## Práctica 1

**Apellidos:** López Pérez

**Nombre:** Marta

**Titulación:** Grado de Ingeniería del Informática

**Grupo:** A

**PC de la práctica:** PC709

1.- Lea el enunciado de la práctica para obtener la traza de Wireshark necesaria para responder las siguientes preguntas

2.- Lea atentamente las notas al final del enunciado de la práctica (recuerde en guardar la traza – fichero p1.pcapng – y tomar capturas de pantallas justificando de dónde obtuvo las respuestas)

3.- No olvide rellenar arriba el equipo en el que realizó las prácticas (en el que capturó el tráfico)

4.- En la memoria entregada, puede borrar este cuadro

**Ejercicio 1. Elija un mensaje dns, y localice en la cabecera Ethernet II** la siguiente información (haga capturas de pantalla donde aparezcan estos datos):

* Número de trama elegida:
* Información de la dirección MAC de su computadora.

Dirección MAC (en hexadecimal): 40:a8:f0:55:12:10

Fabricante de NIC (en hexadecimal): 40:a8:f0 nombre: Hewlett Packard

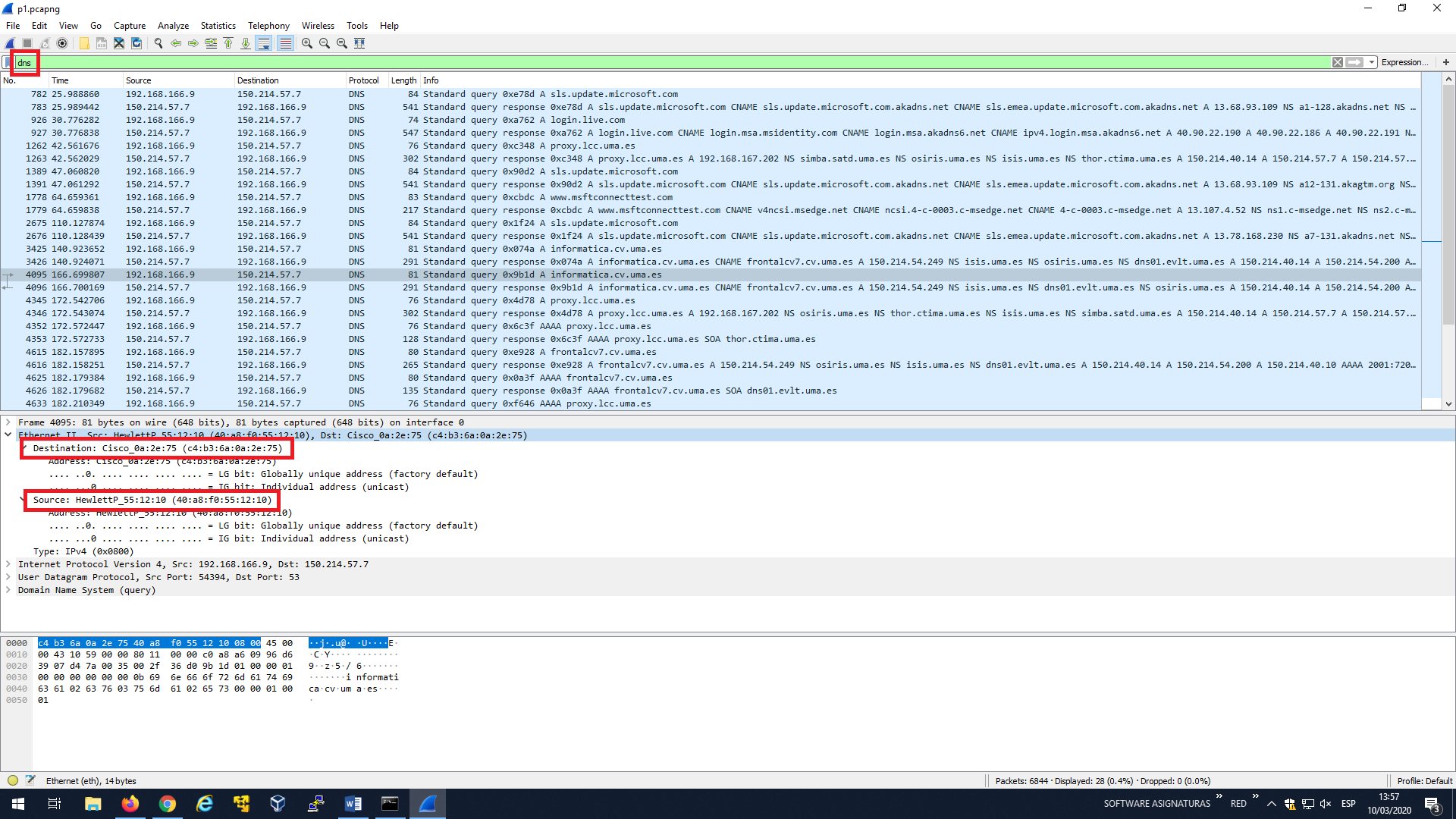
Número de serie de NIC (en hexadecimal): 55:12:10

* Información de la dirección MAC de *gateway/router*:

