ATTACK DEFENSE

by PentesterAcademy

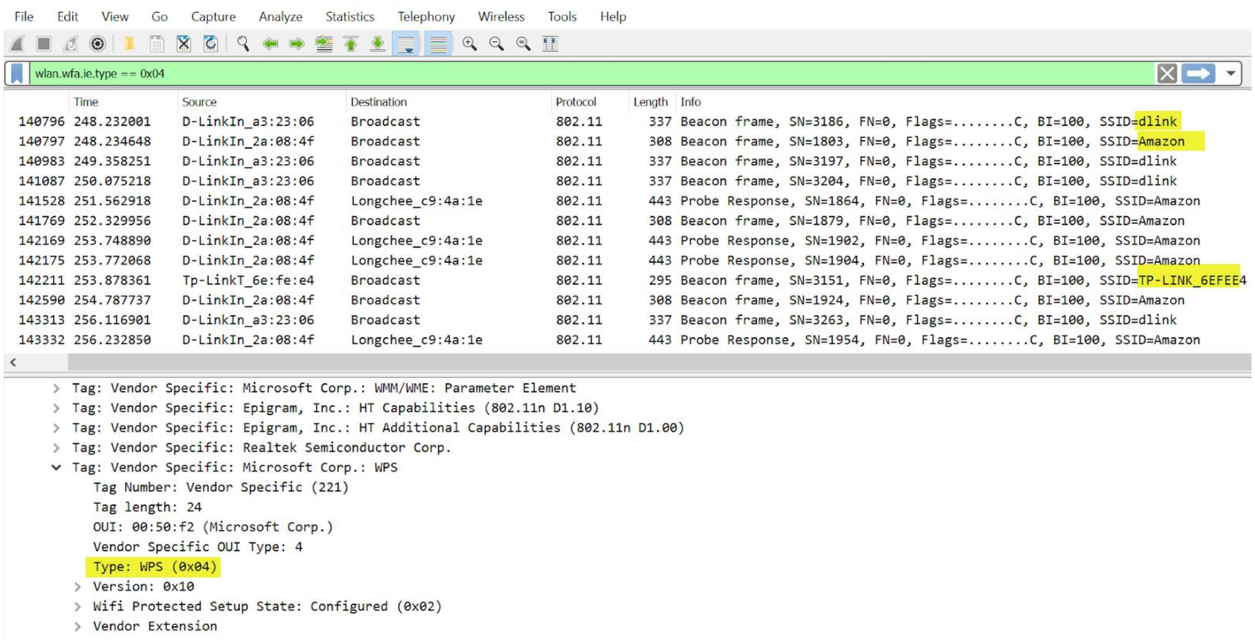
Name	WiFi Security: Traffic Analysis II
URL	https://www.attackdefense.com/challengedetails?cid=1143
Type	WiFi Pentesting: Traffic Analysis

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. How many SSIDs have WPS enabled?

