

Pràctica 4: Anàlisis de protocols

**Arey Ferrero Ramos
Toni Torres**

17 de desembre del 2019

Tasca 1. Captura amb tcpdump

- **sudo su:** Dóna permisos de superusuari.
- **apt-get install tcpdump:** Permet instal·lar el programa tcpdump. Per a que la instal·lació tingui èxit s'ha de fer des del directori home.
- **tcpdump -s 1500 -w datagrams.txt:** S'activa la captura feta amb el programa TCPdump. Per tal de capturar alguna cosa, s'ha de visitar alguna pàgina web com www.google.cat i www.urv.cat. La captura s'atura amb la comanda Ctrl + C.
- **cat datagrams.txt:** Es mostra per pantalla l'arxiu datagrams.txt. L'arxiu es mostra amb un format no llegible (següent imatge).



```
0:0:0
P0>@F00k0000
00r|=000]70BB^E4B0@AQ
0:0(0"P40@00 000000
0P\=00000]a0BB^E4!@10
00.B000LP]0 0<000
j'D=0000]00BB^E401@00
00.B0000x00|<000
j'D=0000]0<<000000k0k0v
Z00000
Z000]0><<^E0(0p00
0!0
000000]00 <<000)00'BB-00)0000;000000][?<<^E0(0p00
0!0
00
BB^E4V0@0P
0A0000>9P0000'0
BB^E420@0Z000
0:00000 -0<0000+
BB^E40@0jdn
0000000GW0000
BB!E0@E400@<0:0
000<0000 -0000
BB!E0@E40@<H00A0
00000>9P0000
BB!E0@E4Vh@<00000
00000G000000
=00X.0000][?<<^E0(0p00
0!0
00
0#R000]\BB!E0@E4!0@=>0000
P00"00,000P00
00P0000000]@BB!E0@E4!0@=>0000
P00"0hmY00S00P00
00P0000000]#BB!E0@E4!0@=>0000
P00"0000]0P(0
00P0000000]7BB!E0@E4!0@=>0000
P00"0s0000P00
00P0000000]0u BB^E4s@H0
00000P00"0sC000
0b00P0000]Fv BB^E4.0@.0
00000P00"00000
0b00P0000]kv BB^E4E@0
00000PY00S"0hn000
0b00P0000]0v BB^E4
0@0R0
00000P,0"0000
0b00P0000]00 <<000)00'BB-00)0000;000000]00
BB!E0@E4!0@=>0000
P00"0V00C0P00
00P0000000]00
BB^E40_@00
00000P00C0"00000
root@d107:/home/milax/Escriptori#
```

