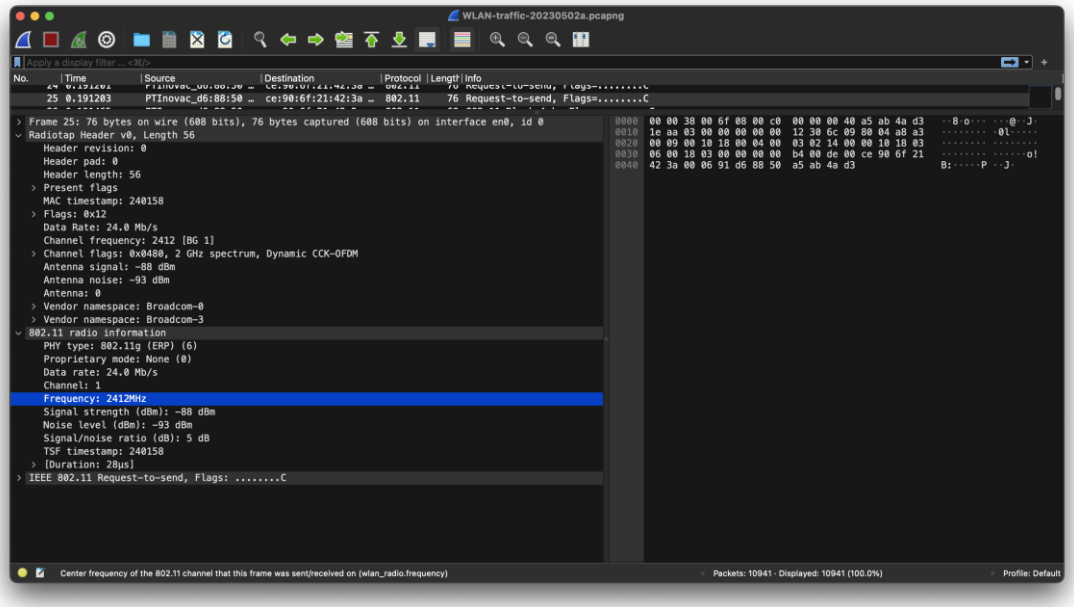
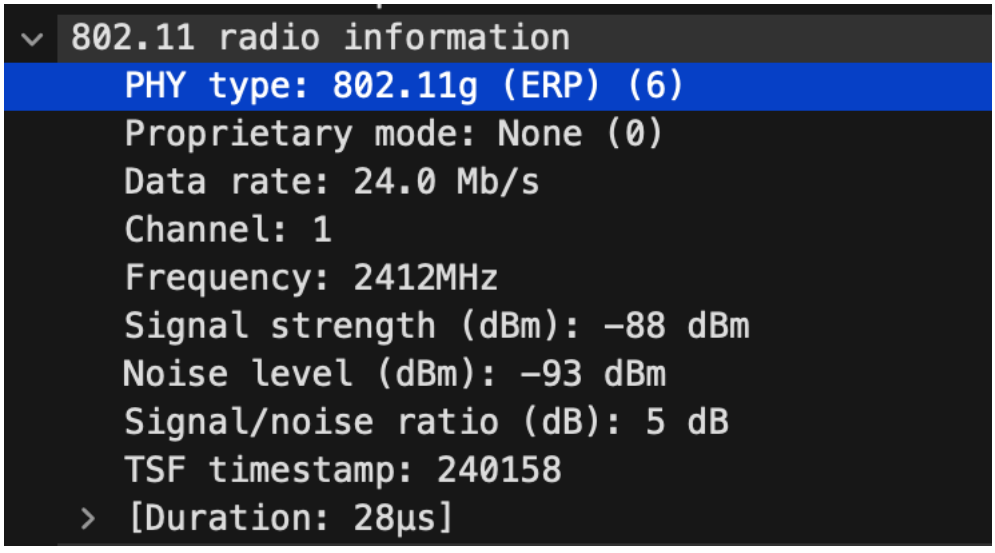
# 4. Redes sem Fio (Wi-Fi)

