



---

# ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

---

## ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 10: ΣΥΣΤΗΜΑΤΑ ΟΝΟΜΑΣΙΑΣ ΠΕΡΙΟΧΩΝ DNS



20 ΔΕΚΕΜΒΡΙΟΥ, 2022

ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

Όνοματεπώνυμο: Θεodorής Αράπης		Ομάδα: 2
Όνομα PC/ΛΣ: pc-a12/ WINDOWS 95		Ημερομηνία: 20/12/2022
Διεύθυνση IP: 147.102.38.62 147.102.131.41 (Άσκηση 2, 2.1-2.20)		Διεύθυνση MAC: 00:11:25:F8:D6:E9

## Άσκηση 1: Υπηρεσία DNS

### 1.1

όπως βλέπουμε, εμφανίζονται οι εξυπηρετητές κορυφής (root name servers), οι οποίοι εξυπηρετούν την περιοχή κορυφής (root zone).

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\labuser>nslookup
Default Server:  achilles.noc.ntua.gr
Address:  147.102.222.210

> server 147.102.222.210
Default Server:  achilles.noc.ntua.gr
Address:  147.102.222.210

> set q=ns
> .
Server:  achilles.noc.ntua.gr
Address:  147.102.222.210

Non-authoritative answer:
(root)  nameserver = c.root-servers.net
(root)  nameserver = a.root-servers.net
(root)  nameserver = l.root-servers.net
(root)  nameserver = b.root-servers.net
(root)  nameserver = h.root-servers.net
(root)  nameserver = f.root-servers.net
(root)  nameserver = i.root-servers.net
(root)  nameserver = d.root-servers.net
(root)  nameserver = g.root-servers.net
(root)  nameserver = m.root-servers.net
(root)  nameserver = k.root-servers.net
(root)  nameserver = e.root-servers.net
(root)  nameserver = j.root-servers.net

a.root-servers.net      internet address = 198.41.0.4
b.root-servers.net      internet address = 199.9.14.201
c.root-servers.net      internet address = 192.33.4.12
d.root-servers.net      internet address = 199.7.91.13
e.root-servers.net      internet address = 192.203.230.10
f.root-servers.net      internet address = 192.5.5.241
g.root-servers.net      internet address = 192.112.36.4
h.root-servers.net      internet address = 198.97.190.53
i.root-servers.net      internet address = 192.36.148.17
j.root-servers.net      internet address = 192.58.128.30
k.root-servers.net      internet address = 193.0.14.129
l.root-servers.net      internet address = 199.7.83.42
m.root-servers.net      internet address = 202.12.27.33
a.root-servers.net      AAAA IPv6 address = 2001:503:ba3e::2:30
b.root-servers.net      AAAA IPv6 address = 2001:500:200::b
```

## 1.2

Εμφανίστηκαν 13 DNS servers, όπως και αναμέναμε. Ένας από αυτούς, ο a.root-servers.net έχει IPv4: 198.41.0.4 και IPv6: 2001:503:ba3e::2:30.

## 1.3

Πληκτρολογούμε την εντολή «server 198.41.0.4».

```
> server 198.41.0.4
Default Server:  a.root-servers.net
Address:  198.41.0.4
```

## 1.4

```
> gr.
Server:  a.root-servers.net
Address:  198.41.0.4

gr      nameserver = gr-d.ics.forth.gr
gr      nameserver = gr-at.ics.forth.gr
gr      nameserver = grdns.ics.forth.gr
gr      nameserver = gr-m.ics.forth.gr
gr      nameserver = estia.ics.forth.gr
gr      nameserver = gr-c.ics.forth.gr
gr-d.ics.forth.gr      internet address = 194.0.11.102
gr-d.ics.forth.gr      AAAA IPv6 address = 2001:678:e:102::53
gr-at.ics.forth.gr      internet address = 78.104.145.227
grdns.ics.forth.gr      internet address = 139.91.1.1
gr-m.ics.forth.gr      internet address = 194.0.4.10
gr-m.ics.forth.gr      AAAA IPv6 address = 2001:678:7::4:10
estia.ics.forth.gr      internet address = 139.91.191.3
estia.ics.forth.gr      AAAA IPv6 address = 2001:648:2c30::191:3
gr-c.ics.forth.gr      internet address = 194.0.1.25
gr-c.ics.forth.gr      AAAA IPv6 address = 2001:678:4::19
```

Εισάγοντας ως εντολή το gr., εμφανίζονται τα παρακάτω, με κατάληξη .gr. Οι DNS εξυπηρετητές αυτοί ανήκουν στο top level domain (κάτω από τη ρίζα).

## 1.5

Όπως βλέπουμε από το screenshot, εμφανίστηκαν 6 υπεύθυνοι εξυπηρετητές DNS για την περιοχή “gr.”. Ένας από αυτούς είναι ο gr-d.ics.forth.gr με IPv4 194.0.11.102 και IPv6 2001:678:e:102::53.

## 1.6

Παρατηρούμε πως εμφανίζονται τα ίδια αποτελέσματα με το 1.4. Συμπεραίνουμε συνεπώς, ότι οι εξυπηρετητές κορυφής δίνουν αποτελέσματα για το δεξιότερο τμήμα της ονομασίας που πληκτρολογούμε (top level domain) αδιαφορώντας για την υποπεριοχή.

```

> ntua.gr.
Server:  a.root-servers.net
Address: 198.41.0.4

gr      nameserver = gr-d.ics.forth.gr
gr      nameserver = gr-at.ics.forth.gr
gr      nameserver = grdns.ics.forth.gr
gr      nameserver = gr-m.ics.forth.gr
gr      nameserver = estia.ics.forth.gr
gr      nameserver = gr-c.ics.forth.gr
gr-d.ics.forth.gr  internet address = 194.0.11.102
gr-d.ics.forth.gr  AAAA IPv6 address = 2001:678:e:102::53
gr-at.ics.forth.gr internet address = 78.104.145.227
grdns.ics.forth.gr internet address = 139.91.1.1
gr-m.ics.forth.gr  internet address = 194.0.4.10
gr-m.ics.forth.gr  AAAA IPv6 address = 2001:678:7::4:10
estia.ics.forth.gr internet address = 139.91.191.3
estia.ics.forth.gr AAAA IPv6 address = 2001:648:2c30::191:3
gr-c.ics.forth.gr  internet address = 194.0.1.25
gr-c.ics.forth.gr  AAAA IPv6 address = 2001:678:4::19

```

## 1.7

Επιλέγουμε τον σέρβερ `estia.ics.forth.gr`, επομένως εκτελούμε την εντολή `server 139.91.191.3`. Ωστόσο, αυτή τη φορά λαμβάνουμε και κάποια έξτρα αποτελέσματα:

```

> server 139.91.191.3
in-addr.arpa      nameserver = e.in-addr-servers.arpa
in-addr.arpa      nameserver = f.in-addr-servers.arpa
in-addr.arpa      nameserver = d.in-addr-servers.arpa
in-addr.arpa      nameserver = c.in-addr-servers.arpa
in-addr.arpa      nameserver = b.in-addr-servers.arpa
in-addr.arpa      nameserver = a.in-addr-servers.arpa
e.in-addr-servers.arpa internet address = 203.119.86.101
e.in-addr-servers.arpa AAAA IPv6 address = 2001:dd8:6::101
f.in-addr-servers.arpa internet address = 193.0.9.1
f.in-addr-servers.arpa AAAA IPv6 address = 2001:67c:e0::1
d.in-addr-servers.arpa internet address = 200.10.60.53
d.in-addr-servers.arpa AAAA IPv6 address = 2001:13c7:7010::53
c.in-addr-servers.arpa internet address = 196.216.169.10
c.in-addr-servers.arpa AAAA IPv6 address = 2001:43f8:110::10
b.in-addr-servers.arpa internet address = 199.253.183.183
b.in-addr-servers.arpa AAAA IPv6 address = 2001:500:87::87
a.in-addr-servers.arpa internet address = 199.180.182.53
a.in-addr-servers.arpa AAAA IPv6 address = 2620:37:e000::53
Default Server:  [139.91.191.3]
Address: 139.91.191.3

```

## 1.8

Αυτή τη φορά λαμβάνουμε διαφορετικά αποτελέσματα σε σχέση με αυτά του 1.6. Ο λόγος που έγινε αυτό είναι πως επιλέγοντας τον DNS εξυπηρετητή στο 1.7 κατεβήκαμε στο δέντρο της DNS ιεραρχίας οπότε και βλέπουμε τους nameservers για το `ntua.gr`. αντί του `gr`.

```

> ntua.gr.
Server: [139.91.191.3]
Address: 139.91.191.3

ntua.gr nameserver = achilles.noc.ntua.gr
ntua.gr nameserver = ulysses.noc.ntua.gr
ntua.gr nameserver = sns1.grnet.gr
ntua.gr nameserver = diomedes.noc.ntua.gr
ntua.gr nameserver = sns0.grnet.gr
diomedes.noc.ntua.gr internet address = 147.102.222.220
achilles.noc.ntua.gr internet address = 147.102.222.210
ulysses.noc.ntua.gr internet address = 147.102.222.230

```

### 1.9

Καταγράφηκαν 5 DNS εξυπηρετητές για την περιοχή ntua.gr.. Το όνομα και η IPv4 ενός εξ αυτών είναι diomedes.noc.ntua.gr και 147.102.222.220 αντίστοιχα.

### 1.10

Η απάντηση που λαμβάνουμε περιλαμβάνει τους ίδιους DNS servers της περιοχής ntua.gr., περιέχει ωστόσο περισσότερα στοιχεία για αυτούς.

```

> server 147.102.222.220
Default Server: [147.102.222.220]
Address: 147.102.222.220

> ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

ntua.gr nameserver = diomedes.noc.ntua.gr
ntua.gr nameserver = sns0.grnet.gr
ntua.gr nameserver = achilles.noc.ntua.gr
ntua.gr nameserver = ulysses.noc.ntua.gr
ntua.gr nameserver = sns1.grnet.gr
sns0.grnet.gr internet address = 83.212.5.89
sns1.grnet.gr internet address = 83.212.5.22
ulysses.noc.ntua.gr internet address = 147.102.222.230
achilles.noc.ntua.gr internet address = 147.102.222.210
diomedes.noc.ntua.gr internet address = 147.102.222.220
sns0.grnet.gr AAAA IPv6 address = 2001:648:2ffc:203::89
sns1.grnet.gr AAAA IPv6 address = 2001:648:2ffc:112::2
ulysses.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::210
diomedes.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::220

```

### 1.11

Λαμβάνουμε τώρα τα παρακάτω. Ένα όνομα που δεν εμφανίστηκε στο ερώτημα 1.9 είναι το psyche.cn.ece.ntua.gr.

```

> cn.ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

cn.ntua.gr      nameserver = psyche.cn.ece.ntua.gr
cn.ntua.gr      nameserver = ulysses.noc.ntua.gr
cn.ntua.gr      nameserver = achilles.noc.ntua.gr
psyche.cn.ece.ntua.gr  internet address = 147.102.40.1
ulysses.noc.ntua.gr    internet address = 147.102.222.230
achilles.noc.ntua.gr   internet address = 147.102.222.210
psyche.cn.ece.ntua.gr  AAAA IPv6 address = 2001:648:2000:28::1
ulysses.noc.ntua.gr    AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr   AAAA IPv6 address = 2001:648:2000:de::210

```

### 1.12

Καταγράφηκαν για τις σχολές HMMY και MMM οι εξής υπεύθυνοι DNS εξυπηρετητές:

```

> ece.ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

ece.ntua.gr      nameserver = diomedes.noc.ntua.gr
ece.ntua.gr      nameserver = ulysses.noc.ntua.gr
ece.ntua.gr      nameserver = achilles.noc.ntua.gr
ulysses.noc.ntua.gr  internet address = 147.102.222.230
achilles.noc.ntua.gr internet address = 147.102.222.210
diomedes.noc.ntua.gr internet address = 147.102.222.220
ulysses.noc.ntua.gr  AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::210
diomedes.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::220
> metal.ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

metal.ntua.gr      nameserver = serifos.metal.ntua.gr
metal.ntua.gr      nameserver = ulysses.noc.ntua.gr
metal.ntua.gr      nameserver = achilles.noc.ntua.gr
metal.ntua.gr      nameserver = diomedes.noc.ntua.gr
serifos.metal.ntua.gr  internet address = 147.102.121.1
ulysses.noc.ntua.gr    internet address = 147.102.222.230
achilles.noc.ntua.gr   internet address = 147.102.222.210
diomedes.noc.ntua.gr   internet address = 147.102.222.220
ulysses.noc.ntua.gr    AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr   AAAA IPv6 address = 2001:648:2000:de::210
diomedes.noc.ntua.gr   AAAA IPv6 address = 2001:648:2000:de::220

```

Όπως βλέπουμε παραπάνω, υπάρχουν 3 υπεύθυνοι εξυπηρετητές DNS κοινοί (diomedes.noc.ntua.gr, ulysses.noc.ntua.gr, achilles.noc.ntua.gr), ωστόσο η σχολή MMM έχει έναν επιπλέον εξυπηρετητή, τον serifos.metal.ntua.gr.

### 1.13

Όπως φαίνεται ακολούθως, ο κύριος εξυπηρετητής της περιοχής cn.ntua.gr είναι ο psyche.cn.ece.ntua.gr με IPv4 147.102.40.1 και σειριακό αριθμό 2022120501.

```

> set q=soa
> cn.ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

cn.ntua.gr
    primary name server = psyche.cn.ece.ntua.gr
    responsible mail addr = hostmaster.cn.ntua.gr
    serial = 2022120501
    refresh = 28800 <8 hours>
    retry = 7200 <2 hours>
    expire = 604800 <7 days>
    default TTL = 86400 <1 day>
cn.ntua.gr    nameserver = psyche.cn.ece.ntua.gr
cn.ntua.gr    nameserver = achilles.noc.ntua.gr
cn.ntua.gr    nameserver = ulysses.noc.ntua.gr
psyche.cn.ece.ntua.gr    internet address = 147.102.40.1
ulysses.noc.ntua.gr    internet address = 147.102.222.230
achilles.noc.ntua.gr    internet address = 147.102.222.210
psyche.cn.ece.ntua.gr    AAAA IPv6 address = 2001:648:2000:28::1
ulysses.noc.ntua.gr    AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr    AAAA IPv6 address = 2001:648:2000:de::210

```

#### 1.14

Ένας δευτερεύων εξυπηρετητής θα αναζητά αλλαγές σχετικά με την παραπάνω περιοχή ανά 8 ώρες (refresh).

#### 1.15

Οι σχετικές με την περιοχή cn.ntua.gr. εγγραφές στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών διατηρούνται για 1 μέρα (24 ώρες) (default TTL).

#### 1.16

