



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

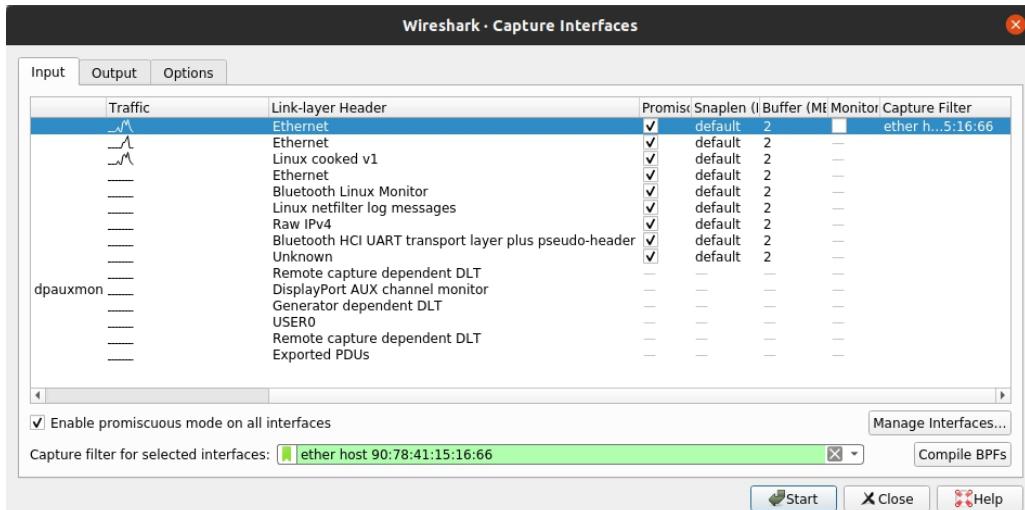
Δίκτυα Υπολογιστών

Αναφορά 2ης Εργαστηριακής Άσκησης

**Ραπτόπουλος Πέτρος (ει19145)
Ομάδα 3**

Άσκηση 1: Στρώμα Ζεύξης Δικτύου

Εφαρμόζουμε κατάλληλο φίλτρο σύλληψης για να καταγράφονται από το Wireshark μόνο πλαίσια που παράγονται ή απευθύνονται στον υπολογιστή μας:



Πατώντας Start αρχίζει η καταγραφή. Ανοίγουμε το terminal, εκτελούμε την εντολή ping 1.1.1.1, την διακόπτουμε μετά το πέρας κάποιων δευτερολέπτων και σταματάμε την καταγραφή:

```
Activities Terminal ▾
petrosrapto@petrosraptoAssistant:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=61 time=3.03 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=61 time=18.4 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=61 time=4.23 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=61 time=3.99 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=61 time=5.70 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=61 time=6.64 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=61 time=3.58 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=61 time=3.85 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=61 time=4.47 ms
64 bytes from 1.1.1.1: icmp_seq=10 ttl=61 time=3.80 ms
64 bytes from 1.1.1.1: icmp_seq=11 ttl=61 time=3.91 ms
64 bytes from 1.1.1.1: icmp_seq=12 ttl=61 time=3.99 ms
64 bytes from 1.1.1.1: icmp_seq=13 ttl=61 time=3.87 ms
64 bytes from 1.1.1.1: icmp_seq=14 ttl=61 time=7.63 ms
64 bytes from 1.1.1.1: icmp_seq=15 ttl=61 time=3.93 ms
64 bytes from 1.1.1.1: icmp_seq=16 ttl=61 time=3.87 ms
64 bytes from 1.1.1.1: icmp_seq=17 ttl=61 time=4.58 ms
64 bytes from 1.1.1.1: icmp_seq=18 ttl=61 time=2.97 ms
64 bytes from 1.1.1.1: icmp_seq=19 ttl=61 time=2.95 ms
64 bytes from 1.1.1.1: icmp_seq=20 ttl=61 time=3.96 ms
64 bytes from 1.1.1.1: icmp_seq=21 ttl=61 time=3.89 ms
64 bytes from 1.1.1.1: icmp_seq=22 ttl=61 time=3.90 ms
64 bytes from 1.1.1.1: icmp_seq=23 ttl=61 time=3.56 ms
64 bytes from 1.1.1.1: icmp_seq=24 ttl=61 time=3.03 ms
64 bytes from 1.1.1.1: icmp_seq=25 ttl=61 time=3.50 ms
64 bytes from 1.1.1.1: icmp_seq=26 ttl=61 time=3.01 ms
64 bytes from 1.1.1.1: icmp_seq=27 ttl=61 time=4.03 ms
64 bytes from 1.1.1.1: icmp_seq=28 ttl=61 time=7.38 ms
64 bytes from 1.1.1.1: icmp_seq=29 ttl=61 time=1.63 ms
64 bytes from 1.1.1.1: icmp_seq=30 ttl=61 time=8.77 ms
64 bytes from 1.1.1.1: icmp_seq=31 ttl=61 time=4.34 ms
64 bytes from 1.1.1.1: icmp_seq=32 ttl=61 time=8.00 ms
64 bytes from 1.1.1.1: icmp_seq=33 ttl=61 time=4.39 ms
64 bytes from 1.1.1.1: icmp_seq=34 ttl=61 time=4.65 ms
64 bytes from 1.1.1.1: icmp_seq=35 ttl=61 time=5.34 ms
64 bytes from 1.1.1.1: icmp_seq=36 ttl=61 time=8.21 ms
64 bytes from 1.1.1.1: icmp_seq=37 ttl=61 time=2.98 ms
64 bytes from 1.1.1.1: icmp_seq=38 ttl=61 time=4.56 ms
64 bytes from 1.1.1.1: icmp_seq=39 ttl=61 time=17.8 ms
64 bytes from 1.1.1.1: icmp_seq=40 ttl=61 time=5.77 ms
64 bytes from 1.1.1.1: icmp_seq=41 ttl=61 time=4.23 ms
64 bytes from 1.1.1.1: icmp_seq=42 ttl=61 time=5.81 ms
64 bytes from 1.1.1.1: icmp_seq=43 ttl=61 time=4.48 ms
64 bytes from 1.1.1.1: icmp_seq=44 ttl=61 time=4.34 ms
64 bytes from 1.1.1.1: icmp_seq=45 ttl=61 time=4.32 ms
64 bytes from 1.1.1.1: icmp_seq=46 ttl=61 time=2.97 ms
64 bytes from 1.1.1.1: icmp_seq=47 ttl=61 time=4.04 ms
64 bytes from 1.1.1.1: icmp_seq=48 ttl=61 time=4.47 ms
64 bytes from 1.1.1.1: icmp_seq=49 ttl=61 time=3.98 ms
64 bytes from 1.1.1.1: icmp_seq=50 ttl=61 time=4.50 ms
64 bytes from 1.1.1.1: icmp_seq=51 ttl=61 time=4.65 ms
64 bytes from 1.1.1.1: icmp_seq=52 ttl=61 time=2.97 ms
64 bytes from 1.1.1.1: icmp_seq=53 ttl=61 time=3.97 ms
64 bytes from 1.1.1.1: icmp_seq=54 ttl=61 time=1.80 ms
^C
-- 1.1.1.1 ping statistics --
108 packets transmitted, 108 received, 0% packet loss, time 107157ms
rtt min/avg/max/dev = 2.566/6.225/109.426/16.822 ms
```

