Δίκτυα Υπολογιστών
Εργαστηριακή Άσκηση 7

Ονοματεπώνυμο: Κυριακόπουλος Γεώργιος – el18153
Ομάδα: 4
Όνομα PC/ΛΣ: George – Windows 10 Pro, 21H1
Ημερομηνία: 06/12/2021
Διεύθυνση IP: 192.168.1.7
Διεύθυνση MAC: 60-A4-B7-75-72-0F

Άσκηση 1:

1.1.
Χρησιμοποίησα το φίλτρο σύλληψης *ip and host 192.168.1.7.*

1.2.
Χρησιμοποίησα το φίλτρο απεικόνισης *ip.dst == 1.1.1.1 or ip.dst == 2.2.2.2 or ip.dst == 147.102.40.1.*

1.3.
Ο υπολογιστής μου προσπαθεί να συνδεθεί στη θύρα 23, η οποία είναι μία θύρα που χρησιμοποιείται συνήθως για το πρωτόκολλο Telnet.

1.4.
Χρησιμοποίησα το φίλτρο απεικόνισης *tcp.port == 23.*

1.5.
Η σημαία SYN μήκους 1 bit ενεργοποιείται για την εκκίνηση της εγκατάστασης της σύνδεσης TCP.

1.6.
Και για τις δύο περιπτώσεις κάνει 5 προσπάθειες να εγκαταστήσει σύνδεση TCP.

1.7.
Οι χρονικές αποστάσεις είναι με τη σειρά 1, 2, 4 και 8 δευτερόλεπτα και για τις δύο περιπτώσεις.

1.8.
Οι χρονικές αποστάσεις είναι ίδιες και στις 2 περιπτώσεις, και μάλιστα φαίνεται να ακολουθούν μία τακτική διπλασιασμού του χρόνου κάθε φορά.

1.9.
Το μόνο βήμα που φαίνεται είναι το πρώτο βήμα της τριπλής χειραψίας, όπου ο υπολογιστής μου στέλνει αίτημα εγκατάστασης της σύνδεσης με χρήση της σημαίας SYN.

1.10.
Ο υπολογιστής μου απλώς εγκαταλείπει την προσπάθεια, αφού δε φαίνεται κάπου να υπάρχει απόλυση της σύνδεσης με χρήση της FIN σημαίας.

1.11.
Χρησιμοποίησα το φίλτρο απεικόνισης *tcp.port == 23 and ip.addr == 147.102.40.1.*

1.12.
Πάλι γίνονται 5 προσπάθειες εγκατάστασης σύνδεσης από τον υπολογιστή μου.

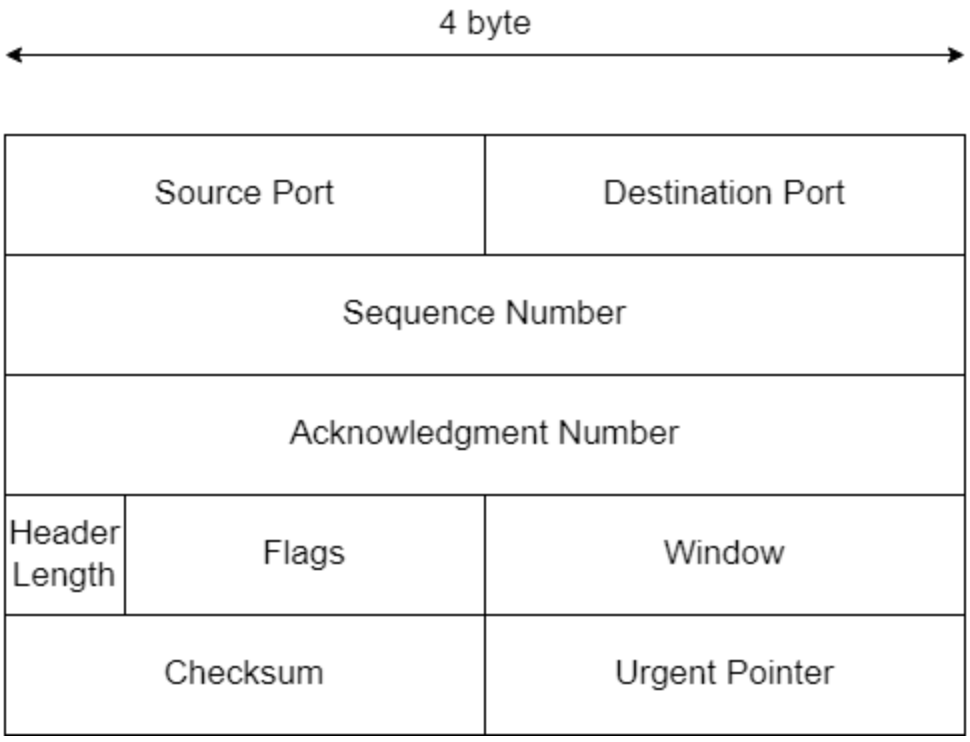
1.13.
Αυτή τη φορά, μετά από κάθε μήνυμα απάντησης από τον 147.102.40.1 με RST, δηλαδή απόρριψη σύνδεσης, ο υπολογιστής μου προσπαθεί πάλι μετά από 0.5 δευτερόλεπτο να εγκαταστήσει σύνδεση.

