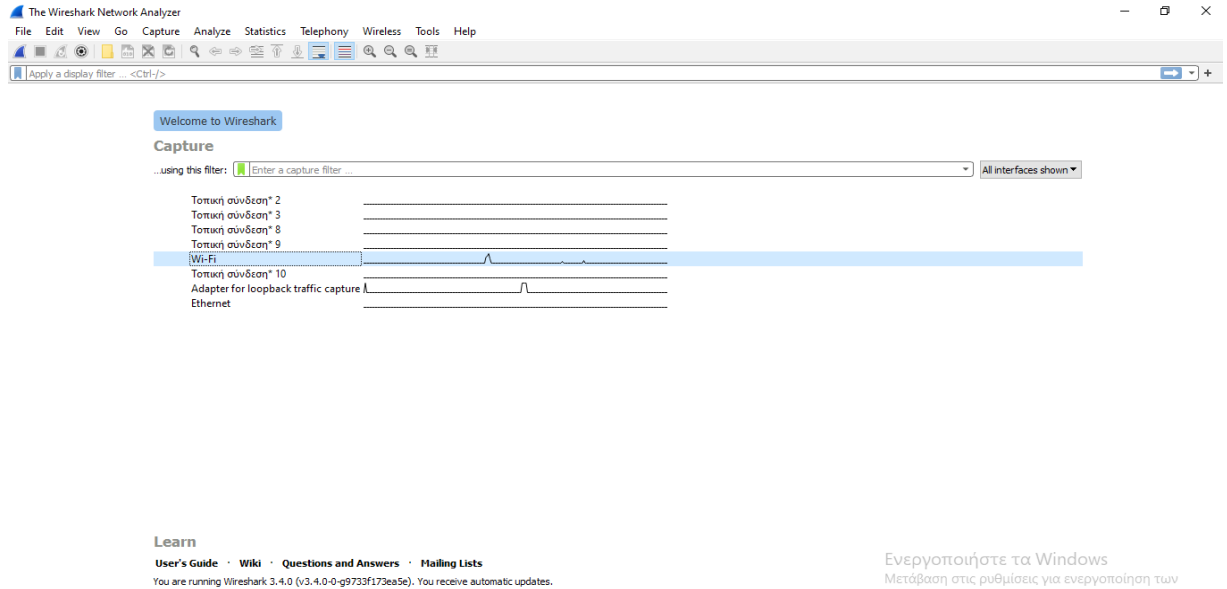


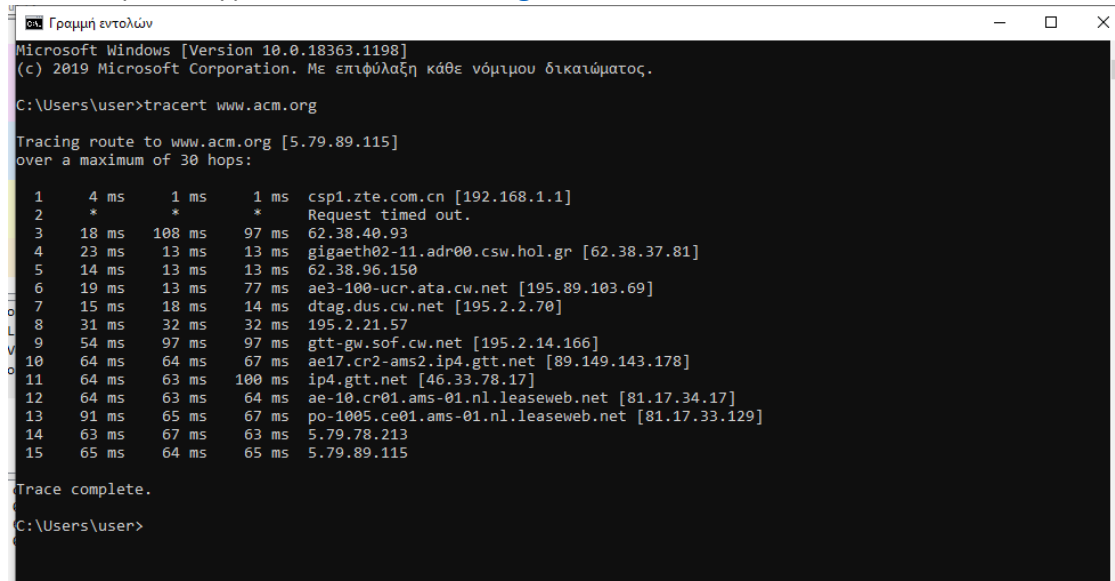
Wireshark Exercise 1

ΔΙΑΔΙΚΑΣΙΑ

