



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Δίκτυα Υπολογιστών

Αναφορά 10ης Εργαστηριακής Άσκησης

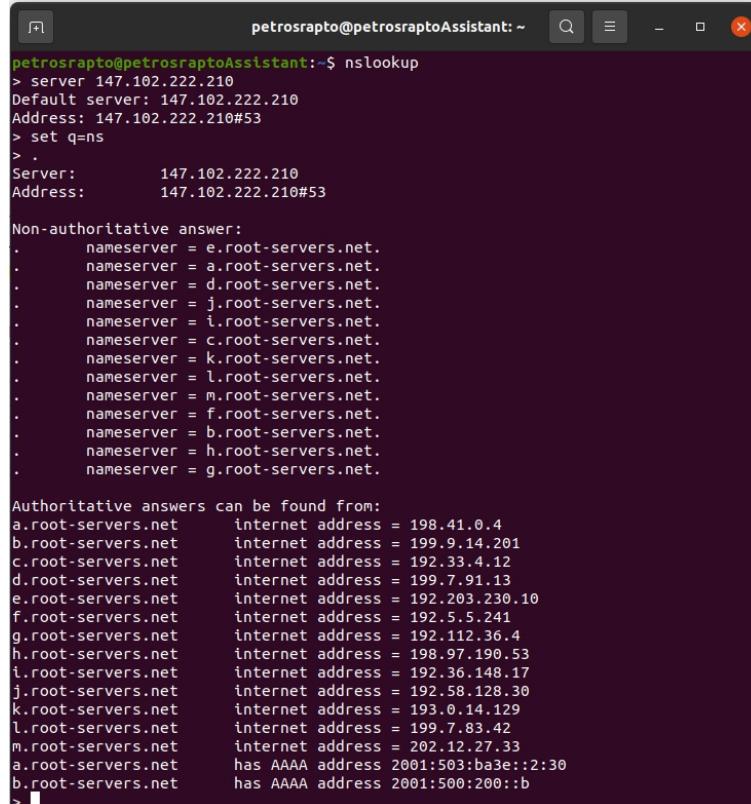
**Ραπτόπουλος Πέτρος (ει19145)
Ομάδα 3**

Άσκηση 1: Υπηρεσία DNS

Ανοίγουμε ένα παράθυρο εντολών και πληκτρολογούμε nslookup ακολουθούμενο από <Enter>.

Στη συνέχεια πληκτρολογούμε server 147.102.222.210 για να επιλέξουμε τον εξυπηρετητή DNS που θα απαντά στη συνέχεια. Μέσω της υπο-εντολής set querytype μπορούμε να προσδιορίσουμε το είδος πληροφοριών που θα αντλήσουμε από τον εξυπηρετητή DNS. Προκειμένου να βρούμε πληροφορίες σχετικές με τους υπεύθυνους εξυπηρετητές μιας περιοχής DNS χρησιμοποιούμε την υπο-εντολή set q=ns.

1.1) Πληκτρολογήστε μια τελεία '.' και μετά <Enter>. Σε ποια περιοχή (στάθμη του Σχήματος 1) ανήκουν οι εξυπηρετητές DNS που εμφανίζονται; **Ανήκουν στην περιοχή της ρίζας (root level) (εξυπηρετητές κορυφής)**



```
petrosrapto@petrosraptoAssistant:~$ nslookup
> server 147.102.222.210
Default server: 147.102.222.210#53
Address: 147.102.222.210#53
> set q=ns
> .
Server:      147.102.222.210
Address:     147.102.222.210#53

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

Authoritative answers can be found from:
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      has AAAA address 2001:503:ba3e::2:30
b.root-servers.net      has AAAA address 2001:500:200::b
>
```

1.2) Καταγράψτε το πλήθος των υπεύθυνων εξυπηρετητών DNS που εμφανίστηκαν: **13**

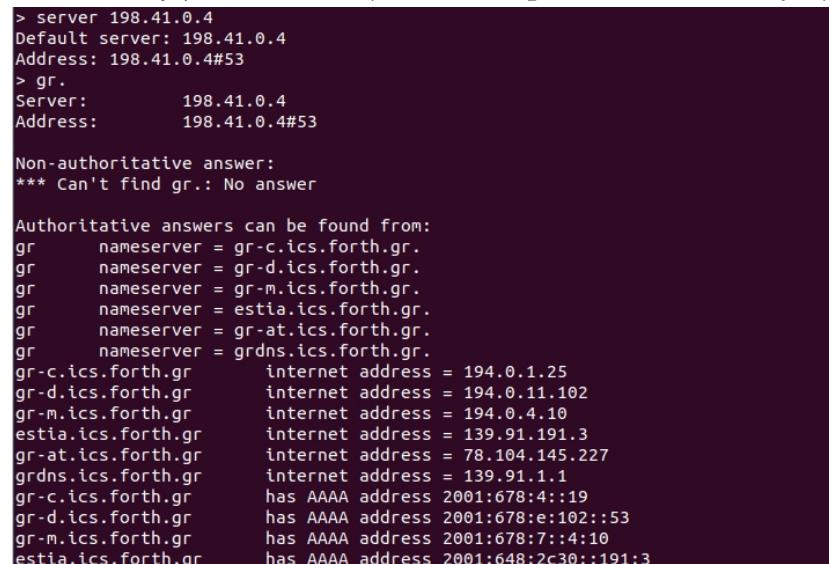
καθώς και το όνομα: **a.root-servers.net**

και τη διεύθυνση IPv4: **198.41.0.4**

και IPv6 εγός μόνο από αυτούς: **2001:503:ba3e::2:30**

1.3) Πληκτρολογήστε μια εντολή ώστε να επιλέξετε ως εξυπηρετητή DNS που θα απαντά στα επόμενα τον εξυπηρετητή του προηγούμενου ερωτήματος. Ποια είναι η σύνταξη της εντολής; **server 198.41.0.4**

1.4) Στη συνέχεια, πληκτρολογήστε 'gr.', προσοχή στην τελεία στο τέλος. Σε ποια περιοχή (στάθμη του Σχήματος 1) ανήκουν οι εξυπηρετητές DNS που εμφανίζονται; **Ανήκουν στο Top Domain Level (περιοχή gr)**



```
> server 198.41.0.4
Default server: 198.41.0.4
Address: 198.41.0.4#53
> gr.
Server:      198.41.0.4
Address:     198.41.0.4#53

Non-authoritative answer:
*** Can't find gr.: No answer

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

1.5) Καταγράψτε το πλήθος των υπεύθυνων εξυπηρετητών DNS για την περιοχή 'gr.': 6

καθώς και το όνομα: **gr-c.ics.forth.gr**

και τη διεύθυνση IPv4: **194.0.1.25**

και IPv6 ενός μόνο από αυτούς: **2001:678:4::19**

1.6) Πληκτρολογήστε τώρα 'ntua.gr.'. Τι αποτελέσματα λαμβάνετε σε σύγκριση με αυτά του ερωτήματος 1.4 και τι συμπεραίνετε για το τι απαντούν οι εξυπηρετητές κορυφής; Δαμβάνουμε την ίδια απόκριση με το ερώτημα 1.4.

Συμπεραίνουμε ότι οι εξυπηρετητές κορυφής υποδεικνύουν τους εξυπηρετητές DNS για την περιοχή ανωτάτου επιπέδου που ζητήθηκε.

