



HACETTEPE UNIVERSITY

DEPARTMENT OF  
COMPUTER ENGINEERING

---

## BBM453: Computer Networks Laboratory Lab 2: DNS

---

*Author*

Kayla AKYÜZ  
21726914  
Batuhan ÖZTÜRK  
21827742

*Advisors*

T.A. Tuğba ERDOĞAN  
[tugba.gurgen@hacettepe.edu.tr](mailto:tugba.gurgen@hacettepe.edu.tr)  
Assoc. Prof. Sevil ŞEN  
[ssen@cs.hacettepe.edu.tr](mailto:ssen@cs.hacettepe.edu.tr)

Group 14  
Source IP : 10.225.15.11

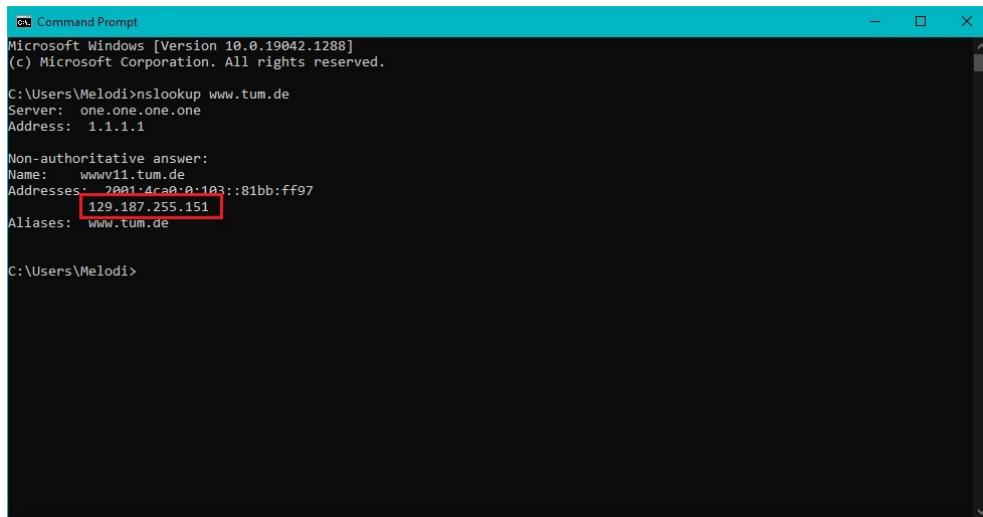
Oct 20,2021

# SOLUTIONS

## nslookup

### 1. Run nslookup to obtain the IP address of a Web server in Europe. What is the IP address of that server?

IP Address of server www.tum.de which is in Europe is 129.187.255.151 as you can see in the screenshot below.



```
Windows Command Prompt
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

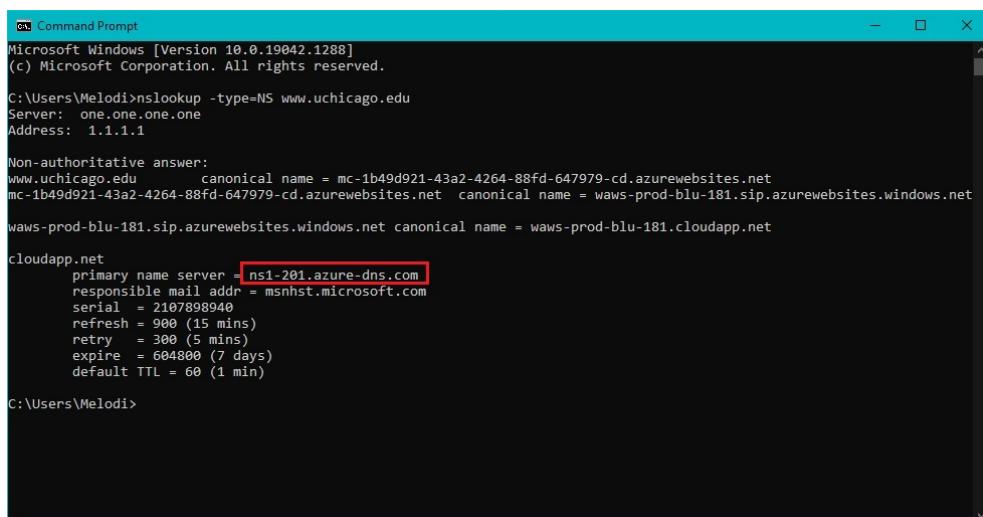
C:\Users\Melodi>nslookup www.tum.de
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name: www11.tum.de
Addresses: 2001:ac00:100::81bb:ff97
          129.187.255.151
Aliases: www.tum.de

C:\Users\Melodi>
```

### 2. Run nslookup to determine the authoritative DNS servers for a university in United States.

We have determined www.uchicago.edu University of Chicago is in DNS server of ns1-201.azure-dns.com. Proof screenshot as follows:



```
Windows Command Prompt
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Melodi>nslookup -type=NS www.uchicago.edu
Server: one.one.one.one
Address: 1.1.1.1

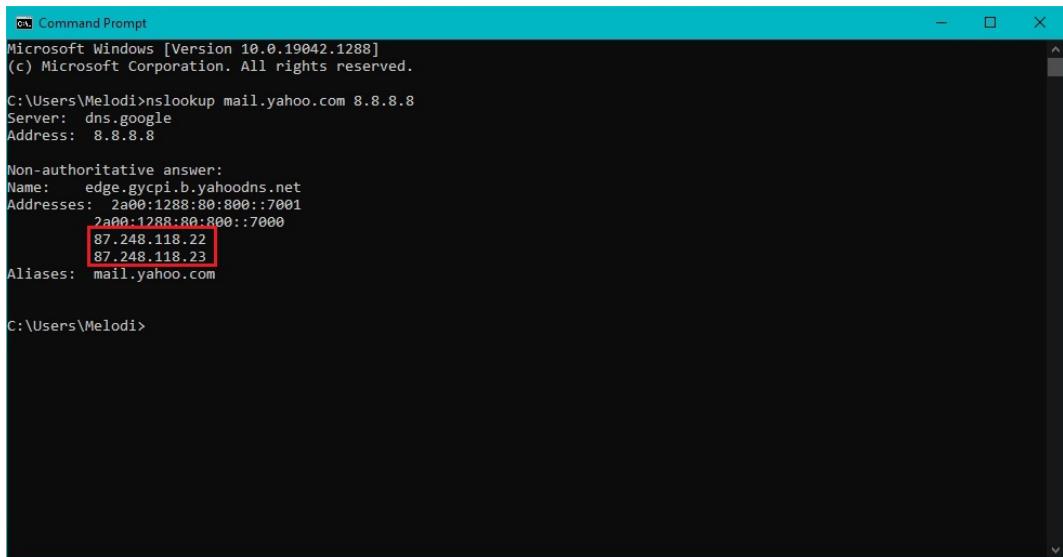
Non-authoritative answer:
www.uchicago.edu canonical name = mc-1b49d921-43a2-4264-88fd-647979-cd.azurewebsites.net
mc-1b49d921-43a2-4264-88fd-647979-cd.azurewebsites.net canonical name = waws-prod-blu-181.sip.azurewebsites.windows.net
waws-prod-blu-181.sip.azurewebsites.windows.net canonical name = waws-prod-blu-181.cloudapp.net

cloudapp.net
primary name server ns1-201.azure-dns.com
responsible mail addr = msdnst.microsoft.com
serial = 2107898940
refresh = 900 (15 mins)
retry = 300 (5 mins)
expire = 604800 (7 days)
default TTL = 60 (1 min)

C:\Users\Melodi>
```

### 3. Run nslookup so that one of the DNS servers of Google is queried for the mail servers for Yahoo! mail. What is its IP address?

