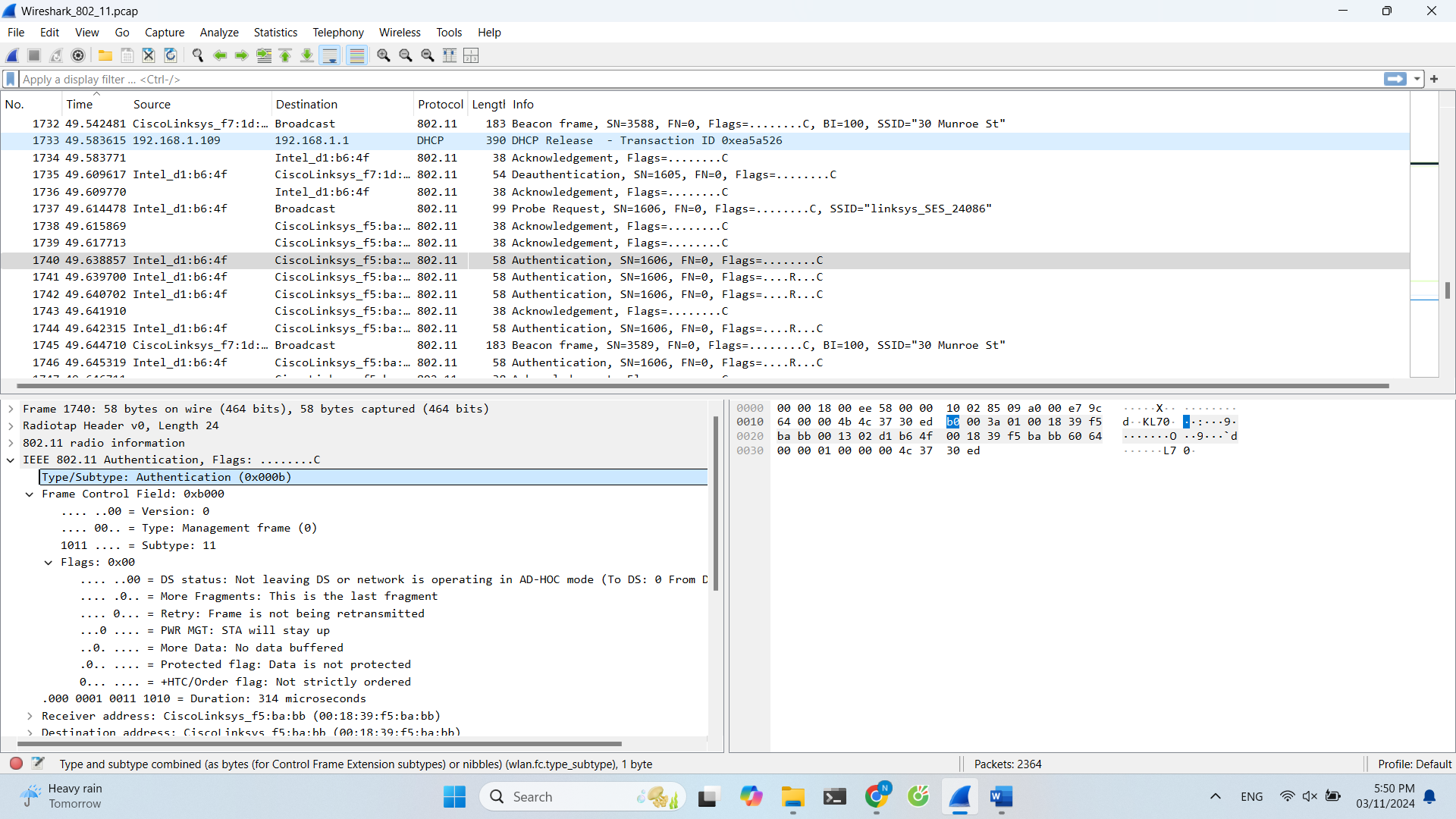
I saw a FCS: 0x3b4a8b9c [unverified]

I, however, did not see a variable length frame body.



