

Όνοματεπώνυμο: Άγγελος Μητροκώτσας	Ομάδα: 6
Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2	Ημερομηνία: 20/1/ 2022
Διεύθυνση IP: 192.168.1.11	Διεύθυνση MAC: F8-63-3F-59-24-C8

Εργαστηριακή Άσκηση 12 Ασφάλεια

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 Status code το 401 και φράση Authorization Required

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Protocol	Length	Destination	Info
5	0.0000102	192.168.1.11	TCP	54	147.102.40.15	63347 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
6	0.0000082	192.168.1.11	TCP	54	147.102.40.15	63348 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
7	0.000323	192.168.1.11	HTTP	500	147.102.40.15	GET /auth/ HTTP/1.1
8	0.014656	147.102.40.15	TCP	590	192.168.1.11	80 → 63348 [ACK] Seq=1 Ack=447 Win=65920 Len=536 [TCP]
9	0.0000000	147.102.40.15	HTTP	240	192.168.1.11	HTTP/1.1 401 Authorization Required (text/html)
10	0.000093	192.168.1.11	TCP	54	147.102.40.15	63348 → 80 [ACK] Seq=447 Ack=723 Win=65792 Len=0
11	5.002786	147.102.40.15	TCP	54	192.168.1.11	80 → 63348 [FIN, ACK] Seq=723 Ack=447 Win=65920 Len=0
12	0.000193	192.168.1.11	TCP	54	147.102.40.15	63348 → 80 [ACK] Seq=447 Ack=724 Win=65792 Len=0
13	3.998559	192.168.1.11	TCP	54	147.102.40.15	63348 → 80 [FIN, ACK] Seq=447 Ack=724 Win=131072 Len=

```

> Frame 9: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A76
> Ethernet II, Src: SernetSu_a7:bb:50 (d0:b6:6f:a7:bb:50), Dst: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
> Internet Protocol Version 4, Src: 147.102.40.15, Dst: 192.168.1.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 63348, Seq: 537, Ack: 447, Len: 186
> [2 Reassembled TCP Segments (722 bytes): #8(536), #9(186)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (12 lines)
<
0000  f8 63 3f 59 24 c8 d0 b6 6f a7 bb 50 08 00 45 00  .c?Y$... o..P..E.
0010  00 e2 d6 56 40 00 3a 06 ec 96 93 66 28 0f c0 a8  ...V@.: ...f(...
0020  01 0b 00 50 f7 74 47 1e 86 4c eb d0 67 01 50 18  ...P.tG. .L..g.P.
0030  04 06 c8 75 00 00 73 73 20 74 68 65 20 64 6f 63  ...u..ss the doc
0040  75 6d 65 6e 74 0a 72 65 71 75 65 73 74 65 64 2e  ument.re quested.

Frame (240 bytes) Reassembled TCP (722 bytes)
Wireshark_Wi-FiE1FDG1.pcapng
Packets: 23 · Displayed: 23 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

```

1.2 To authorization

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays 16 captured frames, mostly TCP segments, with one HTTP request highlighted. The details pane shows the raw HTTP request: `GET /auth/ HTTP/1.1\r\nHost: edu-dy.cn.ntua.gr\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\n\r\nAuthorization: Basic ZWR1lWR50nBhc3N3b3Jk\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36`. The bytes pane shows the binary representation of the captured data.

1.3 Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk

Credentials: edu-dy:password

1.4 edu-dy:password

BASE64 - ONLINE BASE64 DECODER AND ENCODER
DECODING AND ENCODING TEXTS AND FILES.

You can use this base64 sample decoder and encoder to:

- Decode base64 strings (base64 string looks like YTM0NZomIzI2OTsmIzM0NTueYQ==)
- Decode a base64 encoded file (for example ICO files or files from MIME message)
- Convert text data from several code pages and encode them to a base64 string or a file
- New: Try [CSS/base64 analyzer](#) and simple [Base64 decoder](#) and [encoder](#).

Hootsuite
 Try Hootsuite for 2 months

OPEN

The Form SizeLimit is 10000000bytes. Please, do not post more data using this form.
Source data from the Base64 string:
`edu-dy:password`

Type (or copy-paste) some text to a textbox bellow. The text can be a Base64 string to decode or any string to encode to a Base64.

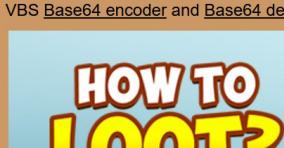
7iBq1JU1PfCgRtLz3N2h22k

Base64 links

[More about Base64 encoding \(wiki\)](#)
[Encode image to a Base64 for html/css](#)
[Css Images analyzer and encoder to Base64](#)

Base64 programming

[Base64 component for ASP/VBS](#)
[VBS Base64 encoder and Base64 decoder](#)

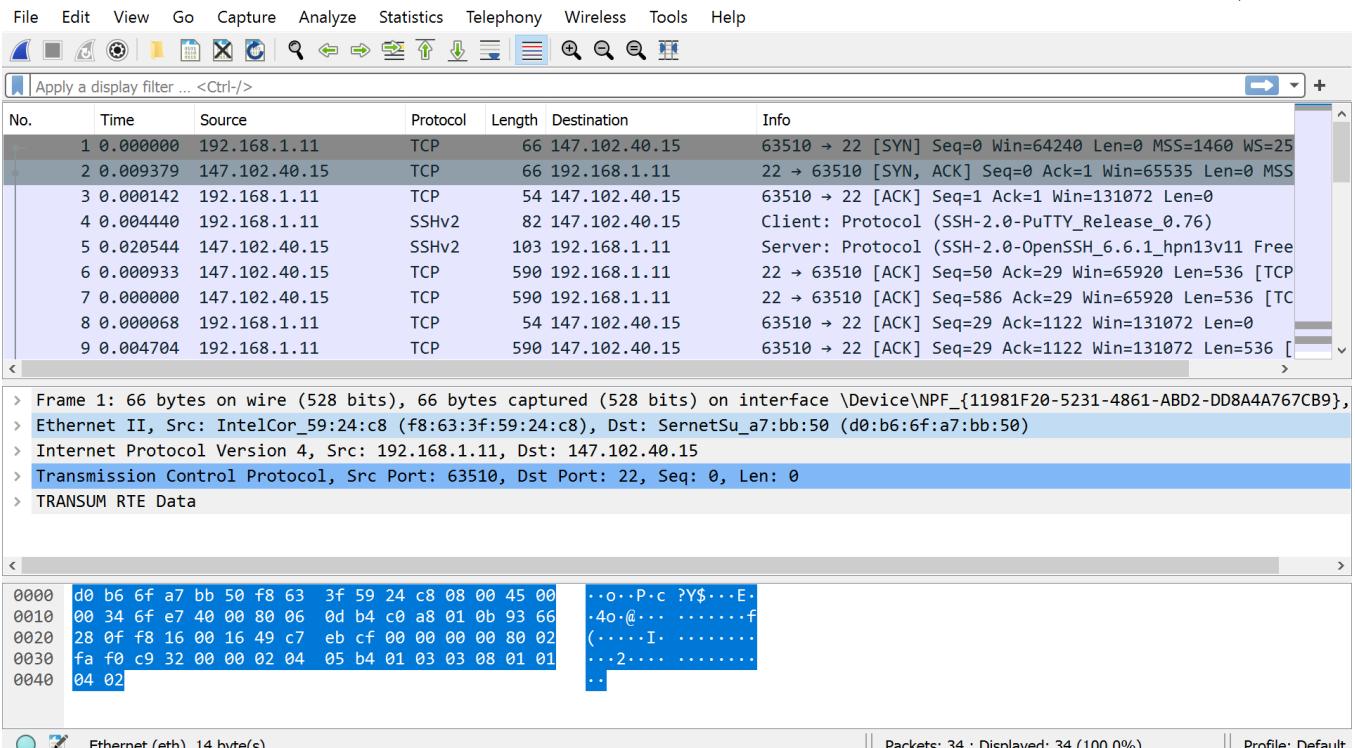


1.5 Ο μηχανισμός ανταλλαγής των credentials που χρησιμοποιείται στο HTTP Base64 είναι πολύ αδύναμος καθώς έχει έλλειψη εμπιστευτικότητας (confidentiality). Οποιοσδήποτε ενδιάμεσος κόμβος μπορεί να μάθει τα στοιχεία ταυτοποίησης του χρήστη