```
> ntua.gr.
Server:          198.41.0.4
Address:         198.41.0.4#53

Non-authoritative answer:
*** Can't find ntua.gr.: No answer

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

1.7) Επιλέξτε ως εξυπηρετητή DNS που θα απαντά στα επόμενα έναν από αυτούς της απάντησης που λάβατε στο προηγούμενο ερώτημα. Γράψτε τη σύνταξη της εντολής. server 194.0.1.25

1.8) Πληκτρολογήστε τώρα 'ntua.gr.'. Η απάντηση που λαμβάνετε είναι ίδια με αυτήν που είδατε στην ερώτηση 1.6; Εξηγήστε γιατί. Όχι δεν είναι η ίδια. Προηγουμένως ο εξυπηρετητής κορυφής που ερωτήθηκε υπέδειξε τον εξυπηρετητή περιοχής ανωτάτου επιπέδου που είναι σε θέση να απαντήσει. Ρωτώντας τώρα έναν από τους εξυπηρετητές αυτούς, επιστρέφεται η ζητούμενη πληροφορία.

```
> server 194.0.1.25
Default server: 194.0.1.25
Address: 194.0.1.25#53
> ntua.gr.
Server:          194.0.1.25
Address:         194.0.1.25#53

Non-authoritative answer:
*** Can't find ntua.gr.: No answer

Authoritative answers can be found from:
ntua.gr nameserver = sns0.grnet.gr.
ntua.gr nameserver = sns1.grnet.gr.
ntua.gr nameserver = ulysses.noc.ntua.gr.
ntua.gr nameserver = achilles.noc.ntua.gr.
ntua.gr nameserver = diomedes.noc.ntua.gr.
achilles.noc.ntua.gr      internet address = 147.102.222.210
diomedes.noc.ntua.gr     internet address = 147.102.222.220
ulysses.noc.ntua.gr      internet address = 147.102.222.230
```

1.9) Καταγράψτε το πλήθος των υπεύθυνων εξυπηρετητών DNS για την περιοχή 'ntua.gr.': 5

καθώς και το όνομα: **achilles.noc.ntua.gr**

και τη διεύθυνση IPv4 ενός μόνο από αυτούς: **147.102.222.210**

1.10) Κατόπιν, επιλέξτε ως εξυπηρετητή DNS αυτόν το όνομα του οποίου καταγράψατε προηγουμένως.

Πληκτρολογήστε και πάλι 'ntua.gr.'. Η απάντηση που λαμβάνετε είναι ίδια με αυτήν που είδατε στην ερώτηση 1.8;

Δεν είναι ακριβώς ίδια. Παρατηρούμε ότι επιστρέφονται

τα ονόματα των εξυπηρετητών που κατέχουν την

ζητούμενη πληροφορία, ωστόσο δεν εμφανίζονται οι

διευθύνσεις IPv4 αυτών όπως προηγουμένως.

```
> server 147.102.222.210
Default server: 147.102.222.210
Address: 147.102.222.210#53
> ntua.gr.
Server:          147.102.222.210
Address:         147.102.222.210#53

ntua.gr nameserver = sns0.grnet.gr.
ntua.gr nameserver = achilles.noc.ntua.gr.
ntua.gr nameserver = diomedes.noc.ntua.gr.
ntua.gr nameserver = ulysses.noc.ntua.gr.
ntua.gr nameserver = sns1.grnet.gr.
```

1.11) Πληκτρολογήστε το όνομα της περιοχής του Εργαστηρίου Δικτύων Υπολογιστών του Ε.Μ.Π. ‘cn.ntua.gr.’ και καταγράψτε το πλήθος των υπεύθυνων εξυπηρετητών DNS: 3

καθώς και το όνομα: **psyche.cn.ece.ntua.gr**

ενός από αυτούς που να μην ταυτίζεται με κάποιον από τους εξυπηρετητές της ερώτησης 1.9.

```
> cn.ntua.gr
Server:          147.102.222.210
Address:         147.102.222.210#53

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.
```

1.12) Βρείτε τα ονόματα των υπεύθυνων εξυπηρετητών DNS για δύο περιοχές Σχολών του ΕΜΠ, η μία εκ των οποίων να είναι κάποια εκ των MMM ή ATM. Τι παρατηρείτε; Παρατηρούμε ότι υπάρχουν κοινοί υπεύθυνοι εξυπηρετητές DNS ανάμεσα σε διαφορετικές σχολές. Ωστόσο παρατηρούμε και έναν εξυπηρετητή που δεν είναι κοινός.

```
> ece.ntua.gr.
Server:          147.102.222.210
Address:         147.102.222.210#53
Σχολ

ece.ntua.gr      nameserver = achilles.noc.ntua.gr.
ece.ntua.gr      nameserver = ulysses.noc.ntua.gr.
ece.ntua.gr      nameserver = diomedes.noc.ntua.gr.
> metal.ntua.gr.
Server:          147.102.222.210
Address:         147.102.222.210#53

metal.ntua.gr    nameserver = ulysses.noc.ntua.gr.
metal.ntua.gr    nameserver = serifos.metal.ntua.gr.
metal.ntua.gr    nameserver = diomedes.noc.ntua.gr.
metal.ntua.gr    nameserver = achilles.noc.ntua.gr.
```

1.13) Καταγράψτε τον κύριο εξυπηρετητή DNS της περιοχής ‘cn.ntua.gr.’: **psyche.cn.ece.ntua.gr την IPv4 διεύθυνσή του: **147.102.40.1** καθώς και τον σειριακό αριθμό: **2022120501****

```
> set q=soa
> cn.ntua.gr.
Server:          147.102.222.210
Address:         147.102.222.210#53

cn.ntua.gr
origin = psyche.cn.ece.ntua.gr
mail addr = hostmaster.cn.ntua.gr
serial = 2022120501
refresh = 28800
retry = 7200
expire = 604800
minimum = 86400
```

```
> server psyche.cn.ece.ntua.gr
Default server: psyche.cn.ece.ntua.gr
Address: 147.102.40.1#53
Default server: psyche.cn.ece.ntua.gr
Address: 2001:648:2000:28::1#53
```

