LAB 3

Name : Eslam Mostafa Mohamed

ID : 20p4797

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server? For caddy server
   - 165.227.20.207

```
C:\Users\eslam>nslookup caddyserver.com
Server:  familyshield.opendns.com
Address:  208.67.222.123

Non-authoritative answer:
Name:    caddyserver.com
Addresses:  2604:a880:2:d0::21b0:6001
          165.227.20.207


C:\Users\eslam>
```

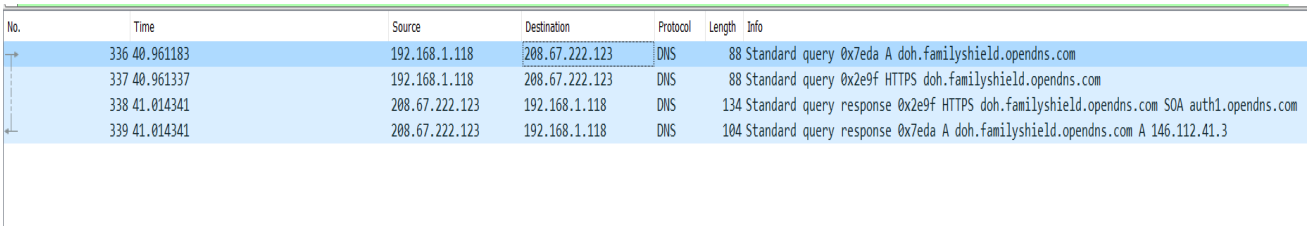
2. Run nslookup to determine the authoritative DNS servers for a university in Europe.
   For new castle university
   -208.67.22.123

```
C:\Users\eslam>nslookup www.ncl.ac.uk
Server:  familyshield.opendns.com
Address:  208.67.222.123

Non-authoritative answer:
Name:    www.ncl.ac.uk
Address:  128.240.216.80
```

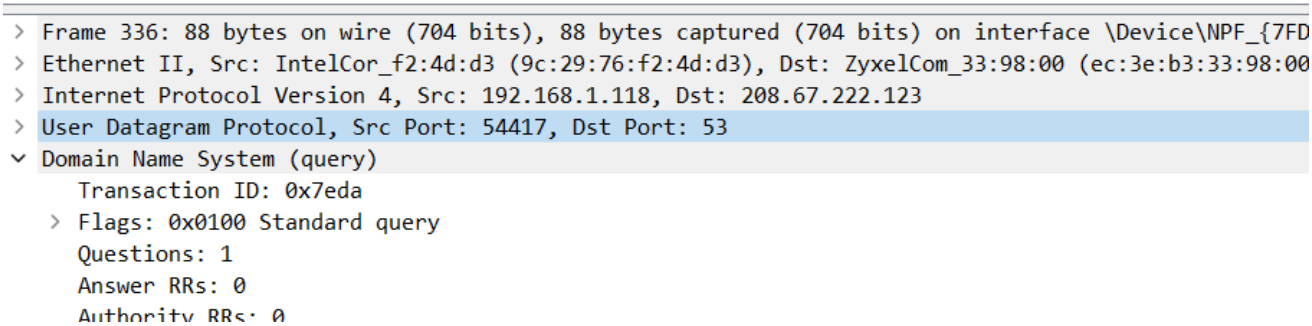
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?
   -128.240.216.80

```
C:\Users\eslam>nslookup www.ncl.ac.uk
Server:  familyshield.opendns.com
Address:  208.67.222.123

Non-authoritative answer:
Name:    www.ncl.ac.uk
Address:  128.240.216.80
```