2

2.1 TCP

2.2 Source: 63510, Destination: 22

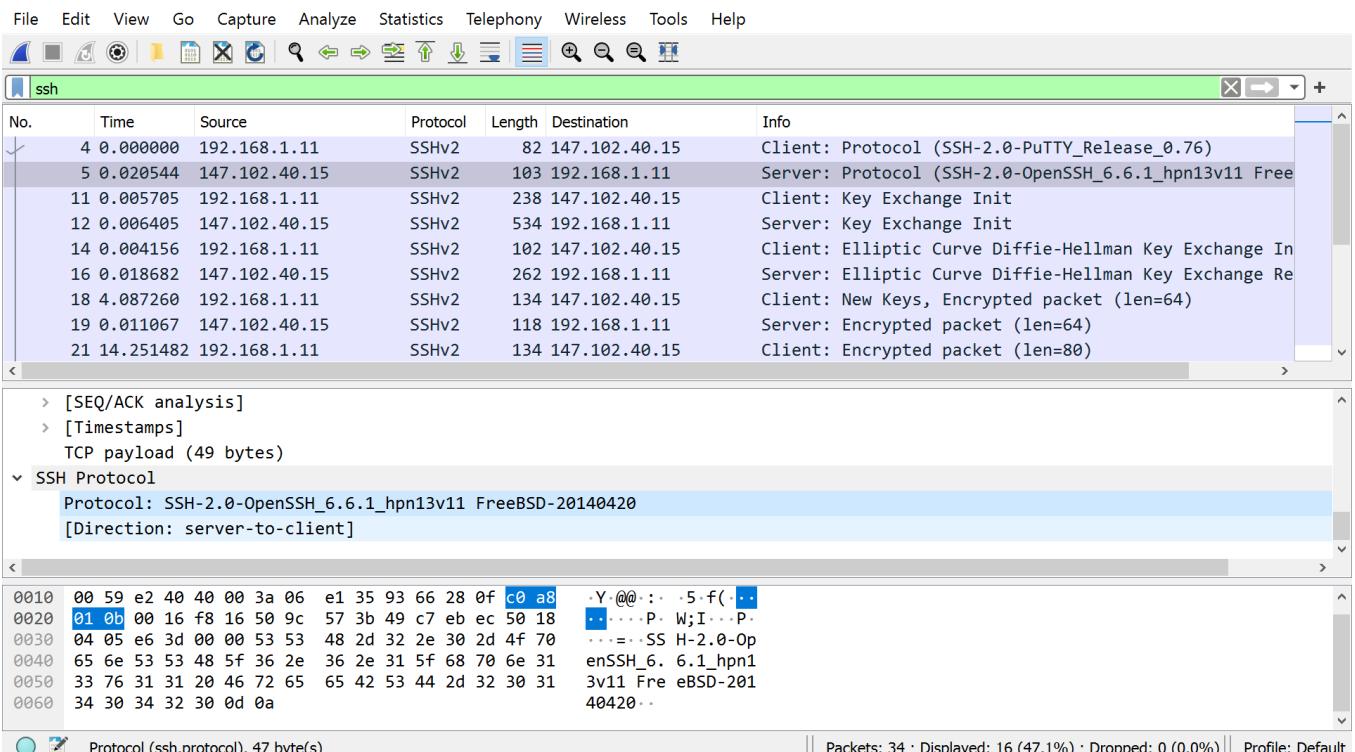


2.3 Η θύρα 22

2.4 ssh

2.5 Έκδοση του πρωτοκόλλου SSH: SSH-2.0

Έκδοση λογισμικού: OpenSSH_6.6.1_hpn13v11 FreeBSD-20140420



2.6 Έκδοση του πρωτοκόλλου SSH: SSH-2.0

Έκδοση λογισμικού: PuTTY_Release_0.76

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssh

Time	Source	Protocol	Length	Destination	Info
0.000000	192.168.1.11	SSHv2	82	147.102.40.15	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
0.020544	147.102.40.15	SSHv2	103	192.168.1.11	Server: Protocol (SSH-2.0-OpenSSH_6.6.1_hpni3v11 FreeBSD-2014...)
0.005705	192.168.1.11	SSHv2	238	147.102.40.15	Client: Key Exchange Init
0.006405	147.102.40.15	SSHv2	534	192.168.1.11	Server: Key Exchange Init
0.004156	192.168.1.11	SSHv2	102	147.102.40.15	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
0.018682	147.102.40.15	SSHv2	262	192.168.1.11	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New...
4.087260	192.168.1.11	SSHv2	134	147.102.40.15	Client: New Keys, Encrypted packet (len=64)
0.011067	147.102.40.15	SSHv2	118	192.168.1.11	Server: Encrypted packet (len=64)
14.251482	192.168.1.11	SSHv2	134	147.102.40.15	Client: Encrypted packet (len=80)

< [SEQ/ACK analysis]
 > [Timestamps]
 TCP payload (28 bytes)
 SSH Protocol
 Protocol: SSH-2.0-PuTTY_Release_0.76
 [Direction: client-to-server]

```
0000 d0 b6 6f a7 bb 50 f8 63 3f 59 24 c8 08 00 45 00 ...o...P.c ?Y$...E.  

0010 00 44 6f e9 40 00 80 06 0d a2 c0 a8 01 0b 93 66 .Do @... ....f  

0020 28 0f f8 16 00 16 49 c7 eb d0 50 9c 57 3b 50 18 (.....I ..P.W;P.  

0030 02 00 64 da 00 00 53 53 48 2d 32 2e 30 2d 50 75 ..d...SS H-2.0-Pu  

0040 54 54 59 5f 52 65 6c 65 61 73 65 5f 30 2e 37 36 TTY_Rele ase_0.76  

0050 0d 0a ..
```

Protocol (ssh.protocol), 26 byte(s) || Packets: 34 · Displayed: 16 (47.1%) · Dropped: 0 (0.0%) || Profile: Default

2.7 Συνολικά είναι 13. Οι πρώτοι 2: curve448-sha512,curve25519-sha256

Wireshark - kex_algorithms string (ssh.kex_algorithms) · Wi-Fi (host 147.102.40.15)

curve448-sha512,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,rsa2048-sha256,rsa1024-sha1,diffie-hellman-group1-sha1,ext-info-c

Frame 11, kex_algorithms string (ssh.kex_algorithms), 315 byte(s).

Decode as None Show as ASCII Start 0 End 315

Find: Print Copy Save as... Close Help Find Next

2.8 Είναι 9. Ο πρώτος: ssh-ed448

A Wireshark screenshot showing a single frame (Frame 11) containing the string "ssh-ed448,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-512,rsa-sha2-256,ssh-rsa,ssh-dss". The interface shows standard Wireshark controls like Decode as, Show as, Start/End filters, and a Find bar.

