

TRABALHO PRÁTICO 4

Redes de Computadores

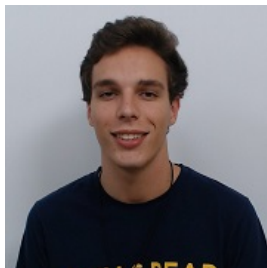
Grupo 14



Inês Bastos A89522



João Freitas A83782



João Félix A89460

Dezembro de 2020

Conteúdo

1	Questões e Respostas	2
2	Conclusão	10

Capítulo 1

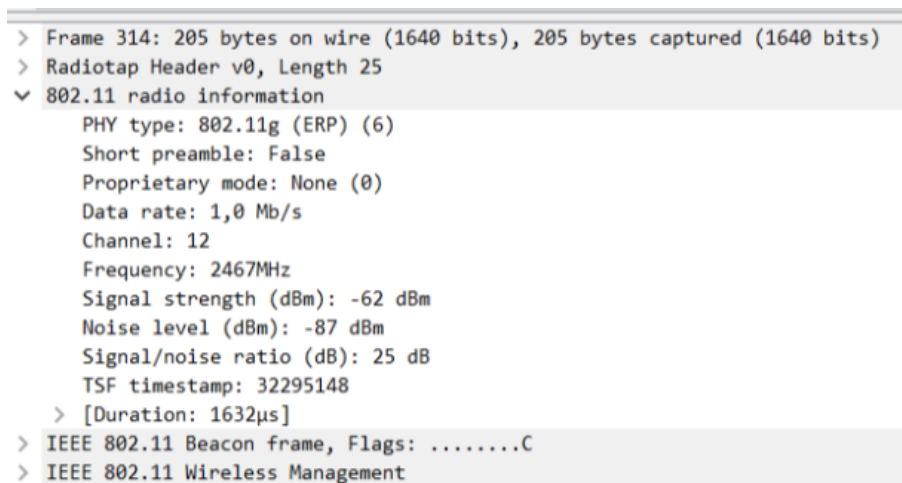
Questões e Respostas

4. Acesso Rápido

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (radio information), para além dos bytes correspondentes a tramas 802.11.

Para a trama correspondente 3XX em que XX corresponde ao seu número de TurnoGrupo (e.g., 11),

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



```
> Frame 314: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 25
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -62 dBm
  Noise level (dBm): -87 dBm
  Signal/noise ratio (dB): 25 dB
  TSF timestamp: 32295148
  > [Duration: 1632µs]
> IEEE 802.11 Beacon frame, Flags: .....C
> IEEE 802.11 Wireless Management
```

Figura 1.1

Frequência: 2467MHz.

Canal: 12.

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

A versão da norma IEEE 802.11 que está a ser usada é a 802.11g como podemos observar na figura 1.1 no campo PHY type : 802.11g .

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

Data rate : 1.0 Mb /s

Como podemos observar na figura 1.1, a trama 314 foi enviada com um Data rate de 1.0Mb/s, como a norma IEEE802.11g tem um débito máximo de 54 Mbps, sabemos que a interface Wifi não está a operar no seu débito máximo. Isto acontece pois esta interface trabalha com o menor débito possível de forma a garantir que o beacon chega a todos os hosts.

5. Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (WiFi). Para a captura de tramas disponibilizada, e considerando XX o seu nº de grupo, responda às seguintes questões:

4) Selecione uma trama beacon (e.g., trama 10XX). Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. 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
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    .... .... 0000 = Fragment number: 0
    1011 0001 1111 .... = Sequence number: 2847
    Frame check sequence: 0xbd4d138a [unverified]
    [FCS Status: Unverified]
  ▼ IEEE 802.11 Wireless Management
    > Fixed parameters (12 bytes)

```

Figura 1.2

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon

Figura 1.3

Selecionamos a trama 1014 e fomos ao Frame Control Field onde observamos que:

Type : 00

Subtype : 1000

Type Description : Management

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

