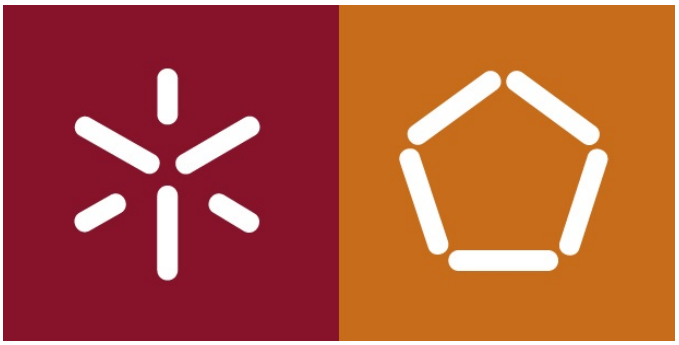
Universidade do Minho

Mestrado Integrado em Engenharia Informática



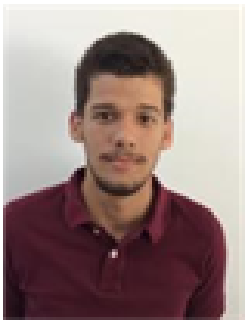
Redes de Computadores

Relatório do Trabalho Prático 4

Redes Sem Fios (802.11)

Grupo 1

Adriana Meireles
A82582



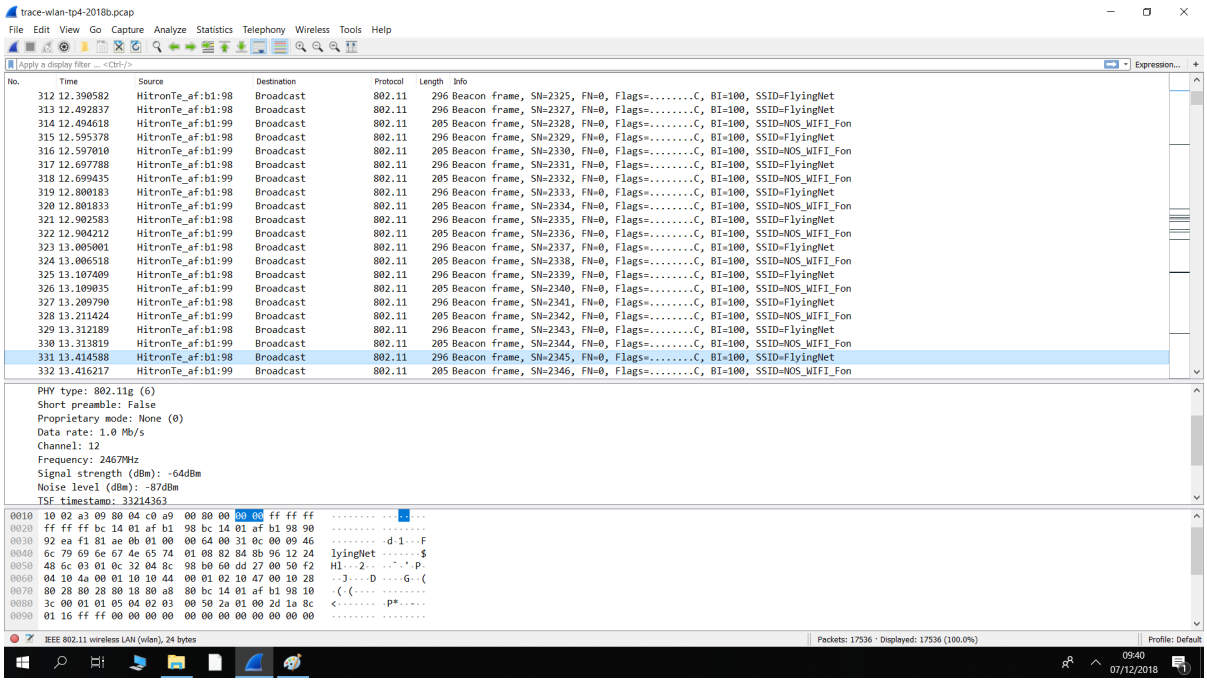
Nuno Silva
A78156

Shahzod Yusupov
A82617

March 22, 2020

Questões e Respostas

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



Está a operar na frequência de 2467 MHz e corresponde ao canal 12.

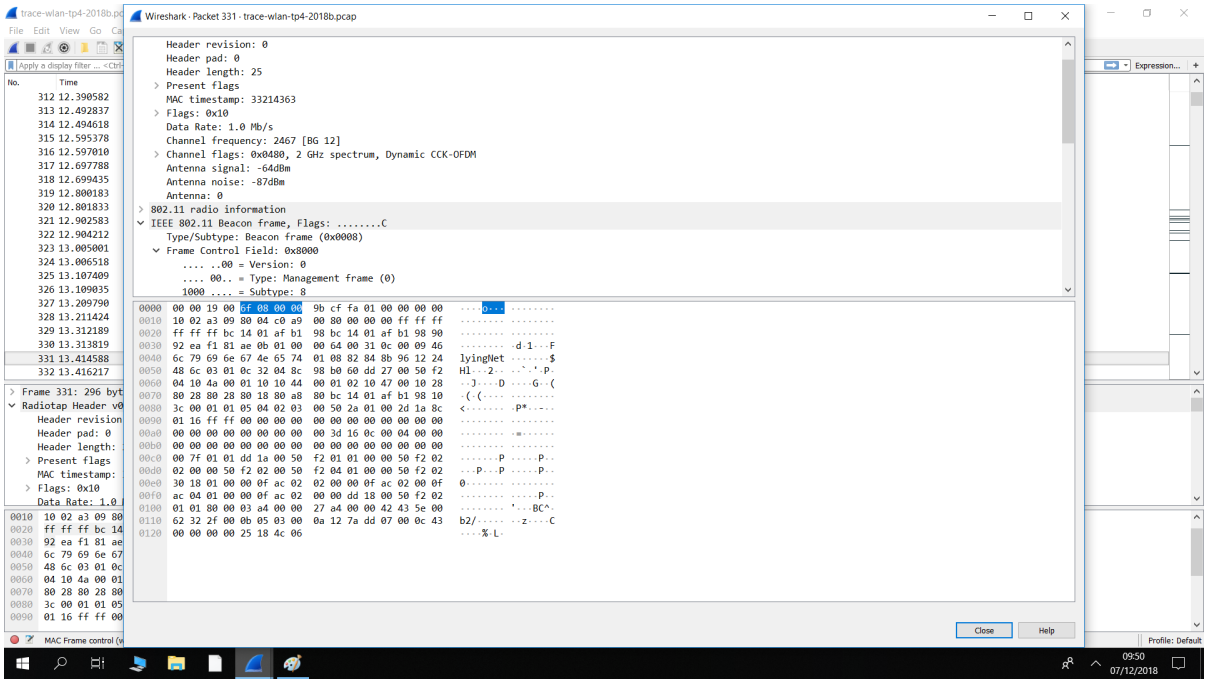
2) Identifique a versão da norma IEEE 802.11 que está a ser usada.

Está a ser usada a versão 802.11g

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

A trama foi enviada a um débito de 1.0 Mb/s, não sendo este o débito máximo que a interface WIfi pode operar, pois na versão 802.11g o débito máximo corresponde a 54 Mb/s.

