



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Δίκτυα Υπολογιστών

Αναφορά 8ης Εργαστηριακής Άσκησης

Ραπτόπουλος Πέτρος (el19145)
Ομάδα 3

Ημερομηνία: 30/11/2022

Άσκηση 1: TELNET

Με τη βοήθεια του Wireshark καταγράφουμε την κίνηση ενώ κάνουμε χρήση της υπηρεσίας Telnet του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15). Εφαρμόζουμε φίλτρο σύλληψης host 147.102.40.15 για να παρατηρήσουμε μόνο την κίνηση που σχετίζεται με το edu-dy.cn.ntua.gr. Για τη χρήση της υπηρεσίας Telnet πληκτρολογούμε telnet edu-dy.cn.ntua.gr σε ένα παράθυρο εντολών.

Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	147.102.237.240	147.102.40.15	TCP	74 39984 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
2	0.001401394	147.102.40.15	147.102.237.240	TCP	74 23 → 39984 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=...
3	0.001445237	147.102.237.240	147.102.40.15	TCP	66 39984 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3743257547...
4	0.001628927	147.102.237.240	147.102.40.15	TELNET	93 Telnet Data ...
5	0.014243113	147.102.40.15	147.102.237.240	TELNET	69 Telnet Data ...
6	0.014278197	147.102.237.240	147.102.40.15	TCP	66 39984 → 23 [ACK] Seq=28 Ack=4 Win=64256 Len=0 TSval=374325756...
7	0.014332562	147.102.237.240	147.102.40.15	TELNET	69 Telnet Data ...
8	0.015394887	147.102.40.15	147.102.237.240	TELNET	93 Telnet Data ...
9	0.015423739	147.102.237.240	147.102.40.15	TCP	66 39984 → 23 [ACK] Seq=31 Ack=31 Win=64256 Len=0 TSval=37432575...
10	0.016971544	147.102.40.15	147.102.237.240	TELNET	72 Telnet Data ...
11	0.016989803	147.102.237.240	147.102.40.15	TELNET	123 Telnet Data ...
12	0.115686798	147.102.40.15	147.102.237.240	TCP	66 23 → 39984 [ACK] Seq=37 Ack=88 Win=65984 Len=0 TSval=41816881...
13	0.115732967	147.102.237.240	147.102.40.15	TELNET	72 Telnet Data ...
14	0.120206953	147.102.40.15	147.102.237.240	TELNET	99 Telnet Data ...
15	0.120231776	147.102.237.240	147.102.40.15	TCP	66 39984 → 23 [ACK] Seq=94 Ack=61 Win=64256 Len=0 TSval=37432576...
16	0.120397818	147.102.237.240	147.102.40.15	TELNET	168 Telnet Data ...
17	0.122698091	147.102.40.15	147.102.237.240	TELNET	69 Telnet Data ...
18	0.122722543	147.102.237.240	147.102.40.15	TCP	66 39984 → 23 [ACK] Seq=196 Ack=64 Win=64256 Len=0 TSval=3743257...
19	0.122811820	147.102.237.240	147.102.40.15	TELNET	60 Telnet Data ...
▶ Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface wlpis0, id 0					
▶ Ethernet II, Src: IntelCor_15:16:66 (90:78:41:15:16:66), Dst: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d)					
▶ Internet Protocol Version 4, Src: 147.102.237.240, Dst: 147.102.40.15					
▶ Transmission Control Protocol, Src Port: 39984, Dst Port: 23, Seq: 1, Ack: 1, Len: 27					
Source Port: 39984					
Destination Port: 23					
[Stream index: 0]					
[TCP Segment Len: 27]					
Sequence number: 1 (relative sequence number)					
Sequence number (raw): 2498019883					
[Next sequence number: 28 (relative sequence number)]					
Acknowledgment number: 1 (relative ack number)					
Acknowledgment number (raw): 1880004028					
1000 = Header Length: 32 bytes (8)					
▶ Flags: 0x018 (PSH, ACK)					
Window size value: 502					
[Calculated window size: 64256]					
[Window size scaling factor: 128]					
Checksum: 0x2cda [unverified]					
[Checksum Status: Unverified]					
Urgent pointer: 0					
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps					
▶ [SEQ/ACK analysis]					
▶ [Timestamps]					
TCP payload (27 bytes)					
▶ Telnet					
▶ Do Suppress Go Ahead					
▶ Will Terminal Type					
▶ Will Negotiate About Window Size					
▶ Will Terminal Speed					
▶ Will Remote Flow Control					
▶ Will Linemode					
▶ Will New Environment Option					
▶ Do Status					
▶ Will X Display Location					
0000 08 ec f5 d0 d9 1d 00 78 41 15 16 66 08 00 45 10x A . f . E					
0010 00 4f ab 96 40 00 40 06 52 36 93 66 ed f0 93 66 - 0 . @ . R6 f . . f					
0020 28 0f 9c 30 00 17 94 e4 c2 20 6b 49 e1 bc 80 18 (- 0 + k I					
0030 01 f6 2c da 00 00 01 01 00 0a 0f 1d 93 cc 18 ec					
0040 bf 7b ff fd 03 ff fb 18 ff fb 1f ff fb 20 ff fb - {					
0050 21 ff fb 22 ff fb 27 ff ff 05 ff fb 23 ! #					

```
petrosrpto@petrosrptoAssistant:~$ telnet edu-dy.cn.ntua.gr
Trying 147.102.40.15...
Connected to edu-dy.cn.ece.ntua.gr.
Escape character is '^['.

FreeBSD/amd64 (edu-dy.cn.ntua.gr) (pts/6)

login: abcd
Password for abcd@edu-dy.cn.ntua.gr:
Login incorrect
login:
telnet> quit
Connection closed.
```

