Práctica:
Captura y Análisis de paquetes con Wireshark.

Cuando dos aplicaciones se comunican a través de la red, éstas generan PDU's con datos de aplicación que es necesario encapsular dentro de otros PDU's de capas inferiores y poder dar así un buen tratamiento a los datos enviados. Dos de las principales capas son la capa de red (Internet) y la capa de Transporte, en las cuales se manejan datos sensibles, tales como las direcciones lógicas de los dispositivos de red que contienen dichas aplicaciones y los identificadores de estas aplicaciones (# de puerto).

Wireshark es una herramienta muy conocida dentro de los analizadores de protocolos (*sniffers*) que permite leer la información contenida dentro de los distintos PDU's de un paquete que viaja por la red. A continuación, mostraremos un ejemplo de una trama (Capa 2) capturada con Wireshark.

Observe la siguiente trama capturada con la herramienta wireshark:

```
0000                                                    00 21 9b ea 8a 7c 00 19
e4 b9 64 b1 08 00 45 00   .!...|.. ..d...E.
0010          7e 2d 40          06  41 9a bb 8d 01 92          .(~-@.<. A.......
0020          00 50 c4 1f 9e bb  03 f9 fe f5 dd bd      11   .A.P.... ......P.
0030           1a 99          00 00 00 00  00 00 00 00
```

Ésta trama puede ser desencapsulada de la siguiente manera:

- **Trama Ethernet2 (Capa de Enlace de Datos)**
  - MAC Destino: 00:21:9b:ea:8a:7c
  - MAC Origen: 00:19:e4:b9:64:b1
  - Tipo de trama: IP(0x800)
  - Trailer: 000000000000
- **Paquete IP (Capa de Red)**
  - Versión: 4
  - Longitud encabezada: 5 (palabras de 32 bits=20 bytes)
  - TOS: 0
  - Longitud total del paquete: 40 palabras de 32 bits (0028) =160 bytes
  - Identificador: 32301(0x7e2d)
  - Banderas: No fragmentar (0x04)
  - Offset: 0(0x00)
  - TTL: 60 (0x3c)
  - Protocolo: TCP (0x06) //RFC 1340
  - Checksum: 0x419a
  - IP Origen: 187.141.1.146 (bb8d0192)
  - IP destino: 192.168.1.65 (c0a80141)
- **Segmento TCP (capa de Transporte)**
  - Puerto Origen: 80 (0x0050) //http RFC 1340
  - Puerto Destino: 50207 (0xc41f)
  - Número de secuencia: 2663056377 (0x9ebb03f9)

- Número de acuse: 4277525949 (0xfef5ddbd)
- Longitud de encabezado: 20 bytes (0x05)
- Banderas: 0x11 (ACK + FIN)
  - 0_____: Reducción de ventana por congestión
  - _0_____: ECN-Echo (Notificación explícita de congestión)
  - __0_____: Urgente
  - ___1____: ACK
  - ____0___: PUSH
  - _____0__: RESET
  - ______0_: SYN
  - _______1: FIN
- Tamaño ventana: 6809 (0x1a99)
- Checksum: 0xd259

Desarrollo:

Uso de Wireshark para examinar las tramas de Ethernet

Paso 1: Revisar las descripciones y las longitudes de los campos de encabezado de Ethernet II

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

Paso 2: Examinar el contenido de encabezado de Ethernet II de una solicitud de ARP

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

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de NIC.
Dirección de destino	Broadcast (ff:ff:ff:ff:ff:ff)	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o seis octetos, expresada 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 seis últimos números hexadecimales corresponden al número de serie de la NIC. La dirección de destino puede ser un broadcast, que contiene todos unos, o un unicast. La dirección de origen es siempre unicast.
Dirección de origen	Dell_24:2a:60 (5c:26:0a:24:2a:60)	
Tipo de trama	0x0806	Para las tramas de Ethernet II, estos campos contienen un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior en el campo de datos. Existen muchos protocolos de capa superior que admite Ethernet II. Dos tipos comunes de trama son: Valor Descripción `0x0800` Protocolo IPv4 `0x0806` Protocolo de resolución de direcciones (ARP)
Datos	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos está entre 46 y 1,500 bytes.
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El valor lo computa la máquina de envío, abarcando las direcciones de trama, campos de datos y tipo. El receptor lo verifica

Analizar las tramas y paquetes de las siguientes direcciones:

i. Capture por lo menos 10 paquetes utilizando Wireshark y para cada uno de ellos rellene los siguientes encabezados

a. Análisis de una **IP** de una **máquina de laboratorio**

- **Trama Ethernet2 (Capa de Enlace de Datos)**
  - MAC Destino: RealtekSemic_68:07:62 (00:e0:4c:68:07:62)
  - MAC Origen: ChongqingFug_80:50:27 (4c:eb:bd:80:50:27)
  - Tipo de trama: IPv4 (0x800)
- **Paquete IP (Capa de Red)**
  - Versión: 4
  - Longitud de encabezado: 20 bytes (5)
  - TOS: 0x00 (valor por defecto, sin prioridad específica)
  - Longitud total del paquete: 1974 bytes
  - Identificador: 0xdb8b (56203)
  - Banderas: 0x0 (Don't Fragment)
    - 0... .... = Reserved bit: Not set
    - .0.. .... = Don't fragment: Not set
    - ..0. .... = More fragments: Not set

- Offset: 0
- TTL (Tiempo de Vida): 128
- Protocolo: ICMP (1)
- Checksum: 0x4a9d [validation disabled]
- IP Origen: 172.100.91.209
- IP Destino: 172.100.95.254