```
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  v Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  > Flags: 0x00
    .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: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  .... .... 0000 = Fragment number: 0
  1011 0001 1111 .... = Sequence number: 2847
  Frame check sequence: 0xbd4d138a [unverified]
  [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
```

Figura 1.4

MAC ADDRESS

Transmitter: (bc:14:01:af:b1:98)

Source: (bc:14:01:af:b1:98)

Destination: (ff:ff:ff:ff:ff:ff)

Estamos numa situação em que um o transmitter está a enviar o beacon para o meio, por isso o transmitter e source mac addresses são iguais, já o adress destination é o de Broadcast.

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

```
.0.. .... = Delayed Block Ack: Not Implemented
0... .... = Immediate Block Ack: Not Implemented
▼ Tagged parameters (231 bytes)
  > Tag: SSID parameter set: FlyingNet
  > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
  > Tag: DS Parameter set: Current Channel: 12
  > Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
  > Tag: Vendor Specific: Microsoft Corp.: WPS
  > Tag: Traffic Indication Map (TIM): DTIM 1 of 3 bitmap
  > Tag: ERP Information
  > Tag: HT Capabilities (802.11n D1.10)
  > Tag: HT Information (802.11n D1.10)
  > Tag: Extended Capabilities (1 octet)
  > Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
  > Tag: RSN Information
  > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  > Tag: QBSS Load Element 802.11e CCA Version
  > Tag: Vendor Specific: Ralink Technology, Corp.
```

Figura 1.5

Os débitos base suportados são : 1(B), 2(B), 5,5(B), 11(B), 9 (Mbit/s), 18 (Mbit/s), 36 (Mbit/sec), 54 (Mbit/s).

Os débitos adicionais (Extended Supported Rates) são: 6(B), 12(B), 24(B), 48 (Mbit/s).

7) Qual o intervalo de tempo previsto entre tramas beacon consecutivas? (nota: este valor é anunciado na própria trama beacon). Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada? Tente explicar porquê.

▼ IEEE 802.11 Wireless Management

▼ Fixed parameters (12 bytes)

Timestamp: 1149709722087

Beacon Interval: 0,102400 [Seconds]

> Capabilities Information: 0x0c31

▼ Tagged parameters (231 bytes)

> Tag: SSID parameter set: FlyingNet

▼ IEEE 802.11 Wireless Management

▼ Fixed parameters (12 bytes)

Timestamp: 1149709724465

Beacon Interval: 0,102400 [Seconds]

> Capabilities Information: 0x0c21

▼ Tagged parameters (140 bytes)

> Tag: SSID parameter set: NOS_WIFI_Fon

O intervalo de tempo previsto entre tramas beacon consecutivas é 0.120400 segundos. Como podemos verificar na figura abaixo, os estes tempos previstos não se verificam. Isto pode dever-se a vários fatores como a distância entre os dispositivos de destino e envio, o congestionamento da da rede local que está a ser utilizada na captura, a falta de precisão de um AP, entre outros.

Time	Source	Destination	Protocol	Length	Info
1006 0.100745	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2839, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1007 0.001632	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2840, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1008 0.100790	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2841, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1009 0.001530	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2842, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1010 0.100733	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2843, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1011 0.001742	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2844, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1012 0.100770	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2845, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1013 0.001548	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2846, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1014 0.100858	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2847, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1015 0.001539	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2848, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1016 0.100867	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2849, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1017 0.001648	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2850, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1018 0.100770	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2851, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1019 0.001613	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2852, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1020 0.100752	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2853, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1021 0.001571	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2854, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1022 0.100767	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SII=2855, FH=0, Flags=.....C, BI=100, SSID=FlyingNet
1023 0.001708	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SII=2856, FH=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

Figura 1.7

8) 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).

Obtivemos os SSIDs que operam na vizinhança da estação (FlyingNet e a NOS_WIFI_Fon) aplicando o filtro `wlan[0] == 0x80` ao tráfego capturado. Em seguida verificamos que os SSIDs acima mencionados são os únicos que enviaram tramas de anúncio.

9) Verifique se está a ser usado o método de deteção de erros (CRC). Justifique.

Use o filtro:

```
(wlan.fc.type_subtype == 0x08)&&(wlan.fcs.status == bad)
```

Que conclui?

Justifique o porquê de usar deteção de erros em redes sem fios.

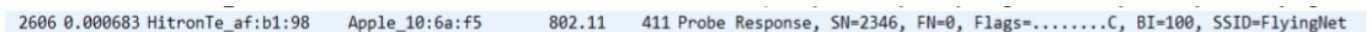
No trace disponibilizado foi também registado scanning ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.

10) Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente.

```
wlan.fc.type == 0 && (wlan.fc.subtype == 4 || wlan.fc.subtype == 5)
```

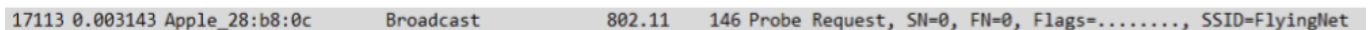
11) Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

Uma vez que o endereço MAC de destino da trama é igual ao endereço MAC de origem da outra trama, significa que se trata de um probing request e probing response.



2606 0.000683 HitronTe_af:b1:98 Apple_10:6a:f5 802.11 411 Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 1.8



17113 0.003143 Apple_28:b8:0c Broadcast 802.11 146 Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet

Figura 1.9

6. Processo de Associação

Numa rede WiFi estruturada, um host deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para a sequência de tramas capturada:

12) Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

4692 83.663250	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	59 Authentication, SN=67, FN=0, Flags=.....C
4694 83.663681	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	59 Authentication, SN=2439, FN=0, Flags=.....C
4696 83.665976	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	153 Association Request, SN=68, FN=0, Flags=.....C, SSID=FlyingNet
4698 83.678873	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225 Association Response, SN=2440, FN=0, Flags=.....C

Figura 1.10: Rede sem fios.

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

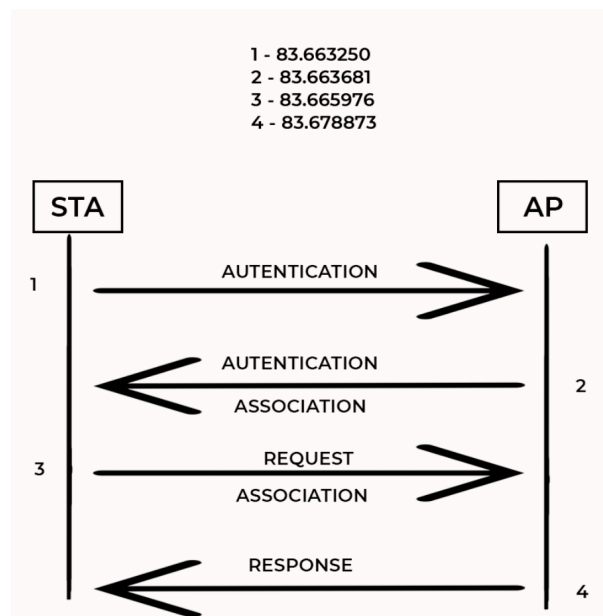


Figura 1.11: Diagrama rede sem fios.

7. Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e de controlo da transferência desses mesmos dados.

14) Considere a trama de dados nº455. 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?

```
▼ Frame Control Field: 0x8842
  .... ..00 = Version: 0
  .... 10.. = Type: Data frame (2)
  1000 .... = Subtype: 8
  ▼ Flags: 0x42
    .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
    .... .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
    .1.. .... = Protected flag: Data is protected
    0... .... = Order flag: Not strictly ordered
  .000 0000 0010 0100 = Duration: 36 microseconds
```

Figura 1.12

Olhando para a figura 1.8 reparamos que o pacote está a entrar num ambiente wireless vindo de DS. Isto vê-se olhando para o campo DS status onde reparamos nos valores: To DS: 0 e From DS: 1.

15) Para a trama de dados nº455, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao host sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição?

