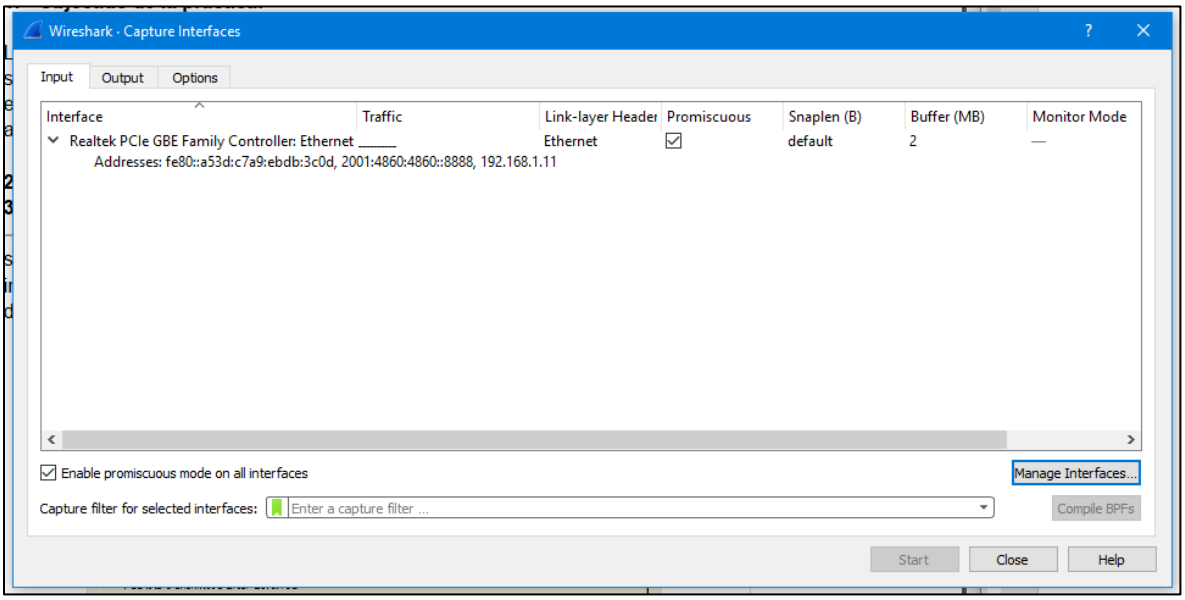
Pràctica 4 - El model OSI

1. *Objectius*

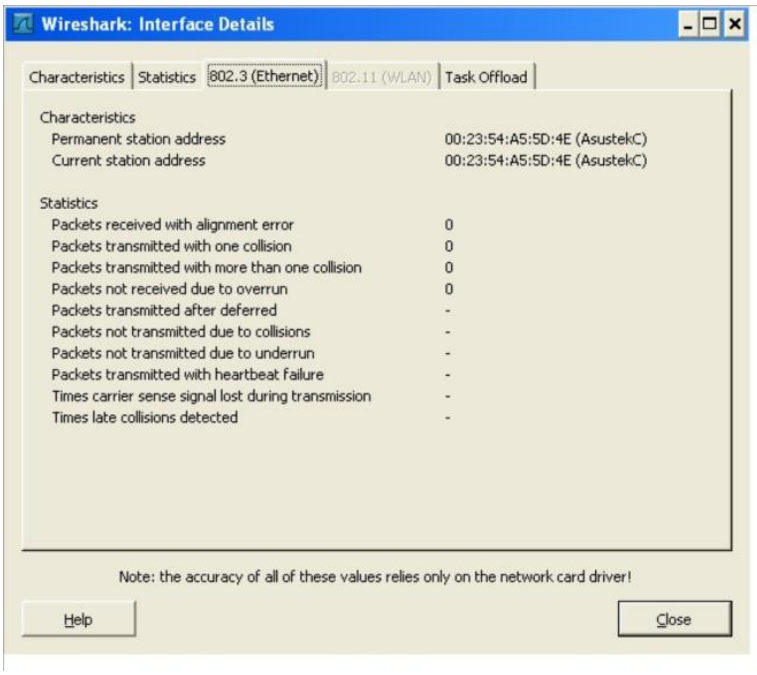
En aquesta pràctica es proposa d'utilització de la eina Wireshark per poder veure d'aprop com es realitza la encapsulació i desencapsulació de les diferents DPU's. D'aquesta manera, entendrem com dos equips amb característiques diferents podem transmetre informació. Concretament, Wireshark ens capturarà el tràfic de la nostre xarxa, de manera que podem veure els paquets que hi circulen amb la seva informació.

