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
Assoc. Prof. Sevil ŞEN
ssen@cs.hacettepe.edu.tr

Group 14
Source IP : 10.225.15.11

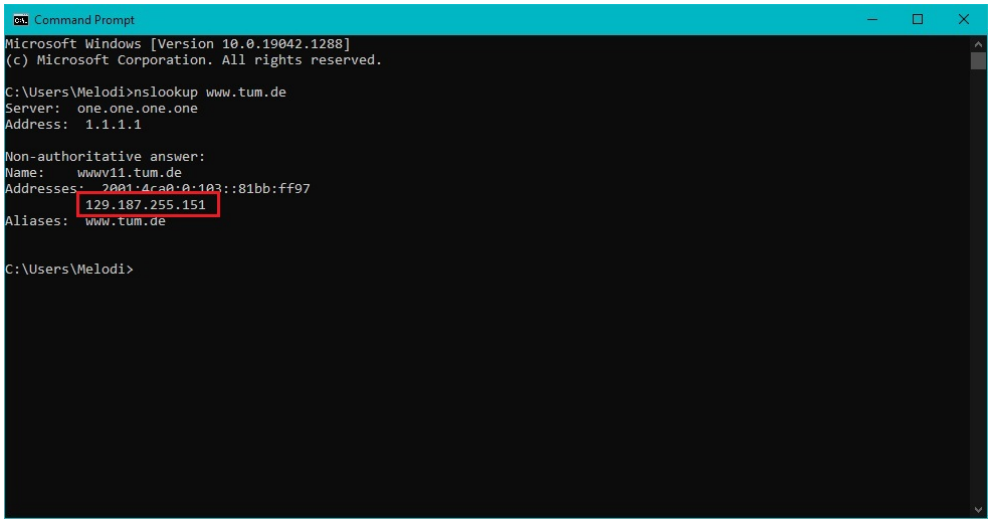
Oct 20,2021

SOLUTIONS

nslookup

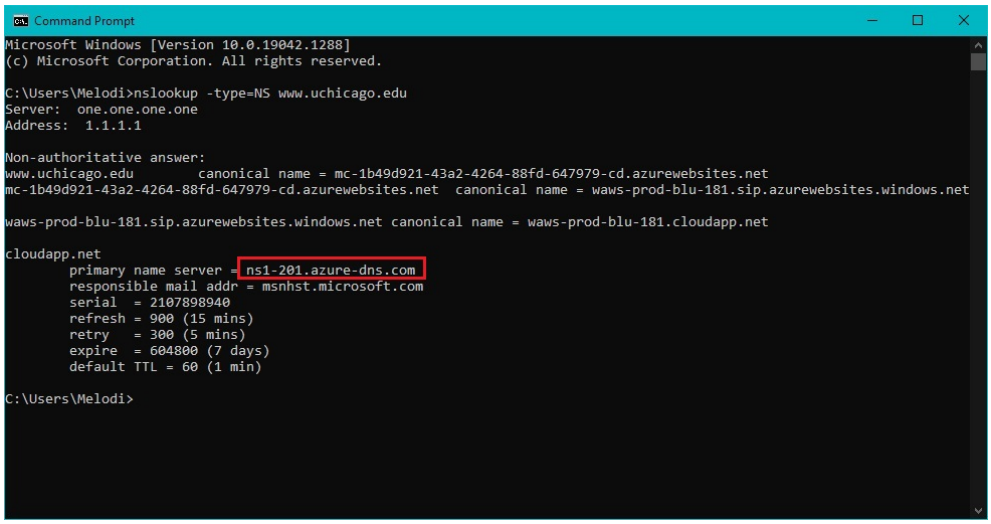
1. Run nslookup to obtain the IP address of a Web server in Europe. What is the IP address of that server?

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



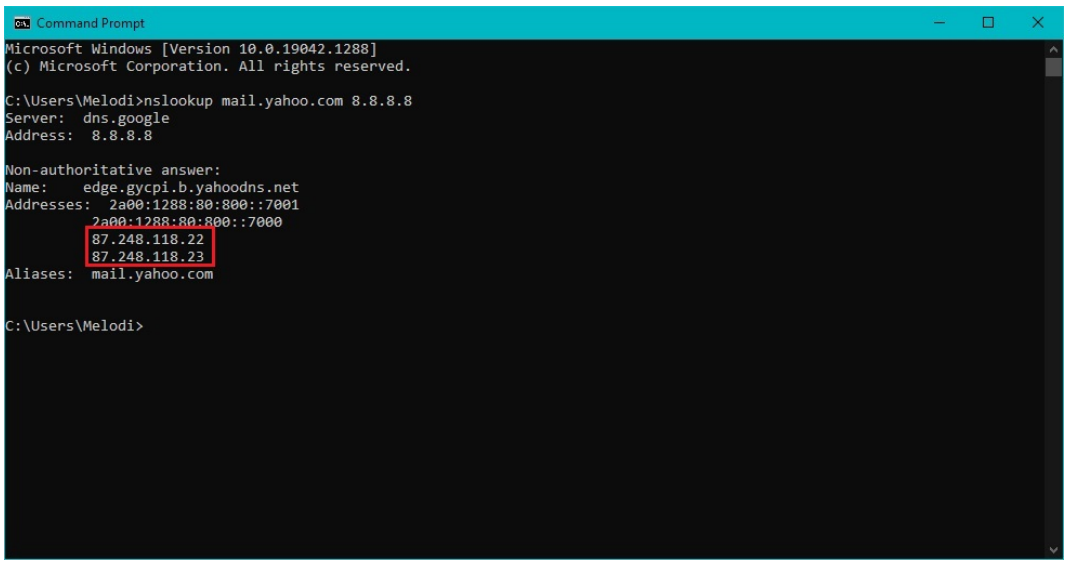
2. Run nslookup to determine the authoritative DNS servers for a university in United States.

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



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?

