Lab 7 Report

By Julian Flum and Miftahul Huq

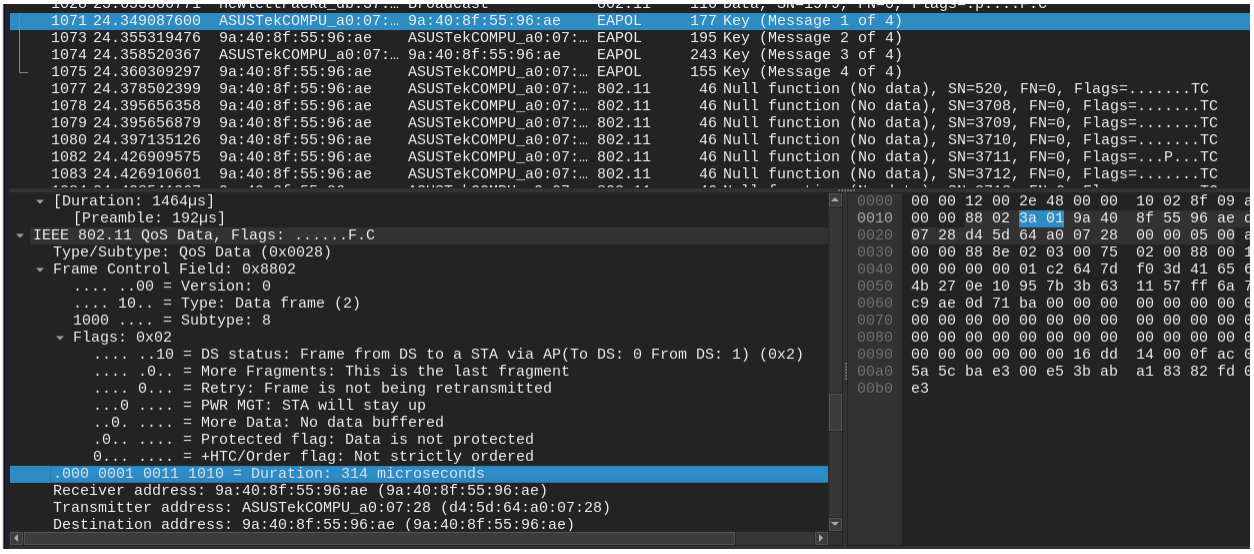
Activity 1

Step 4

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
D4:5D:64:A0:27:20	-31	112	13 0	8	720	WPA3 CCMP	SAE	12345-2.4
D4:5D:64:A0:0C:40	-21	161	0 0	7	720	WPA3 CCMP	SAE	garlec
D4:5D:64:A0:0C:18	-26	111	16 0	9	720	WPA2 CCMP	PSK	LucasNDevonL7
D4:5D:64:A0:07:28	-14	202	0 0	8	720	WPA3 CCMP	SAE	Garfield2.4

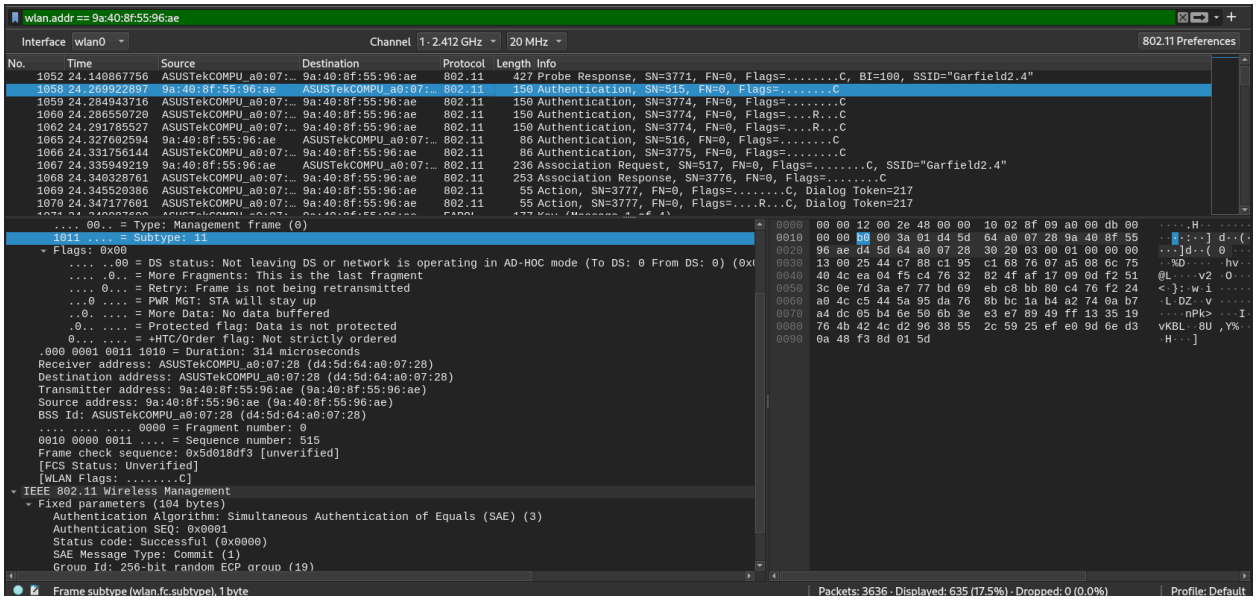
Encryption Type: WPA3
Cipher: CCMP
Authentication: SAE

Q1. What was the duration of one of the management frames you captured (indicated in its MAC header)?