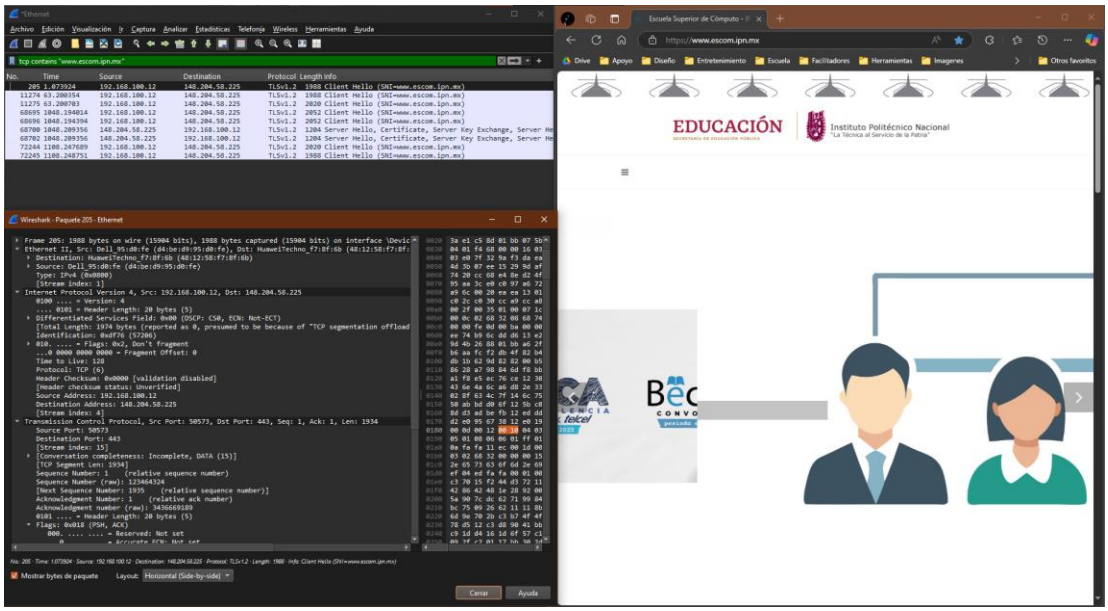
- **ICMP**
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0x4d5a [correct]

b. Análisis de una IP de la página www.escom.ipn.mx

- **Trama Ethernet2 (Capa de Enlace de Datos)**
  - MAC Destino: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
  - MAC Origen: Dell_95:d0:fe (d4:be:d9:95:d0:fe)
  - Tipo de trama: IPv4 (0x800)
- **Paquete IP (Capa de Red)**
  - Versión: 4
  - Longitud de encabezado: 20 bytes (5)
  - TOS: 0x00 (valor por defecto, sin prioridad específica)
  - Longitud total del paquete: 1974 bytes
  - Identificador: 0xdf76 (57206)
  - Banderas: 0x2 (Don't Fragment)
    - 0... .... = Reserved bit: Not set
    - .1.. .... = Don't fragment: Set
    - ..0. .... = More fragments: Not set
  - Offset: 0
  - TTL (Tiempo de Vida): 128
  - Protocolo: TCP (6)
  - Checksum: 0x0000 (no verificado)
  - IP Origen: 192.168.100.12
  - IP Destino: 148.204.58.225
- **Segmento TCP (capa de Transporte)**
  - Puerto Origen: 50573
  - Puerto Destino: 443
  - Número de secuencia: 123463424
  - Número de acuse: 3466069189
  - Longitud de encabezado: 20 bytes
  - Banderas: PSH, ACK (0x018)
    - 000. .... = Reserved: Not set
    - ...0 .... = Accurate ECN: Not set
    - .... 0... .... = Congestion Window Reduced: Not set
    - .... .0.. .... = ECN-Echo: Not set
    - .... ..0. .... = Urgent: Not set

- ....1 .... = Acknowledgment: Set
- .... 1... = Push: Set
- .... .0.. = Reset: Not set
- ....0. = Syn: Not set
- ....0 = Fin: Not set

- Tamaño ventana: 1025
- Checksum: 0x4fa6

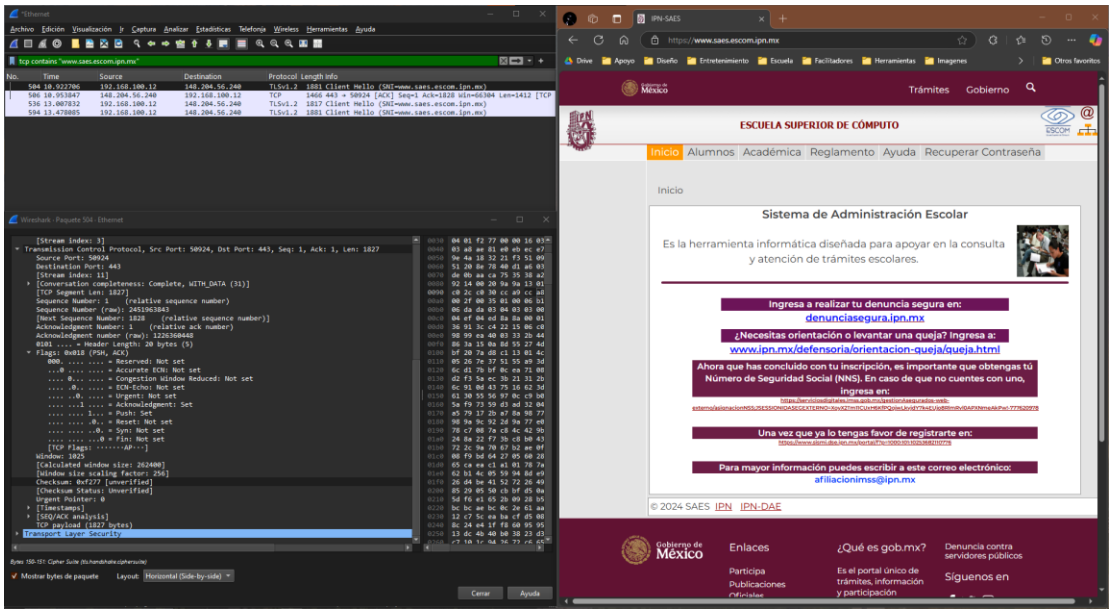


c. Análisis de una IP de la página www.saes.escom.ipn.mx

- **Trama Ethernet2 (Capa de Enlace de Datos)**
  - MAC Destino: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
  - MAC Origen: Dell_95:d0:fe (d4:be:d9:95:d0:fe)
  - Tipo de trama: IPv4 (0x800)
- **Paquete IP (Capa de Red)**
  - Versión: 4
  - Longitud de encabezado: 20 bytes (5)
  - TOS: 0x00 (valor por defecto, sin prioridad específica)
  - Longitud total del paquete: 1867 bytes
  - Identificador: 0xb413 (46099)
  - Banderas: 0x2 (Don't Fragment)
    - 0... .... = Reserved bit: Not set
    - .1.. .... = Don't fragment: Set
    - ..0. .... = More fragments: Not set
  - Offset: 0
  - TTL (Tiempo de Vida): 128
  - Protocolo: TCP (6)
  - Checksum: 0x0000 (no verificado)
  - IP Origen: 192.168.100.12

