
ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Εργασία-Wireshark

3160045-Καλδής Αργύριος

Γραμμή εντολών

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Argy>tracert www.iana.org

Tracing route to iana[www.vip.icann.org] [192.0.32.8]
over a maximum of 30 hops:

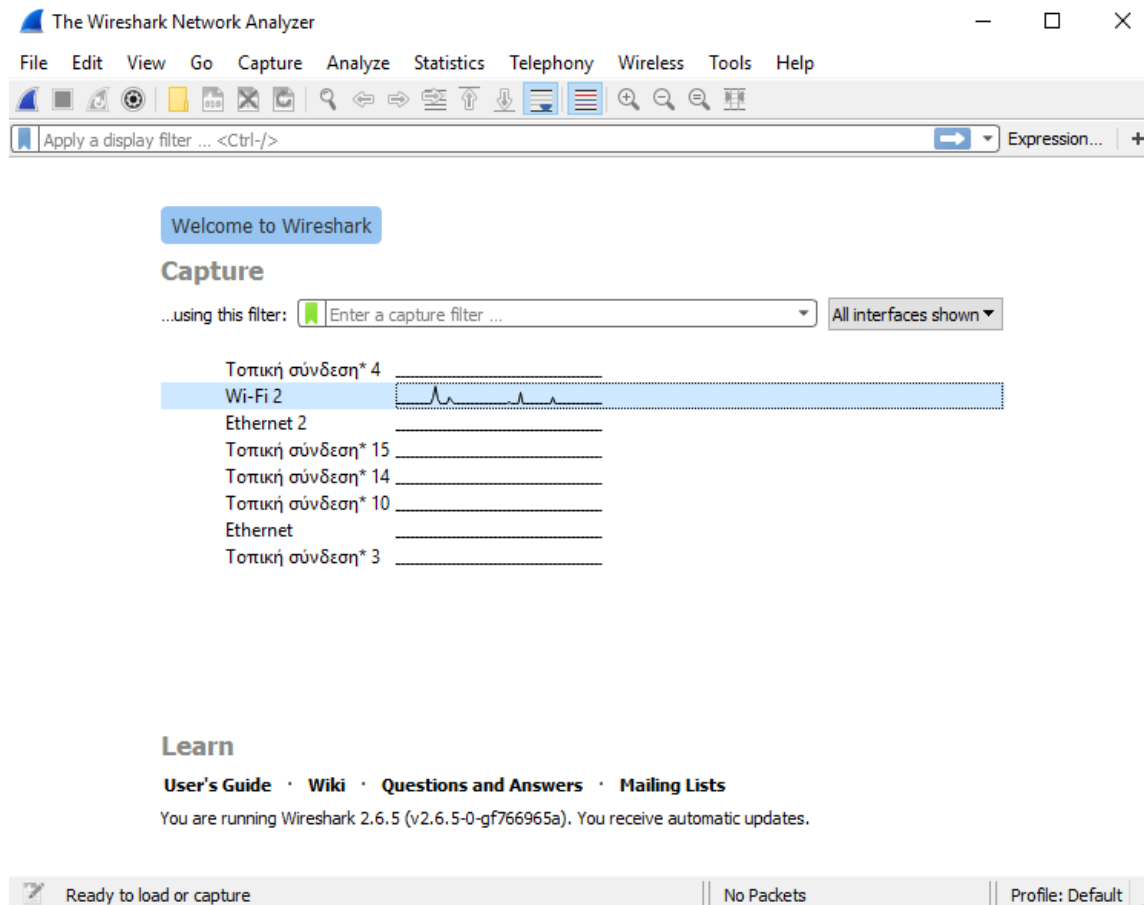
1	11 ms	7 ms	7 ms	192.168.1.1 [192.168.1.1]
2	18 ms	19 ms	18 ms	42.127.103.46.in-addr.arpa [46.103.127.42]
3	24 ms	19 ms	19 ms	117.103.59.178.in-addr.arpa [178.59.103.117]
4	57 ms	22 ms	22 ms	210.2.87.78.in-addr.arpa [78.87.2.210]
5	27 ms	25 ms	29 ms	53.173.218.63.in-addr.arpa [63.218.173.53]
6	83 ms	61 ms	65 ms	138.13.223.63.in-addr.arpa [63.223.13.138]
7	89 ms	81 ms	98 ms	14.0.222.63.in-addr.arpa [63.222.0.14]
8	236 ms	225 ms	213 ms	206.4.250.129.in-addr.arpa [129.250.4.206]
9	68 ms	99 ms	59 ms	144.5.250.129.in-addr.arpa [129.250.5.144]
10	172 ms	148 ms	153 ms	96.4.250.129.in-addr.arpa [129.250.4.96]
11	250 ms	215 ms	213 ms	189.3.250.129.in-addr.arpa [129.250.3.189]
12	236 ms	230 ms	244 ms	49.6.250.129.in-addr.arpa [129.250.6.49]
13	256 ms	222 ms	235 ms	150.254.1.204.in-addr.arpa [204.1.254.150]
14	246 ms	225 ms	226 ms	8.32.0.192.in-addr.arpa [192.0.32.8]

Trace complete.

C:\Users\Argy>

Το λειτουργικό σύστημα που χρησιμοποιείται στη παρακάτω εργασία είναι τα Windows 10 Pro 64-bit.

Η διαδικασία ανίχνευσης πακέτων εκτελείται στη διεπαφή Wi-Fi 2 όπως φαίνεται και παρακάτω.