2.9 aes256-ctr, aes256-cbc

A Wireshark screenshot showing a single frame (Frame 11) containing the string "aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,chacha20-poly1305@openssh.com,3des-ctr,3des-cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128". The interface shows standard Wireshark controls like Decode as, Show as, Start/End filters, and a Find bar.

2.10 hmac-sha2-256,hmac-sha1

A Wireshark screenshot showing a single frame (Frame 11) containing the string "hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-etm@openssh.com". The interface shows standard Wireshark controls like Decode as, Show as, Start/End filters, and a Find bar.

2.11 none (δεν ξέρω αν μετράει), zlib,zlib@openssh.com

A Wireshark screenshot showing a single frame (Frame 11) containing the string "none,zlib,zlib@openssh.com". The interface shows standard Wireshark controls like Decode as, Show as, Start/End filters, and a Find bar.

2.12 Είναι ο curve25519-sha256@libssh.org και το Wireshark τον εμφανίζει σε παρένθεση δίπλα από το Key Exchange

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Protocol Length Destination Info

4	0.000000	192.168.1.11	SSHv2	82	147.102.40.15	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
5	0.020544	147.102.40.15	SSHv2	103	192.168.1.11	Server: Protocol (SSH-2.0-OpenSSH_6.6.1_hpn13v11 Free)
11	0.005705	192.168.1.11	SSHv2	238	147.102.40.15	Client: Key Exchange Init
12	0.006405	147.102.40.15	SSHv2	534	192.168.1.11	Server: Key Exchange Init
14	0.004156	192.168.1.11	SSHv2	102	147.102.40.15	Client: Elliptic Curve Diffie-Hellman Key Exchange In
16	0.018682	147.102.40.15	SSHv2	262	192.168.1.11	Server: Elliptic Curve Diffie-Hellman Key Exchange Re
18	4.087260	192.168.1.11	SSHv2	134	147.102.40.15	Client: New Keys, Encrypted packet (len=64)
19	0.011067	147.102.40.15	SSHv2	118	192.168.1.11	Server: Encrypted packet (len=64)
21	14.251482	192.168.1.11	SSHv2	134	147.102.40.15	Client: Encrypted packet (len=80)

Padding Length: 6

Key Exchange (method:curve25519-sha256@libssh.org)

- Message Code: Key Exchange Init (20)
- Algorithms
 - Cookie: 8046549ac7bd96cbd601936a06be9cce
 - kex_algorithms length: 212
 - kex_algorithms string: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp512,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

Frame (534 bytes) Reassembled TCP (1552 bytes)

Text item (text), 1.547 byte(s) Packets: 34 · Displayed: 16 (47.1%) · Dropped: 0 (0.0%) · Profile: Default

Wireshark - kex_algorithms string (ssh.kex.algorithms) · Wi-Fi (host 147.102.40.15)

curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp512,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

2.13 Τον aes256-ctr

2.14 hmac-sha2-256

2.15 Ο none

2.16 Ναι, σε παρένθεση δίπλα στο πεδίο SSH Version 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Protocol Length Destination Info

4	0.000000	192.168.1.11	SSHv2	82	147.102.40.15	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
5	0.020544	147.102.40.15	SSHv2	103	192.168.1.11	Server: Protocol (SSH-2.0-OpenSSH_6.6.1_hpn13v11 Free)
11	0.005705	192.168.1.11	SSHv2	238	147.102.40.15	Client: Key Exchange Init
12	0.006405	147.102.40.15	SSHv2	534	192.168.1.11	Server: Key Exchange Init
14	0.004156	192.168.1.11	SSHv2	102	147.102.40.15	Client: Elliptic Curve Diffie-Hellman Key Exchange In
16	0.018682	147.102.40.15	SSHv2	262	192.168.1.11	Server: Elliptic Curve Diffie-Hellman Key Exchange Re
18	4.087260	192.168.1.11	SSHv2	134	147.102.40.15	Client: New Keys, Encrypted packet (len=64)
19	0.011067	147.102.40.15	SSHv2	118	192.168.1.11	Server: Encrypted packet (len=64)
21	14.251482	192.168.1.11	SSHv2	134	147.102.40.15	Client: Encrypted packet (len=80)

> Internet Protocol Version 4, Src: 147.102.40.15, Dst: 192.168.1.11
> Transmission Control Protocol, Src Port: 22, Dst Port: 63510, Seq: 1122, Ack: 29, Len: 480
> [3] Reassembled TCP Segments (1552 bytes): #6(536), #7(536), #12(480)]
SSH Protocol
SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
Packet Length: 1548
Padding Length: 6

Frame (534 bytes) Reassembled TCP (1552 bytes)

Text item (text), 1.552 byte(s) Packets: 34 · Displayed: 16 (47.1%) · Dropped: 0 (0.0%) · Profile: Default

2.17 Ναι, τους εξείς: Elliptic Curve Diffie-Hellman Key Exchange Init, Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted Packet.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssh

No.	Time	Source	Protocol	Length	Destination	Info
4	0.000000	192.168.1.11	SSHv2	82	147.102.40.15	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
5	0.020544	147.102.40.15	SSHv2	103	192.168.1.11	Server: Protocol (SSH-2.0-OpenSSH_6.6.1_hpn13v11 Free)
11	0.005705	192.168.1.11	SSHv2	238	147.102.40.15	Client: Key Exchange Init
12	0.006405	147.102.40.15	SSHv2	534	192.168.1.11	Server: Key Exchange Init
14	0.004156	192.168.1.11	SSHv2	102	147.102.40.15	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
16	0.018682	147.102.40.15	SSHv2	262	192.168.1.11	Server: Elliptic Curve Diffie-Hellman Key Exchange Re
18	4.087260	192.168.1.11	SSHv2	134	147.102.40.15	Client: New Keys, Encrypted packet (len=64)
19	0.011067	147.102.40.15	SSHv2	118	192.168.1.11	Server: Encrypted packet (len=64)
21	1.18	192.168.1.11	SSHv2	131	147.102.40.15	Client: Encrypted packet (len=64)

```

> Frame 14: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767^
> Ethernet II, Src: IntelCor_59:24:c8 (f8:63:3f:59:24:c8), Dst: SernetSu_a7:bb:50 (d0:b6:6f:a7:bb:50)
└ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 147.102.40.15
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSFP: CS0, ECN: Not-ECT)
    Total Length: 88

0000 d0 b6 6f a7 bb 50 f8 63 3f 59 24 c8 08 00 45 00  ..o..P..c ?Y$...E...
0010 00 58 6f ee 40 00 80 06 0d 89 c0 a8 01 0b 93 66  .Xo@... ....f...
0020 28 0f f8 16 00 16 49 c7 f0 d4 50 9c 5d 7c 50 18  (.....I..P..]P.
0030 01 ff 6a 23 00 00 00 00 00 2c 06 1e 00 00 00 20  ..j#.... ,.....
0040 d7 2b 59 09 b7 d3 9b 4e a2 0a 7b 8c e9 5a 23 ce  +Y...N ..{..Z#.
0050 f0 b5 b2 02 c8 d3 f3 86 83 c0 3c 20 05 11 af 36  .......< ...6

SSH Protocol: Protocol
Packets: 34 · Displayed: 16 (47.1%) · Dropped: 0 (0.0%) · Profile: Default
  
```

2.18 Οχι, είναι κρυπτογραφημένα (αν και υποθέτω είναι αυτά με τύπο SSH Client: New Keys, Encrypted Packet, και Server: Encrypted Packet)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssh

No.	Time	Source	Protocol	Length	Destination	Info
4	0.000000	192.168.1.11	SSHv2	82	147.102.40.15	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
5	0.020544	147.102.40.15	SSHv2	103	192.168.1.11	Server: Protocol (SSH-2.0-OpenSSH_6.6.1_hpn13v11 Free)
11	0.005705	192.168.1.11	SSHv2	238	147.102.40.15	Client: Key Exchange Init
12	0.006405	147.102.40.15	SSHv2	534	192.168.1.11	Server: Key Exchange Init
14	0.004156	192.168.1.11	SSHv2	102	147.102.40.15	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
16	0.018682	147.102.40.15	SSHv2	262	192.168.1.11	Server: Elliptic Curve Diffie-Hellman Key Exchange Re
18	4.087260	192.168.1.11	SSHv2	134	147.102.40.15	Client: New Keys, Encrypted packet (len=64)
19	0.011067	147.102.40.15	SSHv2	118	192.168.1.11	Server: Encrypted packet (len=64)
21	1.18	192.168.1.11	SSHv2	131	147.102.40.15	Client: Encrypted packet (len=64)

```

> Transmission Control Protocol, Src Port: 22, Dst Port: 63510, Seq: 1810, Ack: 1413, Len: 64
└ SSH Protocol
  < SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
    Packet Length (encrypted): ac9d210b
    Encrypted Packet: 43304c65b6cd29d66cabf874e0cf9ebce36fd121a5c86b5d0c0ac797
    MAC: 940c4aea82738a1822223c9ea25ec8f344a76068de34fb56e2f886fa097de0d3
    [Direction: server-to-client]

0000 f8 63 3f 59 24 c8 d0 b6 6f a7 bb 50 08 00 45 00  .c?Y$... o..P..E...
0010 00 68 e2 50 40 00 3a 06 e1 16 93 66 28 0f c0 a8  .h-P@:. ....f...
0020 01 0b 00 16 f8 16 50 9c 5e 4c 49 c7 f1 54 50 18  .....P. ^L1..TP.
0030 04 06 07 ce 00 00 ac 9d 21 0b 43 30 4c 65 b6 cd  .....! C0Le..
0040 29 d6 6c ab f8 74 e0 cf 9e bc e3 6f d1 21 a5 c8  )..l..t. ....o..!
0050 6b 5d 0c 0a c7 97 94 0c 4a ea 82 73 8a 18 22 22  k].... J..s..""

SSH Protocol: Protocol
Packets: 34 · Displayed: 16 (47.1%) · Dropped: 0 (0.0%) · Profile: Default
  
```

2.19 Πιστοποίηση της αυθεντικότητας: Με την χρήση public-private keys, Εμπιστευτικότητα: Με την κρυπτογράφηση των μυνημάτων/δεδομένων, Ακεραιότητα: Με την συμπίεση των compress και Mac