Dirección MAC (en hexadecimal): c4:b3:6a:0a:2e:75

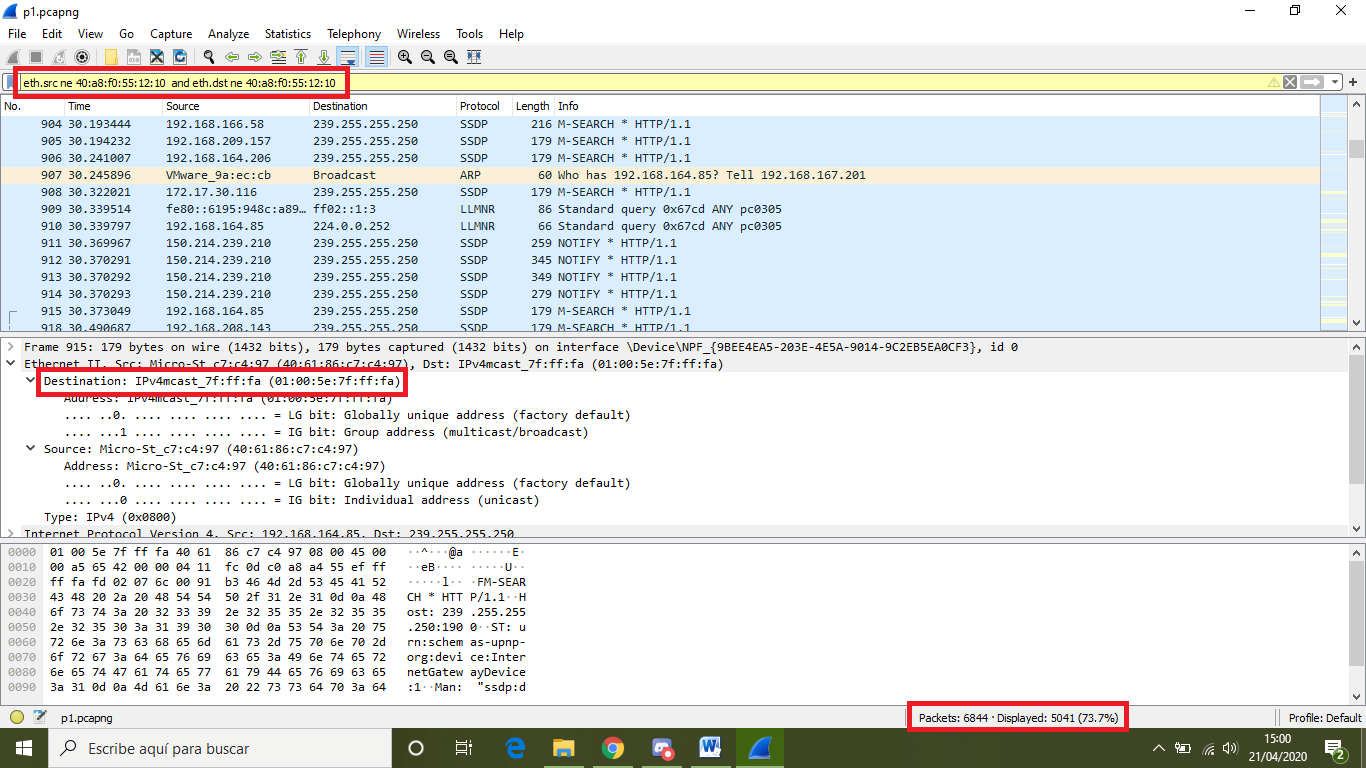
Fabricante de NIC (en hexadecimal): c4:b3:6a nombre: Cisco Systems, Inc

Número de serie de NIC (en hexadecimal): 0a:2e:75



**Ejercicio 2. Indique qué filtro** debe añadir para que se muestren las tramas donde no se utilice su dirección MAC.

* ¿Qué filtro has utilizado? eth.src ne 40:a8:f0:55:12:10 and eth.dst ne 40:a8:f0:55:12:10
* ¿Cuántas tramas recibe? 5041 de 6844
* ¿Por qué recibe esas tramas? (Para responder esta pregunta, observe las características de las direcciones MAC destino de esas tramas)
* Porque hay tramas de tipo broadcast (ff:ff:ff:ff:ff:ff )y IPv4mcast\_7f:ff:fa.



