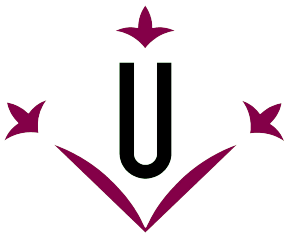


Universitat de Lleida
Escola Politècnica Superior

Xarxes

Pràctica 3: Ànalisi de trànsit

Jordi Rafael Lazo Florensa

5 de juny de 2020

Grau en Enginyeria Informàtica

Índex

Índex de figures

Índex de taules

1 Introducció

Aquesta tercera pràctica de Xarxes, destinada a l'anàlisi del trànsit Ethernet, té com a objectiu principal aprendre posar en pràctica els conceptes bàsics adquirits en les sesions de teoría amb el programa de gestió de protocols *Wireshark*, així com visualitzar i analitzar els continguts dels diferents paquets que es poden transmetre entre dispositius mitjançant la utilització de filtres. Durant aquesta pràctica es veuran protocols de les diferents capes que formen l'estructura de Ethernet: des de diferents versions del mateix enllaç, fins a alguns serveis de la capa d'aplicació i les seves funcionalitats.

2 Caracterització de la xarxa

2.1 Tipus d'adreçament de la capa de xarxa

Els tipus de classes possibles son:

Clase	**Rang**	**Nº xarxes**	**Nº hosts per xarxa**	**Màscara de xarxa**
A	0.0.0.0 - 126.255.255.255	126	16 777 214	255.0.0.0
B	128.0.0.0 - 191.255.255.255	16 384	65 534	255.255.0.0
C	192.0.0.0 - 223.255.255.255	2 097 152	254	255.255.255.0

Taula 1: Rangs i classes de IP

Després d'analitzar mitjançant Wireshark les dades obtingudes en la traça, es pot observar amb facilitat com, o bé l'emissor, o bé el destinatari, sempre formen part d'una mateixa xarxa: **172.16.x.x**. Així doncs, es pot afirmar que els 16 primers bits corresponen a la xarxa, per la qual cosa es tracta d'una classe B.

2.2 Adreça de xarxa

Tal i com es pot observar en el apartat anterior, la xarxa a la qual pertanyen les dades obtingudes, es tracta d'una classe B, això implica que, els 16 primers bits, formen part de la direcció de xarxa i, els 16 posteriors, el host, per tant significa que la màscara de la xarxa és: 255.255.0.0.

Atès que en la direcció de xarxa, la part corresponent al host està formada per 0, es pot arribar a la conclusió que, la direcció de la xarxa analitzada és: 172.16.0.0.

2.3 Adreça de *broadcast*

La adreça de broadcast utilitza la direcció més alta en el rang de la xarxa. Per a dur a terme aquesta comunicació, s'utilitza l'adreça IP de destinatari 255.255.255.255.

Així dons, mitjançant l'aplicació del filtre:

```
eth.dst==ff:ff:ff:ff:ff:ff && !arp
```

es pot visualitzar aquells paquets amb destinació al broadcast, a excepció dels de tipus ARP, per tant es pot concloure que la direcció IP 172.16.255.255 es l'adreça *broadcast*.

2.4 Porta d'enllaç de la xarxa

Amb la finalitat de conèixer la porta d'enllaç a la xarxa, s'ha d'analitzar els paquets DHCP ACK, els quals es troben emprant el filtre:

```
bootp.option.dhcp == 5
```

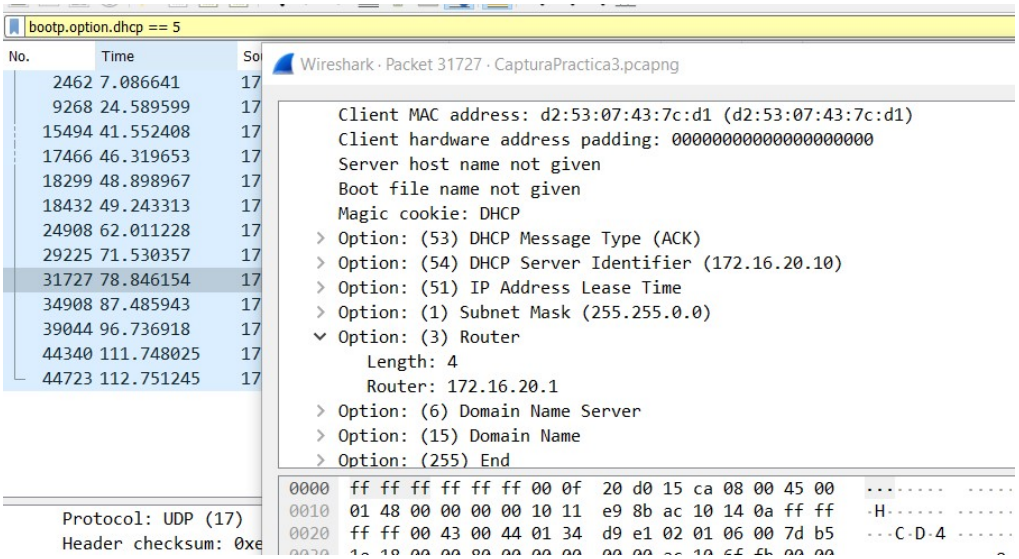


Figura 1: Port enllaç de la xarxa

Qualsevol dels paquets obtinguts posseeix la *Option (3): Router*, la qual indica la IP de l'encaminador i, per tant, la porta d'enllaç a la xarxa, que és: **172.16.20.1**.

3 Anàlisi nivells d'enllaç i de xarxa

3.1 Els protocols encapsulats en les trames de nivell 2

Per trobar els protocols encapsulats de nivell 2, s'empra l'eina *Protocol Hierarchy* dintre del menú *Statistics* de Wireshark. Els protocols encapsulats en la trama son:

Protocol	Type	Descripció
ARP	0x0806	És un protocol de comunicacions de la capa d'enllaç de dades, responsable de trobar l'adreça de maquinari (Ethernet MAC) que correspon a una determinada adreça IP.
IPv4	0x0800	Es la versió 4 de Protocol de Internet (IP) que s'encarrega de dirigir i encaminar els paquets commutats. Utilitza 32 bits per al rang de les adreces.
IPv6	0x86dd	El IPv6 és una actualització al protocol IPv4, dissenyat per a resoldre el problema d'esgotament de direccions.
IPX	0x8137	És un protocol de comunicacions de xarxes utilitzat per a transferir dades d'un node a un altre de la xarxa mitjançant paquets de dades anomenades datagrames.
LLC	NULL	Defineix la forma en què les dades són transferides sobre el medi físic, proporcionant servei a les capes superiors.

