



## ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

### Εργασία WhireShark - Χειμερινό Εξάμηνο 2023-24

Ονοματεπώνυμο:

Μαρία Σχοινάκη

Αριθμός Μητρώου:

3210191

Email:

p3210191@aueb.gr

## Άσκηση 1 – ICMP

**1)** Η χρονική διάρκεια της ανίχνευσης είναι **62.298730 seconds**. Αυτό, μπορούμε να το συμπεράνουμε με πολλούς τρόπους. Ένας από αυτούς είναι, στο menu **statistics**, να επιλέξουμε το option, "**Capture File Properties**" και να ελέγξουμε το πεδίο **Elapsed** στο **Time**. Ένας πιο ακριβής τρόπος, είναι να ελέγξουμε στις λεπτομέρειες του **τελευταίου** πακέτου που στάλθηκε, στο header "**Frame**", το πεδίο **Time since reference or first frame**.

```
Wireshark - Packet 343 - Wi-Fi
▼ Frame 343: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
  Section number: 1
  > Interface id: 0 (\Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90})
  Encapsulation type: Ethernet (1)
  Arrival Time: Jan 16, 2024 20:06:03.864054000 Χειμερινή ώρα GTB
  UTC Arrival Time: Jan 16, 2024 18:06:03.864054000 UTC
  Epoch Arrival Time: 1705428363.864054000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.045855000 seconds]
  [Time delta from previous displayed frame: 0.045855000 seconds]
  [Time since reference or first frame: 62.298730000 seconds]
```

2)

PROTOCOL	LAYER
IPv6	ΔΙΚΤΥΟΥ
IPv4	ΔΙΚΤΥΟΥ
UDP	ΜΕΤΑΦΟΡΑΣ
TCP	ΜΕΤΑΦΟΡΑΣ
LLMNR	ΕΦΑΡΜΟΓΗΣ
SSDP	ΕΦΑΡΜΟΓΗΣ
QUIC	ΕΦΑΡΜΟΓΗΣ
NBNS	ΕΦΑΡΜΟΓΗΣ
DNS	ΕΦΑΡΜΟΓΗΣ
TLS	ΕΦΑΡΜΟΓΗΣ
HTTP	ΕΦΑΡΜΟΓΗΣ
ICMP	ΔΙΚΤΥΟΥ
ARP	ΔΙΚΤΥΟΥ

Wireshark · Protocol Hierarchy Statistics · Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
▼ Frame	100.0	343	100.0	88951	11 k	0	0	0	343
▼ Ethernet	100.0	343	5.4	4802	616	0	0	0	343
▼ Internet Protocol Version 6	0.6	2	0.1	80	10	0	0	0	2
▼ User Datagram Protocol	0.6	2	0.0	16	2	0	0	0	2
Link-local Multicast Name Resolution	0.6	2	0.1	84	10	2	84	10	2
▼ Internet Protocol Version 4	98.3	337	7.6	6740	865	0	0	0	337
▼ User Datagram Protocol	40.2	138	1.2	1104	141	0	0	0	138
Simple Service Discovery Protocol	19.2	66	32.5	28914	3712	66	28914	3712	66
QUIC IETF	3.8	13	11.1	9830	1262	13	8803	1130	15
NetBIOS Name Service	7.3	25	2.0	1752	224	25	1752	224	25
Link-local Multicast Name Resolution	0.6	2	0.1	84	10	2	84	10	2
Domain Name System	9.3	32	2.5	2217	284	32	2217	284	32
▼ Transmission Control Protocol	39.7	136	33.1	29487	3786	102	15487	1988	136
Transport Layer Security	8.7	30	31.9	28380	3644	30	28380	3644	30
Hypertext Transfer Protocol	0.6	2	0.6	538	69	2	538	69	2
Data	0.6	2	0.0	2	0	2	2	0	2
Internet Control Message Protocol	18.4	63	4.4	3876	497	63	3876	497	63
Address Resolution Protocol	1.2	4	0.1	112	14	4	112	14	4

3) Το πρωτόκολλο εφαρμογής **SSDP**, χρησιμοποιεί το πρωτόκολλο μεταφοράς **UDP**

Το πρωτόκολλο εφαρμογής **QUIC**, χρησιμοποιεί το πρωτόκολλο μεταφοράς **UDP**

Το πρωτόκολλο εφαρμογής **NBNS**, χρησιμοποιεί το πρωτόκολλο μεταφοράς **UDP**

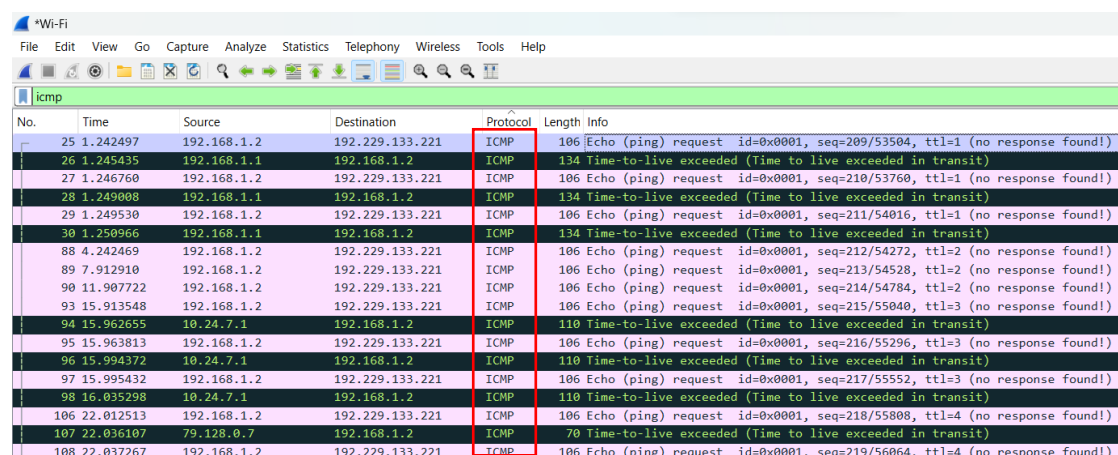
Το πρωτόκολλο εφαρμογής **LLMNR**, χρησιμοποιεί το πρωτόκολλο μεταφοράς **UDP**

Το πρωτόκολλο εφαρμογής **DNS**, χρησιμοποιεί το πρωτόκολλο μεταφοράς **UDP**

Το πρωτόκολλο εφαρμογής **TLS**, χρησιμοποιεί το πρωτόκολλο μεταφοράς **TCP**

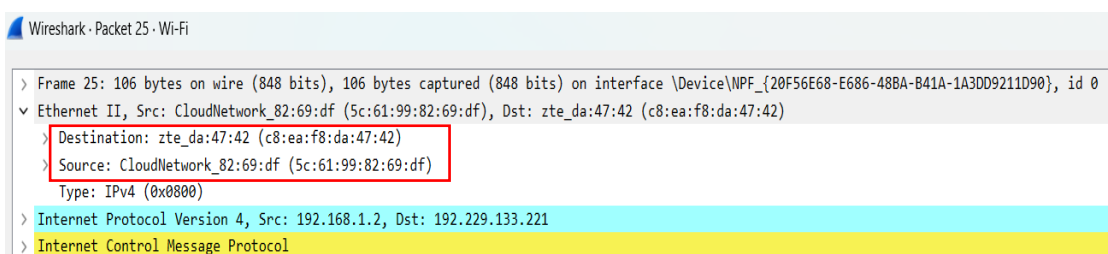
Το πρωτόκολλο εφαρμογής **HTTP**, χρησιμοποιεί το πρωτόκολλο μεταφοράς **TCP**

**4)** Για να εμφανίζονται στο παράθυρο του wireshark μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP, χρησιμοποιούμε το φίλτρο, **icmp**.



No.	Time	Source	Destination	Protocol	Length	Info
25	1.242497	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=209/53504, ttl=1 (no response found!)
26	1.245435	192.168.1.1	192.168.1.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
27	1.246760	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=210/53760, ttl=1 (no response found!)
28	1.249008	192.168.1.1	192.168.1.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
29	1.249530	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=211/54016, ttl=1 (no response found!)
30	1.250966	192.168.1.1	192.168.1.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
88	4.242469	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=212/54272, ttl=2 (no response found!)
89	7.912910	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=213/54528, ttl=2 (no response found!)
90	11.907722	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=214/54784, ttl=2 (no response found!)
93	15.913548	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=215/55040, ttl=3 (no response found!)
94	15.962655	10.24.7.1	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
95	15.963813	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=216/55296, ttl=3 (no response found!)
96	15.994372	10.24.7.1	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
97	15.995432	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=217/55552, ttl=3 (no response found!)
98	16.035298	10.24.7.1	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
106	22.012513	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=218/55808, ttl=4 (no response found!)
107	22.036107	79.128.0.7	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
108	22.037267	192.168.1.2	192.229.133.221	ICMP	106	Echo (ping) request id=0x0001, seq=219/56064, ttl=4 (no response found!)

**5)α)** Οι συσκευές που επικοινωνούν σε επίπεδο **Ethernet** είναι: **CloudNetwork\_82:69:df** , με Mac address (5c:61:99:82:69:df) (*source*) και **zte\_da:47:42** με Mac address: (c8:ea:f8:da:47:42) (*destination*)



Wireshark - Packet 25 - Wi-Fi	
> Frame 25: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0	
v Ethernet II, Src: CloudNetwork_82:69:df (5c:61:99:82:69:df), Dst: zte_da:47:42 (c8:ea:f8:da:47:42)	
Destination: zte_da:47:42 (c8:ea:f8:da:47:42) Source: CloudNetwork_82:69:df (5c:61:99:82:69:df) Type: IPv4 (0x0800)	
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.229.133.221	
> Internet Control Message Protocol	

**b)** Η IP διεύθυνση του υπολογιστή μου είναι η, **192.168.1.2**. Αυτό, μπορούμε να το επιβεβαιώσουμε βλέποντας στο header "**Internet Protocol Version 4**", το πεδίο **Source Address**, καθώς το πρώτο **ICMP Echo request** πακέτο, γίνεται από τον υπολογιστή μου.