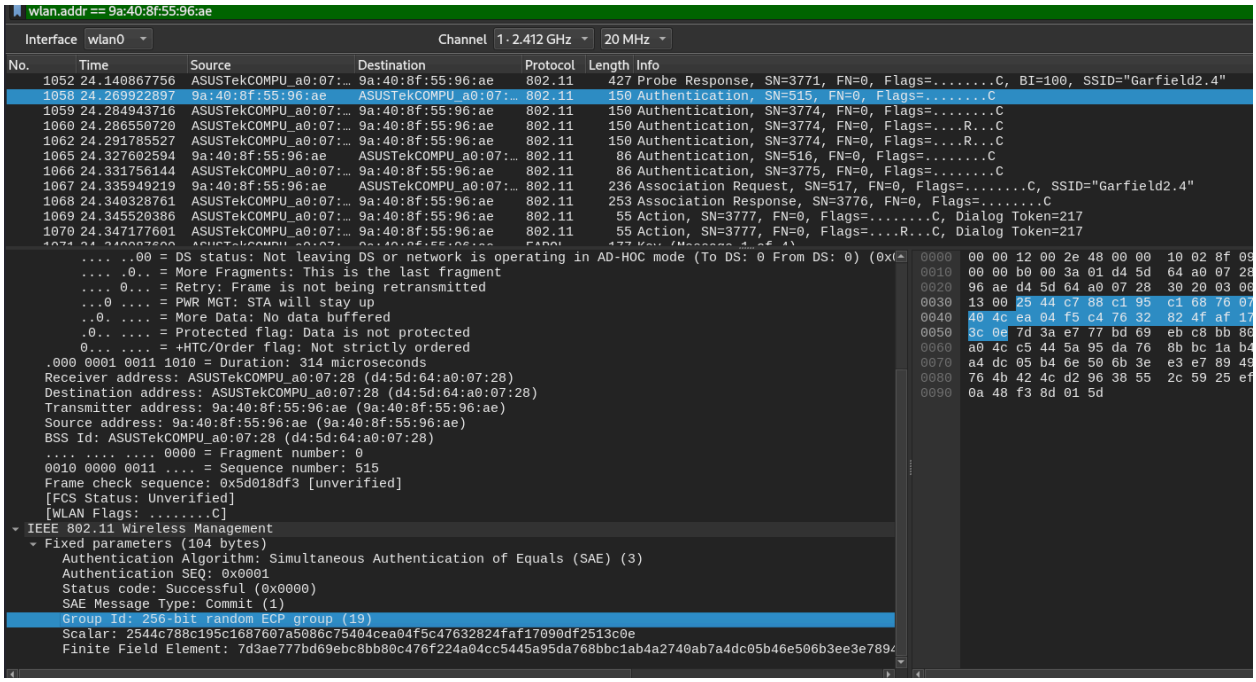
The duration was 314 microseconds.

Q2. Identify the SAE messages in the capture. What type of frame is used for piggybacking SAE messages? What are the sequence numbers of the SAE frames that were sent from the AP to the client?



The type of management frame that's being piggybacked off of is the Authentication frame. The sequence numbers are 515, 3774, 516, are 3775.

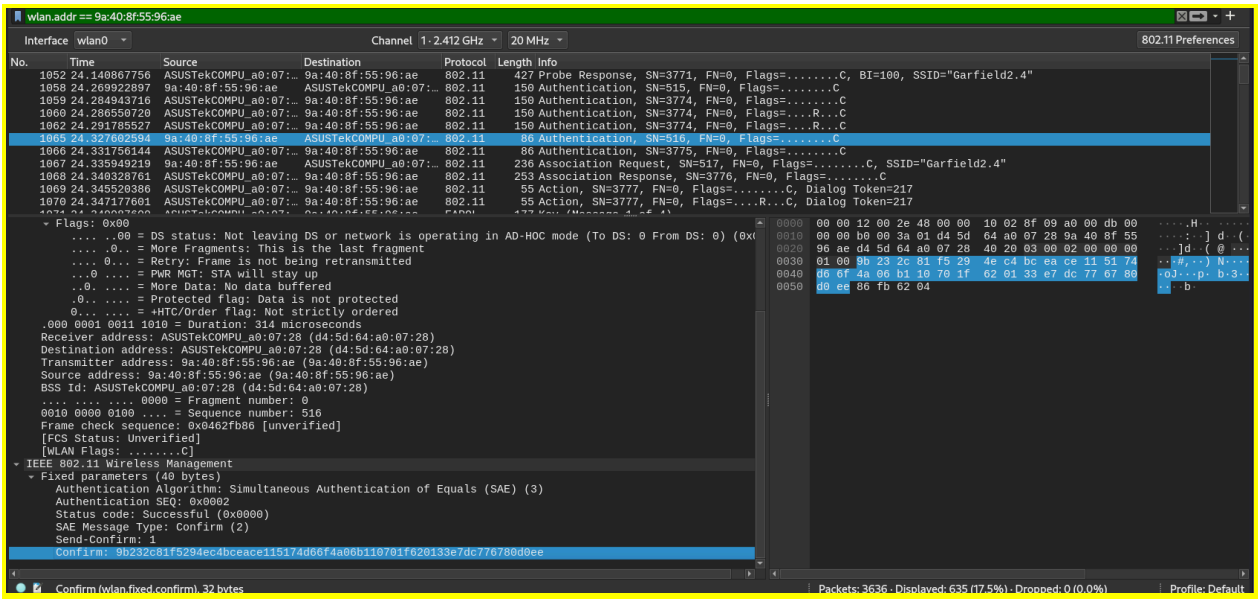
Q3. In one of the SAE Commit messages, identify the elliptic curve group size, the scalar value, and the masked password element. Briefly explain what each of these fields is used for in SAE.

