Assignment 2- A case study

Part 1- : DNS Resource Record Analysis over two networks

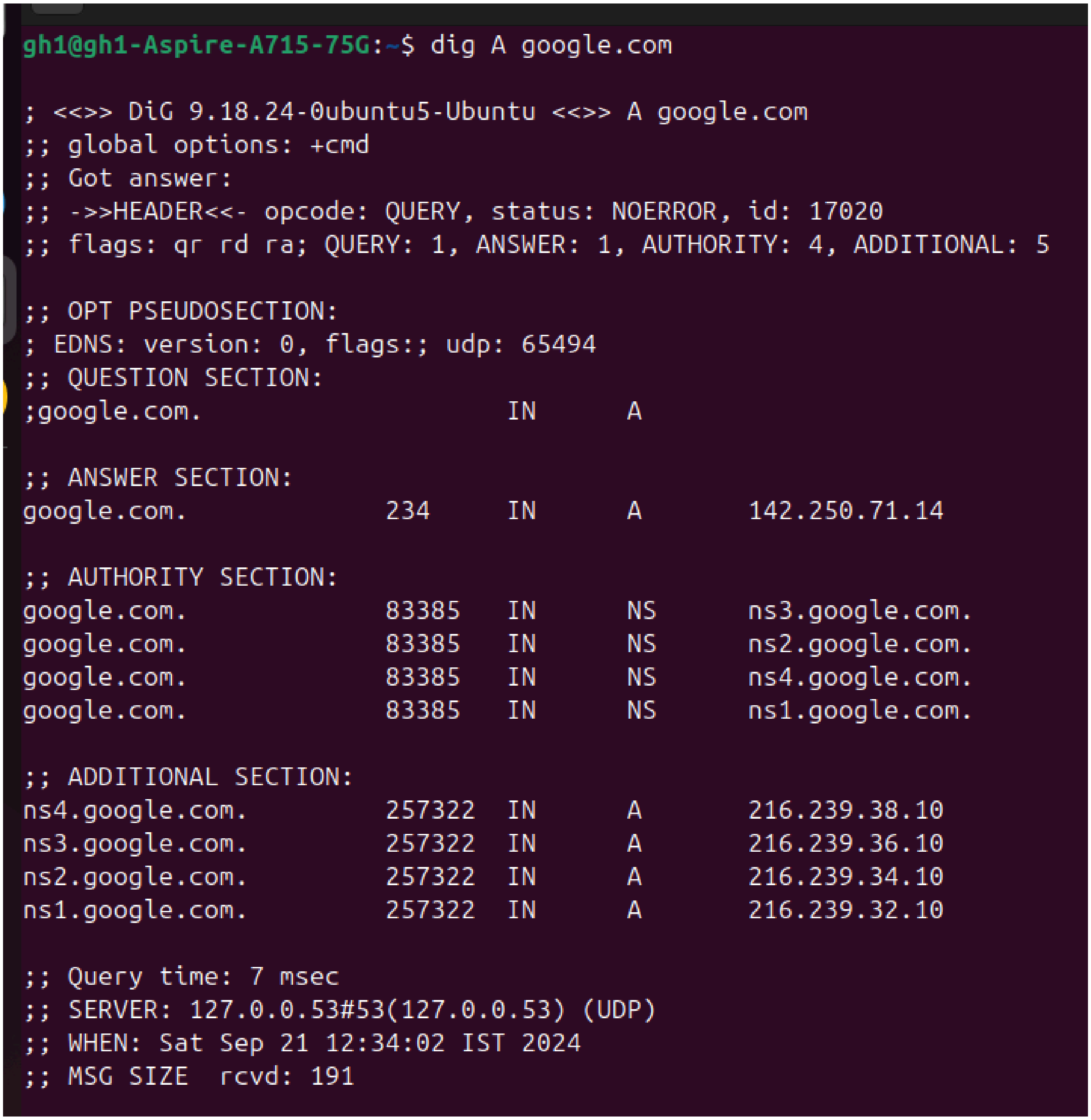
Introduction-

In this section DNS Resource Records (RRs) for google.com, facebook.com, and netflix.com across two different networks first a campus Wi-Fi network (Hostel LAN Wi-FI) and second mobile 4G network. I used DNS querying tool dig to gather information about the A, AAAA, MX, and CNAME and ANY records, for understanding how these DNS records vary between different types of network environments.

Data and Observations-

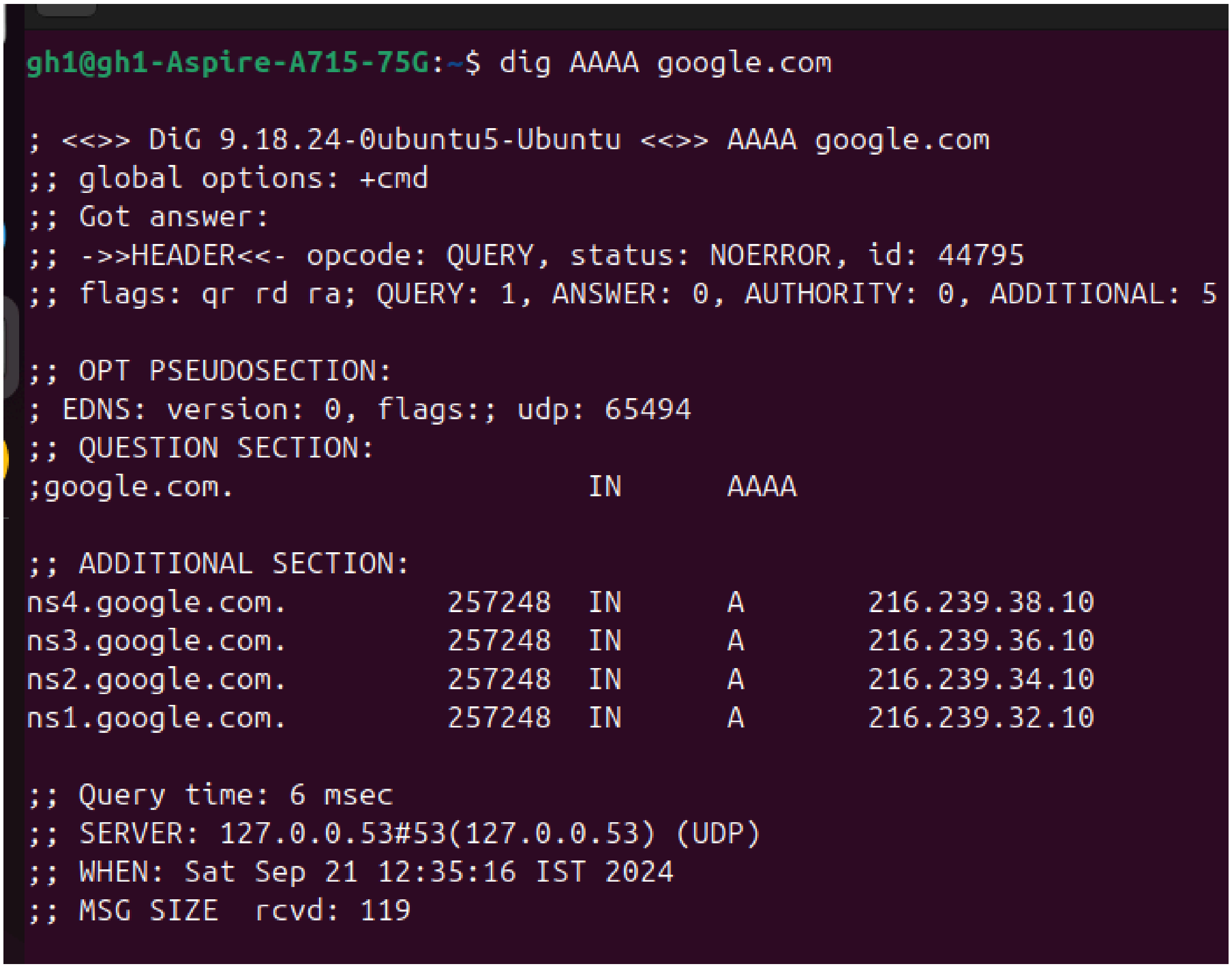
1) For google.com

a) Wi-Fi



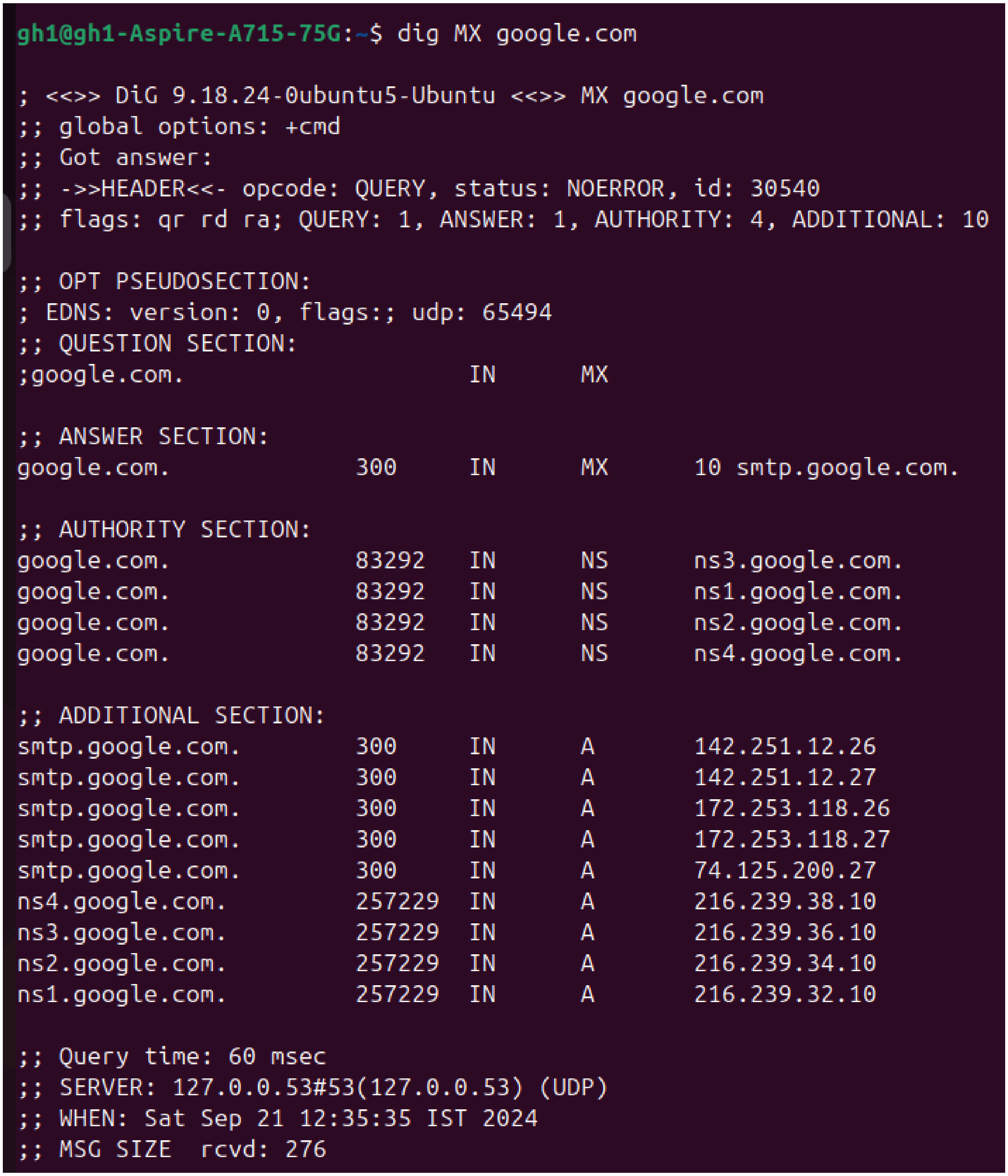
```
gh1@gh1-Aspire-A715-75G:~$ dig A google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> A google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17020
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             234     IN      A       142.250.71.14

;; AUTHORITY SECTION:
google.com.             83385   IN      NS      ns3.google.com.
google.com.             83385   IN      NS      ns2.google.com.
google.com.             83385   IN      NS      ns4.google.com.
google.com.             83385   IN      NS      ns1.google.com.

;; ADDITIONAL SECTION:
ns4.google.com.         257322  IN      A       216.239.38.10
ns3.google.com.         257322  IN      A       216.239.36.10
ns2.google.com.         257322  IN      A       216.239.34.10
ns1.google.com.         257322  IN      A       216.239.32.10

;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:34:02 IST 2024
;; MSG SIZE  rcvd: 191
```

IP Address- 142.250.71.14
TTL- 234 s
Query Time- 7 ms
Additional Information- NS records for Google's name servers (e.g., ns1.google.com, ns2.google.com, etc.), each with their own A records and high TTL values is 257322 s.



```
gh1@gh1-Aspire-A715-75G:~$ dig AAAA google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> AAAA google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44795
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      AAAA

;; ADDITIONAL SECTION:
ns4.google.com.         257248  IN      A       216.239.38.10
ns3.google.com.         257248  IN      A       216.239.36.10
ns2.google.com.         257248  IN      A       216.239.34.10
ns1.google.com.         257248  IN      A       216.239.32.10

;; Query time: 6 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:35:16 IST 2024
;; MSG SIZE  rcvd: 119
```

IP Address- No AAAA record in the answer section here
Query Time- 6 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig MX google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> MX google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30540
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             300     IN      MX      10 smtp.google.com.

;; AUTHORITY SECTION:
google.com.             83292   IN      NS      ns3.google.com.
google.com.             83292   IN      NS      ns1.google.com.
google.com.             83292   IN      NS      ns2.google.com.
google.com.             83292   IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        300     IN      A       142.251.12.26
smtp.google.com.        300     IN      A       142.251.12.27
smtp.google.com.        300     IN      A       172.253.118.26
smtp.google.com.        300     IN      A       172.253.118.27
smtp.google.com.        300     IN      A       74.125.200.27
ns4.google.com.         257229  IN      A       216.239.38.10
ns3.google.com.         257229  IN      A       216.239.36.10
ns2.google.com.         257229  IN      A       216.239.34.10
ns1.google.com.         257229  IN      A       216.239.32.10

;; Query time: 60 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:35:35 IST 2024
;; MSG SIZE  rcvd: 276
```

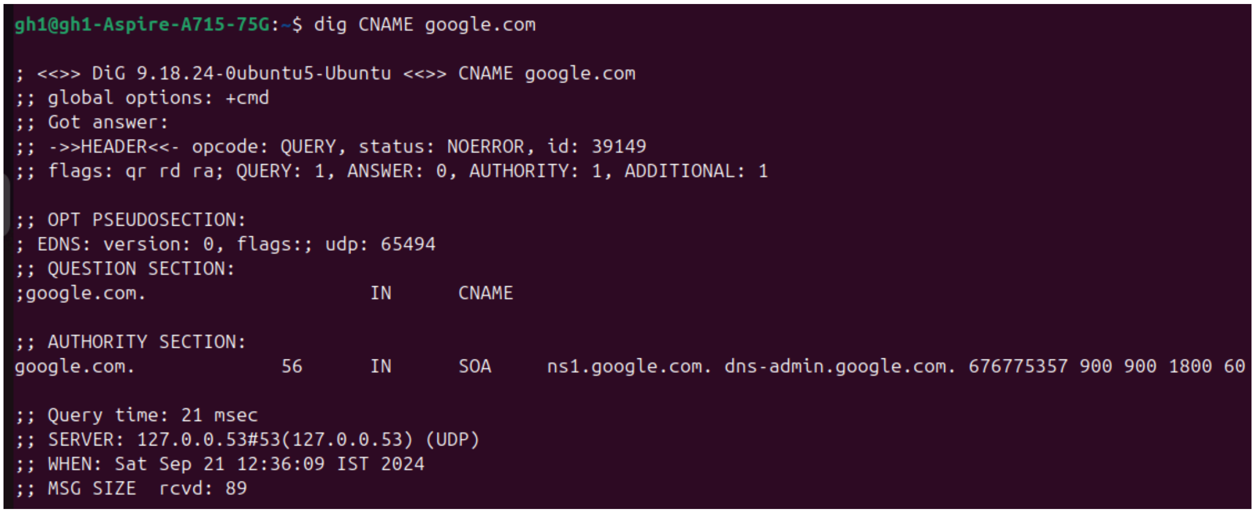
Mail Exchange - smtp.google.com

Priority- 10

TTL- 300 s

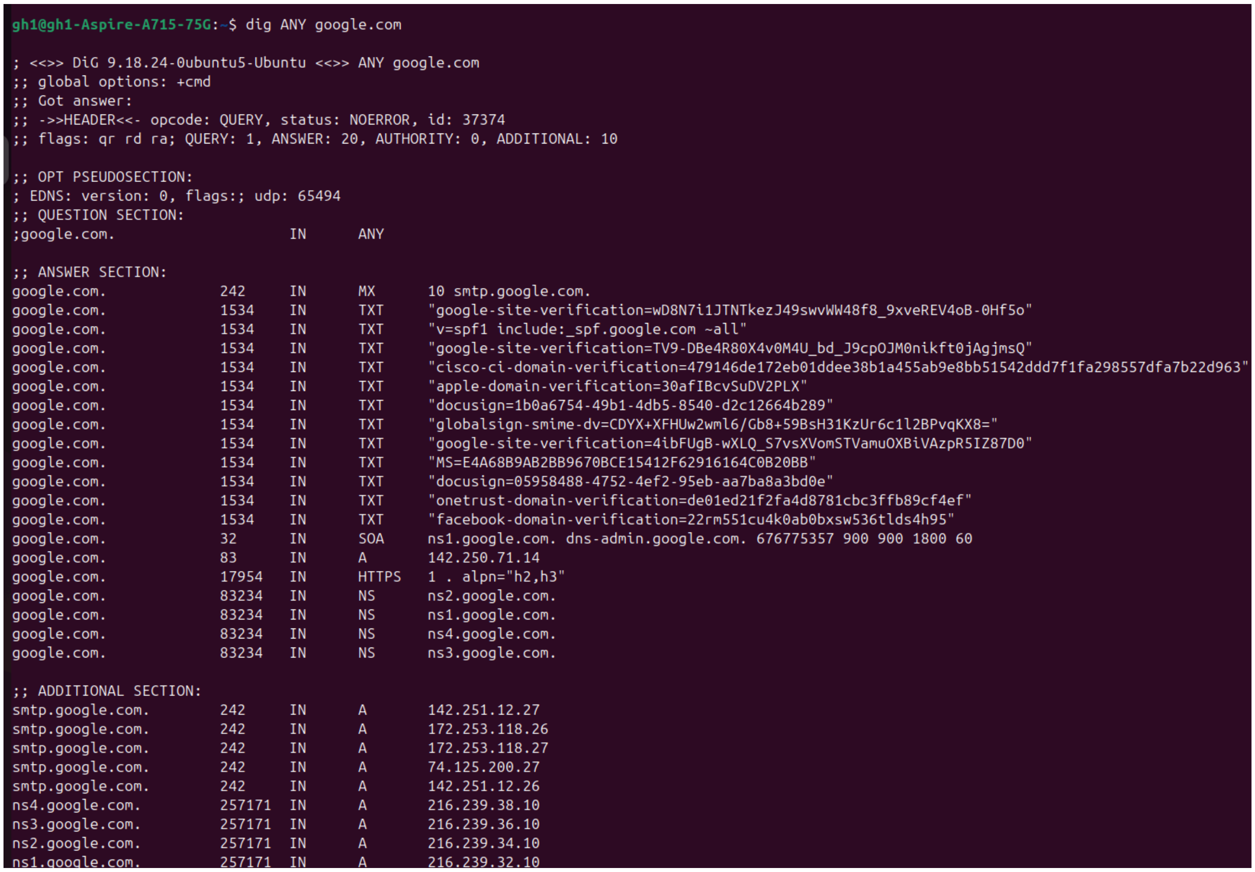
Additional- Multiple A records for smtp.google.com with the following IPs: 142.251.12.26, 172.253.118.26, 74.125.200.27, etc.

Query Time- 60 ms.



