Εργαστήριο Δικτύων - 1η Εργαστηριακή άσκηση

ΣΙΑΜΟΓΛΟΥ ΧΑΡΑΛΑΜΠΟΣ

ΑΜ 235890(ΠΑΛΙΟ)

ΑΜ 1041601(ΝΕΟ)

ΕΤΟΣ 8^{Ο}

ΜΕΡΟΣ Α

1. Η εντολή nslookup www.ceid.upatras.gr μας δινει :

```
C:\Users\bsiam>nslookup www.ceid.upatras.gr
Server:  UnKnown
Address:  192.168.1.254

Non-authoritative answer:
Name:    web.ceid.upatras.gr
Address:  150.140.141.173
Aliases:  www.ceid.upatras.gr
```

2. Η εντολή ipconfig /all μας δίνει :

```
C:\Users\bsiam>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-MODHMJEV
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : Home

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-15
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::315b:ec5a:44e8:a381%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 671744039
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F8-8C-C2-80-C5-F2-F2-7E-2D
   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 Τοπική σύνδεση* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : 82-C5-F2-F2-7E-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

```
Wireless LAN adapter Τοπική σύνδεση* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : 82-C5-F2-F2-7E-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Τοπική σύνδεση* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : 92-C5-F2-F2-7E-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
   Description . . . . . . . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
   Physical Address. . . . . . . . . : 80-C5-F2-F2-7E-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b5a9:4c49:e620:1e1e%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Πέμπτη, 6 Μαΐου 2021 4:00:08 μμ
   Lease Expires . . . . . . . . . . : Παρασκευή, 7 Μαΐου 2021 8:08:18 μμ
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 192988658
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F8-8C-C2-80-C5-F2-F2-7E-2D
   DNS Servers . . . . . . . . . . . : 192.168.1.254
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\bsiam>
```

3. Η εντολή ipconfig /displaydns δίνει :

```
C:\Users\bsiam>ipconfig /displaydns

Windows IP Configuration

    nexusrules.officeapps.live.com
    ----------------------------------------
    Record Name . . . . . : nexusrules.officeapps.live.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 72
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : prod.nexusrules.live.com.akadns.net


    Record Name . . . . . : prod.nexusrules.live.com.akadns.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 72
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 52.109.8.20


    Record Name . . . . . : a11-129.akadns.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 72
    Data Length . . . . . : 4
    Section . . . . . . . : Additional
    A (Host) Record . . . : 84.53.139.129


    Record Name . . . . . : a1-128.akadns.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 72
    Data Length . . . . . : 4
    Section . . . . . . . : Additional
    A (Host) Record . . . : 193.108.88.128


    Record Name . . . . . : a7-131.akadns.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 72
    Data Length . . . . . : 4
    Section . . . . . . . : Additional
    A (Host) Record . . . : 23.61.199.131
```

```
Record Name . . . . . : a9-128.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 72
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 184.85.248.128


Record Name . . . . . : a13-130.akagtm.org
Record Type . . . . . : 1
Time To Live  . . . . : 72
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 2.22.230.130


Record Name . . . . . : a28-129.akagtm.org
Record Type . . . . . : 1
Time To Live  . . . . : 72
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 95.100.173.129


Record Name . . . . . : a3-129.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 72
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 96.7.49.129


Record Name . . . . . : a18-128.akagtm.org
Record Type . . . . . : 1
Time To Live  . . . . : 72
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 95.101.36.128


Record Name . . . . . : a12-131.akagtm.org
Record Type . . . . . : 1
Time To Live  . . . . : 72
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 184.26.160.131
```

```
Record Name . . . . . : a5-130.akagtm.org
Record Type . . . . . : 1
Time To Live  . . . . : 72
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 95.100.168.130


1.0.0.127.in-addr.arpa
--------------------------------------
Record Name . . . . . : 1.0.0.127.in-addr.arpa.
Record Type . . . . . : 12
Time To Live  . . . . : 587909
Data Length . . . . . : 8
Section . . . . . . . : Answer
PTR Record  . . . . . : localhost


azwcus1-client-s.gateway.messenger.live.com
----------------------------------------
Record Name . . . . . : azwcus1-client-s.gateway.messenger.live.com
Record Type . . . . . : 5
Time To Live  . . . . : 211
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : azwcus1-client-s.msnmessenger.msn.com.akadns.net


Record Name . . . . . : azwcus1-client-s.msnmessenger.msn.com.akadns.net
Record Type . . . . . : 5
Time To Live  . . . . : 211
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : ip.azwcus1-client-s.msnmessenger.msn.com.akadns.net


Record Name . . . . . : ip.azwcus1-client-s.msnmessenger.msn.com.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 52.159.49.199


Record Name . . . . . : a11-129.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . . . : Additional
```

```
Record Name . . . . . : a11-129.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 84.53.139.129


Record Name . . . . . : a1-128.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 193.108.88.128


Record Name . . . . . : a7-131.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 23.61.199.131


Record Name . . . . . : a9-128.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 184.85.248.128


Record Name . . . . . : a13-130.akagtm.org
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 2.22.230.130


Record Name . . . . . : a28-129.akagtm.org
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 95.100.173.129
```

```
Record Name . . . . . : a3-129.akadns.net
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 96.7.49.129


Record Name . . . . . : a18-128.akagtm.org
Record Type . . . . . : 1
Time To Live  . . . . : 211
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 95.101.36.128


1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
----------------------------------------
Record Name . . . . . : 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa.
Record Type . . . . . : 12
Time To Live  . . . . : 587907
Data Length . . . . . : 8
Section . . . . . . . : Answer
PTR Record  . . . . . : localhost


graph.instagram.com
----------------------------------------
Record Name . . . . . : graph.instagram.com
Record Type . . . . . : 5
Time To Live  . . . . : 19
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : instagram.c10r.facebook.com


Record Name . . . . . : instagram.c10r.facebook.com
Record Type . . . . . : 1
Time To Live  . . . . : 19
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 157.240.9.52


Record Name . . . . . : a.ns.c10r.facebook.com
Record Type . . . . . : 1
Time To Live  . . . . : 19
Data Length . . . . . : 4
Section . . . . . . . : Additional
```

```
Record Name . . . . . : a.ns.c10r.facebook.com
Record Type . . . . . : 1
Time To Live  . . . . : 19
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 129.134.30.11


Record Name . . . . . : c.ns.c10r.facebook.com
Record Type . . . . . : 1
Time To Live  . . . . : 19
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 185.89.218.11


Record Name . . . . . : b.ns.c10r.facebook.com
Record Type . . . . . : 1
Time To Live  . . . . : 19
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 129.134.31.11


Record Name . . . . . : d.ns.c10r.facebook.com
Record Type . . . . . : 1
Time To Live  . . . . : 19
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 185.89.219.11


Record Name . . . . . : a.ns.c10r.facebook.com
Record Type . . . . . : 28
Time To Live  . . . . : 19
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2a03:2880:f0fc:b:face:b00c:0:99


Record Name . . . . . : c.ns.c10r.facebook.com
Record Type . . . . . : 28
Time To Live  . . . . : 19
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2a03:2880:f1fc:b:face:b00c:0:99
```

```
Record Name . . . . . : c.ns.c10r.facebook.com
Record Type . . . . . : 28
Time To Live  . . . . : 19
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2a03:2880:f1fc:b:face:b00c:0:99


Record Name . . . . . : b.ns.c10r.facebook.com
Record Type . . . . . : 28
Time To Live  . . . . : 19
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2a03:2880:f0fd:b:face:b00c:0:99


Record Name . . . . . : d.ns.c10r.facebook.com
Record Type . . . . . : 28
Time To Live  . . . . : 19
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2a03:2880:f1fd:b:face:b00c:0:99


ocsp.digicert.com
----------------------------------------
Record Name . . . . . : ocsp.digicert.com
Record Type . . . . . : 5
Time To Live  . . . . : 210
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : cs9.wac.phicdn.net


Record Name . . . . . : cs9.wac.phicdn.net
Record Type . . . . . : 1
Time To Live  . . . . : 210
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 93.184.220.29


autodiscover.upatrasgr.onmicrosoft.com
----------------------------------------
Record Name . . . . . : autodiscover.upatrasgr.onmicrosoft.com
Record Type . . . . . : 5
Time To Live  . . . . : 7
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : autodiscover.outlook.com
```

```
autodiscover.upatrasgr.onmicrosoft.com
----------------------------------------
Record Name . . . . . : autodiscover.upatrasgr.onmicrosoft.com
Record Type . . . . . : 5
Time To Live  . . . . : 7
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : autodiscover.outlook.com


Record Name . . . . . : autodiscover.outlook.com
Record Type . . . . . : 5
Time To Live  . . . . : 7
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : autod.ha-autod.office.com


Record Name . . . . . : autod.ha-autod.office.com
Record Type . . . . . : 5
Time To Live  . . . . : 7
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : autod.ms-acdc-autod.office.com


Record Name . . . . . : autod.ms-acdc-autod.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 40.101.54.168


Record Name . . . . . : autod.ms-acdc-autod.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 52.97.128.184


Record Name . . . . . : autod.ms-acdc-autod.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 40.101.55.136
```

```
Record Name . . . . . : autod.ms-acdc-autod.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.101.55.136


Record Name . . . . . : autod.ms-acdc-autod.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.101.55.120


Record Name . . . . . : ns4-ms-acdc.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 150.171.0.2


Record Name . . . . . : ns3-ms-acdc.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 150.171.254.2


Record Name . . . . . : ns2-ms-acdc.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 208.84.4.2


Record Name . . . . . : ns1-ms-acdc.office.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 13.107.244.2
```

```
imap.upnet.gr
----------------------------------------
Record Name . . . . . : imap.upnet.gr
Record Type . . . . . : 5
Time To Live  . . . . : 45847
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . . : xdov1.upnet.gr


Record Name . . . . . : xdov1.upnet.gr
Record Type . . . . . : 1
Time To Live  . . . . : 45847
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 150.140.129.54


