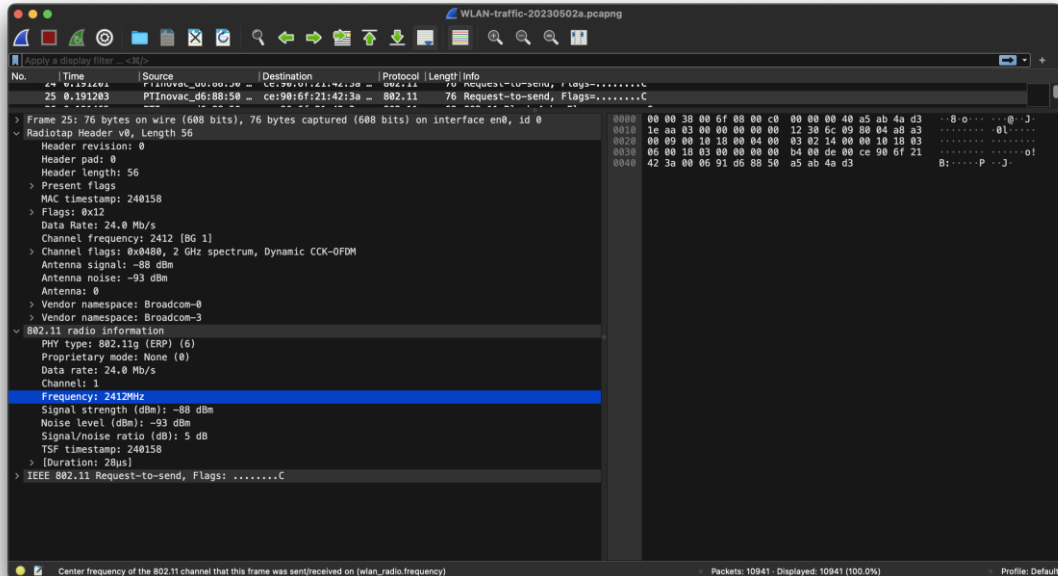


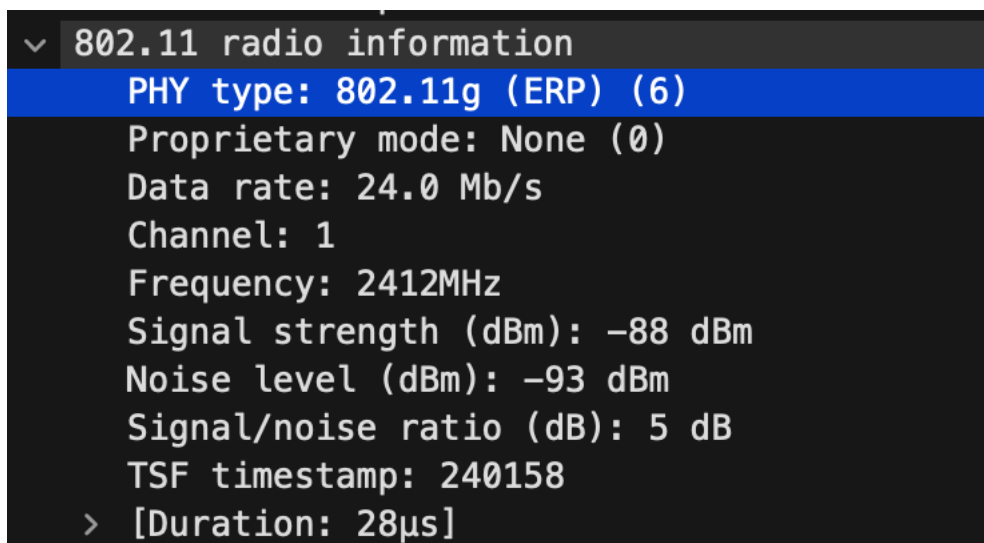
4. Redes sem Fio (Wi-Fi)

1. Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.



