Work by - Nattanat Lertariyamaythee

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server? (**www.anet.net.th** → **203.148.250.185)**

```
PS C:\Users\ASUS> nslookup www.anet.net.th
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    anet.wewyn.com
Address:  203.148.250.185
Aliases:  www.anet.net.th
```

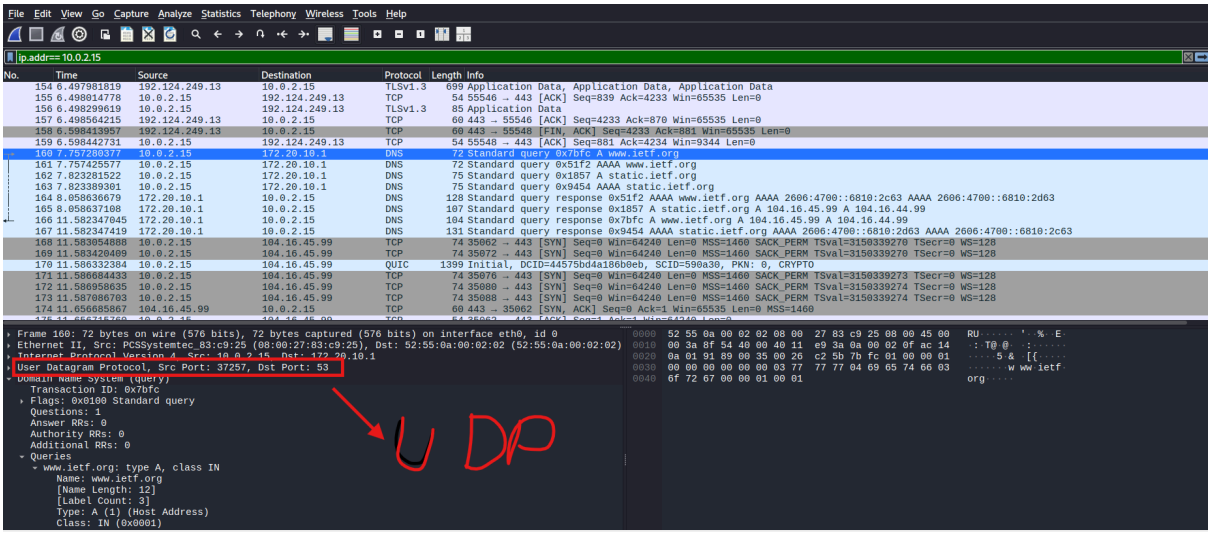
2. Run nslookup to determine the authoritative DNS servers for a university in Europe. **(auth4.dns.ox.ac.uk)**

```
PS C:\Users\ASUS> nslookup www.ox.ac.uk
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    www.ox.ac.uk.cdn.cloudflare.net
Addresses:  172.66.169.161
          104.20.34.13
Aliases:  www.ox.ac.uk

PS C:\Users\ASUS> nslookup -type=NS ox.ac.uk
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk
ox.ac.uk        nameserver = dns1.ox.ac.uk
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk
ox.ac.uk        nameserver = dns0.ox.ac.uk
ox.ac.uk        nameserver = dns2.ox.ac.uk
PS C:\Users\ASUS>
```