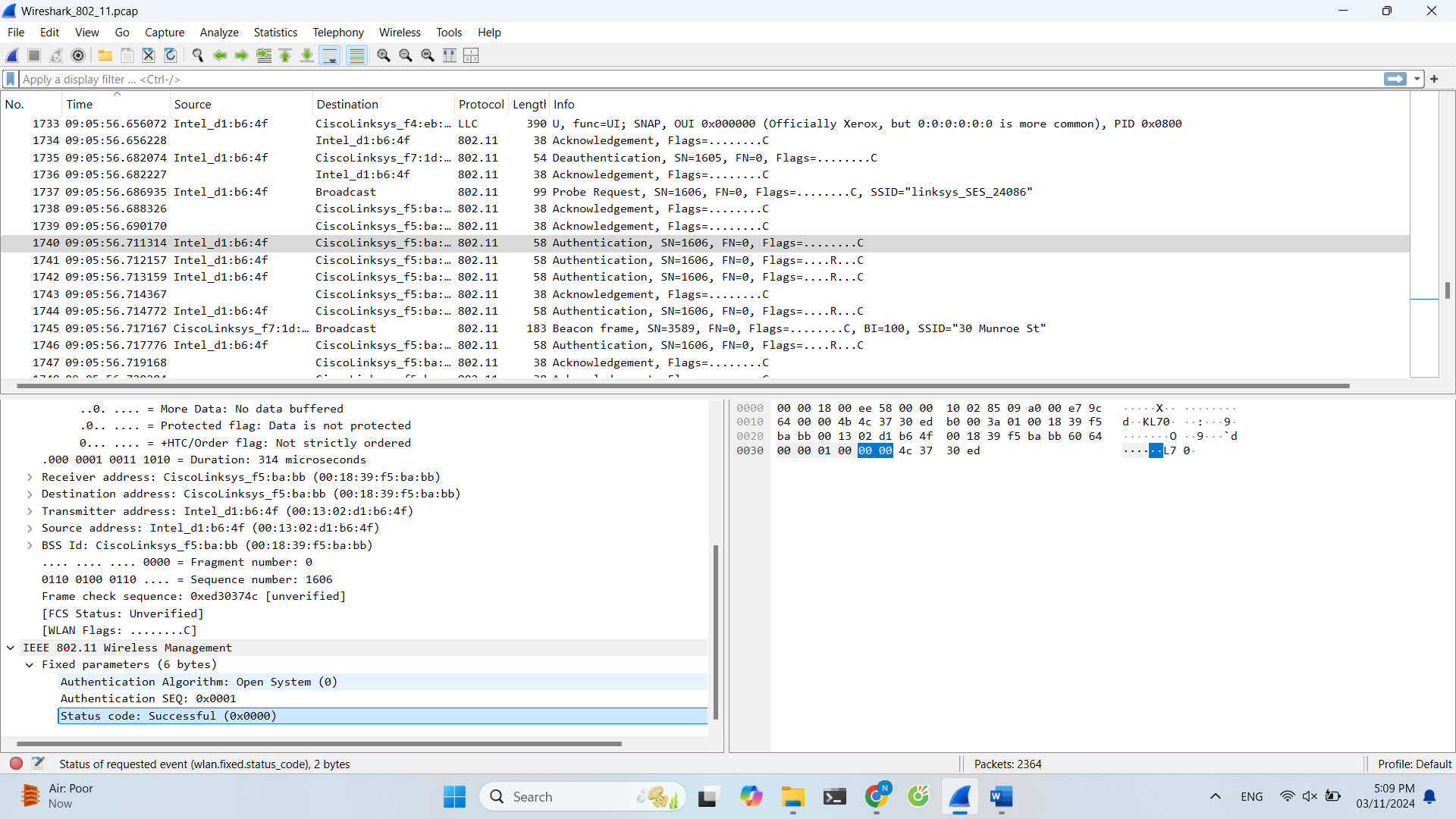
10. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys\_ses\_24086 AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around t=49? .

