Δίκτυα Υπολογιστών

Εργασία 4η

Λουδάρος Ιωάννης (1067400)

Μπορείτε να δείτε την τελευταία έκδοση του Project εδώ ή σκανάροντας τον κωδικό QR που βρίσκεται στην επικεφαλίδα.

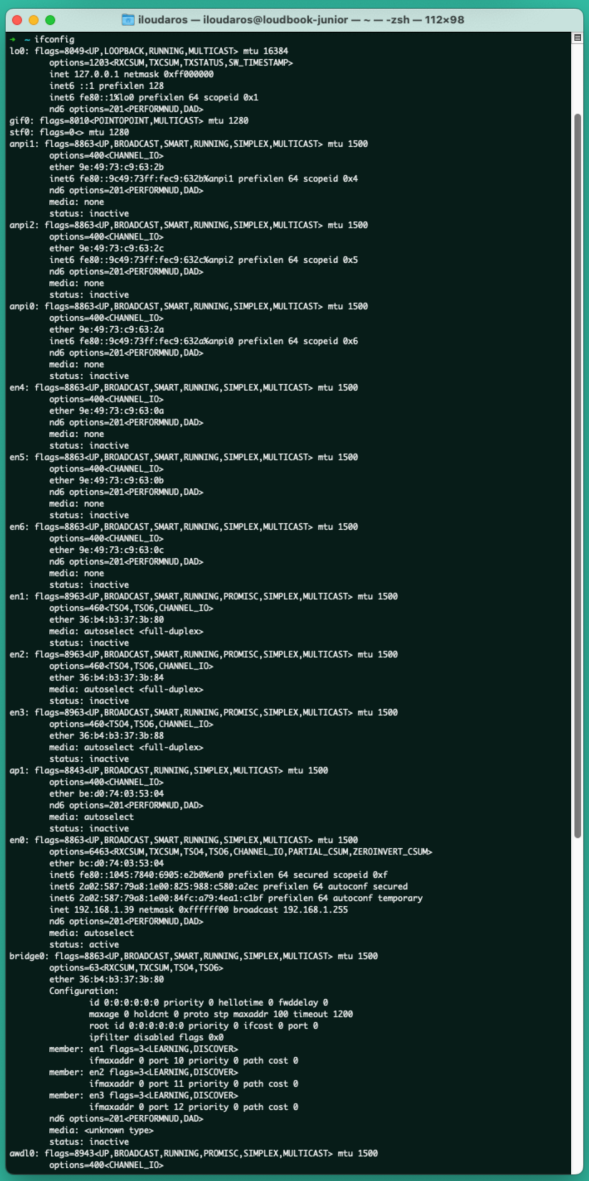
Περιγραφή Αναφοράς

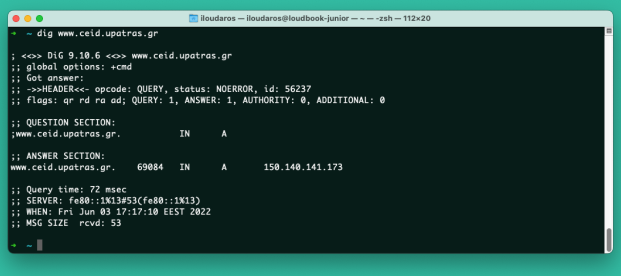
Παρακάτω παραθέτω τις απαντήσεις μου στην "4η Εργασία" του μαθήματος "Δίκτυα Υπολογιστών" καθώς και σχόλια τα οποία προέκυψαν κατά την εκπόνηση του.

Περιεχόμενα

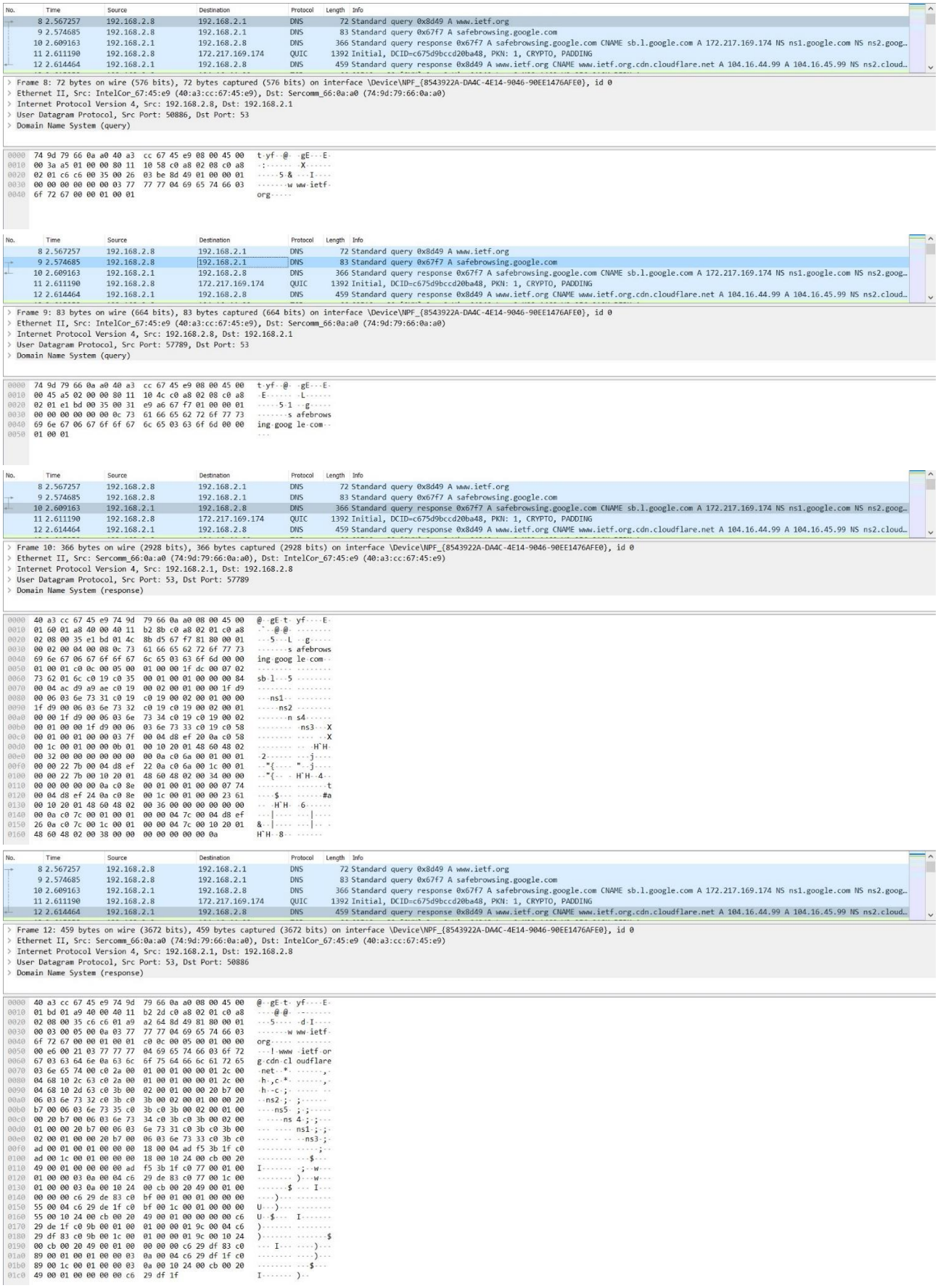
Απαντήσεις

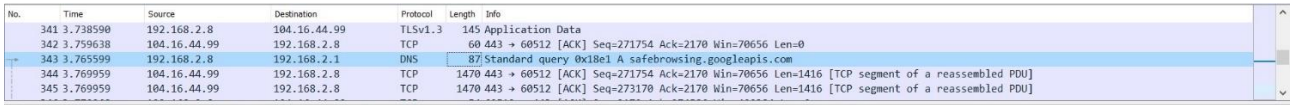
Ανάλυση DNS Πρωτοκόλλου





Οι εικόνες αριστερά, δείχνουν τα αποτελέσματα της εκτέλεσης των εντολών nslookup, ifconfig και dig

