Δίκτυα Υπολογιστών
Εργαστηριακή Άσκηση 10

Ονοματεπώνυμο: Κυριακόπουλος Γεώργιος – el18153
Ομάδα: 4
Όνομα PC/ΛΣ: George – Windows 10 Pro, 21H2
Ημερομηνία: 02/01/2022
Διεύθυνση IP: 192.168.1.8
Διεύθυνση MAC: 60-A4-B7-75-72-0F

Άσκηση 1:

1.1.
Οι εξυπηρετητές DNS που εμφανίζονται ανήκουν στην περιοχή κορυφής (*root zone*), δηλαδή είναι οι εξυπηρετητές κορυφής (*root name servers*).

1.2.
Εμφανίστηκαν 13 εξυπηρετητές κορυφής και η διεύθυνση IPv4 και IPv6 ενός από αυτούς (*a.root-servers.net*) είναι 198.41.0.4 και 2001:503:ba3e::2:30 αντίστοιχα.

1.3.
Η εντολή που χρησιμοποίησα είναι *server 198.41.0.4.*

1.4.
Οι εξυπηρετητές DNS που εμφανίζονται βρίσκονται στην ακριβώς από κάτω περιοχή (σε σχέση με την περιοχή κορυφής).

1.5.
Εμφανίστηκαν 6 εξυπηρετητές για την περιοχή *gr.* και η διεύθυνση IPv4 και IPv6 ενός από αυτούς (*gr-c.ics.forth.gr*) είναι 194.0.1.25 και 2001:678:4::19 αντίστοιχα.

1.6.
Εμφανίζονται οι ίδιοι 6 εξυπηρετητές για την περιοχή *ntua.gr*. Οι εξυπηρετητές κορυφής απαντούν λόγω του *q=ns* με τους υπεύθυνους εξυπηρετητές της περιοχής της ερώτησης. Επομένως, καταλαβαίνουμε πως και για τις δύο αυτές περιοχές αντιστοιχούν οι ίδιοι 6 υπεύθυνοι εξυπηρετητές.

1.7.
Η εντολή που χρησιμοποίησα είναι *server 139.91.191.3.*

1.8.
Αυτή τη φορά λαμβάνω διαφορετικούς εξυπηρετητές υπεύθυνους για την περιοχή *ntua.gr*. Ο λόγος είναι ότι πλέον ο εξυπηρετητής DNS που με εξυπηρετεί βρίσκεται ένα επίπεδο πιο κάτω, άρα έχει διαφορετικούς υπεύθυνους εξυπηρετητές DNS για την περιοχή αυτή.

1.9.
Εμφανίστηκαν 5 εξυπηρετητές για την περιοχή *ntua.gr* και η διεύθυνση IPv4 ενός από αυτούς (*achilles.noc.ntua.gr*) είναι 147.102.222.210.

1.10.
Οι εξυπηρετητές που εμφανίζονται αυτή τη φορά είναι οι ίδιοι 5 με του ερωτήματος 1.8., ωστόσο αυτή τη φορά εμφανίζονται οι διευθύνσεις IPv4 και IPv6 και των 5 εξυπηρετητών, ενώ νωρίτερα εμφανίζονταν μόνο οι διευθύνσεις IPv4 για 3 από αυτούς και καθόλου διευθύνσεις IPv6.

1.11.
Εμφανίστηκαν 3 εξυπηρετητές για την περιοχή *cn.ntua.gr* και το όνομα ενός από αυτούς που να μην ταυτίζεται με κάποιον από τους εξυπηρετητές του ερωτήματος 1.9. είναι *psyche.cn.ece.ntua.gr*.

1.12.
Βρήκα τα ονόματα των υπεύθυνων εξυπηρετητών DNS για τις σχολές ΑΜ και ΗΜΜΥ. Παρατηρώ ότι υπάρχουν 3 κοινοί εξυπηρετητές DNS (*ulysses.noc.ntua.gr, achilles.noc.ntua.gr, diomedes.noc.ntua.gr*), ενώ η σχολή ΑΜ έχει και 3 παραπάνω δικούς της (ανήκουν στην περιοχή *arch.ntua.gr*) υπεύθυνους εξυπηρετητές DNS, δηλαδή σύνολο 6.