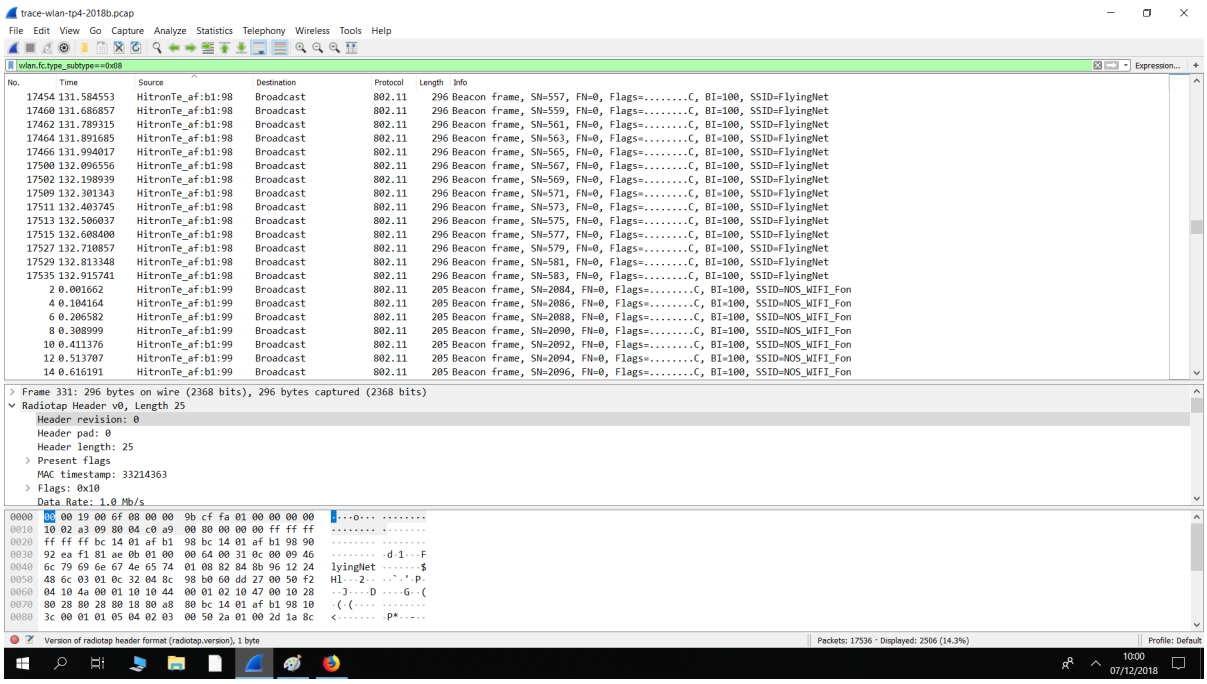
4) Selecione uma *trama beacon* (e.g., a trama 3XX). Esta trama pertence a que tipo de tramas 802.11 ? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?



Esta trama pertence ao tipo de tramas de gestão. O valor do identificador tipo é 0 e do subtipo 8 e estão especificados no byte 25 do cabeçalho da trama.

5) Liste dos os SSIDs dos APs (*Access Points*) que estão a operar na vizinhança da STA de captura? Explicite o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização apropriado (tomando como base a resposta a alínea anterior) que lhe permita obter a listagem pretendida.

Os Access Points que estão a operar na vizinhancça da STA de captura são os que têm os SSIDs de FlyingNet e NOS_WIFI_ZON. Para a obtenção destes SSIDs apilicou-se um filtro que mostrasse apenas as tramas beacon, ou seja que têm o campo subtype a 8. Após isso, ordenou-se as Sources por ordem alfabética



6) Verifique se está a ser usado o método de detecção de erros(CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique o porquê de usar detecção de erros neste tipo de redes locais.

Após termos verificado o campo Frame check sequence para uma trama de cada SSID apercebemo-nos que o método de detecção de erros está a ser usado, no entanto, nem todas as tramas são recebidas corretamente (sem erros), pois o campo FCS, em algumas tramas aparece como incorreto, indicando posteriormente qual devia ser o valor deste campo.Ao contrário das redes cabeladas, as redes sem fios têm maior probabilidade de haver colisões e erros nas tramas daí a necessidade de deteção de erros.

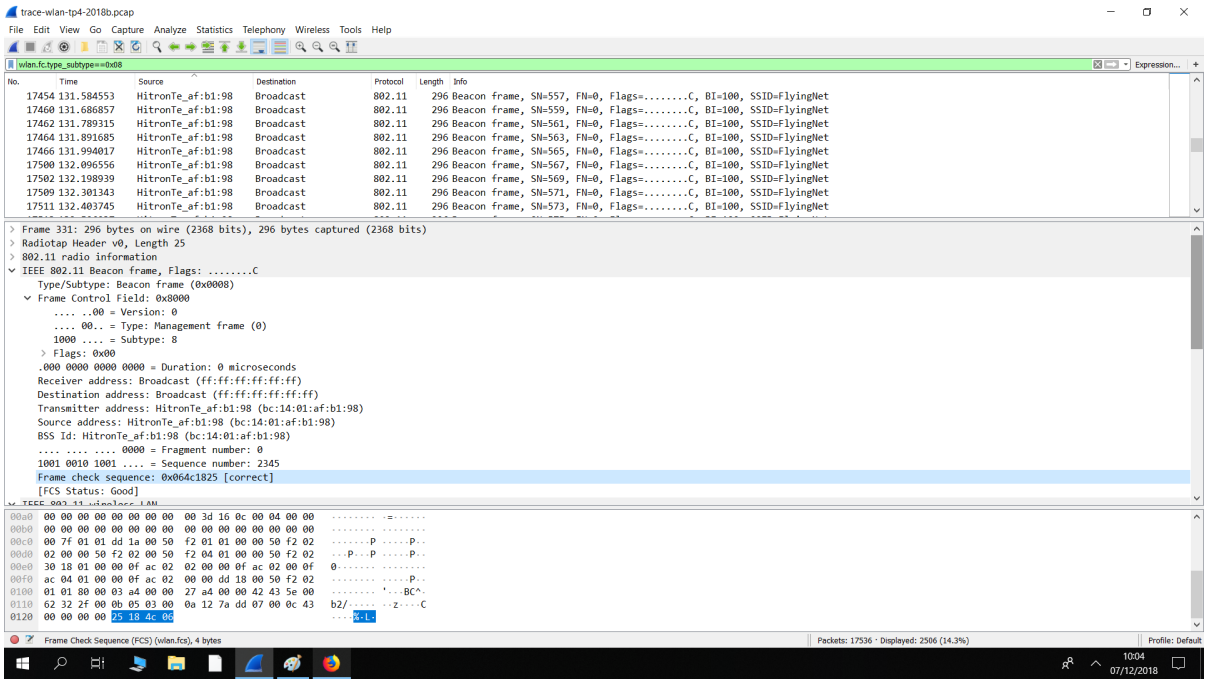


Figure 1: Trama sem erros

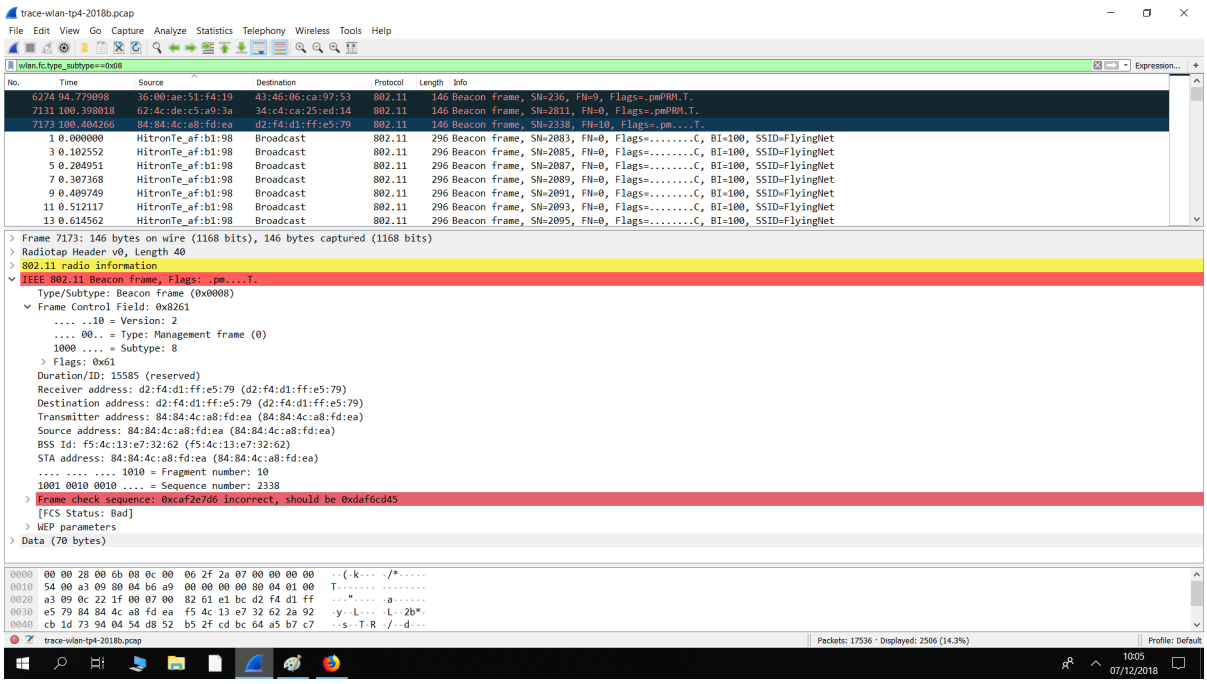


Figure 2: Trama com erros

7) Para dois dos APs identificados, indique qual é o intervalo de tempo previsto entre tramas *beacon* consecutivas? (Nota: este valor é anunciado na própria trama *beacon*). Na prática, a periocidade de tramas *beacon* é verificada? Tente explicar porquê.

