Εθνικό Μετσόβιο Πολυτεχνείο
Δίκτυα Υπολογιστών
Χειμερινό Εξάμηνο 2022-2023
Όνομα:
Ιωάννης Μπασδέκης - 03119198

Όνοματεπώνυμο: Ιωάννης Μπασδέκης	**Ομάδα:** A1
Όνομα PC/ΛΣ: MacBook-Air-Giannes / macOS	**Ημερομηνία:** 14/12/2022
Διεύθυνση IP: 147.102.236.188	**Διεύθυνση MAC:** b0:be:83:20:37:35

9η Εργαστηριακή Αναφορά

Μέρος 1ο

1.1) .net

1.2) 13 nameservers a.root-servers.net.
IPv4 =198.41.0.4 , IPv6 =2001:503:ba3e::2:30

1.3) server 198.41.0.4

1.4) .gr

1.5) 6 nameservers gr-d.ics.forth.gr
IPv4= 194.0.11.102
IPv6= 2001:678:e:102::53

1.6) Είναι τα ίδια γιατί δεν έχουμε αλλάξει server (επίπεδο) και οι top level servers απαντούν για την περιοχή .gr

1.7) server gr-d.ics.forth.gr

1.8) Όχι γιατί αφού αλλάξαμε εξυπηρετητή DNS κατεβήκαμε επίπεδο στην ιεραρχία οπότε παίρνουμε απαντήσεις για την περιοχή .ntua.gr

1.9) 5 (2 grnet.gr 3 ntua.gr) ulysses.noc.ntua.gr internet address = 147.102.222.230

1.10) Ναι

1.11) 3 psyche.cn.ece.ntua.gr

1.12) Τα ΜΜΜ έχουν έναν δικό τους NS και 3 κοινούς ενώ οι άλλες σχολές δεν έχουν δικό τους παρά μόνο τους 3 κοινούς

1.13) psyche.cn.ece.ntua.gr
2022120501
147.102.40.1

1.14) refresh = 28800 (8 ώρες)

1.15) minimum = 86400 (24 ώρες)

1.16) achilles.noc.ntua.gr
2022101000
147.102.222.210
refresh = 86400 (24 ώρες)
minimum = 86400 (24 ώρες)

1.17) Μάλλον είναι κάποια ημερομηνία ή συγκεκριμένη ώρα από την τελευταία ανανέωση καθώς ξεκινάει από το 2022

1.18) ΕΚΠΑ (uoa.gr) -> 195.134.71.229
ΑΠΘ (auth.gr) -> 155.207.1.12
Πάντειο Πανεπιστήμιο(panteion.gr) -> 194.177.218.26

1.19)147.102.40.20 -> syn1.cn.ece.ntua.gr
147.102.40.23 -> cn-monitor-1.cn.ece.ntua.gr

1.20) 23.40.102.147.in-addr.arpa name = cn-monitor-1.cn.ece.ntua.gr.
Είναι σε αντίστροφη μορφή λόγω της αντίστροφης αναζήτησης DNS

1.21) canonical name = lemmy.metal.ntua.gr
147.102.121.10

1.22) diomedes.noc.ntua.gr
f0.mail.ntua.gr

1.23) 10 f0.mail.ntua.gr ή 10 f1.mail.ntua.gr
Έχουν τον μικρότερο αριθμό προτεραιότητας

1.24) Είναι ένα πρωτόκολλο που χρησιμοποιείται για zone transfer. Μεταφέρει ολόκληρο το zone file από το βασικό nameserver στα δευτερεύοντα name servers

1.25) 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.

central.ntua.gr. 86400 IN SOA netsrv0.central.ntua.gr. dnsmaster.central.ntua.gr. 180 21600 1800 604800 900

Μέρος 2ο
(έγινε από το σπίτι με vpn με ip = 147.102.131.154)

2.1) sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder

2.2) host 147.102.131.154

2.3) set q=a
server 147.102.40.1
147.102.40.10
server 147.102.7.1
147.102.40.10

2.4) titan.cn.ece.ntua.gr

2.5) dns

2.6) udp

2.7) 9

2.8) 2 έγιναν για να βρούμε το όνομα της IP 147.102.40.10 και τα άλλα 7 διάφορα domains που ζήτησε ο υπολογιστής μου (όπως openvpn)

2.9) source port: 63219 destination port:53 (για request)

2.10) 53

2.11) 12 bytes

2.12) 0x2d88 . Είναι ίδιο

2.13) 2 bytes

2.14) Το πρώτο

2.15) Το 6ο

2.16) Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

2.17) Ναι

2.18) Questions: 1
Answer RRs: 1
Authority RRs: 3
Additional RRs: 6

2.19) Ναι

2.20) Στο 6ο bit του πεδίου flag =Authoritative: Server is not an authority for domain

2.21) dns.flags.response == 1

2.22) 16

2.23) 1

2.24) 17 RR , 16 type A , 1 type CNAME

2.25) Είναι οι 15 διευθύνσεις IPv4 του www.youtube.com συν μία για το came του

2.26) Γιατί το www.youtube.com είναι alias

2.27) Υπάρχουν παραπάνω από έναν server που κάνουν host το www.youtube.com καθώς έχουμε πολλαπλές IPv4 διευθύνσεις οι οποίες μένουν ίδιες όσες φορές καλέσω την εντολή απλά αλλάζει η σείρα που μάλλον έχει να κάνει με το latency κάθε server