1.14.
Το μήνυμα απόρριψης της σύνδεσης από τον 147.102.40.1 περιλαμβάνει τις σημαίες μήκους 1 bit RST και ACK.

1.15.
Η σημαία RST είναι αυτή που δηλώνει την απόρριψη της σύνδεσης για την οποία αιτήθηκε ο υπολογιστής μου.

1.16.
Η επικεφαλίδα αυτού του τεμαχίου TCP έχει μέγεθος 20 bytes και το πεδίο δεδομένων έχει μήκος 0 bytes.

1.17.
Τα πεδία της επικεφαλίδας του τεμαχίου TCP είναι τα εξής (με το αντίστοιχο μέγεθος σε bytes): Source Port (2), Destination Port (2), Sequence Number (4), Acknowledgment Number (4), Header Length (4 bit), Flags (12 bit), Window (2), Checksum (2), Urgent Pointer (2). Οι θέσεις τους φαίνονται και στο παρακάτω σχήμα:



1.18.
Το πεδίο Data Offset είναι αυτό που μας δείχνει το μέγεθος της επικεφαλίδας σε λέξεις των 4 byte. Στο Wireshark, το πεδίο αυτό έχει όνομα Header Length.

1.19.
Προκύπτει ως λέξεις των 4 byte, δηλαδή μια δεκαεξαδική τιμή 5 (0x5) σημαίνει 5*4 byte = 20 byte μέγεθος επικεφαλίδας.

1.20.
Όχι, δεν υπάρχει πεδίο στην επικεφαλίδα TCP για το μήκος του τεμαχίου.

1.21.
Παίρνουμε από την επικεφαλίδα IPv4 το πεδίο Total Length (πχ. 40 byte) και αφαιρούμε από αυτό το μήκος της επικεφαλίδας IPv4, δηλαδή το πεδίο Header Length (πχ. τιμή 5 άρα 20 byte). Αυτό που προκύπτει είναι το μήκος του τεμαχίου TCP (πχ. 20 byte), στα οποία περιλαμβάνεται και η επικεφαλίδα TCP (στην περίπτωση αυτή είναι και τα 20 byte της επικεφαλίδας).

1.22.
Το μήκος του πρώτου TCP τεμαχίου που στέλνει ο υπολογιστής μου είναι 32 byte.

1.23.
Ναι, υπάρχει μια διαφορά 12 byte, η οποία οφείλεται στο πεδίο Options που βρίσκεται στο τέλος του τεμαχίου και περιέχει πληροφορίες και επιλογές για την εγκατάσταση της σύνδεσης.

Άσκηση 2:

2.1.
Χρησιμοποίησα το φίλτρο σύλληψης *tcp and host edu-dy.cn.ntua.gr.*

2.2.
Ο υπολογιστής μου προσπαθεί να συνδεθεί στη θύρα 21 για να αρχίσει η επικοινωνία με τον εξυπηρετητή FTP, η οποία είναι συνήθως η θύρα ελέγχου FTP.

2.3.
Η σύνδεση για τη μεταφορά δεδομένων γίνεται με τη θύρα 20 του υπολογιστή edu-dy.cn.ntua.gr.

2.4.
Χρησιμοποίησα το φίλτρο απεικόνισης *tcp.port == 21.*

2.5.
Ανταλλάσσονται 3 τεμάχια TCP για την εγκατάσταση της σύνδεσης ελέγχου FTP, τα γνωστά της τριπλής χειραψίας.

2.6.
Χρησιμοποιούνται οι σημαίες SYN και ACK (SYN/SYN, ACK/ACK) για την εγκατάσταση της σύνδεσης TCP.

