

ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΡΓΑΣΙΑ 1

ΜΕΡΟΣ Α

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.

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

Tracing route to e1630.c.akamaiedge.net [104.96.150.193]
over a maximum of 30 hops:

  0  1 ms  1 ms  1 ms  speedport.ip [192.168.1.1]
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  *      *      *      Request timed out.
  4  *      *      *      Request timed out.
  5  *      *      *      Request timed out.
  6  *      *      *      Request timed out.
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
  9  *      *      *      Request timed out.
 10 *      *      *      Request timed out.
 11 *      *      *      Request timed out.
 12 67 ms  63 ms  63 ms a104-96-150-193.deploy.static.akamaitechnologies.com [104.96.150.193]

Trace complete.

C:\Users\jtsin>
```

1)

No.	Time	Source	Destination	Protocol	Length	Info
1376	122.371864	104.16.95.80	192.168.1.5	TCP	66	[TCP Keep-Alive ACK]
1377	122.749848	192.168.1.5	178.79.208.44	TCP	55	[TCP Keep-Alive] 6259
1378	122.797889	178.79.208.44	192.168.1.5	TCP	54	[TCP Keep-Alive ACK]
1379	123.728959	192.168.1.5	104.96.150.193	TCP	55	[TCP Keep-Alive] 6253
1380	123.800828	104.96.150.193	192.168.1.5	TCP	66	[TCP Keep-Alive ACK]
1381	123.810794	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
1382	123.873608	104.96.150.193	192.168.1.5	ICMP	106	Echo (ping) reply
1383	123.874956	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
1384	123.884924	2a02:586:e830:e06a:...	2606:4700::6812:1634	TCP	75	[TCP Keep-Alive] 6254
1385	123.893087	2606:4700::6812:1634	2a02:586:e830:e06a:...	TCP	86	[TCP Keep-Alive ACK]
1386	123.938071	104.96.150.193	192.168.1.5	ICMP	106	Echo (ping) reply
1387	123.940619	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
1388	124.004879	104.96.150.193	192.168.1.5	ICMP	106	Echo (ping) reply
1389	124.005594	192.168.1.5	192.168.1.1	DNS	87	Standard query 0xb3fe
1390	124.008753	192.168.1.1	192.168.1.5	DNS	153	Standard query respon
1391	124.289141	192.168.1.5	104.96.150.193	TCP	55	[TCP Keep-Alive] 6253
1392	124.352061	104.96.150.193	192.168.1.5	TCP	66	[TCP Keep-Alive ACK]

Η ανίχνευση είχε διάρκεια 124.352061 δευτερόλεπτα

2)

LAYER 1(NETWORK)	LAYER 3(TRANSPORT)	LAYER 4 (APPLICATION)
ARP	TCP	DNS
ICMP	HTTP	SSDP
ICMPv6	QUIC	TLSv1.2
		TLSv1.3

3)

Τα πρωτόκολλα DNS, SSDP , QUIC, χρησιμοποιούν UDP.

Τα πρωτόκολλα TLSv1.2 , TLS v1.3 χρησιμοποιούν TCP.

4)

Το φίλτρο που θα χρησιμοποιήσουμε είναι το “icmp” .Το γράφουμε στο πεδίο των φίλτρων και η εφαρμογή μας εμφανίζει μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP.

5)

A)

icmp and icmp.type==8						
No.	Time	Source	Destination	Protocol	Length	Info
33	3.259372	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
34	3.261632	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded
35	3.262184	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
36	3.264322	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded
37	3.265389	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
38	3.267645	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded
116	4.276038	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
192	7.808111	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
551	11.804061	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
592	15.801472	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
726	19.796971	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request

104.96.150.193

B)

icmp and icmp.type==8

No.	Time	Source	Destination	Protocol	Length	Info
33	3.259372	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
34	3.261632	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded
35	3.262184	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
36	3.264322	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded
37	3.265389	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
38	3.267645	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded
116	4.276038	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
192	7.808111	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
551	11.804061	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
592	15.801472	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
726	19.796971	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
771	23.800610	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
802	27.809549	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
803	31.806138	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
827	35.801680	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
850	39.798760	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
866	43.798331	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request
881	47.803868	192.168.1.5	104.96.150.193	ICMP	106	Echo (ping) request

> Frame 33: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0

> Ethernet II, Src: IntelCor_d9:d3:f7 (40:ec:99:d9:d3:f7), Dst: 08:00:27:80:95:49 (08:00:27:80:95:49)

> Internet Protocol Version 4, Src: 192.168.1.5, Destination: 104.96.150.193

> 0100 = Version: 4

> 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0)

> 0000 00.. = Differentiated Services Codepoint

>00 = Explicit Congestion Notification

Total Length: 92

Identification: 0x6d05 (27909)

> 000. = Flags: 0x0

> 0... = Reserved bit: Not set

> .0.. = Don't fragment: Not set

> ..0. = More fragments: Not set

> ...0 0000 0000 0000 = Fragment Offset: 0

> Time to Live: 1

> [Expert Info (Note/Sequence): "Time To Live: 1"]

Protocol: ICMP (1)

Header Checksum: 0x0000 [validation disabled]

0000 10 50 72 eb fb 20 40 ec 99 d9 d3 f7 08 00 45

0010 00 5c 6d 05 00 00 01 01 00 00 c0 a8 01 05 68

0020 96 c1 08 00 f7 34 00 01 00 ca 00 00 00 00 00

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

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00

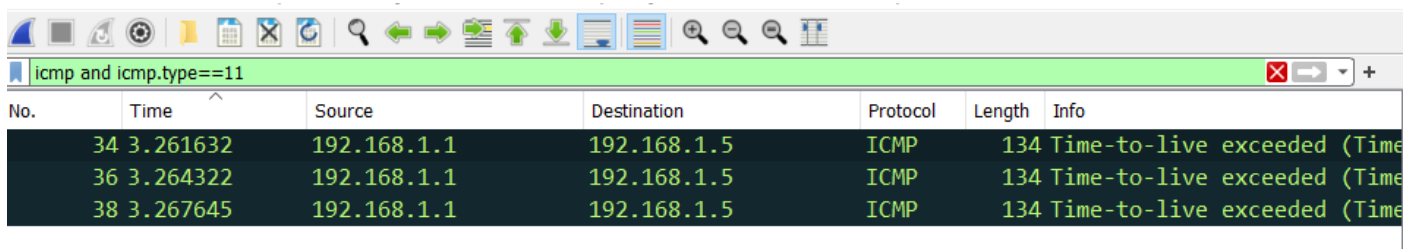
Time to live = 1

C)

[illegible]

Data length = 64

6)



No.	Time	Source	Destination	Protocol	Length	Info
34	3.261632	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded (Time
36	3.264322	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded (Time
38	3.267645	192.168.1.1	192.168.1.5	ICMP	134	Time-to-live exceeded (Time

A)

IP διεύθυνση του destination = 192.168.1.5

B)

IP διεύθυνση του source = 192.168.1.1

7)

Τρέχω την εντολή `tracert www.ieee.org`. Οι ενδιάμεσοι κόμβοι δεν απαντούν (μπορεί να είναι κομμένο το ring στη διαδρομή που ακολουθείται από τον provider μου).

Βλέπω αντιστοιχία στη διεύθυνση 192.168.1.1 η οποία είναι η διεύθυνση του υπολογιστή μου

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

Tracing route to e1630.c.akamaiedge.net [104.96.150.193]
over a maximum of 30 hops:

  1    1 ms    322 ms    2 ms    speedport.ip [192.168.1.1]
  2    *        *        *        Request timed out.
  3    *        *        *        Request timed out.
  4    *        *        *        Request timed out.
  5    *        *        *        Request timed out.
  6    *        *        *        Request timed out.
  7    *        *        *        Request timed out.
  8    *        *        *        Request timed out.
  9    *        *        *        Request timed out.
 10   *        *        *        Request timed out.
 11   *        *        *        Request timed out.
 12   74 ms    63 ms    62 ms    a104-96-150-193.deploy.static.akamaitechnologies.com [104.96.150.193]

Trace complete.
```

