**Lab 7 – 802.11**

**IT 520-A – Enterprise Infrastructure & Networks**

**Due Date: April 10th, 2018**

**Michael Weiler**

Instructions:

Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file Wireshark\_802\_11.pcap. This trace was collected using AirPcap and Wireshark running on a computer in a home network consisting of a Linksys 802.11g combined access point/router, with two wired PCs and one wireless host PC attached to the access point/router. In this trace file, we’ll see frames captured on channel 6. Since the host and AP that we are interested in are not the only devices using channel 6, we’ll see a lot of frames that we’re not interested in for this lab, such as beacon frames advertised by a neighbor’s AP also operating on channel 6. The wireless host activities taken in the trace file are:

• The host is already associated with the 30 Munroe St AP when the trace begins.

• At t = 24.82, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12.

• At t=32.82, the host makes an HTTP request to http://www.cs.umass.edu, whose IP address is 128.119.240.19.

• At t = 49.58, the host disconnects from the 30 Munroe St AP and attempts to connect to the linksys\_ses\_24086. This is not an open access point, and so the host is eventually unable to connect to this AP.

• At t=63.0 the host gives up trying to associate with the linksys\_ses\_24086 AP, and associates again with the 30 Munroe St access point.

Once you have downloaded the trace, and unzip it, you can load it into Wireshark and view the trace using the File pull down menu, choosing Open, and then selecting the Wireshark\_802\_11.pcap trace file. The resulting display should look just like Figure 1.

