Sniffer - Wireshark

Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@July 3, 2024
Wochentage	Mittwoch
Deadline	@July 4, 2024
Status	Sended
Attached files	Unidad_50_Sniffer - Wireshark.pdf

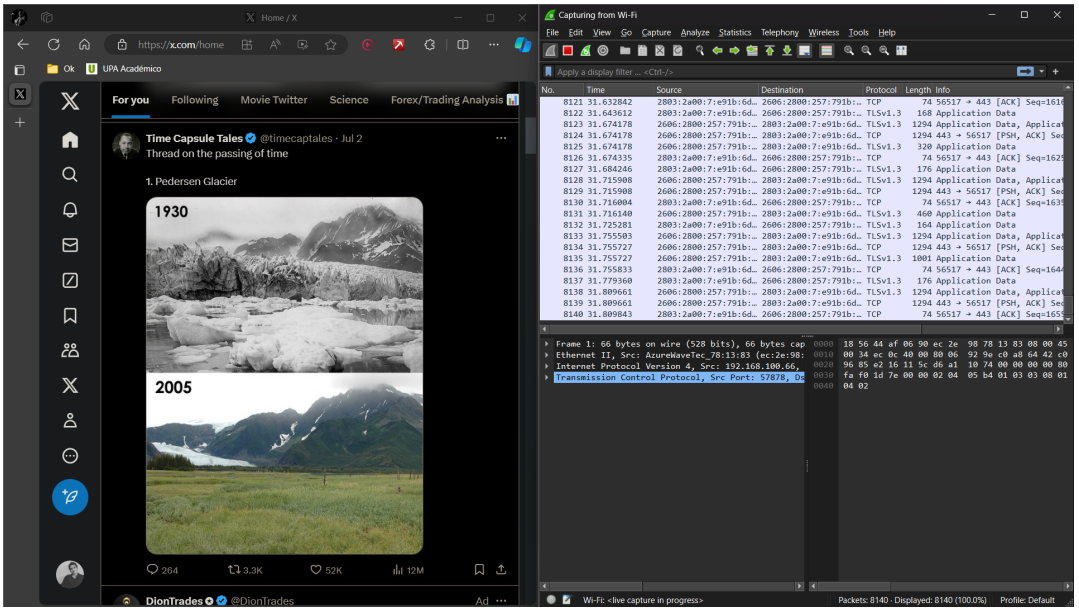
Ejercicios Prácticos

Ejercicio 1: Captura Básica

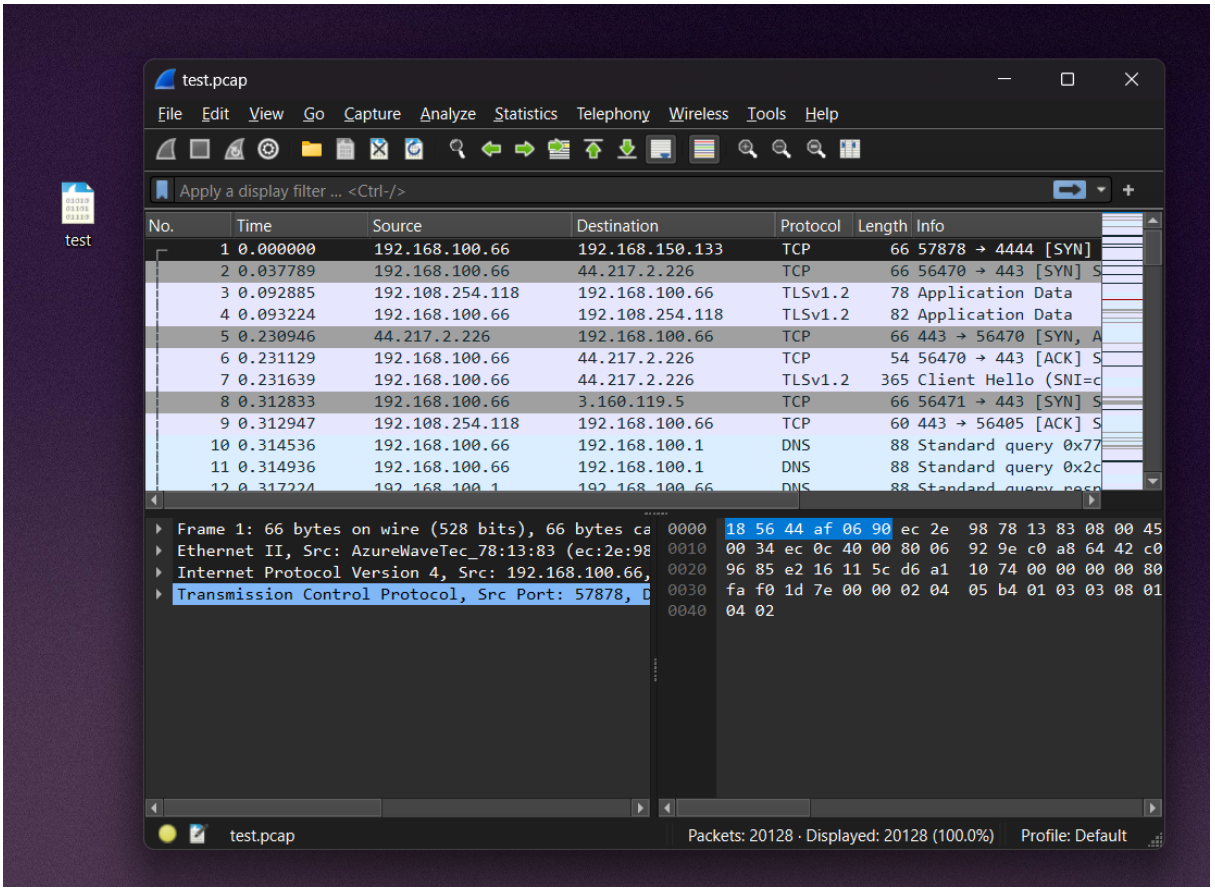
Objetivo: Aprender a capturar tráfico de red.

Pasos:

1. Abre Wireshark y selecciona la interfaz de red que deseas monitorear (e.g., Wi-
   Fi, Ethernet).
2. Haz clic en el botón azul con un tiburón para iniciar la captura.
3. Navega por Internet durante 5 minutos. Puedes visitar algunos sitios web, realizar búsquedas y observar cómo se capturan los paquetes.
4. Después de 5 minutos, haz clic en el botón rojo cuadrado para detener la captura.
5. Guarda el archivo de captura seleccionando Archivo > Guardar como y elige
   un formato como .pcap.



