

ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ

1^Η ΕΡΓΑΣΙΑ

Σιγούρου Άλκηστις Αικατερίνη ΑΜ: 1059661

A ΜΕΡΟΣ

1. nslookup www.ceid.upatras.gr

```
C:\Users\DELL>nslookup www.ceid.upatras.gr
Server: UnKnown
Address: 192.168.1.254

Non-authoritative answer:
Name:    web.ceid.upatras.gr
Address: 150.140.141.173
Aliases: www.ceid.upatras.gr
```

Η nslookup μας προσφέρει πληροφορίες ,σχετικές με την διεύθυνση που της ζητάμε να ψάξει . Μας επιστρέφει το όνομα ,όπως είναι στο A record την IP address , καθώς και το ψευδώνυμο που μπορεί να έχει

2. Ifconfig

```
sigourou@sigourou-Inspiron-3581:~$ ifconfig
enp1s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        ether d8:d0:90:00:20:1e txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 1537 bytes 134936 (134.9 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1537 bytes 134936 (134.9 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.8 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::2f32:60e4:adc1:e54a prefixlen 64 scopeid 0x20<link>
        ether 10:5b:ad:03:9e:1f txqueuelen 1000 (Ethernet)
        RX packets 138877 bytes 187618103 (187.6 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 89201 bytes 12415268 (12.4 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Η ifconfig περιέχει πληροφορίες για την IP διεύθυνση και την μάσκα του δικτύου του υπολογιστή μας .

3. Ipconfig \all .

```
USAGE:
ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid] ]

where
adapter      Connection name
              (wildcard characters * and ? allowed, see examples)

Options:
/?           Display this help message
/all         Display full configuration information.
/release     Release the IPv4 address for the specified adapter.
/release6    Release the IPv6 address for the specified adapter.
/renew       Renew the IPv4 address for the specified adapter.
/renew6      Renew the IPv6 address for the specified adapter.
/flushdns    Purges the DNS Resolver cache.
/registerdns Refreshes all DHCP leases and re-registers DNS names
/displaydns  Display the contents of the DNS Resolver Cache.
/showclassid Displays all the dhcp class IDs allowed for adapter.
/setclassid  Modifies the dhcp class id.
/showclassid6 Displays all the IPv6 DHCP class IDs allowed for adapter.
/setclassid6 Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.
```

Μας δίνει τα options που μπορούμε να συνδυάσουμε με την εντολή ipconfig , καθώς και μια επεξήγηση για το τι κάνουμε με την κάθε μία . Αποτελει το λεγόμενο help directory των εντολών . Μερικά από αυτά είναι και τα /displaydns και /flushdns τα οποία εκτελούμε παρακάτω

4. Ipconfig /displaydns

```
C:\Users\DELL>ipconfig /displaydns

Windows IP Configuration

www.gstatic.com
-----
Record Name . . . . . : www.gstatic.com
Record Type . . . . . : 1
Time To Live . . . . . : 44
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 172.217.17.163

Record Name . . . . . : ns2.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 44
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . . : 216.239.34.10

Record Name . . . . . : ns2.google.com
Record Type . . . . . : 28
Time To Live . . . . . : 44
Data Length . . . . . : 16
Section . . . . . : Additional
AAAA Record . . . . . : 2001:4860:4802:34::a

Record Name . . . . . : ns1.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 44
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . . : 216.239.32.10
```

Μας δίνει τα dns μηνύματα που έχουν ανταλλαχθεί το τελευταίο διάστημα προς την Ip address μου. Δίπλα δίνεται ένα μικρό παράδειγμα από αυτά . Όπως παρατηρούμε , έχουμε πληροφορίες για τα :

Record Name

Record Type

Time To Live

Data Length

Section

(Type) Record

5. Ipconfig /flushdns

```
C:\Users\DELL>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Με αυτήν την εντολή ,καθαρίζουμε την cache του Recursive resolver , που είναι ο nameserver που έρχεται σε άμεση επαφή με τον DNS nameserver .

1. Αφού σταματήσουμε την καταγραφή στο Wireshark ,παρατηρούμε πληθώρα πακέτων . Για να επιλέξουμε μόνο τα πακέτα DNS , στο πεδίο των φίλτρων πέρα από την IP διεύθυνση μας προσθέτουμε και && dns . Στο δικό μου παράδειγμα καταλήξαμε στα εξής 4 :

No.	Time	Source	Destination	Protocol	Length	Info
4	1.809855251	192.168.1.8	192.168.1.254	DNS	72	Standard query 0x1108 A www.ietf.org
5	1.918798471	192.168.1.254	192.168.1.8	DNS	459	Standard query response 0x1108 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85 NS ns3.cloud...
421	4.752552362	192.168.1.8	192.168.1.254	DNS	78	Standard query 0x9816 A analytics.ietf.org
534	4.985271967	192.168.1.254	192.168.1.8	DNS	265	Standard query response 0x9816 A analytics.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.sea1.afillias-nst.info NS ns1.yyz1.af...

Σύμφωνα με το screenshot έχουμε 4 πακέτα , 2 ερωτήσεις και 2 απαντήσεις .

