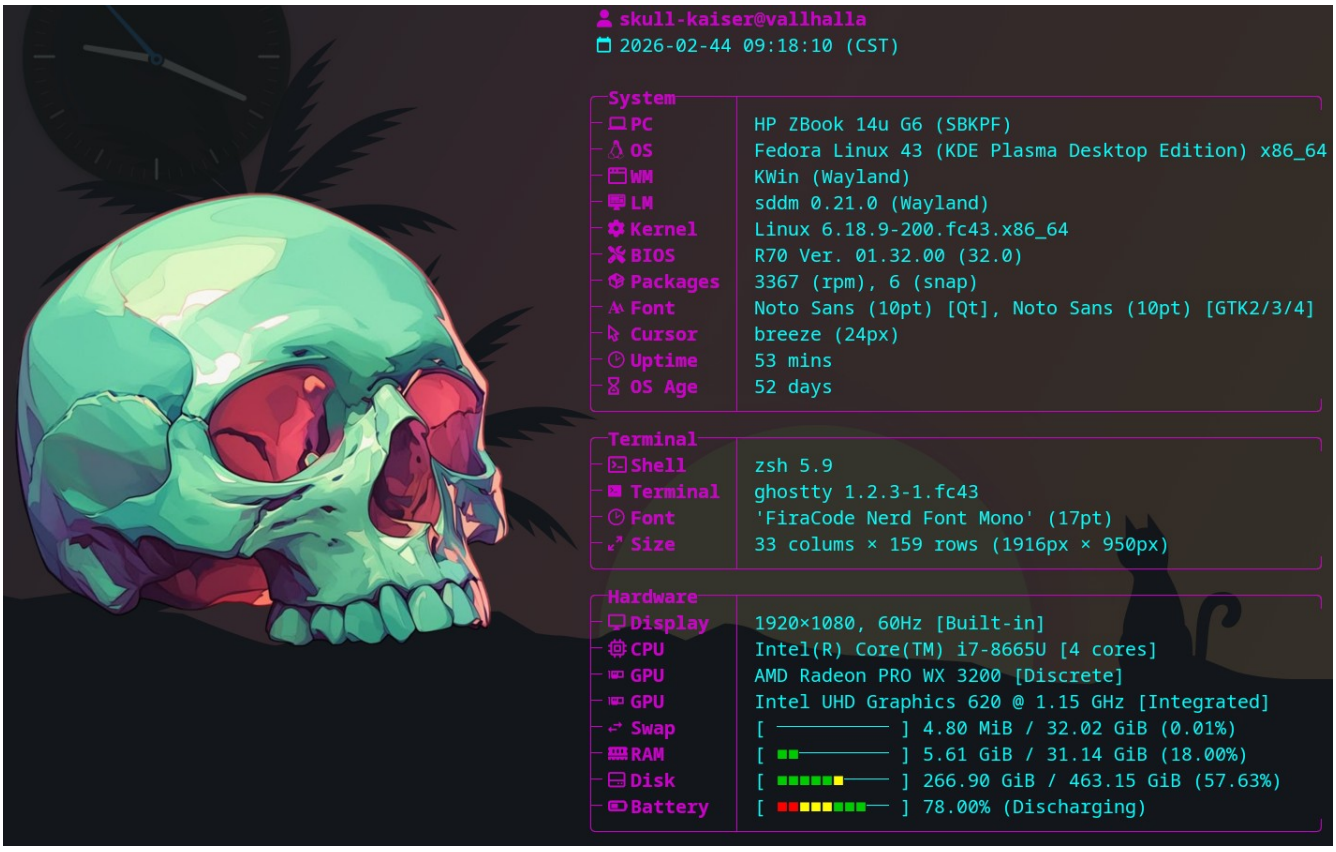
Analisis de encapsulamiento en la arquitectura TPC-IP mediante Wireshark

1. Entorno de trabajo e instalación de Wireshark

Para la actividad, se empleo un entorno de trabajo usando GNU/Linux, mas especificamente la distribución “Fedora 43”. Las especificaciones del equipo son las siguientes:



Ya se tenia la herramienta de Wireshark previamente instalada.