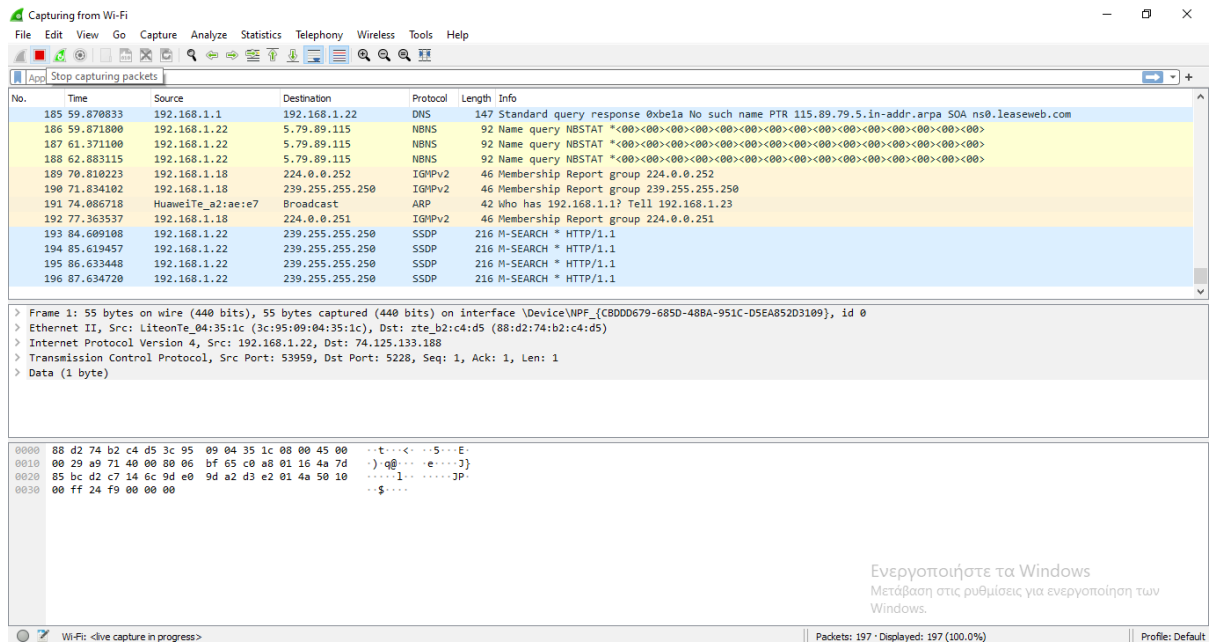
1. Έναρξη της εφαρμογής Wireshark και επιλογή interface “Wi-Fi”.



2. Εκτέλεση εντολής **tracert** www.acm.org

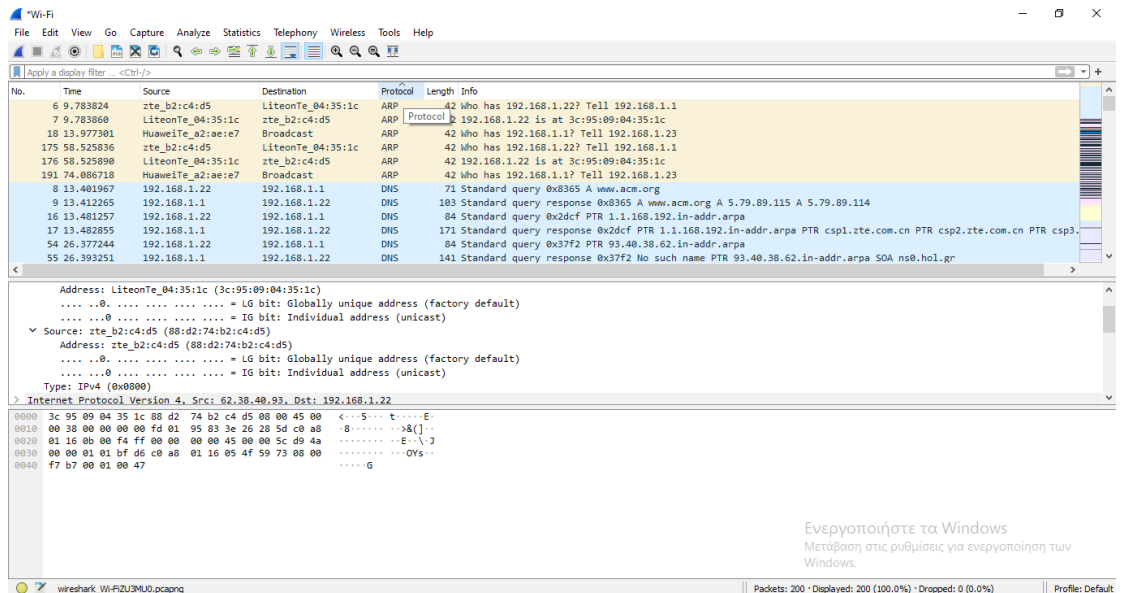


3. Διακοπή capturing



Wireshark interface showing a live capture from Wi-Fi. The packet list shows various protocols including DNS, NBNS, IGMPv2, ARP, and SSDP. The packet details pane shows the structure of an Ethernet II frame, an Internet Protocol Version 4 packet, and a Transmission Control Protocol segment. The packet bytes pane shows the raw data in hexadecimal and ASCII.

4. Εύρεση των πρωτοκόλλων που ανιχνεύτηκαν κατά την χρονική διάρκεια της ανίχνευσης, κάνοντας κλικ στο “Protocol” και εμφανίζοντας τα σε μια σειρά.



Wireshark interface showing a display filter applied to the capture. The packet list shows various protocols including ARP, DNS, and HTTP. The packet details pane shows the structure of an Internet Protocol Version 4 packet, a Transmission Control Protocol segment, and an HTTP GET request. The packet bytes pane shows the raw data in hexadecimal and ASCII.

5. Εύρεση πρωτοκόλλου μεταφοράς που χρησιμοποιεί το πρωτόκολλο εφαρμογής DNS.

[illegible]

6. Ορισμός φίλτρου “icmp” για ανίχνευση πακέτων με πρωτόκολλο ICMP.

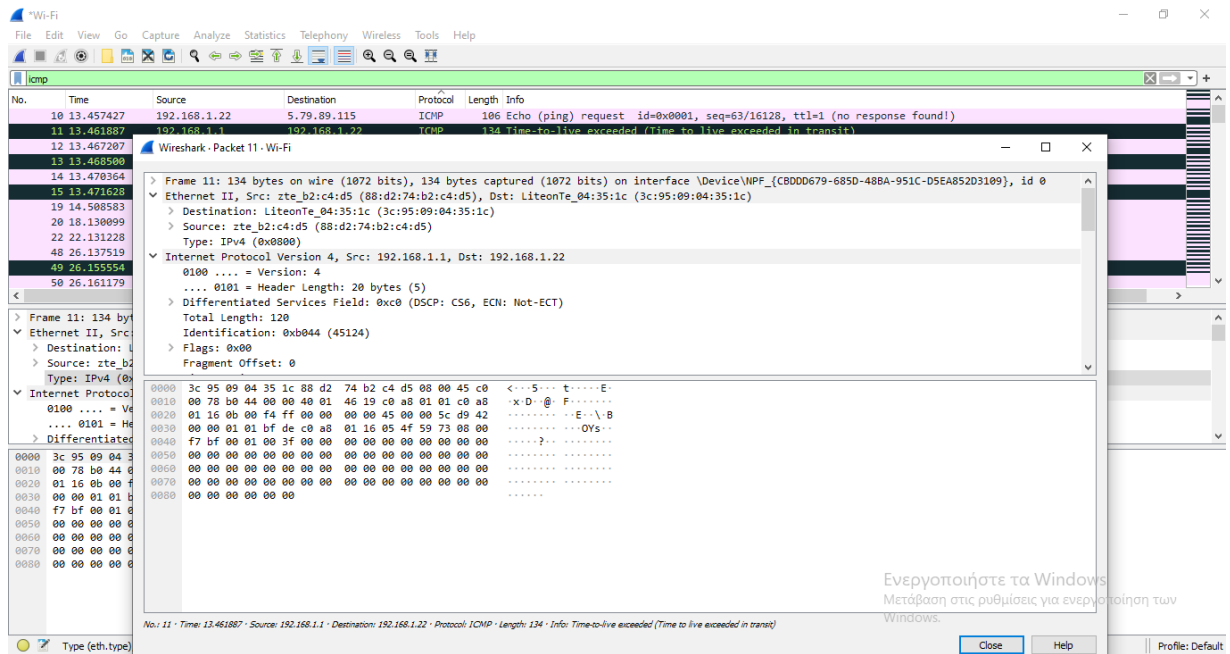
The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for common actions like opening files, saving, and zooming.

The main display area is divided into three panes:

- Packet List Pane (Top):** Shows a list of captured packets. The first packet is an ICMP Echo (ping) request from 192.168.1.22 to 5.79.89.115. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The info column indicates that the ping request timed out (134 Time-to-live exceeded).
- Packet Details Pane (Middle):** Provides a hierarchical view of the selected packet's structure. For the first packet, it shows Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol.
- Packet Bytes Pane (Bottom):** Displays the raw data of the selected packet in hexadecimal and ASCII. The hex data shows the ICMP Echo request structure, including the type, code, and identifier.

The status bar at the bottom provides summary statistics: Packets: 200, Discarded: 95 (47.5%), and Dropped: 0 (0.0%). It also shows the current profile is Default.

7. Εύρεση του πρώτου ICMP Time Exceeded.



Wireshark - Packet 11 - Wi-Fi

Frame 11: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{C80DD679-685D-488A-951C-D5EA852D3109}, id 0

Ethernet II, Src: zte_b2:c4:d5 (88:d2:74:b2:c4:d5), Dst: LiteonTe_04:35:1c (3c:95:09:04:35:1c)

Destination: LiteonTe_04:35:1c (3c:95:09:04:35:1c)

Source: zte_b2:c4:d5 (88:d2:74:b2:c4:d5)

Type: IPv4 (0x0000)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.22

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

Total Length: 120

Identification: 0xb044 (45124)

Flags: 0x00

Fragment Offset: 0

0000 3c 95 09 04 35 1c 00 d2 74 b2 c4 d5 00 00 45 c0 <...5...t...E-
0010 00 78 b0 44 00 00 40 01 46 19 c0 a8 01 01 c0 a8 x-D @: F.....
0020 01 16 00 00 f4 ff 00 00 00 45 00 00 5c d9 42E-...B
0030 00 00 01 01 bf de c0 a8 01 16 05 4f 59 73 08 00OYs...
0040 f7 bf 00 01 00 3f 00 00 00 00 00 00 00 00 00?.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

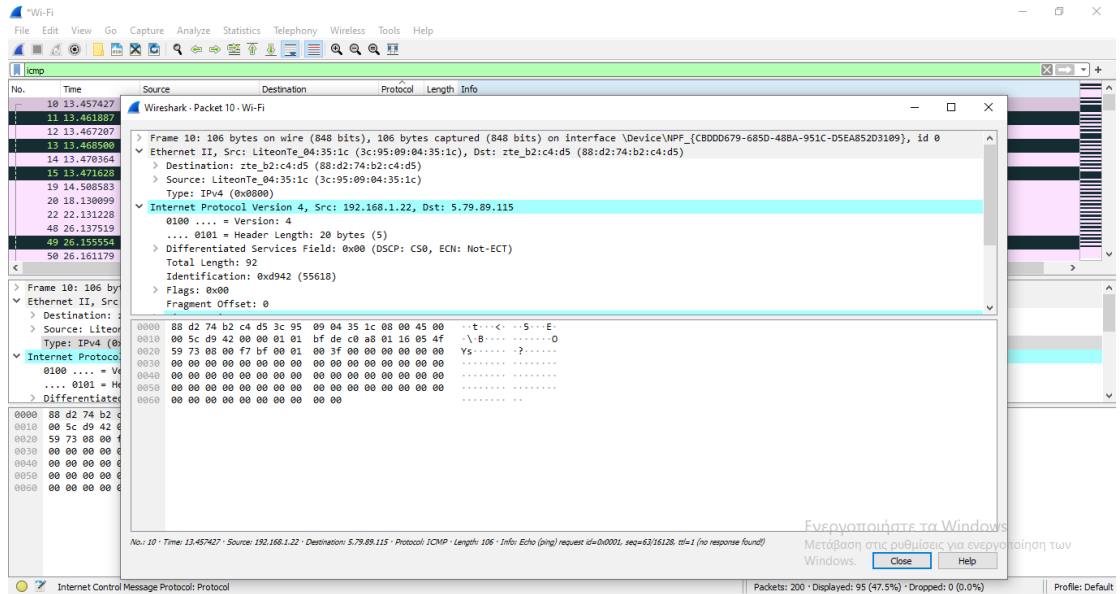
No.: 11 - Time: 13.457427 - Source: 192.168.1.1 - Destination: 192.168.1.22 - Protocol: ICMP - Length: 134 - Info: Time-to-live exceeded (Time to live exceeded in transit)

Type (eth.type)

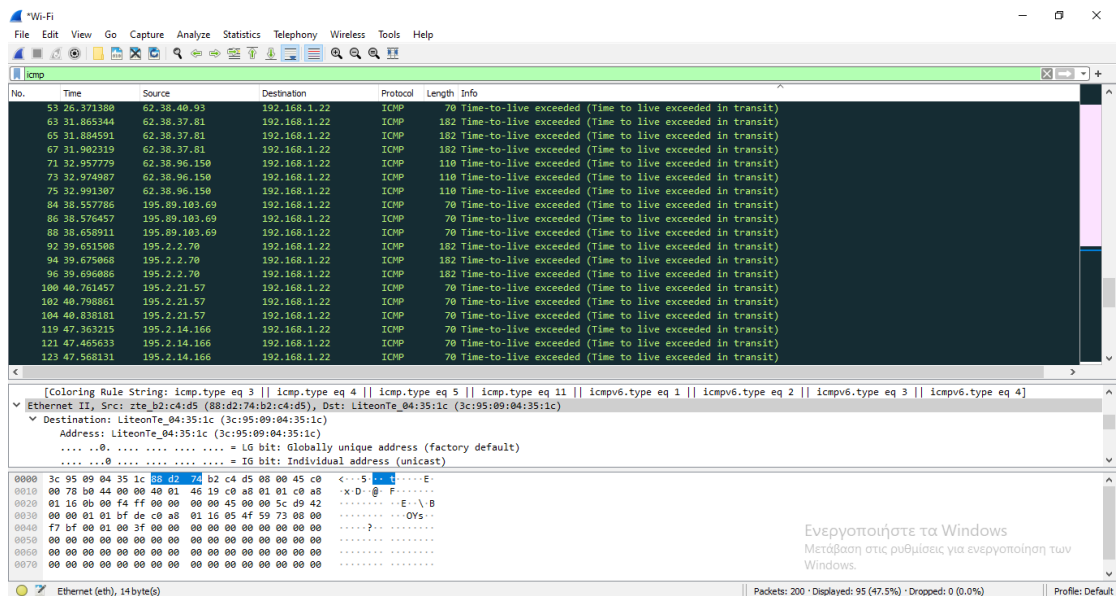
Ενεργοποιήστε τα Windows
Μετάβαση στις ρυθμίσεις για ενεργοποίηση των
Windows.

Close Help Profile: Default

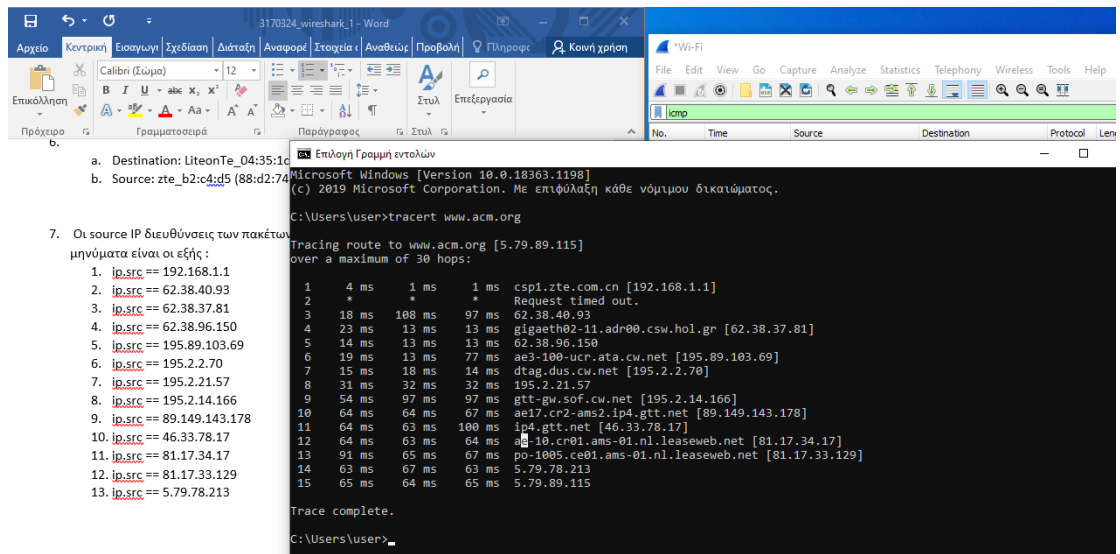
8. Εύρεση του πρώτου ICMP Echo Request



9. Ταξινόμηση τα πρωτόκολλα ICMP Time Exceeded για να αναφέρω τις source IP διευθύνσεις τους.



10. Σύγκριση για αντιστοιχία μεταξύ source IP διευθύνσεις στο wireshark με αυτές που εμφανίζονται στο command prompt.



3170324_wireshark_1 - Word

Αρχείο Κεντρική Εισαγωγή Σχεδίαση Διάταξη Αναφορές Στοιχεία Αναθεώρες Προβολή Τηλεφωνία Κοινή χρήση

Calibri (Σύμμο) 12

Επικόλληση Προέχειρο Γραμματοσειρά Παράγραφος Στυλ

Επεξεργασία

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No. Time Source Destination Protocol Len

Επιλογή Γραμμή εντολών

Microsoft Windows [Version 10.0.18363.1198]
(c) 2019 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.

