Εργαστήριο Wireshark: TCP

Computer Networking: A Top-Down Approach Featuring the Internet

Έκδοση: 2.0

Μετάφραση - Απόδοση: Σ. Τσακιρίδου

Στο εργαστήριο αυτό θα εξετάσουμε λεπτομερώς τη συμπεριφορά του TCP. Θα το κάνουμε αυτό αναλύοντας ένα trace από TCP segments τα οποία στέλνονται και λαμβάνονται κατά τη μεταφορά ενός αρχείου 150 KB (που περιέχει το κείμενο του έργου του Lewis Carrol *Alice's Adventures in Wonderland*) από τον υπολογιστή σας σε έναν απομακρυσμένο server. Θα μελετήσουμε τον τρόπο που το TCP χρησιμοποιεί τους αριθμούς ακολουθίας και επιβεβαίωσης για να παρέχει αξιόπιστη μεταφορά δεδομένων, θα παρατηρήσουμε τον αλγόριθμο ελέγχου συμφόρησης του TCP – αργή εκκίνηση και αποφυγή συμφόρησης – σε δράση και θα εξετάσουμε το μηχανισμό ελέγχου ροής του TCP. Θα εξετάσουμε συνοπτικά την εγκαθίδρυση σύνδεσης TCP και θα διερευνήσουμε την απόδοση (throughput και round-trip time) της σύνδεσης TCP ανάμεσα στον υπολογιστή σας και τον server.

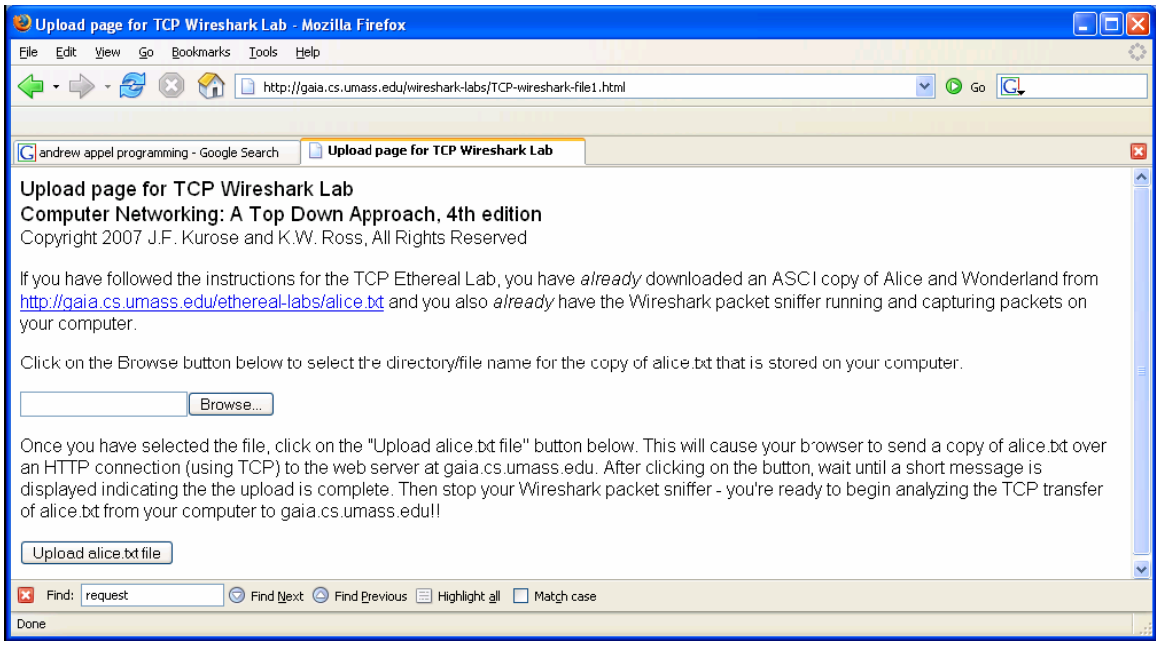
Πριν ξεκινήσετε αυτό το εργαστήριο, πιθανόν να θέλετε να κάνετε μία ανασκόπηση των Ενοτήτων 3.5 και 3.7 του βιβλίου.

