ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Δίκτυα Υπολογιστών

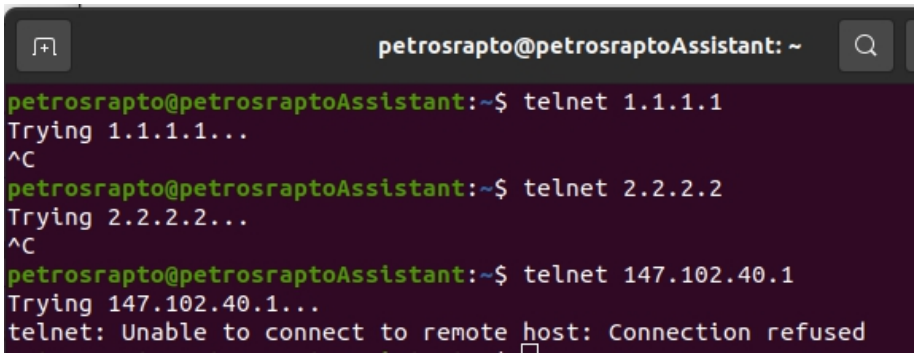
Αναφορά 7ης Εργαστηριακής Άσκησης

Ραπτόπουλος Πέτρος (el19145)
Ομάδα 3

Ημερομηνία: 23/11/2022

Άσκηση 1: Μετάδοση δεδομένων με TCP

Δημιουργούμε ένα φίλτρο σύλληψης στο Wireshark ώστε να καταγράφονται μόνο πακέτα IPv4 που περιλαμβάνουν τη διεύθυνση IPv4 του υπολογιστή μας, ανοίγουμε ένα παράθυρο εντολών και καταγράφουμε την κίνηση που παράγεται όταν κάνουμε telnet στον υπολογιστή 1.1.1.1, που υπάρχει αλλά δεν απαντά, και περιμένουμε μέχρι να τερματίσει η εντολή [Περίπτωση Α]. Μετά επιχειρούμε telnet στον υπολογιστή 2.2.2.2, που εάν υπάρχει δεν απαντά, και περιμένουμε μέχρι να τερματίσει η εντολή [Περίπτωση Β]. Τέλος, επιχειρούμε telnet στον υπολογιστή 147.102.40.1, όπου όμως δεν γίνονται δεκτές τέτοιες συνδέσεις [Περίπτωση Γ]. Όταν τελειώσει η διαδικασία, σταματάμε την καταγραφή των πακέτων.

