

PROTOCOLOS ETHERNET Y ARP – LABORATORIO WIRESHARK

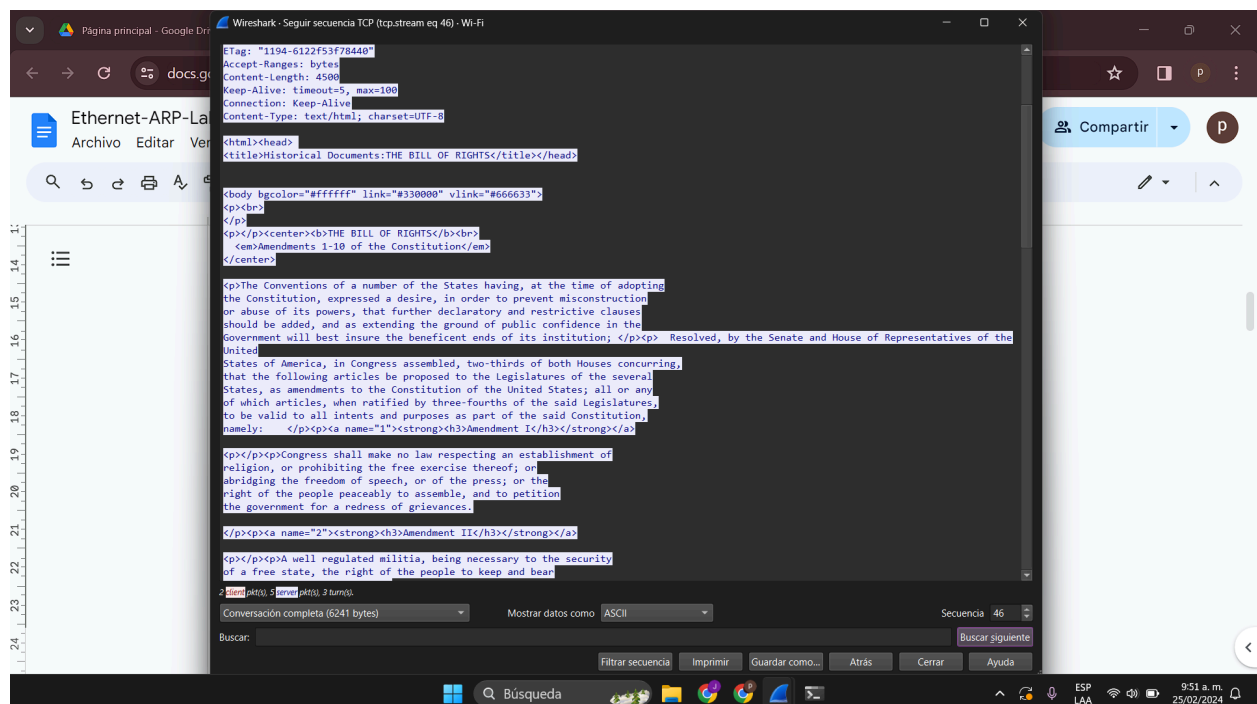
Grupo: Julio Prado, Martín Gómez, Daniel Plazas, Danna López

En el presente laboratorio estudiaremos los protocolos Ethernet y ARP. Esto con el fin de reforzar los conceptos que se estudiaron en clases pasadas.

CAPTURA DE PAQUETES

Emplearemos una captura de una navegación a una página web para analizar las tramas Ethernet. Para este propósito:

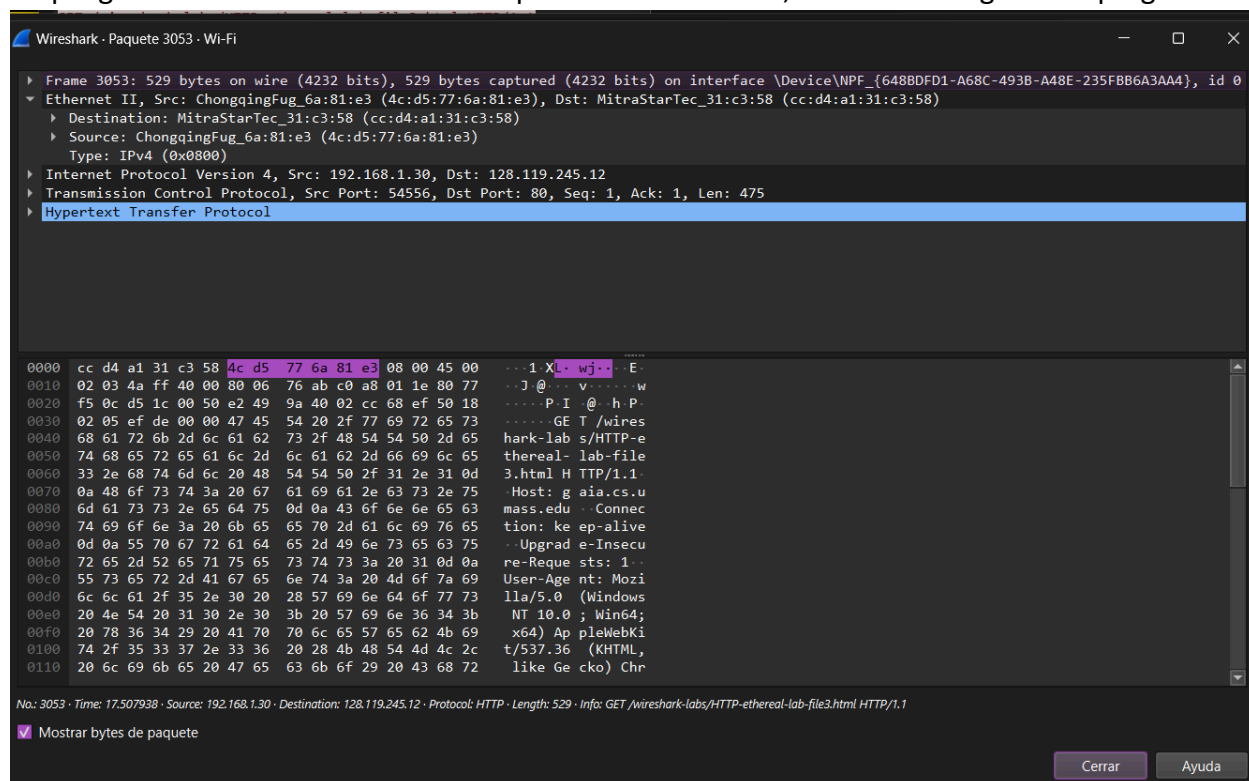
- Limpie el caché de su navegador.
- Abra Wireshark, e inicie la captura por el adaptador de red adecuado.
- Acceda a la siguiente URL en su navegador:
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>
- Detenga la captura.
- Filtre ahora por la dirección IP del servidor remoto. Averigüe la dirección ejecutando el siguiente comando en consola: `nslookup gaia.cs.umass.edu`
- Haga clic derecho sobre uno de los paquetes de la captura, y elija la opción Follow -> TCP Stream
- Wireshark desplegará los paquetes correspondientes a la conexión al servidor y a la descarga de la página web.