1. Σύλληψη μαζικής μεταφοράς TCP από τον υπολογιστή σας σε έναν απομακρυσμένο server

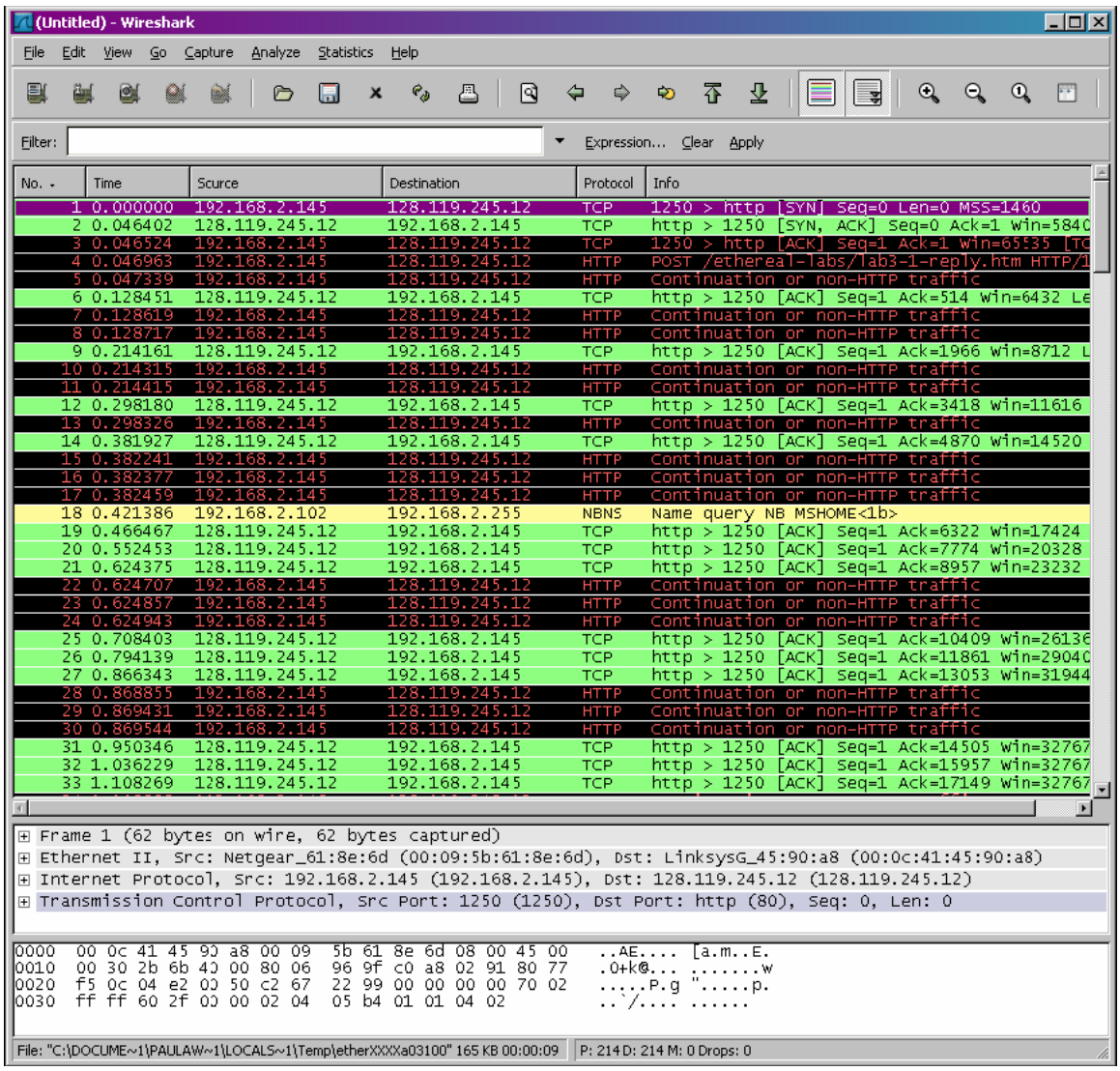
Πριν ξεκινήσουμε την εξερεύνηση του TCP, θα χρειαστεί να χρησιμοποιήσουμε το Wireshark για να αποκτήσουμε το trace των πακέτων της μεταφοράς από το TCP ενός αρχείου από τον υπολογιστή σας σε έναν απομακρυσμένο server. Αυτό θα επιτευχθεί με την πρόσβαση σε μία ιστοσελίδα η οποία θα σας επιτρέψει να εισάγετε το όνομα ενός αποθηκευμένου στον υπολογιστή σας αρχείου (το οποίο περιέχει το κείμενο ASCII του *Alice in Wonderland*) και έπειτα να μεταφέρετε το αρχείο σε ένα Web server χρησιμοποιώντας τη μέθοδο HTTP POST (βλ. Ενότητα 2.2.3 του βιβλίου). Χρησιμοποιούμε τη μέθοδο POST και όχι τη μέθοδο GET καθώς θέλουμε να μεταφέρουμε ένα μεγάλο όγκο δεδομένων *από* τον δικό σας υπολογιστή σε έναν άλλο υπολογιστή. Φυσικά, θα τρέχουμε το Wireshark κατά τη διάρκεια του χρόνου μεταφοράς ώστε να αποκτήσουμε το trace των TCP segments που στέλνονται και λαμβάνονται από τον υπολογιστή σας.