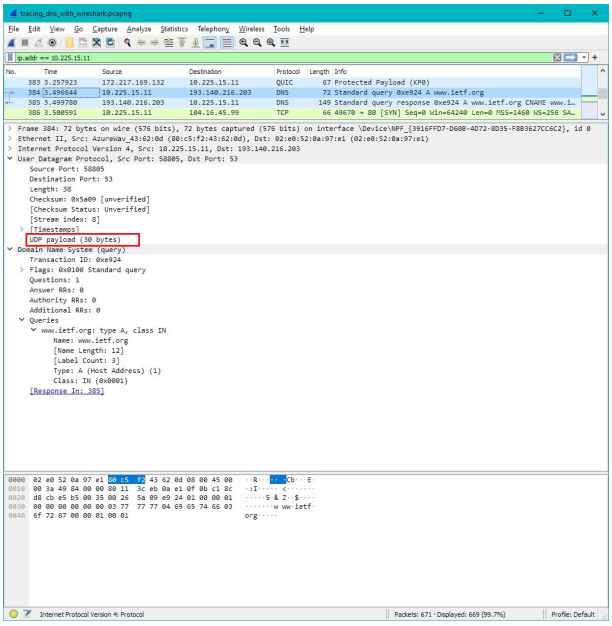
It's IP adress is 87.248.118.22 and 87.248.118.23 as can be seen in screenshot.

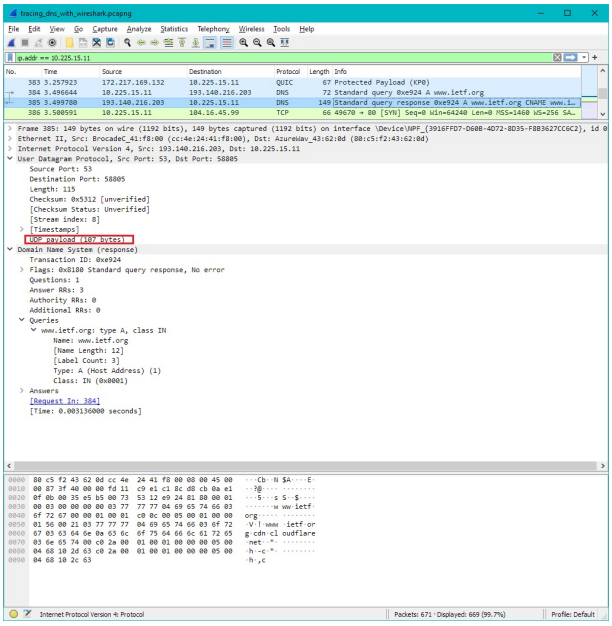


Tracing DNS with Wireshark

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

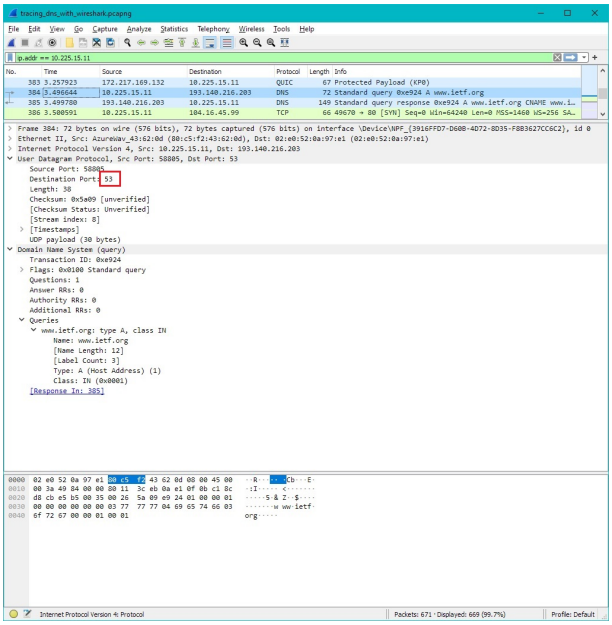
As we can see from below screenshots they are send over UDP.

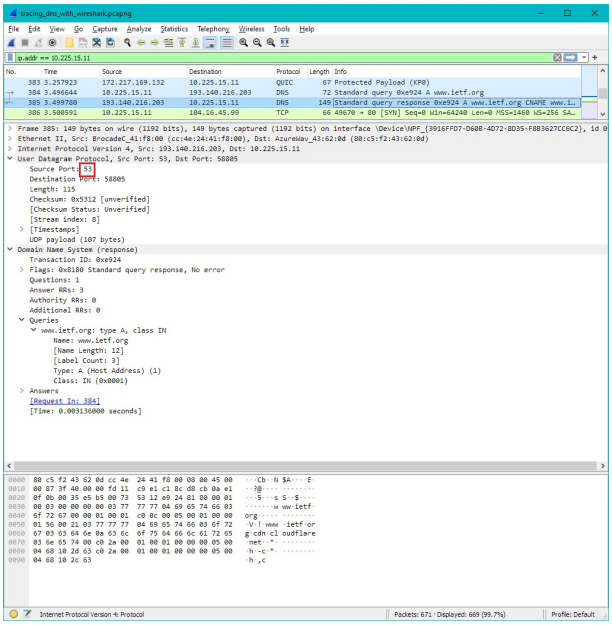




5. What is the destination port for the DNS query message? What is the source port of DNS response message?

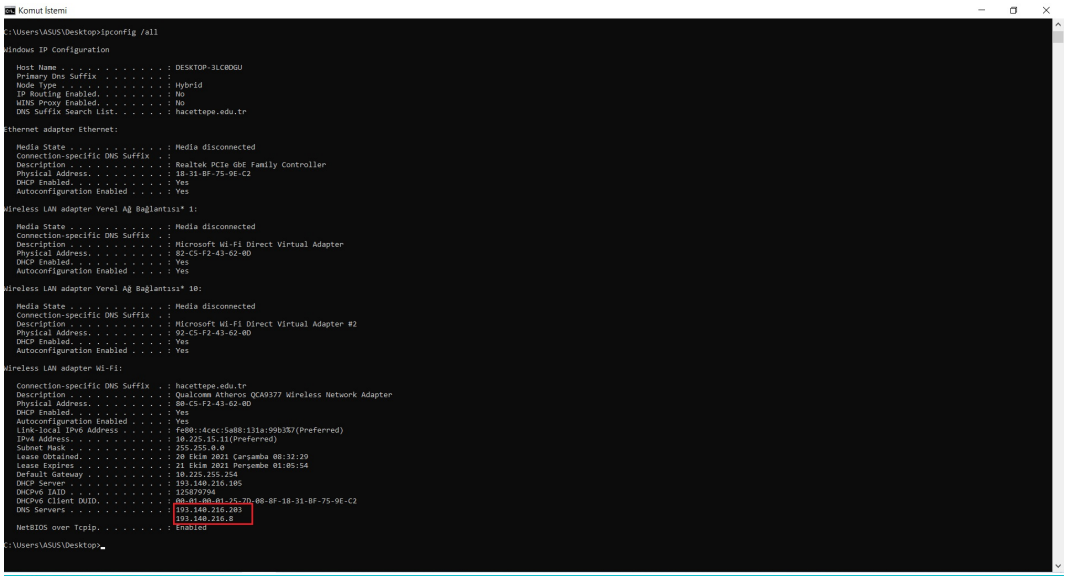
The port 53 is used for DNS query. See screenshots below.

