Ονοματεπώνυμο: Ιωάννης Γιαννούκος			**Ομάδα:** 3
Όνομα PC/ΛΣ: JohnJohn / Windows 11		**Ημερομηνία:**	**13/1/2023**
Διεύθυνση IP: **147.102.200.45**	**Διεύθυνση MAC:**		**3C-6A-A7-9A-B3-CF**

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.

Άσκηση 1

1.1) Οι εξυπηρετητές που εμφανίζονται ανήκουν στην περιοχή κορυφής (root zone), δηλαδή στην πρώτη στάθμη, δηλαδή στο υποδέντρο με ρίζα τον κόμβο ".". Οι εξυπηρετητές αυτοί ονομάζονται εξυπηρετητές κορυφής (root name servers).

1.2) Εμφανίστηκαν 13 εξυπηρετητές. Ένας από αυτούς είναι ο εξής:
Όνομα: b.root-servers.net
IPv4 address: 199.9.14.201
IPv6 address: 2001:500:200::b

1.3) "`lserver b.root-servers.net`"

1.4) Οι εξυπηρετητές που εμφανίζονται αφού εκτελεστεί η εντολή gr. ανήκουν στην 2η στάθμη του Σχήματος 1, στο υποδέντρο με ρίζα τον κόμβο "gr".

1.5) Εμφανίστηκαν 6 εξυπηρετητές, ένας από τους οποίους είναι ο εξής:
Όνομα: estia.ics.forth.gr
IPv4 address: 139.91.191.3
IPv6 address: 2001:648:2c30::191:3

1.6) Από τον εκτέλεση της εντολής "ntua.gr." λαμβάνω ακριβώς τα ίδια αποτελέσματα με αυτά που έλαβα και στο υποερώτημα (1.4), διότι δεν χρησιμοποιώ διαφορετικό εξυπηρετητή DNS. Επομένως, από την διαπίστωση αυτή συμπεραίνουμε ότι οι εξυπηρετητές που εμφανίζονται ανήκουν στις διευθύνσεις των εξυπηρετητών DNS που ανήκουν στο ίδιο επίπεδο με αυτόν που χρησιμοποιώ, δηλαδή τον b.root-servers.net.

1.7) "`lserver estia.ics.forth.gr`"

1.8) Όχι, η απάντηση που εμφανίζεται τώρα διαφέρει με αυτήν του υποερωτήματος (1.6). Αυτό συμβαίνει επειδή ο εξυπηρετητής DNS που χρησιμοποιώ τώρα (estia.ics.forth.gr) βρίσκεται σε χαμηλότερο επίπεδο από την προηγούμενη φορά, και έτσι εμφανίζονται εξυπηρετητές μικρότερου υποδέντρου, το οποίο ανήκει στο παραπάνω του υποερωτήματος (1.6).

1.9) Εμφανίστηκαν 5 εξυπηρετητές, ένας από τους οποίους είναι ο εξής:
Όνομα: diomedes.noc.ntua.gr
IPv4: 147.102.222.220

1.10) Όχι, η απάντηση διαφέρει και σε αυτήν την περίπτωση.

1.11) Εμφανίζονται 3 εξυπηρετητές, ένας από τους οποίους είναι ο εξής:
Όνομα: psyche.cn.ece.ntua.gr
IPv4: 147.102.40.1
IPv6: 2001:648:2000:28::1

1.12) Παρατηρώ ότι σχεδόν όλες οι σχολές έχουν κοινούς εξυπηρετητές. Για παράδειγμα, η αγρονόμοι μηχανικοί πέρα από τους κοινούς εξυπηρετητές, έχουν έναν ακόμα, τον "mercator.survey.ntua.gr".

1.13) Κύριος εξυπηρετητής:
Όνομα: psyche.cn.ece.ntua.gr
IPv4: 147.102.40.1
Serial: 2022120501

1.14) Ένας δευτερεύων εξυπηρετητής θα ρωτά τον κύριο εξυπηρετητή για αλλαγές κάθε 8 ώρες (refresh time).

1.15) Οι εγγραφές σχετικές με την περιοχή "cn.ntua.gr" διατηρούνται στους υπόλοιπους μη-επίσημους εξυπηρετητές για 1 ημέρα (TTL).

