# Εργασία Πρωτόκολλα και αρχιτεκτονικές δικτύων

Περιγραφή Εργασίας: Στην παρούσα εργασία θα πραγματοποιηθεί ανάλυση πακέτων με χρήση του εργαλείου Wireshark που χρησιμοποιήθηκε κατά την διάρκεια του εξαμήνου στο μάθημα. Σκοπός της εργασίας είναι η ανάλυση πακέτων καθώς και η εφαρμογή φίλτρων για την εύρεση πακέτων από συγκεκριμένη πηγή. Επίσης θα εξεταστεί η απόδοση του δικτύου βάσει των πακέτων που μεταφέρονται καθώς και η ποιότητα μεταφοράς.

## ΜΕΡΟΣ Ι ΑΝΑΛΥΣΗ ΔΙΕΠΑΦΗΣ ΔΙΚΤΥΟΥ

**Χρησιμοποιώντας ένα τερματικό καταγράψτε:**

* Την ονομασία της κάρτας δικτύωσης(network adapter)
* Την ταχύτητα σύνδεσης
* Την διεύθυνση MAC σε δεκαεξαδική μορφή
* Τον κατασκευαστή της κάρτας δικτύωσης
* Τα συνδεδεμένα με αυτή πρωτόκολλα δικτύωσης
* Tα πρωτόκολλα δικτύωσης που συνδέονται με στο Interface
* Η ποσότητα των δεδομένων που μεταδίδονται και λαμβάνονται από τον προσαρμογέα δικτύου
* Τις IP διευθύνσεις που ο υπολογιστής σας έχει επικοινωνήσει πρόσφατα

**!! Για όλα τα παραπάνω ερωτήματα θα πρέπει να παρέχεται και το κατάλληλο στιγμιότυπο οθόνης στο οποίο θα πρέπει να είναι διακριτό και το μονοπάτι του που βρίσκεται κατά την εκκίνηση του τερματικού.**

## ΜΕΡΟΣ ΙΙ Σύλληψη και ανάλυση πακέτων με χρήση του Wireshark

Για το δεύτερο μέρος θα πρέπει να πραγματοποιήσετε τα κατάλληλα configurations πριν ξεκινήσετε το capture των πακέτων.

Στο Wireshark, επιλέξτε:

* Κατάλληλο Interface
* Κατάλληλες στήλες

Οι δύο παραπάνω ρυθμίσεις θα χρησιμεύσουν στην ορθή προετοιμασία του περιβάλλοντος για την υλοποίηση του δεύτερου μέρους της άσκησης.

Έπειτα θα χρησιμοποιήσετε το Wireshark για σύλληψη πακέτων DNS που δημιουργούνται κατά την πλοήγηση στο world wide web. **Ποιο συγκεκριμένα:**

* Αδειάστε την DNS Cache του host σας
* Ανοίξτε το Wireshark και εισάγετε το κατάλληλο φίλτρο ώστε στο πεδίο packet summary να εμφανίζονται μόνο πακέτα που προορίζονται για τον host σας.
* Ξεκινήστε την σύλληψη πακέτων
* Επισκεφτείτε την ιστοσελίδα [www.dit.uoi.gr](http://www.dit.uoi.gr)
* Σταματήστε την σύλληψη πακέτων

**Απαντήστε στις ακόλουθες ερωτήσεις:**

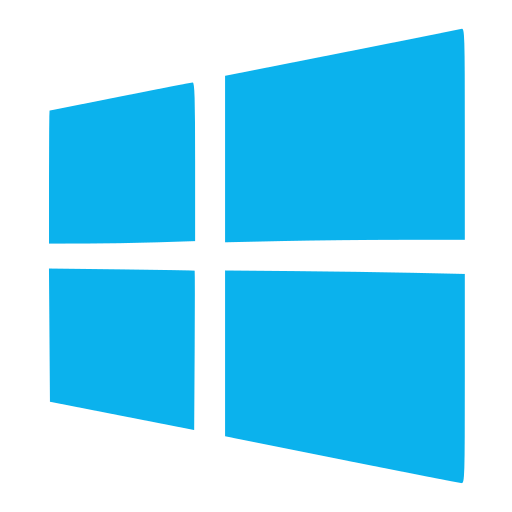
1. Εντοπίστε και καταγράψτε την IP της ιστοσελίδας καθώς και πληροφορίες για τον DNS server που χρησιμοποιεί ο host σας.
2. Εντοπίστε τα μηνύματα ερωτημάτων(query) και αποκρίσεων(response). Ποιο πρωτόκολλο μεταφοράς χρησιμοποιείται για την μεταφορά τους?
3. Επιλέξτε ένα μήνυμα απόκρισης και ένα μήνυμα ερωτήματος. Ποια είναι η θύρα προορισμού του μηνύματος ερωτήματος και ποια η θύρα προορισμού του ερωτήματος απόκρισης
4. Είναι η IP του DNS η ίδια για τα μηνύματα ερωτημάτων(query) και αποκρίσεων(response). Εξηγείστε.
5. H ιστοσελίδα που επισκεφτήκατε περιέχει εικόνες. Χρειάζεται ο host σας να στείλει νέα ερωτήματα DNS πριν από την ανάκτηση κάθε εικόνας(Εξηγείστε)?
6. *Μπορείτε να εντοπίσετε τυχόν πακέτα DNS που χρησιμοποιούν κρυπτογράφηση; Αν ναι, ποιο πρωτόκολλο κρυπτογράφησης χρησιμοποιείται;(Παρουσιάστε με τα κατάλληλα στιγμιότυπα οθόνης τον τρόπο με τον οποίο εντοπίσατε αυτά τα πακέτα και παρέχεται και μία εξήγηση μιας παραγράφου για το ερώτημα 6)*
7. *Εμφανίστε αντίστοιχα στατιστικά με βάση το trace των πακέτων που έχετε πραγματοποιήσει. Περιγράψτε τον τρόπο με τον πραγματοποιήσατε εύρεση στατιστικών μέσω του Wireshark.*