2.28) 5

2.29) CNAME= cnn-tls.map.fastly.net
IPv6 : 2a04:4e42::773

2.30) Δεν παρατηρώ κάποια τρίτη απόκριση (πιθανώς να έπρεπε να πάρω κάποια απόκριση με την εντολή server 1.1.1.1 αλλά ήδη τον χρησιμοποιούσα για DNS server)

2.31) 14 -> 1 SOA , 5 NS , 3 MX , 1 A , 1 AAAA , 3 TXT

2.32) 1

2.33) mname= danaos.cslab.ece.ntua.gr
mail= root.danaos.cslab.ece.ntua.gr

2.34) 1 RR
cname= www.cn.ece.ntua.gr.
TTL = 20 mins

2.35) diomedes.noc.ntua.gr
ulysses.noc.ntua.gr
achilles.noc.ntua.gr
Και οι τρεις έχουν αριθμό προτίμησης = 20 οπότε δεν προτιμάτε κάποιος έναντι κάποιου

2.36) 2 RR
114 bytes length
txt data length = 101 bytes

2.37) Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Γιατί με την επιλογή set q=ns ψάχνουμε nameservers μιας περιοχής. Το www.ntua.gr είναι domain name όχι περιοχή οπότε για αύτο μας παραπέμπει στο SOA του ntua.gr (για να δούμε το master name τις περιοχής)

2.38) 1 αίτημα και 2 αποκρίσεις DNS με πρωτόκολλο tcp

2.39) Source Port =59435 Destination Port = 53
(για τις αποκρίσεις είναι το αντίθετο)

2.40) 48 bytes

2.41) TYPE = AXFR . Είναι ένα πρωτόκολλο για zone transfer (το είδαμε και στο πρώτο μέρος)

2.42) 1η απόκριση -> 97 bytes (1 response)
2η απόκριση -> 563 bytes (8 responses)
Σύνολο 1+8 =9 DNS response μεταφέρουν

2.43) Και οι δύο αποκρίσεις έχουν ίδιο Transaction ID με το αίτημα (0x5c35)

2.44) 1ο DNS Response (στην 1η απόκριση):
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1

Στην 2η απόκριση όλα τα DNS Response έχουν :
Questions: 0
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1

Άρα σύνολο : 1 Question, 9 Answer RRs, 0 Authority RRs, 9 Additional RRs

2.45) Διότι έχουμε μεταφορά ζώνης DNS και μεταφέρουμε εγγραφές άλλης περιοχής θέλουμε να είναι πιο ασφαλής η σύνδεση και για αυτό χρησιμοποιούμε tcp αντί για το σύνηθες udp καθώς είναι πιο secure. Άλλος ένας λόγος είναι το μεγάλο μέγεθος των data

2.46) 1ο byte -> 11000000 (dec = 192) . Κανονικά τα labels με βάση το φαινόμενο της συμπίεσης πρέπει να είναι μέχρι το 63 (00111111). Εδώ ο αριθμός ξεκινάει με 11 που υποδεικνύει ότι είναι ένας pointer με offset = 000000 + το αμέσως επόμενο byte (εδώ είναι 00001100) 0000000000001100 = 12 (dec). Αυτός ο pointer δείχνει σε ποια θέση από την αρχή του μηνύματος (για την ακρίβεια στο RFC1035 σαν αρχή του μηνύματος θεωρεί το ID όχι το length που βρίσκουμε στο wireshark οπότε ό,τι offeset βρίσκουμε το αυξάνουμε κατα 2)βρίσκεται το label που επαναλαμβάνεται. Στην συγκεκριμένη περίπτωση εμφανίζεται πρώτα στο πεδίο Queries στην θέση 14(πρώτη θέση έχει τιμή 0).

11ο byte -> 00000000 . Είναι το πρώτο από τα 2 bytes που αντιστοιχούν στο πεδίο data length . Αυτό το byte μαζί με το επόμενο (00100101) μας κάνουν τον αριθμό 37 (dec) που είναι η τιμή του πεδίου data length

4ο byte (από το τέλος) -> 00000000 . Είναι το πρώτο από τα 4 bytes που αντιστοιχούν στο πεδίο minimun TTL . Αυτό το byte μαζί με τα επόμενα (00000001 01010001 10000000) μας κάνουν τον αριθμό 86400 (dec) που είναι η τιμή του πεδίου minumum TTL (seconds)

Τελευταίο byte -> 10000000 . Είναι το 4ο από τα 4 bytes που αντιστοιχούν στο πεδίο minumum TTL. Η εξήγηση είναι ίδια με το παραπάνω

2.47) Παριστάνουν έναν pointer (11000000 00010110) με offset 0000000010110 = 22 (+2 = 24 για τον λόγο που αναφέραμε στο 2.46) Η χρήση του υποδεικνύει ότι το .ntua.gr label έχει ξαναχρησιμοποιηθεί στην θέση 24 του μηνύματος.

2.48) Ότι έχουμε πάλι περίπτωση pointer (11000000 00111000)και εδώ το offset είναι 56 (+2 = 58) άρα το .noc.ntua.gr έχει ξαναχρησιμοποιηθεί στην θέση 58, το οποιό ισχύει αφού υπάρχει η συγκεκριμένη λίστα από labels στο Primary name server . Το αξιοσημείωτο σε αυτή την περίπτωση είναι ότι και στην περίπτωση του primary name server = achilles.noc.ntua.gr το .ntua.gr παριστάνεται και αυτό με pointer (βλεπε 4.6) οπότε ο pointer που δείχνει στην θέση 58 ουσιαστικά δείχνει στο label .noc του primary name server και σε έναν άλλον δείκτη