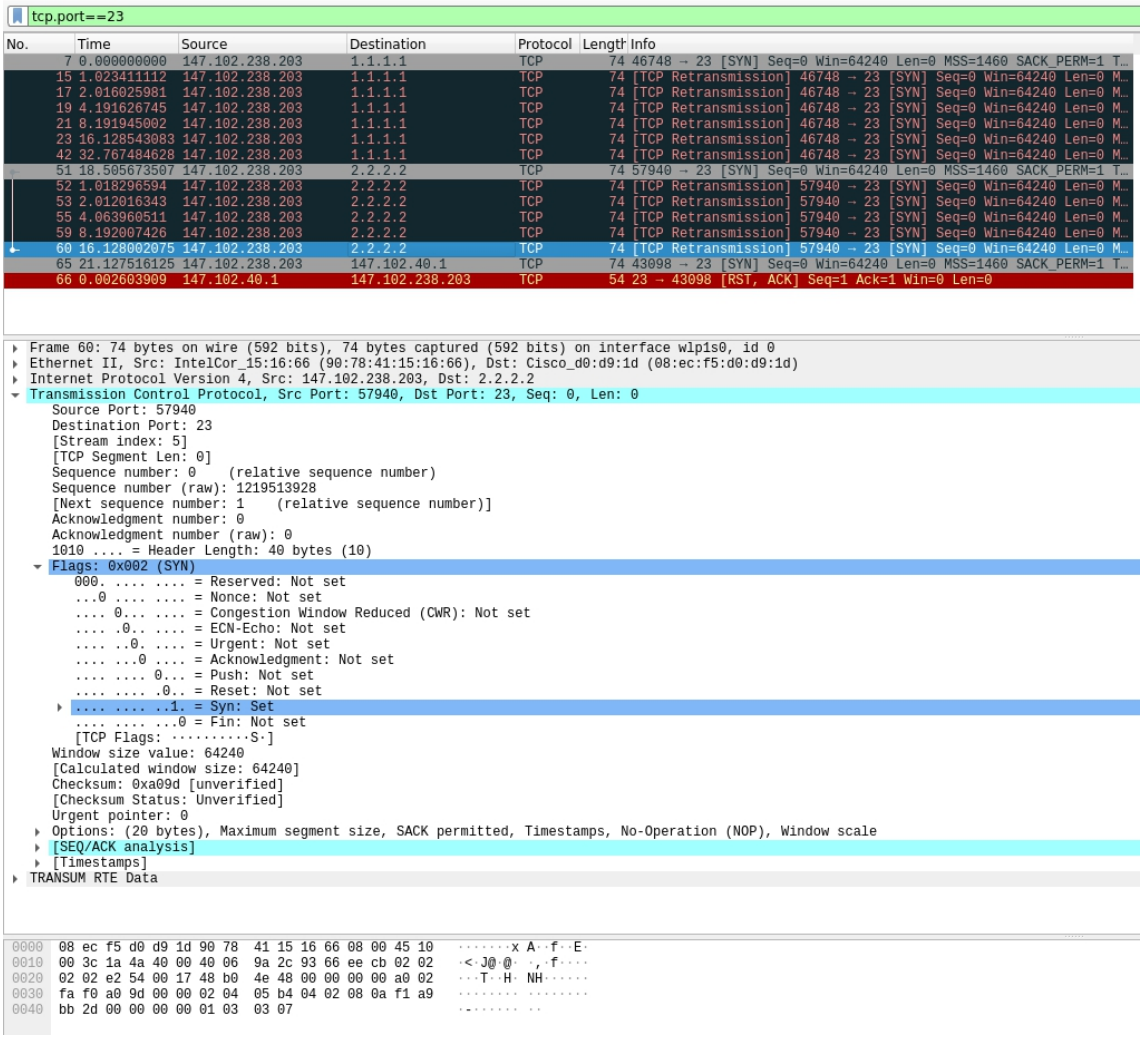


1.1) Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πακέτα που περιλαμβάνουν τη διεύθυνση IPv4 του υπολογιστή σας.: **host 147.102.238.203**

1.2) Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο πακέτα προς κάποιον από τους παραπάνω προορισμούς. Ποια είναι η σύνταξή του;: **ip.addr == 1.1.1.1 or ip.addr == 2.2.2.2 or ip.addr == 147.102.40.1**

1.3) Σε ποια θύρα (του άλλου υπολογιστή) προσπαθεί να συνδεθεί ο δικός σας υπολογιστής;: **θύρα 23 (telnet)**

1.4) Εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια TCP που σχετίζονται με τη θύρα αυτή. Ποια είναι η σύνταξή του;: **tcp.port==23**



1.5) Ποια σημαία μήκους 1 bit ενεργοποιείται για την εκκίνηση της εγκατάστασης της σύνδεσης TCP; **SYN**

1.6) Πόσες προσπάθειες κάνει ο υπολογιστής σας προκείμενου να εγκαταστήσει σύνδεση TCP στις Περιπτώσεις Α και Β; **Περίπτωση Α: 7 προσπάθειες, Περίπτωση Β: 6 προσπάθειες**

1.7) Καταγράψτε τη χρονική απόσταση μεταξύ των διαδοχικών προσπαθειών εγκατάστασης σύνδεσης.
Οι χρονικές αποστάσεις φαίνονται στην παραπάνω εικόνα.

1.8) Τι παρατηρείτε συγκρίνοντας τα αποτελέσματα των περιπτώσεων Α και Β; **Και στις δύο περιπτώσεις έχουμε όμοια συμπεριφορά. Αλλάζει μόνο το Source Port και Sequence Number.**

1.9) Ποια βήματα της τριπλής χειραψίας παρατηρήσατε;
Παρατηρήσαμε μόνο το πρώτο βήμα, δηλαδή την προσπάθεια της μιας πλευράς να εγκαταστήσει σύνδεση TCP. Ωστόσο δεν λάβαμε απάντηση από τον υπολογιστή στόχο για τις πρώτες δύο περιπτώσεις, ενώ για την τρίτη περίπτωση λάβαμε μήνυμα απόλυσης της σύνδεσης.

1.10) Ο υπολογιστής σας απολύει τη σύνδεση ή απλώς εγκαταλείπει την προσπάθεια;
Στις πρώτες δύο περιπτώσεις ο υπολογιστής εγκαταλείπει την προσπάθεια (στην πραγματικότητα όμως εμείς διακόψαμε την έκτέλεση της εντολής telnet στο terminal) ενώ στην τρίτη περίπτωση ο υπολογιστής στόχος απολύει την σύνδεση.

