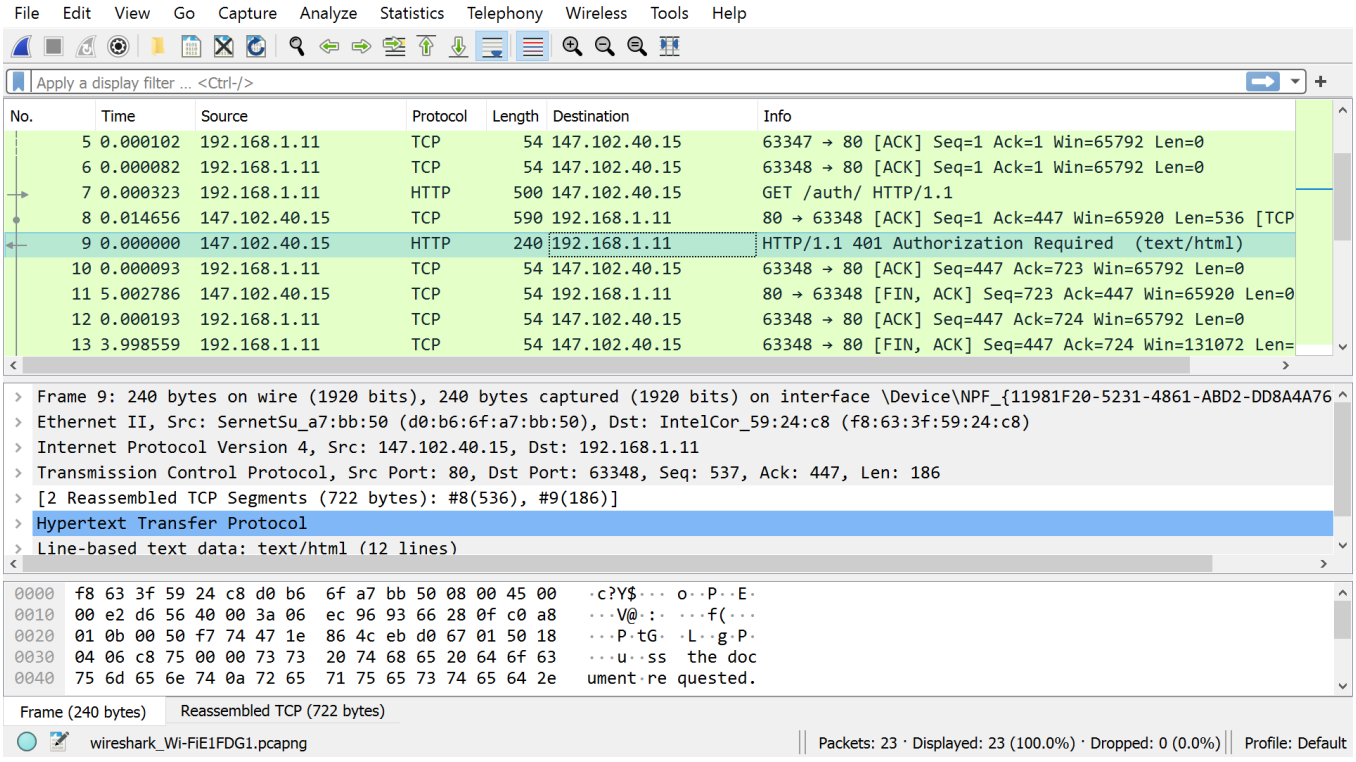
Ονοματεπώνυμο: Άγγελος Μητροκώτσας	**Ομάδα: 6**
Όνομα PC/ΛΣ: DESKTOP-91G20CF/ Windows 10 Pro 20H2	**Ημερομηνία: 20/1/ 2022**
Διεύθυνση IP: 192.168.1.11	**Διεύθυνση MAC: F8-63-3F-59-24-C8**

Εργαστηριακή Άσκηση 12
Ασφάλεια

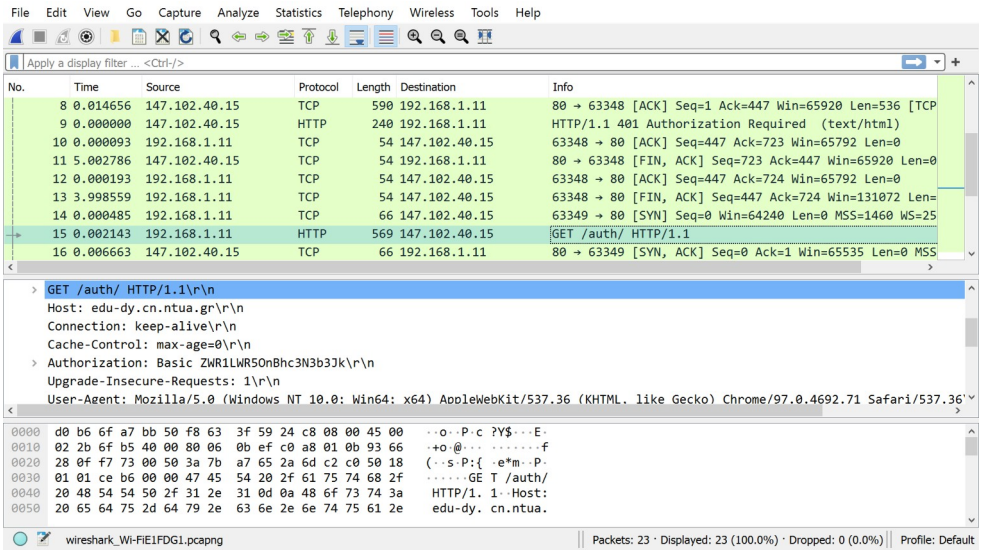
Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 Status code το 401 και φράση Authorization Required



