

PRÁCTICA 1

Ejercicio 1

The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows several TCP and DNS packets between IP addresses 150.244.214.237 and 192.168.174.130. The selected packet is a DNS query response from 192.168.174.130 to 192.168.174.2 on port 53. The packet details pane shows the standard query response for 0xa161 A www.uam.es A 150.244.214.237.

No.	Time	Source	Destination	Protocol	Length	PO	PD	Info
10	2.155156427	150.244.214.237	192.168.174.130	TCP	60	80	1815	80 → 1815 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7	1.135580827	150.244.214.237	192.168.174.130	TCP	60	80	1814	80 → 1814 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4	0.148084852	150.244.214.237	192.168.174.130	TCP	60	80	1813	80 → 1813 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2	0.031709859	192.168.174.2	192.168.174.130	DNS	86	53	33560	Standard query response 0xa161 A www.uam.es A 150.244.214.237
1	0.000000000	192.168.174.130	192.168.174.2	DNS	70	33560	53	Standard query 0xa161 A www.uam.es
11	2.155184644	192.168.174.130	150.244.214.237	TCP	54	1815	80	1815 → 80 [RST] Seq=1 Win=0 Len=0
9	2.069484706	192.168.174.130	150.244.214.237	TCP	54	1815	80	1815 → 80 [SYN] Seq=0 Win=512 Len=0
8	1.135609069	192.168.174.130	150.244.214.237	TCP	54	1814	80	1814 → 80 [RST] Seq=1 Win=0 Len=0
6	1.067757461	192.168.174.130	150.244.214.237	TCP	54	1814	80	1814 → 80 [SYN] Seq=0 Win=512 Len=0
5	0.148121520	192.168.174.130	150.244.214.237	TCP	54	1813	80	1813 → 80 [RST] Seq=1 Win=0 Len=0
3	0.066279605	192.168.174.130	150.244.214.237	TCP	54	1813	80	1813 → 80 [SYN] Seq=0 Win=512 Len=0

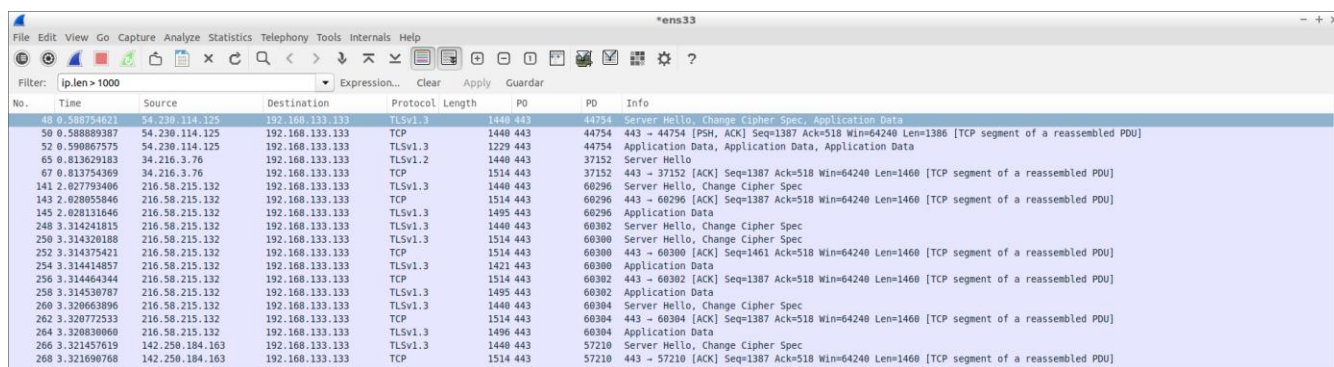
Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Vmware_eb:f2:74 (00:50:56:eb:f2:74), Dst: Vmware_46:3a:97 (00:0c:29:46:3a:97)
Internet Protocol Version 4, Src: 192.168.174.2, Dst: 192.168.174.130
User Datagram Protocol, Src Port: 53, Dst Port: 33560
Source Port: 53
Destination Port: 33560
Length: 52
Checksum: 0xf84b [unverified]
[Checksum Status: Unverified]
Standard query response 0xa161 A www.uam.es A 150.244.214.237
0000 00 0c 29 46 3a 97 00 50 56 eb f2 74 08 00 45 00 ...F...P V...t..E.
0010 00 48 0a ac 00 00 00 11 52 23 c0 a8 ae 02 c0 a8 ...H.....Rf.....
0020 ae 02 00 35 83 18 00 34 f8 4b a1 61 81 00 00 01 ...4.K.a....
0030 00 01 00 00 00 00 03 77 77 77 03 75 61 60 02 65w ww.uam.e
0040 73 00 00 01 00 01 c0 0c 00 01 00 01 00 00 05 s.....
0050 00 04 96 f4 d6 ed
Source Port (udp.srcport), 2 b... Packets: 11 · Displayed: 11 (100,0%) · Dropped: 0 (0,0%) Profile: Default