test.pcap



Ejercicio 2: Filtros de Captura

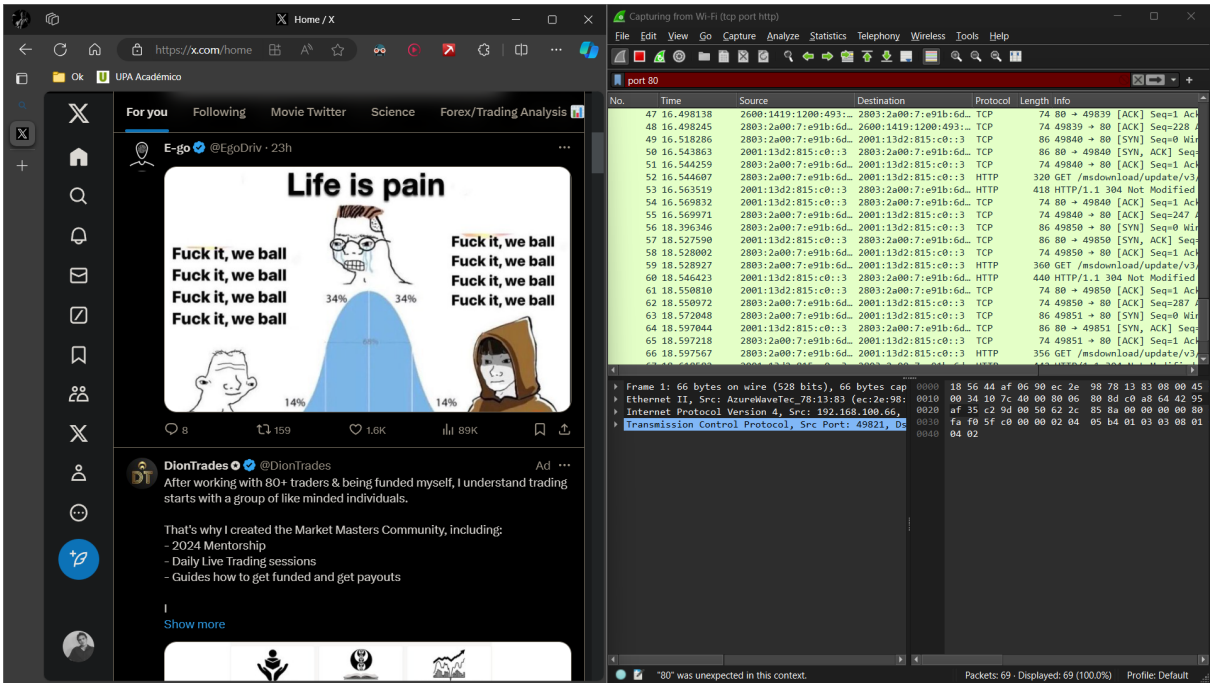
Objetivo: Aprender a aplicar filtros de captura para enfocar el análisis en tráfico específico.

Pasos:

1. Abre Wireshark y selecciona la interfaz de red.
2. Antes de iniciar la captura, aplica un filtro para capturar solo tráfico HTTP. En el campo de filtro de captura, escribe:

```
port 80
```

3. Haz clic en el botón azul con un tiburón para iniciar la captura.
4. Navega a algunos sitios web y observa que solo se capturan paquetes HTTP.
5. Detén la captura después de unos minutos y guarda el archivo.



Ejercicio 3: Análisis de Paquetes

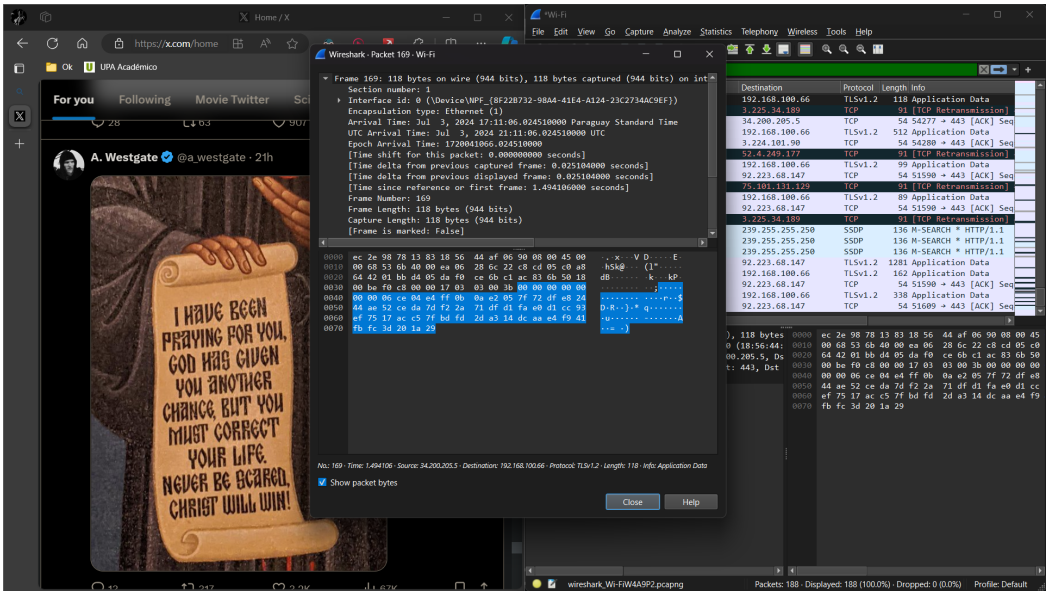
Objetivo: Aprender a analizar los detalles de un paquete específico.

