

Kenneth Woodard

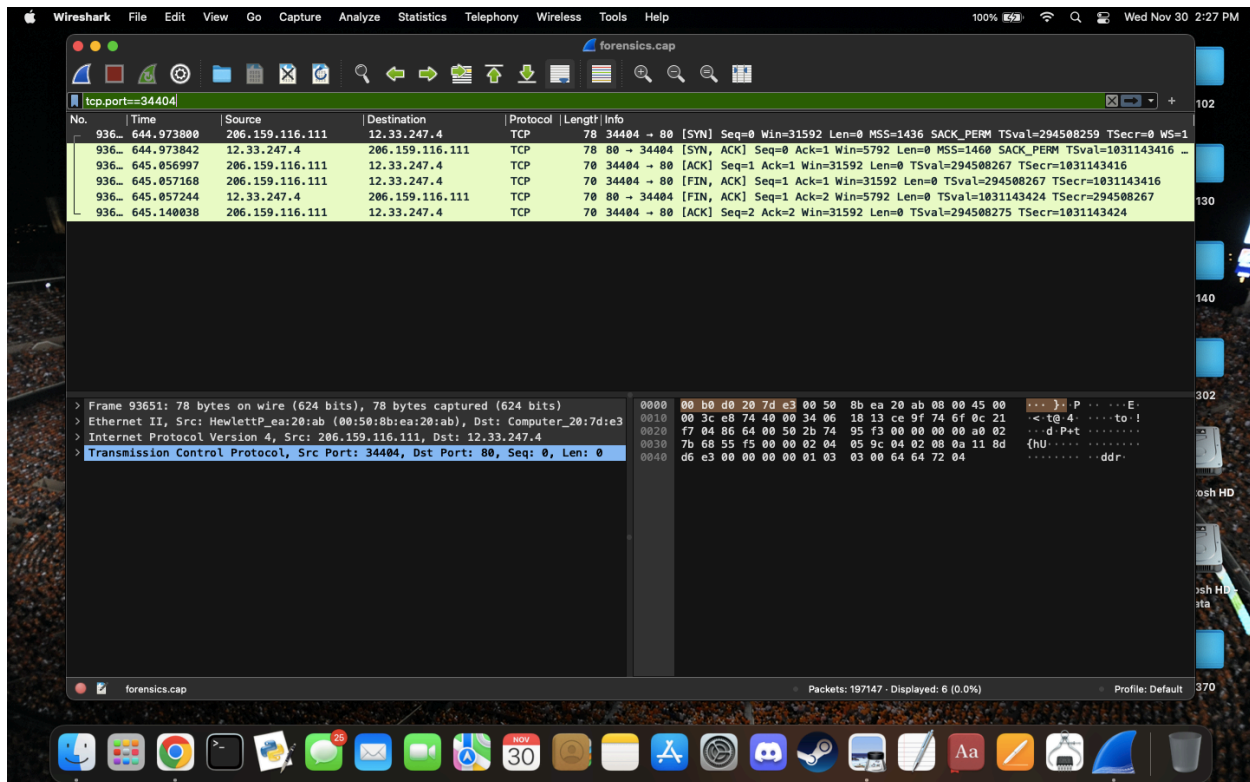
## Programming Assignment 2: Report

CS 366

### Question 1

Six packets are printed out. Here's a list of the flags in each one:

- SYN
- SYN, ACK
- ACK
- FIN, ACK
- FIN, ACK
- ACK



## Question 2

Only one packet is printed. Including `tcp.flags==2` basically narrows it down to only the packets that have only one flag: SYN.

