

**CS 315 : Computer Networks Lab**  
**Assignment - 4**  
**Wireshark Lab: DNS**

**Ayush Mallick**  
**CS22BT008**

---

**Part-2**

**2.1**

```
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: 142.250.193.142
Name:   google.com
Address: 2404:6800:4007:827::200e
```

1.    **iitdh.ac.in**  
      Domain IP address : *10.195.250.62*
- google.com**  
      Domain IP address : *142.250.193.142*
2.    **iitdh.ac.in**  
      DNS resolver IP address : *127.0.0.53*
- google.com**  
      DNS resolver IP address : *127.0.0.53*
3.    **iitdh.ac.in**  
      Port number : *53*
- google.com**  
      Port number : *53*

#### 4. iitdh.ac.in

```
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:~$ dig iitdh.ac.in

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> iitdh.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63171
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;iitdh.ac.in.                IN      A

;; ANSWER SECTION:
iitdh.ac.in.                5987    IN      A      10.195.250.62

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Jan 27 09:21:00 IST 2025
;; MSG SIZE rcvd: 56
```

#### google.com

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ host google.com
google.com has address 142.250.205.238
google.com has IPv6 address 2404:6800:4007:820::200e
google.com mail is handled by 10 smtp.google.com.
```

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

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52837
;; 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.                34      IN      A      142.250.205.238

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Jan 27 09:23:07 IST 2025
;; MSG SIZE rcvd: 55
```

## 2.2

### 1. **iitdh.ac.in**

*idns.iitdh.ac.in*

```
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:
```

### **google.com**

*ns1.google.com*

*ns2.google.com*

*ns3.google.com*

*ns4.google.com*

```
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 = ns4.google.com.
google.com       nameserver = ns3.google.com.
google.com       nameserver = ns1.google.com.

Authoritative answers can be found from:
```

## 2.3

### 1. **A** : Maps a domain name to an IPv4 address.

**NS** : Specifies the authoritative nameservers for the domain.

**MX** : Specifies mail servers responsible for receiving emails for the domain.

### 2. **A** :

*142.250.193.142*

**NS** :

*ns1.google.com*

*ns2.google.com*

*ns3.google.com*

*ns4.google.com*

**MX** :

*smtp.google.com*

```
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: 142.250.193.142
```

```
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:
```

## 2.4

### 1. using ns1.google.com

IPv4 : 142.250.193.142

IPv6 : 2404:6800:4007:820::200e

### using ns2.google.com

IPv4 : 142.250.193.142

IPv6 : 2404:6800:4007:820::200e

### using ns3.google.com

IPv4 : 142.250.193.142

IPv6 : 2404:6800:4007:820::200e

### using ns4.google.com

IPv4 : 142.250.193.142

IPv6 : 2404:6800:4007:820::200e

2. **ns1.google.com**  
IP address : 216.239.32.10

**ns2.google.com**  
IP address : 216.239.34.10

**ns3.google.com**  
IP address : 216.239.36.10

**ns4.google.com**  
IP address : 216.239.38.10

```
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 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
```

```
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
```

## 2.5

1. CMD1 (*nslookup drive.google.com*) resolves using the system's default DNS resolver and provides Non-authoritative answer in most cases.

CMD2 (*nslookup drive.google.com ns1.google.com*) resolves directly using the specified authoritative nameserver (*ns1.google.com*).

2. CMD2 queries the authoritative nameserver directly (*ns1.google.com*), which provides the authoritative answer. Thus, it does not include a Non-authoritative answer line.

```
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: 142.250.71.14
Name:   drive.google.com
Address: 2404:6800:4007:828::200e
```

```
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
```