2.7.
Το μέγεθος των επικεφαλίδων TCP των 3 αυτών τεμαχίων είναι 32, 32 και 20 bytes με τη σειρά.

2.8.
Και τα 3 αυτά τεμάχια TCP μεταφέρουν 0 byte δεδομένων.

2.9.
Το τρίτο τεμάχιο της τριπλής χειραψίας καταγράφεται 0.007819 δευτερόλεπτα μετά το πρώτο, που είναι και η διάρκεια που ψάχνουμε.

2.10.
Ναι, εμφανίζει ακριβώς την ίδια τιμή, δηλαδή 0.007819 δευτερόλεπτα.

2.11.
Ο υπολογιστής μου ανακοινώνει ως αρχικό Sequence Number τον 2407081074 (0x8f792472), ενώ ο εξυπηρετητής TCP ανακοινώνει ως αρχικό τον 2099936444 (0x7d2a7cbc).

2.12.
Ο Acknowledgment Number του τεμαχίου TCP με το οποίο ο εξυπηρετητής FTP δηλώνει την αποδοχή της σύνδεσης προκύπτει από τον αρχικό Sequence Number του υπολογιστή μου αυξημένο κατά ένα.

2.13.
Ο Sequence Number του τελευταίου τεμαχίου της τριπλής χειραψίας προκύπτει ως ο Acknowledgment Number του δεύτερου ή ο Sequence Number του πρώτου αυξημένος κατά ένα. Αντίστοιχα, ο Acknowledgment Number του τελευταίου τεμαχίου προκύπτει ως ο Sequence Number του δεύτερου αυξημένος κατά ένα.

2.14.
Και τα τρία τεμάχια της τριπλής χειραψίας μεταφέρουν 0 byte δεδομένων.

2.15.
Τα πεδία Sequence Number και Acknowledgment Number καταλαμβάνουν χώρο 4 byte (32 bit) το καθένα, επομένως η μέγιστη τιμή που μπορούν να λάβουν είναι 4294967295 ($2^{32} - 1$), θεωρώντας μη-προσημασμένη απεικόνιση.

2.16.
Χρησιμοποίησα το φίλτρο απεικόνισης *tcp.flags.syn == 1 or (tcp.flags.ack == 1 and tcp.len == 0 and ((tcp.seq_raw == 2407081075 and tcp.ack_raw == 2099936445) or (tcp.seq_raw == 4178468175 and tcp.ack_raw == 3748823843)))*. Ουσιαστικά θέλω είτε να είναι ενεργοποιημένη η σημαία SYN, είτε να είναι ενεργοποιημένη η ACK μαζί με μηδενικό μήκος δεδομένων και μαζί με κατάλληλους αριθμούς σειράς και επιβεβαίωσης, ώστε να εμφανίζονται και τα τελευταία τεμάχια από τις τριπλές χειραψίες.

2.17.
Ο υπολογιστής μου ανακοινώνει παράθυρο λήψης μεγέθους 8192 byte, ενώ ο εξυπηρετητής ανακοινώνει παράθυρο λήψης μεγέθους 65535 byte.

2.18.
Η πληροφορία για το μέγεθος του παραθύρου λήψης μεταφέρεται στο πεδίο Window της επικεφαλίδας TCP.

2.19.
Το μικρότερο μέγεθος παραθύρου είναι τα 1030 byte ενώ το μεγαλύτερο είναι τα 65535 byte.

2.20.
Ο υπολογιστής μου ανακοινώνει τιμή 1460 για το MSS.

2.21.
Αυτή προκύπτει από την MTU του υπολογιστή μου (1500 byte) μείον 40 byte, 20 από την επικεφαλίδα TCP και 20 αφού χρησιμοποιείται πρωτόκολλο IPv4, επομένως, MSS ίσο με 1460.

2.22.
Η τιμή του MSS μεταφέρεται στο πεδίο Options της επικεφαλίδας TCP και μάλιστα στην επιλογή TCP Option – Maximum segment size.

2.23.
Ο edu-dy.cn.ntua.gr ανακοινώνει τιμή 536 για το MSS.

2.24.
Προκύπτει ομοίως με το πως προκύπτει η τιμή του MSS του υπολογιστή μου, δηλαδή από την τιμή του MTU (576 byte) μείον 40 byte(20 TCP Header, 20 IPv4 Header), άρα τελικά τιμή 536 για το MSS.