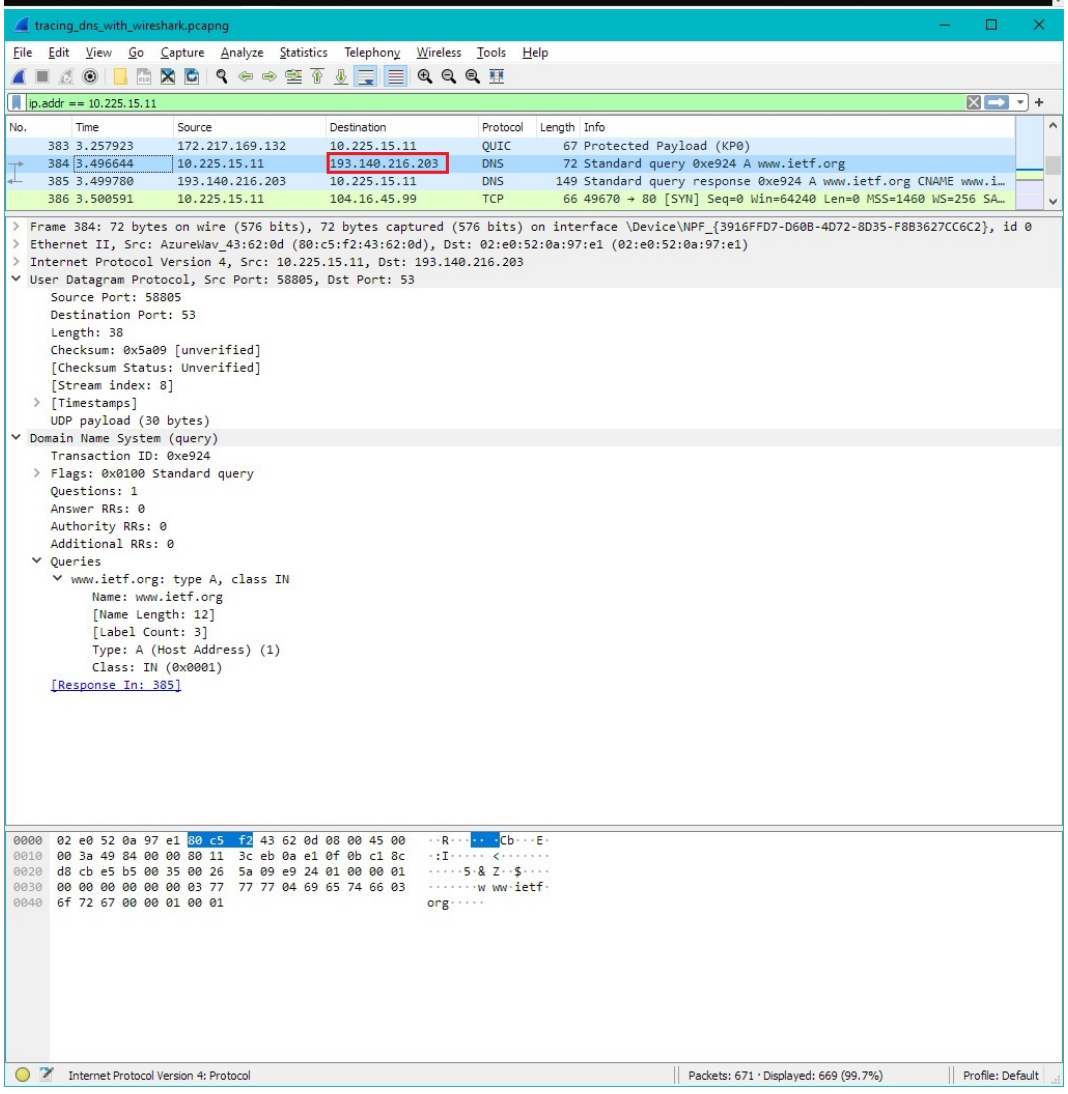




6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

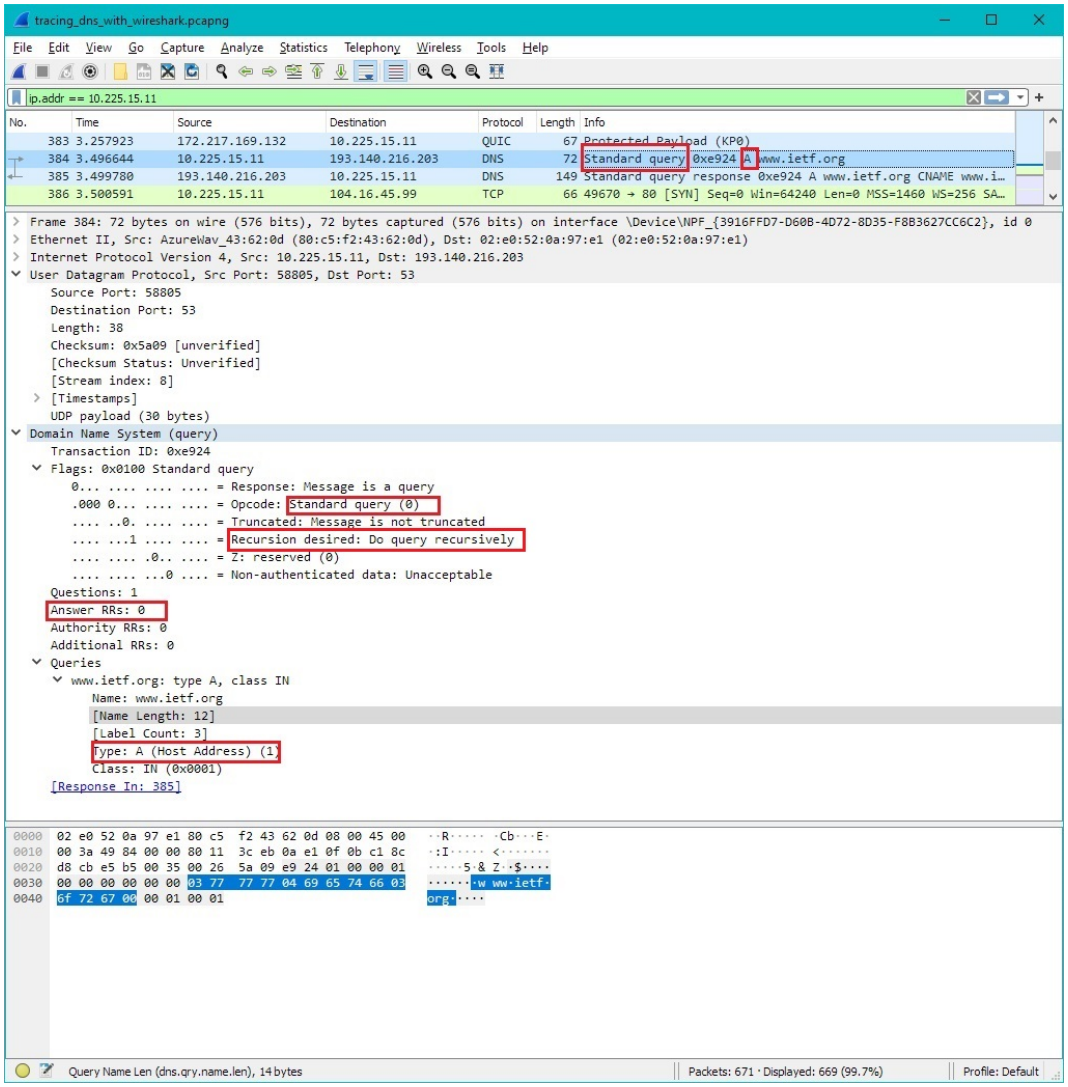
Yep it is same. The IP adress is one of our local DNS servers.





