WioT - Postlab

Lab 1: Wireshark and your local network

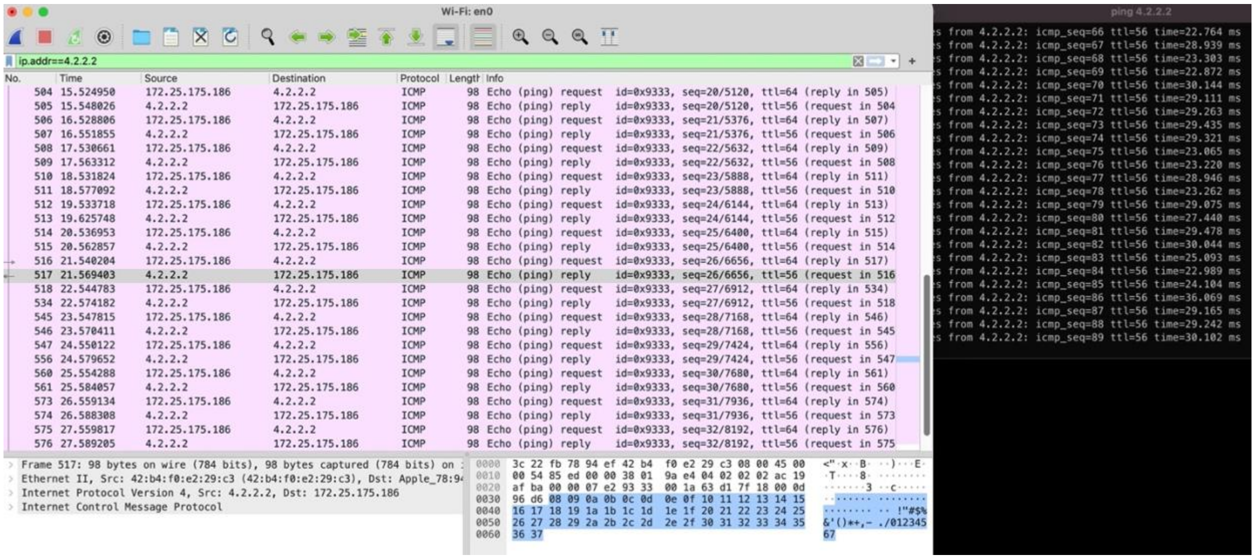
What to submit?

Please use this document as a template, add your responses directly, and export it as a PDF to Gradescope. Each student should submit their own report.

Name: Robert Owens
Computing ID: rao7utn

A: Finding and Inspecting Your Own Traffic

[2pts] Show a screenshot of your captured *ping* traffic:



Wi-Fi: en0

ip.addr==4.2.2.2

```
No.      Time       Source           Destination      Protocol Length Info
     504 15.524950  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=20/5120, ttl=64 (reply in 505)
     505 15.548026  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=20/5120, ttl=56 (request in 504
     506 16.528806  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=21/5376, ttl=64 (reply in 507)
     507 16.551855  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=21/5376, ttl=56 (request in 506
     508 17.530661  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=22/5632, ttl=64 (reply in 509)
     509 17.563312  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=22/5632, ttl=56 (request in 508
     510 18.531824  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=23/5888, ttl=64 (reply in 511)
     511 18.577092  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=23/5888, ttl=56 (request in 510
     512 19.533718  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=24/6144, ttl=64 (reply in 513)
     513 19.625748  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=24/6144, ttl=56 (request in 512
     514 20.536953  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=25/6400, ttl=64 (reply in 515)
     515 20.562857  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=25/6400, ttl=56 (request in 514
     516 21.540204  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=26/6656, ttl=64 (reply in 517)
     517 21.569403  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=26/6656, ttl=56 (request in 516
     518 22.544783  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=27/6912, ttl=64 (reply in 534)
     534 22.574182  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=27/6912, ttl=56 (request in 518
     545 23.547815  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=28/7168, ttl=64 (reply in 546)
     546 23.570411  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=28/7168, ttl=56 (request in 545
     547 24.550122  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=29/7424, ttl=64 (reply in 556)
     556 24.579652  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=29/7424, ttl=56 (request in 547
     560 25.554288  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=30/7680, ttl=64 (reply in 561)
     561 25.584057  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=30/7680, ttl=56 (request in 560
     573 26.559134  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=31/7936, ttl=64 (reply in 574)
     574 26.588308  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=31/7936, ttl=56 (request in 573
     575 27.559817  172.25.175.186   4.2.2.2          ICMP       98 Echo (ping) request  id=0x9333, seq=32/8192, ttl=64 (reply in 576)
     576 27.589205  4.2.2.2          172.25.175.186   ICMP       98 Echo (ping) reply    id=0x9333, seq=32/8192, ttl=56 (request in 575
```

```
> Frame 517: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on :
> Ethernet II, Src: 42:b4:f0:e2:29:c3 (42:b4:f0:e2:29:c3), Dst: Apple_78:94
> Internet Protocol Version 4, Src: 4.2.2.2, Dst: 172.25.175.186
> Internet Control Message Protocol
```

```
0000  3c 22 fb 78 94 ef 42 b4  f0 e2 29 c3 08 00 45 00   <"·x··B· ··)···E·
0010  00 54 85 ed 00 00 38 01  9a e4 04 02 02 02 ac 19   ·T····8· ········
0020  af ba 00 00 07 e2 93 33  00 1a 63 d1 7f 18 00 0d   ·······3 ··c·····
0030  96 d6 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

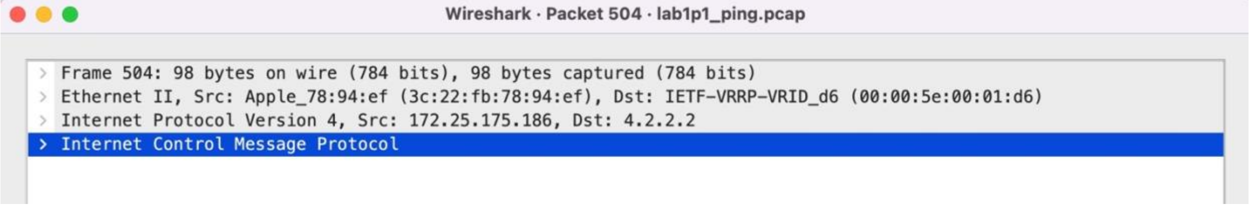
ping 4.2.2.2

```
s from 4.2.2.2: icmp_seq=66 ttl=56 time=22.764 ms
s from 4.2.2.2: icmp_seq=67 ttl=56 time=28.939 ms
s from 4.2.2.2: icmp_seq=68 ttl=56 time=23.303 ms
s from 4.2.2.2: icmp_seq=69 ttl=56 time=22.872 ms
s from 4.2.2.2: icmp_seq=70 ttl=56 time=30.144 ms
s from 4.2.2.2: icmp_seq=71 ttl=56 time=29.111 ms
s from 4.2.2.2: icmp_seq=72 ttl=56 time=29.263 ms
s from 4.2.2.2: icmp_seq=73 ttl=56 time=29.435 ms
s from 4.2.2.2: icmp_seq=74 ttl=56 time=29.321 ms
s from 4.2.2.2: icmp_seq=75 ttl=56 time=23.065 ms
s from 4.2.2.2: icmp_seq=76 ttl=56 time=23.220 ms
s from 4.2.2.2: icmp_seq=77 ttl=56 time=28.946 ms
s from 4.2.2.2: icmp_seq=78 ttl=56 time=23.262 ms
s from 4.2.2.2: icmp_seq=79 ttl=56 time=29.075 ms
s from 4.2.2.2: icmp_seq=80 ttl=56 time=27.440 ms
s from 4.2.2.2: icmp_seq=81 ttl=56 time=29.478 ms
s from 4.2.2.2: icmp_seq=82 ttl=56 time=30.044 ms
s from 4.2.2.2: icmp_seq=83 ttl=56 time=25.093 ms
s from 4.2.2.2: icmp_seq=84 ttl=56 time=22.989 ms
s from 4.2.2.2: icmp_seq=85 ttl=56 time=24.104 ms
s from 4.2.2.2: icmp_seq=86 ttl=56 time=36.069 ms
s from 4.2.2.2: icmp_seq=87 ttl=56 time=29.165 ms
s from 4.2.2.2: icmp_seq=88 ttl=56 time=29.242 ms
s from 4.2.2.2: icmp_seq=89 ttl=56 time=30.102 ms
```

[1pt] *__Postlab:__* What does "ICMP" stand for?

Internet Control Message Protocol

[3pts] *__Postlab:__* For one of your *ping* packets, start from the PHY and list each of the layers that were used to send the packet, and which technology was used:



Wireshark · Packet 504 · lab1p1_ping.pcap

