

CSP334 : Computer Networks
Lab Assignment No 6
Assignment on DNS

Sahil
2016UCS0008

October 26, 2018

1 SET 1: The Basic DNS:

1.1 :

The transport layer protocol used for sending the DNS queries is UDP.

Benefits of UDP: There is no connection establishment in UDP, so there is no need to maintain connection state. Hence, it is a simple protocol.

Also, data is not retransmitted if there is any loss of data, which can be used in time sensitive applications like real-time audio or video.

Drawbacks of UDP: Data loss can occur as it does not provide reliability. Also, no timing and minimum throughput guarantees are provided.

1.2 :

dns						
No.	Time	Source	Destination	Protocol	Length	Info
2	03...	10.0.0.129	75.75.75.75	DNS	66	Standard query 0x4264 A du.edu
3	03...	10.0.0.129	75.75.76.76	DNS	66	Standard query 0x4264 A du.edu
4	03...	2601:86:102:c...	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu
5	03...	2601:86:102:c...	2001:558:feed::2	DNS	86	Standard query 0x4264 A du.edu
6	03...	2001:558:feed...	2601:86:102:cbe4:...	DNS	102	Standard query response 0x4264 A du.edu A 130.253.2.7
7	03...	2001:558:feed...	2601:86:102:cbe4:...	DNS	102	Standard query response 0x4264 A du.edu A 130.253.2.7
9	03...	75.75.75.75	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
10	03...	75.75.76.76	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
20	03...	2601:86:102:c...	2001:558:feed::1	DNS	104	Standard query 0x2016 PTR 7.2.253.130.in-addr.arpa
21	03...	2001:558:feed...	2601:86:102:cbe4:...	DNS	570	Standard query response 0x2016 PTR 7.2.253.130.in-addr.
25	03...	2601:86:102:c...	2001:558:feed::1	DNS	130	Standard query 0x9908 PTR 7.2.253.130.in-addr.arpa
27	03...	2001:558:feed...	2601:86:102:cbe4:...	DNS	1077	Standard query response 0x9908 PTR 7.2.253.130.in-addr.
▶ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0						
▶ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: f6:4b:2a:9f:9f:28 (f6:4b:2a:9f:9f:28)						
▶ Internet Protocol Version 4, Src: 10.0.0.129, Dst: 75.75.75.75						
▼ User Datagram Protocol, Src Port: 36977, Dst Port: 53						
Source Port: 36977						
Destination Port: 53						
Length: 32						
Checksum: 0x38bd [unverified]						
[Checksum Status: Unverified]						
[Stream index: 0]						
▶ Domain Name System (query)						

The port numbers used for sending the packet is 36977 and receiving the packet is 53.

1.3 :

- The destination of packet 2 is 75.75.75.75.
- It is a DNS query of type **A** as shown. In this, we give the host-name in the query and receive the IPA in the response.

```

▶ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: f6:4b:2a:9f:9f:28 (f
▶ Internet Protocol Version 4, Src: 10.0.0.129, Dst: 75.75.75.75
▶ User Datagram Protocol, Src Port: 36977, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x4264
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Truncated: Message is not truncated
    .... 1... .. = Recursion desired: Do query recursively
    .... 0... .. = Z: reserved (0)
    .... 0... .. = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ du.edu: type A, class IN
      Name: du.edu
      [Name Length: 6]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)

```

- The only flag set in the query is **recursion desired**.
- To know the type of DNS server, we check the response to this query.

9	03...	75.75.75.75	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
10	03...	75.75.76.76	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
20	03...	2601:86:102:c...	2001:558:feed::1	DNS	104	Standard query 0x2016 PTR 7.2.253.130.in-addr.arpa
21	03...	2001:558:feed...	2601:86:102:cbe4::...	DNS	570	Standard query response 0x2016 PTR 7.2.253.130.in-addr
25	03...	2601:86:102:c...	2001:558:feed::1	DNS	130	Standard query 0x9908 PTR 7.2.253.130.in-addr.arpa
27	03...	2001:558:feed...	2601:86:102:cbe4::...	DNS	1077	Standard query response 0x9908 PTR 7.2.253.130.in-addr

```

Ethernet II, Src: f6:4b:2a:9f:9f:28 (f6:4b:2a:9f:9f:28), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.129
User Datagram Protocol, Src Port: 53, Dst Port: 36977
Domain Name System (response)
  Transaction ID: 0x4264
  ▼ Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Authoritative: Server is not an authority for domain
    .... 0... .. = Truncated: Message is not truncated
    .... 1... .. = Recursion desired: Do query recursively

```

In the response, the flag **authoritative** is not set. Thus, it must be a local server having the IPA of the hostname cached.

1.4 :

No.	Time	Source	Destination	Protocol	Length	Info
2	03...	10.0.0.129	75.75.75.75	DNS	66	Standard query 0x4264 A du.edu
3	03...	10.0.0.129	75.75.76.76	DNS	66	Standard query 0x4264 A du.edu
4	03...	2601:86:102:c...	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu
5	03...	2601:86:102:c...	2001:558:feed::2	DNS	86	Standard query 0x4264 A du.edu
6	03...	2001:558:feed...	2601:86:102:cbe4...	DNS	102	Standard query response 0x4264 A du.edu A 1...
7	03...	2001:558:feed...	2601:86:102:cbe4...	DNS	102	Standard query response 0x4264 A du.edu A 1...
9	03...	75.75.75.75	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 1...
10	03...	75.75.76.76	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 1...

Total 4 DNS servers are queried for resolving the domain name du.edu.

