

ΕΡΓΑΣΙΑ ΜΕ ΧΡΗΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ Wireshark

ΠΑΛΑΙΟΛΟΓΟΣ ΚΛΕΑΝΘΗΣ p3180136

ΜΑΥΡΙΔΗΣ ΙΩΑΝΝΗΣ p3180106

ΜΕΡΟΣ Α

```
Γραμμή εντολών
Microsoft Windows [Version 10.0.19045.2364]
(c) Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.

C:\Users\kleop>tracert www.ietf.org

Tracing route to e1630.c.akamaiedge.net [184.24.168.125]
over a maximum of 30 hops:
  0  2 ms  2 ms  1 ms  H1600V7.home [192.168.1.1]
  1  8 ms  7 ms  8 ms  80.106.125.100
  2 23 ms 15 ms 16 ms 79.128.225.148
  3 22 ms 21 ms 22 ms 62.75.3.117
  4 50 ms 51 ms 50 ms 62.75.6.190
  5 66 ms 49 ms 50 ms 62.75.27.134
  6 63 ms 62 ms 62 ms ae1.r01.fra02.icn.netarch.akamai.com [23.210.52.34]
  7 75 ms 64 ms 62 ms ae11.r01.fra02.icn.netarch.akamai.com [95.100.192.161]
  8 49 ms 55 ms 58 ms ae1.r02.fra03.icn.netarch.akamai.com [23.210.54.37]
  9 61 ms 196 ms 180 ms ae34.r02.border101.fra03.fab.netarch.akamai.com [23.210.54.23]
 10 * * * Request timed out.
 11 * * * Request timed out.
 12 * * * Request timed out.
 13 * * * Request timed out.
 14 49 ms 49 ms 49 ms e184-24-168-125.deploy.static.akamaitechnologies.com [184.24.168.125]

Trace complete.

C:\Users\kleop>
```

1) Η χρονική διάρκεια της ανίχνευσης είναι 79,866756 sec.

2) Παρουσίαση πίνακα

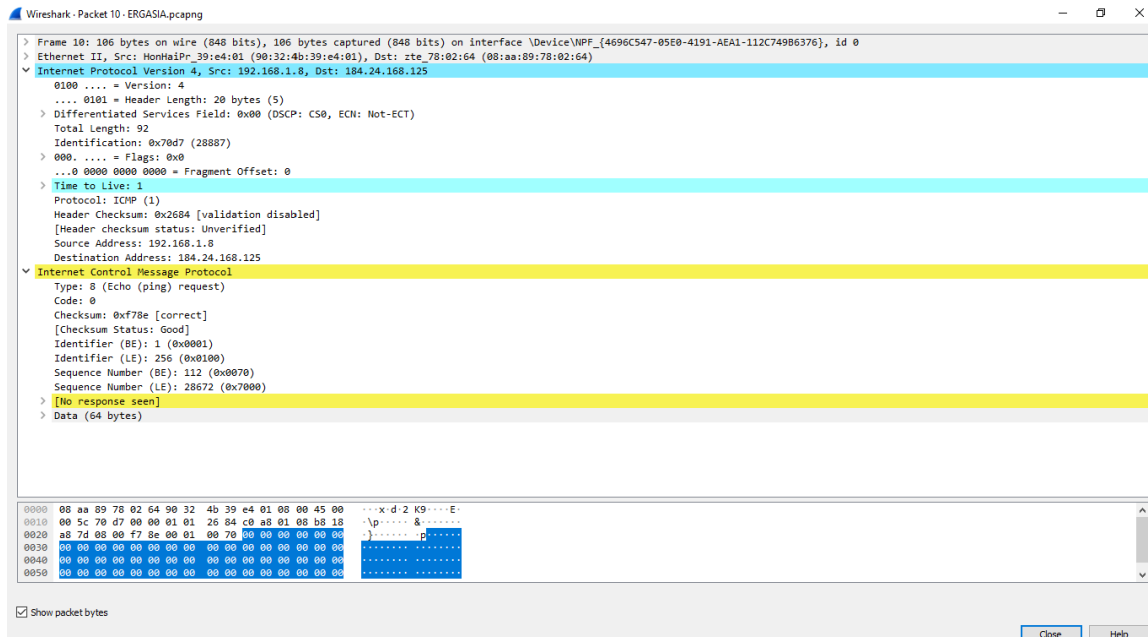
ΕΠΙΠΕΔΟ NETWORK	ΕΠΙΠΕΔΟ TRANSPORT	ΕΠΙΠΕΔΟ APPLICATION
ARP	UDP	TLSv 1.2
ICMPv6	TCP	TLSv 1.3
IPv4		DNS
IPv6		SSDP
		NBNS
		QUIC

