Universidad del Valle de Guatemala
Facultad de Ingeniería
Departamento de Ciencias de la Computación
CC3067 - Redes

Laboratorio #1 – Esquemas de comunicación e Introducción a Wireshark

Semestre II - 2025

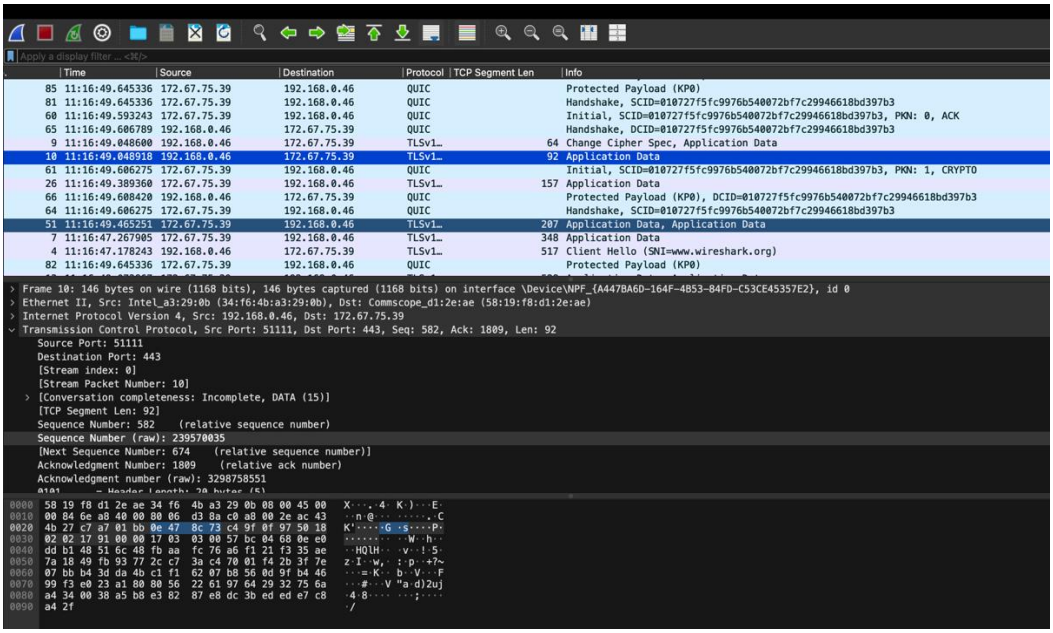
Bryan Carlos Roberto España Machorro – 21550

Introducción:
En este laboratorio exploramos el software wireshark, una herramienta de análisis de protocolos de red para personalizar el entorno, configurar capturas avanzadas, y analizar tráfico HTTP. A través de ejercicios prácticos, se busca fortalecer la comprensión de protocolos como TCP y HTTP, y cómo se comportan en una red local durante sesiones de navegación web.

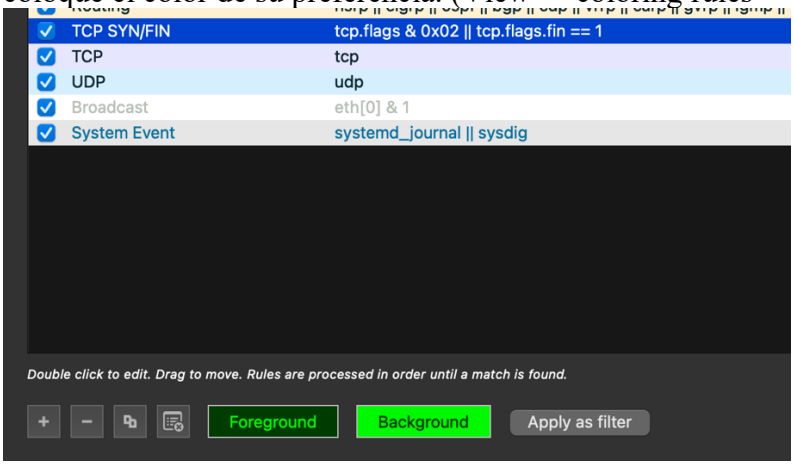
1.1 Personalización del entorno

En la primera parte se realizará la personalización del entorno de Wireshark, de modo que se adapte a nuestras preferencias de uso.