ΜΕΡΟΣ Β

1)

The image shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets, filtered by 'tcp'. The bottom pane shows the detailed view of the selected packet (Frame 19).

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
72	9.705561	192.168.1.5	65.108.131.22	TCP	54	51715 → 80 [ACK] Seq: 1921681511
71	9.705343	65.108.131.22	192.168.1.5	TCP	66	80 → 51715 [SYN, ACK] Seq: 1921681511
70	9.673404	20.73.130.64	192.168.1.5	TCP	54	443 → 51713 [ACK] Seq: 1921681511
69	9.643630	192.168.1.5	65.108.131.22	TCP	66	51716 → 80 [SYN] Seq: 1921681511
68	9.643088	192.168.1.5	65.108.131.22	TCP	66	51715 → 80 [SYN] Seq: 1921681511
67	9.616592	192.168.1.5	20.73.130.64	TCP	54	51713 → 443 [FIN, ACK] Seq: 1921681511
66	9.616212	192.168.1.5	20.73.130.64	TCP	54	51713 → 443 [ACK] Seq: 1921681511
64	9.611029	20.73.130.64	192.168.1.5	TCP	54	443 → 51713 [ACK] Seq: 1921681511
62	9.548620	192.168.1.5	20.73.130.64	TCP	1494	51713 → 443 [ACK] Seq: 1921681511
59	9.537689	2a02:586:e830:e06a::...	2a01:4f9:6b:2ecf::1	TCP	86	51714 → 80 [SYN] Seq: 1921681511
57	9.471658	192.168.1.5	20.73.130.64	TCP	54	51713 → 443 [ACK] Seq: 1921681511
55	9.471338	20.73.130.64	192.168.1.5	TCP	1514	443 → 51713 [ACK] Seq: 1921681511
54	9.471338	20.73.130.64	192.168.1.5	TCP	1514	443 → 51713 [ACK] Seq: 1921681511
53	9.471338	20.73.130.64	192.168.1.5	TCP	1514	443 → 51713 [ACK] Seq: 1921681511
52	9.471338	20.73.130.64	192.168.1.5	TCP	1514	443 → 51713 [ACK] Seq: 1921681511
51	9.412924	2a02:586:e830:e06a::...	2a01:111:f100:9001::...	TCP	74	62197 → 443 [ACK] Seq: 1921681511
49	9.399065	192.168.1.5	20.73.130.64	TCP	54	51713 → 443 [ACK] Seq: 1921681511
48	9.398892	20.73.130.64	192.168.1.5	TCP	66	443 → 51713 [SYN, ACK] Seq: 1921681511

Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Section number: 1

- Interface id: 0 (\Device\NPF_{E1E54C58-D430-...})
- Encapsulation type: Ethernet (1)
- Arrival Time: Jan 13, 2023 16:43:59.511672000
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1673621039.511672000 seconds
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 7.480900000 seconds]
- Frame Number: 19
- Frame Length: 74 bytes (592 bits)
- Capture Length: 74 bytes (592 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ipv6:tcp]
- [Coloring Rule Name: TCP]
- [Coloring Rule String: tcp]
- Ethernet II, Src: Sercomm_eb:fb:20 (10:50:72:eb:fb:20), Dst: 08:00:27:00:00:00

Packet 19 (74 bytes):

0000 40 ec 99 d9 d3 f7 10 50 72 eb fb 20 86 dd 60
0010 30 d5 00 14 06 71 26 03 10 26 24 00 00 01 00
0020 00 00 00 00 00 02 2a 02 05 86 e8 30 e0 6a 60
0030 e3 bf 3b 7a c9 78 01 bb d7 75 94 d7 ce 5f 7d
0040 20 4b 50 10 3f fe fa 4f 00 00

Wireshark interface: wireshark_Wi-FIVJF0Y1.pcapng

Packets: 635 · Displayed: 522 (82.2%) · Dropped: 0 (0.0%) Profile: Default

Στο κάτω μέρος της σελίδας, αφού βάλουμε το φίλτρο tcp, βλέπουμε ότι τα tcp πακέτα που στάλθηκαν είναι 522

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
94	9.823172	192.168.1.1	192.168.1.5	DNS	225	Standard query response
93	9.812453	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
92	9.812315	192.168.1.1	192.168.1.5	DNS	225	Standard query response
91	9.801553	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
90	9.801364	192.168.1.1	192.168.1.5	DNS	228	Standard query response
89	9.791909	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
88	9.791822	192.168.1.1	192.168.1.5	DNS	225	Standard query response
87	9.791584	192.168.1.1	192.168.1.5	DNS	178	Standard query response
86	9.781463	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
85	9.781138	192.168.1.5	192.168.1.1	DNS	91	Standard query 0xc877
41	9.340077	192.168.1.1	192.168.1.5	DNS	342	Standard query response
40	9.338390	192.168.1.1	192.168.1.5	DNS	310	Standard query response
39	9.328717	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xe143
38	9.328468	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xab8e
35	9.326578	192.168.1.1	192.168.1.5	DNS	131	Standard query response
33	9.290370	192.168.1.1	192.168.1.5	DNS	161	Standard query response
23	9.266412	192.168.1.5	192.168.1.1	DNS	78	Standard query 0xa6c6
22	9.266163	192.168.1.5	192.168.1.1	DNS	78	Standard query 0xde11

