

EJERCICIO DE REDES -DNS-

Alejandro Rodríguez Rojas

Sumario

1 Introducci3n.....4

2 Comando Dig.....4

3 Wireshark.....6

1 Introducción

Vamos a utilizar el comando “dig” para verificar que las IP de www.marca.com y www.elmundo.es son iguales.

Para utilizar el comando dig deberemos instalar “dnsutils”:

```
#:apt-get install dnsutils
```

Acto seguido utilizaremos wireshark para verificar el dns de la red www.elmundo.es , para ello debemos instalar el paquete wireshark

```
#:apt-get install wireshark
```

Para ejecutar wireshark tendremos que entrar como root y escribir en la terminal:

```
#:wireshark
```

2 Comando Dig

Para verificar que ambas paginas se alojan en un mismo servidor debemos utilizar el comando dig:

```
dig www.marca.com
```

```
dig www.elmundo.es
```

Utilizaremos dig @1.1.1.1 {Nombre de web}, ya que marca es inutilizable

```
alexrr@pc-alex:~$ dig @1.1.1.1 www.marca.com
; <<>> DiG 9.11.4-P2-3-bpo9+1-Debian <<>> @1.1.1.1 www.marca.com
; (1 server found)
; global options: +cmd
; Got answer:
; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 60234
; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
; QUESTION SECTION:
;www.marca.com.                IN      A
;
; ANSWER SECTION:
www.marca.com.                215     IN      CNAME   marca.edgekey.net.
marca.edgekey.net.            4679    IN      CNAME   e14650.dscj.akamaiedge.net.
e14650.dscj.akamaiedge.net.  23     IN      A        23.60.213.152
; Query time: 250 msec
; SERVER: 1.1.1.1#53(1.1.1.1)
; WHEN: mar dic 18 09:07:10 CET 2018
; MSG SIZE rcvd: 126

alexrr@pc-alex:~$ dig @1.1.1.1 www.elmundo.es
; <<>> DiG 9.11.4-P2-3-bpo9+1-Debian <<>> @1.1.1.1 www.elmundo.es
; (1 server found)
; global options: +cmd
; Got answer:
; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 11331
; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
; QUESTION SECTION:
;www.elmundo.es.              IN      A
;
; ANSWER SECTION:
www.elmundo.es.              67      IN      CNAME   elmundo.edgekey.net.
elmundo.edgekey.net.         4727    IN      CNAME   e14650.dscj.akamaiedge.net.
e14650.dscj.akamaiedge.net.  14      IN      A        23.60.213.152
; Query time: 143 msec
; SERVER: 1.1.1.1#53(1.1.1.1)
; WHEN: mar dic 18 09:07:37 CET 2018
; MSG SIZE rcvd: 129

alexrr@pc-alex:~$
```

Como podemos observar, ambos tienen un mismo servidor conjunto, que es la IP:

23.60.213.152

3 Wireshark

Para utilizar Wireshark primero debemos instalarlo, para ello ejecutamos una terminal en nuestro sistema Linux y escribimos el siguiente comando:

```
#:apt-get install wireshark
```

Al instalarlo deberemos ejecutarlo como root escribiendo wireshark en la terminal o accediendo mediante superusuario al programa(Si no estas en superusuario no te detectará la tarjeta de red).

```
alexrr@pc-alex:~$ sudo wireshark
[sudo] password for alexrr:

```



Seleccionamos la tarjeta de red y ya estará wireshark escuchando.