3) Πάνω από το UDP τρέχουν τα εξής: QUIC, DNS, SSDP, NBNS

Πάνω από το TCP τρέχουν τα εξής: TLSv 1.2, TLSv 1.3

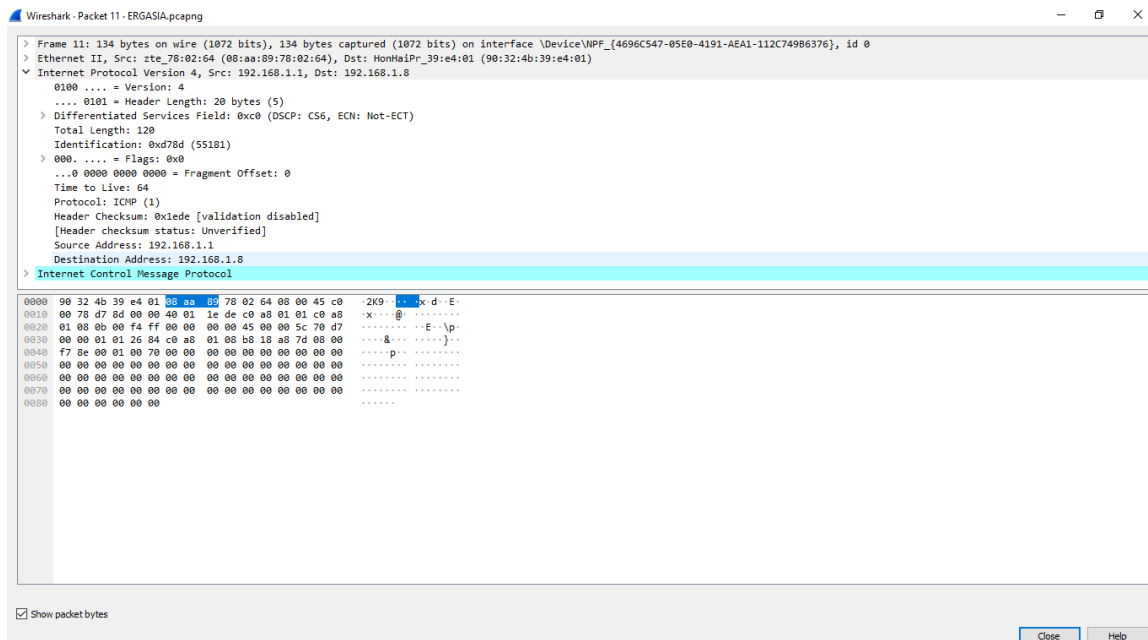
4) Για να εμφανίζονται στο παράθυρο του Wireshark μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP θα χρησιμοποιήσω το φίλτρο icmpv6

- 5) a. Η IP Destination address είναι : 184.24.168.125
b. Το time-to-live του πακέτου είναι 1
c. Το μέγεθος είναι 92 bytes



6)

- 7) a. Η IP Destination address είναι : 192.168.1.8
b. Η IP Source address είναι : 192.168.1.1



8) Οι source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα είναι οι εξής :

- i. 192.168.1.1
- ii. 80.106.125.100
- iii. 79.128.225.148
- iv. 62.75.3.117
- v. 62.75.6.190
- vi. 62.75.27.134
- vii. 23.210.52.34
- viii. 95.100.192.161
- ix. 23.210.54.37
- x. 23.210.54.23

Υπάρχει μερική αντιστοίχιση μεταξύ των διηθήσεων που παρουσιάσαμε παραπάνω και αυτών που εμφανίστηκαν στο command prompt παράθυρο.

ΜΕΡΟΣ Β

1. Για το IPv6 : στάλθηκαν 15 UDP πακέτα και για το TCP 87.

Για το IPv4 : στάλθηκαν 78 UDP πακέτα και για το TCP 337.

Wireshark - Protocol Hierarchy Statistics - B.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU/s
▼ Frame	100.0	521	100.0	297442	234 k	0	0	0	521
▼ Ethernet	100.0	521	2.5	7402	5826	0	0	0	521
▼ Internet Protocol Version 6	20.0	104	1.4	4160	3274	0	0	0	104
> User Datagram Protocol	2.9	15	0.0	120	94	0	0	0	15
> Transmission Control Protocol	16.7	87	15.2	45071	35 k	43	6269	4934	87
Internet Control Message Protocol v6	0.4	2	0.0	56	44	2	56	44	2
▼ Internet Protocol Version 4	80.0	417	2.8	8348	6570	0	0	0	417
> User Datagram Protocol	15.0	78	0.2	624	491	0	0	0	78
> Transmission Control Protocol	64.7	337	73.8	219395	172 k	249	169577	133 k	337
Internet Group Management Protocol	0.4	2	0.0	16	12	2	16	12	2

No display filter.

