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?**

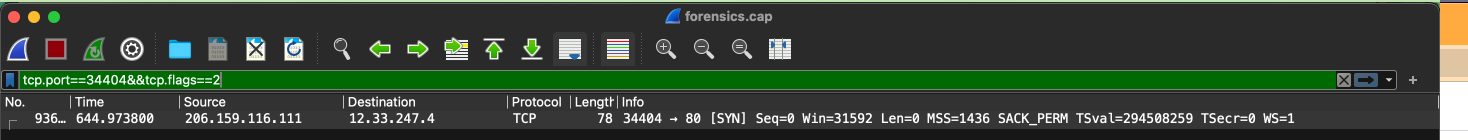
6 packets are printed. The first packet has an SYN flag, the second packet has an SYN and ACK flag, the third packet has an ACK flag, the fourth and fifth have a FIN and ACK flag respectively, and the sixth has an ACK flag.

Graphical user interface

Description automatically generated

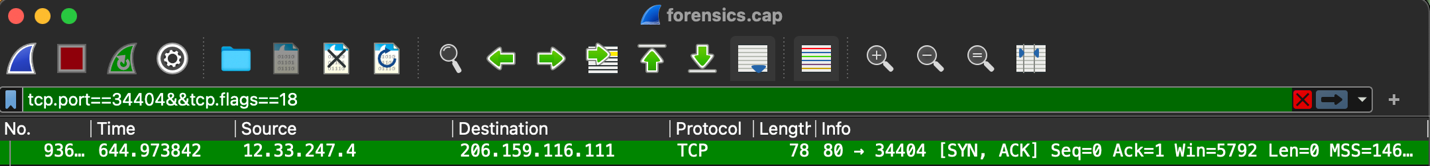
**Q2: With this modified filter, what is being filtered for? How many packets are printed out (screenshot)?**

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



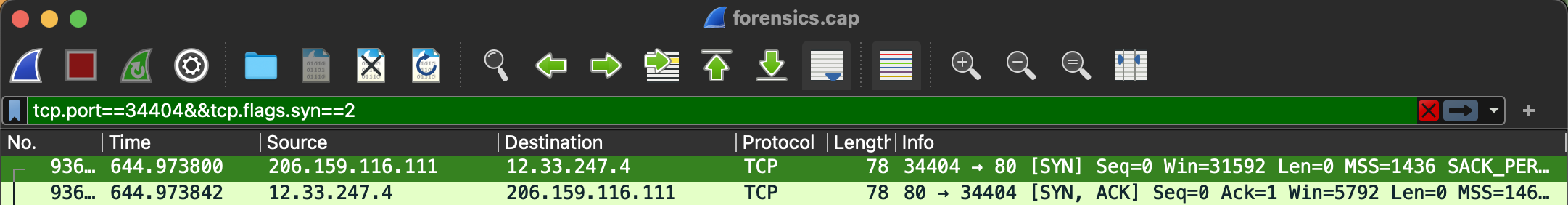
**Q3: How many packets are printed out (screenshot)? What is your filter?**

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.



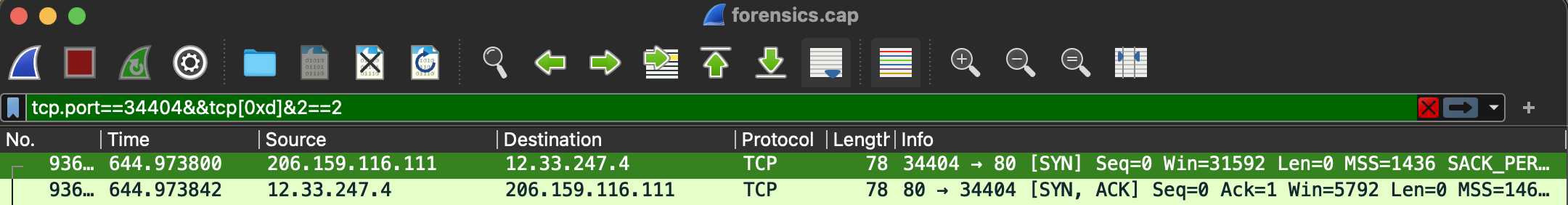
**Q4: How many packets are printed out (screenshot)? What is your filter?**

