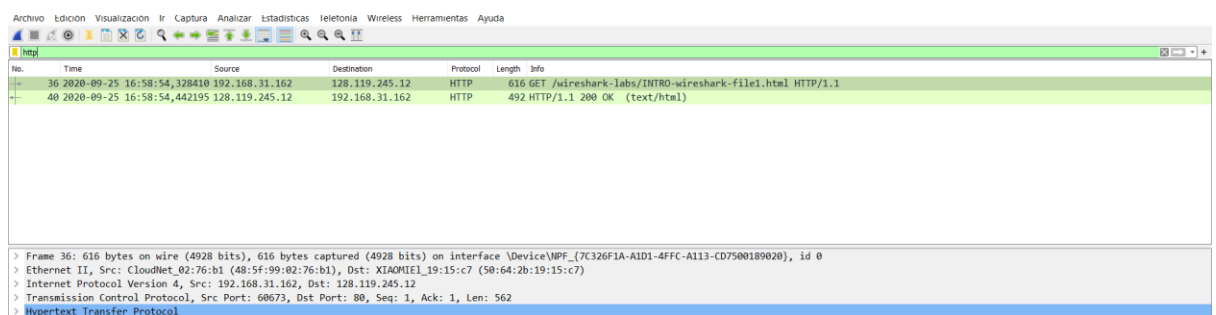


# EJERCICIOS: LAB INTRODUCCIÓN WIRESHARK

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

UDP, DNS and TCP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



No.	Time	Source	Destination	Protocol	Length	Info
36	2020-09-25 16:58:54.328410	192.168.31.162	128.119.245.12	HTTP	616	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
40	2020-09-25 16:58:54.442195	128.119.245.12	192.168.31.162	HTTP	492	HTTP/1.1 200 OK (text/html)

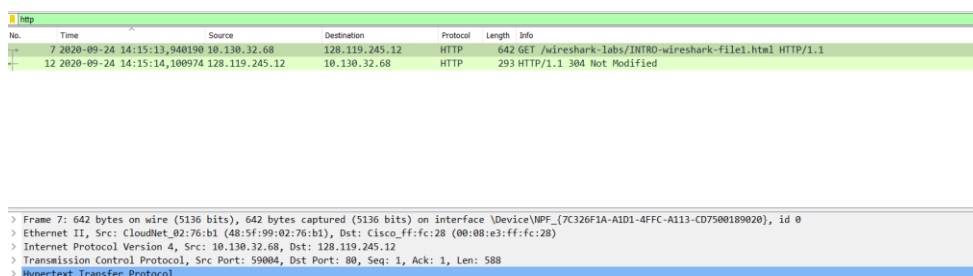
The packages arrived almost at the same time, the time difference is 0,1 s

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

The Internet address of my computer is 192.168.31.162

The internet address of the Gaia.cs.umass.edu is 128.119.245.12

4. Copy the two HTTP messages (GET and OK) referred to in question 2 above (captura la image con la herramienta recortes y pégalos en el doc).



No.	Time	Source	Destination	Protocol	Length	Info
7	2020-09-24 14:15:13.948190	10.130.32.68	128.119.245.12	HTTP	642	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
12	2020-09-24 14:15:14.04874	128.119.245.12	10.130.32.68	HTTP	293	HTTP/1.1 304 Not Modified

## **En el mensaje HTTP GET, en que solicitas la página Web al Servidor:**

5. ¿Qué protocolo se utiliza en la capa de Transporte?

TCP

6. ¿Qué número de puerto utiliza el servidor WEB?

80

7 ¿Qué número de puerto ha utilizado tu equipo?

60673

8. ¿Qué protocolo se utiliza en la capa de Red? ¿Qué versión?

IP versión 4 (IPV4)

9. ¿Qué indica el campo Time to live en las cabeceras de la capa de red?

Es el tiempo que le queda al paquete para ser descartado. Cada vez que el paquete llegue a un router este número se decrementará en 1 hasta llegar a 0 donde finalmente será desechado. De esta forma evitamos que un paquete este viajando de forma indefinida por la red.