Tanto para o AP Flying _Net como NOS_wifi, o intervalo de tempo previsto é de aproximadamente 0.102400 segundos. Para ambos os APs, este tempo não é exatamente o verificado, mas o valor é muito próximo porque o tráfego não é muito elevado.Caso fosse o verificado, o valor prático seria muito maior.

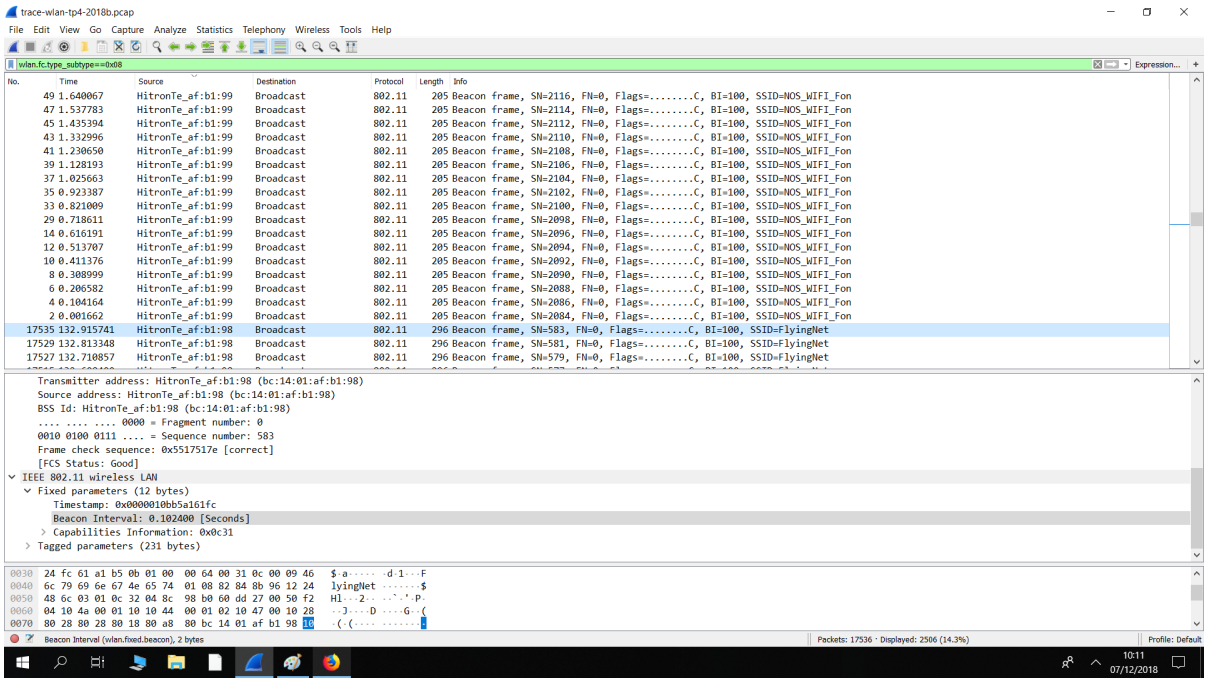


Figure 3: Intervalo de tempo do AP com SSID Flying-net

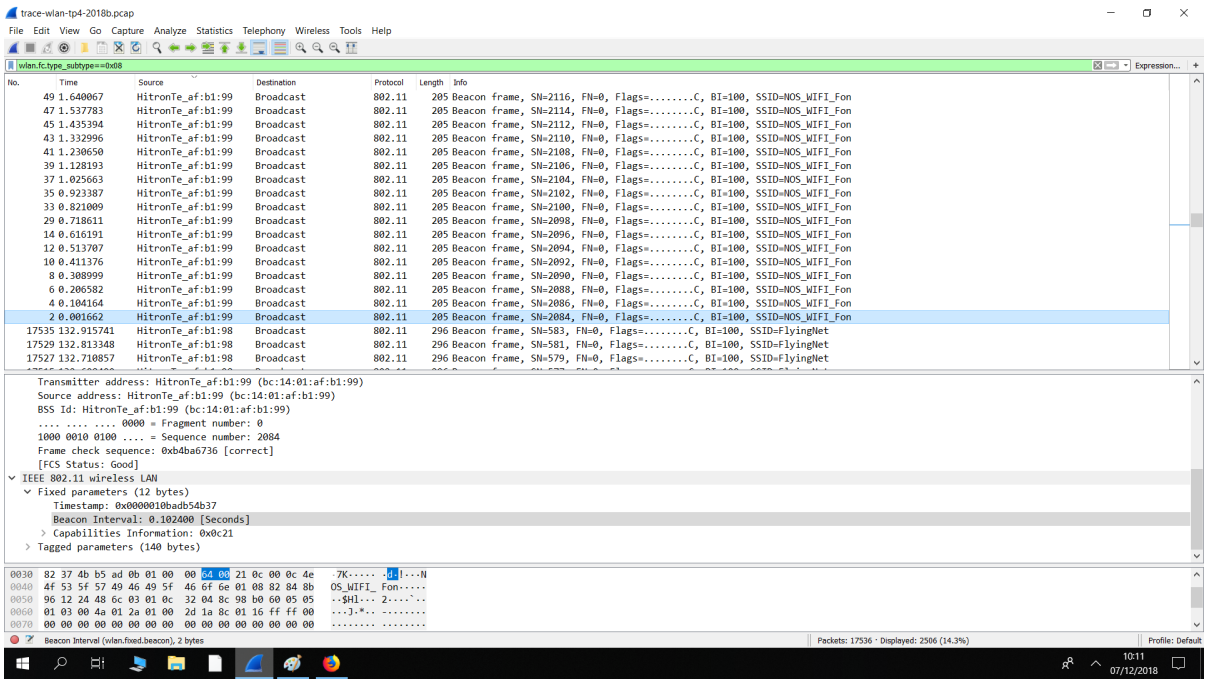


Figure 4: Intervalo de tempo do AP com SSID NOS-wifi

8) Identifique e registe todos os endereços MAC usados nas tramas *beacon* enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11, podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

Para os campos *Receiver address* e *Destination Adress* dos dois SSIDs existentes o endereço MAC é sempre o endereço ff:ff:ff:ff:ff:ff (Broadcast). Para os restantes SSIDs, os campos *Transmiter addresse* *Source Address* são iguais para cada SSID. Para o SSID NOS_wifi, o *Transmitter adress* é bc:14:01:af:b1:99(assim como o *Source Address* e para o SSID Flying_net é bc:14:01:af:b1:98(assim como o respetivo *Source Address*)

