# Sistemas Telemáticos para Medios Audiovisuales Práctica 4: HTTP

Departamento de Teoría de la Señal y Comunicaciones y Sistemas Telemáticos y Computación (GSyC)

#### Noviembre de 2018

Cuando un mensaje HTTP ocupa más de un segmento TCP, Wireshark muestra el siguiente mensaje por cada uno de los segmentos TCP que son parte de dicho mensaje HTTP:

#### [TCP segment of a reassembled PDU]

Cuando Wireshark interpreta que se ha recibido todo el mensaje HTTP, como resultado de haber recibido previamente un conjunto de segmentos TCP segment of a reassembled PDU, Wireshark concatena todos estos segmentos para mostrar el mensaje HTTP completo.

Por ejemplo, en la figura 1 se puede ver como en el segmento 8 se muestra todo el mensaje HTTP que en realidad viajaba en 3 segmentos TCP: segmento 4, 8 y 9.

Time	1 2 3	0.000000		Destination		
2 0.004014 21.0.0.21 13.0.0.13 TCP 74 80 - 54889 [SYM, ACK] Seq=0 ACK=1 Win=5702 Len=0 MSS=1460 . 3 0.004322 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=1 ACK=1 Win=5840 Len=0 TSVal=35096 TS. 4 8.895756 13.0.0.13 21.0.0.21 TCP 92 [TCP seement of a reassembled PDU] 5 8.890608 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 ACK=27 Win=5792 Len=0 TSVal=95458 T. 6 15.845293 13.0.0.13 21.0.0.21 TCP 78 [TCP seement of a reassembled PDU] 7 15.845595 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 ACK=39 Win=5792 Len=0 TSVal=95458 T. 8 17.189318 13.0.0.13 21.0.0.21 HTTP 68 GET /Index.html HTTP/1.1 9 17.189493 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 ACK=39 Win=5792 Len=0 TSVal=96152 T. 10 17.190414 21.0.0.21 13.0.0.13 HTTP 68 GET /Index.html HTTP/1.1 200 K (text/html) 11 17.190928 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=1 ACK=38 Win=5912 Len=0 TSVal=96287 T. 12 29.704320 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=1 ACK=38 Win=5912 Len=0 TSVal=37419. 12 29.704320 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=1 ACK=38 Win=5912 Len=0 TSVal=37419. 12 29.704320 13.0.0.13 21.0.0.21 TCP 91 [TCP segment of a reassembled PDU] Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) Ethernet II, Src: alies21:a9:90:5f (alies21:a9:90:5f), Dst: 7c:24:6e:dd:8f:8e (7e:24:6e:dd:8f:8e) Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21 Transmission Control Protocol, Src Port: 54689 [Sed=1 ACK=38] Port: 80 (80), Seq: 39, ACK: 1, Len: 2 [3 Reassembled TCP Segments (40 bytes): M4(26) [MB(2)] Hypertext Transfer Protocol  FGET /index.html HTTP/1.1\r\n Host: wwwl\r\n   FGET /index.html   HTTP/1.1\r\n   Host: wwwl\r\n   FGET /index.html   HTTP/1.1\r\n   Host: wwwl\r\n   FGET /index.html   HTTP/1.1\r\n   Fort = 66 B0 = 54689   ACK   Seq=1 ACK=27 Win=5792 Len=0 TSVal=37640     FGET /index.html   HTTP/1.1\r\n   FGET /index.html   HTTP/1.1\r\n	2 3		42 0 0 42		Protocol	Length Info
3 0.004322 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=1 Ack=1 Win=5840 [en=0 TSval=35696 TS. 4 8.895756 13.0.0.13 21.0.0.21 TCP 92 [TCP segment of a reassembled PDU]  5 8.896066 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=27 Win=5792 Len=0 TSval=95458 T. 6 15.845293 13.0.0.13 21.0.0.21 TCP 78 [TCP segment of a reassembled PDU]  7 15.845295 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=27 Win=5792 Len=0 TSval=95458 T. 18.918 13.0.0.13 21.0.0.21 HTP 68 GET /index.html HTP/1.1  9 17.189493 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=39 Win=5792 Len=0 TSval=96287 T. 19.190414 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=41 Win=5792 Len=0 TSval=96287 T. 19.190414 21.0.0.21 13.0.0.13 TCP 66 54689 - 80 [ACK] Seq=1 Ack=41 Win=5792 Len=0 TSval=96287 T. 19.17.190928 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=1 Ack=41 Win=5792 Len=0 TSval=96287 T. 19.17.190928 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=1 Ack=41 Win=5792 Len=0 TSval=96287 T. 19.17.190928 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419. 