Austin Melendez
4/14/2024

CSC 138 Lab 3

Task 1

---

1) The web server for amazon.com has multiple IP addresses. The IPv4 address is 108.138.243.224 and the first of eight IPv6 addresses is 2600:9000:234b:5400:7:49a5:5fd3:b641.

```
C:\Users\austi>nslookup www.amazon.com
Server:  cdns01.comcast.net
Address:  75.75.75.75

Non-authoritative answer:
Name:    d3ag4hukkh62yn.cloudfront.net
Addresses:  2600:9000:234b:5400:7:49a5:5fd3:b641
          2600:9000:234b:b600:7:49a5:5fd3:b641
          2600:9000:234b:2c00:7:49a5:5fd3:b641
          2600:9000:234b:b800:7:49a5:5fd3:b641
          2600:9000:234b:ba00:7:49a5:5fd3:b641
          2600:9000:234b:2800:7:49a5:5fd3:b641
          2600:9000:234b:2000:7:49a5:5fd3:b641
          2600:9000:234b:c000:7:49a5:5fd3:b641
          108.138.243.224
Aliases:  www.amazon.com
          tp.47cf2c8c9-frontier.amazon.com
```

2) There are eight authoritative DNS servers for amazon.com.

```
amazon.com      nameserver = ns2.amzndns.co.uk
amazon.com      nameserver = ns2.amzndns.com
amazon.com      nameserver = ns2.amzndns.net
amazon.com      nameserver = ns2.amzndns.org
amazon.com      nameserver = ns1.amzndns.co.uk
amazon.com      nameserver = ns1.amzndns.com
amazon.com      nameserver = ns1.amzndns.net
amazon.com      nameserver = ns1.amzndns.org

ns1.amzndns.co.uk       internet address = 156.154.67.10
ns1.amzndns.co.uk       AAAA IPv6 address = 2001:502:4612::10
ns1.amzndns.com internet address = 156.154.64.10
ns1.amzndns.com AAAA IPv6 address = 2001:502:f3ff::10
ns1.amzndns.net internet address = 156.154.65.10
ns1.amzndns.net AAAA IPv6 address = 2610:a1:1014::10
ns1.amzndns.org internet address = 156.154.66.10
ns1.amzndns.org AAAA IPv6 address = 2610:a1:1015::10
ns2.amzndns.co.uk       internet address = 204.74.120.1
ns2.amzndns.co.uk       AAAA IPv6 address = 2610:a1:32d1::53
ns2.amzndns.com internet address = 156.154.68.10
ns2.amzndns.com AAAA IPv6 address = 2610:a1:1016::10
ns2.amzndns.net internet address = 156.154.69.10
```

Task 3

---

3) The DNS query and response messages are sent over UDP.

```
User Datagram Protocol, Src Port: 58465, Dst Port: 53
   Source Port: 58465
   Destination Port: 53
   Length: 41
```

4) The destination port for the DNS query message is 53, while the source port of the DNS response message is also 53.

```
Destination Port: 53
```

```
Source Port: 53
```

5) The DNS query message is being sent to the IP address 75.75.75.75. According to ipconfig /all the IP address of my local DNS server is 75.75.75.75. Yes, both IP addresses are the same!

No.	Time	Source	Destination	Protocol	Length	Info
2220	6.291504	10.0.0.101	75.75.75.75	DNS	75	Standard query 0x0358 A doh.xfinity.com