- IP Destino: 148.204.56.240

- **Segmento TCP (capa de Transporte)**
  - Puerto Origen: 50924
  - Puerto Destino: 443
  - Número de secuencia: 2451963843
  - Número de acuse: 1226360448
  - Longitud de encabezado: 20 bytes
  - Banderas: PSH, ACK (0x018)
    - 000. .... = Reserved: Not set
    - ...0 .... = Accurate ECN: Not set
    - .... 0... .... = Congestion Window Reduced: Not set
    - .... .0.. .... = ECN-Echo: Not set
    - .... ..0. .... = Urgent: Not set
    - ....1 .... = Acknowledgment: Set
    - .... 1... = Push: Set
    - .... .0.. = Reset: Not set
    - ....0. = Syn: Not set
    - ....0 = Fin: Not set
  - Tamaño ventana: 1025
  - Checksum: 0xf277 [unverified]



d. Análisis de una IP 198.168.100.33 (celular)

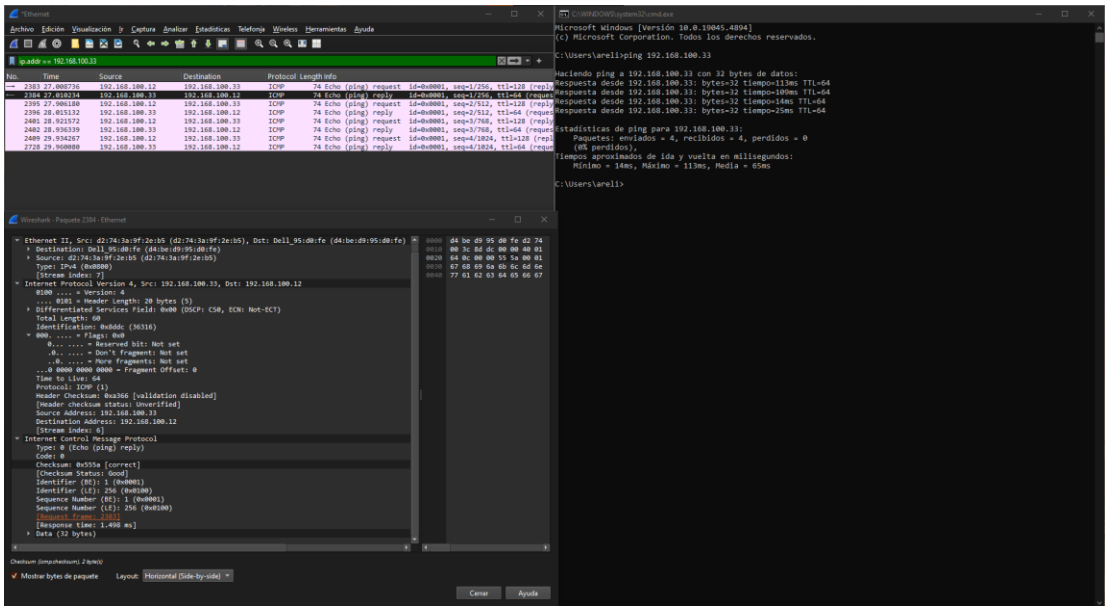
- **Trama Ethernet2 (Capa de Enlace de Datos)**
  - MAC Destino: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
  - MAC Origen: d2:74:3a:9f:2e:b5 (d2:74:3a:9f:2e:b5)
  - Tipo de trama: IPv4 (0x800)

- **Paquete IP (Capa de Red)**

- Versión: 4
- Longitud de encabezado: 20 bytes (5)
- TOS: 0x00 (valor por defecto, sin prioridad específica)
- Longitud total del paquete: 60 bytes
- Identificador: 0x8ddc (36316)
- Banderas: 0x0
  - 0... .... = Reserved bit: Not set
  - .0.. .... = Don't fragment: Not set
  - ..0. .... = More fragments: Not set
- Offset: 0
- TTL (Tiempo de Vida): 64
- Protocolo: ICMP (1)
- Checksum: 0xa366
- IP Origen: 192.168.100.33
- IP Destino: 192.168.100.12

○ **ICMP**

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x555a [correct]



e. Análisis de una IP 148.204.61.254 (Gateway)

○ **Trama Ethernet2 (Capa de Enlace de Datos)**

- MAC Destino: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
- MAC Origen: d2:74:3a:9f:2e:b5 (d2:74:3a:9f:2e:b5)
- Tipo de trama: IPv4 (0x800)

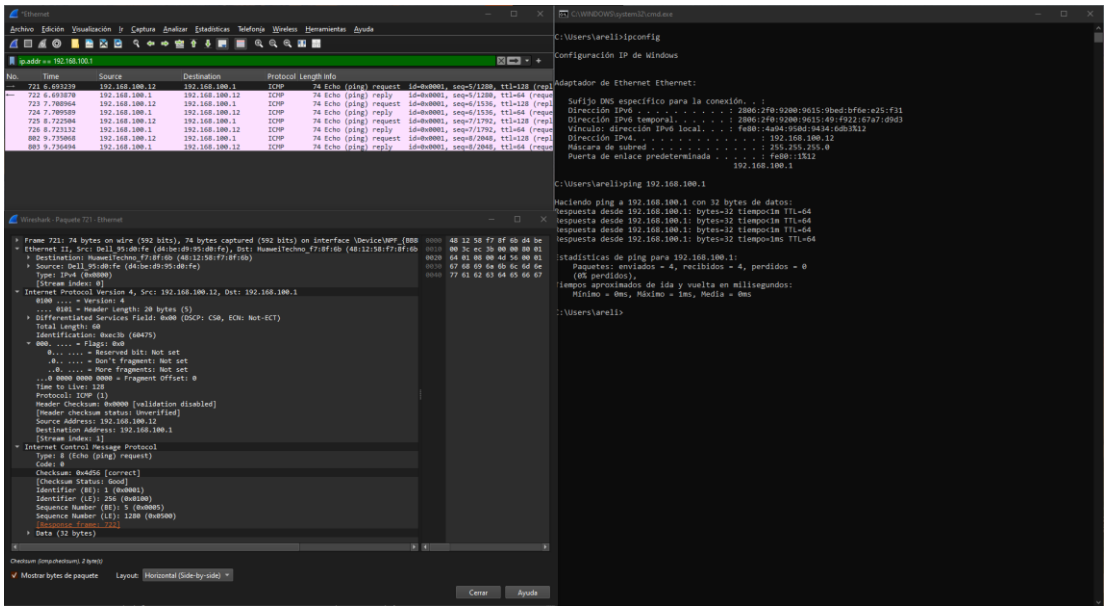
○ **Paquete IP (Capa de Red)**

- Versión: 4
- Longitud de encabezado: 20 bytes (5)