Απαντήσεις Γενικών Ερωτήσεων

1. Ποια ήταν η χρονική διάρκεια της ανίχνευσής σας;

Η χρονική διάρκεια της ανίχνευσής μπορεί να βρεθεί πατώντας στη **επιλογή Statistics -> Capture File Properties** (ή έχοντας ένα χρονόμετρο ακριβείας στη διάθεση μας. JK) . Στη συγκεκριμένη περίπτωση η διάρκεια ήταν **6.043s**. Συγκεκριμένα η χρονική διάρκεια φαίνεται στο πεδίο **Time span, s**.

Wireshark · Capture File Properties · Wi-Fi 2

Details

File

Name: C:\Users\Argy\AppData\Local\Temp\wireshark_A2FCB102-B16C-458A-8FFC-DFCB7EAE888F_20190110133629_a11876.pcapng
Length: 29 kB
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2019-01-10 13:36:29
Last packet: 2019-01-10 13:36:35
Elapsed: 00:00:06

Capture

Hardware: Intel(R) Core(TM) i5-6600K CPU @ 3.50GHz (with SSE4.2)
OS: 64-bit Windows 10, build 17134
Application: Dumpcap (Wireshark) 2.6.5 (v2.6.5-0-gf766965a)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device\NPF_{A2FCB102-B16C-458A-8FFC-DFCB7EAE888F}	0 (0 %)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	88	88 (100.0%)	—
Time span, s	6.043	6.043	—
Average pps	14.6	14.6	—
Average packet size, B	297	297	—
Bytes	26132	26132 (100.0%)	0
Average bytes/s	4324	4324	—
Average bits/s	34 k	34 k	—

Capture file comments

Refresh
Save Comments
Close
Copy To Clipboard
Help

2. Προσδιορίστε σε ένα πίνακα, ποια διαφορετικά πρωτόκολλα χρησιμοποίησε ο υπολογιστής σας στη χρονική διάρκεια της ανίχνευσης, διαχωρίζοντάς τα σύμφωνα με τα επίπεδα στα οποία ανήκουν.

Τα πρωτόκολλα που χρησιμοποίησε ο υπολογιστής μπορούν να βρεθούν μεταβαίνοντας στην επιλογή **Statistics** → **Protocol Hierarchy**.

Πατώντας την επιλογή αυτή εμφανίζονται όλα τα πρωτόκολλα που εντοπίστηκαν στην

Ανίχνευση σε ιεραρχική δομή.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End B
▼ Frame	100.0	88	100.0	26132	34 k	0	0
▼ Ethernet	100.0	88	4.7	1232	1631	0	0
▼ Internet Protocol Version 6	11.4	10	1.5	400	529	0	0
▼ User Datagram Protocol	11.4	10	0.3	80	105	0	0
Domain Name System	11.4	10	2.3	598	791	10	598
▼ Internet Protocol Version 4	88.6	78	6.0	1560	2065	0	0
▼ User Datagram Protocol	8.0	7	0.2	56	74	0	0
Data	8.0	7	1.3	350	463	7	350
▼ Transmission Control Protocol	53.4	47	77.5	20248	26 k	31	13367
Secure Sockets Layer	18.2	16	73.7	19260	25 k	16	19260
Internet Control Message Protocol	27.3	24	6.2	1608	2128	24	1608

No display filter.

Close

Copy

Help

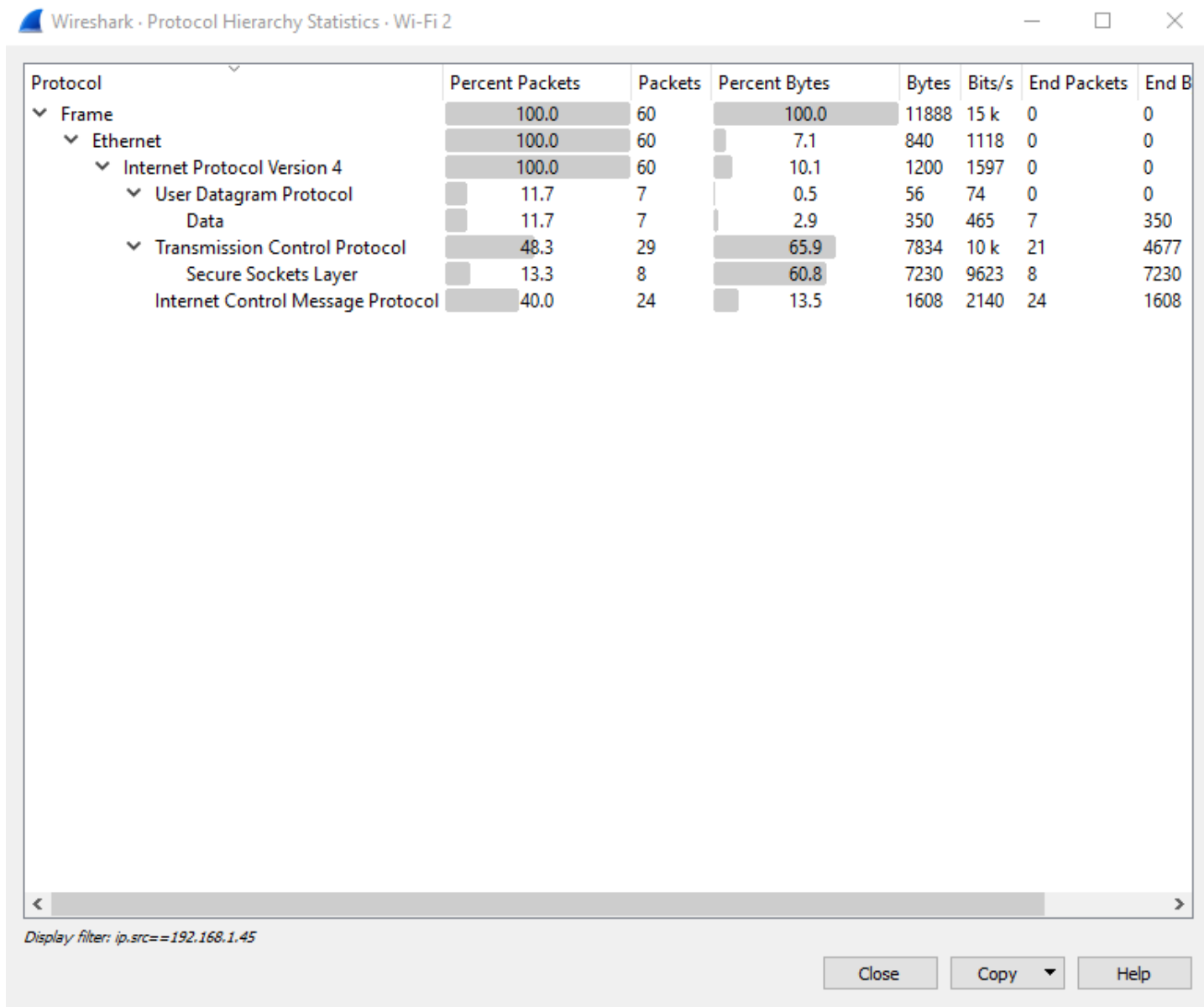
3. Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.