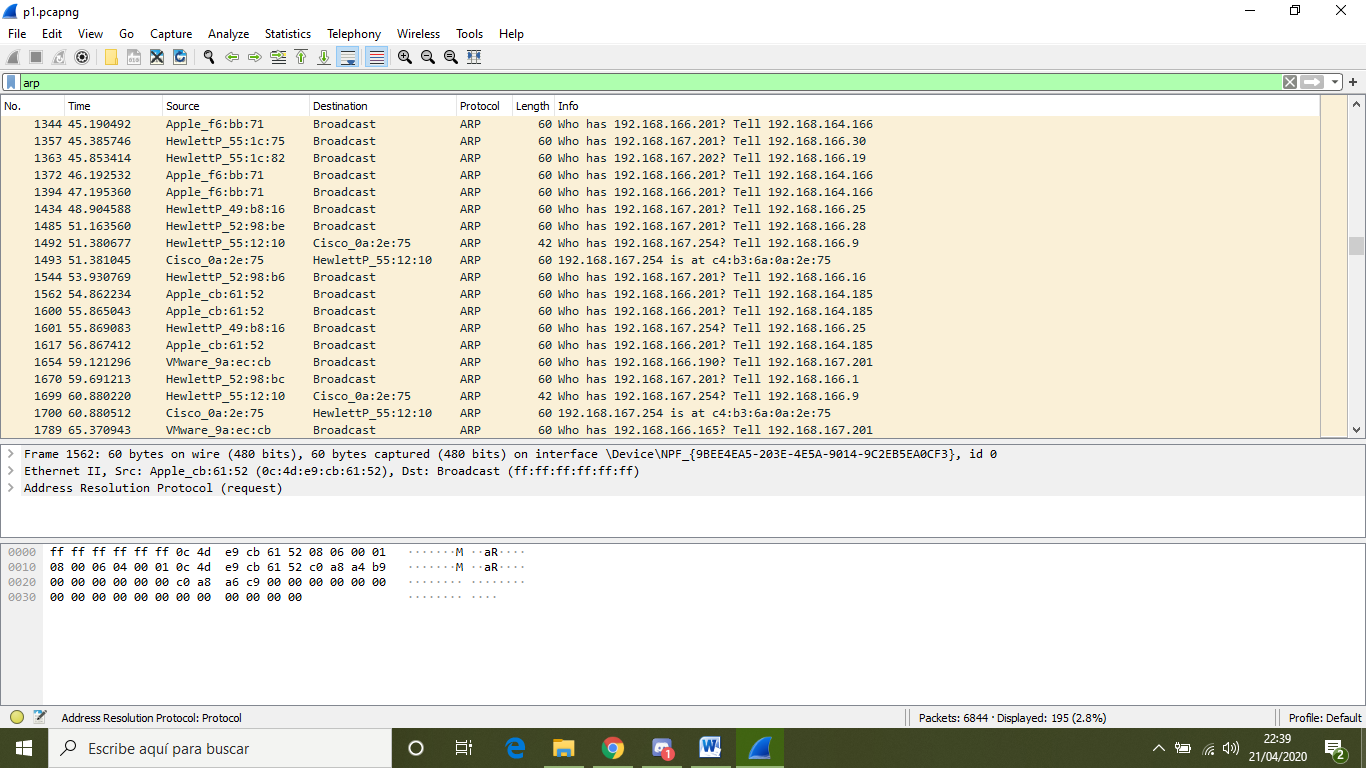
**Ejercicio 3. Dibuje la torre de protocolos** (tal como se ha visto en clase, es decir, en la parte inferior los protocolos de más bajo nivel) de un paquete ARP, uno ICMP, uno DNS y uno HTTP.

* Torre de protocolos de un paquete ARP (número de trama seleccionada: 195 )

- Frame 1562: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0

- Ethernet II, Src: Apple\_cb:61:52 (0c:4d:e9:cb:61:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Address Resolution Protocol (request



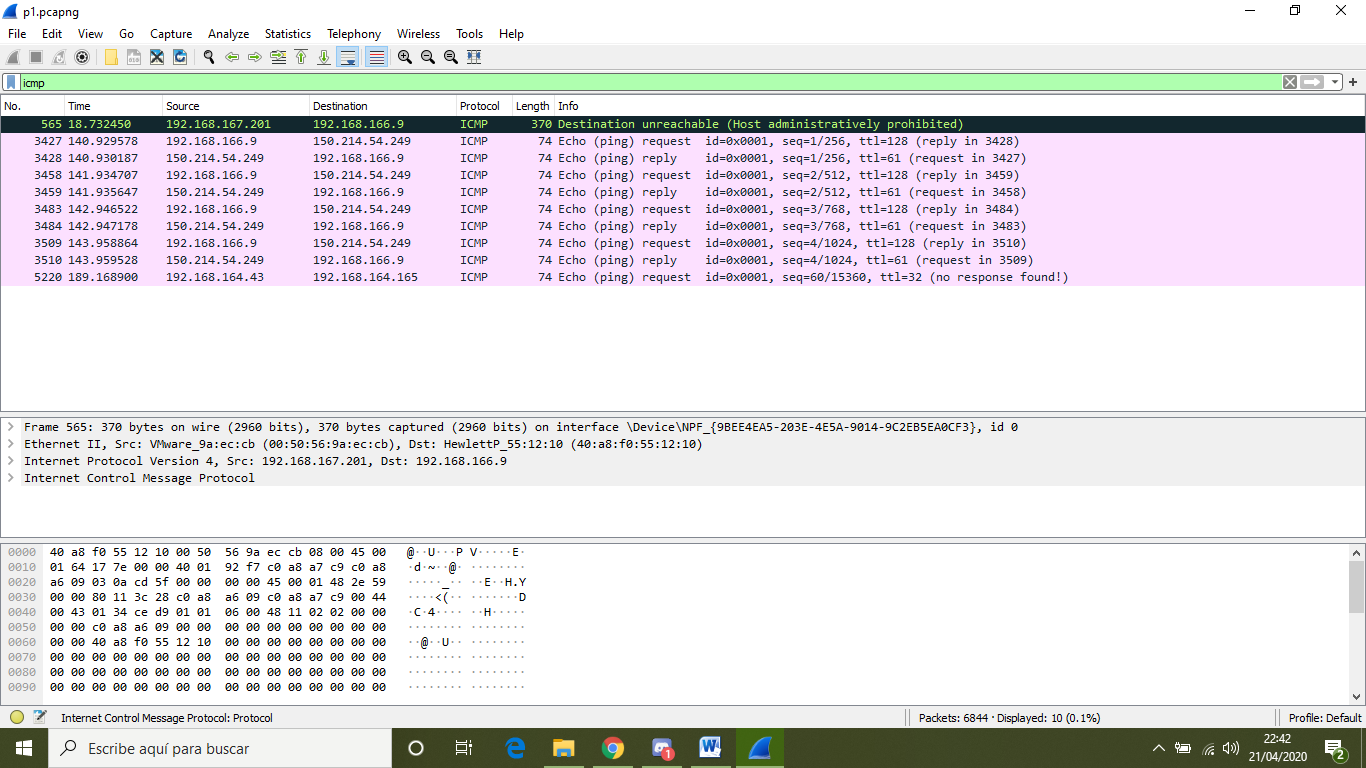
* Torre de protocolos de un paquete ICMP (número de trama seleccionada: 10)