1.13.
Ο κύριος εξυπηρετητής DNS της περιοχής *cn.ntua.gr* είναι ο *psyche.cn.ece.ntua.gr* με διεύθυνση IPv4 147.102.40.1 και σειριακό αριθμό 2021122301.

1.14.
Ένας δευτερεύων εξυπηρετητής θα αναζητήσει αλλαγές σχετικά με την περιοχή *cn.ntua.gr* κάθε 8 ώρες (*refresh = 28800).*

1.15.
Οι εγγραφές σχετικές με την περιοχή *cn.ntua.gr* διατηρούνται στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών για 24 ώρες (*default TTL = 86400).*

1.16.
Ο κύριος εξυπηρετητής DNS της περιοχής *ece.ntua.gr* είναι ο *achilles.noc.ntua.gr* με διεύθυνση IPv4 147.102.222.210 και σειριακό αριθμό 2021100700.
Ένας δευτερεύων εξυπηρετητής θα αναζητήσει αλλαγές σχετικά με την περιοχή ece.*ntua.gr* κάθε 24 ώρες (*refresh =86400).*

Οι εγγραφές σχετικές με την περιοχή *ece.ntua.gr* διατηρούνται στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών για 24 ώρες (*default TTL = 86400).*

1.17.
Φαίνεται πως οι τιμές των σειριακών αριθμών ακολουθούν κάποιο μοτίβο με μορφή YYYY-MM-DD και μετά 2 ψηφία που αυξάνονται κατά 1 κάθε φορά που γίνεται ενημέρωση των εγγράφων RR.

1.18.
Για το ΕΚΠΑ έχουμε: όνομα εξυπηρετητή ιστού *sites2.uoa.gr*, διεύθυνση IPv4 195.134.71.228 και ψευδώνυμο *www.uoa.gr*.
Για το ΟΠΑ έχουμε: όνομα εξυπηρετητή ιστού *www-cl.aueb.gr*, διεύθυνση IPv4 195.251.255.156 και ψευδώνυμο *www.aueb.gr*.
Για το ΑΠΘ έχουμε: όνομα εξυπηρετητή ιστού *www.ccf.auth.gr*, διεύθυνση IPv4 155.207.1.12, διεύθυνση IPv6 2001:648:2800:1:155:207:1:12 και ψευδώνυμο *www.auth.gr*.

1.19.
Για τη διεύθυνση 147.102.40.17 έχουμε όνομα *pegasus.cn.ece.ntua.gr*, ενώ για τη διεύθυνση 147.102.40.29 έχουμε όνομα *bellerephon.cn.ece.ntua.gr*.

1.20.
Η μορφή αναπαράστασης της διεύθυνσης IPv4 είναι, για παράδειγμα για την 147.102.40.17, 17.40.102.147.in-addr.arpa, λόγω του reverse lookup που γίνεται στην περιοχή ανώτατου επιπέδου *arpa,* δεδομένου ότι όσο προχωράνε οι στάθμες κάτω από το ανώτατο επίπεδο, γράφονται τα bytes της IPv4 διεύθυνσης ξεκινώντας από το πρώτο (147), για να γίνει η αντιστοιχία διεύθυνσης και ονόματος, με αποτέλεσμα μετά να διαβάζονται ανάποδα, δηλαδή από το τελευταίο και προς τα πίσω.

1.21.
Το κανονικό όνομα του υπολογιστή που φιλοξενεί την ιστοθέση της Σχολής ΜΜΜ του Ε.Μ.Π. (*www.metal.ntua.gr*) είναι *gyali.metal.ntua.gr*, ενώ η διεύθυνση IPv4 του είναι 147.102.121.5.

1.22.
Δύο από τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής *arch.ntua.gr* είναι οι *diomedes.noc.ntua.gr* και *f1.mail.ntua.gr*.