A. 3

Filter: wlan.wfa.ie.type == 0x04

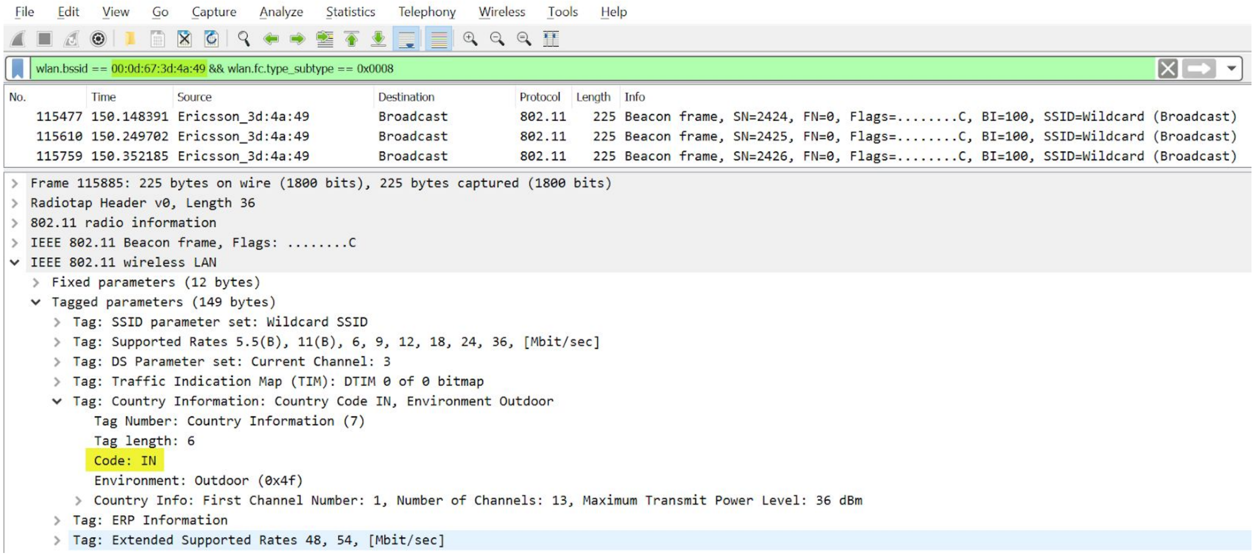


```
wlan.wfa.ie.type == 0x04

       Time        Source             Destination         Protocol  Length Info
140796 248.232001  D-LinkIn_a3:23:06  Broadcast           802.11     337 Beacon frame, SN=3186, FN=0, Flags=........C, BI=100, SSID=dlink
140797 248.234648  D-LinkIn_2a:08:4f  Broadcast           802.11     308 Beacon frame, SN=1803, FN=0, Flags=........C, BI=100, SSID=Amazon
140983 249.358251  D-LinkIn_a3:23:06  Broadcast           802.11     337 Beacon frame, SN=3197, FN=0, Flags=........C, BI=100, SSID=dlink
141087 250.075218  D-LinkIn_a3:23:06  Broadcast           802.11     337 Beacon frame, SN=3204, FN=0, Flags=........C, BI=100, SSID=dlink
141528 251.562918  D-LinkIn_2a:08:4f  Longchee_c9:4a:1e   802.11     443 Probe Response, SN=1864, FN=0, Flags=........C, BI=100, SSID=Amazon
141769 252.329956  D-LinkIn_2a:08:4f  Broadcast           802.11     308 Beacon frame, SN=1879, FN=0, Flags=........C, BI=100, SSID=Amazon
142169 253.748890  D-LinkIn_2a:08:4f  Longchee_c9:4a:1e   802.11     443 Probe Response, SN=1902, FN=0, Flags=........C, BI=100, SSID=Amazon
142175 253.772068  D-LinkIn_2a:08:4f  Longchee_c9:4a:1e   802.11     443 Probe Response, SN=1904, FN=0, Flags=........C, BI=100, SSID=Amazon
142211 253.878361  Tp-LinkT_6e:fe:e4  Broadcast           802.11     295 Beacon frame, SN=3151, FN=0, Flags=........C, BI=100, SSID=TP-LINK_6EFEE4
142590 254.787737  D-LinkIn_2a:08:4f  Broadcast           802.11     308 Beacon frame, SN=1924, FN=0, Flags=........C, BI=100, SSID=Amazon
143313 256.116901  D-LinkIn_a3:23:06  Broadcast           802.11     337 Beacon frame, SN=3263, FN=0, Flags=........C, BI=100, SSID=dlink
143332 256.232850  D-LinkIn_2a:08:4f  Longchee_c9:4a:1e   802.11     443 Probe Response, SN=1954, FN=0, Flags=........C, BI=100, SSID=Amazon

  > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  > Tag: Vendor Specific: Epigram, Inc.: HT Capabilities (802.11n D1.10)
  > Tag: Vendor Specific: Epigram, Inc.: HT Additional Capabilities (802.11n D1.00)
  > Tag: Vendor Specific: Realtek Semiconductor Corp.
  v Tag: Vendor Specific: Microsoft Corp.: WPS
      Tag Number: Vendor Specific (221)
      Tag length: 24
      OUI: 00:50:f2 (Microsoft Corp.)
      Vendor Specific OUI Type: 4
      Type: WPS (0x04)
    > Version: 0x10
    > Wifi Protected Setup State: Configured (0x02)
    > Vendor Extension
```

