UNIVERSIDAD DEL VALLE DE GUATEMALA

Laboratorio 1

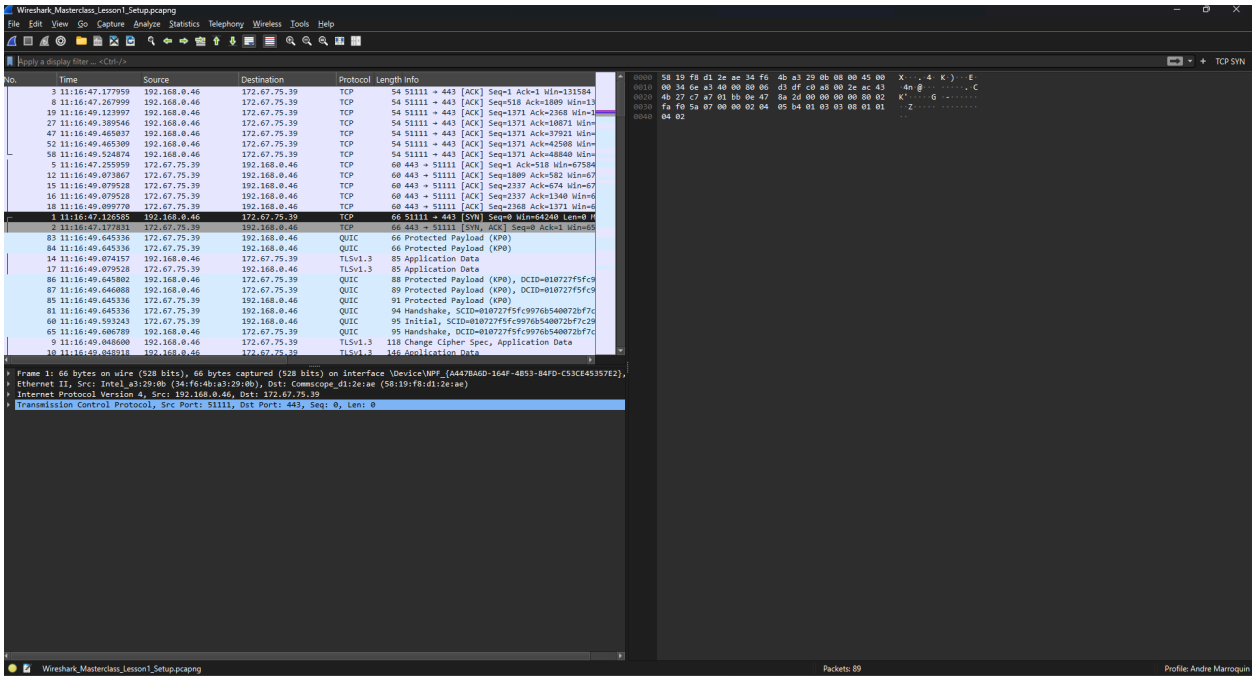
Andre Marroquin Tarot - 22266

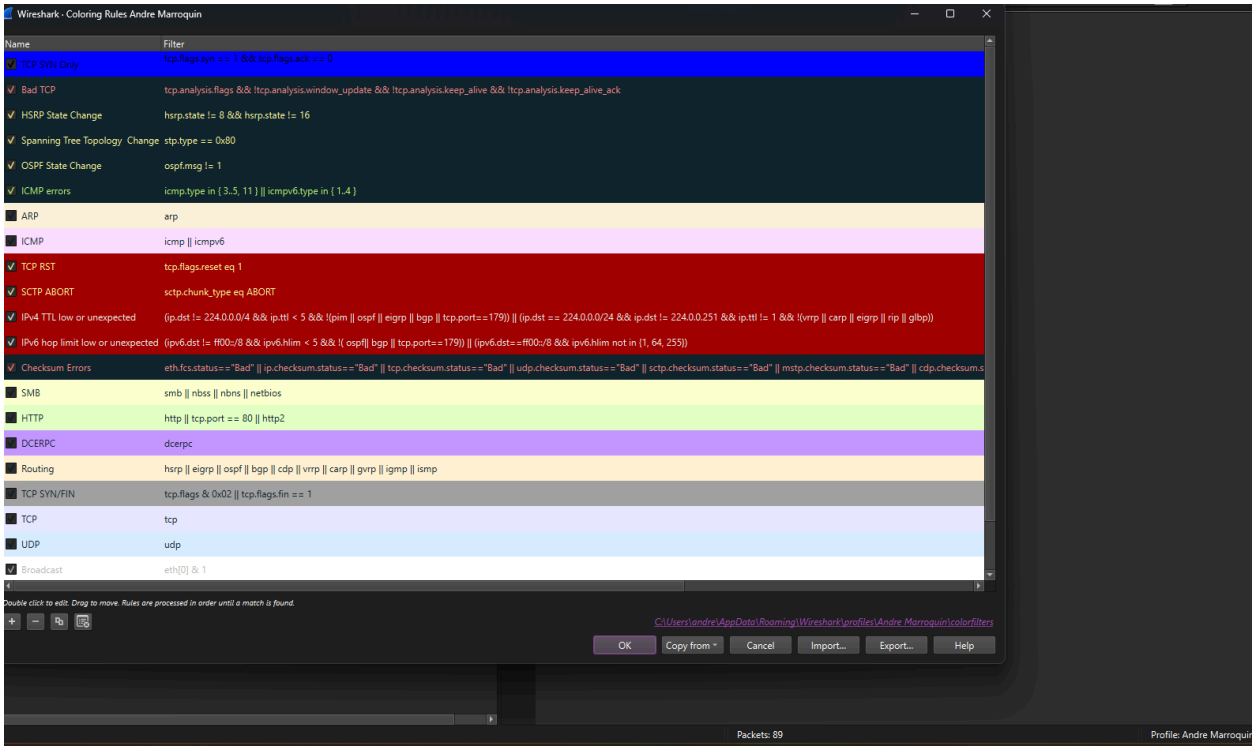
Redes

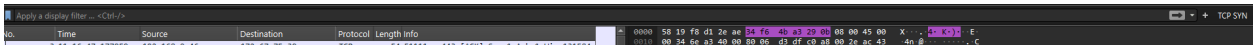
Introduccion

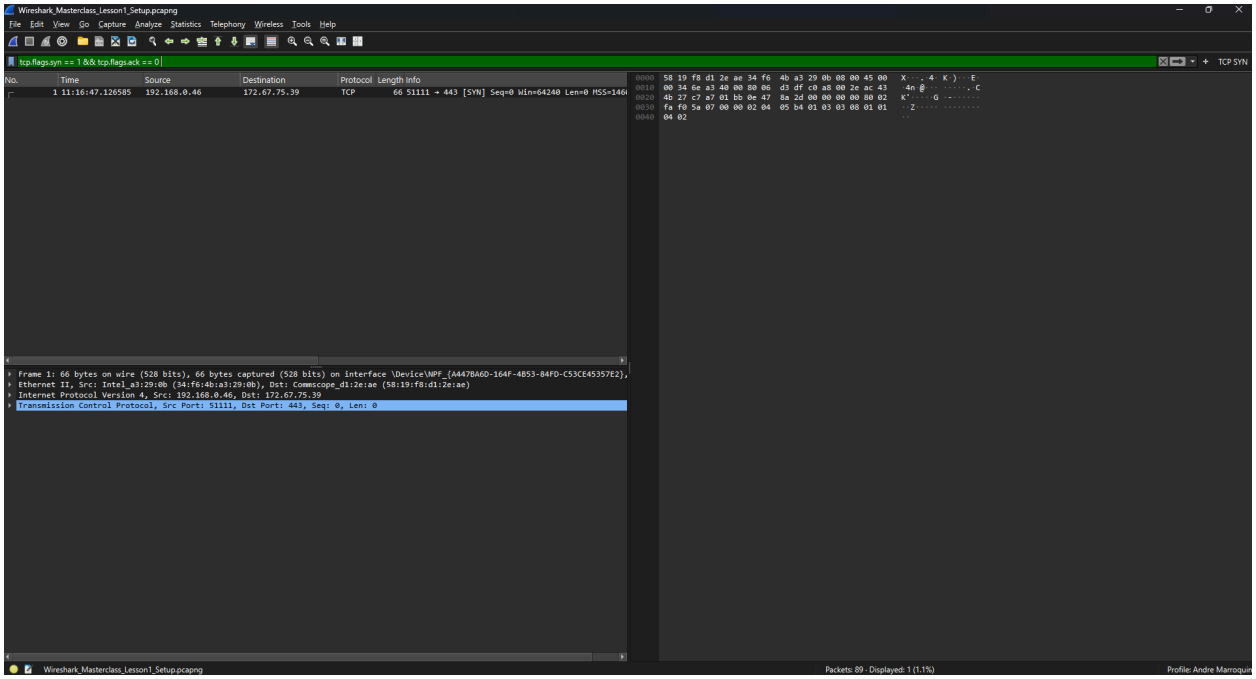
La actividad tuvo como objetivo principal familiarizarse con el uso de Wireshark, una herramienta de análisis de protocolos de red. A través de distintas prácticas, se realizaron capturas de tráfico en tiempo real, se configuraron parámetros de captura como el ring buffer, y se analizaron protocolos clave como HTTP. Estas acciones permitieron comprender el flujo de información en una red, identificar el comportamiento del navegador al acceder a sitios web, y aplicar técnicas básicas de diagnóstico de red.

