Εργαστηριακή Άσκηση 8, TELNET, FTP και TFTP

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΚΟΥΣΤΕΝΗΣ ΧΡΙΣΤΟΣ (03120227)

ΟΜΑΔΑ: 3

ΟΝΟΜΑ PC/ΛΣ: LAPTOP-TK5Q3T95 / WINDOWS 11

ΗΜΕΡΟΜΗΝΙΑ: 28/11/2023

ΔΙΕΥΘΥΝΣΗ IP: 192.168.1.14 / 147.102.131.64/ 147.102.131.204

ΔΙΕΥΘΥΝΣΗ MAC: B4-B5-B6-79-4B-09

1. TELNET

Με τη βοήθεια του Wireshark, θα καταγράψετε την κίνηση ενώ κάνετε χρήση της υπηρεσίας Telnet του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15). Εάν χρησιμοποιείτε λειτουργικό σύστημα Windows θα πρέπει ρητά να ενεργοποιήσετε την εφαρμογή πελάτη telnet από το Turn Windows features on or off. Σε συστήματα Unix/Linux, εάν δεν υπάρχει, θα χρειαστεί να την εγκαταστήσετε. Εφαρμόστε φίλτρο σύλληψης host 147.102.40.15 για να παρατηρείτε μόνο την κίνηση που σχετίζεται με το edu-dy.cn.ntua.gr. Για τη χρήση της υπηρεσίας Telnet πληκτρολογήστε telnet edu-dy.cn.ntua.gr σε ένα παράθυρο εντολών. Στην προτροπή login: πληκτρολογήστε abcd ακολουθούμενο από <Enter>, ενώ στην προτροπή Password: πληκτρολογήστε efgh ακολουθούμενο από <Enter>. Σημειώνεται ότι ο χρήστης abcd δεν υπάρχει στον συγκεκριμένο εξυπηρετητή και η αναγνώριση του χρήστη θα αποτύχει. Στη συνέχεια πληκτρολογήστε <Ctrl>+] και στην προτροπή που θα εμφανισθεί δίνετε την εντολή quit για έξοδο.

Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το TELNET (TCP ή UDP);
`Το TCP πρωτόκολλο.`

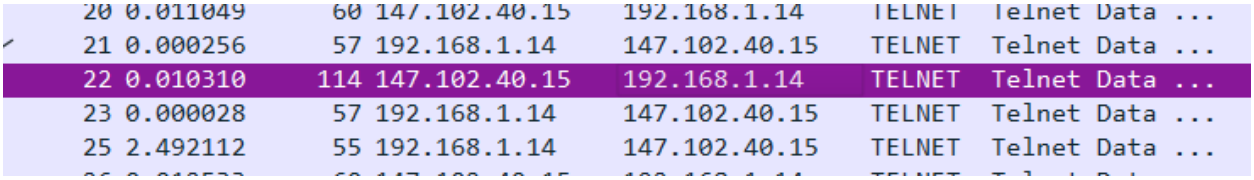
1.2 Καταγράψτε τις θύρες του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία.
`147.102.40.15 --> 23 (edu-dy.cn.ntua.gr).`

`192.168.1.14 --> 57140 (My PC)`

1.3 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής TELNET;
`Port 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;
`Display filter: ***telnet***`

Εντοπίστε το πρώτο μήνυμα TELNET που μεταφέρει την προτροπή για login. [Υπόδειξη: Για να το εντοπίσετε, επιλέξτε το πρώτο μήνυμα TELNET, από το μενού Edit --> Find Packet... ενεργοποιήστε την επιλογή String (αντί για Display filter), στο πεδίο αναζήτησης πληκτρολογήστε login, επιλέξτε Packet Details για αναζήτησε στο πεδίο δεδομένων, και τέλος πατήστε το Find].



20	0.011049	60	147.102.40.15	192.168.1.14	TELNET	Telnet Data ...
21	0.000256	57	192.168.1.14	147.102.40.15	TELNET	Telnet Data ...
22	0.010310	114	147.102.40.15	192.168.1.14	TELNET	Telnet Data ...
23	0.000028	57	192.168.1.14	147.102.40.15	TELNET	Telnet Data ...
25	2.492112	55	192.168.1.14	147.102.40.15	TELNET	Telnet Data ...

Το πακέτο 22 εντοπίζεται με την παραπάνω διαδικασία.

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

Frame No	Source		Destination	Telnet Option
16	147.102.40.15	--->	192.168.1.14	Do Echo.
19	192.168.1.14	--->	147.102.40.15	Will Echo.
20	147.102.40.15	--->	192.168.1.14	Don’t Echo ,Will Echo
21	192.168.1.14	--->	147.102.40.15	Won’t Echo

1.6 Ζητά ο edu-dy.cn.ntua.gr από τον υπολογιστή σας να επαναλαμβάνει (echo) τους χαρακτήρες που λαμβάνει; Εάν ναι, δέχεται ο υπολογιστής σας να τους επαναλαμβάνει;

Ναι ζητάει(Do Echo) και δέχεται.

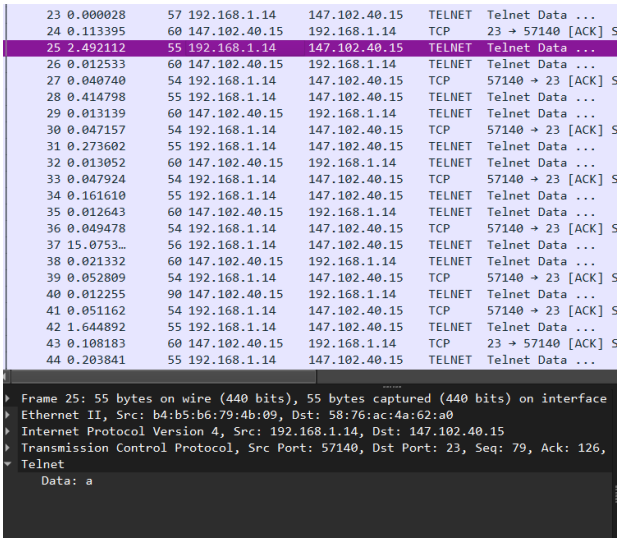
1.7 Ζητά ο edu-dy.cn.ntua.gr από τον υπολογιστή σας να μην επαναλαμβάνει (echo) τους χαρακτήρες που λαμβάνει; Εάν ναι, δέχεται ο υπολογιστής σας να μην τους επαναλαμβάνει;

Ναι(Don’t Echo) και δέχεται(Won’t Echo).