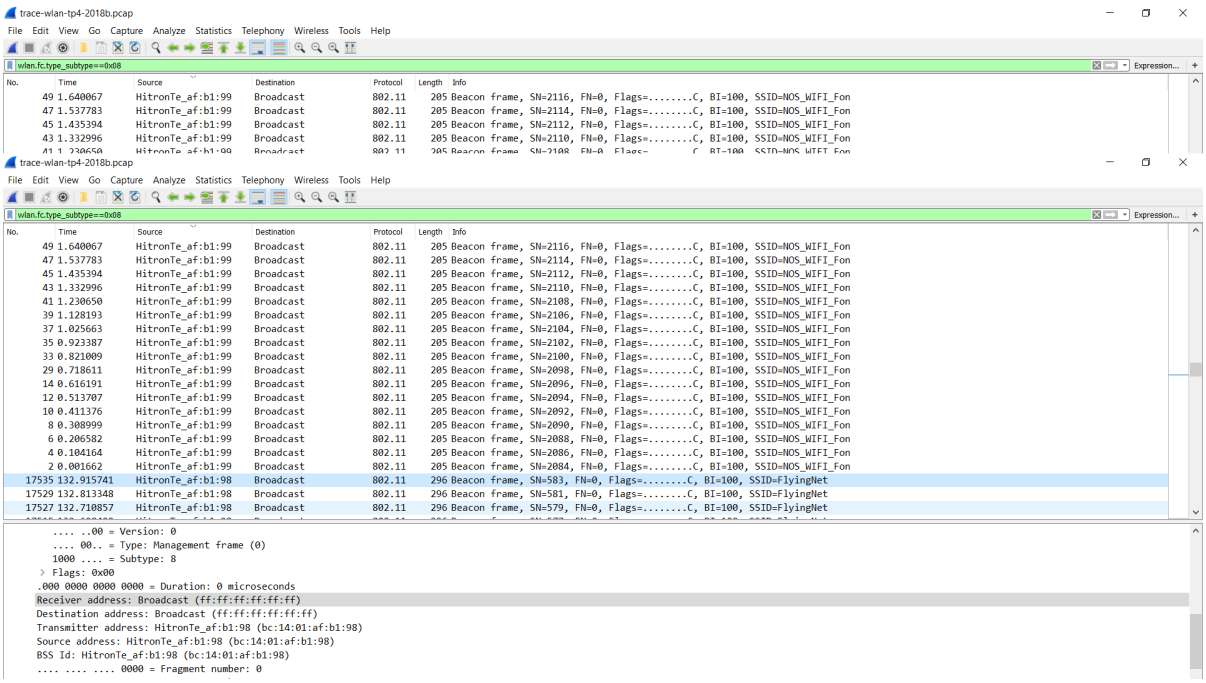


Figure 5: Endereços MAC do AP com SSID Flying-net

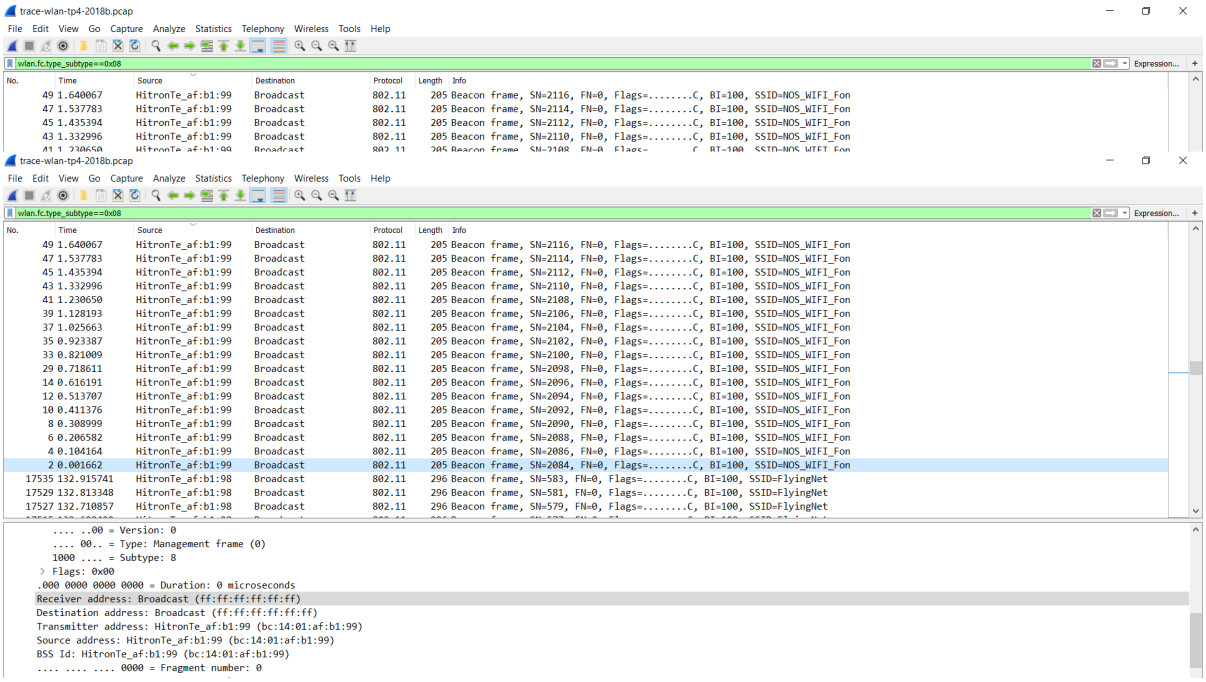


Figure 6: Endereços MAC do AP com SSID NOS-wifi

9) As tramas *beacon* anunciam que o AP pode suportar vários débitos de base assim como vários "*extended supported rates*". *Indique quais são esses débitos?*

Tanto o AP com SSID NOS_wifi como o AP como SSID Flying_net conseguem suportar débitos de base de 1 até 54 Mbs e *"extended supported rates"* de 6 até 48 Mbs.

