4Η ΕΡΓΑΣΙΑ ΕΡΓΑΣΤΗΡΙΟΥ ΔΙΚΤΥΩΝ

Όνομα: Γεώργιος

Επώνυμο: Βέργος

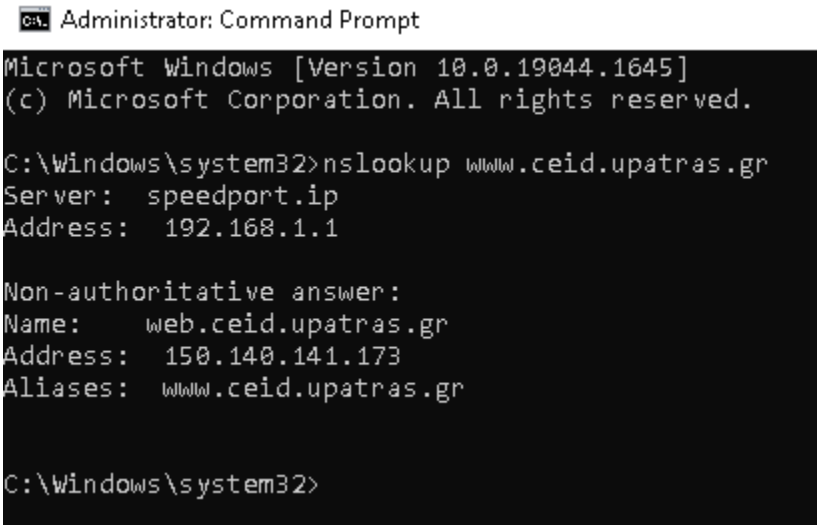
Αριθμός Μητρώου: 1072604

Ημερομηνία: 1/6/2022

Εξάμηνο: 6ο

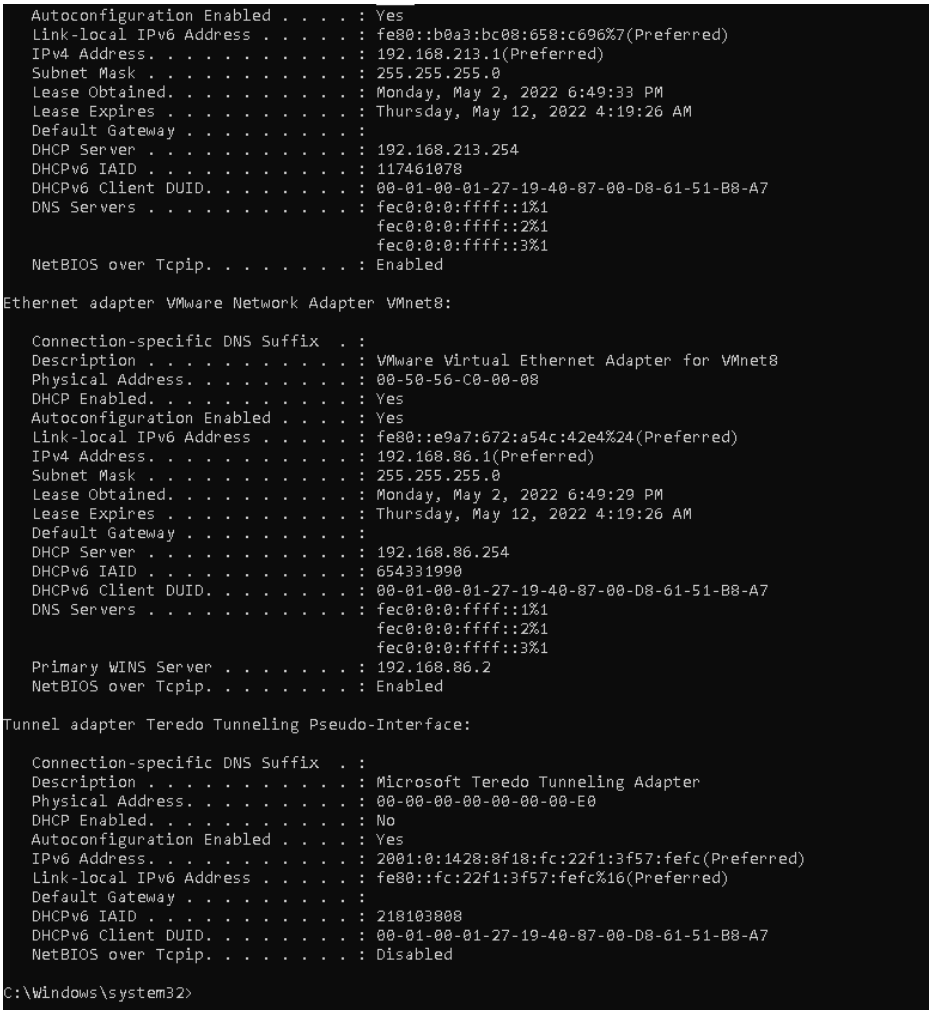
Εκτέλεση Βασικών εντολών

nslookup www.ceid.upatras.gr:



Ipconfig /all:

```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-711LR13
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : home

Ethernet adapter Radmin VPN:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Famatech RadminVPN Ethernet Adapter
   Physical Address. . . . . . . . . : 02-50-FB-B5-1F-6D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fdfd::1a69:414e(Preferred)
   Link-local IPv6 Address . . . . . : fe80::9dae:63a6:fe19:ddda%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 26.105.65.70(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . : 26.0.0.1
   DHCPv6 IAID . . . . . . . . . . . : 922098603
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-19-40-87-00-D8-61-51-B8-A7
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (7) I219-V
   Physical Address. . . . . . . . . : 00-D8-61-51-B8-A7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, May 2, 2022 6:49:39 PM
   Lease Expires . . . . . . . . . . : Thursday, May 12, 2022 6:49:18 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4bf:2d45:bd4e:6539%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 688521255
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-19-40-87-00-D8-61-51-B8-A7
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Loopback:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft KM-TEST Loopback Adapter
   Physical Address. . . . . . . . . : 02-00-4C-4F-4F-50
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a0b3:9bb4:8132:605c%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.137.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 1291976708
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-19-40-87-00-D8-61-51-B8-A7
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   Physical Address. . . . . . . . . : F4-D1-08-A7-C2-22
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : F4-D1-08-A7-C2-23
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : F6-D1-08-A7-C2-22
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-A3-95-31-F6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : Yes
```



