Ονοματεπώνυμο: Ιωάννης Γιαννούκος		**Ομάδα:** 3
Όνομα PC/ΛΣ: JohnJohn / Windows 11		**Ημερομηνία:** 3/12/2022
Διεύθυνση IP: 147.102.201.222	**Διεύθυνση MAC:**	3C-6A-A7-9A-B3-CF

Εργαστηριακή Άσκηση 7
Πρωτόκολλα TCP και UDP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

Άσκηση 1

1.1) Φίλτρο σύλληψης: “host 147.102.201.222”

1.2) Φίλτρο απεικόνισης:
“ip.addr == 1.1.1.1 or ip.addr == 2.2.2.2 or ip.addr == 147.102.40.1”

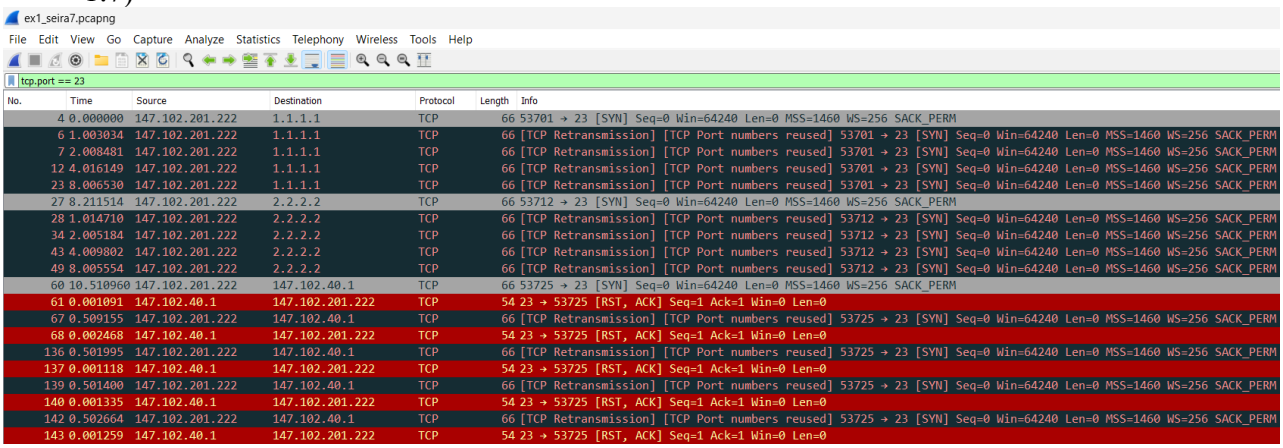
1.3) Ο υπολογιστής μου προσπαθεί να συνδεθεί με την θύρα 23.

1.4) Φίλτρο απεικόνισης: “tcp.port == 23”

1.5) Η σημαία “Syn”.

1.6) Για να εγκατασταθεί μια σύνδεση TCP καταβάλλονται 5 προσπάθειες από τον υπολογιστή μου.

1.7)



1.8) Το μόνο που αλλάζει στις περιπτώσεις Α και Β είναι η θύρα του υπολογιστή μου που χρησιμοποιείται για να σταλθούν τα πακέτα. Όλες οι υπόλοιπες πληροφορίες που φέρουν τα πακέτα είναι ίδιες.

1.9) Στις δύο πρώτες περιπτώσεις παρατήρησα μόνο το πρώτο βήμα της τριπλής χειραψίας, δηλαδή το " [SYN] Seq=0, Ack=0, Len=0 ".
Στην τελευταία περίπτωση, πραγματοποιήθηκε το πρώτο βήμα της τριπλής χειραψίας και το μήνυμα που έλαβα από τον 147.102.40.1 είναι το
" [RST, ACK] Seq=1, Ack=1, Len=0 ".

1.10) Εφόσον η διαδικασία της τριπλής χειραψίας δεν ολοκληρώθηκε σε καμία περίπτωση, ο υπολογιστής μου εγκατέλειψε την προσπάθεια και σταμάτησε να στέλνει πακέτα " [SYN] Seq=0, Ack=0, Len=0 "

1.11) Φίλτρο απεικόνισης: " ip.addr == 147.102.40.1 and tcp "

1.12) Ο υπολογιστής μου καταβάλλει 5 προσπάθειες.

