

Лабораторийн ажлийн тайлан № 3

DNS (DOMAIN NAME SYSTEM)

МТЭС Програм хангамж

О.Энэрэл 22B1NUM0506

3.1 Ажлын зорилго

Энэ лабораторийн ажлаар Домэйн нэрийн системийн (Domain Name System) үйл ажиллагаатай танилцаж, домэйн нэрийг хэрхэн IP хаяг руу хөврүүлдэг талаар судална.

3.2 Даалгавар

3.2.1 nslookup

- а) nslookup командыг ашиглаж дараах веб серверийн IP хаяг, домэйн нэрийг тодорхойлоорой. Мөн дурын 2 вебийн домэйн нэр, IP хаягийг олж хоосон хэсэгт бөглөөрэй.

Вебийн домэйн нэр	IP хаяг	NS сервер
edge-star-mini-shv-01-sin6.facebook.com	157.240.7.35	a.ns.facebook.com
www.instagram.com	163.70.158.174	a.ns.instagram.com
www.wikipedia.org	103.102.166.224	ns0.wikimedia.org
www.harvard.edu	192.0.66.20	ns1.go-vip.net
gaia.cs.umass.edu	128.119.245.12	unix1.cs.umass.edu
alpha.gogo.mn	202.131.225.29	Mdns.mobinet.mn
<a href="http://www.youtube.com">www.youtube.com</a>	142.250.197.14	ns1.google.com
<a href="http://www.num.edu.mn">www.num.edu.mn</a>	202.21.127.145	ns1.num.edu.mn

- а) num.edu.mn гэсэн домэйнтэй холбоотой мэдээллүүдийг авч доорх хүснэгтийг бөглө.

Record-ийн төрөл	IP хаяг эсвэл сервер нэр	NS сервер
MX	mail.num.edu.mn num-edu-mn.mail.protection.outlook.com	ns1.num.edu.mn
NS	ns2.num.edu.mn ns1.num.edu.mn	
A	202.21.127.145	
AAAA	2405:5700:2:3::4	
CNAME		

MX : Имэйл серверийн хаягийг зааж өгдөг.

```
C:\Users\User>nslookup -type=MX num.edu.mn
Server: UnKnown
Address: 2405:5700:2:3::4

Non-authoritative answer:
num.edu.mn      MX preference = 10, mail exchanger = mail.num.edu.mn
num.edu.mn      MX preference = 0, mail exchanger = num-edu-mn.mail.protection.outlook.com
```

Figure 1 MX record

NS: Домэйнд үйлчилдэг нэрийн серверийг зааж өгнө.

```
C:\Users\User>nslookup -type=NS num.edu.mn
Server: UnKnown
Address: 2405:5700:2:3::4

Non-authoritative answer:
num.edu.mn      nameserver = ns2.num.edu.mn
num.edu.mn      nameserver = ns1.num.edu.mn

ns1.num.edu.mn  internet address = 157.15.6.44
ns2.num.edu.mn  internet address = 157.15.7.44
ns2.num.edu.mn  internet address = 64.119.31.44
```

Figure 2 NS record

A: IPv4 хаягийг зааж өгнө.

```
C:\Users\User>nslookup -type=A num.edu.mn
Server: UnKnown
Address: 2405:5700:2:3::4

Non-authoritative answer:
Name:   num.edu.mn
Address: 202.21.127.145
```

Figure 3 A record

AAAA: IPv6 хаягийг зааж өгнө.

```
C:\Users\User>nslookup -type=AAAA num.edu.mn
Server: UnKnown
Address: 2405:5700:2:3::4

Name:   num.edu.mn
```

Figure 4 AAAA record

CNAME: Нэг домэйн нэрийг нөгөө домэйн рүү чиглүүлдэг бичлэг.

```
C:\Users\User>nslookup -type=CNAME num.edu.mn
Server: UnKnown
Address: 2405:5700:2:3::4

num.edu.mn
    primary name server = ns1.num.edu.mn
    responsible mail addr = root.num.edu.mn
    serial = 2014090401
    refresh = 3600 (1 hour)
    retry = 1800 (30 mins)
    expire = 604800 (7 days)
    default TTL = 86400 (1 day)
```

Figure 5 CNAME record байсангүй

### 3.2.2 DNS мессеж дамжуулах

Wireshark програмын тусламжтайгаар домэйн нэр, түүнтэй холбоотой мессежүүд хэрхэн дамжиж байгааг харж болно. Үүний тулд доорх алхмуудыг гүйцэтгэнэ.