```
> Frame 504: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Apple_78:94:ef (3c:22:fb:78:94:ef), Dst: IETF-VRRP-VRID_d6 (00:00:5e:00:01:d6)
> Internet Protocol Version 4, Src: 172.25.175.186, Dst: 4.2.2.2
> Internet Control Message Protocol
```

Frame 504 – 98 bytes ICMP rule

Ethernet II - specifies an IPv4 source and destination address

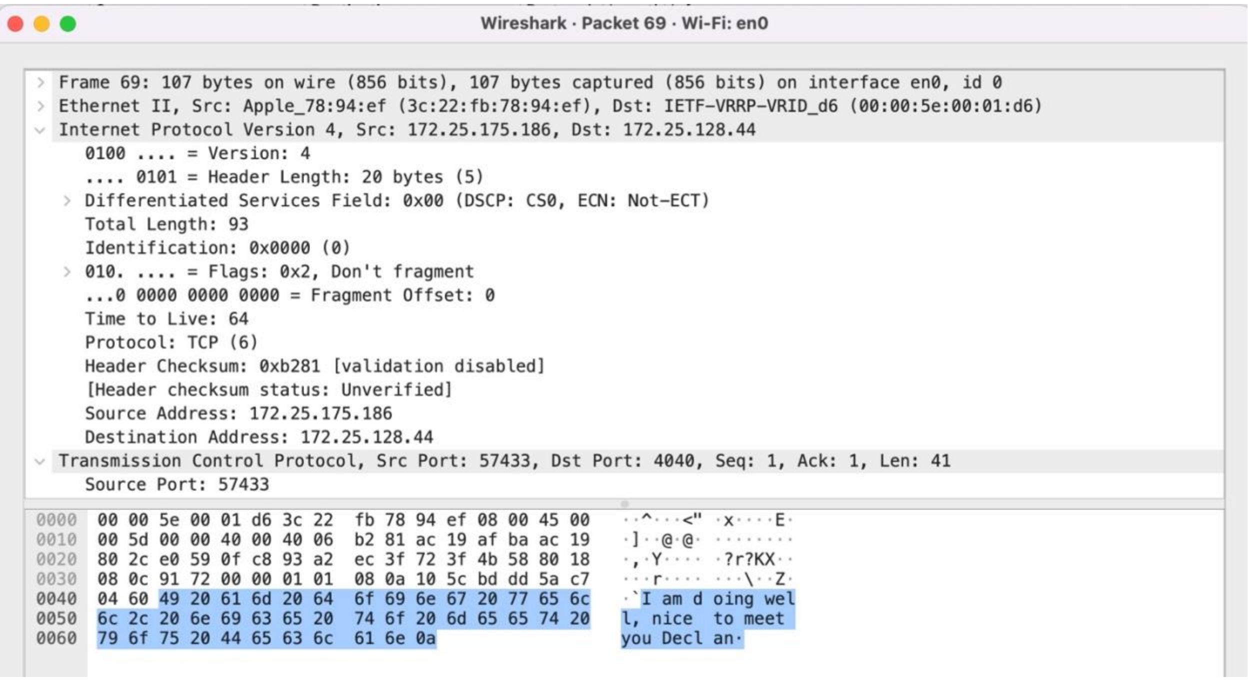
Internet Protocol Version 4 – this looks like the packet header – 20 bytes

Internet Control Message Protocol – I think this is just the returned ping 8 bytes an integer indicating the status is good.

B: Insecure Chat

[3pts] Show a screenshot of your captured *netcat* traffic from both you as a listener and as a sender. Clearly document which case is which.

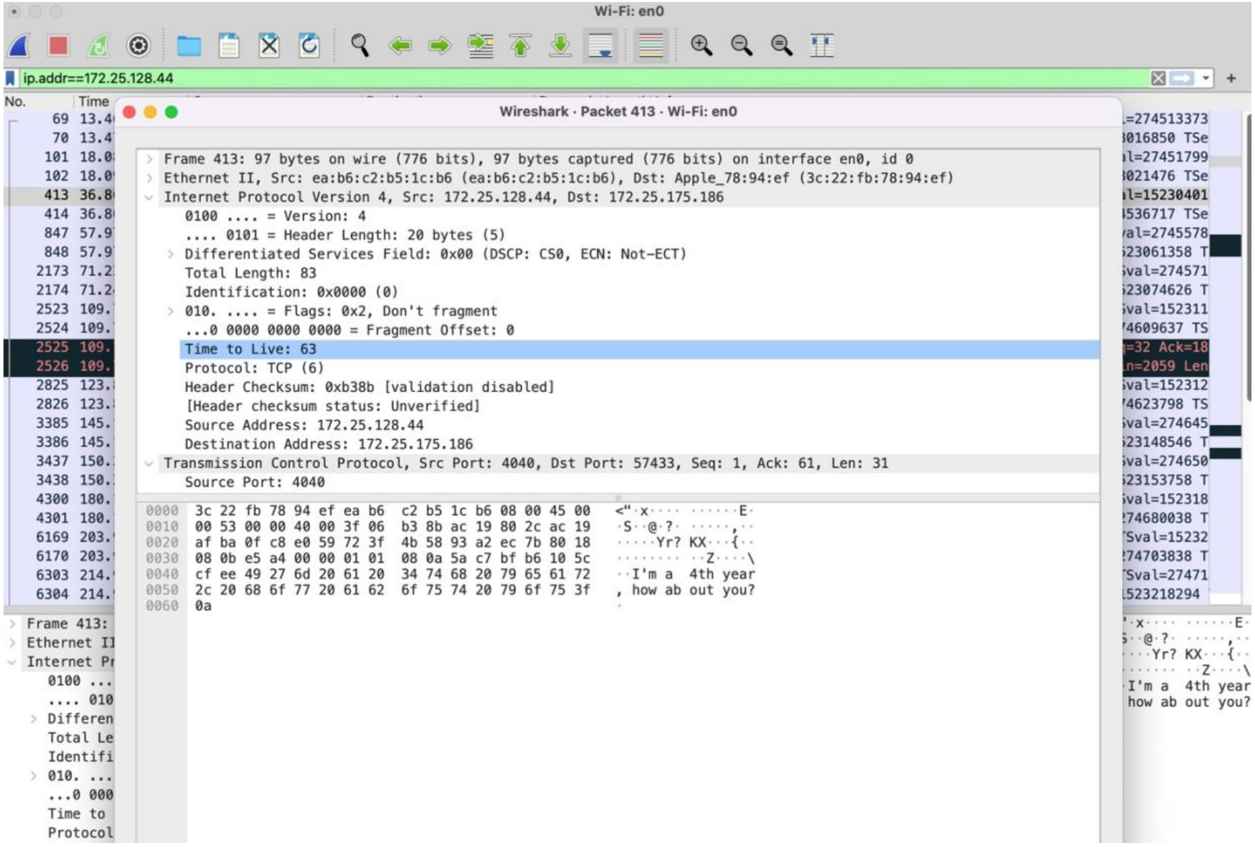
Myself as sender