Ακολουθήστε τα παρακάτω βήματα:

- Ξεκινήστε τον browser σας. Πηγαίνετε στο http://gaia.cs.umass.edu/wireshark-labs/alice.txt και ανακτήσετε ένα αντίγραφο ASCII του *Alice in Wonderland*. Αποθηκεύστε το αρχείο αυτό στον υπολογιστή σας.
- Στη συνέχεια πηγαίνετε στο http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.
- Ο browser σας θα πρέπει να εμφανίσει μία ιστοσελίδα παρόμοια με την παρακάτω:



- Χρησιμοποιείστε το κουμπί *Browse* στη φόρμα αυτή για να εισάγετε το όνομα του αρχείου (πλήρες path name) στον υπολογιστή σας που περιέχει το *Alice in Wonderland* (μπορείτε επίσης να εισάγετε το όνομα με το χέρι). Μην πιέστε ακόμη το κουμπί "*Upload alice.txt file*".
- Ξεκινήστε τώρα το Wireshark και τη σύλληψη πακέτων *(Capture→Options)* και στη συνέχεια πιέστε *OK* στο παράθυρο Επιλογές Σύλληψης Πακέτων (Packet Capture Options) του Wireshark (δε θα χρειαστεί να διαλέξουμε κάποια από τις επιλογές εδώ).
- Επιστρέφοντας στον browser σας, πιέστε το κουμπί "*Upload alice.txt file*" για να φορτώσετε το αρχείο στον server gaia.cs.umass.edu. Αφού ολοκληρωθεί η μεταφορά του αρχείου, ένα μικρό συγχαρητήριο μήνυμα θα εμφανισθεί στο παράθυρο του browser σας.
- Σταματήστε τη σύλληψη πακέτων από το Wireshark. Το παράθυρο του Wireshark θα πρέπει να είναι παρόμοιο με το παράθυρο που φαίνεται παρακάτω:



Εάν δεν είστε σε θέση να τρέξετε το Wireshark σε μία ζωντανή σύνδεση δικτύου, μπορείτε να φορτώσετε ένα αρχείο με το trace πακέτων που συνελήφθη κατά την εκτέλεση των παραπάνω βημάτων στον υπολογιστή του συγγραφέα[1]. Ενδεχομένως να διαπιστώσετε ότι αξίζει να φορτώσετε αυτό το trace ακόμη και αν έχετε συλλάβει το δικό σας και να το χρησιμοποιήσετε παράλληλα με το δικό σας καθώς διερευνάτε τις ερωτήσεις που τίθενται παρακάτω.

