Pràctica 1: Protocol HTTP

**Introducció**

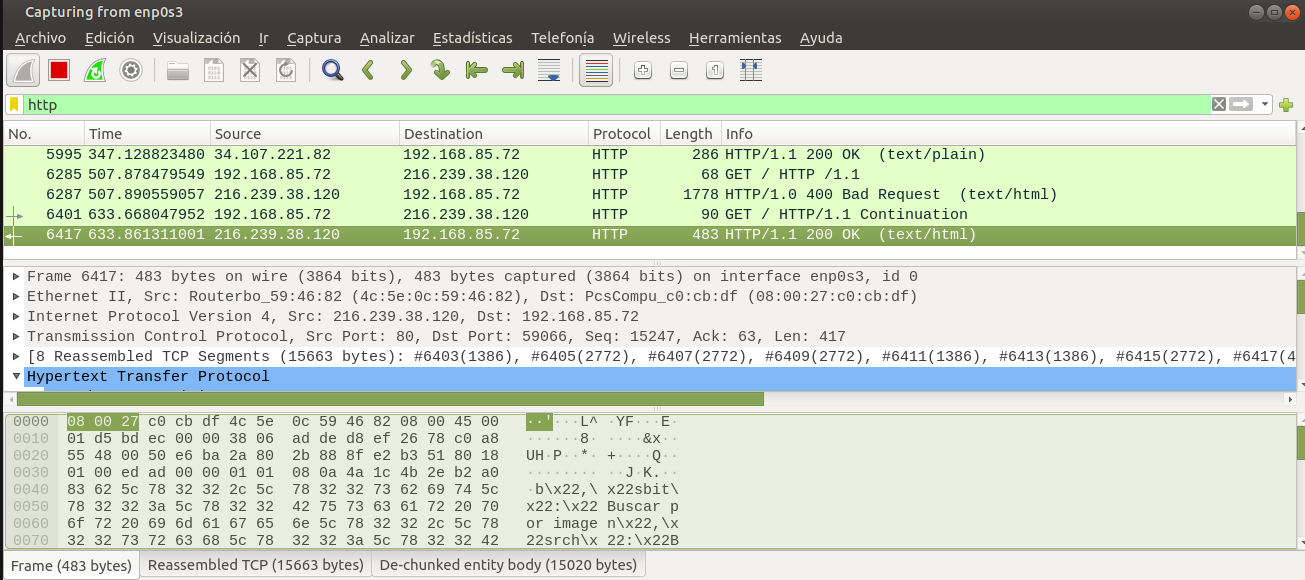
L'objectiu d'aquesta pràctica és l'estudi del funcionament del protocol petició-resposta HTTP. S'han de tenir clars els elements principals que intervenen en les comunicacions web i els protocols TCP/IP i HTTP)

# 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***



Mostra el resultat obtingut amb wireshark, i troba:



* 1. 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

* 1. El port (tipus i valor) utilitzat pel programa telnet i pel servidor web

80

* 1. Quin codi de resposta dóna la capçalera HTTP enviada pel servidor? Què significa?

200 OK (significa que esta correcte)

* 1. En el cas d'obtenir una capçalera *Location* a la resposta del servidor, explica el seu significat.
  2. Que indica la capçalera *Server* de la resposta donada pel servidor? Explica el resultat que has obtingut.

gsw--

* 1. Que indica la capçalera *Content-Type* de la resposta donada pel servidor? Explica el resultat que has obtingut.

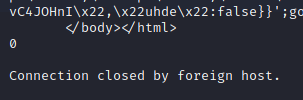
Content – Type Text/Html (Que el contingut era de tipo text i de html)

* 1. Que hi ha al cos del missatge de la resposta donada pel servidor?. El servidor t'ha tornat lapàgina web inicial? Què t'ha tornat?.

El codi html de la pàgina www.google.cat

* 1. Comprova si la connexió es tanca inmediatament després de rebre la resposta del servidor. Hi ha alguna manera de tancar la connexió?