Με βάση τα δεδομένα που καταγράφαμε εφαρμόζουμε το φίλτρο απεικόνισης arp or ip όπως φαίνεται παρακάτω:

1.1) Το φίλτρο arp or ip εμφανίζει τα πλαίσια που περιέχουν πρωτόκολλα στρώματος δικτύου IP ή ARP.

Σημείωση: Το πρωτόκολλο ARP (Address Resolution Protocol) βρίσκεται στο στρώμα ζεύξης δεδομένων, αλλά θεωρείται πρωτόκολλο του στρώματος δικτύου στο Internet, επειδή τα δεδομένα του ARP ενθυλακώνονται απ' ευθείας σε πλαίσια Ethernet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000 79.124.62.82		147.102.202.220	TCP	54	47821 - 10143 [SYN] Seq=0 Win=1024 Len=0
2	0.634619451 147.102.202.220	142.251.209.10		UDP	75	48341 - 443 Len=33
3	0.669113196 142.251.209.10		147.102.202.220	UDP	67	443 - 48341 Len=25
4	6.497280899 147.102.202.220	142.250.180.174		UDP	75	32977 - 443 Len=33
5	6.531157673 142.250.180.174		147.102.202.220	UDP	68	443 - 32977 Len=26
6	6.707041963 147.102.202.220	142.251.209.10		UDP	75	48341 - 443 Len=33
7	7.118119891 142.251.209.10		147.102.202.220	UDP	67	443 - 48341 Len=25
8	8.060860607 147.102.202.220	142.250.180.174		UDP	50	32977 - 443 Len=33
9	8.137892462 147.102.202.220	3.68.61.181		TLSv1.2	120	Application Data
10	8.140413987 147.102.202.220	142.250.180.174		UDP	1007	32977 - 443 Len=965
11	8.150108194 147.102.202.220	142.250.180.174		UDP	333	32977 - 443 Len=291
12	8.189939409 142.250.180.174		147.102.202.220	UDP	72	443 - 32977 Len=30
13	8.189939949 142.250.180.174		147.102.202.220	UDP	72	443 - 32977 Len=30
14	8.193356189 3.68.61.181		147.102.202.220	TLSv1.2	122	Application Data
15	8.193385449 147.102.202.220	3.68.61.181		TCP	66	44304 - 443 [ACK] Seq=55 Ack=57 Win=501 Len=0 TSval=375920025...
16	8.196947341 147.102.202.220	142.250.180.174		UDP	75	32977 - 443 Len=33
17	8.212323232 142.250.180.174		147.102.202.220	UDP	728	443 - 32977 Len=686
18	8.212323649 142.250.180.174		147.102.202.220	UDP	223	443 - 32977 Len=181
19	8.212574589 147.102.202.220	142.250.180.174		UDP	79	32977 - 443 Len=37
20	8.219788607 147.102.202.220	142.250.180.174		UDP	75	32977 - 443 Len=33

1.2) Πεδία Επικεφαλίδας Ethernet: -Destination - Source -Type

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000 79.124.62.82		147.102.202.220	TCP	54	47821 - 10143 [SYN] Seq=0 Win=1024 Len=0
2	0.634619451 147.102.202.220	142.251.209.10		UDP	75	48341 - 443 Len=33
3	0.669113196 142.251.209.10		147.102.202.220	UDP	67	443 - 48341 Len=25
4	6.497280899 147.102.202.220	142.250.180.174		UDP	75	32977 - 443 Len=33
5	6.531157673 142.250.180.174		147.102.202.220	UDP	68	443 - 32977 Len=26
6	6.707041963 147.102.202.220	142.251.209.10		UDP	75	48341 - 443 Len=33
7	7.118119891 142.251.209.10		147.102.202.220	UDP	67	443 - 48341 Len=25
8	8.060860607 147.102.202.220	142.250.180.174		TCP	54	32977 - 443 [SYN] Seq=0 Win=65535 Len=0
9	8.137892462 147.102.202.220	3.68.61.181		TLSv1.2	120	Application Data
10	8.140413987 147.102.202.220	142.250.180.174		UDP	1007	32977 - 443 Len=965
11	8.150108194 147.102.202.220	142.250.180.174		UDP	333	32977 - 443 Len=291
12	8.189939409 142.250.180.174		147.102.202.220	UDP	72	443 - 32977 Len=30
13	8.189939949 142.250.180.174		147.102.202.220	UDP	72	443 - 32977 Len=30
14	8.193356189 3.68.61.181		147.102.202.220	TLSv1.2	122	Application Data
15	8.193385449 147.102.202.220	3.68.61.181		TCP	66	44304 - 443 [ACK] Seq=55 Ack=57 Win=501 Len=0 TSval=375920025...
16	8.196947341 147.102.202.220	142.250.180.174		UDP	75	32977 - 443 Len=33
17	8.212323232 142.250.180.174		147.102.202.220	UDP	728	443 - 32977 Len=686
18	8.212323649 142.250.180.174		147.102.202.220	UDP	223	443 - 32977 Len=181
19	8.212574589 147.102.202.220	142.250.180.174		UDP	79	32977 - 443 Len=37
20	8.219788607 147.102.202.220	142.250.180.174		UDP	75	32977 - 443 Len=33

Σημείωση: Στα πλαίσια με ARP έχουμε ένα επιπλέον πεδίο Padding ή Trailer:

No.	Time	Source	Destination	Protocol	Length	Info
545	60.88276892	ec:be:5f:86:e9:4a	IntelCor_15:16:66	ARP	60	Who has 147.102.202.220? Tell 147.102.203.135
546	60.8827837	IntelCor_15:16:66	ec:be:5f:86:e9:4a	ARP	42	147.102.202.220 is at 90:78:41:15:16:66
892	98.8557681	IntelCor_15:16:66	Cisco_d0:d9:1d	ARP	42	Who has 147.102.200.200? Tell 147.102.202.220
893	98.8580216	Cisco_d0:d9:1d	IntelCor_15:16:66	ARP	56	147.102.200.200 is at 08:ec:f5:d0:d9:1d

1.3) Υπάρχει πεδίο για το συνολικό μήκος των πλαισίου ή των δεδομένων που μεταφέρει;: 'Όχι

1.4) Μήκος διευθύνσεων Ethernet: **6 bytes**

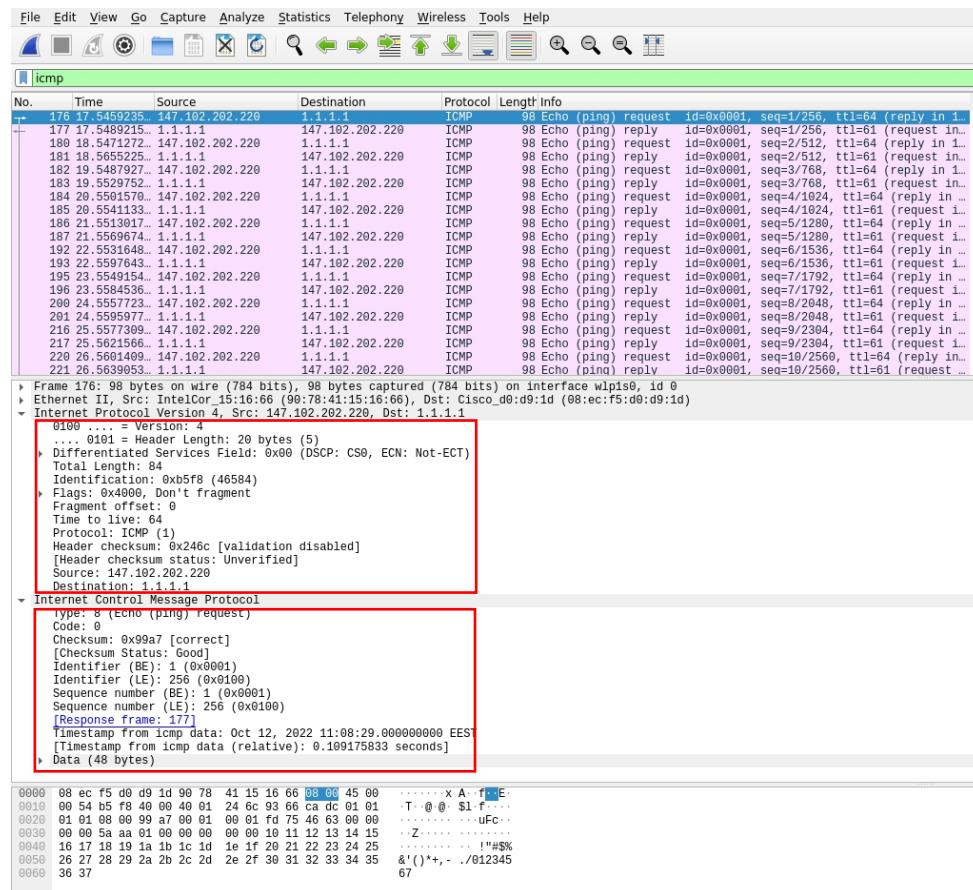
1.5) Συνολικό μήκος επικεφαλίδας Ethernet: **14 bytes** (6 bytes Destination, 6 bytes Source, 2 bytes Type)

Σημείωση: Στα πλαίσια με ARP έχουμε παραπάνω bytes λόγω του πεδίου Padding ή Trailer.

- 1.6) Πεδίο πλαισίου Ethernet που καθορίζει το πρωτόκολλο δικτύου: **Πεδίο type**
- 1.7) Θέση που καταλαμβάνει μέσα στην επικεφαλίδα Ethernet: **2 τελευταία bytes**
- 1.8) Τιμή του πεδίου type για πακέτα IPv4: **0x0800**
- 1.9) Τιμή του πεδίου type για πακέτα ARP: **0x0806**

Άσκηση 2: Στρώμα Δικτύου

Εφαρμόζουμε φίλτρο απεικόνισης *icmp* στην καταγραφή της Άσκησης 1:



2.1) Σημασία φίλτρου *icmp*: Εμφανίζει τα πακέτα με πρωτόκολλο ICMP (Internet Control Message Protocol).

2.2) Μήκος διευθύνσεων IPv4: **4 bytes**

2.3) Ονόματα των πρώτων δύο πεδίων της επικεφαλίδας IPv4: **-Version -Header Length**

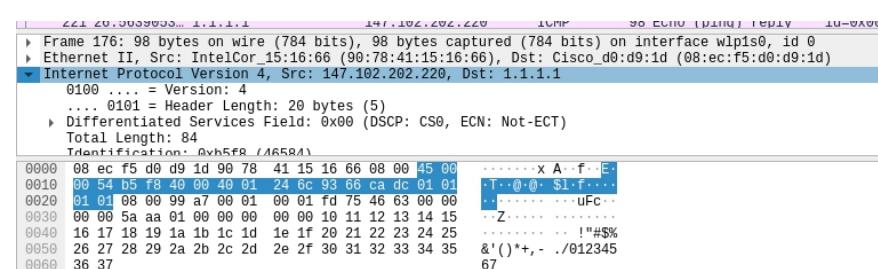
2.4) Μήκος του πεδίου Version: **4 bits**

Μήκος του πεδίου Header Length: **4 bits**

Τιμή του πεδίου Version: **0100** (4 σε δεκαδικό σύστημα)

Τιμή του πεδίου Header Length: **0101** (5 σε δεκαδικό σύστημα)

Για να βρούμε το συνολικό μήκος σε bytes της επικεφαλίδας IPv4 επιλέγουμε το “Internet Protocol Version 4” και μετράμε τα bytes που υπογραμμίζονται στο παράθυρο των περιεχομένων:



2.5) Συνολικό μήκος της επικεφαλίδας IPv4: 20 bytes

2.6) Πως προκύπτει το μήκος από την επικεφαλίδα IPv4:: Από το πεδίο Header Length

Για να βρούμε το συνολικό μήκος σε bytes του πακέτου IPv4 επιλέγουμε το “Internet Protocol Version 4” και μετράμε όχι μόνο τα bytes που υπογραμμίζονται στο παράθυρο των περιεχομένων αλλά και αυτά που ακολουθούν.

