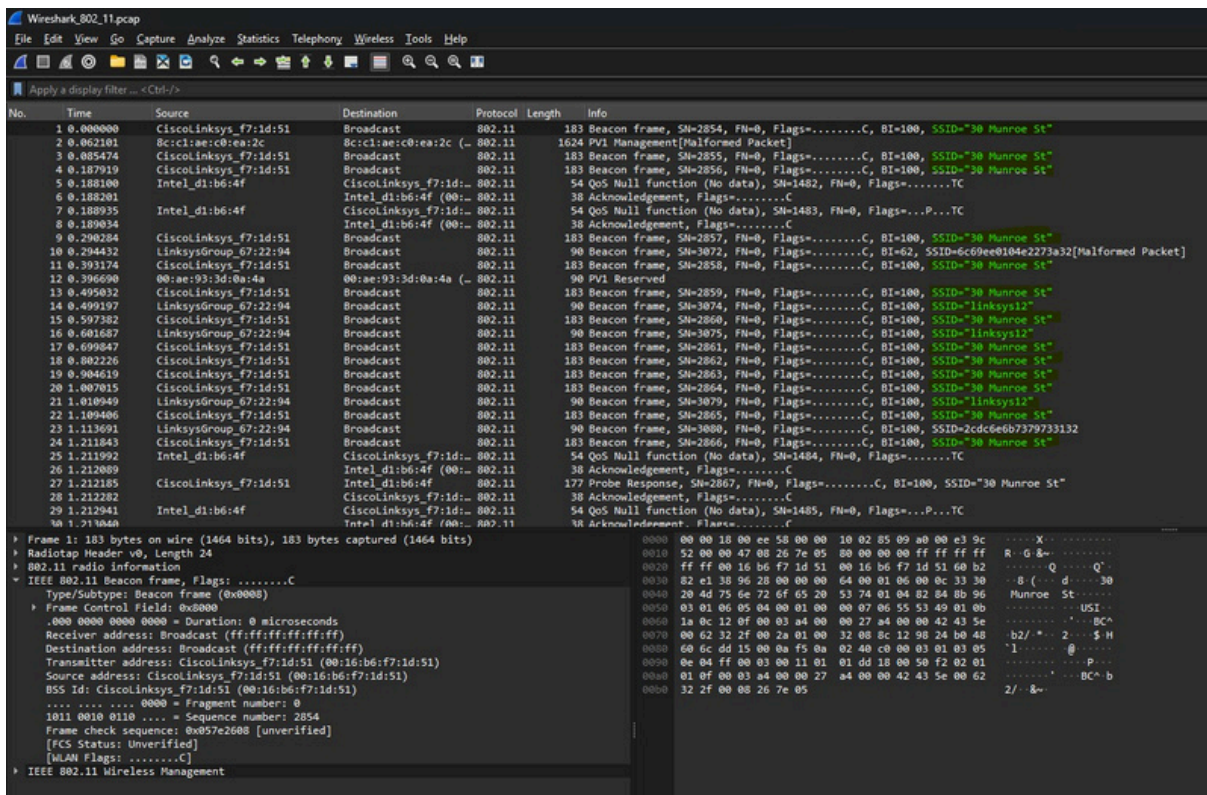


Laboratório Wi-Fi 802.11 Wireshark

Alunos: Eduardo Henrique e Murilo

1. Quais são os SSIDs dos dois pontos de acesso que emitem a maioria dos beacons quadros neste rastreamento?

○ Resposta: "30MunroeSt" e "linksys12".



2.

○ Quais são os intervalos de tempo entre as transmissões dos frames do beacon para o ponto de acesso *linksys_ses_24086*?

Resposta: Não há, pois não houve conexão com esse AP..

○ Do ponto de acesso *30 Munroe St*?

