

Όνοματεπώνυμο: Άγγελος Μητροκώτσας	Ομάδα: 6
Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2	Ημερομηνία: 5/12/2021
Διεύθυνση IP: 192.168.1.14	Διεύθυνση MAC: F8-63-3F-59-24-C8

Εργαστηριακή Άσκηση 7

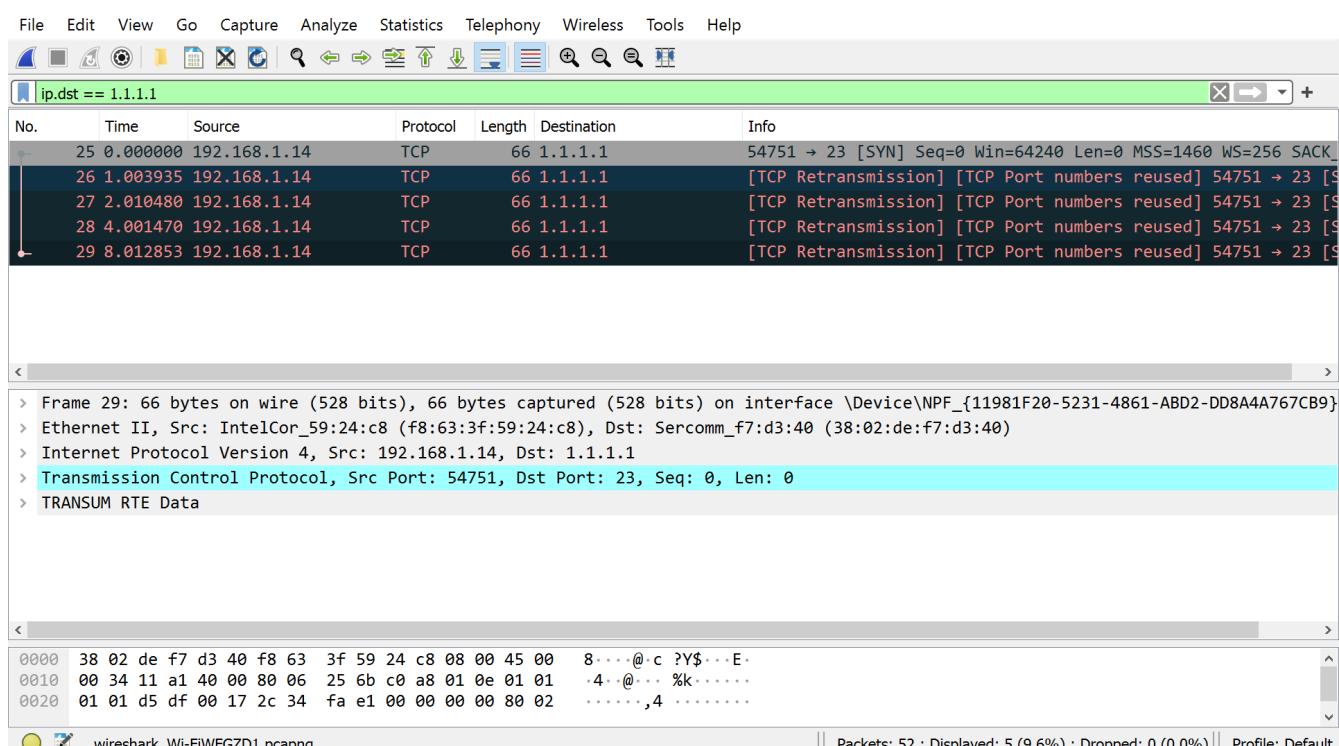
Πρωτόκολλα TCP και UDP

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

1

1.1 host 192.168.1.14

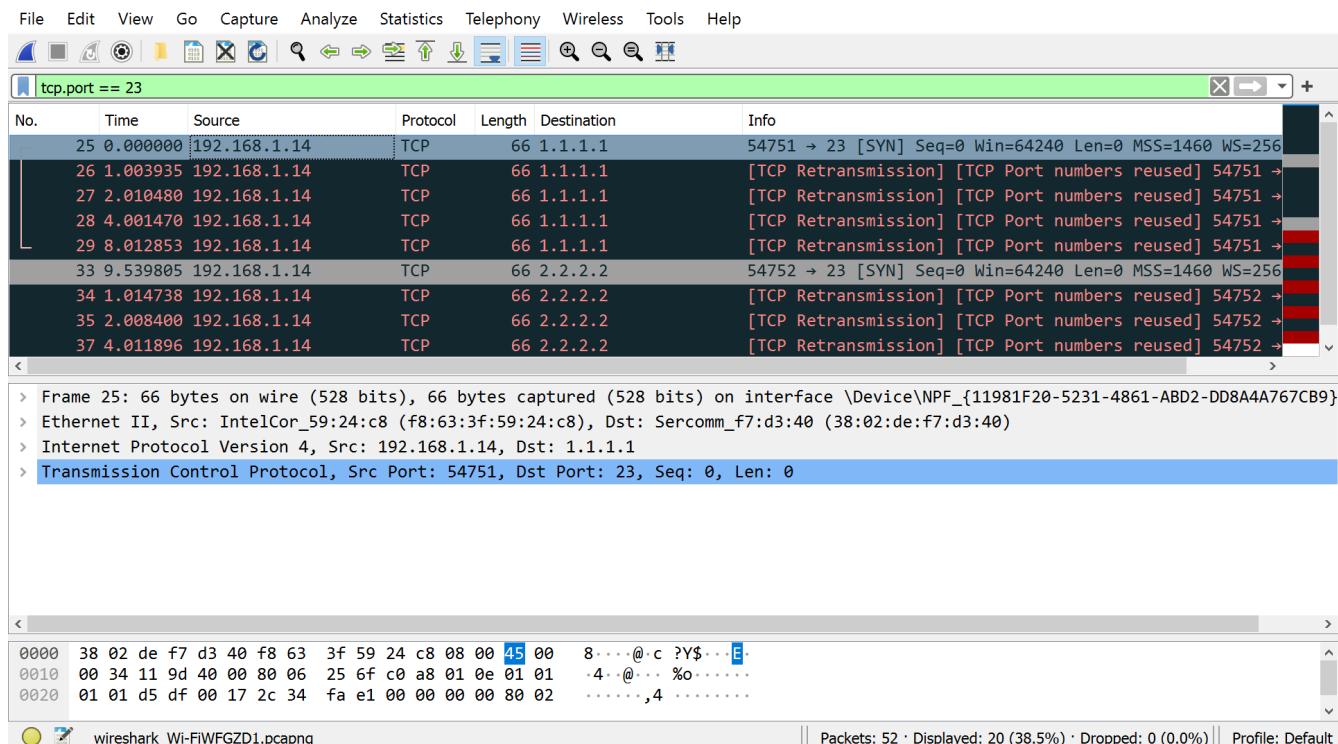
1.2 ip.dst == <IPv4 address>



1.3 Στη θυρα 23 για telnet protocol

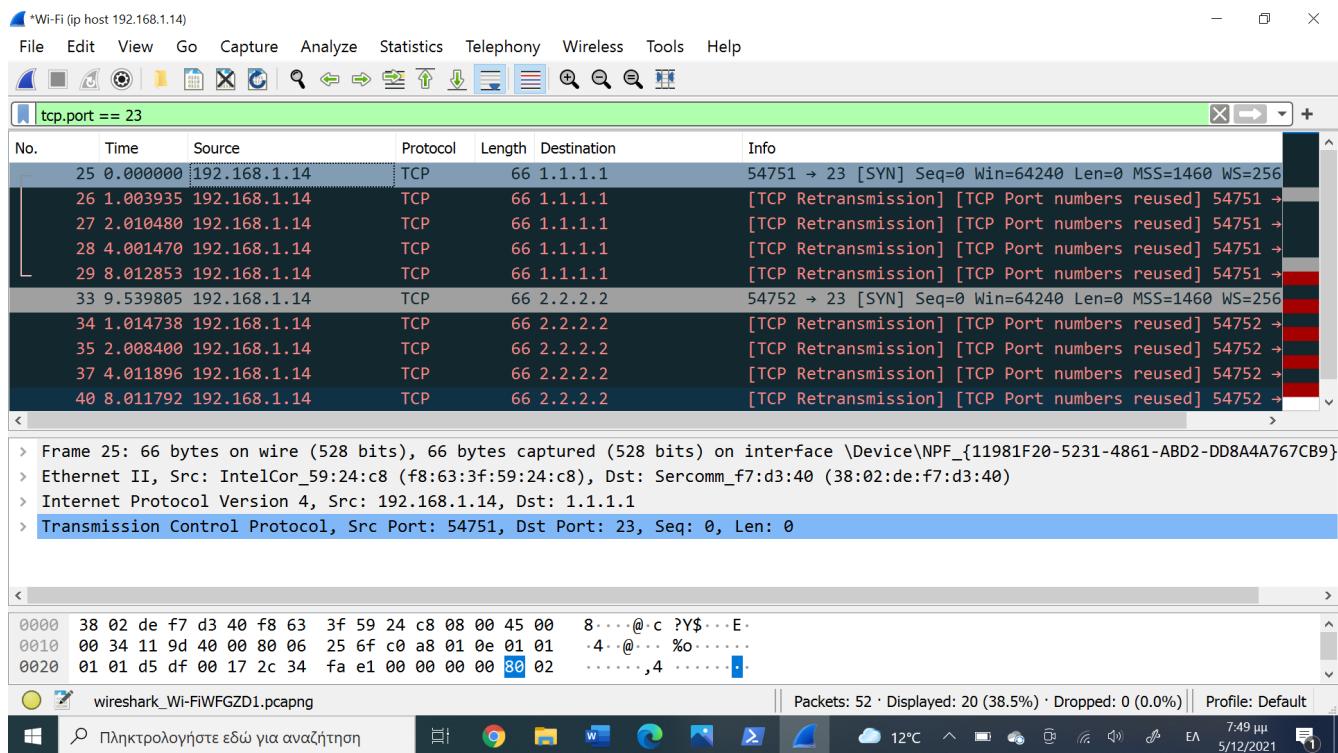
1.4 tcp.port == 23

1.5 H SYN



1.6 5 προσπαθειες σε κάθε περιπτωση

1.7 Από 1 sec για τα 3 πρωτα, 2 sec από το 3^o στο 4^o, 4 sec από το 4^o στο 5^o.



