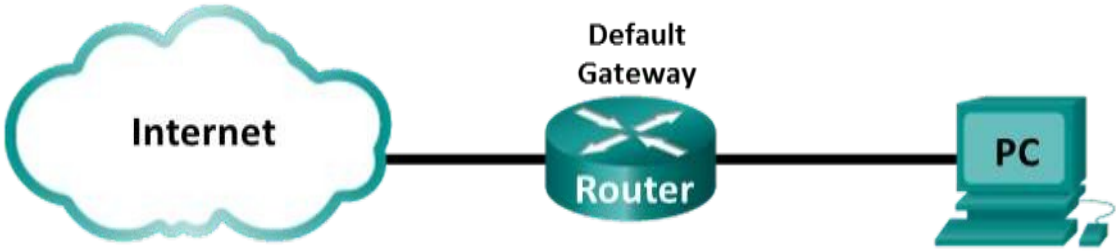
Lab – Using Wireshark to Examine Ethernet Frames

Topology



Objetivos

Part 1: Examinar los campos cabecera de una trama Ethernet II

Part 2: Usar Wireshark para capturar y analizar tramas Ethernet

Conocimiento / Escenario

Cuando protocolos de capa superior comunican entre ellos, los datos fluyen de arriba hacia abajo a través de las capas modelo OSI (Open Systems Interconnection) y son encapsulados en la trama de la capa 2.
La composición de la trama es dependiente del tipo de acceso al medio. Por ejemplo, si los protocolos de las capas superiores son TCP e IP y el acceso al medio es Ethernet, entonces la encapsulación de las tramas en el nivel 2 será Ethernet ll. Esto es típico de las redes LAN.

Recursos requeridos

- 1 PC (Linux Mint) con acceso a Internet y el software Wireshark instalado.

Parte 1: Examinar la cabecera de los campos en una trama Ethernet.

En la Parte 1, examinaras los campos de la cabecera y su contenido en una trama Ethernet ll

Paso 1: Revisar las descripciones de la cabecera de la trama Ethernet ll y su longitud.

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Paso 2: Examinar la configuración de red del PC.

Este PC contiene la dirección de IP 192.168.1.17 y la puerta de enlace es la IP 192.168.1.1.

