Universidad del Valle de Guatemala

Redes

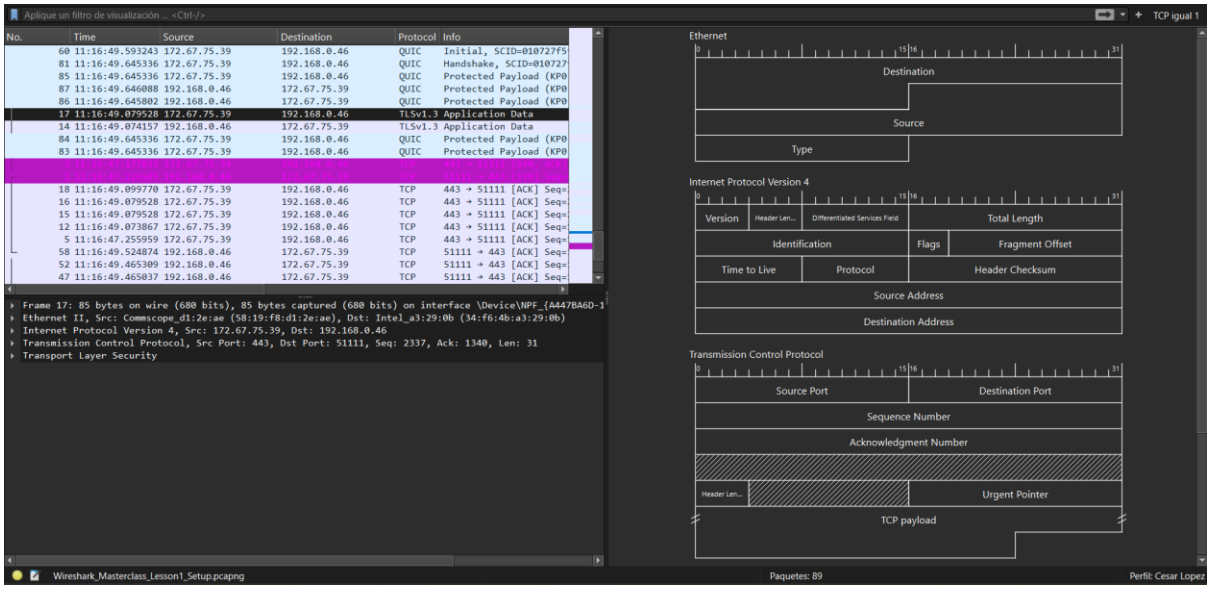
Sección # 20

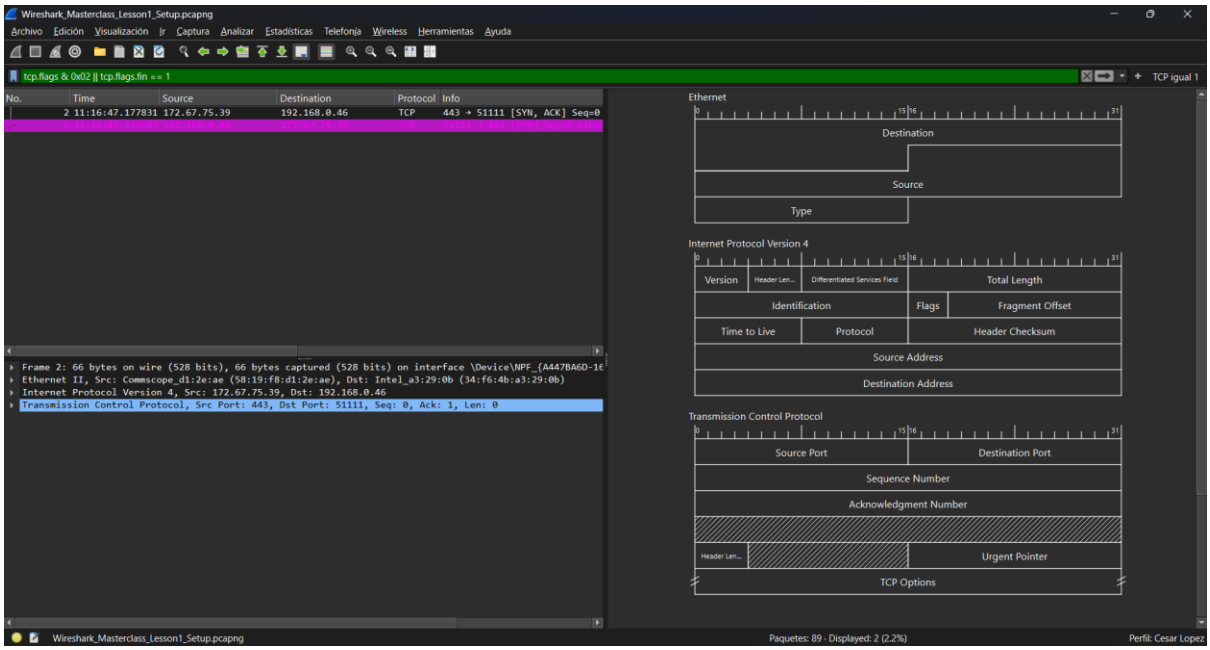
Pablo Cesar Lopez Medina

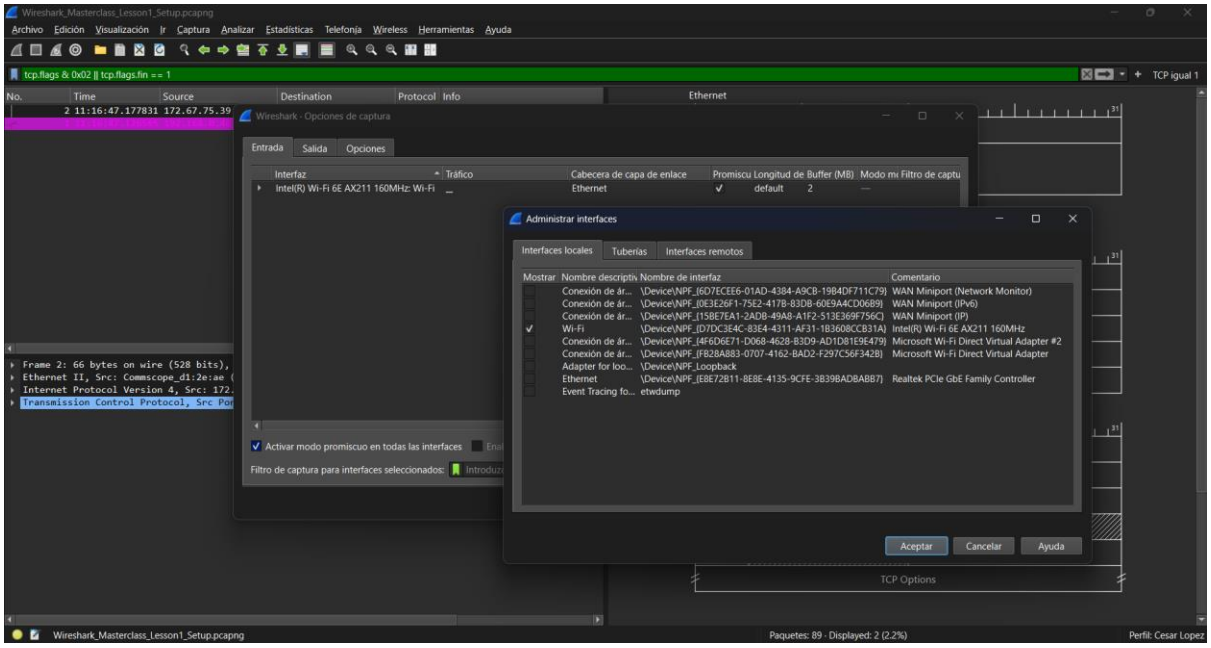
Carnet # 22535

Laboratorio # 1 – Parte 2

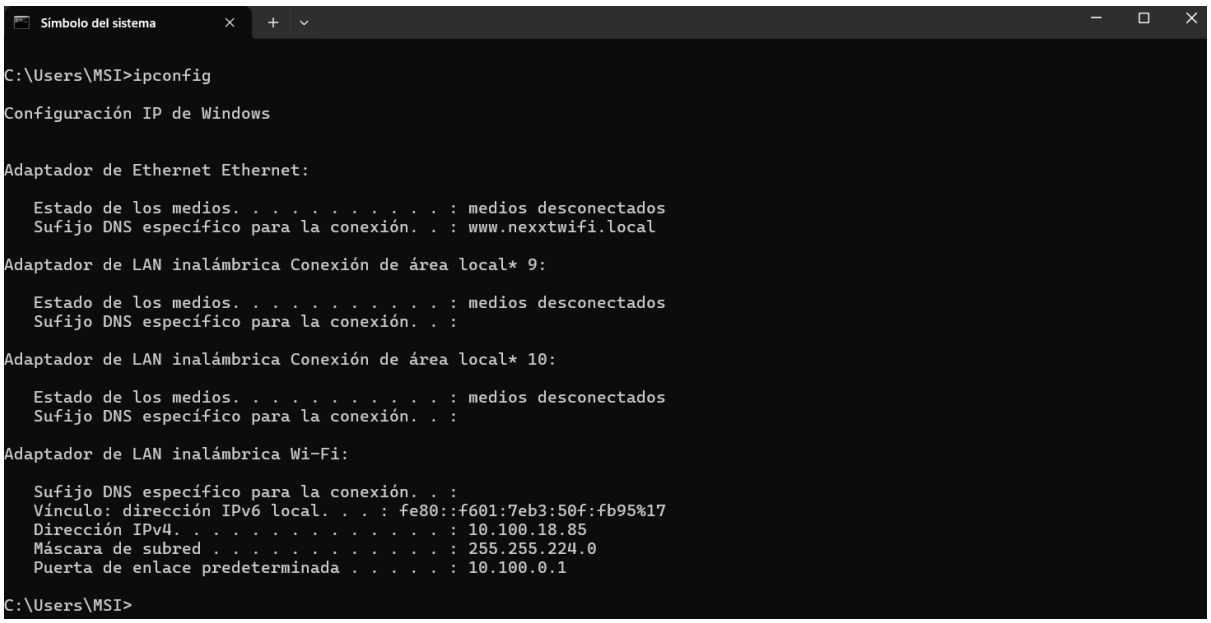
1.1

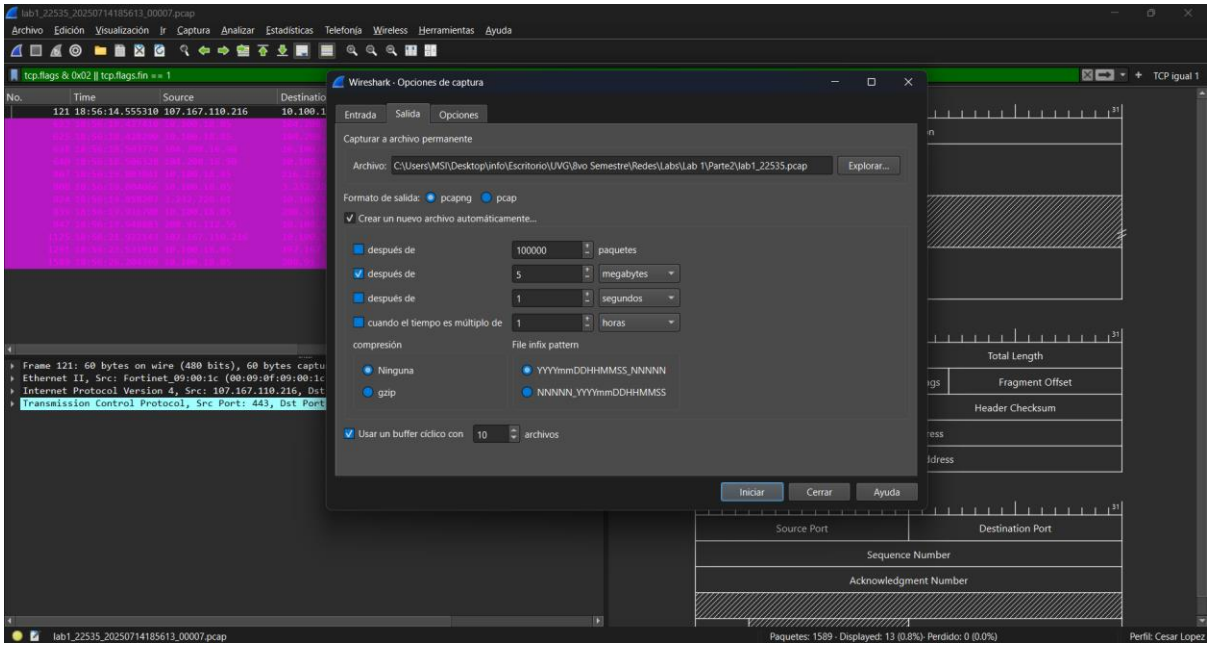


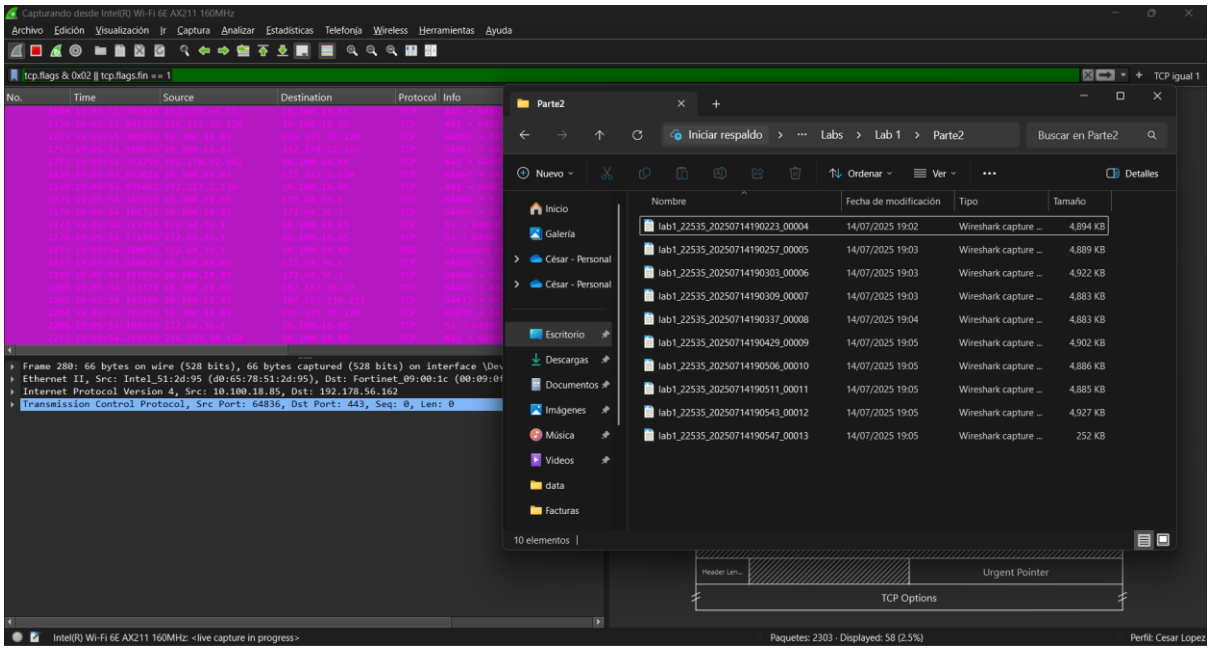


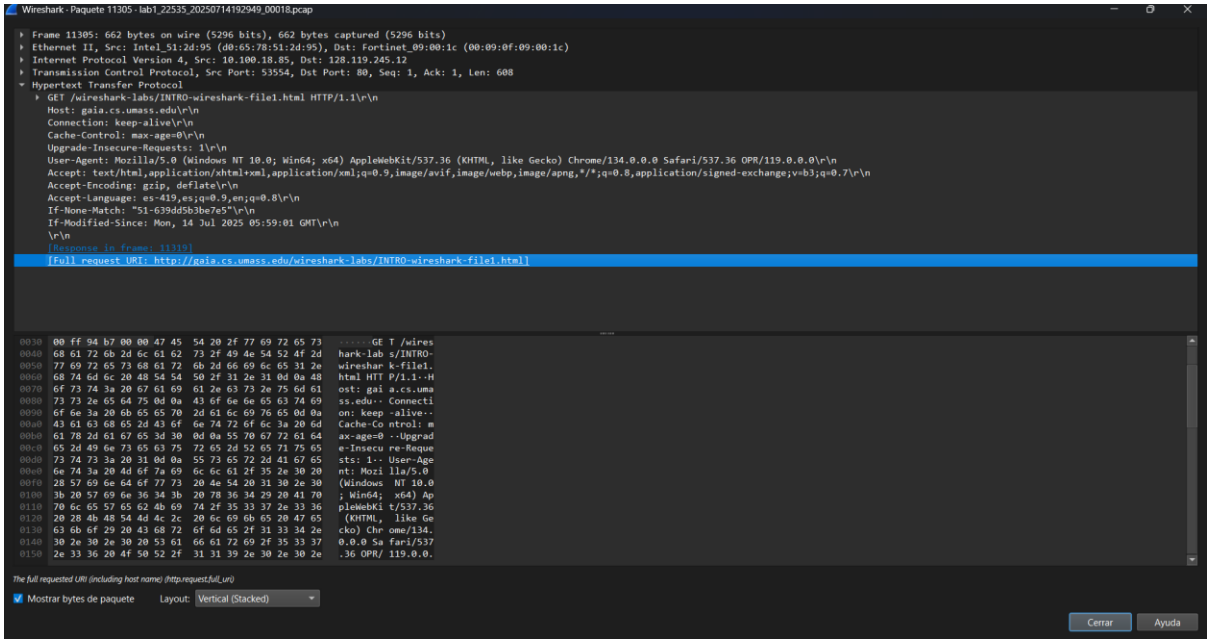

Wireshark_Masterclass_Lesson1_Setup.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
tcp.flags & 0x02 || tcp.flags.fin == 1