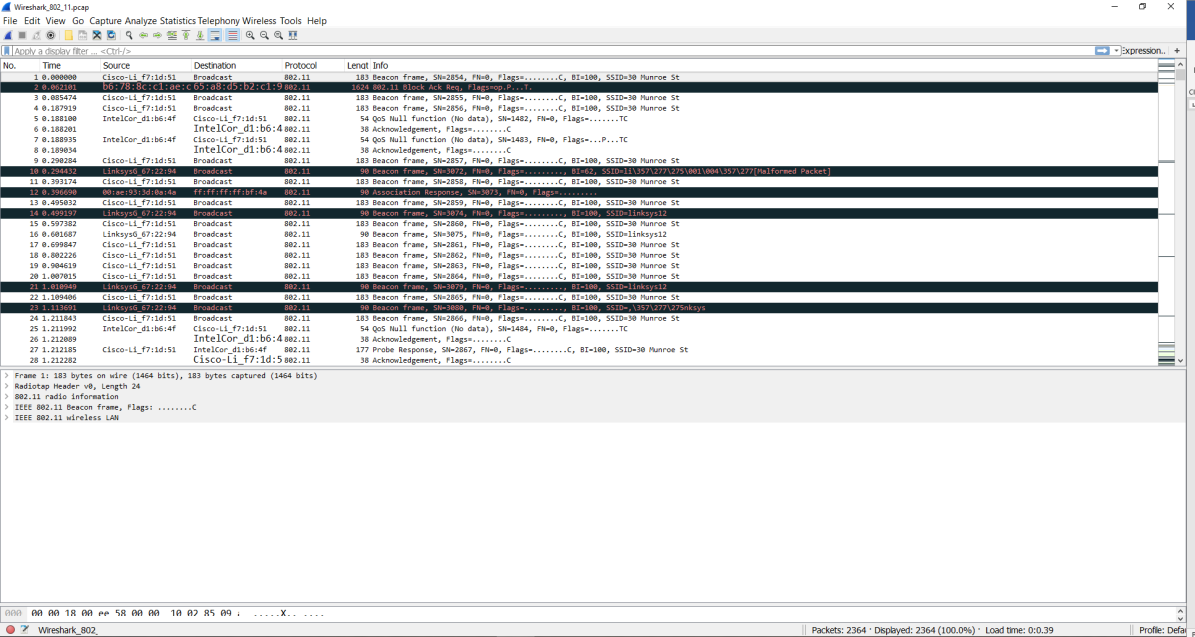


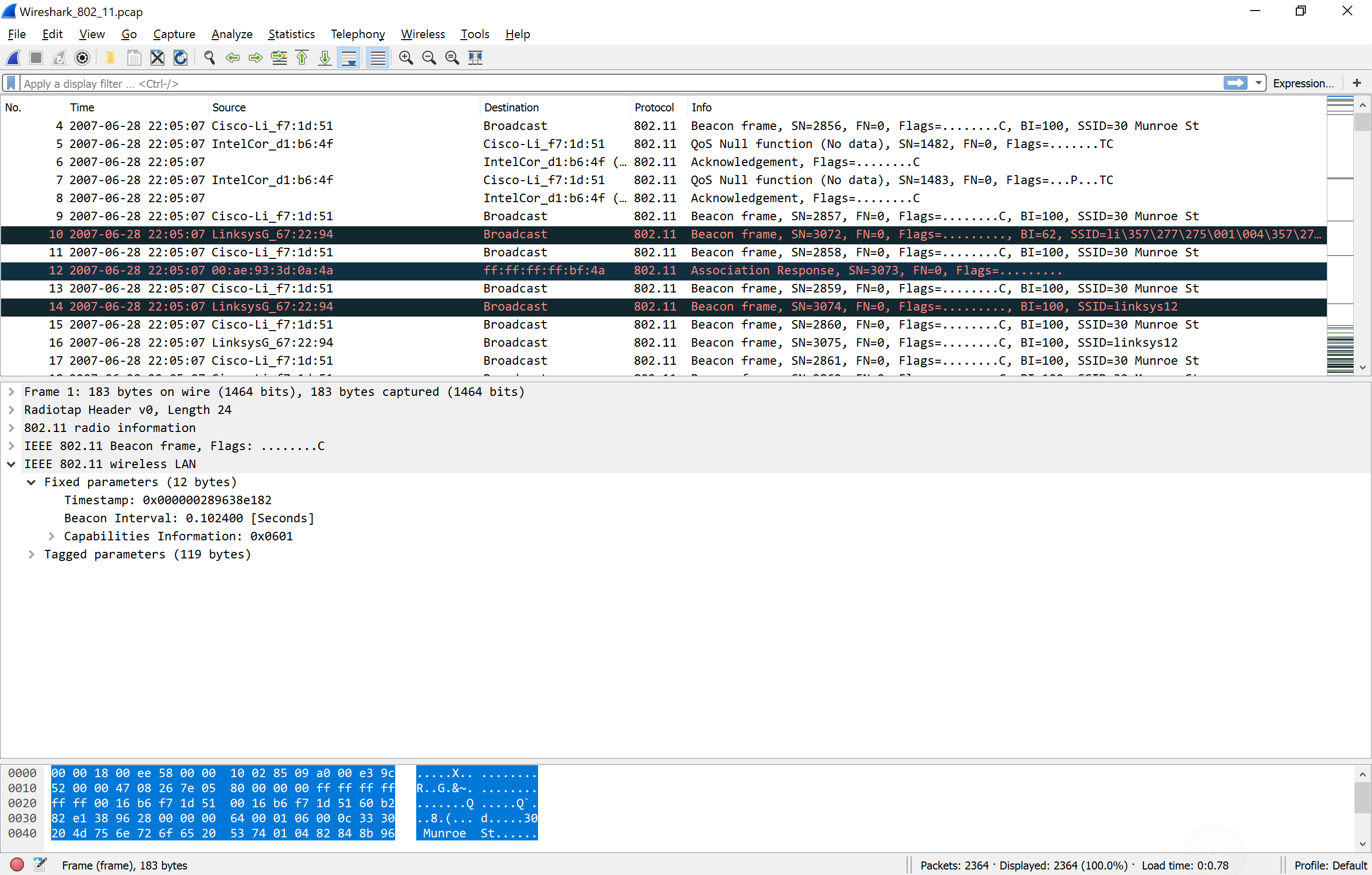
Figure 1: Wireshark window, after opening the Wireshark\_802\_11.pcap file

Recall that beacon frames are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you’ll want to look at the details of the “IEEE 802.11” frame and subfields in the middle Wireshark window. When answering a question below, you should hand in a screenshot of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