1.8 Είναι παρόμοια, σχεδόν ολόιδια.

1.9 Μόνο το πρώτο βήμα (το SYN)

1.10 Εγκαταλείπει την προσπάθεια

1.11 tcp.port == 23 and ip.addr == 147.102.40.1 (αρκεί και σκέτο ip.addr == 147.102.40.1 σε αυτή την περιπτωση)

1.12 Κανει 5 προσπάθειες, την εκκίνηση της εγκατάστασης της σύνδεσης TCP (φαίνεται από τη σημαία SYN) και 4 Retransmissions.

tcp.port==23 and ip.addr == 147.102.40.1

No.	Time	Source	Protocol	Length	Destination	Info
43	0.000000	192.168.1.14	TCP	66	147.102.40.1	54753 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
44	0.016036	147.102.40.1	TCP	54	192.168.1.14	23 → 54753 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
45	0.510321	192.168.1.14	TCP	66	147.102.40.1	[TCP Retransmission] [TCP Port numbers reused] 54753 → 23 [S
46	0.014970	147.102.40.1	TCP	54	192.168.1.14	23 → 54753 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47	0.512889	192.168.1.14	TCP	66	147.102.40.1	[TCP Retransmission] [TCP Port numbers reused] 54753 → 23 [S
48	0.024155	147.102.40.1	TCP	54	192.168.1.14	23 → 54753 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	0.507155	192.168.1.14	TCP	66	147.102.40.1	[TCP Retransmission] [TCP Port numbers reused] 54753 → 23 [S
50	0.014579	147.102.40.1	TCP	54	192.168.1.14	23 → 54753 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
51	0.501008	192.168.1.14	TCP	66	147.102.40.1	[TCP Retransmission] [TCP Port numbers reused] 54753 → 23 [S
52	0.014153	147.102.40.1	TCP	54	192.168.1.14	23 → 54753 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 44: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767CB9}
> Ethernet II, Src: Sercomm_f7:d3:40 (38:02:de:f7:d3:40), Dst: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
> Internet Protocol Version 4, Src: 147.102.40.1, Dst: 192.168.1.14
> Transmission Control Protocol, Src Port: 23, Dst Port: 54753, Seq: 1, Ack: 1, Len: 0

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 00 .c?Y\$.8. . .@. .E.
0010 00 28 00 00 40 00 39 06 c4 b2 93 66 28 01 c0 a8 .(.@ 9. . .f(...
0020 01 0e 00 17 d5 e1 00 00 00 00 45 ab 6e a7 50 14E.n.P.

Source or Destination Port: Unsigned integer, 2 bytes || Packets: 52 · Displayed: 10 (19.2%) · Dropped: 0 (0.0%) || Profile: Default

1.13 Ο υπολογιστής μου στη Γ περίπτωση έλαβε απάντηση από την 147.102.40.1 και εχουμε και το 2^o βημα της τριτλης χειραψίας (το acknowledgement, ACK)

1.14 Reserved: 0, Nonce: 0, Congestion Window Reduced (CWR): 0, ECN-Echo: 0, Urgent: 0, **Acknowledgment: 1**, Push: 0, **Reset: 1**, Syn: 0, Fin: 0

(Οπου εχω 0 είναι Not Set, ενώ όπου έχω 1 είναι Set)

tcp.port==23 and ip.addr == 147.102.40.1

No.	Time	Source	Protocol	Length	Destination	Info
43	0.000000	192.168.1.14	TCP	66	147.102.40.1	54753 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
44	0.016036	147.102.40.1	TCP	54	192.168.1.14	23 → 54753 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
45	0.510321	192.168.1.14	TCP	66	147.102.40.1	[TCP Retransmission] [TCP Port numbers reused] 54753 → 23 [S

> Flags: 0x014 (RST, ACK)

- 000. = Reserved: Not set
-0 = Nonce: Not set
- 0... = Congestion Window Reduced (CWR): Not set
-0.. = ECN-Echo: Not set
-0. = Urgent: Not set
-1 = Acknowledgment: Set
- 0... = Push: Not set
-1.. = Reset: Set
-0. = Syn: Not set
-0 = Fin: Not set

[TCP Flags:A.R..]
Window: 0
[Calculated window size: 0]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xa88677 [unverified]

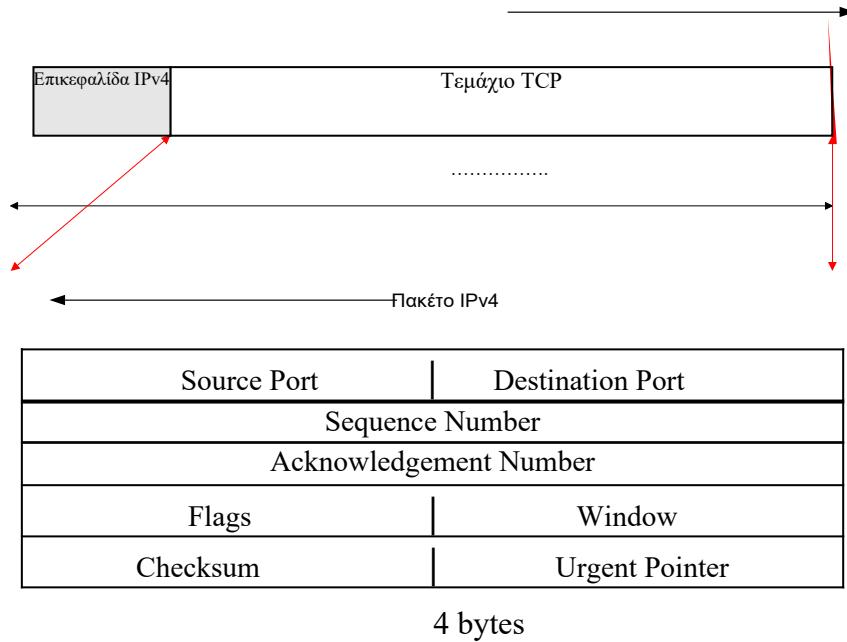
0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 00 .c?Y\$.8. . .@. .E.
0010 00 28 00 00 40 00 39 06 c4 b2 93 66 28 01 c0 a8 .(.@ 9. . .f(...
0020 01 0e 00 17 d5 e1 00 00 00 00 45 ab 6e a7 50 14E.n.P.

Ethernet (eth), 14 byte(s) || Packets: 52 · Displayed: 10 (19.2%) · Dropped: 0 (0.0%) || Profile: Default

1.15 Η σημαία Reset

1.16 Μέγεθος Επικεφαλίδας: 20 bytes, Μέγεθος Περιεχομένων: 0 bytes.

1.17 Source Port: 2 bytes, Destination Port: 2 bytes, Sequence Number: 4 bytes, Acknowledgment Number: 4 bytes, Flags: 2 bytes, Window: 2 bytes, Checksum: 2 bytes, Urgent Pointer: 2 bytes

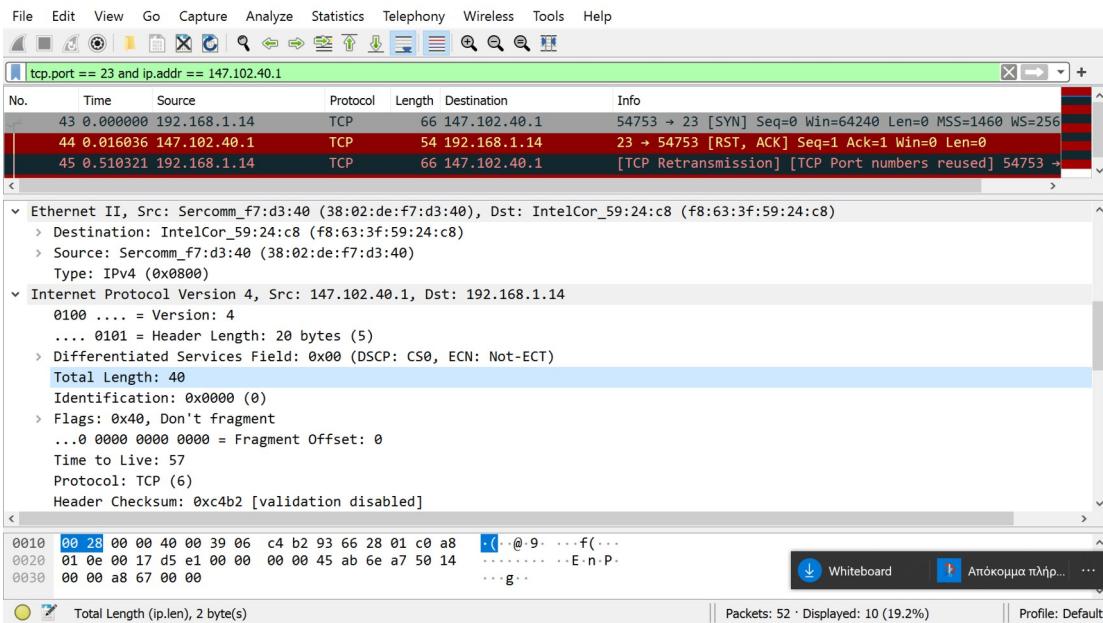


1.18 Το όνομα του πεδίου είναι Data Offset, ενώ το ίδιο πεδίο στο Wireshark έχει όνομα Header Length.