1.8 Προτίθεται ο edu-dy.cn.ntua.gr να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή σας;

Ναι, προτίθεται (Will Echo).

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

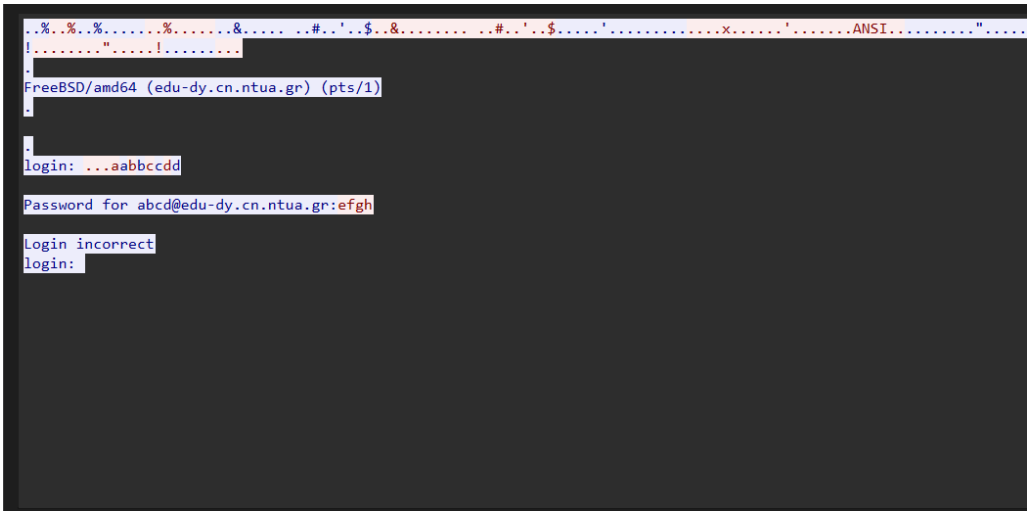


Το πακέτο 25 μεταφέρει από τον υπολογιστή μας τον χαρακτήρα «a».

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;

Στο πακέτο 23 ο υπολογιστής μας στέλνει εντολή TELNET «***Do echo***» στον edu-dy.cn.ntua.gr.

Από το μενού Analyze επιλέγοντας Follow TCP Stream, εμφανίζεται παράθυρο όπου μπορείτε να παρατηρήσετε ολόκληρη τη ροή κίνησης TCP κατά την επικοινωνία. Με μπλε χρώμα παρουσιάζεται η κίνηση από την πλευρά του εξυπηρετητή, ενώ με κόκκινο η δική σας. Εντοπίστε την πρώτη προτροπή login (εν ανάγκη μεγεθύνετε το παράθυρο ώστε να δείτε το τέλος των γραμμών όπου εμφανίζονται οι χαρακτήρες ASCII).



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

Αμέσως μετά την προτροπή login (τεμάχιο 22), εμφανίζονται αρχικά 3 τελείες από τη μεριά μας (τεμάχιο 23), το οποίο στο Wireshark βλέπουμε πως μεταφράζεται σε Do Echo, δηλαδή ο υπολογιστής μας ζητάει από τον edu-dy.cn.ntua.gr να επαναλαμβάνει τους χαρακτήρες που λαμβάνει. Στη συνέχεια, βλέπουμε την αποστολή του χαρακτήρα 'a' (κόκκινο χρώμα) από τον υπολογιστή μας (τεμάχιο 25) και την εμφάνισή του επίσης στον σέρβερ (μπλε χρώμα). Το ίδιο συμβαίνει και για τους υπόλοιπους χαρακτήρες που εισάγουμε κατά το login, δηλαδή τους πληκτρολογούμε και αυτοί εμφανίζονται επίσης στον 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.

Το φαινόμενο που παρατηρήσαμε, δικαιολογείται, καθώς όπως είδαμε νωρίτερα, ο edu-dy.cn.ntua.gr προτίθεται να επαναλαμβάνει τους χαρακτήρες που του στέλνουμε και επιπλέον ο δικός μας υπολογιστής του έχει ζητήσει να το κάνει.

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;

Display filter: ***ip.src == 192.168.1.14 and ip.dst == 147.102.40.15 and telnet***

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

Χρειάζονται 4 πακέτα ένα για κάθε χαρακτήρα.

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

Χρειάζονται 4 πακέτα ένα για κάθε χαρακτήρα.

Ακυρώστε το προηγούμενο φίλτρο απεικόνισης και εφαρμόστε νέο ώστε να παρατηρείτε 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 δεν τη στέλνει.

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

Ενώ πριν την εισαγωγή των χαρακτήρων για το login, βλέπουμε πως ο υπολογιστής μας στέλνει Do Echo (τεμάχιο 23), δε παρατηρούμε κάποια εντολή Don't Echo πριν τη μεταφορά του κωδικού.

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

Δεν εμφανίζεται γιατί θα μπορούσε να υποκλαπεί από κακόβουλο χρήστη/λογισμικό.

1.18 Σχολιάστε την ασφάλεια της υπηρεσίας Telnet.