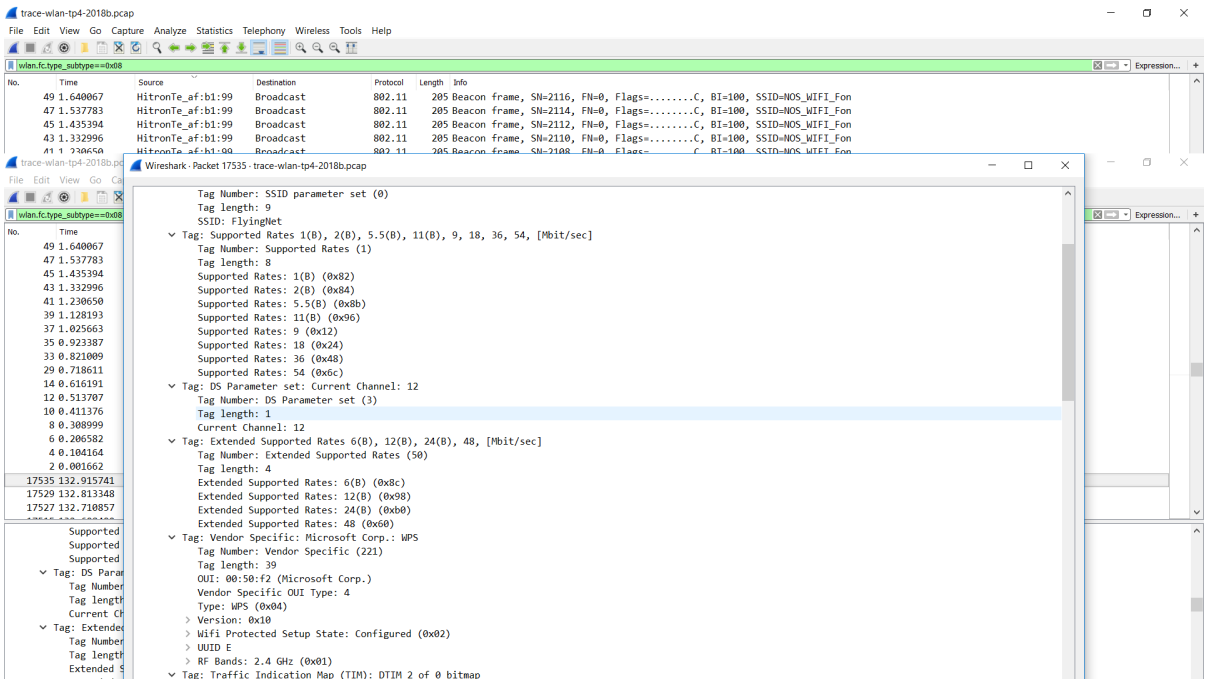


Figure 7: Débito de Base e Extended supported Rate do AP com SSID Flying-net

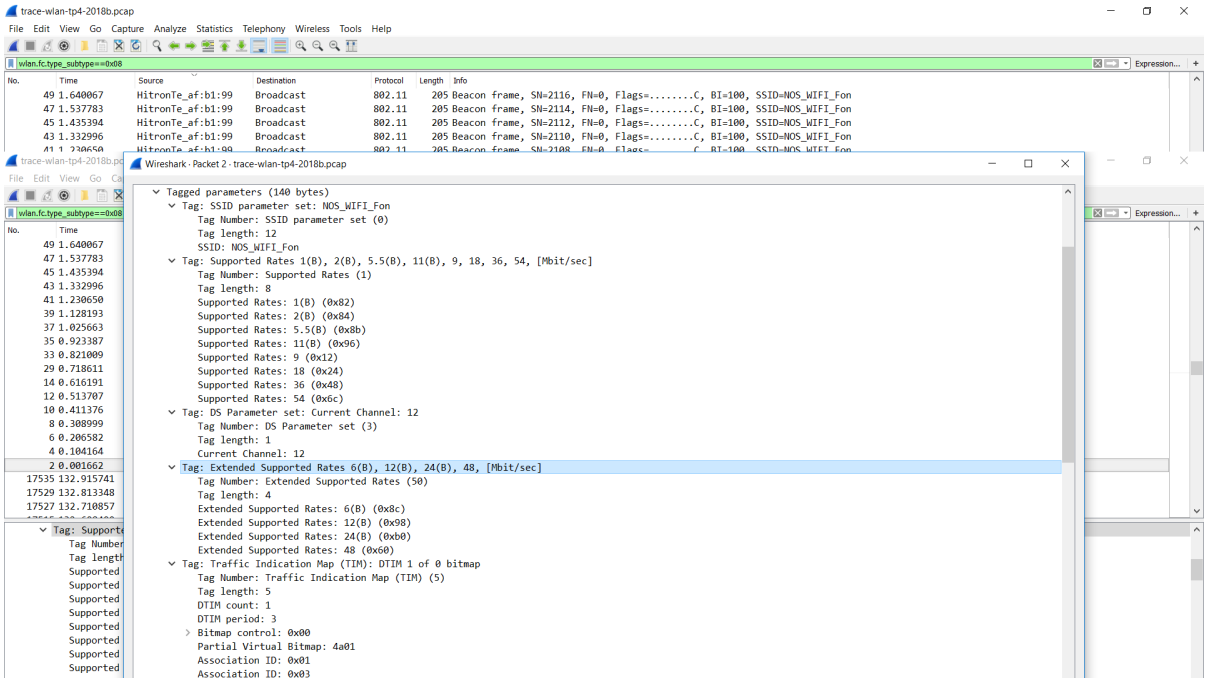
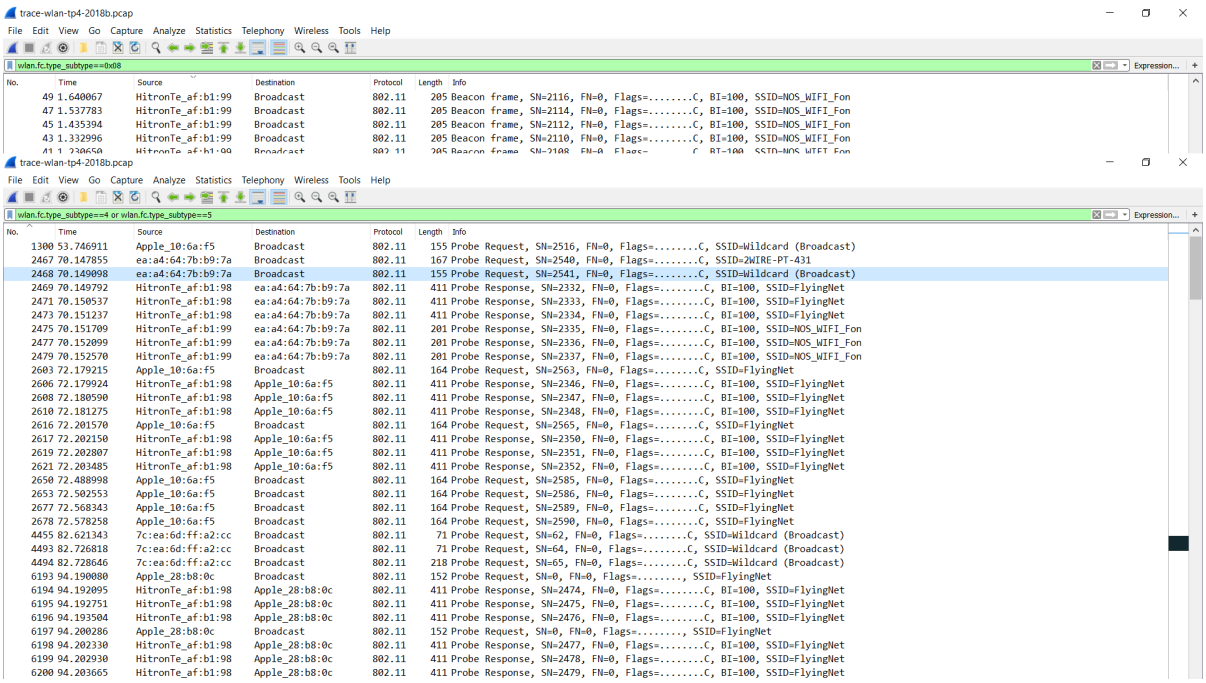


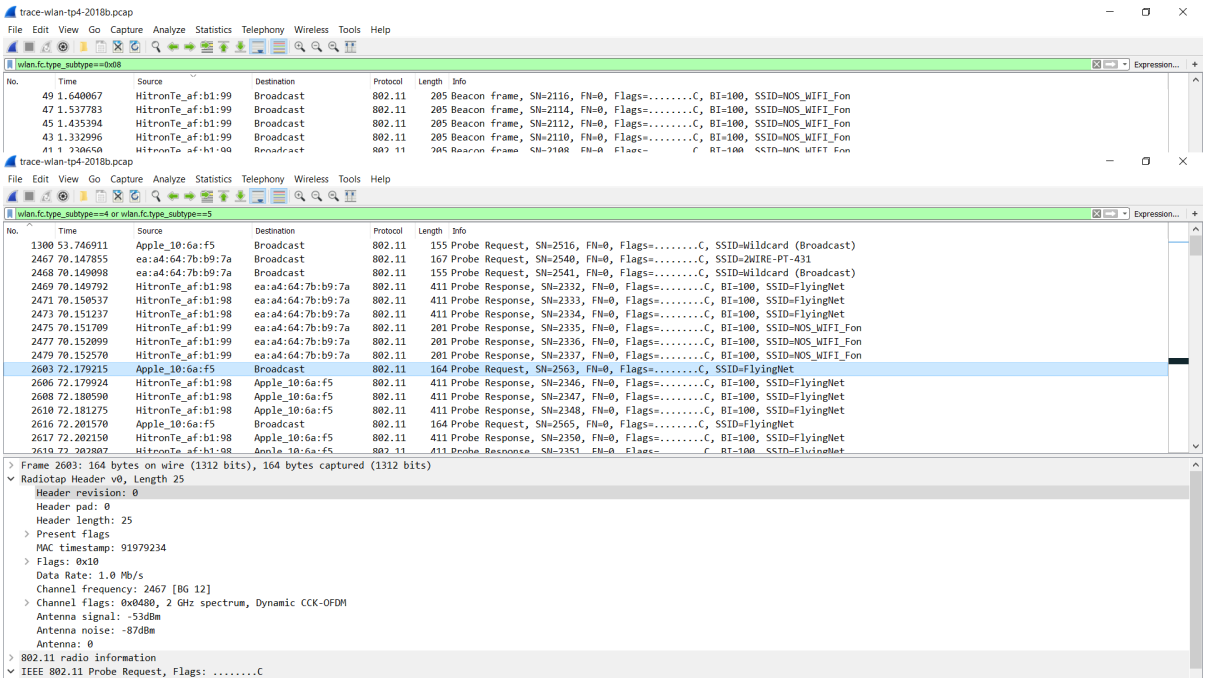
Figure 8: Débito de Base e Extended supported Rate do AP com SSID NOS-wifi

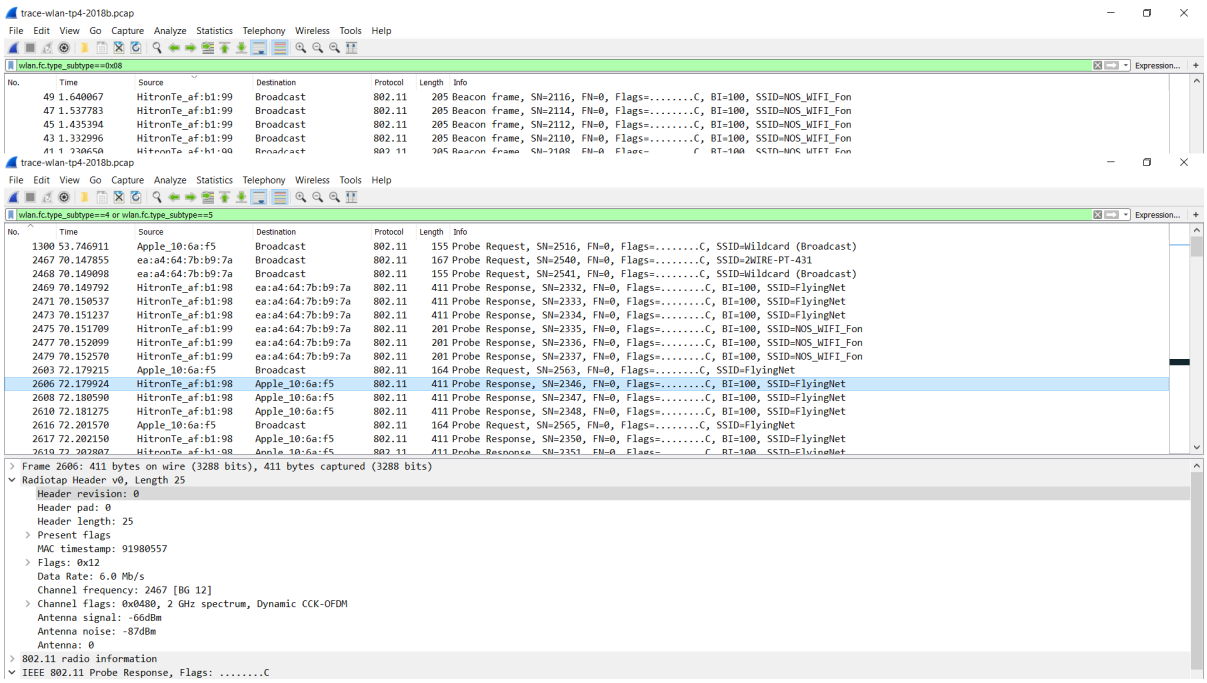
10) Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente. O filtro que nos permite visualizar todas as tramas *probing request* e *response* está explícito no print em baixo.