[1] Φορτώστε το αρχείο zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip και εξάγετε το αρχείο tcp-ethereal-trace-1. Τα traces που περιέχονται σε αυτό το αρχείο zip συλλέχθηκαν από το Wireshark ενώ εκτελούνταν τα βήματα που περιγράφονται στο εργαστήριο Wireshark στον υπολογιστή του συγγραφέα. Αφού λάβετε το trace, μπορείτε να το φορτώσετε στο Wireshark και να το δείτε στο παράθυρο χρησιμοποιώντας το μενού *File*, επιλέγοντας *Open* και στη συνέχεια επιλέγοντας το αρχείο tcp-ethereal-trace-1 του trace.

2. Μία πρώτη ματιά στο trace

Πριν αναλύσουμε λεπτομερώς τη συμπεριφορά της σύνδεσης TCP, ας κάνουμε μία γενική επισκόπηση του trace.

- Πρώτα φιλτράρετε τα πακέτα που παρουσιάζονται στο παράθυρο του Wireshark εισάγοντας "tcp" (με μικρά γράμματα, χωρίς εισαγωγικά και χωρίς να ξεχάσετε να πιέσετε return μετά την εισαγωγή) στο παράθυρο των προδιαγραφών του φίλτρου παρουσίασης που βρίσκεται προς το επάνω μέρος του παραθύρου του Wireshark.

Στο παράθυρο καταλόγου πακέτων θα πρέπει να δείτε μία σειρά από μηνύματα TCP και HTTP να ανταλλάσσονται μεταξύ του υπολογιστή σας και του server gaia.cs.umass.edu. Θα πρέπει να δείτε την αρχική χειραψία τριών βημάτων που περιέχει ένα μήνυμα SYN. Θα πρέπει να δείτε ένα μήνυμα HTTP POST και μία σειρά από μηνύματα "HTTP Continuation" να στέλνονται από τον υπολογιστή σας στο gaia.cs.umass.edu. Υπενθυμίζεται, από την συζήτηση στο προηγούμενο εργαστήριο Wireshark για το HTTP, ότι δεν υπάρχουν μηνύματα Continuation στο HTTP – το Wireshark χρησιμοποιεί αυτόν τον τρόπο για να υποδείξει ότι χρησιμοποιούνται πολλαπλά TCP segments για τη μεταφορά ενός μηνύματος HTTP. Θα πρέπει επίσης να δείτε TCP segments με επιβεβαιώσεις (ACK) να επιστρέφουν από το gaia.cs.umass.edu στον υπολογιστή σας.