O espectro tem uma frequência de 2412MHz e pertence ao canal 1.

2. Identifique a versão da norma IEEE 802.11 que está a ser usada.



A versão da norma é 802.11g (ERP) (6).

3. Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface Wi-Fi pode operar? Justifique.

```
✓ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Proprietary mode: None (0)
  Data rate: 24.0 Mb/s
  Channel: 1
  Frequency: 2412MHz
  Signal strength (dBm): -88 dBm
  Noise level (dBm): -93 dBm
  Signal/noise ratio (dB): 5 dB
  TSF timestamp: 240158
  > [Duration: 28µs]
```

O débito de envio é de 24Mb/s e não corresponde ao débito máximo pois o débito máximo possível é de 54Mb/s.

Essa diferença deve-se ao facto de o ruído ser maior que o sinal.

4. Verifique qual a força do sinal (*Signal strength*) e a qualidade expectável de receção da trama, sabendo que:

```
✓ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Proprietary mode: None (0)
  Data rate: 24.0 Mb/s
  Channel: 1
  Frequency: 2412MHz
  Signal strength (dBm): -88 dBm
  Noise level (dBm): -93 dBm
  Signal/noise ratio (dB): 5 dB
  TSF timestamp: 240158
  > [Duration: 28µs]
```

A força do sinal é de -88dBm e espera-se uma ligação com uma força não confiável.

5. Selecione uma *trama beacon* cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

```
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
    > Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
```

Estão especificados no Frame Control Field.

6. Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
Source address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
BSS Id: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
```

Conclui-se que o recetor e o destino têm o mesmo endereço, assim como o transmissor e a origem. A transmissão realiza-se numa área local.

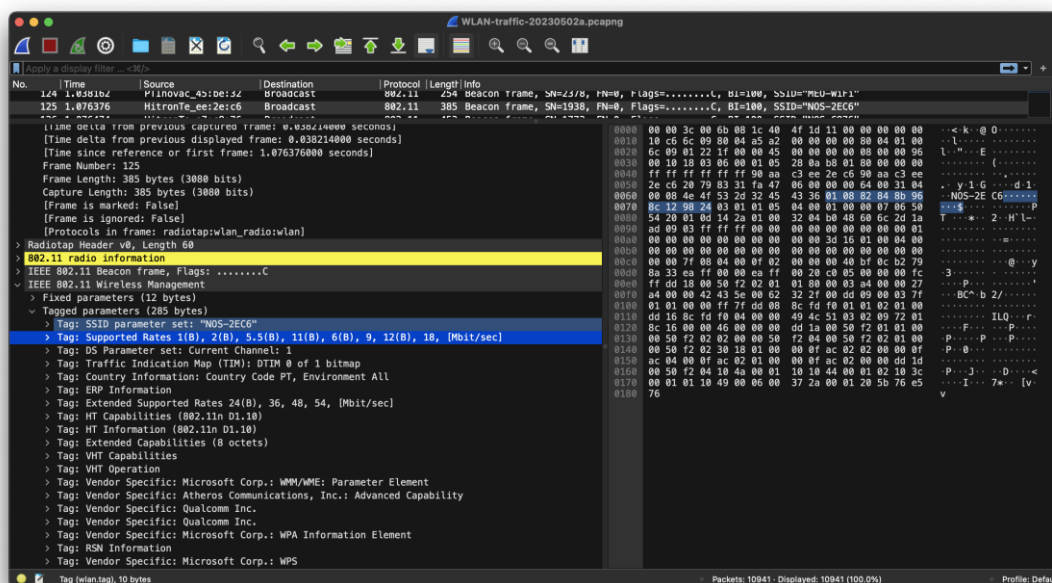
7. Verifique se está a ser usado o método de deteção de erros (CRC). Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