2.7) Συνολικό μήκος του πακέτου IPv4: 84 bytes

2.8) Πεδίο στην επικεφαλίδα σχετικό με το μήκος πακέτου IPv4: Πεδίο Total Length, συμφωνεί με 2.7)

Για να βρούμε το συνολικό μήκος σε bytes των δεδομένων του πακέτου IPv4 επιλέγουμε το “Internet Protocol Version 4” και μετράμε τα bytes που ακολουθούν των υπογραμμισμένων. Μετράμε δηλαδή ό,τι είναι μετά την επικεφαλίδα.

2.9) Συνολικό μήκος δεδομένων (payload) του πακέτου IPv4: 64 bytes

2.10) Πως προκύπτει το μήκος δεδομένων από την επικεφαλίδα: Total Length - Header Length

2.11) Πεδίο επικεφαλίδας IPv4 που καθορίζει το πρωτόκολλο ανώτερου στρώματος TCP/IP: Πεδίο Protocol

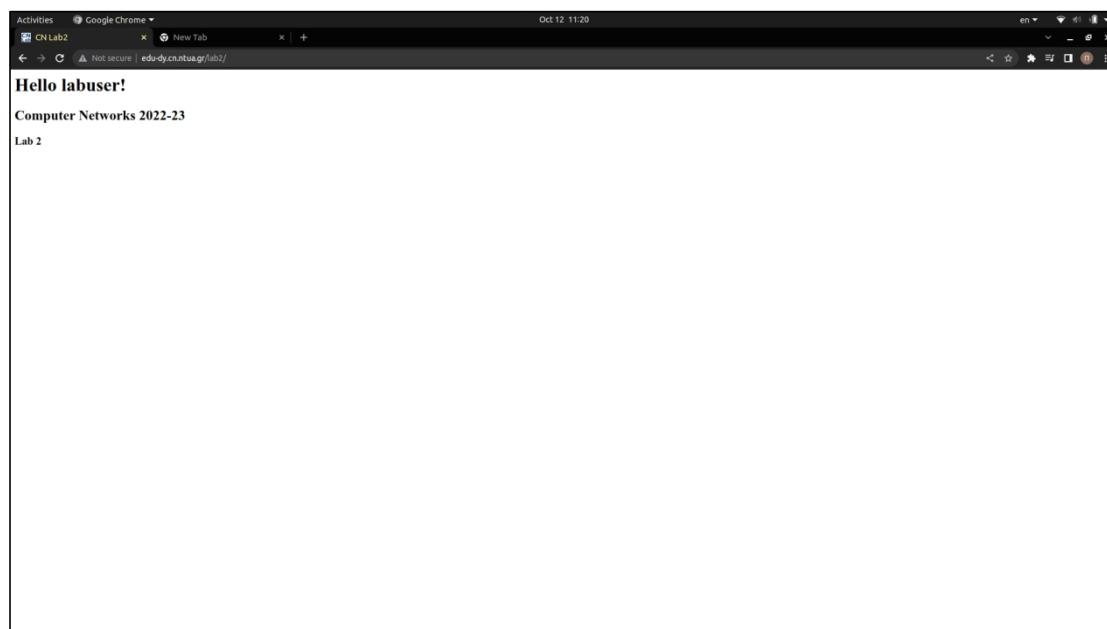
Επιλέγουμε το πεδίο Protocol και παρατηρούμε το υπογραμμισμένο κομμάτι στα περιεχόμενα.

2.12) Θέση του πεδίου Protocol από την αρχή της επικεφαλίδας: 10^o bytes από την αρχή της επικεφαλίδας

2.13) Τιμή για το πρωτόκολλο ICMP: 0x01

Άσκηση 3: Στρώματα Μεταφοράς

Εκτελούμε την εντολή “sudo systemd-resolve --flush-caches”, αρχίζουμε μια νέα καταγραφή στο Wireshark και επισκεπτόμαστε την ιστοσελίδα <http://edu-dy.cn.ntua.gr/lab2/>. Σταματάμε την καταγραφή μετά την ολοκλήρωση της ιστοσελίδας και ενεργοποιούμε το φίλτρο απεικόνισης `tcp or udp`.



3.1) Σημασία φίλτρου απεικόνισης `tcp or udp`: Εμφανίζει τα πλαίσια με πρωτόκολλο στρώματος μεταφοράς TCP (Transmission Control Protocol) ή UDP (User Datagram Protocol).

3.2) Πρωτόκολλα στρώματος μεταφοράς που παρατηρούμε: TCP, UDP.

Σημείωση: Παρατηρούμε και πρωτόκολλα όπως DNS, HTTP. Αυτά θεωρούνται στου στρώματος εφαρμογής.

Ακόμη το πρωτόκολλο TLS τοποθετείται ανάμεσα στο στρώμα εφαρμογής και μεταφοράς.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	147.102.202.220	142.250.180.131	UDP	1292	53383 → 443 Len=1250
2	0.000250616	147.102.202.220	142.250.180.131	UDP	119	53383 → 443 Len=77
3	0.001162332	147.102.202.220	142.250.180.131	UDP	564	53383 → 443 Len=522
4	0.001385512	147.102.202.220	142.250.180.131	UDP	153	53383 → 443 Len=111
5	0.002160975	184.105.139.122	147.102.202.220	TCP	54	22614 → 80 [ACK] Seq=1 Ack=1
6	0.047227789	142.250.180.131	147.102.202.220	UDP	1292	443 → 53383 Len=1250
7	0.047228220	142.250.180.131	147.102.202.220	UDP	823	443 → 53383 Len=781
8	0.047228230	142.250.180.131	147.102.202.220	UDP	120	443 → 53383 Len=78
9	0.047980137	147.102.202.220	142.250.180.131	UDP	121	53383 → 443 Len=79
10	0.04818181	147.102.202.220	142.250.180.131	UDP	75	53383 → 443 Len=33
11	0.073468323	147.102.202.220	142.250.180.131	UDP	75	53383 → 443 Len=33
12	0.105653939	142.250.180.131	147.102.202.220	UDP	67	443 → 53383 Len=25
13	0.105654419	142.250.180.131	147.102.202.220	UDP	67	443 → 53383 Len=25
14	0.105654495	142.250.180.131	147.102.202.220	UDP	655	443 → 53383 Len=613
15	0.105654579	142.250.180.131	147.102.202.220	UDP	68	443 → 53383 Len=26
16	0.105654661	142.250.180.131	147.102.202.220	UDP	129	443 → 53383 Len=87
17	0.105654749	142.250.180.131	147.102.202.220	UDP	67	443 → 53383 Len=25
18	0.105654838	142.250.180.131	147.102.202.220	UDP	162	443 → 53383 Len=129
19	0.106143269	147.102.202.220	142.250.180.131	UDP	77	53383 → 443 Len=35
20	0.106392822	147.102.202.220	142.250.180.131	UDP	77	53383 → 443 Len=35