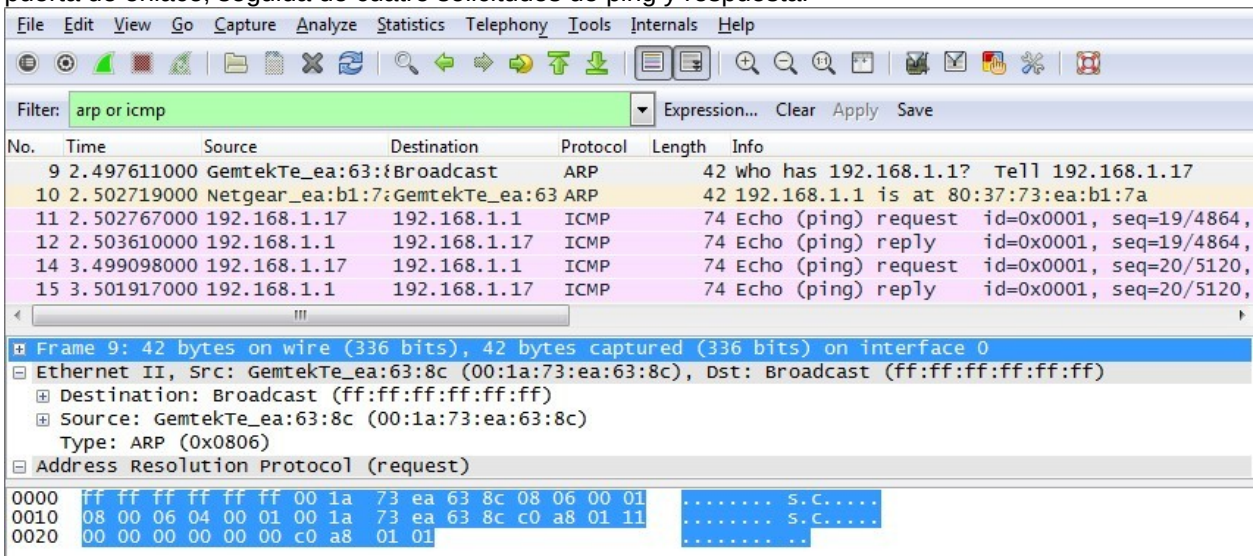
```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom 802.11a/b/g WLAN
   Physical Address. . . . . . . . . : 00-1A-73-EA-63-8C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.17(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, June 16, 2015 6:59:54 AM
   Lease Expires . . . . . . . . . . : Wednesday, June 17, 2015 6:59:54 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 234887795
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-07-0A-E1-00-1E-EC-15-74-C2

   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Paso 3: Examinar trama Ethernet en una captura Wireshark.

La captura de Wireshark a continuación muestra los paquetes generados por un ping que se emite desde un host de PC a su puerta de enlace predeterminada. Se ha aplicado un filtro a Wireshark para ver solo los protocolos ARP e ICMP. La sesión comienza con una consulta ARP para la dirección MAC del enrutador de puerta de enlace, seguida de cuatro solicitudes de ping y respuesta.



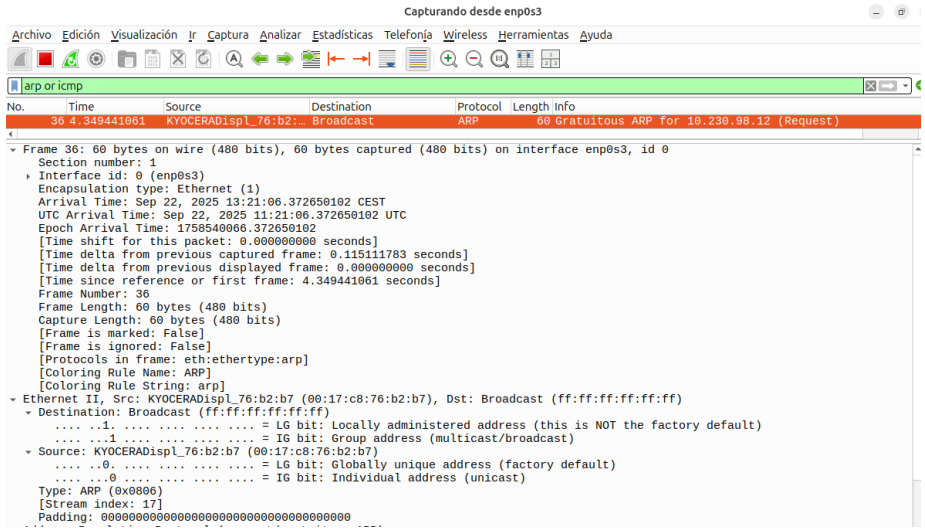
Paso 4: Examinar el contenido de la cabecera Ethernet II de una petición ARP.

En la tabla siguiente se toma la primera trama de la captura de Wireshark y se muestran los datos en los campos de encabezado Ethernet II

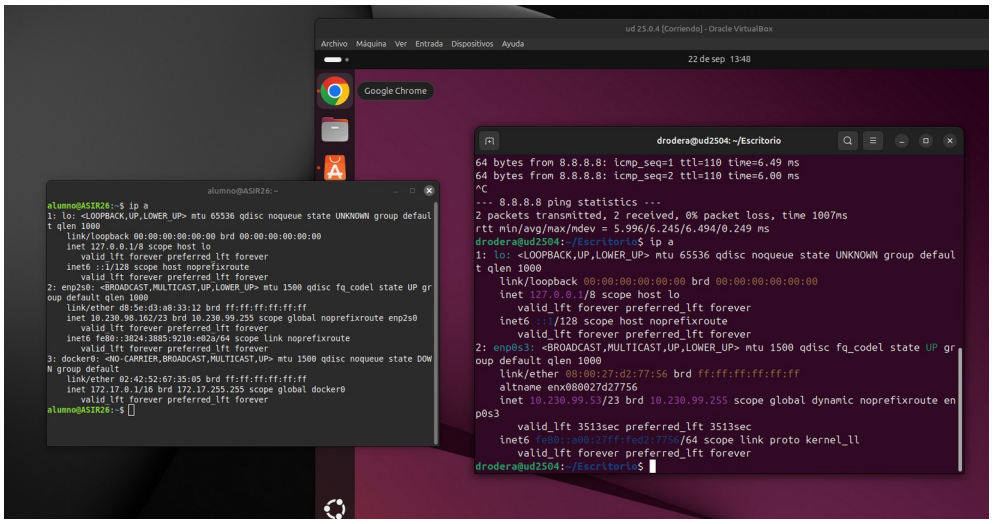
Field	Value	Description
Preamble	No mostrado en esta captura	Contiene bits de sincronización procesados por la tarjeta de red (NIC hardware).
Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)	Direcciones de capa 2 para el marco. Cada dirección tiene 48 bits de largo, o 6 octetos, expresados como 12 dígitos hexadecimales, 0-9, A-F. Un formato común es 12:34:56:78:9A:BC. Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC), los últimos seis números son el número de serie de la NIC. La dirección de destino puede ser una emisión, que contiene todas, o una unidifusión. La dirección de origen es siempre unicast.