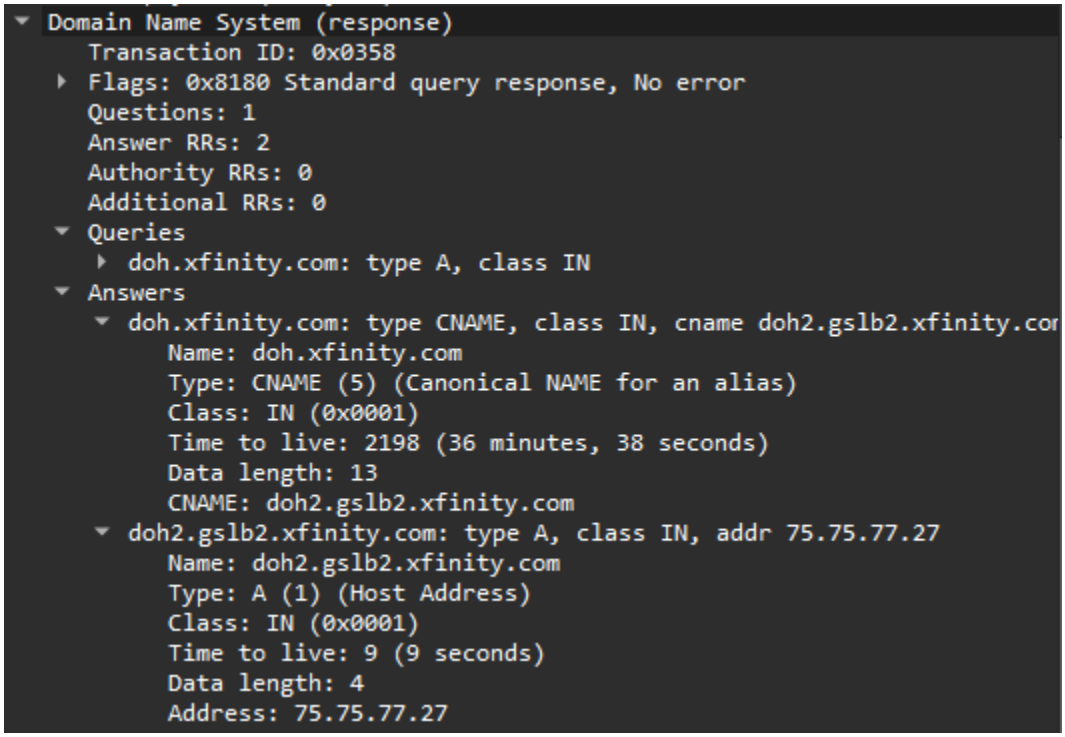
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : hsd1.ca.comcast.net
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 90-CC-DF-BE-EF-E7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.0.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, April 14, 2024 12:58:15 PM
   Lease Expires . . . . . . . . . . : Tuesday, April 16, 2024 12:58:18 PM
   Default Gateway . . . . . . . . . : 10.0.0.1
   DHCP Server . . . . . . . . . . . : 10.0.0.1
   DNS Servers . . . . . . . . . . . : 75.75.75.75
                                       75.75.76.76
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

6) It appears to be a type A DNS query, the query message does not contain an answer field.

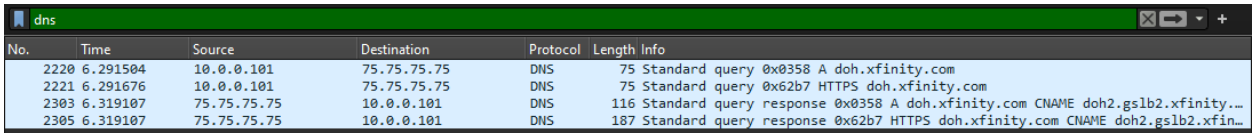
```
▼ Domain Name System (query)
    Transaction ID: 0x0358
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ doh.xfinity.com: type A, class IN
        Name: doh.xfinity.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 2303]
```

7) There are two answers provided in the response message to the one query message. The first answer contains the CNAME record of the queried DNS address. The second answer contains the A record or IP address of the canonical name given in the first answer.

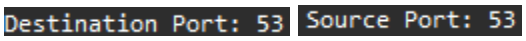


8) Yes, the destination IP address of the subsequent TCP message is the IP address in our second answer in the response query. (75.75.77.27)

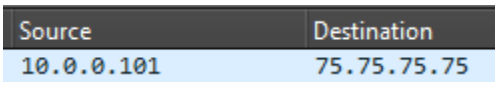
9) No, the only DNS queries that my host issued were the DNS query we looked at and another DNS query for HTTPS.