1.13) Τα πακέτα TCP που στέλνονται από τον υπολογιστή μου εξακολουθούν να είναι πανομοιότυπα, με εξαίρεση την θύρα την οποία χρησιμοποιεί ο υπολογιστής μου για να στείλει τα πακέτα και η διεύθυνση προορισμού τους.

1.14) Τα τεμάχια αυτά περιλαμβάνουν τις εξής σημαίες: Reserved, Accurate ECN, Congestion Window Reduced, ECN-Echo, Urgent, Acknowledgement, Push, Reset, Syn και Fin.

1.15) Η σημαία Reset είναι αυτή που δηλώνει άρνηση εγκατάστασης σύνδεσης.

1.16) Το τεμάχιο αυτό έχει μέγεθος επικεφαλίδας 20 bytes και 0 bytes δεδομένων. Στην φάση της εγκατάστασης σύνδεσης στέλνονται πάντα πακέτα χωρίς δεδομένα.

1.17)

<table>
<tr><td colspan="2">Source Port
[2 bytes]</td><td>Destination Port
[2 bytes]</td></tr>
<tr><td colspan="3">Sequence Number
[4 bytes]</td></tr>
<tr><td colspan="3">Acknowledgement Number
[4 bytes]</td></tr>
<tr><td>Header Length
[½ byte]</td><td>Flags
[1½ bytes]</td><td>Window
[2 bytes]</td></tr>
<tr><td colspan="2">Checksum
[2 bytes]</td><td>Urgent Pointer
[2 bytes]</td></tr>
</table>

1.18) "Header Length"

1.19) Η τιμή του πεδίου "Header Length" είναι 5. Επομένως, το μήκος σε bytes του τεμαχίου είναι 4 φορές την τιμή του πεδίου "Header Length".

1.20) Όχι.

1.21) Αν αφαιρέσουμε από το πεδίο "Total Length" της επικεφαλίδας IPv4 την τιμή των πεδίων "Header Length" της επικεφαλίδας IPv4 και TCP, θα μπορέσουμε να υπολογίσουμε το μήκος των δεδομένων που αποστέλλονται.

1.22) 32 bytes.

1.23) Ναι, η διαφορά έχει μέγεθος 12 bytes. Αυτό οφείλεται στο πεδίο "Options" που περιέχεται στο πρώτο τεμάχιο TCP που στέλνει ο υπολογιστής μου.

Άσκηση 2 (IP: 147.102.239.119)

2.1) Φίλτρο σύλληψης: “ tcp and host 147.102.239.119 ”

2.2) Προσπαθεί να συνδεθεί στην θύρα 21.

2.3) Με την θύρα 20.

2.4) Φίλτρο απεικόνισης: “ tcp.port == 20 ”

2.5) Ανταλλάσσονται 8 τεμάχια για την διαδικασία login.

2.6) Οι σημαίες “ SYN “ και “ ACK “.

2.7) 32 bytes

2.8) 12 bytes

2.9) Διαρκεί 0.002076 secs.

2.10) Ναι, η τιμή του πεδίου iRTT περιγράφει αυτήν ακριβώς την πληροφορία.

2.11) Ο υπολογιστής μου: 2486393558
Ο edu-dy.cn.ntua.gr: 2865612216

2.12) Ο αριθμός ACK του τεμαχίου TCP που στέλνει ο εξυπηρετητής FTP δηλώνει το επόμενο τεμάχιο που είναι έτοιμος να λάβει, καθώς έχει επιτυχώς λάβει όλα τα προηγούμενα. Αφού, επομένως, έχει λάβει μόνο το πρώτο πακέτο με Seq = 0 (σχετικό), ο εξυπηρετητής ανακοινώνει στον υπολογιστή μου ότι είναι έτοιμος να λάβει το τεμάχιο με Seq = 1 θέτοντας το πεδίο Ack=1.

2.13) Ο εξυπηρετητής FTP έχει στείλει συνολικά 1 πακέτο μέχρι εκείνη την στιγμή με Seq=0. Έτσι, το επόμενο πακέτο που θα στείλει θα έχει Seq ίσο με τον επόμενο ακέραιο αριθμό, δηλαδή Seq = 1.
Επιπλέον, έχει λάβει επιτυχώς από τον υπολογιστή μου ένα πακέτο με Seq = 0, επομένως το πεδίο Ack θα έχει τιμή με τον επόμενο ακέραιο αριθμό, δηλαδή Ack = 1.

2.14) Κάθε ένα πακέτο που ανταλλάχθηκε στην περίοδο της τριπλής χειραψίας είχε μηδενικό μήκος δεδομένων (Len = 0).