Q2. The BSSID 00:0d:67:3d:4a:49 is operating in which country? Provide the standard two character country code e.g. US, UK.

A. IN

Filter: wlan.bssid == 00:0d:67:3d:4a:49 && wlan.fc.type_subtype == 0x0008

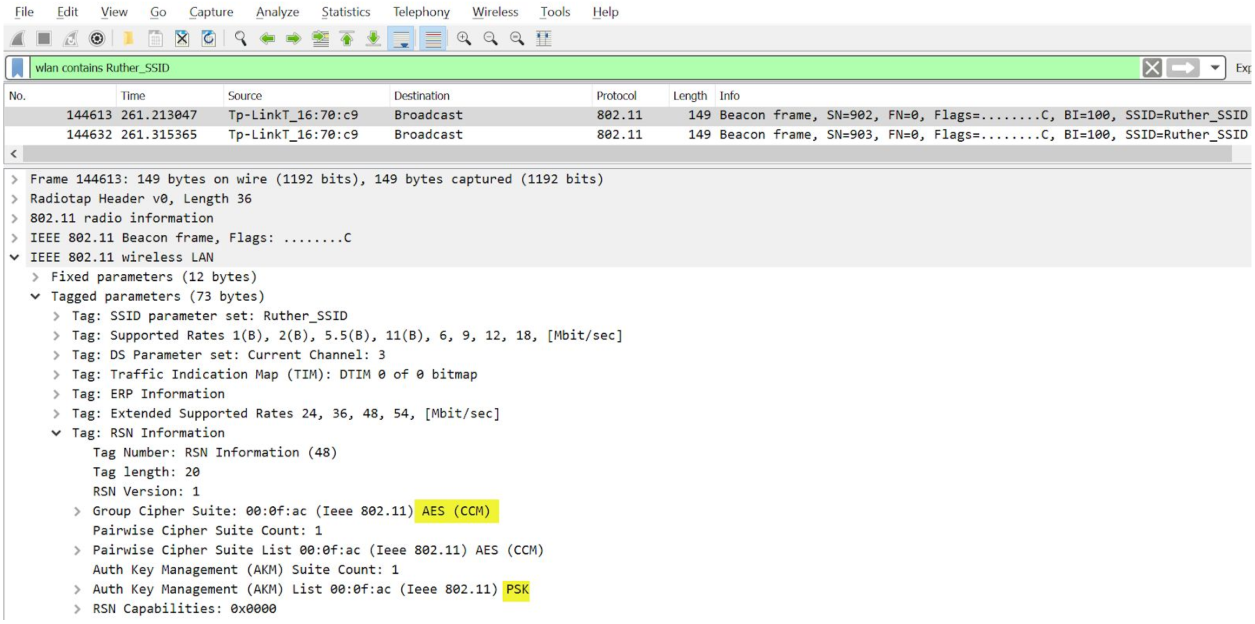


```
wlan.bssid == 00:0d:67:3d:4a:49 && wlan.fc.type_subtype == 0x0008

No.     Time        Source              Destination    Protocol  Length  Info
 115477 150.148391  Ericsson_3d:4a:49   Broadcast      802.11       225  Beacon frame, SN=2424, FN=0, Flags=........C, BI=100, SSID=Wildcard (Broadcast)
 115610 150.249702  Ericsson_3d:4a:49   Broadcast      802.11       225  Beacon frame, SN=2425, FN=0, Flags=........C, BI=100, SSID=Wildcard (Broadcast)
 115759 150.352185  Ericsson_3d:4a:49   Broadcast      802.11       225  Beacon frame, SN=2426, FN=0, Flags=........C, BI=100, SSID=Wildcard (Broadcast)

> Frame 115885: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 wireless LAN
  > Fixed parameters (12 bytes)
  v Tagged parameters (149 bytes)
    > Tag: SSID parameter set: Wildcard SSID
    > Tag: Supported Rates 5.5(B), 11(B), 6, 9, 12, 18, 24, 36, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 3
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    v Tag: Country Information: Country Code IN, Environment Outdoor
        Tag Number: Country Information (7)
        Tag length: 6
        Code: IN
        Environment: Outdoor (0x4f)
      > Country Info: First Channel Number: 1, Number of Channels: 13, Maximum Transmit Power Level: 36 dBm
    > Tag: ERP Information
    > Tag: Extended Supported Rates 48, 54, [Mbit/sec]
```