Taula 2: Protocols encapsulats en les trames nivell 2

Les estructures de les trames del protocols encapsulats anomenats anteriorment son:

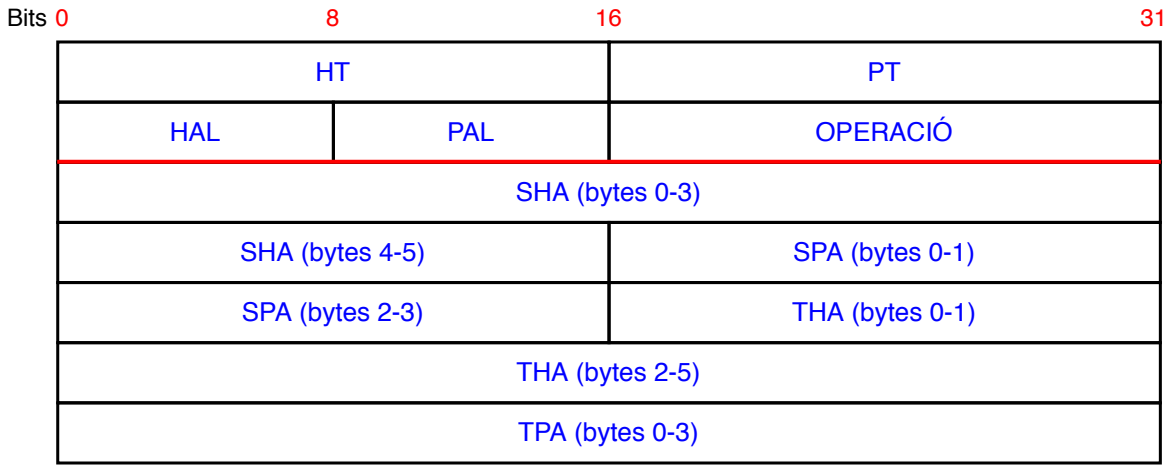


Figura 2: Trama ARP

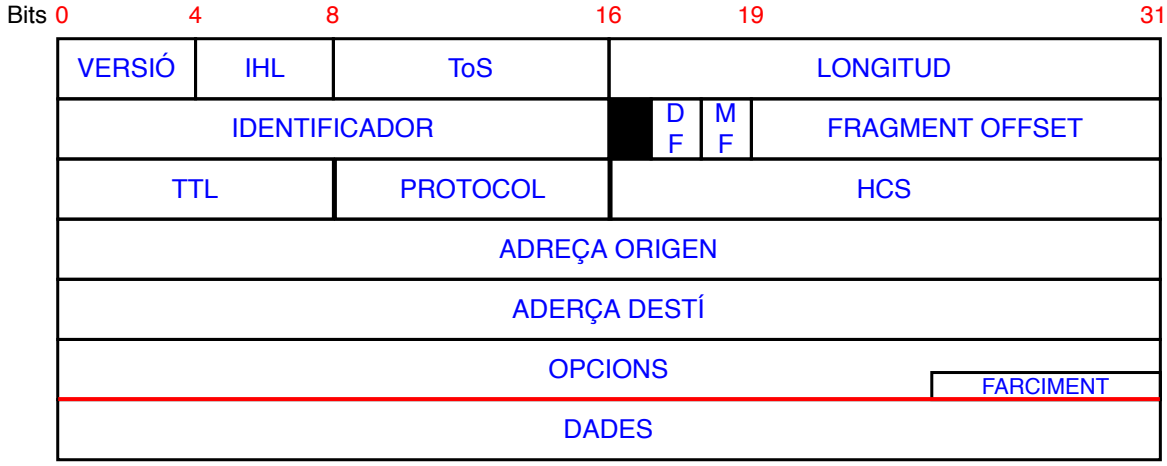


Figura 3: Trama IPv4

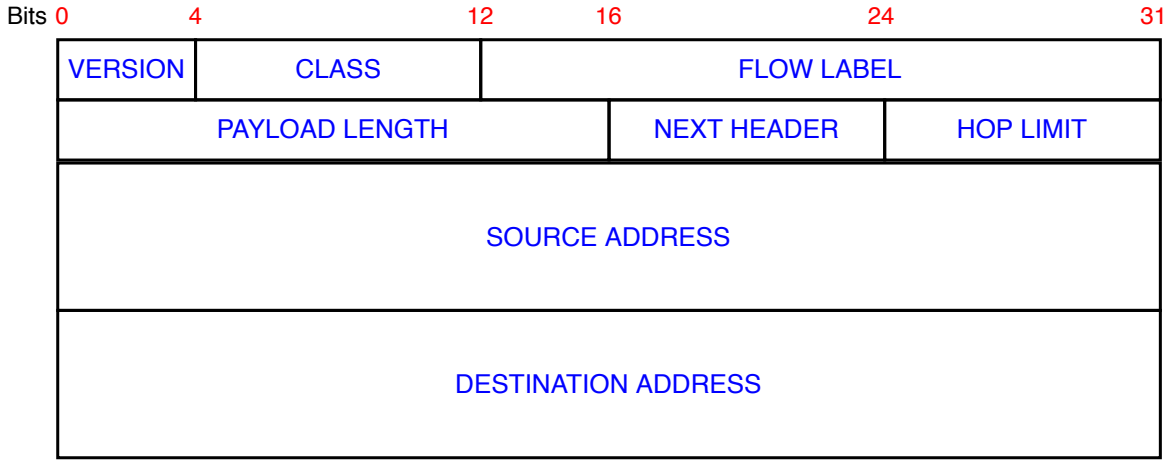


Figura 4: Trama IPv6

CHECKSUM	PACKET LENGTH	TRANSPORT CONTROL	PACKET TYPE	DESTINATION NETWORK
2 Bytes	2 Bytes	1 Byte	1 Bytes	4 Bytes