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

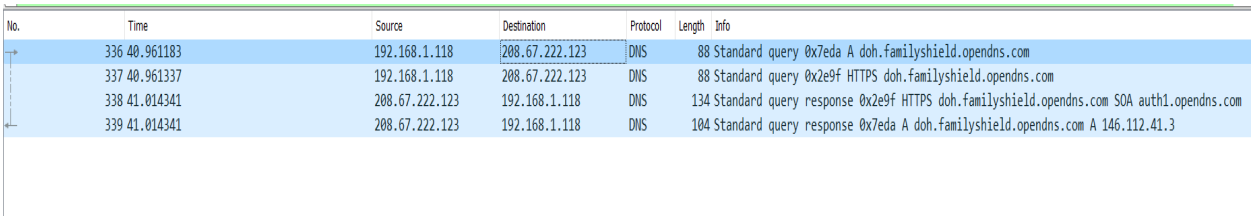


No.	Time	Source	Destination	Protocol	Length	Info
336	40.961183	192.168.1.118	208.67.222.123	DNS	88	Standard query 0x7eda A doh.familyshield.opendns.com
337	40.961337	192.168.1.118	208.67.222.123	DNS	88	Standard query 0x2e9f HTTPS doh.familyshield.opendns.com
338	41.014341	208.67.222.123	192.168.1.118	DNS	134	Standard query response 0x2e9f HTTPS doh.familyshield.opendns.com SOA auth1.opendns.com
339	41.014341	208.67.222.123	192.168.1.118	DNS	104	Standard query response 0x7eda A doh.familyshield.opendns.com A 146.112.41.3



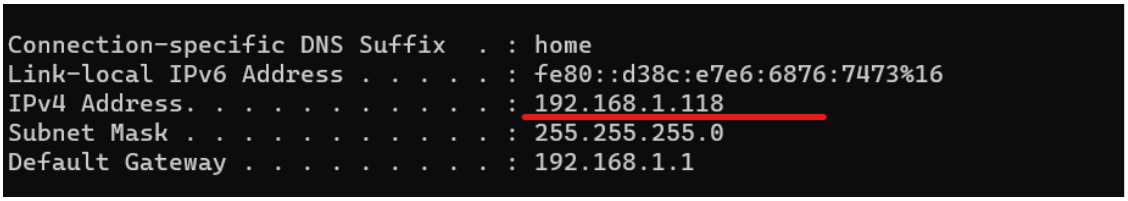
```
> Frame 336: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{7FD
> Ethernet II, Src: IntelCor_f2:4d:d3 (9c:29:76:f2:4d:d3), Dst: ZyxelCom_33:98:00 (ec:3e:b3:33:98:00
> Internet Protocol Version 4, Src: 192.168.1.118, Dst: 208.67.222.123
> User Datagram Protocol, Src Port: 54417, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x7eda
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

5. What is the destination port for the DNS query message? What is the source port of DNS response message?
   -source : 192.168.1.118
   -destination : 208.67.222.123

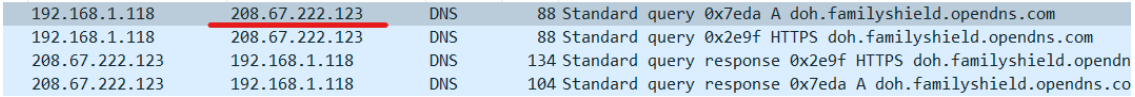


No.	Time	Source	Destination	Protocol	Length	Info
336	40.961183	192.168.1.118	208.67.222.123	DNS	88	Standard query 0x7eda A doh.familyshield.opendns.com
337	40.961337	192.168.1.118	208.67.222.123	DNS	88	Standard query 0x2e9f HTTPS doh.familyshield.opendns.com
338	41.014341	208.67.222.123	192.168.1.118	DNS	134	Standard query response 0x2e9f HTTPS doh.familyshield.opendns.com SOA auth1.opendns.com
339	41.014341	208.67.222.123	192.168.1.118	DNS	104	Standard query response 0x7eda A doh.familyshield.opendns.com A 146.112.41.3

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?
   -yes



```
Connection-specific DNS Suffix  . : home
Link-local IPv6 Address . . . . . : fe80::d38c:e7e6:6876:7473%16
IPv4 Address. . . . . . . . . . . : 192.168.1.118
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```



192.168.1.118	208.67.222.123	DNS	88	Standard query 0x7eda A doh.familyshield.opendns.com
192.168.1.118	208.67.222.123	DNS	88	Standard query 0x2e9f HTTPS doh.familyshield.opendns.com
208.67.222.123	192.168.1.118	DNS	134	Standard query response 0x2e9f HTTPS doh.familyshield.opendn
208.67.222.123	192.168.1.118	DNS	104	Standard query response 0x7eda A doh.familyshield.opendns.co