Resposta: 0,102400

No.	Time	Source	Destination	Protocol	Length	Info
141	6.460863	CiscoLinksys_F7:1d:51	Intel_1f:57:13	002.11	177	Probe Response, SM=2926, FN=0, Flags=.....R....C, BI=100, SSID="30 Munroe St"
142	6.461563	CiscoLinksys_F7:1d:51	Intel_1f:57:13	002.11	177	Probe Response, SM=2926, FN=0, Flags=.....R....C, BI=100, SSID="30 Munroe St"
143	6.463862	CiscoLinksys_F7:1d:51	Intel_1f:57:13	002.11	177	Probe Response, SM=2926, FN=0, Flags=.....R....C, BI=100, SSID="30 Munroe St"
144	6.464563	CiscoLinksys_F7:1d:51	Intel_1f:57:13	002.11	177	Probe Response, SM=2926, FN=0, Flags=.....R....C, BI=100, SSID="30 Munroe St"
145	6.536322	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2927, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
146	6.638718	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2928, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
147	6.741163	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2929, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
148	6.845991	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2930, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
149	6.945991	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2931, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
150	7.048366	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2932, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
151	7.150671	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2933, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
152	7.253159	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2934, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
153	7.355483	CiscoLinksys_F7:1d:51	Broadcast	002.11	183	Beacon frame, SM=2935, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
154	7.355800	Intel_d1:b6:4f	CiscoLinksys_F7:1d:51	002.11	54	QoS Null Function (No data), SM=4996, FN=0, Flags=.....TC
155	7.355704	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	Intel_d1:b6:4f	002.11	38	Acknowledgement, Flags=.....C
156	7.355800	CiscoLinksys_F7:1d:51	Intel_d1:b6:4f	002.11	177	Probe Response, SM=2936, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
157	7.355897	CiscoLinksys_F7:1d:51	CiscoLinksys_F7:1d:51 (00:16:b6:f7:1d:51) (RA)	002.11	38	Acknowledgement, Flags=.....C
Frame 153: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on 0 Radiotap Header v0, Length 24 Header revision: 0 Header pad: 0 Header length: 24 Present flags Flags: 0x0 Data Rate: 1.0 Mb/s Channel frequency: 2437 [80.6] Channel flags: 0x00ab, Complementary Code Keying (CKK), 2 GHz spectrum Antenna signal: -30 dBm Antenna noise: -180 dBm Signal Quality: 100 Antenna: 0 dB antenna signal: 70 dB RX flags: 0x014c 802.11 radio information IEEE 802.11 Beacon frame, Flags:C IEEE 802.11 Wireless Management Fixed parameters (12 bytes) Timestamp: 174326374700 Beacon Interval: 6.180000 [Seconds] Capabilities Information: 0x0001 Tagged parameters (119 bytes) Tag: SSID parameter set: "30 Munroe St" Tag: Supported Rates 1(0), 2(0), 5.5(0), 11(0), [Mbit/sec] Tag: DS Parameter set: Current Channel: 6 Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap Tag: Country Information: Country Code US, Environment Indoor Tag: EDCA Parameter Set Tag: ERP Information Tag: Extended Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec] Tag: Vendor Specific: Airgo Networks, Inc. Tag: Vendor Specific: Microsoft Corp.: MPV/MPE: Parameter Element						

3. Qual é (em notação hexadecimal) o endereço MAC de origem no quadro de beacon de 30 Munroe St?

☐ Resposta:00:16:b6:f7:1d:51

4. Qual (em notação hexadecimal) é o endereço MAC de destino no beacon quadro de 30 Munroe St?

☐ Resposta:ff:ff:ff:ff:ff:ff

```

▶ Frame 153: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
▼ Radiotap Header v0, Length 24
  Header revision: 0
  Header pad: 0
  Header length: 24
  ▶ Present flags
  ▶ Flags: 0x10
  Data Rate: 1,0 Mb/s
  Channel frequency: 2437 [BG 6]
  ▶ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
  Antenna signal: -30 dBm
  Antenna noise: -100 dBm
  Signal Quality: 100
  Antenna: 0
  dB antenna signal: 70 dB
  ▶ RX flags: 0x814c
▶ 802.11 radio information
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▶ Frame Control Field: 0x8000
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  .... 0000 = Fragment number: 0
  1011 0111 0111 .... = Sequence number: 2935
  Frame check sequence: 0x8d22814c [unverified]
  [FCS Status: Unverified]
  [WLAN Flags: .....C]
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (12 bytes)
    Timestamp: 174326374786
    Beacon Interval: 0,102400 [Seconds]
    ▶ Capabilities Information: 0x0601
  ▼ Tagged parameters (119 bytes)
    ▶ Tag: SSID parameter set: "30 Munroe St"
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 6
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    ▶ Tag: Country Information: Country Code US, Equipment Id 00000000

```

5. Qual (em notação hexadecimal) é o ID MAC BSS no quadro de beacon de 30 Munroe St?

○ Resposta: 00:16:b6:f7:1d:51

6. Os quadros de beacon do ponto de acesso 30 Munroe St anunciam que o ponto de acesso pode suportar quatro taxas de dados e oito "taxas suportadas estendidas" adicionais. Quais são essas taxas?