- 1.1) Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το TELNET (TCP ή UDP); **TCP**
- 1.2) Καταγράψτε τις θύρες του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία. **Θύρα 23 για τον υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15) και θύρα 39984 για τον υπολογιστή μας.**
- 1.3) Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής TELNET; **Θύρα 23**
- 1.4) Εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια που σχετίζονται με το πρωτόκολλο εφαρμογής TELNET. Ποια είναι η σύνταξή του; **telnet**

Εντοπίζουμε το πρώτο μήνυμα TELNET που μεταφέρει την προτροπή για login.

- 1.5) Καταγράψτε τις εντολές (command) TELNET τύπου echo και τον αποστολέα τους, μεταξύ του υπολογιστή σας και του edu-dy.cn.ntua.gr, που προηγούνται του μηνύματος αυτού.

Do Echo Source: 147.102.40.15 - Destination: 147.102.237.240,
Won't Echo Source: 147.102.237.240 - Destination: 147.102.40.15,
Will Echo Source: 147.102.40.15 - Destination: 147.102.237.240,
Do Echo Source: 147.102.237.240 - Destination: 147.102.40.15

- 1.6) Ζητά ο edu-dy.cn.ntua.gr από τον υπολογιστή σας να επαναλαμβάνει (echo) τους χαρακτήρες που λαμβάνει; **Ναι, αφού έχουμε Do Echo Source: 147.102.40.15 - Destination: 147.102.237.240**
- Εάν ναι, δέχεται ο υπολογιστής σας να τους επαναλαμβάνει; **Όχι, αφού Won't Echo Source: 147.102.237.240 - Destination: 147.102.40.15**

1.7) Ζητά ο edu-dy.cn.ntua.gr από τον υπολογιστή σας να μην επαναλαμβάνει (echo) τους χαρακτήρες που λαμβάνει; **Όχι**

1.8) Προτίθεται ο edu-dy.cn.ntua.gr να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή σας; **Ναι** αφού **Will Echo Source: 147.102.40.15 - Destination: 147.102.237.240**

Εντοπίζουμε το μήνυμα TELNET από τον υπολογιστή μας προς τον edu-dy.cn.ntua.gr που μεταφέρει τον πρώτο χαρακτήρα "a" του ονόματος χρήστη.

1.9) Έχει προηγηθεί του μηνύματος αυτού εντολή TELNET με την οποία ο υπολογιστής σας ζητά την επανάληψη των χαρακτήρων από τον edu-dy.cn.ntua.gr;

Ναι όπως καταγράψαμε στο ερώτημα 1.5) έχουμε **Do Echo Source: 147.102.237.240 - Destination: 147.102.40.15**

