### WUOLAH



### wireshark.pdf

Practica WireShark Resuelta

- 3° Redes de Ordenadores
- Escuela Politécnica Superior
  Universidad Carlos III de Madrid



## Descarga la APP de Wuolah. Ya disponible para el móvil y la tablet.







#### Parte 1. Capa de transporte.

Pregunta 1. Identifique los mensajes correspondientes al proceso de "three-way-handshake". ¿Qué información se intercambia en cada uno de ellos? ¿Cuáles son los números de secuencia y de ACK en cada mensaje?

Se intercambia puerto origen, puerto destino, num\_seq, ACK. SYN. SYN-ACK ACK.

Cliente PC Servidor 192.168.1.60 185.103.39.27

| 1600::410:000:920 | I GOM!! TAGT! NTOM! OF" | ILF   | 00 31403 → 30505 [WCV] 364-330 WCV-503 MIH-5043 FEH-A 13A91-040. |
|-------------------|-------------------------|-------|--|
| 192.168.1.60      | 185.103.39.27           | TCP   | 78 58212 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval. |
| 185.103.39.27     | 192.168.1.60            | TCP   | 74 443 → 58212 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1452 . |
| 192.168.1.60      | 185.103.39.27           | TCP   | 66 58212 → 443 [ACK] Seq=1 Ack=1 Win=132480 Len=0 TSval=9757338. |
| 192.168.1.60      | 185.103.39.27           | TLSv1 | 699 Client Hello   |
| 185.103.39.27     | 192.168.1.60            | TCP   | 66 443 → 58212 [ACK] Seg=1 Ack=634 Win=45056 Len=0 TSval=122236. |

(Recordar que TCP trabaja con flujo de byte. Que ACK es el próximo byte que se quiere recibir y que número de seq es el número de byte q se envía. Transporte fiable) + Acordarse del timeout. SYN para iniciar la comuniación.

Pregunta 2. Identifica el primer mensaje enviado una vez realizado el "three-way-handshake". ¿Cuáles son la IP y puerto de origen del mensaje? ¿Y la IP y puerto de destino? ¿Qué número de secuencia tiene el mensaje? ¿Cuál será el número de ACK esperado en la respuesta a este mensaje?

Client hello es el primer mensaje.

```
Frame 75: 699 bytes on wire (5592 bits), 699 bytes captured (5592 bits) on interface 0

Ethernet II, Src: Apple_2a:a6:20 (8c:85:90:2a:a6:20), Dst: Mitrasta_2f:6e:06 (cc:d4:a1:2f:6e:06)

Internet Protocol Version 4, Src: 192.168.1.60, Dst: 185.103.39.27

Transmission Control Protocol, Src Port: 58212, Dst Port: 443, Seq: 1, Ack: 1, Len: 633

Source Port: 58212

Destination Port: 443

[Stream index: 5]

[TCP Segment Len: 633]

Sequence number: 1 (relative sequence number)

[Next sequence number: 634 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

1000 .... = Header Length: 32 bytes (8)

Flags: 0x018 (PSH ΔCK)
```

**ORIGEN:** 

IP + puerto: 192.168.1.60 + 58212



**DESTINO:** 

IP + puerto: 185.103.39.72 + 443

Num\_seq mensaje: 1.

ACK esperado en la respuesta a este mensaje: 634.

| 132110011100  | 103110313311  |        | an north . Lin flight and T link T HTH Thrips roll a lotar plaint |
|---------------|---------------|--------|---|
| 192.168.1.60  | 185.103.39.27 | TLSv1  | 699 Client Hello  |
| 185.103.39.27 | 192.168.1.60  | TCP    | 66 443 → 58212 [ACK] Seq=1 Ack=634 Win=45056 Len=0 TSval=12223    |
| 185 182 38 27 | 102 168 1 68  | TI Cv1 | 216 Caruar Hallo Change Cinhar Char Annlication Data Annlica      |

Pregunta 3. Identifique el primer mensaje enviado en el test de bajada. ¿Cuál es el puerto de destino de la conexión? ¿Y el puerto origen? Adjunte una captura de pantalla.