C:\Users\user>tracert www.acm.org

Tracing route to www.acm.org [5.79.89.115]
over a maximum of 30 hops:

```
 1  4 ms  1 ms  1 ms  csp1.zte.com.cn [192.168.1.1]
 2  *      *      *      Request timed out.
 3  18 ms 108 ms 97 ms  62.38.40.93
 4  23 ms 13 ms 13 ms  gigaeth02-11.adr00.csw.hol.gr [62.38.37.81]
 5  14 ms 13 ms 13 ms  62.38.96.150
 6  19 ms 13 ms 77 ms  ae3-100-ucr.ata.cw.net [195.89.103.69]
 7  15 ms 18 ms 14 ms  dtag.dus.cw.net [195.2.2.70]
 8  31 ms 32 ms 32 ms  195.2.21.57
 9  54 ms 97 ms 97 ms  gtt-gw.sof.cw.net [195.2.14.166]
10  64 ms 64 ms 67 ms  ae17-cr2-ams2.ip4.gtt.net [89.149.143.178]
11  64 ms 63 ms 100 ms  ip4.gtt.net [46.33.78.17]
12  64 ms 63 ms 64 ms  a-10-cr01.ams-01.nl.leaseweb.net [81.17.34.17]
13  91 ms 65 ms 67 ms  po-1005.ce01.ams-01.nl.leaseweb.net [81.17.33.129]
14  63 ms 67 ms 63 ms  5.79.78.213
15  65 ms 64 ms 65 ms  5.79.89.115
```

Trace complete.

C:\Users\user>

7. Οι source IP διευθύνσεις των πακέτων μηνύματα είναι οι εξής:

1. `ip.src == 192.168.1.1`
2. `ip.src == 62.38.40.93`
3. `ip.src == 62.38.37.81`
4. `ip.src == 62.38.96.150`
5. `ip.src == 195.89.103.69`
6. `ip.src == 195.2.2.70`
7. `ip.src == 195.2.21.57`
8. `ip.src == 195.2.14.166`
9. `ip.src == 89.149.143.178`
10. `ip.src == 46.33.78.17`
11. `ip.src == 81.17.34.17`
12. `ip.src == 81.17.33.129`
13. `ip.src == 5.79.78.213`

ΕΡΩΤΗΣΕΙΣ

1. Η χρονική διάρκεια της ανίχνευσης μου ήταν “91.791759”.
- 2.

Πρωτόκολλα	Επίπεδο
ARP	Δικτύου
DNS	Εφαρμογής
ICMP	Δικτύου
ICMPv6	Δικτύου
ICMPv2	Δικτύου
NBNS	
SSDP	
TCP	Μεταφοράς
TLSv1.2	Δικτύου

3. Το πρωτόκολλο επιπέδου εφαρμογής DNS χρησιμοποιεί το UDP πρωτόκολλο επιπέδου μεταφοράς.(Διαδικασία 5).
4. Το φίλτρο που χρησιμοποίησα για να εμφανίζονται στο παράθυρο του wireshark μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το

πρωτόκολλο ICMP είναι το "icmp".(όπως φαίνεται και στο 5^ο βήμα της διαδικασίας που ακολούθησα).

5.
 - a. Destination: zte_b2:c4:d5 (88:d2:74:b2:c4:d5)
 - b. [Expert Info (Note/Sequence): "Time To Live" only 1]
 - c. [Length: 64]
6.
 - a. Destination: LiteonTe_04:35:1c (3c:95:09:04:35:1c)
 - b. Source: zte_b2:c4:d5 (88:d2:74:b2:c4:d5)
7. Οι source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα είναι οι εξής :
 1. ip.src == 192.168.1.1
 2. ip.src == 62.38.40.93
 3. ip.src == 62.38.37.81
 4. ip.src == 62.38.96.150
 5. ip.src == 195.89.103.69
 6. ip.src == 195.2.2.70
 7. ip.src == 195.2.21.57
 8. ip.src == 195.2.14.166
 9. ip.src == 89.149.143.178
 10. ip.src == 46.33.78.17
 11. ip.src == 81.17.34.17
 12. ip.src == 81.17.33.129
 13. ip.src == 5.79.78.213

Όπως φαίνεται και στο screenshot του βήματος 10 στην διαδικασία που ακολούθησα πιο πάνω ,υπάρχει η αντιστοιχία των IP διευθύνσεων εκτός της τελευταίας στο command prompt «5.79.89.115».