ipconfig /displaydns:

```
C:\Windows\system32>ipconfig /displaydns

Windows IP Configuration

    22.229.128.79.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 22.229.128.79.in-addr.arpa
    Record Type . . . . . : 12
    Time To Live  . . . . : 34793
    Data Length . . . . . : 8
    Section . . . . . : Answer
    PTR Record  . . . . . : patr-asr9ka-patr-asr99a.backbone.otenet.net


    cm1-vie1.cm.steampowered.com
    ----------------------------------------
    Record Name . . . . . : cm1-vie1.cm.steampowered.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1427
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 146.66.155.38


    cm2-sto2.cm.steampowered.com
    ----------------------------------------
    Record Name . . . . . : CM2-sto2.Cm.steampowered.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1050
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 155.133.252.54


    example.org
    ----------------------------------------
    Record Name . . . . . : example.org
    Record Type . . . . . : 1
    Time To Live  . . . . : 25566
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 93.184.216.34


    example.org
    ----------------------------------------
    Record Name . . . . . : example.org
    Record Type . . . . . : 1
    Time To Live  . . . . : 25566
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 93.184.216.34


    cache4-fra1.steamcontent.com
    ----------------------------------------
    Record Name . . . . . : CaCHE4-fra1.steAmcONTenT.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1548
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 162.254.197.21
```

```
    api-js.mixpanel.com
    ----------------------------------------
    Record Name . . . . . : api-js.mixpanel.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1570
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 130.211.34.183


    Record Name . . . . . : api-js.mixpanel.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1570
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 35.190.25.25


    Record Name . . . . . : api-js.mixpanel.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1570
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 107.178.240.159


    Record Name . . . . . : api-js.mixpanel.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1570
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 35.186.241.51


    desktop-7111r13.mshome.net
    ----------------------------------------
    Record Name . . . . . : DESKTOP-7111R13.mshome.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 0
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 192.168.137.1


    desktop-7111r13.mshome.net
    ----------------------------------------
    No records of type AAAA


    cm1-fra2.cm.steampowered.com
    ----------------------------------------
    Record Name . . . . . : cm1-fra2.cm.steampowered.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1402
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 155.133.226.75


    cm2-fra1.cm.steampowered.com
    ----------------------------------------
    Record Name . . . . . : Cm2-fra1.Cm.STEAmpoWERED.com
```

```
Record Type . . . . . : 1
Time To Live  . . . . : 1445
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.254.197.54


cache1-fra1.steamcontent.com
----------------------------------------
Record Name . . . . . : cache1-fra1.steamcontent.com
Record Type . . . . . : 1
Time To Live  . . . . : 1389
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.254.197.6


cm6-sto1.cm.steampowered.com
----------------------------------------
Record Name . . . . . : cm6-sto1.cm.steampowered.com
Record Type . . . . . : 1
Time To Live  . . . . : 1492
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.254.198.104


ipv4only.arpa
----------------------------------------
Record Name . . . . . : ipv4only.arpa
Record Type . . . . . : 1
Time To Live  . . . . : 25570
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 192.0.0.170


Record Name . . . . . : ipv4only.arpa
Record Type . . . . . : 1
Time To Live  . . . . : 25570
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 192.0.0.171


mail1.upnet.gr
----------------------------------------
Record Name . . . . . : mail1.upnet.gr
Record Type . . . . . : 1
Time To Live  . . . . : 25695
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 150.140.129.17


1.1.168.192.in-addr.arpa
----------------------------------------
Record Name . . . . . : 1.1.168.192.in-addr.arpa
Record Type . . . . . : 12
Time To Live  . . . . : 77325
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record  . . . . . : speedport.ip
```

```
cache2-fra1.steamcontent.com
----------------------------------------
Record Name . . . . . : cache2-fra1.steamcontent.com
Record Type . . . . . : 1
Time To Live  . . . . : 1620
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.254.197.18


cache7-fra2.steamcontent.com
----------------------------------------
Record Name . . . . . : cache7-fra2.steamcontent.com
Record Type . . . . . : 1
Time To Live  . . . . : 1412
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 155.133.226.35


spclient.wg.spotify.com
----------------------------------------
Record Name . . . . . : spclient.wg.spotify.com
Record Type . . . . . : 5
Time To Live  . . . . : 61
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . . : edge-web.dual-gslb.spotify.com


Record Name . . . . . : edge-web.dual-gslb.spotify.com
Record Type . . . . . : 1
Time To Live  . . . . : 61
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 35.186.224.25


cm2-fra2.cm.steampowered.com
----------------------------------------
Record Name . . . . . : cm2-fra2.cm.steampowered.com
Record Type . . . . . : 1
Time To Live  . . . . : 1489
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 155.133.226.70


login.microsoftonline.com
----------------------------------------
Record Name . . . . . : login.microsoftonline.com
Record Type . . . . . : 5
Time To Live  . . . . : 117
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . . : ak.privatelink.msidentity.com


Record Name . . . . . : ak.privatelink.msidentity.com
Record Type . . . . . : 5
Time To Live  . . . . : 117
```

```
Data Length . . . . . : 0
Section . . . . . : Answer
CNAME Record  . . . : www.tm.ak.prd.aadg.akadns.net


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.190.160.12


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.137


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.69


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.139


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.190.160.15


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.135


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.73


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
```

```
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.190.160.13


login.microsoftonline.com
----------------------------------------
Record Name . . . . . : login.microsoftonline.com
Record Type . . . . . : 5
Time To Live  . . . . : 117
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . : ak.privatelink.msidentity.com


Record Name . . . . . : ak.privatelink.msidentity.com
Record Type . . . . . : 5
Time To Live  . . . . : 117
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . : www.tm.ak.prd.aadg.akadns.net


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.190.160.12


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.137


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.69


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.139


Record Name . . . . . : www.tm.ak.prd.aadg.akaDNS.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
```

```
Section . . . . . : Answer
A (Host) Record . . . : 20.190.160.15


Record Name . . . . . : www.tm.ak.prd.aadg.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.135


Record Name . . . . . : www.tm.ak.prd.aadg.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.73


Record Name . . . . . : www.tm.ak.prd.aadg.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 117
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.190.160.13


eclass.upatras.gr
----------------------------------------
Record Name . . . . . : eclass.upatras.gr
Record Type . . . . . : 5
Time To Live  . . . . : 33795
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . . : owl.upnet.gr


Record Name . . . . . : owl.UPNet.gr
Record Type . . . . . : 1
Time To Live  . . . . : 33795
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 150.140.129.14


eclass.upatras.gr
----------------------------------------
Record Name . . . . . : eclass.upatras.gr
Record Type . . . . . : 5
Time To Live  . . . . : 33795
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . . : owl.upnet.gr


Record Name . . . . . : owl.UPNet.gr
Record Type . . . . . : 1
Time To Live  . . . . : 33795
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 150.140.129.14
```

```
webmail.ceid.upatras.gr
----------------------------------------
Record Name . . . . . : webmail.ceid.upatras.gr
Record Type . . . . . : 5
Time To Live  . . . . : 33848
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . . : web.ceid.upatras.gr


Record Name . . . . . : web.ceid.upatras.gr
Record Type . . . . . : 1
Time To Live  . . . . : 33848
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 150.140.141.173


cm5-sto1.cm.steampowered.com
----------------------------------------
Record Name . . . . . : cm5-sto1.cm.steampowered.com
Record Type . . . . . : 1
Time To Live  . . . . : 1543
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.254.198.44


web.ceid.upatras.gr
----------------------------------------
Record Name . . . . . : web.ceid.upatras.gr
Record Type . . . . . : 1
Time To Live  . . . . : 37329
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 150.140.141.173


ld5-sync.com
----------------------------------------
Record Name . . . . . : ld5-sync.com
Record Type . . . . . : 1
Time To Live  . . . . : 12166
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 141.95.98.71


Record Name . . . . . : ld5-sync.com
Record Type . . . . . : 1
Time To Live  . . . . : 12166
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 141.95.98.69


Record Name . . . . . : ld5-sync.com
Record Type . . . . . : 1
Time To Live  . . . . : 12166
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 141.95.98.64
```

```
Record Name . . . . . : ids-sync.com
Record Type . . . . . : 1
Time To Live  . . . . : 12166
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 141.95.98.65


Record Name . . . . . : ids-sync.com
Record Type . . . . . : 1
Time To Live  . . . . : 12166
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 141.95.98.66


Record Name . . . . . : ids-sync.com
Record Type . . . . . : 1
Time To Live  . . . . : 12166
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 141.95.98.68


Record Name . . . . . : ids-sync.com
Record Type . . . . . : 1
Time To Live  . . . . : 12166
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 141.95.98.67


Record Name . . . . . : ids-sync.com
Record Type . . . . . : 1
Time To Live  . . . . : 12166
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 141.95.98.70


marketplace.visualstudio.com
----------------------------------------
Record Name . . . . . : marKEtPlACE.vISuaLSTUdiO.Com
Record Type . . . . . : 1
Time To Live  . . . . : 77
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 13.107.42.18


30.226.128.79.in-addr.arpa
----------------------------------------
Record Name . . . . . : 30.226.128.79.in-addr.arpa
Record Type . . . . . : 12
Time To Live  . . . . : 37503
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record  . . . . . : maro7609a-nyma-asr99a.backbone.otenet.net


233.240.128.79.in-addr.arpa
----------------------------------------
Record Name . . . . . : 233.240.128.79.in-addr.arpa
Record Type . . . . . : 12
Time To Live  . . . . : 35230
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record  . . . . . : athe-asr99b-athe-cgnb.backbone.otenet.net


discord.com
----------------------------------------
Record Name . . . . . : dISCoRd.com
Record Type . . . . . : 1
Time To Live  . . . . : 156
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.159.128.233


Record Name . . . . . : dISCoRd.com
Record Type . . . . . : 1
Time To Live  . . . . : 156
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.159.136.232


Record Name . . . . . : dISCoRd.com
Record Type . . . . . : 1
Time To Live  . . . . : 156
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.159.138.232


Record Name . . . . . : dISCoRd.com
Record Type . . . . . : 1
Time To Live  . . . . : 156
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.159.135.232


Record Name . . . . . : dISCoRd.com
Record Type . . . . . : 1
Time To Live  . . . . : 156
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.159.137.232


cache3-fra2.steamcontent.com
----------------------------------------
Record Name . . . . . : cache3-fRA2.sTeAmcONTent.com
Record Type . . . . . : 1
Time To Live  . . . . : 1660
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 155.133.226.34


cm1-fra1.cm.steampowered.com
----------------------------------------
```

```
----------------------------------------
Record Name . . . . . : CM1-FRA1.CM.STEAMpowERed.com
Record Type . . . . . : 1
Time To Live  . . . . : 1422
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 162.254.197.39


1.137.168.192.in-addr.arpa
----------------------------------------
Record Name . . . . . : 1.137.168.192.in-addr.arpa.
Record Type . . . . . : 12
Time To Live  . . . . : 0
Data Length . . . . . : 8
Section . . . . . . . : Answer
PTR Record  . . . . . : DESKTOP-711LR13.mshome.net


cache6-fra2.steamcontent.com
----------------------------------------
Record Name . . . . . : cache6-fra2.steamcontent.com
Record Type . . . . . : 1
Time To Live  . . . . : 1534
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 155.133.226.19


cm1-sto2.cm.steampowered.com
----------------------------------------
Record Name . . . . . : cm1-sto2.cm.steampowered.com
Record Type . . . . . : 1
Time To Live  . . . . : 1513
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 155.133.252.39


owl.upnet.gr
----------------------------------------
Record Name . . . . . : owl.UPNet.gr
Record Type . . . . . : 1
Time To Live  . . . . : 33039
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 150.140.129.14


www.ceid.upatras.gr
----------------------------------------
Record Name . . . . . : www.ceid.upatras.gr
Record Type . . . . . : 5
Time To Live  . . . . : 35506
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : web.ceid.upatras.gr


Record Name . . . . . : web.ceid.upatras.gr
Record Type . . . . . : 1
```