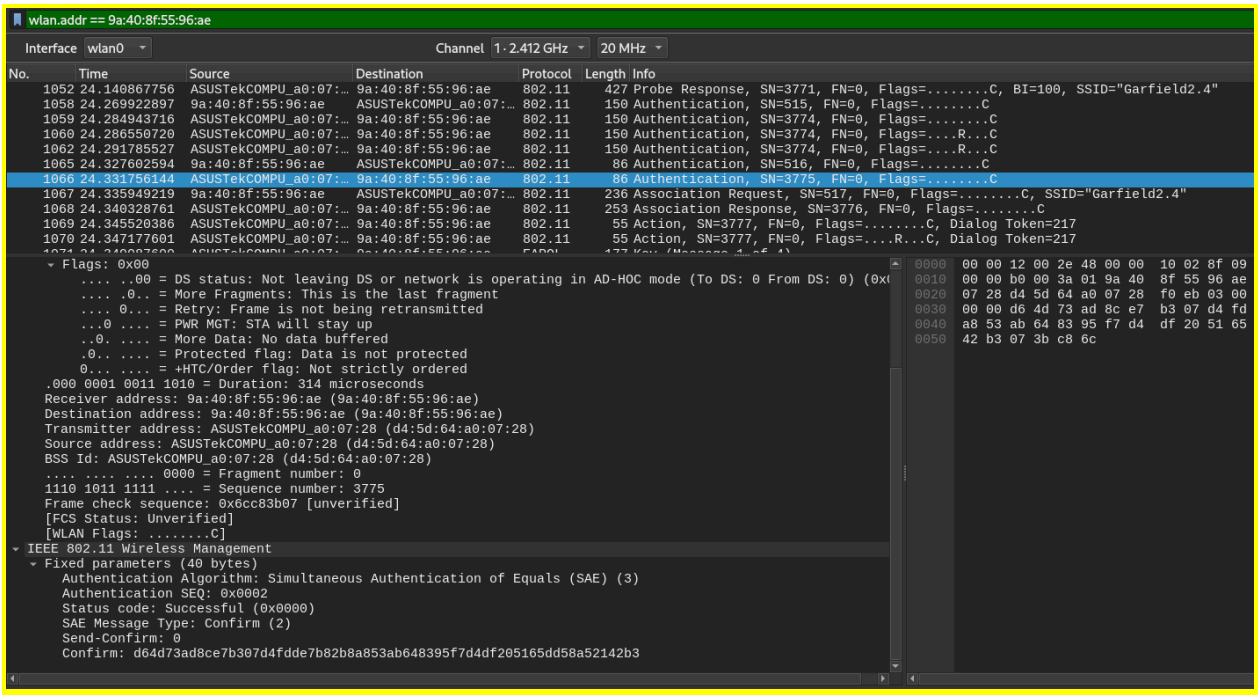


The group size is 256 bits, the scalar value is 2544c788c195c1687607a5086c75404cea04f5c47632824faf17090df2513c0e, and the masked password element is 7d3ae777bd69ebc8bb80c476f224a04cc5445a95da768bbc1ab4a2740ab7a4dc05b46e506b3ee3e78949ff133519764b424cd29638552c5925efe09d6ed30a48.

The size helps to determine the length of the data, which helps determine what the final decrypted value will look like, the scalar is used to de-obfuscate the disguised password data, and the masked password element is what will be decrypted to reveal the password.

Q4. In one of the SAE Confirm messages, identify the token element. Briefly explain what this value is for.

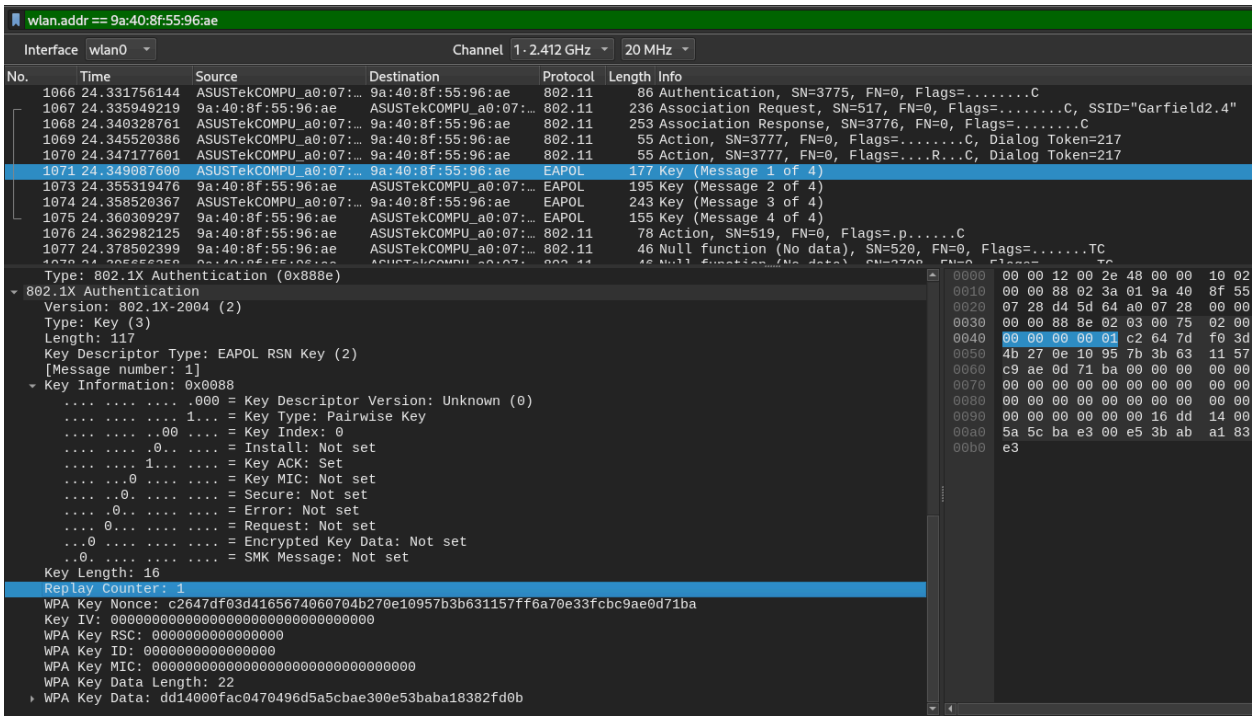


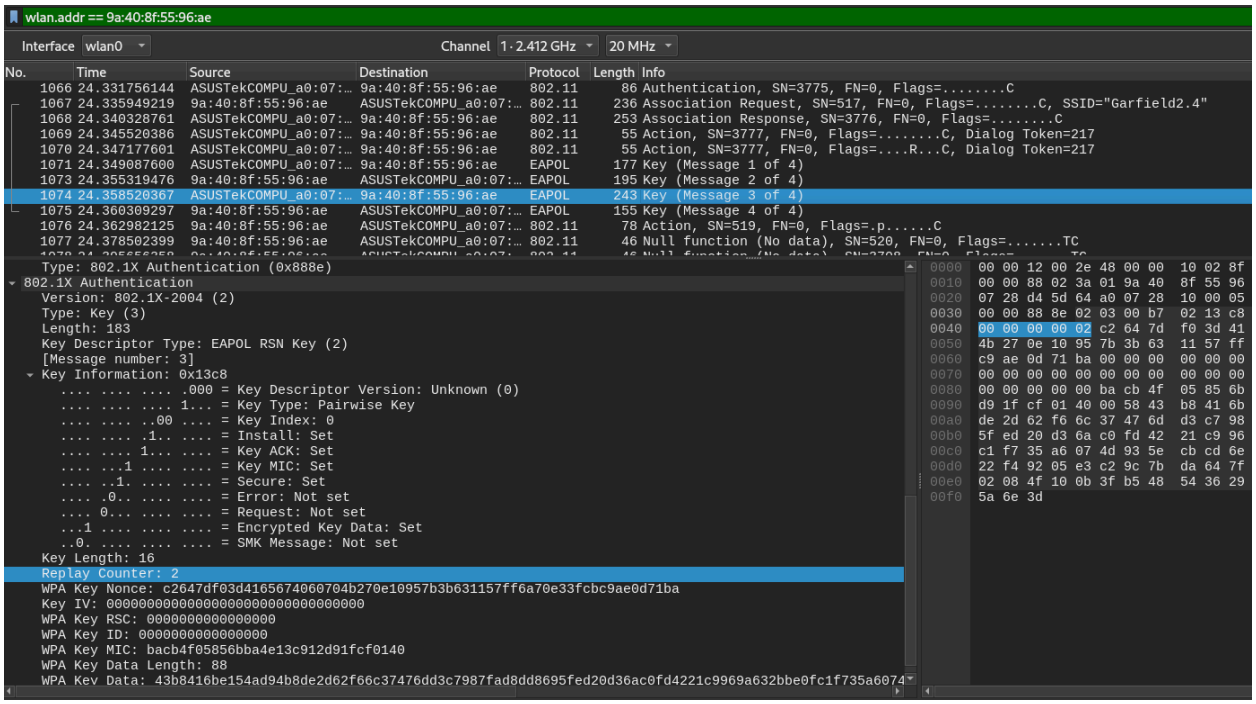


The token elements are 9b232c81f5294ec4bceace115174d66f4a06b110701f620133e7dc776780d0ee and d64d73ad8ce7b307d4fdde7b82b8a853ab648395f7d4df205165dd58a52142b3

