

# 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

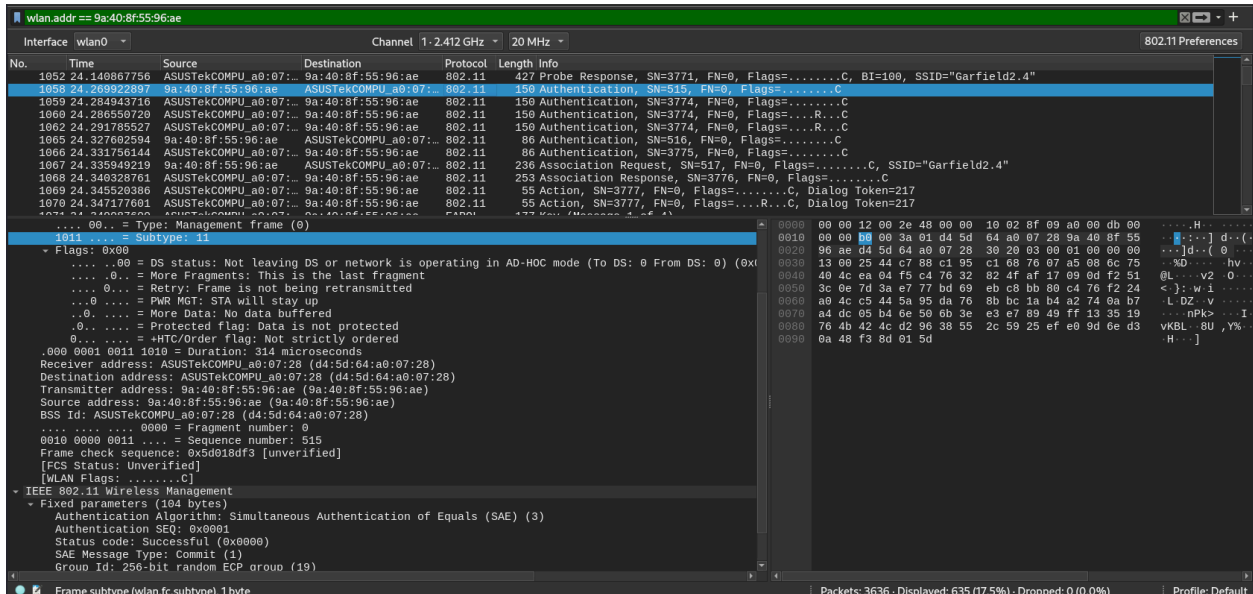
Authentication: SAE

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

The image shows a Wireshark packet capture of an IEEE 802.11 QoS Data frame. The packet list on the left shows a frame at 1071.24 seconds with a duration of 1464µs. The packet details pane shows the frame structure: Preamble (192µs), IEEE 802.11 QoS Data (Flags: F.C), Type/Subtype: QoS Data (0x0028), Frame Control Field: 0x8802, Version: 0, Type: Data frame (2), Subtype: 8, Flags: 0x02, DS status: Frame from DS to a STA via AP (To DS: 0, From DS: 1) (0x2), More Fragments: This is the last fragment, Retry: Frame is not being retransmitted, PWR MGT: STA will stay up, More Data: No data buffered, Protected flag: Data is not protected, HT/Order flag: Not strictly ordered, and Duration: 314 microseconds. The packet bytes pane shows the raw data, with the duration field (314) highlighted in blue.