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

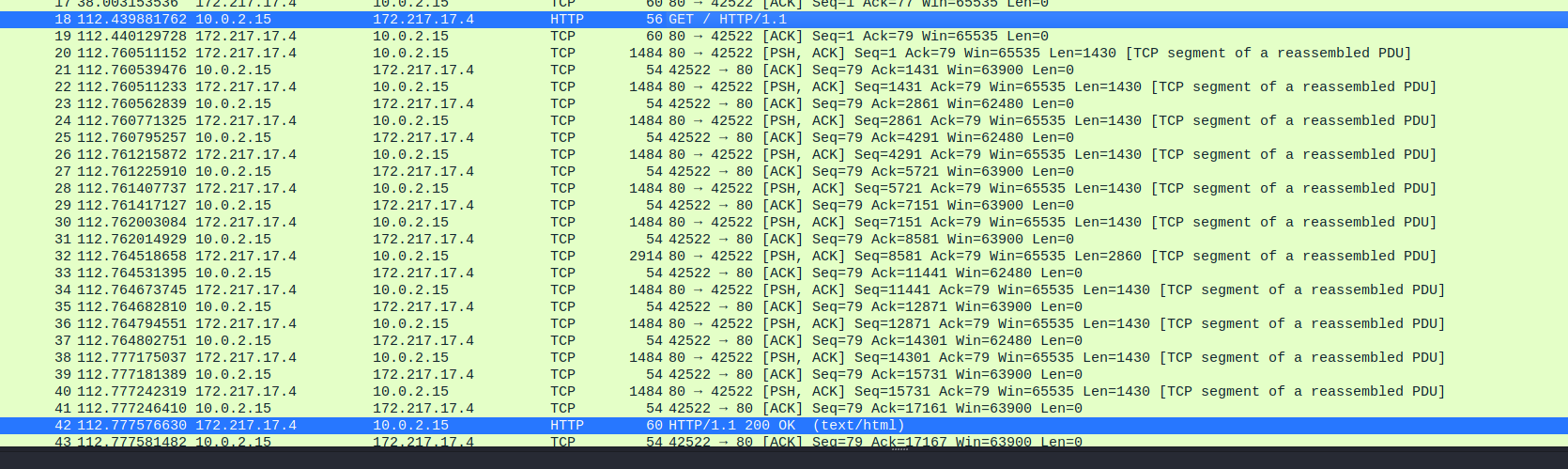
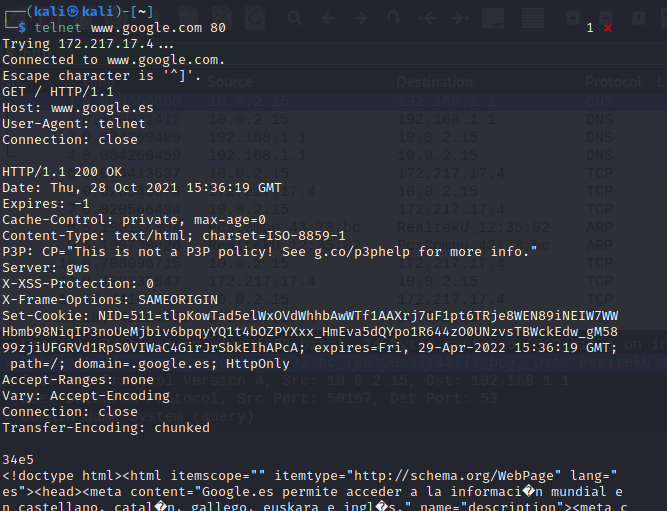


1. Fes la següent petició HTTP utilitzant: ***telnet www.google.com 80***

Forma

Descripción generada automáticamente con confianza media

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

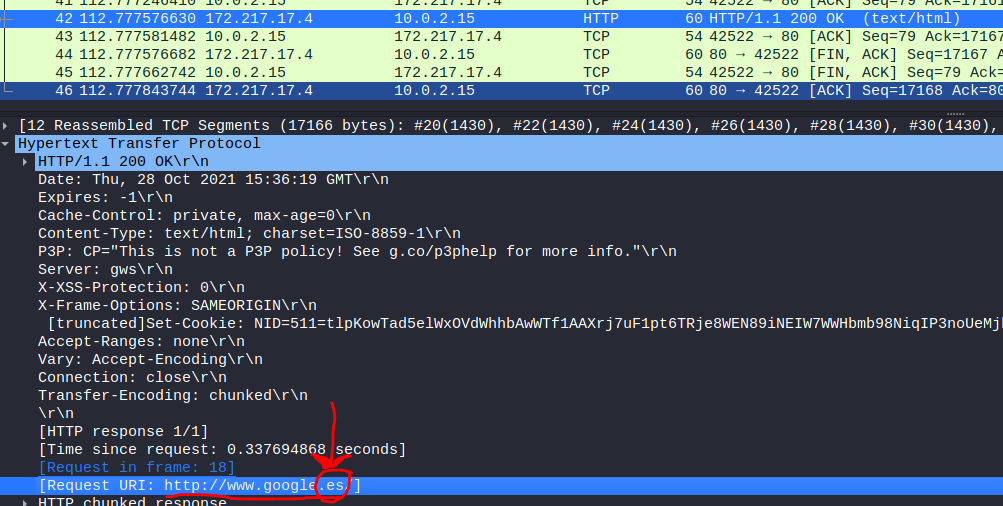


* 1. Per què serveix la capçalera *Connection: close*? Què passa al executar la petició amb *Connection:close* a diferència de l'exercici anterior?