It's IP address is 87.248.118.22 and 87.248.118.23 as can be seen in screenshot.



```
Windows PowerShell [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Melodi>nslookup mail.yahoo.com 8.8.8.8
Server:  dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: edge.gycpi.b.yahoodns.net
Addresses: 2a00:1288:80:800::7001
           2a00:1288:80:800::7000
           87.248.118.22
           87.248.118.23
Aliases: mail.yahoo.com

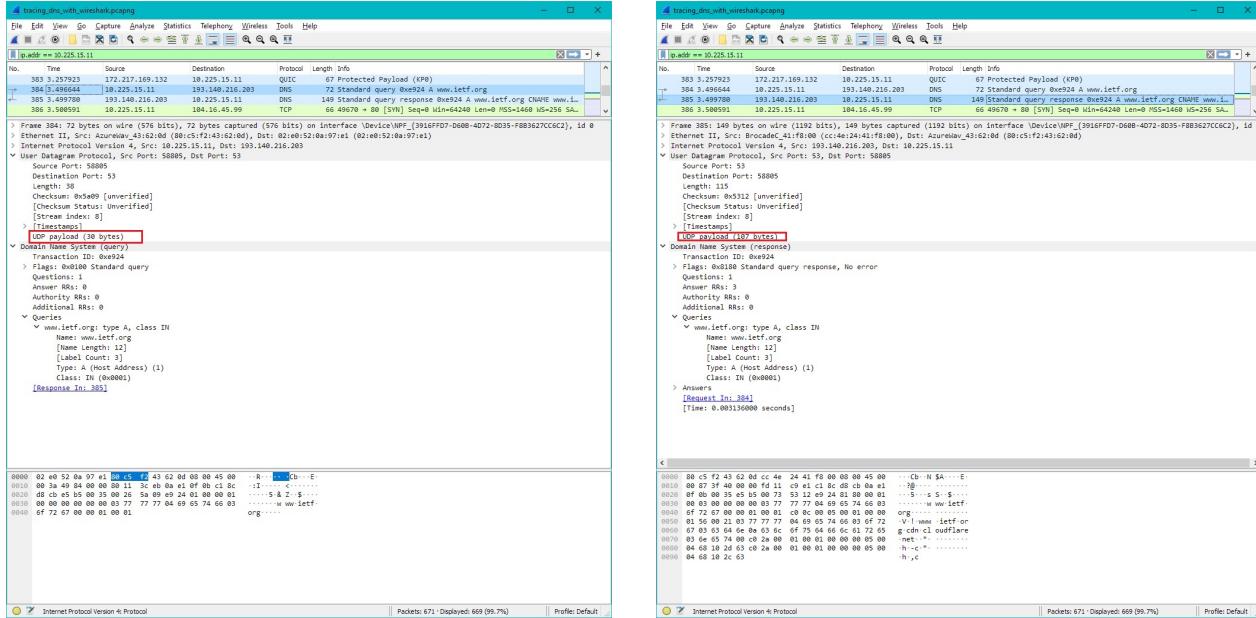
C:\Users\Melodi>
```

The screenshot shows a Microsoft Windows Command Prompt window titled "Command Prompt". The output of the command "nslookup mail.yahoo.com 8.8.8.8" is displayed. The "Aliases" section shows "mail.yahoo.com" with two IP addresses highlighted with a red box: "87.248.118.22" and "87.248.118.23".

# Tracing DNS with Wireshark

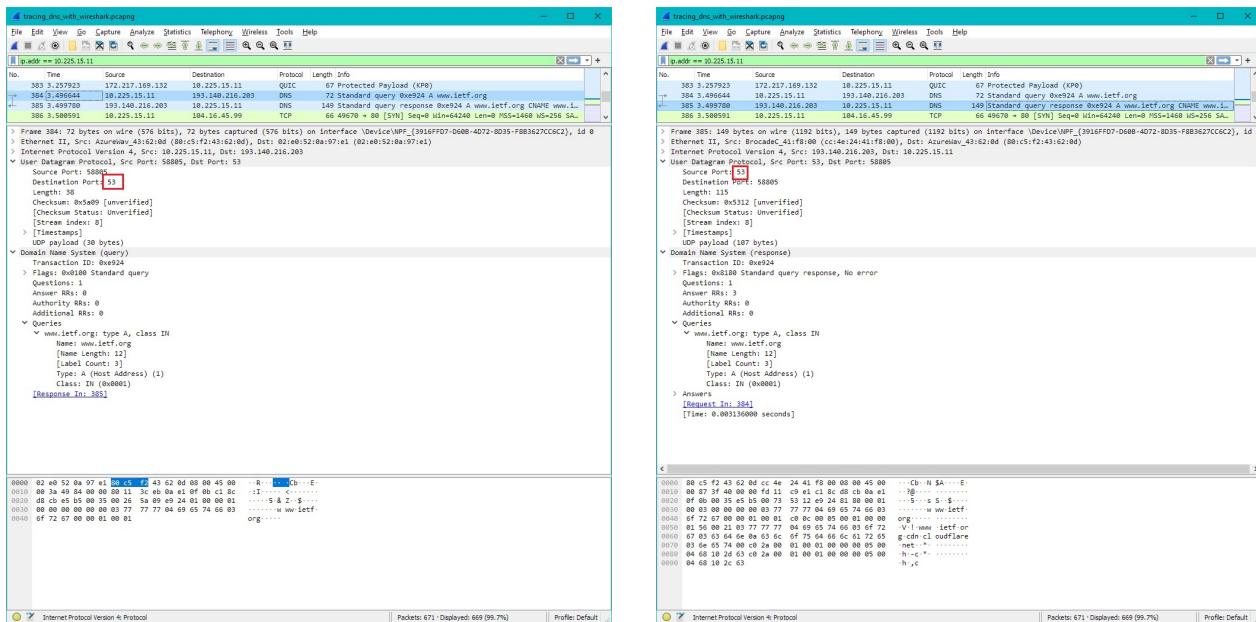
## 4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

As we can see from below screenshots they are send over UDP.



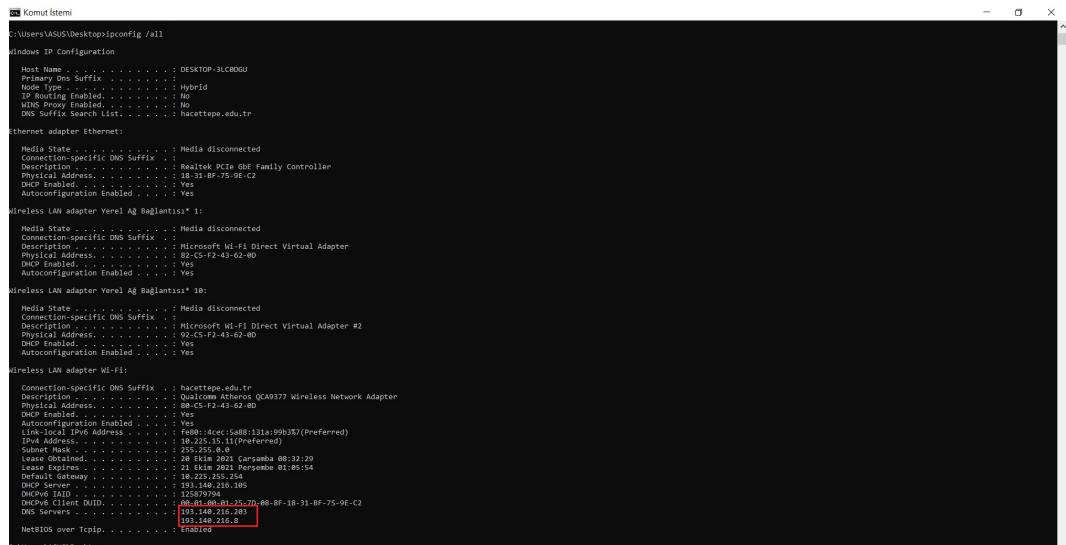
## 5. What is the destination port for the DNS query message? What is the source port of DNS response message?