DESTINATION NODE	DESTINATION SOCKET	SOURCE NETWORK	SOURCE NODE	SOURCE SOCKET
6 Bytes	2 Bytes	4 Byte	6 Bytes	2 Bytes

Figura 5: Trama IPX

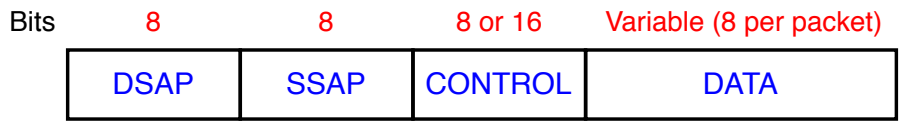


Figura 6: Trama LLC

3.2 Adreça IPv4 que empra el protocol MDNS per IPv6

El primer pas consisteix en aplicar el filtre:

`mdns`

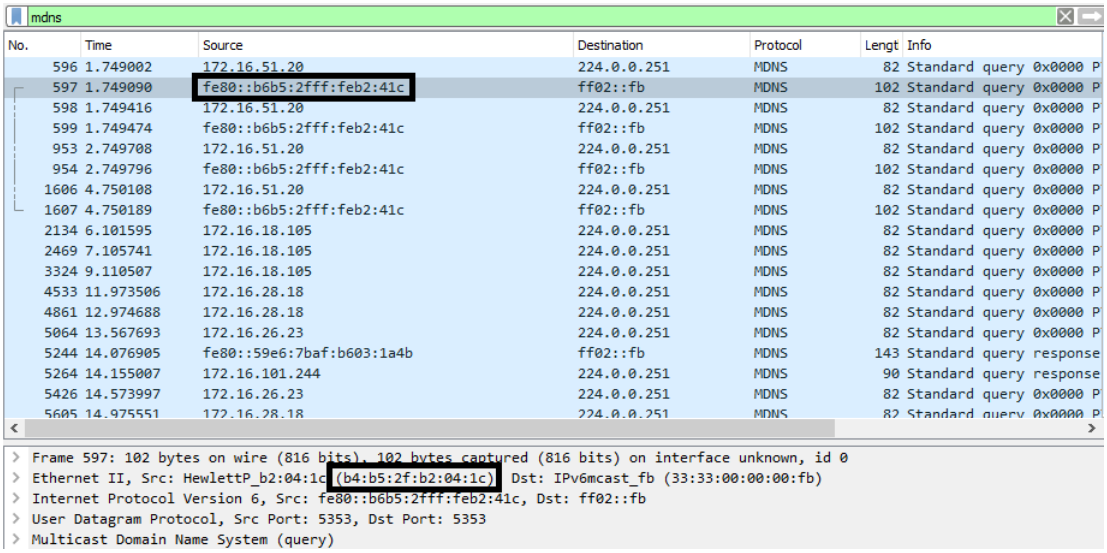


Figura 7: Paquets MDNS

A continuació amb l'adreça MAC de cada IPv6 s'aplica el següent el filtre:

`eth.src == <adreçaMAC>`

Per a buscar una per una la seva adreça IPv4.

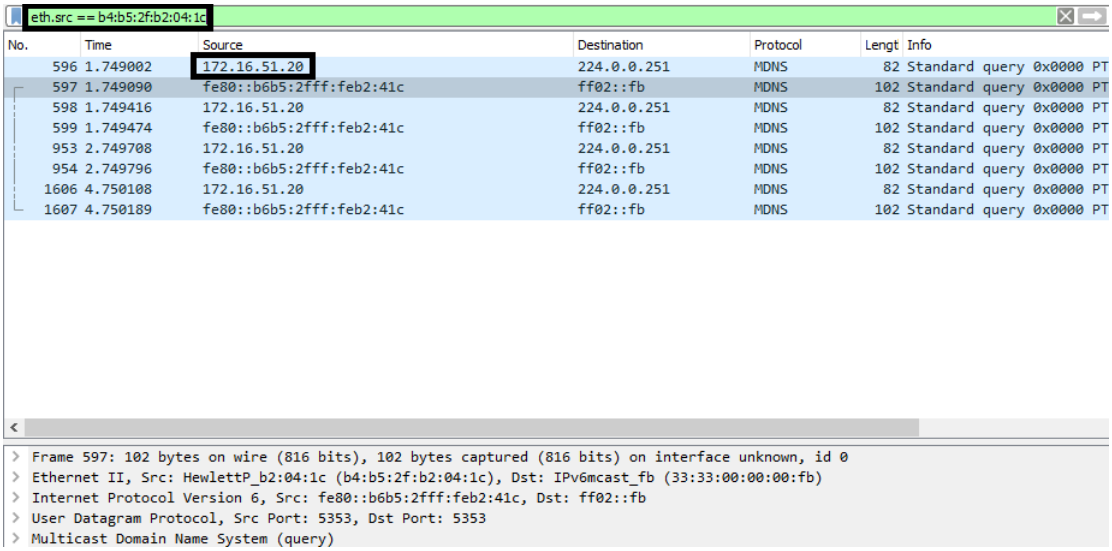


Figura 8: Eth.src d'una adreça MAC

Aquest procediment es repeteix per a totes les adreces MACs.

Els resultats obtinguts son els següents:

IPv6	MAC	IPv4
fe80::b6b5:2fff:feb2:41c	b4:b5:2f:b2:04:1c	172.16.51.20
fe80::59e6:7baf:b603:1a4b	70:71:bc:5d:92:92	172.16.101.244
fe80::26be:5ff:fe1c:edf7	24:be:05:1c:ed:f7	172.16.51.34
fe80::20f:feff:fe98:c253	00:0f:fe:98:c2:53	172.16.26.151
fe80::1093:c39a:6dbe:4378	48:0f:cf:3e:5e:1a	172.16.12.6
fe80::4d5:32ca:ba89:5d43	b4:b5:2f:ba:8d:45	172.16.18.113
fe80::b6b5:2fff:feb2:39f	b4:b5:2f:b2:03:9f	172.16.51.43
fe80::6d66:f968:cee6:5b9	00:0f:fe:7d:c4:ca	172.16.26.158

Taula 3: Relació IPv6, MAC, IPv4

3.3 Adreces *multicast*

Per a trobar les direccions *multicast*, es fa ús del següent filtre:

```
eth.dst[0] & 1 and !eth.dst == ff:ff:ff:ff:ff:ff
```

