Διαχείριση Δικτύων
Τμήμα Μηχανικών ΤΕ
ΤΕΙ Ηπείρου

Άσκηση εξοικείωσης με την εφαρμογή Wireshark

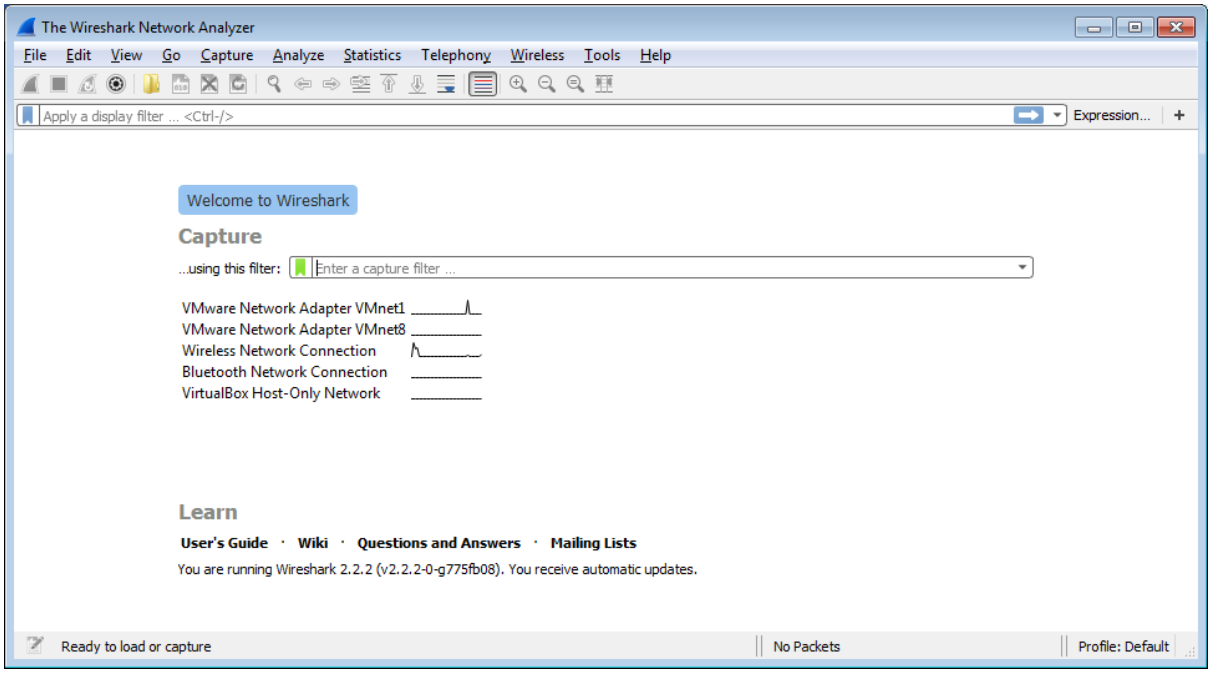
Η εφαρμογή Wireshark μας δίνει την δυνατότητα να συλλέξουμε όλη την δικτυακή κίνηση που μπορεί να γίνει αντιληπτή από τις επαφές δικτύου μας. Επίσης μας δίνει την δυνατότητα να επιθεωρήσουμε τα περιεχόμενα των πακέτων που στέλνονται ή λαμβάνονται από τον υπολογιστή μας. Εμείς θα την χρησιμοποιήσουμε σαν ένα μέσο για να γίνουν πιο κατανοητές ορισμένες έννοιες του μαθήματος όπως η ενθυλάκωση πακέτων και η λειτουργία των πρωτοκόλλων που εξετάζουμε.