> Frame 1: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface wlpi0, id 0
 > Ethernet II, Src: IntelCor_15:16:66 (08:ec:f5:d0:09:1d), Dst: Cisco_d0:09:1d (08:ec:f5:d0:09:1d)
 > Internet Protocol Version 4, Src: 147.102.202.220, Dst: 142.250.180.131

> User Datagram Protocol, Src Port: 53383, Dst Port: 443

Source Port: 53383
 Destination Port: 443
 Len: 1250
 Checksum: 0x5daf [unverified]
 [Checksum Status: Unverified]
 [Stream index: 0]
 [Timestamps]
 Data (1250 bytes)

```
0028 b4 83 d0 87 03 bb 04 ea 5d af c1 08 00 00 00 01 08 . . . .
0030 cd d9 b0 0e 51 8b 84 aa 09 40 00 fc 21 9a 0a . . . . 0F . .
0040 96 c7 6c 17 a9 6d 71 f5 bb 6b 19 82 31 a2 39 4d . . . . 1 - m1 - k - 1 0M
0050 0a 91 5f 81 5b 40 49 95 02 b4 0f 1b 56 44 07 . . . . [01] . . . . VA
0060 6e 7b 25 76 8f d6 a8 38 95 20 cf 39 51 79 61 . . . . [02] . . . . 8 quya
0070 2e 57 d5 cc 6b ec 19 f9 07 7d 40 4c dc 8c c7 ce . . . . W k - . . . . PBN
0080 42 44 89 7c e9 1b 09 34 82 69 dc 32 0b 0e 71 b8 BD | . . . . 4 j 2 - q
0090 db cc 75 41 37 36 2a cb 6e 89 c7 04 7b 15 0f aa uA76* n { . . . .
00a0 24 e1 06 a4 11 b4 23 5c a3 c1 1f 6c 94 ac ab $ . . . . # \ . .
00b0 14 71 7c f5 fd 4e e2 db 9e 0b 97 db 57 93 . . . . z . .
00c0 a9 94 00 ee 4b 48 b3 8c 96 b2 b4 42 7e eb cf . . . . @ B - .
00d0 87 95 05 ba 73 b1 c5 18 7a 15 35 7d ea 49 5d . . . . J s . . . . z5 - I]
00e0 08 ff f4 1a e9 fa 5a 7d 07 8b 2c e1 3b ea a2 bd . . . . Z ) + ; . .
00f0 8c 63 4d 34 ee 14 e6 0a d4 67 2c 56 fb 74 fd f5 97 cM . . . . g,Vt - .
0100 87 a2 f6 e6 39 2f 28 2b 17 e4 af 8a ac 07 60 . . . . 9 / ( . .
0110 7a 27 f3 4b 64 57 8c bc 78 61 7b 2d 08 a4 16 85 z' KdW xap . .
0120 77 a9 dc 49 0b 96 0d 8b 9c 97 58 f8 bf 7b 6b d6 w @ . . . . X - k
0130 f4 b8 c2 91 1e 30 3d 0f b7 df 6b 98 df fc b7 0= . . . . 0 = . .
0140 e9 38 8c 12 46 da 49 17 26 e4 74 c4 a1 02 7c 6 - F . I - & t - .
0150 89 9d e9 08 c3 91 5c 33 b9 57 fb 4a 78 d9 . . . . \ 3; W x
0160 73 e8 86 ee ab ee 0c 45 ac 54 f7 7b 53 d9 da 83 s . . . . E - T { S
0170 9b ee b8 f5 21 7d 22 63 27 11 75 4b a8 42 c6 47 ) c' t uH B G
0180 83 57 0d cd 75 0b 75 f7 89 77 d2 76 7e d9 83 f9 . . . . w V - .
0190 18 5f 4d ff 66 77 50 f7 c9 ea c9 1f 0c af 40 _ M - w . . . . @
01a0 7f a7 c7 49 9f 57 0e 6e be 1b dd 33 14 e7 ba f6 F - n . . . . 3
01b0 15 b1 fa 8a fa 15 95 77 ff 68 ff 45 a2 0c 53 5a . . . . w - h E - SZ
01c0 92 f2 43 47 62 49 e2 a7 cc b1 c2 e9 1c 8a CGDI . . . .
01d0 ad e4 87 ad 97 1e da 12 bb c5 a8 af 21 72 6b ee k - ! - .
01e0 ic 62 13 cd 74 40 78 f6 aa 2f c7 ef b3 df 11 dd b - t@x . . . .
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	147.102.202.220	142.250.180.131	UDP	1292	53383 → 443 Len=1250
2	0.000250616	147.102.202.220	142.250.180.131	UDP	119	53383 → 443 Len=77
3	0.001162332	147.102.202.220	142.250.180.131	UDP	564	53383 → 443 Len=522
4	0.001385512	147.102.202.220	142.250.180.131	UDP	153	53383 → 443 Len=111
5	0.002160975	184.105.139.122	147.102.202.220	TCP	54	22614 → 80 [ACK] Seq=1 Ack=1 Win=83 Len=0
6	0.047227789	142.250.180.131	147.102.202.220	UDP	1292	443 → 53383 Len=1250
7	0.047228220	142.250.180.131	147.102.202.220	UDP	823	443 → 53383 Len=781
8	0.047228230	142.250.180.131	147.102.202.220	UDP	120	443 → 53383 Len=78
9	0.047980137	147.102.202.220	142.250.180.131	UDP	142	250.180.131
10	0.04818181	147.102.202.220	142.250.180.131	UDP	75	53383 → 443 Len=33
11	0.073468323	147.102.202.220	142.250.180.131	UDP	75	53383 → 443 Len=33
12	0.105653939	142.250.180.131	147.102.202.220	UDP	67	443 → 53383 Len=25
13	0.105654419	142.250.180.131	147.102.202.220	UDP	67	443 → 53383 Len=25
14	0.105654495	142.250.180.131	147.102.202.220	UDP	655	443 → 53383 Len=613
15	0.105654579	142.250.180.131	147.102.202.220	UDP	68	443 → 53383 Len=26
16	0.105654661	142.250.180.131	147.102.202.220	UDP	121	53383 → 443 Len=67
17	0.105654749	142.250.180.131	147.102.202.220	UDP	142	250.180.131
18	0.105654838	142.250.180.131	147.102.202.220	UDP	162	443 → 53383 Len=120
19	0.106143269	147.102.202.220	142.250.180.131	UDP	77	53383 → 443 Len=35
20	0.106392822	147.102.202.220	142.250.180.131	UDP	77	53383 → 443 Len=35

> Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface wlpi0, id 0
 > Ethernet II, Src: IntelCor_15:16:66 (08:ec:f5:d0:09:1d), Dst: Cisco_d0:09:1d (08:ec:f5:d0:09:1d)
 > Internet Protocol Version 4, Src: 147.102.202.220, Dst: 142.250.180.131

> User Datagram Protocol, Src Port: 22614, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 22614
 Destination Port: 80
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Sequence number (raw): 3255073472
 Next sequence number: 1 (relative sequence number)
 Acknowledgment number: 1 (relative ack number)
 Acknowledgment number (raw): 5933307
 O101: . . . Header Length: 20 bytes (5)
 Flags: 0x010 (ACK)
 Window size value: 83
 [Calculated window size: 83]
 [Window size scaling factor: 1 (unknown)]
 Checksum: 0x19ab [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [Timestamps]

0000 00 78 41 15 16 66 08 ec f5 d0 9d 1d 08 00 45 a4 xA - f - E
 0010 00 28 d4 8b 0d 08 00 36 d3 c2 b9 6b 9d 7a 93 66 (- 0 - i - z - f
 0020 ca dc 5b 56 0d 59 c2 04 ya c9 03 09 5a bb 50 1c 1V Y z - Z P
 0030 0b 53 19 ab 00 00 00 S

Transmission Control Protocol (tcp), 20 bytes

Protocol: TCP (6)

Protocol: UDP (17)

3.3) Τιμή του πεδίου Protocol στην επικεφαλίδα IPv4 για το πρωτόκολλο:

TCP: **0x06** (6 σε δεκαδικό σύστημα) UDP: **0x11** (17 σε δεκαδικό σύστημα)

3.4) Ονόματα των πεδίων επικεφαλίδας των τεμαχίων TCP και δεδομένων γραμμάτων UDP που είναι κοινά:
-Source Port **-Destination Port** **-Checksum**

3.5) Μήκος της επικεφαλίδας των δεδομένων γραμμάτων UDP: 8 bytes

3.6) Υπάρχει πεδίο στην επικεφαλίδα για το συνολικό μήκος των δεδομένων γραμμάτων UDP;; Ναι - Πεδίο Length

3.7) Πεδίο που καθορίζει το μήκος της επικεφαλίδας του τεμαχίου TCP: Πεδίο Header Length

Θέση του πεδίου: **13° byte από την αρχή της επικεφαλίδας**