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

```
 88 Standard query 0x7eda A doh.familyshield.opendns.com
 88 Standard query 0x2e9f HTTPS doh.familyshield.opendns.com
134 Standard query response 0x2e9f HTTPS doh.familyshield.opendns.com SOA auth1.opendns.com
104 Standard query response 0x7eda A doh.familyshield.opendns.com A 146.112.41.3
```

```
Domain Name System (query)
    Transaction ID: 0x7eda
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
   - Not have any answers

```
Domain Name System (response)
    Transaction ID: 0x2e9f
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
```

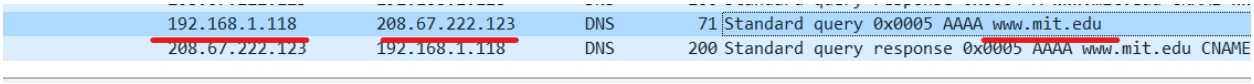
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
   - Same

	Time	Source	Destination	Protocol
2	1.773376	192.168.1.118	20.250.77.142	TCP
3	1.849961	20.250.77.142	192.168.1.118	TCP

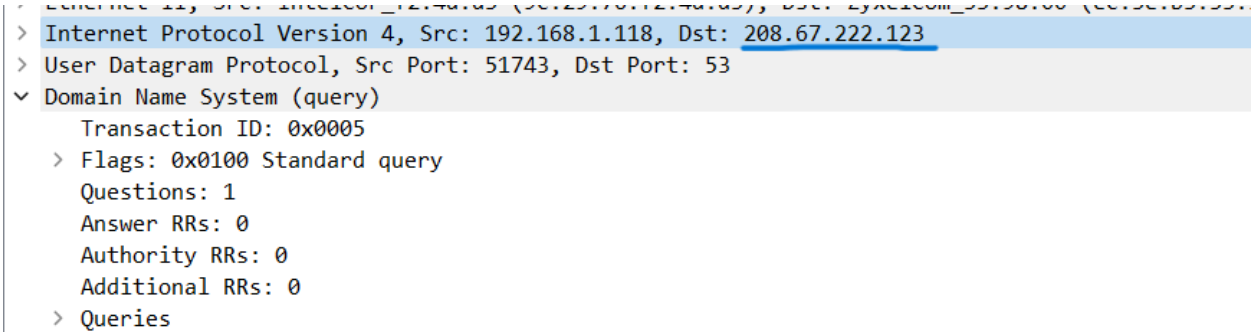
	Time	Source	Destination	Protocol	Length	Info