2. Το κάθε πακέτο αποτελείται από τα πεδία :

- **Frame (No. package)**, σε αυτό το πεδίο έχουμε πληροφορίες σχετικά με το Interface id, τι τύπου ενθυλάκωσης χρησιμοποιεί το μήνυμα, το timestamp της παραλαβή του μηνύματος, επίσης έχουμε το Epoch timestamp , το οποίο μετράει τον χρόνο που έχει περάσει σε δευτερόλεπτα από την στιγμή 0 στα Unix συστήματα (1^η Ιανουαρίου 1970). Έχουμε ακόμα το νούμερο του Frame ,δηλαδή σε ποια σειρά καταγράφηκε το συγκεκριμένο πακέτο από το Wireshark, όπως και το μέγεθος του Frame και του capture. Και τέλος έχουμε μια αναφορά των πρωτοκόλλων που χρησιμοποιούνται .
- **Ethernet II, Src, Dst**, σε αυτό το πεδίο έχουμε πληροφορίες σχετικά με την διεύθυνση του οικιακού μας router και του router με τον οποίο κάναμε διασύνδεση ,καθώς και τύπου IP διεύθυνση είναι η πηγή.
- **Internet Protocol Version 4, Src, Dst** , σε αυτό το πεδίο έχουμε πληροφορίες σχετικά με το IP Header. Μας δίνει ποιο version Ip έχουμε , ποιο είναι το μέγεθος του Header , τα Differentiated Services και ποιο είναι το συνολικό μέγεθος με αυτά .Έχουμε επίσης το identification και πληροφορίες για τα Flags , πιο είναι το fragment offset , πόσος είναι ο χρόνος TTL ,πιο πρωτόκολλο χρησιμοποιείται στην συνέχεια στο επίπεδο μεταφοράς και πιο είναι το header checksum
- **User Datagram Protocol, Src Port , Dst Port**, σε αυτό το πεδίο έχουμε πληροφορίες σχετικά με την θύρα αποστολής και την θύρα πηγή του πακέτου , το μέγεθος του , καθώς και το checksum.
- **Domain Name System ()**, σε αυτό το πεδίο έχουμε πληροφορίες σχετικά με το αν το πακέτο μας είναι τύπου ερώτησης (query) ή απάντησης (response) . Βλέπουμε το ID με το οποίο έγινε η επικοινωνία , τα flags του dns header , όπως και μας δίνει το πλήθος των ερωτήσεων και απαντήσεων που περιέχει το μήνυμα . Επιπλέον έχουμε το πλήθος των resource records στο πεδίο της απάντησης. Και το πλήθος των resource records στο επιπρόσθετο resource πεδίο.

Για τα DNS μηνύματα χρησιμοποιήθηκε το πρωτόκολλο UDP και αυτό μπορούμε να το δούμε στο πεδίο IPv4 στην υποενότητα Protocol

STANDAR QUERY

▶ Frame 4: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface wlp2s0, id 0		
▶ Ethernet II, Src: MegaWell_03:9e:1f (10:5b:ad:03:9e:1f), Dst: Tp-LinkT_0d:e3:d8 (34:e8:94:0d:e3:d8)		
▶ Internet Protocol Version 4, Src: 192.168.1.8, Dst: 192.168.1.254		
▶ User Datagram Protocol, Src Port: 42680, Dst Port: 53		
▶ Domain Name System (query)		
0000	34 e8 94 0d e3 d8 10 5b ad 03 9e 1f 08 00 45 00	4[.....E·
0010	00 3a 74 08 40 00 00 11 42 54 c0 a8 01 08 c0 a8	·:t·@·@· BT·.....
0020	01 fe a6 b8 00 35 00 26 84 8e 11 08 01 00 00 015·&
0030	00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03w ww·ietf·
0040	6f 72 67 00 00 01 00 01	org·.....

STANDAR RESPONSE

```
▶ Frame 5: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface wlp2s0, id 0
▶ Ethernet II, Src: Tp-LinkT_0d:e3:d8 (34:e8:94:0d:e3:d8), Dst: MegaWell_03:9e:1f (10:5b:ad:03:9e:1f)
▶ Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.8
▶ User Datagram Protocol, Src Port: 53, Dst Port: 42680
▶ Domain Name System (response)
```

```
0000 10 5b ad 03 9e 1f 34 e8 94 0d e3 d8 08 00 45 00 .[...4...E...
0010 01 bd a6 ff 00 00 40 11 4d da c0 a8 01 fe c0 a8 .....@..M.....
0020 01 08 00 35 a6 b8 01 a9 d4 d9 11 08 81 80 00 01 ....S.....
0030 00 03 00 05 00 0a 03 77 77 77 04 69 65 74 66 03 .....w ww.ietf.
0040 6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00 org.....
0050 01 51 00 21 03 77 77 77 04 69 65 74 66 03 6f 72 .Q! www.ietf.or
0060 67 03 63 64 6e 0a 63 6c 6f 75 64 66 6c 61 72 65 g.cdn.cl oudflare
0070 03 6e 65 74 00 c0 2a 00 01 00 01 00 00 01 2c 00 .net.*.....
0080 04 68 14 00 55 c0 2a 00 01 00 01 00 00 01 2c 00 .h.U.*.....
0090 04 68 14 01 55 c0 3b 00 02 00 01 00 00 49 52 00 .h.U.; ....IR.
00a0 06 03 6e 73 33 c0 3b c0 3b 00 02 00 01 00 00 49 .ns3; ; .....I
00b0 52 00 06 03 6e 73 32 c0 3b c0 3b 00 02 00 01 00 R..ns2; ; .....
00c0 00 49 52 00 06 03 6e 73 31 c0 3b c0 3b 00 02 00 .IR..ns 1; ; ....
00d0 01 00 00 49 52 00 06 03 6e 73 35 c0 3b c0 3b 00 .IR...ns5; ; ....
00e0 02 00 01 00 00 49 52 00 06 03 6e 73 34 c0 3b c0 .IR...ns4; ; ....
00f0 9b 00 01 00 01 00 00 00 ea 00 04 ad f5 3b 1f c0 .....$....
0100 9b 00 1c 00 01 00 00 00 ea 00 10 24 00 cb 00 20 .....$....
0110 49 00 01 00 00 00 00 ad f5 3b 1f c0 09 00 01 00 I.....).....
0120 01 00 00 02 92 00 04 c6 29 de 83 c0 09 00 1c 00 .....$....I...
0130 01 00 00 02 93 00 10 24 00 cb 00 20 49 00 01 00 .....$....I...
0140 00 00 00 c6 29 de 83 c0 77 00 01 00 01 00 00 00 .....$....I...
0150 8f 00 04 c6 29 de 1f c0 77 00 1c 00 01 00 00 00 .....$....I...
0160 8f 00 10 24 00 cb 00 20 49 00 01 00 00 00 00 c6 .....$....I...
0170 29 de 1f c0 bf 00 01 00 01 00 00 00 ad 00 04 c6 .....$....I...
0180 29 df 83 c0 bf 00 1c 00 01 00 00 00 ad 00 10 24 .....$....I...
0190 00 cb 00 20 49 00 01 00 00 00 c6 29 df 83 c0 .....$....I...
01a0 ad 00 01 00 01 00 00 03 20 00 04 c6 29 df 1f c0 .....$....I...
01b0 ad 00 1c 00 01 00 00 03 20 00 10 24 00 cb 00 20 .....$....I...
01c0 49 00 01 00 00 00 00 c6 29 df 1f .....$....I...)
```

