

Φίλιππος Δουραχαλής

3170045

1. Η χρονική διάρκεια της ανίχνευσης όπως φαίνεται από τις ιδιότητες του αρχείου καταγραφής ήταν 33 δευτερόλεπτα

Time

First packet: 2020-01-17 15:16:45
Last packet: 2020-01-17 15:17:18
Elapsed: 00:00:33

2. Τα πρωτόκολλα που χρησιμοποιούνται είναι τα εξής:

<u>Επίπεδο</u>	Εφαρμογής	<u>Πρωτόκολλα</u>		
		Μεταφοράς	Διαδικτύου	Σύνδεσης
	SSL	UDP	IPv4	ARP
	DNS	TCP	IPv6	
		TLSv1.2	ICMP v6	
			ICMP	

3. Το πρωτόκολλο DNS σε επίπεδο μεταφοράς χρησιμοποιεί το πρωτόκολλο UDP

Το πρωτόκολλο SSL χρησιμοποιεί σε επίπεδο μεταφοράς το πρωτόκολλο TCP

4. Πακέτα TCP που στάλθηκαν : 76

Πακέτα UDP που στάλθηκαν : 14

5. Τα διαφορετικά endpoints σε επίπεδο Ethernet που υπάρχουν είναι : 6, τα ονόματα των οποίων είναι τα εξής:

Ethernet · 6		IPv6 · 4		TCP · 16		UDP · 17	
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	
MitsumiE_e5:4f:0a	3	126	3	126	0	0	
IntelCor_51:6a:80	3	4386	3	4386	0	0	
Technico_5a:cc:a0	232	77 k	119	50 k	113	26 k	
LiteonTe_a2:26:3c	227	77 k	113	26 k	114	50 k	
HuaweiTe_39:87:db	2	84	2	84	0	0	
Broadcast	13	4806	0	0	13	4806	

☒ Name resolution

☐ Limit to display filter

Endpoint Types ▾

6. Τα διαφορετικά endpoints που υπάρχει επικοινωνίας σε επίπεδο IP είναι 4.

Δεν υπάρχει ταύτιση μεταξύ των endpoints αυτών και των endpoints σε επίπεδο Ethernet

7.

- Για την αποστολή ερωτημάτων προς τον DNS Server ο υπολογιστής χρησιμοποιεί ως θύρες προέλευσης τις:

51730, 61076, 60736, 55875, 49869, 63692, 54829, 54453, 62149, 65189, 62987, 59913, 51399 και 59805

Ως θύρα προορισμού χρησιμοποιείται πάντα η θύρα 53.

- Οι απαντήσεις του DNS Server στέλνονται στον υπολογιστή με τη χρήση της θύρας 53 ως θύρα προέλευσης
Ενώ ως θύρες προορισμού χρησιμοποιούνται οι
61076, 51730, 60736, 55875, 49869, 63669, 54829, 54453, 62149, 65189, 62987, 59913, 51399 και 59805, αντίστοιχα με τις θύρες που χρησιμοποιήθηκαν προηγουμένως για την αποστολή των ερωτημάτων.

8. Στην κεφαλίδα των πακέτων DNS χρησιμοποιείται ένα πεδίο ενός bit για να προσδιοριστεί εάν αυτά περιέχουν ένα ερώτημα προς τον DNS Server ή μια απάντηση από εκείνον.

Αυτό μπορούμε να το δούμε και μέσω του Wireshark για κάθε πακέτο ξεχωριστά, όπου στις πληροφορίες αναγράφεται αν το συγκεκριμένο πακέτο περιέχει ερώτηση (0 = query) ή απάντηση (1 = response).

