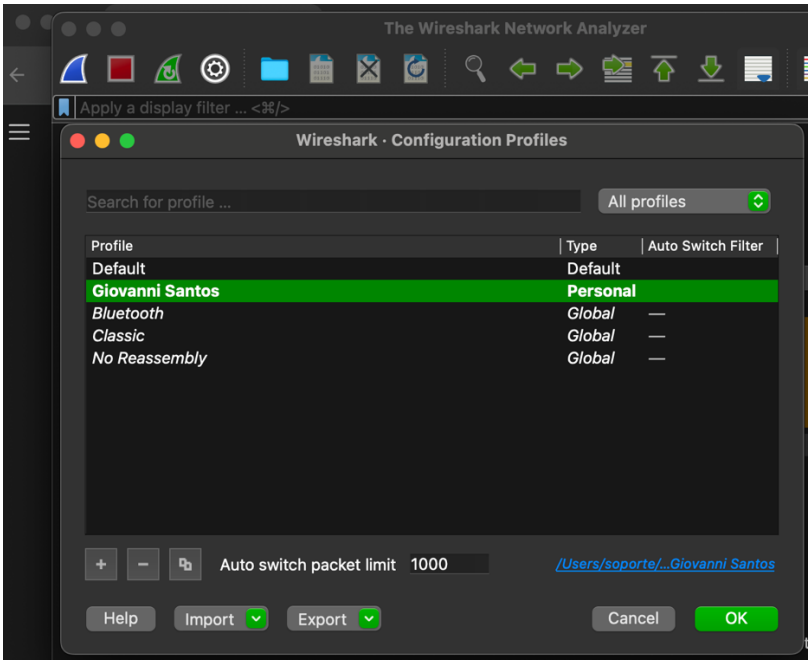
Laboratorio No. 1 – Esquemas de comunicación e Introducción a Wireshark