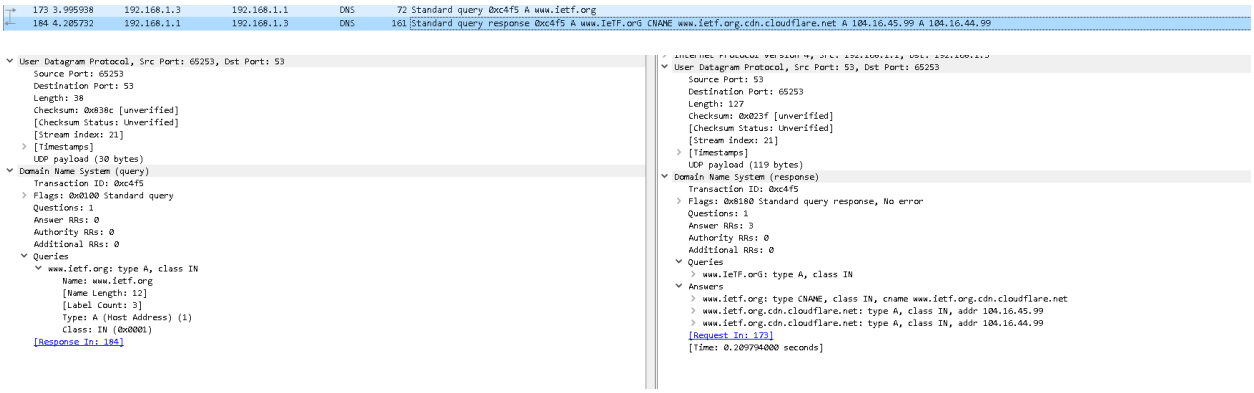
```
  Time To Live  . . . . : 35506
  Data Length . . . . . : 4
  Section . . . . . . . : Answer
  A (Host) Record . . . : 150.140.141.173


  cm2-vie1.cm.steampowered.com
  ----------------------------------------
  Record Name . . . . . : CM2-viE1.Cm.STEAmpoWERED.com
  Record Type . . . . . : 1
  Time To Live  . . . . : 1438
  Data Length . . . . . : 4
  Section . . . . . . . : Answer
  A (Host) Record . . . : 146.66.155.54


  237.240.128.79.in-addr.arpa
  ----------------------------------------
  Record Name . . . . . : 237.240.128.79.in-addr.arpa
  Record Type . . . . . : 12
  Time To Live  . . . . : 37479
  Data Length . . . . . : 8
  Section . . . . . . . : Answer
  PTR Record  . . . . . : athe-asr99a-athe-cgnb.backbone.otenet.net


  cache3-fra1.steamcontent.com
  ----------------------------------------
  Record Name . . . . . : cache3-fra1.STeamconteNT.com
  Record Type . . . . . : 1
  Time To Live  . . . . : 1683
  Data Length . . . . . : 4
  Section . . . . . . . : Answer
  A (Host) Record . . . : 162.254.197.7
```

Ipconfig /flushdns:

```
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>
```

ΑΝΑΛΥΣΗ DNS ΠΡΩΤΟΚΟΛΛΟΥ

1)



Χρησιμοποιήθηκε το UDP πρωτόκολλο.

2)

Η θύρα προορισμού για το μήνυμα ερώτησης DNS(DNS query) είναι η θύρα 53. Αυτό φαίνεται και στην παρακάτω εικόνα:

```
> User Datagram Protocol, Src Port: 65253, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xc4f5
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 184]
```

Η θύρα προέλευσης του μηνύματος απόκρισης DNS είναι η 53 φαίνεται από κάτω:

```
v User Datagram Protocol, Src Port: 53, Dst Port: 65253
    Source Port: 53
    Destination Port: 65253
    Length: 127
    Checksum: 0x023f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 21]
  > [Timestamps]
    UDP payload (119 bytes)
```

3)

Το μήνυμα ερώτησης DNS έχει ως Ip διεύθυνση προορισμού την 192.168.1.1 και προέλευσης 192.168.1.3. Οπότε ως DNS server έχουμε τον 192.168.1.1.
Τρέχοντας την εντολή ipconfig /all παίρνουμε :

```
   Default Gateway . . . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . . . : 192.168.1.1
                                           192.168.1.1
   NetBIOS over Tcpip. . . . . . . . . . : Enabled
```

Εμφανίζεται στην διεύθυνση 192.168.1.1:

Οι δύο αυτές διευθύνσεις συμφωνούν/είναι ίδιες.

4)

```
▾ Domain Name System (query)
    Transaction ID: 0xc4f5
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.ietf.org: type A, class IN
    [Response In: 184]
```

Δε περιέχει απαντήσεις και είναι τύπου Α.

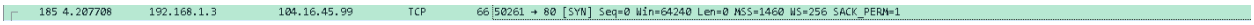
5)

```
Domain Name System (response)
    Transaction ID: 0xc4f5
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.IeTF.orG: type A, class IN
  v Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    [Request In: 173]
    [Time: 0.209794000 seconds]
```

Περιέχει 3 απαντήσεις .

6)

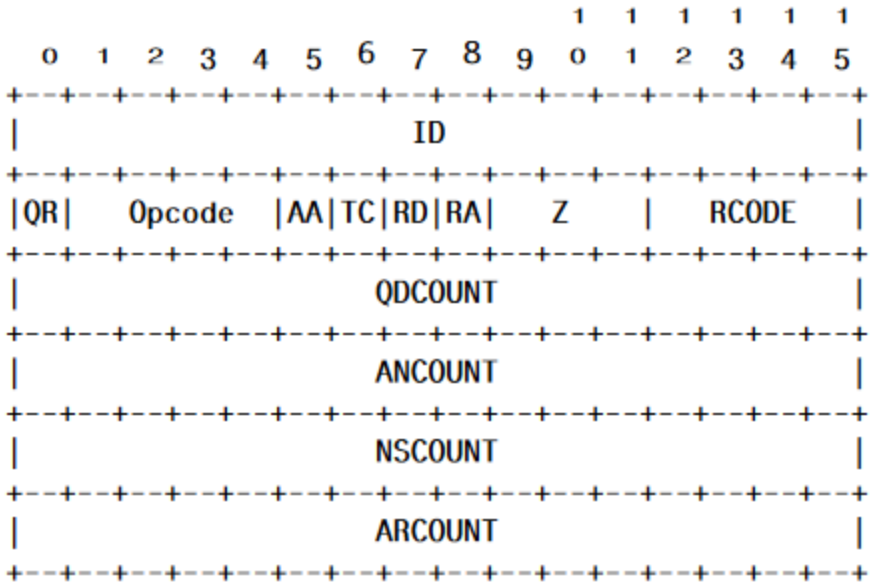
Το ζητούμενο TCP SYN πακέτο είναι το παρακάτω:



Με διεύθυνση 104.16.44.99 που αντιστοιχεί στη Ip διεύθυνση στις απαντήσεις του DNS response πακέτου.

7)

Το header ενός dns πακέτου έχει την ακόλουθη μορφή:



ID: Ένα 16-bit αναγνωριστικό το οποίο εκχωρείται από οποιοδήποτε πρόγραμμα που παράγει μία ερώτηση dns. Αυτό το αναγνωριστικό αντιγράφεται στην αντίστοιχη απάντηση και μπορεί αν χρησιμοποιηθεί από αυτόν που στέλνει την ερώτηση

Το QR bit είναι ένα bit ανάλογα την τιμή του ξέρουμε αν το dns μήνυμα είναι dns query ή dns response.

Το opcode είναι ένα 4bito πεδίο το οποίο δηλώνει το είδος του ερωτήματος dns.

AA: Το bit αυτό λέει αν ο αποκρινόμενος διακομιστής είναι κάποια εξουσία στο κομμάτι του dns όνομα ενός query.

Το TC είναι ένα bit το οποίο η τιμή του δηλώνει εάν το μήνυμα έχει υποστεί αποκοπή ή όχι, δηλαδή εφόσον το μήνυμα αποτελείται από μία ακολουθία από bits εάν στο τέλος έχουν αφαιρεθεί τα κάποια ή καθόλου bits.

Το RD bit ‘’λέει’’ στον διακομιστή ονοματοδοσίας του dns εκτελέσει αναδρομικά το αίτημα/ερώτημα(query).

Το RA bit σε μία απάντηση ενός ερωτήματος πρέπει να έχει την τιμή 0 και δηλώνει εάν είναι διαθέσιμη στον διακομιστή ονοματοδοσίας του dns υποστήριξη για αναδρομική εκτέλεση αιτημάτων.

Το Z παίρνει τιμή 0.

Το RCODE είναι μία 4-bitη συμβολοσειρά και αποτελεί μέρος των dns αποκρίσεων. Οι εξής τιμές σημαίνουν τα παρακάτω:

0- Καμία συνθήκη σφάλματος
1- Ο διακομιστής ονοματοδοσίας του dns δε μπόρεσε να ‘’καταλάβει’’ το αίτημα
2- Ο διακομιστής ονοματοδοσίας του dns δε μπόρεσε να επεξεργαστεί το αίτημα λόγω κάποιου προβλήματος με τον διακομιστή ονοματοδοσίας του dns.
3- Δείχνει ότι το ενσωματωμένο στο αίτημα dns domain name δεν υπάρχει.
4- Ο διακομιστής ονοματοδοσίας του dns δεν υποστηρίζει το συγκεκριμένο είδος αιτήματος
5- Ο διακομιστής ονοματοδοσίας του dns απέρριψε το συγκεκριμένο αίτημα λόγω πολιτικής ασφαλείας.