Parte 1.1 Entorno Wireshark

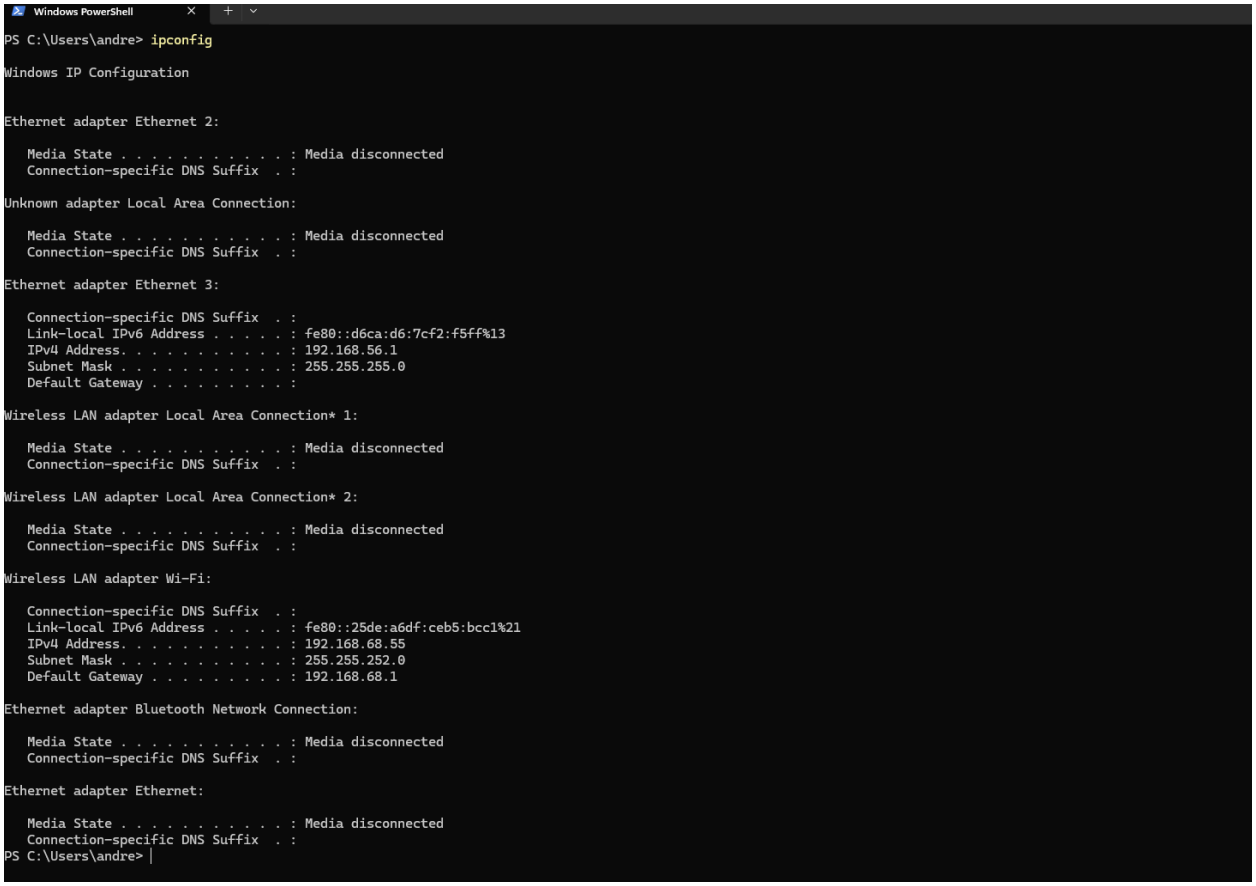



Wireshark · Coloring Rules Andre Marroquin
Name
Filter
TCP SYN Only
tcp.flags.syn == 1 && tcp.flags.ack == 0
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
IPv4 TTL low or unexpected
(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf || eigrp || bgp || tcp.port==179)) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp || eigrp || rip || glbp))
IPv6 hop limit low or unexpected
(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tcp.port==179)) || (ipv6.dst==ff00::/8 && ipv6.hlim not in {1, 64, 255})
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || mstp.checksum.status=="Bad" || cdp.checksum.s
SMB
smb || nbss || nbns || netbios
HTTP
http || tcp.port == 80 || http2
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
Double click to edit. Drag to move. Rules are processed in order until a match is found.
C:\Users\andre\AppData\Roaming\Wireshark\profiles\Andre Marroquin\colorfilters
OK
Copy from
Cancel
Import...
Export...
Help
Packets: 89
Profile: Andre Marroquin


Apply a display filter ... <Ctrl-/>
TCP SYN
No.
Time
Source
Destination
Protocol
Length Info


Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 && tcp.flags.ack == 0
TCP SYN
No. Time Source Destination Protocol Length Info
1 11:16:47.126585 192.168.0.46 172.67.75.39 TCP 66 51111 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A447BA6D-164F-4B53-84FD-C53CE45357E2},
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:0b), Dst: Commscope_d1:2e:ae (58:19:f8:d1:2e:ae)
Internet Protocol Version 4, Src: 192.168.0.46, Dst: 172.67.75.39
Transmission Control Protocol, Src Port: 51111, Dst Port: 443, Seq: 0, Len: 0
Wireshark_Masterclass_Lesson1_Setup.pcapng
Packets: 89 - Displayed: 1 (1.1%)
Profile: Andre Marroquin

Parte 1.2



Varias interfaces de red aparecen como desconectadas, incluyendo:

- Ethernet adapter Ethernet 2
- Unknown adapter Local Area Connection
  Local Area Connections 1 y 2
- Bluetooth Network Connection
- Ethernet adapter Ethernet

Estas no están activas actualmente estado: Media disconnected.