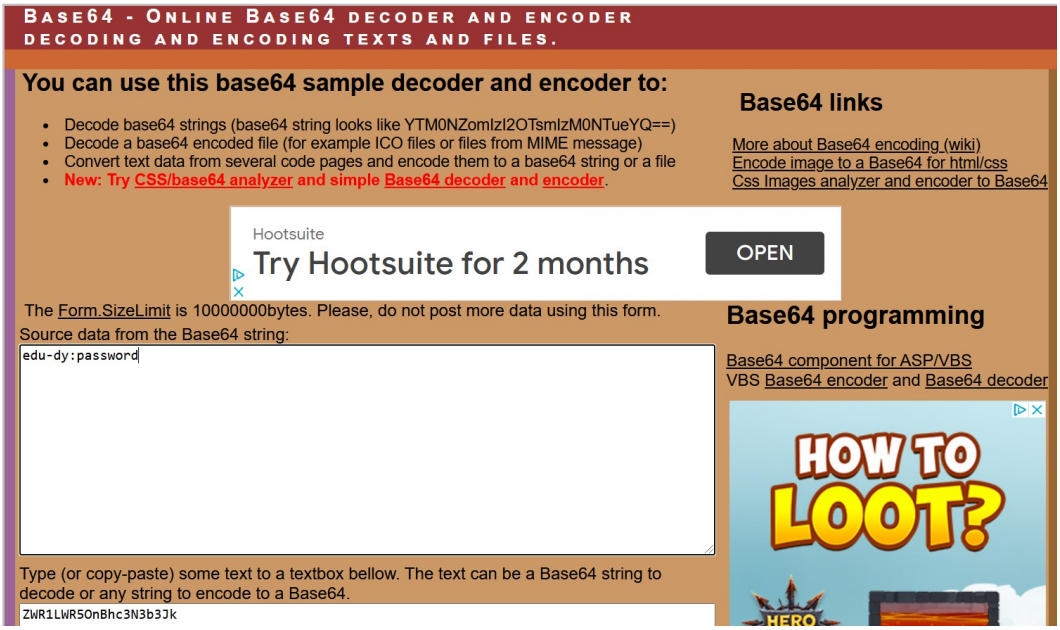
1.2 Το authorization



1.3 Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk

Credentials: edu-dy:password

1.4 edu-dy:password

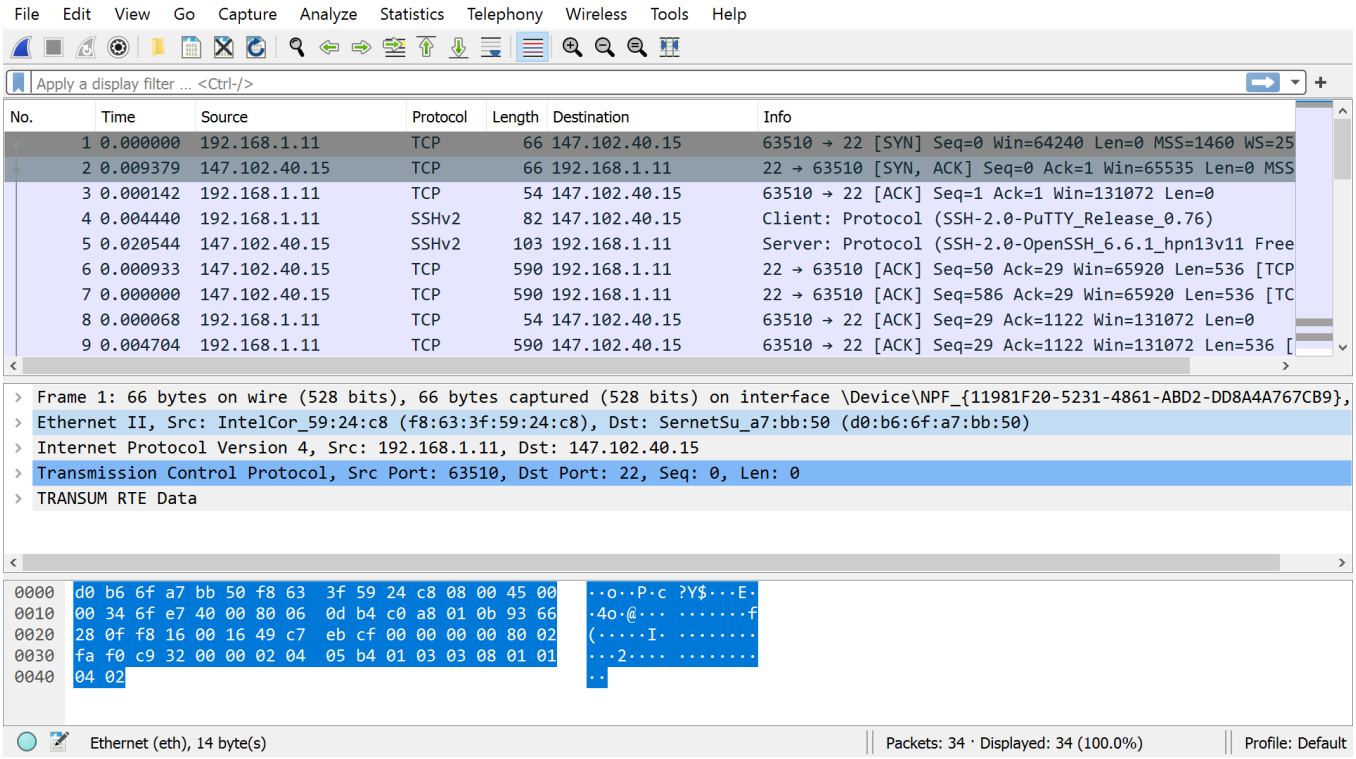


1.5 Ο μηχανισμός ανταλλαγής των credentials που χρησιμοποιείται στο HTTP Base64 είναι πολύ αδύναμος καθώς έχει έλλειψη εμπιστευτικότητας (confidentiality). Οποιοσδήποτε ενδιάμεσος κόμβος μπορεί να μάθει τα στοιχεία ταυτοποίησης του χρήστη

