ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΡΟΗ Δ - ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ (COMPUTER NETWORKS)

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ 03120827

ΑΝΑΦΟΡΑ 10ΗΣ ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ

Ομάδα: 2
Λογισμικο: Linux Ubuntu 2e0.04
Ονομα PC: glaptop
Διεύθυνση IP: 147.102.237.32
Διεύθυνση MAC: 70:9c:d1:03:b0:15

ΑΣΚΗΣΗ 1: Υπηρεσία DNS

1.1 Οι εξπηρετητές DNS που εμφανίζονται ανήκουν στην ρίζα του δέντρου (περιοχή .root-servers.net.)

1.2 Εμφανίζονται 13 υπεύθυνοι εξυπηρετητές DNS. Ενδεικτικά:
a.root-servers.net internet address = 198.41.0.4
a.root-servers.net has AAAA address 2001:503:ba3e::2:30

1.3 Η εντολή που χρησιμοποίηση είναι: server 198.41.0.4

1.4 Οι εξπηρετητές DNS που εμφανίζονται ανήκουν στην 1η σταθμη του σχήματος 1, δηλαδή στο gr.

1.5 Εμφανίζονται 6 υπεύθυνοι εξυπηρετητές DNS. Ενδεικτικά:
gr-d.ics.forth.gr internet address = 194.0.11.102
gr-d.ics.forth.gr has AAAA address 2001:678:e:102::53

1.6 Το αποτέλεσμα που λαμβάνω είναι ίδιο με αυτό του ερωτήματος 1.4, εμφανίζονται δηλαδή οι ίδιοι εξυπηρετητές. Επομένως, συμπεραίνω ότι απαντάνε οι εξυπηρετητές κορυφής (root name servers) που βρίσκονται στο επίπεδο gr (1η στάθμη)

1.7 Η εντολή που χρησιμοποίηση είναι: server 194.0.11.102

1.8 Η απάντηση τώρα είναι διαφορετική, καθώς αλλάξαμε server που ρωτάμε, και ο καινούργιος βρίσκεται σε διαφορετικό επίπεδο.

1.9 Εμφανίζονται 5 υπεύθυνοι εξυπηρετητές DNS. Ενδεικτικά:
ulysses.noc.ntua.grinternet address = 147.102.222.230

1.10 Χρησιμοποίωντας τώρα τον 147.102.222.230 ως τον server που στέλνουμε το αιτημα, παρατηρούμε ότι στην ερώτηση ntua.gr παίρνουμε ίδια απάντηση

1.11 Εμφανίζονται 3 υπεύθυνοι εξυπηρετητές DNS. Ενδεικτικά:
cn.ntua.gr nameserver = psyche.cn.ece.ntua.gr.

1.12 Για το αίτημα: ece.ntua.gr προκύπτει:
ece.ntua.gr nameserver = ulysses.noc.ntua.gr.

ece.ntua.gr nameserver = achilles.noc.ntua.gr.
ece.ntua.gr nameserver = diomedes.noc.ntua.gr.

Ενώ για το metal.ntua.gr προκύπτει:

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

Παρατηρώ, ότι εμφανίζονται οι ίδιοι 3 εξυπηρετητές DNS και στις 2 σχολές, αλλά στην ΜΜΜ εμφανίζεται ένας επιπλέον

1.13 Ο κύριος εξυπηρετητής DNS της περιοχής cn.ntua.gr. είναι ο psyche.cn.ece.ntua.gr, έχει διεύθυνση 147.102.40.1 και σειριακό αριθμό 2023112802

1.14 Ένας δευτερεύων εξυπηρετητής θα αναζητήσει αλλαγές κάθε 8 ώρες (refresh = 28800)

1.15 Οι σχετικές εγγραφές διατηρούνται στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών για 24 ώρες (minimum = 86400)

1.16 Ο κύριος εξυπηρετητής DNS της περιοχής ece.ntua.gr. είναι ο achilles.noc.ntua.gr, έχει διεύθυνση 147.102.222.210 και σειριακό αριθμό 2023090800. Ένας δευτερεύων εξυπηρετητής θα αναζητήσει αλλαγές κάθε 24 ώρες (refresh = 86400) και οι σχετικές εγγραφές διατηρούνται για 24 ώρες (minimum = 86400)

1.17 Για τον σειριακό αριθμό παρατηρώ ότι πρόκειται για ημερομηνία καθώς οι πρώτοι 4 αριθμοί είναι η χρονολογία.