Q3. What kind of security scheme is defined for SSID 'Ruther_SSID'? Your options are: OPEN, WEP, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK, WPA-EAP, WPA2-EAP?

A. WPA2-PSK

Filter: wlan contains Ruther_SSID

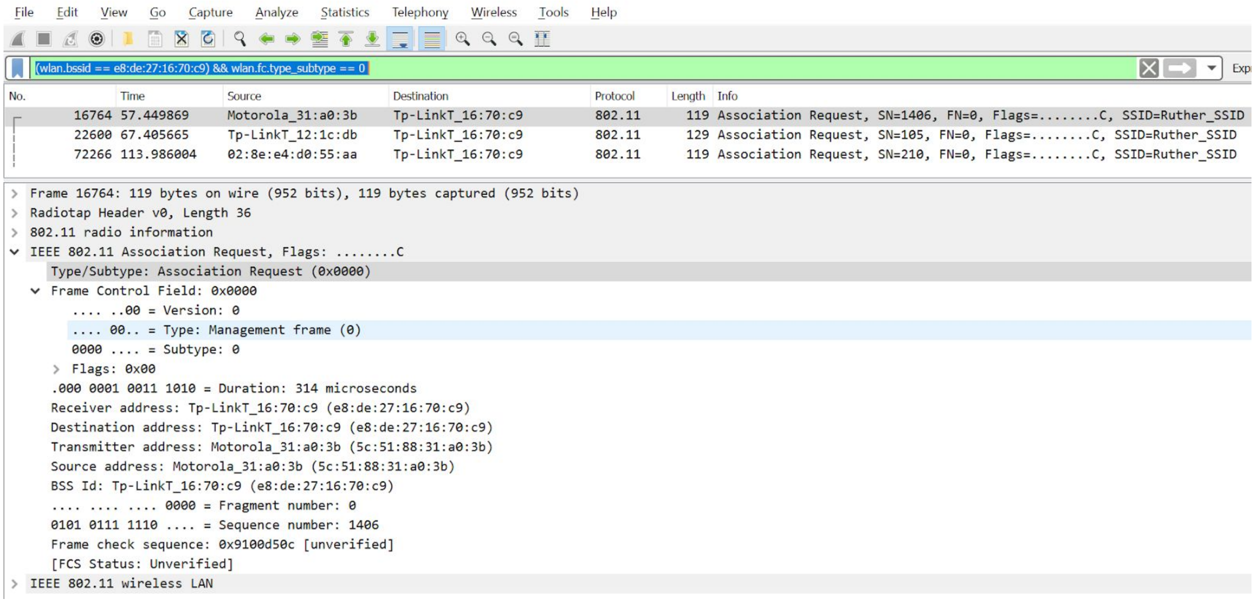


```
wlan contains Ruther_SSID

No.         Time         Source              Destination          Protocol   Length  Info
     144613 261.213047   Tp-LinkT_16:70:c9   Broadcast            802.11        149  Beacon frame, SN=902, FN=0, Flags=........C, BI=100, SSID=Ruther_SSID
     144632 261.315365   Tp-LinkT_16:70:c9   Broadcast            802.11        149  Beacon frame, SN=903, FN=0, Flags=........C, BI=100, SSID=Ruther_SSID

> Frame 144613: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 wireless LAN
  > Fixed parameters (12 bytes)
  v Tagged parameters (73 bytes)
    > Tag: SSID parameter set: Ruther_SSID
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 3
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    > Tag: ERP Information
    > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    v 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
```