- Frame 565: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF\_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0

- Ethernet II, Src: VMware\_9a:ec:cb (00:50:56:9a:ec:cb), Dst: HewlettP\_55:12:10 (40:a8:f0:55:12:10)

- Internet Protocol Version 4, Src: 192.168.167.201, Dst: 192.168.166.9

- Internet Control Message Protocol



* Torre de protocolos de un paquete DNS (número de trama seleccionada: 28)

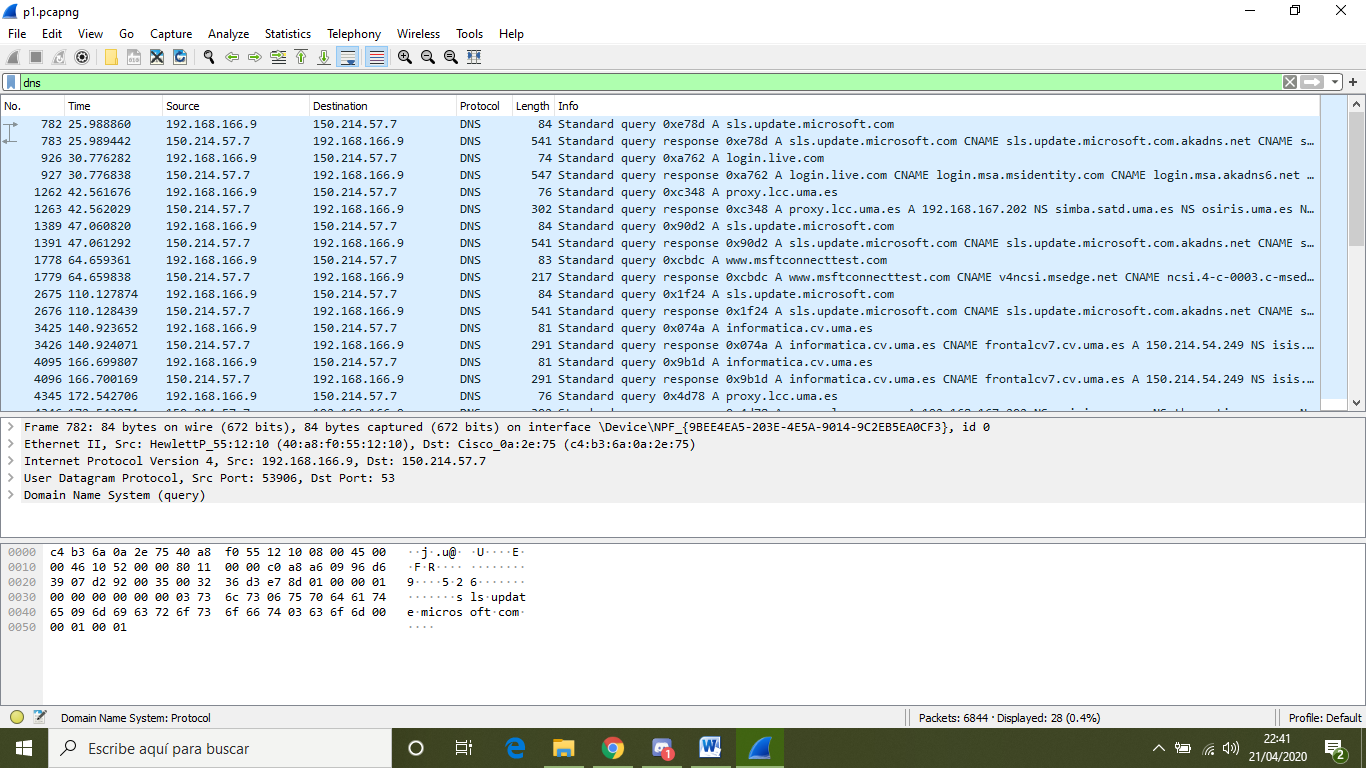
- Frame 782: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF\_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0

- Ethernet II, Src: HewlettP\_55:12:10 (40:a8:f0:55:12:10), Dst: Cisco\_0a:2e:75 (c4:b3:6a:0a:2e:75)

- Internet Protocol Version 4, Src: 192.168.166.9, Dst: 150.214.57.