The port 53 is used for DNS query. See screenshots below.



## 6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Yep it is same. The IP address is one of our local DNS servers.



```
C:\Users\ASUS\Desktop>ipconfig /all
Windows IP Configuration

Host Name . . . . . : DESKTOP-3LCB0GU
Primary Dns Suffix . . . . . :
Node Suffix . . . . . :
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : haccettepe.edu.tr

ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Realtek PCIe GbE Family Controller
    Physical Address . . . . . : 0B-31-BF-75-0E-C2
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

wireless LAN adapter Yerel Ağ Baglantısı* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address . . . . . : 92-C5-F2-43-62-00
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

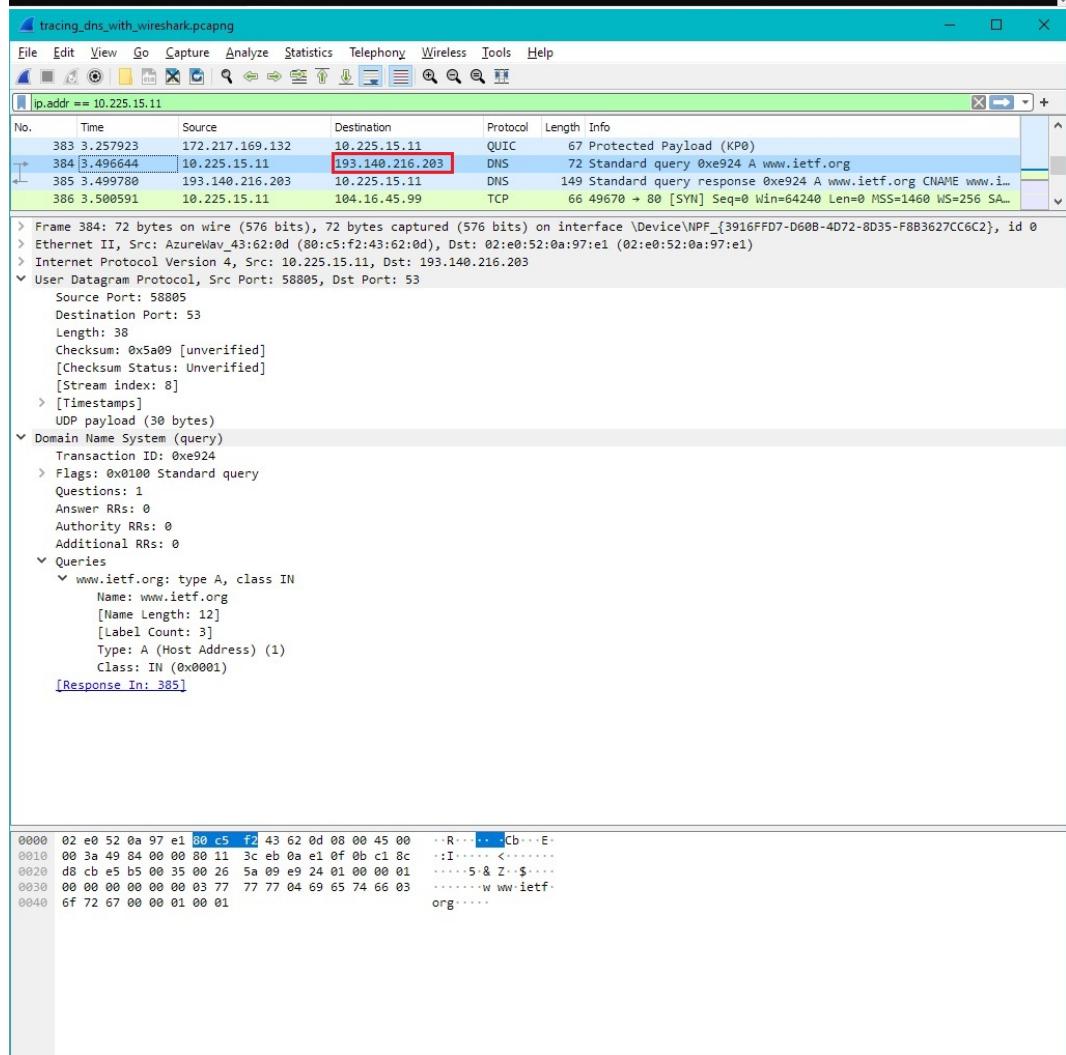
wireless LAN adapter Yerel Ağ Baglantısı* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address . . . . . : 92-C5-F2-43-62-00
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . . . . . : haccettepe.edu.tr
    Description . . . . . : Intel Dual Band Wireless-AC 9260
    Physical Address . . . . . : B8-C5-F2-43-62-00
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : Fe80::4cec:5a88:131a:99b3%7 (Preferred)
    IPv4 Address . . . . . : 193.140.216.203(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained . . . . . : 20 Ekim 2023 Çarşamba 08:32:29
    Lease Expires . . . . . : 20 Ekim 2023 Çarşamba 01:05:54
    Default Gateway . . . . . : 193.140.216.105
    DHCP Server . . . . . : 193.140.216.105
    DNS Servers . . . . . : 193.140.216.203
    DHCPv6 Client DUID . . . . . : 00-01-00-01-25-70-00-0f-18-31-bf-75-0e-c2
    DNS Servers . . . . . : 193.140.216.203
    NetBIOS over Tcpip . . . . . : Enabled

C:\Users\ASUS\Desktop>
```

No.	Time	Source	Destination	Protocol	Length	Info
383	3.257923	172.217.169.132	<b>10.225.15.11</b>	QUIC	67	Protected Payload (KPO)
384	3.496644	<b>10.225.15.11</b>	<b>193.140.216.203</b>	DNS	72	Standard query 0xe924 A www.ietf.org
385	3.499780	193.140.216.203	10.225.15.11	DNS	149	Standard query response 0xe924 A www.ietf.org CNAME www.i...
386	3.500591	10.225.15.11	104.16.45.99	TCP	66	49670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA...

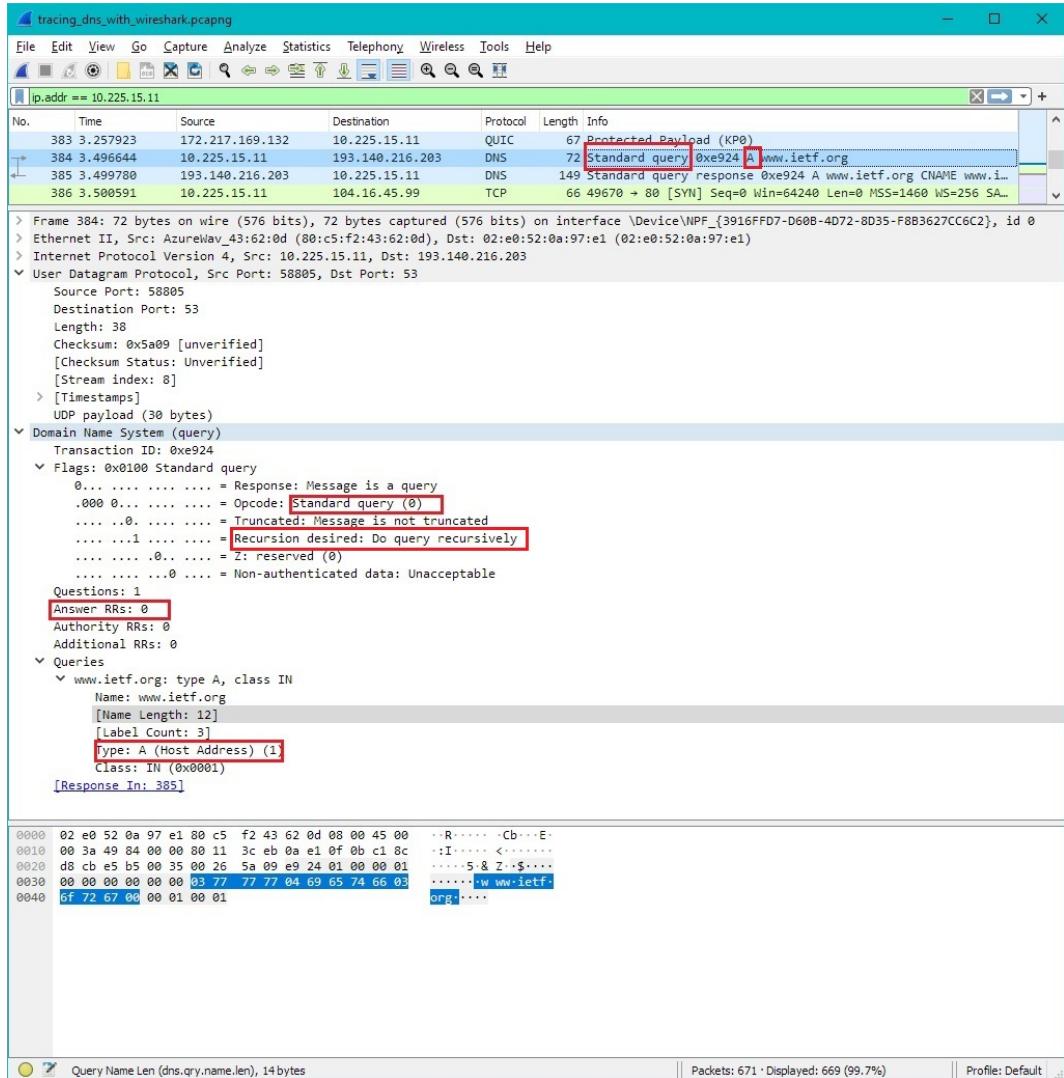
> Frame 384: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{3916FFD7-D60B-4D72-8D35-F883627CC6C2}, id 0
> Ethernet II, Src: Azureway\_43:62:0d (80:c5:f2:43:62:0d), Dst: 02:e0:52:0a:97:e1 (02:e0:52:0a:97:e1)
> Internet Protocol Version 4, Src: 10.225.15.11, Dst: 193.140.216.203
▼ User Datagram Protocol, Src Port: 58805, Dst Port: 53
 Source Port: 58805
 Destination Port: 53
 Length: 38
 Checksum: 0x5a09 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 8]
 > [Timestamps]
 UDP payload (30 bytes)
 ▼ Domain Name System (query)
 Transaction ID: 0xe924
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > www.ietf.org: type A, class IN
 Name: www.ietf.org
 [Name Length: 12]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 385]

0000 02 e0 52 0a 97 e1 80 c5 f2 43 62 0d 08 00 45 00 ·R...·.Cb·.E·
0010 00 3a 49 84 00 00 80 11 3c eb 0a e1 0f 0b c1 8c ·:I.....<.....
0020 d8 cb e5 b5 00 35 00 26 5a 09 e9 24 01 00 00 01 ····5&Z:\$···
0030 00 00 00 00 00 00 03 77 77 04 69 65 74 66 03 ····w ww.ietf·
0040 6f 72 67 00 00 01 00 00 1 ····org···

Internet Protocol Version 4: Protocol | Packets: 671 · Displayed: 669 (99.7%) | Profile: Default

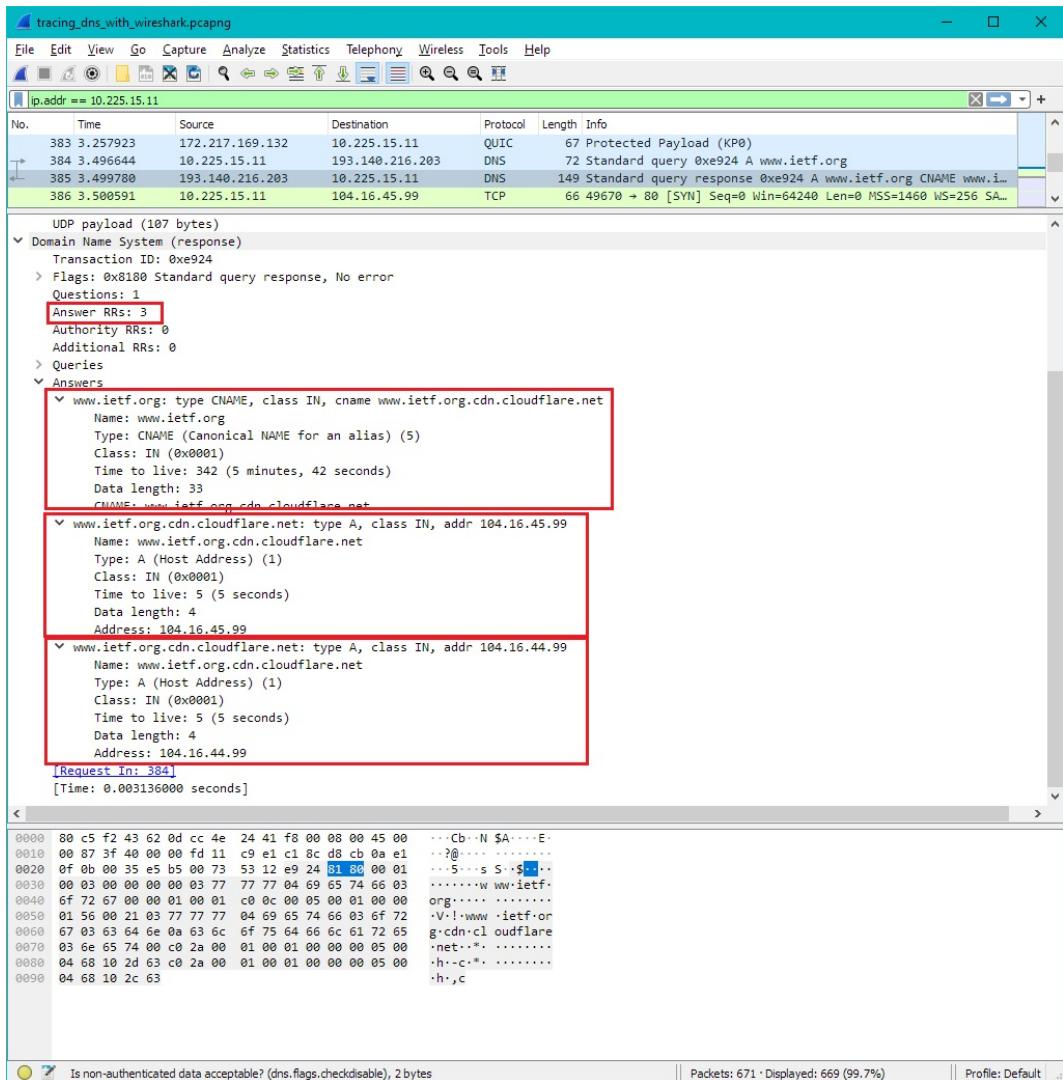
## 7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The query message is Standard Query type A. DNS query type is recursive query. It contains 0 answer aka no answer. Check screenshot below.



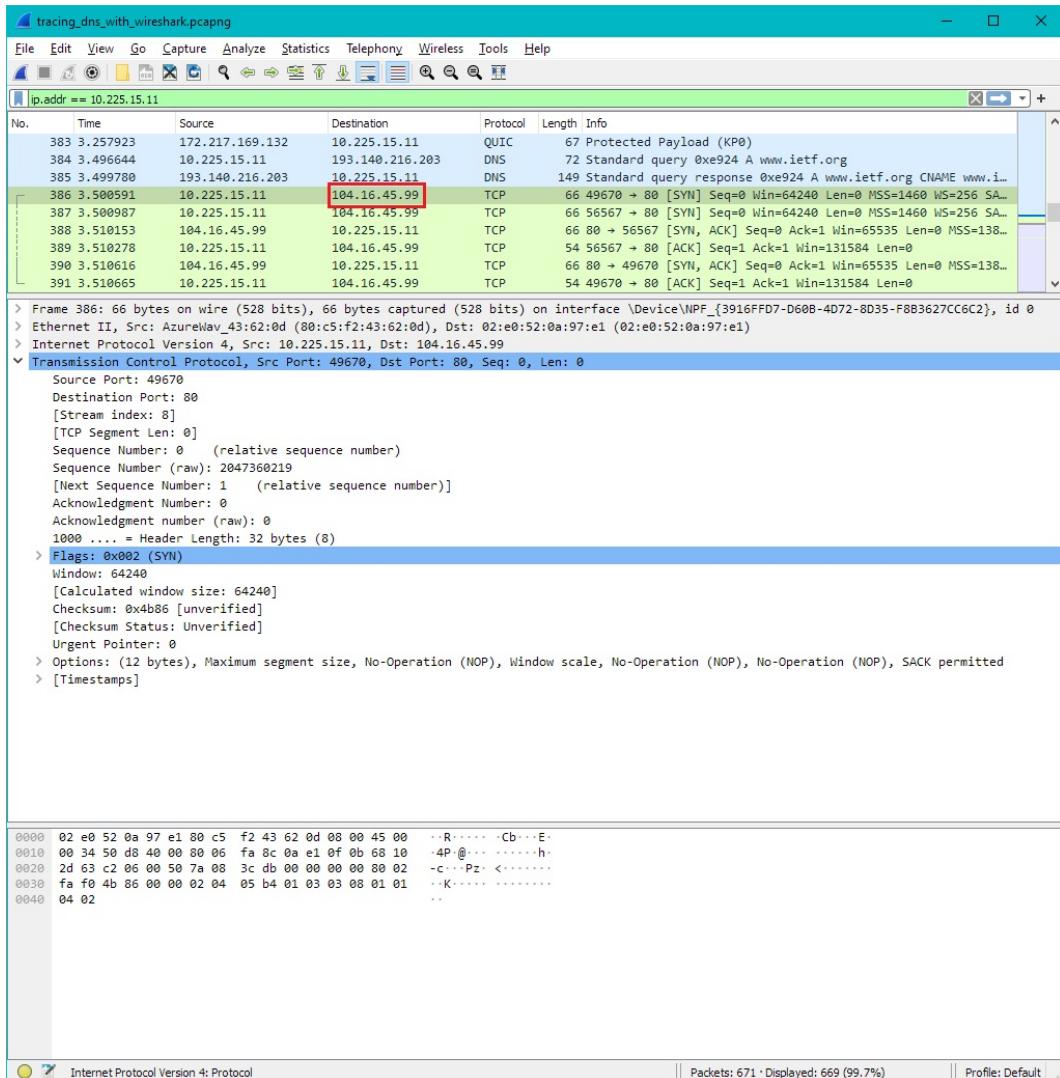
## 8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

There are 3 answers total. First answer is type CNAME meaning it's "Name: " is alias for some name used for that DNS servers while value "CNAME: " is the canonical name. Other two are type A meaning "Name: " is host name while the values are IP addresses. They also contain class and data length attributes. Check screenshot below.



## 9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Yep it is the 104.16.45.99 one.



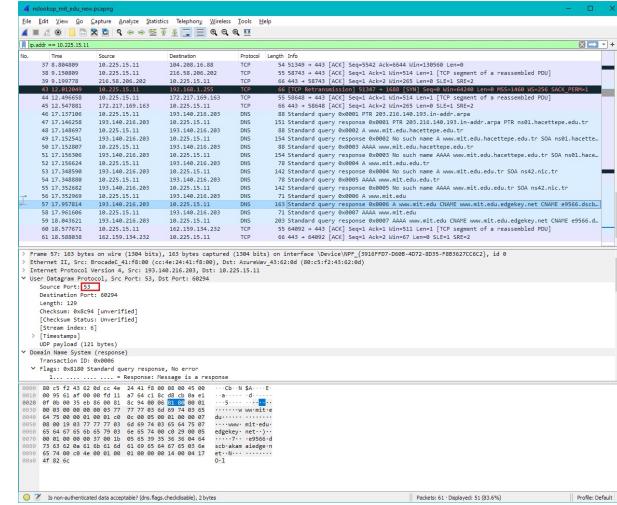
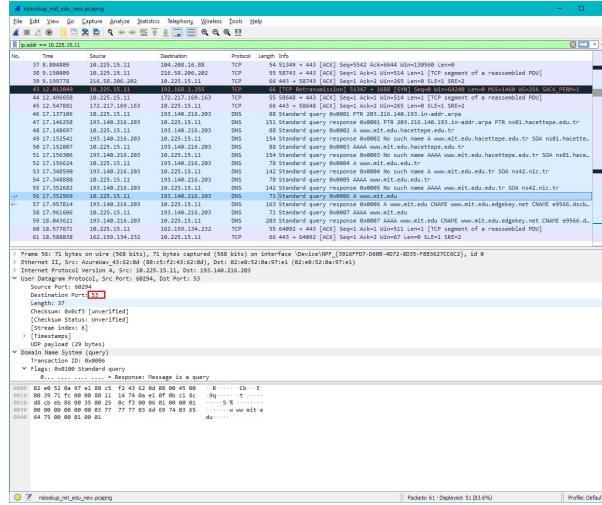
## 10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No, It does not issue new DNS queries when it already obtained for the "www.ietf.org". It issues new DNS queries only when trying to reach new servers like: "analytics.ietf.org". So it would issue a query only if the images were on different server. Since images are on the same server it does not issue. We can not show a screenshot for this answer because it would be too complex so it is only explanation.

# Nslookup www.mit.edu

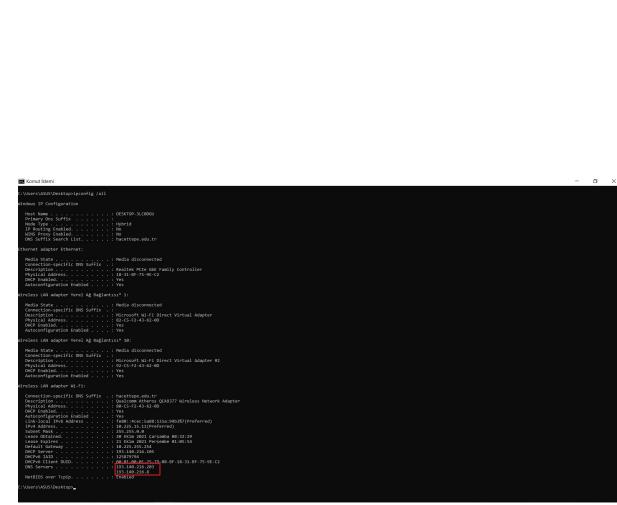
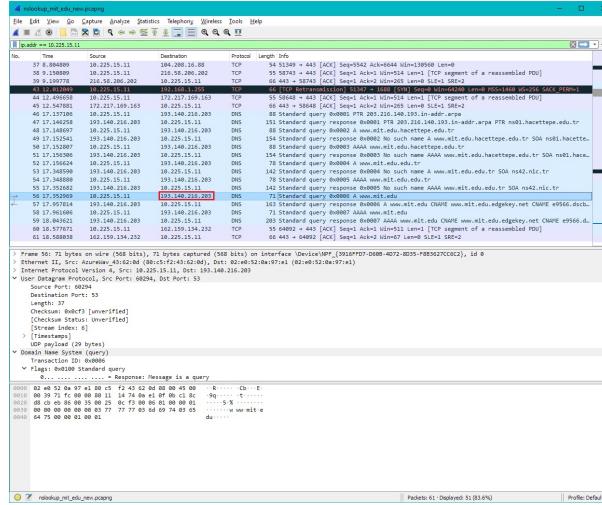
## 11. What is the destination port for the DNS query message? What is the source port of DNS response message?

It is 53 for both. We think this is because for DNS queries port 53 is used as standard.



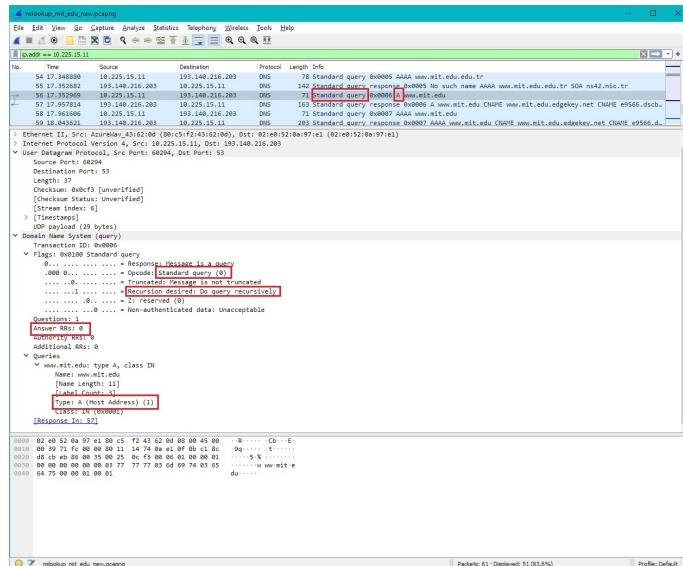
## 12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

It is send to 193.140.216.203 which is one of our local DNS servers and the default one.



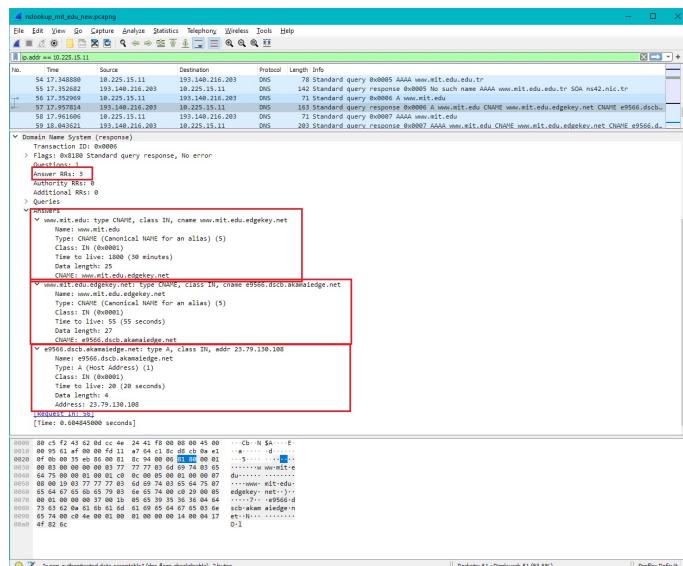
## 13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The query message is Standard Query type A. DNS query type is recursive query. It contains 0 answer aka no answer. Check screenshot below.



## 14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

It contains 3 answers. First two answers a type CNAME meaning "Name: " will be alias and value "CNAME: " will be the canonical name. Last one is type A meaning "Name: " will be hostname and value "Address: " will be the IP address. Also "Class: " and data length attributes are contained. Check screenshot below.



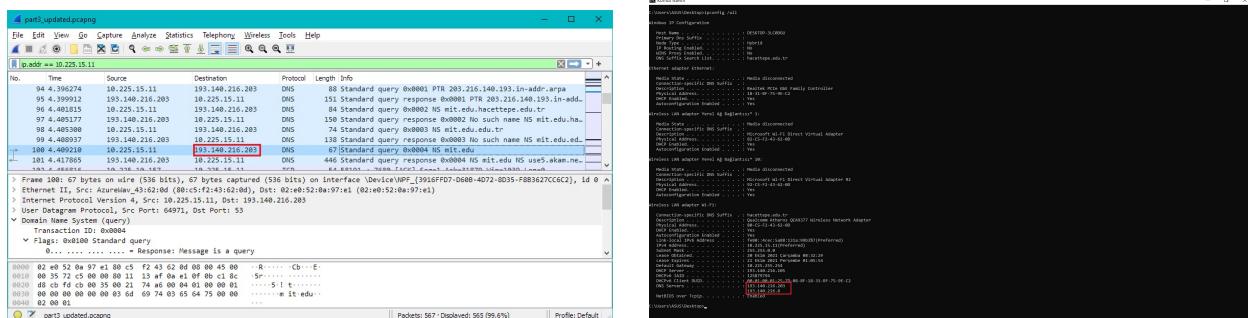
## 15. Provide a screenshot.

Screenshots are provided for each answer.

## nslookup -type=NS mit.edu

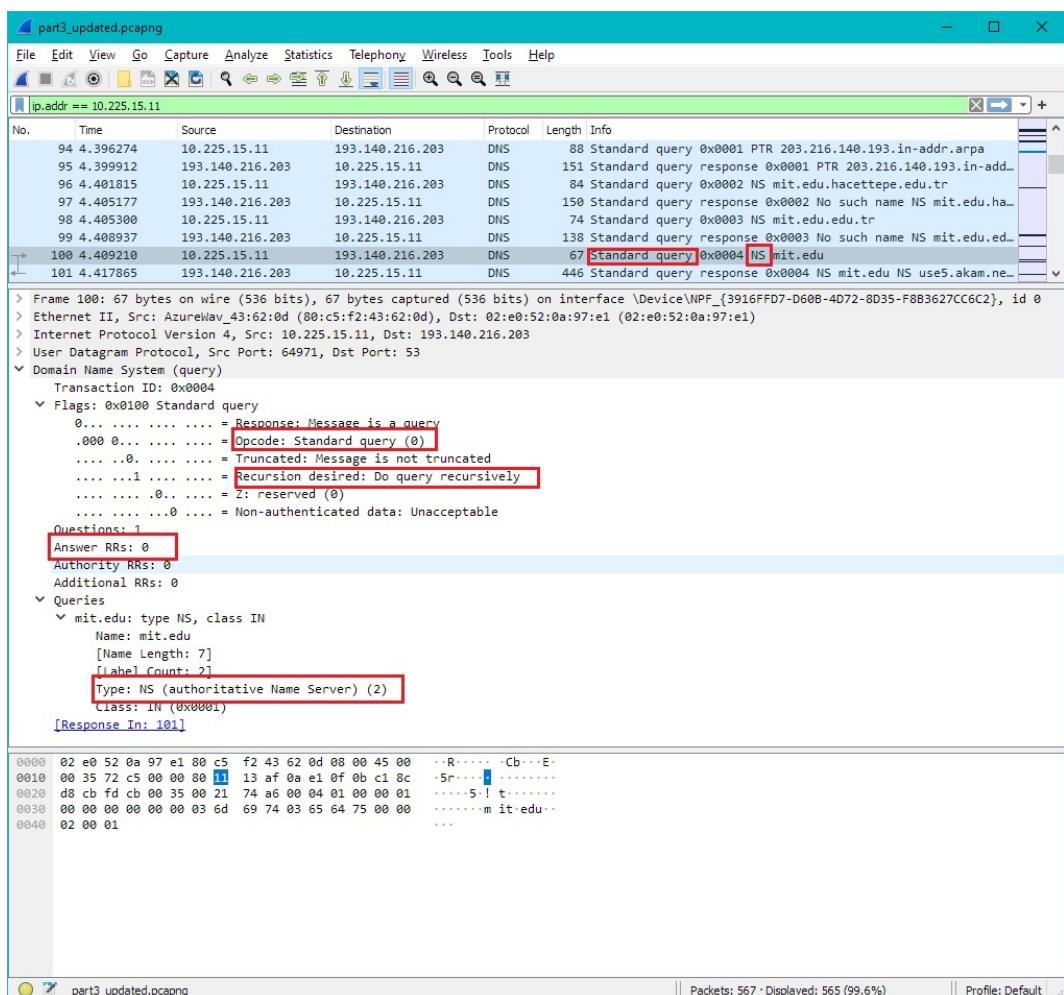
### 16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

It is send to 193.140.216.203 which is one of our local DNS servers and the default one.



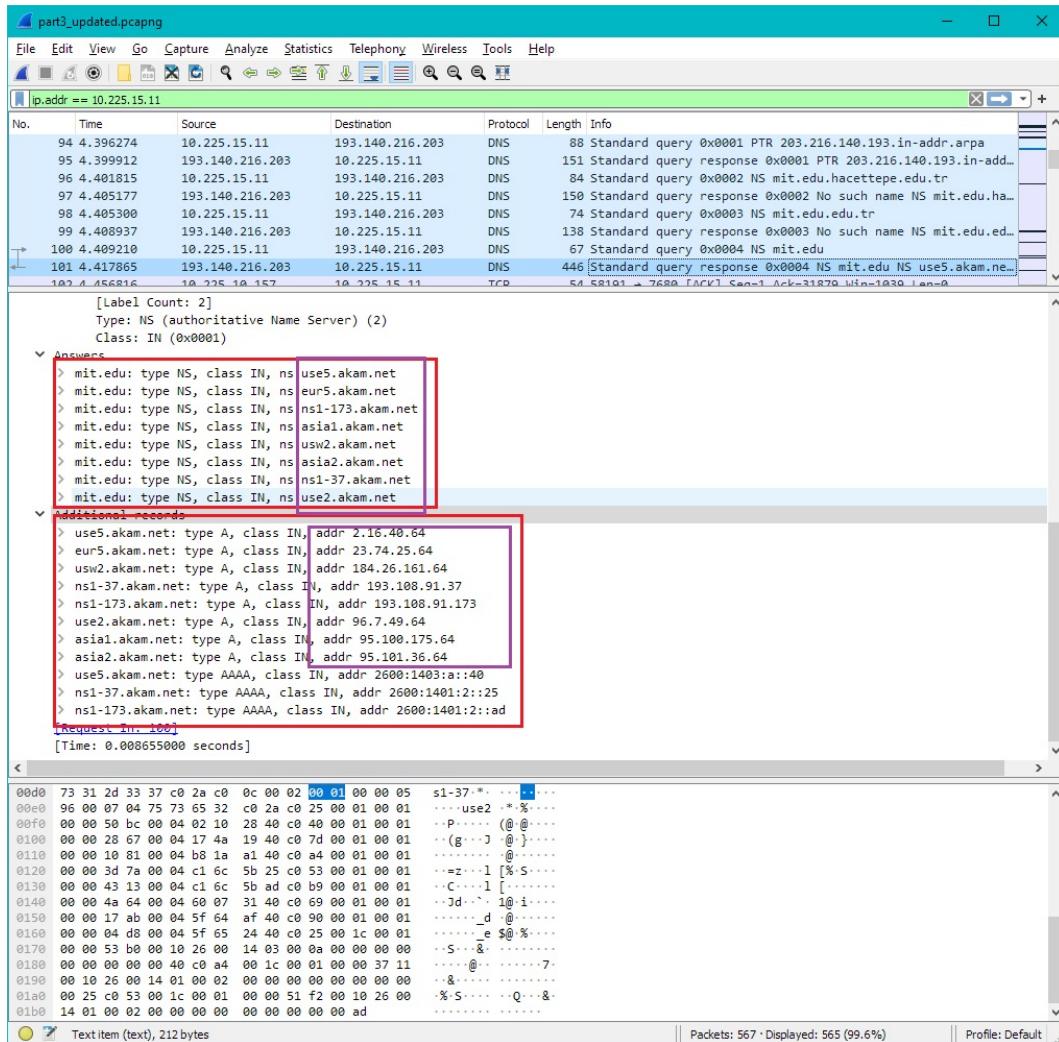
### 17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The query message is Standard Query type NS. DNS query type is recursive query. It contains 0 answers aka no answer. Check screenshot below.



## 18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

Response message contains the following name servers: "use5.akam.net", "eur5.akam.net", "ns1-173.akam.net", "asia1.akam.net", "usw2.akam.net", "asia2.akam.net", "ns1-37.akam.net", "use2.akam.net". Yes it provides ip addresses for all of these name servers. We think it wouldn't provide the ones we already had but since we done DNS flush it provides all.



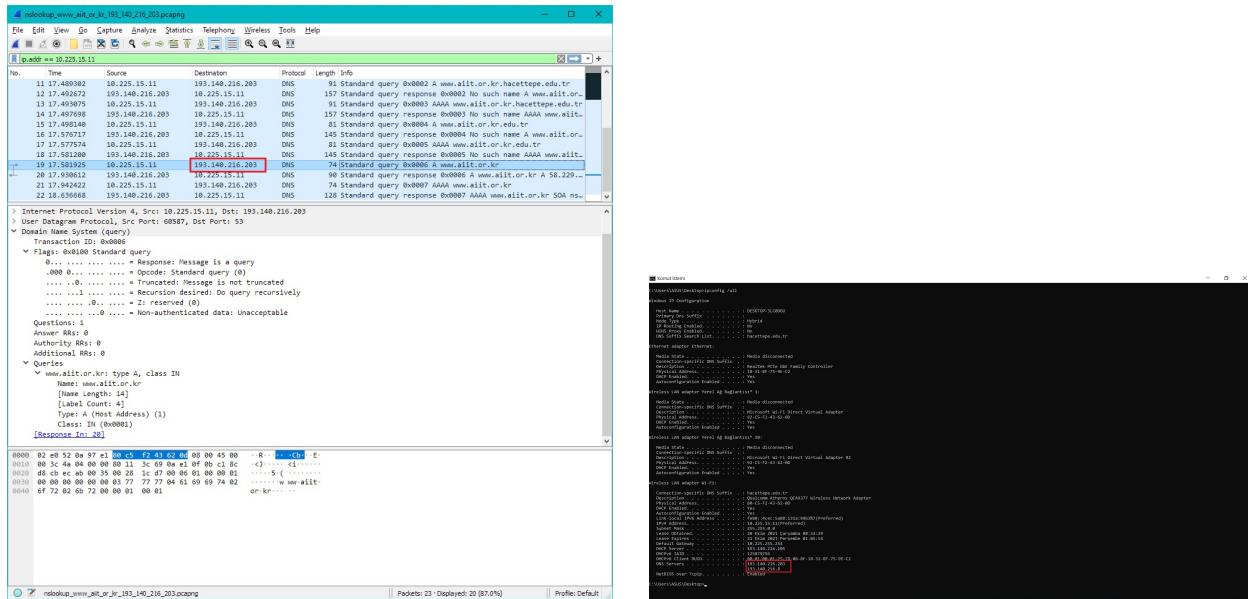
## 19. Provide a screenshot.

Screenshots are provided for each answer.

## nslookup www.aiit.or.kr 193.140.216.203

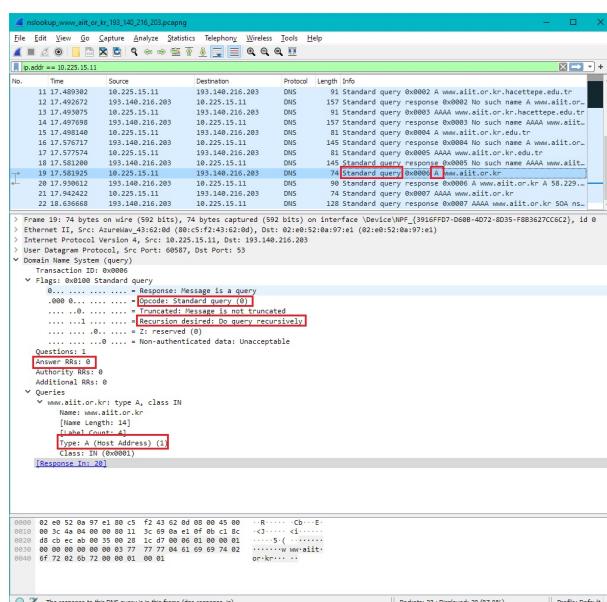
**20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?**

It is sent to 193.140.216.203 which is the parameter we entered but also our default local DNS server. TA gave us Hacettepe DNS for testing and We think aim was to make us realize the difference but we were already doing the test with in Hacettepe University so entering parameter did not change our DNS since it is the same with parameter. Regardless the importance is understood and noted.



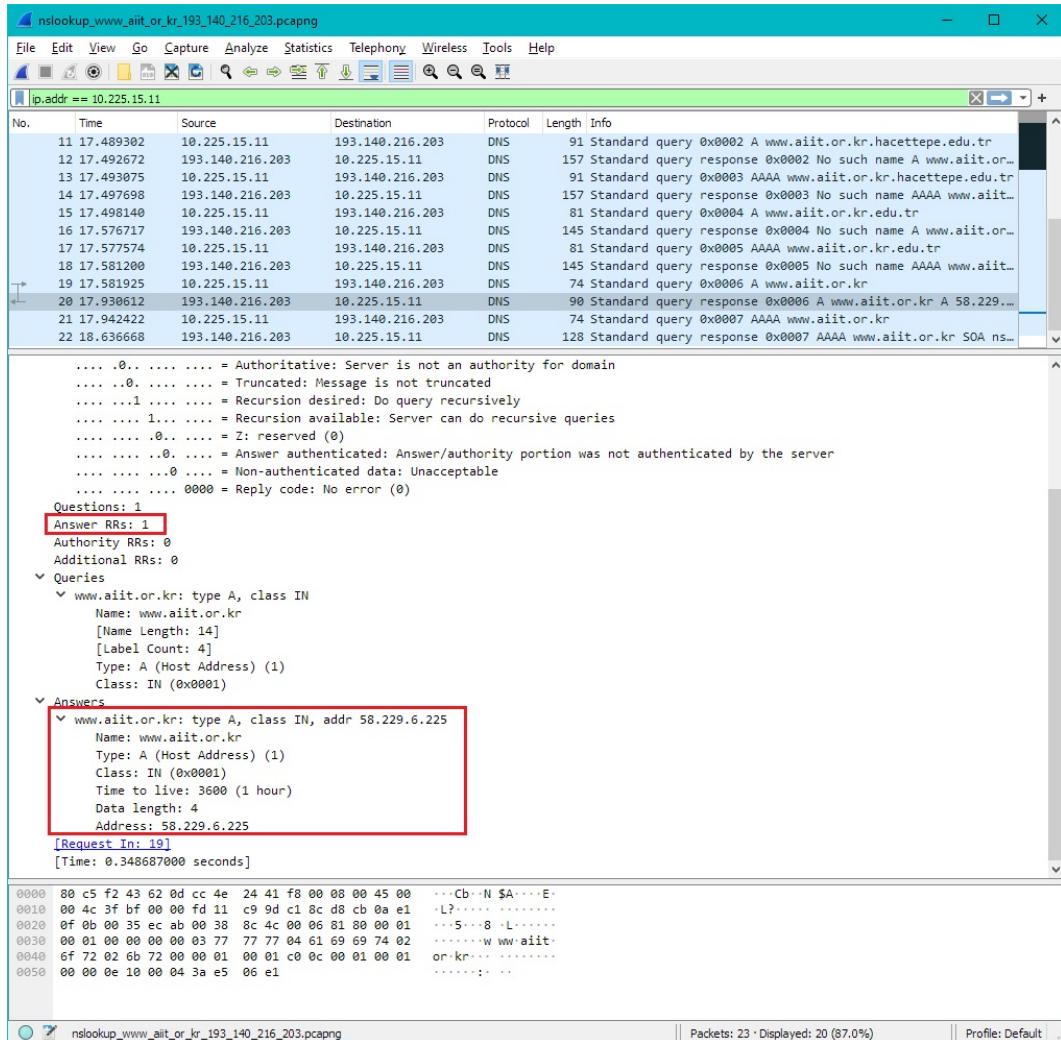
**21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

The query message is Standard Query type NS. DNS query type is recursive query. It contains 0 answer aka no answer. Check screenshot below.



## 22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

One answer is provided. It is type A meaning the "Name: " will correspond to hostname and value "Address: " will be the IP address. It also contains type, class, time to live, data length attributes.



## 23. Provide a screenshot.

Screenshots are provided for each answer.

## **REFERENCES**

LaTex Tutorials  
Assignment Paper  
Wireshark FAQ  
Wireshark User's Guide  
IBM's Query Type Definition  
NS1.com's Query Type Definition