

**ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ**



ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

Δίκτυα Επικοινωνιών

2023-2024

Ονοματεπώνυμο:

Κεχριώτη Ελένη

Αριθμός Μητρώου:

3210078

Email:

ρ3210078@aueb.gr

Άσκηση 1

Τα αποτελέσματα από την εκτέλεση της εντολής **tracert** www.w3schools.com φαίνονται παρακάτω.

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

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

  1    8 ms    19 ms    20 ms    speedport.ip [192.168.1.1]
  2   23 ms    21 ms    32 ms    80.106.125.100
  3   22 ms    23 ms    41 ms    79.128.225.53
  4  131 ms   133 ms   144 ms   pirg-asr9ka-patr-asr9kb.backbone.otenet.net [79.128.234.22]
  5  158 ms   197 ms   162 ms   kolasr01-hu-0-5-0-0.ath.OTEGlobe.gr [62.75.3.13]
  6   56 ms    55 ms    57 ms    62.75.4.146
  7   58 ms    56 ms    57 ms    ae-126.border1.frn.edgecastcdn.net [152.195.101.210]
  8   58 ms    58 ms    65 ms    ae-66.core1.frb.edgecastcdn.net [152.195.101.131]
  9   98 ms   103 ms   100 ms   192.229.133.221

Trace complete.
```

1. Ποια ήταν η χρονική διάρκεια της ανίχνευσής σας;

Η χρονική διάρκεια της ανίχνευσης ήταν ≈ 35.2 δευτερόλεπτα. (τελευταίο πακέτο)

Μπορούμε όμως να το δούμε και από τα στατιστικά της ανίχνευσης

