Alexis Calderon

Práctica 2.1: Protocolo HTTP

Objetivo:

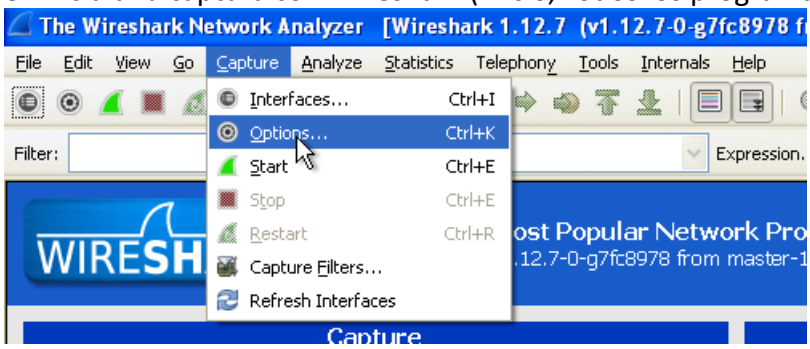
En esta práctica se analiza la información de los mensajes de petición y respuesta del protocolo HTTP.

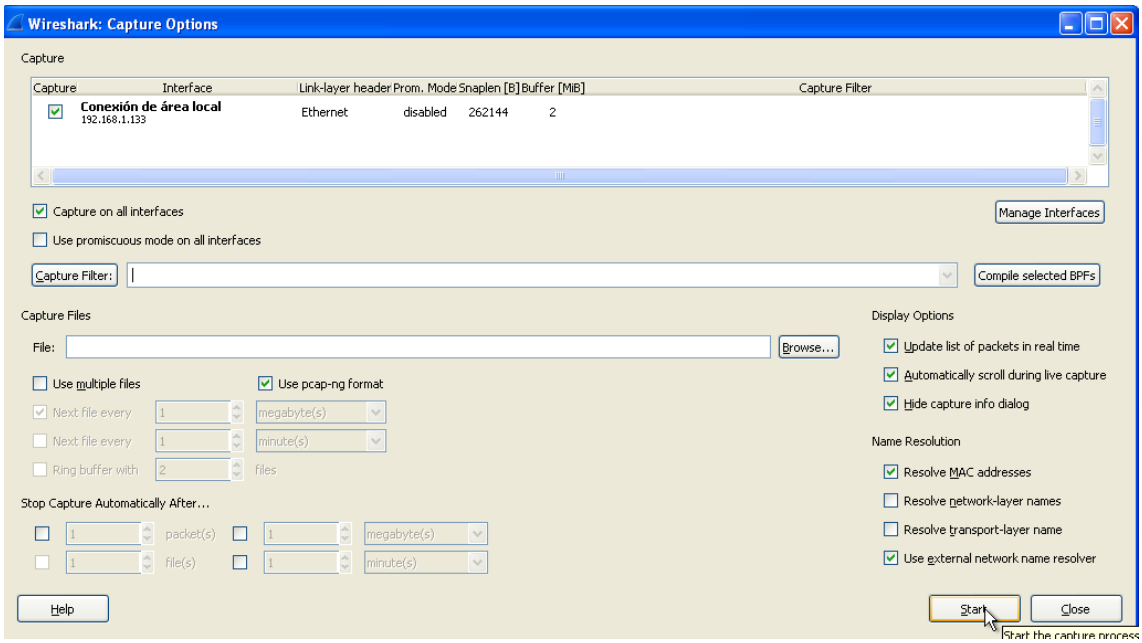
Pasos Previos:
Instalar el programa wireshark, cuyo ejecutable está en FTP.

