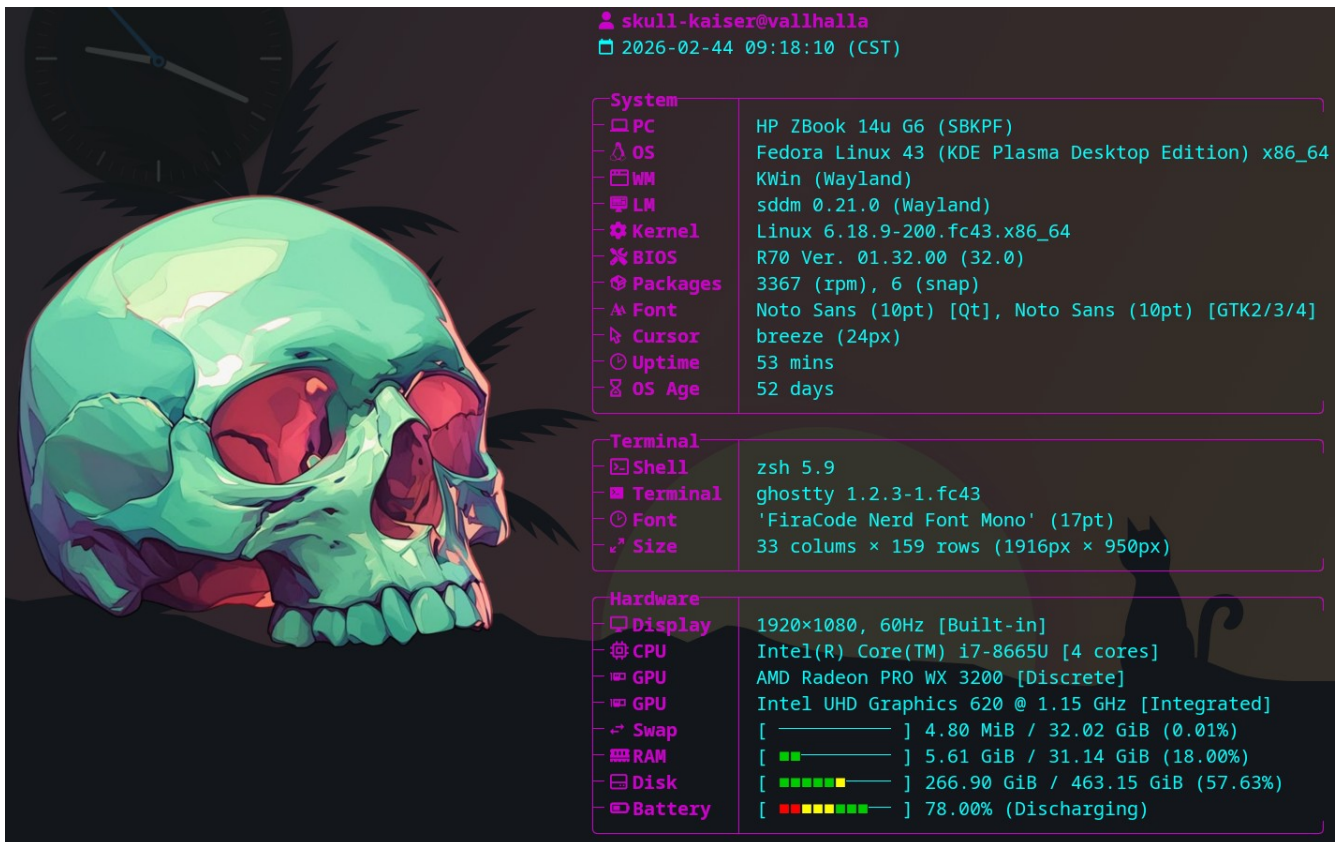


# Analisis de encapsulamiento en la arquitectura TPC-IP mediante Wireshark

## 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:



```
skull-kaiser@vallhalla
2026-02-44 09:18:10 (CST)

System
PC HP ZBook 14u G6 (SBKPF)
OS Fedora Linux 43 (KDE Plasma Desktop Edition) x86_64
WM KWin (Wayland)
LM sddm 0.21.0 (Wayland)
Kernel Linux 6.18.9-200.fc43.x86_64
BIOS R70 Ver. 01.32.00 (32.0)
Packages 3367 (rpm), 6 (snap)
Font Noto Sans (10pt) [Qt], Noto Sans (10pt) [GTK2/3/4]
Cursor breeze (24px)
Uptime 53 mins
OS Age 52 days

Terminal
Shell zsh 5.9
Terminal ghostty 1.2.3-1.fc43
Font 'FiraCode Nerd Font Mono' (17pt)
Size 33 colums × 159 rows (1916px × 950px)

Hardware
Display 1920×1080, 60Hz [Built-in]
