

ΑΣΚΗΣΗ 1

1. Το πρώτο πακέτο έφτασε 0 και το τελευταίο 112 δηλαδή κράτησε 1 λεπτό και 52 δευτερόλεπτα. Αυτό μπορούμε να το επιβεβαιώσουμε και άμα πάμε Statistics-> Capture File Properties μέσα σε αυτό το παράθυρο θα δούμε μια κατηγορία Time και εκεί αναγράφεται ο συνολικός χρόνος (elapsed).
2. Παραθέτω τον πίνακα που έφτιαξα και τον πίνακα του wireshark

	A	B
1	Επίπεδο	Πρωτόκολλα
2	Physical Layer	Frame (Wireshark Level)
3	Data Link Layer	Ethernet
4	Network Layer	Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6), Address Resolution Protocol (ARP)
5	Transport Layer	Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP)
6	Application Layer	QUIC IETF, Domain Name System (DNS), Multicast DNS, Transport Layer Security (TLS), eXtensible Markup Language (XML), NetBIOS, Simple Service Discovery Protocol (SSDP)

Protocol	Percent Packets	Packets	Percent Bytes
▼ Frame	100.0	659	100.0
▼ Ethernet	100.0	659	6.4
▼ Internet Protocol Version 6	30.3	200	5.0
▼ User Datagram Protocol	17.5	115	0.6
QUIC IETF	6.5	43	12.2
Multicast Domain Name System	0.2	1	0.0
eXtensible Markup Language	1.1	7	2.9
Domain Name System	9.7	64	3.5
▼ Transmission Control Protocol	10.8	71	0.9
Transport Layer Security	4.4	29	3.6
Data	0.5	3	0.0
Internet Control Message Protocol v6	2.1	14	0.4
▼ Internet Protocol Version 4	52.4	345	4.3
▼ User Datagram Protocol	5.5	36	0.2
Simple Service Discovery Protocol	0.6	4	0.4
NetBIOS Name Service	2.7	18	0.6
Multicast Domain Name System	0.2	1	0.0
eXtensible Markup Language	1.1	7	2.9
Domain Name System	0.3	2	0.1
Data	0.6	4	0.1
▼ Transmission Control Protocol	33.4	220	2.9
Transport Layer Security	12.1	80	56.6
Data	0.5	3	0.0
Internet Group Management Protocol	0.3	2	0.0
Internet Control Message Protocol	13.2	87	4.2
Address Resolution Protocol	17.3	114	2.0

3. Επίπεδα μεταφοράς που αναγράφονται είναι το TCP και το UDP.

TCP χρησιμοποιείται από:

TLP(Transport Layer Security)

Data

UDP χρησιμοποιείται από:

QUIC

MDNS(Multicast Domain Name System)

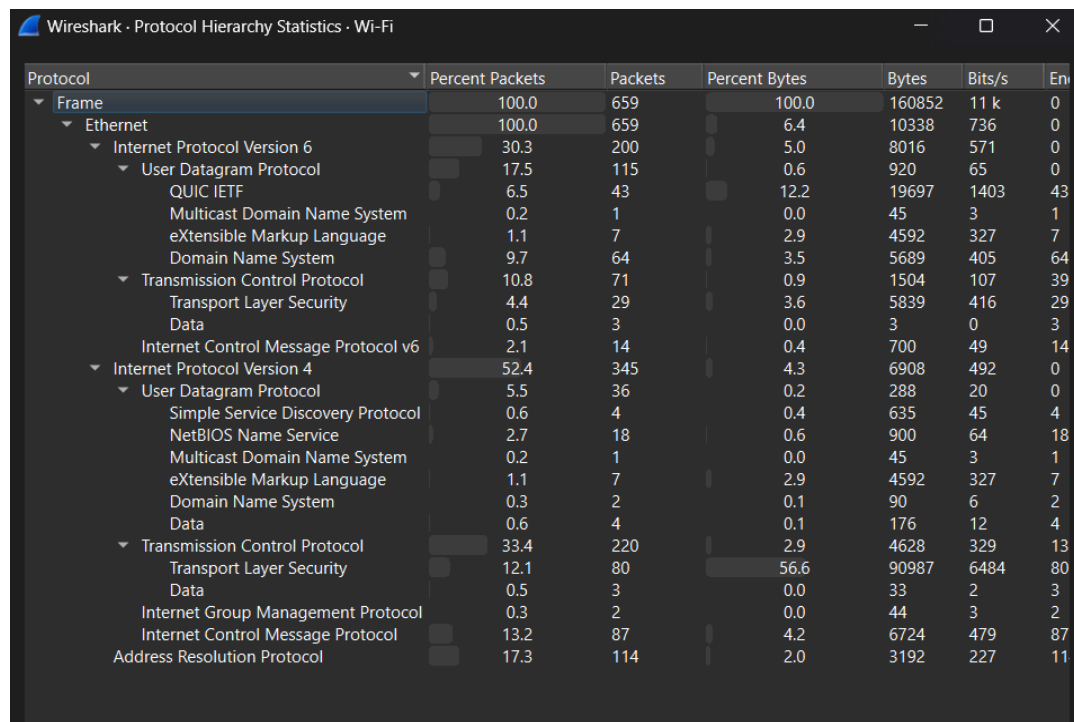
XML (eXtensive Markup Language)

DNS (Domain Name System)

SSDP (Simple Service Discovery Protocol)

NBNS (NetBIOS Name Service)

Data



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	Errors
Frame	100.0	659	100.0	160852	11 k	0
Ethernet	100.0	659	6.4	10338	736	0
Internet Protocol Version 6	30.3	200	5.0	8016	571	0
User Datagram Protocol	17.5	115	0.6	920	65	0
QUIC IETF	6.5	43	12.2	19697	1403	43
Multicast Domain Name System	0.2	1	0.0	45	3	1
eXtensible Markup Language	1.1	7	2.9	4592	327	7
Domain Name System	9.7	64	3.5	5689	405	64
Transmission Control Protocol	10.8	71	0.9	1504	107	39
Transport Layer Security	4.4	29	3.6	5839	416	29
Data	0.5	3	0.0	3	0	3
Internet Control Message Protocol v6	2.1	14	0.4	700	49	14
Internet Protocol Version 4	52.4	345	4.3	6908	492	0
User Datagram Protocol	5.5	36	0.2	288	20	0
Simple Service Discovery Protocol	0.6	4	0.4	635	45	4
NetBIOS Name Service	2.7	18	0.6	900	64	18
Multicast Domain Name System	0.2	1	0.0	45	3	1
eXtensible Markup Language	1.1	7	2.9	4592	327	7
Domain Name System	0.3	2	0.1	90	6	2
Data	0.6	4	0.1	176	12	4
Transmission Control Protocol	33.4	220	2.9	4628	329	13
Transport Layer Security	12.1	80	56.6	90987	6484	80
Data	0.5	3	0.0	33	2	3
Internet Group Management Protocol	0.3	2	0.0	44	3	2
Internet Control Message Protocol	13.2	87	4.2	6724	479	87
Address Resolution Protocol	17.3	114	2.0	3192	227	11

4. icmp
5. a. Οι συσκευές που επικοινωνούν είναι ο αποστολέας του ICMP echo request δηλαδή η συσκευή μου και ο παραλήπτης δηλαδή πιθανά το router μου. Έχουν mac address 4c:22:f3:18:a0:1a και 50:5a:65:21:f9:61 αντιστοίχως
- b. Η ip address του υπολογιστή μου είναι η ip address του source που αναγράφεται στο πρώτο ICMP echo request 192.168.1.1
- c. Η ip του destination είναι 192.168.1.153 όπου είναι αναγράφεται και αυτή στο πρώτο ICMP echo request
- d. Το time to live αναγράφεται πάνω στο package ως ttl και είναι 1
- e. Το total length αναγράφεται στις λεπτομέρειες του επιλεγμένου πακέτου και συγκεκριμένα στο internet protocol και είναι 84

No.	Time	Source	Destination	Protocol	Length	Info
20	5.478998	192.168.1.1	192.168.1.153	ICMP	98	Echo (ping) request id=0x3019
205	26.030627	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
206	26.035663	192.168.1.1	192.168.1.153	ICMP	134	Time-to-live exceeded (Time to
207	26.036372	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
208	26.040481	192.168.1.1	192.168.1.153	ICMP	134	Time-to-live exceeded (Time to
209	26.041089	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
210	26.045797	192.168.1.1	192.168.1.153	ICMP	134	Time-to-live exceeded (Time to
213	27.062455	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
214	27.072729	10.106.108.100	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to
215	27.073700	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
216	27.083853	10.106.108.100	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to
217	27.084769	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
218	27.094183	10.106.108.100	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to
237	33.026011	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
238	33.037421	79.128.248.41	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to
239	33.038468	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
240	33.049328	79.128.248.41	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to
241	33.050192	192.168.1.153	140.82.121.4	ICMP	106	Echo (ping) request id=0x0001
242	33.061097	79.128.248.41	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to

Frame 20: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{E96C881A-B...}
Ethernet II, Src: Arcadyan 18:a0:1a (4c:22:f3:18:a0:1a), Dst: AzureWaveTec 21:f9:61 (50:5a:65:21:f9:61)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.153
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0xc8fd (51453)
010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
[Expert Info (Note/Sequence): "Time To Live" only 1]
Protocol: ICMP (1)
Header Checksum: 0x2cc1 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1
Destination Address: 192.168.1.153
[Stream index: 2]
Internet Control Message Protocol

6. a. Η ip του Source είναι η ip του υπολογιστή μου.

b. Η ip του Destination είναι η ip του επόμενο δέκτη δηλαδή πιθανά του router και οι δυο ip αναγράφονται παραπάνω.

7. Οι ip που βρέθηκαν στο wireshark

192.168.1.1
 10.106.108.100
 79.128.248.41
 79.128.226.32
 79.128.250.118
 79.128.35.133
 79.128.250.117
 62.75.3.137
 62.75.4.126
 80.81.196.79

Δεν υπάρχει πλήρης αντιστοιχία με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt παράθυρο καθώς αντιστοιχούνται όλες εκτός από την 140.82.121.4 όπου υπάρχει στο command prompt και όχι στο wireshark.

```
Tracing route to github.com [140.82.121.4]
over a maximum of 30 hops:
```

```
  1      5 ms      4 ms      4 ms  telekom.ip [192.168.1.1]
  2     10 ms     10 ms      9 ms  10.106.108.100
  3     11 ms     10 ms     10 ms  nyma-asr99a-nyma-asr9ka.backbone.otenet.net [79.128.248.41]
  4     11 ms      9 ms      9 ms  79.128.226.32
  5     11 ms      9 ms     11 ms  79.128.250.118
  6     10 ms      *      10 ms  79.128.35.133
  7     14 ms     13 ms     11 ms  79.128.250.117
  8     13 ms     30 ms     11 ms  kolasr02-hu-0-1-0-0.ath.OTEGlobe.gr [62.75.3.137]
  9     45 ms     46 ms     45 ms  62.75.4.126
 10     52 ms     83 ms     43 ms  de-cix.fra.github.com [80.81.196.79]
 11      *        *        *    Request timed out.
 12      *        *        *    Request timed out.
 13     45 ms     45 ms     45 ms  lb-140-82-121-4-fra.github.com [140.82.121.4]
```

No.	Time	Source	Destination	Protocol	Length	Info
206	26.035663	192.168.1.1	192.168.1.153	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
208	26.040481	192.168.1.1	192.168.1.153	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
210	26.045797	192.168.1.1	192.168.1.153	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
214	27.072729	10.106.108.100	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
216	27.083853	10.106.108.100	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
218	27.094183	10.106.108.100	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
238	33.037421	79.128.248.41	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
240	33.049328	79.128.248.41	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
242	33.061097	79.128.248.41	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
246	34.083787	79.128.226.32	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
248	34.094775	79.128.226.32	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
250	34.105172	79.128.226.32	192.168.1.153	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
296	40.077516	79.128.250.118	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
298	40.088501	79.128.250.118	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
300	40.100370	79.128.250.118	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
335	46.056099	79.128.35.133	192.168.1.153	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
347	49.944774	79.128.35.133	192.168.1.153	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
365	55.903358	79.128.250.117	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
367	55.917547	79.128.250.117	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
369	55.930428	79.128.250.117	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
389	61.883125	62.75.3.137	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
393	61.915212	62.75.3.137	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
395	61.928674	62.75.3.137	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
404	62.992318	62.75.4.126	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
406	63.039370	62.75.4.126	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
408	63.085943	62.75.4.126	192.168.1.153	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
493	69.039577	80.81.196.79	192.168.1.153	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
495	69.123688	80.81.196.79	192.168.1.153	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
500	69.168745	80.81.196.79	192.168.1.153	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

ΑΣΚΗΣΗ 2

1. tcp πακέτα που στάλθηκαν είναι 11455
udp πακέτα που στάλθηκαν είναι 1145
το βρήκα κάνοντας filter με tcp και udp αναλόγως.

2. 1. ff:ff:ff:ff:ff:ff
2. 50:5a:65:21:f9:61
3. 4c:22:f3:18:a0:21
4. 4c:22:f3:18:a0:1a
5. 33:33:00:00:00:fb
6. 33:33:00:00:00:16
7. 33:33:00:00:00:01
8. 01:00:5e:7f:ff:fa
9. 01:00:5e:00:00:fb
10. 01:00:5e:00:00:16
11. 01:00:5e:00:00:01

11 διαφορετικά endpoints.

Δεν κατάφερα να εντοπίσω για πλήρως τι συσκευές είναι όλα τα endpoints αλλά κατάφερα να βρω τα εξής.

50:5a:65:21:f9:61= μια συσκευή που έστειλε και δέχτηκε τα περισσότερα πακέτα. Το OUI της αντιστοιχεί στην AzureWave technologies . Η συγκεκριμένη εταιρία συνδέεται με κάρτες wifi οπότε υποθέτω ότι είναι η κάρτα wifi του laptop μου.

4c:22:f3:18:a0:21,4c:22:f3:18:a0:1a=

Το OUI και των δύο αντιστοιχεί στην εταιρεία Arcadyan Technology Corp που παρέχει υπηρεσίες επικοινωνίας και το 3ο endpoint έχει στείλει μόνο πακέτα άρα υποθέτω ότι μπορεί να είναι κάποιος server η κάποιο κομμάτι που χρησιμεύει στην επικοινωνία.

Τα υπόλοιπα endpoints χρησιμοποιούνται για τα πρωτόκολλα IPV4 και IPV6

Endpoint Settings

☒ Name resolution

☒ Limit to display filter

Copy

Map

Ethernet · 11

IPv4 · 24

IPv6 · 33

TCP · 126

UDP · 159

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
ff:ff:ff:ff:ff:ff	28	1 kB	0	0 byte	28	1 kB
50:5a:65:21:f9:61	12.616	13 MB	5.712	745 kB	6.904	13 MB
4c:22:f3:18:a0:21	5.055	10 MB	5.055	10 MB	0	0 byte
4c:22:f3:18:a0:1a	7.584	3 MB	1.879	2 MB	5.705	744 kB
33:33:00:00:00:fb	1	107 byte	0	0 byte	1	107 byte
33:33:00:00:00:16	2	260 byte	0	0 byte	2	260 byte
33:33:00:00:00:01	2	256 byte	0	0 byte	2	256 byte
01:00:5e:7f:ff:fa	1	167 byte	0	0 byte	1	167 byte
01:00:5e:00:00:fb	1	87 byte	0	0 byte	1	87 byte
01:00:5e:00:00:16	1	70 byte	0	0 byte	1	70 byte
01:00:5e:00:00:01	1	52 byte	0	0 byte	1	52 byte

3. Έχουμε για IPV4 24 και IPV6 33 διαφορετικά endpoints . Συνολικά 57.

Δεν αντιστοιχίζονται πλήρως με το ethernet καθώς για μια συσκευής στο ethernet υπάρχει ένα Mac Adress Όμως η ίδια συσκευή μπορεί να έχει πολλά ipv4 και ipv6 αναλόγως. Επίσης Τα mac addreses αντιστοιχούν για την τοπική επικοινωνία. για εξωτερικές συσκευές χρησιμοποιούν τα ip address.

4. Χρησιμοποιούμε το φίλτρο dns και βλέπουμε ποια packets είναι query(αιτήματος) και ποια response(απάντησης).Κάθε αίτημα query διαθέτει ένα transaction id.Το response Που απαντάει στο σε ένα συγκεκριμένο query έχει το ίδιο transaction id με αυτό. Έτσι το αίτημα αντιστοιχίζεται με την απάντηση του.
5. Ναι υπάρχει κάποιο flag που απαντάει αν ο server που μας απαντάει είναι authoritative η όχι για το συγκεκριμένο domain. Βρίσκουμε την απάντηση του query για τον server που μας ενδιαφέρει και κοιτάμε το Domain Name System στις πληροφορίες της εγγραφής. Στην κατηγορία flags θα βρούμε το authoritative flag που μας λέει αν ο συγκεκριμένος server είναι η όχι authoritative.Ο συγκεκριμένος server δεν είναι authoritative καθώς η τιμή του flag είναι 0.
6. Το www.faqs.org είναι alias καθώς άμα βρούμε σε κάποιο response για το query που ζητά για τον www.faqs.org και ψάξουμε το Domain Name System στις πληροφορίες της εγγραφής. Στην κατηγορία Answers θα βρούμε να λέει Type: CNAME (5) (Canonical NAME for an alias) και ποιο κάτω αναφέρεται το όνομα του alias όπου είναι faqs.org.
7. Χρησιμοποίησα το ping www.faqs.org για να μπορέσω να βρώ την ip του www.faqs.org και την χρησιμοποίησα ως φίλτρο στο whireshark για να βρω τα tcp packets που έχουν είτε source είτε destination ip την ip του www.faqs.org.Έπειτα βρήκα τα πρώτα τρία tcp segment που έχουν [SYN],[SYN,ACK],[ACK] και τα επιβεβαιώνω ότι επικοινωνούν μεταξύ τους μέσα από το seqment analysis.
 Το No 558 στέλνει αίτημα από τον υπολογιστή μου στον server του faqs.org ώστε να δημιουργηθεί σύνδεση [SYN].
 Το No 636 είναι η επιβεβαίωση της σύνδεσης από τον server στον υπολογιστή μου[SYN-ACK].
 Το No 638 είναι η επιβεβαίωση από τον υπολογιστή μου[ACK].

exercise 2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==199.231.164.68

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
558	12.959058	192.168.1.153	199.231.164.68	TCP	66	52876	443	52876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
636	13.142390	199.231.164.68	192.168.1.153	TCP	66	443	52876	443 → 52876 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM
638	13.142486	192.168.1.153	199.231.164.68	TCP	54	52876	443	52876 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
639	13.142847	192.168.1.153	199.231.164.68	TCP	1506	52876	443	52876 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=1452 [TCP PDU reassemb]
640	13.142847	192.168.1.153	199.231.164.68	TLSv1.2	357	52876	443	Client Hello (SNI=www.faqs.org.)
645	13.311167	199.231.164.68	192.168.1.153	TCP	54	443	52876	443 → 52876 [ACK] Seq=1 Ack=1453 Win=64128 Len=0
646	13.311167	199.231.164.68	192.168.1.153	HTTP	541	443	52876	HTTP/1.1 400 Bad Request (text/html)
647	13.311167	199.231.164.68	192.168.1.153	TCP	54	443	52876	443 → 52876 [FIN, ACK] Seq=488 Ack=1453 Win=64128 Len=0
649	13.311231	192.168.1.153	199.231.164.68	TCP	54	52876	443	52876 → 443 [ACK] Seq=1756 Ack=489 Win=131584 Len=0
650	13.311459	192.168.1.153	199.231.164.68	HTTP	61	52876	443	Continuation
651	13.311804	192.168.1.153	199.231.164.68	TCP	54	52876	443	52876 → 443 [FIN, ACK] Seq=1763 Ack=489 Win=131584 Len=0
652	13.312210	192.168.1.153	199.231.164.68	TCP	66	52877	443	52877 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
653	13.356593	199.231.164.68	192.168.1.153	TCP	54	443	52876	443 → 52876 [ACK] Seq=489 Ack=1756 Win=64128 Len=0
654	13.468508	199.231.164.68	192.168.1.153	TCP	54	443	52876	443 → 52876 [ACK] Seq=489 Ack=1763 Win=64128 Len=0
655	13.468508	199.231.164.68	192.168.1.153	TCP	54	443	52876	443 → 52876 [ACK] Seq=489 Ack=1764 Win=64128 Len=0
656	13.472493	199.231.164.68	192.168.1.153	TCP	66	443	52877	443 → 52877 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM
657	13.472544	192.168.1.153	199.231.164.68	TCP	54	52877	443	52877 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
658	13.472874	192.168.1.153	199.231.164.68	TCP	1506	52877	443	52877 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=1452 [TCP PDU reassemb]
659	13.472874	192.168.1.153	199.231.164.68	TLSv1.2	389	52877	443	Client Hello (SNI=www.faqs.org.)
660	13.642479	199.231.164.68	192.168.1.153	TCP	54	443	52877	443 → 52877 [ACK] Seq=1 Ack=1453 Win=64128 Len=0
661	13.642479	199.231.164.68	192.168.1.153	HTTP	541	443	52877	HTTP/1.1 400 Bad Request (text/html)

Source Port: 52876
 Destination Port: 443
 [Stream index: 11]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 0 (relative sequence number)
 Sequence Number (raw): 3739743208

8. Όπως φαίνεται στο screenshot που έβαλα στο προηγούμενο ερώτημα βλέπουμε μια επικοινωνία μεταξύ των port 52876 και 443 το 52876 πρόκειται για το προσωρινό port που αντιστοιχείται με τον υπολογιστή μου και το 433 είναι του http.
9. Μπορώ να δω τα http get χρησιμοποιώντας το filter http και ψάχνοντας το info για να δούμε το GET. Οι ip διευθύνσεις που χρησιμοποιήθηκαν είναι οι η δικιά μου και του αντίστοιχου server που κάνουμε ο αίτημα get.
10.
 - a. πρώτο http get προς τον host του faqs χρησιμοποιούμε την έκδοση HTTP/1.1
 - b. Η σύνδεση είναι presistans γιατί άμα πάμε στις λεπτομέρειες του πακέτου στην κατηγορία του Hypertext Transfer Protocol θα δούμε ότι Connection:keep-alive που σημαίνει ότι η σύνδεση είναι presistans.
11.
 - a. Στο μήνυμα απάντηση ο server χρησιμοποιεί και αυτός HTTP/1.1.
 - b. Το λογισμικό που υλοποιεί τον web server είναι το apache.
 - c. Το μέγεθος είναι 233 Bytes και ο τύπος είναι text/html.
12. Το πρώτο frame που βρέθηκε είναι dns και ο στόχος του είναι να πάρει την ip του aueb.gr από το domain name server.
13. Το port που δέχεται αιτήματα είναι το 433 καθώς είναι το μόνο που αντιστοιχεί στην ip του www.aueb.gr.
14. Όχι δεν μπορώ να δω το περιεχόμενο των http μηνυμάτων καθώς χρησιμοποιεί το port 443 που προσφέρει κρυπτογράφηση.
15. Πάλι χρησιμοποιώντας την ip του aueb.gr για να φιλτράρουμε τα αντίστοιχα πακέτα βλέπουμε ότι στο tls server hello χρησιμοποιεί την έκδοση TLS 1.2