Les direccions multicast obtingudes, així com els protocols emprats, respectivament, són els següents:

Adreça *multicast*	**Protocol**
ff02::1:2	DHCPv6
ff02::1:3	LLMNR
224.0.0.252	LLMNR
ff02::1	IPv6, ICMPv6
224.0.0.251	MNDS, IGMPv2
ff02::fb	MNDS
ff02::16	ICMPv6
ff02::c	UDP, SSDP
224.0.0.18	VRRP
224.0.0.1	BNJP, IGMPv2
224.0.0.22	IGMPv3
ff02::2	ICMPv6
ff02::1:ff12:6af4	ICMPv6

Taula 4: Adreces *multicast*

La descripció del protocols trobats:

- **DCHPv6**: *Dynamic Host Configuration Protocol version 6* és un protocol client-servidor, que proporciona una configuració administrada de dispositius sobre IPv6.
- **LLMNR**: *Link-Local Multicast Name Resolution* és un protocol basat DNS que permet que els hosts IPv4 i IPv6 realitzin la resolució de noms per a hosts en el mateix enllaç local.
- **IPv6**: *Internet Protocol version 6* protocol de telecomunicacions que, a través de combinacions numèriques, permet la connexió entre els milions d'ordinadors i dispositius.
- **ICMPv6**: *Internet Control Message Protocol version 6* protocol que permet administrar informació relacionada amb errors dels equips de xarxa.
- **MDNS**: *Multicast DNS* resol els noms de host a adreces IP dins de les xarxes petites que no inclouen un servidor de noms local.
- **IGMPv2**: *Internet Group Management Protocol version 2* s'utilitza per a intercanviar informació sobre l'estat de pertinença entre encaminadors IP que admeten la multidifusió i membres de grups de multidifusió.
- **UDP**: *User Datagram Protocol* és un protocol del nivell de transport basat en l'intercanvi de datagrames que permet l'enviament d'aquests a través de la xarxa sense que s'hagi establert prèviament una connexió.
- **SSDP**: *Simple Service Discovery Protocol* és un protocol que serveix per a la cerca de dispositius UPnP en una xarxa.
- **VRRP**: *Virtual Router Redundancy Protocol* és un protocol de comunicacions dissenyat per a augmentar la disponibilitat de la porta d'enllaç per defecte donant servei a màquines en la mateixa subxarxa.
- **BNJP**: *Canon BJNP Protocol* és un protocol de descobriment de servei LAN personalitzat utilitzat per impressores i escàners Canon. Els sistemes informàtics uti-

litzen aquest protocol per a descobrir automàticament els dispositius Cànon en la xarxa.

- **IGMPv3**: *Internet Group Management Protocol version 3* s'utilitza per a intercanviar informació sobre l'estat de pertinença entre encaminadors IP que admeten la multidifusió i membres de grups de multidifusió.

3.4 Gràfica de distribució dels protocols de nivell 3

Per a generar la gràfica dels protocols de nivell 3, s'ha emprat l'eina *Protocol Hierarchy*, dintre del menú *Statistics* de Wireshark. Els resultats obtinguts son:

Protocol	Percentatge d'ús
LLC	0.02 %
IPX	0.02 %
IPv6	3.94 %
IPv4	64.06 %
ARP	31.96 %

Taula 5: Distribució dels protocols nivell 3

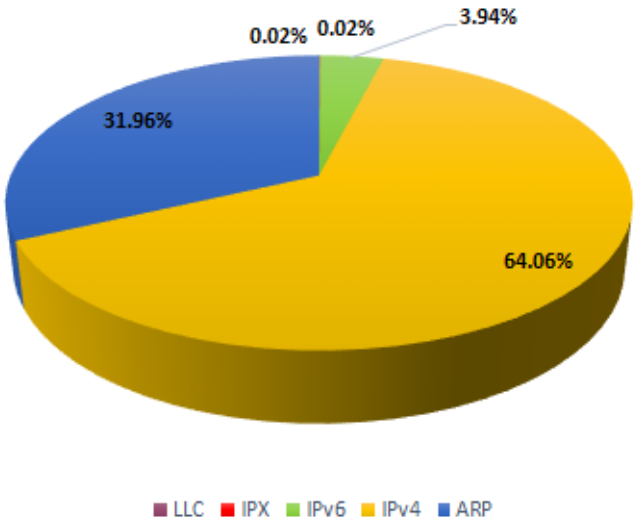


Figura 9: Gràfica distribució dels protocols de nivell 3

4 Anàlisi nivell de transport

Abans d'iniciar l'anàlisi del nivell de transport caldrà desestimar els següents paquets i protocols:

- El paquets que tenen com a destí l'adreça broadcast de nivell 2.
- Els paquets d'IPv6.
- Els paquets de multicast.
- Els protocols ARP, DNS i NTP.

Per a desestimar aquest paquets s'ha aplicat el següent filtre:

```
!eth.dst[0]&1 and !ipv6 and !eth.dst == ff:ff:ff:ff:ff:ff and !arp && !dns && !ntp
```

4.1 Comunicacions TCP no dutes a terme

Per a trobar les comuniaccions TCP que no s'han dut a terme s'ha aplicat el següent filtre:

```
tcp and tcp.flags.syn == 1 and tcp.flags.ack == 0
```