1. Inicia sesión en Windows.

2. Abre el navegador que tengas en tu equipo.

3. Inicia una captura con Wireshark (Inicio, Todos los programas, Wireshark)





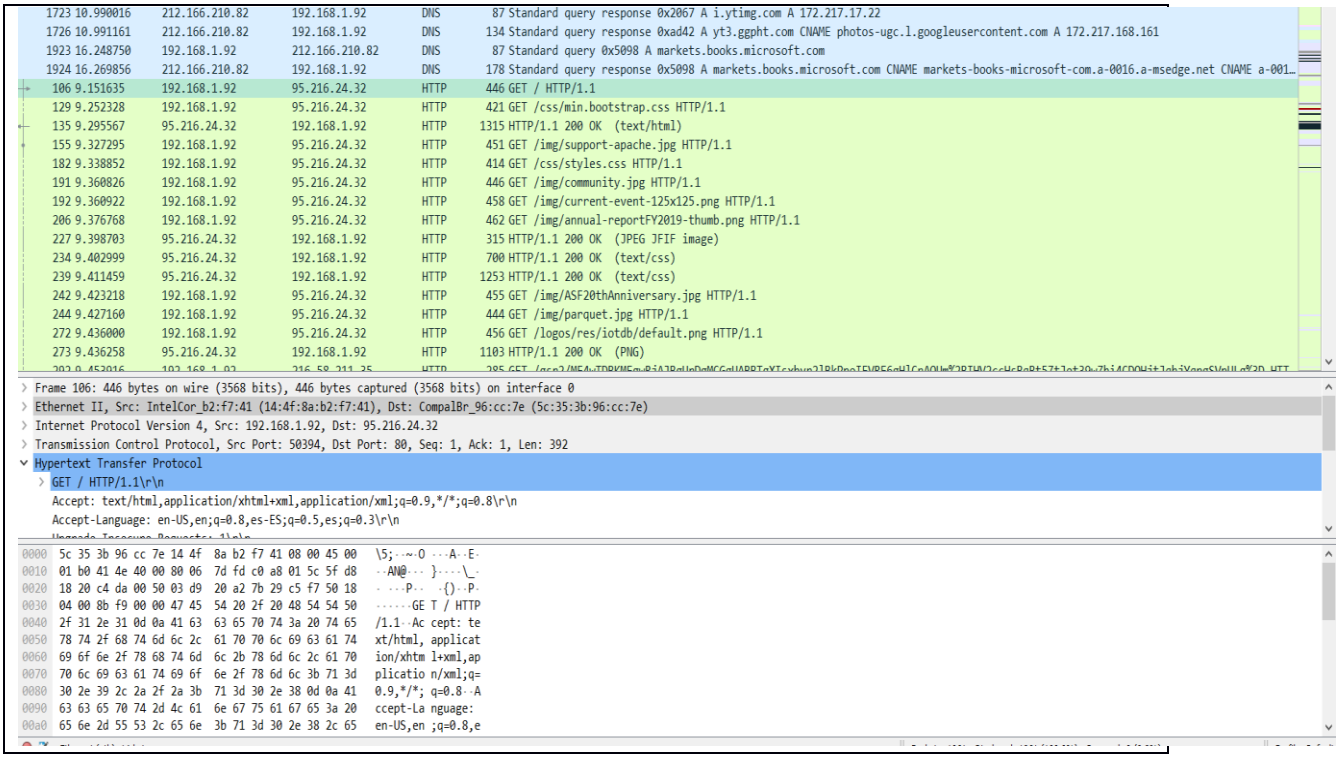
Nota: Desactivar el modo promiscuous

Capture=> Interfaces=> **Start**.

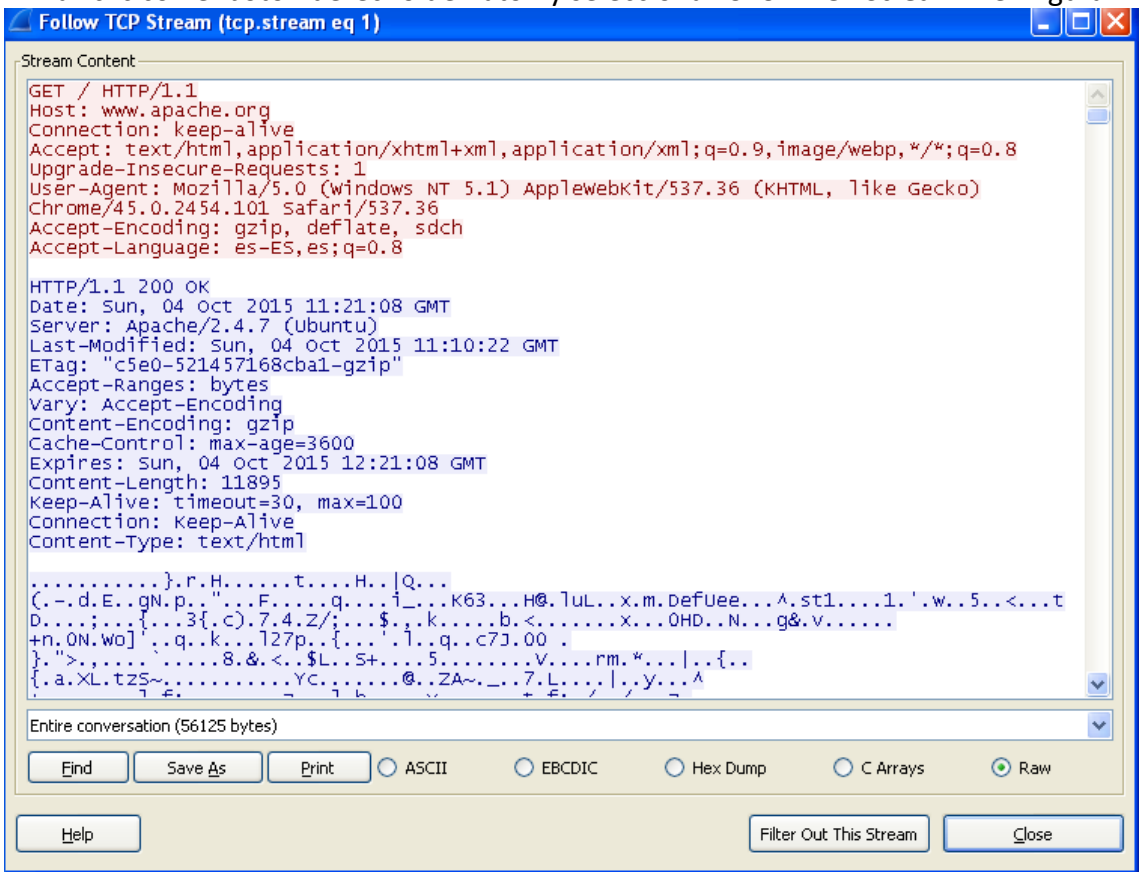
4. Desde el navegador establece una conexión a **http://www.apache.org/**.