```
125 1.076376 HitronTe_ee:2e:c6 Broadcast 802.11 385 Beacon frame,
> Radiotap Header v0, Length 60
< 802.11 radio information
  PHY type: 802.11n (HT) (7)
  MCS index: 0
  Bandwidth: 20 MHz (0)
  Short GI: False
  Greenfield: False
  FEC: BEC (0)
  Data rate: 6.5 Mb/s
  Channel: 1
  Frequency: 2412MHz
  Signal strength (dBm): -91 dBm
  Noise level (dBm): -94 dBm
  Signal/noise ratio (dB): 3 dB
  TSF timestamp: 1121615
  .... 1 = Last part of an A-MPDU: True
  .... 0 = A-MPDU delimiter CRC error: False
A-MPDU aggregate ID: 0
```

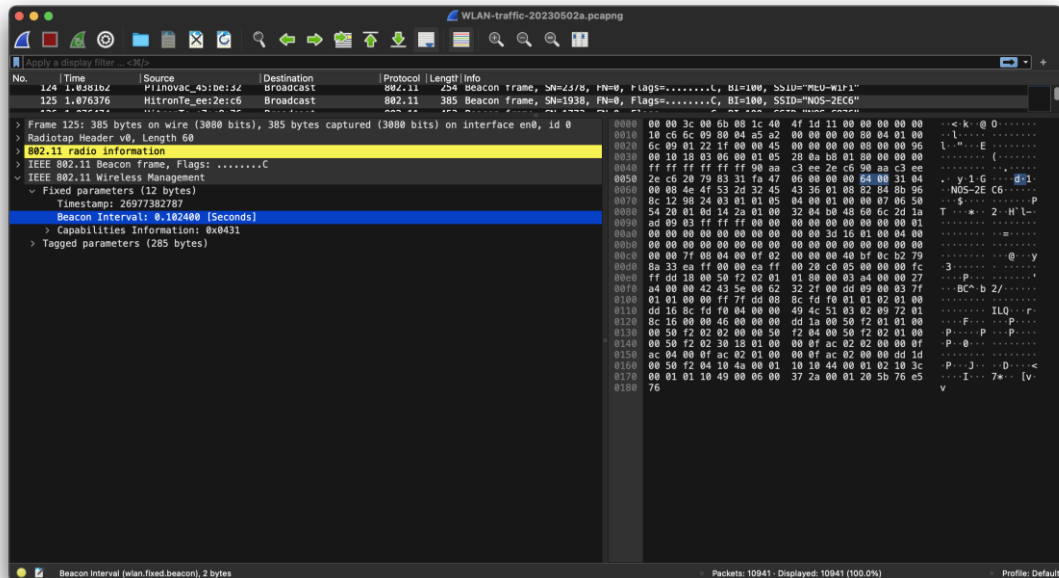
Está a ser usado o método CRC. O mesmo demonstrou que não foram encontrados erros com a flag False.

É necessário usar um método de deteção de erros para uma rede sem fios, devido ao facto de o meio estar mais propenso ao ruído.

8. Uma trama beacon anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos.



9) Qual o intervalo de tempo previsto entre tramas beacon consecutivas (este valor é anunciado na própria trama beacon)? Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.



Na prática, a periodicidade não é verificada com precisão pois há vários fatores externos (ruído, congestão da rede...) que influenciam essa variável.

10. Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura. Explícite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

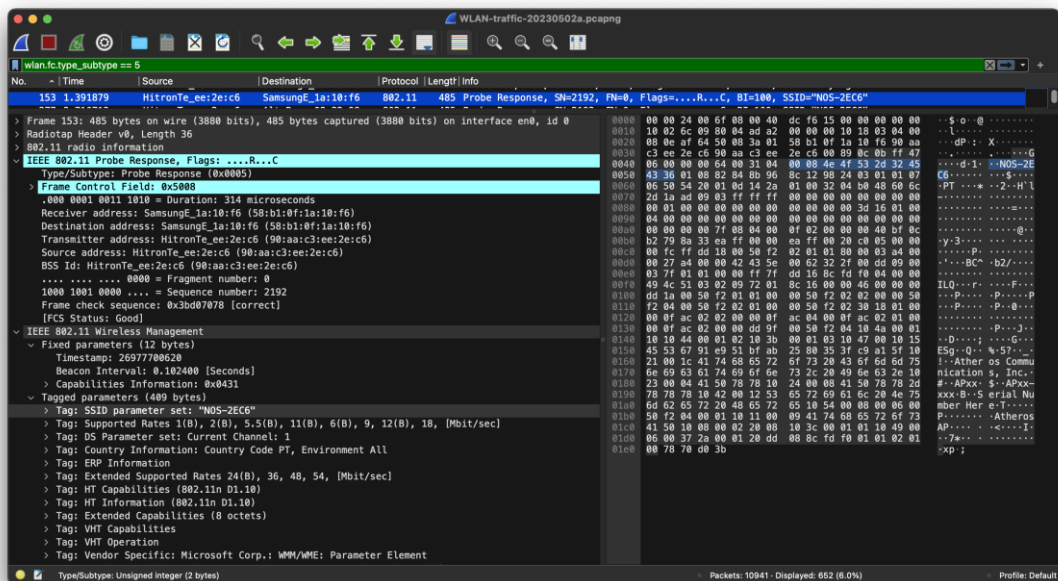
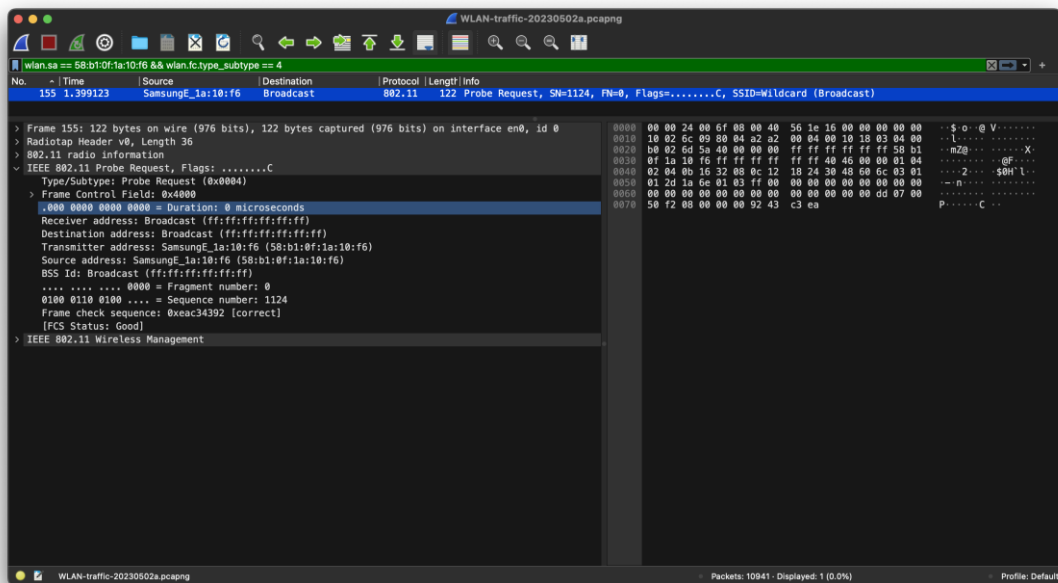
```
"\"FlyingNet\"",
"\"MEO-9BF2A0\"",
"\"Masmorra do Sexo\"",
"\"K6000 Plus\"",
"\"MEO-9E9BB0\"",
"\"NOS-2EC6\"",
"\"MEO-WiFi\"",
"\"NOS-C876\"",
"\"MEO-45BE30\"",
"\"TP-LINK_AP_AF08\"",
"\"MEO-D68850\"",
"\"MEO-FCF0A0\"",
```

Utilizamos o filtro "wlan.fc.type_subtype == 8" e filtramos os diferentes SSIDs através de um programa simples que criamos.

11. Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request e probing response, simultaneamente.

O filtro pode ser “wlan.fc.type_subtype == 0x04 || wlan.fc.type_subtype == 0x05”

12. Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?



Request: Samsung como origem/transmissor e é transmitido em Broadcast.

Response: HitronTE como origem/transmissor e Samsung como destino/receiver.

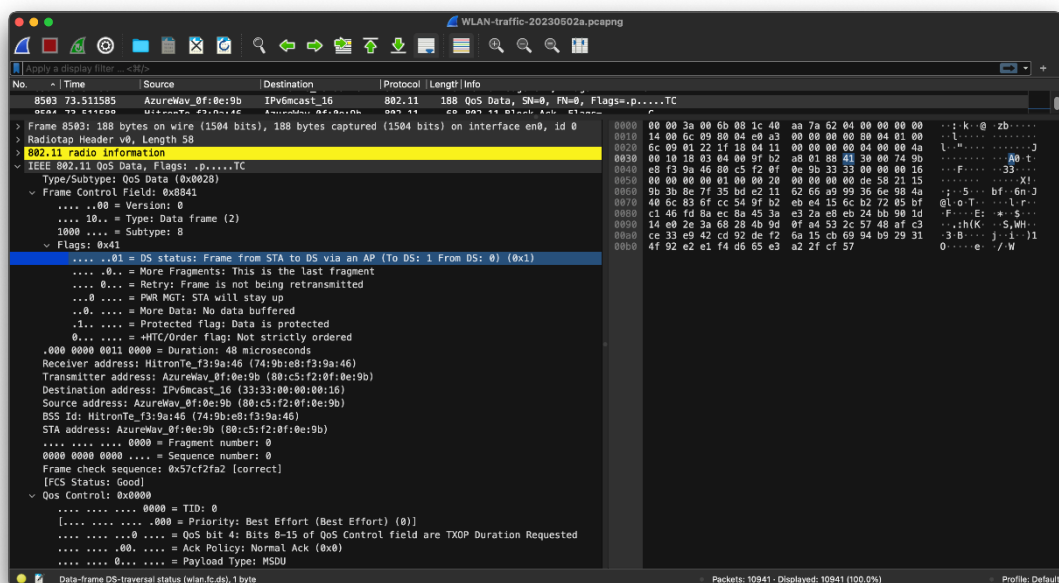
Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

8472	73.450730	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70 Authentication, SN=262, FN=0, Flags=.....C
8474	73.450775	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	70 Authentication, SN=1965, FN=0, Flags=.....C