2.25.
Εάν πάρουμε το MSS του edu-dy.cn.ntua.gr (536 byte, που είναι και το ελάχιστο αποδεκτό) και προσθέσουμε τα 20 byte της επικεφαλίδας τότε προκύπτει το μέγεθος του μεγαλύτερου τεμαχίου TCP που μπορεί να στείλει ο υπολογιστής μου προς τον εξυπηρετητή, δηλαδή 556 byte.

2.26.
Η σημαία FIN ενεργοποιείται για να εκκινήσει η απόλυση της σύνδεσης TCP.

2.27.
Χρησιμοποίησα το φίλτρο απεικόνισης *tcp.flags.fin == 1.*

2.28.
Ο 147.102.40.15 είναι αυτός που εκκινεί την απόλυση της σύνδεσης TCP, καθώς πρώτα αυτός στέλνει TCP πακέτο με FIN σημαία από τη θύρα 21, αφού έχει προηγηθεί η ολοκλήρωση του κατεβάσματος του αρχείου και η απόλυση και εκείνης της σύνδεσης με τη θύρα δεδομένων FTP (θύρα 20).

2.29.
Φαίνονται 4 τεμάχια να ανταλλάσσονται, που έχουν τη σημαία FIN ενεργοποιημένη. Ωστόσο από αυτά, το πρώτο τεμάχιο σηματοδοτεί το τέλος του κατεβάσματος του αρχείου PCATTCP.exe και την απόλυση της σύνδεσης με τη θύρα δεδομένων FTP σε συνδυασμό με το δεύτερο, ενώ τα υπόλοιπα 2 είναι αυτά που ουσιαστικά απολύουν τη σύνδεση TCP. Φυσικά, υπάρχουν εξίσου άλλα 4 τεμάχια με σημαία ACK ως απάντηση σε κάθε ένα από αυτά, αλλά δεν εμφανίζονται, αφού έχω φίλτρο απεικόνισης για τη FIN σημαία. Επομένως, συνολικά είναι 4 τα σχετικά με την απόλυση της σύνδεσης TCP.

2.30.
Και τα 4 αυτά τεμάχια έχουν μήκος επικεφαλίδας ίσο με 20 byte.

2.31.
Το πρώτο εξ’ αυτών με σημαία FIN έχει μήκος δεδομένων 336 byte, καθώς μεταφέρει τα τελευταία δεδομένα του αρχείου PCATTCP.exe που κατεβάζει ο υπολογιστής μου. Τα υπόλοιπα 3 με σημαία FIN έχουν μήκος δεδομένων ίσο με 0 byte.

2.32.
Το πακέτο IPv4 που μεταφέρει το τεμάχιο TCP με το οποίο απολύει τη σύνδεση ο υπολογιστής

μου έχει μήκος 40 bytes, εκ των οποίων τα 20 είναι το IPv4 Header και τα άλλα 20 είναι το TCP Header με 0 bytes δεδομένων.

2.33.
Το πακέτο IPv4 που μεταφέρει το αντίστοιχο τεμάχιο TCP από τον edu-dy.cn.ntua.gr έχει και αυτό μήκος 40 bytes, εκ των οποίων τα 20 είναι το IPv4 Header και τα άλλα 20 είναι το TCP Header με 0 bytes δεδομένων και εδώ.

2.34.
Από την πλευρά του edu-dy.cn.ntua.gr στάλθηκαν 375 byte δεδομένων, ενώ από την πλευρά του υπολογιστή μου στάλθηκαν 117 byte δεδομένων.

2.35.
Το πλήθος των byte που στάλθηκαν από κάθε πλευρά βρέθηκε παρατηρώντας το Relative Sequence Number του τελευταίου απεσταλμένου πακέτου από κάθε πλευρά, δεδομένου ότι το Sequence Number (και επομένως και το Relative Sequence Number) αυξάνεται κάθε φορά ανάλογα με το πόσα byte έχουν σταλεί.

2.36.
Χρησιμοποίησα το φίλτρο απεικόνισης *tcp.port == 20.*

2.37.
Ο υπολογιστής μου ανακοινώνει την τιμή 1460 για το MSS, ενώ ο edu-dy.cn.ntua.gr ανακοινώνει την τιμή 536 για το MSS.