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



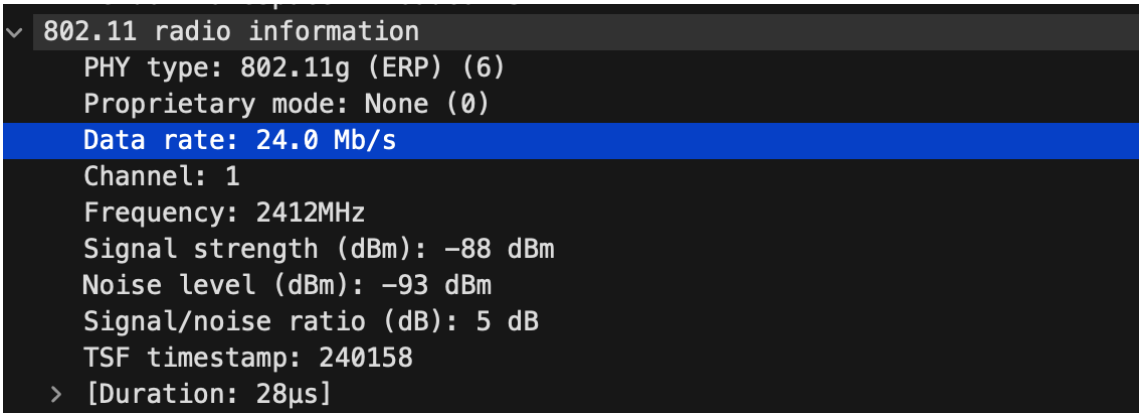

O espectro tem uma frequência de 2412MHz e pertence ao canal 1.

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



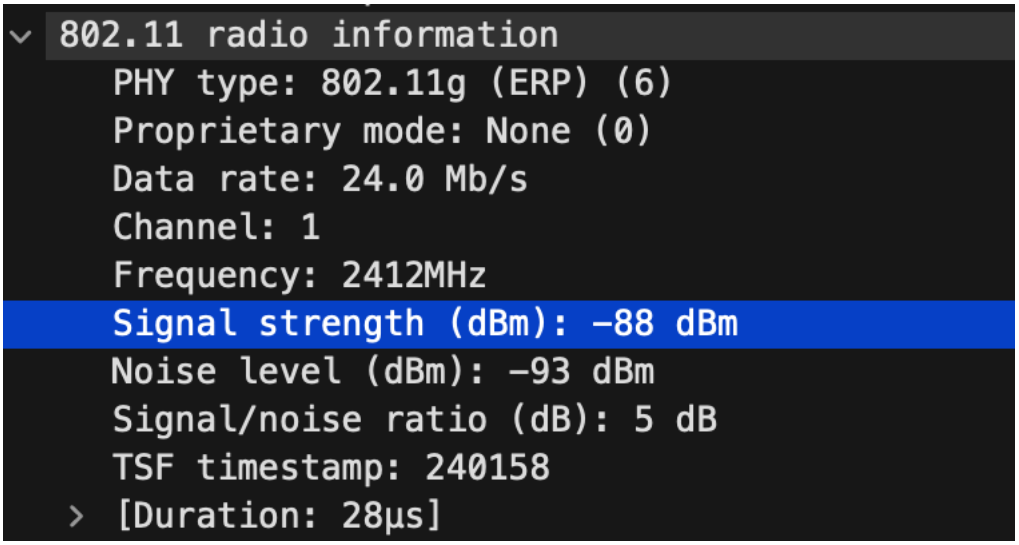

A versão da norma é 802.11g (ERP) (6).

