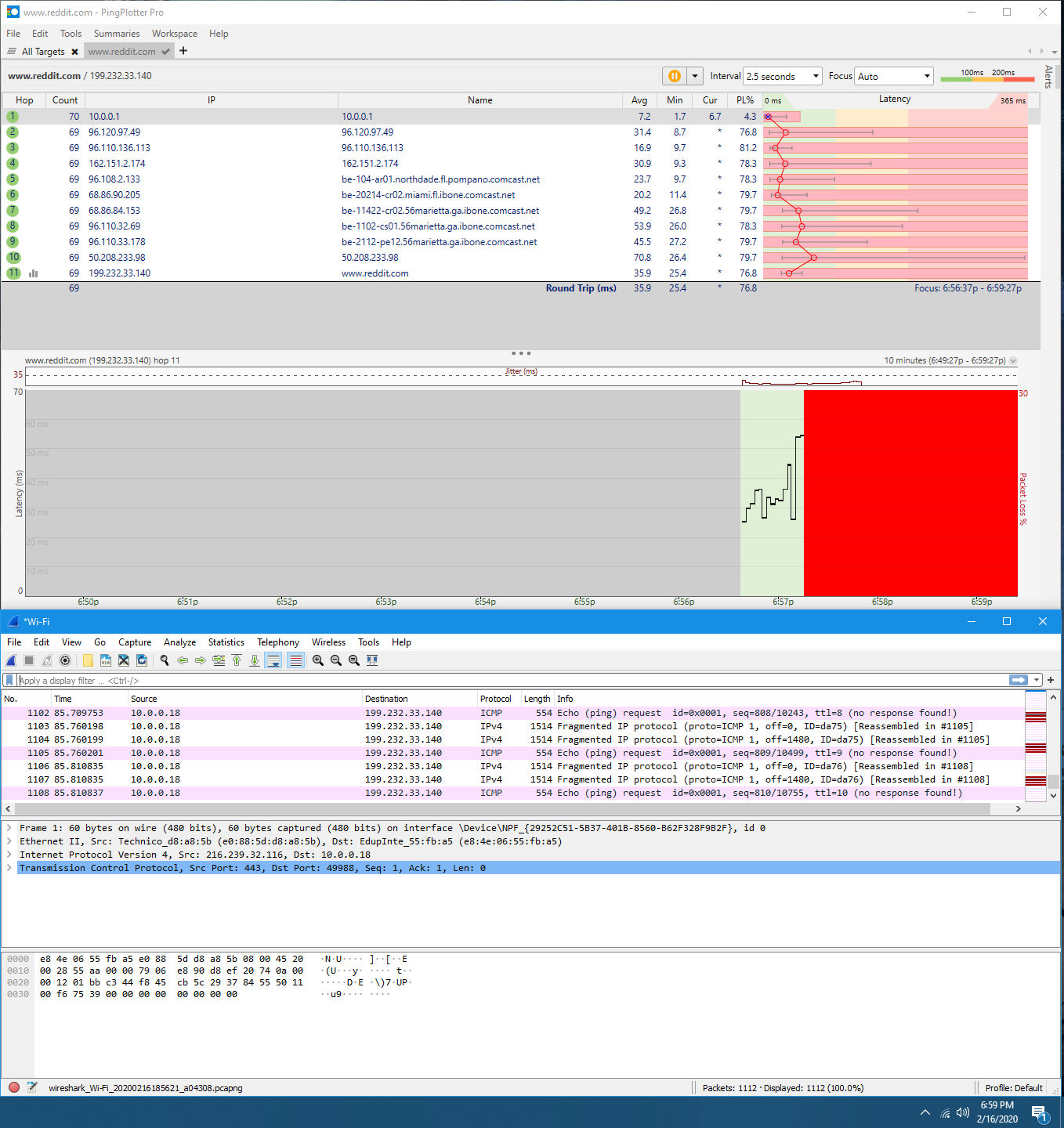
Anaisy Garcia

PID: 5734454

Project 2

Problem 1

(60 pts) Do the Wireshark exercise attached below. Attach the screenshot of your Wireshark results.

