Ονοματεπώνυμο: ΔΗΜΗΤΡΙΟΣ ΓΕΩΡΓΟΥΣΗΣ		AM: 03119005		Ομάδα: 4
Όνομα PC/ΛΣ: dimitris-Laptop / WINDOWS 11 HOME   Ημεφομηνία: 15/12/2022				
Διεύθυνση IPv4: 147.102.236.96	Διεύθυνση MAC: 10-6F-D9-64-91-87			

## 1. Υπη*ρεσία DNS*

- 1.1: Στην περιοχή .net
- 1.2: Το πλήθος τους είναι 13. Ένας από αυτούς είναι ο "a.root-servers.net" με διεύθυνση IPv4 198.41.0.4 και διεύθυνση IPv6 2001:503:ba3e::2:30.
- 1.3: Η εντολή είναι: server 198.41.0.4
- 1.4: Ανήκουν στην περιοχή .gr
- 1.5: Οι εξυπηρετητές είναι 6. 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: Έλαβα τα ίδια αποτελέσματα. Συμπεραίνουμε ότι οι εξυπηρετητές κορυφής απαντούν με τις διευθύνσεις των εξυπηρετητών που βρίσκονται στο πρώτο επίπεδο (.gr)
- 1.7: server 194.0.11.102
- 1.8: Οι απαντήσεις δεν είναι ίδιες. Είμαστε σε διαφορετικό (κατώτερο) σημείο στην ιεραρχία και οι απαντήσεις που παίρνουμε για τους υπεύθυνους εξυπηρετητές είναι διαφορετικές.
- 1.9: Είναι 5. Ένας από αυτούς είναι ο "diomedes.noc.ntua.gr" με IPv4 147.102.222.220
- 1.10: Η απάντηση δεν είναι η ίδια ακριβώς. Μου δίνει τους ίδιους server, ωστόσο, τώρα παίρνω περισσότερες πληροφορίες για τις διευθύνσεις IPv4, IPv6 αυτών.
- 1.11: Το πλήθος τος είναι 3. Ένας που δεν ταυτίζεται με αυτούς του ερωτήματος 1.9 είναι ο "psyche.cn.ece.ntua.gr"
- 1.12: Μεταλλειολόγοι: Έχω 4 servers τα ονόματα των οποίων είναι: achilles.noc.ntua.gr, diomedes.noc.ntua.gr, serifos.metal.ntua.gr, ulysses.noc.ntua.gr

Χημικοί: Έχω 3 servers με ονόματα: diomedes.noc.ntua.gr, achilles.noc.ntua.gr, ulysses.noc.ntua.gr

- 1.13: Ο κύοιος DNS για την πεοιοχή αυτή είναι: psyche.cn.ece.ntua.gr με IPv4 147.102.40.1 και serial 2022120501
- 1.14: refresh time = 8 hours
- 1.15: TTL = 1 day

1.16: Για τη περιοχή ece.ntua.gr έχουμε: achilles.noc.ntua.gr με IPv4 147.102.222.210 και serial 2022101000

refresh time = 1 day, TTL = 1 day

1.17: Παρατηρούμε ότι παράγονται από κάποια ημερομηνία

1.18:	Πανεπιστήμιο	Όνομα	Διευθύνσεις
	Πανεπιστήμιο Θεσσαλίας	uth.gr	194.177.200.19 (IPv4)
	ЕМП	ntua.gr	147.102.224.101 (IPv4)
			2001:648:2000:de::210 (IPv6)
	Οικ. Πανεπιστήμιο Αθηνών	aueb.gr	195.251.255.156 (IPv4)

1.19: 147.102.40.18 → bbb.cn.ece.ntua.gr 147.102.40.19 → bbb2.cn.ece.ntua.gr

1.20: Η διεύθυνση IPv4 είναι γραμμένη ανάποδα ως προς τα byte της (πρώτα το λιγότερο σημαντικό byte). Ο τρόπος αναπαράστασης αυτός ταιριάζει με την μορφή που χρησιμοποιείται στην περιοχή .arpa που είναι υπεύθυνη για την απάντηση αντίστροφων ερωτήσεων (ονόματα από διευθύνσεις)

1.21: Όνομα: lemmy.metal.ntua.gr και IPv4: 147.102.121.10

1.22: f1.mail.ntua.gr και achilles.noc.ntua.gr

1.23: Θα προτιμηθεί αυτός με τον μικρότερο αριθμό προτίμησης (MX preference). Δηλαδή, ο f1.mail.ntua.gr