No. Time Source Destination Protocol Info
2 11:16:47.177831 172.67.75.39
Ethernet
Wireshark · Opciones de captura
Entrada Salida Opciones
Interfaz Tráfico Cabecera de capa de enlace Promiscu Longitud de Buffer (MB) Modo mi Filtro de captu
Intel(R) Wi-Fi 6E AX211 160MHz: Wi-Fi Ethernet default 2
Administrar interfaces
Interfaces locales Tuberías Interfaces remotos
Mostrar Nombre descripti Nombre de interfaz Comentario
Conexión de ár... \Device\NPF_{6D7ECEE6-01AD-4384-A9CB-19B4DF711C79} WAN Miniport (Network Monitor)
Conexión de ár... \Device\NPF_{0E3E26F1-75E2-417B-B3DB-60E9A4CD06B9} WAN Miniport (IPv6)
Conexión de ár... \Device\NPF_{158E7EA1-2ADB-49A8-A1F2-513E369F756C} WAN Miniport (IP)
Wi-Fi \Device\NPF_{D7DC3E4C-B3E4-4311-AF31-1B3608CCB31A} Intel(R) Wi-Fi 6E AX211 160MHz
Conexión de ár... \Device\NPF_{4F6D6E71-D068-4628-B3D9-AD1D81E9E479} Microsoft Wi-Fi Direct Virtual Adapter #2
Conexión de ár... \Device\NPF_{FB28A883-0707-4162-BAD2-F297C56F342B} Microsoft Wi-Fi Direct Virtual Adapter
Adapter for loo... \Device\NPF_Loopback
Ethernet \Device\NPF_{E8E72B11-8E8E-4135-9CFE-3B39BADBABB7} Realtek PCIe GbE Family Controller
Event Tracing fo... etwdump
Activar modo promiscuo en todas las interfaces
Filtro de captura para interfaces seleccionados:
Aceptar Cancelar Ayuda
Frame 2: 66 bytes on wire (528 bits),
Ethernet II, Src: Commscope_d1:2e:ae (
Internet Protocol Version 4, Src: 172.
Transmission Control Protocol, Src Por
TCP Options
Wireshark_Masterclass_Lesson1_Setup.pcapng
Paquetes: 89 · Displayed: 2 (2.2%)
Perfil: Cesar Lopez

1.2


Símbolo del sistema
C:\Users\MSI>ipconfig
Configuración IP de Windows
Adaptador de Ethernet Ethernet:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . : www.nexxtwifi.local
Adaptador de LAN inalámbrica Conexión de área local* 9:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de LAN inalámbrica Conexión de área local* 10:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de LAN inalámbrica Wi-Fi:
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::f601:7eb3:50f:fb95%17
Dirección IPv4. . . . . : 10.100.18.85
Máscara de subred . . . . . : 255.255.224.0
Puerta de enlace predeterminada . . . . . : 10.100.0.1
C:\Users\MSI>


