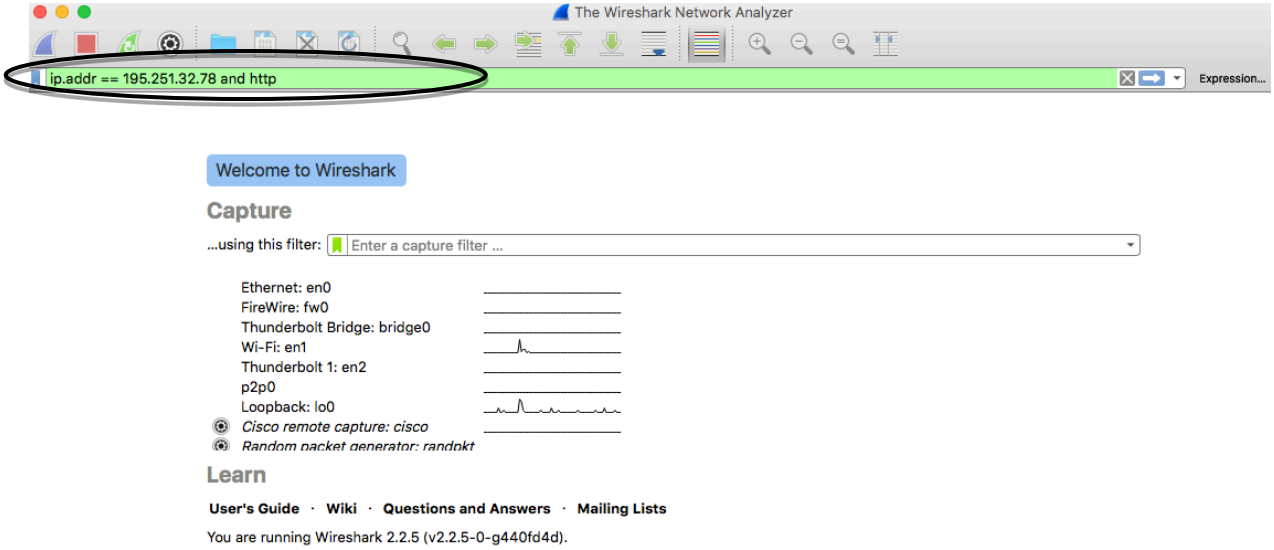
Εργαστηριακή Άσκηση

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;

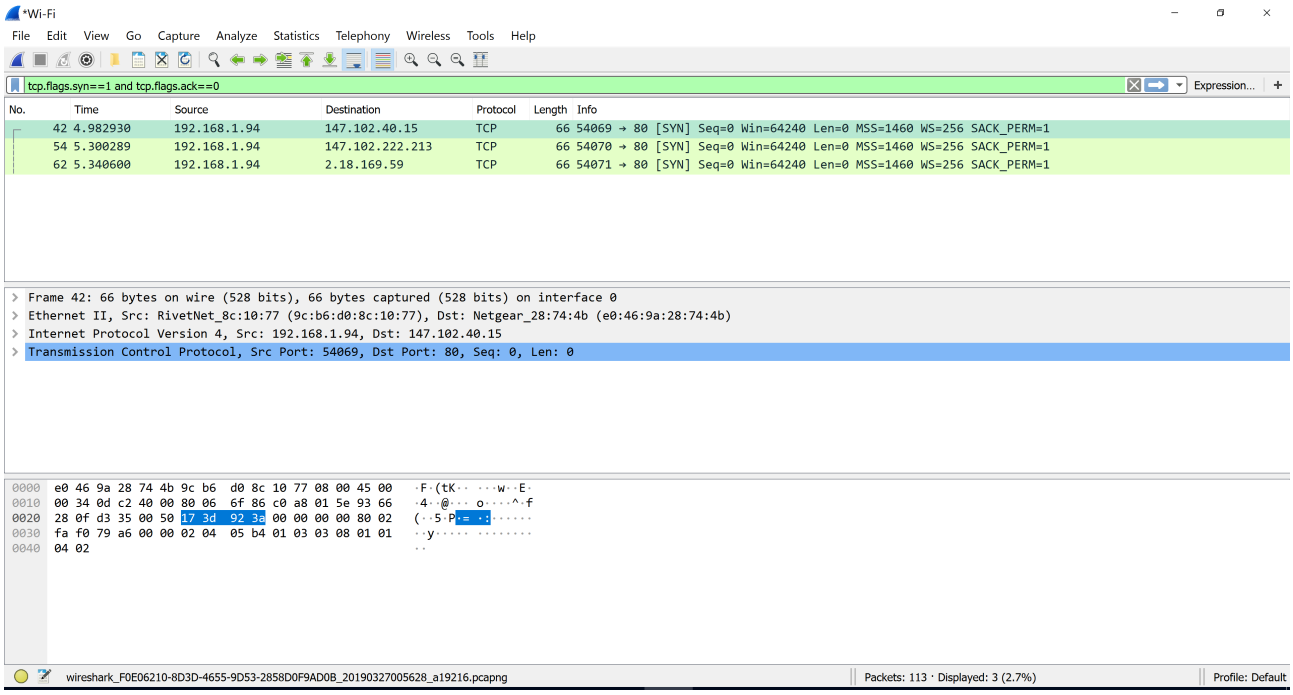
2.11 Πώς προκύπτει το μέγεθος του τελευταίου εξ αυτών;

