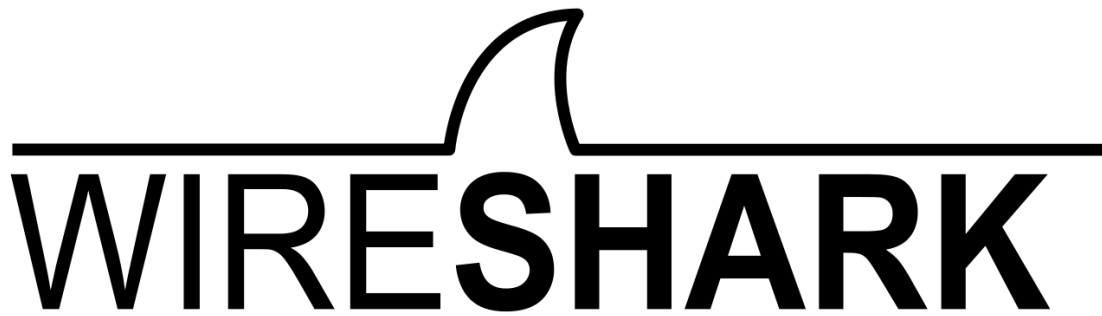


**Τελική Εργασία Εξαμήνου-Ανάλυση πακέτων μέσω
Wireshark**



ΗΜΕΡΟΜΗΝΙΑ ΤΕΛΙΚΗΣ ΥΠΟΒΟΛΗΣ: 20/05/2025

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.

!!ΣΗΜΕΙΩΣΗ Κάθε ρύθμιση στο Wireshark θα πρέπει να ακολουθείται από το αντίστοιχο στιγμιότυπο οθόνης. Επίσης κάθε ερώτηση που θα απαντήσετε και εμπεριέχει την χρήση κάποιας εντολής θα πρέπει στην απάντηση να ενσωματώνεται η εντολή.

Τα στιγμιότυπα οθόνης, τις εντολές, τα αποτελέσματα και ότι άλλο σας ζητείται ως απάντηση τα ενσωματώνετε σε αρχείο Word. Το όνομα του αρχείου θα είναι: “επίθετο_αρ.μητρώου”, όπου επίθετο το επίθετό σας και αρ.μητρώου, ο αριθμός μητρώου σας.

Η εργασία θα πρέπει να έχει αποσταλεί μέσω mail με τίτλο “Εργασία πρωτόκολλα_ επίθετο_αρ.μητρώου”, στην διεύθυνση “ddimop@uoi.gr” το αργότερο μέχρι την Τρίτη 20 Μαΐου. Δεν θα γίνονται δεκτές εκπρόθεσμες εργασίες.

ΜΕΡΟΣ Ι ΑΝΑΛΥΣΗ ΔΙΕΠΑΦΗΣ ΔΙΚΤΥΟΥ (Μονάδες 2)

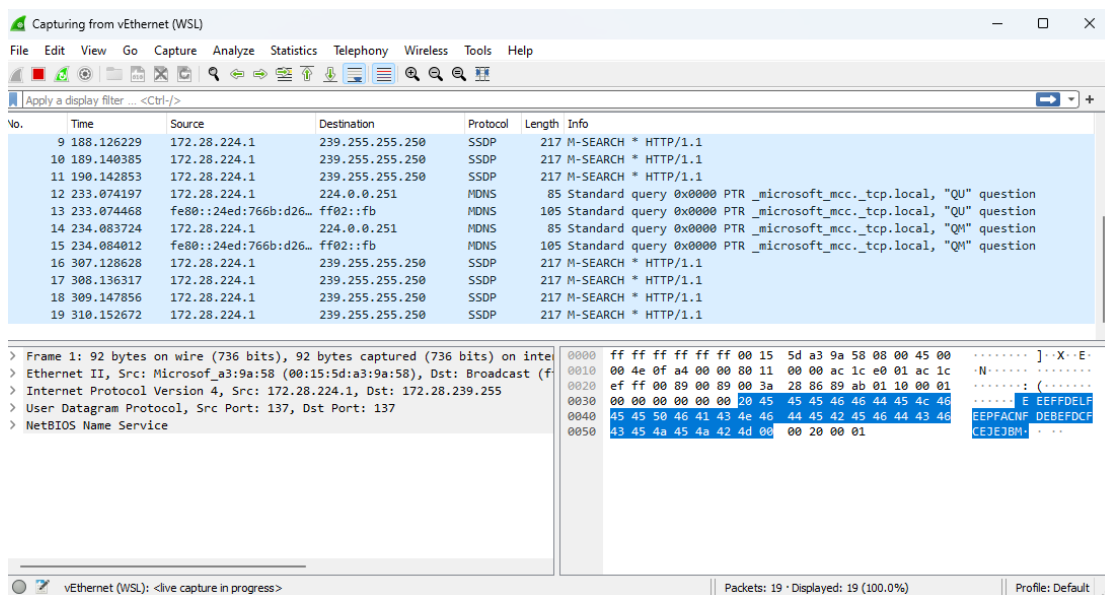
Χρησιμοποιώντας ένα τερματικό καταγράψτε:

Την ονομασία της κάρτας δικτύωσης (network adapter)

- 1) Την ταχύτητα σύνδεσης
- 2) Την διεύθυνση MAC σε δεκαεξαδική μορφή
- 3) Τον κατασκευαστή της κάρτας δικτύωσης
- 4) Τα συνδεδεμένα με αυτή πρωτόκολλα δικτύωσης
- 5) Τα πρωτόκολλα δικτύωσης που συνδέονται με στο Interface
- 6) Η ποσότητα των δεδομένων που μεταδίδονται και λαμβάνονται από τον προσαρμογέα δικτύου
- 7) Τις IP διευθύνσεις που ο υπολογιστής σας έχει επικοινωνήσει πρόσφατα

ΜΕΡΟΣ ΙΙ Σύλληψη και ανάλυση πακέτων με χρήση του Wireshark (Μονάδες 3.5)

Στο δεύτερο μέρος της εργασίας θα πραγματοποιήσετε σύλληψη πακέτων μέσω του Wireshark, έχοντας πραγματοποιήσει επίσκεψη σε μία ιστοσελίδα κατά την διάρκεια λειτουργίας του sniffer. Αρχικά θα πρέπει να έχετε παραμετροποιήσει κατάλληλα το Wireshark ώστε να έχετε μία δομή αντίστοιχη της παρακάτω εικόνας



Θα πρέπει να ρυθμίσετε το Wireshark επιλέγοντας:

- ✓ Κατάλληλο Interface
- ✓ Κατάλληλα Columns
- ✓ Κατάλληλα capture options και filter options

Έπειτα θα χρησιμοποιήσετε το Wireshark για σύλληψη πακέτων DNS που δημιουργούνται κατά την πλοήγηση στο world wide web. Συγκεκριμένα θα πρέπει να υλοποιήσετε και αιτιολογήσετε(με χρήση screenshots) τα ακόλουθα ερωτήματα :

Εντοπίστε και καταγράψτε την IP της ιστοσελίδας καθώς και πληροφορίες για τον DNS server που χρησιμοποιεί ο host σας.


- 1) Εντοπίστε τα μηνύματα ερωτημάτων(query) και αποκρίσεων(response). Ποιο πρωτόκολλο μεταφοράς χρησιμοποιείται για την μεταφορά τους?
- 2) Επιλέξτε ένα μήνυμα απόκρισης και ένα μήνυμα ερωτήματος. Ποια είναι η θύρα προορισμού του μηνύματος ερωτήματος και ποια η θύρα προορισμού του ερωτήματος απόκρισης
- 3) Είναι η IP του DNS η ίδια για τα μηνύματα ερωτημάτων(query) και αποκρίσεων(response). Εξηγήστε.

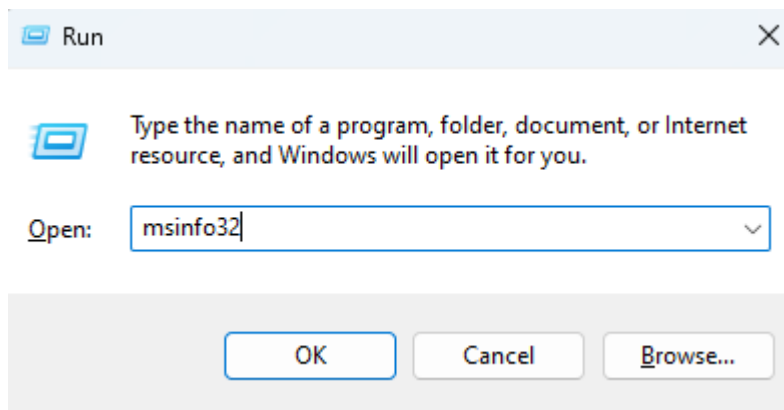
- 4) Η ιστοσελίδα που επισκεφτήκατε περιέχει εικόνες. Χρειάζεται ο host σας να στείλει νέα ερωτήματα DNS πριν από την ανάκτηση κάθε εικόνας (Εξηγείστε)?
- 5) Μπορείτε να εντοπίσετε τυχόν πακέτα DNS που χρησιμοποιούν κρυπτογράφηση; Αν ναι, ποιο πρωτόκολλο κρυπτογράφησης χρησιμοποιείται; (Παρουσιάστε με τα κατάλληλα στιγμιότυπα οθόνης τον τρόπο με τον οποίο εντοπίσατε αυτά τα πακέτα και παρέχεται και μία εξήγηση μιας παραγράφου για το ερώτημα 5)
- 6) Εμφανίστε αντίστοιχα στατιστικά με βάση το trace των πακέτων που έχετε πραγματοποιήσει. Περιγράψτε τον τρόπο με τον οποίο πραγματοποιήσατε εύρεση στατιστικών μέσω του Wireshark.