QDCOUNT Ένας 16-bit μη προσημασμένος ακέραιος που δηλώνει τον αριθμό καταχωρήσεων στο ‘’κομμάτι’’ των dns αιτημάτων.

ANCOUNT Ένας 16-bit μη προσημασμένος ακέραιος που δηλώνει τον αριθμό των εγγραφών πόρων στο τμήμα απαντήσεων.

NSCOUNT Ένας 16-bit μη προσημασμένος ακέραιος που δηλώνει τον αριθμό των εγγραφών πόρων του διακομιστή ονοματοδοσίας dns στο τμήμα καταχωρήσεων εξουσιοδοτημένης πρόσβασης.

ARCOUNT Ένας 16-bit μη προσημασμένος ακέραιος που δηλώνει τον αριθμό των εγγραφών πόρων στο τμήμα πρόσθετων εγγραφών.

8)

Αναλύοντας το πακέτο:

48 F8 B3 26 DF 49 BA BA BA BA BA BA 08 00 45 00 00 38 66 BD 00
00 80 11 02 0C C0 A8 01 34 08 08 08 08 D5 39 00 35 00 24 44 8F 00 03
01 00 00 01 00 00 00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00
01 00 01

Στο packetor έχουμε:

```
⊞ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
⊞ Ethernet II, Src: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba), Dst: Cisco-Li_26:df:49 (48:f8:b3:26:df:49)
⊞ Internet Protocol Version 4, Src: 192.168.1.52, Dst: 8.8.8.8
⊞ User Datagram Protocol, Src Port: 54585, Dst Port: 53
⊞ Domain Name System (query)
```

Και αναλυτικά:

- Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
  - Encapsulation type: Ethernet (1)
  - Arrival Time: May 29, 2022 18:26:22.000000000 UTC
  - Time shift for this packet: 0.000000000 seconds
  - Epoch Time: 1653848782.000000000 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: 0.000000000 seconds
  - Frame Number: 1
  - Frame Length: 70 bytes (560 bits)
  - Capture Length: 70 bytes (560 bits)
  - Frame is marked: False
  - Frame is ignored: False
  - Protocols in frame: eth:ethertype:ip:udp:dns
- Ethernet II, Src: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba), Dst: Cisco-Li_26:df:49 (48:f8:b3:26:df:49)
  - Destination: Cisco-Li_26:df:49 (48:f8:b3:26:df:49)
  - Source: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.52, Dst: 8.8.8.8
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 56
  - Identification: 0x66bd (26301)
  - Flags: 0x0000
  - Time to live: 128
  - Protocol: UDP (17)
  - Header checksum: 0x020c [correct]
  - Header checksum status: Good
  - Calculated Checksum: 0x020c
  - Source: 192.168.1.52
  - Source or Destination Address: 192.168.1.52
  - Source Host: 192.168.1.52
  - Source or Destination Host: 192.168.1.52
  - Destination: 8.8.8.8
  - Source or Destination Address: 8.8.8.8
  - Destination Host: 8.8.8.8
  - Source or Destination Host: 8.8.8.8
- User Datagram Protocol, Src Port: 54585, Dst Port: 53
  - Source Port: 54585
  - Destination Port: 53
  - Source or Destination Port: 54585
  - Source or Destination Port: 53
  - Length: 36
  - Checksum: 0x448f [correct]
  - Checksum Status: Good
  - Stream index: 0
- Domain Name System (query)
  - Transaction ID: 0x0003
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries

Ζητά την IP για το domain:

```
Queries
  google.com: type A, class IN
```

Αφορά ένα DNS query πακέτο τύπου A.

9)

Έχοντας το πακέτο:

BA BA BA BA BA BA 48 F8 B3 26 DF 49 08 00 45 08 00 E8 B2 EF 00
00 37 11 FE 21 08 08 08 08 C0 A8 01 34 00 35 D5 39 00 D4 28 A2 00 03
81 80 00 01 00 0B 00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00
01 00 01 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 23 C0 0C 00
01 00 01 00 00 00 04 00 04 4A 7D EC 25 C0 0C 00 01 00 01 00 00 00 04
00 04 4A 7D EC 27 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 20
C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 28 C0 0C 00 01 00 01
00 00 00 04 00 04 4A 7D EC 21 C0 0C 00 01 00 01 00 00 00 04 00 04 4A
7D EC 29 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 22 C0 0C 00
01 00 01 00 00 00 04 00 04 4A 7D EC 24 C0 0C 00 01 00 01 00 00 00 04
00 04 4A 7D EC 2E C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 26

στο packetor έχουμε:

```
Frame 1: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
Ethernet II, Src: Cisco-Li_26:df:49 (48:f8:b3:26:df:49), Dst: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.52
User Datagram Protocol, Src Port: 53, Dst Port: 54585
Domain Name System (response)
```

Και αναλυτικά:

- Frame 1: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
  - Encapsulation type: Ethernet (1)
  - Arrival Time: May 29, 2022 18:29:23.000000000 UTC
  - Time shift for this packet: 0.000000000 seconds
  - Epoch Time: 1653848963.000000000 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: 0.000000000 seconds
  - Frame Number: 1
  - Frame Length: 246 bytes (1968 bits)
  - Capture Length: 246 bytes (1968 bits)
  - Frame is marked: False
  - Frame is ignored: False
  - Protocols in frame: eth:ethertype:ip:udp:dns
- Ethernet II, Src: Cisco-Li_26:df:49 (48:f8:b3:26:df:49), Dst: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba)
  - Destination: ba:ba:ba:ba:ba:ba (ba:ba:ba:ba:ba:ba)
  - Source: Cisco-Li_26:df:49 (48:f8:b3:26:df:49)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.52
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x08 (DSCP: Unknown, ECN: Not-ECT)
  - Total Length: 232
  - Identification: 0xb2ef (45807)
  - Flags: 0x0000
  - Time to live: 55
  - Protocol: UDP (17)
  - Header checksum: 0xfe21 [correct]
  - Header checksum status: Good
  - Calculated Checksum: 0xfe21
  - Source: 8.8.8.8
  - Source or Destination Address: 8.8.8.8
  - Source Host: 8.8.8.8
  - Source or Destination Host: 8.8.8.8
  - Destination: 192.168.1.52
  - Source or Destination Address: 192.168.1.52
  - Destination Host: 192.168.1.52
  - Source or Destination Host: 192.168.1.52
- User Datagram Protocol, Src Port: 53, Dst Port: 54585
  - Source Port: 53
  - Destination Port: 54585
  - Source or Destination Port: 53
  - Source or Destination Port: 54585
  - Length: 212
  - Checksum: 0x28a2 [correct]
  - Checksum Status: Good
  - Stream index: 0
- Domain Name System (response)
  - Transaction ID: 0x0003
  - Flags: 0x8180 Standard query response, No error
  - Questions: 1
  - Answer RRs: 11
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
  - Answers
  - Unsolicited: True

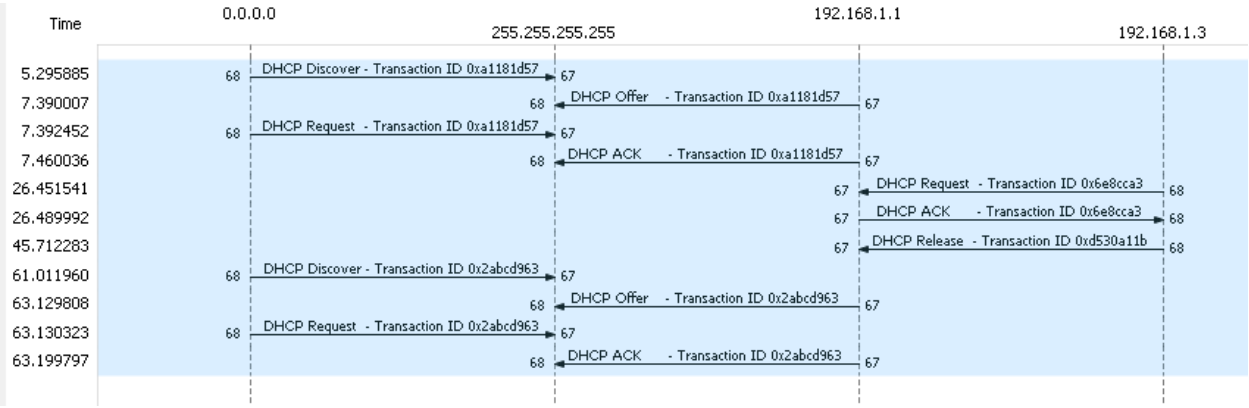
Αφορά ένα dns response πακέτο τύπου A:

```
Answers
    google.com: type A, class IN, addr 74.125.236.35
    google.com: type A, class IN, addr 74.125.236.37
    google.com: type A, class IN, addr 74.125.236.39
    google.com: type A, class IN, addr 74.125.236.32
    google.com: type A, class IN, addr 74.125.236.40
    google.com: type A, class IN, addr 74.125.236.33
    google.com: type A, class IN, addr 74.125.236.41
    google.com: type A, class IN, addr 74.125.236.34
    google.com: type A, class IN, addr 74.125.236.36
    google.com: type A, class IN, addr 74.125.236.46
    google.com: type A, class IN, addr 74.125.236.38
```