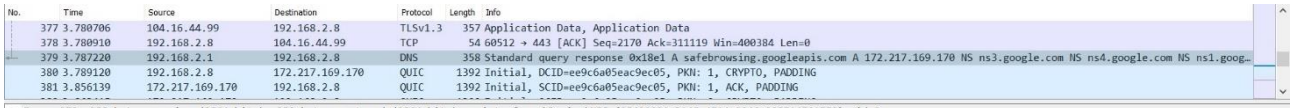

No. Time Source Destination Protocol Length Info
8 2.567257 192.168.2.8 192.168.2.1 DNS 72 Standard query 0x8d49 A www.ietf.org
9 2.574685 192.168.2.8 192.168.2.1 DNS 83 Standard query 0x67f7 A safebrowsing.google.com
10 2.609163 192.168.2.1 192.168.2.8 DNS 366 Standard query response 0x67f7 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.169.174 NS ns1.google.com NS ns2.goog…
11 2.611190 192.168.2.8 172.217.169.174 QUIC 1392 Initial, DCID=c675d9bccd20ba48, PKN: 1, CRYPTO, PADDING
12 2.614464 192.168.2.1 192.168.2.8 DNS 459 Standard query response 0x8d49 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 NS ns2.cloud…
Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
Ethernet II, Src: IntelCor_67:45:e9 (40:a3:cc:67:45:e9), Dst: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0)
Internet Protocol Version 4, Src: 192.168.2.8, Dst: 192.168.2.1
User Datagram Protocol, Src Port: 50886, Dst Port: 53
Domain Name System (query)
0000 74 9d 79 66 0a a0 40 a3 cc 67 45 e9 08 00 45 00 t·yf··@· ·gE···E·
0010 00 3a a5 01 00 00 80 11 10 58 c0 a8 02 08 c0 a8 ·:····· ·X·····
0020 02 01 c6 c6 00 35 00 26 03 be 8d 49 01 00 00 01 ·····5·& ···I····
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03 ·······w ww·ietf·
0040 6f 72 67 00 00 01 00 01 org·····
No. Time Source Destination Protocol Length Info
8 2.567257 192.168.2.8 192.168.2.1 DNS 72 Standard query 0x8d49 A www.ietf.org
9 2.574685 192.168.2.8 192.168.2.1 DNS 83 Standard query 0x67f7 A safebrowsing.google.com
10 2.609163 192.168.2.1 192.168.2.8 DNS 366 Standard query response 0x67f7 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.169.174 NS ns1.google.com NS ns2.goog…
11 2.611190 192.168.2.8 172.217.169.174 QUIC 1392 Initial, DCID=c675d9bccd20ba48, PKN: 1, CRYPTO, PADDING
12 2.614464 192.168.2.1 192.168.2.8 DNS 459 Standard query response 0x8d49 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 NS ns2.cloud…
Frame 9: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
Ethernet II, Src: IntelCor_67:45:e9 (40:a3:cc:67:45:e9), Dst: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0)
Internet Protocol Version 4, Src: 192.168.2.8, Dst: 192.168.2.1
User Datagram Protocol, Src Port: 57789, Dst Port: 53
Domain Name System (query)
0000 74 9d 79 66 0a a0 40 a3 cc 67 45 e9 08 00 45 00 t·yf··@· ·gE···E·
0010 00 45 a5 02 00 00 80 11 10 4c c0 a8 02 08 c0 a8 ·E····· ·L·····
0020 02 01 e1 bd 00 35 00 31 e9 a6 67 f7 01 00 00 01 ·····5·1 ··g·····
0030 00 00 00 00 00 00 0c 73 61 66 65 62 72 6f 77 73 ·······s afebrows
0040 69 6e 67 06 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 ing·goog le·com··
0050 01 00 01 ···
No. Time Source Destination Protocol Length Info
8 2.567257 192.168.2.8 192.168.2.1 DNS 72 Standard query 0x8d49 A www.ietf.org
9 2.574685 192.168.2.8 192.168.2.1 DNS 83 Standard query 0x67f7 A safebrowsing.google.com
10 2.609163 192.168.2.1 192.168.2.8 DNS 366 Standard query response 0x67f7 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.169.174 NS ns1.google.com NS ns2.goog…
11 2.611190 192.168.2.8 172.217.169.174 QUIC 1392 Initial, DCID=c675d9bccd20ba48, PKN: 1, CRYPTO, PADDING
12 2.614464 192.168.2.1 192.168.2.8 DNS 459 Standard query response 0x8d49 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 NS ns2.cloud…
Frame 10: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
Ethernet II, Src: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0), Dst: IntelCor_67:45:e9 (40:a3:cc:67:45:e9)
Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.8
User Datagram Protocol, Src Port: 53, Dst Port: 57789
Domain Name System (response)
0000 40 a3 cc 67 45 e9 74 9d 79 66 0a a0 08 00 45 00 @··gE·t· yf····E·
0010 01 60 01 a8 40 00 40 11 b2 8b c0 a8 02 01 c0 a8 ·`··@·@· ········
0020 02 08 00 35 e1 bd 01 4c 8b d5 67 f7 81 80 00 01 ···5···L ··g·····
0030 00 02 00 04 00 08 0c 73 61 66 65 62 72 6f 77 73 ·······s afebrows
0040 69 6e 67 06 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 ing·goog le·com··
0050 01 00 01 c0 0c 00 05 00 01 00 00 1f dc 00 07 02 ········ ········
0060 73 62 01 6c c0 19 c0 35 00 01 00 01 00 00 00 84 sb·l···5 ········
0070 00 04 ac d9 a9 ae c0 19 00 02 00 01 00 00 1f d9 ········ ········
0080 00 06 03 6e 73 31 c0 19 c0 19 00 02 00 01 00 00 ···ns1·· ········
0090 1f d9 00 06 03 6e 73 32 c0 19 c0 19 00 02 00 01 ·····ns2 ········
00a0 00 00 1f d9 00 06 03 6e 73 34 c0 19 c0 19 00 02 ·······n s4······
00b0 00 01 00 00 1f d9 00 06 03 6e 73 33 c0 19 c0 58 ········ ·ns3···X
00c0 00 01 00 01 00 00 03 7f 00 04 d8 ef 20 0a c0 58 ········ ···· ···X
00d0 00 1c 00 01 00 00 0b 01 00 10 20 01 48 60 48 02 ········ ·· H`H·
00e0 00 32 00 00 00 00 00 00 0a c0 6a 00 01 00 01 ·2·····j ····
00f0 00 00 22 7b 00 04 d8 ef 22 0a c0 6a 00 1c 00 01 ··"{···· "··j····
0100 00 00 22 7b 00 10 20 01 48 60 48 02 00 34 00 00 ··"{·· H`H··4··
0110 00 00 00 00 00 0a c0 8e 00 01 00 01 00 00 07 74 ········ ·······t
0120 00 04 d8 ef 24 0a c0 8e 00 1c 00 01 00 00 23 61 ····$··· ·····#a
0130 00 10 20 01 48 60 48 02 00 36 00 00 00 00 00 00 ·· H`H· ·6····
0140 00 0a c0 7c 00 01 00 01 00 00 04 7c 00 04 d8 ef ···|···· ···|····
0150 26 0a c0 7c 00 1c 00 01 00 00 04 7c 00 10 20 01 &··|···· ···|·· ·
0160 48 60 48 02 00 38 00 00 00 00 00 00 0a H`H··8·· ·····
No. Time Source Destination Protocol Length Info
8 2.567257 192.168.2.8 192.168.2.1 DNS 72 Standard query 0x8d49 A www.ietf.org
9 2.574685 192.168.2.8 192.168.2.1 DNS 83 Standard query 0x67f7 A safebrowsing.google.com
10 2.609163 192.168.2.1 192.168.2.8 DNS 366 Standard query response 0x67f7 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.169.174 NS ns1.google.com NS ns2.goog…
11 2.611190 192.168.2.8 172.217.169.174 QUIC 1392 Initial, DCID=c675d9bccd20ba48, PKN: 1, CRYPTO, PADDING
12 2.614464 192.168.2.1 192.168.2.8 DNS 459 Standard query response 0x8d49 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 NS ns2.cloud…
Frame 12: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
Ethernet II, Src: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0), Dst: IntelCor_67:45:e9 (40:a3:cc:67:45:e9)
Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.8
User Datagram Protocol, Src Port: 53, Dst Port: 50886
Domain Name System (response)
0000 40 a3 cc 67 45 e9 74 9d 79 66 0a a0 08 00 45 00 @··gE·t· yf····E·
0010 01 bd 01 a9 40 00 40 11 b2 2d c0 a8 02 01 c0 a8 ····@·@· ·-······
0020 02 08 00 35 c6 c6 01 a9 a2 64 8d 49 81 80 00 01 ···5···· ·d·I····
0030 00 03 00 05 00 0a 03 77 77 77 04 69 65 74 66 03 ·······w ww·ietf·
0040 6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00 org····· ········
0050 00 e6 00 21 03 77 77 77 04 69 65 74 66 03 6f 72 ···!·www ·ietf·or
0060 67 03 63 64 6e 0a 63 6c 6f 75 64 66 6c 61 72 65 g·cdn·cl oudflare
0070 03 6e 65 74 00 c0 2a 00 01 00 01 00 00 01 2c 00 ·net··*· ······,·
0080 04 68 10 2c 63 c0 2a 00 01 00 01 00 00 01 2c 00 ·h·,c·*· ······,·
0090 04 68 10 2d 63 c0 3b 00 02 00 01 00 00 20 b7 00 ·h·-c·;· ····· ··
00a0 06 03 6e 73 32 c0 3b c0 3b 00 02 00 01 00 00 20 ··ns2·;· ;·····
00b0 b7 00 06 03 6e 73 35 c0 3b c0 3b 00 02 00 01 00 ····ns5· ;·;·····
00c0 00 20 b7 00 06 03 6e 73 34 c0 3b c0 3b 00 02 00 · ····ns 4·;·;···
00d0 01 00 00 20 b7 00 06 03 6e 73 31 c0 3b c0 3b 00 ··· ···· ns1·;·;·
00e0 02 00 01 00 00 20 b7 00 06 03 6e 73 33 c0 3b c0 ····· ·· ··ns3·;·
00f0 ad 00 01 00 01 00 00 00 18 00 04 ad f5 3b 1f c0 ········ ·····;··
0100 ad 00 1c 00 01 00 00 00 18 00 10 24 00 cb 00 20 ········ ···$···
0110 49 00 01 00 00 00 00 ad f5 3b 1f c0 77 00 01 00 I····· ·;··w···
0120 01 00 00 03 0a 00 04 c6 29 de 83 c0 77 00 1c 00 ········)···w···
0130 01 00 00 03 0a 00 10 24 00 cb 00 20 49 00 01 00 ·····$· ··· I···
0140 00 00 00 c6 29 de 83 c0 bf 00 01 00 01 00 00 00 ····)··· ········
0150 55 00 04 c6 29 de 1f c0 bf 00 1c 00 01 00 00 00 U···)··· ········
0160 55 00 10 24 00 cb 00 20 49 00 01 00 00 00 00 c6 U··$··· I·······
0170 29 de 1f c0 9b 00 01 00 01 00 00 01 9c 00 04 c6)····· ········
0180 29 df 83 c0 9b 00 1c 00 01 00 00 01 9c 00 10 24)····· ·······$
0190 00 cb 00 20 49 00 01 00 00 00 00 c6 29 df 83 c0 ··· I··· ····)···
01a0 89 00 01 00 01 00 00 03 0a 00 04 c6 29 df 1f c0 ········ ····)···
01b0 89 00 1c 00 01 00 00 03 0a 00 10 24 00 cb 00 20 ········ ···$···
01c0 49 00 01 00 00 00 00 c6 29 df 1f I·····)··