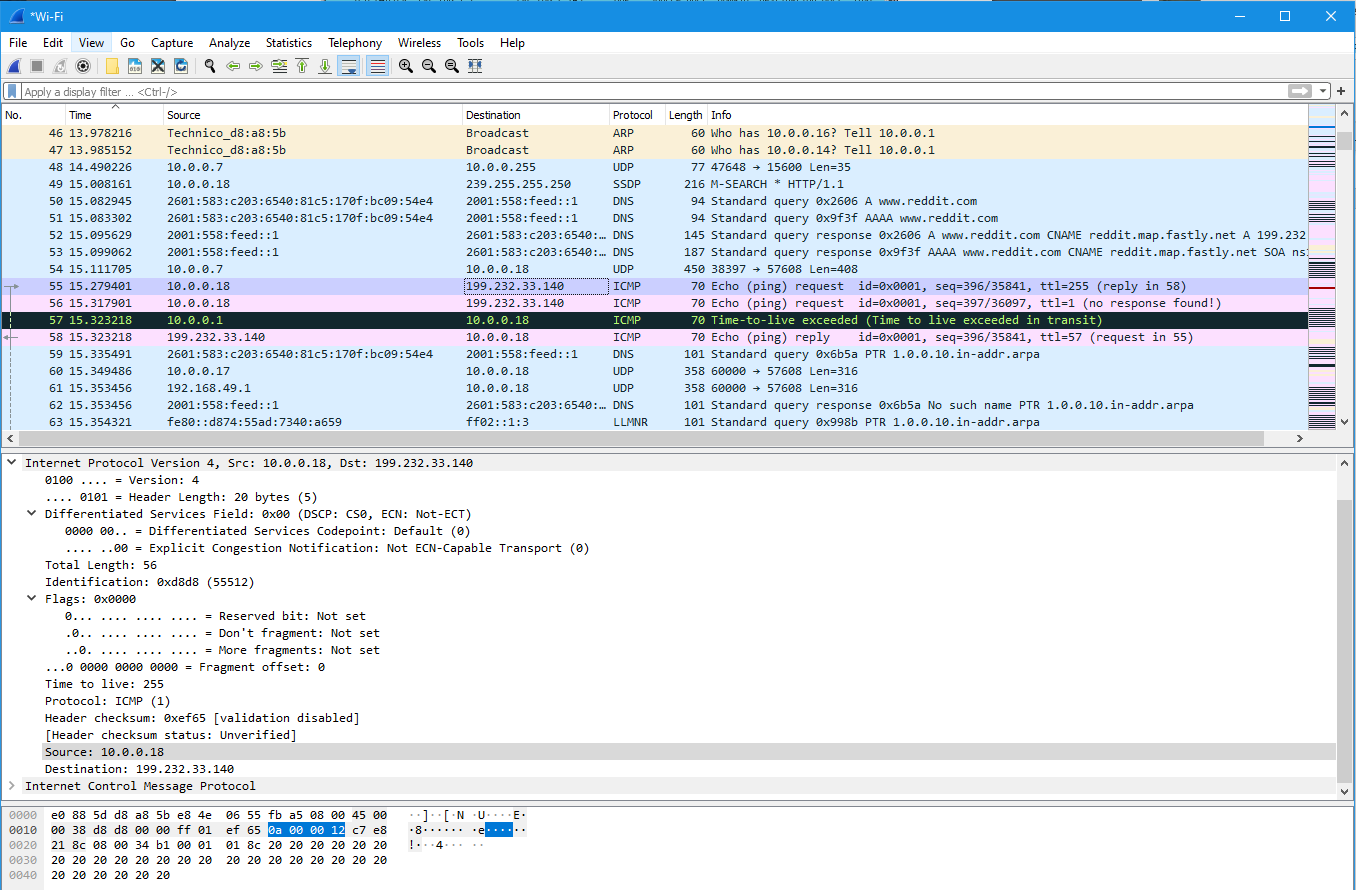


1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

IPv4: 10.0.0.18

IPv6: 2601:583:c203:6540::2

1. Within the IP packet header, what is the value in the upper layer protocol field?



ICMP (1)

1. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.



Header bytes: 20



Payload bytes: 36 (total length 56 – header bytes 20 = payload bytes 36)

1. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.



In the more fragments data bit it is equal to 0. Therefore, data is not fragmented.

1. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

Identification (incrementing), time to live (TTL) (incrementing), and header checksum will always change.

1. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Fields that stay constant across the IP datagrams:

Source IP – receiving from same source

Header Length – ICMP packets

Version – IPv4 for all packets

Destination IP – sending from same destination

Upper Layer Protocol – ICMP packets

Differentiated Services – All ICMP packets use the same type of service class

Fields that must stay constant:

Source IP – receiving from same source

Header Length – ICMP packets

Version – IPv4 for all packets

Destination IP – sending from same destination

Upper Layer Protocol – ICMP packets

Differentiated Services – All ICMP packets use the same type of service class

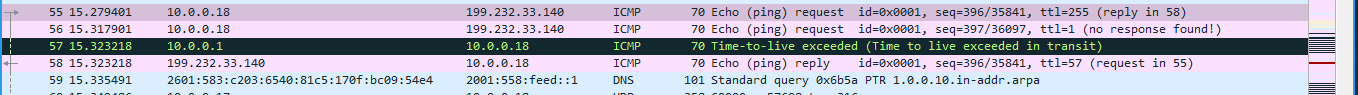
Fields that must change:

Time to live – (traceroute increments each subsequent packet)

Header Checksum – (header changes, must checksum)

Identification – (Packets must have different ids)

1. Describe the pattern you see in the values in the Identification field of the IP datagram.



IP header identification fields increment with each ICMP echo (ping) request.

1. What is the value in the Identification field and the TTL field?



Identification = 55512



TTL = 255

1. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The identification field must change for all ICMP TTL replies because it is a unique value. When two are the same, it means the IP datagrams are fragments of a larger IP datagram. The TTL field stays unaffected because the TTL for the first hop router is always the same.

1. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file]

The packet has been fragmented across more than one IP datagram.

1. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

The more fragments data bit it is equal to 1. Therefore, data is fragmented. The fragments offset is equal to 0. Therefore, this is the first fragment.

Total Length = 1500.

1. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

The fragment offset is equal to 1480. Therefore, this is not the first fragment. The more fragments data bit is equal to 0 and states not set on the right. Therefore, this is the last fragment.

1. What fields change in the IP header between the first and second fragment?

The IP header fields that change are the total length, the flags, the fragment offset, and checksum.

1. How many fragments were created from the original datagram?

At 3500, there are 3 packets created from the original datagram.

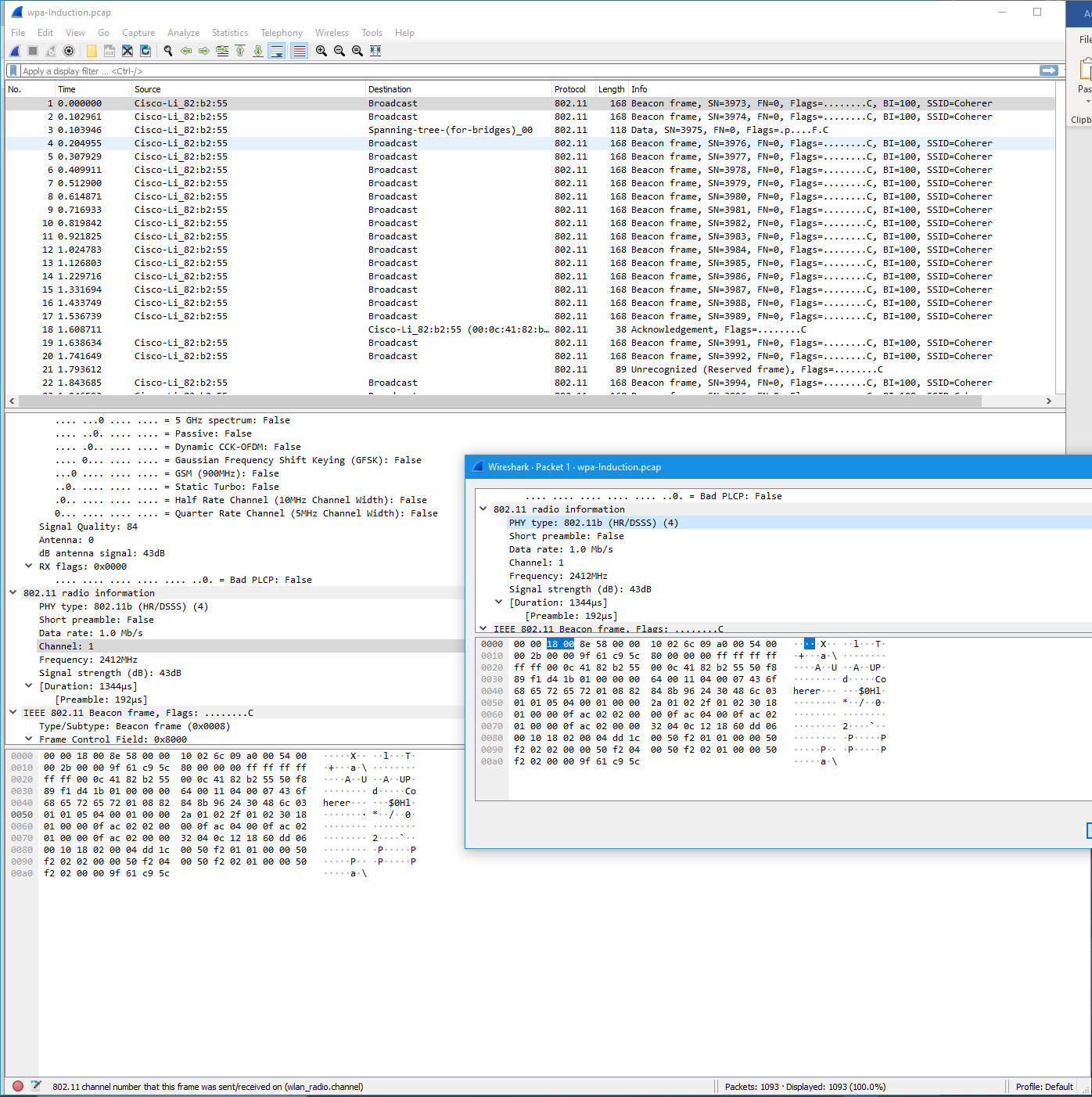
1. What fields change in the IP header among the fragments?

