

Pràctica 1: Protocol HTTP

Introducció

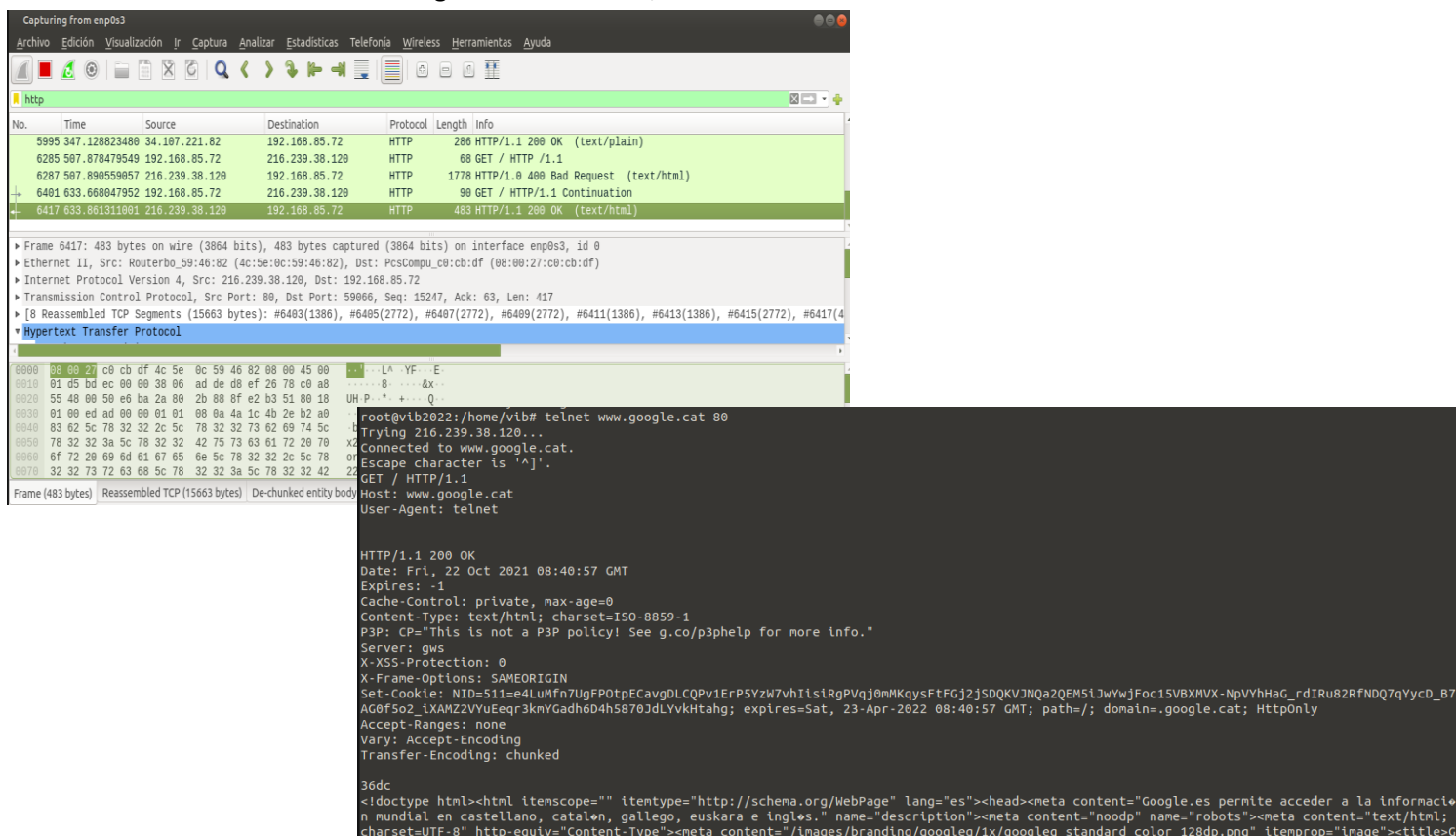
L'objectiu d'aquesta pràctica és l'estudi del funcionament del protocol petició-resposta HTTP. S'han de tenir clars els elements principals que intervenen en les comunicacions web i els protocols TCP/IP i HTTP)

B) Peticions i respostes HTTP treballant amb Telnet i Wireshark (45 %)

1. Filtra el contingut de les captures de manera que només es mostrin els continguts dels missatges HTTP. Fes la següent petició HTTP utilitzant: **telnet www.google.cat 80**

```
GET / HTTP/1.1
Host: www.google.cat
User-Agent: telnet
```