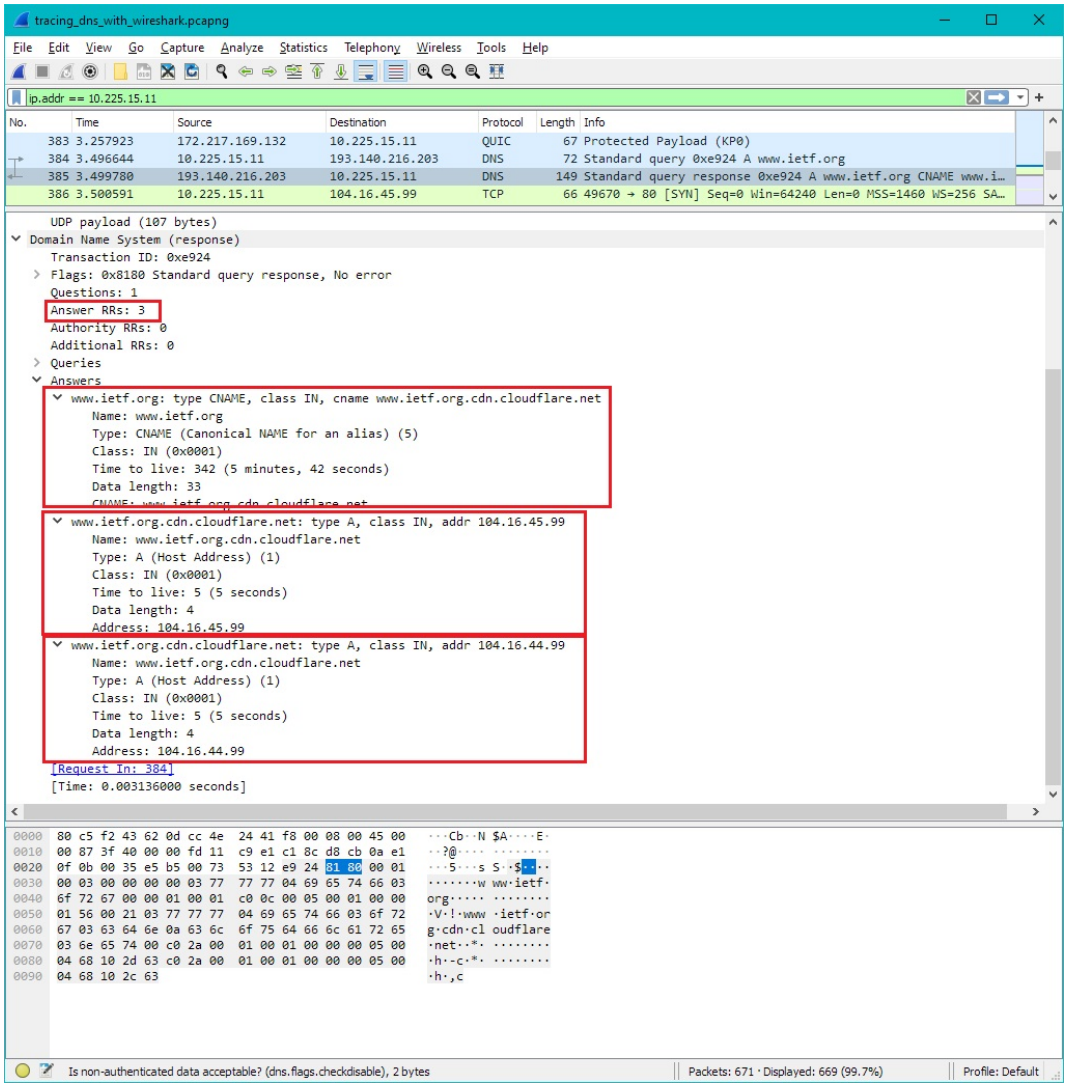
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

