



GRUPO:	MIEMBROS:
	Orianna Milone, Paloma de Madrid, Carlos Moragón

Fecha límite entrega 23/10/2022

Enviar mediante campus virtual

1. Pasos previos

- *Wireshark* (www.wireshark.org). Existen versiones de este analizador de protocolos para Windows, Linux y otros sistemas operativos. Se recomienda leer la ayuda de *Wireshark* para familiarizarse con su utilización. En la web puede encontrarse también un manual de usuario. En distintos apartados de la práctica analizaremos el archivo **practica.pcap** publicado junto a este enunciado.

Nota: Desactivar la resolución de nombres MAC (Edit → Preferences → Name Resolution → Desactivar la primera casilla “*Resolve MAC addresses*” → *Apply*)



2. Funcionamiento de Wireshark

Abra el fichero de captura de ejemplo (practica3.pcap) y familiarícese con el entorno de *Wireshark*:

2.1. Ventana de lista de paquetes (*packet list*)

a) Explore la lista de paquetes utilizando los comandos del menú *Go* para navegar en ella. Anote el número de paquetes presentes en esta captura.

= Numero de paquetes: 2744

b) Observe los campos de la lista y note que la lista puede ordenarse por cada campo. ¿Cuál es el significado de los campos *Source* y *Destination*? ¿De dónde se obtiene dicha información? Anote el valor de estos campos para las tramas 53 y 54. ¿Son estos valores del mismo tipo en dichos paquetes? ¿Corresponden a algún tipo de dirección conocida?

=

Destination: dirección IP del destinatario.

Source: dirección IP desde donde se envía el paquete.

¿De dónde se obtiene dicha información?

Ambas direcciones vienen asignadas según la red de área local (a la que pertenezcan), seguido de esto cada red será “modificada” por los routers para asegurar que la dirección de IP sea privada.

52	2.742789	192.168.1.39	52.114.77.34	TCP	66 50427 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
53	2.877082	MitraSta_20:ce:cc	Broadcast	ARP	60 Who has 192.168.1.39? Tell 192.168.1.1
54	2.877118	IntelCor_de:f1:b1	MitraSta_20:ce:cc	ARP	42 192.168.1.39 is at 74:70:fd:de:f1:b1
55	2.881163	52.114.77.34	192.168.1.39	TCP	54 443 → 50374 [FIN, ACK] Seq=1 Ack=2 Win=1026 Len=0

53: source = MitraSta_20:ce:cc , destination = Broadcast

54: source = IntelCor_de:f1:b1 . destination = MitraSta_20:ce:cc

¿Son estos valores del mismo tipo en dichos paquetes?

Sí, si consideramos que ambas son IPv6

¿Corresponden a algún tipo de dirección conocida?

Sí, si las traducimos a IPv4 pertenecen a redes privadas, además llevan en común el protocolo ARP.

c) Observe el campo *Protocol* de los distintos paquetes. ¿Qué significa este campo? Anote el valor de este campo para los paquetes 28, 54, 176, 289 y 2586. ¿Corresponden al mismo nivel en la pila de protocolos?

El tipo de protocolo que transportan.

28: DHCP (nivel de aplicación)

54: ARP (nivel de red a nivel de enlace)

176: DNS (nivel de aplicación)

289: HTTP (nivel de aplicación)

2586: TCP (nivel de transporte)



Podemos concluir que no pertenecen a la misma pila.

d) Observe el campo *Info* de los distintos paquetes. ¿Cuál es su significado? Anote el valor de este campo para el paquete 53 y explique su significado.

Información adicional sobre los paquetes.

=

53: "who has 192.168.1.39 ? Tell 192.168.1.1"

Está enviando a todos los hosts de la red (vía broadcast) quien tiene la dirección MAC correspondiente a la IP 192.168.1.39 , y a dónde debe enviarla quien la tenga.

e) Explique por qué los paquetes de la lista se muestran con colores diferentes. Busque y explique qué son las *Coloring Rules*. ¿Por qué los paquetes números 2588 a 2590 se muestran del mismo color?

=

Los colores permiten diferenciar los distintos tipos de tráfico (generalmente se asocian a los protocolos que transportan).

Las reglas de coloreado indican el protocolo o los protocolos que llevan dicho paquete como TCP(violeta), TCP SYN/FIN (gris fuerte) o UDP(azul cielo)

2.2. Ventana de bytes del paquete (*Packet Bytes*)

a) Seleccione en la lista la trama número 217. Explique qué se muestra en la parte inferior de la pantalla (*packet bytes*). Redimensione dicho marco para ver su contenido completo.