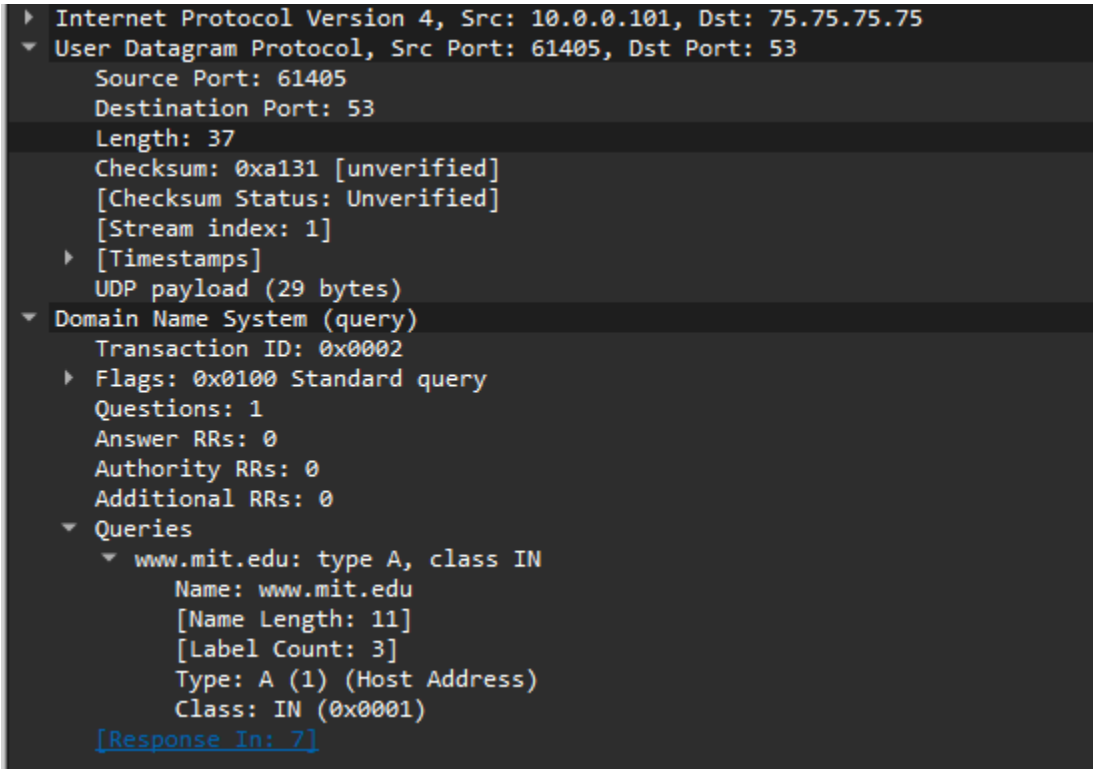
10) The destination port for the DNS query message is 53, and the source port of the response message is also 53.



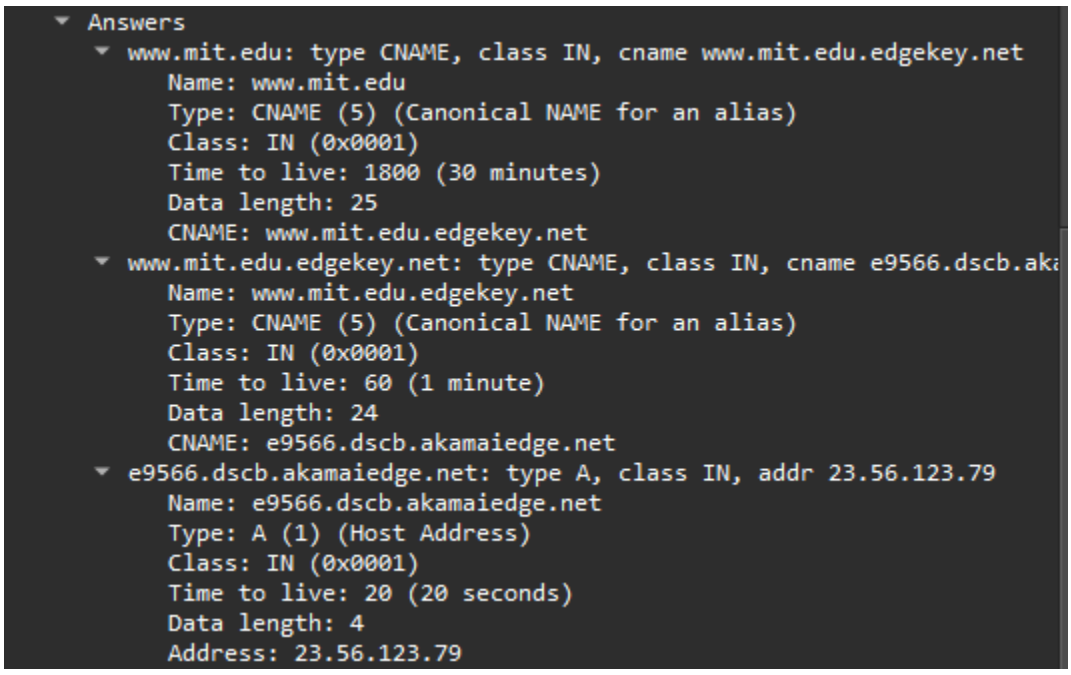
11) The DNS query message is sent to the IP address 75.75.75.75, which is the IP address of my local DNS server.