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



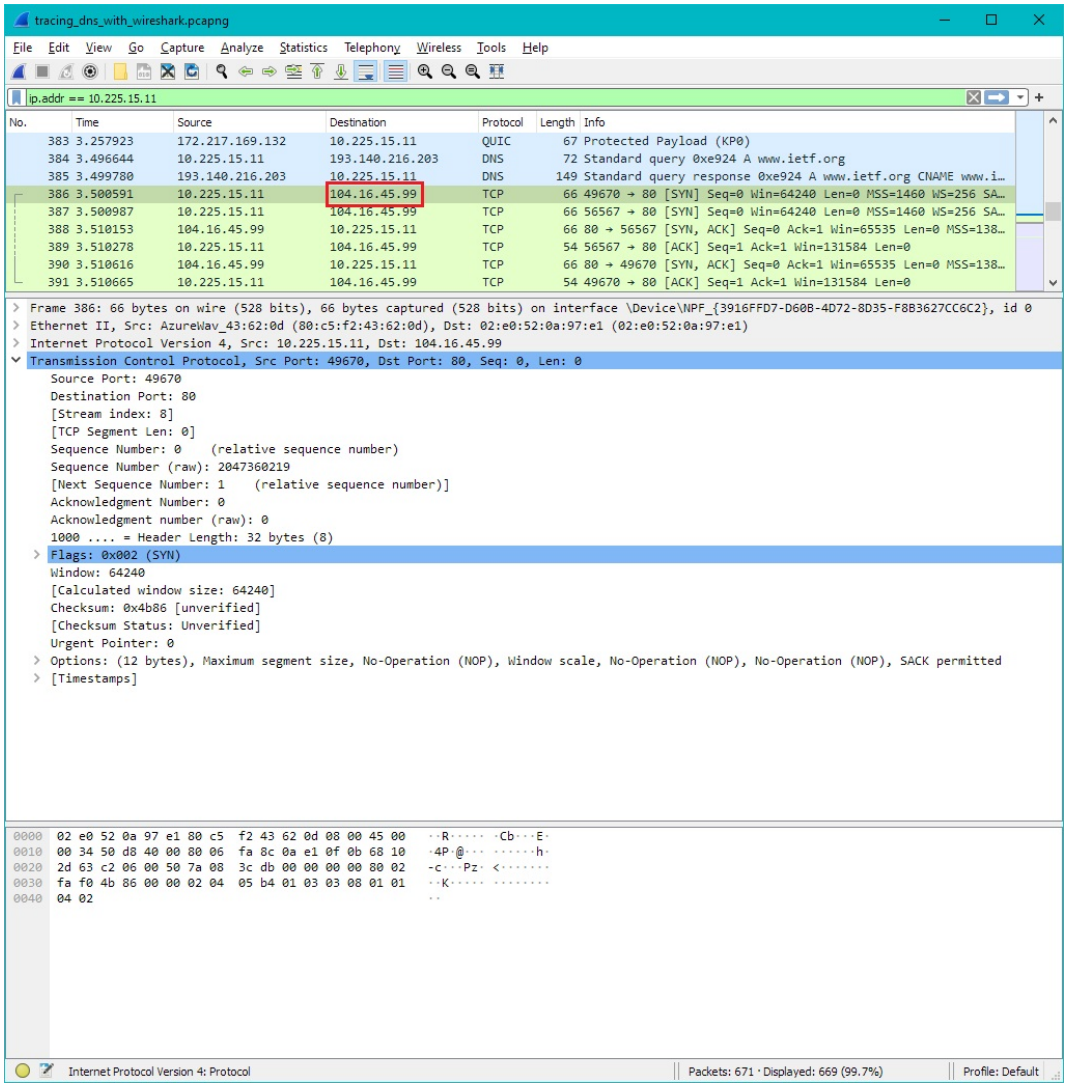
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

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.



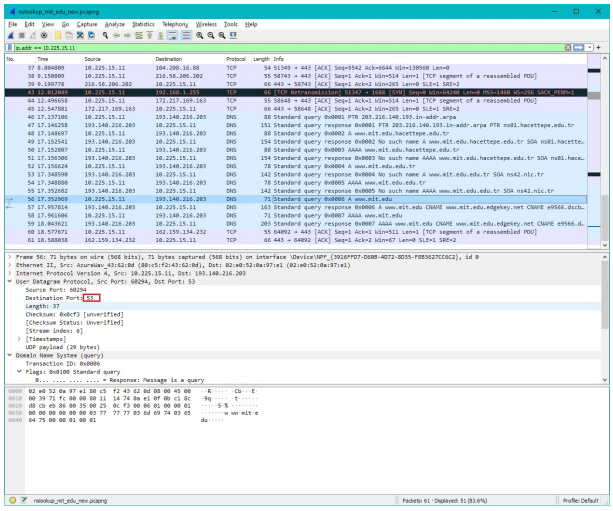
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

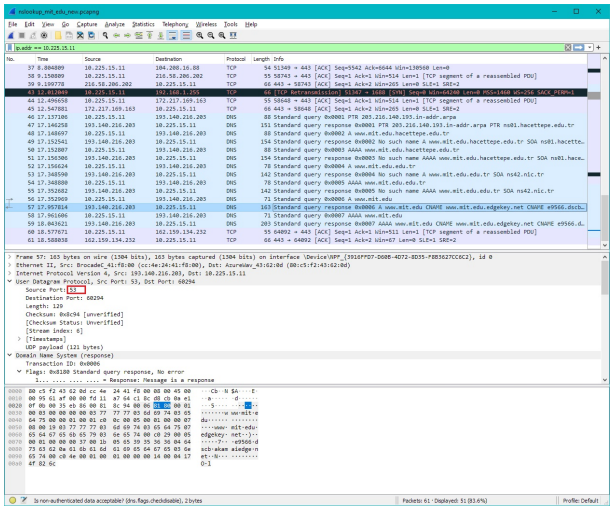
No, It does not issue new DNS queries when it already obtained for the "www.ietf.org". It issues new DNS queries only when trying to reach new servers like: "analytics.ietf.org". So it would issue a queire only if the images were on different server. Since images are on the save server it does not issue. 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?

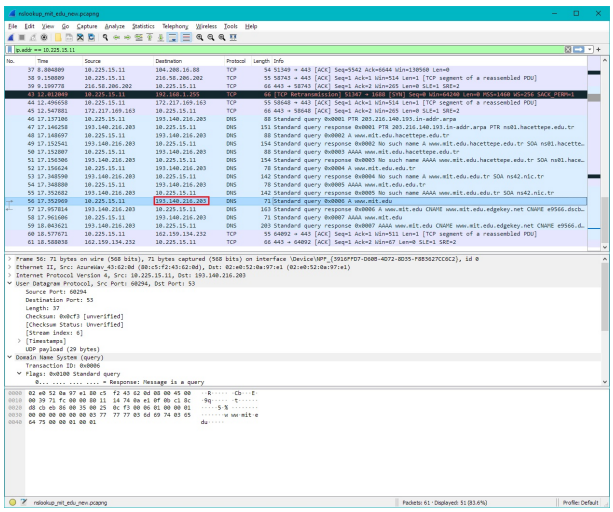
It is 53 for both. We think this is because for DNS queries port 53 is used as standard.