3. Η θύρα προορισμού για το μήνυμα του DNS query είναι η: port 53

```
▼ User Datagram Protocol, Src Port: 42680, Dst Port: 53
  Source Port: 42680
  Destination Port: 53
  Length: 38
  Checksum: 0x848e [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  ▼ [Timestamps]
    [Time since first frame: 0.000000000 seconds]
    [Time since previous frame: 0.000000000 seconds]
```

4. Η θύρα προέλευσης για το μήνυμα του DNS response είναι η : port 53

```
▼ User Datagram Protocol, Src Port: 53, Dst Port: 42680
  Source Port: 53
  Destination Port: 42680
  Length: 425
  Checksum: 0xd4d9 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  ▼ [Timestamps]
    [Time since first frame: 0.108935220 seconds]
    [Time since previous frame: 0.108935220 seconds]
```

5. Το μήνυμα DNS ερώτησης (query) στάλθηκε στη διεύθυνση IP 192.168.1.254 που είναι η διεύθυνση IP του τοπικού μου προκαθορισμένου διακομιστή DNS

```
▼ Internet Protocol Version 4, Src: 192.168.1.8, Dst: 192.168.1.254
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 58
  Identification: 0x7408 (29704)
  ► Flags: 0x4000, Don't fragment
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x4254 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.8
  Destination: 192.168.1.254
```

, όπως φαίνεται αν τρέξουμε την εντολή ifconfig .

6. Στο Frame 4 , ο τύπος του μηνύματος DNS ερώτησης (query) είναι Standard Query Type: A (Host address) και δεν περιέχει καμία απάντηση (Answer RRs: 0)

```
▼ Domain Name System (query)
  Transaction ID: 0x1108
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..0.. .... = Z: reserved (0)
    .... ..0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ► Queries
    [Response In: 5]
```

7. Παρέχονται 3 απαντήσεις

Στις απαντήσεις περιέχονται πληροφορίες για το τι τύπο μηνύματος έχουμε (εάν είναι CNAME ή A) ,σε τι κλάση ανήκει και ποια είναι η IP διεύθυνση του συνδέσμου . Σε περίπτωση τύπου CNAME , το οποίο μας λέει ότι το url που πληκτρολογήσαμε είναι ψευδώνυμο (alias) , μας επιστρέφει αντί για την IP address , το πραγματικό όνομα στο A records .

```
▼ Domain Name System (response)
  Transaction ID: 0x1108
  ▼ 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: 3
  Authority RRs: 5
  Additional RRs: 10
  ▼ Queries
    ► www.ietf.org: type A, class IN
  ▼ Answers
    ► www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    ► www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    ► www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  ▼ Authoritative nameservers
```

8. Η διεύθυνση προορισμού του πακέτου SYN (SYN packet ή SYN segment) που στέλνει το TCP που τρέχει στον host αντιστοιχεί στη διεύθυνση IP 104.20.1.85 του server www.ietf.org.cdn.cloudflare.net που παρέχεται στην 3^η απάντηση του DNS απόκρισης.

```

5 1.918798471 192.168.1.254 192.168.1.8 DNS 459 Standard query response 0x1188 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.8
6 1.919399598 192.168.1.8 104.20.1.85 TCP 74 35260 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2902775196 TSecr=0 WS=128
7 1.919650275 192.168.1.8 104.20.1.85 TCP 74 35262 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2902775196 TSecr=0 WS=128
8 1.919650275 192.168.1.8 104.20.1.85 TCP 74 35262 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2902775196 TSecr=0 WS=128
Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp2s0, id 0
Ethernet II, Src: MegaWell_03:9e:1f (10:5b:ad:03:9e:1f), Dst: Tp-LinkT_0d:e3:d8 (34:e8:94:0d:e3:d8)
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 104.20.1.85
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 60
Identification: 0xbae9 (47849)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x54b9 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.8
Destination: 104.20.1.85

```

Αφού έτρεξε την εντολή nslookup www.ceid.upatras.gr η αναζήτηση μου εντόπισε 4 πακέτα DNS 2 ερωτήσεις και 2 απαντήσεις .

No.	Time	Source	Destination	Protocol	Length	Info
27	19.887123843	192.168.1.8	192.168.1.254	DNS	79	Standard query 0xe6e0 A www.ceid.upatras.gr
28	19.927364264	192.168.1.254	192.168.1.8	DNS	187	Standard query response 0xe6e0 A www.ceid.upatras.gr CNAME web.ceid.upatras.gr A 150.140.141.173 NS NIC.upatras.gr NS FOO.up...
29	19.929030001	192.168.1.8	192.168.1.254	DNS	79	Standard query 0x48fe AAAA web.ceid.upatras.gr
30	19.964967527	192.168.1.254	192.168.1.8	DNS	123	Standard query response 0x48fe AAAA web.ceid.upatras.gr SOA NIC.upatras.gr

Αγνοούμε το πρώτο ζευγάρι και αναλύουμε το 2^ο .

9. Η θύρα προορισμού στο μήνυμά ερώτησης είναι η port 53 .