Record Name . . . . . : nic.upatras.gr
Record Type . . . . . : 1
Time To Live  . . . . : 45847
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 150.140.129.30


localhost
----------------------------------------
Record Name . . . . . : localhost
Record Type . . . . . : 1
Time To Live  . . . . : 1200
Data Length . . . . . : 4
Section . . . . . : Question
A (Host) Record . . . : 127.0.0.1


localhost
----------------------------------------
Record Name . . . . . : localhost
Record Type . . . . . : 28
Time To Live  . . . . : 1200
Data Length . . . . . : 16
Section . . . . . : Question
AAAA Record . . . . . : ::1
```

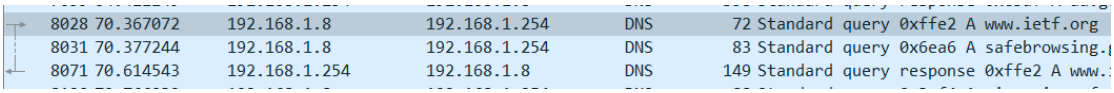
```
localhost
---------------------------------------
Record Name . . . . . : localhost
Record Type . . . . . : 28
Time To Live  . . . . : 1200
Data Length . . . . . : 16
Section . . . . . : Question
AAAA Record . . . . . : ::1


clients4.google.com
---------------------------------------
Record Name . . . . . : clients4.google.com
Record Type . . . . . : 5
Time To Live  . . . . : 4
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record  . . . . : clients.l.google.com


Record Name . . . . . : clients.l.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 4
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 216.58.212.46


Record Name . . . . . : ns4.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 4
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 216.239.38.10


Record Name . . . . . : ns3.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 4
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . : 216.239.36.10


Record Name . . . . . : ns1.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 4
Data Length . . . . . : 4
Section . . . . . : Additional
```

```
Record Name . . . . . : ns1.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 4
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 216.239.32.10


Record Name . . . . . : ns2.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 4
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 216.239.34.10


Record Name . . . . . : ns4.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 4
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2001:4860:4802:38::a


Record Name . . . . . : ns3.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 4
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2001:4860:4802:36::a


Record Name . . . . . : ns1.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 4
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2001:4860:4802:32::a


Record Name . . . . . : ns2.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 4
Data Length . . . . . : 16
Section . . . . . . . : Additional
AAAA Record . . . . . : 2001:4860:4802:34::a
```

4.

```
C:\Users\bsiam>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\bsiam>
```

1)



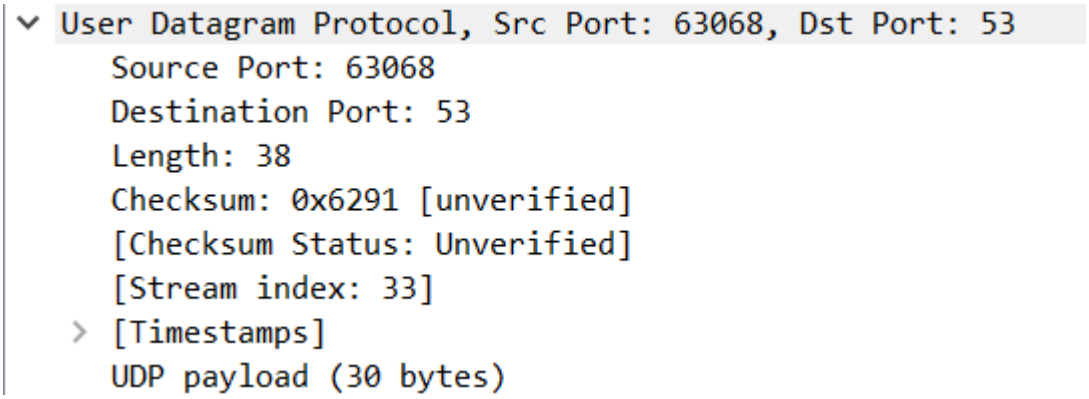
8028	70.367072	192.168.1.8	192.168.1.254	DNS	72	Standard query 0xffe2 A www.ietf.org
8031	70.377244	192.168.1.8	192.168.1.254	DNS	83	Standard query 0x6ea6 A safebrowsing.
8071	70.614543	192.168.1.254	192.168.1.8	DNS	149	Standard query response 0xffe2 A www.

2)

<u>DNS Request Μηνύματος</u>

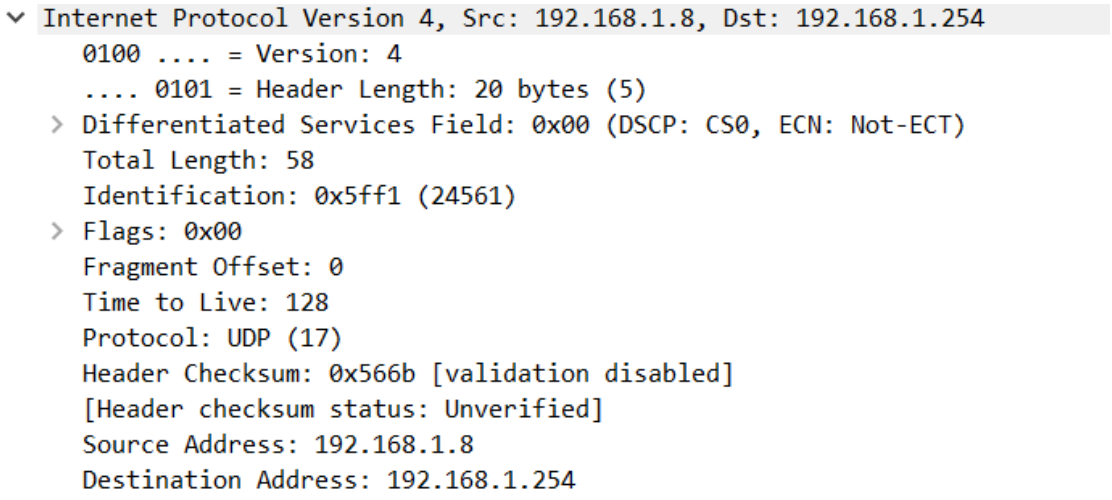
```
> Frame 8028: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{9365C723-F9A6-4AED-8AB4-786A9C9BE7C8}, id 0
> Ethernet II, Src: AzureWav_f2:7e:2d (80:c5:f2:f2:7e:2d), Dst: Tp-LinkT_e6:8c:20 (c4:71:54:e6:8c:20)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 192.168.1.254
> User Datagram Protocol, Src Port: 63068, Dst Port: 53
> Domain Name System (query)
```

Χρησιμοποιήθηκε το πρωτόκολλο **<u>UDP(User Datagram Protocol)</u>** όπως φαίνεται στο προηγούμενο screenshot



Βλέπουμε ότι το port του αποστολέα (Src Port) είναι το **63068** και το port του παραλήπτη (Dst Port) είναι το **53**

Παρατηρούμε επίσης ότι το μέγεθος UDP πακέτου 38 bytes



Παρατηρούμε ότι η IP του αποστολέα (Src) είναι η **192.168.1.8** και η IP του παραλήπτη (Dst) είναι το **192.168.1.254**

Το Time to Live είναι 128

Παρατηρούμε επίσης ότι το μέγεθος UDP πακέτου 38 bytes

Domain Name System (query):

```
Domain Name System (query)
    Transaction ID: 0xffe2
    Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 8071]
```

Στο πεδίο Questions έχουμε την τιμή 1 που δείχνει ότι έχουμε να κάνουμε με ερώτημα DNS

Στο Queries φαίνεται το εκάστοτε url για το οποίο θέλουμε την IP του

Στο Response In: 8071 φαίνεται ο αριθμός του πακέτου απάντησης

Η κεφαλίδα DNS ξεκινά με ένα Transaction ID

```
Transaction ID: 0xffe2
```

Μετά έχουμε το πεδίο των flags :

Το πρώτο flag μας δείχνει αν το DNS πακέτο είναι query η response και όπως βλέπουμε :

```
0... .... .... .... = Response: Message is a query
```

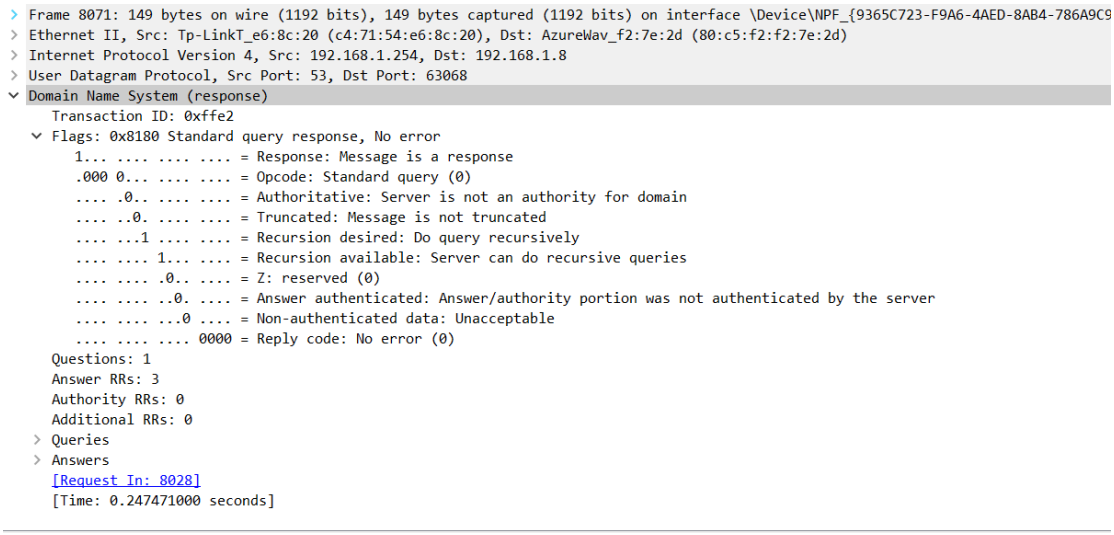
Είναι το πεδίο Questions με τιμή 1

Είναι το πεδίο Answer RRs με τιμή 0

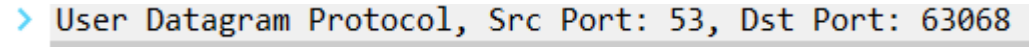
Είναι το πεδίο Authority RRs με τιμή 0

Και τέλος όπως βλέπουμε το πεδίο Additional RRs με τιμή 0

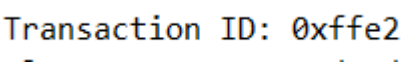
DNS Response Μηνύματος



Το μήνυμα προκύπτει από το port 53 του server dns

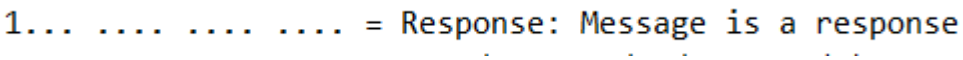


Η κεφαλίδα DNS ξεκινά με ένα Transaction ID ίδιο με το Transaction ID του DNS Request



Μετά έχουμε τα flags :

Το πρώτο flag δείχνει ότι το DNS είναι response :



Το πεδίο Questions με τιμή 1

Το πεδίο Answer RRs με τιμή 3

Το πεδίο Authority RRs με τιμή 0

Το πεδίο Additional RRs με την τιμή 0

Μετά ακολουθεί το πεδίο Queries :

