Homework 2 - Arnav Kucheriya - DNS

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

```
C:\Users\Arnav>nslookup www.titech.ac.jp
Server:  CR1000A.mynetworksettings.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    web-a1n.westeurope.cloudapp.azure.com
Address:  20.107.116.39
Aliases:  www.titech.ac.jp
          titech-www-top.trafficmanager.net
```

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

```
C:\Users\Arnav>nslookup -type=NS tum.de
Server:  CR1000A.mynetworksettings.com
Address:  192.168.1.1
```

Authoritative Answer

```
dns2.lrz.bayern internet address = 141.40.9.211
dns3.lrz.eu     internet address = 78.128.211.180
```

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?

```
C:\Users\Arnav>nslookup -type=MX yahoo.com dns2.lrz.eu
*** Can't find server address for 'dns2.lrz.eu':
Server:  CR1000A.mynetworksettings.com
Address:  192.168.1.1

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

mta7.am0.yahoodns.net   internet address = 98.136.96.77
mta7.am0.yahoodns.net   internet address = 67.195.204.74
mta7.am0.yahoodns.net   internet address = 67.195.204.79
mta7.am0.yahoodns.net   internet address = 67.195.204.77
mta7.am0.yahoodns.net   internet address = 98.136.96.75
mta7.am0.yahoodns.net   internet address = 67.195.204.73
mta7.am0.yahoodns.net   internet address = 98.136.96.74
mta7.am0.yahoodns.net   internet address = 67.195.228.94
mta5.am0.yahoodns.net   internet address = 67.195.204.72
mta5.am0.yahoodns.net   internet address = 67.195.228.110
mta5.am0.yahoodns.net   internet address = 98.136.96.74
mta5.am0.yahoodns.net   internet address = 67.195.228.109
mta5.am0.yahoodns.net   internet address = 67.195.228.106
mta5.am0.yahoodns.net   internet address = 67.195.204.77
mta5.am0.yahoodns.net   internet address = 98.136.96.91
mta5.am0.yahoodns.net   internet address = 98.136.96.75
mta6.am0.yahoodns.net   internet address = 98.136.96.74
mta6.am0.yahoodns.net   internet address = 67.195.228.106
mta6.am0.yahoodns.net   internet address = 67.195.204.77
mta6.am0.yahoodns.net   internet address = 67.195.228.110
mta6.am0.yahoodns.net   internet address = 67.195.204.74
mta6.am0.yahoodns.net   internet address = 98.136.96.76
mta6.am0.yahoodns.net   internet address = 98.136.96.91
mta6.am0.yahoodns.net   internet address = 67.195.228.111
```

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

UDP

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

Destination port (query): 53
Source port (response): 53

6. What is the IP address of the DNS server to which the query was sent? Is this your local DNS server?

DNS query destination IP: 128.238.38.102
local DNS servers:
192.168.1.1 (IPv4)
2600:4041:42aa:ac00::1 (IPv6).
Not the same.

7. What is the query type? Does the query message contain any answers?

Query type: A (IPv4 address)

8. In the DNS response, how many answers are provided? What do they contain?

Number of answers: 2
Contain: A records for www.ietf.org = 132.151.6.75 and 65.246.255.51

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, SYN destination IP = 132.151.6.75, which matches the DNS answer.

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

No, the host did not issue additional DNS queries for embedded objects in this capture.

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

Query destination port = 53, Response source port = 53.

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

Destination IP = 128.238.38.102.
Local DNS server = 192.168.1.1 / 2600:4041:42aa:ac00::1.
Not the same.