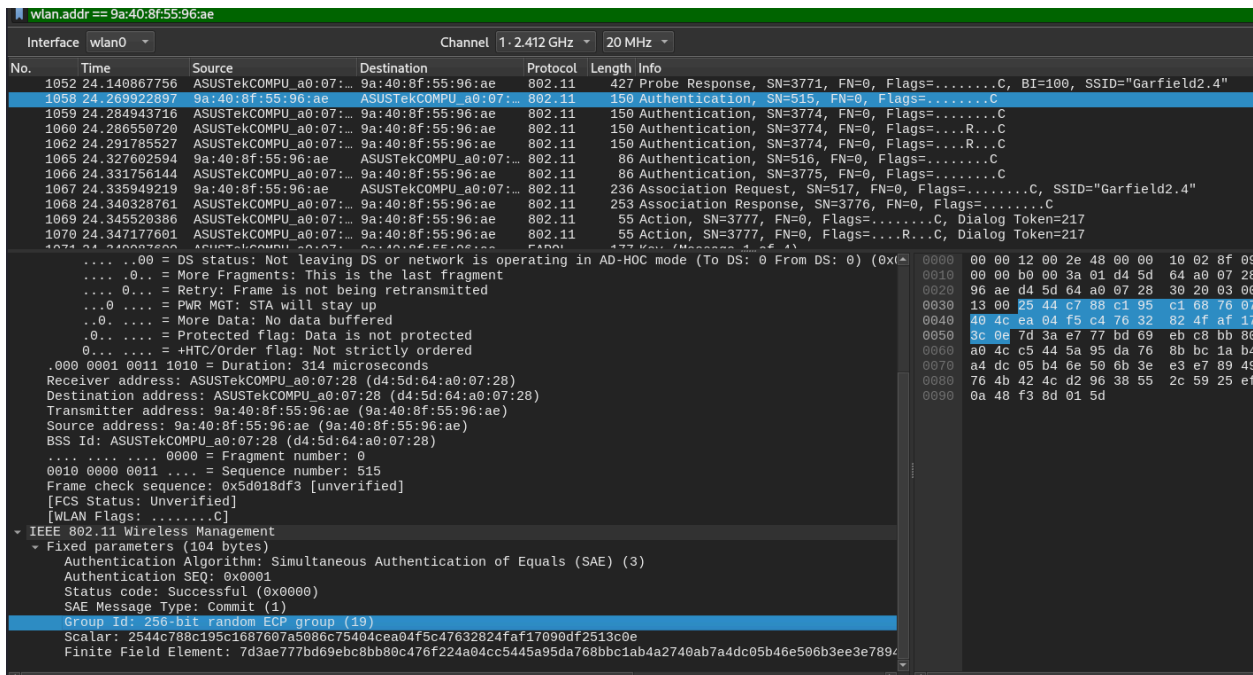
The duration was 314 microseconds.

**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 7d3ae777bd69ebc8bb80c476f224a04cc5445a95da768bbcb1ab4a2740ab7a4dc05b46e506b3ee3e78949ff133519764b424cd29638552c5925efe09d6ed30a48.

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 image shows a Wireshark packet capture of a wireless network interface (wlan0) on channel 1-2.412 GHz, 20 MHz. The packet list shows a sequence of frames from ASUSTekCOMPU\_a0:07:28 to 9a:40:8f:55:96:ae. The selected packet is a SAE Confirm message (Frame 1066, Length 116 bytes). The packet details pane shows the following structure:

- Flags: 0x00
- DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
- More Fragments: This is the last fragment
- Retry: Frame is not being retransmitted
- PWR MGT: STA will stay up
- More Data: No data buffered
- Protected flag: Data is not protected
- HTC/Order flag: Not strictly ordered
- Duration: 314 microseconds
- Receiver address: ASUSTekCOMPU\_a0:07:28 (d4:5d:64:a0:07:28)
- Destination address: ASUSTekCOMPU\_a0:07:28 (d4:5d:64:a0:07:28)
- Transmitter address: 9a:40:8f:55:96:ae (9a:40:8f:55:96:ae)
- Source address: 9a:40:8f:55:96:ae (9a:40:8f:55:96:ae)
- BSS Id: ASUSTekCOMPU\_a0:07:28 (d4:5d:64:a0:07:28)
- Fragment number: 0
- Sequence number: 316
- Frame check sequence: 0x0462fb86 [unverified]
- [FCS Status: Unverified]
- [WLAN Flags: .....C]
- IEEE 802.11 Wireless Management
- Fixed parameters (40 bytes)
- Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
- Authentication SEQ: 0x0002
- Status code: Successful (0x0000)
- SAE Message Type: Confirm (2)
- Send-Confirm: 1
- Confirm: 9b232c81f5294ec4bceace115174d66f4a06b110701f620133e7dc776780d0ee

The packet bytes pane shows the raw data of the SAE Confirm message, starting with 0000 00 00 12 00 2e 48 00 00 10 02 8f 09 a0 00 db 09.

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 image displays two Wireshark packet captures of a 4-way handshake between a client and an access point. The interface is wlan0, channel 1-2.412 GHz, 20 MHz.