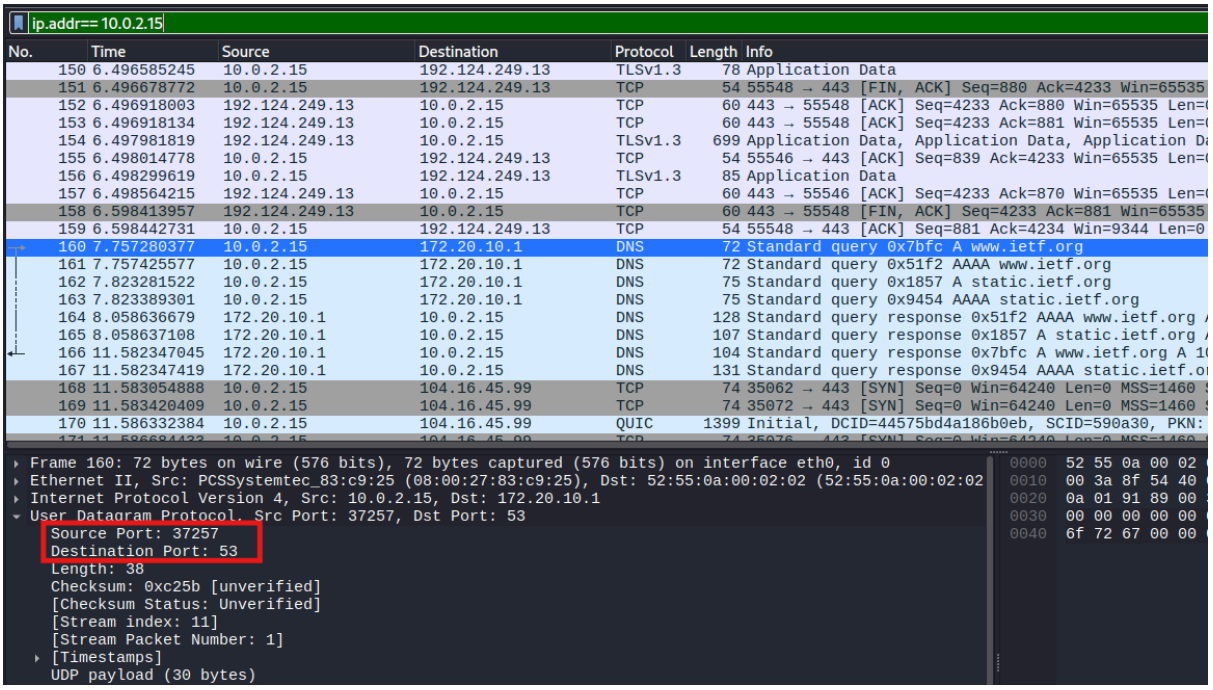
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address? **(Cannot find mail.yahoo.com)**

```
PS C:\Users\ASUS> nslookup www.mail.yahoo.com auth4.dns.ox.ac.uk
Server:  UnKnown
Address:  45.33.127.156

*** UnKnown can't find www.mail.yahoo.com: Query refused
```

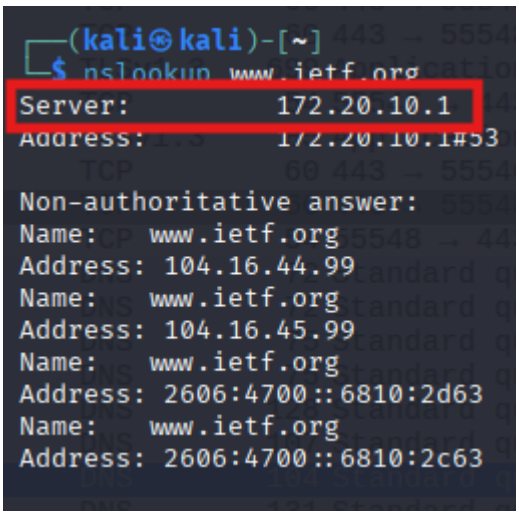
4. Locate the DNS query and response messages. Are then sent over UDP or TCP? **(UDP)**

