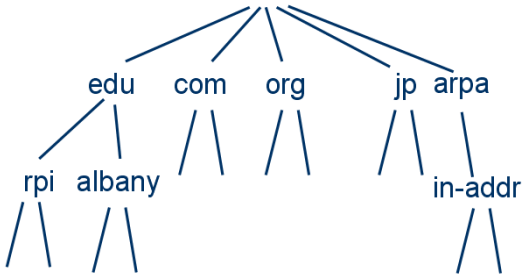
Εργαστηριακή Άσκηση 11
DNS

Ο σκοπός αυτού του εργαστηρίου είναι η εξέταση του πρωτοκόλλου εφαρμογής DNS, που χρησιμοποιείται ευρύτατα στο διαδίκτυο για την αντιστοίχηση ονομάτων σε διευθύνσεις IP, με τη βοήθεια του αναλυτή πρωτοκόλλων Wireshark. Περισσότερες πληροφορίες για τα μηνύματα του DNS μπορείτε να βρείτε στην ιστοσελίδα: http://www.networksorcery.com/enp/protocol/dns.htm.

1. Υπηρεσία DNS

Όπως αναφέρθηκε και στην Εργαστηριακή Άσκηση 2, το διαδίκτυο είναι χωρισμένο νοητά σε εκατοντάδες διαφορετικές **περιοχές** (domains) υψηλού επιπέδου, οι οποίες χωρίζονται με τη σειρά τους σε άλλες υποπεριοχές (subdomains) με πολλούς hosts η καθεμία. Η ιεραρχία των περιοχών μπορεί να παρασταθεί με ένα δέντρο (Σχήμα 1). Το όνομα κάθε host αποτελείται από μια ακολουθία *ετικετών* (labels) που χωρίζονται με τελείες (π.χ. www.mit.edu). Μια περιοχή είναι ένα υποδέντρο του παγκόσμιου δέντρου ονομάτων. Το όνομα περιοχής (domain name) για ένα host είναι η ακολουθία των ετικετών που οδηγούν από το host (φύλλο στο δέντρο ονομάτων) στην κορυφή (ρίζα) του παγκόσμιου δέντρου ονομάτων.



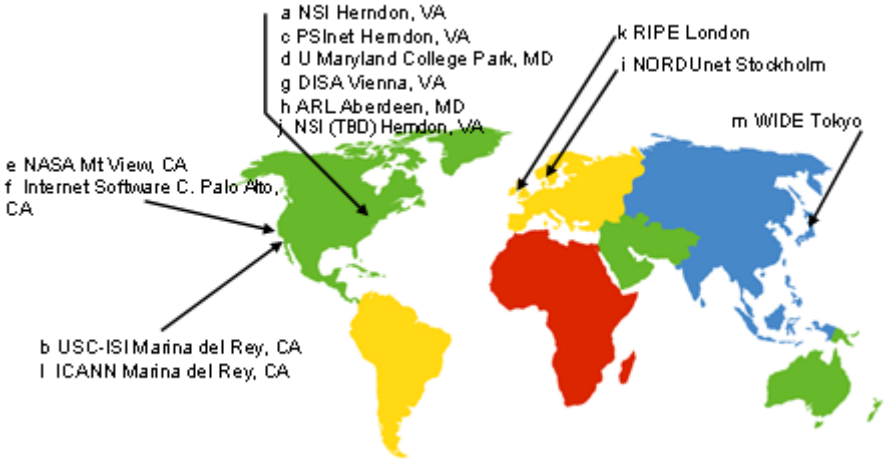
Σχήμα 1: Ιεραρχία DNS

Σε κάθε περιοχή στο διαδίκτυο (π.χ. ntua.gr) υπάρχει ένας ή περισσότεροι εξυπηρετητές DNS. Αυτοί περιέχουν μια βάση δεδομένων που αντιστοιχίζει τα ονόματα των κόμβων της συγκεκριμένης περιοχής (π.χ. atlas.central.ntua.gr) σε διευθύνσεις **IPv4** και/ή **IPv6**. Επίσης μπορεί να περιέχει εγγραφές τύπου NS με τις διευθύνσεις άλλων εξυπηρετητών DNS «υπεύθυνων» για την περιοχή (name servers), εγγραφές τύπου MX με τα ονόματα εξυπηρετητών ηλεκτρονικού ταχυδρομείου (mail exchangers), εγγραφές τύπου CNAME για τα επίσημα ονόματα υπολογιστών (canonical names), κλπ. Οι εξυπηρετητές DNS απαντούν σε αιτήσεις άλλων εξυπηρετητών DNS καθώς και χρηστών του διαδικτύου για την αντιστοιχία ενός ονόματος σε διεύθυνση IP και το αντίστροφο, ερευνώντας την παγκόσμια ιεραρχία DNS γι' αυτά. Επειδή για την εξυπηρέτηση μιας αίτησης μπορεί να γίνουν διαδοχικές ερωτήσεις σε άλλους εξυπηρετητές, ακολουθώντας την παγκόσμια ιεραρχία DNS, το αποτέλεσμα θα είναι αυξημένη καθυστέρηση. Για την αποφυγή του παραπάνω οι εξυπηρετητές DNS διαθέτουν μια προσωρινή μνήμη (cache) όπου κρατούν τις πιο πρόσφατες αιτήσεις.