Το πρωτόκολλο DNS χρησιμοποιούν το πρωτόκολλο UDP ενώ τα υπόλοιπα πρωτόκολλα συμπεριλαμβανομένου των ICMP και SSL χρησιμοποιούν τα πρωτόκολλα TCP.

4. Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;

Εκτελώντας την εντολή `ip.src==192.168.1.45` βλέπουμε τα πακέτα που σταλθηκαν.

Στη συγκεκριμένη περίπτωση είναι UDP=7 και TCP= 29.



5. Πόσα και ποια είναι τα διαφορετικά endpoints (η σχετική πληροφορία βρίσκεται στο μενού Statistics) με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet; Μπορείτε να βρείτε σε ποιες συσκευές αντιστοιχούν;

Ο πίνακας Endpoints εμφανίζει της MAC διευθύνσεις των διαφορετικών συσκευών. Στο παρακάτω πίνακα φαίνονται η συνδέσεις και τα ονόματα τις κάθε συσκευής.

Wireshark · Endpoints · Wi-Fi 2

Ethernet · 3

IPv4 · 8

IPv6 · 2

TCP · 3

UDP · 8

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
IPv4mcast_01	7	644	0	0	7	644
Tp-LinkT_18:02:2f	88	26 k	53	11 k	35	14 k
Zte_cf:bb:b0	81	25 k	35	14 k	46	10 k

☒ Name resolution☐ Limit to display filter

Endpoint Types

CopyCloseHelp

Wireshark · Conversations · Wi-Fi 2

Ethernet · 2

IPv4 · 7

IPv6 · 1

TCP · 2

UDP · 6

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
IPv4mcast_01	Tp-LinkT_18:02:2f	7	644	0	0	7	644
Tp-LinkT_18:02:2f	Zte_cf:bb:b0	81	25 k	46	10 k	35	14 k

☒ Name resolution☐ Limit to display filter☐ Absolute start time

Conversation Types

CopyFollow Stream...Graph...CloseHelp

6. Πόσα και ποια είναι τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP; Ταυτίζονται με τα endpoints σε επίπεδο Ethernet; Αν όχι, εξηγήστε γιατί συμβαίνει αυτό.

Οι διευθύνσεις IPv4 που εντοπίστηκαν κατά την ανίχνευση ήταν 8 δηλαδή 5 περισσότερα από τα Ethernet. Αυτό οφείλετε στο γεγονός ότι το κάθε επίπεδο δικτύου επικοινωνεί με κόμβους του διαδικτύου ενώ το επίπεδο σύνδεσης δεδομένων με κόμβους στους οποίους ο υπολογιστής συνδέεται άμεσα.

Τα μόνα endpoint που ταυτίζονται είναι οι διεύθυνσης του υπολογιστή.

Wireshark · Endpoints · Wi-Fi 2

Ethernet · 3

IPv4 · 8

IPv6 · 2

TCP · 3

UDP · 8

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:01	7	644	0	0	7	644
18:d6:c7:18:02:2f	88	26 k	53	11 k	35	14 k
74:a7:8e:cf:bb:b0	81	25 k	35	14 k	46	10 k

☐ Name resolution☐ Limit to display filter

Endpoint Types

CopyCloseHelp

Wireshark · Endpoints · Wi-Fi 2

Ethernet · 3

IPv4 · 8

IPv6 · 2

TCP · 3

UDP · 8

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number
46.103.127.42	3	210	3	210	0	0	—	—	—
52.114.128.10	47	21 k	18	13 k	29	8820	—	—	—
78.87.2.210	3	330	3	330	0	0	—	—	—
178.59.103.117	3	210	3	210	0	0	—	—	—
192.0.32.8	12	1272	0	0	12	1272	—	—	—
192.168.1.1	3	402	3	402	0	0	—	—	—
192.168.1.45	78	24 k	48	10 k	30	14 k	—	—	—
230.0.0.1	7	644	0	0	7	644	—	—	—