Εφόσον η επικοινωνία δεν είναι κρυπτογραφημένη, με έναν αναλυτή πακέτων όπως το Wireshark είναι εύκολο να αναγνωστούν τα δεδομένα αυτά. Αρκεί κάποιος να μπορεί να "ακούει" την επικοινωνία μεταξύ 2 κόμβων για να υποκλέψει ευαίσθητα δεδομένα. Επομένως, το telnet υστερεί σε θέματα ασφαλείας.

2. FTP

Για τη συνέχεια θα πρέπει να είστε συνδεδεμένοι στο εσωτερικό δίκτυο του ΕΜΠ. Με τη βοήθεια του Wireshark, θα καταγράψετε την κίνηση ενώ κάνετε χρήση της υπηρεσίας FTP

του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15) χρησιμοποιώντας τον ενεργό τρόπο λειτουργίας. Όπως πριν, εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με το edu-dy.cn.ntua.gr. Αρχίστε μια καταγραφή και σε ένα παράθυρο εντολών πληκτρολογήστε ftp -d edu-dy.cn.ntua.gr σε περιβάλλον Windows (ή ftp -A -d edu-dy.cn.ntua.gr σε περιβάλλον Linux). Στην προτροπή User: πληκτρολογήστε anonymous, ενώ στην προτροπή Password: πληκτρολογήστε labuser@cn. Αφού συνδεθείτε, δώστε τις εντολές help και remotehelp (ή rhelp σε συστήματα Linux). Στη συνέχεια δώστε την εντολή ls για να δείτε τα περιεχόμενα του τρέχοντος καταλόγου και

πληκτρολογήστε bye για έξοδο.

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.
Capture filter: ***host 147.102.40.15***

2.2 Τι σημαίνει το –d στη γραμμή εντολής που πληκτρολογήσατε; [Υπόδειξη: Πληκτρολογήστε ftp-help στη γραμμή εντολών].
Επιτρέπει τον εντοπισμό σφαλμάτων, εμφανίζοντας όλες τις εντολές ftp που μεταβιβάζονται μεταξύ του πελάτη και του εξυπηρετητή.

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

2.4 Καταγράψτε τις θύρες (πηγής και προορισμού) που χρησιμοποιούνται για την επικοινωνία FTP με τον edu-dy.cn.ntua.gr.
Παρατηρούμε 4 ομάδες πακέτων :

- Source Port : 53215(147.102.131.64) ---> Destination Port : 21(147.102.40.15)
- Source Port : 21(147.102.40.15) ---> Destination Port : 53215(147.102.131.64)
- Source Port : 53224 (147.102.131.64) ---> Destination Port : 20(147.102.40.15)
- Source Port : 20(147.102.40.15) ---> Destination Port : 53224(147.102.131.64)

2.5 Σύμφωνα με την απάντηση στην προηγούμενη ερώτηση, ποιος είναι ο αριθμός θύρας TCP για την εγκατάσταση της σύνδεσης ελέγχου και ποιος για την για τη μεταφορά δεδομένων στην πλευρά του εξυπηρετητή κατά τον ενεργό τρόπο λειτουργίας του FTP;
Για τη σύνδεση ελέγχου έχουμε αριθμό θύρας 21 και για τη μεταφορά δεδομένων στην πλευρά του εξυπηρετήτη έχουμε αριθμό θύρας 20 κατά τον ενεργό τρόπο λειτουργίας.

2.6 Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η σύνδεση TCP για τη μεταφορά δεδομένων FTP;
Από την πλευρά του πελάτη για την μεταφορά δεδομένων από τον εξυπηρετητή προς τον πελάτη.

2.7 Καταγράψτε τις εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή. [Υπόδειξη: Χρησιμοποιήστε φίλτρο απεικόνισης ftp.request.command].
FTP commands :

- OPTS UTF8 ON
- USER anonymous
- PASS labuser@cn
- HELP

- PORT 147, 102, 131, 64, 207, 232
- NLST
- QUIT

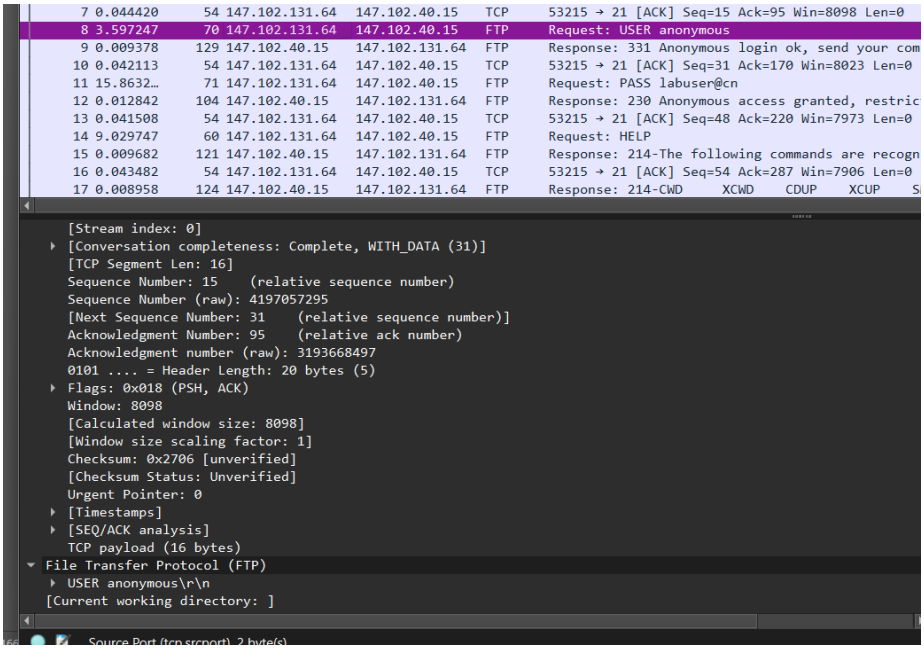
2.8 Εμφανίζονται αυτές οι εντολές FTP στις πληροφορίες αποσφαλμάτωσης (debugging) στην οθόνη του προγράμματος φλοιού ftp και με ποιον τρόπο;

```
C:\Users\koust>ftp -d edu-dy.cn.ntua.gr
Connected to edu-dy.cn.ece.ntua.gr.
220 ProFTPD 1.3.4a Server (ProFTPD Default Installation) [147.102.40.15]
---> OPTS UTF8 ON
200 UTF8 set to on
User (edu-dy.cn.ece.ntua.gr:(none)): anonymous
---> USER anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
---> PASS labuser@cn
230 Anonymous access granted, restrictions apply
```