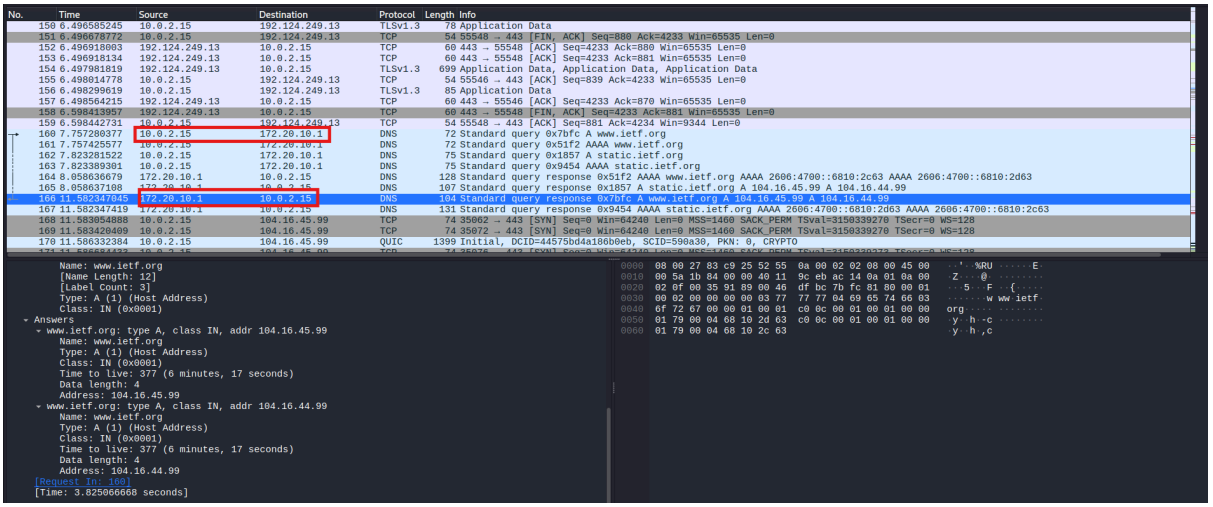


5. What is the destination port for the DNS query message? What is the source port of DNS response message? **(src: 37257, dst.: 53)**

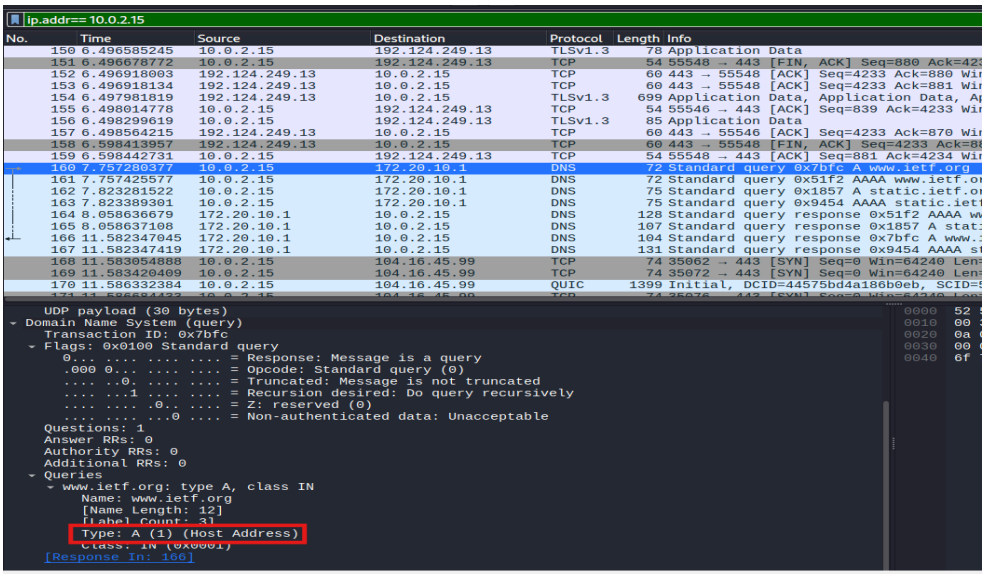


6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same? **(Yes, they are the same)**