[Μπορείτε να εγκαταστήσετε την εφαρμογή και στον προσωπικό σας υπολογιστή κατεβάζοντας την έκδοση που ταιριάζει από την σελίδα: https://www.wireshark.org/#download]

Διαδικασία Εξοικείωσης

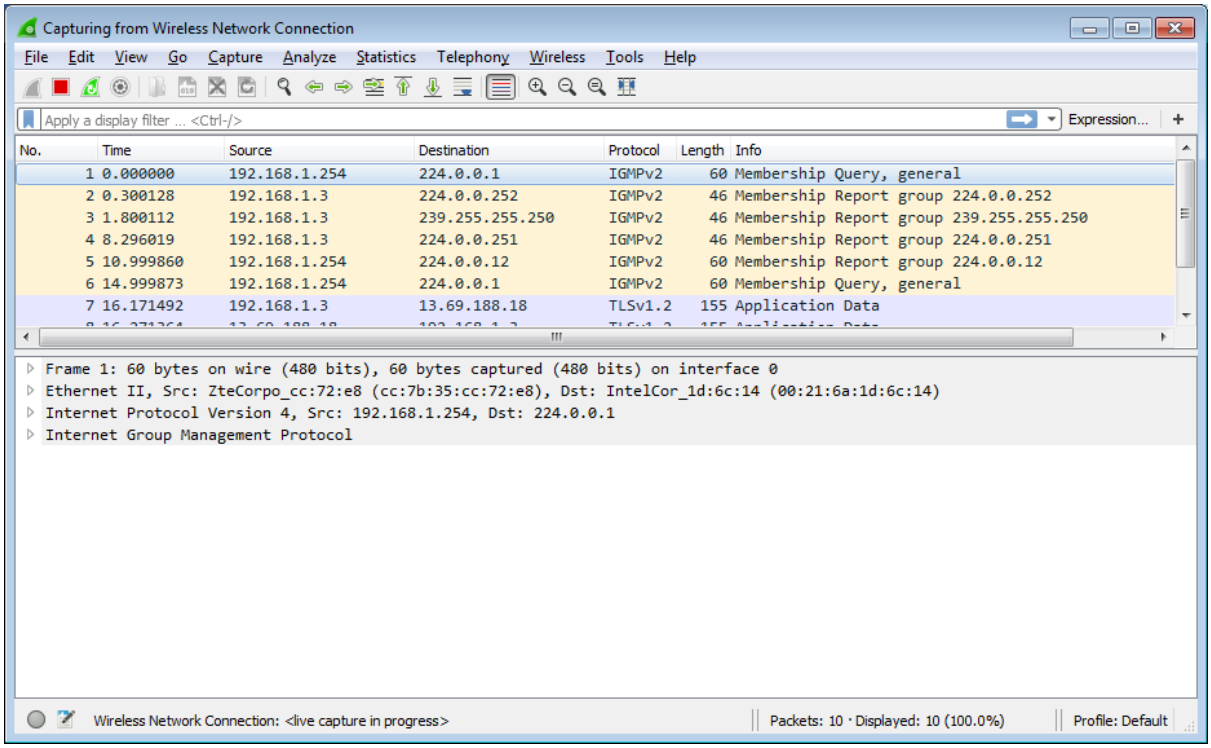
Εμφανίστε την γραμμή εντολών για να την έχετε διαθέσιμη ώστε να δώσετε κάποια επιπλέον εντολή.

Στην συνέχεια ξεκινήστε την εφαρμογή Wireshark. Θα εμφανιστεί μια εικόνα όπως η παρακάτω



Στο κέντρο της σελίδας εμφανίζονται οι προσαρμογείς δικτύου για τους οποίους μπορούμε να συλλέξουμε κίνηση. Συνήθως θα μας ενδιαφέρει είτε μια σύνδεση Ethernet είτε μια ασύρματη

(wireless) σύνδεση. Επιλέξτε την Ethernet κάνοντας διπλό κλικ. Με τον τρόπο αυτό θα ξεκινήσει η συλλογή πακέτων και την σύνδεση που επιλέξατε και θα εμφανιστεί το ακόλουθο παράθυρο.