3.8) Υπάρχει πεδίο στην επικεφαλίδα για το συνολικό μήκος των τεμαχίων TCP;; 'Οχι

Το μήκος προκύπτει: **Total Length(Πεδίο του IP) - Header Length(Πεδίο του IP) - Header Length(Πεδίο του TCP)**

3.9) Υπάρχει πεδίο στην επικεφαλίδα TCP ή UDP που να προσδιορίζει τον τύπο του πρωτοκόλλου εφαρμογής;;

To Destination Port/Source Port πεδίο αποκαλύπτει ποιο πρωτόκολλο στρώματος εφαρμογής χρησιμοποιείται.

3.10) Πρωτόκολλα εφαρμογής που παρατηρούμε μεταξύ άλλων: DNS, HTTP

Άσκηση 4: Στρώμα Εφαρμογής

Ενεργοποιούμε το φίλτρο απεικόνισης https or dns στην καταγραφή της Άσκησης 3.

4.1) Πρωτόκολλο μεταφοράς που χρησιμοποιεί το DNS: UDP

4.2) Πρωτόκολλο μεταφοράς που χρησιμοποιεί το HTTP: TCP

4.3) Bit της σημαίας στην επικεφαλίδα DNS που καθορίζει αν πρόκειται για ερώτηση ή απάντηση: 17° bit μετά την αρχή της επικεφαλίδας (αρχίζοντας την μέτρηση από το 1), δηλαδή το 1° bit του πεδίου flags.

Αν το bit είναι ο τότε το μήνυμα είναι ερώτηση, ενώ αν είναι 1 το μήνυμα είναι απάντηση.

No.	Time	Source	Destination	Protocol	Length	Info
1	38 11 0928352	147.102.202.228	147.102.224.243	DNS	81	Standard query 0xc95a A google.com OPT
2	39 11 0946738	147.102.224.243	147.102.202.228	DNS	97	Standard query response 0xc95a A google.com A 142.251.209.46 ..
3	160 30 9999505	147.102.202.228	147.102.224.243	DNS	86	Standard query 0x2fcf A ssl.gstatic.com OPT
4	161 31 0040928	147.102.224.243	147.102.202.228	DNS	102	Standard query response 0x2fcf A ssl.gstatic.com A 142.251.20..
5	257 39 6623199	147.102.202.228	147.102.224.243	DNS	85	Standard query 0xa2e4 A www.google.com OPT
6	258 39 6635901	147.102.224.243	147.102.202.228	DNS	101	Standard query response 0xa2e4 A www.google.com A 142.250.180..
7	387 44 2955058	147.102.202.228	147.102.224.243	DNS	106	Standard query 0x8d9f A optimizationguide-pa.googleapis.com O..
8	388 44 2962127	147.102.202.228	147.102.224.243	DNS	88	Standard query 0xd401 A edu-dy.cn.ntua.gr OPT
9	389 44 2985953	147.102.224.243	147.102.202.228	DNS	234	Standard query response 0x8d9f A optimizationguide-pa.googleapis..
10	390 44 2994742	147.102.202.228	147.102.224.243	DNS	94	Standard query 0x185e A safebrowsing.google.com OPT
11	393 44 3021826	147.102.224.243	147.102.202.228	DNS	129	Standard query response 0x185e A safebrowsing.google.com CNAM..
12	396 44 3058871	147.102.224.243	147.102.202.228	DNS	132	Standard query response 0xd401 A edu-dy.cn.ntua.gr CNAME edu-..
13	401 44 3101333	147.102.202.228	147.102.40.15	HTTP	577	GET /lab2/ HTTP/1.1
14	404 44 3268502	147.102.40.15	147.102.202.228	HTTP	604	HTTP/1.1 200 OK (text/html)

Frame 38: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface wlpis0, id 0
Ethernet II, Src: IntelCor_15:16:66 (00:78:41:15:16:66), Dst: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d)
Internet Protocol Version 4, Src: 147.102.202.228, Dst: 147.102.224.243
User Datagram Protocol, Src Port: 49408, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xc95a
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
Additional records
[Response In: 391]
TRANSMIT RTE Data
0000 08 ec f5 d0 d9 1d 00 48 00 40 11 64 2d 93 66 ca dc 93 66 .:.....x A. f...E:
0010 00 43 03 e0 00 48 00 40 11 64 2d 93 66 ca dc 93 66 .C. @ @ d. f...f
0020 e0 f3 c1 00 09 35 00 2f 65 a6 c9 5a 01 00 00 015. e [Z] ..
0030 00 00 00 00 01 00 67 07 67 67 6c 65 03 63 67 m.....) ..
0040 6d 00 00 01 00 00 29 02 00 00 00 00 00 00 00 00 m.....) ..
0050 00 ..

No.	Time	Source	Destination	Protocol	Length	Info
38 11 0928352	147.102.202.228		147.102.224.243	DNS	81	Standard query 0xc95a A google.com OPT
39 11 0946738	147.102.224.243		147.102.202.228	DNS	97	Standard query response 0xc95a A google.com A 142.251.209.46 ..
160 30 9999505	147.102.202.228		147.102.224.243	DNS	86	Standard query 0x2fcf A ssl.gstatic.com OPT
161 31 0040928	147.102.224.243		147.102.202.228	DNS	102	Standard query response 0x2fcf A ssl.gstatic.com A 142.251.20..
257 39 6623199	147.102.202.228		147.102.224.243	DNS	85	Standard query 0xa2e4 A www.google.com OPT
258 39 6635901	147.102.224.243		147.102.202.228	DNS	101	Standard query response 0xa2e4 A www.google.com A 142.250.180..
387 44 2955058	147.102.202.228		147.102.224.243	DNS	106	Standard query 0x8d9f A optimizationguide-pa.googleapis.com O..
388 44 2962127	147.102.202.228		147.102.224.243	DNS	88	Standard query 0xd401 A edu-dy.cn.ntua.gr OPT
389 44 2985953	147.102.224.243		147.102.202.228	DNS	234	Standard query response 0x8d9f A optimizationguide-pa.googleapis..
390 44 2994742	147.102.202.228		147.102.224.243	DNS	94	Standard query 0x185e A safebrowsing.google.com OPT
393 44 3021826	147.102.224.243		147.102.202.228	DNS	129	Standard query response 0x185e A safebrowsing.google.com CNAM..
396 44 3058871	147.102.224.243		147.102.202.228	DNS	132	Standard query response 0xd401 A edu-dy.cn.ntua.gr CNAME edu-..
401 44 3101333	147.102.202.228		147.102.40.15	HTTP	577	GET /lab2/ HTTP/1.1
404 44 3268502	147.102.40.15		147.102.202.228	HTTP	604	HTTP/1.1 200 OK (text/html)

Frame 401: 577 bytes on wire (4616 bits), 577 bytes captured (4616 bits) on interface wlpis0, id 0
Ethernet II, Src: IntelCor_15:16:66 (00:78:41:15:16:66), Dst: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d)
Internet Protocol Version 4, Src: 147.102.202.228, Dst: 147.102.40.15
Transmission Control Protocol, Src Port: 32876, Dst Port: 80, Seq: 1, Ack: 1, Len: 511
hypertext Transfer Protocol
GET /Lab2/ HTTP/1.1\r\n
Host: edu-dy.cn.ntua.gr\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 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\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Language: el-GR,el;q=0.9,en;q=0.8\r\n
Cookie: _ga=GA1.2.1793078283.1571500183; _gid=GA1.2.1300710032.1665474687\r\n
[Full request URI: http://edu-dy.cn.ntua.gr/lab2/]
[HTTP request 1/1]
[Response in frame: 404]
TRANSMIT RTE Data

