ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

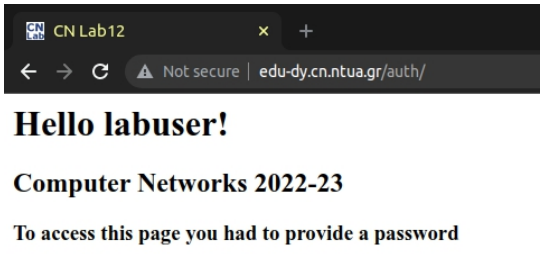
Δίκτυα Υπολογιστών

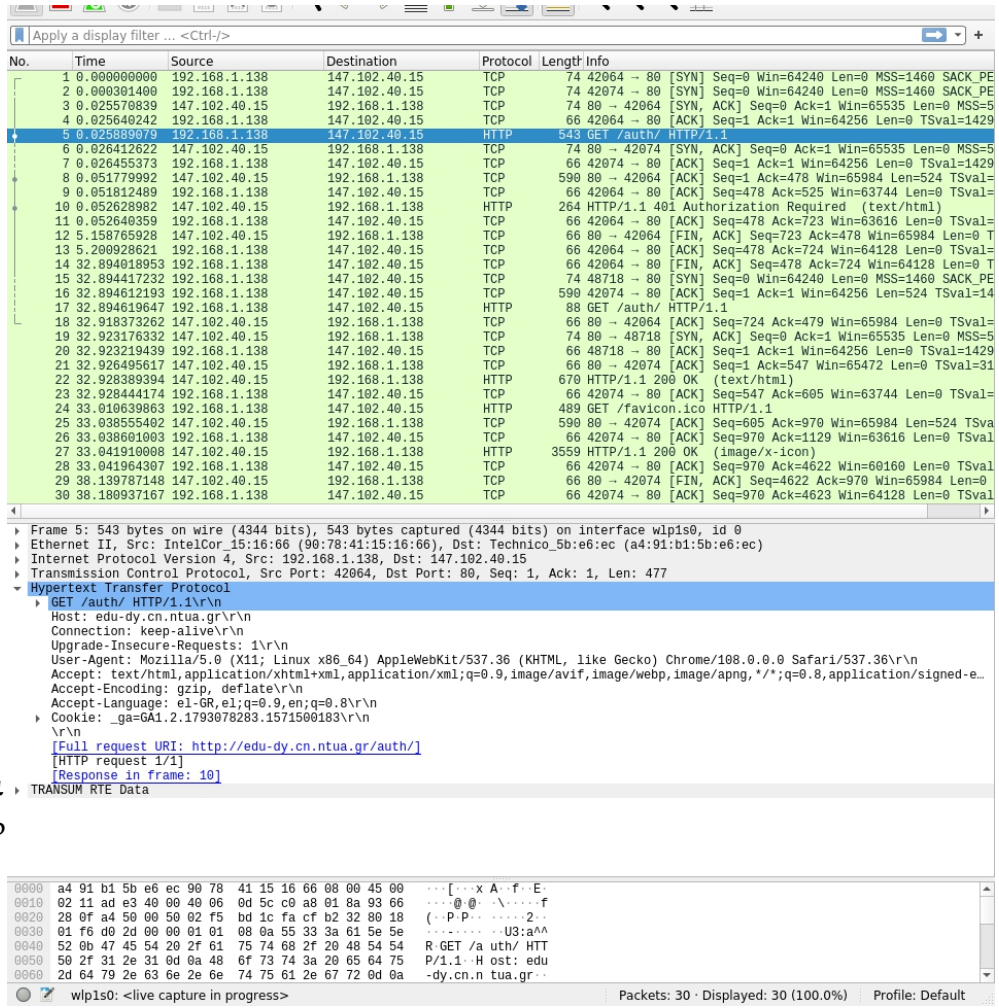
Αναφορά 12ης Εργαστηριακής Άσκησης

Ραπτόπουλος Πέτρος (el19145)
Ομάδα 3

Άσκηση 1: Πιστοποίηση αυθεντικότητας στο πρωτόκολλο HTTP

Με τη βοήθεια του Wireshark καταγράφουμε την κίνηση ενώ κάνουμε χρήση της υπηρεσίας HTTP του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15). Εφαρμόζουμε φίλτρο σύλληψης host 147.102.40.15 για να παρατηρούμε μόνο την κίνηση που σχετίζεται με αυτόν. Ξεκινάμε μία καταγραφή κίνησης και επισκεπτόμαστε τη σελίδα http://edu-dy.cn.ntua.gr/auth/. Επαληθεύουμε την ταυτότητά μας και σταματάμε την καταγραφή.





1.1) Να καταγραφεί ο αριθμητικός κωδικός κατάστασης (status code) και η φράση που επιστρέφει ο εξυπηρετητής ως απόκριση στο αρχικό αίτημα HTTP τύπου GET του πλοηγού ιστού.: **401 - Authorization Required**

1.2) Στην απόκριση ο εξυπηρετητής υποδεικνύει τη μέθοδο (scheme) πιστοποίησης αυθεντικότητας που πρέπει να χρησιμοποιήσει ο πλοηγός ώστε να επιτραπεί η πρόσβαση. Ποιο είναι το όνομα της σχετικής επικεφαλίδας HTTP **WWW-Authenticate** και ποια μέθοδο υποδεικνύει; **Basic**

1.3) Ο πλοηγός ιστού συμμορφούμενος με την υπόδειξη στέλνει δεύτερο αίτημα HTTP τύπου GET στον εξυπηρετητή όπου περιλαμβάνει τα διαπιστευτήριά του. Ποιο είναι το όνομα της σχετικής επικεφαλίδας HTTP; **Authorization**

1.4) Το περιεχόμενο της επικεφαλίδας περιλαμβάνει τη μέθοδο πιστοποίησης αυθεντικότητας που βρήκατε στην ερώτηση 1.2 καθώς και τα σχετικά διαπιστευτήρια. Καταγράψτε τα όπως αυτά εμφανίζονται στο παράθυρο με τα περιεχόμενα του επιλεγμένου πλαισίου σε μορφή ASCII.: **Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk**