```
gh1@gh1-Aspire-A715-75G:~$ dig CNAME google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> CNAME google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39149
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      CNAME

;; AUTHORITY SECTION:
google.com.             56      IN      SOA     ns1.google.com. dns-admin.google.com. 676775357 900 900 1800 60

;; Query time: 21 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:36:09 IST 2024
;; MSG SIZE  rcvd: 89
```

CNAME- No CNAME found here
TTL- 56 s
Query Time- 21 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig ANY google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> ANY google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37374
;; flags: qr rd ra; QUERY: 1, ANSWER: 20, AUTHORITY: 0, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             242     IN      MX      10 smtp.google.com.
google.com.             1534    IN      TXT     "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com.             1534    IN      TXT     "v=spf1 include:_spf.google.com ~all"
google.com.             1534    IN      TXT     "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com.             1534    IN      TXT     "cisco-ci-domain-verification=479146de172eb01ddee38b1a455ab9e8bb51542ddd7f1fa298557dfa7b22d963"
google.com.             1534    IN      TXT     "apple-domain-verification=30afIBcvSuDV2PLX"
google.com.             1534    IN      TXT     "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com.             1534    IN      TXT     "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com.             1534    IN      TXT     "google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0"
google.com.             1534    IN      TXT     "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com.             1534    IN      TXT     "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com.             1534    IN      TXT     "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
google.com.             1534    IN      TXT     "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com.             32      IN      SOA     ns1.google.com. dns-admin.google.com. 676775357 900 900 1800 60
google.com.             83      IN      A       142.250.71.14
google.com.             17954   IN      HTTPS   1 . alpn="h2,h3"
google.com.             83234   IN      NS      ns2.google.com.
google.com.             83234   IN      NS      ns1.google.com.
google.com.             83234   IN      NS      ns4.google.com.
google.com.             83234   IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        242     IN      A       142.251.12.27
smtp.google.com.        242     IN      A       172.253.118.26
smtp.google.com.        242     IN      A       172.253.118.27
smtp.google.com.        242     IN      A       74.125.200.27
smtp.google.com.        242     IN      A       142.251.12.26
ns4.google.com.         257171  IN      A       216.239.38.10
ns3.google.com.         257171  IN      A       216.239.36.10
ns2.google.com.         257171  IN      A       216.239.34.10
ns1.google.com.         257171  IN      A       216.239.32.10
```

MX Record- smtp.google.com

TXT Records- Several verification and SPF records.

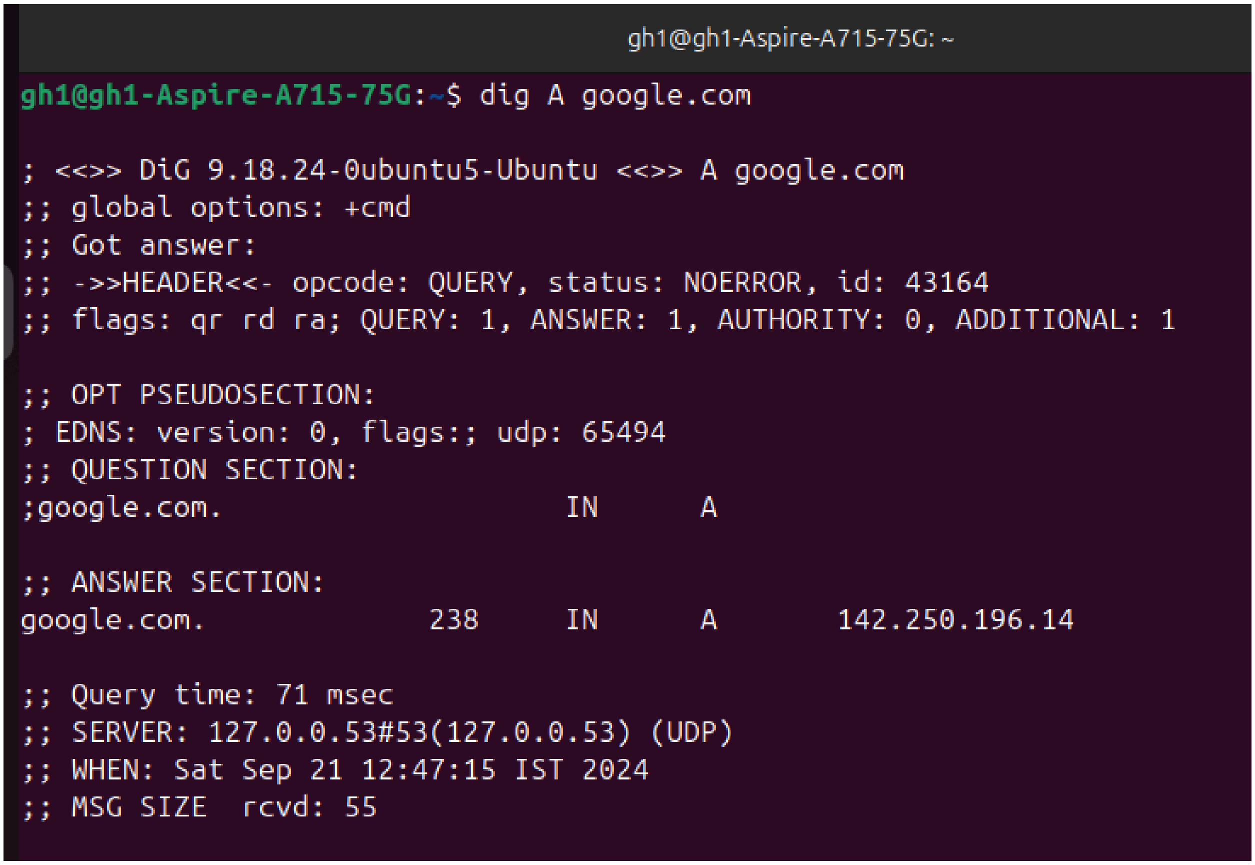
A Record- 142.250.71.14

NS Records- ns1.google.com, ns2.google.com, ns3.google.com, ns4.google.com

TTL- Varies, with the A record at 83 s and others going up to 83234 s

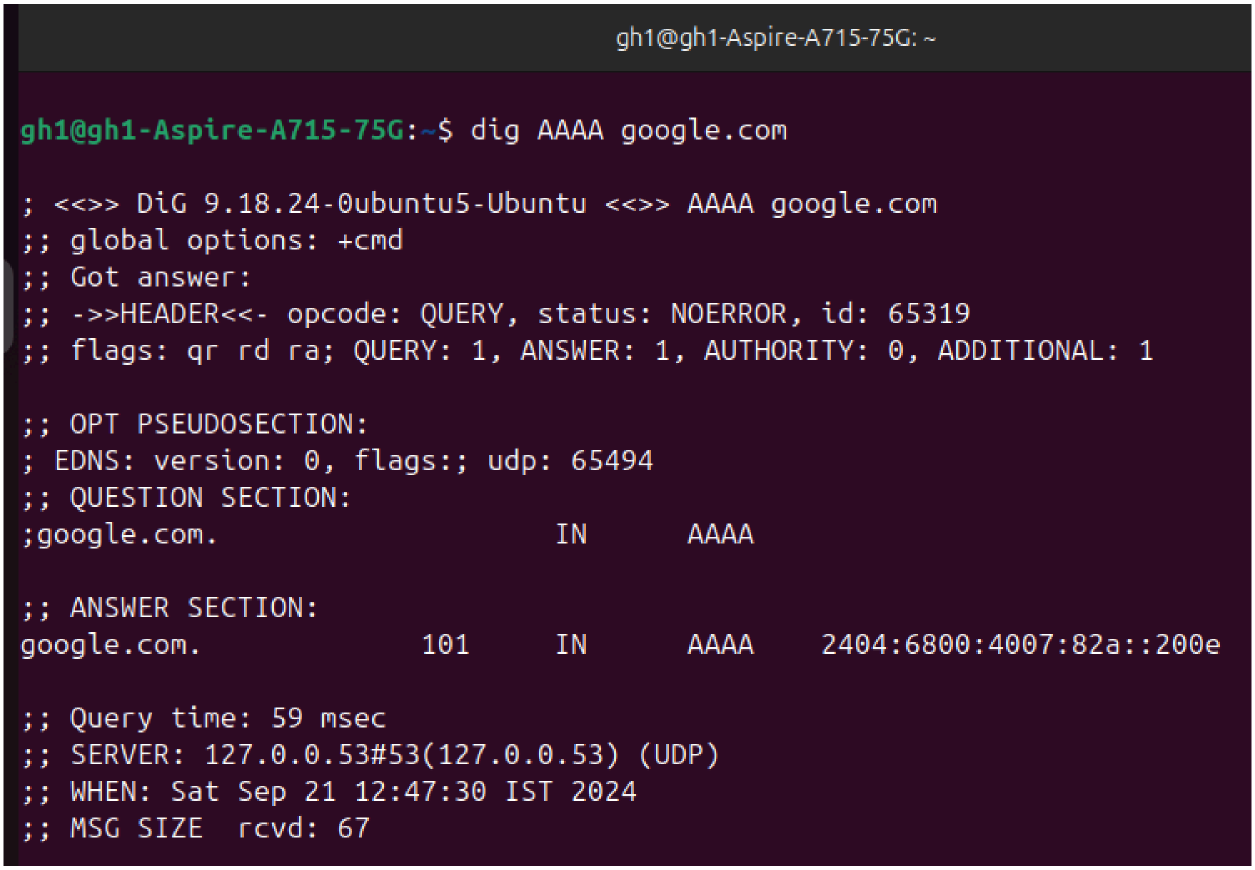
Query Time- 6 ms

b) Mobile network



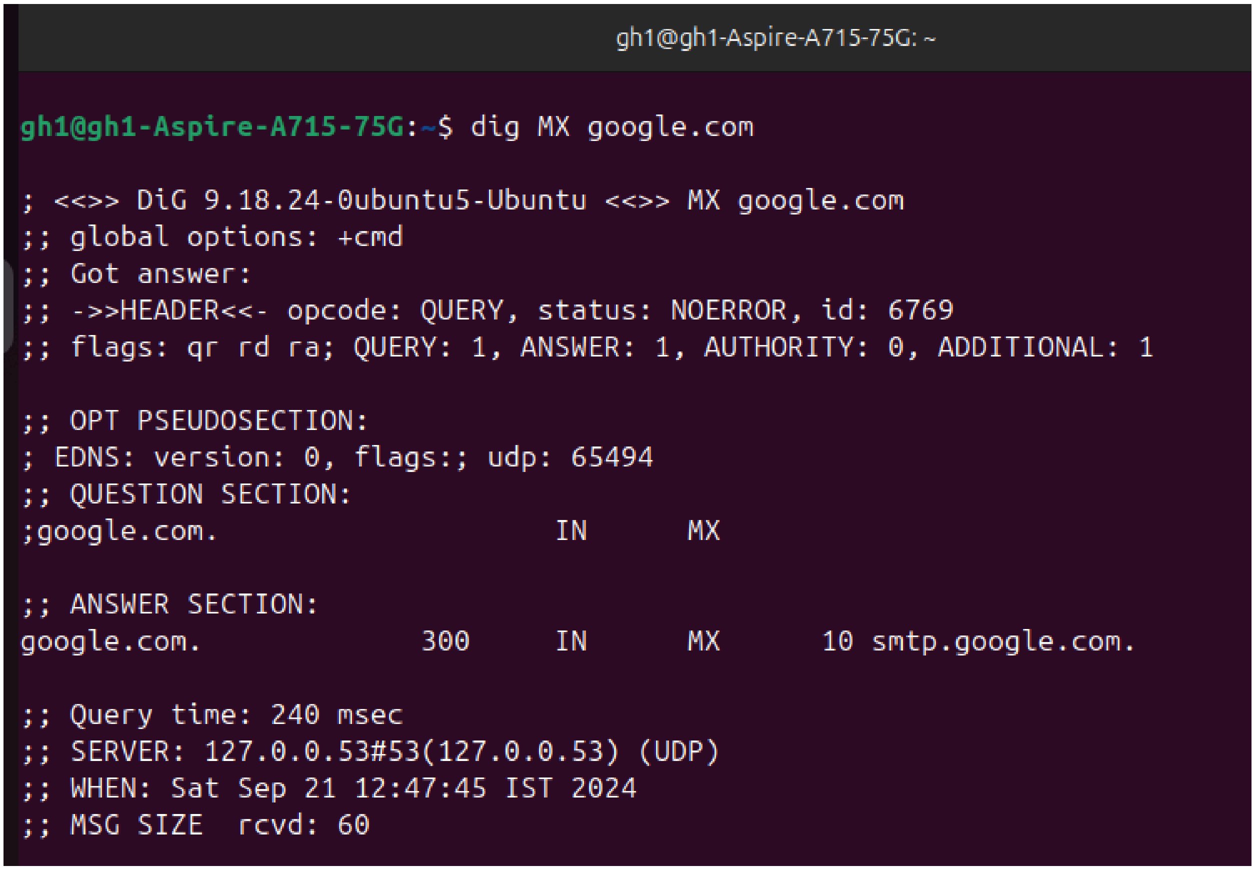
```
gh1@gh1-Aspire-A715-75G:~$ dig A google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> A google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43164
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             238     IN      A       142.250.196.14

;; Query time: 71 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:47:15 IST 2024
;; MSG SIZE  rcvd: 55
```

IP Address- 142.250.196.14
TTL- 238 s
Query Time- 71 ms



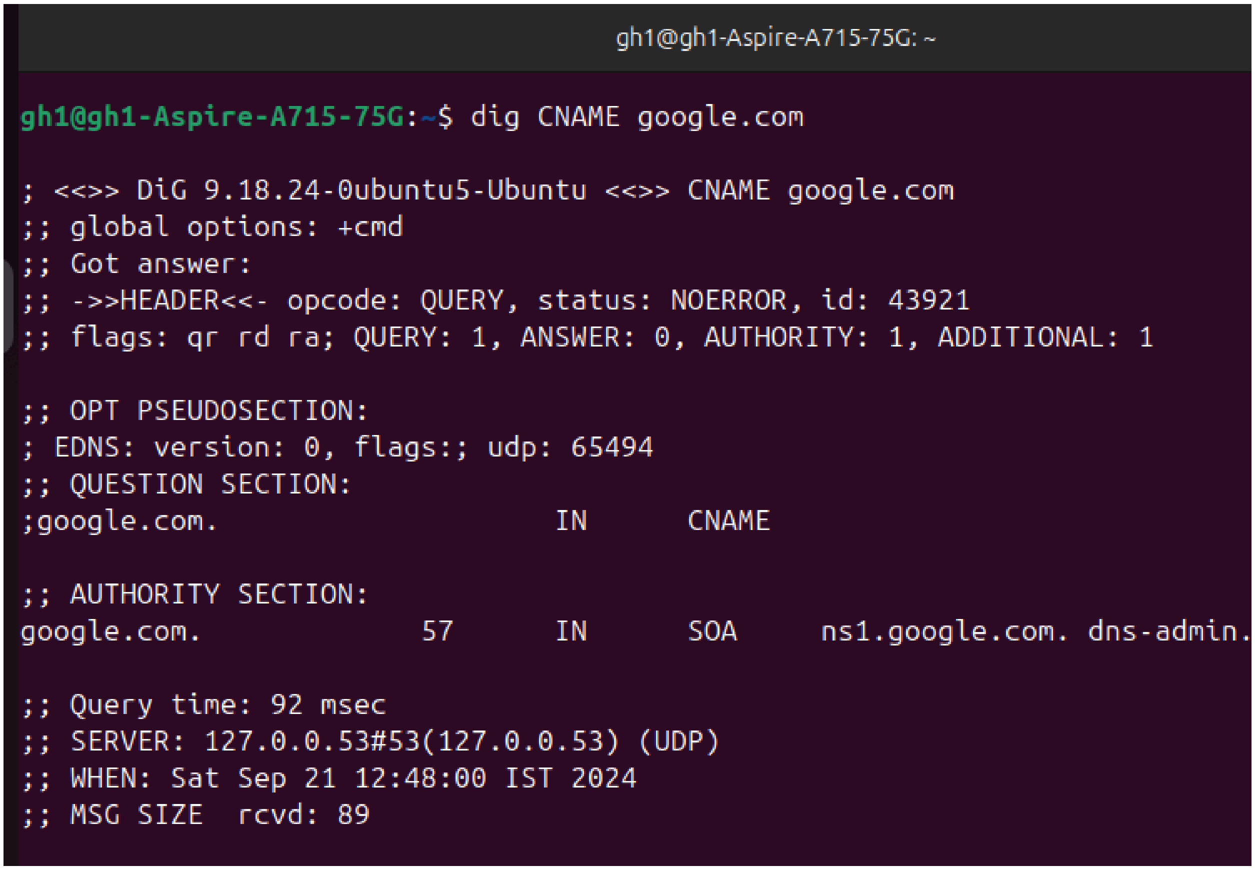
```
gh1@gh1-Aspire-A715-75G:~$ dig AAAA google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> AAAA google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65319
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      AAAA

;; ANSWER SECTION:
google.com.             101     IN      AAAA    2404:6800:4007:82a::200e

;; Query time: 59 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:47:30 IST 2024
;; MSG SIZE  rcvd: 67
```