Wireshark - Opciones de captura
Entrada
Salida
Opciones
Capturar a archivo permanente
Archivo: C:\Users\MSI\Desktop\info\Escritorio\UVG\8vo Semestre\Redes\Labs\Lab 1\Parte2\lab1_22535.pcap
Explorar...
Formato de salida: pcapng pcap
Crear un nuevo archivo automáticamente...
después de 100000 paquetes
después de 5 megabytes
después de 1 segundos
cuando el tiempo es múltiplo de 1 horas
compresión
Ninguna
gzip
File infix pattern
YYYYmmDDHHMMSS_NNNNN
NNNNN_YYYYmmDDHHMMSS
Usar un buffer ciclico con 10 archivos
Iniciar
Cerrar
Ayuda
Total Length
Fragment Offset
Header Checksum
Source Port
Destination Port
Sequence Number
Acknowledgment Number


Parte2
Iniciar respaldo
Labs
Lab 1
Parte2
Buscar en Parte2
Nuevo
Ordenar
Ver
Detalles
Inicio
Galería
César - Personal
Escritorio
Descargas
Documentos
Imágenes
Música
Videos
data
Facturas
Nombre
Fecha de modificación
Tipo
Tamaño
lab1_22535_20250714190223_00004 14/07/2025 19:02 Wireshark capture ... 4,894 KB
lab1_22535_20250714190257_00005 14/07/2025 19:03 Wireshark capture ... 4,889 KB
lab1_22535_20250714190303_00006 14/07/2025 19:03 Wireshark capture ... 4,922 KB
lab1_22535_20250714190309_00007 14/07/2025 19:03 Wireshark capture ... 4,883 KB
lab1_22535_20250714190337_00008 14/07/2025 19:04 Wireshark capture ... 4,883 KB
lab1_22535_20250714190429_00009 14/07/2025 19:05 Wireshark capture ... 4,902 KB
lab1_22535_20250714190506_00010 14/07/2025 19:05 Wireshark capture ... 4,886 KB
lab1_22535_20250714190511_00011 14/07/2025 19:05 Wireshark capture ... 4,885 KB
lab1_22535_20250714190543_00012 14/07/2025 19:05 Wireshark capture ... 4,927 KB
lab1_22535_20250714190547_00013 14/07/2025 19:05 Wireshark capture ... 252 KB
10 elementos
Urgent Pointer
TCP Options



Responda las siguientes preguntas:

a. ¿Qué versión de HTTP está ejecutando su navegador?

Http /1.1

b. ¿Qué versión de HTTP está ejecutando el servidor?

Http/1.1

c. ¿Qué lenguajes (si aplica) indica el navegador que acepta a el servidor?

Accept-Language: es-419,es;q=0.9,en;q=0.8\r\n

d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?

Capture Length: 662 bytes (5296 bits)

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

Se recomienda escuchar los paquetes en el cliente (10.100.18.85), para detectar retrasos, pérdidas o tiempos de espera. No es necesario instalar Wireshark en el servidor, a menos que el problema está en la generación de la respuesta. Mejor capturar desde otro punto para evitar afectar el rendimiento o comprometer la seguridad del servidor.

Comentarios:

El laboratorio me pareció bastante útil para comprender de manera práctica el funcionamiento de los protocolos de red y el análisis de tráfico mediante herramientas como Wireshark. Pude observar directamente cómo se transmiten los datos y los distintos encabezados que acompañan a los paquetes. La actividad de conmutación también permitió entender mejor los problemas que pueden surgir al haber intermediarios en la red.

Conclusiones:

El monitoreo desde el cliente es menos invasivo que desde el servidor, y más recomendable para evitar problemas de rendimiento y seguridad.

Las herramientas como Wireshark son fundamentales para el diagnóstico y análisis de redes, ya que permiten ver en detalle cómo viajan los datos.

Es complicado capturar el trafico de HTPP ya que algunos navegadores redirigen directamente a otro protocolo y el cache tiene que estar limpio para que capture el trafico nuevo.

Referencias:

https://support.atlassian.com/atlassian-knowledge-base/kb/how-to-capture-http-traffic-using-wireshark-fiddler-or-tcpdump/