☐ Name resolution☐ Limit to display filter

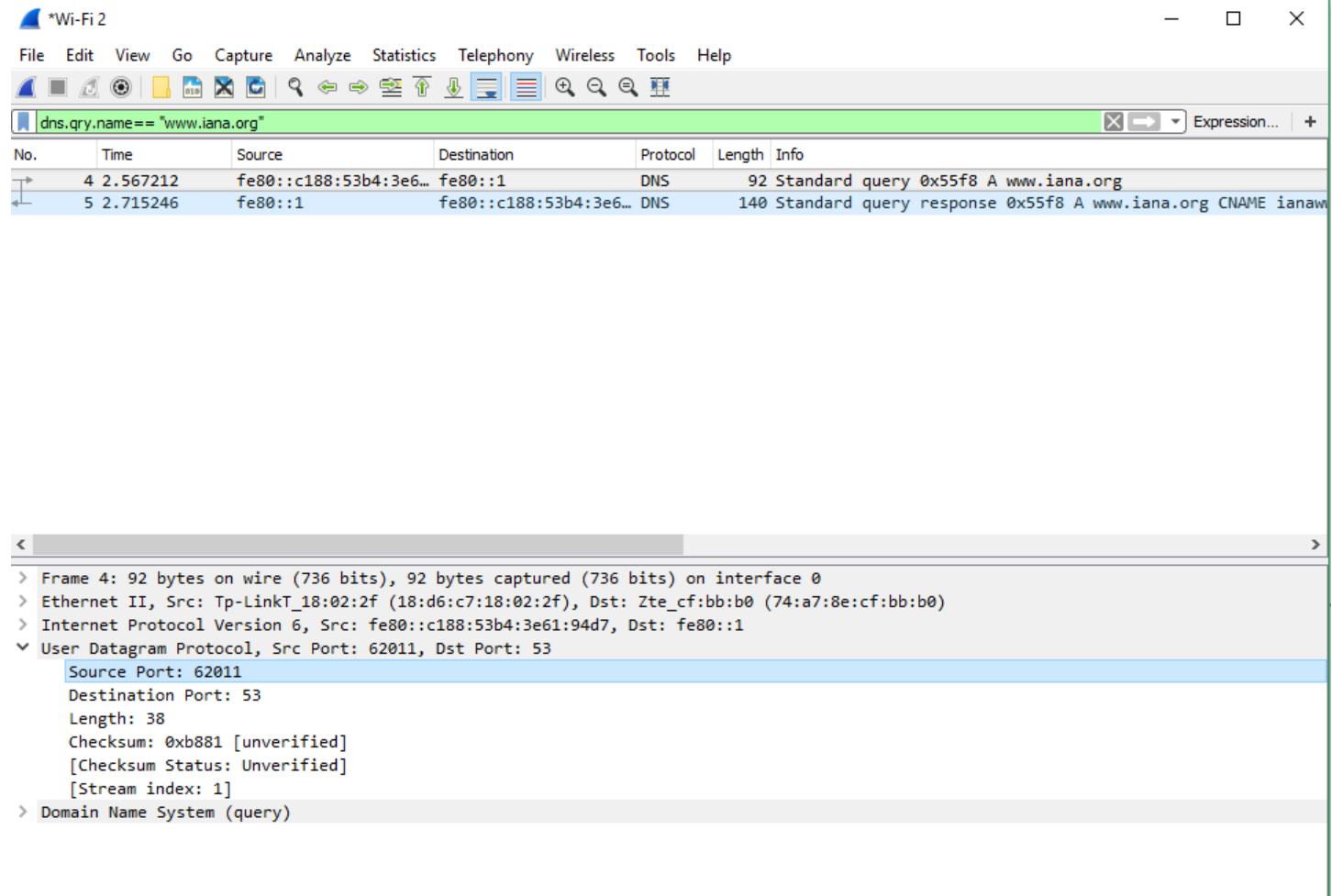
Endpoint Types

CopyCloseHelp

Ερωτήσεις σχετικά με το DNS

7. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για την ερώτηση από τον υπολογιστή σας προς τον DNS server και για την απάντηση του DNS server.

Εφαρμόζοντας την εντολή `dns.qry.name == "www.iana.org"` βρίσκουμε τον αποστολέα και τον παραλήπτη.



The image shows a Wireshark capture of a DNS transaction. The filter bar at the top is set to `dns.qry.name == "www.iana.org"`. The packet list shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
4	2.567212	fe80::c188:53b4:3e6...	fe80::1	DNS	92	Standard query 0x55f8 A www.iana.org
5	2.715246	fe80::1	fe80::c188:53b4:3e6...	DNS	140	Standard query response 0x55f8 A www.iana.org CNAME ianaw

The packet details pane for packet 4 shows the following information:

- Frame 4: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
- Ethernet II, Src: Tp-LinkT_18:02:2f (18:d6:c7:18:02:2f), Dst: Zte_cf:bb:b0 (74:a7:8e:cf:bb:b0)
- Internet Protocol Version 6, Src: fe80::c188:53b4:3e61:94d7, Dst: fe80::1
- User Datagram Protocol, Src Port: 62011, Dst Port: 53
 - Source Port: 62011
 - Destination Port: 53
 - Length: 38
 - Checksum: 0xb881 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 1]
- Domain Name System (query)

Κατά την αποστολή η UDP Θύρα είναι η 62011 , και η θύρα παραλαβής είναι η 53.