- User Datagram Protocol, Src Port: 53906, Dst Port: 53

- Domain Name System (query)



* Torre de protocolos de un paquete HTTP (número de trama seleccionada: 374)

- Frame 529: 1181 bytes on wire (9448 bits), 1181 bytes captured (9448 bits) on interface \Device\NPF\_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0

- Ethernet II, Src: VMware\_9a:b3:8a (00:50:56:9a:b3:8a), Dst: HewlettP\_55:12:10 (40:a8:f0:55:12:10)

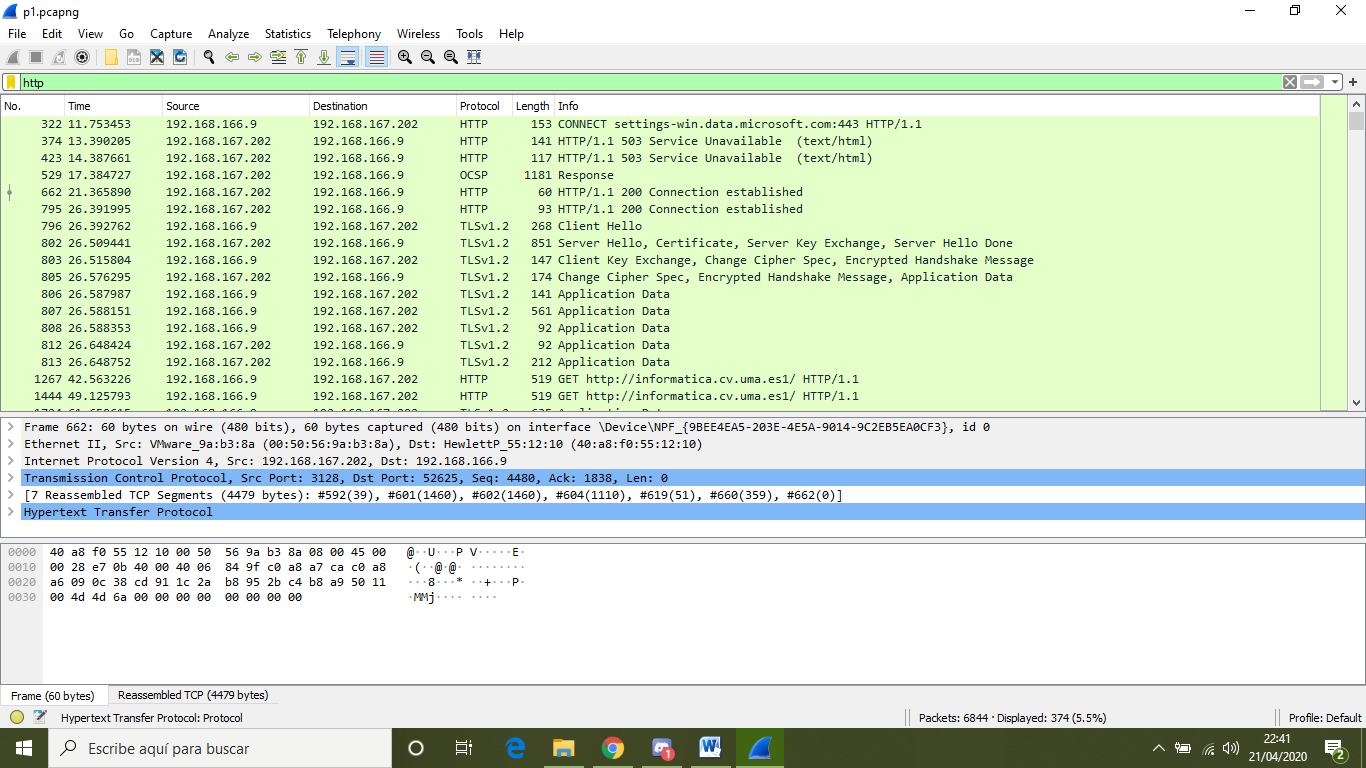
- Internet Protocol Version 4, Src: 192.168.167.202, Dst: 192.168.166.9

- Transmission Control Protocol, Src Port: 3128, Dst Port: 52621, Seq: 1461, Ack: 1, Len: 1127

- [ 2 Reassembled TCP Segments (2587 bytes): #528(1460), #529(1127) ]