11) Identifique um *probing request* para o qual tenha havido um *probing response*.

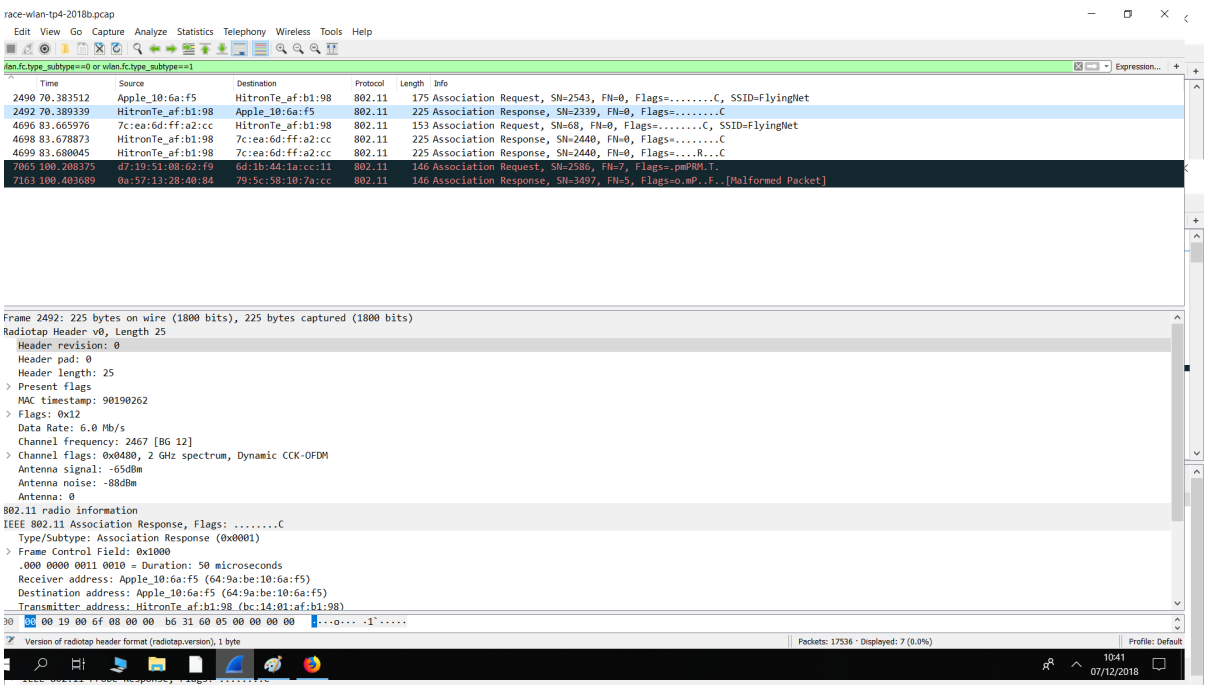
As tramas 2603 e 2606 tratam-se de um *probing requeste* de um *probing response* respetivamente. A trama *probing request* trata-se de uma STA(Apple_10:6a:f5) que a emite para procurar um AP, logo é uma trama emitida para todos os equipamentos naquela rede.A trama *probing response* é a resposta do AP(HitronTe_af:b1:98)para a STA. O propósito da trama *probing request* é informar a STA(Apple_10:6a:f5) quais os APs que estão na sua vizinhança através de tramas *probing responses* nas quais estão incluídas informações sobre as taxas de dados suportadas.



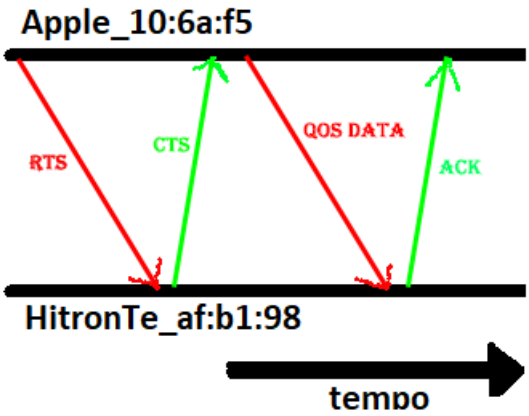


12) Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

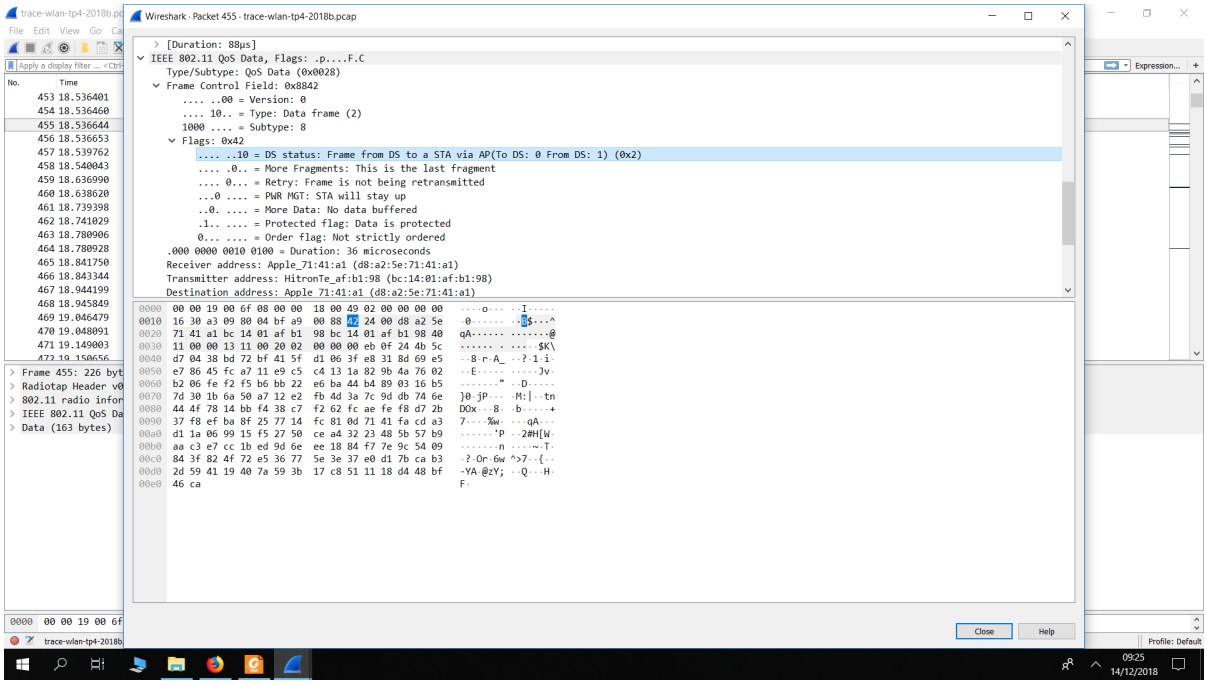
Após ter sido aplicado o respetivo filtro para encontrar as tramas *association request* e *association response*.A trama 2490 corresponde a um pedido de associação e a trama 2492 corresponde a uma resposta de associação.Esquecemo-no de tirar print ,no entanto, depois disto, foi realizada uma captura sem filtros e ordenada por ordem temporal e foi possível observar uma trama de autenticação(autentication) que inicia a fase de autenticação e uma trama confirmação da receção(acknoledgment) que termina a fase de autenticação.Posteriormente, foi possível observar a fase de associação que se inicia numa trama pedido de associação(nº 2490)e termina numa trama confirmação de receção(nº2492) que indica que não existiam erros na trama de dados enviada imediatamente antes.