- Taxas de dados suportadas (4): 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps
- Taxas de dados suportadas estendidas (8): 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps

```

IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
    Timestamp: 174326374786
    Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x00601
  Tagged parameters (119 bytes)
    Tag: SSID parameter set: "30 Munroe St"
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 6
    Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    Tag: Country Information: Country Code US, Environment Indoor
    Tag: EDCA Parameter Set
    Tag: ERP Information
    Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: Vendor Specific: Airgo Networks, Inc.
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  
```

7. Encontre o quadro 802.11 contendo o segmento TCP SYN para esta primeira sessão TCP (que baixa alice.txt).

- Quais são os três campos de endereço MAC no quadro 802.11?
 - Endereço MAC do receptor (Receiver Address): 00:16:b6:f7:1d:51 (Ponto de Acesso)
 - Endereço MAC do destino (Destination Address): 00:16:b6:f4:eb:a8 (Roteador de Primeiro Salto)
 - Endereço MAC da origem (Source Address): 00:13:02:d1:b6:4f (Host sem fio)

```

No.    Time    Source                Destination            Protocol Length  Info
--
480    24.828253  192.168.1.109        128.119.245.12        HTTP      537      GET /wireshark-labs/alice.txt HTTP/1.1
    Frame 480: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface 0
    Radiotap Header v0, Length 24
    802.11 radio information
      PHY type: 802.11g (ERP) (6)
      Proprietary mode: None (0)
      Data rate: 48.0 Mb/s
      Channel: 6
      Frequency: 2437MHz
      Signal strength (dB): 62 dBm
      Signal strength (dBm): -38 dBm
      Noise level (dBm): -100 dBm
      Signal/noise ratio (dB): 62 dB
      [Duration: 180µs]
      [Preamble: 20µs]
    IEEE 802.11 QoS Data, Flags: .....TC
      Type/Subtype: QoS Data (0x002B)
      Frame Control Field: 0x8801
      .0000 0000 0010 1100 = Duration: 44 microseconds
      Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
      Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
      Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
      Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
      BSS ID: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
      STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
      .... = Fragment number: 0
      0000 0011 0011 .... = Sequence number: 51
      Frame check sequence: 0x147e6bd9 [unverified]
      [FCS Status: Unverified]
      [MLAN Flags: .....TC]
      QoS Control: 0x0000
    Logical-Link Control
    Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
    Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 1, Ack: 1, Len: 435
    Hypertext Transfer Protocol
      [Community ID: 1:1T0936Caesdl5pv+A5nf8XecwH8=]
    TRANSMISSION Data
  
```

- ☐ Qual endereço MAC neste quadro corresponde ao host sem fio (dê a representação hexadecimal do endereço MAC para o host)?
 - Hostsemfio(WirelessHost):00:13:02:d1:b6:4f
- ☐ Para o ponto de acesso?
 - PontodeAcesso(AccessPoint):00:16:b6:f7:1d:51
- ☐ Para o roteador de primeiro salto?
 - RoteadordePrimeiroSalto(First-HopRouter):00:16:b6:f4:eb:a8
- ☐ Qual é o endereço IP do host sem fio que envia este segmento TCP?
 - EndereçoIPdoHostsemfio:192.168.1.109
- ☐ Qual é o endereço IP de destino?
 - EndereçoIPdeDestino:128.119.245.12
- ☐ Este endereço IP de destino corresponde ao host, ponto de acesso, roteador de primeiro salto ou algum outro dispositivo conectado à rede? Explique.
 - Corresponde a um dispositivo remoto, que é um servidor da Internet. Ele não corresponde ao host sem fio, ao ponto de acesso ou ao roteador de primeiro salto. Este é o destino final do segmento TCP que está sendo enviado. O roteador de primeiro salto (MAC: 00:16:b6:f4:eb:a8) encaminha o pacote para a Internet, onde ele será entregue ao servidor remoto identificado pelo endereço IP 128.119.245.12.

8. Encontre o quadro 802.11 contendo o segmento SYNACK para esta sessão TCP.

The image shows a Wireshark packet capture of a wireless network. The top pane displays a list of packets. Packet 1013 is selected, showing a SYNACK segment. The packet details pane on the left shows the 802.11 frame structure, including the PHY type (802.11g), data rate (48.0 Mb/s), and various signal strength metrics. The packet bytes pane on the right shows the raw data of the SYNACK segment, including the TCP header and payload. The packet list pane on the left shows the packet details, including the source and destination IP addresses (192.168.1.109 and 128.119.245.12) and the sequence number (3314).