1.16) Κύριος εξυπηρετητής:
Όνομα: achilles.noc.ntua.gr
IPv4: 147.102.222.210
Serial: 2022101000
Refresh Time: 1 ημέρα
TTL: 1 ημέρα

1.17) Ναι. Κάθε φορά που ανανεώνεται ο σειριακός αριθμός ενός κύριου εξυπηρετητή DNS για πρώτη φορά μία ημέρα, τα 8 πρώτα ψηφία δηλώνουν την ημερομηνία, δηλαδή ΕΕΕΕΜΜΗΗ, και τα δύο τελευταία υπάρχουν για να διαφοροποιούνται οι εγγραφές μεταξύ τους σε περίοδο μίας ημέρας, αυξάνοντας σε κάθε ανανέωση κατά 1.

1.18) www.unipi.gr → IPv4: 195.251.229.4
www.uoa.gr → 195.134.71.228
www.uop.gr → 195.251.38.44

1.19) bbb.cn.ece.ntua.gr → 147.102.40.18
cn-monitor-1.cn.ece.ntua.gr → 147.102.40.23

1.20) Όχι, δεν έχει τη συνήθη μορφή διευθύνσεων IP. Για τις δύο παραπάνω διευθύνσεις εμφανίστηκαν τα παρακάτω αποτελέσματα:
bbb.cn.ece.ntua.gr → 18.40.102.147.in-addr.arpa
cn-monitor-1.cn.ece.ntua.gr → 23.40.102.147.in-addr.arpa

1.21) Κανονικό όνομα: serifos.metal.ntua.gr
IPv4: 147.102.121.1

1.22) f0.mail.ntua.gr → 147.102.222.195
f1.mail.ntua.gr → 147.102.222.196

1.23) Προτιμάται ο εξυπηρετητής με τον μικρότερο αριθμός προτίμησης MX Preference. Στην προκειμένη περίπτωση, οι αριθμοί MX Preference των δύο εξυπηρετητών είναι ίσοι με 10. Επομένως, μόνο σε αυτήν την περίπτωση, θα προτιμηθεί ένας εκ των δύο είτε με άλλο κριτήριο, είτε τυχαία.

1.24) Με την υποεντολή "`ls -d central.ntua.gr`" ζητούμε να εμφανισθούν όλες οι εγγραφές της περιοχής central.ntua.gr.

1.25)

Τιμή1	***Είδος***	***Τιμή2***
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	achilles.noc.ntua.gr
adminasa	A	147.102.243.222
acoustics2010	CNAME	oldwebhoster.central.ntua.gr

Άσκηση 2 (IP: 147.102.238.43)

2.1) `ipconfig /flushdns`

2.2) Φίλτρο σύλληψης: "host 147.102.238.43"

2.3)
> `set domain=ntua.gr`
> `147.102.40.10 147.102.40.1`
> `147.102.40.10 147.102.7.1`

2.4) Το όνομα της διεύθυνσης IP 147.102.40.10 είναι «titan.cn.ece.ntua.gr».

2.5) Φίλτρο απεικόνισης: "dns".

2.6) Από το DNS χρησιμοποιήθηκε το πρωτόκολλο UDP.

2.7) Ο υπολογιστής μου έκανε 3 αιτήματα προς εξυπηρετητές DNS.

2.8) Συνέβησαν 3 αιτήματα, επειδή το πρώτο έγινε για να εντοπιστεί ο εξυπηρετητής DNS με διεύθυνση IP "147.102.1.1" στον οποίο θα γίνουν τα αιτήματα.

2.9) Για το αίτημα του ονόματος με διεύθυνση 147.102.40.10 από τον εξυπηρετητή 147.102.40.1 έχουμε τα εξής:

Source Port: 53505
Destination Port: 53

Για την απόκριση στο παραπάνω αίτημα έχουμε:

Source Port: 53
Destination Port: 53505

2.10) Στο DNS πρωτόκολλο αντιστοιχεί η θύρα 53.

2.11) Η επικεφαλίδα DNS έχει μήκος 42 bytes.

2.12) Transaction ID αιτήματος: 0x0002
Transaction ID απόκρισης: 0x0002

Παρατηρούμε λοιπόν ότι για κάθε ερώτημα (query) χρησιμοποιείται το ίδιο αναγνωριστικό.

2.13) Το πεδίο Flags έχει μήκος 2 bytes.