12.9.704320 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419. 12.9.704320 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419. 12.9.704320 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419. 12.0.0.21 TCP 67 40 [TCP Segment of a reassembled PDU]  Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)  [Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)  [Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (546 bits)  [Frame 8: 68 bytes on wire (540 bits)	3	0.004014	13.0.0.13	21.0.0.21	TCP	74 54689 - 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1
4 8.895756 13.6.9.13 21.6.9.21 TCP 92 [TCP segment of a reassembled PDU] 5 8.896080 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=27 Win=5792 Len=0 TSval=95458 T. 6 15.84593 13.0.0.13 21.0.0.21 TCP 78 [TCP segment of a reassembled PDU] 7 15.845955 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=27 Win=5792 Len=0 TSval=95458 T. 8 17.189318 13.0.0.13 21.0.0.21 HTTP 68 88 - 54689 [ACK] Seq=1 Ack=39 Win=5792 Len=0 TSval=96152 T. 9 17.189493 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=39 Win=5792 Len=0 TSval=96152 T. 10 17.190414 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=41 Win=5792 Len=0 TSval=96287 T. 11 17.190412 13.0.0.13 TCP 66 54689 - 80 [ACK] Seq=1 Ack=353 Win=6912 Len=0 TSval=96287 T. 11 17.190412 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=1 Ack=353 Win=6912 Len=0 TSval=37419. 11 29.704320 13.0.0.13 21.0.0.21 TCP 91 [TCP segment of a reassembled PDU]  Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)  Ethernet II, Src: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)  Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21  Transmission Control Protocol, Src Port: 54689 (54689) Dst Port: 80 (80), Seq: 39, Ack: 1, Len: 2  [3 Reassembled TCP Segments (40 bytes): #4(26) #8(2)]  Hypertext Transfer Protocol  FGET /index.html HTTP/1.1\r\n  Host: wwwl\r\n \r\n  [Full request URI: http://www1/index.html]  [HTTP request URI: http://www1/index.html]  [HTTP request URI: http://www1/index.html]  [Response in frame: 10]			21.0.0.21	13.0.0.13	TCP	
\$ 8.896868 21.6.0.21	4					
6 15.845293 13.6.0.13 21.6.0.21 TCP 78 [TCP segment of a reassembled PDU] 7 15.845595 21.0.0.21 13.0.0.13 TCP 66 80 - 54089 [ACK] Seq=1 Ack=39 Win=5792 Len=0 TSval=96152 T. 8 17.189318 13.0.0.13 21.0.0.21 HTTP 68 GET /Index.html HTTP/1.1 9 17.189493 21.0.0.21 13.0.0.13 TCP 66 80 - 54089 [ACK] Seq=1 Ack=41 Win=5792 Len=0 TSval=96287 T. 10 17.190414 21.0.0.21 13.0.0.13 HTTP 418 HTTP/1.1 290 OK (text/html) 11 17.190928 13.0.0.13 21.0.0.21 TCP 66 54089 - 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=96287 T. 12 29.704320 13.0.0.13 21.0.0.21 TCP 66 54089 - 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419. 12 29.704320 13.0.0.13 21.0.0.21 TCP 91 [TCP segment of a reassembled PDU] Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) Ethernet II, Src: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f), Dst: 70:24:60:dd:8f:00 (70:24:60:dd:8f:00) Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21 Transmission Control Protocol, Src Port: 54089 [ASK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419. 13 Reassembled TCP Segments (40 bytes): W4(26) P0: W4(26) P0						