12) It appears to be a type A DNS query, the query message does not contain an answer field.



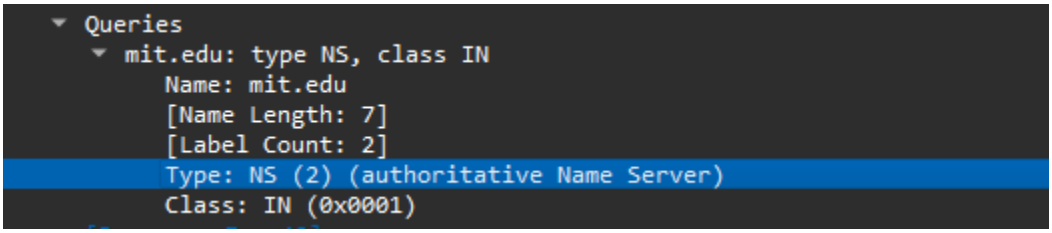
13) There are three answers provided in my DNS response message. The first answer is a CNAME lookup of the address. The second answer is another CNAME lookup of the alias to find the root canonical name. The third answer is a type A lookup to find the IP address of the server.



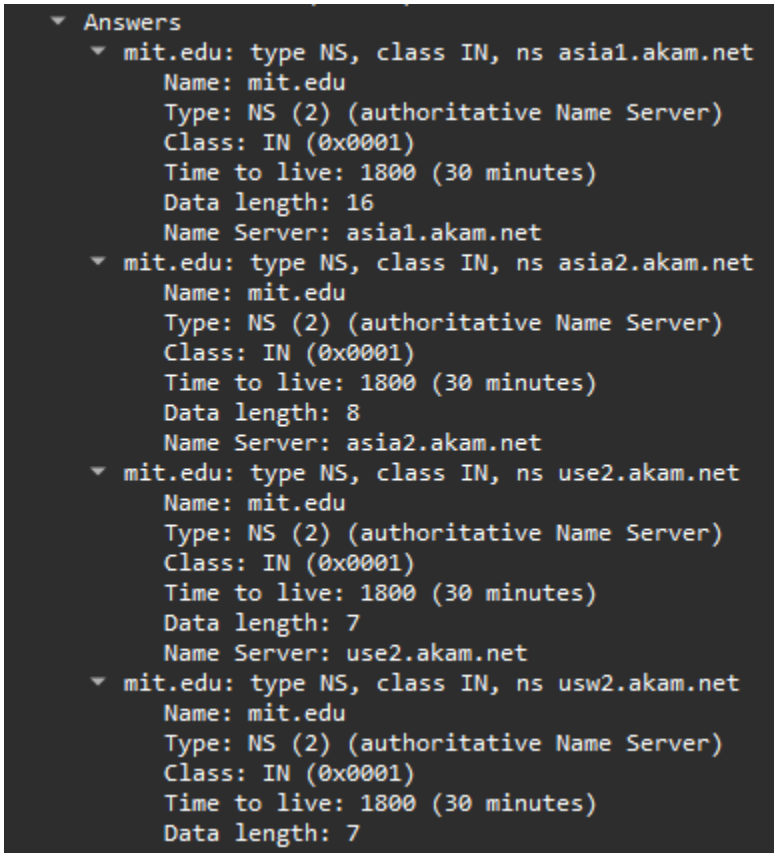
15) The DNS query message is sent to the IP address 75.75.75.75, which is the IP address of my local DNS server.