No.	Time	Source	Destination	Protocol	Length	Info
341	3.738590	192.168.2.8	104.16.44.99	TLSv1.3	145	Application Data
342	3.759638	104.16.44.99	192.168.2.8	TCP	60	443 → 60512 [ACK] Seq=271754 Ack=2170 Win=70656 Len=0
343	3.765599	192.168.2.8	192.168.2.1	DNS	87	Standard query 0x18e1 A safebrowsing.googleapis.com
344	3.769959	104.16.44.99	192.168.2.8	TCP	1470	443 → 60512 [ACK] Seq=271754 Ack=2170 Win=70656 Len=1416 [TCP segment of a reassembled PDU]
345	3.769959	104.16.44.99	192.168.2.8	TCP	1470	443 → 60512 [ACK] Seq=273170 Ack=2170 Win=70656 Len=1416 [TCP segment of a reassembled PDU]

```
> Frame 343: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: IntelCor_67:45:e9 (40:a3:cc:67:45:e9), Dst: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0)
> Internet Protocol Version 4, Src: 192.168.2.8, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 61962, Dst Port: 53
> Domain Name System (query)
```

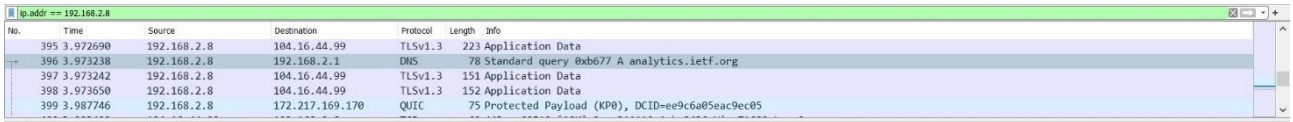
```
0000  74 9d 79 66 0a a0 40 a3  cc 67 45 e9 08 00 45 00   t·yf··@· ·gE···E·
0010  00 49 a5 03 00 00 80 11  10 47 c0 a8 02 08 c0 a8   ·I····· ·G······
0020  02 01 f2 0a 00 35 00 35  5d 80 18 e1 01 00 00 01   ·····5·5 ]·······
0030  00 00 00 00 00 00 0c 73  61 66 65 62 72 6f 77 73   ·······s afebrows
0040  69 6e 67 0a 67 6f 6f 67  6c 65 61 70 69 73 03 63   ing·goog leapis·c
0050  6f 6d 00 00 01 00 01                              om·····
```



No.	Time	Source	Destination	Protocol	Length	Info
377	3.780706	104.16.44.99	192.168.2.8	TLSv1.3	357	Application Data, Application Data
378	3.780910	192.168.2.8	104.16.44.99	TCP	54	60512 → 443 [ACK] Seq=2170 Ack=311119 Win=400384 Len=0
379	3.787220	192.168.2.1	192.168.2.8	DNS	358	Standard query response 0x18e1 A safebrowsing.googleapis.com A 172.217.169.170 NS ns3.google.com NS ns4.google.com NS ns1.goog…
380	3.789120	192.168.2.8	172.217.169.170	QUIC	1392	Initial, DCID=ee9c6a05eac9ec05, PKN: 1, CRYPTO, PADDING
381	3.856139	172.217.169.170	192.168.2.8	QUIC	1392	Initial, SCID=ee9c6a05eac9ec05, PKN: 1, ACK, PADDING

```
> Frame 379: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0), Dst: IntelCor_67:45:e9 (40:a3:cc:67:45:e9)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.8
> User Datagram Protocol, Src Port: 53, Dst Port: 61962
> Domain Name System (response)
```

```
0000  40 a3 cc 67 45 e9 74 9d  79 66 0a a0 08 00 45 00   @··gE·t· yf····E·
0010  01 58 02 12 40 00 40 11  b2 29 c0 a8 02 01 c0 a8   ·X··@·@· ·)······
0020  02 08 00 35 f2 0a 01 44  3d 31 18 e1 81 80 00 01   ···5···D =1······
0030  00 01 00 04 00 08 0c 73  61 66 65 62 72 6f 77 73   ·······s afebrows
0040  69 6e 67 0a 67 6f 6f 67  6c 65 61 70 69 73 03 63   ing·goog leapis·c
0050  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om······ ········
0060  2d 00 04 ac d9 a9 aa c0  19 00 02 00 01 00 00 00   -······· ········
0070  0d 00 0d 03 6e 73 33 06  67 6f 6f 67 6c 65 c0 24   ····ns3· google·$
0080  c0 19 00 02 00 01 00 00  00 0d 00 06 03 6e 73 34   ········ ·····ns4
0090  c0 4d c0 19 00 02 00 01  00 00 00 0d 00 06 03 6e   ·M······ ·······n
00a0  73 31 c0 4d c0 19 00 02  00 01 00 00 00 0d 00 06   s1·M···· ········
00b0  03 6e 73 32 c0 4d c0 74  00 01 00 01 00 00 03 d3   ·ns2·M·t ········
00c0  00 04 d8 ef 20 0a c0 74  00 1c 00 01 00 00 08 8f   ···· ··t ········
00d0  00 10 20 01 48 60 48 02  00 32 00 00 00 00 00 00   ·· ·H`H· ·2······
00e0  00 0a c0 86 00 01 00 01  00 00 06 a7 00 04 d8 ef   ········ ········
00f0  22 0a c0 86 00 1c 00 01  00 00 25 24 00 10 20 01   "····· ··%$·· ·
0100  48 60 48 02 00 34 00 00  00 00 00 00 0a c0 49      H`H··4·· ·····I
0110  00 01 00 01 00 00 10 77  00 04 d8 ef 24 0a c0 49   ·······w ····$··I
0120  00 1c 00 01 00 00 10 77  00 10 20 01 48 60 48 02   ·······w ·· ·H`H·
0130  00 36 00 00 00 00 00 00  00 0a c0 62 00 01 00 01   ·6····· ···b····
0140  00 00 04 75 00 04 d8 ef  26 0a c0 62 00 1c 00 01   ···u···· &··b····
0150  00 00 04 75 00 10 20 01  48 60 48 02 00 38 00 00   ···u···· H`H··8··
0160  00 00 00 00 00 0a                                 ·····
```

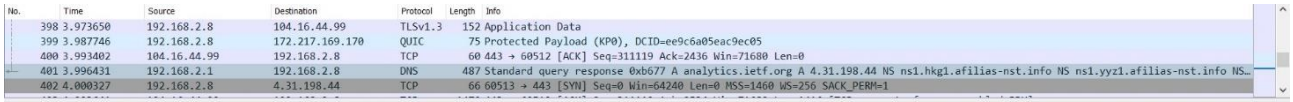


ip.addr == 192.168.2.8

No.	Time	Source	Destination	Protocol	Length	Info
395	3.972690	192.168.2.8	104.16.44.99	TLSv1.3	223	Application Data
396	3.973238	192.168.2.8	192.168.2.1	DNS	78	Standard query 0xb677 A analytics.ietf.org
397	3.973242	192.168.2.8	104.16.44.99	TLSv1.3	151	Application Data
398	3.973650	192.168.2.8	104.16.44.99	TLSv1.3	152	Application Data
399	3.987746	192.168.2.8	172.217.169.170	QUIC	75	Protected Payload (KP0), DCID=ee9c6a05eac9ec05

```
> Frame 396: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: IntelCor_67:45:e9 (40:a3:cc:67:45:e9), Dst: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0)
> Internet Protocol Version 4, Src: 192.168.2.8, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 49653, Dst Port: 53
> Domain Name System (query)
```

```
0000  74 9d 79 66 0a a0 40 a3  cc 67 45 e9 08 00 45 00   t·yf··@· ·gE···E·
0010  00 40 a5 04 00 00 80 11  10 4f c0 a8 02 08 c0 a8   ·@····· ·O······
0020  02 01 c1 f5 00 35 00 2c  9e 2a b6 77 01 00 00 01   ·····5·, ·*·w····
0030  00 00 00 00 00 00 09 61  6e 61 6c 79 74 69 63 73   ·······a nalytics
0040  04 69 65 74 66 03 6f 72  67 00 00 01 00 01         ·ietf·or g·····
```



