

Όνοματεπώνυμο: Άγγελος Μητροκώτσας	Ομάδα: 6
Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2	Ημερομηνία: 11/ 12/ 2021
Διεύθυνση IP: 192.168.1.14	Διεύθυνση MAC: F8-63-3F-59-24-C8

Εργαστηριακή Άσκηση 8 TELNET, FTP και TFTP

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

1

1.1 TCP

1.2 192.168.1.14 → 147.102.40.15: Port 23

147.102.40.15 → 192.168.1.14: Port 51981

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.14	TCP	66	147.102.40.15	51981 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
2	0.011437	147.102.40.15	TCP	66	192.168.1.14	23 → 51981 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
3	0.000280	192.168.1.14	TCP	54	147.102.40.15	51981 → 23 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	0.078459	147.102.40.15	TELNET	57	192.168.1.14	Telnet Data ...
5	0.000245	192.168.1.14	TELNET	57	147.102.40.15	Telnet Data ...
6	0.026562	147.102.40.15	TELNET	62	192.168.1.14	Telnet Data ...
7	0.000246	192.168.1.14	TELNET	62	147.102.40.15	Telnet Data ...
8	0.016423	147.102.40.15	TFTP	72	192.168.1.14	Telnet Data ...

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767CB9} ^

> Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: Sercomm_f7:d3:40 (38:02:de:f7:d3:40)

> Internet Protocol Version 4, Src: 192.168.1.14, Dst: 147.102.40.15

▼ Transmission Control Protocol, Src Port: 51981, Dst Port: 23, Seq: 0, Len: 0

Source Port: 51981

Destination Port: 23

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Offset	Hex	ASCII
0000	38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00	8...@.c ?Y\$...E.
0010	00 34 cc 23 40 00 80 06 b1 74 c0 a8 01 0e 93 66	.4.#@... .t....f
0020	28 0f cb 0d 00 17 8d de 72 da 00 00 00 00 80 02	(..... r.....
0030	fa f0 2b 16 00 00 02 04 05 b4 01 03 03 08 01 01	..+.....

wireshark_Wi-FiS6CID1.pcapng | Packets: 58 · Displayed: 58 (100.0%) | Profile: Default

1.3 Η θύρα 23

1.4 telnet

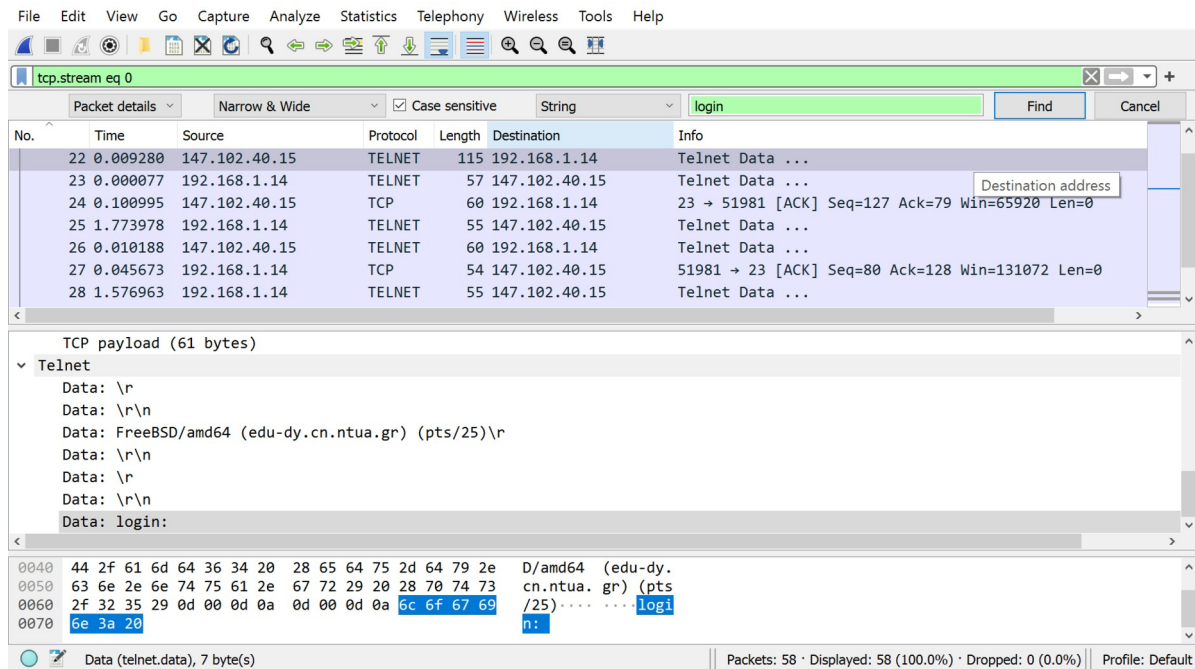
1.5 147.102.40.15 → 192.168.1.14: Do Echo