Η απάντηση περιέχει τις θύρες αποστολής και παραλαβής αντεστραμμένες όπως φαίνεται και στη παραπάνω εικόνα.

8. Πώς διακρίνετε αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα που έχετε κάνει; Πώς συνδέονται το πακέτο μιας απάντησης με το πακέτο της ερώτησης;

The image shows a Wireshark capture of a DNS transaction. The top pane displays a list of packets with a filter 'dns.qry.name == "www.iana.org"'. Two packets are shown: a query (No. 4) and a response (No. 5). The middle pane shows the details of the selected packet (No. 5), which is a 'Domain Name System (query)' packet. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4	2.567212	fe80::c188:53b4:3e6...	fe80::1	DNS	92	Standard query 0x55f8 A www.iana.org
5	2.715246	fe80::1	fe80::c188:53b4:3e6...	DNS	140	Standard query response 0x55f8 A www.iana.org CNAME ianaw

Details of packet 5 (Domain Name System (query)):

- Transaction ID: 0x55f8
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries: [Response In: 5]

Raw packet data (hex/ASCII):

```

0030  00 00 00 00 00 01 f2 3b 00 35 00 26 b8 81 55 f8  .....; 5&..U.
0040  01 00 00 01 00 00 00 00 00 00 03 77 77 77 04 69  .....www.i
0050  61 6e 61 03 6f 72 67 00 00 01 00 01          ana.org. ....
  
```

Bottom status bar: The response to this DNS query is in this frame (dns.response_in) | Packets: 88 · Displayed: 2 (2.3%) · Dropped: 0 (0.0%) | Profile: Default

Η διάκριση μεταξύ ενός πακέτου αιτήματος και ενός απάντησης σε ερώτημα θα μπορούσε να διακριθεί από το πεδίο κάτω απ το Queries (Παραπάνω εικόνα) όπου εάν είναι αίτημα τότε αναγράφεται “Response In:___” Ενώ αν είναι απάντηση τότε είναι “Request In:___”.

- Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει για το www.iana.org είναι authoritative για το συγκεκριμένο domain; Είναι ο name server που μας έχει απαντήσει authoritative για το συγκεκριμένο domain;

Στη συγκεκριμένη περίπτωση ο server δεν είναι authoritative όπως φαίνεται στη παρακάτω εικόνα.

The image shows a Wireshark capture of a DNS transaction. The top pane shows a list of packets, with packet 5 selected. The middle pane shows the details of the selected packet, which is a DNS Standard query response. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet 5: 2.715246, Source: fe80::1, Destination: fe80::c188:53b4:3e6..., Protocol: DNS, Length: 140, Info: Standard query response 0x55f8 A www.iana.org CNAME ianaww

Details of packet 5:

- User Datagram Protocol, Src Port: 53, Dst Port: 62011
- Domain Name System (response)
 - Transaction ID: 0x55f8
 - Flags: 0x8180 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)
 - Questions: 1
 - Answer RRs: 2
 - Authority RRs: 0
 - Additional RRs: 0

Raw packet data (hex/ASCII):

```
0040 81 80 00 01 00 02 00 00 00 00 03 77 77 77 04 69 ..... www.i
0050 61 6e 61 03 6f 72 67 00 00 01 00 01 c0 0c 00 05 ana.org .....
0060 00 01 00 00 01 0a 00 14 07 69 61 6e 61 77 77 77 ..... ianaww
```

10. Το όνομα www.iana.org είναι domain name ή πρόκειται για canonical name;

Όπως φαίνεται στη πάνω εικόνα στα info της απάντησης, μετά την διεύθυνση www.iana.org υπάρχει η λέξη CNAME που σημαίνει ότι το ονομα είναι canonical και όχι domain.

11. Ποια είναι η IP διεύθυνση που αντιστοιχεί στον www.iana.org; Ποια είναι η IP διεύθυνση του δικού σας υπολογιστή;

Το ip του υπολογιστή μας είναι το 192.168.1.45

Και του www.iana.org είναι το 192.0.32.8

```
Επιλογή Γραμμή εντολών
Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Τοπική σύνδεση* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Τοπική σύνδεση* 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::c188:53b4:3e61:94d7%17
    IPv4 Address. . . . . : 192.168.1.45
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Users\Argy>ipconfig

Questions: 1

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Argy>tracert www.iana.org

Tracing route to ianawww.vip.icann.org [192.0.32.8]
over a maximum of 30 hops:

  1  11 ms  7 ms  7 ms  192.168.1.1 [192.168.1.1]
  2  18 ms  19 ms  18 ms  42.127.103.46.in-addr.arpa [46.103.127.42]
  3  24 ms  19 ms  19 ms  117.103.59.178.in-addr.arpa [178.59.103.117]
  4  57 ms  22 ms  22 ms  210.2.87.78.in-addr.arpa [78.87.2.210]
  5  27 ms  25 ms  29 ms  53.173.218.63.in-addr.arpa [63.218.173.53]
  6  83 ms  61 ms  65 ms  138.13.223.63.in-addr.arpa [63.223.13.138]
  7  89 ms  81 ms  98 ms  14.0.222.63.in-addr.arpa [63.222.0.14]
  8  236 ms  225 ms  213 ms  206.4.250.129.in-addr.arpa [129.250.4.206]
  9  68 ms  99 ms  59 ms  144.5.250.129.in-addr.arpa [129.250.5.144]
 10 172 ms 148 ms 153 ms  96.4.250.129.in-addr.arpa [129.250.4.96]
 11 250 ms 215 ms 213 ms  189.3.250.129.in-addr.arpa [129.250.3.189]
 12 236 ms 230 ms 244 ms  49.6.250.129.in-addr.arpa [129.250.6.49]
 13 256 ms 222 ms 235 ms  150.254.1.204.in-addr.arpa [204.1.254.150]
 14 246 ms 225 ms 226 ms  8.32.0.192.in-addr.arpa [192.0.32.8]

Trace complete.

C:\Users\Argy>
```

Ερωτήσεις σχετικά με το ICMP

12. Πως θα δείτε μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP;

Εκτελούμε την εντολή icmp στο πλαίσιο.