```
167 35.174604 2603:1020:5:4::e 2a02:587:a024:4518:... TCP 74 443 → 50595 [ACK] Seq=367 Ack=122 Win=501 Len=0
```

Time span, s 35.175

2. Προσδιορίστε σε ένα πίνακα, ποια διαφορετικά πρωτόκολλα ανιχνεύθηκαν κατά τη χρονική διάρκεια της ανίχνευσης, διαχωρίζοντάς τα σύμφωνα με τα επίπεδα στα οποία ανήκουν (όπως τα εμφανίζει το wireshark).

Τα πρωτόκολλα που ανιχνεύθηκαν είναι TLSv1.2, TCP, UDP, DNS, ICMP, ICMPv6, NBNS, ARP, MDNS, IPv4, IPv6.

Layer 3 (network)	Layer 4 (transport)	Layer 5 (application)
ICMP	TCP	DNS
ARP	UDP	TLSv1.2
ICMPv6		NBNS
IPv4		MDNS
IPv6		

Το ethernet είναι το πρωτόκολλο που είναι η “ρίζα” κάθε πρωτοκόλλου και ανήκει στο επίπεδο σύνδεσης. Δεν το έβαλα στον πίνακα γιατί δεν ανιχνεύεται “καθαρά” στο wireshark πάνω σε πακέτο, αλλά βρίσκεται πίσω από όλα τα πρωτόκολλα, όπως π.χ. εδώ [Protocols in frame: eth:ethertype:ip:tcp:tls]

Protocol

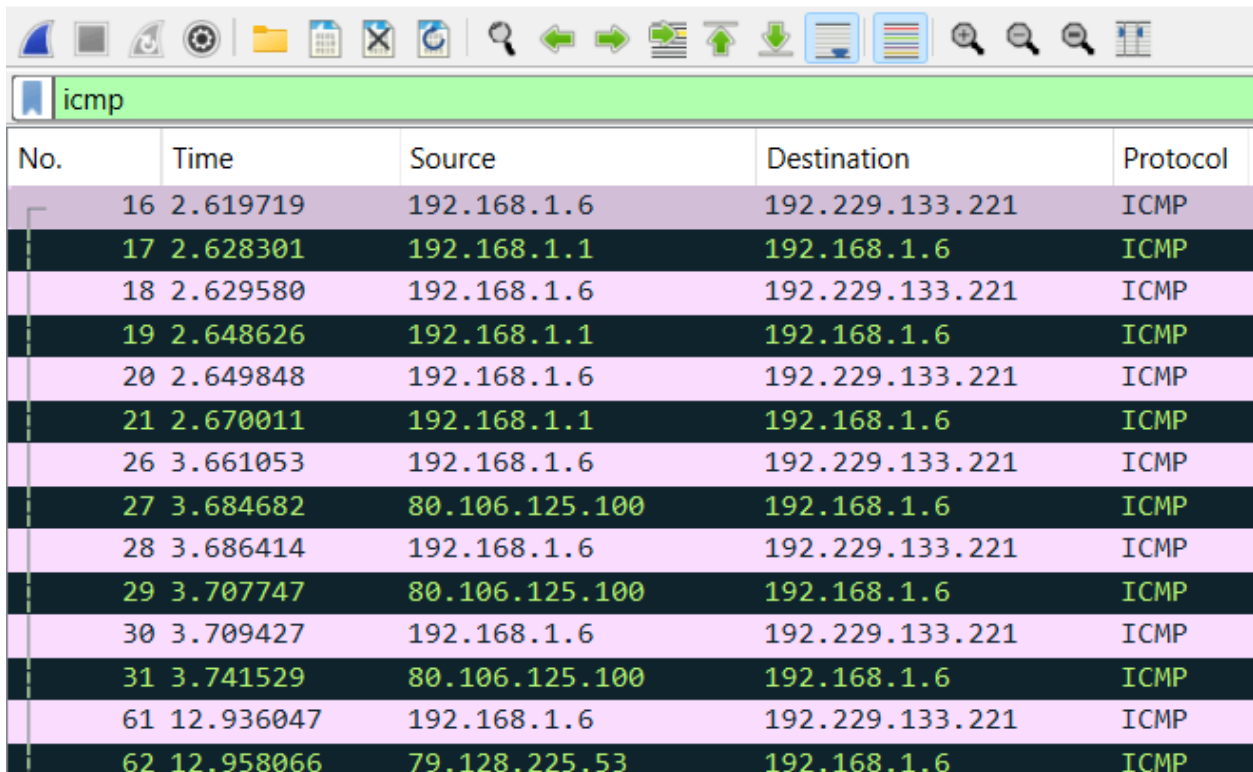
- Internet Protocol Version 6
 - User Datagram Protocol
 - Domain Name System
 - Transmission Control Protocol
 - Transport Layer Security
 - Internet Control Message Protocol v6
 - Internet Protocol Version 4
 - User Datagram Protocol
 - NetBIOS Name Service
 - Multicast Domain Name System
 - Domain Name System
 - Transmission Control Protocol
 - Transport Layer Security
 - Internet Control Message Protocol
 - Address Resolution Protocol

3. Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.

Τα πρωτόκολλα DNS, MDNS, NBNS χρησιμοποιούν UDP. Το πρωτόκολλο TLSv1.2 χρησιμοποιεί TCP.

4. Ποιο φίλτρο θα χρησιμοποιήσετε ώστε να εμφανίζονται στο παράθυρο του wireshark μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP;

Στο filter γράφουμε icmp για να δούμε μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP.



The image shows the Wireshark network protocol analyzer interface. The packet list pane on the left has a filter 'icmp' applied. The main packet list pane displays a table of captured packets, all of which are ICMP. The table has five columns: No., Time, Source, Destination, and Protocol. The packets are numbered 16 through 62, with some gaps. The source and destination IP addresses vary, including 192.168.1.6, 192.229.133.221, 192.168.1.1, 80.106.125.100, and 79.128.225.53. All protocols listed are ICMP.

No.	Time	Source	Destination	Protocol
16	2.619719	192.168.1.6	192.229.133.221	ICMP
17	2.628301	192.168.1.1	192.168.1.6	ICMP
18	2.629580	192.168.1.6	192.229.133.221	ICMP
19	2.648626	192.168.1.1	192.168.1.6	ICMP
20	2.649848	192.168.1.6	192.229.133.221	ICMP
21	2.670011	192.168.1.1	192.168.1.6	ICMP
26	3.661053	192.168.1.6	192.229.133.221	ICMP
27	3.684682	80.106.125.100	192.168.1.6	ICMP
28	3.686414	192.168.1.6	192.229.133.221	ICMP
29	3.707747	80.106.125.100	192.168.1.6	ICMP
30	3.709427	192.168.1.6	192.229.133.221	ICMP
31	3.741529	80.106.125.100	192.168.1.6	ICMP
61	12.936047	192.168.1.6	192.229.133.221	ICMP
62	12.958066	79.128.225.53	192.168.1.6	ICMP

5. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Echo Request.

a. Ποιες είναι οι συσκευές που επικοινωνούν σε επίπεδο Ethernet; Ποιες είναι οι MAC διευθύνσεις τους;

Η διεύθυνση MAC πηγής είναι 5c:fb:3a:53:74:ef και αντιστοιχεί στον υπολογιστή μου. Η διεύθυνση MAC προορισμού είναι 60:ce:86:48:c3:40 και αντιστοιχεί δρομολογητή του οικιακού δικτύου, μέσω του οποίου γίνεται η σύνδεση στο Διαδίκτυο.

- Destination: Sercomm_48:c3:40 (60:ce:86:48:c3:40)
- Source: ChongqingFug_53:74:ef (5c:fb:3a:53:74:ef)

b. Ποια είναι η IP διεύθυνση του υπολογιστή σας;

Η IP διεύθυνση του υπολογιστή μου είναι 192.168.1.6

c. Ποια είναι η IP διεύθυνση του destination;

Η IP διεύθυνση του προορισμού είναι 192.229.133.221

d. Πόσο είναι το time-to-live του πακέτου (ή το hop limit αν στο δίκτυο του provider τρέχει η IPv6 και όχι η IPv4 έκδοση του πρωτοκόλλου IP);

Το time-to-live του πακέτου είναι 1.

e. Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει;

Το μέγεθος των δεδομένων (data-length) είναι 64 bytes. Το συνολικό μέγεθος είναι 92 bytes, 20 για το IP header, 8 για ICMP και 64 για data.