▼ Frame 22: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 Section number: 1
 > Interface id: 0 (\Device\NPF_{E1E54C58-D430-4...})
 Encapsulation type: Ethernet (1)
 Arrival Time: Jan 13, 2023 16:44:01.296881000
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1673621041.296881000 seconds
 [Time delta from previous captured frame: 0.000000000 seconds]
 [Time delta from previous displayed frame: 0.000000000 seconds]
 [Time since reference or first frame: 9.266163 seconds]
 Frame Number: 22
 Frame Length: 78 bytes (624 bits)
 Capture Length: 78 bytes (624 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]
 > Ethernet II, Src: IntelCor_d9:d3:f7 (40:ec:99:d3:f7:00), Dst: IntelCor_d9:d3:f7 (40:ec:99:d3:f7:00)

0000 10 50 72 eb fb 20 40 ec 99 d9 d3 f7 08 00 45
 0010 00 40 59 26 00 00 80 11 00 00 c0 a8 01 05 c0
 0020 01 01 df 6d 00 35 00 2c 83 94 de 13 01 00 00
 0030 00 00 00 00 00 00 03 77 77 77 0a 6f 70 65 6e
 0040 66 66 69 63 65 03 6f 72 67 00 00 01 00 01

wireshark_Wi-FiVJF0Y1.pcapng Packets: 635 · Displayed: 99 (15.6%) · Dropped: 0 (0.0%) Profile: Default

Στο κάτω μέρος της σελίδας , αφού βάλουμε το φίλτρο udp , βλέπουμε ότι τα udp πακέτα που στάλθηκαν είναι 99.

2)

The image shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets, with four DNS packets highlighted. The bottom pane shows the 'Endpoints' view for the selected Wi-Fi interface, displaying a table of endpoints and their associated traffic statistics. The 'Endpoint Settings' panel on the left is configured with 'Name resolution' checked and 'Limit to display filter' unchecked. The 'Protocol' list on the left shows 'Ethernet', 'IPv4', and 'IPv6' selected.

No.	Time	Source	Destination	Protocol	Length	Info
94	9.823172	192.168.1.1	192.168.1.5	DNS	225	Standard query response
93	9.812453	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
92	9.812315	192.168.1.1	192.168.1.5	DNS	225	Standard query response
91	9.801553	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4

Endpoint Settings	
<input checked="" type="checkbox"/> Name resolution	
<input type="checkbox"/> Limit to display filter	
Copy	
Map	
Protocol	
<input type="checkbox"/>	Bluetooth
<input type="checkbox"/>	DCCP
<input checked="" type="checkbox"/>	Ethernet
<input type="checkbox"/>	FC
<input type="checkbox"/>	FDDI
<input type="checkbox"/>	IEEE 802.11
<input type="checkbox"/>	IEEE 802.15.4
<input checked="" type="checkbox"/>	IPv4
<input checked="" type="checkbox"/>	IPv6
<input type="checkbox"/>	IPX
<input type="checkbox"/>	JXTA
<input type="checkbox"/>	MPTCP
<input type="checkbox"/>	NCP
Filter list for specific type	

Ethernet · 2						
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
IntelCor_d9:d3:f7	635 bytes	354.530 KiB	265 bytes	54.056 KiB	370 bytes	300.475 KiB
Sercomm_eb:fb:20	635 bytes	354.530 KiB	370 bytes	300.475 KiB	265 bytes	54.056 KiB

Close Help

wireshark_Wi-FivJF0Y1.pcapng | Packets: 635 · Displayed: 635 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Τα διαφορετικά endpoints είναι 2 και είναι αυτά που αναφέρονται στο παραπάνω screenshot. Με την επιλογή Name Resolution είναι ορατά και τα ονόματα των συσκευών: Intelcor , Sercom

3)

Wireshark · Endpoints · MEPOΣ B.pcapng

Endpoint Settings

☐ Name resolution

☐ Limit to display filter

Copy

Map

Protocol

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ MPTCP

☐ NCP

☐ openSAFETY

☐ RSVP

☐ SCTP

☐ SLL

☒ TCP

☐ Token Ring

Filter list for specific type

Ethernet · 2	IPv4 · 14	IPv6 · 13	TCP · 62	UDP · 35				
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City
20.73.130.64	41 bytes	24.945 KiB	21 bytes	18.036 KiB	20 bytes	6.909 KiB		
34.120.195.249	11 bytes	5.010 KiB	6 bytes	2.412 KiB	5 bytes	2.598 KiB		
34.149.211.227	16 bytes	9.795 KiB	6 bytes	1.088 KiB	10 bytes	8.707 KiB		
35.246.250.148	21 bytes	10.250 KiB	12 bytes	6.146 KiB	9 bytes	4.104 KiB		
40.74.219.49	2 bytes	121 bytes	1 bytes	66 bytes	1 bytes	55 bytes		
44.198.131.217	17 bytes	8.419 KiB	9 bytes	6.823 KiB	8 bytes	1.596 KiB		
52.0.253.11	2 bytes	344 bytes	1 bytes	290 bytes	1 bytes	54 bytes		
52.113.199.39	3 bytes	269 bytes	1 bytes	102 bytes	2 bytes	167 bytes		
65.108.131.22	250 bytes	195.108 KiB	162 bytes	179.236 KiB	88 bytes	15.872 KiB		
104.17.108.108	3 bytes	926 bytes	2 bytes	522 bytes	1 bytes	404 bytes		
162.159.135.234	4 bytes	303 bytes	2 bytes	141 bytes	2 bytes	162 bytes		
192.168.1.1	88 bytes	11.499 KiB	44 bytes	8.040 KiB	44 bytes	3.459 KiB		
192.168.1.5	497 bytes	283.428 KiB	208 bytes	46.178 KiB	289 bytes	237.250 KiB		
195.251.255.227	39 bytes	16.484 KiB	22 bytes	14.373 KiB	17 bytes	2.111 KiB		

Close Help

MEPOΣ B.pcapng

Packets: 635 · Displayed: 635 (100.0%) Profile: Default

Wireshark · Endpoints · MEPOS B.pcapng

Endpoint Settings

☐ Name resolution

☐ Limit to display filter

Copy

Map

Protocol

- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ JXTA
- ☐ MPTCP
- ☐ NCP
- ☐ openSAFETY
- ☐ RSVP
- ☐ SCTP
- ☐ SLL
- ☒ TCP
- ☐ Token Ring