1.23.
Θα προτιμηθεί ο *f1.mail.ntua.gr*, καθώς αυτός έχει το μικρότερο *MX preference = 10,* ενώ ο *diomedes.noc.ntua.gr* έχει *MX preference = 100.*

1.24.
α) Με τη χρήση αυτής της εντολής βλέπουμε τις εγγραφές της περιοχής *central.ntua.gr*, μέσω του εξυπηρετητή DNS *achilles.noc.ntua.gr,* ο οποίος είχε οριστεί νωρίτερα.

1.25.
Για το είδος εγγραφής NS έχουμε: *central.ntua.gr. NS achilles.noc.ntua.gr.*
Για το είδος εγγραφής MX έχουμε: *central.ntua.gr. MX 10 achilles.noc.ntua.gr.*
Για το είδος εγγραφής A έχουμε: *central.ntua.gr. A 147.102.222.46.*
Για το είδος εγγραφής CNAME έχουμε: *acadinfo CNAME beta.central.ntua.gr.*
Για το είδος εγγραφής TXT έχουμε: central.ntua.gr. *TXT "v=spf1 ip4:147.102.222.0/24 ip6:2001:648:2000:de::/64 a -all"*
Για το είδος εγγραφής SOA έχουμε: *central.ntua.gr. SOA netsrv0.central.ntua.gr dnsmaster.central.ntua.gr. (176 21600 1800 604800 900)*
Για όσα είδη δεν αναφέρθηκε κάτι, δεν υπήρχε κάποια σχετική εγγραφή (AAAA, HINFO).

Άσκηση 2:

2.1.
Χρησιμοποίησα την εντολή *$ ipconfig /flushdns.*

2.2.
Χρησιμοποίησα το φίλτρο σύλληψης *host 147.102.131.232.*

2.3.
Χρησιμοποίησα με τη σειρά τις υπο-εντολές *set domain=., server 147.102.40.1, set q=ptr, 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.
Χρησιμοποίησα το φίλτρο απεικόνισης *dns*.

2.6.
Το πρωτόκολλο εφαρμογής DNS χρησιμοποιεί το πρωτόκολλο μεταφοράς UDP.

2.7.
Έγιναν σύνολο 6 αιτήματα προς εξυπηρετητές DNS από τον υπολογιστή μου.

2.8.
Τα παραπάνω από 2 αιτήματα έγιναν διότι πριν τρέξω τις αναζητήσεις των ονομάτων των 2 υπολογιστών, είχα καθαρίσει την DNS cache του υπολογιστή μου και χρειάστηκε να τρέξουν κάποια παραπάνω αιτήματα για να ανακαλύψει τα ονόματα/διευθύνσεις για άλλους υπολογιστές.

2.9.
Για το αίτημα χρησιμοποιήθηκαν η θύρα προέλευσης 49391 και προορισμού 53, ενώ για την απόκριση η θύρα προέλευσης 53 και προορισμού 49391.

2.10.
Η θύρα 53 αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS.

2.11.
Η επικεφαλίδα DNS έχει μήκος 12 byte.

2.12.
Το *Transaction ID* για το πρώτο αίτημα για το όνομα του 147.102.40.10 είναι ίσο με 0x0003. Το ίδιο ακριβώς έχει και η απόκριση για αυτό το αίτημα, ώστε να υποδεικνύει ότι αποτελεί απάντηση σε αυτό.

2.13.
Το πεδίο *Flags* της επικεφαλίδας DNS έχει μήκος 2 byte.

2.14.
Το πρώτο bit του πεδίου *Flags* είναι αυτό που δηλώνει εάν το μήνυμα είναι αίτημα ή απόκριση.

2.15.
Το έκτο bit του πεδίου *Flags* είναι αυτό που δηλώνει κατά πόσο η απόκριση προέρχεται από τον επίσημο εξυπηρετητή DNS.

2.16.
Στο πρώτο αίτημα για το όνομα του 147.102.40.10 περιέχεται 1 ερώτηση και τίποτα άλλο.