5. Vuelve a Wireshark y para la captura (Capture, **Stop**).

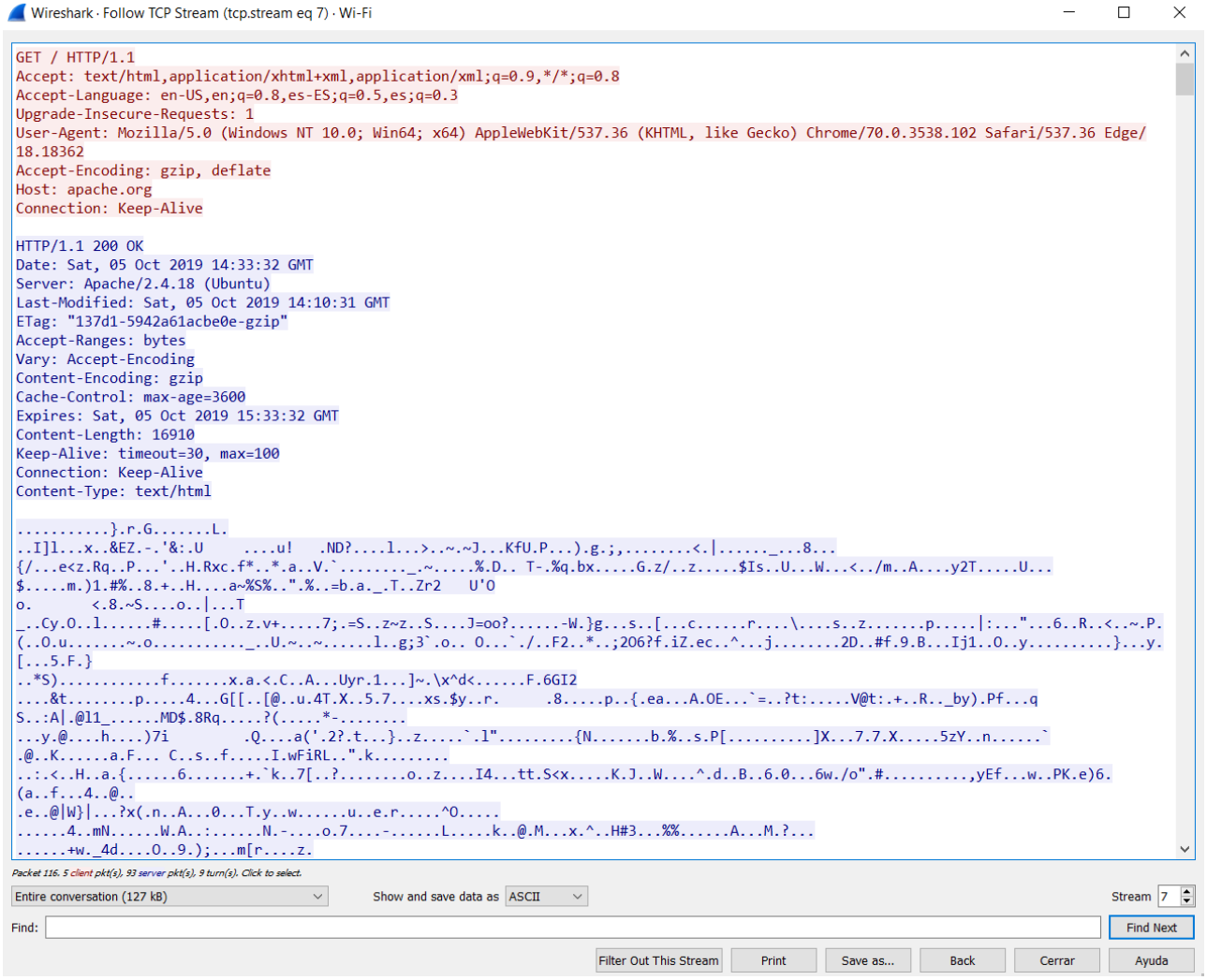
6. Buscar una trama HTTP en donde la petición sea **GET / HTTP/1.1**, e incluye el pantallazo en la práctica.



7. Haz clic con el botón derecho del ratón y selecciona **Follow TCP Stream**. Ver Figura



Incluye en la práctica tu pantallazo



8. Responde a las siguientes preguntas:

8.1. ¿Cuál es la IP de la máquina donde se ejecuta el servidor Web?

95.216.24.32

8.2. ¿Qué versión de HTTP se utiliza?

La 1.1

8.3. ¿Qué método de petición se utiliza?