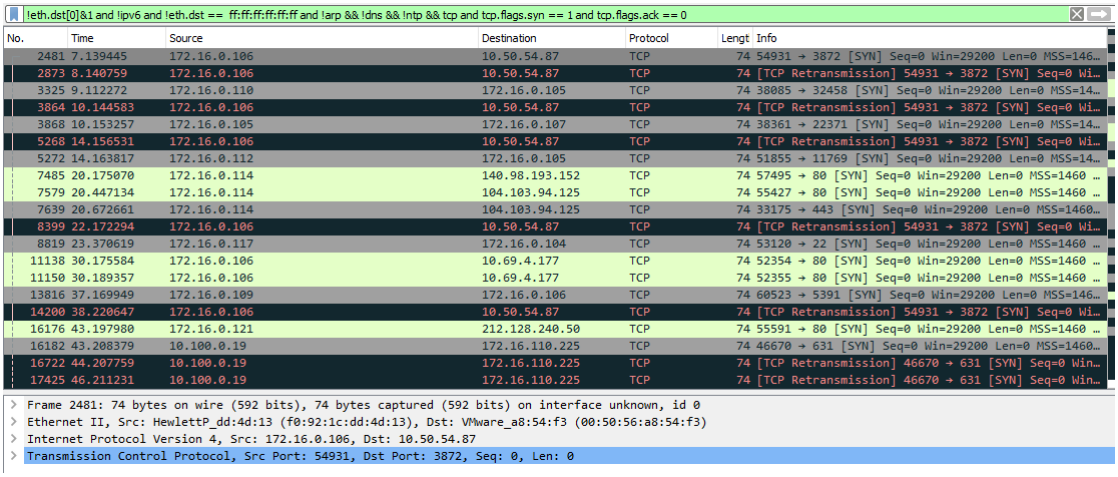


Figura 10: Filtre *tcp and tcp.flags.syn == 1 and tcp.flags.ack == 0*

Un cop aplicat el filtre el següent pas consisteix en seleccionar l'opció de *Conversations* dintre del menú *Statistics*. A continuació apareixerà la finestra següent:

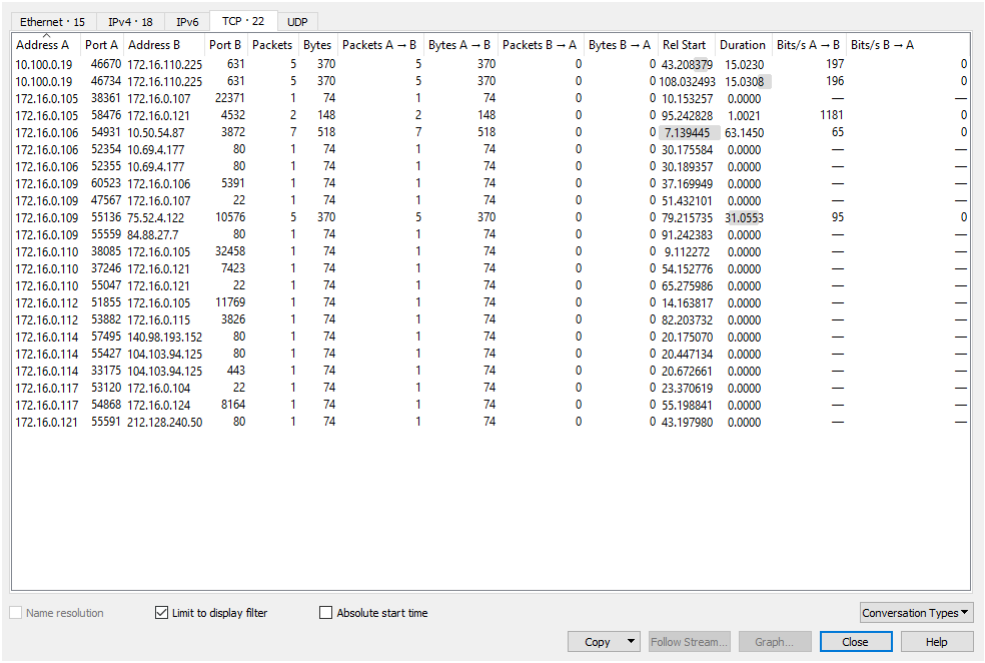


Figura 11: *Limit to display filter TCP*

S'ha pres la decisió de considerar dos casos, llistats a continuació, com a errors:

- L'emissor envia un paquet SYN actiu, i no rep contestació per part del receptor.
- En qualsevol moment de la comunicació, es rep un paquet TCP amb el flag RST actiu.

Els resultats obtinguts son:

IP-Origen	**Port-Origen**	**IP-Destí**	**Port-Destí**	**Motiu-Fallada**
10.100.0.19	46670	172.16.110.255	631	SYN, ACK
10.100.0.19	46734	172.16.110.255	631	SYN, ACK
172.16.0.105	38361	172.16.0.107	22371	RST
172.16.0.109	54931	10.50.54.87	3872	SYN, ACK
172.16.0.109	60523	172.16.0.106	5391	RST
172.16.0.110	55136	172.16.4.122	10576	SYN, ACK
172.16.0.110	37246	172.16.0.121	7423	RST
172.16.0.114	33175	104.103.94.125	443	RST

Taula 6: Comunicacions TCP no dutes a terme

4.2 Comunicacions TCP completes

4.2.1 Comunicacions HTTP i HTTPS

El filtre que s'ha d'aplicar per trobar les comunicacions HTTP completes és el següent:

```
tcp.post == 80 or tcp.port == 443
```

Posteriorment, s'estudien les comunicacions trobades, obtenint els resultats exposats a continuació:

IP-Origen	IP-Destí
172.16.0.121	212.128.240.50
172.16.0.106	10.69.4.177
172.16.0.109	84.88.27.7
172.16.0.114	104.103.94.125
172.16.0.114	140.98.193.152

Taula 7: Comunicacions HTTP completades

IP-Origen	IP-Destí
172.16.0.114	104.103.94.125

Taula 8: Comunicacions HTTPS completades

4.2.2 Resta de comunicacions TCP

IP-Origen	Port-Origen	MTU-Origen	Finestra-Origen-Inicial	IP-Destí	Port-Destí	MTU-Destí	Finestra-Destí-Inicial
172.16.0.105	58476	1500	3737600	172.16.0.121	4532	1500	3706880
172.16.0.109	47567	1500	3737600	172.16.0.107	22	1500	3706880
172.16.0.110	38085	1500	3737600	172.16.0.105	32458	1500	3706880
172.16.0.110	55047	1500	3737600	172.16.0.121	22	1500	3706880
172.16.0.112	51855	1500	3737600	172.16.0.105	11769	1500	3706880
172.16.0.112	53882	1500	3737600	172.16.0.115	3826	1500	3706880
172.16.0.117	53120	1500	3737600	172.16.0.104	22	1500	3706880
172.16.0.117	54868	1500	3737600	172.16.0.124	8164	1500	3706880

Taula 9: Resta de comunicacions TCP

4.3 Comuncacions UDP no dutes a terme

Per a visualitzar les comunicacions *UDP* no dutes a terme s'ha fet ús del següent filtre:

```
udp && icmp
```

Aquest filtre permet visualitzar els paquets d'error relacionats amb *UDP*. De tots els paquets filtrats, s'han de triar tan sols aquells l'error dels quals sigui *Port Unreachable*.