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

Επίλυση εργαστηριακής άσκησης

1.1:

Χρησιμοποιούμε το φίλτρο:
tcp.flags.syn==1 and tcp.flags.ack==0
Υπάρχουν 3 TCP συνδέσεις στην εν λόγω καταγραφή.

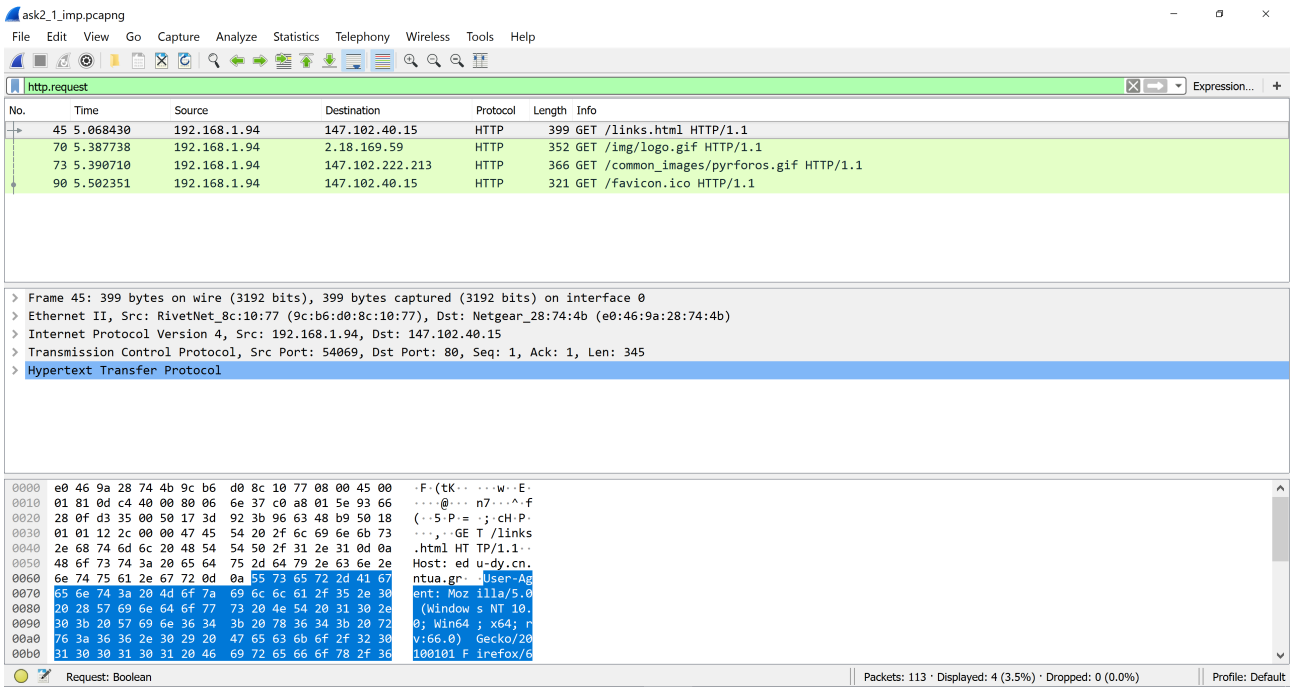


1.2:

Οι IP διευθύνσεις προορισμού είναι οι: 147.102.40.15, 147.102.222.213 και 2.18.169.59

1.3:

Εφαρμόζουμε το φίλτρο: http.request ώστε να παραμείνουν μόνο οι αιτήσεις HTTP από τον υπολογιστή μας προς τους υπολοίπους. Έχουν καταγραφεί 4 εντολές τύπου HTTP GET.



1.4:

Για τα 4 αυτά HTTP GET, οι IP διευθύνσεις προορισμού ήταν αντίστοιχα:

- 147.102.40.15 – Εξυπηρετητής edu-dy.cn.ntua.gr
- 2.18.169.59 – Εξυπηρετητής www.mit.edu
- 147.102.222.213 – Εξυπηρετητής old.ntua.gr
- 147.102.40.15 – Εξυπηρετητής edu-dy.cn.ntua.gr