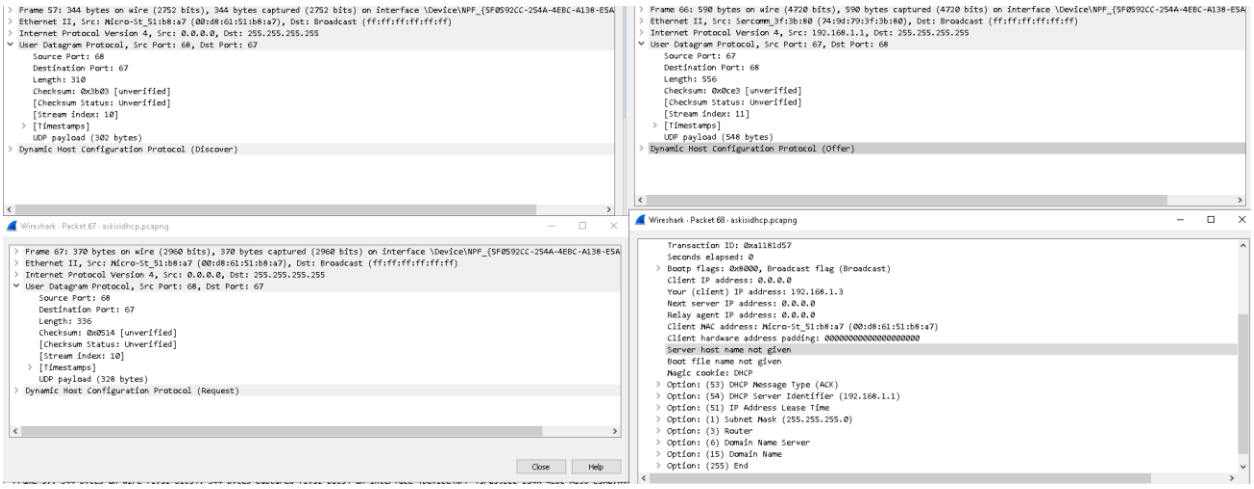
Ανάλυση DHCP πρωτοκόλλου

57	5.295885	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xa1181d57
66	7.390007	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0xa1181d57
67	7.392452	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xa1181d57
68	7.460036	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0xa1181d57
1127	26.451541	192.168.1.3	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0x6e8cca3
1128	26.489992	192.168.1.1	192.168.1.3	DHCP	590	DHCP ACK - Transaction ID 0x6e8cca3
1543	45.712283	192.168.1.3	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xd530a11b
1684	61.011960	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x2abcd963
1711	63.129808	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x2abcd963
1712	63.130323	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x2abcd963
1714	63.199797	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x2abcd963

Το datagram χρονισμού φαίνεται στη παρακάτω εικόνα:



Για κάθε πακέτο δείχνουμε τα port numbers πηγής και προορισμού:



2)

Χρησιμοποίειται το UDP πρωτόκολλο με θύρα προέλευσης την θύρα 68 και θύρα προορισμού τη θύρα 67:

```
User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 310
    Checksum: 0x3b03 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 10]
  > [Timestamps]
    UDP payload (302 bytes)
```

3)

Η διεύθυνση του επιπέδου ζεύξης δεδομένων του Ethernet του υπολογιστή μου είναι η MAC διεύθυνση και είναι η :

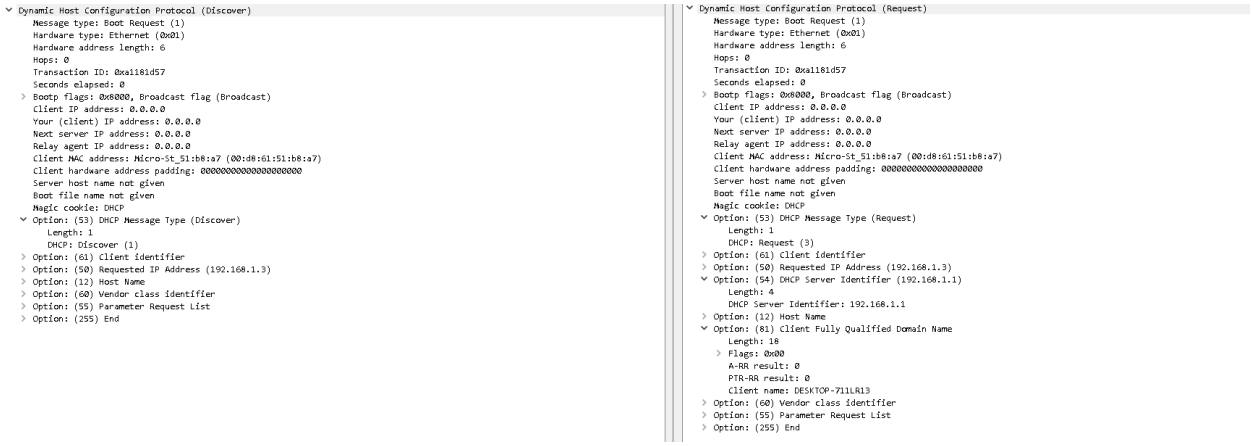
```
   Physical Address. . . . . . . . . : 00-D8-61-51-B8-A7
```

Η οποία φαίνεται και στα πακέτα:

```
> Source: Micro-St_51:b8:a7 (00:d8:61:51:b8:a7)
```

4)

Στη παρακάτω εικόνα φαίνονται οι διαφορές μεταξύ των μηνυμάτων DHCP discover και DHCP request.

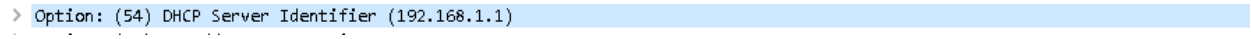


5)

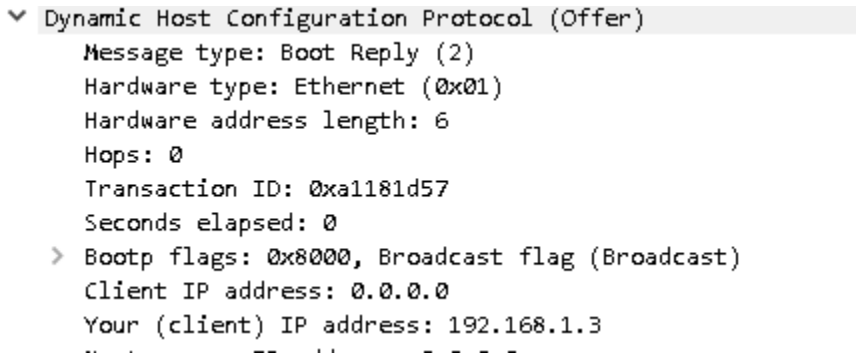
0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover
192.168.1.1	255.255.255.255	DHCP	590 DHCP Offer
0.0.0.0	255.255.255.255	DHCP	370 DHCP Request
192.168.1.1	255.255.255.255	DHCP	590 DHCP ACK

6)

Η Ip διεύθυνση του dhcp server είναι η 192.168.1.1 κάτι που φαίνεται στην παρακάτω εικόνα από το πακέτο τύπου Offer:



Η Ip διεύθυνση που μου προσφέρεται από τον dhcp server είναι η 192.168.1.3:

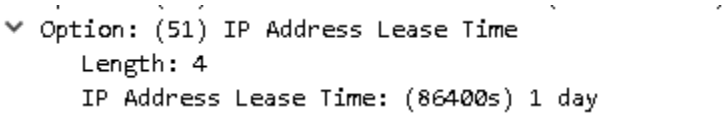


Από το πακέτο τύπου Request.

7)

Ο lease time είναι ο χρόνος σε δευτερόλεπτα που μπορεί μία διεπαφή δικτύου στη συγκεκριμένη περίπτωση ο Ethernet Adapter να κρατήσει/χρησιμοποιήσει

μία Ip διέυθυνση σε ένα δίκτυο. Στη συγκεκριμένη περώπτωση είναι 86400 sec το οποίο φαίνεται και στην παρακάτω εικόνα:



8)

Το μήνυμα DHCP release εμφανίζεται όταν εκτελούμε την εντολή ipconfig /release όπου εξαναγκάζουμε τον client(εμάς δηλαδή) να ‘’παρατήσει’’ την Ip διεύθυνση που έχει στέλνοντας το μήνυμα αυτό στον dhcp server προκειμένου να μαρκάει τη διεύθυνση που ‘’παράτησε’’ ο client ως διαθέσιμη.

Ωστόσο ο dhcp server δεν στέλνει επιβεβαίωση λήψης του μηνύματος DHCP request. Αν το μήνυμα αυτό χαθεί ο υπολογιστής ‘’παρατάει’’ την διεύθυνση Ip , αλλά ο dhcp server δε θα αναθέσει στον υπολογιστή μας Ip διεύθυνση παρά μόνο όταν περάσει το χρονικό διάστημα του lease time.

