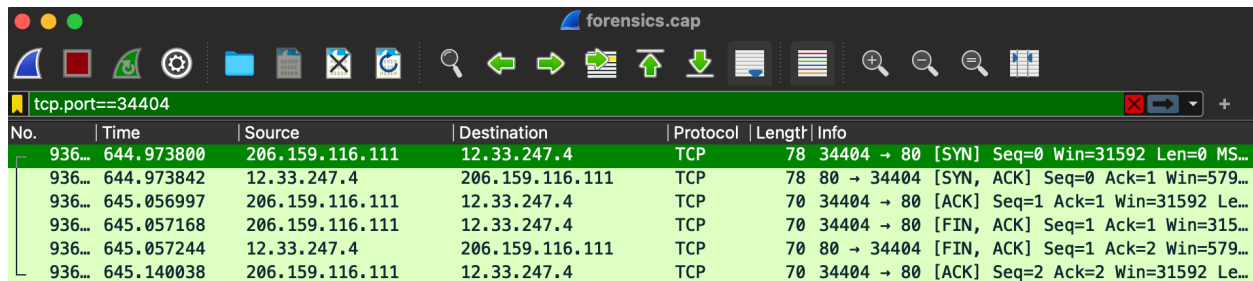


Swasti Mishra
Professor Sun
COSC 366
29 November 2022

COSC 366 Programming Assignment 2

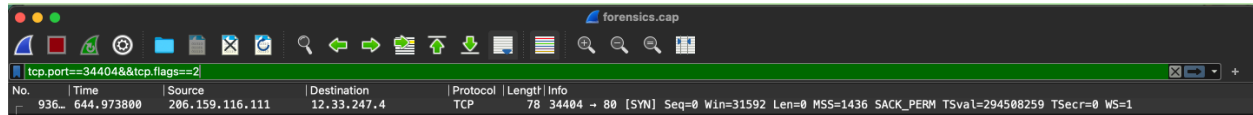
Q1: How many packets are printed out (screenshot)? What are the TCP flags in each packet?
6 packets are printed. The first packet has an SYN flag, the second packet has an SYN and ACK flag, the third packet has an ACK flag, the fourth and fifth have a FIN and ACK flag respectively, and the sixth has an ACK flag.



No.	Time	Source	Destination	Protocol	Length	Info
936...	644.973800	206.159.116.111	12.33.247.4	TCP	78	34404 → 80 [SYN] Seq=0 Win=31592 Len=0 MS...
936...	644.973842	12.33.247.4	206.159.116.111	TCP	78	80 → 34404 [SYN, ACK] Seq=0 Ack=1 Win=579...
936...	645.056997	206.159.116.111	12.33.247.4	TCP	70	34404 → 80 [ACK] Seq=1 Ack=1 Win=31592 Le...
936...	645.057168	206.159.116.111	12.33.247.4	TCP	70	34404 → 80 [FIN, ACK] Seq=1 Ack=1 Win=315...
936...	645.057244	12.33.247.4	206.159.116.111	TCP	70	80 → 34404 [FIN, ACK] Seq=1 Ack=2 Win=579...
936...	645.140038	206.159.116.111	12.33.247.4	TCP	70	34404 → 80 [ACK] Seq=2 Ack=2 Win=31592 Le...

Q2: With this modified filter, what is being filtered for? How many packets are printed out (screenshot)?

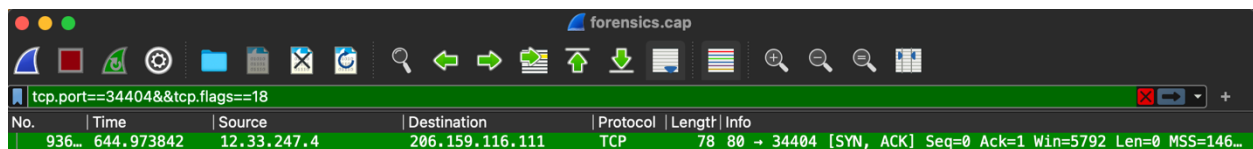
This setting filters for the SYN flag. Because only one packet had only an SYN flag, only one packet is displayed.



No.	Time	Source	Destination	Protocol	Length	Info
936...	644.973800	206.159.116.111	12.33.247.4	TCP	78	34404 → 80 [SYN] Seq=0 Win=31592 Len=0 MSS=1436 SACK_PERM TSval=294508259 TSecr=0 WS=1

Q3: How many packets are printed out (screenshot)? What is your filter?

The filter I used was tcp.port==34404&&tcp.flags==18. Only one packet is output because only one packet had both SYN and ACK flags.



No.	Time	Source	Destination	Protocol	Length	Info
936...	644.973842	12.33.247.4	206.159.116.111	TCP	78	80 → 34404 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=146...

