

[illegible]

Name	Tool: Termshark
URL	https://www.attackdefense.com/challengedetails?cid=1314
Type	WiFi Pentesting : WiFi Tools

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Open the PCAP file in Termshark and answer the following questions:

Q1. What is the BSSID for SSID 'Home_Network'?

Solution:

Open the PCAP in Termshark.

Command: termshark -r capture.pcap

```
root@attackdefense:~# termshark -r capture.pcap
```

termshark v1.0.0							<Menu>
Filter: <input type="text"/>							<Apply> <Recent>
No. -	Time -	Source -	Destination -	Protocol -	Length -	Info -	
1	0.000000	D-LinkIn_5f:81:74	Broadcast	802.11	309	Beacon frame, SN=1939, FN=0, Flags=.....C, BI=100,	
2	0.092045	D-LinkIn_5f:81:74	Broadcast	802.11	309	Beacon frame, SN=1940, FN=0, Flags=.....C, BI=100,	
3	0.194397	D-LinkIn_5f:81:74	Broadcast	802.11	309	Beacon frame, SN=1941, FN=0, Flags=.....C, BI=100,	
4	0.296816	D-LinkIn_5f:81:74	Broadcast	802.11	309	Beacon frame, SN=1942, FN=0, Flags=.....C, BI=100,	
5	0.399190	D-LinkIn_5f:81:74	Broadcast	802.11	309	Beacon frame, SN=1943, FN=0, Flags=.....C, BI=100,	
6	0.501658	D-LinkIn_5f:81:74	Broadcast	802.11	309	Beacon frame, SN=1944, FN=0, Flags=.....C, BI=100,	
7	0.604028	D-LinkIn_5f:81:74	Broadcast	802.11	309	Beacon frame, SN=1945, FN=0, Flags=.....C, BI=100,	
[-] IEEE 802.11 Beacon frame, Flags:C							
Type/Subtype: Beacon frame (0x0008)							
[+] Frame Control Field: 0x8000							
.000 0001 0011 1010 = Duration: 314 microseconds							
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)							
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)							
Transmitter address: D-LinkIn_5f:81:74 (6c:19:8f:5f:81:74)							
Source address: D-LinkIn_5f:81:74 (6c:19:8f:5f:81:74)							
0000	00 00 24 00 2f 40 00 a0	20 08 00 00 00 00 00 00	..\$./@..			
0010	bf b4 a0 32 00 00 00 00	10 02 85 09 a0 00 cb 00	...2....			
0020	00 00 a6 00 80 00 3a 01	ff ff ff ff ff ff 6c 19			
0030	8f 5f 81 74 6c 19 8f 5f	81 74 40 79 7c f1 8c ef	...tl... .t@y ...				
0040	01 00 00 00 64 00 11 04	00 0c 48 6f 6d 65 5f 4ed... .Home_N				
0050	65 74 77 6f 72 6b 01 08	82 84 8b 96 0c 12 18 24	etwork..\$			
0060	03 01 06 05 04 00 01 00	00 2a 01 04 32 04 30 482.0H			

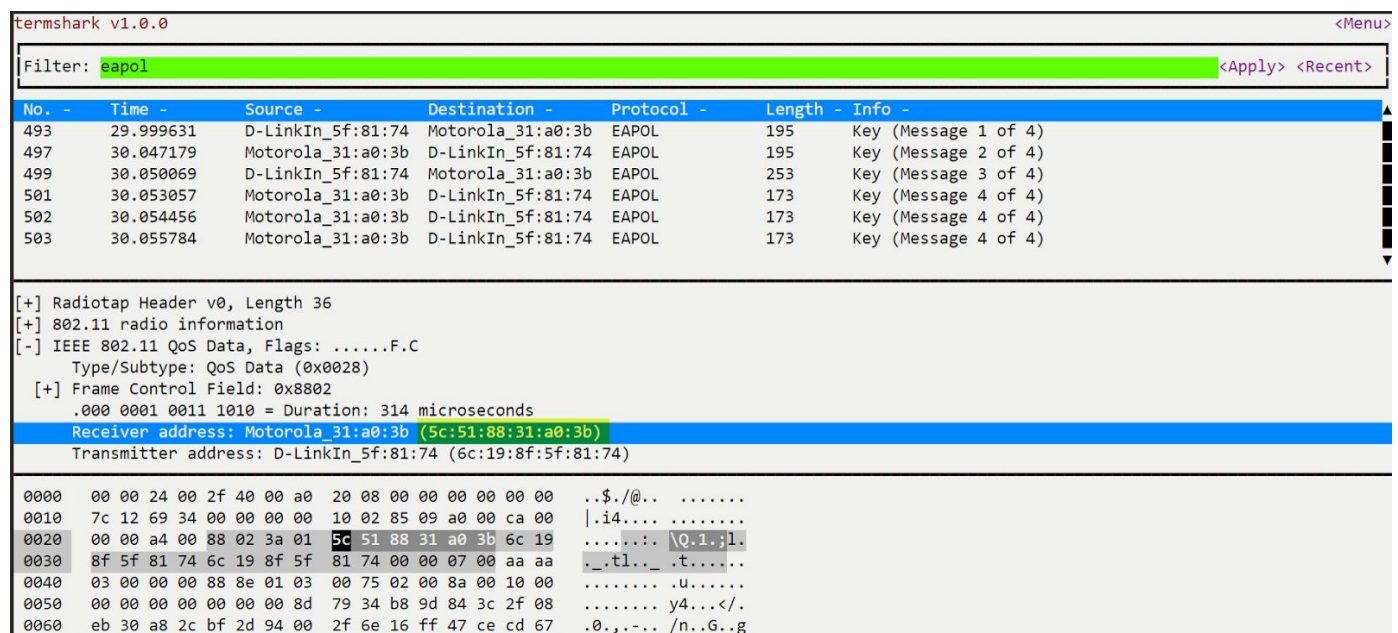
From a beacon frame of the network 'Home_Network', one can find out the BSSID.