2.38.
Εάν πάρουμε το MSS του υπολογιστή μου (1460 byte) και προσθέσουμε τα 20 byte της επικεφαλίδας τότε προκύπτει το μέγεθος του μεγαλύτερου τεμαχίου TCP που μπορεί να στείλει ο εξυπηρετητής προς τον υπολογιστή μου, δηλαδή 1480 byte. Ωστόσο, πολλές φορές, παρά τη δήλωση ενός MSS, επιλέγεται μικρότερη τιμή, η οποία να βοηθάει στο να αποφευχθούν τυχόν θρυμματισμοί ή άλλες καθυστερήσεις κατά τη μετάδοση των πακέτων σε οποιοδήποτε από τα δύο άκρα της σύνδεσης. Επομένως, γνωρίζοντας ότι ο edu-dy.cn.ntua.gr έχει MSS ίσο με 536 και παρά τη γνωστοποίηση του MSS του υπολογιστή μου (1460), ο edu-dy.cn.ntua.gr διαλέγει να στέλνει πακέτα με βάση το δικό του MSS (δεδομένου και του MTU της διεπαφής του), άρα το μέγεθος του μεγαλύτερου τεμαχίου TPC είναι και πάλι τα 536 + 20 = 556 byte.

2.39.
Η τιμή του RTT είναι 0.000218 δευτερόλεπτα, όπως προκύπτει από την ανταλλαγή των δύο πρώτων τεμαχίων της τριπλής χειραψίας.

2.40.
Όχι, δεν στέλνει πάντα επιβεβαιώσεις για κάθε τεμάχιο TCP που λαμβάνει. Το πιο σύνηθες είναι να στέλνει ανά 2 τεμάχια TCP, αλλά υπήρξαν φορές που έστειλε ανά ένα ή ανά τρία τεμάχια TCP.

2.41.
Η τιμή στο πεδίο Window αλλάζει από 65535 byte σε 512 και στο τέλος σε 511, όμως αλλάζει και το window size scaling factor από 1 σε 256, επομένως και το calculated window size από 65535 byte σε 131072 και τέλος σε 130816.

2.42.
Το μέγεθος του πλαισίου είναι 590 byte, το μέγεθος της επικεφαλίδας Ethernet 14 byte, της IP 20 byte και της TCP 20 byte.

2.43.
Ναι, το μέγεθος των δεδομένων είναι 536 byte, ίσο με το MSS του edu-dy.cn.ntua.gr, αλλά όχι ίσο με το μεγαλύτερο 1460 MSS του υπολογιστή μου, καθώς μάλλον συνέβη ένα συμβιβασμός σαν αυτόν που περιγράφεται στο 2.38.

2.44.
Εάν το μήκος των δεδομένων ξεπερνάει την προηγούμενη συμφωνημένη τιμή, θα χρειαζόταν να γίνει Source Fragmentation, δηλαδή να πραγματοποιηθεί θρυμματισμός στην πηγή (τον edu-dy.cn.ntua.gr) και μετά να αποσταλούν τα δεδομένα προς τον υπολογιστή μου.

2.45.
Από τον edu-dy.cn.ntua.gr μεταδόθηκαν συνολικά 61440 byte (Acknowledgement Number τελευταίου πακέτου ίσο με 61442 από όπου αφαιρούμε 2 αυξήσεις, λόγω του SYN της σύνδεσης και του FIN της αποσύνδεσης), ενώ από τον υπολογιστή μου 0 byte (Acknowledgment Number τελευταίου πακέτου ίσο με 2, από όπου αφαιρούμε 2 αυξήσεις, λόγω του SYN της σύνδεσης και του FIN της αποσύνδεσης).

2.46.
Ο ρυθμός μεταφοράς δεδομένων σε Kbyte/sec από τον εξυπηρετητή στον υπολογιστή μου ήταν 3233.68Kbytes/sec.

2.47.
Δεν παρατήρησα κάποια αναμετάδοση τεμαχίων κατά τη μεταφορά δεδομένων.

Άσκηση 3:

3.1.
Χρησιμοποίησα το φίλτρο απεικόνισης *tcp.port == 20.*

3.2.
Η διεύθυνση του υπολογιστή που κατέβασε το αρχείο PCATTCP.exe είναι η 94.65.141.44.

3.3.
Το RTT της σύνδεσης είναι ίσο με 0.014626 δευτερόλεπτα, μεγαλύτερο από τα 0.000218 δευτερόλεπτα που είχα υπολογίσει στο 2.39.