IP-Origen	Port-Origen	IP-Destí	Port-Destí	Motiu-Fallada
172.16.0.115	37134	172.16.0.113	34588	Port Unreachable
172.16.0.114	50062	172.16.0.115	7556	Port Unreachable
172.16.0.119	37758	172.16.0.116	11345	Port Unreachable

Taula 10: Comunicacions UDP no dutes a terme

4.4 Comunicacions UDP dutes a terme

S'ha trobat comunicació o, almenys, no hi ha hagut cap rebuig de connexió, en 6 comunicacions.

Per a trobar aquestes comunicacions s'ha fet ús del filtre:

`udp && !icmp`

IP-Origen	Port-Origen	IP-Destí	Port-Destí
172.16.0.103	37134	172.16.0.115	34588
172.16.0.105	50062	172.16.0.114	7556
172.16.0.107	60907	172.16.0.109	18599
172.16.0.115	56308	172.16.0.116	27823
172.16.0.116	55976	172.16.0.119	5822
172.16.0.116	37758	172.16.0.119	11345

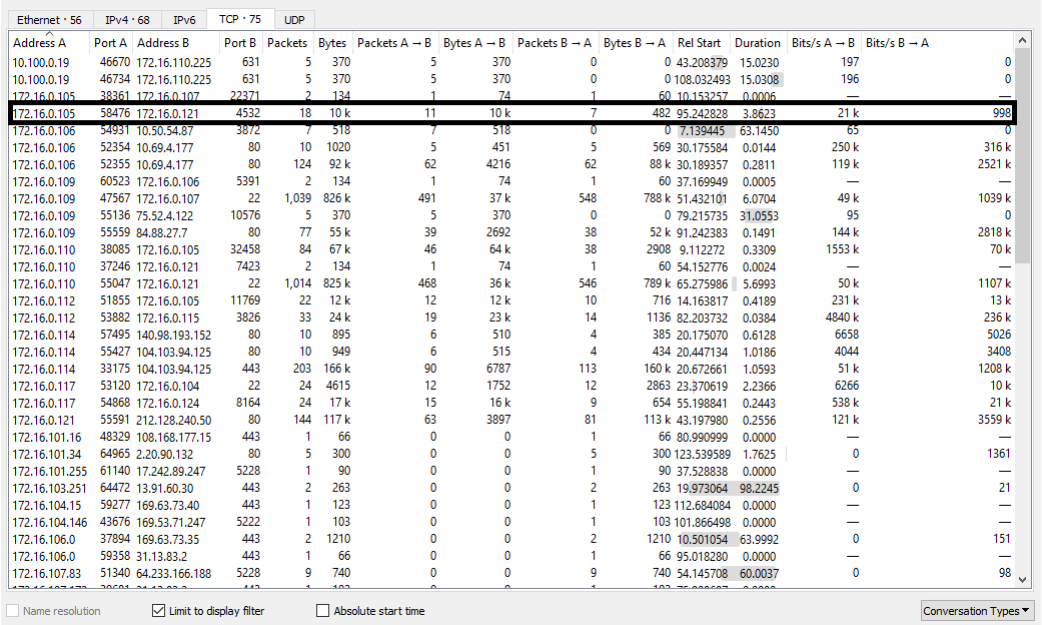
Taula 11: Comunicacions UDP dutes a terme

4.5 Altres comuncacions TCP

Per a cada una de les comunicacions primer s'aplica el filtre:

`tcp`

A continuació es selecciona l'apartat *Conversations* del menú *Statistics* i s'aplica el filtre *Limit to display filter* tot seguit es selecciona el paquet TCP entre les adreces IP que es desitja i finalmente es selecciona l'opció de *Follow Stream* per analitzar els paquets, bytes, cabal útil i seqüencies.



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.100.0.19	46670	172.16.110.225	631	5	370	5	370	0	0	43.208379	15.0230	197	0
10.100.0.19	46734	172.16.110.225	631	5	370	5	370	0	0	108.032493	15.0308	196	0
172.16.0.105	38361	172.16.0.107	22371	2	134	1	74	1	60	10.153257	0.0006	—	—
172.16.0.105	58476	172.16.0.121	4532	18	10 k	11	10 k	7	482	95.242828	3.8623	21 k	998
172.16.0.106	54931	10.50.54.87	3872	7	518	7	518	0	0	7.139445	63.1450	65	0
172.16.0.106	52354	10.69.4.177	80	10	1020	5	451	5	569	30.175584	0.0144	250 k	316 k
172.16.0.106	52355	10.69.4.177	80	124	92 k	62	4216	62	88 k	30.189357	0.2811	119 k	2521 k
172.16.0.109	60523	172.16.0.106	5391	2	134	1	74	1	60	37.169949	0.0005	—	—
172.16.0.109	47567	172.16.0.107	22	1,039	826 k	491	37 k	548	788 k	51.432101	6.0704	49 k	1039 k
172.16.0.109	55136	75.52.4.122	10576	5	370	5	370	0	0	79.215735	31.0553	95	0
172.16.0.109	55559	84.88.27.7	80	77	55 k	39	2692	38	52 k	91.242383	0.1491	144 k	2818 k
172.16.0.110	38085	172.16.0.105	32458	84	67 k	46	64 k	38	2908	9.112272	0.3309	1553 k	70 k
172.16.0.110	37246	172.16.0.121	7423	2	134	1	74	1	60	54.152776	0.0024	—	—
172.16.0.110	55047	172.16.0.121	22	1,014	825 k	468	36 k	546	789 k	65.275986	5.6993	50 k	1107 k
172.16.0.112	51855	172.16.0.105	11769	22	12 k	12	12 k	10	716	14.163817	0.4189	231 k	13 k
172.16.0.112	53882	172.16.0.115	3826	33	24 k	19	23 k	14	1136	82.203732	0.0384	4840 k	236 k
172.16.0.114	57495	140.98.193.152	80	10	895	6	510	4	385	20.175070	0.6128	6658	5026
172.16.0.114	55427	104.103.94.125	80	10	949	6	515	4	434	20.447134	1.0186	4044	3408
172.16.0.114	33175	104.103.94.125	443	203	166 k	90	6787	113	160 k	20.672661	1.0593	51 k	1208 k
172.16.0.117	53120	172.16.0.104	22	24	4615	12	1752	12	2863	23.370619	2.2366	6266	10 k
172.16.0.117	54868	172.16.0.124	8164	24	17 k	15	16 k	9	654	55.198841	0.2443	538 k	21 k
172.16.0.121	55591	212.128.240.50	80	144	117 k	63	3897	81	113 k	43.197980	0.2556	121 k	3559 k
172.16.101.16	48329	108.168.177.15	443	1	66	0	0	1	66	80.990999	0.0000	—	—
172.16.101.34	64965	2.20.90.132	80	5	300	0	0	5	300	123.539589	1.7625	0	1361
172.16.101.255	61140	17.242.89.247	5228	1	90	0	0	1	90	37.528838	0.0000	—	—
172.16.103.251	64472	13.91.60.30	443	2	263	0	0	2	263	19.973064	98.2245	0	21
172.16.104.15	59277	169.63.73.40	443	1	123	0	0	1	123	112.684084	0.0000	—	—
172.16.104.146	43676	169.53.71.247	5222	1	103	0	0	1	103	101.866498	0.0000	—	—
172.16.106.0	37894	169.63.73.35	443	2	1210	0	0	2	1210	10.501054	63.9992	0	151
172.16.106.0	59358	31.13.83.2	443	1	66	0	0	1	66	95.018280	0.0000	—	—
172.16.107.83	51340	64.233.166.188	5228	9	740	0	0	9	740	54.145708	60.0037	0	98