```

> ece.ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

ece.ntua.gr
    primary name server = achilles.noc.ntua.gr
    responsible mail addr = noc.ntua.gr
    serial = 2022101000
    refresh = 86400 <1 day>
    retry = 86400 <1 day>
    expire = 86400 <1 day>
    default TTL = 86400 <1 day>
ece.ntua.gr    nameserver = achilles.noc.ntua.gr
ece.ntua.gr    nameserver = diomedes.noc.ntua.gr
ece.ntua.gr    nameserver = ulysses.noc.ntua.gr
ulysses.noc.ntua.gr    internet address = 147.102.222.230
achilles.noc.ntua.gr    internet address = 147.102.222.210
diomedes.noc.ntua.gr    internet address = 147.102.222.220
ulysses.noc.ntua.gr    AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr    AAAA IPv6 address = 2001:648:2000:de::210
diomedes.noc.ntua.gr    AAAA IPv6 address = 2001:648:2000:de::220

```



Για την περιοχή ece.ntua.gr λαμβάνουμε τα εξής:

- **Κύριος εξυπηρετητής DNS**: achilles.noc.ntua.gr, IPv4 147.102.222.210 και
- **Σειριακός Αριθμός**: 2022101000
- **Refresh Time**: 1 μέρα (24 ώρες)
- **Default TTL**: 1 μέρα (24 ώρες)

### 1.17

Παρατηρούμε ότι τα 4 πρώτα ψηφία του serial number αντιστοιχούν στο τρέχον έτος.

### 1.18

Επιλέξαμε τα πανεπιστήμια Ε.Κ.Π.Α., Π.Α.Δ.Α και Α.Π.Θ:

- **www.auth.gr (Α.Π.Θ.)**: 155.207.1.12 (IPv4)/ 2001:648:2800:1:155:207:1:12 (IPv6)
- **www.uniwa.gr (Π.Α.Δ.Α.)**: 195.130.100.8 (IPv4)
- **www.uoa.gr (Ε.Κ.Π.Α.)**: 195.134.71.228 (IPv4)

### 1.19

Αρχικά κάνουμε set q=ptr ώστε οι IPv4 διευθύνσεις να αντιστοιχιστούν σε ονόματα. Αφού έχουμε το υποδίκτυο 147.102.40.16/29 τότε μπορούμε να επιλέξουμε ανάμεσα σε 8 hosts (147.102.40.16 - 147.102.40.23). Επιλέγουμε τις διευθύνσεις 147.102.40.16 και 147.102.40.17, οι οποίες βρίσκουμε πως αντιστοιχούν στο trillium.cn.ece.ntua.gr και το pegasus.cn.ece.ntua.gr.

```
> set q=ptr
> 147.102.40.16
Server: [147.102.222.220]
Address: 147.102.222.220

16.40.102.147.in-addr.arpa      name = trillium.cn.ece.ntua.gr
40.102.147.in-addr.arpa nameserver = psyche.cn.ece.ntua.gr
40.102.147.in-addr.arpa nameserver = achilles.noc.ntua.gr
40.102.147.in-addr.arpa nameserver = ulysses.noc.ntua.gr
psyche.cn.ece.ntua.gr internet address = 147.102.40.1
ulysses.noc.ntua.gr internet address = 147.102.222.230
achilles.noc.ntua.gr internet address = 147.102.222.210
psyche.cn.ece.ntua.gr AAAA IPv6 address = 2001:648:2000:28::1
ulysses.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::210
> 147.102.40.17
Server: [147.102.222.220]
Address: 147.102.222.220

17.40.102.147.in-addr.arpa      name = pegasus.cn.ece.ntua.gr
40.102.147.in-addr.arpa nameserver = achilles.noc.ntua.gr
40.102.147.in-addr.arpa nameserver = psyche.cn.ece.ntua.gr
40.102.147.in-addr.arpa nameserver = ulysses.noc.ntua.gr
psyche.cn.ece.ntua.gr internet address = 147.102.40.1
ulysses.noc.ntua.gr internet address = 147.102.222.230
achilles.noc.ntua.gr internet address = 147.102.222.210
psyche.cn.ece.ntua.gr AAAA IPv6 address = 2001:648:2000:28::1
ulysses.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::210
```



## 1.20

Παρατηρούμε πως στην απόκριση η διεύθυνση IPv4 αναπαρίσταται λίγο διαφορετικά. Πιο συγκεκριμένα, βλέπουμε πως εμφανίζονται ως: 16.40.102.147.in-addr.arpa και 17.40.102.147.in-addr.arpa για τις IPv4 147.102.40.16 και 147.102.40.17 αντίστοιχα.

## 1.21

Καταγράφουμε ως κανονικό όνομα το lemmy.metal.ntua.gr

```
> set q=cname
> www.metal.ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

www.metal.ntua.gr      canonical name = lemmy.metal.ntua.gr
metal.ntua.gr          nameserver = diomedes.noc.ntua.gr
metal.ntua.gr          nameserver = achilles.noc.ntua.gr
metal.ntua.gr          nameserver = serifos.metal.ntua.gr
metal.ntua.gr          nameserver = ulysses.noc.ntua.gr
serifos.metal.ntua.gr  internet address = 147.102.121.1
ulysses.noc.ntua.gr    internet address = 147.102.222.230
achilles.noc.ntua.gr   internet address = 147.102.222.210
diomedes.noc.ntua.gr   internet address = 147.102.222.220
ulysses.noc.ntua.gr    AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr   AAAA IPv6 address = 2001:648:2000:de::210
diomedes.noc.ntua.gr   AAAA IPv6 address = 2001:648:2000:de::220
```

Προκειμένου να καταγράψουμε και την IP του υπολογιστή που φιλοξενεί την ιστοθέρση αυτή, ξανακάνουμε set q=a οπότε και παίρνουμε την IP: 147.102.121.10.

```
> set q=a
> www.metal.ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

Name:    lemmy.metal.ntua.gr
Address: 147.102.121.10
Aliases: www.metal.ntua.gr
```

## 1.22

```
> set q=mx
> arch.ntua.gr
Server: [147.102.222.220]
Address: 147.102.222.220

arch.ntua.gr  MX preference = 100, mail exchanger = achilles.noc.ntua.gr
arch.ntua.gr  MX preference = 10, mail exchanger = f1.mail.ntua.gr
arch.ntua.gr  MX preference = 100, mail exchanger = diomedes.noc.ntua.gr
arch.ntua.gr  MX preference = 100, mail exchanger = ulysses.noc.ntua.gr
arch.ntua.gr  MX preference = 10, mail exchanger = f0.mail.ntua.gr
arch.ntua.gr  nameserver = diomedes.noc.ntua.gr
arch.ntua.gr  nameserver = ulysses.noc.ntua.gr
arch.ntua.gr  nameserver = achilles.noc.ntua.gr
f0.mail.ntua.gr internet address = 147.102.222.195
f1.mail.ntua.gr internet address = 147.102.222.196
ulysses.noc.ntua.gr internet address = 147.102.222.230
achilles.noc.ntua.gr internet address = 147.102.222.210
diomedes.noc.ntua.gr internet address = 147.102.222.220
ulysses.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::230
achilles.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::210
diomedes.noc.ntua.gr AAAA IPv6 address = 2001:648:2000:de::220
```

Καταγράφονται μεταξύ άλλων, οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου f1.mail.ntua.gr (147.120.222.196) και achilles.noc.ntua.gr (147.102.222.210).

### 1.23

Κοιτώντας το παραπάνω στιγμιότυπο, παρατηρούμε ότι θα προτιμηθεί ή ο εξυπηρετητής f0.mail.ntua.gr ή ο f1.mail.ntua.gr, καθώς έχουν τον μικρότερο αριθμό προτίμησης (MX preference = 10).

### 1.24