The screenshot shows a Wireshark packet capture of an ICMP Echo request. The packet list on the left shows 'Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.229.133.221'. The packet details pane on the right shows the 'Internet Protocol Version 4' header with 'Source Address: 192.168.1.2' highlighted in a red box. Below it, the 'Internet Control Message Protocol' section is highlighted in yellow.

```

Wireshark - Packet 25 - Wi-Fi
> Frame 25: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: CloudNetwork_82:69:df (5c:61:99:82:69:df), Dst: zte_da:47:42 (c8:ea:f8:da:47:42)
> Internet Protocol Version 4, Src: 192.168.1.2, 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: 0x4f24 (20260)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x6210 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.2
  Destination Address: 192.229.133.221
> Internet Control Message Protocol
  
```

**c)** Η IP διεύθυνση του destination είναι η, **192.229.133.221**. Αυτό, μπορούμε να το επιβεβαιώσουμε βλέποντας στο header "**Internet Protocol Version 4**", το πεδίο **Destination Address**, στο πρώτο **ICMP Echo request** πακέτο.

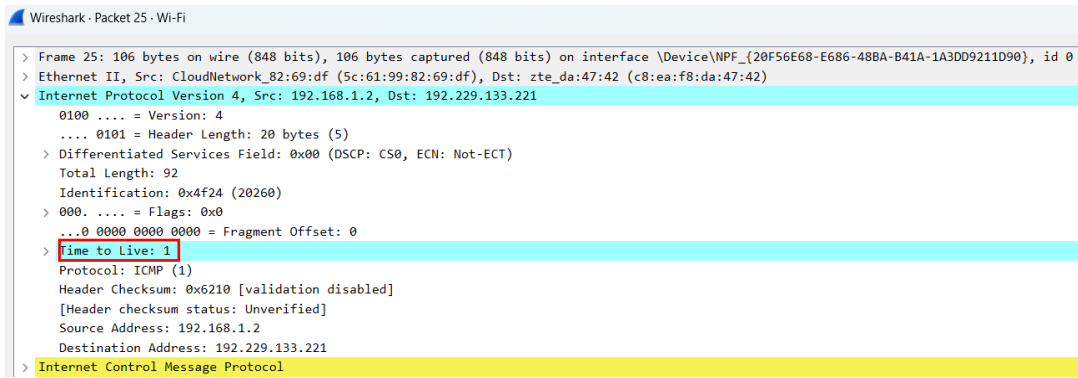
The screenshot shows a Wireshark packet capture of an ICMP Echo request. The packet list on the left shows 'Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.229.133.221'. The packet details pane on the right shows the 'Internet Protocol Version 4' header with 'Destination Address: 192.229.133.221' highlighted in a red box. Below it, the 'Internet Control Message Protocol' section is highlighted in yellow.

```

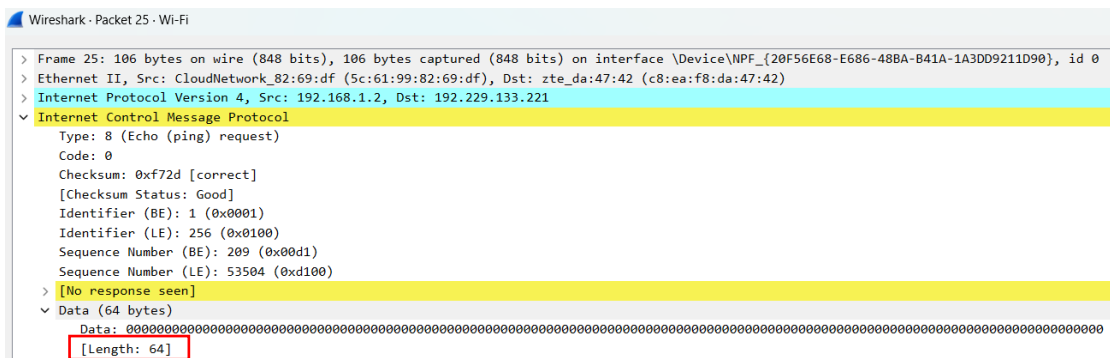
Wireshark - Packet 25 - Wi-Fi
> Frame 25: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: CloudNetwork_82:69:df (5c:61:99:82:69:df), Dst: zte_da:47:42 (c8:ea:f8:da:47:42)
> Internet Protocol Version 4, Src: 192.168.1.2, 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: 0x4f24 (20260)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x6210 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.2
  Destination Address: 192.229.133.221
> Internet Control Message Protocol
  
```

**d)** Το **time-to-live** του πρώτου **ICMP Echo request** πακέτου είναι, **1**. Αυτό, μπορούμε να το επιβεβαιώσουμε βλέποντας στο header "**Internet Protocol Version 4**", το πεδίο **Time To Live**, στο πρώτο **ICMP Echo request** πακέτο.

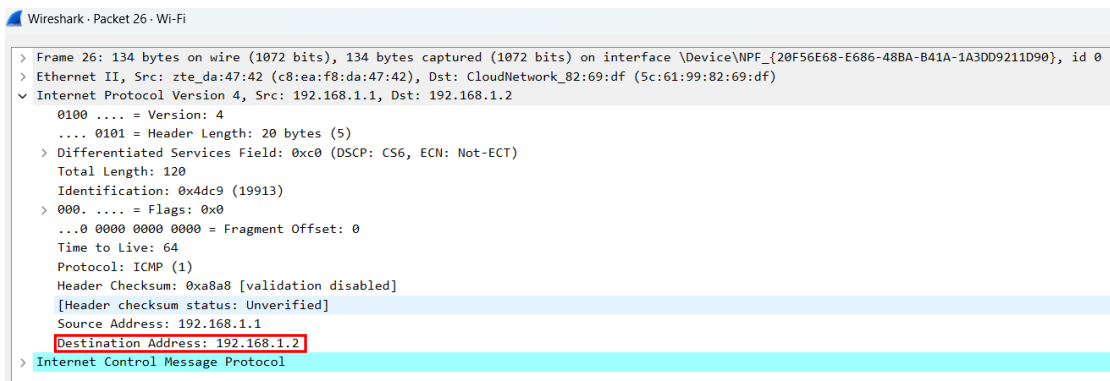
## Εργασία WireShark



**e)** Το μέγεθος των δεδομένων που μεταφέρει το πρώτο **ICMP Echo request** πακέτο, είναι **64 bytes**. Αυτό, μπορούμε να το επιβεβαιώσουμε βλέποντας στο header "**Internet Control Message Protocol**", το πεδίο **Data(Length)**, στο πρώτο **ICMP Echo request** πακέτο.



**6)α)** Η IP διεύθυνση του **destination** στο πακέτο που μεταφέρει το πρώτο **ICMP Time Exceeded**, είναι η, **192.168.1.2** (ο υπολογιστής μου). Αυτό, μπορούμε να το επιβεβαιώσουμε βλέποντας στο header "**Internet Protocol Version 4**", το πεδίο **Destination Address**, στο πρώτο **ICMP Time Exceeded** πακέτο.



**b)** Η IP διεύθυνση του **source** στο πακέτο που μεταφέρει το πρώτο **ICMP Time Exceeded**, είναι η, **192.168.1.1** (το *router μου*). Αυτό, μπορούμε να το επιβεβαιώσουμε βλέποντας στο header "**Internet Protocol Version 4**", το πεδίο **Source Address**, στο πρώτο **ICMP Time Exceeded** πακέτο.

```

Wireshark · Packet 26 · Wi-Fi
> Frame 26: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: zte_da:47:42 (c8:ea:f8:da:47:42), Dst: CloudNetwork_82:69:df (5c:61:99:82:69:df)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 120
  Identification: 0x4dc9 (19913)
  > 0000 .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0xa8a8 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.1
  Destination Address: 192.168.1.2
> Internet Control Message Protocol
  
```

**7)** Οι IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα φαίνονται παρακάτω:

192.168.1.1
10.24.7.1
79.128.0.7
79.128.0.2
79.128.249.50
62.75.3.9
62.75.27.69
62.75.27.94
152.195.100.131

No.	Time	Source	Destination	Protocol	Length	Info
26	1.245435	192.168.1.1	192.168.1.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
28	1.249008	192.168.1.1	192.168.1.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
30	1.250966	192.168.1.1	192.168.1.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
94	15.962655	10.24.7.1	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
96	15.994372	10.24.7.1	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
98	16.035298	10.24.7.1	192.168.1.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
107	22.036107	79.128.0.7	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
109	22.055776	79.128.0.7	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
111	22.086094	79.128.0.7	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
122	28.076479	79.128.0.2	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
124	28.096704	79.128.0.2	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
126	28.126387	79.128.0.2	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
213	34.116731	79.128.249.50	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
215	34.138058	79.128.249.50	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
217	34.154079	79.128.249.50	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
230	40.157115	62.75.3.9	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
232	40.174224	62.75.3.9	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
234	40.201081	62.75.3.9	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
238	41.291342	62.75.27.69	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
240	41.348004	62.75.27.69	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
242	41.412720	62.75.27.69	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
253	47.430129	62.75.27.94	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
255	47.489385	62.75.27.94	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
257	47.548902	62.75.27.94	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
268	53.577178	152.195.100.131	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
270	53.643472	152.195.100.131	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
272	53.700568	152.195.100.131	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