Es change cipher spec, application data o bien solo application data.

|   | 132110011100 | 1031103133111 |       | an nert . I'm friend and any tien for their there i fell a later and |
|---|--------------|---------------|-------|--|
| t | 192.168.1.60 | 185.103.39.27 | TLSv1 | 146 Change Cipher Spec, Application Data                             |
|   | 192.168.1.60 | 185.103.39.27 | TLSv1 | 112 Application Data   |
|   |              |               |       |  |

Puerto de destino: 443

Puerto de origen: 58512

```
Frame 81: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0

Ethernet II, Src: Apple_2a:a6:20 (8c:85:90:2a:a6:20), Dst: Mitrasta_2f:6e:06 (cc:d4:a1:2f:6e:06)

Internet Protocol Version 4, Src: 192.168.1.60, Dst: 185.103.39.27

▼ Transmission Control Protocol, Src Port: 58212, Dst Port: 443, Seq: 714, Ack: 251, Len: 46

Source Port: 58212

Destination Port: 443

[Stream index: 5]

[TCP Segment Len: 46]

Sequence number: 714 (relative sequence number)
```

Pregunta 4. Identifique el primer mensaje enviado en el test de subida. ¿Cuál es el puerto de destino de la conexión? ¿Y el puerto origen? ¿Son los mismos puertos que en la prueba de bajada? Adjunte una captura de pantalla.

```
192.168.1.60
                     217.116.8.155
                                          TCP
                                                     78 58213 → 8081 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSV
217.116.8.155
                     192.168.1.60
                                          TCP
                                                     74 8081 → 58213 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=145
192.168.1.60
                     217.116.8.155
                                          TCP
                                                     66 58213 → 8081 [ACK] Seq=1 Ack=1 Win=132480 Len=0 TSval=97573
                                          TLSv1...
192.168.1.60
                     217.116.8.155
                                                    264 Client Hello
217.116.8.155
                     192.168.1.60
                                          TCP
                                                     66 8081 → 58213 [ACK] Seg=1 Ack=199 Win=15872 Len=0 TSval=4652
217.116.8.155
                     192.168.1.60
                                          TLSv1...
                                                   1506 Server Hello
217.116.8.155
                     192.168.1.60
                                          TLSv1...
                                                   1506 Certificate [TCP segment of a reassembled PDU]
217.116.8.155
                     192.168.1.60
                                          TLSv1...
                                                    273 Server Key Exchange, Server Hello Done
                                                     66 58213 → 8081 [ACK] Seq=199 Ack=2881 Win=129600 Len=0 TSval=
192.168.1.60
                     217.116.8.155
                                          TCP
192.168.1.60
                     217.116.8.155
                                          TCP
                                                     66 58213 → 8081 [ACK] Seq=199 Ack=3088 Win=129344 Len=0 TSval=
192.168.1.60
                     217.116.8.155
                                          TLSv1...
                                                    141 Client Key Exchange
                                                     72 Change Cipher Spec
192.168.1.60
                     217.116.8.155
                                          TLSv1...
192.168.1.60
                     217.116.8.155
                                          TLSv1...
                                                    111 Encrypted Handshake Message
                     192.168.1.60
                                          TCP
                                                     66 8081 → 58213 [ACK] Seq=3088 Ack=325 Win=15872 Len=0 TSval=4
217.116.8.155
217.116.8.155
                     192.168.1.60
                                          TLSv1...
                                                    117 Change Cipher Spec, Encrypted Handshake Message
                                          TCP
                                                     66 58213 → 8081 [ACK] Seq=325 Ack=3139 Win=131008 Len=0 TSval=
192.168.1.60
                     217.116.8.155
192.168.1.60
                     217.116.8.155
                                          TLSv1.
                                                    893 Application Data
217.116.8.155
                     192.168.1.60
                                          TLSv1...
                                                     224 Application Data
                                                     66 58213 - 8081 [ACK] Sen=1152 Ack=3297 Win=130880 Len=0 TSval
197 168 1 68
                     217 116 8 155
```