2

2.1 TCP

2.2 Source: 63510, Destination: 22

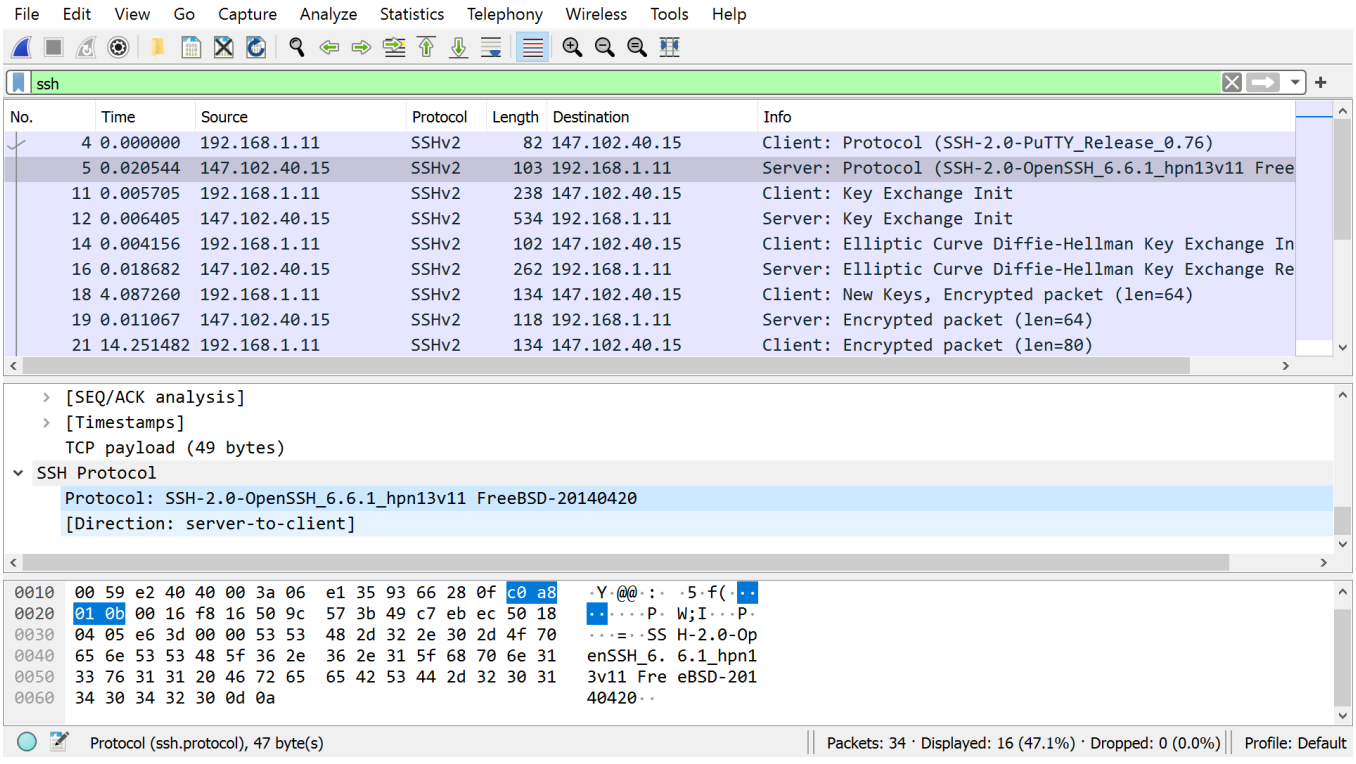


2.3 Η θύρα 22

2.4 ssh

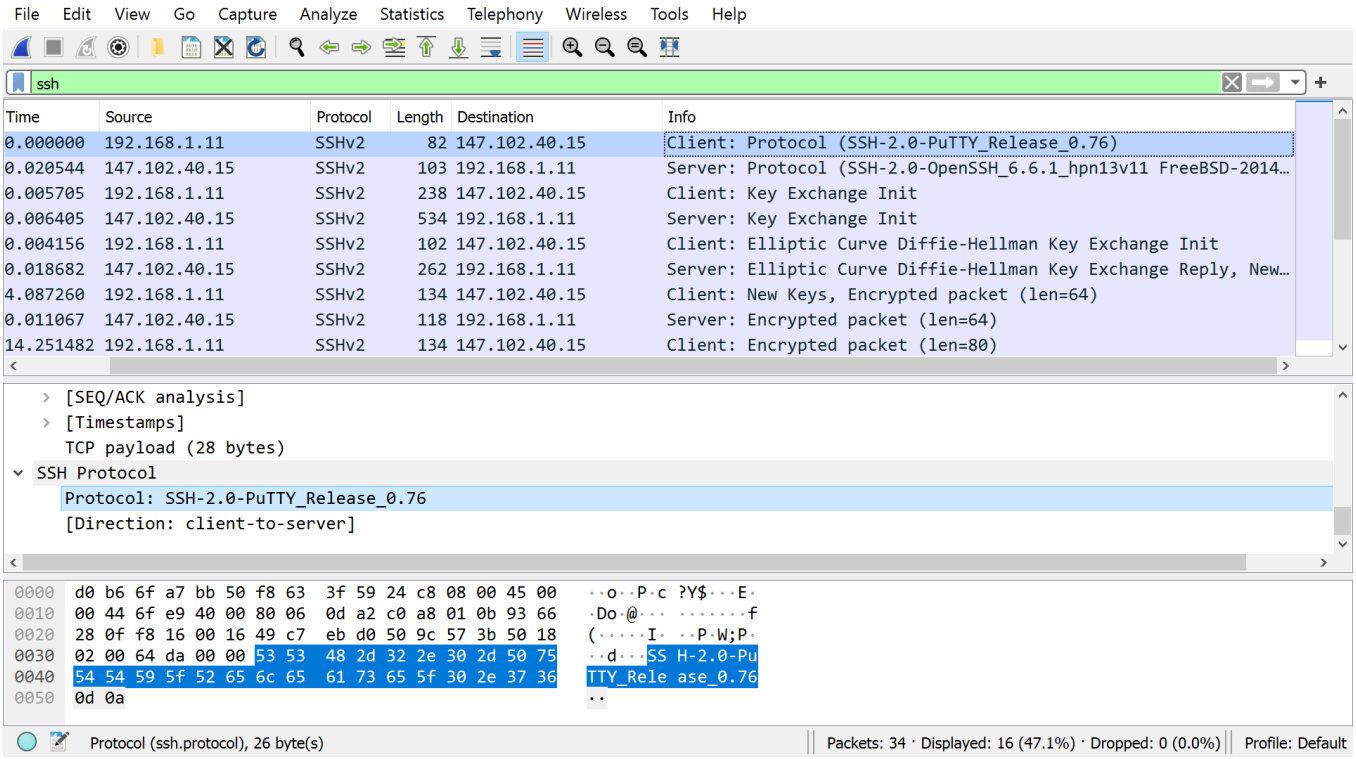
2.5 Έκδοση του πρωτοκόλλου SSH: SSH-2.0

Έκδοση λογισμικού: OpenSSH_6.6.1_hpn13v11 FreeBSD-20140420

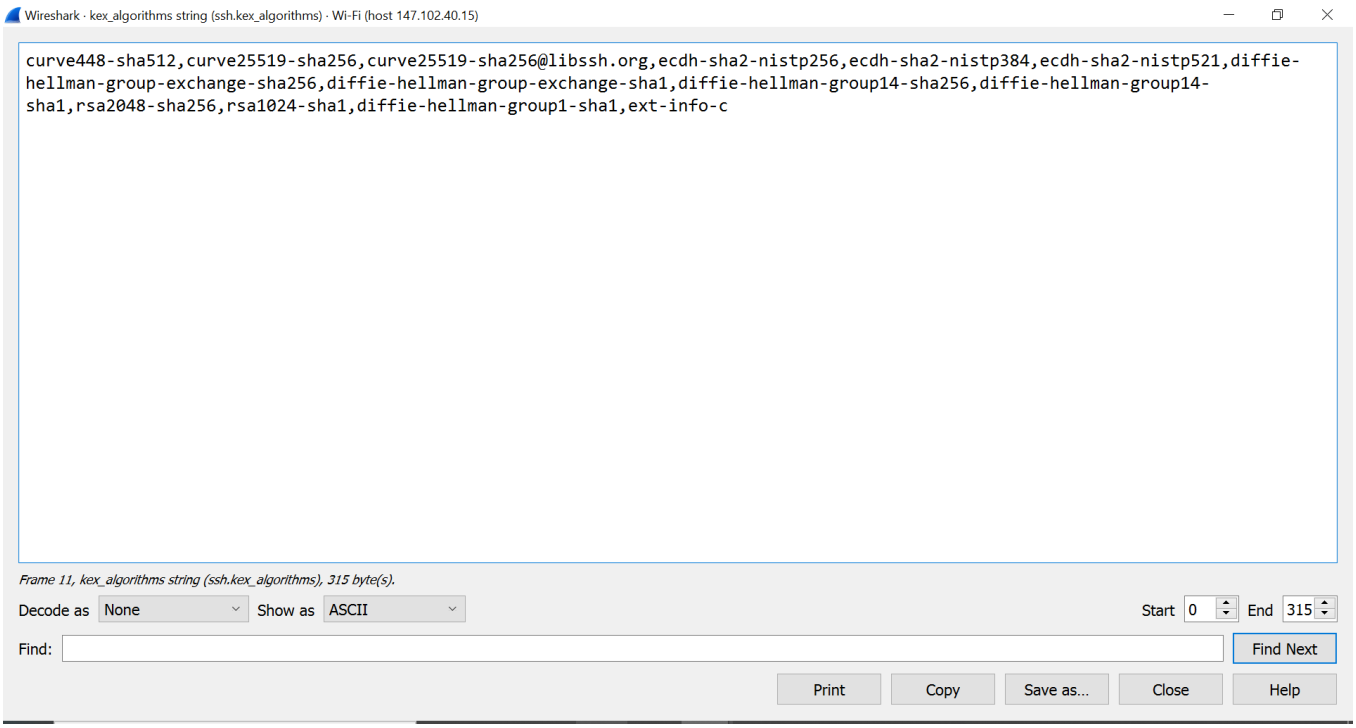


2.6 Έκδοση του πρωτοκόλλου SSH: SSH-2.0

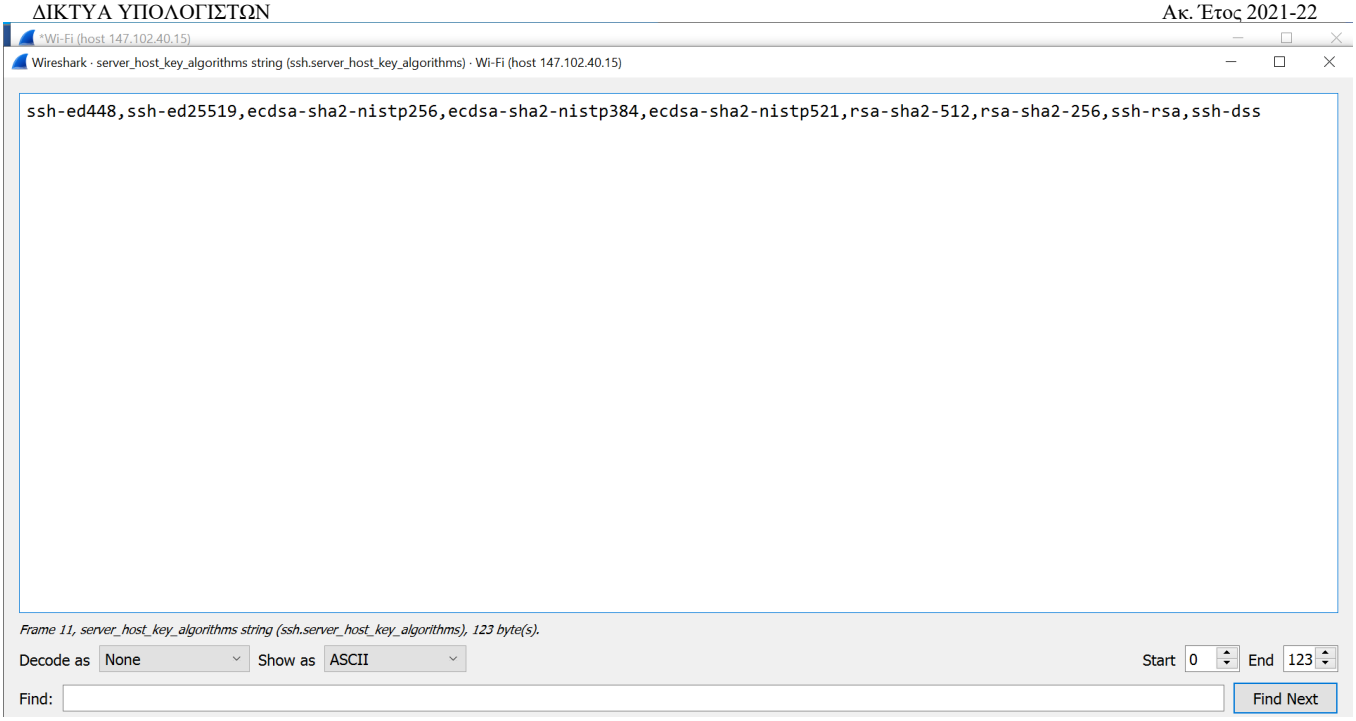
Έκδοση λογισμικού: PuTTY_Release_0.76



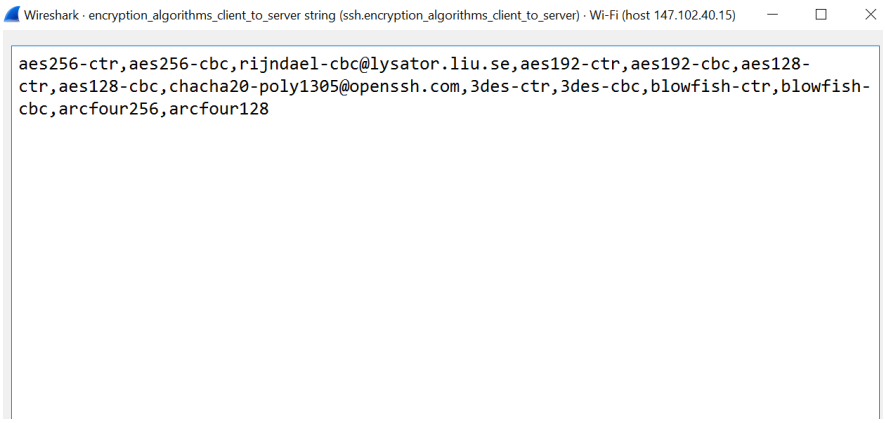
2.7 Συνολικά είναι 13. Οι πρώτοι 2: curve448-sha512,curve25519-sha256



