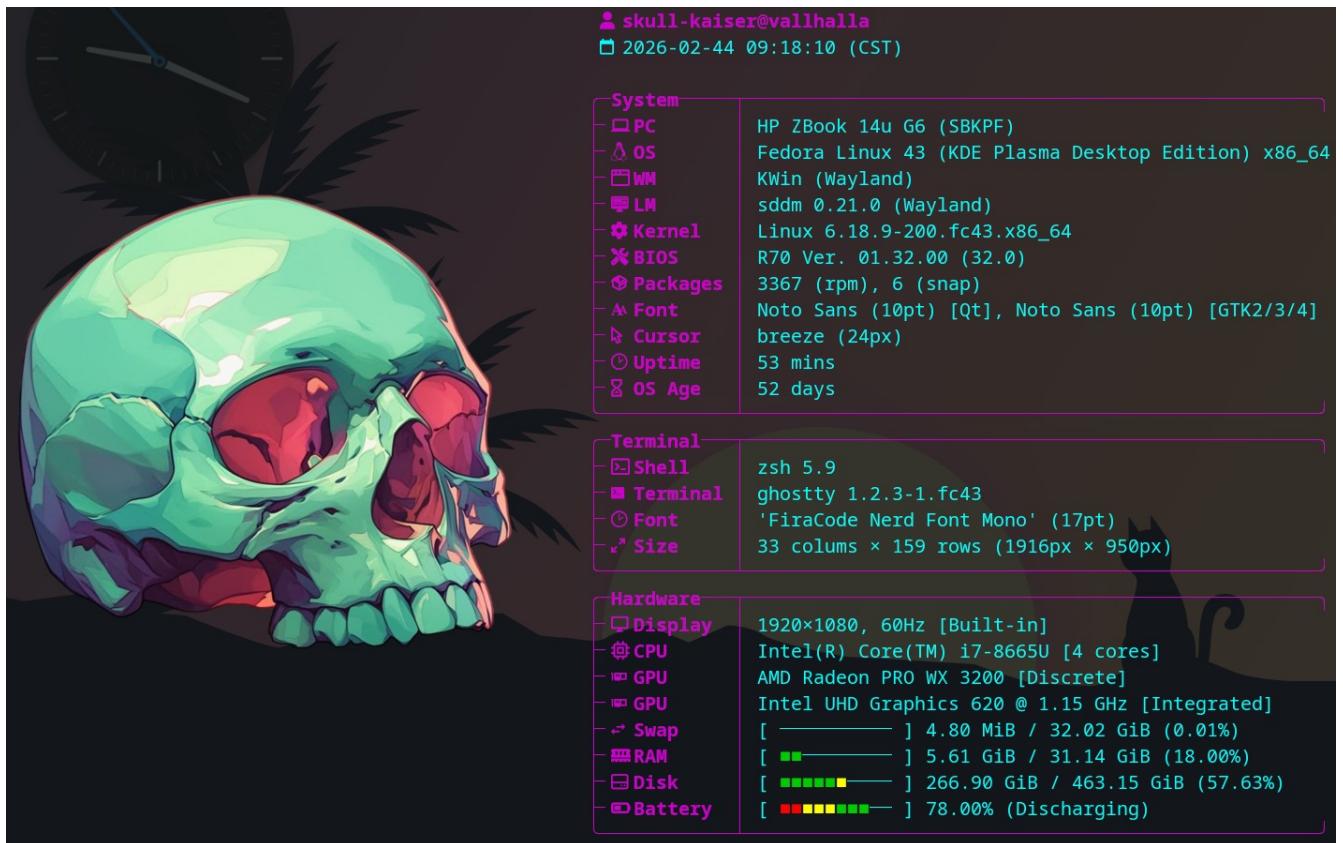


# Analisis de encapsulamiento en la arquitectura TPC-IP mediante Wireshark

## 1. Entorno de trabajo e instalación de Wireshark

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



Ya se tenia la herramienta de Wireshark previamente instalada.