- `ipconfig /flushdns` команд ашиглаж төхөөрөмжийнхөө DNS кэшийг цэвэрлэнэ. Ингэснээр домэйн нэрийн хүсэлтийг серверээс авах боломжтой болно.

```
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Figure 6 flushdns

- Мөн ашигладаг интернэт хөтчийнхөө кэшийг цэвэрлэх хэрэгтэй.
- Wireshark програмын *Capture* цэснээс *Start* товчийг дарж сүлжээний урсгалыг цуглуулж эхэлнэ. Ингэснээр зааж өгсөн IP хаяг бүхий сүлжээний картаар дамжиж байгаа бүх пакетыг Wireshark программ цуглуулна.
- Дараа нь веб хөтчөө нээгээд <http://www.ietf.org> хуудсанд хандаарай.
- Веб хуудас бүрэн ачааллаж дууссаны дараа Wireshark программ дээр *Capture* цэснээс *Stop* дарж урсгал цуглуулах процесс зогсооно.

**Жич:** Хэрэв уг үйлдлийг хийхгүй бол дараагийн бүх сүлжээний урсгалыг цуглуулсаар байх бөгөөд төхөөрөмжийн санах ойд хэт ачаалал үүсэх эрсдэлтэй.

- Wireshark-ыг нээгээд шүүлтүүр хэсэгт “dns” протоколоор хайлт хийж, DNS query болон DNS query response мессежийг ажиглан дараах асуултуудын эхний 5 асуулт, мөн 7-р асуултад тус тус хариулна. Шүүлтүүр хэсэгт “ip.addr == answered IP address” ашиглан, гарсан үр дүнгээс зөвхөн 6-р асуултад хариулна.
- www.ietf.org домэйн нэртэй холбоотой локал DNS сервер рүү илгээсэн query болон response мессежүүдийг олж. Эдгээр мессежүүд нь 4-р түвшинд UDP эсвэл TCP протоколын алийг ашиглан дамжуулж байна вэ? DNS query мессежийн хүлээн авах порт нь ямар байна вэ?

1923	14.229174	2405:5700:301:1ee0:159a:5a22:4180:9e63	2405:5700:2:3::4	DNS	92 Standard query 0xb05a AAAA www.ietf.org
1924	14.229725	2405:5700:301:1ee0:159a:5a22:4180:9e63	2405:5700:2:3::4	DNS	92 Standard query 0xf65a A www.ietf.org
1925	14.230188	2405:5700:301:1ee0:159a:5a22:4180:9e63	2405:5700:2:3::4	DNS	92 Standard query 0xb2b1 HTTPS www.ietf.org
1926	14.233392	2405:5700:2:3::4	2405:5700:301:1ee0:159a:5a22:4180:9e63	DNS	234 Standard query response 0x1335 AAAA safebrowsing.google.com CNAME sb.l.go
1927	14.233682	2405:5700:2:3::4	2405:5700:301:1ee0:159a:5a22:4180:9e63	DNS	186 Standard query response 0xd574 A safebrowsing.google.com CNAME sb.l.googl
1928	14.234422	2405:5700:2:3::4	2405:5700:301:1ee0:159a:5a22:4180:9e63	DNS	172 Standard query response 0x067 HTTPS safebrowsing.google.com CNAME sb.l.g
1929	14.234766	2405:5700:2:3::4	2405:5700:301:1ee0:159a:5a22:4180:9e63	DNS	148 Standard query response 0xb05a AAAA www.ietf.org AAAA 2508:4700::6810:2c6
1930	14.235428	2405:5700:2:3::4	2405:5700:301:1ee0:159a:5a22:4180:9e63	DNS	124 Standard query response 0xf65a A www.ietf.org A 104.16.45.99 A 104.16.44.
1931	14.235573	2405:5700:2:3::4	2405:5700:301:1ee0:159a:5a22:4180:9e63	DNS	165 Standard query response 0xb2b1 HTTPS www.ietf.org HTTPS

  

Frame 1923:	92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{96D4538E-98D3-4805-B282-000905E2F5C7}, id 0000	60 f1 8a 45 14 fc 7c b2 7d ab 4c e9
Ethernet II, Src: Intel_ab:4c:e9 (7c:b2:7d:ab:4c:e9), Dst: HuaweiTechno_45:14:fc (60:f1:8a:45:14:fc)		0010 60 6e 00 26 11 40 24 05 57 00 03 01
Internet Protocol Version 6, Src: 2405:5700:301:1ee0:159a:5a22:4180:9e63, Dst: 2405:5700:2:3::4		0020 5a 22 41 80 9e 63 24 05 57 00 00 02
User Datagram Protocol, Src Port: 61657, Dst Port: 53		0030 00 00 00 00 00 04 f0 d9 00 35 00 26
Domain Name System (query)		0040 01 00 00 01 00 00 00 00 00 03 77
		0050 65 74 66 02 65 77 67 00 00 1c 00 00

Figure 7 UDP protocol

Мессежүүд нь 4-р түвшинд UDP протоколыг ашиглан дамжуулж байна.