ΜΕΡΟΣ III Σύλληψη μαζικής μεταφοράς TCP από τον υπολογιστή σας σε έναν απομακρυσμένο server (Μονάδες 4.5)

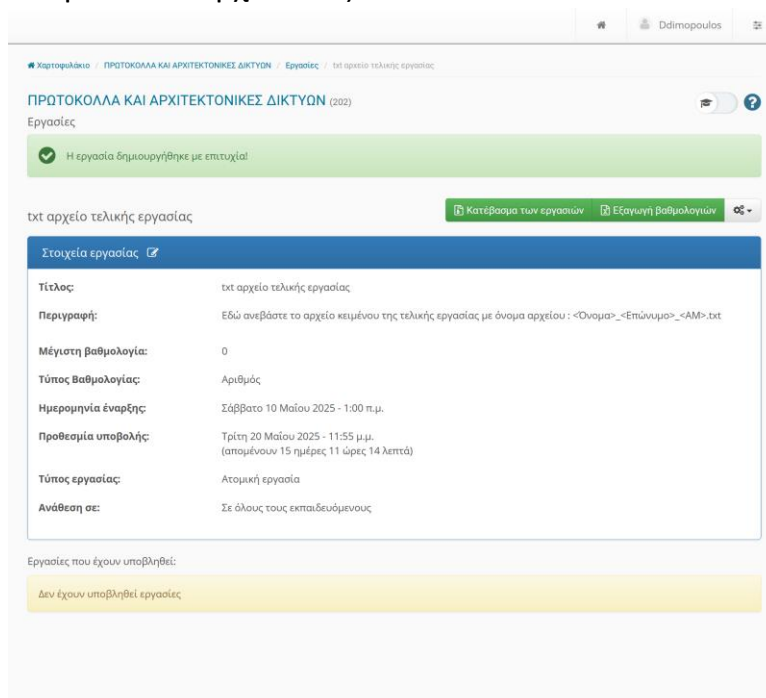
Στο τρίτο μέρος της εργασίας θα εξεταστεί η μεταφορά TCP segments κατά την διενέργεια σύνδεσης ανάμεσα στον υπολογιστή σας και ένα server. Για αυτό τον σκοπό θα χρησιμοποιήσετε το Wireshark για να αποκτήσετε το trace της μεταφοράς ενός αρχείου, το οποίο θα περιέχει στοιχεία του υλικό του υπολογιστή σας,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

Πρώτο βήμα εργασίας:

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



- Έπειτα επιλέξτε File>Export
- Το αρχείο θα έχει όνομα της μορφής <Όνομα>_<Επώνυμο>_<ΑΜ>.txt
- Για Linux 
 - 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.
- Αναβάστε το αρχείο σας στο eclass



Δεύτερο βήμα εργασίας:

- ✓ Μετανομάστε το αρχείο που δημιουργήσατε στο προηγούμενο βήμα σε `alice.txt` κρατώντας τα ίδια περιεχόμενα
- ✓ Επισκεφτείτε την ιστοσελίδα <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html> (Αντίστοιχη εργαστηρίου 4)
- ✓ Ξεκινήστε το Wireshark
- ✓ Ανεβάστε το αρχείο που μετανομάσατε σε `alice.txt`
- ✓ Κάντε Upload του αρχείου
- ✓ Σταματήστε το Wireshark

Απαντήστε στις ακόλουθες ερωτήσεις:

- 1) Θα εφαρμόσετε κάποιο είδος φιλτραρίσματος στα πακέτα που έχουν γίνει capture. Αν ναι περιγράψτε τι διαδικασία που ακολουθείται για να καταλήξετε στο φίλτρο καθώς και φίλτρο που θα χρησιμοποιήσετε
- 2) Ποια η IP διεύθυνση του server. Εξηγήστε με ποια εντολή βρήκατε την IP;
- 3) Ποιος ο αριθμός ακολουθίας του TCP segment SYN που χρησιμοποιείται για την εκκίνηση της σύνδεσης TCP μεταξύ του client και του **gaia.cs.umass.edu**
- 4) 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 **gaia.cs.umass.edu**; Ποιο στοιχείο του segment προσδιορίζει ότι πρόκειται για ένα SYNACK segment;
- 5) Υπάρχουν επαναμεταδιδόμενα segments στο αρχείο του trace; Σε τι είδους έλεγχο του trace βασίσατε την απάντησή σας στην ερώτηση αυτή;
- 6) 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;

- 7) Ποιο το throughput (αριθμός μεταφερόμενων bytes ανά μονάδα χρόνου) της σύνδεσης TCP; Εξηγείστε τον τρόπο με τον οποίο υπολογίσατε την τιμή αυτή.
- 8) Ποιο το μήκος καθενός από τα TCP segments από και προς το **gaia.cs.umass.edu**
- 9) Εμφανίστε στατιστικά σχετικά με τα TCP segments καθώς και Time Sequence Graphs για αυτά
- 10) Ποια είναι τα διάφορα πεδία σε ένα τμήμα TCP και ποιος ο σκοπός κάθε πεδίου;

Καλή Επιτυχία!!