2. Τα endpoints είναι τα εξής :

Wireshark - Endpoints - B.pcapng

Endpoint Settings

☐ Name resolution

☐ Limit to display filter

Copy

Map

Protocol

☐ Bluetooth

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ MPTCP

☐ NCP

☐ openSAFETY

☐ RSVP

☐ SCTP

☐ SLL

☐ ...

Filter list for specific type

Ethernet · 8

IPv4 · 10

IPv6 · 7

TCP · 33

UDP · 31

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:02	1	46 byte	0	0 byte	1	46 byte
01:00:5e:00:00:f6	17	4,650 KiB	0	0 byte	17	4,650 KiB
08:aa:89:78:02:64	392	180,350 KiB	189	143,662 KiB	203	36,688 KiB
08:aa:89:78:02:65	94	100,541 KiB	94	100,541 KiB	0	0 byte
33:33:00:00:00:16	2	180 byte	0	0 byte	2	180 byte
33:33:00:00:00:f6	15	4,709 KiB	0	0 byte	15	4,709 KiB
52:59:52:a0:34:24	35	9,580 KiB	35	9,580 KiB	0	0 byte
90:32:4b:39:e4:01	486	280,891 KiB	203	36,688 KiB	283	244,203 KiB

Close

Help

Οι συσκευές είναι οι εξής:

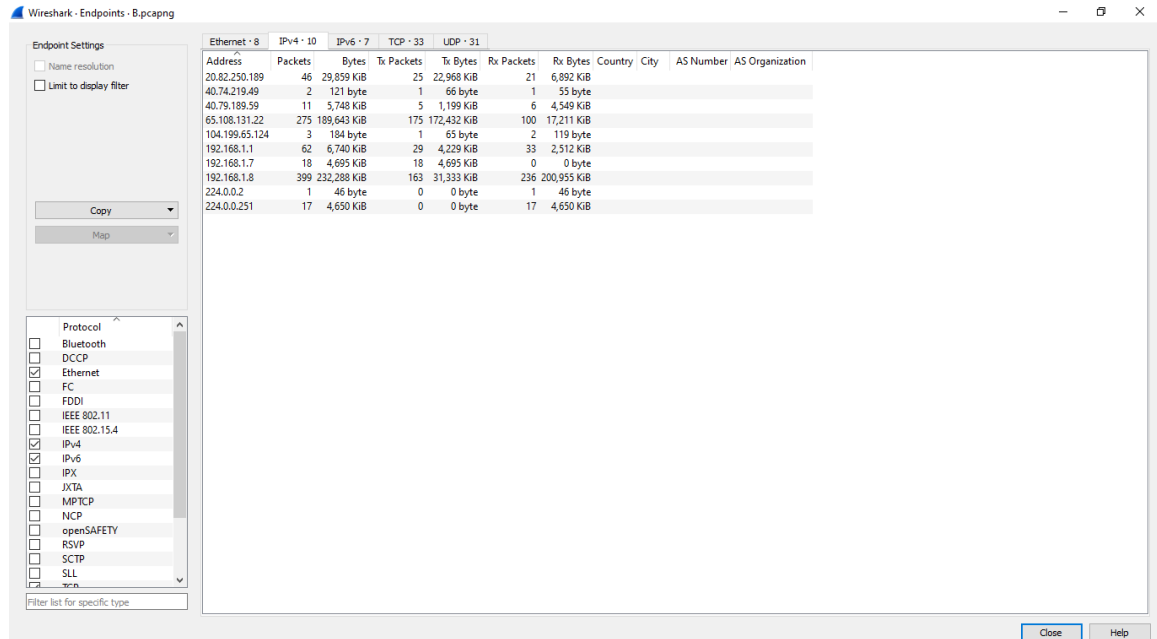
08:aa:89:78:02:64

08:aa:89:78:02:64

52:59:52:a0:34:24

90:32:4b:39:e4:01

3. endpoints IPv4 :