Στη συνέχεια, εφαρμόζουμε νέο φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια TCP που σχετίζονται με τον υπολογιστή της Περίπτωσης Γ.

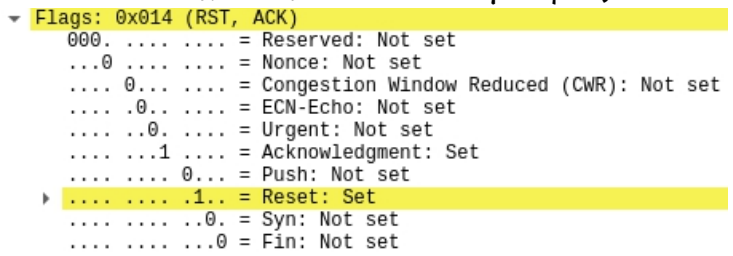
1.11) Ποια είναι η σύνταξή του; **ip.addr == 147.102.40.1 and tcp**

1.12) Πόσες προσπάθειες κάνει ο υπολογιστής σας προκείμενου να εγκαταστήσει σύνδεση TCP; **Μία**

1.13) Συγκρίνοντας με την απάντηση σας στο ερώτημα 1.8, ποιες διαφορές παρατηρείτε;
Ξανά αλλάζει μόνο το Source Port και Sequence Number.

Επιλέξτε ένα (ή το μοναδικό) από τα τεμάχια TCP που στέλνει ο 147.102.40.1 στον υπολογιστή σας προκειμένου να απορρίψει τη σύνδεση TCP.

1.14) Ποιες σημαίες μήκους 1 bit περιλαμβάνει;



1.15) Ποια εξ αυτών δηλώνει άρνηση της εγκατάστασης σύνδεσης TCP; **Reset flag**

1.16) Ποιο είναι το μέγεθος της επικεφαλίδας και ποιο το μέγεθος του πεδίου δεδομένων αυτού του τεμαχίου TCP;
Header Length: 20 bytes, Data: 0 bytes

1.17) Καταγράψτε τα ονόματα και το μήκος σε bit των πεδίων της επικεφαλίδας του τεμαχίου TCP:
Source Port(2 bytes), Destination Port(2 bytes), Sequence Number(4 bytes), Acknowledgment number(4 bytes), Header Length(4 bits), Flags(12 bits), Window Size value(2 bytes), Checksum(2 bytes), Urgent pointer(2 bytes)

1.18) Ποιο είναι το όνομα του πεδίου που προσδιορίζει το μέγεθος της επικεφαλίδας TCP.: **Data Offset**
Ποιο όνομα χρησιμοποιεί το Wireshark για το πεδίο αυτό της επικεφαλίδας TCP στο παράθυρο με τις λεπτομέρειες του επιλεγμένου πακέτου;: **Header Length**

1.19) Πώς προκύπτει το μήκος της επικεφαλίδας TCP από την τιμή που παρατηρείτε στα περιεχόμενα πακέτου σε δεκαεξαδική τιμή; **Πολλαπλασιάζουμε την τιμή με 32 bits. Έχουμε Header Length: 5(hex), δηλαδή 5(dec), άρα Header Length: 5*32bits = 20bytes**

1.20) Υπάρχει πεδίο της επικεφαλίδας TCP που να δηλώνει το μήκος του τεμαχίου; **Όχι**

1.21) Πώς προκύπτει το μήκος αυτό με βάση τα στοιχεία των επικεφαλίδων IPv4 και TCP;
Μήκος τεμαχίου(δεν συμπεριλαμβάνετε η επικεφαλίδα) = IP.total_length - IP.header_length - TCP.header_length

1.22) Ποιο είναι το μέγεθος της επικεφαλίδας του πρώτου ή μοναδικού τεμαχίου TCP που στέλνει ο υπολογιστής σας στον 147.102.40.1 για την εγκατάσταση σύνδεσης TCP; **40 bytes**

1.23) Υπάρχει διαφορά στο μέγεθος της επικεφαλίδας TCP των δύο παραπάνω τεμαχίων; Εάν ναι,που οφείλεται;
Ναι υπάρχει διαφορά. Οφείλεται στα πεδία Options(20 bytes) που παρουσιάζονται μόνο στο πακέτο που στάλθηκε προκειμένου να εγκατασταθεί η σύνδεση.