8476	73.459546	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	164 Association Request, SN=263, FN=0, Flags=.....C, SSID="FlyingNet"
8478	73.459638	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	210 Association Response, SN=1966, FN=0, Flags=.....C

14) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

STA Probe request -> AP Probe response -> STA authentication -> AP authentication -> Association Request -> Association Response .

15) Considere a trama de dados nº8503. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?



Neste caso como o to_{DS} é 1, a direção vai do STA para o DS, nestas circunstâncias, vai para um AP que está ligado a outro dispositivo.

16) Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

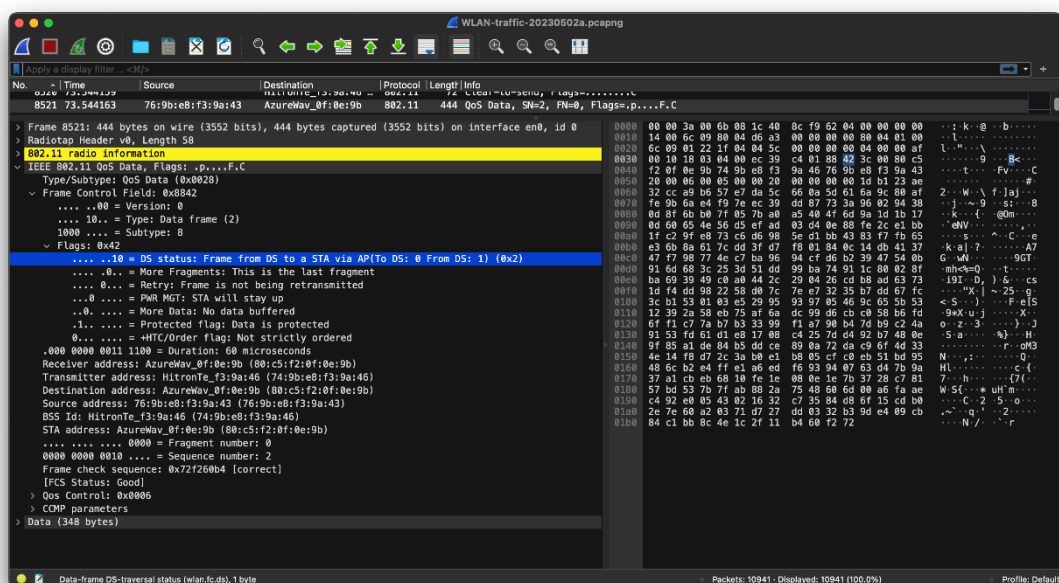
```
Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Destination address: IPv6mcast_16 (33:33:00:00:00:16)
Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
```

Endereço STA: 80:c5:f2:0f:0e:9b

Endereço AP: 74:9b:e8:f3:9a:46

Endereço DS: 33:33:00:00:00:16

17) Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?



Como o to DS é 0 e o from DS é 1, a direção é do DS para o STA.