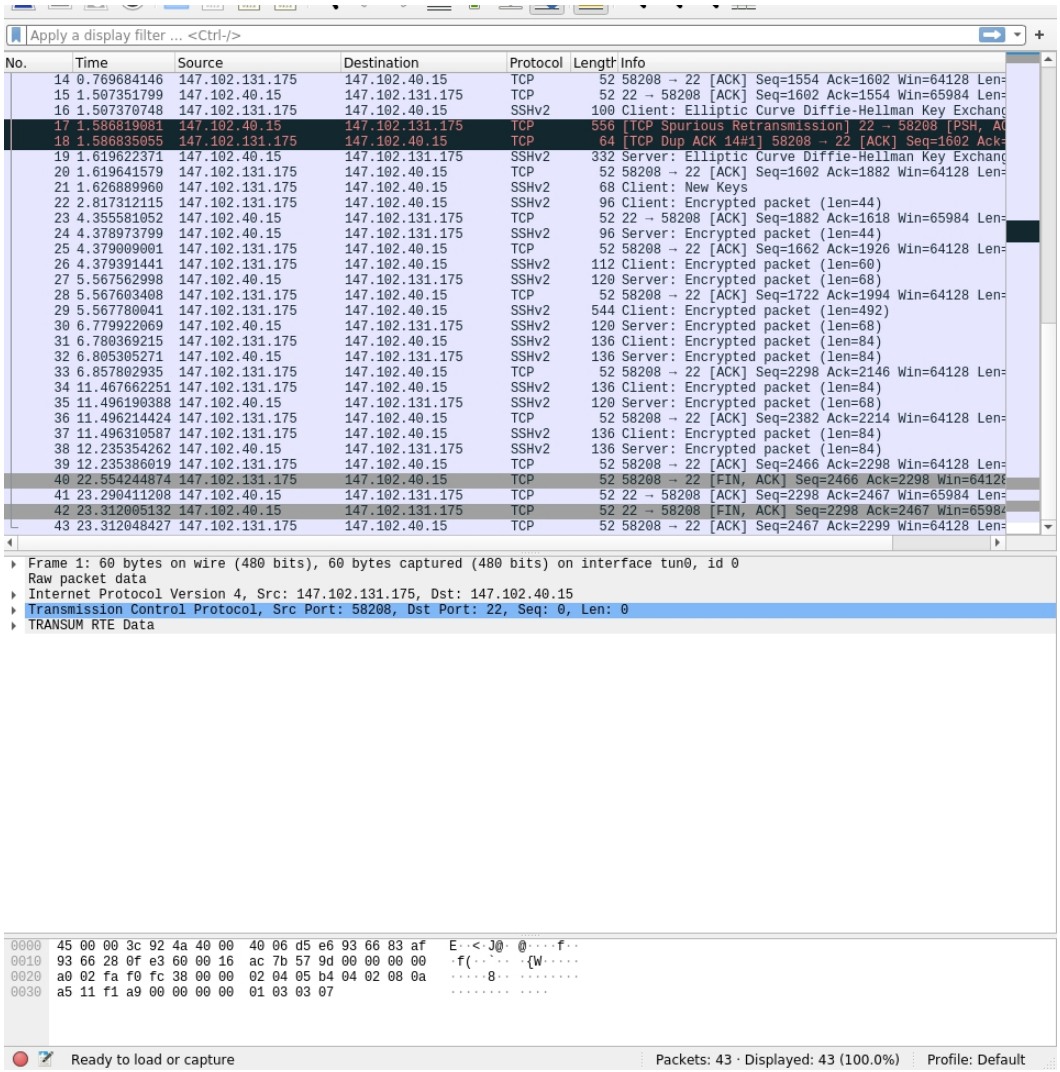
1.5) Επισκεφτείτε την ιστοσελίδα https://www.base64encode.org/, επιλέξτε το Decode στην κορυφή της σελίδας και εισάγετε στο παράθυρο που θα εμφανισθεί τα διαπιστευτήρια που καταγράψατε στο ερώτημα 1.4. Αποκωδικοποιήστε το περιεχόμενό τους κάνοντας κλικ στο κουμπί "DECODE" και καταγράψτε το αποτέλεσμα . **edu-dy:password**

1.6) Τι συμπεραίνετε για την ασφάλεια του βασικού μηχανισμού πιστοποίησης αυθεντικότητας που παρέχει το HTTP; **Δεν παρέχει εμπιστευτικότητα (confidentiality) για τα μεταδιδόμενα credentials. Είναι απλά κωδικοποιημένα με "Base64" και δεν είναι κρυπτογραφημένα.**

Άσκηση 2: Υπηρεσία SSH – Secure SHell

Καταγράφουμε με τη βοήθεια του Wireshark την κίνηση ενώ κάνουμε χρήση της υπηρεσίας SSH του υπολογιστή edu-dy.cn.ntua.gr.

```
petrosrapto@petrosraptoAssistant:~$ ssh abcd@147.102.40.15
Password for abcd@edu-dy.cn.ntua.gr:
Password for abcd@edu-dy.cn.ntua.gr:
```



2.1) Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το SSH (TCP ή UDP); **TCP**

2.2) Καταγράψτε τις θύρες του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία μεταξύ του υπολογιστή σας και του edu-dy.cn.ntua.gr. **22, 58208**

2.3) Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής SSH; **22**

2.4) Εφαρμόστε φίλτρο ώστε να παραμείνουν μόνο τα μηνύματα SSH. Ποια είναι η σύνταξη του φίλτρου που χρησιμοποιήσατε; **ssh**