```

v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.229.133.221
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xcc29 (52265)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0xe506 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.6
    Destination Address: 192.229.133.221
v Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7c7 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 55 (0x0037)
  Sequence Number (LE): 14080 (0x3700)
  > [No response seen]
  > Data (64 bytes)

```

6. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Time Exceeded.

a. Ποια είναι η IP διεύθυνση του destination;

Η IP διεύθυνση του προορισμού είναι 192.168.1.6

b. Ποια είναι η IP διεύθυνση του source;

Η IP διεύθυνση της πηγής είναι 192.168.1.1

17 2.628301	192.168.1.1	192.168.1.6	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
-------------	-------------	-------------	------	--

7. Αναφέρατε όλες τις source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα. Υπάρχει αντιστοιχία με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt παράθυρο;

Οι source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα είναι οι εξής:

- 192.168.1.1
- 80.106.125.100
- 79.128.225.53
- 79.128.234.22
- 62.75.3.13
- 62.75.4.146
- 152.195.101.210
- 152.195.101.131

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

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

  1    8 ms    19 ms    20 ms  speedport.ip [192.168.1.1]
  2    23 ms    21 ms    32 ms  80.106.125.100
  3    22 ms    23 ms    41 ms  79.128.225.53
  4   131 ms   133 ms   144 ms  pirg-asr9ka-patr-asr9kb.backbone.otenet.net [79.128.234.22]
  5   158 ms   197 ms   162 ms  kolasr01-hu-0-5-0-0.ath.OTEGlobe.gr [62.75.3.13]
  6    56 ms    55 ms    57 ms  62.75.4.146
  7    58 ms    56 ms    57 ms  ae-126.border1.frn.edgecastcdn.net [152.195.101.210]
  8    58 ms    58 ms    65 ms  ae-66.core1.frb.edgecastcdn.net [152.195.101.131]
  9    98 ms   103 ms   100 ms  192.229.133.221

Trace complete.
```

Παρατηρούμε ότι τα 8 πρώτα IP's στο cmd μετά την εκτέλεση της εντολής tracert είναι ίδια με αυτά που βρήκαμε και στο wireshark. Το τελευταίο IP source που βλέπουμε στο cmd αναφέρεται στο τελευταίο Echo reply.

152	30.294952	192.229.133.221	192.168.1.6	ICMP	106 Echo (ping) reply
-----	-----------	-----------------	-------------	------	-----------------------

Άσκηση 2

1. Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;

Για IPv4 στάλθηκαν 400 πακέτα TCP και για IPv6 στάλθηκαν 36 πακέτα UDP και 45 πακέτα TCP.

Internet Protocol Version 6	17.0	82
> User Datagram Protocol	7.5	36
> Transmission Control Protocol	9.3	45
Internet Control Message Protocol v6	0.2	1
Internet Protocol Version 4	83.0	400
> Transmission Control Protocol	83.0	400

2. Πόσα και ποια είναι τα διαφορετικά endpoints (η σχετική πληροφορία βρίσκεται στο μενού Statistics) με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet; Μπορείτε να βρείτε σε τί είδους συσκευές αντιστοιχούν;

Τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο ethernet είναι τα εξής:

- 5c:fb:3a:53:74:ef
- 60:ce:86:48:c3:40

Ethernet · 2	IPv4 · 9	IPv6 · 7	TCP · 39	UDP · 5		
Address ^	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
5c:fb:3a:53:74:ef	482	236 kB	205	26 kB	277	209 kB
60:ce:86:48:c3:40	482	236 kB	277	209 kB	205	26 kB

Ethernet · 2	IPv4 · 9
Address ^	Pac
ChongqingFug_53:74:ef	
Sercomm_48:c3:40	

και τα ονόματα που τους αντιστοιχούν είναι

Η διεύθυνση MAC 5c:fb:3a:53:74:ef αντιστοιχεί στον υπολογιστή μου. Η διεύθυνση MAC 60:ce:86:48:c3:40 αντιστοιχεί δρομολογητή του οικιακού δικτύου, μέσω του οποίου γίνεται η σύνδεση στο Διαδίκτυο.