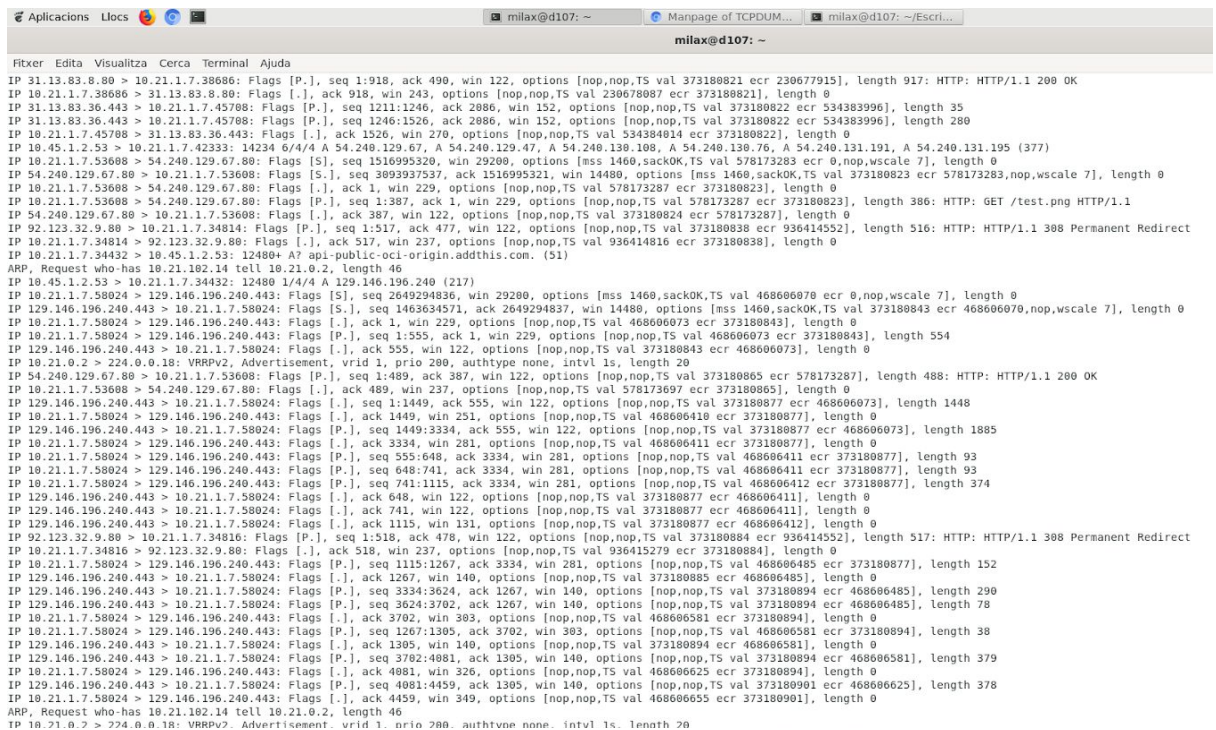
Tasca 2. Mostra de paquets capturats

- **tcpdump -tn -r datagrams.txt:** Permet mostrar el contingut de l'arxiu datagrams.txt seguint un format llegible. El paràmetre **-t** serveix per a que no s'imprimeixi per pantalla el timestamp de cada una de les línies. El paràmetre **-n** serveix per a mostrar les adreces IP de les pàgines web en lloc del seu nom de domini.

Tasca 3. Filtres amb tcpdump

Pots destriar paquets per mitjà de comandes que permeten filtrar la informació:

- **tcpdump -tn -r datagrams.txt tcp port 80** → Filtra els paquets que han passat pel port 80. El protocol http utilitza el protocol TCP.
- **tcpdump -tn -r datagrams.txt tcp port 80 and dst host www.urv.cat** → Filtra els paquets que han passat pel port 80 i dels quals el destí és urv.cat.
- **tcpdump -tn -r datagrams.txt udp port 53 or tcp port 80** → Filtra els paquets que han passat pel port 53 o pel port 80. No es mostren els paquets del protocol ARP. El protocol DNS utilitza el protocol UDP.
- **tcpdump -tn -r datagrams.txt not (dst host www.google.cat)** → Filtra els paquets dels quals el destí no sigui google.cat. El port no té importància.



```
Fixer Edita Visualitza Cerca Terminal Ajuda
milax@d107: ~
IP 31.13.83.0.90 > 10.21.1.7.38686: Flags [P.], seq 1:918, ack 490, win 122, options [nop,nop,TS val 373180821 ecr 230677915], Length 917: HTTP: HTTP/1.1 200 OK
IP 10.21.1.7.38686 > 31.13.83.0.90: Flags [P.], ack 918, win 243, options [nop,nop,TS val 230678087 ecr 373180821], Length 0
IP 31.13.83.36.443 > 10.21.1.7.45788: Flags [P.], seq 1211:1246, ack 2086, win 152, options [nop,nop,TS val 373180822 ecr 534383996], Length 35
IP 31.13.83.36.443 > 10.21.1.7.45788: Flags [P.], seq 1246:1526, ack 2086, win 152, options [nop,nop,TS val 373180822 ecr 534383996], Length 280
IP 10.21.1.7.45788 > 31.13.83.36.443: Flags [P.], ack 1526, win 270, options [nop,nop,TS val 534384014 ecr 373180822], Length 0
IP 10.45.1.2.53 > 10.21.1.7.42333: 14234 6/4/A 54.240.129.67, A 54.240.129.47, A 54.240.130.108, A 54.240.130.76, A 54.240.131.191, A 54.240.131.195 (377)
IP 10.21.1.7.53608 > 54.240.129.67.80: Flags [S], seq 1516995320, win 29200, options [mss 1460,sackOK,TS val 578173283 ecr 0,nop,wscale 7], Length 0
IP 54.240.129.67.80 > 10.21.1.7.53608: Flags [S.], seq 3809937537, ack 1516995321, win 14480, options [mss 1460,sackOK,TS val 373180823 ecr 578173283,nop,wscale 7], Length 0
IP 10.21.1.7.53608 > 54.240.129.67.80: Flags [P.], seq 1:387, ack 1, win 229, options [nop,nop,TS val 578173287 ecr 373180823], Length 0
IP 10.21.1.7.53608 > 54.240.129.67.80: Flags [P.], seq 1:387, ack 1, win 229, options [nop,nop,TS val 578173287 ecr 373180823], Length 386: HTTP: GET /test.png HTTP/1.1
IP 54.240.129.67.80 > 10.21.1.7.53608: Flags [P.], seq 387, win 122, options [nop,nop,TS val 373180824 ecr 578173287], Length 0
IP 10.21.1.7.34814 > 10.21.1.7.34814: Flags [P.], seq 1:517, ack 477, win 122, options [nop,nop,TS val 373180838 ecr 936414552], Length 516: HTTP: HTTP/1.1 308 Permanent Redirect
IP 10.21.1.7.34814 > 92.123.32.9.88: Flags [P.], ack 517, win 237, options [nop,nop,TS val 936414816 ecr 373180838], Length 0
IP 10.21.1.7.34432 > 10.45.1.2.53: 12480* A? api-public-oci-origin.addthis.com. (51)
ARP, Request who-has 10.21.102.14 tell 10.21.0.2, Length 46
IP 10.45.1.2.53 > 10.21.1.7.34432: 12480 1/4/A 129.146.196.240 (217)
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [S], seq 2649294836, win 29200, options [mss 1460,sackOK,TS val 468606070 ecr 0,nop,wscale 7], Length 0
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [S.], seq 1463634571, ack 2649294837, win 14480, options [mss 1460,sackOK,TS val 373180843 ecr 468606070,nop,wscale 7], Length 0
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], ack 1, win 229, options [nop,nop,TS val 468606073 ecr 373180843], Length 0
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], seq 1:555, ack 1, win 229, options [nop,nop,TS val 468606073 ecr 373180843], Length 554
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], ack 555, win 122, options [nop,nop,TS val 373180843 ecr 468606073], Length 0
IP 10.21.0.2 > 224.0.0.18: VRRPV2, Advertisement, vrid 1, prio 200, authtype none, intvl 1s, Length 20
IP 54.240.129.67.80 > 10.21.1.7.53608: Flags [P.], seq 1:489, ack 387, win 122, options [nop,nop,TS val 373180865 ecr 578173287], Length 488: HTTP: HTTP/1.1 200 OK
IP 10.21.1.7.53608 > 54.240.129.67.80: Flags [P.], ack 489, win 237, options [nop,nop,TS val 578173697 ecr 373180865], Length 0
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], seq 1:1449, ack 555, win 122, options [nop,nop,TS val 373180877 ecr 468606073], Length 1448
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], ack 1449, win 231, options [nop,nop,TS val 468606410 ecr 373180877], Length 0
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], seq 1449:3334, ack 555, win 122, options [nop,nop,TS val 373180877 ecr 468606073], Length 1885
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], ack 3334, win 281, options [nop,nop,TS val 468606411 ecr 373180877], Length 0
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], seq 555:648, ack 3334, win 281, options [nop,nop,TS val 468606411 ecr 373180877], Length 93
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], seq 648:741, ack 3334, win 281, options [nop,nop,TS val 468606411 ecr 373180877], Length 93
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], seq 741:1115, ack 3334, win 281, options [nop,nop,TS val 468606412 ecr 373180877], Length 374
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], ack 648, win 122, options [nop,nop,TS val 373180877 ecr 468606411], Length 0
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], ack 741, win 122, options [nop,nop,TS val 373180877 ecr 468606411], Length 0
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], ack 1115, win 131, options [nop,nop,TS val 373180877 ecr 468606412], Length 0
IP 92.123.32.9.88 > 10.21.1.7.34816: Flags [P.], seq 1:518, ack 478, win 122, options [nop,nop,TS val 373180884 ecr 936414552], Length 517: HTTP: HTTP/1.1 308 Permanent Redirect
IP 10.21.1.7.34816 > 92.123.32.9.88: Flags [P.], ack 518, win 237, options [nop,nop,TS val 936415279 ecr 373180884], Length 0
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], seq 1115:1267, ack 3334, win 281, options [nop,nop,TS val 468606485 ecr 373180877], Length 152
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], ack 1267, win 140, options [nop,nop,TS val 373180885 ecr 468606485], Length 0
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], seq 3334:3624, ack 1267, win 140, options [nop,nop,TS val 373180894 ecr 468606485], Length 290
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], seq 3624:3702, ack 1267, win 140, options [nop,nop,TS val 373180894 ecr 468606485], Length 78
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], ack 3702, win 303, options [nop,nop,TS val 468606581 ecr 373180894], Length 0
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], seq 1267:1305, ack 3702, win 303, options [nop,nop,TS val 468606581 ecr 373180894], Length 38
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], ack 1305, win 140, options [nop,nop,TS val 373180894 ecr 468606581], Length 0
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], seq 3702:4081, ack 1305, win 140, options [nop,nop,TS val 373180894 ecr 468606581], Length 379
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], ack 4081, win 326, options [nop,nop,TS val 468606625 ecr 373180894], Length 0
IP 129.146.196.240.443 > 10.21.1.7.58024: Flags [P.], seq 4081:4459, ack 1305, win 140, options [nop,nop,TS val 373180901 ecr 468606625], Length 378
IP 10.21.1.7.58024 > 129.146.196.240.443: Flags [P.], ack 4459, win 349, options [nop,nop,TS val 468606655 ecr 373180901], Length 0
ARP, Request who-has 10.21.102.14 tell 10.21.0.2, Length 46
IP 10.21.0.2 > 224.0.0.18: VRRPV2, Advertisement, vrid 1, prio 200, authtype none, intvl 1s, Length 20
```