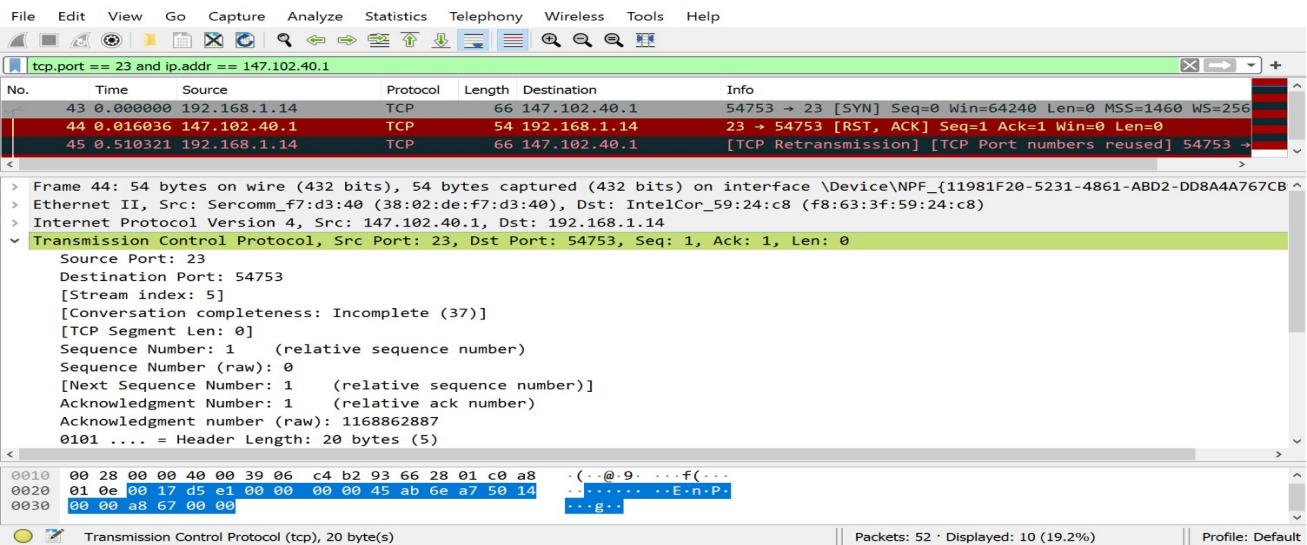
1.19 Η η τιμή του πεδίου στο Wireshark είναι 5 (0x0101). Η τιμή υπολογίζεται ως $4 \cdot 5 = 20$ bytes.

1.20 'Όχι

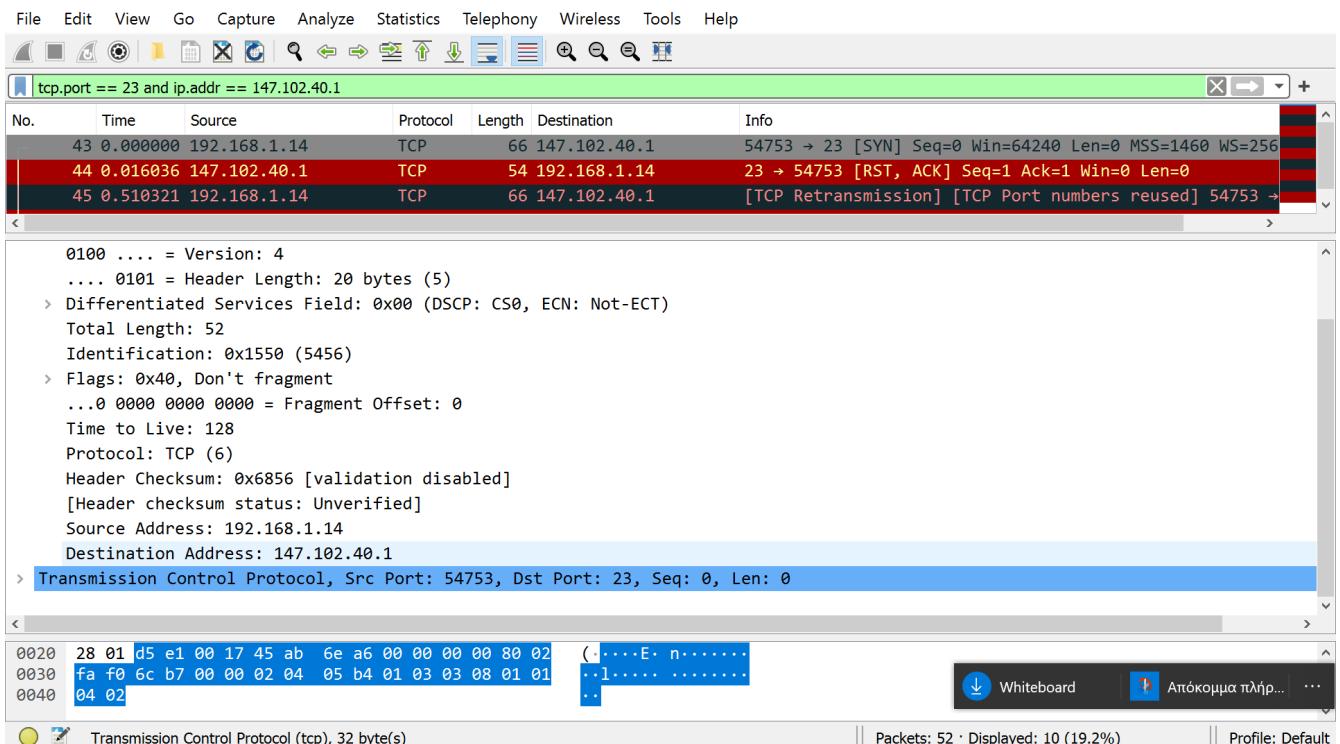
1.21 Βρίσκω από το πεδίο Total Length του IP Header βλέπουμε ότι έχει συνολικό μήκος 40 bytes



και βρίσκω το μήκος του τεμαχίου TCP αν αφαιρέσουμε τα μήκη των επικεφαλίδων Header Length από την IP επικεφαλίδα και Data Offset ή Header Length από την TCP επικεφαλίδα



1.22 32 bytes.



1.23 Ναι υπάρχει διαφορά. Αυτό οφείλεται στο πεδίο Options, μεγέθους 24 bytes, που περιέχει η επικεφαλίδα του TCP πακέτου. Στο πεδίο αυτό βρίσκονται πληροφορίες για την σύναψη της σύνδεσης μεταξύ των κόμβων.

2

```
[Administrator: Windows PowerShell]
PS C:\Windows\system32> ftp edu-dy.cn.ntua.gr
Connected to edu-dy.cn.ece.ntua.gr.
220 ProFTPD 1.3.44 Server (ProFTPD Default Installation) [147.102.40.15]
200 UTF8 set to on
User (edu-dy.cn.ece.ntua.gr:(none)): Anonymous
331 Password required for Anonymous
Password:
530 Login incorrect.
Login failed.
Ftp> clear
Invalid command.
Ftp> bye
221 Goodbye.
PS C:\Windows\system32> ftp edu-dy.cn.ntua.gr
Connected to edu-dy.cn.ece.ntua.gr.
220 ProFTPD 1.3.44 Server (ProFTPD Default Installation) [147.102.40.15]
200 UTF8 set to on
User (edu-dy.cn.ece.ntua.gr:(none)): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Ftp> bin
200 Type set to I
Ftp> lcd desktop
Invalid command.
Ftp> lcd desktop
desktop: File not found
Ftp> lcd desktop
desktop: File not found
Ftp> lcd Desktop
Desktop: File not found
Ftp> lcd Επίπεδα Εργασιών
lcd local directory.
Ftp> get PCATTCP.exe
200 PORT command successful
150 Opening BINARY mode data connection for PCATTCP.exe (61440 bytes)
226 Transfer complete
Ftp: 61440 bytes received in 0.07Seconds 819.20Kbytes/sec.
Ftp> bye
221 Goodbye.
PS C:\Windows\system32>
```

2.1 ip host edu-dy.cn.ntua.gr

2.2 Στην Port 21

2.3 Με την Port 20 (FTP (Data Tranfer))

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Protocol	Length	Destination	Info
14	13.1016...	192.168.1.14	FTP	62	147.102.40.15	Request: TYPE I
15	0.015145	147.102.40.15	FTP	73	192.168.1.14	Response: 200 Type set to I
16	0.042989	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=74 Ack=239 Win=7954 Len=0
17	46.9800...	192.168.1.14	FTP	80	147.102.40.15	Request: PORT 192,168,1,14,216,32
18	0.013304	147.102.40.15	FTP	83	192.168.1.14	Response: 200 PORT command successful
19	0.005572	192.168.1.14	FTP	72	147.102.40.15	Request: RETR PCATTCP.exe
20	0.013819	147.102.40.15	TCP	74	192.168.1.14	20 → 55328 [SYN] Seq=0 Win=65535 Len=0 MSS=536 WS=64 S
21	0.000114	192.168.1.14	TCP	66	147.102.40.15	55328 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=64 S
22	0.014313	147.102.40.15	TCP	60	192.168.1.14	20 → 55328 [ACK] Seq=1 Ack=1 Win=65920 Len=0
23	0.000000	147.102.40.15	FTP	125	192.168.1.14	Response: 150 Opening BINARY mode data connection for
24	0.000000	147.102.40.15	FTP-DA...	1126	192.168.1.14	FTP Data: 1072 bytes (PORT) (RETR PCATTCP.exe)

Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767CB^

> Interface id: 0 (\Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767CB9})

Encapsulation type: Ethernet (1)

Arrival Time: Dec 6, 2021 11:54:46.692458000 Χειμερινή ώρα GTB

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1638784486.692458000 seconds

[Time delta from previous captured frame: 0.013819000 seconds]

0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 00 .c?Y\$·8. ···@·E·

0010 00 3c 27 c8 40 00 39 06 9c c8 93 66 28 0f c0 a8 .<'@·9. ···f(...

0020 01 0e 00 14 d8 20 d9 14 a0 35 00 00 00 00 a0 02 5.....

Packets: 82 · Displayed: 82 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

2.4 tcp.port == 21

2.5 3 τεμάχια.