```

User Datagram Protocol, Src Port: 50249, Dst Port: 53
  Source Port: 50249
  Destination Port: 53
  Length: 40
  Checksum: 0x67ce [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (32 bytes)

```

Figure 8 port number

DNS query мессежийнхүлээн авах порт нь 53 байна.

## 2. DNS query response-ийн илгээх порт ямар байна вэ?

```

1926 14.233392 2405:5700:2:3::4 2405:5700:301:1ee0:159a:5a22:4180:9e63 DNS 234 Standard query response 0x1335
1927 14.233682 2405:5700:2:3::4 2405:5700:301:1ee0:159a:5a22:4180:9e63 DNS 186 Standard query response 0xd574
1928 14.234422 2405:5700:2:3::4 2405:5700:301:1ee0:159a:5a22:4180:9e63 DNS 172 Standard query response 0xb0d67
1929 14.234766 2405:5700:2:3::4 2405:5700:301:1ee0:159a:5a22:4180:9e63 DNS 148 Standard query response 0xb05a
1930 14.235428 2405:5700:2:3::4 2405:5700:301:1ee0:159a:5a22:4180:9e63 DNS 124 Standard query response 0xf65a
1931 14.235573 2405:5700:2:3::4 2405:5700:301:1ee0:159a:5a22:4180:9e63 DNS 165 Standard query response 0x2b21

Frame 1926: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{96D4538E-98D3-4805-B282-000905E2F5C7},
Ethernet II, Src: HuaweiTechno_45:14:fc (60:f1:8a:45:14:fc), Dst: Intel_ab:4c:e9 (7c:b2:7d:ab:4c:e9)
Internet Protocol Version 6, Src: 2405:5700:2:3::4, Dst: 2405:5700:301:1ee0:159a:5a22:4180:9e63
User Datagram Protocol, Src Port: 53, Dst Port: 52296
  Source Port: 53
  Destination Port: 52296
  Length: 180
  Checksum: 0x3a00 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 52]
  [Stream Packet Number: 2]
  [Timestamps]
  UDP payload (172 bytes)

```

Figure 9 response port number

DNS query response-ийн илгээх порт нь 53.

## 3. DNS query мессежийг ямар IP хаяг руу илгээсэн байна вэ? Local DNS серверийн IP хаяг ямар байна вэ? /ipconfig ашиглан шалгана/ Энэ хоёр IP хаяг ижил байна уу, батлан харуулна уу.

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : mcscom.mn
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : 7C-B2-7D-AB-4C-E9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2405:5700:301:1ee0::7(Preferred)
Lease Obtained. . . . . : Wednesday, September 25, 2024 10:00:59 PM
Lease Expires . . . . . : Thursday, September 26, 2024 4:00:58 AM
IPv6 Address. . . . . : 2405:5700:301:1ee0:db5:19b9:df98:5932(Preferred)
Temporary IPv6 Address. . . . . : 2405:5700:301:1ee0:159a:5a22:4180:9e63(Preferred)
Link-local IPv6 Address . . . . . : fe80::c788:7994:104f:2228%15(Preferred)
IPv4 Address. . . . . : 192.168.1.94(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, September 25, 2024 8:15:08 PM
Lease Expires . . . . . : Thursday, September 26, 2024 12:00:56 AM
Default Gateway . . . . . : fe80::1%15
                          192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 243053181
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-8B-C3-31-7C-B2-7D-AB-4C-E9
DNS Servers . . . . . : 2405:5700:2:3::4
                          2405:5700:2:5::4
                          103.57.94.2
                          59.153.112.2
NetBIOS over Tcpip. . . . . : Enabled