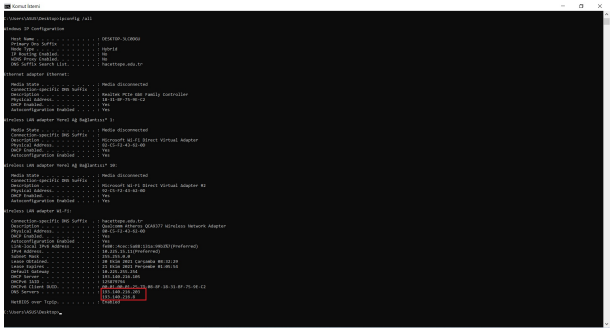




12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

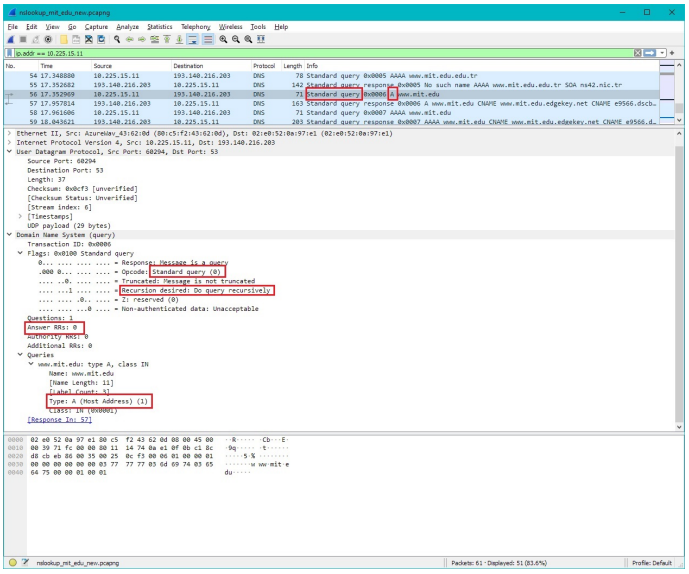
It is send to 193.140.216.203 which is one of our local DNS servers and the default one.





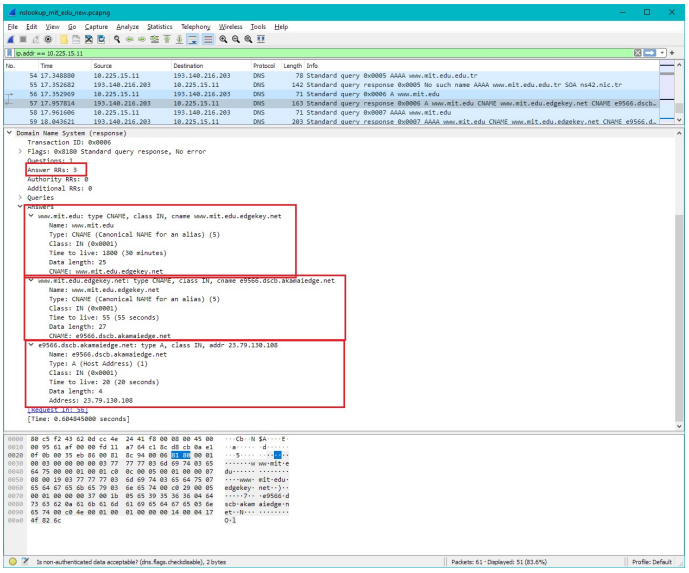
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

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.



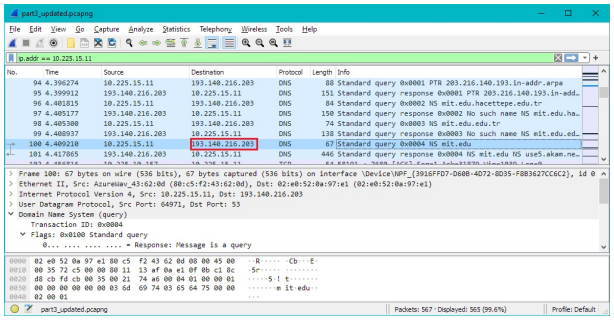
15. Provide a screenshot.

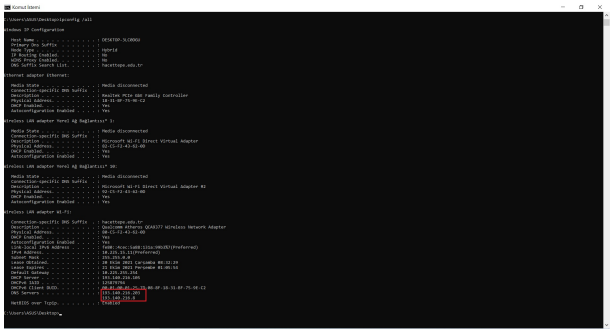
Screenshots are provided for each answer.

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?