Η ονομασία περιοχής ανωτάτου επιπέδου `arpa` (ίδιας στάθμης με τις `com`, `edu`, `gov`, `int`, `mil`, `net`, `org`, `ae`, …, `gr`, …, `zw`) μαζί με την περιοχή `in-addr` (που βρίσκεται αμέσως από κάτω της) χρησιμοποιείται από το DNS προκειμένου να απαντηθούν οι ερωτήσεις για το ποιο είναι το όνομα ενός υπολογιστή, δοθείσης της διεύθυνσης IP αυτού (Reverse Lookup). Στην περίπτωση του `ntua.gr`, η διεύθυνση υποδικτύου IP είναι η `147.102.0.0/16` (πρώην κατηγορία B – πρόθεμα μήκους 16 bit). Έτσι, η πρώτη στάθμη κάτω από το `in-addr.arpa` πρέπει να είναι το πρώτο byte της διεύθυνσης IP (147), η επόμενη στάθμη πρέπει να είναι το δεύτερο byte (102), κοκ. Αυτό σημαίνει ότι το όνομα DNS του υπολογιστή `147.102.222.210` είναι το

`210.222.102.147.in-addr.arpa`. Χωρίς αυτόν τον κλάδο του δέντρου DNS θα ήταν πρακτικά αδύνατη η μετάφραση διευθύνσεων σε ονόματα (για να απαντηθεί μια τέτοια ερώτηση θα έπρεπε να ερωτηθούν όλοι οι κόμβοι του δέντρου DNS κάτι που θα έπαιρνε εβδομάδες με το σημερινό μέγεθος του Internet).

Το ανώτατο επίπεδο στην ιεραρχία του DNS (η ρίζα του δέντρου) ονομάζεται περιοχή κορυφής (**root zone**), ενώ οι αντίστοιχοι επίσημοι (*authoritative*) εξυπηρετητές ονομάζονται εξυπηρετητές κορυφής (**root name servers**). Η φυσική θέση των εξυπηρετητών κορυφής φαίνεται στο Σχήμα 2. Κάθε αναζήτηση ονόματος DNS ξεκινάει είτε άμεσα από κάποιον εξυπηρετητή κορυφής ή έμμεσα από πληροφορία η οποία έχει ήδη ανακτηθεί από αυτόν και βρίσκεται στη μνήμη προσωρινής αποθήκευσης κάποιου εξυπηρετητή που βρίσκεται χαμηλότερα στην ιεραρχία. Το DNS είναι απαραίτητο για τη σωστή λειτουργία του παγκοσμίου ιστού (www), για την αποστολή ηλεκτρονικού ταχυδρομείου (e-mail), για τη χρήση περιφερειακών υπηρεσιών όπως FTP, Telnet κλπ.



Σχήμα 2: Root name servers

Η εντολή φλοιού `nslookup` μπορεί να χρησιμοποιηθεί για τη λήψη πληροφοριών από ένα εξυπηρετητή DNS. Μέσω της εντολής φλοιού `nslookup` μπορεί κανείς να ερωτήσει οποιοδήποτε εξυπηρετητή DNS για κάποια εγγραφή DNS. Ο ερωτώμενος εξυπηρετητής DNS μπορεί να είναι ένας εξυπηρετητής κορυφής, ο υπεύθυνος εξυπηρετητής της περιοχής ή οποιοσδήποτε άλλος ενδιάμεσος εξυπητερετητής. Για το σκοπό αυτό η `nslookup` στέλνει μια ερώτηση στον προσδιοριζόμενο εξυπηρετητή, λαμβάνει την απάντηση από τον εξυπηρετητή αυτό και εμφανίζει το αποτέλεσμα. Η `nslookup` μπορεί να κληθεί με ή χωρίς παραμέτρους και έχει δύο τρόπους λειτουργίας. Στο μη διαλογικό τρόπο λειτουργίας (non-interactive mode) ζητείται μια συγκεκριμένη πληροφορία, ενώ στη διαλογική χρήση (interactive mode) αναζητούνται περισσότερες της μίας πληροφορίες.