No.	Time	Source	Destination	Protocol	Length	Info
1013	32.825631	128.119.240.19	192.168.1.109	TCP	110	00 → 2541 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM

Frame 1013: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0

RadioTap Header v0, Length 24

802.11 radio information

- PHY type: 802.11g (ERP) (6)
- Proprietary mode: None (0)
- Data rate: 48.0 Mb/s
- Channel: 6
- Frequency: 2437MHz
- Signal strength (dB): 66 dB
- Signal strength (dBm): -34 dBm
- Noise level (dBm): -100 dBm
- Signal/noise ratio (dB): 66 dB
- [Duration: 36µs]
- [Preamble: 20µs]

IEEE 802.11 QoS Data, Flags:F.C

Type/Subtype: QoS Data (0x0028)

Frame Control Field: 0x8802

- 0000 0000 0010 1000 = Duration: 40 microseconds
- Receiver address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
- Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
- Destination address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
- Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
- BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
- STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
- 0000 = Fragment number: 0
- 1100 1111 0010 = Sequence number: 3314
- Frame check sequence: 0x20e725d9 [unverified]
- [FCFS Status: Unverified]
- [WLAN Flags:F.C]
- QoS Control: 0x0300

Logical-Link Control

Internet Protocol Version 4, Src: 128.119.240.19, Dst: 192.168.1.109

Transmission Control Protocol, Src Port: 80, Dst Port: 2541, Seq: 0, Ack: 1, Len: 0

[Community ID: 1:4521QoeGAX6kp@Wd0VA9XA7320=]

- Quais são os três campos de endereço MAC no quadro 802.11?
 - Endereço MAC do receptor (Receiver Address): 00:13:02:d1:b6:4f (Host sem fio)
 - Endereço MAC do transmissor (Transmitter Address): 00:16:b6:f7:1d:51 (Ponto de Acesso)
 - Endereço MAC do destino (Destination Address): 00:13:02:d1:b6:4f (Host sem fio)
 - BSSID (Basic Service Set Identifier): 00:16:b6:f7:1d:51 (Ponto de Acesso)

The image shows a Wireshark packet capture. The selected packet is a radio frame (No. 1013) with a duration of 0.000000000 seconds. The frame is captured on the interface 'eth0' and is 110 bytes long. The frame details are as follows:

- Frame 1013:** 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 'eth0'
- RadioTap Header v0, Length 24:**
 - PHY type: 802.11g (ERP) (6)
 - Proprietary mode: None (0)
 - Data rate: 40.0 Mb/s
 - Channel: 6
 - Frequency: 2437MHz
 - Signal strength (dB): 66 dB
 - Signal strength (dBm): -34 dBm
 - Noise level (dBm): -100 dBm
 - Signal/noise ratio (dB): 66 dB
 - [Duration: 36µs]
- IEEE 802.11 QoS Data, Flags:F.C**
 - Type/Subtype: QoS Data (0x0028)
 - Frame Control Field: 0x8802
 - Duration: 40 microseconds
 - Receiver address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
 - Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
 - Destination address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
 - Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
 - BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
 - STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
 - Fragment number: 0
 - Sequence number: 3314
 - Frame check sequence: 0x20e725d9 [unverified]
 - [FC Status: Unverified]
 - [LAN Flags:F.C]
 - QoS Control: 0x0300
 - Logical-Link Control
 - Internet Protocol Version 4, Src: 128.119.240.19, Dst: 192.168.1.109
 - Transmission Control Protocol, Src Port: 50, Dst Port: 2541, Seq: 0, Ack: 1, Len: 0
 - [Community ID: 1:452NqegXGkpWwL6vA9AATJ2Z=]

- Qual endereço MAC neste quadro corresponde ao host?
 - Host sem fio (Wireless Host): 00:13:02:d1:b6:4f
- Ao ponto de acesso?
 - Ponto de Acesso (Access Point): 00:16:b6:f7:1d:51
- Ao roteador de primeiro salto?
 - O roteador de primeiro salto não é diretamente referenciado neste quadro. Ele está representado no nível de IP, mas seu endereço MAC não aparece neste quadro 802.11.
- O endereço MAC do remetente no quadro corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado dentro deste datagrama?
 - Sim. O endereço IP do remetente (neste caso, o dispositivo que enviou o segmento SYNACK) é 128.119.240.19, e este datagrama está encapsulado no quadro 802.11. O remetente do quadro 802.11 é o ponto de acesso (MAC: 00:16:b6:f7:1d:51), que transmite os pacotes recebidos do roteador para o host sem fio.

9.

- Quais são as duas ações tomadas (isto é, os quadros são enviados) pelo host no rastreamento logo após t=49, para encerrar a associação com o AP 30 Munroe St que estava inicialmente em vigor quando a coleta de rastreamento começou?

■ UmDHCPéenviadopara192.168.1.1.

■ O host envia um quadro de DEAUTHENTICATION após 0,02 segundos.