Q4. How many clients tried to connect with SSID 'Ruther_SSID'? Consider all connection attempts and not only the successful connections.

A. 3

Filter: (wlan.bssid == e8:de:27:16:70:c9) && wlan.fc.type_subtype == 0



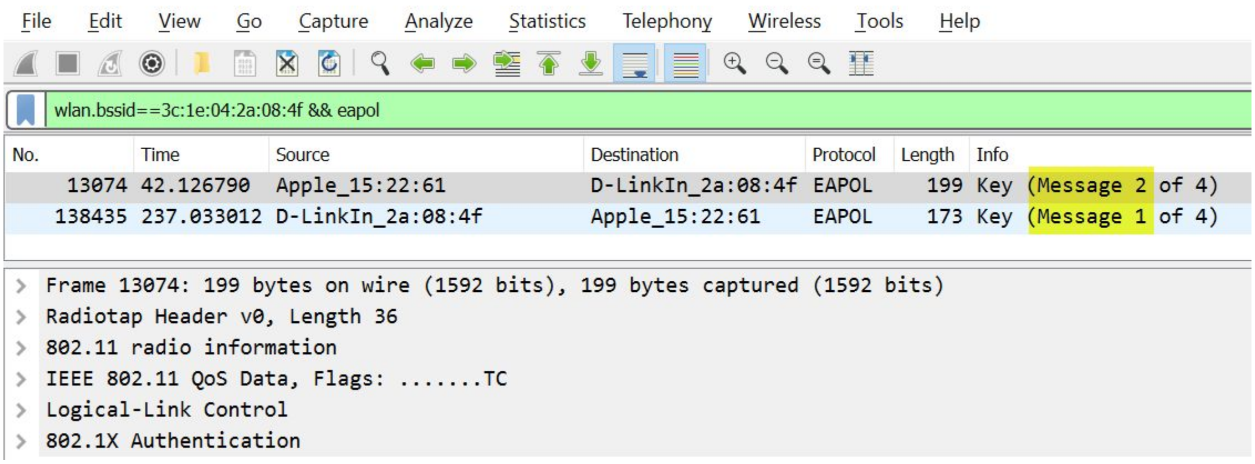
```
(wlan.bssid == e8:de:27:16:70:c9) && wlan.fc.type_subtype == 0

No.         Time         Source              Destination          Protocol   Length  Info
      16764 57.449869    Motorola_31:a0:3b   Tp-LinkT_16:70:c9    802.11        119  Association Request, SN=1406, FN=0, Flags=........C, SSID=Ruther_SSID
      22600 67.405665    Tp-LinkT_12:1c:db   Tp-LinkT_16:70:c9    802.11        129  Association Request, SN=105, FN=0, Flags=........C, SSID=Ruther_SSID
      72266 113.986004   02:8e:e4:d0:55:aa   Tp-LinkT_16:70:c9    802.11        119  Association Request, SN=210, FN=0, Flags=........C, SSID=Ruther_SSID

> Frame 16764: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
v IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  v Frame Control Field: 0x0000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0000 .... = Subtype: 0
    > Flags: 0x00
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Tp-LinkT_16:70:c9 (e8:de:27:16:70:c9)
    Destination address: Tp-LinkT_16:70:c9 (e8:de:27:16:70:c9)
    Transmitter address: Motorola_31:a0:3b (5c:51:88:31:a0:3b)
    Source address: Motorola_31:a0:3b (5c:51:88:31:a0:3b)
    BSS Id: Tp-LinkT_16:70:c9 (e8:de:27:16:70:c9)
    .... .... .... 0000 = Fragment number: 0
    0101 0111 1110 .... = Sequence number: 1406
    Frame check sequence: 0x9100d50c [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 wireless LAN
```

Q5. Is it possible to launch a passphrase cracking attack on SSID ‘Amazon’? State Yes or No.