IP Address- 2404:6800:4007:82a::200e
TTL- 101 s
Query Time- 59 ms



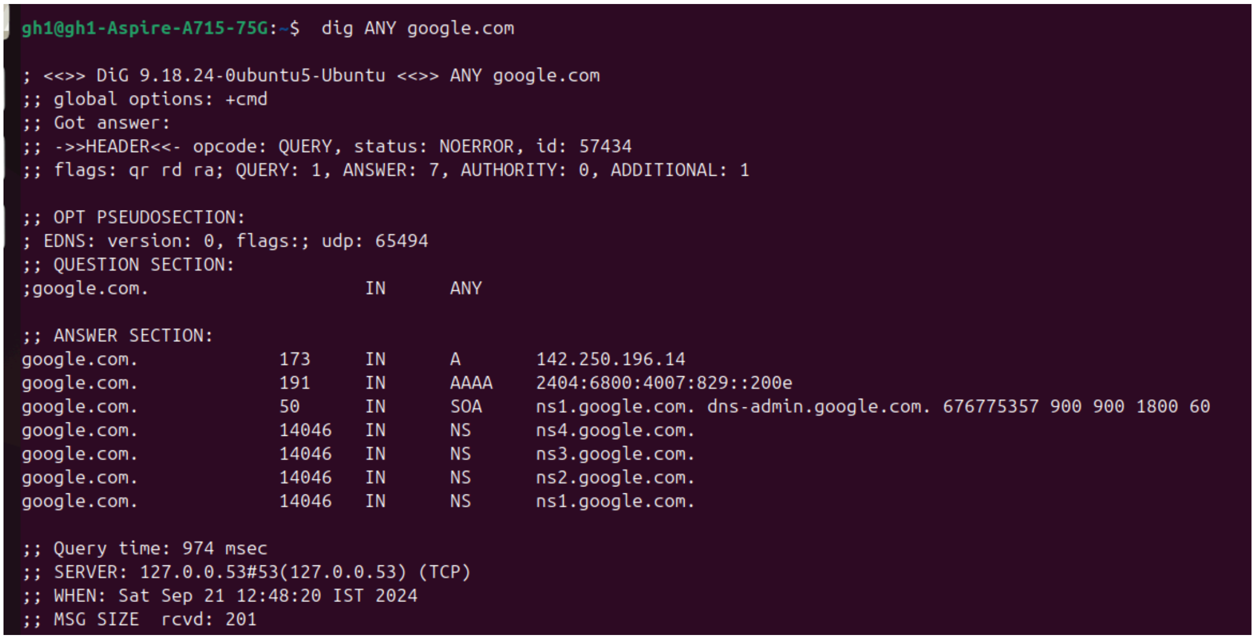
```
gh1@gh1-Aspire-A715-75G:~$ dig MX google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> MX google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6769
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             300     IN      MX      10 smtp.google.com.

;; Query time: 240 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:47:45 IST 2024
;; MSG SIZE  rcvd: 60
```

Mail Exchange (MX)- smtp.google.com
Priority- 10
TTL- 300 s
Query Time- 240 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig CNAME google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> CNAME google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43921
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      CNAME

;; AUTHORITY SECTION:
google.com.             57      IN      SOA     ns1.google.com. dns-admin.

;; Query time: 92 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:48:00 IST 2024
;; MSG SIZE  rcvd: 89
```

CNAME- No CNAME found.
TTL- 57 s
Query Time- 92 ms



```
gh1@gh1-Aspire-A715-75G:~$  dig ANY google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> ANY google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57434
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             173     IN      A       142.250.196.14
google.com.             191     IN      AAAA    2404:6800:4007:829::200e
google.com.             50      IN      SOA     ns1.google.com. dns-admin.google.com. 676775357 900 900 1800 60
google.com.             14046   IN      NS      ns4.google.com.
google.com.             14046   IN      NS      ns3.google.com.
google.com.             14046   IN      NS      ns2.google.com.
google.com.             14046   IN      NS      ns1.google.com.

;; Query time: 974 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Sat Sep 21 12:48:20 IST 2024
;; MSG SIZE  rcvd: 201
```

Various Records are obtained here-

- **A Record-** 142.250.196.14
- **AAAA Record-** 2404:6800:4007:829::200e
- **NS Records-** ns1.google.com, ns2.google.com, ns3.google.com, ns4.google.com
- **TTL-** The lowest is 50 seconds for the SOA, and the highest is 14046 seconds for the NS records.

Query Time: 974 ms

Analysis-

Lets see comparative analysis and other information for google.com-

1. A Record (IPv4)

A record is resolved to different IP addresses depending on network (Wi-Fi vs. mobile). This is due to the fact that Google's DNS infrastructure is geographically distributed. To direct users to the least congested server or nearest server based on their location and network, google employs geo-routing techniques and load balancing.

Wi-Fi resolves to 142.250.71.14.

Mobile resolves to 142.250.196.14, which is a different IP from the one resolved on Wi-Fi as observed. They both belong to address blocks of Google but they might correspond to different edge servers or data centers.

The query time for the mobile network is 71 ms which is significantly longer than Wi-Fi which is7 ms. This could be due to-

- Higher latency on mobile networks compared to wired or Wi-Fi networks.
- Network congestion or different routing paths.

2. AAAA Record (IPv6)

- On Wi-Fi, no IPv6 address was returned in above output which i got, but mobile network provided an IPv6 address 2404:6800:4007:82a::200e.
  - The adoption of IPv6 varies by network means different levels of support for IPv6 or some networks might have incomplete.
  - For handling growing device counts, IPv6 has been widely adopted in the mobile network design, hence mobile networks especially in certain regions, tend to have better adoption of IPv6 compared to older Wi-Fi.
  - Both IPv4 and IPv6 are supported by Google's services but version of IP returned depends on DNS resolver configurations and querying network.

- Query time for mobile network is 59 ms which is similar to the A record query which is 71 ms, which indicates stable performance.

3. MX Record (Mail Exchange)

- Both wifi and mobile network resolve to same mail exchange record, smtp.google.com, Wi-Fi network had provided additional A records associated with smtp.google.com, whereas mobile network did not provided that. This indicates differences in resolver behavior, where we can observe Wi-Fi resolver pre-fetches more information compared to mobile network.
- Query time is slower on the mobile network which is 240 ms, which indicates resolver delays or network performance limitations.

4. CNAME Record

- Instead of providing a CNAME record, both networks wifi and mobile network had provided an SOA record instead of a CNAME record. This is because google.com is not an alias for another domain, it is root domain, meaning it owns its own authoritative DNS configuration.

5. ANY Query

- ANY query on Wi-Fi returned more records, which includs TXT and HTTPS records. This shows that the Wi-Fi network resolver is more complete in delivering additional information and pre-fetching.
- The mobile network query returned fewer records compared to Wi-Fi and took much longer (974 ms vs. 6 ms on Wi-Fi). This is due to caching differences, resolver configuration,network limitations.
- The higher query time on the mobile network indicates possible inefficiency or latency in DNS resolution chain.

Key Differences Between Wi-Fi and Mobile Networks

1. **IP Address Assignment**:
   - Each network returned different IPv4 addresses. This shows that Google uses anycast to route traffic to least congested data center or the nearest or depending on the user's network. Both IP addresses belong to Google only but they may represent different physical locations.
   - Mobile network also returned an IPv6 address, but Wi-Fi does not. This indicates better IPv6 adoption on the mobile network.
2. **DNS Record Results**:

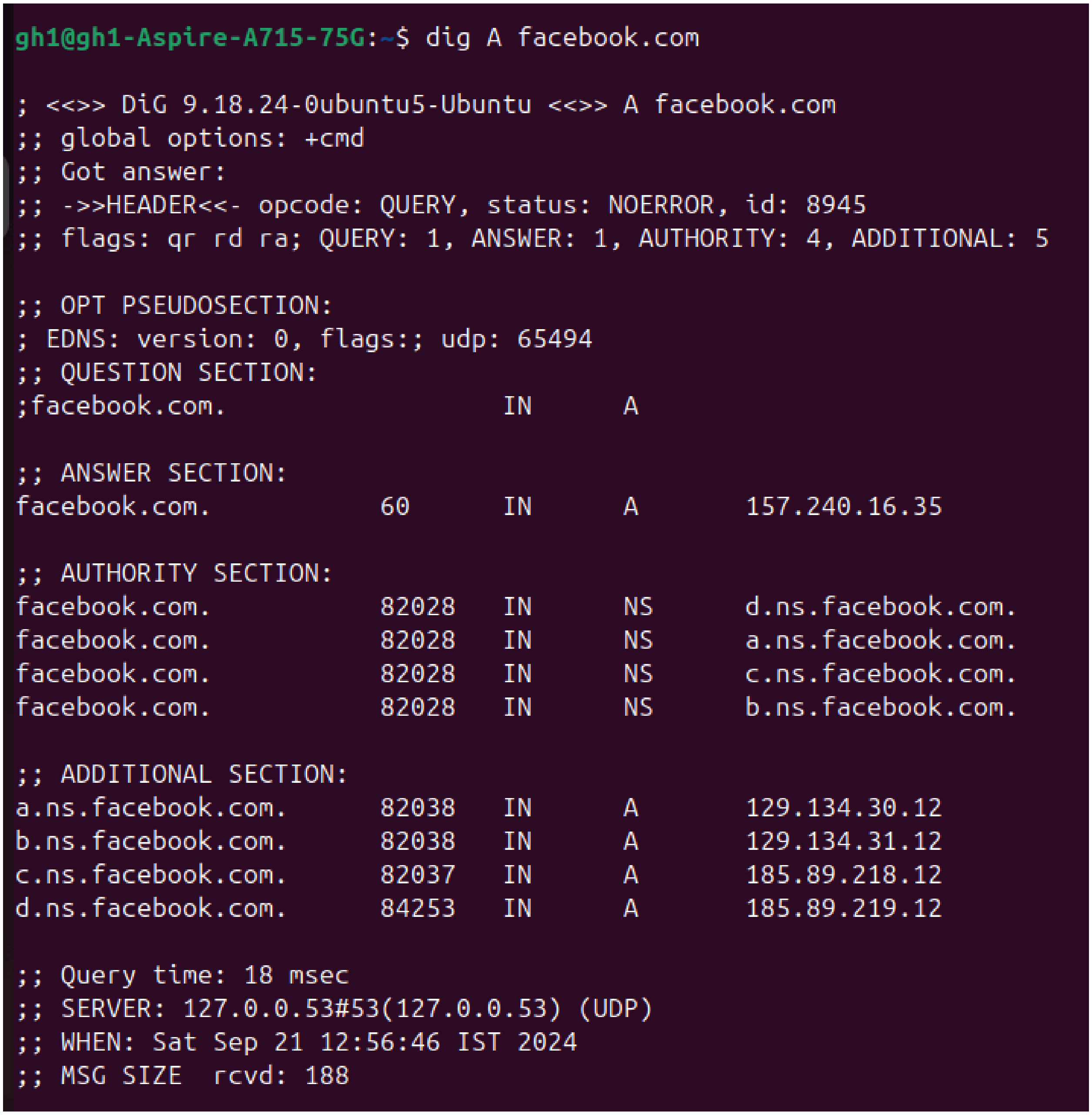
    - For MX and ANY queries, the mobile network had returned fewer details compared to Wi-Fi network. This indicates that the mobile DNS resolver is optimized for lightweight responses or performs fewer lookups .
    - As observed Wi-Fi responses were more complete (e.g., i got additional A records for MX queries, more TXT records for ANY queries).
3. **Query Time**:
    - Much faster query times across all DNS record types is observed in Wi-Fi consistently. For example, the A record lookup took 7 ms on Wi-Fi but 71 ms on mobile.
    - The mobile network experienced significantly higher latency, especially in the ANY query which is 974 ms, which indicates network is congested, additional routing overheads or slower DNS resolver.

Conclusion-

The difference in query results between the mobile network and Wi-Fi reflects impact of network architecture and Google's load-balancing infrastructure DNS resolver behavior. As observed mobile networks generally face higher latency, and the DNS resolvers may be configured to minimize data transfer hence fewer additional records. On the other hand, Wi-Fi network benefits from more detailed DNS response and lower latency.

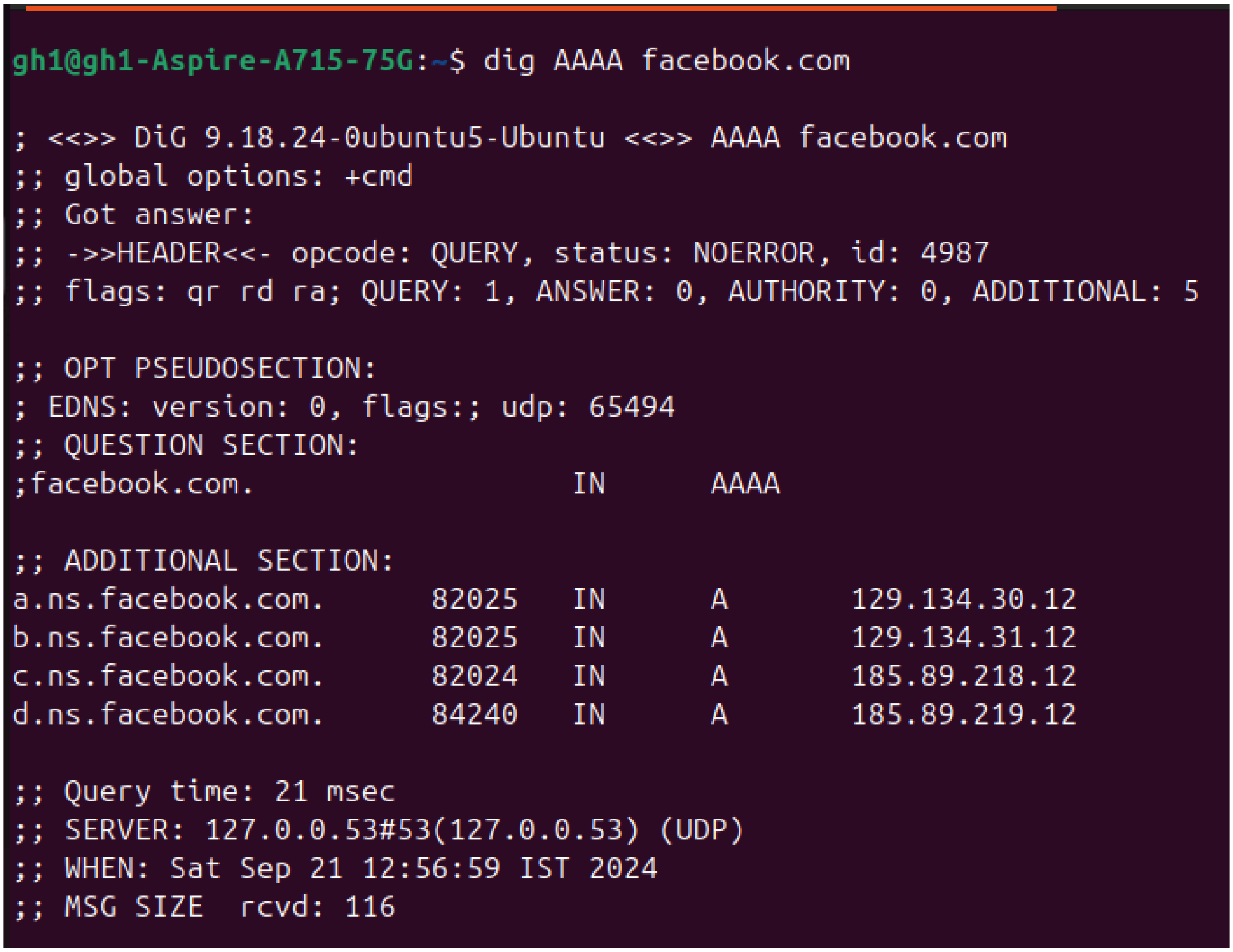
2) For Facebook.com

a) Wi-Fi



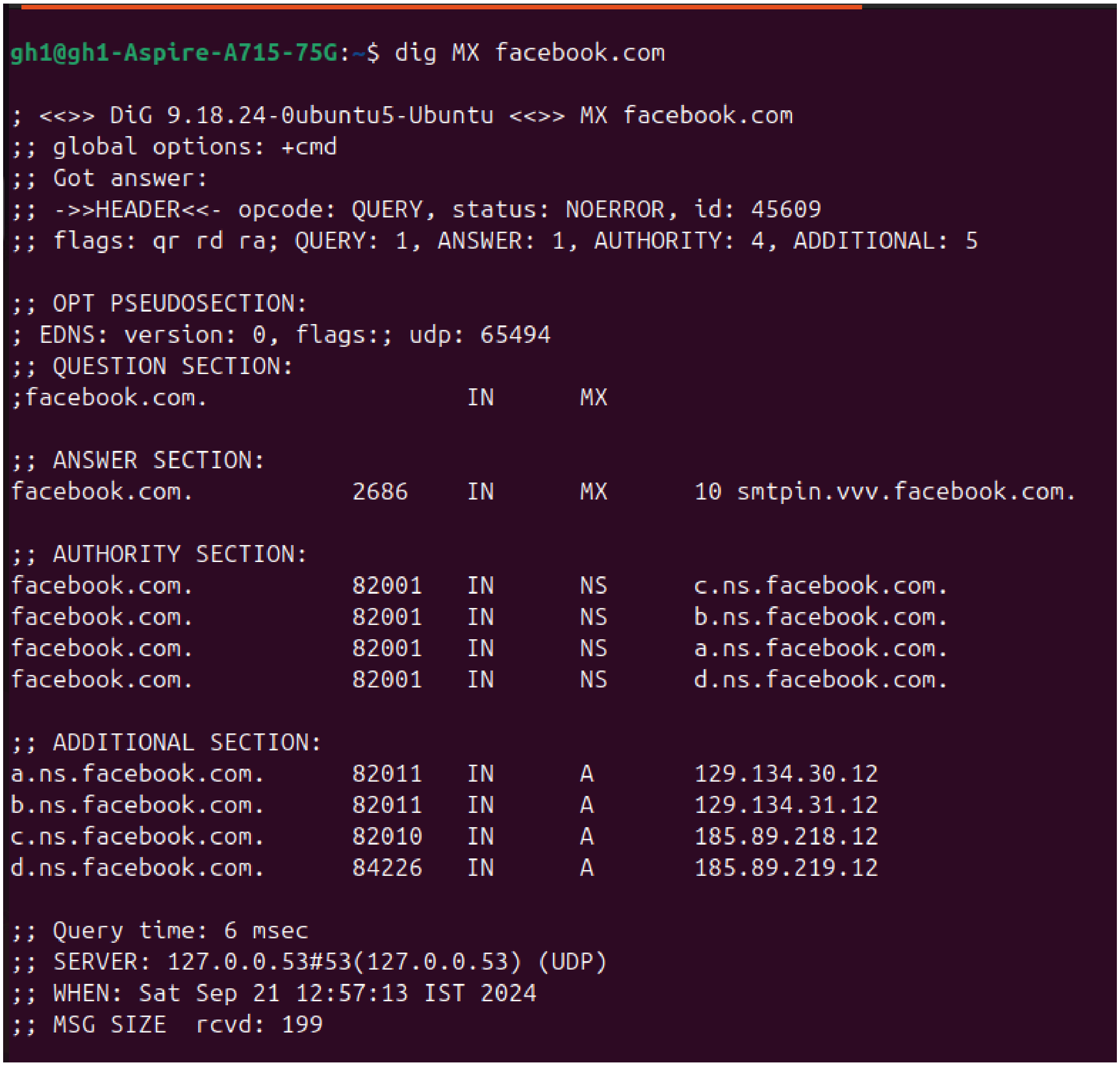
```
gh1@gh1-Aspire-A715-75G:~$ dig A facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> A facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8945
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      A