2.15) Maximum Sequence Number: 4,294,967,295 (Hex: ff ff ff ff)
Maximum Acknowledgement Number: 4,294,967,295 (Hex: ff ff ff ff)

2.16) Φίλτρο απεικόνισης:
“ ((tcp.seq == 0) or (tcp.seq==1 and tcp.ack == 1)) and tcp.len == 0 ”.

2.17) Κατά την τριπλή χειραψία στην σύνδεση ελέγχου ο υπολογιστής μου ανακοινώνει παράθυρο Win = 8192, ενώ στη σύνδεση δεδομένων FTP ανακοινώνει Win = 65535.

2.18) Ο εξυπηρετητής ανακοινώνει παράθυρο μεγέθους Win = 65535.

2.19) Στο πεδίο “Window”.

2.20)
Κατά την διάρκεια της τριπλής χειραψίας στη σύνδεση ελέγχου:
Window scale του PC μου: 0 (multiply by 1)
Window scale του server: 6 (multiply by 64)
Κατά την διάρκεια της τριπλής χειραψίας στη σύνδεση δεδομένων FTP:
Window scale του PC μου: 8 (multiply by 256)
Window scale του server: 6 (multiply by 64)

2.21) Στο πεδίο TCP Option – Window scale.

2.22) Στο πεδίο “TCP Option – Maximum segment size” φαίνεται ότι ο υπολογιστής μου ανακοινώνει τιμή MSS = 1460 bytes.

2.23) Η MTU της διεπαφής του υπολογιστή μου έχει τιμή 1500 bytes. Επειδή χρησιμοποιούνται πακέτα IPv4, η τιμή της επικεφαλίδας του στρώματος δικτύου είναι 40bytes (IPv4). Επομένως, η τιμή MSS προκύπτει από την εξής σχέση:
$MSS = MTU - (\mu\acute{\eta}\kappa o\varsigma\ \varepsilon\pi\iota\kappa\varepsilon\phi\alpha\lambda\acute{\iota}\delta\alpha\varsigma\ IPv4)$

2.24) Φαίνεται στο πεδίο “TCP Option – Maximum segment size”.

2.25) 536bytes

2.26) Το πακέτο TCP θα μπορεί να έχει μέγιστη τιμή 536 bytes, επειδή η MTU της διεπαφής του edu-dy.cn.ntua.gr είναι 576 bytes και το πακέτο ενθυλακώνεται σε IPv4 πακέτο. Σημειώνεται ότι ισχύει η σχέση:
$MTU = MSS + (\mu\acute{\eta}\kappa o\varsigma\ \varepsilon\pi\iota\kappa\varepsilon\phi\alpha\lambda\acute{\iota}\delta\alpha\varsigma\ IPv4)$

2.27) 1460 bytes

2.28) Ενεργοποιείται η σημαία “Fin”.

2.29) Φίλτρο απεικόνισης: “tcp.flags.fin == 1”.

2.30) Ο εξυπηρετητής edu-dy.cn.ntua.gr. Στην ουσία, στέλνεται από τον υπολογιστή μου ένα αίτημα απόλυσης σύνδεσης στον εξυπηρετητή FTP και, αφού αυτός το λάβει και το εγκρίνει, ξεκινά την διαδικασία απόλυσης σύνδεσης.

2.31) Ανταλλάσσονται συνολικά 4 τεμάχια TCP για την απόλυση σύνδεσης.

2.32) 20 bytes

2.33) Τα τεμάχια αυτά φέρουν μηδενικό μήκος δεδομένων.

2.34) Το πακέτο IPv4 που στέλνει ο υπολογιστής μου για τη διαδικασία απόλυσης σύνδεσης έχει μήκος 40 bytes = 20 bytes (IPv4 header) + 20 bytes (TCP header).

2.35) Το τεμάχιο αυτό περιέχει στα αλήθεια την επικεφαλίδα IPv4 και την επικεφαλίδα TCP. Υπενθυμίζεται ότι περιέχει μηδενικό μήκος δεδομένων. Έτσι το μήκος του θα είναι 20 bytes (επικεφαλίδα IPv4) + 20 bytes (επικεφαλίδα TCP) = 40 bytes.

2.36) Μεταδόθηκαν συνολικά 108 bytes από κάθε πλευρά.