```
Queries
    www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Στη συνέχεια το πεδίο Answer :

```
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 104.16.44.99
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
```

Και θα καταλήξουμε με το πεδίο Requests in :

```
[Request In: 8028]
[Time: 0.247471000 seconds]
```

3) Η θύρα προορισμού του μηνύματος απόκρισης DNS είναι :

```
User Datagram Protocol, Src Port: 63068, Dst Port: 53
    Source Port: 63068
    Destination Port: 53
    Length: 38
    Checksum: 0x6291 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 33]
    [Timestamps]
    UDP payload (30 bytes)
```

Το Dst Port για το μήνυμα ερώτησης είναι το 53

4) Η θύρα προέλευσης του μηνύματος απόκρισης DNS είναι :

```
User Datagram Protocol, Src Port: 53, Dst Port: 63068
    Source Port: 53
    Destination Port: 63068
    Length: 115
    Checksum: 0x07e6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 33]
  > [Timestamps]
    UDP payload (107 bytes)
```

Το Dst Port για το μήνυμα ερώτησης DNS είναι το port 53

5)

```
8028 70.367072     192.168.1.8          192.168.1.254
```

Και εκτελώντας και την εντολή ipconfig/all :

```
DNS Servers . . . . . . . . . . . : 192.168.1.254
```

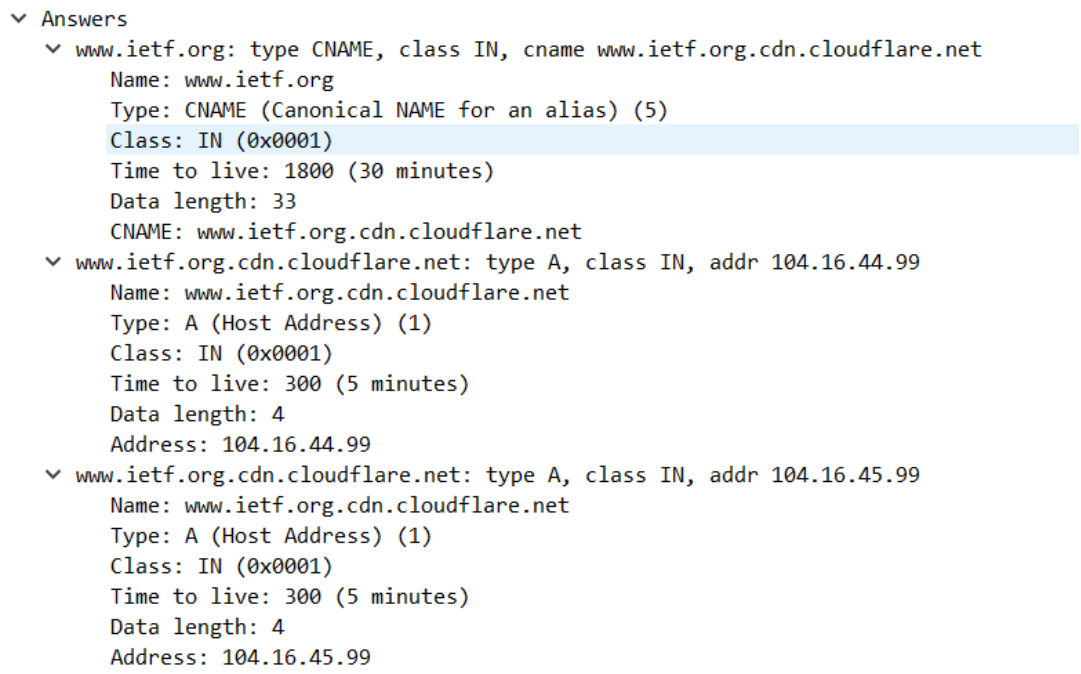
Βλέπουμε ότι και 2 τρέχουσες διευθύνσεις IP είναι ίδιες

6)

```
Queries
  www.ietf.org: type A, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 8071]
```

το ερώτημα είναι ένα type Ακαι δεν περιέχει καμία απολύτως απάντηση

7)



3 απαντήσεις από 3 διαφορετικούς DNS server Οι απαντήσεις περιέχουν:

Name: www.ietf.org

Type: CNAME

Time to Live: 1800

Data length : 33

Address : 104.16.44.99

8)

```
▾ Answers
  ▾ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
```

Στη πορεία δίνουμε στο wireshark την εντολή tcp.flags.syn==1&&tcp.flags.ack==0

4022	49.126921	192.168.1.8	216.58.206.196	TCP	66 53420 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4079	49.388113	192.168.1.8	68.232.34.200	TCP	66 53421 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4121	49.615690	192.168.1.8	142.250.184.142	TCP	66 53422 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4335	50.625773	192.168.1.8	172.217.169.174	TCP	66 53423 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4351	50.705838	192.168.1.8	185.26.182.111	TCP	66 53424 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4875	53.930231	192.168.1.8	52.159.49.199	TCP	66 53425 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5006	54.959372	192.168.1.8	108.177.15.113	TCP	66 53426 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5111	55.690356	192.168.1.8	185.26.182.111	TCP	66 53427 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5193	56.270488	192.168.1.8	216.58.214.141	TCP	66 53428 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5531	59.179746	192.168.1.8	216.58.206.196	TCP	66 53429 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5745	60.684238	192.168.1.8	185.26.182.111	TCP	66 53430 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5811	61.067684	192.168.1.8	172.217.169.206	TCP	66 53431 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5960	61.895155	192.168.1.8	216.58.206.196	TCP	66 53432 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5968	61.942443	192.168.1.8	172.217.169.131	TCP	66 53433 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6021	62.133464	192.168.1.8	216.58.212.42	TCP	66 53434 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6177	62.560008	192.168.1.8	69.94.67.71	TCP	66 53435 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6542	63.123467	192.168.1.8	172.217.17.193	TCP	66 53436 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6658	63.389821	192.168.1.8	69.94.67.71	TCP	66 53437 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6835	63.848415	192.168.1.8	172.217.17.202	TCP	66 53442 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7043	64.305420	192.168.1.8	172.217.169.174	TCP	66 53443 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7062	64.418168	192.168.1.8	172.217.169.110	TCP	66 53444 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7276	65.698150	192.168.1.8	185.26.182.111	TCP	66 53445 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8072	70.618564	192.168.1.8	104.16.44.99	TCP	66 53446 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8074	70.620691	192.168.1.8	104.16.44.99	TCP	66 53447 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8076	70.623770	192.168.1.8	104.16.44.99	TCP	66 53448 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8078	70.638719	192.168.1.8	104.16.44.99	TCP	66 53449 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8101	70.711293	192.168.1.8	185.26.182.111	TCP	66 53450 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8146	70.832972	192.168.1.8	52.205.144.169	TCP	66 53454 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8204	71.017376	192.168.1.8	52.205.144.169	TCP	66 53455 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8310	71.446434	192.168.1.8	142.250.187.110	TCP	66 53456 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8485	72.439222	192.168.1.8	69.94.67.71	TCP	66 53457 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8550	72.565794	192.168.1.8	172.217.169.206	TCP	66 53458 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8714	73.182837	192.168.1.8	216.58.212.42	TCP	66 53461 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8749	73.444464	192.168.1.8	4.31.198.44	TCP	66 53462 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8951	73.671848	192.168.1.8	4.31.198.44	TCP	66 53463 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9919	75.702641	192.168.1.8	185.26.182.111	TCP	66 53464 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10749	80.700358	192.168.1.8	185.26.182.111	TCP	66 53465 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

2239	26.169656	192.168.1.8	192.168.1.254	DNS	79 Standard query 0x62d7 A www.ceid.upatras.gr
2242	26.170888	192.168.1.8	192.168.1.254	DNS	79 Standard query 0x0450 A maps.googleapis.com
2243	26.172280	192.168.1.254	192.168.1.8	DNS	95 Standard query response 0x62d7 A www.ceid.upatras.gr A 150.140.141.173

```
C:\Users\bsiam>nslookup www.ceid.upatras.gr
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.254

DNS request timed out.
    timeout was 2 seconds.
Name:    www.ceid.upatras.gr
Address:  150.140.141.173
```

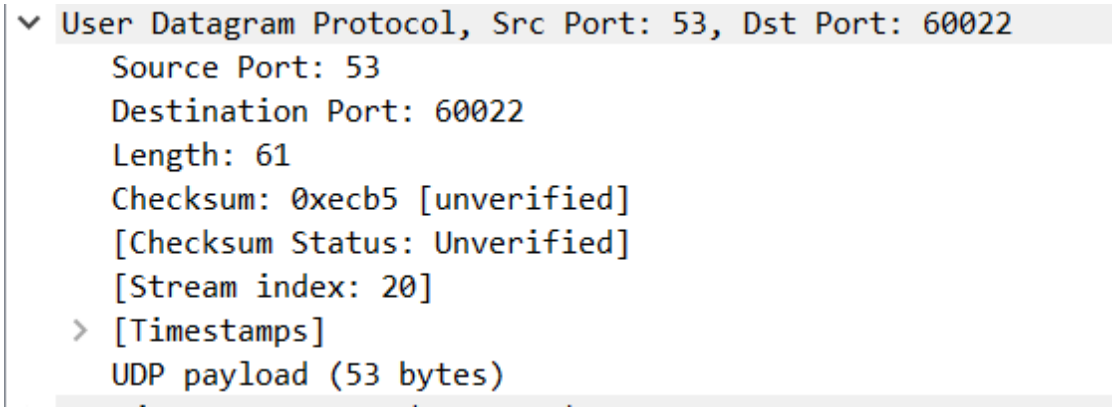
9)