Filter list for specific type

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
2603:1026:2400:1::2	4 bytes	366 bytes	2 bytes	148 bytes	2 bytes	218 bytes
2606:4700::6812:1613	21 bytes	7.847 KiB	11 bytes	5.997 KiB	10 bytes	1.850 KiB
2a01:111:f100:9001::1761:9472	3 bytes	327 bytes	1 bytes	121 bytes	2 bytes	206 bytes
2a01:4f9:6b:2ecf::1	8 bytes	688 bytes	0 bytes	0 bytes	8 bytes	688 bytes
2a02:26f0:6c00:1a4::3b8f	5 bytes	394 bytes	3 bytes	246 bytes	2 bytes	148 bytes
2a02:26f0:6c00:1b6::1011	2 bytes	161 bytes	1 bytes	86 bytes	1 bytes	75 bytes
2a02:582:a00::d4cd:7e21	4 bytes	320 bytes	2 bytes	172 bytes	2 bytes	148 bytes
2a02:582:a00::d4cd:7e53	7 bytes	1.633 KiB	3 bytes	1.097 KiB	4 bytes	549 bytes
2a02:586:e830:e06a:602e:e3bf:3b7a:c978	126 bytes	70.329 KiB	53 bytes	7.671 KiB	73 bytes	62.658 KiB
2a04:4e42::644	70 bytes	58.479 KiB	49 bytes	54.726 KiB	21 bytes	3.753 KiB
fe80::1	8 bytes	712 bytes	6 bytes	540 bytes	2 bytes	172 bytes
fe80::6add:766c:6780:844d	2 bytes	172 bytes	1 bytes	86 bytes	1 bytes	86 bytes
ff02::1	4 bytes	368 bytes	0 bytes	0 bytes	4 bytes	368 bytes

Close Help

MEPOS B.pcapng

Packets: 635 · Displayed: 635 (100.0%) Profile: Default

Τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP συνολικά είναι 27(14 είναι IPv4 και 13 είναι IPv6)

Σε επίπεδο IP, υπάρχουν 2 διαφορετικά endpoints, η IP διεύθυνση προέλευσης και η IP διεύθυνση προορισμού. Σε επίπεδο Ethernet, τα endpoints είναι η MAC διεύθυνση προέλευσης και η MAC διεύθυνση προορισμού. Τα endpoints σε επίπεδο Ethernet δεν αντιστοιχούν απαραίτητα στα endpoints σε επίπεδο IP, επειδή η επικοινωνία σε επίπεδο Ethernet είναι περιορισμένη στο δίκτυο ενός οργανισμού, ενώ η επικοινωνία σε επίπεδο IP μπορεί να πραγματοποιηθεί σε διαφορετικά δίκτυα.

4)

MEPOΣ B.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
22	9.266163	192.168.1.5	192.168.1.1	DNS	78	Standard query 0xde13
23	9.266412	192.168.1.5	192.168.1.1	DNS	78	Standard query 0xa6c6
33	9.290370	192.168.1.1	192.168.1.5	DNS	161	Standard query response
35	9.326578	192.168.1.1	192.168.1.5	DNS	131	Standard query response
38	9.328468	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xab8a
39	9.328717	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xe141
40	9.338390	192.168.1.1	192.168.1.5	DNS	310	Standard query response
41	9.340077	192.168.1.1	192.168.1.5	DNS	342	Standard query response
85	9.781138	192.168.1.5	192.168.1.1	DNS	91	Standard query 0xc877
86	9.781463	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
87	9.791584	192.168.1.1	192.168.1.5	DNS	178	Standard query response
88	9.791822	192.168.1.1	192.168.1.5	DNS	225	Standard query response
89	9.791909	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
90	9.801364	192.168.1.1	192.168.1.5	DNS	228	Standard query response
91	9.801553	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
92	9.812315	192.168.1.1	192.168.1.5	DNS	225	Standard query response
93	9.812453	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
94	9.823172	192.168.1.1	192.168.1.5	DNS	225	Standard query response
95	9.823543	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
97	9.834276	192.168.1.1	192.168.1.5	DNS	228	Standard query response
104	9.842453	192.168.1.5	192.168.1.1	DNS	77	Standard query 0x41f3
105	9.842701	192.168.1.5	192.168.1.1	DNS	77	Standard query 0x1329
106	9.852521	192.168.1.1	192.168.1.5	DNS	134	Standard query response
107	9.856546	192.168.1.1	192.168.1.5	DNS	146	Standard query response
139	9.945002	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x9446
140	9.945213	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x5761
150	9.956280	192.168.1.1	192.168.1.5	DNS	122	Standard query response
151	9.959010	192.168.1.1	192.168.1.5	DNS	184	Standard query response

User Datagram Protocol, Src Port: 57197, Dst Port: 53

Source Port: 57197

Destination Port: 53

Length: 44

Checksum: 0x8394 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

[Timestamps]

UDP payload (36 bytes)

0000 10 50 72 eb fb 20 40 ec 99 d9 d3 f7 08 00 45

0010 00 40 59 26 00 00 80 11 00 00 c0 a8 01 05 c0

0020 01 01 df 6d 00 35 00 2c 83 94 de 13 01 00 00

0030 00 00 00 00 00 00 03 77 77 77 0a 6f 70 65 6e

0040 66 66 69 63 65 03 6f 72 67 00 00 01 00 01

MEPOΣ B.pcapng

Packets: 635 · Displayed: 88 (13.9%)

Profile: Default

Θα πρέπει να φιλτράρουμε τα πακέτα που περιέχουν την θύρα προέλευσης 53 και την θύρα προορισμού 53 για την ερώτηση από τον υπολογιστή μας προς τον DNS server και την θύρα προέλευσης 53 και διαφορετική θύρα προορισμού για την απάντηση από τον DNS server στον υπολογιστή μας.

5)

MEPOΣ B.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
35	9.326578	192.168.1.1	192.168.1.5	DNS	131	Standard query response
38	9.328468	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xab8a
39	9.328717	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xe141
40	9.338390	192.168.1.1	192.168.1.5	DNS	310	Standard query response
41	9.340077	192.168.1.1	192.168.1.5	DNS	342	Standard query response
85	9.781138	192.168.1.5	192.168.1.1	DNS	91	Standard query 0xc877
86	9.781463	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
87	9.791584	192.168.1.1	192.168.1.5	DNS	178	Standard query response
88	9.791822	192.168.1.1	192.168.1.5	DNS	225	Standard query response
89	9.791909	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
90	9.801364	192.168.1.1	192.168.1.5	DNS	228	Standard query response
91	9.801553	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
92	9.812315	192.168.1.1	192.168.1.5	DNS	225	Standard query response
93	9.812453	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
94	9.823172	192.168.1.1	192.168.1.5	DNS	225	Standard query response
95	9.823543	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
97	9.834276	192.168.1.1	192.168.1.5	DNS	228	Standard query response
104	9.842453	192.168.1.5	192.168.1.1	DNS	77	Standard query 0x41f3
105	9.842701	192.168.1.5	192.168.1.1	DNS	77	Standard query 0x1329
106	9.852521	192.168.1.1	192.168.1.5	DNS	134	Standard query response
107	9.856546	192.168.1.1	192.168.1.5	DNS	146	Standard query response
139	9.945002	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x9446

Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.5
Destination Address: 192.168.1.1
> User Datagram Protocol, Src Port: 62231, Dst Port: 53
v Domain Name System (query)
Transaction ID: 0x73e4
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
[Response In: 94]

0000 10 50 72 eb fb 20 40 ec 99 d9 d3 f7 08 00 45
0010 00 4d 59 2e 00 00 80 11 00 00 c0 a8 01 05 c0
0020 01 01 f3 17 00 35 00 39 83 a1 73 e4 01 00 00
0030 00 00 00 00 00 00 0b 77 65 62 61 64 76 69 73
0040 72 63 04 72 65 73 74 03 67 74 69 06 6d 63 61
0050 65 65 03 63 6f 6d 00 00 1c 00 01

MEPOΣ B.pcapng | Packets: 635 · Displayed: 88 (13.9%) | Profile: Default

Εδώ έχουμε ερώτηση (query) , το οποίο το βλέπουμε στην καρτέλα DNS , αφού επιλέξαμε ένα πακέτο.

MEPOΣ B.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
35	9.326578	192.168.1.1	192.168.1.5	DNS	131	Standard query response
38	9.328468	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xab8a
39	9.328717	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xe141
40	9.338390	192.168.1.1	192.168.1.5	DNS	310	Standard query response
41	9.340077	192.168.1.1	192.168.1.5	DNS	342	Standard query response
85	9.781138	192.168.1.5	192.168.1.1	DNS	91	Standard query 0xc877
86	9.781463	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
87	9.791584	192.168.1.1	192.168.1.5	DNS	178	Standard query response
88	9.791822	192.168.1.1	192.168.1.5	DNS	225	Standard query response
89	9.791909	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
90	9.801364	192.168.1.1	192.168.1.5	DNS	228	Standard query response
91	9.801553	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
92	9.812315	192.168.1.1	192.168.1.5	DNS	225	Standard query response
93	9.812453	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
94	9.823172	192.168.1.1	192.168.1.5	DNS	225	Standard query response
95	9.823543	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
97	9.834276	192.168.1.1	192.168.1.5	DNS	228	Standard query response
104	9.842453	192.168.1.5	192.168.1.1	DNS	77	Standard query 0x41f3
105	9.842701	192.168.1.5	192.168.1.1	DNS	77	Standard query 0x1329
106	9.852521	192.168.1.1	192.168.1.5	DNS	134	Standard query response
107	9.856546	192.168.1.1	192.168.1.5	DNS	146	Standard query response
139	9.945002	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x9446

Source Address: 192.168.1.1
Destination Address: 192.168.1.5
> User Datagram Protocol, Src Port: 53, Dst Port: 53
▼ Domain Name System (response)
Transaction ID: 0xab8a
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
> Queries
> Answers
[\[Request In: 38\]](#)
[Time: 0.009922000 seconds]

0000 40 ec 99 d9 d3 f7 10 50 72 eb fb 20 08 00 00 00 00
0010 01 28 5a 96 40 00 40 11 5b d8 c0 a8 01 01 00 00
0020 01 05 00 35 ce 17 01 14 bd a6 ab 8a 81 80 00 00
0030 00 03 00 00 00 00 08 6e 61 76 2d 65 64 67 65
0040 73 6d 61 72 74 73 63 72 65 65 6e 09 6d 69 65
0050 6f 73 6f 66 74 03 63 6f 6d 00 00 01 00 01 00
0060 61 76 2d 65 64 67 65 0b 73 6d 61 72 74 73 65
0070 65 65 6e 09 6d 69 63 72 6f 73 6f 66 74 c0 73
0080 05 00 01 00 00 07 7c 00 28 13 74 6d 2d 70 70
0090 64 2d 77 64 2d 63 73 70 2d 65 64 67 65 0e 73
00a0 61 66 66 69 63 6d 61 6e 61 67 65 72 03 6e 65
00b0 00 c0 5f 00 05 00 01 00 00 00 c7 00 37 17 73
00c0 2d 70 72 6f 64 2d 73 73 2d 65 75 2d 77 65 73
00d0 2d 31 2d 66 65 0a 77 65 73 74 65 75 72 6f 73
00e0 08 63 6c 6f 75 64 61 70 70 05 61 7a 75 72 65
00f0 63 6f 6d 00 17 77 64 2d 70 72 6f 64 2d 73 73

MEPOΣ B.pcapng | Packets: 635 · Displayed: 88 (13.9%) | Profile: Default

Εδώ έχουμε απάντηση (response) , όπως φαίνεται στην καρτέλα DNS αφού επιλέξαμε ένα πακέτο.

Το πακέτο μιας απάντησης DNS συνδέεται με το πακέτο της αντίστοιχης ερώτησης με χρήση του πεδίου "Transaction ID" στα πακέτα DNS. Ένας μοναδικός αριθμός συναλλαγής (Transaction ID) αναπαριστά το μοναδικό αναγνωριστικό που επισυνάπτεται σε μια ερώτηση DNS και στην αντίστοιχη απάντηση. Έτσι, όταν η απάντηση DNS παραλαμβάνεται, το πρόγραμμα περιήγησης ή ο DNS client σας μπορεί να αναγνωρίσει ότι η απάντηση αντιστοιχεί στην αντίστοιχη ερώτηση που έστειλε, βασισμένο στον μοναδικό αριθμό συναλλαγής.

Κάτω παραθέτουμε παράδειγμα 2 πακέτων με ίδιο Transaction ID:

MEPOΣ B.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
105	9.842701	192.168.1.5	192.168.1.1	DNS	77	Standard query 0x1329
106	9.852521	192.168.1.1	192.168.1.5	DNS	134	Standard query respon
107	9.856546	192.168.1.1	192.168.1.5	DNS	146	Standard query respon
139	9.945002	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x9446
140	9.945213	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x5761
150	9.956280	192.168.1.1	192.168.1.5	DNS	122	Standard query respon
151	9.959010	192.168.1.1	192.168.1.5	DNS	184	Standard query respon
152	9.959693	192.168.1.5	192.168.1.1	DNS	74	Standard query 0xf1fe
154	9.959931	192.168.1.5	192.168.1.1	DNS	74	Standard query 0x456c
179	9.970951	192.168.1.1	192.168.1.5	DNS	205	Standard query respon
180	9.973477	192.168.1.1	192.168.1.5	DNS	226	Standard query respon
182	9.975887	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x29d1
183	9.976157	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa
187	9.985470	192.168.1.1	192.168.1.5	DNS	207	Standard query respon
188	9.985470	192.168.1.1	192.168.1.5	DNS	257	Standard query respon
189	9.985618	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa
192	9.998237	192.168.1.1	192.168.1.5	DNS	257	Standard query respon
193	9.998921	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa
197	10.008299	192.168.1.1	192.168.1.5	DNS	257	Standard query respon
198	10.008393	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa
207	10.021607	192.168.1.1	192.168.1.5	DNS	260	Standard query respon
208	10.021697	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa

Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.5
Destination Address: 192.168.1.1
> User Datagram Protocol, Src Port: 52754, Dst Port: 53
v Domain Name System (query)
Transaction ID: 0x69aa
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
[Response In: 188]

0000 10 50 72 eb fb 20 40 ec 99 d9 d3 f7 08 00 45
0010 00 4a 59 37 00 00 80 11 00 00 c0 a8 01 05 c0
0020 01 01 ce 12 00 35 00 36 83 9e 69 aa 01 00 00
0030 00 00 00 00 00 00 03 6d 69 70 03 61 70 69 10
0040 63 61 66 65 65 77 65 62 61 64 76 69 73 6f 72
0050 63 6f 6d 00 00 1c 00 01

Header checksum status (ip.checksum.status) | Packets: 635 · Displayed: 88 (13.9%) | Profile: Default

MEPOΣ B.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
105	9.842701	192.168.1.5	192.168.1.1	DNS	77	Standard query 0x1329
106	9.852521	192.168.1.1	192.168.1.5	DNS	134	Standard query response
107	9.856546	192.168.1.1	192.168.1.5	DNS	146	Standard query response
139	9.945002	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x9446
140	9.945213	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x5761
150	9.956280	192.168.1.1	192.168.1.5	DNS	122	Standard query response
151	9.959010	192.168.1.1	192.168.1.5	DNS	184	Standard query response
152	9.959693	192.168.1.5	192.168.1.1	DNS	74	Standard query 0xf1fe
154	9.959931	192.168.1.5	192.168.1.1	DNS	74	Standard query 0x456c
179	9.970951	192.168.1.1	192.168.1.5	DNS	205	Standard query response
180	9.973477	192.168.1.1	192.168.1.5	DNS	226	Standard query response
182	9.975887	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x29d1
183	9.976157	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa
187	9.985470	192.168.1.1	192.168.1.5	DNS	207	Standard query response
188	9.985470	192.168.1.1	192.168.1.5	DNS	257	Standard query response
189	9.985618	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa
192	9.998237	192.168.1.1	192.168.1.5	DNS	257	Standard query response
193	9.998921	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa
197	10.008299	192.168.1.1	192.168.1.5	DNS	257	Standard query response
198	10.008393	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa
207	10.021607	192.168.1.1	192.168.1.5	DNS	260	Standard query response
208	10.021697	192.168.1.5	192.168.1.1	DNS	88	Standard query 0x69aa

Header Checksum: 0x5bd5 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.1
 Destination Address: 192.168.1.5
 > User Datagram Protocol, Src Port: 53, Dst Port: 53
 > Domain Name System (response)
 Transaction ID: 0x69aa
 > Flags: 0x8185 Standard query response, Refused
 Questions: 1
 Answer RRs: 0
 Authority RRs: 1
 Additional RRs: 0
 > Queries
 > Authoritative nameservers
 [Request ID: 1931]

0010 00 f3 5a ce 40 00 40 11 5b d5 c0 a8 01 01 01
 0020 01 05 00 35 ce 12 00 df 44 f1 69 aa 81 85 00
 0030 00 00 00 01 00 00 03 6d 69 70 03 61 70 69
 0040 63 61 66 65 65 77 65 62 61 64 76 69 73 6f
 0050 63 6f 6d 00 00 1c 00 01 03 6d 69 70 03 61
 0060 10 4d 43 41 46 65 45 57 65 62 61 44 76 69
 0070 72 03 63 6f 6d 00 00 05 00 01 00 00 00 d8
 0080 14 57 41 43 6c 6f 75 64 4c 42 2d 31 38 30
 0090 37 37 39 34 30 09 75 73 2d 65 61 73 74 2d
 00a0 65 6c 62 09 61 6d 61 7a 6f 6e 61 77 73 c0
 00b0 6b 00 06 00 01 00 00 00 0a 00 46 07 6e 73
 00c0 31 31 39 09 61 77 73 64 6e 73 2d 31 31 03
 00d0 67 00 11 61 77 73 64 6e 73 2d 68 6f 73 74
 00e0 73 74 65 72 06 61 6d 61 7a 6f 6e c0 47 00
 00f0 01 00 00 1c 20 00 00 03 84 00 12 75 00 00
 0100 3c

Header checksum status (ip.checksum.status) | Packets: 635 · Displayed: 88 (13.9%) | Profile: Default

6)

Ναι, υπάρχει ένα πεδίο στα πακέτα DNS στην καρτέλα Flags το "Authoritative" που προσδιορίζει αν ο name server που απαντάει είναι authoritative για το συγκεκριμένο domain.

> Domain Name System (response)

Transaction ID: 0x69aa

> Flags: 0x8185 Standard query response, Refused

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)

7)

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a list of captured packets, with packet 23 selected. The packet details pane shows the structure of the selected packet, which is a DNS query. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
22	9.266163	192.168.1.5	192.168.1.1	DNS	78	Standard query 0xde13
23	9.266412	192.168.1.5	192.168.1.1	DNS	78	Standard query 0xa6c6
33	9.290370	192.168.1.1	192.168.1.5	DNS	161	Standard query respon
35	9.326578	192.168.1.1	192.168.1.5	DNS	131	Standard query respon
38	9.328468	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xab8a
39	9.328717	192.168.1.5	192.168.1.1	DNS	94	Standard query 0xe141
40	9.338390	192.168.1.1	192.168.1.5	DNS	310	Standard query respon
41	9.340077	192.168.1.1	192.168.1.5	DNS	342	Standard query respon
85	9.781138	192.168.1.5	192.168.1.1	DNS	91	Standard query 0xc877
86	9.781463	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
87	9.791584	192.168.1.1	192.168.1.5	DNS	178	Standard query respon
88	9.791822	192.168.1.1	192.168.1.5	DNS	225	Standard query respon
89	9.791909	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
90	9.801364	192.168.1.1	192.168.1.5	DNS	228	Standard query respon
91	9.801553	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
92	9.812315	192.168.1.1	192.168.1.5	DNS	225	Standard query respon
93	9.812453	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
94	9.823172	192.168.1.1	192.168.1.5	DNS	225	Standard query respon
95	9.823543	192.168.1.5	192.168.1.1	DNS	91	Standard query 0x73e4
97	9.834276	192.168.1.1	192.168.1.5	DNS	228	Standard query respon
104	9.842453	192.168.1.5	192.168.1.1	DNS	77	Standard querv 0x41f3