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.**



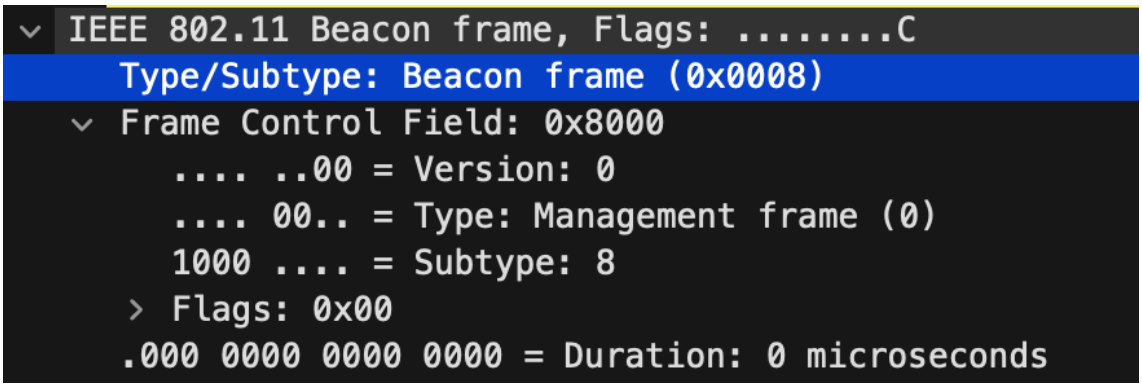

O débito de envio é de 24Mb/s e não corresponde ao débito máximo pois o débito máximo possível é de 54Mb/s.
Essa diferença deve-se ao facto de o ruído ser maior que o sinal.

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



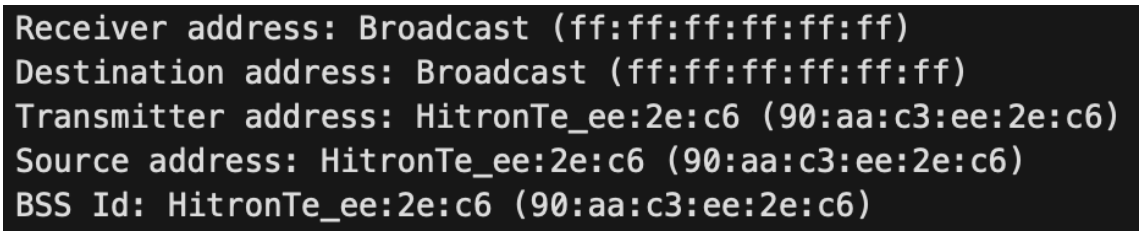

A força do sinal é de -88dBm e espera-se uma ligação com uma força não confiável.

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)?**



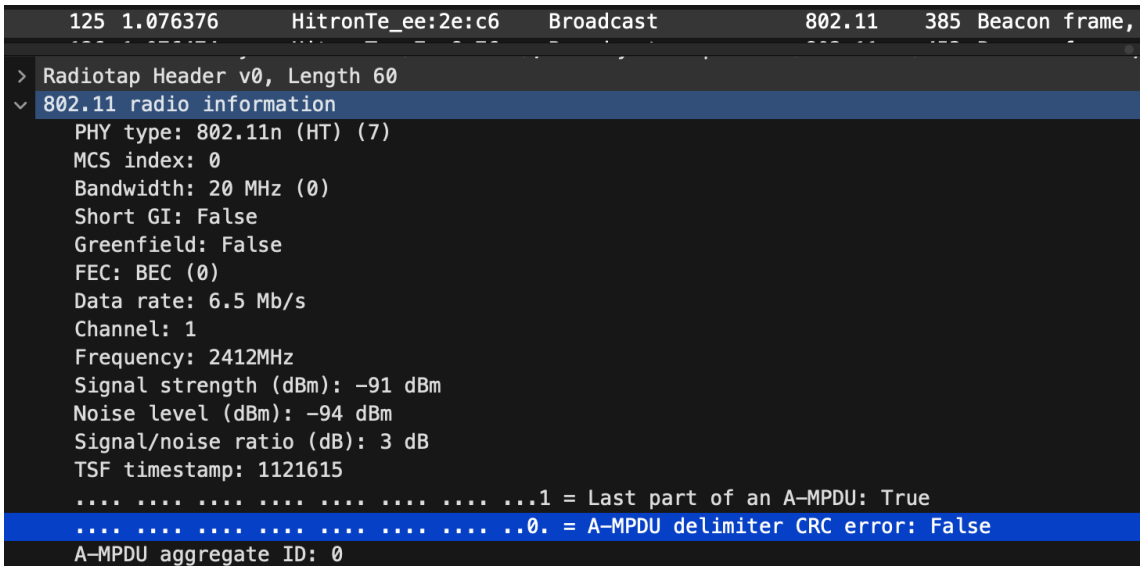

Estão especificados no Frame Control Field.