3.4.
Ουσιαστικά βλέπουμε ότι η αποστολή ξεκινάει με 1 τεμάχιο και αυξάνεται σταδιακά, ενώ οι αποστολές αυτές έχουν ένα περίπου σταθερό χρονικό διάστημα ανάμεσα τους, όπου ο edu-dy.cn.ntua.gr περιμένει το ACK από τον 94.65.141.44.

3.5.
Στο πρώτο RTT έστειλε 4 τεμάχια. Το πλήθος αυτό είναι σύμφωνο με ότι προβλέπει το RFC 5681 σχετικά με το slow start, καθώς σύμφωνα με αυτό το SMSS είναι 536, άρα το initial window τίθεται στα 4 * 536 = 2144 byte και το όριο των τεμαχίων στα το πολύ 4 τεμάχια.

3.6.
Στο δεύτερο RTT έστειλε 6 τεμάχια, ενώ στο τρίτο RTT έστειλε 10. Το congestion window είχε μεγαλώσει (αρχικά ήταν 4), με κάθε ένα εκ των ACK που έστειλε ο 94.65.141.44 πίσω, επιτρέποντας στον edu-dy.cn.ntua.gr να στείλει περισσότερα τεμάχια μαζί.

3.7.
Το διάγραμμα είναι παρόμοιο με του αρχείου που κατέβασα. Ωστόσο παρατηρώ ότι υπήρχε αρκετά μεγαλύτερο initial window, καθώς στάλθηκαν 10, 19 και 34 τεμάχια στο πρώτο, δεύτερο και τρίτο RTT αντίστοιχα. Επίσης, το congestion window μεγαλώνει με παρόμοιο τρόπο, με κάθε ένα εκ των ACK που έστελνε ο υπολογιστής μου πίσω, επιτρέποντας στον edu-dy.cn.ntua.gr να στείλει περισσότερα τεμάχια μαζί.

Άσκηση 4:

4.1.
Χρησιμοποίησα το φίλτρο σύλληψης *udp.*

4.2.
Τα ονόματα των πεδίων της επικεφαλίδας δεδομενογράμματος UDP είναι τα εξής (με το μήκος σε byte): Source Port (2), Destination Port (2), Length (2), Checksum (2).

4.3.
Η επικεφαλίδα UDP έχει συνολικό μέγεθος 8 byte.

4.4.
Το πακέτο IPv4 έχει Total Length ίσο με 291 bytes, εκ των οποίων τα 20 είναι το IPv4 Header, άρα το δεδομενόγραμμα UDP έχει μήκος 271 bytes.

4.5.
Το πεδίο Length της επικεφαλίδας UDP εκφράζει το συνολικό μέγεθος του δεδομενογράμματος UDP (271), δηλαδή το μήκος της επικεφαλίδας (8) συν το μήκος των δεδομένων που μεταφέρει (263).

4.6.
Το ελάχιστο μέγεθος ενός δεδομενογράμματος UDP είναι τα 8 byte (δηλαδή επικεφαλίδα χωρίς δεδομένα), ενώ το μέγιστο είναι ίσο με το μέγιστο μέγεθος IPv4 πακέτου, δηλαδή 65535 byte, μείον τα 20 της επικεφαλίδας IPv4, επομένως 65515 byte.

4.7.
Το μέγιστο μήκος πακέτου UDP που μπορεί να μεταδοθεί με βεβαιότητα είναι ίσο με το ελάχιστο μέγεθος IPv4 πακέτου που μπορούν να διαχειριστούν όλοι οι κόμβοι (576) μείον το μέγιστο μέγεθος της επικεφαλίδα IPv4 (60), επομένως 516 byte.

4.8.
Όχι, δεν παρατήρησα τέτοια μηνύματα, εκτός των DNS πρωτοκόλλων.

4.9.
Χρησιμοποίησα το φίλτρο απεικόνισης *dns.*

4.10.
Η διεύθυνση IPv6 του εξυπηρετητή DNS που απάντησε στην ερώτηση για τη διεύθυνση του edu-dy.cn.ntua.gr είναι η fe80::1.

4.11.
Η θύρα προέλευσης της ερώτησης στον εξυπηρετητή DNS είναι η 64434, ενώ η θύρα προορισμού είναι η 53.

4.12.
Η θύρα προέλευσης της απάντησης του εξυπηρετητή DNS είναι η 53, ενώ η θύρα προορισμού είναι η 64434.

4.13.
Η θύρα 53 αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS.