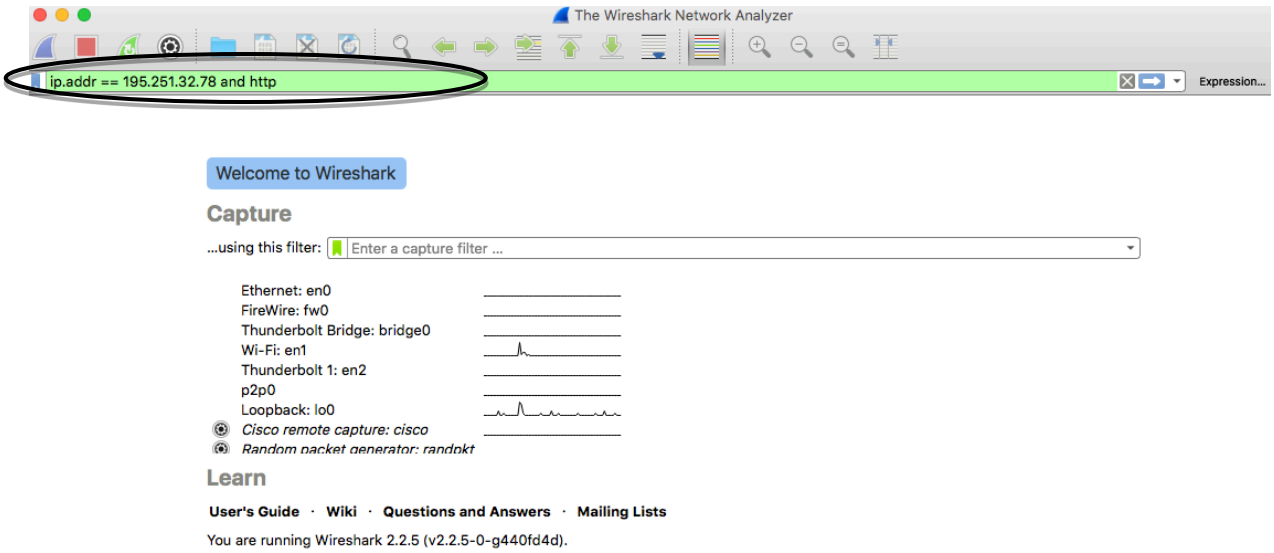
Εργαστηριακή Άσκηση

Ερώτηση 1

Για την εκτέλεση της Ερώτησης 1, θα πρέπει να χρησιμοποιήσετε το εργαλείο *Wireshark,* το οποίο είναι δωρεάν διαθέσιμο στο http://www.wireshark.org/download.html για λειτουργικά συστήματα Windows/Linux/Mac. Το Wireshark είναι ένα εργαλείο το οποίο «συλλαμβάνει» και εμφανίζει την κίνηση του δικτύου στον υπολογιστή σας. Αφού ξεκινήσετε το λογισμικό Wireshark θα εμφανιστεί ένα παράθυρο παρόμοιο με αυτό της παρακάτω εικόνας. Για τη χρήση του, θα πρέπει να κάνετε διπλό κλικ στην κατάλληλη διεπαφή που χρησιμοποιείτε για την πρόσβασή σας στο Διαδίκτυο (μέσα από τη διαθέσιμη λίστα του εργαλείου), όπως εμφανίζεται στην παρακάτω εικόνα (π.χ. την ενσύρματη σύνδεση Ethernet ή τη σύνδεση μέσω Wi-Fi).



Χρησιμοποιήστε το πεδίο του φίλτρου «απεικόνισης» (display filter) για να παρουσιάζονται μόνο τα πακέτα που σας ενδιαφέρουν[1].

Σε αυτήν την ερώτηση, θα καταγραφούν τα μηνύματα HTTP που παράγονται κατά την επίσκεψη μιας ιστοσελίδας με χρήση ενός πλοηγού ή φυλλομετρητή Ιστού[2]. Προτού αρχίσετε την καταγραφή φροντίστε να αδειάσετε την προσωρινή μνήμη (cache) του πλοηγού από την επιλογή *Ιστορικό > Εκκαθάριση πρόσφατου ιστορικού*.

