

Πρωτόκολλα και Αρχιτεκτονικές δικτύων

Εργαστήριο 3

Τμήμα Πληροφορικής και τηλεπικοινωνιών
Πανεπιστήμιο Ιωαννίνων, Άρτα

2023-04-04



Περιεχόμενα

1	Ασκήσεις Nslookup και ipconfig	2
2	Άσκηση στο Wireshark	4
2.1	ΣΕΤ 1	6
2.2	ΣΕΤ 2	9
2.3	ΣΕΤ 3	12

1 Ασκησης Nslookup και ipconfig

1. nslookup

(a) nslookup www.google.com

```
PS C:\WINDOWS\system32> nslookup www.google.com
Server:  pdns1.grnet.gr
Address:  194.177.210.210

Non-authoritative answer:
Name:     www.google.com
Addresses: 2a00:1450:4002:403::2004
          142.250.180.164
```

(b) nslookup - 8.8.8.8

```
PS C:\WINDOWS\system32> nslookup - 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

>
> exit
```

(c) nslookup -type=mx yahoo.com

```
PS C:\WINDOWS\system32> nslookup -type=mx yahoo.com
Server:  pdns1.grnet.gr
Address:  194.177.210.210

Non-authoritative answer:
yahoo.com      MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
```

(d) nslookup -type=ns amazon.com

```
PS C:\WINDOWS\system32> nslookup -type=ns amazon.com
Server:  pdns1.grnet.gr
Address:  194.177.210.210

Non-authoritative answer:
amazon.com     nameserver = ns4.p31.dynect.net
amazon.com     nameserver = ns2.p31.dynect.net
amazon.com     nameserver = ns1.p31.dynect.net
amazon.com     nameserver = pdns6.ultradns.co.uk
amazon.com     nameserver = pdns1.ultradns.net
amazon.com     nameserver = ns3.p31.dynect.net
```

(e) nslookup www.dit.uoi.com

```

PS C:\WINDOWS\system32> nslookup www.dit.uoi.gr
Server:  pdns1.grnet.gr
Address:  194.177.210.210

Non-authoritative answer:
Name:     webserver.dit.uoi.gr
Address:  83.212.170.184
Aliases:  www.dit.uoi.gr

```

2. ipconfig

(a) ipconfig

```

PS C:\WINDOWS\system32> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::4d45:1efa:f317:369f%11
    IPv4 Address. . . . . : 195.130.74.155
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . : 195.130.74.190

Ethernet adapter vEthernet (WSL):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e3db:2bd4:3990:de08%24
    IPv4 Address. . . . . : 172.25.96.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 

```

(b) ipconfig /renew (Δεν θα εκτελεστεί γιατί οι υπολογιστές έχουν public και private static ip addresses configured στα εργαστήρια)

```

PS C:\WINDOWS\system32> ipconfig /renew

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.
PS C:\WINDOWS\system32> ipconfig /release

Windows IP Configuration

```

(c) ipconfig /release (Δεν υπάρχει setted DHCP server)

```

PS C:\WINDOWS\system32> ipconfig /release

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.

```

(d) ipconfig /all — findstr /i "dns servers"

```
PS C:\WINDOWS\system32> ipconfig /all | findstr /i "dns servers"
Primary Dns Suffix . . . . . :
Connection-specific DNS Suffix . :
DNS Servers . . . . . : 194.177.210.210
Connection-specific DNS Suffix . :
```

(e) `ipconfig /all — findstr /i "physical address"`

```
PS C:\WINDOWS\system32> ipconfig /all | findstr /i "physical address"
Physical Address. . . . . : 18-C0-4D-0C-84-44
Link-local IPv6 Address . . . . : fe80::4d45:1efa:f317:369f%11(Preferred)
IPv4 Address. . . . . : 195.130.74.155(Preferred)
Physical Address. . . . . : 00-15-5D-C5-A7-90
Link-local IPv6 Address . . . . : fe80::e3db:2bd4:3990:de08%24(Preferred)
IPv4 Address. . . . . : 172.25.96.1(Preferred)
```

(f) `ipconfig /all`

```
PS C:\WINDOWS\system32> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-SAE2RII
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) I211 Gigabit Network Connection
Physical Address. . . . . : 18-C0-4D-0C-84-44
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4d45:1efa:f317:369f%11(Preferred)
IPv4 Address. . . . . : 195.130.74.155(Preferred)
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . : 195.130.74.190
DHCPv6 IAID . . . . . : 119062605
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-24-AB-01-18-C0-4D-0C-84-44
DNS Servers . . . . . : 194.177.210.210
                        195.130.72.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter vEthernet (WSL):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-C5-A7-90
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e3db:2bd4:3990:de08%24(Preferred)
IPv4 Address. . . . . : 172.25.96.1(Preferred)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 402658653
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-24-AB-01-18-C0-4D-0C-84-44
NetBIOS over Tcpip. . . . . : Enabled
```

2 Άσκηση στο Wireshark

Πρώτα επιλέξτε το κατάλληλο interface όπως στην εικόνα 1, επιλέγοντας **Capture → Options → Manage Interfaces**, και έχοντας επιλεγμένα τα τις στήλες της εικόνας 2.