Μήνυμα ερώτησης (request Message)

```
User Datagram Protocol, Src Port: 60022, Dst Port: 53
    Source Port: 60022
    Destination Port: 53
    Length: 45
    Checksum: 0xbe3b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 20]
  > [Timestamps]
    UDP payload (37 bytes)
```

Όπως βλέπουμε από το screenshot η Dst port για το μήνυμα ερώτησης DNS είναι η 53

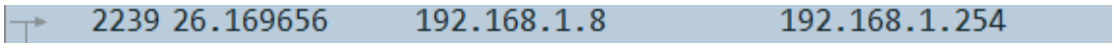
Μήνυμα Απόκρισης (Response Message)



Από το screenshot βλέπουμε πως η Dst Port του μηνύματος απόκρισης DNS είναι η 53

10)

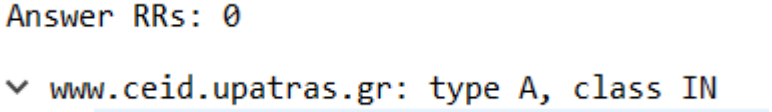
IP το μηνύματος ερώτησης DNS :



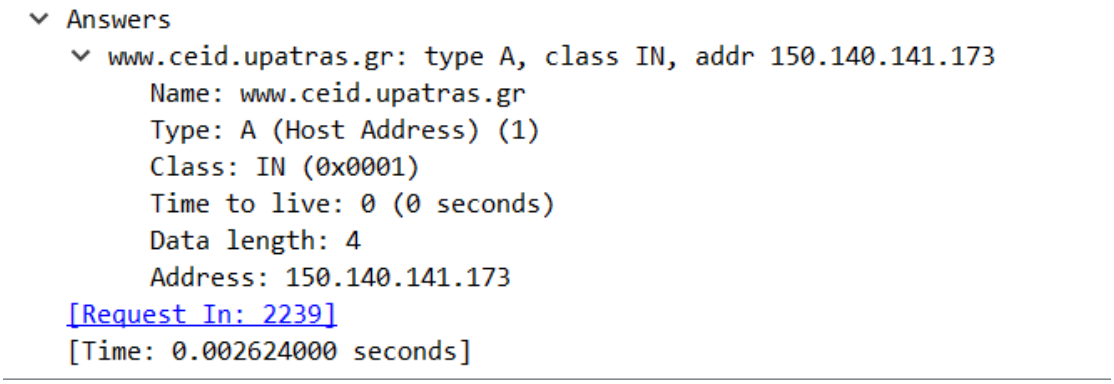
IP του τοπικού διακομιστή DNS :

11)

Το μήνυμα ερώτησης DNS είναι type A και δεν περιέχει καθόλου απαντήσεις



12)



Name: www.ceid.upatras.gr

Type: A

Time to Live : 0

Data length : 4

Address: 150.140.141.173

13)

Recursive resolver

Το Recursive DNS είναι μεταξύ του καταναλωτή και των εξουσιοδοτημένων διακομιστών DNS που φιλοξενούν τομείς μιας εταιρείας και των IP addresses που σχετίζονται με ένα όνομα τομέα και έχει φτιαχτεί για να παίρνει ερωτήματα DNS και είναι το πρώτο βήμα σε ένα ερώτημα DNS. Το recursive DNS κάνει δύο σημαντικές εργασίες:

Όταν ένας χρήστης πληκτρολογεί μια URL στο πρόγραμμα περιήγησής, η διεύθυνση URL στέλνεται πρώτα στον αναδρομικό διακομιστή DNS. Το πρώτο μέλημα του αναδρομικού διακομιστή DNS είναι να κάνει έλεγχο της κρυφής μνήμης για να δει αν η διεύθυνση IP για το τρέχον URL είναι ήδη αποθηκευμένη μέσα σε αυτή . Εάν οι πληροφορίες για τις ζητούμενες διεύθυνσης IP είναι ήδη στη μνήμη, τότε ο αναδρομικός διακομιστής DNS θα δώσει αμέσως τη διεύθυνση IP στο πρόγραμμα περιήγησης και ο χρήστης θα μεταφερθεί στον ιστιότοπο της επιθυμίας του .

Εάν ο αναδρομικός διακομιστής DNS δεν έχει τη ζητούμενη διεύθυνση IP στη κρυφή μνήμη, θα προσπαθήσει να ανακτήσει την διεύθυνση IP και θα την επιστρέψει στον εκάστοτε χρήστη. Ο αναδρομικός διακομιστής DNS θα αποθηκεύσει στη συνέχεια

αυτή τη διεύθυνση IP στη κρυφή μνήμη για ένα συγκεκριμένο χρονικό διάστημα το οποίο καθορίζεται από το "Time To Live" (TTL).

Οι αναδρομικοί διακομιστές DNS είναι γνωστοί και ως δημόσιοι διακομιστές και ένα γνωστό παράδειγμα ενός τέτοιου είδους διακομιστή είναι ο 8.8.8.8 της γνωστής σε όλους μας Google

Μια κύρια διαφορά μεταξύ των Recursive resolvers και authoritative name servers είναι ότι οι πρώτοι επιστρέφουν απαντήσεις για όλα τα ερωτήματα που φθάνουν σε αυτούς.

Root nameserver

Ο διακομιστής root name είναι ένας διακομιστής ονόματος στη ρίζα του συστήματος DNS του Διαδικτύου. Απαντά άμεσα αιτήματα forecords στη root zone και απαντά σε άλλα αιτήματα επιστρέφοντας μια λίστα με τους έγκυρους διακομιστές ονομάτων για τον TLD . Οι διακομιστές root name είναι ένα κρίσιμο μέρος της δομής του Διαδικτύου, επειδή είναι το πρώτο βήμα στη μετάφραση ορατών αναγνώσιμων από τον άνθρωπο διευθύνσεων IP που χρησιμοποιούνται στην επικοινωνία μεταξύ των συνδεμένων υπολογιστών του Διαδικτύου.

Ένας συνδυασμός ορίων στο DNS και συγκεκριμένων πρωτοκόλλων όπως του User Datagram Protocol (UDP), οδήγησε σε μια απόφαση να περιοριστεί ο αριθμός των rootservers σε δεκατρείς διευθύνσεις διακομιστή.

TLD nameserver

Ένας TLD nameserver κρατάει τις πληροφορίες για όλα τα ονόματα που έχουν την ίδια επέκταση , όπως .gr, .com και πολλά άλλα Έτσι ένας διακομιστής TLD. gr περιέχει πληροφορίες για κάθε όνομα τομέα που τελειώνει με το ".gr" .

Εάν ένας user του ιστού ψάξει έναν αναλυτή για το instagram.com, αφού πρώτα λάβει μια απάντηση από έναν root nameserver, ο αναδρομικός αναλυτής DNS θα στείλει μια ερώτηση σε ένα nameserver TLD .com ο οποίος προφανώς θα απαντήσει δίνοντας πληροφορίες με τον σωστό nameserver για τον εκάστοτε τομέα.

Authoritative nameserver

Ο εξουσιοδοτημένος διακομιστής ονομάτων είναι συνήθως το τελευταίο βήμα στο ταξίδι μιας διεύθυνσης IP και παρέχει πολύ συγκεκριμένες πληροφορίες για το όνομα του τομέα που εξυπηρετεί η συγκεκριμένη διεύθυνση και επίσης μπορεί να παρέχει μια αναδρομική λύση με την IP διεύθυνση του διακομιστή που είναι τοποθετημένος στην εγγραφή DNS.

14)

Τα dns πακέτα έχουν σαν πρώτο πεδίο :

id

Το ID είναι ένα αναγνωριστικό των 16 bit που εκχωρείται από το πρόγραμμα που δημιουργεί οποιοδήποτε είδος ερωτήματος.

Το ακόλουθο επίπεδο είναι για τα flags με αυτή τη σειρά:

QR:1	OPCODE:0	AA:0	TC:0	RD:0	RA:0	Z	AD:0	CD:0	RCODE:0

- **Bit 1 QR** : Όταν το bit=0 το message είναι query Όταν το bit=1 το message είναι response
- **Bits 2-5 Opcode :** Η τιμή 0 σημαίνει normal query, η τιμή 1 σημαίνει reverse query και η τιμή 2 δείχνει το server status
- **Bit 6 AA**
- **Bit 7 TC**: Ενεργοποιείται όταν μόνο το πακέτο είναι μεγαλύτερο απο το μέγιστο μέγεθος των 512 bytes.
- **Bit 8 RD** : Αν είναι 0 τοτε έχουμε iterative query. Αν είναι 1 τοτε recursive query
- **Bit 9 RA** : Γίνεται response όταν ο server δέχεται recursion
- **Bit 10 Z : Πρέπει να είναι 0**
- **Bit 11 AD**: Σε πολύ παλίες μηχανές θεωρείται μέρος του Z
- **Bit 12: CD :** Χρησιμοποιείται στο DNSSEC και Θεωρείται και αυτό μέρος του Z σε παλαιότερες μηχανές.
- **Bit 13-16 RCODE** : Είναι σε γενικές γραμμές 0

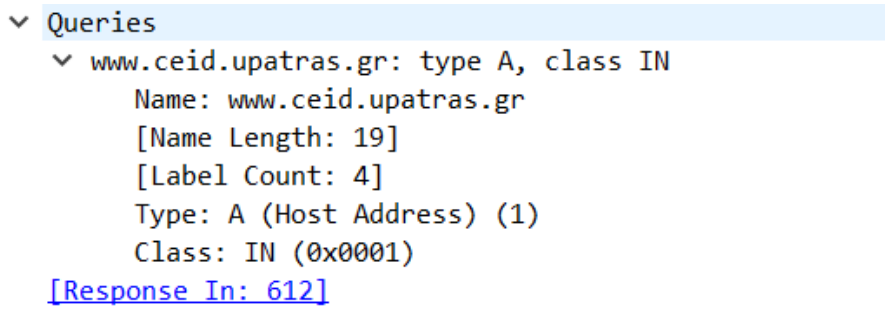
Τα υπόλοιπα τέσσερα πεδία του header είναι ο αριθμός ερωτήσεων , οι εγγραφές απαντήσεων , οι εγγραφές authority και οι πρόσθετες εγγραφές πόρων.