1.5 :

	Time	Source	Destination	Proto	Length	Info
2	03:40:10.1...	10.0.0.129	75.75.75.75	DNS	66	Standard query 0x4264 A du.edu
3	03:40:10.1...	10.0.0.129	75.75.76.76	DNS	66	Standard query 0x4264 A du.edu
4	03:40:10.1...	2601:86:102:cbe...	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu
5	03:40:10.1...	2601:86:102:cbe...	2001:558:feed::2	DNS	86	Standard query 0x4264 A du.edu
6	03:40:10.1...	2001:558:feed::1	2601:86:102:cbe4...	DNS	102	Standard query response 0x4264 A du.edu A 130.253.2.7
7	03:40:10.1...	2001:558:feed::2	2601:86:102:cbe4...	DNS	102	Standard query response 0x4264 A du.edu A 130.253.2.7
9	03:40:14.6...	75.75.75.75	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
10	03:40:14.6...	75.75.76.76	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
20	03:40:16.4...	2601:86:102:cbe...	2001:558:feed::1	DNS	104	Standard query 0x2016 PTR 7.2.253.130.in-addr.arpa
21	03:40:16.5...	2001:558:feed::1	2601:86:102:cbe4...	DNS	570	Standard query response 0x2016 PTR 7.2.253.130.in-addr.arpa
25	03:40:16.5...	2601:86:102:cbe...	2001:558:feed::1	DNS	130	Standard query 0x9908 PTR 7.2.253.130.in-addr.arpa
27	03:40:16.6...	2001:558:feed::1	2601:86:102:cbe4...	DNS	1077	Standard query response 0x9908 PTR 7.2.253.130.in-addr.arpa

Packet #9 contains the response of the query sent in packet #2 as highlighted. The flags set are response, recursion desired and recursion available.

Domain Name System (response)
Transaction ID: 0x4264
Flags: 0x8180 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
.... 0... .. = Authoritative: Server is not an authority for domain
.... 0... .. = Truncated: Message is not truncated
.... 1... .. = Recursion desired: Do query recursively
.... 1... .. = Recursion available: Server can do recursive queries
.... 0... .. = Z: reserved (0)
.... 0... .. = Answer authenticated: Answer/authority portion was not at
.... 0... .. = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1

1.6 :

```

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ du.edu: type A, class IN
    Name: du.edu
    [Name Length: 6]
    [Label Count: 2]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
▼ Answers
  ▼ du.edu: type A, class IN, addr 130.253.2.7
    Name: du.edu
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 600
    Data length: 4
    Address: 130.253.2.7

```

We get one answer from the server. The response is not from an authoritative server as this flag is not set.

No.	Time	Source	Destination	Protocol	Length	Info
9	03:40:14.6...	75.75.75.75	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
10	03:40:14.6...	75.75.76.76	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
20	03:40:16.4...	2601:86:102:cbe...	2601:558:feed::1	DNS	104	Standard query 0x2016 PTR 7.2.253.130.in-addr.arpa
21	03:40:16.5...	2601:558:feed::1	2601:86:102:cbe4...	DNS	570	Standard query response 0x2016 PTR 7.2.253.130.in-addr
25	03:40:16.5...	2601:86:102:cbe...	2601:558:feed::1	DNS	130	Standard query 0x9908 PTR 7.2.253.130.in-addr.arpa
27	03:40:16.6...	2601:558:feed::1	2601:86:102:cbe4...	DNS	1077	Standard query response 0x9908 PTR 7.2.253.130.in-addr

```

► Frame 9: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
► Ethernet II, Src: f6:4b:2a:9f:9f:20 (f6:4b:2a:9f:9f:20), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
► Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.129
► User Datagram Protocol, Src Port: 53, Dst Port: 36977
▼ Domain Name System (response)
  Transaction ID: 0x4264
  ▼ Flags: 0x0100 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Authoritative: Server is not an authority for domain
    .... 0... .. = Truncated: Message is not truncated
    .... 1... .. = Recursion desired: Do query recursively
    .... 1... .. = Recursion available: Server can do recursive queries
    .... 0... .. = Z: reserved (0)
    .... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... 0... .. = Non-authenticated data: Unacceptable
    .... 0000 = Reply code: No error (0)
  Questions: 1

```

1.7 :

25	03...	2601:86:...	2001:558:...	DNS	130	Standard query 0x9908 PTR 7.2.253.130.in-addr.arpa
27	03...	2001:558...	2601:86:1...	DNS	1077	Standard query response 0x9908 PTR 7.2.253.130.in-addr.arpa

▶ Frame 25: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0 ▶ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: f6:4b:2a:9f:9f:28 (f6:4b:2a:9f:9f:28) ▶ Internet Protocol Version 6, Src: 2601:86:102:cbe4:d4ad:822b:ead:1c8a, Dst: 2001:558:feed::1 ▶ Transmission Control Protocol, Src Port: 55267, Dst Port: 53, Seq: 2893886349, Ack: 2584129860, ▶ Domain Name System (query) Length: 42 Transaction ID: 0x9908 ▼ Flags: 0x0100 Standard query 0... .. = Response: Message is a query .000 0... .. = Opcode: Standard query (0) = Truncated: Message is not truncated 1... .. = Recursion desired: Do query recursively 0... .. = Z: reserved (0) 0... .. = Non-authenticated data: Unacceptable Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 ▼ Queries ▼ 7.2.253.130.in-addr.arpa: type PTR, class IN Name: 7.2.253.130.in-addr.arpa [Name Length: 24] [Label Count: 6] Type: PTR (domain name PoinTeR) (12) Class: IN (0x0001)

The query in packet #25 is of the type PTR and it is used for reverse DNS lookup, i.e. given the IPA, the hostname is provided in the response.

1.8 :

The packet #27 contains the response of the packet #25.

21	03:40:16.5...	2001:558:feed::1	2601:86:102:cbe4...	DNS	570	Standard query response 0x2016 PTR 7.2.253.130.in-addr.arpa PTR
25	03:40:16.5...	2601:86:102:cbe...	2001:558:feed::1	DNS	130	Standard query 0x9908 PTR 7.2.253.130.in-addr.arpa
27	03:40:16.6...	2001:558:feed::1	2601:86:102:cbe4...	DNS	1077	Standard query response 0x9908 PTR 7.2.253.130.in-addr.arpa PTR

```

Answer RRs: 42
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ 7.2.253.130.in-addr.arpa: type PTR, class IN
    Name: 7.2.253.130.in-addr.arpa
    [Name Length: 24]
    [Label Count: 6]
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
▼ Answers
  ▼ 7.2.253.130.in-addr.arpa: type PTR, class IN, notagora.du.edu
    Name: 7.2.253.130.in-addr.arpa
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
    Time to live: 86400
    Data length: 17
    Domain Name: notagora.du.edu
  ▼ 7.2.253.130.in-addr.arpa: type PTR, class IN, mme.du.edu
    Name: 7.2.253.130.in-addr.arpa
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
    Time to live: 86400
    Data length: 6
    Domain Name: mme.du.edu
  ▼ 7.2.253.130.in-addr.arpa: type PTR, class IN, m.du.edu
    Name: 7.2.253.130.in-addr.arpa
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)

```

The response contains 42 resource records. All of them contain the hostname to which the queried IPA maps to.

2 SET 2: Using the DNS_2.pcapng:

2.1 :

No.	▲ Time	Source	Destination	Proto	Lengt	Info
10	11:35:40.4...	192.168.0.7	208.78.70.24	DNS	66	Standard query 0xcb6e A du.edu
11	11:35:40.5...	208.78.70.24	192.168.0.7	DNS	276	Standard query response 0xcb6e A du.edu A 130.253.2.7
160	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	67	Standard query 0xba83 A mit.edu
161	11:35:50.9...	208.78.70.24	192.168.0.7	DNS	67	Standard query response 0xba83 Refused A mit.edu
162	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	72	Standard query 0x52da A mit.edu.Home
163	11:35:51.0...	208.78.70.24	192.168.0.7	DNS	72	Standard query response 0x52da Refused A mit.edu.Home

The destination IPA of the server is 208.78.70.24.

10	11:35:40.5...	192.168.0.7	208.78.70.24	DNS	66	Standard query	0xcb6e A du.edu
11	11:35:40.5...	208.78.70.24	192.168.0.7	DNS	276	Standard query response	0xcb6e A du.edu A 130.253.2.7 NS
160	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	67	Standard query	0xba83 A mit.edu
161	11:35:50.9...	208.78.70.24	192.168.0.7	DNS	67	Standard query response	0xba83 Refused A mit.edu
162	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	72	Standard query	0x52da A mit.edu.Home
163	11:35:51.0...	208.78.70.24	192.168.0.7	DNS	72	Standard query response	0x52da Refused A mit.edu.Home

▶ Frame 11: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits) on interface 0 ▶ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: Apple_01:98:8c (80:e6:50:01:98:8c) ▶ Internet Protocol Version 4, Src: 208.78.70.24, Dst: 192.168.0.7 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 62847 ▾ Domain Name System (response) Transaction ID: 0xcb6e ▶ Flags: 0x8500 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 6 Additional RRs: 2 ▶ Queries ▶ Answers ▾ Authoritative nameservers ▶ du.edu: type NS, class IN, ns cpnr-authdns-dhcp-vm-1.du.edu ▶ du.edu: type NS, class IN, ns cpnr-authdns-dhcp-phys-1.du.edu ▶ du.edu: type NS, class IN, ns ns3.p24.dynect.net ▶ du.edu: type NS, class IN, ns ns2.p24.dynect.net ▾ du.edu: type NS, class IN, ns ns1.p24.dynect.net Name: du.edu Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 3600 Data length: 6 Name Server: ns1.p24.dynect.net ▶ du.edu: type NS, class IN, ns ns4.p24.dynect.net

The request is being sent to the authoritative name server **ns1.p24.dynect.net** as seen in the response in the packet #11.

2.2 :

No.	▲ Time	Source	Destination	Proto	Length	Info
10	11:35:40.4...	192.168.0.7	208.78.70.24	DNS	66	Standard query 0xcb6e A du.edu
11	11:35:40.5...	208.78.70.24	192.168.0.7	DNS	276	Standard query response 0xcb6e A du.edu A 130.253.2.7 NS
160	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	67	Standard query 0xba83 A mit.edu
161	11:35:50.9...	208.78.70.24	192.168.0.7	DNS	67	Standard query response 0xba83 Refused A mit.edu
162	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	72	Standard query 0x52da A mit.edu.Home
163	11:35:51.0...	208.78.70.24	192.168.0.7	DNS	72	Standard query response 0x52da Refused A mit.edu.Home

Packet #11 contains the reply of the query sent in the packet #10. Yes, the DNS server replied as we are getting a standard query response.

11	11:35:40.5...	208.78.70.24	192.168.0.7	DNS	276	Standard query response 0xcb6e A du.edu A 130.253.2.7
160	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	67	Standard query 0xba83 A mit.edu
161	11:35:50.9...	208.78.70.24	192.168.0.7	DNS	67	Standard query response 0xba83 Refused A mit.edu
162	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	72	Standard query 0x52da A mit.edu.Home
163	11:35:51.0...	208.78.70.24	192.168.0.7	DNS	72	Standard query response 0x52da Refused A mit.edu.Home

►	Frame 11: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits) on interface 0
►	Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: Apple_01:98:8c (80:e6:50:01:98:8c)
►	Internet Protocol Version 4, Src: 208.78.70.24, Dst: 192.168.0.7
►	User Datagram Protocol, Src Port: 53, Dst Port: 62847
▼	Domain Name System (response)
	Transaction ID: 0xcb6e
▼	Flags: 0x8500 Standard query response, No error
	1... .. = Response: Message is a response
	.000 0... .. = Opcode: Standard query (0)
1... .. = Authoritative: Server is an authority for domain
0... .. = Truncated: Message is not truncated
1... .. = Recursion desired: Do query recursively
0... .. = Recursion available: Server can't do recursive queries
0... .. = Z: reserved (0)
0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
0... .. = Non-authenticated data: Unacceptable
0000 = Reply code: No error (0)
	Questions: 1
	Answer RRs: 1
	Authority RRs: 6
	Additional RRs: 2

The response, recursion desired and authoritative flags are set in the response.