7 15.84595 21.8.9.21 13.8.9.13 TCP 66 88 - 54689 [ACK] Seq=1 Ack=39 Win=5792 Len=8 TSval=96152 T. 8 17.189318 13.8.0.13 21.8.0.21 HTTP 68 GET /index.html HTTP/1.1 9 17.189493 21.8.0.21 13.8.0.13 TCP 66 88 - 54689 [ACK] Seq=1 Ack=34 Win=5792 Len=8 TSval=96287 T. 16 17.199414 21.8.0.21 13.8.0.13 HTTP 418 HTTP/1.1 280 OK (text/html) 11 17.199928 13.8.0.13 21.8.0.21 TCP 66 54689 = 88 [ACK] Seq=1 Ack=35 Win=592 Len=8 TSval=96287 T. 12 29.704320 13.8.0.13 21.0.0.21 TCP 91 [TCP segment of a reassembled PDU]  Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) Ethernet II, Src. a2:ea:221:a9:99:5f (a2:ea:21:a9:99:5f), Dst: 7e:24:6e:dd:8f:8e (7e:24:6e:dd:8f:8e) Internet Protocol Version 4, Src: 13.8.0.13, Dst: 21.8.9.21 Transmission Control Protocol, Src Port: 54689 (54689) Dst Port: 80 (80), Seq: 39, Ack: 1, Len: 2 [3 Reassembled TCP Segments (40 bytes): 74(26)						
8 17.189318 13.8.9.13 21.8.9.21 HTTP 68 CET /Index.html HTTP/1.3 9 17.189493 21.0.0.21 13.0.0.13 TCP 66 80 - 54689 [ACK] Seq=1 Ack=41 Win=5792 Len=0 TSval=96287 T. 10 17.190414 21.0.0.21 13.0.0.13 HTTP 418 HTTP/1.1 200 OK (text/html) 11 17.190928 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419. 12 29.704320 13.0.0.13 21.0.0.21 TCP 91 [TCP segment of a reassembled PDU]  Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) Ethernet II, Src: azica:21:a9:99:5f (azica:21:a9:99:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e) Internet Protocol Version 4, Src: 13.8.0.13, Dst: 21.0.0.21  Transmission Control Protocol, Src Port: 54689 (54689) Bst Port: 80 (80), Seq: 39, Ack: 1, Len: 2 [3 Reassembled TCP Segments (40 bytes): #4(26) #8(2)]  Hypertext Transfer Protocol Hypertext Transfer Protocol Hypertext Transfer Protocol Hypertext Transfer Protocol FGET /index.html HTTP/1.1\n Host: www1\r\n Full request URI: http://www1/index.html] [HTTP request URI: http://www1/index.html] [HTTP request URI: http://www1/index.html] [Response in frame: 10]						
9 17.189493						
18 17.1989414 21.8.9.21 13.8.9.13 HTTP 418 HTTP/1.1 280 0K (text/html) 11 17.198928 13.8.0.13 21.8.0.21 TCP 66 54689 - 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419. 12 29.704320 13.0.0.13 21.0.0.21 TCP 91 [TCP segment of a reassembled PDU]  Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) Ethernet II, Src: a2:ea:21:a9:96:5f (a2:ea:21:a9:96:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e) Internet Protocol Version 4, Src: 13.8.0.13, Dst: 21.0.0.21  Transmission Control Protocol, Src Port: 54680 (54680) [3 Reassembled TCP Segments (40 bytes): m4(25)						
11 17.196928 13.0.0.13 21.0.0.21 TCP 66 54689 - 80 [ACK] Seq-41 Ack=353 Win=6912 Len=0 TSval=37419.  12 29.704320 13.0.0.13 21.0.0.21 TCP 91 [TCP segment of a reassembled PDU]  Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)  Ethernet II, Src: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)  Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21  Transmission Control Protocol, Src Port: 54680 (54689), Dst Port: 80 (80), Seq: 39, Ack: 1, Len: 2  [3 Reassembled TCP Segments (40 bytes): #4(26)]  **Portext Transfer Protocol  **GET /index.html HTTP/1.1\r\n  Host: www1\r\n \r\n  [Full request URI: http://www1/index.html]  [HTTP request 1/2]  [Response in frame: 10]						
12 29.704320 13.0.0.13 21.0.0.21 TCP 91 [TCP segment of a reassembled PDU]  Frame 8: 08 bytes on wire (544 bits), 08 bytes captured (544 bits)  Ethernet II, Src. a2:ea:221:a9:96:5f (a2:ea:21:a9:96:f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)  Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21  Transmission Control Protocol, Src Port: 54889 (54889)  [3 Reassembled TCP Segments (40 bytes): 74426)  Hypertext Transfer Protocol  FGET /index.html HTTP/1.1\r\n  Host: Whwi\r\n \r\n  [Full request URI: http://www1/index.html]  [HTTP request 1/2]  [Response in frame: 10]						
Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)  Ethernet II, Src: a2:ea:21:a9:99:5f (a2:ea:21:a9:99:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)  Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21  Transmission Control Protocol, Src Port: 54880 (54880) Dst Port: 80 (80), Seq: 39, Ack: 1, Len: 2  [3 Reassembled TCP Segments (40 bytes): #4(25) #6(12) #8(2)]  **Port: 80 (80), Seq: 39, Ack: 1, Len: 2  [6ET /index.html HTTP/1.l\r\n  Host: www1\r\n \r\n  [Full request URI: http://www1/index.html] [HTTP request 1/2] [Response in frame: 10]						
[Response in frame: 10]	Intern Transm [3 Rea Hypert • GET	net Protocol mission Contr assembled TCP ext Transfer /index.html	Version 4, Src: 13 ol Protocol, Src F Segments (40 byte Protocol	3.0.0.13, Dst: 21.0.0. Port: 54689 (54689), D	21 <u>st Po</u> rt: 80 (8	
	Intern Transm [3 Rea Hypert • GET Host \r\n [Fu]	net Protocol mission Contr missembled TCP mext Transfer /index.html min	Version 4, Src: 13 ol Protocol, Src 8 Segments (40 byte Protocol HTTP/1.1\r\n	3.0.0.13, Dst: 21.0.0. Port: 54689 (54689) Des): #4(26) #6(12)	21 <u>st Po</u> rt: 80 (8	· · · · · · · · · · · · · · · · · · ·
Tueste radianae vir rigina val	Intern Transm [3 Rea Hypert FGET Host \r\n [Fu] [HTT	net Protocol mission Contr missembled TCP missemble	Version 4, Src: 13 ol Protocol, Src F Segments (40 byte Protocol HTTP/1.1\r\n  II: http://www1/in- 2]	3.0.0.13, Dst: 21.0.0. Port: 54689 (54689) Des): #4(26) #6(12)	21 <u>st Po</u> rt: 80 (8	· · · · · · · · · · · · · · · · · · ·
	Intern Transm [3 Rea Hypert FGET Host \r\n [Fu] [HTT [Res	net Protocol mission Contr missembled TCP missemble	Version 4, Src: 10 ol Protocol, Src: 6 Segments (40 byte Protocol HTTP/1.1\r\n (1: http://www1/in- 2] me: 10]	3.0.0.13, Dst: 21.0.0. Port: 54689 (54689) Des): #4(26) #6(12)	21 <u>st Po</u> rt: 80 (8	· · · · · · · · · · · · · · · · · · ·
	Intern Transm [3 Rea Hypert F GET Host \r\n [Fu] [HTT	net Protocol mission Contr missembled TCP missemble	Version 4, Src: 10 ol Protocol, Src: 6 Segments (40 byte Protocol HTTP/1.1\r\n (1: http://www1/in- 2] me: 10]	3.0.0.13, Dst: 21.0.0. Port: 54689 (54689) Des): #4(26) #6(12)	21 <u>st Po</u> rt: 80 (8	· · · · · · · · · · · · · · · · · · ·
	Intern Transm [3 Rea Hypert FGET Host \r\n [Fu] [HTT	net Protocol mission Contr missembled TCP missemble	Version 4, Src: 10 ol Protocol, Src: 6 Segments (40 byte Protocol HTTP/1.1\r\n (1: http://www1/in- 2] me: 10]	3.0.0.13, Dst: 21.0.0. Port: 54689 (54689) Des): #4(26) #6(12)	21 <u>st Po</u> rt: 80 (8	
	Intern Transm [3 Rea Hypert FGET Host \r\n [Fu] [HTT [Res	net Protocol issaion Contr issambled TCP ext Transfer /index.html t: www.lr\n il request U/ pponse in fra ct request in	Version 4, Src: 12 ol Protocol, Src F Segments (40 byte Protocol HTTP/1.1\r\n iI: http://www1/in 2] me: 10] i frame: 16]	3.6.9.13, Dst: 21.6.6. port: 54689 (54689) poes: #4(26) po poe	21 st Port: 80 (8 6(2)]	30), Seq: 39, Ack: 1, Len: 2
000 47 45 54 20 2f 69 6e 64 65 78 2e 68 74 6d 6c 20 0ET /ind ex.html 010 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1Host:	Intern Transm [3 Rea Hypert + GET Host \r\n [Full [HTT] [Res [Nex	net Protocol nission Contr nissembled TCP next Transfer /index.html t: www1\r\n n ll request UP FP request UP FP request in fract request in	Version 4, Src: 12 ol Protocol, Src F Segments (40 byte Protocol HTTP/1.1\r\n  I: http://www1/ine 2] me: 10] frame: 16]	3.8.8.13, Dat: 21.8.0. Port: 54689 (54689) po (12)  dex.html]	21 st Port: 80 (8 8(2))	80), Seq: 39, Ack: 1, Len: 2