```
> ls -d central.ntua.gr
[[147.102.222.220]]
central.ntua.gr. SOA      netsrv0.central.ntua.gr dnsmaster.central
.ntua.gr. (180 21600 1800 604800 900)
central.ntua.gr. A       147.102.222.46
central.ntua.gr. NS      netsrv0.central.ntua.gr
central.ntua.gr. NS      ulysses.noc.ntua.gr
central.ntua.gr. NS      achilles.noc.ntua.gr
central.ntua.gr. NS      diomedes.noc.ntua.gr
central.ntua.gr. MX      10 ulysses.noc.ntua.gr
central.ntua.gr. MX      10  achilles.noc.ntua.gr
central.ntua.gr. MX      10  diomedes.noc.ntua.gr
central.ntua.gr. TXT      "v=spf1 ip4:147.102.222.0/24 ip6
:2001:648:2000:de::/64 a -all"
243gateway      A       147.102.243.200
246gateway      A       147.102.246.200
acadinfo        CNAME   beta.central.ntua.gr
acoustics2010   CNAME   oldwebhoster.central.ntua.gr
adminasa        A       147.102.243.222
agents          A       147.102.243.137
aps             A       147.102.243.101
arccislicenses CNAME   licenses0.central.ntua.gr
aspenlicenses  CNAME   licenses2.central.ntua.gr
backend         A       147.102.243.119
bastion0        A       147.102.243.58
beta            A       147.102.243.133
career          CNAME   career.ntua.gr
catiallicenses  CNAME   licenses2.central.ntua.gr
cloudfront      CNAME   webhoster.central.ntua.gr
cloudfront0     A       147.102.243.84
cloudproxy      A       147.102.243.90
cloudstorage    A       147.102.246.113
```

Με την εντολή «ls -d central.ntua.gr» εμφανίστηκαν όλες οι εγγραφές της περιοχής central.ntua.gr (το στιγμιότυπο απεικονίζει ένα κομμάτι της απόκρισης που λάβαμε).

### 1.25

Σχηματίζουμε τον παρακάτω πίνακα με τα ζητούμενα στοιχεία:

Είδος εγγραφής	Στοιχείο 1	Στοιχείο 2	Στοιχείο 3
NS	central.ntua.gr	netsrv0.central.ntua.gr	-
MX	central.ntua.gr	10	diomedes.noc.ntua.gr
A	central.ntua.gr	147.102.222.46	-
SOA	central.ntua.gr	netsrv0.central.ntua.gr dnsmas- ter.central.ntua.gr	(180 21600 1800 604800 900)
CNAME	acadinfo	beta.central.ntua.gr	-
TXT	central.ntua.gr	"v=spf1 ip4:147.102.222.0/24 ip6:2001:648:2000:de::/64 a -all"	-

## Άσκηση 2: Πρωτόκολλο DNS

### 2.1

Χρησιμοποιήθηκε η εντολή «ipconfig/flushdns».

### 2.2

Χρησιμοποιήθηκε το φίλτρο σύλληψης «host 147.102.38.62».

### 2.3

Δείχνουμε τις εντολές που χρησιμοποιήσαμε στα παρακάτω στιγμιότυπα:

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Theodore>nslookup - 147.102.1.1
Default Server:  theseas.softlab.ece.ntua.gr
Address:  147.102.1.1

> set domain=.
> 147.102.40.10 147.102.40.1
Server:  [147.102.40.1]
Address:  147.102.40.1

Name:    titan.cn.ece.ntua.gr
Address:  147.102.40.10

> 147.102.40.10 147.102.7.1
Server:  [147.102.7.1]
Address:  147.102.7.1

Name:    titan.cn.ece.ntua.gr
Address:  147.102.40.10
```

## 2.4

Το όνομα του 147.102.40.10 είναι titan.cn.ece.ntua.gr.

## 2.5

Χρησιμοποιήθηκε το φίλτρο απεικόνισης «dns».

## 2.6

Χρησιμοποιήθηκε το UDP.

## 2.7

Έγιναν 3 αιτήματα προς εξυπηρέτηση DNS από τον υπολογιστή μας, προς τους εξυπηρετητές 147.102.1.1, 147.102.40.1 και 147.102.7.1 .

No.	Time	Source	Destination	Protocol	Length	Info
17	4.497812	147.102.131.41	147.102.1.1	DNS	84	Standard query 0x0001 PTR 1.1.102.147.in-addr.arpa
18	4.509310	147.102.1.1	147.102.131.41	DNS	125	Standard query response 0x0001 PTR 1.1.102.147.in-addr.arpa PTR theseas.softlab.ece.ntua.gr
24	13.518208	147.102.131.41	147.102.40.1	DNS	86	Standard query 0x0002 PTR 10.40.102.147.in-addr.arpa
25	13.530398	147.102.40.1	147.102.131.41	DNS	322	Standard query response 0x0002 PTR 10.40.102.147.in-addr.arpa PTR titan.cn.ece.ntua.gr NS achilles.noc.ntua.gr NS
29	16.015241	147.102.131.41	147.102.7.1	DNS	86	Standard query 0x0003 PTR 10.40.102.147.in-addr.arpa
30	16.026474	147.102.7.1	147.102.131.41	DNS	322	Standard query response 0x0003 PTR 10.40.102.147.in-addr.arpa PTR titan.cn.ece.ntua.gr NS ulysses.noc.ntua.gr NS

## 2.8

Ο πρώτος από τους προαναφερθέντες εξυπηρετητές DNS είναι ο default, ο 2ος είναι εκείνος που ζητήθηκε να διευθετήσει τη δεδομένη IP την πρώτη φορά και ο 3ος εκείνος που χρησιμοποιήθηκε την τελευταία φορά.

## 2.9

Επιλέγουμε ο πρώτο ζεύγος αιτήματος-απόκρισης:

Αίτημα: Θύρα προέλευσης: 51654 / Θύρα προορισμού: 53.

Απόκριση: Θύρα προέλευσης: 53 / Θύρα προορισμού: 51654.

## 2.10

Η θύρα 53.

## 2.11

Παρατηρούμε ότι η επικεφαλίδα DNS έχει μήκος 12 bytes.

### 2.12

Καταγράφουμε το Transaction ID των πακέτων 24 (πρώτο αίτημα για το 147.102.40.10) και 25 (απόκριση) με τιμές αντίστοιχα 0x0002 και 0x0002. Παρατηρούμε πως έχουν ίδιες τιμές.