Puerto de origen: 58213 Puerto destino: 8081

(Creo q esto es de otra conexión no de la pagina)

```
Wireshark · Packet 93 · Wi-Fi: en0
▶ Frame 93: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
▶ Ethernet II, Src: Apple_2a:a6:20 (8c:85:90:2a:a6:20), Dst: Mitrasta_2f:6e:06 (cc:d4:a1:2f:6e:06)
▶ Internet Protocol Version 4, Src: 192.168.1.60, Dst: 185.103.39.27
▼ Transmission Control Protocol, Src Port: 58212, Dst Port: 443, Seq: 1075, Ack: 647, Len: 31
     Source Port: 58212
     Destination Port: 443
    [Stream index: 5]
     [TCP Segment Len: 31]
     Sequence number: 1075
                             (relative sequence number)
     [Next sequence number: 1106
                                   (relative sequence number)]
     Acknowledgment number: 647
                                    (relative ack number)
     1000 .... = Header Length: 32 bytes (8)
  Flags: 0x018 (DSH ACK)
0000 cc d4 a1 2f 6e 06 8c 85
                                 90 2a a6 20 08 00 45 00
                                                             · · · /n · · · * · · · E ·
                                                             · S · · @ · @ · · > · · < · g
      00 53 00 00 40 00 40 06
                                 98 3e c0 a8 01 3c b9 67
                                                            '..d.\.,_(.%...
...{....:(.N·I
/r........K...r.
0020 27 1b e3 64 01 bb 5c 15
                                 2c 5f 28 ae 25 89 80 18
      08 0b e0 7b 00 00 01 01
                                08 0a 3a 28 84 4e 07 49
0040 2f 72 17 03 03 00 1a 1e
                                1d d9 4b 90 04 db 72 03
0050 35 28 22 0f 3a e3 54 88
                                e2 dc 40 e4 c6 a6 71 36
                                                             5("·:·T· ··@···q6
0060 e4
```

No son los mismos puertos que en la prueba de bajada.

En el 3 y 4. Test de bajada: de la ip 185 a 192 y test de subida de 192 a 185 (CREO).





# Descarga la APP de Wuolah. Ya disponible para el móvil y la tablet.

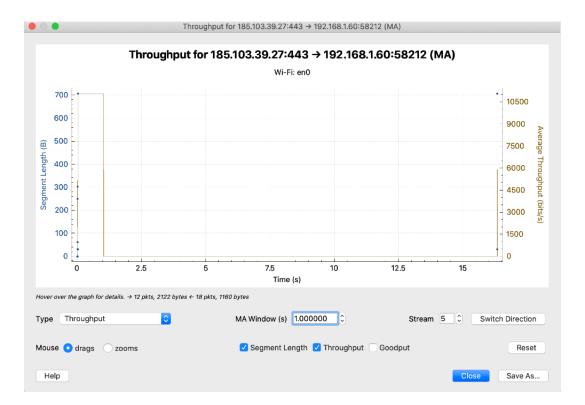






pony

Problema 5. Seleccione el primer mensaje enviado en el test de bajada. Adjunte una captura de pantalla con la gráfica del "Throughput" (Statistics TCP Stream Graph...).



CREO que el test de bajada es de 185 a 192.

P6. ¿Cuánto tiempo ha durado el test de bajada?

El test de bajada ha durado: 17.5 s.

P7. ¿Se corresponde la velocidad media de descarga con la obtenida en el test? ¿Qué velocidad es esa (en KBytes/s)? ¿Ha sido la velocidad más o menos constante a lo largo de la prueba? ¿Por qué cree que ha sido así? Justifique todas las respuestas.

222.94 Megabits / s. (La del test). -- > En KBytes / s : 27867,5.

¿Donde se ve la velocidad media de descarga?



#### Parte 2. Nivel de red.

Pregunta 1. ¿Cuál es el tamaño total del mensaje ICMP? ¿Cuántos datos se envían dentro del mensaje ICMP? Describa cuánto ocupa cada parte del mensaje.