- ▼ User Datagram Protocol, Src Port: 42680, Dst Port: 53
 - Source Port: 42680
 - Destination Port: 53
 - Length: 38
 - Checksum: 0x848e [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 1]
 - ▼ [Timestamps]
 - [Time since first frame: 0.000000000 seconds]
 - [Time since previous frame: 0.000000000 seconds]

Η οποία είναι η ίδια με την θύρα προέλευσης στο μήνυμά απόκρισης

- ▼ User Datagram Protocol, Src Port: 53, Dst Port: 44616
 - Source Port: 53
 - Destination Port: 44616
 - Length: 89
 - Checksum: 0x69ea [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 4]
 - ▼ [Timestamps]
 - [Time since first frame: 0.035937526 seconds]
 - [Time since previous frame: 0.035937526 seconds]

10. Το μήνυμά ερώτησης φεύγει από την IP 192.168.1 και καταλήγει στην IP 192.168.1.254 , που είναι η διεύθυνσης IP του προεπιλεγμένου τοπικού διακομιστή dns

```

Internet Protocol Version 4, Src: 192.168.1.8, Dst: 192.168.1.254
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 65
Identification: 0xacbd (44221)
Flags: 0x4000, Don't fragment
0... .. = Reserved bit: Not set
.1.. .. = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x0998 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.8
Destination: 192.168.1.254

```


11. Το DNS ερώτημα είναι Type : AAAA και δεν περιέχει καμία απάντηση

```
▼ Domain Name System (query)
  Transaction ID: 0x1108
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    ....0... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    .... ..0... .. = Z: reserved (0)
    .... ..0... .. = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▶ Queries
    [Response In: 5]
```

12. Το DNS απάντηση επίσης δεν περιέχει καμία απάντηση

```
▼ Domain Name System (response)
  Transaction ID: 0x48fe
  ▼ 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: 0
  Authority RRs: 1
  Additional RRs: 0
  ▼ Queries
    ▶ web.ceid.upatras.gr: type AAAA, class IN
  ▶ Authoritative nameservers
    [Request In: 29]
    [Time: 0.035937526 seconds]
```

, αλλά το άλλο DNS απάντηση (Frame 28) περιέχει 2 απαντήσεις .

```
▶ Frame 28: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits) on interface wlp2s0, id 0
▶ Ethernet II, Src: Tp-LinkT_0d:e3:d8 (34:e8:94:0d:e3:d8), Dst: MegaWell_03:9e:1f (10:5b:ad:03:9e:1f)
▶ Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.8
▶ User Datagram Protocol, Src Port: 53, Dst Port: 36924
▼ Domain Name System (response)
  Transaction ID: 0xe6e0
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 2
  Additional RRs: 2
  ▼ Queries
    ▶ www.ceid.upatras.gr: type A, class IN
  ▼ Answers
    ▶ www.ceid.upatras.gr: type CNAME, class IN, cname web.ceid.upatras.gr
    ▶ web.ceid.upatras.gr: type A, class IN, addr 150.140.141.173
  ▼ Authoritative nameservers
    ▶ ceid.upatras.gr: type NS, class IN, ns NIC.upatras.gr
    ▶ ceid.upatras.gr: type NS, class IN, ns F00.upnet.gr
  ▼ Additional records
    ▶ NIC.upatras.gr: type A, class IN, addr 150.140.129.30
    ▶ F00.upnet.gr: type A, class IN, addr 150.140.129.130
    [Request In: 27]
    [Time: 0.040240421 seconds]
```

Στις απαντήσεις περιέχονται πληροφορίες για το τι τύπο μηνύματος έχουμε (type A) ,σε τι κλάση ανήκει και ποια είναι η IP διεύθυνση του συνδέσμου .

14.

14.

ΚΕΦΑΛΙΔΑ DNS

ID							
QR	OPCODE	AA	TC	RD	RA	Z	RCODE
QDCOUNT							
ANCOUNT							
NSCOUNT							
ARCOUNT							

ID: 16-bit αναγνωριστικό, το οποίο καθορίζεται από το πρόγραμμα που γεννάει οποιοδήποτε ερώτημα. Το αναγνωριστικό αυτό μπορεί να αντιγράφει την αντίστοιχη απάντηση και μπορεί να χρησιμοποιηθεί από τον αιτούντα να ταιριάζει τις απαντήσεις στα εκκρεμή ερωτήματα .

QR: 1bit πεδίο, το οποίο διευκρινίζει εάν το μήνυμα είναι ερώτηση (0) ή είναι απάντηση (1)

OPCODE: 4-bit πεδίο, το οποίο διευκρινίζει τι είδους ερώτημα περιλαμβάνεται στο μήνυμα

AA (Authoritative Answer): 1 bit, έχει νόημα μόνο αν μιλάμε για απαντήσεις, και διευκρινίζει αν ο ανταποκριτής name server είναι ο αξιόπιστος (authority) για το domain όνομα στο πεδίο της ερώτησης.

TC(TurnCation): 1 bit, το οποίο προσδιορίζει αν το μήνυμα ήταν κομμένο.

RD (Recursion Desired): 1bit, το οποίο κατευθύνει τον name server να εξετάσει επανειλημμένα το ερώτημα.

RA (Recursion Available): 1 bit, το bit αυτό είναι είτε 1 είτε 0 στις απαντήσεις και καθορίζει αν το recursive ερώτημα υπάρχει στο name server ή όχι

Z: 3 bit, κρατούνται για μελλοντική χρήση.

RCODE (Response code): 4 bit, αποτελεί πεδίο των απαντήσεων. Οι τιμές που παίρνει έχουν τις ανάλογες ερμηνείες :

0 -> Συνθήκη ότι δεν υπήρξε error

1 -> Format error , O name server δεν μπόρεσε να μεταφράσει το ερώτημα

2 -> Server failure, O name server δεν μπόρεσε να επεξεργαστεί το ερώτημα λόγω προβλήματος που προέκυψε με τον name server

3 -> Name Error , έχει σημασία μόνο για τις απαντήσεις από έναν authoritative name server , αυτός ο κωδικός από bit προσδιορίζει ότι το domain όνομα που αναφέρεται στην ερώτηση δεν υπάρχει .