1.18 Βρήκα τις ακόλουθες πληροφορίες για 3 Ελληνικά Πανεπιστήμια:
uoa.gr: 195.134.71.229 (ΕΚΠΑ)
auth.gr: 155.207.1.12 (Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης)
uoc.gr: 147.52.80.1 (Πανεπιστήμιο Κρήτης)

1.19 Για το υποδίκτυο 147.102.40.16/29 έχουμε:
147.102.40.16: trillium.cn.ece.ntua.gr.
147.102.40.17: pegasus.cn.ece.ntua.gr.

1.20 Όχι, δεν εχει τη συνήθη αριθμητική μορφή μιας διεύθυνσης IPv4. Ωστόσο έχουν την μορφή reverse lookup
Πχ: 17.40.102.147.in-addr.arpa

1.21 Για τον υπολογιστή που φιλοξενεί την ιστοθέση της Σχολής ΜΜΜ ισχύει ότι έχει: canonical name = lemmy.metal.ntua.gr.

1.22 Δύο από τους εξυπηρετήτές ηλεκτρονικού ταχυδρομείου της περιοχής ‘arch.ntua.gr.’ είναι:
f0.mail.ntua.gr με διεύθυνση 147.102.222.195
f1.mail.ntua.gr με διεύθυνση 147.102.222.196

1.23 Ο πρώτος που θα προτιμηθεί είναι αυτός με τον μικρότερο αριθμό MX Preference. Στην συγκεκριμένη περίπτωση οι 2 αυτοί εξυπηρετητές έχουν ίδιο τέτοιο αριθμο (10) , και μικρότερο από όλους τους άλλους, άρα θα επιλεχθεί είτε ο ένας είτε ο άλλος.

1.24 (Σε Ubuntu Linux) Το afxr στην εντολή που χρησιμοποίησα σημαίνει να αντιγραφούν όλα τα δεδομένα DNS από τον ένα εξυπηρετητή στον άλλο

1.25 Συναντάμε τις περιπτώσεις: SOA, TXT, MX, NS, A και CNAME:

```
central.ntua.gr.        86400 IN    SOA   netsrv0.central.ntua.gr.
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    ulysses.noc.ntua.gr.
central.ntua.gr.        86400 IN    A     147.102.222.46
acadinfo.central.ntua.gr. 86400 IN  CNAME  beta.central.ntua.gr.
```

ΑΣΚΗΣΗ 2: Πρωτόκολλο DNS

2.1 Για τον καθαρισμό της προσωρινής μνήμης DNS χρησιμοποίησα την εντολή: sudo resolvectl flush-caches (ubuntu linux)

2.2 Το φίλτρο σύλληψης που χρησιμοποίησα είναι: host 147.102.237.32

2.3 Για να βρω το ζητούμενο όνομα υπολογιστή χρησιμοποίησα τις υποεντολές:

```
set q=ptr
server 147.102.40.1
147.102.40.10
server 147.102.7.1
147.102.40.10
```

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

2.5 Το φίλτρο απεικόνισης που χρησιμοποίησα είναι: dns

2.6 Το πρωτόκολλο μεταφοράς που χρησιμοποιήθηκε από το DNS είναι: udp

2.7 Παρατηρώ 5 αιτήματα προς εξυπηρετητές DNS από τον υπολογιστή μου

2.8 Το 1 από αυτά τα 5 είναι αίτημα connectivity-check καθώς καθαρίσαμε την dns cache πριν τα βασικά αιτήματα. Επειτα κάθε ερώτηση που κάνω από τον υπολογιστή μου δημιουργει 2 αιτήματα προς τους εξυπηρετητές DNS με πολύ μικρή χρονική διαφορά (ιδιοτροπία του λογισμικού).
Για παράδειγμα:

```
48 49.063496…  147.102.237.32   147.102.40.1   DNS   86 Standard query 0x12e8 PTR 10.40.102.147.in-addr.arpa
49 0.000166446 147.102.237.32   147.102.40.1   DNS   86 Standard query 0x12e8 PTR 10.40.102.147.in-addr.arpa
```

2.9 Οι θύρες που χρησιμοποιήθηκαν είναι:
Αίτημα: Θύρα Προέλευσης: 32898 / Θύρα Προορισμού: 53
Απόκριση: Θύρα Προέλευσης: 53 / Θύρα Προορισμού: 32898

2.10 Η θύρα που αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS είναι η 53.