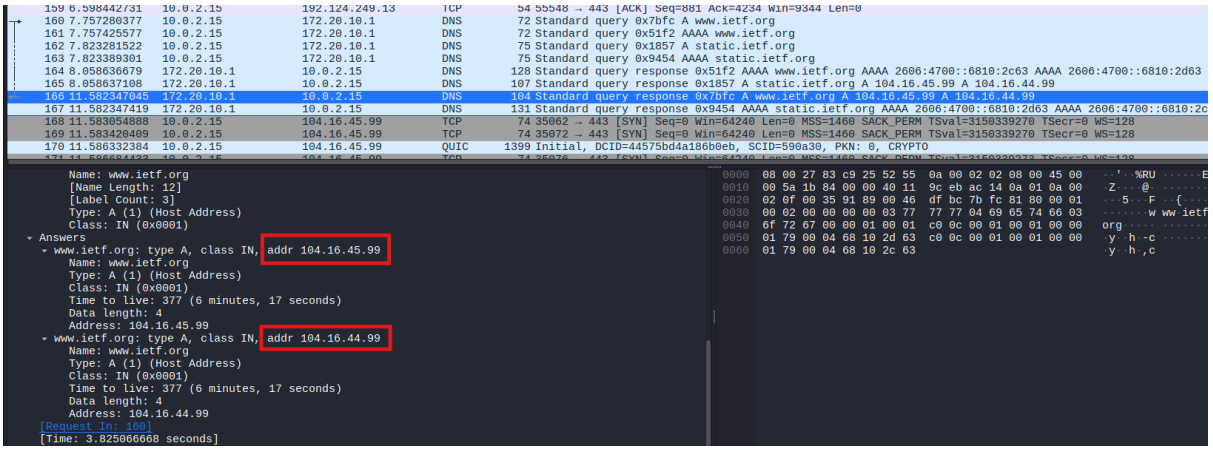




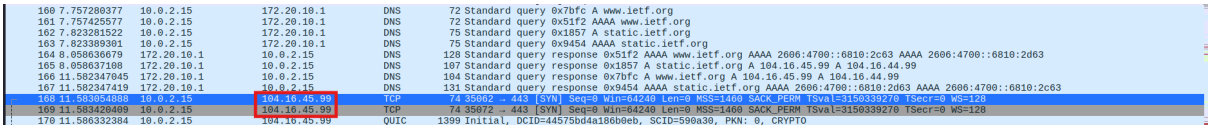
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? **(Type A, no answers)**



8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? **(2 answers, they contain name, class, type, ttl, data, and address)**