No.	Time	Source	Destination	Protocol	Length	Info
47	6.443320952	172.22.1.248	192.168.102.2	DNS	74	Standard query 0xb563 A www.elmundo.es
48	6.44332085	172.22.1.248	192.168.102.2	DNS	74	Standard query 0x237c AAAA www.elmundo.es
49	6.442970756	192.168.102.2	172.22.1.248	DNS	484	Standard query response 0xb563 A www.elmundo.es CNAME elmundo.edgekey.net CNAME e14450.dscj.akamaiedge.net A 92.123.218.83 NS ns5dscj.akamaiedge.net NS ns4dscj.akamaiedge.net NS ns2dscj.akamaiedge.net
50	6.442970682	192.168.102.2	172.22.1.248	DNS	524	Standard query response 0x237c AAAA www.elmundo.es CNAME elmundo.edgekey.net CNAME e14650.dscj.akamaiedge.net AAAA 2001:1498:13:189::393a AAAA 2001:1498:13:184::393a NS ns5dscj.akamaiedge.net
51	6.443301877	2001:1498:13:189::3	2001:1498:13:189::3	TCP	94	38876 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1096286179 TSecr=0 WS=128
53	6.559484897	2001:1498:13:189::3	2001:1498:13:189::3	TCP	94	38878 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1096286295 TSecr=0 WS=128
57	6.708310863	2001:1498:13:189::3	2001:1498:13:189::3	TCP	94	38880 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1096286436 TSecr=0 WS=128
58	6.728259992	2001:1498:13:189::3	2001:1498:13:189::3	TCP	94	80 → 38876 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1523421919 TSecr=1096286179 WS=128
59	6.728280769	2001:1498:13:189::3	2001:1498:13:189::3	TCP	86	38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286456 TSecr=1523421919
60	6.777276539	2001:1498:13:189::3	2001:1498:13:189::3	TCP	94	80 → 38878 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1523421980 TSecr=1096286295 WS=128
61	6.777336671	2001:1498:13:189::3	2001:1498:13:189::3	TCP	86	38878 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286513 TSecr=1523421980
62	6.823688959	2001:1498:13:189::3	2001:1498:13:189::3	TCP	94	80 → 38880 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1421791760 TSecr=1096286436 WS=128
63	6.823711008	2001:1498:13:189::3	2001:1498:13:189::3	TCP	86	38880 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286500 TSecr=1421791760
65	7.396674472	2001:1498:13:189::3	2001:1498:13:189::3	TCP	1514	38878 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=1428 TSval=1096287127 TSecr=1523421919 [TCP segment of a reassembled PDU]
66	7.396678370	2001:1498:13:189::3	2001:1498:13:189::3	HTTP	765	GET / HTTP/1.1
67	7.391704330	2001:1498:13:189::3	2001:1498:13:189::3	ICMPv6	1284	Packet Too Big
68	7.391114543	2001:1498:13:189::3	2001:1498:13:189::3	TCP	1494	[TCP Out-of-Order] 38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=1408 TSval=1096287127 TSecr=1523421919
69	7.391115698	2001:1498:13:189::3	2001:1498:13:189::3	TCP	785	[TCP Retransmission] 38876 → 80 [PSH, ACK] Seq=1408 Ack=1 Win=28800 Len=880 TSval=1096287127 TSecr=1523421919
70	7.405149537	2001:1498:13:189::3	2001:1498:13:189::3	TCP	86	38876 → 80 [FIN, ACK] Seq=2108 Ack=1 Win=28800 Len=0 TSval=1096287141 TSecr=1523421919
71	7.406319089	2001:1498:13:189::3	2001:1498:13:189::3	TCP	94	20212 → 443 [SYN] Seq=0 Win=28400 Len=0 MSS=1420 SACK_PERM=1 TSval=1096287142 TSecr=0 WS=128

▶ Frame 47: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶ Ethernet II, Src: LcfcHefe_ea:aa:a0 (8c:16:45:ea:aa:a0), Dst: Dell_3b:c9:43 (00:25:64:3b:c9:43)
▶ Internet Protocol Version 4, Src: 172.22.1.248, Dst: 192.168.102.2
▶ User Datagram Protocol, Src Port: 14205, Dst Port: 53
▶ Domain Name System (query)

0000	00 25 64 3b c9 43 8c 16 45 ea a0 00 00 00 45 00	%d; C...E....E
0010	00 3c 1e fc 40 00 40 11 46 fc ac 16 01 fe c0 a8	<< @ @ F.....
0020	66 02 37 7d 00 00 35 00 28 fe c7 b5 63 01 00 00 01	f 7) S' (...C....
0030	00 00 00 00 00 00 03 77 77 77 07 65 6c 6d 75 9eW w elmun
0040	64 6f 62 65 73 00 00 01 00 01	do es

Hypertext Transfer Protocol: Protocol Packets: 5024 · Displayed: 4898 (97.5%) · Dropped: 0 (0.0%) Profile: Default

Filtramos por dns, tcp y http y ya tendremos la captura lista.