192.168.1.14 → 147.102.40.15: Will Echo

147.102.40.15 → 192.168.1.14: Don't Echo

147.102.40.15 → 192.168.1.14: Will Echo

192.168.1.14 → 147.102.40.15: Won't Echo



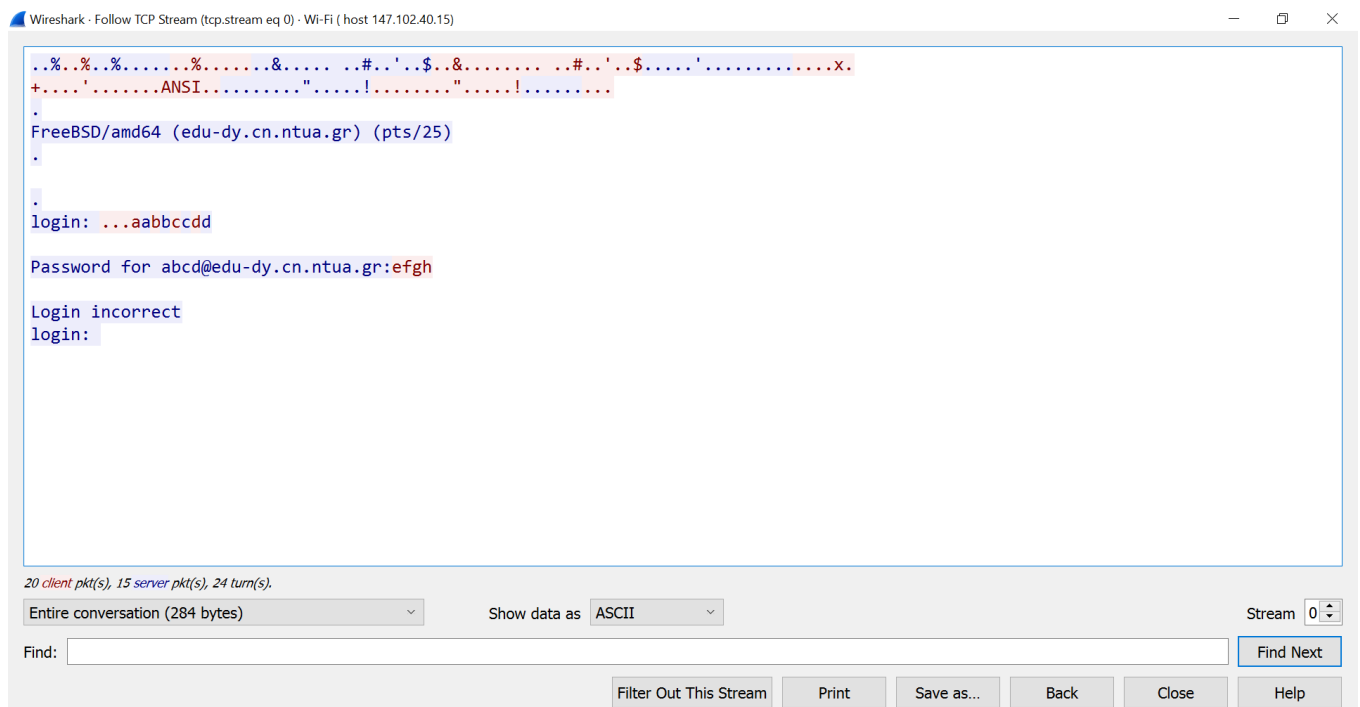
1.6 Ναι και ο υπολογιστής μου δέχεται να τους επαναλαμβάνει

1.7 Ναι, και ο υπολογιστής μου δέχεται να μην τους επαναλαμβάνει.