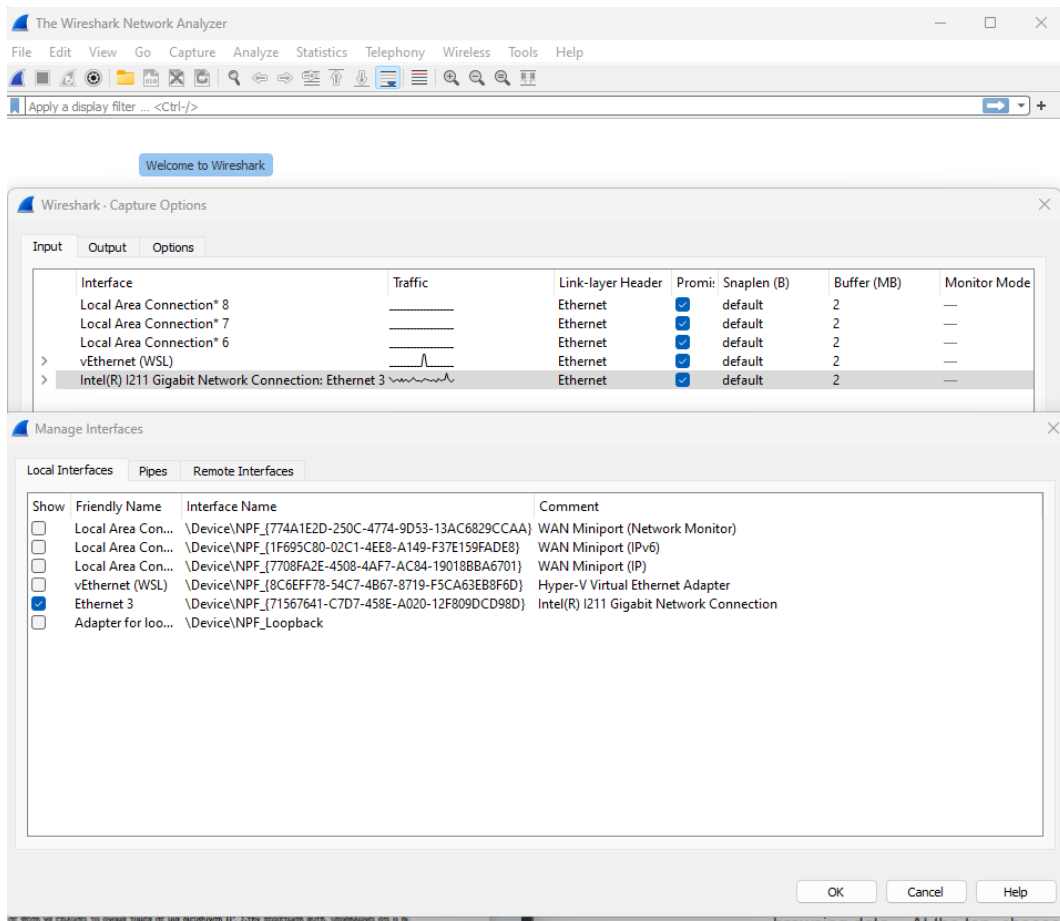


Figure 1: Manage Interfaces

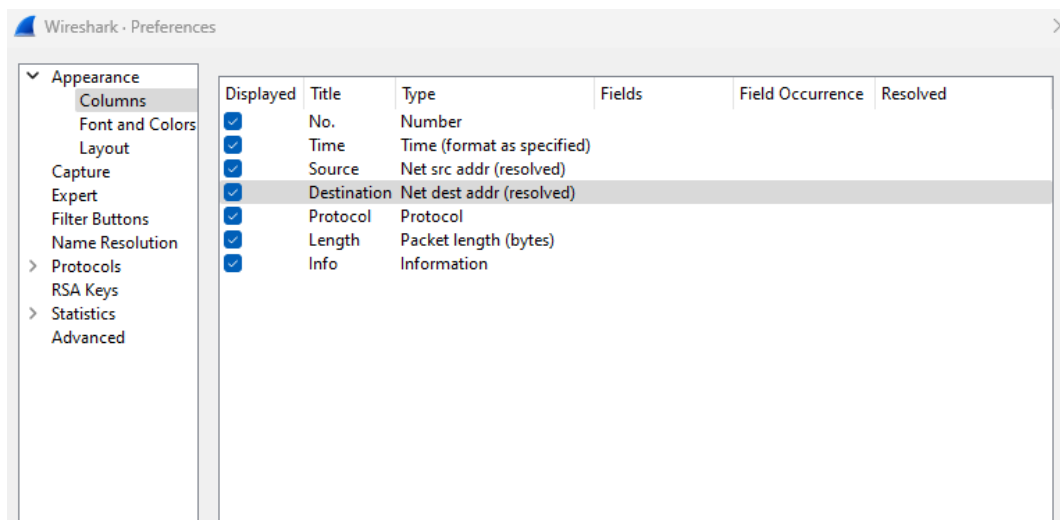


Figure 2: Wireshark selected columns

No.	Time	Source	Destination	Protocol	Length	Info
1849	11.736676	195.130.74.155	84.70.69.246	TCP	896	Continuation
1852	11.784412	195.130.74.155	195.130.72.176	TCP	54	54444 → 3389 [ACK] Seq=1 Ack=387 Win=512 Len=0
1854	11.798249	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1861	11.800644	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1864	11.800803	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1867	11.811922	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1870	11.812723	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1875	11.813268	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1880	11.815625	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1889	11.816925	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1898	11.826972	195.130.74.155	104.16.44.99	QUIC	85	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1899	11.854805	195.130.74.155	104.16.44.99	QUIC	690	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1904	11.930808	195.130.74.155	195.226.194.51	TCP	91	Continuation
1905	11.970808	195.130.74.155	195.226.194.51	TCP	91	Continuation
1928	12.403677	195.130.74.155	103.39.94.37	TCP	347	Continuation
1927	12.413659	195.130.74.155	103.39.94.37	TCP	54	3389 → 60240 [ACK] Seq=1214 Ack=1321 Win=62688 Len=0
1932	12.413659	195.130.74.155	103.39.94.37	TCP	66	3389 → 58075 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
1939	12.709638	195.130.74.155	104.16.44.99	QUIC	86	Protected Payload (QPO), DCID=01f16d4d8f2c942e3f1d3d4def2e0f738508700
1943	12.714962	195.130.74.155	104.16.44.99	QUIC	66	3389 → 58075 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
1942	12.729776	195.130.74.155	195.130.72.176	RDPUDP	53	[Malformed Packet]
1944	12.745978	195.130.74.155	195.130.72.176	RDPUDP	54	SYNEX(Malformed Packet)
1950	12.768745	195.130.74.155	118.68.218.218	RDP	73	Negotiate Response
1959	12.981537	195.130.74.155	118.68.218.218	RDP	73	Negotiate Response
1973	13.048419	195.130.74.155	118.68.218.218	TCP	896	Continuation
1979	13.115792	195.130.74.155	118.68.218.218	TCP	66	3389 → 59030 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM

Figure 3: Captured πακέτα μετά την χρήση φίλτρου

Το φίλτρο που θα χρησιμοποιήσετε είναι: `ip.src==<ip υπολογιστή> && ip.dst==<ip https://www.ietf.org/>`

2.1 ΣΕΤ 1

1. Χρησιμοποιήστε πρωτόκολλο μεταφοράς UDP.