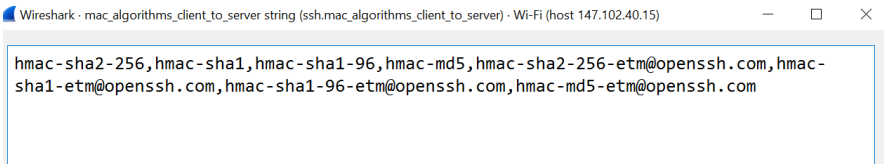
2.8 Είναι 9. Ο πρώτος: ssh-ed448



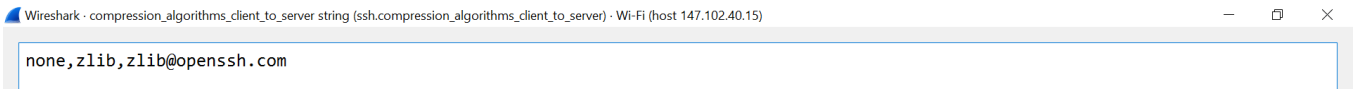
2.9 aes256-ctr, aes256-cbc



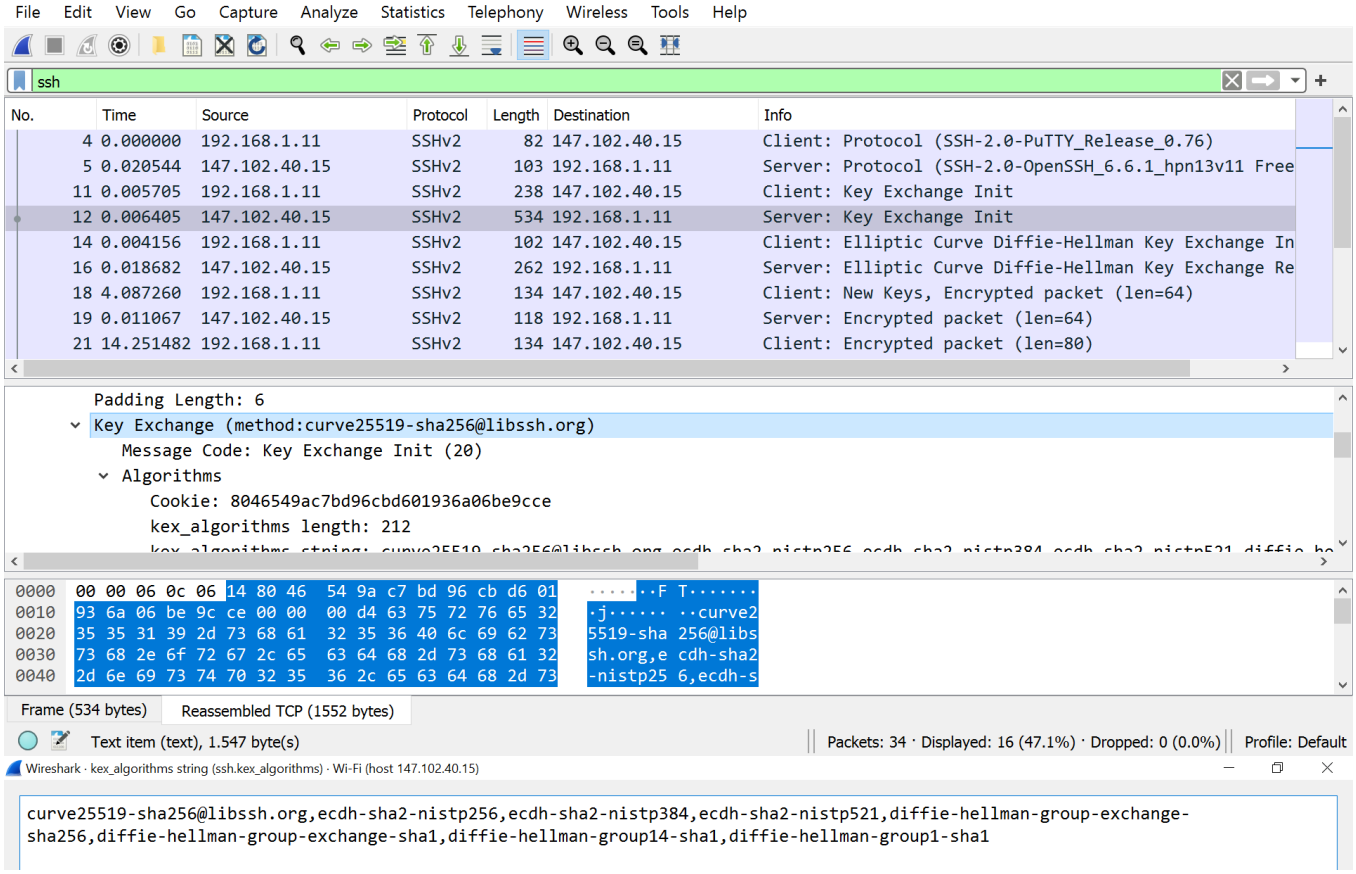
2.10 hmac-sha2-256,hmac-sha1



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



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

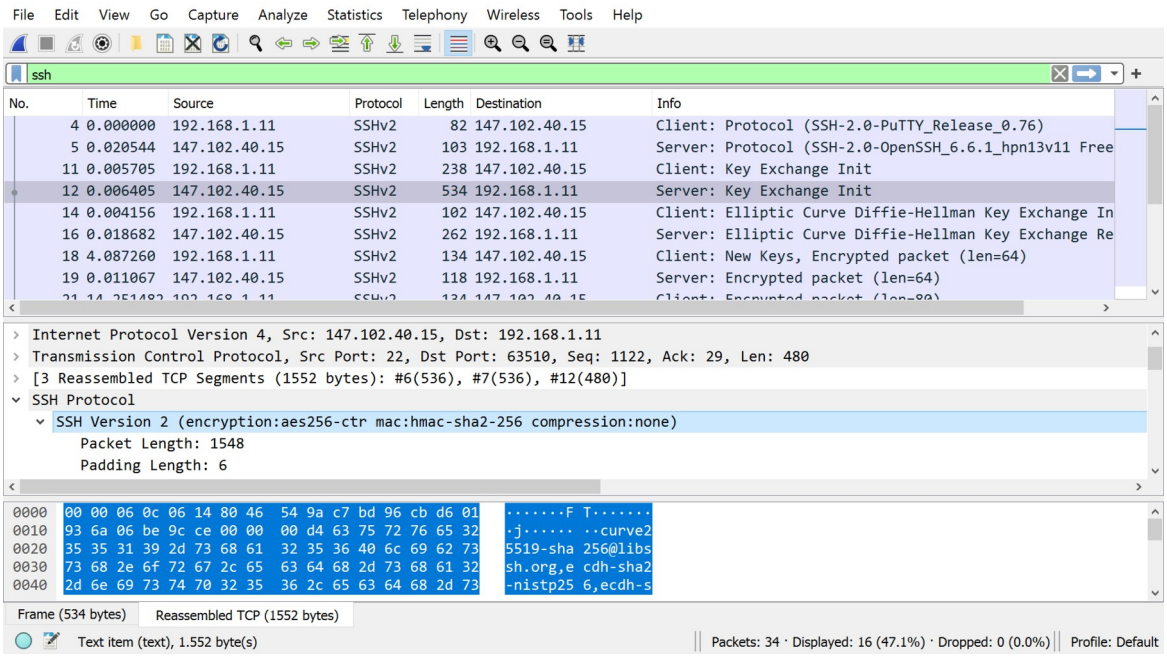


2.13 Τον aes256-ctr

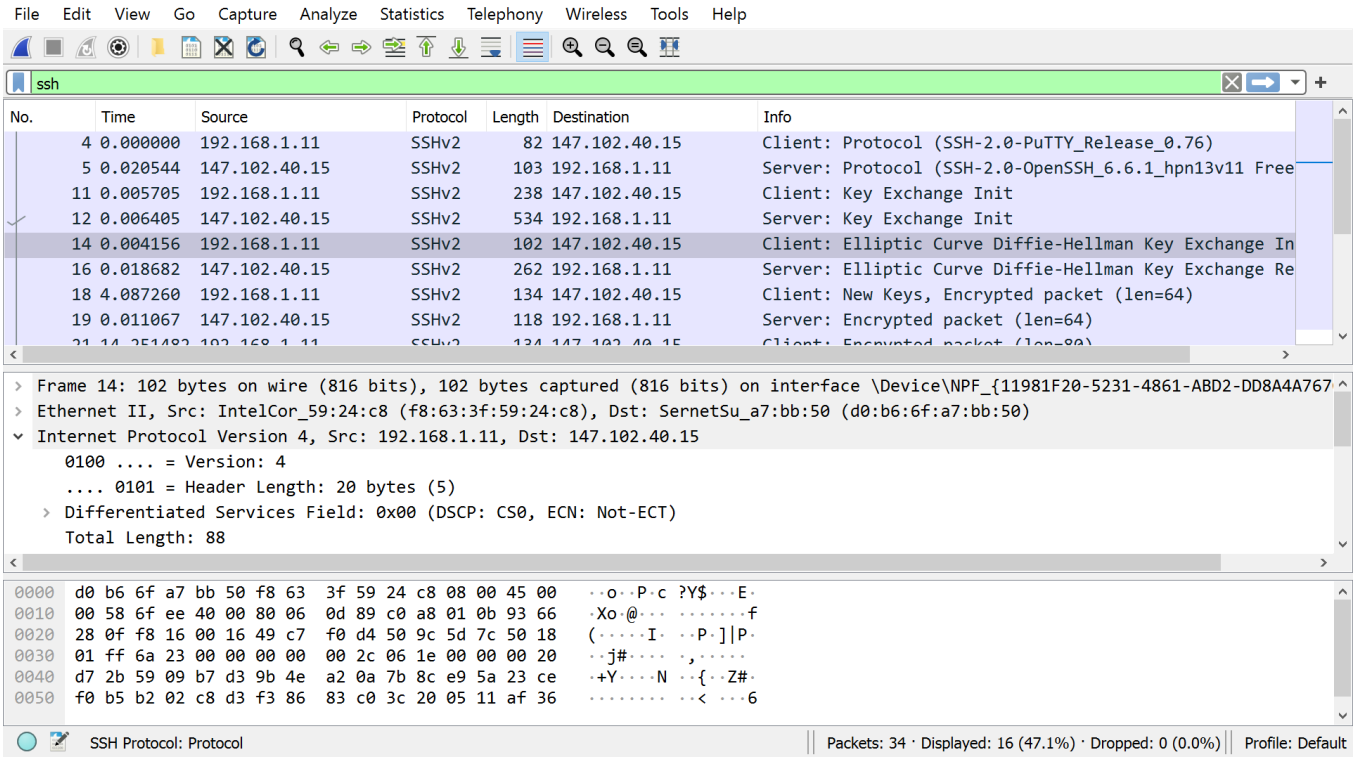
2.14 hmac-sha2-256

2.15 Ο none

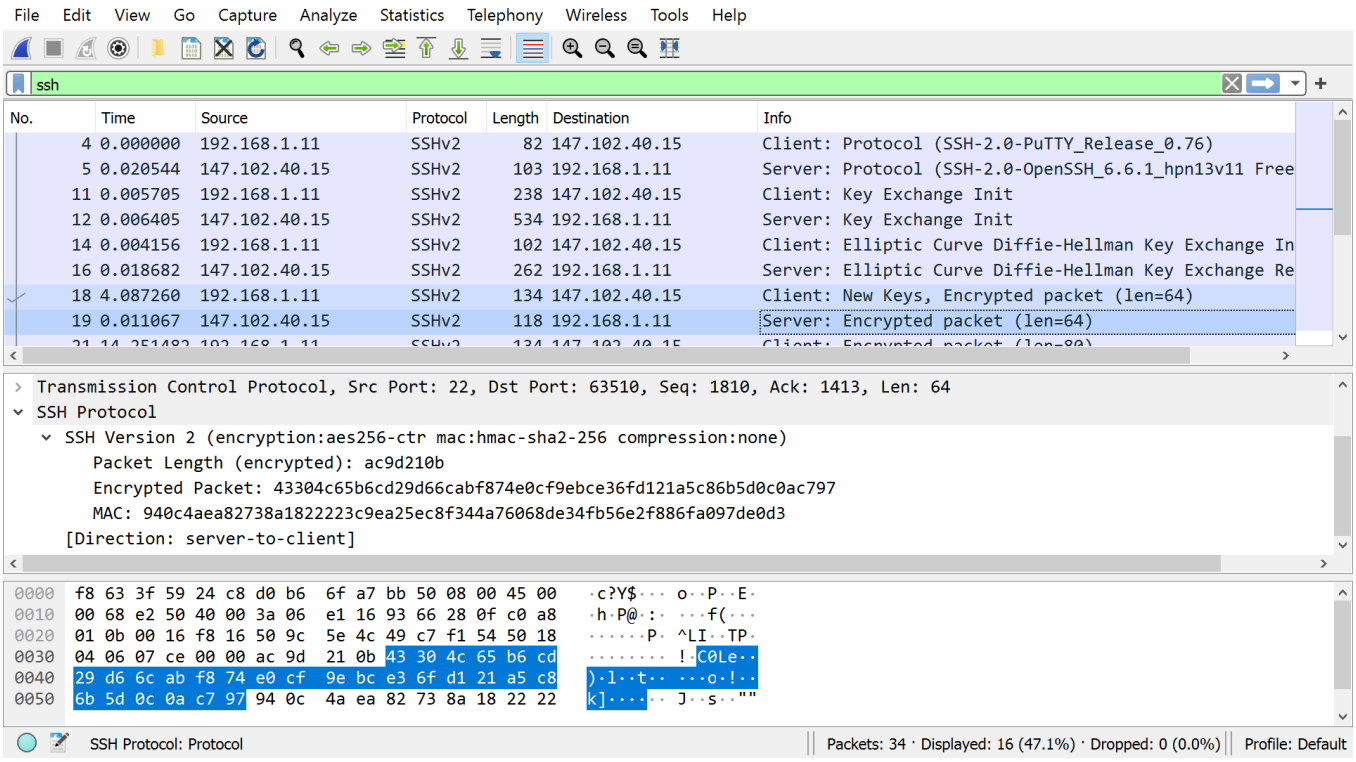
2.16 Ναι, σε παρένθεση δίπλα στο πεδίο SSH Version 2