1.8 Ναι, προτίθεται

1.9 Ναι έχει προηγηθεί

1.10 Ο εξυπηρετητής επαναλαμβάνει κάθε γράμμα που πληκτρολογώ



1.11 Το φαινόμενο είναι λογικό καθώς ο edu-dy.cn.ntua.gr προτίθεται να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή μου

1.12 telnet and ip.src == 192.168.1.14

1.13 Χρειάζονται 4 πακέτα για τα γράμματα (1 για κάθε γραμμα/χαρακτήρα που πληκτρολογώ) και 1 για το ENTER (την αλλαγή γραμμής \r\n). Δηλαδή συνολικά 5 πακέτα

1.14 Ομοίως χρειάζονται 5 πακέτα, 1 για κάθε χαρακτήρα και 1 για την αλλαγή γραμμής

1.15 (το φίλτρο: telnet and ip.src == 147.102.40.15)

Όχι δεν στέλνει (Στέλνει μόνο την ηχώ των χαρακτήρων του login: abcd)

1.16 Όχι

1.17 Φαντάζομαι πως ο Telnet, για λόγους ασφαλείας δεν επαναλαμβάνει τον κωδικό του χρήστη

1.18 Προφανώς, απ ότι είδαμε, η ασφάλεια που παρέχει η υπηρεσία Telnet είναι δεν είναι επαρκής, καθώς, παρόλο που δεν επαναλαμβάνει τον κωδικό ασφαλείας του χρήστη, μπορεί ο οποιοσδήποτε να παρακολουθήσει την συνομιλία του υπολογιστή μου με τον εξυπηρετητή, άρα και να υποκλέψει ευαίσθητα στοιχεία

2

(assigned IP: 147.102.131.110)

2.1 ip host 147.102.40.15

2.2 Σημαίνει ότι είναι σε debug mode

2.3 TCP

2.4 Για τις εντολές ελέγχου:

Θύρα πηγής: 61304 Θύρα προορισμού: 21

Για τη μεταφορά δεδομένων:

Θύρα πηγής: 61316 Θύρα προορισμού: 20

2.5 Από την πλευρά του εξυπηρετητή

2.6 OPTS UTF8 ON, USER anonymous, PASS labuser@cn, HELP, PORT 147,102,131,110,239,132, NLST, QUIT

2.7 Ναι εμφανίζονται, με τον τρόπο που φαίνεται στα στιγμιότυπα οθόνης:

```

Administrator: Windows PowerShell
PS C:\Windows\system32> 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
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      MOTM      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
---> PORT 147,102,131,110,239,132
200 PORT command successful
---> NLST
150 Opening ASCII mode data connection for file list
FreeBSD10.4.ova
PCATTCP.exe
lab6.cap
router.ova
FreeBSD.ova
FreeBSD10.ova
firewall.ova
MagicAdb.exe
Asterisk.ova
TDIQ.exe
MacAddr2.exe
putty.exe
FreeBSD11.3.ova
psftp.exe
pcattcp.pcap
icmpv6.pcap
226 Transfer complete
ftp> bye
---> QUIT
221 Goodbye.
PS C:\Windows\system32>

```

2.8 Με την εντολή USER

2.9 Ένα

2.10 Με την εντολή PASS

2.11 Πάλι ένα

2.12 Η ομοιότητα τους είναι ότι κανένα από τα δύο δεν χρησιμοποιεί κρυπτογράφηση. Και μια διαφορά τους, είναι ότι με το telnet στέλνεται κάθε χαρακτήρας ξεχωριστά ενώ στο FTP πάνε όλοι μαζί (σε ένα πακέτο)

2.13 Οχι

2.14 PROT και AUTH

2.15 Από τον υπολογιστή μου στάλθηκε ένα, από τον εξυπηρετητή στάλθηκαν 9 πακέτα

2.16 Το δηλώνει με το να μη βάλει "-" (Hyphen) στην αρχή της γραμμής.

2.17 Την IPv4 διεύθυνση του υπολογιστή μου

2.18 Προκύπτει αν πολλαπλασιάσουμε το 5^ο byte με το 2⁸=256 και προσθέσουμε στο αποτέλεσμα το 6^ο

2.19 Η εντολή LIST.