Figura 12: Filtre TCP

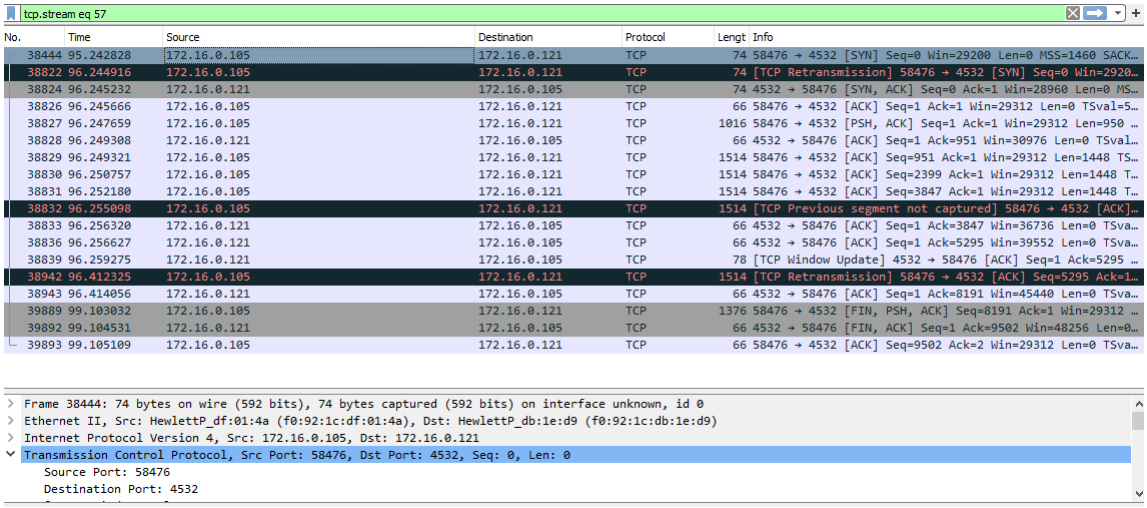


Figura 13: *Follow Stream*

4.5.1 172.16.0.105 ⇔ 172.16.0.121

Paquets apertura		Paquets tancament	
SYN	38444	FIN, PSH, ACK	39889
SYN, ACK	38824	FIN, ACK	39892
ACK	38826	ACK	39893

Taula 12: Paquets apertura i tancament 172.16.0.105 ⇔ 172.16.0.121

Bytes d'usuari	
172.16.0.105 ⇔ 172.16.0.121	10 KB

Taula 13: Bytes d'usuari 172.16.0.105 ⇔ 172.16.0.121

Bytes transmesos	
172.16.0.105 ⇔ 172.16.0.121	10 KB
172.16.0.121 ⇔ 172.16.0.105	482 Bytes

Taula 14: Bytes transmesos 172.16.0.105 ⇔ 172.16.0.121

Sentit comunicació	Cabal brut	Cabal útil
172.16.0.105 ⇔ 172.16.0.121	30542,42 bytes/s	4123,96 bytes/s
172.16.0.121 ⇔ 172.16.0.105	19436,08 bytes/s	2624,34 bytes/s

Taula 15: Cabal brut i útil 172.16.0.105 ⇔ 172.16.0.121

TCP enviats a la fase de connexió	
Maximum segment size:	1460 Bytes
SACK Permitted Option:	True
Timestamps:	TSval 5025645, TSecr 0
No-Operation:	(NOP)
Window scale:	7 (multiply by 128)

Taula 16: TCP intercanviats durant la fase de connexió 172.16.0.105 ⇔ 172.16.0.121

A continuació, s'especifica una breu descripció de les opcions trobades en els paquets anteriors.

- **Maximum segment size**: determina el nombre de bytes que es poden rebre en un sol segment TCP.
- **SACK Premitted Option**: permet detallar quins paquets, missatges o segments han estat rebuts o no.
- **Timestamps**: s'utilitza per mesurar el RTT i per al mecanisme *Protect Against Wrapped Sequences*, el qual elimina duplicats antics de segments que podrien corrompre una connexió TCP oberta.
- **No-Operation**: s'utilitza per a acabar d'omplir la capçalera d'opcions.
- **Window scale**: determina el multiplicador a aplicar a *Window size*.