= Se encuentra la información del paquete cifrada.

b) ¿Qué significa la columna de la izquierda? ¿En qué base de numeración están representados los valores de esta columna?

= El cifrado codificado en hexadecimal

c) ¿Y la columna de la derecha? ¿En qué formato código se muestran los valores de dicha columna? ¿Para qué puede ser esto útil?

= Esta cifrado en SSL, y es un protocolo del modelo OSI, que cifra la información.

2.3. Ventana de detalles del paquete (*Packet Details*)

a) Con la trama número 217 todavía seleccionada, observe la parte central de la pantalla (*packet details*). Explique qué representan las líneas que aparecen en esta ventana.

= Este panel muestra los protocolos y los campos de protocolo del paquete seleccionado en el panel "Lista de paquetes". Las líneas de resumen del protocolo y los campos del paquete se muestran en un árbol que se puede expandir y contraer.

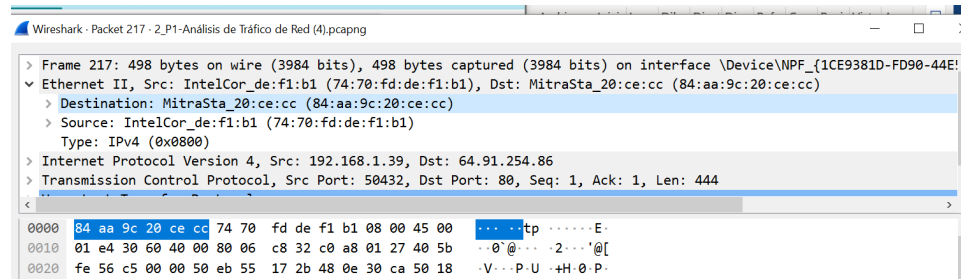
b) Seleccione la primera línea de la ventana de detalles del paquete. Observe los bytes resaltados en la ventana de bytes del paquete. ¿Cuántos son y qué representan dichos bytes?

= 498 bytes enviados y 498 bytes recibidos. Se refiere al flujo de bytes que puede pasar por el cable.



c) Repita el análisis del punto anterior para el resto de las líneas de la ventana de detalles del paquete. En la ventana inferior, ¿Qué representan los bytes resaltados? ¿Y los no resaltados?

= Al seleccionar una línea en específico, los bytes que se resaltan abajo, representan esa misma información, solo que se encuentra cifrada.





3. Encapsulamiento de protocolos

3.1. Para la trama 217 de la captura:

a) Realice un esquema del encapsulamiento que tiene lugar. Utilice para ello la información obtenida en la Ventana de detalles del paquete. Represente únicamente la cabecera de cada nivel (no especifique los campos de cada cabecera).

=
Aplicación: Hypertext Transfer Protocol

TCP: Transmission Control Protocol

IP: IPv4

Enlace: Ethernet II

Físico: frame 217

Aplicación va dentro de TCP, TCP va dentro de IP, IP va dentro de enlace y enlace va dentro del nivel físico.

b) Fíjese en la segunda línea de la ventana de detalles del paquete. ¿Cuáles son las direcciones origen y destino de la misma? ¿Qué tipo de información (protocolo) transporta dicha trama? ¿Cuál es su código de protocolo (*Ethertype*)?

Destination: MitraSta_20:ce:cc (84:aa:9c:20:ce:cc)

Source: IntelCor_de:f1:b1 (74:70:fd:de:f1:b1)

Type: IPv4 (0x0800)

c) Fíjese en la tercera línea de la ventana de detalles del paquete. ¿A qué protocolo transportado por la trama corresponde? Despliegue dicha línea y visualice los campos de la cabecera del paquete de dicho protocolo. Seleccione el campo de dirección destino. Indique su valor y los bytes correspondientes en la ventana de bytes del paquete. ¿Hay coincidencia entre ambos? ¿Qué tiempo valor tiene el campo TTL? ¿Qué significa? En caso de que el tamaño de la trama fuera superior a la MTU de una de las redes por las que tiene que transitar, ¿qué pasaría con la misma? ¿Por qué?