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

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

  1    3 ms    2 ms    1 ms    CPE [192.168.1.1]
  2    *      *      *      Request timed out.
  3   49 ms   30 ms   40 ms   10.24.7.1
  4   23 ms   18 ms   29 ms   79.128.0.7
  5   24 ms   19 ms   27 ms   79.128.0.2
  6   29 ms   19 ms   15 ms   79.128.249.50
  7   26 ms   16 ms   25 ms   kolasr01-hu-0-0-0-0.ath.OTEGlobe.gr [62.75.3.9]
  8   58 ms   55 ms   64 ms   62.75.27.69
  9   60 ms   58 ms   58 ms   62.75.27.94
 10   65 ms   65 ms   56 ms   ae-65.core1.frb.edgecastcdn.net [152.195.100.131]
 11   69 ms   49 ms   47 ms   192.229.133.221

Trace complete.
```

Όλες οι Source IP που εμφανίζονται στα πακέτα που μεταφέρουν ICMP Time Exceeded μηνύματα, εμφανίζονται και στο cmd window.

## Άσκηση 2 – DNS & HTTP

1) Στάλθηκαν συνολικά **1456** πακέτα **TCP** και συνολικά **578** πακέτα **UDP**. Αυτό φαίνεται βλέποντας το **Protocol Hierarchy** option από το menu **Statistics**.

Wireshark - Protocol Hierarchy Statistics - Wi-Fi									
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
Frame	100.0	2034	100.0	1026511	343 k	0	0	0	2034
Ethernet	100.0	2034	2.8	28476	9542	0	0	0	2034
Internet Protocol Version 4	100.0	2034	4.0	40680	13 k	0	0	0	2034
User Datagram Protocol	28.4	578	0.5	4624	1549	0	0	0	578
Simple Service Discovery Protocol	1.4	28	1.1	11327	3795	28	11327	3795	28
Real-time Transport Control Protocol	1.6	33	0.1	1012	339	32	960	321	34
Malformed Packet	0.0	1	0.0	0	0	1	0	0	1
QUIC IETF	16.0	326	20.8	213205	71 k	326	208255	69 k	336
Domain Name System	2.1	42	0.2	2341	784	42	2341	784	42
Data	7.3	149	2.5	26115	8750	149	26115	8750	149
Transmission Control Protocol	71.6	1456	68.1	698723	234 k	1124	496621	166 k	1456
Transport Layer Security	9.8	199	30.4	311571	104 k	199	302119	101 k	206
Hypertext Transfer Protocol	6.5	132	34.9	358442	120 k	44	52987	17 k	132
Media Type	0.7	14	46.5	477284	159 k	14	477284	159 k	14
Line-based text data	0.8	16	52.8	541768	181 k	16	541768	181 k	16
JPEG File Interchange Format	0.0	1	2.8	28590	9580	1	28590	9580	1
eXtensible Markup Language	2.7	55	2.5	25888	8674	55	25888	8674	55
Data	0.1	3	0.2	1939	649	3	1939	649	3

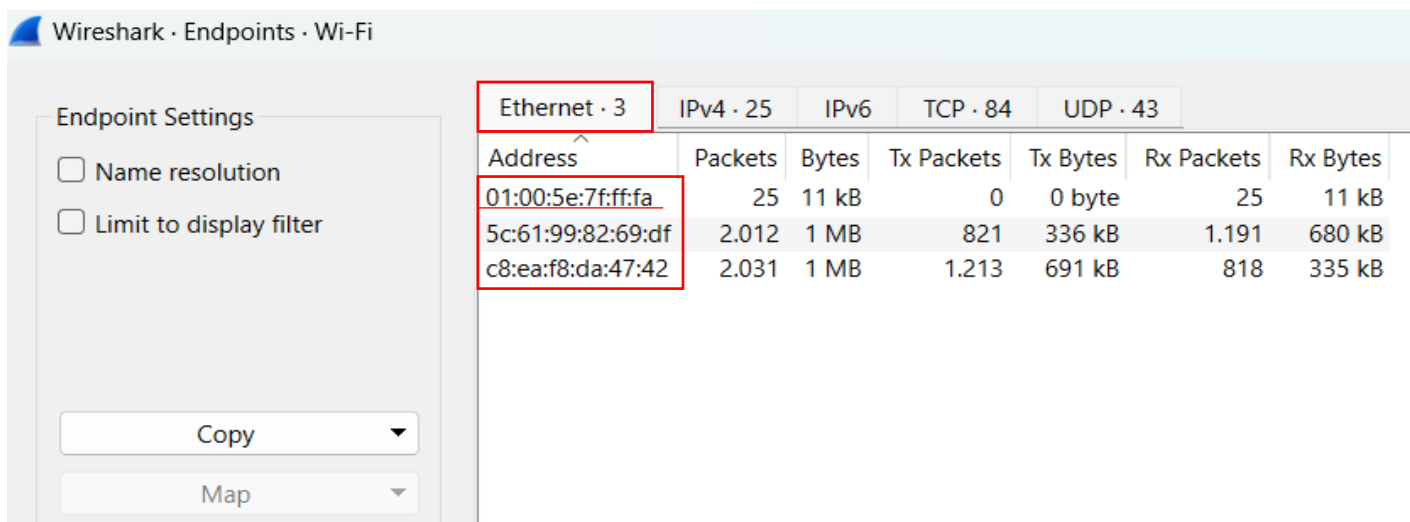


**2)** Τα διαφορετικά **endpoints** με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet είναι **3**. Αυτό, μπορούμε να το διαπιστώσουμε, βλέποντας το **endpoints** option από το menu **Statistics**. Τα διαφορετικά **endpoints** παρουσιάζονται παρακάτω:

"01:00:5e:7f:ff:fa"

"5c:61:99:82:69:df"

"c8:ea:f8:da:47:42"



Wireshark · Endpoints · Wi-Fi						
Endpoint Settings						
<input type="checkbox"/> Name resolution						
<input type="checkbox"/> Limit to display filter						
<div>Copy</div> <div>Map</div>						
Ethernet · 3						
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:7f:ff:fa	25	11 kB	0	0 byte	25	11 kB
5c:61:99:82:69:df	2.012	1 MB	821	336 kB	1.191	680 kB
c8:ea:f8:da:47:42	2.031	1 MB	1.213	691 kB	818	335 kB

Δεν υπάρχει κάποιος άμεσος τρόπος να αντιστοιχίσουμε τις μας αυτές διευθύνσεις με μία συσκευή. Όμως, μπορούμε να υποθέσουμε σε τι συσκευή μπορεί να ανήκουν, βάση του ονόματος που τους προσδίδει το **wireshark** και φυσικά, τι συσκευές αναμένουμε να δούμε εφόσον, κοιτάμε το **Ethernet** επίπεδο. Αναμένουμε συσκευές όπως κάρτες δικτύου(ο υπολογιστής μου), routers, switches κτλπ, συσκευές δηλαδή που συμμετέχουν στην ανταλλαγή δεδομένων σε ένα τοπικό δίκτυο. Έτσι, η διεύθυνση "**5c:61:99:82:69:df**" αντιστοιχεί πιθανότατα στον **υπολογιστή** μου, η διεύθυνση "**c8:ea:f8:da:47:42**" αντιστοιχεί στο **router** μου και η διεύθυνση "**01:00:5e:7f:ff:fa**" πιθανότατα αντιστοιχεί σε **multicast traffic** το οποίο χρησιμοποιείται από το πρωτόκολλο **SSDP**.



## Εργασία Wireshark

Wireshark · Endpoints · Wi-Fi

Endpoint Settings

- ☒ Name resolution
- ☐ Limit to display filter

Copy

Map

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
CloudNetwork_82:69:df	2.012	1 MB	821	336 kB	1.191	680 kB
IPv4mcast_7f:ff:fa	25	11 kB	0	0 byte	25	11 kB
zte_da:47:42	2.031	1 MB	1.213	691 kB	818	335 kB

3) Τα διαφορετικά **endpoints** με τα οποία υπάρχει επικοινωνία σε επίπεδο **IP** είναι **25**.

Wireshark · Endpoints · Wi-Fi

Endpoint Settings

- ☐ Name resolution
- ☐ Limit to display filter

Copy

Map

Protocol

- ☐ Bluetooth
- ☐ BPV7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ JXTA

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
20.250.77.142	2	109 byte	1	54 byte	1	55 byte						
34.104.35.123	17	6 kB	9	4 kB	8	2 kB						
34.155.84.81	33	8 kB	19	6 kB	14	2 kB						
52.111.231.17	2	143 byte	1	54 byte	1	89 byte						
64.233.167.188	2	121 byte	1	66 byte	1	55 byte						
66.22.243.36	167	29 kB	153	28 kB	14	1 kB						
83.212.207.19	465	356 kB	296	280 kB	169	76 kB						
142.250.181.227	94	76 kB	68	73 kB	26	3 kB						
142.250.181.238	54	23 kB	30	17 kB	24	6 kB						
142.250.185.74	43	18 kB	24	14 kB	19	4 kB						
142.250.185.99	240	172 kB	93	19 kB	147	152 kB						
142.250.185.132	15	10 kB	7	7 kB	8	3 kB						
142.250.185.163	49	22 kB	27	10 kB	22	11 kB						
142.250.185.202	54	20 kB	31	16 kB	23	3 kB						
142.250.186.78	96	44 kB	54	22 kB	42	22 kB						
142.250.187.195	7	8 kB	4	5 kB	3	3 kB						
142.251.168.188	2	109 byte	1	54 byte	1	55 byte						
162.159.129.235	4	334 byte	2	165 byte	2	169 byte						
162.159.136.234	6	913 byte	3	751 byte	3	162 byte						
172.217.18.99	47	19 kB	25	14 kB	22	5 kB						
192.168.1.1	460	79 kB	248	49 kB	212	30 kB						
192.168.1.2	2.012	1 MB	821	336 kB	1.191	680 kB						
195.251.255.227	166	135 kB	113	125 kB	53	10 kB						
208.115.231.114	6	327 byte	3	162 byte	3	165 byte						
239.255.255.250	25	11 kB	0	0 byte	25	11 kB						

Τα **IP endpoints** **δεν** ταυτίζονται με τα **Ethernet endpoints**. Τα **IP endpoints** αναφέρονται σε συσκευές σε ένα δίκτυο που είναι αναγνωρίσιμες με μια διεύθυνση **IP**. Τα endpoints σε επίπεδο **Ethernet** αναφέρονται σε συσκευές που επικοινωνούν μεταξύ τους μέσω της φυσικής σύνδεσης **Ethernet**. Η διεύθυνση **IP** είναι μια **32 bits (IPv4) λογική διεύθυνση** που χρησιμοποιείται στο επίπεδο δικτύου (*Layer 3*), ενώ η διεύθυνση **Ethernet** είναι μια **12 ψηφία (XX:XX:XX:XX:XX:XX, όπου κάθε "X" αναπαριστά ένα δεκαεξαδικό ψηφίο (0-9 ή A-F)) φυσική**

## διεύθυνση που χρησιμοποιείται στο επίπεδο σύνδεσης δεδομένων (Layer 2).

Συνήθως, υπάρχει μια αντιστοιχία μεταξύ των διευθύνσεων IP και των διευθύνσεων MAC, αλλά δεν είναι πάντα ένα προς ένα, καθώς υπάρχουν διάφοροι τρόποι να γίνεται η αντιστοίχιση, όπως με τη χρήση του πρωτοκόλλου ARP.

4)

No.	Time	Source	Destination	Protocol	Length	Info
173	7.527551	192.168.1.2	192.168.1.1	DNS	74	Standard query 0x3ef7 A ccslab.aueb.gr
174	7.527791	192.168.1.2	192.168.1.1	DNS	74	Standard query 0x4423 HTTPS ccslab.aueb.gr
183	7.567483	192.168.1.1	192.168.1.2	DNS	90	Standard query response 0x3ef7 A ccslab.aueb.gr A 83.212.207.19
187	7.573461	192.168.1.2	192.168.1.1	DNS	74	Standard query 0x62c3 A ccslab.aueb.gr
188	7.573630	192.168.1.2	192.168.1.1	DNS	74	Standard query 0x65b5 HTTPS ccslab.aueb.gr
189	7.610298	192.168.1.1	192.168.1.2	DNS	90	Standard query response 0x62c3 A ccslab.aueb.gr A 83.212.207.19
202	7.615449	192.168.1.1	192.168.1.2	DNS	125	Standard query response 0x4423 HTTPS ccslab.aueb.gr SOA hermes.aueb.gr
203	7.615449	192.168.1.1	192.168.1.2	DNS	125	Standard query response 0x65b5 HTTPS ccslab.aueb.gr SOA hermes.aueb.gr
340	8.004696	192.168.1.2	192.168.1.1	DNS	77	Standard query 0xfe79 A fonts.gstatic.com
341	8.004902	192.168.1.2	192.168.1.1	DNS	77	Standard query 0x934e HTTPS fonts.gstatic.com
343	8.025897	192.168.1.1	192.168.1.2	DNS	93	Standard query response 0xfe79 A fonts.gstatic.com A 142.250.181.227
369	8.073599	192.168.1.1	192.168.1.2	DNS	134	Standard query response 0x934e HTTPS fonts.gstatic.com SOA ns1.google.com
412	8.252807	192.168.1.2	192.168.1.1	DNS	79	Standard query 0xa517 A clients4.google.com
413	8.253037	192.168.1.2	192.168.1.1	DNS	79	Standard query 0xc9c2 HTTPS clients4.google.com
416	8.272791	192.168.1.1	192.168.1.2	DNS	129	Standard query response 0xa517 A clients4.google.com CNAME clients.l.google.com A 142.250.186.78
425	8.312799	192.168.1.1	192.168.1.2	DNS	153	Standard query response 0xc9c2 HTTPS clients4.google.com CNAME clients.l.google.com SOA ns1.google.com
537	8.595740	192.168.1.2	192.168.1.1	DNS	80	Standard query 0xb52d A fonts.googleapis.com
538	8.595971	192.168.1.2	192.168.1.1	DNS	80	Standard query 0x2f8 HTTPS fonts.googleapis.com

Για την ερώτηση από τον υπολογιστή μου προς τον DNS server χρησιμοποιήθηκαν, η θύρα προέλευσης (source) 50208 και θύρα προορισμού (destination) 53. Η θύρα προέλευσης (source) 50208, αντιστοιχεί σε κάποια θύρα από τις διαθέσιμες του υπολογιστή μου, ενώ η θύρα προορισμού (destination) 53, αντιστοιχεί στο πρωτόκολλο DNS.

Wireshark · Packet 173 · Wi-Fi

- > Frame 173: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
- > Ethernet II, Src: CloudNetwork\_82:69:df (5c:61:99:82:69:df), Dst: zte\_da:47:42 (c8:ea:f8:da:47:42)
- > Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
- > User Datagram Protocol, Src Port: 50208, Dst Port: 53
  - Source Port: 50208
  - Destination Port: 53
  - Length: 40
  - Checksum: 0x047f [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 4]
  - > [Timestamps]
  - UDP payload (32 bytes)
- > Domain Name System (query)

Για την απάντηση από τον **DNS server**, προς τον υπολογιστή μου χρησιμοποιήθηκαν, η θύρα προέλευσης (**source**) **53** και η θύρα προορισμού (**destination**) **50208**. Η θύρα προέλευσης (**source**) **53**, αντιστοιχεί στο πρωτόκολλο **DNS**, ενώ η θύρα προορισμού (**destination**) **50208**, αντιστοιχεί σε κάποια θύρα από τις διαθέσιμες του υπολογιστή μου.