CPU Intel(R) Core(TM) i7-8665U [4 cores]
GPU AMD Radeon PRO WX 3200 [Discrete]
GPU Intel UHD Graphics 620 @ 1.15 GHz [Integrated]
Swap [ ] 4.80 MiB / 32.02 GiB (0.01%)
RAM [ ] 5.61 GiB / 31.14 GiB (18.00%)
Disk [ ] 266.90 GiB / 463.15 GiB (57.63%)
Battery [ ] 78.00% (Discharging)
```

Ya se tenia la herramienta de Wireshark previamente instalada.



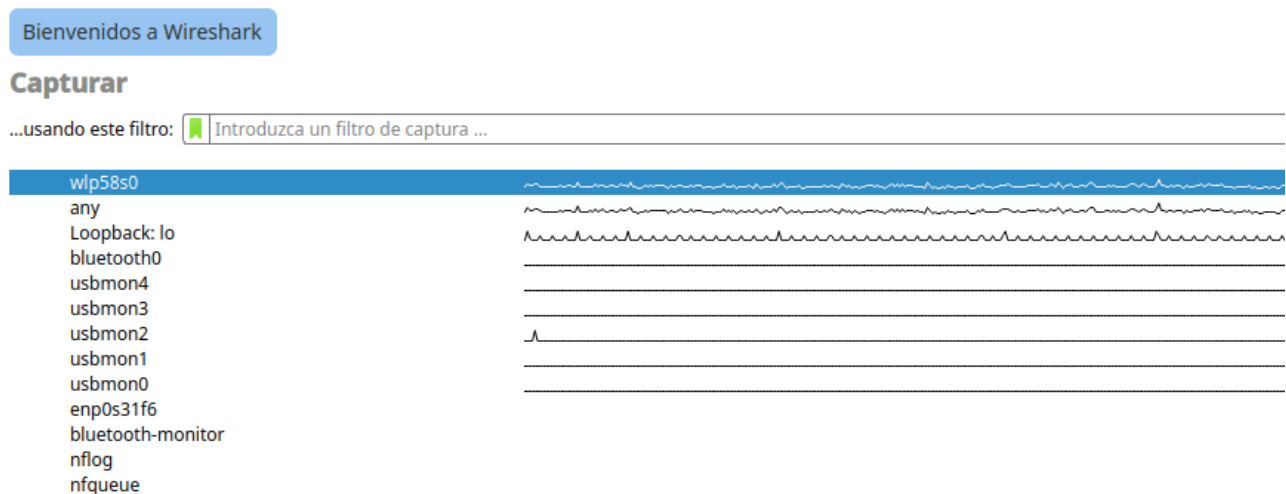
```
) sudo dnf install wireshark
[sudo] contraseña para skull-kaiser:
Actualizando y cargando repositorios:
Repositorios cargados.
El paquete "wireshark-1:4.6.3-1.fc43.x86_64" ya está instalado.

Nada que hacer.
```

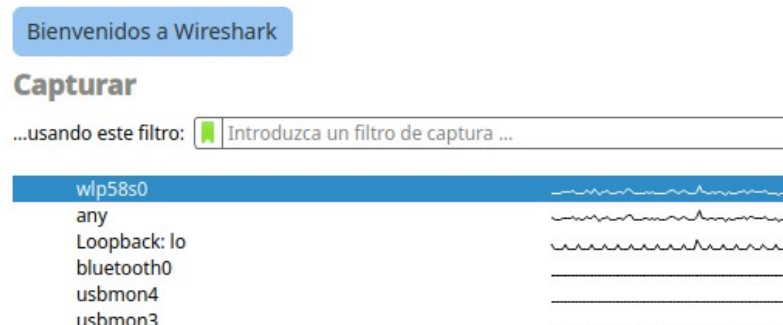
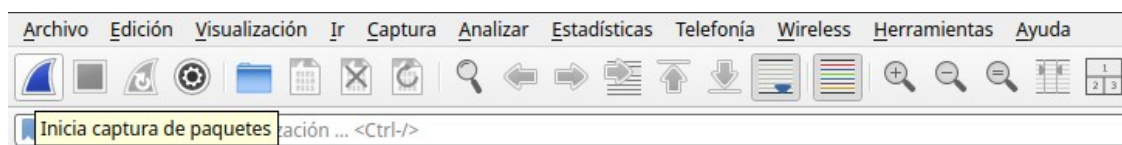
## 2. Inicio de la practica