Answer: the AP received t = 49.638857 messages from the AUTHENTICATION



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

This is contained in the 1740th packet instance, a t = 49.638857, and further located in the IEEE 802.11 wireless LAN management frame. It indicates an Authentication Algorithm field of “Open System (0)”, and Authentication SEQ of 0x0001, as well as a Status Code of Successful, or 0x0000. This is a shared key system

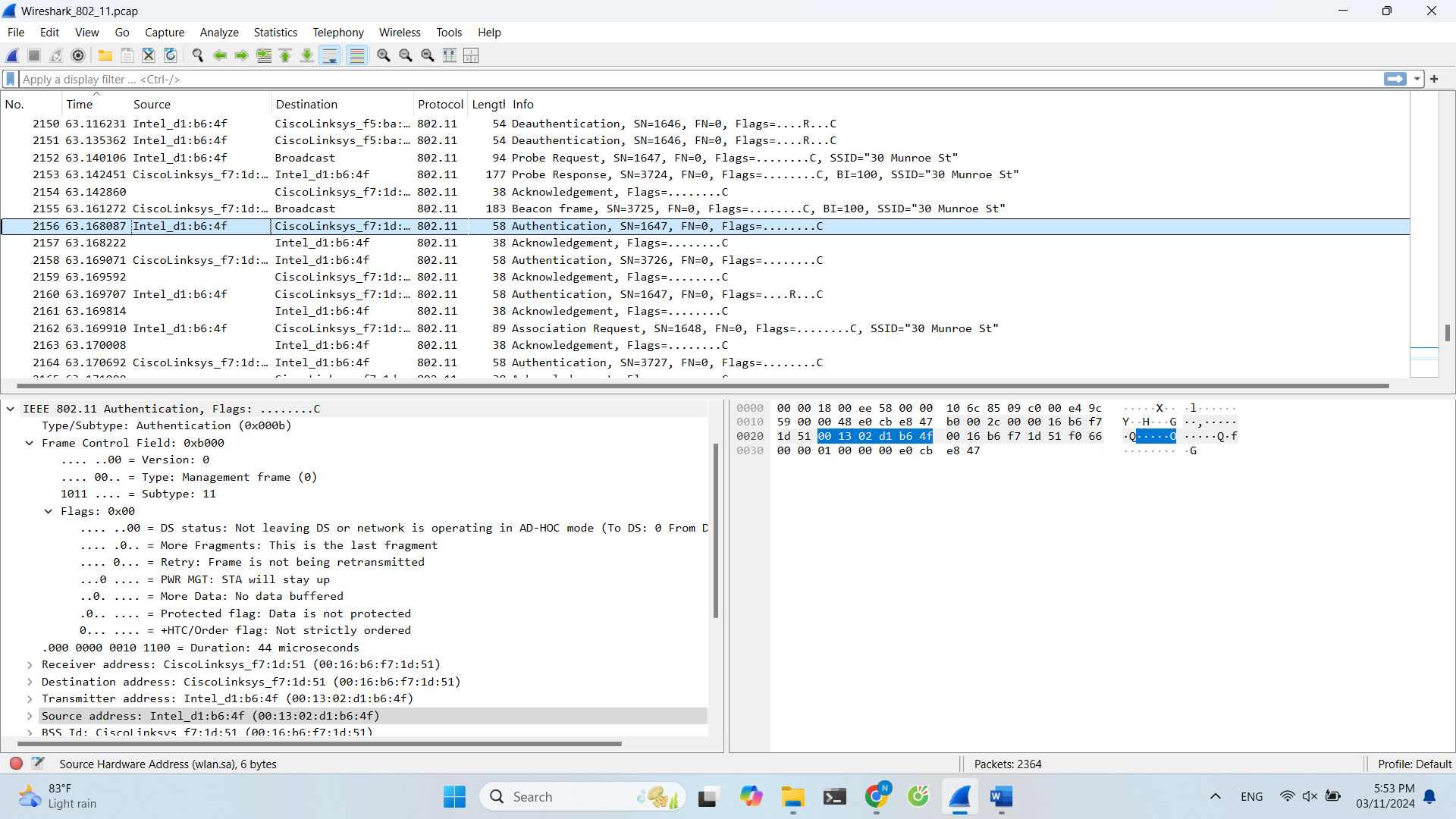


12. Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?

