

[illegible]

Name	WiFi Security: Traffic Analysis I
URL	https://www.attackdefense.com/challengedetails?cid=1141
Type	WiFi Pentesting: Traffic Analysis

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.

Q1. What is the name of the Open (No Security) SSID present in the packet dump?

A. SecurityTube_Open

Filter: (wlan.fc.type_subtype == 0x0008) && (!(wlan.wfa.ie.wpa.version == 1)) && !(wlan.tag.number == 48)

Wireshark packet capture interface showing a list of 802.11 Beacon frames. The filter '(wlan.fc.type_subtype == 0x0008) && (!(wlan.wfa.ie.wpa.version == 1)) && !(wlan.tag.number == 48)' is applied. The packet list shows multiple beacon frames from 16491 to 19414, all with SSID=SecurityTube_Open. The packet details pane for frame 16491 is expanded, showing the IEEE 802.11 wireless LAN section with a Fixed parameters (12 bytes) and Tagged parameters (44 bytes) section. The Tagged parameters include SSID parameter set: SecurityTube_Open, Supported Rates, DS Parameter set, Traffic Indication Map (TIM), and Extended Capabilities.

Here tag 48 refers to RSN IE.

▼ Tag: RSN Information

```
Tag Number: RSN Information (48)
Tag length: 24
RSN Version: 1
▶ Group Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
Pairwise Cipher Suite Count: 2
▼ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) TKIP 00:0f:ac (Ieee 802.11) AES (CCM)
  ▼ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
    Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Pairwise Cipher Suite type: TKIP (2)
  ▼ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Pairwise Cipher Suite type: AES (CCM) (4)
Auth Key Management (AKM) Suite Count: 1
▼ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
  ▶ Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
▶ RSN Capabilities: 0x0000
```

And, wlan.wfa.ie.wpa.version == 1 is to filter put a vendor IE

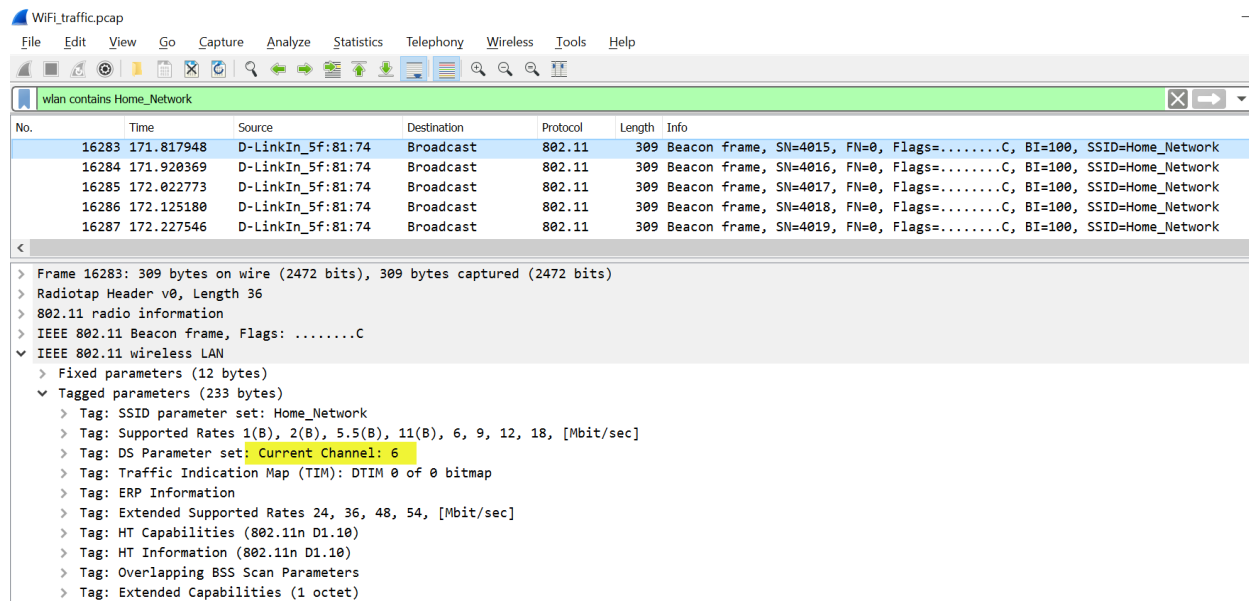
▼ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element

```
Tag Number: Vendor Specific (221)
Tag length: 28
OUI: 00:50:f2 (Microsoft Corp.)
Vendor Specific OUI Type: 1
Type: WPA Information Element (0x01)
WPA Version: 1
▶ Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
Unicast Cipher Suite Count: 2
▶ Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) AES (CCM) 00:50:f2 (Microsoft Corp.) TKIP
Auth Key Management (AKM) Suite Count: 1
▶ Auth Key Management (AKM) List 00:50:f2 (Microsoft Corp.) PSK
```

