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

a) 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
www.youtube.com	142.250.197.14	ns1.google.com
www.num.edu.mn	202.21.127.145	ns1.num.edu.mn

a) 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 программын тусламжтайгаар домэйн нэр, түүнтэй холбоотой мессежүүд хэрхэн дамжиж байгааг харж болно. Үүний тулд доорх алхмуудыг гүйцэтгэнэ.

a. *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

b. Мөн ашигладаг интернэт хөтчийнхөө кэшийг цэвэрлэх хэрэгтэй.
c. Wireshark программын *Capture* цэснээс *Start* товчийг дарж сүлжээний урсгалыг цуглуулж эхэлнэ. Ингэснээр зааж өгсөн IP хаяг бүхий сүлжээний картаар дамжиж байгаа бүх пакетыг Wireshark программ цуглуулна.
d. Дараа нь веб хөтчөө нээгээд http://www.ietf.org хуудсанд хандаарай.
e. 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.
f. 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.

1. www.ietf.org домэйн нэртэй холбоотой локал DNS сервер рүү илгээсэн query болон response мессежүүдийг олъё. 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?

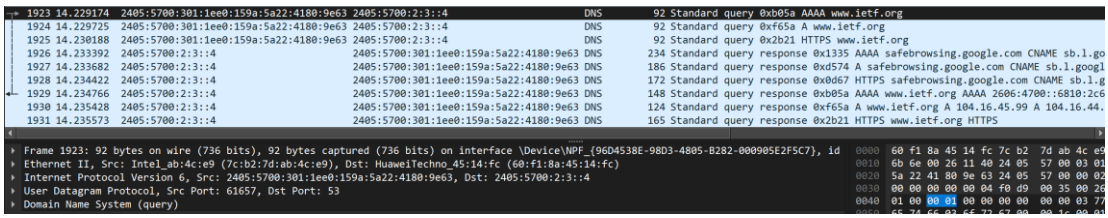

Figure 7 UDP protocol

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

Figure 8 port number

DNS query мессежийнхүлээн авах порт нь 53 байна.

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

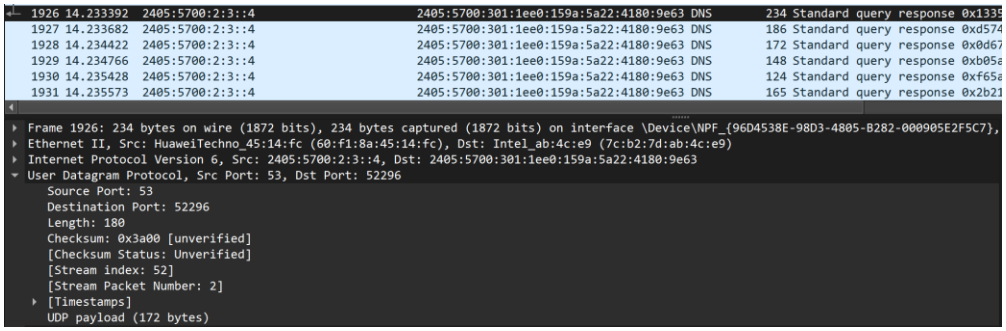

Figure 9 response port number

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.

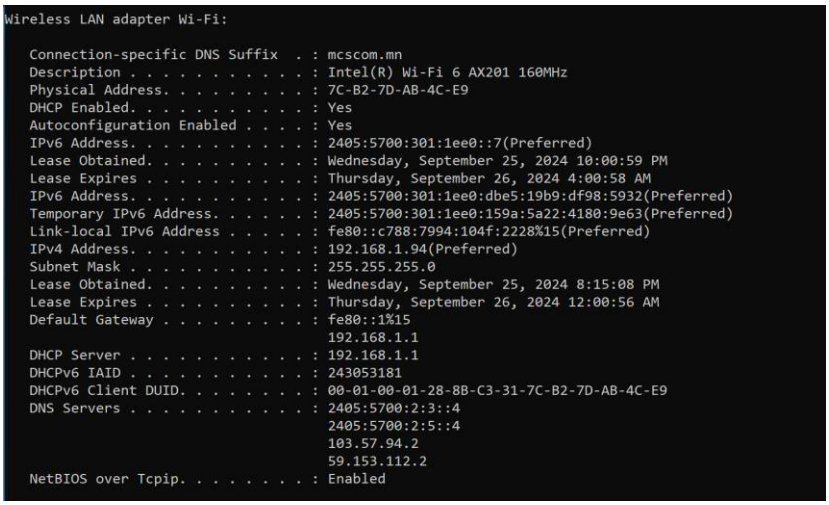

Figure 10 ipconfig\all result

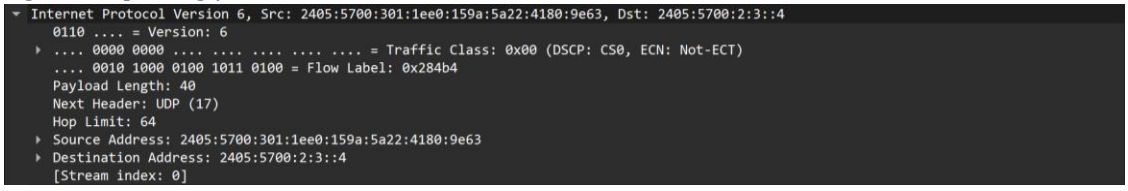

Figure 11 destination IP

DNS query мессежийг 2405:5700:2:3::4 IP хаяг руу илгээсэн. Local DNS серверийн IP хаяг нь DNS query мессежий 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?