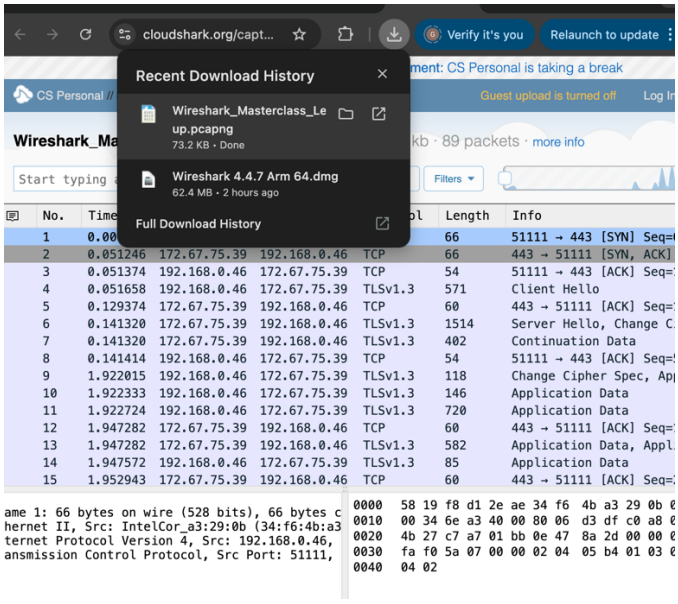
Giovanni Santos – 22523

Segunda parte: Introducción a Wireshark

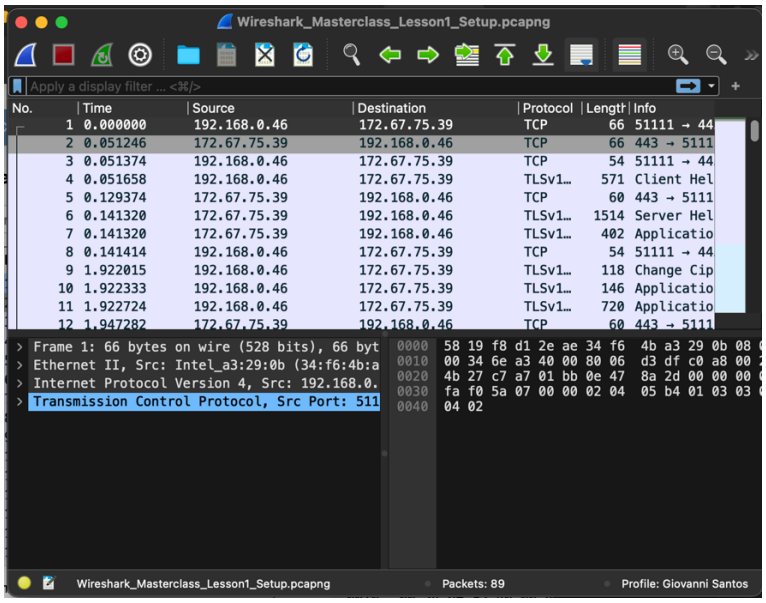
1. Personalización del entorno
    1. Inicie Wireshark
    2. Cree un perfil con su primer nombre y primer apellido (edit -> configuration profile)



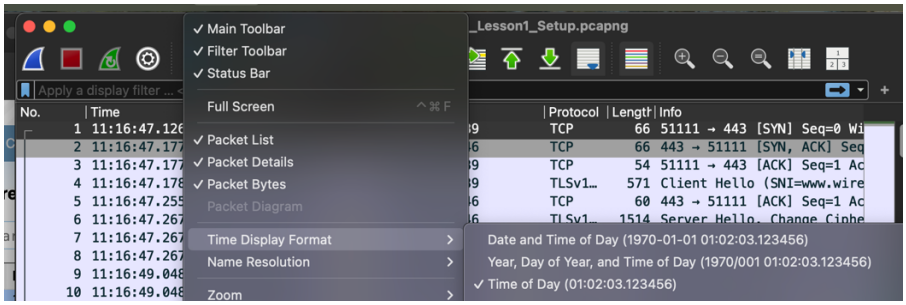
    3. Descargue el archivo https://www.cloudshark.org/captures/e6fb36096dbb (Export -> Download)



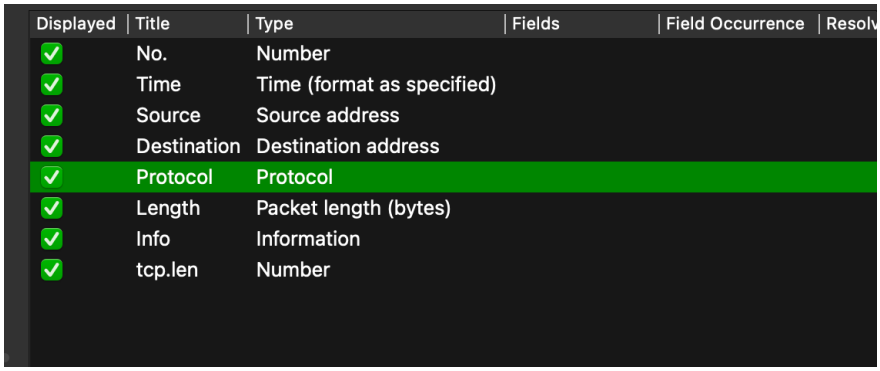
    4. Abra el archivo descargado, el archivo contiene transmisiones capturadas, y existen diversas columnas que representan la data.



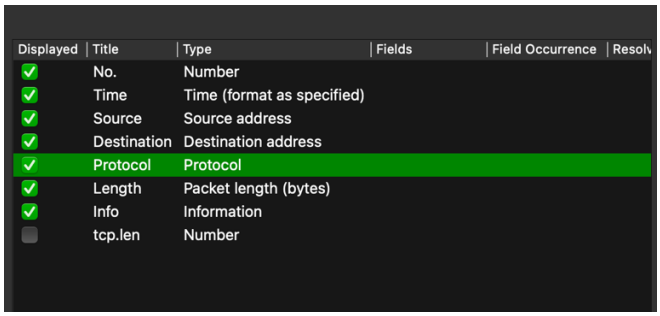
5. Aplique el formato de tiempo Time of Day (view -> Time Display Format)