Wireshark - Endpoints - B.pcapng

Endpoint Settings

- ☐ Name resolution
- ☐ Limit to display filter

Copy

Map

Protocol

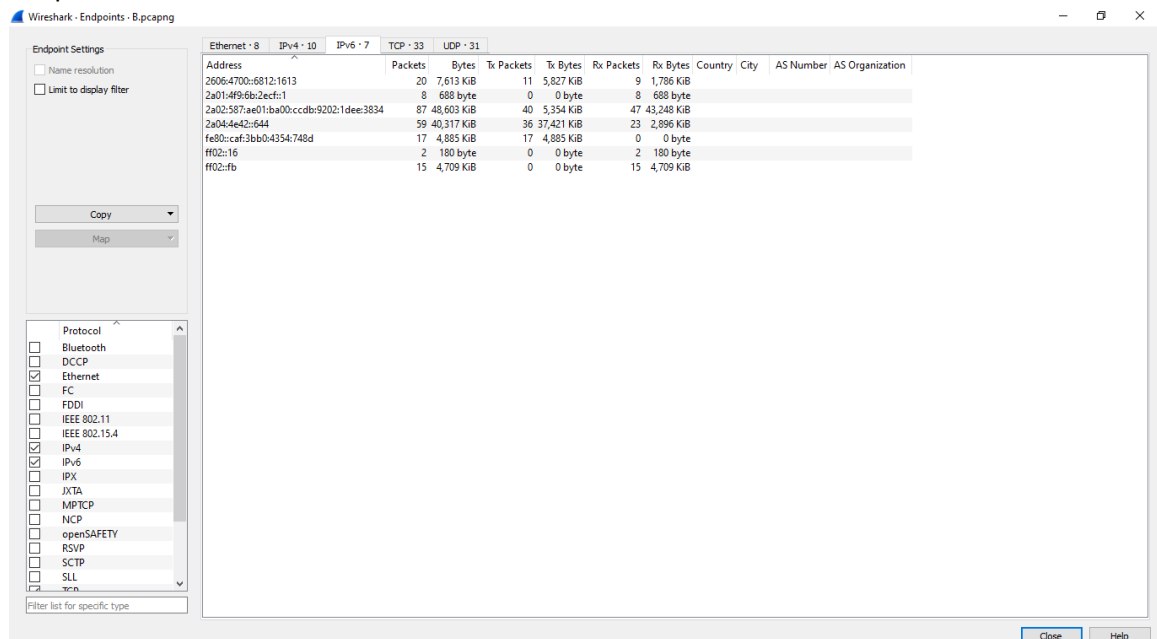
- ☐ Bluetooth
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ JXTA
- ☐ MPTCP
- ☐ NCP
- ☐ openSAFETY
- ☐ RSVP
- ☐ SCTP
- ☒ SLL

Filter list for specific type

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
20.82.250.189	46	29,859 KiB	25	22,968 KiB	21	6,892 KiB				
40.74.219.49	2	121 byte	1	66 byte	1	55 byte				
40.79.189.59	11	5,748 KiB	5	1,199 KiB	6	4,549 KiB				
65.108.131.22	275	189,643 KiB	175	172,432 KiB	100	17,211 KiB				
104.199.65.124	3	184 byte	1	65 byte	2	119 byte				
192.168.1.1	62	6,740 KiB	29	4,229 KiB	33	2,512 KiB				
192.168.1.7	18	4,695 KiB	18	4,695 KiB	0	0 byte				
192.168.1.8	399	232,288 KiB	163	31,333 KiB	236	200,955 KiB				
224.0.0.2	1	46 byte	0	0 byte	1	46 byte				
224.0.0.251	17	4,650 KiB	0	0 byte	17	4,650 KiB				

Close Help

endpoints IPv6 :



Wireshark - Endpoints - B.pcapng

Endpoint Settings

- ☐ Name resolution
- ☐ Limit to display filter

Copy

Map

Protocol

- ☐ Bluetooth
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ JXTA
- ☐ MPTCP
- ☐ NCP
- ☐ openSAFETY
- ☐ RSVP
- ☐ SCTP
- ☒ SLL

Filter list for specific type

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
2606:4700:f812:1613	20	7,613 KiB	11	5,827 KiB	9	1,786 KiB				
2a01:4f9:6b:2ecf::1	8	688 byte	0	0 byte	8	688 byte				
2a02:587:ae01:ba00:ccdb:9202:1dee:3834	87	48,603 KiB	40	5,354 KiB	47	43,248 KiB				
2a04:4e42::644	59	40,317 KiB	36	37,421 KiB	23	2,896 KiB				
fe80::caf:3bb0:4354:748d	17	4,885 KiB	17	4,885 KiB	0	0 byte				
ff02::16	2	180 byte	0	0 byte	2	180 byte				
ff02::fb	15	4,709 KiB	0	0 byte	15	4,709 KiB				

Close Help

Δεν υπάρχει κάποια ταύτιση των endpoints επίπεδο ethernet με αυτά του επιπέδου IP καθώς τα μεν αναφέρονται σε MAC διευθύνσεις και τα δε σε IP.