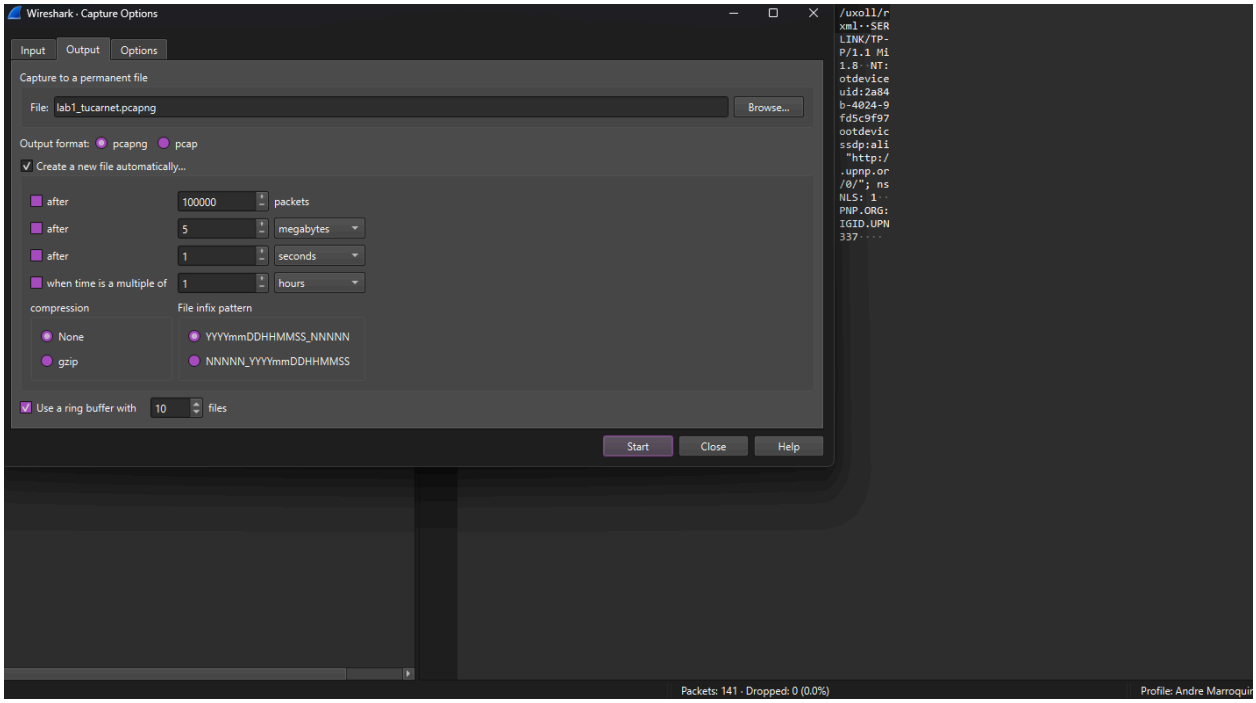
Interfaz activa por cable (Ethernet 3):

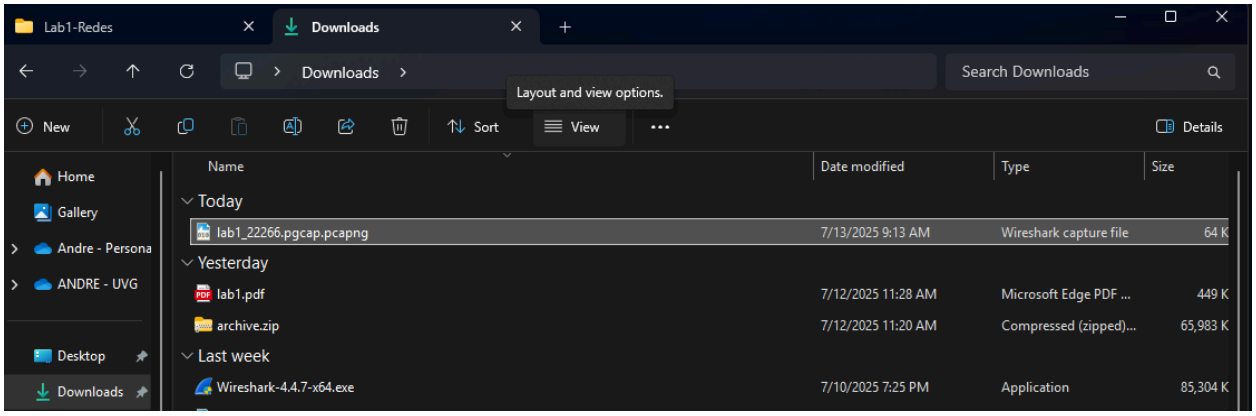
- IP privada: 192.168.56.1
- Máscara: 255.255.255.0
- Sin puerta de enlace visible una red interna o virtual, como VirtualBox