Για περισσότερες πληροφορίες σχετικά με το `nslookup` συμβουλευτείτε το Help των Windows. Πηγαίνετε στο *Start* → *Help and Support*, και στο πλαίσιο *Search* πληκτρολογήστε "TCP/IP utilities", οπότε εμφανίζονται όλες οι σχετικές εντολές. Μελετήστε προσεκτικά τις υπο-εντολές (nslookup subcommands) της εντολής `nslookup`, που θα βρείτε στο σύνδεσμο Related Topics, και εστιάστε ιδιαίτερα στην υπο-εντολή `set querytype`. Ακολουθεί παράδειγμα εκτέλεσης της εντολή `nslookup` σε μη διαλογικό τρόπο λειτουργίας (non-interactive mode).

```
C:\nslookup www.mit.edu
Server:  psyche.cn.ece.ntua.gr
Address:  147.102.40.1

Non-authoritative answer:
Name:    www.mit.edu
Address:  18.7.22.169
```

Στην προκειμένη περίπτωση ζητείται η διεύθυνση IP του host `www.mit.edu`. Επειδή στα ορίσματα της εντολής δεν ορίστηκε ο εξυπηρετητής DNS που θα ερωτηθεί, χρησιμοποιείται αυτός που έχει οριστεί τοπικά στο σύστημα (στο παράδειγμα είναι ο `psyche.cn.ece.ntua.gr`). Η έξοδος από την εκτέλεση της εντολής παρέχει δύο πληροφορίες: α) το όνομα και τη διεύθυνση IP του εξυπηρετητή DNS που απάντησε στην ερώτηση (`psyche.cn.ece.ntua.gr`) και β) την ίδια την απάντηση (`18.7.22.169`). Στο επόμενο παράδειγμα χρησιμοποιείται η `nslookup` ώστε να επιστραφεί η εγγραφή NS (δηλαδή, τα ονόματα των υπεύθυνων εξυπηρετητών) για την περιοχή `mit.edu`.

```
C:\nslookup -type=NS mit.edu
Server:  psyche.cn.ece.ntua.gr
Address:  147.102.40.1

Non-authoritative answer:
mit.edu nameserver = STRAWB.mit.edu
mit.edu nameserver = BITSY.mit.edu
mit.edu nameserver = W20NS.mit.edu

BITSY.mit.edu   internet address = 18.72.0.3
```

Τέλος, με τον ακόλουθο τρόπο κλήσης της `nslookup` ερωτάται απευθείας ο `bitsy.mit.edu`, αντί του τοπικού εξυπητετητή (`psyche.cn.ece.ntua.gr`), για την διεύθυνση IP του εξυπηρετητή ιστού `www.cn.ntua.gr` του εργαστηρίου Δικτύων Υπολογιστών.

```
C:\nslookup www.cn.ntua.gr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    www.cn.ece.ntua.gr
Address:  147.102.40.1
Aliases:  www.cn.ntua.gr
```

Για τους σκοπούς αυτής της άσκησης θα χρησιμοποιήσετε την εντολή `nslookup` στο διαλογικό τρόπο λειτουργίας (interactive mode). Ανοίξτε ένα παράθυρο εντολών και πληκτρολογήστε `nslookup` ακολουθούμενο από <Enter>. Στη συνέχεια πληκτρολογήστε `server 147.102.222.230` για να επιλέξετε τον εξυπηρετητή DNS που θα απαντά στη συνέχεια. Μέσω της υπο-εντολής `set querytype` μπορείτε να προσδιορίσετε το είδος πληροφοριών (RR-Resource Records[1]) που θα αντλήσετε από τον εξυπηρετητή DNS. Προκειμένου να βρείτε πληροφορίες σχετικές με τους υπεύθυνους εξυπηρετητές μιας περιοχής DNS χρησιμοποιείται η υπο-εντολή `set q=ns`.