2.5) Εντοπίσετε τα μηνύματα SSH τύπου Protocol. Αναλύοντας το αναγνωριστικό που στέλνει ο εξυπηρετητής στον πελάτη, ποια έκδοση του πρωτοκόλλου SSH: **2.0** και
ποια έκδοση λογισμικού χρησιμοποιεί ο εξυπηρετητής; **OpenSSH_6.6.1_hpn13v11**
Περιλαμβάνονται σχόλια στο αναγνωριστικό αυτό; Αν ναι, να καταγραφούν. **Ναι, FreeBSD-20140420**

2.6) Αναλύοντας το αναγνωριστικό που στέλνει ο πελάτης στον εξυπηρετητή, ποια έκδοση του πρωτοκόλλου SS: **2.0** και ποια έκδοση λογισμικού χρησιμοποιεί ο πελάτης; **OpenSSH_8.2p1**
Περιλαμβάνονται σχόλια στο αναγνωριστικό αυτό; Αν ναι, να καταγραφούν. **Ναι, Ubuntu-4ubuntu0.5**

2.7) Εντοπίσετε το μήνυμα SSH τύπου Key Exchange Init που έστειλε ο πελάτης και βρείτε τη λίστα με τους αλγόριθμους ανταλλαγής κλειδιών (kex). Καταγράψτε το πλήθος τους: **10**
και τους πρώτους δύο.: **`curve25519-sha256,curve25519-sha256@libssh.org`**

2.8) Από τη λίστα των αλγορίθμων παραγωγής κλειδιών (server host key) που υποστηρίζει ο πελάτης καταγράψτε το πλήθος τους: **18** και τους πρώτους δύο εξ αυτών.

ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com

2.9) Από τις λίστες αλγόριθμων κρυπτογράφησης (encryption) που υποστηρίζει ο πελάτης καταγράψτε τους δύο πρώτους για την κατεύθυνση πελάτης -> εξυπηρετητής.

chacha20-poly1305@openssh.com,aes128-ctr

2.10) Από τις λίστες αλγόριθμων πιστοποίησης αυθεντικότητας μηνυμάτων (mac) που υποστηρίζει ο πελάτης καταγράψτε τους δύο πρώτους για την κατεύθυνση πελάτης->εξυπηρετητής.

umac-64-etm@openssh.com,umac-128-etm@openssh.com

2.11) Από τις λίστες αλγόριθμων συμπίεσης (compression) που υποστηρίζει ο πελάτης καταγράψτε τους δύο πρώτους για την κατεύθυνση πελάτης->εξυπηρετητής. **none,zlib@openssh.com**

2.12) Εντοπίσετε το μήνυμα SSH τύπου Key Exchange Init που έστειλε ο εξυπηρετητής και προσδιορίστε τον αλγόριθμο ανταλλαγής κλειδιών που θα ακολουθήσουν τα δύο μέρη. Τον εμφανίζει κάπου το Wireshark;

Εμφανίζεται στο πεδίο Key Exchange. Θα ακολουθηθεί ο `curve25519-sha256@libssh.org`.

Είναι ο πρώτος της λίστας του πελάτη που υπάρχει και στη λίστα του εξυπηρετητή.

2.13) Από τις λίστες με τους αλγόριθμους κρυπτογράφησης που υποστηρίζει ο εξυπηρετητής, βρείτε αυτόν που τελικά θα χρησιμοποιηθεί στην κατεύθυνση πελάτης->εξυπηρετητής. **aes128-ctr**

2.14) Από τις λίστες με τους αλγόριθμους πιστοποίησης αυθεντικότητας μηνυμάτων που υποστηρίζει ο εξυπηρετητής, βρείτε αυτόν που τελικά θα χρησιμοποιηθεί στην κατεύθυνση πελάτης->εξυπηρετητής.

hmac-sha1-etm@openssh.com

2.15) Από τις λίστες με τους αλγόριθμων συμπίεσης που υποστηρίζει ο εξυπηρετητής, βρείτε αυτόν που τελικά θα χρησιμοποιηθεί στην κατεύθυνση πελάτης->εξυπηρετητής. **none**