10. ¿Qué protocolo se utiliza en la capa de enlace?

IPV4

11. ¿Cuál es la dirección física de destino? ¿A qué tipo de dispositivo crees que corresponde esta dirección física, un router, un switch, un hub, un equipo, ...? ¿Por qué? (Recuerda el servicio que proporciona la capa de enlace.)

La dirección física de destino es 50:64:2B:19:15:C7

12. ¿Cuál es la dirección física origen? ¿Qué compañía es el fabricante de la tarjeta de red a la que está asignada esta dirección física? ¿Cómo puedes obtener esta información?

La dirección física origen es 48:5F:99:02:76:B1

Para saber el fabricante de la tarjeta de red se utilizan los 6 primeros dígitos de la dirección MAC. En este caso la dirección física pertenece a Cloud Network Technology (Samoa).

13. ¿Qué protocolo se utiliza en la capa física? ¿Por qué?

Ethernet.

## **En el mensaje HTTP OK, en el que el Servidor Web te envía la página web solicitada:**

14. ¿Coinciden los números de puertos con los del mensaje HTTP GET correspondiente? ¿Por qué?

Sí, coinciden

15. ¿Cuál es la IP de tu equipo? ¿Es pública o privada?

En este caso la IP de mi equipo coincide con la dirección de destino del paquete 192.168.31.162  
Es privada ya que identifica al dispositivo conectado en nuestra red.

16. ¿Y la del servidor Web?

La dirección del servidor es 128.119.245.12

17. Indica brevemente la principal diferencia entre una IP pública y privada.

La IP pública es la dirección que identifica nuestra red desde el exterior, la del router que tenemos en casa. En cambio, la IP privada es la que identifica a cada uno de los dispositivos conectados a nuestra red. Esto quiere decir que todos los dispositivos conectados a nuestra red tienen diferentes direcciones IP privadas pero la misma pública

18. ¿Qué tecnología crees que está permitiendo que tus paquetes puedan acceder a Internet con “esa IP”? Explica brevemente su funcionamiento.

**Arranca de nuevo el capturador de mensajes y haz desde línea de comandos (Ejecutar-> cmd.exe) un ping a la nasa. Detén la captura de paquetes.**

```
C:\Users\Carmen>tracert www.nasa.gov

Tracing route to iznasa.hs.llnwd.net [87.248.222.209]
over a maximum of 30 hops:

  1    1 ms    1 ms    1 ms  10.20.48.1
  2    <1 ms   <1 ms   <1 ms  10.253.0.1
  3    1 ms    1 ms    1 ms  n111009.unileon.es [193.146.111.9]
  4    2 ms    <1 ms   <1 ms  n111003.unileon.es [193.146.111.3]
  5    2 ms    3 ms    3 ms  185.179.107.225
  6    3 ms    3 ms    2 ms  redcyl.xe5-3-0.uva.rt1.cyl.red.rediris.es [130.206.201.121]
  7    5 ms    6 ms    6 ms  uva.ae2.ciemat.rt1.mad.red.rediris.es [130.206.245.9]
  8    6 ms    5 ms    5 ms  limelight.baja.espanix.net [193.149.1.91]
  9   21 ms   24 ms   21 ms  lag14.fr3.cdg1.llnw.net [68.142.88.85]
 10   22 ms   22 ms   21 ms  vl2013.dr01.cdg1.llnw.net [185.178.52.15]
 11   22 ms   23 ms   21 ms  https-87-248-222-209.cdg1.llnw.net [87.248.222.209]

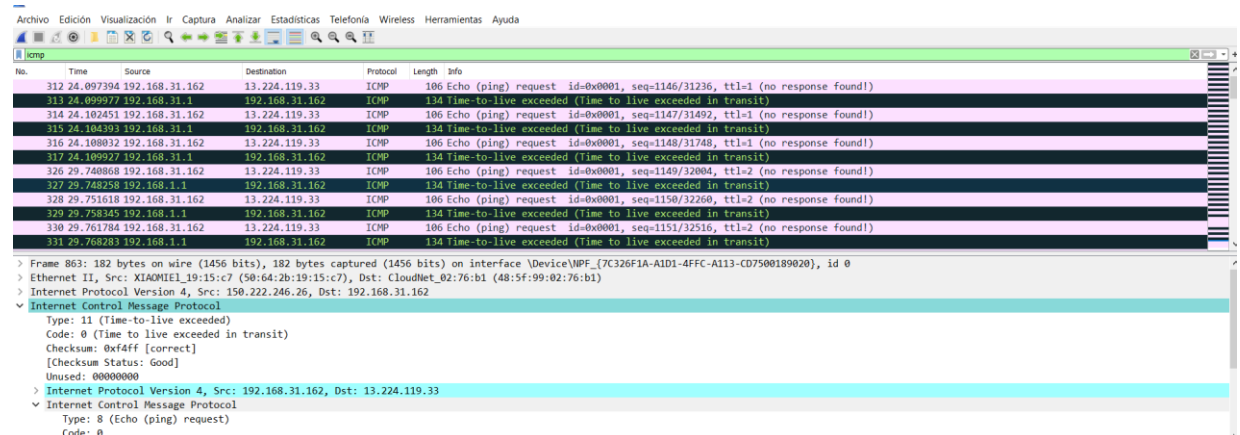
Trace complete.
```