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




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.

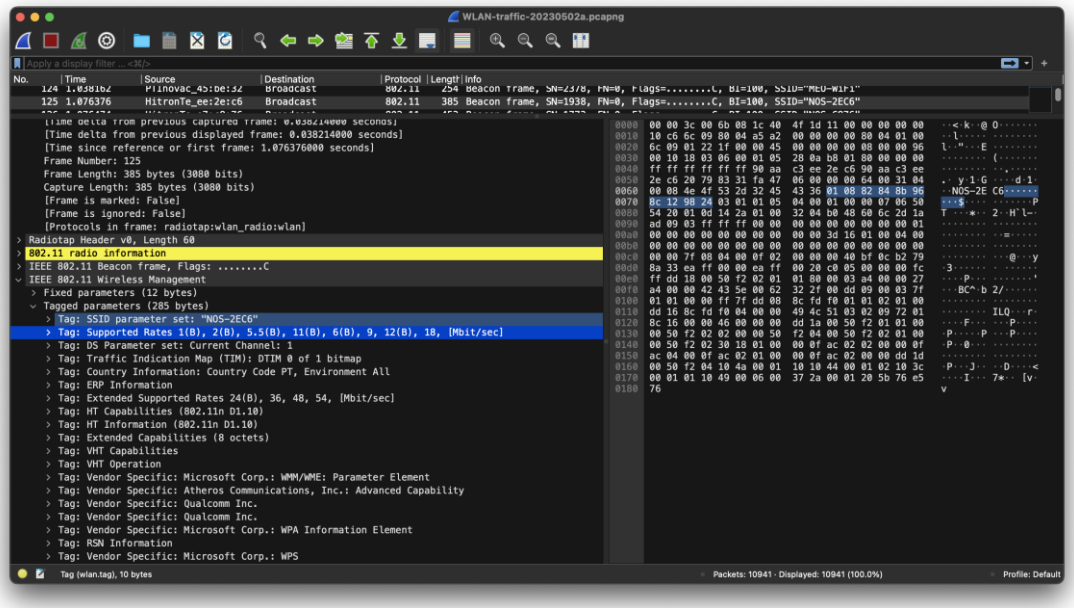
7. **Verifique se está a ser usado o método de deteção de erros (CRC). Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.**



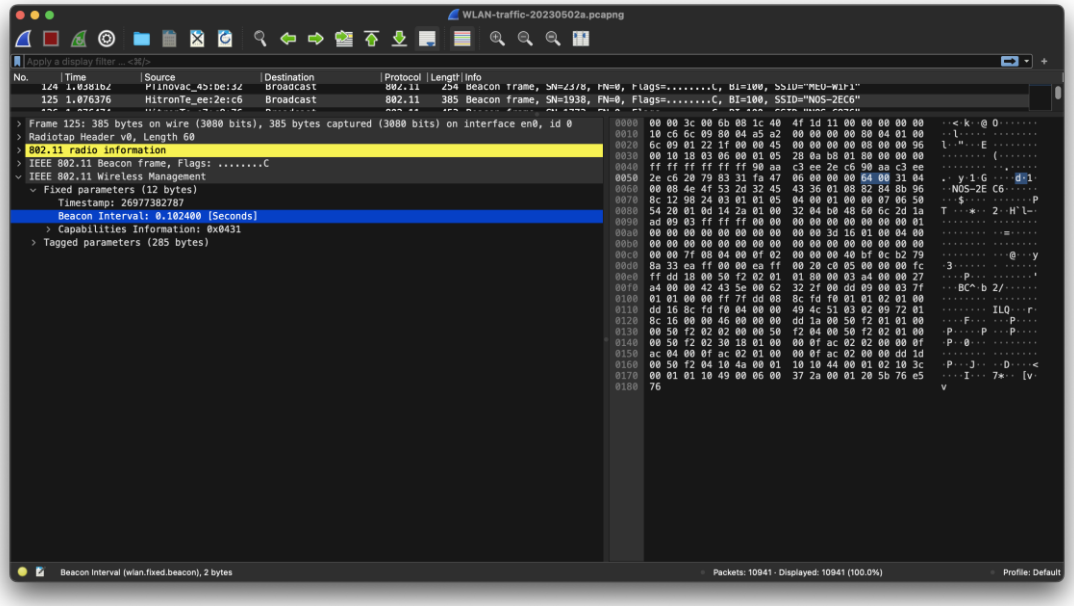

Está a ser usado o método CRC. O mesmo demonstrou que não foram encontrados erros com a flag False.