2.3 :

160	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	67	Standard query 0xba83 A mit.edu
161	11:35:50.9...	208.78.70.24	192.168.0.7	DNS	67	Standard query response 0xba83 Ref
162	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	72	Standard query 0x52da A mit.edu.Hc
163	11:35:51.0...	208.78.70.24	192.168.0.7	DNS	72	Standard query response 0x52da Ref

►	Frame 160: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
►	Ethernet II, Src: Apple_01:98:8c (80:e6:50:01:98:8c), Dst: Actionte_c0:27:a0 (40:8b:07:c0:27:a0)
►	Internet Protocol Version 4, Src: 192.168.0.7, Dst: 208.78.70.24
►	User Datagram Protocol, Src Port: 63882, Dst Port: 53
▼	Domain Name System (query)
	Transaction ID: 0xba83
►	Flags: 0x0100 Standard query
	Questions: 1
	Answer RRs: 0
	Authority RRs: 0
	Additional RRs: 0
▼	Queries
▼	mit.edu: type A, class IN
	Name: mit.edu
	[Name Length: 7]
	[Label Count: 2]
	Type: A (Host Address) (1)
	Class: IN (0x0001)

The DNS request in #160 is sent to **ns1.p24.dynect.net**. The DNS request asks the IPA of the hostname **mit.edu** as the type of query is **A**.

2.4 :

The response from the DNS server for the query sent in packet #160, as shown in the packet #161, contains no answer RRs. The reply code is refused. So, the server did not resolve the DNS request.

161	11:35:50.9...	208.78.70.24	192.168.0.7	DNS	67	Standard query response 0xba83 Refused A mit.edu
162	11:35:50.9...	192.168.0.7	208.78.70.24	DNS	72	Standard query 0x52da A mit.edu.Home
163	11:35:51.0...	208.78.70.24	192.168.0.7	DNS	72	Standard query response 0x52da Refused A mit.edu.Home

▶ Frame 161: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▶ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: Apple_01:98:8c (80:e6:50:01:98:8c)
▶ Internet Protocol Version 4, Src: 208.78.70.24, Dst: 192.168.0.7
▶ User Datagram Protocol, Src Port: 53, Dst Port: 63882
▼ Domain Name System (response)
Transaction ID: 0xba83
▼ Flags: 0x8105 Standard query response, Refused
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
.... 0... .. = Authoritative: Server is not an authority for domain
.... 0... .. = Truncated: Message is not truncated
.... 1... .. = Recursion desired: Do query recursively
.... 0... .. = Recursion available: Server can't do recursive queries
.... 0... .. = Z: reserved (0)
.... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
.... 0... .. = Non-authenticated data: Unacceptable
.... 0101 = Reply code: Refused (5)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
▼ mit.edu: type A, class IN
Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)

3 SET 3: Using the DNS_3.pcapng:

3.1 :

No.	Time	Source	Destination	Proto	Lengt	Info
1	09:11:23.0...	192.168.0.13	192.168.0.1	DNS	78	Standard query 0xf339 A a.root-servers.net
2	09:11:23.0...	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xf339 A a.root-servers.net
3	09:11:23.0...	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xd73d AAAA a.root-servers.net
4	09:11:23.0...	192.168.0.1	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4
5	09:11:23.0...	205.171.2.25	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4

The DNS query in packet #1 is sent to the IPA 192.168.0.1. It is a local DNS server.

3.2 :

No.	Time	Source	Destination	Proto	Length	Info
1	09:11:23.0...	192.168.0.13	192.168.0.1	DNS	78	Standard query 0xf339 A a.root-servers.net
2	09:11:23.0...	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xf339 A a.root-servers.net
3	09:11:23.0...	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xd73d AAAA a.root-servers.net
4	09:11:23.0...	192.168.0.1	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4
5	09:11:23.0...	205.171.2.25	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4

The DNS query in packet #2 is sent to the IPA 205.171.2.25. It is a local DNS server.

3.3 :

No.	Time	Source	Destination	Proto	Length	Info
1	09:11:23.0...	192.168.0.13	192.168.0.1	DNS	78	Standard query 0xf339 A a.root-servers.net
2	09:11:23.0...	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xf339 A a.root-servers.net
3	09:11:23.0...	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xd73d AAAA a.root-servers.net
4	09:11:23.0...	192.168.0.1	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4
5	09:11:23.0...	205.171.2.25	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4

Packet #5 contains the response of the packet sent in the query #2.

5	09:11:23.0...	205.171.2.25	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A
Frame 5: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0 Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf) Internet Protocol Version 4, Src: 205.171.2.25, Dst: 192.168.0.13 User Datagram Protocol, Src Port: 53, Dst Port: 64981 Domain Name System (response) Transaction ID: 0xf339 Flags: 0x8180 Standard query response, No error 1... .. = Response: Message is a response .000 0... .. = Opcode: Standard query (0) 0... .. = Authoritative: Server is not an authority for domain 0... .. = Truncated: Message is not truncated 1... .. = Recursion desired: Do query recursively 1... .. = Recursion available: Server can do recursive queries 0... .. = Z: reserved (0) 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server 0... .. = Non-authenticated data: Unacceptable 0000 = Reply code: No error (0) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 Queries a.root-servers.net: type A, class IN Name: a.root-servers.net [Name Length: 18] [Label Count: 3] Type: A (Host Address) (1) Class: IN (0x0001) Answers a.root-servers.net: type A, class IN, addr 198.41.0.4 Name: a.root-servers.net Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 600564 Data length: 4 Address: 198.41.0.4 [Request In: 2]						

In the response, we get the IPA of the hostname **a.root-servers.net** which was what was queried as the type of query is **A**.

3.4 :

No.	Time	Source	Destination	Pr	▲	Length	Info
2	09:11...	192.168.0.13	205.171.2.25	DNS		78	Standard query 0xf339 A a.root-servers.net
3	09:11...	192.168.0.13	205.171.2.25	DNS		78	Standard query 0xd73d AAAA a.root-servers.net
4	09:11...	192.168.0.1	192.168.0.13	DNS		94	Standard query response 0xf339 A a.root-servers.net
5	09:11...	205.171.2.25	192.168.0.13	DNS		94	Standard query response 0xf339 A a.root-servers.net
7	09:11...	205.171.2.25	192.168.0.13	DNS		106	Standard query response 0xd73d AAAA a.root-servers.net
8	09:11...	192.168.0.13	198.41.0.4	DNS		67	Standard query 0x9936 A mit.edu
9	09:11...	198.41.0.4	192.168.0.13	DNS		302	Standard query response 0x9936 A mit.edu NS f.e

▶ Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 ▶ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actionte_c0:27:a0 (40:8b:07:c0:27:a0)
 ▶ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 205.171.2.25
 ▶ User Datagram Protocol, Src Port: 64981, Dst Port: 53
 ▼ Domain Name System (query)
 Transaction ID: 0xf339
 ▶ Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 ▼ Queries
 ▼ a.root-servers.net: type A, class IN
 Name: a.root-servers.net
 [Name Length: 18]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 5]

The difference between query in packet #2 and packet #3 is the type of the query. In #2, query has type **A** which resolves the IPA in IPv4 whereas in #3, query has type **AAAA** which resolves the IPA in IPv6.