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



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



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

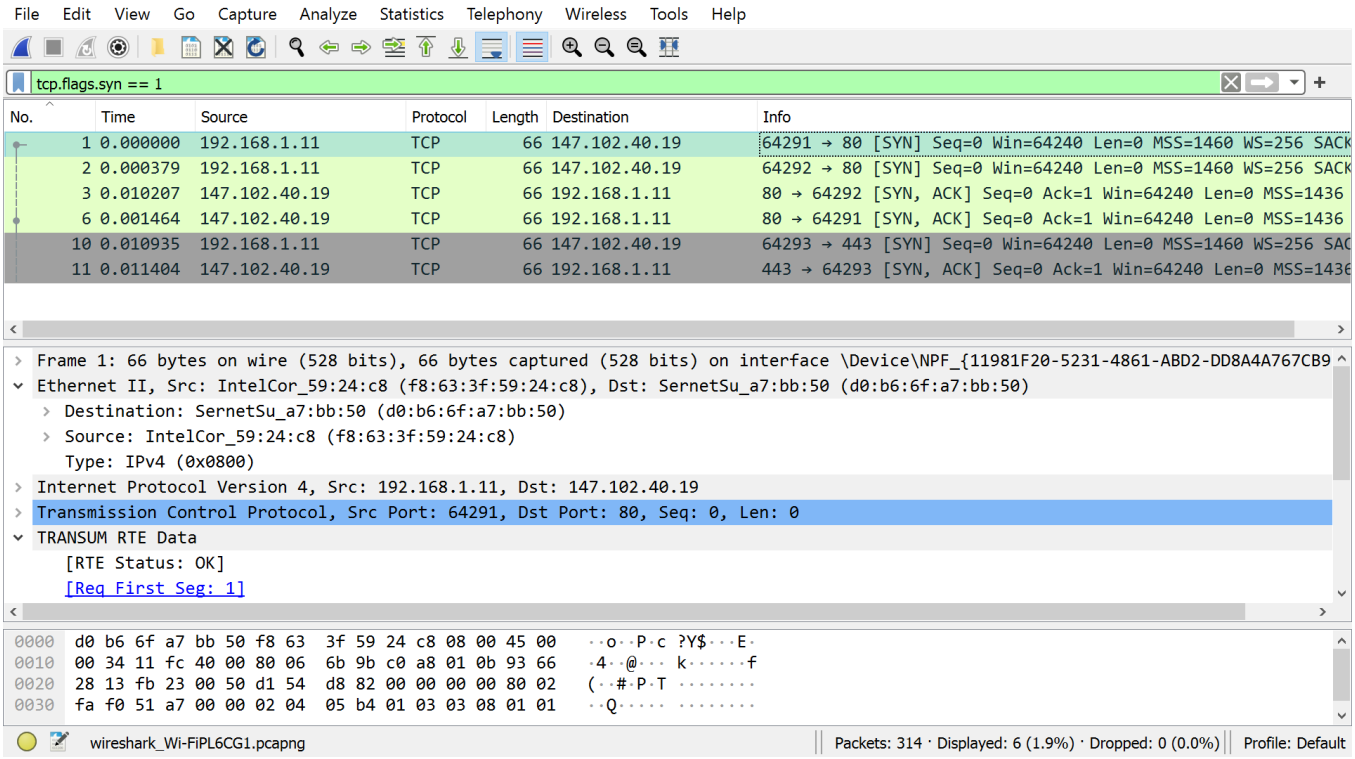
3.1 host bbb2.cn.ntua.gr

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

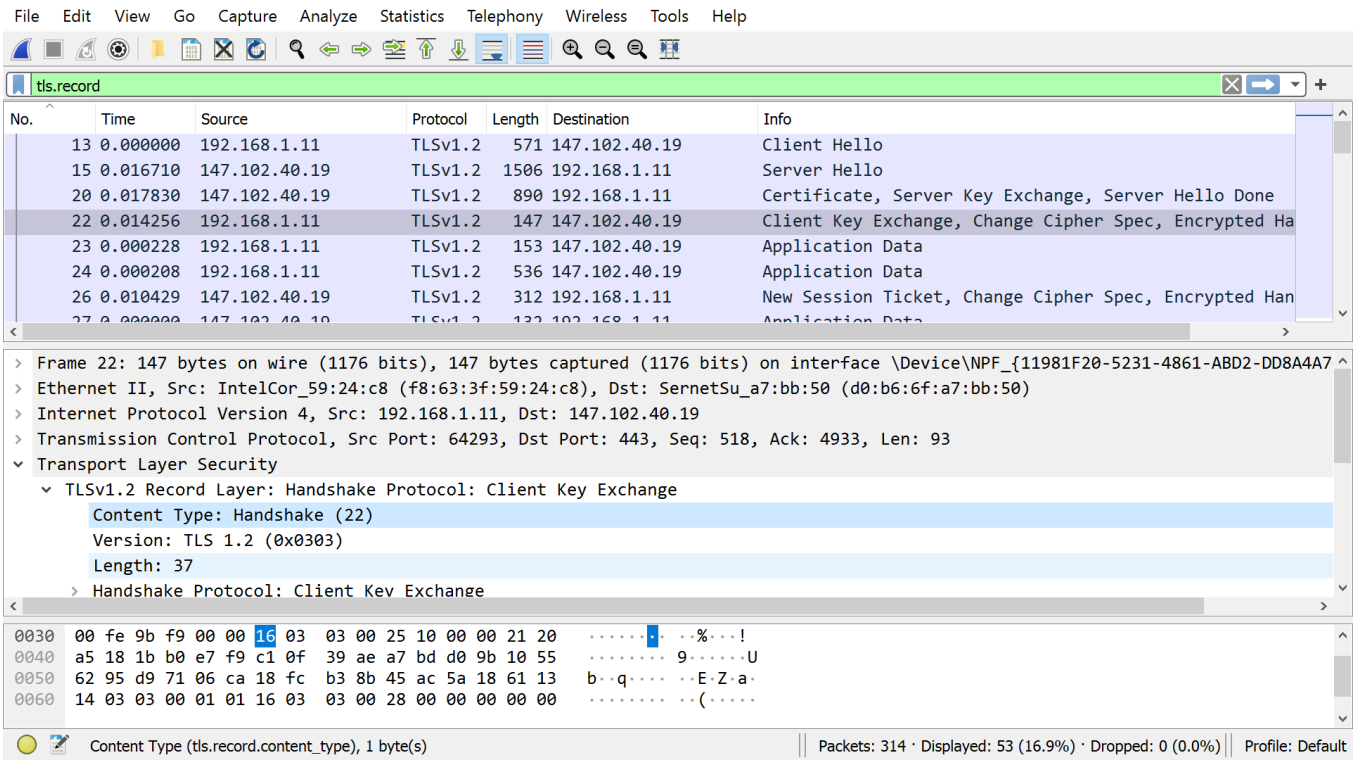
3.5 3 στην περίπτωση του HTTP



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

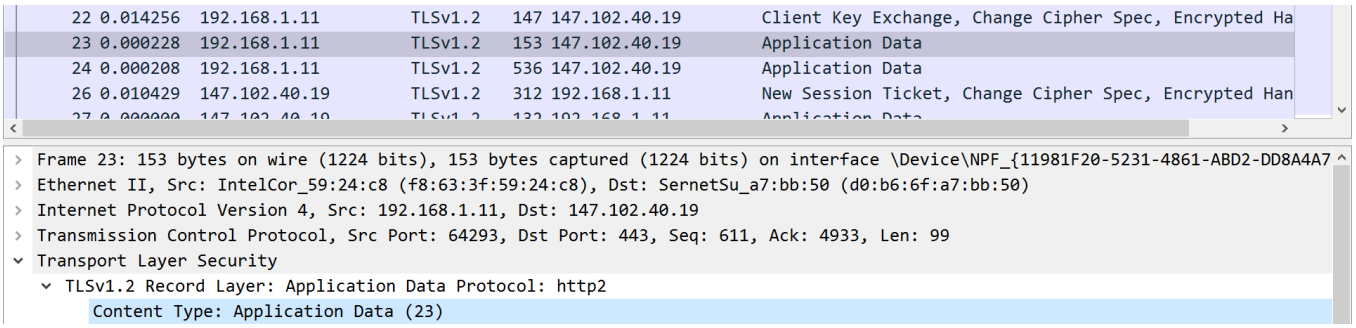
3.6 Η θύρα 64293

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

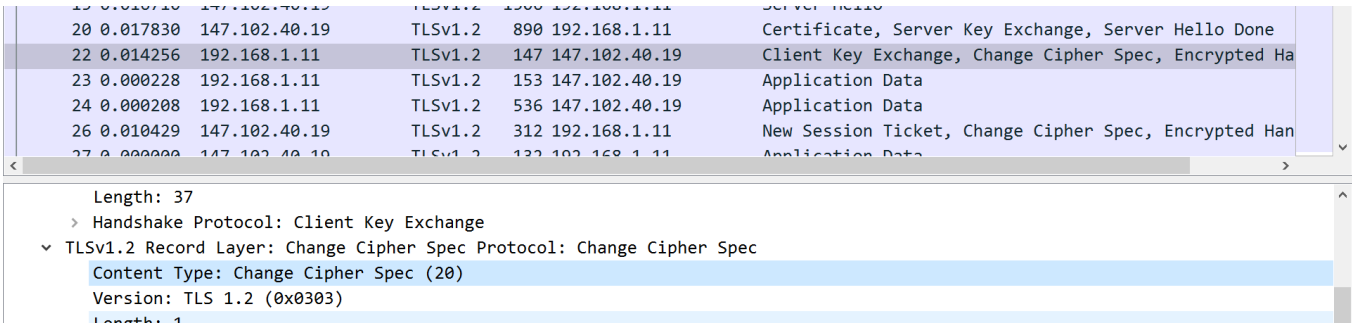


3.8 Content Type: Handshake(22)

Content Type: Application Data (23)