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

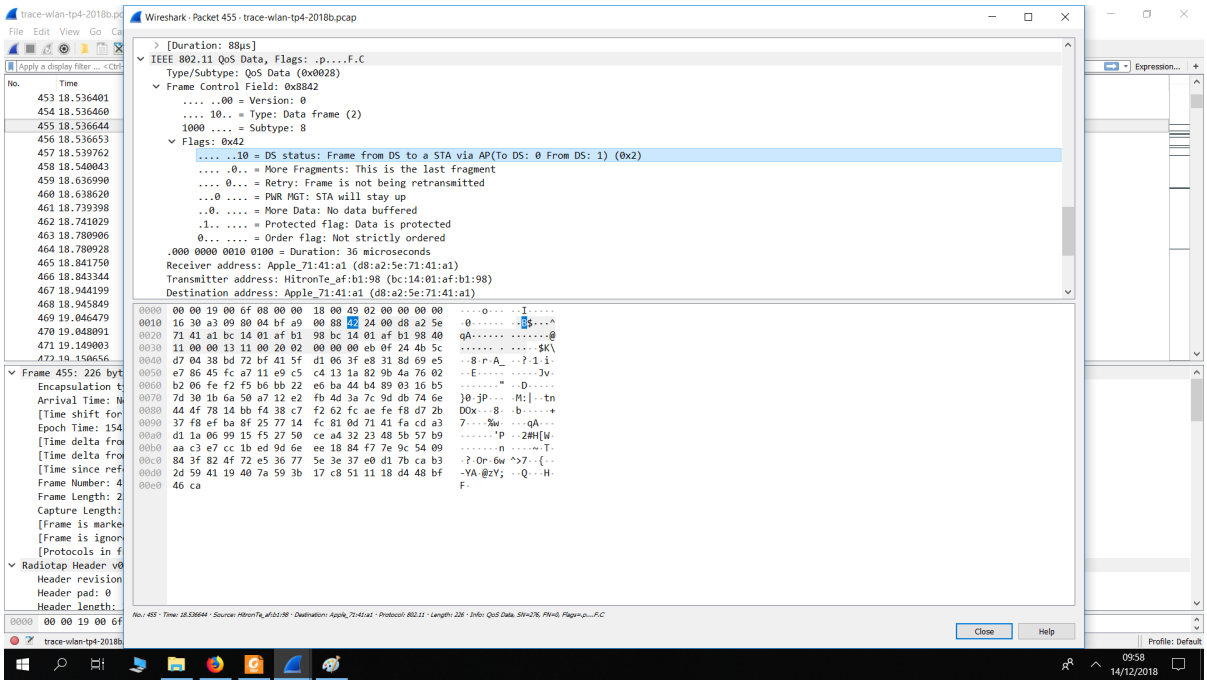


14) Considere a trama de dados nº455. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?



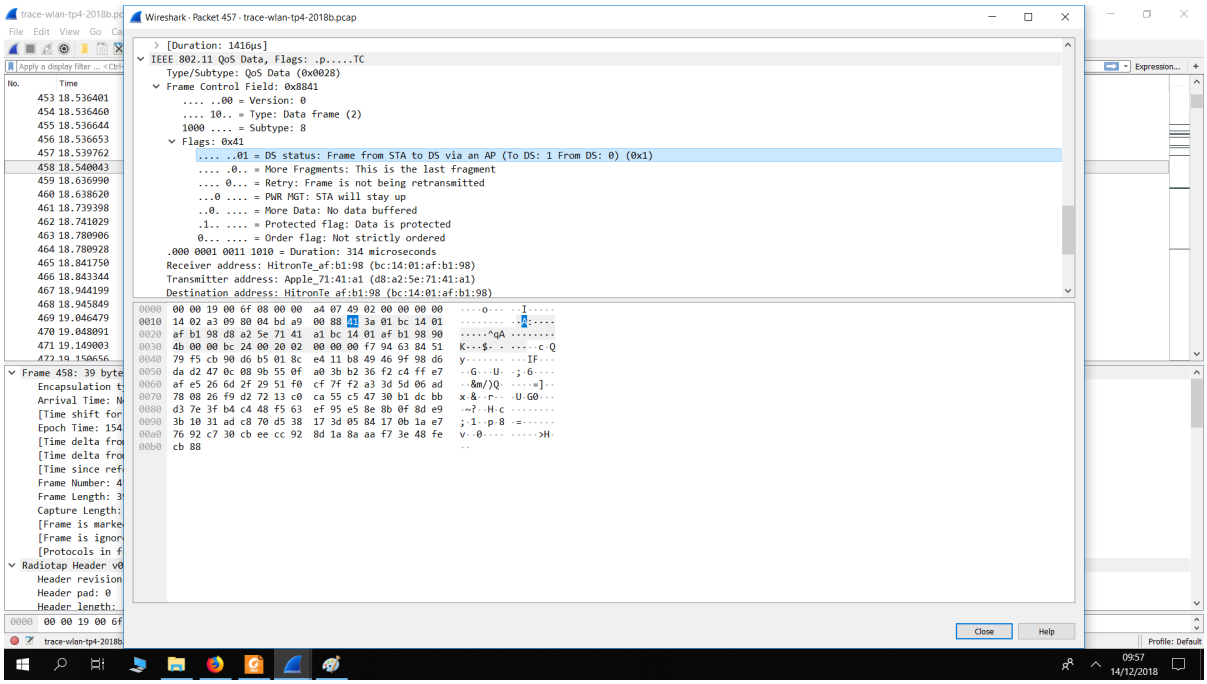
Não é local à WLAN pois como indica a flag "TO DS:0 FROM DS:1,a trama recebida vem do sistema de distribuição(HitronTe_af:b1:98) para a STA(Apple_71:41:a1),através do AP(HitronTe_af:b1:98)

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?



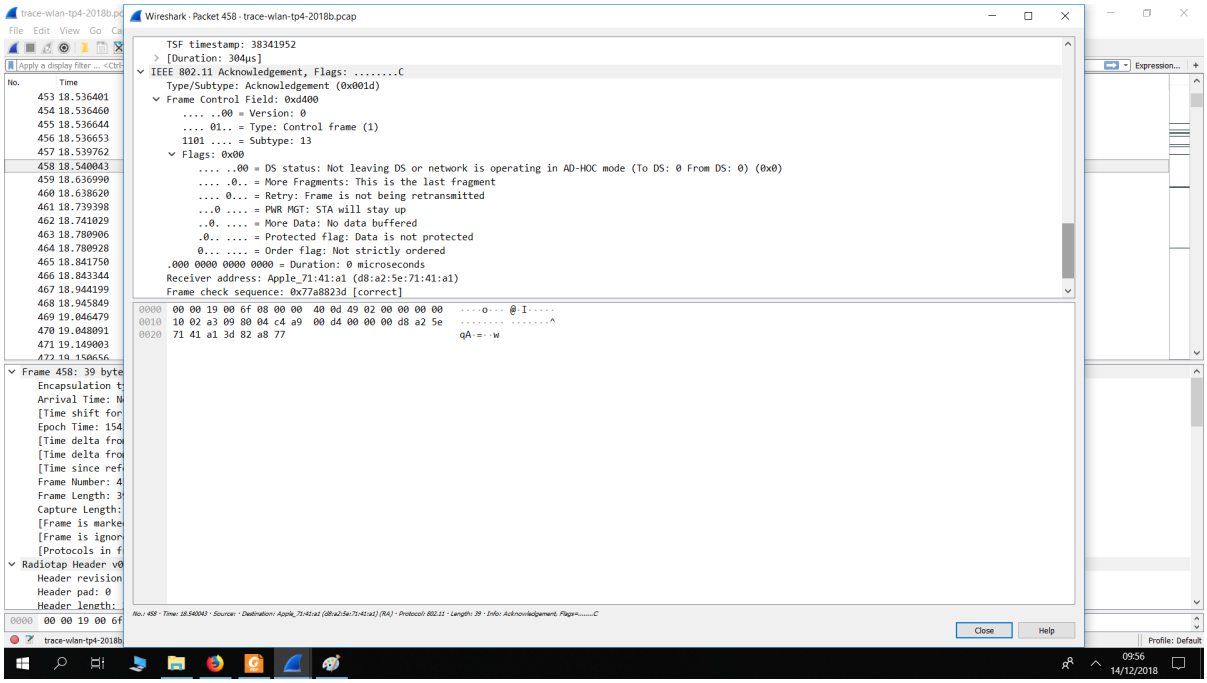
Com base na informação disposta pela trama nº455, é nos possivel identificar que o endereço MAC bc:14:01:af:b1:98 (*Transmisson address*) corresponde ao AP, o endereço MAC d8:a2:5e:71:41:a1 (*Receiver address*) representa o host sem fios(STA), e por fim o endereço MAC d8:a2:5e:71:41:a1 (*Destination address*) diz respeito ao router de acesso ao sistema de distribuição.