1.1. Πληκτρολογήστε μια τελεία (‘`.`’) και μετά <Enter>. Σε ποια περιοχή (στάθμη του Σχήματος 1) ανήκουν οι εξυπηρετητές DNS που εμφανίζονται;
1.2. Καταγράψτε το **πλήθος** των υπεύθυνων εξυπηρετητών DNS που εμφανίστηκαν καθώς και το όνομα και τη διεύθυνση IPv4 **ενός μόνο** από αυτούς.
1.3. Πληκτρολογήστε μια εντολή ώστε να επιλέξετε ως εξυπηρετητή DNS που θα απαντά στις ερωτήσεις εκείνον τον εξυπηρετητή που διαλέξατε στο ερώτημα 1.2. Ποια είναι η σύνταξη της εντολής;
1.4. Στη συνέχεια, πληκτρολογήστε ‘`gr.`’. Σε ποια περιοχή (στάθμη του Σχήματος 1) ανήκουν οι εξυπηρετητές DNS που εμφανίζονται;
1.5. Καταγράψτε το **πλήθος** των υπεύθυνων εξυπηρετητών DNS που εμφανίστηκαν καθώς και το όνομα και τη διεύθυνση IPv6 **ενός μόνο** από αυτούς.
1.6. Πληκτρολογήστε τώρα ‘`ntua.gr.`’. Τι αποτελέσματα λαμβάνετε σε σύγκριση με αυτά του ερωτήματος 1.4;

[1] Στην ιστοθέση http://en.wikipedia.org/wiki/List_of_DNS_record_types θα βρείτε μια λίστα με τα είδη εγγραφών στα αρχεία ζώνης (zone files) του DNS.

1.7. Κατόπιν, επιλέξτε ως εξυπηρετητή DNS που θα απαντά στη συνέχεια τον `147.102.222.220` (πληκτρολογώντας την κατάλληλη εντολή). Πληκτρολογήστε και πάλι '`ntua.gr.`'. Η απάντηση που λαμβάνετε είναι ίδια με αυτήν που είδατε στο ερώτημα 1.6; Εξηγείστε γιατί.
1.8. Πληκτρολογήστε το όνομα της περιοχής του Εργαστηρίου Δικτύων Υπολογιστών του Ε.Μ.Π. (`cn.ntua.gr.`) και καταγράψτε το πλήθος των υπεύθυνων εξυπηρετητών DNS καθώς και το όνομα και την IPv4 και IPv6 διεύθυνση ενός από αυτούς.
1.9. Βρείτε τα ονόματα των υπεύθυνων εξυπηρετητών DNS για **δύο** περιοχές Σχολών του ΕΜΠ εκτός της ΣΗΜΜΥ (`ece.ntua.gr`). Τι παρατηρείτε; *[Υπόδειξη: Για να βρείτε το όνομα των περιοχών επισκεφθείτε τη σελίδα www.ntua.gr και στη συνέχεια κάντε κλικ σε δύο από τα εικονίδια-ζεύξεις (Σχολές) στο κάτω μέρος της σελίδας. (Προσοχή: αφαιρέστε το www. από το όνομα των εξυπηρετητών ιστού των Τμημάτων για να βρείτε το όνομα της περιοχής)]*

Η πρώτη εγγραφή σε οποιοδήποτε αρχείο περιοχής DNS αποκαλείται Start of Authority (SOA). Η εγγραφή SOA δηλώνει ότι ο αυτός ο εξυπηρετητής DNS είναι η επίσημη πηγή πληροφόρησης για τα δεδομένα αυτής της περιοχής DNS. Η εγγραφή SOA εκτός από το όνομα του κύριου εξυπηρετητή DNS της περιοχής, περιέχει πληροφορίες για το κάθε πότε (refresh time) ένας δευτερεύων εξυπηρετητής DNS ερωτά τον κύριο εξυπηρετητή DNS για αλλαγές. Εάν για κάποιο λόγο η μεταφορά πληροφορίας από τον κύριο εξυπηρετητή αποτύχει, ο δευτερεύων εξυπηρετητής επαναλαμβάνει μετά από λίγο (retry time) μέχρις ότου λήξει ο χρόνος (expire time). Σε αυτήν την περίπτωση, ο δευτερεύων σταματά να απαντά σε ερωτήσεις. Τέλος, με την παράμετρο TTL δηλώνεται ο χρόνος ζωής σε δευτερόλεπτα των δεδομένων στην προσωρινή μνήμη άλλων εξυπηρετητών. Κατά τη διάρκεια αυτή ένας εξυπηρετητής μπορεί να χρησιμοποιήσει τα αποθηκευμένα δεδομένα χωρίς να απευθυνθεί εκ νέου στους επίσημους εξυπηρετητές. Μπορείτε να αντλήσετε πληροφορίες (RR) σχετικές με την αρχή επίσημης πληροφόρησης για μια περιοχή πληκτρολογώντας την υπο-εντολή `set q=soa`.