Get

8.4. ¿Qué recurso se solicita al servidor?

La raíz, pero buscara el index de apache.org

8.5. ¿Qué valor tiene la cabecera Host?

www.apache.org

8.6. ¿Se envían cookies en la petición HTTP?

No por ser la primera vez que entramos

8.7. ¿Qué lenguaje utiliza el navegador?

Html, xhtml+xml

8.8. ¿Qué código de estado tiene la respuesta HTTP?

200 ok

8.9. ¿Qué servidor Web y versión se utiliza?

Apache/2.4.18 (Ubuntu)

8.10. ¿De qué tipo MIME es el recurso recibido?

text/html

8.11. ¿Se han utilizado conexiones persistentes, es decir, en la misma conexión TCP hay varias peticiones y respuestas HTTP? ¿Qué significa Keep alive?

El protocolo Keep alive permite que el la conexión entre cliente y servidor este abierta por lo que puede pedir todo lo que necesite (lo del html), el cliente lo solicita y el servidor lo acepta o no.

8.12. ¿Existen peticiones y respuestas de imágenes? Obtener pantallazo

Si de 2 imágenes y unos logos

```
`.......GET /img/ASF20thAnniversary.jpg HTTP/1.1
Referer: http://apache.org/
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.8,es-ES;q=0.5,es;q=0.3
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
70.0.3538.102 Safari/537.36 Edge/18.18362
Host: apache.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sat, 05 Oct 2019 14:33:32 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Tue, 26 Mar 2019 05:45:48 GMT
ETag: "11a32-584f8d54464b3"
Accept-Ranges: bytes
Content-Length: 72242
Cache-Control: max-age=3600
Expires: Sat, 05 Oct 2019 15:33:32 GMT
Keep-Alive: timeout=30, max=98
Connection: Keep-Alive
Content-Type: image/jpeg

......JFIF.....H.H.....@Exif..MM.*.......i.....................................................8Photoshop
3.0.8BIM........8BIM.%.....................      ...B~.....................................................
```

8.13.- Lanza de nuevo una captura de red con wireshark. ¿Qué observas al hacer una petición a www.google.es? ¿Qué protocolo se está utilizando a nivel de aplicación? ¿Qué diferencias observas con la petición anterior?

9.- CONCLUSIONES: Se trata de realizar el seguimiento de las tramas que pertenecen a una determinada petición HTTP, introduciendo una URL determinada desde el navegador y haciendo el seguimiento de todos los protocolos implicados que posibilitan esa "conversación" (conjunto de peticiones/respuestas) entre los equipos origen y destino, en concreto el envío de mensaje de petición HTTP del navegador al servidor y la respuesta de éste al cliente que inició la comunicación.

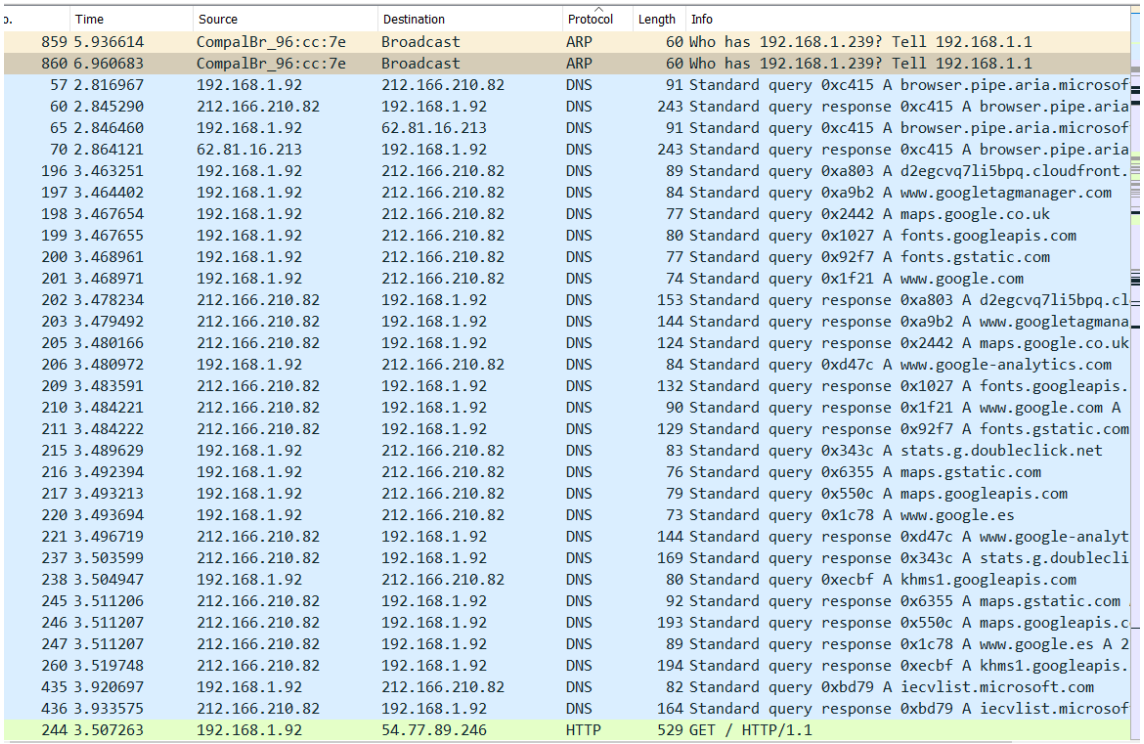
Se pide:

Iniciar el analizador de red (wireshark) y lanzar una determinada petición http, esperar a que la página se haya cargado, parar la captura, guardar la captura y a continuación, explicar el proceso seguido y los protocolos intervinientes. Si no obtenemos lo esperado, utilizad los comandos apropiados para borrar de la caché las direcciones

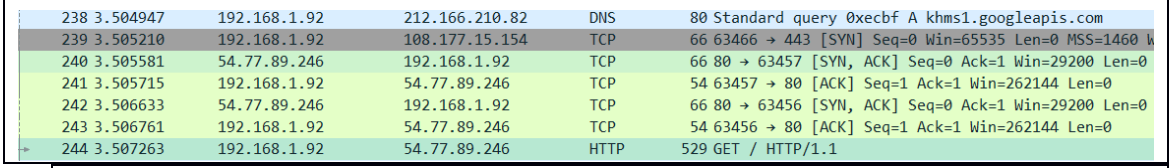
MAC asociadas a IPs, así como las IPs asociadas a los nombres de dominio correspondientes (URL).

9.1.- CONCLUSIONES:

Realizaremos el seguimiento de las tramas, similar a lo anteriormente que hicimos, primero iniciamos la captura de wireshark, con lo que primero que veremos el el protocolo ARP buscando la dirección red y luego obteniendo la mac del router, luego pediremos una pagina web en el navegador, por lo que en la captura lo primero que veremos será al DNS cambiando la url por la dirección IP, una vez que nos responda estableceremos una conexión entre el cliente y servidor (sync, sync ack,ack), una vez hecho esto se realiza el protocolo HTTP get \ 1.1 y dependiendo de este nos responderá con un código 200 en el caso de que sea correcto, a partir de ahí si el cliente necesita mas recursos de la pagina lo conseguira porque estarán en keep alive.



No.	Time	Source	Destination	Protocol	Length	Info
859	5.936614	CompalBr_96:cc:7e	Broadcast	ARP	60	Who has 192.168.1.239? Tell 192.168.1.1
860	6.960683	CompalBr_96:cc:7e	Broadcast	ARP	60	Who has 192.168.1.239? Tell 192.168.1.1
57	2.816967	192.168.1.92	212.166.210.82	DNS	91	Standard query 0xc415 A browser.pipe.aria.microsof
60	2.845290	212.166.210.82	192.168.1.92	DNS	243	Standard query response 0xc415 A browser.pipe.aria
65	2.846460	192.168.1.92	62.81.16.213	DNS	91	Standard query 0xc415 A browser.pipe.aria.microsof
70	2.864121	62.81.16.213	192.168.1.92	DNS	243	Standard query response 0xc415 A browser.pipe.aria
196	3.463251	192.168.1.92	212.166.210.82	DNS	89	Standard query 0xa803 A d2egcvq7li5bpq.cloudfront.
197	3.464402	192.168.1.92	212.166.210.82	DNS	84	Standard query 0xa9b2 A www.googletagmanager.com
198	3.467654	192.168.1.92	212.166.210.82	DNS	77	Standard query 0x2442 A maps.google.co.uk
199	3.467655	192.168.1.92	212.166.210.82	DNS	80	Standard query 0x1027 A fonts.googleapis.com
200	3.468961	192.168.1.92	212.166.210.82	DNS	77	Standard query 0x92f7 A fonts.gstatic.com
201	3.468971	192.168.1.92	212.166.210.82	DNS	74	Standard query 0x1f21 A www.google.com
202	3.478234	212.166.210.82	192.168.1.92	DNS	153	Standard query response 0xa803 A d2egcvq7li5bpq.cl
203	3.479492	212.166.210.82	192.168.1.92	DNS	144	Standard query response 0xa9b2 A www.googletagmana
205	3.480166	212.166.210.82	192.168.1.92	DNS	124	Standard query response 0x2442 A maps.google.co.uk
206	3.480972	192.168.1.92	212.166.210.82	DNS	84	Standard query 0xd47c A www.google-analytics.com
209	3.483591	212.166.210.82	192.168.1.92	DNS	132	Standard query response 0x1027 A fonts.googleapis.
210	3.484221	212.166.210.82	192.168.1.92	DNS	90	Standard query response 0x1f21 A www.google.com A
211	3.484222	212.166.210.82	192.168.1.92	DNS	129	Standard query response 0x92f7 A fonts.gstatic.com
215	3.489629	192.168.1.92	212.166.210.82	DNS	83	Standard query 0x343c A stats.g.doubleclick.net
216	3.492394	192.168.1.92	212.166.210.82	DNS	76	Standard query 0x6355 A maps.gstatic.com
217	3.493213	192.168.1.92	212.166.210.82	DNS	79	Standard query 0x550c A maps.googleapis.com
220	3.493694	192.168.1.92	212.166.210.82	DNS	73	Standard query 0x1c78 A www.google.es
221	3.496719	212.166.210.82	192.168.1.92	DNS	144	Standard query response 0xd47c A www.google-analyt
237	3.503599	212.166.210.82	192.168.1.92	DNS	169	Standard query response 0x343c A stats.g.doublecli
238	3.504947	192.168.1.92	212.166.210.82	DNS	80	Standard query 0xecbf A khms1.googleapis.com
245	3.511206	212.166.210.82	192.168.1.92	DNS	92	Standard query response 0x6355 A maps.gstatic.com
246	3.511207	212.166.210.82	192.168.1.92	DNS	193	Standard query response 0x550c A maps.googleapis.c
247	3.511207	212.166.210.82	192.168.1.92	DNS	89	Standard query response 0x1c78 A www.google.es A 2
260	3.519748	212.166.210.82	192.168.1.92	DNS	194	Standard query response 0xecbf A khms1.googleapis.
435	3.920697	192.168.1.92	212.166.210.82	DNS	82	Standard query 0xbd79 A iecvlist.microsoft.com
436	3.933575	212.166.210.82	192.168.1.92	DNS	164	Standard query response 0xbd79 A iecvlist.microsof
244	3.507263	192.168.1.92	54.77.89.246	HTTP	529	GET / HTTP/1.1