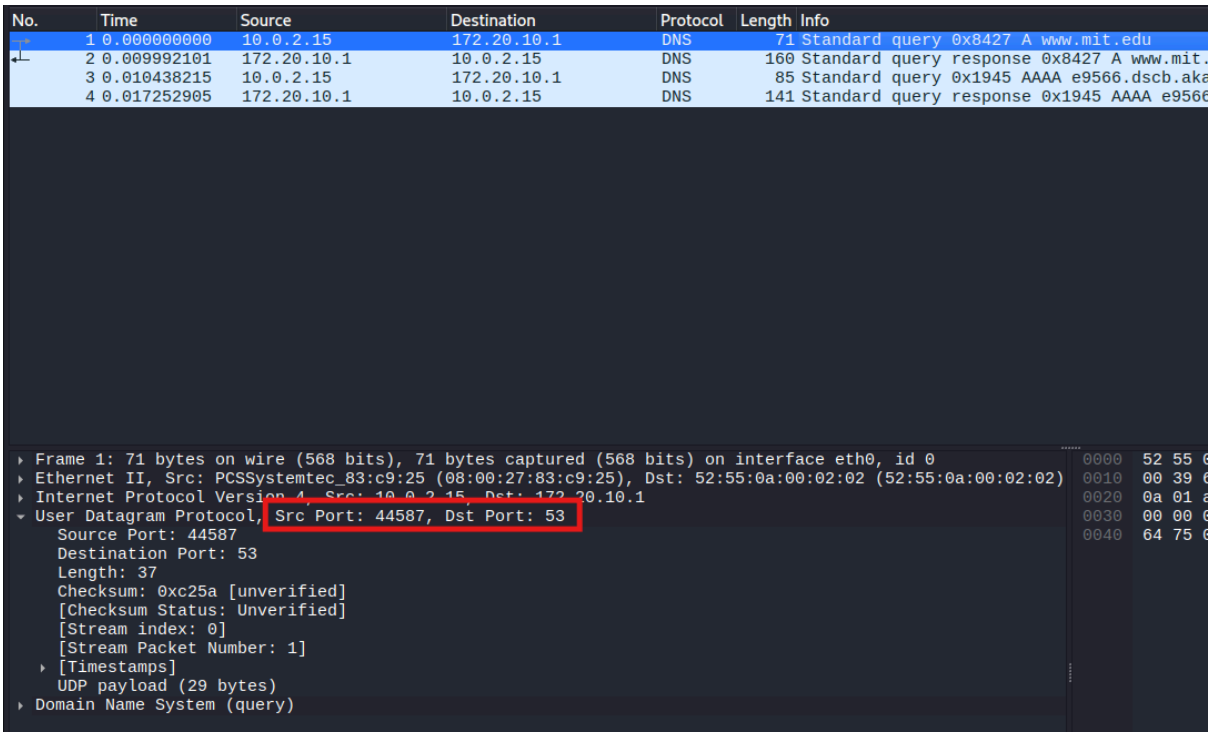


9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message? **(Yes)**

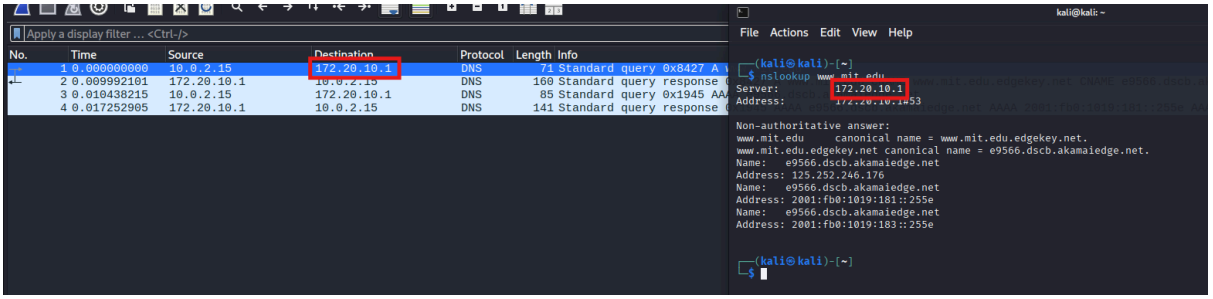


10. This web page contains images. Before retrieving each image, does your host issue new DNS queries? **(No)**

11. What is the destination port for the DNS query message? What is the source port of DNS response message? **(src: 44587, dst: 53)**