2.16) Εμφανίζει σε κάποιο σημείο το Wireshark τους επιλεχθέντες αλγόριθμους κρυπτογράφησης, πιστοποίησης αυθεντικότητας μηνυμάτων και συμπίεσης; **Όχι**

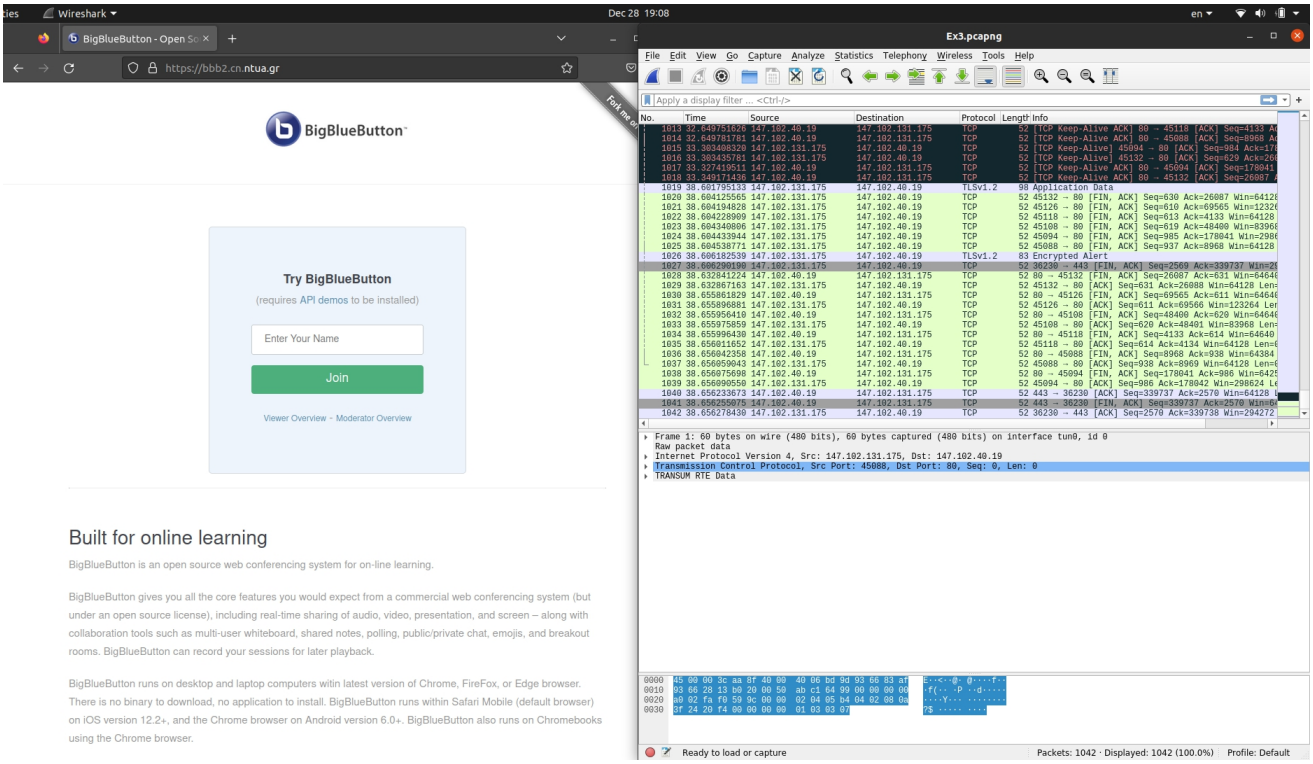
2.17) Μετά την ολοκλήρωση της διαπραγμάτευσης αλγορίθμων και ανταλλαγής κλειδιών, ακολουθεί η φάση παραγωγής του κοινού μυστικού που θα χρησιμοποιηθεί για την κρυπτογράφηση της μετάδοσης δεδομένων. Ποιους άλλους σχετικούς με τη φάση αυτή τύπους μηνυμάτων SSH καταγράψατε; **Elliptic Curve Diffie-Hellman Key Exchange Init (30), Elliptic Curve Diffie-Hellman Key Exchange Reply (31), New Keys (21)**