#### ¿El PING es a la ip del router?

| 61  | 3.65402/ | 192.168.1.60 | 192.168.1.1  | ICMP | 98 | Echo | (ping) | reques |
|-----|----------|--------------|--------------|------|----|------|--------|--------|
| 62  | 3.658201 | 192.168.1.1  | 192.168.1.60 | ICMP | 98 | Echo | (ping) | reply  |
| 65  | 4.655277 | 192.168.1.60 | 192.168.1.1  | ICMP | 98 | Echo | (ping) | reques |
| 66  | 4.672907 | 192.168.1.1  | 192.168.1.60 | ICMP | 98 | Echo | (ping) | reply  |
| 84  | 5.660533 | 192.168.1.60 | 192.168.1.1  | ICMP | 98 | Echo | (ping) | reques |
| 85  | 5.664351 | 192.168.1.1  | 192.168.1.60 | ICMP | 98 | Echo | (ping) | reply  |
| 88  | 6.665809 | 192.168.1.60 | 192.168.1.1  | ICMP | 98 | Echo | (ping) | reques |
| 89  | 6.670081 | 192.168.1.1  | 192.168.1.60 | ICMP | 98 | Echo | (ping) | reply  |
| 90  | 7.671341 | 192.168.1.60 | 192.168.1.1  | ICMP | 98 | Echo | (ping) | reques |
| 91  | 7.675359 | 192.168.1.1  | 192.168.1.60 | ICMP | 98 | Echo | (ping) | reply  |
| 110 | 8.676423 | 192.168.1.60 | 192.168.1.1  | ICMP | 98 | Echo | (ping) | reques |
| 111 | 8.679397 | 192.168.1.1  | 192.168.1.60 | ICMP | 98 | Echo | (ping) | reply  |
| 112 | 0 601041 | 102 160 1 60 | 102 160 1 1  | TCMD | no | Echo | (ning) | roduor |

#### Tamaño total es 98.

Los datos que se envían dentro del mensaje ICMP:

▼ Data (48 bytes)

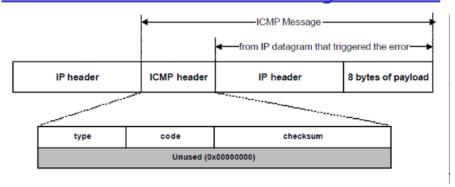
Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...

[Length: 48]

#### Describe cuanto ocupa cada parte del mensaje ICMP:

|                           |                        | IP Datagram     |            |            |  |  |  |  |
|---------------------------|------------------------|-----------------|------------|------------|--|--|--|--|
|                           | Bits 0-7               | Bits 8-15       | Bits 16-23 | Bits 24-31 |  |  |  |  |
|                           | Version/IHL            | Type of service | Len        | gth        |  |  |  |  |
|                           | Identif                | cation          | flags an   | d offset   |  |  |  |  |
| IP Header<br>(20 bytes)   | Time To Live<br>(TTL)  | Protocol        | Checksum   |            |  |  |  |  |
|                           | Source IP address      |                 |            |            |  |  |  |  |
|                           | Destination IP address |                 |            |            |  |  |  |  |
| ICMP Header               | Type of message        | Code            | Checksum   |            |  |  |  |  |
| (8 bytes)                 | Header Data            |                 |            |            |  |  |  |  |
| CMP Payload<br>(optional) |                        | Payloa          | ad Data    |            |  |  |  |  |

#### TOME THE COLLECTION MESSAGE FROIDCOL



Pregunta 2. ¿Cuál es el puerto origen y destino del mensaje ICMP? ¿Por qué cree que es así? Justifique las respuestas.

Puerto origen:

Puerto destino:

ICMP no tiene puerto origen ni puerto destino. Lo que tiene es IP origen e IP destino.

```
▶ Internet Protocol Version 4, Src: 192.168.1.60, Dst: 192.168.1.1
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
```

Repita los pasos anteriores, pero esta vez envíe 60000 bytes en cada mensaje. Conteste las siguientes preguntas:

Pregunta 3. Explique detalladamente cómo ha cambiado la situación ahora con respecto a la prueba anterior.

TERMINAR.ç



#### PARTE 3. Ethernet.

Pregunta 1. ¿Cuál es la dirección MAC de origen y de destino en el mensaje ICMP?

```
tenting rate String. 1cmp || 1cmpvo]
Ethernet II, Src: Apple_2a:a6:20 (8c:85:90:2a:a6:20), Dst: Mitrasta_2f:6e:06 (cc:d4:a1:2f:6e:06)
▶ Destination: Mitrasta_2f:6e:06 (cc:d4:a1:2f:6e:06)
▶ Source: Apple_2a:a6:20 (8c:85:90:2a:a6:20)
Type: IPv4 (0x0800)
```

Pregunta 2. ¿Puede ver en el mensaje la dirección IP de la puerta de enlace? ¿Y su MAC? Justifique todas las respuestas.

En mensaje ICMP, Ethernet solo puedo ver las MAC no las IP.

Pregunta 3. ¿Qué significan los flags del mensaje ICMP en la capa Ethernet?

DUUUUDAAAAAAA. No sé que flags son.