Answers

- Www.openoffice.org: type CNAME, class IN, cname tlpserver-he-fi.apache.org
 - Name: Www.openoffice.org
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 63 (1 minute, 3 seconds)
 - Data length: 25
 - CNAME: tlpserver-he-fi.apache.org
- tlpserver-he-fi.apache.org: type AAAA, class IN, addr 2a01:4f9:6b:2ecf::1
 - Name: tlpserver-he-fi.apache.org
 - Type: AAAA (IPv6 Address) (28)
 - Class: IN (0x0001)
 - Time to live: 1800 (30 minutes)
 - Data length: 16
 - AAAA Address: 2a01:4f9:6b:2ecf::1

[\[Request In: 23\]](#)

Number of answers in packet (dns.count.answers), 2 bytes | Packets: 635 · Displayed: 88 (13.9%) | Profile: Default

Στην καρτέλα Answers στο Type βλέπουμε ότι το όνομα είναι κανονικό .

Η IP διεύθυνση που του αντιστοιχεί είναι 65.108.131.22 και 2a01:4f9:6b:2ecf::1.

.....

8)

MEPOΣ B.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && ip.addr == 65.108.131.22

No.	Time	Source	Destination	Protocol	Length	Info
68	9.643088	192.168.1.5	65.108.131.22	TCP	66	51715 → 80 [SYN] Seq=
69	9.643630	192.168.1.5	65.108.131.22	TCP	66	51716 → 80 [SYN] Seq=
71	9.705343	65.108.131.22	192.168.1.5	TCP	66	80 → 51715 [SYN, ACK]
72	9.705561	192.168.1.5	65.108.131.22	TCP	54	51715 → 80 [ACK] Seq=
73	9.707018	192.168.1.5	65.108.131.22	HTTP	503	GET / HTTP/1.1
74	9.707673	65.108.131.22	192.168.1.5	TCP	66	80 → 51716 [SYN, ACK]
75	9.707889	192.168.1.5	65.108.131.22	TCP	54	51716 → 80 [ACK] Seq=
76	9.770250	65.108.131.22	192.168.1.5	TCP	54	80 → 51715 [ACK] Seq=
77	9.774055	65.108.131.22	192.168.1.5	TCP	1514	80 → 51715 [ACK] Seq=
78	9.774055	65.108.131.22	192.168.1.5	TCP	1514	80 → 51715 [PSH, ACK]
79	9.774055	65.108.131.22	192.168.1.5	TCP	1514	80 → 51715 [ACK] Seq=
80	9.774055	65.108.131.22	192.168.1.5	TCP	1514	80 → 51715 [PSH, ACK]
81	9.774055	65.108.131.22	192.168.1.5	TCP	1514	80 → 51715 [ACK] Seq=
82	9.774055	65.108.131.22	192.168.1.5	TCP	1514	80 → 51715 [PSH, ACK]
83	9.774055	65.108.131.22	192.168.1.5	HTTP	516	HTTP/1.1 200 OK (tex
84	9.774187	192.168.1.5	65.108.131.22	TCP	54	51715 → 80 [ACK] Seq=
96	9.828093	192.168.1.5	65.108.131.22	HTTP	415	GET /css/ooo.css HTTP
99	9.839398	192.168.1.5	65.108.131.22	TCP	66	51718 → 80 [SYN] Seq=
101	9.841455	192.168.1.5	65.108.131.22	HTTP	411	GET /download/globalv
112	9.890050	65.108.131.22	192.168.1.5	TCP	1514	80 → 51715 [ACK] Seq=
113	9.890050	65.108.131.22	192.168.1.5	HTTP	1196	HTTP/1.1 200 OK (tex
114	9.890144	192.168.1.5	65.108.131.22	TCP	54	51715 → 80 [ACK] Seq=
115	9.890750	192.168.1.5	65.108.131.22	HTTP	416	GET /css/home.css HTT
119	9.900461	65.108.131.22	192.168.1.5	TCP	66	80 → 51718 [SYN, ACK]
120	9.900715	192.168.1.5	65.108.131.22	TCP	54	51718 → 80 [ACK] Seq=

1000 = Header Length: 32 bytes (8)

Flags: 0x002 (SYN)

- 000. = Reserved: Not set
- ...0 = Accurate ECN: Not set
- 0... = Congestion Window Reduced: Not set
-0.. = ECN-Echo: Not set
-0. = Urgent: Not set
-0 = Acknowledgment: Not set
- 0... = Push: Not set
-0.. = Reset: Not set
- >1. = Syn: Set
-0 = Fin: Not set

0000 10 50 72 eb fb 2

0010 00 34 5e 6d 40 0

0020 83 16 ca 03 00 5

0030 fa f0 86 56 00 0

0040 04 02

Η διαδικασία χειραψίας τριών βημάτων (3-way Handshake) είναι η διαδικασία που χρησιμοποιείται από το TCP για να εγκαταστήσει μια σύνδεση μεταξύ δύο συστημάτων. Τα 3 βήματα της διαδικασίας είναι τα εξής:

- I. (SYN) Ο πελάτης(εμείς) θέλει να εγκαθιδρύσει σύνδεση με τον server, του στέλνει ένα segment με SYN. Το SYN δηλώνει με ποιόν αριθμό ξεκινάει τα segments του. Με την αποστολή αυτή δηλώνει ότι είναι πολύ πιθανό να ξεκινήσει επικοινωνία με τον server.