No.	Time	Source	Destination	Protocol	Length	Info
323	2.960481	195.130.74.155	194.177.210.210	DNS	84	Standard query 0xbfb94 AAAA prd-collector-anon.ex.co
331	2.981985	194.177.210.210	195.130.74.155	DNS	169	Standard query response 0xbfb94 AAAA prd-collector-anon.
402	3.472866	195.130.74.155	194.177.210.210	DNS	72	Standard query 0xeb33 A www.ietf.org
405	3.515592	195.130.74.155	195.130.72.1	DNS	72	Standard query 0xeb33 A www.ietf.org
425	3.769689	194.177.210.210	195.130.74.155	DNS	149	Standard query response 0xeb33 A www.ietf.org CNAME www
427	3.770670	195.130.74.155	194.177.210.210	DNS	91	Standard query 0xf65 A www.ietf.org.cdn.cloudflare.net
435	3.791238	194.177.210.210	195.130.74.155	DNS	123	Standard query response 0xf65 A www.ietf.org.cdn.cloudflare
436	3.791577	195.130.74.155	194.177.210.210	DNS	91	Standard query 0xe514 AAAA www.ietf.org.cdn.cloudflare.
440	3.815069	194.177.210.210	195.130.74.155	DNS	147	Standard query response 0xe514 AAAA www.ietf.org.cdn.cl
493	3.997510	195.130.74.155	194.177.210.210	DNS	90	Standard query 0x5fe2 A incoming.telemetry.mozilla.org
494	3.999081	195.130.74.155	194.177.210.210	DNS	78	Standard query 0xc946 A analytics.ietf.org
498	4.018416	194.177.210.210	195.130.74.155	DNS	222	Standard query response 0x5fe2 A incoming.telemetry.moz
499	4.019008	195.130.74.155	194.177.210.210	DNS	103	Standard query 0xf5f2 A prod.investigation-edge.prod.dataoo

Το UDP είναι το πιο συχνά χρησιμοποιούμενο πρωτόκολλο για ερωτήματα DNS, επειδή είναι ταχύτερο και πιο αποτελεσματικό από το TCP για μικρές μεταφορές δεδομένων. Τα περισσότερα ερωτήματα DNS χρησιμοποιούν UDP, συμπεριλαμβανομένων των τυπικών ερωτημάτων DNS και των ερωτημάτων για εγγραφές πόρων, όπως οι εγγραφές A, MX και NS. Ωστόσο, για μεγαλύτερα ερωτήματα DNS ή απαντήσεις που υπερβαίνουν το μέγιστο μέγεθος που επιτρέπεται από το UDP (το

οποίο είναι 512 bytes), χρησιμοποιείται αντί αυτού το TCP. Αυτό περιλαμβάνει ερωτήματα μεταφοράς ζώνης και άλλους τύπους ερωτημάτων DNS που απαιτούν μεγαλύτερες ποσότητες δεδομένων προς μεταφορά.

2. Η θύρα προορισμού (destination port) του μηνύματος ερωτήματος είναι 56650 και η θύρα πηγής (source port) του μηνύματος απόκρισης είναι 53.

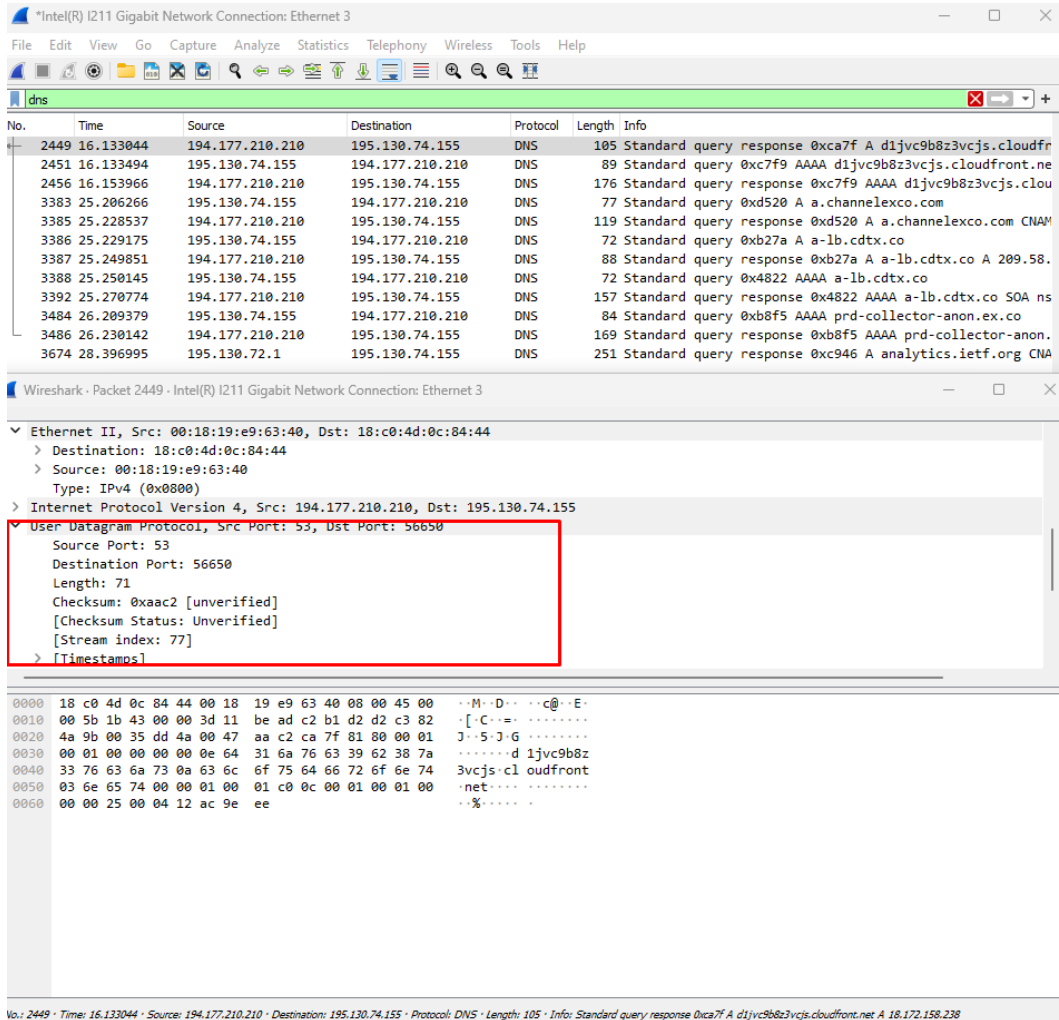


Figure 4: Message Summary

Η θύρα προορισμού για ένα μήνυμα ερωτήματος DNS είναι η θύρα 53 και η θύρα προέλευσης για το αντίστοιχο μήνυμα απάντησης DNS είναι ένας τυχαία εκχωρημένος αριθμός θύρας μεγαλύτερος από 1023. Για να το εντοπίσετε στο Wireshark εκτελέστε τα ακόλουθα βήματα

- Ανοίξτε το αρχείο καταγραφής Wireshark που περιέχει τα μηνύματα ερωτήματος και απάντησης DNS.
- Εντοπίστε το μήνυμα ερωτήματος DNS στη λίστα πακέτων και επιλέξτε το.
- Στο παράθυρο λεπτομερειών στο κάτω μέρος του παραθύρου, επεκτείνετε την ενότητα "Domain Name System (query)" για να δείτε τις λεπτομέρειες του μηνύματος ερωτήματος DNS.
- Στην ενότητα "Transmission Control Protocol" (Πρωτόκολλο ελέγχου μετάδοσης) του παραθύρου λεπτομερειών, θα δείτε τις θύρες προέλευσης και προορισμού για το μήνυμα ερωτήματος DNS. Η θύρα προορισμού θα πρέπει να είναι 53, η οποία είναι ο γνωστός αριθμός θύρας που χρησιμοποιείται από τους διακομιστές DNS.
- Εντοπίστε το αντίστοιχο μήνυμα απάντησης DNS στη λίστα πακέτων και επιλέξτε το.

- Στο παράθυρο λεπτομερειών, επεκτείνετε την ενότητα "Domain Name System (response)" (Σύστημα ονομάτων τομέα (απάντηση)) για να δείτε τις λεπτομέρειες του μηνύματος απάντησης DNS.
 - Στην ενότητα "Transmission Control Protocol" (Πρωτόκολλο ελέγχου μετάδοσης) του παραθύρου λεπτομερειών, θα δείτε τις θύρες προέλευσης και προορισμού για το μήνυμα απάντησης DNS. Η θύρα προέλευσης πρέπει να είναι ένας τυχαία εκχωρημένος αριθμός θύρας μεγαλύτερος από 1023, ο οποίος χρησιμοποιείται από τον πελάτη DNS για τη λήψη της απάντησης από το διακομιστή DNS.
3. Το μήνυμα που επιλέξαμε στάλθηκε στην IP διεύθυνση του DNS server.
 4. Κοιτάμε το μήνυμα απόκρισης από τον DNS στον Host

```

▼ Frame 228: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface \Device\NPF_{71567641-C7D7-458E-A020-12F8090CD98D}, id 0
  Section number: 1
  > Interface id: 0 (\Device\NPF_{71567641-C7D7-458E-A020-12F8090CD98D})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 28, 2023 14:05:49.108232000 GTB Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600001549.108232000 seconds
    [Time delta from previous captured frame: 0.002205000 seconds]
    [Time delta from previous displayed frame: 0.020434000 seconds]
    [Time since reference or first frame: 2.324385000 seconds]
    Frame Number: 228
    Frame Length: 123 bytes (984 bits)
    Capture Length: 123 bytes (984 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]

▼ Ethernet II, Src: 00:18:19:e9:63:40, Dst: 18:c0:4d:0c:84:44
  > Destination: 18:c0:4d:0c:84:44
  > Source: 00:18:19:e9:63:40
  Type: IPv4 (0x0800)

```

5. Dns answers

```

▼ Answers
  ▼ mail.google.com: type AAAA, class IN, addr 2a00:1450:4002:402::2005
    Name: mail.google.com
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 130 (2 minutes, 10 seconds)
    Data length: 16
    AAAA Address: 2a00:1450:4002:402::2005
    [Request In: 30]

```

6. Όταν ένας κεντρικός υπολογιστής στέλνει ένα πακέτο SYN για να ξεκινήσει μια σύνδεση TCP, συνήθως περιλαμβάνει τη διεύθυνση IP του διακομιστή στο πεδίο διεύθυνσης προορισμού του πακέτου. Η διεύθυνση IP μπορεί να έχει ληφθεί από ένα μήνυμα απόκρισης DNS, εάν ο κεντρικός υπολογιστής έχει επιλύσει το όνομα τομέα του διακομιστή σε μια διεύθυνση IP χρησιμοποιώντας DNS. Επομένως, εάν το μήνυμα απόκρισης DNS παρείχε μια διεύθυνση IP για τον διακομιστή με τον οποίο ο κεντρικός υπολογιστής προσπαθεί να δημιουργήσει μια σύνδεση, τότε είναι πιθανό η διεύθυνση προορισμού του πακέτου SYN που αποστέλλεται από το TCP να αντιστοιχεί σε αυτή τη διεύθυνση IP. Ωστόσο, εάν η απάντηση DNS δεν παρείχε διεύθυνση IP για τον διακομιστή, τότε η διεύθυνση προορισμού στο πακέτο SYN μπορεί να είναι διαφορετική.


```

> Ethernet II, Src: 00:18:19:e9:63:40, Dst: 18:c0:4d:0c:84:44
> Internet Protocol Version 4, Src: 104.16.44.99, Dst: 195.130.74.155
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 61
    Protocol: TCP (6)
    Header Checksum: 0x9b33 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 104.16.44.99
    Destination Address: 195.130.74.155
> Transmission Control Protocol, Src Port: 443, Dst Port: 62155, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 62155
  [Stream index: 11]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 232260910
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3171786881
  1000 .... = Header Length: 32 bytes (8)
> Flags: 0x012 (SYN, ACK)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x6c99 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Oper
    > TCP Option - Maximum segment size: 1400 bytes
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - SACK permitted
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 13 (multiply by 8192)
  > [Timestamps]
    [Time since first frame in this TCP stream: 0.013094000 seconds]
    [Time since previous frame in this TCP stream: 0.013094000 seconds]
  > [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 107]
    [The RTT to ACK the segment was: 0.013094000 seconds]
    [iRTT: 0.013160000 seconds]

```

7. Όχι, αφού ο υπολογιστής σας έχει επιλύσει το ερώτημα DNS για το όνομα τομέα "ietf.org" σε μια διεύθυνση IP, δεν χρειάζεται να στέλνει νέα ερωτήματα DNS για κάθε εικόνα στον ιστότοπο. Οι εικόνες στον ιστότοπο συνήθως φιλοξενούνται στον ίδιο διακομιστή με τον ίδιο τον ιστότοπο, οπότε ο υπολογιστής σας μπορεί να χρησιμοποιήσει την ίδια διεύθυνση IP για να ζητήσει όλο το περιεχόμενο που σχετίζεται με αυτό το όνομα τομέα. Ωστόσο, εάν οι εικόνες φιλοξενούνται σε διαφορετικό διακομιστή με διαφορετικό όνομα τομέα, ο υπολογιστής σας θα πρέπει να στείλει ένα νέο ερώτημα DNS για να επιλύσει το όνομα τομέα σε μια διεύθυνση IP πριν από την ανάκτηση της εικόνας.

2.2 ΣΕΤ 2

Τα βήματα που θα ακολουθήσετε είναι τα εξής:

- Εισάγεται ως φίλτρο το αλφαριθμητικό dns
- Ξεκινήστε τη σύλληψη πακέτων.
- Τρέξτε το nslookup για το όνομα host www.mit.edu.

No.	Time	Source	Destination	Protocol	Length	Info
335	4.063710	195.130.74.155	194.177.210.210	DNS	88	Standard query 0x0001 PTR 210.210.177.194.
336	4.084311	194.177.210.210	195.130.74.155	DNS	116	Standard query response 0x0001 PTR 210.210.1
337	4.084914	195.130.74.155	194.177.210.210	DNS	71	Standard query 0x0002 A www.mit.edu
357	4.283611	194.177.210.210	195.130.74.155	DNS	160	Standard query response 0x0002 A www.mit.edu
358	4.285824	195.130.74.155	194.177.210.210	DNS	71	Standard query 0x0003 AAAA www.mit.edu
361	4.333090	194.177.210.210	195.130.74.155	DNS	200	Standard query response 0x0003 AAAA www.mi

- Σταματήστε τη σύλληψη πακέτων.

Η ακολουθία των πακέτων (trace) που απεικονίζεται στο Wireshark θα πρέπει να μοιάζει με αυτήν που φαίνεται στην εικόνα 2.2 (Με βάση πάντα τον δικό σας host).

No.	Time	Source	Destination	Protocol	Length	Info
335	4.063710	195.130.74.155	194.177.210.210	DNS	88	Standard query 0x0001 PTR 210.210.177.194.in
336	4.084311	194.177.210.210	195.130.74.155	DNS	116	Standard query response 0x0001 PTR 210.210.1
337	4.084914	195.130.74.155	194.177.210.210	DNS	71	Standard query 0x0002 A www.mit.edu
357	4.283611	194.177.210.210	195.130.74.155	DNS	160	Standard query response 0x0002 A www.mit.edu
358	4.285824	195.130.74.155	194.177.210.210	DNS	71	Standard query 0x0003 AAAA www.mit.edu
361	4.333090	194.177.210.210	195.130.74.155	DNS	200	Standard query response 0x0003 AAAA www.mit.

Όπως φαίνεται, το nslookup έστειλε στην πραγματικότητα τρία ερωτήματα DNS και έλαβε, αντίστοιχα, τρεις αποκρίσεις. Για να απαντήσετε στις παρακάτω ερωτήσεις αγνοείτε τα δύο πρώτα ζεύγη ερωτημάτων, αποκρίσεων καθώς αφορούν το nslookup και κατά κανόνα δεν δημιουργούνται από συνήθεις ιαδικτυακές εφαρμογές. Επικεντρωθείτε, λοιπόν, στο τελευταίο ερώτημα και την τελευταία απόκριση DNS όπως παρουσιάζεται στη εικόνα 2.2.

1. Ποια η θύρα προορισμού (destination port) του μηνύματος ερωτήματος; Ποια η θύρα πηγής (source port) του μηνύματος απόκρισης;

```

> Internet Protocol Version 4, Src: 194.177.210.210, Dst: 195.130.74.155
> User Datagram Protocol, Src Port: 53, Dst Port: 57476
v Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  
```

2. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server; **Ναι η 194.177.210.210 είναι η κύρια διεύθυνση του dns server.**
3. Εξετάστε το μήνυμα ερωτήματος. Ποιο το “είδος” (“Type”) του ερωτήματος; Περιέχονται “απαντήσεις” (“answers”) στο μήνυμα ερωτήματος; Στο Wireshark, ο τύπος του μηνύματος σε ένα καταγεγραμμένο πακέτο υποδεικνύεται από το πεδίο “Πρωτόκολλο”. Το Wireshark αναλύει τα περιεχόμενα του πακέτου και χρησιμοποιεί διάφορες ευρετικές μεθόδους για να προσδιορίσει τον τύπο πρωτοκόλλου. Για παράδειγμα, εάν το πακέτο περιέχει επικεφαλίδες και ωφέλιμο φορτίο TCP, το πεδίο “Protocol” στο Wireshark θα εμφανίσει “TCP” ως τύπο μηνύματος. Ομοίως, εάν το πακέτο περιέχει επικεφαλίδες και ωφέλιμο φορτίο UDP, το πεδίο “Πρωτόκολλο” θα εμφανίσει “UDP”. Εάν το πακέτο περιέχει επικεφαλίδες και ωφέλιμο φορτίο DNS, το πεδίο “Protocol” θα εμφανίσει “DNS” ως τύπο μηνύματος. Άλλοι συνηθισμένοι τύποι μηνυμάτων που μπορεί να εμφανιστούν στο Wireshark περιλαμβάνουν HTTP, ICMP, ARP και Ethernet. Είναι σημαντικό να σημειωθεί ότι η ικανότητα του Wireshark να προσδιορίζει σωστά τον τύπο πρωτοκόλλου βασίζεται στην ικανότητά του να αποκωδικοποιεί τα περιεχόμενα του πακέτου. Εάν το πακέτο είναι

κρυπτογραφημένο ή χρησιμοποιεί ένα ιδιόκτητο πρωτόκολλο με το οποίο το Wireshark δεν είναι εξοικειωμένο, το πεδίο "Protocol" (Πρωτόκολλο) μπορεί να εμφανίσει την ένδειξη "Unknown" (Άγνωστο) ή "Unrecognized" (Μη αναγνωρισμένο).

```
▼ Domain Name System (query)
  Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    > www.mit.edu: type AAAA, class IN
      [Response In: 361]
```

4. Εξετάστε το μήνυμα απόκρισης. Πόσες "απαντήσεις" περιέχονται στο μήνυμα αυτό; Τι περιέχει καθεμία από τις απαντήσεις αυτές;

```
▼ Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    > www.mit.edu: type AAAA, class IN
  ▼ Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:f700:485::255e
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:f700:495::255e
      [Request In: 358]
  [Time: 0.047266000 seconds]
```

- **Όνομα:** Το όνομα τομέα για το οποίο έγινε το ερώτημα DNS. Αυτό το πεδίο συμπίπτει συχνά με τη χρήση μιας δυαδικής μορφής που ονομάζεται "συμπίεση ονόματος" για εξοικονόμηση χώρου.
- **Τύπος:** Ο τύπος της εγγραφής πόρου DNS που επιστρέφεται στην απάντηση. Αυτό το πεδίο καθορίζει τον τύπο δεδομένων που περιλαμβάνονται στην απόκριση, όπως μια διεύθυνση IP, ένα όνομα κεντρικού υπολογιστή ή κάποιο άλλο είδος δεδομένων.
- **Κατηγορία:** Η κλάση της εγγραφής πόρου DNS. Αυτό το πεδίο προσδιορίζει συνήθως το πρωτόκολλο δικτύου που χρησιμοποιείται, όπως το πρωτόκολλο Internet Protocol (IP).
- **Time to Live (TTL):** Το χρονικό διάστημα για το οποίο η απάντηση DNS θα πρέπει να αποθηκευτεί στην προσωρινή μνήμη από τον επιλύτη ή τον πελάτη DNS που κάνει την αίτηση. Η τιμή αυτή δίνεται σε δευτερόλεπτα και καθορίζει για πόσο χρονικό διάστημα τα δεδομένα μπορούν να θεωρηθούν έγκυρα προτού χρειαστεί να ανανεωθούν από τον έγκυρο διακομιστή DNS.
- **Μήκος δεδομένων:** Το μήκος του πεδίου δεδομένων που περιέχει τα πραγματικά δεδομένα της εγγραφής πόρων DNS.
- **Διεύθυνση AAAA:** Εάν το πεδίο Type υποδεικνύει ότι η εγγραφή πόρου DNS περιέχει διεύθυνση IPv6, αυτό το πεδίο θα περιέχει τα πραγματικά δεδομένα διεύθυνσης IPv6. Ο τύπος εγγραφής AAAA χρησιμοποιείται για την αντιστοίχιση ενός ονόματος τομέα σε μια διεύθυνση IPv6.

Αξίζει να σημειωθεί ότι η μορφή μιας απάντησης DNS μπορεί να διαφέρει ανάλογα με τον τύπο του ερωτήματος DNS που έγινε, καθώς και με τη συγκεκριμένη υλοποίηση του διακομιστή DNS που χειρίζεται το αίτημα. Ωστόσο, τα πεδία που αναφέρονται παραπάνω χρησιμοποιούνται συνήθως στις περισσότερες απαντήσεις DNS.

5. Παρέχεται εικόνα για το παραπάνω ερώτημα

```

Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1544 (25 minutes, 44 seconds)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:f700:485::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 16
    AAAA Address: 2a02:26f0:f700:485::255e
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:f700:495::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 16
    AAAA Address: 2a02:26f0:f700:495::255e

```

2.3 ΣΕΤ 3

Επαναλάβετε το προηγούμενο πείραμα για την εντολή: `nslookup -type=NS www.mit.edu`

124	1.242908	195.130.74.155	194.177.210.210	DNS	67 Standard query 0xdc13 A mit.edu
127	1.283437	195.130.74.155	195.130.72.1	DNS	67 Standard query 0xdc13 A mit.edu
130	1.306970	194.177.210.210	195.130.74.155	DNS	83 Standard query response 0xdc13 A mit.edu A 2
131	1.309005	195.130.74.155	2.19.42.129	DNS	84 Standard query 0x0001 PTR 129.42.19.2.in-add
340	3.312039	195.130.74.155	2.19.42.129	DNS	68 Standard query 0x0002 A ♦type=NS
517	5.317615	195.130.74.155	2.19.42.129	DNS	68 Standard query 0x0003 AAAA ♦type=NS
522	5.351165	195.130.72.1	195.130.74.155	DNS	446 Standard query response 0xdc13 A mit.edu A 2

Απαντήστε στις παρακάτω ερωτήσεις:

- Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server;

124	1.242908	195.130.74.155	194.177.210.210	DNS	67 Standard query 0xdc13 A mit.edu
127	1.283437	195.130.74.155	195.130.72.1	DNS	67 Standard query 0xdc13 A mit.edu
130	1.306970	194.177.210.210	195.130.74.155	DNS	83 Standard query response 0xdc13 A mit.edu A 2
131	1.309005	195.130.74.155	2.19.42.129	DNS	84 Standard query 0x0001 PTR 129.42.19.2.in-add
340	3.312039	195.130.74.155	2.19.42.129	DNS	68 Standard query 0x0002 A ♦type=NS
517	5.317615	195.130.74.155	2.19.42.129	DNS	68 Standard query 0x0003 AAAA ♦type=NS
522	5.351165	195.130.72.1	195.130.74.155	DNS	446 Standard query response 0xdc13 A mit.edu A 2

Ναι η ip παραλήπτη είναι η ip του dns server.

- Εξετάστε το μήνυμα ερωτήματος. Ποιο το “είδος” (“Type”) του ερωτήματος; Περιέχονται “απαντήσεις” (“answers”) στο μήνυμα ερωτήματος; Το είδος της απάντησης είναι το πρωτόκολλο dns. Στο μήνυμα ερωτήματος δεν περιέχονται απαντήσεις.
- Εξετάστε το μήνυμα απόκρισης. Ποια ονόματα nameservers του MIT παρέχονται στο μήνυμα απόκρισης; Στο μήνυμα απόκρισης παρέχονται και οι διευθύνσεις IP των nameservers του MIT;

```

Name Server: n3dscb.akamaiedge.net
  ▾ dscb.akamaiedge.net: type NS, class IN, ns n3dscb.akamaiedge.net
    Name: dscb.akamaiedge.net
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 189 (3 minutes, 9 seconds)
    Data length: 9
    Name Server: n3dscb.akamaiedge.net
  ▾ dscb.akamaiedge.net: type NS, class IN, ns n4dscb.akamaiedge.net
    Name: dscb.akamaiedge.net
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 189 (3 minutes, 9 seconds)
    Data length: 9
    Name Server: n4dscb.akamaiedge.net
  ▾ dscb.akamaiedge.net: type NS, class IN, ns n5dscb.akamaiedge.net
    Name: dscb.akamaiedge.net
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 189 (3 minutes, 9 seconds)
    Data length: 9
    Name Server: n5dscb.akamaiedge.net
  ▾ dscb.akamaiedge.net: type NS, class IN, ns n6dscb.akamaiedge.net
    Name: dscb.akamaiedge.net
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 189 (3 minutes, 9 seconds)
    Data length: 9
    Name Server: n6dscb.akamaiedge.net
  ▾ dscb.akamaiedge.net: type NS, class IN, ns n7dscb.akamaiedge.net
    Name: dscb.akamaiedge.net
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 189 (3 minutes, 9 seconds)
    Data length: 9
    Name Server: n7dscb.akamaiedge.net

```

Με βάση τις διαθέσιμες πληροφορίες, προκύπτει ότι το "n6dscb.akamaiedge.net" είναι διακομιστής DNS MIT. Η Akamai Technologies είναι πάροχος δικτύου διανομής περιεχομένου (CDN) που προσφέρει υπηρεσίες σε ένα ευρύ φάσμα πελατών, συμπεριλαμβανομένων πανεπιστημίων όπως το MIT. Είναι πιθανό ότι το "n6dscb.akamaiedge.net" είναι ένας διακομιστής DNS της Akamai που χρησιμοποιείται από το MIT για την παροχή περιεχομένου, αλλά δεν είναι ένας εξουσιοδοτημένος διακομιστής ονομάτων για τον τομέα "mit.edu".

- Παρέχεται εικόνα για το παραπάνω ερώτημα.

```

Internet Protocol Version 4, Src: 195.130.72.1, Dst: 195.130.74.155
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 314
    Identification: 0x0324 (804)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 254
    Protocol: UDP (17)
    Header Checksum: 0x5eed [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 195.130.72.1
    Destination Address: 195.130.74.155
User Datagram Protocol, Src Port: 53, Dst Port: 51550
  Source Port: 53
  Destination Port: 51550
  Length: 294
  Checksum: 0x24d9 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 18]
  > [Timestamps]
  UDP payload (286 bytes)
Domain Name System (response)
  Transaction ID: 0x01a0
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 8
  Additional RRs: 0
  > Queries
  > Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net

```

Επαναλάβετε το προηγούμενο πείραμα για την εντολή: `nslookup www.aiit.or.kr ip.bitsy.mit.edu`

Απαντήστε στις ακόλουθες ερωτήσεις:

1. Σε ποια διεύθυνση IP στάλθηκε το μήνυμα ερωτήματος; Πρόκειται για τη διεύθυνση IP του τοπικού σας DNS server; Εάν όχι, σε τι αντιστοιχεί η συγκεκριμένη διεύθυνση IP;

16 0.177152	195.130.74.175	192.168.0.1	DNS	88 Standard query 0x165c PTR 142.194.226.195
594 6.154196	195.130.74.155	194.177.210.210	DNS	88 Standard query 0x0001 PTR 210.210.177.194
595 6.174274	194.177.210.210	195.130.74.155	DNS	116 Standard query response 0x0001 PTR 210.210.177.194
596 6.175426	195.130.74.155	194.177.210.210	DNS	81 Standard query 0x0002 A n6dscb.akamaiedge.net
598 6.195105	194.177.210.210	195.130.74.155	DNS	97 Standard query response 0x0002 A n6dscb.akamaiedge.net
599 6.197185	195.130.74.155	194.177.210.210	DNS	81 Standard query 0x0003 AAAA n6dscb.akamaiedge.net
606 6.259994	194.177.210.210	195.130.74.155	DNS	147 Standard query response 0x0003 AAAA n6dscb.akamaiedge.net
770 8.087645	195.130.74.155	194.177.210.210	DNS	75 Standard query 0xe8e5 A mail.google.com
773 8.107290	194.177.210.210	195.130.74.155	DNS	91 Standard query response 0xe8e5 A mail.google.com
774 8.108186	195.130.74.155	194.177.210.210	DNS	75 Standard query 0xa1ab AAAA mail.google.com
778 8.127790	194.177.210.210	195.130.74.155	DNS	103 Standard query response 0xa1ab AAAA mail.google.com
859 8.531384	195.130.74.155	194.177.210.210	DNS	75 Standard query 0xa432 A play.google.com
861 8.551048	194.177.210.210	195.130.74.155	DNS	91 Standard query response 0xa432 A play.google.com
862 8.551693	195.130.74.155	194.177.210.210	DNS	75 Standard query 0x002c AAAA play.google.com