### 2.13

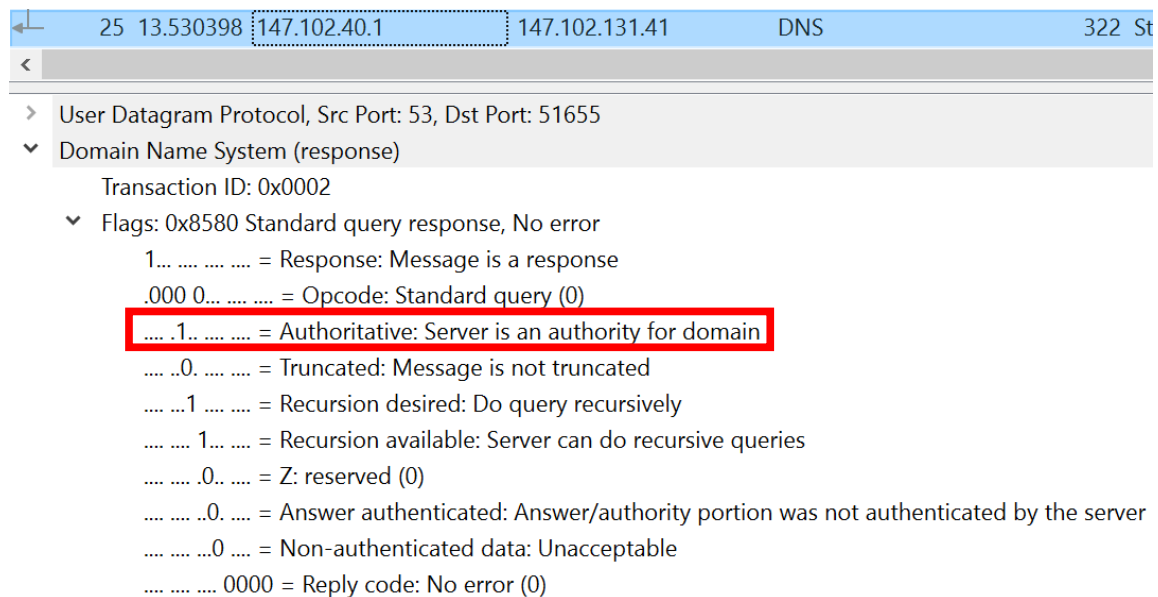
Το πεδίο flags καταλαμβάνει 2 bytes.

### 2.14

Το πρώτο bit του πεδίου Flags δηλώνει εάν το μήνυμα πρόκειται για query (0) ή response (1).

### 2.15

Το 6ο bit του πεδίου Flags δηλώνει ότι η απόκριση προέρχεται από επίσημο DNS Server.



25 13.530398 147.102.40.1 147.102.131.41 DNS 322 St

<

> User Datagram Protocol, Src Port: 53, Dst Port: 51655

▼ Domain Name System (response)

Transaction ID: 0x0002

▼ Flags: 0x8580 Standard query response, No error

- 1... .. = Response: Message is a response
- .000 0... .. = Opcode: Standard query (0)
- .... 1... .. = Authoritative: Server is an authority for domain
- .... 0... .. = Truncated: Message is not truncated
- .... 1... .. = Recursion desired: Do query recursively
- .... 1... .. = Recursion available: Server can do recursive queries
- .... 0... .. = Z: reserved (0)
- .... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
- .... 0... .. = Non-authenticated data: Unacceptable
- .... 0000 = Reply code: No error (0)

### 2.16

1 ερώτηση, 0 εγγραφές RR απαντήσεων, 0 εγγραφές επίσημων εξυπηρετητών και 0 επιπρόσθετες εγγραφές.

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0

### 2.17

Όπως βλέπουμε, στο επόμενο πακέτο (25) περιλαμβάνεται η ερώτηση την οποία αυτό απαντά.

```
Questions: 1
Answer RRs: 1
Authority RRs: 3
Additional RRs: 6
▼ Queries
  > 10.40.102.147.in-addr.arpa: type PTR, class IN
```

### 2.18

Περιλαμβάνει 1 εγγραφή RR απαντήσεων, 3 επίσημων εξυπηρετητών και 6 επιπρόσθετων.

### 2.19

Όχι δεν εμφανίστηκαν όλες.

### 2.20

Όπως βλέπουμε, το 6ο bit του πεδίου FLAGS είναι 0, άρα δεν προέρχεται από τον επίσημο εξυπηρετητή DNS.

```
30 16.026474 147.102.7.1 147.102.131.41 DNS
<
> User Datagram Protocol, Src Port: 53, Dst Port: 51656
▼ Domain Name System (response)
  Transaction ID: 0x0003
  ▼ Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... .0... .. = Authoritative: Server is not an authority for domain
```

### 2.21

Φίλτρο απεικόνισης «dns.flags.response == 1».

### 2.22

Όπως βλέπουμε το www.youtube.com έχει 16 IPv4 διευθύνσεις:

```

C:\Documents and Settings\labuser>nslookup
Default Server: achilles.noc.ntua.gr
Address: 147.102.222.210

> server 1.1.1.1
Default Server: one.one.one.one
Address: 1.1.1.1

> set domain=.
> set q=a
> www.youtube.com
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name: youtube-ui.l.google.com
Addresses: 142.251.140.78, 216.58.206.174, 216.58.213.110, 216.58.212.14
172.217.17.110, 142.251.140.46, 172.217.169.142, 172.217.17.142, 142.2
50.187.174
142.251.141.46, 142.251.140.14, 172.217.17.206, 216.58.212.46, 172.217
.20.78
172.217.169.206, 216.58.206.206
Aliases: www.youtube.com

```

## 2.23

Περιλαμβάνει 1 ερώτηση.

## 2.24

Στην παραπάνω απόκριση περιλαμβάνονται 17 Answer RRs, 0 Authority RRs και 0 Additional RRs.

13	24.078569	1.1.1.1	147.102.38.62	DNS
42	30.753788	1.1.1.1	147.102.38.62	DNS

- > Frame 13: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface \De
- > Ethernet II, Src: 08:ec:f5:d0:d9:1d, Dst: 00:11:25:f8:d6:e9
- > Internet Protocol Version 4, Src: 1.1.1.1, Dst: 147.102.38.62
- > User Datagram Protocol, Src Port: 53, Dst Port: 1379
- ▼ Domain Name System (response)
  - Transaction ID: 0x0003
  - > Flags: 0x8180 Standard query response, No error
  - Questions: 1
  - Answer RRs: 17
  - Authority RRs: 0

## 2.25

Από τις 17 εγγραφές RR απαντήσεων, οι 16 περιέχουν την IP του www.youtube.com ενώ η εναπομένουσα το κανονικό όνομα του ιστότοπου.



- ▼ Answers
  - > www.youtube.com: type CNAME, class IN, cname youtube-ui.l.google.com
  - > youtube-ui.l.google.com: type A, class IN, addr 142.251.140.14
  - > youtube-ui.l.google.com: type A, class IN, addr 216.58.212.14
  - > youtube-ui.l.google.com: type A, class IN, addr 142.251.140.78
  - > youtube-ui.l.google.com: type A, class IN, addr 172.217.20.78
  - > youtube-ui.l.google.com: type A, class IN, addr 216.58.214.142
  - > youtube-ui.l.google.com: type A, class IN, addr 172.217.169.110
  - > youtube-ui.l.google.com: type A, class IN, addr 172.217.169.142
  - > youtube-ui.l.google.com: type A, class IN, addr 216.58.212.46
  - > youtube-ui.l.google.com: type A, class IN, addr 142.250.184.142
  - > youtube-ui.l.google.com: type A, class IN, addr 216.58.206.206
  - > youtube-ui.l.google.com: type A, class IN, addr 172.217.17.142
  - > youtube-ui.l.google.com: type A, class IN, addr 142.251.141.46
  - > youtube-ui.l.google.com: type A, class IN, addr 172.217.17.206
  - > youtube-ui.l.google.com: type A, class IN, addr 216.58.206.174
  - > youtube-ui.l.google.com: type A, class IN, addr 216.58.213.110
  - > youtube-ui.l.google.com: type A, class IN, addr 142.251.140.46

## 2.26

Στην παραπάνω απόκριση υπάρχει και η εγγραφή CNAME προκειμένου να μας δώσει το κανονικό όνομα μιας και το `www.youtube.com` είναι alias.