2. *Resposta a les diferents qüestions*

a. A la finestra de captura, tenim una icona on es llisten les interfícies que té el nostre sistema. Per exemple, en el cas de l'autor, apareix una interfície associada a la Ethernet i una interfície associada a la WiFi. Visualitzeu les característiques de cada interfície clicant al botó de "details". Indiqueu que teniu i expliqueu detalladament que apareix.
La meva versió de Wireshark sembla haver abandonat aquest menú. He buscat a internet aquesta pestanya i la he trobat en versions anteriors. Fins i tot a la documentació oficial et diu com arribar-hi. A la versió que tinc instal·lada, a dins de "Capture Interfaces" no em surt cap opció ni botó de Details:



De totes maneres, he agafat una captura que he trobat d'internet per respondre la pregunta:

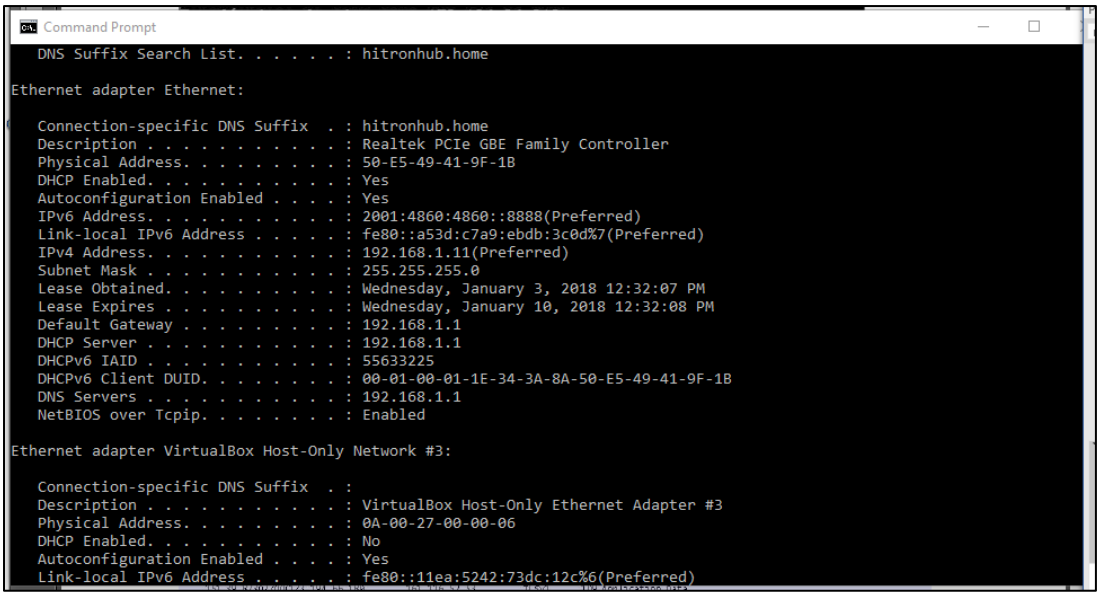


Puc observar la MAC del equip, sota les descripcions de Permanent Adress Station i Current Adress Station. També puc veure la marca comerial. No hi ha informació de paquets ja que al moment de la captura no s'ha enviat res. També puc observar característiques com la velocitat o els drivers.

b. <u>Seleccioneu la interfície d'Ethernet. Apunteu l'adreça MAC que surt i executeu des de consola un ipconfig /all. Identifiqueu la IP associada a aquesta MAC. Descriviu curosament els detalls a l'informe.</u>

La MAC que surt és 50-E5-49-41-9F-1B.

Al realitzar *ipconfig /all* aconsegueixo veure la meva adreça IP, 192.168.1.11. També indica la màscara, la direcció física (MAC), la adreça dels servidors i la porta d'enllaç:



c. Exercici 1

i. Com es descriu la vostra adreça MAC?