### 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.







**ONLINE BANKING LOGIN**

**PERSONAL**

**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](#)

## Online Banking Login

Username:

Password:

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	6.829808980	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	6.580924569	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	6.820908980	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 wlp58s0, 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)				0000 46 94 73 7e 1f f9 fa 6b 59 17 c1 cc 08 00 45 00 F...s...k Y.....E: 0010 01 09 8f a8 40 00 40 00 c2 3c 0a df 11 62 41 3d ... ..0 .. ... ..bA= 0020 89 75 8f d4 00 59 30 08 6d 4e 0b 7e 85 a7 80 18 u... ..00 mH..... 0030 00 3f e8 b5 00 00 01 01 08 0a f8 be d5 de 45 f4 ?..... ..E: 0040 a3 12 47 45 54 20 2f 6c 6f 67 69 6e 2e 6a 73 70 ..GET /l ogin.jsp 0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1. 1. Host: 0060 20 64 65 6d 6f 2e 74 65 73 74 66 69 72 65 2e 6e demo.te stfire.n 0070 65 74 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 et-User -Agent: 0080 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 Mozilla/ 5.0 (X11 0090 3b 29 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 ; Linux x86_64; 00a0 72 76 3a 31 34 37 2e 30 29 20 47 65 63 6b 6f 2f rv:147.0 ) Gecko/ 00b0 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 20100101 Firefox 00c0 2f 31 34 37 2e 30 0d 0a 41 63 63 65 70 74 3a 20 /147.0.0 Accept: 00d0 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 text/htm l,applic 00e0 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 70 6d 6c 2c ation/xh tml+xml, 00f0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 70 6d 6c 3b applicat ion/xml; 0100 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d q=0.9,*/* ;q=0.8 0110 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 Accept- Language 0120 3a 20 65 73 2d 4d 58 2c 65 73 3b 71 3d 30 2e 39 : es-MX, es;q=0.9 0130 2c 65 6e 2d 55 53 3b 71 3d 30 2e 38 2c 65 6e 3b ,en-US;q =0.8,en; 0140 71 3d 30 2e 37 0d 0a 41 63 63 65 70 74 2d 45 6e q=0.7 Accept-En 0150 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip, de 0160 66 6c 61 74 65 0d 0a 52 65 66 65 72 65 72 3a 20 fflate Referer: 0170 68 74 74 70 3a 2f 2f 64 65 6d 6f 2e 74 65 73 74 http://d emo.test 0180 66 69 72 65 2e 6e 65 74 2f 6c 6f 67 69 6e 2e 6a fire.net /login.j 0190 73 70 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 sp-Conn ection: 01a0 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 keep-aliv e Upgr 01b0 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 ade-Inse cure-Req 01c0 75 65 73 74 73 3a 20 31 0d 0a 50 72 69 6f 72 69 uests: 1 -Priori 01d0 74 79 3a 20 75 3d 30 2c 20 69 0d 0a 0d 0a ty: u=0, i.....			
--	--	--	--	---	--	--	--