```
Wireshark · Packet 183 · Wi-Fi
> Frame 183: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: zte_da:47:42 (c8:ea:f8:da:47:42), Dst: CloudNetwork_82:69:df (5c:61:99:82:69:df)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
> User Datagram Protocol, Src Port: 53, Dst Port: 50208
  Source Port: 53
  Destination Port: 50208
  Length: 56
  Checksum: 0x9369 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
> [Timestamps]
  UDP payload (48 bytes)
> Domain Name System (response)
```

**5)** Για να καταλάβουμε αν ένα πακέτο περιέχει αίτημα προς τον **DNS server** ή απάντηση σε ένα ερώτημα που έχει γίνει, κοιτάμε στο header **DNS** του πακέτου. Αν το πακέτο είναι ερώτημα, το πεδίο **queries** είναι γεμάτο και μάλιστα με τις πληροφορίες της ερώτησης. Αν πρόκειται για απάντηση, είναι γεμάτο και το πεδίο **queries**, καθώς και το πεδίο **answers**, με τις πληροφορίες της απάντησης.

```
Wireshark · Packet 173 · Wi-Fi
> Frame 173: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: CloudNetwork_82:69:df (5c:61:99:82:69:df), Dst: zte_da:47:42 (c8:ea:f8:da:47:42)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 50208, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x3ef7
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > ccslab.aueb.gr: type A, class IN
    [Response In: 183]
```

## Εργασία WireShark

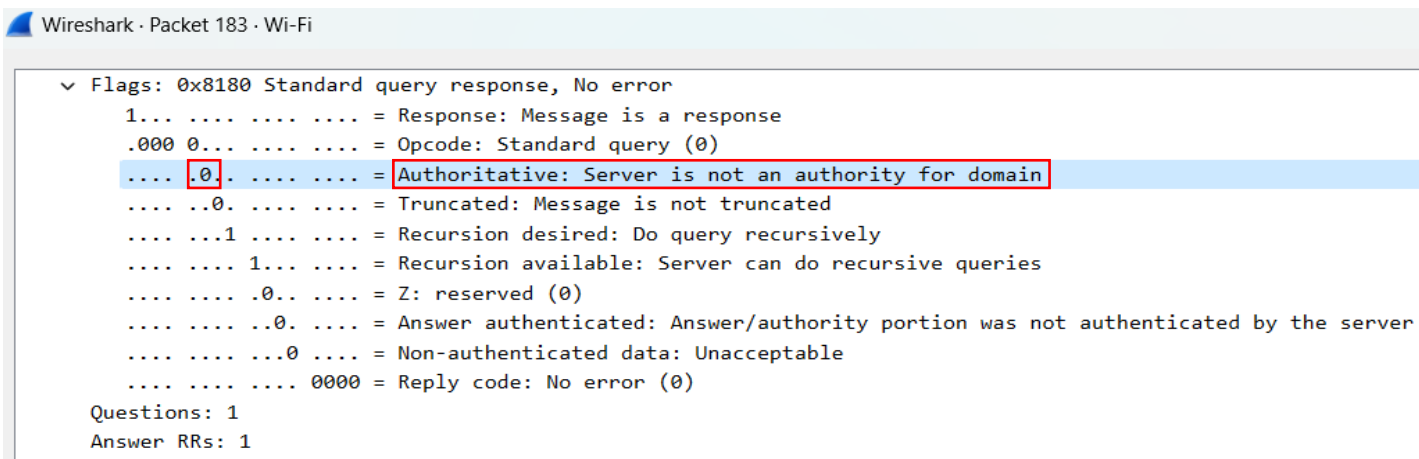
```
Wireshark · Packet 183 · Wi-Fi
> Frame 183: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: zte_da:47:42 (c8:ea:f8:da:47:42), Dst: CloudNetwork_82:69:df (5c:61:99:82:69:df)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
> User Datagram Protocol, Src Port: 53, Dst Port: 50208
▼ Domain Name System (response)
  Transaction ID: 0x3ef7
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > Answers
    [Request In: 173]
    [Time: 0.039932000 seconds]
```

Το πακέτο μιας απάντησης με το πακέτο μιας ερώτησης, συνδέονται μέσω του **αναγνωριστικού ID**, που βρίσκεται μέσα στην επικεφαλίδα **DNS**. Το αναγνωριστικό, είναι **κοινό** και στα 2 πακέτα και μάλιστα μοναδικό.