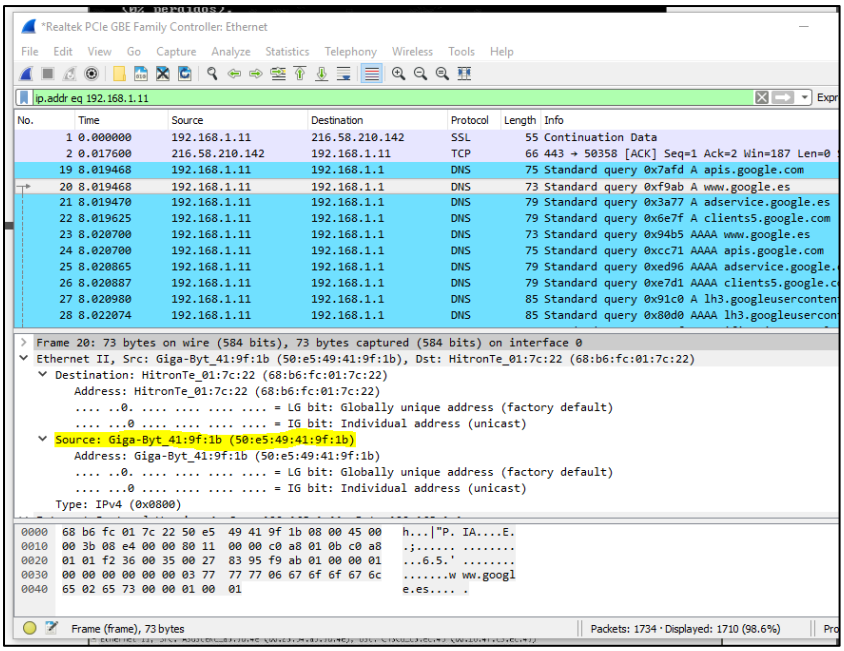
Segons Wikipedia, es descriu en un total de 6 octets separats per dos punts. Cada octet té 8 bits, de b7 fins a b0: MM:MM:MM:SS:SS:SS.

ii. A la adreça MAC hi han dues parts clarament diferenciades. A que corresponen?

Els primer 6 dígits són anomenats "prefix" i estan associats al adaptador del fabricant. Els dígits restants representen el número d'identificació d'un dispositiu concret.

iii. Compara el que apareix amb el que surt amb un ipconfig/all.

Doncs si trio un paquet en concret, puc veure en la secció de Source la meva adreça MAC, la mateixa que hem visualitzat a ipconfig/all.



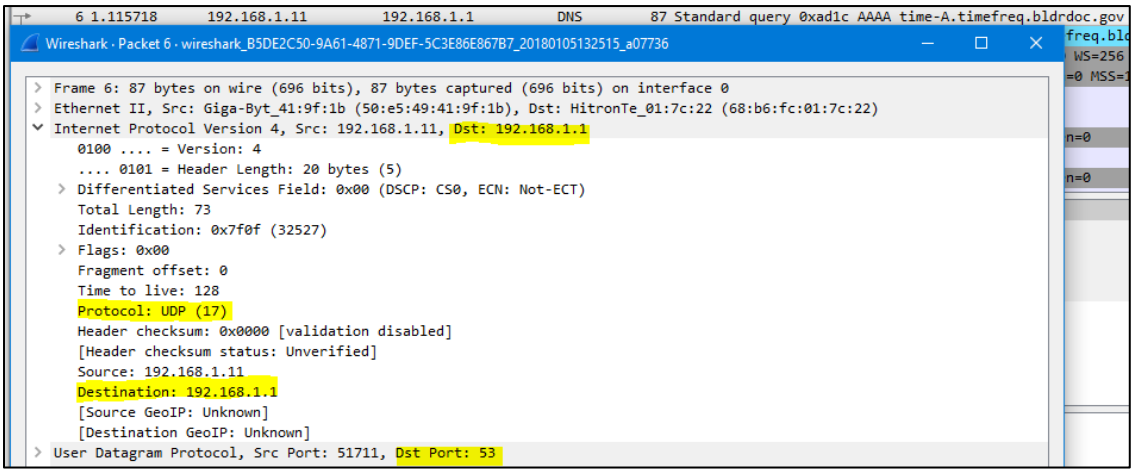
iv. Repassa els diferents camps que apareixen a la capçalera IP i amb l'ajut dels llibres i/o Internet identifica que fa cada un dels camps.

Qualsevol adreça IP es descompon en dos camps, identificador de xarxa, *netid* i identificador d'estació, *hostid.* La meva IP (192.168.1.11) és una IP de classe C, i per tant tindrà com a primer camp els dígits "110". El *netid* és 192.168.1 i el meu *hostid* és 11.