1.10. Καταγράψτε τον κύριο εξυπηρετητή DNS της περιοχής `cn.ntua.gr`, την IPv4 και IPv6 διεύθυνσή του.
1.11. Κάθε πόσες ώρες θα αναζητήσει αλλαγές σχετικά με την περιοχή `cn.ntua.gr` ένας δευτερεύων εξυπηρετητής;
1.12. Για πόσες ώρες διατηρούνται οι σχετικές με την περιοχή `cn.ntua.gr` εγγραφές στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών;
1.13. Επαναλάβετε τις ερωτήσεις 1.10 και 1.12 για την περιοχή μιας σχολής του ΕΜΠ.

Για πληροφορίες (RR) σχετικές με την αντιστοίχηση ονομάτων σε IP διευθύνσεις χρησιμοποιείται η υπο-εντολή `set q=a`. Το αντίστροφο γίνεται χρησιμοποιώντας την υπο-εντολή `set q=ptr`.

1.14. Επισκεφθείτε τη σελίδα http://www.ntua.gr/gr_ked/www.htm, κάντε κλικ στο σύνδεσμο *Ανώτατη Εκπαίδευση* και βρείτε τη διεύθυνση IP του εξυπηρετητή ιστού τριών ελληνικών πανεπιστημίων. *[Υπόδειξη: Όταν αναζητούμε πληροφορίες για έναν συγκεκριμένο υπολογιστή, π.χ. έναν εξυπηρετητή ιστού, δεν παραλείπουμε να προσθέσουμε το "www.", σε αντίθεση με την αναζήτηση πληροφοριών για περιοχές (domains).]*
1.15. Βρείτε και καταγράψτε το όνομα για δύο διευθύνσεις IP (της προτίμησής σας) στο υπο-δίκτυο 147.102.40.0/28.
1.16. Αφού παρατηρήσετε τα μηνύματα της απάντησης του εξυπηρετητή στο προηγούμενο ερώτημα, καταγράψετε τη μορφή αναπαράστασης της διεύθυνσης IP, η οποία χρησιμοποιείται από το σύστημα ονοματοδότησης. Έχει τη συνήθη αριθμητική μορφή μιας διεύθυνσης IP;

Ένας υπολογιστής μπορεί να είναι γνωστός στο διαδίκτυο με πολλά ονόματα (aliases). Ένα συνηθισμένο παράδειγμα τέτοιων υπολογιστών είναι αυτοί που φιλοξενούν ιστοσελίδες στο διαδίκτυο, όπου το δευτερεύον όνομά τους είναι το όνομα της ιστοθέσης που φιλοξενούν. Για την

εύρεση του επίσημου ονόματος (canonical name) ενός υπολογιστή πληκτρολογήστε την υπο-εντολή `set q=cname`.

1.17. Καταγράψτε το επίσημο όνομα και τη διεύθυνση IPv4 του υπολογιστή που φιλοξενεί την ιστοθέση του Ε.Μ.Π.

Για την εύρεση των εξυπηρετητών ηλεκτρονικού ταχυδρομείου μιας περιοχής χρησιμοποιείται η υπο-εντολή `set q=mx`. Η σχετική εγγραφή περιλαμβάνει και την προτεραιότητα του εκάστοτε εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Το πρωτόκολλο SMTP προσπαθεί να παραδώσει το ηλεκτρονικό ταχυδρομείο στον εξυπηρετητή με τον μικρότερο αριθμό προτίμησης.

1.18. Καταγράψτε τα ονόματα και τις διευθύνσεις IPv4 και IPv6 των εξυπηρετητών ηλεκτρονικού ταχυδρομείου της περιοχής `chemeng.ntua.gr`.
1.19. Ποιος από αυτούς είναι ο πρώτος που θα προτιμηθεί για την παράδοση ηλεκτρονικού ταχυδρομείου;

Ένας εξυπηρετητής DNS μπορεί να πληροφορηθεί σχετικά με τις εγγραφές μιας άλλης περιοχής ζητώντας μια μεταφορά ζώνης (zone transfer). Αντίστοιχα, στο `nslookup` μπορείτε να ζητήσετε τις εγγραφές μιας άλλης περιοχής μέσω της υπο-εντολής `ls`.

1.20. Πληκτρολογήστε την υπο-εντολή `ls –d central.ntua.gr`. Ποια είναι η σημασία της παραπάνω σύνταξης της υπο-εντολής `ls`;
1.21. Για κάθε είδος εγγραφής (π.χ. NS, MX, A, AAAA, CNAME, HINFO, SOA, κλπ.) που θα συναντήσετε στην απάντηση της υπο-εντολής `ls` καταγράψτε τα πλήρη στοιχεία **δύο** περιπτώσεων.