;; ANSWER SECTION:
facebook.com.           60      IN      A       157.240.16.35

;; AUTHORITY SECTION:
facebook.com.           82028   IN      NS      d.ns.facebook.com.
facebook.com.           82028   IN      NS      a.ns.facebook.com.
facebook.com.           82028   IN      NS      c.ns.facebook.com.
facebook.com.           82028   IN      NS      b.ns.facebook.com.

;; ADDITIONAL SECTION:
a.ns.facebook.com.      82038   IN      A       129.134.30.12
b.ns.facebook.com.      82038   IN      A       129.134.31.12
c.ns.facebook.com.      82037   IN      A       185.89.218.12
d.ns.facebook.com.      84253   IN      A       185.89.219.12

;; Query time: 18 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:56:46 IST 2024
;; MSG SIZE  rcvd: 188
```

- **IP Address-** 157.240.16.35
- **TTL-** 60 s
- **Query Time-** 18 ms



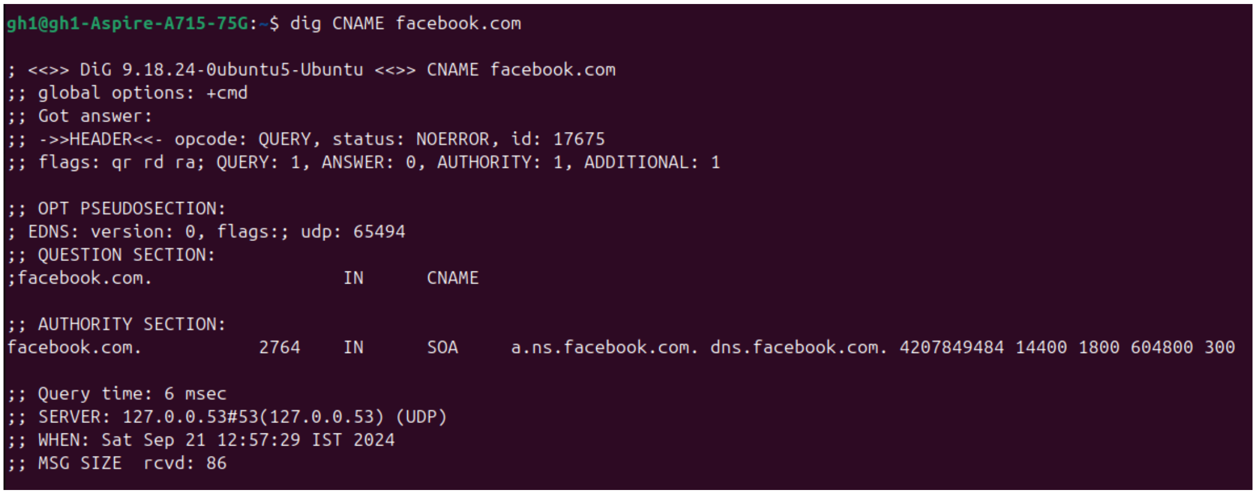
```
gh1@gh1-Aspire-A715-75G:~$ dig AAAA facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> AAAA facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4987
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      AAAA

;; ADDITIONAL SECTION:
a.ns.facebook.com.      82025   IN      A       129.134.30.12
b.ns.facebook.com.      82025   IN      A       129.134.31.12
c.ns.facebook.com.      82024   IN      A       185.89.218.12
d.ns.facebook.com.      84240   IN      A       185.89.219.12

;; Query time: 21 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:56:59 IST 2024
;; MSG SIZE  rcvd: 116
```

- **IPv6 Address-** No record returned here
- **Query Time-** 21 ms



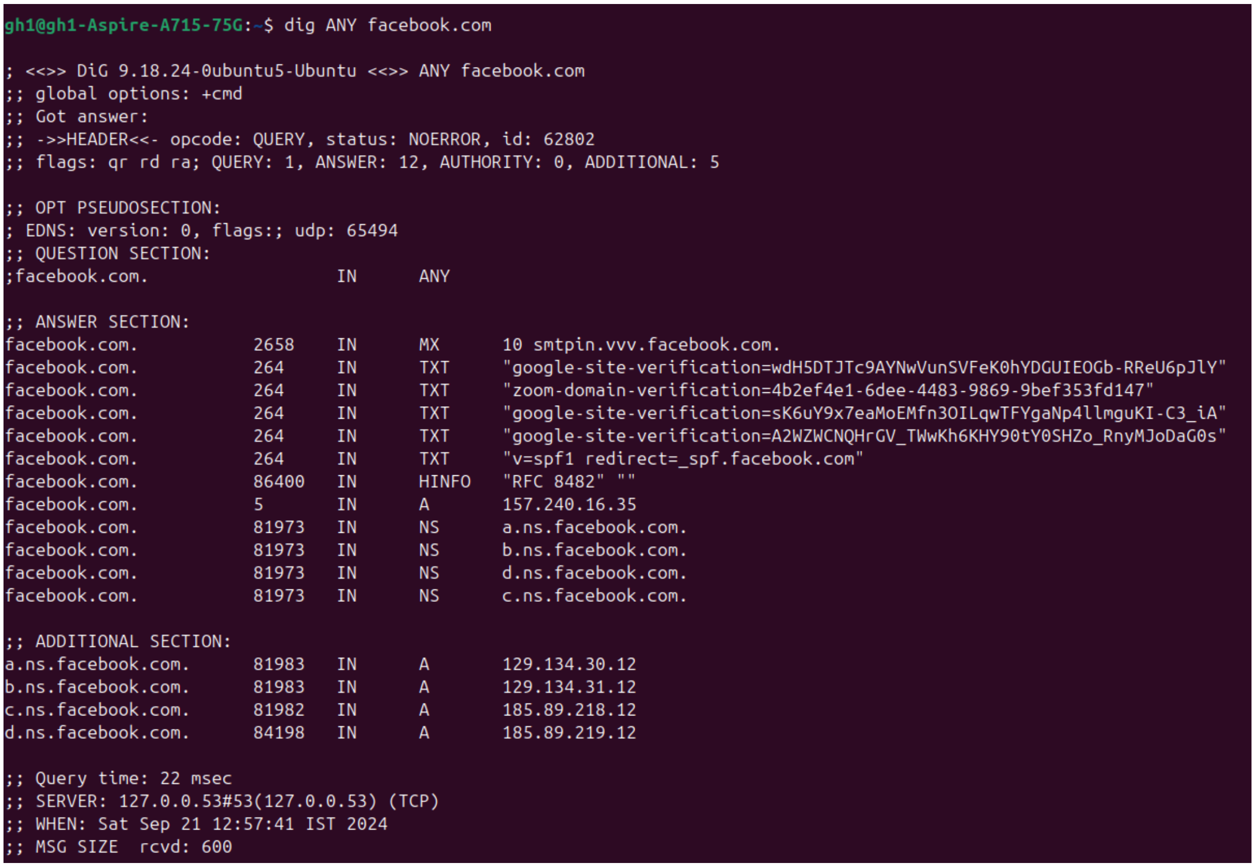
```
gh1@gh1-Aspire-A715-75G:~$ dig MX facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> MX facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45609
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      MX

;; ANSWER SECTION:
facebook.com.           2686    IN      MX      10 smtpin.vvv.facebook.com.

;; AUTHORITY SECTION:
facebook.com.           82001   IN      NS      c.ns.facebook.com.
facebook.com.           82001   IN      NS      b.ns.facebook.com.
facebook.com.           82001   IN      NS      a.ns.facebook.com.
facebook.com.           82001   IN      NS      d.ns.facebook.com.

;; ADDITIONAL SECTION:
a.ns.facebook.com.      82011   IN      A       129.134.30.12
b.ns.facebook.com.      82011   IN      A       129.134.31.12
c.ns.facebook.com.      82010   IN      A       185.89.218.12
d.ns.facebook.com.      84226   IN      A       185.89.219.12

;; Query time: 6 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:57:13 IST 2024
;; MSG SIZE  rcvd: 199
```

- **MX Record-** smtpin.vvv.facebook.com
- **Priority-** 10
- **TTL:**-2686 s
- **Query Time-** 6 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig CNAME facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> CNAME facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17675
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      CNAME

;; AUTHORITY SECTION:
facebook.com.           2764    IN      SOA     a.ns.facebook.com. dns.facebook.com. 4207849484 14400 1800 604800 300

;; Query time: 6 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 12:57:29 IST 2024
;; MSG SIZE  rcvd: 86
```

- **CNAME Record-** No record returned here
- **Query Time-** 6 ms

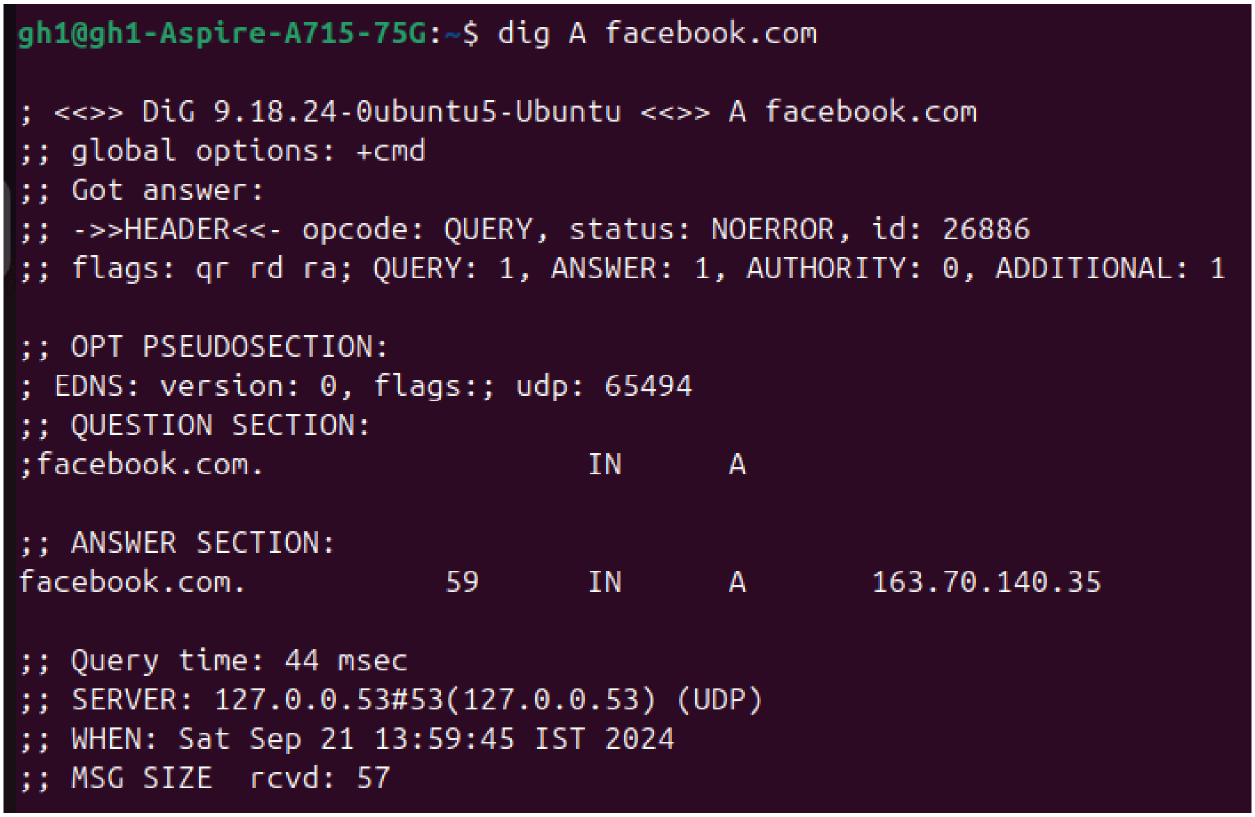


```
gh1@gh1-Aspire-A715-75G:~$ dig ANY facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> ANY facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62802
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      ANY

;; ANSWER SECTION:
facebook.com.           2658    IN      MX      10 smtpin.vvv.facebook.com.
facebook.com.           264     IN      TXT     "google-site-verification=wdH5DTJTc9AYNwVunSVFeK0hYDGUIEOGb-RReU6pJlY"
facebook.com.           264     IN      TXT     "zoom-domain-verification=4b2ef4e1-6dee-4483-9869-9bef353fd147"
facebook.com.           264     IN      TXT     "google-site-verification=sK6uY9x7eaMoEMfn3OILqwTFYgaNp4llmguKI-C3_iA"
facebook.com.           264     IN      TXT     "google-site-verification=A2WZWCNQHrGV_TWwKh6KHY90tY0SHZo_RnyMJoDaG0s"
facebook.com.           264     IN      TXT     "v=spf1 redirect=_spf.facebook.com"
facebook.com.           86400   IN      HINFO   "RFC 8482" ""
facebook.com.           5       IN      A       157.240.16.35
facebook.com.           81973   IN      NS      a.ns.facebook.com.
facebook.com.           81973   IN      NS      b.ns.facebook.com.
facebook.com.           81973   IN      NS      d.ns.facebook.com.
facebook.com.           81973   IN      NS      c.ns.facebook.com.

;; ADDITIONAL SECTION:
a.ns.facebook.com.      81983   IN      A       129.134.30.12
b.ns.facebook.com.      81983   IN      A       129.134.31.12
c.ns.facebook.com.      81982   IN      A       185.89.218.12
d.ns.facebook.com.      84198   IN      A       185.89.219.12

;; Query time: 22 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Sat Sep 21 12:57:41 IST 2024
;; MSG SIZE  rcvd: 600
```