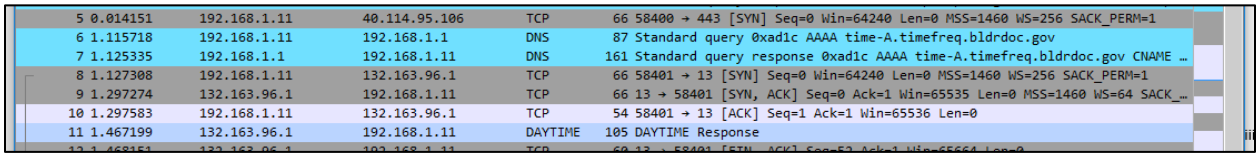
d. Exercici 2

i. Tenint en compte que no heu introduït una adreça IP, busqueu el protocol DNS que permet connectar-nos amb un servidor de DNS per tal de discernir quina IP correspon a la màquina time-A.timefreq.bldrdoc.gov.
Segons la captura de a continuació, Wireshark em diu que la IP del destinatari és 192.168.1.1 (Aquesta captura correspon al paquet de la connexió amb el servidor).

ii. Un cop determinada la IP, a quin port ens estem connectant? Quin protocol de transport fem servir?
En la captura també mostro que el protocol és UDP i que el port de destinació és el 53 mentre que el d'origen és 51711:

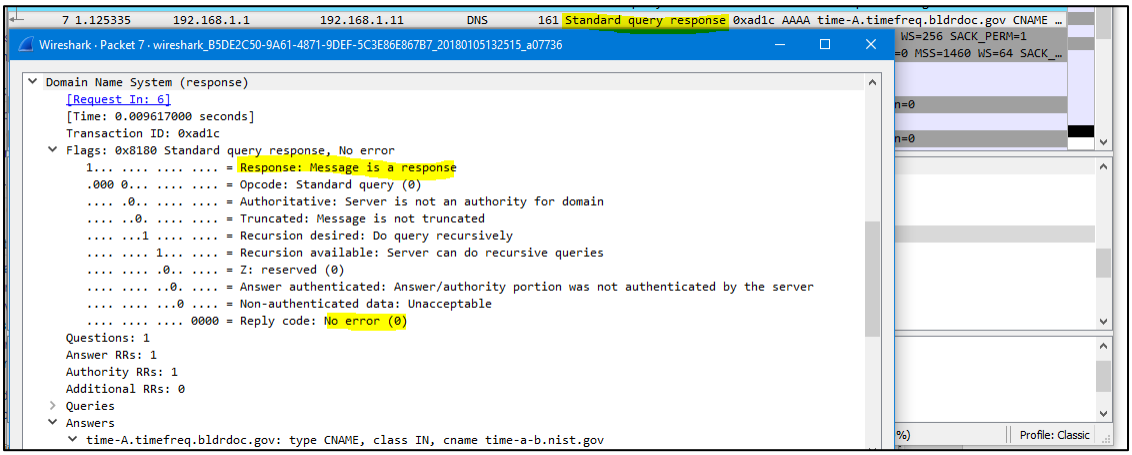


iii. Identifica l'intercanvi de comunicacions que es produeix a nivell de DNS. Quin protocol de transport fa servir DNS? Perquè? Quina és la IP del servidor de DNS?
En la captura mostro l'intercanvi. Fa servir, com ja he dit abans, el protocol UDP. El fa servir perquè és el protocol més simple i eficaç avui en dia, ja que permet l'enviament de datagrames (User Datagram Protocol) sense que hi hagi necessàriament una connexió prèvia. La IP del servir DNS suposo que és la IP de destí, és a dir, 192.168.1.1.