Source Address	GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)	
Frame Type	0x0806	Para las tramas Ethernet II, este campo contiene un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior en el campo de datos. Existen numerosos protocolos de capa superior compatibles con Ethernet II. Dos tipos de marcos comunes son: Descripción del valor 0x0800 Protocolo IPv4 0x0806 protocolo de resolución de direcciones (ARP)
Data	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos está entre 46 – 1.500 bytes.
FCS	Not shown in capture	Frame Check Sequence, usado por la NIC para identificar errores durante la transmission. Este campo es enviado por el emisor y verificado por el receptor.

Paso 5. ¿Cuáles son los datos desde tu máquina?

Adjunta una captura de tu trama y muestra los campos más destacados de la misma.



En esta última captura se muestra que tanto el ordenador como la máquina virtual están en la misma red.



Paso 6. ¿Te diste cuenta?

¿Qué tiene de significativo el contenido del campo de dirección de destino?

Significa que el mensaje ARP es enviado a todas la IP de la red, (es broadcast) porque aún no conoce la mac de la IP 10.230.98.12

¿Por qué el PC envía un ARP de difusión antes de enviar la primera solicitud de ping?

Porque antes de mandar el paquete el ordenador necesita la MAC del gateway, y para eso tiene que preguntar a toda la red con un ARP broadcast.

¿Cuál es la dirección MAC de la fuente en la primera trama?

La dirección MAC es 00:17:c8:76:b2:b7.

¿Cuál es el ID de proveedor (OUI) de la NIC del origen? ¿Qué parte de la dirección MAC es la OUI?