**!! Για κάθε ερώτημα να καταγραφεί όπου χρειάζεται οι εντολές η τα αντίστοιχα Φίλτρα που χρησιμοποιήσατε.**

## ΜΕΡΟΣ ΙΙΙ Σύλληψη μαζικής µμεταφοράς TCP από τον υπολογιστή σας σε έναν απομακρυσμένο server

Για το τρίτο μέρος της εργασίας θα εξεταστεί του TCP κατά την διενέργεια σύνδεσης ανάμεσα στον υπολογιστή σας και ένα server. Για αυτό τον σκοπό θα χρησιμοποιήσετε το Wireshark για να αποκτήσετε το trace της μεταφοράς ενός αρχείου από τον υπολογιστή σας σε έναν απομακρυσμένο server.

**Βασικά βήματα εργασίας:**

* Εξάγεται πληροφορίες για τον υπολογιστή σας(System and Hardware Information)
  + Για Windows 
    - Πατήστε Windows+R και στο πεδίο που θα εμφανιστεί πληκτρολογίστε **msinfo32**

Εικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, γραμματοσειρά, αριθμός

Περιγραφή που δημιουργήθηκε αυτόματα

* + - Έπειτα επιλέξτε **File>Export**
    - Το αρχείο θα έχει όνομα της μορφής <Όνομα>\_<Επώνυμο>\_<ΑΜ>.txt
  + Για Linux Linux - Free logo icons
    - Ανοίξτε ένα τερματικό και πληκτρολογήστε **sudo apt install lshw-gtk**
    - Έπειτα πληκτρολογήστε **sudo lshw>**<Όνομα>\_<Επώνυμο>\_<ΑΜ>.txt
  + Το αρχείο που θα δημιουργηθεί περιέχει πληροφορίες σχετικά με το Hardware υπολογιστή σας.
* Έπειτα επισκεφτείτε την ακόλουθη σελίδα <https://hcilab.dit.uoi.gr/protocols_and_telecommunications.php> και ανεβάστε το αρχείο ακολουθώντας τα παρακάτω βήματα

!!!! Θα περιγράψω τα βήματα με το που έχω έτοιμη την σελίδα

* Στην συνέχεια ανοίξτε το Wireshark πραγματοποιώντας τις κατάλληλες ρυθμίσεις
* Ξεκινήστε την σύλληψη των πακέτων
* Στην ιστοσελίδα που έχετε φορτώσει το αρχείο σταματήστε πιέστε το κουμπί upload
* Στην συνέχεια σταματήστε την σύλληψη των πακέτων. Το παράθυρο του Wireshark θα πρέπει να είναι παρόµοιο µε το παράθυρο που φαίνεται παρακάτω

!!! Εδώ εικόνα

**Απαντήστε στις ακόλουθες ερωτήσεις:**

* Ποιος ο αριθµός ακολουθίας του TCP segment SYN που χρησιµοποιείται για την εκκίνηση της σύνδεσης TCP µεταξύ του client και του **hcilab.dit.uoi.gr**
* Ποιος ο αριθµός ακολουθίας του segment SYNACK που στέλνεται από το gaia.cs.umass.edu στον client ως απόκριση στο segment SYN; Ποια η τιµή του πεδίου ACK στο segment SYNACK; Με ποιο τρόπο καθορίστηκε η τιµή αυτή από το **hcilab.dit.uoi.gr**; Ποιο στοιχείο του segment προσδιορίζει ότι πρόκειται για ένα SYNACK segment;
* Υπάρχουν επαναµεταδιδόµενα segments στο αρχείο του trace; Σε τι είδους έλεγχο του trace βασίσατε την απάντησή σας στην ερώτηση αυτή;
* Ποιος ο ελάχιστος διαθέσιµος χώρος αποθήκευσης (buffer space) που ανακοινώνεται από τον παραλήπτη σε ολόκληρο το trace; Συµβαίνει ποτέ η στον παραλήπτη να περιορίζει το ρυθµό του αποστολέα;
* *Ποιο το throughput (αριθµός µεταφερόµενων bytes ανά µονάδα χρόνου) της σύνδεσης TCP; Εξηγείστε τον τρόπο µε τον οποίο υπολογίσατε την τιµή αυτή.*
* Ποιο το µήκος καθενός από τα TCP segments από και προς το **hcilab.dit.uoi.gr**
* Εμφανίστε στατιστικά σχετικά με τα TCP segments καθώς και Time Sequence Graphs για αυτά