The image shows a Wireshark capture of ICMP traffic. The packet list pane displays several ICMP Echo (ping) requests and time-to-live exceeded messages. The packet details pane shows the structure of the first ICMP Echo request (Frame 6).

No.	Time	Source	Destination	Protocol	Length	Info
6	2.740962	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=
7	2.752837	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
8	2.755185	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=108/27648, ttl=
9	2.762988	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
10	2.765326	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=109/27904, ttl=
11	2.772946	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
41	3.778967	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=110/28160, ttl=
42	3.797755	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
43	3.799791	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=111/28416, ttl=
44	3.819622	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
45	3.821958	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=112/28672, ttl=
46	3.840661	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
71	4.841312	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=113/28928, ttl=
72	4.865877	178.59.103.117	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
73	4.868238	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=114/29184, ttl=
74	4.887869	178.59.103.117	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra

Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_18:02:2f (18:d6:c7:18:02:2f), Dst: Zte_cf:bb:b0 (74:a7:8e:cf:bb:b0)
> Internet Protocol Version 4, Src: 192.168.1.45, Dst: 192.0.32.8
> Internet Control Message Protocol

0000 74 a7 8e cf bb b0 18 d6 c7 18 02 2f 08 00 45 00 t......./..E.
0010 00 5c 61 63 00 00 01 01 b6 60 c0 a8 01 2d c0 00 .\ac.....
0020 20 08 08 00 f7 93 00 01 00 6b 00 00 00 00 00 00k.....

wireshark_A2FCB102-B16C-458A-8FFC-DFCB7EAE888F_20190110133629_a11876.pcapng | Packets: 88 · Displayed: 24 (27.3%) · Dropped: 0 (0.0%) | Profile: Default

13. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Echo Request.

- Ποια είναι η IP διεύθυνση του destination;
- Πόσο είναι το time-to-live του πακέτου;
- Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει;

a) Η IP διεύθυνση του destination όπως φαίνεται και στη παραπάνω εικόνα είναι η: 192.0.32.8

- b) Κάνοντας κλικ στο πεδίο Internet Protocol Version 4 μπορούμε να βρούμε το πεδίο Time to live όπου στη συγκεκριμένη περίπτωση είναι 1.

The image shows a Wireshark packet capture on a *Wi-Fi 2 interface. The packet list pane displays several ICMP Echo (ping) requests and responses. The packet details pane for the selected packet (No. 7) shows the Internet Protocol Version 4 header with a Time to live field set to 1. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
6	2.740962	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=
7	2.752837	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
8	2.755185	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=108/27648, ttl=
9	2.762988	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
10	2.765326	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=109/27904, ttl=
11	2.772946	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
41	3.778967	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=110/28160, ttl=
42	3.797755	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
43	3.799791	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=111/28416, ttl=
44	3.819622	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
45	3.821958	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=112/28672, ttl=
46	3.840661	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
71	4.841312	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=113/28928, ttl=
72	4.865877	178.59.103.117	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
73	4.868238	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=114/29184, ttl=
74	4.887869	178.59.103.117	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra

Packet details for packet 7:

- Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
- Ethernet II, Src: Tp-LinkT_18:02:2f (18:d6:c7:18:02:2f), Dst: Zte_cf:bb:b0 (74:a7:8e:cf:bb:b0)
- Internet Protocol Version 4, Src: 192.168.1.45, Dst: 192.0.32.8
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 92
 - Identification: 0x6163 (24931)
 - > Flags: 0x0000
 - > Time to live: 1
 - > [Expert Info (Note/Sequence): "Time To Live" only 1]
 - Protocol: ICMP (1)
 - Header checksum: 0xb660 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.45
 - Destination: 192.0.32.8
 - > Internet Control Message Protocol