▶ Frame 102: Packet, 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface wlp58s0, 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	0.447470566	10.223.17.98	146.112.61.106	TCP	74 50730 → 443 [SYN] Seq=339861144 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1586474666 TSecr=0 WS=1024
7	0.455901871	146.112.61.106	10.223.17.98	TCP	74 443 → 50736 [SYN, ACK] Seq=1767026852 Ack=339861145 Win=14480 Len=0 MSS=1382 SACK_PERM TSval=1173659809 TSecr=1586474666 WS=256
24	1.009348974	10.223.17.98	146.112.61.106	TCP	74 50748 → 443 [SYN] Seq=3737367192 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1586475228 TSecr=0 WS=1024
25	1.015440741	146.112.61.106	10.223.17.98	TCP	74 443 → 50748 [SYN, ACK] Seq=1250184775 Ack=3737367193 Win=14480 Len=0 MSS=1382 SACK_PERM TSval=1173659865 TSecr=1586475228 WS=256
43	1.235406604	10.223.17.98	146.112.61.106	TCP	74 50752 → 443 [SYN] Seq=2424092011 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1586475454 TSecr=0 WS=1024
44	1.242899069	146.112.61.106	10.223.17.98	TCP	74 443 → 50752 [SYN, ACK] Seq=3213182419 Ack=2424092012 Win=14480 Len=0 MSS=1382 SACK_PERM TSval=1173659888 TSecr=1586475454 WS=256
58	1.481127530	10.223.17.98	146.112.61.106	TCP	74 50768 → 443 [SYN] Seq=2069908666 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1586475706 TSecr=0 WS=1024
60	1.732319253	10.223.17.98	146.112.61.106	TCP	74 50776 → 443 [SYN] Seq=438323855 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1586475951 TSecr=0 WS=1024
61	1.765085825	146.112.61.106	10.223.17.98	TCP	74 443 → 50776 [SYN, ACK] Seq=1569316323 Ack=438323856 Win=14480 Len=0 MSS=1382 SACK_PERM TSval=1173659940 TSecr=1586475951 WS=256
74	6.577729517	10.223.17.98	65.61.137.117	TCP	74 80 → 40916 [SYN] Seq=819489570 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4173255915 TSecr=0 WS=1024
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 TSval=4173255915 TSecr=0 WS=1024
96	6.586376683	65.61.137.117	10.223.17.98	TCP	74 80 → 40916 [SYN, ACK] Seq=3950937309 Ack=819489571 Win=14480 Len=0 MSS=1382 SACK_PERM TSval=1173660422 TSecr=4173255915 WS=256

Frame 96: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp880, id 0		0000	fa 6b 59 17 c1 cc 10 80 7e 1f f9 08 00 45 00	..K.Y...E
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)		0010	00 3c 06 a3 40 00 3f 06 4e 26 41 3d 09 75 0a df	...c...u
Destination: fa:6b:59:17:c1:cc (fa:6b:59:17:c1:cc)		0020	11 62 00 50 9f d4 eb 7e 84 dd 30 d8 6b 23 a0 12	...b.P...k#...
Source: 46:94:73:7e:1f:f9 (46:94:73:7e:1f:f9)		0030	38 90 c5 97 00 00 02 04 05 66 04 02 08 0a 45 f4	8.....f....E
Transmission Control Protocol, Src Port: 80, Dst Port: 40916, Seq: 3950937309, Ack: 819489571, Len: 0		0040	a3 06 f8 be d4 eb 01 03 03 08	.....

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 TSval=4173255915 TSecr=0 WS=1024
96	6.586376683	65.61.137.117	10.223.17.98	TCP	74 80 → 40916 [SYN, ACK] Seq=3950937309 Ack=819489571 Win=14480 Len=0 MSS=1382 SACK_PERM TSval=1173660422 TSecr=4173255915 WS=256
97	6.586480163	10.223.17.98	65.61.137.117	TCP	66 40916 → 80 [ACK] Seq=819489571 Ack=3950937310 Win=64512 Len=0 TSval=4173255924 TSecr=1173660422

- ¿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

No.

Time

Source

Destination

Protocol

Length

Info

73

12.476253541

10.223.17.98

35.162.251.77

TLSv1.2

179

Application Data

74

12.476402946

10.223.17.98

35.162.251.77

TLSv1.2

1314

Application Data

82

12.491197282

10.223.17.98

148.226.1.37

TLSv1.2

1789

Client Hello (SN=ds1api.es.uv.mx)

93

12.512889862

148.226.1.37

10.223.17.98

TLSv1.2

945

Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done

95

12.532169431

10.223.17.98

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

10.223.17.98

148.226.1.37

TLSv1.2

993

Application Data

98

12.555164831

148.226.1.37

10.223.17.98

TLSv1.2

1159

Application Data

99

12.567246178

10.223.17.98

148.226.1.37

TLSv1.2

1223

Application Data

100

12.589561839

35.162.251.77

10.223.17.98

TLSv1.2

381

Application Data, Application Data

103

12.649966812

148.226.1.37

10.223.17.98

TLSv1.2

727

Application Data

104

12.666963688

10.223.17.98

148.226.1.37

TLSv1.2

1255

Application Data

112

12.745534795

148.226.1.37

10.223.17.98

TLSv1.2

1436

Application Data

114

12.745739848

10.223.17.98

148.226.1.37

TLSv1.2

1288

Application Data

116

12.832544369

10.223.17.98

35.162.251.77

TLSv1.2

179

Application Data

117

12.832643931

10.223.17.98

35.162.251.77

TLSv1.2

472

Application Data

120

12.918824775

10.223.17.98

148.226.1.37

TLSv1.2

1143

Application Data

126

12.930313466

10.223.17.98

148.226.1.37

TLSv1.2

1853

Client Hello (SN=ds1api.es.uv.mx)