49	12.704222	192.168.1.118	208.67.222.123	DNS	89	Standard query 0xdbcc A v10.events.data.microsoft.com
51	12.756295	208.67.222.123	192.168.1.118	DNS	226	Standard query response 0xdbcc A v10.events.data.microsoft.com CNAME win-glc

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

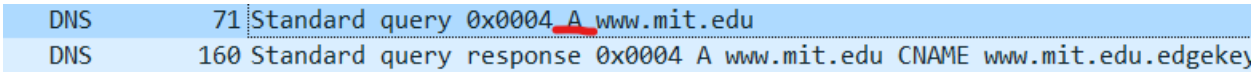
11. What is the destination port for the DNS query message? What is the source port of DNS response message?
    -source : 192.168.1.118
    -destination : 208.67.222.123

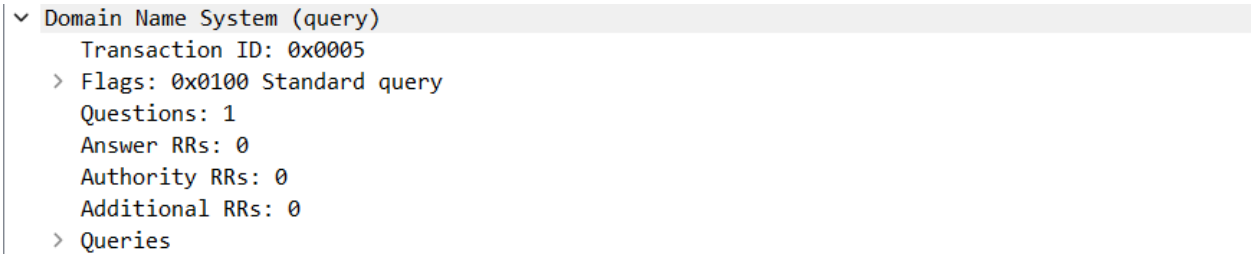


12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    -208.67.222.123

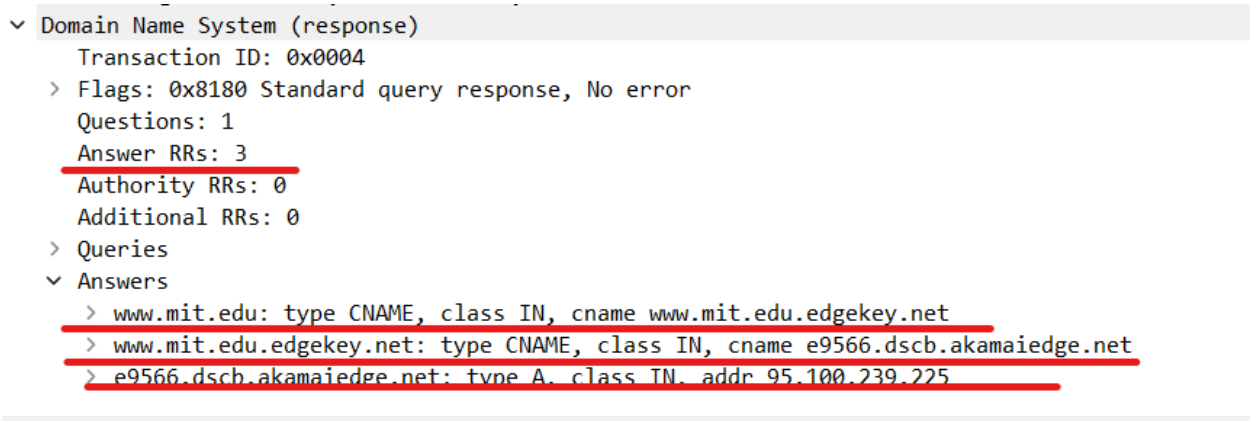


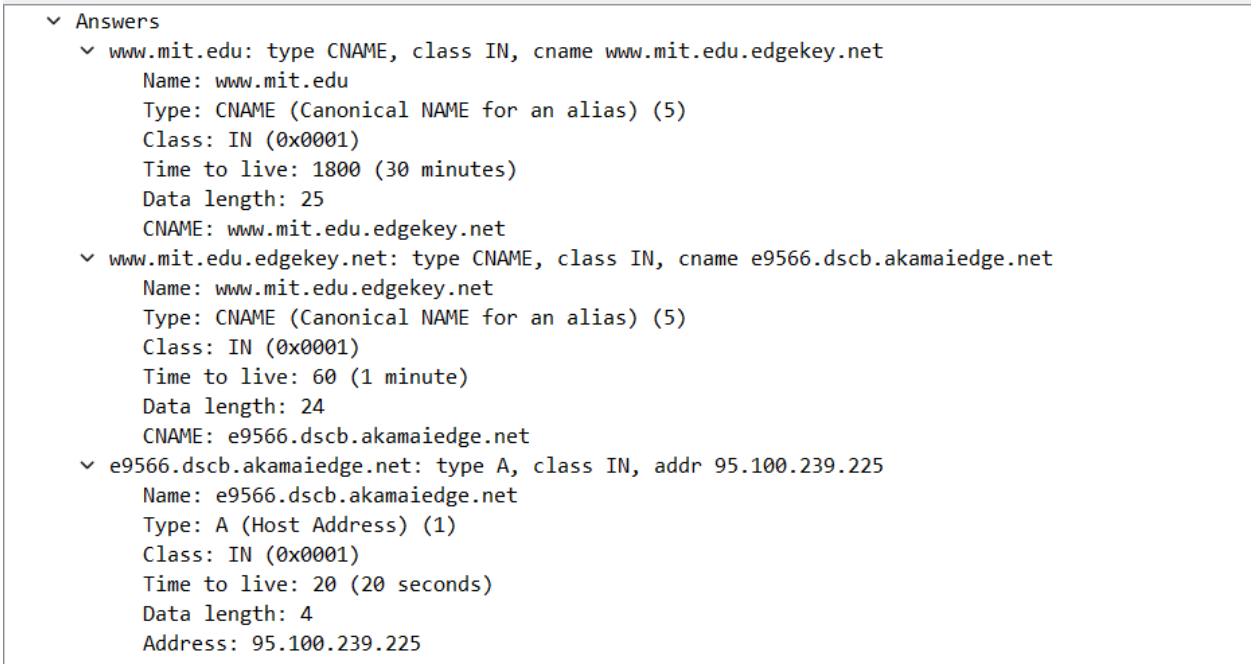
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    - Type "A"
    - Doesn't have any answer





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





Now repeat the previous experiment, but instead issue the command: 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?