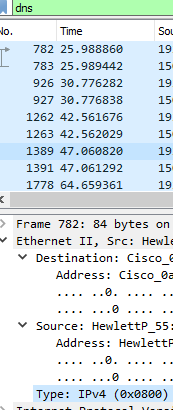
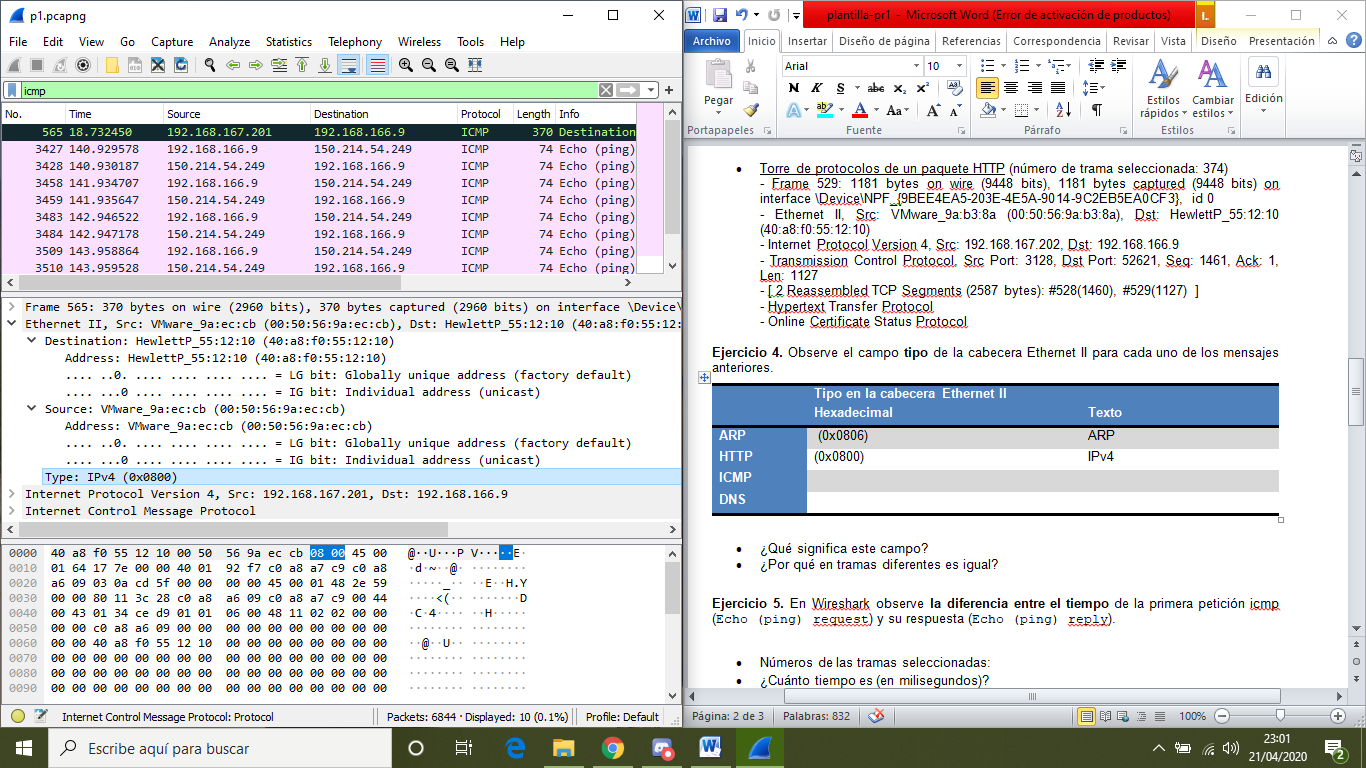
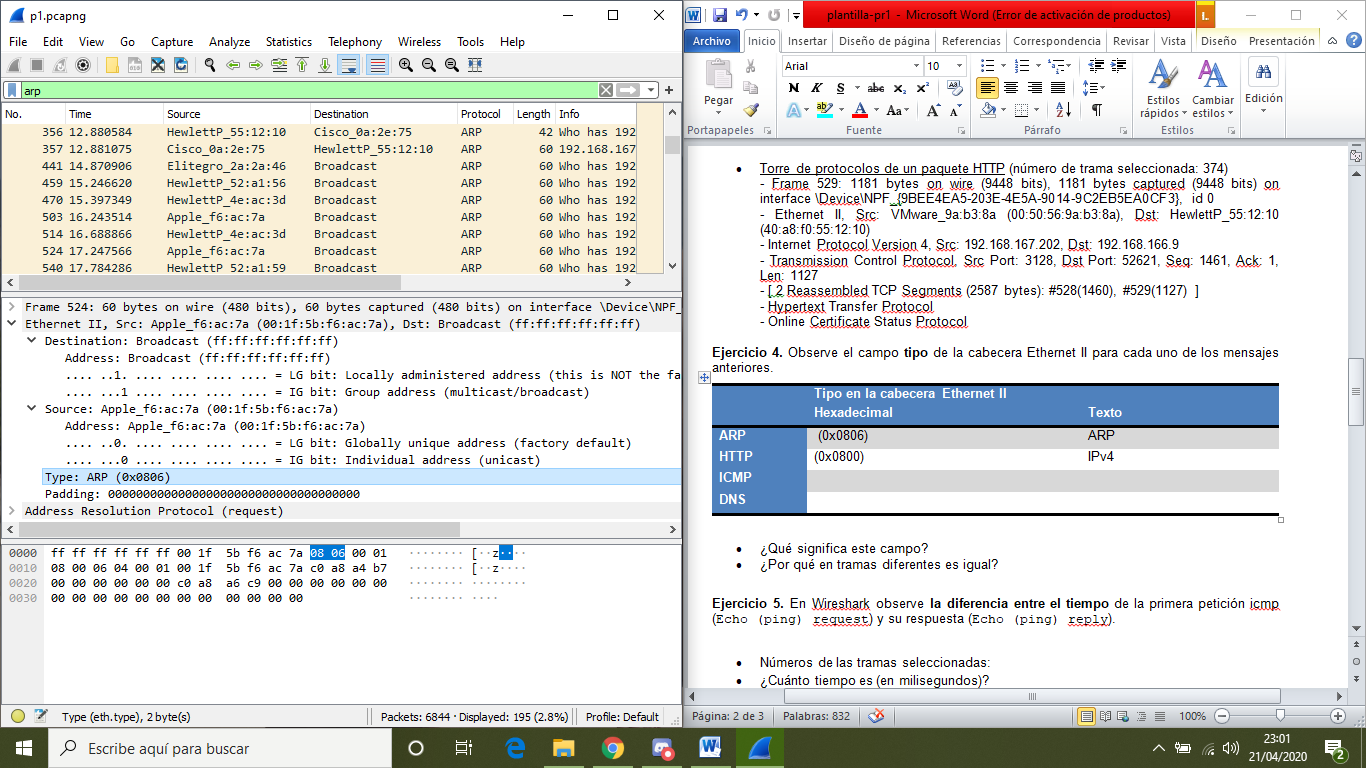
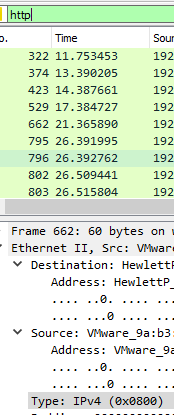
- Hypertext Transfer Protocol