ANÁLISIS DE LAS TRAMAS ETHERNET

En este punto, emplee la trama que contiene el comando HTTP GET (suele ser la cuarta trama, selecciónela y verifique en el panel inferior de la ventana, donde aparece el CONTENIDO de los paquetes, que aparezca la orden GET).

Ahora, vaya al panel intermedio de la ventana (que muestra la jerarquía de protocolos) y despliegue el encabezado Ethernet. Empleando dicha trama, conteste las siguientes preguntas:



1. ¿Cuál es la dirección Ethernet (48 bits) fuente? ¿A cuál equipo corresponde? ¿Cómo puede comprobarlo?

// La dirección ethernet fuente es ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3), corresponde a la laptop del compañero Julio, se puede comprobar ejecutando el comando get-netadapter en la consola, obteniendo la dirección Mac del Wi-Fi (pues hicimos la captura de paquetes por medio Wi-Fi) y finalmente comparando con la que da Wireshark. En este caso coincide al ser 4c:d5:77:6a:81:e3.

```
PS C:\Users\julio> get-netadapter
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
Ethernet 2	VirtualBox Host-Only Ethernet Adapter	17	Up	0A-00-27-00-00-11	1 Gbps
Conexión de red Bluetooth	Bluetooth Device (Personal Area Netw...	13	Disconnected	4C-D5-77-6A-81-E4	3 Mbps
Wi-Fi	MediaTek Wi-Fi 6 MT7921 Wireless LAN...	12	Up	4C-D5-77-6A-81-E3	866.7 Mbps

2. ¿Cuál es la dirección Ethernet de destino? ¿Corresponde a la dirección Ethernet de gaia.cs.umass.edu? En caso negativo, ¿a qué equipo corresponde esta dirección Ethernet?

```
entries and entries on the loop-back interface will be shown.
inet_addr      Specifies an internet address.
-N if_addr     Displays the ARP entries for the network interface specified
               by if_addr.
-d            Deletes the host specified by inet_addr. inet_addr may be
               wildcarded with * to delete all hosts.
-s            Adds the host and associates the Internet address inet_addr
               with the Physical address eth_addr. The Physical address is
               given as 6 hexadecimal bytes separated by hyphens. The entry
               is permanent.
eth_addr       Specifies a physical address.
if_addr        If present, this specifies the Internet address of the
               interface whose address translation table should be modified.
               If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.
PS C:\Users\agaza> arp -a 128.119.245.12
No ARP Entries Found.
PS C:\Users\agaza> ping 128.119.245.12

Pinging 128.119.245.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 128.119.245.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\agaza> |
```

// La dirección ethernet de destino es MitraStarTec_31:c3:58 (cc:d4:a1:31:c3:58) corresponde al servidor de Gaia.

3. ¿Cuál es el valor del tipo de trama? ¿Qué indica este valor?

```

Type: IPv4 (0x0800)
0000 cc d4 a1 31 c3 58 4c d5 77 6a 81 e3 08 00 45 00 ...1·XL· wj·...·E·
0010 02 03 4a ff 40 00 80 06 76 ab c0 a8 01 1e 80 77 ...J·@·... v·...·w
0020 f5 0c d5 1c 00 50 e2 49 9a 40 02 cc 68 ef 50 18 ...·P·I· ·@··h·P·
0030 02 05 ef de 00 00 47 45 54 20 2f 77 69 72 65 73 ...·GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 hark-lab s/HTTP-e
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 thereal- lab-file
0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 3.html H TTP/1.1
0070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 ·Host: g aia.cs.u
0080 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 mass.edu ·Connec
0090 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive
00a0 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ·Upgrad e-Insecu
00b0 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Reque sts: 1·
00c0 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
00d0 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 lla/5.0 (Windows
00e0 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b NT 10.0 ; Win64;
00f0 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 x64) Ap pleWebKi
0100 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c t/537.36 (KHTML,
0110 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 like Ge cko) Chr
Type (eth.type), 2 byte(s)
Mostrar bytes de paquete

```

EtherType es un campo en los marcos Ethernet que indica qué tipo de datos están dentro del marco y cómo deben ser procesados. También se utiliza para determinar el tamaño de algunos marcos. Se usa en el etiquetado VLAN y es asignado por la Autoridad de Registro de IEEE. En este caso el valor de tipo de trama es 0x0800, lo que indica que es ipv4

4. ¿A cuántos bytes del inicio de la trama aparece la “G” de “GET”?