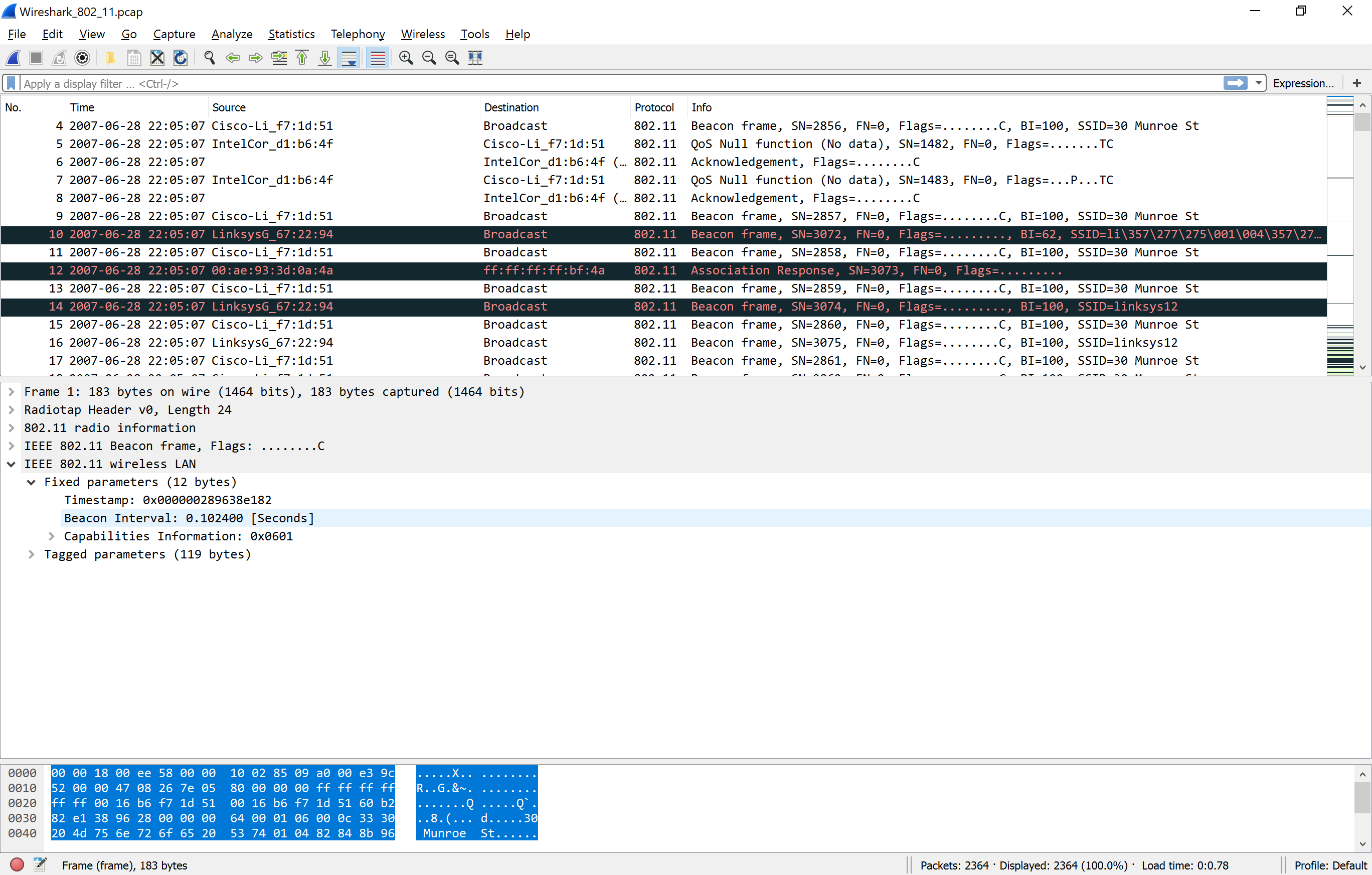
Questions:

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

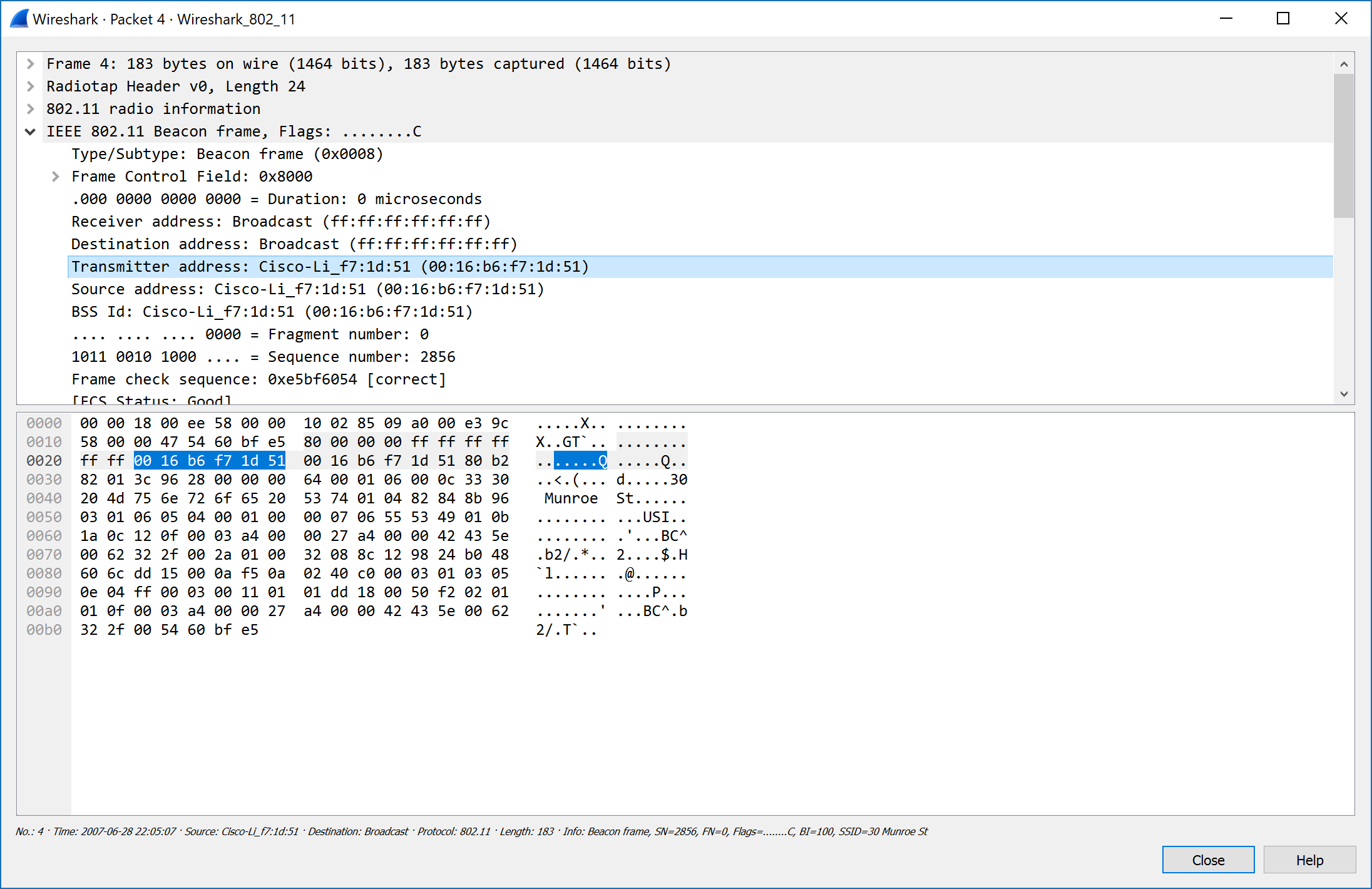
Lynksys and 30 Monroe



1. 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). .102400



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). 00:16:b6f76:1d:51



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

See Above ff:ff:ff:ff:ff:ff

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

Same as #3 00:16:b6f76:1d:51