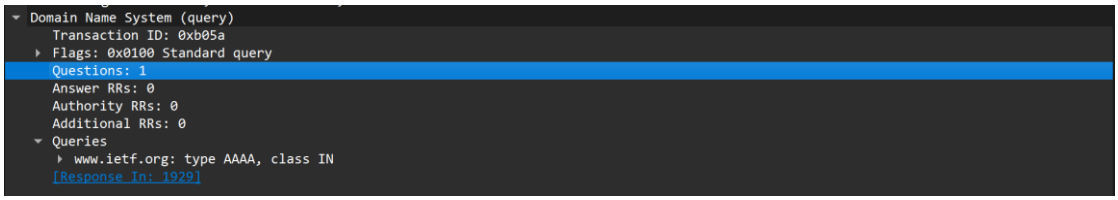

Figure 12 record

DNS query нь AAAA ба A 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.

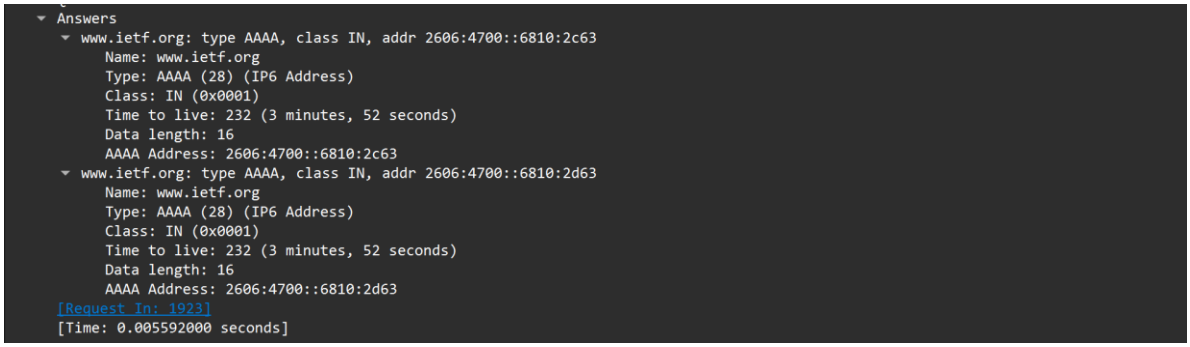

Figure 13 answer

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?

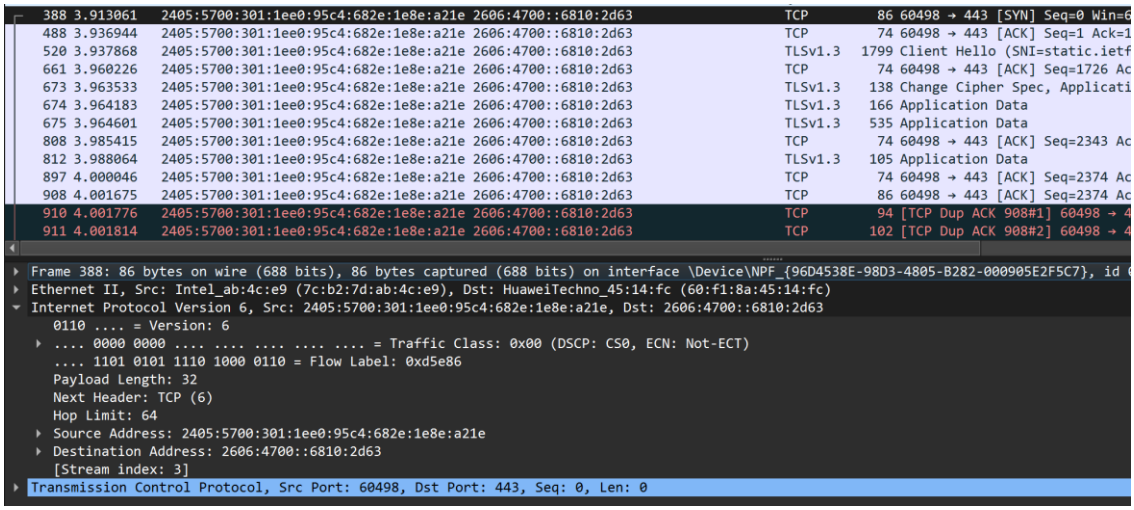

Figure 14 ip.addr-р шүүсэн үр дүн

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?

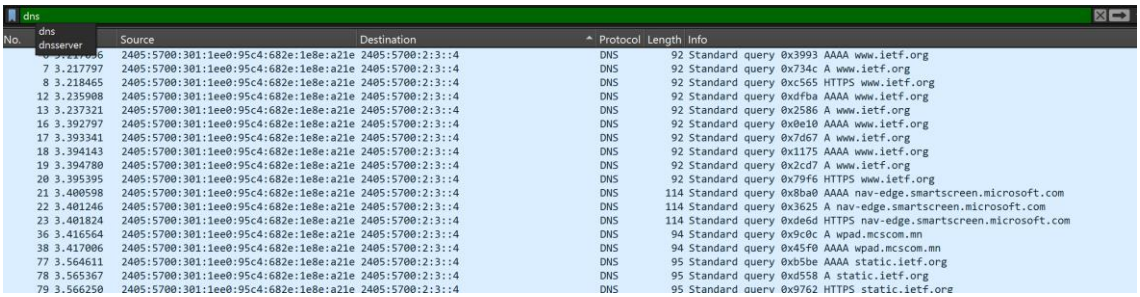

Figure 15 dns query

Зураг бүрийг авахаасаа өмнө хостоосDNS 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 сервэрийн 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-authoratitive 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 соммандийг ашиглаж DNS серверээс дурын домайн нэрийн талаар хүсэлт илгээж үзсэн. Мөн Wireshark програмын тусламжтайгаар домайн нэр, түүнтэй холбоотой мессежүүд хэрхэн дамжиж байгааг ажигасан.