Q2. The SSID 'Home_Network' is operating on which channel?

A. 6

Filter: wlan contains Home_Network



Q3. Which security mechanism is configured for SSID 'LazyArtists'? Your options are: OPEN, WPA-PSK, WPA2-PSK.

A. WPA2-PSK

Filter: wlan contains LazyArtists

WiFi_traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan contains LazyArtists

No.	Time	Source	Destination	Protocol	Length	Info
22717	152441.9655...	Microsof_13:3b:f0	Shanghai_91:71:...	802.11	93	Probe Request, SN=1028, FN=0, Flags=.....C, SSID=LazyArtists
34305	152456.4337...	Shanghai_91:71:e0	Broadcast	802.11	148	Beacon frame, SN=3422, FN=0, Flags=.....C, BI=100, SSID=LazyArtists
46924	152484.1889...	Shanghai_91:71:e0	Broadcast	802.11	148	Beacon frame, SN=410, FN=0, Flags=.....C, BI=100, SSID=LazyArtists
56139	152511.1248...	Shanghai_91:71:e0	Broadcast	802.11	148	Beacon frame, SN=1462, FN=0, Flags=.....C, BI=100, SSID=LazyArtists

<

> IEEE 802.11 Beacon frame, Flags:C

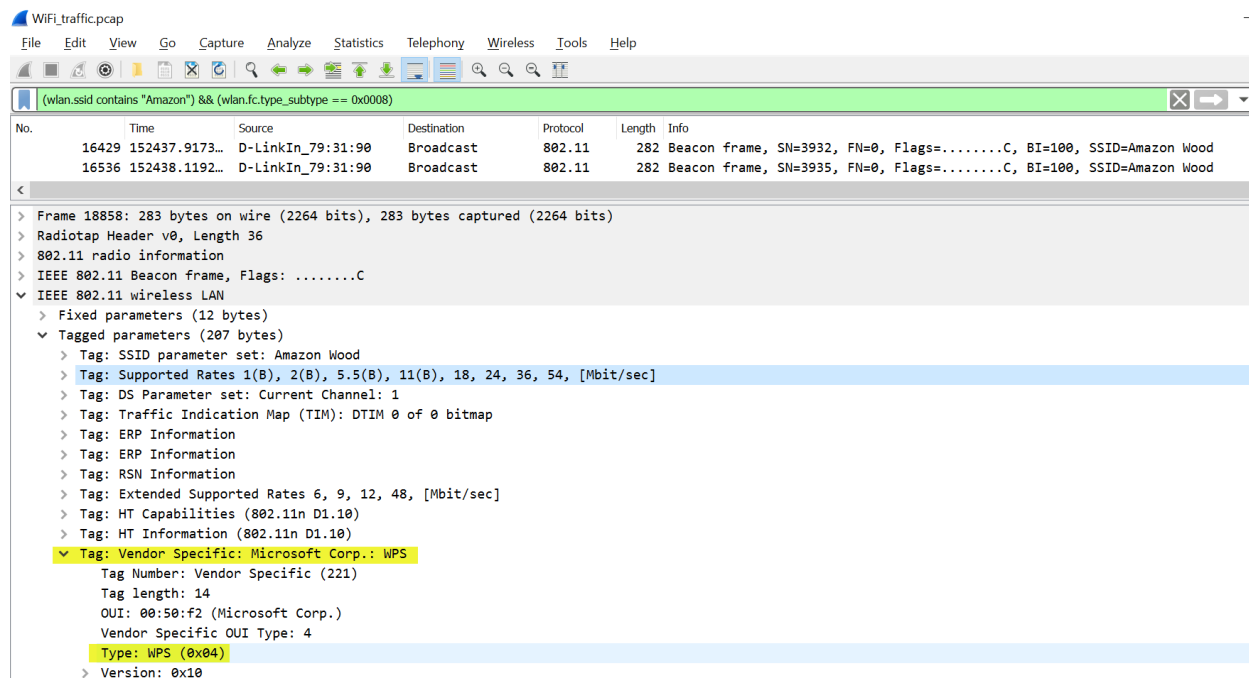
▼ IEEE 802.11 wireless LAN

- > Fixed parameters (12 bytes)
- ▼ Tagged parameters (72 bytes)
 - > Tag: SSID parameter set: LazyArtists
 - > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
 - > Tag: DS Parameter set: Current Channel: 2
 - > Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
 - > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
 - > Tag: ERP Information
 - ▼ Tag: RSN Information
 - Tag Number: RSN Information (48)
 - Tag length: 20
 - RSN Version: 1
 - > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
 - Pairwise Cipher Suite Count: 1
 - > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
 - Auth Key Management (AKM) Suite Count: 1
 - > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
 - > RSN Capabilities: 0x0000
- > Tag: Vendor Specific: Ralink Technology, Corp.

Q4. Is WiFi Protected Setup (WPS) enabled on SSID 'Amazon Wood'? State Yes or No.

A. Yes

Filter: (wlan.ssid contains "Amazon") && (wlan.fc.type_subtype == 0x0008)



Q5. What is the total count of packets which were either transmitted or received by the device with MAC e8:de:27:16:87:18?

A: 5701

Filter: (wlan.ta == e8:de:27:16:87:18) || (wlan.ra == e8:de:27:16:87:18)

Wireshark packet capture analysis of a Wi-Fi beacon frame. The packet list shows a beacon frame from 802.11 to 120, with details expanded to show the IEEE 802.11 wireless LAN header and frame body. The frame body contains the SSID 'SecurityTube_Open'.

No.	Time	Source	Destination	Protocol	Length	Info