No.	Time	Source	Destination	Pr	▲	Length	Info
2	09:11...	192.168.0.13	205.171.2.25	DNS		78	Standard query 0xf339 A a.root-servers.net
3	09:11...	192.168.0.13	205.171.2.25	DNS		78	Standard query 0xd73d AAAA a.root-servers.net
4	09:11...	192.168.0.1	192.168.0.13	DNS		94	Standard query response 0xf339 A a.root-servers.net
5	09:11...	205.171.2.25	192.168.0.13	DNS		94	Standard query response 0xf339 A a.root-servers.net
7	09:11...	205.171.2.25	192.168.0.13	DNS		106	Standard query response 0xd73d AAAA a.root-servers.net
8	09:11...	192.168.0.13	198.41.0.4	DNS		67	Standard query 0x9936 A mit.edu
9	09:11...	198.41.0.4	192.168.0.13	DNS		302	Standard query response 0x9936 A mit.edu NS f.e

▶ Frame 3: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 ▶ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actionte_c0:27:a0 (40:8b:07:c0:27:a0)
 ▶ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 205.171.2.25
 ▶ User Datagram Protocol, Src Port: 26149, Dst Port: 53
 ▼ Domain Name System (query)
 Transaction ID: 0xd73d
 ▶ Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 ▼ Queries
 ▼ a.root-servers.net: type AAAA, class IN
 Name: a.root-servers.net
 [Name Length: 18]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 7]

3.5 :

8	09:11...	192.168.0.13	198.41.0.4	DNS	67	Standard query 0x9936 A mit.edu
9	09:11...	198.41.0.4	192.168.0.13	DNS	302	Standard query response 0x9936 A mit
...	09:11...	192.168.0.13	205.171.2.25	DNS	77	Standard query 0x868a A a.edu-server
...	09:11...	192.168.0.13	205.171.2.25	DNS	77	Standard query 0x4a06 AAAA a.edu-server
▶ Frame 8: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0						
▶ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actionte_c0:27:a0 (40:8b:						
▶ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 198.41.0.4						
▶ User Datagram Protocol, Src Port: 39300, Dst Port: 53						
▼ Domain Name System (query)						
Transaction ID: 0x9936						
▶ Flags: 0x0100 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 0						
▼ Queries						
▼ mit.edu: type A, class IN						
Name: mit.edu						
[Name Length: 7]						
[Label Count: 2]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
[Response In: 9]						

The query in packet #8 is used to get the IPA of the hostname **mit.edu** as the type of query is **A**. Since the IPA to which packet is sent is 198.41.0.4 which was earlier resolved for the hostname **a.root-servers.net**, also the response in packet #9 contains the list of .edu TLD servers, thus it is a **root server**.

3.6 :

```

9 09:11... 198.41.0.4 192.168.0.13 DNS 302 Standard query response 0x9936 A mit.edu NS f.edu-servers.net NS a.edu-servers.net NS g...
... 09:11... 192.168.0.13 205.171.2.25 DNS 77 Standard query 0x868a A a.edu-servers.net
... 09:11... 192.168.0.13 205.171.2.25 DNS 77 Standard query 0x405 AAAA a.edu-servers.net
User Datagram Protocol, Src Port: 53, Dst Port: 39300
Domain Name System (response)
Transaction ID: 0x9936
  Flags: 0x8100 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    ....0... .. = Authoritative: Server is not an authority for domain
    ....0... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    ....0... .. = Recursion available: Server can't do recursive queries
    ....0... .. = Z: reserved (0)
    ....0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    ....0... .. = Non-authenticated data: Unacceptable
    ....0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 6
Additional RRs: 7
Queries
  mit.edu: type A, class IN
    Name: mit.edu
    [Name Length: 7]
    [Label Count: 2]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
  Authoritative nameservers
    edu: type NS, class IN, ns f.edu-servers.net
      Name: edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 172800
      Data length: 19
      Name Server: f.edu-servers.net
    edu: type NS, class IN, ns a.edu-servers.net
      Name: edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 172800
      Data length: 4
      Name Server: a.edu-servers.net

```

The packet #9 contains the response of the query sent in packet #8. The flags set in this are response and recursion desired. No, it does not have the answer the user wants as the no. of answer RRs = 0. It provides the list of .edu TLD servers.

3.7 :

16	09:11...	192.168.0.13	192.5.6.30	DNS	67	Standard query 0x97ae A mit.edu
17	09:11...	192.5.6.30	192.168.0.13	DNS	446	Standard query response 0x07ae A m
▶ Frame 16: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0						
▶ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actionte_c0:27:a0 (40:8b:f						
▶ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 192.5.6.30						
▶ User Datagram Protocol, Src Port: 36260, Dst Port: 53						
▼ Domain Name System (query)						
Transaction ID: 0x97ae						
▶ Flags: 0x0100 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 0						
▼ Queries						
▼ mit.edu: type A, class IN						
Name: mit.edu						
[Name Length: 7]						
[Label Count: 2]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
[Response In: 17]						

TLD server is being queried in the packet #16. It is thus not a local DNS server.