No.	Time	Source	Destination	Protocol	Length	Info
398	3.973650	192.168.2.8	104.16.44.99	TLSv1.3	152	Application Data
399	3.987746	192.168.2.8	172.217.169.170	QUIC	75	Protected Payload (KP0), DCID=ee9c6a05eac9ec05
400	3.993402	104.16.44.99	192.168.2.8	TCP	60	443 → 60512 [ACK] Seq=311119 Ack=2436 Win=71680 Len=0
401	3.996431	192.168.2.1	192.168.2.8	DNS	487	Standard query response 0xb677 A analytics.ietf.org A 4.31.198.44 NS ns1.hkg1.afilias-nst.info NS ns1.yyz1.afilias-nst.info NS…
402	4.000327	192.168.2.8	4.31.198.44	TCP	66	60513 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

```
> Frame 401: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0), Dst: IntelCor_67:45:e9 (40:a3:cc:67:45:e9)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.8
> User Datagram Protocol, Src Port: 53, Dst Port: 49653
> Domain Name System (response)
```

```
0000  40 a3 cc 67 45 e9 74 9d  79 66 0a a0 08 00 45 00   @··gE·t· yf····E·
0010  01 d9 02 1d 40 00 40 11  b1 9d c0 a8 02 01 c0 a8   ····@·@· ········
0020  02 08 00 35 c1 f5 01 c5  97 d0 b6 77 81 80 00 01   ···5···· ···w····
0030  00 01 00 06 00 0b 09 61  6e 61 6c 79 74 69 63 73   ·······a nalytics
0040  04 69 65 74 66 03 6f 72  67 00 00 01 00 01 c0 0c   ·ietf·or g·······
0050  00 01 00 01 00 00 00 e6  00 04 04 1f c6 2c c0 16   ········ ·····,··
0060  00 02 00 01 00 00 17 ec  00 1b 03 6e 73 31 04 68   ········ ···ns1·h
0070  6b 67 31 0b 61 66 69 6c  69 61 73 2d 6e 73 74 04   kg1·afil ias-nst·
0080  69 6e 66 6f 00 c0 16 00  02 00 01 00 00 17 ec 00   info···· ········
0090  0b 03 6e 73 31 04 79 79  7a 31 c0 49 c0 16 00 02   ··ns1·yy z1·I····
00a0  00 01 00 00 17 ec 00 0e  03 6e 73 30 04 61 6d 73   ········ ·ns0·ams
00b0  6c 03 63 6f 6d 00 c0 16  00 02 00 01 00 00 17 ec   l·com··· ········
00c0  00 0b 03 6e 73 31 04 61  6d 73 31 c0 49 c0 16 00   ···ns1·a ms1·I···
00d0  02 00 01 00 00 17 ec 00  0b 03 6e 73 31 04 73 65   ········ ··ns1·se
00e0  61 31 c0 49 c0 16 00 02  00 01 00 00 17 ec 00 0b   a1·I···· ········
00f0  03 6e 73 31 04 6d 69 61  31 c0 49 c0 7e 00 01 00   ·ns1·mia 1·I·~···
0100  01 00 00 00 e6 00 04 04  1f c6 28 c0 7e 00 1c 00   ········ ··(·~···
0110  01 00 00 00 e8 00 10 20  01 19 00 30 01 00 11 00   ········ ···0····
0120  00 00 00 00 00 00 28 c0  98 00 01 00 01 00 00 06   ······(· ········
0130  e3 00 04 41 16 06 4f c0  40 00 01 00 01 00 00 06   ···A··O· @·······
0140  e3 00 04 41 16 06 01 c0  40 00 1c 00 01 00 00 12   ···A···· @·······
0150  1b 00 10 2a 01 88 40 00  06 00 00 00 00 00 00 00   ···*··@· ········
0160  00 00 01 c0 c6 00 01 00  01 00 00 07 ed 00 04 41   ········ ·······A
0170  16 07 01 c0 c6 00 1c 00  01 00 00 07 ed 00 10 2a   ········ ·······*
0180  01 88 40 00 07 00 00 00  00 00 00 00 00 01 c0      ··@····· ·····
0190  af 00 01 00 01 00 00 06  e3 00 04 41 16 08 01 c0   ········ ····A···
01a0  af 00 1c 00 01 00 00 12  1b 00 10 2a 01 88 40 00   ········ ···*··@·
01b0  08 00 00 00 00 00 00 00  00 00 01 c0 67 00 01 00   ········ ····g···
01c0  01 00 00 06 e3 00 04 41  16 09 01 c0 67 00 1c 00   ·******A ····g···
```

Πακέτα DNS

DNS Packet 1

Protocols: Ethernet, IPv4, UDP, DNS Source Port: 50886
Destination Port: 53
Transaction ID: 0x8d49

0... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively

Standard query 0x8d49 A www.ietf.orf (No answers) **DNS Packet 2**

Protocols: Ethernet, IPv4, UDP, DNS Source Port: 57789
Destination Port: 53
Transaction ID: 0x67f7

0... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively

Standard query 0x67f7 A safebrowsing.google.com (No answers)

DNS Packet 3

Protocols: Ethernet, IPv4, UDP, DNS Source Port: 53
Destination Port: 57789
Transaction ID: 0x67f7

1... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively

Standard query response 0x67f7 A safebrowsing.google.com

2 Answers: safebrowsing.google.com – Type: CNAME, Class: IN, cname: sb.l.google.com

sb.l.google.com – Type: A, Class: IN, addr: 172.217.169.174

Response to DNS Packet 2

DNS Packet 4

Protocols: Ethernet, IPv4, UDP, DNS Source Port: 53

Destination Port: 50886
Transaction ID: 0x8d49
1... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively

Standard query response 0x8d49
3 Answers: www.ietf.org – Type: CNAME, Class: IN, cname:

www.ietf.org.cdn.cloudflare.net
www.ietf.org.dcn.cloudflare.net – Type: A, Class: IN, addr: 104.16.44.99
www.ietf.org.cdn.cloudflare.net – Type: A, Class: IN, addr: 104.16.45.99 Response to DNS Packet 1

DNS Packet 5

Protocols: Ethernet, IPv4, UDP, DNS Source Port: 61962
Destination Port: 53
Transaction ID: 0x18e1

1... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively

Standard query 0x18e1 A safebrowsing.googleapis.com (No answers)

DNS Packet 6

Protocols: Ethernet, IPv4, UDP, DNS Source Port: 53
Destination Port: 61962
Transaction ID: 0x18e1

1... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively

Standard query response 0x18e1 A safebrowsing.googleapis.com

1 Answer: safebrowsing.googleapis.com – Type: A, Class: IN, addr: 172.217.169.170

Response to DNS Packet 5

DNS Packet 7

Protocols: Ethernet, IPv4, UDP, DNS Source Port: 49653
Destination Port: 53
Transaction ID: 0xb677

0... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively

Standard query 0xb677 A analytics.ietf.org (No answers)

DNS Packet 8

Protocols: Ethernet, IPv4, UDP, DNS Source Port: 53
Destination Port: 49653
Transaction ID: 0xb677

1... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively

Standard query response 0xb677 A analytics.ietf.org
1 Answer: analytics.ietf.org – Type: A, Class: IN, addr: 4.31.198.44 Response to DNS Packet 7

Παρατηρήσεις

- Παρατηρούμε ότι σε κάθε περίπτωση, οι απαντήσεις περιέχουν τα εξής πεδία: Domain Name, Name Length, Label Count, DNS Message Type, DNS Class

- Το Destination Address είναι κοινό σε όλα τα queries (192.168.2.1). Το οποίο είναι λογικό αφού στα System Preferences του δικτύου φαίνεται να είναι αυτή η διεύθυνση σεταρισμένη ως DNS.

- Εξετάζονται το επόμενο πακέτο TCP SYN μετά από κάθε response packet, παρατηρούμε πως το source address του TCP SYN πακέτου έχει την ίδια destination address με το response DNS packet.

nslookup www.ceid.upatras.gr και καταγραφή πακέτων

Source Port: 53 Destination Port: 50314

Το μήνυμα ερώτησης έχει Destination Address 192.168.2.1, η οποία όπως θα περιμέναμε είναι η IP address του προεπιλεγμένου DNS Server.

Ανάλυση:

0... ....= Response: Message is a query
.000 0... ....= Opcode: Standard query (0)
....1 ....= Recursion desired: Do query recursively Type: AAAA (IPv6 Address) (28)
No answers

Ανάλυση Απάντησης

1 Answer: www.ceid.upatras.gr – Type: CNAME, Class: IN, cname: web.ceid.upatras.gr

Name: www.ceid.upatras.gr

Type: CNAME (Canonical NAME for an alias) (5) Class: IN (0x0001)
Time To Live: 4186 (1 hour, 9 minutes, 46 seconds) Data Length: 6

CNAME: web.ceid.upatras.gr

Γενικά ερωτήματα για τον τρόπο λειτουργίας του DNS

DNS Header Fields

- Identification
- Flags
- Number of questions
- Number of answers
- Number of authority resource records (RRs)
- Number of additional RRs

Identification: Δείχνει ένα ολοκληρωμένο transaction (request και αντίστοιχο response)
Flags: QR (query/reply), OPCODE (standard query, inverse query, server status request), AA (authoritative answer), TC (truncation), RD (recursion desired), RA (recursion available), Z (zero), RCODE (response code).

Number of questions: Αριθμός ερωτήσεων σε ένα πακέτο.
Number of answers: Αριθμός απαντήσεων σε ένα πακέτο.
Number of authority resource records (RRs): Data records (A, CNAME, SOA, PTR, NS). Number of additional RRs: Data records τα οποία ίσως φανούν χρήσιμα στον client.