- Olhando para a especificação 802.11, há outro quadro que você esperava ver, mas não vê aqui?

No.	Time	Source	Destination	Protocol	Length	Info
1729	49.440041	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, B1=100, SSID="30 Munroe St"
1730	49.440146	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
1731	49.440243	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	36	Acknowledgement, Flags=.....C
1732	49.542401	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3585, FN=0, Flags=.....C, B1=100, SSID="30 Munroe St"
1733	49.583615	192.168.1.100	192.168.1.1	DHCP	300	DHCP Release - Transaction ID 0x5a526
1734	49.583771	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	36	Acknowledgement, Flags=.....C
1735	49.600617	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.600770	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	36	Acknowledgement, Flags=.....C
1737	49.614478	Intel_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID="linksys Ses_24086"
1738	49.615869	CiscoLinksys_f5:ba:bb	(00:18:39:f5:ba:bb) (RA)	802.11	36	Acknowledgement, Flags=.....C
1739	49.617213	CiscoLinksys_f5:ba:bb	(00:18:39:f5:ba:bb) (RA)	802.11	36	Acknowledgement, Flags=.....C
1740	49.630557	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.630700	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C
1742	49.640702	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C
1743	49.641910	CiscoLinksys_f5:ba:bb	(00:18:39:f5:ba:bb) (RA)	802.11	36	Acknowledgement, Flags=.....C
1744	49.642315	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C
1745	49.644710	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3589, FN=0, Flags=.....C, B1=100, SSID="30 Munroe St"
1746	49.645310	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C
1747	49.647111	CiscoLinksys_f5:ba:bb	(00:18:39:f5:ba:bb) (RA)	802.11	36	Acknowledgement, Flags=.....C

Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)	0000 00 00 18 00 4e 58 00 00 10 02 05 09 a0 00 e7 9cX.....
RadioTap Header v0, Length 24	0010 64 00 00 4b 4c 37 30 ed b0 00 3a 01 00 18 39 f5	d KL70 : : 9
802.11 radio information	0020 3a 1b 00 13 02 d1 b6 4f 00 18 39 f5 ba bb 60 64O 9 : : d
IEEE 802.11 Authentication, Flags:C	0030 00 00 01 00 00 4c 37 30 edL7 0

```

Type/Subtype: Authentication (0x0000)
  Frame Control Field: 0x0000
    .... 00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1811 .... = Subtype: 11
    = Flags: 0x00
      .... 00 = OS status: Not leaving OS or network is operating in AD-HOC mode (To OS: 0)
      .... 00.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PMF NOT: STA will stay up
      ..0 .... = More Data: No data buffered
      ..0 .... = Protected flag: Data is not protected
      R... .... = WTC/Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    Destination address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
    .... 0000 = Fragment number: 0
    0110 0100 0110 .... = Sequence number: 1606
    Frame check sequence: 0xed30374c [unverified]
    [CS Status: Unverified]
    [Auth Flags: .....C]
  IEEE 802.11 Wireless Management
    Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication Seq: 0x0001
      Status code: Successful (0x0000)

```

10.Examine o arquivo de rastreamento e procure quadros de AUTENTICAÇÃO enviados do host para um AP e vice-versa.

- QuantasmensagensdeAUTENTICAÇÃO são enviadas do host sem fio para o AP *linksys_ses_24086* (que tem um endereço MAC Cisco_Li_f5:ba:bb) começando por volta de t=49?

■ Resposta:2.

1740 49.647827	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	36	Acknowledgement, Flags=.....C
1740 49.649705	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R...C
1750 49.651878	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1607, FN=0, Flags=.....C, SSID="linksys Ses_24086"
1751 49.653218	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1607, FN=0, Flags=.....R...C, SSID="linksys Ses_24086"
1752 49.662857	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	36	Acknowledgement, Flags=.....C
1753 49.663950	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	36	Acknowledgement, Flags=.....C
1754 49.665704	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	36	Acknowledgement, Flags=.....C

11.O host deseja que a autenticação exija uma chave ou seja aberta?

- Resposta:Exige.