The token element is derived using the shared secret, and then is used to confirm the guess, and derive the PMK at both sides.

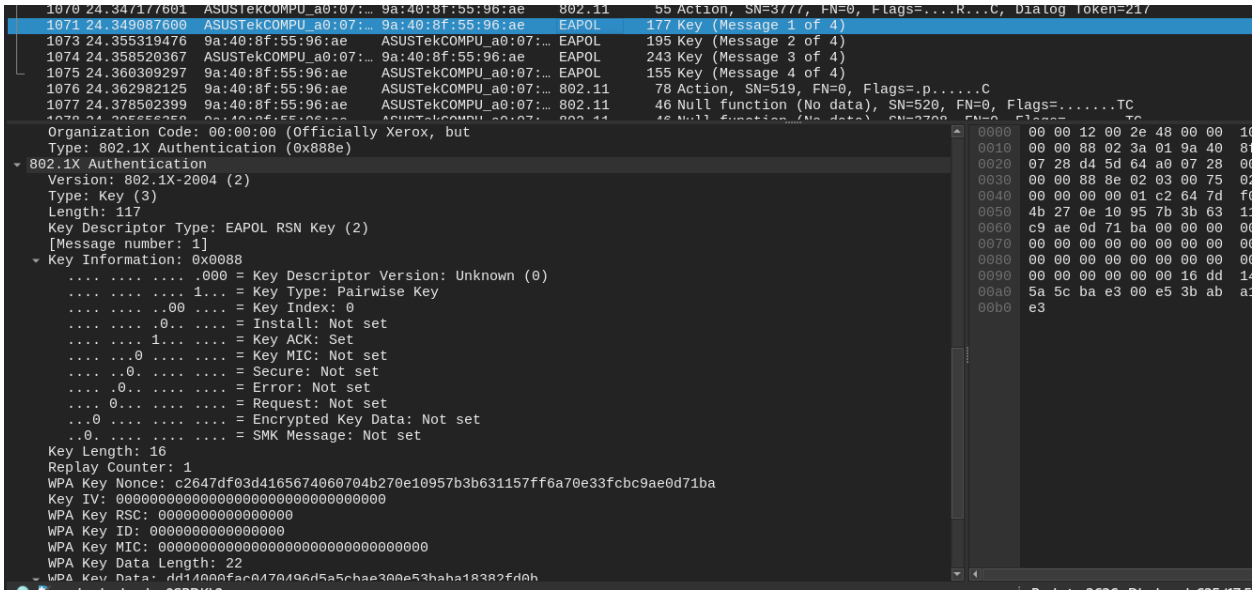
Q5. Examine the 4-way handshake messages and identify the value of the replay counter in each.