4 -> Not implemented , O name server δεν υποστηρίζει το είδος της αιτούμενης ερώτησης.

5 -> Refused , O name server αρνείται να εκτελέσει την συγκεκριμένη διαδικασία για λόγους προστασίας.

QDCOUNT: 16 bit, υποδεικνύει το πλήθος των ερωτήσεων που έχει το μήνυμα.

ANCOUNT: 16 bit, υποδεικνύει το πλήθος των απαντήσεων που διατίθενται για το ερώτημα.

NSCOUNT: 16 bit, υποδεικνύει το πλήθος των resource records στο πεδίο της απάντησης.

ARCOUNT: 16 bit, υποδεικνύει το πλήθος των resource records στο επιπρόσθετο resource πεδίο.

15. Έχουμε το παρακάτω DNS πακέτο :

Mac Header (14bytes)	48F8 B326 DF49 BABA BABA BABA 0800
IP Header (20bytes)	4500 0038 66BD 0000 8011 020C C0A8 0134 0808 0808
UDP Header (8bytes)	D539 0035 0024 448F
DNS Header	0003 0100 0001 0000 0000 0000
data	0667 6F6F 676C 6503 636F 6D00 0001 0001

Field	Sub-Field	Value	Interpretation
ID		0x0003	Η απάντηση του πρέπει να έχει ID 0x0003
Flags		0x0100	
	QR	0	Είναι ερώτηση
	OPCODE	0000	Standard query
	AA	0	Δεν είναι authoritative
	TC	0	Δεν είναι κομμένο
	RD	1	Ζητάει επανάληψη
	RA	0	Η απάντηση δεν είναι διαθέσιμη στον nameserver
	Z	000	
	RCODE	0000	Δεν υπήρξε error
QDCOUNT		0x0001	Το μήνυμα περιείχε 1 ερώτηση
ANCOUNT		0x0000	Το μήνυμα δεν περιείχε απαντήσεις
NSCOUNT		0x0000	
ARCOUNT		0x0000	

Για να βρούμε για ποιο domain ζητάει την IP πρέπει να αποκωδικοποιήσουμε το υπόλοιπο κομμάτι από το DNS Header . Έχουμε:

0x06 -> Το επόμενο string έχει μήκος 6 bytes

0x676F6F676C65 -> google

0x03 -> Το επόμενο string έχει μήκος 3 bytes

0x63676D -> com

0x00 -> Η διεύθυνση τελείωσε.

Επομένως το domain είναι το google.com

16. Έχουμε το παρακάτω frame :

Mac Header (14bytes)	BABA BABA BABA 48F8 B326 DF49 0800
IP Header (20bytes)	4508 00E8 B2EF 0000 3711 FE21 0808 0808 C0A8 0134
UDP Header (8bytes)	0035 D539 00D4 28A2
DNS Header	0003 8180 0001 000B 0000 0000
Data	0667 6F6F 676C 6503 636F 6D00 0001 0001
Απάντηση 1	C00C 0001 0001 0000 0004 0004 4A7D EC23
Απάντηση 2	C00C 0001 0001 0000 0004 0004 4A7D EC25
Απάντηση 3	C00C 0001 0001 0000 0004 0004 4A7D EC27
Απάντηση 4	C00C 0001 0001 0000 0004 0004 4A7D EC20
Απάντηση 5	C00C 0001 0001 0000 0004 0004 4A7D EC28
Απάντηση 6	C00C 0001 0001 0000 0004 0004 4A7D EC21
Απάντηση 7	C00C 0001 0001 0000 0004 0004 4A7D EC29
Απάντηση 8	C00C 0001 0001 0000 0004 0004 4A7D EC22
Απάντηση 9	C00C 0001 0001 0000 0004 0004 4A7D EC24
Απάντηση 10	C00C 0001 0001 0000 0004 0004 4A7D EC2E
Απάντηση 11	C00C 0001 0001 0000 0004 0004 4A7D EC26

Field	Sub-Field	Value	Interpretation
ID		0x0003	Απαντάει στην ερώτηση με ID 0x0003
Flags		0x8180	
	QR	1	Είναι απάντηση
	OPCODE	0000	Standard query
	AA	0	Δεν είναι authoritative
	TC	0	Δεν είναι κομμένο
	RD	1	Ζητάει επανάληψη
	RA	1	Ο server μπορεί να κάνει αναδρομή
	Z	000	
	RCODE	0000	Δεν υπήρξε error
QDCOUNT		0x0001	Το μήνυμα περιείχε 1 ερώτηση
ANCOUNT		0x000B	Το μήνυμα περιείχε 11 απαντήσεις
NSCOUNT		0x0000	
ARCOUNT		0x0000	

Από το πεδίο data βρίσκουμε το Domain Name ως εξής :

0x06 -> Ακολουθεί string 6 bytes

0x676F6F676C65 -> google

0x03 -> Ακολουθεί string 3 bytes

0x636F6D -> com

0x00 -> Το domain όνομα τελείωσε

Επίσης έχουμε ότι :

0x0001 -> Η ερωτηση είναι τύπου A

0x0001 -> Η ερωτηση ανήκει στην κλάση IN

Οι απαντήσεις αναλύονται ως εξής :

0xC -> Το όνομα είναι pointer

0x00C -> Ο pointer είναι στο ονομα με offset 0x00C

0x0001 -> Η απάντηση είναι τύπου A

0x0001 -> Η απάντηση ανήκει στην κλάση IN

0x00000004 -> Η απάντηση παραμένει έγκυρη για 4 δευτερόλεπτα

0x0004 -> Η διεύθυνση είναι 4 bytes

Τα παραπάνω πεδία είναι κοινά σε όλες τις απαντήσεις που φέρει το μήνυμα , το μόνο που διαφοροποιείται είναι η IP διεύθυνση .