- **Returned Records-**

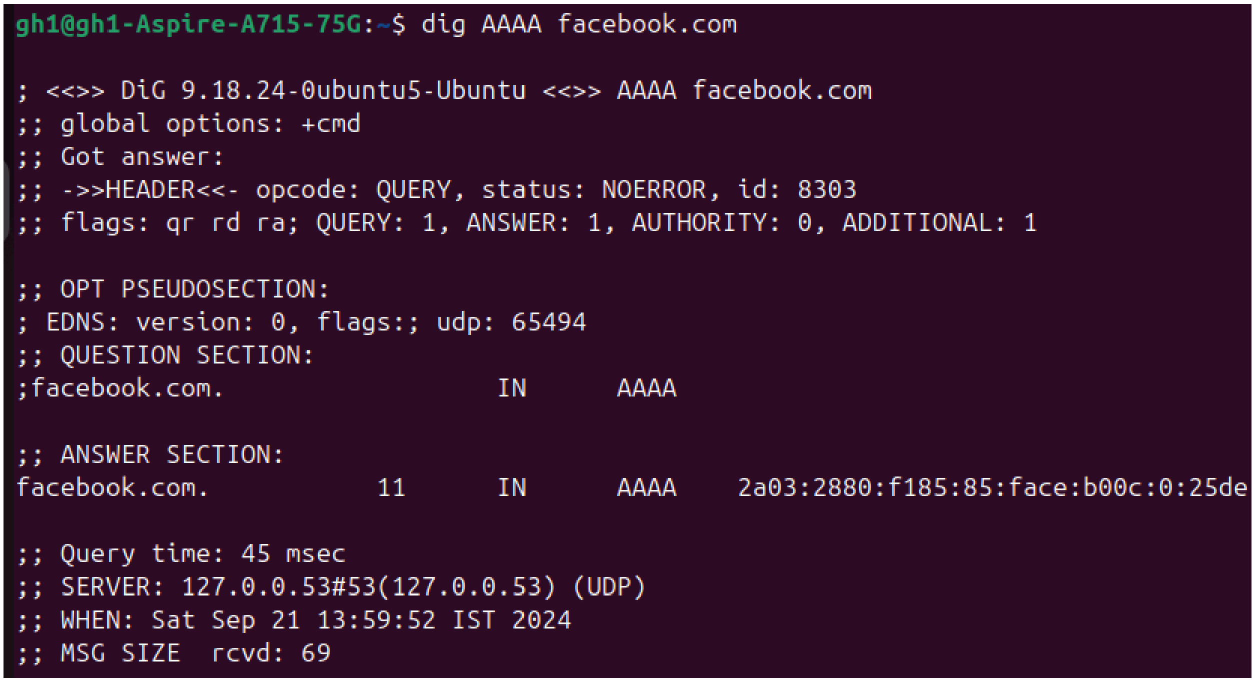
    - **MX Record-** smtpin.vvv.facebook.com (Priority: 10, TTL: 2658 s)
    - **TXT Records-** Various verifications (TTL: 264 s each)
    - **A Record-** 157.240.16.35 (TTL: 2658 s)
    - **NS Records-** a.ns.facebook.com, b.ns.facebook.com, c.ns.facebook.com, d.ns.facebook.com (TTL: 81973 s)
- **Query Time-** 22 ms

b)Mobile Network



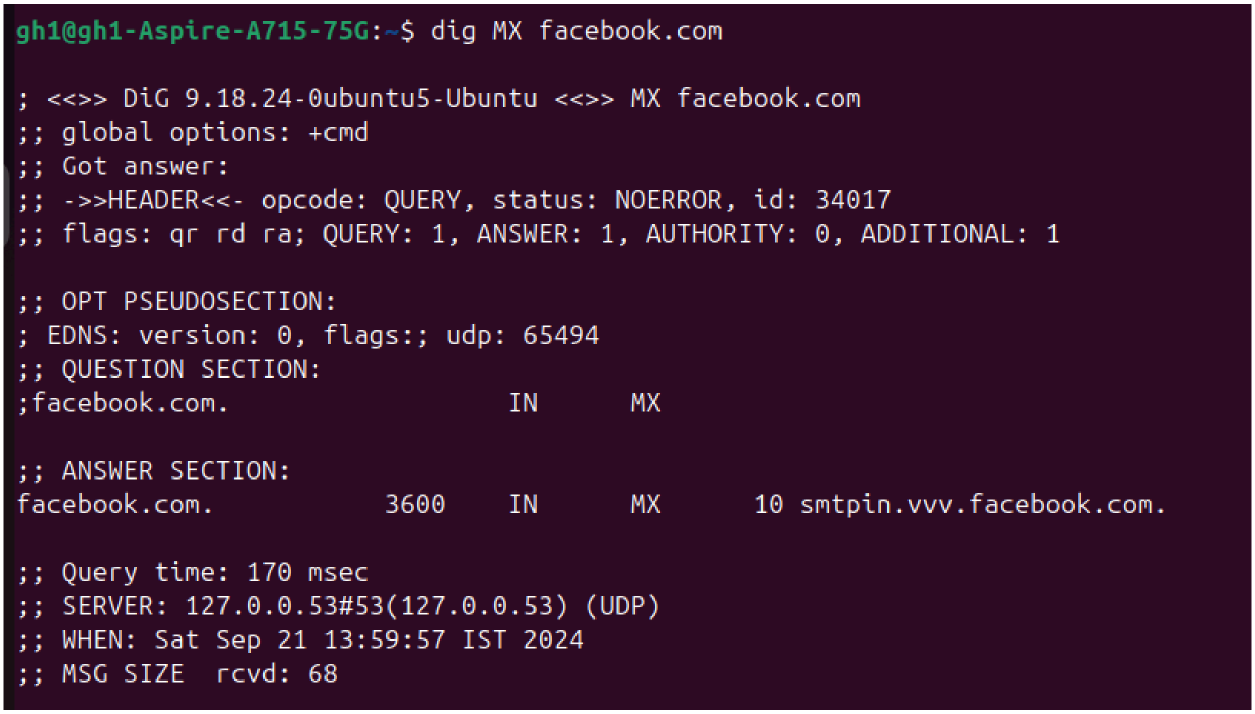
```
gh1@gh1-Aspire-A715-75G:~$ dig A facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> A facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26886
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      A

;; ANSWER SECTION:
facebook.com.           59      IN      A       163.70.140.35

;; Query time: 44 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 13:59:45 IST 2024
;; MSG SIZE  rcvd: 57
```

- **IP Address-** 163.70.140.35
- **TTL-** 59 s
- **Query Time-** 44 ms



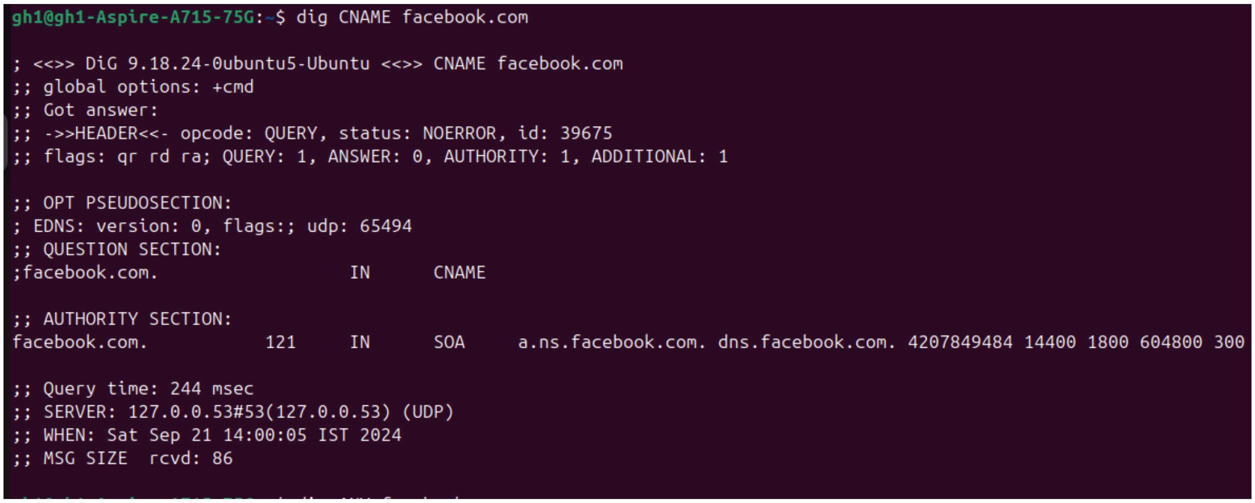
```
gh1@gh1-Aspire-A715-75G:~$ dig AAAA facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> AAAA facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8303
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      AAAA

;; ANSWER SECTION:
facebook.com.           11      IN      AAAA    2a03:2880:f185:85:face:b00c:0:25de

;; Query time: 45 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 13:59:52 IST 2024
;; MSG SIZE  rcvd: 69
```

- **IPv6 Address-** 2a03:2880:f185:85:face:b00c:0:25de
- **TTL-** 11 s
- **Query Time-** 45 ms



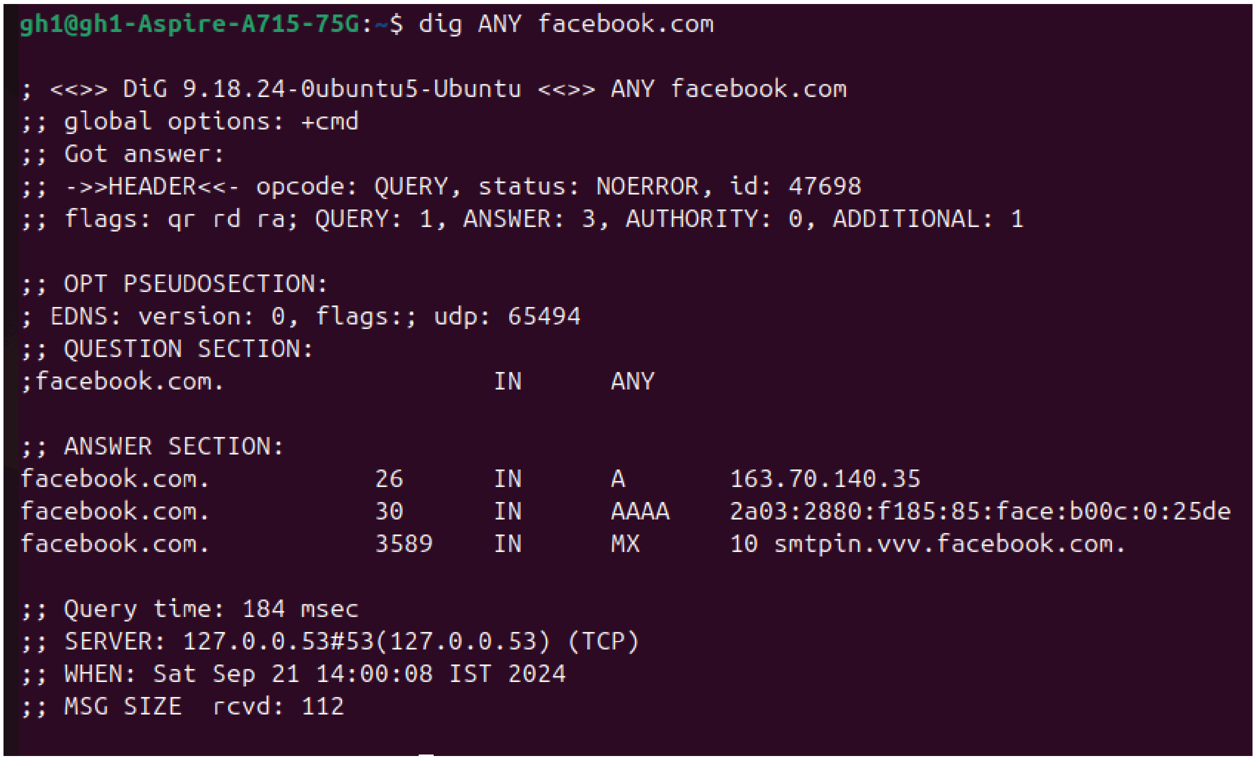
```
gh1@gh1-Aspire-A715-75G:~$ dig MX facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> MX facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34017
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      MX

;; ANSWER SECTION:
facebook.com.           3600    IN      MX      10 smtpin.vvv.facebook.com.

;; Query time: 170 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 13:59:57 IST 2024
;; MSG SIZE  rcvd: 68
```

- **MX Record-** smtpin.vvv.facebook.com
- **Priority-** 10
- **TTL-** 3600 s
- **Query Time-** 170 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig CNAME facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> CNAME facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39675
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      CNAME

;; AUTHORITY SECTION:
facebook.com.           121     IN      SOA     a.ns.facebook.com. dns.facebook.com. 4207849484 14400 1800 604800 300

;; Query time: 244 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:00:05 IST 2024
;; MSG SIZE  rcvd: 86
```

- **CNAME Record-** No record returned here
- **Query Time-** 244 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig ANY facebook.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> ANY facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47698
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN      ANY

;; ANSWER SECTION:
facebook.com.           26      IN      A       163.70.140.35
facebook.com.           30      IN      AAAA    2a03:2880:f185:85:face:b00c:0:25de
facebook.com.           3589    IN      MX      10 smtpin.vvv.facebook.com.

;; Query time: 184 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Sat Sep 21 14:00:08 IST 2024
;; MSG SIZE  rcvd: 112
```

- **Returned Records-**
  - **MX Record-** smtpin.vvv.facebook.com (Priority: 10, TTL: 3589 s)
  - **A Record-** 163.70.140.35 (TTL: 26s)
  - **AAAA Record-** `2a03:2880:f185:85:face:b00c:0:25de` (TTL: 30)
- **Query Time-** 184 ms

Analysis-

Lets see comparative analysis and other information for facebook.com-

1. A Record

- A record resolves to the different IP addresses depending upon network (Wi-Fi vs mobile), which can be attributed to distributed server infrastructure of Facebook.
- The TTL for both records is observed relatively short which indicating frequent updates in DNS records for reflecting changes in server availability.
- Query times are higher on mobile which is 44 ms compared to Wi-Fi which have 18 ms, suggesting increased latency in the mobile network.

2. AAAA Record

- The Wi-Fi network doesnt returned any IPv6 address but the mobile network provided a valid IPv6 address, which indicates support across networks or differing levels of IPv6 adoption.
- We can observe the TTL for the IPv6 address on mobile is shorter than typical values, which is reflecting rapid changes in server configurations.

3. MX Record (Mail Exchange)

- Both networks Wi-Fi and mobile network resolve to the same mail exchange record, smtpin.vvv.facebook.com having the same priority.
- The TTL on the mobile network is observed higher, which indicates changes to the mail server information are less frequent updates compared to Wi-Fi.
- The query time is observed slower on mobile which is 170 ms, which indicates network performance issues.

4. CNAME Record

- Neither of mobile network or Wi-Fi network had returned a CNAME record, which is expected as facebook.com is a root domain.
- The higher query time on mobile which is 244 ms which suggests network inefficiencies or delays.

5. ANY Query

- Compared to the mobile network, the ANY query on Wi-Fi returned more records which indicates better resolver behavior on Wi-Fi that pre-fetches additional information.
- The query time on mobile is higher which is 198 ms compared to Wi-Fi which is 22 ms, reflecting increased latency or potential inefficiencies in mobile DNS resolution process.

Key Differences Between Wi-Fi and Mobile Networks

1. **IP Address Assignment:**
    - Due to Facebook's load-balancing infrastructure, different IPv4 addresses were returned for each network.
    - The mobile network returned an IPv6 address, while the Wi-Fi network did not which reflects variations in IPv6 support.
2. **DNS Record Results:**
    - Compared to Wi-Fi the mobile network provided fewer details for the MX and ANY queries which indicate that the mobile DNS resolver is optimized for lightweight responses or may perform fewer lookups.
    - Wi-Fi responses were more complete, with additional A records and TXT records.
3. **Query Time:**

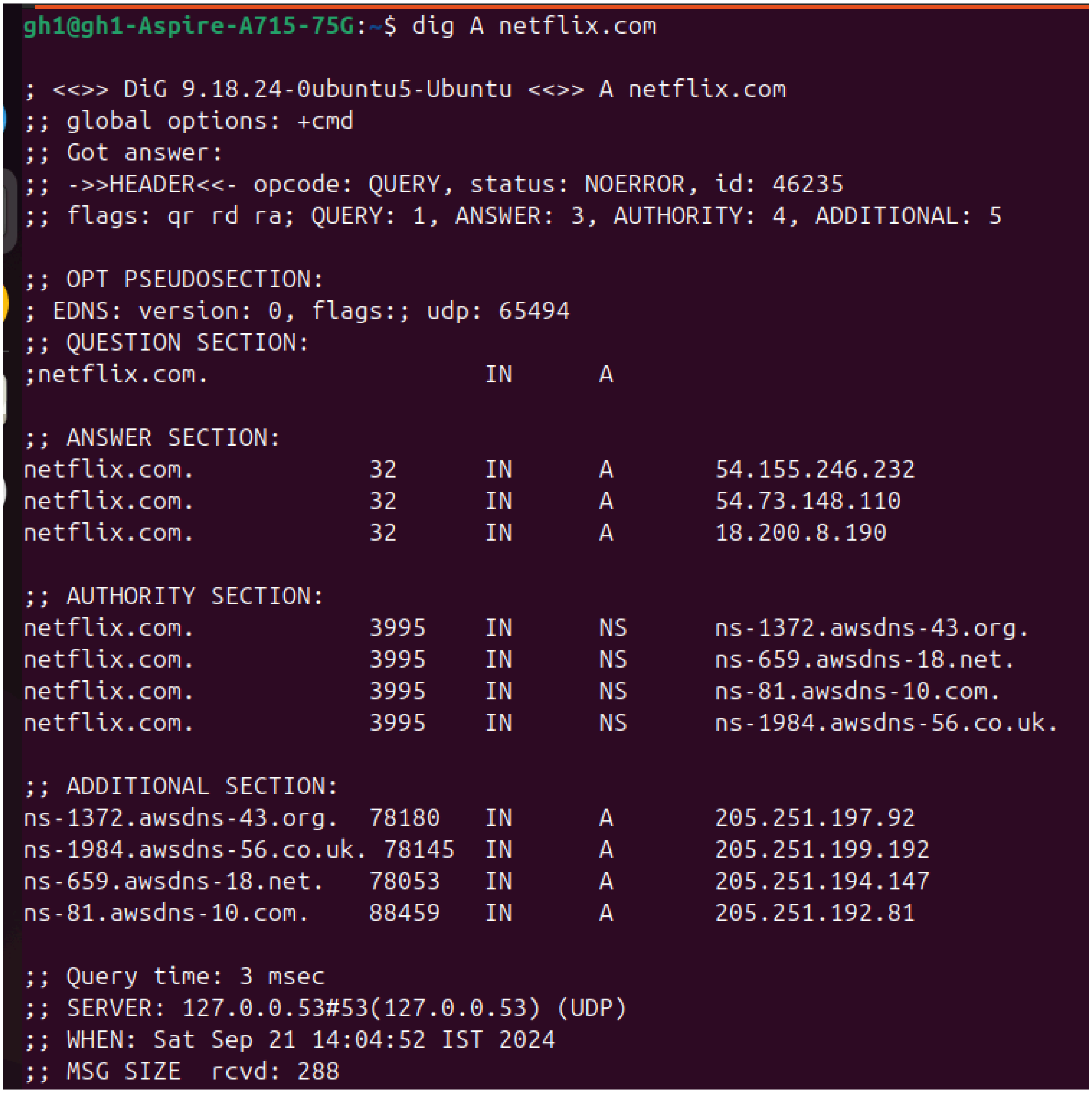
- Wi-Fi had consistently much faster query times across all the DNS record types. For example herem the A record lookup took 18 ms on Wi-Fi but 44 ms on mobile.
- The mobile network experienced higher latency, particularly for the ANY query which is 198 ms in that case, which indicates slower DNS resolution or network congestion.