3

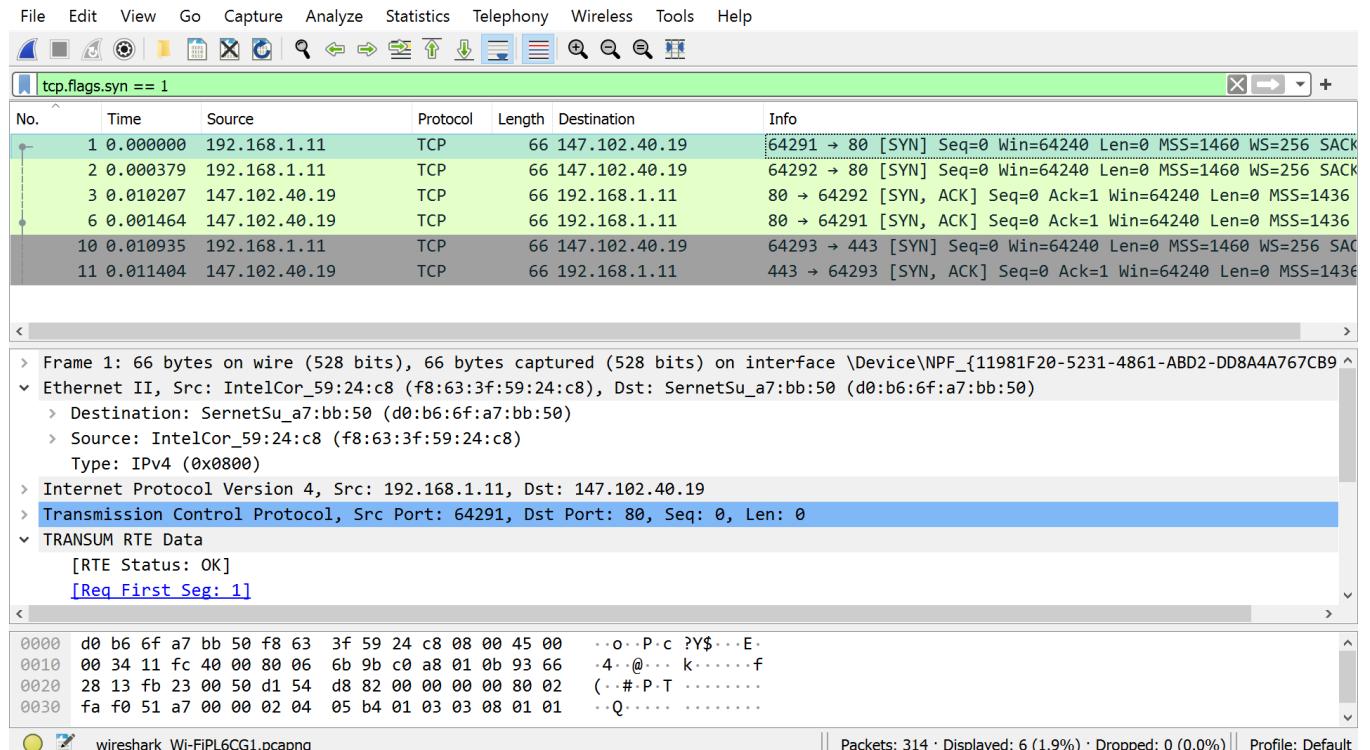
3.1 host bbb2.cn.ntua.gr

3.2 tcp.flags.syn == 1

3.3 Οι θύρες 80 και 443

3.4 Η 80 αντιστοιχεί στο πρωτόκολλο εφαρμογής HTTP, η 443 στο HTTPS

3.5 3 στην περίπτωση του HTTP

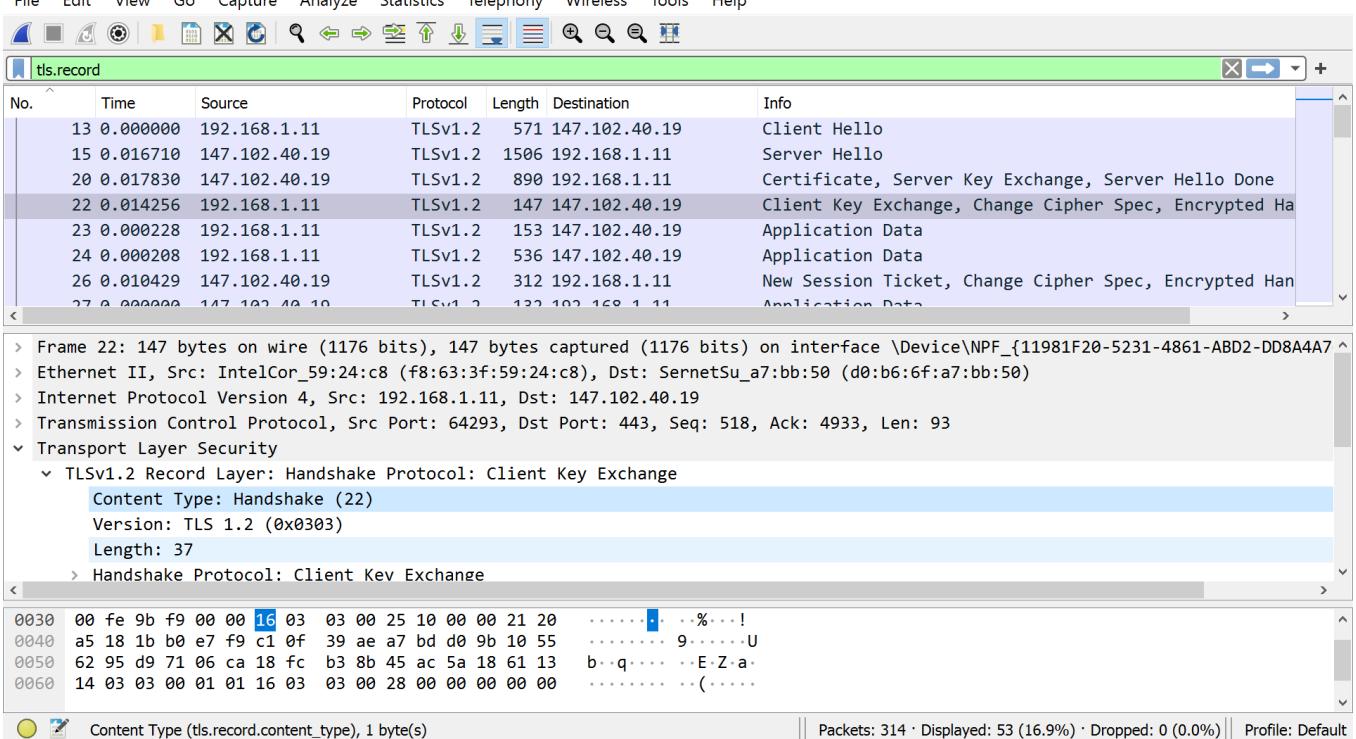


και 1 στου HTTPS (από τον αριθμό 293 και μετά)

3.6 Η θύρα 64293

3.7 Content Type: 1 byte, Version: 2 bytes και Length: 2 bytes

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

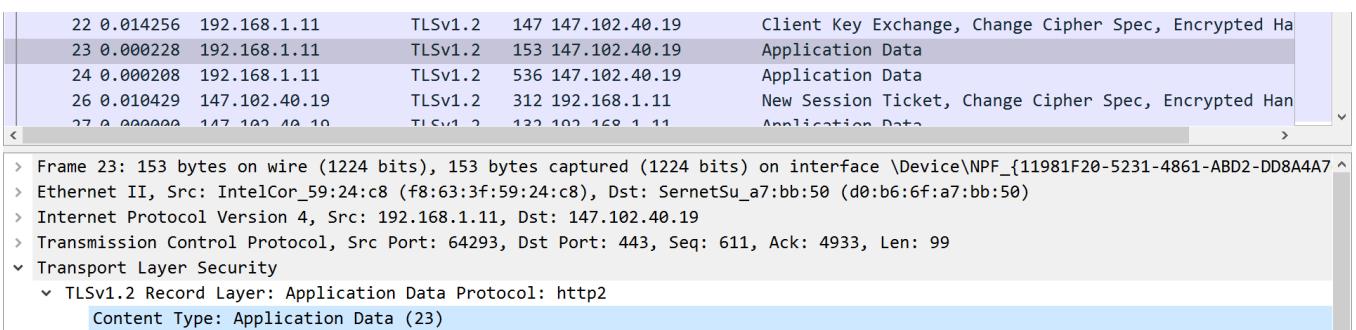


The screenshot shows a Wireshark capture titled "tls.record". The packet list pane displays a sequence of TLS frames. The details pane shows the structure of a TLSv1.2 Client Key Exchange message, including fields like Content Type (Handshake (22)), Version (TLS 1.2 (0x0303)), and Length (37). The bytes pane shows the raw hex and ASCII data for these fields. The bottom status bar indicates 314 total packets, 53 displayed (16.9%), 0 dropped (0.0%), and the profile set to Default.

3.8 Content Type: Handshake(22)

Content Type: Application Data (23)

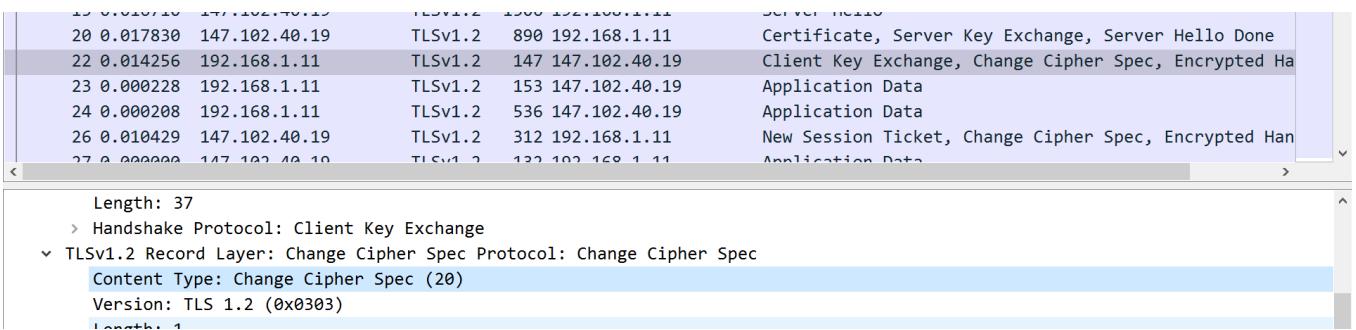
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



This section of the Wireshark capture shows Application Data frames (Content Type 23). It includes frames 23 (153 bytes), 24 (536 bytes), and 26 (312 bytes). The details pane shows the structure of an Application Data message, including Content Type (Application Data (23)). The bottom status bar indicates 314 total packets, 53 displayed (16.9%), 0 dropped (0.0%), and the profile set to Default.

Content Type: Change Cipher Spec (20)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



This section shows Change Cipher Spec frames (Content Type 20). It includes frames 20 (890 bytes), 22 (147 bytes), and 23 (153 bytes). The details pane shows the structure of a Change Cipher Spec message, including Content Type (Change Cipher Spec (20)) and Version (TLS 1.2 (0x0303)). The bottom status bar indicates 314 total packets, 53 displayed (16.9%), 0 dropped (0.0%), and the profile set to Default.

3.9 Client Hello (1), Server Hello (2), Certificate (11), Server Key Exchange (12), Client Key Exchange (16), Encrypted Handshake Message, Server Hello Done (14), New Session Ticket (4)

3.10 Έστειλε 1 μήνυμα hello που αντιστοιχεί στη 1 σύνδεση με πρωτόκολλο TCP

3.11 Είναι η TLS1.0

Time	Source	Protocol	Length	Destination	Info
0.000000	192.168.1.11	TLSv1.2	571	147.102.40.19	Client Hello
0.016710	147.102.40.19	TLSv1.2	1506	192.168.1.11	Server Hello
0.017830	147.102.40.19	TLSv1.2	890	192.168.1.11	Certificate, Server Key Exchange, Server Hello Done
0.014256	192.168.1.11	TLSv1.2	147	147.102.40.19	Client Key Exchange, Change Cipher Spec, Encrypted Handshake ...
0.000228	192.168.1.11	TLSv1.2	153	147.102.40.19	Application Data
0.000208	192.168.1.11	TLSv1.2	536	147.102.40.19	Application Data
0.010429	147.102.40.19	TLSv1.2	312	192.168.1.11	New Session Ticket, Change Cipher Spec, Encrypted Handshake M...
0.000000	147.102.40.19	TLSv1.2	132	192.168.1.11	Application Data

```

> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 147.102.40.19
> Transmission Control Protocol, Src Port: 64293, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
  > Transport Layer Security
    > TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    > Handshake Protocol: Client Hello
  > TRANSMISSION RTE Data

```

```

0000 d0 b6 6f a7 bb 50 f8 63 3f 59 24 c8 08 00 45 00 ..o..P..c ?Y$...E.
0010 02 2d 12 03 40 00 80 06 69 9b c0 a8 01 0b 93 66 ...@... i....f
0020 28 13 fb 25 01 bb 3b 5d df ea 8d 25 03 d8 50 18 (%-;) ...%..P.
0030 01 02 dc 8e 00 00 16 03 01 02 00 01 00 01 fc 03 .....