A. Yes

BSSID belongs to SSID Amazon.

Filter: wlan.bssid==3c:1e:04:2a:08:4f && eapol



wlan.bssid==3c:1e:04:2a:08:4f && eapol

No.	Time	Source	Destination	Protocol	Length	Info
13074	42.126790	Apple_15:22:61	D-LinkIn_2a:08:4f	EAPOL	199	Key (Message 2 of 4)
138435	237.033012	D-LinkIn_2a:08:4f	Apple_15:22:61	EAPOL	173	Key (Message 1 of 4)

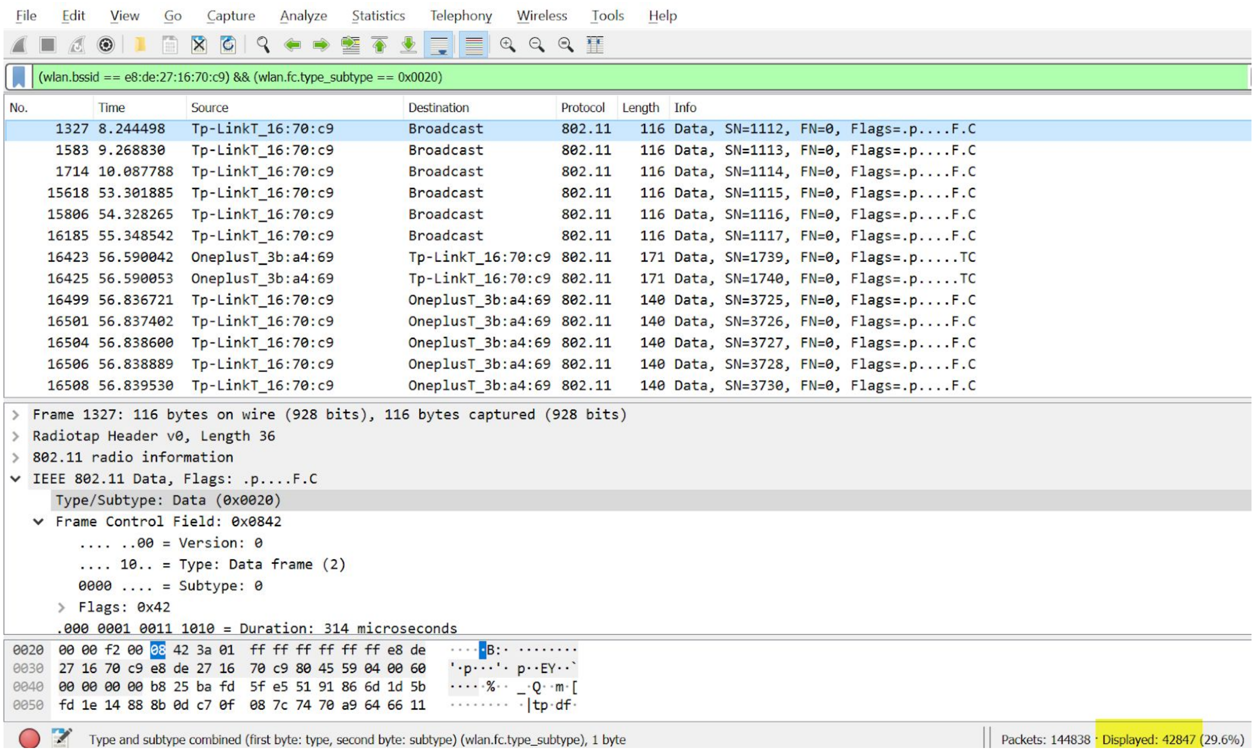
```
> Frame 13074: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
> 802.1X Authentication
```

All information needed for launching cracking attack is present in Message 1 and 2 of 4-way handshake.