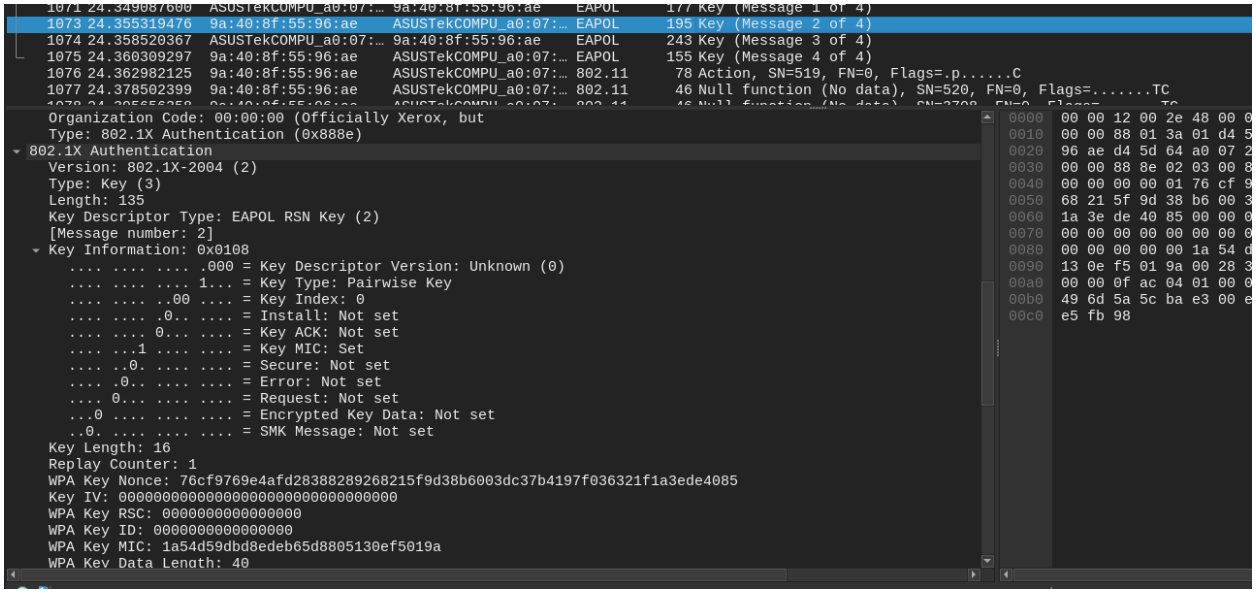


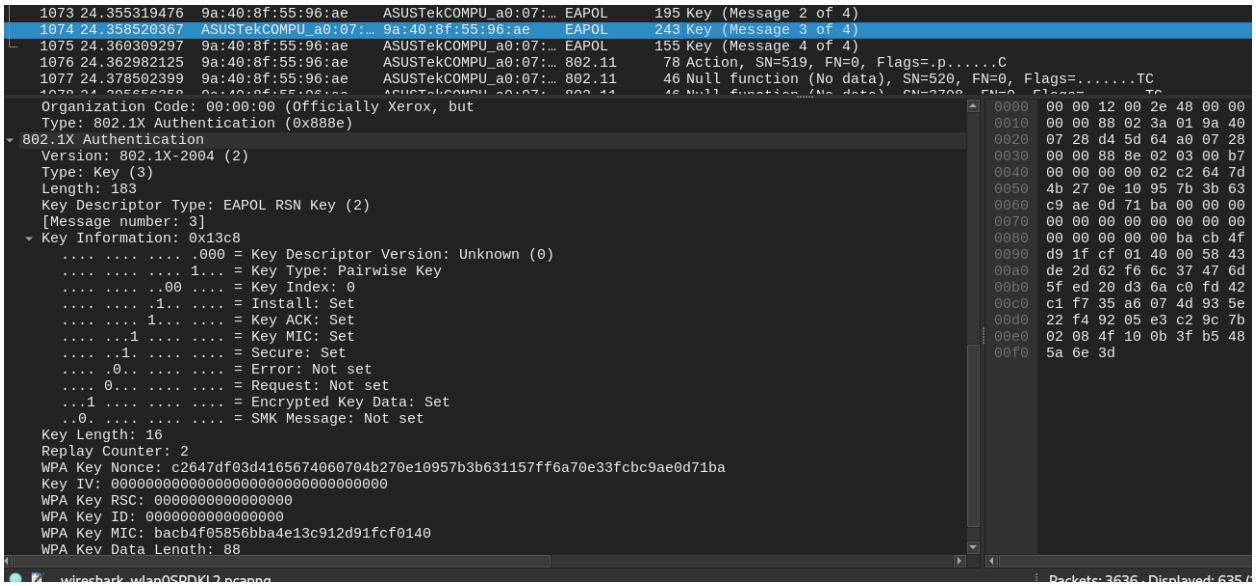


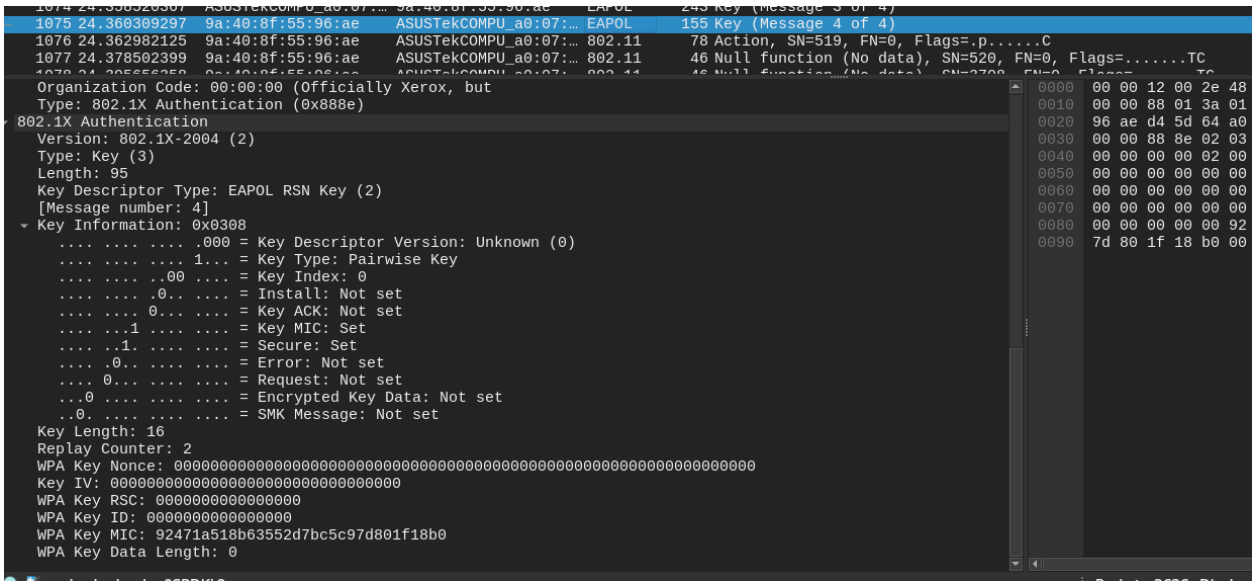
The replay counter value is 1 in the first two parts of the 4-way handshake, and 2 in the second parts of the 4-way handshake.

Q6. Inspect the Key Information flags in the 4-way handshake messages. Which messages do set the Install, Key Ack, and Secure fields, respectively? Briefly explain why they are sent in the order you observed.