16491	152437.873811	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=941, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
16512	152438.076295	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=942, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
16593	152438.479053	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=943, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
16828	152438.281318	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=944, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
17217	152438.383574	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=945, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
17512	152438.486593	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=946, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
17884	152438.589734	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=947, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
18155	152438.690901	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=948, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
18369	152438.797140	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=949, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
18687	152438.895641	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=950, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
19120	152438.998031	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=951, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open
19414	152439.101062	Tp-LinkT_16:87:18	Broadcast	802.11	120	Beacon frame, SN=952, FN=0, Flags=.....C, BI=100, SSID=SecurityTube_Open

Frame 16491: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
 Radiotap Header v0, Length 36
 802.11 radio information
 IEEE 802.11 Beacon frame, Flags:C
 IEEE 802.11 wireless LAN

0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00 --\$-/0--
 0010 cc 3e cc 05 00 00 00 00 10 02 bc 09 a0 00 ea 00 -->-----1-----
 0020 00 00 ea 00 00 00 00 00 ff ff ff ff ff ff e8 de -----a-----
 0030 27 16 87 18 e8 de 27 16 87 18 00 3a 00 61 cc 05 -----d-----Securi
 0040 00 00 00 00 64 00 01 00 00 11 53 65 63 75 72 69 tyTube_0 pen-----
 0050 74 79 54 75 62 65 5f 4f 70 65 6e 01 04 82 84 0b -----
 0060 16 03 01 01 05 04 00 02 00 00 7f 08 00 00 00 00 --@--6--
 0070 00 00 00 40 08 b4 36 11 -----

Q6. What is the MAC address of the station which exchanged data packets with SSID 'SecurityTube_Open'?

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

SSID SecurityTube_Open is hosted on BSSID e8:de:27:16:87:18.