The image shows a Wireshark packet capture of a DNS transaction. The top pane displays a list of packets, with packet 8 selected. The middle pane shows the details of the selected packet, which is a 'Domain Name System (query)' packet. The bottom pane shows the raw packet data in hexadecimal and ASCII. The packet is a standard query (type 0) from source IP fdfd:3427:2509:0:54d9:ef2d:978b:ac6e to destination IP fdfd:3427:2509::1. The query is for the domain 'www.ietf.org'.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.204575	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	92	Standard query 0x77d0 A www.ietf.org
7	0.204796	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	92	Standard query response 0xbbee AAAA www.ietf.org
8	0.215213	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	166	Standard query response 0xbbee AAAA www.ietf.org CNAME www.ietf.org.
9	0.229600	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	179	Standard query response 0x77d0 A www.ietf.org CNAME www.ietf.org.ed.
16	0.254152	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	104	Standard query 0x3fa1 PTR 1.1.168.192.in-addr.arpa
17	0.262383	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	129	Standard query response 0x3fa1 PTR 1.1.168.192.in-addr.arpa PTR Ope.
20	5.876950	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	166	Standard query 0xf1f6 PTR 11.246.16.213.in-addr.arpa
38	5.883471	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	152	Standard query response 0xf1f6 PTR 11.246.16.213.in-addr.arpa PTR b.
40	11.448126	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	107	Standard query 0x87cf PTR 225.247.16.213.in-addr.arpa
41	11.455352	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	155	Standard query response 0x87cf PTR 225.247.16.213.in-addr.arpa PTR ..
79	17.026917	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	105	Standard query 0xf54d PTR 158.110.1.62.in-addr.arpa
80	17.053163	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	147	Standard query response 0xf54d PTR 158.110.1.62.in-addr.arpa PTR be.
82	17.763409	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	95	Standard query 0x95b8 AAAA d.docs.live.net
83	17.768954	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	331	Standard query response 0x95b8 AAAA d.docs.live.net CNAME odc.route.
117	18.129879	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	95	Standard query 0x9567 AAAA d.docs.live.net

Domain Name System (query)
Transaction ID: 0x77d0
Flags: 0xb00 Standard query
0... .. = Response: Message is a query
...000 0... .. = Opcode: Standard query (0)
...0... .. = Truncated: Message is not truncated
...1... .. = Recursion desired: Do query recursively
...0... .. = Z: reserved (0)
...0... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

0000 04 91 b1 5a cc 04 a4 db 30 a2 26 3c 66 dd 60 00 ...Z... 0 &c...
0010 00 00 00 26 11 40 fd fd 34 27 25 09 00 00 54 d9 ...&... 4'...T...
0020 ef 2d 97 8b ac 6e fd fd 34 27 25 09 00 00 00 00 ...n... 4'...
0030 00 00 00 00 01 ca 12 00 35 00 26 65 f5 77 d8 ...n... 5 &e w...
0040 00 00 01 00 00 00 00 00 00 03 77 77 77 04 69 ...www.i...
0050 65 65 65 63 6f 72 67 00 00 01 00 01 00 01 ...ee.org:....

Στην κεφαλίδα του πακέτου, που στέλνει ο υπολογιστής για να υποβάλει ένα ερώτημα (standard query) προς τον DNS Server, υπάρχει επίσης ένα πεδίο με το ID του ερωτήματος. Έτσι όταν ο server απαντάει (standard query response) σε αυτό, το πακέτο που στέλνει πίσω περιέχει ακριβώς το ίδιο ID, ώστε να υπάρχει αντιστοίχιση με το πακέτο που έστειλε ο υπολογιστής μας, κάτι που φαίνεται και μέσα απο το Wireshark καθώς κάθε πακέτο απάντησης έχει το ίδιο ID με το ερώτημα στο οποίο απαντάει.

9. Στην κεφαλίδα ενός DNS πακέτου που στέλνει ο server περιέχεται ένα πεδίο του ενός bit για να προσδιοριστεί αν εκείνος είναι Authoritative, όπως φαίνεται και στην εικόνα παρακάτω. Αν το bit είναι 0, σημαίνει πως ο DNS Server δεν είναι authoritative, ενώ αν το bit είναι 1, σημαίνει πως εκείνος είναι.

Επομένως βλέπουμε πως ο name server που μας απαντάει δεν είναι authoritative καθώς το bit του συγκεκριμένου πεδίου είναι 0.