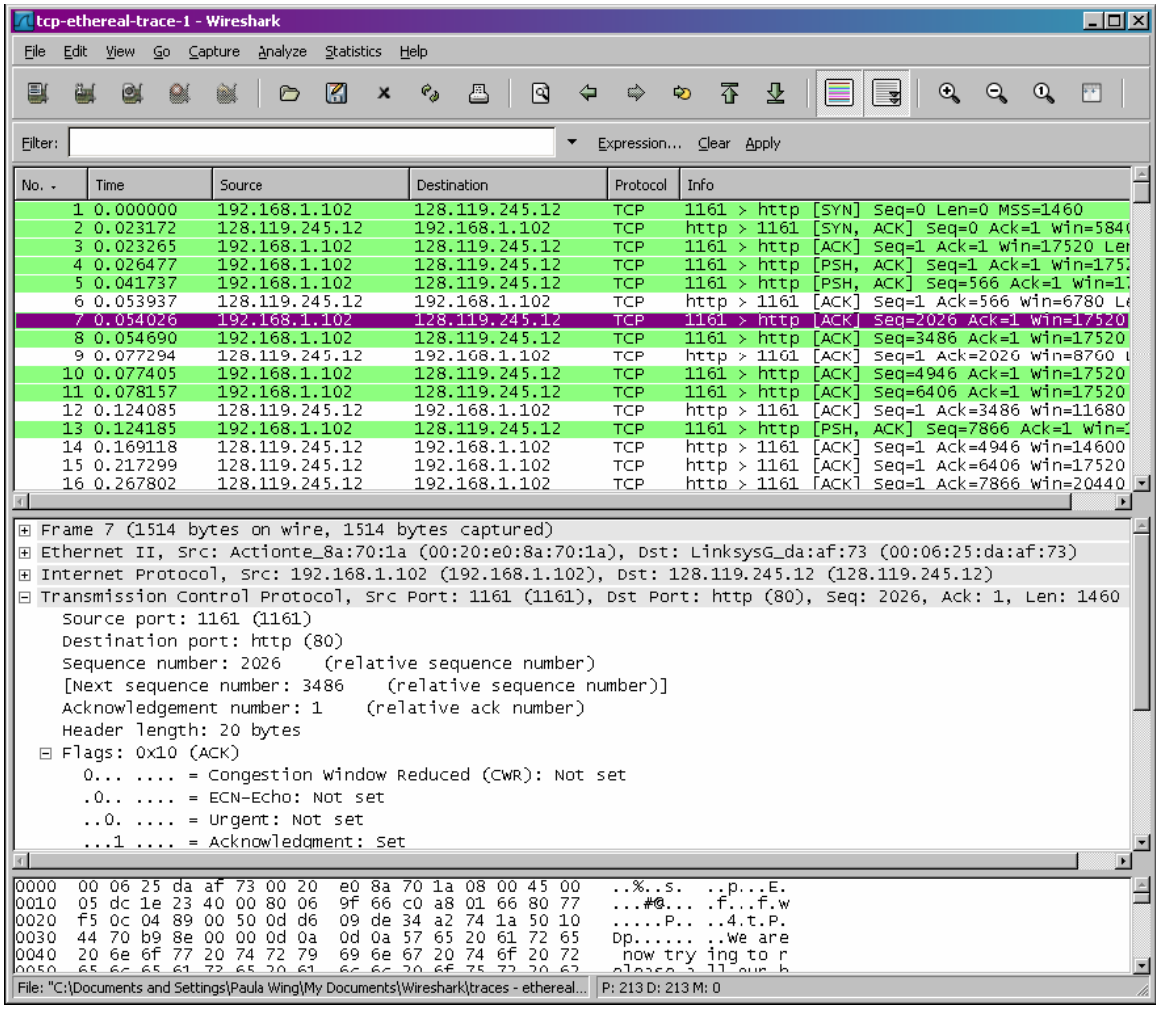
Ανοίξτε το αρχείο *tcp-ethereal-trace-1* των πακέτων που έχουν συλληφθεί από το Wireshark που περιέχεται στο http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip (δηλαδή, φορτώστε το trace και ανοίξτε το στο Wireshark - βλ. υποσημείωση 1) και στη συνέχεια απαντήστε στις ακόλουθες ερωτήσεις. Όπου είναι δυνατό, η απάντησή σας θα πρέπει να συνοδεύεται από μία εκτύπωση των πακέτων του trace που χρησιμοποιήσατε για να απαντήσετε στην ερώτηση. Σημειώστε επάνω στην εκτύπωση τα σημεία εκείνα που αιτιολογούν την απάντησή σας. Για να εκτυπώσετε ένα πακέτο, χρησιμοποιήστε *File→Print*, επιλέξτε *Selected packet only*, επιλέξτε *Packet summary line* και επιλέξτε το ελάχιστο ποσό λεπτομερειών πακέτου που χρειάζεστε για να απαντήσετε στην ερώτηση.

1. Ποια η διεύθυνση IP και ποιος ο αριθμός θύρας TCP που χρησιμοποιείται από τον client (πηγή) που μεταφέρει το αρχείο στο gaia.cs.umass.edu; Για να απαντήσετε στην ερώτηση αυτή είναι μάλλον ευκολότερο να επιλέξετε ένα μήνυμα HTTP και να εξετάσετε τις λεπτομέρειες του πακέτου TCP που χρησιμοποιήθηκε για να μεταφέρει αυτό το μήνυμα, χρησιμοποιώντας το παράθυρο με τις λεπτομέρειες επικεφαλίδας επιλεγμένου πακέτου (βλ. Σχήμα 2 στο εισαγωγικό εργαστήριο Wireshark για απορίες σχετικά με τα παράθυρα του Wireshark).
2. Ποια η διεύθυνση IP του gaia.cs.umass.edu; Σε ποιο αριθμό θύρας στέλνει και λαμβάνει segments για αυτήν τη σύνδεση TCP;

Εάν έχετε κατορθώσει να δημιουργήσετε το δικό σας trace, απαντήστε στην ακόλουθη ερώτηση:

3. Ποια η διεύθυνση IP και ποιος ο αριθμός θύρας TCP που χρησιμοποιείται από τον δικό σας client (πηγή) για τη μεταφορά του αρχείου στο gaia.cs.umass.edu;

Επειδή το εργαστήριο αυτό εστιάζει στο TCP και όχι στο HTTP, ας μεταβάλλουμε το παράθυρο καταλόγου πακέτων του Wireshark ώστε να παρουσιάζει πληροφορίες σχετικά με τα TCP segments που περιέχουν τα μηνύματα HTTP αντί για τα μηνύματα HTTP. Για να το κάνει αυτό το Wireshark, επιλέξτε *Analyze→Enabled Protocols*. Στη συνέχεια ξεμαρκάρετε το κουτί HTTP και επιλέξτε *OK*. Θα πρέπει τώρα να δείτε ένα παράθυρο Wireshark παρόμοιο με το ακόλουθο:



Αυτός ήταν ο επιδιωκόμενος στόχος - μία σειρά από TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του gaia.cs.umass.edu. Στο υπόλοιπο μέρος αυτού του εργαστηρίου, θα χρησιμοποιήσουμε το trace των πακέτων που έχετε συλλάβει (και το trace πακέτων *tcp-ethereal-trace-1* στο http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip - βλ. υποσημείωση 1) για να μελετήσουμε τη συμπεριφορά του TCP.

3. Βασικά χαρακτηριστικά του TCP

Απαντήστε στις ακόλουθες ερωτήσεις για τα TCP segments:

4. 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; Ποιο στοιχείο του segment προσδιορίζει ότι πρόκειται για ένα SYN segment;
5. 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;
6. Ποιος ο αριθμός ακολουθίας του TCP segment που περιέχει την εντολή HTTP POST; Σημειώνεται ότι για να εντοπίσετε την εντολή POST θα χρειαστεί να ψάξετε στο πεδίο περιεχομένων πακέτου που βρίσκεται στο κάτω μέρος του παραθύρου Wireshark αναζητώντας ένα segment που περιέχει τους χαρακτήρες "POST" στο πεδίο των δεδομένων του.
7. Θεωρείστε το TCP segment που περιέχει την εντολή HTTP POST ως το πρώτο segment της σύνδεσης TCP. Ποιοι οι αριθμοί ακολουθίας των πρώτων έξι segments της σύνδεσης TCP (συμπεριλαμβανομένου και του segment που περιέχει την εντολή HTTP POST); Ποιος ο χρόνος αποστολής του κάθε segment; Ποιος ο χρόνος λήψης της επιβεβαίωσης ACK για κάθε segment; Δεδομένης της διαφοράς μεταξύ του χρόνου αποστολής ενός TCP segment και του χρόνου λήψης της επιβεβαίωσής του, ποια η τιμή του RTT για καθένα από τα έξι segments; Ποια η τιμή της μεταβλητής `EstimatedRTT` (βλ. σελίδα 236 βιβλίου) μετά τη λήψη της κάθε επιβεβαίωσης ACK; Υποθέστε ότι η τιμή του `EstimatedRTT` είναι ίση με τον μετρούμενο χρόνο RTT για το πρώτο segment, ενώ για τα όλα τα επόμενα segments υπολογίζεται από την εξίσωση που δίνεται για το `EstimatedRTT` στη σελίδα 236 του βιβλίου.

   Σημείωση: Το Wireshark διαθέτει ένα χαρακτηριστικό γνώρισμα που σας επιτρέπει να παραστήσετε γραφικά το χρόνο RTT για καθένα από τα απεσταλμένα TCP segments. Στο παράθυρο καταλόγου πακέτων επιλέξτε ένα TCP segment το οποίο στέλνεται από τον client στον server gaia.cs.umass.edu. Στη συνέχεια επιλέξτε *Statistics→TCP Stream Graph →Round Trip Time Graph.*
8. Ποιο το μήκος καθενός από τα έξι πρώτα TCP segments[2];
9. Ποιος ο ελάχιστος διαθέσιμος χώρος αποθήκευσης (buffer space) που ανακοινώνεται από τον παραλήπτη σε ολόκληρο το trace; Συμβαίνει ποτέ η