2.18) Μπορείτε να εντοπίσετε τα πακέτα όπου μεταφέρεται η πληροφορία για την προτροπή login και password στην περίπτωση του SSH; Να δικαιολογήσετε την απάντησή σας. **Όχι, αφού η πληροφορία είναι κρυπτογραφημένη.**

2.19) Σχολιάστε την ασφάλεια της υπηρεσίας SSH όσον αφορά την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων συγκρίνοντας με άλλα πρωτόκολλα ανταλλαγής δεδομένων. **Η κρυπτογράφηση που χρησιμοποιείται στο SSH παρέχει εμπιστευτικότητα (confidentiality) και διασφαλίζει την ακεραιότητα (integrity) των μεταδιδόμενων δεδομένων. Άλλα πρωτόκολλα ανταλλαγής δεδομένων (πχ Telnet) δεν είναι τόσο ασφαλή. Ωστόσο παρέχεται και πιστοποίηση αυθεντικότητας (authenticity) αποστέλλοντας κατάλληλα μηνύματα στην άλλη πλευρά. Αν αυτή κατέχει private key τότε μπορεί να αποκρυπτογραφήσει το μήνυμα και να απαντήσει αναλόγως.**

Άσκηση 3: Υπηρεσία HTTPS

Ξεκινάμε μια νέα καταγραφή εφαρμόζοντας φίλτρο σύλληψης ώστε να παρατηρούμε μόνο την κίνηση που σχετίζεται με τον bbb2.cn.ntua.gr. Επισκεπτόμαστε με τον πλοηγό ιστού την ιστοσελίδα http://bbb2.cn.ntua.gr/.
Μόλις φορτωθεί η σελίδα, την επισκεπτόμαστε πάλι, χρησιμοποιώντας αυτή τη φορά το πρωτόκολλο HTTPS.
Για το σκοπό αυτό, πληκτρολογούμε τη διεύθυνση https://bbb2.cn.ntua.gr/.
Όταν φορτωθεί πλήρως η σελίδα περιμένουμε λίγο, κλείνουμε τον πλοηγό ιστού και σταματάμε την καταγραφή.



3.1) Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε; **host bbb2.cn.ntua.gr**
3.2) Εφαρμόστε κατάλληλο φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα πρώτα τεμάχια TCP των τριμερών χειραψιών που διεξήχθησαν με τον εξυπηρετητή bbb2.cn.ntua.gr. Ποια είναι η σύνταξή του;
ip.addr==147.102.40.19 and (tcp.flags.syn == 1 or (tcp.ack == 1 and tcp.seq == 1 and tcp.len == 0))
3.3) Σε ποιες (πασίγνωστες) θύρες του εξυπηρετητή bbb2.cn.ntua.gr γίνονται οι συνδέσεις; **80, 443**
3.4) Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής HTTP: **80** και ποια στο HTTPS;: **443**
3.5) Βρείτε πόσες συνδέσεις ανοίχθηκαν μεταξύ του υπολογιστή σας και του εξυπηρετητή ιστού bbb2.cn.ntua.gr στην περίπτωση HTTP: **6** και πόσες στην περίπτωση HTTPS.: **1**
3.6) Για τις συνδέσεις TCP της περίπτωσης HTTPS καταγράψτε τις θύρες πηγής.: **Source Port: 36230**