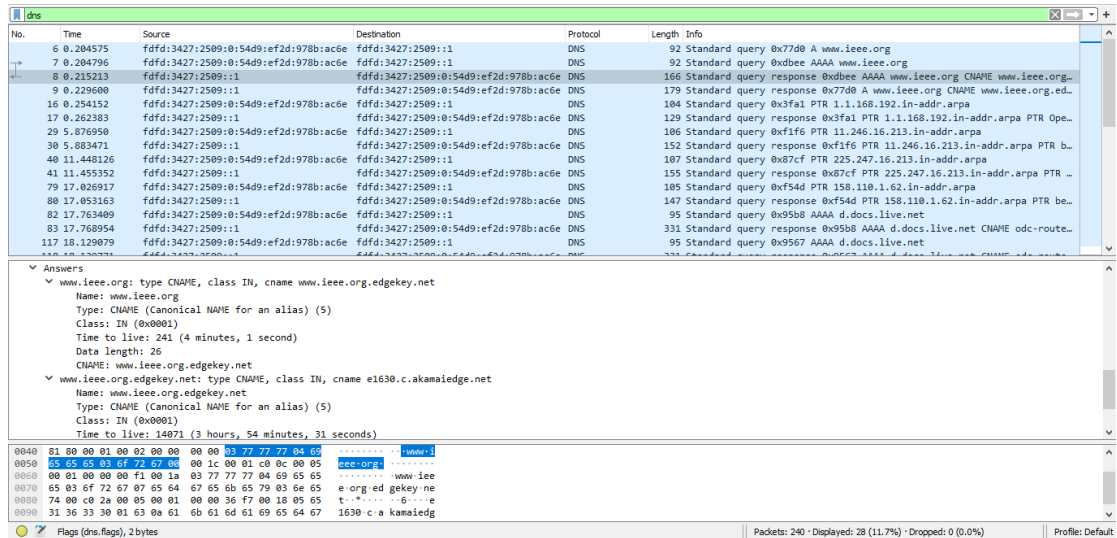
The image shows a Wireshark packet capture of a DNS transaction. The top pane displays a list of packets, with packet 8 selected. The middle pane shows the details of the selected packet, which is a 'Domain Name System (response)' packet. The bottom pane shows the raw packet data in hexadecimal and ASCII. The packet is a standard query response (type 1) from source IP fdfd:3427:2509:0:54d9:ef2d:978b:ac6e to destination IP fdfd:3427:2509::1. The response is for the domain 'www.ietf.org'.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.204575	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	92	Standard query 0x77d0 A www.ietf.org
7	0.204796	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	92	Standard query response 0xbbee AAAA www.ietf.org
8	0.215213	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	166	Standard query response 0xbbee AAAA www.ietf.org CNAME www.ietf.org.
9	0.229600	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	179	Standard query response 0x77d0 A www.ietf.org CNAME www.ietf.org.ed.
16	0.254152	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	104	Standard query 0x3fa1 PTR 1.1.168.192.in-addr.arpa
17	0.262383	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	129	Standard query response 0x3fa1 PTR 1.1.168.192.in-addr.arpa PTR Ope.
20	5.876950	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	166	Standard query 0xf1f6 PTR 11.246.16.213.in-addr.arpa
38	5.883471	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	152	Standard query response 0xf1f6 PTR 11.246.16.213.in-addr.arpa PTR b.
40	11.448126	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	107	Standard query 0x87cf PTR 225.247.16.213.in-addr.arpa
41	11.455352	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	155	Standard query response 0x87cf PTR 225.247.16.213.in-addr.arpa PTR ..
79	17.026917	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	105	Standard query 0xf54d PTR 158.110.1.62.in-addr.arpa
80	17.053163	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	147	Standard query response 0xf54d PTR 158.110.1.62.in-addr.arpa PTR be.
82	17.763409	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	95	Standard query 0x95b8 AAAA d.docs.live.net
83	17.768954	fdfd:3427:2509::1	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	331	Standard query response 0x95b8 AAAA d.docs.live.net CNAME odc.route.
117	18.129879	fdfd:3427:2509:0:54d9:ef2d:978b:ac6e	fdfd:3427:2509::1	DNS	95	Standard query 0x9567 AAAA d.docs.live.net

Domain Name System (response)
Transaction ID: 0xbbee
Flags: 0xb00 Standard query response, No error
1... .. = Response: Message is a response
...000 0... .. = Opcode: Standard query (0)
...0... .. = Authoritative: Server is not an authority for domain
...0... .. = Truncated: Message is not truncated
...1... .. = Recursion desired: Do query recursively
...1... .. = Recursion available: Server can do recursive queries
...0... .. = Z: reserved (0)
...0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
...0... .. = Non-authenticated data: Unacceptable
...0000 ... = Reply code: No error (0)

0040 81 00 00 01 00 00 00 00 00 03 77 77 77 04 69 ...www.i...
0050 65 65 65 63 6f 72 67 00 01 c0 00 01 c0 0c 00 05 ...ee.org:....
0060 00 01 00 00 00 f1 0a 03 77 77 77 04 69 65 65 ...www.ief...
0070 65 63 6f 72 67 07 65 64 67 65 65 65 79 03 6e 65 ...e.org.ed gekey-ne...
0080 74 00 c0 2a 00 05 00 01 00 00 36 17 00 18 05 65 ...e... 6...e...
0090 31 36 33 30 81 63 0a 61 6b 61 6d 61 69 65 64 67 1630 c-a kamaiedg

10.