[2] Τα TCP segments στο αρχείο tcp-ethereal-trace-1 του trace είναι όλα μικρότερα από 1460 bytes. Αυτό οφείλεται στο γεγονός ότι ο υπολογιστής που χρησιμοποιήθηκε για τη συλλογή του trace έχει μία κάρτα Ethernet η οποία περιορίζει το μέγιστο μήκος ενός IP datagram σε 1500 bytes (40 bytes για τις επικεφαλίδες TCP/IP και 1460 bytes ωφέλιμου φορτίου TCP). Αυτή η τιμή των 1500 bytes αποτελεί το καθιερωμένο μέγιστο επιτρεπτό μήκος στο Ethernet. Εάν το δικό σας trace εμφανίζει ένα TCP segment με μήκος μεγαλύτερο από 1460 bytes και ο υπολογιστής σας χρησιμοποιεί μία σύνδεση Ethernet, τότε το Wireshark αναφέρει λάθος μήκος TCP segment. Είναι πολύ πιθανό επίσης να δείχνει μόνο ένα μεγάλο TCP segment αντί για πολλαπλά μικρότερα segments. Στην πραγματικότητα, ο υπολογιστής σας μάλλον στέλνει πολλαπλά μικρότερα segments όπως υποδεικνύεται από τις πολλαπλές επιβεβαιώσεις που λαμβάνει. Αυτή η ασυνέπεια στα αναφερόμενα μήκη των segments οφείλεται στην αλληλεπίδραση μεταξύ του Ethernet driver και του λογισμικού Wireshark. Σε περίπτωση που αντιμετωπίζετε αυτό το πρόβλημα, συνιστούμε να χρησιμοποιήσετε το trace του αρχείου tcp-ethereal-trace-1 για το εργαστήριο αυτό.

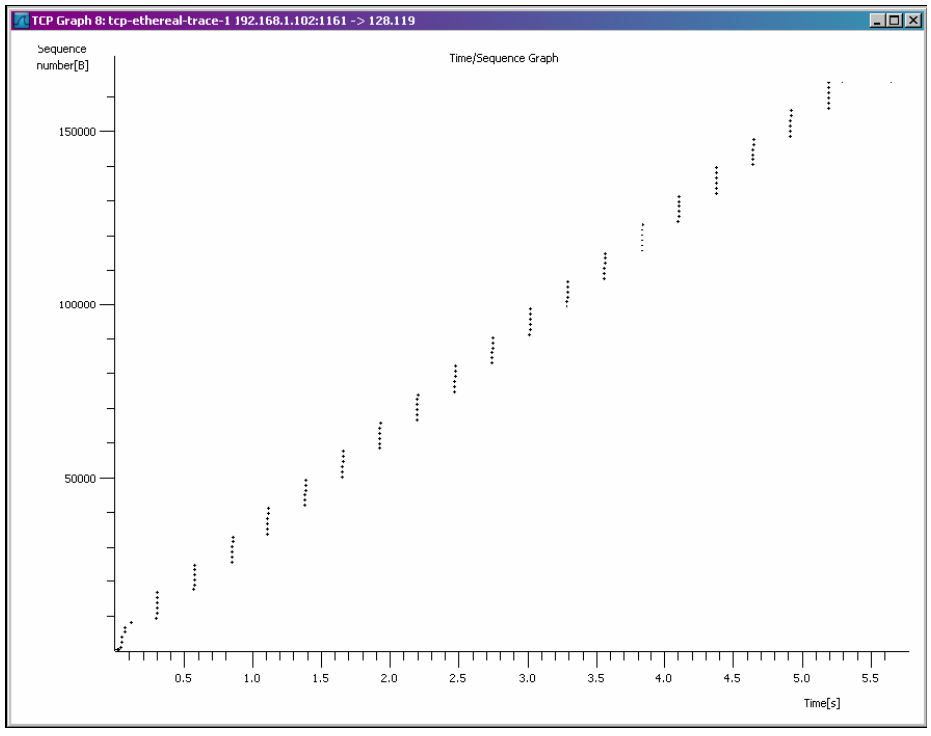
έλλειψη χώρου αποθήκευσης στον παραλήπτη να περιορίζει το ρυθμό του αποστολέα;