Άσκηση 2: Εγκατάσταση σύνδεσης, μεταφορά δεδομένων, απόλυση σύνδεσης TCP

Χρησιμοποιώντας το κατάλληλο φίλτρο σύλληψης στο Wireshark, αφού ανοίξουμε ένα παράθυρο εντολών, καταγράφουμε τα διερχόμενα τεμάχια TCP όταν χρησιμοποιώντας την εφαρμογή ftp συνδεόμαστε στον υπολογιστή edu-dy.cn.ntua.gr.

2.1) Ποιο φίλτρο σύλληψης χρησιμοποιήσατε για την καταγραφή της κίνησης; **tcp**

Εγκατάσταση Σύνδεσης
Παρατηρούμε τα τεμάχια TCP που ανταλλάχθηκαν και εντοπίζουμε τα σχετικά με την τριπλή χειραψία.
Βρίσκουμε δύο τριπλές χειραψίες: μία για την εγκατάσταση της σύνδεσης ελέγχου FTP και μία για τη μεταφορά δεδομένων FTP.
2.2) Σε ποια θύρα (ελέγχου FTP) του edu-dy.cn.ntua.gr προσπαθεί να συνδεθεί ο υπολογιστής σας για να αρχίσει η επικοινωνία με τον εξυπηρετητή FTP; **Θύρα 21**
2.3) Με ποια θύρα (δεδομένων FTP) του υπολογιστή edu-dy.cn.ntua.gr γίνεται η σύνδεση για τη μεταφορά δεδομένων (του αρχείου PCATTCP.exe); **49035**

Εφαρμόζουμε ένα φίλτρο απεικόνισης της μορφής tcp.port ώστε να παραμείνουν μόνο τα τεμάχια TCP που σχετίζονται με τη θύρα ελέγχου FTP.
2.4) Ποια είναι η σύνταξη του φίλτρου; **tcp.port == 21**
2.5) Πόσα τεμάχια TCP ανταλλάσσονται για την εγκατάσταση της σύνδεσης ελέγχου FTP; **3**
2.6) Ποιες σημαίες χρησιμοποιούνται για την εγκατάσταση της σύνδεσης TCP; **SYN, ACK**
2.7) Ποιο είναι το μέγεθος των επικεφαλίδων TCP των τεμαχίων αυτών; **40 για τα δύο πρώτα τεμάχια και 32 για το 3°**
2.8) Ποιο είναι το μέγεθος δεδομένων των τεμαχίων αυτών; **Δεν έχουμε δεδομένα για τα εν λόγω τεμάχια.**
2.9) Πόσο διαρκεί η διαδικασία της τριπλής χειραψίας; **0.001393341 seconds**
2.10) Συμφωνεί η τιμή που βρήκατε προηγουμένως με το iRTT που εμφανίζει το Wireshark κάτω από το [SEQ/ACK analysis] στο παράθυρο με τις λεπτομέρειες επικεφαλίδας; **[iRTT: 0.001393341 seconds], άρα συμφωνεί.**
2.11) Ποιοι είναι οι αρχικοί αριθμοί σειράς (Sequence Number) που ανακοινώνει η κάθε πλευρά;
Αρχικοί αριθμοί σειράς του υπολογιστή μας: Σχετικός αριθμός: 0, Απόλυτος αριθμός: 2955362915
Αρχικοί αριθμοί σειράς της άλλης πλευράς: Σχετικός αριθμός: 0, Απόλυτος αριθμός: 1800742591
2.12) Πώς προκύπτει ο αριθμός επιβεβαίωσης (Acknowledgement Number) του τεμαχίου TCP με το οποίο ο εξυπηρετητής FTP δηλώνει ότι αποδέχεται τη σύνδεση;
Το πεδίο Acknowledgement Number δείχνει τον αριθμό σειράς του επόμενου byte δεδομένων που αναμένεται. Συνεπώς σε περίπτωση αποδοχής της σύνδεση ο εξυπηρετητής FTP στέλνει τεμάχιο TCP με Acknowledgement Number ίσο με 1 αφού το πακέτο που παρέλαβε είχε Sequence Number ίσο με 0.
2.13) Πώς προκύπτουν ο αριθμός σειράς και ο αριθμός επιβεβαίωσης (Sequence Number και Acknowledgement Number) του τελευταίου τεμαχίου TCP της τριπλής χειραψίας με το οποίο ολοκληρώνεται η εγκατάσταση της σύνδεσης; **Το πεδίο Sequence number δείχνει τον αριθμό σειράς του πρώτου byte δεδομένων του τεμαχίου. Αν η σημαία SYN τεθεί, ο Sequence number είναι ο αρχικός αριθμός σειράς και το πρώτο byte δεδομένων έχει +1 αυτού. Συνεπώς ο Sequence number του τελευταίου τεμαχίου TCP ισούται με 1. Σύμφωνα με τα προαναφερθέντα στο ερώτημα 2.12) ο Acknowledgement Number πρέπει να ισούται με 1, αφού το τελευταίο τεμάχιο που παρέλαβε από την απέναντι πλευρά είχε Sequence number ίσο με 1.**