Packet bytes:

```
0010  00 5c 61 63 00 00 01 01 b6 60 c0 a8 01 2d c0 00  .\ac... .k.....
0020  20 08 08 00 f7 93 00 01 00 6b 00 00 00 00 00 00  .....k.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

- c) Το μέγεθος των δεδομένων είναι 92-20=72.

14. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Time Exceeded.

- a. Ποια είναι η IP διεύθυνση του destination; Ποια είναι η IP διεύθυνση του Source;

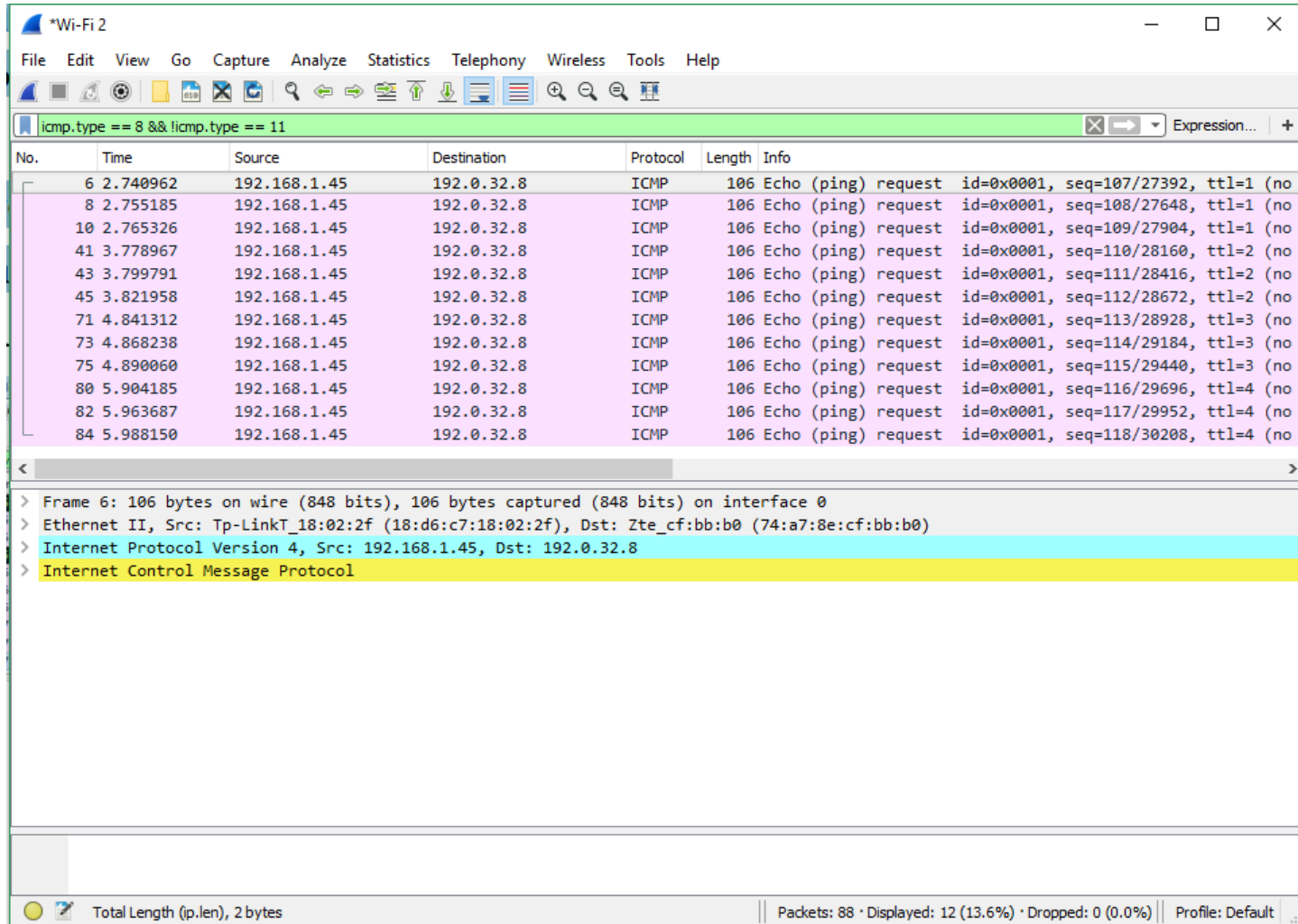
Εφαρμόζω την εντολή **icmp.type == 11** και μου εμφανίζει τη λίστα με όλα τα ICMP Time Exceeded.

Όπως φαίνεται και στη παρακάτω εικόνα το ip του Source είναι: 192.168.1.1

Και του destination είναι: 192.18.1.45

15. Ελέγχοντας το time-to-live των διαδοχικών πακέτων ICMP Echo Request, τί παρατηρείτε; Για ποιο λόγο γίνεται αυτό;

Παρατηρώ ότι το TTL αυξάνεται κατά 1 ανά τρία πακέτα ξεκινώντας από TTL ίσο με 1. Η διαδικασία traceroute προσπαθεί να διαπιστώσει όλους του κόμβους του δικτύου μέχρι τη διεύθυνση του host που έχουμε ορίσει. Αυτό το επιτυγχάνει χρησιμοποιώντας τα ICMP πακέτα τύπου Time Exceeded που στέλνονται στον αποστολέα ενός πακέτου όταν ο χρόνος ζωής του πακέτου εξαντληθεί. Γι αυτόν τον λόγο αυξάνει σταδιακά το TTL των εξερχόμενων πακέτων ώστε αυτό να εξαντλείτε σε διαφορετικό κόμβο κάθε φορά. Για πιο έγκυρα αποτελέσματα η διαδικασία στέλνει τρία πακέτα πριν αυξήσει το TTL.



No.	Time	Source	Destination	Protocol	Length	Info
6	2.740962	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=1 (no
8	2.755185	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=108/27648, ttl=1 (no
10	2.765326	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=109/27904, ttl=1 (no
41	3.778967	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=110/28160, ttl=2 (no
43	3.799791	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=111/28416, ttl=2 (no
45	3.821958	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=112/28672, ttl=2 (no
71	4.841312	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=113/28928, ttl=3 (no
73	4.868238	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=114/29184, ttl=3 (no
75	4.890060	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=115/29440, ttl=3 (no
80	5.904185	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=116/29696, ttl=4 (no
82	5.963687	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=117/29952, ttl=4 (no
84	5.988150	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=118/30208, ttl=4 (no

> Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_18:02:2f (18:d6:c7:18:02:2f), Dst: Zte_cf:bb:b0 (74:a7:8e:cf:bb:b0)
> Internet Protocol Version 4, Src: 192.168.1.45, Dst: 192.0.32.8
> Internet Control Message Protocol

Total Length (ip.len), 2 bytes | Packets: 88 · Displayed: 12 (13.6%) · Dropped: 0 (0.0%) | Profile: Default

16. Υπολογίστε το χρόνο ανάμεσα στο 1ο ICMP Echo Request και το αντίστοιχο (1ο) ICMP Time Exceeded και συγκρίνετέ τον με τους χρόνους που δίνει αντίστοιχα το πρώτο βήμα της εκτέλεσης της εντολής traceroute στο command prompt παράθυρο.

Το πρώτο ICMP echo Request είναι: 2.740962

Το πρώτο ICMP Time Exceeded είναι: 2.752837

Οπου $2.740962 - 2.752837 = 0.011875$ δηλαδή 11ms όπως λείει και το traceroute

Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp.type == 11

No.	Time	Source	Destination	Protocol	Length	Info
6	2.740962	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=
7	2.752837	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
8	2.755185	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=108/27648, ttl=
9	2.762988	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