1.24: Μας εμφανίζει μια λίστα με τις εγγραφές της περιοχής central.ntua.gr

1.25:

NS: central.ntua.gr. NS netsrv0.central.ntua.gr

MX: central.ntua.gr. MX 10 achilles.noc.ntua.gr

A: 243gateway A 147.102.243.200

ΑΑΑΑ: δεν βοέθηκε

CNAME: acadinfo CNAME beta.central.ntua.gr

ΗΙΝΓΟ: δεν βοέθηκε

TXT: central.ntua.gr. TXT "v=spf1 ip4:147.102.222.0/24

ip6:2001:648:2000:de::/64 a -all"

SOA: central.ntua.gr. SOA netsrv0.central.ntua.gr dnsmaster.central.ntua.gr.

(180 21600 1800 604800 900)

## 2 – Ποωτόκολλο DNS

- 2.1: ipconfig -flushdns
- 2.2: Φίλτρο σύλληψης: host 147.102.236.96
- 2.3: Θέλαμε να χρησιμοποιήσουμε τον DNS server 147.102.40.1 οπότε χρησιμοποιήσαμε την εντολή "server 147.102.40.1" και θέλαμε να βρούμε ένα όνομα από μια διεύθυνση άρα την εντολή "set q=ptr"
- 2.4: Όνομα (147.102.40.10) = titan.cn.ece.ntua.gr
- 2.5: Φίλτρο απεικόνισης: dns
- 2.6: Πρωτόκολλο μεταφοράς: UDP
- 2.7: Έγιναν 4 αιτήματα DNS
- 2.8: Έγιναν περισσότερα των 2 γιατί στην αρχή κάναμε εκκαθάριση της DNS cache
- 2.9: Προέλευση Προορισμός
  Αίτημα 62960 53
  Απάντηση 53 62960
- 2.10: Η θύρα 53 αντιστοιχεί στο DNS
- 2.11: Μήκος επικεφαλίδας DNS = 12 bytes
- 2.12: Transaction ID (πρώτου αιτήματος για το όνομα του 147.102.40.10) = 0x0003. Η αντίστοιχη απόκριση έχει το ίδιο Transaction ID
- 2.13: Length(Flags) = 2 bytes
- 2.14: Το πρώτο bit
- 2.15: To 6° bit
- 2.16: Questions: 1

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

- 2.17: Ναι
- 2.18: Answer RRs: 1

Authority RRs: 3 Additional RRs: 6

2.19: Ναι, εμφανίστηκαν

- 2.20: Ναι, την πληφοφοφία την βρίσκουμε στα Flags
- 2.21: Φίλτρο απεικόνισης: dns.flags.response == 1 and ip.src!= 147.102.236.96
- 2.22: 16 ΙΡν4 διευθύνσεις
- 2.23: Περιλαμβάνει 1 ερώτηση
- 2.24: Περιλαμβάνει 17 Answer RRs
- 2.25: Κάθε μία από τις εγγραφές αυτές αντιστοιχεί σε μία από τις διευθύνσεις που είδαμε στο ερώτημα 2.22. Η  $17^{\eta}$  απάντηση σχετίζεται με το alias της σελίδας που βρέθηκε
- 2.26: Υπάρχει μια τέτοια εγγραφή γιατί αυτή μας δίνει πληροφορία για την alias της σελίδας για την οποία ρωτήσαμε
- 2.27: Φιλοξενείται από πολλούς υπολογιστές, αφού υπάρχουν πολλές ΙΡ για αυτό
- 2.28: Πεοιλαμβάνει 5 Answer RRs
- 2.29: cnn-tls.map.fastly.net: type AAAA, class IN, addr 2a04:4e42::773
- 2.30: Η επιπλέον καταγραφή που παρατηρούμε απαντά στο ερώτημα
- 1.1.1.1.in-addr.arpa: type PTR, class IN, one.one.one.one
- 2.31: 14 Answer RRs
- 2.32: 1 Answer RR
- 2.33: Όνομ $\alpha$  = danaos.cslab.ece.ntua.gr και Διεύθυνση ηλ. Ταχυδομείου = root.danaos.cslab.ece.ntua.gr
- 2.34: 1 Answer RR. Το κανονικό όνομα είναι "www.cn.ece.ntua.gr" και η διάρκεια ζωής της εγγραφής είναι 20 minutes
- 2.35: 3 Answer RRs. Το όνομα του πλέον προτιμότερου είναι το "achilles.noc.ntua.gr". Βέβαια όλοι έχουν preference 20 αλλά αυτόν δείχνει πρώτο, οπότε αναφέρω αυτόν
- 2.36: 2 Answer RRs. Μήκος εγγραφής TXT = 81 bytes και μεταφέρει 69 bytes πληροφορίας
- 2.37: 1 Authority RR και 0 στα υπόλοιπα. Η απόκοιση παραπέμπει στην αρχή πληροφορίας για την περιοχή ntua.gr γιατί, όπως είδαμε και στο ερώτημα 1.12, προτιμούμε να αφαιρέσουμε το "www." από το όνομα του εξυπηρετητή ιστού για να βρούμε το όνομα της περιοχής
- 2.38: Έγιναν 2 αιτήματα και πήρα απάντηση και στα δύο. Χρησιμοποιήθηκε το πρωτόκολλο μεταφοράς UDP για το πρώτο και TCP για το δεύτερο