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



Na trama 457, a direcionalidade é "To DS:1 From DS:0, o que nos indica que a trama está a ser transmitida para fora da rede local. O *transmiter address* é a STA com endereço d8:a2:5e:71:41:a1,o *receiver address* é o AP com endereço bc:14:01:af:b1:98 e o *destination address* é o Router de acesso com endereço bc:14:01:af:b1:98. O pacote chega da STA ao sistema de distribuição pelo AP.

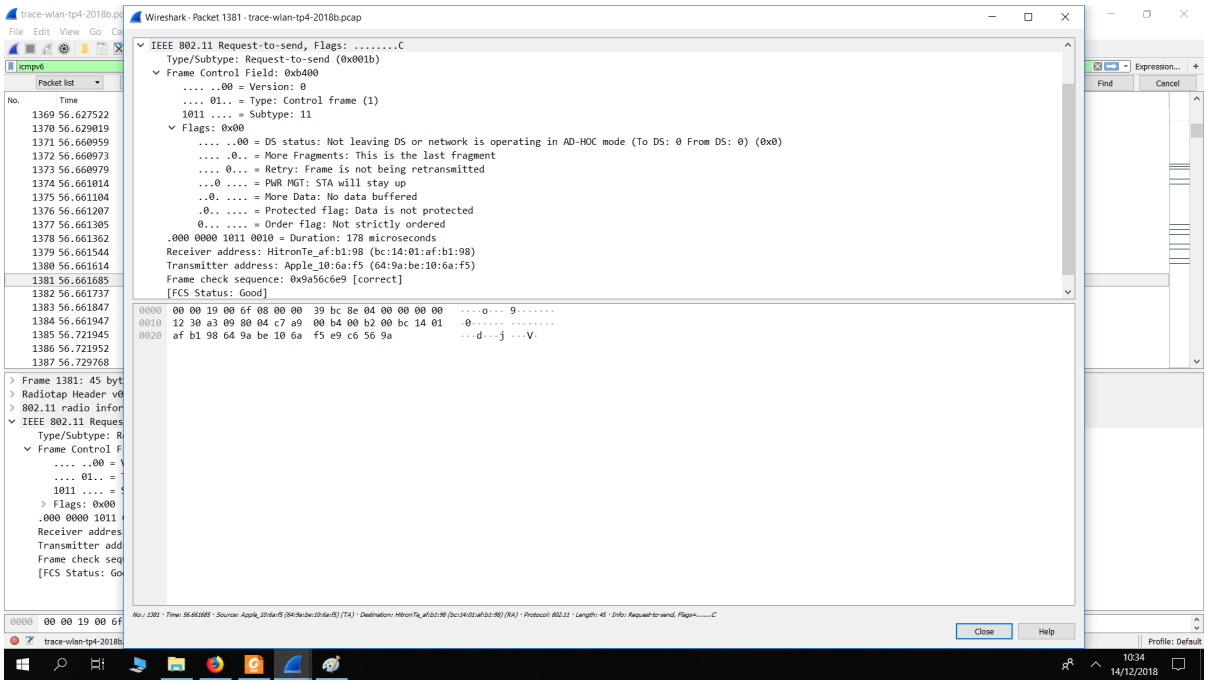
17) Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar porque razão têm de existir (contrariamente ao que acontece numa rede Ethernet.)

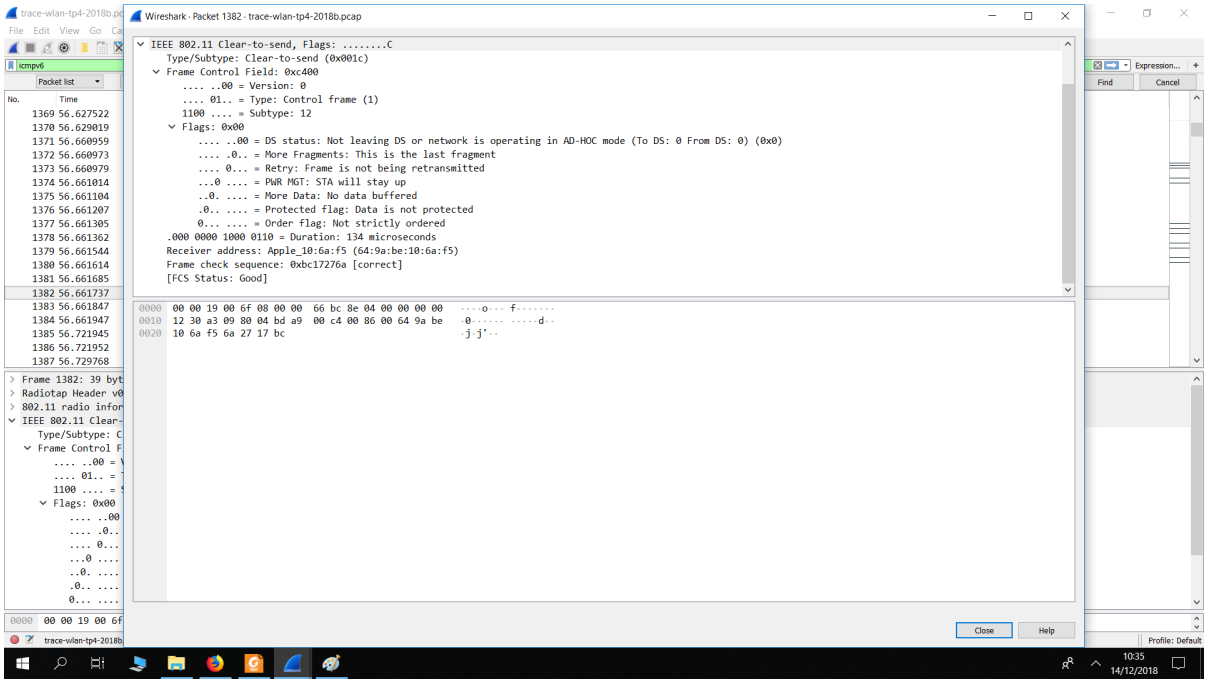


É transmitida uma trama de controlo, de subtipo *acknowledgement*, ou seja, uma "confirmação de receção". Este tipo de tramas sao emitidas se não existir nenhum erro e a sua existência é imprescindivel devido aos erros que ocorrem neste tipo de redes. Por exemplo, numa rede WLAN, a mensagem pode nunca chegar ao destino pretendido. Com a rececao de um trama *acknowledgement*, sabemos que a trama de dados enviada chegou ao destino, se nao chegasse, a trama de dados seria reenviada. Esta situação não ocorre numa rede Ethernet pois não existem interferências, tornando desnecessária a existência deste tipo de mensagens.

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 sis-

temas envolvidos.





As opções *Request To Send* (RTS) e *Clear To Send* (CTS) estão a ser usadas na troca de dados entre a STA e o AP/Router da WLAN. Nos prints apresentados em cima, podemos ver que as tramas 1381 e 1382 se tratam de um RTS e um CTS, respetivamente.

Após uma análise dos prints é também percetível que a direccionalidade das tramas é TO DS: 0 FROM DS: 0, o que nos diz que estas estão a operar localmente à WLAN.

A STA envia uma trama RTS ao AP, informando-o que lhe pretende transmitir dados e este, posteriormente, informa o AP, com uma trama CTS, que os pode enviar. Este CTS informa as outras estações na WLAN que está a ser processado um envio de dados, evitando assim possíveis colisões, atraves de um valor temporal.

Conclusão

Com a realização deste trabalho adquirimos conhecimento que nos permite analisar tramas da norma IEEE 802.11(redes wi-fi). Observamos características específicas dos tipos de conexões da WLAN, como os débitos suportados pelas conexões que existem, o alcance ,entre outras.

Primeiramente, vimos o funcionamento do *scanning* passivo e ativo que têm a ver com o modo como os APs emitem os *beacons*. Foi feita uma análise detalhada da forma como os APs se relacionam e se dão a conhecer à rede que integram. Ficamos também a perceber como funcionam e o que especificam outros campos das tramas *beacon* como, por exemplo, o campo de erros, os campos que identificam a rede, os campos que identificam os endereços dos equipamentos MAC.

Posteriormente, analisamos o processo que antecede a autenticação e a consequente associação dos equipamentos que irão trocar informação.

Relativamente à forma como os APs se relacionam, podemos inferir que, no nosso quotidiano, estamos constantemente a realizar interações com os nossos quipamentos, por exemplo, quando fazemos refresh nas definições da internet para ficarmos a conhecer que redes estão ao nosso alcance,e à medida que nos deslocamos os APs vão ser diferentes

Em suma, esta forma de comunicação, como as redes Wifi e/ou Bluetooth, está a evoluir cada vez mais, preparando-nos melhor para resolver certos problemas que tenham a ver com este tipo de redes.