Ονοματεπώνυμο: Χαράλαμπος Καμπουγέρης **Ομάδα:** 3, Τετάρτη 10:45-12:30, Αιθ.Α2

Όνομα PC/ΛΣ: CHARALAMPOSs-MacBook-Air/ macOS 14.0 **Ημερομηνία:** 26/12/2023

Διεύθυνση IP: 147.102.131.186 **Διεύθυνση MAC:** 0c:e4:41:e1:6c:74

Εργαστηριακή Άσκηση 10
Σύστημα Ονομασίας Περιοχών DNS

Άσκηση 1

1.1 Στη ρίζα του δέντρου

1.2 Εμφανίζονται 13 εξυπηρετητές DNS. Ένα παράδειγμα είναι ο εξυπηρετητής:
nameserver = a.root-servers.net, IPv4: 198.41.0.4, IPv6: 2001:503:ba3e::2:30

1.3 server a.root-servers.net

1.4 Στη δεύτερη στάθμη (.gr)

1.5 Υπάρχουν 6 υπεύθυνοι εξυπηρετητές DNS σε αυτή την κορυφή. Ένα παράδειγμα είναι ο εξυπηρετητής:
nameserver = gr-d.ics.forth.gr, IPv4: 194.0.11.102, IPv6: 2001:678:e:102::53

1.6 Είναι οι ίδιοι εξυπηρετητές με πριν. Άρα απαντούν οι εξυπηρετητές κορυφής για το επίπεδο που βρισκόμαστε

1.7 server 139.91.191.3

1.8 Η απάντηση δεν είναι ίδια αφού αλλάξαμε το επίπεδο στο οποίο αναζητούμε

1.9 Καταγράφηκαν 5 εξυπηρετητές και ένα παράδειγμα είναι ο diomedes.noc.ntua.gr

1.10 Ναι

1.11 Καταγράφηκαν 3 εξυπηρετητές και ένας από αυτούς που δεν εμφανίζεται στο **1.9** είναι ο psyche.cn.ece.ntua.gr.

1.12 Καταγράφηκαν τα ονόματα των υπεύθυνων εξυπηρετητών DNS για τις σχολές ΗΜΜΥ και ΜΜΜ. Παρατηρούμε ότι και στις δύο σχολές υπάρχουν 3 κοινοί εξυπηρετητές DNS (diomedes.noc.ntua.gr, achilles.noc.ntua.gr, ulysses.noc.ntua.gr), ωστόσο στη σχολή ΜΜΜ υπάρχει ένας επιπλέον εξυπηρετητής (serifos.metal.ntua.gr)

1.13 Είναι ο psyche.cn.ece.ntua.gr με IPv4 147.102.40.1 και σειριακό αριθμό 2023122201

1.14 Κάθε 28800 δευτερόλεπτα δηλαδή 8 ώρες

1.15 Για 24 ώρες

1.16

- SOA: achilles.noc.ntua.gr με διεύθυνση IPv4: 147.102.222.210 και Σειριακό Αριθμό: 2023090800
- Refresh Time: 24 ώρες
- Default TTL: 24 ώρες

1.17 Παρατηρώ ότι πρόκειται για ημερομηνία αφού ξεκινούν με 2023

1.18 ΕΚΠΑ —> www.uoa.gr (195.134.71.229)
ΑΠΘ —> www.auth.gr (155.207.1.12) και IPv6 (2001:648:2800:1:155:207:1:12)
Πανεπιστήμιο Κρήτης —> www.uoc.gr (147.52.201.72)

1.19 147.102.40.16 —> trillium.cn.ece.ntua.gr
147.102.40.20 —> bbb.cn.ece.ntua.gr

1.20 Όχι, έχουν την μορφή reverse lookup (<ip.addr>.in-addr.arpa)

1.21 canonical name = lemmy.metal.ntua.gr Address: 147.102.121.10

1.22 f0.mail.ntua.gr (147.102.222.195), diomedes.noc.ntua.gr (147.102.222.220)

1.23 Θα προτιμηθούν οι f0.mail.ntua.gr και f1.mail.ntua.gr γιατι έχουν το μικρότερο αριθμό προτίμησης

1.24 Το πρωτόκολλο AXFR χρησιμοποιείται για zone transfers, δηλαδή για αντιγραφή δεδομένων DNS μεταξύ εξυπηρετητών

1.25

central.ntua.gr. 900 IN **SOA** achilles.noc.ntua.gr. noc.ntua.gr. 2023122102 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 **A** 147.102.222.46

central.ntua.gr. 86400 IN **MX** 10 ulysses.noc.ntua.gr.

central.ntua.gr. 86400 IN **NS** diomedes.noc.ntua.gr.

career.central.ntua.gr. 86400 IN **CNAME** career.ntua.gr.