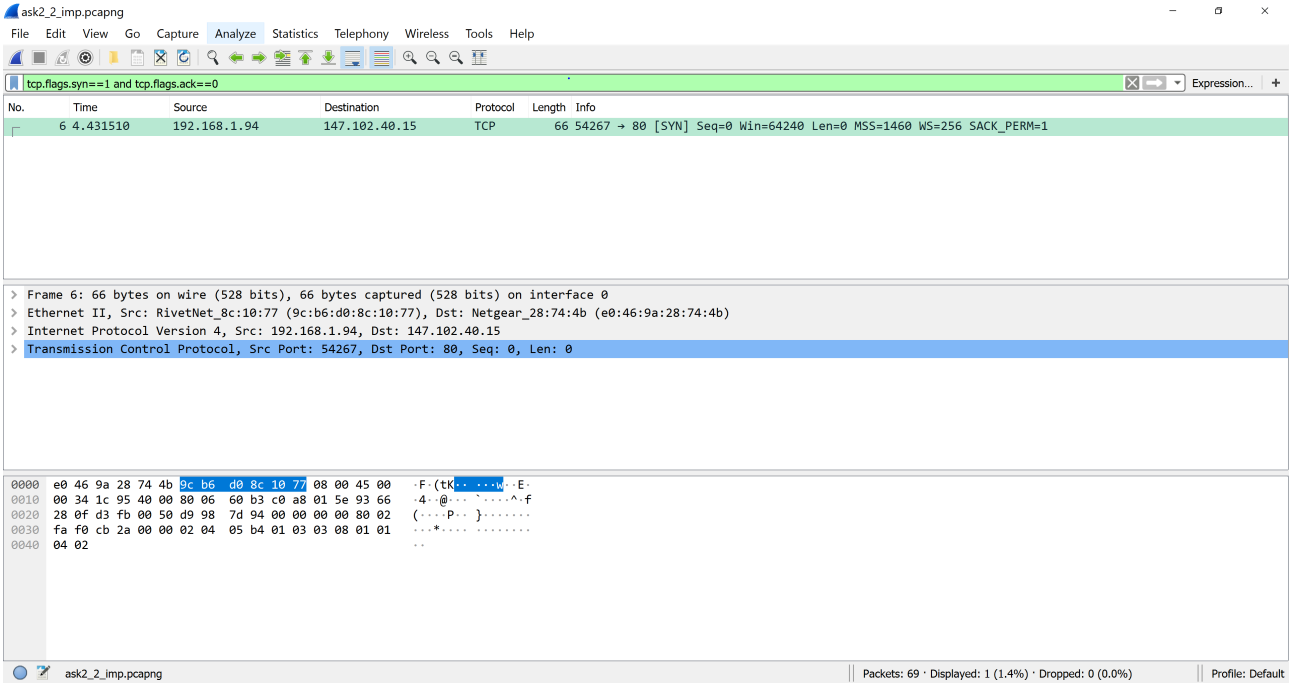
1.5:

Παρατηρούμε δύο HTTP GET προς τον υπολογιστή 147.102.40.15: ένα με σκοπό το κατέβασμα της σελίδας links.html και ένα με σκοπό το κατέβασμα του εικονιδίου favicon.ico. Επίσης, παρατηρούμε ένα HTTP GET προς τον υπολογιστή 147.102.222.213, με σκοπό το κατέβασμα της εικόνας pyrforos.gif, καθώς και ένα προς τον υπολογιστή 2.18.169.59 (του MIT), με σκοπό το κατέβασμα της εικόνας logo.gif.

Απάντηση στην Ερώτηση 2

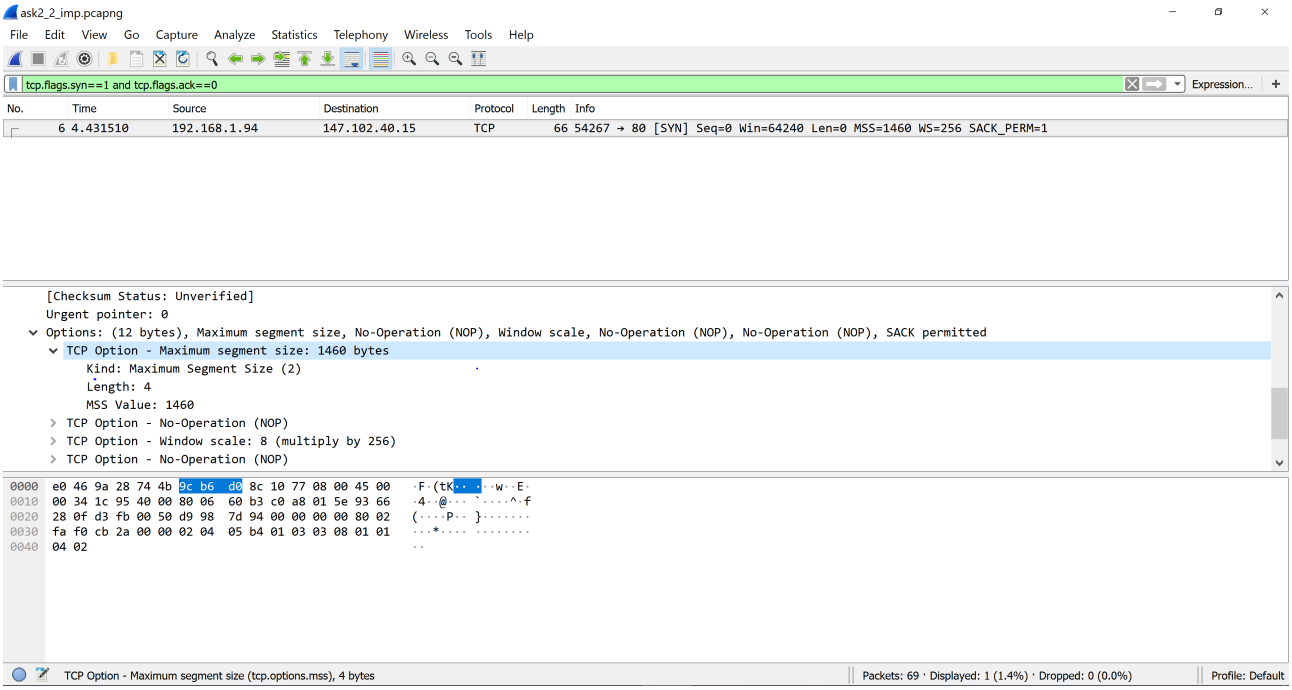
2.1:

Εφαρμόζουμε και πάλι το φίλτρο: tcp.flags.syn==1 and tcp.flags.ack==0 και διαπιστώνουμε ότι έχει εγκατασταθεί μία μόνο σύνδεση TCP.

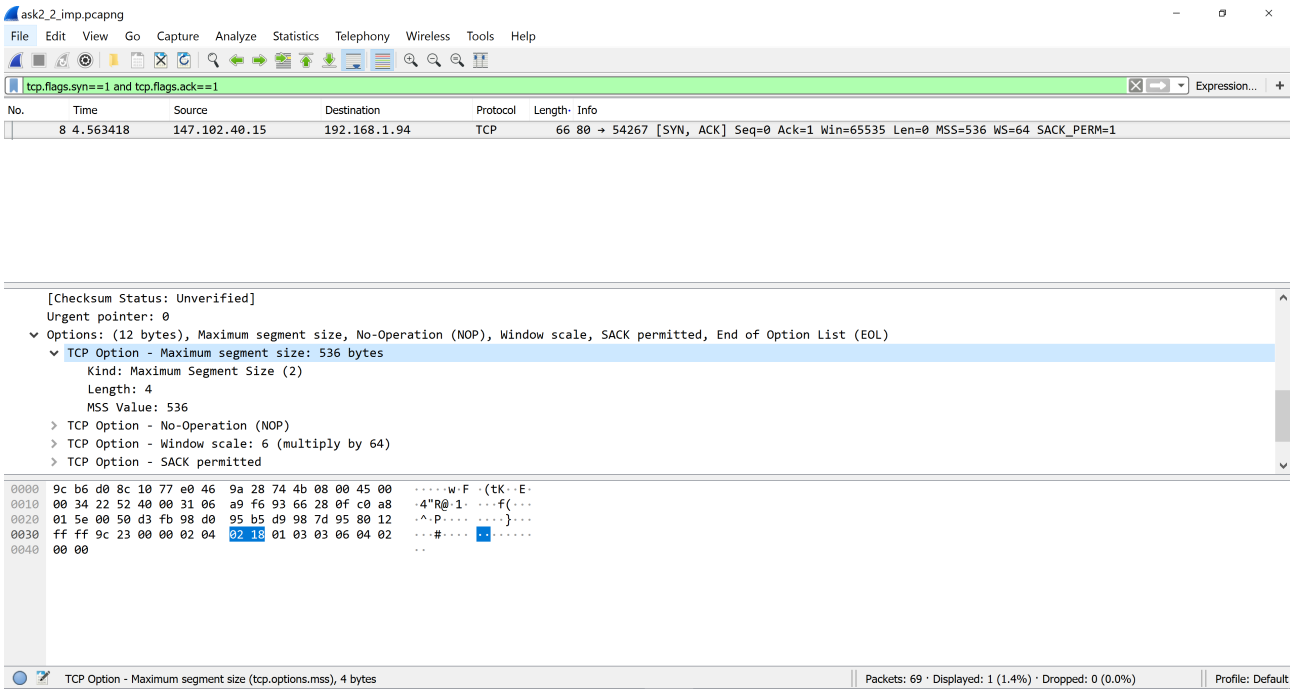


2.2:

Αναλύουμε την επικεφαλίδα TCP. Στο συγκεκριμένο παράδειγμα του screenshot, παρατηρούμε ότι η πλευρά του δικού μας υπολογιστή ανακοινώνει MSS ίσο με 1460 bytes.