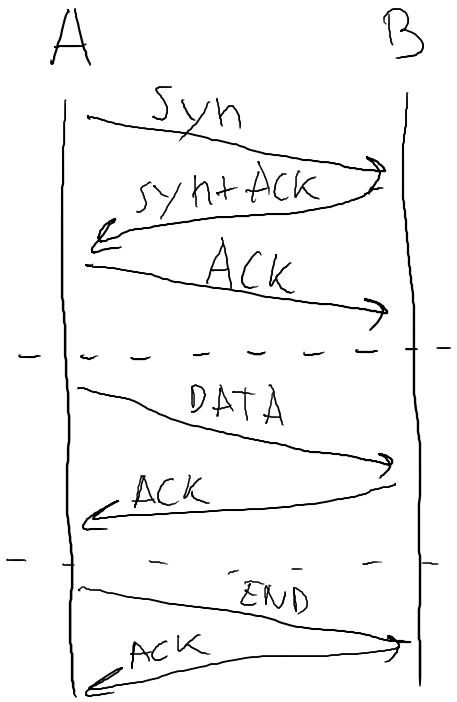
iv. <u>Com s'especifica la resposta? Què respon?</u>

La resposta s'especifica en un paquet anomenat "Standard query". Dit d'una altre manera, és el missatge de resposta de la meva sol·licitud, és a dir, un ACK. A la captura podem veure aquesta connexió i la confirmació de la inexistència d'errors:



v. <u>Feu el diagrama temporal descrivint detalladament l'intercanvi d'informació entre el vostre ordinador i el servidor de DNS.</u>

La connexió és sol·licita amb un paquet de sincronització. El receptor, si tot va bé, autoritza aquesta amb la resposta d'un missatge de sincronització que funciona a la vegada com un ACK, ja que accepta la sol·licitud. El que l'ha sol·licitat informa que aquesta confirmació ha estat rebuda correctament. Després de l'enviament de la data corresponent (en aquest cas, la data ("fecha") en aquell moment), s'acaba la connexió amb un missatge de "fi" i el seu conseqüent ACK.



vi. Un cop coneguda la IP destí, proporcionada pel servidor de DNS, identifica l'intercanvi de control que es produeix a nivell de TCP per la transmissió de la informació. Expliqueu que fa cada paquet i feu un diagrama temporal on es representa aquest intercanvi. Pren molta rellevància la utilització dels flags a TCP. Indiqueu que fan i com es fan servir per gestionar la comunicació

L'intercanvi de control és una resposta en tres passos, és a dir, sol·licito una connexió de sincronisme, em respon amb un altre paquet de sincronisme i torno a enviar un ACK per informar de que ja estem connectats. Els *flags* usats són els següents:

- Reserved Bit: no està especificat
- No-fragmentat: activat (*set)*
- More fragments: no està especificat

e. Exercici 3

i. Expliqueu detalladament la captura, tal i com s'ha fet en l'exercici anterior

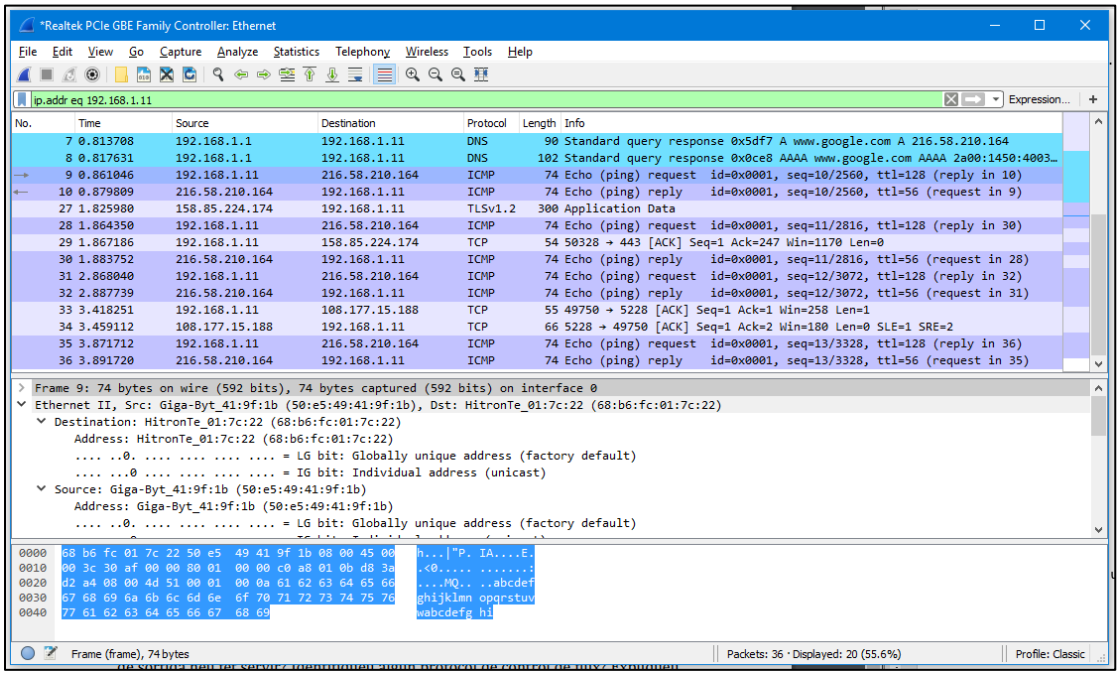
Aquí podem veure el *ping* a la IP 216.58.210.164, corresponent a www.google.com . Podem veure l'enviament de 4 paquets, dels quals cap s'ha perdut. TTL és el Time To Live, el nombre de salts que ha fet el paquet.

```
C:\Users\blair>ping www.google.com

Pinging www.google.com [216.58.210.164] with 32 bytes of data:
Reply from 216.58.210.164: bytes=32 time=19ms TTL=56
Reply from 216.58.210.164: bytes=32 time=19ms TTL=56
Reply from 216.58.210.164: bytes=32 time=19ms TTL=56
Reply from 216.58.210.164: bytes=32 time=20ms TTL=56

Ping statistics for 216.58.210.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 20ms, Average = 19ms
```