- 2.39: αίτημα προς εξυπηρετητή 147.102.222.210 προέλευση προορισμός 51234 53
- 2.40: Length = 37 bytes και 2 bytes που αναφέρονται ως Extraneous Data
- 2.41: type: AXFR και χοησιμοποιείται για μεταφορά ζώνης DNS, η οποία είναι μηχανισμός για replication μιας DNS βάσης δεδομένων
- 2.42: Ο εξυπηρετητής απάντησε με 2 πακέτα. Το πρώτο μεταφέρει 1 μήνυμα DNS και το δεύτερο μεταφέρει 8 μηνύματα DNS. Έχουν μεγέθη 84, 55, 56, 56, 56, 56, 51, 55, 78 bytes
- 2.43: Έχουν το ίδιο Transaction ID με το αίτημά μας
- 2.44: Όλες οι απαντήσεις έχουν 1 Answer RR και κανενός άλλου τύπου RR
- 2.45: Η αλλαγή πρωτοκόλλου στρώματος μεταφοράς σε TCP έγινε ώστε η μεταφορά των δεδομένων να είναι πιο αξιόπιστη
- 2.46: Φίλτρο σύλληψης: port 53
- 2.47: Bytes (Δεδομένων) Τιμές
  1° c0
  11° 00
  4° ποιν το τέλος 00
  τελευταίο 80

Το  $1^{\circ}$  byte της απόκοισης είναι c0, αλλά καλύτερα να δούμε τα πρώτα 2 bytes μαζί που είναι c0 0c. Με βάση τους δείκτες που αναφέρονται στο RFC 1035 έχουμε ότι τα πρώτα δύο bit είναι μονάδες σηματοδοτώντας ότι η δυάδα αυτή είναι δείκτης σε προηγούμενη εμφάνιση του ίδιου ονόματος. Τα υπόλοιπα bit, δηλαδή, ο αριθμός c δηλώνει το offset από την αρχή του ID πεδίου του DNS πακέτου στο οποίο εμφανίζεται το όνομα στο οποίο δείχνει αυτός ο δείκτης (θεωρώντας το πρώτο byte του ID ως offset = 0)

To 110 byte είναι 00 γιατί είναι κομμάτι του πεδίου Data Length = 00 25 ή 37 (decimal)

Το  $4^{\circ}$  byte  $\alpha \pi \acute{o}$  το τέλος είναι 00 γιατί είναι μέρος του  $\pi ε \acute{o}$ ίου Minimum TTL = 00 01 51 80

Το τελευταίο byte είναι 80 γιατί είναι το τελευταίο byte του παραπάνω πεδίου

- 2.48: achilles.noc.ntua.gr, όμως έχουμε ξανασυναντήσει το όνομα ntua.gr. Τα δύο τελευταία byte c0 16 (εξαιρώντας τα 2 πρώτα bit που είναι μονάδες σηματοδοτώντας ότι τα δύο αυτά bytes είναι δείκτης) μας λένε ότι θα βρούμε το όνομα ntua.gr στη θέση με offset = 0x16 μέσα στο DNS πακέτο, είναι δείκτης σε προηγούμενη εμφάνιση αυτού του ονόματος
- 2.49: Η διεύθυνση αυτή είναι ένας δείκτης μόνο. Δείχνει στην εμφάνιση του noc.ntua.gr στη θέση με offset = 0x38, η οποία παρατηρούμε ότι είναι η εμφάνιση του ονόματος αυτού μέσα στο όνομα του κύριου εξυπηρετητή DNS (achilles.noc.ntua.gr) που είδαμε προηγουμένως