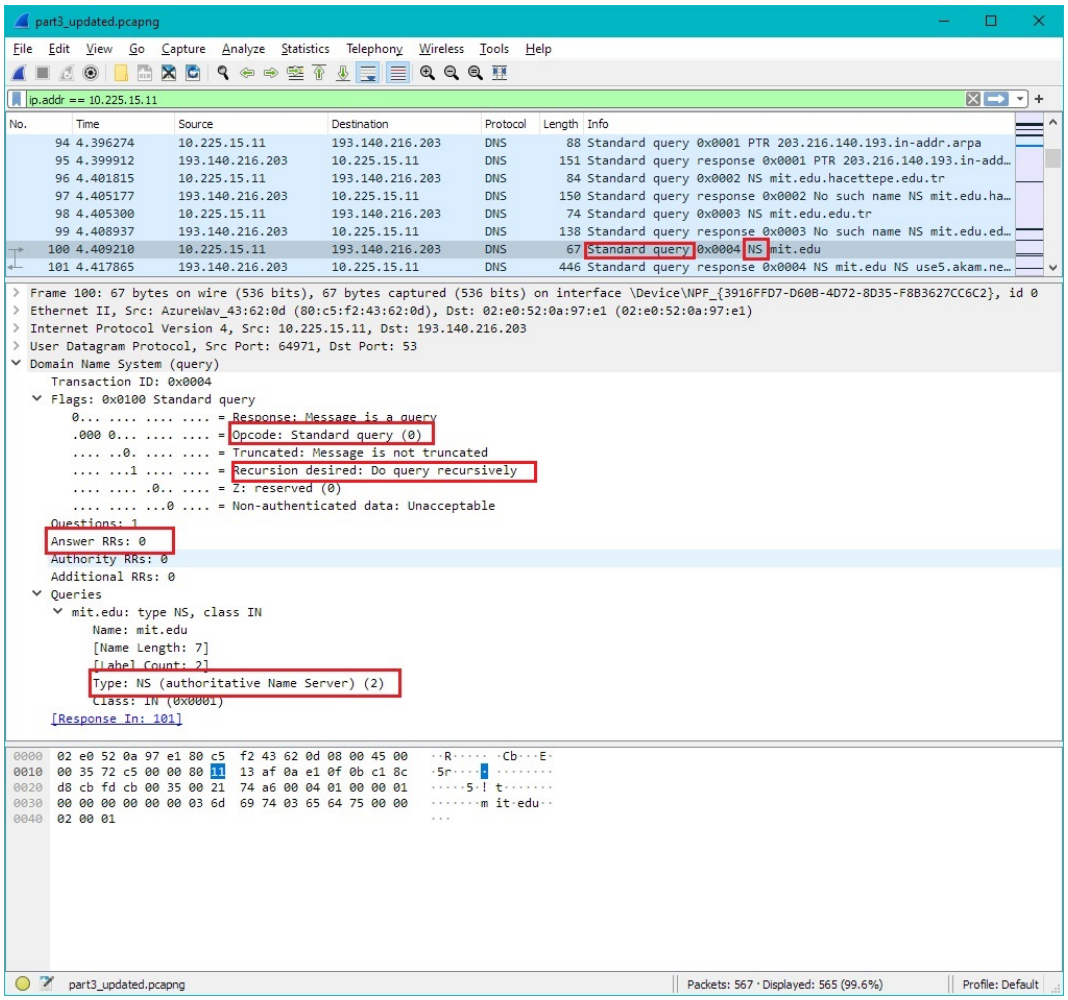
It is send to 193.140.216.203 which is one of our local DNS servers and the default one.





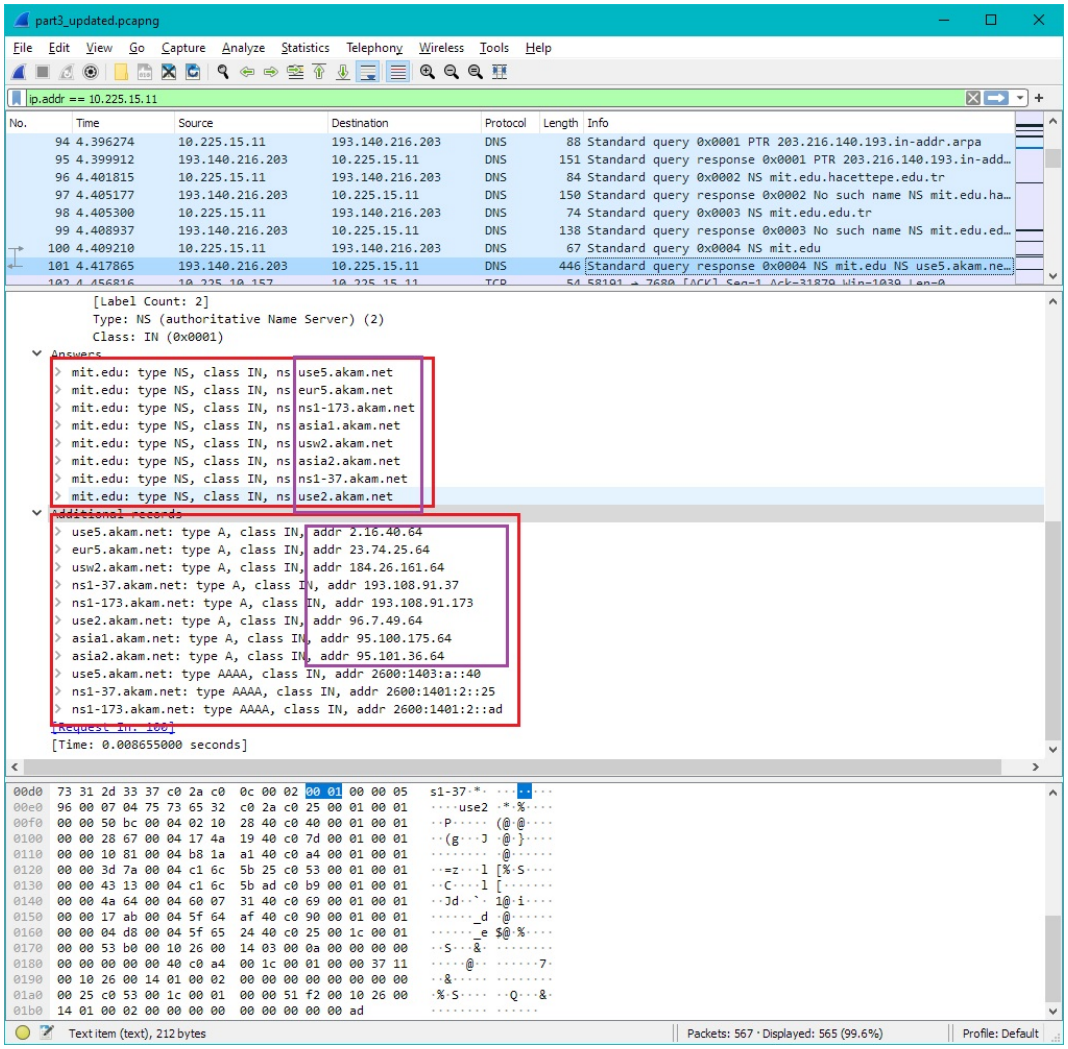
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The query message is Standard Query type NS. DNS query type is recursive query. It contains 0 answer 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.



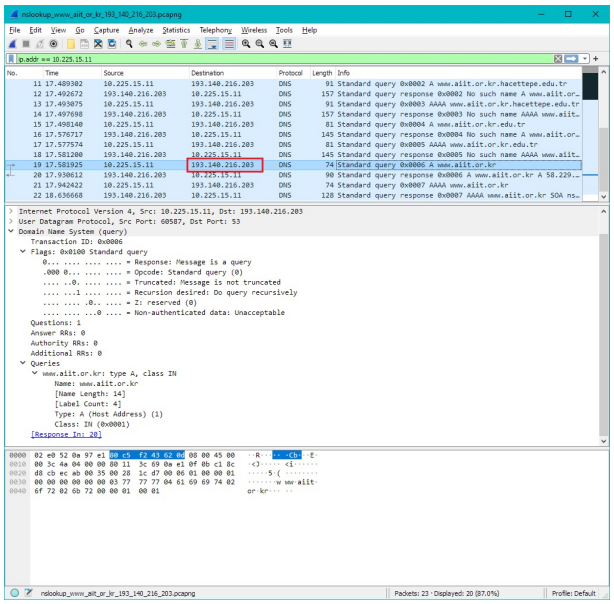
19. Provide a screenshot.