No.	Time	Source	Destination	Protocol	Length	Info
6	0.204575	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	fdff:3427:2509::1	DNS	92	Standard query 0x77d0 A www.ietf.org
7	0.204796	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	fdff:3427:2509::1	DNS	92	Standard query 0x77d0 AAAA www.ietf.org
8	0.215213	fdff:3427:2509::1	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	166	Standard query response 0x77d0 A www.ietf.org CNAME www.ietf.org
9	0.229600	fdff:3427:2509::1	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	179	Standard query response 0x77d0 A www.ietf.org CNAME www.ietf.org
16	0.254152	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	fdff:3427:2509::1	DNS	104	Standard query 0x3fa1 PTR 1.1.168.192.in-addr.arpa
17	0.262383	fdff:3427:2509::1	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	129	Standard query response 0x3fa1 PTR 1.1.168.192.in-addr.arpa PTR Ope...
29	5.876950	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	fdff:3427:2509::1	DNS	106	Standard query 0xf1f6 PTR 11.246.16.213.in-addr.arpa
30	5.883471	fdff:3427:2509::1	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	152	Standard query response 0xf1f6 PTR 11.246.16.213.in-addr.arpa PTR b...
40	11.448126	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	fdff:3427:2509::1	DNS	187	Standard query 0x07cf PTR 225.247.16.213.in-addr.arpa
41	11.455352	fdff:3427:2509::1	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	155	Standard query response 0x07cf PTR 225.247.16.213.in-addr.arpa PTR ...
79	17.826917	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	fdff:3427:2509::1	DNS	105	Standard query 0xf54d PTR 158.110.1.62.in-addr.arpa
80	17.853163	fdff:3427:2509::1	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	147	Standard query response 0xf54d PTR 158.110.1.62.in-addr.arpa PTR be...
82	17.763409	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	fdff:3427:2509::1	DNS	95	Standard query 0x95b8 AAAA d.docs.live.net
83	17.768954	fdff:3427:2509::1	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	331	Standard query response 0x95b8 AAAA d.docs.live.net CNAME odc-route...
117	18.129079	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	fdff:3427:2509::1	DNS	95	Standard query 0x9567 AAAA d.docs.live.net

Answers

- www.ietf.org: type CNAME, class IN, cname www.ietf.org.edgekey.net
 - Name: www.ietf.org
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 241 (4 minutes, 1 second)
 - Data length: 26
 - CNAME: www.ietf.org.edgekey.net
- www.ietf.org.edgekey.net: type CNAME, class IN, cname e1630.c.akamaiedge.net
 - Name: www.ietf.org.edgekey.net
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 14071 (3 hours, 54 minutes, 31 seconds)


0040 81 00 00 01 00 02 00 00 00 00 03 77 77 77 04 65www.i
0050 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55eet.org
0060 00 01 00 00 f1 00 1a 03 77 77 77 04 60 65 65www.iet
0070 65 03 6f 72 67 07 65 64 67 65 6b 65 79 03 6e 65e.org:ed gekey.ne
0080 74 00 c0 2a 00 05 00 01 00 00 36 f7 00 18 05 65t.....6...e
0090 31 36 33 30 01 63 0a 61 6b 61 6d 61 69 65 64 67 1630 c:a kamaied

Flags (dns.flags), 2 bytes | Packets: 240 · Displayed: 28 (11.7%) · Dropped: 0 (0.0%) | Profile: Default

Όπως φαίνεται στην εικόνα, το όνομα www.ietf.org είναι Canonical Name (CNAME)