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



**Q5: What is your filter?**

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



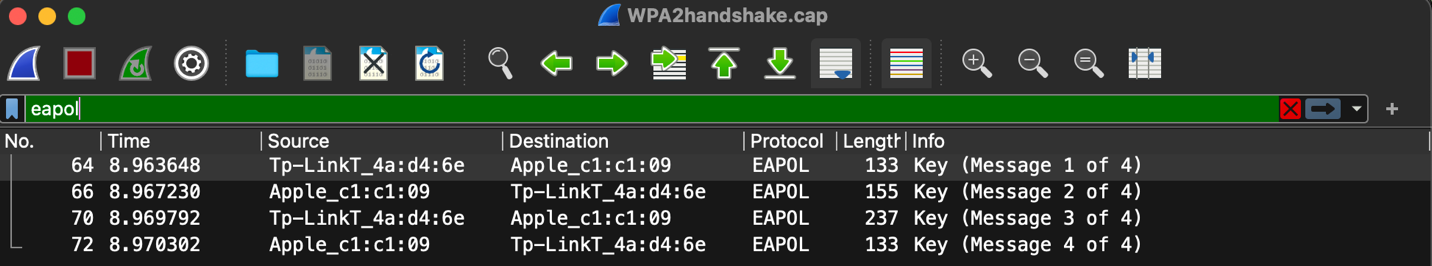
**Q6: What are the IP addresses of the HTTP and DNS servers? (If there are multiple   
HTTP or DNS servers, show the IP address all of them.) Describe the method you used.**

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.