```
> Frame 69: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface en0, id 0
> Ethernet II, Src: Apple_78:94:ef (3c:22:fb:78:94:ef), Dst: IETF-VRRP-VRID_d6 (00:00:5e:00:01:d6)
v Internet Protocol Version 4, Src: 172.25.175.186, Dst: 172.25.128.44
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 93
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xb281 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.25.175.186
    Destination Address: 172.25.128.44
v Transmission Control Protocol, Src Port: 57433, Dst Port: 4040, Seq: 1, Ack: 1, Len: 41
    Source Port: 57433

0000  00 00 5e 00 01 d6 3c 22  fb 78 94 ef 08 00 45 00   ··^···<" ·x····E·
0010  00 5d 00 00 40 00 40 06  b2 81 ac 19 af ba ac 19   ·]··@·@· ········
0020  80 2c e0 59 0f c8 93 a2  ec 3f 72 3f 4b 58 80 18   ·,·Y···· ·?r?KX··
0030  08 0c 91 72 00 00 01 01  08 0a 10 5c bd dd 5a c7   ···r···· ···\··Z·
0040  04 60 49 20 61 6d 20 64  6f 69 6e 67 20 77 65 6c   ·`I am d oing wel
0050  6c 2c 20 6e 69 63 65 20  74 6f 20 6d 65 65 74 20   l, nice  to meet 
0060  79 6f 75 20 44 65 63 6c  61 6e 0a                  you Decl an·
```

Myself as listener