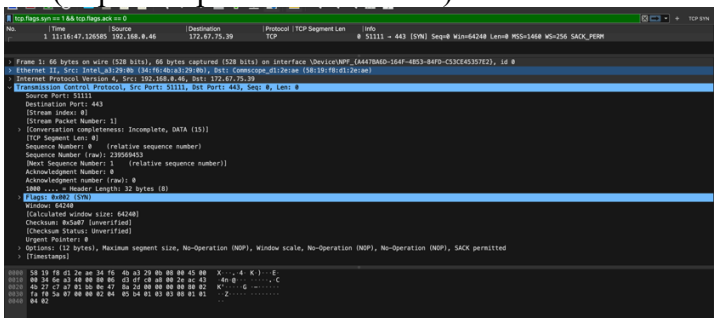
1. Inicie Wireshark
2. Cree un perfil con su primer nombre y primer apellido (edit -> configuration profile)
3. Descargue el archivo https://www.cloudshark.org/captures/e6fb36096dbb (Export -> Download)
4. Abra el archivo descargado, el archivo contiene transmisiones capturadas, y existen diversas columnas que representan la data.
5. Aplique el formato de tiempo Time of Day (view -> Time Display Format)
6. Agregue una columna con la longitud del protocolo (preferences -> column -> +)
7. Elimine u oculte la columna Longitud (click derecho -> desmarcar columna)
8. Aplique un esquema de paneles que sea de su preferencia (que no sea el esquema por defecto) (preferences -> Layout
   Cambios aplicados desde el punto 1 al 8:



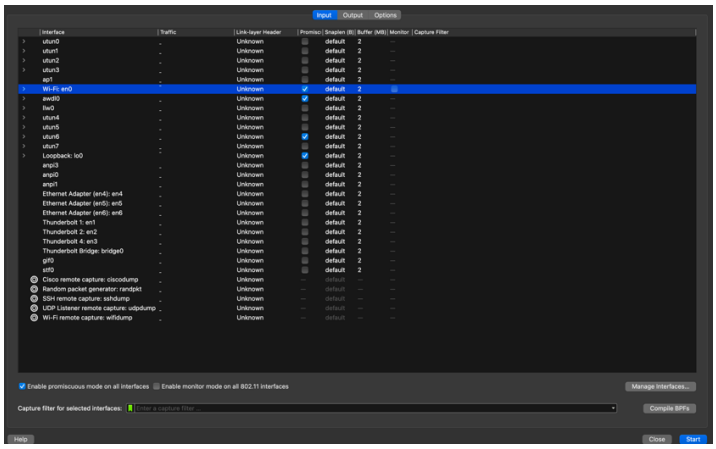
9. Aplique una regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia. (View -> coloring rules -> +)



10. Cree un botón que aplique un filtro para paquetes TCP con la bandera SYN igual a 1. (esquina superior derecha -> +)



11. Oculte las interfaces virtuales (en caso aplique: capture -> options)

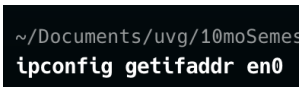


Se debe realizar tomas de pantalla que muestren el entorno final personalizado, el nombre del perfil y el uso de las regla de color y botón del filtro, así como la lista simplificada de las interfaces
de captura.

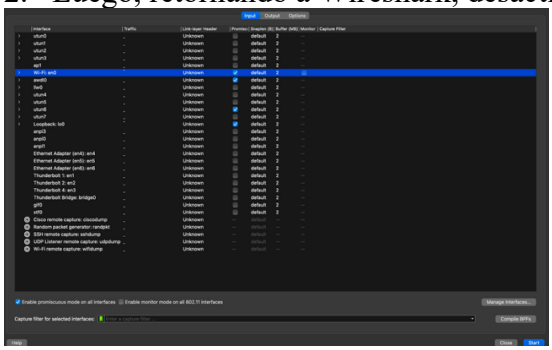
1.2 Configuración de la captura de paquetes

En la segunda parte, se realizará una captura de paquetes con un ring buffer.