```
> Frame 2607: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{7FD207
> Ethernet II, Src: IntelCor_f2:4d:d3 (9c:29:76:f2:4d:d3), Dst: ZyxelCom_33:98:00 (ec:3e:b3:33:98:00)
> Internet Protocol Version 4, Src: 192.168.1.118, Dst: 208.67.222.123
> User Datagram Protocol, Src Port: 49862, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x2933
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

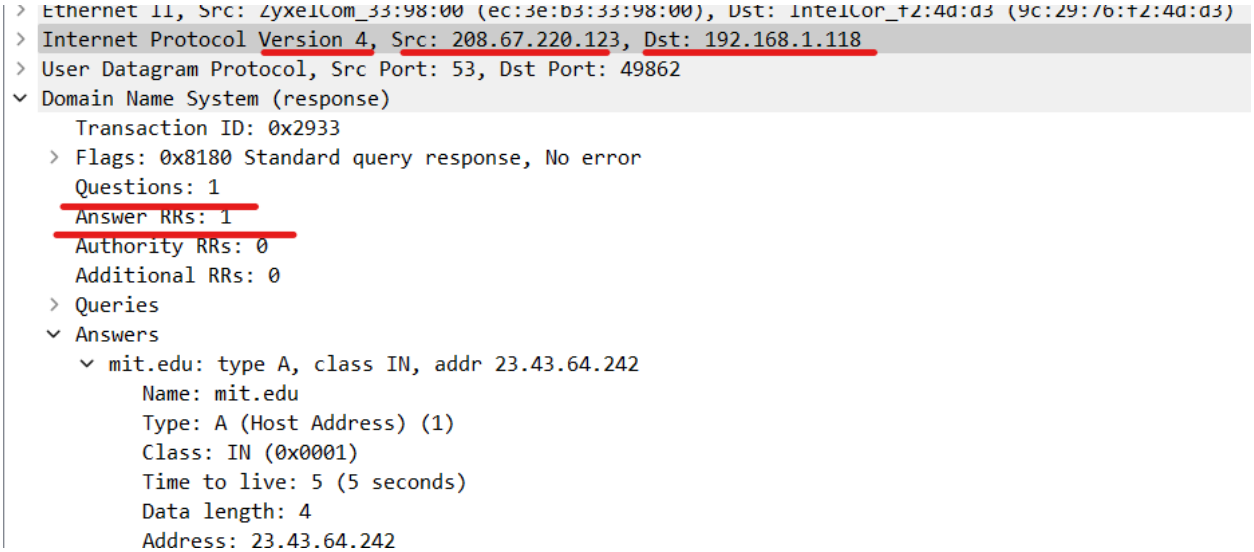
17.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

- Type “A”
- Have no message answer

```
192.168.1.118     208.67.222.123     DNS     67 Standard query 0x2933 A mit.edu
192.168.1.118     208.67.220.123     DNS     67 Standard query 0x2933 A mit.edu
208.67.220.123    192.168.1.118      DNS     83 Standard query response 0x2933 A mit.edu
```