Εφαρμόζουμε φίλτρο απεικόνισης tls.record ώστε να παραμείνουν πλαίσια τα οποία περιλαμβάνουν εγγραφές TLS.
3.7) Αναπτύσσοντας τις επικεφαλίδες Στρώματος Εγγραφών TLS κάθε πλαισίου θα παρατηρήσετε ότι τα τρία πρώτα πεδία είναι κοινά. Ποια είναι αυτά και ποιο το μήκος τους; **Content Type(1 byte), Version(2 bytes), Length(2 bytes)**
3.8) Ένα από τα πεδία είναι ο τύπος περιεχομένου (content type). Να καταγραφούν τα ονόματα των διαφορετικών τύπων εγγραφών TLS που εμφανίζονται στην καταγραφή και οι αριθμητικές τους τιμές.
Handshake(22), Change Cipher Spec(20), Application Data(23), Alert(21)
3.9) Το πεδίο version δείχνει την έκδοση του πρωτοκόλλου. Ποια είναι η έκδοση πρωτοκόλλου Στρώματος Εγγραφών TLS που δηλώνεται: **TLS 1.0** και ποια η αριθμητική της τιμή;: **0x0301**
3.10) Για το πρωτόκολλο χειραψίας (handshake protocol) καταγράψτε τους διαφορετικούς τύπους μηνυμάτων χειραψίας που παρατηρήσατε και τις αριθμητικές τους τιμές.: **Client Hello (1), Server Hello (2), Certificate (11), Server Key Exchange (12), Client Key Exchange (16), Encrypted Handshake Message, New Session Ticket (4)**