2.9 Με ποια εντολή του πρωτοκόλλου FTP μεταφέρεται το όνομα χρήστη;

Με την εντολή USER anonymous.

2.10 Πόσα πακέτα IP χρειάζονται για να μεταφερθεί το όνομα του χρήστη;

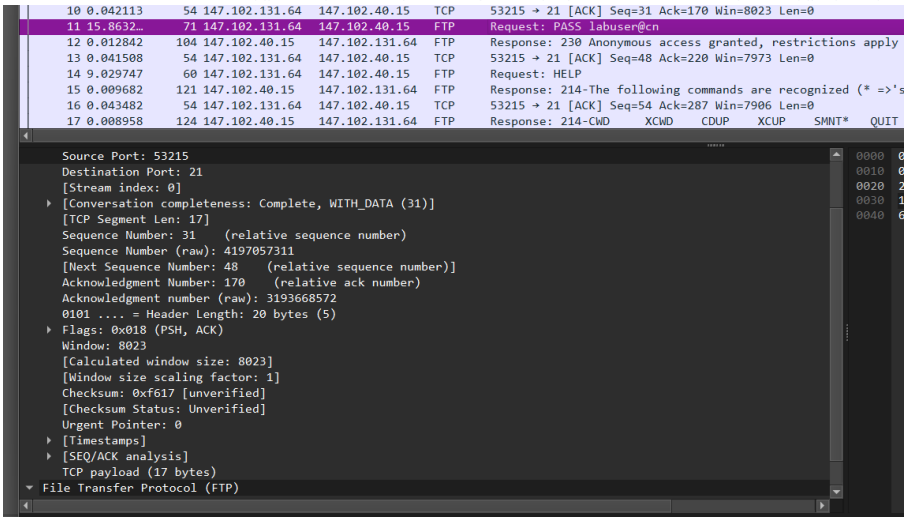


Απαιτείται ένα πακέτο το 8.

2.11 Με ποια εντολή του πρωτοκόλλου FTP μεταφέρεται ο κωδικός χρήστη;

Με τη εντολή PASS labuser@cn

2.12 Πόσα πακέτα IP χρειάζονται για να μεταφερθεί ο κωδικός του χρήστη;



Ένα πακέτο το 11.

2.13 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 : Δεν είναι κρυπτογραφημένα,

Διαφορά : Το FTP τα μεταφέρει ως ένα πακέτο, ενώ το TELNET ως πολλαπλά πακέτα ένα για κάθε χαρακτήρα.

2.14 Η εντολή help του προγράμματος φλοιού ftp μεταφράζεται σε εντολή του πρωτοκόλλου FTP;

```
ftp> help
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
ftp> remotehelp
---> HELP
214-The following commands are recognized (* =>'s unimplemented):
214-CWD     XCWD    CDUP    XCUP    SMNT*   QUIT    PORT    PASV
214-EPRT    EPSV    ALLO*   RNFR    RNTO    DELE    MDTM    RMD
214-XRMD    MKD     XMKD    PWD     XPWD    SIZE    SYST    HELP
214-NOOP    FEAT    OPTS    AUTH*   CCC*    CONF*   ENC*    MIC*
214-PBSZ*   PROT*   TYPE    STRU    MODE    RETR    STOR    STOU
214-APPE    REST    ABOR    USER    PASS    ACCT*   REIN*   LIST
214-NLST    STAT    SITE    MLSD    MLST
214 Direct comments to root@edu-dy.cn.ece.ntua.gr
ftp> ls
```

Όχι, δε μεταφράζεται ενώ η remotehelp μεταφράζεται στο FTP command HELP.

2.15 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.

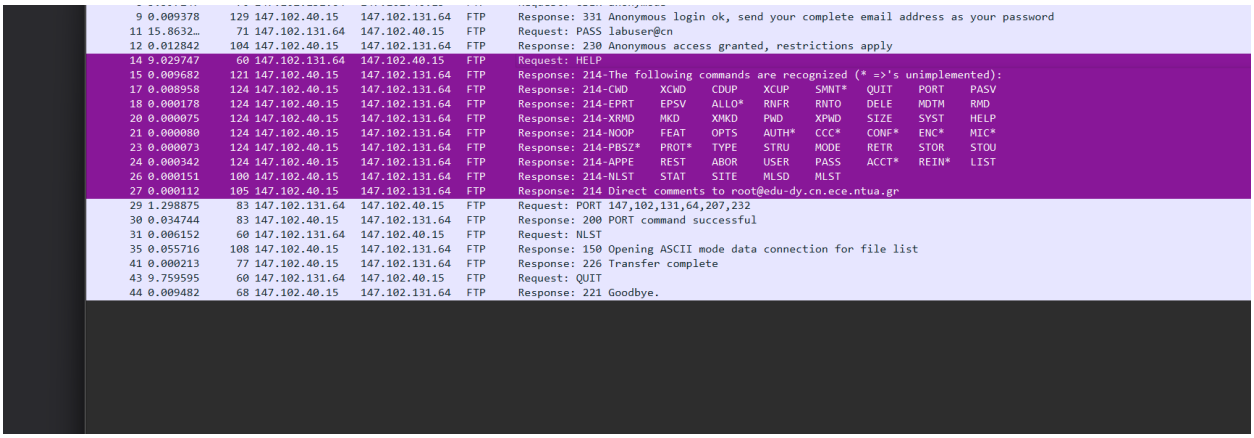
Δύο από όσες δεν υποστηρίζονται είναι οι:

- ACCT
- REIN

Εφαρμόστε τώρα το φίλτρο απεικόνισης ftp ώστε να εμφανισθεί όλος ο διάλογος (μεταξύ του υπολογιστή σας και του εξυπηρετητή) στη σύνδεση ελέγχου FTP.

