Lab 2

Student: Ivan Martinovic
WPI username: imartinovic

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

baidu.com -> 220.181.38.148 and 39.156.69.79

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

University of Sarajevo: www.unsa.ba

una.utic.net.ba = 204.61.216.117
bosna.utic.net.ba = 195.130.35.5
sava.utic.net.ba = 195.130.35.3
una.utic.net.ba IPv6 = 2001:500:14:6117:ad::1

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

I've chosen una.utic.net.ba as my DNS server

I've obtained 2 IPv6 and 2 IPv4 addresses:
2a00:1288:80:800::7001
2a00:1288:80:800::7000
87.248.118.23
87.248.118.22

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

Both the DNS query and response message are sent via UDP.

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

The source port of the DNS message is 54066.
The destination port of the DNS message is 53.

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?

The DNS query is sent to 212.39.98.164
My two local dns servers are: 212.39.98.163 and 212.39.98.164

Hence the message was sent to the local DNS server.

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

It is a “Standard query”. The query contains one question but no answers.

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

4 Aswers have been provided:
The first answer says that www.ietf.org is an alias for the canonical hostname www.ietf.org.cdn.cloudflare.net
The subsequent three answers provide type A records for www.ietf.org.cdn.cloudflare.net , or in other words they provide the actual ip address we asked for in the first place: these include 104.20.110.6, 172.67.33.249 and 104.20.111.6

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?

Yes, almost all of the TCP packets seemed to have been sent to 104.20.111.6

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

No, my host just issues new HTTP queries and creates new TCP connections. There is no need to look for the ip address of the server again since we already know it from our previous DNS query.

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

Destination port is 53.
Source port is 57082.

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

The query was sent to 212.39.98.163. This matches one of my default local DNS servers.

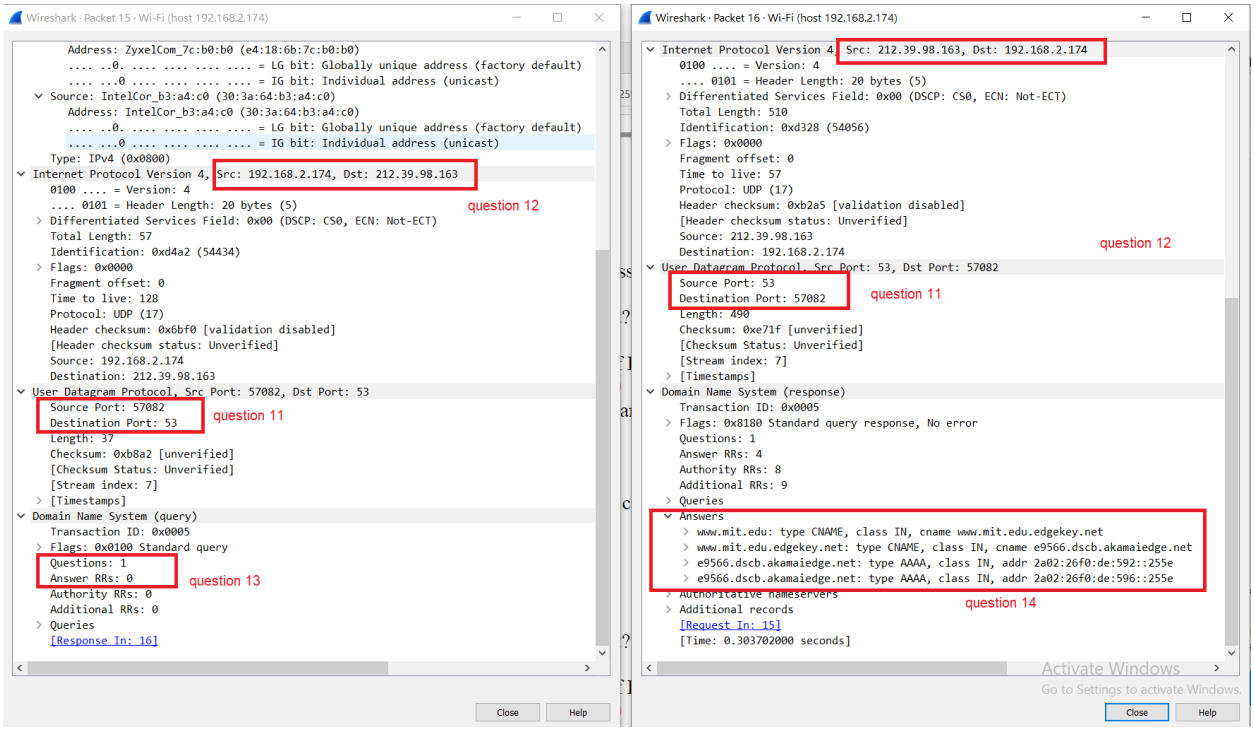
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The query is of type “Standard query”. The query does not contain any answers.