## Part-3

1. IP addresses shown : 3 (each of IPv4 and IPv6)

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

Yes, the same is observed in the DNS response packets.

```

  ▾ Domain Name System (response)
    Transaction ID: 0x8c2d
    ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    ▾ Queries
      ▾ machinelearningmastery.com: type A, class IN
        Name: machinelearningmastery.com
        [Name Length: 26]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
      ▾ Answers
        ▾ machinelearningmastery.com: type A, class IN, addr 104.26.0.148
          Name: machinelearningmastery.com
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 300 (5 minutes)
          Data length: 4
          Address: 104.26.0.148
        ▾ machinelearningmastery.com: type A, class IN, addr 172.67.72.46
          Name: machinelearningmastery.com
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 300 (5 minutes)
          Data length: 4
          Address: 172.67.72.46
        ▾ machinelearningmastery.com: type A, class IN, addr 104.26.1.148
          Name: machinelearningmastery.com
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 300 (5 minutes)
          Data length: 4
          Address: 104.26.1.148
        [Request In: 36]
        [Time: 3.232812878 seconds]

  ▾ Domain Name System (response)
    Transaction ID: 0xffbb
    ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    ▾ Queries
      ▾ machinelearningmastery.com: type AAAA, class IN
        Name: machinelearningmastery.com
        [Name Length: 26]
        [Label Count: 2]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
      ▾ Answers
        ▾ machinelearningmastery.com: type AAAA, class IN, addr 2606:4700:20::681a:194
          Name: machinelearningmastery.com
          Type: AAAA (IPv6 Address) (28)
          Class: IN (0x0001)
          Time to live: 300 (5 minutes)
          Data length: 16
          AAAA Address: 2606:4700:20::681a:194
        ▾ machinelearningmastery.com: type AAAA, class IN, addr 2606:4700:20::ac43:482e
          Name: machinelearningmastery.com
          Type: AAAA (IPv6 Address) (28)
          Class: IN (0x0001)
          Time to live: 300 (5 minutes)
          Data length: 16
          AAAA Address: 2606:4700:20::ac43:482e
        ▾ machinelearningmastery.com: type AAAA, class IN, addr 2606:4700:20::681a:94
          Name: machinelearningmastery.com
          Type: AAAA (IPv6 Address) (28)
          Class: IN (0x0001)
          Time to live: 300 (5 minutes)
          Data length: 16
          AAAA Address: 2606:4700:20::681a:94
        [Request In: 42]
        [Time: 0.046016084 seconds]
```

2. A Record : Maps the domain to IPv4 addresses.

AAAA Record : Maps the domain to IPv6 addresses.

3. Client IP address : 10.240.118.106

DNS resolver IP address :10.250.200.3

Domain IP addresses : 104.26.0.148, 172.67.72.46, 104.26.1.148

dns						
No.	Time	Source	Destination	Protocol	Length	Info
36	11.442859289	10.240.118.106	10.250.200.3	DNS	86	Standard query 0x8c2d A machinelearningmastery.com
41	14.675672167	10.250.200.3	10.240.118.106	DNS	134	Standard query response 0x8c2d A machinelearningmastery.com A ...
42	14.676830359	10.240.118.106	10.250.200.3	DNS	86	Standard query 0xffbb AAAA machinelearningmastery.com
43	14.722846443	10.250.200.3	10.240.118.106	DNS	170	Standard query response 0xffbb AAAA machinelearningmastery.com...

#### 4. for A record (IPv4)

Source port number : 53325

Destination port number : 53

#### for AAAA record (IPv6)

Source port number : 43612

Destination port number : 53

Port 53 is designated for DNS traffic, allowing queries to resolve domain names to IP addresses.

Transport Layer Protocol used :

UDP (User Datagram Protocol)

- ▼ User Datagram Protocol, Src Port: 53325, Dst Port: 53
  - Source Port: 53325
  - Destination Port: 53
  - Length: 52
  - Checksum: 0x549d [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 8]
  - ▼ [Timestamps]
    - [Time since first frame: 0.000000000 seconds]
    - [Time since previous frame: 0.000000000 seconds]
  - UDP payload (44 bytes)
- ▼ User Datagram Protocol, Src Port: 43612, Dst Port: 53
  - Source Port: 43612
  - Destination Port: 53
  - Length: 52
  - Checksum: 0x549d [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 10]
  - ▼ [Timestamps]
    - [Time since first frame: 0.000000000 seconds]
    - [Time since previous frame: 0.000000000 seconds]
  - UDP payload (44 bytes)