Mostra el resultat obtingut amb Wireshark, i troba:



- a) Dins de la capçalera IP, l'adreça IP del teu ordinador i la del servidor.
Propia: 192.168.85.72
Servidor: 216.239.38.120
- b) El port (tipus i valor) utilitzat pel programa telnet i pel servidor web
80
- c) Quin codi de resposta dóna la capçalera HTTP enviada pel servidor? Què significa?
200 OK (significa que està correcte)

- d) En el cas d'obtenir una capçalera *Location* a la resposta del servidor, explica el seu significat.
- e) Que indica la capçalera *Server* de la resposta donada pel servidor? Explica el resultat que has obtingut.
gsw--
- f) Que indica la capçalera *Content-Type* de la resposta donada pel servidor? Explica el resultat que has obtingut.
Content – Type Text/Html (Que el contingut era de tipo text i de html)
- g) Que hi ha al cos del missatge de la resposta donada pel servidor?. El servidor t'ha tornat la pàgina web inicial? Què t'ha tornat?.
El codi html de la pàgina www.google.cat
- h) Comprova si la connexió es tanca immediatament després de rebre la resposta del servidor. Hi ha alguna manera de tancar la connexió?

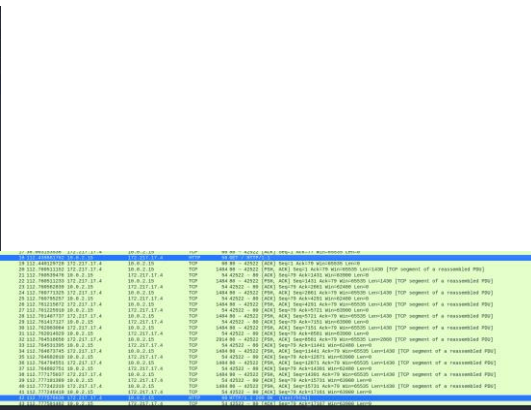
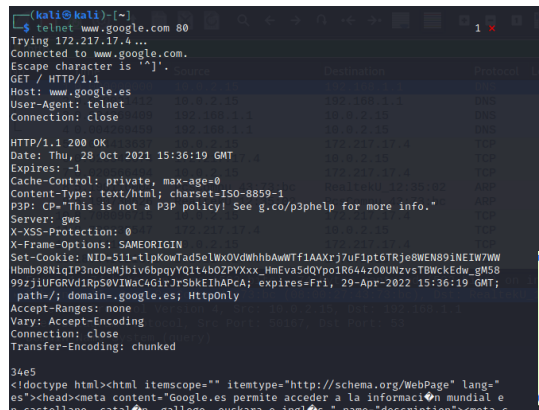
Si es tanca, però també hi ha una opció que es “connection: close”

```
vC4JOHnI\x22,\x22uhde\x22:false}}';gc
</body></html>
0
Connection closed by foreign host.
```

2. Fes la següent petició HTTP utilitzant: **telnet www.google.com 80**

```
GET / HTTP/1.1
Host: www.google.es
User-Agent: telnet
Connection: close
```

Mostra el resultat obtingut amb wireshark, i respon a les següents preguntes:

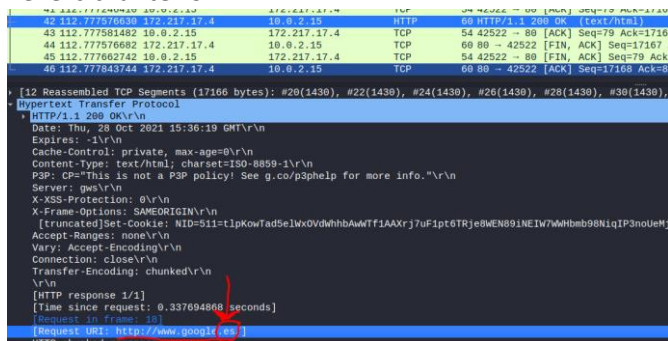


a) Per què serveix la capçalera **Connection: close**? Què passa al executar la petició amb **Connection:close** a diferència de l'exercici anterior?

Basicamente sive para que el servidor cierre la conexión despues de enviar ese message

Que la conexi3n se pierde. Que directamente la petici3n se cierra

b) Fixa't que a la petici3n el **Host** ara és **www.google.es**. Aix3 ha fet que la resposta sigui diferent? Per què? Mostra la resposta i comenta el resultat obtingut i les diferències amb l'exercici anterior.



