**Protocolos e Interfaces de Comunicación**

**Grado en Ingeniería Telemática**

**E.T.S.I. Telecomunicación**

**Curso 2021/2022**

**Práctica 1. Revisión de protocolos TCP/IP con Wireshark.**

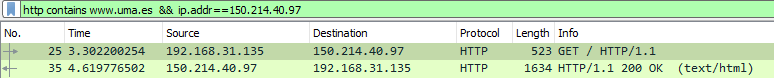
Se sugiere entregar una memoria respondiendo a las siguientes preguntas.

**1. Ejercicio 1. Realiza una captura del tráfico al entrar en www.uma.es**

a. Señala al menos 3 protocolos diferentes que puedas observar en la captura.

**Se observan protocolos como ARP, UDP o TCP.**

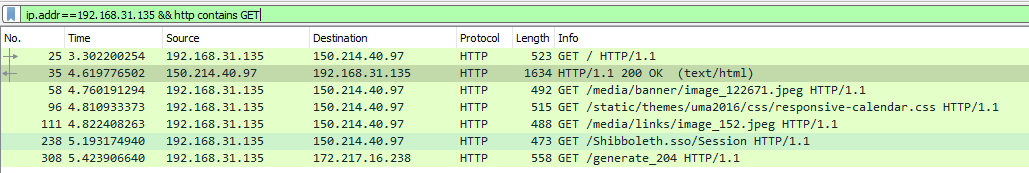
*b.* ¿Cuánto tiempo transcurre desde que se envía el primer HTTP GET hasta que se recibe el primer HTTP OK? *[recomendación: usar filtros y referencias de tiempo]*



c. ¿Cuál es la IP de www.uma.es? ¿Y la de tu ordenador?

**La IP de** [**www.uma.es**](http://www.uma.es) **es 150.214.40.97 y la nuestra es 192.168.31.135**

d. ¿Cuántos mensajes HTTP GET ha enviado tu navegador?



e. Imprime en un archivo de texto la información del primer paquete HTTP GET y HTTP OK. ¿Cuáles son las principales diferencias y similitudes que ves entre ellos?

**La petición contiene lo relacionado al documento que se le pide, mientras que la página contiene la página html solicitada por la petición. Similitudes comparten en el encapsulado y en la relación que deben de tener los paquetes ya que son contiguos como los puertos y el número secuencial, que son solo unos ejemplos.**

• ¿Cuál es la versión de HTTP que utiliza tu navegador? ¿y el servidor?

**El navegador,HTTP/1.1, y el servidor, HTTP/1.1**

• ¿Cuál es el código de HTTP GET? ¿Y el de HTTP OK? ¿Qué tipos de

código utiliza HTTP? ¿Por qué el famoso error 404 empieza por 4?

**200(respuesta satisfactoria).**

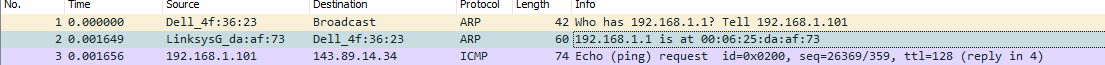
**El famoso 404 entra dentro de la gama del 4XX(400-499), que corresponde con errores por parte de los clientes.**

• ¿Cuándo fue modificado por última vez el documento que estás recibiendo?



**2. Ejercicio 2. Traza *Ping\_1* y *Ping\_2*.**

a. Abre la primera traza. ¿Cuál es la dirección IP de “tu dispositivo”? ¿Y la del destino? Razona por qué has seleccionado una IP como el origen y la otra como el destino, y no al revés.



**La ip del dispositivo es la 192.168.1.101 debido a que el primer paquete ARP lo que te dice es que está buscando a la GateWay para poder conectarse fuera de red como se ve en los paquetes siguientes, y destino son 192.168.1.1 y la 143.89.14.34**

b. Examina uno de los REQUEST de ping enviados. ¿Cuáles son el tipo de ICMP y el código? ¿Qué significa? ¿Qué otros campos tiene el paquete ICMP? ¿Cuántos bytes ocupa el checksum?