Es 00:17:c8. Son los tres primeros octetos de la dirección MAC.

¿Cuál es el número de serie NIC de la fuente?

Es 76:b2:b7.

Parte 2: Usa Wireshark para capturar y analizar trazas Ethernet

En la Parte 2, utilizará Wireshark para capturar tramas Ethernet locales y remotas. A continuación, examinará la información contenida en los campos de encabezado del marco.

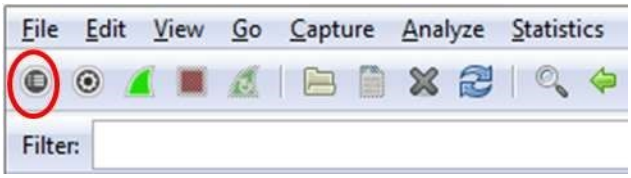
Paso 1: Determina la dirección IP de la puerta de enlace por defecto de tu PC.

Abra una ventana del símbolo del sistema y emita el comando “ip a”. ¿Cuál es la dirección IP de la puerta de enlace predeterminada de PC?

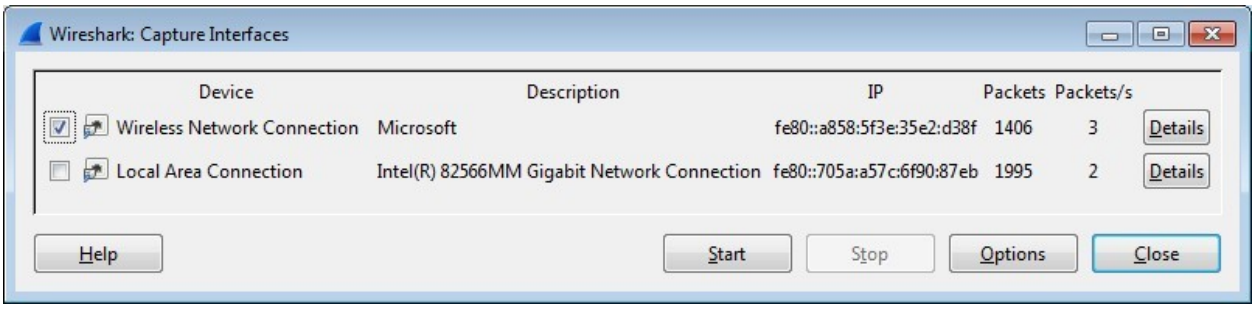
Es 10.230.98.1.

Paso 2: Comienza capturando tráfico en la tarjeta de red de tu PC.

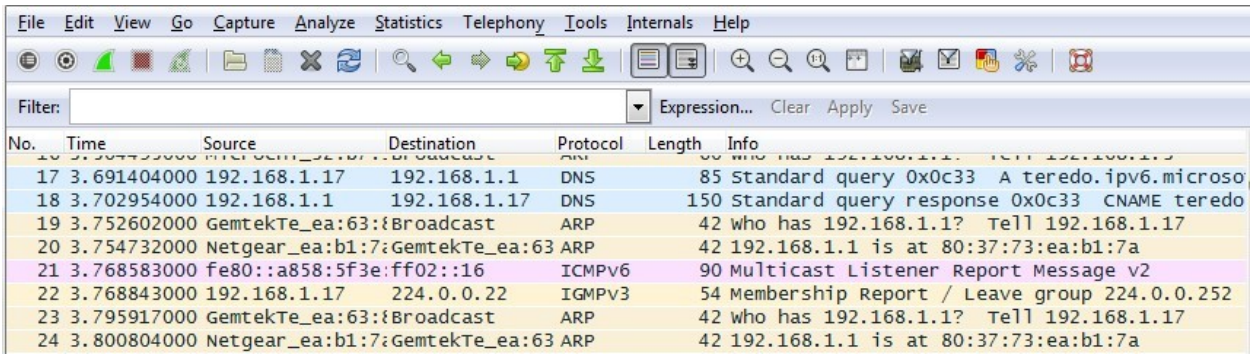
a. Abrir Wireshark
b. Sobre la barra de superior, clicar en la lista de interfaces



c. En la ventana Wireshark: Interfaces de captura, seleccione la interfaz para iniciar la captura de tráfico haciendo clic en la casilla de verificación correspondiente y, a continuación, haga clic en Iniciar. Si no está seguro de qué interfaz comprobar, haga clic en Detalles para obtener más información acerca de cada interfaz enumerada.



d. d. Observe el tráfico que aparece en la ventana Lista de paquetes.



Paso 3: Filtrar Wireshark para visualizar tráfico ICMP

Puede usar el filtro en Wireshark para bloquear la visibilidad del tráfico no deseado. El filtro no bloquea la captura de datos no deseados; solo filtra qué mostrar en pantalla. Por ahora, solo mostrará el tráfico ICMP.

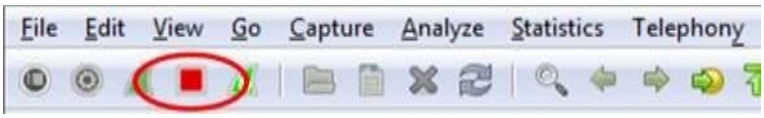
En el cuadro Filtro wireshark, escriba icmp. El cuadro debe ponerse verde si ha escrito el filtro correctamente. Si el cuadro es verde, haga clic en Aplicar para aplicar el filtro.