No.	Time	Source	Destination	Protocol	Length	Info
238	3.504947	192.168.1.92	212.166.210.82	DNS	80	Standard query 0xecbf A khms1.googleapis.com
239	3.505210	192.168.1.92	108.177.15.154	TCP	66	63466 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W
240	3.505581	54.77.89.246	192.168.1.92	TCP	66	80 → 63457 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
241	3.505715	192.168.1.92	54.77.89.246	TCP	54	63457 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
242	3.506633	54.77.89.246	192.168.1.92	TCP	66	80 → 63456 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
243	3.506761	192.168.1.92	54.77.89.246	TCP	54	63456 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
244	3.507263	192.168.1.92	54.77.89.246	HTTP	529	GET / HTTP/1.1

- Podemos ver que primero se hace un ARP para buscar las direcciones mac físicas, luego con la salida (router) hace una petición DNS para pasar del url http:// www.chinokaiyue.es/ a su dirección ip publica una vez obtenida, entonces empieza el protocolo TCP a establecer una comunicación entre cliente y servidor con el protocolo de 3 pasos, y finalmente hacemos la petición HTTP get de la pagina web.

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.8,es-ES;q=0.5,es;q=0.3
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362
Accept-Encoding: gzip, deflate
Host: www.chinokaiyue.es
Connection: Keep-Alive
Cookie: _gid=GA1.2.1069125237.1570809601; _ga=GA1.2.1628648008.1570809601

HTTP/1.1 200 OK
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 11 Oct 2019 16:05:45 GMT
Server: nginx
X-Cache-Status: HIT
X-Frame-Options: DENY
Content-Length: 10762
Connection: keep-alive

