Ονοματεπώνυμο: Πυλιώτης Αθανάσιος		**Ομάδα: 3**
Όνομα PC/ΛΣ: DESKTOP-5DLG3IF	**Ημερομηνία:**	**13/12/2022**
Διεύθυνση IP: 147.102.203.229	**Διεύθυνση MAC:**	**98:54:1b:bd:69:97**

Εργαστηριακή Άσκηση 10
Σύστημα Ονομασίας Περιοχών DNS

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 root-servers.**net**

1.2 13 servers εμφανίστηκαν.

a.root-servers.net internet address = 198.41.0.4

a.root-servers.net AAAA IPv6 address = 2001:503:ba3e::2:30

1.3 server 198.41.0.4

1.4 Ανήκουν στη περιοχή ics.forth**.gr**

1.5 6 περιοχές.

estia.ics.forth.gr internet address = 139.91.191.3

estia.ics.forth.gr AAAA IPv6 address = 2001:648:2c30::191:3

1.6 Είναι ίδιες με τις απαντήσεις του 1.4 . Παρατηρούμε πως ανήκουν στην ίδια περιοχή και τα gr. Και τα ntua.gr. Συμπεραίνουμε πως απαντούν με τις περιοχές DNS που βρίσκονται στο πρώτο επίπεδο.

1.7 server 139.91.191.3

1.8 Nope, καθώς τώρα εμείς βρισκόμαστε στο .gr και σε άλλο επίπεδο είναι το αμέσως επόμενο, δηλαδή τα grnet.gr και ntua.gr σε αυτή τη περίπτωση.

1.9 3 απάντησαν μόνο και μία από αυτές είναι:

achilles.noc.ntua.gr internet address = 147.102.222.210

1.10 Το αρχικό μέρος της απάντησης είναι ίδιο, αλλά στη συνέχεια μας δίνει επίσης και τις IPv6 διευθύνσεις όλων, καθώς και τις IPv4 διευθύνσεις των grnet.gr που μας έδειξε πριν.

1.11 3 εμφανίστηκαν, εκ των οποίων 2 είχαν εμφανιστεί και στο 1.9 . Αυτό που δεν έιχε εμφανιστεί είναι το:

psyche.cn.ece.ntua.gr internet address = 147.102.40.1

1.12 Για τους Μεταλλειολόγους έχουμε τη περιοχή:

serifos.metal.ntua.gr internet address = 147.102.121.1

και τις 3 που βρήκαμε στο 1.9

Για τη ΣΕΜΦΕ εχουμε τη περιοχή:

Έχουμε τις 3 που απάντησαν μόνο στο 1.9

Αυτό συμβαίνει επειδή έχει άλλο εξυπηρετητή για τις σχολές ΜΜΜ και ΑΤΜ που αναφέρονται.

1.13 primary name server = psyche.cn.ece.ntua.gr

IPv4 = 147.102.40.1

Serial Number = 2022120501

1.14 refresh Κάθε 8 ώρες

1.15 default TTL = 86400 (1 day) 1*24 = 24 ώρες

1.16 primary name server = achilles.noc.ntua.gr

IPv4 = 147.102.222.230

Serial Number = 2022101000

refresh = 86400 (1 day)

default TTL =86400 (1 day)

1.17 Δείχνει την τελευταία ημερομηνία που έγινε ανανέωση της ζώνης στους πρώτους 8 αριθμούς (έτος, μήνας, μέρα) και μετά δείχνει το sequence της ενημέρωσης στη μέρα εκείνη (0, 1 κτλ). Πολλές φορές μπορεί να μην ανανεωθεί ωστόσο.

1.18 www.auth.gr , IPv4 = 155.207.1.12, IPv6 = δεν μας δίνει

www.uoc.gr , IPv4 = 147.52.80.1 , IPv6 = 2001:648:2c00:50::1

www.tuc.gr , IPv4 = 147.27.15.134 , IPv6 = δεν μας δίνει

1.19 theseas.softlab.ece.ntua.gr (147.102.1.1), ulysses.noc.ntua.gr (147.102.222.230)

1.20 όχι είναι reverse lookup, είναι της μορφής 1.1.102.147.in-addr.arpa

1.21 primary name server = serifos.metal.ntua.gr με IPv4: 147.102.121.1

1.22 mail exchanger = f1.mail.ntua.gr, IPv4 = 147.102.222.196

mail exchanger = f0.mail.ntua.gr, IPv4 = 147.102.222.195

1.23 Έχουν ίδια τιμή ex preference οι δύο παραπάνω και τη μικρότερη, άρα ένας από αυτούς τους δύο, είτε τυχαία είτε ο f0.mail.ntua.gr γιατί έχει μικρότερη διεύθυνση IPv4.