1.14) Κάθε πόσες ώρες θα αναζητήσει αλλαγές σχετικά με την περιοχή ‘cn.ntua.gr.’ ένας δευτερεύων εξυπηρετητής; 8

1.15) Για πόσες ώρες διατηρούνται οι σχετικές με την περιοχή ‘cn.ntua.gr.’ εγγραφές στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών; 24

1.16) Επαναλάβετε τις ερωτήσεις 1.13 ως 1.15 για την περιοχή ‘ece.ntua.gr.’ της σχολής HMMY του ΕΜΠ.

```
> ece.ntua.gr.
Server:          147.102.222.210
Address:         147.102.222.210#53

ece.ntua.gr
origin = achilles.noc.ntua.gr
mail addr = noc.ntua.gr
serial = 2022101000
refresh = 86400
retry = 86400
expire = 86400
minimum = 86400
```

```
> server achilles.noc.ntua.gr
Default server: achilles.noc.ntua.gr
Address: 147.102.222.210#53
Default server: achilles.noc.ntua.gr
Address: 2001:648:2000:de::210#53
```

1.13) **achilles.noc.ntua.gr**

147.102.222.210

2022101000

1.14) 24

1.15) 24

1.17) Από τις τιμές των σειριακών αριθμών που καταγράψατε, μπορείτε να διακρίνετε κάποιο κανόνα σχετικό με το πώς μπορούν να παραχθούν αυτές, πλην του προφανούς της αύξησης κατά 1 κάθε φορά που γίνεται ενημέρωση των εγγραφών RR; **Ίσως να αποθηκεύεται η ημερομηνία ενημέρωσης των αντίστοιχων εγγραφών.** (πχ 2022-10-1)

1.18) Αναζητήστε στο διαδίκτυο και βρείτε τα ονόματα εξυπηρετητών ιστού τριών ελληνικών πανεπιστημάτων.

ΕΜΠ: ntua.gr, **ΕΚΠΑ:** uoa.gr, **ΑΠΘ:** auth.gr

Καταγράψτε τα ονόματα και τις διευθύνσεις IPv4 (και IPv6 εάν διαθέτουν) αυτών των εξυπηρετητών ιστού.

ntua.gr - 147.102.224.101 - 2001:648:2000:de::210

uoa.gr - 195.134.71.229

auth.gr - 155.207.1.12

1.19) Βρείτε και καταγράψτε το όνομα για δύο διευθύνσεις IPv4 (της προτίμησής σας) στο υποδίκτυο 147.102.40.16/29.

```
> set q=ptr
> 147.102.40.17
Server:          147.102.222.210
Address:         147.102.222.210#53

17.40.102.147.in-addr.arpa      name = pegasus.cn.ece.ntua.gr.
> 147.102.40.18
Server:          147.102.222.210
Address:         147.102.222.210#53

18.40.102.147.in-addr.arpa      name = bbb.cn.ece.ntua.gr.
```

1.20) Αφού παρατηρήσετε την απόκριση του εξυπηρετητή στο προηγούμενο αίτημα, καταγράψετε τη μορφή αναπαράστασης της διεύθυνσης IPv4, η οποία χρησιμοποιείται από το σύστημα ονοματοδότησης. Έχει τη συνήθη αριθμητική μορφή μιας διεύθυνσης IPv4; **Ναι με την προσθήκη της κατάληξης .in-addr.arpa η ο οποία χρησιμοποιείται από το σύστημα DNS ώστε να αντιστοιχιστούν διευθύνσεις IPv4 με ονόματα εξυπηρετητών.**

1.21) Καταγράψτε το κανονικό όνομα και τη διεύθυνση IPv4 του υπολογιστή που φιλοξενεί την ιστοθέση της Σχολής ΜΜΜ του Ε.Μ.Π.

```
> set q cname
> metal.ntua.gr.
Server:          147.102.222.210
Address:         147.102.222.210#53

*** Can't find metal.ntua.gr.: No answer
```

1.22) Καταγράψτε τα ονόματα και τις διευθύνσεις IPv4 δύο εκ των εξυπηρετητών ηλεκτρονικού ταχυδρομείου της περιοχής 'arch.ntua.gr.'

```
> set q=mx
> arch.ntua.gr.
Server:          147.102.222.210
Address:         147.102.222.210#53

arch.ntua.gr    mail exchanger = 100 diomedes.noc.ntua.gr.
arch.ntua.gr    mail exchanger = 10 f1.mail.ntua.gr.
arch.ntua.gr    mail exchanger = 10 f0.mail.ntua.gr.
arch.ntua.gr    mail exchanger = 100 ulysses.noc.ntua.gr.
arch.ntua.gr    mail exchanger = 100 achilles.noc.ntua.gr.
> server ulysses.noc.ntua.gr
Default server: ulysses.noc.ntua.gr
Address: 147.102.222.230#53
Default server: ulysses.noc.ntua.gr
Address: 2001:648:2000:de::230#53
> server achilles.noc.ntua.gr
Default server: achilles.noc.ntua.gr
Address: 147.102.222.210#53
Default server: achilles.noc.ntua.gr
Address: 2001:648:2000:de::210#53
```

1.23) Ποιος από τους εξυπηρετητές είναι ο πρώτος που θα προτιμηθεί για την παράδοση ηλεκτρονικού ταχυδρομείου και γιατί; **Είτε o fo.mail.ntua.gr είτε o fi.mail.ntua.gr διότι έχουν τον χαμηλότερο αριθμό προτίμησης.**

1.24) Αφού εξέλθετε της nslookup με exit, πληκτρολογήστε dig axfr central.ntua.gr @147.102.222.210.

