
ATTACK
DEFENSE
by PentesterAcademy

Name	Filtering Advanced: WiFi
URL	https://www.attackdefense.com/challengedetails?cid=4
Type	Traffic Analysis: Tshark Fu

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.

Set A:

Q1. What command can be used to show only WiFi traffic?

Answer: tshark -r WiFi_traffic.pcap -Y "wlan"

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y "wlan"
    1   0.000000 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1939, FN=0, Flags=........C, BI=100, SSID=Home_Network
    2   0.092045 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1940, FN=0, Flags=........C, BI=100, SSID=Home_Network
    3   0.194397 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1941, FN=0, Flags=........C, BI=100, SSID=Home_Network
    4   0.296816 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1942, FN=0, Flags=........C, BI=100, SSID=Home_Network
    5   0.399190 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1943, FN=0, Flags=........C, BI=100, SSID=Home_Network
    6   0.501658 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1944, FN=0, Flags=........C, BI=100, SSID=Home_Network
    7   0.604028 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1945, FN=0, Flags=........C, BI=100, SSID=Home_Network
    8   0.704155 D-LinkIn_5f:81:74 ? SamsungE_1d:97:78 802.11 303 Probe Response, SN=1947, FN=0, Flags=........C, BI=100, SSID=Home_Network
    9   0.706592 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1946, FN=0, Flags=........C, BI=100, SSID=Home_Network
   10   0.725570 D-LinkIn_5f:81:74 ? SamsungE_1d:97:78 802.11 303 Probe Response, SN=1948, FN=0, Flags=........C, BI=100, SSID=Home_Network
   11   0.748555 D-LinkIn_5f:81:74 ? SamsungE_1d:97:78 802.11 303 Probe Response, SN=1949, FN=0, Flags=........C, BI=100, SSID=Home_Network
   12   0.808809 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1950, FN=0, Flags=........C, BI=100, SSID=Home_Network
   13   0.911226 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1951, FN=0, Flags=........C, BI=100, SSID=Home_Network
   14   0.980795 D-LinkIn_5f:81:74 ? LgElectr_f6:69:dd 802.11 303 Probe Response, SN=1952, FN=0, Flags=........C, BI=100, SSID=Home_Network
   15   1.013620 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1953, FN=0, Flags=........C, BI=100, SSID=Home_Network
   16   1.048064 D-LinkIn_5f:81:74 ? LgElectr_f6:69:dd 802.11 303 Probe Response, SN=1954, FN=0, Flags=........C, BI=100, SSID=Home_Network
   17   1.060033 D-LinkIn_5f:81:74 ? LgElectr_f6:69:dd 802.11 303 Probe Response, SN=1955, FN=0, Flags=........C, BI=100, SSID=Home_Network
   18   1.065658 D-LinkIn_5f:81:74 ? LgElectr_f6:69:dd 802.11 303 Probe Response, SN=1956, FN=0, Flags=........C, BI=100, SSID=Home_Network
   19   1.116042 D-LinkIn_5f:81:74 ? Broadcast    802.11 309 Beacon frame, SN=1957, FN=0, Flags=........C, BI=100, SSID=Home_Network
   20   1.189746 D-LinkIn_5f:81:74 ? LgElectr_f6:69:dd 802.11 303 Probe Response, SN=1958, FN=0, Flags=........C, BI=100, SSID=Home_Network
   21   1.195922 D-LinkIn_5f:81:74 ? LgElectr_f6:69:dd 802.11 303 Probe Response, SN=1959, FN=0, Flags=........C, BI=100, SSID=Home_Network
```

Q2. What command can be used only view the deauthentication packets?

Answer: tshark -r WiFi_traffic.pcap -Y "wlan.fc.type_subtype==0x000c"

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y "wlan.fc.type_subtype==0x000c"
15694 127.895235 Motorola_31:a0:3b ? D-LinkIn_5f:81:74 802.11 66 Deauthentication, SN=1626, FN=0, Flags=........C
33477 152455.676623 Motorola_31:a0:3b ? AsustekC_c3:5e:01 802.11 66 Deauthentication, SN=876, FN=0, Flags=........C
student@attackdefense:~$
```

Q3. What command can be used to only display WPA handshake packets?

Answer: tshark -r WiFi_traffic.pcap -Y "eapol"

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y "eapol"
  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)
student@attackdefense:~$
```

Q4. What command can be used to only print the SSID and BSSID values for all beacon frames?

Answer: tshark -r WiFi_traffic.pcap -Y "wlan.fc.type_subtype==8" -Tfields -e wlan.ssid -e wlan.bssid

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y "wlan.fc.type_subtype==8" -Tfields -e wlan.ssid -e wlan.bssid
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
Home_Network    6c:19:8f:5f:81:74
```

Set B:

Q1. What is BSSID of SSID “LazyArtists”?

Answer: fc:b0:c4:91:71:e0

Command: tshark -r WiFi_traffic.pcap -Y "wlan.ssid==LazyArtists" -Tfields -e wlan.bssid

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y "wlan.ssid==LazyArtists" -Tfields -e wlan.bssid
fc:b0:c4:91:71:e0
fc:b0:c4:91:71:e0
fc:b0:c4:91:71:e0
fc:b0:c4:91:71:e0
fc:b0:c4:91:71:e0
student@attackdefense:~$
```

Q2. SSID "Home_Network" is operating on which channel?

Answer: 6

Command: tshark -r WiFi_traffic.pcap -Y "wlan.ssid==Home_Network" -Tfields -e wlan_radio.channel

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y "wlan.ssid==Home_Network" -Tfields -e wlan_radio.channel | uniq
6
student@attackdefense:~$
```

Q3. Which two devices received the deauth messages? State the MAC addresses of both.

Answer: 6c:19:8f:5f:81:74 bc:ae:c5:c3:5e:01

Command: tshark -r WiFi_traffic.pcap -Y "wlan.fc.type_subtype==0x000c" -Tfields -e wlan.ra

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y "wlan.fc.type_subtype==0x000c" -Tfields -e wlan.ra
6c:19:8f:5f:81:74
bc:ae:c5:c3:5e:01
student@attackdefense:~$
```

Q4. Which device does MAC 5c:51:88:31:a0:3b belongs to? Mention manufacturer and model number of the device.

Answer: Motorola MotG3

Command: tshark -r WiFi_traffic.pcap -Y "wlan.ta==5c:51:88:31:a0:3b && http" -Tfields -e http.user_agent

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y "wlan.ta==5c:51:88:31:a0:3b && http" -Tfields -e http.user_agent
Dalvik/2.1.0 (Linux; U; Android 6.0; MotoG3 Build/MPI24.65-25)
Dalvik/2.1.0 (Linux; U; Android 6.0; MotoG3 Build/MPI24.65-25)
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
Mozilla/5.0 (Linux; Android 6.0; MotoG3 Build/MPI24.65-25) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.83 Mobile Safari/537.36
```

References:

1. Tshark (https://www.wireshark.org/docs/man-pages/tshark.html)
2. Wireshark (https://www.wireshark.org/)