2.17.
Η απόκριση του πρώτου αιτήματος περιλαμβάνει την ερώτηση για την οποία απαντά.

2.18.
Αυτή η απόκριση περιλαμβάνει 1 εγγραφή RR απάντησης, 3 επίσημων εξυπηρετητών και 6 επιπρόσθετες.

2.19.
Ναι, εμφανίζονται στο παράθυρο της γραμμής εντολών η 1 απάντηση, οι 3 των επίσημων εξυπηρετητών και οι 6 επιπρόσθετες με τις διευθύνσεις IPv4 και IPv6 αυτών.

2.20.
Χρησιμοποίησα το φίλτρο απεικόνισης *dns.flags.response == 1*.

2.21.
Το *www.youtube.com* φαίνεται να έχει 16 διευθύνσεις IPv4 σύμφωνα με το nslookup.

2.22.
Το μήνυμα της απόκρισης για τη διεύθυνση IPv4 του *www.youtube.com* περιλαμβάνει 1 ερώτηση.

2.23.
Η παραπάνω απόκριση περιλαμβάνει 17 εγγραφές RR απάντησης, 4 επίσημων εξυπηρετητών και 5 επιπρόσθετες.

2.24.
Οι 16 από τις 17 εγγραφές RR απάντησης είναι οι 16 διευθύνσεις IPv4, ενώ αυτή που απομένει μας ενημερώνει για το cname του *www.youtube.com*, δηλαδή το *youtube-ui.l.google.com*.

2.25.
Αυτή η εγγραφή RR τύπου *CNAME* υπάρχει διότι το *www.youtube.com* αποτελεί ψευδώνυμο του *youtube-ui.l.google.com* που είναι το κανονικό όνομα του ιστότοπου, δηλαδή το *cname* του.

2.26.
Με μία δεύτερη αναζήτηση βρέθηκαν διαφορετικές IPv4 διευθύνσεις (2 λιγότερες). Επομένως, μπορούμε να καταλάβουμε ότι φιλοξενείται από περισσότερους από έναν υπολογιστές και για αυτό βλέπουμε αυτή τη διαφορά που ίσως να οφείλεται σε κάποιο downtime ή αλλαγή σε κάποιον υπολογιστή.

2.27.
Η απόκριση για τη διεύθυνση IPv6 του *www.cnn.com* περιλαμβάνει 2 εγγραφές RR απάντησης.

2.28.
Η απόκριση αυτή περιλαμβάνει 4 εγγραφές επίσημων εξυπηρετητών. Αυτοί οι εξυπηρετητές είναι υπεύθυνοι για την περιοχή *fastly.net*. Αυτό δικαιολογείται από το γεγονός ότι το *www.cnn.com* είναι και αυτό ένα ψευδώνυμο για το κανονικό όνομα (*cname*) *turner-tls.map.fastly.net*.

2.29.
Η απόκριση αυτή περιλαμβάνει 4 επιπρόσθετες εγγραφές. Αυτές περιλαμβάνουν τις διευθύνσεις IPv4 των 4 επίσημων εξυπηρετητών.

2.30.
Ένας από τους 4 επίσημους εξυπηρετητές είναι ο *ns1.fastly.net* με διεύθυνση IPv4 23.235.32.32.

2.31.
Η απόκριση για τον *www.ntua.gr* περιλαμβάνει 2 εγγραφές RR απάντησης, 5 επίσημων εξυπηρετητών και 9 επιπρόσθετες. Οι 2 απάντησης περιλαμβάνουν τις διευθύνσεις IPv4 και IPv6, οι 5 επίσημων εξυπηρετητών περιλαμβάνουν τους 5 επίσημους εξυπηρετητές και οι 9 επιπρόσθετες περιλαμβάνουν τις 5 διευθύνσεις IPv4 των επίσημων εξυπηρετητών και 4 διευθύνσεις IPv6 αυτών (ένας δεν έχει).