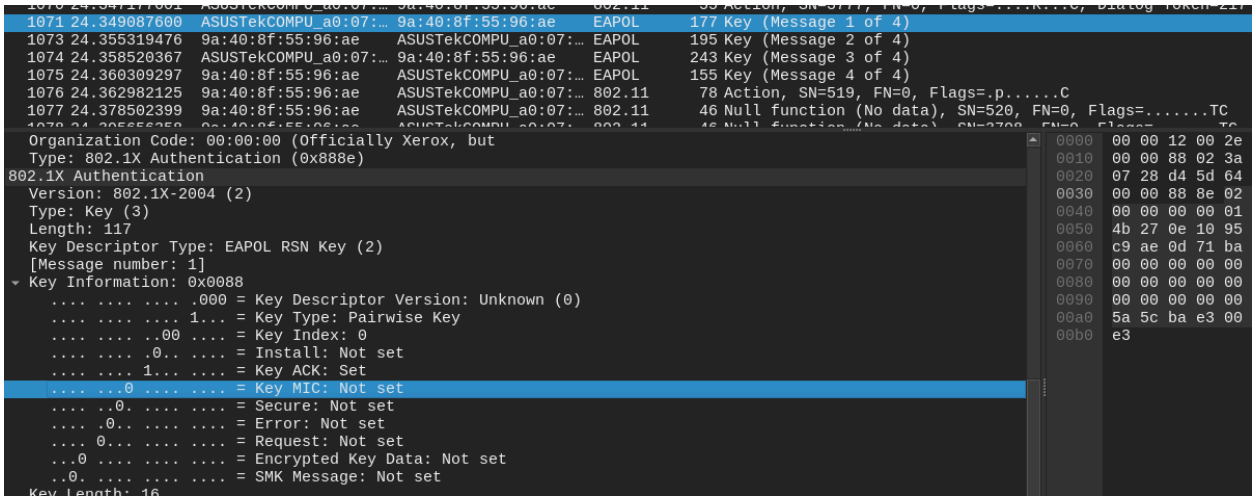


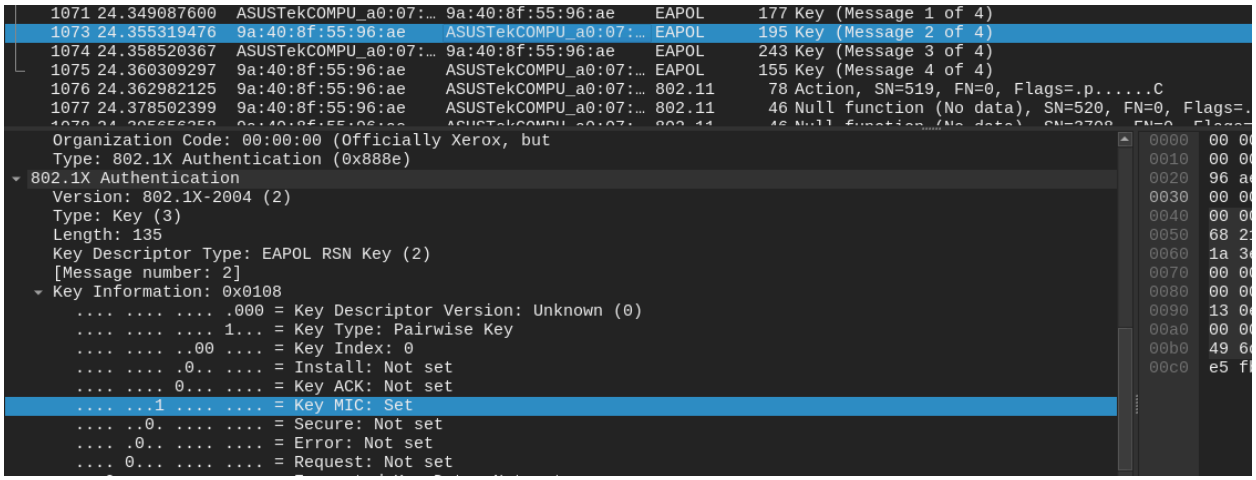


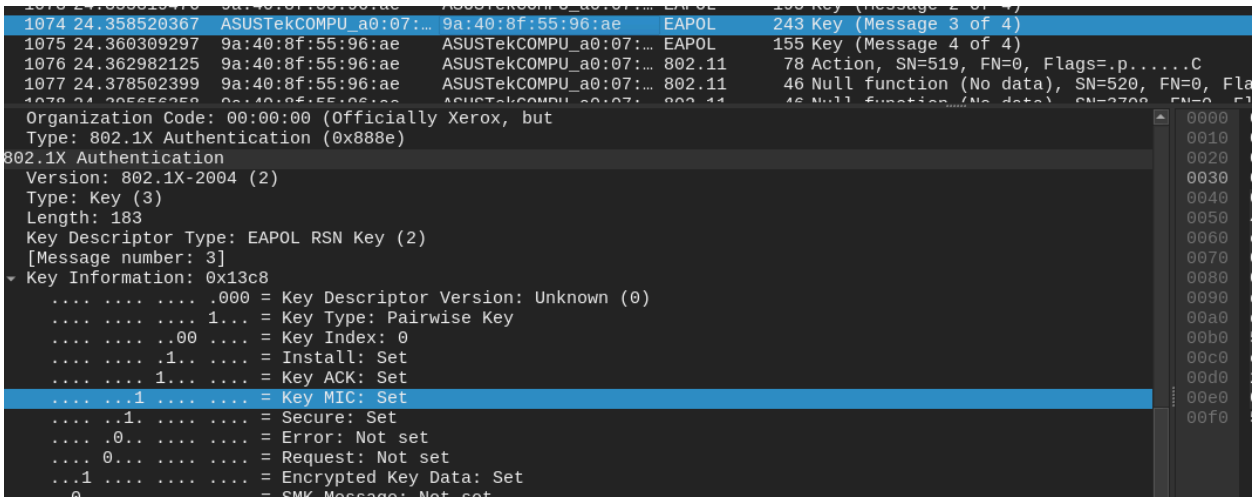
The Install is set by message 3, the Ack is set by messages 1 and 3, and the Secure field is set by messages 3 and 4.

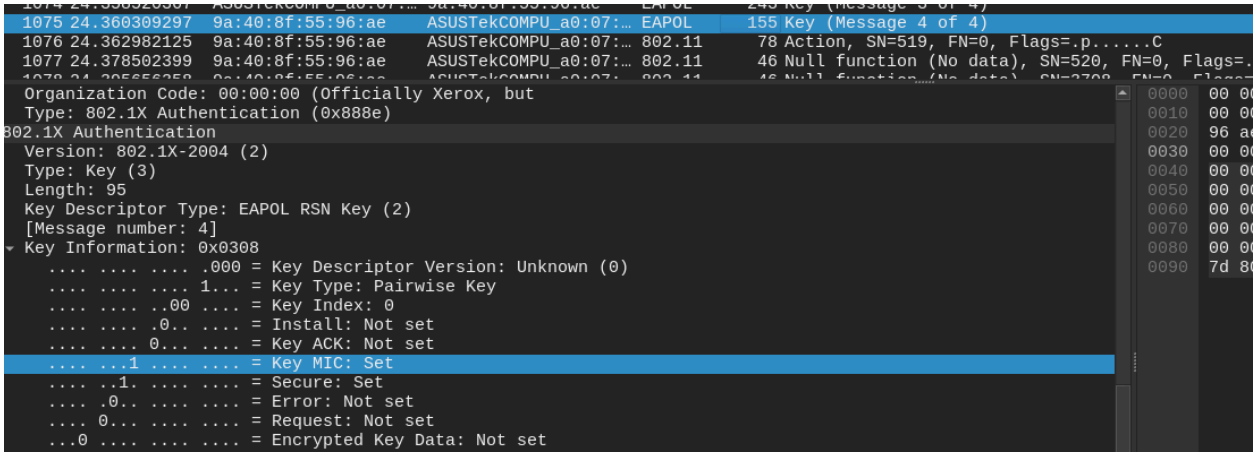
The install is set at message 3, because the authenticator needs to inform the supplicant at the end, and 3 is the final message from the authenticator. The acknowledgement is set by messages 1 and 3, as the authenticator needs to let the supplicant know the key is proper during both of its messages. The secure field is set in messages 3 and 4, as those are the end of the handshake, and it's meant to ensure that the information was secured by both sides.