2.20 Αυτό συμβαίνει επειδή γίνεται σύναψη νέας σύνδεσης (τριμερής χειραψίας με την θύρα δεδομένων).

2.21 Στην εντολή QUIT.

2.22 Με το μήνυμα "221 Goodbye."

2.23 tcp.flags.fin == 1

2.24 Τόσο για τις εντολές ελέγχου όσο και για τα μηνύματα δεδομένων,

2.25 (assigned IP: 147.102.131.222)

Για τις εντολές ελέγχου:

Θύρα πηγής: 58205 Θύρα προορισμού: 21

Για τη μεταφορά δεδομένων:

Θύρα πηγής: 58207 Θύρα προορισμού: 58304

2.26 USER anonymous, PASS IEUser@, opts utf8 on, PWD, CWD, TYPE A, PASV, LIST, QUIT (θα επρεπε να βγαλει QUIT αλλα δεν εβγαλε γιατι εκλεισα βιαστικά το παράθυρο εντολών πριν πληκτρολογήσω bye)

The screenshot shows a Wireshark packet capture of an FTP session. The packet list on the left shows several FTP requests from 147.102.131.222 to 147.102.40.15. The selected packet (No. 37) is an FTP LIST request. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol (Port 58206 to 21), and File Transfer Protocol (FTP). The FTP details show the current directory as '/', command response frames as 2, and command response bytes as 1026.

No.	Time	Source	Protocol	Length	Destination	Info
5	0.000000	147.102.131.222	FTP	68	147.102.40.15	Request: OPTS UTF8 ON
8	4.871024	147.102.131.222	FTP	70	147.102.40.15	Request: USER anonymous
11	7.169628	147.102.131.222	FTP	72	147.102.40.15	Request: PASS labuser@cn.
19	4.430639	147.102.131.222	FTP	70	147.102.40.15	Request: USER anonymous
22	0.193566	147.102.131.222	FTP	68	147.102.40.15	Request: PASS IEUser@
25	0.190130	147.102.131.222	FTP	68	147.102.40.15	Request: opts utf8 on
28	0.211810	147.102.131.222	FTP	59	147.102.40.15	Request: PWD
31	0.074637	147.102.131.222	FTP	61	147.102.40.15	Request: CWD /
34	0.033734	147.102.131.222	FTP	62	147.102.40.15	Request: TYPE A
37	0.091458	147.102.131.222	FTP	60	147.102.40.15	Request: PASV
43	0.406616	147.102.131.222	FTP	60	147.102.40.15	Request: LIST

2.27 Χρησιμοποίησε το anonymous ως όνομα χρήστη και το labuser@cn. ως κωδικό.

2.28 Την εντολή LIST

2.29 227 Entering Passive Mode (147,102,40,15,227,192)

The screenshot shows a Wireshark packet capture of an FTP session. The packet list on the left shows several FTP responses from 147.102.40.15 to 147.102.131.222. The selected packet (No. 38) is an FTP LIST response. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol (Port 21 to 58206), and File Transfer Protocol (FTP). The FTP details show the response as 227 Entering Passive Mode (147,102,40,15,227,192).

Time	Source	Protocol	Length	Destination	Info
0.211510	147.102.40.15	FTP	74	147.102.131.222	Response: 200 UTF8 set to on
0.000300	147.102.131.222	FTP	59	147.102.40.15	Request: PWD
0.073857	147.102.40.15	FTP	88	147.102.131.222	Response: 257 "/" is the current directory
0.000780	147.102.131.222	FTP	61	147.102.40.15	Request: CWD /
0.032764	147.102.40.15	FTP	82	147.102.131.222	Response: 250 CWD command successful
0.000970	147.102.131.222	FTP	62	147.102.40.15	Request: TYPE A
0.090542	147.102.40.15	FTP	73	147.102.131.222	Response: 200 Type set to A
0.000916	147.102.131.222	FTP	60	147.102.40.15	Request: PASV
0.199862	147.102.40.15	FTP	106	147.102.131.222	Response: 227 Entering Passive Mode (147,102,40,15,227,192).
0.206754	147.102.131.222	FTP	60	147.102.40.15	Request: LIST
0.202899	147.102.40.15	FTP	108	147.102.131.222	Response: 150 Opening ASCII mode data connection for file list
0.268971	147.102.40.15	FTP	77	147.102.131.222	Response: 226 Transfer complete