The image shows a Wireshark packet capture window. The filter bar at the top contains the expression `tcp.port==34404&&tcp.flags==2`. The packet list pane shows a single packet, No. 936, at time 644.973800, from source 206.159.116.111 to destination 12.33.247.4. The packet details pane shows the following layers:

- Frame 93651: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
- Ethernet II, Src: HewlettP\_ea:20:ab (00:50:8b:ea:20:ab), Dst: Computer\_20:7d:e3 (00:b0:d0:7d:e3)
- Internet Protocol Version 4, Src: 206.159.116.111, Dst: 12.33.247.4
- Transmission Control Protocol, Src Port: 34404, Dst Port: 80, Seq: 0, Len: 0

The packet bytes pane shows the raw data of the packet, which is a SYN packet with the following hex representation:

```
0000 00 b0 d0 20 7d e3 00 50 8b ea 20 ab 00 00 45 00 ... } .P . . . .E
0010 00 3c e8 74 48 00 34 06 18 13 ce 9f 74 6f 0c 21 < . @ 4 . . . .to:
0020 f7 84 86 64 00 50 2b 74 95 f3 00 00 00 ab 02 . . d P + . . . .
0030 7b 68 55 f5 00 00 02 04 05 9c 04 02 00 0a 11 8d { h U . . . . .
0040 d6 e3 00 00 00 01 03 03 00 64 64 72 04 . . . . . d d r .
```

The status bar at the bottom indicates that 107147 packets were captured and 1 packet is displayed (0.0%).

## Question 3

609 packets were displayed upon using “tcp.flags==18.”

The image shows a Wireshark packet capture interface. The top pane displays a list of packets filtered by 'tcp.flags==18'. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are all TCP SYN-ACKs from 103.108.0276 to 103.108.3253. The bottom pane shows the details of packet 356, which is a TCP SYN-ACK from 12.33.247.4 to 236.852664. The packet details include Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes are shown in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1385	7.928427	12.33.247.3	68.58.116.78	TCP	78	25 → 42285 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=484943985 TSecr=75428
1579	9.551421	12.33.247.11	68.58.116.78	TCP	78	22 → 42286 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1789957384 TSecr=75428
2208	13.598316	12.33.247.4	167.216.183.93	TCP	78	80 → 60999 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031080276 TSecr=29444
2212	13.597663	12.33.247.4	206.159.116.111	TCP	78	80 → 60532 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031080277 TSecr=29444
6969	43.350877	12.33.247.4	167.216.183.93	TCP	78	80 → 32863 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031083252 TSecr=29444
6974	43.358476	12.33.247.4	206.159.116.111	TCP	78	80 → 60629 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031083253 TSecr=29444
101...	64.175768	12.33.247.3	68.58.116.78	TCP	78	25 → 42288 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=484949610 TSecr=75421
115...	72.804631	12.33.247.4	167.216.183.93	TCP	78	80 → 32962 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031086198 TSecr=29444
115...	72.810323	12.33.247.4	206.159.116.111	TCP	78	80 → 60728 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031086198 TSecr=29445
162...	103.074837	12.33.247.4	167.216.183.93	TCP	78	80 → 33061 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031089225 TSecr=29445
162...	103.082645	12.33.247.4	206.159.116.111	TCP	78	80 → 60827 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031089226 TSecr=29445
207...	133.648259	12.33.247.4	167.216.183.93	TCP	78	80 → 33163 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031089228 TSecr=29445
207...	133.655999	12.33.247.4	206.159.116.111	TCP	78	80 → 60929 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031089228 TSecr=29445
252...	164.757659	12.33.247.4	167.216.183.93	TCP	78	80 → 33269 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031089393 TSecr=29445
252...	164.765419	12.33.247.4	206.159.116.111	TCP	78	80 → 32802 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031089394 TSecr=29446
294...	194.280294	12.33.247.4	167.216.183.93	TCP	78	80 → 33365 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031089346 TSecr=29446
294...	194.289304	12.33.247.4	206.159.116.111	TCP	78	80 → 32898 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031089346 TSecr=29446
338...	224.642628	12.33.247.4	167.216.183.93	TCP	78	80 → 33465 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031101382 TSecr=29446
338...	224.650024	12.33.247.4	206.159.116.111	TCP	78	80 → 32998 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031101383 TSecr=29446
356...	236.675995	12.33.247.4	4.41.46.146	TCP	66	80 → 1311 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
356...	236.852664	12.33.247.9	12.33.247.4	TCP	78	3307 → 53561 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1790040432 TSecr=103

Frame 93652: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0  
Ethernet II, Src: Computer\_20:7d:e3 (00:b0:d0:20:7d:e3), Dst: HewlettP\_ea:28:ab (00:50:80:00:00:00)  
Internet Protocol Version 4, Src: 12.33.247.4, Dst: 206.159.116.111  
Transmission Control Protocol, Src Port: 80, Dst Port: 34404, Seq: 0, Ack: 1, Len: 0

Flags: Unsigned integer (2 bytes)      Packets: 197147 - Displayed: 609 (0.3%)      Profile: Default

## Question 4

1803 packets are displayed. "tcp.flags & 0x02" is the filter I used.