Nombre de seqüència inicial real	
172.16.0.105 ⇔ 172.16.0.121	1938687936
172.16.0.121 ⇔ 172.16.0.105	176333506

Taula 17: Nombre de seqüència inicial real 172.16.0.105 ⇔ 172.16.0.121

4.5.2 172.16.0.112 ⇔ 172.16.0.115

Paquets apertura		Paquets tancament	
SYN	32889	ACK	32926
SYN, ACK	32890	FIN, ACK	32927
ACK	32891	ACK	32928

Taula 18: Paquets apertura i tancament 172.16.0.112 ⇔ 172.16.0.115

Bytes d'usuari	
172.16.0.112 ⇔ 172.16.0.115	24 KB

Taula 19: Bytes d'usuari 172.16.0.112 ⇔ 172.16.0.115

Bytes transmesos	
172.16.0.112 ⇔ 172.16.0.115	23 KB
172.16.0.115 ⇔ 172.16.0.112	1136 Bytes

Taula 20: Bytes transmesos 172.16.0.112 ⇔ 172.16.0.115

Sentit comunicació	Cabal brut	Cabal útil
172.16.0.112 ⇔ 172.16.0.115	12044713,54 bytes/s	716458,33 bytes/s
172.16.0.115 ⇔ 172.16.0.112	8875052,08 bytes/s	527916,66 bytes/s

Taula 21: Cabal brut i útil 172.16.0.105 172.16.0.112 ⇔ 172.16.0.115

TCP enviats a la fase de connexió	
Maximum segment size:	1460 Bytes
SACK Permitted Option:	True
Timestamps:	TSval 4997616, TSecr 0
No-Operation:	(NOP)
Window scale:	7 (multiply by 128)

Taula 22: TCP intercanviats durant la fase de connexió 172.16.0.112 ⇔ 172.16.0.115

Nombre de seqüència inicial real	
172.16.0.112 ⇔ 172.16.0.115	38062695
172.16.0.115 ⇔ 172.16.0.112	3635342010

Taula 23: Nombre de seqüència inicial real 172.16.0.112 ⇔ 172.16.0.115

4.5.3 172.16.0.117 ⇔ 172.16.0.124

Paquets apertura		Paquets tancament	
SYN	21081	FIN, PSH, ACK	21262
SYN, ACK	21082	FIN, ACK	21263
ACK	21083	ACK	21266

Taula 24: Paquets apertura i tancament 172.16.0.117 ⇔ 172.16.0.124

Bytes d'usuari	
172.16.0.117 ⇔ 172.16.0.124	17 KB

Taula 25: Bytes d'usuari 172.16.0.117 ⇔ 172.16.0.124

Bytes transmesos	
172.16.0.117 ⇔ 172.16.0.124	16 KB
172.16.0.124 ⇔ 172.16.0.117	654 Bytes

Taula 26: Bytes transmesos 172.16.0.117 ⇔ 172.16.0.124

Sentit comunicació	Cabal brut	Cabal útil
172.16.0.117 ⇔ 172.16.0.124	1049447,40 bytes/s	88907,08 bytes/s
172.16.0.124 ⇔ 172.16.0.117	629668,44 bytes/s	53344,25 bytes/s

Taula 27: Cabal brut i útil 172.16.0.117 ⇔ 172.16.0.124

TCP enviats a la fase de connexió	
Maximum segment size:	1460 Bytes
SACK Permitted Option:	True
Timestamps:	TSval 3223872613, TSecr 0
No-Operation:	(NOP)
Window scale:	7 (multiply by 128)

Taula 28: TCP intercanviats durant la fase de connexió 172.16.0.117 ⇔ 172.16.0.124

Nombre de seqüència inicial real	
172.16.0.117 ⇔ 172.16.0.124	1064479517
172.16.0.124 ⇔ 172.16.0.117	829581103

Taula 29: Nombre de seqüència inicial real 172.16.0.117 ⇔ 172.16.0.124

4.6 Gràfica de trànsit en el temps

Per a generar la gràfica dintre del menú de *statics* s'ha d'escollir l'opció *I/O Graph*. A continuació s'afegeixen els filtres de *tcp*, *udp*, *All Packets* de manera que queda la següent gràfica:

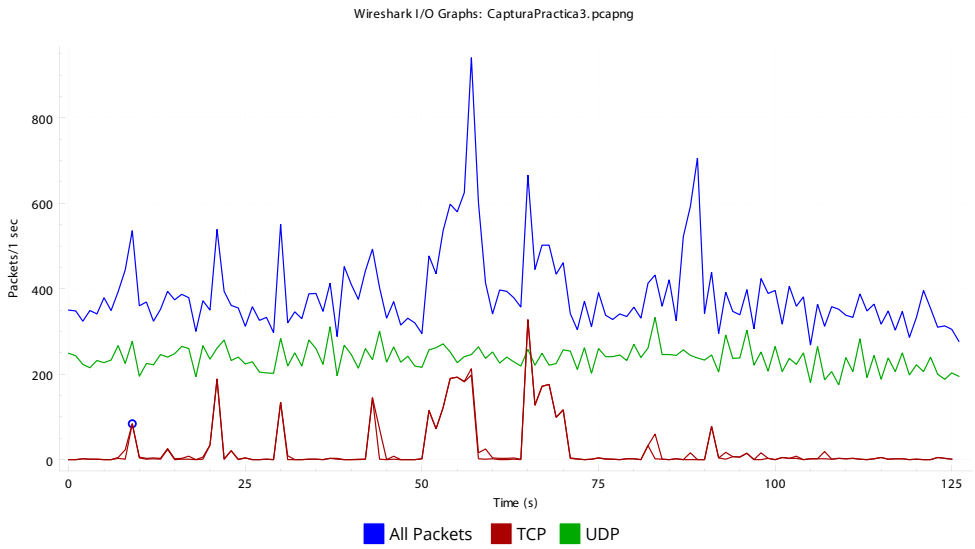


Figura 14: Gràfica trànsit en el temps

5 Conclusió

La realització d'aquesta pràctica m'ha permès observar la gran varietat d'eines que disposa el *Wireshark* i a experimentar la gran utilitat que pot arribar a tenir aquest programa per resoldres problemes relacionats amb les comunicacions. A més a més, el desenvolupament d'aquesta activitat suposa l'adquisició de nocions i competències en la tasca d'anàlisi de trànsit d'una xarxa en un entorn real. Gràcies a aquesta pràctica s'ha aconseguit consolidar i aprofundir en els conceptes adquirits en les sesions de teroría durant tot el curs de xarxes.