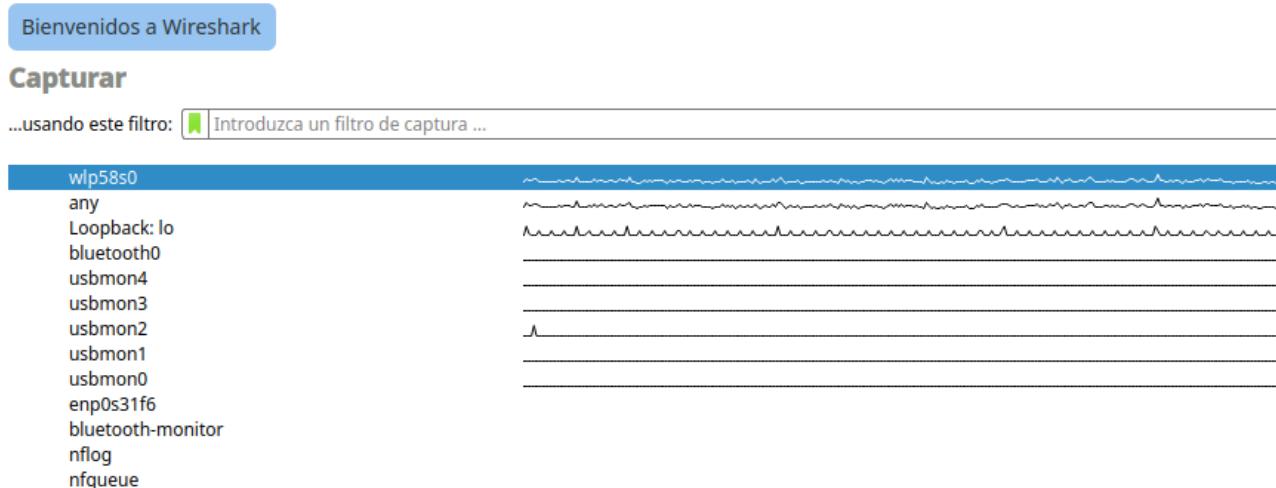
```
> sudo dnf install wireshark
[sudo] contraseña para skull-kaiser:
Actualizando y cargando repositorios:
Repositorios cargados.
El paquete "wireshark-1:4.6.3-1.fc43.x86_64" ya está instalado.

Nada que hacer.
```