*enp7s0

File Edit View Go Capture Analyse Statistics Telephony Wireless Tools Help

dns || tcp || http

No.	Time	Source	Destination	Protocol	Length	Info
47	6.442320952	172.22.1.248	192.168.102.2	DNS	74	Standard query 0xb563 A www.elmundo.es
48	6.442332885	172.22.1.248	192.168.102.2	DNS	74	Standard query 0x237c AAAA www.elmundo.es
49	6.442970756	192.168.102.2	172.22.1.248	DNS	484	Standard query response 0xb563 A www.elmundo.es CNAME elmundo.edgekey.net CNAME e14650.dscj.akamaiedge.net A 92.123.218.83 NS n5dscj.akamaiedge.net NS n4dscj.akamaiedge.net NS n2dscj.aka.
50	6.442982682	192.168.102.2	172.22.1.248	DNS	524	Standard query response 0x237c AAAA www.elmundo.es CNAME elmundo.edgekey.net CNAME e14650.dscj.akamaiedge.net AAAA 2001:1408:13:189::393a AAAA 2001:1408:13:184::393a NS n5dscj.akamaiedge..
51	6.44301877	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	94	38876 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1096286179 TSecr=0 WS=128
53	6.559484897	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	94	38876 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1096286295 TSecr=0 WS=128
57	6.708310863	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	94	38880 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1096286436 TSecr=0 WS=128
58	6.720259992	2001:1408:13:189::3.	2001:470:ccba:0:8e9.	TCP	94	80 → 38876 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1523421919 TSecr=1096286179 WS=128
59	6.720280769	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	86	38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286456 TSecr=1523421919
60	6.777276539	2001:1408:13:189::3.	2001:470:ccba:0:8e9.	TCP	94	80 → 38876 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1523421980 TSecr=1096286295 WS=128
61	6.777336671	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	86	38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286513 TSecr=1523421980
62	6.823668959	2001:1408:13:189::3.	2001:470:ccba:0:8e9.	TCP	94	80 → 38880 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1421791760 TSecr=1096286436 WS=128
63	6.823711088	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	86	38880 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286560 TSecr=1421791760
65	7.390674472	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	1514	38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=1428 TSval=1096287127 TSecr=1523421919 [TCP segment of a reassembled PDU]
66	7.390678370	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	HTTP	765	GET / HTTP/1.1
67	7.391079430	2001:470:ccba::1	2001:470:ccba:0:8e9.	ICMPv6	1294	Packet Too Big
68	7.39114543	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	1494	[TCP Out-Of-Order] 38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=1408 TSval=1096287127 TSecr=1523421919

El ejercicio se resolvería así:

No.	Time	Source	Destination	Protocol	Length	Info
47	6.442320952	172.22.1.248	192.168.102.2	DNS	74	Standard query 0xb563 A www.elmundo.es
48	6.442332885	172.22.1.248	192.168.102.2	DNS	74	Standard query 0x237c AAAA www.elmundo.es
49	6.442970756	192.168.102.2	172.22.1.248	DNS	484	Standard query response 0xb563 A www.elmundo.es CNAME elmundo.edgekey.net CNAME e14650.dscj.akamaiedge.net A 92.123.218.83 NS n5dscj.akamaiedge.net NS n4dscj.akamaiedge.net NS n2dscj.aka.
50	6.442982682	192.168.102.2	172.22.1.248	DNS	524	Standard query response 0x237c AAAA www.elmundo.es CNAME elmundo.edgekey.net CNAME e14650.dscj.akamaiedge.net AAAA 2001:1408:13:189::393a AAAA 2001:1408:13:184::393a NS n5dscj.akamaiedge..
53	6.559484897	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	94	38876 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1096286295 TSecr=0 WS=128
57	6.708310863	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	94	38880 → 80 [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1096286436 TSecr=0 WS=128
58	6.720259992	2001:1408:13:189::3.	2001:470:ccba:0:8e9.	TCP	94	80 → 38876 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1523421919 TSecr=1096286179 WS=128
59	6.720280769	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	86	38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286456 TSecr=1523421919
60	6.777276539	2001:1408:13:189::3.	2001:470:ccba:0:8e9.	TCP	94	80 → 38876 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1523421980 TSecr=1096286295 WS=128
61	6.777336671	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	86	38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286513 TSecr=1523421980
62	6.823668959	2001:1408:13:189::3.	2001:470:ccba:0:8e9.	TCP	94	80 → 38880 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1421791760 TSecr=1096286436 WS=128
63	6.823711088	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	86	38880 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1096286560 TSecr=1421791760
65	7.390674472	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	1514	38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=1428 TSval=1096287127 TSecr=1523421919 [TCP segment of a reassembled PDU]
66	7.390678370	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	HTTP	765	GET / HTTP/1.1
67	7.391079430	2001:470:ccba::1	2001:470:ccba:0:8e9.	ICMPv6	1294	Packet Too Big
68	7.39114543	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	1494	[TCP Out-Of-Order] 38876 → 80 [ACK] Seq=1 Ack=1 Win=28800 Len=1408 TSval=1096287127 TSecr=1523421919
69	7.39115599	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	785	[TCP Retransmission] 38876 → 80 [PSH, ACK] Seq=1409 Ack=1 Win=28800 Len=699 TSval=1096287127 TSecr=1523421919
70	7.495149537	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	86	38876 → 80 [FIN, ACK] Seq=2108 Ack=1 Win=28800 Len=0 TSval=1096287141 TSecr=1523421919
71	7.498319089	2001:470:ccba:0:8e9.	2001:1408:13:189::3.	TCP	94	28212 → 443 [SYN] Seq=0 Win=28400 Len=0 MSS=1420 SACK_PERM=1 TSval=1096287142 TSecr=0 WS=128

El cuadrado azul representa el DNS hacia el servidor, el cuadrado amarillo representa la resolución TCP, (SYN_ACK y ACK) y la verde representa la resolución HTTP

4 Conclusión

Con esto hemos aprendido a utilizar wireshark y verificar que los servidores de marca y elmundo son los mismos.