Επειδή τα μηνύματα HTTP μεταφέρονται σε περισσότερα από ένα πακέτα, αφού ξεκινήσετε το Wireshark, μεταβείτε στο μενού *Edit>Preferences,* κάντε κλικ στο σύμβολο δίπλα στο *Protocols* στην αριστερή πλευρά του παραθύρου, κατόπιν εντοπίστε και κάντε κλικ στο πρωτόκολλο HTTP και βεβαιωθείτε ότι όλες οι επιλογές περί ανασύνθεσης και αποσυμπίεσης είναι επιλεγμένες. Στη συνέχεια, στο πρωτόκολλο TCP βεβαιωθείτε ότι το *Allow subdissector to reassemble TCP streams* είναι επιλεγμένο και φροντίστε το *Validate the TCP*

[1] Το φίλτρο που εφαρμόζεται στην εικόνα είναι απλώς ένα παράδειγμα.
[2] Προτείνεται η χρήση του Firefox, αφού πρώτα έχετε καθαρίσει την προσωρινή του μνήμη (cache).

checksum if possible[3] να **μην** είναι επιλεγμένο. Τέλος, πιέστε OK για να κλείσει το παράθυρο και εφαρμοστούν οι αλλαγές σας. Με τις επιλογές αυτές, μηνύματα που μεταφέρονται σε περισσότερα από ένα πακέτα θα αποκωδικοποιηθούν από το Wireshark ως πλήρη μηνύματα HTTP και όχι αποσπασματικά.

Όπως ήδη γνωρίζετε, μια σελίδα HTML είναι μια συλλογή αντικειμένων (π.χ. ενός αρχείου HTML, διαφόρων εικόνων JPEG, αρχείων ήχου, JavaScripts, Java applets κ.λπ.) και μπορεί να περιέχει παραπομπές προς άλλες ιστοσελίδες. Στην ερώτηση αυτή, θα μελετήσετε την κίνηση που παρατηρείται στην περίπτωση όπου ο πλοηγός ιστού κατεβάζει μια σελίδα που περιέχει ενσωματωμένα αντικείμενα (embedded objects).

Ξεκινήστε μια καταγραφή (επιλογή: *Capture>Start* ή *Ctrl+E*), επισκεφτείτε την ιστοσελίδα http://edu-dy.cn.ntua.gr/links.html [4] και σταματήστε την καταγραφή (επιλογή: *Capture>Stop* ή *Ctrl+E*) όταν φορτωθεί πλήρως η σελίδα. Η συγκεκριμένη σελίδα περιλαμβάνει διευθύνσεις URL που αναφέρονται σε δύο εικόνες που βρίσκονται σε διαφορετικούς από τον edu-dy.cn.ntua.gr εξυπηρετητές ιστού. Μόλις η σελίδα φορτωθεί πλήρως, σταματήστε την καταγραφή.

Εφαρμόστε κατάλληλο φίλτρο ώστε να παραμείνουν μόνο τα μηνύματα του πρωτοκόλλου HTTP.

1.1 Εφαρμόστε κατάλληλο φίλτρο απεικόνισης (Apply a display filter) ώστε να παραμείνουν μόνο τα **πρώτα** τεμάχια TCP των τριμερών χειραψιών που διεξήχθησαν. Πόσες συνδέσεις TCP έγιναν;

1.2 Με ποιους υπολογιστές έγιναν οι συνδέσεις TCP;

1.3 Εφαρμόστε κατάλληλο φίλτρο ώστε να παραμείνουν μόνο οι εντολές HTTP προς εξυπηρετητές ιστού. Πόσες εντολές HTTP τύπου GET έχει καταγράψει το Wireshark;

1.4 Ποια είναι η διεύθυνση IP προορισμού κάθε εντολής HTTP τύπου GET; Εξηγήστε.