```
0049 fc 9e 47 45 54 28 2f 6c 61 82 32 2f 20 48 54 54 :GET /1 ab2/ HTI
0050 50 2f 11 24 34 0d 0a 09 6f 74 9a 20 65 64 P/1.1. H ttp/1
0051 2d 64 79 2e 63 6e 2e 6e 24 75 6e 2e 67 72 0d 0a /edu-dy.cn.n tua.gr
0078 43 6f 66 6e 65 63 74 69 6f 66 39 6b 65 65 78 Connecti on: keep
0089 2d 61 6c 69 76 0d 0a 55 79 67 72 61 64 65 2d -alive.. Upgrade-
0099 44 6e 73 65 75 72 65 2d 65 71 75 65 73 74 Insecure - Request
0098 73 3a 2d 31 0d 0a 55 73 65 72 2d 41 67 65 66 74 s: 1; Us er-Agent:
0099 3a 20 4d 6f 74 69 6c 61 2f 35 2e 39 29 28 58 : Mozilla/5.0 (X
00c0 31 31 2b 29 4c 69 66 75 78 20 78 38 36 5f 36 34 11; Linu x x86_64
0008 29 20 41 70 70 6c 65 57 65 62 48 69 74 2f 35 33 ) AppleWebKit/53
00e6 37 2e 33 36 29 28 4b 54 4d 4c 2c 20 6c 69 6b 7.36 (KHTML, like
00f8 65 20 47 65 63 6b 67 29 20 43 68 72 67 6d 65 2f Gecko) Chrome/
0100 31 30 37 2e 30 2e 30 2e 30 26 51 66 61 72 69 106.0.0.0 Safari
0110 2f 35 33 37 2e 33 36 0d 0e 41 63 63 65 70 74 3a /537.36. Accept:
0128 20 74 65 78 74 2f 68 74 66 2c 61 70 70 6c 69 text/ht ml,appli
0130 63 61 74 69 6f 6e 2f 78 66 6c 2b 78 6d 6c cation/x htm l+xml
0140 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c , applica tion/xml
0158 3c 71 3d 39 2e 39 2c 69 66 61 67 65 2f 61 76 69 ;q=0.9, image/avif
0168 66 2c 69 6d 61 67 65 2f 77 65 62 70 72 69 6d 61 ,image/ webp,ina
0178 67 65 2f 61 70 66 67 2c 2f 27 2a 3d 71 3d 30 2a ge/apng, /*?q=0.
0188 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 8, applic ation/si
0198 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d gned-exc hange,v
```

4.4) Θύρα προορισμού των ερωτήσεων DNS: 53 (φαίνεται στις πληροφορίες του UDP - destination port για query)

4.5) Θύρα πηγής των ερωτήσεων DNS: Μεταβλητό (φαίνεται στις πληροφορίες του UDP - source port για query)

4.6) Θύρα πηγής των απαντήσεων DNS: 53 (φαίνεται στις πληροφορίες του UDP - source port για response)

4.7) Θύρα προορισμού των απαντήσεων DNS: Μεταβλητό (φαίνεται στο UDP - destination port για response)

Σημείωση: Όπου Μεταβλητό είναι μεταξύ άλλων οι θύρες 58621, 49408, 35121...

4.8) Παρατήρηση για τη σχέση θυρών πηγής των ερωτήσεων με τις θύρες προορισμού των απαντήσεων: Η απάντηση στέλνεται στην θύρα από όπου έγινε η αντίστοιχη ερώτηση.

4.9) Θύρα που ακούει ο εξυπηρετητής DNS: 53

4.10) Θύρα προορισμού των μηνυμάτων HTTP που παράγει ο υπολογιστής μας: 80

4.11) Θύρα πηγής των μηνυμάτων HTTP που έστειλε ο υπολογιστής μας: 32876

4.12) Θύρα πηγής των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού: 80

4.13) Θύρα προορισμού των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού: 32876

4.14) Θύρα που ακούει ο εξυπηρετητής HTTP: 80

4.15) Παρατήρηση για τη σχέση θυρών πηγής των ερωτήσεων με τις θύρες προορισμού των απαντήσεων: **Η απάντηση στέλνεται στην θύρα από όπου έγινε η αντίστοιχη ερώτηση.**

Επιλέγουμε το πρώτο μήνυμα πρωτοκόλλου HTTP και από το μενού “Analyze” επιλέγουμε “Follow TCP Stream”:

```
GET /lab2/ HTTP/1.1
Host: edu-dy.cn.ntua.gr
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: el-GR,el;q=0.9,en;q=0.8
Cookie: _ga=GA1.2.1793078283.1571500183; _gid=GA1.2.1300710032.1665474687

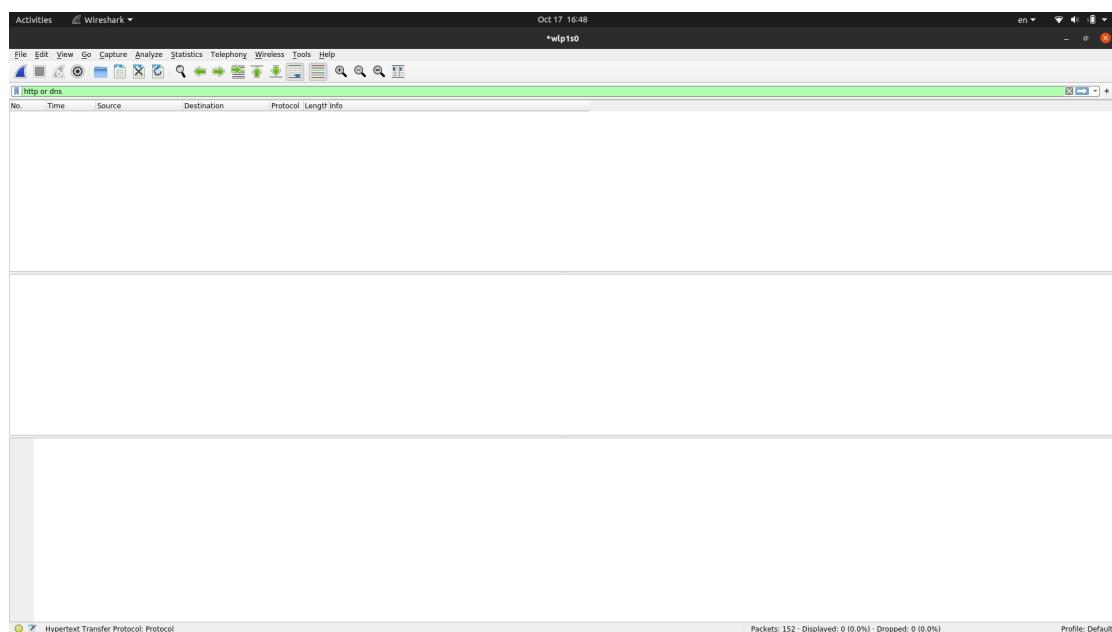
HTTP/1.1 200 OK
Date: Tue, 11 Oct 2022 14:05:46 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freedom DAV/2
Last-Modified: Sat, 08 Oct 2022 21:43:41 GMT
ETag: "18afaf-a3-5ea8cd1e01d48"
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: max-age=84600, public
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<HTML>
  <HEAD>
    <TITLE>CN Lab2</TITLE>
  </HEAD>
  <body>
    <h1>Hello labuser!</h1>
    <h2>Computer Networks 2022-23</h2>
    <h3>Lab 2</h3>
  </body>
</HTML>
```

4.16) Ονομασία πρώτης μεθόδου HTTP: GET /lab2/HTTP/1.1

4.17) Κωδικός κατάστασης που επιστρέφει ο εξυπηρετητής ιστού στην απάντησή μας: HTTP/1.1 200 OK

Επαναλαμβάνουμε την καταγραφή της διερχόμενης κίνησης με το Wireshark για τον εν λόγω ιστότοπο.



Παρατηρούμε ότι δεν ελήφθησαν/στάλθηκαν “πακέτα” DNS/HTTP.

4.18) Χρησιμότητα εκτέλεσης της εντολής sudo systemd-resolve --flush-caches: **Καθαρισμός της μνήμης cache.**

Σε περίπτωση που έχουμε ξαναεπισκεφτεί την σελίδα, αυτή έχει φορτωθεί στην μνήμη και δεν χρειάζεται να ξαναληφθούν τα δεδομένα του ιστοτόπου.