No.	Time	Source	Destination	Protocol	Length	Info
1738	49.615869		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1739	49.617713		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1740	49.638857	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1742	49.640702	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1743	49.641910		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1744	49.642315	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1745	49.644710	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3589, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
1746	49.645319	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1747	49.646711		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1748	49.647827		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1749	49.649705	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1750	49.651078	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID="linksys_SES_24086"
1751	49.653218	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID="linksys_SES_24086"
1752	49.662857		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1753	49.663950		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1754	49.665704		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1755	49.669072		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
1756	49.671321		CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb) (RA)	802.11	38	Acknowledgement, Flags=.....C
Frame 1751: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)						
Ethernet II Header, Length 24						
IEEE 802.11 Association Request, Flags:R...C						
IEEE 802.11 Wireless Management						
Fixed parameters (4 bytes)						
Capabilities Information: 0x0011						
.....1 = ESS capabilities: Transmitter is an AP						
.....0 = IBSS status: Transmitter belongs to a BSS						
.....0 = Reserved: 0						
.....0 = Reserved: 0						
.....1 = Privacy: Data confidentiality required						
.....0 = Short Preamble: Not Allowed						
.....0 = Critical Update Flag: False						
.....0 = Nontransmitted BSSIDs: Critical Update Flag: False						
.....0 = Spectrum Management: Not Implemented						
.....0 = QoS: Not Implemented						
.....0 = Short Slot Time: Not in use						
.....0 = Automatic Power Save delivery: Not Implemented						
.....0 = Radio Measurement: Not Implemented						
.....0 = EPD: Not Implemented						
.....0 = Reserved: 0						
.....0 = Reserved: 0						
Listen Interval: 0x000a						
Tagged parameters (51 bytes)						
Tag: SSID parameter set: "linksys_SES_24086"						
Tag Number: SSID parameter set (0)						
Tag length: 17						
SSID: "linksys_SES_24086"						
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]						
Tag Number: Supported Rates (1)						
Tag length: 4						
Supported Rates: 1(B) (0x02)						
Supported Rates: 2(B) (0x04)						
Supported Rates: 5.5(B) (0x0b)						
Supported Rates: 11(B) (0x0e)						
Tag: Vendor Specific: Microsoft Corp.: WPA Information Element						

12. Você vê uma resposta AUTENTICAÇÃO do AP *linksys_ses_24086* no rastrear?

☐ Resposta: Não.

13. Agora, vamos considerar o que acontece quando o host desiste de tentar se associar ao AP *linksys_ses_24086* e tentar se associar ao AP *30 Munroe St*.

Procure por quadros AUTHENTICATION enviados do host para um AP e vice-versa. Em que momentos há um quadro AUTHENTICATION do host para o AP *30 Munroe St* e quando há uma resposta AUTHENTICATION enviada desse AP para o host em resposta?

(Observe que você pode usar a expressão de filtro "wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" para exibir apenas os quadros AUTHENTICATION neste rastreamento para este host sem fio.)

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R..C
1742	49.640702	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R..C
1744	49.642315	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R..C
1746	49.643310	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R..C
1749	49.649705	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....R..C
1821	53.785833	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....R..C
1822	53.787070	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....R..C
1921	57.889232	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....R..C
1922	57.890325	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....R..C
1923	57.891321	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....R..C
1924	57.896970	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....R..C
2122	62.171951	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....R..C
2123	62.172946	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....R..C
2124	62.174070	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....R..C
2156	63.168007	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R..C
2158	63.169071	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R..C
2160	63.169767	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R..C
2164	63.170692	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R..C

<pre> Frame 2156: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) Radiotap Header v0, Length 24 IEEE 802.11 radio information IEEE 802.11 Authentication, Flags:C Type/Subtype: Authentication (0x0000) Frame Control Field: 0xb000 00 = Version: 0 00.. = Type: Management frame (0) 1011 = Subtype: 11 Flags: 0x000 00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0) 0... = More Fragments: This is the last fragment 0... = Retry: Frame is not being retransmitted ...0 = PWR MTF: STA will stay up ..0 = More Data: No data buffered .0. = Protected flag: Data is not protected 0... = HT/Order flag: Not strictly ordered .000 0000 0010 1100 = Duration: 44 microseconds Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f) Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f) BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) 0000 = Fragment number: 0 0110 0110 1111 = Sequence number: 1647 Frame check sequence: 0x47edcbe0 [unverified] [FCS Status: Unverified] [WLAN Flags:C] </pre>	<pre> 0000 00 00 18 00 ee 58 00 00 10 6c 85 09 c0 00 e4 9c X...1..... 0010 59 00 00 48 e9 cb e8 47 b0 00 2c 00 00 16 b6 f7 Y...G..... 0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f7 1d 51 f0 66 Q...Q...f 0030 00 00 01 00 00 e0 cb e8 47 G </pre>
--	--

14.Uma ASSOCIATE REQUEST do host para o AP e um quadro ASSOCIATE RESPONSEcorrespondentedoAPparaohostsãousados paraqueohost seja associado a um AP.

○ Em que momento há uma ASSOCIATE REQUEST do host para o 30 Munroe St AP?