Tasca 4. Captura amb Wireshark

S'han trobat dues diferències fonamentals.

- Quan s'atura la captura de paquet, ens hem fixat que quan accedim a `https://www.example.com` després d'haver accedit a `http://www.example.com` no accedim al servidor DNS per a conèixer la IP de la pàgina web. Això, és degut al fet que com hem accedit dos cops a la mateixa pàgina web, el primer cop que hem accedit a aquesta s'ha guardat l'adreça a la caché i per tant la segona vegada que hem d'accedir a aquesta adreça, no accedim al DNS per a conèixer la IP, sinó que accedim a ella directament a partir de les dades de la caché.
- Ens hem trobat que a l'accedir a la web amb protocol HTTPS si fem Follow>SSL Stream veiem les dades del paquet encriptades i no tal com ho fèiem al fer Follow>HTTP Stream quan accedíem per HTTP, que ens permetia veure el codi de la pàgina enviat als paquets. Això és conseqüència de l'encriptació amb doble clau (pública i privada) que fa servir el protocol HTTPS.

-

Tasca 5. Filtrat de paquets

S'analitzen els dos primers paquets del protocol DNS. Al primer paquet el client envia l'adreça (`www.example.com`) de la qual vol la IP. Com que la URV té el seu propi DNS la IP a la qual enviem aquest paquet forma part de la xarxa de la URV. Al segon paquet el DNS ens retorna la IP que correspon a l'adreça demanada pel client.

- **Protocol HTTP:** Es un protocol de transferència que permet fer una petició de dades i recursos. Té la limitació de que quan s'intenta reconstruir una conversa, aquesta es mostra encriptada i no permet veure la informació.

The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like packet list, packet details, packet bytes, and filters. The packet list pane shows two captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
83	22.061728291	10.21.1.7	93.184.216.34	HTTP	578	GET / HTTP/1.1
86	22.326746047	93.184.216.34	10.21.1.7	HTTP	1880	HTTP/1.1 200 OK (text/html)

The packet details pane for the selected packet (No. 83) shows the following structure:

- Frame 83: 578 bytes on wire (4624 bits), 578 bytes captured (4624 bits) on interface 0
- Ethernet II, Src: EncantoN_01:07:01 (00:10:21:01:07:01), Dst: IETF-VRRP-VRLD_01 (00:00:5e:00:01:01)
- Internet Protocol Version 4, Src: 10.21.1.7, Dst: 93.184.216.34
- Transmission Control Protocol, Src Port: 38736, Dst Port: 80, Seq: 1, Ack: 1, Len: 512
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the packet, with a hex dump on the left and a ASCII representation on the right. The ASCII representation shows the following text:

```
GET / HTTP/1.1
Host: www.examp
ple.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8
```

- **Protocol HTTPS:** Es similar al protocol HTTP, però utilitza una encriptació amb clau pública i privada, on el client aconsegueix la clau pública a través d'un certificat. Soluciona el problema que té el protocol anterior al reconstruir una conversa