## 2.27

Εφόσον λαμβάνουμε πολλές διαφορετικές IP συμπεραίνουμε πως φιλοξενείται από πολλούς υπολογιστές.

## 2.28

```
> set q=aaaa
> www.cnn.com
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net
cnn-tls.map.fastly.net AAAA IPv6 address = 2a04:4e42::773
cnn-tls.map.fastly.net AAAA IPv6 address = 2a04:4e42:200::773
cnn-tls.map.fastly.net AAAA IPv6 address = 2a04:4e42:400::773
cnn-tls.map.fastly.net AAAA IPv6 address = 2a04:4e42:600::773
```

Εντοπίζονται 5 Answer RRs (τέσσερις για τη διεύθυνση IPv6 και μία για το CNAME).

- ▼ Answers
  - > www.cnn.com: type CNAME, class IN, cname cnn-tls.map.fastly.net
  - > cnn-tls.map.fastly.net: type AAAA, class IN, addr 2a04:4e42::773
  - > cnn-tls.map.fastly.net: type AAAA, class IN, addr 2a04:4e42:200::773
  - > cnn-tls.map.fastly.net: type AAAA, class IN, addr 2a04:4e42:400::773
  - > cnn-tls.map.fastly.net: type AAAA, class IN, addr 2a04:4e42:600::773

## 2.29

Ένας εκ των εξυπηρετητών της παραπάνω απόκρισης είναι:

**Επίσημο όνομα/IPv6:** `cnn-tls.map.fastly.net / 2a04:4e42::773`

## 2.30

Παρατηρούμε το ακόλουθο ζεύγος ερωταπάντησης:

6	10.260792	147.102.38.62	147.102.222.210	DNS	80	Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
7	10.261165	147.102.222.210	147.102.38.62	DNS	335	Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa P

Το είδος της ερώτησης είναι η ζήτηση του domain name συσχετισμένο με την IP του (PTR records), προκειμένου να γίνει η αλλαγή του σέρβερ που μας εξυπηρετεί.

## 2.31

```
> server 8.8.8.8
Default Server: dns.google
Address: 8.8.8.8

> set q=any
> ntua.gr
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
ntua.gr
      primary name server = achilles.noc.ntua.gr
      responsible mail addr = noc.ntua.gr
      serial = 2022121501
      refresh = 43200 (12 hours)
      retry = 3600 (1 hour)
      expire = 604800 (7 days)
      default TTL = 86400 (1 day)
ntua.gr nameserver = sns0.grnet.gr
ntua.gr nameserver = sns1.grnet.gr
ntua.gr nameserver = diomedes.noc.ntua.gr
ntua.gr nameserver = achilles.noc.ntua.gr
ntua.gr nameserver = ulyssees.noc.ntua.gr
ntua.gr MX preference = 20, mail exchanger = diomedes.noc.ntua.gr
ntua.gr MX preference = 20, mail exchanger = ulyssees.noc.ntua.gr
ntua.gr MX preference = 20, mail exchanger = achilles.noc.ntua.gr
ntua.gr internet address = 147.102.222.101
ntua.gr AAAA IPv6 address = 2001:648:2000:de::210
ntua.gr text =
      "cisco-ci-domain-verification=4d4bf81f7a19cce571ce607bc70a79a2f923189b77
7c5bdc5e6b64e5d482be85 "
ntua.gr text =
      "google-site-verification=kka15C_ZY7VLA1Hb1hSnnPJvX0I5IYs6m2YCooFji7I"
ntua.gr text =
      "MS=ms79440458"
> set q=soa
> cslab.ntua.gr
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
cslab.ntua.gr
      primary name server = danaos.cslab.ece.ntua.gr
      responsible mail addr = root.danaos.cslab.ece.ntua.gr
      serial = 2022102600
      refresh = 21600 (6 hours)
      retry = 7200 (2 hours)
      expire = 720000 (8 days 8 hours)
      default TTL = 86400 (1 day)
> set q=cname
> www.cn.ntua.gr
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
www.cn.ntua.gr canonical name = www.cn.ece.ntua.gr
> set q=nx
> elab.ntua.gr
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
elab.ntua.gr MX preference = 20, mail exchanger = diomedes.noc.ntua.gr
elab.ntua.gr MX preference = 20, mail exchanger = achilles.noc.ntua.gr
elab.ntua.gr MX preference = 20, mail exchanger = ulyssees.noc.ntua.gr
> set q=txt
> telecom.ntua.gr
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
telecom.ntua.gr text =
      "v=spf1 ip4:147.102.222.0/24 ip4:147.102.7.1 ip6:2001:648:2000:de::/64 i
p6:2001:648:2000:7::/64 a -all"
telecom.ntua.gr text =
      "google-site-verification=Hb0wpc5iqVoDWmOfubp4saUokG9tW07_Gtr640cyUHo"
> set q=ns
> www.ntua.gr
Server: dns.google
Address: 8.8.8.8

ntua.gr
      primary name server = achilles.noc.ntua.gr
      responsible mail addr = noc.ntua.gr
      serial = 2022121501
      refresh = 43200 (12 hours)
      retry = 3600 (1 hour)
      expire = 604800 (7 days)
      default TTL = 86400 (1 day)
```

Περιέχει 14 Answer RRs, με τύπους: 1 SOA, 5 NS, 3 MX, 1 A, 1 AAAA, 3 TXT.

29	7.961084	8.8.8.8	147.102.38.62	DNS	525	Standard query response 0x000d ANY ntua.gr
> Frame 29: 525 bytes on wire (4200 bits), 525 bytes captured (4200 bits) on interface \Device\NPF_{6DB1BAA9-9537-4936-94A1-167676CF0541}, id 0						
> Ethernet II, Src: 08:ec:f5:d0:d9:1d, Dst: 00:11:25:f8:d6:e9						
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 147.102.38.62						
> User Datagram Protocol, Src Port: 53, Dst Port: 1410						
▼ Domain Name System (response)						
Transaction ID: 0x000d						
> Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 14						
Authority RRs: 0						
Additional RRs: 0						
▼ Answers						
> ntua.gr: type SOA, class IN, mname achilles.noc.ntua.gr						
> ntua.gr: type NS, class IN, ns sns0.gnet.gr						
> ntua.gr: type NS, class IN, ns sns1.gnet.gr						
> ntua.gr: type NS, class IN, ns diomedes.noc.ntua.gr						
> ntua.gr: type NS, class IN, ns achilles.noc.ntua.gr						
> ntua.gr: type NS, class IN, ns ulysses.noc.ntua.gr						
> ntua.gr: type MX, class IN, preference 20, mx diomedes.noc.ntua.gr						
> ntua.gr: type MX, class IN, preference 20, mx ulysses.noc.ntua.gr						
> ntua.gr: type MX, class IN, preference 20, mx achilles.noc.ntua.gr						
> ntua.gr: type A, class IN, addr 147.102.224.101						
> ntua.gr: type AAAA, class IN, addr 2001:648:2000:de::210						
> ntua.gr: type TXT, class IN						
> ntua.gr: type TXT, class IN						
> ntua.gr: type TXT, class IN						

## 2.32

Περιέχει 1 Answer RRs τύπου SOA.