```

Figure 10 ipconfig\all result

```

Internet Protocol Version 6, Src: 2405:5700:301:1ee0:159a:5a22:4180:9e63, Dst: 2405:5700:2:3::4
  0110 .... = Version: 6
  .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0010 1000 0100 1011 0100 = Flow Label: 0x284b4
  Payload Length: 40
  Next Header: UDP (17)
  Hop Limit: 64
  Source Address: 2405:5700:301:1ee0:159a:5a22:4180:9e63
  Destination Address: 2405:5700:2:3::4
  [Stream index: 0]

```

Figure 11 destination IP

DNS query мессежийг 2405:5700:2:3::4 IP хаяг руу илгээсэн. Local DNS серверийн IP хаяг нь DNS query мессежийн destination IP хаягтай ижилхэн 2405:5700:2:3::4 байна.

4. DNS query мессежийг шалгана уу. DNS query ямар “төрөл”-ийн рекорд байна вэ? Query мессежинд “хариултууд” (answers) агуулагдаж байна уу?

```

Domain Name System (query)
Transaction ID: 0xb05a
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  www.ietf.org: type AAAA, class IN
  [Response In: 1929]

```

Figure 12 record

DNS query нь AAAA ба А гэсэн 2 төрлийн record-тай байсан. Хариулт агуулаагүй.

5. DNS query response мессежийг шалгая. Хэдэн “хариулт” илгээсэн байна бэ? Эдгээр хариулт тус бүр нь ямар талбаруудыг агуулж байна вэ? Query бүрт 2 хариулт ирсэн.

```

Answers
  www.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2c63
    Name: www.ietf.org
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 232 (3 minutes, 52 seconds)
    Data length: 16
    AAAA Address: 2606:4700::6810:2c63
  www.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2d63
    Name: www.ietf.org
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 232 (3 minutes, 52 seconds)
    Data length: 16
    AAAA Address: 2606:4700::6810:2d63
  [Request In: 1923]
  [Time: 0.005592000 seconds]

```

Figure 13 answer

Хандсан вэб сайтийн домайн нэр, DNS query-ийн record-ийн төрөл, Class, TTL, Data Length, вэб сайтийн ipv6 хаяг зэрэг талбарууд байна.

6. DNS серверээс серверийн IP хаягийн мэдээлэл хүлээн авсны дараа хостоос TCP SYN пакетыг веб сервер рүү илгээж холболт тогтоосон байгаа. SYN сегментий хүлээн авах IP хаяг өмнөх DNS хариу мессежинд өгөгдсөн IP хаягуудын аль нэгтэй таарч байна уу?

```

388 3.913061 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TCP 86 60498 → 443 [SYN] Seq=0 Win=6
488 3.936944 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TCP 74 60498 → 443 [ACK] Seq=1 Ack=1
520 3.937868 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TLSv1.3 1799 Client Hello (SNI=static.ietf
661 3.960226 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TCP 74 60498 → 443 [ACK] Seq=1726 Ac
673 3.963533 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TLSv1.3 138 Change Cipher Spec, Applicati
674 3.964183 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TLSv1.3 166 Application Data
675 3.964601 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TLSv1.3 535 Application Data
808 3.985415 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TCP 74 60498 → 443 [ACK] Seq=2343 Ac
812 3.988064 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TLSv1.3 105 Application Data
897 4.000046 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TCP 74 60498 → 443 [ACK] Seq=2374 Ac
908 4.001675 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TCP 86 60498 → 443 [ACK] Seq=2374 Ac
910 4.001776 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TCP 94 [TCP Dup ACK 908#1] 60498 → 4
911 4.001814 2405:5700:301:1ee0:95c4:682e:1e8e:a21e 2606:4700::6810:2d63 TCP 102 [TCP Dup ACK 908#2] 60498 → 4

Frame 388: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{96D4538E-98D3-4805-B282-000905E2F5C7}, id 0
Ethernet II, Src: Intel_ab:4c:e9 (7c:b2:7d:ab:4c:e9), Dst: HuaweiTechno_45:14:fc (60:f1:8a:45:14:fc)
Internet Protocol Version 6, Src: 2405:5700:301:1ee0:95c4:682e:1e8e:a21e, Dst: 2606:4700::6810:2d63
  0110 .... = Version: 6
  .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 1101 0101 1110 1000 0110 = Flow Label: 0xd5e86
  Payload Length: 32
  Next Header: TCP (6)
  Hop Limit: 64
  Source Address: 2405:5700:301:1ee0:95c4:682e:1e8e:a21e
  Destination Address: 2606:4700::6810:2d63
  [Stream index: 3]
Transmission Control Protocol, Src Port: 60498, Dst Port: 443, Seq: 0, Len: 0