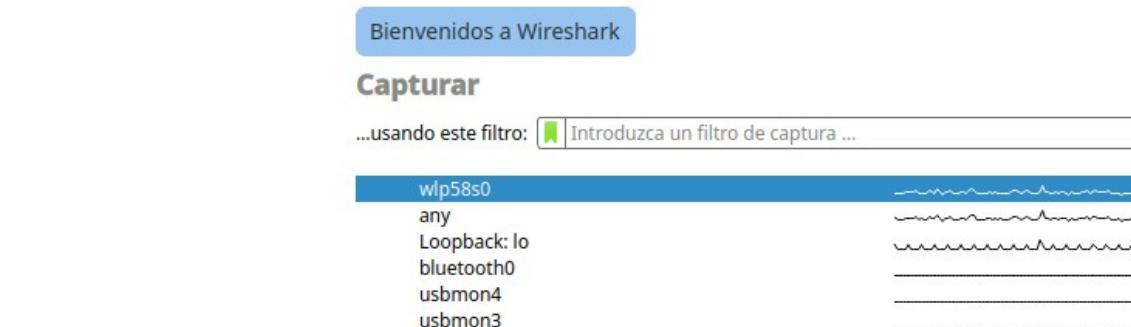
## 2. Inicio de la practica

### 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.





<a href="#"> ONLINE BANKING LOGIN</a>	PERSONAL
<p><u>PERSONAL</u></p> <ul style="list-style-type: none"><li>• <a href="#">Deposit Product</a></li><li>• <a href="#">Checking</a></li><li>• <a href="#">Loan Products</a></li><li>• <a href="#">Cards</a></li><li>• <a href="#">Investments &amp; Insurance</a></li><li>• <a href="#">Other Services</a></li></ul> <p><u>SMALL BUSINESS</u></p> <ul style="list-style-type: none"><li>• <a href="#">Deposit Products</a></li><li>• <a href="#">Lending Services</a></li><li>• <a href="#">Cards</a></li><li>• <a href="#">Insurance</a></li><li>• <a href="#">Retirement</a></li><li>• <a href="#">Other Services</a></li></ul> <p><u>INSIDE ALTORO MUTUAL</u></p> <ul style="list-style-type: none"><li>• <a href="#">About Us</a></li><li>• <a href="#">Contact Us</a></li><li>• <a href="#">Locations</a></li><li>• <a href="#">Investor Relations</a></li><li>• <a href="#">Press Room</a></li><li>• <a href="#">Careers</a></li><li>• <a href="#">Subscribe</a></li></ul>	<h2>Online Banking Login</h2> <p>Username: <input type="text" value="abraham"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>

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)						

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	6.820808888	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)

► Frame 102: Packet, 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface wlp5s0, id 0
► Ethernet II, Src: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc), Dst: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9)
Destination: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9)
.... .1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
.... .0. .... .... .... = IG bit: Individual address (unicast)
Source: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc)
.... .1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
.... .0. .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
► Internet Protocol Version 4, Src: 10.223.17.98, Dst: 65.61.137.117
► Transmission Control Protocol, Src Port: 40916, Dst Port: 80, Seq: 556, Ack: 202, Len: 412