No

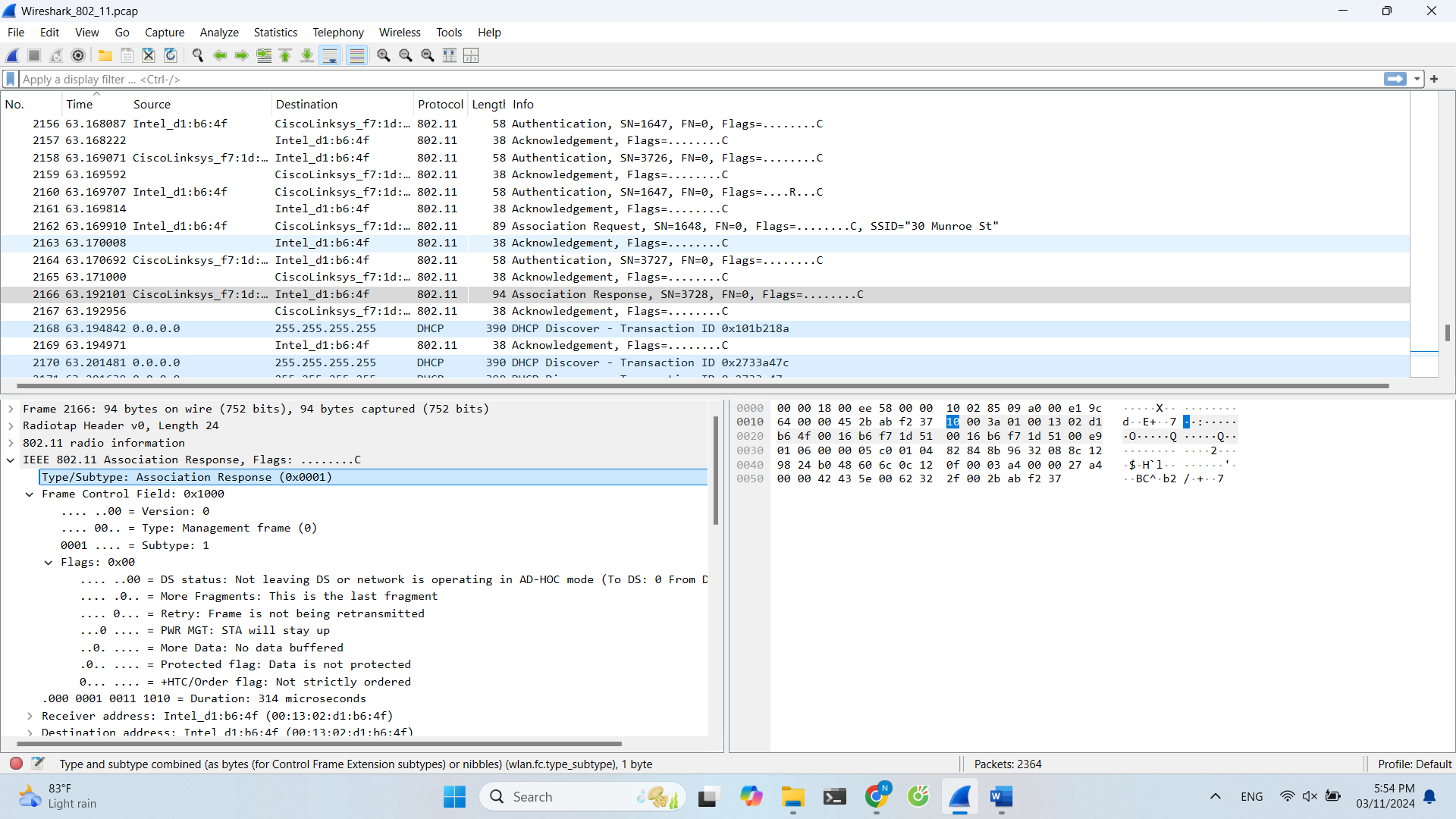
13. Now let’s consider what happens as the host gives up trying to associate with the linksys\_ses\_24086 AP and now tries to associate with the 30 Munroe St AP. Look for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to 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.)

t = 63.168087 there is a authentication frame sent from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51 at t = 63.169071 there is an authentication sent back