3 (assigned IP: 147.102.131.156)

3.1 UDP

3.2 Θύρα πηγής: 60628, Θύρα προορισμού: 69

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	147.102.131.156	TFTP	65	147.102.40.15	Read Request, File: rfc1350.txt, Transfer type: netas
2	0.058357	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 1
3	0.000550	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 1
4	0.013005	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 2
5	0.000283	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 2
6	0.072142	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 3
7	0.000382	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 3
8	0.121575	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 4
9	0.000208	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 4
10	0.019755	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 5

> Frame 1: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface \Device\NPF_{50A5BB09-D0AB-46DB-AD4F-BB793E23887D},
 > Ethernet II, Src: 00:ff:50:a5:bb:09 (00:ff:50:a5:bb:09), Dst: 00:ff:51:a5:bb:09 (00:ff:51:a5:bb:09)
 > Internet Protocol Version 4, Src: 147.102.131.156, Dst: 147.102.40.15
 > User Datagram Protocol, Src Port: 60628, Dst Port: 69
 > Trivial File Transfer Protocol

0000 00 ff 51 a5 bb 09 00 ff 50 a5 bb 09 08 00 45 00 ..Q.... P.....E.
 0010 00 33 39 5d 00 00 08 11 2e e5 93 66 83 9c 93 66 .39].... .f...f
 0020 28 0f ec d4 00 45 00 1f 5f 15 00 01 72 66 63 31 (....E... ..rfc1
 0030 33 35 30 2e 74 78 74 00 6e 65 74 61 73 63 69 69 350.txt: netascii
 0040 00

wireshark_EthernetMH26D1.pcapng | Packets: 101 · Displayed: 101 (100.0%) | Profile: Default

3.3 Θύρα πηγής(εξυπηρετητής): 34559, Θύρα προορισμού (πελάτης): 58825

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	147.102.131.156	TFTP	65	147.102.40.15	Read Request, File: rfc1350.txt, Transfer type: netas
2	0.058357	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 1
3	0.000550	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 1
4	0.013005	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 2
5	0.000283	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 2
6	0.072142	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 3
7	0.000382	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 3
8	0.121575	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 4
9	0.000208	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 4
10	0.019755	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 5

> Frame 2: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface \Device\NPF_{50A5BB09-D0AB-46DB-AD4F-BB793E23887D},
 > Ethernet II, Src: 00:ff:51:a5:bb:09 (00:ff:51:a5:bb:09), Dst: 00:ff:50:a5:bb:09 (00:ff:50:a5:bb:09)
 > Internet Protocol Version 4, Src: 147.102.40.15, Dst: 147.102.131.156
 > User Datagram Protocol, Src Port: 40733, Dst Port: 60628
 > Trivial File Transfer Protocol
 > Data (512 bytes)

0000 00 ff 50 a5 bb 09 00 ff 51 a5 bb 09 08 00 45 00 ..P.... Q.....E.
 0010 02 20 58 78 00 00 3e 11 4f dd 93 66 28 0f 93 66 . Xx...> .O..f...f
 0020 83 9c 9f 1d ec d4 02 0c 91 24 00 03 00 01 0d 0a \$......
 0030 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 4e 65 74 77 6f 72Networ
 0040 6b 20 57 6f 72 6b 69 6e 67 20 47 72 6f 75 70 20 k Workin g Group

wireshark_EthernetMH26D1.pcapng | Packets: 101 · Displayed: 101 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

3.4 H 69

3.5 Είναι οι πρώτες διαθέσιμες θύρες (η θύρα προορισμού είναι η θύρα με την οποία επικοινωνήσε αρχικά ο υπολογιστής μου)

3.6 Με ASCII

3.7 Στο πρώτο μήνυμα που στέλνει ο πελάτης στον εξυπηρετητή και κάνει το request (καθορίζεται στο πεδίο Type με τιμή netascii)

The screenshot shows a Wireshark capture of a TFTP session. The packet list shows a Read Request (Block 1) from 147.102.131.156 to 147.102.40.15. The details pane shows the Trivial File Transfer Protocol section with the following information:

- Opcode: Read Request (1)
- Source File: rfc1350.txt
- Type: netascii

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column highlights the text "rfc1350.txt" and "netascii".