Άσκηση 2

2.1 sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder

2.2 host 147.102.131.186

2.3 set q=ptr

2.4 titan.cn.ece.ntua.gr

2.5 dns

2.6 UDP

2.7 Έγιναν συνολικά 10 αιτήματα

2.8 Αυτό οφείλεται στην εκκαθάριση της DNS cache

2.9 Θύρα προέλευσης: 52631 και θύρα προορισμού: 53 και στην απόκριση προφανώς οι θύρες αντιστρέφονται

2.10 Η 53

2.11 12 bytes

2.12 Transaction ID: 0xf639. Το ίδιο τόσο για το αίτημα όσο και για την απόκριση.

2.13 2 bytes

2.14 Το πρώτο bit, με το (0) να δηλώνει αίτημα(query) και το (1) να δηλώνει απόκριση (response)

2.15 Το έκτο

2.16 Περιέχονται 1 ερώτηση, καμία εγγραφή RR απαντήσεων, καμία RR επίσημων εξυπηρετητών και καμία επιπρόσθετη RR

2.17 Ναι

2.18 1 εγγραφή RR απαντήσεων, καμία RR επίσημων εξυπηρετητών και καμία επιπρόσθετη RR

2.19 Όχι

2.20 Όχι. Αυτό φαίνεται στα flags (στο 6^{ο} bit) στην απόκριση για το δεύτερο αίτημα

2.21 dns.flags.response==1

2.22 Φαίνεται να έχει 14 διευθύνσεις IPv4

2.23 Περιλαμβάνει 1 ερώτηση

2.24 Περιλαμβάνει 15 απαντήσεις RR

2.25 Πρόκειται για τις 14 διευθύνσεις του προηγούμενου ερωτήματος συν την απάντηση που πήραμε για το canonical name του YouTube

2.26 Γιατί το www.youtube.com είναι alias

2.27 Παρατηρώ ότι οι διευθύνσεις IPv4 εμφανίζονται με διαφορετική σειρά

2.28 Το www.youtube.com βρίσκεται σε πολλούς servers για αυτό και υπάρχουν περισσότερες από 1 διευθύνσεις IP

2.29 5 RR απαντήσεις

2.30 cnn-tls.map.fastly.net (2a04:4e42::773)

2.31 SOA

2.32 Έχουμε 18 RR απαντήσεις (SOA, NS, A, AAAA, MX, TXT)

2.33 1 RR απάντηση

2.34 mname: danaos.cslab.ece.ntua.gr
rname: root.danaos.cslab.ece.ntua.gr

2.35 1 RR απάντηση, cname=www.cn.ece.ntua.gr, TTL= 1200 (20 minutes)

2.36 3 RR απαντήσεις, ενώ δεν υπάρχει προτιμότερος καθώς και οι τρεις έχουν preference=20

2.37 2 RR απαντήσεις. Μία TXT απάντηση έχει μήκος 81 byte με μήκος πληροφορίας 69 bytes

2.38 Η απόκριση περιέχει 1 επίσημο εξυπηρετητή μόνο. Η απόκριση παραπέμπει την αρχή πληροφόρησης για το ntua.gr επειδή υποδεικνύει ότι ο συγκεκριμένος διακομιστής DNS είναι υπεύθυνος για τη διατήρηση και την παροχή ακριβών πληροφοριών σχετικά με τις εγγραφές DNS που σχετίζονται με το "ntua.gr".

2.39 Έγιναν: 1 αίτημα DNS, 2 αποκρίσεις DNS

2.40 Χρησιμοποιήθηκε το πρωτόκολλο TCP

Θύρα προέλευσης: 51123, θύρα προορισμού: 53

2.41 dns

2.42 Γιατί με το AXFR μεταφέρεται μεγάλος όγκος δεδομένων και επίσης χρειάζεται αξιοπιστία

2.43 48 bytes

2.44 Είναι μήνυμα τύπου AXFR και χρησιμοποιείται για την αντιγραφή όλων των εγγραφών μεταξύ εξυπηρετητών AXFR.

2.45 Έχουμε 9 DNS responses. Η πρώτη απόκριση έχει 1 DNS response ενώ η δεύτερη 8

2.46 Έχουν όλα τα μηνύματα το ίδιο Transaction ID

2.47

DNS Response #	Questions	Answer RRs	Authority RRs	Additional Rrs
1	1	1	0	1
2	0	1	0	1
3	0	1	0	1
4	0	1	0	1
5	0	1	0	1
6	0	1	0	1
7	0	1	0	1
8	0	1	0	1
9	0	1	0	1

2.48 Το πεδίο Length είναι 2 bytes. Αυτό το πεδίο μήκους επιτρέπει στη χαμηλού επιπέδου επεξεργασία να συναρμολογήσει ένα πλήρες μήνυμα προτού αρχίσει να το αναλύει.

2.49

- Το 1ο byte έχει τιμή HEX: (C0) -> BINARY: 11000000 (υποδεικνύει ότι είναι pointer)
- Το 11^{ο} HEX: (00) -> BINARY: 00000000 (το 1ο byte απο το data length πεδίο)
- Το 4ο πριν το τέλος HEX: (00) -> BINARY: 00000000 (1ο byte από το minimum TTL πεδίο)
- Το τελευταίο 10000000 (τελευταίο byte από το minimum TTL πεδίο)

2.50 Είναι pointer με offset 10110 = 22

2.51 Είναι και πάλι pointer με offset 111000 = 56