```

Figure 14 ip.addr-p шүүсэн үр дүн

Таарч байна, хоёулаа 2606:4700::6810:2d63 байна.

7. Дээрх веб хуудас нь зураг агуулсан байгаа. Зураг бүрийг авахаасаа өмнө хостоос



## DNS query илгээж байна уу?

No.	dns server	Source	Destination	Protocol	Length	Info
6		2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0x3993 AAAA www.ietf.org
7	3.217797	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0x734c A www.ietf.org
8	3.218465	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0xc565 HTTPS www.ietf.org
12	3.235908	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0xd9fa AAAA www.ietf.org
13	3.237321	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0x2586 A www.ietf.org
16	3.392797	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0x8e10 AAAA www.ietf.org
17	3.393341	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0x7d67 A www.ietf.org
18	3.394143	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0x1175 AAAA www.ietf.org
19	3.394780	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0x2cd7 A www.ietf.org
20	3.395395	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	92	Standard query 0x79f6 HTTPS www.ietf.org
21	3.400598	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	114	Standard query 0x8ba0 AAAA nav-edge.smartscreen.microsoft.com
22	3.401246	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	114	Standard query 0x3625 A nav-edge.smartscreen.microsoft.com
23	3.401824	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	114	Standard query 0xd6e6 HTTPS nav-edge.smartscreen.microsoft.com
36	3.416564	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	94	Standard query 0x9c0c A wpad.mcscom.mn
38	3.417006	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	94	Standard query 0x45f9 AAAA wpad.mcscom.mn
77	3.564611	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	95	Standard query 0xb50e AAAA static.ietf.org
78	3.565367	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	95	Standard query 0xd558 A static.ietf.org
79	3.566250	2405:5700:301:1ee0:95c4:682e:1e8e:a21e	2405:5700:213:4	DNS	95	Standard query 0x9762 HTTPS static.ietf.org

Figure 15 dns query

Зураг бүрийг авахаасаа өмнө хостоос DNS query илгээж байна.

### 3.3 Сорих асуулт

#### 1. DNS протокол үүссэн үндсэн зорилго юу вэ?

DNS протоколын үндсэн зорилго нь интернэт дэх домэйн нэрүүдийг IP хаяг руу хөрвүүлэх явдал юм. Энэ нь хэрэглэгчдэд домэйн нэрээр нэвтрэх боломжийг олгодог бөгөөд интернэт дэх нөөцүүдийг илүү хялбар удирдах, зохион байгуулахад тусалдаг. DNS нь интернэтэд байршил, хаяглалт, нөөцийн удирдлагын системийн үндэс суурь нь болдог.

#### 2. DNS серверийн шаталсан бүтцийн талаар тайлбарла.

- Root сервер: Энэ нь DNS системийн хамгийн дээд түвшин юм. Root серверүүд домэйн нэрийн системийн үндсэн хаяглалтыг агуулдаг. Тухайлбал .com, .org, .net гэх мэт дэд домэйнүүдийг таньж, тухайн дэд домэйн серверүүд рүү чиглүүлдэг.
- Top-Level Domain (TLD) сервер: Root серверээс авсан зааврын дагуу TLD серверүүд нь домэйн нэрийн дээд түвшний хэсгийг хариуцдаг. TLD серверүүд нь тухайн домэйн нэрийн authoritative DNS серверүүдийн хаягийг хадгалдаг.
- Authoritative сервер: Энэ сервер нь тодорхой домэйн нэрийн мэдээллийг хадгалдаг бөгөөд домэйн нэрийг IP хаяг руу хөрвүүлэх хүсэлтийг хариулдаг.