```
Wireshark · Packet 173 · Wi-Fi
> Frame 173: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: CloudNetwork_82:69:df (5c:61:99:82:69:df), Dst: zte_da:47:42 (c8:ea:f8:da:47:42)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 50208, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x3ef7
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ ccslab.aueb.gr: type A, class IN
      Name: ccslab.aueb.gr
      [Name Length: 14]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
    [Response In: 183]
```

```
Wireshark · Packet 183 · Wi-Fi
> Frame 183: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: zte_da:47:42 (c8:ea:f8:da:47:42), Dst: CloudNetwork_82:69:df (5c:61:99:82:69:df)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
> User Datagram Protocol, Src Port: 53, Dst Port: 50208
▼ Domain Name System (response)
  Transaction ID: 0x3ef7
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ ccslab.aueb.gr: type A, class IN
      Name: ccslab.aueb.gr
      [Name Length: 14]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  ▼ 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: 3449 (57 minutes, 29 seconds)
      Data length: 4
      Address: 83.212.207.19
    [Request In: 173]
    [Time: 0.039932000 seconds]
```

**6)** Ναι, υπάρχει σημαία (flag) στα πακέτα **DNS** που προσδιορίζει εάν ο name server που μας απαντάει είναι **authoritative** για το συγκεκριμένο domain. Η σημαία αυτή είναι η "**Authoritative**" flag. Η σημαία βρίσκεται στο πεδίο "**Flags**" της επικεφαλίδας **DNS** στις λεπτομέρειες ενός πακέτου. Όταν η flag έχει την τιμή **1**, αυτό υποδεικνύει ότι ο name server που έστειλε την απάντηση είναι **authoritative**. Όταν έχει την τιμή **0**, δεν είναι **authoritative**. Ο **name server** που έχει απαντήσει **δεν** είναι **authoritative** για το συγκεκριμένο domain, αφού η σημαία έχει τιμή **0**.



```

Wireshark · Packet 183 · Wi-Fi

▼ 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: 1
  
```

**7)** Το όνομα **ccslab.aueb.gr** είναι **κανονικό dns** όνομα. Αυτό μπορούμε να το συμπεράνουμε αν ανοίγοντας ένα πακέτο απάντησης από τον **DNS server** και πηγαίνοντας στην επικεφαλίδα **DNS**, μέσα στο πεδίο **answers**, το όνομα είναι **type A(host address)**. Η **IP** διεύθυνση που του αντιστοιχεί είναι το **address** της επικεφαλίδας **DNS** στο πεδίο **answers** (εφόσον είναι και **dns** όνομα, ειδικά θα μας παρέπεμπε αλλού). Στο συγκεκριμένο ερώτημα είναι η: **"83.212.207.19"**.

## Εργασία WireShark