► Hypertext Transfer Protocol
0000 46 94 73 7e 1f f9 fa 6b 59 17 c1 cc 00 00 45 00 F-s-...k Y-...E
0001 01 d0 8f 49 40 00 49 06 c2 8c 0a df 11 62 41 3d u- P0 mN ~
0002 89 75 97 d4 00 50 30 d8 6d 4e eb 7e 85 a7 80 18 ?-..... E
0003 00 3f e9 b5 00 00 01 01 08 0a 78 be d5 a4 f4 :GET /1/login.jsp
0004 a3 12 47 45 54 29 2f 6c 6f 67 69 6e 2e 6a 73 70 HTTP/1.1 Host:
0005 28 48 54 54 59 21 31 2e 31 0d 0a 48 6f 73 74 3a denote site.sirvape.h
0006 28 48 54 54 59 21 31 2e 31 0d 0a 48 6f 73 74 3a er User-Agent: Mozilla/5.0 (X11
0007 65 74 ad 0e 55 03 03 2d 6f 67 65 6e 74 2d 09 Mozilla/5.0 (X11
0008 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 29 28 58 31 31 ; Linux x86_64;
0009 3b 29 4c 69 6e 75 78 29 78 38 35 5f 36 34 3b 20 Gecko/ rv:147.0 ) Gecko/
000a 72 76 3a 31 34 37 2e 39 29 28 47 65 63 6b 6f 2f 20100101 Firefox/
000b 2f 31 34 37 2e 30 0d 0a 41 63 63 65 70 74 3a 20 /147.0 Accept:
000c 74 65 78 74 2f 68 74 6d 6c 2c 61 79 70 69 63 text/html,application/xhtml+xml
000d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 accept-language:en;q=0.9,
000e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 application/xml;q=0.9,
000f 71 3d 30 2e 39 2c 2a 2f 2b 71 3d 30 2e 39 0d q=0.9,*/*;q=0.8,
0110 0a 41 63 63 65 79 74 2d 4c 61 6e 67 75 61 67 65 Accept-Language: : es-MX, es;q=0.9
0111 2a 28 65 73 2d 44 58 2c 65 73 3b 71 3d 33 2e 39 ,en-US;q=0.8,en;q=0.7: Acept-En
0112 2c 65 6e 2d 55 53 3b 71 3d 30 2e 38 2c 65 6e 3b coding: gnutella-de
0113 71 3d 30 2e 37 0d 0a 41 63 63 65 79 74 2d 45 6e q=0.7 - Acept-En
0114 69 64 64 69 66 66 67 3a 29 67 7a 69 70 2c 29 64 65 accept-language:de;q=0.9,
0115 66 6c 64 64 66 66 67 3a 29 67 7a 69 70 2c 29 64 65 accept-language:es;q=0.9,
0116 68 74 74 70 3a 2f 2f 64 65 6d 6f 2e 74 65 73 74 http://elmo.test
0117 66 69 72 65 2e 66 65 74 2f 6c 6f 67 69 6e 2e 6a sp-Conn ection:keep-alive; Upgr ade-Inse cure-Req
0118 73 70 0d 0a 43 6f 6e 66 65 73 69 6f 6e 3a 20 uests: 1 - Priori ty: u=0, i...
0119 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72
0120 61 64 65 2d 49 66 73 65 65 75 72 65 2d 52 65 71
0121 75 65 73 74 73 3a 28 31 0d 0a 50 72 69 6f 72 69
0122 74 79 3a 20 75 3d 30 2c 20 69 6d 0a 0d 0a