9)

Ανταλλάχθηκαν ARP πακέτα κατά τη διάρκεια ανταλλαγής DHCP τα οποία φαίνονται στην παρακάτω εικόνα:

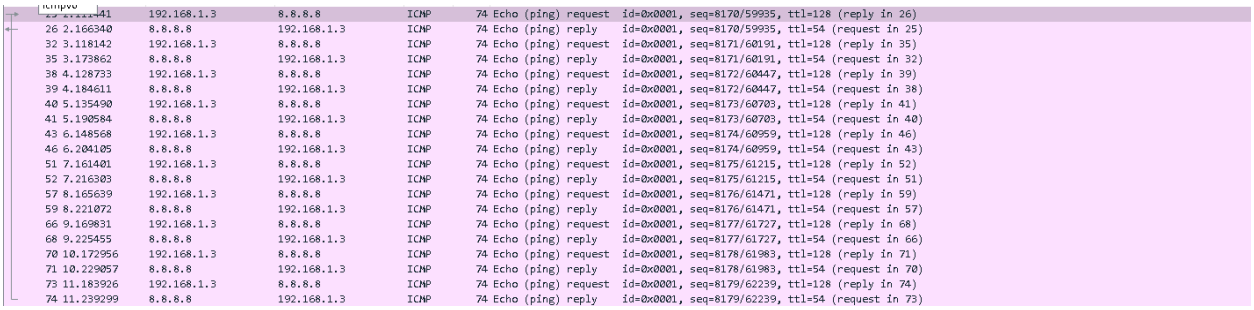
1	0.000000	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
19	0.999932	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
33	1.999987	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
47	3.824431	Sercomm_3f:3b:80	Broadcast	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
55	4.819938	Sercomm_3f:3b:80	Broadcast	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
58	5.297908	Sercomm_3f:3b:80	Broadcast	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
59	5.820049	Sercomm_3f:3b:80	Broadcast	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
64	6.875968	Sercomm_3f:3b:80	Broadcast	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
70	7.494640	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.3
73	7.495302	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 192.168.1.1 is at 74:9d:79:3f:3b:80
77	7.556578	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.3
78	7.558081	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 192.168.1.1 is at 74:9d:79:3f:3b:80
102	7.904430	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.3
103	7.904637	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 192.168.1.1 is at 74:9d:79:3f:3b:80
104	7.912494	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.3? (ARP Probe)
199	8.908879	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.3? (ARP Probe)
362	9.918063	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.3? (ARP Probe)
550	10.909422	Micro-St_51:b8:a7	Broadcast	ARP	42 ARP Announcement for 192.168.1.3
1116	25.559840	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
1117	25.559871	Micro-St_51:b8:a7	Sercomm_3f:3b:80	ARP	42 192.168.1.3 is at 00:d8:61:51:b8:a7
1541	44.889777	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
1542	44.889806	Micro-St_51:b8:a7	Sercomm_3f:3b:80	ARP	42 192.168.1.3 is at 00:d8:61:51:b8:a7
1569	52.413805	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 169.254.78.99? (ARP Probe)
1572	53.408619	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 169.254.78.99? (ARP Probe)
1576	54.417474	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 169.254.78.99? (ARP Probe)
1582	55.408584	Micro-St_51:b8:a7	Broadcast	ARP	42 ARP Announcement for 169.254.78.99
1685	61.013863	Sercomm_3f:3b:80	Broadcast	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
1707	62.759677	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 Who has 192.168.1.3? Tell 192.168.1.1
1724	64.642196	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.3
1725	64.643032	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 192.168.1.1 is at 74:9d:79:3f:3b:80
1746	64.918288	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.3? (ARP Probe)
1757	65.049815	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.3
1758	65.049972	Sercomm_3f:3b:80	Micro-St_51:b8:a7	ARP	60 192.168.1.1 is at 74:9d:79:3f:3b:80
1818	65.909622	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.3? (ARP Probe)
1860	66.918882	Micro-St_51:b8:a7	Broadcast	ARP	42 Who has 192.168.1.3? (ARP Probe)
2085	67.912604	Micro-St_51:b8:a7	Broadcast	ARP	42 ARP Announcement for 192.168.1.3

Ανάλυση ICMP πρωτοκόλλου – Ping

1)

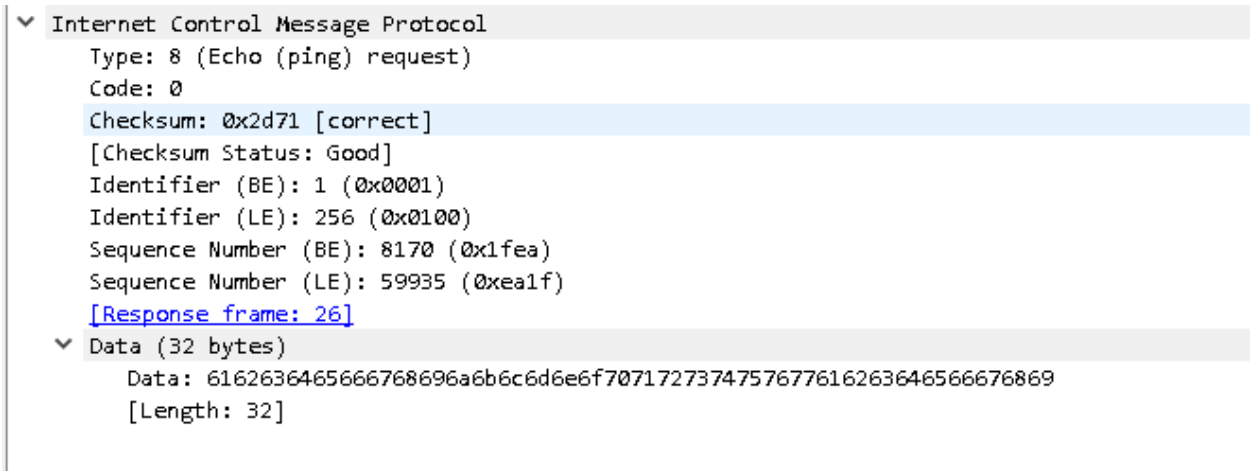
```
C:\Windows\system32>ping -n 10 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=55ms TTL=54
Reply from 8.8.8.8: bytes=32 time=57ms TTL=54
Reply from 8.8.8.8: bytes=32 time=58ms TTL=54
Reply from 8.8.8.8: bytes=32 time=55ms TTL=54
Reply from 8.8.8.8: bytes=32 time=55ms TTL=54
Reply from 8.8.8.8: bytes=32 time=55ms TTL=54
Reply from 8.8.8.8: bytes=32 time=54ms TTL=54
Reply from 8.8.8.8: bytes=32 time=56ms TTL=54
Reply from 8.8.8.8: bytes=32 time=55ms TTL=54
Reply from 8.8.8.8: bytes=32 time=55ms TTL=54

Ping statistics for 8.8.8.8:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 58ms, Average = 55ms

C:\Windows\system32>
```

2)



[illegible]	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8170/59935, ttl=128 (reply in 26)
26 2.166340	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8170/59935, ttl=54 (request in 25)
32 3.118142	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8171/60191, ttl=128 (reply in 35)
35 3.173862	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8171/60191, ttl=54 (request in 32)
38 4.128733	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8172/60447, ttl=128 (reply in 39)
39 4.184611	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8172/60447, ttl=54 (request in 38)
40 5.135490	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8173/60703, ttl=128 (reply in 41)
41 5.190584	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8173/60703, ttl=54 (request in 40)
43 6.148568	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8174/60959, ttl=128 (reply in 46)
46 6.204105	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8174/60959, ttl=54 (request in 43)
51 7.161401	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8175/61215, ttl=128 (reply in 52)
52 7.216303	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8175/61215, ttl=54 (request in 51)
57 8.165639	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8176/61471, ttl=128 (reply in 59)
59 8.221072	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8176/61471, ttl=54 (request in 57)
66 9.169831	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8177/61727, ttl=128 (reply in 68)
68 9.225455	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8177/61727, ttl=54 (request in 66)
70 10.172956	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8178/61983, ttl=128 (reply in 71)
71 10.229057	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8178/61983, ttl=54 (request in 70)
73 11.183926	192.168.1.3	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8179/62239, ttl=128 (reply in 74)
74 11.239299	8.8.8.8	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=8179/62239, ttl=54 (request in 73)