2.14) Το πρώτο bit (bit0) δηλώνει αν το μήνυμα είναι αίτημα ή απόκριση.

2.15) Το έκτο bit (bit5) δηλώνει αν η απόκριση προέρχεται από επίσημο εξυπηρετητή DNS.

2.16) Για το πρώτο αίτημα για την εύρεση του ονόματος του 147.102.40.10 έχουμε:

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

2.17) Ναι, η απόκριση περιλαμβάνει το ερώτημα στο οποίο απαντά στην επικεφαλίδα «Queries».

2.18) Για την απόκριση του αιτήματος (υποερώτημα 2.16) έχουμε:

Answer RRs: 1
Authority RRs: 3
Additional RRs: 6

2.19) Όχι, οι παραπάνω πληροφορίες δεν εμφανίστηκαν στο παράθυρο εντολών.

2.20) Όχι, η απόκριση στο δεύτερο αίτημα για την εύρεση του ονόματος 147.102.40.10 δεν προέρχεται από τον επίσημο εξυπηρετητή DNS, πράγμα που φαίνεται από το έκτο bit της επικεφαλίδας Flags.

2.21) Φίλτρο απεικόνισης: “dns.flags.response == 1”.

2.22) Το www.youtube.com φαίνεται να έχει 16 διευθύνσεις IP.

2.23) Περιλαμβάνει 1 ερώτηση.

2.24) Η παραπάνω απόκριση περιλαμβάνει 1 απάντηση τύπου CNAME και 16 τύπου A.

2.25) Καθώς το www.youtube.com έχει πολλές διευθύνσεις IP, για κάθε μία διεύθυνση IP πρέπει να επιστραφεί μια απάντηση. Στο ερώτημα 2.22 είδαμε ότι το www.youtube.com έχει 16 διευθύνσεις, επομένως επιστράφηκαν 16 απαντήσεις τύπου A.

2.26) Η εγγραφή τύπου CNAME επιστράφηκε, επειδή το www.youtube.com φαίνεται να είναι ψευδώνυμο, και με την εγγραφή αυτή επιστράφηκε το κανονικό όνομά του.

2.27) Η ιστοθέση www.youtube.com βρίσκεται σε περισσότερους από έναν εξυπηρετητές. Το πλήθος τους δεν είναι εύκολο να διαπιστωθεί, καθώς αξίζει να επισημανθεί ότι κάθε διεύθυνση IP αντιστοιχεί σε μία διεπαφή και όχι εξολοκλήρου σε έναν εξυπηρετητή. Ωστόσο, από τα διαφορετικά προθέματα στις διευθύνσεις είναι ασφαλές να αποφανθούμε ότι φιλοξενείται σε περισσότερους από 3 εξυπηρετητές.

2.28) Το μήνυμα-απόκριση στο αίτημα για διευθύνσεις IPv6 του www.cnn.com περιλαμβάνει 4 εγγραφές.

2.29) Όνομα: cnn-tls.map.fastly.net
IPv6 address: 2a04:4e42:400::773

2.30) Η επιπλέον απάντηση απευθύνεται στην ερώτηση που ζητά το κανονικό όνομα του www.cnn.com.

2.31) Επιστράφηκαν 14 εγγραφές με τύπους SOA(1), NS(5), MX(3), A(1), AAAA(1) και TXT(3).

2.32) Επιστράφηκε 1 εγγραφή για το ερώτημα για την περιοχή cslab.ntua.gr.

2.33) Primary name server: danaos.cslab.ece.ntua.gr
Responsible mail addr: root.danaos.cslab.ece.ntua.gr

2.34) Επιστράφηκε 1 εγγραφή ως απάντηση στο ερώτημα. Το κανονικό όνομα του www.cn.ntua.gr είναι www.cn.ece.ntua.gr και η διάρκεια ζωής της εγγραφής είναι 20 λεπτά.

2.35) Επιστράφηκαν 3 εγγραφές. Οι τρεις εξυπηρετητές που αναφέρεται έχουν ίσες τιμές στο πεδίο MX preference, επομένως δεν θα προτιμηθεί κάποιος συγκεκριμένα.

2.36) Επιστράφηκαν 2 εγγραφές. Η πρώτη από τις εγγραφές που επιστρέφονται έχει μήκος 68 bytes και η πληροφορία που μεταφέρει έχει μήκος 69 bytes.