- TOS: 0x00 (valor por defecto, sin prioridad específica)
- Longitud total del paquete: 60 bytes
- Identificador: 0xec3b (60475)
- Banderas: 0x0
  - 0... .... = Reserved bit: Not set
  - .0.. .... = Don't fragment: Not set
  - ..0. .... = More fragments: Not set
- Offset: 0
- TTL (Tiempo de Vida): 128
- Protocolo: ICMP (1)
- Checksum: 0x0000
- IP Origen: 192.168.100.12
- IP Destino: 192.168.100.1

○ **ICMP**

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d56 [correct]



f. Análisis de una de la pagina www.ipn.mx

○ **Trama Ethernet2 (Capa de Enlace de Datos)**

- MAC Destino: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
- MAC Origen: d2:74:3a:9f:2e:b5 (d2:74:3a:9f:2e:b5)
- Tipo de trama: IPv4 (0x800)

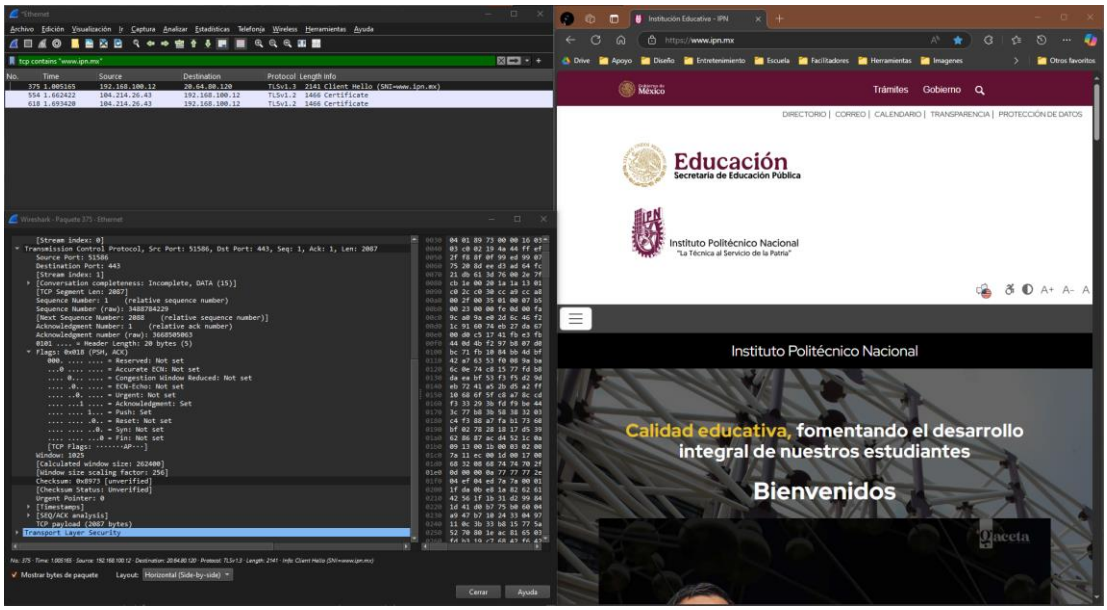
○ **Paquete IP (Capa de Red)**

- Versión: 4
- Longitud de encabezado: 20 bytes (5)
- TOS: 0x00 (valor por defecto, sin prioridad específica)
- Longitud total del paquete: 60 bytes

- Identificador: 0x1ccb (7371)
- Banderas: 0x02
  - 0... .... = Reserved bit: Not set
  - .1.. .... = Don't fragment: Set
  - ..0. .... = More fragments: Not set
- Offset: 0
- TTL (Tiempo de Vida): 128
- Protocolo: TCP (6)
- Checksum: 0x0000
- IP Origen: 192.168.100.12
- IP Destino: 20.64.80.120

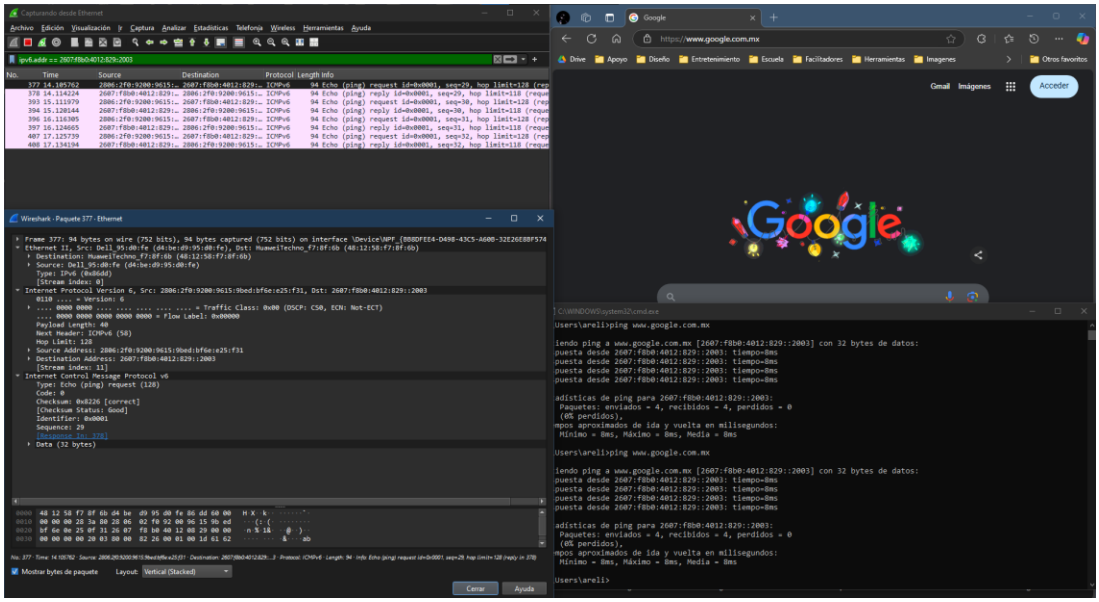
○ **Segmento TCP (capa de Transporte)**

- Puerto Origen: 51586
- Puerto Destino: 443
- Número de secuencia: 3488784229
- Número de acuse: 3668505063
- Longitud de encabezado: 20 bytes
- Banderas: PSH, ACK (0x018)
  - 000. .... = Reserved: Not set
  - ...0 .... = Accurate ECN: Not set
  - .... 0... .... = Congestion Window Reduced: Not set
  - .... .0.. .... = ECN-Echo: Not set
  - .... ..0. .... = Urgent: Not set
  - ....1 .... = Acknowledgment: Set
  - .... 1... = Push: Set
  - .... .0.. = Reset: Not set
  - ....0. = Syn: Not set
  - ....0 = Fin: Not set
- Tamaño ventana: 1025
- Checksum: 0x8973 [unverified]