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

The DNS response message contains 4 answers.
The first answer tells us that www.mit.edu is an alias for the canonical hostname www.mit.edu.edgekey.net
The second answer tells us that www.mit.edu.edgekey.net is also an alias for the canonical hostname e9566.dscb.akamaiedge.net.
The last two answers tell us that the server we are looking for may have the following two IPv6 addresses: 2a02:26f0:de:592::255e and 2a02:26f0:de:596::255e

15. Provide a screenshot.



Note: For better visibility please see the screenshot “Questions 11-16” in the Screenshots folder

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

The query is sent to the address 212.39.98.163
This corresponds to one of the my default local DNS servers.

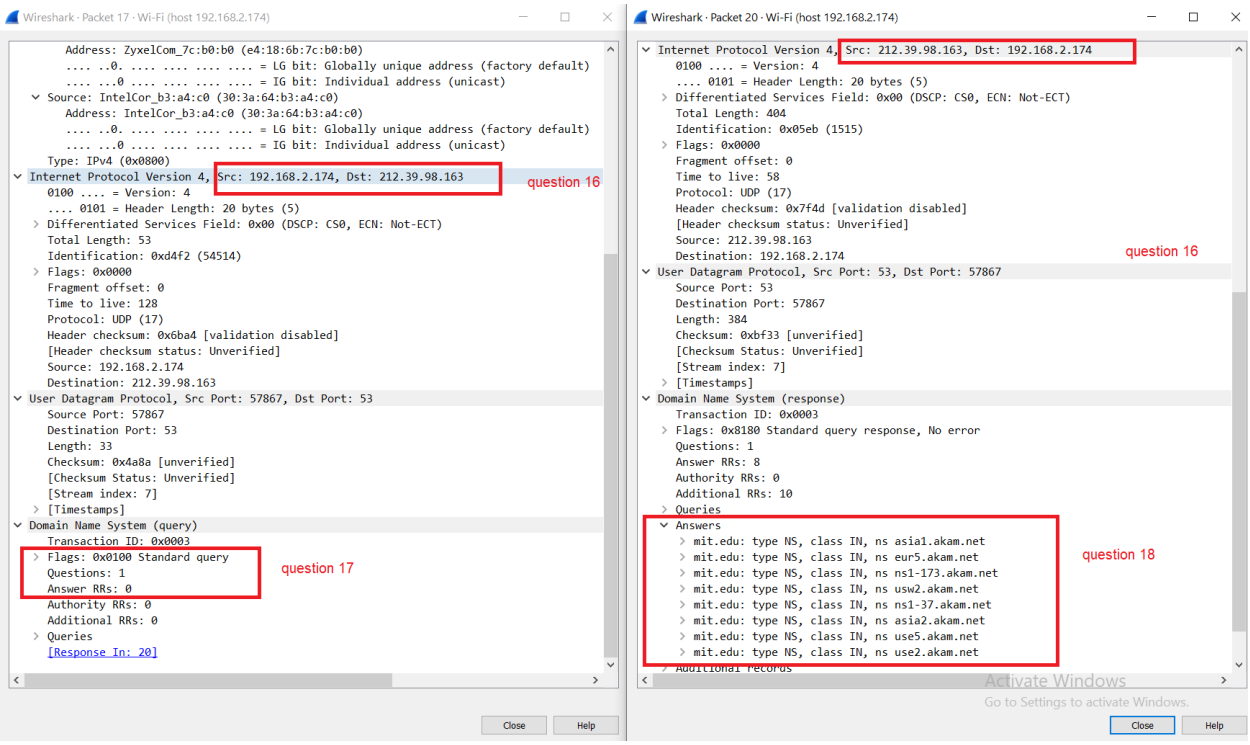
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The query is of type “Standard query”. The query does not contain any answers.