2.37) Τα τεμάχια TCP που στάλθηκαν για να πραγματοποιηθεί η απόλυση σύνδεσης FTP είναι 4: 2 με ενεργοποιημένη τη σημαία FIN και 2 για την επαλήθευση αποστολής των προαναφερθέντων (ACK = 1). Κάθε ένα από αυτά τα τεμάχια μετέφερε μηδενικό μήκος δεδομένων, επομένως το συνολικό μήκος κάθε πακέτου υπολογίζεται από την επικεφαλίδα Ethernet, IPv4 και TCP, δηλαδή 14 bytes + 20 bytes + 20 bytes = 54 bytes. Κάθε πλευρά έστειλε 1 πακέτο [FIN , ACK] και ένα πακέτο [ACK]. Άρα 2 x 54 = 108 bytes.

2.38) Φίλτρο απεικόνισης: “ftp.port == 20”.

2.39) Ο υπολογιστής μου ανακοινώνει MSS = 1460 bytes και ο εξυπηρετητής FTP ανακοινώνει MSS = 536 bytes.

2.40) 1460 bytes

2.41) RTT = 0.001852 secs

2.42) Όχι.

2.43) 117 τεμάχια TCP

2.44) 18 τεμάχια TCP

2.45) Window == 8118

2.46) Η τιμή αυτή διαφέρει με αυτήν του υποερωτήματος 2.17 κατά 74 bytes.

2.47) Η τιμή του πεδίου Window στο τεμάχιο TCP [ACK] κατά την τριπλή χειραψία για την εκκίνηση μεταφοράς δεδομένων είναι 65535, δηλαδή η μέγιστη τιμή που μπορεί να πάρει το πεδίο αυτό. Ωστόσο, κατά την μεταφορά του αρχείου τα τεμάχια TCP [ACK] έχουν τιμή Window = 4097, και αυτή είναι η μικρότερη τιμή που παίρνει το πεδίο αυτό στα υπόλοιπα αντίστοιχα τεμάχια.

2.48) Η τιμή του πεδίου Window δηλώνει το αριθμό των bytes που μπορεί να λάβει ο υπολογιστής πριν χρειαστεί επαλήθευση πακέτων. Συμπερασματικά, αν η υπολογιστής μου ανακοίνωνε Window = 0, τότε θα σταματούσε η αποστολή πακέτων από τον εξυπηρετητή, και η διαδικασία θα βρισκόταν σε παύση.

2.49) **Ethernet Header Length**: 14 bytes

IP Header Length: 20 bytes
TCP Header Length: 32 bytes

2.50) Όχι, μάλιστα είναι πολύ μικρότερο του 1460.
2.51) Απαραίτητη προϋπόθεση για κάθε υπολογιστή/εξυπηρετητή στο δίκτυο είναι να διαθέτει buffer μεγέθους 576 bytes. Επομένως, για να σταλθεί πακέτο μεγαλύτερο των 576 bytes είναι υποχρεωτικό να ανακοινωθεί από τον εκάστοτε παραλήπτη. Έτσι, εάν ο εξυπηρετητής ήθελε να αποστείλει δεδομένων μεγαλύτερα των 567 bytes, και ο buffer του υπολογιστή μου είχε την ελάχιστη χωρητικότητα, θα χάνονταν bytes από το αρχείο που μεταφέρεται. Εν κατακλείδι, ο πομπός μπορεί να στείλει τεμάχια μεγαλύτερα των 567 bytes μόνο από αίτημα του αντίστοιχου παραλήπτη.

2.52) Μεταδόθηκαν συνολικά 61441 bytes από τον εξυπηρετητή FTP στον υπολογιστή μου. Επίσης, δεν μεταδόθηκαν bytes δεδομένων από τον υπολογιστή μου, καθώς τα τεμάχια επιβεβαίωσης TCP [ACK] φέρουν μηδενικό μήκος δεδομένων.

2.53) Μεταδόθηκαν 61441 bytes σε 0,035654 seconds, επομένως ο ρυθμός μεταφορά δεδομένων είναι 1,723.256 Kbyte/sec.

2.54) Ναι υπήρξαν αναμεταδόσεις τεμαχίων. Το αντιλήφθηκα από το γεγονός ότι από το ερώτημα 2.43 γνωρίζουμε ότι στάλθηκαν 117 πακέτα από τον εξυπηρετητή. Τα 116 από αυτά έχουν μήκος 576 bytes και το τελευταίο είχε 184 bytes. Αυτά δίνουν άθροισμα 67000. Ωστόσο, το αρχείο έχει μέγεθος 61441 bytes. Επομένως, αφού στάλθηκαν παραπάνω bytes από το μέγεθος του αρχείου, πρέπει να υπήρξε κάποια αναμετάδοση πακέτων.