En la imagen no se muestran los paquetes en orden, se puede apreciar que los paquetes de protocolo TCP son intercambiados entre nosotros – con IP 192.168.174.138 – y el servidor de la UAM – con IP 150.244.214.237 -. Asimismo, se observa que el puerto de origen de los paquetes emitidos por los servidores de la universidad tiene puerto 80, mientras que nosotros hemos transmitido desde los puertos 1815, 1814 y 1813. Cabe destacar que la IP 150.244.214.237 recibe el doble de paquetes de los que entrega.

Una vez seguido el procedimiento indicado y añadidas las dos columnas con puertos de origen y destino, se puede observar un paquete con PO 53 – el paquete seleccionado en la imagen -. No se han encontrado problemas durante la realización del ejercicio, y el procedimiento realizado es exactamente el indicado en el enunciado.

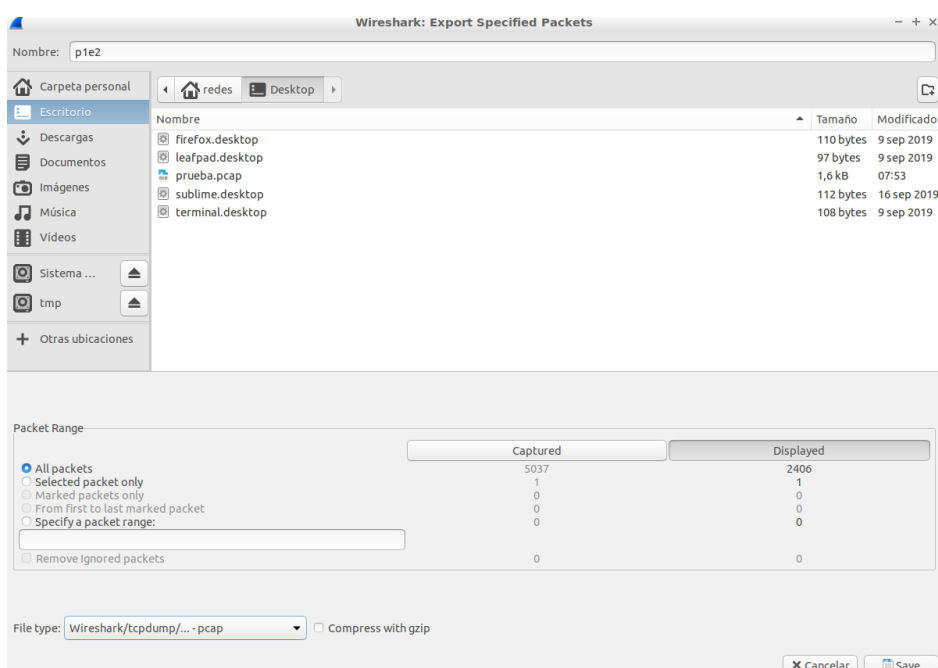
Ejercicio 2

2.1 El filtro empleado es **ip.len > 1000**, que selecciona aquellos paquetes de tipo IP con un tamaño mayor a 1000 bytes. Se puede apreciar su uso en la parte superior izquierda de la imagen, en el campo *Filter*.