```

0030 02 05 ef de 00 00 47 45 54 20 2f 77 69 72 65 73 ...GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 hark-lab s/HTTP-e
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 thereal- lab-file
0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 3.html H TTP/1.1
0070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 ·Host: g aia.cs.u
0080 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 mass.edu ·Connec
0090 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive
00a0 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ·Upgrad e-Insecu
00b0 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Reque sts: 1·
00c0 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
00d0 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 lla/5.0 (Windows
00e0 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b NT 10.0 ; Win64;
00f0 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 x64) Ap pleWebKi
0100 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c t/537.36 (KHTML,
0110 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 like Ge cko) Chr
0120 6f 6d 65 2f 31 32 32 2e 30 2e 30 2e 30 20 53 61 ome/122. 0.0.0 Sa
0130 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 fari/537 .36 ·Acc
0140 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 ept: tex t/html,a
Bytes 54-56: Request Method (http.request.method)

```

A 54 bytes del inicio de la trama aparece la G del get.

5. Revise la estructura de una trama Ethernet, en sus apuntes o mediante una búsqueda en la web. ¿Por qué Wireshark no muestra el campo de FCS?

Building block		Tamaño	Función
PreambleStart delimiter (SFD)	frame	8 bytes	Sincronización de los receptoresSecuencia de bits que inicia la trama
Destination (MAC)	address	6 bytes	Dirección de hardware del adaptador de red de destino
Source address (MAC)		6 bytes	Dirección de hardware del adaptador de red de origen
Tag		4 bytes	Etiqueta VLAN opcional para la integración en redes VLAN (IEEE 802.1q)
Type		2 bytes	Ethernet II: etiquetado de protocolos de la capa 3
Length		2 bytes	Longitud de la información sobre el registro
Destination access point (DSAP)	service	1 byte	Dirección individual del punto de acceso al servicio
Source point (SSAP)	service access	1 byte	Dirección de origen del dispositivo de envío
Control		1 byte	Define el marco de la LLC (enlace lógico)
SNAP		5 bytes	Campo para la definición del identificador único de la organización (OUI) del fabricante y el número de protocolo (como "Type").
Data		44-1 500 depending structure)	bytes (limit on frame Los datos que deben transmitirse

Frame check sequence 4 bytes (FCS)

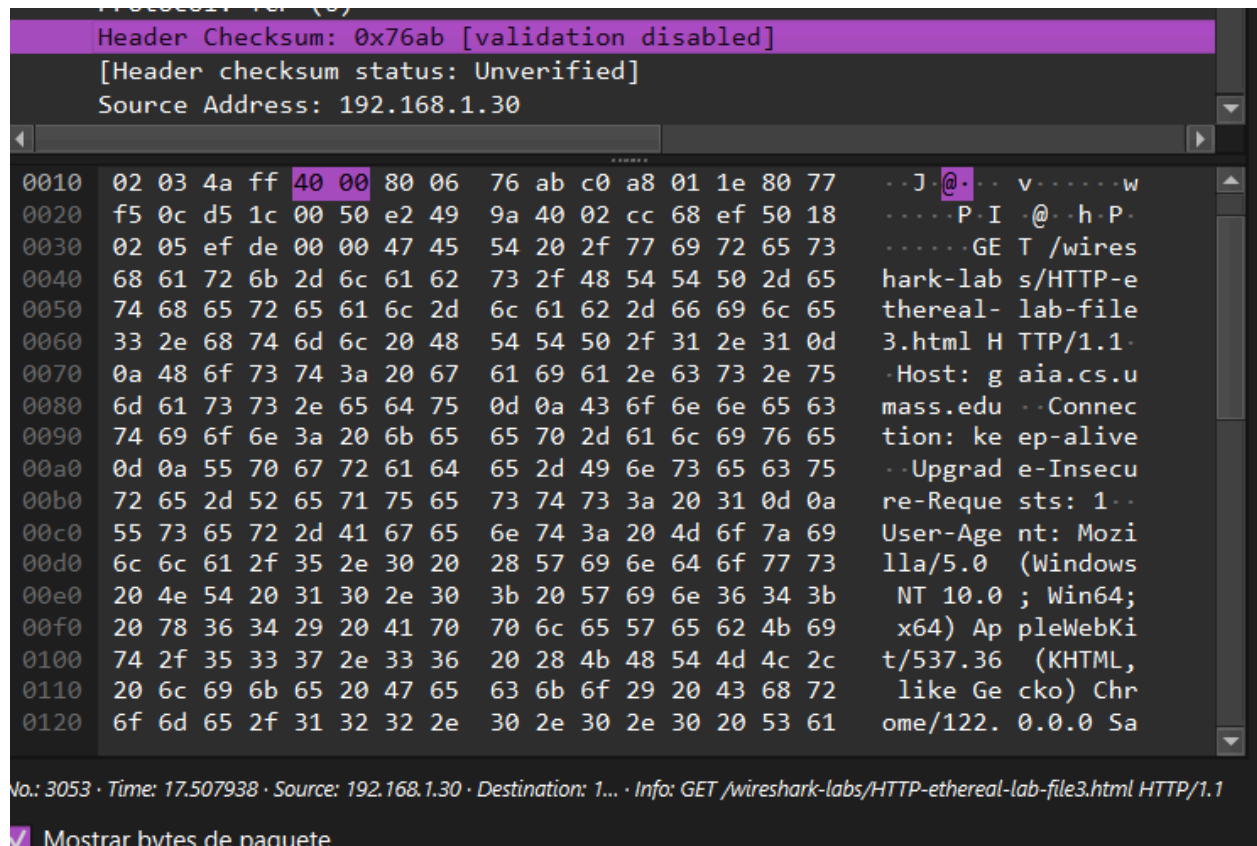
Suma de comprobación que calcula la trama completa

Inter frame gap (IFS) -

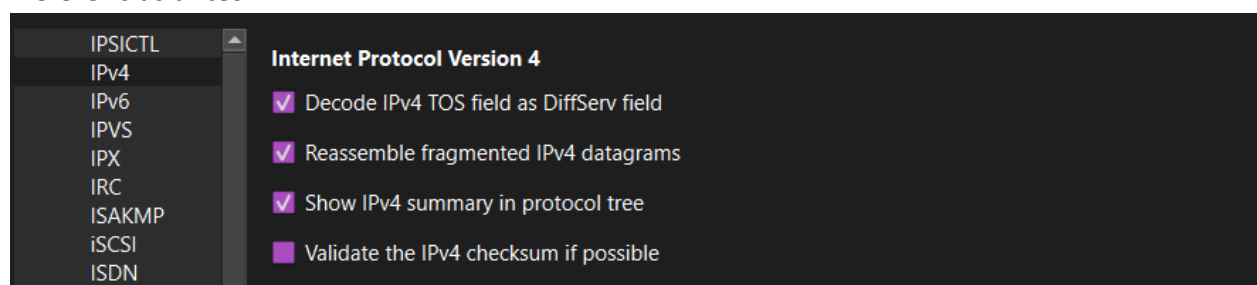
Parada de transmisión de 9.6 µs

A nosotros Wireshark nos muestra el campo FCS solo que dice que no está validado. Para que se valide basta con modificar las preferencias de la aplicación activando el “Validate the IPv4 checksum if possible”.

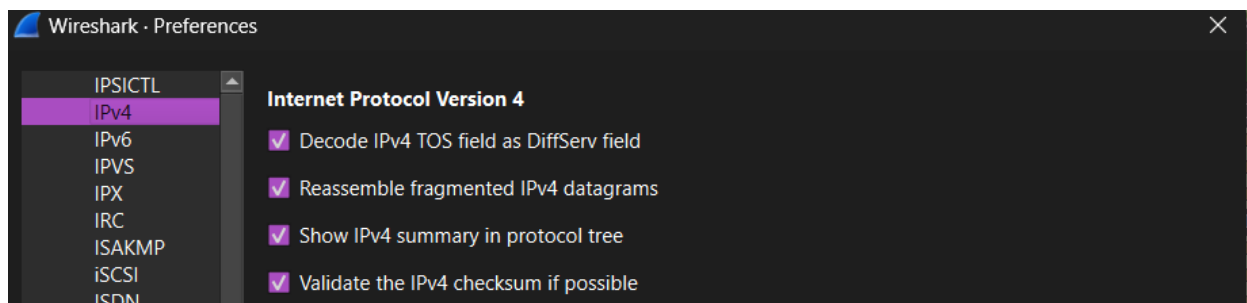
Antes