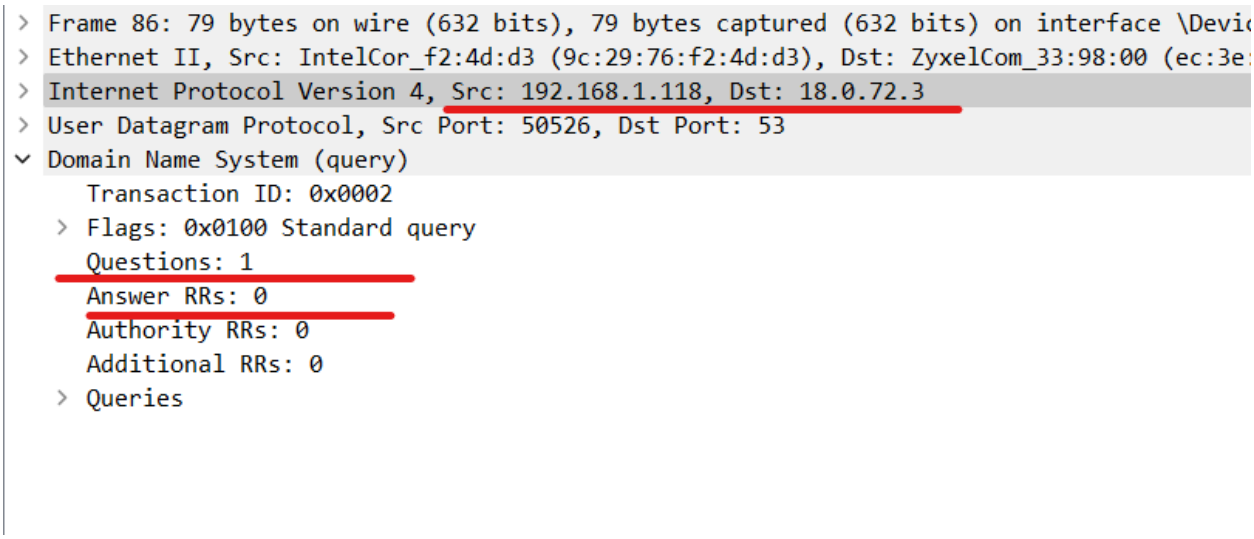
```
> User Datagram Protocol, Src Port: 49862, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x2933
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 2611]
```

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?



Now repeat the previous experiment, but instead issue the command: nslookup www.aiit.or.kr bitsy.mit.edu

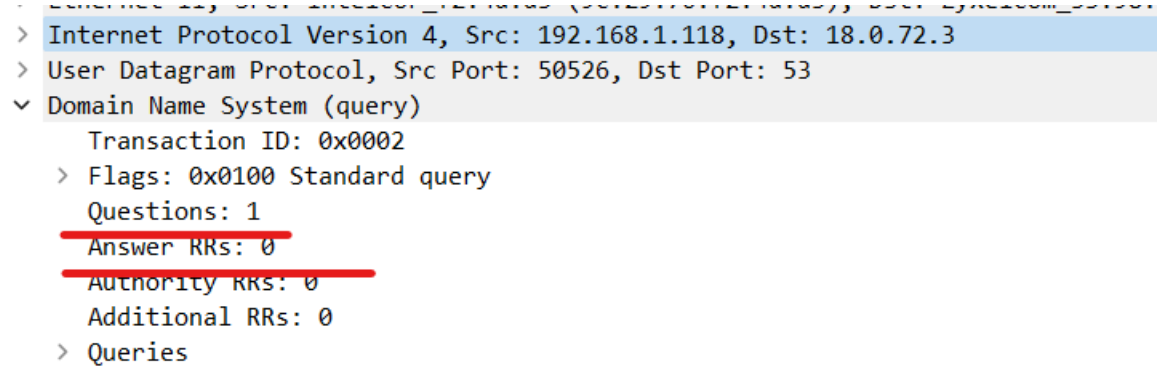
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

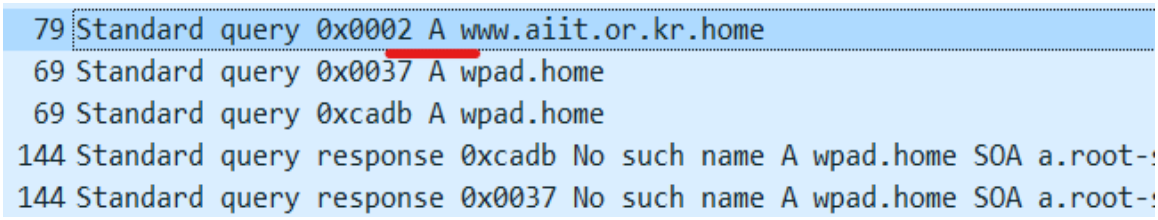


21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

-type A

- no answer





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