Answer: 6c:19:8f:5f:81:74

Q2. One client was successfully connected to 'Home_Network'? What is the MAC address of that client?

Filter 4-way handshake packets and check if the handshake was completed.

Filter: eapol



The screenshot shows the Wireshark network protocol analyzer interface. The top filter bar contains the text 'eapol'. Below it, a list of captured packets is displayed, filtered to show only EAPOL packets. The selected packet is number 503, which is a 'Key (Message 4 of 4)' with a length of 173 bytes. The packet details pane on the right shows the structure of this EAPOL packet, including the Radiotap header, IEEE 802.11 radio information, and the Frame Control field. The 'Receiver address' is highlighted as 'Motorola_31:a0:3b (5c:51:88:31:a0:3b)' and the 'Transmitter address' is 'D-LinkIn_5f:81:74 (6c:19:8f:5f:81:74)'. The packet bytes pane at the bottom shows the raw data of the selected packet, with the MAC address '5c:51:88:31:a0:3b' highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
493	29.999631	D-LinkIn_5f:81:74	Motorola_31:a0:3b	EAPOL	195	Key (Message 1 of 4)
497	30.047179	Motorola_31:a0:3b	D-LinkIn_5f:81:74	EAPOL	195	Key (Message 2 of 4)
499	30.050069	D-LinkIn_5f:81:74	Motorola_31:a0:3b	EAPOL	253	Key (Message 3 of 4)
501	30.053057	Motorola_31:a0:3b	D-LinkIn_5f:81:74	EAPOL	173	Key (Message 4 of 4)
502	30.054456	Motorola_31:a0:3b	D-LinkIn_5f:81:74	EAPOL	173	Key (Message 4 of 4)
503	30.055784	Motorola_31:a0:3b	D-LinkIn_5f:81:74	EAPOL	173	Key (Message 4 of 4)

[+] Radiotap Header v0, Length 36
[+] 802.11 radio information
[-] IEEE 802.11 QoS Data, Flags:F.C
Type/Subtype: QoS Data (0x0028)
[+] Frame Control Field: 0x8802
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: Motorola_31:a0:3b (5c:51:88:31:a0:3b)
Transmitter address: D-LinkIn_5f:81:74 (6c:19:8f:5f:81:74)

0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00 ..\$./@..

0010 7c 12 69 34 00 00 00 00 10 02 85 09 a0 00 ca 00 |.i4....

0020 00 00 a4 00 88 02 3a 01 5c 51 88 31 a0 3b 6c 19 \Q.1;l.

0030 8f 5f 81 74 6c 19 8f 5f 81 74 00 00 07 00 aa aa ._tl._.t.....

0040 03 00 00 00 88 8e 01 03 00 75 02 00 8a 00 10 00u.....

0050 00 00 00 00 00 00 00 8d 79 34 b8 9d 84 3c 2f 08 y4...</.

0060 eb 30 a8 2c bf 2d 94 00 2f 6e 16 ff 47 ce cd 67 .0.,... /n..G..g

Answer: 5c:51:88:31:a0:3b

Q3. How many deauthentication packets were sent by the client to BSSID?

Filter for deauthentication packets.

Filter: wlan.fc.type_subtype==0x000C

termshark v1.0.0 <Menu>

Filter: wlan.fc.type_subtype==0x000C <Apply> <Recent>

No. -	Time -	Source -	Destination -	Protocol -	Length -	Info -
15694	127.895235	Motorola_31:a0:3b	D-LinkIn_5f:81:74	802.11	66	Deauthentication, SN=1626, FN=0, Flags=.....C

[+] Frame 15694: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

[+] Radiotap Header v0, Length 36

[+] 802.11 radio information

[+] IEEE 802.11 Deauthentication, Flags:C

[+] IEEE 802.11 wireless LAN

```

0000  00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00  .$./@.. .....
0010  db db 3e 3a 00 00 00 00 10 0c 85 09 c0 00 cd 00  ..>:.... .....
0020  00 00 cd 00 c0 00 3c 00 6c 19 8f 5f 81 74 5c 51  .....<. l._.t\Q
0030  88 31 a0 3b 6c 19 8f 5f 81 74 a0 65 03 00 46 23  .1;l._.t.e..F#
0040  3f 2d  ?-

```

Only one deauthentication packet is present in the PCAP.

Answer: 1