# Descarga la APP de Wuolah. Ya disponible para el móvil y la tablet.







405416\_arts\_esce ues2016juny.pdf

#### Top de tu gi



Rocio





Pregunta 4. ¿Cuál es la dirección MAC de origen y de destino en el mensaje ICMP?

MAC origen:

MAC destino:

# Ethernet II, Src: Apple\_2a:a6:20 (8c:85:90:2a:a6:20), Dst: Mitrasta\_2f:6e:06 (cc:d4:a1:2f:6e:06) ▶ Destination: Mitrasta\_2f:6e:06 (cc:d4:a1:2f:6e:06) ▶ Source: Apple\_2a:a6:20 (8c:85:90:2a:a6:20) Type: IPv4 (0x0800)

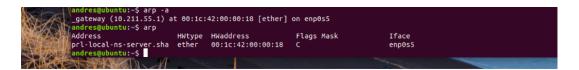
Pregunta 5. ¿Puede ver en el mensaje la dirección IP de Google? ¿Y su MAC? Justifique todas las respuestas.

En ethernet no puedo ver la ip pero la mac si aunq no de google si no q la mac es la de mi router.

| T* | 112 14.670576 | 192.168.1.60  | 172.217.17.14 | ICMP | 98 Echo (ping) reques |
|----|---------------|---------------|---------------|------|-----------------------|
| _  | 113 14.676282 | 172.217.17.14 | 192.168.1.60  | ICMP | 98 Echo (ping) reply  |
|    | 128 15.671768 | 192.168.1.60  | 172.217.17.14 | ICMP | 98 Echo (ping) reques |
|    | 129 15.678493 | 172.217.17.14 | 192.168.1.60  | ICMP | 98 Echo (ping) reply  |
|    | 302 16.675225 | 192.168.1.60  | 172.217.17.14 | ICMP | 98 Echo (ping) reques |
|    | 304 16.680343 | 172.217.17.14 | 192.168.1.60  | ICMP | 98 Echo (ping) reply  |
|    | 603 17.676066 | 192.168.1.60  | 172.217.17.14 | ICMP | 98 Echo (ping) reques |
|    | COA 17 CO24CO | 173 317 17 14 | 100 100 1 60  | TCMD | 00 Faba (mina) manl.  |

#### **ARP**

Pregunta 6. Haciendo uso del comando arp, obtenga la tabla ARP de la máquina. Describa los distintos campos y adjunta una captura de pantalla.



Flags->8

The flags indicate if the mac address has been learned, manually set, published (announced by another node than the requested) or is incomplete.



I think you can must check your kernel source to figure out what the flags mean or you simply try it. My system translates

- 0x0 incomplete
- 0x2 complete
- 0x6 complete and manually set

"Each complete entry in the ARP cache will be marked with the C flag. Permanent entries are marked with M and published entries have the P flag."

Mask no se q es. Mask es mascara de la misma forma q el prefijo ip.

IFace creo que es interface.

Adresss dirección a la que va.

HWType es protocolo. Ether de ethernet.

Pregunta 7. Localice todos los mensajes que han permitido obtener la IP de Google (tanto DNS como ARP), y justifique cómo se ha podido llevar a cabo, paso a paso, la identificación del mismo.

| No.        |     | Time      | Source       | Destination  | Protocol | Length | Info     |       |       |
|------------|-----|-----------|--------------|--------------|----------|--------|----------|-------|-------|
| <b>⊤</b> * | 147 | 8.915097  | 192.168.1.60 | 80.58.61.254 | DNS      | 75     | Standard | query | 0x670 |
| 4          | 150 | 8.922245  | 80.58.61.254 | 192.168.1.60 | DNS      | 174    | Standard | query | respo |
|            | 883 | 33.588131 | 192.168.1.60 | 80.58.61.254 | DNS      | 70     | Standard | query | 0x16c |
|            | 884 | 33.593050 | 80.58.61.254 | 192.168.1.60 | DNS      | 86     | Standard | query | respo |
|            | 943 | 39.613216 | 192.168.1.60 | 80.58.61.254 | DNS      | 96     | Standard | query | 0xe58 |
|            | 946 | 39.619129 | 80.58.61.254 | 192.168.1.60 | DNS      | 282    | Standard | query | respo |

Explicar como funciona DNS.