=

Destination address: 64.91.254.86

Los bytes correspondientes son: 40 5b fe 56

Sí hay correspondencia entre ambos sistemas. Estando los números de la dirección en base decimal y los bytes en base hexadecimal.

```
Internet Protocol Version 4, Src: 192.168.1.39, Dst: 64.91.254.86
Transmission Control Protocol, Src Port: 50432, Dst Port: 80, Seq: 1, Ack: 1, Len
  Source Port: 50432
  Destination Port: 80
  ... ..tp .....E
000 84 aa 9c 20 ce cc 74 70 fd de f1 b1 08 00 45 00 ... ..tp .....E
010 01 e4 30 60 40 00 80 06 c8 32 c0 a8 01 27 40 5b ..0`@...-2...@I
020 fe 56 c5 00 00 50 eb 55 17 2b 48 0e 30 ca 50 18 .V...P.U.+H.0.P
```

Protocolo UDP



TimeToLive (TTL): 128. Contador de los saltos que va dando el paquete, para que no se pierda en la red. En cada salto se resta 1 a dicho contador. En el caso de que llegue a 0, el paquete se descarta.

MTU; se refiere al Maximun Transfer Unit. Cada vez que el paquete pasa de una red a otra (cada una tendrá un tamaño máximo de unidad que pueda enviar), si el tamaño del paquete fuese superior, tendría que fragmentarse hasta que paquete a paquete pueda transitar.

d) Fíjese ahora en la cuarta línea de la ventana de detalles del paquete. ¿A qué protocolo transportado por la trama corresponde? Despliegue dicha línea y visualice los campos de la cabecera del paquete de dicho protocolo.

Protocolo transportado: TCP

e) Seleccione el campo de puerto destino en la cabecera anterior. Indique su valor y los bytes correspondientes en la ventana de bytes del paquete. ¿Hay coincidencia? ¿Relaciona este valor con algún servicio estándar en Internet?

Destination port: 80 Bytes(00 50) Sí hay correspondencia entre el decimal y el hexadecimal.

Es un puerto por defecto para un servicio web con un protocolo HTTP no seguro.

f) Por último, fíjese en la quinta línea de la ventana de detalles de la misma trama. ¿A qué protocolo transportado por la trama corresponde? Despliegue dicha línea y visualice los campos de la cabecera del paquete de dicho protocolo. Examinando dichos campos, realice una hipótesis sobre qué tipo de mensaje se trata y su significado dentro del protocolo en cuestión.

Protocolo: HTTP (El Protocolo de transferencia de hipertexto (en inglés, *Hypertext Transfer Protocol*, abreviado HTTP) es el protocolo de comunicación que permite las transferencias de información a través de archivos (XML, HTML...) en la World Wide Web.)

Se trata de una solicitud a la página web www.hablemosderelojes.com

4. Filtrado de paquetes

4.1. Tráfico DNS

Vamos a estudiar el tráfico de DNS (*Domain Name System*) intercambiado

a) Realizar un filtro de visualización para analizar este tráfico. ¿Cuántos paquetes de la captura corresponden al mismo? ¿Cuál es la IP de en qué número de paquete se obtiene?

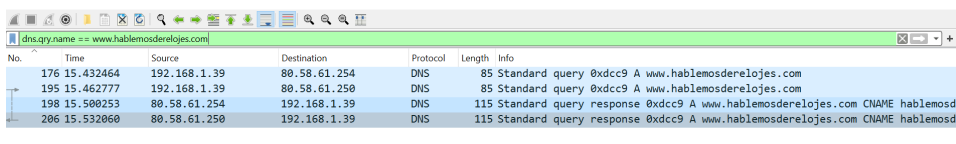
Filtro utilizado: dns

The screenshot shows the Wireshark interface with a filter applied to 'dns'. The packet list displays several DNS packets. The selected packet is a standard query response from 192.168.1.39 to 80.58.61.254. The packet details pane shows the query structure, including the question section with a PTR record for 1.144.168.192.in-addr.arpa. The packet bytes pane shows the raw data of the packet.



A ese filtro pertenecen 96 paquetes.

Filtro: dns.qry.name == www.hablemosderejes.com



No.	Time	Source	Destination	Protocol	Length	Info
176	15.432464	192.168.1.39	80.58.61.254	DNS	85	Standard query 0xdcc9 A www.hablemosderejes.com
195	15.462777	192.168.1.39	80.58.61.250	DNS	85	Standard query 0xdcc9 A www.hablemosderejes.com
198	15.500253	80.58.61.254	192.168.1.39	DNS	115	Standard query response 0xdcc9 A www.hablemosderejes.com CNAME hablemosd...
206	15.532060	80.58.61.250	192.168.1.39	DNS	115	Standard query response 0xdcc9 A www.hablemosderejes.com CNAME hablemosd...