► Frame 102: Packet, 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface wlp5s0, id 0
► Ethernet II, Src: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc), Dst: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9)
Destination: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9)
.... .1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
.... .0. .... .... .... = IG bit: Individual address (unicast)
Source: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc)
.... .1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
.... .0. .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
► Internet Protocol Version 4, Src: 10.223.17.98, Dst: 65.61.137.117
► Transmission Control Protocol, Src Port: 40916, Dst Port: 80, Seq: 556, Ack: 202, Len: 412
► Hypertext Transfer Protocol

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

tcp.flags.syn==1						
No.	Time	Source	Destination	Protocol	Length Info	
6	0.447470506	10.223.17.98	146.112.61.106	TCP	74 50736 - 443	[SYN] Seq=339861144 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1586474666 TSectr=0 WS=1024
7	0.455901874	146.112.61.106	10.223.17.98	TCP	74 443 - 50736	[SYN, ACK] Seq=1767026854 Win=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586474666 TSectr=0 WS=256
24	1.015187474	10.223.17.98	146.112.61.106	TCP	74 443 - 50748	[SYN, ACK] Seq=1770915450 Win=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586475228 TSectr=0 WS=256
28	1.015144074	146.112.61.106	10.223.17.98	TCP	74 443 - 50748	[SYN, ACK] Seq=1259184775 Ack=3737367193 Win=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586475228 TSectr=0 WS=256
43	1.235406604	10.223.17.98	146.112.61.106	TCP	74 50752 - 443	[SYN] Seq=2424092811 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1586475454 TSectr=0 WS=1024
44	1.242899004	146.112.61.106	10.223.17.98	TCP	74 443 - 50752	[SYN, ACK] Seq=3213182419 Ack=2424092812 Win=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586475454 WS=256
58	1.481127532	10.223.17.98	146.112.61.106	TCP	74 50768 - 443	[SYN] Seq=20699988666 Win=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586475704 TSectr=0 WS=1024
66	1.732319253	10.223.17.98	146.112.61.106	TCP	74 50776 - 443	[SYN, ACK] Seq=438323858 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1586475951 TSectr=0 WS=1024
61	1.765005825	146.112.61.106	10.223.17.98	TCP	74 443 - 50776	[SYN, ACK] Seq=1569318323 Ack=438323858 Win=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586475951 TSectr=0 WS=256
74	2.495907889	10.223.17.98	146.112.61.106	TCP	74 50768 - 443	[TCP Retransmission] Seq=20699988666 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1586476715 TSectr=0 WS=1024
75	2.513842769	146.112.61.106	10.223.17.98	TCP	74 443 - 50768	[SYN, ACK] Seq=1569318323 Ack=438323858 Win=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586476715 TSectr=0 WS=256
95	6.577729517	10.223.17.98	65.61.137.117	TCP	74 40916 - 80	[SYN] Seq=819489570 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1586489571 TSectr=0 WS=1024
96	6.586376803	65.61.137.117	10.223.17.98	TCP	74 40916 - 80	[SYN, ACK] Seq=3950937309 Ack=819489571 Win=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586489571 TSectr=0 WS=256