Απάντηση 1	4A 7D EC 23	74. 125. 236. 35
Απάντηση 2	4A 7D EC 25	74. 125. 236. 37
Απάντηση 3	4A 7D EC 27	74. 125. 236. 39
Απάντηση 4	4A 7D EC 20	74. 125. 236. 32
Απάντηση 5	4A 7D EC 28	74. 125. 236. 40
Απάντηση 6	4A 7D EC 21	74. 125. 236. 33
Απάντηση 7	4A 7D EC 29	74. 125. 236. 41
Απάντηση 8	4A 7D EC 22	74. 125. 236. 34
Απάντηση 9	4A 7D EC 24	74. 125. 236. 36
Απάντηση 10	4A 7D EC 2E	74. 125. 236. 46
Απάντηση 11	4A 7D EC 26	74. 125. 236. 38

B ΜΕΡΟΣ

1. Έχουμε το παρακάτω frame δεδομένων

Mac Header (14bytes)	00A0 9248 7245 0000 0C05 C358 0800
IP Header (20bytes)	4500 0029 DBFB 4000 FE06 7DCB 816E 1E1A 816E 0211
TCP Header (20bytes)	0203 0050 6A86 7B57 B6B6 B020 5010 2400 17c4 0000
Data	0254 414D 494C D787 6CA4

IP Header Analysis :

Version (4bits) -> 4

IHL (4bits) -> 5

Differentiated Services (8bits) -> 00

Total length (16bits) -> 0029

Identification (16bits) -> DBFB

Flags (3bits) -> 010₂

Fragment offset (13bits) -> 0₂000₁₆

TTL (8bits) -> FE

Protocol (8bits) -> 06

Header checksum (16bits) -> 7DCB

Source IP address (32bits) -> 81 6E 1E 1A

Destination IP address (32bits) -> 81 6E 02 11

- 1) Για να βρούμε τη διεύθυνση προορισμού και τη διεύθυνση αποστολής θα χωρίσουμε τις 16αδικές διευθύνσεις σε 4 ίδια μέρη και ύστερα θα τις μετατρέψουμε στο 10δικό σύστημα .

Διεύθυνση προορισμού :

81	6E	1E	1A ₁₆
↓	↓	↓	↓
129.	110.	30.	26 ₁₀

Διεύθυνση αποστολής :

81	6E	02	11 ₁₆
↓	↓	↓	↓
129.	110	.2.	17 ₁₀

- 2) Το μήκος του IP μέρους είναι 41 bytes
- 3) Το frame δεν αποτελεί μέρος μεγαλύτερου πακέτου , το καταλαβαίνουμε από το offset που δείχνει ότι είμαστε στο 1^ο κομμάτι ακόμα και από τα Flags που το 2^ο bit αντιστοιχεί στο DF ,που είναι για Don't Fragment , άρα δεν έχει γίνει διαχωρισμός . Άρα είναι το μοναδικό frame στο πακέτο .
- 4) Η TCP θύρα αποστολέα είναι η port 0x203 (515) και του δέκτη , η port 0x0050 (80)
- 5) Η τιμή του header checksum είναι 7DCB. Για να υπολογίσουμε αν είναι σωστό , θα πρέπει να προσθέσουμε ανά 16 bits ,όλο το header του IP ,εκτός από τα 16 bits του checksum . Ύστερα θα μετατρέψουμε το τελικό άθροισμα σε συμπλήρωμα ως προς 1 και αν το συμπλήρωμα ταυτίζεται με το checksum , τότε έχουμε την σωστή τιμή .

Άρα έχουμε :

4500 -> 1000101000000000

0029 -> 101001

4500+0029 -> 100010100101001 (**4529**)

DBFB -> 1101101111111011

4529+ DBFB -> 10010000100100100 (Θέλουμε μόνο 16 bits για το checksum ,οπότε προσθέτουμε το msb στο υπόλοιπο άθροισμα)

0010000100100100 + 1 -> 0010000100100101 (**2125**)

4000 -> 1000000000000000

2125 + 4000 -> 0110000100100101 (**6125**)

FE06 -> 1111111000000110

6125 + FE06 -> 10101111100101011 (Θέλουμε μόνο 16 bits για το checksum ,οπότε προσθέτουμε το msb στο υπόλοιπο άθροισμα)

0101111100101011 + 1 -> 0101111100101100 (**5F2C**)

816E -> 1000000101101110

5F2C + 816E -> 1110000010011010 (**E09A**)

1E1A -> 1111000011010

E09A +1E1A -> 1111111010110100 (**FEB4**)

816E -> 1000000101101110

FEB4+816E -> 1000000000100010 (Θέλουμε μόνο 16 bits για το checksum ,οπότε προσθέτουμε το msb στο υπόλοιπο άθροισμα)

1000000000100010 +1 -> 1000000000100011 (**8023**)

0211 ->1000010001

8023 + 0211 -> 1000001000110100 (**8234**)

Παίρνουμε το άθροισμα 8234₁₆ και το πηγαίνουμε σε συμπλήρωμα ως προς 1

1000 0010 0011 0100 -> 0111 1101 1100 1011

0111110111001011₂ -> 7DCB₁₆

Άρα καταλήξαμε ότι είναι σωστή η τιμή στο frame

2.