2 – Πρωτόκολλο DNS

Στην άσκηση αυτή θα δείτε τη δομή των μηνυμάτων που χρησιμοποιεί το πρωτόκολλο DNS με τη βοήθεια του Wireshark. Θα χρησιμοποιήσετε τη λειτουργία *Capture* με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Υπενθυμίζεται ότι το φίλτρο απεικόνισης *(Display)*, που επιλέγετε από το μενού *Analyze,* μπορεί να (απ)ενεργοποιηθεί οποιαδήποτε στιγμή κατά τη διάρκεια της καταγραφής, καθώς επίσης και μετά την ολοκλήρωση αυτής, προκειμένου να αποκρύπτει (αποκαλύπτει) κάποια από τα συλληφθέντα πλαίσια, ενώ το φίλτρο σύλληψης, που επιλέγετε από το μενού *Capture*, ενεργοποιείται πάντοτε **πριν** ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων. Προσοχή: η απενεργοποίηση του φίλτρου απεικόνισης γίνεται πιέζοντας το κουμπί Clear (η διαγραφή του φίλτρου στο πεδίο εισαγωγής δεν το ακυρώνει!). Επίσης, αφού ξεκινήσετε το πρόγραμμα Wireshark πηγαίνετε στο *Edit → Preferences* και στη λίστα επιλογών στα αριστερά διαλέξτε το *Name Resolution*, βεβαιωθείτε ότι το Enable MAC name resolution και το Enable transport name resolution στα δεξιά είναι επιλεγμένα και πατήστε *OK*.

Με τη βοήθεια του Wireshark να καταγράψετε την κίνηση ενώ κάνετε χρήση της υπηρεσίας DNS. Εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με την διεύθυνση IP του υπολογιστή σας και ξεκινήστε την καταγραφή. Ανοίξτε ένα παράθυρο εντολών και καθαρίστε την προσωρινή μνήμη DNS (DNS cache) που διατηρεί ο υπολογιστής χρησιμοποιώντας την εντολή φλοιού `ipconfig` με την κατάλληλη επιλογή. Στη συνέχεια εκτελέστε το πρόγραμμα `nslookup` ακολουθούμενο από `<Enter>` ώστε να εισέλθετε στο διαλογικό τρόπο λειτουργίας. Μετά εκτελώντας τις κατάλληλες υπο-εντολές της `nslookup` βρείτε το όνομα του υπολογιστή `147.102.40.9` έχοντας ως εξυπηρετητή DNS τον υπολογιστή `147.102.222.210` και τερματίστε την καταγραφή. Εφαρμόστε κατάλληλο φίλτρο απεικόνισης ώστε να παραμείνουν μόνο μηνύματα του πρωτοκόλλου DNS.

2.1 Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε;
2.2 Ποια είναι η ακριβής σύνταξη της εντολής για τον καθαρισμό της προσωρινής μνήμης DNS; *[Υπόδειξη: Για βοήθεια πληκτρολογήστε* `ipconfig /?`*]*.

2.3 Ποιες υπο-εντολές της `nslookup` χρησιμοποιήσατε για να βρείτε το ζητούμενο όνομα υπολογιστή;
2.4 Ποιο είναι το όνομα αυτό;
2.5 Ποια είναι η σύνταξη του φίλτρου απεικόνισης που χρησιμοποιήσατε;
2.6 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε από το DNS (TCP ή UDP);
2.7 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν για την πρώτη ερώτηση και απόκριση τύπου PTR.
2.8 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS;
2.9 Πόσες *ερωτήσεις* τύπου PTR γίνονται από τον υπολογιστή σας;
2.10 Για ποιο λόγο γίνεται η πρώτη ερώτηση τύπου PTR; *[Υπόδειξη: Συμβουλευτείτε τα αποτελέσματα που εμφανίζονται στην οθόνη στο παράθυρο εντολών.]*
2.11 Καταγράψτε την IP διεύθυνση προορισμού και την MAC διεύθυνση προορισμού αυτού του μηνύματος.
2.12 Σε ποιους υπολογιστές ανήκουν αυτές οι διευθύνσεις; *[Υπόδειξη: Αναφορικά με τον υπολογιστή στον οποίο ανήκει η διεύθυνση MAC, συμβουλευθείτε και τον πίνακα ARP του υπολογιστή σας]*
2.13 Για ποιο λόγο γίνεται η δεύτερη ερώτηση τύπου PTR;
2.14 Σε ποιους υπολογιστές ανήκουν η IP διεύθυνση προορισμού και η MAC διεύθυνση προορισμού του μηνύματος DNS για τη δεύτερη ερώτηση τύπου PTR;
2.15 Για ποιο λόγο γίνεται η τρίτη ερώτηση τύπου PTR;

Παρατηρώντας το περιεχόμενο των πεδίων της επικεφαλίδας όλων των μηνυμάτων DNS, απαντήστε τις επόμενες ερωτήσεις.