2.16 Πόσα πακέτα IP, σχετικά με την εντολή remotehelp (rhelp), στάλθηκαν από τον υπολογιστή σας και πόσα από τον εξυπηρετητή;

Όπως φαίνεται στην παρακάτω εικόνα 10 πακέτα συνολικά αφορούσαν την εντολή remotehelp. Από αυτά μόνο ένα στάλθηκε από τον υπολογιστή μου προς τον εξυπηρετητή και τα άλλα εννέα στάλθηκαν από τον εξυπηρετητή προς τον υπολογιστή μου.



2.17 Πώς δηλώνει ο εξυπηρετητής ότι τελείωσε η αποστολή πακέτων σχετικών με την εντολή remotehelp (rhelp); [Υπόδειξη: Αναζητήστε τη λέξη hyphen στην παράγραφο 4.2 FTP Replies στο RFC 959.]

Υπάρχει whitespace αντί για παύλα "-" (hyphen) μετά το reply/response στο τελευταίο πακέτο

2.18 Εντοπίστε στη λίστα καταγεγραμμένων πακέτων του Wireshark το μήνυμα FTP που μεταφέρει την εντολή PORT. Τι παριστάνουν οι 4 πρώτοι δεκαδικοί αριθμοί;

Την IP του αποστολέα.

Οι δύο τελευταίοι δεκαδικοί αριθμοί της εντολής PORT ορίζουν τη θύρα που ανακοινώνει ο πελάτης στον εξυπηρετητή προκειμένου να λάβει εκεί δεδομένα από αυτόν, την οποία έχετε καταγράψει προηγουμένως στην απάντηση της ερώτησης 2.4.

2.19 Πώς προκύπτει αυτός ο αριθμός θύρας από τα δεδομένα της εντολής PORT; [Υπόδειξη: Συμβουλευτείτε το παράδειγμα που περιγράφεται στην ενότητα "Active FTP Example" στην ιστοσελίδα http://slacksite.com/other/ftp.html].

Προκύπτει ως εξής : προτελευταίος αριθμός*256 + τελευταίος αριθμός

Άρα, 207*256+232 = 53224 .

2.20 Ποια εντολή του πρωτοκόλλου FTP εμφανίζει τα περιεχόμενα του τρέχοντος καταλόγου;
Η εντολή NLST του πρωτοκόλλου FTP.

2.21 Γιατί η εντολή PORT του πρωτοκόλλου FTP προηγείται της εντολής της ερώτησης 2.20;
Γιατί πρέπει να έχει υπολογιστεί πρώτα η κατάλληλη πόρτα.

2.22 Σε ποια εντολή του πρωτοκόλλου FTP μεταφράζεται η εντολή bye του προγράμματος φλοιού ftp;
Στην εντολή QUIT.

2.23 Με ποιο μήνυμα αποκρίνεται ο εξυπηρετητής FTP στην εντολή bye του προγράμματος φλοιού ftp;
221 Goodbye

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

2.25 Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση των συνδέσεων TCP που αφορούν τις εντολές ελέγχου και μηνύματα δεδομένων του FTP;
Παρατηρούμε πως η απόλυση των συνδέσεων έγινε από την πλευρά του εξυπηρετητή όσον αφορά τα μηνύματα δεδομένων (πακέτο 36) και από την πλευρά του πελάτη(client) όσον αφορά τις εντολές ελέγχου FTP (πακέτο 45).

Στη συνέχεια θα παρατηρήσετε την κίνηση όταν χρησιμοποιείτε τον παθητικό τρόπο λειτουργίας του ftp. Αρχίστε μια νέα καταγραφή με το Wireshark και συνδεθείτε με anonymous ftp στο edu-dy.cn.ntua.gr χρησιμοποιώντας το γραφικό περιβάλλον του υπολογιστή σας. Σε Windows ανοίξτε τον File Explorer, κάντε κλικ στο Quick Access και γράψτε ftp://edu-dy.cn.ntua.gr. Σε περιβάλλον Linux, εάν δεν υπάρχει, εγκαταστήστε ένα πελάτη ftp όπως π.χ. FileZilla, δώστε edu-dy.cn.ntua.gr ως προορισμό και επιλέξτε anonymous πρόσβαση. Αφού εμφανισθεί στην οθόνη η λίστα των αρχείων του edu-dy.cn.ntua.gr, κλείστε το παράθυρο και σταματήστε την καταγραφή.