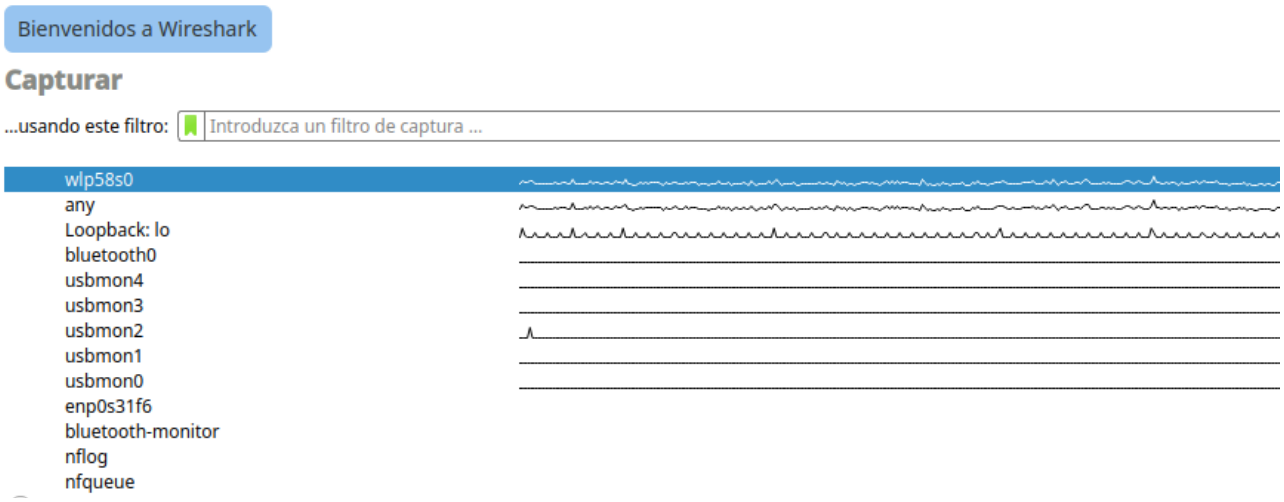
```
❱ sudo dnf install wireshark
[sudo] contraseña para skull-kaiser:
Actualizando y cargando repositorios:
Repositorios cargados.
El paquete "wireshark-1:4.6.3-1.fc43.x86_64" ya está instalado.

Nada que hacer.
```