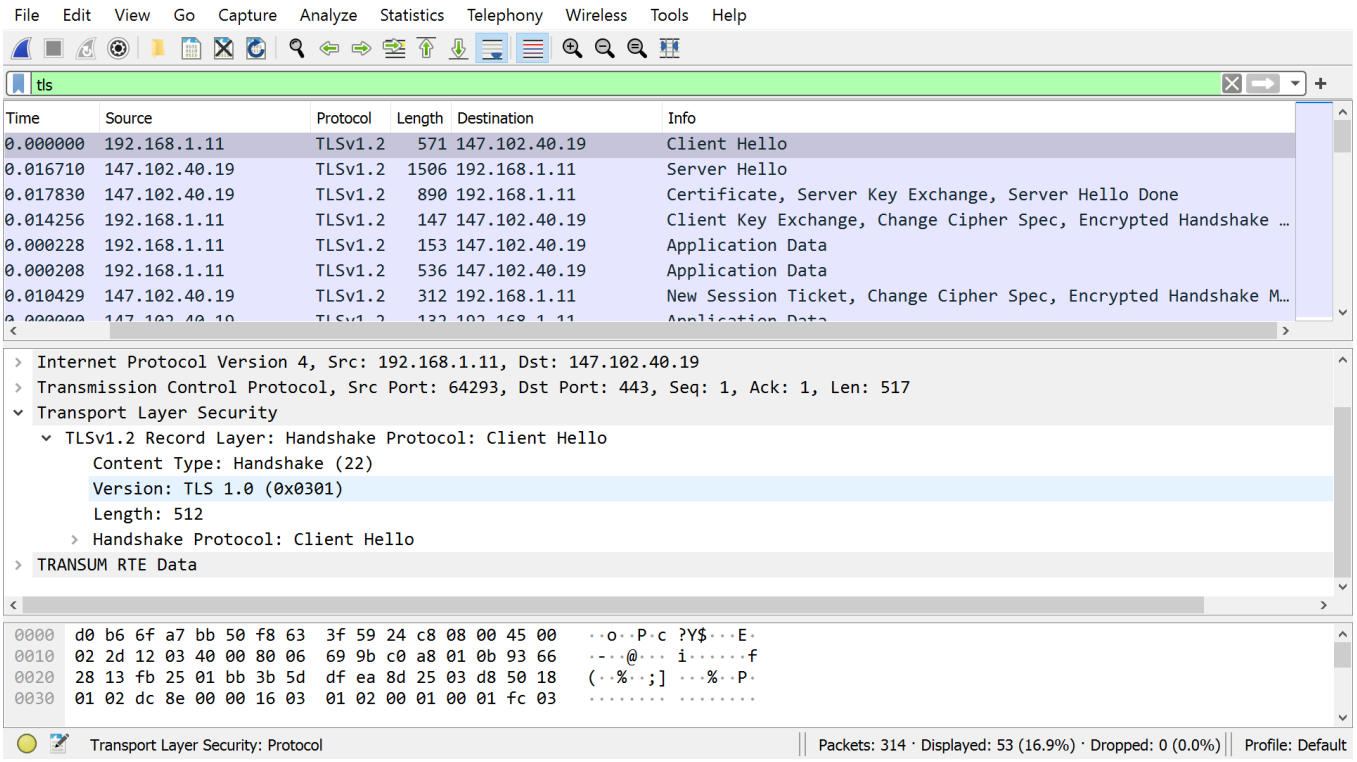
Content Type: Change Cipher Spec (20)



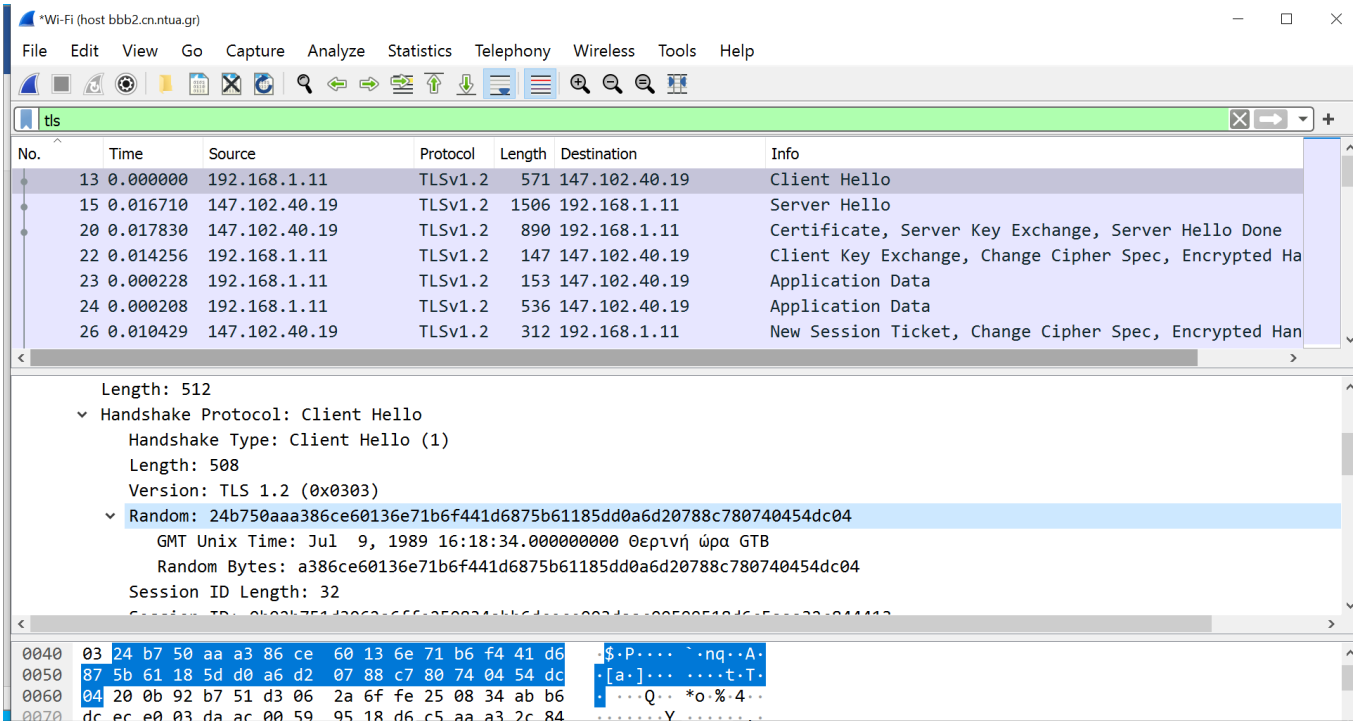
3.9 Client Hello (1), Server Hello (2), Certificate (11), Server Key Exchange (12), Client Key Exchange (16), Encrypted Handshake Message, Server Hello Done (14), New Session Ticket (4)

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

3.11 Είναι η TLS1.0

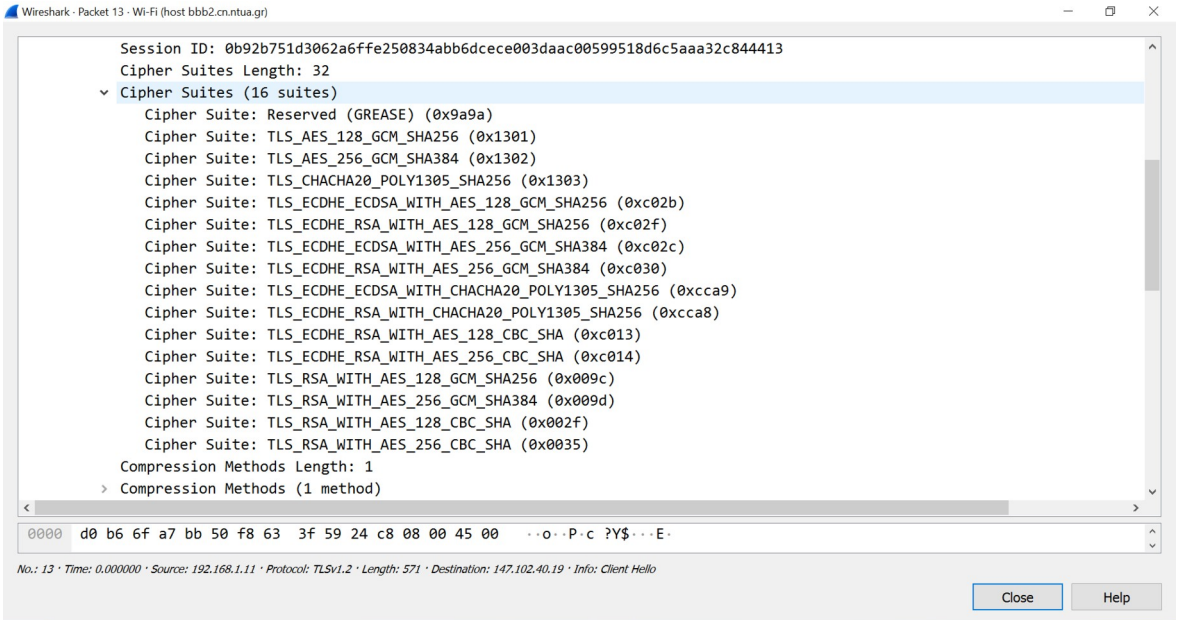


3.12 24 b7 50 aa … (συνολικά 32 bytes)