1.24 Δείχνει όλες τις καταγραφές του DNS domain. Όλα τα SOA, Cname, NS, MX, TXT, A, AAAA δηλαδή που βλέπαμε τόση ώρα από το central.ntua.gr. -d απλά δείχνει τα πάντα που έχουν καταγραφεί

1.25 central.ntua.gr. **SOA** netsrv0.central.ntua.gr dnsmaster.central.ntua.gr. (180 21600 1800 604800 900)

central.ntua.gr. **TXT** "v=spf1 ip4:147.102.222.0/24 ip6:2001:648:2000:de::/64 a -all"

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

central.ntua.gr. **NS** netsrv0.central.ntua.gr

243gateway **A** 147.102.243.200

acadinfo **CNAME** beta.central.ntua.gr

2

2.1 ipconfig /flushdns

2.2 host 147.102.203.229

2.3 set q=a (που είναι το default)

2.4 titan.cn.ece.ntua.gr

2.5 dns

2.6 UDP

2.7 9 πακέτα

2.8 Έγιναν 6 από αυτά για να βρουν τη διεύθυνση μέσω του in-addr.arpa, που έχει inverse lookup για να βρούμε τις διευθύνσεις που ψάχνουμε και τα αντίστοιχα ονόματα τους. Τα άλλα 3 είναι τα 2 για σύνδεση με Microsoft και το api τους, τα οποία πιθανότατα δεν είναι μέρος της άσκησης.

2.9 Src Port: 58092 (αλλάζει σε κάθε αίτημα), Dst Port: 53

2.10 53, στο destination, αντιστοιχεί σε DNS service.

2.11 12 bytes

2.12 Transaction ID: 0x0004

Transaction ID: 0x0004

Είναι ίδια! Για να καταλαβαίνουν πως πρόκειται για την απάντηση στο συγκεκριμένο request.

2.13 2 bytes

2.14 το 1ο

2.15 το 6ο

2.16 Domain Name System (query)

Transaction ID: 0x0004

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

2.17 Domain Name System (response)

Transaction ID: 0x0004

Flags: 0x8580 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 3

Additional RRs: 6

Queries

Answers

Authoritative nameservers

Additional records

Ναι περιέχει την ερώτηση στο Queries ακριβώς ίδια.

2.18 Answer RRs: 1

Authority RRs: 3

Additional RRs: 6

2.19 όχι δεν εμφανίστηκαν, μόνο το answer.

2.20 Όχι, η πληροφορία βρίσκεται στα flags και συγκεκριμένα στο 6ο bit:

.... .0.. .... = Authoritative: Server is not an authority for domain

2.21 dns.flags.response == 1

2.22 16 IPv4 addresses

2.23 1 question only

2.24 Answer RRs: 17 so only 17 Answer RRs εγγραφές RR.

2.25 Η μία απάντηση είναι για CNAME με τη διεύθυνση και μετά οι 16 IPv4 addresses που αντιστοιχούν στο YouTube, ίδιες με αυτές που μας έδειξε το nslookup.

2.26 Επειδή χρειάζεται να μας δείξει την actual ονομασία του domain, γιατί το www.youtube.com είναι alias και το original domain είναι youtube-ui.l.google.com

2.27 Σίγουρα θα φιλοξενείται σε περισσότερους υπολογιστές. Κάθε ένας από αυτούς μπορεί να έχει ένα πλήθος από διευθύνσεις, αλλά δεν είναι δυνατόν μια τόσο μεγάλη υπηρεσία με τόσα πολλά IP Addresses να είναι σε ένα μόνο υπολογιστή. Σε ομάδα που είμαι και έχουμε μια σελιδούλα για μερικές χιλιάδες άτομα, έχουμε 2 servers για παράδειγμα :)

2.28 5 answer RRs

2.29 CNAME: cnn-tls.map.fastly.net

AAAA Address: 2a04:4e42::773

2.30 υπάρχουν άλλα 4 (τα 3 ωστόσο είναι για google, inbox and whatsapp, άρα άκυρα με την άσκηση). Υπάρχει ένα πρώτο που χρησιμοποιείται για να δοθεί στον server η ονομασία του one.one.one.one. Άρα απαντάει το PTR για τον 1.1.1.1 server.