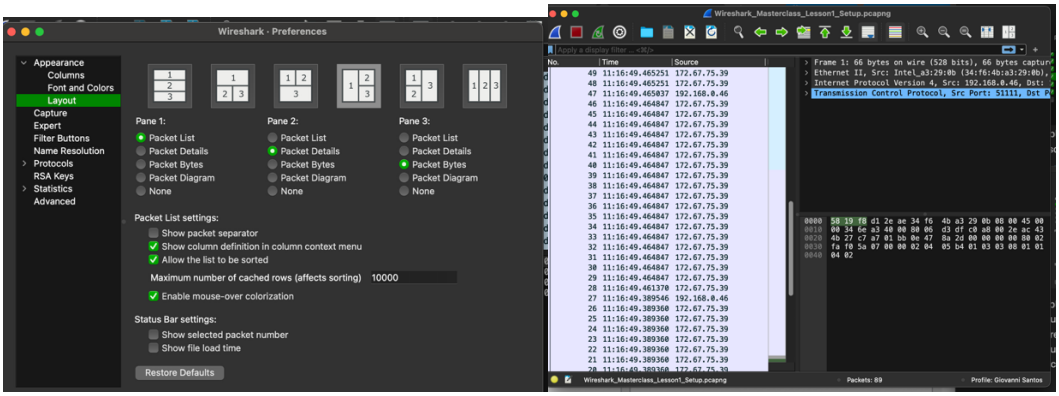
6. Agregue una columna con la longitud del protocolo (preferences -> column -> +)



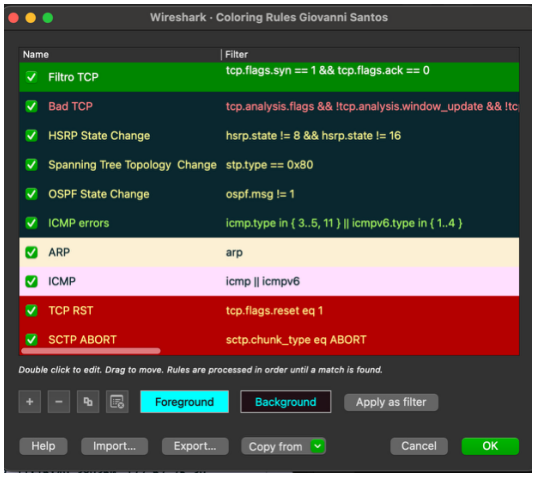
7. Elimine u oculte la columna Longitud (click derecho -> desmarcar columna)



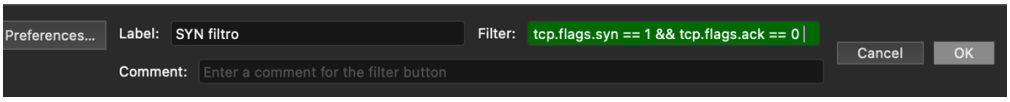
8. Aplique un esquema de paneles que sea de su preferencia (que no sea el esquema por defecto) (preferences -> Layout)



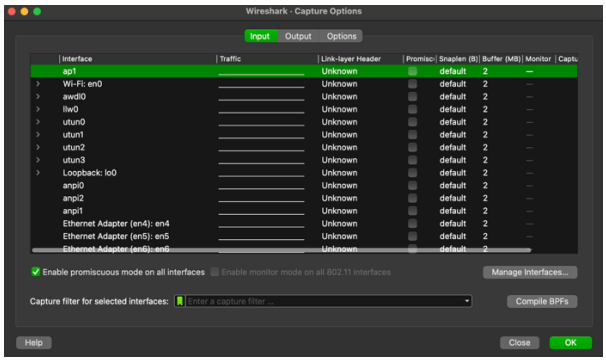
9. Aplique una regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia. (View -> coloring rules -> +)



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)