Figura 1: Mensaje HTTP compuesto de varios segmentos.

## 1. Comunicación cliente-servidor HTTP

Abre la captura http1.cap y responde a las siguientes preguntas:

- 1. Indica qué dirección IP es la de la máquina cliente HTTP y cuál la del servidor.
- 2. Indica qué versión HTTP están utilizando cliente/servidor
- 3. Indica si están utilizando conexiones persistentes o no persistentes y el número de conexiones que se ven en el fichero de captura.
- 4. ¿Cuántas peticiones GET observas desde el cliente?
- 5. ¿Cuántas URLs crees que ha escrito el usuario en el navegador para obtener dicha captura? ¿Cuál/es? ¿Por qué?
- 6. Fíjate en el contenido de la página index.html que se ha descargado el cliente. ¿Qué crees que ocurrirá cuando el navegador se haya descargado index.html?

Abre la captura http2.cap y responde a las siguientes preguntas:

- 7. Indica qué versión HTTP están utilizando cliente/servidor
- 8. Indica si están utilizando conexiones persistentes o no persistentes y el número de conexiones que se ven en el fichero de captura. ¿Por qué?

# 2. Diferentes tipos de respuestas de un servidor

Abre una pestaña en el navegador y selecciona en el menú Herramientas  $\rightarrow$  Desarrollador web  $\rightarrow$  Alternar herramientas. Selecciona la pestaña Red y HTML:



Esta vista del navegador te permitirá observar todos los mensajes HTTP que se están intercambiando al cargar una página.

Explica lo que ocurre al cargar las siguientes URLs:

1. Dentro de esa pestaña carga la página http://www.google.es/prueba. Selecciona dentro de las herramientas del desarrollador la petición GET y la pestaña Cabeceras.



Referrer-Policy: no-referrerCabeceras de la petición (850 B)

Accept-Encoding: gzip, deflateAccept-Language: en-US,en;q=0.5

Accept: text/html,application/xhtml+xm...plication

Fíjate en el campo Código de estado que indica el tipo de respuesta recibida y explica su contenido.

2. En esa misma pestaña carga la página http://www.wikipedia.com. Explíca qué ocurre en la primera petición GET y a partir de las líneas de cabecera que ves en la respuesta, explica la segunda petición GET. A la derecha del "Código de Estado", pulsa en "Cabeceras sin procesar" para ver la solicitud y la respuesta tal y como han sido transmitidas.

### 3. Formularios en HTTP

Abre la captura http3.cap y responde a las siguientes preguntas:

- 1. Indica qué tipo de conexiones HTTP utilizan el cliente y servidor e indica el número de conexiones entre cliente y servidor que aparecen en la captura.
- 2. Busca en la captura el segmento donde el servidor le envía al cliente un formulario. Indica los nombres de los campos del formulario que rellenará el usuario.
- 3. Indica si es el cliente o el servidor el que decide cómo debe enviar el cliente los datos del formulario (GET/POST) . ¿Qué método están usando en este caso? ¿Cómo lo sabes?
- 4. Busca en la captura el segmento donde el cliente le envía los datos del formulario al servidor y comprueba que se está realizando con el método GET
- 5. Fíjate cómo se llama el programa del servidor que va a recibir esos datos.
- 6. ¿Dónde viajan los datos que el cliente le envía al servidor? ¿Cuáles son esos datos?
- 7. Indica qué cabecera es la que representa el tipo de contenido del mensaje que el cliente envía al servidor con los datos del formulario.