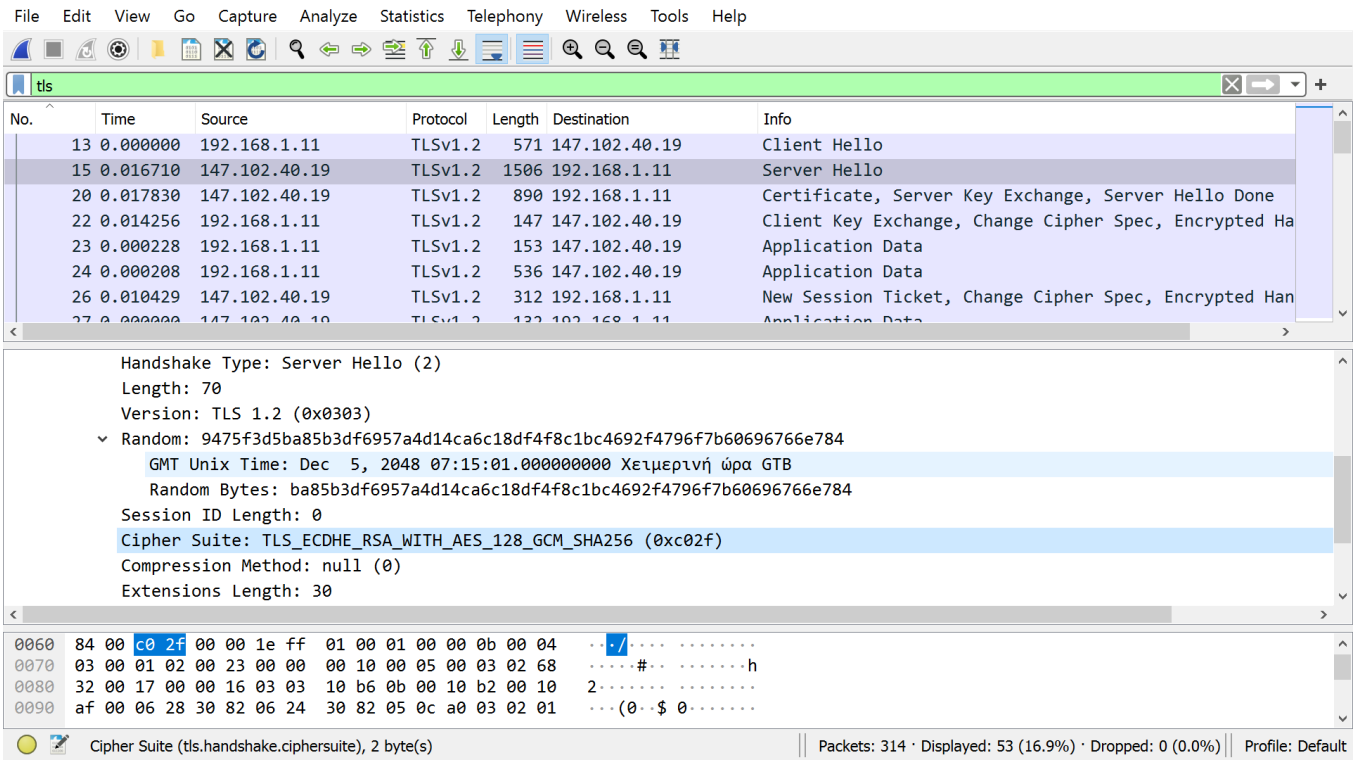


Τα 4 πρώτα bytes κανονικά αναπαριστούν τη χρονική στιγμή της αποστολής του πακέτου (εδώ όχι, η χρονική στιγμή είναι τυχαία)

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

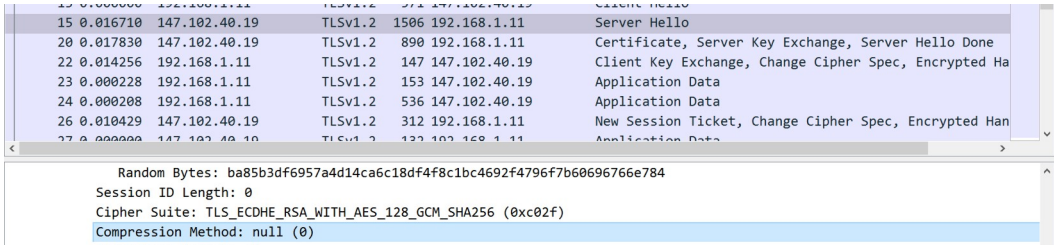


3.14 Version: TLS 1.2 (0x0303). Η σουίτα κωδίκων κρυπτογράφησης: 0xc02f



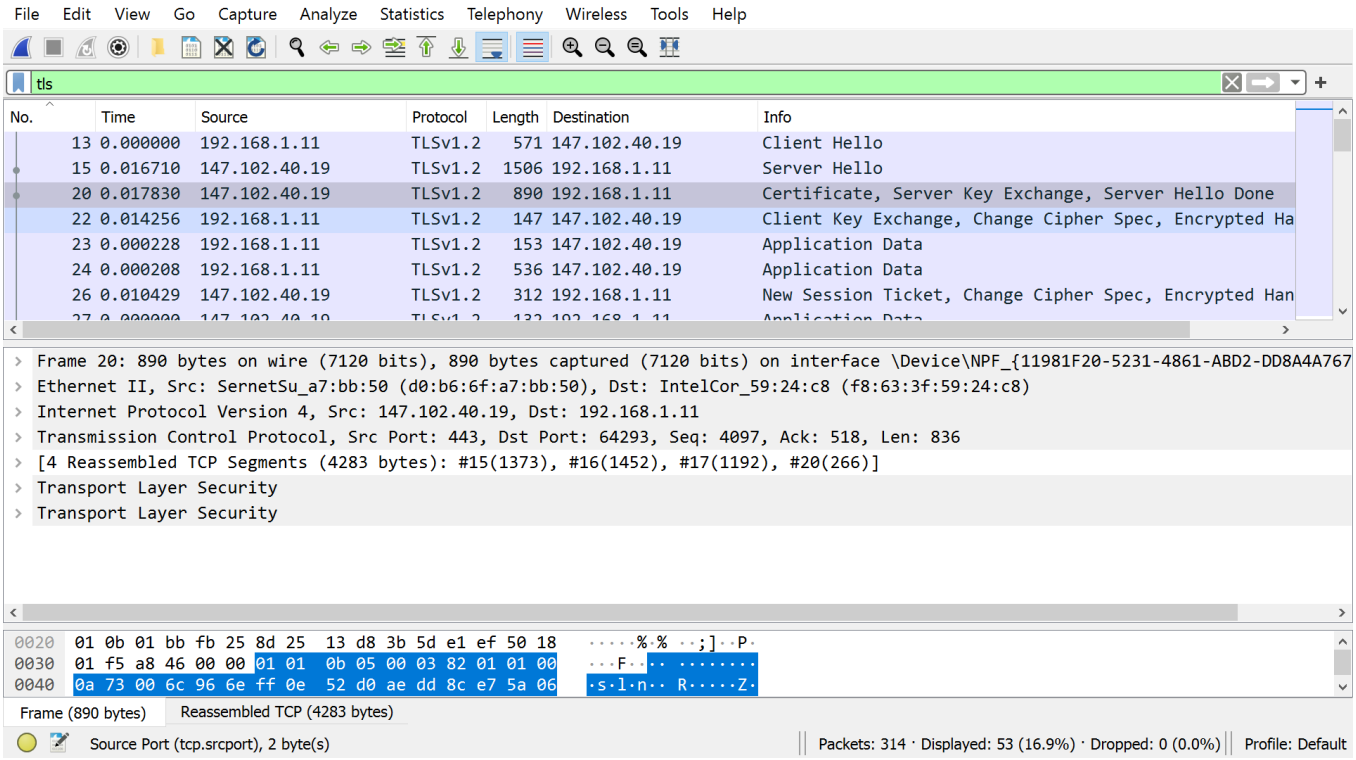
3.15 Μήκος: 32 bytes. 4 πρώτα byte του τυχαίου μέρους: ba 85 b3 df

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

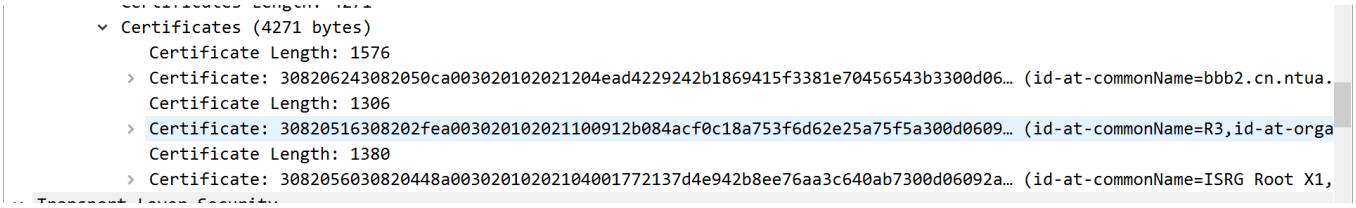


3.19 Μεταφέρονται 3 πιστοποιητικά:

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

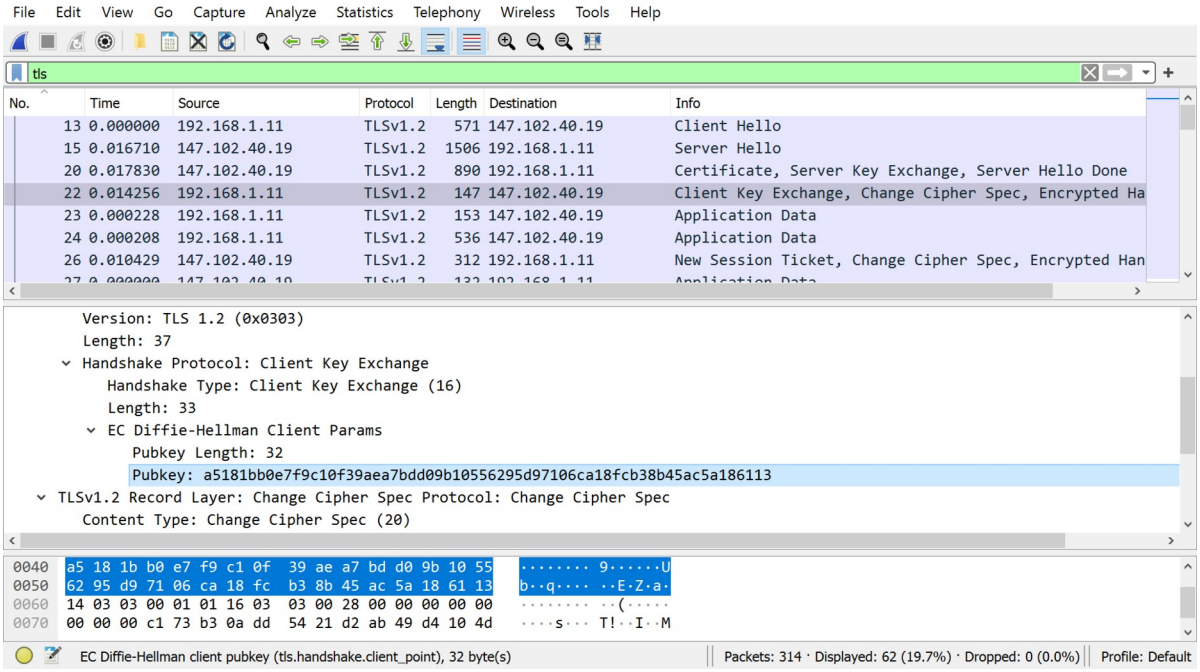
Certificate: 30820516308202fea003020102021100912b084acf0c18a753f6d62e25a75f5a300d0609… (id-at-commonName=R3,id-at-organizationName=Let's Encrypt,id-at-countryName=US)

Και Certificate: 3082056030820448a003020102021040017721 37d4e942b8ee76aa3c640ab7300d06092a… (id-at-commonName=ISRG Root X1,id-at-organizationName=Internet Security Research Group,id-at-countryName=US)



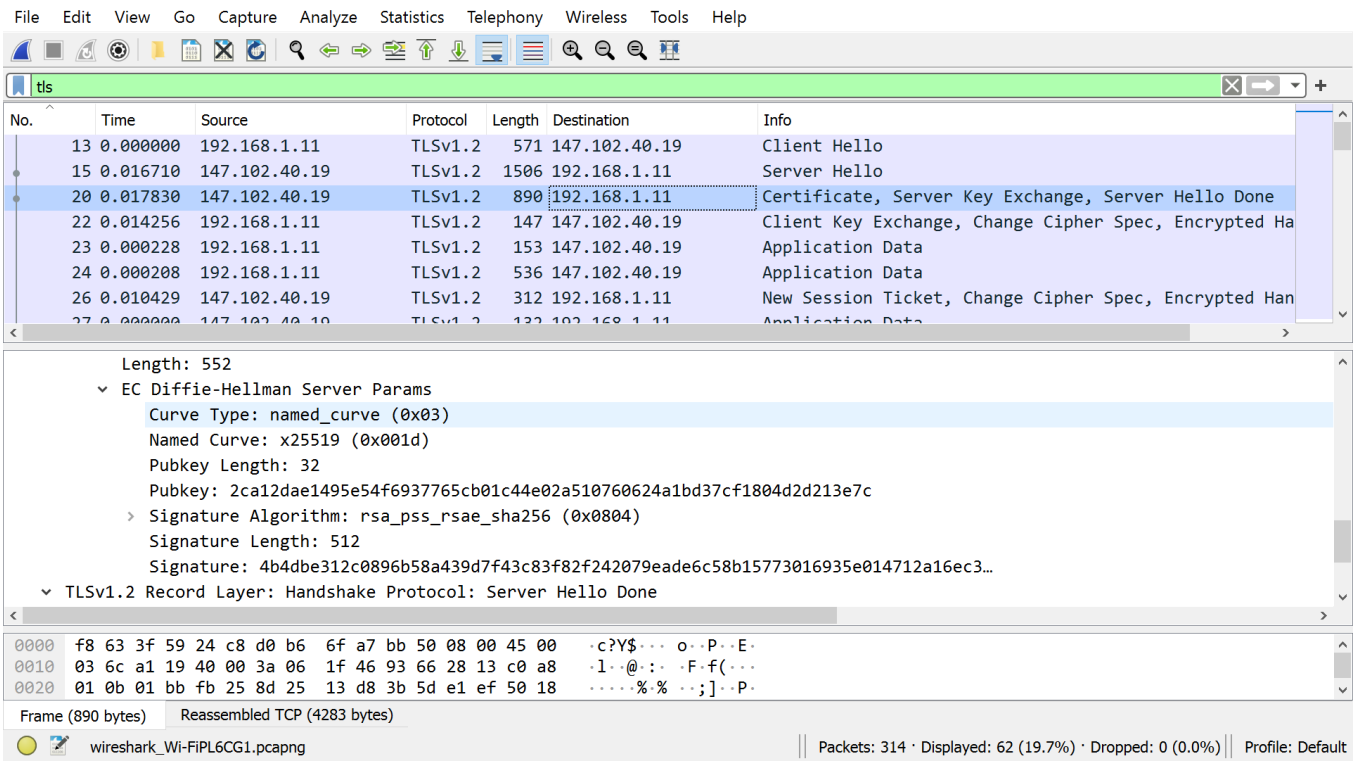
3.20 Παρατηρώ 4 πλαίσια Ethernet.

3.21 Pubkey: a5181bb0e7f9c10f39aea7bdd09b10556295d97106ca18fcb38b45ac5a186113

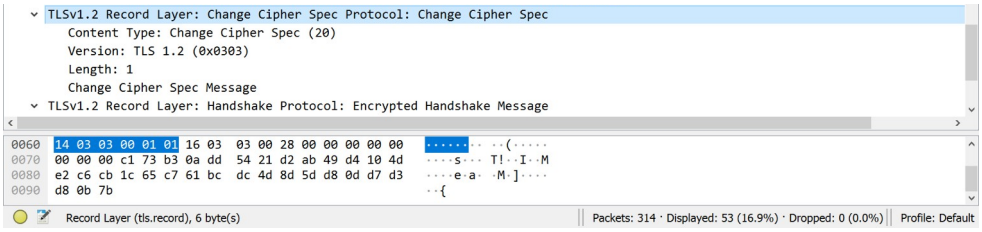


Άρα για τον πελάτη είναι: Μήκος κλειδιού: 32 bytes με 5 πρώτα γράμματα τα: a5181

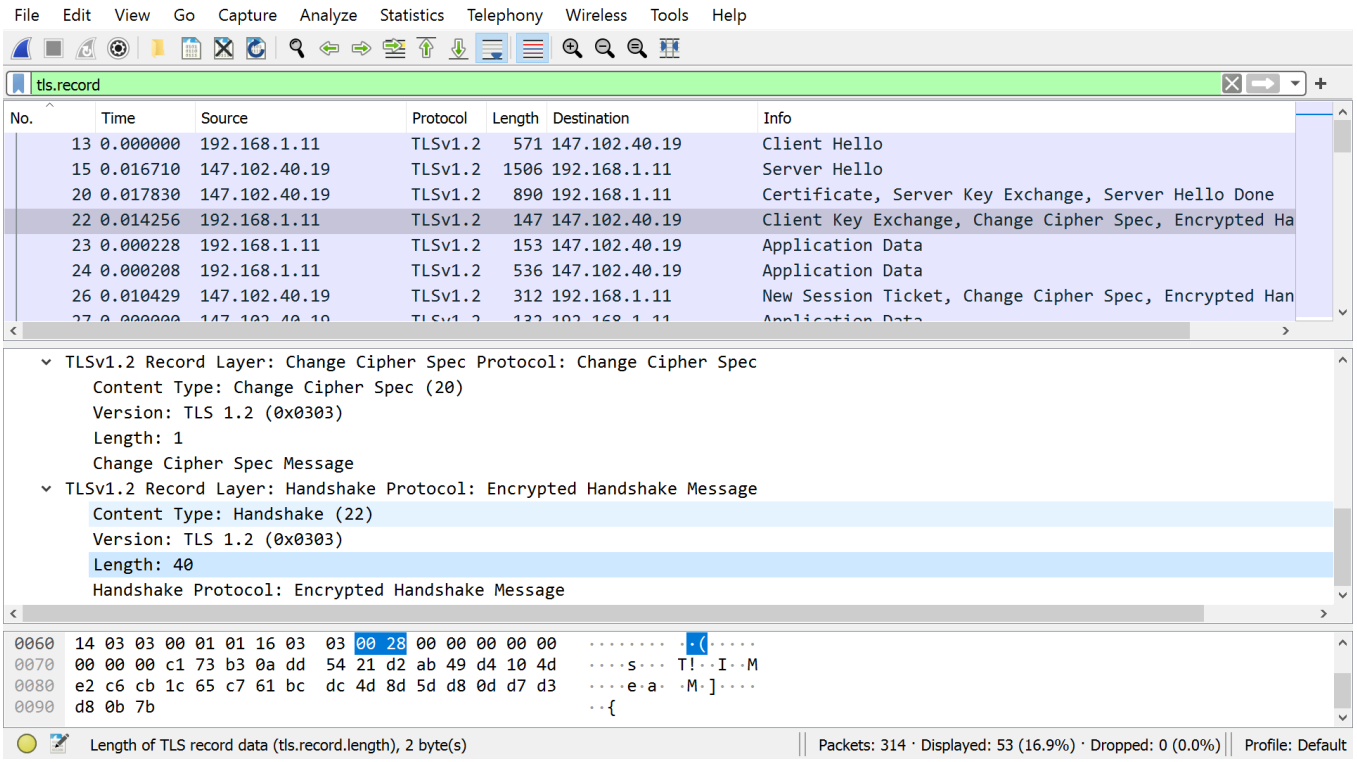
Και για τον εξυπηρετητή είναι: Μήκος κλειδιού: 32 bytes με 5 πρώτα γράμματα τα: 2ca12



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