Paso 4: Desde la terminal, haga un ping a la Puerta de enlace de su PC.

En la ventana de comandos, haga ping a la puerta de enlace predeterminada con la dirección IP que registró en el paso 1.

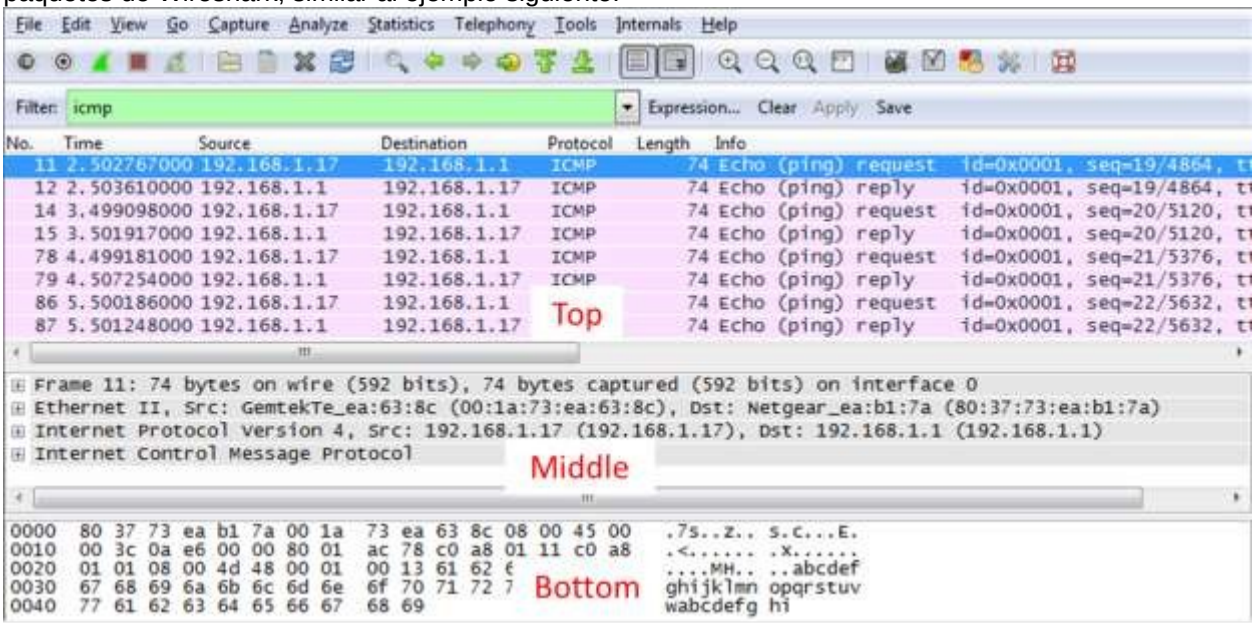
Paso 5: Para capturas de tráfico de red sobre el adaptador NIC.

Hacer Click en el icono Parar Captura (**Stop Capture)** para parar la captura de tramas.



Paso 6: Examina la primera petición Echo (ping) en Wireshark.

La ventana principal de Wireshark se divide en tres secciones: el panel Lista de paquetes (arriba), el panel Detalles del paquete (centro) y el panel Bytes de paquetes (abajo). Si seleccionó la interfaz correcta para la captura de paquetes en el paso 3, Wireshark debería mostrar la información ICMP en el panel Lista de paquetes de Wireshark, similar al ejemplo siguiente.



a. En el panel Lista de paquetes (sección superior), haga clic en el primer fotograma de la lista. Debería ver la solicitud de eco (ping) en el encabezado Información. Esto debería resaltar la línea azul.

b. Examine la primera línea en el panel Detalles del paquete (sección central). Esta línea muestra la longitud del marco; 74 bytes en este ejemplo.

¿Cuál es la dirección MAC de la NIC de la PC?

08:00:27:be:16:62.

¿Cuál es la dirección MAC de la puerta de enlace predeterminada?

08:00:27:d2:77:56.

c. Puede hacer clic en el signo más (+) al comienzo de la segunda línea para obtener más información sobre la trama de Ethernet II. Observe que el signo más cambia a un signo menos (-).

¿Qué tipo de marco se muestra?

El marco muestra una trama identificada por el campo "Type" con el número 0x0800, el cual indica que esta trasportando un paquete IPv4. Este apartado contiene la MAC de origen y de destino, las cuales solo se pueden usar para comunicaciones entre dispositivos de la misma red local.