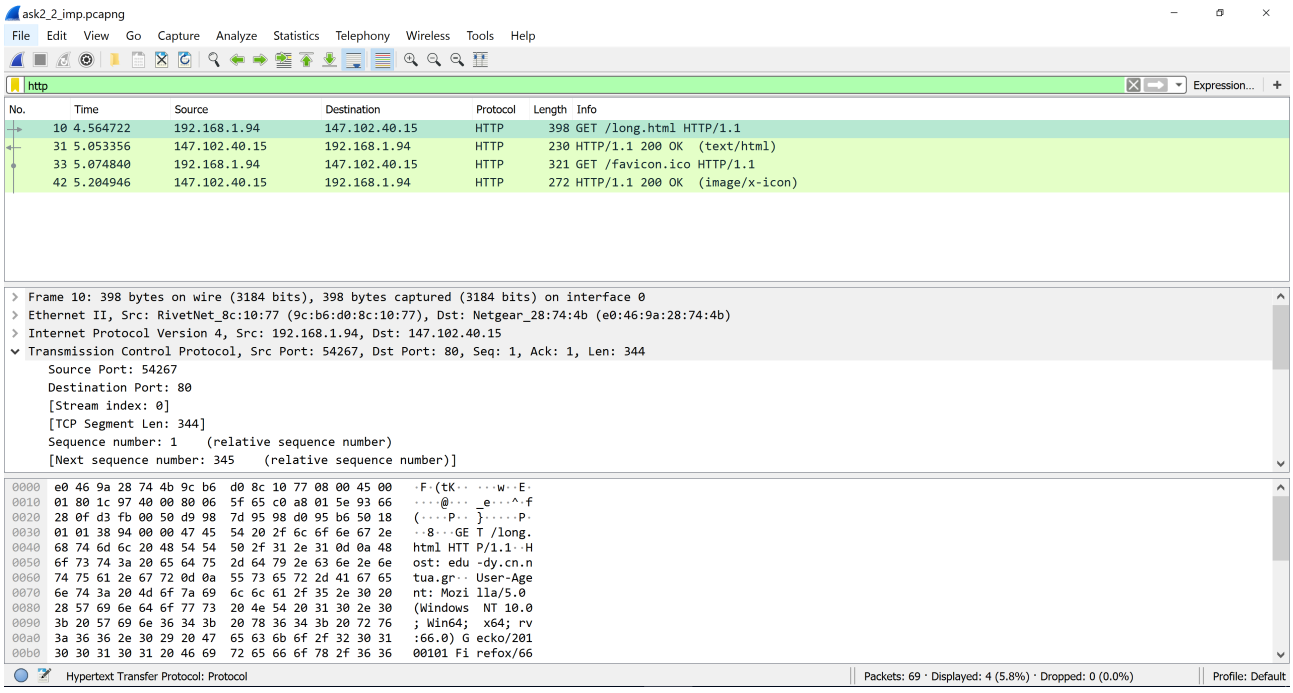
Εν συνεχεία, τροποποιούμε το φίλτρο ώστε να παραμείνουν μόνο τα δεύτερα τεμάχια κάθε τριμερούς χειραψίας. Παρατηρούμε ότι η πλευρά του εξυπηρετητή ανακοινώνει MSS ίσο με 536 bytes.



Σημείωση: Ως MSS θα επιλεγεί η μικρότερη εκ των δύο τιμών που ανακοινώνονται, δηλ. εν προκειμένω η τιμή των 536 bytes.

2.3:

Εφαρμόζουμε το φίλτρο http και παρατηρούμε ότι στάλθηκαν δύο HTTP αιτήσεις τύπου GET.