3. Πόσα είναι τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP; Ταυτίζονται με τα endpoints σε επίπεδο Ethernet; Αν όχι, εξηγήστε γιατί συμβαίνει αυτό.

Τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP είναι τα εξής 16 (9 IPv4 και 7 IPv6):

- 20.50.201.195
- 20.82.247.147
- 34.111.115.192
- 44.241.53.189
- 83.212.207.19
- 192.168.1.1
- 192.168.1.6
- 192.229.221.95
- 195.251.255.227
- 2603:1026:240a::
- 2620:1ec:c11::239
- 2a00:1450:4001:811::2003
- 2a00:1450:4001:828::200a
- 2a02:587:a024:4518:982e:5a93:7043:a397
- fe80::1
- ff02::1

Τα endpoints αυτά δεν ταυτίζονται με τα endpoints σε επίπεδο ethernet αφού του ethernet αναφέρονται σε MAC ενώ αυτά σε IP.

Ethernet · 2	IPv4 · 9	IPv6 · 7
Address	Packets	Bytes
20.50.201.195	2	121 bytes
20.82.247.147	2	145 bytes
34.111.115.192	1	97 bytes
44.241.53.189	13	3 kB
83.212.207.19	76	92 kB
192.168.1.1	208	14 kB
192.168.1.6	400	207 kB
192.229.221.95	3	162 bytes
195.251.255.227	95	98 kB

Ethernet · 2	IPv4 · 9	IPv6 · 7
Address		
2603:1026:240a::		
2620:1ec:c11::239		
2a00:1450:4001:811::2003		
2a00:1450:4001:828::200a		
2a02:587:a024:4518:982e:5a93:7043:a3'		
fe80::1		
ff02::1		

4. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για την ερώτηση από τον υπολογιστή σας προς τον DNS server και για την απάντηση του DNS server.

Οι θύρες(ports) που χρησιμοποιήθηκαν για ερώτηση από τον υπολογιστή μου προς τον DNS server είναι οι εξής:

Source Port: 59926

59927, 59928, 59929, 59930, 59931, 59933, 59932, 59935, 59936, 59937, 59938, 59939, 59940, 59941, 59942

με Destination Port: 53

Οι θύρες(ports) που χρησιμοποιήθηκαν για την απάντηση του DNS server είναι οι εξής:

Destination Port: 59928, 59929, 59930, 59926, 59932, 59931, 59933, 59927, 59935, 59936, 59937, 59939, 59938, 59940, 59941, 59942

με Source Port: 53

Είναι εμφανές ότι ο DNS server χρησιμοποιεί μόνο την TCP port 53.

5. Πώς διακρίνεται αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα που έχετε κάνει; Πώς συνδέονται το πακέτο μιας απάντησης με το πακέτο της ερώτησης;

Αν ένα πακέτο περιέχει απάντηση σε ερώτημα το κατανοούμε διότι το destination είναι η IP διεύθυνση μας, το src port είναι 53 και επίσης αναγράφεται Standard query response.

```
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6
> Transmission Control Protocol, Src Port: 53, Dst Port: 59926, Seq: 2, Ack: 35, Len: 84
> [2 Reassembled TCP Segments (85 bytes): #114(1), #153(84)]
✓ Domain Name System (response)
```

Αν το πακέτο περιέχει αίτημα προς τον DNS server τότε γίνεται κατανοητό επειδή το src είναι η IP διεύθυνση μας, το dst port είναι 53 και αναγράφεται απλώς Standard query.

```
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1
> Transmission Control Protocol, Src Port: 59926, Dst Port: 53, Seq: 3, Ack: 1, Len: 32
> [2 Reassembled TCP Segments (34 bytes): #33(2), #34(32)]
✓ Domain Name System (query)
```

6. Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει είναι authoritative για το συγκεκριμένο domain; Ο name server που έχει απαντήσει είναι authoritative για το συγκεκριμένο domain;