Bascicamente sive para que el servidor cierre la conexión despues de envar ese mensage

Que la conexión se pierde. Que directamente la petición se cierra

* 1. Fixa't que a la petició el *Host* ara és [www.google.es.](http://www.google.es/) Això 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

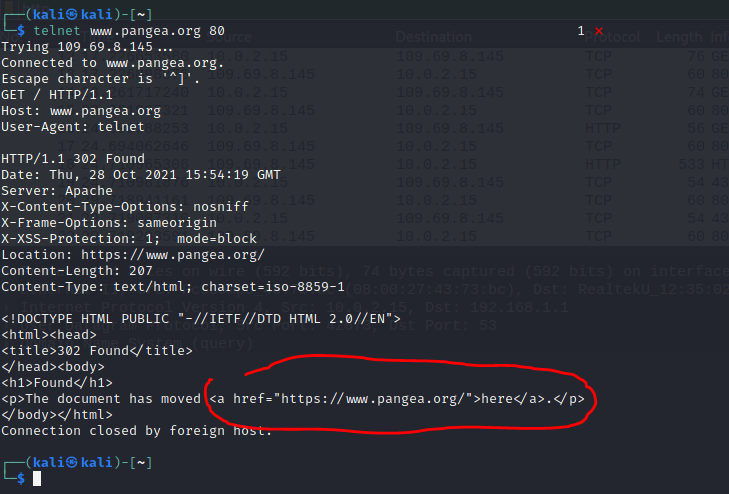
* 1. Què significat pel navegador que el Expires valgui -1 i que el camp max-age de Cache-Control sigui igual a 0?

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

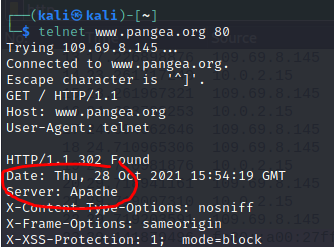
1. Amb l'eina telnet connectat a la web **www.pangea.org.** Amb wireshark comprova:
   1. Quina reposta dóna el servidor. Indica el significat de la reposta.

302 Found l’arxiu solicitat ha cambiat de lloc.

* 1. Indica quina és la nova adreça del servidor i quin camp de la capçalera dóna la nova URL



* 1. Indica el programa servidor de pàgines web utilitzat per pangea.org.



1. 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:

Forma

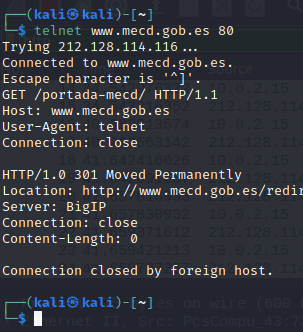
Descripción generada automáticamente con confianza media

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

Forma

Descripción generada automáticamente con confianza media

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



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

1. 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 aixi podries validar i comprobar cada cuant es conecta i la data de expiració

1. A partir de quina data la validesa del recurs expira? Què significa això?

Apartir de la sessió, cuant expira es cuant es recarga i alla esperd.

1. 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***).

Forma

Descripción generada automáticamente con confianza media

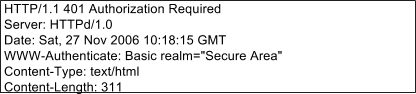
Quin codi de resposta has obtingut? Explica el significat del codi i raona el motiu pel qual obtens aquest codi a partir d'explicar el funcionament de les capçaleres utilitzades.

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

1. 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 peticio 303, es decir, no se acutaliza y se rearga de cache.

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



Forma

Descripción generada automáticamente con confianza media

Forma

Descripción generada automáticamente con confianza media

Primero se pide una peticion de usario a servidor de localhost(local), en el archivo *private*index2.html

El servidor(que es si mismo pero funciona como servidor),envia una respuesta de que se necesita autentificación, 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.