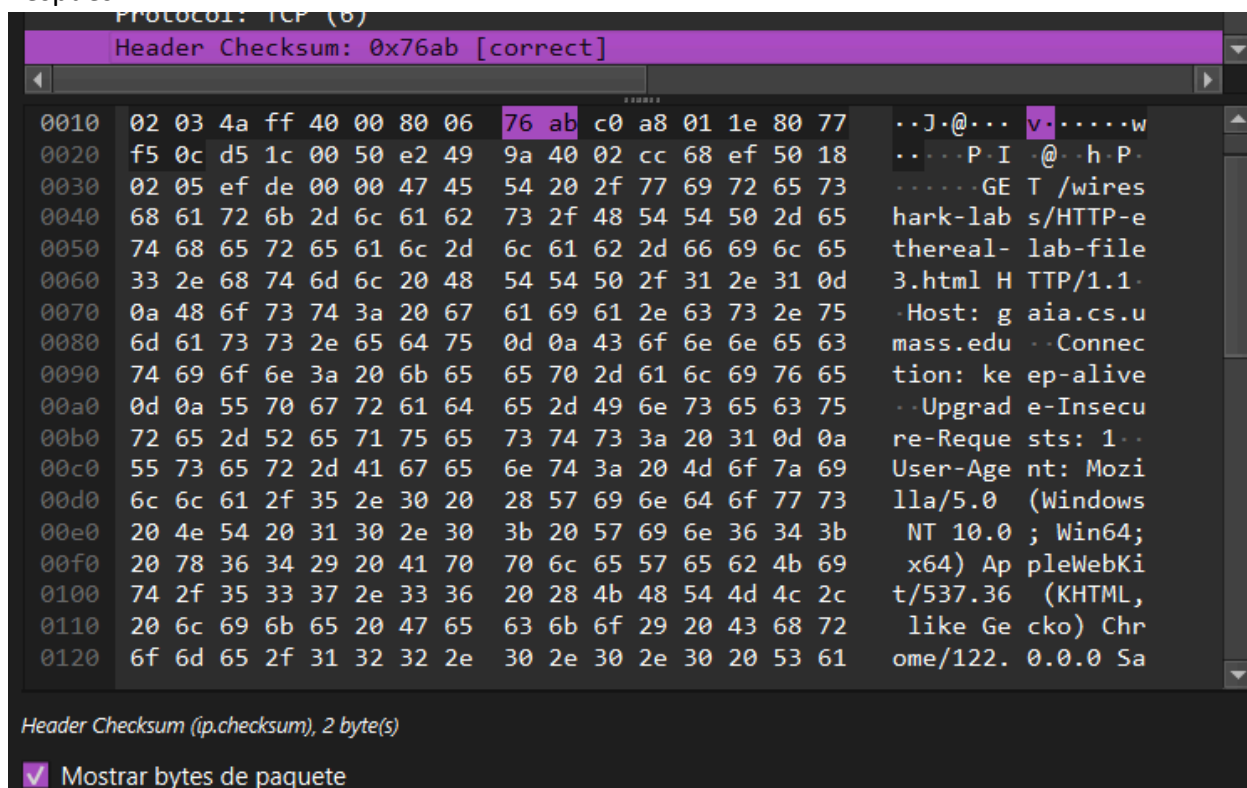
Preferencias antes



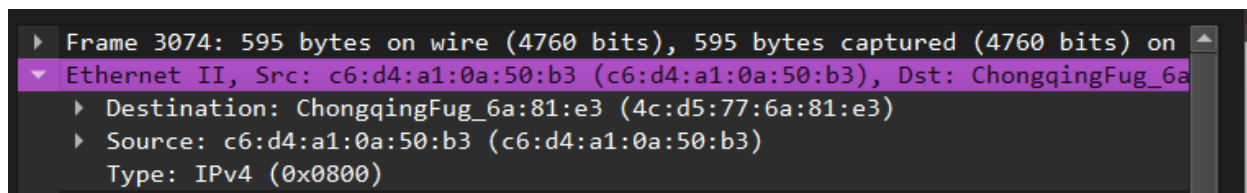
Habilitar la validación del checksum



Después



Busque ahora la trama que contiene el texto “HTTP/1.1 200 OK” en el panel inferior de CONTENIDO. Con base en dicha trama, conteste las siguientes preguntas:



6. ¿Cuál es la dirección fuente Ethernet? ¿A qué equipo corresponde?

Source: c6:d4:a1:0a:50:b3 (c6:d4:a1:0a:50:b3)

7. ¿Cuál es la dirección destino Ethernet? ¿A qué equipo corresponde?

Destination: ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3), corresponde al portátil del compañero Julio.

8. ¿Cuál es el valor del tipo de trama? ¿Qué indica este valor?

The image shows a Wireshark packet capture analysis. The packet list on the left shows a packet of type Ethernet II. The packet details pane on the right shows the following information:

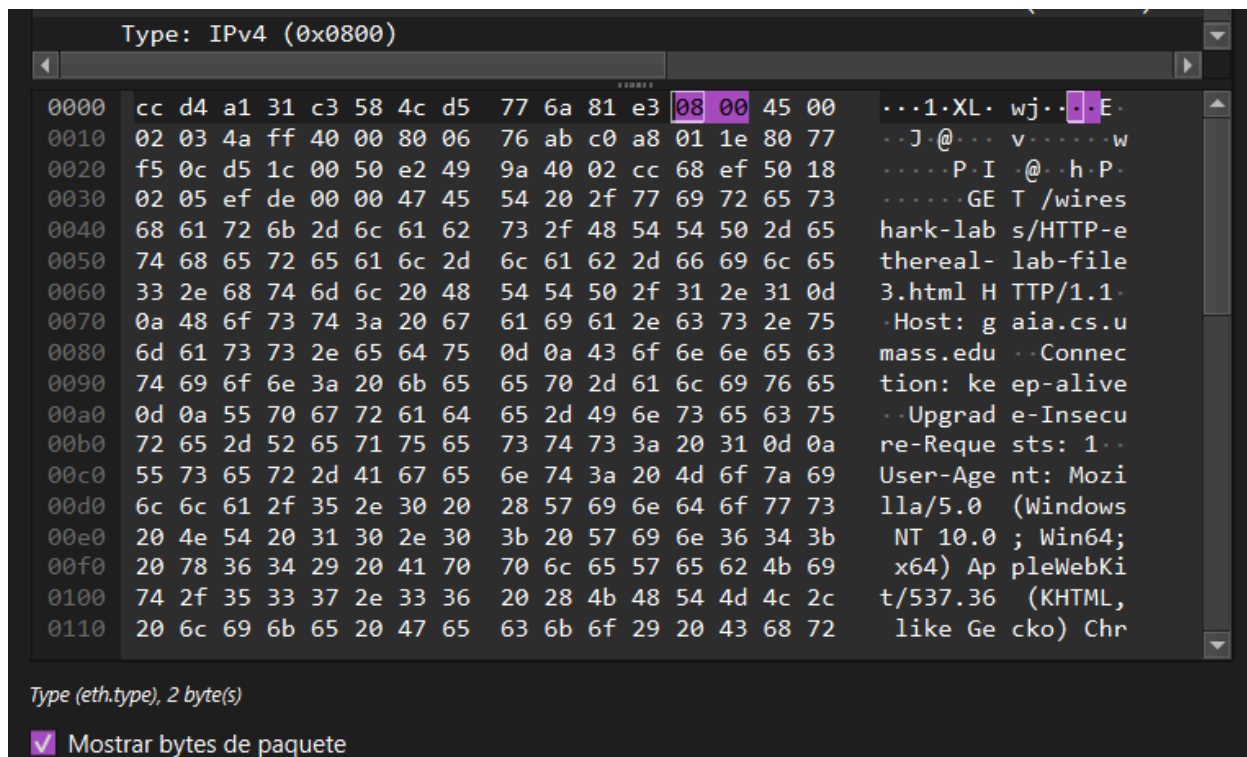
- Ethernet II, Src: c6:d4:a1:0a:50:b3 (c6:d4:a1:0a:50:b3), Dst: ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3)
 - Destination: ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3)
 - Source: c6:d4:a1:0a:50:b3 (c6:d4:a1:0a:50:b3)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.30
- Transmission Control Protocol, Src Port: 80, Dst Port: 54556, Seq: 4321, Ack: 4
- [4 Reassembled TCP Segments (4861 bytes): #3071(1440), #3072(1440), #3073(1440)]
- Hypertext Transfer Protocol
- Line-based text data: text/html (98 lines)