d. Las dos últimas líneas que se muestran en la sección central proporcionan información sobre el campo de datos del marco.

Observe que los datos contienen la información de la dirección IPv4 de origen y destino.

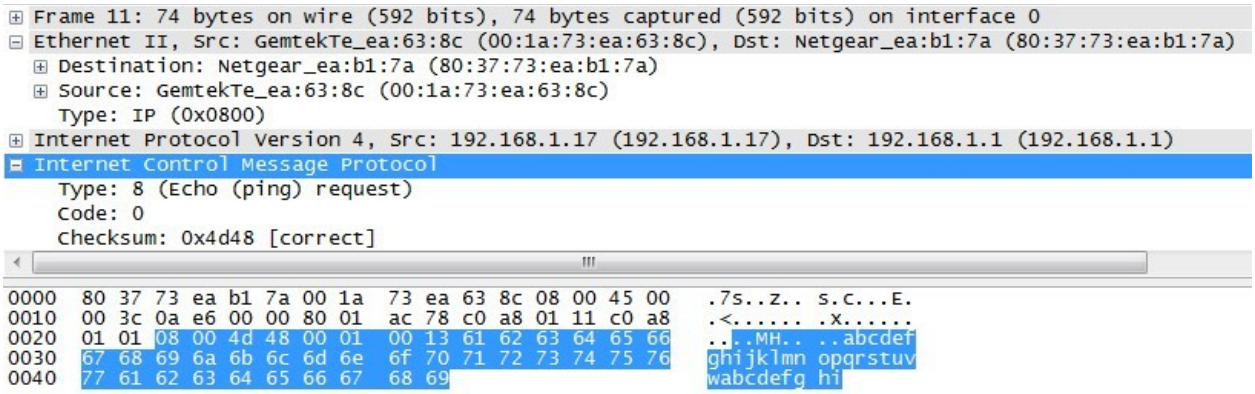
¿Cuál es la dirección IP de origen?

10.230.99.217

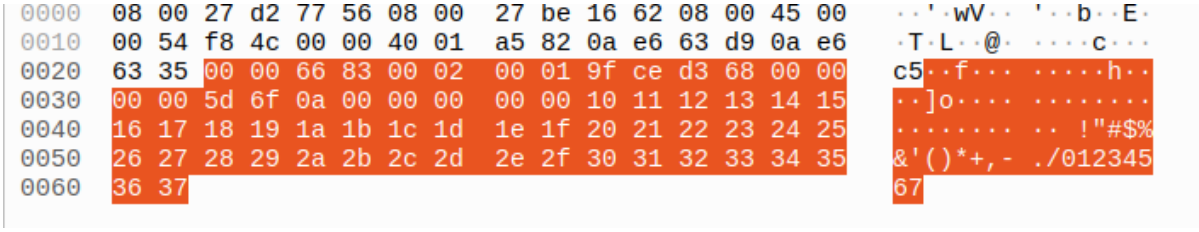
¿Cuál es la dirección IP de destino?

10.230.99.53

e. Puede hacer clic en cualquier línea de la sección central para resaltar esa parte del marco (hexadecimal y ASCII) en el panel de bytes del paquete (sección inferior). Haga clic en la línea Protocolo de mensajes de control de Internet en la sección central y examine lo que está resaltado en el panel Bytes de paquetes.



¿Qué deletrean los dos últimos octetos resaltados?



Significa:

0x36 → carácter ASCII “6”

0x37 → carácter ASCII “7”

f. Haga clic en el siguiente cuadro en la sección superior y examine un cuadro de respuesta de Echo. Observe que las direcciones MAC de origen y destino se han invertido, porque esta trama se envió desde el enrutador de puerta de enlace predeterminado como respuesta al primer ping.

¿Qué dispositivo y dirección MAC se muestra como dirección de destino?

08:00:27:d2:77:56.

Paso 7: reinicie la captura de paquetes en Wireshark.

Haga clic en el icono Iniciar captura para iniciar una nueva captura de Wireshark. Recibirá una ventana emergente que le preguntará si desea guardar los paquetes capturados anteriormente en un archivo antes de comenzar una nueva captura. Haga clic en Continuar sin guardar

Paso 8: En la ventana del símbolo del sistema, haga ping a www.cisco.com.