Conclusion

Differences in DNS query results between the mobile networks and Wi-Fi shows the effects of DNS resolver behavior, network architecture and Facebook's infrastructure. Mobile networks generally face higher latency compared to Wi-Fi and their DNS resolvers may be configured to minimize data transfer. The Wi-Fi network have benefits of more comprehensive DNS responses and lower latency.

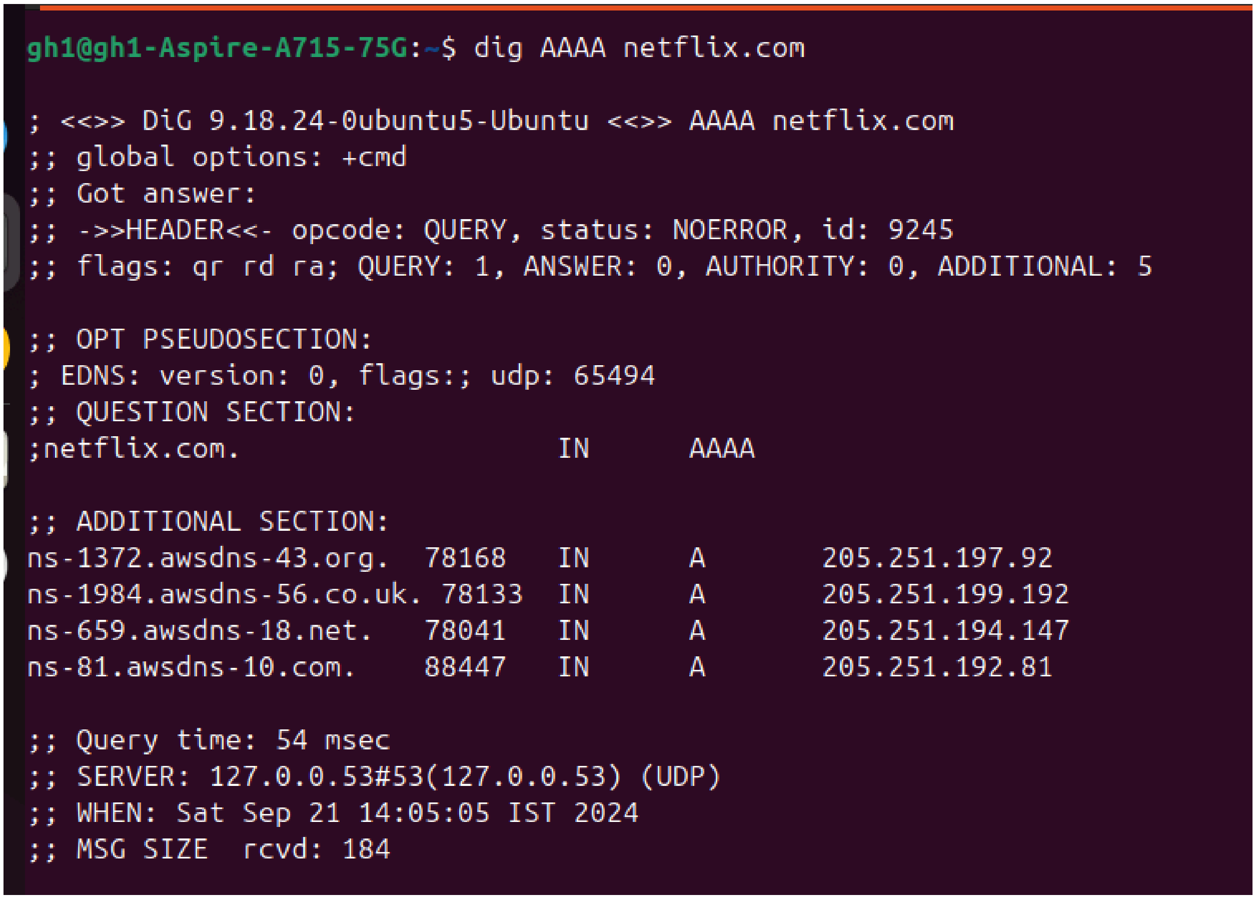
3) For netflix.com

a) Wi-Fi



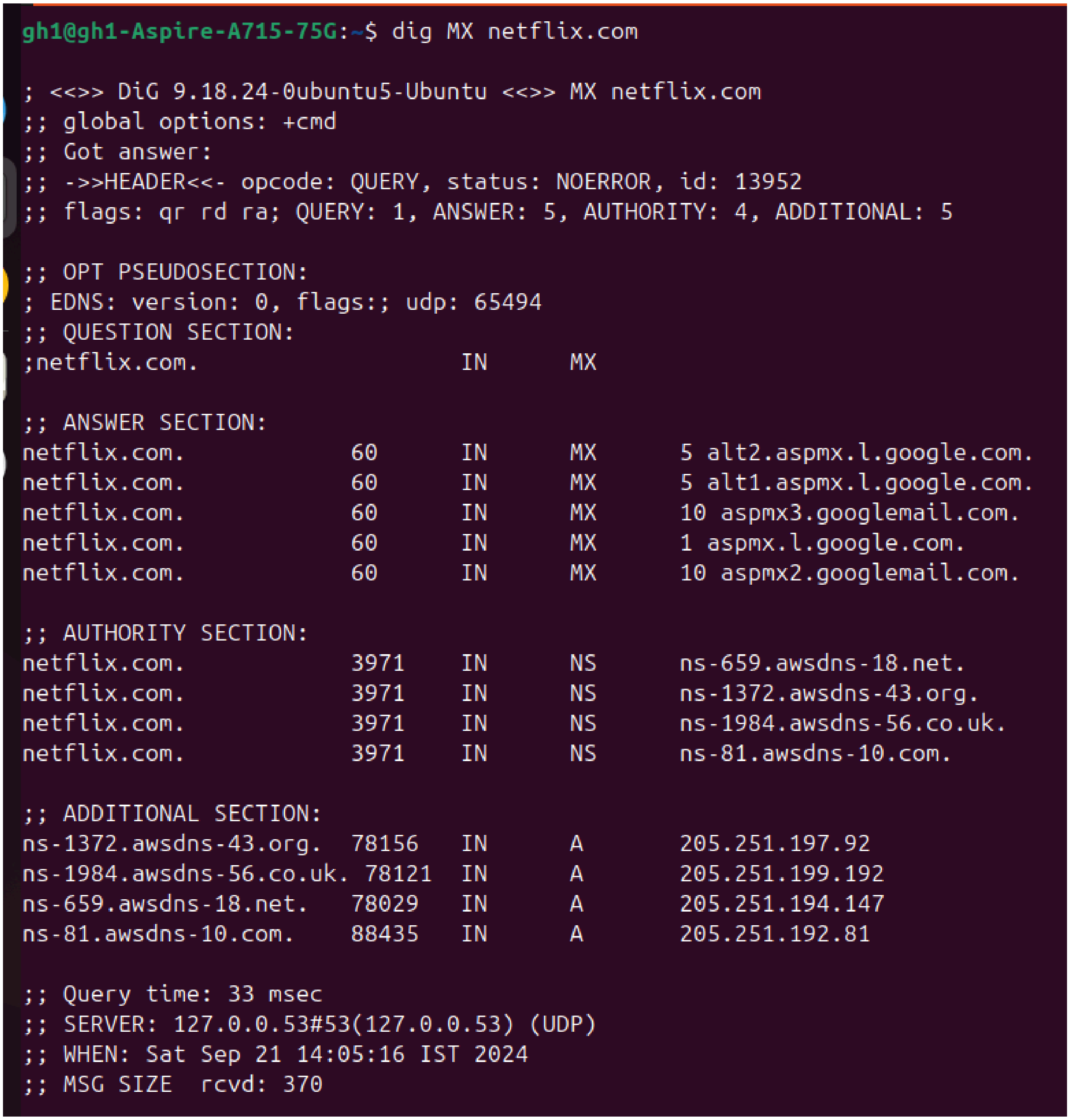
```
gh1@gh1-Aspire-A715-75G:~$ dig A netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> A netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46235
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      A

;; ANSWER SECTION:
netflix.com.            32      IN      A       54.155.246.232
netflix.com.            32      IN      A       54.73.148.110
netflix.com.            32      IN      A       18.200.8.190

;; AUTHORITY SECTION:
netflix.com.            3995    IN      NS      ns-1372.awsdns-43.org.
netflix.com.            3995    IN      NS      ns-659.awsdns-18.net.
netflix.com.            3995    IN      NS      ns-81.awsdns-10.com.
netflix.com.            3995    IN      NS      ns-1984.awsdns-56.co.uk.

;; ADDITIONAL SECTION:
ns-1372.awsdns-43.org.  78180   IN      A       205.251.197.92
ns-1984.awsdns-56.co.uk. 78145  IN      A       205.251.199.192
ns-659.awsdns-18.net.   78053   IN      A       205.251.194.147
ns-81.awsdns-10.com.    88459   IN      A       205.251.192.81

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:04:52 IST 2024
;; MSG SIZE  rcvd: 288
```

- IP Addresses-
    - 54.155.246.232
    - 54.73.148.110
    - 18.200.8.190
- Query Time- 3 ms



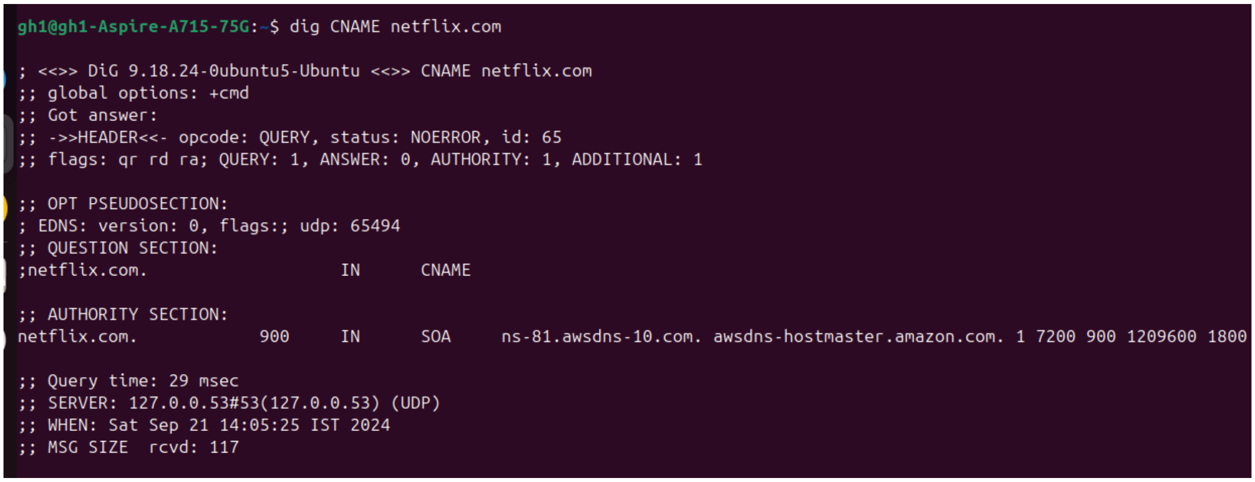
```
gh1@gh1-Aspire-A715-75G:~$ dig AAAA netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> AAAA netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9245
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      AAAA

;; ADDITIONAL SECTION:
ns-1372.awsdns-43.org.  78168   IN      A       205.251.197.92
ns-1984.awsdns-56.co.uk. 78133  IN      A       205.251.199.192
ns-659.awsdns-18.net.   78041   IN      A       205.251.194.147
ns-81.awsdns-10.com.    88447   IN      A       205.251.192.81

;; Query time: 54 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:05:05 IST 2024
;; MSG SIZE  rcvd: 184
```

- No IPv6 address returned here
- Query Time- 54 ms



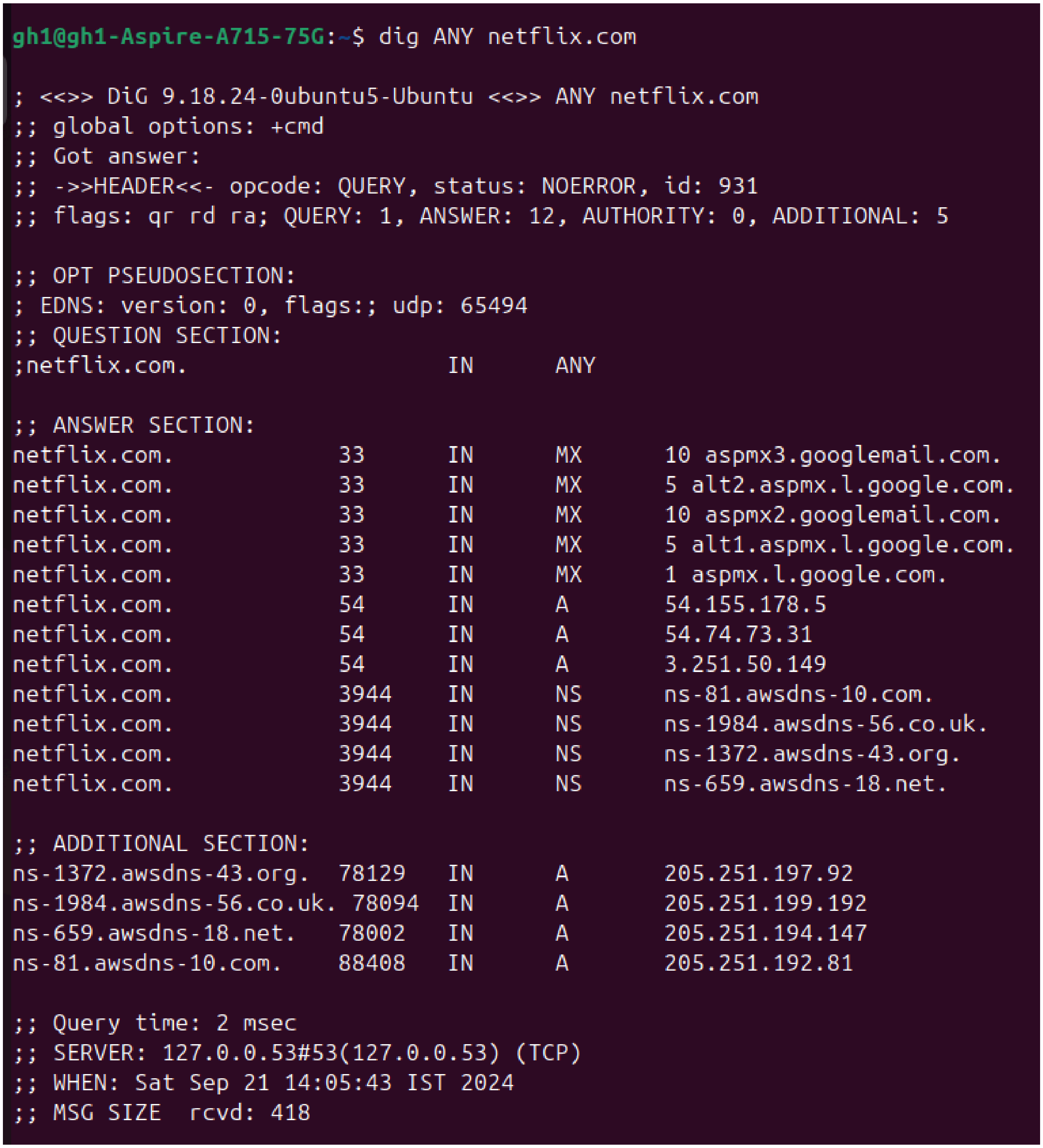
```
gh1@gh1-Aspire-A715-75G:~$ dig MX netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> MX netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13952
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      MX

;; ANSWER SECTION:
netflix.com.            60      IN      MX      5 alt2.aspmx.l.google.com.
netflix.com.            60      IN      MX      5 alt1.aspmx.l.google.com.
netflix.com.            60      IN      MX      10 aspmx3.googlemail.com.
netflix.com.            60      IN      MX      1 aspmx.l.google.com.
netflix.com.            60      IN      MX      10 aspmx2.googlemail.com.

;; AUTHORITY SECTION:
netflix.com.            3971    IN      NS      ns-659.awsdns-18.net.
netflix.com.            3971    IN      NS      ns-1372.awsdns-43.org.
netflix.com.            3971    IN      NS      ns-1984.awsdns-56.co.uk.
netflix.com.            3971    IN      NS      ns-81.awsdns-10.com.

;; ADDITIONAL SECTION:
ns-1372.awsdns-43.org.  78156   IN      A       205.251.197.92
ns-1984.awsdns-56.co.uk. 78121  IN      A       205.251.199.192
ns-659.awsdns-18.net.   78029   IN      A       205.251.194.147
ns-81.awsdns-10.com.    88435   IN      A       205.251.192.81

;; Query time: 33 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:05:16 IST 2024
;; MSG SIZE  rcvd: 370
```

- MX Records-
  - 5 alt2.aspmx.l.google.com
  - 5 alt1.aspmx.l.google.com
  - 10 aspmx3.googlemail.com
  - 1 aspmx.l.google.com
  - 10 aspmx2.googlemail.com
- Query Time-33 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig CNAME netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> CNAME netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      CNAME

;; AUTHORITY SECTION:
netflix.com.            900     IN      SOA     ns-81.awsdns-10.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 1800