Packet 1

DNS Standard query 0x0003 A google.com
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
....1 .... = Recursion desired: Do query recursively google.com – Type: A, Class: IN

Name: google.com
Name Length: 10
Label Count: 2
Type: A (Host Address) (1) Class: IN (0x0001)

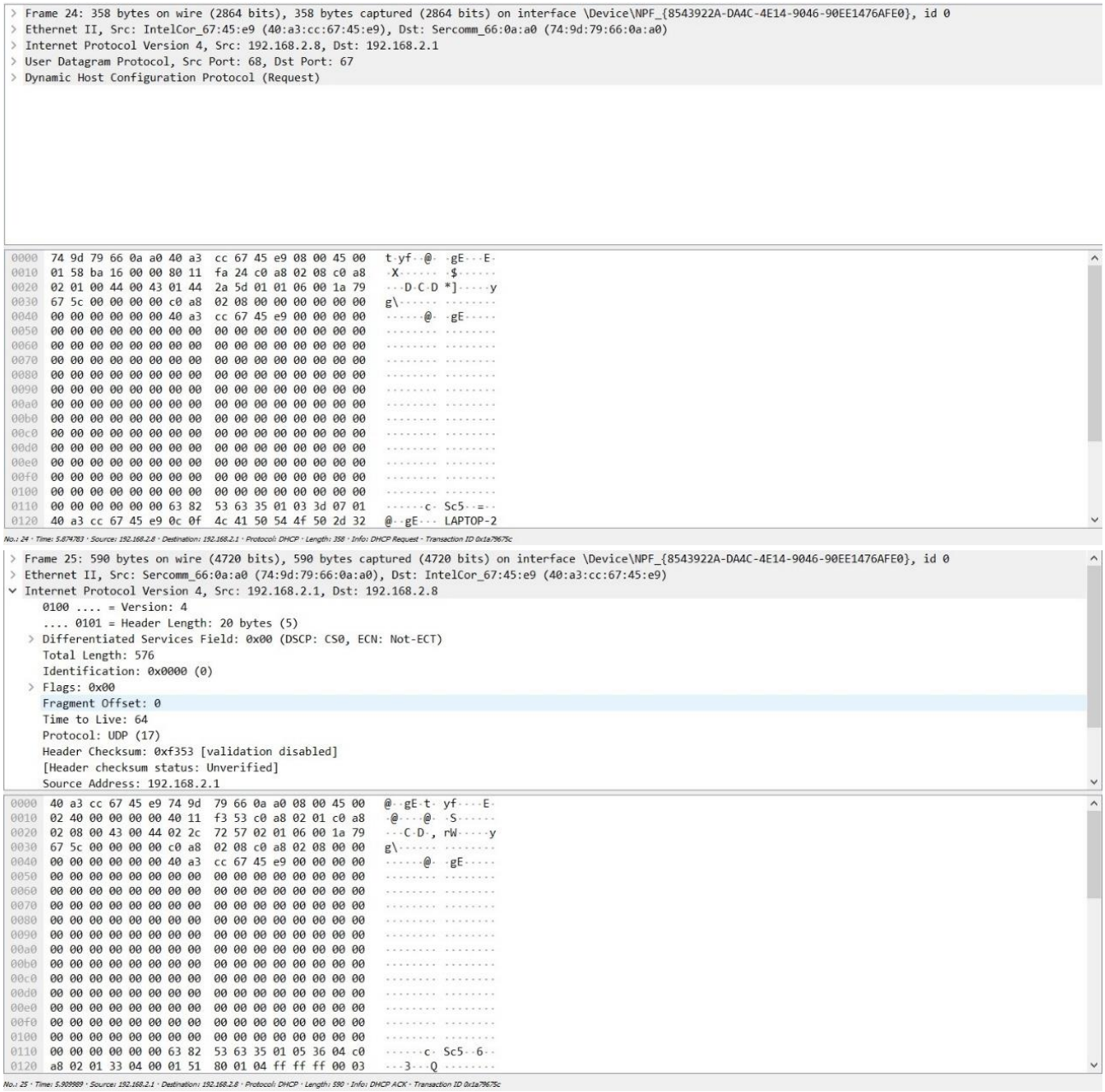
Packet 2

DNS Standard query response 0x0003 A google.com A 1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)

