ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

# Δίκτυα Υπολογιστών

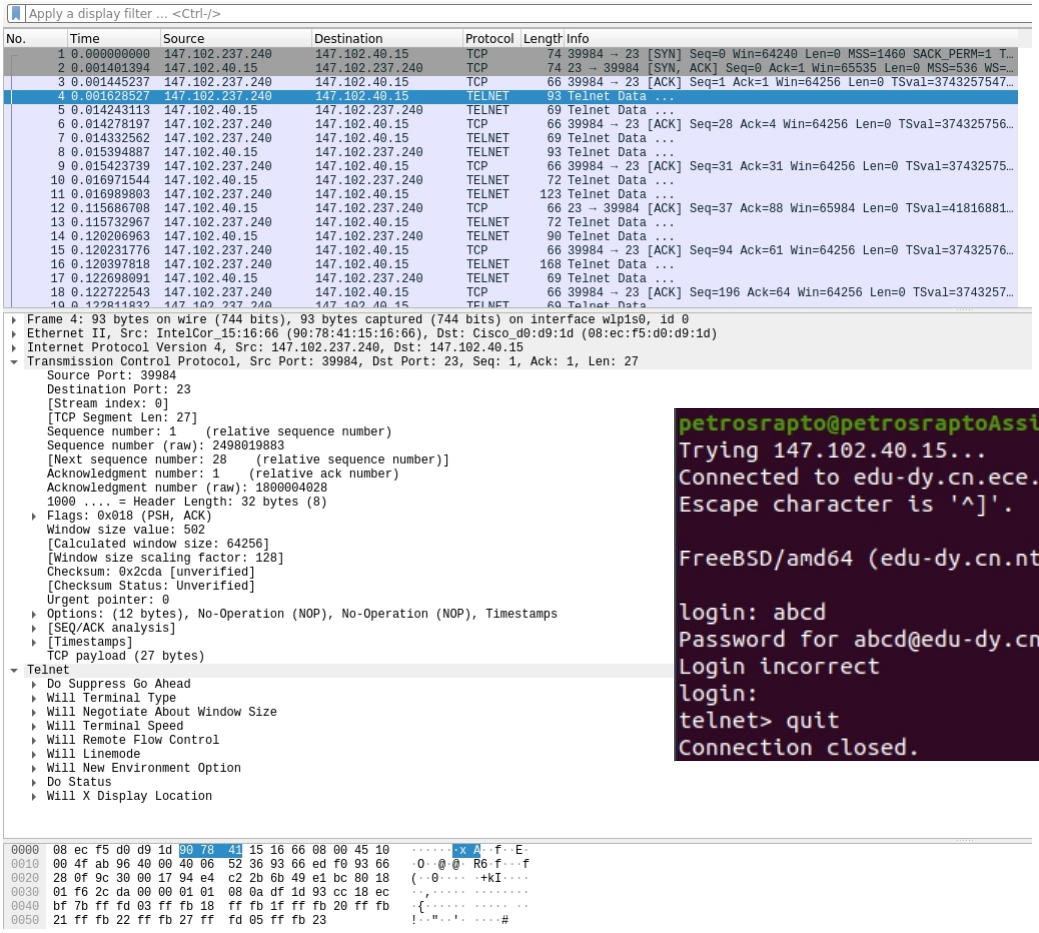
## Αναφορά 8ης Εργαστηριακής Άσκησης

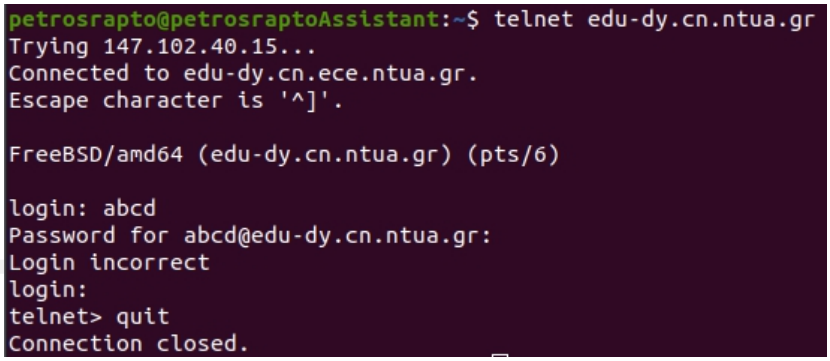
**Ραπτόπουλος Πέτρος (el19145)**
**Ομάδα 3**

**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.




**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.


**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*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)**