CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-4

Wireshark Lab: DNS

January 27, 2025

Part-1: Flushing DNS on Different Operating Systems

DNS caching improves resolution speed by storing recently resolved domain names. However, stale or incorrect DNS entries can cause issues, making it necessary to flush the DNS cache. In this section, you will:

1) Learn how DNS caching works and its role in resolving domain names.
2) Understand the steps to flush DNS caches on various operating systems, such as:
    a) Windows: Using the ipconfig /flushdns command.
    b) MacOS: Using sudo dscacheutil -flushcache and sudo killall -HUP mDNSResponder
    c) Linux: Using resolvectl flush-caches

Part-2: Using nslookup for DNS Queries

Part 2.1: Use `nslookup` command on two domains (`iitdh.ac.in`, and `google.com`) separately (as shown in the below figure), and answer the following questions.

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ resolvectl flush-caches
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup iitdh.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   iitdh.ac.in
Address: 10.195.250.62

user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.67.46
Name:   google.com
Address: 2404:6800:4007:820::200e
```

Q.1. [1 mark] What is the IP address of the requested domain?

Domain	**IP address of requested domain**
`iitdh.ac.in`	10.195.250.62
`google.com`	**IPV4:** 142.250.67.46 **IPV6:** 2404:6800:4007:820::200e

Q.2. [1 mark] What is the IP address of the DNS resolver?

Domain	IP address of DNS resolver
`iitdh.ac.in`	127.0.0.53
`google.com`	127.0.0.53

Q.3. [1 mark] Which port number is used to resolve the domain?

Domain	Port Number
`iitdh.ac.in`	53
`google.com`	53

Q.4. [3 marks] Verify the IP address obtained using the DNS for the requested domain using the `host`, `whois`, and `dig` commands (refer slides for the commands).

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ host iitdh.ac.in
iitdh.ac.in has address 10.195.250.62
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ host google.com
google.com has address 142.250.193.142
google.com has IPv6 address 2404:6800:4007:827::200e
google.com mail is handled by 10 smtp.google.com.
```

The **host command** will return the IP address(es) associated with the domain name (here ex: iitdh.ac.in).

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ dig +short google.com
142.250.183.238
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ dig -x 142.250.183.238

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> -x 142.250.183.238
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56459
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;238.183.250.142.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
238.183.250.142.in-addr.arpa. 7184 IN   PTR     maa05s23-in-f14.1e100.net.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Jan 27 09:12:53 IST 2025
;; MSG SIZE  rcvd: 96
```

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ dig +short iitdh.ac.in
10.195.250.62
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ dig -x 10.195.250.62

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> -x 10.195.250.62
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57930
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;62.250.195.10.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
62.250.195.10.in-addr.arpa. 86400 IN    PTR     www.iitdh.ac.in.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Jan 27 10:40:48 IST 2025
;; MSG SIZE  rcvd: 84
```

The **dig command** provides detailed DNS resolution information. This command is used to retrieve the IP address of the domain. The IP addresses listed are the same as that obtained using the **host command**, confirming the consistency of the DNS information.

```
tejaswinich17@TEJASWINICHIDURALA:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-02-02T10:34:12Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

```
tejaswinich17@TEJASWINICHIDURALA:~$ whois iitdh.ac.in
Domain Name: iitdh.ac.in
Registry Domain ID: D414400000001173465-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2023-11-06T06:46:21Z
Creation Date: 2016-06-17T07:36:37Z
Registry Expiry Date: 2026-06-17T07:36:37Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: IIT Dharwad
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: dns1.iitdh.ac.in
Name Server: dns2.iitdh.ac.in
Name Server: dns3.iitdh.ac.in
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2025-02-02T10:36:13Z <<<
```

- The **whois** command provides registration details about the domain such as-Registrar information (who manages the domain), Domain creation and expiration dates, Name servers, Registrant contact information.
- The **whois** output does not include the IP address directly because its purpose is to provide administrative and ownership details rather than real-time DNS resolution data.
- For verifying the IP address obtained via DNS for a given domain, rely on **host** and **dig** since they directly query DNS records. The consistency of their outputs confirms that the domain is correctly mapped to its IP address.

Part 2.2: Use `nslookup` command on two domains (`iitdh.ac.in`, and `google.com`) separately (as shown in the below figure), and answer the following questions.

Q.1. [4 marks] List the nameservers you are observing for the above-requested domain names.

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup -type=NS google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.

Authoritative answers can be found from:
```

- **Domain:** google.com
- **Name Servers:** ns2.google.com, ns1.google.com, ns4.google.com, and ns3.google.com

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup -type=NS iitdh.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
iitdh.ac.in     nameserver = idns.iitdh.ac.in.