3.8 :

```

17 09:11... 192.5.6.30 192.168.0.13 DNS 446 Standard query response 0x97ae A mit.edu NS usw2.akam.net NS asia1.akam.net NS
▼ Domain Name System (response)
  Transaction ID: 0x97ae
  ▼ Flags: 0x0100 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Authoritative: Server is not an authority for domain
    .... 0... .. = Truncated: Message is not truncated
    .... 1... .. = Recursion desired: Do query recursively
    .... 0... .. = Recursion available: Server can't do recursive queries
    .... 0... .. = Z: reserved (0)
    .... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... 0... .. = Non-authenticated data: Unacceptable
    .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 8
  Additional RRs: 11
  ▼ Queries
    ▼ mit.edu: type A, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
    ▼ Authoritative nameservers
      ▼ mit.edu: type NS, class IN, ns usw2.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to Live: 172800
        Data length: 15
        Name Server: usw2.akam.net
      ▼ mit.edu: type NS, class IN, ns asia1.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)

```

Packet #17 contains the response of the query sent in the packet #16. The flags set in this are response and recursion desired. No, it does not have the answer the user wants. It provides the information about the authoritative name servers as shown.

3.9 :

22	09:11...	192.168.0.13	184.26.161....	DNS	67	Standard query 0x85b6 A mit.edu
23	09:11...	184.26.161....	192.168.0.13	DNS	83	Standard query response 0x85b6 A mit.edu
6	09:11...	192.168.0.13	205.171.2.25	ICMP	122	Destination unreachable (Port unreachable)

▶	Frame 22: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▶	Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actionte_c0:27:a0 (40:8b:07:c0:27:a0)
▶	Internet Protocol Version 4, Src: 192.168.0.13, Dst: 184.26.161.64
▶	User Datagram Protocol, Src Port: 56524, Dst Port: 53
▼	Domain Name System (query)
	Transaction ID: 0x85b6
▶	Flags: 0x0100 Standard query
	Questions: 1
	Answer RRs: 0
	Authority RRs: 0
	Additional RRs: 0
▼	Queries
▼	mit.edu: type A, class IN
	Name: mit.edu
	[Name Length: 7]
	[Label Count: 2]
	Type: A (Host Address) (1)
	Class: IN (0x0001)
	[Response In: 23]

The query in packet #22 is used to get the IPA of the hostname **mit.edu** as the type of query is **A**. An authoritative name server is being queried.

3.10 :

```

23 09:11... 184.26.161... 192.168.0.13 DNS 83 Standard query response 0x85b6 A mit.edu A 23.195.140.181
6 09:11... 192.168.0.13 205.171.2.25 TC 122 Destination unreachable (Port unreachable)
▶ User Datagram Protocol, Src Port: 53, Dst Port: 56524
▼ Domain Name System (response)
  Transaction ID: 0x85b6
  ▼ Flags: 0x8500 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... .1.. .... = Authoritative: Server is an authority for domain
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..0... .. = Recursion available: Server can't do recursive queries
    .... ..0... .. = Z: reserved (0)
    .... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... ..0... .. = Non-authenticated data: Unacceptable
    .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ mit.edu: type A, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
    ▼ Answers
      ▼ mit.edu: type A, class IN, addr 23.195.140.181
        Name: mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20
        Data length: 4
        Address: 23.195.140.181
        [Request In: 22]

```

The packet #23 contains the response of the packet #22. The flags set in this are response, recursion desired and authoritative. Yes, it has the answer the user wants. It provides the IPA of the hostname **mit.edu**.

4 Using dig command:

4.1 :

```
$ dig mit.edu NS

; <<>> DiG 9.10.6 <<>> mit.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13688
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
mit.edu.                IN      NS

;; ANSWER SECTION:
mit.edu.                1383    IN      NS      asia2.akam.net.
mit.edu.                1383    IN      NS      usw2.akam.net.
mit.edu.                1383    IN      NS      asia1.akam.net.
mit.edu.                1383    IN      NS      use2.akam.net.
mit.edu.                1383    IN      NS      ns1-173.akam.net.
mit.edu.                1383    IN      NS      use5.akam.net.
mit.edu.                1383    IN      NS      ns1-37.akam.net.
mit.edu.                1383    IN      NS      eur5.akam.net.

;; Query time: 104 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct 26 12:05:12 IST 2018
;; MSG SIZE rcvd: 203
```

The dig command used to determine the authoritative DNS servers for *mit.edu* is: **dig mit.edu NS** as highlighted.

4.2 :

```
$ dig www.du.edu ritchieschool.du.edu NS

; <=> DiG 9.10.6 <=> www.du.edu ritchieschool.du.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61279
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;www.du.edu.                IN      A

;; ANSWER SECTION:
www.du.edu.                297     IN      CNAME   www.du.edu.cdn.cloudflare.net.
www.du.edu.cdn.cloudflare.net. 137     IN      A       104.25.203.95
www.du.edu.cdn.cloudflare.net. 137     IN      A       104.25.204.95

;; Query time: 58 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct 26 12:08:53 IST 2018
;; MSG SIZE rcvd: 114

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34366
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;ritchieschool.du.edu.      IN      NS

;; ANSWER SECTION:
ritchieschool.du.edu.      3599    IN      CNAME   ritchieschool.wengine.com.

;; AUTHORITY SECTION:
wengine.com.              1799    IN      SOA     jim.ns.cloudflare.com. dns.cloudflare.com.

;; Query time: 382 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct 26 12:08:54 IST 2018
;; MSG SIZE rcvd: 147
```

The command used to determine the authoritative DNS servers for *www.du.edu* and *ritchieschool.du.edu* in a single dig command is: **dig www.du.edu ritchieschool.du.edu NS**.