2. Εξετάστε το μήνυμα ερωτήματος. Ποιο το “είδος” (“Type”) του ερωτήματος; Περιέχονται “απαντήσεις” (“answers”) στο μήνυμα ερωτήματος;


```

    >>> payload (14 bytes)
  ▾ Domain Name System (response)
    Transaction ID: 0x0001
    > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    > Queries
  ▾ Answers
    ▾ 210.210.177.194.in-addr.arpa: type PTR, class IN, pdns1.grnet.gr
      Name: 210.210.177.194.in-addr.arpa
      Type: PTR (domain name PointeR) (12)
      Class: IN (0x0001)
      Time to live: 2246 (37 minutes, 26 seconds)
      Data length: 16
      Domain Name: pdns1.grnet.gr
      [Request In: 594]
      [Time: 0.020078000 seconds]

  ▾ Ethernet II, Src: 00:18:19:e9:63:40, Dst: c4:e9:84:f5:e2:ef
    > Destination: c4:e9:84:f5:e2:ef
    > Source: 00:18:19:e9:63:40
    Type: IPv4 (0x0800)

  ▾ Internet Protocol Version 4, Src: 195.130.74.175, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 74
    Identification: 0x5564 (21860)
    > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: UDP (17)
    Header Checksum: 0x5764 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 195.130.74.175
    Destination Address: 192.168.0.1

  ▾ User Datagram Protocol, Src Port: 59380, Dst Port: 53
    Source Port: 59380
    Destination Port: 53
    Length: 54
    Checksum: 0x383d [unverified]

```

- Εξετάστε το μήνυμα απόκρισης. Πόσες “απαντήσεις” περιέχονται στο μήνυμα αυτό; Τι περιέχει καθεμία από τις απαντήσεις αυτές;
- Εάν εκτελέσετε την εντολή `nslookup www.dit.uoi.gr` αφού αδειάσετε την DNS cache, θα περάσετε από τους ίδιους nameservers για να λάβετε την απάντηση;

Πρώτα εκτελούμε την εντολή `ipconfig /flushdns`

```

  929 10.411907 195.130.74.155 194.177.210.210 DNS 88 Standard query 0x0001 PTR 210.210.177.194.ir
  934 10.431546 194.177.210.210 195.130.74.155 DNS 116 Standard query response 0x0001 PTR 210.210.1
  936 10.432261 195.130.74.155 194.177.210.210 DNS 74 Standard query 0x0002 A www.dit.uoi.gr
  945 10.451955 194.177.210.210 195.130.74.155 DNS 114 Standard query response 0x0002 A www.dit.uoi
  946 10.453909 195.130.74.155 194.177.210.210 DNS 74 Standard query 0x0003 AAAA www.dit.uoi.gr
  947 10.473825 194.177.210.210 195.130.74.155 DNS 157 Standard query response 0x0003 AAAA www.dit.
  1089 12.426594 195.130.74.155 194.177.210.210 DNS 86 Standard query 0x844f A maxineapi.razersynap
  1093 12.446582 194.177.210.210 195.130.74.155 DNS 182 Standard query response 0x844f A maxineapi.r
  1156 13.060870 195.130.74.155 194.177.210.210 DNS 90 Standard query 0xa887 A deals-assets-cdn.ra
  1161 13.160077 194.177.210.210 195.130.74.155 DNS 287 Standard query response 0xa887 A deals-asset

```

Είναι πιθανό να περάσετε από τους ίδιους διακομιστές ονομάτων για να λάβετε την απάντηση όταν εκτελείτε το `nslookup www.dit.uoi.gr` μετά την εκκαθάριση της προσωρινής μνήμης DNS, αλλά αυτό δεν είναι εγγυημένο. Όταν καθαρίζετε την προσωρινή μνήμη DNS, το σύστημά σας θα πρέπει να ζητήσει από τους εξουσιοδοτημένους διακομιστές DNS για τον τομέα για να επιλύσει το ερώτημα DNS. Οι έγκυροι διακομιστές DNS είναι αυτοί που κατέχουν τα επίσημα αρχεία για έναν τομέα,

συμπεριλαμβανομένων των διευθύνσεων IP που σχετίζονται με το όνομα τομέα. Η διαδρομή που ακολουθεί το ερώτημά σας DNS για να φτάσει στους εξουσιοδοτικούς διακομιστές DNS μπορεί να εξαρτάται από διάφορους παράγοντες, όπως η διαμόρφωση του δικτύου σας και ο επιλύτης DNS που χρησιμοποιείται. Εάν οι διακομιστές ονομάτων στους οποίους κατευθύνθηκε προηγουμένως το ερώτημά σας εξακολουθούν να θεωρούνται η καλύτερη επιλογή από τον επιλύτη DNS, τότε το ερώτημά σας μπορεί να κατευθυνθεί ξανά σε αυτούς τους διακομιστές ονομάτων. Ωστόσο, είναι επίσης πιθανό το ερώτημά σας να κατευθυνθεί σε διαφορετικούς διακομιστές ονομάτων. Οι επιλύτες DNS χρησιμοποιούν συνήθως διάφορους μηχανισμούς για να καθορίσουν τους καλύτερους διακομιστές ονομάτων που πρέπει να χρησιμοποιηθούν, συμπεριλαμβανομένης της εξισορρόπησης φορτίου και της γεωγραφικής θέσης, οπότε δεν είναι ασυνήθιστο τα ερωτήματα DNS να κατευθύνονται σε διαφορετικούς διακομιστές ονομάτων με την πάροδο του χρόνου.