Εντοπίζουμε την πρώτη προτροπή login παρατηρώντας τη ροή κίνησης TCP.

```
.....!..".'.#..%..%.....!..".'.#..&..$...P.....".....b.....b.... B.
.....&..$.....#.....'.....38400,38400.....#..petrosrptoAssistant:
0.....'.DISPLAY.petrosrptoAssistant:0.....xterm-256color.....!.....".....".....
.....
FreeBSD/amd64 (edu-dy.cn.ntua.gr) (pts/6)
.
login: aabbccdd
Password for abcd@edu-dy.cn.ntua.gr:.....efgh
Login incorrect
login:
```

1.10) Τι συμβαίνει κατά τη μεταφορά του ονόματος χρήστη που αποστείλατε μετά την πρώτη προτροπή login;

Έχουμε επανάληψη των χαρακτήρων από τον υπολογιστή edu-dy.cn.ntua.gr

1.11) Εξηγήστε το φαινόμενο που παρατηρείτε στο προηγούμενο ερώτημα με βάση την απάντηση στα ερωτήματα 1.8 και 1.9. **Όπως προειπώθηκε στα ερωτήματα αυτά ο υπολογιστής μας ζητάει να επαναλαμβάνει ο υπολογιστής edu-dy.cn.ntua.gr τους χαρακτήρες που παραλαμβάνει. Ο υπολογιστής edu-dy.cn.ntua.gr το αποδέχεται.**

1.12) Κλείστε τώρα το παράθυρο Follow TCP Stream και εφαρμόζοντας φίλτρο απεικόνισης εντοπίστε τα πακέτα IPv4 που μεταφέρουν μηνύματα TELNET από τον υπολογιστή σας προς τον εξυπηρετητή. Ποια είναι η σύνταξή του; **telnet and ip.src == 147.102.237.240 and ip.dst == 147.102.40.15**

1.13) Πόσα πακέτα IPv4 χρειάζονται για να μεταφερθεί η πληροφορία για το όνομα (abcd) του χρήστη; **5**

1.14) Πόσα πακέτα IPv4 χρειάζονται για να μεταφερθεί η πληροφορία για τον κωδικό του χρήστη (efgh); **5**

Ακυρώνουμε το προηγούμενο φίλτρο απεικόνισης και εφαρμόζουμε νέο ώστε να παρατηρούμε και τα μηνύματα TELNET που στέλνει ο εξυπηρετητής.

1.15) Ο εξυπηρετητής στέλνει την ηχώ των χαρακτήρων efgh του κωδικού χρήστη προς τον πελάτη; **Όχι**

1.16) Παρατηρήσατε εντολή TELNET "Don't Echo" πριν τη μεταφορά του κωδικού; **Όχι**

1.17) Εάν η απάντηση στην προηγούμενη ερώτηση είναι όχι, γιατί δεν εμφανίζεται στην οθόνη ο κωδικός;

Γιατί δεν παραλαμβάνονται οι χαρακτήρες στον υπολογιστή μας, αφού ο εξυπηρετητής δεν τους επαναλαμβάνει.

1.18) Σχολιάστε την ασφάλεια της υπηρεσίας Telnet. **Οι πληροφορίες (συμπεριλαμβανομένου του κωδικού χρήστη) που ανταλλάσσονται με τη βοήθεια του πρωτοκόλλου Telnet δεν κρυπτογραφούνται και συνεπώς υπόκεινται σε υποκλοπή αν κάποιος τρίτος παραλάβει και αναλύσει τα διερχόμενα πακέτα.**

Άσκηση 2: FTP

Σημείωση: Η υπηρεσία FTP για active mode δεν λειτουργούσε ορθά στον υπολογιστή μου. Γίνεται χρήση καταγραφή συναδέλφου.

2.1) Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πακέτα που περιλαμβάνουν τη διεύθυνση IP του edu-dy.cn.ntua.gr. **host 147.102.40.15**

2.2) Τι σημαίνει το -d στη γραμμή εντολής που πληκτρολογήσατε; [Υπόδειξη: Πληκτρολογήστε ftp -help στη γραμμή εντολών]. **Enable debugging**

2.3) Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το FTP (TCP ή UDP); **TCP**

2.4) Καταγράψτε τις θύρες (πηγής και προορισμού) που χρησιμοποιούνται για την επικοινωνία FTP τόσο για τις εντολές ελέγχου όσο και για τη μεταφορά δεδομένων.