Number of Questions
Number of Answers RRs
Number of Authority RRs
Number of Additional RRs

Με τη χρήση το wareshark θα δείξουμε πιο πρακτικά αυτά τα πεδία απλά αναλύωντας ένα dns πακέτο αφού πιο πριν ανοίξαμε το site www.ceid.upatras.gr :

ΕΡΩΤΗΣΗ (QUESTION)

Η ερώτηση υπάρχει τόσο στο query όσο και στο response μήνυμα. Ορισμένα εργαλεία όπως το Wareshark που χρησιμοποιήσαμε στη παρούσα εργασία το αποκαλεί **Queries** :



Η ερώτηση αποτελείται από 3 μέρη :

- Από το **Name** το οποίο είναι ένα όνομα κεντρικού υπολογιστή όπως www.ceid.upatras.gr
- Από το **Type** το οποίο στο συγκεκριμένο παράδειγμα είναι **A**
- Από το **Class** το οποίο στο συγκεκριμένο είναι **IN**

Το Type του ερωτήματος διαχωρίζεται σε :

- **A, IPv4 address**
- **AAAA, Quad-A, IPv6 address record**
- **NS, Name Server record**

ΕΓΓΡΑΦΕΣ ΑΠΑΝΤΗΣΗΣ (ANSWER)

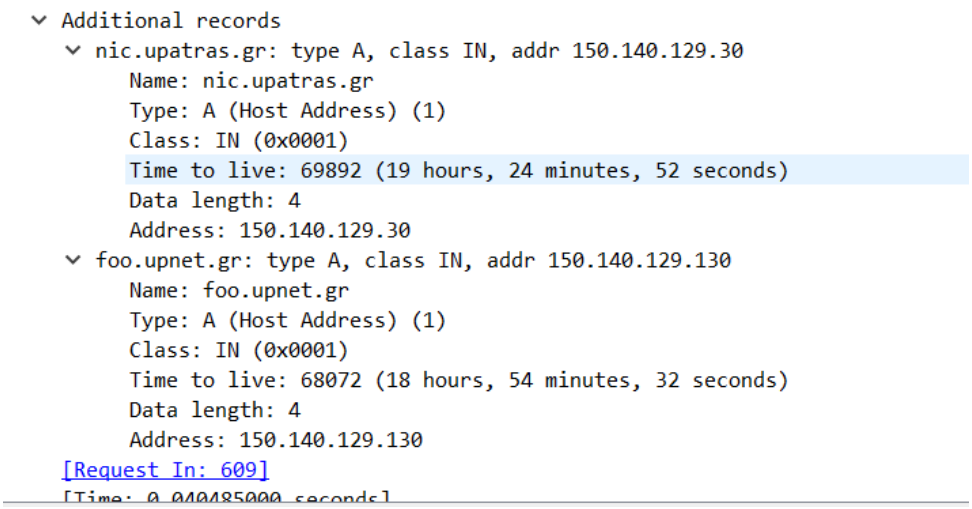
```
Answers
  www.ceid.upatras.gr: type CNAME, class IN, cname web.ceid.upatras.gr
      Name: www.ceid.upatras.gr
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 32542 (9 hours, 2 minutes, 22 seconds)
      Data length: 6
      CNAME: web.ceid.upatras.gr
  web.ceid.upatras.gr: type A, class IN, addr 150.140.141.173
      Name: web.ceid.upatras.gr
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 8152 (2 hours, 15 minutes, 52 seconds)
      Data length: 4
      Address: 150.140.141.173
```

ΕΓΓΡΑΦΕΣ ΠΟΡΩΝ ΑΡΧΗΣ(AUTHORITY)

```
Authoritative nameservers
  ceid.upatras.gr: type NS, class IN, ns FOO.upnet.gr
      Name: ceid.upatras.gr
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 6304 (1 hour, 45 minutes, 4 seconds)
      Data length: 12
      Name Server: FOO.upnet.gr
  ceid.upatras.gr: type NS, class IN, ns NIC.upatras.gr
      Name: ceid.upatras.gr
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 6304 (1 hour, 45 minutes, 4 seconds)
      Data length: 6
      Name Server: NIC.upatras.gr
```

Αυτά τα NS αρχεία είναι διαφορετικά από τα αρχεία A καθώς έχουν ένα ονομα τομέα και στα δύο πεδία RR name και RR. Σε αντίθεση με την answer section, η authority section μπορεί να έχει μονο αρχεία NS τα οποία σαφώς και μπορούν να σταλούν σε άλλα τμήματα

ADDITIONAL RECORDS



15)

Ethernet Header
IP Header
UDP Header
DNS Header

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
48	F8	B3	26	DF	49	BA	BA	BA	BA	BA	BA	08	00	45	00	00	38	66	BD

21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
00	00	80	11	02	0C	C0	A8	01	34	08	08	08	08	D5	39	00	35	00	24

41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
44	8F	00	03	01	00	00	01	00	00	00	00	00	00	06	67	6F	6F	67	6C

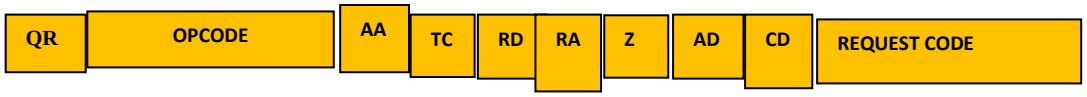
61	62	63	64	65	66	67	68	69	70
65	03	63	6F	6D	00	00	01	00	01

BYTES ΠΟΥ ΑΦΟΡΟΥΝ ΤΟ DNS HEADER

- Τα bytes **43-44** είναι το Transaction ID (Message ID) και έχουν περιεχόμενο 00 και 03
- Τα bytes **45-46** που έχουν περιεχόμενο 01 και 00 αντίστοιχα είναι τα flags του Header :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

flags



Δηλαδή :

QR : 0 , OPCODE : 0 , AA : 0 , TC : 0 , RD : 1 , RA : 0 , Z : 0 , AD : 0 , CD :0 και REQUEST CODE : 0

- Επομένως το DNS πακέτο είναι **Request πακέτο**
- Τα **47-48** με περιεχόμενα 00 και 01 αντίστοιχα είναι το πεδίο

Questions άρα στο μήνυμα υπάρχει μόνο 1 ερώτημα

- Τα **<u>49-50</u>** με περιεχόμενο 00 00 είναι το **Answer RRs** που είναι 0 διότι το μήνυμα είναι ερώτημα
- Τα **<u>51-52</u>** με περιεχόμενο 00 00 είναι το **Authority RRs** που είναι 0 διότι το μήνυμα είναι ερώτημα
- Τα **<u>53-54</u>** με περιεχόμενο 00 00 είναι το **Additional RRs** που είναι 0 διότι το μήνυμα είναι ερώτημα
- Τα **<u>55-70</u>** είναι το πεδίο **Queries** σε ένα DNS μήνυμα τύπου query

16)

Όπως με τον ίδιο τρόπο του προηγούμενου ερωτήματος

Ethernet Header
IP Header
UDP Header
DNS Header

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
BA	BA	BA	BA	BA	BA	48	F8	B3	26	DF	49	08	00	45	08	00	E8	B2	EF

21	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
00	00	37	11	FE	21	08	08	08	08	C0	A8	01	34	00	35	D5	39	00	D4

41	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**
28	A2	00	03	81	80	00	01	00	0B	00	00	00	00	06	67	6F	6F	67	6C

61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
65	03	63	6F	6D	00	00	00	01	00	01	C0	0C	00	01	00	01	00	00	04

81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	09	100
00	04	4A	7D	EC	23	C0	0C	00	01	00	01	00	00	00	04	00	04	4A	7D

101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
EC	25	C0	0C	00	01	00	01	00	00	00	04	00	04	4A	7D	EC	27	C0	0C

121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
00	01	00	01	00	00	00	04	00	04	4A	7D	EC	20	C0	0C	00	01	00	01

141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
00	00	00	04	00	04	4A	7D	EC	28	C0	0C	00	01	00	01	00	00	00	04

161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
00	04	4A	7D	EC	21	C0	0C	00	01	00	01	00	00	00	04	00	04	4A	7D

181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
EC	29	C0	0C	00	01	00	01	00	00	00	04	00	04	4A	7D	EC	22	C0	0C

201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
00	01	00	01	00	00	00	04	00	04	4A	7D	EC	24	C0	0C	00	01	00	01

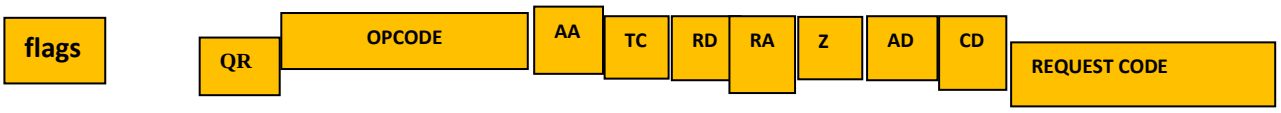
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
00	00	00	04	00	04	4A	7D	EC	2E	C0	0C	00	01	00	01	00	00	00	04

241	242	243	244	225	226
00	04	4A	7D	EC	26

ΒΥΤΕS ΠΟΥ ΑΦΟΡΟΥΝ ΤΟ DNS HEADER

- Τα bytes **43-44** είναι το Transaction ID (Message ID) και έχουν περιεχόμενο 00 και 03
- Τα bytes **45-46** που έχουν περιεχόμενο 81 και 80 αντίστοιχα είναι τα flags του Header :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0



Δηλαδή :

QR : 1 , OPCODE : 0 , AA : 0 , TC : 0 , RD : 0 , RA : 0 , Z : 0 , AD : 0 , CD :0 και REQUEST CODE : 0

- Επομένως το DNS πακέτο είναι **Request response(απόκρισης)**
- Τα **47-48** με περιεχόμενα 00 και 01 αντίστοιχα είναι το πεδίο **Questions** άρα στο μήνυμα υπάρχει μόνο 1 ερώτημα
- Τα **49-50** με περιεχόμενο 00 0B είναι το **Answer RRs** που λόγω δεκαδικής μορφής (11) δείχνει ότι έχει 11 απαντήσεις
- Τα **51-52** με περιεχόμενο 00 00 είναι το **Authority RRs** που είναι 0 διότι το μήνυμα δεν έχει authority RRs
- Τα **53-54** με περιεχόμενο 00 00 είναι το **Additional RRs** που είναι 0 διότι το μήνυμα που είναι απάντηση δεν περιλαμβάνει επιπλέον additional RRs