3.11) Πόσα μηνύματα Client Hello έστειλε ο πελάτης και ποια η σχέση τους με τις συνδέσεις TCP που καταγράψατε προηγουμένως; **1 μήνυμα. Υπενθυμίζεται ότι καταγράψαμε 1 σύνδεση TCP.**
3.12) Εντοπίστε το πρώτο μήνυμα Client Hello που στέλνει ο πελάτης κατά τη χειραψία του πρωτοκόλλου TLS. Ποια έκδοση του πρωτοκόλλου TLS δηλώνεται: **TLS 1.0** και ποια η αριθμητική της τιμή;: **0x0301**
Είναι ταυτόσημη με αυτήν της ερώτησης 3.9; **Ναι**
3.13) Εάν ο πλοηγός σας είναι συμβατός με την έκδοση TLS 1.3 του πρωτοκόλλου, τότε στην επικεφαλίδα επέκτασης supported_versions δηλώνει όλες τις υποστηριζόμενες εκδόσεις TLS.
Εάν ναι, πόσες: **2** και ποιες δηλώνονται; **TLS 1.2, TLS 1.3** Ποια είναι η αριθμητική τιμή για την έκδοση TLS1.3; **0x0304**
3.14) Εάν ο πλοηγός σας είναι συμβατός με HTTP/2, τότε δηλώνει τις υποστηριζόμενες εκδόσεις στην επικεφαλίδα επέκτασης application_layer_protocol_negotiation. Εάν ναι, ποια πρωτόκολλα δηλώνονται; **h2, http/1.1**
3.15) Ποιο είναι το μήκος σε byte του τυχαίου αριθμού που περιέχει το μήνυμα Client Hello;: **32 bytes**
Καταγράψτε τα πρώτα 4 byte. **3e e7 cf 44** Τι παριστάνουν; **?**
3.16) Στην επικεφαλίδα για τις σουίτες κωδίκων (cipher suites) δηλώνονται αυτές που υποστηρίζει ο πελάτης. Να καταγραφεί το πλήθος τους: **17** και οι δεκαεξαδικές τιμές των δύο πρώτων από αυτές.: **0x1301, 0x1303**
3.17) Εντοπίστε το μήνυμα Server Hello με το οποίο απαντά ο εξυπηρετητής στη χειραψία που ξεκίνησε με το προηγούμενο Client Hello. Εξετάζοντας την επικεφαλίδα του μηνύματος, καταγράψτε την έκδοση TLS που θα χρησιμοποιηθεί. **TLS 1.2**
3.18) Ποιο είναι το μήκος σε byte του τυχαίου αριθμού που περιέχει;: **32 bytes** Καταγράψτε τα πρώτα 4 byte.: **9c 94 c7 01**
Συγκρίνοντας με την ερώτηση 3.14, τι συμπεραίνατε για το πώς παράγονται; **?**
3.19) Χρησιμοποιείται κάποια μέθοδος συμπίεσης από τον εξυπηρετητή και τον πελάτη; **Όχι**
3.20) Ποιο είναι το όνομα: **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** και η δεκαεξαδική τιμή **(0xc02f)** της σουίτας κωδίκων που τελικά επιλέχθηκε; Ποιοι είναι οι αλγόριθμοι ανταλλαγής κλειδιών: **ECDHE**, πιστοποίησης ταυτότητας: **RSA**, κρυπτογράφησης: **AES_128_GCM** και η συνάρτηση κατακερματισμού: **SHA256** ;