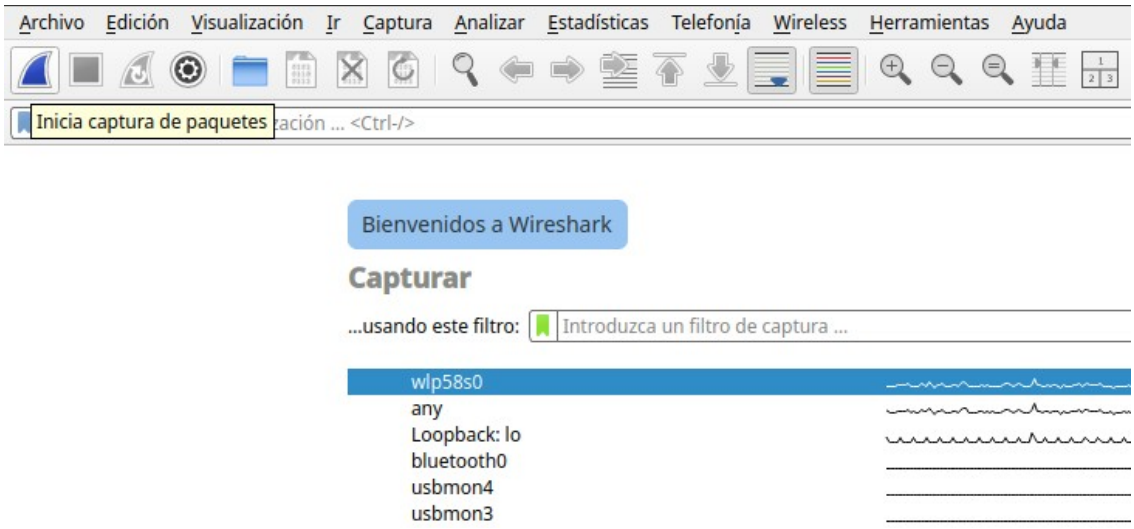
2. Inicio de la practica

2.1. Capas en un paquete HTTP

En este caso, no aparece como tal una opción llamada “Wifi” sino que aparece la opción del adaptador de red, en este caso, el adaptor wifi es “wlp58s0”.



Despues de escoger la opción del adaptador de red, se inicia la captura de paquetes.



AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

PERSONAL

Online Banking Login

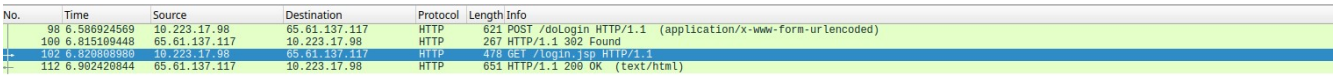
Username: abraham

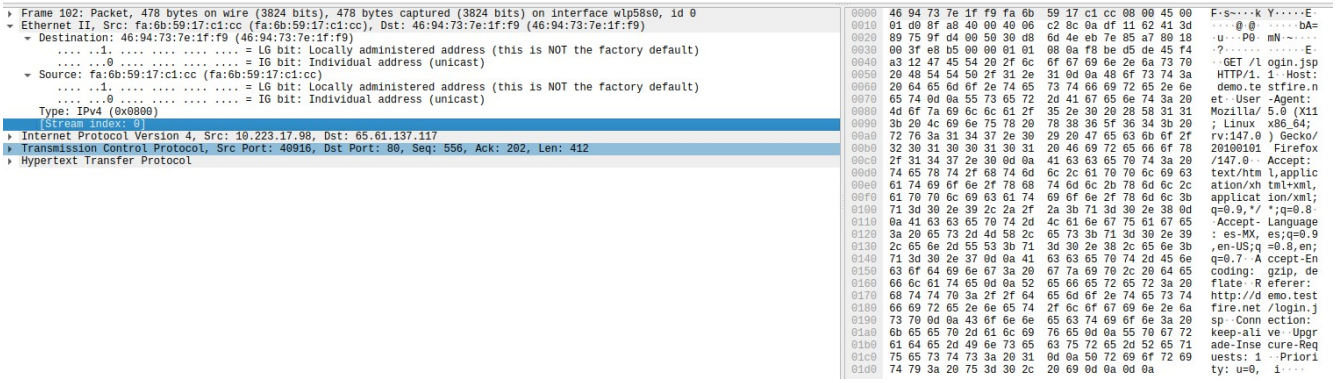
Password: •••••••

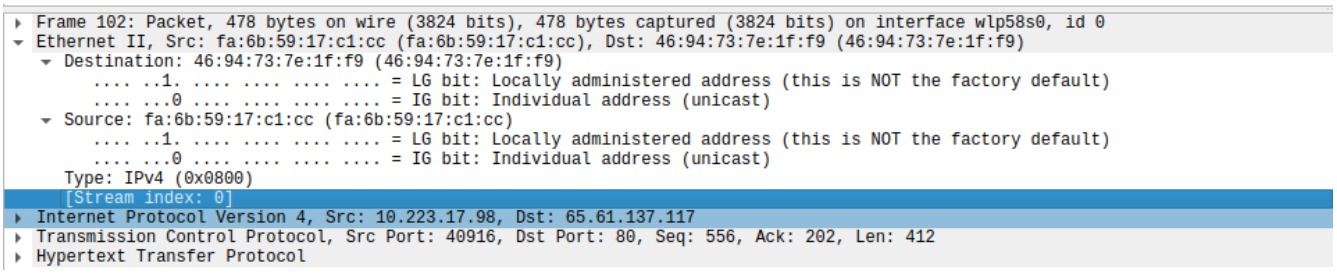
Login

http

No.	Time	Source	Destination	Protocol	Length	Info
98	6.586924569	10.223.17.98	65.61.137.117	HTTP	621	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
100	6.815109448	65.61.137.117	10.223.17.98	HTTP	267	HTTP/1.1 302 Found
102	6.820808980	10.223.17.98	65.61.137.117	HTTP	478	GET /login.jsp HTTP/1.1
112	6.902420844	65.61.137.117	10.223.17.98	HTTP	651	HTTP/1.1 200 OK (text/html)

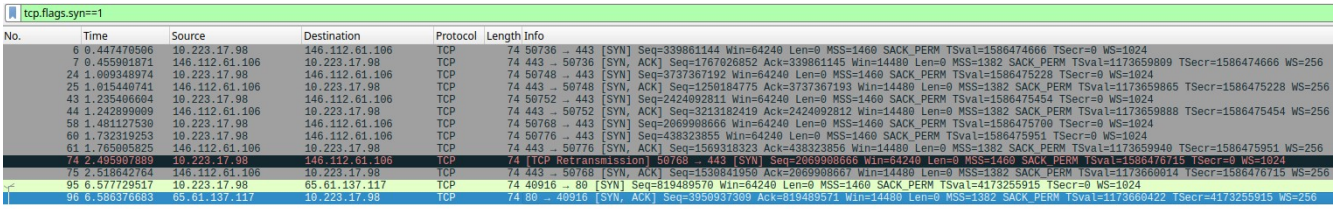


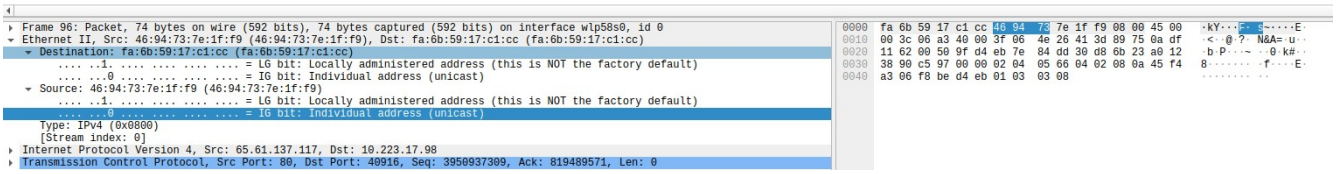


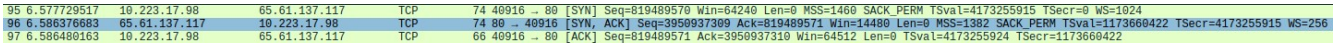


Capa	Campo observado	Valor
Ethernet	MAC Origen	Fa:6b:59:17:c1:cc
Ethernet	MAC Destino	46:94:73:7e:1f:f9
IP	IP Origen	10.223.17.98
IP	IP Destino	65.61.137.117
TPC	Puerto origen	40916
TCP	Puerto destino	80
HTTP	Metodo	GET