Authoritative answers can be found from:
```

- **Domain:** iitdh.ac.in
- **Name Servers:** idns.iitdh.ac.in

Part 2.3: Use `nslookup -type=[RECORD] google.com` Where, RECORD can be A, NS, and MX Answer the following questions based on the above command:

Q.1. [3 marks] Mention the significance of each of the record types.

1. A (Address) Record

- **Purpose:** Maps a domain name (here ex: google.com) to its corresponding IPV4 address (142.250.182.78).

- **Significance:** Translates human-readable domain names into machine-readable IP addresses.

2. NS (Name Server) Record

- **Purpose:** Specifies the authoritative name servers for a domain, responsible for handling DNS queries.
- **Significance:** Ensures DNS delegation by directing queries to the correct name servers.

3. MX (Mail Exchange) Record

- **Purpose:** Defines the mail servers responsible for handling incoming emails for a domain.
- **Significance:** Ensures proper email routing by directing email traffic to the appropriate mail servers & Supports load balancing and failover mechanisms, enhancing email reliability.

Q.2. [3 marks] List the IP addresses in the "Non-authoritative answer" for all the above record types.

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup -type=A google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.182.78
```

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup -type=NS google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.

Authoritative answers can be found from:
```

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup -type=MX google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
```

Type Record command used	IP Address in "Non-authoritative answer"
nslookup -type=A google.com	142.250.182.78
nslookup -type=NS google.com	We get list of all name servers→ ns2.google.com ns1.google.com ns4.google.com ns3.google.com
nslookup -type=MX google.com	mail exchanger = 10 smtp.google.com **Explanation:** **10** → Priority value (lower values indicate higher priority). **smtp.google.com** → The mail server responsible for processing emails for google.com.

- The **"Non-authoritative answer"** does not provide direct IP addresses for **Mail Exchange (MX) records** and **Name Server (NS) records**.

Part 2.4: Use `nslookup` to resolve `drive.google.com` using all the nameservers of `google.com` and answer the following questions.

Q.1. [4 marks] What are the IPV4 and IPV6 addresses of `drive.google.com` from all the nameservers of `google.com`?

From list of all name servers of google.com →ns1.google.com

ns3.google.com

ns4.google.com

ns2.google.com

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup drive.google.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   drive.google.com
Address: 142.250.193.142
Name:   drive.google.com
Address: 2404:6800:4007:820::200e

user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup drive.google.com ns3.google.com
Server:         ns3.google.com
Address:        216.239.36.10#53

Name:   drive.google.com
Address: 142.250.193.142
Name:   drive.google.com
Address: 2404:6800:4007:820::200e

user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup drive.google.com ns4.google.com
Server:         ns4.google.com
Address:        216.239.38.10#53

Name:   drive.google.com
Address: 142.250.193.142
Name:   drive.google.com
Address: 2404:6800:4007:820::200e

user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup drive.google.com ns2.google.com
Server:         ns2.google.com
Address:        216.239.34.10#53

Name:   drive.google.com
Address: 142.250.193.142
Name:   drive.google.com
Address: 2404:6800:4007:820::200e
```

Name servers	**IPV4 Address**	**IPV6 Address**
ns1.google.com	**142.250.193.142**	2404:6800:4007:820::200e
ns3.google.com	**142.250.193.142**	2404:6800:4007:820::200e
ns4.google.com	**142.250.193.142**	2404:6800:4007:820::200e
ns2.google.com	**142.250.193.142**	2404:6800:4007:820::200e

Q.2. [4 marks] List the IP addresses of all `NS` of `google.com`.

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup ns2.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns2.google.com
Address: 216.239.34.10
Name:   ns2.google.com
Address: 2001:4860:4802:34::a

user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup ns1.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns1.google.com
Address: 216.239.32.10
Name:   ns1.google.com
Address: 2001:4860:4802:32::a

user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup ns4.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns4.google.com
Address: 216.239.38.10
Name:   ns4.google.com
Address: 2001:4860:4802:38::a

user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup ns3.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns3.google.com
Address: 216.239.36.10
Name:   ns3.google.com
Address: 2001:4860:4802:36::a
```

Name Servers(NS)	**IPV4 and IPV6 Addresses**
ns2.google.com	216.239.34.10 and 2001:4860:4802:34::a
ns1.google.com	216.239.32.10 and 2001:4860:4802:32::a
ns4.google.com	216.239.38.10 and 2001:4860:4802:38::a
ns3.google.com	216.239.36.10 and 2001:4860:4802:36::a

Part 2.5: Use the following commands to answer the following questions.