Άσκηση 3

3.1) Φίλτρο απεικόνισης: “tcp.port == 20”.

3.2) IPv4 address: 94.65.141.44

3.3) RTT = 0.000097 secs. Συγκριτικά με το υποερώτημα 2.41, η τιμή εδώ είναι σημαντικά μικρότερη.

3.4) Ο εξυπηρετητής στέλνει ανά τακτά χρονικά διαστήματα τεμάχια TCP, το πλήθος των οποίων είναι ανάλογο με την χρονική στιγμή που στάλθηκαν. Δηλαδή, ξεκινά να στέλνει λίγα τεμάχια και με το πέρασμα του χρόνου στέλνει όλο και περισσότερα, έως ότου να τελειώσει η διαδικασία μεταφορά δεδομένων.

3.5) Έστειλε 4 τεμάχια στο πρώτο RTT, τιμή που είναι συμφωνεί με την αναγραφόμενη στην παράγραφο 3.1 του RFC 5681.

3.6) Κατά το 2^{ο} RTT στάλθηκαν 6 τεμάχια, κατά το 3^{ο} 10 τεμάχια και κατά το 4^{ο} 16 τεμάχια.

3.7) Στο 1^{ο}, 2^{ο} 3^{ο} και 4^{ο} RTT στάλθηκαν αντιστοίχως 2, 3, 5 και 8 ACKs. Παρατηρώ ότι τα τεμάχια επιβεβαίωσης που στέλνονται από τον υπολογιστή μου είναι περίπου

τα μισά αυτών που λαμβάνει σε κάθε RTT, τιμή που συμφωνεί με την παράγραφο 2.3 στο RFC 3465.

3.8) Το διάγραμμα αυτό είναι αντίστοιχο με αυτό του δοσμένου αρχείου, ωστόσο στην περίπτωση της δικιάς μου καταγραφής στέλνονται αρχικά εμφανώς περισσότερα πακέτα σε κάθε RTT. Ενδεικτικά, κατά το 1ο, 2ο, 3ο και 4ο RTT στέλνονται 10, 8, 8 και 8 τεμάχια.

Άσκηση 4

4.1) Φίλτρο σύλληψης: "udp"

4.2) **Source Port:** 2 bytes
Destination Port: 2 bytes
Length: 2 bytes
Checksum: 2 bytes

4.3) Συνολικό μέγεθος επικεφαλίδας UDP: 8 bytes

4.4) Το συγκεκριμένο δεδομενόγραμμα UDP έχει μέγεθος 116 bytes, που απαρτίζονται από 40 bytes (IPv6 header) + 8 bytes (UCP header) + 168 bytes (UDP payload length).

4.5) Εκφράζει το συνολικό μέγεθος του δεδομενογράμματος, δηλαδή το μέγεθος της επικεφαλίδας και το μέγεθος των δεδομένων που αυτό φέρει.

4.6) 8 bytes, σε περίπτωση που το δεδομενόγραμμα φέρει μηδενικό μήκος δεδομένων.

4.7) Το ελάχιστο μέγεθος μηνύματος που μπορεί να σταλεί από ένα πακέτο IPv4 είναι 20 bytes (IPv4 header) + 8 bytes (UDP header) = 28 bytes.
Το μέγιστο μέγεθος μηνύματος που μπορεί να σταλεί είναι 65.567 bytes = 20 bytes (IPv4 header) + 0xffff bytes (65.535 bytes, UDP header + UDP payload).

4.8) 556 bytes

4.9) Άλλα πρωτόκολλα που καταγράφηκαν είναι τα εξής: DHCP, LLMNR, MDNS, SSDP και UDP.

4.10) Φίλτρο απεικόνισης: "dns".

4.11) Ο εξυπηρετητής DNS που απάντησε είναι 2001:648:2000:2000::1 (IPv6).

4.12) Source-Destination Ports of Standard query:
Source Port: 53
Destination Port: 61255

4.13) Source-Destination Ports of Standard query response:

Source Port: 61255
Destination Port: 53

4.14) Η θύρα 53 αντιστοιχεί στην εφαρμογή του πρωτοκόλλου εφαρμογής DNS.