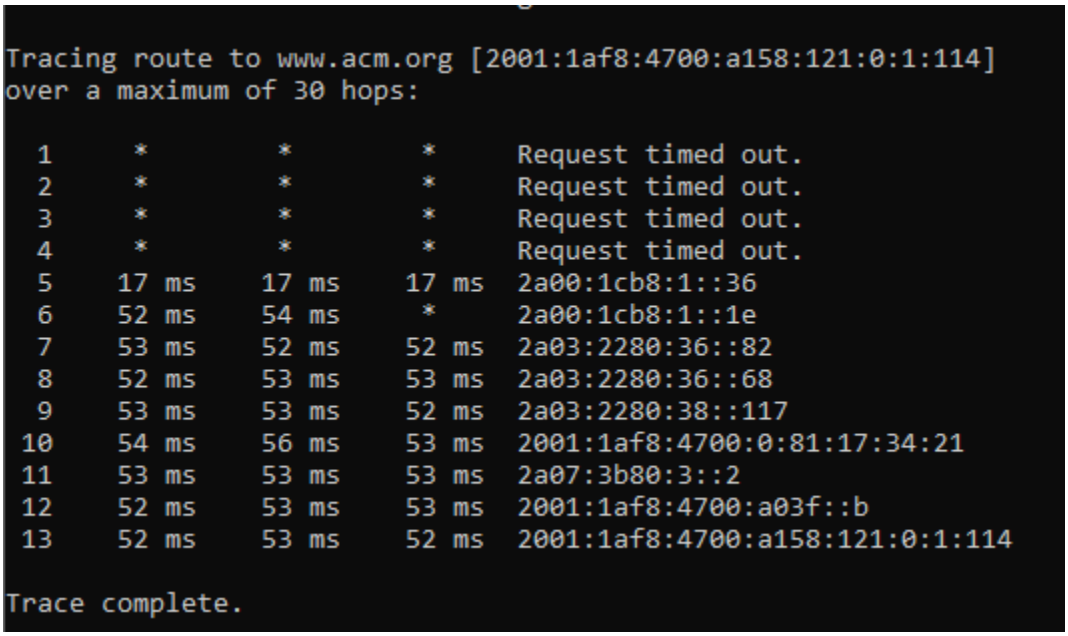
Εργασία 1 Wireshark

Δημήτριος Τσιομπίκας 3180223

Φωτογραφία εντολής tracert.



```
Tracing route to www.acm.org [2001:1af8:4700:a158:121:0:1:114]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5    17 ms    17 ms    17 ms  2a00:1cb8:1::36
  6    52 ms    54 ms     *     2a00:1cb8:1::1e
  7    53 ms    52 ms    52 ms  2a03:2280:36::82
  8    52 ms    53 ms    53 ms  2a03:2280:36::68
  9    53 ms    53 ms    52 ms  2a03:2280:38::117
 10    54 ms    56 ms    53 ms  2001:1af8:4700:0:81:17:34:21
 11    53 ms    53 ms    53 ms  2a07:3b80:3::2
 12    52 ms    53 ms    53 ms  2001:1af8:4700:a03f::b
 13    52 ms    53 ms    52 ms  2001:1af8:4700:a158:121:0:1:114

Trace complete.
```

[Ερώτηση 1]

Ο χρόνος ανίχνευσης ήταν 72.762954 δευτερόλεπτα.

Ερώτηση 2

Τα πρωτόκολλα που βρήκα ήταν : TCP , TLS v1.2 , TLS v1.3, DNS, ICMPv6, ARP, SSDP, UDP, HTTP.

Επίπεδο Σύνδεσης	Επίπεδο Δικτύου	Επίπεδο Μεταφοράς	Επίπεδο Εφαρμογών
ARP	ICMPv6	UDP	TLS v1.2
	ARP	TCP	TLS v1.3
			DNS
			SSDP
			HTTP

Ερώτηση 3

TLS v1.2 : χρησιμοποιεί το UDP και TCP.

TLS v1.3 : όμοια με το v1.2

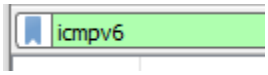
DNS : το DNS χρησιμοποιεί το UDP.

SSDP : χρησιμοποιεί το UDP.

HTTP : χρησιμοποιεί κυρίως το TCP , αλλά με προσαρμογές μπορεί να χρησιμοποιήσει και το UDP.

Ερώτηση 4

Κανονικά με αυτό το φίλτρο αλλά επειδή σε μένα «πιάστηκαν» πακέτα που είχαν μόνο ICMPv6 θα χρησιμοποιήσω αυτό :



Ερώτηση 5

a)

```
Destination Address: 2001:1af8:4700:a158:121:0:1:114
```

Πλήρης IP διεύθυνση του destination.

b)

```
Hop Limit: 1
```

c)

```
Payload Length: 72
```

```
Data (64 bytes)
    Data: 0000000000000000000000000000000000000000000000000000000000000000…
    [Length: 64]
```

Ερώτηση 6

a)

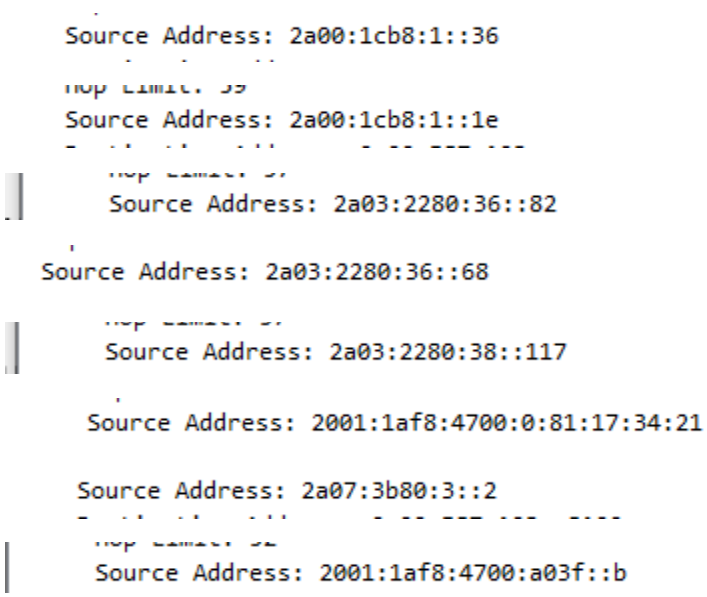
```
Destination Address: 2a02:587:123e:8100:a9cb:cb96:9865:930f
```

b)

```
Source Address: 2a00:1cb8:1::36
```

Ερώτηση 7

Βρέθηκαν 17 πακέτα με ICMP Time Exceeded μηνύματα. Κάποια είχαν ίδιες διευθύνσεις Source. Οι διευθύνσεις ήταν οι εξής :



Υπάρχει αντιστοιχία με τις παραπάνω διευθύνσεις στα Hops 5 έως 12 της εντολής tracert όπου είναι ίδιες με αυτές των πακέτων. Επίσης υπάρχει αντιστοιχία της διεύθυνσης του hop 13 με τη διεύθυνση προορισμού (destination) του πακέτου στο ερώτημα 5 a).