.... .0.. .... = Authoritative: Server is not an authority for domain 11 Answers

Ανάλυση DHCP πρωτοκόλλου

Μετά την καταγραφή πακέτων, παρατηρήθηκαν τα παρακάτω DHCP Packets.



```
> Frame 59: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: IntelCor_67:45:e9 (40:a3:cc:67:45:e9), Dst: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0)
v Internet Protocol Version 4, Src: 192.168.2.8, Dst: 192.168.2.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 344
    Identification: 0xba17 (47639)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xfa23 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.2.8
```

```
0000  74 9d 79 66 0a a0 40 a3  cc 67 45 e9 08 00 45 00   t·yf··@· ·gE···E·
0010  01 58 ba 17 00 00 80 11  fa 23 c0 a8 02 08 c0 a8   ·X····· ·#······
0020  02 01 00 44 00 43 01 44  c7 4d 01 01 06 00 7d f7   ···D·C·D ·M····}·
0030  66 ed 00 00 00 00 c0 a8  02 08 00 00 00 00 00 00   f····... ········
0040  00 00 00 00 00 00 40 a3  cc 67 45 e9 00 00 00 00   ······@· ·gE·····
0050  00 00 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 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  40 a3 cc 67 45 e9 0c 0f  4c 41 50 54 4f 50 2d 32   @··gE··· LAPTOP-2
```

```
No.: 59 · Time: 11.719628 · Source: 192.168.2.8 · Destination: 192.168.2.1 · Protocol: DHCP · Length: 358 · Info: DHCP Request · Transaction ID 0x7df766ed
```

```
> Frame 60: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0), Dst: IntelCor_67:45:e9 (40:a3:cc:67:45:e9)
v Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 576
    Identification: 0x0000 (0)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xf353 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.2.1
```

```
0000  40 a3 cc 67 45 e9 74 9d  79 66 0a a0 08 00 45 00   @··gE·t· yf····E·
0010  02 40 00 00 00 00 40 11  f3 53 c0 a8 02 01 c0 a8   ·@····@· ·S······
0020  02 08 00 43 00 44 02 2c  0f 48 02 01 06 00 7d f7   ···C·D·, ·H····}·
0030  66 ed 00 00 00 00 c0 a8  02 08 c0 a8 02 08 00 00   f····... ········
0040  00 00 00 00 00 00 40 a3  cc 67 45 e9 00 00 00 00   ······@· ·gE·····
0050  00 00 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 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 36 04 c0   ····· c· Sc5··6··
```

```
> Frame 100: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: IntelCor_67:45:e9 (40:a3:cc:67:45:e9), Dst: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0)
v Internet Protocol Version 4, Src: 192.168.2.8, Dst: 192.168.2.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0xba18 (47640)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xfa32 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.2.8
```

```
0000  74 9d 79 66 0a a0 40 a3  cc 67 45 e9 08 00 45 00   t·yf··@· ·gE···E·
0010  01 48 ba 18 00 00 80 11  fa 32 c0 a8 02 08 c0 a8   ·H····· ·2······
0020  02 01 00 44 00 43 01 34  d9 b0 01 01 06 00 aa f5   ···D·C·4 ········
0030  dc 45 00 00 00 00 c0 a8  02 08 00 00 00 00 00 00   ·E····· ········
0040  00 00 00 00 00 00 40 a3  cc 67 45 e9 00 00 00 00   ······@· ·gE·····
0050  00 00 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 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 07 36 04 c0   ····· c· Sc5··6··
0120  a8 02 01 3d 07 01 40 a3  cc 67 45 e9 ff 00 00 00   ···=··@· ·gE·····
```

```
No.: 100 · Time: 18.677000 · Source: 192.168.2.8 · Destination: 192.168.2.1 · Protocol: DHCP · Length: 342 · Info: DHCP Release · Transaction ID 0xaaf5dc45
```

```
> Frame 129: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: IntelCor_67:45:e9 (40:a3:cc:67:45:e9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

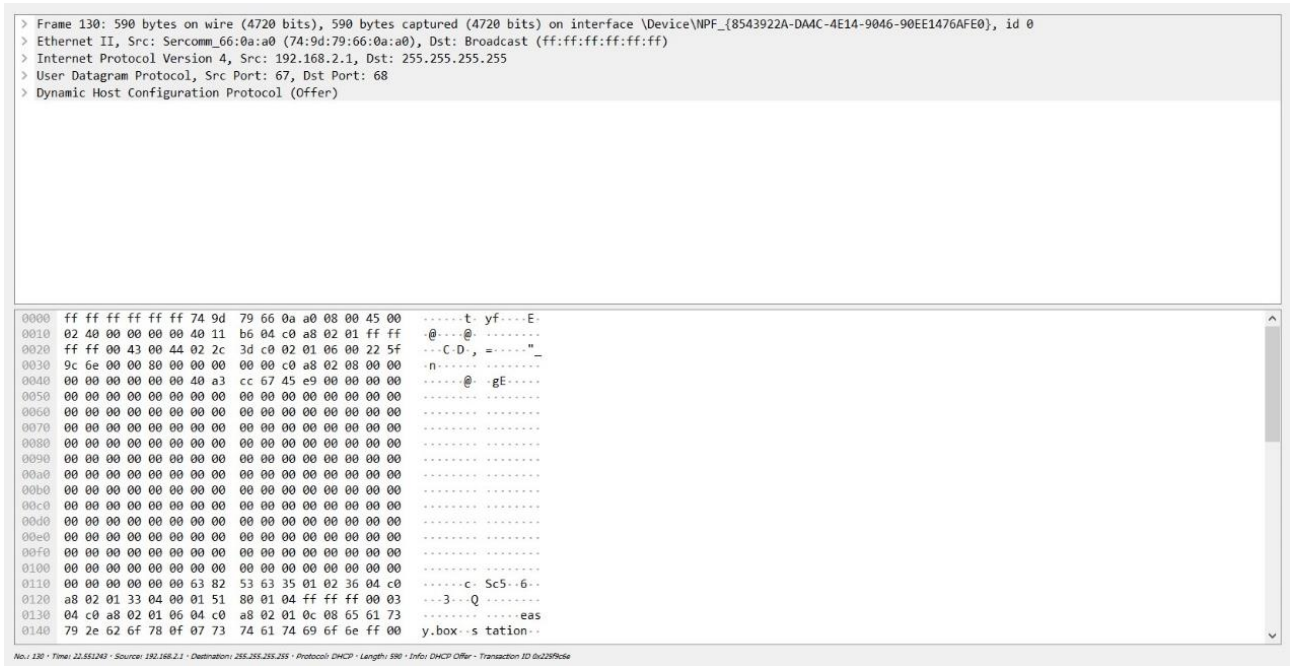
```
0000  ff ff ff ff ff ff 40 a3  cc 67 45 e9 08 00 45 00   ......@· ·gE···E·
0010  01 4a d4 72 00 00 80 11  65 31 00 00 00 00 ff ff   ·J·r···· e1······
0020  ff ff 00 44 00 43 01 36  e4 1e 01 01 06 00 22 5f   ···D·C·6 ·····"_
0030  9c 6e 00 00 80 00 00 00  00 00 00 00 00 00 00 00   ·n····· ········
0040  00 00 00 00 00 00 40 a3  cc 67 45 e9 00 00 00 00   ......@· ·gE·····
0050  00 00 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 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d 07 01   ......c· Sc5··=··
0120  40 a3 cc 67 45 e9 32 04  c0 a8 02 08 0c 0f 4c 41   @··gE·2· ......LA
0130  50 54 4f 50 2d 32 36 4c  46 47 49 4b 30 3c 08 4d   PTOP-26L FGIK0<·M
0140  53 46 54 20 35 2e 30 37  0e 01 03 06 0f 1f 21 2b   SFT 5.07 ......!+
```

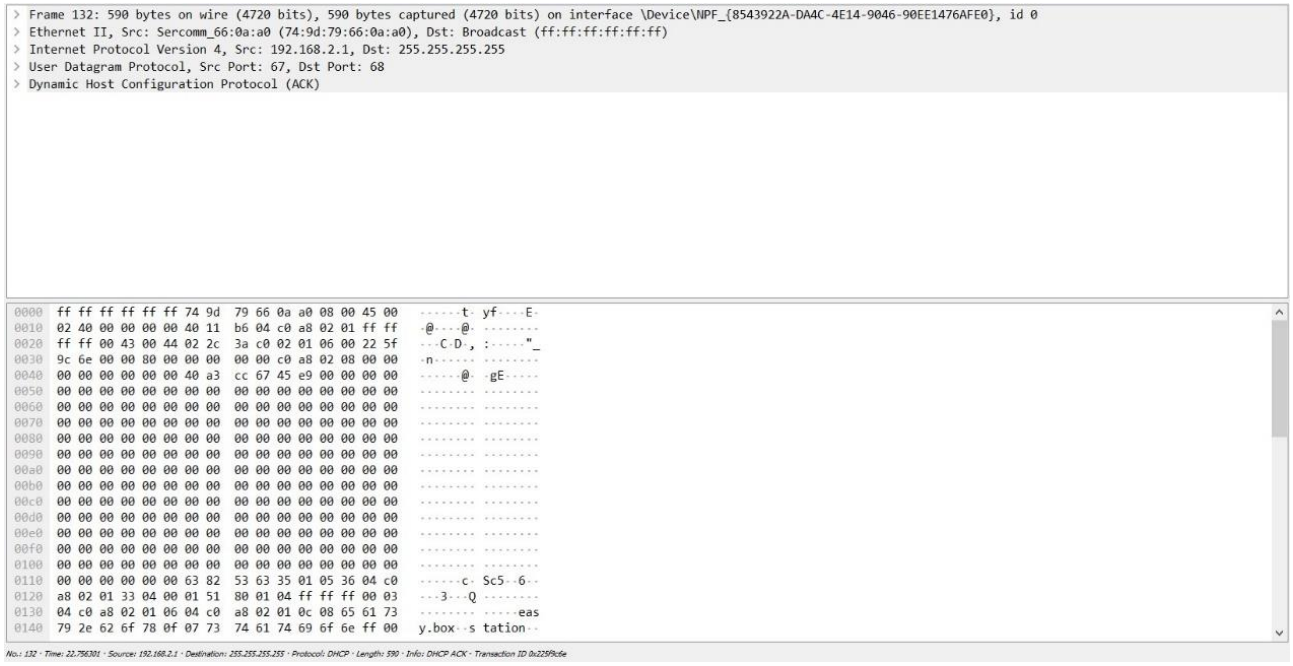
No.: 129 · Time: 22.500962 · Source: 0.0.0.0 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 344 · Info: DHCP Discover - Transaction ID 0x2259c6e

```
> Frame 130: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{8543922A-DA4C-4E14-9046-90EE1476AFE0}, id 0
> Ethernet II, Src: Sercomm_66:0a:a0 (74:9d:79:66:0a:a0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
> Dynamic Host Configuration Protocol (Offer)
```

```
0000  ff ff ff ff ff ff 74 9d  79 66 0a a0 08 00 45 00   ......t· yf····E·
0010  02 40 00 00 00 00 40 11  b6 04 c0 a8 02 01 ff ff   ·@····@· ········
0020  ff ff 00 43 00 44 02 2c  3d c0 02 01 06 00 22 5f   ···C·D·, =·····"_
0030  9c 6e 00 00 80 00 00 00  00 00 c0 a8 02 08 00 00   ·n····· ········
0040  00 00 00 00 00 00 40 a3  cc 67 45 e9 00 00 00 00   ......@· ·gE·····
0050  00 00 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 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 02 36 04 c0   ......c· Sc5··6··
0120  a8 02 01 33 04 00 01 51  80 01 04 ff ff ff 00 03   ···3···Q ........
0130  04 c0 a8 02 01 06 04 c0  a8 02 01 0c 08 65 61 73   ........ .....eas
0140  79 2e 62 6f 78 0f 07 73  74 61 74 69 6f 6e ff 00   y.box··s tation··
```

No.: 130 · Time: 22.551243 · Source: 192.168.2.1 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 590 · Info: DHCP Offer - Transaction ID 0x2259c6e





Για τα DHCP packets χρησιμοποιείται το πρωτόκολλο UDP 17 (User Datagram Protocol, port 17) και για το καθένα ισχύουν τα εξής:

DHCP Packet 1

DHCP Request

DHCP Packet 2

DHCP ACK

DHCP Packet 3

DHCP Request

DHCP Packet 4

DHCP ACK

DHCP Packet 5

DHCP Release

```
User Datagram Protocol, Src Port: 68, Dst Port: 67
User Datagram Protocol, Src Port: 67, Dst Port: 68
User Datagram Protocol, Src Port: 68, Dst Port: 67
User Datagram Protocol, Src Port: 67, Dst Port: 68
User Datagram Protocol, Src Port: 68, Dst Port: 67
```

DHCP Packet 6

DHCP Discover

DHCP Packet 7

DHCP Offer

DHCP Packet 8

DHCP Request

DHCP Packet 9

DHCP ACK

Οι διαφοροποιήσεις μεταξύ των πακέτων του DHCP Discover packet και το ακριβώς επόμενό του DHCP Request είναι στα πεδία: Total Length, Identification, Header Checksum, Checksum, Host Name, Vendor Class Identifier.

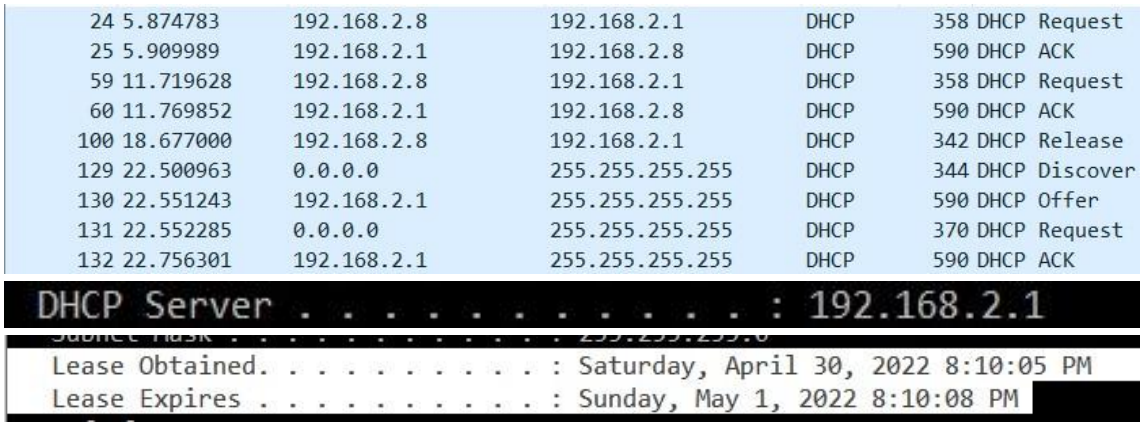
Οι διευθύνσεις IP (source και destination) φαίνονται στην παρακάτω εικόνα.

DCHP Server

Η IP διεύθυνση που ανατίθεται από το DCHP είναι προσωρινή και έχει προκαθορισμένη διάρκεια ζωής. Αυτή η διάρκεια ζωής λέγεται DHCP lease time. Ο DCHP Server υποθέτει πως όλες οι IP διευθύνσεις είναι προσωρινές και λήγουν μετά από ένα διάστημα, εκτός αν δηλωθεί το αντίθετο. Όπως φαίνεται και παραπάνω το lease time είναι 24 ώρες.

Το DHCP Lease Renewal (Release) είναι η διαδικασία κατά την οποία ο DHCP client ανανεώνει ή ενημερώνει τις IP διευθύνσεις του πριν την λήξη του lease .