**Tipo 8 y código 0, significa solicitud de eco. El paquete ICMP tiene otros campos como lo son el checksum, el identificador, número de secuencia y los datos.**

**El checksum ocupa entre 16 y 31 bits del paquete ICMP**

c. Examina un paquete de respuesta de ping. ¿Cuáles son las diferencias encontradas con el anterior?

**El tipo es distinto debido a que uno corresponde con una solicitud y este último con una respuesta**

d. Abre la segunda traza. Examina un mensaje de error y comenta cuáles son las diferencias con los paquetes anteriores.

**La diferencia está en que en su cabecera ICMP, los mensajes de error tiene tipo 11, quiere decir que no ha podido alcanzar a la ip asociada del paquete. Los demás paquetes, tienen tipo 8 que es solicitud y tipo 0 que es que ha podido conectarse y dar respuesta.**

e. ¿Qué ocurre al final de la captura?

**A medida que se enviaron los paquetes el TTL fue aumentando, a resumidas cuentas es el tiempo de vida del paquete, que por cada salto que realiza buscando la ip del destinatario se reduce en 1, por lo que puede ocurrir lo visto anteriormente. Al final, ocurre que encuentra al equipo deseado y este le contesta.**

**3. Ejercicio 3. Traza *TCP\_1*.**

a. ¿Cuáles son los puertos de origen y de destino?

**Puerto de Origen: 1161**

**Puerto de Destino: 80**

b. ¿Cuáles son los flags de los tres primeros paquetes TCP (paquetes de establecimiento de conexión)? ¿Cuáles son los números de secuencia y de ACK de cada uno? Atiende a cómo evolucionan.

**El primer paquete especifica SYN para sincronizar los números secuenciales que van a compartir los paquetes durante su comunicación. En el segundo tiene activado el flag SYN y el flag Acknowledge, que sirve para decir que se sabe que ha recibido el mensaje correctamente. Y el tercero solo se activa el flag Adknowledge. Los números de secuencia evolucionan del 0 al 1, y van por pares, debido a que un mensaje de petición corresponde a un de respuesta por lo que tendrán el mismo número de secuencia pero el siguiente debe de tener uno más.**

c. ¿Qué paquete TCP corresponde al comando HTTP POST? *[recomendación: mirar en los datos en bruto de los paquetes]*

**El paquete que tiene el número 199, también tiene el flag de push activo.**

d. En el paquete nº 5: ¿Cuál es la longitud del paquete capturado? ¿Cuál es la longitud del paquete IP (con cabecera)? ¿Cuál es la longitud del paquete TCP (sin cabecera)?

**Longitud: 1514**

**Longitud del paquete IP(con cabecera): 1500**

**Longitud del paquete TCP (sin cabecera): 1460**

*e.* ¿Qué está ocurriendo en esta captura? *[recomendación: usar la herramienta “follow” de Wireshark]*

**Ha accedido a una página para leer el libro de Alicia en el País de las Maravillas y después se lo ha descargado**

**4. Ejercicio 4. Traza UDP\_1.**

a. ¿Cuántos campos hay en la cabecera UDP? A qué se refiere el valor “length” en este caso.

**Dirección destino y origen, la longitud, el checksum y los datos. Se refiere a la longitud del mensaje.**

b. ¿Cuál es el tamaño más grande posible de puerto?

**Los puertos van desde el 0 al 65536.**

c. ¿En qué nivel de la pila se encuentra el protocolo UDP en la captura*?*

**Se encuentra en la pila de transporte.**

d. ¿Qué es SNMP? Buscar para qué se utiliza.

**Es un protocolo para intercambiar información de administración entre dispositivos de red. Sirve para monitorear el hardware y el software de los paquetes.**