■ Resposta:63.169910

No.	Time	Source	Destination	Protocol	Length	Info
1824	53.789944	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1613, FN=0, Flags=.....C, SSID="Linksys_SIS_24000"
1825	53.789943	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1613, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
1826	53.789568	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1613, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
1920	57.889099	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1628, FN=0, Flags=.....C, SSID="Linksys_SIS_24000"
1922	57.892065	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1628, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
1932	57.911195	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1628, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
1933	57.912065	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1628, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
1934	57.924199	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1628, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
1935	57.930254	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1628, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
1937	57.939196	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1628, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
2126	62.170040	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1645, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
2127	62.170184	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	187	Association Request, SN=1645, FN=0, Flags=.....R..C, SSID="Linksys_SIS_24000"
2162	63.169000	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	84	Association Request, SN=1646, FN=0, Flags=.....C, SSID="Munroe St"
2164	63.169281	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	84	Association Request, SN=1728, FN=0, Flags=.....C, SSID="Munroe St"

<pre> Frame 2162: 84 bytes on wire (712 bits), 84 bytes captured (712 bits) Radiotap Header v0, Length 24 IEEE 802.11 radio information IEEE 802.11 Association Request, Flags:C Type/Subtype: Association Request (0x0000) Frame Control Field: 0xb000 00 = Version: 0 00.. = Type: Management frame (0) 0000 = Subtype: 0 Flags: 0x000 00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0) 0... = More Fragments: This is the last fragment 0... = Retry: Frame is not being retransmitted ...0 = PWR MTF: STA will stay up ..0 = More Data: No data buffered .0. = Protected flag: Data is not protected 0... = HT/Order flag: Not strictly ordered .000 0000 1000 0000 = Duration: 44 microseconds Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f) Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f) BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) 0000 = Fragment number: 0 0110 0110 0000 = Sequence number: 1646 Frame check sequence: 0x47edcbe0 [unverified] [FCS Status: Unverified] [WLAN Flags:C] </pre>	<pre> 0000 00 00 18 00 ee 58 00 00 10 6c 85 09 c0 00 e4 9c X...1..... 0010 59 00 00 47 c8 ad 30 f0 00 00 2c 00 00 16 b6 f7 d...G..... 0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f7 1d 51 f0 66 Q...Q...f 0030 01 c8 00 00 00 33 30 20 42 75 6e 72 4f 50 20 Munroe 0040 53 74 8e 00 82 64 00 0c 12 10 24 2e 42 90 12 Munroe...G..2 0050 04 50 40 00 c8 ad 30 f0 1... </pre>
---	--

○ Quando a ASSOCIATE REPLY correspondente é enviada?

```

wlan.fc.subtype < 2 && wlan.fc.type == 0 && wlan.addr == 00:13:02:d1:b6:4f
No.    Time           Source                Destination            Protocol Length  Info
1824   53.789944 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1613, FN=0, Flags=.....C, SSID="linksys_SE5_24086"
1825   53.789945 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1613, FN=0, Flags=.....R...C, SSID="linksys_SE5_24086"
1827   53.793588 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1613, FN=0, Flags=.....C, SSID="linksys_SE5_24086"
1926   57.983699 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1620, FN=0, Flags=.....C, SSID="linksys_SE5_24086"
1927   57.984945 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1620, FN=0, Flags=.....R...C, SSID="linksys_SE5_24086"
1932   57.913105 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1620, FN=0, Flags=.....R...C, SSID="linksys_SE5_24086"
1933   57.915945 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1620, FN=0, Flags=.....R...C, SSID="linksys_SE5_24086"
1934   57.924199 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1620, FN=0, Flags=.....R...C, SSID="linksys_SE5_24086"
1935   57.926216 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1620, FN=0, Flags=.....R...C, SSID="linksys_SE5_24086"
1937   57.939196 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1620, FN=0, Flags=.....R...C, SSID="linksys_SE5_24086"
2126   62.176945 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1645, FN=0, Flags=.....C, SSID="linksys_SE5_24086"
2127   62.178194 Intel_d1:b6:4f CiscoLinksys_f5:ba:bb 802.11 107 Association Request, SM=1645, FN=0, Flags=.....R...C, SSID="linksys_SE5_24086"
2162   63.160910 Intel_d1:b6:4f CiscoLinksys_f7:1d:51 802.11 89 Association Request, SM=1645, FN=0, Flags=.....C, SSID="30 Munroe St"
2166   63.192181 CiscoLinksys_f7:1d:51 Intel_d1:b6:4f 802.11 94 Association Response, SM=3728, FN=0, Flags=.....C

+ Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
+ Radiotap header=0, length 24
+ 802.11 radio information
+ IEEE 802.11 Association Response, Flags: .....C
  Type/Subtype: Association Response (0x0000)
  + Frame Control Field: 0x1000
    .... 00.. = Version: 0
    .... 00.. = Type: Management frame (0)
    0001 .... = Subtype: 1
    + Flags: 0x000
      .... 00.. = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0)
      .... 00.. = More Fragments: This is the last fragment
      .... 00.. = Retry: Frame is not being retransmitted
      ...0.... = PMR MGT: STA will stay up
      ..0.... = More Data: No data buffered
      ..0.... = Protected flag: Data is not protected
      0.... = HT/Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    .... 0000 = Fragment number: 0
    1110 1001 0000 .... = Sequence number: 3728
    Frame check sequence: 0x37f2ab2b [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: .....C]
+ IEEE 802.11 Wireless Management