```
> Frame 413: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface en0, id 0
> Ethernet II, Src: ea:b6:c2:b5:1c:b6 (ea:b6:c2:b5:1c:b6), Dst: Apple_78:94:ef (3c:22:fb:78:94:ef)
v Internet Protocol Version 4, Src: 172.25.128.44, Dst: 172.25.175.186
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 83
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: TCP (6)
    Header Checksum: 0xb38b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.25.128.44
    Destination Address: 172.25.175.186
v Transmission Control Protocol, Src Port: 4040, Dst Port: 57433, Seq: 1, Ack: 61, Len: 31
    Source Port: 4040

0000  3c 22 fb 78 94 ef ea b6  c2 b5 1c b6 08 00 45 00   <"·x···· ······E·
0010  00 53 00 00 40 00 3f 06  b3 8b ac 19 80 2c ac 19   ·S··@·?· ·····,··
0020  af ba 0f c8 e0 59 72 3f  4b 58 93 a2 ec 7b 80 18   ·····Yr? KX···{··
0030  08 0b e5 a4 00 00 01 01  08 0a 5a c7 bf b6 10 5c   ········ ··Z····\
0040  cf ee 49 27 6d 20 61 20  34 74 68 20 79 65 61 72   ··I'm a  4th year
0050  2c 20 68 6f 77 20 61 62  6f 75 74 20 79 6f 75 3f   , how ab out you?
0060  0a                                                 ·
```

[2pts] *__Postlab:__* Can you see other *netcat* traffic from other students in the class? Why or why not?

No. Because I did not run the command for my ncat to listen to other students. If I had then I would be about to see their ncat traffic, I think.

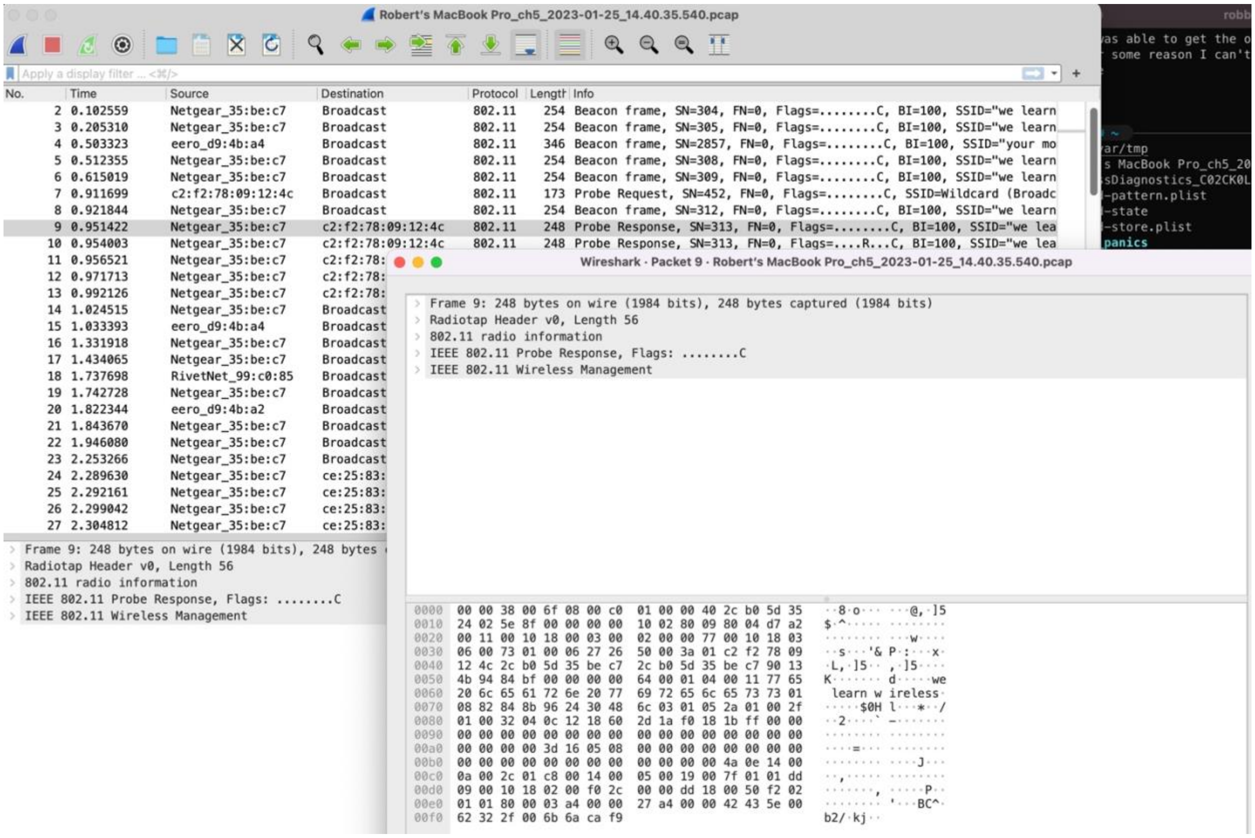
[2pts] *__Postlab:__* Imagine you were having a *netcat* conversation with a friend at George Mason. Besides you and your friend, who else could see the contents of your conversation?

Anyone who could packet sniff the packets in transit. So, at UVA people connected to the eduroam wifi. The IPS provider routes the packet from Charlottesville to George Mason. And then anyone who is packet sniffing at the George Mason wifi networks.

C: Discover WiFi Networks Around You

[2pts] What is the name of the WiFi network we set up?

we learn wireless. Netgear_35:be:c7



Robert's MacBook Pro_ch5_2023-01-25_14.40.35.540.pcap

Apply a display filter ... <⌘/>