Εντολές ελέγχου: Θύρα υπολογιστή μας: 55421, Θύρα εξυπηρετητή 21

Εντολές δεδομένων: Θύρα υπολογιστή μας: 55422, Θύρα εξυπηρετητή 20

2.5) Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η σύνδεση TCP για τη μεταφορά δεδομένων FTP; **Την έναρξη της σύνδεσης την επιδιώκει η πλευρά του εξυπηρετητή στέλνοντας SYN.**

2.6) Καταγράψτε τις εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή.

USER anonymous, PASS labuser@cn, SYST, FEAT, HELP, EPRT, LIST, QUIT

2.7) Εμφανίζονται αυτές οι εντολές FTP στις πληροφορίες αποσφαλμάτωσης (debugging) στην οθόνη του προγράμματος φλοιού ftp και με ποιον τρόπο; **Εμφανίζονται**

2.8) Με ποια εντολή του πρωτοκόλλου FTP μεταφέρεται το όνομα χρήστη; **USER**

2.9) Πόσα πακέτα χρειάζονται για να μεταφερθεί το όνομα του χρήστη; **1**

2.10) Με ποια εντολή του πρωτοκόλλου FTP μεταφέρεται ο κωδικός χρήστη; **PASS**

2.11) Πόσα πακέτα IP χρειάζονται για να μεταφερθεί ο κωδικός του χρήστη; **1**

2.12) Περιγράψτε μια ομοιότητα και μια διαφορά στον τρόπο λειτουργίας των πρωτοκόλλων FTP και TELNET σε σχέση με ό,τι παρατηρήσατε για τη μεταφορά του ονόματος και του κωδικού χρήστη.

Ομοιότητα: Έχουμε μεταφορά των ονομάτων/κωδικών χωρίς κρυπτογράφησή τους.

Διαφορά: Στο πρωτόκολλο FTP δεν έχουμε echo του ονόματος χρήστη όπως είχαμε στο πρωτόκολλο TELNET.

2.13) Η εντολή help του προγράμματος φλοιού ftp μεταφράζεται σε εντολή του πρωτοκόλλου FTP; **Ναι, HELP**

2.14) Βάσει των αποτελεσμάτων από την εκτέλεση της εντολής remotehelp (rhelp) που πληκτρολογήσατε στο παράθυρο της γραμμής εντολών, καταγράψτε δύο εντολές FTP που δεν υποστηρίζονται από τον εξυπηρετητή.

PROT, MIC (unimplemented)

Εφαρμόζουμε φίλτρο απεικόνισης ftp ώστε να εμφανισθεί όλος ο διάλογος (μεταξύ του υπολογιστή μας και του εξυπηρετητή) στη σύνδεση ελέγχου FTP.

2.15) Πόσα πακέτα, σχετικά με την εντολή remotehelp (rhelp), στάλθηκαν από τον υπολογιστή σας και πόσα από τον εξυπηρετητή; **1 από τον υπολογιστή μας (request) και 9 από τον εξυπηρετητή**

2.16) Πώς δηλώνει ο εξυπηρετητής ότι τελείωσε η αποστολή πακέτων σχετικών με την εντολή remotehelp (rhelp); **Το τελευταίο πακέτο που αφορά την εντολή rhelp δεν έχει παύλα μετά το response code αλλά κενό.**

2.17) Εντοπίστε στη λίστα καταγεγραμμένων πακέτων του Wireshark το μήνυμα FTP που μεταφέρει την εντολή PORT. Τι παριστάνουν οι 4 πρώτοι δεκαδικοί αριθμοί; **Εντολή EPRT: Extended Active Address Family (IPv4), Extended Active IP address (147.102.200.213), Extended active port (55422)**

2.18) Πώς προκύπτει αυτός ο αριθμός αυτής της θύρας από τα δεδομένα της εντολής PORT;

Έχουμε την εντολή EPRT. Για την εντολή αυτή η πληροφορία για τη θύρα μεταφέρεται μέσω 5 byte όπου το καθένα αντιπροσωπεύει κάθε ψηφίο της θύρας σε κώδικα ASCII. Πχ έχουμε 35 35 34 32 32 για θύρα 55422, αφού ο κώδικας

ASCII για το '2' είναι το 32, για το '4' είναι το 34 και για το '5' είναι το 35.

2.19) Ποια εντολή του πρωτοκόλλου FTP εμφανίζει τα περιεχόμενα του τρέχοντος καταλόγου; **LIST**

2.20) Γιατί η εντολή PORT του πρωτοκόλλου FTP προηγείται της εντολής της ερώτησης 2.19;

Η εντολή PORT στέλνεται από τον client ώστε να εγκαθιδρύσει μια δεύτερη σύνδεση (διεύθυνση και θύρα) για να μεταφερθούν τα δεδομένα. Για αυτό προηγείται της LIST όπου έχουμε μεταφορά δεδομένων.