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. Explicite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).**

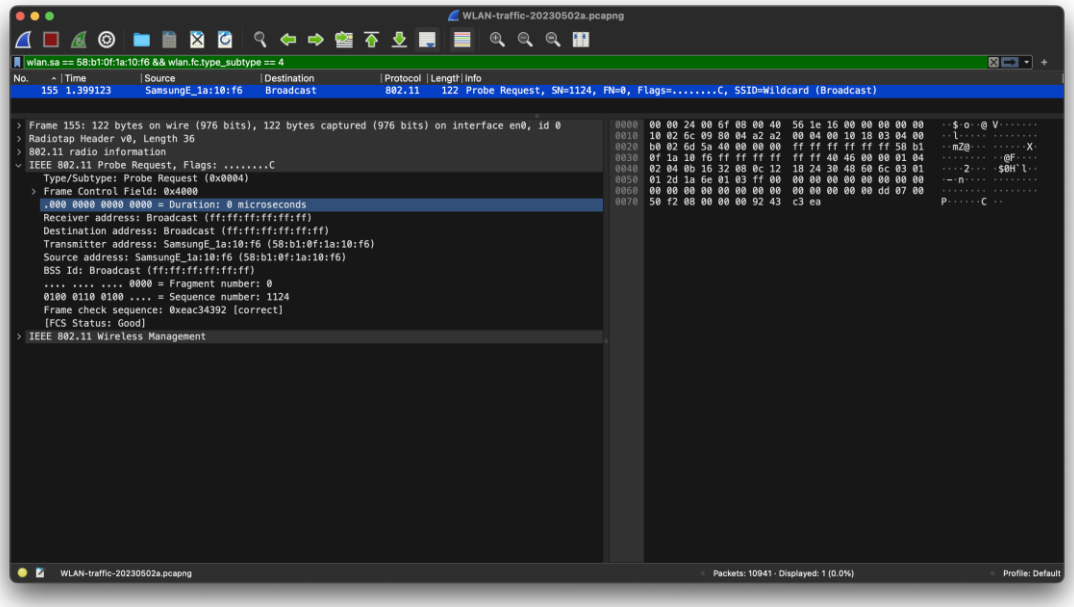
```
"\"FlyingNet\"",
"\"MEO-9BF2A0\"",
"\"Masmorra do Sexo\"",
"\"K6000 Plus\"",
"\"MEO-9E9BB0\"",
"\"NOS-2EC6\"",
"\"MEO-WiFi\"",
"\"NOS-C876\"",
"\"MEO-45BE30\"",
"\"TP-LINK_AP_AF08\"",
"\"MEO-D68850\"",
"\"MEO-FCF0A0\"",
```