Τι σημαίνει το axfr; **Σημαίνει "Authoritative Zone Transfer" και μεταφέρει ολόκληρη ζώνη αρχείων από τον πρωτεύοντα εξυπηρετητή σε δευτερεύοντα εξυπηρετητή.**

1.25) Για κάθε είδος εγγραφής (π.χ. NS, MX, A, AAAA, CNAME, HINFO, TXT, SOA, κλπ.) που θα συναντήσετε στην απάντηση της προηγούμενης ερώτησης καταγράψτε τα πλήρη στοιχεία μίας περίπτωσης.

```
petrosrapto@petrosraptoAssistant:~$ dig axfr central.ntua.gr @147.102.222.210
; <>> DiG 9.16.1-Ubuntu <>> axfr central.ntua.gr @147.102.222.210
;; global options: +cmd
central.ntua.gr. 86400 IN SOA netsrv0.central.ntua.gr. dnsmastr
er.central.ntua.gr. 180 21600 1800 604800 900
central.ntua.gr. 3600 IN TXT "v=spf1 ip4:147.102.222.0/24 ip6
:2001:648:2000:de::/64 a -all"
central.ntua.gr. 86400 IN MX 10 ulysses.noc.ntua.gr.
central.ntua.gr. 86400 IN NS netsrv0.central.ntua.gr.
```

central.ntua.gr.	86400	IN	A	147.102.222.46
acadinfo.central.ntua.gr.	86400	IN	CNAME	beta.central.ntua.gr.

Άσκηση 2: Πρωτόκολλο DNS

Με τη βοήθεια του Wireshark καταγράφουμε την κίνηση ενώ κάνουμε χρήση της υπηρεσίας DNS. Εφαρμόζουμε φίλτρο σύλληψης για να παρατηρούμε μόνο την κίνηση που σχετίζεται με τη διεύθυνση IP του υπολογιστή σας και ξεκινήστε την καταγραφή. Καθαρίζουμε την προσωρινή μνήμη DNS. Στη συνέχεια:

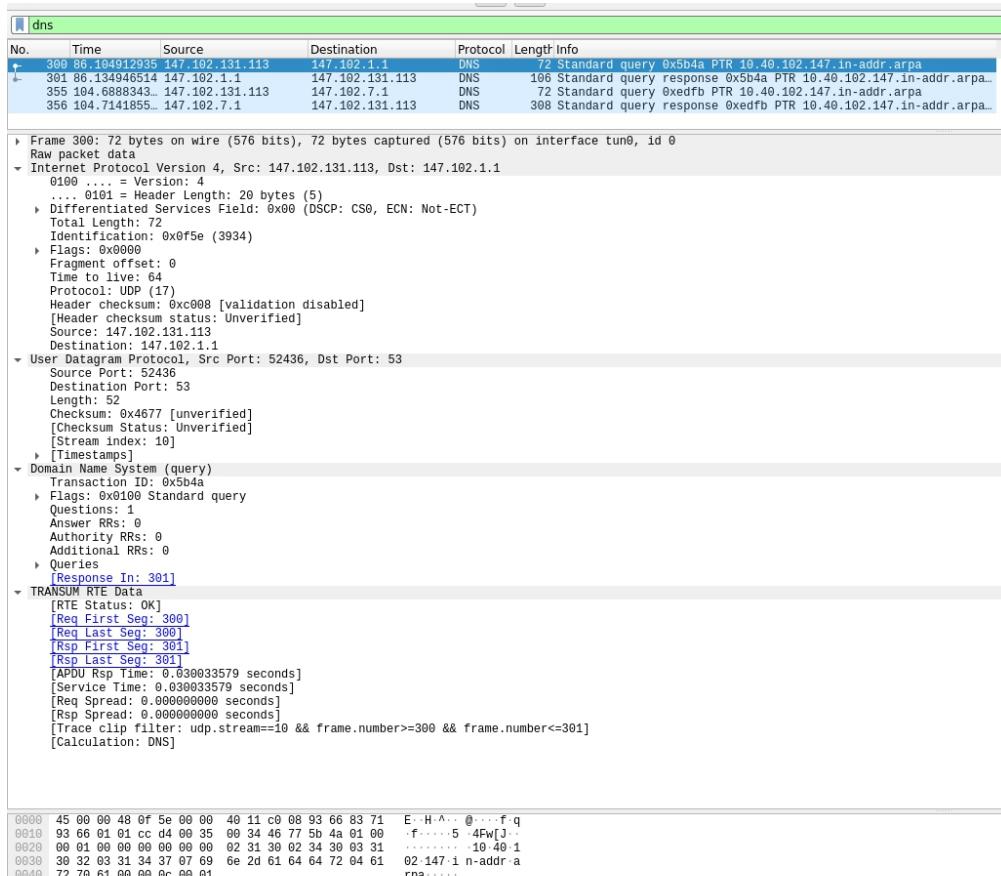
```
petrosrapt0@petrosrapt0Assistant:~$ sudo systemd-resolve --flush-caches
petrosrapt0@petrosrapt0Assistant:~$ nslookup - 147.102.1.1
> set domain=.
> set q=ptr
> 147.102.40.10
Server:      147.102.1.1
Address:     147.102.1.1#53

Non-authoritative answer:
10.40.102.147.in-addr.arpa    name = titan.cn.ece.ntua.gr.

Authoritative answers can be found from:
> server 147.102.7.1
Default server: 147.102.7.1
Address: 147.102.7.1#53
> 147.102.40.10
Server:      147.102.7.1
Address:     147.102.7.1#53

Non-authoritative answer:
10.40.102.147.in-addr.arpa    name = titan.cn.ece.ntua.gr.

Authoritative answers can be found from:
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
psyche.cn.ece.ntua.gr   has AAAA address 2001:648:2000:28::1
ulysses.noc.ntua.gr    internet address = 147.102.222.230
ulysses.noc.ntua.gr    has AAAA address 2001:648:2000:de::230
achilles.noc.ntua.gr  internet address = 147.102.222.210
achilles.noc.ntua.gr  has AAAA address 2001:648:2000:de::210
```



2.1) Ποια είναι η ακριβής σύνταξη της εντολής που χρησιμοποιήσατε για τον καθαρισμό της προσωρινής μνήμης DNS; sudo systemd-resolve --flush-caches

2.2) Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε; host 147.102.131.113

2.3) Ποιες υπο-εντολές της nslookup χρησιμοποιήσατε για να βρείτε το ζητούμενο όνομα υπολογιστή; set q=ptr

2.4) Ποιο είναι το όνομα του 147.102.40.10; **titan.cn.ece.ntua.gr**

2.5) Ποια είναι η σύνταξη του φίλτρου απεικόνισης που χρησιμοποιήσατε; **dns**

2.6) Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε από το DNS (TCP ή UDP); **UDP**

2.7) Πόσα αιτήματα προς εξυπηρετητές DNS έγιναν από τον υπολογιστή σας; **2**

2.8) Εάν έγιναν περισσότερα των δύο, ποιος ήταν ο λόγος; **'Έγιναν ακριβώς δύο.**

2.9) Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν σε ένα αίτημα και την αντίστοιχη απόκριση.