A este filtro corresponden 4 paquetes.

Hemos encontrado la IP de www.hablemosderejes.com. Haciendo un ping

```
C:\> Símbolo del sistema

Microsoft Windows [Versión 10.0.19043.2130]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\LENOVO>ping www.hablemosderejes.com

Haciendo ping a relojes.discoursehosting.net [138.68.102.202] con 32 bytes de datos:
Respuesta desde 138.68.102.202: bytes=32 tiempo=33ms TTL=51
Respuesta desde 138.68.102.202: bytes=32 tiempo=36ms TTL=51
Respuesta desde 138.68.102.202: bytes=32 tiempo=35ms TTL=51
Respuesta desde 138.68.102.202: bytes=32 tiempo=38ms TTL=51

Estadísticas de ping para 138.68.102.202:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 33ms, Máximo = 38ms, Media = 35ms
```

IP: 138.68.102.202

b) Analizar el Encapsulamiento de este servicio. ¿En que puerto escuchan los servidores de DNS?

Puerto 53

c) Realizar un nuevo filtro de visualización, utilizando ahora como condición que el puerto de destino sea el del servidor de DNS. ¿Visualiza ahora todo el tráfico de este servicio? ¿Por qué? Identificar los servidores de DNS a los que se están lanzando las peticiones, indicando en qué direcciones IP se encuentran.

Filtro utilizado: udp.dstport0053

80.58.61.254

80.58.61.250

d) ¿Que se solicita en la trama 295?

Se solicita ir a la página www.gmodules.com

4.2. Tráfico ARP

Una manera de identificar los diferentes equipos presentes en la red es analizando el tráfico ARP (*Address Resolution Protocol*). A partir de estos paquetes vamos a estudiar las características de la red en la que se ha realizado esta captura.

a) Realizar un filtro de visualización para el tráfico ARP. ¿Cuántos paquetes de la captura corresponden a este protocolo? Aunque no podemos estudiar la máscara de esta red, ¿Qué direccionamiento intuye que se está utilizando?



Filtro utilizado: arp

Número de paquetes: 4.

Direccionamiento: Privado.

b) Uno de los *hosts* identificados es el router de salida a Internet. ¿En qué dirección IP se encuentra? (puede analizar los paquetes dirigidos a alguna dirección IP externa a nuestra red, cualquiera de las que ya se han identificado a lo largo de la práctica; mediante ARP será posible identificar la IP de este router). Indicar claramente el proceso seguido: tramas analizadas e información obtenida

84:aa:9c:20:ce:cc

Hemos filtrado con “arp”. Y analizado la línea con dirección destino broadcast. Dentro de las especificaciones del paquete hemos hallado la IP.

c) Explique el significado de las tramas 53 y 54:

En la trama 53 se pide por medio del protocolo ARP vía broadcast cual es la dirección MAC correspondiente a esta IP 192.168.1.39. Y que le envíen la respuesta a la dirección 192.168.1.1

La trama 54 envía la respuesta.

4.3. Tráfico ICMP

Vamos a estudiar el tráfico de ICMP.

a) Realizar un filtro de visualización para el tráfico ICMP. ¿Cuántos paquetes de la captura corresponden a este protocolo?

Filtro: icmp

Número de paquetes: 36

b) Se observan mensajes ICMP del tipo “Echo Request” y “TTL Exceeded in transit”, ¿Qué significan y a quien van dirigidos? ¿Qué prueba se estaría realizando que generan esos mensajes?

Echo Request: va dirigido al 8.8.8.8 es decir google. Está haciendo un ping.

TTL Exceeded in transit: va dirigido a la 192.68.1.39. Significa que se han agotado los saltos.

Realizar Captura de tráfico

Para capturar tráfico en Wireshark es necesario cerrar el archivo de captura. Se debe seleccionar el interface de red en el que vamos a hacer la captura. Es posible definir un filtro para limitar las tramas capturadas, aunque no se recomienda filtrar en esta fase y hacerlo posteriormente en la fase de visualización.

Nota: es posible configurar más opciones de captura en el menú *Capture → Options* (Ctrl+K)

4.4. Tráfico ICMP

Vamos a analizar el modo de operación que usan las herramientas de trazado (*traceroute* o *tracert*) para visualizar la ruta hacia un *host* destino. Para ello necesitamos una conexión de red sin restricciones de



salida hacia Internet y trazaremos el camino hacia el host con dirección 151.101.133.50. Podemos lanzar el comando desde la máquina anfitriona o desde una máquina virtual, y capturaremos un archivo con todo el tráfico intercambiado.