11. Παρατηρούμε πως η IP του www.ietf.org είναι: 23.43.116.56

Η IP του υπολογιστή είναι η: fdff:3427:2509:0:54d9:ef2d:978b:ac6e



No.	Time	Source	Destination	Protocol	Length	Info
9	0.229600	fdff:3427:2509::1	fdff:3427:2509:0:54d9:ef2d:978b:ac6e	DNS	179	Standard query response 0x77d0 A www.ietf.org CNAME www.ietf.org.edgekey.net CNAME

Answers

- www.ietf.org: type CNAME, class IN, cname www.ietf.org.edgekey.net
 - Name: www.ietf.org
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 241 (4 minutes, 1 second)
 - Data length: 26
 - CNAME: www.ietf.org.edgekey.net
- www.ietf.org.edgekey.net: type CNAME, class IN, cname e1630.c.akamaiedge.net
 - Name: www.ietf.org.edgekey.net
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 14071 (3 hours, 54 minutes, 31 seconds)
- e1630.c.akamaiedge.net: type A, class IN, addr 23.43.116.56
 - Name: e1630.c.akamaiedge.net
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 28 (28 seconds)
 - Data length: 4
 - Address: 23.43.116.56

12. Εφαρμόζουμε ένα φίλτρο “icmp” στο Wireshark με αποτέλεσμα να εμφανίζονται μόνο τα πακέτα που βασίζονται στο συγκεκριμένο πρωτόκολλο.

13. a. Η IP του προορισμού όπως φαίνεται παρακάτω είναι 23.43.116.56

b. Σύμφωνα με το Wireshark, το TTL του συγκεκριμένου πακέτου είναι 1 κόμβος

c. Όπως φαίνεται στην παρακάτω εικόνα το μέγεθος του συγκεκριμένου πακέτου είναι 106 Bytes

No.	Time	Source	Destination	Protocol	Length	Info
10	0.237548	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=16/4096, ttl=1 (no response fou...
11	0.242855	192.168.1.1	192.168.1.118	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12	0.244369	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=17/4352, ttl=1 (no response fou...
13	0.248092	192.168.1.1	192.168.1.118	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
14	0.249715	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=18/4608, ttl=1 (no response fou...
15	0.252222	192.168.1.1	192.168.1.118	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
23	5.808350	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=19/4864, ttl=2 (no response fou...
24	5.830030	213.16.246.11	192.168.1.118	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
25	5.831577	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=2 (no response fou...
26	5.851713	213.16.246.11	192.168.1.118	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
27	5.853377	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=2 (no response fou...
28	5.874885	213.16.246.11	192.168.1.118	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
34	11.306009	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=3 (no response fou...
35	11.406258	213.16.247.225	192.168.1.118	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
36	11.407020	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=3 (no response fou...

Internet Protocol Version 4, Src: 192.168.1.118, Dst: 23.43.116.56						
0100 = Version: 4						
... 0101 = Header Length: 20 bytes (5)						
Differeniated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 92						
Identification: 0xcceb (52936)						
Flags: 0x0000						
...0 0000 0000 0000 = Fragment offset: 0						
Time to live: 1						
[Expert Info (Note/Sequence): "Time To Live" only 1]						
Protocol: ICMP (1)						
Header checksum: 0x9d57 (validation disabled)						
[Header checksum status: Unverified]						

0000	a4 91 b1 5a cc a0 a4 db 30 a2 26 3c 00 00 45 00	...Z...0:8...E
0010	00 5c ce c8 00 01 01 9d 57 c0 a8 01 76 17 2b	\\.....M...V+
0020	74 38 08 00 f7 ee 00 01 00 10 00 00 00 00 00	t8.....
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00

Ethernet (eth), 14 bytes | Packets: 240 | Displayed: 36 (15.0%) | Dropped: 0 (0.0%) | Profile: Default

14. α. Η IP διεύθυνση του προορισμού είναι 192.168.1.118, ενώ της προέλευσης είναι 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
10	0.237548	192.168.1.118	23.43.116.56	ICMP	106	Echo (ping) request id=0x0001, seq=16/4096, ttl=1 (no response fou...
11	0.242855	192.168.1.1	192.168.1.118	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)

15. Οι διαφορετικές διευθύνσεις προέλευσης των συγκεκριμένων IP πακέτων είναι:

- 192.168.1.1
- 213.16.246.11
- 213.16.247.255
- 62.1.110.158
- 80.81.195.168

Παρατηρούμε ότι υπάρχει αντιστοιχία μεταξύ μερικών από αυτές και εκείνες που φαίνονται κατά την εκτέλεση της εντολής tracert

```
C:\Users\Satellite>tracert www.ieee.org

Tracing route to e1630.c.akamaiedge.net [23.43.116.56]
over a maximum of 30 hops:

  1      5 ms      3 ms      2 ms  OpenWrt.lan [192.168.1.1]
  2     21 ms     20 ms     21 ms  bbras-llu-klm-021500.forthnet.gr [213.16.246.11]
  3     19 ms     18 ms     19 ms  te0-4-0-6.distr-klm-03.forthnet.gr [213.16.247.225]
  4     19 ms     19 ms     19 ms  be33.core-klm-04.forthnet.gr [62.1.110.158]
  5     78 ms     77 ms     77 ms  decix-fra10.netarch.akamai.com [80.81.195.168]
  6     77 ms     77 ms     76 ms  a23-43-116-56.deploy.static.akamaitechnologies.com [23.43.116.56]

Trace complete.
```

Β' Μέρος)

1.

No.	Time	Source	Destination	Protocol	Length	Info
470	5.504911	192.168.1.118	194.177.214.44	HTTP	383	GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?43me3 HTTP/1.1

Παρατηρούμε πως η διεύθυνση IP που αντιστοιχεί στην www.ekt.gr είναι 194.177.214.44

2.

465	5.478407	192.168.1.118	194.177.214.44	TCP	66	56053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
468	5.504634	194.177.214.44	192.168.1.118	TCP	62	80 → 56052 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1
469	5.504755	192.168.1.118	194.177.214.44	TCP	54	56052 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Η διαδικασία της χειραψίας 3 βημάτων βάσει των πληροφοριών που περιέχονται στα πακέτα είναι η εξής:

A. Ο υπολογιστής στέλνει ένα πακέτο TCP στο οποίο το bit της σημαίας SYN είναι 1 ώστε να ενημερώσει τον server πως πρόκειται να συνδεθεί μαζί του. Ο αριθμός ακολουθίας (Sequence number) είναι 0.

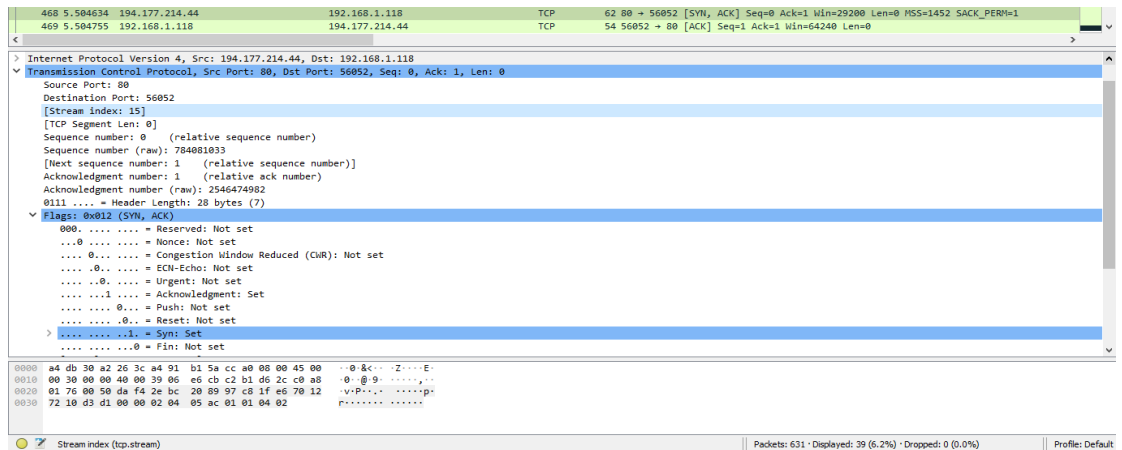
465	5.478407	192.168.1.118	194.177.214.44	TCP	66	56053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
468	5.504634	194.177.214.44	192.168.1.118	TCP	62	80 → 56052 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1
469	5.504755	192.168.1.118	194.177.214.44	TCP	54	56052 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