...........}[s.7...?U.;`.....D.b.....e;v";*K.7'.rA...<..13R...a...}H......n.
....e%.............@........t..
....Y7.a......PpoW?vG"..?.*.q.......-3).#.k.Kq1.U.b.0.E.Y/...{.8.}...Ve
c.....}..X._.(.e...I$.~.'.....|..eC%N{+.8.G.;.S.L......|,.v?.u.Q..).I...L...?
r/.......W......I.......
S...D../....
./....._c,l%k..>.m.y[i.Z...D4..H..N.(...N<.#.......{......6.w6.V.2.....
\..y.g.D..Dq....K.S".....8..;...}H
.n'}..!...x...^..k?.....1.%.....Oz......o...D.Wr..00....3..s......d#..*...,N.Xx...
%........X.>.x..:&..U8.*.....C]..C.@.i......1Zs!N".C...r...J.`..
[{.b.?.w...'.w...&...^o."..........J...x.......kX.7....3.+.*.\..M..9........ .$....\\
\..E.[./...V...........).c..        {.K.c).2.u.......
.y6D.CO.!":.:.J..i..Y...v....]...|dh..<.
{-......R.o...O..Y..<.em-.r1..4..0....I.Ws:.L0.:....0X...uc.
.V:..t.v~]..e
...z.$...p.(..$u(m]..Q.......S.I.9>..^+..o.p..s:9`I..^+Q@..........z.^..
+...Y.......*;NV.k...U.T..#..%lc.F........f.<g......G...d.....6.2.`..Y2..z..
8..5...0.%.u'`..S.O`....Z.@{..{-.....jQ....J..E...o.. ..7_.x(U=k...+.......
4.0.,..:S.....9.YA.8.m^..J@.0#t./w.<.8.??    ...J.n.<._9.I.........../O/
```

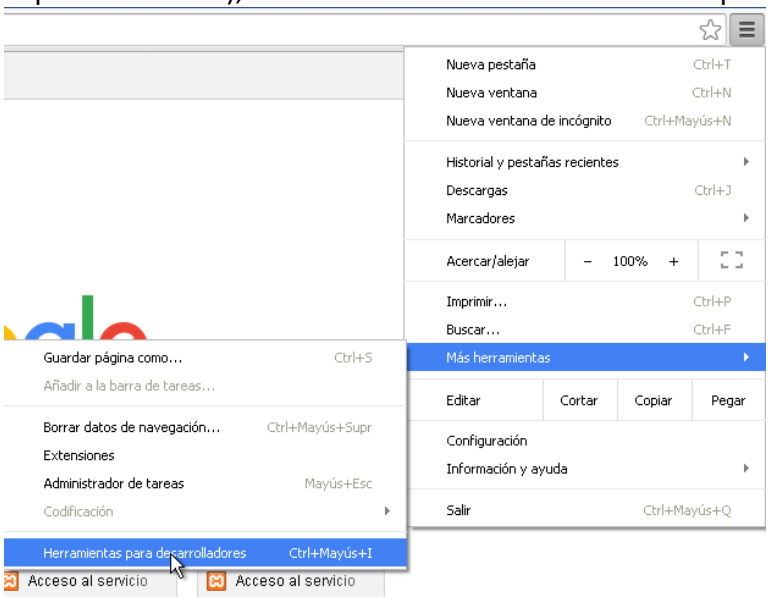
-podemos ver que hacemos una petición get y el servidor nos responde con un “200 OK” confirmando que es correcto y manteniendo la conexión keep-alive, a continuación si necesita algo mas se lo pedirá y este (servidor) nos lo facilitara.

9.2.- Comandos:

Arp -a
Arp -d
Ipconfig /displaydns