```
No.   Time      Source              Destination         Protocol Length Info
    2 0.102559  Netgear_35:be:c7    Broadcast           802.11    254 Beacon frame, SN=304, FN=0, Flags=........C, BI=100, SSID="we learn
    3 0.205310  Netgear_35:be:c7    Broadcast           802.11    254 Beacon frame, SN=305, FN=0, Flags=........C, BI=100, SSID="we learn
    4 0.503323  eero_d9:4b:a4       Broadcast           802.11    346 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID="your mo
    5 0.512355  Netgear_35:be:c7    Broadcast           802.11    254 Beacon frame, SN=308, FN=0, Flags=........C, BI=100, SSID="we learn
    6 0.615019  Netgear_35:be:c7    Broadcast           802.11    254 Beacon frame, SN=309, FN=0, Flags=........C, BI=100, SSID="we learn
    7 0.911699  c2:f2:78:09:12:4c   Broadcast           802.11    173 Probe Request, SN=452, FN=0, Flags=........C, SSID=Wildcard (Broadc
    8 0.921844  Netgear_35:be:c7    Broadcast           802.11    254 Beacon frame, SN=312, FN=0, Flags=........C, BI=100, SSID="we learn
    9 0.951422  Netgear_35:be:c7    c2:f2:78:09:12:4c   802.11    248 Probe Response, SN=313, FN=0, Flags=........C, BI=100, SSID="we lea
   10 0.954003  Netgear_35:be:c7    c2:f2:78:09:12:4c   802.11    248 Probe Response, SN=313, FN=0, Flags=....R...C, BI=100, SSID="we lea
   11 0.956521  Netgear_35:be:c7    c2:f2:78:
   12 0.971713  Netgear_35:be:c7    c2:f2:78:
   13 0.992126  Netgear_35:be:c7    c2:f2:78:
   14 1.024515  Netgear_35:be:c7    Broadcast
   15 1.033393  eero_d9:4b:a4       Broadcast
   16 1.331918  Netgear_35:be:c7    Broadcast
   17 1.434065  Netgear_35:be:c7    Broadcast
   18 1.737698  RivetNet_99:c0:85   Broadcast
   19 1.742728  Netgear_35:be:c7    Broadcast
   20 1.822344  eero_d9:4b:a2       Broadcast
   21 1.843670  Netgear_35:be:c7    Broadcast
   22 1.946080  Netgear_35:be:c7    Broadcast
   23 2.253266  Netgear_35:be:c7    Broadcast
   24 2.289630  Netgear_35:be:c7    ce:25:83:
   25 2.292161  Netgear_35:be:c7    ce:25:83:
   26 2.299042  Netgear_35:be:c7    ce:25:83:
   27 2.304812  Netgear_35:be:c7    ce:25:83:
```

```
> Frame 9: 248 bytes on wire (1984 bits), 248 bytes
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: ........C
> IEEE 802.11 Wireless Management
```