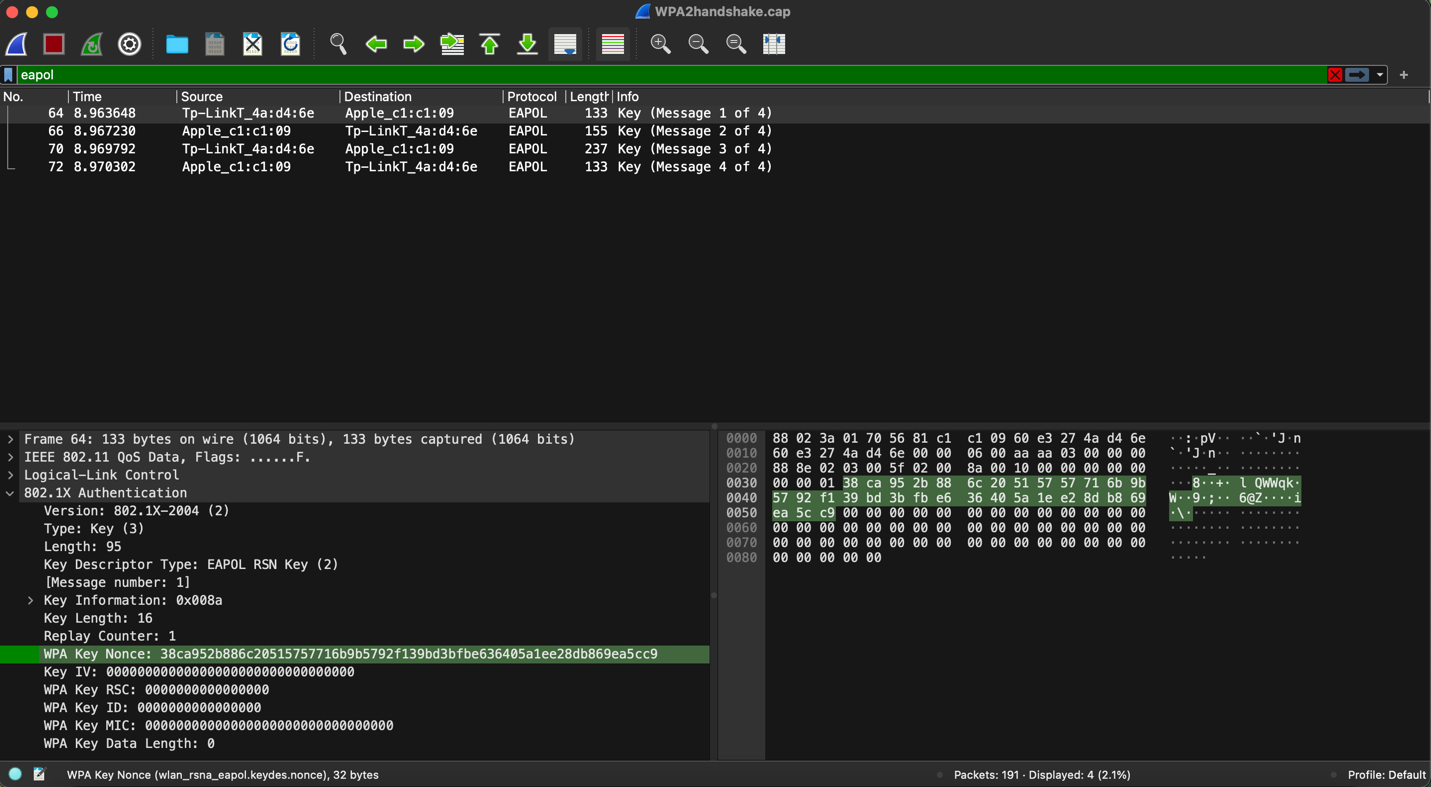
****

**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.

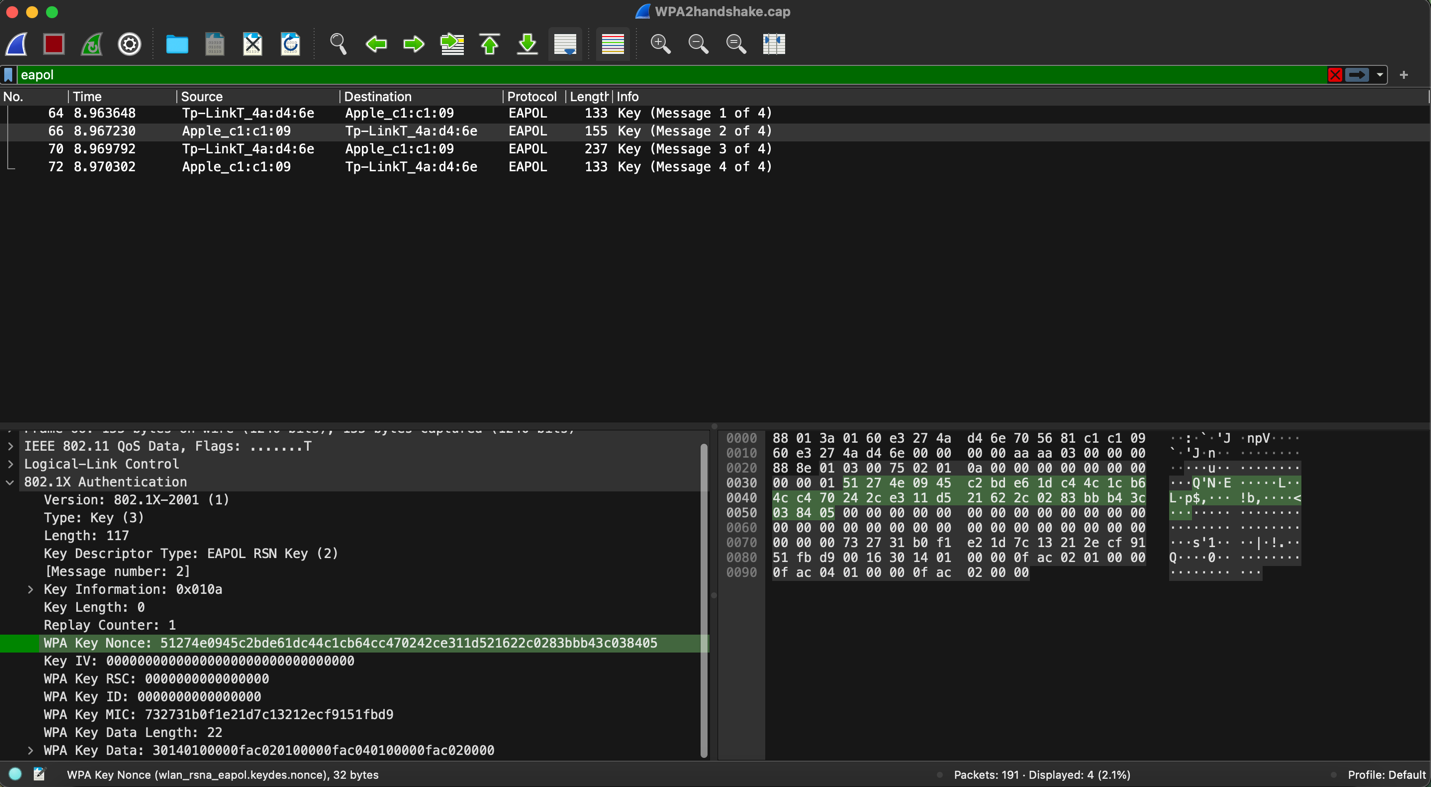
****

* **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.