The packet bytes pane at the bottom shows the raw data of the packet, with the first 12 bytes highlighted in purple. The text data is displayed as HTML, showing a paragraph of text and a heading.

Frame (595 bytes) Reassembled TCP (4861 bytes)

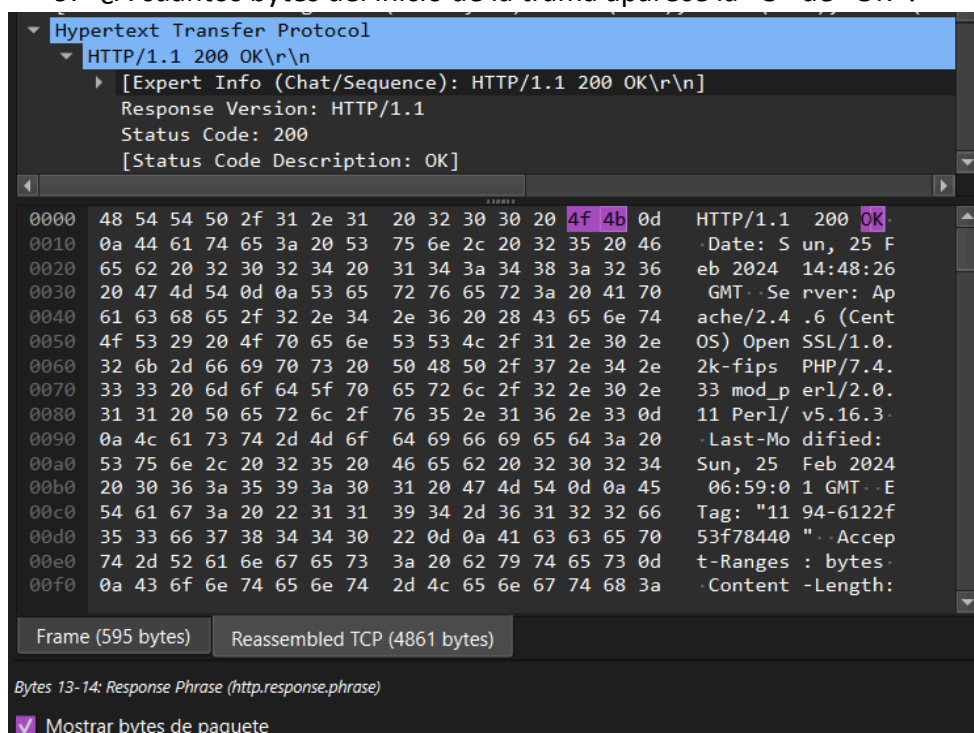
Bytes 12-13: Type (eth.type)

☒ Mostrar bytes de paquete



EtherType es un campo en los marcos Ethernet que indica qué tipo de datos están dentro del marco y cómo deben ser procesados. También se utiliza para determinar el tamaño de algunos marcos. Se usa en el etiquetado VLAN y es asignado por la Autoridad de Registro de IEEE. En este caso el valor de tipo de trama es 0x0800, lo que indica que es ipv4

9. ¿A cuántos bytes del inicio de la trama aparece la “O” de “OK”?



La “O” de “OK” está a 13 bytes del inicio de la trama.

EL PROTOCOLO ARP

10. ¿Cuál es la función del protocolo ARP?

El Protocolo de Resolución de Direcciones (ARP, por sus siglas en inglés) se utiliza para mapear direcciones IP a direcciones MAC en una red local. Su función principal es encontrar la dirección MAC asociada a una dirección IP dada dentro de una red local, permitiendo así la comunicación entre dispositivos en la misma red. Esto es fundamental para la comunicación en capa de enlace de datos en redes Ethernet y otros tipos de redes locales.

Recuerde que el protocolo ARP conserva un caché de equivalencias entre direcciones IP y Ethernet. El comando `arp` se puede emplear para manipular el contenido de dicha tabla.

Consulte la tabla ARP de su equipo, ejecutando el siguiente comando:

- `arp -a` (en Windows y Mac)
- `arp -n` (en Linux)