2.21) Σε ποια εντολή του πρωτοκόλλου FTP μεταφράζεται η εντολή bye του προγράμματος φλοιού ftp; **QUIT**

2.22) Με ποιο μήνυμα αποκρίνεται ο εξυπηρετητής FTP στην εντολή bye του προγράμματος φλοιού ftp; **Goodbye**

2.23) Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια με τη σημαία FIN ενεργοποιημένη. Ποια είναι η σύνταξή του; **tcp.flags.fin == 1**

2.24) Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση των συνδέσεων TCP που αφορούν τις εντολές ελέγχου και μηνύματα δεδομένων του FTP;

Για τις εντολές ελέγχου έχουμε απόλυση της σύνδεσης από τη μεριά του πελάτη.

Για τα μηνύματα δεδομένων έχουμε απόλυση της σύνδεσης από τη μεριά του εξυπηρετητή.

Αρχίζουμε μια νέα καταγραφή με το Wireshark και συνδεόμαστε με anonymous ftp στο edu-dy.cn.ntua.gr χρησιμοποιώντας το γραφικό περιβάλλον του υπολογιστή μας (FileZilla). Αφού εμφανισθεί στην οθόνη η λίστα των αρχείων του edu-dy.cn.ntua.gr κλείνουμε το παράθυρο και σταματάμε την καταγραφή.

2.25) Καταγράψτε τις θύρες (πηγής και προορισμού) που χρησιμοποιούνται για την επικοινωνία FTP τόσο για τις εντολές ελέγχου όσο και για τη μεταφορά δεδομένων.

Εντολές ελέγχου: Θύρα υπολογιστή μας: 52828, Θύρα εξυπηρετητή: 21

Εντολές δεδομένων: Θύρα υπολογιστή μας: 51603, Θύρα εξυπηρετητή 17669

2.26) Καταγράψτε τις εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή. **AUTH TLS, AUTH SSL,**

USER anonymous, PASS anonymous@example.com, SYST, FEAT, OPTS UTF8 ON, PWD, TYPE I, PASV, MLSD

2.27) Αν η σύνδεση στον εξυπηρετητή FTP γινόταν με χρήση της διεύθυνσης ftp://user:password@edu-dy.cn.ntua.gr, στην καταγραφή ως όνομα χρήστη θα βλέπατε το user και ως κωδικό χρήστη το password. Στη δική σας περίπτωση, ποιο όνομα και ποιος κωδικός χρήστη χρησιμοποιήθηκε; **user: anonymous, password: anonymous@example.com**

2.28) Ποια εντολή του πρωτοκόλλου FTP χρησιμοποιήθηκε για την εμφάνιση της λίστας αρχείων; **MLSD**

2.29) Καταγράψτε το μήνυμα με το οποίο αποκρίνεται ο εξυπηρετητής στην εντολή PASV.

Response: 277 Entering Passive Mode (147,102,40.15,69,5)

2.30) Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η εγκατάσταση της σύνδεσης TCP που αφορά τα μηνύματα δεδομένων του FTP; **Από πλευρά του πελάτη**

2.31) Για τη μεταφορά δεδομένων FTP, ο εξυπηρετητής δεν χρησιμοποιεί τη θύρα 20. Ποια θύρα του εξυπηρετητή χρησιμοποιείται και πώς προκύπτει ο αριθμός της από τα στοιχεία της απάντησης που καταγράψατε στην ερώτηση 2.29; **Χρησιμοποιείται η θύρα 17669, προκύπτει από την πράξη $69 \cdot 256 + 5$, όπου 69, 5 στοιχεία της απάντησης του 2.29.**

2.32) Πώς προκύπτει ο αριθμός θύρας της σύνδεσης TCP για μεταφορά δεδομένων FTP στην πλευρά του πελάτη; **Γίνεται δυναμική και τυχαία επιλογή θύρας από τον πελάτη.**

Εφαρμόζουμε φίλτρο ftp-data ώστε να εμφανισθεί η ανταλλαγή δεδομένων μέσω της σύνδεσης δεδομένων FTP.