```
Wireshark · Packet 183 · Wi-Fi
> Frame 183: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: zte_da:47:42 (c8:ea:f8:da:47:42), Dst: CloudNetwork_82:69:df (5c:61:99:82:69:df)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
> User Datagram Protocol, Src Port: 53, Dst Port: 50208
▼ Domain Name System (response)
  Transaction ID: 0x3ef7
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  ▼ Answers
    ▼ cslab.aueb.gr: type A, class IN, addr 83.212.207.19
      Name: cslab.aueb.gr
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 3449 (57 minutes, 29 seconds)
      Data length: 4
      Address: 83.212.207.19
    [Request In: 173]
    [Time: 0.039932000 seconds]
```

8)

No.	Time	Source	Destination	Protocol	Length	Info
198	7.614331	192.168.1.2	83.212.207.19	TCP	66	58987 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
199	7.614481	192.168.1.2	83.212.207.19	TCP	66	58988 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
204	7.615873	192.168.1.2	83.212.207.19	TCP	66	58989 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
206	7.634887	83.212.207.19	192.168.1.2	TCP	66	80 → 58988 [SYN, ACK] Seq=0 Ack=1 Win=22304 Len=0 MSS=1332 WS=16 SACK_PERM
208	7.635047	192.168.1.2	83.212.207.19	TCP	54	58988 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
209	7.635186	83.212.207.19	192.168.1.2	TCP	66	80 → 58987 [SYN, ACK] Seq=0 Ack=1 Win=22304 Len=0 MSS=1332 WS=16 SACK_PERM
210	7.635221	192.168.1.2	83.212.207.19	TCP	54	58987 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
217	7.643321	83.212.207.19	192.168.1.2	TCP	66	443 → 58989 [SYN, ACK] Seq=0 Ack=1 Win=22304 Len=0 MSS=1332 WS=16 SACK_PERM
218	7.643395	192.168.1.2	83.212.207.19	TCP	54	58989 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
219	7.643881	192.168.1.2	83.212.207.19	TLSv1	588	Client Hello (SNI=cslab.aueb.gr)
233	7.667445	83.212.207.19	192.168.1.2	TCP	54	443 → 58989 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
234	7.668353	192.168.1.2	83.212.207.19	TCP	66	58990 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
235	7.669911	83.212.207.19	192.168.1.2	TCP	54	443 → 58989 [RST, ACK] Seq=1 Ack=535 Win=0 Len=0
239	7.686861	83.212.207.19	192.168.1.2	TCP	66	443 → 58990 [SYN, ACK] Seq=0 Ack=1 Win=22304 Len=0 MSS=1332 WS=16 SACK_PERM
240	7.686940	192.168.1.2	83.212.207.19	TCP	54	58990 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
241	7.687347	192.168.1.2	83.212.207.19	TLSv1	620	Client Hello (SNI=cslab.aueb.gr)
258	7.710552	83.212.207.19	192.168.1.2	TCP	54	443 → 58990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
259	7.715243	83.212.207.19	192.168.1.2	TCP	54	443 → 58990 [RST, ACK] Seq=1 Ack=567 Win=0 Len=0

Η χειραψία τριών βημάτων (*Three-Way Handshake*) είναι μια διαδικασία που χρησιμοποιείται στο πρωτόκολλο **TCP** για την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο συστημάτων. Το **1<sup>ο</sup> TCP segment** δεν περιέχει δεδομένα, όμως περιέχει την σημαία **SYN** ενεργοποιημένη, που σημαίνει, ξεκίνημα σύνδεσης και μεταδίδεται από την θύρα **58987** (θύρα του υπολογιστή μου), στην θύρα **80** (θύρα για *HTTP*), με αποστολέα τον υπολογιστή μου και παραλήπτη το *cslab.aueb.gr*. Το **2<sup>ο</sup> segment** από την θύρα **80** (θύρα για *HTTP*), στην θύρα **58987**

(θύρα του υπολογιστή μου) και με αποστολέα τον ccslab.aueb.gr και παραλήπτη τον υπολογιστή μου, περιέχει την απάντηση, με σημαίες **SYN**, **ACK** και **ack=1**, επιβεβαιώνει το **SYN** που έλαβε από τον υπολογιστή μου. Τέλος, το **3<sup>ο</sup> segment** αποτελεί την απάντηση του υπολογιστή μου στο ccslab.aueb.gr, από την θύρα **58987** (θύρα του υπολογιστή μου) στην θύρα **80** (θύρα για **HTTP**), με την σημαία **ACK** ενεργοποιημένη, και **ack=1**, να επιβεβαιώνει το **ACK** που λάβαμε από τον ccslab.aueb.gr στο προηγούμενο **segment**. Τα **segments**, δεν περιέχουν δεδομένα, όμως το **3<sup>ο</sup> segment** έχει **seq=1**, που σημαίνει ότι η **TCP σύνδεση**, ξεκινά με την αποστολή δεδομένων με αριθμό ακολουθίας **1**.

**9) Οι 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 είναι:**

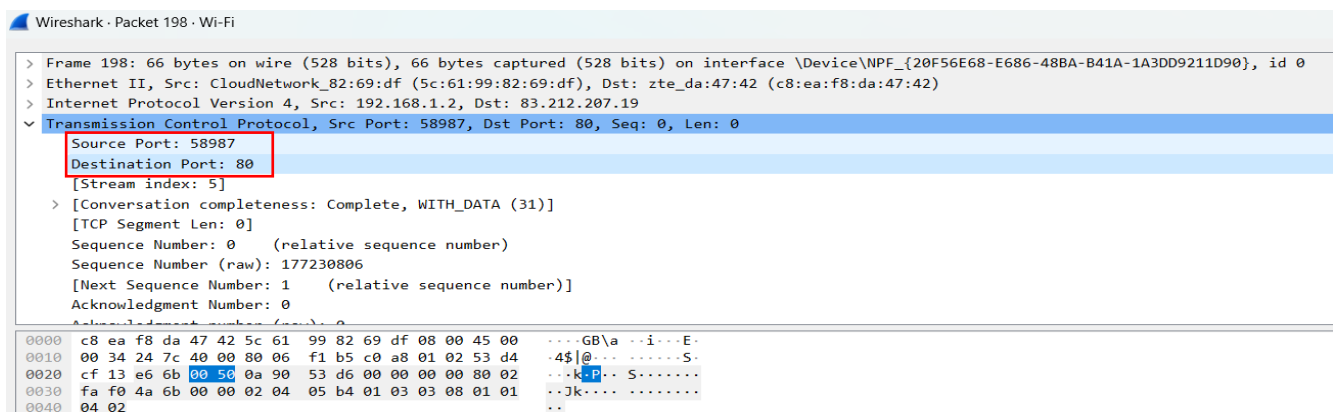
**58987 <-> 80**

**58988 <-> 80**

**58989 <-> 443**

**58990 <-> 443**

Ο υπολογιστής μου (**192.168.1.2**) προσπαθεί να καθιερώσει συνδέσεις με τον **server (83.212.207.19)** σε διάφορες θύρες προορισμού. Η θύρα **80** χρησιμοποιείται για απλή **HTTP** επικοινωνία, ενώ η θύρα **443** χρησιμοποιείται για ασφαλή επικοινωνία (**HTTPS**).



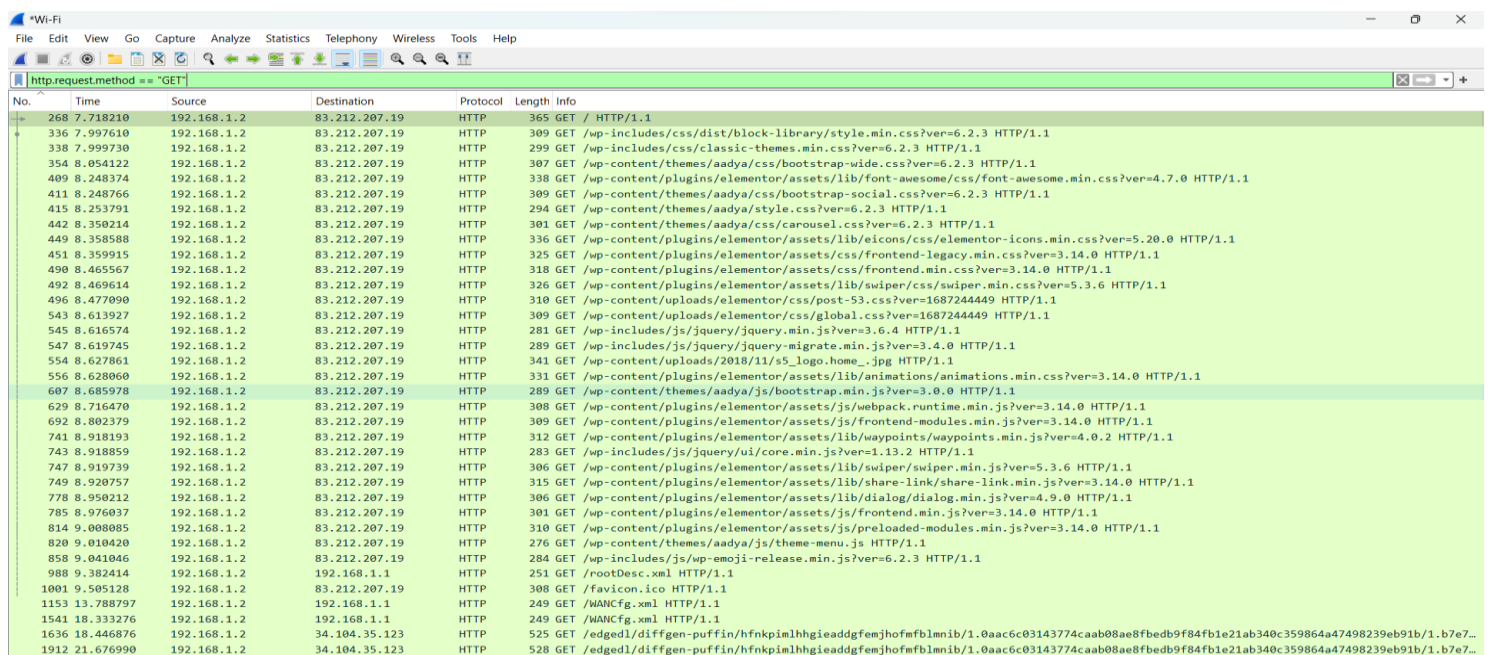


**10)** Ναι, με το φίλτρο "`http.request.method == "GET"`", μπορώ να δω τα πακέτα που περιέχουν **HTTP GET** αίτημα από τον Browser μου προς τον Web Server. Τα πακέτα αυτά, στάλθηκαν προς τις παρακάτω IP διευθύνσεις:

**"83.212.207.19" ccsclab.aueb.gr**

**"192.168.1.1" router**

**"34.104.35.123" edgedl.me.gvt1.com**



No.	Time	Source	Destination	Protocol	Length	Info
268	7.718210	192.168.1.2	83.212.207.19	HTTP	365	GET / HTTP/1.1
336	7.997610	192.168.1.2	83.212.207.19	HTTP	309	GET /wp-includes/css/dist/block-library/style.min.css?ver=6.2.3 HTTP/1.1
338	7.999730	192.168.1.2	83.212.207.19	HTTP	299	GET /wp-includes/css/classic-themes.min.css?ver=6.2.3 HTTP/1.1
354	8.054122	192.168.1.2	83.212.207.19	HTTP	307	GET /wp-content/themes/aadys/css/bootstrap-wide.css?ver=6.2.3 HTTP/1.1
409	8.248374	192.168.1.2	83.212.207.19	HTTP	338	GET /wp-content/plugins/elementor/assets/lib/font-awesome/css/font-awesome.min.css?ver=4.7.0 HTTP/1.1
411	8.248766	192.168.1.2	83.212.207.19	HTTP	309	GET /wp-content/themes/aadys/css/bootstrap-social.css?ver=6.2.3 HTTP/1.1
415	8.253791	192.168.1.2	83.212.207.19	HTTP	294	GET /wp-content/themes/aadys/style.css?ver=6.2.3 HTTP/1.1
442	8.350214	192.168.1.2	83.212.207.19	HTTP	301	GET /wp-content/themes/aadys/css/carousel.css?ver=6.2.3 HTTP/1.1
449	8.358588	192.168.1.2	83.212.207.19	HTTP	336	GET /wp-content/plugins/elementor/assets/lib/eicons/css/elementor-icons.min.css?ver=5.20.0 HTTP/1.1
451	8.359915	192.168.1.2	83.212.207.19	HTTP	325	GET /wp-content/plugins/elementor/assets/css/frontend-legacy.min.css?ver=3.14.0 HTTP/1.1
490	8.465567	192.168.1.2	83.212.207.19	HTTP	318	GET /wp-content/plugins/elementor/assets/css/frontend.min.css?ver=3.14.0 HTTP/1.1
492	8.469614	192.168.1.2	83.212.207.19	HTTP	326	GET /wp-content/plugins/elementor/assets/lib/swiper/css/swiper.min.css?ver=5.3.6 HTTP/1.1
496	8.477090	192.168.1.2	83.212.207.19	HTTP	310	GET /wp-content/uploads/elementor/css/post-53.css?ver=1687244449 HTTP/1.1
543	8.613927	192.168.1.2	83.212.207.19	HTTP	309	GET /wp-content/uploads/elementor/css/global.css?ver=1687244449 HTTP/1.1
545	8.616574	192.168.1.2	83.212.207.19	HTTP	281	GET /wp-includes/js/jquery/jquery.min.js?ver=3.6.4 HTTP/1.1
547	8.619745	192.168.1.2	83.212.207.19	HTTP	289	GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.0 HTTP/1.1
554	8.627861	192.168.1.2	83.212.207.19	HTTP	341	GET /wp-content/uploads/2018/11/s5_logo.home_.jpg HTTP/1.1
556	8.628060	192.168.1.2	83.212.207.19	HTTP	331	GET /wp-content/plugins/elementor/assets/lib/animations/animations.min.css?ver=3.14.0 HTTP/1.1
607	8.685978	192.168.1.2	83.212.207.19	HTTP	289	GET /wp-content/themes/aadys/js/bootstrap.min.js?ver=3.0.0 HTTP/1.1
629	8.716470	192.168.1.2	83.212.207.19	HTTP	308	GET /wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.14.0 HTTP/1.1
692	8.802379	192.168.1.2	83.212.207.19	HTTP	309	GET /wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.14.0 HTTP/1.1
741	8.918193	192.168.1.2	83.212.207.19	HTTP	312	GET /wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2 HTTP/1.1
743	8.918859	192.168.1.2	83.212.207.19	HTTP	283	GET /wp-includes/js/jquery/ui/core.min.js?ver=1.13.2 HTTP/1.1
747	8.919739	192.168.1.2	83.212.207.19	HTTP	306	GET /wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6 HTTP/1.1
749	8.920757	192.168.1.2	83.212.207.19	HTTP	315	GET /wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=3.14.0 HTTP/1.1
778	8.950212	192.168.1.2	83.212.207.19	HTTP	306	GET /wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.9.0 HTTP/1.1
785	8.976037	192.168.1.2	83.212.207.19	HTTP	301	GET /wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.14.0 HTTP/1.1
814	9.008085	192.168.1.2	83.212.207.19	HTTP	310	GET /wp-content/plugins/elementor/assets/js/preloaded-modules.min.js?ver=3.14.0 HTTP/1.1
820	9.010420	192.168.1.2	83.212.207.19	HTTP	276	GET /wp-content/themes/aadys/js/theme-menu.js HTTP/1.1
858	9.041046	192.168.1.2	83.212.207.19	HTTP	284	GET /wp-includes/js/wp-emoji-release.min.js?ver=6.2.3 HTTP/1.1
988	9.382414	192.168.1.2	192.168.1.1	HTTP	251	GET /rootDesc.xml HTTP/1.1
1001	9.505128	192.168.1.2	83.212.207.19	HTTP	308	GET /favicon.ico HTTP/1.1
1153	13.788797	192.168.1.2	192.168.1.1	HTTP	249	GET /WANCFG.xml HTTP/1.1
1541	18.333276	192.168.1.2	192.168.1.1	HTTP	249	GET /WANCFG.xml HTTP/1.1
1636	18.446876	192.168.1.2	34.104.35.123	HTTP	525	GET /edgedl/diffgen-puffin/hfnkplmhhgleadddgfemjhofmblmnb/1.0aac6c03143774caab08ae8fbedb9f84fb1e21ab340c3598644a7498239eb91b/1.b7e7...
1912	21.676990	192.168.1.2	34.104.35.123	HTTP	528	GET /edgedl/diffgen-puffin/hfnkplmhhgleadddgfemjhofmblmnb/1.0aac6c03143774caab08ae8fbedb9f84fb1e21ab340c3598644a7498239eb91b/1.b7e7...

**11) α)** Όχι, δεν έχει πραγματοποιηθεί **fragmentation** στο συγκεκριμένο **IP datagram**, καθώς το πεδίο "**Don't Fragment**", στο header "**Internet Protocol Version 4**", έχει τιμή **1**, που σημαίνει ότι η σημαία "**Don't Fragment**" είναι ενεργοποιημένη για το συγκεκριμένο πακέτο IP.

## Εργασία WireShark

No.	Time	Source	Destination	Protocol	Length	Info
268	7.718210	192.168.1.2	83.212.207.19	HTTP	365	GET / HTTP/1.1
336	7.997610	192.168.1.2	83.212.207.19	HTTP	309	GET /wp-includes/css/dist/block-library/style.min.css?ver=6.2.3 HTTP/1.1
338	7.999730	192.168.1.2	83.212.207.19	HTTP	299	GET /wp-includes/css/classic-themes.min.css?ver=6.2.3 HTTP/1.1
354	8.054122	192.168.1.2	83.212.207.19	HTTP	307	GET /wp-content/themes/aadya/css/bootstrap-wide.css?ver=6.2.3 HTTP/1.1
409	8.248374	192.168.1.2	83.212.207.19	HTTP	338	GET /wp-content/plugins/elementor/assets/lib/font-awesome/css/font-awesome.min.css?ver=4.7.0 HTTP/1.1
411	8.248766	192.168.1.2	83.212.207.19	HTTP	309	GET /wp-content/themes/aadya/css/bootstrap-social.css?ver=6.2.3 HTTP/1.1
415	8.253791	192.168.1.2	83.212.207.19	HTTP	294	GET /wp-content/themes/aadya/style.css?ver=6.2.3 HTTP/1.1
442	8.350214	192.168.1.2	83.212.207.19	HTTP	301	GET /wp-content/themes/aadya/css/carousel.css?ver=6.2.3 HTTP/1.1
449	8.358588	192.168.1.2	83.212.207.19	HTTP	336	GET /wp-content/plugins/elementor/assets/lib/eicons/css/elementor-icons.min.css?ver=5.20.0 HTTP/1.1
451	8.359915	192.168.1.2	83.212.207.19	HTTP	325	GET /wp-content/plugins/elementor/assets/css/frontend-legacy.min.css?ver=3.14.0 HTTP/1.1
490	8.465567	192.168.1.2	83.212.207.19	HTTP	318	GET /wp-content/plugins/elementor/assets/css/frontend.min.css?ver=3.14.0 HTTP/1.1
492	8.469614	192.168.1.2	83.212.207.19	HTTP	326	GET /wp-content/plugins/elementor/assets/lib/swiper/css/swiper.min.css?ver=5.3.6 HTTP/1.1
496	8.477890	192.168.1.2	83.212.207.19	HTTP	310	GET /wp-content/uploads/elementor/css/post-53.css?ver=1687244449 HTTP/1.1
543	8.613927	192.168.1.2	83.212.207.19	HTTP	309	GET /wp-content/uploads/elementor/css/global.css?ver=1687244449 HTTP/1.1
545	8.616574	192.168.1.2	83.212.207.19	HTTP	281	GET /wp-includes/js/jquery/jquery.min.js?ver=3.6.4 HTTP/1.1
547	8.619745	192.168.1.2	83.212.207.19	HTTP	289	GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.0 HTTP/1.1
554	8.627861	192.168.1.2	83.212.207.19	HTTP	341	GET /wp-content/uploads/2018/11/s5_logo_home_.jpg HTTP/1.1
556	8.628060	192.168.1.2	83.212.207.19	HTTP	331	GET /wp-content/plugins/elementor/assets/lib/animations/animations.min.css?ver=3.14.0 HTTP/1.1
607	8.685978	192.168.1.2	83.212.207.19	HTTP	289	GET /wp-content/themes/aadya/js/bootstrap.min.js?ver=3.0.0 HTTP/1.1
629	8.716470	192.168.1.2	83.212.207.19	HTTP	308	GET /wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.14.0 HTTP/1.1
692	8.802379	192.168.1.2	83.212.207.19	HTTP	309	GET /wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.14.0 HTTP/1.1
741	8.918193	192.168.1.2	83.212.207.19	HTTP	312	GET /wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2 HTTP/1.1
743	8.918859	192.168.1.2	83.212.207.19	HTTP	283	GET /wp-includes/js/jquery/ui/core.min.js?ver=1.13.2 HTTP/1.1
747	8.919739	192.168.1.2	83.212.207.19	HTTP	306	GET /wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6 HTTP/1.1
749	8.920757	192.168.1.2	83.212.207.19	HTTP	315	GET /wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=3.14.0 HTTP/1.1
778	8.950212	192.168.1.2	83.212.207.19	HTTP	306	GET /wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.9.0 HTTP/1.1
785	8.976037	192.168.1.2	83.212.207.19	HTTP	301	GET /wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.14.0 HTTP/1.1
814	9.008085	192.168.1.2	83.212.207.19	HTTP	310	GET /wp-content/plugins/elementor/assets/js/preloaded-modules.min.js?ver=3.14.0 HTTP/1.1
820	9.010420	192.168.1.2	83.212.207.19	HTTP	276	GET /wp-content/themes/aadya/js/theme-menu.js HTTP/1.1
858	9.041046	192.168.1.2	83.212.207.19	HTTP	284	GET /wp-includes/js/wp-emoji-release.min.js?ver=6.2.3 HTTP/1.1
988	9.382414	192.168.1.2	192.168.1.1	HTTP	251	GET /rootDesc.xml HTTP/1.1
1001	9.505128	192.168.1.2	83.212.207.19	HTTP	308	GET /favicon.ico HTTP/1.1
1153	13.788797	192.168.1.2	192.168.1.1	HTTP	249	GET /NANCfg.xml HTTP/1.1
1541	18.333276	192.168.1.2	192.168.1.1	HTTP	249	GET /NANCfg.xml HTTP/1.1
1636	18.446876	192.168.1.2	34.104.35.123	HTTP	525	GET /edgedl/diffgen-puffin/hfknplmhhgieaddgfemjhofefblmnb/1.0aac6c03143774caab08ae8fbedb9f84fb1e21ab340c359864a47498239eb91b/1.b7e7...
1912	21.676990	192.168.1.2	34.104.35.123	HTTP	528	GET /edgedl/diffgen-puffin/hfknplmhhgieaddgfemjhofefblmnb/1.0aac6c03143774caab08ae8fbedb9f84fb1e21ab340c359864a47498239eb91b/1.b7e7...

Wireshark · Packet 268 · Wi-Fi

Internet Protocol Version 4, Src: 192.168.1.2, 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: 351

Identification: 0x2487 (9351)

> 010. .... = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0xf07f [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.2

Destination Address: 83.212.207.19

> Transmission Control Protocol, Src Port: 58987, Dst Port: 80, Seq: 1333, Ack: 1, Len: 311

> [2 Reassembled TCP Segments (1643 bytes): #267(1332), #268(311)]

> Hypertext Transfer Protocol

b) Ο browser μου χρησιμοποιεί έκδοση **HTTP/1.1**. Αυτό φαίνεται αναλύοντας ένα get πακέτο και επισκέπτοντας στην επικεφαλίδα "**Hypertext Transfer Protocol**", το πεδίο **Request Version**.

## Εργασία Wireshark