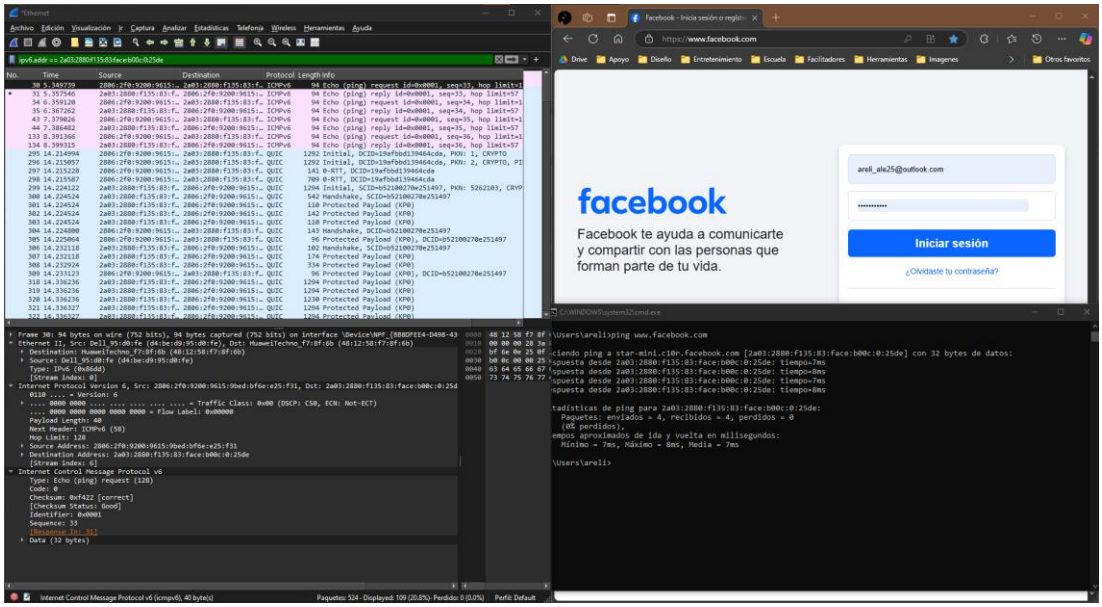
g. Análisis de una de la pagina www.google.com.mx

- **Ethernet II**
  - Destination: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
  - Source: Dell_95:d0:fe (d4:be:d9:95:d0:fe)
  - Type: IPv6 (0x86dd)
- **Internet Protocol Version 6**
  - 0110 .... = Version: 6
  - .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
  - Payload Length: 40
  - Next Header: ICMPv6 (58)
  - Hop Limit: 128
  - Source Address: 2806:2f0:9200:9615:9bed:bf6e:e25:f31
  - Destination Address: 2607:f8b0:4012:829::2003
- **Internet Control Message Protocol v6**
  - Type: Echo (ping) request (128)
  - Code: 0
  - Checksum: 0x8226 [correct]
  - Identifier: 0x0001
  - Sequence: 29
  - Data (32 bytes)



h. Análisis de una de la página www.facebook.com

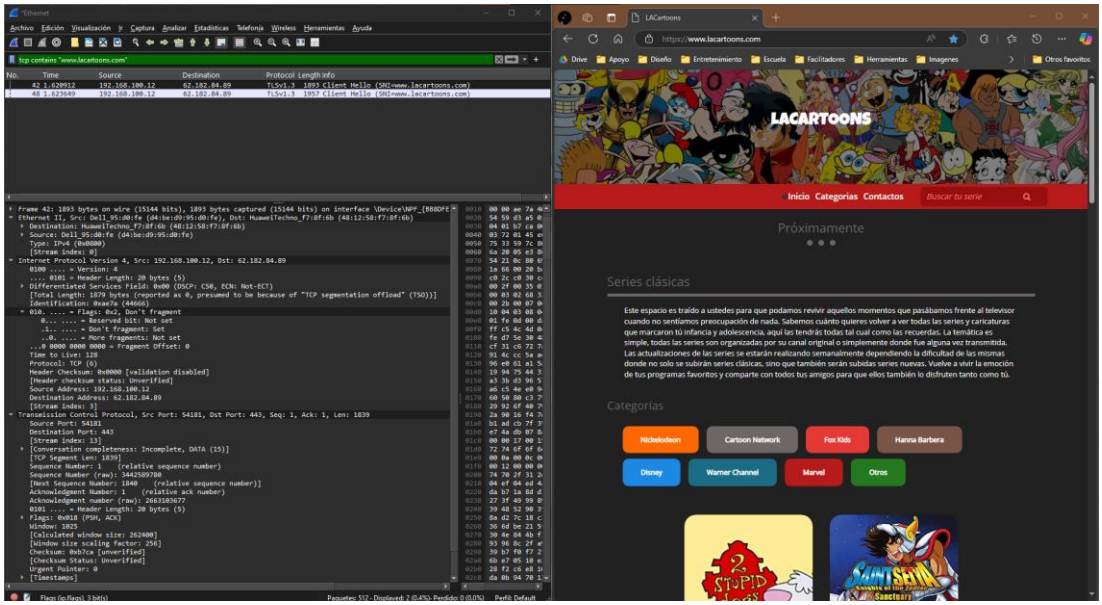
- **Trama Ethernet2 (Capa de Enlace de Datos)**
  - MAC Destino: Destination: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
  - MAC Origen: Source: Dell_95:d0:fe (d4:be:d9:95:d0:fe)
  - Tipo de trama: IPv6 (0x86dd)
- **Paquete IP (Capa de Red)**
  - Src: 2806:2f0:9200:9615:9bed:bf6e:e25:f31
  - Dst: 2a03:2880:f135:83:face:b00c:0:25de
  - 0110 .... = Version: 6
  - .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - .... 1010 0010 0100 1111 0001 = Flow Label: 0xa24f1
  - Payload Length: 1233
  - Next Header: UDP (17)
  - Hop Limit: 64
  - Source Address: 2806:2f0:9200:9615:9bed:bf6e:e25:f31
  - Destination Address: 2a03:2880:f135:83:face:b00c:0:25de
- **Internet Control Message Protocol v6**
  - Type: Echo (ping) request (128)
  - Code: 0
  - Checksum: 0xf422 [correct]
  - [Checksum Status: Good]
  - Identifier: 0x0001
  - Sequence: 33
  - Data (32 bytes)