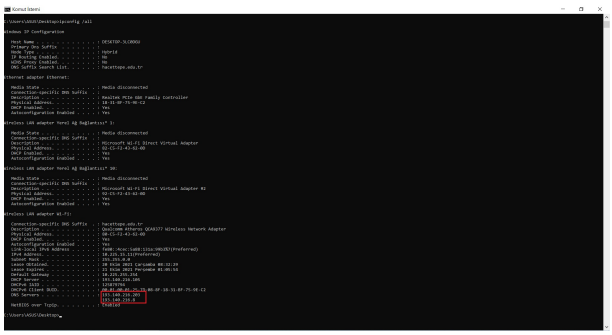
Screenshots are provided for each answer.

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?

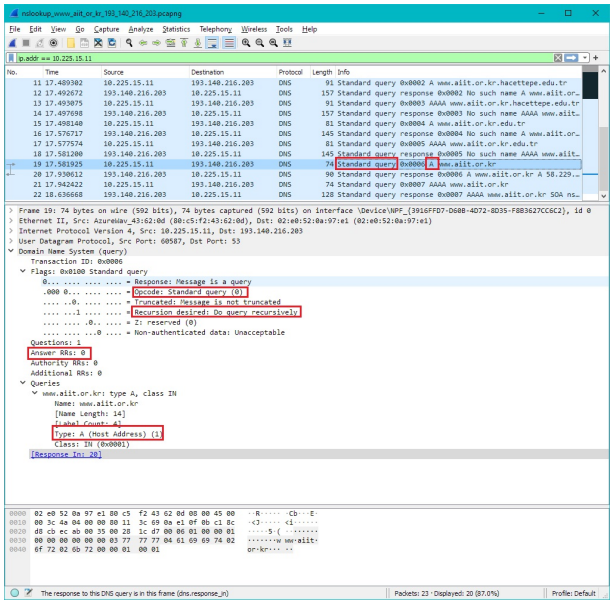
It is sent to 193.140.216.203 which is the parameter we entered but also our default local DNS server. TA gave us Hacettepe DNS for testing and We think aim was to make us realize the difference but we were already doing the test with in Hacettepe University so entering parameter did not change our DNS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





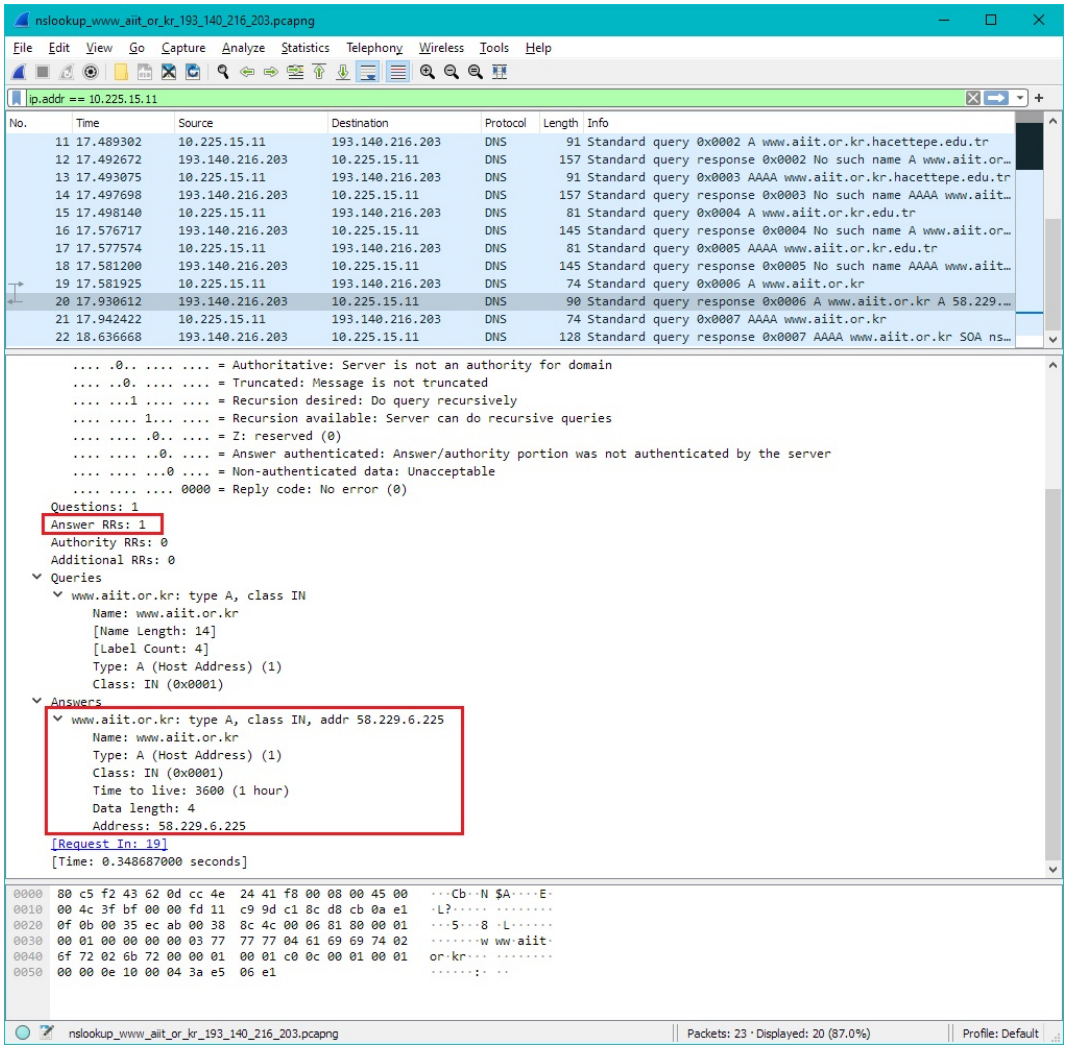
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

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