2.14) Ποιο είναι το μήκος δεδομένων των τριών τεμαχίων της τριπλής χειραψίας; **0**
2.15) Ποια είναι η μέγιστη τιμή που μπορεί να λάβουν οι αριθμοί σειράς και επιβεβαίωσης;
Η μέγιστη τιμή είναι 2^{32}-1 αφού το κάθε πεδίου αποτελείται από 32 bits.
2.16) Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια TCP για την τριπλή χειραψία. Ποια η σύνταξή του; **tcp.port == 21 and (tcp.flags.syn == 1 or (tcp.ack == 1 and tcp.seq == 1 and tcp.len == 0))**
2.17) Προσδιορίστε το μέγεθος του παραθύρου λήψης που ανακοινώνει ο υπολογιστής σας κατά τη διάρκεια της τριπλής χειραψίας στις συνδέσεις ελέγχου και δεδομένων FTP. **64240 bytes**
2.18) Ποιο είναι το αντίστοιχο μέγεθος παραθύρου λήψης που ανακοινώνει ο εξυπηρετητής; **65535 bytes**
2.19) Σε ποιο πεδίο της επικεφαλίδας μεταφέρεται η σχετική πληροφορία; **Window size value**
2.20) Ποια τιμή κλίμακας παραθύρου (window scale) ανακοινώνουν οι δύο πλευρές σε κάθε σύνδεση;
Ο υπολογιστής μας ανακοινώνει κλίμακα 7 ενώ ο εξυπηρετητής ανακοινώνει 6.
2.21) Σε ποιο πεδίο της επικεφαλίδας μεταφέρεται η σχετική πληροφορία; **TCP Option (Window Scale)**
2.22) Ποια τιμή MSS ανακοινώνει ο υπολογιστής σας κατά την εγκατάσταση της σύνδεσης ελέγχου FTP. **1460 bytes**
2.23) Πώς προκύπτει η παραπάνω τιμή από την MTU της διεπαφής του υπολογιστή σας; **MSS = MTU – 40 (bytes)**
2.24) Σε ποιο πεδίο της επικεφαλίδας TCP μεταφέρεται η τιμή του MSS; TCP **Option (Maximum Segment Size)**
2.25) Ποια τιμή του MSS ανακοινώνει ο edu-dy.cn.ntua.gr. **536 bytes**
2.26) Πώς προκύπτει αυτή από την MTU (576 byte) της διεπαφής του edu-dy.cn.ntua.gr; **MSS = MTU – 40 (bytes)**
2.27) Ποιο είναι το μέγεθος του μεγαλύτερου τεμαχίου TCP που μπορεί να στείλει ο υπολογιστής σας προς τον εξυπηρετητή στη σύνδεση που εγκαταστάθηκε κατά την τριπλή χειραψία TCP στη θύρα ελέγχου του FTP;
536 bytes (δεν περιλαμβάνεται η επικεφαλίδα TCP).