10	2.765326	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=109/27904, ttl=
11	2.772946	192.168.1.1	192.168.1.45	ICMP	134	Time-to-live exceeded (Time to live exceeded in tra
41	3.778967	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=110/28160, ttl=
42	3.797755	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
43	3.799791	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=111/28416, ttl=
44	3.819622	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
45	3.821958	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=112/28672, ttl=
46	3.840661	46.103.127.42	192.168.1.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
71	4.841312	192.168.1.45	192.0.32.8	ICMP	106	Echo (ping) request id=0x0001, seq=113/28928, ttl=

> Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0

> Ethernet II, Src: Tp-LinkT_18:02:2f (18:d6:c7:18:02:2f), Dst: Zte_cf:bb:b0 (74:a7:8e:cf:bb:b0)

> Internet Protocol Version 4, Src: 192.168.1.45, Dst: 192.0.32.8

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 92

Identification: 0x6163 (24931)

> Flags: 0x0000

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0xb660 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.45

Destination: 192.0.32.8

0010 00 5c 61 63 00 00 01 01 b6 60 c0 a8 01 2d c0 00 .\ac....`.....

0020 20 08 08 00 f7 93 00 01 00 6b 00 00 00 00 00 00k.....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00k.....

Total Length (ip.len), 2 bytes

Packets: 88 · Displayed: 24 (27.3%) · Dropped: 0 (0.0%) | Profile: Default

17. Αναφέρατε όλες τις source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα. Υπάρχει αντιστοιχία με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt παράθυρο;

Εφαρμόζω το φίλτρο **icmp** όπου θα μου εμφανίσει όλα τα Icmp πακέτα Echo Request και Time exceeded.

Ανοίγοντας τα endpoints για IPV4 παρατηρούμε ότι υπάρχει αντιστοιχία μεταξύ των source IP και της εντολής tracer στο cmd.

Γραμμή εντολών

Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\Argy>tracert www.iana.org
Tracing route to ianawww.vip.icann.org [192.0.32.8]
over a maximum of 30 hops:

 1 11 ms 7 ms 7 ms 192.168.1.1 [192.168.1.1]
 2 18 ms 19 ms 18 ms 42.127.103.46.in-addr.arpa [46.103.127.42]
 3 24 ms 19 ms 19 ms 117.103.59.178.in-addr.arpa [178.59.103.117]
 4 57 ms 22 ms 22 ms 210.2.87.78.in-addr.arpa [78.87.2.210]
 5 27 ms 25 ms 29 ms 53.173.218.63.in-addr.arpa [63.218.173.53]
 6 83 ms 61 ms 65 ms 138.13.223.63.in-addr.arpa [63.223.13.138]
 7 89 ms 81 ms 98 ms 14.0.222.63.in-addr.arpa [63.222.0.14]
 8 236 ms 225 ms 213 ms 206.4.250.129.in-addr.arpa [129.250.4.206]
 9 68 ms 99 ms 59 ms 144.5.250.129.in-addr.arpa [129.250.5.144]
10 172 ms 148 ms 153 ms 96.4.250.129.in-addr.arpa [129.250.4.96]
11 250 ms 215 ms 213 ms 189.3.250.129.in-addr.arpa [129.250.3.189]
12 236 ms 230 ms 244 ms 49.6.250.129.in-addr.arpa [129.250.6.49]
13 256 ms 222 ms 235 ms 150.254.1.204.in-addr.arpa [204.1.254.150]
14 246 ms 225 ms 226 ms 8.32.0.192.in-addr.arpa [192.0.32.8]

Trace complete.
C:\Users\Argy>

Wireshark · Endpoints · kappa2.pcapng

Ethernet · 2		IPv4 · 6		IPv6		TCP		UDP											
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	A									
46.103.127.42	3	210	3	210	0	0	—	—	—	—									
78.87.2.210	3	330	3	330	0	0	—	—	—	—									
178.59.103.117	3	210	3	210	0	0	—	—	—	—									
192.0.32.8	12	1272	0	0	12	1272	—	—	—	—									
192.168.1.1	3	402	3	402	0	0	—	—	—	—									
192.168.1.45	24	2424	12	1272	12	1152	—	—	—	—									

☐ Name resolution ☒ Limit to display filter Endpoint Types Copy Close Help