**Packet 1071:** EAPOL Key (Message 1 of 4). The Key Information field shows a Replay Counter of 1.

**Packet 1073:** EAPOL Key (Message 2 of 4).

**Packet 1074:** EAPOL Key (Message 3 of 4).

**Packet 1075:** EAPOL Key (Message 4 of 4).

**Packet 1076:** Action, SN=519, FN=0, Flags=p.....C.

**Packet 1077:** Null function (No data), SN=520, FN=0, Flags=.....TC.

**Packet 1078:** Null function (No data), SN=520, FN=0, Flags=.....TC.

**Packet 1079:** 802.1X Authentication (0x888e).

**Packet 1080:** 802.1X Authentication (0x888e). The Key Information field shows a Replay Counter of 2.

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

```
1070 24.347177601 ASUSTekCOMPU_a0:07:... 9a:40:8f:55:96:ae 802.11 55 Action, SN=3777, FN=0, Flags=....R...C, Dialog Token=217
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
1078 24.385552350 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
Replay Counter: 1
WPA Key Nonce: c2647df03d4165674060704b270e10957b3b631157ff6a70e33fbc9ae0d71ba
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 00000000000000000000000000000000
WPA Key Data Length: 22
WPA Key Data: dd14000afac0470496d5a5chape300e53baha18382fd0b

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
1078 24.385552350 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: 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
.....0... = Encrypted Key Data: Not set
.....0... = SMK Message: Not set
Key Length: 16
Replay Counter: 1
WPA Key Nonce: 76cf9769e4afd28388289268215f9d38b6003dc37b4197f036321f1a3ede4085
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 1a54d59dbd8ede65d805130ef5019a
WPA Key Data Length: 40
```





```

1070 24.349087600 ASUSTekCOMPU_a0:07:... 9a:40:8f:55:96:ae 802.11 78 Action, SN=519, FN=0, Flags=.p.....C
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
1078 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: Unknownn (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=.
1078 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: Unknownn (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
0000 00 00 00 00 00
0010 00 00 00 00 00
0020 96 a0 00 00 00
0030 00 00 00 00 00
0040 00 00 00 00 00
0050 68 21 00 00 00
0060 1a 30 00 00 00
0070 00 00 00 00 00
0080 00 00 00 00 00
0090 13 00 00 00 00
00a0 00 00 00 00 00
00b0 49 60 00 00 00
00c0 e5 f0 00 00 00

```

```

1070 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, Fla
1078 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: Unknownn (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
.... .0... = SMK Message: Not set
0000 00 00 00 00 00
0010 00 00 00 00 00
0020 00 00 00 00 00
0030 00 00 00 00 00
0040 00 00 00 00 00
0050 00 00 00 00 00
0060 00 00 00 00 00
0070 00 00 00 00 00
0080 00 00 00 00 00
0090 00 00 00 00 00
00a0 00 00 00 00 00
00b0 00 00 00 00 00
00c0 00 00 00 00 00
00d0 00 00 00 00 00
00e0 00 00 00 00 00
00f0 00 00 00 00 00

```

```

1074 24.360309297 9a:40:8f:55:96:ae ASUSTekCOMPU_a0:07:... EAPOL 245 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=.
1078 24.385552358 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: 95
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 4]
Key Information: 0x0308
.....0000 = 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
.....1... = Secure: Set
.....0... = Error: Not set
.....0... = Request: Not set
.....0... = Encrypted Key Data: Not 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.

```

File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x

CH 9 ][ Elapsed: 18 s ][ 2024-04-02 18:18 ][ WPA handshake: D4:5D:64:A0:07:28

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
D4:5D:64:A0:07:28 -27 51 95 12 0 9 720 WPA2 CCMP PSK Garfield2.4