3.8 Read Request, Data Packet και Acknowledgement.

3.9 Χωρίζει τα πακέτα με ένα αριθμό Block και για κάθε ένα που στέλνει ο εξυπηρετητής, ο πελάτης απαντά με ένα πακέτο τύπου Acknowledgement με το αντίστοιχο αριθμό Block

3.10 Ο τύπος Acknowledgement στο πεδίο επικεφαλίδας Opcode

3.11 Ολόκληρο το μήνυμα TFTP έχει μέγεθος 516 bytes (512bytes των Data συν 4 της επικεφαλίδας)

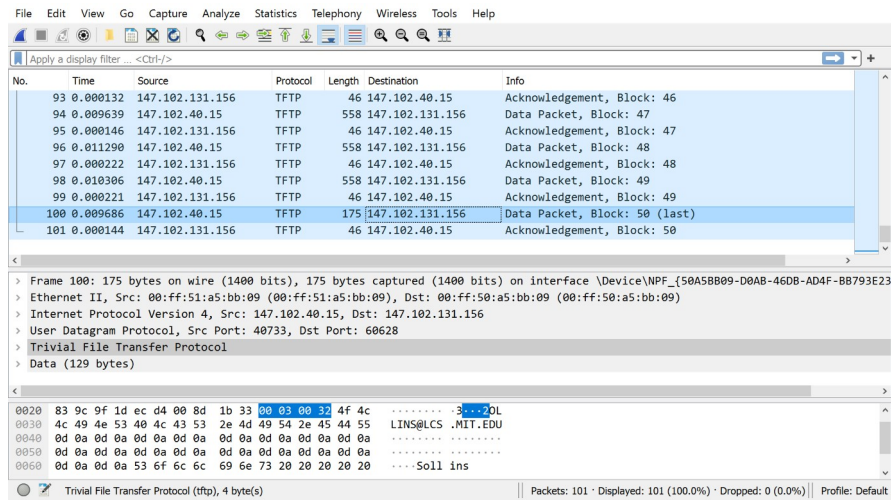
The screenshot shows a Wireshark capture of a TFTP session. The packet list shows a Read Request (Block 1) from 147.102.131.156 to 147.102.40.15. The details pane shows the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Trivial File Transfer Protocol sections. The Trivial File Transfer Protocol section shows the following information:

- Source File: rfc1350.txt
- Type: netascii
- Block: 1

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column highlights the text "rfc1350.txt" and "netascii".

3.12 512 bytes

3.13 Ο πελάτης το αντιλαμβάνεται με το που λάβει πακέτο TFTP που έχει λιγότερα από 512 bytes δεδομένων, και δίπλα από τον αριθμό του Block γράφει (Last)



Wireshark packet capture showing TFTP traffic. The packet list pane displays the following packets:

No.	Time	Source	Protocol	Length	Destination	Info
93	0.000132	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 46
94	0.009639	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 47
95	0.000146	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 47
96	0.011290	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 48
97	0.000222	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 48
98	0.010306	147.102.40.15	TFTP	558	147.102.131.156	Data Packet, Block: 49
99	0.000221	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 49
100	0.009686	147.102.40.15	TFTP	175	147.102.131.156	Data Packet, Block: 50 (last)
101	0.000144	147.102.131.156	TFTP	46	147.102.40.15	Acknowledgement, Block: 50

The packet details pane for packet 100 shows the following structure:

- Frame 100: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface \Device\NPF_{50A5BB09-D0AB-46DB-AD4F-BB793E23}
- Ethernet II, Src: 00:ff:51:a5:bb:09 (00:ff:51:a5:bb:09), Dst: 00:ff:50:a5:bb:09 (00:ff:50:a5:bb:09)
- Internet Protocol Version 4, Src: 147.102.40.15, Dst: 147.102.131.156
- User Datagram Protocol, Src Port: 40733, Dst Port: 60628
- Trivial File Transfer Protocol
- Data (129 bytes)

The packet bytes pane shows the raw data of the packet, with the last 4 bytes highlighted in blue, indicating the end of the data block.