Ονοματεπώνυμο: ΙΟΡΔΑΝΙΔΗΣ ΚΡΙΤΩΝ
Ομαδα: 1
Όνομα PC/OS: Kriton’s Air / MacOS 13.0.1
Ημερομηνία: 20/12/2022
Διεύθυνση IP: 147.102.203.123
Διεύθυνση MAC: –

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 10: ΣΥΣΤΗΜΑ ΟΝΟΜΑΣΙΑΣ ΠΕΡΙΟΧΩΝ DNS

Άσκηση 1

1.1 Στη ρίζα του δέντρου (.net)
1.2 Εμφανίζονται 13 εξυπηρετητές DNS. Ένα παράδειγμα είναι ο a.root-servers.net με διεύθυνση IPv4 την 198.41.0.4 και IPv6 την 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 αυτήν την περιοχή. Ένα παράδειγμα είναι ο gr-d.ics.forth.gr με IPv4 διεύθυνση την 194.0.11.102 και IPv6 την 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 gr-d.ics.forth.gr
1.8 Η απάντηση προφανώς δεν είναι ίδια αφου αλλάξαμε επίπεδο στο οποίο αναζητούμε
1.9 Υπάρχουν 5 εξυπηρετητές και ένα παράδειγμα είναι ο diomedes.noc.ntua.gr με IPv4 διεύθυνση την 147.102.222.220
1.10 Ναι
1.11 Είναι 3 και ένας από αυτούς είναι ο psyche.cn.ece.ntua.gr
1.12 Εμφανίζεται ένα υποσύνολο απο τους εξυπηρετητές του ntua.gr και στο survey.ntua.gr εμφανίζει επίσης τον mercator.survey.ntua.gr
1.13 Είναι ο psyche.cn.ece.ntua.gr με IPv4 147.102.40.1 και σειριακό αριθμό 2022120501
1.14 Κάθε 8 ώρες
1.15 Για 24 ώρες
1.16 Για την περιοχή ece.ntua.gr, έχουμε κύριο εξυπηρετητή τον achilles.noc.ntua.gr με διεύθυνση 147.102.222.210 και σειριακό αριθμό 2022101000. Ένας δευτερεύων εξυπηρετητής αναζητά αλλαγές κάθε 24 ώρες και οι εγγραφές διατηρούνται στη προσωρινή μνήμη για 24 ώρες
1.17 Παρατηρώ ότι πρόκειται για ημερομηνία αφού ξεκινούν με 2022
1.18 ΕΚΠΑ –> uoa.gr (195.134.71.229), ΑΠΘ –> auth.gr (155.207.1.12), Πανεπιστήμιο Κρήτης –> uoc.gr (147.52.80.1)
1.19 147.102.40.16 –> trillium.cn.ece.ntua.gr
147.102.40.17–> pegasus.cn.ece.ntua.gr
1.20 Όχι, έχουν την μορφή reverse lookup (<ip.addr>.in-addr.arpa)
1.21 lemmy.metal.ntua.gr
1.22 ulysses.noc.ntua.gr (147.102.222.230), 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 Παραδείγματα:

central.ntua.gr. 86400 IN SOA netsrv0.central.ntua.gr. dnsmaster.central.ntua.gr. 180 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 MX 10 ulysses.noc.ntua.gr.
central.ntua.gr. 86400 IN NS netsrv0.central.ntua.gr.
central.ntua.gr. 86400 IN A 147.102.222.46
acadinfo.central.ntua.gr. 86400 IN CNAME beta.central.ntua.gr.

Άσκηση 2

2.1 sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder
2.2 host 147.102.203.123
2.3 set q=ptr
2.4 titan.cn.ece.ntua.gr
2.5 dns
2.6 UDP
2.7 4
2.8 Αυτό οφείλεται στο ότι καθάρισα τη DNS cache
2.9 θύρα προέλευσης: 59926 και θύρα προορισμού: 53 στο αίτημα και στην απόκριση προφανώς οι θύρες αντιστρέφονται
2.10 Η 53
2.11 12 bytes
2.12 0x0b97. Προφανώς είναι το ίδιο και για το αίτημα και για την απόκριση
2.13 2 bytes
2.14 Το πρώτο
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
2.21 dns.flags.response==1
2.22 16
2.23 1
2.24 Περιλαμβάνει 17 απαντήσεις RR
2.25 Πρόκειται για τις 16 διευθύνσεις του προηγούμενου ερωτήματος συν την απάντηση που πήραμε για το canonical name του YouTube
2.26 Γιατι το www.youtube.com είναι alias
2.27 Σαφώς το YouTube φιλοξενείται από πολλούς υπολογιστές και για αυτό βλέπουμε πολλαπλές διευθύνσεις IPv4
2.28 5 RR απαντήσεις
2.29 cname=cnn-tls.map.fastly.net (2a04:4e42::773)
2.30 SOA
2.31 Έχουμε 14 RR απαντήσεις (SOA, NS, A, AAAA, MX, TXT)
2.32 1 RR απάντηση
2.33 mname: danaos.cslab.ece.ntua.gr, rname: root.danaos.cslab.ece.ntua.gr
2.34 1 RR απάντηση, cname=www.cn.ece.ntua.gr, TTL=20 min
2.35 3 RR απαντήσεις, ενώ δεν υπάρχει προτιμότερος καθώς και οι τρεις έχουν preference=20
2.36 2 RR απαντήσεις. Μία TXT απάντηση έχει μήκος 81 byte με μήκος πληροφορίας 69 bytes

2.37 Η απόκριση περιέχει 1 επίσημο εξυπηρετητή μόνο. Η απόκριση παραπέμπει την αρχή πληροφόρησης για το ntua.gr ίσως επειδή δεν υπάρχουν εγγραφές για το όνομα που ζητήθηκε
2.38 Έγιναν: 1 αίτημα DNS, 2 αποκρίσεις DNS και χρησιμοποιήθηκε το πρωτόκολλο TCP
2.39 Θύρα προέλευσης: 49313, θύρα προορισμού: 53
2.40 60 bytes
2.41 Είναι μήνυμα τύπου AXFR και χρησιμοποιείται για την αντιγραφή όλων των εγγραφών μεταξύ εξυπηρετητών AXFR
2.42 Έχουμε 9 DNS responses. Αυτά έχουν μήκος: 123, 94, 95, 95, 91, 95, 90, 94 και 117
2.43 Έχουν όλα τα μηνύματα το ίδιο Transaction ID
2.44

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

2.45 Γιατί με το AXFR μεταφέρεται μεγάλος όγκος δεδομένων και επίσης χρειάζεται αξιοπιστία
2.46 port 53
2.47 Το 1ο byte έχει τιμή 11000000 (υποδεικνύει ότι είναι pointer), το 11ο 00000000 (το 1ο byte απο το data length πεδίο), το 4ο πριν το τέλος 00000000 (1ο byte από το minimum TTL πεδίο) και το τελευταίο 10000000 (τελευταίο byte από το minimum TTL πεδίο)
2.48 Είναι pointer με offset 10110=22
2.49 Είναι και πάλι pointer