The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets, filtered by "tcp.flags & 0x02". The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the detailed view of a selected packet (No. 93651), displaying the raw packet data in hexadecimal and ASCII, along with the packet structure (Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol).

No.	Time	Source	Destination	Protocol	Length	Info
1384	7.928352	68.58.116.78	12.33.247.3	TCP	78	42205 → 25 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=754208819 TSecr=0 WS=1
1385	7.928427	12.33.247.3	68.58.116.78	TCP	78	25 → 42205 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=484943985 TSecr=75420
1578	9.551352	68.58.116.78	12.33.247.11	TCP	78	42206 → 22 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=754208982 TSecr=0 WS=1
1579	9.551421	12.33.247.11	68.58.116.78	TCP	78	22 → 42206 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1789957304 TSecr=75420
2207	13.590219	167.216.183.93	12.33.247.4	TCP	78	60999 → 80 [SYN] Seq=0 Win=31592 Len=0 MSS=1436 SACK_PERM TSval=294443272 TSecr=0 WS=1
2208	13.590316	12.33.247.4	167.216.183.93	TCP	78	80 → 60999 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031080276 TSecr=29444
2211	13.597624	206.159.116.111	12.33.247.4	TCP	78	60532 → 80 [SYN] Seq=0 Win=31592 Len=0 MSS=1436 SACK_PERM TSval=294445126 TSecr=0 WS=1
2212	13.597663	12.33.247.4	206.159.116.111	TCP	78	80 → 60532 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1031080277 TSecr=29444
3951	24.319622	148.64.147.168	12.33.247.30	TCP	64	2237 → 328 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
4144	25.307302	148.64.147.168	12.33.247.30	TCP	64	2238 → 491 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
4218	25.691743	148.64.147.168	12.33.247.30	TCP	64	2239 → 724 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
4445	27.090637	148.64.147.168	12.33.247.30	TCP	64	2240 → 903 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
4447	27.091187	148.64.147.168	12.33.247.30	TCP	64	2241 → 515 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
4530	27.614911	148.64.147.168	12.33.247.30	TCP	64	2242 → 573 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
4725	28.969999	148.64.147.168	12.33.247.30	TCP	64	2244 → 165 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
4897	30.202148	148.64.147.168	12.33.247.30	TCP	64	2245 → 432 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
4946	30.618542	148.64.147.168	12.33.247.30	TCP	64	2246 → 669 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
5356	33.046539	148.64.147.168	12.33.247.30	TCP	64	2247 → 686 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
5435	33.504081	148.64.147.168	12.33.247.30	TCP	64	2248 → 373 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
5437	33.505693	148.64.147.168	12.33.247.30	TCP	64	2249 → 890 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460
5439	33.506532	148.64.147.168	12.33.247.30	TCP	64	2251 → 508 [SYN, Reserved] Seq=0 Win=8192 Len=0 MSS=1460

Packet 93651: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0  
Ethernet II, Src: Hewlett-Packard (08:00:27:00:00:00), Dst: Computer\_20:7d:e3 (08:b0:d0:00:00:00)  
Internet Protocol Version 4, Src: 206.159.116.111, Dst: 12.33.247.4  
Transmission Control Protocol, Src Port: 34404, Dst Port: 80, Seq: 0, Len: 0

0000 00 b0 d0 20 7d e3 00 50 8b ea 20 ab 08 00 45 00 ... }..P....E  
0010 00 3c e8 74 40 00 34 06 18 13 ce 9f 74 6f 0c 21 ... <.t@.4....to!  
0020 f7 04 86 64 00 50 2b 74 95 f3 00 00 00 00 a0 02 ... d.P+t.....  
0030 7b 60 55 f5 00 00 02 04 05 0c 04 02 00 0a 11 8d {b.....  
0040 d6 e3 00 00 00 00 01 03 03 00 64 64 72 04 .....ddr

## Question 5

My alternative filter for question 4 is "tcp.flags bitwise\_and 2."