31	13.500305	8.8.8.8	147.102.38.62	DNS	131	Standard query response 0x000e SOA cslab.ntua.gr SOA danaos.cslab.ece.ntua.gr
> Frame 31: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface \Device\NPF_{6DB1BAA9-9537-4936-94A1-167676CF0541}, id 0						
> Ethernet II, Src: 08:ec:f5:d0:d9:1d, Dst: 00:11:25:f8:d6:e9						
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 147.102.38.62						
> User Datagram Protocol, Src Port: 53, Dst Port: 1411						
▼ Domain Name System (response)						
Transaction ID: 0x000e						
> Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 1						
Authority RRs: 0						
Additional RRs: 0						
> Queries						
▼ Answers						
> cslab.ntua.gr: type SOA, class IN, mname danaos.cslab.ece.ntua.gr						

## 2.33

Όπως βλέπουμε, το όνομα του κύριου εξυπηρετητή DNS της περιοχής cslab.ntua.gr είναι danaos.cslab.ece.ntua.gr, ενώ η διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστή αυτής είναι root.danaos.cslab.ece.ntua.gr

Primary name server: danaos.cslab.ece.ntua.gr  
Responsible authority's mailbox: root.danaos.cslab.ece.ntua.gr

### 2.34

Περιέχει 1 Answer RRs, με κανονικό όνομα `www.cn.ntua.gr` και διάρκεια ζωής 20 λεπτά.

36	16.633718	8.8.8.8	147.102.38.62	DNS	99	Standard query response 0x000f CNAME www.cn.ntua.gr CNAME www.ece.ntua.gr
> Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 1						
Authority RRs: 0						
Additional RRs: 0						
> Queries						
▼ Answers						
▼ www.cn.ntua.gr: type CNAME, class IN, cname www.ece.ntua.gr						
Name: www.cn.ntua.gr						
Type: CNAME (Canonical NAME for an alias) (5)						
Class: IN (0x0001)						
Time to live: 1200 (20 minutes)						
Data length: 13						
CNAME: www.ece.ntua.gr						

### 2.35

Η απόκριση σχετικά με τους αρμόδιους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής `elab.ntua.gr` περιλαμβάνει 3 Answer RRs, 0 Authority RRs και 0 Additional RRs. Σχετικά με τον προτιμότερο, παρατηρούμε πως και οι 3 πιθανοί έχουν ίδιο MX ίσο με 20, επομένως είναι και οι 3 το ίδιο προτιμητέοι (`diomedes.noc.ntua.gr`, `achilles.noc.ntua.gr`, `ulysses.noc.ntua.gr`).

51	18.677153	8.8.8.8	147.102.38.62	DNS	150	Standard query response 0x0010 MX elab.ntua.gr MX
Frame 51: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{6DB1BAA9-9537-4936-94A1-167676CF0541}, id 0						
Ethernet II, Src: 08:ec:f5:d0:d9:1d, Dst: 00:11:25:f8:d6:e9						
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 147.102.38.62						
User Datagram Protocol, Src Port: 53, Dst Port: 1413						
Domain Name System (response)						
Transaction ID: 0x0010						
> Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 3						
Authority RRs: 0						
Additional RRs: 0						
> Queries						
▼ Answers						
> elab.ntua.gr: type MX, class IN, preference 20, mx diomedes.noc.ntua.gr						
> elab.ntua.gr: type MX, class IN, preference 20, mx achilles.noc.ntua.gr						
> elab.ntua.gr: type MX, class IN, preference 20, mx ulysses.noc.ntua.gr						

### 2.36

Η απόκριση του `telecom.ntua.gr` περιλαμβάνει 2 Answers RRs. Μία από τις εγγραφές TXT (η πρώτη) έχει μήκος, σε byte, 114, ενώ το μήκος της πληροφορίας είναι 101.

53	20.813895	8.8.8.8	147.102.38.62	DNS	270	Standard query response 0x0011 TXT telecom.ntua.gr TXT TXT
Transaction ID: 0x0011						
> Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 2						
Authority RRs: 0						
Additional RRs: 0						
> Queries						
▼ Answers						
▼ telecom.ntua.gr: type TXT, class IN						
Name: telecom.ntua.gr						
Type: TXT (Text strings) (16)						
Class: IN (0x0001)						
Time to live: 20600 (5 hours, 43 minutes, 20 seconds)						
Data length: 102						
TXT Length: 101						
TXT: v=spf1 ip4:147.102.222.0/24 ip4:147.102.7.1 ip6:2001:648:2000:de::/64 ip6:2001:648:2000:7::/64 a -all						
> telecom.ntua.gr: type TXT, class IN						

## 2.37

Η απόκριση του `www.ntua.gr` περιλαμβάνει 0 Answers RRs, 1 Authority RRs και 0 Additional RRs. Συμπεραίνουμε ότι η απόκριση παραπέμπει στην αρχή πληροφόρησης για την περιοχή `ntua.gr`, που σημαίνει πώς ο `Achilles.noc.ntua.gr` είναι ο υπεύθυνος εξυπηρετητής και για τα δύο domains.

61	23.894364	8.8.8.8	147.102.38.62	DNS	120	Standard query response 0x0012 NS www.ntua.gr SOA achilles.noc.ntua.gr
> Frame 61: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface \Device\NPF_{6DB1BAA9-9537-4936-94A1-167676CF0541}, id 0						
> Ethernet II, Src: 08:ec:f5:d0:d9:1d, Dst: 00:11:25:f8:d6:e9						
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 147.102.38.62						
> User Datagram Protocol, Src Port: 53, Dst Port: 1415						
▼ Domain Name System (response)						
Transaction ID: 0x0012						
> Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 0						
Authority RRs: 1						
Additional RRs: 0						
> Queries						
▼ Authoritative nameservers						
> ntua.gr: type SOA, class IN, mname achilles.noc.ntua.gr						

## 2.38

```
> server 147.102.222.210
Default Server: achilles.noc.ntua.gr
Address: 147.102.222.210

> ls -d planetlab.ntua.grss
[achilles.noc.ntua.gr]
*** Can't list domain planetlab.ntua.grss: BAD ERROR VALUE
> exit

C:\Documents and Settings\labuser>nslookup
Default Server: achilles.noc.ntua.gr
Address: 147.102.222.210

> server 147.102.222.210
Default Server: achilles.noc.ntua.gr
Address: 147.102.222.210

> ls -d planetlab.ntua.gr
[achilles.noc.ntua.gr]
planetlab.ntua.gr. SOA achilles.noc.ntua.gr noc.ntua.gr. (200707
2300 43200 3600 604800 86400)
planetlab.ntua.gr. NS ulysses.noc.ntua.gr
planetlab.ntua.gr. NS achilles.noc.ntua.gr
planetlab.ntua.gr. NS diomedes.noc.ntua.gr
stella A 147.102.224.228
stella-man A 147.102.224.230
vicky A 147.102.224.227
vicky-man A 147.102.224.229
planetlab.ntua.gr. SOA achilles.noc.ntua.gr noc.ntua.gr. (200707
2300 43200 3600 604800 86400)
```

dns						
No.	Time	Source	Destination	Protocol	Length	Info
2	1.537327	147.102.38.62	147.102.222.210	DNS	88	Standard query 0x0001 PTR 210.222.102.147.in-addr.arpa
3	1.537606	147.102.222.210	147.102.38.62	DNS	313	Standard query response 0x0001 PTR 210.222.102.147.in-addr.arpa PTR achilles.noc.ntua.gr
4	4.132346	147.102.38.62	147.102.222.210	DNS	88	Standard query 0x0002 PTR 210.222.102.147.in-addr.arpa
5	4.132641	147.102.222.210	147.102.38.62	DNS	313	Standard query response 0x0002 PTR 210.222.102.147.in-addr.arpa PTR achilles.noc.ntua.gr
49	10.917876	147.102.38.62	147.102.222.210	DNS	91	Standard query 0x0003 AXFR planetlab.ntua.gr
50	10.918295	147.102.222.210	147.102.38.62	DNS	140	Standard query response 0x0003 AXFR planetlab.ntua.gr SOA achilles.noc.ntua.gr
52	11.046890	147.102.222.210	147.102.38.62	DNS	529	Standard query response 0x0003 SOA achilles.noc.ntua.gr

Έχουμε τα εξής:

Είδος Μηνύματος	Θύρα Προέλευσης	Θύρα Προορισμού
Αίτημα	1442	53
Απόκριση 1	53	1442
Απόκριση 2	53	1442

**2.40**

Το αίτημα έχει μήκος 39 bytes.