3.21) Εντοπίστε το μήνυμα Certificate που μεταφέρει τα πιστοποιητικά του εξυπηρετητή. Ποιο είναι το μήκος του σύμφωνα με το πεδίο length της επικεφαλίδας στρώματος εγγραφών TLS;: **4276 bytes**
3.22) Πόσα πιστοποιητικά μεταφέρονται: **3** και τι μήκος έχει το καθένα από αυτά;: **1574, 1306, 1380 bytes**
3.23) Πόσα πλαίσια Ethernet χρειάστηκαν ώστε να μεταφερθεί η παραπάνω εγγραφή TLS; **5**
3.24) Εντοπίστε τα μηνύματα για την ανταλλαγή κλειδιών Diffie–Hellman (ClientKeyExchange, ServerKeyExchange). Ποιο είναι το μήκος του δημόσιου κλειδιού που αποστέλλει ο πελάτης: **32 bytes** και ποιο του εξυπηρετητή;: **32 bytes**
Καταγράψτε τα 5 πρώτα γράμματα αμφότερων των κλειδιών. **9cf0a, 99a32**
3.25) Ποιο είναι το μήκος της εγγραφής TLS τύπου ChangeCipherSpec που μεταφέρει στον εξυπηρετητή την υπόδειξη ότι η επικοινωνία από εδώ και πέρα θα είναι κρυπτογραφημένη: **6 B** και ποιο το μήκος του αντίστοιχου μηνύματος; **1 B**
3.26) Ποιο είναι το μήκος σε byte του μηνύματος EncryptedHandshakeMessage που περιέχει από την πλευρά του πελάτη το αποτέλεσμα της συνάρτησης κατακερματισμού επί των προηγούμενων μηνυμάτων της χειραψίας;: **40 bytes**
3.27) Παρατηρήσατε εγγραφή TLS με την υπόδειξη (ChangeCipherSpec) και μήνυμα με το αποτέλεσμα της συνάρτησης κατακερματισμού (EncryptedHandshakeMessage) από την πλευρά του εξυπηρετητή; **Ναι**
3.28) Εντοπίστε μια εγγραφή TLS για πρωτόκολλο εφαρμογής. Ποιου πρωτοκόλλου δεδομένα μεταφέρονται σύμφωνα με τις ενδείξεις του Wireshark; **http2**
3.29) Παρατηρήσατε εγγραφές TLS πρωτοκόλλου Alert (Encrypted Alert);: **Ναι** Από ποια πλευρά στάλθηκαν; **Πελάτη**
3.30) Εάν ναι, γιατί νομίζετε ότι υπάρχουν; **Ακολουθεί απόλυση της σύνδεσης TCP.**
3.31) Επιλέξτε από την ιστοσελίδα μια φράση με λατινικούς χαρακτήρες (π.χ. “BigBlueButton”). Προσπαθήστε να βρείτε το πακέτο που μεταφέρει την πληροφορία. Τι παρατηρείτε στην περίπτωση του HTTP σε σύγκριση με αυτή του HTTPS; **Μπορούμε να εντοπίσουμε την φράση στην περίπτωση πρωτοκόλλου HTTP, αλλά όχι του HTTPS.**
3.32) Σχολιάστε την ασφάλεια του πρωτοκόλλου HTTPS σε σύγκριση με το απλό HTTP, όσον αφορά την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. **Το πρωτόκολλο HTTPS παρέχει αυθεντικότητα, εμπιστευτικότητα και ακεραιότητα δεδομένων σε σύγκριση με το HTTP που δεν τα παρέχει.**