2.11 Η επικεφαλίδα DNS έχει μήκος 12 bytes

2.12 Στο πρώτο αίτημα το Transaction ID είναι: 0x12e8. Στην αντίστοιχη απόκριση παρατηρώ το ίδιο Transaction ID

2.13 Το πεδίο Flags έχει μήκος 2 bytes

2.14 Για να δούμε αν ένα συγκεκριμένο μήνυμα είναι αίτημα ή απόκριση πρέπει να κοιτάξουμε το 1ο bit

2.15 Για να δούμε αν μία ανάμνηση προέρχεται από επίσημο εξυπηρετητή

πρέπει να κοιτάξουμε το 6ο bit

2.16 Παρατηρώ:

1 ερώτηση / 0 εγγραφές RR για απαντήσεις / 0 εγγραφές RR για επίσημους εξυπηρετητές / 0 επιπρόσθετες εγγραφές RR

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

2.17 Ναι, οι αποκρίσεις περιλαμβάνουν την ερώτηση για την οποία απαντούν

2.18 Στις αποκρίσεις παρατηρώ:

1 ερώτηση / 1 εγγραφές RR για απαντήσεις / 3 εγγραφές RR για επίσημους εξυπηρετητές / 6 επιπρόσθετες εγγραφές RR

```
Questions: 1
Answer RRs: 1
Authority RRs: 3
Additional RRs: 6
```

2.19 Ναι, οι προηγούμενες πληροφορίες για τις RR εμφανίσθηκαν στην γραμμή εντολών

2.20 Όχι, η αποκριση αυτή δεν προέρχεται από τον επίσημο εξυπηρετητή DNS και το καταλαβαίνουμε αυτό από το 6ο bit των flags

2.21 Το φίλτρο απεικόνισης που χρησιμοποίησα είναι: dns.flags.response == 1

2.22 Το www.youtube.com φαίνεται να έχει 16 διευθύνσεις IPv4

2.23 Το μήνυμα αυτό περιλαμβάνει 1 ερώτηση.

2.24 Το μήνυμα περιλαμβάνει:

Answer RRs: 17
Authority RRs: 0
Additional RRs: 0

2.25 Οι εγγραφές RR για απαντήσεις είναι ίσες με το πλήθος διευθύνσεων του ερωτήματος 2.22 + 1 για το cname

2.26 Υπάρχει μια εγγραφή για το cname καθώς το www.youtube.com είναι ψευδώνυμο (alias)

2.27 Αν ξαναψάξουμε τις διευθύνσεις του www.youtube.com, παρατηρούμε ότι εμφανίζονται λιγότερες διευθύνσεις (load sharing)

2.28 Η ιστοθέση www.youtube.com φιλοξενείται από περισσότερους από έναν υπολογιστές και αυτό το καταλαβαίνουμε από τις πολλές (και διαφορετικές σε κάθε ερώτηση) διευθύνσεις IPv4 που εμφανίζονται.

2.29 Στο μήνυμα απόκρισης για το όνομα του www.cnn.com, εμφανίζονται 4 εγγραφές RR για διευθύνσεις IPv6.

2.30 Η απόκριση περιλαμβάνει:

Επίσημο όνομα: cnn-tls.map.fastly.net
Διεύθυνση IPv6 ενός εκ των εξυπηρετητών DNS: 2a04:4e42::773

2.31 Στα ubuntu linux, δεν φαίνεται κάποια επιπλέον απόκριση (Στα windows θα εμφάνιζε επιπλέον ένα PTR ερώτημα για την IP 1.1.1.1)

2.32 Στην απόκριση για την περιοχή ntua.gr περιέχονται:

Answer RRs: 18 (με τύπους: SOA, NS, MX, A, AAAA, TXT)

2.33 Στην απόκριση για την αρχή πληροφόρησης για την περιοχή cslab.ntua.gr περιέχονται: Answer RRs: 1

2.34 Το όνομα του κύριου εξυπηρετητή DNS της περιοχής cslab.ntua.gr είναι: danaos.cslab.ece.ntua.gr και η διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστή είναι: root.danaos.cslab.ece.ntua.gr

2.35 Στην απόκριση για το κανονικό όνομα του www.cn.ntua.gr περιέχονται: Answer RRs: 1
Επίσης, το κανονικό όνομα αυτού είναι: www.cn.ece.ntua.gr. και η διάρκεια ζωής της εγγραφής είναι: Time to live: 1200 (20 minutes)

2.36 Στην απόκριση για τους αρμόδιους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής elab.ntua.gr περιέχονται:
Answer RRs: 3
Επίσης, κανείς εξ αυτών δεν είναι προτιμότερος, καθώς έχουν ίδια τιμή preference (20)