ΜΕΡΟΣ Β

1)

- Τα bytes **1-6** έχουντη Dst MAC Address του παραληπτη
- Τα bytes **7-12** έχουν τη Src MAC Address του εκάστοτε αποστολεα
- Τα bytes **13-14** έχουν τον τύπο πρωτοκόλλου κεφαλίδα IP
- Το byte **15** έχει το μέγεθος κεφαλίδας
- Τα bytes **17-18** έχουν το συνολικό μέγεθος του frame
- Το byte **23** έχει το TTL του frame
- Το byte **24** έχουν το πρωτόκολλο είναι TCP
- Τα bytes **25-26** έχουν το checksum
- Τα bytes **27-30** έχουν την IP διεύθυνση του αποστολέα
- Τα bytes **31-34** έχουν την IP διεύθυνση του παραλήπτη
- Τα bytes **35-36** έχουν την TCP θύρα αποστολέα
- Τα bytes **37-38** έχουν την TCP θύρα δέκτη
- Τα bytes **41-42** έχουν το checksum του μηνύματος

- Επομένως η IP διεύθυνσης αποστολής είναι τα bytes 27-30 με περιεχόμενο 81 6E 1E 1A ενώ της διεύθυνσης προορισμού είναι τα bytes 31-34 με περιεχόμενο 81 6E 02 11

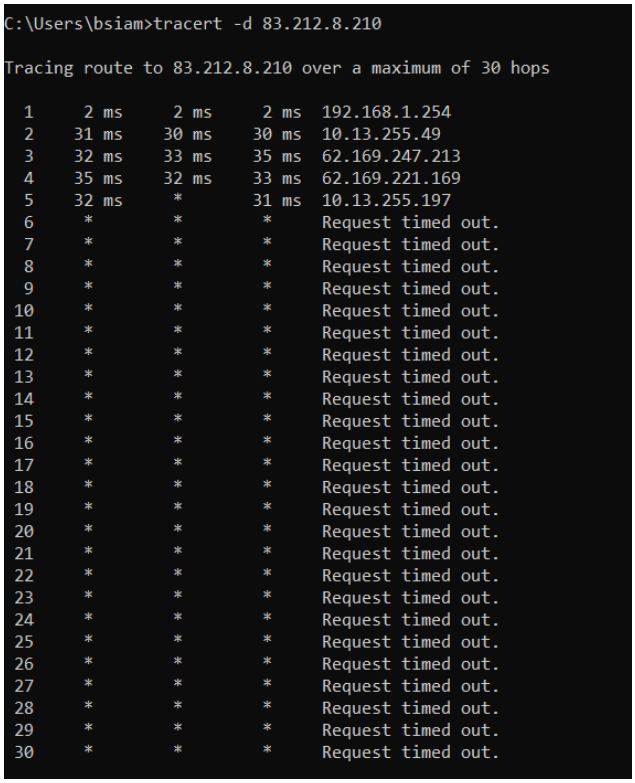
- Το μήκος του IP μέρους είναι τα bytes από 15-34

- Η TCP θύρα αποστολέα είναι τα bytes 35-36 με περιεχόμενο 02 03 ενώ η TCP θύρα παραλήπτη είναι τα bytes 37-38 με περιεχόμενο 00 50

- Η τιμή του Header Checksum είναι τα bytes 25-26 με περιεχόμενο 7D CB

2)

1. Στο cmd line θα εκτελέσουμε την tracert -d 83.212.8.210 και έχουμε :



2. Στο cmd line δίνουμε την εντολή ipconfig /all για να βρούμε τη MAC του υπολογιστή μου στο πλαίσιο Physical Address του πεδίου Wirelless Lan adapter Wi - Fi :

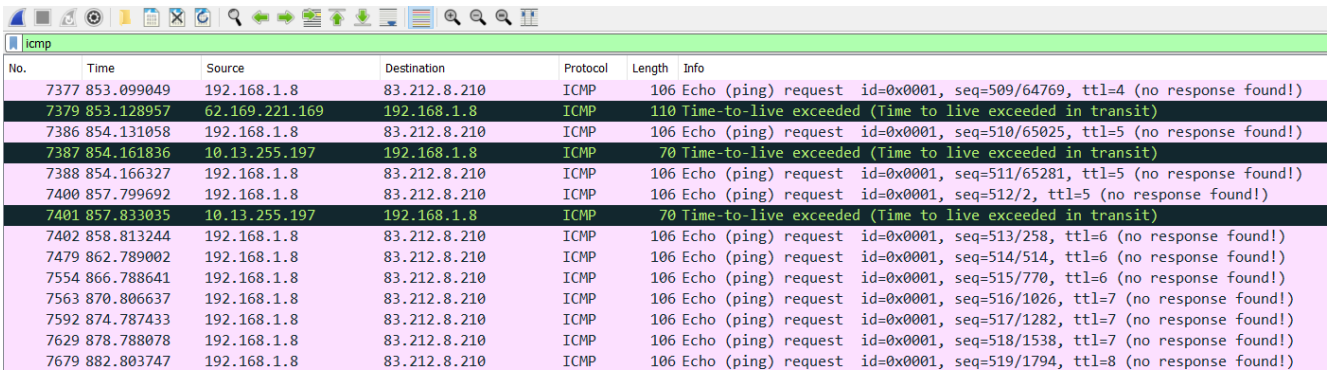
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
   Description . . . . . . . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
   Physical Address. . . . . . . . . : 80-C5-F2-F2-7E-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b5a9:4c49:e620:1e1e%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Παρασκευή, 7 Μαΐου 2021 2:15:38 πμ
   Lease Expires . . . . . . . . . . : Κυριακή, 9 Μαΐου 2021 3:00:10 μμ
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 192988658
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F8-8C-C2-80-C5-F2-F2-7E-2D
   DNS Servers . . . . . . . . . . . : 192.168.1.254
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Και συγκεκριμένα :

```
Physical Address. . . . . . . . . : 80-C5-F2-F2-7E-2D
```

3. Στο Wireshark γράφω το φίλτρο **eth.src == 80-C5-F2-F2-7E-2D** για να υπάρξει φιλτράρισμα των πλαισίων σε σχέση με την MAC του υπολογιστή

Δίνουμε την εντολή tracert -d 83.212.8.210 στο cmdline και ενώ η εντολή αυτή βρίσκεται σε εξέλιξη δίνουμε στο WireShark το φίλτρο **icmp** και έχουμε το εξής screenshot :



icmp

No.	Time	Source	Destination	Protocol	Length	Info
7377	853.099049	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=509/64769, ttl=4 (no response found!)
7379	853.128957	62.169.221.169	192.168.1.8	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
7386	854.131058	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=510/65025, ttl=5 (no response found!)
7387	854.161836	10.13.255.197	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7388	854.166327	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=511/65281, ttl=5 (no response found!)
7400	857.799692	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=512/2, ttl=5 (no response found!)
7401	857.833035	10.13.255.197	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7402	858.813244	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=513/258, ttl=6 (no response found!)
7479	862.789002	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=514/514, ttl=6 (no response found!)
7554	866.788641	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=515/770, ttl=6 (no response found!)
7563	870.806637	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=516/1026, ttl=7 (no response found!)
7592	874.787433	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=517/1282, ttl=7 (no response found!)
7629	878.788078	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=518/1538, ttl=7 (no response found!)
7679	882.803747	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=519/1794, ttl=8 (no response found!)

4.

Στη συνέχεια κλικάρουμε ένα ICMP type Echo request και βλέπουμε τις λεπτομέρειες του :

```
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 83.212.8.210
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xd112 (53522)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 6
    Protocol: ICMP (1)
    Header Checksum: 0xc538 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.8
    Destination Address: 83.212.8.210
> Internet Control Message Protocol
```

Η διεύθυνση IP του υπολογιστή μας είναι η 192.168.1.8. (Src) Η IP βρίσκεται στα πεδία 27,28,29,30 της επικεφαλίδας :

```
> Frame 7402: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interfa
> Ethernet II, Src: AzureWav_f2:7e:2d (80:c5:f2:f2:7e:2d), Dst: Tp-LinkT_e6:8c:20 (c
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 83.212.8.210
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xd112 (53522)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 6
    Protocol: ICMP (1)
    Header Checksum: 0xc538 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.8
    Destination Address: 83.212.8.210
> Internet Control Message Protocol
```

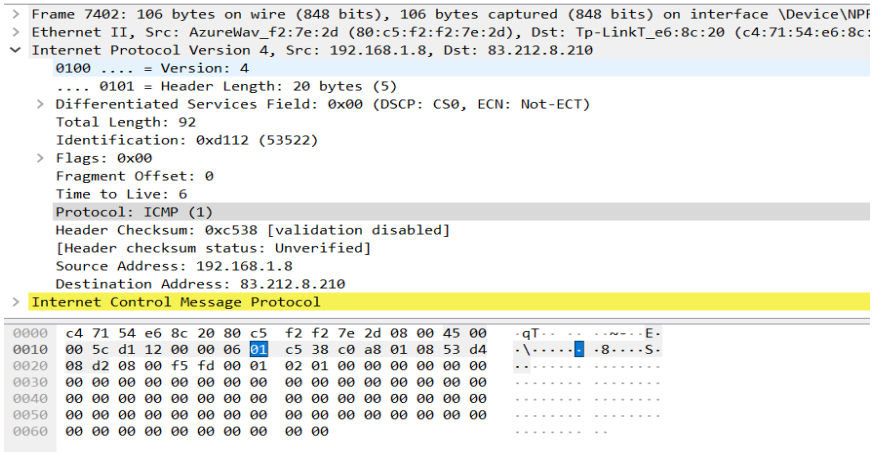
```
0000  c4 71 54 e6 8c 20 80 c5  f2 f2 7e 2d 08 00 45 00   ·qT·· ·· ··~-··E·
0010  00 5c d1 12 00 00 06 01  c5 38 c0 a8 01 08 53 d4   ·\····· ·8····S·
0020  08 d2 08 00 f5 fd 00 01  02 01 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
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                     ········ ··
```

Και πιο συγκεκριμένα :

```
c0 a8 01 08
```

5.