Pasos:

1. Abre Wireshark y selecciona la interfaz de red.
2. Captura tráfico de tu red doméstica durante unos minutos.
3. Detén la captura y usa el campo de filtro de visualización para encontrar paquetes DNS. Escribe:

```
dns
```

4. Selecciona un paquete DNS y en el panel inferior, expande las capas para analizar los campos del paquete DNS. Describe los campos como la consulta, la respuesta, el nombre del dominio, etc.

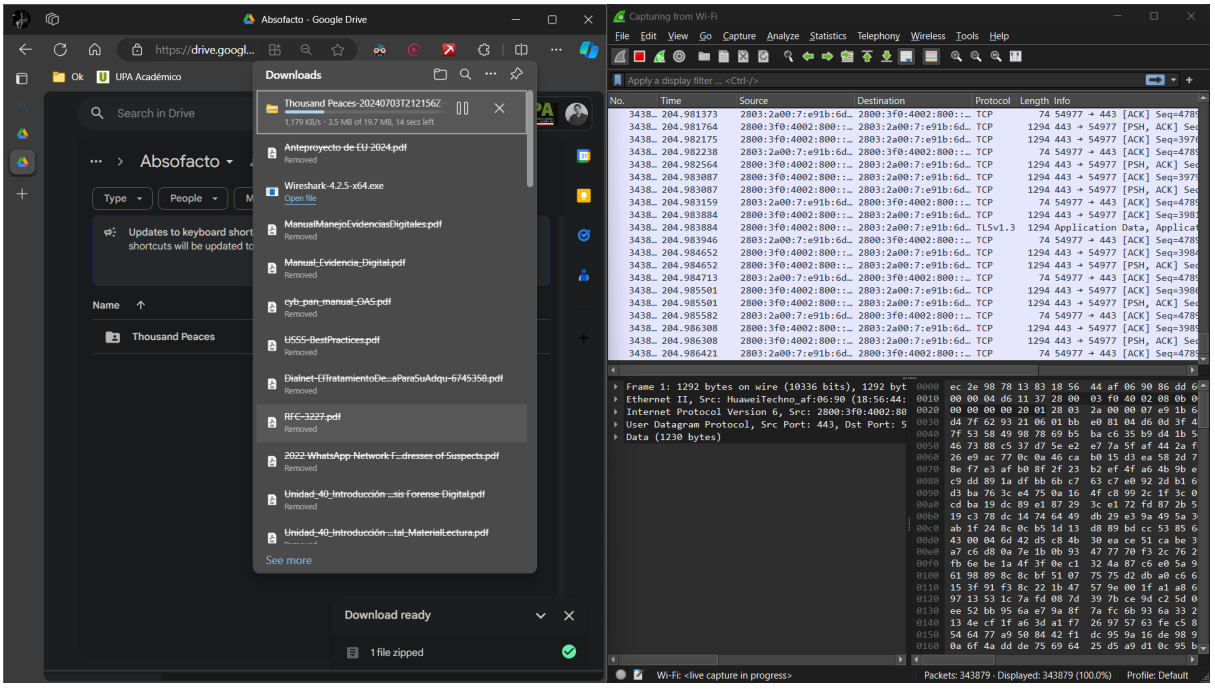


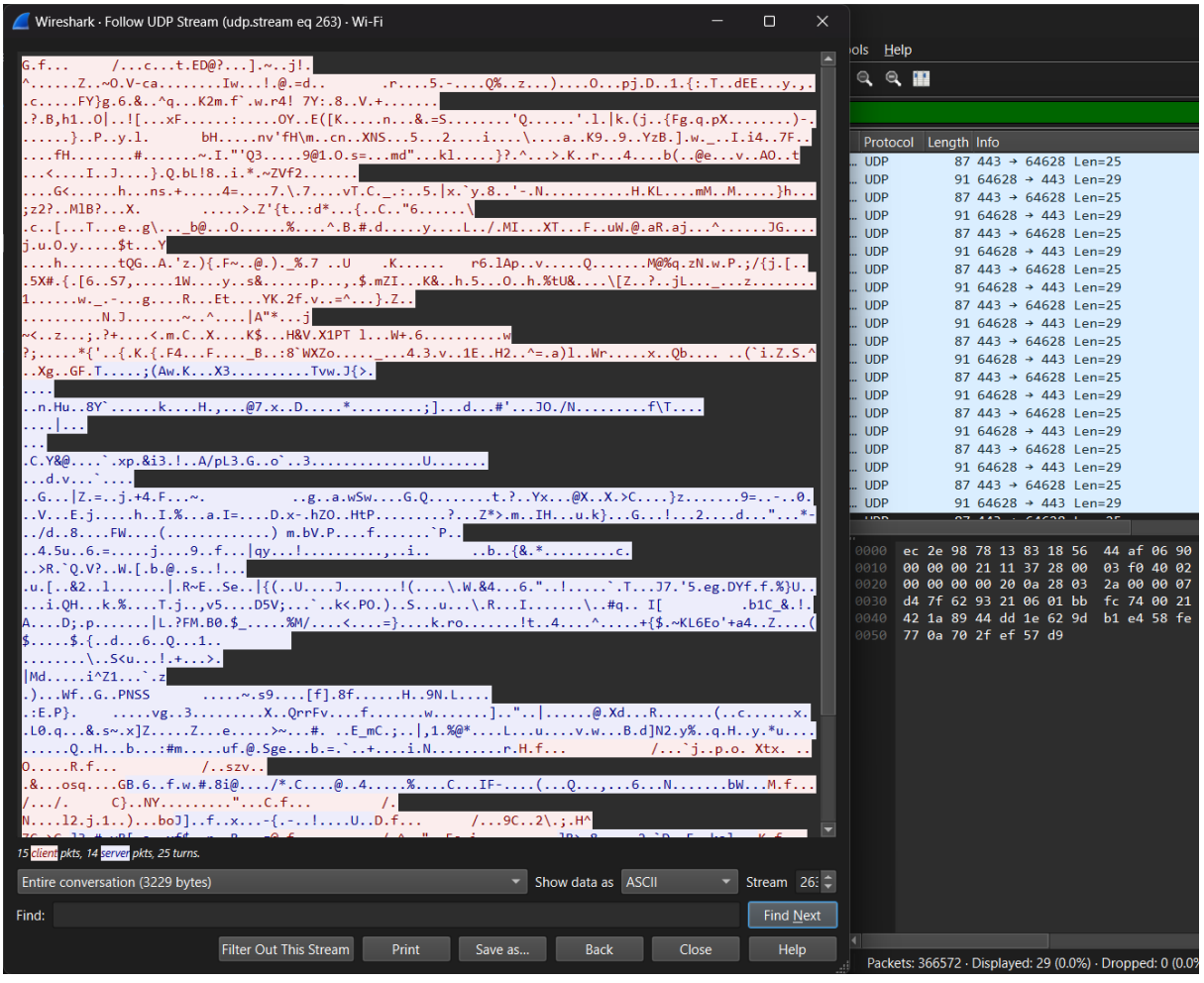
Ejercicio 4: Seguimiento de Sesión

Objetivo: Aprender a reconstruir y visualizar sesiones de comunicación completas.

Pasos:

1. Abre Wireshark y selecciona la interfaz de red.
2. Captura tráfico mientras descargas un archivo grande.
3. Detén la captura una vez que la descarga haya finalizado.
4. Usa la función de seguimiento de flujo TCP:
   o Selecciona un paquete de la descarga.
   o Haz clic derecho y selecciona Seguir > Flujo TCP.
   o Observa la conversación completa entre el cliente y el servidor.
5. Analiza los datos reconstruidos y describe el proceso de transferencia.





Durante la transferencia de un archivo grande, el cliente y el servidor intercambian datos en múltiples segmentos, gestionando la conexión y

confirmando la recepción de los datos para asegurar una transmisión completa y fiable.