2.26 Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια τριπλών χειραψιών με τη σημαία SYN ενεργοποιημένη. Ποια είναι η σύνταξή του;
Display filter : ***tcp.flags.syn == 1***

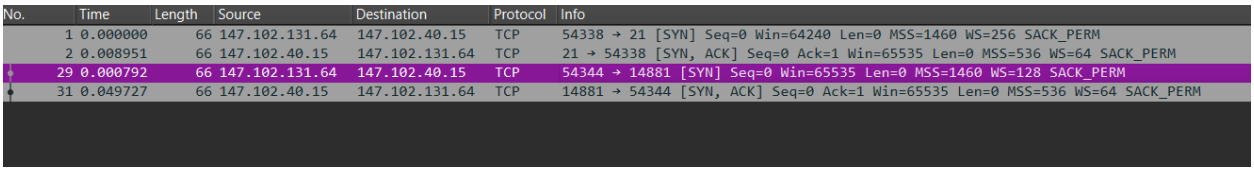
2.27 Καταγράψτε τις θύρες (πηγής και προορισμού) που χρησιμοποιούνται για την επικοινωνία FTP τόσο για τις εντολές ελέγχου όσο και για τη μεταφορά δεδομένων.
Source port : 54338(147.102.131.64) ---> Destination port : 21 (147.102.40.15)

Source port : 21(147.102.40.15) ---> Destination port : 54338(147.102.131.64)

Source port : 54344(147.102.131.64) ---> Destination port : 14881(147.102.40.15)

Source port : 14881(147.102.40.15) ---> Destination port : 54344(147.102.131.64)

2.28 Ποιος είναι ο αριθμός θύρας και από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η εγκατάσταση της σύνδεσης TCP για τη μεταφορά δεδομένων FTP;



No.	Time	Length	Source	Destination	Protocol	Info
1	0.000000	66	147.102.131.64	147.102.40.15	TCP	54338 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.008951	66	147.102.40.15	147.102.131.64	TCP	21 → 54338 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=64 SACK_PERM
29	0.000792	66	147.102.131.64	147.102.40.15	TCP	54344 → 14881 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM
31	0.049727	66	147.102.40.15	147.102.131.64	TCP	14881 → 54344 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=64 SACK_PERM

Στο πακέτο 29 ο client κάνει initiate τη σύνδεση TCP για τη μεταφορά δεδομένων FTP από το port 14881 του εξυπηρετητή στο port 54344 του client.

2.29 Καταγράψτε τις εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή. [Υπόδειξη: Χρησιμοποιήστε φίλτρο απεικόνισης ftp.request==1].

- AUTH TLS
- AUTH SSL
- USER anonymous
- PASS anonymous@example.com
- SYST
- FEAT
- OPTS UTF8 ON
- PWD
- TYPE I
- PASV
- MLSD

2.30 Ποιο όνομα και ποιος κωδικός χρήστη χρησιμοποιήθηκε;

Όνομα : anonymous
Κωδικός χρήστη : anonymous@example.com

2.31 Ποια εντολή του πρωτοκόλλου FTP χρησιμοποιήθηκε για την εμφάνιση της λίστας αρχείων;

MLSD

2.32 Τροποποιήστε το φίλτρο απεικόνισης ώστε να βλέπετε και τις αποκρίσεις στις εντολές FTP. Με ποιο μήνυμα αποκρίνεται ο εξυπηρετητής στην εντολή PASV;

Response: 227 Entering Passive Mode (147,102,40,15,58,33).

2.33 Στον παθητικό τρόπο λειτουργίας ο εξυπηρετητής δεν χρησιμοποιεί τη θύρα 20. Πώς προκύπτει ο αριθμός της θύρας για μεταφορά δεδομένων FTP που καταγράψατε στην ερώτηση 2.28 από τα στοιχεία της απάντησης στην ερώτηση 2.32;

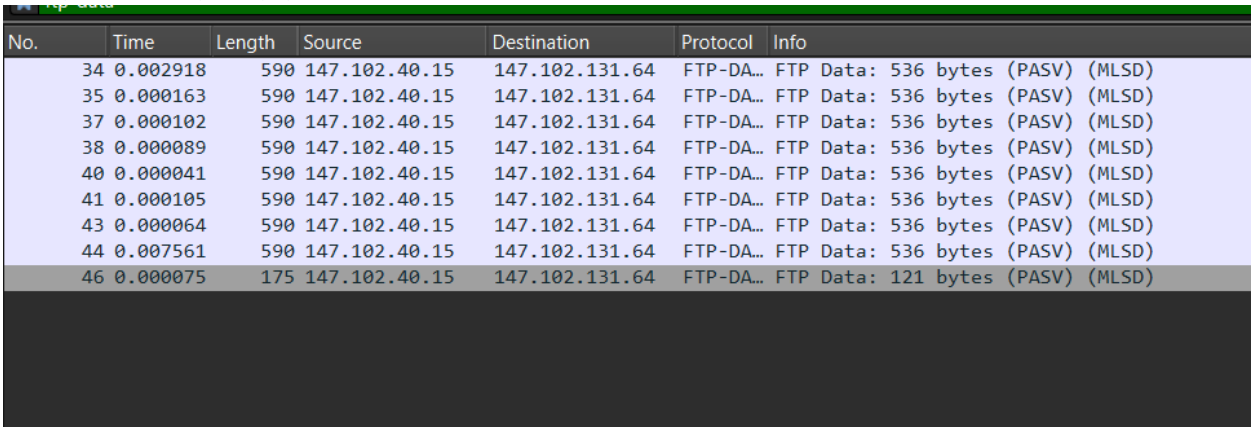
(Προτετελευταίος δεκαδικός)*256 + (τελευταίος δεκαδικός) = 58*256+33 = 14881

2.34 Πώς προκύπτει ο αριθμός θύρας της σύνδεσης TCP για μεταφορά δεδομένων FTP στην πλευρά του πελάτη;

Θεωρητικά θα είναι το port με αριθμό N+1 όπου N το port της σύνδεσης ελέγχου(54338). Στην πράξη θα είναι το πρώτο διαθέσιμο port μεγαλύτερου αριθμού από το N.

Εφαρμόστε τώρα το φίλτρο απεικόνισης ftp-data ώστε να εμφανισθεί η ανταλλαγή δεδομένων μέσω της σύνδεσης δεδομένων FTP.