- II. II. (SYN, ACK) ο server απαντάει στο αίτημα του πελάτη με ένα σεν από SYN-ACK signal bits. Το ACK(acknowledgement) δηλώνει την απάντηση στο segment που ο χρήστης έστειλε και το SYN δηλώνει τον αριθμό με τον οποίο ο server θα ξεκινάει τα segments του.
- III. III. (ACK) Ο πελάτης τώρα αναγνωρίζει το response από τον server και πλέον εγκαθιδρύεται μια secure/reliable σύνδεση μεταξύ τους για μεταφορά data.

i. Παρατηρούμε ότι το sequence number (raw) που στέλνει ο πελάτης είναι Initialized, είναι το SYN που στέλνεται στον server. Επίσης αν πάμε στα flags θα δούμε ότι το SYN: set. Από αυτό γίνεται κατανοητό ότι είμαστε στο πρώτο Part του 3-way-hanshaking.

```

Transmission Control Protocol, Src Port: 51715, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 51715
  Destination Port: 80
  [Stream index: 13]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0      (relative sequence number)
  Sequence Number (raw): 1680103562
  [Next Sequence Number: 1      (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x002 (SYN)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...0 = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....S.]
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x8656 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale
    > TCP Option - Maximum segment size: 1460 bytes
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 8 (multiply by 256)
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - SACK permitted
    > [Timestamps]

```

ii. Παρατηρούμε ότι το sequence number που στέλνει ο server είναι Initialized, είναι το SYN που στέλνεται στον πελάτη για να ξέρει με ποιόν αριθμό θα ξεκινάνε τα segments του ο server. Και το acknowledgement number έχει value και δηλώνει response προς το αίτημα του πελάτη. Επίσης αν πάμε στα flags θα δούμε ότι το SYN: set και το ACK: set. Από αυτό γίνεται κατανοητό ότι είμαστε στο δεύτερο part του 3-way-hanshaking.

```
✓ Transmission Control Protocol, Src Port: 80, Dst Port: 51715, Seq: 0, Ack: 1,
  Source Port: 80
  Destination Port: 51715
  [Stream index: 13]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0      (relative sequence number)
  Sequence Number (raw): 4176268690
  [Next Sequence Number: 1      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 1680103563
  1000 .... = Header Length: 32 bytes (8)
  ✓ Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....A..S.]
```

ii. Παρατηρούμε ότι το sequence number είναι ίδιο με το αρχικό που έστειλε ο πελάτης(δλδ είναι αυτό με το οποίο αναγνωρίζεται ότι το segment είναι δικό του). Και το acknowledgement number έχει value και δηλώνει response του πελάτη στον server(δηλαδή είναι το ok για την εγκαθίδρυση της σύνδεσης). Επίσης αν πάμε στα flags θα δούμε ότι το ACK: set. Από αυτό γίνεται κατανοητό ότι είμαστε στο τρίτο και τελευταίο part του 3-way-hanshaking.

- ✓ Transmission Control Protocol, Src Port: 51715, Dst Port: 80, Seq: 1, Ack: 1,
 - Source Port: 51715
 - Destination Port: 80
 - [Stream index: 13]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 0]
 - Sequence Number: 1 (relative sequence number)
 - Sequence Number (raw): 1680103563
 - [Next Sequence Number: 1 (relative sequence number)]
 - Acknowledgment Number: 1 (relative ack number)
 - Acknowledgment number (raw): 4176268691
 - 0101 = Header Length: 20 bytes (5)
 - ✓ Flags: 0x010 (ACK)
 - 000. = Reserved: Not set
 - ...0 = Accurate ECN: Not set
 - 0... = Congestion Window Reduced: Not set
 -0.. = ECN-Echo: Not set
 -0. = Urgent: Not set
 -1 = Acknowledgment: Set
 - 0... = Push: Not set
 -0.. = Reset: Not set
 -0. = Syn: Not set
 -0 = Fin: Not set
 - [TCP Flags:A....]

9)

Οι θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το TCP πρωτόκολλο για την επικοινωνία με τον server που φιλοξενεί το www.openoffice.org είναι 51715 (ο υπολογιστής μας) και 80 (ο σερβερ της ιστοσελίδας)

10)

http.request.method == GET						
No.	Time	Source	Destination	Protocol	Length	Info
73	9.707018	192.168.1.5	65.108.131.22	HTTP	503	GET / HTTP/1.1
96	9.828093	192.168.1.5	65.108.131.22	HTTP	415	GET /css/ooo.css HTTP/1.1
101	9.841455	192.168.1.5	65.108.131.22	HTTP	411	GET /download/globalvars.js HTTP/1.1
115	9.890750	192.168.1.5	65.108.131.22	HTTP	416	GET /css/home.css HTTP/1.1
121	9.901700	192.168.1.5	65.108.131.22	HTTP	418	GET /css/styles.css HTTP/1.1
127	9.905583	192.168.1.5	65.108.131.22	HTTP	422	GET /css/exceptions.css HTTP/1.1
149	9.955172	192.168.1.5	65.108.131.22	HTTP	405	GET /msg_prop_l10n.js HTTP/1.1
178	9.968995	192.168.1.5	65.108.131.22	HTTP	410	GET /download/languages.js HTTP/1.1
186	9.982690	2a02:586:e830:e06a:...	2a02:582:a00::d4cd:...	HTTP	315	GET /MFMwUTBPME0wSzAJBgUrDgMCGGUABBRI2smg%2ByvTLU%2
206	10.018198	192.168.1.5	65.108.131.22	HTTP	409	GET /download/download.js HTTP/1.1
226	10.054277	192.168.1.5	65.108.131.22	HTTP	475	GET /images/A00_logos/100MillA00100px.png HTTP/1.1
245	10.087342	192.168.1.5	65.108.131.22	HTTP	461	GET /images/logo-rss-16.png HTTP/1.1
246	10.090243	192.168.1.5	65.108.131.22	HTTP	466	GET /images/logo-facebook-16.png HTTP/1.1
265	10.152725	192.168.1.5	65.108.131.22	HTTP	465	GET /images/logo-twitter-16.png HTTP/1.1
266	10.153106	192.168.1.5	65.108.131.22	HTTP	465	GET /images/logo-youtube-16.png HTTP/1.1
284	10.182102	192.168.1.5	65.108.131.22	HTTP	464	GET /images/asf_logo_small.png HTTP/1.1
293	10.207681	192.168.1.5	65.108.131.22	HTTP	473	GET /images/action-info.png HTTP/1.1
294	10.208543	192.168.1.5	65.108.131.22	HTTP	477	GET /images/action-download.png HTTP/1.1
295	10.208876	192.168.1.5	65.108.131.22	HTTP	473	GET /images/action-help.png HTTP/1.1
301	10.216611	192.168.1.5	65.108.131.22	HTTP	475	GET /images/action-extend.png HTTP/1.1
302	10.217282	192.168.1.5	65.108.131.22	HTTP	480	GET /images/action-participate.png HTTP/1.1
325	10.246739	192.168.1.5	65.108.131.22	HTTP	475	GET /images/action-social.png HTTP/1.1
354	10.276251	192.168.1.5	65.108.131.22	HTTP	478	GET /images/campaign-divider.png HTTP/1.1
405	10.678297	192.168.1.5	65.108.131.22	HTTP	450	GET /favicon.ico HTTP/1.1
577	14.582687	192.168.1.5	65.108.131.22	HTTP	503	GET / HTTP/1.1

Οι διευθύνσεις IP που στάλθηκαν είναι η IP διεύθυνση του web server που φιλοξενεί τον ιστότοπο που θέλουμε να μπούμε.(<http://www.openoffice.org>)