Frame 96: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp58s0, id 0	
Ethernet II, Src: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9), Dst: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc)	
Destination: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc)	
... .1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)	
... .0. .... .... .... = IG bit: Individual address (unicast)	
Source: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9)	
... .1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)	
... .0. .... .... .... = IG bit: Individual address (unicast)	
Type: IPv4 (0x0800)	
[Stream index: 0]	
Internet Protocol Version 4, Src: 65.61.137.117, Dst: 10.223.17.98	
Transmission Control Protocol, Src Port: 80, Dst Port: 40916, Seq: 3950937309, Ack: 819489571, Len: 0	

05 6.577729517 10.223.17.98	65.61.137.117	TCP	74 40916 - 80	[SYN] Seq=819489570 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=1586489571 TSectr=0 WS=1024
86 6.586376803 65.61.137.117	10.223.17.98	TCP	74 88 - #0916	[SYN, ACK] Seq=3950937309 Ack=819489571 Min=14480 Len=0 MSS=1460 SACK_PERM TStamp=1586489571 TSectr=0 WS=256
97 6.586486163 10.223.17.98	65.61.137.117	TCP	66 40916 - 80	[ACK] Seq=819489571 Ack=3950937310 Win=64512 Len=0 TStamp=1586489571 TSectr=0 WS=256

- ¿Qué puerto utiliza el servidor? Puerto 80
- ¿Por qué TCP necesita este proceso? Para verificar que existe 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

No.	Time	Source	Destination	Protocol	Length Info
73	12.476253541	16.223.17.98	35.162.251.77	TLSv1.2	179 Application Data
74	12.476429246	16.223.17.98	35.162.251.77	TLSv1.2	1314 Application Data
82	12.491197282	16.223.17.98	148.226.1.37	TLSv1.2	1789 Client Hello (SNI=dsiapes.uv.mx)
93	12.50312789862	16.223.17.98	10.223.17.98	TLSv1.2	246 Server Hello Certificate, Certificate Status, Server Key Exchange, Server Hello Done
94	12.50312789862	16.223.17.98	148.226.1.37	TLSv1.2	248 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
96	12.547465295	148.226.1.37	10.223.17.98	TLSv1.2	141 Change Cipher Spec, Encrypted Handshake Message
97	12.548336259	16.223.17.98	148.226.1.37	TLSv1.2	983 Application Data
98	12.555164931	148.226.1.37	10.223.17.98	TLSv1.2	1159 Application Data
99	12.567246178	16.223.17.98	148.226.1.37	TLSv1.2	1223 Application Data
100	12.589581839	35.162.251.77	10.223.17.98	TLSv1.2	301 Application Data, Application Data
102	12.649966812	148.226.1.37	10.223.17.98	TLSv1.2	727 Application Data
104	12.6689636368	16.223.17.98	148.226.1.37	TLSv1.2	1255 Application Data
111	12.685352552	148.226.1.37	10.223.17.98	TLSv1.2	1403 Application Data
114	12.745739948	148.226.1.37	10.223.17.98	TLSv1.2	2088 Application Data
116	12.823544269	10.223.17.98	35.162.251.77	TLSv1.2	179 Application Data
117	12.832643931	16.223.17.98	35.162.251.77	TLSv1.2	472 Application Data
129	12.918824775	10.223.17.98	148.226.1.37	TLSv1.2	1143 Application Data
128	12.939131466	16.223.17.98	148.226.1.37	TLSv1.2	1853 Client Hello (SNI=dsiapes.uv.mx)
129	12.932115970	10.223.17.98	148.226.1.37	TLSv1.2	1853 Client Hello (SNI=dsiapes.uv.mx)
142	12.950745534	148.226.1.37	10.223.17.98	TLSv1.2	2866 Application Data
151	12.959735521	148.226.1.37	10.223.17.98	TLSv1.2	248 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
155	12.959739144	148.226.1.37	10.223.17.98	TLSv1.2	131 Server Hello, Change Cipher Spec, Encrypted Handshake Message
168	12.960905582	148.226.1.37	10.223.17.98	TLSv1.2	1436 Application Data
181	12.980896699	148.226.1.37	10.223.17.98	TLSv1.2	2806 Application Data
187	12.994418193	10.223.17.98	148.226.1.37	TLSv1.2	141 Change Cipher Spec, Encrypted Handshake Message
188	12.995032708	10.223.17.98	148.226.1.37	TLSv1.2	141 Change Cipher Spec, Encrypted Handshake Message
194	13.023684215	10.223.17.98	148.226.1.37	TLSv1.2	1143 Application Data
196	13.023830987	148.226.1.37	10.223.17.98	TLSv1.2	1436 Application Data
197	13.023831511	148.226.1.37	10.223.17.98	TLSv1.2	1436 Application Data