#### 3. DNS кэш гэж юу вэ?

DNS кэш нь DNS серверт түр хадгалагдсан DNS record-ийн мэдээлэл юм. DNS кэш нь хэрэглэгч домэйн нэрийг асуухад, эхлээд Local DNS серверийн кэшээс олно хэрэв олж чадвал, шууд хариулах боломжтой. Олж чадаагүй бол DNS query-г цааш дамжуулж хариулт авсны дараа, local DNS кэшт тодорхой хугацаанд хадгалж, дараа дахин адил асуулт ирвэл кэшийг ашиглан хурдан хариулна.

#### 4. Primary DNS болон Secondary DNS хоорондын ялгааг тайлбарла.

Primary DNS нь хэрэглэгчийн төхөөрөмжийн эсвэл сүлжээний эхлээд хандах DNS сервер юм. Энэ нь хамгийн түрүүнд IP хаягийг өгч, интернэтээр дамжин вэб хуудас руу хандах боломжийг олгодог. Хэрэв Primary DNS сервер ажиллахгүй бол сүлжээний хандалт түр зогсож болно. Secondary DNS сервер нь Primary DNS сервер ажиллахгүй тохиолдолд нөөц сервер болон ажилладаг. Энэ нь Primary DNS сервертэй ижил мэдээллийг агуулдаг бөгөөд Primary DNS серверийн алдаа гарсан үед хэрэглэгчийн хандалтыг үргэлжлүүлж, интернетийн үйлчилгээг

тасалдуулахгүй байлгах зориулалттай.

5. PTR гэж юу вэ?

PTR нь DNS record-ийн нэг төрөл бөгөөд гол үүрэг нь IP хаягтай холбогдсон домэйн нэрийг олох юм. Энгийн DNS нь домэйн нэрээс IP хаягыг олох бол, PTR нь IP хаягаас домэйн нэрийг олох үүрэгтэй юм.

6. TLD болон SLD-ний ялгааг тайлбарла.

TLD нь домэйн нэрийн хамгийн өндөр түвшин бөгөөд ихэвчлэн ерөнхий эсвэл газарзүйн ангиллыг илэрхийлдэг бол, SLD нь вэбсайтын үндсэн нэрийг илэрхийлдэг бөгөөд ихэвчлэн компанийн нэр эсвэл брэндтэй холбоотой байдаг.

7. DNS Resource Record-ийг хэрхэн ашигладаг вэ?

DNS Resource Record-ийг DNS-ийн тархсан мэдээллийг хадгалахад ашигладаг, DNS нь хариу илгээх болгонд 1 буюу түүнээс их Resource Record-ийг ашигладаг.

8. Local DNS сервер ямар үүрэгтэй вэ?

Хэрэглэгч домэйн нэрээр хандалт хийх үед эхлээд Local DNS сервер рүү хүсэлт илгээгддэг. Хэрэв Local DNS сервер нь тухайн домэйн нэрийг кэшдээ хадгалсан бол IP хаягийг шууд өгнө. Хэрэв байхгүй бол Local DNS сервер нь DNS серверийн шаталсан бүтэц рүү хүсэлтийг илгээдэг.

9. Authoritative болон non-authoritative answer-уудын ялгааг тайлбарла.

Authoritative answer нь Primary DNS серверээс ирдэг баталгаажсан, хамгийн сүүлийн үеийн хариулт юм. Non-authoritative answer нь кэшлэгдсэн буюу түр хадгалсан хариулт бөгөөд энэ нь хамгийн сүүлийн үеийн мэдээлэл байгаа эсэхийг баталгаажуулж чадахгүй.

## Дүгнэлт

Тухайн лабораторийн ажлаар DNS хэрхэн ажиллаж байгааг олж мэсэн. Nslookup, ipconfig командийг ашиглаж DNS серверээс дурын домэйн нэрийн талаар хүсэлт илгээж үзсэн. Мөн Wireshark програмын тусламжтайгаар домэйн нэр, түүнтэй холбоотой мессежүүд хэрхэн дамжиж байгааг ажигасан.