Filter: ((wlan.bssid == e8:de:27:16:87:18)) && (wlan.fc.type_subtype == 0x0020)

WiFi_traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

((wlan.bssid == e8:de:27:16:87:18)) && (wlan.fc.type_subtype == 0x0020)

No.	Time	Source	Destination	Protocol	Length	Info
34477	152456.5578...	::	ff02::1:ff31:a0...	ICMPv6	136	Neighbor Solicitation for fe80::5e51:88ff:fe31:a03b
34490	152456.5657...	::	ff02::16	ICMPv6	148	Multicast Listener Report Message v2
34496	152456.5693...	::	ff02::16	ICMPv6	148	Multicast Listener Report Message v2
34590	152456.6645...	0.0.0.0	255.255.255.255	DHCP	412	DHCP Discover - Transaction ID 0xc698cee9
34598	152456.6725...	0.0.0.0	255.255.255.255	DHCP	412	DHCP Discover - Transaction ID 0xc698cee9
34599	152456.6734...	Tp-LinkT_16:87:18	Broadcast	ARP	100	Who has 192.168.3.10? Tell 192.168.3.1

> Frame 34477: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Data, Flags:F.C

Type/Subtype: Data (0x0020)

> Frame Control Field: 0x0020

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: IPv6mcast_ff:31:a0:3b (33:33:ff:31:a0:3b)

Transmitter address: Tp-LinkT_16:87:18 (e8:de:27:16:87:18)

Destination address: IPv6mcast_ff:31:a0:3b (33:33:ff:31:a0:3b)

Source address: Motorola_31:a0:3b (5c:51:88:31:a0:3b)

BSS Id: Tp-LinkT_16:87:18 (e8:de:27:16:87:18)

STA address: IPv6mcast_ff:31:a0:3b (33:33:ff:31:a0:3b)

.... 0000 = Fragment number: 0

0000 0000 0000 = Sequence number: 0

Frame check sequence: 0xe4277127 [unverified]

[FCS Status: Unverified]

> Logical-Link Control

Q7. From the last question, we know that a station was connected to SSID 'SecurityTube_Open'. Provide TSF timestamp of the association response sent from the access point to this station.

A. 115152625

Filter: (((wlan.bssid == e8:de:27:16:87:18)) && (wlan.addr==5c:51:88:31:a0:3b)) && (wlan.fc.type_subtype == 0x0001)

WiFi_traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(((wlan.bssid == e8:de:27:16:87:18)) && (wlan.addr==5c:51:88:31:a0:3b)) && (wlan.fc.type_subtype == 0x0001)

No.	Time	Source	Destination	Protocol	Length	Info
33637	152455.8577...	Tp-LinkT_16:87:18	Motorola_31:a0:3b	802.11	86	Association Response, SN=55, FN=0, Flags=.....C

> Frame 33637: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

> Radiotap Header v0, Length 36

▼ 802.11 radio information

- PHY type: 802.11b (4)
- Short preamble: False
- Data rate: 1.0 Mb/s
- Channel: 1
- Frequency: 2412MHz
- Signal strength (dBm): -21dBm
- TSF timestamp: 115152625
- [Duration: 592μs]

▼ IEEE 802.11 Association Response, Flags:C

- Type/Subtype: Association Response (0x0001)
- > Frame Control Field: 0x1000
 - .000 0000 0000 0000 = Duration: 0 microseconds
 - Receiver address: Motorola_31:a0:3b (5c:51:88:31:a0:3b)
 - Destination address: Motorola_31:a0:3b (5c:51:88:31:a0:3b)
 - Transmitter address: Tp-LinkT_16:87:18 (e8:de:27:16:87:18)
 - Source address: Tp-LinkT_16:87:18 (e8:de:27:16:87:18)
 - BSS Id: Tp-LinkT_16:87:18 (e8:de:27:16:87:18)
 - 0000 = Fragment number: 0
 - 0000 0011 0111 = Sequence number: 55

References:

1. Wireshark (<https://www.wireshark.org/>)
2. Pentester Academy WiFi course (<https://www.pentesteracademy.com/course?id=9>)