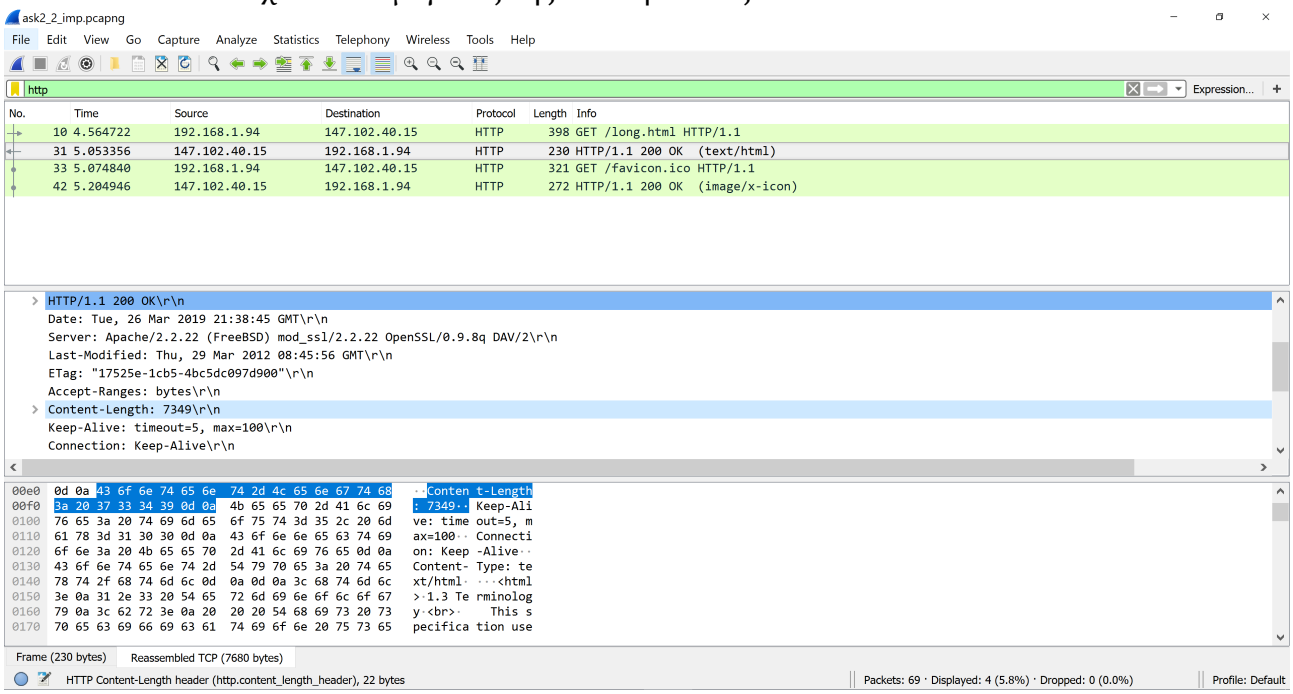


2.4:

Η απόκριση του εξυπηρετητή είναι HTTP/1.1 200 OK και στις δύο περιπτώσεις.

2.5:

Επικεντρωνόμαστε στην απόκριση που αφορά το αντικείμενο long.html. Αναλύουμε την επικεφαλίδα HTTP και εντοπίζουμε το πεδίο Content-Length, που έχει τιμή 7349 bytes. Αυτό σημαίνει ότι το μέγεθος της σελίδας long.html είναι ίσο με 7349 bytes.
Παρατηρούμε, επίσης, ότι το συνολικό HTTP περιεχόμενο έχει μέγεθος 7680 bytes, εκ των οποίων τα 7349 bytes είναι το μέγεθος της σελίδας ενώ τα υπόλοιπα αντιστοιχούν στο μέγεθος της επικεφαλίδας HTTP.

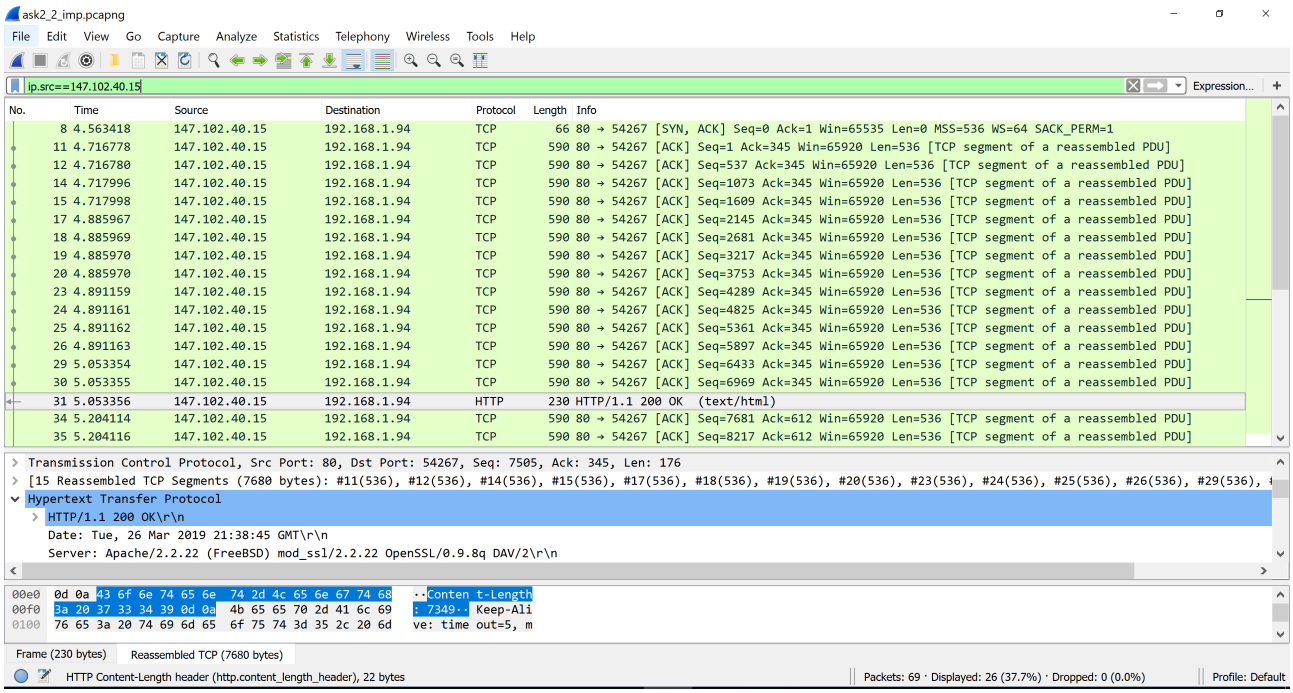


2.6:

Επειδή θέλουμε να εμφανίζεται η κίνηση που προέρχεται από τον εξυπηρετητή 147.102.40.15, επιλέγουμε ως φίλτρο το: ip.src==147.102.40.15

2.7:

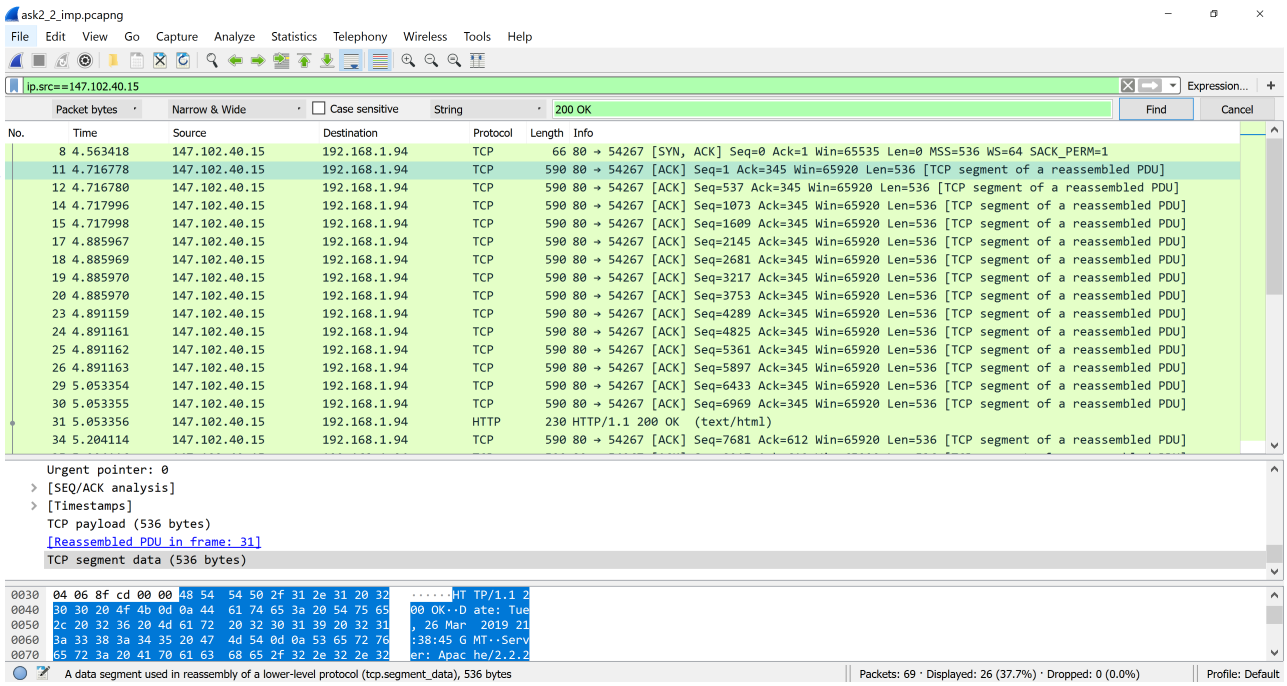
Χρειάστηκαν συνολικά 15 τεμάχια TCP. *Σημείωση*: Το πρώτο τεμάχιο TCP που εμφανίζεται στο screenshot δεν το μετράμε, καθώς αντιστοιχεί στην δεύτερο μέρος της τριμερούς χειραψίας. Ωστόσο, σύμφωνα με την υπόδειξη που μας δίνεται, συμπεριλαμβάνουμε στην καταμέτρηση το επισημασμένο (επιλεγμένο) τεμάχιο που φαίνεται στο screenshot (αυτό για το οποίο εμφανίζεται HTTP στη στήλη Protocol), επειδή είναι το τελευταίο της σειράς.



2.8:

Για να εκτελέσουμε την αναζήτηση, αρχικά κάνουμε κλικ στο πρώτο πακέτο (πάνω πάνω) και κατόπιν επιλέγουμε Edit>Find Packet ή πληκτρολογούμε Ctrl+F. Εν συνεχεία, επιλέγουμε να κάνουμε αναζήτηση μέσα στα “Packet bytes” και να αναζητήσουμε ένα “String”. Στο πεδίο αναζήτησης θα πρέπει να πληκτρολογήσουμε ως κείμενο αναζήτησης το: 200 OK (με αγγλικούς χαρακτήρες).