The IP headers that changed were the fragment offset and checksum. Between the first two packets and the last there is a change in total length and in flags. The first two packets have a total length of 1500 and the more fragment bit is set to 1. The last packet has a total length of 540 and the more fragment bit is set to 0.

Problem 2

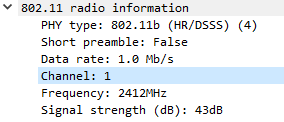
1. What is the IEEE 802.11 standard (e.g., a/b/g/n) used by the access point (AP)? Show the screen capture of the packet within the trace that you used to answer this question.

IEEE 802.11b



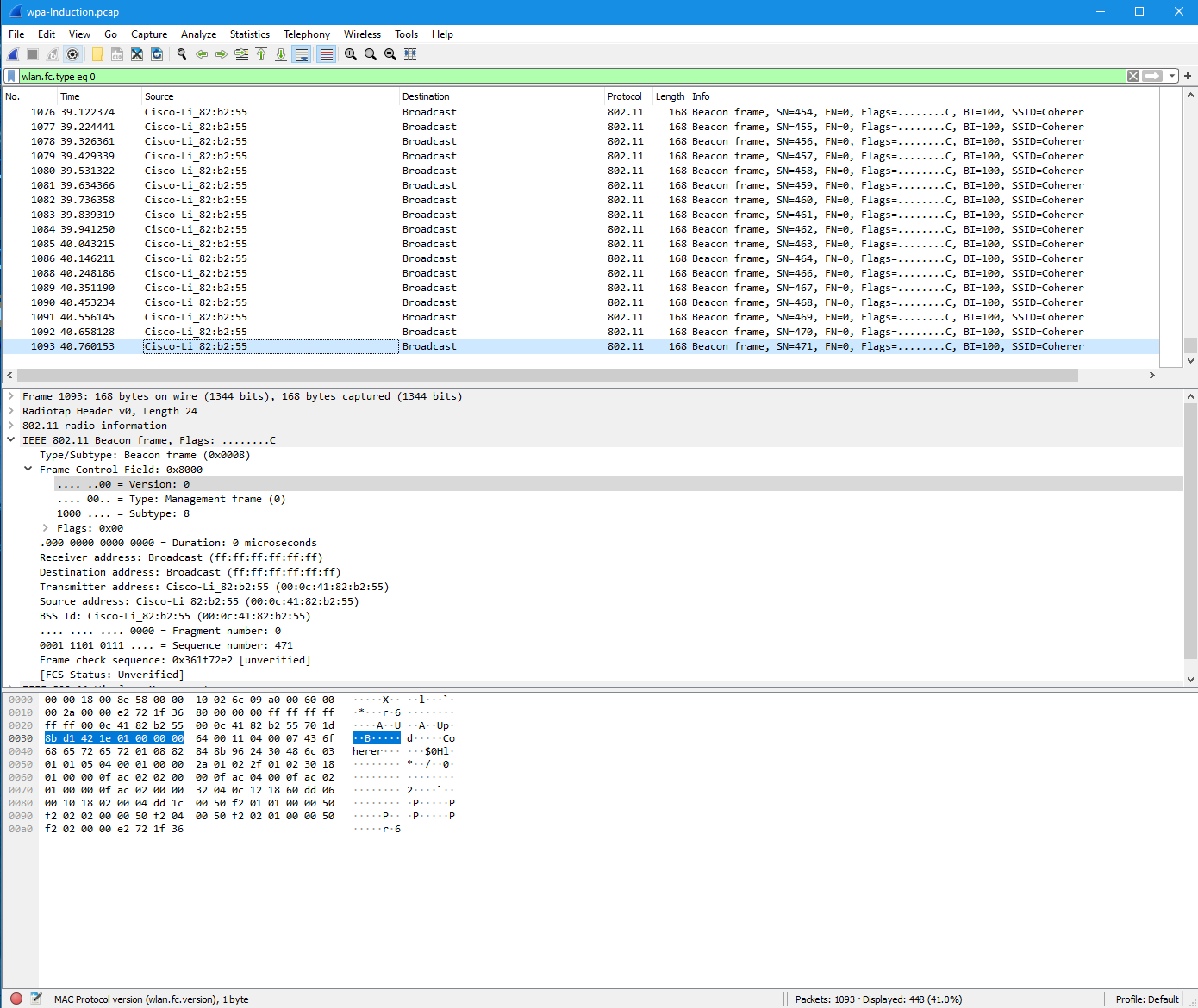
1. In which channel (e.g., channel 1, 2, 3, 4, etc) does this AP work?