BSSID STATION PWR Rate Lost Frames Notes Probes
(not associated) D0:39:57:1D:E5:C3 -82 0 - 6 0 1
(not associated) 50:E0:85:DD:3A:3D -57 0 - 5 0 1
(not associated) E6:5D:63:BC:66:6E -34 0 - 1 0 2
(not associated) DE:72:0C:3A:5A:06 -39 0 - 1 0 1
(not associated) BE:6B:30:25:FE:1B -81 0 - 1 0 1
(not associated) 38:7A:0E:70:42:CA -77 0 - 5 0 1
(not associated) F2:F9:53:3A:22:5F -73 0 - 1 0 2
D4:5D:64:A0:07:28 5C:52:84:86:CC:E6 -27 1e- 1 801 1467 EAPOL Garfield2.4

```

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.



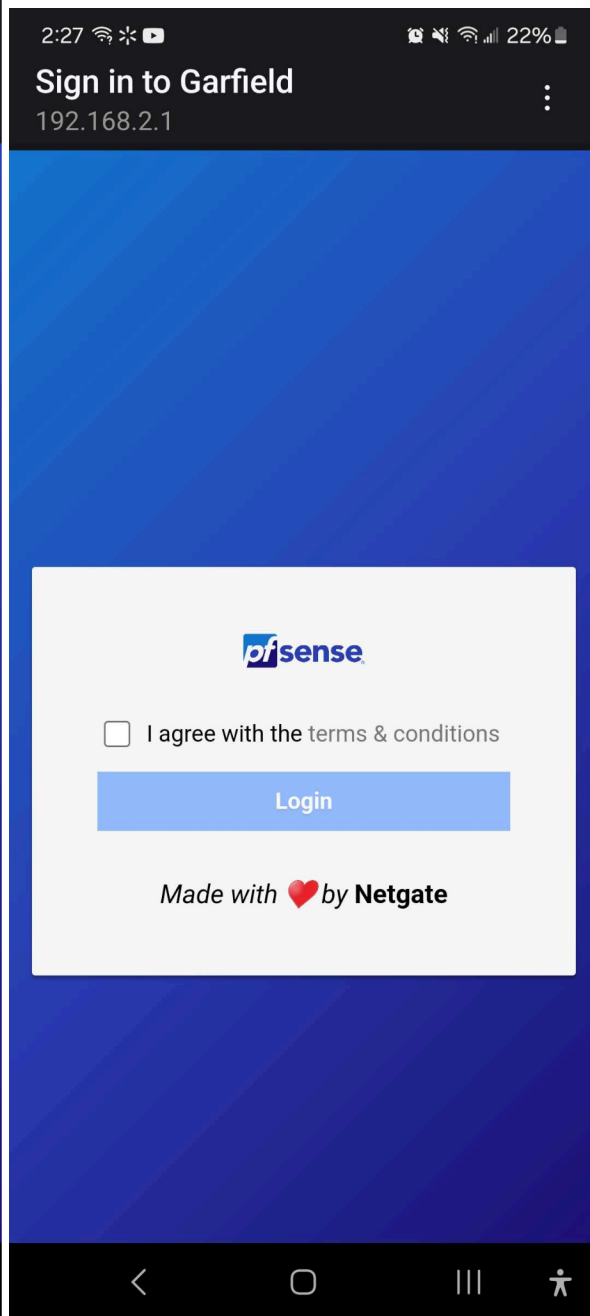
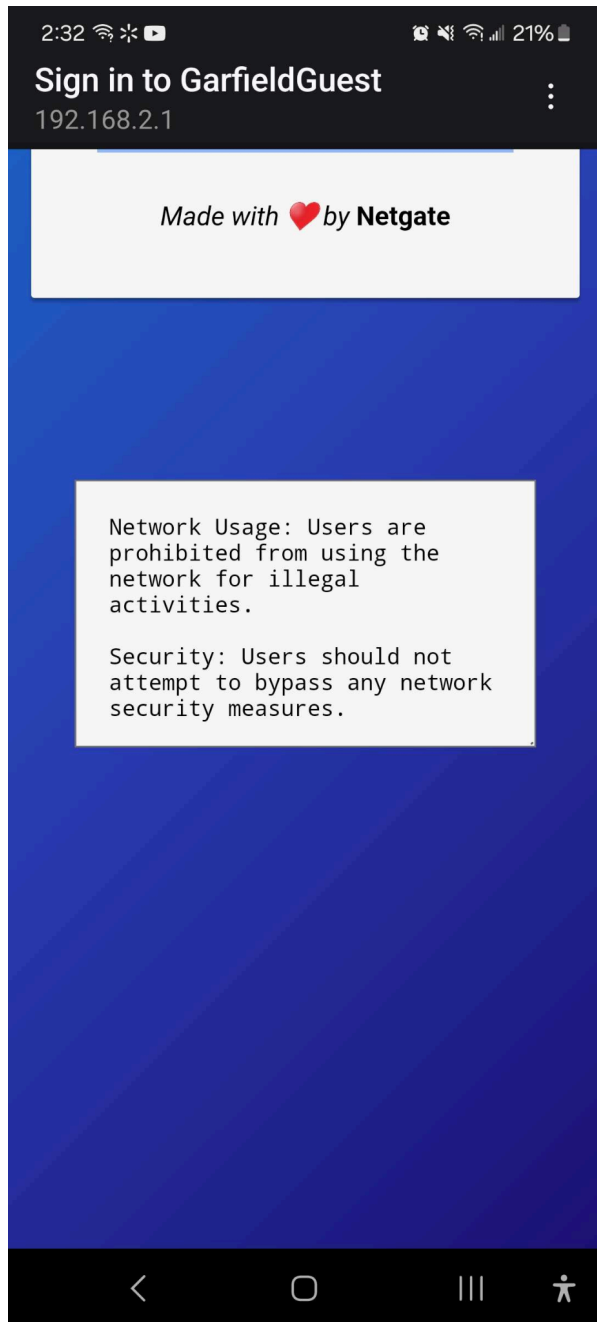
**Q9.** Was the attack successful this time? Briefly describe why the attack does (or does not) work this time.

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