Δίκτυα Επικοινωνιών – Εργασία Wireshark

Παντελίδης Ιπποκράτης – p3210150

Άσκηση 1)

1. Η χρονική διάρκεια της ανίχνευσης φαίνεται αν από το μενού επιλογών ακολουθήσουμε την διαδρομή Statistics > Capture File Properties. Ο πίνακας που ακολουθεί μας δείχνει ότι η ανίχνευση διήρκησε 1 λεπτό και 41 δευτερόλεπτα.

Time

First packet:	2024-01-14 20:51:43
Last packet:	2024-01-14 20:53:25
Elapsed:	00:01:41

2. Για να βρούμε τα διαφορετικά πρωτόκολλα που ανιχνεύθηκαν πηγαίνουμε από το μενού επιλογών στο Statistics > Protocol Hierarchy και προκύπτει ο παρακάτω πίνακας που τα εμφανίζει διαχωρισμένα σύμφωνα με το επίπεδο.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	2950	100.0	2257771	153 k	0	0	0	2950
Ethernet	100.0	2950	1.8	41300	2815	0	0	0	2950
Address Resolution Protocol	0.5	14	0.0	392	26	14	392	26	14
Internet Protocol Version 4	99.3	2930	2.6	58600	3994	0	0	0	2930
Internet Control Message Protocol	3.1	91	0.3	6078	414	85	5592	381	91
NetBIOS Name Service	0.2	6	0.0	270	18	6	270	18	6
Transmission Control Protocol	83.7	2469	88.3	1993801	135 k	1950	1559885	106 k	2469
Data	0.0	1	0.0	1	0	1	1	0	1
Hypertext Transfer Protocol	1.3	37	47.6	1074634	73 k	18	4401	300	37
Data	0.0	1	42.0	947704	64 k	1	947704	64 k	1
Line-based text data	0.1	2	0.0	44	2	2	44	2	2
Media Type	0.5	16	5.1	116060	7911	16	116060	7911	16
Transport Layer Security	16.3	481	38.3	864557	58 k	481	593055	40 k	511
User Datagram Protocol	12.5	370	0.1	2960	201	0	0	0	370
Data	0.1	2	0.1	1312	89	2	1312	89	2
Domain Name System	4.4	130	0.7	16053	1094	130	16053	1094	130
Link-local Multicast Name Resolution	0.1	2	0.0	90	6	2	90	6	2
NetBIOS Name Service	1.0	30	0.1	1500	102	30	1500	102	30
QUIC IETF	6.8	202	5.9	133574	9105	202	130813	8917	209
Simple Service Discovery Protocol	0.1	4	0.0	704	47	4	704	47	4
Internet Protocol Version 6	0.2	6	0.0	240	16	0	0	0	6
User Datagram Protocol	0.2	6	0.0	48	3	0	0	0	6
Data	0.1	2	0.1	1312	89	2	1312	89	2
DHCPv6	0.1	2	0.0	190	12	2	190	12	2
Link-local Multicast Name Resolution	0.1	2	0.0	90	6	2	90	6	2

Αναλυτικότερα :

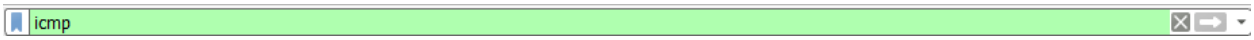
a) Application Layer : DNS, SSDP, NBNS
b) Transport Layer : TCP, UDP
c) Network Layer : ICMP

d) Link Layer : ARP

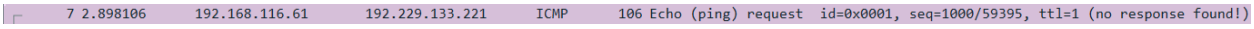
3. Τα πρωτόκολλα επιπέδου εφαρμογής που έχουν εντοπιστεί είναι το DNS, το NBNS και το SSDP και όπως φαίνεται παρακάτω χρησιμοποιούν το UDP ως το πρωτόκολλο επιπέδου μεταφοράς.

```
Protocol: UDP (17)
```

4. Για να εμφανίζονται στο παράθυρο του Wireshark μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP χρησιμοποιούμε το φίλτρο icmp όπως φαίνεται και από την παρακάτω εικόνα.