<u>CMD1</u>: `nslookup drive.google.com`

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup drive.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   drive.google.com
Address: 142.250.182.78
Name:   drive.google.com
Address: 2404:6800:4007:806::200e
```

<u>CMD2</u>: `nslookup drive.google.com ns1.google.com`

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup drive.google.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   drive.google.com
Address: 142.250.193.142
Name:   drive.google.com
Address: 2404:6800:4007:820::200e
```

Q.1. [1 mark] What is the difference you observe on the terminal for these two commands?

- **CMD1:** The **Non-authoritative answer** line indicates that the response is from a DNS server that does not directly manage the domain (*drive.google.com*) but has cached the information.
- **CMD2:** The **Non-authoritative answer** line is missing because the response comes directly from the authoritative DNS server (*ns1.google.com*) for the domain.

Q.2. [1 mark] Why does <u>CMD2</u> not show the "Non-authoritative answer" line in its output?

CMD2 does not show the **Non-authoritative answer** line because the response is coming directly from the authoritative DNS server (*ns1.google.com*) for the domain *drive.google.com*. Authoritative DNS servers are responsible for managing the DNS records of the domain, so their responses are considered authoritative and do not need to be labeled as **non-authoritative.**

Part-3: Capturing and Analyzing DNS Queries with Wireshark

Q.1. [6 marks] How many IP addresses are available in the terminal for machinelearningmastery.com? Do you observe the same in DNS response packet in Wireshark?

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ resolvectl flush-caches
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ nslookup machinelearningmastery.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   machinelearningmastery.com
Address: 172.67.72.46
Name:   machinelearningmastery.com
Address: 104.26.1.148
Name:   machinelearningmastery.com
Address: 104.26.0.148
Name:   machinelearningmastery.com
Address: 2606:4700:20::681a:194
Name:   machinelearningmastery.com
Address: 2606:4700:20::681a:94
Name:   machinelearningmastery.com
Address: 2606:4700:20::ac43:482e
```

dns.qry.name == "machinelearningmastery.com"

Time	No.	Source	Destination	Protocol	Length	Info
13.960448729	90	10.240.118.101	10.250.200.3	DNS	86	Standard query 0xf651 A machinelearningmastery.com
17.002386315	112	10.250.200.3	10.240.118.101	DNS	134	Standard query response 0xf651 A machinelearningmastery.com A 1…
17.003643324	113	10.240.118.101	10.250.200.3	DNS	86	Standard query 0x8bd9 AAAA machinelearningmastery.com
17.046759564	114	10.250.200.3	10.240.118.101	DNS	170	Standard query response 0x8bd9 AAAA machinelearningmastery.com …
42.272841885	280	10.240.118.101	10.250.200.3	DNS	86	Standard query 0xd711 NS machinelearningmastery.com
42.316365098	281	10.250.200.3	10.240.118.101	DNS	138	Standard query response 0xd711 NS machinelearningmastery.com NS…
48.672520910	301	10.240.118.101	10.250.200.3	DNS	86	Standard query 0xc648 MX machinelearningmastery.com
51.691939932	312	10.250.200.3	10.240.118.101	DNS	216	Standard query response 0xc648 MX machinelearningmastery.com MX…

```
▸ Frame 112: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interfac
▸ Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: HP_0a:7b:78 (e0:73:e7:0a:
▸ Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.118.101
▸ User Datagram Protocol, Src Port: 53, Dst Port: 56636
▾ Domain Name System (response)
    Transaction ID: 0xf651
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▸ machinelearningmastery.com: type A, class IN, addr 172.67.72.46
    ▸ machinelearningmastery.com: type A, class IN, addr 104.26.1.148
    ▸ machinelearningmastery.com: type A, class IN, addr 104.26.0.148
    [Request In: 90]
    [Time: 3.041937586 seconds]
```