Cada paquet està format per dues parts, la capçalera i la informació. A vegades, els paquets de ping contenen el temps en el que han estat enviats, però normalment contenen caràcters aleatoris. Els paquets són de 32 bytes + la capçalera.



ii. Què és el protocol ICMP? Com funciona aquest protocol? Quins identificadors i flags fa servir?

El ICMP (Internet Control Message Protocol) és un protocol que fa ús del protocol IP dins del TCP/IP. S'utilitza per informar de l'estat i situacions d'error en el funcionament de la capa de xarxa. Precisament, també s'anomena protocol de Ping. Aquest protocol envia un o varis missatges per determinar si un *host* està disponible. De la mateixa manera, mesura el temps que triguen els paquets en arribar/tornar i la quantitat de nodes (*hosts*) pels que passa.

MAC header	IP header	ICMP header	Data :::

ICMP type 8, Echo request message:

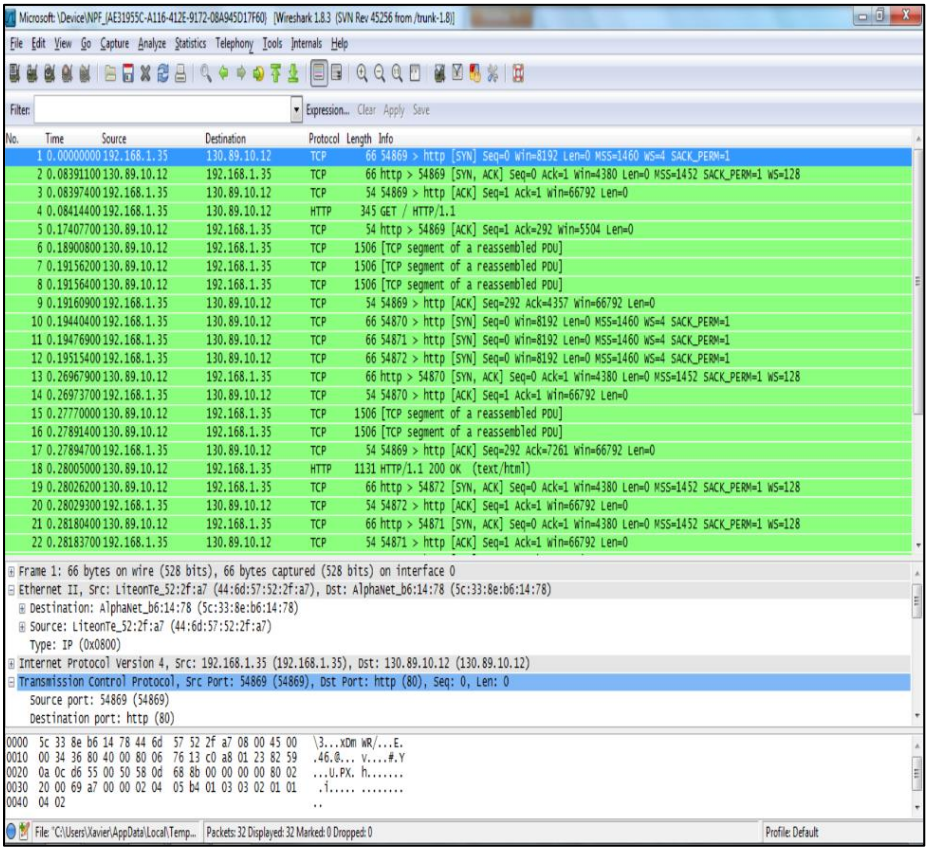
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type								Code								ICMP header checksum															
Identifier																Sequence number															
Data :::																															