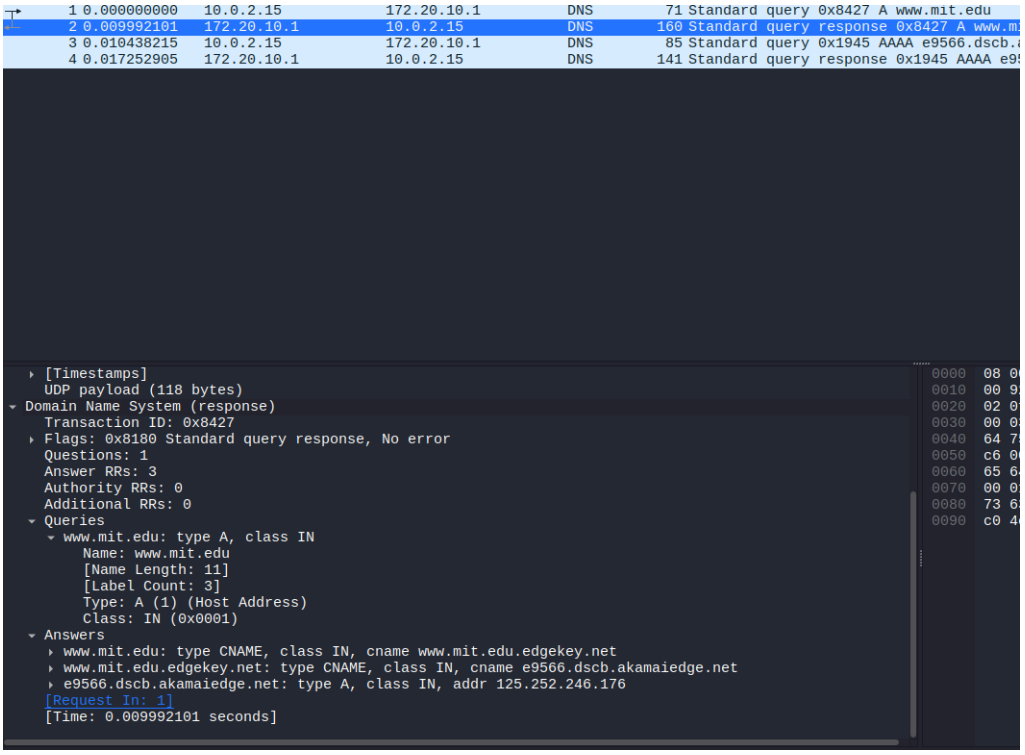


12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**(Yes, they are the same)**

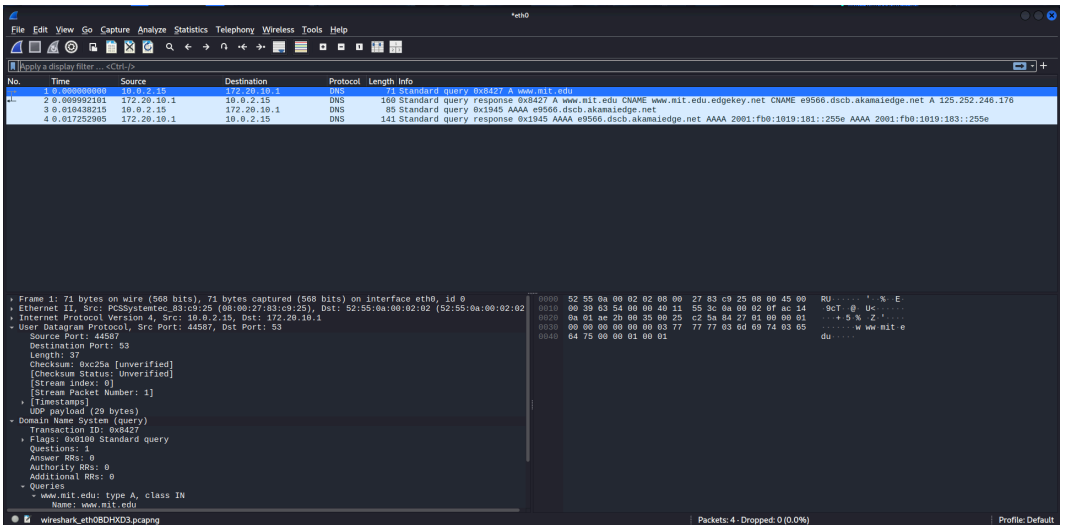


13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? **(Type A, and no answers)**

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? **(3 answers, each contain name, class, type, ttl, data, and address)**



15. Provide a screenshot.



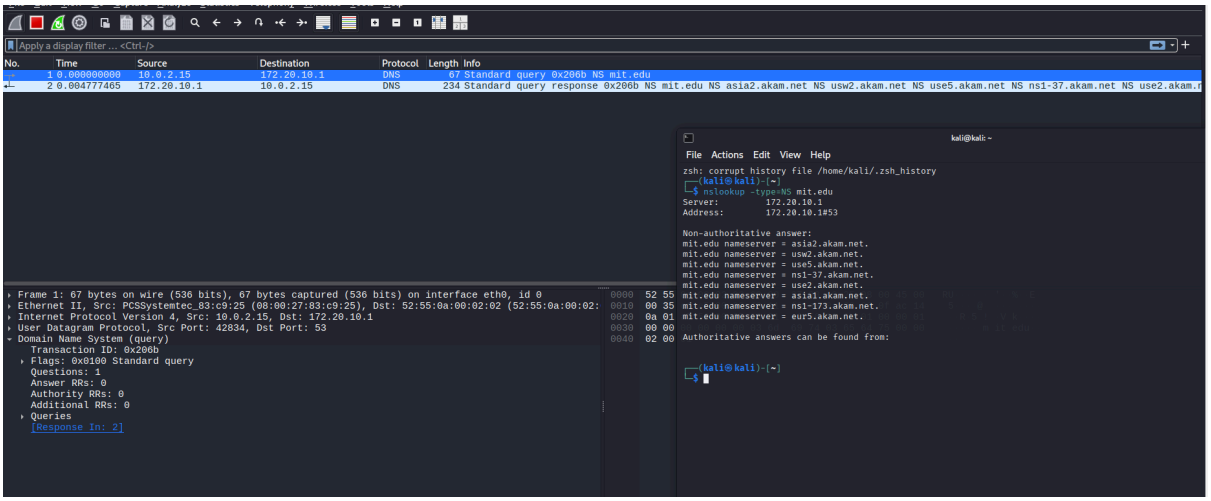
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? **(Yes, they are the same)**