10. Υπάρχουν επαναμεταδιδόμενα segments στο αρχείο του trace; Σε τι είδους έλεγχο του trace βασίσατε την απάντησή σας στην ερώτηση αυτή;
11. Πόσα bytes δεδομένων επιβεβαιώνει συνήθως ο παραλήπτης σε μία επιβεβαίωση; Μπορείτε να διακρίνετε περιπτώσεις όπου ο παραλήπτης επιβεβαιώνει κάθε δεύτερο λαμβανόμενο segment (βλ. Πίνακα 3.2 στη σελίδα 244 του βιβλίου);
12. Ποιο το throughput (αριθμός μεταφερόμενων bytes ανά μονάδα χρόνου) της σύνδεσης TCP; Εξηγείστε τον τρόπο με τον οποίο υπολογίσατε την τιμή αυτή.

4. Ο αλγόριθμος συμφόρησης του TCP σε δράση

Ας εξετάσουμε τώρα τον όγκο των δεδομένων που στέλνονται ανά μονάδα χρόνου από τον client στον server. Αντί να υπολογίσουμε το μέγεθος αυτό από τα ανεπεξέργαστα δεδομένα του παραθύρου του Wireshark, θα χρησιμοποιήσουμε ένα από τα βοηθητικά γραφικά εργαλεία του Wireshark για το TCP - *Time-Sequence-Graph(Stevens)* - για να παραστήσουμε γραφικά τα δεδομένα.

- Επιλέξτε ένα TCP segment στο παράθυρο καταλόγου πακέτων του Wireshark. Κατόπιν επιλέξτε το μενού *Statistics→TCP Stream Graph→Time-Sequence-Graph(Stevens)*. Θα πρέπει να δείτε μία γραφική παράσταση παρόμοια με την ακόλουθη η οποία δημιουργήθηκε για τα δεδομένα του trace πακέτων *tcp-ethereal-trace-1* που περιέχεται στο http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip (βλ. υποσημείωση 1):



Στην παραπάνω γραφική παράσταση, όπου κάθε κουκκίδα παριστάνει ένα απεσταλμένο TCP segment, δίνεται ο αριθμός ακολουθίας του segment και ο χρόνος αποστολής του. Παρατηρήστε ότι ένα σύνολο κουκκίδων, με τη μία κουκκίδα πάνω από την άλλη, αναπαριστά μία ακολουθία πακέτων που στάλθηκαν το ένα αμέσως μετά το άλλο (back-to-back).

Απαντήστε στις ακόλουθες ερωτήσεις για τα TCP segments του trace πακέτων *tcp-ethereal-trace-1* που περιέχεται στο http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

13. Χρησιμοποιείστε το γραφικό εργαλείο *Time-Sequence-Graph(Stevens)* για να λάβετε τη γραφική παράσταση του αριθμού ακολουθίας ως προς το χρόνο των segments που στέλνονται από τον client στον server gaia.cs.umass.edu. Μπορείτε να προσδιορίσετε πότε αρχίζει και τελειώνει η φάση αργής εκκίνησης (slow start) του TCP, και πότε γίνεται μετάβαση στη φάση αποφυγής συμφόρησης (congestion avoidance); Προσέξτε ότι στο "πραγματικό" αυτό trace, η συμπεριφορά του TCP διαφέρει από την ιδανική που παρουσιάζεται στο Σχήμα 3.51 του βιβλίου (προσέξτε επίσης ότι τα μεγέθη στον κατακόρυφο άξονα των δύο γραφικών παραστάσεων είναι διαφορετικά).
14. Σχολιάστε τις διαφορές ανάμεσα στα δεδομένα των μετρήσεων και στην εξιδανικευμένη συμπεριφορά του TCP που μελετήσαμε στο βιβλίο.
15. Απαντήστε σε καθεμία από τις δύο παραπάνω ερωτήσεις για το trace που συλλέξατε εσείς κατά τη μεταφορά του αρχείου από τον υπολογιστή σας στο gaia.cs.umass.edu.