Since it does not provide any answer resource record of type NS, we run the command **dig +trace www.du.edu ritchieschool.du.edu** to see the complete execution of the DNS request.

```

$ dig +trace www.du.edu ritchieschool.du.edu NS

; <<> DiG 9.10.6 <<> +trace www.du.edu ritchieschool.du.edu NS
;; global options: +cmd
.      250802 IN      NS      m.root-servers.net.
.      250802 IN      NS      b.root-servers.net.
.      250802 IN      NS      c.root-servers.net.
.      250802 IN      NS      d.root-servers.net.
.      250802 IN      NS      e.root-servers.net.
.      250802 IN      NS      f.root-servers.net.
.      250802 IN      NS      g.root-servers.net.
.      250802 IN      NS      h.root-servers.net.
.      250802 IN      NS      i.root-servers.net.
.      250802 IN      NS      a.root-servers.net.
.      250802 IN      NS      j.root-servers.net.
.      250802 IN      NS      k.root-servers.net.
.      250802 IN      NS      l.root-servers.net.
.      250802 IN      RRSIG   NS 8 0 518400 20181106050000 20
gEjDDjzBNqNGDKbRpjD+oesysqP28S tipkyErUvzWE0qXtmsFR46j/ihaSX8D49CKJ76fEndQzFTA
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 58 ms

edu.    172800 IN      NS      m.edu-servers.net.
edu.    172800 IN      NS      l.edu-servers.net.
edu.    172800 IN      NS      j.edu-servers.net.
edu.    172800 IN      NS      k.edu-servers.net.
edu.    172800 IN      NS      f.edu-servers.net.
edu.    172800 IN      NS      e.edu-servers.net.
edu.    172800 IN      NS      g.edu-servers.net.
edu.    172800 IN      NS      b.edu-servers.net.
edu.    172800 IN      NS      i.edu-servers.net.
edu.    172800 IN      NS      a.edu-servers.net.
edu.    172800 IN      NS      c.edu-servers.net.
edu.    172800 IN      NS      h.edu-servers.net.
edu.    172800 IN      NS      d.edu-servers.net.
edu.    86400 IN      DS      28065 8 2 4172496CDE85534E51129
edu.    86400 IN      RRSIG   DS 8 1 86400 20181107170000 201
H7UX4UA4/DtJkyY+kMlYY6j7fMPTOD bUrpri/3L9w/etdPPF08KsEmFBMqCfJDyblGBSTQd3zj75tM
;; Received 1169 bytes from 192.203.230.10#53(e.root-servers.net) in 349 ms

du.edu. 172800 IN      NS      ns3.p24.dynect.net.
du.edu. 172800 IN      NS      ns1.p24.dynect.net.
du.edu. 172800 IN      NS      ns2.p24.dynect.net.
du.edu. 172800 IN      NS      ns4.p24.dynect.net.
9DHS4EP5G85PF9NUFK06HEK0048QGK77.edu. 86400 IN NSEC3 1 1 0 - 9VSL4LUB1VNJ9EQQLI
9DHS4EP5G85PF9NUFK06HEK0048QGK77.edu. 86400 IN RRSIG NSEC3 8 2 86400 2018110206
go8KoyfikQD7FdNK7YGCioEx554Ei jk5byGK4WhpV HtA=
RVR5QJQFI939GKP56SL55C48QCCG7BRQ.edu. 86400 IN NSEC3 1 1 0 - S31H6N28EA1T4CUQRJ
RVR5QJQFI939GKP56SL55C48QCCG7BRQ.edu. 86400 IN RRSIG NSEC3 8 2 86400 2018110115
Cf3jBu0db15P9SkaF9pNa1mZnGBVfyUoI/jrvr4FFj r2w=
;; Received 674 bytes from 192.42.93.30#53(g.edu-servers.net) in 168 ms

www.du.edu. 600 IN CNAME www.du.edu.cdn.cloudflare.net.

```

```

www.du.edu.      600    IN      CNAME    www.du.edu.cdn.cloudflare.net.
;; Received 82 bytes from 204.13.251.24#53(ns4.p24.dynect.net) in 48 ms

.                227791 IN      NS      a.root-servers.net.
.                227791 IN      NS      b.root-servers.net.
.                227791 IN      NS      c.root-servers.net.
.                227791 IN      NS      d.root-servers.net.
.                227791 IN      NS      e.root-servers.net.
.                227791 IN      NS      f.root-servers.net.
.                227791 IN      NS      g.root-servers.net.
.                227791 IN      NS      h.root-servers.net.
.                227791 IN      NS      i.root-servers.net.
.                227791 IN      NS      j.root-servers.net.
.                227791 IN      NS      k.root-servers.net.
.                227791 IN      NS      l.root-servers.net.
.                227791 IN      NS      m.root-servers.net.
.                227791 IN      RRSIG   NS 8 0 518400 20181106050000 20181106050000
lOMUVYmU Xe8xBpHhzl1mFShXoNDnOW0tLgEjDDjzBNqnGDKbRpjD+oesysyzqP28S tipkyErUvzWE
zPBtjZyz2fNEJMyEChsnjmFafGAjj4cc gMQj/Q==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 16 ms

edu.             172800 IN      NS      d.edu-servers.net.
edu.             172800 IN      NS      c.edu-servers.net.
edu.             172800 IN      NS      j.edu-servers.net.
edu.             172800 IN      NS      g.edu-servers.net.
edu.             172800 IN      NS      h.edu-servers.net.
edu.             172800 IN      NS      b.edu-servers.net.
edu.             172800 IN      NS      e.edu-servers.net.
edu.             172800 IN      NS      f.edu-servers.net.
edu.             172800 IN      NS      m.edu-servers.net.
edu.             172800 IN      NS      l.edu-servers.net.
edu.             172800 IN      NS      i.edu-servers.net.
edu.             172800 IN      NS      k.edu-servers.net.
edu.             172800 IN      NS      a.edu-servers.net.
edu.             86400 IN      DS      28065 8 2 4172496CDE85534E5112
edu.             86400 IN      RRSIG   DS 8 1 86400 20181107170000 20181107170000
YgpRELC A9B8+Y3C7K0aZgakzj0y60Hg5AH7UX4UA4/DtJkyY+kMLYY6j7FMPTOD bUrpri/3L9w/e
UAzVTLuiSAU2WrmUqXYiwYr1ztGUEkf SngQng==
;; Received 1179 bytes from 192.5.5.241#53(f.root-servers.net) in 60 ms

du.edu.          172800 IN      NS      ns3.p24.dynect.net.
du.edu.          172800 IN      NS      ns1.p24.dynect.net.
du.edu.          172800 IN      NS      ns2.p24.dynect.net.
du.edu.          172800 IN      NS      ns4.p24.dynect.net.
9DHS4EP5G85PF9NUFK06HEK0048QKG77.edu. 86400 IN NSEC3 1 1 0 - 9V5L4LUB1VNJ9EQQL
9DHS4EP5G85PF9NUFK06HEK0048QKG77.edu. 86400 IN RRSIG NSEC3 8 2 86400 201811020
HU1IRgADVLGPV7e2Y0K f/R8u+1Uv63Fqpg08KoyfikQD7FdNK7YGCioEx554Eijjk5byGK4WhpV.H
RVRSQJQFI939GKP56SL55C4BQCCG7BRQ.edu. 86400 IN NSEC3 1 1 0 - S31H6N28EA1T4CUQR
RVRSQJQFI939GKP56SL55C4BQCCG7BRQ.edu. 86400 IN RRSIG NSEC3 8 2 86400 201811011
KNh30dpG5PCaV234VME CYG9CC1I4c8LKDCf3jBu0db15P9SkaF9pNo1mZnGBVfyUoI/jrvr4FFj r
;; Received 684 bytes from 192.48.79.30#53(j.edu-servers.net) in 193 ms

ritchieschool.du.edu. 3600 IN      CNAME    ritchieschool.wpengine.com.
;; Received 89 bytes from 208.78.70.24#53(ns1.p24.dynect.net) in 38 ms