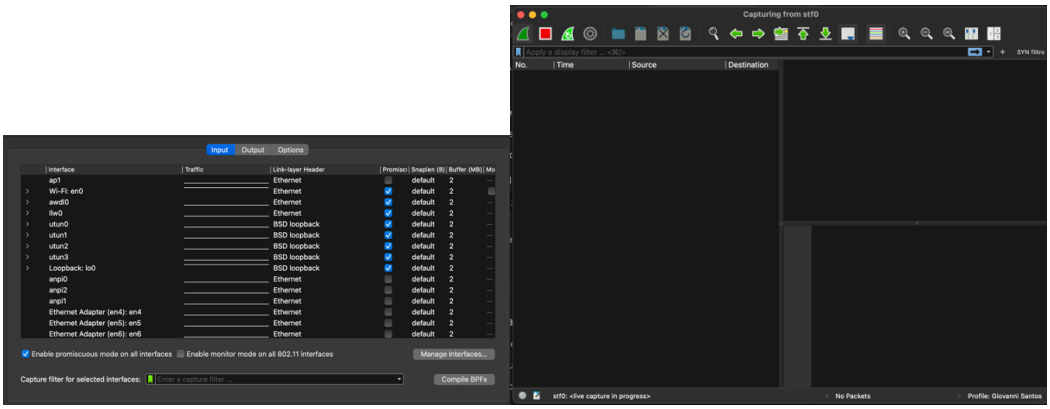


2. Configuración de la captura de paquetes
    1. Abra una terminal y ejecute el comando ifconfig/ipconfig (dependiendo de su OS). Detalle y explique lo observado, investigue (i.e.: 'man ifconfig', documentación) de ser necesario.
        i. Se puede observar las interfaces de red disponibles como lo que son lo0, en0, y en1. Además, se tienen distintos campos como inet que indica la dirección IPv4 asignada, el estatus o el ether que indica la dirección MAC.

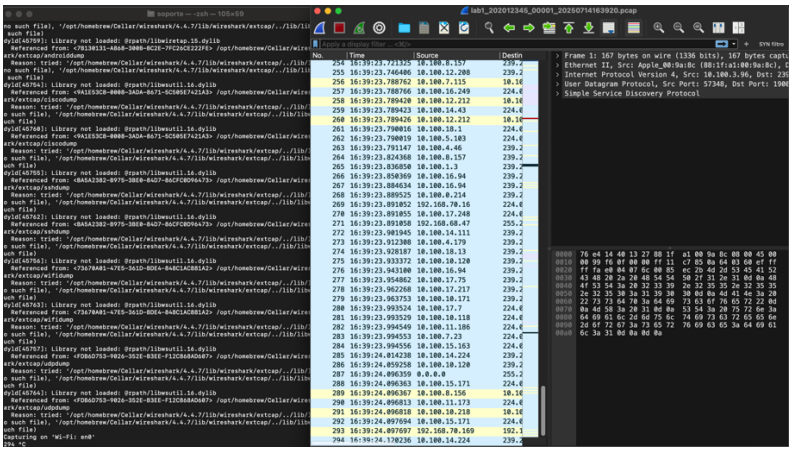
```
(base) soporte@Gios-MacBook-Pro ~ % ifconfig

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 86:45:99:46:1e:fc
        media: none
        status: inactive
anpi2: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 86:45:99:46:1e:fe
        media: none
        status: inactive
anpi1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 86:45:99:46:1e:fd
        media: none
        status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 86:45:99:46:1e:dc
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 86:45:99:46:1e:dd
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en6: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 86:45:99:46:1e:de
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:cb:e4:1e:13:80
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:cb:e4:1e:13:84
        media: autoselect <full-duplex>
        status: inactive
en3: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:cb:e4:1e:13:88
        media: autoselect <full-duplex>
        status: inactive
ap1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether d2:b7:e1:77:80:b3
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (none)
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 76:e4:14:40:13:27
```

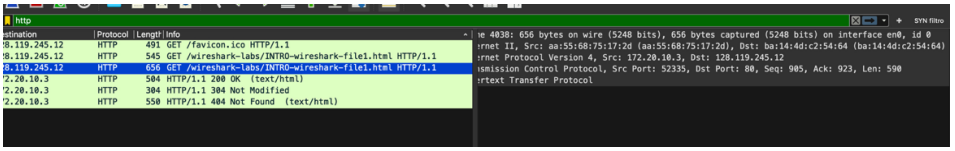
2. Luego, retornando a Wireshark, desactive las interfaces virtuales o que no aplique.