1.5 Καταγράψτε τα ονόματα των αρχείων εικόνων που κατέβασε ο πλοηγός από κάθε εξυπηρετητή.

Ερώτηση 2

Υπάρχουν περιπτώσεις όπου το ζητούμενο αρχείο HTML είναι αρκετά μεγάλο και δεν χωράει σε ένα τεμάχιο TCP. Στην περίπτωση αυτή, το μήνυμα HTTP τεμαχίζεται στο στρώμα μεταφοράς. Ξεκινήστε μια νέα καταγραφή με το Wireshark. Με τον πλοηγό ιστού επισκεφθείτε τη σελίδα http://edu-dy.cn.ntua.gr/long.html [5] και σταματήστε την καταγραφή μόλις ολοκληρωθεί το φόρτωμα της σελίδας.

[3] Η επιβεβαίωση του TCP checksum (επειδή γίνεται στην κάρτα δικτύου) παρενοχλεί τη διαδικασία επανασύνθεσης.
[4] Παρατηρείστε ότι χρησιμοποιείται http:// αντί για https://
[5] Παρατηρείστε ότι χρησιμοποιείται http:// αντί για https://

2.1 Πόσες συνδέσεις TCP έγιναν;

2.2 Ποιο είναι το μέγεθος της MSS (Maximum Segment Size) που ανακοινώνει η κάθε πλευρά;

Εφαρμόστε κατάλληλο φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο μηνύματα του πρωτοκόλλου HTTP.

2.3 Πόσες αιτήσεις HTTP τύπου GET στάλθηκαν από τον πλοηγό ιστού;

2.4 Να καταγραφεί η γραμμή κατάστασης (status line) της απόκρισης που επιστρέφει ο εξυπηρετητής.

2.5 Εντοπίστε την HTTP απόκριση που αφορά το αρχείο long.html. Πόσο είναι το συνολικό μέγεθος HTTP περιεχομένου (επικεφαλίδα και δεδομένα μαζί) και πόσο είναι το μήκος του αρχείου long.html;

Εφαρμόστε νέο φίλτρο απεικόνισης στο Wireshark, ώστε να παραμείνει μόνο η κίνηση IP που *προέρχεται* από τον εξυπηρετητή ιστού.

2.6 Ποια είναι η σύνταξή του παραπάνω φίλτρου;

2.7 Πόσα τεμάχια TCP, που περιείχαν δεδομένα, χρειάστηκαν για τη μεταφορά της απόκρισης στο μήνυμα HTTP τύπου GET; *[Υπόδειξη: Μαζί με το τελευταίο τεμάχιο της σειράς, το Wireshark εμφανίζει στο παράθυρο καταγεγραμμένων πακέτων την ανασύνθεση της απόκρισης HTTP.]*

2.8 Ποιο τεμάχιο TCP του προηγούμενου ερωτήματος περιλαμβάνει τη γραμμή κατάστασης του πρωτοκόλλου HTTP; *[Υπόδειξη: Αναζητήστε[6] το περιεχόμενο της γραμμής κατάστασης στο παράθυρο με τα περιεχόμενα του επιλεγμένου πλαισίου.]*

2.9 Ποιο είναι το μέγεθος του περιεχομένου HTTP που μεταφέρει κάθε ένα από τα τεμάχια αυτά; *[Υπόδειξη: Αναπτύξτε το περιεχόμενο της επικεφαλίδας TCP στο παράθυρο με τις λεπτομέρειες επικεφαλίδας.]*

2.10 Γιατί το μέγεθος των πλαισίων Ethernet που μεταφέρουν τα προηγούμενα τεμάχια TCP (πλην του τελευταίου) είναι σταθερό;

2.11 Πώς προκύπτει το μέγεθος του τελευταίου εξ αυτών;

[6] Αφού κάνουμε κλικ στο πρώτο εμφανιζόμενο πακέτο, πληκτρολογούμε Ctrl+F. Επιλογές αναζήτησης: “Packet bytes” και “String”.