**Analitzadors de protocols**

Deixant de banda les possibilitats que ofereixen per a la pirateria informàtica, els analitzadors de protocols (també anomenats **sniffers**) poden ser útils per:

* Analitzar i resoldre problemes d'una xarxa
* Comprovar el funcionament del programari de comunicacions
* Conèixer el funcionament de les xarxes i els protocols de comunicació
* Desenvolupar i provar nous protocols

Un dels programes lliures més coneguts, útils i senzills d'utilitzar és el **Wireshark**.

Amb aquesta pràctica es pretén que conegueu algunes possibilitats d'aquest programa, però sobre tot l'estructura de les dades que viatgen per la xarxa.

***ANÀLISI DE TRAMES AMB WIRESHARK (6 punts)***

**ATENCIÓ:** si no es diu el contrari, quan es parla de capes, sempre es fa referència al model TCP/IP, no al model OSI

Obre amb Wireshark la captura de dades **google.pcapng**

Realitza els següents exercicis i contesta les preguntes en **color blau**.

* Analitza el protocol TCP
* Quines són les trames amb què s'estableix la connexió amb el servidor?

**7, 8 i 9**

* Quines són les trames amb què es tanca la connexió amb el servidor?

**71, 72, 73**

* Mira el “Acknowledgment number” de la trama 32. Què indica aquest número?

**19004 Indica el número de bytes enviats.**

* En la trama 32:
* Quins són els ports origen i destí?

**Src port: 49193 (Origen) Destination port: 80 (Destí)**

* A quin protocol correspon el port de destí?

**TCP**

* Per a què s’utilitza aquest protocol?

**Transmisió de hypertext**

* Analitza la trama nº 52
* Quins protocols utilitza a les capes 3 i 4?

**A la capa 3 hi ha UDP i a la capa 4 hi ha DNS**

* Què es demana en aquest missatge?

**Demana la IP de maps.google.es**

* Indica les IPs i els ports d'origen i de destí

**Src: 192.168.0.40, Dst: 192.168.0.1**

* Fes un esquema de la trama indicant el protocol i la mida de cada encapçalament

**Capa 1:Ethernat 14 bytes Capa 2:IP 20 bytes Capa 3:TCP, 20 bytes Capa 4: HTTP 587 bytes**

* En quina trama es troba la resposta a aquesta petició?

**Trama 56**

* Quina és la resposta?

**IP de maps.google.es**

* Analitza les trames que utilitzen el protocol HTTP
* En quina trama es fa la petició de la URL [**www.google.es**](http://www.google.es/)?

10

* Indica les IPs i els ports d'origen i de destí

Src: 192.168.0.40, Dst: 173.194.34.216

Src Port: 49193, Dst Port: 80

* Fes un esquema de la trama indicant el protocol i la mida de cada encapçalament

**Capa 1:Ethernat 14 bytes Capa 2:IP 20 bytes Capa 3:UDP, 8 bytes Capa 4: DNS 32 bytes**

* En quina trama s'obté la resposta?

42

* Quants segments conté la resposta?

21

* Quina és la mida de la majoria dels segments?

1420 bytes

***CAPTURA I ANÀLISI DE TRAMES (2 punts)***

Realitza els següents exercicis amb Wireshark i contesta les preguntes en **color blau**.

Abans de començar la captura de dades tingues preparades les següents accions:

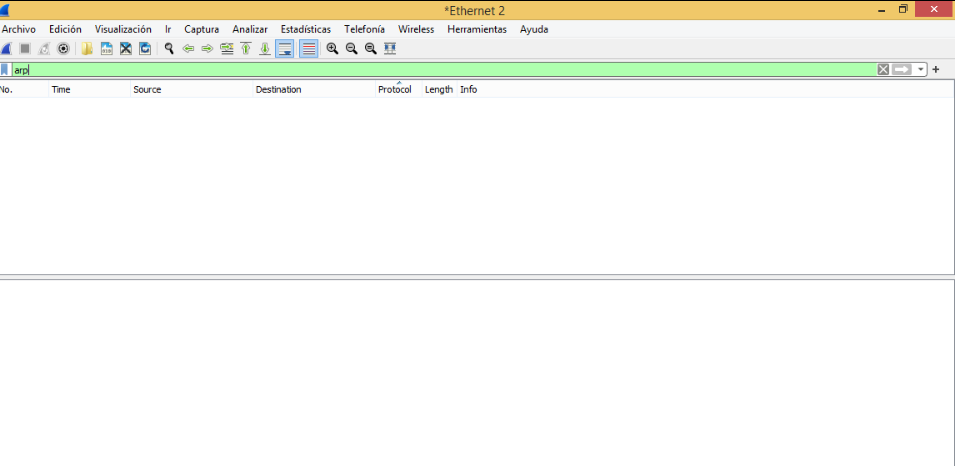
* En un terminal, escriu la comanda **ping 142.250.185.3**
* En un terminal, escriu la comanda **ping google.es**

Obre el navegador i posa l'adreça **google.es**

Comença la captura i executa les accions anteriors

Atura la captura de dades i guarda-la

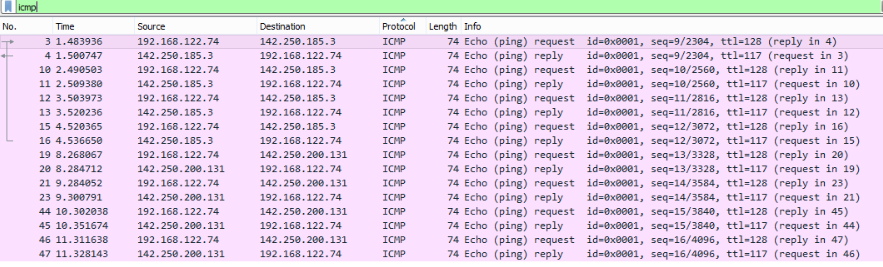
* Filtra el protocol **ARP** i enganxa a continuació una captura de pantalla.



* Quin filtre addicional aplicaries per filtrar només els missatges de Broadcast?

(eth.dst[0] & 1)

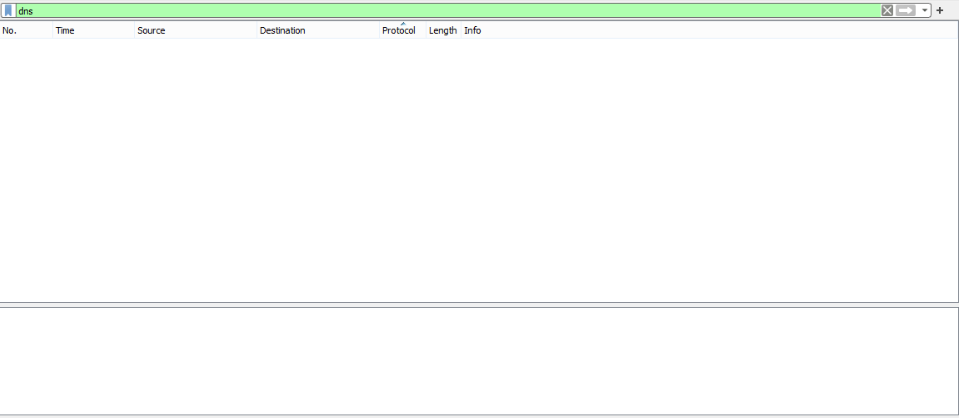
* Filtra el protocol **ICMP** i enganxa a continuació una captura de pantalla.



* Quin filtre addicional aplicaries per filtrar només el missatges de resposta al ping?

ttl=117

* Filtra el protocol **DNS** i enganxa a continuació una captura de pantalla.



* Filtra el protocol **HTTP** i enganxa a continuació una captura de pantalla.