Query: Source Port: 52436 Destination Port: 53

Response: Source Port: 53 Destination Port: 52436

2.10) Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS; **53**

2.11) Τι μήκος έχει η επικεφαλίδα DNS; **44 bytes**

2.12) Καταγράψτε το Transaction ID του πρώτου αιτήματος για το όνομα του 147.102.40.10 και της αντίστοιχης απόκρισης. Ποια είναι η σχέση μεταξύ τους; **Query: ox5b4a, Response: ox5b4a, είναι ίδια**

2.13) Τι μήκος έχει το πεδίο Flags της επικεφαλίδας DNS; **2 bytes**

2.14) Ποιο κατά σειρά bit του πεδίου Flags της επικεφαλίδας DNS δηλώνει αν το συγκεκριμένο μήνυμα είναι αίτημα ή απόκριση; **To πρώτο bit**

2.15) Ποιο κατά σειρά bit του πεδίου Flags δείχνει το κατά πόσο η απόκριση προέρχεται από τον επίσημο εξυπηρετητή DNS; **To έκτο bit**

2.16) Στο πρώτο αίτημα για την εύρεση του ονόματος του 147.102.40.10, πόσες ερωτήσεις περιέχονται: **1** πόσες εγγραφές RR για απαντήσεις: **0**

πόσες RR για επίσημους εξυπηρετητές: **0**

πόσες επιπρόσθετες RR:; **0**

2.17) Παρατηρήστε την απόκριση στο προηγούμενο αίτημα. Περιλαμβάνει την ερώτηση για την οποία απαντά; **Nαι**

2.18) Πόσες εγγραφές RR για απαντήσεις: **1**

πόσες RR για επίσημους εξυπηρετητές: **0**

και πόσες επιπρόσθετες RR περιλαμβάνει:; **0**

2.19) Εμφανίσθηκαν όλες οι προηγούμενες πληροφορίες για εγγραφές RR στο παράθυρο της γραμμής εντολών; **Nαι**

2.20) Η απόκριση στο δεύτερο αίτημα για την εύρεση του ονόματος του 147.102.40.10 προέρχεται από τον επίσημο εξυπηρετητή DNS; **'Όχι** Που βρήκατε τη σχετική πληροφορία; **Authoritative Bit DNS Header Flags**

Ξεκινάμε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης. Ορίζουμε ως εξυπηρετητή που θα απαντά τον 1.1.1.1, εκτελούμε την υπο-εντολή set q=a της nslookup για να βρούμε τη διεύθυνση IPv4 του www.youtube.com και κατόπιν την υπο-εντολή set q=aaaa για να βρείτε τη διεύθυνση IPv6 του www.cnn.com. Στη συνέχεια σταματάμε την καταγραφή και εφαρμόζουμε κατάλληλο φίλτρο ώστε να παραμείνουν μόνο μηνύματα DNS, αποκρίσεις, από τον εξυπηρετητή DNS.

```
petrosrapto@petrosraptoAssistant:~$ nslookup
> server 1.1.1.1
Default server: 1.1.1.1
Address: 1.1.1.1#53
> set q=a
> youtube.com
Server:      1.1.1.1
Address: 1.1.1.1#53

Non-authoritative answer:
Name: youtube.com
Address: 142.251.140.14

> set q=aaaa
> cnn.com
Server:      1.1.1.1
Address: 1.1.1.1#53

Non-authoritative answer:
Name: cnn.com
Address: 2a04:4e42:600::773
Name: cnn.com
Address: 2a04:4e42:200::773
Name: cnn.com
Address: 2a04:4e42:c00::773
Name: cnn.com
Address: 2a04:4e42:e00::773
Name: cnn.com
Address: 2a04:4e42::773
Name: cnn.com
Address: 2a04:4e42:a00::773
Name: cnn.com
Address: 2a04:4e42:800::773
Name: cnn.com
Address: 2a04:4e42:400::773
```

No.	Time	Source	Destination	Protocol	Length	Info
96	37.280352693	147.102.131.113	1.1.1.1	DNS	57	Standard query 0x7438 A youtube.com
97	37.361886241	1.1.1.1	147.102.131.113	DNS	73	Standard query response 0x7438 A youtube.com A 142.251.140.14
119	60.229563470	147.102.131.113	1.1.1.1	DNS	53	Standard query 0xf6a0 AAAA cnn.com
121	60.264523584	1.1.1.1	147.102.131.113	DNS	277	Standard query response 0xf6a0 AAAA cnn.com AAAA 2a04:4e42:60...
Frame 96: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface tun0, id 0 Raw packet data						
- Internet Protocol Version 4, Src: 147.102.131.113, Dst: 1.1.1.1						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 57						
Identification: 0x2486 (9350)						
> Flags: 0x0000						
Fragment offset: 0						
Time to live: 64						
Protocol: UDP (17)						
Header checksum: 0xd55 [validation disabled]						
[Header checksum status: Unverified]						
Source: 147.102.131.113						
Destination: 1.1.1.1						
- User Datagram Protocol, Src Port: 34537, Dst Port: 53						
Source Port: 34537						
Destination Port: 53						
Length: 37						
Checksum: 0x27d9 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 2]						
> [Timestamps]						
- Domain Name System (query)						
Transaction ID: 0x7438						
> Flags: 0x0100 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 0						
Queries						
> [Response In: 97]						
- TRANSMIT RTE Data						
[RTE Status: OK]						
> [Req First Seg: 96]						
> [Req Last Seg: 96]						
> [Rsp First Seg: 97]						
> [Rsp Last Seg: 97]						
[TAPDU Rsp Time: 0.081534148 seconds]						
[Service Time: 0.081534148 seconds]						
[Req Spread: 0.000000000 seconds]						
[Rsp Spread: 0.000000000 seconds]						
[Trace clip filter: udp.stream==2 && frame.number>=96 && frame.number<=97]						
[Calculation: DNS]						
0000	45.00	00.39.24.86.00.00	40.11.3d.55.93.66.83.71	E..9\$...@=U-f-q		
0010	01.01.01.01.86.e9.00.35	00.25.27.d9.74.38.01.00	5.%'t8..		
0020	00.01.00.00.00.00.00.00	07.79.6f.75.74.75.62.65	youtube		
0030	03.63.6f.6d.00.00.01.00	01		.com.....		