2.2 El proceso para exportar los paquetes filtrados es:

File -> Export specified packets -> marcar la opción displayed



2.3 Tomando cinco paquetes, se observa que hay una diferencia igual en todos los paquetes.

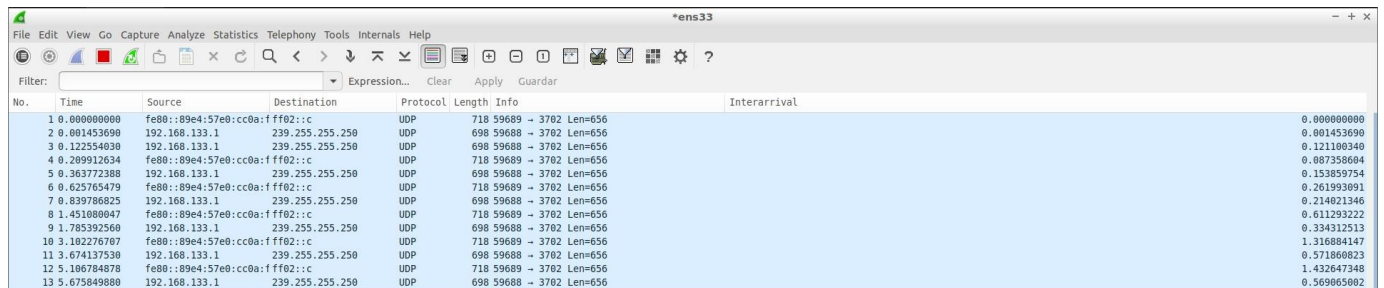
<i>Captured lenght</i>	<i>Campo ip.len</i>	<i>Diferencia (lenght – ip.len)</i>
1440	1426	14
1494	1480	14
1514	1500	14
1440	1426	14
1514	1500	14

Cabe destacar que en la imagen se muestran a partir del paquete 48. La tabla recoge los valores de los primeros paquetes.

Ejercicio 3

El procedimiento seguido para añadir la columna es:

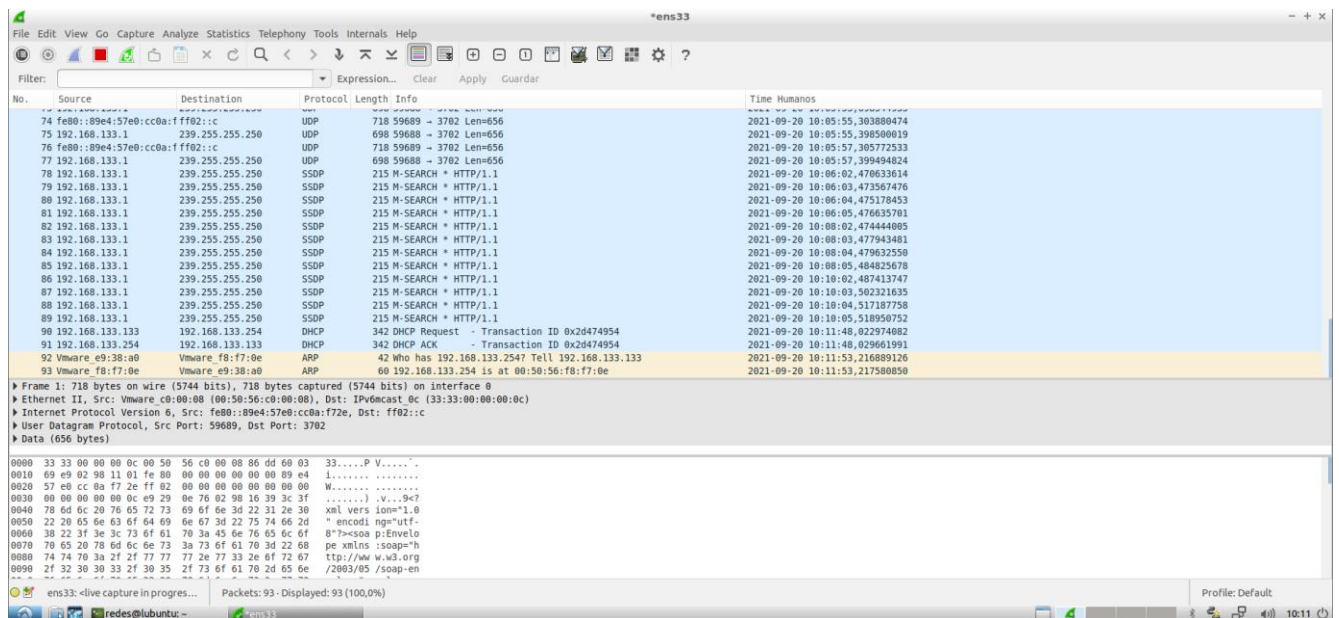
Edit -> Preferences -> User interface -> Columns -> Add Column -> tipo Delta Time (diferencia de tiempo) -> nombre *Interarrival*