Aplicacions Llocs milax@d107: ~ Examp

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
78	22.055860746	10.21.1.7	10.45.1.2	DNS	75	Standard query 0x9a51 A www.example.
79	22.057195665	10.45.1.2	10.21.1.7	DNS	139	Standard query response 0x9a51 A www.example.
88	22.371309387	10.21.1.7	10.45.1.2	DNS	72	Standard query 0x4c89 A www.iana.org
90	22.487387866	10.45.1.2	10.21.1.7	DNS	320	Standard query response 0x4c89 A www.iana.org

▶ Frame 78: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
 ▶ Ethernet II, Src: EncantoN 01:07:01 (00:10:21:01:07:01), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
 ▶ Internet Protocol Version 4, Src: 10.21.1.7, Dst: 10.45.1.2
 ▶ User Datagram Protocol, Src Port: 51148, Dst Port: 53
 ▶ Domain Name System (query)

```

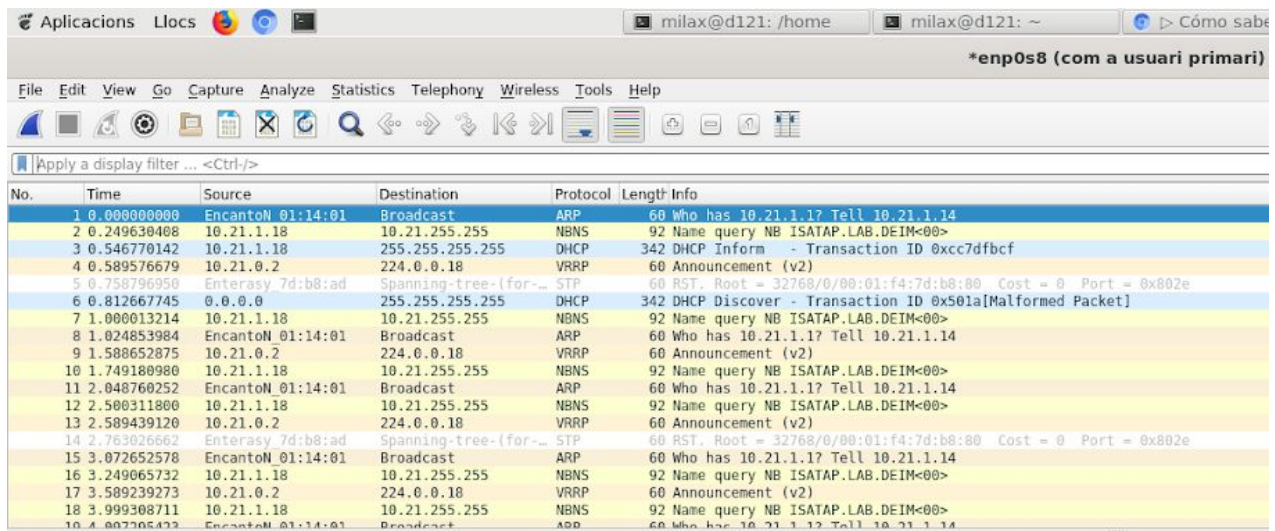
0000  00 00 5e 00 01 01 00 10 21 01 07 01 00 00 45 00  ..^.....!....E-
0010  00 3d cb 1f 40 00 40 11 59 46 0a 15 01 07 0a 2d  -==:@ YF.....
0020  01 02 c7 cc 00 35 00 29 16 85 9a 51 01 00 00 01  ....S.)...Q....
0030  00 00 00 00 00 00 03 77 77 77 07 65 78 61 6d 70  ....www.examp
0040  6c 65 03 63 6f 6d 00 00 01 00 01                le.com-...
  