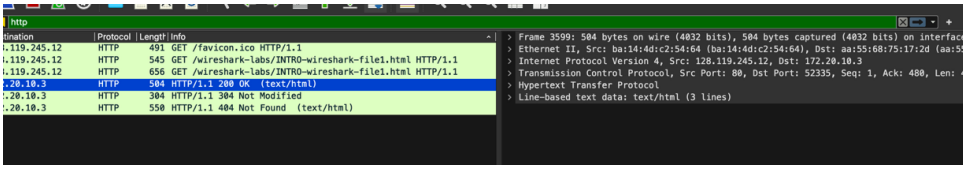
3. Realice una captura de paquetes con la interfaz de Ethernet o WiFi con una configuración de ring buffer, con un tamaño de 5 MB por archivo y un número máximo de 10 archivos. Genere tráfico para que los archivos se creen. Defina el nombre de los archivos de la siguiente forma: lab1_carnet.pgcap (options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



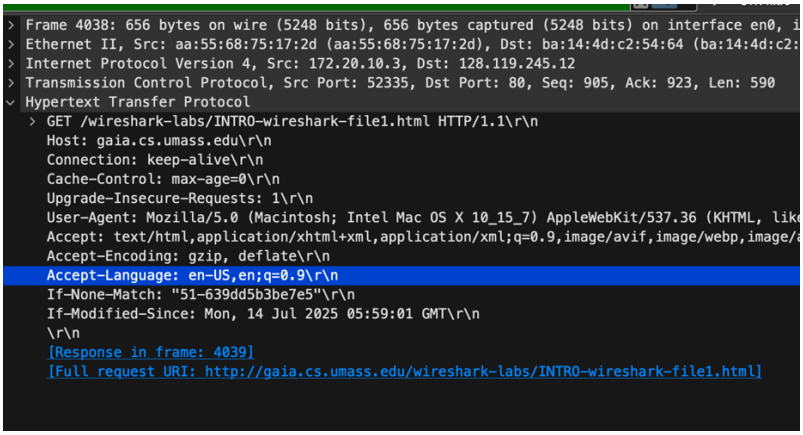
3. Análisis de paquetes
    1. Responda las siguientes preguntas:
        a. ¿Qué versión de HTTP está ejecutando su navegador?
            a. Se está ejecutando la versión 1.1



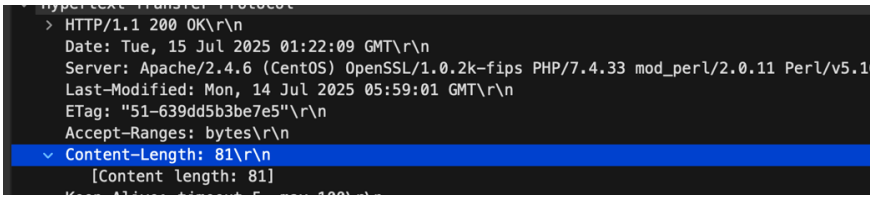
        b. ¿Qué versión de HTTP está ejecutando el servidor?
            a. Se ejecuta la versión 1.1.



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



d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?
    a. 81 bytes de contenido



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.
    a. En el caso de problemas de rendimiento, conviene escuchar al punto de red de cliente, router y servidor. No es conveniente instalarlo directamente en el servidor ya que consume recursos que afectan el rendimiento.

Discusión:

Una forma de observar el funcionamiento del protocolo HTTP a nivel de red es mediante Wireshark. En este laboratorio, pude capturar solicitudes y respuestas generadas después de acceder a una página web en la que pude observar elementos como la versión del protocolo y los datos intercambiados. Adicionalmente, pude observar las versiones del navegador y del servidor y pude entender que están bajo la misma versión debido a la compatibilidad o configuración de los servicios. Por otro

lado, aprendí a utilizar Wireshark y a tener un entendimiento práctico sobre cómo funciona esta herramienta.

Comentarios

- Después de utilizar Wireshark, tengo un mejor entendimiento sobre la comunicación de dispositivos y los detalles técnicos de su funcionamiento.
- Fue interesante ver el diagnostico de red y me interesa seguir aprendiendo sobre temas como el tráfico.