Q7. Inspect the MIC field in each 4-way handshake message. Which message(s) have non-zero MICs? Explain why those message(s) contain non-zero MIC values (and why other message(s) have an all-zero MIC)


1071 24.349087600 ASUSTekCOMPU_a0:07:… 9a:40:8f:55:96:ae EAPOL 177 Key (Message 1 of 4)
1073 24.355319476 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… EAPOL 195 Key (Message 2 of 4)
1074 24.358520367 ASUSTekCOMPU_a0:07:… 9a:40:8f:55:96:ae EAPOL 243 Key (Message 3 of 4)
1075 24.360309297 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… EAPOL 155 Key (Message 4 of 4)
1076 24.362982125 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… 802.11 78 Action, SN=519, FN=0, Flags=.p.....C
1077 24.378502399 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… 802.11 46 Null function (No data), SN=520, FN=0, Flags=.....TC
Organization Code: 00:00:00 (Officially Xerox, but
Type: 802.1X Authentication (0x888e)
802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 117
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 1]
Key Information: 0x0088
.... .000 = Key Descriptor Version: Unknown (0)
.... 1... = Key Type: Pairwise Key
....00 .... = Key Index: 0
.... .0.. .... = Install: Not set
.... 1... .... = Key ACK: Set
....0 .... = Key MIC: Not set
.... ..0. .... = Secure: Not set
.... .0.. .... = Error: Not set
.... 0... .... = Request: Not set
...0 .... = Encrypted Key Data: Not set
..0. .... = SMK Message: Not set
Key Length: 16
0000 00 00 12 00 2e
0010 00 00 88 02 3a
0020 07 28 d4 5d 64
0030 00 00 88 8e 02
0040 00 00 00 00 01
0050 4b 27 0e 10 95
0060 c9 ae 0d 71 ba
0070 00 00 00 00 00
0080 00 00 00 00 00
0090 00 00 00 00 00
00a0 5a 5c ba e3 00
00b0 e3


1071 24.349087600 ASUSTekCOMPU_a0:07:… 9a:40:8f:55:96:ae EAPOL 177 Key (Message 1 of 4)
1073 24.355319476 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… EAPOL 195 Key (Message 2 of 4)
1074 24.358520367 ASUSTekCOMPU_a0:07:… 9a:40:8f:55:96:ae EAPOL 243 Key (Message 3 of 4)
1075 24.360309297 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… EAPOL 155 Key (Message 4 of 4)
1076 24.362982125 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… 802.11 78 Action, SN=519, FN=0, Flags=.p.....C
1077 24.378502399 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… 802.11 46 Null function (No data), SN=520, FN=0, Flags=.
Organization Code: 00:00:00 (Officially Xerox, but
Type: 802.1X Authentication (0x888e)
802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 135
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 2]
Key Information: 0x0108
.... .000 = Key Descriptor Version: Unknown (0)
.... 1... = Key Type: Pairwise Key
....00 .... = Key Index: 0
.... .0.. .... = Install: Not set
.... 0... .... = Key ACK: Not set
....1 .... = Key MIC: Set
.... ..0. .... = Secure: Not set
.... .0.. .... = Error: Not set
.... 0... .... = Request: Not set

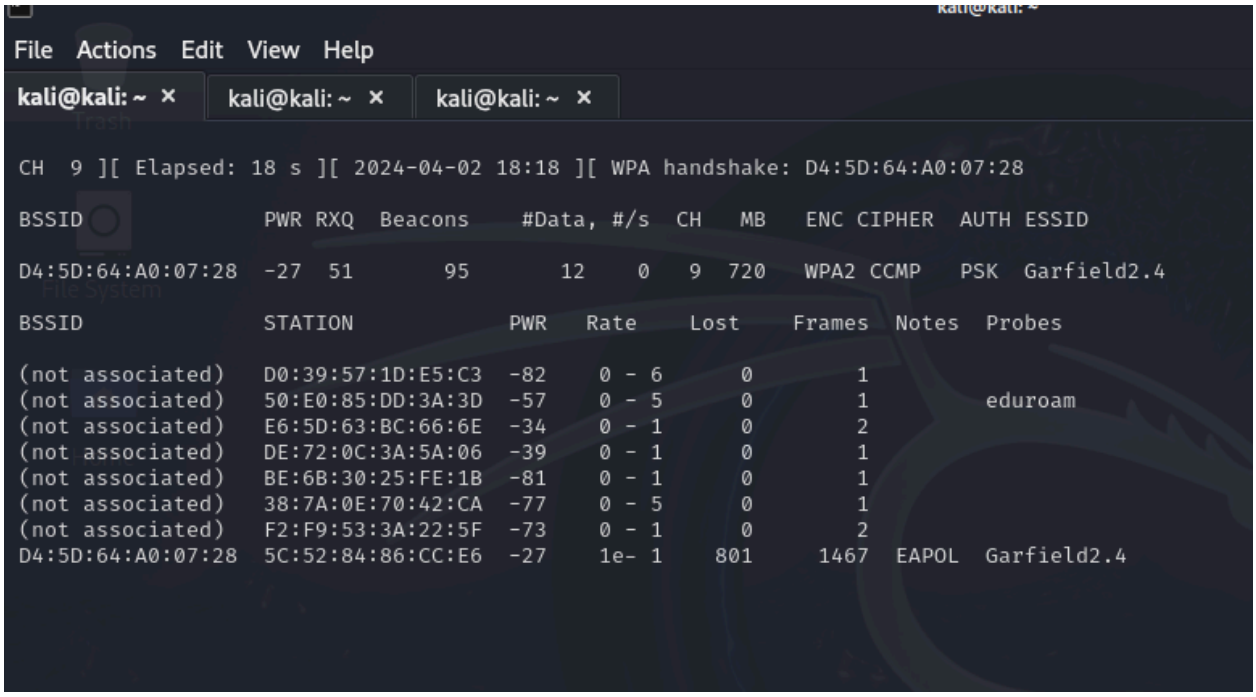

1074 24.358520367 ASUSTekCOMPU_a0:07:… 9a:40:8f:55:96:ae EAPOL 243 Key (Message 3 of 4)
1075 24.360309297 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… EAPOL 155 Key (Message 4 of 4)
1076 24.362982125 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… 802.11 78 Action, SN=519, FN=0, Flags=.p.....C
1077 24.378502399 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:… 802.11 46 Null function (No data), SN=520, FN=0, Fla
Organization Code: 00:00:00 (Officially Xerox, but
Type: 802.1X Authentication (0x888e)
802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 183
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 3]
Key Information: 0x13c8
.... .000 = Key Descriptor Version: Unknown (0)
.... 1... = Key Type: Pairwise Key
....00 .... = Key Index: 0
.... .1.. .... = Install: Set
.... 1... .... = Key ACK: Set
....1 .... = Key MIC: Set
.... ..1. .... = Secure: Set
.... .0.. .... = Error: Not set
.... 0... .... = Request: Not set
...1 .... = Encrypted Key Data: Set



Messages 2, 3, and 4 have non-zero MIC values. This field identifies when the MIC is being passed back and forth, which happens in every step in the handshake, except for the first message. So, when it's non-zero, the MIC is present. When it's all-zero, the MIC is not present. This lines up with 1 not having MIC, and 2, 3, and 4 all having MIC.