```
drodera@ud2504:~/Escritorio$ ping www.cisco.com
PING e2867.dsca.akamaiedge.net (2.17.153.67) 56(84) bytes o
f data.
64 bytes from a2-17-153-67.deploy.static.akamaitechnologies
.com (2.17.153.67): icmp_seq=1 ttl=50 time=6.92 ms
64 bytes from a2-17-153-67.deploy.static.akamaitechnologies
.com (2.17.153.67): icmp_seq=2 ttl=50 time=6.83 ms
64 bytes from a2-17-153-67.deploy.static.akamaitechnologies
.com (2.17.153.67): icmp_seq=3 ttl=50 time=6.97 ms
64 bytes from a2-17-153-67.deploy.static.akamaitechnologies
.com (2.17.153.67): icmp_seq=4 ttl=50 time=6.89 ms
64 bytes from a2-17-153-67.deploy.static.akamaitechnologies
.com (2.17.153.67): icmp_seq=5 ttl=50 time=6.73 ms
^C
--- e2867.dsca.akamaiedge.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 403
9ms
rtt min/avg/max/mdev = 6.729/6.867/6.973/0.084 ms
```

Paso 9: Deje de capturar paquetes.

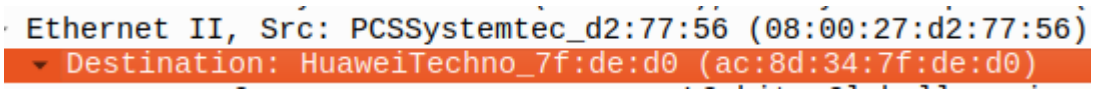
Paso 10: Examine los nuevos datos en el panel de la lista de paquetes de Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
277	35.801389026	10.230.99.53	2.17.153.67	ICMP	98	Echo (pi
278	35.808287268	2.17.153.67	10.230.99.53	ICMP	98	Echo (pi
283	36.807700159	10.230.99.53	2.17.153.67	ICMP	98	Echo (pi
285	36.814473416	2.17.153.67	10.230.99.53	ICMP	98	Echo (pi
292	37.828263979	10.230.99.53	2.17.153.67	ICMP	98	Echo (pi
293	37.835196396	2.17.153.67	10.230.99.53	ICMP	98	Echo (pi
299	38.830601243	10.230.99.53	2.17.153.67	ICMP	98	Echo (pi
300	38.837475394	2.17.153.67	10.230.99.53	ICMP	98	Echo (pi
312	39.840652436	10.230.99.53	2.17.153.67	ICMP	98	Echo (pi
313	39.847367651	2.17.153.67	10.230.99.53	ICMP	98	Echo (pi

En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y destino?

Origen: **08:00:27:d2:77:56**

Destino: **ac:8d:34:7f:de:d0**



¿Cuáles son las direcciones IP de origen y destino contenidas en el campo de datos del marco?

Origen: **10.230.99.53**

Destino: **2.17.153.67**

Compare estas direcciones con las direcciones que recibió en el Paso 6.

La única dirección que cambió es la dirección IP de destino. ¿Por qué ha cambiado la dirección IP de destino, mientras que la dirección MAC de destino sigue siendo la misma?

Porque la dirección MAC siempre va a ser la del router porque es por donde pasa la información. En cambio la dirección IP no es la misma porque necesita saber el destinatario final para transmitir la información.