```
PS C:\Users\julio> arp -a

Interfaz: 192.168.1.30 --- 0xc
  Dirección de Internet      Dirección física      Tipo
  192.168.1.1                cc-d4-a1-31-c3-58     dinámico
  192.168.1.255              ff-ff-ff-ff-ff-ff     estático
  224.0.0.2                  01-00-5e-00-00-02     estático
  224.0.0.22                 01-00-5e-00-00-16     estático
  224.0.0.251                01-00-5e-00-00-fb     estático
  224.0.0.252                01-00-5e-00-00-fc     estático
  239.255.255.250            01-00-5e-7f-ff-fa     estático
  255.255.255.255            ff-ff-ff-ff-ff-ff     estático

Interfaz: 192.168.56.1 --- 0x11
  Dirección de Internet      Dirección física      Tipo
  192.168.56.255            ff-ff-ff-ff-ff-ff     estático
  224.0.0.22                01-00-5e-00-00-16     estático
  224.0.0.251               01-00-5e-00-00-fb     estático
  224.0.0.252               01-00-5e-00-00-fc     estático
  239.255.255.250           01-00-5e-7f-ff-fa     estático
```

11. Tome una línea cualquiera del informe e interprétela. Por favor escriba dicha interpretación.

```
PS C:\Users\agaza> arp -a
```

```
Interface: 192.168.1.9 --- 0xb
```

Internet Address	Physical Address	Type
192.168.1.1	fc-12-63-80-86-f0	dynamic
192.168.1.47	fc-12-63-5c-a9-3a	dynamic
192.168.1.102	48-55-5e-85-cd-ca	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Interface: 192.168.1.7 --- 0xe
```

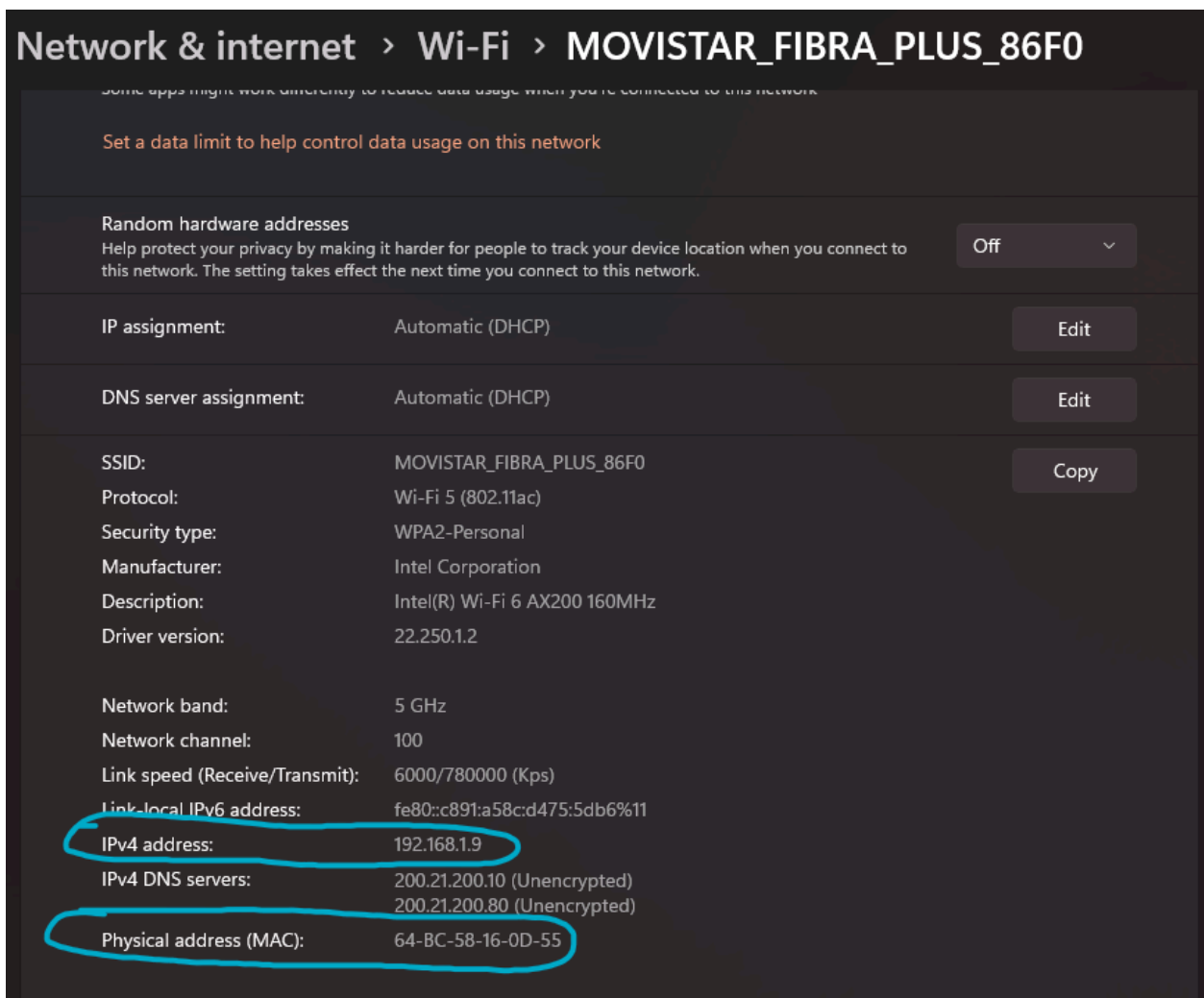
Internet Address	Physical Address	Type
192.168.1.1	fc-12-63-80-86-f0	dynamic
192.168.1.6	4a-09-e5-e9-32-e3	dynamic
192.168.1.9	64-bc-58-16-0d-55	dynamic
192.168.1.47	fc-12-63-5c-a9-3a	dynamic
192.168.1.102	48-55-5e-85-cd-ca	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Interface: 192.168.56.1 --- 0x13
```

Internet Address	Physical Address	Type
192.168.56.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

```
PS C:\Users\agaza>
```

Tomemos la línea subrayada como ejemplo. Es posible observar que el dispositivo con IP 192.168.1.9 tiene asociada la dirección MAC 64-bc-58-16-0d-55.



Al entrar a los detalles de red podemos observar la dirección ipv4 del modem junto con MAC que coinciden con los mostrados en el “arp -a”

Para poder capturar tramas ARP, es necesario borrar el contenido de esta tabla. Proceda a borrarla ejecutando el siguiente comando:

- `arp -d *` (en Windows, como administrador)
- `sudo ip -s -s neigh flush all` (en Linux)
- `sudo arp -d -a` (en Mac)

Ahora haga lo siguiente:

- Limpie el caché de su navegador.
- Abra Wireshark, e inicie la captura por el adaptador de red adecuado.
- Acceda a la siguiente URL en su navegador:
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>
- Detenga la captura.
- Filtre las tramas del protocolo ARP (escriba `arp` en el campo de filtro y presione ENTER).

12. ¿Cuáles son los valores de las direcciones fuente y destino de la trama Ethernet que contiene la solicitud ARP?

El valor de la dirección fuente es c6:d4:a1:0a:50:b3 (c6:d4:a1:0a:50:b3), y el de destino es ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3).