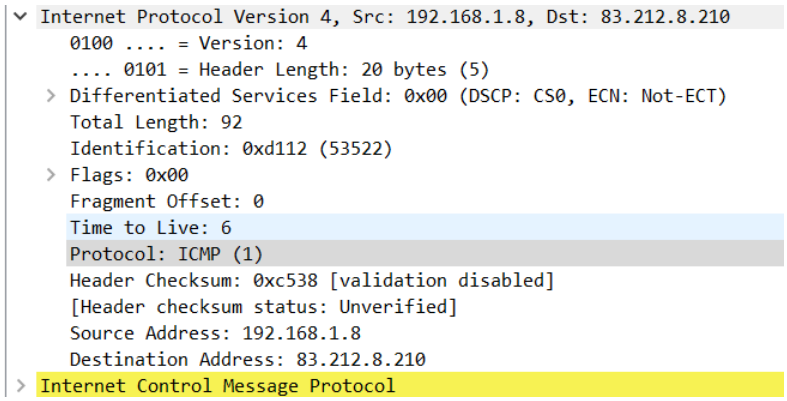
Το πεδίο Protocol δηλαδή το πεδίο 24 της επικεφαλίδας της IP έχει την τιμή 01 όπως φαίνεται και στο ακόλουθο screenshot :



Και πιο συγκεκριμένα :

```
01
```

Και ο τύπος του Protocol είναι ICMP(1) :



Και πιο συγκεκριμένα :

```
Protocol: ICMP (1)
```

6.

Στη κεφαλίδα IP Header υπάρχουν 20 bytes στο σύνολο :

```
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 83.212.8.210
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xd112 (53522)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 6
    Protocol: ICMP (1)
    Header Checksum: 0xc538 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.8
    Destination Address: 83.212.8.210
> Internet Control Message Protocol
```

Και πιο συγκεκριμένα :

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

7.

Στη κεφαλίδα IP Header έχουμε όπως προαναφέραμε 20 bytes :

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

Και συνολικό μήκος (Total Length) έχουμε 92 bytes :

```
Total Length: 92
```

Επομένως τα bytes που μεταφέρει το πακέτο IP στο πεδίο δεδομένων είναι :

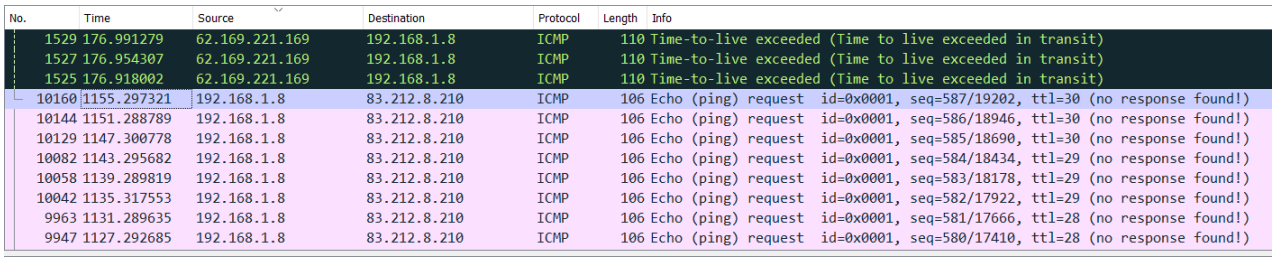
92-20=72bytes

8.

Το παραπάνω μήκος από το πεδίο δεδομένων προκύπτει όπως και προηγουμένως αναφέραμε με μια απλή αφαίρεση του Header Length (20bytes) από το συνολικό μήκος Total Length (92bytes) άρα 72bytes.

9.

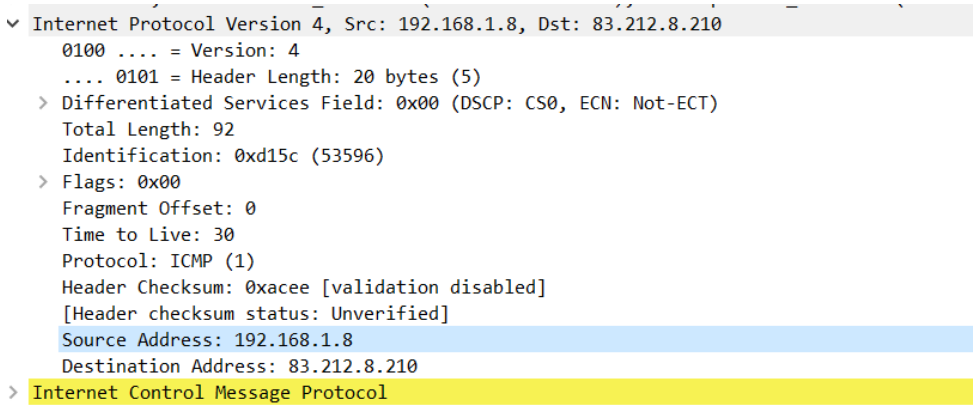
Στη πορεία εκτελώντας ότι μας ζητάει η άσκηση έχουμε :



No.	Time	Source	Destination	Protocol	Length	Info
1529	176.991279	62.169.221.169	192.168.1.8	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1527	176.954307	62.169.221.169	192.168.1.8	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
1525	176.918002	62.169.221.169	192.168.1.8	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
10160	1155.297321	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=587/19202, ttl=30 (no response found!)
10144	1151.288789	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=586/18946, ttl=30 (no response found!)
10129	1147.300778	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=585/18690, ttl=30 (no response found!)
10082	1143.295682	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=584/18434, ttl=29 (no response found!)
10058	1139.289819	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=583/18178, ttl=29 (no response found!)
10042	1135.317553	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=582/17922, ttl=29 (no response found!)
9963	1131.289635	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=581/17666, ttl=28 (no response found!)
9947	1127.292685	192.168.1.8	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=580/17410, ttl=28 (no response found!)

Και με βάση Source είναι σε φθίνουσα σειρά

το βελάκι όπως βλέπουμε είναι προς τα κάτω και επιλέγουμε να αναλύσουμε το πρώτο ICMP πακέτο :



Τα πεδία **Identification**, **Time to live** και **Header checksum** αλλάζουν πάντα από ένα πακέτο στο επόμενο.

Πιο συγκεκριμένα :

- το πεδίο **Identification** είναι μοναδικό διότι τα διαφορετικά IP πακέτα πρέπει να έχουν και διαφορετικό ID προφανώς για να αναγνωρίζονται
- Η traceroute όπως είναι γνωστό αυξάνει κάθε πακέτο που έρχεται άρα το πεδίο **Time to live** προφανώς και αυτό είναι διαφορετικό
- Και τέλος αφού σε κάθε πακέτο αλλάζει το Header προφανώς σε κάθε πακέτο θα υπάρχει διαφορετική τιμή στο πεδίο **Header checksum**

10.

Αντίστοιχα τα πεδία της επικεφαλίδας που παραμένουν αναλλοίωτα και αμετάβλητα είναι :

- Το πεδίο **Version**

```
Version: 4
```

- Το πεδίο **Header Length**

```
Header Length: 20 bytes
```

- Το πεδίο **Differentiated Services**

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

- Το πεδίο **Protocol**

```
Protocol: ICMP (1)
```

- Το πεδίο **Source Address**

```
Source Address: 192.168.1.8
```

- Και τέλος το πεδίο **Destination Address**

```
Destination Address: 83.212.8.210
```

11.

Οι λόγοι που τα προαναφερθέντα πεδία παραμένουν αναλλοίωτα και αμετάβλητα είναι :

- Για το πεδίο **Version** γνωρίζουμε ότι παντού χρησιμοποιείται το πρωτόκολλο **IPV4**

```
Internet Protocol Version 4
```

- Για το πεδίο **Header Length** γνωρίζουμε ότι όλα τα ICMP πακέτα έχουν το ίδιο Header Length
- Το πεδίο **Differentiated Services** είναι και αυτό ίδιο σε όλα τα ICMP πακέτα διότι χρησιμοποιούν το ίδιο τύπο Service
- Το πεδίο **Protocol**

`Protocol: ICMP (1)` Προφανώς είναι ίδιο για όλα τα ICMP πακέτα

- Το πεδίο **Source Address** είναι ίδιο για όλα τα πακέτα γιατί στέλνονται από τον ίδιο αποστολέα
- Και τέλος το πεδίο **Destination Address** και αυτό παραμένει αμετάβλητο επειδή όλα τα πακέτα στέλνονται στον ίδιο παραλήπτη.

12.

Όπως ακριβώς αναφέραμε και στο ερώτημα 9 τα πεδία της επικεφαλίδας IP που πρέπει να αλλάξουν είναι τα **Identification**, **Time to live** και **Header checksum** για τους λόγους που αναφέραμε σε εκείνο το ερώτημα

13.

Η διεύθυνση IP του κοντινότερου προς τον υπολογιστή μας δρομολογητή είναι αυτή στο 1ο βήμα traceroute αφού πρώτα δώσουμε στο cmd line την εντολή :

```
C:\Users\bsiam>tracert -d 83.212.8.210
```

```
C:\Users\bsiam>tracert -d 83.212.8.210

Tracing route to 83.212.8.210 over a maximum of 30 hops

  1     2 ms     2 ms     6 ms  192.168.1.254
```

Επομένως η διεύθυνση IP είναι :

```
192.168.1.254
```

14.