5. Το IP πακέτο που μεταφέρει το πρώτο ICMP Echo Request είναι το :



και αφού το επιλέξουμε βρίσκουμε τα εξής :

a) Οι συσκευές που επικοινωνούν σε επίπεδο Ethernet είναι αυτή που ξεκίνησε την επικοινωνία και η συσκευή προορισμού και φαίνονται στην παρακάτω φωτογραφία μαζί με τις MAC διευθύνσεις τους. Για να τις βρούμε επεκτείνουμε την καρτέλα Ethernet II.

```
Ethernet II, Src: Intel_a8:6b:00 (f0:77:c3:a8:6b:00), Dst: ca:3f:21:b6:e4:c8 (ca:3f:21:b6:e4:c8)
  > Destination: ca:3f:21:b6:e4:c8 (ca:3f:21:b6:e4:c8)
  > Source: Intel_a8:6b:00 (f0:77:c3:a8:6b:00)
    Type: IPv4 (0x0800)
```

b) Για να βρούμε την IP address του υπολογιστή μας επεκτείνουμε την καρτέλα Internet Protocol Version 4 και κοιτάμε την Source Address η οποία φαίνεται παρακάτω :

```
Source Address: 192.168.116.61
```

c) Όμοια για να βρούμε την IP address του destination επεκτείνουμε πάλι την ίδια καρτέλα και κοιτάμε την Destination Address η οποία είναι η :

```
Destination Address: 192.229.133.221
```

d) Το time-to-live του πακέτου το βρίσκουμε επίσης επεκτείνοντας την ίδια καρτέλα, στο πεδίο Time to Live και είναι :

```
Time to Live: 1
  > [Expert Info (Note/Sequence): "Time To Live" only 1]
```

e) Το μέγεθος των δεδομένων που μεταφέρει το πακέτο το βρίσκουμε από την καρτέλα Internet Control Message Protocol στο πεδίο Data και έχει length 64 bytes :

```
> Data (64 bytes)
```

6. Το IP πακέτο που μεταφέρει το πρώτο ICMP Time Exceeded είναι το :

```
   8 2.976861    192.168.116.81    192.168.116.61    ICMP    134 Time-to-live exceeded (Time to live exceeded in transit)
```

και αφού το επιλέξουμε βρίσκουμε τα εξής :

a) Για να βρούμε την IP του destination επεκτείνουμε ξανά την καρτέλα Internet Protocol Version 4 και κοιτάμε το πεδίο Destination Address το οποίο έχει την :

```
Destination Address: 192.168.116.61
```

Μπορούμε να παρατηρήσουμε ότι είναι η IP address του υπολογιστή μας το οποίο είναι φυσιολογικό λόγω του πρωτοκόλλου ICMP.

b) Για την IP του source επεκτείνουμε πάλι την ίδια καρτέλα και κοιτάμε το πεδίο Source Address το οποίο τώρα έχει την :

```
Source Address: 192.168.116.81
```

7. Για να βρούμε όλες τις source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα αρχικά φιλτράρουμε τα πακέτα με τον τρόπο που φαίνεται στην παρακάτω φωτογραφία ώστε να κρατήσουμε μόνο τα ζητούμενα και έπειτα κοιτάμε την στήλη με όνομα Source.

```
icmp && icmp.type == 11
```

No.	Time	Source	Destination	Protocol	Length	Info
8	2.976861	192.168.116.81	192.168.116.61	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
10	2.987027	192.168.116.81	192.168.116.61	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12	2.995914	192.168.116.81	192.168.116.61	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
43	9.321235	172.23.241.168	192.168.116.61	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
45	9.525412	172.23.241.168	192.168.116.61	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
47	9.737691	172.23.241.168	192.168.116.61	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
59	15.772894	172.23.240.25	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
61	15.805352	172.23.240.25	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
64	15.974563	172.23.240.25	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
102	33.689784	62.169.192.109	192.168.116.61	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
104	33.714575	62.169.192.109	192.168.116.61	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
107	33.832656	62.169.192.109	192.168.116.61	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
124	39.936448	62.169.243.21	192.168.116.61	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
126	40.140771	62.169.243.21	192.168.116.61	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
128	40.173791	62.169.243.21	192.168.116.61	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
141	46.285309	62.169.243.238	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
143	46.311351	62.169.243.238	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
145	46.414399	62.169.243.238	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
173	64.514030	62.169.252.246	192.168.116.61	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
175	64.718593	62.169.252.246	192.168.116.61	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
177	64.819059	62.169.252.246	192.168.116.61	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
200	78.952541	195.22.211.192	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
203	79.874604	195.22.211.33	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
205	79.973814	195.22.211.33	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
207	80.076774	195.22.211.33	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	86.325212	195.22.214.131	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
222	86.635624	195.22.214.131	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
224	86.733490	195.22.214.131	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
241	93.390902	152.195.100.131	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
243	93.491222	152.195.100.131	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
245	93.593374	152.195.100.131	192.168.116.61	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Παρατηρούμε ότι αυτές οι source IP addresses ταυτίζονται πλήρως με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt παράθυρο, όπως μπορούμε να δούμε παρακάτω.

```
C:\Users\ippok>tracert www.w3schools.com

Tracing route to cs837.wac.edgecastcdn.net [192.229.133.221]
over a maximum of 30 hops:

  1    78 ms     6 ms     6 ms  192.168.116.81
  2   280 ms   202 ms   210 ms  172.23.241.168
  3   285 ms    31 ms   165 ms  172.23.240.25
  4     *        *        *     Request timed out.
  5    90 ms    22 ms   115 ms  62.169.192.109
  6   254 ms   202 ms    31 ms  62.169.243.21
  7   136 ms    23 ms    98 ms  62.169.243.238
  8     *        *        *     Request timed out.
  9   415 ms   202 ms    97 ms  62.169.252.246
 10     *        *      356 ms  ae11.francoforte73.fra.seabone.net [195.22.211.192]
 11   260 ms    97 ms   102 ms  195.22.211.33
 12   396 ms   308 ms    96 ms  195.22.214.131
 13   776 ms    98 ms   100 ms  ae-65.core1.frb.edgecastcdn.net [152.195.100.131]
 14   212 ms   112 ms    86 ms  192.229.133.221

Trace complete.
```

Άσκηση 2)

1. Για να βρούμε πόσα πακέτα TCP και πόσα UDP στάλθηκαν θα βάλουμε ως φίλτρο tcp και udp αντίστοιχα και δούμε πόσα πακέτα γίνονται display. Για το TCP έχουμε : Packets: 4135 · Displayed: 1545 (37.4%) ενώ για το UDP : Packets: 4135 · Displayed: 2590 (62.6%)

2. Τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet είναι 5 και είναι τα ακόλουθα :

Ethernet · 5 | TCP | UDP · 120

Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:fb	6	492 bytes	6	100.00%	0	0 bytes	6	492 bytes
01:00:5e:7f:ff:fa	4	868 bytes	4	100.00%	0	0 bytes	4	868 bytes
33:33:00:00:00:fb	6	612 bytes	6	100.00%	0	0 bytes	6	612 bytes
aa:81:7e:69:4c:64	2,574	2 MB	4,119	62.49%	1,512	1 MB	1,062	508 kB
f0:77:c3:a8:6b:00	2,590	2 MB	4,135	62.64%	1,078	510 kB	1,512	1 MB

Οι πρώτες 3 είναι multicast MAC Addresses και η τελευταία αντιστοιχεί στον υπολογιστή μας.

3. Τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP είναι 39 : IPv4 · 37 IPv6 · 2 και δεν ταυτίζονται με αυτά σε επίπεδο Ethernet καθώς σε αυτή την περίπτωση τα endpoints αναφέρονται σε διευθύνσεις IP ενώ στην άλλη σε MAC addresses.

4. Για την πρώτη ερώτηση (ccslab.aueb.gr) οι θύρες προέλευσης και προορισμού για την ερώτηση προς τον DNS Server είναι οι :

```
User Datagram Protocol, Src Port: 49969, Dst Port: 53
    Source Port: 49969
    Destination Port: 53
```

ενώ για την απάντηση του οι :

```
User Datagram Protocol, Src Port: 53, Dst Port: 49969
    Source Port: 53
    Destination Port: 49969
```

Αντίστοιχα για το δεύτερο ερώτημα (eclass.aueb.gr) οι θύρες προέλευσης και προορισμού για την ερώτηση προς τον DNS Server είναι οι :

```
User Datagram Protocol, Src Port: 61354, Dst Port: 53
    Source Port: 61354
    Destination Port: 53
```

ενώ για την απάντηση του οι :

```
User Datagram Protocol, Src Port: 53, Dst Port: 61354
    Source Port: 53
    Destination Port: 61354
```

5. Ένα πακέτο περιέχει αίτημα προς τον DNS Server αν υπάρχει η λέξη query δίπλα στο Domain Name System `Domain Name System (query)` ,ενώ όταν περιέχει απάντηση από τον Server υπάρχει η λέξη response `Domain Name System (response)` . Το πακέτο μιας απάντησης συνδέεται με το πακέτο της ερώτησης με το Transaction ID το οποίο είναι 16-bit πεδίο που συσχετίζει το αίτημα με την αντίστοιχη απάντηση.

6. Υπάρχει κάποια σημαία που μας λέει αν ο name server που μας απαντάει είναι authorivative για το συγκεκριμένο domain και αυτό το βρίσκουμε αφού επεκτείνουμε την καρτέλα Domain Name System του πακέτου και στην συνέχεια την Flags. Εκεί θα βρούμε το flag authorivative που και στις δύο απαντήσεις μας έχει την τιμή 0 άρα ο name server που έχει απαντήσει δεν είναι authorivative για το συγκεκριμένο domain.

```
.... .0.. .... .... = Authoritative: Server is not an authority for domain
```

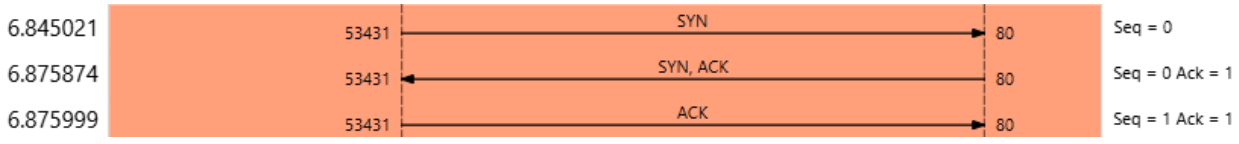
7. Το όνομα ccslab.aueb.gr φαίνεται να είναι κανονικό dns και όχι alias καθώς δεν φαίνεται να υπάρχει πουθενά η εντολή CNAME παρά μόνο η A. Η IP που του αντιστοιχεί φαίνεται παρακάτω :

```
Answers
  ccslab.aueb.gr: type A, class IN, addr 83.212.207.19
      Name: ccslab.aueb.gr
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 4438 (1 hour, 13 minutes, 58 seconds)
      Data length: 4
      Address: 83.212.207.19
```

8. Τα πρώτα 3 TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή μας και του ccslab.aueb.gr υλοποιούν την εγκαθίδρυση της σύνδεσης με την χειραψία 3 βημάτων και είναι τα ακόλουθα :

```
1480 6.845021   172.20.10.4     83.212.207.19   TCP   66 53431 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1486 6.875874   83.212.207.19   172.20.10.4     TCP   66 80 → 53431 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1396 SACK_PERM WS=1024
1487 6.875999   172.20.10.4     83.212.207.19   TCP   54 53431 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
```

Μπορούμε επίσης ακολουθώντας από το μενού επιλογών την διαδρομή Statistics > Flow Graph και αφού έχουμε κάνει το απαραίτητο filtering να τα δούμε και σε σχήμα όπως φαίνεται παρακάτω :



Οι δύο παραπάνω φωτογραφίες μας δίνουν πληροφορίες για την διαδικασία χειραψίας τριών βημάτων η οποία είναι η εξής :

i) Το πρώτο πακέτο στέλνεται από τον πελάτη που έχει IP address 172.20.10.4 στον εξυπηρετητή με IP 83.202.207.19 και είναι ένα SYN πακέτο, το οποίο εγκαθιδρύει την σύνδεση στην θύρα 80 και περιέχει πληροφορίες για τον αρχικό αριθμό σειράς, για το μέγεθος του παραθύρου και άλλες.

ii) Το δεύτερο πακέτο στέλνεται από τον server πίσω στον πελάτη και είναι ένα SYN, ACK πακέτο, το οποίο αποτελεί την απόκριση του server στο αίτημα του client δηλώνοντας ότι είναι έτοιμος για την εγκαθίδρυση (ACK = 1).

iii) Το τρίτο πακέτο είναι ένα ACK πακέτο αυτή την φορά από τον client στον server το οποίο επιβεβαιώνει ότι ο πελάτης έλαβε την απάντηση του server και η τριπλή χειραψία ολοκληρώνεται με την εγκαθίδρυση της σύνδεσης.

9. Όταν η επικοινωνία ξεκινάει από το client και πάει προς τον server έχουμε Source Port : 53431 και Destination Port : 80, ενώ αντίστροφα Source Port : 80 και Destination Port : 53431. Για καθένα από τα πακέτα της τριπλής χειραψίας οι θύρες φαίνονται παρακάτω :

Packet 1	Packet 2	Packet 3
Source Port: 53431 Destination Port: 80	Source Port: 80 Destination Port: 53431	Source Port: 53431 Destination Port: 80

10. Μπορούμε να δούμε τα πακέτα που περιέχουν HTTP GET αιτήματα από τον Browser μας προς τον Web Server φιλτράροντας με τον τρόπο που φαίνεται στην παρακάτω φωτογραφία. Παρατηρούμε, επίσης ότι υπάρχουν δύο πακέτα με IP διεύθυνση προορισμού την 83.212.207.19

http.request.method == "GET"

No.	Time	Source	Destination	Protocol	Length	Info
1506	6.945589	172.20.10.4	83.212.207.19	HTTP	495	GET / HTTP/1.1
1737	7.503152	172.20.10.4	83.212.207.19	HTTP	438	GET /favicon.ico HTTP/1.1

11. Το πρώτο HTTP GET μήνυμα του υπολογιστή μας προς τον Web Server που φιλοξενεί το ccslab.aueb.gr είναι το πρώτο εκ των δύο της παραπάνω φωτογραφίας, και για αυτό ισχύουν :

a) Για να δούμε αν το συγκεκριμένο IP datagram έχει υποστεί fragmentation επεκτείνουμε την καρτέλα Internet Protocol Version 4 του πακέτου και σύμφωνα με τις τιμές των πεδίων της IP κεφαλίδας παρατηρούμε ότι δεν έχει πραγματοποιηθεί κατακερματισμός αφού το bit Don't Fragment (DF) είναι 1.

```
▾ 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment Offset: 0
```

b) Ο Browser μας όπως μπορούμε να δούμε και επεκτείνοντας την καρτέλα HyperText Transfer Protocol του πακέτου χρησιμοποιεί την έκδοση 1.1 του HTTP.

```
▾ Hypertext Transfer Protocol
  › GET / HTTP/1.1\r\n
```

c) Επεκτείνοντας πάλι την ίδια καρτέλα μπορούμε να δούμε το πεδίο `Connection: keep-alive\r\n` το οποίο υποδηλώνει ότι η σύνδεση είναι persistent.

12. Το μήνυμα με το οποίο απαντάει ο web server στο GET HTTP είναι το ακόλουθο :

```
1574 7.068349    83.212.207.19    172.20.10.4    HTTP    864 HTTP/1.1 200 OK  (text/html)
```

και για αυτό ισχύουν :

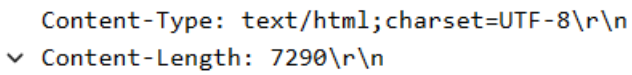
a) Η έκδοση του HTTP που χρησιμοποιεί ο server είναι η 1.1, ίδια με προηγουμένως :

```
▾ Hypertext Transfer Protocol
  › HTTP/1.1 200 OK\r\n
```

b) Το λογισμικό που υλοποιεί τον web server είναι το :

```
Server: Apache/2.4.18 (Ubuntu)\r\n
```

c) Το μέγεθος και ο τύπος του αρχείου φαίνονται αντίστοιχα από το content-length και content-type της παρακάτω λήψης :



13. Το πρώτο frame που ανταλλάσσεται μεταξύ του υπολογιστή μας και του server που φιλοξενεί το eclass.aueb.gr είναι το :

και αυτό που κάνει είναι να προσπαθεί να εγκαθιδρύσει σύνδεση για HTTPS όπως φαίνεται από την θύρα προορισμού 443.

14. Όπως απαντήθηκε και στην προηγούμενη ερώτηση, λόγω του γεγονότος ότι το eclass.aueb.gr χρησιμοποιεί το πρωτόκολλο HTTPS,σημαίνει ότι ο server δέχεται τα αιτήματα μηνυμάτων από τους πελάτες στην θύρα 443.

15. Όπως προαναφέρθηκε, επειδή το eclass.aueb.gr χρησιμοποιεί το πρωτόκολλο HTTPS, τα HTTP μηνύματα που ανταλλάσσει ο υπολογιστης μας με τον web server που φιλοξενεί το eclass.aueb.gr είναι κρυπτογραφημένα και δεν μπορούμε να τα δούμε μέσω του Wireshark

16. Ο υπολογιστής και το eclass.aueb.gr στην μεταξύ τους επικοινωνία χρησιμοποιούν την έκδοση `TLSv1.2` του Transport Layer Security.