19. Recuerda/investiga para qué sirve y cómo funciona el programa tracert.

Traceroute es una herramienta de diagnóstico que se inicia usando una línea de comandos y le informa al usuario sobre la ruta de un paquete de datos en la red. El programa determina el router y los nodos por los que pasó antes de llegar al host de destino. Además del número de estaciones, el usuario también recibe información sobre los tiempos de respuesta, y sobre aquellos puntos de la ruta donde se generó congestión. Traceroute también informa acerca de routers no alcanzados.

## 20. Analiza los mensajes ICMP que se han enviado/recibido.

Se reciben dos tipos de mensaje ICMP



## 21. ¿Qué tipos y códigos de ICMP identificas en los mensajes?

Aparecen dos tipos de mensajes ICMP. El primero es Echo Reply cuyo tipo es 8 y código es 0. El otro tipo es el de tiempo excedido cuyo tipo es el 11 y código 0.

## 22. Observa el campo Time to live de la capa de red, protocolo IP. ¿Cómo variando este campo desde el primer mensaje ICMP Request hasta el último? ¿Por qué?

El campo Time to live disminuye en una unidad antes de enviar el paquete al siguiente punto del camino. Por eso gracias al TTL podemos saber la cantidad de saltos que ha dado el paquete desde el origen hasta el destino. Aunque puede darse el caso de que el TTL llegue a 0 sin que el paquete haya llegado a su destino, en ese caso el router devolverá un mensaje ICMP de “Tiempo Agotado”.

## 23. Observa las direcciones físicas origen y destino de todos los mensajes ICMP Request enviados para realizar el tracert. ¿Cambian? ¿Por qué?

No.

## Redes- Comandos importantes

## 24. Abre un terminal. Indica el comando con el que visualizas la configuración básica de la red de tu equipo ¿Qué información te aporta y qué significa?

ipconfig

## 25. Ahora indica con qué comando visualizas más información sobre la configuración de red, por ejemplo, las IPs de los servidores DNS, la IP del servidor DHCP.

ipconfig/all

26. La IP de tu equipo es estática o dinámica. ¿Qué diferencia hay?

La IP estática se asigna de forma permanente a un dispositivo mientras que la IP dinámica es distinta cada vez que el dispositivo se conecta a internet. La IP de mi equipo es estática.

**Activa el capturador de WireShark y accede a [www.indipro.es](http://www.indipro.es) . Tras ello contesta a las siguientes preguntas:**

27. Filtra los paquetes capturados mediante http. ¿Puedes observar el acceso a la web citada anteriormente? En caso negativo ¿qué filtro deberías aplicar en Wireshark para ello?

No.

28. ¿Observas alguna diferencia entre las capturas http y la realizada en este dominio web? ¿Usan ambos el puerto 80?

No usan ambos el mismo puerto.