Η τιμή του πεδίου TTL του πρώτου πακέτου της σειράς είναι **30** :

```
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 83.212.8.210
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xd15c (53596)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 30
    Protocol: ICMP (1)
    Header Checksum: 0xacee [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.8
```

```
Time to Live: 30
```

Η αλλιώς **1e** :

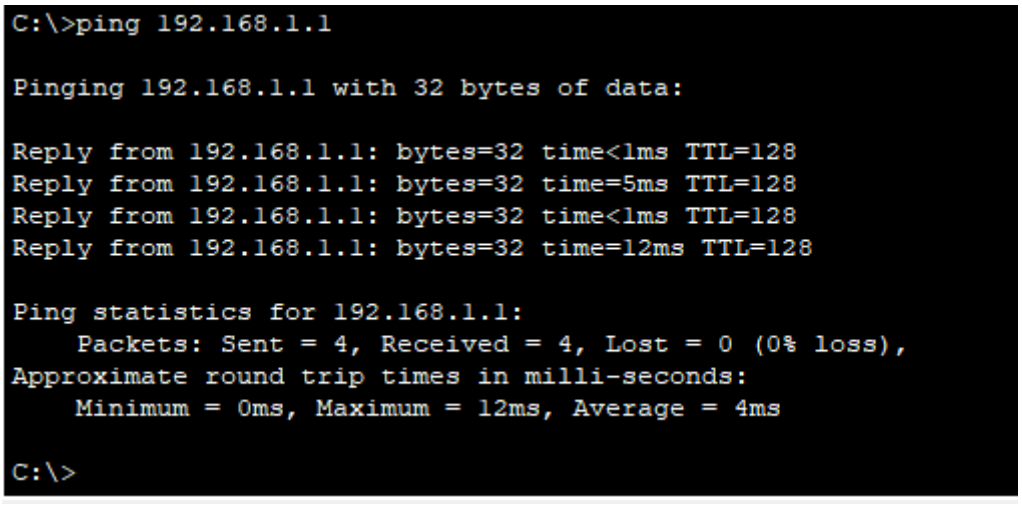
```
0000  c4 71 54 e6 8c 20 80 c5  f2 f2 7e 2d 08 00 45 00
0010  00 5c d1 5c 00 00 1e 01  ac ee c0 a8 01 08 53 d4
0020  08 d2 08 00 f5 b3 00 01  02 4b 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00
```

15.

Οι τιμές του πεδίου TTL αλλάζουν διότι η traceroute όπως είναι γνωστό αυξάνει κάθε πακέτο που έρχεται άρα το πεδίο Time to live προφανώς και αυτό είναι διαφορετικό.

Γ ΜΕΡΟΣ

I. Απευθύνεται στο τοπικό Interface του PCO και αυτό συμβαίνει διότι η IP 192.168.1.1 δόθηκε στο PCO



II. Ναι έχουμε απάντηση όπως βλέπουμε και από το παρακάτω screenshot:

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

III. Ναι έχουμε απάντηση όπως βλέπουμε και από παρακάτω screenshot:

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Δ ΜΕΡΟΣ

ΜΕΡΟΣ $1^{Ο}$

Κάνουμε κλικ στο PC0 και επιλέγουμε το command prompt και γράφουμε την εντολή telnet 10.10.10.2 και στην πορεία τον default κωδικό cisco

```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open


User Access Verification

Password:
S1>
```

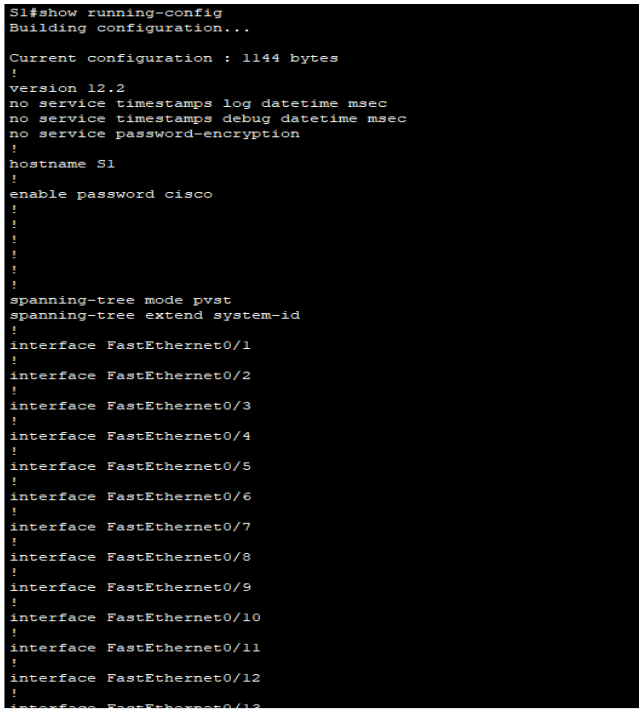
Μετά δίνουμε την εντολή en και σαν password πάλι cisco

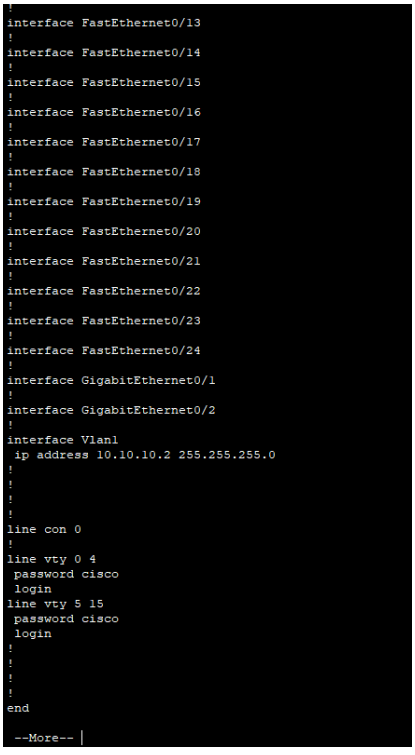
```
Password:
S1>en
Password:
S1#
```

Στην συνέχεια δίνω την εντολή στο command copy running-config startup-config για την αποθήκευση της μέχρι τώρα διαμόρφωσης

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Για να εμφανίσουμε στην οθόνη μας της παρούσαςδιαμόρφωση δίνουμε την εντολή show running-config





Όπως βλέπουμε από τα screenshot οι κωδικοί φαίνονται να μην είναι κρυπτογραφημένοι

Για να κρυπτογραφήσουμε τους κωδικούς δίνουμε για αρχή τις εντολές

conf-ter και service password-encryption και στη συνέχεια την εντολή exit

όπως φαίνεται παρακάτω :

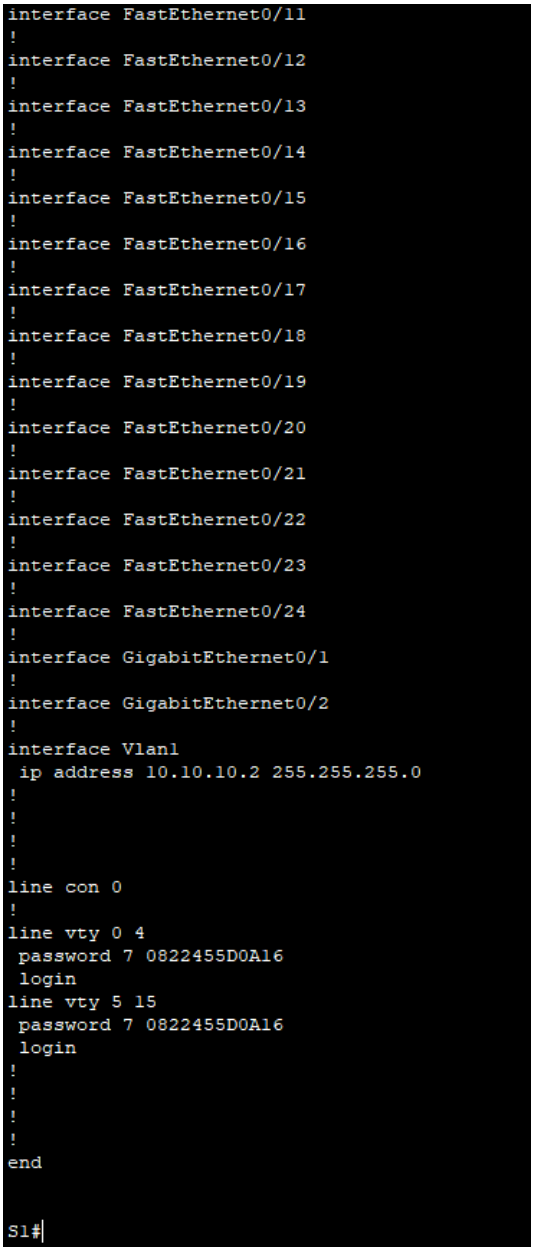
```
S1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#service password-encryption
S1(config)#exit
S1#
```

Στη συνέχεια γράφω την εντολή show running-config για να εμφανίσουμε

πάλι την τρέχουσα διαμόρφωση και παρατηρούμε πλέον ότι οι κωδικοί είναι

κρυπτογραφημένοι :

```
S1#show running-config
Building configuration...

Current configuration : 1168 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable password 7 0822455D0A16
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
```



ΜΕΡΟΣ 2^{Ο}

Δίνω πάλι την εντολή conf-ter

```
S1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
```

Στη συνέχεια δίνω την εντολή ip domain-name netacad.pka

```
S1(config)#ip domain-name netcad.pka
```

Μετά δίνω εντολή crypt key generate rsa και στο πεδίο που μας ζητάει βάζω

τον αριθμό 1024

```
S1(config)#crypt key generate rsa
The name for the keys will be: S1.netcad.pka
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#
```

Μετά την εντολή S1(config)#username ceid5890 secret ceid5890

```
S1(config)#username ceid5890 secret ceid5890
*Mar 1 9:30:0.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
```

Για να δημιουργήσουμε έναν χρήστη administrator με τη λέξη cisco ως

μυστικό κωδικό πρόσβασης δίνουμε την εντολή S1(config)#username

administrator secret Cisco

Μετά δίνουμε τις εντολές τις παρακάτω

S1 (config)#line vty 0 15

S1 (config-line)#! login local

S1 (config-line)#transport input ssh

S1 (config-line)#login local

S1 (config-line)#no password cisco

S1 (config-line)#exit

S1 (config)#exit

S1#exit

ΜΕΡΟΣ 3^{Ο}

Δίνω την εντολή telnet 10.10.10.2 :

```
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open

[Connection to 10.10.10.2 closed by foreign host]
C:\>
```

Μετά δίνω την εντολή ssh -l administrator 10.10.10.2 και βάζω σαν κωδικό Cisco:

```
C:\>ssh -l administrator 10.10.10.2

Password:



S1>
```

Εναλλακτικά μπορούμε να μπούμε με την εντολή ssh -l ceid5890 10.10.10.2

και βάζω σαν κωδικό ceid5890 :