4. Τα ports που χρησιμοποιήθηκαν για ερώτηση προς τον DNS Server είναι τα εξής:

Src Port: 62084 Dst port:53

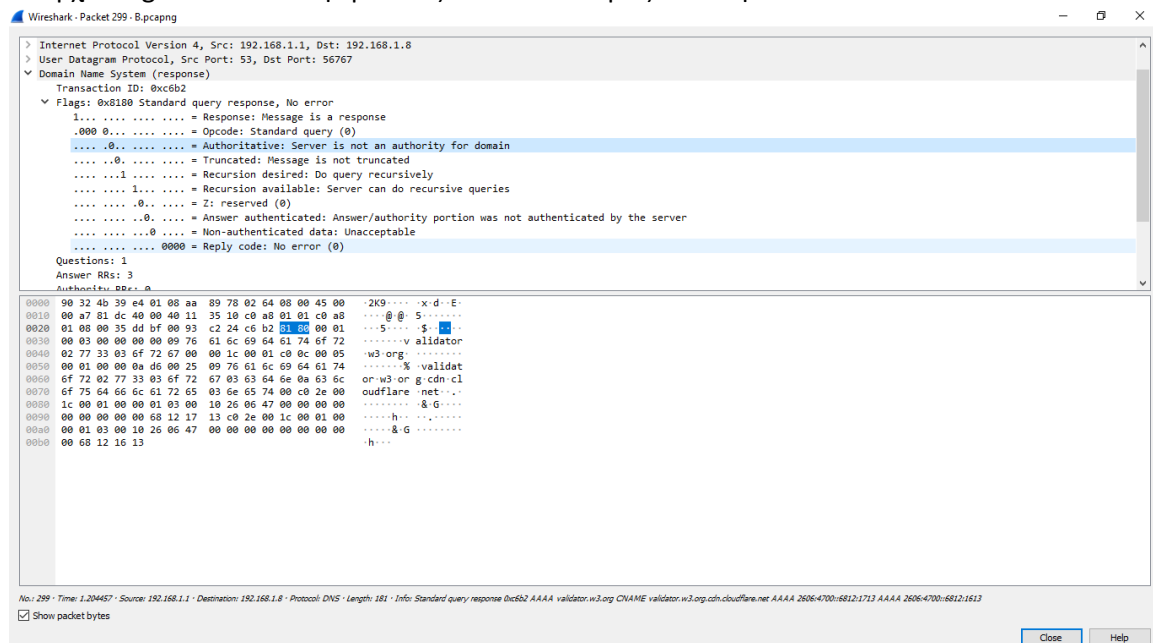
Src Port: 53755 Dst port:53

Src Port: 59280 Dst port:53
Src Port: 54361 Dst port:53
Src Port: 50870 Dst port:53
Src Port: 58998 Dst port:53
Src Port: 63285 Dst port:53
Src Port: 64404 Dst port:53
Src Port: 64086 Dst port:53
Src Port: 62723 Dst port:53
Src Port: 49451 Dst port:53
Src Port: 51934 Dst port:53
Src Port: 58664 Dst port:53
Src Port: 64427 Dst port:53
Src Port: 60222 Dst port:53
Src Port: 55975 Dst port:53
Src Port: 53988 Dst port:53
Src Port: 56767 Dst port:53
Src Port: 58701 Dst port:53
Src Port: 63585 Dst port:53
Src Port: 51548 Dst port:53
Src Port: 65334 Dst port:53
Src Port: 61111 Dst port:53
Src Port: 56110 Dst port:53
Src Port: 58963 Dst port:53
Src Port: 52663 Dst port:53