```
0000  e0 73 e7 0a 7b 78 bc d2  95 13 e0 82 08 00 45 00   ·s··{x····
0010  00 78 9a 33 40 00 3f 11  4c ef 0a fa c8 03 0a f0   ·x·3@·?· L
0020  76 65 00 35 dd 3c 00 64  c1 fa f6 51 81 80 00 01   ve·5·<·d
0030  00 03 00 00 00 00 16 6d  61 63 68 69 6e 65 6c 65   ·····m a
0040  61 72 6e 69 6e 67 6d 61  73 74 65 72 79 03 63 6f   arningma s
0050  6d 00 00 01 00 01 c0 0c  00 01 00 01 00 00 01 2c   m·····
0060  00 04 ac 43 48 2e c0 0c  00 01 00 01 00 00 01 2c   ···CH.··
0070  00 04 68 1a 01 94 c0 0c  00 01 00 01 00 00 01 2c   ··h·····
0080  00 04 68 1a 00 94                                  ··h···
```

dns.qry.name == "machinelearningmastery.com"

Time	No.	Source	Destination	Protocol	Length	Info
13.960448729	90	10.240.118.101	10.250.200.3	DNS	86	Standard query 0xf651 A machinelearningmastery.com
17.002386315	112	10.250.200.3	10.240.118.101	DNS	134	Standard query response 0xf651 A machinelearningmastery.com A 1…
17.003643324	113	10.240.118.101	10.250.200.3	DNS	86	Standard query 0x8bd9 AAAA machinelearningmastery.com
17.046759564	114	10.250.200.3	10.240.118.101	DNS	170	Standard query response 0x8bd9 AAAA machinelearningmastery.com …
42.272841885	280	10.240.118.101	10.250.200.3	DNS	86	Standard query 0xd711 NS machinelearningmastery.com
42.316365098	281	10.250.200.3	10.240.118.101	DNS	138	Standard query response 0xd711 NS machinelearningmastery.com NS…
48.672520910	301	10.240.118.101	10.250.200.3	DNS	86	Standard query 0xc648 MX machinelearningmastery.com
51.691939932	312	10.250.200.3	10.240.118.101	DNS	216	Standard query response 0xc648 MX machinelearningmastery.com MX…

```
▸ Frame 114: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interfac
▸ Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: HP_0a:7b:78 (e0:73:e7:0a:
▸ Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.118.101
▸ User Datagram Protocol, Src Port: 53, Dst Port: 50963
▾ Domain Name System (response)
    Transaction ID: 0x8bd9
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▸ machinelearningmastery.com: type AAAA, class IN, addr 2606:4700:20::681a:194
    ▸ machinelearningmastery.com: type AAAA, class IN, addr 2606:4700:20::681a:94
    ▸ machinelearningmastery.com: type AAAA, class IN, addr 2606:4700:20::ac43:482e
    [Request In: 113]
    [Time: 0.043116240 seconds]
```