| lo. |     | Time      | Source            | Destination | Protocol | Length | Info    |                                    |
|-----|-----|-----------|-------------------|-------------|----------|--------|---------|------------------------------------|
|     | 67  | 0.916262  | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 68  | 0.916266  | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.337 Tell 192.168.1.48    |
|     | 172 | 10.337532 | Apple_b6:af:37    | Broadcast   | ARP      | 42     | Who has | 169.254.255.255? Tell 192.168.1.50 |
|     | 179 | 14.023525 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 180 | 14.023531 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 192 | 14.844479 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 193 | 14.844922 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 228 | 15.866663 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.337 Tell 192.168.1.48    |
|     | 229 | 15.866667 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 243 | 16.890942 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 244 | 16.890948 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 247 | 17.914951 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 248 | 17.914956 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 249 | 18.938975 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.337 Tell 192.168.1.48    |
|     | 250 | 18.938982 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 872 | 32.046383 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 873 | 32.046389 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 874 | 33.070995 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 875 | 33.071001 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 887 | 33.889858 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.337 Tell 192.168.1.48    |
|     | 888 | 33.889864 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.337 Tell 192.168.1.48    |
|     | 900 | 34.915444 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 901 | 34.915804 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 64     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | 907 | 35.937663 | Ubiquiti_76:b8:22 | Broadcast   | ARP      | 60     | Who has | 192.168.1.33? Tell 192.168.1.48    |
|     | nan | חב מחדרים | Uhimuiti 76.60.22 | Danadanat   | ADD      | CA     | Wha has | 102 160 1 222 Tall 102 160 1 40    |



| 916  | 36.961875 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 60 Who has 192.168.1.33? Tell 192.168.1.48    |
|------|-----------|-------------------|-------------------|-----|---|
| 917  | 36.961882 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 64 Who has 192.168.1.33? Tell 192.168.1.48    |
| 931  | 38.604571 | Mitrasta_2f:6e:06 | Apple_2a:a6:20    | ARP | 60 Who has 192.168.1.60? Tell 192.168.1.1     |
| 932  | 38.604687 | Apple_2a:a6:20    | Mitrasta_2f:6e:06 | ARP | 42 192.168.1.60 is at 8c:85:90:2a:a6:20       |
| 1010 | 47.816296 | Apple_b6:af:37    | Broadcast         | ARP | 42 Who has 169.254.255.255? Tell 192.168.1.50 |
| 1031 | 50.069257 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 60 Who has 192.168.1.33? Tell 192.168.1.48    |
| 1032 | 50.069264 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 64 Who has 192.168.1.33? Tell 192.168.1.48    |
| 1039 | 51.093684 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 60 Who has 192.168.1.33? Tell 192.168.1.48    |
| 1040 | 51.093691 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 64 Who has 192.168.1.33? Tell 192.168.1.48    |
| 1083 | 52.117338 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 60 Who has 192.168.1.33? Tell 192.168.1.48    |
| 1084 | 52.117345 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 64 Who has 192.168.1.33? Tell 192.168.1.48    |
| 1085 | 53.141102 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 60 Who has 192.168.1.33? Tell 192.168.1.48    |
| 1086 | 53.141105 | Ubiquiti_76:b8:22 | Broadcast         | ARP | 64 Who has 192.168.1.33? Tell 192.168.1.48    |

Explicar como funciona ARP.

Pregunta 8. Explique para qué sirven los comandos del paso 2.

sudo ip neigh flush dev eth0 --> Para eliminar de la cache ARP eth0

sudo /etc/init.d/nscd restart --> elimina la cache DNS.

Pregunta 9. Localice todos los mensajes que han permitido obtener la IP de Google (tanto DNS como ARP). ¿Ha cambiado algo respecto al caso analizado en la P6? Justifique la respuesta.

VERRRRRRRRRRRR no me ejecutan estos comandos debería ser Linux.

Pregunta 10. Adjunte capturas de pantalla significativas en las que se muestre la nueva tabla ARP y los mensajes capturados por Wireshark. Describa el procedimiento empleado para conseguir el desvío de tráfico propuesto, indicando los comandos utilizados y justificando su uso.

Para conseguir el desvio de tráfico propuesto. Asociar dirección MAC del atacante con la dirección Ip del atacado así, de esta forma se consigue desviar .



arp -s address hw\_adress