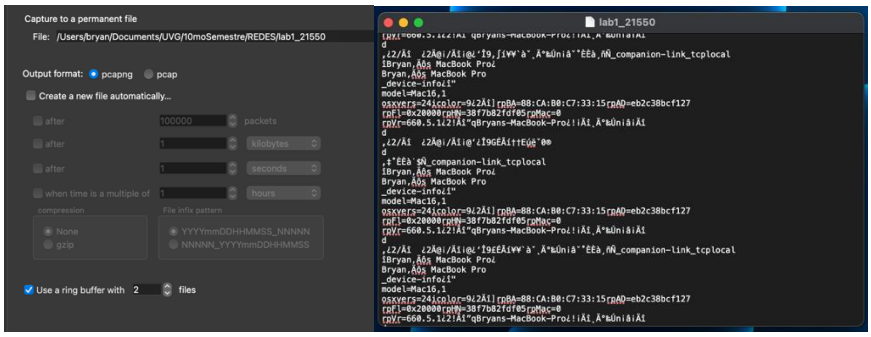
1. Abra una terminal y ejecute el comando ifconfig/ipconfig (dependiendo de su OS). Detalle y explique lo observado, investigue (i.e.: 'man ifconfig', documentación) de ser necesario.



2. Luego, retornando a Wireshark, desactive las interfaces virtuales o que no aplique.



3. Realice una captura de paquetes con la interfaz de Ethernet o WiFi con una configuración de ring buffer, con un tamaño de 5 MB por archivo y un número máximo de 10 archivos (puede hacerlo por medio de la interfaz de usuario o por medio de comandos) Genere tráfico para que los archivos se creen. Defina el nombre de los archivos de la siguiente forma: lab1_carnet.pgcap (options -> capture -> output)



Se debe realizar tomas de pantalla de la configuración o comandos para la creación del ring buffer, así como los archivos generados.

1.3 Anàlisis de paquetes

En la tercera parte se analizará el protocolo HTTP. Debe realizar tomas de pantalla que validen sus respuestas.

Abra su navegador, inicie una captura de paquetes en Wireshark (sin filtro) en la

1. interfaz y acceda a la siguiente direccion: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
2. Detenga la captura de paquetes (si desea realizar una nueva captura de la página deberá borrar el caché de su navegador, de lo contrario no se realizará la captura del protocol HTTP).

10.100.1.60	128.119.245.12	HTTP	533 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
128.119.245.12	10.100.1.60	HTTP	438 HTTP/1.1 200 OK (text/html)
10.100.1.60	128.119.245.12	HTTP	479 GET /favicon.ico HTTP/1.1
128.119.245.12	10.100.1.60	HTTP	484 HTTP/1.1 404 Not Found (text/html)

   NOTA: me pase a windows ya que en mac no me salia nunca el http solo me salia SSDP
3. 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,es-ES;q=0.8,en;q=0.7,en-GB;q=0.6,en-US;q=0.5
   d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?
   e. 533 bytes
   f. 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.
      Para diagnosticar problemas de rendimiento yo creo que seria bueno ver primero el router/switch principal de la red para ver el tráfico general o ver los puntos de acceso cercano al servidor para analizar la carga que tiene el servidor

      Y si es conveninente instalar wireshark en el servidor para poder ver el registro de request hechos en el servidor y como responden

Comentarios:

Durante el laboratorio presente algunas dificultades al capturar tráfico HTTP en macOS debido a las limitaciones de la interfaz WiFi. Esto se resolvió cambiando a un entorno Windows, donde fue posible observar correctamente los paquetes HTTP. Además, el uso de curl ayudó a generar

tráfico HTTP visible en Wireshark. Estas herramientas complementarias facilitaron el análisis preciso del protocolo.

Conclusiones:
La experiencia con Wireshark permitió comprender la importancia de elegir correctamente la interfaz de red, aplicar filtros adecuados, y personalizar el entorno para facilitar el análisis. El uso de ring buffer demostró ser útil para capturas prolongadas o con mucho tráfico. También se evidenció cómo los navegadores modernos pueden redirigir automáticamente a HTTPS, lo cual afecta la visibilidad de protocolos como HTTP en una red. El análisis detallado de cabeceras HTTP refuerza conceptos esenciales de comunicación cliente-servidor.

Referencias Utilizadas:

- Wireshark Foundation. (s. f.). Wireshark documentation. Recuperado de https://www.wireshark.org/docs/

- El protocolo Simple Service Discovery Protocol
  Revista Transformación Digital. (18 de noviembre de 2021). El protocolo Simple Service Discovery Protocol. Recuperado de https://www.revistatransformaciondigital.com/2021/11/18/el-protocolo-simple-service-discovery-protocol/