No.	Time	Source IP	Destination IP	Protocol	Length	Info
49	10.917876	147.102.38.62	147.102.222.210	DNS	91	Standard query 0x0003 AXFR planetlab.ntua.gr
50	10.918295	147.102.222.210	147.102.38.62	DNS	140	Standard query response 0x0003 AXFR planetlab.ntua.gr
52	11.046890	147.102.222.210	147.102.38.62	DNS	529	Standard query response 0x0003 SOA achilles.noc.ntua.gr

- > Frame 49: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface Vde0
- > Ethernet II, Src: 00:11:25:f8:d6:e9, Dst: 00:00:5e:00:01:25
- > Internet Protocol Version 4, Src: 147.102.38.62, Dst: 147.102.222.210
- > Transmission Control Protocol, Src Port: 1442, Dst Port: 53, Seq: 3, Ack: 1, Len: 37
- > [2 Reassembled TCP Segments (39 bytes): #47(2), #49(37)]
- > Domain Name System (query)

```

0000  00 25 00 03 01 00 00 01 00 00 00 00 00 09 70  %-.....p
0010  6c 61 6e 65 74 6c 61 62 04 6e 74 75 61 02 67 72  lanetlab.ntua.gr
0020  00 00 fc 00 01 4d 53                               ....MS
    
```

**2.41**

Το αίτημα είναι τύπου AXFR. Αυτός ο τύπος μηνυμάτων χρησιμοποιείται όταν μια δευτερεύουσα βάση (ο πελάτης) ζητάει δεδομένα από μια κύρια βάση (εξυπηρετητής) σε αυτή την επικοινωνία μεταξύ εξυπηρετητών που όμως μοιάζει με επικοινωνία πελάτη εξυπηρετητή.

- Queries
  - planetlab.ntua.gr: type AXFR, class IN

## 2.42

Η πρώτη απάντηση έχει μήκος 140 bytes και μεταφέρει 1 DNS response μήνυμα, ενώ η δεύτερη απάντηση έχει μήκος 529 bytes και μεταφέρει 8 DNS responses.

## 2.43

Καταλαβαίνουμε ότι αποτελούν απάντηση στο αίτημα που έγινε καθώς έχουν το ίδιο Transaction ID.

## 2.44

Η 1η απάντηση περιλαμβάνει 1 ερώτηση (question) και 1 Answer RR, ενώ κάθε μήνυμα της 2ης απάντησης περιλαμβάνει από 1 Answer RR.

## 2.45

Χρησιμοποιείται το TCP αντί του UDP (παρόλο που υποστηρίζεται και το 2ο), καθώς το UDP είναι επιρρεπές σε ρίσκο απώλειας πακέτων ή packet spoofing.

## 2.46

Πρέπει να χρησιμοποιήσουμε το φίλτρο σύλληψης «port 53»

## 2.47

**1<sup>ο</sup> byte:** c0 (192<sub>10</sub>)

**11<sup>ο</sup> byte:** 00 (0<sub>10</sub>)

**4<sup>ο</sup> από το τέλος byte:** 00 (0<sub>10</sub>)

**Τελευταίο byte:** 80 (128<sub>10</sub>)

Offset	Hex	ASCII
0040	00 00 00 00 09 70 6c 61 6e 65 74 6c 61 62 04 6e	.....pla netlab n
0050	74 75 61 02 67 72 00 00 fc 00 01 c0 0c 00 06 00	tua gr.....
0060	01 00 01 51 80 00 25 08 61 63 68 69 6c 6c 65 73	...Q...%... achilles
0070	03 6e 6f 63 c0 16 c0 38 77 a1 7e 2c 00 00 a8 c0	...noc...8 w...;
0080	00 00 0e 10 00 09 3a 80 00 01 51 80	.....:Q...

Αφού το πρώτο byte ξεκινάει με τιμή 192<sub>10</sub> (11000000<sub>2</sub>), τότε έχουμε pointer με offset 12<sub>10</sub> (00000000001100<sub>2</sub>) που σημαίνει ότι το όνομα έχει αναφερθεί στο offset 12 του μηνύματος απάντησης (ξεκινώντας το μέτρημα από το πρώτο byte που ακολουθεί από το Transaction ID). Τα υπόλοιπα bytes της ερώτησης δεν μας αφορούν καθώς χρησιμοποιήθηκε compression, άρα δεν έχουν σχέση με κάποιο όνομα.

## 2.48

Έχουμε πάλι compression. Τα δύο τελευταία byte δηλώνουν ότι το μέρος “ntua.gr” έχει δηλωθεί προηγουμένως στο offset 22 του μηνύματος απάντησης, αφού το c0 δηλώνει χρήση pointer (c0<sub>16</sub> 16<sub>16</sub> = 192<sub>10</sub> 22<sub>10</sub> = 11000000<sub>2</sub> 00010110<sub>2</sub>).



Time to live: 86400 (1 day)  
 Data length: 37  
 Primary name server: achilles.noc.ntua.gr

0060	01 00 01 51 80 00 25 08 61 63 68 69 6c 6c 65 73	...Q...% achille
0070	03 6e 6f 63 c0 16 c0 38 77 a1 7e 2c 00 00 a8 c0	...noc...8 w... ,...
0080	00 00 0e 10 00 09 3a 80 00 01 51 80	.....:Q

## 2.49

Έχουμε πάλι compression. Τα bytes που επιλέχθηκαν στα περιεχόμενα έχουν τιμές  $c0_{16}$   $38_{16} = 192_{10}$   $56_{10} = 11000000_2$   $00111000_2$ , δηλαδή το mail έχει ξαναδηλωθεί στο offset 56 του μηνύματος απόκρισης, το οποίο βρίσκεται στο πεδίο του primary name server (μόνο τα bytes που περιέχουν το όνομα noc.ntua.gr, από τα οποία όπως είδαμε παραπάνω το όνομα ntua.gr δηλώνεται και αυτό με pointer).

Data length: 37  
 Primary name server: achilles.noc.ntua.gr  
 Responsible authority's mailbox: noc.ntua.gr

0060	01 00 01 51 80 00 25 08 61 63 68 69 6c 6c 65 73	...Q...% achilles
0070	03 6e 6f 63 c0 16 c0 38 77 a1 7e 2c 00 00 a8 c0	...noc...8 w... ,...
0080	00 00 0e 10 00 09 3a 80 00 01 51 80	.....:Q