```

(Observe que você pode usar a expressão de filtro “wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f” para exibir apenas os quadros ASSOCIATE REQUEST e ASSOCIATE RESPONSE para este rastreamento.)

15.

○ Quais taxas de transmissão o host está disposto a usar?

```

Tagged parameters (33 bytes)
  Tag: SSID parameter set: "30 Munroe St"
    Tag Number: SSID parameter set (0)
    Tag length: 12
    SSID: "30 Munroe St"
  Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
    Supported Rates: 6(B) (0x8c)
    Supported Rates: 9 (0x12)
    Supported Rates: 12(B) (0x98)
    Supported Rates: 18 (0x24)
  Tag: QoS Capability
    Tag Number: QoS Capability (46)
    Tag length: 1
    QoS Information (STA): 0x00
  Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 4
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 36 (0x48)
    Extended Supported Rates: 48 (0x60)
    Extended Supported Rates: 54 (0x6c)

```

○ AAP?

```

[WLAN Flags: .....C]
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
    Capabilities Information: 0x0601
      ....1 = ESS capabilities: Transmitter is an AP
      ....0 = IBSS status: Transmitter belongs to a BSS
      ....0 = Reserved: 0
      ....0 = Reserved: 0
      ....0 = Privacy: Data confidentiality not required
      ....0 = Short Preamble: Not Allowed
      ....0 = Critical Update Flag: False
      ....0 = Nontransmitted BSSIDs Critical Update Flag: False
      ....0 = Spectrum Management: Not Implemented
      ....1 = QoS: Implemented
      ....1 = Short Slot Time: In use
      ....0 = Automatic Power Save Delivery: Not Implemented
      ....0 = Radio Measurement: Not Implemented
      ....0 = EPD: Not Implemented
      ....0 = Reserved: 0
      ....0 = Reserved: 0
    Status code: Successful (0x0000)
    ..00 0000 0000 0101 = Association ID: 0x0005
  Tagged parameters (36 bytes)
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
      Tag Number: Supported Rates (1)
      Tag length: 4
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
    Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 8
      Extended Supported Rates: 6(B) (0x8c)
      Extended Supported Rates: 9 (0x12)
      Extended Supported Rates: 12(B) (0x98)
      Extended Supported Rates: 18 (0x24)
      Extended Supported Rates: 24(B) (0xb0)
      Extended Supported Rates: 36 (0x48)
      Extended Supported Rates: 48 (0x60)
      Extended Supported Rates: 54 (0x6c)
    Tag: EDCA Parameter Set
      Tag Number: EDCA Parameter Set (12)
      Tag length: 18
      WME QoS Info: 0x0f
      Reserved: 00
      Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECWmin/max 4/10 (CWmin/max 15/10)
      Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 4/10 (CWmin/max 15/10)
      Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 3/4 (CWmin/max 7/15), TXOP 4
      Ac Parameters ACI 3 (Voice), ACM no, AIFSN 2, ECWmin/max 2/3 (CWmin/max 3/7), TXOP 4

```

Para responder a essa pergunta, você precisará examinar os campos de parâmetros do quadro de gerenciamento de LAN sem fio 802.11.

16.

☐ Quais são os endereços MAC do remetente, do receptor e do BSSID nesses frames?

■ Probe request:

1. Origem: 00:12:f0:1f:57:13, Destino: ff:ff:ff:ff:ff:ff, BSSID: ff:ff:ff:ff:ff:ff

■ Probe response:

1. Origem: 00:16:b6:f7:1d:51, Destino: 00:16:b6:f7:1d:51, BSSID: 0:16:b6:f7:1d:51

☐ Qual é a finalidade desses dois tipos de molduras?

■ O probe request é um broadcast enviado pelo host para escanear por um access point. O probe response é utilizado pelo access point para responder ao host.