i. Análisis de una de la página www.lacartoons.com

- **Ethernet II**
  - Destination: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
  - Source: Dell_95:d0:fe (d4:be:d9:95:d0:fe)
  - Type: IPv4 (0x0800)
  - [Stream index: 0]
- **Internet Protocol Version 4**
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Total Length: 1879 bytes
  - Identification: 0xae7a (44666)
  - 010. .... = Flags: 0x2, Don't fragment
    - 0... .... = Reserved bit: Not set
    - .1.. .... = Don't fragment: Set
    - ..0. .... = More fragments: Not set
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 128
  - Protocol: TCP (6)
  - Header Checksum: 0x0000 [validation disabled]
  - Source Address: 192.168.100.12
  - Destination Address: 62.182.84.89
- **Transmission Control Protocol**
  - Source Port: 54181
  - Destination Port: 443
  - [TCP Segment Len: 1839]
  - Sequence Number (raw): 3442589780

- Acknowledgment number (raw): 2663103677
- 0101 .... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 1025
- Checksum: 0xb7ca [unverified]
- Urgent Pointer: 0
- TCP payload (1839 bytes)



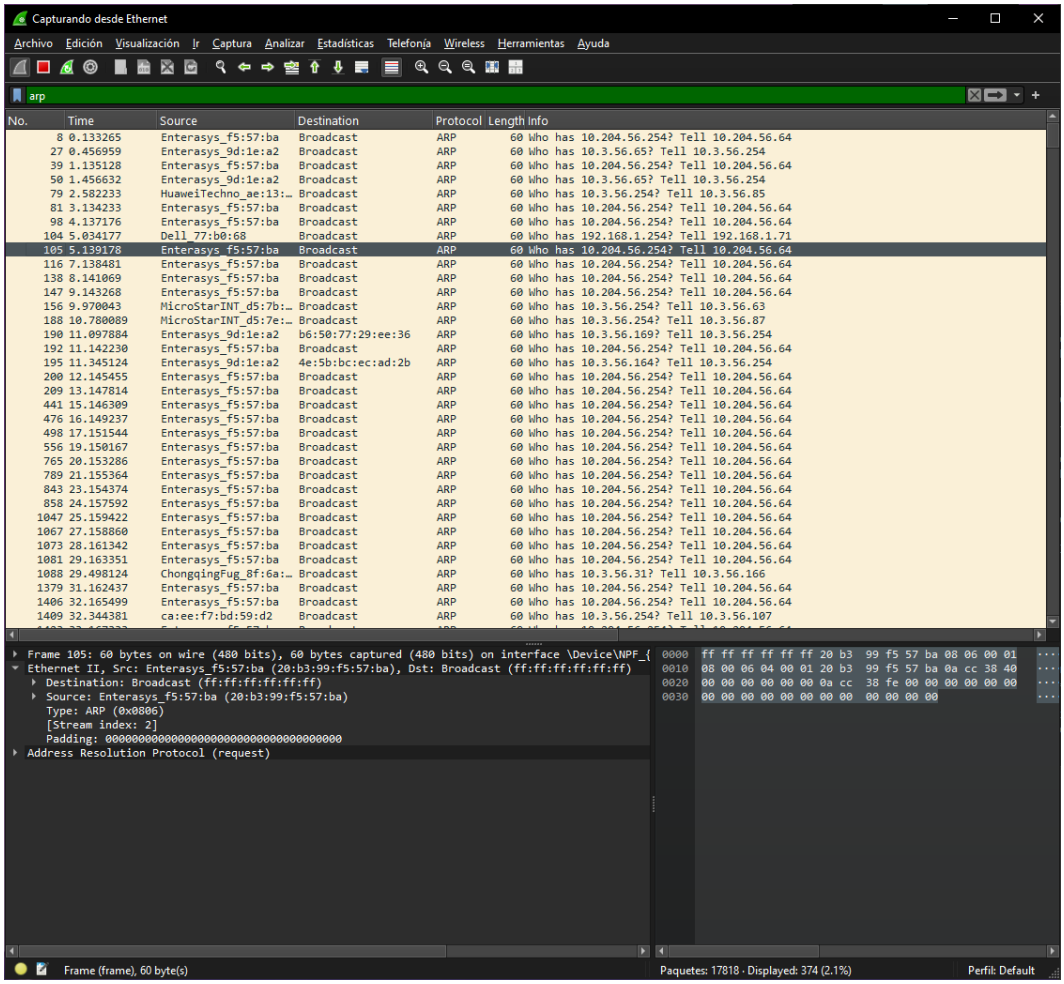
j. Análisis ARP

○ **Ethernet II**

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: FiberhomeTel_96:f7:f0 (ac:4e:65:96:f7:f0)
- Type: ARP (0x0806)
- Trailer: fa0100000000000000000000000000000000

○ **Address Resolution Protocol (request)**

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Sender MAC address: FiberhomeTel_96:f7:f0 (ac:4e:65:96:f7:f0)
- Sender IP address: 192.168.100.2
- Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
- Target IP address: 192.168.100.1