```
User Datagram Protocol, Src Port: 68, Dst Port: 67
User Datagram Protocol, Src Port: 67, Dst Port: 68
User Datagram Protocol, Src Port: 68, Dst Port: 67
User Datagram Protocol, Src Port: 67, Dst Port: 68
```



24	5.874783	192.168.2.8	192.168.2.1	DHCP	358	DHCP Request
25	5.909989	192.168.2.1	192.168.2.8	DHCP	590	DHCP ACK
59	11.719628	192.168.2.8	192.168.2.1	DHCP	358	DHCP Request
60	11.769852	192.168.2.1	192.168.2.8	DHCP	590	DHCP ACK
100	18.677000	192.168.2.8	192.168.2.1	DHCP	342	DHCP Release
129	22.500963	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
130	22.551243	192.168.2.1	255.255.255.255	DHCP	590	DHCP Offer
131	22.552285	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request
132	22.756301	192.168.2.1	255.255.255.255	DHCP	590	DHCP ACK

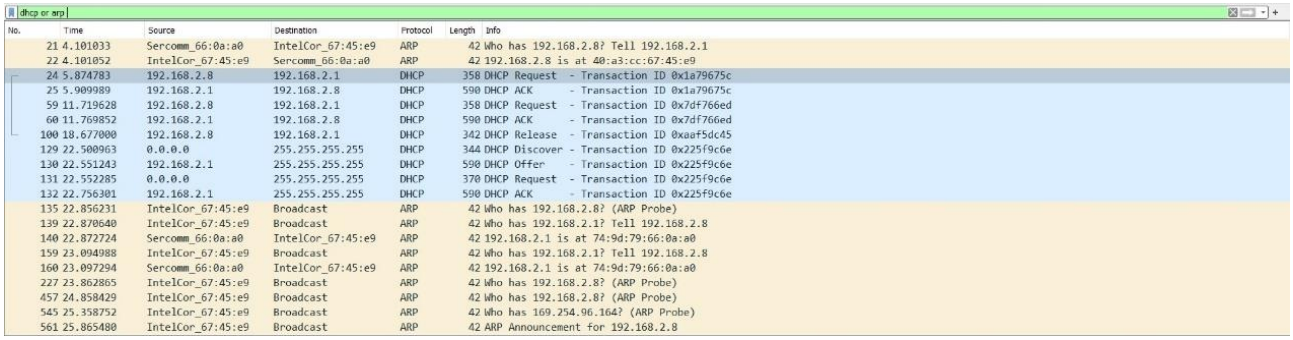
Το DHCP Release δεν λαμβάνει πακέτο ACK. Η απώλειά του οδηγεί σε duplicate IPs ανάμεσα σε συσκευές.

Κατά την διάρκεια ανταλλαγής DHCP μηνυμάτων, ανταλλάχθηκαν ARP μηνύματα ως εξής:

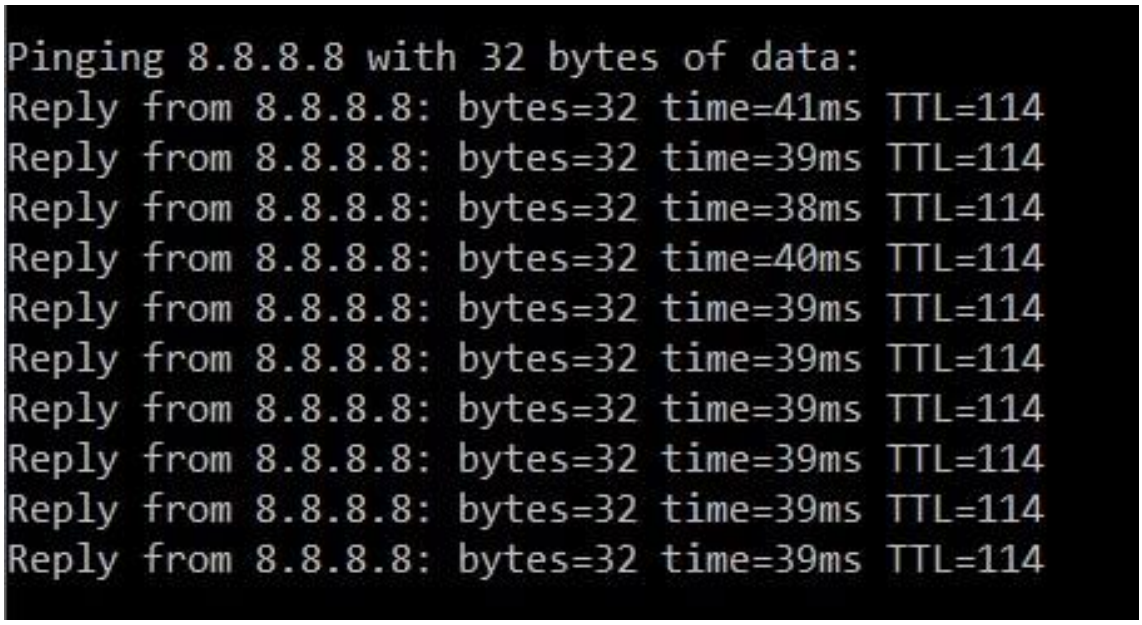
Το ARP είναι το πρωτόκολλο που χρησιμοποιείται για να συσχετίσει την IP address με μία MAC address. Χρησιμοποιείται για να εξασφαλίσει σε μία συσκευή πως καμία άλλη δεν χρησιμοποιεί την εκάστοτε IP διεύθυνση, πριν ξεκινήσει να την χρησιμοποιεί.

Ανάλυση ICMP πρωτοκόλλου – Ping

Τα αποτελέσματα της εκτέλεσης του ping -n 10 8.8.8.8 φαίνονται παρακάτω.



No.	Time	Source	Destination	Protocol	Length	Info
21	4.101033	Sercomm_66:0a:a0	IntelCor_67:45:e9	ARP	42	Who has 192.168.2.8? Tell 192.168.2.1
22	4.101052	IntelCor_67:45:e9	Sercomm_66:0a:a0	ARP	42	192.168.2.8 is at 40:a3:cc:67:45:e9
24	5.874783	192.168.2.8	192.168.2.1	DHCP	358	DHCP Request - Transaction ID 0x1a79675c
25	5.909989	192.168.2.1	192.168.2.8	DHCP	590	DHCP ACK - Transaction ID 0x1a79675c
59	11.719628	192.168.2.8	192.168.2.1	DHCP	358	DHCP Request - Transaction ID 0x7df766ed
60	11.769852	192.168.2.1	192.168.2.8	DHCP	590	DHCP ACK - Transaction ID 0x7df766ed
100	18.677000	192.168.2.8	192.168.2.1	DHCP	342	DHCP Release - Transaction ID 0xaaf5dc45
129	22.500963	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x225f9c6e
130	22.551243	192.168.2.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x225f9c6e
131	22.552285	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x225f9c6e
132	22.756301	192.168.2.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x225f9c6e
135	22.856231	IntelCor_67:45:e9	Broadcast	ARP	42	Who has 192.168.2.8? (ARP Probe)
139	22.870640	IntelCor_67:45:e9	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.8
140	22.872724	Sercomm_66:0a:a0	IntelCor_67:45:e9	ARP	42	192.168.2.1 is at 74:9d:79:66:0a:a0
159	23.094988	IntelCor_67:45:e9	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.8
160	23.097294	Sercomm_66:0a:a0	IntelCor_67:45:e9	ARP	42	192.168.2.1 is at 74:9d:79:66:0a:a0
227	23.862865	IntelCor_67:45:e9	Broadcast	ARP	42	Who has 192.168.2.8? (ARP Probe)
457	24.858429	IntelCor_67:45:e9	Broadcast	ARP	42	Who has 192.168.2.8? (ARP Probe)
545	25.358752	IntelCor_67:45:e9	Broadcast	ARP	42	Who has 169.254.96.164? (ARP Probe)
561	25.865480	IntelCor_67:45:e9	Broadcast	ARP	42	ARP Announcement for 192.168.2.8



Average RTT : **39ms**

Τα ICMP πακέτα

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4bd5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 390 (0x0186)
    Sequence Number (LE): 34305 (0x8601)
    [Response frame: 9]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53d5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 390 (0x0186)
    Sequence Number (LE): 34305 (0x8601)
    [Request frame: 8]
    [Response time: 41.355 ms]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53d4 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 391 (0x0187)
    Sequence Number (LE): 34561 (0x8701)
    [Request frame: 10]
    [Response time: 38.785 ms]
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4bd4 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 391 (0x0187)
    Sequence Number (LE): 34561 (0x8701)
    [Response frame: 12]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53d3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 392 (0x0188)
    Sequence Number (LE): 34817 (0x8801)
    [Request frame: 15]
    [Response time: 38.531 ms]
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4bd3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 392 (0x0188)
    Sequence Number (LE): 34817 (0x8801)
    [Response frame: 16]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53d2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 393 (0x0189)
    Sequence Number (LE): 35073 (0x8901)
    [Request frame: 19]
    [Response time: 39.818 ms]
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4bd2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 393 (0x0189)
    Sequence Number (LE): 35073 (0x8901)
    [Response frame: 20]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53d2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 393 (0x0189)
    Sequence Number (LE): 35073 (0x8901)
    [Request frame: 19]
    [Response time: 39.818 ms]
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4bd1 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 394 (0x018a)
    Sequence Number (LE): 35329 (0x8a01)
    [Response frame: 22]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53d1 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 394 (0x018a)
    Sequence Number (LE): 35329 (0x8a01)
    [Request frame: 21]
    [Response time: 39.180 ms]
```