- 2.21) Ποια είναι η σύνταξη του νέου φίλτρου απεικόνισης; dns.flags.response == 1**

2.22) Πόσες διευθύνσεις IPv4 έχει το www.youtube.com σύμφωνα με το αποτέλεσμα της εντολής nslookup; 1

2.23) Εντοπίστε το μήνυμα που μεταφέρει την απόκριση του εξυπηρετητή DNS στο αίτημα για να βρεθεί η διεύθυνση IPv4 του ονόματος www.youtube.com. Πόσες ερωτήσεις περιλαμβάνει; 1

2.24) Πόσες και ποιου είδους εγγραφές RR περιλαμβάνει το τμήμα της απάντησης στην παραπάνω απόκριση;

1 Answer RRs, o Authority RRs, o Additional RRs, type: A

2.25) Πώς σχετίζονται οι εγγραφές αυτές με τις διευθύνσεις IPv4 που προσδιορίσατε στην ερώτηση 2.22;
Παρατηρούμε ότι η εγγραφή απάντησης περιλαμβάνει την ίδια IPv4 διεύθυνση που εμφανίζεται στο terminal.

**2.26) Για ποιο λόγο στο τμήμα της απάντησης στην παραπάνω απόκριση υπάρχει και μια εγγραφή RR τύπου CNAME;
Δεν παρατηρείται εγγραφή RR τύπου CNAME, ωστόσο αν υπήρχε θα ήταν λόγω ύπαρξης διαφορετικών ονομάτων του εξυπηρετητή ιστού.**

**2.27) Κατά τη γνώμη σας, η ιστοθέση www.youtube.com φιλοξενείται από έναν υπολογιστή ή περισσότερους;
Αιτιολογήστε. Ξαναβρίσκουμε την IPv4 της ιστοθέσης www.youtube.com μέσω της nslookup. Παρατηρούμε ότι η διεύθυνση άλλαξε. Η εν λόγω ιστοθέση λοιπόν φιλοξενείται από πολλούς υπολογιστές, πράγμα λογικό ώστε να διεκπεραιωθεί η υπέρογκη ζήτηση στο youtube.**

2.28) Εντοπίστε το μήνυμα που μεταφέρει την απόκριση του εξυπηρετητή DNS στο αίτημα για να βρεθεί η διεύθυνση IPv6 του ονόματος www.cnn.com. Πόσες εγγραφές RR περιλαμβάνει το τμήμα της απάντησης για διευθύνσεις IPv6 του www.cnn.com; 8 Answer RRs, o Authority RRs, o Additional RRs

2.29) Καταγράψτε το επίσημο όνομα και τη διεύθυνση IPv6 ενός εκ των εξυπηρετητών που περιλαμβάνει η απόκριση για το www.cnn.com; Name: cnn.com, Address: 2a04:4e42:600::773

2.30) Πέραν των προηγούμενων δύο αποκρίσεων στην καταγραφή θα παρατηρήσετε άλλη μία. Σε ποιου είδους ερώτηση απαντά; Δεν παρατηρείται άλλη απόκριση.

Ξεκινάμε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης. Στη συνέχεια ακολουθούμε τα παρακάτω βήματα:

```

petrosraptos@petrosraptosAssistant:~$ nslookup
> server 8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set q=any
> ntua.gr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
ntua.gr text = "google-site-verification=kkalSC_zY7WLA1Hb1hSnMPJvX0I5IYs6m2YCooFj17I"
ntua.gr text = "cisco-ci-domain-verification=4d4bf81f7a19cce571ce607bc79a7f923189b777c5bcd5e6b64e5d482be85 "
ntua.gr text = "MS=ms79440458"
Name: ntua.gr
Address: 2001:648:2000:de::210
Name: ntua.gr
Address: 147.102.224.101
ntua.gr mail exchanger = 20 achilles.noc.ntua.gr.
ntua.gr mail exchanger = 20 ulysses.noc.ntua.gr.
ntua.gr mail exchanger = 20 diomedes.noc.ntua.gr.
ntua.gr
    origin = achilles.noc.ntua.gr
    mail addr = noc.ntua.gr
    serial = 2022122203
    refresh = 43200
    retry = 3600
    expire = 604800
    minimum = 86400
ntua.gr nameserver = ulysses.noc.ntua.gr.
ntua.gr nameserver = diomedes.noc.ntua.gr.
ntua.gr nameserver = sns1.grnet.gr.
ntua.gr nameserver = sns0.grnet.gr.
ntua.gr nameserver = achilles.noc.ntua.gr.

Authoritative answers can be found from:
> set q=soa
> cslab.ntua.gr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
cslab.ntua.gr
    origin = danaos.cslab.ece.ntua.gr
    mail addr = root.danaos.cslab.ece.ntua.gr
    serial = 2022102600
    refresh = 21600
    retry = 7200
    expire = 720000
    minimum = 86400
Authoritative answers can be found from:
> set q cname
> www.cn.ntua.gr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.cn.ntua.gr canonical name = www.cn.ece.ntua.gr.

Authoritative answers can be found from:
> set q=mx
> elab.ntua.gr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
elab.ntua.gr mail exchanger = 20 achilles.noc.ntua.gr.
elab.ntua.gr mail exchanger = 20 ulysses.noc.ntua.gr.
elab.ntua.gr mail exchanger = 20 diomedes.noc.ntua.gr.

Authoritative answers can be found from:
> set q=txt
> telecom.ntua.gr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
telecom.ntua.gr text = "google-site-verification=Hb0Wpc5iqYoDWMOfubp4saVokG9tWA7_Gtr640cyVHo"
telecom.ntua.gr text = "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"

Authoritative answers can be found from:
> set q=ns
> www.ntua.gr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
*** Can't find www.ntua.gr: No answer

Authoritative answers can be found from:
ntua.gr
    origin = achilles.noc.ntua.gr
    mail addr = noc.ntua.gr
    serial = 2022122203
    refresh = 43200
    retry = 3600
    expire = 604800
    minimum = 86400

```

2.31) Καταγράψτε το πλήθος των RR για απαντήσεις στην απόκριση για την περιοχή ntua.gr:

Answer RRs: 14, Authority RRs: 0, Additional RRs: 0

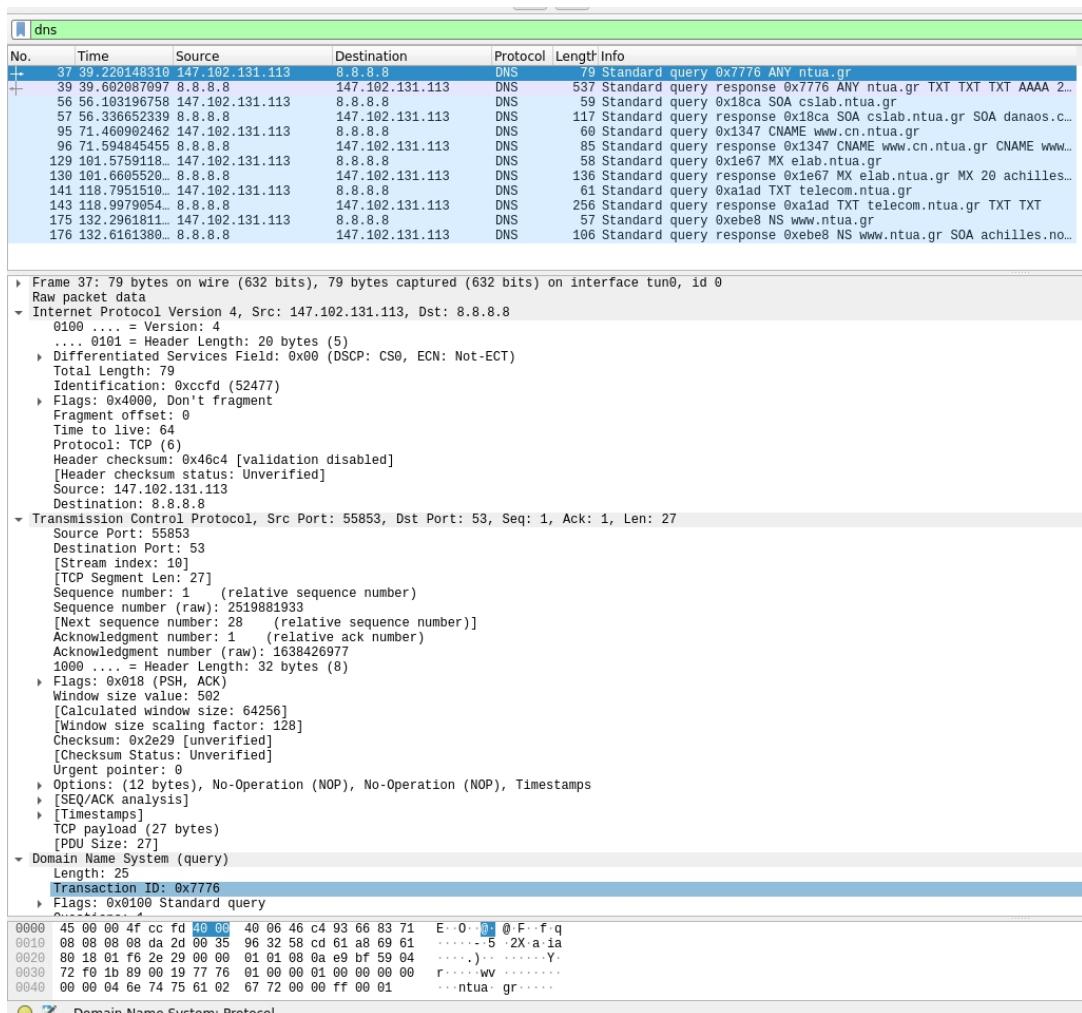
καθώς και το είδος τους.: type: TXT, AAAA, A, MX, SOA, NS

2.32) Καταγράψτε το πλήθος των RR για απαντήσεις στην απόκριση σχετικά με την αρχή πληροφόρησης για την περιοχή cslab.ntua.gr. Answer RRs: 1, Authority RRs: 0, Additional RRs: 0

2.33) Ποιο είναι το όνομα (mname – master name) του κύριου εξυπηρετητή DNS της περιοχής cslab.ntua.gr: danaos.cslab.ece.ntua.gr και ποια η διεύθυνση ηλεκτρονικού ταχυδρομείου (rname – responsible's name) του διαχειριστή αυτής: root.danaos.cslab.ece.ntua.gr

2.34) Καταγράψτε το πλήθος των RR για απαντήσεις στην απόκριση σχετικά με το κανονικό όνομα του www.cn.ntua.gr: Answer RRs: 1, Authority RRs: 0, Additional RRs: 0

το κανονικό όνομα αυτού: www.cn.ece.ntua.gr.
καθώς και τη διάρκεια ζωής της εγγραφής: 20 minutes



2.35) Καταγράψτε το πλήθος των RR για απαντήσεις στην απόκριση σχετικά με τους αρμόδιους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής elab.ntua.gr: Answer RRs: 3, Authority RRs: 0, Additional RRs: 0 καθώς και το όνομα του πλέον προτιμότερου εξ αυτών.: achilles.noc.ntua.gr.

2.36) Καταγράψτε το πλήθος των RR για απαντήσεις στην απόκριση για την περιοχή telecom.ntua.gr.:

Answer RRs: 2, Authority RRs: 0, Additional RRs: 0

Ποιο είναι το μήκος σε byte μίας εκ των εγγραφών TXT: 68

και ποιο το μήκος της πληροφορίας που αυτή μεταφέρει.: 69

2.37) Καταγράψτε το πλήθος των RR για απαντήσεις, RR για επίσημους εξυπηρετητές και επιπρόσθετες RR που περιέχει η απόκριση για τους αρμόδιους εξυπηρετητές DNS του www.ntua.gr.

Answer RRs: 0, Authority RRs: 1, Additional RRs: 0

Γιατί νομίζετε ότι η απόκριση παραπέμπει στην αρχή πληροφόρησης για την περιοχή ntua.gr;

Διότι το query που πραγματοποιήθηκε αφορά NS Record, το οποίο παρέχει πληροφορίες για το ποιος DNS server είναι ο πρωτεύων για το συγκεκριμένο domain.

Ξεκινάμε νέα καταγραφή με το Wireshark με φίλτρα καταγραφής και απεικόνισης όπως πριν. Στη συνέχεια:

```

petrosrapto@petrosraptoAssistant:~$ dig axfr planetlab.ntua.gr @147.102.222.210
.
; <>> DiG 9.16.1-Ubuntu <>> axfr planetlab.ntua.gr @147.102.222.210.
;; global options: +cmd
planetlab.ntua.gr.          86400  IN      SOA      achilles.noc.ntua.gr. noc.ntua.
gr. 2007072300 43200 3600 604800 86400
planetlab.ntua.gr.          86400  IN      NS       ulysses.noc.ntua.gr.
planetlab.ntua.gr.          86400  IN      NS       achilles.noc.ntua.gr.
planetlab.ntua.gr.          86400  IN      NS       diomedes.noc.ntua.gr.
stella.planetlab.ntua.gr.   86400  IN      A        147.102.224.228
stella-man.planetlab.ntua.gr. 86400  IN      A        147.102.224.230
vicky.planetlab.ntua.gr.    86400  IN      A        147.102.224.227
vicky-man.planetlab.ntua.gr. 86400  IN      A        147.102.224.229
planetlab.ntua.gr.          86400  IN      SOA      achilles.noc.ntua.gr. noc.ntua.
gr. 2007072300 43200 3600 604800 86400
;; Query time: 116 msec
;; SERVER: 147.102.222.210#53(147.102.222.210)
;; WHEN: Tue Dec 27 10:24:13 EET 2022
;; XFR size: 9 records (messages 9, bytes 894)