Q6. How many data packets were exchanged through BSSID e8:de:27:16:70:c9?

A. 42847

Filter: (wlan.bssid == e8:de:27:16:70:c9) && (wlan.fc.type_subtype == 0x0020)



```
(wlan.bssid == e8:de:27:16:70:c9) && (wlan.fc.type_subtype == 0x0020)
```

```
No.    Time       Source              Destination         Protocol Length Info
 1327 8.244498    Tp-LinkT_16:70:c9   Broadcast           802.11    116 Data, SN=1112, FN=0, Flags=.p....F.C
 1583 9.268830    Tp-LinkT_16:70:c9   Broadcast           802.11    116 Data, SN=1113, FN=0, Flags=.p....F.C
 1714 10.087788   Tp-LinkT_16:70:c9   Broadcast           802.11    116 Data, SN=1114, FN=0, Flags=.p....F.C
15618 53.301885   Tp-LinkT_16:70:c9   Broadcast           802.11    116 Data, SN=1115, FN=0, Flags=.p....F.C
15806 54.328265   Tp-LinkT_16:70:c9   Broadcast           802.11    116 Data, SN=1116, FN=0, Flags=.p....F.C
16185 55.348542   Tp-LinkT_16:70:c9   Broadcast           802.11    116 Data, SN=1117, FN=0, Flags=.p....F.C
16423 56.590042   OneplusT_3b:a4:69   Tp-LinkT_16:70:c9   802.11    171 Data, SN=1739, FN=0, Flags=.p.....TC
16425 56.590053   OneplusT_3b:a4:69   Tp-LinkT_16:70:c9   802.11    171 Data, SN=1740, FN=0, Flags=.p.....TC
16499 56.836721   Tp-LinkT_16:70:c9   OneplusT_3b:a4:69   802.11    140 Data, SN=3725, FN=0, Flags=.p....F.C
16501 56.837402   Tp-LinkT_16:70:c9   OneplusT_3b:a4:69   802.11    140 Data, SN=3726, FN=0, Flags=.p....F.C
16504 56.838600   Tp-LinkT_16:70:c9   OneplusT_3b:a4:69   802.11    140 Data, SN=3727, FN=0, Flags=.p....F.C
16506 56.838889   Tp-LinkT_16:70:c9   OneplusT_3b:a4:69   802.11    140 Data, SN=3728, FN=0, Flags=.p....F.C
16508 56.839530   Tp-LinkT_16:70:c9   OneplusT_3b:a4:69   802.11    140 Data, SN=3730, FN=0, Flags=.p....F.C
```

```
> Frame 1327: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
v IEEE 802.11 Data, Flags: .p....F.C
    Type/Subtype: Data (0x0020)
  v Frame Control Field: 0x0842
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0000 .... = Subtype: 0
    > Flags: 0x42
    .000 0001 0011 1010 = Duration: 314 microseconds
```

```
0020  00 00 f2 00 08 42 3a 01  ff ff ff ff ff ff e8 de   ·····B:· ········
0030  27 16 70 c9 e8 de 27 16  70 c9 80 45 59 04 00 60   '·p···'· p··EY··`
0040  00 00 00 00 b8 25 ba fd  5f e5 51 91 86 6d 1d 5b   ·····%·· _·Q··m·[
0050  fd 1e 14 88 8b 0d c7 0f  08 7c 74 70 a9 64 66 11   ········ ·|tp·df·
```

```
Type and subtype combined (first byte: type, second byte: subtype) (wlan.fc.type_subtype), 1 byte    Packets: 144838 · Displayed: 42847 (29.6%)
```

References:

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