```
0000  e0 73 e7 0a 7b 78 bc d2  95 13 e0 82 08 00 45 00   ·s··{x····
0010  00 9c 9a 53 40 00 3f 11  4c ab 0a fa c8 03 0a f0   ···S@·?· L
0020  76 65 00 35 c7 13 00 88  fa 50 8b d9 81 80 00 01   ve·5·····
0030  00 03 00 00 00 00 16 6d  61 63 68 69 6e 65 6c 65   ·····m a
0040  61 72 6e 69 6e 67 6d 61  73 74 65 72 79 03 63 6f   arningma s
0050  6d 00 00 1c 00 01 c0 0c  00 1c 00 01 00 00 01 2c   m·····
0060  00 10 26 06 47 00 00 20  00 00 00 00 00 00 68 1a   ··&·G··
0070  01 94 c0 0c 00 1c 00 01  00 00 01 2c 00 10 26 06   ·····
0080  47 00 00 20 00 00 00 00  00 00 68 1a 00 94 c0 0c   G··
0090  00 1c 00 01 00 00 01 2c  00 10 26 06 47 00 00 20   ·····, ·
00a0  00 00 00 00 00 00 ac 43  48 2e                     ·····C H
```

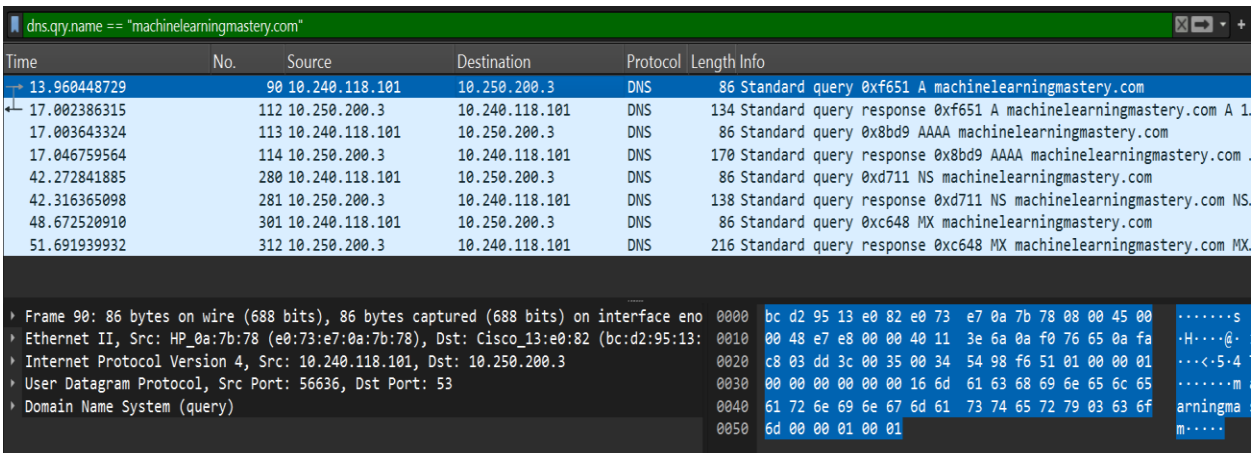
In the terminal for **machinelearningmastery.com,** we observe

- IPv4 →**172.67.72.46**, **104.26.1.148**, **104.26.0.148 &**
- IPV6→**2606:4700:20::681a:94**,**2606:4700:20::681a:194**,**2606:4700:20::ac43:482e**.

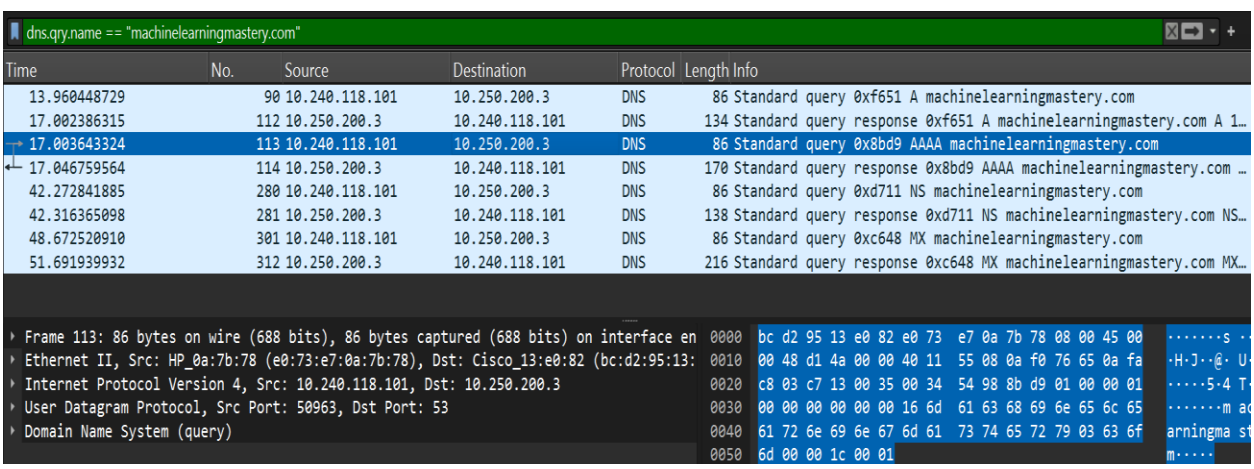
The DNS response packet in **Wireshark** confirms the same addresses. The **Type A** response provides IPv4 addresses, while the **Type AAAA** response provides IPv6 addresses, as shown in the captured DNS query response packets.