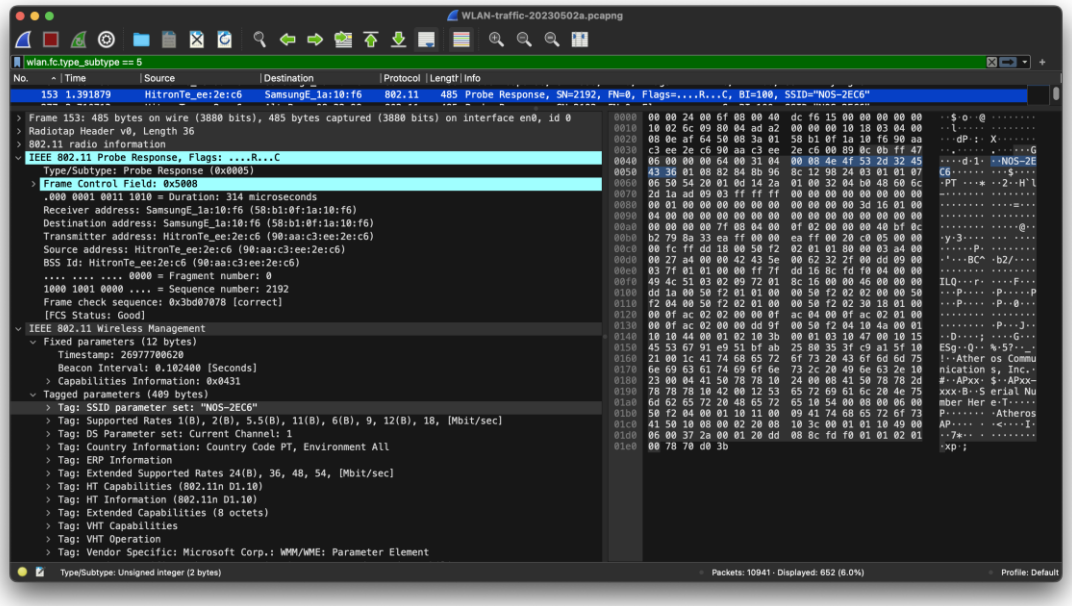
Utilizamos o filtro “wlan.fc.type_subtype == 8” e filtramos os diferentes SSIDs através de um programa simples que criamos.