;; Query time: 29 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:05:25 IST 2024
;; MSG SIZE  rcvd: 117
```

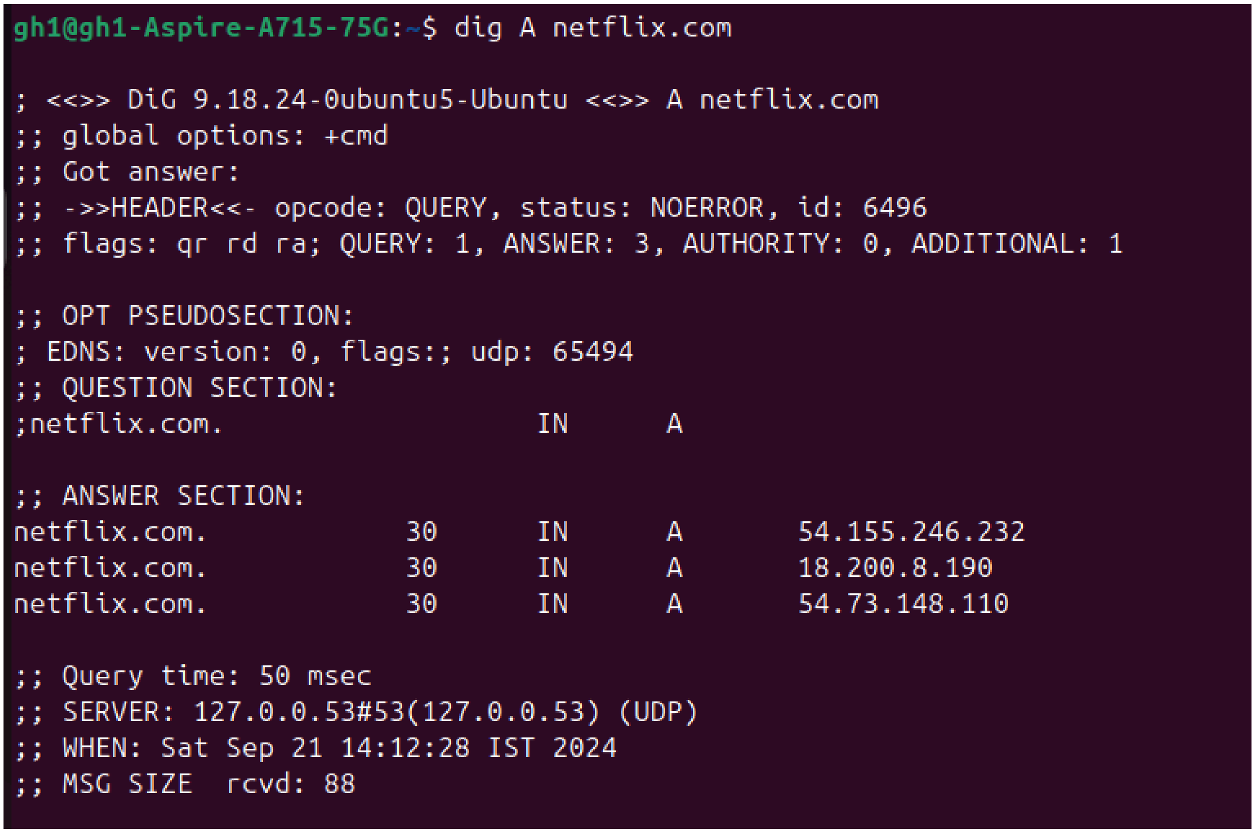
- No CNAME record returned; instead, an SOA (Start of Authority) record was provided
- Query time- 29 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig ANY netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> ANY netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 931
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      ANY

;; ANSWER SECTION:
netflix.com.            33      IN      MX      10 aspmx3.googlemail.com.
netflix.com.            33      IN      MX      5 alt2.aspmx.l.google.com.
netflix.com.            33      IN      MX      10 aspmx2.googlemail.com.
netflix.com.            33      IN      MX      5 alt1.aspmx.l.google.com.
netflix.com.            33      IN      MX      1 aspmx.l.google.com.
netflix.com.            54      IN      A       54.155.178.5
netflix.com.            54      IN      A       54.74.73.31
netflix.com.            54      IN      A       3.251.50.149
netflix.com.            3944    IN      NS      ns-81.awsdns-10.com.
netflix.com.            3944    IN      NS      ns-1984.awsdns-56.co.uk.
netflix.com.            3944    IN      NS      ns-1372.awsdns-43.org.
netflix.com.            3944    IN      NS      ns-659.awsdns-18.net.

;; ADDITIONAL SECTION:
ns-1372.awsdns-43.org.  78129   IN      A       205.251.197.92
ns-1984.awsdns-56.co.uk. 78094  IN      A       205.251.199.192
ns-659.awsdns-18.net.   78002   IN      A       205.251.194.147
ns-81.awsdns-10.com.    88408   IN      A       205.251.192.81

;; Query time: 2 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Sat Sep 21 14:05:43 IST 2024
;; MSG SIZE  rcvd: 418
```

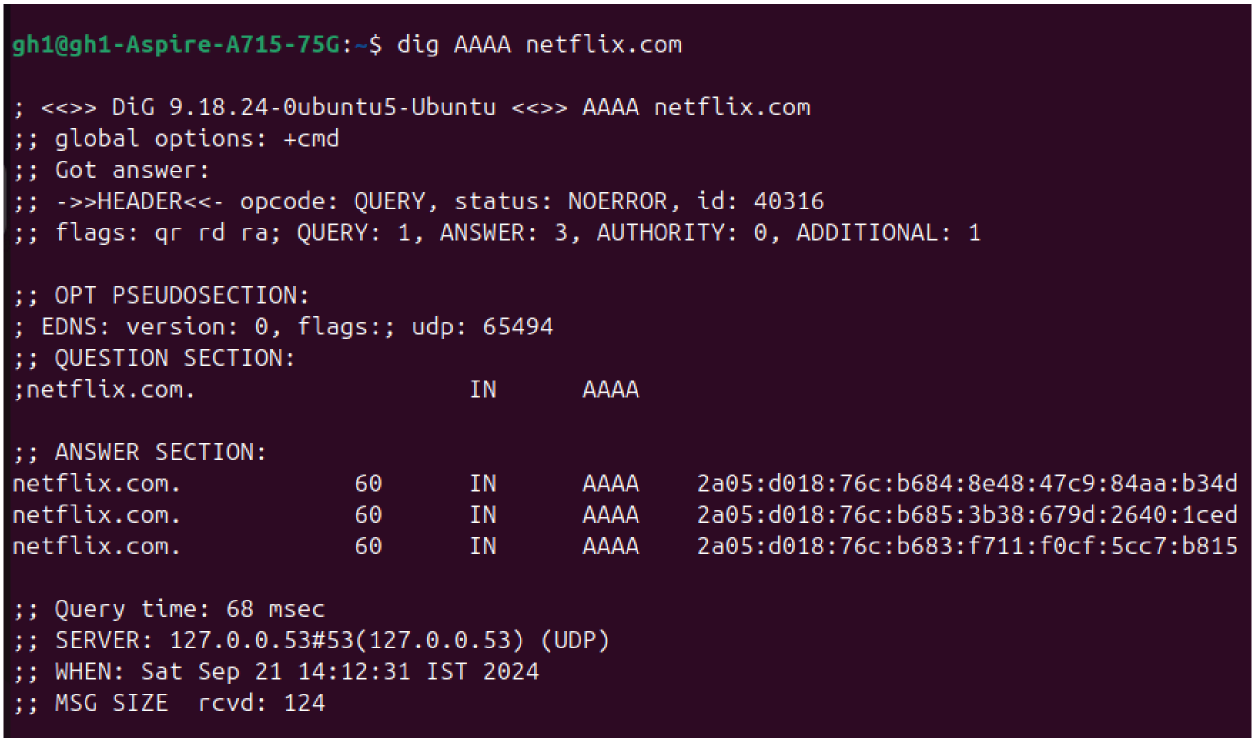
- Number of Responses: 12
- Records Returned: A (IPv4), MX, and NS records.

b)Mobile Network



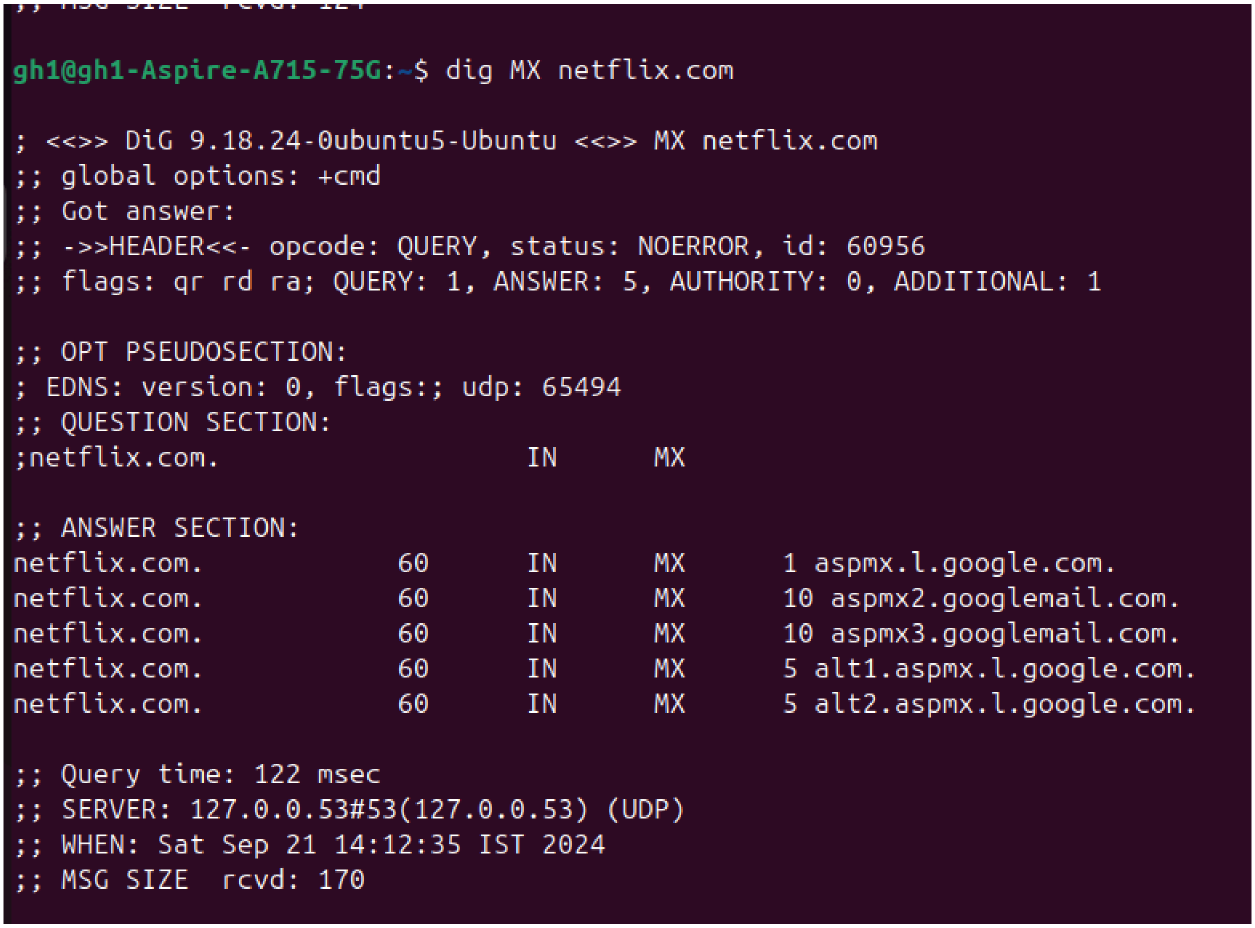
```
gh1@gh1-Aspire-A715-75G:~$ dig A netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> A netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6496
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      A

;; ANSWER SECTION:
netflix.com.            30      IN      A       54.155.246.232
netflix.com.            30      IN      A       18.200.8.190
netflix.com.            30      IN      A       54.73.148.110

;; Query time: 50 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:12:28 IST 2024
;; MSG SIZE  rcvd: 88
```

- IP Addresses-
    - 54.155.246.232
    - 18.200.8.190
    - 54.73.148.110
- Query Time- 50 ms



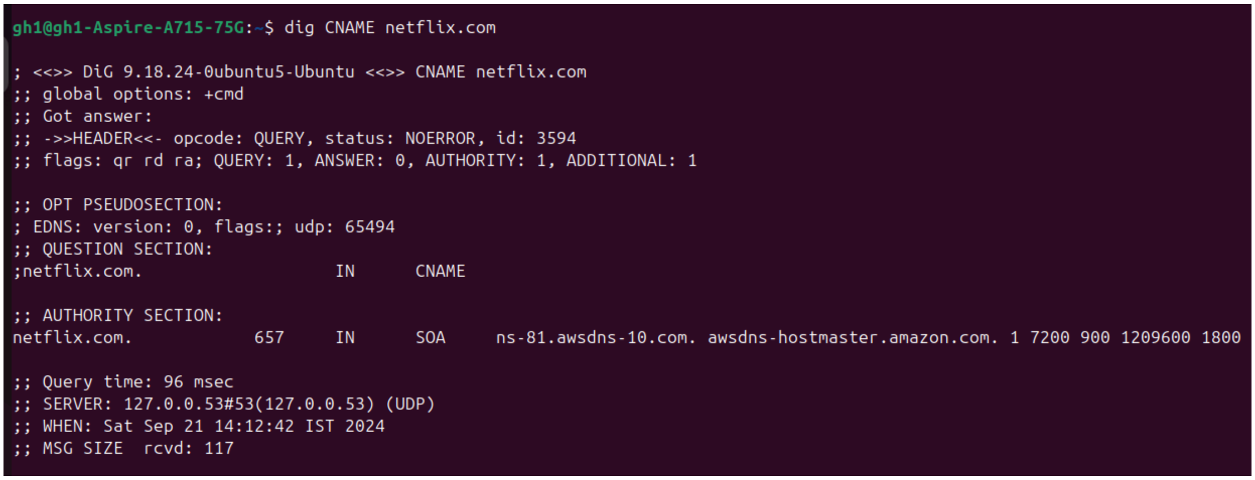
```
gh1@gh1-Aspire-A715-75G:~$ dig AAAA netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> AAAA netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40316
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      AAAA

;; ANSWER SECTION:
netflix.com.            60      IN      AAAA    2a05:d018:76c:b684:8e48:47c9:84aa:b34d
netflix.com.            60      IN      AAAA    2a05:d018:76c:b685:3b38:679d:2640:1ced
netflix.com.            60      IN      AAAA    2a05:d018:76c:b683:f711:f0cf:5cc7:b815

;; Query time: 68 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:12:31 IST 2024
;; MSG SIZE  rcvd: 124
```

- IPv6 Addresses-
    - 2a05:d018:76c:b684:8e48:47c9:84aa
    - 2a05:d018:76c:b685:3b38:679d:2640:1ced
    - 2a05:d018:76c:b683:f711:f0cf:5cc7
- Query Time- 68 ms



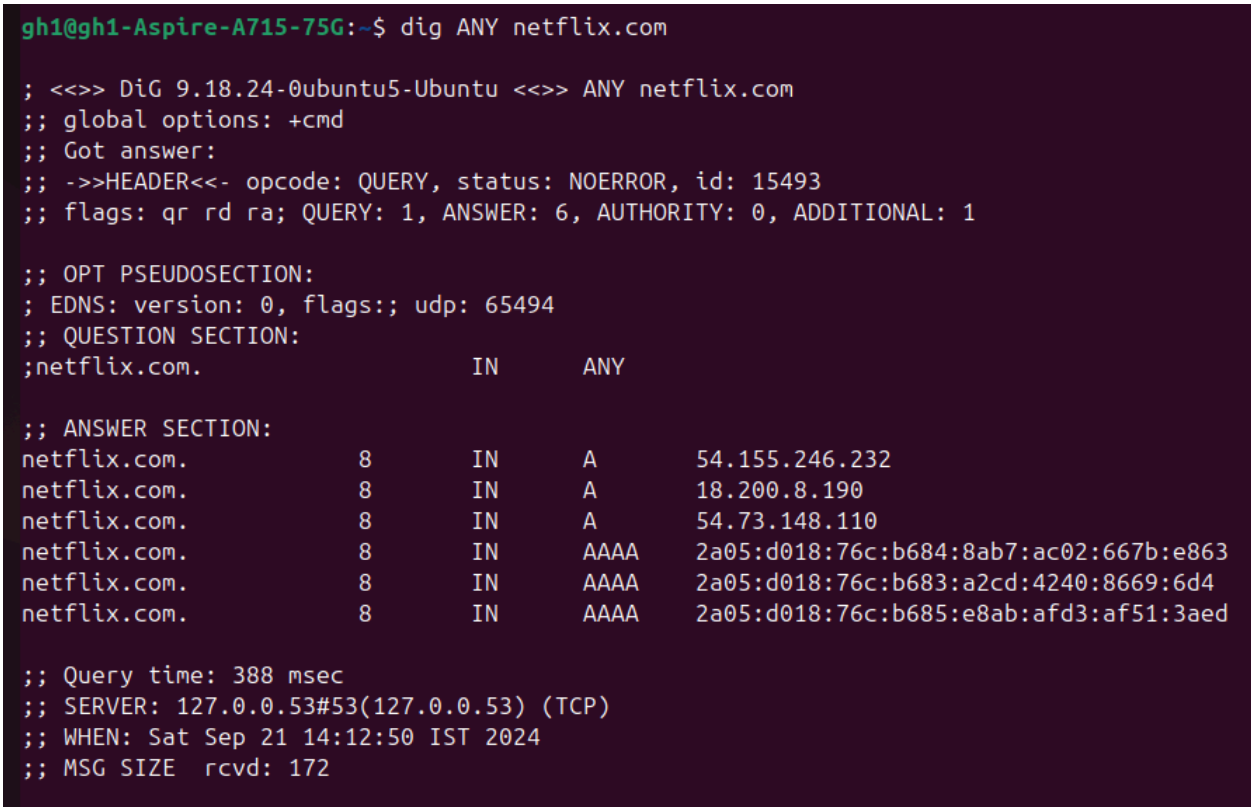
```
;; MSG SIZE  rcvd: 124

gh1@gh1-Aspire-A715-75G:~$ dig MX netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> MX netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60956
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      MX

;; ANSWER SECTION:
netflix.com.            60      IN      MX      1 aspmx.l.google.com.
netflix.com.            60      IN      MX      10 aspmx2.googlemail.com.
netflix.com.            60      IN      MX      10 aspmx3.googlemail.com.
netflix.com.            60      IN      MX      5 alt1.aspmx.l.google.com.
netflix.com.            60      IN      MX      5 alt2.aspmx.l.google.com.

;; Query time: 122 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:12:35 IST 2024
;; MSG SIZE  rcvd: 170
```

- MX Records-
  - 1 aspmx.l.google.com
  - 5 alt1.aspmx.l.google.com
  - 10 aspmx2.googlemail.com
  - 10 aspmx3.googlemail.com
  - 5 alt2.aspmx.l.google.com
- Query Time- 122 ms



```
gh1@gh1-Aspire-A715-75G:~$ dig CNAME netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> CNAME netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3594
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      CNAME

;; AUTHORITY SECTION:
netflix.com.            657     IN      SOA     ns-81.awsdns-10.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 1800

;; Query time: 96 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Sep 21 14:12:42 IST 2024
;; MSG SIZE  rcvd: 117
```

- No CNAME record returned here ,an SOA record was provided.



```
gh1@gh1-Aspire-A715-75G:~$ dig ANY netflix.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> ANY netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15493
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netflix.com.                   IN      ANY

;; ANSWER SECTION:
netflix.com.            8       IN      A       54.155.246.232
netflix.com.            8       IN      A       18.200.8.190
netflix.com.            8       IN      A       54.73.148.110
netflix.com.            8       IN      AAAA    2a05:d018:76c:b684:8ab7:ac02:667b:e863
netflix.com.            8       IN      AAAA    2a05:d018:76c:b683:a2cd:4240:8669:6d4
netflix.com.            8       IN      AAAA    2a05:d018:76c:b685:e8ab:afd3:af51:3aed

;; Query time: 388 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Sat Sep 21 14:12:50 IST 2024
;; MSG SIZE  rcvd: 172
```

- Number of Responses- 6
- Records Returned: A (IPv4) & AAAA (IPv6) addresses.