Όταν πατήσουμε το Find, θα επισημανθεί το πακέτο που περιέχει τον συγκεκριμένο κωδικό. Όπως αναμενόταν, το πακέτο αυτό είναι το πρώτο από τα 15 της σειράς (βλ. Screenshot).

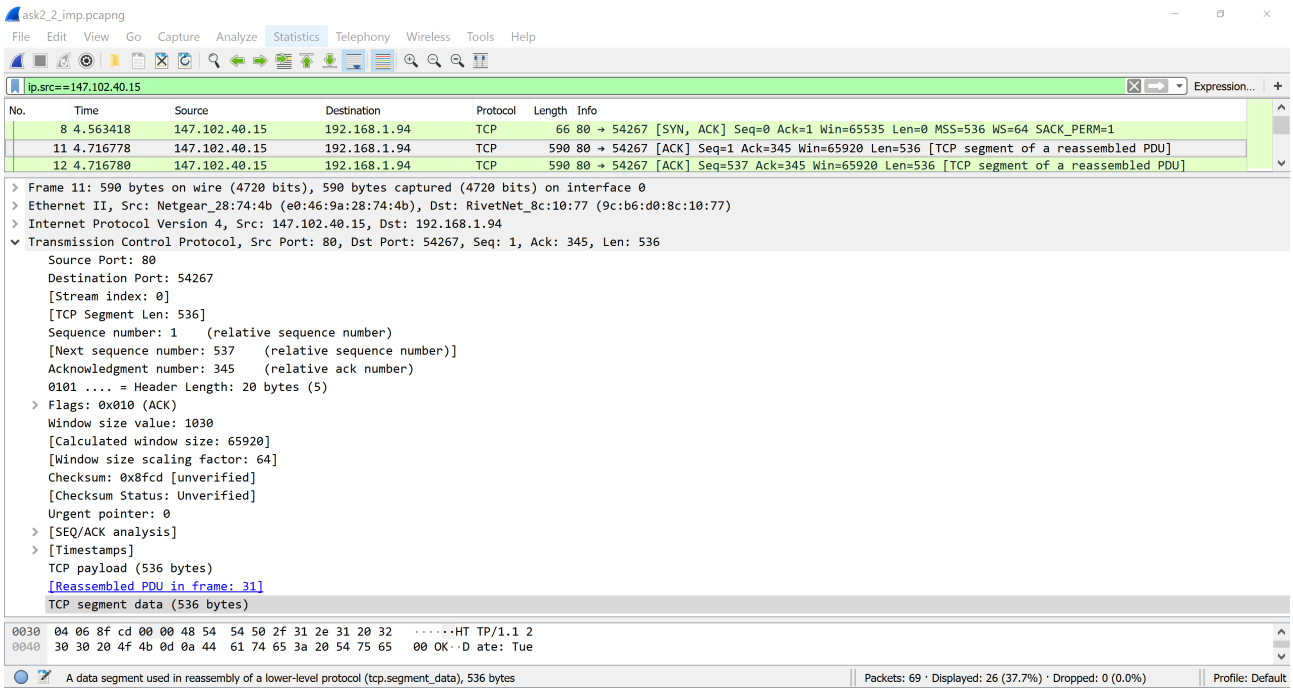


2.9:

Όπως φαίνεται και στο παραπάνω screenshot, το μέγεθος περιεχομένου HTTP (δηλ. TCP payload) στο εν λόγω τεμάχιο αλλά και στα υπόλοιπα της σειράς με εξαίρεση το τελευταίο είναι: 536 bytes (όσο δηλ. και το MSS).

2.10:

Το μέγεθος των 14 πρώτων από τα 15 πλαίσια της σειράς είναι σταθερό και ίσο με 590 bytes, το οποίο προκύπτει ως εξής: 14 bytes (Ethernet επικεφαλίδα) + 20 bytes (IP επικεφαλίδα) + 20 bytes (TCP επικεφαλίδα) + 536 bytes (HTTP περιεχόμενο) = 590 bytes. Σε όλα αυτά τα τεμάχια, το TCP payload ταυτίζεται με το MSS και είναι ίσο με 536 bytes.



2.11:

Όπως είδαμε στο ερώτημα 2.5, το συνολικό μέγεθος HTTP περιεχομένου (δεδομένα και επικεφαλίδα) είναι 7680 bytes. Με τα 14 πρώτα τεμάχια της σειράς μεταφέρθηκαν: 14*536 = 7504 bytes. Επομένως, απομένουν 7680 – 7504 = 176 bytes να μεταφερθούν. Το 15ο πλαίσιο έχει μέγεθος 230 bytes διότι: 14 bytes (Ethernet επικεφαλίδα) + 20 bytes (IP επικεφαλίδα) + 20 bytes (TCP επικεφαλίδα) + 176 bytes (εναπομείναν HTTP περιεχόμενο) = 230 bytes.