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

+ 13970 65.550265551 10.223.17.98 65.61.137.117 HTTP 674 POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)	+ 6060 fa 6b 59 17 c1 cc 46 9d 61 76 1f f9 98 86 45 66 -key...- : - - -E
-+ 13972 65.656812318 65.61.137.117 10.223.17.98 65.61.137.117 HTTP 531 GET /login.jsp HTTP/1.1	+ 6061 ff 6b 59 17 c1 cc 46 9d 61 76 1f f9 98 86 45 66 -xg?...- : - - -E
-+ 13989 65.739218248 2806:370:7273:c4e0... 2600:1901:0:38d7:: HTTP 417 GET /success.txt?ipv6 HTTP/1.1	+ 6062 11 62 01 bb d7 94 ec c8 cb 20 dd 56 3e 41 80 18 b... : - - -V-A-
-+ 14004 65.8370449426 55.137.117.117 10.223.17.98 65.61.137.117 HTTP 304 HTTP/1.1 200 OK (text/plain)	+ 6063 04 4e 31 99 00 01 09 0a 45 f8 b6 f2 91 -N- : - - -E
-+ 14149 18.579078448 10.223.17.98 34.197.221.82 HTTP 380 GET /canonical.html HTTP/1.1	+ 6064 1b e1 96 a1 27 08 e5 d9 ce ct a3 78 39 da 0a e9 -... : - - -x- .
-+ 14251 70.668323302 34.197.221.82 10.223.17.98 HTTP 364 HTTP/1.1 200 OK (text/html)	+ 6065 06 db 87 f8 50 93 f2 79 57 1b 0f fe 18 80 31 c7 -B... : - - -Rn - - -
-+ 14166 70.673574513 34.197.221.82 10.223.17.98 HTTP 397 GET /success.txt?ipv4 HTTP/1.1	+ 6066 42 93 a3 3a df 39 69 ff 52 6e df 8b 7f fa d4 a5 B... : - - -Rn - - -
-+ 14179 71.138627672 10.223.17.98 34.197.221.82 HTTP 397 GET /success.txt?ipv4 HTTP/1.1	+ 6067 a5 6b a6 36 31 63 8a 14 e9 e8 38 cb 6c 34 77 49 -[ -1c - - -8 14 I
-+ 14183 71.134422418 10.223.17.98 34.197.221.82 HTTP 380 GET /canonical.html HTTP/1.1	+ 6068 3f fb 1d 0f fe 0f 78 3d 20 80 0d 0e 09 29 -? t[" - - -X - - -
-+ 14191 71.169969955 34.197.221.82 10.223.17.98 HTTP 282 HTTP/1.1 200 OK (text/plain)	+ 6069 09 a3 31 87 09 81 04 06 09 55 1d 0f 01 - - -0 - - -U - - -
-+ 14193 71.182017394 34.197.221.82 10.223.17.98 HTTP 364 HTTP/1.1 200 OK (text/html)	+ 6070 01 ff 04 04 03 02 07 89 39 13 06 03 55 1d 25 04 - - -0 - - -U - - -
-+ 14195 71.185218515 10.223.17.98 34.197.221.82 HTTP 397 GET /success.txt?ipv4 HTTP/1.1	+ 6071 0c 39 04 06 08 2b 06 01 05 05 07 03 09 03 09 06 - - -0 + - - -0 - - -
+ Frame 13970: Packet, 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits) on interface wlp5s0, id 0	+ 6072 03 55 13 10 01 01 ff 04 02 30 09 30 14 06 03 55 U - - -0 0 - - -U
-+ Ethernet II, Src: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9), Dst: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc)	+ 6073 01 0d 0e 14 04 14 e9 07 9d fe t9 7b ba 50 88 13 C... : - - -P - - -
-+ Destination: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc)	+ 6074 46 2f 02 63 cb 01 2f 74 3d 39 1f 00 03 55 10 F/... : - - -P - - -
-+ ... .1. .... .0. .... . = L6 bit: Locally administered address (this is NOT the factory default)	+ 6075 23 04 12 39 16 89 14 46 cb bd 27 8e cc 34 83 30 # - - -0 - - -4 0
-+ Source: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9)	+ 6076 a2 33 d7 6c b6 05 04 2c 08 03 90 00 09 29 3 - - -1 , - - -0 +
-+ ... .1. .... .0. .... . = L6 bit: Locally administered address (this is NOT the factory default)	+ 6077 02 03 05 06 07 08 09 01 05 06 07 00 00 00 0d 0f 01 - - -0 - - -0 - - -
-+ Type: IPv4 (0x0800)	+ 6078 2a 86 48 77 0d 01 01 0b 05 09 03 82 01 01 09 -H - - -
-+ [Mac Address] (0x0806)	+ 6079 04 4c 46 ac 52 cc a3 20 6d df cf c5 8a 59 a8 25 LN R - m - - P %
-+ Internet Protocol Version 4, Src: 148.226.1.37, Dst: 10.223.17.98	+ 6080 bd a3 37 51 7d 0c 3c 26 19 4c 6e 1b 2b 2f 81 28 -7Q) <& L - +/ (
-+ Transmission Control Protocol, Src Port: 443, Dst Port: 55188, Seq: 3972582176, Ack: 3713416769, Len: 879	+ 6081 07 8a 27 04 3c 69 ec e5 0c fe 7a 0e 28 2c 69 -N< - - z (, i
-+ [5 Reassembled TCP Segments (6671 bytes): #85(1370), #87(1370), #89(1370), #91(1682), #93(870)]	+ 6082 f3 4d 24 cd 8c 13 7d 7e 49 87 e4 a9 c1 99 18 07 MS - I - - -
-+ Transport Layer Security	+ 6083 a3 4d 8a c1 12 5a 57 f2 3f 7e 71 c7 77 e3 67 98 M - [W - ? w g -

¿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

0240	34 34 41 41 31 0d 0a 55	70 67 72 61 64 65 2d 49	44AA1..U pgrade-I
0250	6e 73 65 63 75 72 65 2d	52 65 71 75 65 73 74 73	nsecure- Requests
0260	3a 20 31 0d 0a 50 72 69	6f 72 69 74 79 3a 20 75	: 1..Pri ority: u
0270	3d 30 2c 20 69 0d 0a 0d	0a 75 69 64 3d 61 62 72	=0, i.... uid=abr
0280	61 68 61 6d 26 70 61 73	73 77 3d 61 62 72 61 68	aham&pas sw=abrah
0290	61 6d 26 62 74 6e 53 75	62 6d 69 74 3d 4c 6f 67	am&btnSu bmit=Log
02a0	69 6e		in

¿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 usuarios