2.37) Για το μήνυμα-απόκριση αυτό έχουμε:
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Υπάρχει παραπομπή στην αρχή πληροφόρησης, καθώς δεν έχει ο ίδιος ο εξυπηρετητής απάντηση (επιστρέφονται 0 εγγραφές).

2.38) Έγιναν 2 αιτήματα DNS, λήφθηκαν 3 αποκρίσεις και χρησιμοποιήθηκαν δύο πρωτόκολλα: το UDP για το πρώτο ζευγάρι ερώτησης – απάντησης και το TCP για το δεύτερο ερώτημα και τις δύο τελευταίες αποκρίσεις σε αυτό.

2.39) Για το αίτημα προς τον εξυπηρετητή 147.102.222.210 έχουμε (UDP):
Source port: 56957
Destination port: 53
Για την απόκριση στο παραπάνω αίτημα έχουμε:
Source port: 53
Destination port: 56957

2.40) Το μήκος του αιτήματος είναι 23 bytes.

2.41) Ο τύπος του αιτήματος προς τον εξυπηρετητή είναι AXFR και χρησιμοποιείται για την μεταφορά DNS ζώνης.

2.42) Το μήκος των αποκρίσεων είναι αντίστοιχα 84 και 55 bytes. Η πρώτη απόκριση μεταφέρει 1 μήνυμα απόκριση και η δεύτερη μεταφέρει 8 μηνύματα αποκρίσεις.

2.43) Μπορούμε να αποφανθούμε για το αν οι αποκρίσεις αναφέρονται στο αίτημα που έγινε από το πεδίο Transaction ID. Ένα αίτημα και κάθε απόκριση σε αυτό φέρουν την ίδια τιμή στο προαναφερθέν πεδίο.

2.44)

	Questions	*Answer RRs*	*Authority RRs*	*Additional RRs*
1η απόκριση	1	1	0	0
2η απόκριση	0	1	0	0
3η απόκριση	0	1	0	0
4η απόκριση	0	1	0	0
5η απόκριση	0	1	0	0
6η απόκριση	0	1	0	0
7η απόκριση	0	1	0	0
8η απόκριση	0	1	0	0
9η απόκριση	0	1	0	0

2.45) Καθώς οι πληροφορίες που έπρεπε να μεταφερθούν είχαν μεγαλύτερο μέγεθος, έγινε αλλαγή στο πρωτόκολλο μεταφοράς για να γίνει πιο αξιόπιστη μεταφορά δεδομένων.

2.46) Φίλτρο σύλληψης για DNS: “port 53”

2.47) Το 1ο byte έχει τιμή 09, το 11ο byte έχει τιμή 04, το 4ο από το τέλος byte έχει τιμή 02 και το τελευταίο byte έχει τιμή 00. Το όνομα «planetlab.ntua.gr» έχει την εξής μορφή: ο πρώτος χαρακτήρας ορίζει το πλήθος των χαρακτήρων που έπονται και βρίσκονται πριν την πρώτη τελεία (.). Στο επόμενο byte από τους πρώτους χαρακτήρες βρίσκεται το επόμενο byte που ορίζει πόσοι χαρακτήρες έπονται πριν την επόμενη τελεία (.) κ.ο.κ. Το τελευταίο byte έχει τιμή 00, διότι το όνομα δεν έχει άλλους χαρακτήρες, δηλαδή ακολουθείται η ίδια λογική.

2.48) Ο προηγούμενος τρόπος αναπαράστασης ονομάτων χρησιμοποιεί όπως είδαμε ετικέτες. Για λόγους εξοικονόμησης χώρου, όταν σε ένα όνομα περιέχονται ετικέτες που έχουν εμφανιστεί προηγουμένως, τα 2 επόμενα bytes έπειτα από το τέλος του ονόματός του χρησιμοποιούνται ως δείκτης που δείχνουν στο πρώτο byte της ετικέτας που ανήκει στο εν λόγω όνομα.

2.49) Επειδή όλο το όνομα της διεύθυνσης του διαχειριστή έχει εμφανιστεί ολόκληρο προηγουμένως, δεν δίνεται κανένας χαρακτήρας, ωστόσο μόνο ένας δείκτης που δείχνει στο σημείο που ξεκινά η ετικέτα με την οποία ξεκινά η εν λόγω διεύθυνση.