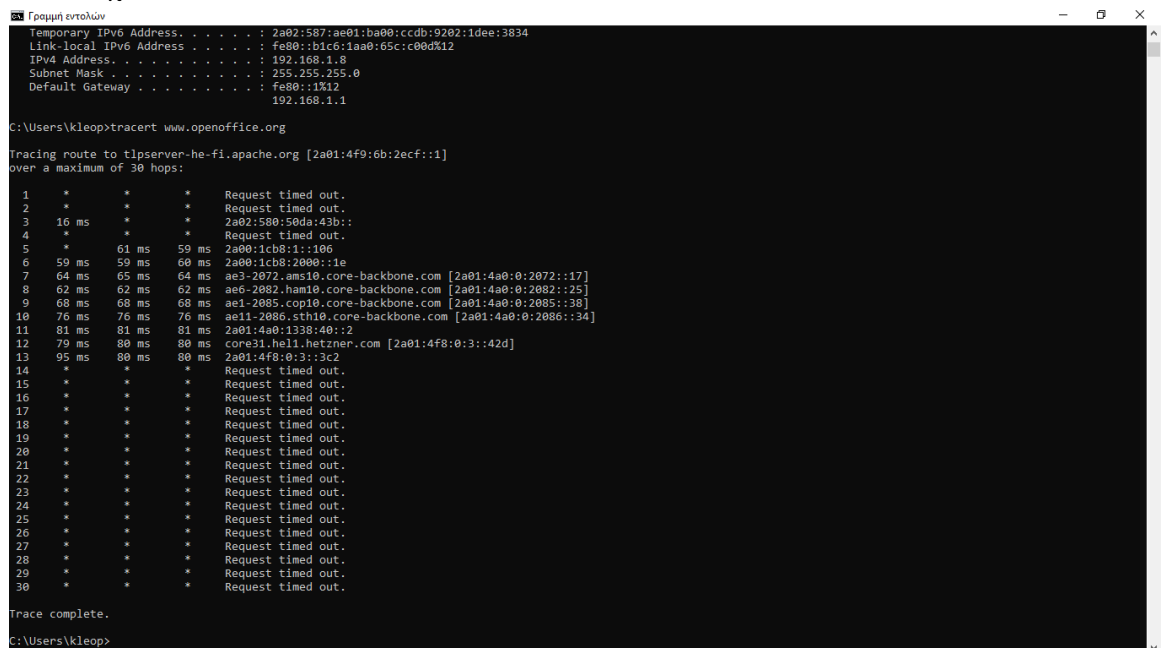
Τα αντίστοιχα που χρησιμοποιήθηκαν για την απάντηση του DNS server είναι ίδια με τα παραπάνω αλλά αντίστροφα.

5. Ο DNS server έχει το port 53 άρα κάθε αίτημα προς αυτόν έχει destination port 53 και το source είναι η IP διεύθυνσή μας. Επίσης, αν το πακέτο περιέχει αίτημα προς τον DNS αναγράφεται query : **Domain Name System (query)** και αν περιέχει απάντηση αναγράφεται response : **Domain Name System (response)**.

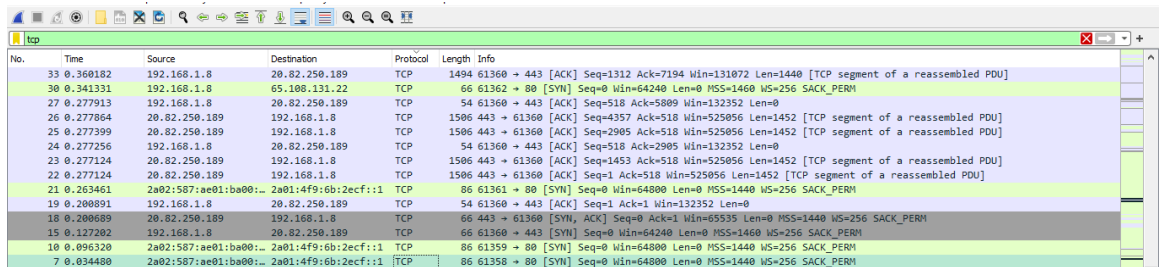
6. Υπάρχει flag το οποίο αναφέρει πως ο server που μας απάντησε δεν είναι authoritative.



7. Το όνομα www.openoffice.org είναι κανονικό dns όνομα και η διεύθυνση που του αντιστοιχεί είναι : 2a01:4f9:6b:2ecf::1



8.