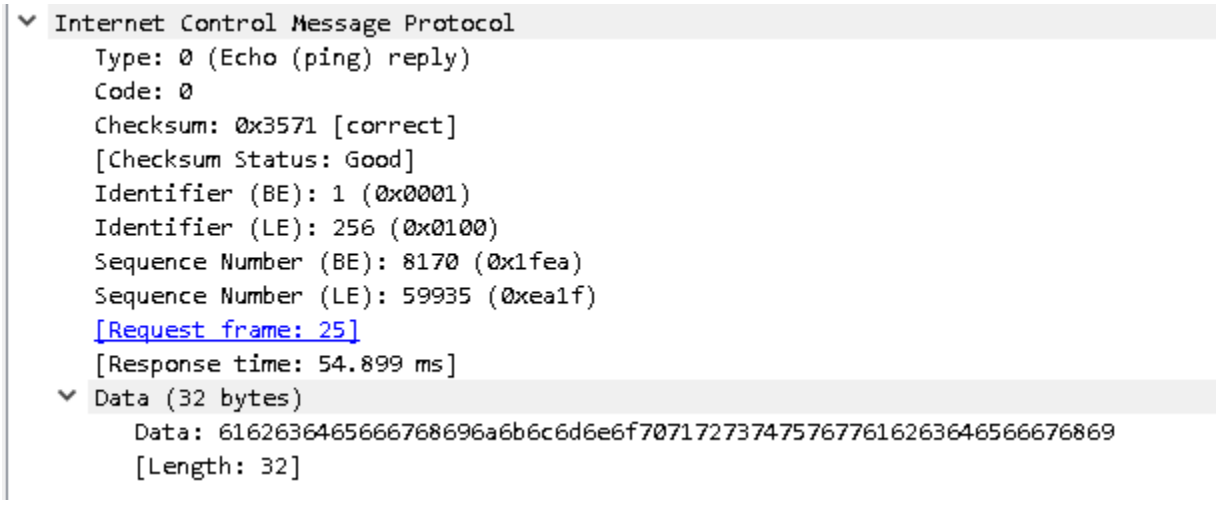
Ο Τύπος το άθροισμα ελέγχου, το αναγνωριστικό, ο αύξοντας αριθμός και το code του ICMP μηνύματος φαίνονται στην παρακάτω εικόνα:



3)

Ένα ICMP πακέτο δεν έχει τους αριθμούς θυρών πηγής και προορισμού γιατί σχεδιάστηκε για τη μετάδοση πληροφορίας στο επίπεδο δικτύου μεταξύ χρηστών και routers και όχι μεταξύ διεργασιών στο επίπεδο εφαρμογής.

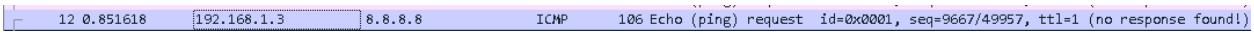
4)



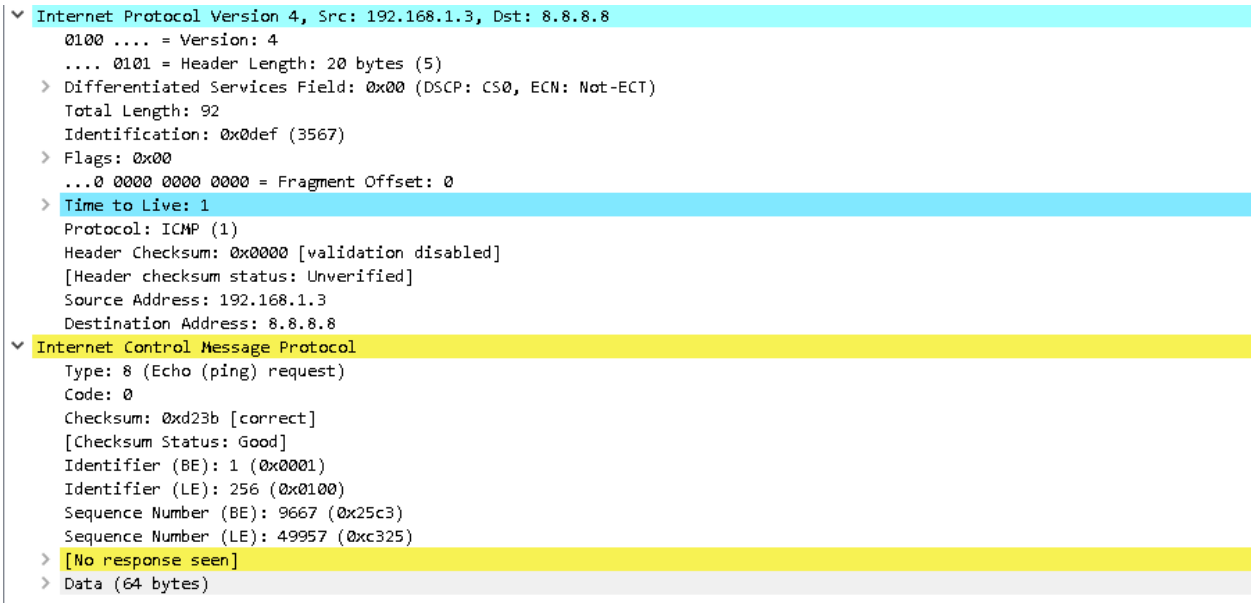
Τα πεδία identifier,checksum και sequence number αποτελούνται το καθένα από 4 δεκαεξαδικά ψηφία οπότε το μέγεθος εκάστου είναι 2 bytes.

Ανάλυση ICMP πρωτοκόλλου – Traceroute

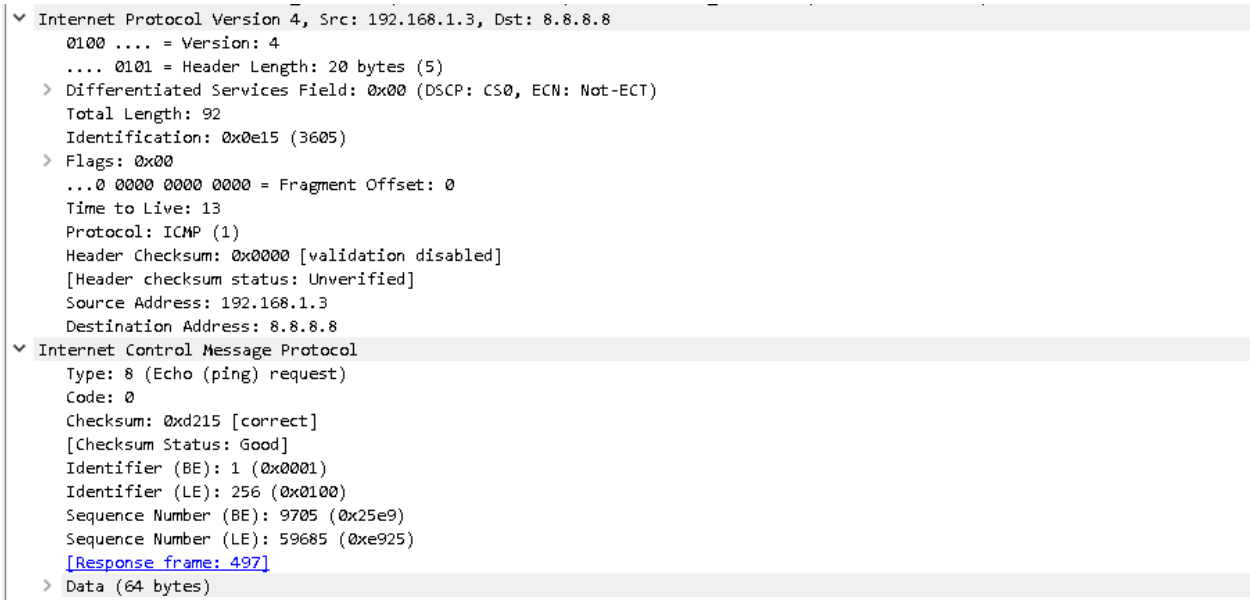
```
C:\Windows\system32>tracert 8.8.8.8

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

  1    <1 ms    <1 ms    <1 ms  speedport.ip [192.168.1.1]
  2    14 ms    14 ms    14 ms  10.106.108.100
  3    17 ms    17 ms    17 ms  79.128.234.0
  4    17 ms    17 ms    18 ms  patr-asr9ka-patr-asr99a.backbone.otenet.net [79.128.229.22]
  5    17 ms    17 ms    17 ms  79.128.234.163
  6     *        *        *     Request timed out.
  7    17 ms    18 ms    18 ms  athe-asr99a-athe-cgnb.backbone.otenet.net [79.128.248.233]
  8    19 ms    19 ms    20 ms  kolasr01-hu-0-5-0-0.ath.OTEGlobe.gr [62.75.3.13]
  9    56 ms    56 ms    57 ms  62.75.27.37
 10    56 ms    56 ms    55 ms  74.125.51.154
 11    57 ms    57 ms    57 ms  142.251.65.75
 12    56 ms    57 ms    57 ms  142.250.46.247
 13    56 ms    55 ms    55 ms  dns.google [8.8.8.8]

Trace complete.
```



Πρώτο πακέτο Echo Request:

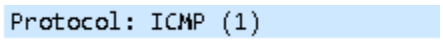


Τελευταίο πακέτο echo Request:



5)

Αν το ICMP στείλει UDP πακέτα (όπως στα Unix/Linux), ο αριθμός IP πρωτοκόλλου δεν θα ήταν 01 όπως στην εικόνα:



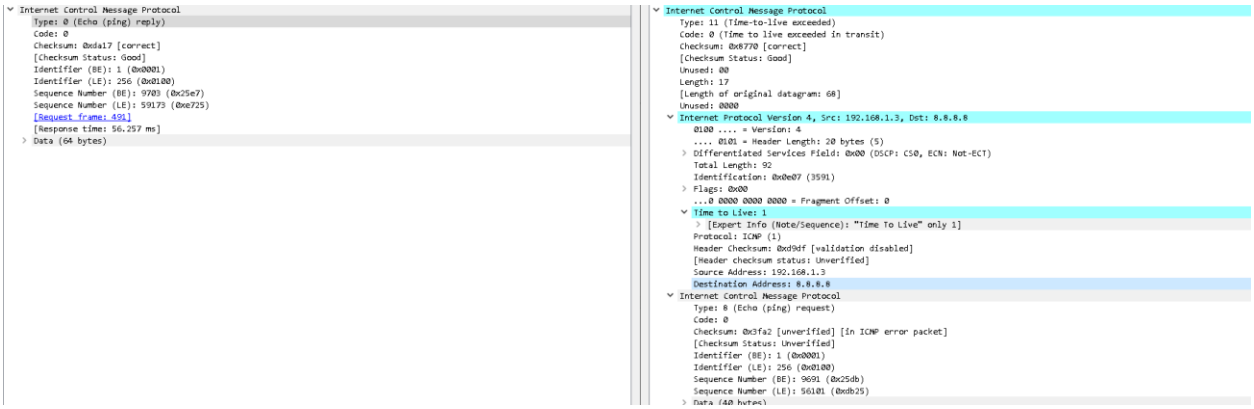
αλλά 11.