Q4: How many packets are printed out (screenshot)? What is your filter?

Two packets are outputted with the filter tcp.port==34404&&tcp[0xd]&2==2.

No.	Time	Source	Destination	Protocol	Length	Info
936...	644.973800	206.159.116.111	12.33.247.4	TCP	78	34404 → 80 [SYN] Seq=0 Win=31592 Len=0 MSS=1436 SACK_PER...
936...	644.973842	12.33.247.4	206.159.116.111	TCP	78	80 → 34404 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=146...

Q5: What is your filter?

The same two packets are outputted with the filter `tcp.port==34404&&tcp.flags.syn==2`.

No.	Time	Source	Destination	Protocol	Length	Info
936...	644.973800	206.159.116.111	12.33.247.4	TCP	78	34404 → 80 [SYN] Seq=0 Win=31592 Len=0 MSS=1436 SACK_PER...
936...	644.973842	12.33.247.4	206.159.116.111	TCP	78	80 → 34404 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=146...

Q6: What are the IP addresses of the HTTP and DNS servers? (If there are multiple HTTP or DNS servers, show the IP address all of them.) Describe the method you used.

There are multiple HTTP and DNS servers. Using the following filters, we can find them.

- `tcp.port==53&&dns` yields a DNS server of 12.33.247.3
- `udp.port==53&&dns&&ip.src!=12.33.247.3&&ip.src!=12.33.246.130` yields a DNS server of 12.33.246.131
- `udp.port==53&&dns&&ip.src!=12.33.247.3` yields a DNS server of 12.33.246.130
- `udp.port==53&&dns&&ip.src!=12.33.247.3&&ip.src!=12.33.246.130&&ip.src!=12.33.246.131` yields a DNS server of 12.33.247.11
- `tcp.port == 80&&http.server` yields an HTTP server of 12.33.247.10
- `tcp.port == 80&&http.server && ip.src!=12.33.247.10` yields an HTTP server of 12.33.247.4

Q7: What are the messages you see?

These are the messages filtered.

No.	Time	Source	Destination	Protocol	Length	Info
64	8.963648	Tp-LinkT_4a:d4:6e	Apple_c1:c1:09	EAPOL	133	Key (Message 1 of 4)
66	8.967230	Apple_c1:c1:09	Tp-LinkT_4a:d4:6e	EAPOL	155	Key (Message 2 of 4)
70	8.969792	Tp-LinkT_4a:d4:6e	Apple_c1:c1:09	EAPOL	237	Key (Message 3 of 4)
72	8.970302	Apple_c1:c1:09	Tp-LinkT_4a:d4:6e	EAPOL	133	Key (Message 4 of 4)

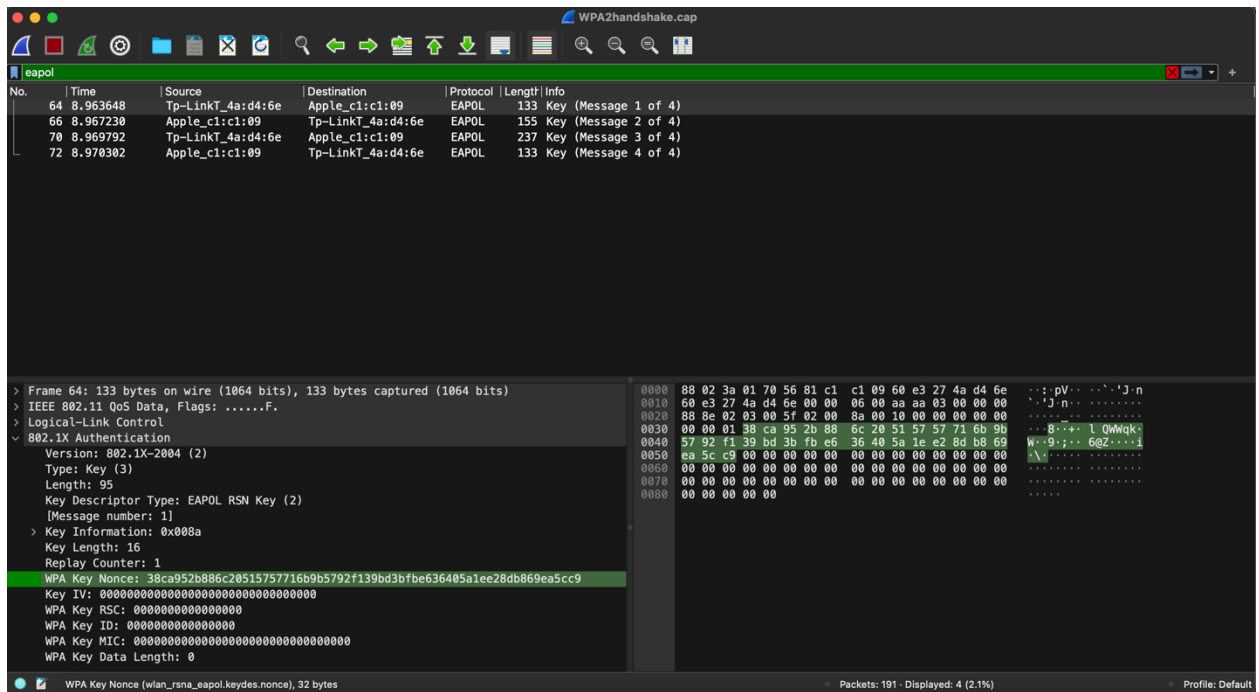
Q8: Inspect these messages by expanding them.

- What is the Anonce value (screenshot with this number highlighted)? How long is it in bits?

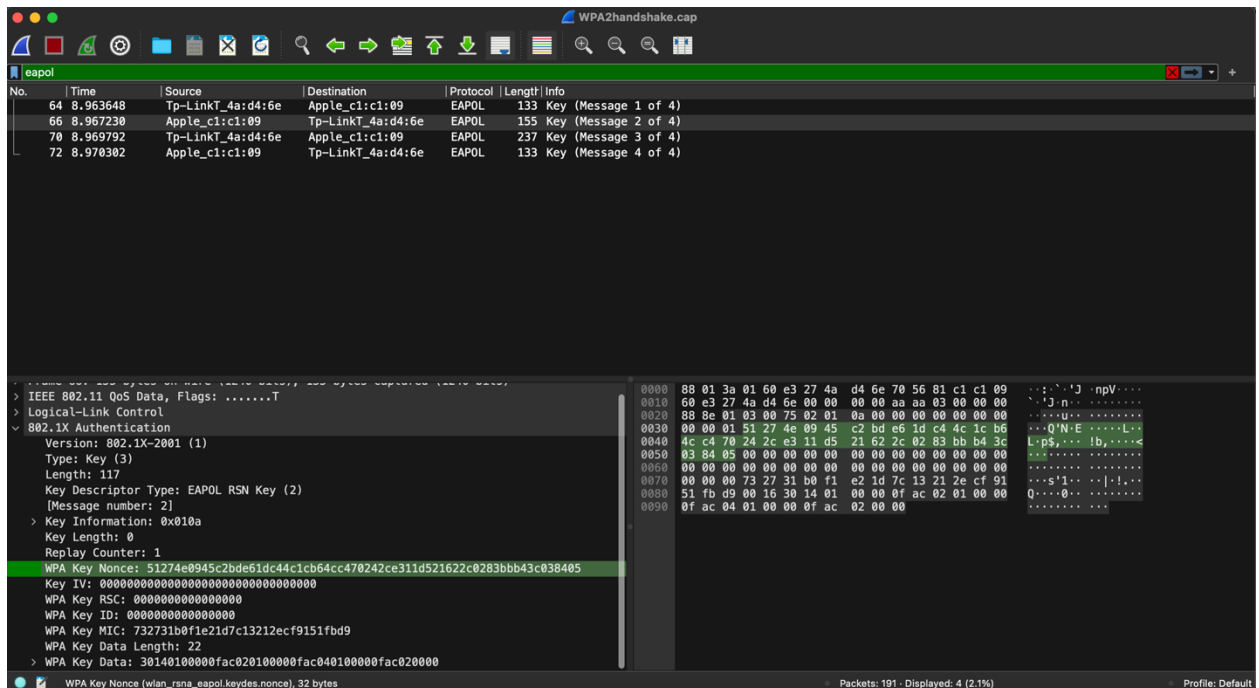
The value is

38ca952b886c20515757716b9b5792f139bd3bfbe636405a1ee28db869ea5cc9.

It is 256 bits long.



- What is the Snonce value (Screenshot with this number highlighted)? How long is it?
 The value is
 51274e0945c2bde61dc44c1cb64cc470242ce311d521622c0283bbb43c038405.
 It is 256 bits long.



- **How many different non-zero MACs, or Message Authentication Codes are there in the messages? How long are they?**

There are three non-zero MACs that are each 48-bit addresses.

- **Explain the use of the nonces and MACs in this scenario.**

The nonces and MACs are used for calculating both the pairwise master key (PMK) and the pairwise transit key (PTK). The PTK is a unique key used to encrypt traffic between the client station and access point, and the PMK is generated when a device authenticates with the access point.

Q9: When can WEP be cracked?

A: Always.

Q10: When can WPA2 be cracked?

B: Only if a weak key/passphrase is chosen.