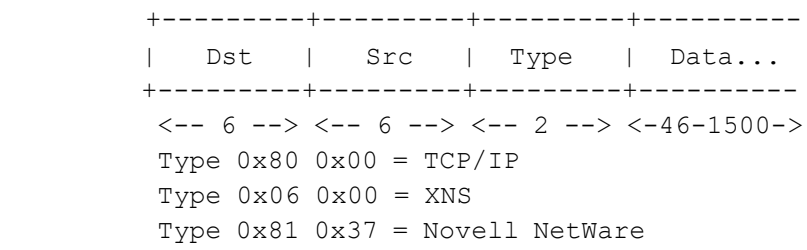
11. Análisis de una **IP 8.8.8.8**

- **Ethernet II**
    - Destination: HuaweiTechno_f7:8f:6b (48:12:58:f7:8f:6b)
    - Source: Dell_95:d0:fe (d4:be:d9:95:d0:fe)
    - Type: IPv4 (0x0800)
    - [Stream index: 2]
- **Internet Protocol Version 4**
    - 0100 .... = Version: 4
    - .... 0101 = Header Length: 20 bytes (5)
    - Total Length: 60
    - Identification: 0xba7e (47742)
    - 000. .... = Flags: 0x0
        - 0... .... = Reserved bit: Not set
        - .0.. .... = Don't fragment: Not set
        - ..0. .... = More fragments: Not set
    - ...0 0000 0000 0000 = Fragment Offset: 0
    - Time to Live: 128
    - Protocol: ICMP (1)

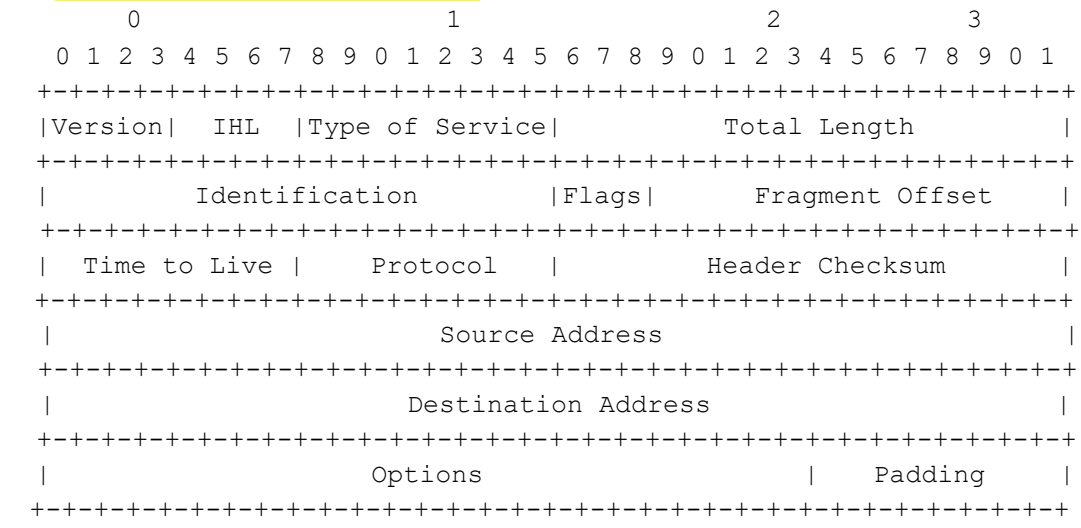
- Header Checksum: 0x0000 [validation disabled]
- Source Address: 192.168.100.12
- Destination Address: 8.8.8.8

- **Internet Control Message Protocol**
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0x4d34 [correct]
  - Identifier (BE): 1 (0x0001)
  - Identifier (LE): 256 (0x0100)
  - Sequence Number (BE): 39 (0x0027)
  - Sequence Number (LE): 9984 (0x2700)

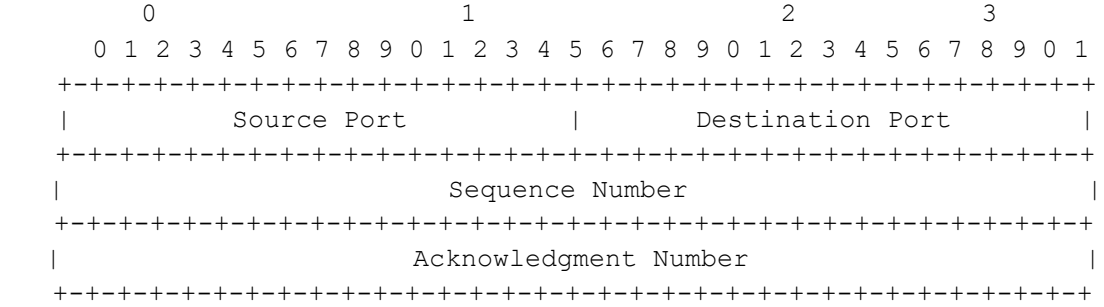
Trama Ethernet 2 (Capa de Enlace de Datos)

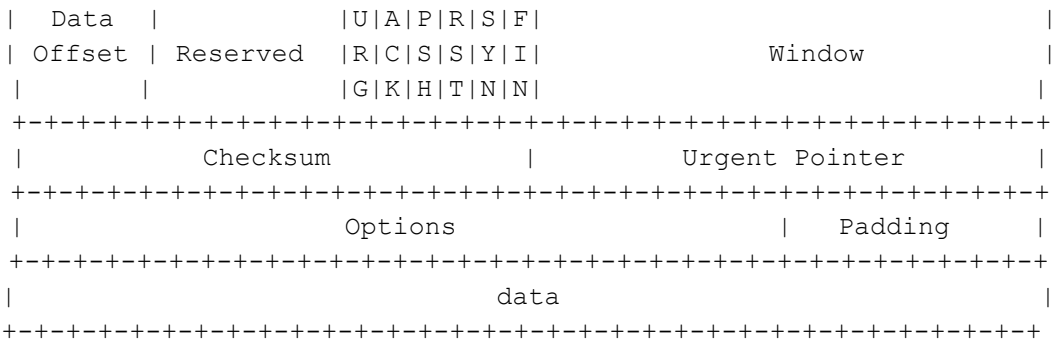


Encabezado IP (Capa de red)



Encabezado TCP (capa de Transporte)

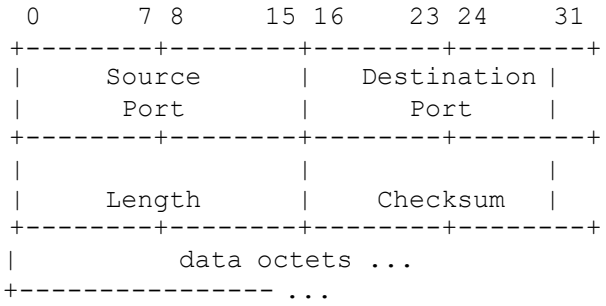




El campo Indicadores, que se encuentra junto al campo Ventana. Los valores a la derecha de la «b» representan los indicadores TCP que se establecen para esta etapa de la conversación de datos. Cada uno de los seis lugares corresponde a una bandera. La presencia de un «1» en cualquier lugar indica que el indicador está establecido. Se puede configurar más de una bandera a la vez. Los valores de las banderas se muestran a continuación.