2.37 Στην απόκριση για την περιοχή telecom.ntua.gr. περιέχονται:
Answer RRs: 2
Επίσης, μία εκ των εγγραφών TXT έχει μήκος 80 bytes το μήκος της πληροφορίας που αυτή μεταφέρει είναι 69 bytes (data length=text length (1 byte)+ text)

2.38 Στην απόκριση για τους αρμόδιους εξυπηρετητές DNS του www.ntua.gr περιέχονται: Authority RRs: 1 / Answer RRs: 0 / Additional RRs: 0
Η απόκριση παραπέμπει στην αρχή πληροφόρησης καθώς δεν υπάρχουν εγγραφές για το όνομα που ζητήθηκε
(Εμφανίζεται το μήνυμα: Non-authoritative answer:
*** Can't find www.ntua.gr: No answer)

2.39 Έγινε 1 DNS αίτημα και ληφθηκαν 2 αποκρίσεις DNS

2.40 Χρησιμοποιήθηκε το πρωτόκολλο μεταφοράς TCP. Οι θύρες που χρησιμοποιήθηκαν είναι:
43499 (Ο υπολογιστής μου) / 53 (Ο εξυπηρετητής)

2.41 Θα έπρεπε να χρησιμποποιήσω το φίλτρο σύλληψης: port 53

2.42 Η αλλαγή πρωτοκόλλου στρώματος μεταφοράς έγινε για μεγαλύτερη αξιοπιστία στη μετάδοση και λόγω μεγαλύτερου όγκου πληροφορίας που χρειάζεται το axfr=zone transfer

2.43 Το μήκος του αιτήματος προς τον εξυπηρετητή 147.102.222.210 είναι 60 bytes (ubuntu linux) (με βάση τις οδηγίες που δίνονται στην εκφώνηση)

2.44 Ο τύπος αιτήματος είναι AXFR και χρησιμοποιείται για μεταφορά DNS ζώνης

2.45 Εντοπίζοντας τις αποκρίσεις DNS του εξυπηρετηρή, παρατηρούμε ότι περιέχουν 9 μηνύματα response (1 η πρωτη και 8 η δευτερη)

2.46 Καταλαβαίνουμε ότι τα προηγούμενα μηνύματα DNS αποτελούν την απάντηση στο αίτημα που έγινε καθώς όλα έχουν την ίδια τιμή στο πεδίο

Transaction ID (την 0xb1e6)

2.47 Τα DNS response μηνύματα περιέχουν:
Στην πρώτη απόκριση (1 μήνυμα):
Questions: 1 / Answer RRs: 1 / Authority RRs: 0 / Additional RRs: 1
Στην δεύτερη απόκριση (8 μηνύματα):
Questions: 0 / Answer RRs: 1 / Authority RRs: 0 / Additional RRs: 1
(Ιδιο περιεχόμενο σε κάθε μήνυμα αυτής της απόκρισης)

2.48 Πριν από την επικεφαλίδα DNS υπάρχει το πεδίο Length. Το πεδίο αυτό έχει μήκος 2 byte και χρειάζεται γιατι επιτρέπει στη χαμηλού επιπέδου επεξεργασία να συναρμολογήσει ένα πλήρες μήνυμα πριν αρχίσει να το αναλύει. (RFC 1035)

2.49 Στην απόκριση για την εγγραφή τύπου SOA της περιοχής planetlab.ntua.gr παρατηρούμε ότι:
1ο byte: Τιμή c0 (11000000): Δειχνει ότι είναι pointer
11ο byte: Τιμή 00 (00000000): Δειχνει ότι είναι label
4ο byte πριν το τελος: Τιμή 00 (00000000): Δείχνει ότι είναι label
Τελευταίο byte: Τιμή 80 (10000000): Δείχνει ότι είναι reserved για μελλοντική χρήση

2.50 Τα δύο τελευταία bytes στο παράθυρο με τα περιεχόμενα του ονόματος του κύριου εξυπηρετητή DNS είναι c0 16. Τα δύο πρώτα bits είναι 11 το οποίο μας δείχνει ότι πρόκειται για pointer. Τα επόμενα 14 bits είναι 00000000010110 (22 σε δεκαδικό) και είναι το offset που δείχνει τη 22η θέση από το πεδίο transaction id και μετά δηλαδή το όνομα ntua.gr

2.51 Επιλέγοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστή πάλι παρατηρούμε pointer (διπλός ασσος στην αρχή) και το αντίστοιχο offset (συγκεκριμένα offset= 111000).