2.6 SYN, SYN ACK και ACK αντίστοιχα για κάθε τεμάχιο.

2.7 Είναι 32 bytes, 32 bytes και 20 bytes αντίστοιχα

2.8 Και τα 3 τεμάχια δεν έχουν δεδομένα (Μεγεθος: 0)

2.9 0.013337 sec

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.14	TCP	66	147.102.40.15	55326 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 S
2	0.013370	147.102.40.15	TCP	66	192.168.1.14	21 → 55326 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
3	0.013456	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.039087	147.102.40.15	FTP	128	192.168.1.14	Response: 220 ProFTPD 1.3.4a Server (ProFTPD Default
5	0.047226	192.168.1.14	FTP	68	147.102.40.15	Request: OPTS UTF8 ON
6	0.061961	147.102.40.15	FTP	74	192.168.1.14	Response: 200 UTF8 set to on

2.10 Ναι, συμφωνεί

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.14	TCP	66	147.102.40.15	55326 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 S
2	0.013370	147.102.40.15	TCP	66	192.168.1.14	21 → 55326 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
3	0.000086	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.025631	147.102.40.15	FTP	128	192.168.1.14	Response: 220 ProFTPD 1.3.4a Server (ProFTPD Default
5	0.008139	192.168.1.14	FTP	68	147.102.40.15	Request: OPTS UTF8 ON
6	0.014735	147.102.40.15	FTP	74	192.168.1.14	Response: 200 UTF8 set to on
7	0.052131	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=15 Ack=95 Win=8098 Len=0
8	6.286776	192.168.1.14	FTP	70	147.102.40.15	Request: USER anonymous
9	0.032454	147.102.40.15	FTP	129	192.168.1.14	Response: 331 Anonymous login ok, send your complete
10	0.046548	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=31 Ack=170 Win=8023 Len=0
11	10.505883	192.168.1.14	FTP	89	147.102.40.15	Request: PASS aggelosmitrokotsas@gmail.com

Urgent Pointer: 0
 > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, End of Option List (EOL)
 > [Timestamps]
 > [SEQ/ACK analysis]
[\[This is an ACK to the segment in frame: 1\]](#)
 [The RTT to ACK the segment was: 0.013370000 seconds]
 [iRTT: 0.013456000 seconds]

```
0020 01 0e 00 15 d8 1e ac 53 23 be 5c 3c 16 91 80 12 .....S #.\<....  

0030 ff ff db 60 00 00 02 04 02 18 01 03 03 06 04 02 .....`.....  

0040 00 00 .....
```

How long time it took to ACK the segment (RTT) (tcp.analysis.ack_rtt) | Packets: 82 · Displayed: 82 (100.0%) | Profile: Default

2.11

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.14	TCP	66	147.102.40.15	55326 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 S
2	0.013370	147.102.40.15	TCP	66	192.168.1.14	21 → 55326 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
3	0.000086	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.025631	147.102.40.15	FTP	128	192.168.1.14	Response: 220 ProFTPD 1.3.4a Server (ProFTPD Default
5	0.008139	192.168.1.14	FTP	68	147.102.40.15	Request: OPTS UTF8 ON
6	0.014735	147.102.40.15	FTP	74	192.168.1.14	Response: 200 UTF8 set to on
7	0.052131	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=15 Ack=95 Win=8098 Len=0
8	6.286776	192.168.1.14	FTP	70	147.102.40.15	Request: USER anonymous
9	0.032454	147.102.40.15	FTP	129	192.168.1.14	Response: 331 Anonymous login ok, send your complete
10	0.046548	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=31 Ack=170 Win=8023 Len=0
11	10.505883	192.168.1.14	FTP	89	147.102.40.15	Request: PASS aggelosmitrokotsas@gmail.com

Destination Port: 21
 [Stream index: 0]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 0 (relative sequence number)
 Sequence Number (raw): 1547441808
 [Next Sequence Number: 1 (relative sequence number)]

```
0000 38 02 de f7 d3 40 f8 63 3f 59 24 c8 08 00 45 00 8....@.c ?Y$...E.  

0010 00 34 47 d9 40 00 80 06 35 bf c0 a8 01 0e 93 66 .4G@.... 5.....f  

0020 28 0f d8 1e 00 15 5c 3c 16 90 00 00 00 80 02 (....\<.....
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 21

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.14	TCP	66	147.102.40.15	55326 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 S
2	0.013370	147.102.40.15	TCP	66	192.168.1.14	21 → 55326 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
3	0.000086	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.025631	147.102.40.15	FTP	128	192.168.1.14	Response: 220 ProFTPD 1.3.4a Server (ProFTPD Default
5	0.008139	192.168.1.14	FTP	68	147.102.40.15	Request: OPTS UTF8 ON
6	0.014735	147.102.40.15	FTP	74	192.168.1.14	Response: 200 UTF8 set to on
7	0.052131	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=15 Ack=95 Win=8098 Len=0
8	6.286776	192.168.1.14	FTP	70	147.102.40.15	Request: USER anonymous
9	0.032454	147.102.40.15	FTP	129	192.168.1.14	Response: 331 Anonymous login ok, send your complete
10	0.046548	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=31 Ack=170 Win=8023 Len=0
11	10.505883	192.168.1.14	FTP	89	147.102.40.15	Request: PASS aggelosmitrokotsas@gmail.com

```
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0      (relative sequence number)
Sequence Number (raw): 2891129790
[Next Sequence Number: 1      (relative sequence number)]
Acknowledgment Number: 1      (relative ack number)
Acknowledge number (raw): 1547441809
0000 f8 63 3f 59 24 c8 38 02 de f7 d3 40 08 00 45 00 .c?Y$ 8. .@. E.
0010 00 34 26 b9 40 00 39 06 9d df 93 66 28 0f c0 a8 .4&.@.9. .f(...
0020 01 0e 00 15 d8 1e ac 53 23 be 5c 3c 16 91 80 12 .....S #\<...
```

Header length in 32-bit words (ip.hdr_len), 1 byte(s) || Packets: 82 · Displayed: 29 (35.4%) · Dropped: 0 (0.0%) || Profile: Default

192.168.1.14 → 147.102.40.15 Sequence Number (raw): 1547441808

147.102.40.15 → 192.168.1.14 Sequence Number (raw): 2891129790

2.12 Προκύπτει από το Sequence Number (raw) του τελευταίου τεμαχίου που ελήφθη αυξημένο κατά ένα.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 21

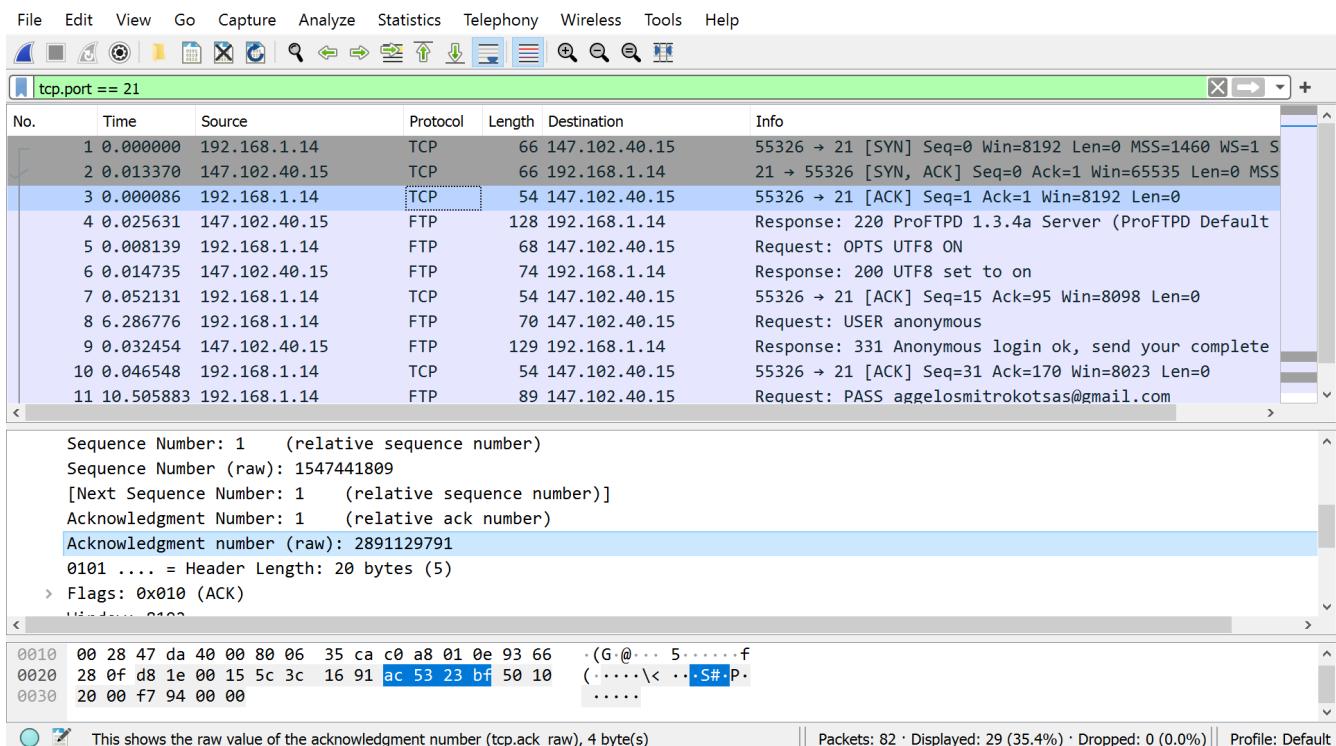
No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.14	TCP	66	147.102.40.15	55326 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 S
2	0.013370	147.102.40.15	TCP	66	192.168.1.14	21 → 55326 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
3	0.000086	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.025631	147.102.40.15	FTP	128	192.168.1.14	Response: 220 ProFTPD 1.3.4a Server (ProFTPD Default
5	0.008139	192.168.1.14	FTP	68	147.102.40.15	Request: OPTS UTF8 ON
6	0.014735	147.102.40.15	FTP	74	192.168.1.14	Response: 200 UTF8 set to on
7	0.052131	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=15 Ack=95 Win=8098 Len=0
8	6.286776	192.168.1.14	FTP	70	147.102.40.15	Request: USER anonymous
9	0.032454	147.102.40.15	FTP	129	192.168.1.14	Response: 331 Anonymous login ok, send your complete
10	0.046548	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=31 Ack=170 Win=8023 Len=0
11	10.505883	192.168.1.14	FTP	89	147.102.40.15	Request: PASS aggelosmitrokotsas@gmail.com