```
Wireshark · Packet 268 · Wi-Fi

> Frame 268: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: CloudNetwork_82:69:df (5c:61:99:82:69:df), Dst: zte_da:47:42 (c8:ea:f8:da:47:42)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 83.212.207.19
> Transmission Control Protocol, Src Port: 58987, Dst Port: 80, Seq: 1333, Ack: 1, Len: 311
> [2 Reassembled TCP Segments (1643 bytes): #267(1332), #268(311)]
▼ 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: el-GR,el;q=0.9,en;q=0.8\r\n
    [truncated]Cookie: _ga_HP0HBFBQTF=GS1.2.1687461826.1.0.1687461826.0.0.0; _ga_TX2FZN050D=GS1.1.1687461826.1.1.1687461930.60.0.0; _ga_JRNR6NN16=GS1.2
```

c) Η σύνδεση είναι **persistent** καθώς, η τιμή του πεδίου **connection** στις πληροφορίες του πακέτου, στο "**Hypertext Transfer Protocol**", είναι "**keep-alive**".

```
Wireshark · Packet 268 · Wi-Fi

> Frame 268: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: CloudNetwork_82:69:df (5c:61:99:82:69:df), Dst: zte_da:47:42 (c8:ea:f8:da:47:42)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 83.212.207.19
> Transmission Control Protocol, Src Port: 58987, Dst Port: 80, Seq: 1333, Ack: 1, Len: 311
> [2 Reassembled TCP Segments (1643 bytes): #267(1332), #268(311)]
▼ 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: el-GR,el;q=0.9,en;q=0.8\r\n
    [truncated]Cookie: _ga_HP0HBFBQTF=GS1.2.1687461826.1.0.1687461826.0.0.0; _ga_TX2FZN050D=GS1.1.1687461826.1.1.1687461930.60.0.0; _ga_JRNR6N
```

12) a) Ο **server** χρησιμοποιεί έκδοση **HTTP/1.1**. Αυτό φαίνεται αναλύοντας ένα **Response Get** πακέτο και επισκέπτοντας στην επικεφαλίδα "**Hypertext Transfer Protocol**", το πεδίο **Response Version**.

## Εργασία Wireshark

```
Wireshark · Packet 326 · Wi-Fi
> Frame 326: 1185 bytes on wire (9480 bits), 1185 bytes captured (9480 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: zte_da:47:42 (c8:ea:f8:da:47:42), Dst: CloudNetwork_82:69:df (5c:61:99:82:69:df)
> Internet Protocol Version 4, Src: 83.212.207.19, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 58987, Seq: 6661, Ack: 1644, Len: 1131
> [6 Reassembled TCP Segments (7791 bytes): #321(1332), #322(1332), #323(1332), #324(1332), #325(1332), #326(1131)]
▼ 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
      Date: Fri, 12 Jan 2024 12:14:59 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/", <http://ccslab.aueb.gr/index.php/wp-json/wp/v2/pages/2>; rel="altern
      Vary: Accept-Encoding\r\n
      Content-Encoding: gzip\r\n
      Access-Control-Allow-Origin: *\r\n
    > Content-Length: 7290\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
```

**b)** Το λογισμικό που υλοποιεί τον **web server** είναι το **Apache(Ubuntu)**, στην έκδοση **2.4.18**. Αυτό φαίνεται αν αναλύοντας ένα **Response Get** πακέτο και επισκέπτοντας στην επικεφαλίδα "**Hypertext Transfer Protocol**", το πεδίο **server**.