```

No.	Time	Source	Destination	Protocol	Length	Info
+	55 25. 537392845	147.102.131.113	147.102.222.210	DNS	112	Standard query 0xc537 AXFR planetlab.ntua.gr OPT
+	57 25. 629781845	147.102.222.210	147.102.131.113	DNS	177	Standard query response 0xc537 AXFR planetlab.ntua.gr SOA ach..
+	59 25. 652024241	147.102.222.210	147.102.131.113	DNS	839	Standard query response 0xc537 SOA achilles.noc.ntua.gr OPT

Frame 55: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface tun0, id 0
Raw packet data: 0x0000000000000000 -> 0x0000000000000000
Internet Protocol Version 4, Src: 147.102.131.113, Dst: 147.102.222.210
... 0100 ... = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 112
Identification: 0x77b (42875)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x00fc [validation disabled]
[Header checksum status: Unverified]
Source: 147.102.131.113
Destination: 147.102.222.210
Transmission Control Protocol, Src Port: 45041, Dst Port: 53, Seq: 1, Ack: 1, Len: 60
Source Port: 45041
Destination Port: 53
[Stream index: 6]
[TCP Segment Len: 60]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 2903687406
[Next sequence number: 61 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 587448953
1000 = Header Length: 32 bytes (8)
> Flags: 0x0101 (PSH, ACK)
Window size value: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0x0093 [Unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
> [Timestamps]
TCP payload: (60 bytes)
[PPS Size: 60]
Domain Name System (query)
Length: 58
Transaction ID: 0xc537
> Flags: 0x00020 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
> Queries
> Additional records
[Response In: 57]

0000	45 00 00 70	a7 7b 40 00	40 00 09 fc	93 66 83 71	E .. p { @ @ .. f q
0010	93 00 00 d2	a7 f1 00 30	ad 12 c0 2d	00 00 00 79	.. f 5 .. # y
0020	00 00 00 01	f6 ac 93 00	02 00 00	3e 00 00 00(.
0030	ba 00 f3	00 00 c5 37	00 20 00 01	00 00 00 00	.. H : 7 ..
0040	00 01 00 70	ec 61 00 05	74 00 61 62	04 00 74 75	.. plane tlab ntua

2.38) Πόσα αιτήματα DNS έγιναν: **1**, πόσες αποκρίσεις DNS λήφθηκαν: **2**

και ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε: **TCP**

2.39) Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκε για το αίτημα προς τον εξυπηρετητή 147.102.222.210 και τις αποκρίσεις που ελήφθησαν.

Query: Source Port: 45041 Destination Port: 53

Response_1: Source Port: 53 Destination Port: 45041

Response_2: Source Port: 53 Destination Port: 45041

2.40) Ποιο είναι το μήκος του αιτήματος προς τον εξυπηρετητή 147.102.222.210: **60 bytes**

2.41) Ποιος είναι ο τύπος του αιτήματος και ποιο το νόημά του; **type: AXFR - DNS zone transfer - αντιγραφή DNS Records ανάμεσα σε DNS servers.**

2.42) Εντοπίστε τις αποκρίσεις του εξυπηρετητή 147.102.222.210. Τι μήκος έχουν και πόσα μηνύματα αποκρίσεις DNS (response) μεταφέρονται με αυτές;

1st DNS message: 125bytes 1 response

2nd DNS message: 96+97+97+93+97+92+96+119 = 787 bytes, 8 responses

2.43) Πώς γίνεται κατανοητό ότι τα προηγούμενα μηνύματα DNS αποτελούν την απάντηση στο αίτημα που έγινε; **'Έχουν ίδιο Transaction ID με αυτό του αιτήματος.**

2.44) Πόσες εγγραφές RR για ερωτήσεις, απαντήσεις, επίσημους εξυπηρετητές και επιπρόσθετες πληροφορίες περιλαμβάνει το κάθε μήνυμα DNS (response) που περιέχεται στις αποκρίσεις του εξυπηρετητή 147.102.222.210;

Response_1: Answer RRs: 1, Authority RRs: 0, Additional RRs: 1

Response_2: Answer RRs: 1, Authority RRs: 0, Additional RRs: 1 για κάθε response

2.45) Γιατί νομίζετε ότι έγινε η αλλαγή πρωτοκόλλου στρώματος μεταφοράς που εντοπίσατε στην ερώτηση 2.38;

Το πρωτόκολλο UDP χρησιμοποιείται για την ανταλλαγή πληροφοριών μικρού μεγέθους ενώ το TCP χρησιμοποιείται για μεγαλύτερα μεγέθη. Ακόμα το TCP είναι πιο αξιόπιστο, κάτι που είναι επιθυμητό για zone transfers.

2.46) Ποιο φίλτρο σύλληψης πρέπει να χρησιμοποιήσετε στο Wireshark για να καταγράφετε μόνο μηνύματα DNS; **dns**

2.47) Στην προηγούμενη καταγραφή, στο παράθυρο με τις λεπτομέρειες, επιλέξτε το όνομα της περιοχής planetlab.ntua.gr στην απόκριση για την εγγραφή τύπου SOA ώστε να εμφανισθούν υπογραμμισμένα τα αντίστοιχα δεδομένα στο παράθυρο με τα περιεχόμενα. Ποια τιμή έχει το πρώτο: **0x09**, το ενδέκατο: **0x04**, το τέταρτο πριν το τέλος **0x02** και το τελευταίο byte των δεδομένων: **0x00** Γιατί;

Πρώτο byte: Το πρώτο byte του δείκτη υποδεικνύει το μέγεθος του label που ακολουθεί.

Ενδέκατο byte: Πλήθος byte του ακολουθούμενου label (ntua).

Τέταρτο πριν το τέλος byte: Πλήθος byte του ακολουθούμενου label (gr).

Τελευταίο byte: Το τελευταίο byte τελειώνει με 0.

2.48) Στην ίδια απόκριση, επιλέξτε το όνομα του κύριου εξυπηρετητή DNS. Τι παριστάνουν τα δύο τελευταία byte στο παράθυρο με τα περιεχόμενα; **Είναι pointer προς προηγούμενη εμφάνιση του ntua.gr**

2.49) Στη συνέχεια επιλέξτε τη διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστή. Τι παρατηρείτε;

Αποτελείται μόνο από pointer σε προηγούμενη ακολουθία χαρακτήρων.