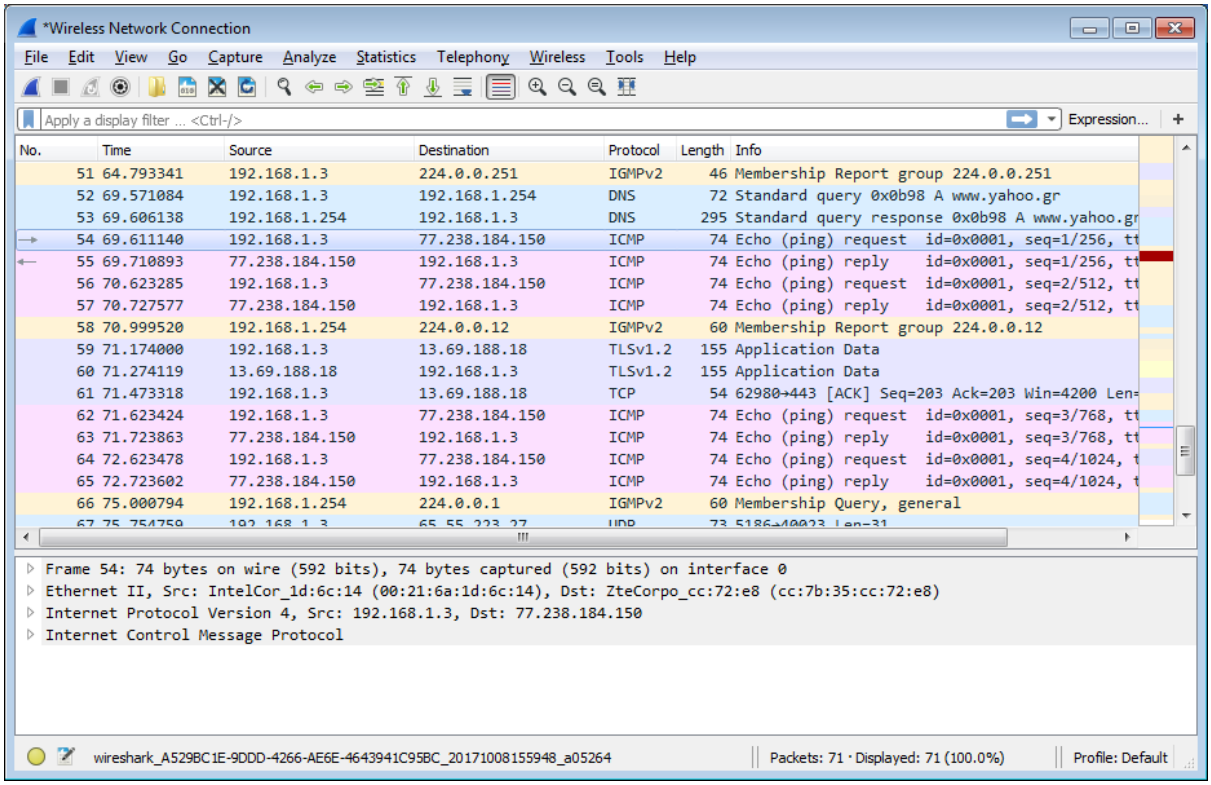


Θα παρατηρήσετε ότι στο πάνω μέρος του εσωτερικού παραθύρου εμφανίζεται ένας πίνακας με γραμμές. Κάθε μια αντιπροσωπεύει ένα πλαίσιο που έγινε αντιληπτό από την εφαρμογή.

Ενώ τρέχει η εφαρμογή δώστε στην γραμμή εντολών μια εντολή ping για παράδειγμα:

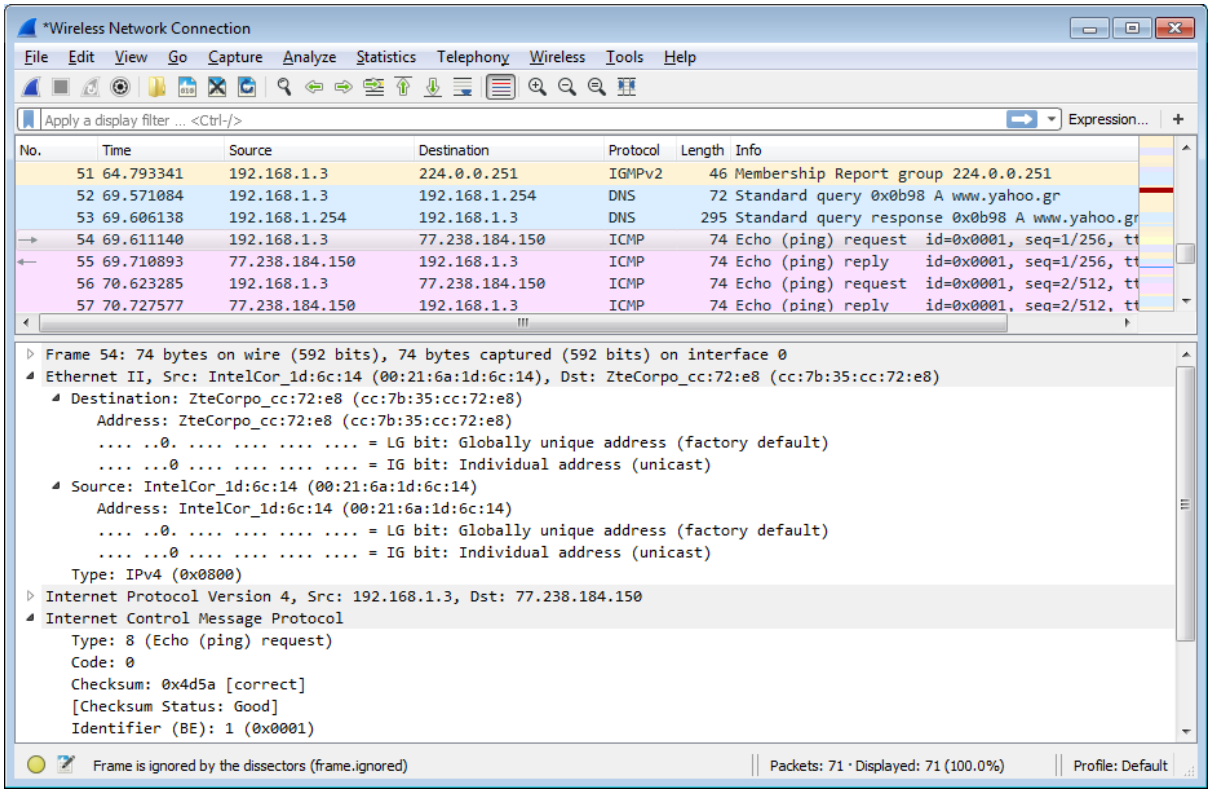
ping www.yahoo.com

Θα παρατηρήσετε ότι στο παράθυρο της εφαρμογής εμφανίζονται κάποια νέα πακέτα που αντιπροσωπεύουν τα μηνύματα ICMP Echo Request και Echo Reply που στέλνει και λαμβάνει η εντολή ping, όπως φαίνονται στην ακόλουθη εικόνα.



Στο σημείο αυτό μπορούμε να διακόψουμε την συλλογή πακέτων πατώντας το κόκκινο κουμπί που βρίσκεται πάνω αριστερά κάτω από το μενού εντολών.

Στο κάτω τμήμα του παραθύρου βρίσκεται η περιοχή που εμφανίζει λεπτομέρειες για κάθε πλαίσιο που επιλέγεται στην πάνω λίστα. Υπάρχουν διαφορετικές περιοχές στις οποίες μπορείτε να εξετάζεται πληροφορίες που τοποθετούνται από τα πρωτόκολλα διαφορετικών επιπέδων. Μπορείτε να βλέπετε αυτές τις πληροφορίες ανοίγοντας τις αντίστοιχες καρτέλες.



Τέλος μπορείτε να εμφανίσετε την σειρά byte του επιλεγμένου πακέτου επιλέγοντας **View->Packet Bytes**

Τερματίστε την εφαρμογή επιλέγοντας **Stop and Quit Without Saving.**