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? **(Type NS, no answers.)**

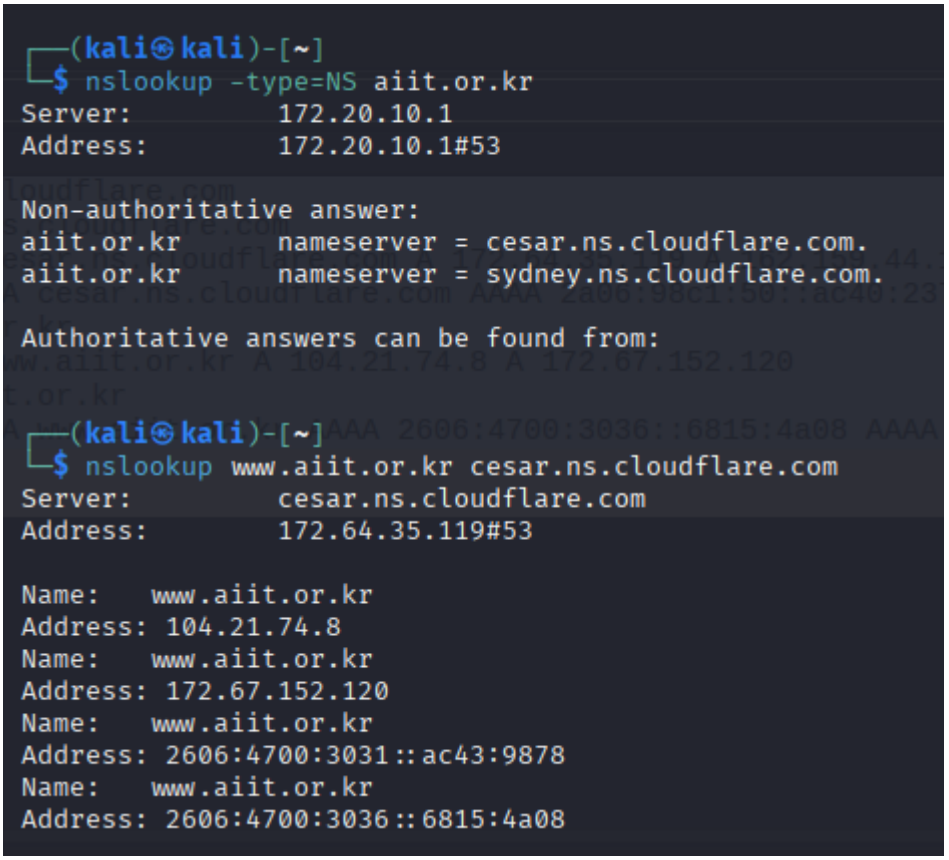
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers? **(No IP address provided.)**

```
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
  ▾ Answers
    ▾ mit.edu: type NS, class IN, ns asia2.akam.net
        Name: mit.edu
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
        Time to live: 2252 (37 minutes, 32 seconds)
        Data length: 16
        Name Server: asia2.akam.net
    ▾ mit.edu: type NS, class IN, ns usw2.akam.net
        Name: mit.edu
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
        Time to live: 2252 (37 minutes, 32 seconds)
        Data length: 7
        Name Server: usw2.akam.net
    ▾ mit.edu: type NS, class IN, ns use5.akam.net
        Name: mit.edu
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
        Time to live: 2252 (37 minutes, 32 seconds)
        Data length: 7
        Name Server: use5.akam.net
    ▾ mit.edu: type NS, class IN, ns ns1-37.akam.net
        Name: mit.edu
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
        Time to live: 2252 (37 minutes, 32 seconds)
        Data length: 9
        Name Server: ns1-37.akam.net
    ▾ mit.edu: type NS, class IN, ns use2.akam.net
```