2.31 Answer RRs: 14, types: 3 TXT, 1 AAAA, 1 A, 3 MX, 1 SOA, 5 NS

2.32 Answer RRs: 1, μόνο το SOA που ζητήσαμε

2.33 Primary name server: danaos.cslab.ece.ntua.gr

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

2.34 Answer RRs: 1

CNAME: www.cn.ece.ntua.gr

Time to live: 1200 (20 minutes)

2.35 Answer RRs: 3

Όλα έχουν ίδια προτίμηση 20, άρα το Mail Exchange: ulysses.noc.ntua.gr που ήταν πρώτο μάλλον, αλλιώς έχει ίδια προτίμηση με τα Mail Exchange: achilles.noc.ntua.gr και Mail Exchange: diomedes.noc.ntua.gr

2.36 Answer RRs: 2

Είναι 81 bytes όλη η απάντηση και 69 data length και 68 TXT Length (που για τη δεύτερη πληροφορία χρειάστηκε 1 byte για να την πάρουμε).

2.37 Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

Μας στέλνει σε αυτή επειδή λογικά δεν έχει το authority να απαντήσει και μας στέλνει σε αυτόν που ξέρει πως έχει το authority, δηλαδή τον Primary name server: achilles.noc.ntua.gr.

2.38 5 DNS που έχουν να κάνουν με την άσκηση, 3 responses. UDP το πρώτο και TCP τα τελευταία.

2.39 Transmission Control Protocol, Src Port: 51940, Dst Port: 53, (request)

Transmission Control Protocol, Src Port: 53, Dst Port: 51940 (response)

Transmission Control Protocol, Src Port: 53, Dst Port: 51940 (response)

2.40 39 bytes

2.41 Type: AXFR (transfer of an entire zone) (252). Χρησιμοποιεί TCP και παίρνει τη μορφή client-server transaction. Στέλνει ένα κομμάτι από το database ως μια ζώνη. Ο χρήστης που ζητάει το zone transfer μπορεί να είναι δευτερεύων που ζητάει δεδομένα από πρωτεύων.

2.42 86 bytes στο zone transfer και 53 – 80 bytes στο δεύτερο και ήρθαν 8 DNS responses. (ταιριάζει με το πλήθος στο command prompt).

2.43 Έχουν ίδιο transaction ID: 0x0003

2.44 Στο zone transfer έχει 1 questions, 1 Answer RRs. Στο άλλο είναι:

1 Answer RRs σε κάθε ένα και τα υπόλοιπα είναι όλα 0.

2.45 Θέλουμε να υπάρχει consistency στο DNS Zone Database. Για αυτό χρησιμοποιείται TCP, επειδή το TCP είναι αξιόπιστο και βεβαιώνεται πως τα zone data είναι consistent επειδή μεταφέρουν όλη τη ζώνη σε άλλους DNS Servers που έχουν ζητήσει δεδομένα.

2.46 port 53, δεν έχει DNS αλλά μπορεί να καταγράφει μόνο το port για το DNS.

2.47 1^{ο} : 09, 11^{ο} : 04, 4^{ο} από τέλος: 02, τελευταίο: 00 . Το 09 δείχνει πως μετά από αυτό έρχονται 9 byte, το 04 δείχνει πως μετά από αυτό έρχονται 4 bytes, μετά από το 02 έρχονται 2 bytes και το 00 αποτελεί το τελευταίο byte και δείχνει πως τελειώνει το όνομα. Είναι για λόγους συμπίεσης που αναφέρονται παραπάνω.

2.48 Τα πρώτα 2 bit είναι 11 όπως σε κάθε pointer και τα υπόλοιπα 14 είναι 00000000010110 που δείχνει σε αυτή τη τοποθεσία που είναι τα δεδομένα που θέλει να βρει για να συνεχίσει.

2.49 Ξεκινάει επίσης με 11 και μετά είναι 00000000111000 που είναι άλλο σημείο κοντά στο προηγούμενο λογικά, γιατί μοιάζουν πολύ (απλά έχει και το noc. Αντί για το .ntua.gr)