129

12.932115979

10.223.17.98

148.226.1.37

TLSv1.2

1853

Client Hello (SN=ds1api.es.uv.mx)

142

12.949455534

148.226.1.37

10.223.17.98

TLSv1.2

2886

Application Data

151

12.959795189

148.226.1.37

10.223.17.98

TLSv1.2

231

Server Hello, Change Cipher Spec, Encrypted Handshake Message

155

12.959789144

148.226.1.37

10.223.17.98

TLSv1.2

231

Server Hello, Change Cipher Spec, Encrypted Handshake Message

168

12.969965593

148.226.1.37

10.223.17.98

TLSv1.2

1436

Application Data

181

12.988996669

148.226.1.37

10.223.17.98

TLSv1.2

2886

Application Data

187

12.994441893

10.223.17.98

148.226.1.37

TLSv1.2

141

Change Cipher Spec, Encrypted Handshake Message

188

12.995932788

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

1436

Application Data

196

13.023839987

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

Frame 93: Packet, 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits) on interface wlp58s0, id 0

Ethernet II, Src: fa:6b:59:17:c1:c0 (fa:6b:59:17:c1:c0), Dst: fa:6b:59:17:c1:c0 (fa:6b:59:17:c1:c0)

Destination: fa:6b:59:17:c1:c0 (fa:6b:59:17:c1:c0)

... .. LG bit: Locally administered address (this is NOT the factory default)

... .. LG bit: Individual address (unicast)

Source: 10.223.17.98 (10.223.17.98)

... .. LG bit: Locally administered address (this is NOT the factory default)

... .. LG bit: Individual address (unicast)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 148.226.1.37, Dst: 10.223.17.98

Transmission Control Protocol, Src Port: 443, Dst Port: 55188, Seq: 3972582176, Ack: 3713416769, Len: 879

[5 Reassembled TCP Segments (5671 bytes): #85(1370), #87(1370), #89(1370), #91(1682), #93(879)]

Transport Layer Security

0000

fa 6b 59 17 c1 c0

10 22 31 79 88 06 45 00

7e 1f 99 88 06 45 00

...

...

...

0001

03 a3 02 78 40 00 0f 06

83 95 94 e2 01 25 0a df

...

...

...

0020

11 62 01 bb 07 94 ec c8

cb 20 d0 56 3e 41 89 18

...

...

...

0030

00 4e c8 31 00 00 01 01

08 45 f8 b6 f2 91 de

...

...

...

0040

1b 1e 96 a1 27 68 e5 09

ce cf a3 78 39 da ba 09

...

...

...

0050

06 08 b7 f8 50 93 f2 79

57 1b 0f fe 18 80 31 c7

...

...

...

0060

42 93 a8 3a d7 3b 6f 0f

52 6e df 8b 7f fa 04 a5

...

...

...

0070

a6 5a b6 31 63 14 0e

48 38 cb 6c 34 a7 49

...

...

...

0080

ac 16 15 3d 1c 7e 89 52

70 a8 c3 bb 74 ef bf e7

...

...

...

0090

3f bf 74 5b 27 af 9f bd

78 f8 81 b9 06 82 93 01

...

...

...

00a0

00 01 a3 81 87 39 81 84

08 0e 63 55 1d 0f 01

...

...

...

00b0

01 ff 04 04 03 02 07 80

33 10 06 03 51 1d 25 04

...

...

...

00c0

0c 55 14 0a 06 08 02 01

95 05 07 03 09 30 c8 06

...

...

...

00d0

03 55 1d 13 01 81 01 04

92 30 39 1d 06 83 55

...

...

...

00e0

1d 0e 04 16 04 14 e9 0f

9d fe f9 7b ba 50 88 13

...

...

...

00f0

46 2f 02 63 cb a7 f1 42

7 c 3d 30 1f 06 03 55 1d

...

...

...

0100

23 04 18 39 16 08 10 40

2 c 8d 27 b8 cc 34 83 30

...

...

...

0110

42 33 07 7f 6c b3 70 64

2 c 80 c8 30 8f 06 99 2b

...

...

...

0120

06 01 05 05 07 39 01 05

04 02 05 06 39 06 06 09

...

...

...

0130

2a 86 48 86 7f 0d 01 01

0b 65 0d 00 82 01 81 05

...

...

...