Q.2. [2 marks] What are the different types of DNS records you observe in Wireshark?

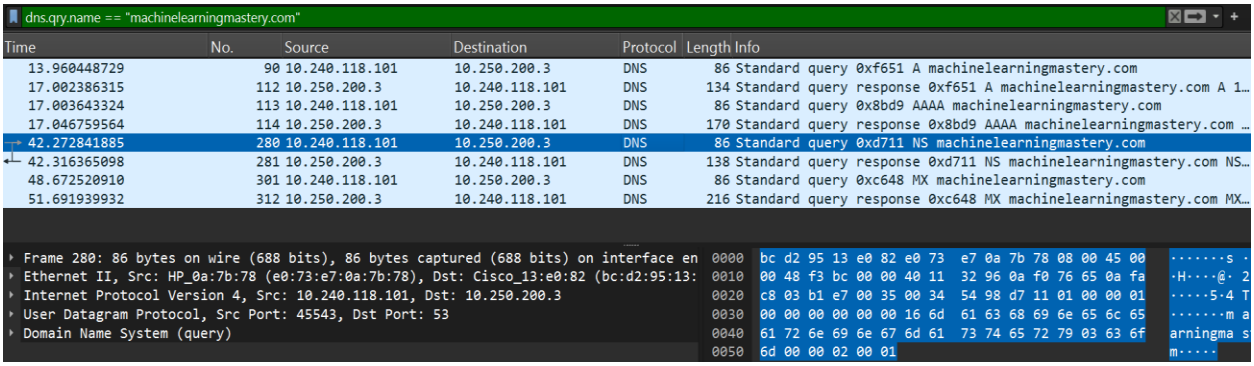
In Wireshark, we observe the following types of DNS records:



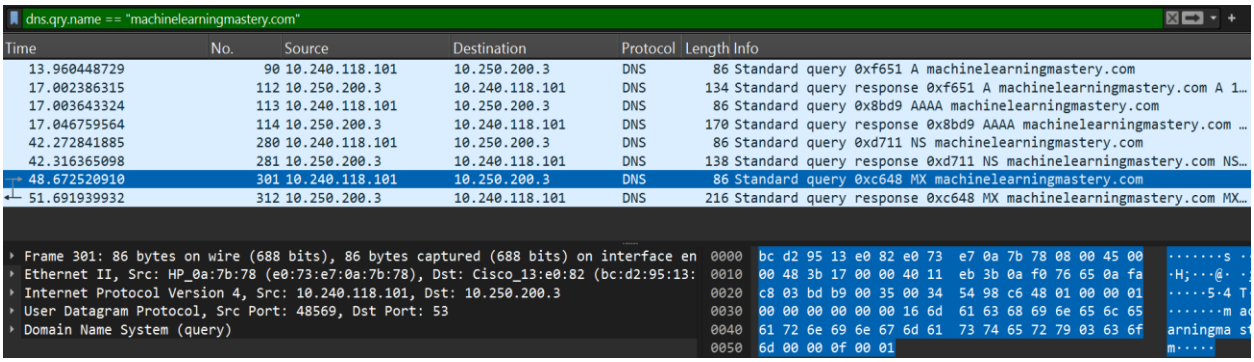
- **A (Address Record):** Provides IPv4 addresses.



- **AAAA (IPv6 Address Record):** Provides IPv6 addresses.

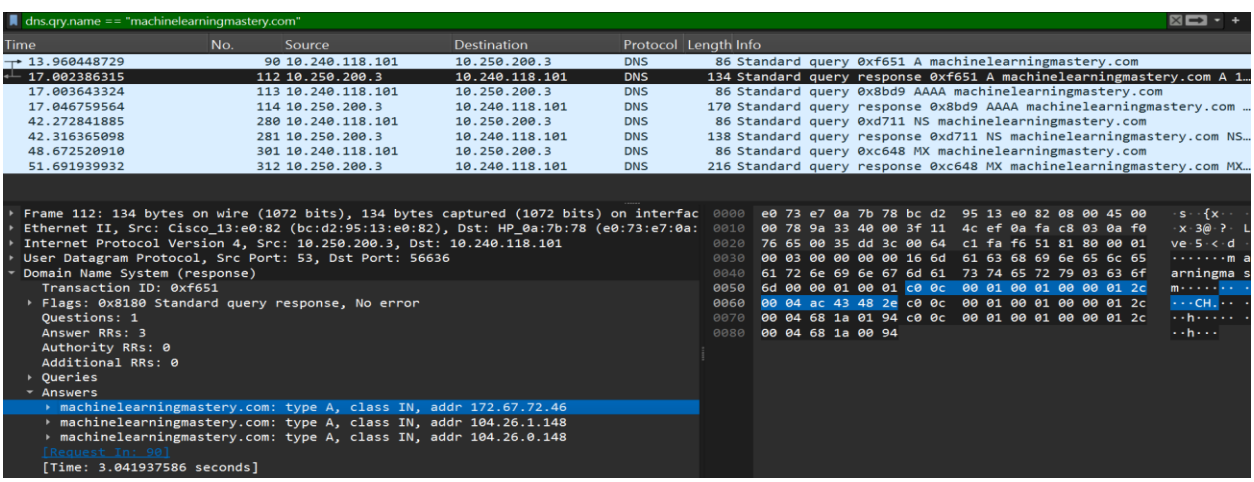


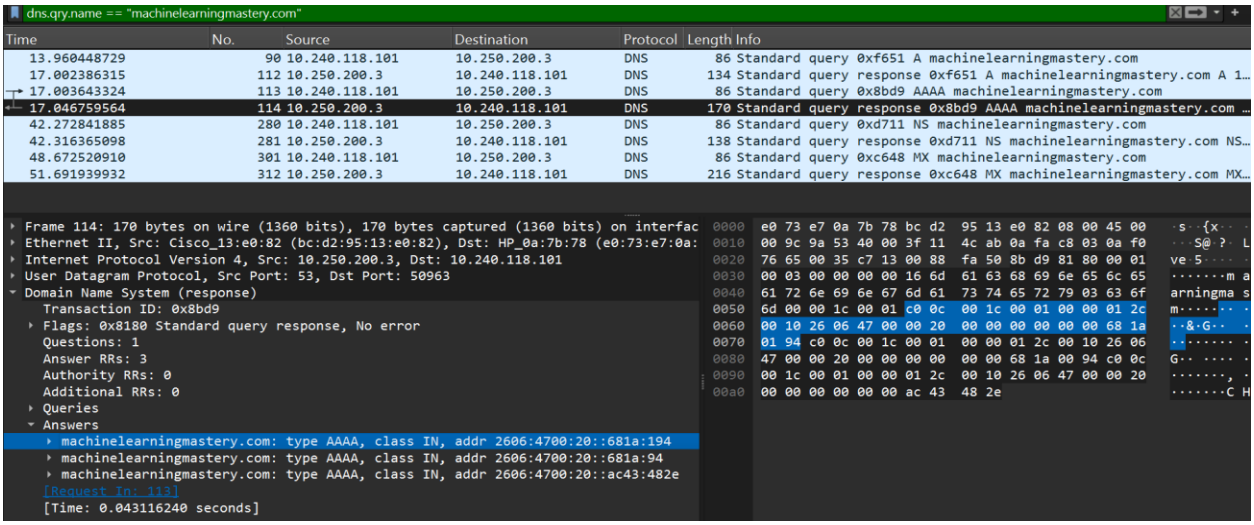
- **NS (Name Server Record):** Specifies the authoritative name servers for the domain.



- **MX (Mail Exchange Record):** Specifies the mail servers for the domain.

Q.3. [3 marks] List out the IP addresses of client (your system), DNS resolver, and the domain you have requested.





IP Address of Client(system)	10.240.118.101
IP Address of DNS resolver	10.250.200.3
IP Address of domain requested	**For type A→** 172.67.72.46, 104.26.1.148, 104.26.0.148 **For type AAAA→** 2606:4700:20::681a:194, 2606:4700:20::681a:94, 2606:4700:20::ac43:482e

Q.4. [3 marks] What are the source and destination port numbers the DNS request made? What is the significance of the destination port and also which transport layer protocol is used to make the request?

When a DNS request is made, the source port and destination port number are (from **Q.2** images)-

Source and Destination Port Numbers in a DNS Request:

- The **source port** is randomly assigned by the client for each DNS request.
- The **destination port** is **port 53**, which is the well-known port used for DNS services.

Significance of the Destination Port:

- **Port 53** is the standard port for DNS (Domain Name System) queries.
- It is used to resolve domain names (e.g., google.com) into IP addresses.

- This port facilitates communication between clients (such as your computer) and DNS servers.

DNS request – `type=[RECORD]`	Source Port Number	Destination Port Number
`A`	56636	53
`AAAA`	50963	53
`NS`	45543	53
`MX`	48569	53

Transport Layer Protocol Used for DNS Requests:

- **UDP (User Datagram Protocol)** is primarily used because:
    - It is faster and has minimal overhead (no connection setup required).
    - Most DNS queries and responses are small enough to fit in a single UDP packet.

  Thus, DNS primarily uses UDP on port 53 for quick lookups.