



ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

1η Εργασία με χρήση του λογισμικού WireShark

Αριστείδης Χρονόπουλος Ρ3160194

ΕΡΩΤΗΣΕΙΣ:

1.Η ανίχνευση είχε διάρκεια 35.997847 sec.

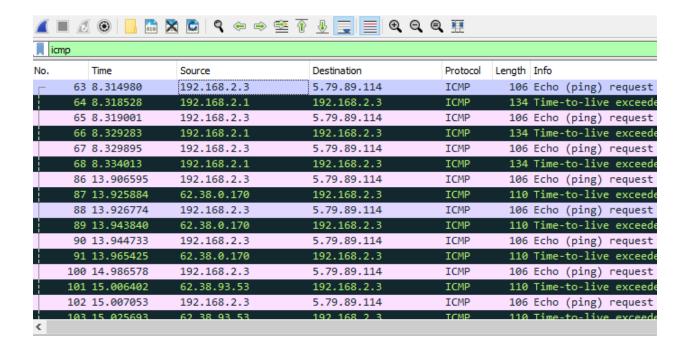
2.

NETWORK	TRANSPORT	APPLICATION
ARP	TCP	DNS
ICMP	UDP	MDNS
IGMPv.2		TLSv1.2
		QUIC
		SSDP

3. UDP χρησιμοποιούν τα εξής πρωτόκολλα: DNS, MDNS, SSDP, QUIC.

TCP χρησιμοποιούν τα εξής πρωτόκολλα: TLSv1.2.

4. Για να δούμε μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP χρησιμοποιούμε το φίλτρο icmp στο αντίστοιχο filter πεδίο.



- **5. a.** H ip διεύθυνση του destination ειναι: 5.79.89.114.
 - **b.**To time-to-live του πακέτου ειναι 1.
 - **c.** To data length είναι 64 bytes.

```
▼ Internet Protocol Version 4, Src: 192.168.2.3, Dst: 5.79.89.114

     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 92
     Identification: 0xc110 (49424)
   > Flags: 0x00
     Fragment Offset: 0
  > Time to Live: 1
     Protocol: ICMP (1)
     Header Checksum: 0x0000 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.2.3
     Destination Address: 5.79.89.114

▼ Internet Control Message Protocol

     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0xf56b [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
     Sequence Number (BE): 659 (0x0293)
     Sequence Number (LE): 37634 (0x9302)
   > [No response seen]
  > Data (64 bytes)
```

6. a. H ip διεύθυνση του destination είναι: 192.168.2.3

b. Η ip διεύθυνση του source είναι: 192.168.2.1

No.	Time	Source	Destination	Protocol	Length	Info
6	8.314980	192.168.2.3	5.79.89.114	ICMP	106	Echo (ping) request :
6	4 8.318528	192.168.2.1	192.168.2.3	ICMP	134	Time-to-live exceeded

7.

- 192.168.2.1
- 62.38.0.170
- 62.38.93.53

- 62.38.96.150
- 195.89.103.69
- 195.2.2.70
- 195.2.21.57
- 195.2.14.166
- 89.149.143.178
- 46.33.78.21
- 81.17.34.23
- 81.17.33.139
- 5.79.78.212

Παρατηρούμε οτι τα πρώτα 13 ip's απο το cmd είναι ίδια με το wireshark.

```
Tracing route to www.acm.org [5.79.89.114]
over a maximum of 30 hops:
                        4 ms vodafone.station [192.168.2.1]
       3 ms
               10 ms
                       20 ms loopback2004.med01.dsl.hol.gr [62.38.0.170]
 2
      19 ms
               17 ms
 3
                       18 ms 62.38.93.53
      19 ms
              18 ms
                       17 ms 62.38.96.150
      28 ms
              20 ms
      17 ms
              17 ms
                       18 ms ae3-100-ucr.ata.cw.net [195.89.103.69]
 6
      18 ms
              18 ms
                       17 ms dtag.dus.cw.net [195.2.2.70]
                       35 ms 195.2.21.57
      37 ms
               35 ms
                       38 ms gtt-gw.sof.cw.net [195.2.14.166]
 8
      38 ms
               36 ms
            65 ms 64 ms ae17.cr2-ams2.ip4.gtt.net [89.149.143.178]
 9
      65 ms
10
      68 ms
            66 ms 67 ms ip4.gtt.net [46.33.78.21]
11
      65 ms
            65 ms
                       66 ms be-11.cr02.ams-01.nl.leaseweb.net [81.17.34.23]
12
      64 ms
              64 ms
                       65 ms
                              po-1004.ce02.ams-01.nl.leaseweb.net [81.17.33.139]
13
               65 ms
                       65 ms 5.79.78.212
      66 ms
14
      66 ms
               72 ms
                              5.79.89.114
               64 ms
                       63 ms 5.79.89.114
15
      63 ms
Trace complete.
```