```

As we can see from this, the DNS servers are the same for both.

4.3 :

```
$ dig +trace mit.edu

; <>> DiG 9.10.6 <>> +trace mit.edu
;; global options: +cmd
.      241658  IN      NS      a.root-servers.net.
.      241658  IN      NS      b.root-servers.net.
.      241658  IN      NS      c.root-servers.net.
.      241658  IN      NS      d.root-servers.net.
.      241658  IN      NS      e.root-servers.net.
.      241658  IN      NS      f.root-servers.net.
.      241658  IN      NS      g.root-servers.net.
.      241658  IN      NS      h.root-servers.net.
.      241658  IN      NS      i.root-servers.net.
.      241658  IN      NS      j.root-servers.net.
.      241658  IN      NS      k.root-servers.net.
.      241658  IN      NS      l.root-servers.net.
.      241658  IN      NS      m.root-servers.net.
.      241658  IN      RRSIG  NS 8 0 518400 20181107170000 20181025160000 2134 . neNmFDkn0Z053yxo+QPWTA61cNlb+
zhi2Mcjr5Nixgkd38nAY1MKGETy55Hk s85Td027JDibCImhAPz3bcJrzQuCDP8OFF16gdcIEjJ59D2/L2qTM3Jo 8PVcA/LngVx0zAcDvopiMhyJIWjfiPyRE/L4VH6
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 57 ms

edu.    172800  IN      NS      a.edu-servers.net.
edu.    172800  IN      NS      b.edu-servers.net.
edu.    172800  IN      NS      c.edu-servers.net.
edu.    172800  IN      NS      d.edu-servers.net.
edu.    172800  IN      NS      e.edu-servers.net.
edu.    172800  IN      NS      f.edu-servers.net.
edu.    172800  IN      NS      g.edu-servers.net.
edu.    172800  IN      NS      h.edu-servers.net.
edu.    172800  IN      NS      i.edu-servers.net.
edu.    172800  IN      NS      j.edu-servers.net.
edu.    172800  IN      NS      k.edu-servers.net.
edu.    172800  IN      NS      l.edu-servers.net.
edu.    172800  IN      NS      m.edu-servers.net.
edu.    86400  IN      DS      28065 8 2 4172496CDE85534E511290403558D0481FCFEBAE996DFDDE652006F6 F882CE76
edu.    86400  IN      RRSIG  DS 8 1 86400 20181107170000 20181025160000 2134 . psSRvwEZHAGtaQ0fDmbX8y6V9GhIKa4
H7UX4UA4/DtJkyY+kMLYY6j7fMPTOD bUrpri/3L9w/etdPfp08KsEmFBMqCfJDyblLGBSTQd3zj75tMY2LeEAMf bDrBMpHZkM4EQ1ElgXnuamuVeVarnCNLN0ca0LD1
;; Received 1166 bytes from 199.7.91.13#53(d.root-servers.net) in 88 ms

mit.edu. 172800  IN      NS      usw2.akam.net.
mit.edu. 172800  IN      NS      asia1.akam.net.
mit.edu. 172800  IN      NS      asia2.akam.net.
mit.edu. 172800  IN      NS      use2.akam.net.
mit.edu. 172800  IN      NS      ns1-37.akam.net.
mit.edu. 172800  IN      NS      ns1-173.akam.net.
mit.edu. 172800  IN      NS      eur5.akam.net.
mit.edu. 172800  IN      NS      use5.akam.net.
9DHS4EP5G85PF9NUFK06HEK0048QGK77.edu. 86400 IN NSEC3 1 1 0 - 9V5L4LUB1VNJ9EQQLIHEQCBEACL2500 NS SOA RRSIG DNSKEY NSEC3PARAM
9DHS4EP5G85PF9NUFK06HEK0048QGK77.edu. 86400 IN RRSIG NSEC3 8 2 86400 20181102060921 20181026045921 37217 edu. P98gM6Vr2/3yyeBR/2
go8KoyfikQD7FdNK7YGcioEx554Eijjk5byGK4WhpV HtA=
H1SPUQIV7KAEG07MNVFS0014TGESK44N.edu. 86400 IN NSEC3 1 1 0 - HVGNRMR5BULGQQ5KMPPIZ78Q71T5F6S NS DS RRSIG
H1SPUQIV7KAEG07MNVFS0014TGESK44N.edu. 86400 IN RRSIG NSEC3 8 2 86400 20181102065302 20181026054302 37217 edu. iqs4zGW0v40EPH2J86
G2RZuS8oD0Rmm7TIvEo0Ko7b778xg8g0FjqtZMyAGR RpY=
;; Received 900 bytes from 192.42.93.30#53(g.edu-servers.net) in 161 ms

mit.edu. 20      IN      A      2.20.166.185
;; Received 52 bytes from 96.7.49.64#53(use2.akam.net) in 192 ms
```

We can infer from this output that the DNS request first goes to the root servers, then it goes to the .edu TLD servers and then finally the authoritative name servers for mit.edu.