**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.

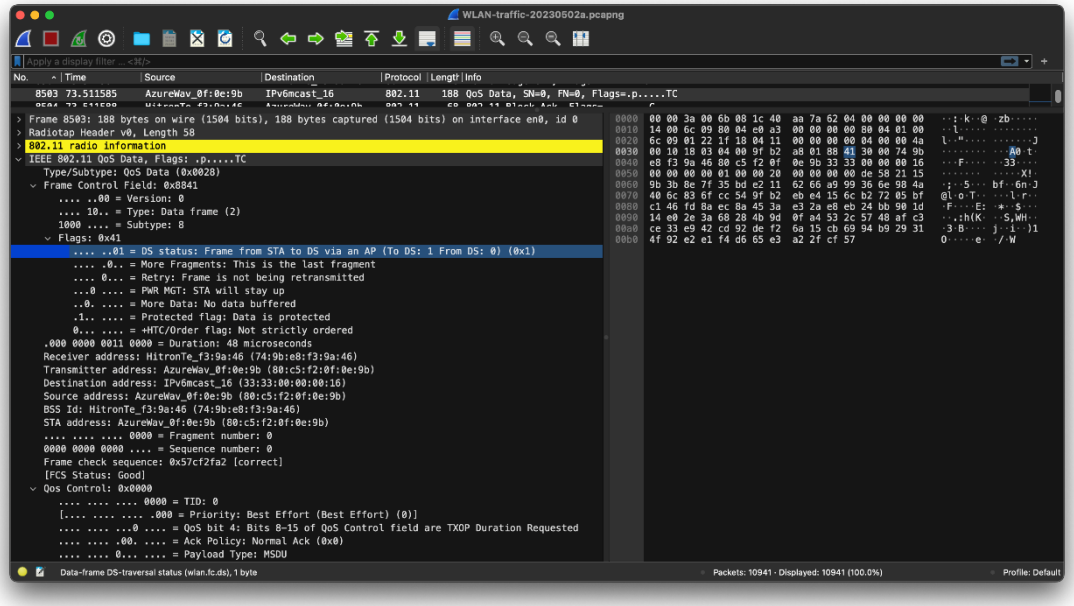
**Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.**

```
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 sequencia 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?**



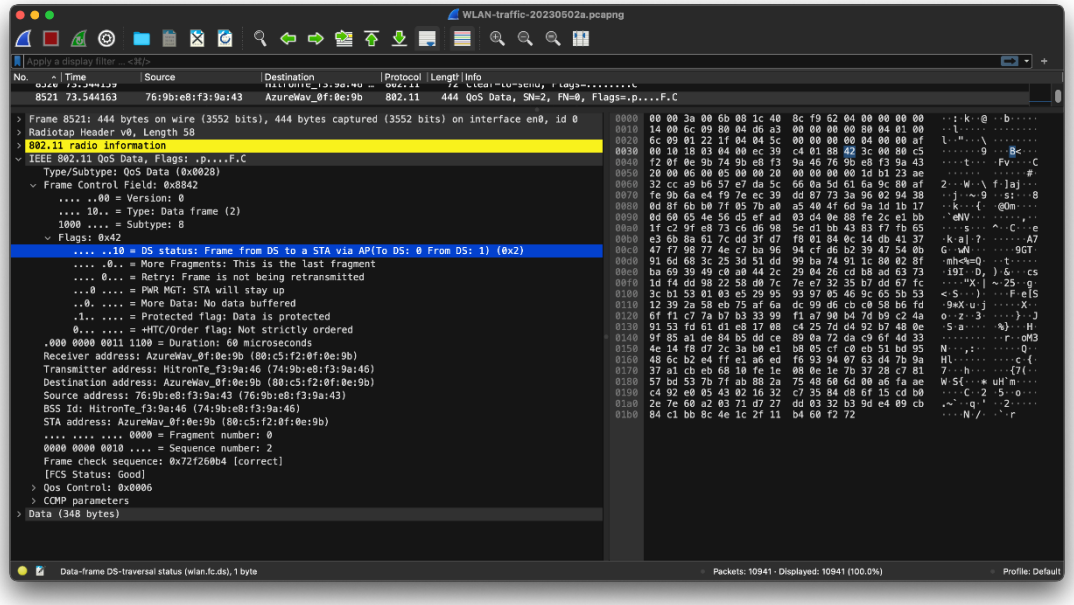
Neste caso como o to DS é 1, a direção vai do STA para o DS, nestas circunstâncias, vai para um AP que está ligado a outro dispositivo.

**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

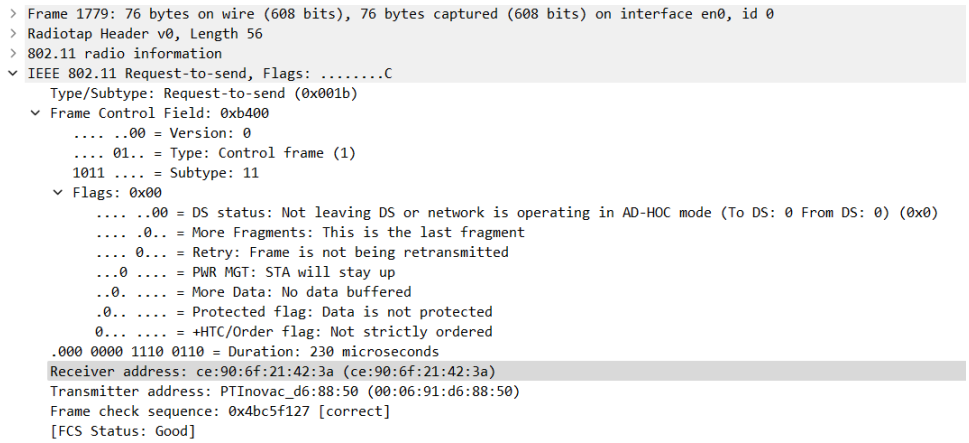
**18) Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar a razão de terem de existir (contrariamente ao que acontece numa rede Ethernet.)**

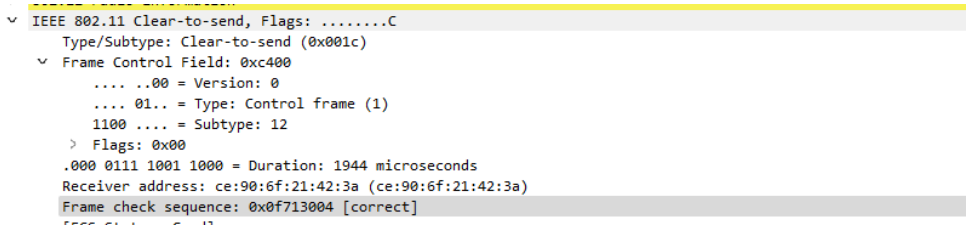
Conseguimos identificar as três tramas de controlo; ACK, CTS e RTS. Essas 3 tramas de controlo são importantes de modo a evitar colisões, lidar com obstáculos, interferências e ajudam na mobilidade dos dispositivos.

**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**




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 associaçao e a transferencia de dados