Aixo no s'altera, ja que es com tindre un subdomini i el agafa igualment

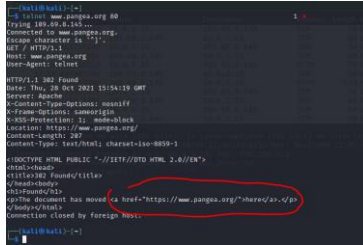
c) Què significat pel navegador que el **Expires** valgui -1 i que el camp **max-age** de **Cache-Control** sigui igual a 0?

El Expires es per s'hago de descarregar tota la informaci3n cada vegada que es recarregui la pagina web

3. Amb l'eina telnet connectat a la web **www.pangea.org**. Amb wireshark comprova:

- a) Quina reposta dóna el servidor. Indica el significat de la reposta.
302 Found l'arxiu sol·licitat ha canviat de lloc.

- b) Indica quina és la nova adreça del servidor i quin camp de la capçalera dóna la nova URL

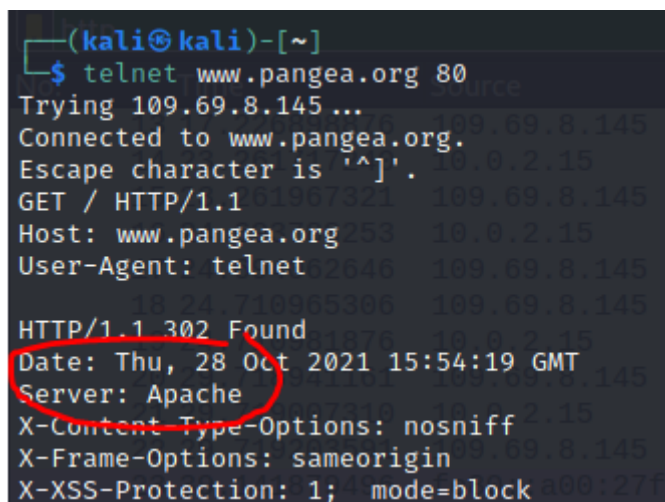


```
~(kali@kali):~$ telnet www.pangea.org 80
Trying 109.69.8.145...
Connected to www.pangea.org.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.pangea.org
User-Agent: telnet

HTTP/1.1 302 Found
Date: Thu, 28 Oct 2021 15:54:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Frame-Options: sameorigin
X-XSS-Protection: 1; mode=block
Location: https://www.pangea.org/home/4/pa/
Content-Type: text/html; charset=iso-8859-1
Content-Length: 209

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<title>302 Found</title>
<head>
<meta charset="utf-8" />
</head>
<body>
<p>The document has moved <a href="https://www.pangea.org/home/4/pa/">here</a>.
</p>
</body>
</html>
Connection closed by foreign host.
```

- c) Indica el programa servidor de pàgines web utilitzat per pangea.org.



```
~(kali@kali)-[~]$ telnet www.pangea.org 80
Trying 109.69.8.145...
Connected to www.pangea.org.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.pangea.org
User-Agent: telnet

HTTP/1.1 302 Found
Date: Thu, 28 Oct 2021 15:54:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Frame-Options: sameorigin
X-XSS-Protection: 1; mode=block
```

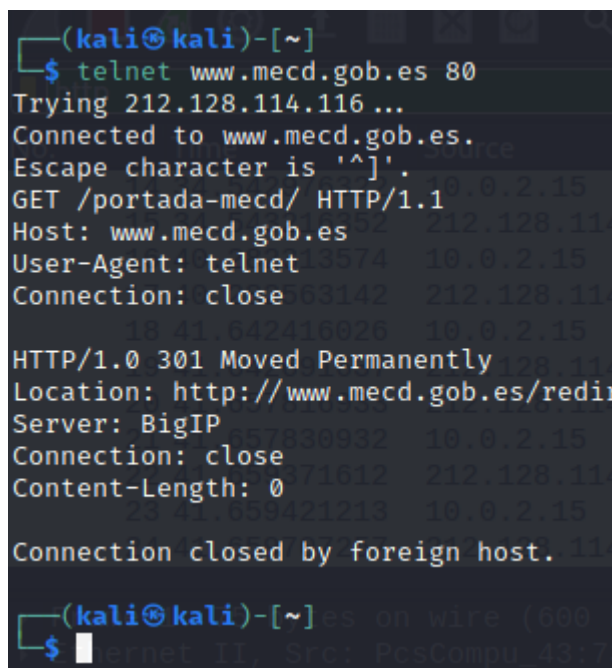
4. Com ja sabeu els navegadors tenen memòria cau per agilitzar les peticions dels recursos web. Aquesta gestió de la memòria cau (*cache*) es fa gràcies a la informació de les capçaleres HTTP. Cada objecte de la memòria cau està identificat i també marcat amb la data d'obtenció. Connectat per *telnet* al servidor **www.mecd.gob.es** al port **80** i realitza la següent petició:

```
GET /portada-mecd/ HTTP/1.1
Host: www.mecd.gob.es
User-Agent: telnet
Connection: close
```