No.	Time	Source	Destination	Protocol	Length	Info	Interarrival
1	0.000000000	fe80::89e4:57e0:cc0a:fff02::c	192.168.133.1	UDP	718	59689 → 3702 Len=656	0.000000000
2	0.001453690	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	0.001453690
3	0.122554630	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	0.121106940
4	0.209912634	fe80::89e4:57e0:cc0a:fff02::c	192.168.133.1	UDP	718	59689 → 3702 Len=656	0.087358604
5	0.363772388	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	0.153859754
6	0.625765479	fe80::89e4:57e0:cc0a:fff02::c	192.168.133.1	UDP	718	59689 → 3702 Len=656	0.261993091
7	0.839786825	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	0.214021346
8	1.451080647	fe80::89e4:57e0:cc0a:fff02::c	192.168.133.1	UDP	718	59689 → 3702 Len=656	0.611293222
9	1.785392560	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	0.334312513
10	3.102276707	fe80::89e4:57e0:cc0a:fff02::c	192.168.133.1	UDP	718	59689 → 3702 Len=656	1.316804147
11	3.674137530	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	0.571860823
12	5.106784878	fe80::89e4:57e0:cc0a:fff02::c	192.168.133.1	UDP	718	59689 → 3702 Len=656	1.432647348
13	5.675849880	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	0.569065002

Ejercicio 4

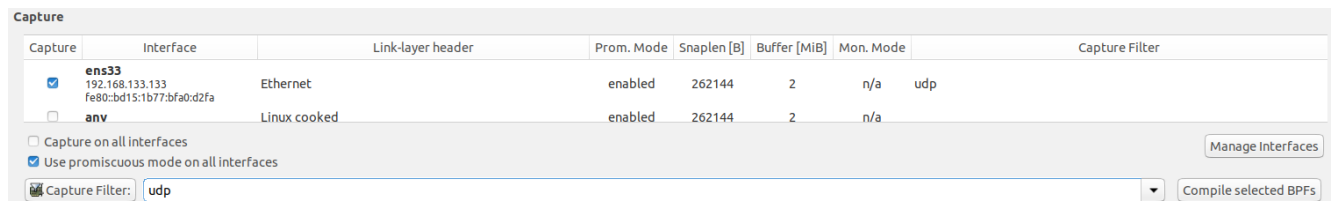
Cambiamos el tipo de columna a UTC date and time y así vemos la fecha con el tiempo de los humanos y el tiempo de UNIX.



No.	Source	Destination	Protocol	Length	Info	Time Humanos
74	fe80::89e4:57e0:cc0a:fff02::c	192.168.133.1	UDP	718	59689 → 3702 Len=656	2021-09-20 10:05:55.303880474
75	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	2021-09-20 10:05:55.398500019
76	fe80::89e4:57e0:cc0a:fff02::c	192.168.133.1	UDP	718	59689 → 3702 Len=656	2021-09-20 10:05:57.305772533
77	192.168.133.1	239.255.255.250	UDP	698	59688 → 3702 Len=656	2021-09-20 10:05:57.399494024
78	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:06:02.470633614
79	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:06:03.473567476
80	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:06:04.475178453
81	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:06:05.476635701
82	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:08:02.474444005
83	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:08:03.477943401
84	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:08:04.479632550
85	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:08:05.484825678
86	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:10:02.487413747
87	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:10:03.502321635
88	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:10:04.517187758
89	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:18:05.518950752
90	192.168.133.133	192.168.133.254	DHCP	342	DHCP Request - Transaction ID 0x26474954	2021-09-20 10:11:48.022974082
91	192.168.133.254	192.168.133.133	DHCP	342	DHCP ACK - Transaction ID 0x26474954	2021-09-20 10:11:48.029661991
92	Vmware e9:38:a0	Vmware f8:f7:0e	ARP	42	Who has 192.168.133.254? Tell 192.168.133.133	2021-09-20 10:11:53.216889126
93	Vmware f8:f7:0e	Vmware e9:38:a0	ARP	60	192.168.133.254 is at 00:50:56:f8:f7:0e	2021-09-20 10:11:53.217580850

Ejercicio 5

Como se ve subrayado, el protocolo de los paquetes que captura son de tipo UDP. Para conseguir esto hemos puesto en Capture filters **udp**.