Abre la captura http4.cap y responde a las siguientes preguntas:

- 9. Busca en la captura el segmento donde el servidor le envía al cliente un formulario. Indica los nombres de los campos del formulario que rellenará el usuario.
- 10. Indica si es el cliente o el servidor el que decide cómo debe enviar el cliente los datos del formulario (GET/POST). ¿Qué método están usando en este caso? ¿Cómo lo sabes?
- 11. Busca en la captura el segmento donde el cliente le envía los datos del formulario al servidor y comprueba que se está realizando con el método POST.
- 12. Fíjate cómo se llama el programa del servidor que va a recibir esos datos.
- 13. Indica qué cabecera es la que representa el tipo de contenido que el cliente envía al servidor y cuál es su valor.
- 14. Indica en qué parte del mensaje van los datos del formulario que el cliente le envía al servidor.
- 15. Explica si en este caso es necesario la cabecera Content-Length en el mensaje HTTP que el cliente envía al servidor con los datos del formulario. ¿Por qué?
- 16. Observa si el servidor le manda alguna respuesta cuando recibe los datos del formulario del cliente. En caso afirmativo localiza el número de segmento y observa en las cabeceras HTTP: tipo de contenido, longitud y cuerpo del mensaje

### 4. Cookies

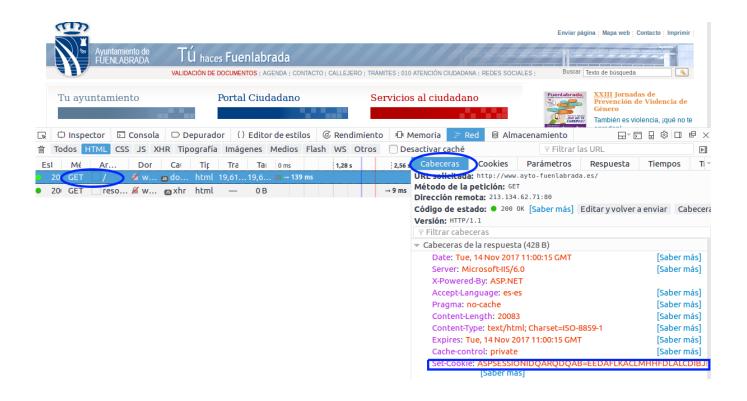
### 4.1. Almacén de cookies en el navegador Firefox

Para ver las Cookies en el navegador Firefox, selecciona la opción de menú: Editar → Preferencias. En la zona de la izquierda selecciona la pestaña Privacidad y seguridad. Dentro de la sección Historial, en Cookies y Datos pulsa en "Administrar Datos". Podrás consultar la lista de cookies que tienes almacenadas actualmente. Mira si tienes cookies del sitio web del Ayuntamiento de Fuenlabrada ayto-fuenlabrada.es/ (si las tienes, elimina sólo esas cookies).

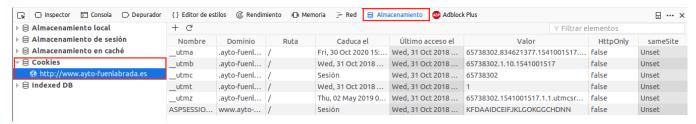
Abre otra pestaña en el navegador y selecciona en el menú Herramientas  $\rightarrow$  Desarrollador web  $\rightarrow$  Alternar herramientas. Selecciona la pestaña Red y HTML:



Dentro de esa pestaña carga la página http://www.ayto-fuenlabrada.es/. Selecciona dentro de las herramientas del desarrollador la petición GET y la pestaña Cabeceras.