Interfaz activa por Wi-Fi:

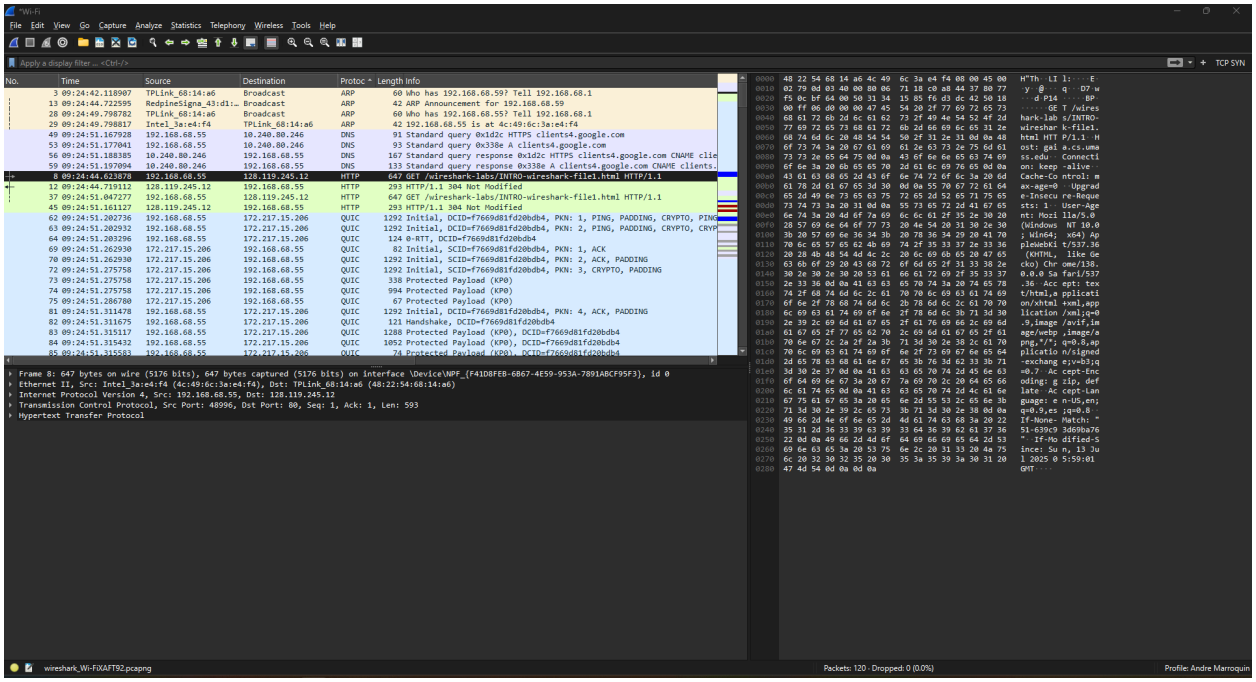
- IP privada: 192.168.68.55

- Máscara: 255.255.252.0
- Gateway: 192.168.68.1 → Esta es la red realmente conectada a internet.