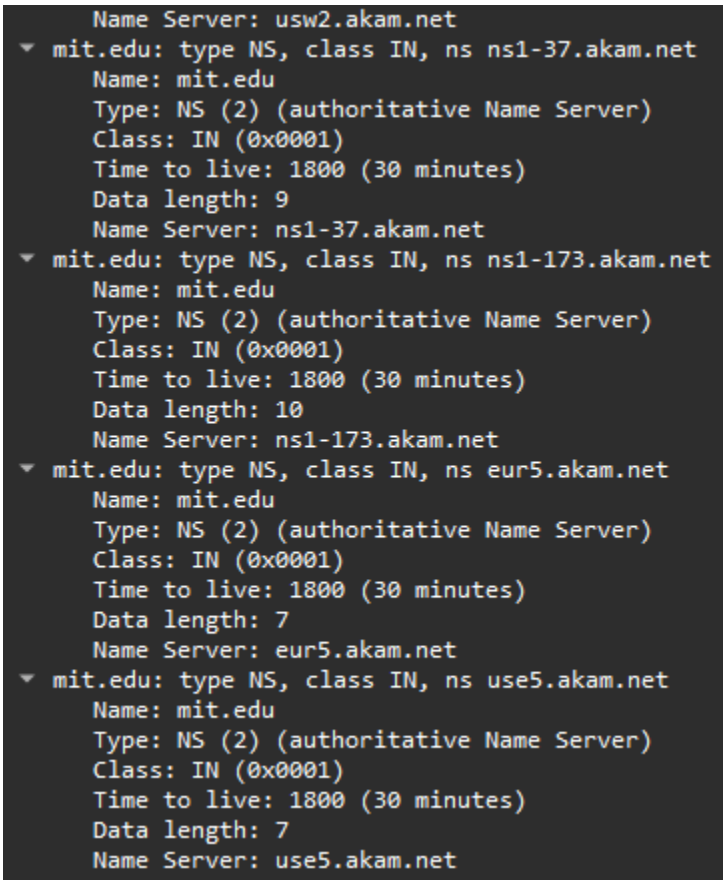
Destination	Protocol	Length	Info
75.75.75.75	DNS	84	Standard query 0x0001 PTR 75.75.
10.0.0.101	DNS	116	Standard query response 0x0001 P
75.75.75.75	DNS	67	Standard query 0x0002 NS mit.edu