Υπάρχει flag (0x8180) και μας λέει ότι ο server που μας έχει απαντήσει δεν είναι authoritative για το συγκεκριμένο domain.

```
✓ Flags: 0x8180 Standard query response, No error
  1... .. = Response: Message is a response
  .000 0... .. = Opcode: Standard query (0)
  .... .0.. .. = Authoritative: Server is not an authority for domain
  .... ..0. .... = Truncated: Message is not truncated
  .... ...1 .... = Recursion desired: Do query recursively
  .... .... 1... .. = Recursion available: Server can do recursive queries
  .... .... .0.. .... = Z: reserved (0)
  .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
  .... .... ...0 .... = Non-authenticated data: Unacceptable
  .... .... .... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
```

7. Το όνομα ccslab.aueb.gr είναι κανονικό dns όνομα ή alias; Ποια είναι η IP διεύθυνση που του αντιστοιχεί;

Το όνομα ccslab.aueb.gr είναι κανονικό dns όνομα. Η IP διεύθυνση που του αντιστοιχεί είναι 83.212.207.19.

```
ccslab.aueb.gr: type SOA, class IN, mname hermes.aueb.gr
```

```
Name: ccslab.aueb.gr
Type: SOA (6) (Start Of a zone of Authority)
Class: IN (0x0001)
Time to live: 900 (15 minutes)
Data length: 39
Primary name server: hermes.aueb.gr
Responsible authority's mailbox: nameadm.aueb.gr
Serial Number: 2018112101
Refresh Interval: 86400 (1 day)
Retry Interval: 3600 (1 hour)
Expire limit: 1209600 (14 days)
Minimum TTL: 86400 (1 day)
```

8. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το ccslab.aueb.gr υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων. Δώστε ένα screenshot από το Wireshark που να περιέχει τα segments αυτά. Εξηγήστε τη διαδικασία χειραψίας τριών βημάτων με βάση την πληροφορία που περιέχεται στα TCP segments αυτά.

2.863200	192.168.1.6	83.212.207.19	TCP	66 59934 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2.891199	83.212.207.19	192.168.1.6	TCP	66 80 → 59925 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1436 SACK_PERM WS=128
2.891405	192.168.1.6	83.212.207.19	TCP	54 59925 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0

I. (SYN) Ο πελάτης, δηλαδή εμείς, θέλει να εγκαθίδρυση σύνδεση με τον server, οπότε του στέλνει ένα segment με SYN. Το SYN δηλώνει με ποιόν αριθμό ξεκινάει τα segments του.

Παρατηρούμε ότι το sequence number που στέλνει ο πελάτης είναι αρχικοποιημένο, είναι το SYN (0) που στέλνεται στον server. Επίσης αν κοιτάξουμε στα flags θα δούμε ότι στο πεδίο του SYN γράφει set. Από αυτό γίνεται κατανοητό ότι είμαστε στο πρώτο μέρος του 3-way-handshaking.

```
Transmission Control Protocol, Src Port: 59934, Dst Port: 80, Seq: 0, Len: 0
```

```
Source Port: 59934
```

```
Destination Port: 80
```

```
[Stream index: 12]
```

```
> [Conversation completeness: Incomplete, ESTABLISHED (7)]
```

```
[TCP Segment Len: 0]
```

```
Sequence Number: 0 (relative sequence number)
```

```
Sequence Number (raw): 1714126444
```

```
[Next Sequence Number: 1 (relative sequence number)]
```

```
Acknowledgment Number: 0
```

```
Acknowledgment number (raw): 0
```

```
1000 .... = Header Length: 32 bytes (8)
```

```
▼ Flags: 0x002 (SYN)
```

```
000. .... = Reserved: Not set
```

```
...0 .... = Accurate ECN: Not set
```

```
.... 0... = Congestion Window Reduced: Not set
```

```
.... .0.. = ECN-Echo: Not set
```

```
.... ..0. = Urgent: Not set
```

```
.... ...0 .... = Acknowledgment: Not set
```

```
.... .... 0... = Push: Not set
```

```
.... .... .0.. = Reset: Not set
```

```
> .... .... ..1. = Syn: Set
```

```
.... .... ...0 = Fin: Not set
```

```
[TCP Flags: .....S.]
```

II. (SYN, ACK) ο server απαντάει στο αίτημα του πελάτη με ένα σετ από SYN-ACK signal bits. Το ACK (acknowledgement) δηλώνει την απάντηση στο segment που ο χρήστης έστειλε και το SYN δηλώνει τον αριθμό με τον οποίο ο server θα ξεκινάει τα segments του.