```
Sequence Number: 0      (relative sequence number)
Sequence Number (raw): 2891129790
[Next Sequence Number: 1      (relative sequence number)]
Acknowledgment Number: 1      (relative ack number)
Acknowledge number (raw): 1547441809
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x012 (SYN, ACK)
0020 01 0e 00 15 d8 1e ac 53 23 be 5c 3c 16 91 80 12 .....S #\<...
0030 ff ff db 60 00 00 02 04 02 18 01 03 03 06 04 02 ..... .
0040 00 00 ..
```

This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 byte(s) || Packets: 82 · Displayed: 29 (35.4%) · Dropped: 0 (0.0%) || Profile: Default

2.13 To Sequence Number (raw) προκύπτει από το προηγούμενο Sequence Number (raw) του ίδιου κόμβου αυξημένο κατά ένα.

Το Acknowledgment number (raw) προκύπτει από Sequence Number (raw) του κόμβου που επικοινωνεί αυξημένο κατα ένα (αυτό του τελευταίου τεμαχίου που ελήφθη).

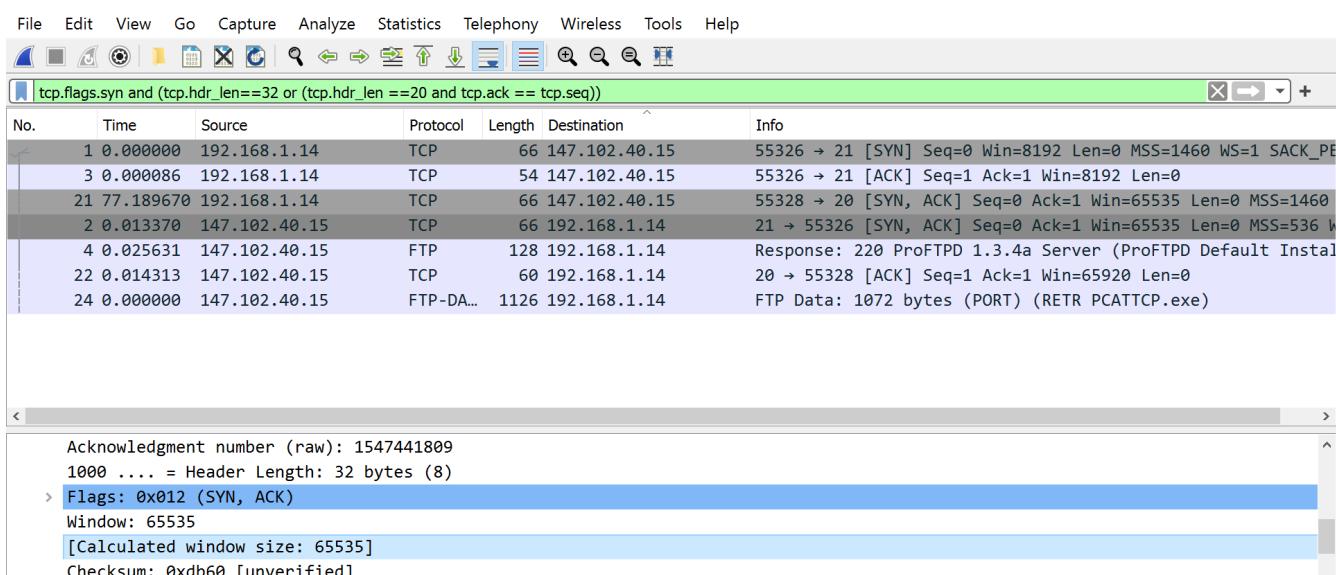


2.14 0 (δεν έχουν δεδομένα)

2.15 Γνωρίζουμε ότι τα πεδία Sequence Number και Acknowledgment number λαμβάνουν χώρο 32 bit. Άρα γνωρίζουμε ότι ο μέγιστος μη προσιμασμένος αριθμός 32 bit είναι ο 2^{32}

2.16 `tcp.flags.syn and (tcp.hdr_len==32 or (tcp.hdr_len ==20 and tcp.ack == tcp.seq))`

2.17 Ο υπολογιστής μου ανακοίνωσε παράθυρο μεγέθους 65535 bytes και ο εξυπηρετητής ανακοίνωσε παράθυρο μεγέθους 65520 bytes.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn and (tcp.hdr_len==32 or (tcp.hdr_len ==20 and tcp.ack == tcp.seq))

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.14	TCP	66	147.102.40.15	55326 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PEE
3	0.000086	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
21	77.189670	192.168.1.14	TCP	66	147.102.40.15	55328 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
2	0.013370	147.102.40.15	TCP	66	192.168.1.14	21 → 55326 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=1
4	0.025631	147.102.40.15	FTP	128	192.168.1.14	Response: 220 ProFTPD 1.3.4a Server (ProFTPD Default Instal
22	0.014313	147.102.40.15	TCP	60	192.168.1.14	20 → 55328 [ACK] Seq=1 Ack=1 Win=65920 Len=0
24	0.000000	147.102.40.15	FTP-DA...	1126	192.168.1.14	FTP Data: 1072 bytes (PORT) (RETR PCATTCP.exe)

Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1547441809
0101 = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 1030
[Calculated window size: 65920]
[Window size scaling factor: 64]

2.18 Στο πεδίο Window

2.19 min:1030 max:65535

2.20 1460 bytes

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn and (tcp.hdr_len==32 or (tcp.hdr_len ==20 and tcp.ack == tcp.seq))

No.	Time	Source	Protocol	Length	Destination	Info
1	0.000000	192.168.1.14	TCP	66	147.102.40.15	55326 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PEE
3	0.000086	192.168.1.14	TCP	54	147.102.40.15	55326 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
21	77.189670	192.168.1.14	TCP	66	147.102.40.15	55328 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
2	0.013370	147.102.40.15	TCP	66	192.168.1.14	21 → 55326 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=1
4	0.025631	147.102.40.15	FTP	128	192.168.1.14	Response: 220 ProFTPD 1.3.4a Server (ProFTPD Default Instal
22	0.014313	147.102.40.15	TCP	60	192.168.1.14	20 → 55328 [ACK] Seq=1 Ack=1 Win=65920 Len=0
24	0.000000	147.102.40.15	FTP-DA...	1126	192.168.1.14	FTP Data: 1072 bytes (PORT) (RETR PCATTCP.exe)

Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
> TCP Option - Maximum segment size: 1460 bytes
> TCP Option - No-Operation (NOP)
> TCP Option - Window scale: 0 (multiply by 1)
> TCP Option - No-Operation (NOP)
> TCP Option - No-Operation (NOP)
> TCP Option - SACK permitted

0020 28 0f d8 1e 00 15 5c 3c 16 90 00 00 00 00 00 02 (.....\x.....
0030 20 00 86 ec 00 00 02 04 05 b4 01 03 03 00 01 01 ..
0040 04 02 ..

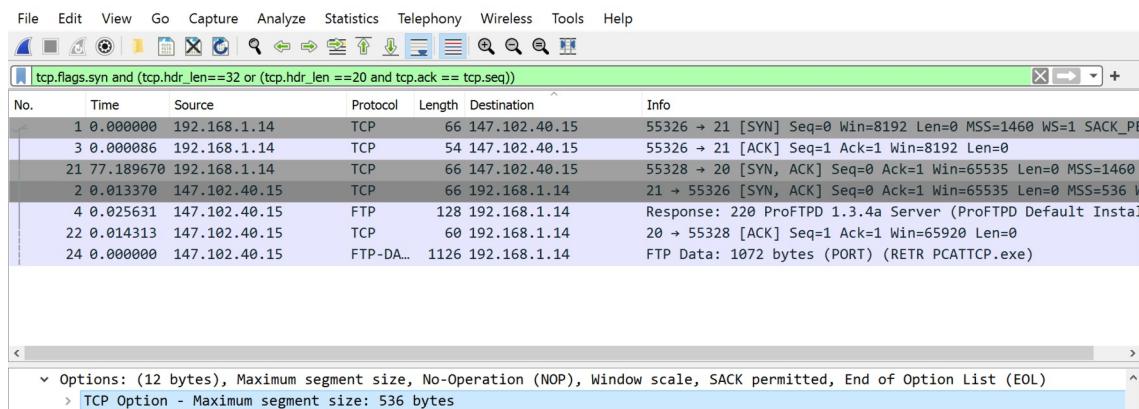
TCP Option - Maximum segment size (tcp.options.mss), 4 byte(s)

Packets: 82 · Displayed: 7 (8.5%) · Dropped: 0 (0.0%) | Profile: Default

2.21 Από την τιμή MTU (1500 bytes) αφαιρούμε το μέγεθος του επικεφαλίδας IP (20 bytes) και επικεφαλίδας TCP (20 bytes) και προκύπτει το MSS.

2.22 Στο Options

2.23 536 bytes



2.24 Όπως πριν (βλ 2.21)

Από την τιμή MTU (576 bytes) αφαιρούμε το μέγεθος του επικεφαλίδας IP (20 bytes) και επικεφαλίδας TCP (20 bytes) και προκύπτει το MSS.

2.25 Είναι 556 bytes, 536 (το MSS) συν 20 bytes της επικεφαλίδας.

2.26 Η σημαία FIN

2.27 tcp.flags.fin

2.28 Απ' την πλευρά του υπολογιστή μου

2.29 4 τεμάχια

2.30 20 bytes

2.31 0 bytes (δεν μεταφέρονται δεδομένα)

2.32 Ip Header: 20 bytes + TCP Header: 20 bytes + Data: 0 bytes = 40 bytes

2.33 Είναι ακριβώς το ίδιο: Ip Header: 20 bytes + TCP Header: 20 bytes + Data: 0 bytes = 40 bytes

2.34 377 bytes ο εξυπηρετητής και 124 bytes ο υπολογιστής μου.

2.35 Από τα Relative Sequence Numbers των τελευταίων πακέτων που καταγράφηκαν στο Wireshark. Αφού τα Sequence Numbers αυξάνονται βάση των bytes που έχουν σταλεί