```
as able to get the o
 some reason I can't
ar/tmp
s MacBook Pro_ch5_20
sDiagnostics_C02CK0L
-pattern.plist
-state
-store.plist
panics
```

Wireshark · Packet 9 · Robert's MacBook Pro_ch5_2023-01-25_14.40.35.540.pcap

```
> Frame 9: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: ........C
> IEEE 802.11 Wireless Management
```

```
0000  00 00 38 00 6f 08 00 c0  01 00 00 40 2c b0 5d 35   ··8·o··· ···@,·]5
0010  24 02 5e 8f 00 00 00 00  10 02 80 09 80 04 d7 a2   $·^····· ········
0020  00 11 00 10 18 00 03 00  02 00 00 77 00 10 18 03   ········ ···w····
0030  06 00 73 01 00 06 27 26  50 00 3a 01 c2 f2 78 09   ··s···'& P·:···x·
0040  12 4c 2c b0 5d 35 be c7  2c b0 5d 35 be c7 90 13   ·L,·]5·· ,·]5····
0050  4b 94 84 bf 00 00 00 00  64 00 01 04 00 11 77 65   K······· d·····we
0060  20 6c 65 61 72 6e 20 77  69 72 65 6c 65 73 73 01    learn w ireless·
0070  08 82 84 8b 96 24 30 48  6c 03 01 05 2a 01 00 2f   ·····$0H l···*··/
0080  01 00 32 04 0c 12 18 60  2d 1a f0 18 1b ff 00 00   ··2····` -·······
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 3d 16 05 08  00 00 00 00 00 00 00 00   ····=··· ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 4a 0e 14 00   ········ ····J···
00c0  0a 00 2c 01 c8 00 14 00  05 00 19 00 7f 01 01 dd   ··,····· ········
00d0  09 00 10 18 02 00 f0 2c  00 00 dd 18 00 50 f2 02   ·······, ·····P··
00e0  01 01 80 00 03 a4 00 00  27 a4 00 00 42 43 5e 00   ········ '···BC^·
00f0  62 32 2f 00 6b 6a ca f9                            b2/·kj··
```

[2pts] *__Postlab:__* What are the types of probe packets that you see?

Broadcast – Beacon frame

Broadcast – Probe Request

[2pts] *__Postlab:__* What filter did you use to see only packets from our test network?

wlan.bssid == 2c:b0:5d:35:be:c7

[2pts] *__Postlab:__* What is the MAC address of the router for the test network?

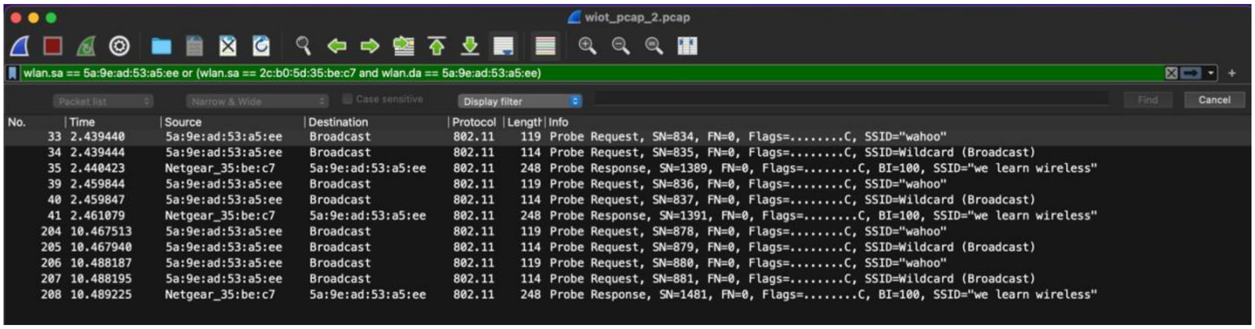
2c:b0:5d:35:be:c7

D: Snooping Connection Formation

[4pts] Filter the traffic to isolate the connection process.
How did you identify the correct set of packets?

I first filtered packets that came from “we learn wireless” mac address and were being sent to the device trying to connect. Or packets being sent by the device trying to connect

Show a screenshot of connection formation here:



```
wlan.sa == 5a:9e:ad:53:a5:ee or (wlan.sa == 2c:b0:5d:35:be:c7 and wlan.da == 5a:9e:ad:53:a5:ee)
```