Se recomienda no convertir las direcciones IP en nombres (opciones -n o -d, por ejemplo en CMD: tracert -d 151.101.133.50)

a) Adjuntar en la memoria un pantallazo con el resultado obtenido del trazado ¿Cuántos saltos tiene que dar el datagrama hasta alcanzar el destino? ¿Son direcciones públicas o privadas? ¿Que significa cuando aparece *?

```
C:\Users\cmora>tracert -d 151.101.133.50

Traza a 151.101.133.50 sobre caminos de 30 saltos como máximo.

 1  10 ms    6 ms    4 ms  192.168.4.1
 2  26 ms    7 ms    6 ms  192.168.1.1
 3  22 ms    *      13 ms  192.168.144.1
 4  *        37 ms   8 ms  81.46.65.21
 5  *        *      *      Tiempo de espera agotado para esta solicitud.
 6  *        *      *      Tiempo de espera agotado para esta solicitud.
 7  9 ms     9 ms   11 ms  216.184.113.180
 8  *        *      *      Tiempo de espera agotado para esta solicitud.
 9  11 ms    16 ms   8 ms  151.101.133.50

Traza completa.
```

Ha tomado 9 saltos.

Del 1-3 hay direcciones privadas

Para la 4, 7, 9 son públicas.

Cuando aparece *, significa que el tiempo de espera se ha agotado para la solicitud, a su vez, esto significa que el contador de saltos para esos paquetes se ha agotado.

b) Indicar el número total de mensajes ICMP intercambiados ¿De qué tipo son los mensajes ICMP? ¿Ha aplicado algún filtro para facilitar el análisis?

Filtro: icmp

43 mensajes ICMP

Tipos de mensajes ICMP:

Time to live exceeded

Echo (ping) request

Echo (ping) replay

c) A la vista de los resultados obtenidos describir el proceso que siguen los comandos de trazado (traceroute o tracert) para obtener la ruta hacia un destino ¿Qué característica tiene los datagramas intercambiados?



Hemos analizado el recorrido desde el primer salto hasta el destino (151.101.133.50).

Durante los primeros tres saltos, hemos deducido que el paquete viaja entre una misma red de área local -hace saltos dentro de la misma red privada-, en el cuatro salto, cuando debe hacerlo a una red pública, hemos entendido que hay un retraso, pero si logra completar el salto. Es probable que ahora que el paquete se encuentra saltando de redes públicas entre redes públicas ha excedido el tiempo de espera tanto en el 5to como el 6to salto. Para el 7mo salto ya ha ubicado a donde debe llegar, aunque volverá a exceder su tiempo (buscando la mayor coincidencia en las tablas, para saltar a la dirección deseada). En el noveno salto finalmente llega.

Todos los datagramas que son intercambiados poseen la misma característica, y es que su valor de "protocol = 1"

d) Lance un PING a la IP destino 151.101.133.50 de tamaño 10000 bytes. Localice el fragmento en el que está la cabecera del mensaje ICMP (adjunte captura de pantalla significativa).

```
Traza completa.  
C:\Users\cmora>ping 151.101.133.50 -l 1000  
  
Haciendo ping a 151.101.133.50 con 1000 bytes de datos:  
Respuesta desde 151.101.133.50: bytes=1000 tiempo=14ms TTL=56  
Respuesta desde 151.101.133.50: bytes=1000 tiempo=9ms TTL=56  
Respuesta desde 151.101.133.50: bytes=1000 tiempo=7ms TTL=56  
Respuesta desde 151.101.133.50: bytes=1000 tiempo=17ms TTL=56  
  
Estadísticas de ping para 151.101.133.50:  
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
    (0% perdidos),  
    Tiempos aproximados de ida y vuelta en milisegundos:  
        Mínimo = 7ms, Máximo = 17ms, Media = 11ms  
  
C:\Users\cmora>
```

Ping 11 ms

e) ¿Por qué no se recibe ninguna respuesta hasta que el destino no ha recibido todos los fragmentos en lugar de contestar uno a uno?

Porque por el protocolo IP almacena en una memoria temporal todos los fragmentos recibidos hasta que tenerlos todos, y si no ha excedido el tiempo se reensamblan en el destino, mandando la respuesta al final.