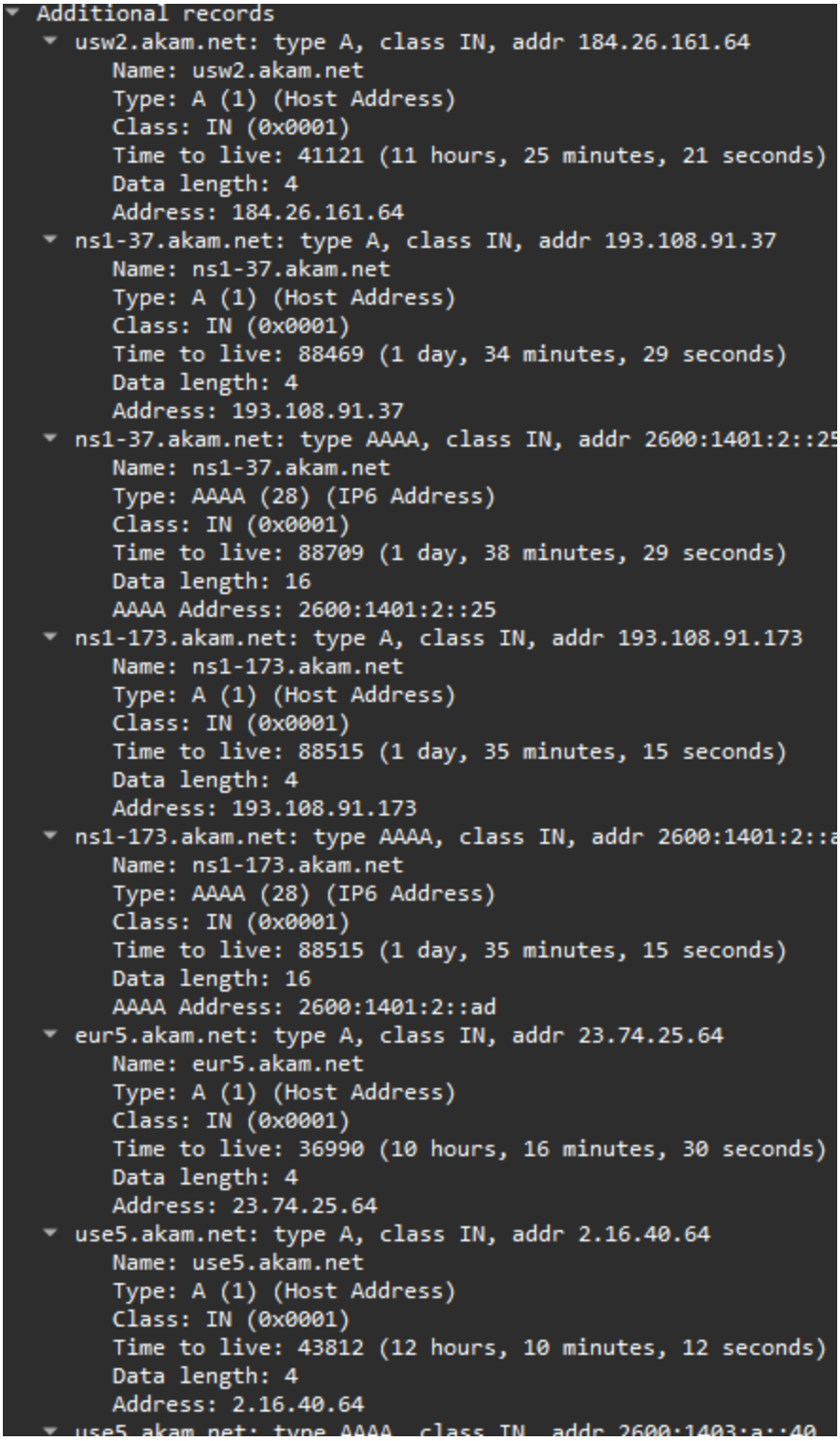
16) It appears to be a type NS DNS query, the query message does not contain an answer field.



17) The response message contains 8 nameservers. asia1.akam.net , asia2.akam.net , use2.akam.net , usw2.akam.net , ns1-37.akam.net , ns1-173.akam.net , eur5.akam.net , use5.akam.net . The response message also contains 11 A type records or the IP addresses to MIT nameservers.






Additional records
usw2.akam.net: type A, class IN, addr 184.26.161.64
Name: usw2.akam.net
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 41121 (11 hours, 25 minutes, 21 seconds)
Data length: 4
Address: 184.26.161.64
ns1-37.akam.net: type A, class IN, addr 193.108.91.37
Name: ns1-37.akam.net
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 88469 (1 day, 34 minutes, 29 seconds)
Data length: 4
Address: 193.108.91.37
ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
Name: ns1-37.akam.net
Type: AAAA (28) (IP6 Address)
Class: IN (0x0001)
Time to live: 88709 (1 day, 38 minutes, 29 seconds)
Data length: 16
AAAA Address: 2600:1401:2::25
ns1-173.akam.net: type A, class IN, addr 193.108.91.173
Name: ns1-173.akam.net
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 88515 (1 day, 35 minutes, 15 seconds)
Data length: 4
Address: 193.108.91.173
ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::a
Name: ns1-173.akam.net
Type: AAAA (28) (IP6 Address)
Class: IN (0x0001)
Time to live: 88515 (1 day, 35 minutes, 15 seconds)
Data length: 16
AAAA Address: 2600:1401:2::ad
eur5.akam.net: type A, class IN, addr 23.74.25.64
Name: eur5.akam.net
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 36990 (10 hours, 16 minutes, 30 seconds)
Data length: 4
Address: 23.74.25.64
use5.akam.net: type A, class IN, addr 2.16.40.64
Name: use5.akam.net
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 43812 (12 hours, 10 minutes, 12 seconds)
Data length: 4
Address: 2.16.40.64
use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40