2.32.
Η απόκριση για την περιοχή *cslab.ntua.gr* περιέχει 1 εγγραφή RR απάντησης, 4 επίσημων εξυπηρετητών και 7 επιπρόσθετες.

2.33.
Το όνομα (*mname - master name)* του κύριου εξυπηρετητή DNS της περιοχής *cslab.ntua.gr* είναι *danaos.cslab.ece.ntua.gr*, ενώ η διεύθυνση ηλεκτρονικού ταχυδρομείου (*rname - reponsible's name)* του διαχειριστή αυτής είναι *root.danaos.cslab.ece.ntua.gr*.

2.34.
Εκτός από τον κύριο εξυπηρετητή, οι άλλοι επίσημοι εξυπηρετητές για την περιοχή *cslab.ntua.gr* είναι οι *diomedes.noc.ntua.gr, ulysses.noc.ntua.gr και achilles.noc.ntua.gr*.

2.35.
Η απόκριση για το κανονικό όνομα (cname) του *www.cn.ntua.gr* περιέχει 1 εγγραφή RR

απάντησης, 3 επίσημων εξυπηρετητών και 6 επιπρόσθετες, ενώ το κανονικό όνομα αυτού είναι το *www.cn.ece.ntua.gr*.

2.36.
Η απόκριση σχετικά με τους αρμόδιους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής *elab.ntua.gr* περιέχει 3 εγγραφές RR απάντησης, 3 επίσημων εξυπηρετητών και 6 επιπρόσθετες, ενώ οι 3 εξυπηρετητές ηλεκτρονικού ταχυδρομείου του (*achilles.noc.ntua.gr, diomedes.noc.ntua.gr, ulysses.noc.ntua.gr*) είναι ισότιμοι με *MX preference = 20*.

2.37.
Έγιναν 2 αιτήματα DNS, λήφθηκαν 3 αποκρίσεις DNS και χρησιμοποιήθηκαν τόσο το πρωτόκολλο μεταφορά UDP όσο και το TCP.

2.38.
Για το αίτημα χρησιμοποιήθηκαν η θύρα προέλευσης 64840 και προορισμού 53, ενώ για τις αποκρίσεις η θύρα προέλευσης 53 και προορισμού 64840.

2.39.
Το μήκος του αιτήματος DNS είναι 39 byte.

2.40.
Ο τύπος του αιτήματος είναι *AXFR (transfer of an entire zone)* και το νόημα του είναι η αναπαραγωγή μίας βάσης δεδομένων ενός εξυπηρετητή DNS σε έναν ή περισσότερους άλλους εξυπηρετητές DNS.

2.41.
Οι αποκρίσεις του 147.102.222.210 έχουν μήκος 86 και 475 byte και μεταφέρουν 1 και 8 μηνύματα DNS (response) αντίστοιχα.

2.42.
Τα προηγούμενα μηνύματα DNS φαίνεται ότι αποτελούν απάντηση στο αίτημα DNS που έγινε, αφού όλα τα πεδία *Transaction ID* των επικεφαλίδων DNS έχουν την ίδια τιμή (0x000f), ίση με την τιμή του αντίστοιχου πεδίου του αιτήματος.

2.43.
Όλα τα 9 μηνύματα περιλαμβάνουν 1 εγγραφή RR απάντησης και 0 από τα υπόλοιπα.

2.44.
Το πρωτόκολλο DNS, αρχικά, επέτρεπε μέχρι και 512 byte μέγεθος πακέτου. Για μεγαλύτερο μέγεθος χρησιμοποιούταν το TCP πρωτόκολλο μεταφοράς, όπως συνέβαινε με τα πακέτα σχετικά με μεταφορά ζώνης (*AXFR*), κάτι που έμεινε, παρά την αλλαγή του ορίου για το μέγεθος ενός πακέτου DNS.

2.45.
Πρέπει να χρησιμοποιήσω το φίλτρο σύλληψης *port 53*, ώστε να καταγράφονται μόνο

μηνύματα DNS (περνάνε από τη θύρα 53, η οποία αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS, πάντα).