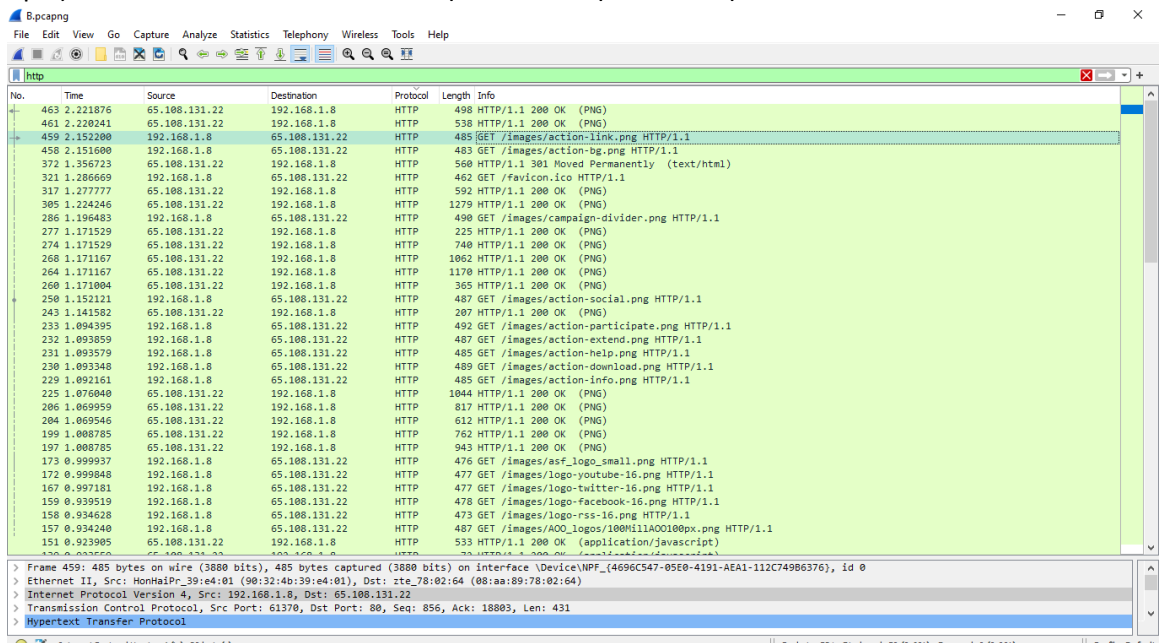
No.	Time	Source	Destination	Protocol	Length	Info
33	0.360182	192.168.1.8	20.82.250.189	TCP	1494	61360 → 443 [ACK] Seq=1312 Ack=7194 Win=131072 Len=1440 [TCP segment of a reassembled PDU]
30	0.341331	192.168.1.8	65.108.131.22	TCP	66	61362 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
27	0.277913	192.168.1.8	20.82.250.189	TCP	54	61360 → 443 [ACK] Seq=518 Ack=5809 Win=132352 Len=0
26	0.277864	20.82.250.189	192.168.1.8	TCP	1506	443 → 61360 [ACK] Seq=4357 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
25	0.277399	20.82.250.189	192.168.1.8	TCP	1506	443 → 61360 [ACK] Seq=2905 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
24	0.277256	192.168.1.8	20.82.250.189	TCP	54	61360 → 443 [ACK] Seq=518 Ack=2905 Win=132352 Len=0
23	0.277124	20.82.250.189	192.168.1.8	TCP	1506	443 → 61360 [ACK] Seq=1453 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
22	0.277124	20.82.250.189	192.168.1.8	TCP	1506	443 → 61360 [ACK] Seq=1 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
21	0.263461	2a02:587:ae01:ba00::2a01:4f9:6b:2ecf::1	192.168.1.8	TCP	86	61361 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
19	0.208891	192.168.1.8	20.82.250.189	TCP	54	61360 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
18	0.208689	20.82.250.189	192.168.1.8	TCP	66	443 → 61360 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
15	0.127202	192.168.1.8	20.82.250.189	TCP	66	61360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10	0.096320	2a02:587:ae01:ba00::2a01:4f9:6b:2ecf::1	192.168.1.8	TCP	86	61359 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
7	0.034400	2a02:587:ae01:ba00::2a01:4f9:6b:2ecf::1	192.168.1.8	TCP	86	61358 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM

Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή μας και του συστήματος που φιλοξενεί το www.openoffice.org είναι αυτά με τα νούμερα 7, 10, 15.

9. Όπως βλέπουμε παρακάτω, εμείς στέλνουμε αιτήματα μέσω των port : 61360, 61368, 61372, 61373 κλπ. και ο server λαμβάνει και στέλνει αιτήματα μέσω του port 443.

```
Transmission Control Protocol, Src Port: 61360, Dst Port: 443, Seq: 0, Len: 0
Transmission Control Protocol, Src Port: 61368, Dst Port: 443, Seq: 0, Len: 0
Transmission Control Protocol, Src Port: 61372, Dst Port: 443, Seq: 0, Len: 0
Transmission Control Protocol, Src Port: 61373, Dst Port: 443, Seq: 0, Len: 0
```

10. Μπορούμε να δούμε τα πακέτα που περιέχουν HTTP GET αίτημα από τον Browser μας προς τον Web Server. Η IP διεύθυνση που στάλθηκαν είναι η : 65.108.131.22