Analysis-

- **A Record (IPv4)**

  Both networks mobile network and the Wi-Fi network resolve to the same IP addresses for the A record which indicates that Netflix uses geo-routing strategies across different networks and consistent load balancing.

  The query time is significantly less which is 3 ms on Wi-Fi compared to mobile which is 50 ms, may be due to the inherent latency in mobile networks, which can include factors like network congestion and signal strength.

- **AAAA Record (IPv6)**

  The Wi-Fi network did not return any IPv6 addresses in this case, whereas we can observe the mobile network provided multiple IPv6 addresses. This shows differences in IPv6 support and configuration between networks.

  The longer query time of 68 ms is observed for the mobile network which indicates additional latency associated with IPv6 resolution,may be due to less optimization in mobile networks.

- **MX Record (Mail Exchange)**

  Both networks resolved the same MX records for netflix.com which indicates that email delivery infrastructure is consistent across networks for this case.

  The query time is notably higher on mobile which is 122 ms compared to Wi-Fi 33 ms, which shows increased overhead on the mobile DNS resolver.

- **CNAME Record**

  Neither of mobile network or Wi-Fi network returned a CNAME record for netflix.com, which indicates that there is no aliasing for the root domain in the DNS setup. Both networks returned the same SOA record which indicates the fact of consistent authoritative DNS settings.

  Netflix's preference for direct resolution for its primary domain is indicated by the absence of CNAME records , which can lead to faster lookups.

- **ANY Record**

  Compared to the mobile network the Wi-Fi network returned a more set of records. This may be due to the mobile network's resolver being configured to limit the amount of information returned for ANY queries as observed in output.

The difference in responses seen suggests variations in DNS resolver behavior, which shows the relationship of how services can leverage DNS records based on the querying network.

Key Differences Between Wi-Fi and Mobile Networks for Netflix

- **IP Address Assignment-** Both networks returned the same IPv4 addresses here, but mobile also returned IPv6 addresses which is showing better IPv6 adoption on mobile.

- **DNS Record Results-** Similar A, MX, and ANY responses across networks observed here, though mobile had slightly fewer details in my output which, indicats optimizations for lightweight responses.

- **Query Time-** Wi-Fi had much faster query times (in my output,, A record took 3 ms vs. 50 ms on mobile). Mobile had higher latency, especially in the ANY query which is 388 ms, suggesting network congestion or slower DNS resolution.

This structure offers a comprehensive overview of the differences in DNS query results for Netflix on Wi-Fi and mobile networks, highlighting query times, IP addresses,, analyses for each record type.

DNS Caching Influence-

DNS caching significantly affects TTL values and resolution times as observed here. A cached result will return much faster and less time will be required, and the TTL value indicates how long the record is cached before the DNS resolver queries to authoritative server again.

Higher TTL values (like those seen on mobile networks in my terminal output) suggests that caching servers might be more aggressive which may leads to fewer frequent DNS queries. On the other hand, lower TTLs on Wi-Fi might indicate fresher data, but they are with slightly more overhead in frequent querying.

Different CDNs are being used, if DNS responses are optimized for particular geographic regions?

Yes, different CDNs are likely being used, as evidenced by the different IP addresses and TTL values across Wi-Fi and mobile networks seen in my output. These differences suggest that DNS responses are optimized based on network and geographic regions, directing users to most efficient CDN node or nearest node for faster content delivery with respect to location of that particular user. For example, Google and Facebook returned different IPs across networks as observed in my output, indicating traffic is routed through geographically optimized CDNs, while Netflix showed consistent IPs in my output, implying a less dynamic CDN setup.

Effect of Anycast routing or Geo-DNS -

Based on the user's network and geographic location , anycast routing and Geo-DNS generally direct DNS queries to nearest or most optimal serve for that user. This proves why different IP addresses and TTL values were observed between Wi-Fi and mobile networks in my output.. Latency is reduced by connecting users to the closest server in case of Anycast routing,, while users are directed to CDN nodes optimized for their region, improving load times and overall performance in case of Geo-DNS.

In conclusion, the DNS records show network-specific optimizations, with mobile and Wi-Fi networks receiving different IPs, TTL values, and response times. CDNs and Anycast routing seem to play a significant role in optimizing traffic based on the network. DNS caching also impacts resolution times, as seen from the varying TTLs across networks.

Part 2: CDN Architecture Analysis

1) CDN and Multi-CDN Optimization-

Introduction-

In this part I studied Content Delivery Network (CDN) architecture, focused on the CDN and multi CDN optimization techniques, and usage of reverse proxy for enhanced security. I also explored how CDNs improve performance and security for globally distributed users

.

Analysis-

Employment of Multi CDN strategy for optimizing content delivery for Global Streaming Service-

A multi CDN strategy works by using multiple CDN providers for ensuring better streaming quality, high availability ad lower latency for optimizing content delivery for global streaming service. This approach reduces dependence on a single CDN and distributes content across multiple networks which improves reliability.

In the multi CDN strategy, the best CDN is selected dynamically based on real time network conditions,traffic and geography which will results in improving content availability and reducing latency which will ensures a better experience for end users.

Benefits of Multi-CDN-

1) Geographical Optimization- Depending on users location, they will be directed to best CDN server is ensured by the multi CDN strategy which minimizes the latency, buffering, packet loss and improves experience of user.
2) Redundancy and Failover- Traffic will go to another CDN provider for keeping uninterrupted service when there is any network issue with one CDN provider.
3) Load Balancing- For load balancing based on factors like user location, server load, optimizing performance , minimizing strain on server and server load, the traffic will be dynamically distributed between CDNs.
4) Reduced Latency- Multi CDN strategy speed up content delivery and minimizes round trip time by routing users to CDN server which is near to their location.
5) Adaptive Bitrate Streaming - For streaming platforms multi CDN technology is very beneficial allowing for smooth adaptation to network conditions. For maintaining best possible user experience under fluctuating conditions also, services like google media CDN or netflix adjust video quality dynamically.

Open Connect for Google Media CDN or Netflix-

Google media CDN optimization-
Google media CDN supports anycast routing and bitrate streaming for better video delivery.

Caching and Edge computing- To reduce need for users to fetch content from origin servers, google media CDN caches content near to end user with help of extensive edge network.

Load Balancers: Traffic across regions is dynamically managed by the google global load balancer and it also ensures that content is delivered to end users with lower latency.

Anycast Routing- Google media CDN enhances content delivery by distributing user traffic to many locations for minimizing the latency and improving the load distribution. Based on real time network conditions, the request will be directed to most optimal server or nearest server.

Netflix media CDN optimization-

By placing dedicated open connect appliances in ISP’s data centers, netflix open connect optimized video delivery which brings content close to users.

Anycast Routing and Load Balancing- To send users to nearest CDN node for reduced buffering, better and fastest delivery netflix uses anycast routing.

Adaptive Bitrate Streaming- For providing an uninterrupted streaming experience, video quality is adjusted based on users available bandwidth.

Netflix and google media both open connect allows flexible streaming of video by using adaptation to real time network conditions, delivering consistent user experience and reducing latency.

CDN Selection and Justification:
Multi CDN strategy ensures-

1) Geographical Optimization- Based on th performance in specific regions, CDNs are selected.
2) High Availability- As the content is redundant across multiple CDN providers, it is always available.
3) Improved Performance During high traffic- Multi CDN system distributes traffic efficiently for avoiding bottlenecks when there is any sudden spikes in demand or live events.
4) Failover & disaster recovery- In case when any one CDN provider fails then other will take over without disturbing user experience.

Diagram-

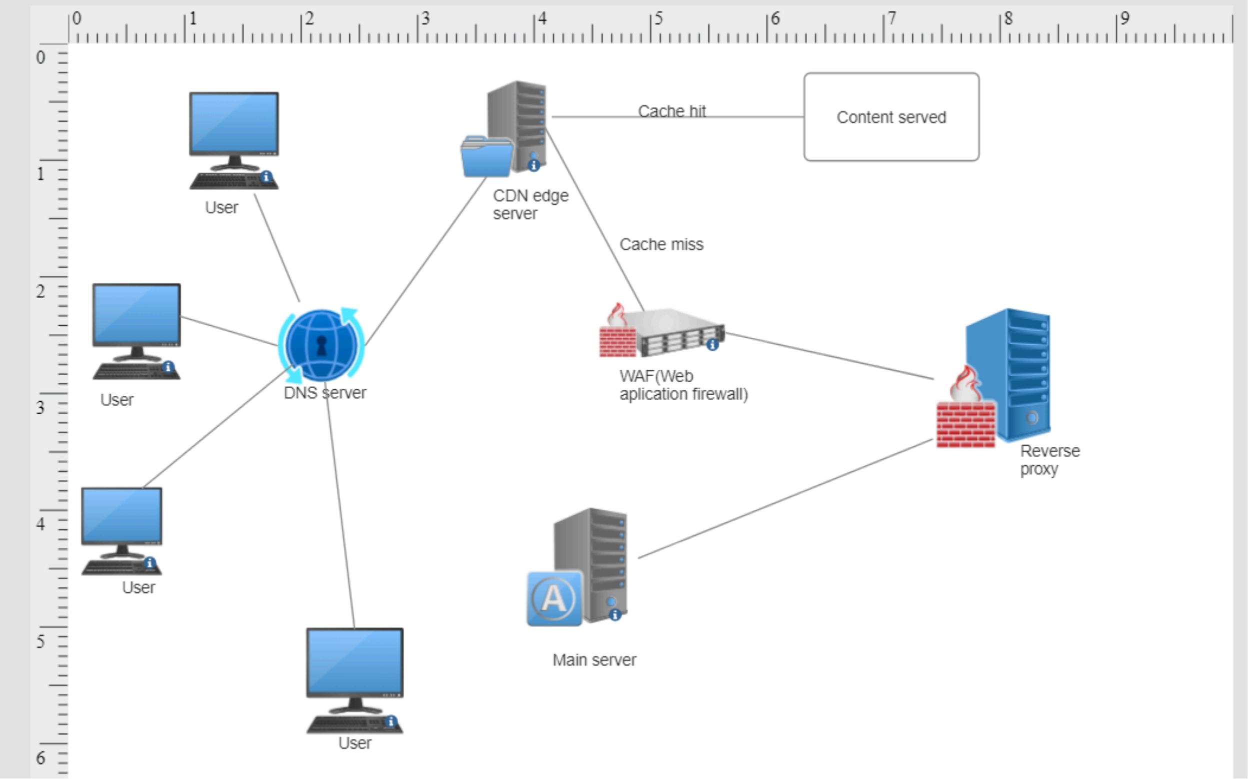


Fig. Global streaming service with CDN and reverse proxies

Comparison to Netflix Open Connect-

Open connect for Netflix is optimized for its particular requirements that is it places OCAs within ISPs to cache content closer to users but in case of multi CDN strategy offers more redundancy and flexibility.By balancing traffic actress multiple providers, a multi CDN approach mitigates network bottlenecks.Open connect might not suit all streaming platforms.

2. Reverse Proxy and Security

Cloudflare as a Reverse Proxy for websites-

Cloudflare operates as a reverse proxy for websites by standing between user(client) and origin server of website. It intercepts incoming traffic and then it processes the requests then forward that to corresponding web servers. To improve performance and security of websites, cloudflare global network of data centers handles several tasks. Cloudflare does th e following to act as reverse proxy- Performance enhancement, Security improvements, Customizability and analytics, Scalability and reliability.

Cloudflare handles these tasks at global network of edge servers which results in reduced load on origin server, improves reliability and speed of website and improves overall user experience and security. Performance and security improvements are explained below. The website owners can handles customizability and reliability by monitoring security and performance in real time and traffic management rules with the help of cloudflare advanced analytics tools. Load balancing , failover capabilities and traffic distribution ensures that the website will remain available even if there is server failures or heavy traffic. By doing there at global network edge, it reduces load on origin servers and makes improvement in websites reliability and speed.

1) Performance Improvement-
   For speeding up delivery and reducing load on origin servers, the CLoudflare acts as reverse proxy with caching web content closer to user.
   Content Caching- To reduce need for repeated requests to origin server, frequently accessed content is cached at Cloudflare edge servers.
   It ensures secure communication between user and server by handling certificates and encryption considering reduction in the processing load on origin server.

2) Security Improvement-
   Web Application Firewall (WAF)- If blocks malicious requests at the edge for protecting web applications which improves security against many vulnerabilities.

   Distributed Denial of Service Protection- Cloudflare filters malicious traffic before it reaches origin server for preventing from distributed denial of service attacks.

Interaction between Reverse Proxies, DNS, and CDNs-

Reverse proxies, CDNs and DNS server work together for ensuring the security and optimizing delivery of content. In the overall content delivery system for a streaming platform each of these plays interdependent and distinct role.

a) DNS- DNS translates human readable domain names into IP addresses that computers use to identify servers in content delivery. If any user try for accessing website then the request first goes to DNS server which converts the domain name to IP address of closest reverse proxy or CDN server. DNS helps to improve content delivery speed and reduce latency by directing user to nearest edge server.

b) Reverse Proxy- After resolving IP address by the DNS the request of user will be directed to reverse proxy. It will handle request and then request will be forwarded to origin server. Depending on the need either dynamic content or non cached content the reverse proxy may give the content which is cached directly from its edge server or it may pass request to origin server. The performance is improved and load is reduced in the origin server by offloading other tasks like DDoS mitigation and SSL termination to reverse proxy.

c) CDN- Content delivery network consists of distributed network of edge servers which caches the content close to end users. Reverse proxy like generally integrates with CDNs for reducing load on the origin server and caching content. Reverse proxy provides security services while CDN delivers the content which is cached.

SSL Termination importance- Cloudflare ensures a secure connection by handling SSL at edge to encrypt data between user and proxy server. For performance and security, SSL termination at reverse proxy level is essential. The reverse proxy can handle computationally intensive task of decrypting SSL/ TLS requests by terminating the SSL connection at edge which allows origin server to focus on dynamic content serving.

DDoS Protection and Caching importance- For ensuring origin server remains unaffected, cloudflare inspects the incoming flow of traffic for detecting and blocking attacks. Cached content is responsible for speed up delivery and the reduction in load on origin server.

Importance of Content caching at the proxy level- To reduce the need of repeated requests to origin server, the reverse proxy can cache static content at the edge which results in improved scalability and performance particularly when content is requested by multiple users in high traffic platforms like streaming services.

Google Global Load Balancer and Cloudflare:

Google global load balancer distributes traffic efficiently across many regions which directs users to nearest or most available instance and it works well with infrastructure of google cloud offering features like traffic management and autoscaling across zones. On the other hand Cloudflare acts both like proxy server and CDN which focuses on security features such as WAF and Distributed Denial of Service Protection. Cloudflare is best in securing delivery of content and providing enhancements in performance. Google global load balancer does not inherently cache content but it can integrate with cloud CDN of google for global content distribution. On the other hand cloudflare have build in CDN for content caching which improves load times by serving cached content from closest edge location.

Choice for Platform-

My choice is Cloudflare because of its strong focus on security features such as WAF, SSL termination and Distributed Denial of Service Protection. THe caching and edge computing of cloudflare ensures that content will be delivered to the users quickly regardless of location of user. Security features of cloudflare makes it perfect for the global streaming service which requires both best security and performance for handling cyber threats and big volumes of traffic.

References-

1. https://cloud.google.com/load-balancing/docs/application-load-balancer#use-cases
2. https://blog.jiocinema.com/tag/cdn/
3. https://www.cloudflare.com/en-gb/learning/
4. https://www.geeksforgeeks.org/details-on-dns/
5. https://www.geeksforgeeks.org/designing-content-delivery-network-cdn-system-design/
6. https://youtu.be/f19KCM_xxxk?si=hbajTNzPBEn1C5FK
7. https://youtu.be/iESSCDnC74k?si=REtRgkuuFWxviL_K
8. https://youtu.be/RI9np1LWzqw?si=3rhU516YmT9vHIoE

Anti-Plagiarism Statement:

By submitting this assignment, I certify that the work presented here is my own, based on my personal research, observations, and understanding. I affirm that:

- All data, diagrams, and content used from external sources (e.g., blogs, articles, papers, videos, podcasts) have been appropriately cited and acknowledged in the report.
- Diagrams or visuals borrowed from online sources have been clearly credited, and I have provided my own explanations or insights for all included visuals.
- This assignment has not been copied in part or whole from any other student or individual, and I have not used pre-written solutions or responses generated by LLMs (e.g., ChatGPT) without significant personalization, verification, and adaptation.
- If I used any AI-based tools, I have appropriately acknowledged their usage and ensured that the work has been refined through my own understanding and knowledge.
- I understand that failure to adhere to these guidelines may result in penalties for academic misconduct, as outlined by the institution’s policies.

I also pledge to uphold the principles of honesty and integrity during this course and report any violations of the academic code of conduct if I become aware of them