Activity 2

Q8. Was the attack successful? Briefly describe why the attack does (or does not) work and include screenshot(s) from your capture as necessary to support your answer.



Yes. This is because protected management frames are meant to protect from attacks like this, since it prevents deauthentication frames from being sent. Since they were not present, the deauth frame was able to work.

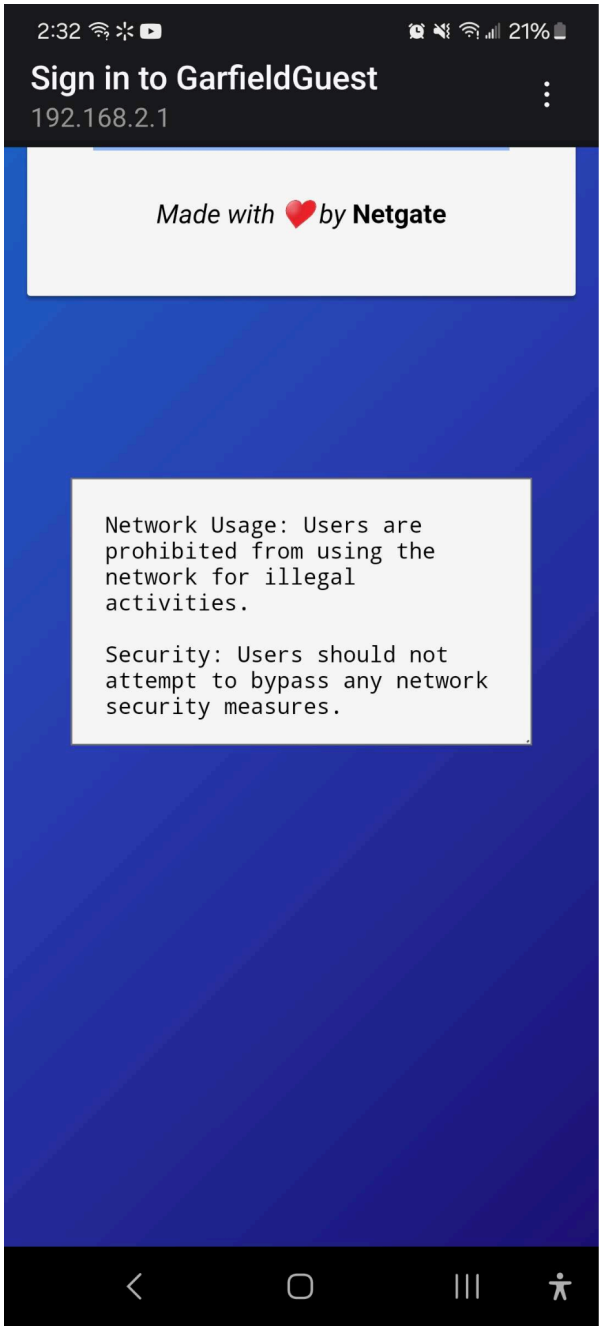
Q9. Was the attack successful this time? Briefly describe why the attack does (or does not) work this time.

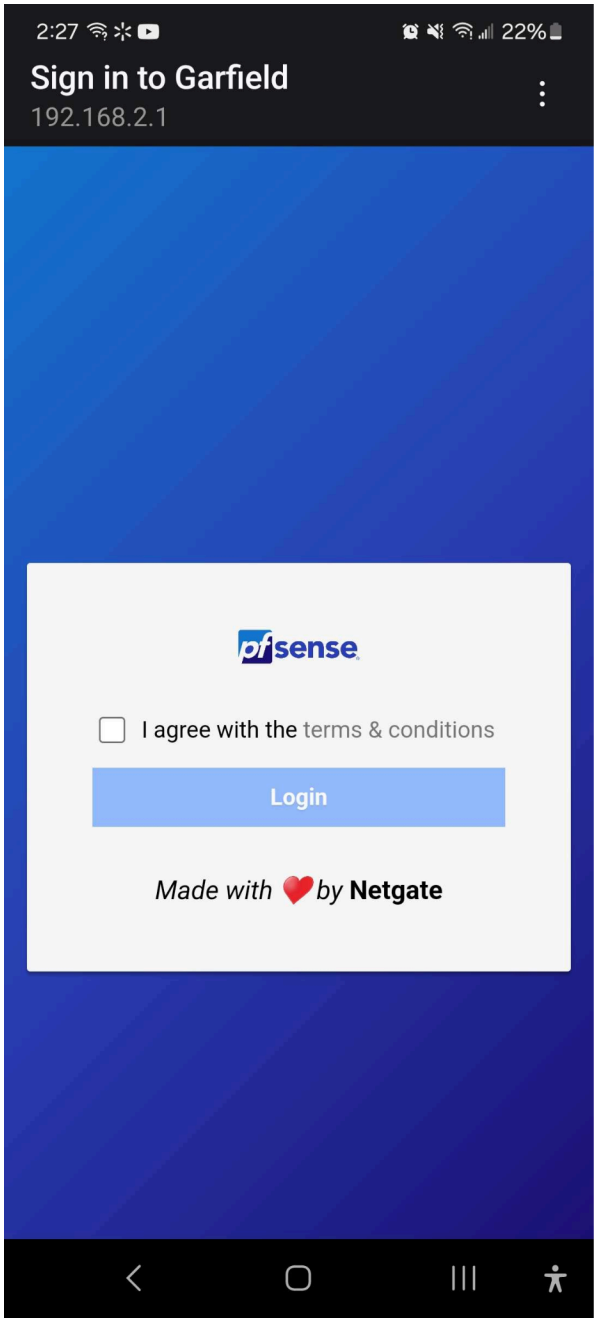
No. This is because protected management frames are meant to protect from attacks like this, since it prevents deauthentication frames from being sent. Since they were here, deauth frames could not be sent.

Q10. Were you able to disable management frame protection for WPA3? Briefly explain why (or why not).

No. This is because protected management frames are mandatory in WPA3 onward, which prevents the attack.

Activity 3





SSID: Garfield
wireless security: lasagna123

Router Login: GarfieldCat
Password: jon_arbuckle