```
Receiver address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Destination address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
```

Figura 1.13

Quanto à correspondência dos endereços, o Destination address corresponde ao STA, o BSS Id address corresponde ao AP e o Source address corresponde ao router de acesso.

16) Como interpreta a trama nº457 face à sua direccionalidade e endereçamento MAC?

```

  Frame Control Field: 0x8841
    .... 00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  Flags: 0x41
    .... 01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
    .... 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
    .1.. .... = Protected flag: Data is protected
    0... .... = Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds

```

Figura 1.14

Ao contrário do que aconteceu na trama nº 455, esta trama tem direccionalidade para DS. Isto vê-se olhando para o campo DS status onde reparamos nos valores: To DS: 1 e From DS: 0.

Quanto à correspondência dos endereços, o Destination address corresponde ao router de acesso, o BSS id address corresponde ao STA e o Source address corresponde ao AP.

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

455 18.536644	HitronTe_af:b1:98	Apple_71:41:a1	802.11	226 QoS Data, SN=276, FN=0, Flags=.p....F.C
456 18.536653		HitronTe_af:b1:98 (...)	802.11	39 Acknowledgement, Flags=.....C
457 18.539762	Apple_71:41:a1	HitronTe_af:b1:98	802.11	178 QoS Data, SN=1209, FN=0, Flags=.p....TC
458 18.540043		Apple_71:41:a1 (d8:...)	802.11	39 Acknowledgement, Flags=.....C

Figura 1.15

Porque existem grandes possibilidades de falha na rede, tramas de controlo são enviadas para verificar se outras tramas enviadas chegaram ao destino.

18) 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.

No exemplo anterior esse tipo de tramas não foram utilizados, apenas tramas ACK no entanto ao longo do histórico de tramas fornecido para realização deste trabalho elas aparecem.

Eis um exemplo onde podemos ver tramas CTS (Clear To Send), RTS (Request To Send) e ainda também mais uma vez ACK (Acknowledgement)

718 27.138490	HitronTe_af:b1:98 (...)	Apple_10:6a:f5 (64:...)	802.11	45 Request-to-send, Flags=.....C
719 27.138558		HitronTe_af:b1:98 (...)	802.11	39 Clear-to-send, Flags=.....C
720 27.138613	HitronTe_af:b1:96	Apple_10:6a:f5	802.11	146 QoS Data, SN=842, FN=0, Flags=.p....F.C
721 27.138666	Apple_10:6a:f5 (64:...)	HitronTe_af:b1:98 (...)	802.11	57 802.11 Block Ack, Flags=.....C
722 27.154862	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53 Null function (No data), SN=2507, FN=0, Flags=...P...TC
723 27.154880		Apple_10:6a:f5 (64:...)	802.11	39 Acknowledgement, Flags=.....C

Figura 1.16

Capítulo 2

Conclusão

Concluída a realização do trabalho prático número 4, os conhecimentos adquiridos ao longo das aulas foram reforçados e melhorados.

A elaboração deste trabalho apresentou, pela primeira vez, o conceito de Redes Wireless numa fase prática, sendo que, ajudou a consolidar a parte teórica que tem vindo a ser abordada ao longo das aulas. Vários conceitos como , por exemplo, tipos e subtipos de tramas, STA's, AP's e direcionalidade de tramas foram trabalhados e recordados ao longo das duas aulas que foram dadas para a realização do trabalho retratado.

Concluindo, deste trabalho, a parte que achámos mais interessante foi o facto de podermos ver no Wireshark um histórico de tramas de gestão IEEE 802.11, e de que forma elas se distinguem das tramas que temos visto nos trabalhos práticos anteriores.