No.	Time	Source	Destination	Protocol	Length	Info
463	2.221876	65.108.131.22	192.168.1.8	HTTP	498	HTTP/1.1 200 OK (PNG)
461	2.220241	65.108.131.22	192.168.1.8	HTTP	538	HTTP/1.1 200 OK (PNG)
459	2.152280	192.168.1.8	65.108.131.22	HTTP	485	GET /images/action-link.png HTTP/1.1
458	2.151600	192.168.1.8	65.108.131.22	HTTP	483	GET /images/action-bg.png HTTP/1.1
372	1.356723	65.108.131.22	192.168.1.8	HTTP	560	HTTP/1.1 301 Moved Permanently (text/html)
321	1.286669	192.168.1.8	65.108.131.22	HTTP	462	GET /favicon.ico HTTP/1.1
317	1.277777	65.108.131.22	192.168.1.8	HTTP	592	HTTP/1.1 200 OK (PNG)
305	1.224246	65.108.131.22	192.168.1.8	HTTP	1279	HTTP/1.1 200 OK (PNG)
286	1.196483	192.168.1.8	65.108.131.22	HTTP	490	GET /images/campaign-divider.png HTTP/1.1
277	1.171529	65.108.131.22	192.168.1.8	HTTP	225	HTTP/1.1 200 OK (PNG)
274	1.171529	65.108.131.22	192.168.1.8	HTTP	740	HTTP/1.1 200 OK (PNG)
268	1.171167	65.108.131.22	192.168.1.8	HTTP	1062	HTTP/1.1 200 OK (PNG)
264	1.171167	65.108.131.22	192.168.1.8	HTTP	1170	HTTP/1.1 200 OK (PNG)
260	1.171004	65.108.131.22	192.168.1.8	HTTP	365	HTTP/1.1 200 OK (PNG)
250	1.152121	192.168.1.8	65.108.131.22	HTTP	487	GET /images/action-social.png HTTP/1.1
243	1.141502	65.108.131.22	192.168.1.8	HTTP	207	HTTP/1.1 200 OK (PNG)
233	1.094395	192.168.1.8	65.108.131.22	HTTP	492	GET /images/action-participate.png HTTP/1.1
232	1.093859	192.168.1.8	65.108.131.22	HTTP	487	GET /images/action-extend.png HTTP/1.1
231	1.093579	192.168.1.8	65.108.131.22	HTTP	485	GET /images/action-help.png HTTP/1.1
230	1.093340	192.168.1.8	65.108.131.22	HTTP	489	GET /images/action-download.png HTTP/1.1
229	1.092161	192.168.1.8	65.108.131.22	HTTP	485	GET /images/action-info.png HTTP/1.1
225	1.076040	65.108.131.22	192.168.1.8	HTTP	1044	HTTP/1.1 200 OK (PNG)
206	1.069959	65.108.131.22	192.168.1.8	HTTP	817	HTTP/1.1 200 OK (PNG)
204	1.069546	65.108.131.22	192.168.1.8	HTTP	612	HTTP/1.1 200 OK (PNG)
199	1.008785	65.108.131.22	192.168.1.8	HTTP	762	HTTP/1.1 200 OK (PNG)
197	1.008785	65.108.131.22	192.168.1.8	HTTP	943	HTTP/1.1 200 OK (PNG)
173	0.999937	192.168.1.8	65.108.131.22	HTTP	476	GET /images/asf_logo_small.png HTTP/1.1
172	0.999848	192.168.1.8	65.108.131.22	HTTP	477	GET /images/logo-youtube-16.png HTTP/1.1
167	0.997181	192.168.1.8	65.108.131.22	HTTP	477	GET /images/logo-twitter-16.png HTTP/1.1
159	0.939519	192.168.1.8	65.108.131.22	HTTP	478	GET /images/logo-facebook-16.png HTTP/1.1
158	0.934628	192.168.1.8	65.108.131.22	HTTP	473	GET /images/logo-rss-16.png HTTP/1.1
157	0.934240	192.168.1.8	65.108.131.22	HTTP	487	GET /images/AOO_logos/100x111AAO100px.png HTTP/1.1
151	0.923905	65.108.131.22	192.168.1.8	HTTP	533	HTTP/1.1 200 OK (application/javascript)

> Frame 459: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface DeviceNPF_{4696C547-05E0-4191-AE41-112C74986376}, id 0
> Ethernet II, Src: NonHaltPr, 39:e4:01 (98:32:4b:39:e4:01), Dst: zte_78:02:64 (08:aa:09:78:02:64)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 65.108.131.22
> Transmission Control Protocol, Src Port: 61370, Dst Port: 80, Seq: 856, Ack: 18803, Len: 431
> Hypertext Transfer Protocol