19. Provide a screenshot



Note: I change bitsy.mit.edu to cesar.ns.cloudflare.com



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?

- At first, it sent the query to default DNS(127.20.10.1) to find "***cesar.ns.cloudflare.com***".
- We get that ***cesar.ns.cloudflare.com*** IP is 172.64.35.119
- Then I sent query to cesar.ns.cloudflare.com (172.64.35.119) to find "www.aiit.or.kr"
- We get that www.aiit.or.kr IP is 104.21.74.8

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

- **One with type A and one with type AAAA**
- **Both have no answers.**

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

- **For cloudfare, both type A and type AAA response have 3 answers, each composes of name, class, type, ttl, data, and address**

```
▸ Internet Protocol Version 4, Src: 172.20.10.1, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 33687
▾ Domain Name System (response)
    Transaction ID: 0x1e27
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ cesar.ns.cloudflare.com: type A, class IN
        Name: cesar.ns.cloudflare.com
        [Name Length: 23]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Answers
    ▸ cesar.ns.cloudflare.com: type A, class IN, addr 172.64.35.119
    ▸ cesar.ns.cloudflare.com: type A, class IN, addr 162.159.44.119
    ▸ cesar.ns.cloudflare.com: type A, class IN, addr 108.162.195.119
    [Request In: 1]
    [Time: 0.006158660 seconds]
```

```
▸ Internet Protocol Version 4, Src: 172.20.10.1, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 33687
▾ Domain Name System (response)
    Transaction ID: 0xb225
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ cesar.ns.cloudflare.com: type AAAA, class IN
        Name: cesar.ns.cloudflare.com
        [Name Length: 23]
        [Label Count: 4]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  ▾ Answers
    ▸ cesar.ns.cloudflare.com: type AAAA, class IN, addr 2a06:98c1:50::ac40:2377
    ▸ cesar.ns.cloudflare.com: type AAAA, class IN, addr 2803:f800:50::6ca2:c377
    ▸ cesar.ns.cloudflare.com: type AAAA, class IN, addr 2606:4700:58::a29f:2c77
    [Request In: 2]
    [Time: 0.005871993 seconds]
```

- **for www.aiit.or.kr both type A and type AAA response have 2 answers, each composes of name, class, type, ttl, data, and address**

```
▸ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_83:c9:25 (08:00:27:83:c9:25
▸ Internet Protocol Version 4, Src: 172.64.35.119, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 57683
▾ Domain Name System (response)
    Transaction ID: 0x4297
  ▸ Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Answers
    ▸ www.aiit.or.kr: type A, class IN, addr 104.21.74.8
    ▸ www.aiit.or.kr: type A, class IN, addr 172.67.152.120
    [Request In: 5]
    [Time: 0.061595654 seconds]
```

```
▸ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_83:c9:25 (08:00:27:83:c9:25
▸ Internet Protocol Version 4, Src: 172.64.35.119, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 50764
▾ Domain Name System (response)
    Transaction ID: 0xda0a
  ▸ Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.aiit.or.kr: type AAAA, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  ▾ Answers
    ▸ www.aiit.or.kr: type AAAA, class IN, addr 2606:4700:3036::6815:4a08
    ▸ www.aiit.or.kr: type AAAA, class IN, addr 2606:4700:3031::ac43:9878
    [Request In: 7]
    [Time: 0.019575259 seconds]
```

23. Provide a screenshot.