Parte 1.3



Respuestas a preguntas

a. ¿Qué versión de HTTP está ejecutando su navegador?
El navegador está utilizando HTTP/1.1, como se observa en la solicitud GET capturada en Wireshark.

b. ¿Qué versión de HTTP está ejecutando el servidor?
El servidor también está utilizando HTTP/1.1, lo cual se confirma en el paquete de respuesta identificado con el código HTTP/1.1 304 Not Modified.

c. ¿Qué lenguajes (si aplica) indica el navegador que acepta al servidor?
El navegador indica que acepta contenido en inglés estadounidense y en inglés genérico, mediante el encabezado Accept-Language: en-US,en;q=0.9, donde en-US tiene prioridad alta y en prioridad secundaria.

d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?
El servidor no devolvió contenido, es decir, 0 bytes, ya que respondió con el código 304 Not Modified, lo cual significa que el recurso solicitado ya se encontraba en caché en el navegador y no fue necesario reenviarlo.

e. En el caso que haya un problema de rendimiento mientras se descarga la página, ¿en qué elementos de la red convendría "escuchar" los paquetes? ¿Es conveniente instalar Wireshark en el servidor? Justifique.

Para diagnosticar problemas de rendimiento conviene capturar paquetes en el cliente, en el gateway o firewall, y en servidores intermedios si existen, para analizar latencias, pérdidas o cuellos de botella, instalar Wireshark en el servidor no es recomendable salvo que se tenga acceso administrativo, ya que en la mayoría de los casos no se tiene control sobre servidores remotos y capturar tráfico desde allí podría violar políticas de seguridad.

Discusión sobre la actividad, experiencia y hallazgos:

Durante la actividad se realizaron capturas de paquetes en Wireshark usando distintas configuraciones y enfoques. En la primera parte se identificaron correctamente las interfaces activas mediante el comando ipconfig, reconociendo que la interfaz Wi-Fi era la principal vía de conexión. Luego, se configuró un buffer circular ring buffer para almacenar múltiples archivos de captura con un límite de tamaño y cantidad, lo cual permitió observar cómo Wireshark rota archivos al alcanzar los valores definidos.

En la segunda parte, se analizó el protocolo HTTP accediendo a un sitio específico gaia.cs.umass.edu sin cifrado, lo que permitió capturar el tráfico en texto claro. Se identificaron correctamente las versiones de HTTP utilizadas por el navegador y el servidor, los encabezados enviados como Accept-Language y el tipo de respuesta del servidor código 304, lo que evidenció el uso de caché del navegador.

Comentarios:

La actividad permitió familiarizarse con el entorno de Wireshark y sus funciones como filtros, reglas de color y configuración de salidas personalizadas. Se comprobó la utilidad del análisis de tráfico para entender el comportamiento real de aplicaciones web, los protocolos, y el funcionamiento de la caché HTTP. También se evidenció la importancia de ubicar correctamente los puntos de captura dependiendo del tipo de red y acceso disponible.

Conclusiones:

- Wireshark es una herramienta fundamental para el análisis de redes, ya que permite observar el tráfico en tiempo real y entender el funcionamiento de los protocolos.

- La actividad permitió reforzar conceptos de redes, como el protocolo HTTP, la identificación de interfaces de red activas y el uso de buffers de captura.

- Se comprobó la utilidad de capturar tráfico en los puntos correctos de la red, como el cliente o el gateway, para identificar cuellos de botella, pérdidas de paquetes o problemas de latencia.

- También se resaltó la importancia de tener acceso administrativo al servidor, en caso de necesitar análisis desde ese punto, especialmente cuando se trata de redes privadas o entornos controlados.

- En resumen, la actividad brindó una comprensión práctica del monitoreo y análisis de tráfico de red, útil tanto para diagnóstico como para aprendizaje de protocolos.

Referencias:

- Garn, D. (2024, 7 agosto). *Examine a captured packet using Wireshark*. Search Networking. https://www.techtarget.com/searchnetworking/tutorial/Examine-a-captured-packet-using-Wireshark

- Seltzer, H. (2025, 7 julio). Is There Really a Difference Between Wi-Fi vs. Ethernet? I Tested Both to Find Out. *CNET*. https://www.cnet.com/home/internet/wi-fi-vs-ethernet/