- Online Certificate Status Protocol



**Ejercicio 4.** Observe el campo **tipo** de la cabecera Ethernet II para cada uno de los mensajes anteriores.

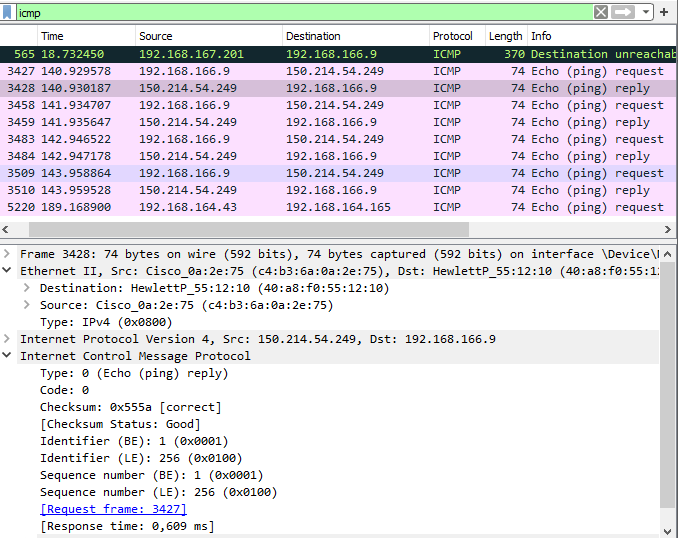
|  |  |  |
| --- | --- | --- |
|  | Tipo en la cabecera Ethernet II  Hexadecimal | Texto |
| ARP | (0x0806) | ARP |
| HTTP | (0x0800) | IPv4 |
| ICMP | (0x0800) | IPv4 |
| DNS | (0x0800) | IPv4 |



* ¿Qué significa este campo?
* Define varios protocolos en la capa de red.
* ¿Por qué en tramas diferentes es igual?
* ARP / IPv4 representa la forma en que se transmite, por lo que puede haber distintos tramas que lo transmitan de la misma de la misma forma.

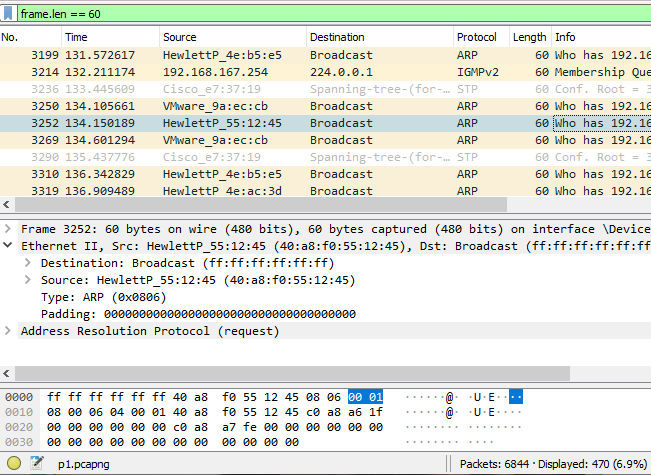
**Ejercicio 5.** En Wireshark observe **la diferencia entre el tiempo** de la primera petición icmp (Echo (ping) request) y su respuesta (Echo (ping) reply).

* Números de las tramas seleccionadas:
* 3427,3428
* ¿Cuánto tiempo es (en milisegundos)?
* [Response time: 0,609 ms
* ¿A qué concepto visto en la parte de teoría equivale dicho tiempo?
* Round-trip time



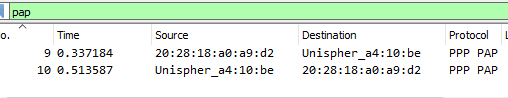
**Ejercicio 6.** Según la teoría vista en clase, las tramas Ethernet deben tener un **tamaño mínimo** de 64 bytes. Wireshark no muestra el campo FCS (ya que es tratado automáticamente por la tarjeta de red), por lo que la trama mostrada en Wireshark tendrá un tamaño de 60 bytes o más.

* Busque una trama con tamaño 60 (filtro: frame.len == 60), proporciona el número de trama. ¿Cuántas tramas tienen esta característica?
* Trama número 3252, se capturan 470 tramas con ese filtro.
* ¿Qué mecanismo se utiliza para completar el tamaño si los datos transmitidos son más pequeños de 46 bytes)?
* Padding.