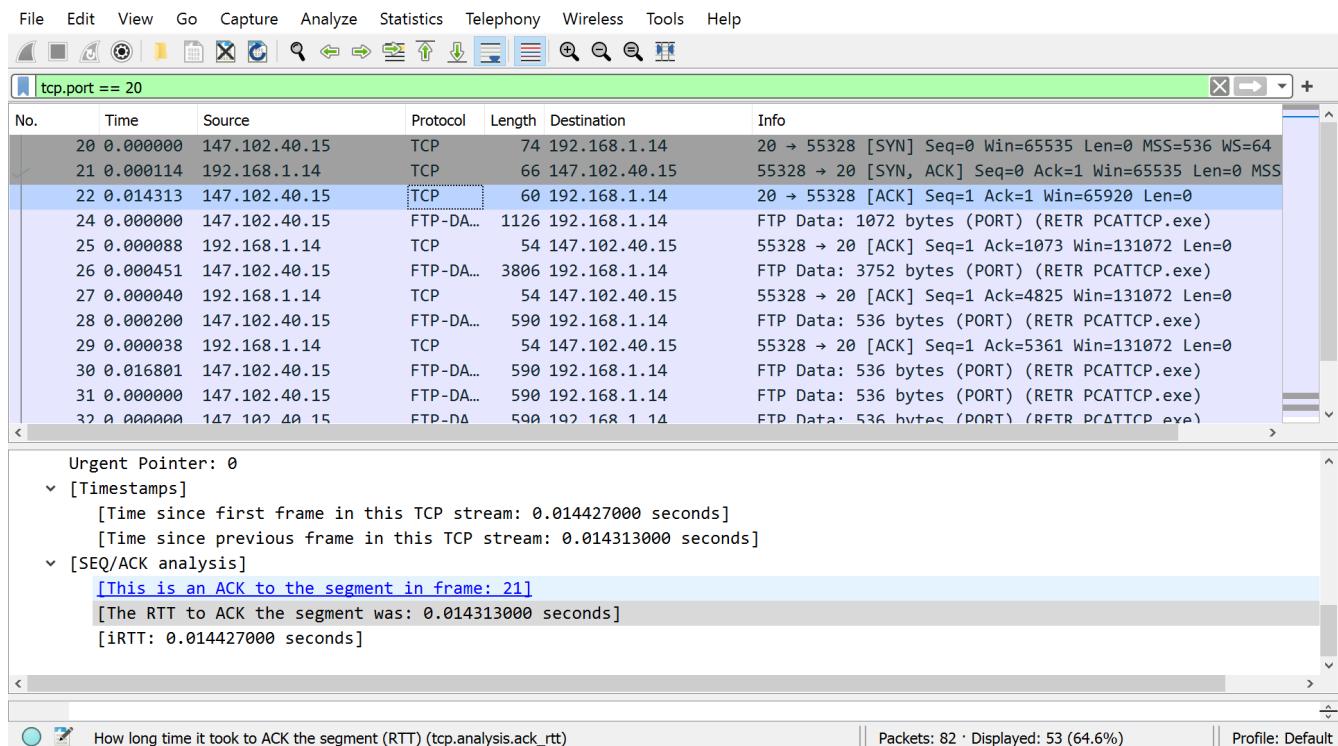
2.36 tcp.port == 20

2.37 192.168.1.14 → 147.102.40.15 MSS Value: 1460

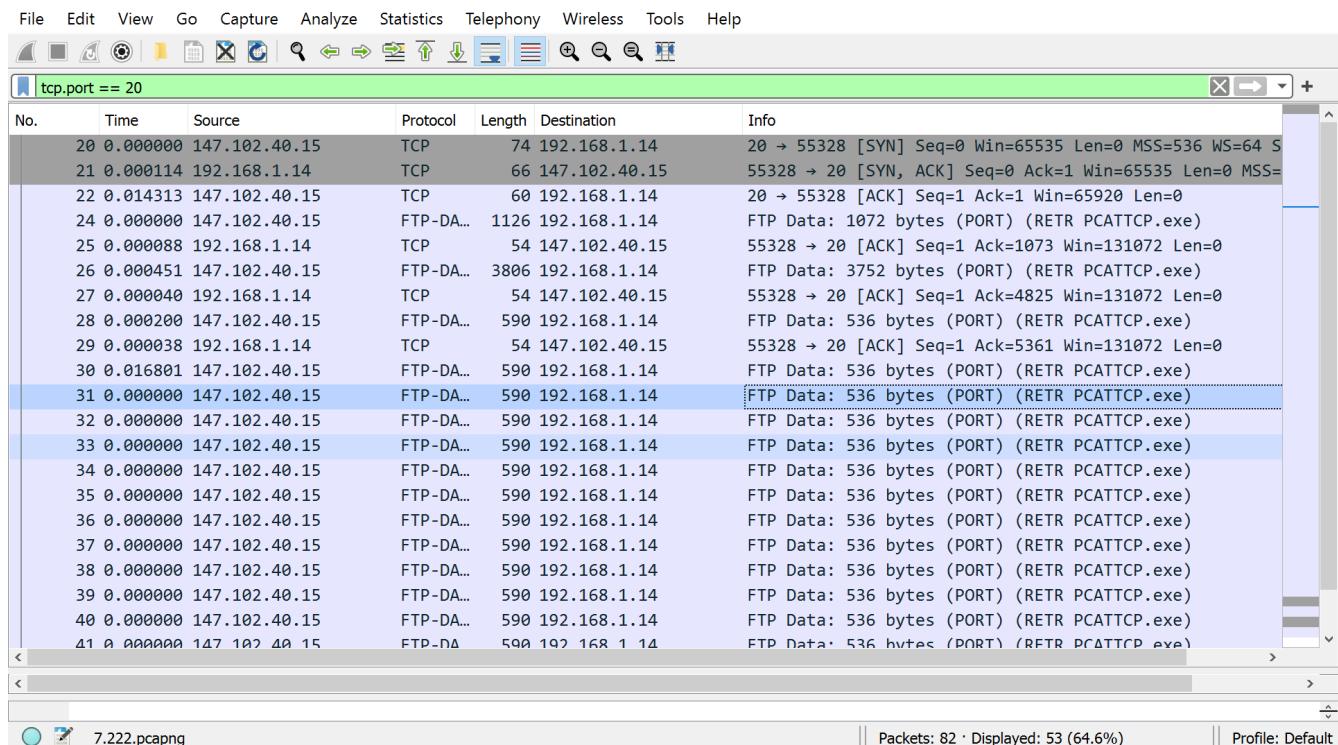
147.102.40.15 → 192.168.1.14 MSS Value: 536

2.38 Είναι 556 bytes, 536 (το MSS) συν 20 bytes της επικεφαλίδας (όπως στο 2.23)

2.39 0.000114 sec



2.40 Συνήθως ναι, εκτός από μία περιπτωση που εστειλε ACK αφού έλαβε 15 τεμάχια



No.	Time	Source	Protocol	Length	Destination	Info
29	0.000038	192.168.1.14	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=5361 Win=131072 Len=0
30	0.016801	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
31	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
32	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
33	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
34	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
35	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
36	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
37	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
38	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
39	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
40	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
41	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
42	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
43	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
44	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
45	0.000066	192.168.1.14	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=13401 Win=131072 Len=0
46	0.013631	147.102.40.15	FTP-DA...	1126	192.168.1.14	FTP Data: 1072 bytes (PORT) (RETR PCATTCP.exe)
47	0.000042	192.168.1.14	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=14473 Win=131072 Len=0
48	0.001767	147.102.40.15	FTP-DA...	8094	192.168.1.14	FTP Data: 8040 bytes (PORT) (RETR PCATTCP.exe)
49	0.000000	192.168.1.14	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=22513 Win=131072 Len=0

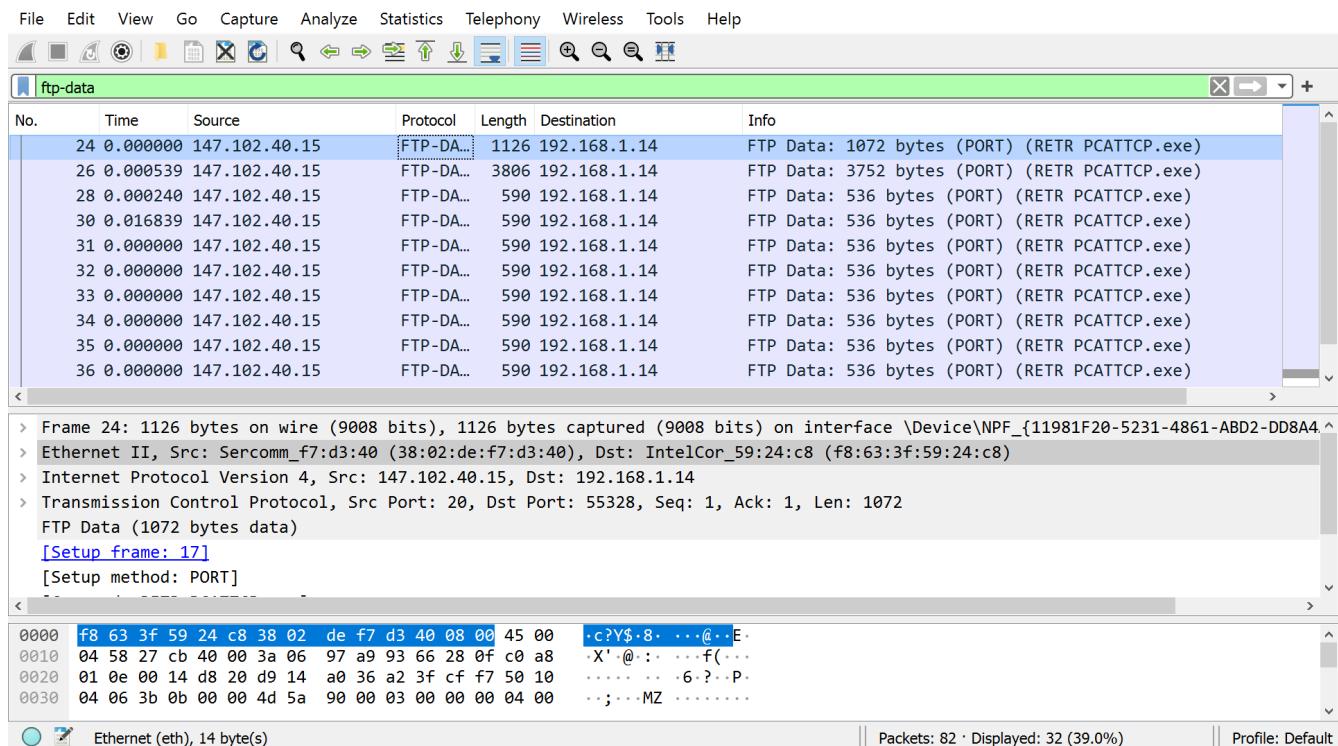
Και εκτός από μία ακόμα περίπτωση που εστειλε επιβεβαίωση αφού ελαβε 2 μηνυματα

No.	Time	Source	Protocol	Length	Destination	Info
61	0.003977	147.102.40.15	FTP-DA...	3806	192.168.1.14	FTP Data: 3752 bytes (PORT) (RETR PCATTCP.exe)
62	0.000059	192.168.1.14	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=39129 Win=131072 Len=0
63	0.001534	147.102.40.15	FTP-DA...	10238	192.168.1.14	FTP Data: 10184 bytes (PORT) (RETR PCATTCP.exe)
64	0.000067	192.168.1.14	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=49313 Win=131072 Len=0
65	0.012639	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
66	0.001128	147.102.40.15	FTP-DA...	5414	192.168.1.14	FTP Data: 5360 bytes (PORT) (RETR PCATTCP.exe)
67	0.000064	[192.168.1.14]	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=55209 Win=131072 Len=0
68	0.0000497	147.102.40.15	FTP-DA...	4878	192.168.1.14	FTP Data: 4824 bytes (PORT) (RETR PCATTCP.exe)
69	0.000057	192.168.1.14	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=60033 Win=131072 Len=0
70	0.001558	147.102.40.15	FTP-DA...	1126	192.168.1.14	FTP Data: 1072 bytes (PORT) (RETR PCATTCP.exe)

2.41 Οχι δεν αλλάζουν, η μικρότερη (όλες οι τιμές δηλαδη) σίναι 512 bytes

No.	Time	Source	Protocol	Length	Destination	Info
28	0.000200	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
29	0.000038	[192.168.1.14]	TCP	54	147.102.40.15	55328 → 20 [ACK] Seq=1 Ack=5361 Win=131072 Len=0
30	0.016801	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
31	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
32	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
33	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
34	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
35	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
36	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)
37	0.000000	147.102.40.15	FTP-DA...	590	192.168.1.14	FTP Data: 536 bytes (PORT) (RETR PCATTCP.exe)

2.42 1126 bytes, επικεφαλιδα Ethernet: 14 bytes, επικεφαλιδα IPv4 : 20 bytes, επικεφαλιδα TCP: 20 bytes

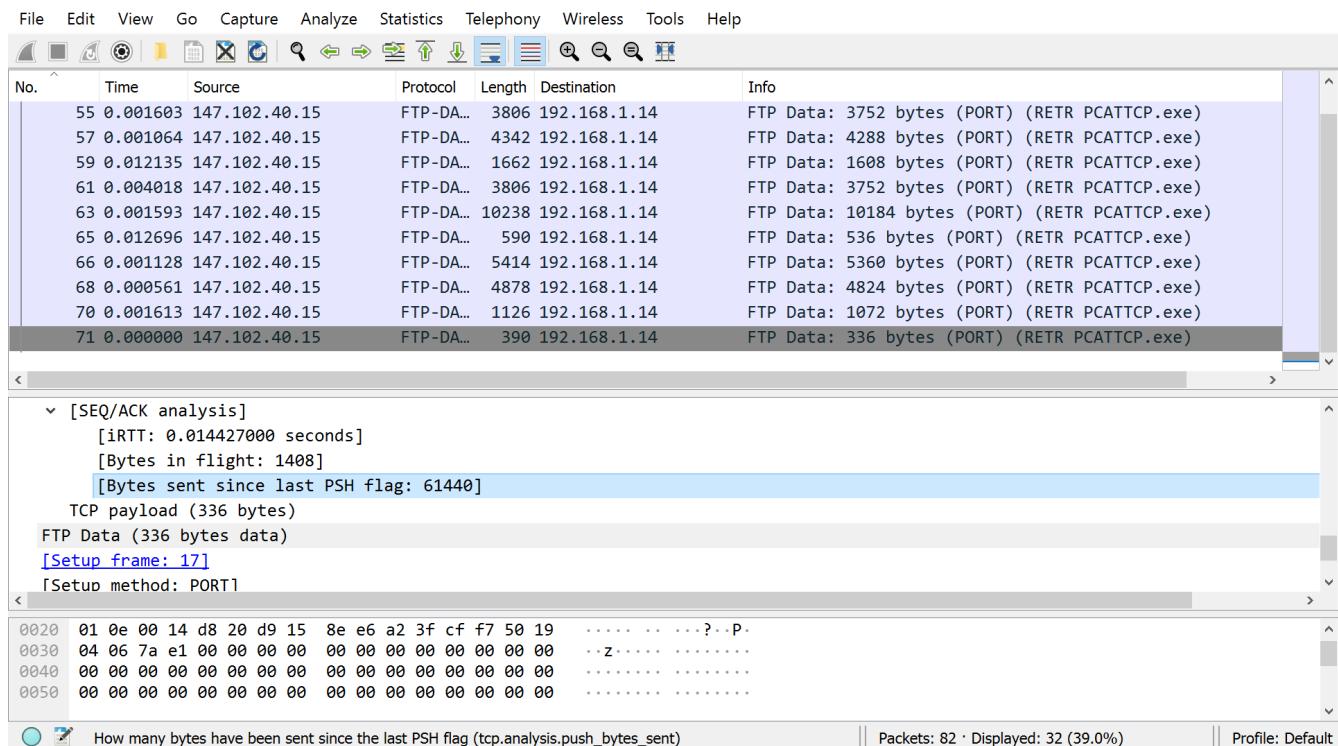


2.43 Είναι Data: 1072 bytes, ακριβώς το διπλάσιο από το αναμενόμενο με βάση το 2.38 (παρατηρώ ότι παρακάτω υπάρχουν τεμάχια με μέγεθος 590, που έχουν το αναμενόμενο μέγεθος -536 bytes- Data) (κανονικά επρεπε να είναι και εδώ 590, όχι 1121 ή ποσο μαλλον 3806 που έχει κάτω)

2.44 Σε αυτή την περίπτωση τα TCP τεμάχια θα θρυματιστούν σε μικρότερα κομμάτια και θα αποσταλούν έτσι, υπο την προυπόθεση ότι δεν έχει τεθεί ενεργό το don't fragment bit (στην περίπτωση που φέρει αυτή τη σημαία θα πρέπει να απορριφθεί αυτό το πακέτο και να σταλθεί ICMP μήνυμα σφάλματος)

2.45 192.168.1.14 → 147.102.40.15 Sequence Number: 0 bytes (όλα τα πακέτα έχουν relative acknowledgement number = 1)

147.102.40.15 → 192.168.1.14 Sequence Number: 61440 bytes



2.46 819.20Kbytes/sec (φαίνεται στο παράθυρο εντολών)