Channel 1



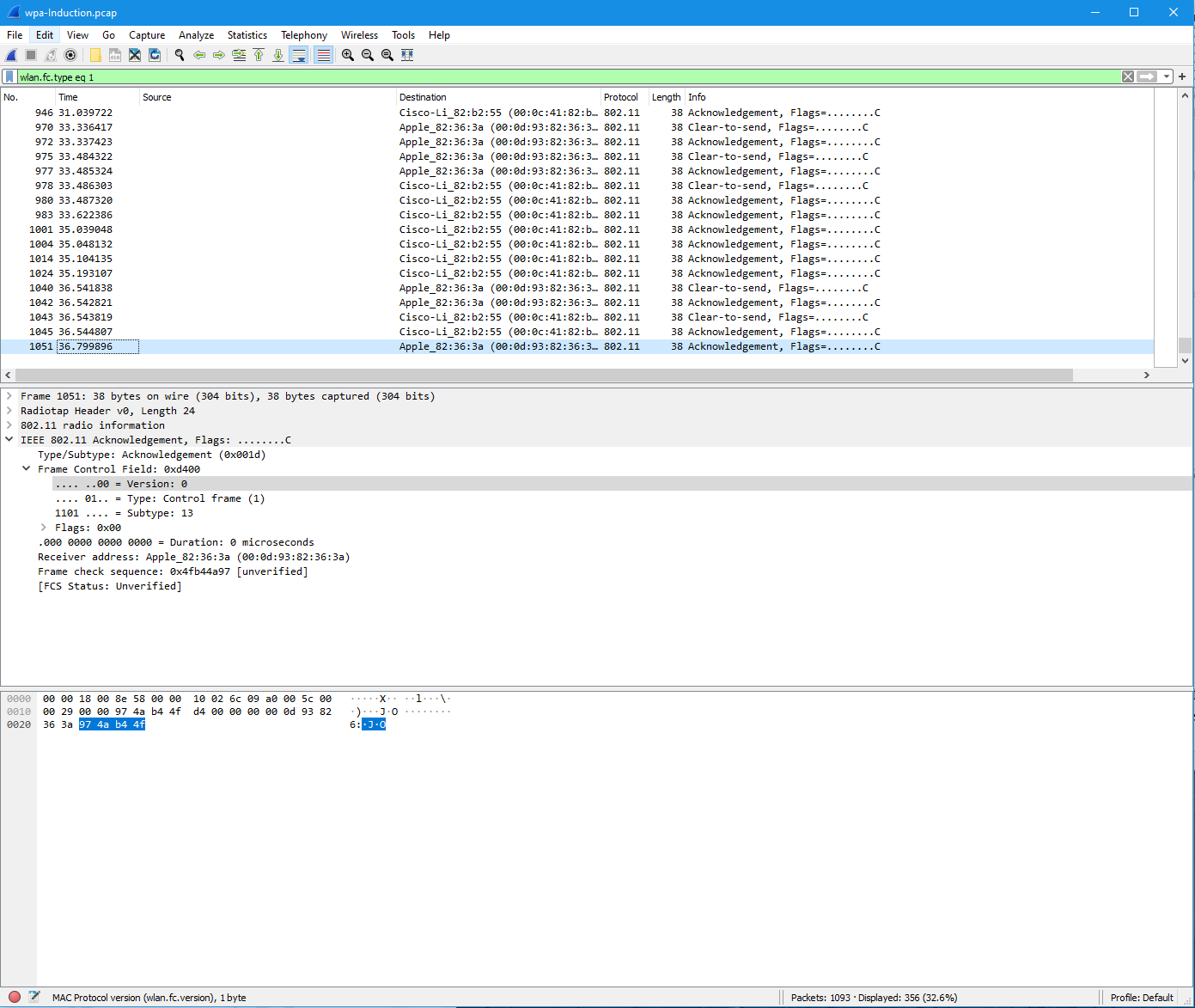
1. List management frames in the trace

There are 1093 management frames in the trace. Filter used: wlan.fc.type eq 0.



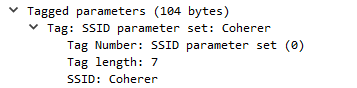
1. List control frames in the trace

There are 1051 control frames in the trace. Filter used: wlan.fc.type eq 1.



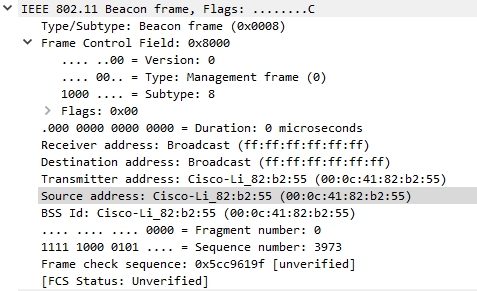
1. What is the SSID of the AP?

Coherer



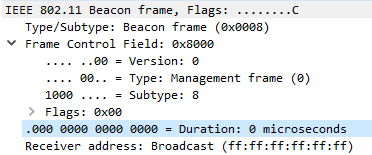
1. What (in hexadecimal notation) is the source MAC address on the beacon frame?

MAC = 00:0c:41:82:b2:55



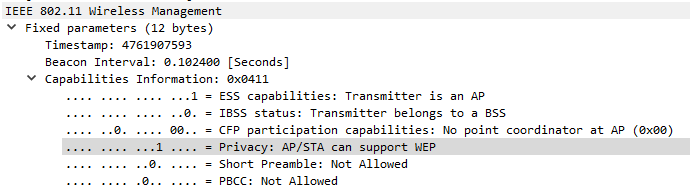
1. What is the interval of time between the transmissions of the beacon frames? (Hint: this interval of time is contained in the beacon frame itself).

.000 0000 0000 0000 = Duration: 0 microseconds



1. What is the security standard used by the AP?

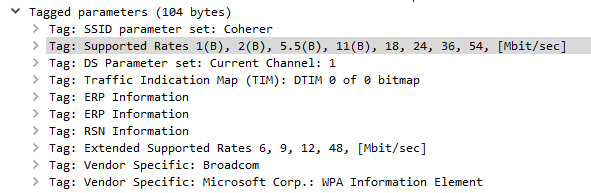
SSID and WEP



1. Find the authentication request from a host to an AP in the trace. Does the host want the authentication to require a key or be open? Explain your answer.

The host wants the authentication key to be OPEN with algorithm open system.

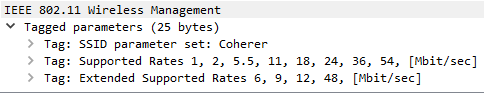
1. Find the association request from a host to an AP in the trace. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.



Host transmission rates:

1, 2, 5.5, 11, 18, 24, 36, 54 [Mbit/sec]

Extended: 6, 9, 12, 48 [Mbit/sec]



AP transmission rates:

1, 2, 5.5, 11, 18, 24, 36, 54 [Mbit/sec]

Extended: 6, 9, 12, 48 [Mbit/sec]