Hauries d'obtenir una resposta amb una capçalera HTTP semblant a aquesta:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Magnolia-Registration: Registered
Pragma:
Cache-Control: max-age=600, public
Expires: Sat, 17 Sep 2016 15:08:28 GMT
Last-Modified: Sat, 17 Sep 2016 14:03:11 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 376769
Date: Sat, 17 Sep 2016 14:58:28 GMT
Connection: close
Set-Cookie: BIGipServerpool_web=1124081580.36895.0000; path=/
```

(Nota: Les dates i hores poden canviar en funció del moment de realització de la pràctica)



```
(kali@kali)-[~]
$ telnet www.mecd.gob.es 80
Trying 212.128.114.116 ...
Connected to www.mecd.gob.es.
Escape character is '^]'.
GET /portada-mecd/ HTTP/1.1
Host: www.mecd.gob.es
User-Agent: telnet
Connection: close
HTTP/1.0 301 Moved Permanently
Location: http://www.mecd.gob.es/redir...
Server: BigIP
Connection: close
Content-Length: 0
Connection closed by foreign host.
```

Ja que la pagina web esta fora de servei explicare com si funcionés

- Realitza un connexió i mostra la informació de la capçalera obtinguda. Quina informació dona la capçalera *Last-Modified* de la resposta? Veus alguna utilitat en saber aquesta informació?
Mostraria la data de connexió. Sí, ja que així podries validar i comprobar cada quant es connecta i la data de expiració
- A partir de quina data la validesa del recurs expira? Què significa això?
A partir de la sessió, quant expira es quant es recarga i alla esperd.
- Aquest apartat s'ha de fer immediatament després de l'anterior petició per poder observar el resultat desitjat. Torna a fer la mateixa petició però utilitzant una capçalera addicional (*IfModified-Since*), el valor ha de ser la data de la darrera modificació que es troba a la resposta anterior (**a partir dels valors de la teva execució i no utilitzant els valors de l'exemple**).

```
GET /portada-mecd/ HTTP/1.1
Host: www.mecd.gob.es
User-Agent: telnet
If-Modified-Since: Mon, 05 Oct 2015 11:07:46 GMT
Connection: close
```

Quin codi de resposta has obtingut? Explica el significat del codi i raona el motiu pel qual obtens aquest codi a partir d'explicar el funcionament de les capçaleres utilitzades.

Basicament el protocol *IfModified-Since* permet que si el protocolo no se ha cambiado, pos envía una petición 303, es decir, sin cambio pero sin recarga otra vez del servidor.

- d) Torna a fer la mateixa petició però utilitzant el valor de la capçalera addicional *If-Modified-Since igual a Mon, 05 Oct 2015 09:07:46 GMT* (o sigui, dues hores abans). Comprova ara si el servidor torna la pàgina web senceera i també el codi de resposta obtingut.

Envia una petición 303, es decir, no se actualiza y se rearga de cache.

5. **Analitza la següent “conversa” HTTP entre un client i un servidor i descriu allò que està passant:**

```
GET /private/index2.html HTTP/1.1
Host: localhost
```

```
HTTP/1.1 401 Authorization Required
Server: HTTPd/1.0
Date: Sat, 27 Nov 2006 10:18:15 GMT
WWW-Authenticate: Basic realm="Secure Area"
Content-Type: text/html
Content-Length: 311
```

```
GET /private/index2.html HTTP/1.1
Host: localhost
Authorization: Basic QWxhZGRpbjpvGVulHNlc2FtZQ==
```

```
HTTP/1.1 200 OK
Server: HTTPd/1.0
Date: Sat, 27 Nov 2006 10:19:07 GMT
Content-Type: text/html
Content-Length: 10476
```

Primero se pide una petición de usuario a servidor de localhost(local), en el archivo *privateindex2.html*

El servidor(que es si mismo pero funciona como servidor),envia una respuesta de que se necesita autenticación, y allá se muestra la hora de connexion.

Despues el usuario envia la clave para conectarse encriptada para el servidor especificando el mismo archivo

Y finalmente el servidor envia el archivo y mostranto tambien la hora de conexión, el formato de contenido, la longitud y el tipo de servidor.