```
No.      Time         Source              Destination         Protocol  Length Info
  33  2.439440   5a:9e:ad:53:a5:ee   Broadcast           802.11    119 Probe Request, SN=834, FN=0, Flags=........C, SSID="wahoo"
  34  2.439444   5a:9e:ad:53:a5:ee   Broadcast           802.11    114 Probe Request, SN=835, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
  35  2.440423   Netgear_35:be:c7    5a:9e:ad:53:a5:ee   802.11    248 Probe Response, SN=1389, FN=0, Flags=........C, BI=100, SSID="we learn wireless"
  39  2.459844   5a:9e:ad:53:a5:ee   Broadcast           802.11    119 Probe Request, SN=836, FN=0, Flags=........C, SSID="wahoo"
  40  2.459847   5a:9e:ad:53:a5:ee   Broadcast           802.11    114 Probe Request, SN=837, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
  41  2.461079   Netgear_35:be:c7    5a:9e:ad:53:a5:ee   802.11    248 Probe Response, SN=1391, FN=0, Flags=........C, BI=100, SSID="we learn wireless"
 204 10.467513   5a:9e:ad:53:a5:ee   Broadcast           802.11    119 Probe Request, SN=878, FN=0, Flags=........C, SSID="wahoo"
 205 10.467940   5a:9e:ad:53:a5:ee   Broadcast           802.11    114 Probe Request, SN=879, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
 206 10.488187   5a:9e:ad:53:a5:ee   Broadcast           802.11    119 Probe Request, SN=880, FN=0, Flags=........C, SSID="wahoo"
 207 10.488195   5a:9e:ad:53:a5:ee   Broadcast           802.11    114 Probe Request, SN=881, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
 208 10.489225   Netgear_35:be:c7    5a:9e:ad:53:a5:ee   802.11    248 Probe Response, SN=1481, FN=0, Flags=........C, BI=100, SSID="we learn wireless"
```

[1pt] *__Postlab:__* What is the first type of packet that the computer sends to the router to initiate connection formation?

Packet number 34. It is a wildcard Probe Request Packet. the device is asking for wifi connection

[2pt] *__Postlab:__* How do you figure out which packet is sent next? Is there some information in the packet that helps you identify this?

Packet number 35 is the wireless router informing the device that it is available to connect. The identifying information is that it is the next sequential packet and it is the router sending a packet to that specific device and not a broadcast.

[1pt] *__Postlab:__* How do you know when the connection is established?

Packet 41 is a second probe response from the router to the device and then when un-applying the filter the router sends an acknowledgment for packet 42 as a broadcast which I believe is the router informing the network of the new devices' local IP address

E: Inspecting Protocol Information

[2pts] What is the Tag Number for the SSID tag?

Tag number 0.

[1pt] Is the same tag number used for the SSID tag in all beacon packets?

Yes

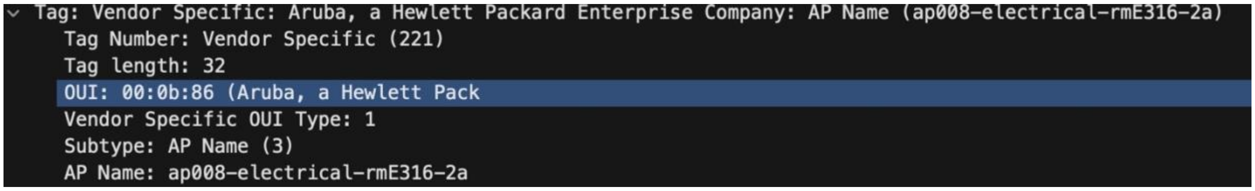
[2pts] What is the Tag Number for the vendor specific tag?

221

[2pts] What is the access point name that ITS used?

Ap008-electrical-rmE316-2a

Include a screenshot from wireshark showing the AP name here:



```
Tag: Vendor Specific: Aruba, a Hewlett Packard Enterprise Company: AP Name (ap008-electrical-rmE316-2a)
    Tag Number: Vendor Specific (221)
    Tag length: 32
    OUI: 00:0b:86 (Aruba, a Hewlett Pack
    Vendor Specific OUI Type: 1
    Subtype: AP Name (3)
    AP Name: ap008-electrical-rmE316-2a
```