```

Transport Layer Security: Protocol | Packets: 314 · Displayed: 53 (16.9%) · Dropped: 0 (0.0%) | Profile: Default

3.12 24 b7 50 aa ... (συνολικά 32 bytes)

No.	Time	Source	Protocol	Length	Destination	Info
13	0.000000	192.168.1.11	TLSv1.2	571	147.102.40.19	Client Hello
15	0.016710	147.102.40.19	TLSv1.2	1506	192.168.1.11	Server Hello
20	0.017830	147.102.40.19	TLSv1.2	890	192.168.1.11	Certificate, Server Key Exchange, Server Hello Done
22	0.014256	192.168.1.11	TLSv1.2	147	147.102.40.19	Client Key Exchange, Change Cipher Spec, Encrypted Handshake ...
23	0.000228	192.168.1.11	TLSv1.2	153	147.102.40.19	Application Data
24	0.000208	192.168.1.11	TLSv1.2	536	147.102.40.19	Application Data
26	0.010429	147.102.40.19	TLSv1.2	312	192.168.1.11	New Session Ticket, Change Cipher Spec, Encrypted Handshake ...

```

Length: 512
  > Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
    > Random: 24b750aaa386ce60136e71b6f441d6875b61185dd0a6d20788c780740454dc04
      GMT Unix Time: Jul 9, 1989 16:18:34.000000000 Θερινή ώρα GTB
      Random Bytes: a386ce60136e71b6f441d6875b61185dd0a6d20788c780740454dc04
    Session ID Length: 32

```

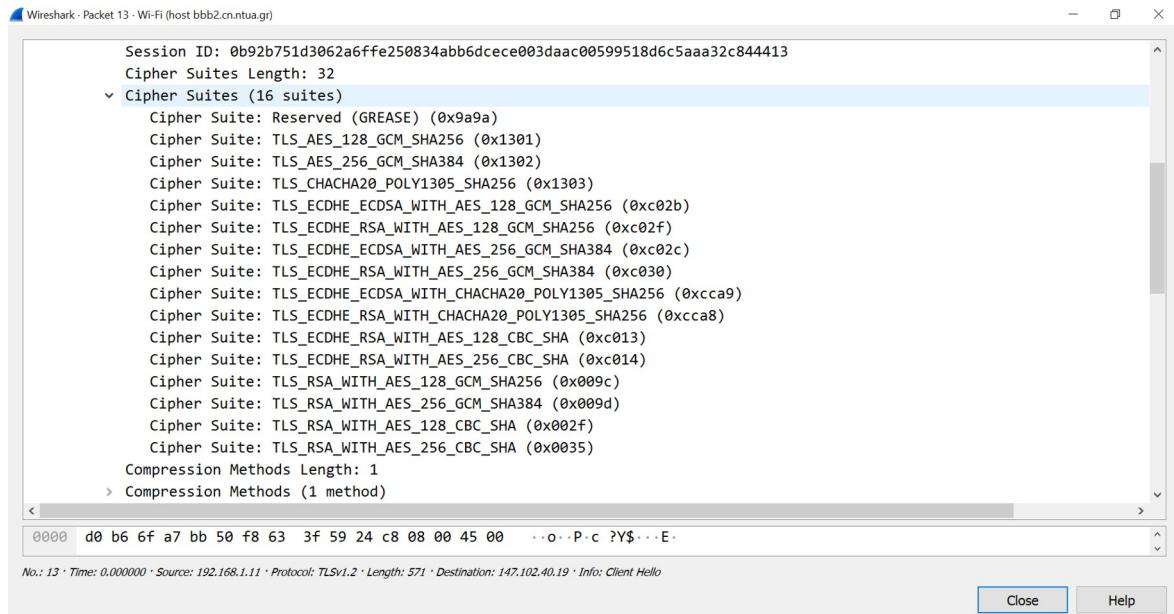
```

0040 03 24 b7 50 aa a3 86 ce 60 13 6e 71 b6 f4 41 d6 .$.P....`..nq..A.
0050 87 5b 61 18 5d d0 a6 d2 07 88 c7 80 74 04 54 dc .[a]....t.T.
0060 04 20 0b 92 b7 51 d3 06 2a 6f fe 25 08 34 ab b6 .Q..*o.%4..
0070 dc ec e0 03 da ac 00 59 95 18 d6 c5 aa a3 2c 84 .....

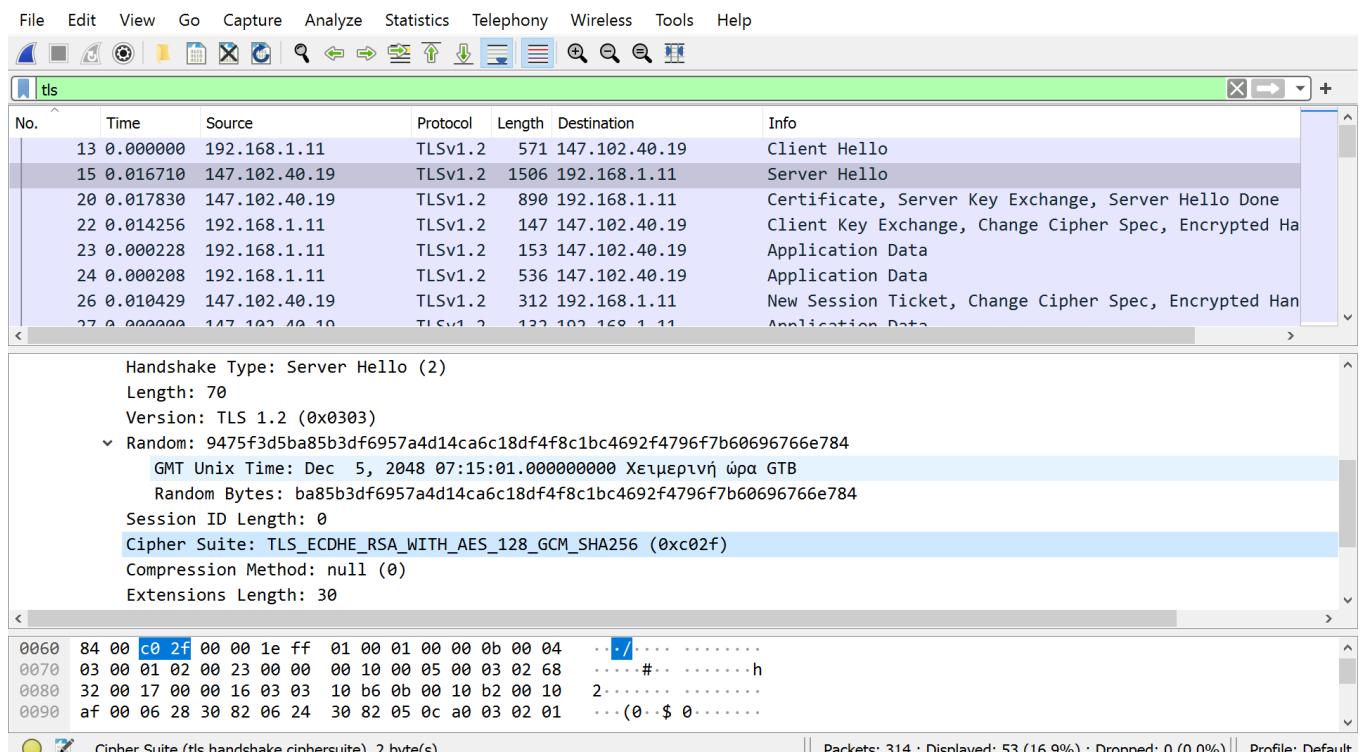
```