2.2. Análisis del Three-Way Handshake

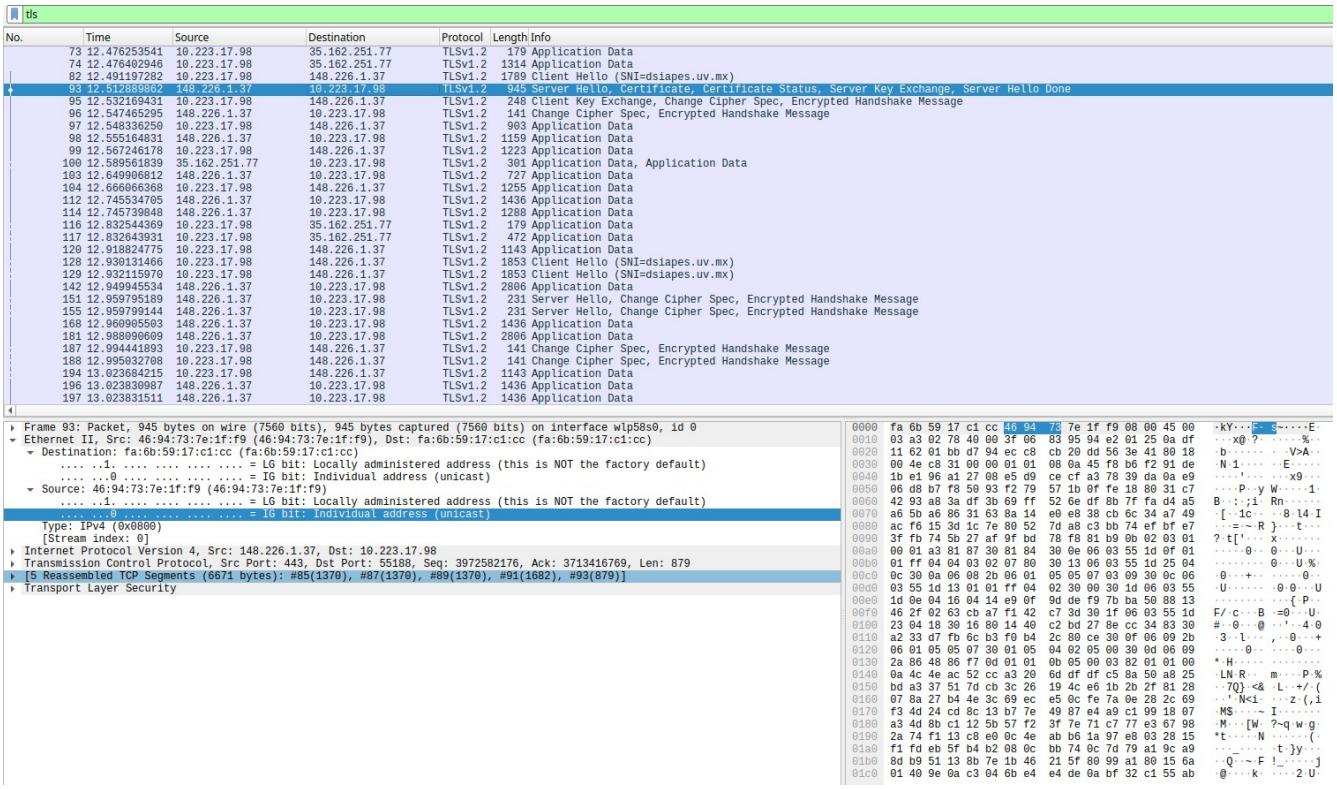




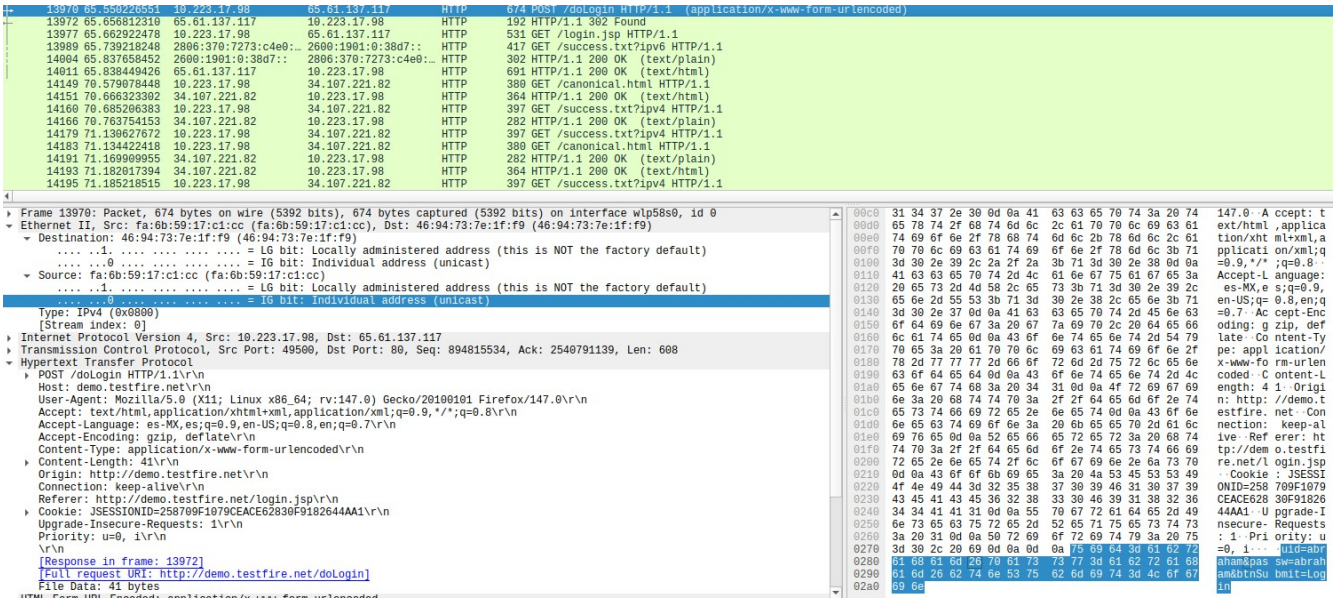


- ¿Qué puerto utiliza el servidor? Puerto 80
- ¿Por qué TCP necesita este proceso? Para verificar que exista un servidor destino.
- ¿Cuáles son los valores de SYN, SYN-ACK y ACK?
  - SYN: 819489570
  - ACK: 3950937309
  - SYN-ACK: Seq=3950937309 Ack=819489571

2.3. Comparacion HTTP vs HTTPS

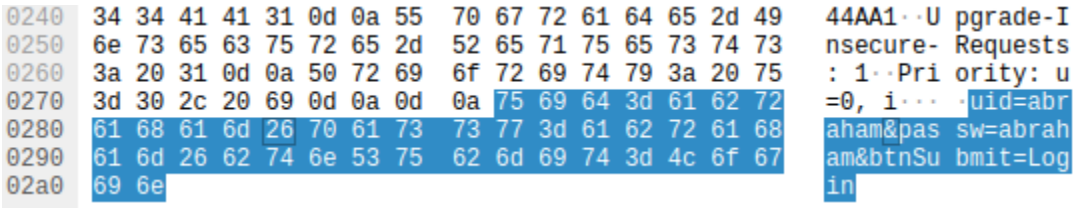


¿Puedes entender el contenido de los mensajes? No, estan cifrados.



¿Puedes entender los mensajes? Si

¿Puedes encontrar en texto plano el nombre de usuario y contraseña que ingresaste en la página http://demo.testfire.net/login.jsp? Si



¿Puedes identificar en texto plano la cookie con el número de sesión activa? Si

a) ¿En qué capa crees que ocurre el cifrado? En la capa de transporte.
b) ¿Qué protocolo protege la comunicación? HTTPS
c) ¿Qué información viaja sin cifrar en HTTP? El nombre de usuario y la contraseña para iniciar sesión
d) ¿Qué riesgos implica usar HTTP en redes públicas? Que un agente malicioso con conocimientos para capturar paquetes puede obtener información valiosa de diversos usuario