0140

0a 4c 4e ac 52 cc a3 20

6d df cf c5 8a 50 a8 28

...

...

...

0150

bd a3 37 51 70 cb 3c 26

19 4c 4e 1b 20 27 81 28

...

...

...

0160

07 8a 27 b4 4e 3c 69 ec

e5 9c 7a 0e 28 2c 69

...

...

...

0170

f3 40 24 cd 83 b7 7e

49 87 e4 a9 c1 99 18 07

...

...

...

0180

a3 40 8b c1 12 5b 57 02

3f 7e f1 c7 77 63 67 98

...

...

...

0190

2a 74 f1 13 c8 09 ec 4e

bb 1a 17 98 03 28 15

...

...

...

01a0

f1 fd eb 5f b4 b2 98 ec

bb 74 0c 7d 79 a1 9c a9

...

...

...

01b0

8d b9 51 13 8b 7e 1b 4e

21 5f 80 99 a1 80 15 6a

...

...

...

01c0

01 40 9e 0a c8 04 b6 e4

6a 04 ba bf 32 c1 55 ab

...

...

...

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

```
# # # # #
13972 65.656812310 65.65681231 19.223.17.98 HTTP 192 HSTS /dologin HTTP/1.1 application/x-www-form-urlencoded)
13977 65.662922478 65.66292247 19.223.17.98 HTTP 531 GET /login.jsp HTTP/1.1
13988 65.739182448 2886:370:7273:c4e0:: 2698:1901:8:3bd7:: HTTP 412 GET /success.txt?ip= IPv4/HSTP/1.1
14001 65.837658458 2886:370:7273:c4e0:: 2698:376:7273:c4e0:: HTTP 302 HTTP/1.1 200 OK (text/plain)
14011 65.838449426 65.61.137.117 19.223.17.98 HTTP 691 HTTP/1.1 200 OK (text/html)
14149 70.579878448 65.61.137.117 19.223.17.98 HTTP 380 GET /canonical.html HTTP/1.1
14150 70.666323382 34.107.221.82 19.223.17.98 HTTP 364 HTTP/1.1 200 OK (text/html)
14151 70.685206018 34.107.221.82 19.223.17.98 HTTP 397 GET /success.txt?ip= IPv4/HSTP/1.1
14166 70.763754153 34.107.221.82 19.223.17.98 HTTP 282 HTTP/1.1 200 OK (text/plain)
14179 71.130627672 19.223.17.98 34.107.221.82 HTTP 397 GET /success.txt?ip= IPv4/HSTP/1.1
14183 71.134422418 19.223.17.98 34.107.221.82 HTTP 380 GET /canonical.html HTTP/1.1
14191 71.160909952 19.223.17.98 34.107.221.82 HTTP 282 HTTP/1.1 200 OK (text/plain)
14193 71.182617394 34.107.221.82 19.223.17.98 HTTP 364 HTTP/1.1 200 OK (text/html)
14195 71.185219515 19.223.17.98 34.107.221.82 HTTP 397 GET /success.txt?ip= IPv4/HSTP/1.1

# # # # #
Frame 13978: Packet, 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits) on interface wlan58s0, id 0
Ethernet II, Src: Fa-60:59:1f:cfc (fa:60:59:1f:cfc), 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)
... .. . = IG bit: Locally administered address (this is NOT the factory default)
Source MAC Address: ... .. = IG bit: Individual address (unicast)
Source IP Address: Fa-60:59:1f:cfc (fa:60:59:1f:cfc)
... .. . = IG bit: Locally administered address (this is NOT the factory default)
Type: IPv4 (0x0600)
Stream index: 0
Internet Protocol Version 4, Src: 19.223.17.98, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 49500, Dst Port: 80, Seq#: 894815534, Ack#: 2546971139, Len: 688
Hypertext Transfer Protocol
POST /dologin HTTP/1.1\r\n
Host: demo.testfire.net\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: es-MX,en;q=0.8,en-US;q=0.7,en-GB;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 41\r\n
Origin: http://demo.testfire.net/\r\n
Connection: keep-alive\r\n
Referer: http://demo.testfire.net/login.jsp\r\n
Cookie: JSESSIONID=25B70F6C107BCACE6E2B3CF918264AAA1\r\n
Upgrade-Insecure-Requests: 1\r\n
Priority: u=0,\r\n
\r\n
[Response in Frame: 13972]
Full request URI: http://demo.testfire.net/dologin
File Data: 41 bytes
```

¿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 usuario