Τα 4 πρώτα bytes κανονικά αναπαριστούν τη χρονική στιγμή της αποστολής του πακέτου (εδώ όχι, η χρονική στιγμή είναι τυχαία)

3.13 16 suites στο πλήθος. Η 16δική μορφή των 2 πρώτων: 0x9a9a και 0x1301

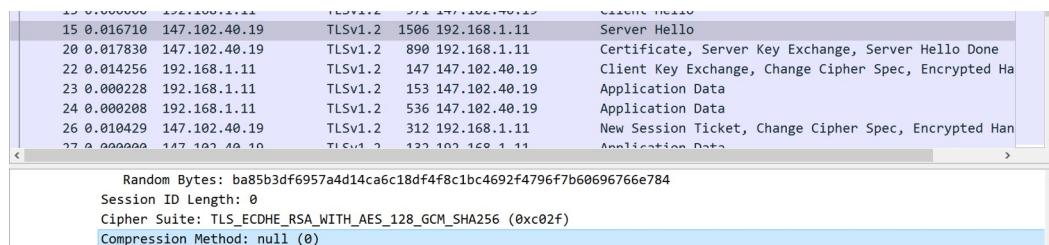


3.14 Version: TLS 1.2 (0x0303). Η συνίτα κωδίκων κρυπτογράφησης: 0xc02f



3.15 Μήκος: 32 bytes. 4 πρώτα byte του τυχαίου μέρους: ba 85 b3 df

3.16 Όχι



3.17 Αλγόριθμος ανταλλαγής κλειδιών: ECDHE, Αλγόριθμος πιστοποίησης ταυτότητας: RSA, Αλγόριθμος κρυπτογράφησης: AES_128_GCM, Συνάρτηση κατακερματισμού: SHA256

3.18 890 bytes

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

No.	Time	Source	Protocol	Length	Destination	Info
13	0.000000	192.168.1.11	TLSv1.2	571	147.102.40.19	Client Hello
15	0.016710	147.102.40.19	TLSv1.2	1506	192.168.1.11	Server Hello
20	0.017830	147.102.40.19	TLSv1.2	890	192.168.1.11	Certificate, Server Key Exchange, Server Hello Done
22	0.014256	192.168.1.11	TLSv1.2	147	147.102.40.19	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	0.000228	192.168.1.11	TLSv1.2	153	147.102.40.19	Application Data
24	0.000208	192.168.1.11	TLSv1.2	536	147.102.40.19	Application Data
26	0.010429	147.102.40.19	TLSv1.2	312	192.168.1.11	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
27	0.000000	147.102.40.19	TLSv1.2	122	192.168.1.11	Application Data

```
> Frame 20: 890 bytes on wire (7120 bits), 890 bytes captured (7120 bits) on interface \Device\NPF_{11981F20-5231-4861-ABD2-DD8A4A767
> Ethernet II, Src: SernetSu_a7:bb:50 (d0:b6:6f:a7:bb:50), Dst: IntelCor_59:24:c8 (f8:63:3f:59:24:c8)
> Internet Protocol Version 4, Src: 147.102.40.19, Dst: 192.168.1.11
> Transmission Control Protocol, Src Port: 443, Dst Port: 64293, Seq: 4097, Ack: 518, Len: 836
> [4 Reassembled TCP Segments (4283 bytes): #15(1373), #16(1452), #17(1192), #20(266)]
> Transport Layer Security
> Transport Layer Security
```

Frame (890 bytes) Reassembled TCP (4283 bytes)

Source Port (tcp.srcport), 2 byte(s) || Packets: 314 · Displayed: 53 (16.9%) · Dropped: 0 (0.0%) || Profile: Default

3.19 Μεταφέρονται 3 πιστοποιητικά:

Certificate:

308206243082050ca003020102021204ead4229242b1869415f3381e70456543b3300d06... (id-at-commonName=bbb2.cn.ntua.gr)

Certificate:

30820516308202fea003020102021100912b084acf0c18a753f6d62e25a75f5a300d0609... (id-at-commonName=R3,id-at-organizationName=Let's Encrypt,id-at-countryName=US)

Kαι Certificate:

3082056030820448a00302010202104001772137d4e942b8ee76aa3c640ab7300d06092a... (id-at-commonName=ISRG Root X1,id-at-organizationName=Internet Security Research Group,id-at-countryName=US)

Certificates Length: 1576 bytes

- Certificates (4271 bytes)
 - Certificate Length: 1576 bytes
 - Certificate: 308206243082050ca003020102021204ead4229242b1869415f3381e70456543b3300d06... (id-at-commonName=bbb2.cn.ntua.gr)
 - Certificate Length: 1306 bytes
 - Certificate: 30820516308202fea003020102021100912b084acf0c18a753f6d62e25a75f5a300d0609... (id-at-commonName=R3,id-at-organizationName=Let's Encrypt,id-at-countryName=US)
 - Certificate Length: 1380 bytes
 - Certificate: 3082056030820448a00302010202104001772137d4e942b8ee76aa3c640ab7300d06092a... (id-at-commonName=ISRG Root X1)

3.20 Παρατηρώ 4 πλαίσια Ethernet.

3.21 Pubkey: a5181bb0e7f9c10f39aea7bdd09b10556295d97106ca18fcb38b45ac5a186113

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

No.	Time	Source	Protocol	Length	Destination	Info
13	0.000000	192.168.1.11	TLSv1.2	571	147.102.40.19	Client Hello
15	0.016710	147.102.40.19	TLSv1.2	1506	192.168.1.11	Server Hello
20	0.017830	147.102.40.19	TLSv1.2	890	192.168.1.11	Certificate, Server Key Exchange, Server Hello Done
22	0.014256	192.168.1.11	TLSv1.2	147	147.102.40.19	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	0.000228	192.168.1.11	TLSv1.2	153	147.102.40.19	Application Data
24	0.000208	192.168.1.11	TLSv1.2	536	147.102.40.19	Application Data
26	0.010429	147.102.40.19	TLSv1.2	312	192.168.1.11	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
27	0.000000	147.102.40.19	TLSv1.2	122	192.168.1.11	Application Data

Version: TLS 1.2 (0x0303)
Length: 37
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 33
EC Diffie-Hellman Client Params
Pubkey Length: 32
Pubkey: a5181bb0e7f9c10f39aea7bdd09b10556295d97106ca18fcb38b45ac5a186113
TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)

0040 a5 18 1b b0 e7 f9 c1 0f 39 ae a7 bd d0 9b 10 55 9 U
0050 62 95 d9 71 06 ca 18 fc b3 8b 45 ac 5a 18 61 13 b . q . . . E . Z . a .
0060 14 03 03 00 01 01 16 03 03 00 28 00 00 00 00 (.
0070 00 00 00 c1 73 b3 0a dd 54 21 d2 ab 49 d4 10 4d . . . s . . T ! . I . . M