2.35 Πόσα μηνύματα δεδομένων FTP στάλθηκαν από τον εξυπηρετητή και ποιο το μέγεθος των δεδομένων που μεταφέρουν;

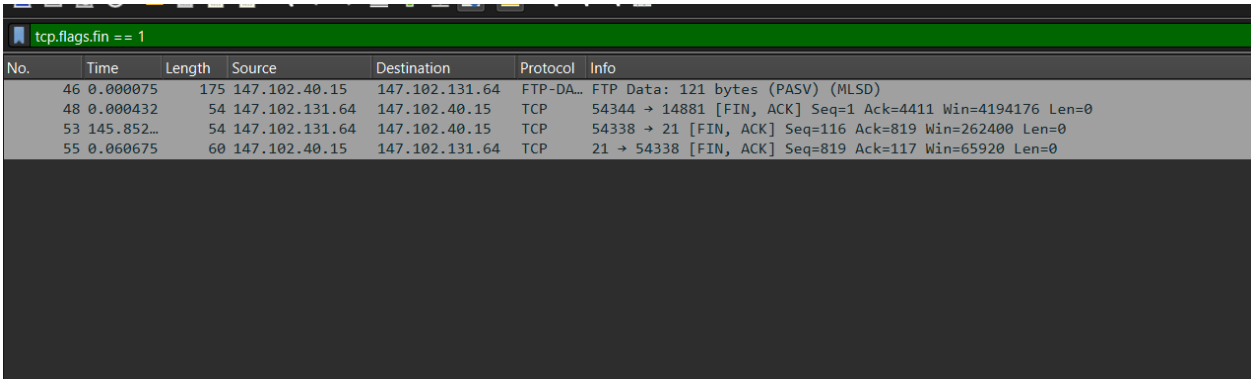


No.	Time	Length	Source	Destination	Protocol	Info
34	0.002918	590	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 536 bytes (PASV) (MLSD)
35	0.000163	590	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 536 bytes (PASV) (MLSD)
37	0.000102	590	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 536 bytes (PASV) (MLSD)
38	0.000089	590	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 536 bytes (PASV) (MLSD)
40	0.000041	590	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 536 bytes (PASV) (MLSD)
41	0.000105	590	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 536 bytes (PASV) (MLSD)
43	0.000064	590	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 536 bytes (PASV) (MLSD)
44	0.007561	590	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 536 bytes (PASV) (MLSD)
46	0.000075	175	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 121 bytes (PASV) (MLSD)

9 πακέτα μεγέθους 590 bytes ως πλαίσια με μέγεθος FTP-Data 536 bytes εκτός από το τελευταίο που έχει μέγεθος 175 bytes και 121 bytes FTP-Data.

2.36 Δικαιολογήστε το μέγεθος του πρώτου από τα προηγούμενα μηνύματα δεδομένων FTP.
Ινωρίζουμε πως ο σέρβερ 147.102.40.15 έχει MTU 576 bytes (άρα συνολικά με την προσθήκη του Ethernet Header 590 bytes).

2.37 Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση της σύνδεσης TCP που αφορά τη μεταφορά δεδομένων FTP;



tcp.flags.fin == 1

No.	Time	Length	Source	Destination	Protocol	Info
46	0.000075	175	147.102.40.15	147.102.131.64	FTP-DA…	FTP Data: 121 bytes (PASV) (MLSD)
48	0.000432	54	147.102.131.64	147.102.40.15	TCP	54344 → 14881 [FIN, ACK] Seq=1 Ack=4411 Win=4194176 Len=0
53	145.852…	54	147.102.131.64	147.102.40.15	TCP	54338 → 21 [FIN, ACK] Seq=116 Ack=819 Win=262400 Len=0
55	0.060675	60	147.102.40.15	147.102.131.64	TCP	21 → 54338 [FIN, ACK] Seq=819 Ack=117 Win=65920 Len=0

Από τον εξυπηρετητή γίνεται η απόλυση της σύνδεσης που αφορά τη μεταφορά δεδομένων FTP.

2.38 Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια με τη σημαία FIN ενεργοποιημένη. Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση της σύνδεσης TCP που αφορά τις εντολές ελέγχου FTP;
Από την πλευρά του πελάτη γίνεται η απόλυση της σύνδεσης TCP που αφορά τις εντολές ελέγχου FTP.

3. TFTP

Παραμένοντας συνδεδεμένοι στο εσωτερικό δίκτυο του ΕΜΠ, καταγράψτε με τη βοήθεια του Wireshark την κίνηση ενώ κάνετε χρήση της υπηρεσίας TFTP του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15). Όπως πριν, εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με το edu-dy.cn.ntua.gr. Για τη χρήση της υπηρεσίας TFTP στα Windows πληκτρολογήστε tftp edu-dy.cn.ntua.gr get rfc1350.txt σε ένα παράθυρο εντολών. Σε περιβάλλον Unix/Linux πληκτρολογήστε tftp edu-dy.cn.ntua και μετά get rfc1350.txt. Αφού σταματήσετε την καταγραφή κίνησης, εφαρμόστε το φίλτρο απεικόνισης για να παρατηρείτε μόνο την κίνηση (πακέτα IPv4) που σχετίζεται με το edu-dy.cn.ntua.gr. Οι νεότερες εκδόσεις του Wireshark δεν αποκωδικοποιούν όλα τα μηνύματα TFTP. Για να αποκωδικοποιηθούν όλα, επιλέξτε το πρώτο πακέτο που έστειλε ο edu-dy.cn.ntua.gr και με δεξί κλικ επιλέξτε το Decode As…. Στο παράθυρο που θα εμφανισθεί κάντε κλικ στο (none) στη στήλη Current και επιλέξτε ως πρωτόκολλο για αποκωδικοποίηση το TFTP.

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

3.2 Καταγράψτε όλους του τύπους μηνυμάτων TFTP που παρατηρήσατε.