> Ethernet II, Src: LiteonTe_a2:26:3c (a4:db:30:a2:26:3c), Dst: Technico_5a:ccc:a0 (a4:91:b1:5a:cc:a0)	
> Internet Protocol Version 4, Src: 192.168.1.118, Dst: 194.177.214.44	
▼ Transmission Control Protocol, Src Port: 56053, Dst Port: 80, Seq: 0, Len: 0	
Source Port: 56053	
Destination Port: 80	
[Stream index: 16]	
[TCP Segment Len: 0]	
Sequence number: 0 (relative sequence number)	
Sequence number (raw): 2987063125	
[Next sequence number: 1 (relative sequence number)]	
Acknowledgment number: 0	
Acknowledgment number (raw): 0	
1000 = Header Length: 32 bytes (8)	
▼ Flags: 0x002 (SYN)	
0000 = Reserved: Not set	
...0 = Nonce: Not set	
...0 = Congestion Window Reduced (CWR): Not set	
....0... = ECN-Echo: Not set	
....0... = Urgent: Not set	
....0... = Acknowledgment: Not set	
....0... = Push: Not set	
....0... = Reset: Not set	
>0... = Syn: Set	

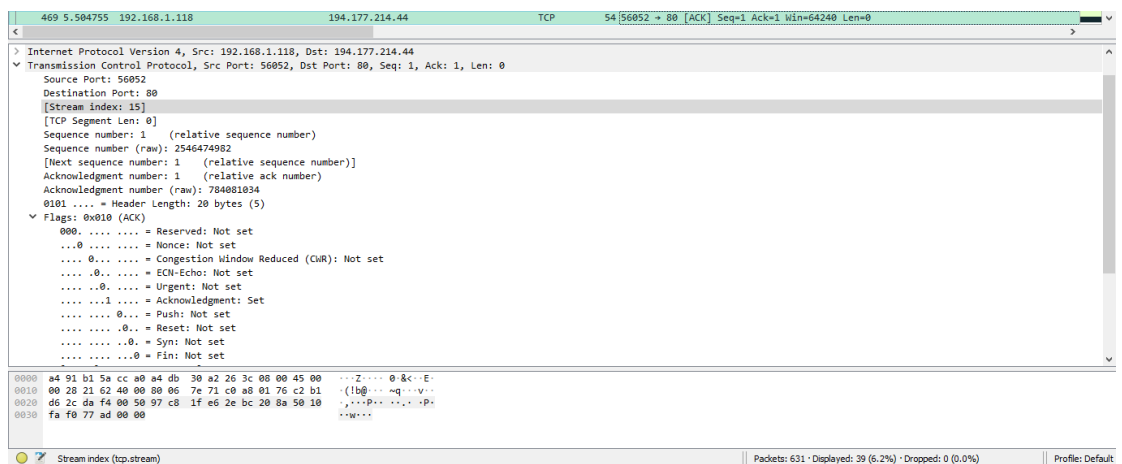
0000	a4 91 b1 5a cc a0	5a cc a0	00 00 45 00	...	Z...	E
0010	00 34 21 61 40 00	00 05 7e 56 c9 a0	01 76 c2 b1	41a0	...	f...
0020	d6 2c da f5 00 50	b2 0a f7 55 00	00 00 00 02	...	P...	U...
0030	fa f0 94 7c 00 00	02 04 05 b4 01	03 03 08 01	01
0040	04 02					

Stream index (tcp.stream) | Packets: 631 · Displayed: 39 (6.2%) · Dropped: 0 (0.0%) | Profile: Default

B. Στη συνέχεια ο server στέλνει ένα πακέτο όπου είναι ενεργοποιημένα τα bit Syn και Acknowledgment, που σημαίνει ότι αποδέχεται το αίτημα του υπολογιστή/πελάτη και θέτει τον acknowledge number ίσο με τον sequence number του πελάτη συν 1, δηλαδή 1. Ο αριθμός ακολουθίας είναι και εδώ 0.



Γ. Ο πελάτης αναγνωρίζει το αίτημα του server απαντώντας με ένα πακέτο στο οποίο το bit acknowledgment είναι 1 και ο αριθμός επιβεβαίωσης (Acknowledgment number) είναι επίσης 1 (δηλαδή ο αριθμός ακολουθίας του server που λήφθηκε συν 1).