6)

Τα ICMP πακέτα στα παραπάνω screenshot είναι ίδια με τα πακέτα ερωτημάτων ICMP.

7)

Στην παρακάτω εικόνα φαίνονται τα πεδία που διαφέρει το πακέτο σφάλματος από το echo πακέτο.



8)

Το πακέτο σφάλματος διαφέρει από τα 3 τελευταία που παρέλαβε ο host της πηγής στο ότι το πακέτο σφάλματος έχει τύπο 11 ενώ τα υπόλοιπα 0. Είναι διαφορετικά γιατί τα τελευταία 3 πακέτα φτάνουν στον προορισμό τους πριν τελειώσει το time to live.

9)

```
⊞ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
⊞ Ethernet II, Src: Cisco_26:3f:e9 (00:e0:f7:26:3f:e9), Dst: Oracle_86:35:4b (08:00:20:86:35:4b)
⊞ Internet Protocol Version 4, Src: 139.133.233.2, Dst: 139.133.217.110
⊟ Internet Control Message Protocol
   ☐ Type: 0 (Echo (ping) reply)
   ☐ Code: 0
   ☐ Checksum: 0x45da [correct]
   ☐ Checksum Status: Good
   ☐ Identifier (BE): 7776 (0x1e60)
   ☐ Identifier (LE): 24606 (0x601e)
   ☐ Sequence number (BE): 0 (0x0000)
   ☐ Sequence number (LE): 0 (0x0000)
   ⊞ data
```

Το παραπάνω πακέτο είναι τύπου 0 δηλαδή απάντηση echo ερωτήματος(ping).

10)

```
+ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
+ Ethernet II, Src: RPTInter_49:03:5f (00:40:95:49:03:5f), Dst: Lite-OnU_63:08:1b (00:a0:cc:63:08:1b)
+ Internet Protocol Version 4, Src: 192.168.1.32, Dst: 192.168.1.64
- Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x485c [correct]
    Checksum Status: Good
    Identifier (BE): 256 (0x0100)
    Identifier (LE): 1 (0x0001)
    Sequence number (BE): 1024 (0x0400)
    Sequence number (LE): 4 (0x0004)
  + data
```

Είναι τύπου 8 δηλαδή echo request.

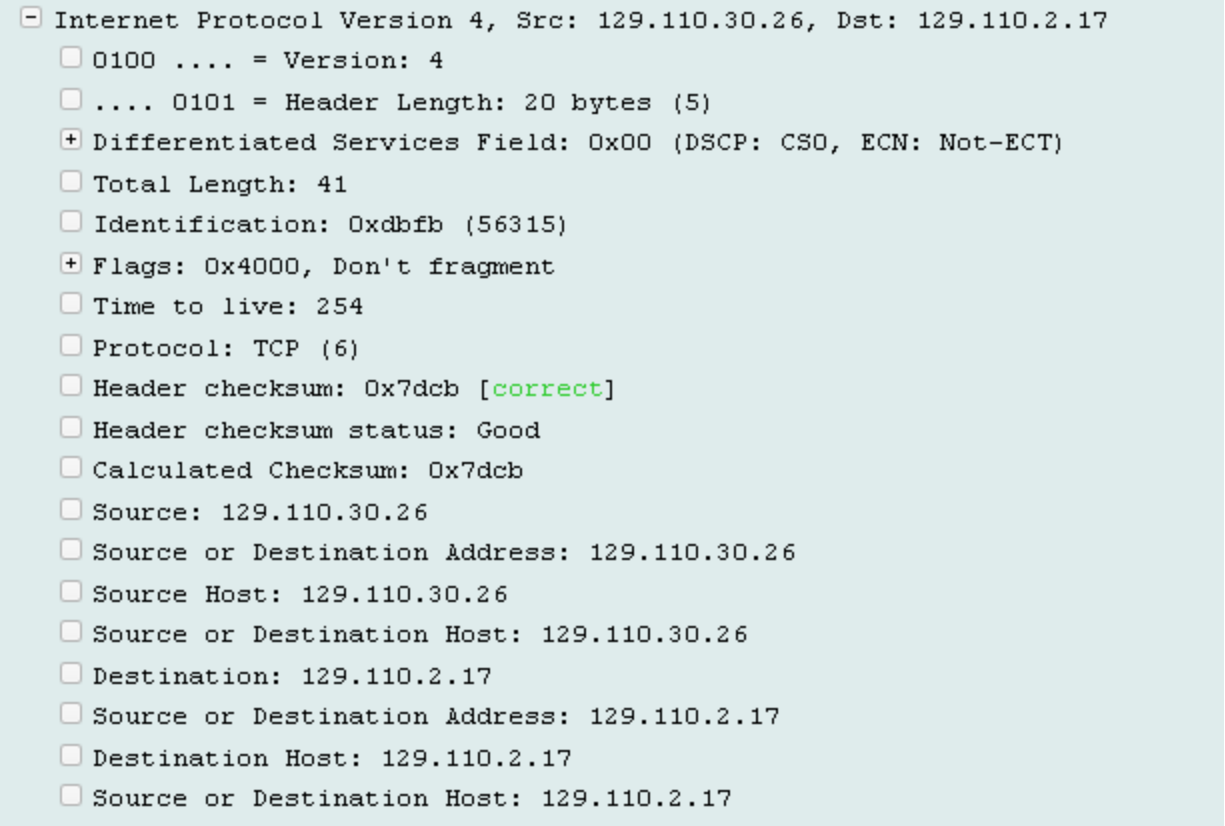
11)

```
+ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
+ Ethernet II, Src: Cisco_eb:6b:40 (00:12:7f:eb:6b:40), Dst: AsustekC_b3:01:84 (00:1d:60:b3:01:84)
+ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.0.2
- Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xfc5d [correct]
    Checksum Status: Good
    Unused: 00000000
```

Είναι τύπου 3 Destination Unreachable.

Ανάλυση IP πρωτοκόλλου

1)



IP διεύθυνση προορισμού: 129.110.2.17

IP διεύθυνση πηγής/αποστολής: 129.110.30.26

2)

Το μήκος του IP header είναι 20 bytes:

```
Internet Protocol Version 4, Src: 129.110.30.26, Dst: 129.110.2.17
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
    Identification: 0xdbfb (56315)
    Flags: 0x4000, Don't fragment
    Time to live: 254
    Protocol: TCP (6)
    Header checksum: 0x7dcb [correct]
    Header checksum status: Good
    Calculated Checksum: 0x7dcb
    Source: 129.110.30.26
    Source or Destination Address: 129.110.30.26
    Source Host: 129.110.30.26
    Source or Destination Host: 129.110.30.26
    Destination: 129.110.2.17
    Source or Destination Address: 129.110.2.17
    Destination Host: 129.110.2.17
    Source or Destination Host: 129.110.2.17
```

Το μήκος όλου του πακέτου είναι 64 bytes:

```
Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
```

3)

Δεν είναι μέρος ενός μεγαλύτερου πακέτου.

4)

Η θύρα αποστολέα/πηγής είναι η 515 ενώ η θύρα προορισμού/δέκτη είναι η 80 και φαίνεται στην παρακάτω εικόνα:

```
Transmission Control Protocol, Src Port: 515, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
    Source Port: 515
    Destination Port: 80
    Source or Destination Port: 515
    Source or Destination Port: 80
    Stream index: 0
    TCP Segment Len: 1
    Sequence number: 1 (relative sequence number)
    Next sequence number: 2 (relative sequence number)
    Acknowledgment number: 1 (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window size value: 9216
    Calculated window size: 9216
    Window size scaling factor: -1 (unknown)
    Checksum: 0x17c4 [correct]
    Checksum Status: Good
    Calculated Checksum: 0x17c4
    Urgent pointer: 0
    SEQ/ACK analysis
    Timestamps
    TCP payload (1 byte)
```

5)

Η τιμή στο Checksum είναι η 7DCB(HEX) και φαίνεται στην παρακάτω εικόνα:

```
    Header checksum: 0x7dcb [correct]
    Header checksum status: Good
    Calculated Checksum: 0x7dcb
```

Η οποία είναι σωστή.