- 1) Το option -d στην tracerf είναι ότι οι IP διευθύνσεις δεν γίνονται resolve, δεν μεταφράζονται δηλαδή σε διευθύνσεις με φυσικά όνοματα ,που είναι εύκολο να κατανοήσει ο άνθρωπος .
- 2) Το φίλτρο που χρησιμοποιήθηκε ήταν το εξής : eth.addr == 4C:BB:58:D1:BA:25
- 3) Το φίλτρο που χρησιμοποιήθηκε ήταν το εξής : eth.addr == 4C:BB:58:D1:BA:25 && icmp

No.	Time	Source	Destination	Protocol	Length	Info
11123	9.528706	192.168.1.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=294/9729, ttl=1 (no response)
11127	9.530770	192.168.1.254	192.168.1.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11131	9.531744	192.168.1.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=295/9985, ttl=1 (no response)
11135	9.533641	192.168.1.254	192.168.1.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11139	9.534515	192.168.1.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=296/10241, ttl=1 (no response)
11145	9.539035	192.168.1.254	192.168.1.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
13199	10.538564	192.168.1.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=297/10497, ttl=2 (no response)
13309	10.600516	62.169.255.238	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
13310	10.602554	192.168.1.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=298/10753, ttl=2 (no response)
13345	10.651691	62.169.255.238	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
13346	10.653728	192.168.1.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=299/11009, ttl=2 (no response)
13369	10.686977	62.169.255.238	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
14318	11.657829	192.168.1.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=300/11265, ttl=3 (no response)
14328	11.695903	62.169.247.185	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
14336	11.701271	192.168.1.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=301/11521, ttl=3 (no response)
14422	11.747899	62.169.247.185	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 11123: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{FE54E48D-5D07-4215-98DA-4E9C278076BD}, id 0
> Ethernet II, Src: ChiconyE_d1:ba:25 (4c:bb:58:d1:ba:25), Dst: Tp-LinkT_0d:e3:d8 (34:e8:94:0d:e3:d8)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 83.212.8.210
> Internet Control Message Protocol

0000 34 e8 94 0d e3 d8 4c bb 58 d1 ba 25 00 00 45 00 4.....L.X.%.E.
0010 00 5c 66 5b 00 00 01 01 34 f3 c0 a8 01 05 53 d4 .\f[....4....S.
0020 08 d2 08 00 f6 d8 00 01 01 26 00 00 00 00 00 00&.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 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

- 4) Η διεύθυνση IP του υπολογιστή μου είναι η : 192.168.1.5 και εμφανίζεται στο πεδίο source ip address (από το 13^ο έως το 16^ο byte της κεφαλίδας IP)
- 5)

Internet Protocol Version 4, Src: 192.168.1.5, Dst: 83.212.8.210
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x665b (26203)
> Flags: 0x0000
Fragment offset: 0
> Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x34f3 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.5
Destination: 83.212.8.210

- 6) Η κεφαλίδα του IP έχει 20 Bytes
- 7) Το πακέτο IP μεταφέρει 72 bytes στο πεδίο δεδομένων
- 8) Έχουμε ότι το total length είναι 92 Bytes και γνωρίζουμε ότι το Header είναι 20 Bytes , επομένως το πεδίο των δεδομένων είναι 92-20 = 72 bytes .
- 9) Αλλάζουν τα πεδία Identification και Time to Live,τα οποία μειώνονται όσο προχωράμε στα πακέτα. Επίσης αλλάζει και το header checksum.
- 10) Αμετάβλητα παραμένουν τα : version , header length ,source IP , destination IP, differentiated services και το protocol.
- 11) Τα πεδία που πρέπει να παραμείνουν αμετάβλητα είναι τα Version ,γιατί χρησιμοποιούμε μόνο IPv4 πρωτοκολλά και επομένως και το header length γιατί είναι σταθερό σε κάθε version . Επίσης τα πεδία με τις διευθύνσεις αποστολής και πηγής πρέπει να παραμείνουν ίδια αφού όλα τα μηνύματα αναφέρονται πάνω σε αυτά. Ακόμα έχουμε τα ίδια πρωτόκολλα κάθε φορά ,επομένως πρέπει να παραμείνουν σταθερά και τα πεδία : Differentiated services και protocol.

12) Πρέπει να αλλάζουν τα πεδία : Identification , γιατί το κάθε IP datagram έχει διαφορετικό ID και το Time to live , γιατί με αυτόν τον τρόπο δουλεύει η εντολή tracerf , μειώνει σε κάθε επανάληψη κατά μια μονάδα τον χρόνο της ώστε να μπορέσει να τερματίσει μετά από κάποια άλματα.

13) Η διεύθυνση του κοντινότερου δρομολογητή σε σχέση με τον υπολογιστή μου είναι η : 192.168.1.254

13369	10.686977	62.169.255.238	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
13345	10.651691	62.169.255.238	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
13309	10.600516	62.169.255.238	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
16923	13.993239	62.169.252.234	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
16866	13.945469	62.169.252.234	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
16861	13.907139	62.169.252.234	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
15724	12.897304	62.169.247.189	192.168.1.5	ICMP	70 Time-to-live exceeded (Time to
15715	12.859722	62.169.247.189	192.168.1.5	ICMP	70 Time-to-live exceeded (Time to
15652	12.817577	62.169.247.189	192.168.1.5	ICMP	70 Time-to-live exceeded (Time to
14504	11.792831	62.169.247.185	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
14422	11.747899	62.169.247.185	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
14328	11.695903	62.169.247.185	192.168.1.5	ICMP	110 Time-to-live exceeded (Time to
11145	9.539035	192.168.1.254	192.168.1.5	ICMP	70 Time-to-live exceeded (Time to
11135	9.533641	192.168.1.254	192.168.1.5	ICMP	70 Time-to-live exceeded (Time to
11127	9.530770	192.168.1.254	192.168.1.5	ICMP	70 Time-to-live exceeded (Time to

14) Η τιμή του πεδίου TTL είναι 254

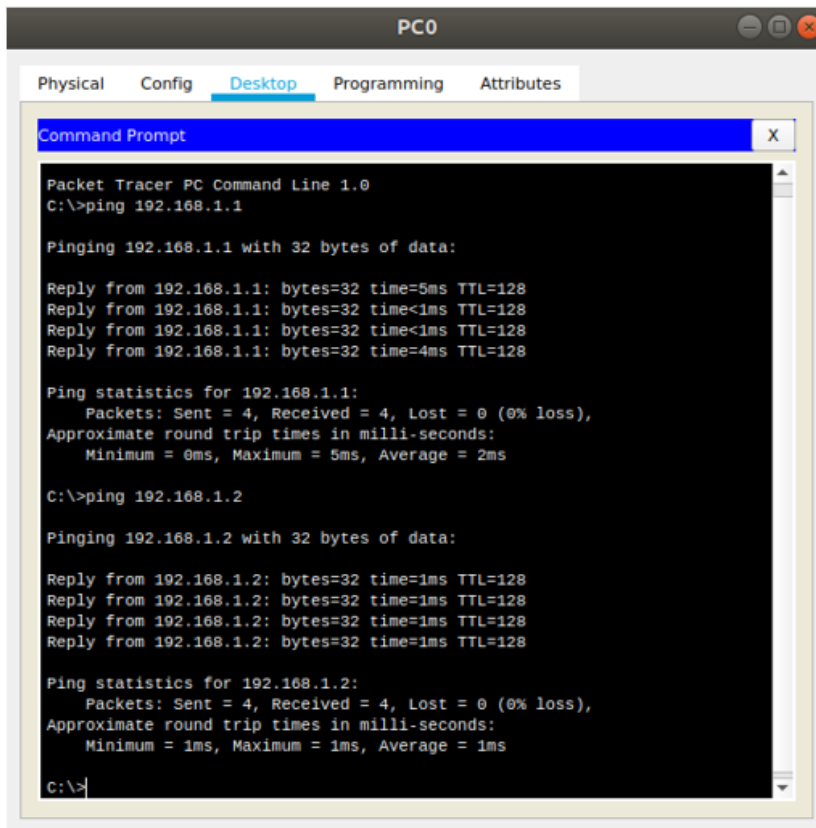
No.	Time	Source	Destination	Protocol	Length	Info
13369	10.686977	62.169.255.238	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to
13345	10.651691	62.169.255.238	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to
13309	10.600516	62.169.255.238	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to
16923	13.993239	62.169.252.234	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to
16866	13.945469	62.169.252.234	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to
16861	13.907139	62.169.252.234	192.168.1.5	ICMP	110	Time-to-live exceeded (Time to

>	Frame 13369: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{FE54E48D-5D07-...}
>	Ethernet II, Src: Tp-LinkT_0d:e3:d8 (34:e8:94:0d:e3:d8), Dst: ChiconyE_d1:ba:25 (4c:bb:58:d1:ba:25)
>	Internet Protocol Version 4, Src: 62.169.255.238, Dst: 192.168.1.5
>	0100 = Version: 4
> 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	Total Length: 96
>	Identification: 0x8d05 (36101)
>	Flags: 0x0000
>	Fragment offset: 0
>	Time to live: 254
>	Protocol: ICMP (1)
>	Header checksum: 0x2f52 [validation disabled]
>	[Header checksum status: Unverified]
>	Source: 62.169.255.238
>	Destination: 192.168.1.5

15) Ναι παραμένουν σταθερά , γιατί ο TTL αλλάζει σε κάθε άλμα που κάνει από έναν δρομολογητή σε άλλο , οπότε μηνύματα που φεύγουν από τον ίδιο δρομολογητή δεν επιδέχονται μείωση στο TTL τους.

Γ ΜΕΡΟΣ

1. Το ring αυτό απευθύνεται στον τοπικό interface του PC0 , καθώς η διεύθυνση IP 192.168.1.1 είναι ορισμένη ως η IP του PC0
2. Ναι έχουμε απαντήσεις φαίνονται στο πεδίο received στα στατιστικά του ring στην 192.168.1.2



The screenshot shows a Packet Tracer PC Command Prompt window for PC0. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with Desktop selected. The Command Prompt displays the results of two ping commands. The first command is 'ping 192.168.1.1', which shows four successful replies with varying times (5ms, <1ms, <1ms, 4ms) and a TTL of 128. The statistics for 192.168.1.1 show 4 packets sent, 4 received, 0 lost (0% loss), with an average round trip time of 2ms. The second command is 'ping 192.168.1.2', which shows four successful replies with a time of 1ms and a TTL of 128. The statistics for 192.168.1.2 show 4 packets sent, 4 received, 0 lost (0% loss), with an average round trip time of 1ms.

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=5ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 2ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Δ ΜΕΡΟΣ

3. Οι εντολές που εκτελέστηκαν είναι οι εξής :

Μέρος 1: Ασφαλείς κωδικοί πρόσβασης

- C:> **telnet 10.10.10.2**
- password: **cisco**
- s1> **enable**
- password: **cisco**
- S1# **copy running-config startup-config**
- (yes) **enter**
- S1# **show running-config**
- S1# **configure terminal**
- S1(config)# **service password-encryption**
- S1(config)# **end**
- S1# **show running-config**

Μέρος 2 : Κρυπτογράφηση επικοινωνιών

- S1# **configure terminal**
- S1(config) # **ip domain-name netacad.pka**
- S1(config)# **crypto key generate rsa**
- **1024**
- S1(config)# **username up1059661 password up1059661**
- S1(config)# **line vty 0 15**
- S1(config-line) # **login local**
- S1(config-line) # **transport input ssh**
- S1(config-line) # **no password cisco**

Μέρος 3: Επαλήθευση της εφαρμογής SSH

- S1(config-line) # **exit**
- S1(config)# **exit**
- S1# **exit**
- C> **telnet 10.10.10.2**
- C> **ssh**
- C> **ssh -l up1059661 10.10.10.2**
- Password: **up1059661**
- s1> **enable**
- password: **cisco**
- S1# **copy running-config startup-config**
- (yes)**enter**
- S1# **exit**

Υποσημείωση : Όσο αφορά τις υλοποιήσεις για το Wireshark , το μέρος Α έχει γίνει σε λειτουργικό Linux Ubuntu18.04 , αλλά καθώς αντιμετωπίσα δυσκολίες με την traceroute στα Linux , το μέρος Β έχει υλοποιηθεί σε άλλο μηχάνημα με Windows 10 . Σε αυτό οφείλονται και οι διαφορετικές IP ανάμεσα στα 2 μέρη.