## Question 6

For the https servers the IP source address was either 12.33.247.2, 12.33.247.4, or 12.33.247.10. The DNS source addresses were either 12.33.247.3, 12.33.247.7, 12.33.247.11, 12.33.247.130, or 12.33.247.131. The method I used was filtering with this string “ip.src==12.33.0.0/16 && (http || dns)” and sorting by protocol. Then, I went through the list and compared IP source addresses. I’m going to include a screenshot for explanation.

The screenshot displays a Wireshark network traffic capture. The top pane shows a list of packets filtered by the expression `ip.src==12.33.0.0/16 && (http || dns)`. The packets are sorted by protocol. The middle pane shows the details of the selected packet (No. 194, Time 1305.472194, Source 12.33.247.3, Destination 12.33.246.131, Protocol DNS). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
194	1304.832504	12.33.247.3	193.95.93.77	DNS	212	Standard query response 0xa7f8 A www.dshield.org A 63.100.47.44 NS ns1.homepc.org NS ns2.giac.ne
194	1305.472194	12.33.247.3	12.33.246.131	DNS	89	Standard query 0x7167 PTR 7.128.65.212.in-addr.arpa
194	1305.960091	12.33.247.3	203.139.160.74	DNS	139	Standard query response 0xd980 No such name A ns1.giac.net.giac.org SOA iceman.giac.org
195	1311.964679	12.33.247.3	24.29.99.83	DNS	228	Standard query response 0xe2d9 A www.incidents.org CNAME incidents.org A 63.100.47.45 NS iceman.
195	1313.020954	12.33.247.3	68.60.32.6	DNS	212	Standard query response 0xb4ea A www.dshield.org A 63.100.47.44 NS ns1.homepc.org NS ns2.giac.ne
195	1313.771153	12.33.247.3	64.136.21.39	DNS	64	Standard query response 0x3237 Format error
195	1313.780019	12.33.247.3	64.136.21.39	DNS	226	Standard query response 0x2042 A rr.sans.org NS NS1.GIAC.NET NS NS1.HOMEPC.org NS NS2.GIAC.NET N
196	1318.482447	12.33.247.3	206.13.28.11	DNS	91	Standard query 0x7f26 PTR 123.144.166.64.in-addr.arpa
196	1318.577864	12.33.247.3	198.6.1.83	DNS	91	Standard query 0x9c63 PTR 196.255.238.62.in-addr.arpa
196	1318.612855	12.33.247.3	212.115.192.193	DNS	91	Standard query 0xb81f PTR 196.255.238.62.in-addr.arpa
196	1319.976450	12.33.247.3	203.2.193.70	DNS	212	Standard query response 0xab25 A www.dshield.org A 63.100.47.44 NS ns1.homepc.org NS ns2.giac.ne
196	1321.343915	12.33.247.3	200.62.22.108	DNS	212	Standard query response 0xbf8f A www.dshield.org A 63.100.47.44 NS ns1.homepc.org NS ns2.giac.ne
196	1321.631801	12.33.247.3	212.115.192.195	DNS	91	Standard query 0xb81f PTR 196.255.238.62.in-addr.arpa
196	1323.581739	12.33.247.3	12.33.246.130	DNS	91	Standard query 0x716b PTR 196.255.238.62.in-addr.arpa
357	236.867878	12.33.247.4	4.41.46.146	HTTP	1518	HTTP/1.1 200 OK [Packet size limited during capture]
357	236.867995	12.33.247.4	4.41.46.146	HTTP	1518	Continuation[Packet size limited during capture]
357	237.039830	12.33.247.4	4.41.46.146	HTTP	260	Continuation
406	271.596874	12.33.247.4	24.73.20.159	HTTP	1518	HTTP/1.1 200 OK [Packet size limited during capture]
406	271.596997	12.33.247.4	24.73.20.159	HTTP	1518	Continuation[Packet size limited during capture]
406	271.673622	12.33.247.4	24.73.20.159	HTTP	260	Continuation
685	466.557753	12.33.247.4	212.73.184.57	HTTP	1518	HTTP/1.1 200 OK [Packet size limited during capture]