EC Diffie-Hellman client pubkey (tls.handshake.client_point), 32 byte(s) || Packets: 314 · Displayed: 62 (19.7%) · Dropped: 0 (0.0%) || Profile: Default

Άρα για τον πελάτη είναι: Μήκος κλειδιού: 32 bytes με 5 πρώτα γράμματα τα: a5181

Και για τον εξυπηρετητή είναι: Μήκος κλειδιού: 32 bytes με 5 πρώτα γράμματα τα: 2ca12

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

No.	Time	Source	Protocol	Length	Destination	Info
13	0.000000	192.168.1.11	TLSv1.2	571	147.102.40.19	Client Hello
15	0.016710	147.102.40.19	TLSv1.2	1506	192.168.1.11	Server Hello
20	0.017830	147.102.40.19	TLSv1.2	890	192.168.1.11	Certificate, Server Key Exchange, Server Hello Done
22	0.014256	192.168.1.11	TLSv1.2	147	147.102.40.19	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	0.000228	192.168.1.11	TLSv1.2	153	147.102.40.19	Application Data
24	0.000208	192.168.1.11	TLSv1.2	536	147.102.40.19	Application Data
26	0.010429	147.102.40.19	TLSv1.2	312	192.168.1.11	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
27	0.000000	147.102.40.19	TLSv1.2	122	192.168.1.11	Application Data

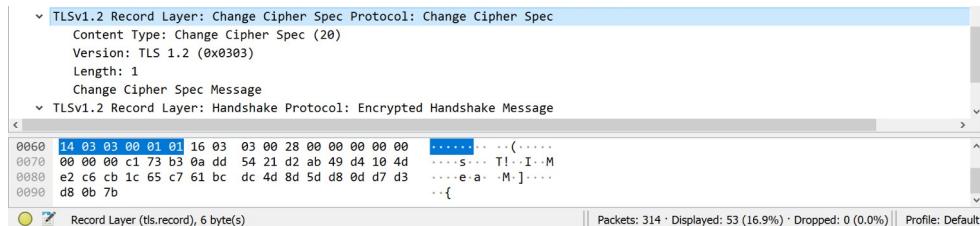
Length: 552
EC Diffie-Hellman Server Params
Curve Type: named_curve (0x03)
Named Curve: x25519 (0x001d)
Pubkey Length: 32
Pubkey: 2ca12dae1495e54f6937765cb01c44e02a510760624a1bd37cf1804d2d213e7c
Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
Signature Length: 512
Signature: 4b4dbe312c0896b58a439d7f43c83f82f242079ead6c58b15773016935e014712a16ec3...
TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

0000 f8 63 3f 59 24 c8 d0 b6 6f a7 bb 50 08 00 45 00 . c ? Y \$. . o . P . E .
0010 03 6c a1 19 40 00 3a 06 1f 46 93 66 28 13 c0 a8 . l . @ : . . F . f (. . .
0020 01 0b 01 bb fb 25 8d 25 13 d8 3b 5d e1 ef 50 18 . . . % . . ; . . P .

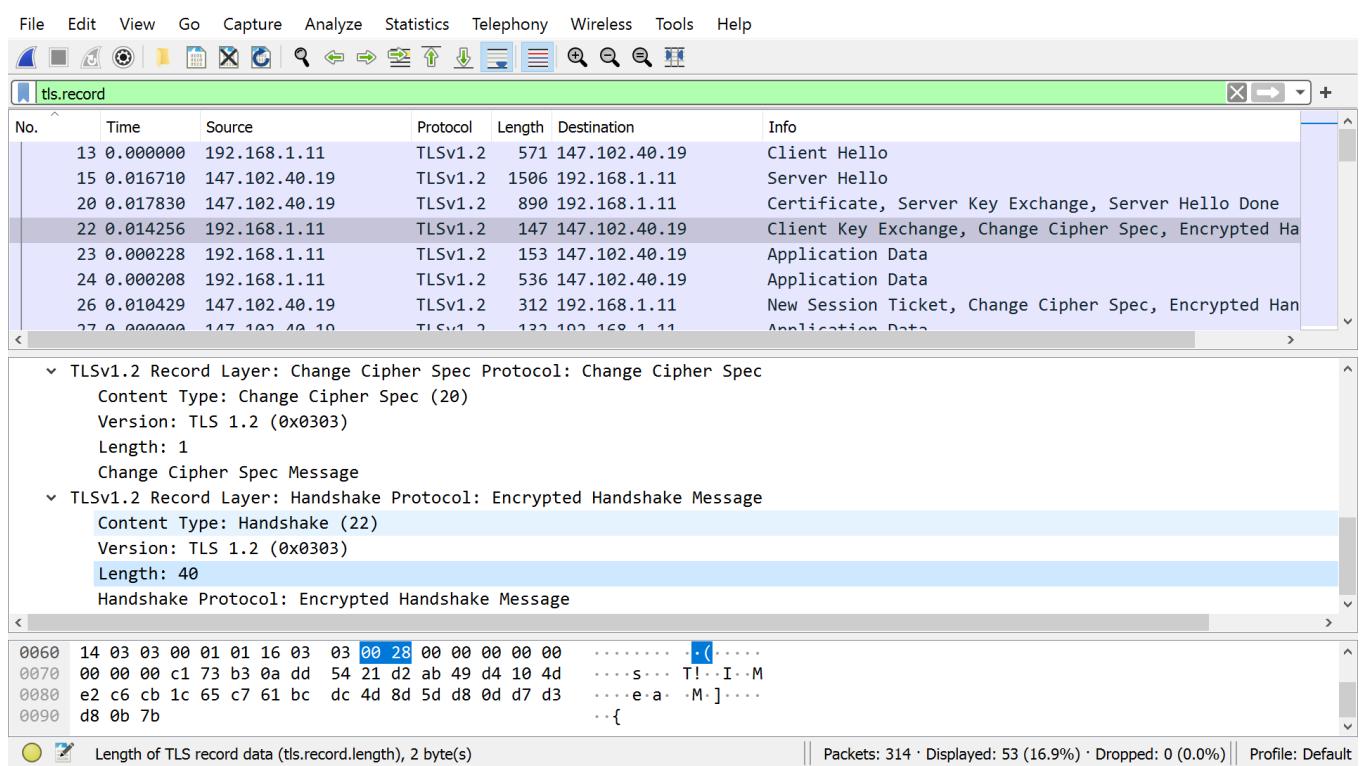
Frame (890 bytes) Reassembled TCP (4283 bytes) || Packets: 314 · Displayed: 62 (19.7%) · Dropped: 0 (0.0%) || Profile: Default

EC Diffie-Hellman client pubkey (tls.handshake.client_point), 32 byte(s) || Packets: 314 · Displayed: 62 (19.7%) · Dropped: 0 (0.0%) || Profile: Default

3.22 6 bytes



3.23 40 bytes



3.24 Ναι

3.25 Όχι (θεωρητικά και από τις 2 πλευρές μπορούν να σταλούν)

3.26 (Λογικά ακολουθεί ο τερματισμός της σύνδεσης στη συγκεκριμένη θύρα)

3.27 Σε καμία περίπτωση δεν μου εμφάνισε τίποτα

3.28 Για το πρωτόκολλο HTTPS: Πιστοποίηση της αυθεντικότητας: Με την χρήση των certificates, Εμπιστευτικότητα: Με την κρυπτογράφηση των μυνημάτων/δεδομένων, Ακεραιότητα: Με χρήση των hash functions