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

The response message provides the following MIT nameservers:
asia1.akam.net
eur5.akam.net
ns1-173.akam.net
usw2.akam.net
ns1-37.akam
asia2.akam.net
use5.akam.net
use2.akam.net

19. Provide a screenshot.



Note: Fore better visibility please see screenshot “Questions 16-19” in the screenshots folder

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?

Note: I’ve used dns.google
The DNS query was sent to 8.8.8.8

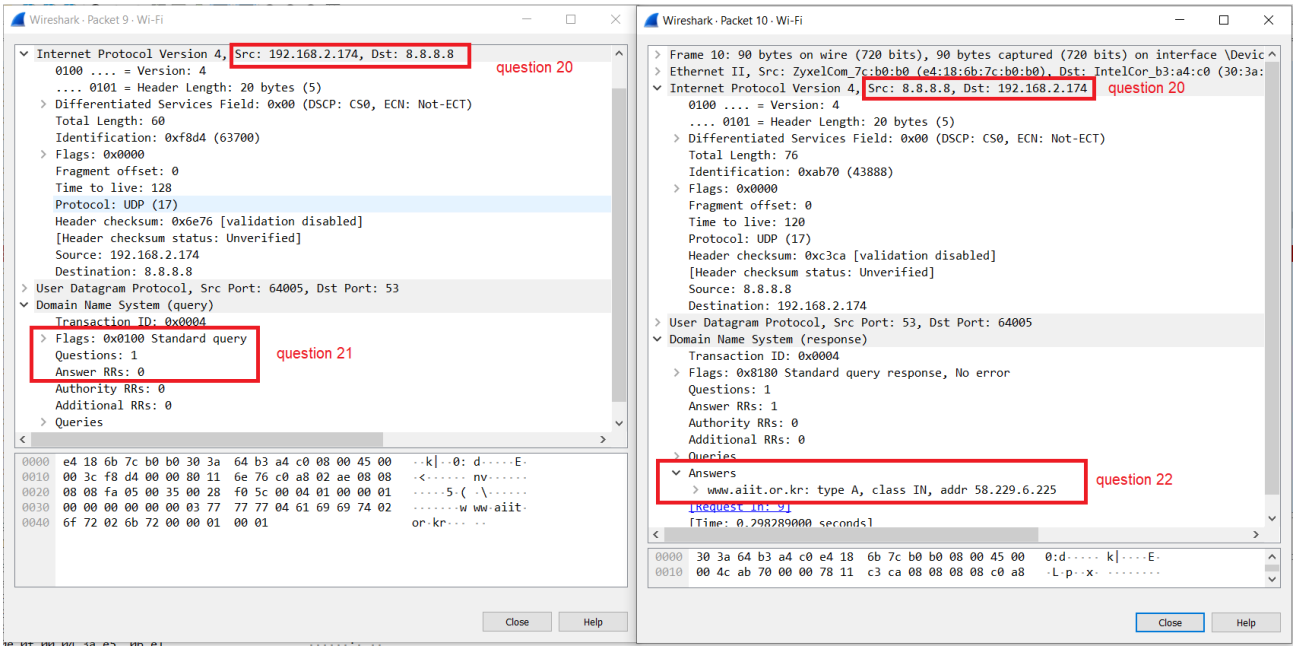
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The DNS query is of type “Standard query”. It contains no answers.

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

The DNS response provides one answer RR. The answer RR says that the IP address of www.aiit.or.kr is 58.229.6.225

23. Provide a screenshot.



Note: Fore better visibility please see screenshot “Questions 20-23” in the screenshots folder