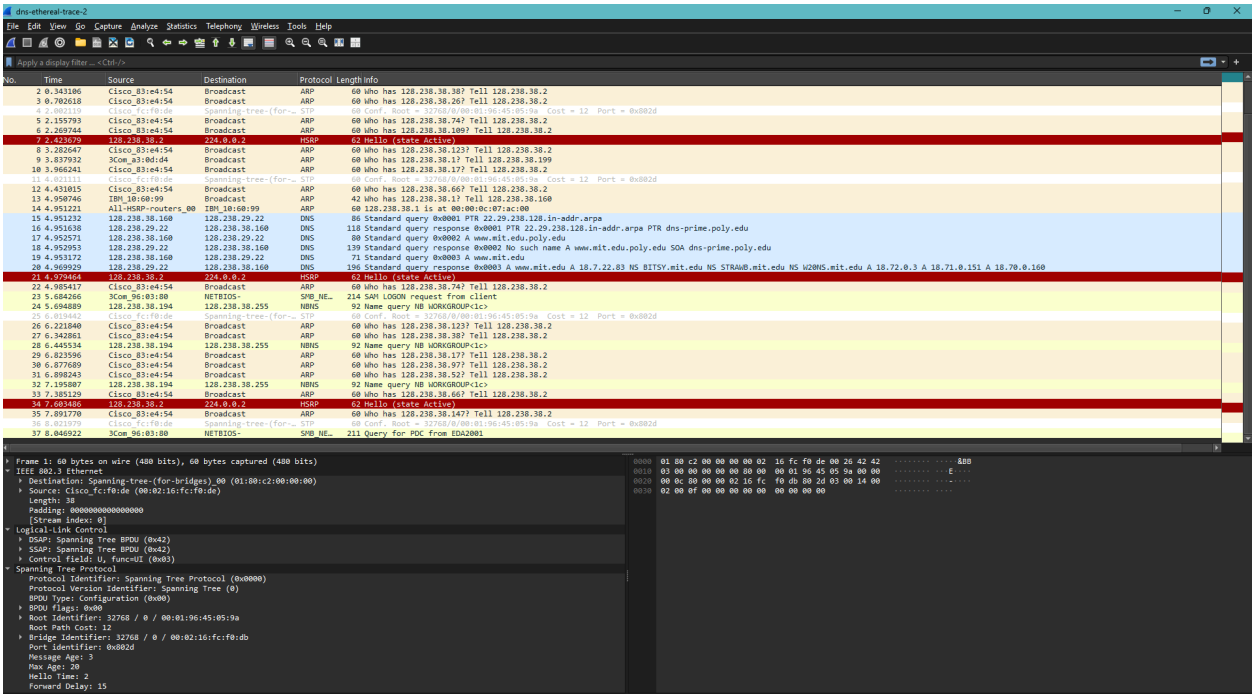
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Query type = A.
No Answers in Query

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

3 answers:
18.72.0.3,
18.71.0.151,
18.70.0.160

15. Provide a screenshot



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

Destination IP = 128.238.38.102.
local DNS = 192.168.1.1 (IPv4) and 2600:4041:42aa:ac00::1 (IPv6).
Not the same.

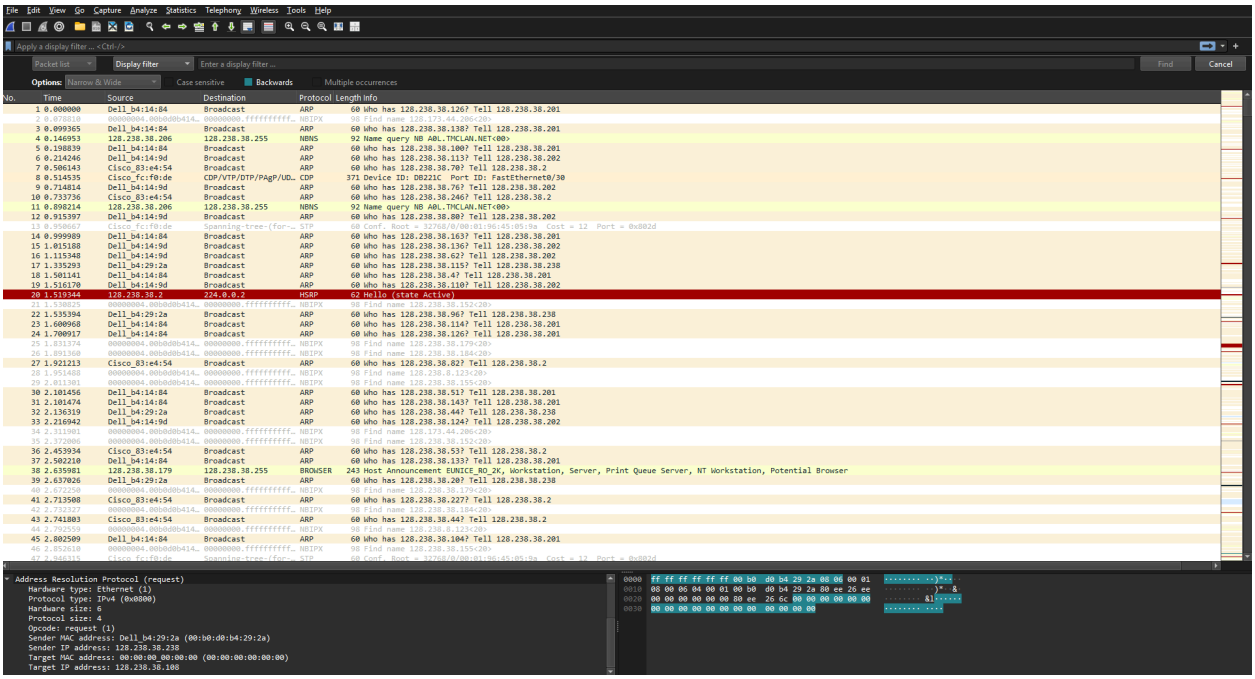
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

> Query type = NS (nameserver)

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?

> Nameservers returned:
> BITSY.mit.edu,
> STRAWB.mit.edu,
> W20NS.mit.edu.

19. Provide a screen shot



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?

> DNS query destination IP = 18.72.0.3.
> This is not my default local DNS server
> (local DNS server: 192.168.1.1 / 2600:4041:42aa:ac00::1).

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

> Query type = A (IPv4)