Απόλυση σύνδεσης
Εντοπίζουμε τα τεμάχια TCP που σχετίζονται με την απόλυση της σύνδεσης ελέγχου FTP.
2.28) Ποια σημαία μήκους 1 bit ενεργοποιείται για την εκκίνηση της απόλυσης της σύνδεσης TCP; **FIN (και ACK)**
2.29) Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια TCP που φέρουν τη σημαία αυτή.
Ποια η σύνταξή του; **tcp.flags.fin == 1**
2.30) Ποια πλευρά εκκινεί τη διαδικασία απόλυσης; **Ο εξυπηρετητής ftp**
2.31) Πόσα τεμάχια TCP ανταλλάσσονται συνολικά; **2 (με σημαία FIN)**
2.32) Ποιο είναι το μέγεθος των επικεφαλίδων TCP των τεμαχίων αυτών; **32 bytes**
2.33) Ποιο είναι το μέγεθος δεδομένων των τεμαχίων αυτών; **0**
2.34) Δικαιολογήστε το μήκος του πακέτου IPv4 που μεταφέρει το τεμάχιο TCP με το οποίο απολύει τη σύνδεση ο υπολογιστής σας. **Έχουμε IP.total_length = 52 bytes, όμως IP.total_length = IP.header_length+TCP.header_length, ενώ IP.header_length = 20 bytes και TCP.header_length = 32 bytes.**
2.35) Δικαιολογήστε το μήκος του πακέτου IPv4 που μεταφέρει το αντίστοιχο τεμάχιο TCP από τον edu-dy.cn.ntua.gr. **Έχουμε IP.total_length = 52 bytes, όμως IP.total_length = IP.header_length+TCP.header_length, ενώ IP.header_length = 20 bytes και TCP.header_length = 32 bytes.**
2.36) Πόσα byte μεταδόθηκαν συνολικά στη σύνδεση ελέγχου FTP από κάθε πλευρά; **398 bytes από την πλευρά του υπολογιστή μας και 88 bytes από την πλευρά του εξυπηρετητή ftp.**
2.37) Με ποιο τρόπο προσδιορίσατε το πλήθος τους; **Από το πεδίο Sequence Number.**

Μεταφορά δεδομένων
Εφαρμόζουμε νέο φίλτρο απεικόνισης της μορφής tcp.port ώστε να παραμείνουν μόνο τα τεμάχια TCP που σχετίζονται με τη θύρα δεδομένων FTP.
2.38) Ποια είναι η σύνταξή του φίλτρου αυτού; **tcp.port == 49035**
2.39) Ποια τιμή του MSS ανακοινώνει η κάθε πλευρά κατά την τριπλή χειραψία TCP στη θύρα δεδομένων FTP;
Ο υπολογιστής μας: 1460 bytes, ο εξυπηρετητής ftp: 536 bytes

2.40) Ποιο είναι το μέγεθος του μεγαλύτερου τεμαχίου TCP που μπορεί να στείλει ο εξυπηρετητής προς τον υπολογιστή σας στη σύνδεση που εγκαταστάθηκε κατά την τριπλή χειραψία TCP στη θύρα δεδομένων του FTP; **1460 bytes (δεν περιλαμβάνεται η επικεφαλίδα TCP).**
2.41) Ποια είναι η τιμή του RTT (Round Trip Time) όπως αυτή προκύπτει από την ανταλλαγή των δύο πρώτων τεμαχίων της τριπλής χειραψίας; **Περίπου 0.01 seconds**
2.42) Ο υπολογιστής σας στέλνει επιβεβαιώσεις για κάθε τεμάχιο TCP που λαμβάνει; **Ναι (περίπου)**
2.43) Εφαρμόστε φίλτρο ώστε να παραμείνουν μόνο τεμάχια της σύνδεσης δεδομένων TCP με πηγή τον εξυπηρετητή. Πόσα τεμάχια με δεδομένα έστειλε ο εξυπηρετητής; **27**
2.44) Εφαρμόστε φίλτρο ώστε να παραμείνουν μόνο τεμάχια της σύνδεσης δεδομένων TCP με προορισμό τον εξυπηρετητή. Πόσα τεμάχια ACK έστειλε ο υπολογιστής σας για τα δεδομένα που έλαβε; **25**
2.45) Ποια τιμή παραθύρου (window) ανακοινώνει ο υπολογιστής σας στο πρώτο μετά την τριπλή χειραψία τεμάχιο ACK; **482 bytes**
2.46) Είναι ίδια με αυτή που προσδιορίσατε προηγουμένως στην ερώτηση 2.17; Εάν όχι, πώς προκύπτει;
Όχι, το MSS αλλάζει ανάλογα με τη διαθέσιμη μνήμη του υπολογιστή μας την εκάστοτε χρονική στιγμή.
2.47) Αλλάζει η τιμή του παραθύρου καθώς προχωρά η μεταφορά του αρχείου; Ποια είναι η μικρότερη τιμή που παρατηρήσατε; **Ναι αλλάζει. Η μικρότερη τιμή που παρατηρείται είναι 392 bytes.**
2.48) Εάν ο υπολογιστής σας ανακοίνωνε μηδενική τιμή για το παράθυρο, τι θα έκανε ο εξυπηρετητής;
Ο εξυπηρετητής θα σταματούσε να στέλνει δεδομένα. Όταν ο client στείλει τεμάχιο TCP Window Update θα συνεχιστεί η ροή δεδομένων από τον σέρβερ προς τον υπολογιστή μας.