2.33) Πόσα μηνύματα δεδομένων FTP στάλθηκαν από τον εξυπηρετητή και ποιο το μέγεθος των δεδομένων που μεταφέρουν; **Έχουμε 2 μηνύματα δεδομένων, 2620 και 1514 bytes.**

2.34) Δικαιολογήστε το μέγεθος του πρώτου από τα προηγούμενα μηνύματα δεδομένων FTP.

Σχετίζεται με τις τιμές Maximum Segment Size που διαπραγματεύτηκαν οι δύο πλευρές κατά την σύνδεση.

2.35) Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση των συνδέσεων TCP που αφορούν τις εντολές ελέγχου του FTP; **Από τη πλευρά του πελάτη**

2.36) Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση της σύνδεσης TCP που αφορά τα μηνύματα δεδομένων FTP; **Από τη πλευρά του εξυπηρετητή.**

Άσκηση 3: TTP

Παραμένοντας συνδεδεμένοι στο εσωτερικό δίκτυο του ΕΜΠ, καταγράφουμε με τη βοήθεια του Wireshark την κίνηση ενώ κάνουμε χρήση της υπηρεσίας TFTP του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15).

Όπως πριν, εφαρμόζουμε φίλτρο σύλληψης για να παρατηρήσουμε μόνο την κίνηση που σχετίζεται με το edu-dy.cn.ntua.gr. Πληκτρολογούμε tftp edu-dy.cn.ntua.gr και μετά get rfc1350.txt. Αφού σταματήσουμε την καταγραφή κίνησης, εφαρμόζουμε το φίλτρο απεικόνισης για να παρατηρήσουμε μόνο την κίνηση (πακέτα IPv4) που σχετίζεται με το edu-dy.cn.ntua.gr.

3.1) Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το TFTP (TCP ή UDP); **UDP**

3.2) Καταγράψτε τις θύρες (πηγής και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την πρώτη επικοινωνία του πελάτη με τον εξυπηρετητή TFTP. **Θύρα πηγής: 39378, Θύρα προορισμού: 69**

3.3) Καταγράψτε τις θύρες (πηγής και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται κατά τη μεταφορά δεδομένων. **Θύρα πηγής: 41323, Θύρα προορισμού: 39378**

3.4) Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής TFTP; **Θύρα 69**

3.5) Πώς προκύπτουν οι αριθμοί θυρών που χρησιμοποιούνται κατά τη μεταφορά δεδομένων; **Τυχαία επιλογή.**

3.6) Η μεταφορά του αρχείου rfc1350.txt γίνεται σε δυαδικό (binary) τρόπο (mode) ή ASCII; **ASCII**

3.7) Σε ποιο μήνυμα TFTP μεταξύ πελάτη – εξυπηρετητή καθορίζεται αυτό και με ποιο τρόπο;

Στο Read Request, στο πεδίο Type του πρωτοκόλλου Trivial Transfer Protocol. Έχουμε netascii.

3.8) Καταγράψτε όλους του τύπους μηνυμάτων TFTP που παρατηρήσατε. **Read Request - File, Data Packet - Block**

3.9) Το πρωτόκολλο μεταφοράς UDP είναι αναξιόπιστο καθώς δεν παρέχει μηχανισμό επιβεβαιώσεων, όπως το TCP. Πώς αντιμετωπίζει το πρόβλημα αυτό το TFTP; **Θεωρητικά στέλνονται πακέτα ACK ωστόσο δεν παρατηρούνται στην καταγραφή του Wireshark.**

3.10) Ποιος τύπος μηνύματος TFTP και ποιο πεδίο της επικεφαλίδας χρησιμοποιείται για τον σκοπό αυτό;

Τύπος μηνύματος: Acknowledge, Πεδίο: Opcode

3.11) Ποιο είναι το μέγεθος των μηνυμάτων TFTP που μεταφέρουν τα προς μετάδοση δεδομένα; **516 bytes**

3.12) Ποιο είναι το μέγεθος των δεδομένων που μεταφέρονται από αυτά τα μηνύματα TFTP; **512 bytes**

3.13) Πώς αντιλαμβάνεται ο πελάτης το τέλος της μετάδοσης δεδομένων; **Το τέλος της μεταφοράς σηματοδοτείται από πακέτο δεδομένων το οποίο έχει μέγεθος μικρότερο από 516 bytes (ανάμεσα σε 0 και 511 bytes)**