Lugar de la bandera	6	5	4	3	2	1
Valor	URG	ACK	PSH	RST	SYN	FIN

Encabezado UDP (capa de Transporte)



De las capturas de los paquetes de los encabezados anteriores responde las preguntas:

1. Análisis de una **IP** de una **máquina de laboratorio**

MAC destino	IP destino	MAC origen	Puerto Origen
00:e0:4c:68:07:62	172.100.95.254	4c:eb:bd:80:50:27	172.100.91.209

2. Análisis de una **IP** de la página **www.escom.ipn.mx**

MAC destino	IP destino	Puerto destino	MAC origen	IP origen	Puerto Origen
48:12:58:f7:8f:6b	148.204.58.225	443	d4:be:d9:95:d0:fe	192.168.100.12	50573

3. Análisis de una **IP** de la pagina **www.saes.escom.ipn.mx**

MAC destino	IP destino	Puerto destino	MAC origen	IP origen	Puerto Origen
48:12:58:f7:8f:6b	148.204.56.240	443	d4:be:d9:95:d0:fe	192.168.100.12	50924

4. Análisis de una **IP 198.168.100.33 (celular)**

MAC destino	IP destino	MAC origen	Puerto Origen
48:12:58:f7:8f:6b	192.168.100.12	d2:74:3a:9f:2e:b5	192.168.100.33

5. Análisis de una **IP 148.204.61.254 (Gateway)**

MAC destino	IP destino	MAC origen	Puerto Origen
48:12:58:f7:8f:6b	192.168.100.1	d2:74:3a:9f:2e:b5	192.168.100.12

6. Análisis de una de la página **www.ipn.mx**

MAC destino	IP destino	Puerto destino	MAC origen	IP origen	Puerto Origen
48:12:58:f7:8f:6b	20.64.80.120	443	d2:74:3a:9f:2e:b5	192.168.100.12	51586

7. Análisis de una de la pagina **www.google.com.mx**

MAC destino	IP destino	MAC origen	IP origen
48:12:58:f7:8f:6b	2607:f8b0:4012:829::2003	d4:be:d9:95:d0:fe	2806:2f0:9200:9615:9bed:bf6e:e25:f31

8. Análisis de una de la pagina **www.facebook.com**

MAC destino	IP destino	MAC origen	IP origen
48:12:58:f7:8f:6b	2806:2f0:9200:9615:9bed:bf6e:e25:f31	d4:be:d9:95:d0:fe	2a03:2880:f135:83:face:b00c:0:25de

9. Análisis de una de la página http://www.lacartoons.com/

MAC destino	IP destino	Puerto destino	MAC origen	IP origen	Puerto Origen
48:12:58:f7:8f:6b	62.182.84.89	443	d2:74:3a:9f:2e:b5	192.168.100.12	54181

10. Análisis de una **IP 8.8.8.8**

MAC destino	IP destino	MAC origen	IP origen
48:12:58:f7:8f:6b	8.8.8.8	d4:be:d9:95:d0:fe	192.168.100.12

11. Capturar una trama ARP (mandar un ping a la **IP 148.204.56.255**) y rellenar los campos para una trama ARP

MAC destino	MAC origen	Tipo
ff:ff:ff:ff:ff:ff	ac:4e:65:96:f7:f0	ARP (0x0806)

Reflexión

12. ¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?

    Wireshark solo puede capturar direcciones MAC dentro del alcance de la red local porque las direcciones MAC no se propagan más allá de un segmento de red local (LAN). En redes basadas en TCP/IP, cuando los paquetes se envían fuera de la red local, las direcciones MAC se reemplazan en cada salto por las direcciones de origen y destino de los dispositivos intermedios, como routers. Por esta razón, solo es posible ver las direcciones MAC locales directamente conectadas al segmento de red en el que se realiza la captura.

13. ¿Cuál es la importancia del análisis de una red con el programa Wireshark?

    Permite diagnosticar problemas de red, mejorar la seguridad al detectar actividades sospechosas, optimizar el rendimiento identificando cuellos de botella, y entender mejor los protocolos y comunicaciones de red.

Conclusiones

Conclusión 1 (Areli Alejandra Guevara Badillo)

Wireshark ha demostrado ser una herramienta indispensable para el análisis y diagnóstico de redes, permitiendo visualizar la estructura detallada de los paquetes que transitan por la red. Durante la práctica, fue posible identificar aspectos críticos como direcciones MAC, IPs de origen y destino, y datos encapsulados en las distintas capas del modelo OSI. Además, su capacidad para capturar y filtrar tramas específicas resulta fundamental para localizar problemas como configuraciones erróneas, fallos de conectividad o incluso tráfico anómalo que podría indicar vulnerabilidades de seguridad. En el ámbito académico, esta práctica sirvió para consolidar conocimientos sobre el funcionamiento interno de las redes y los protocolos, conectando la teoría con aplicaciones prácticas esenciales en entornos reales.

Conclusión 2 (Rebeca Hernández Simón)

La experiencia con Wireshark permitió comprender en profundidad la importancia de analizar las comunicaciones dentro de una red, mostrando cómo se procesan y transportan los datos en cada capa. Este análisis facilita la detección de errores en configuraciones de red y posibles amenazas al monitorear actividades no autorizadas o inusuales. Durante la práctica, se logró identificar los diferentes componentes de una trama, desde las direcciones físicas hasta los puertos de las aplicaciones, lo cual resulta esencial para garantizar un rendimiento óptimo y la seguridad de las redes. Este tipo de herramientas no solo es vital para la resolución de problemas en redes empresariales o domésticas, sino también para el diseño eficiente de infraestructuras, mejorando la calidad de los servicios de comunicación en cualquier entorno.

Firma de la practica

Práctica Analisis de Red

10/12/2024

·Guevara Badillo Areli Alejandra
·Hernandez Simón Rebeca