Εφαρμόζουμε φίλτρο απεικόνισης ftp-data ώστε να εμφανίζονται μόνο τα τεμάχια TCP που αφορούν μεταφορά δεδομένων FTP και επιλέγουμε το πρώτο που στέλνει ο edu-dy.cn.ntua.gr.
2.49) Να καταγραφεί το μέγεθος πλαισίου (frame) σε byte και το μήκος των επικεφαλίδων Ethernet, IP και TCP.
Μήκος πλαισίου: 2686 bytes, Μήκος επικεφαλίδας Ethernet: 14 bytes, IP: 20 bytes, TCP: 32 bytes
2.50) Είναι το μέγεθος των δεδομένων του τεμαχίου TCP το αναμενόμενο βάσει της τιμής του ερωτήματος 2.40; **Όχι**
2.51) Εάν για κάποιο λόγο έπρεπε ο εξυπηρετητής να αποστείλει δεδομένα μεγαλύτερα από την τιμή που βρήκατε πριν, τι θα συνέβαινε; **Θα προτιμούσε να γίνει ο τεμαχισμός στην πηγή και όχι σε ενδιάμεσο κόμβο.**
2.52) Πόσα byte δεδομένων μεταδόθηκαν συνολικά στη σύνδεση δεδομένων από κάθε πλευρά;
Από την πλευρά του υπολογιστή μας 0, από την πλευρά του server 61442 bytes.
2.53) Ποιος ήταν ο ρυθμός μεταφοράς δεδομένων σε kbyte/sec από τον εξυπηρετητή στο PC σας; **περίπου 3127kb/sec**
2.54) Υπήρξαν αναμεταδόσεις τεμαχίων κατά τη μεταφορά δεδομένων; Εάν ναι, πώς το αντιληφτήκατε; **Όχι**

Άσκηση 3: Αποφυγή συμφόρησης στο TCP

3.1) Ανοίξτε το αρχείο pcattcp.pcap στο Wireshark και εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια TCP που σχετίζονται με τη θύρα δεδομένων FTP. Ποια η σύνταξή του; **tcp.port == 20**
3.2) Εντοπίστε τα τεμάχια της τριπλής χειραψίας. Ποια η διεύθυνση IPv4 του υπολογιστή που κατέβασε το αρχείο PCATTCP.exe; **94.65.141.44**
3.3) Ποιο είναι το RTT της σύνδεσης όπως προκύπτει από την ανταλλαγή των δύο πρώτων τεμαχίων της τριπλής χειραψίας; Συγκρίνετε με αυτήν που βρήκατε προηγουμένως στο ερώτημα 2.41. **Περίπου 0.014626 seconds. Παρατηρούμε ότι οι δύο τιμές ταυτίζονται.**
3.4) Παρατηρώντας προσεκτικά το διάγραμμα, τι συμπεραίνετε σχετικά με τον τρόπο που στέλνονται τα τεμάχια TCP από τον edu-dy.cn.ntua.gr; Παρατηρούμε ότι τα τεμάχια που στέλνονται κάθε φορά διπλασιάζονται (περίπου).
3.5) Πόσα τεμάχια έστειλε ο edu-dy.cn.ntua.gr στο πρώτο RTT; Είναι το πλήθος τους σύμφωνο με ότι προβλέπει το RFC 5681 στην παρ. 3.1;
Έστειλε 4 τεμάχια. Το πλήθος αυτό είναι σύμφωνο με τό RFC 5681 αφού έχουμε MSS = 536 bytes.

3.6) Πόσα τεμάχια έστειλε κατά το δεύτερο, τρίτο και τέταρτο RTT; **6, 10 και 16**
3.7) Δείτε το αντίστοιχο διάγραμμα για την κίνηση από την άλλη πλευρά κάνοντας κλικ στο Switch Direction. Πόσα ACK στάλθηκαν στο πρώτο, δεύτερο και τρίτο RTT; Τι παρατηρείτε σε σχέση με την απάντησή σας στο προηγούμενο ερώτημα; **1, 2, 3 Παρατηρούμε ότι αφενός στέλνονται όλα τα ACK τεμάχια μαζί και αφετέρου δεν έχουμε ένα ACK τεμάχιο για κάθε τεμάχιο που στέλνεται. Αυτό συμβαίνει για λόγους βελτιστοποίησης.**
3.8) Στη δική σας καταγραφή επιλέξτε το πρώτο τεμάχιο δεδομένων FTP από τον edu-dy.cn.ntua.gr και εμφανίστε το αντίστοιχο διάγραμμα αριθμών σειράς συναρτήσει του χρόνου από το edu- dy.cn.ntua.gr προς τον υπολογιστή σας. Είναι παρόμοιο με αυτό του αρχείου που κατεβάσατε; Συγκρίνετε με τις απαντήσεις στα προηγούμενα ερωτήματα; **Ναι είναι παρόμοιο ωστόσο δεν παρατηρείται μεγάλη αύξηση του αριθμού των τεμαχίων που στέλνονται κάθε φορά.**