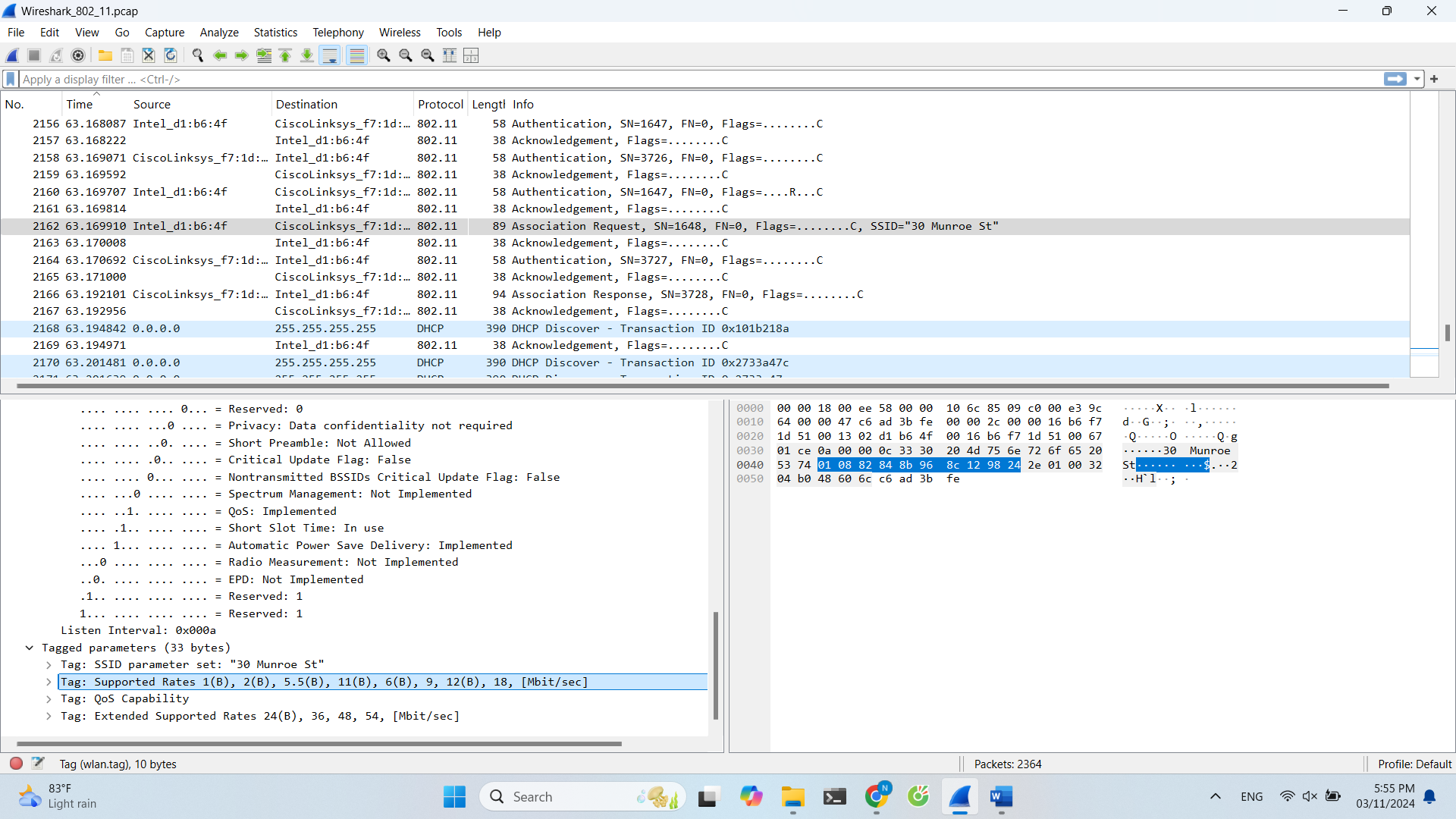
14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the 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.)

t = 63.169910 there is a ASSOCIATE REQUEST frame sent from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51 at t = 63.192101 there is an ASSOCIATE RESPONSE



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.

the host uses ASSOCIATION REQUEST frame. the supported rates are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps



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).

PROBE REQUEST source 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, and BSSID: ff:ff:ff:ff:ff:ff

PROBE RESPONSE source: 00:16:b6:f7:1d:51, destination:00:16:b6:f7:1d:51, and BSSID: 00:16:b6:f7:1d:51

a PROBE REQUEST is used by a host to scan for an Access Point so the PROBE RESPONSE can be sent by the access point to the host.