- 1. Fíjate en la línea de cabecera que el servidor le envía al cliente con el contenido de las cookies.
- 2. Pulsa sobre la pestaña "Cookies" para poder ver de forma más clara el contenido de las cookies. Copia los campos importantes. Fíjate que no hay fecha de expiración, eso quiere decir que la Cookie se eliminará cuando se cierre el navegador.
- 3. Selecciona ahora la herramienta de desarrollador "Almacenamiento" y en el panel de la izquierda despliega "Cookies" para ver las cookies almacenadas al descargar esta página:



Indica qué cookies tienes almacenadas para el sitio ayto-fuenlabrada.es. Las cookies \_\_utmc, \_\_utmt son debidas a que el sitio web usa Google Analytics, es decir, al descargar la página del Ayuntamiento de Fuenlabrada se ha descargado también una biblioteca en javascript que ha creado estas cookies para este sitio web dentro de nuestro navegador. Estas cookies permiten medir la interacción de los usuarios con el sitio web. No te fijes en esas cookies de Google Analytics.

4. Vuelve a la herramienta de desarrollador "Red" y pulsa sobre la segunda petición GET que aparece, y oberva las cookies que se envían. Usa también la pestaña Cookies para poder ver mejor los valores que se envían.

# 4.2. Envío de Cookies en mensajes HTTP

Abre la captura http5.cap y responde a las siguientes preguntas:

- 1. Indica qué cookies envía el servidor al cliente:
- 2. Indica qué cookies enviará el cliente al servidor cuando acceda a la página con la URL: http://elcortebritanico/tienda/index.html
- 3. ¿Y si el cliente accediera en el año 2025 a dicha URL?
- 4. ¿Y si el cliente accediera en el año 2035 a dicha URL?

Abre la captura http6.cap y responde a las siguientes preguntas:

- 5. Indica qué cookies el cliente está enviando al servidor.
- 6. ¿Por qué crees que le envía dichas cookies?
- 7. Escribe un ejemplo de la posibles cabeceras que le habrá enviado dicho servidor al cliente previamente.
- 8. A partir de la información de la captura ¿crees que si el cliente accede a otra página con la URL: http://www2/dir1/dir2/index.html enviaría esas cookies, más o menos?
- 9. A partir de la información de la captura ¿crees que si el cliente accede a otra página con la URL: http://www2/index.html enviaría esas cookies, más o menos?
- 10. A partir de la información de la captura ¿crees que si el cliente accede a otra página con la URL: http://www/index.html enviaría esas cookies, más o menos?

# 5. Comunicación a través de proxy HTTP

Abre la captura http7.cap y responde a las siguientes preguntas:

- 1. Indica qué dirección IP es el cliente, el proxy y el servidor final.
- 2. ¿Qué diferencia la petición HTTP que realiza el cliente de la petición que realiza el proxy?
- 3. Identifica el nombre de la máquina donde se encuentra el servidor HTTP.
- 4. ¿Se puede saber de la petición que realiza el proxy que dicho proxy tiene almacenada en su caché esa página?

Abre la captura http8.cap y responde a las siguientes preguntas:

- 5. Indica qué tipo de conexiones HTTP utilizan el cliente y servidor e indica el número de conexiones entre cliente y servidor que aparecen en la captura.
- 6. Explica qué es lo que se está descargando el cliente del servidor HTTP y cuantos objetos se descarga.
- 7. Observa en las cabeceras HTTP el tipo de contenido de cada uno de los objetos.
- 8. ¿Podrías saber si los paquetes capturados se corresponde a la comunicación entre un cliente y un proxy HTTP, entre un cliente y servidor final HTTP o entre un proxy y el servidor final HTTP? ¿Por qué?

9. Sabiendo que la comunicación se ha realizado a través de un proxy HTTP, mira las cabeceras HTTP que envía dicho proxy para ver si en ellas existe alguna que muestre cuál es su nombre.

Abre la captura http9.cap y responde a las siguientes preguntas:

10. ¿Podrías saber si los paquetes capturados se corresponde a la comunicación entre un cliente y un proxy HTTP, entre un cliente y servidor final HTTP o entre un proxy y el servidor final HTTP? ¿Por qué?