```
Wireshark · Packet 326 · Wi-Fi
> Frame 326: 1185 bytes on wire (9480 bits), 1185 bytes captured (9480 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: zte_da:47:42 (c8:ea:f8:da:47:42), Dst: CloudNetwork_82:69:df (5c:61:99:82:69:df)
> Internet Protocol Version 4, Src: 83.212.207.19, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 58987, Seq: 6661, Ack: 1644, Len: 1131
> [6 Reassembled TCP Segments (7791 bytes): #321(1332), #322(1332), #323(1332), #324(1332), #325(1332), #326(1131)]
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 12 Jan 2024 12:14:59 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/", <http://ccslab.aueb.gr/index.php/wp-json/wp/v2/pages/2>; rel="alter
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
    Access-Control-Allow-Origin: *\r\n
  > Content-Length: 7290\r\n
    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 1/8]
  [Time since request: 0.116929000 seconds]
  [Request in frame: 268]
  [Next request in frame: 3361]
```

**c)** Το μέγεθος του αρχείου που στέλνει πίσω ο **web server** είναι **29322 bytes**, ενώ ο **τύπος** του αρχείου που στέλνει πίσω ο **web server** είναι ένα **HTML** αρχείο που χρησιμοποιεί κωδικοποίηση **UTF-8**(*text/html; charset=UTF-8*). Αυτό φαίνεται αν αναλύοντας ένα **Response Get** πακέτο και επισκέπτοντας στην επικεφαλίδα "**Hypertext Transfer Protocol**", το πεδίο **Content-Type** και **File Data**.

```

Wireshark - Packet 326 - Wi-Fi
> Frame 326: 1185 bytes on wire (9480 bits), 1185 bytes captured (9480 bits) on interface \Device\NPF_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0
> Ethernet II, Src: zte_da:47:42 (c8:ea:f8:da:47:42), Dst: CloudNetwork_82:69:df (5c:61:99:82:69:df)
> Internet Protocol Version 4, Src: 83.212.207.19, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 58987, Seq: 6661, Ack: 1644, Len: 1131
> [6 Reassembled TCP Segments (7791 bytes): #321(1332), #322(1332), #323(1332), #324(1332), #325(1332), #326(1131)]
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 12 Jan 2024 12:14:59 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/", <http://ccslab.aueb.gr/index.php/wp-json/wp/v2/pages/2>; rel="alternate"
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
    Access-Control-Allow-Origin: *\r\n
  > Content-Length: 7290\r\n
    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 1/8]
  [Time since request: 0.116929000 seconds]
  [Request in frame: 268]
  [Next request in frame: 336]
  [Next response in frame: 368]
  [Request URI: http://ccslab.aueb.gr/]
  Content-encoded entity body (gzip): 7290 bytes -> 29322 bytes
  File Data: 29322 bytes
  
```

**13)** Αυτό το **frame** περιγράφει ένα πακέτο **TCP** που περιλαμβάνει ένα αίτημα σύνδεσης (**SYN**) από τον υπολογιστή μου στον server στη θύρα **443**. Αυτό το πακέτο είναι μέρος του **Three-way Handshake** του πρωτοκόλλου **TCP** και αποτελεί το αίτημα **SYN** για την εγκατάσταση της σύνδεσης με προορισμό τη θύρα **443**.

## Εργασία Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1264	16.322253	192.168.1.2	195.251.255.227	TCP	66	59010 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1265	16.331204	192.168.1.2	195.251.255.227	TCP	66	59011 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1266	16.359179	195.251.255.227	192.168.1.2	TCP	66	443 → 59011 [SYN, ACK] Seq=0 Ack=1 Win=22304 Len=0 MSS=1332 WS=16 SACK_PERM
1267	16.359179	195.251.255.227	192.168.1.2	TCP	66	443 → 59010 [SYN, ACK] Seq=0 Ack=1 Win=22304 Len=0 MSS=1332 WS=16 SACK_PERM
1268	16.359303	192.168.1.2	195.251.255.227	TCP	54	59011 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
1269	16.359361	192.168.1.2	195.251.255.227	TCP	54	59010 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
1270	16.359739	192.168.1.2	195.251.255.227	TLSv1.2	588	Client Hello (SNI=eclass.aueb.gr)
1271	16.360001	192.168.1.2	195.251.255.227	TLSv1.2	620	Client Hello (SNI=eclass.aueb.gr)
1273	16.400996	195.251.255.227	192.168.1.2	TCP	54	443 → 59010 [ACK] Seq=1 Ack=535 Win=21840 Len=0
1274	16.401992	195.251.255.227	192.168.1.2	TCP	54	443 → 59011 [ACK] Seq=1 Ack=567 Win=21872 Len=0
1275	16.415336	195.251.255.227	192.168.1.2	TLSv1.2	1386	Server Hello
1276	16.417398	195.251.255.227	192.168.1.2	TCP	1386	443 → 59010 [PSH, ACK] Seq=1333 Ack=535 Win=21840 Len=1332 [TCP segment of a reassembled PDU]
1277	16.417398	195.251.255.227	192.168.1.2	TCP	1386	443 → 59010 [PSH, ACK] Seq=2665 Ack=535 Win=21840 Len=1332 [TCP segment of a reassembled PDU]
1278	16.417525	192.168.1.2	195.251.255.227	TCP	54	59010 → 443 [ACK] Seq=535 Ack=3997 Win=131840 Len=0
1279	16.417601	195.251.255.227	192.168.1.2	TLSv1.2	1386	Server Hello
1280	16.417601	195.251.255.227	192.168.1.2	TCP	154	443 → 59010 [PSH, ACK] Seq=3997 Ack=535 Win=21840 Len=100 [TCP segment of a reassembled PDU]
1281	16.417645	192.168.1.2	195.251.255.227	TCP	54	59010 → 443 [ACK] Seq=535 Ack=4097 Win=131584 Len=0
1282	16.418221	195.251.255.227	192.168.1.2	TCP	1386	443 → 59011 [PSH, ACK] Seq=1333 Ack=567 Win=21872 Len=1332 [TCP segment of a reassembled PDU]

Wireshark · Packet 1264 · Wi-Fi

Frame 1264: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0  
Section number: 1  
> Interface id: 0 (\Device\NPF\_{20F56E68-E686-48BA-B41A-1A3DD9211D90})  
Encapsulation type: Ethernet (1)  
Arrival Time: Jan 12, 2024 14:15:04.709143000 Χειμερινή ώρα GTB  
UTC Arrival Time: Jan 12, 2024 12:15:04.709143000 UTC  
Epoch Arrival Time: 1705061704.709143000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.145680000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 16.322253000 seconds]  
Frame Number: 1264  
Frame Length: 66 bytes (528 bits)  
Capture Length: 66 bytes (528 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]  
> Ethernet II, Src: CloudNetwork\_82:69:df (5c:61:99:82:69:df), Dst: zte\_da:47:42 (c8:ea:f8:da:47:42)  
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 195.251.255.227  
> Transmission Control Protocol, Src Port: 59010, Dst Port: 443, Seq: 0, Len: 0

**14)** Ο server δέχεται αιτήματα πελατών για το site eclass.aueb.gr στο port **443**. Αυτό φαίνεται στο header **TCP** στο πεδίο **destination port**.

Wireshark · Packet 1264 · Wi-Fi

> Frame 1264: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{20F56E68-E686-48BA-B41A-1A3DD9211D90}, id 0  
> Ethernet II, Src: CloudNetwork\_82:69:df (5c:61:99:82:69:df), Dst: zte\_da:47:42 (c8:ea:f8:da:47:42)  
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 195.251.255.227  
> Transmission Control Protocol, Src Port: 59010, Dst Port: 443, Seq: 0, Len: 0  
Source Port: 59010  
Destination Port: 443  
[Stream index: 29]  
> [Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 4190664752  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 0  
Acknowledgment number (raw): 0  
1000 .... = Header Length: 32 bytes (8)  
> Flags: 0x002 (SYN)  
Window: 64240  
[Calculated window size: 64240]



**15) Όχι**, δεν μπορώ να δω το περιεχόμενο των **HTTP** μηνυμάτων που ανταλλάσσει ο υπολογιστής μου με τον **web server** που φιλοξενεί το **eclass.aueb.gr**. Ο λόγος είναι, ότι η επικοινωνία με τον web server γίνεται μέσω **HTTPS**, οπότε τα δεδομένα είναι κρυπτογραφημένα. Αυτό φαίνεται, αφού ο **web server** έχει ως θύρα προορισμού την **443** που είναι θύρα για **HTTPS**.

**16)** Η έκδοση του **Transport Layer Security** πρωτοκόλλου χρησιμοποιούν στη μεταξύ τους επικοινωνία ο υπολογιστής μου με το **eclass.aueb.gr** είναι η **TLSv1.2**. Αυτό φαίνεται κοιτάζοντας τις λεπτομέρειες κάποιου **TLS handshake** πακέτου, στο **header Transport Layer Security**, το πεδίο **Version**.