```
Επιλογή Administrator: Windows PowerShell
5 C:\Windows\system32> ftp edu-dy.cn.ntua.gr
Connected to edu-dy.cn.ece.ntua.gr.
20 ProFTPD 1.3.4a Server (ProFTPD Default Installation) [147.102.40.15]
00 UTF8 set to on
ser (edu-dy.cn.ece.ntua.gr:(none)): Anonymous
31 Password required for Anonymous
password:
30 Login incorrect.
login failed.
tp> clear
invalid command.
tp> bye
21 Goodbye.
5 C:\Windows\system32> ftp edu-dy.cn.ntua.gr
Connected to edu-dy.cn.ece.ntua.gr.
20 ProFTPD 1.3.4a Server (ProFTPD Default Installation) [147.102.40.15]
00 UTF8 set to on
ser (edu-dy.cn.ece.ntua.gr:(none)): anonymous
31 Anonymous login ok, send your complete email address as your password
password:
30 Anonymous access granted, restrictions apply
tp> bin
00 Type set to I
tp> lcd desktop
rvalid command.
tp> lcd desktop
esktop: file not found
tp> lcd Desktop
esktop: file not found
tp> lcd Εργασίας
cd local directory.
tp> get PCATTCP.exe
00 PORT command successful
50 Opening BINARY mode data connection for PCATTCP.exe (61440 bytes)
26 Transfer complete
tp: 61440 bytes received in 0.07seconds 819.20Kbytes/sec.
tp> bye
21 Goodbye.
5 C:\Windows\system32>
```

2.47 Δεν υπήρξαν αναμεταδόσεις (Αν υπήρχαν αναμεταδόσεις θα το καταλάβαινα αφού τα ίδια τεμάχια θα έχουν ίδιο Sequence Number)

3