Παρατηρούμε ότι το sequence number που στέλνει ο server είναι αρχικοποιημένο, είναι το SYN που στέλνεται στον πελάτη για να ξέρει με ποιον αριθμό θα ξεκινάνε τα segments του ο server. Και το acknowledgement number έχει value (1) και δηλώνει response προς το αίτημα του πελάτη. Επίσης αν κοιτάξουμε στα flags θα δούμε ότι στο πεδίο του SYN γράφει set (1) και στο ACK γράφει set (1). Από αυτό γίνεται κατανοητό ότι είμαστε στο δεύτερο μέρος του 3-way-handshaking.

```

Transmission Control Protocol, Src Port: 80, Dst Port: 59925, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 59925
  [Stream index: 3]
> [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0      (relative sequence number)
  Sequence Number (raw): 4231067513
  [Next Sequence Number: 1      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 3123920541
  1000 .... = Header Length: 32 bytes (8)
  ✓ Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... 0... = ECN-Echo: Not set
    .... .0.  = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... ...0 = Push: Not set
    .... ...0 = Reset: Not set
  > .... ...1 = Syn: Set
    .... ...0 = Fin: Not set
  [TCP Flags: .....A..S.]

```

III. (ACK) Ο πελάτης τώρα αναγνωρίζει το response από τον server και πλέον εγκαθιδρύεται μια ασφαλή σύνδεση μεταξύ τους για τη μεταφορά δεδομένων.

Παρατηρούμε ότι το sequence number είναι ίδιο με το αρχικό που έστειλε ο πελάτης. Και το acknowledgement number έχει value και δηλώνει response του πελάτη στον server. Επίσης αν κοιτάξουμε στα flags θα δούμε ότι στο πεδίο του ACK γράφει set. Από αυτό γίνεται κατανοητό ότι είμαστε στο τρίτο και τελευταίο part του 3-way-handshaking.

```

Transmission Control Protocol, Src Port: 59925, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 59925
  Destination Port: 80
  [Stream index: 3]
> [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3123920541
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4231067514
  0101 .... = Header Length: 20 bytes (5)
  ✓ Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  [TCP Flags: .....A....]

```

9. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το TCP πρωτόκολλο για την επικοινωνία με τον server που φιλοξενεί το `ccslab.aueb.gr`.

Παρατηρούμε ότι ο server χρησιμοποιεί το port 80, ενώ ο πελάτης(εμείς) τα ports 59934 και 59925. Στέλνουμε αίτημα μέσω των ports 59934 , 59934 και λαμβάνουμε response μέσω αυτών. Ο server στέλνει response μέσω του port 80 και λαμβάνει request μέσω του ίδιου port. Η θύρα 80 είναι η default θύρα που χρησιμοποιείται για διαδικτυακές συναλλαγές και συγκεκριμένα για το HTTP πρωτόκολλο.

```

Source Port: 59925      Source Port: 80
Destination Port: 80    Destination Port: 59925

```

```

Source Port: 59934      Source Port: 80
Destination Port: 80    Destination Port: 59934

```

10. Μπορείτε να δείτε τα πακέτα που περιέχουν HTTP GET αίτημα από τον Browser σας προς τον Web Server; Αν ναι, προς ποιες IP διευθύνσεις στάλθηκαν. Αν όχι, εξηγήστε γιατί.

Ναι μπορώ να δω τα πακέτα που περιέχουν HTTP GET αιτήματα, γιατί γίνονται σε σελίδα που χρησιμοποιεί το HTTP πρωτόκολλο. Ο browser έστειλε 2 HTTP GET request. Τα μηνύματα αυτά στάλθηκαν στην IP διεύθυνση του ccslab.aueb.gr που είναι: 83.212.207.19

http.request.method==GET						
No.	Time	Source	Destination	Protocol	Length	Info
102	2.891805	192.168.1.6	83.212.207.19	HTTP	1139	GET / HTTP/1.1
229	3.457989	192.168.1.6	83.212.207.19	HTTP	1231	GET /wp-content/plugins/elementor/assets/lib/

11. Βρείτε το πρώτο HTTP GET μήνυμα του υπολογιστή σας προς τον server που φιλοξενεί το ccslab.aueb.gr.

a. Έχει πραγματοποιηθεί fragmentation στο συγκεκριμένο IP datagram; Εξηγήστε την απάντησή σας με βάση τιμές πεδίων της IP επικεφαλίδας.