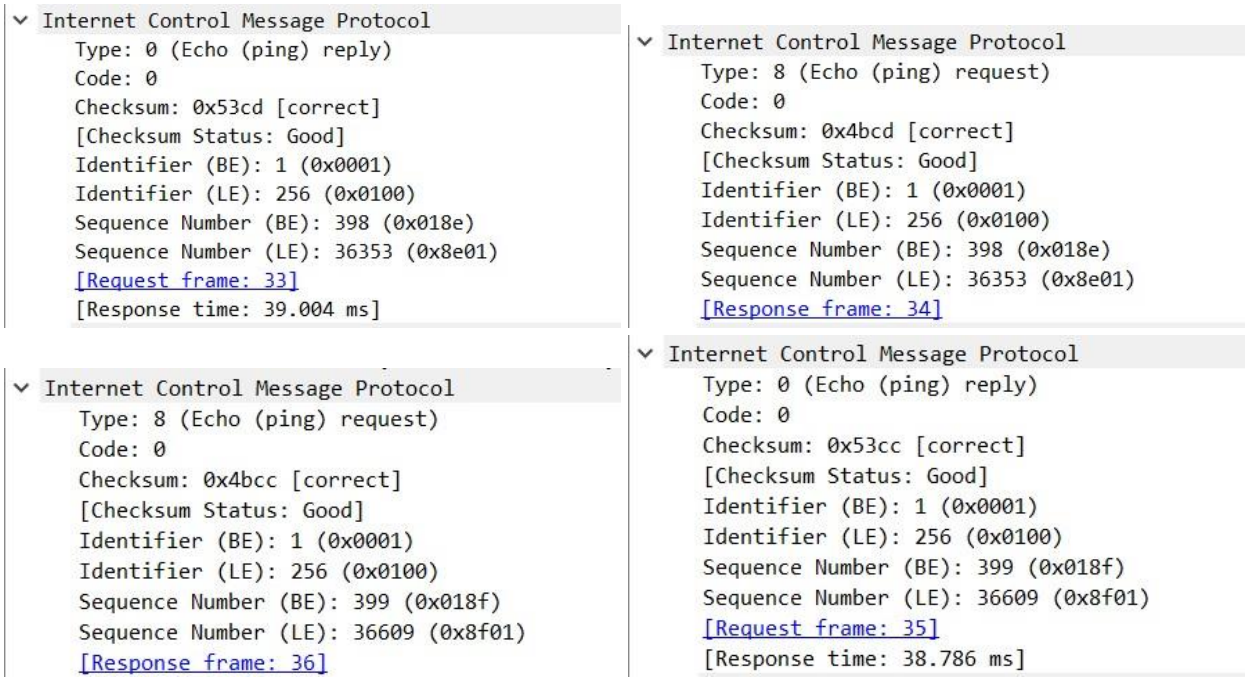
```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53d1 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 394 (0x018a)
    Sequence Number (LE): 35329 (0x8a01)
    [Request frame: 21]
    [Response time: 39.180 ms]
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4bd0 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 395 (0x018b)
    Sequence Number (LE): 35585 (0x8b01)
    [Response frame: 26]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53d0 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 395 (0x018b)
    Sequence Number (LE): 35585 (0x8b01)
    [Request frame: 25]
    [Response time: 39.087 ms]
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4bcf [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 396 (0x018c)
    Sequence Number (LE): 35841 (0x8c01)
    [Response frame: 28]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x53cf [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 396 (0x018c)
    Sequence Number (LE): 35841 (0x8c01)
    [Request frame: 27]
    [Response time: 39.390 ms]
```



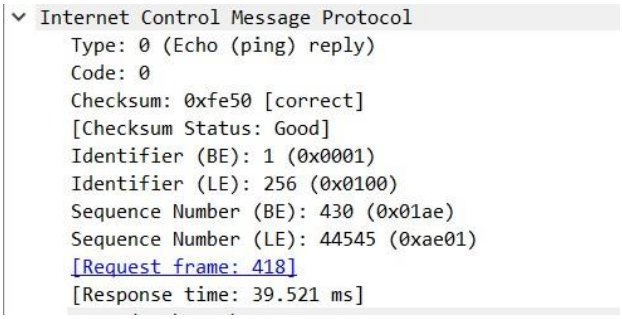
Ένα ICMP πακέτο δεν έχει αριθμούς για τα source και destination ports, καθώς είναι σχεδιασμένο να διανέμει network layer πληροφορίες μεταξύ hosts και routers και όχι μεταξύ application layer διαδικασίες. Κάθε ICMP packet έχει ένα πεδίο type και code, ενώ ο συνδυασμός τους είναι αναγνωριστικό για το εκάστοτε μήνυμα που λαμβάνεται. Εφόσον το ίδιο το δίκτυο ερμηνεύει όλα τα ICMP μηνύματα, δεν χρειάζονται αριθμοί θυρών για να κατευθύνουν τα μηνύματα σε κάποιο application layer process.

Ανάλυση ICMP πρωτοκόλλου – Traceroute

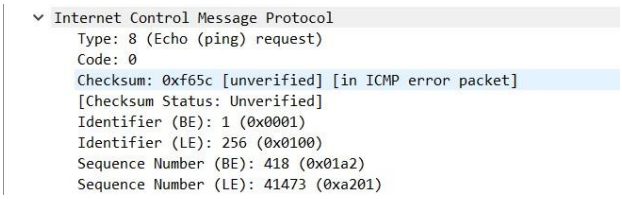
tracert 8.8.8.8

```
Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     1 ms     2 ms     2 ms  vodafone.station [192.168.2.1]
  2   119 ms    25 ms    24 ms  loopback2004.med01.dsl.hol.gr [62.38.0.170]
  3    25 ms    24 ms    25 ms  62.38.99.93
  4    56 ms    86 ms   137 ms  62.38.96.150
  5     *       24 ms    24 ms  62.74.30.194
  6    24 ms    24 ms    25 ms  ae3-100-ucr.ata.cw.net [195.89.103.69]
  7    39 ms    39 ms    39 ms  ae1-xcr1.sof.cw.net [195.2.27.9]
  8    41 ms    39 ms    38 ms  72.14.208.246
  9    39 ms    39 ms    45 ms  216.239.59.239
 10    39 ms    39 ms    39 ms  142.251.227.195
 11    39 ms    38 ms    39 ms  dns.google [8.8.8.8]

Trace complete.
```

Το πακέτο echo ICMP, παρουσιάζεται παρακάτω.



ICMP error πακέτο



Ανάλυση ICMP πακέτων

Γενικά, η δομή των ICMP πακέτων είναι η εξής:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | Type
| Code | Checksum | +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+-+-+-+-+-+-+ | Identifier | Sequence Number | +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | Data ...
```

9. TYPE -> 0f (Type 15 — Information Request (Deprecated)) CODE -> 00
   CHECKSUM -> 08 00
   ID -> 4f 00
   SEQUENCE NUMBER -> 00 64
   & DATA

10. TYPE -> 0f (Type 15 — Information Request (Deprecated))
    CODE -> 00
    CHECKSUM -> 08 00
    ID -> 4f 00
    SEQUENCE NUMBER -> 00 64 & DATA

11. TYPE -> 00 (Type 0 — Echo Reply) CODE -> 1d
    CHECKSUM -> 60 b3
    ID -> 01 84
    SEQUENCE NUMBER -> 00 12 & DATA

Ανάλυση IP πρωτοκόλλου

Ανάλυση Πλαισίου

Source: 129.110.30.26
Destination: 129.110.2.17
3 protocols in packet: Ethernet, IPv4, TCP Frame Length: 64 bytes (512 bits)
Source Port: 515
Destination Port: 80
Header checksum: 0x7dcb

Για τον υπολογισμό του checksum,αθροίζουμε τις τιμές των 16 bit του header. Έπειτα παίρνουμε το συμπλήρωμα ως προς 1 του αποτελέσματος και ύστερα μετατρέπουμε σε δεαεξαδικό.

Length of IP Packet = 41

Για τον υπολογισμό του μήκους του IP πακέτου παρατηρούμε τους τετραψήφιους hex αριθμούς του πακέτου. Ο πρώτος είναι ο 4500 και ο δεύτερος είναι **0029.** Μετατρέποντάς τον σε δεκαδικό έχουμε την τιμή που δείχνει το μήκος του IP packet.