```

▶ Frame 860: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{648BDFD1
▶ Ethernet II, Src: c6:d4:a1:0a:50:b3 (c6:d4:a1:0a:50:b3), Dst: ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3)
  ▶ Destination: ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3)
  ▶ Source: c6:d4:a1:0a:50:b3 (c6:d4:a1:0a:50:b3)
  Type: ARP (0x0806)
  ▶ Trailer: 00000000000000000000000000007a68169f
▶ Address Resolution Protocol (request)

```

```

0000  4c d5 77 6a 81 e3 c6 d4 a1 0a 50 b3 08 06 00 01  L.wj...P...
0010  08 00 06 04 00 01 cc d4 a1 31 c3 58 c0 a8 01 01  .....1X...
0020  00 00 00 00 00 00 c0 a8 01 1e 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 7a 68 16 9f  .....zh..

```

Bytes 12-13: Type (eth.type)

14. Estudie la siguiente descripción del protocolo ARP:

a. ¿Cuántos bytes hay entre el inicio de la trama Ethernet y el campo opcode de ARP?

b. ¿Cuál es el valor del campo opcode? ¿Qué indica?

- 1 para una solicitud ARP (ARP Request), indicando que se está preguntando por la dirección MAC asociada a una dirección IP.

- 2 para una respuesta ARP (ARP Reply), indicando que se está proporcionando la dirección MAC asociada a una dirección IP.

c. ¿Contiene el mensaje ARP la dirección IP del equipo que lo envía?

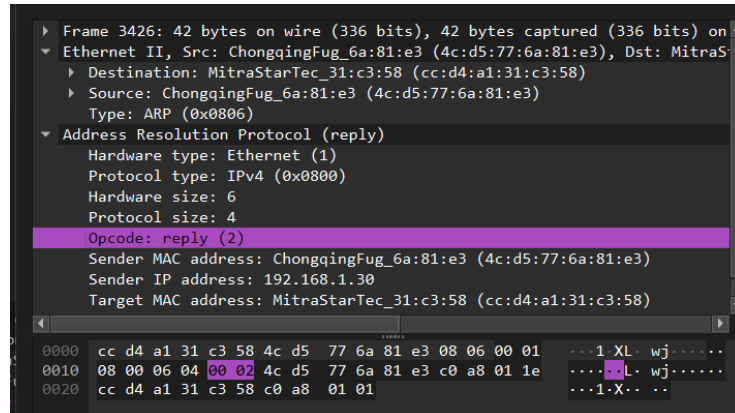
Mensaje ARP y la dirección IP del equipo que lo envía**: Sí, el mensaje ARP contiene la dirección IP del equipo que lo envía. Tanto en una solicitud ARP como en una respuesta ARP, la dirección IP del remitente se incluye en el campo "dirección IP del remitente" dentro del mensaje ARP.

- d. ¿En qué posición del mensaje ARP aparece la “pregunta”? (o sea, la dirección Ethernet de la máquina cuya dirección Ethernet está siendo averiguada).

Posición de la "pregunta" en el mensaje ARP**: En una solicitud ARP (opcode = 1), la "pregunta" se refiere a la dirección Ethernet del equipo cuya dirección MAC se está buscando. En el mensaje ARP, esta dirección Ethernet del equipo se encuentra en el campo "dirección Ethernet del destino", que generalmente está ubicado en los bytes 22-27 de la trama Ethernet, justo después del campo opcode.

15. Ahora, encuentre la trama que contiene la respuesta ARP a la solicitud anterior.

- a. ¿Cuál es el valor del campo opcode? ¿Qué indica?



Opcode: This field specifies the nature of the ARP message being sent. The first two values (1 and 2) are used for regular ARP. Numerous other values are also defined to support other protocols that use the ARP frame format, such as RARP, some of which are more widely used than others:

Opcode	ARP Message Type
1	ARP Request
2	ARP Reply
3	RARP Request
4	RARP Reply
5	DRARP Request
6	DRARP Reply
7	DRARP Error
8	InARP Request
9	InARP Reply

El valor del campo Opcode es 00 02, y significa que es una respuesta a la solicitud anterior.

- b. ¿En qué posición del mensaje ARP aparece la “respuesta”? (o sea, la dirección Ethernet de la máquina cuya dirección Ethernet está siendo averiguada).

```
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3)
  Sender IP address: 192.168.1.30
  Target MAC address: MitraStarTec_31:c3:58 (cc:d4:a1:31:c3:58)
  ...
0000 cc d4 a1 31 c3 58 4c d5 77 6a 81 e3 08 06 00 01 ... 1 XL wj .....
0010 08 00 06 04 00 02 4c d5 77 6a 81 e3 c0 a8 01 1e ... L wj .....
0020 cc d4 a1 31 c3 58 c0 a8 01 01 ... 1 X ..
```

Bytes 32-37: Target MAC address (arp.dst.hw_mac)

La dirección ethernet de la máquina cuya dirección ethernet está siendo averiguada aparece desde el byte 32 hasta el byte 37.

16. ¿Cuáles son los valores de las direcciones fuente y destino de la trama Ethernet que contiene la respuesta ARP?

El valor de la fuente de la trama Ethernet que contiene la respuesta ARP es ChongqingFug_6a:81:e3 (4c:d5:77:6a:81:e3), y la de destino es MitraStarTec_31:c3:58 (cc:d4:a1:31:c3:58).