En total té 32 bits. El primer camp és tipus, de 8 bits. El segon és Code, també de 8. A continuació tenim el *header cheksum*, de 16 bits, el qual es fa servir per la comprovació d'errors cada vegada que es rep/s'envia el missatge. Seguidament tenim un identificador, també de 16 bits, el qual es fa servir per "ajudar" a unir les sol·licituds (echo) amb la resposta associada. Finalment, tenim el Sequence number, amb una funció similar a la del identificador, i Data.

iii. Obriu el navegador i poseu http://ip_obtinguda a través del ping. S'obre la pàgina? Que captura el sniffer? Feu una explicació detallada.

S'obra la pàgina a la perfecció, ja que accedir directament amb la IP a la qual s'ha realitzat el ping és el mateix que accedir amb la direcció web (s'obra Google, per tant).

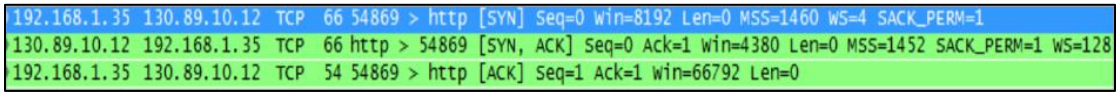
A continuació podem veure les transferències de dades realitzades entre la pàgina web i el nostre ordinador per establir connexió:



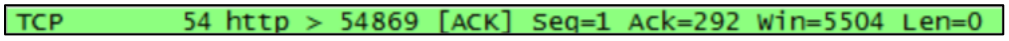
iv. Desglosseu la captura per connectar amb la web. Aneu al protocol TCP. Quin port de sortida heu fet servir? Identifiqueu algun protocol de control de flux? Expliqueu detalladament el que heu capturat.

Per tal d'establir la connexió segons el protocol IP, es necessari realitzar la negociació en tres passos. Consisteix en:

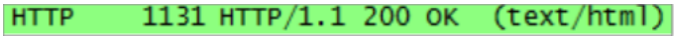
- El meu PC envia un missatge de sincronització (SYN).
- El destinatari (www.simpleweb.org) respon amb un ACK

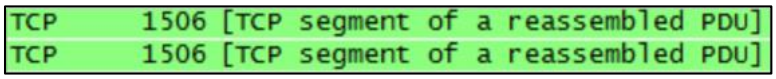


S'estableix la connexió després d'aquesta confirmació. Mitjançant el protocol *http*, el meu PC indica quina pàgina necessita. A continuació rebem l'ACK de la petició.

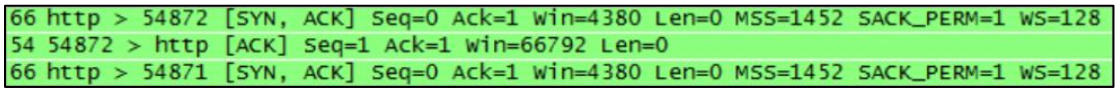


Seguidament, rebem els paquets en HTML de la estructura de la pàgina web. En aquest cas, està dividida en 3 paquets, els quals s'ajuntaran més tard.





Finalment, es tanca la connexió amb el mateix procediment que l'establiment de la connexió, és a dir, en 3 passos:



3. *Conclusions*

La connexió entre dos equips de característiques diferents es pot realitzar per l'enviament d'informació gràcies a l'existència de protocols estàndards: DPU i TCP. Mitjançant el filtratge d'IP's o de paquets tipus *ping* s'ha observat aquesta comunicació així com els passos necessaris que porten cap a ella. Wireshark ens ha permès veure en detall els camps d'aquets paquets que hem estudiat a teoria.

Per altra banda, hem vist una mica el protocol DNS amb un servidor concret i d'aquesta manera hem pogut aplicar els diagrames temporals vistos a classe "a la vida real".