Το flags έχει τιμή 010, το πρώτο bit (0) είναι δεσμευμένο, το δεύτερο bit (1) είναι η τιμή του DF που σημαίνει Don't Fragment και με τιμή ένα σημαίνει ότι δεν κατακερματίζουμε το πακέτο και τελευταίο το τρίτο bit (0) που σημαίνει ότι δεν υπάρχουν περισσότερα κομμάτια (MF).

```
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 83.212.207.19
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1125
    Identification: 0x2f27 (12071)
  ✓ 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
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0xe2d5 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.6
  Destination Address: 83.212.207.19
```

b. Ποια έκδοση του HTTP χρησιμοποιεί ο browser σας;

Η έκδοση του HTTP που τρέχει ο browser μου είναι: HTTP/1.1 .

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
```

c. Η σύνδεση είναι persistent ή non-persistent; Πως το συμπεραίνετε;

Από την τελευταία γραμμή του screenshot βλέπουμε ότι η σύνδεση είναι keep-alive, που σημαίνει ότι η σύνδεση είναι persistent. Στη 1.1 έκδοση του HTTP είναι default η persistent σύνδεση.

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: ccslab.aueb.gr\r\n
      Connection: keep-alive\r\n
```

12. Εντοπίστε το μήνυμα με το οποίο απαντάει στο HTTP GET αυτό ο web server.

129	3.071491	83.212.207.19	192.168.1.6	HTTP	585	HTTP/1.1 200 OK (text/html)
297	3.789219	83.212.207.19	192.168.1.6	HTTP	553	HTTP/1.1 200 OK

a. Ποια έκδοση του HTTP χρησιμοποιεί ο server;

Η έκδοση του HTTP που τρέχει ο server είναι: HTTP/1.1

Hypertext Transfer Protocol

✓ HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

b. Ποιο είναι το λογισμικό που υλοποιεί τον web server;

Το λογισμικό που υλοποιεί τον web server είναι το Ubuntu Apache έκδοση 2.4.18.

Date: Tue, 26 Dec 2023 09:50:57 GMT\r\n

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

Link: <http://ccslab.aueb.gr/index.php/wp-json/>; rel="https://api.w.org/",

c. Ποιο είναι το μέγεθος και ο τύπος του αρχείου που στέλνει πίσω ο web server;

Το μέγεθος που στέλνει πίσω είναι 29322 bytes και ο τύπος του είναι text/html με encoding UTF-8.

Content-Length: 7290\r\n

[Content length: 7290]

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/2]

[Time since request: 0.179686000 seconds]

[\[Request in frame: 102\]](#)

[\[Next request in frame: 229\]](#)

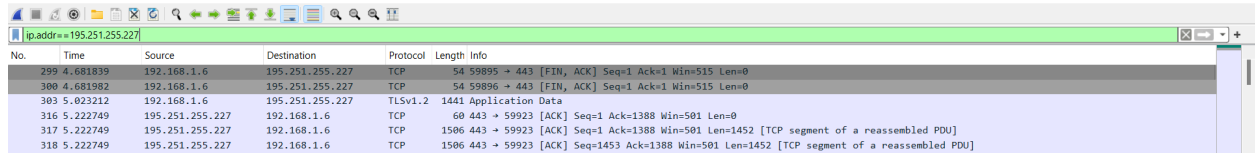
[\[Next response in frame: 297\]](#)

[Request URI: http://ccslab.aueb.gr/]

Content-encoded entity body (gzip): 7290 bytes -> 29322 bytes

File Data: 29322 bytes

13. Ποιο είναι το πρώτο frame που ανταλλάσσεται μεταξύ του υπολογιστή σας και του server που φιλοξενεί το eclass.aueb.gr; Ποια η λειτουργία του frame αυτού;



No.	Time	Source	Destination	Protocol	Length	Info
299	4.681839	192.168.1.6	195.251.255.227	TCP	54	59895 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
300	4.681992	192.168.1.6	195.251.255.227	TCP	54	59896 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
303	5.023212	192.168.1.6	195.251.255.227	TLSv1.2	1441	Application Data
316	5.222749	195.251.255.227	192.168.1.6	TCP	60	443 → 59923 [ACK] Seq=1 Ack=1388 Win=501 Len=0
317	5.222749	195.251.255.227	192.168.1.6	TCP	1506	443 → 59923 [ACK] Seq=1 Ack=1388 Win=501 Len=1452 [TCP segment of a reassembled PDU]
318	5.222749	195.251.255.227	192.168.1.6	TCP	1506	443 → 59923 [ACK] Seq=1453 Ack=1388 Win=501 Len=1452 [TCP segment of a reassembled PDU]