- Read Request
- Data Packet
- Acknowledgment

3.3 Ποιο είναι το πεδίο της επικεφαλίδας TFTP που καθορίζει τον τύπο του μηνύματος και ποιο το μήκος του;
Το πεδίο Opcode με μήκος 2 bytes.

3.4 Καταγράψτε τις θύρες (πηγής και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την πρώτη επικοινωνία του πελάτη με τον εξυπηρετητή TFTP.
Source port : 53084(147.102.131.204) --> Destination port : 69(147.102.40.15)

3.5 Καταγράψτε τις θύρες (πηγής και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται κατά τη μεταφορά δεδομένων.
Source port : 23760(147.102.40.15) --> Destination port : 53084(147.102.131.204)

Source port : 53084(147.102.131.204)--> Destination port : 23760(147.102.40.15)

3.6 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής TFTP;
Η θύρα 69.

3.7 Πώς προκύπτουν οι αριθμοί θυρών που χρησιμοποιούνται κατά τη μεταφορά δεδομένων; [Υπόδειξη: Δείτε παράγραφο για το Initial Connection Protocol στο RFC 1350].
Σχετικά με τους αριθμούς θυρών γνωρίζουμε τα εξής. Προκειμένου να δημιουργηθεί μια σύνδεση, κάθε άκρο επιλέγει ένα Transfer Identifier (TID), το οποίο και θα χρησιμοποιείται κατά τη διάρκεια της σύνδεσης. Το κάθε άκρο της επικοινωνίας αυτής επιλέγει τυχαία μία από τις διαθέσιμες θύρες, έτσι ώστε να μειωθεί στο ελάχιστο η πιθανότητα τα 2 άκρα να επέλεξαν ίδια θύρα. Κάθε πακέτο που μεταδίδεται κατά τη σύνδεση αυτή φέρει και τα 2 TID των τερματικών της σύνδεσης, τα οποία και δίνει στο UPD πρωτόκολλο ως Source και Destination Port. Ο κόμβος που κάνει την αρχική αίτηση (εν προκειμένω ο δικός μας, ο οποίος στέλνει RRQ – Read Request), έχει επιλέξει

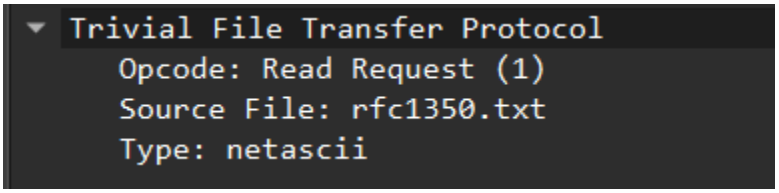
τυχαία τη θύρα που θα χρησιμοποιήσει και στέλνει το αρχικό αίτημα στη θύρα 69 στον εξυπηρετητή. Με τη σειρά του, ο σέρβερ αποκρίνεται, υπό κανονικές συνθήκες με το TID που εκείνος επέλεξε και που διατηρεί για το υπόλοιπο της σύνδεσης.

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

Το αρχείο rfc1350.txt μεταφέρεται σε ASCII.

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

Ο τρόπος μεταφοράς καθορίζεται στο πρώτο πακέτο και ειδικότερα στο πεδίο Type της επικεφαλίδας TFTP.



3.10 Το πρωτόκολλο μεταφοράς UDP είναι αναξιόπιστο καθώς δεν παρέχει μηχανισμό επιβεβαιώσεων, όπως το TCP. Πώς αντιμετωπίζει το πρόβλημα αυτό το TFTP;

Ενώ το UDP είναι αναξιόπιστο λόγω έλλειψης μηχανισμού επιβεβαιώσεων, το TFTP λύνει αυτό το πρόβλημα, καθώς για κάθε πακέτο που λαμβάνεται με έναν συγκεκριμένο (αύξοντα) αριθμό Block από το ένα άκρο, στέλνεται και ένα TFTP μήνυμα τύπου Acknowledgment για το Block από το άλλο άκρο με τον ίδιο αριθμό προκειμένου να σιγουρευτούμε πως ολοκληρώθηκε επιτυχώς η μεταφορά.

3.11 Ποια πληροφορία περιλαμβάνουν για τον σκοπό αυτό τα μηνύματα TFTP που μεταφέρουν δεδομένα;

Τον αριθμό του block που εντοπίζεται στο πεδίο Block της επικεφαλίδας TFTP.

3.12 Ποιο είναι το μέγεθος των μηνυμάτων TFTP (πλην του τελευταίου) που μεταφέρουν δεδομένα;

Κάθε μήνυμα TFTP που μεταφέρει δεδομένα από τον σέρβερ σε εμάς (πλην του τελευταίου) έχει μέγεθος 516 bytes (αφορά το μέγεθος της επικεφαλίδας TFTP και των δεδομένων TFTP, το συνολικό μέγεθος του πακέτου είναι 558 bytes).

3.13 Ποιο είναι το μέγεθος των δεδομένων που μεταφέρονται από αυτά τα μηνύματα TFTP;

512 bytes.

3.14 Δικαιολογήστε το μέγεθος πλαισίου Ethernet για τα παραπάνω μηνύματα TFTP.

Το πλαίσιο Ethernet έχει μήκος 544 + 14 bytes(Ethernet header) = 558 bytes.

Το μέγεθος αυτό οφείλεται στην MTU ενδιάμεσων κόμβων ή του κόμβου προορισμού.

MTU–(Ethernet header size+IP header size+UDP header size)=TFTP payload size = 514 bytes

3.15 Πώς αντιλαμβάνεται ο πελάτης το τέλος της μετάδοσης δεδομένων; [Υπόδειξη: Αναζητήστε τον όρο Normal Termination στο RFC 1350].

Ο πελάτης αντιλαμβάνεται το τέλος της μετάδοσης δεδομένων όταν λαμβάνει πακέτο με δεδομένα μεγέθους το πολύ έως 511 bytes.