```

Domain Name System: Protocol

Tasca 6. Anàlisi del tràfic total

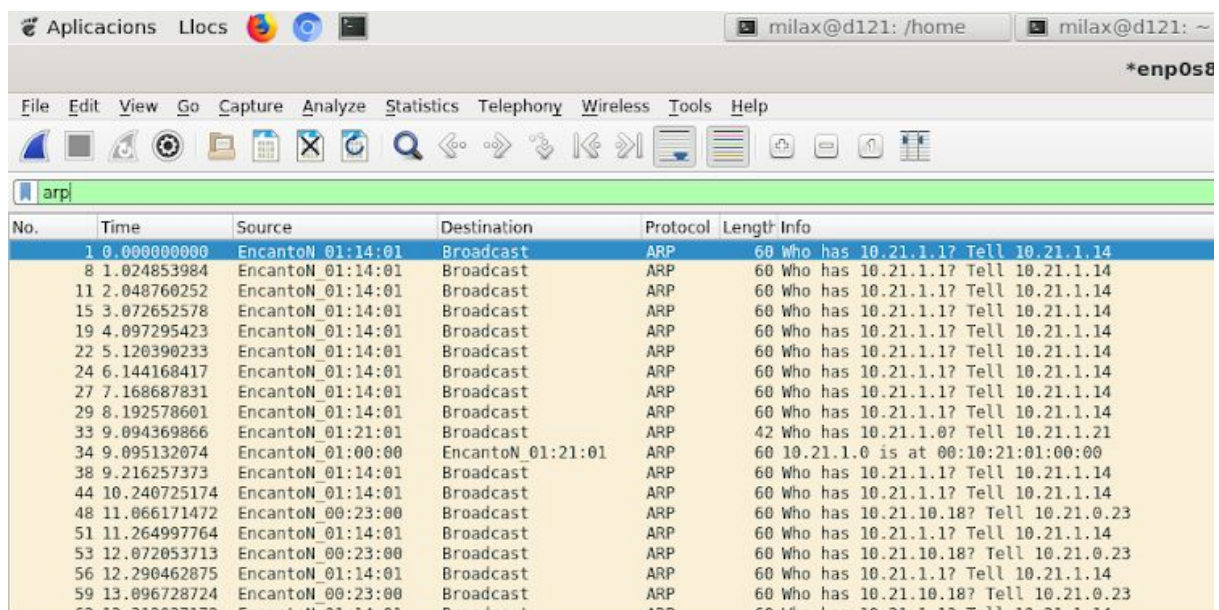
- **apt-get install wireshark:** Permet instal·lar el programa tcpdump. Per a que la instal·lació tingui èxit s'ha de fer des del directori home.

- **sudo -E wireshark:** Permet activar el programa wireshark. Apareixerà tot el tràfic que hi ha a la xarxa d'àrea local a la que està connectada aquest dispositiu.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
2	0.249630408	10.21.1.18	10.21.255.255	NBNS	92	Name query NB ISATAP.LAB.DEIM<00>
3	0.546770142	10.21.1.18	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xcc7dfbcb
4	0.589576679	10.21.0.2	224.0.0.18	VRRP	60	Announcement (v2)
5	0.758796950	Enterasy 7d:b8:ad	Spanning-tree-(for...	STP	60	RST, Root = 32768/0/00:01:f4:7d:b8:80 Cost = 0 Port = 0x802e
6	0.812667745	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x501a[Malformed Packet]
7	1.000013214	10.21.1.18	10.21.255.255	NBNS	92	Name query NB ISATAP.LAB.DEIM<00>
8	1.024853984	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
9	1.588652875	10.21.0.2	224.0.0.18	VRRP	60	Announcement (v2)
10	1.749180980	10.21.1.18	10.21.255.255	NBNS	92	Name query NB ISATAP.LAB.DEIM<00>
11	2.048760252	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
12	2.500311800	10.21.1.18	10.21.255.255	NBNS	92	Name query NB ISATAP.LAB.DEIM<00>
13	2.589439120	10.21.0.2	224.0.0.18	VRRP	60	Announcement (v2)
14	2.763826662	Enterasy 7d:b8:ad	Spanning-tree-(for...	STP	60	RST, Root = 32768/0/00:01:f4:7d:b8:80 Cost = 0 Port = 0x802e
15	3.072652578	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
16	3.249065732	10.21.1.18	10.21.255.255	NBNS	92	Name query NB ISATAP.LAB.DEIM<00>
17	3.589239273	10.21.0.2	224.0.0.18	VRRP	60	Announcement (v2)
18	3.999308711	10.21.1.18	10.21.255.255	NBNS	92	Name query NB ISATAP.LAB.DEIM<00>
19	4.007205423	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14