**Ejercicio 7.**  Analizando esas trazas,

* ¿qué mecanismo de autenticación se usa?
* PAP (password authentication protocol)
* ¿En qué tramas (indique el número) se negocia la utilización de dicho campo?
* Tramas 9 y 10

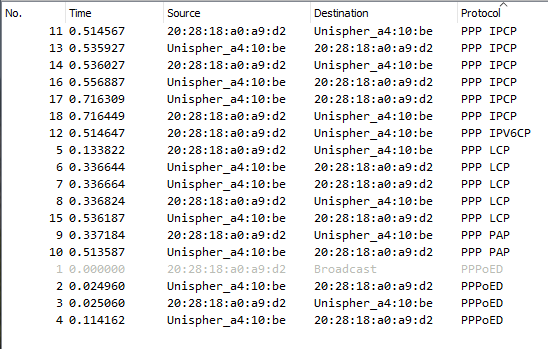


**Ejercicio 8.**  En la traza se ve el proceso correspondiente a las fases de establecer, autenticar y red vista en los apuntes.

* Indique cada trama (sin considerar las que excluyeron en el primer párrafo de este paso) a qué fase corresponde.

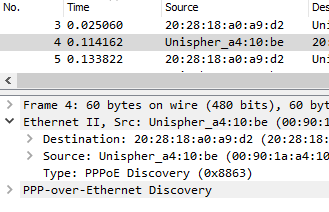
RED

ESTABLECER



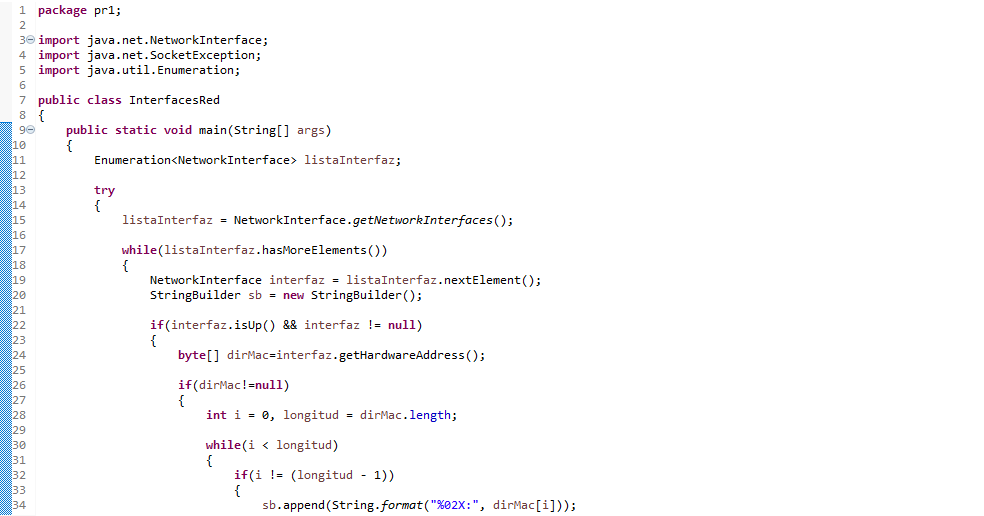
AUTENTICAR

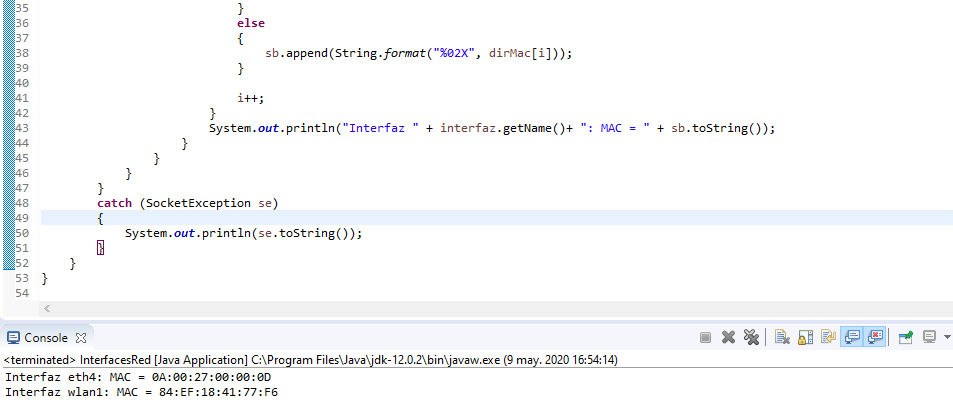
* ¿Qué protocolo del nivel de red se va a usar para transmitir los datos?
* Protocolo PPPoE.



**Ejercicio 9.**  Desarrolle un código Java que usando la clase previa liste todos los interfaces de red activos mostrando su nombre y MAC.

* Incluya una captura de pantalla con la salida obtenida.





* Explique el código.

Se crea una lista enumerada y la completamos con las distintas interfaces. Mientras la lista creada tenga elementos vamos a ir comprobando que el siguiente elemento no sea null y que esté activo. Si todo esto se cumple y existe una dirección mac para esa interfaz se va a ir agregando esta dirección byte a byte.

Por pantalla se va a mostrar el resultado en el formato

🡪 Interfaz \*nombre\*: MAC = \*dirección mac\*.

En caso que se encontrase algún error se mostraría también por pantalla gracias a que recogemos todo el código con el try y capturamos las excepciones que puedan aparecer.