Ipconfig /flushdns

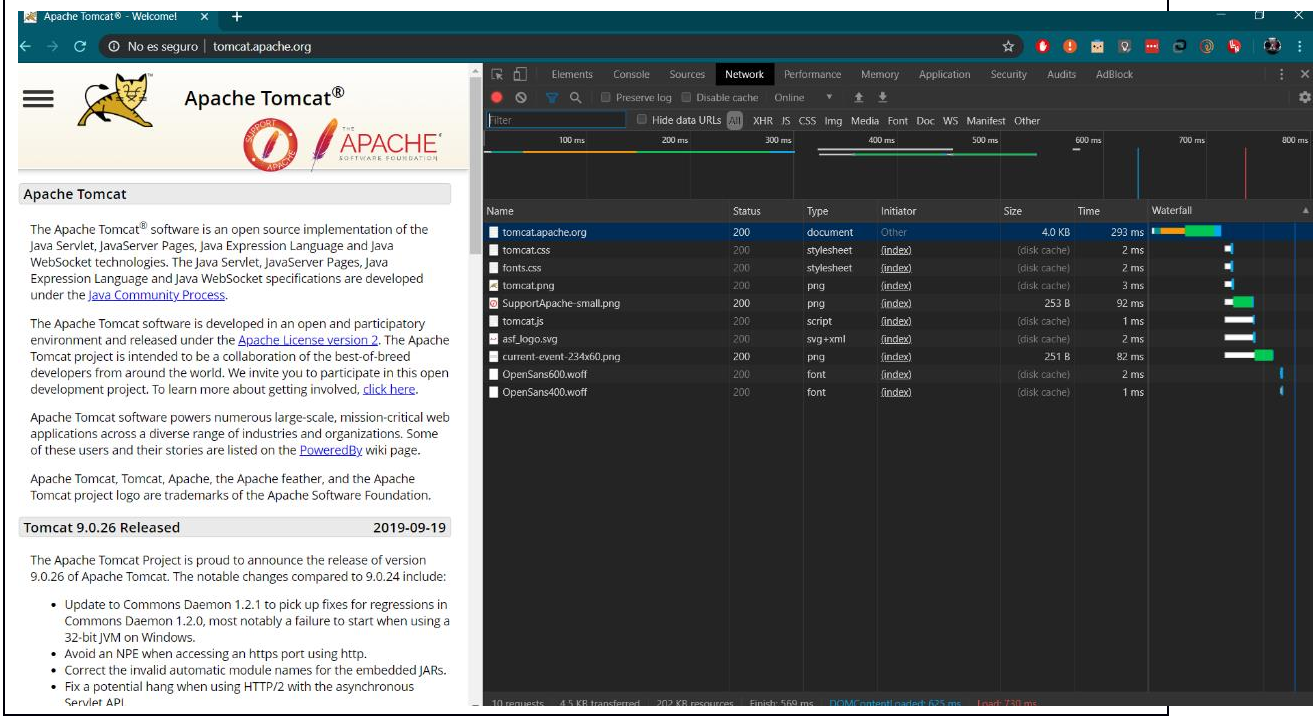
Inicamos la captura en el wireshark
Accedemos en el navegador a http://www.apache.org/
Detenemos la captura
Buscamos la petición GET y filtramos para ver su recorrido

10. Accede a las opciones de configuración de Google Chrome (cuadrado en la parte superior derecha), Más Herramientas => Herramientas para desarrolladores.



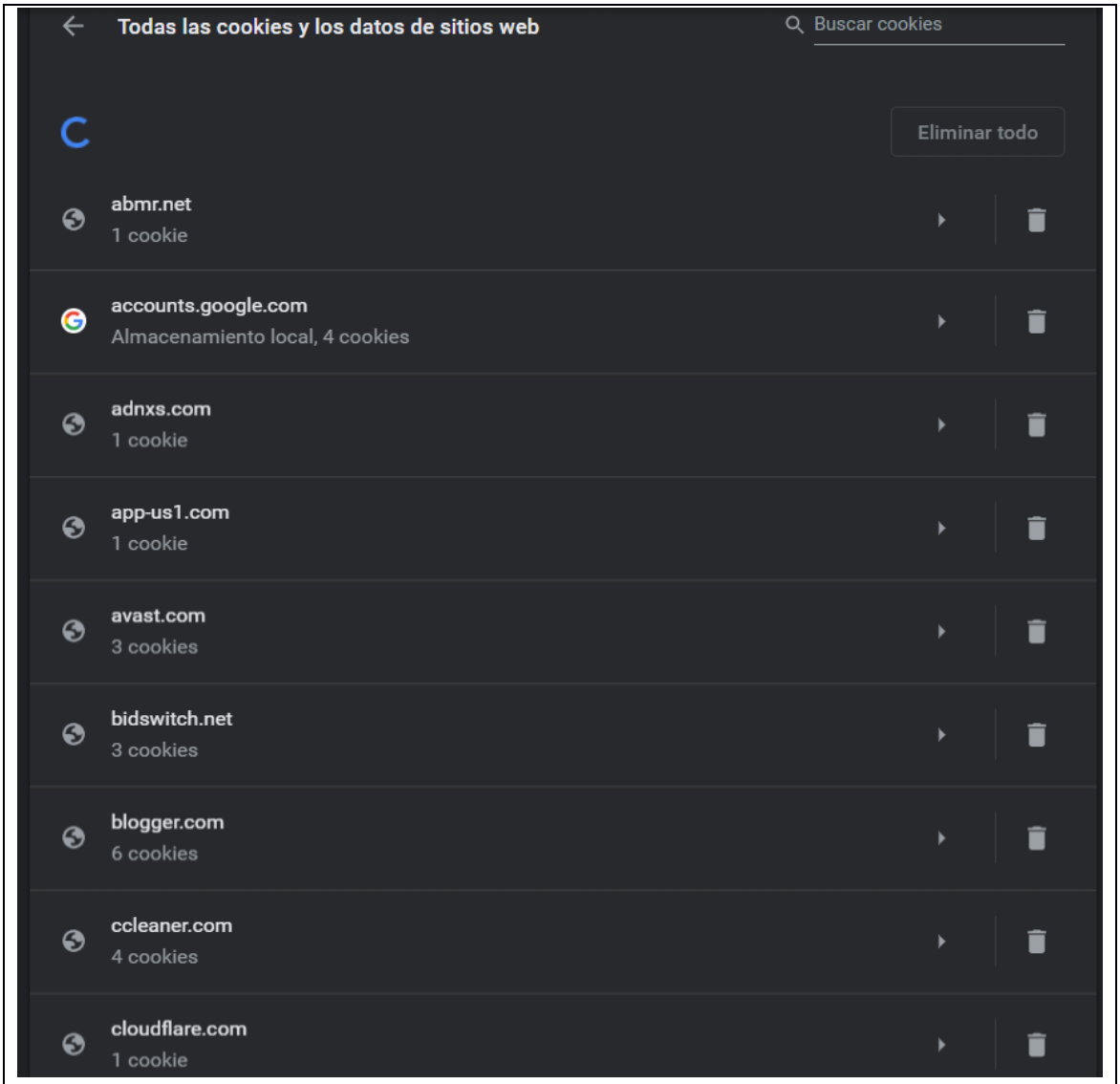
Accede a http://tomcat.apache.org/ y analiza las peticiones y respuestas HTTP, qué métodos usan, los códigos de respuesta, los recursos que envía el servidor. Obtén el pantallazo.

Usan el método get , los codigos de respuesta son 200 (correcto) y los recursos son todas las imágenes, logos, javascript y css.



11. Accede a las opciones de configuración de Google Chrome (cuadrado en la parte superior derecha), Configuración => Mostrar Configuración Avanzada => Configuración de contenido => Todas las cookies y los datos de sitios.
Observa las cookies que tiene almacenadas el navegador. Obtén Pantallazo.

Elimina todas las cookies.



Aquí podemos ver algunas de las cookies que almacena el ordenador de las diferentes paginas que visitamos, las usa para cuando hacemos una petición verificar si ya tenemos ciertos datos y no tener que descargarlos otra vez.

Borramos las cookies en historial-> eliminar cookies

Y con esto borraremos todos los datos que almacenan las paginas web de nosotros