### 5.1. Caché en el proxy

Estudia las capturas http10.cap y http11.cap, teniendo en cuenta que las direcciones 11.0.0.1 y 12.0.0.1 corresponden a la misma máquina. Responde a las siguientes preguntas:

- 1. Indica cuáles son las direcciones IP del cliente, proxy y servidor web. ¿Cómo lo sabes?
- 2. Explica qué es lo que ocurre en estas capturas.
- 3. Localiza los campos relevantes con respecto al tratamiento de caché que incluye en las líneas de cabecera el servidor. ¿Qué significan?
- 4. Explica qué ocurre en la segunda consulta que realiza el cliente.
- 5. Viendo los paquetes 14 y 16 de la captura http10.cap indica cómo se puede saber que el contenido proviene de una caché.
- 6. ¿Crees que el cliente tiene caché?

# 6. Caché en el navegador

Busca en las preferencias del navegador la opción para eliminar el contenido de la caché.

Para ver cómo funciona la caché del navegador, despliega las herramientas del desarrollador tal y como lo hiciste en 4.1.

#### 6.1. Sitio web ICANN

Carga en la URL la dirección de ICANN (Internet Corporation for Assigned Names and Numbers, organización que coordina la asignación de identificadores en Internet: direcciones IPs, números de ASs, etc): http://www.icann.org.

Selecciona la petición GET / y la pestaña Cabeceras (el color verde intenso en el "200" al lado de la petición GET indica que se ha solicitado el recurso al servidor y se ha obtenido respuesta con el recurso):



Al desplegar la pestaña Cabeceras de la respuesta y de la petición observarás las cabeceras que se han incluido en el mensaje de respuesta y petición para obtener el recurso "/".

- 1. Despliega la pestaña de las cabeceras de la respuesta e indica qué tipo de caché se permite.
- 2. A la vista de los resultados, ¿qué crees que ocurrirá si se recarga la página en el navegador?
- 3. Abre otra pestaña en el navegador, selecciona de nuevo en las herramientas → desarrollador web → alternar herramientas. Teclea en esta nueva pestaña la mism URL: http://www.icann.org, observarás que se muestra nuevamente el recurso solicitado y la respuesta con el mismo (junto a la solicitud se muestra el recuadro verde intenso).

#### 6.2. Sitio web IETF

Carga en esa misma pestaña del navegador la dirección del IETF (Internet Engineering Task Force): http://www.ietf.org.

- 4. Selecciona la petición GET / y observa en las líneas de cabecera de respuesta qué tipo de caché se permite.
- 5. Indica cuándo expirará el recurso en la caché. Relaciona los valores de las cabeceras: Date, Expires y Cache-Control.
- 6. A la vista de los resultados ¿qué crees que ocurrirá si desde otra pestaña se solicita la misma URL?
- 7. Abre otra pestaña en el navegador, selecciona de nuevo en las herramientas → desarrollador web → alternar herramientas. Teclea en esta nueva pestaña la mism URL: http://www.ietf.org. Selecciona de nuevo la petición GET /. Al posicionar el ratón sobre el nombre de la petición GET, observarás que se muestra que el contenido estaba cacheado (fíjate que ahora toda la petición se muestra "atenuada", incluyendo el recuadro verde al lado de GET /, que ahora está atenuado). Fíjate en las líneas de cabecera: Date, Expires y Last-modified y explica si han cambiado y por qué.



#### 6.3. Sitio web MECD

Carga en una de las pestañas donde tengas abiertas las herramientas del desarrollador, la dirección del Ministerio de Educación: www.mecd.gob.es/portada-mecd/, selecciona la petición GET /portada-mecd/ y responde a las siguientes preguntas:

- 9. Observa las líneas de cabecera de la respuesta e indica qué tipo de caché se permite.
- 10. Indica cuándo expirará el recurso en la caché. Relaciona los valores de las cabeceras: Date, Expires y Cache-Control.
- 11. Abre una nueva pestaña del navegador con las herramientas del desarrollador visibles. Indica qué ocurre si tecleas la misma URL.

- 12. Espera el tiempo necesario para que la información caduque en la caché y abre una nueva pestaña con las herramientas del desarrollador visibles. Explica qué sucede cuando vuelves a teclear esta URL.
- 13. ¿Se está usando validación fuerte o débil?