```

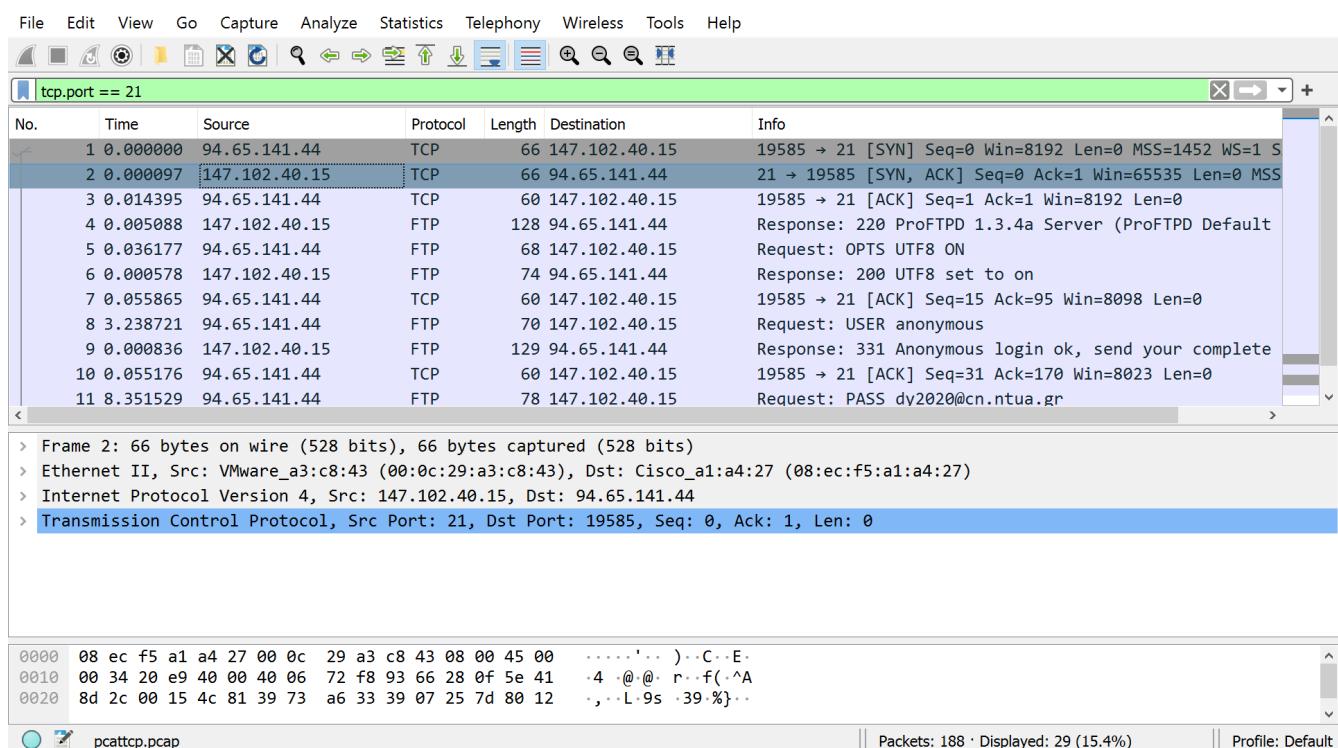
Administrator: Windows PowerShell
PS C:\Windows\system32> ftp edu-dy.cn.ntua.gr
Connected to edu-dy.cn.ece.ntua.gr.
220 ProFTPD 1.3.4a Server (ProFTPD Default Installation) [147.102.40.15]
200 UTF8 set to on
User (edu-dy.cn.ece.ntua.gr:(none)): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
ftp> bin
200 Type set to I
ftp> lcd Επίδειξη Εργασίας
lcd local directory.
ftp> lcd desktop
desktop: File not found
ftp> lcd Επίδειξη Εργασίας
lcd local directory.
ftp> get pcattcp.pcap
200 PORT command successful
150 Opening BINARY mode data connection for pcattcp.pcap (75461 bytes)
226 Transfer complete
ftp: 75461 bytes received in 0.11Seconds 686.01kbytes/sec.
ftp> bye
221 Goodbye.
PS C:\Windows\system32>

```

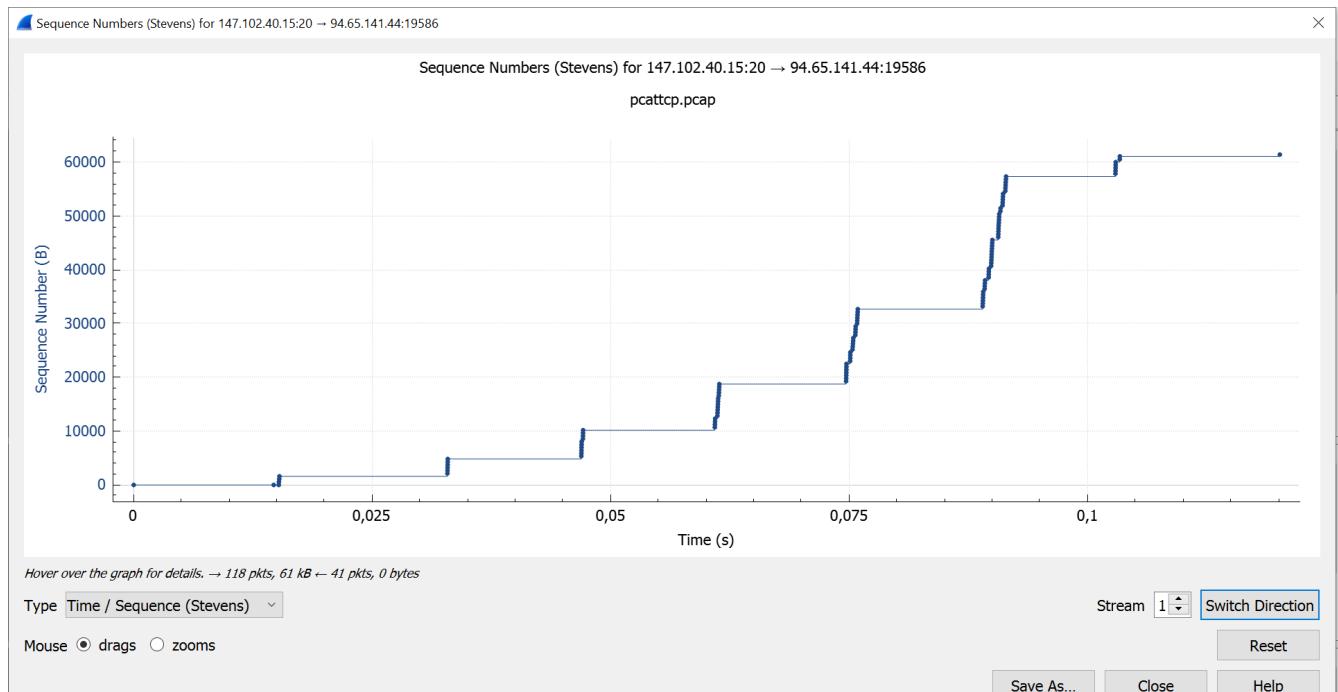
3.1 tcp.port== 21

3.2 94.65141.44

3.3 Το RTT είναι 97ms, μικρότερο από αυτό της 2.39 (πολύ μικρότερο)



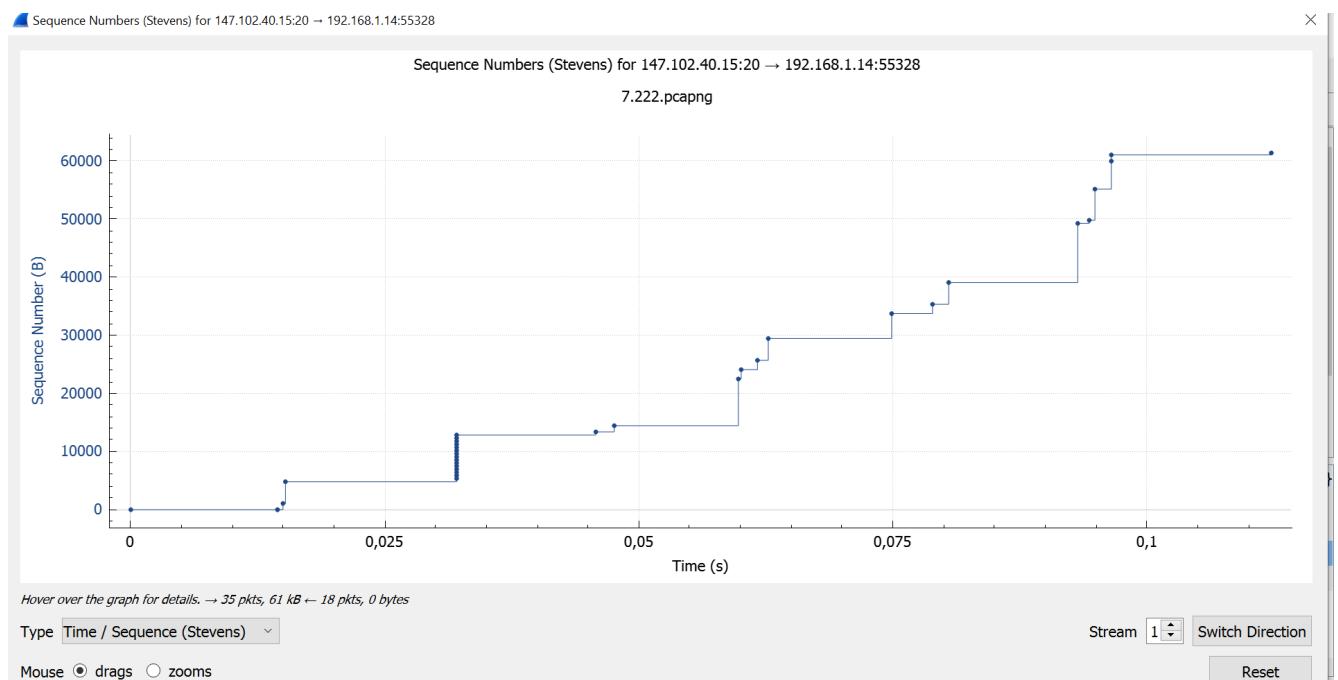
3.4 Στέλνονται πολλά τεμάχια πρακτικά ταυτόχρονα, τα οποία ακολουθούνται από μεγάλο κενό προκειμένου να ληφθεί το αντίστοιχο ACK (acknowledgement)



3.5 Στάλθηκαν 4 τεμάχια. Ναι, είναι συμφωνο

3.6 Έστειλε 6 τεμάχια στο 2^o RTT και 10 τεμαχια στο 3ο. Αυτό συνέβη διότι μετά από κάθε ACK μεγαλώνει το congestion window

3.7 Είναι παρομοιο (σαν σχήμα), στο δικό μου διάγραμμα στο πρώτο RTT έστειλε 1 τεμάχιο, στο 2^o 1 παλι, στο 3^o επισης 1, και έπειτα τα 15 μαζεμένα.



4

```
Administrator: Windows PowerShell
PS C:\Windows\system32> nslookup edu-dy.cn.ntua.gr
Server: speedport.ip
Address: 192.168.1.1

Non-authoritative answer:
Name:   edu-dy.cn.ece.ntua.gr
Address: 147.102.40.15
Aliases: edu-dy.cn.ntua.gr

PS C:\Windows\system32>
```

4.1 udp

4.2 Source Port: 2 bytes, Destination Port: 2 bytes, Length: 2 bytes, Checksum: 2 bytes

4.3 8 bytes

4.4 121 bytes

4.5 Το συνολικό μήκος του UDP δεδομενογράμματος.

4.6 min: 8 bytes(η επικεφαλίδα), max: $65535 - 20 = 65515$ bytes (max IP – επικεφαλίδα IPv4)

4.7 556 bytes ($576 - 20$ (μεγεθος επικεφαλίδας IPv4))

4.8 DNS, QUIC, UDP

4.9 udp and dns

4.10 η 192.168.1 (η διεύθυνση του DNS server)

4.11 Src: Port 62779, Dst: Port 53

4.12 Src: Port 53, Dst: Port 62779

4.13 H 53.