Capture	Interface	Link-layer header	Prom. Mode	Snapplen [B]	Buffer [MiB]	Mon. Mode	Capture Filter
<input checked="" type="checkbox"/> ens33	192.168.133.133	Ethernet	enabled	262144	2	n/a	udp
<input type="checkbox"/> anv		Linux cooked	enabled	262144	2	n/a	

☐ Capture on all interfaces
☒ Use promiscuous mode on all interfaces

Capture Filter: **udp** Compile selected BPFs

AUTORES: ALBERTO RUEDA Y EDUARDO TERRES
PRÁCTICAS REDES DE COMUNICACIONES I

Capturing from ens33 (udp)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Guardar

No.	Source	Destination	Protocol	Length	Info	Time	Humanos
1	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:20:03,505698915	
2	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:20:04,507926670	
3	192.168.133.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1	2021-09-20 10:20:05,512025729	
4	192.168.133.133	192.168.133.2	DNS	95	Standard query 0x96ad A detectportal.firefox.com OPT	2021-09-20 10:20:15,905688389	
5	192.168.133.133	192.168.133.2	DNS	95	Standard query 0xa0b2 AAAA detectportal.firefox.com OPT	2021-09-20 10:20:15,906318130	
6	192.168.133.2	192.168.133.133	DNS	190	Standard query response 0xa0b2 AAAA detectportal.firefox.com CNAME	2021-09-20 10:20:15,919082139	
7	192.168.133.2	192.168.133.133	DNS	206	Standard query response 0x96ad A detectportal.firefox.com CNAME	2021-09-20 10:20:15,919186014	
8	192.168.133.133	192.168.133.2	DNS	113	Standard query 0x42a6 AAAA prod.detectportal.prod.cloudops.mozgc	2021-09-20 10:20:15,919539546	
9	192.168.133.2	192.168.133.133	DNS	113	Standard query response 0x42a6 AAAA prod.detectportal.prod.cloud	2021-09-20 10:20:15,930631619	
10	192.168.133.133	192.168.133.2	DNS	100	Standard query 0x3f5d A location.services.mozilla.com OPT	2021-09-20 10:20:16,309079600	
11	192.168.133.133	192.168.133.2	DNS	100	Standard query 0x0cc6 AAAA locprod2-elb-us-west-2.prod.mozaws	2021-09-20 10:20:16,315268570	
12	192.168.133.2	192.168.133.133	DNS	234	Standard query response 0x0cc6 AAAA location.services.mozilla.cc	2021-09-20 10:20:16,315268570	
13	192.168.133.2	192.168.133.133	DNS	248	Standard query response 0x3f5d A location.services.mozilla.com	2021-09-20 10:20:16,315302710	
14	192.168.133.133	192.168.133.2	DNS	109	Standard query 0x2d35 AAAA locprod2-elb-us-west-2.prod.mozaws	2021-09-20 10:20:16,315585048	
15	192.168.133.2	192.168.133.133	DNS	194	Standard query response 0x2d35 AAAA locprod2-elb-us-west-2.prod	2021-09-20 10:20:16,324348818	
16	192.168.133.133	192.168.133.2	DNS	100	Standard query 0xfbb2 A firefox.settings.services.mozilla.com	2021-09-20 10:20:16,395662375	
17	192.168.133.133	192.168.133.2	DNS	108	Standard query 0x95ec AAAA firefox.settings.services.mozilla.com	2021-09-20 10:20:16,395894865	
18	192.168.133.2	192.168.133.133	DNS	192	Standard query response 0x95ec AAAA firefox.settings.services.moz	2021-09-20 10:20:16,401775377	
19	192.168.133.2	192.168.133.133	DNS	172	Standard query response 0xfbb2 A firefox.settings.services.mozil	2021-09-20 10:20:16,401799389	
20	192.168.133.133	192.168.133.2	DNS	86	Standard query 0xe12c A www.mozilla.org OPT	2021-09-20 10:20:16,646496933	
21	192.168.133.133	192.168.133.2	DNS	86	Standard query 0xe12c A www.mozilla.org OPT	2021-09-20 10:20:16,646733613	

Internet Protocol Version 4, Src: 192.168.133.133, Dst: 192.168.133.2

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 86
Identification: 0x832e (33582)
Flags: 0x4000, Don't fragment
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x2b90 [validation disabled]

0000 00 50 56 ea 2d 8c 00 0c 29 e9 38 a0 08 00 45 00 .PV....).B...E.
0010 00 56 83 2e 40 00 40 11 2b 90 c0 a8 85 85 c0 a8 .V..@.@+.....
0020 85 02 c0 c2 00 35 00 42 53 b4 0c c6 01 00 00 01S.B S.....
0030 00 00 00 00 01 08 6c 6f 63 61 74 09 6f 6e 08l ocation...
.... ..

ens33: <live capture in progres... Packets: 477 - Displayed: 477 (100,0%)

Profile: Default

10:22