3. Οι θύρες προέλευσης και προορισμού που χρησιμοποιούνται από το πρωτόκολλο HTTP είναι οι:

80, 56034, 56035, 56044, 56046, 56048, 56052 και 56053

4. Ο Browser έστειλε 5 πακέτα που περιείχαν αιτήματα GET. Οι διευθύνσεις στις οποίες στάλθηκαν αυτά είναι οι εξής:

- 62.1.38.41
- 194.177.214.44

No.	Time	Source	Destination	Protocol	Length	Info
54	1.747766	192.168.1.118	62.1.38.41	HTTP	360	GET /success.txt HTTP/1.1
79	1.852554	192.168.1.118	62.1.38.41	HTTP	365	GET /success.txt?ip= HTTP/1.1
478	5.504911	192.168.1.118	194.177.214.44	HTTP	383	GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?43me3 HTTP/1.1
473	5.505556	192.168.1.118	194.177.214.44	HTTP	405	GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?43me3 HTTP/1.1
500	5.857500	192.168.1.118	194.177.214.44	HTTP	478	GET /sites/ekt-site/themes/ekt/images/ektgr_header_e1.jpg HTTP/1.1

5. Όπως φαίνεται ο Browser τρέχει την έκδοση 1.1

54	1.747766	192.168.1.118	62.1.38.41	HTTP	360 GET /success.txt HTTP/1.1
79	1.852554	192.168.1.118	62.1.38.41	HTTP	365 GET /success.txt?ipv4 HTTP/1.1
470	5.504911	192.168.1.118	194.177.214.44	HTTP	383 GET /sites/ekt-site/libraries/tablesorter/jquery.metadata.js?443e3 HTTP/1.1
473	5.505556	192.168.1.118	194.177.214.44	HTTP	405 GET /sites/ekt-site/libraries/tablesorter/addons/pager/jquery.tablesorter.pager.js?443e3 HTTP/1.1
500	5.857500	192.168.1.118	194.177.214.44	HTTP	478 GET /sites/ekt-site/themes/ekt/images/ektgr_header_el.jpg HTTP/1.1

>	Frame 54: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF_{83977EF1-88D0-47C4-ADF8-EAEB9C6A8991}, id 0
>	Ethernet II, Src: LiteonTe_a2:26:3c (a4:db:30:a2:26:3c), Dst: Technico_5a:cc:a0 (a4:91:b1:5a:cc:a0)
>	Internet Protocol Version 4, Src: 192.168.1.118, Dst: 62.1.38.41
>	Transmission Control Protocol, Src Port: 56834, Dst Port: 80, Seq: 1, Ack: 1, Len: 306
>	Hypertext Transfer Protocol
>	GET /success.txt HTTP/1.1\r\n
>	Host: detectportal.firefox.com\r\n
>	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0\r\n
>	Accept: */*\r\n
>	Accept-Language: en-US,en;q=0.5\r\n
>	Accept-Encoding: gzip, deflate\r\n
>	Cache-Control: no-cache\r\n

Αντίστοιχα ο server τρέχει και εκείνος την έκδοση 1.1

492	5.668754	194.177.214.44	192.168.1.118	HTTP	750 HTTP/1.1 404 Not Found (text/html)
495	5.814394	194.177.214.44	192.168.1.118	HTTP	59 HTTP/1.1 404 Not Found (text/html)
500	5.857500	192.168.1.118	194.177.214.44	HTTP	478 GET /sites/ekt-site/themes/ekt/images/ektgr_header_el.jpg HTTP/1.1

>	Frame 492: 750 bytes on wire (6000 bits), 750 bytes captured (6000 bits) on interface \Device\NPF_{83977EF1-88D0-47C4-ADF8-EAEB9C6A8991}, id 0
>	Ethernet II, Src: Technico_5a:cc:a0 (a4:91:b1:5a:cc:a0), Dst: LiteonTe_a2:26:3c (a4:db:30:a2:26:3c)
>	Internet Protocol Version 4, Src: 194.177.214.44, Dst: 192.168.1.118
>	Transmission Control Protocol, Src Port: 80, Dst Port: 56852, Seq: 1, Ack: 330, Len: 696
>	Hypertext Transfer Protocol
>	HTTP/1.1 404 Not Found\r\n
>	Date: Fri, 17 Jan 2020 18:59:13 GMT\r\n
>	Server: Apache/2.4.6 (CentOS)\r\n
>	Content-Type: text/html; charset=utf-8\r\n
>	Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n
>	Cache-Control: no-cache, must-revalidate\r\n
>	X-Content-Type-Options: nosniff\r\n