Το πρώτο frame που ανταλλάσσεται μεταξύ του υπολογιστή μου και του server που φιλοξενεί το eclass.aueb.gr είναι το παρακάτω

192.168.1.6	195.251.255.227	TCP	54	59895 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
-------------	-----------------	-----	----	--

```
Frame 299: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF
Section number: 1
> Interface id: 0 (\Device\NPF_{2977C6FC-B31B-4B9E-AAC7-C7BCE189A1D4})
Encapsulation type: Ethernet (1)
Arrival Time: Dec 26, 2023 11:50:59.788431000 GTB Standard Time
UTC Arrival Time: Dec 26, 2023 09:50:59.788431000 UTC
Epoch Arrival Time: 1703584259.788431000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.892452000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 4.681839000 seconds]
Frame Number: 299
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
```

Το συγκεκριμένο frame αρχίζει τη διαδικασία κλεισίματος της σύνδεσης. Ο client, δηλαδή εμείς, στέλνει ACK για το τελευταίο πακέτο δεδομένων και FIN για να κλείσει τη σύνδεση με τον server.

```
Flags: 0x011 (FIN, ACK)
```

```
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 .... = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..0. = Syn: Not set
> .... .... ...1 = Fin: Set
```

14. Σε ποιο port δέχεται αιτήματα πελατών ο server για το site `eclass.aueb.gr`;

Ο server δέχεται αιτήματα πελατών στη θύρα 443. Η συγκεκριμένη θύρα είναι η default θύρα για το https πρωτόκολλο.

`Destination Port: 443`

15. Μπορείτε να δείτε το περιεχόμενο των HTTP μηνυμάτων που ανταλλάσσει ο υπολογιστής σας με τον web server που φιλοξενεί το `eclass.aueb.gr`; Εξηγήστε την απάντησή σας.

Όχι, δεν μπορούμε να δούμε το περιεχόμενο των HTTP μηνυμάτων που ανταλλάσσει ο υπολογιστής σας με τον web server που φιλοξενεί το `eclass.aueb.gr`. Τα δεδομένα προστατεύονται από το πρωτόκολλο TLSv1.2 και όπως φαίνεται παρακάτω είναι encrypted. Επίσης, βλέπουμε και τη διαφορά μεταξύ του πως φαίνονται τα μηνύματα με τον server που φιλοξενεί το `ccslab.aueb.gr` και το `eclass.aueb.gr` αντίστοιχα με τη μόνη διαφορά να είναι η ύπαρξη του πρωτοκόλλου TLSv1.2.

Line-based text data: text/html (278 lines)

```
<!DOCTYPE html>\n
<!--[if IE 7]>\n
<html class="ie ie7" lang="en-US">\n
<![endif]-->\n
<!--[if IE 8]>\n
<html class="ie ie8" lang="en-US">\n
<![endif]-->\n
<!--[if !(IE 7) | !(IE 8) ]><!-->\n
<html lang="en-US">\n
<!--<![endif]-->\n
<head>\n
<meta charset="UTF-8" />\n
<meta http-equiv="X-UA-Compatible" content="IE=edge">\n
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0">\n
<link rel="profile" href="http://gmpg.org/xfn/11" />\n
<link rel="pingback" href="http://ccslab.aueb.gr/xmlrpc.php" />\n
<title>ccslab.aueb.gr &#8211; Ιστότοπος Εργαστηρίου Υπολογιστών και Επικοινωνιών</title>\n
<meta name='robots' content='max-image-preview:large' />\n
<link rel="alternate" type="application/rss+xml" title="ccslab.aueb.gr &raquo; Feed" href="f
<link rel="alternate" type="application/rss+xml" title="ccslab.aueb.gr &raquo; Comments Feec
<script type="text/javascript">\n
[truncated>window._wpemojiSettings = {"baseUrl":"https://s.w.org/images/core/emoji/14
```

Transport Layer Security

```
✓ TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
  Content Type: Application Data (23)
  Version: TLS 1.2 (0x0303)
  Length: 16408
  Encrypted Application Data [truncated]: 9f0758f7745e33bb2fab0b2fb9c50da31e15a84
  [Application Data Protocol: Hypertext Transfer Protocol]
```

16. Ποια έκδοση του Transport Layer Security πρωτοκόλλου χρησιμοποιούν στη μεταξύ τους επικοινωνία ο υπολογιστής σας με το `ccslab.aueb.gr`;

Χρησιμοποιούν την έκδοση 1.2 του TLS.

Version: TLS 1.2 (0x0303)