Άσκηση 4: Μετάδοση δεδομένων με UDP

Με τη βοήθεια του Wireshark καταγράφουμε την κίνηση ενώ κάνουμε χρήση της υπηρεσίας DNS. Εφαρμόζουμε φίλτρο σύλληψης για να παρατηρούμε μόνο κίνηση του πρωτοκόλλου UDP και ξεκινάμε την καταγραφή. Ανοίγουμε ένα παράθυρο εντολών και καθαρίζουμε την προσωρινή μνήμη DNS (DNS cache) που διατηρεί ο υπολογιστής. Στη συνέχεια τρέχουμε το πρόγραμμα host σε περιβάλλον Unix, για να ζητήσουμε τη διεύθυνση IP του edu-dy.cn.ntua.gr.
4.1) Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε; **udp**
Παρατηρούμε το πρώτο δεδομενόγραμμα UDP που αποστάλθηκε από τον υπολογιστή μας.
4.2) Καταγράψτε τα ονόματα και το μήκος των πεδίων της επικεφαλίδας δεδομενογράμματος UDP.
Source Port(2 bytes), Destination Port(2 bytes), Length(2 bytes), Checksum(2 bytes)
4.3) Ποιο είναι το συνολικό μέγεθος της επικεφαλίδας UDP; **8 bytes**
4.4) Ποιο είναι το μήκος του συγκεκριμένου δεδομενογράμματος βάσει του μεγέθους του πακέτου IPv4 ή IPv6 εντός του οποίου ενθυλακώνεται; **425 bytes**
4.5) Τι εκφράζει το πεδίο μήκος (Length) της επικεφαλίδας UDP; **Το μήκος σε bytes του UDP header και των ενθυλακωμένων δεδομένων.**
4.6) Ποια είναι η ελάχιστη τιμή του πεδίου μήκους της επικεφαλίδας UDP; **8**
4.7) Ποιο είναι το ελάχιστο και ποιο το μέγιστο μέγεθος μηνύματος που μπορεί να μεταφερθεί από ένα πακέτο IPv4 χρησιμοποιώντας το πρωτόκολλο UDP; Αιτιολογήστε την απάντησή σας.
Το ελάχιστο είναι 0 καθώς το τεμάχιο UDP μπορεί να μην φέρει καθόλου δεδομένα.
Το μέγιστο είναι 0xFFFF δηλαδή 65535 bytes (πλην της επικεφαλίδας UDP και IP) αφού το πεδίο length του IP πρωτοκόλλου είναι 2 bytes. Άρα max = 65507bytes.
4.8) Δοθέντος ότι όλοι οι κόμβοι στο διαδίκτυο οφείλουν να δέχονται πακέτα IPv4 μεγέθους μέχρι 576 byte (θρυμματισμένα ή μη), ποιο είναι το μέγιστο μέγεθος μηνύματος που μπορεί να σταλεί και παραληφθεί με βεβαιότητα χρησιμοποιώντας το πρωτόκολλο UDP. **556 bytes**
4.9) Παρατηρήσατε στην καταγραφή σας να μεταφέρονται με δεδομενογράμματα UDP μηνύματα άλλων πλην του DNS πρωτοκόλλων; Εάν ναι, για ποια πρωτόκολλα πρόκειται; **DNS/MDNS**
Εφαρμόζουμε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο μηνύματα DNS.
4.10) Ποια είναι η σύνταξη του φίλτρου απεικόνισης που χρησιμοποιήσατε; **dns**
4.11) Ποια είναι η διεύθυνση IPv4 ή IPv6 του εξυπηρετητή DNS που απάντησε στην ερώτηση για τη διεύθυνση του edu-dy.cn.ntua.gr; **147.102.238.203**
4.12) Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν για ερώτηση (query) στον εξυπηρετητή DNS. **Source Port: 51762, Destination Port: 53**
4.13) Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν στην απόκριση (response) του εξυπηρετητή DNS. **Source Port: 53, Destination Port: 51762**
4.14) Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS; **Θύρα 53**