2.16 Καταγράψτε το Transaction ID της πρώτης ερώτησης και της αντίστοιχης απάντησης. Ποια είναι η σχέση μεταξύ τους;
2.17 Ποιο bit του πεδίου Flags της επικεφαλίδας DNS δηλώνει αν το συγκεκριμένο μήνυμα είναι ερώτηση ή απάντηση;
2.18 Το μήνυμα της πρώτης ερώτησης περιλαμβάνει "απαντήσεις";
2.19 Πόσες και ποιου είδους "απαντήσεις" περιλαμβάνει το μήνυμα της πρώτης απάντησης;

Ξεκινήστε μια νέα καταγραφή με το προηγούμενα φίλτρο σύλληψης. Εκτελέστε την υπο-εντολή `set q=a` της `nslookup` και βρείτε τη διεύθυνση IP του ονόματος `www.cnn.com`. Στη συνέχεια σταματήστε την καταγραφή και εφαρμόστε κατάλληλο φίλτρο ώστε να παραμείνουν μόνο μηνύματα DNS (αποκρίσεις) από τον εξυπηρετητή DNS.

2.20 Ποια είναι η σύνταξή του νέου φίλτρου απεικόνισης; *[Υπόδειξη: Πιέζοντας το Add Expression… για φίλτρο απεικόνισης βρείτε την κατάλληλη σύνταξη για να καθορίστε την τιμή που πρέπει να έχει το πεδίο (bit) του ερωτήματος 2.17.]*
2.21 Πόσες διευθύνσεις IP φέρεται να έχει το `www.cnn.com` σύμφωνα με το αποτέλεσμα της εντολής `nslookup`;
2.22 Δοθέντος ότι οι αποκρίσεις περιλαμβάνουν και την ερώτηση που τις προκάλεσε, εντοπίστε το μήνυμα που μεταφέρει την απόκριση του εξυπηρετητή DNS στην εντολή για να βρεθεί η διεύθυνση IP του ονόματος `www.cnn.com`. Πόσες ερωτήσεις περιλαμβάνει;
2.23 Πόσες απαντήσεις περιλαμβάνει η παραπάνω απόκριση;
2.24 Πως σχετίζονται οι απαντήσεις αυτές με τις διευθύνσεις IP που προσδιορίσατε στο ερώτημα 2.21;
2.25 Κατά τη γνώμη σας, η ιστοθέση `www.cnn.com` φιλοξενείται από έναν υπολογιστή ή περισσότερους; Αιτιολογείστε. *[Υπόδειξη: Μέσω της `nslookup` ξαναβρείτε την διεύθυνση IP του `www.cnn.com` και παρατηρείστε τις διαφορές με την προηγούμενη απάντηση του εξυπηρετητή DNS.]*

Στις αποκρίσεις του εξυπηρετητή DNS, εκτός των απαντήσεων, περιλαμβάνονται και πληροφορίες για τους επίσημους (*authoritative*) εξυπηρετητές DNS καθώς και επιπρόσθετες εγγραφές (additional records).

2.26 Πόσοι είναι οι επίσημοι εξυπηρετητές DNS για το `www.cnn.com`;
2.27 Πόσες επιπρόσθετες εγγραφές επιστρέφονται για το `www.cnn.com` και τι τύπου είναι αυτές;
2.28 Καταγράψτε το όνομα και τη διεύθυνση ενός εκ των επίσημων εξυπηρετητών DNS για το `www.cnn.com`;

Ξεκινήστε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης. Εκτελέστε τις επόμενες υπο-εντολές της `nslookup`:

- `set q=soa` και βρείτε την αρχή πληροφόρησης για την περιοχή `cslab.ntua.gr.`,
- `set q=cname` και βρείτε το επίσημο όνομα του `www.cn.ntua.gr`
- `set q=mx` και βρείτε τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής `elab.ntua.gr.`

σταματήστε την καταγραφή και εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο μηνύματα σχετικά με το πρωτόκολλο DNS. Με βάση τα αποτελέσματα της καταγραφής απαντήστε στις ακόλουθες ερωτήσεις:

2.29 Καταγράψτε το πλήθος των εγγραφών που περιέχει η απάντηση σχετικά με τον κύριο εξυπηρετητή DNS της περιοχής `cslab.ntua.gr` καθώς και το όνομα αυτού.
2.30 Καταγράψτε το πλήθος των εγγραφών που περιέχει η απάντηση σχετικά με το επίσημο όνομα του `www.cn.ntua.gr` καθώς και το όνομα αυτό.
2.31 Καταγράψτε το πλήθος των εγγραφών που περιέχει η απάντηση σχετικά με τους αρμόδιους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής `elab.ntua.gr` καθώς και το όνομα του πλέον προτιμότερου εξ αυτών.

Στη συνέχεια ξεκινήστε νέα καταγραφή με το Wireshark με φίλτρα καταγραφής και απεικόνισης όπως πριν. Προσοχή: Επειδή τα μηνύματα DNS των ερωτήσεων που ακολουθούν μεταφέρονται σε περισσότερα από ένα πακέτα, αφού ξεκινήσετε το Wireshark, ακολουθήστε από το μενού του κεντρικού παραθύρου τη διαδρομή στο *Edit → Preferences*, κάνετε κλικ στο σύμβολο δίπλα στο Protocols στην αριστερή πλευρά του παραθύρου. Κατόπιν εντοπίστε και κάνετε κλικ στο πρωτόκολλο DNS και βεβαιωθείτε ότι η επιλογή περί ανασύνθεσης είναι επιλεγμένη. Στη συνέχεια, στο πρωτόκολλο TCP, βεβαιωθείτε ότι το *Allow subdissector to reassemble TCP streams* είναι επιλεγμένο και φροντίστε το Validate the TCP checksum if possible[2] να μην είναι επιλεγμένο. Τέλος, πιέστε OK για να κλείσει το παράθυρο και να εφαρμοσθούν οι αλλαγές σας. Με τις επιλογές αυτές, μηνύματα που μεταφέρονται σε περισσότερα από ένα πακέτα θα αποκωδικοποιηθούν από το Wireshark ως πλήρη μηνύματα DNS και όχι αποσπασματικά. Στο παράθυρο εντολών της `nslookup` δώστε τις υπο-εντολές `server 147.102.40.1` και `ls –d cn.ece.ntua.gr`. Στη συνέχεια πληκτρολογήστε `exit` για έξοδο και σταματήστε την καταγραφή.

2.32 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε για καθεμιά από τις ερωτήσεις DNS;
2.33 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκε για τη δεύτερη ερώτηση προς τον εξυπηρετητή και την αντίστοιχη απάντηση.
2.34 Εντοπίστε το μήνυμα της δεύτερης ερώτησής σας προς τον εξυπηρετητή. Ποιο είναι το μήκος του μηνύματος ερώτησης DNS; *[Υπόδειξη: Επιλέξτε τη γραμμή που αντιστοιχεί στο πρωτόκολλο DNS στο παράθυρο με τις λεπτομέρειες επικεφαλίδας του Wireshark, οπότε στο κατώτατο μέρος της οθόνης θα εμφανισθεί το πλήθος των byte που το συνθέτουν.]*
2.35 Ποιος είναι ο τύπος της δεύτερης ερώτησης και ποιο το νόημά της; *[Υπόδειξη:Αναζητήστε τον όρο AXFR στην ιστοσελίδα http://en.wikipedia.org/wiki/List_of_DNS_record_types.]*

[2] Η επιβεβαίωση του TCP checksum (επειδή αυτή γίνεται στην κάρτα δικτύου) παρενοχλεί τη διαδικασία επανασύνθεσης.

2.36 Εντοπίστε το μήνυμα της απάντησης του εξυπηρετητή. Ποιο είναι το μήκος του μηνύματος απάντησης DNS;
2.37 Πόσες απαντήσεις μεταφέρονται με την απόκριση;
2.38 Γιατί νομίζετε ότι έγινε η αλλαγή πρωτοκόλλου στρώματος μεταφοράς που εντοπίσατε στο ερώτημα 2.32;

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 11
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 .....

1.2 .....

.....

1.3 .....

1.4 .....

1.5 .....

.....

1.6 .....

.....

1.7 .....

.....

1.8 .....

.....

1.9 .....

.....

.....

1.10 .....

.....

1.11 .....

1.12 .....

1.13 .....

.....

.....

1.14 .....

.....

.....

1.15 .....

.....

2