- **ip a:** Llista totes les interfícies de xarxa d'un dispositiu. Es busca aquella interfície de xarxa que tingui una adreça IP associada i es busca la seva corresponent adreça MAC en el tràfic mostrat pel programa wireshark. Degut a que l'ordinador no ha generat tràfic, no es trobarà cap trama que associada a aquesta adreça MAC.
- **ping 10.21.1.0:** Es genera tràfic de dades contra el dispositiu al que correspon l'adreça IP. Serveix per a comprobar si els dos ordinadors poden establir una connexió a través de la xarxa. La primera vegada que es fa ping contra un ordinador, es veurà que totes les trames enviades entre els dos dispositius segueixen un protocol ARP.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
8	1.024853984	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
11	2.048760252	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
15	3.072652578	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
19	4.097295423	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
22	5.120390233	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
24	6.144168417	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
27	7.168687831	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
29	8.192578601	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
33	9.094369866	EncantoN 01:21:01	Broadcast	ARP	42	Who has 10.21.1.0? Tell 10.21.1.21
34	9.095132074	EncantoN 01:00:00	EncantoN 01:21:01	ARP	60	10.21.1.0 is at 00:10:21:01:00:00
38	9.216257373	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
44	10.240725174	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
48	11.066171472	EncantoN 00:23:00	Broadcast	ARP	60	Who has 10.21.10.18? Tell 10.21.0.23
51	11.264997764	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
53	12.072053713	EncantoN 00:23:00	Broadcast	ARP	60	Who has 10.21.10.18? Tell 10.21.0.23
56	12.290462875	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14
59	13.096728724	EncantoN 00:23:00	Broadcast	ARP	60	Who has 10.21.10.18? Tell 10.21.0.23
62	13.212037173	EncantoN 01:14:01	Broadcast	ARP	60	Who has 10.21.1.1? Tell 10.21.1.14

- **Protocol ARP:** Es el protocolo encarregat d'obtenir l'adreça física (adreça MAC) d'un dispositiu amb el que es vol establir una connexió a partir de la seva adreça IP. Pot funcionar amb broadcast o amb unicast pero, en aquest cas funciona amb broadcast. Si funciona amb broadcast, s'envia un missatge a tots els dispositius connectats a la xarxa en el que es pregunta a quin d'aquests dispositius pertany l'adreça IP que s'incorpora en el missatge. Quan un dels dispositius indica que aquesta adreça IP li correspon a ell, s'estableix la connexió. En el nostre exemple, hi ha un total de 22 paquets ARP dels 98 paquets totals. En conseqüència, el 22,5% del tràfic registrat fa servir protocols ARP.
- **ping 10.21.1.0:** Es torna a generar tràfic de dades contra el dispositiu al que correspon l'adreça IP. Al tornar a fer ping contra el mateix ordinador, es veurà que ara totes les trames enviades segueixen un protocol ICMP. Aquest canvi és degut a que els dos ordinadors han emmagatzemat l'adreça IP de l'altre a la memòria caché.
- **Protocol ICMP:** Es un protocol que serveix per comprovar si existeix connexió de xarxa entre dos dispositius. En cas que no existeix aquesta connexió s'envia un missatge d'error. Es el protocol típicament associat a la comanda ping.

Tasca 7. Anàlisi d'un ping

- Analitzeu una captura que hagueu fet mentre s'executa dos pings:
 - Un ping serà contra una màquina Linux
 - Un altre ping contra una màquina Windows
 - (el professor us anotarà les IP a la pissarra)
- Primer de tot hem de activar les peticions ICMP perquè si no no ens surtiran aquests paquets a wireshark. Per establir la connexió amb un ordinador que utilitzi el sistema operatiu Windows s'ha de desactivar el tallafocs d' aquest ordinador.

✓ Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impres...	Domí...	Sí	Permitir	No
✓ Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impres...	Priva...	Sí	Permitir	No
✓ Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada)	Compartir archivos e impres...	Domí...	Sí	Permitir	No
✓ Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada)	Compartir archivos e impres...	Priva...	Sí	Permitir	No

- Quines dades transporta el datagrama?

El protocol ICMP, com hem comentat abans, és una subprotocol del protocol IP, és per això que als paquets ICMP podem distingir dos conjunts de dades: la capçalera IP i el subpaquet ICMP.

– Utilitza UDP, TCP...?

Es fa servir el ICMP (Internet Control Message Protocol)

– On trobareu el valor del TTL? Quines diferències trobeu a nivell de TTL entre la màquina Windows i la Linux?

El valor de TTL el trobem en el protocol ICMP.

- De Linux a Linux TTL=64,
- De windows a Linux TTL=122
- De Linux a windows TTL=64

El time to leave(TTL) té l'objectiu d'evitar bucles infinits causats per un mal enrutament. El host estableix un TTL específic i en cada salt a un host diferent el TTL disminueix en 1, si el TTL arriba a 0 el router ha de retornar un missatge ICMP de "time exceeded".