Frame 10: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0  
> Ethernet II, Src: Computer\_20:7d:9b (00:b0:d0:20:7d:9b), Dst: HewlettP\_ea:20:ab (00:50:8b:00:20:ab)  
> Internet Protocol Version 4, Src: 12.33.247.3, Dst: 192.153.124.2  
> User Datagram Protocol, Src Port: 2136, Dst Port: 53  
> Domain Name System (query)

Source Address: IPv4 address  
Packets: 197147 - Displayed: 14398 (7.3%)  
Profile: Default

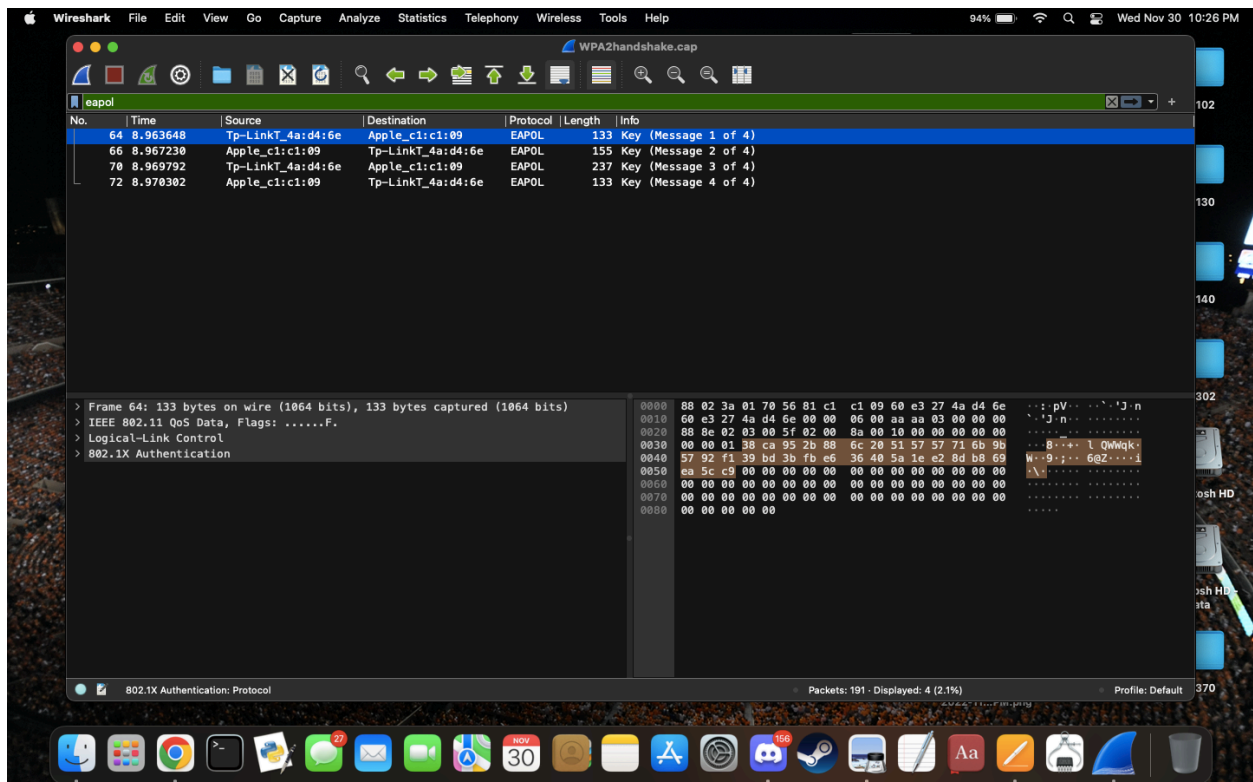
### Question 7

The messages are basically just bytes representing information for encryption/

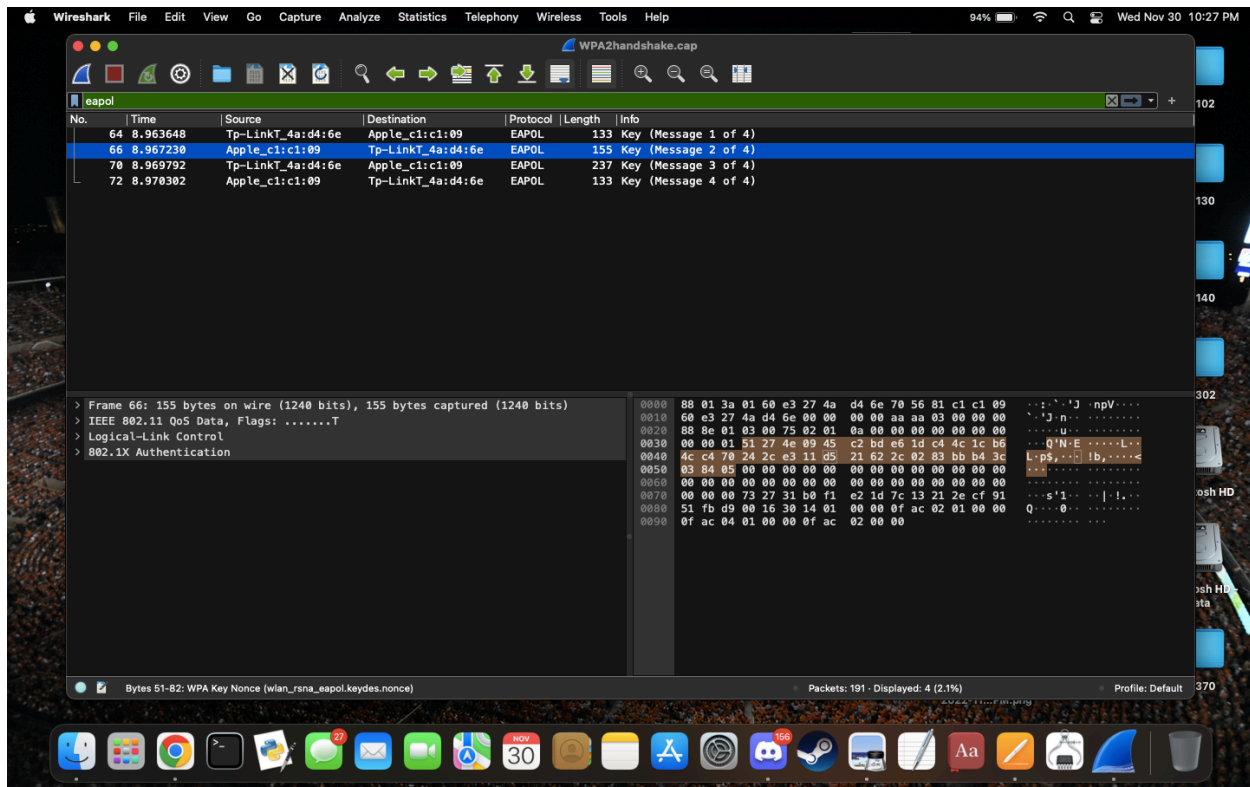
decryption: addresses, keys, etc.

### Question 8

- The ANonce value is 32 bytes, 256 bits long.



- The SNonce value is 32 bytes, 256 bits long.



- I found three non-zero MACs in the messages. They were each 16 bytes, 128 bits long.
- The authenticator sends the ANonce to the receiver. Now the receiver now can make the pairwise key. Then, the client sends the SNonce and the MAC to the host so that the authenticator can have the pairwise key. Now, the authenticator constructs a group key and sends it back with a MAC to protect it.

### Question 9

A. Always.

### Question 10

B. Only if a weak key/passphrase is used.