```
Receiver address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Transmitter address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Destination address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Source address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
```

Endereço STA: 80:c5:f2:0f:0e:9b

Endereço AP: 74:9b:e8:f3:9a:46

Endereço DS: 76:9b:e8:f3:9a:46

18) Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar a razão de terem de existir (contrariamente ao que acontece numa rede Ethernet.)

Conseguimos identificar as três tramas de controlo; ACK, CTS e RTS. Essas 3 tramas de controlo são importantes de modo a evitar colisões, lidar com obstáculos, interferências e ajudam na mobilidade dos dispositivos.

19) O uso de tramas Request To Send e Clear To Send, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

Filtro usado:

wlan.fc.type_subtype == 0x1B || wlan.fc.type_subtype == 0x1C

```

> Frame 1779: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
v IEEE 802.11 Request-to-send, Flags: .....C
  Type/Subtype: Request-to-send (0x001b)
  v Frame Control Field: 0xb400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1011 .... = Subtype: 11
  v Flags: 0x00
    .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
    0... .... = +HTC/Order flag: Not strictly ordered
  .000 0000 1110 0110 = Duration: 230 microseconds
Receiver address: ce:90:6f:21:42:3a (ce:90:6f:21:42:3a)
Transmitter address: PTInovac_d6:88:50 (00:06:91:d6:88:50)
Frame check sequence: 0x4bc5f127 [correct]
[FCS Status: Good]

```

```

v IEEE 802.11 Clear-to-send, Flags: .....C
  Type/Subtype: Clear-to-send (0x001c)
  v Frame Control Field: 0xc400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1100 .... = Subtype: 12
  > Flags: 0x00
  .000 0111 1001 1000 = Duration: 1944 microseconds
Receiver address: ce:90:6f:21:42:3a (ce:90:6f:21:42:3a)
Frame check sequence: 0x0f713004 [correct]

```

Em ambas as imagens acima são tramas, a RTC e CTS, são tramas locais devido a ter o To Ds e o From Ds a 0.

Conclusão

Através deste trabalho conseguimos aprofundar os conhecimentos sobre as Redes sem Fios (Wi-Fi / IEEE 802.11) e o seu funcionamento. Através da captura, podemos observar o scanning passivo e ativo, o processo de associação e a transferência de dados

