Sohag University
Faculty of Engineering

3rd-year Communication Dept.
Network Fundamentals

LAB 4

By: Zaynab Al-Ariny

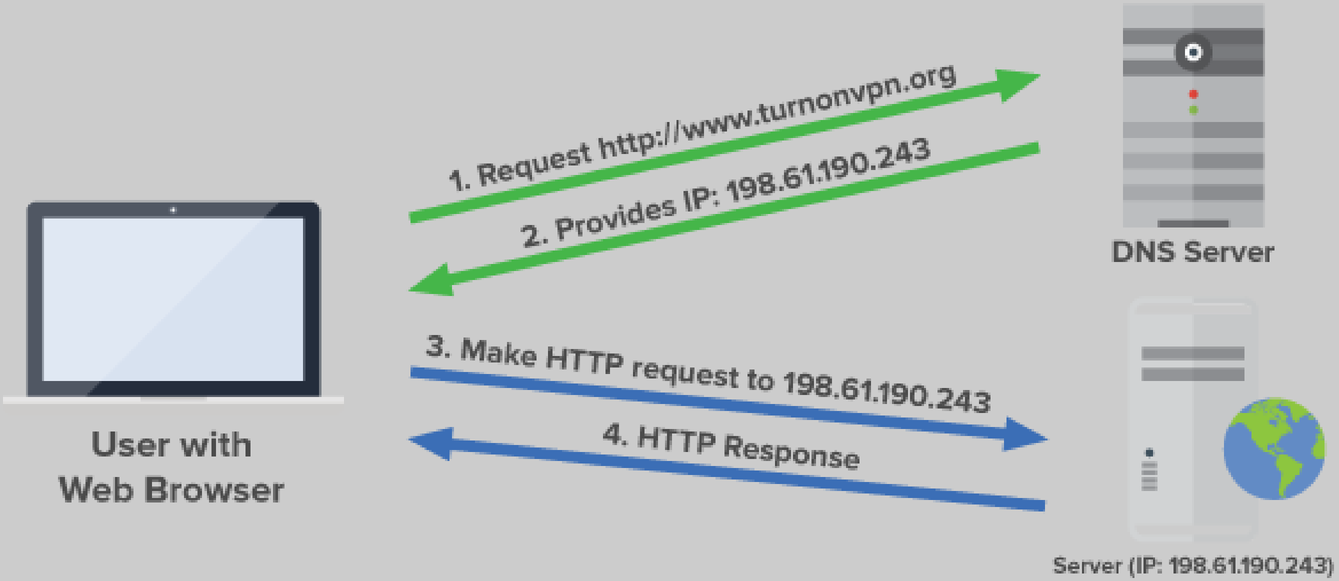
Objectives :

→ Investigate DNS protocol

DNS Protocol

- What is DNS?

→ Domain Name System (DNS) is application layer protocol .
→ DNS translates Internet hostnames to IP addresses.


1. Request http://www.turnonvpn.org
2. Provides IP: 198.61.190.243
DNS Server
3. Make HTTP request to 198.61.190.243
4. HTTP Response
User with
Web Browser
Server (IP: 198.61.190.243)

→ DNS message format can vary, depending on ether it is query or Reply

- DNS Query

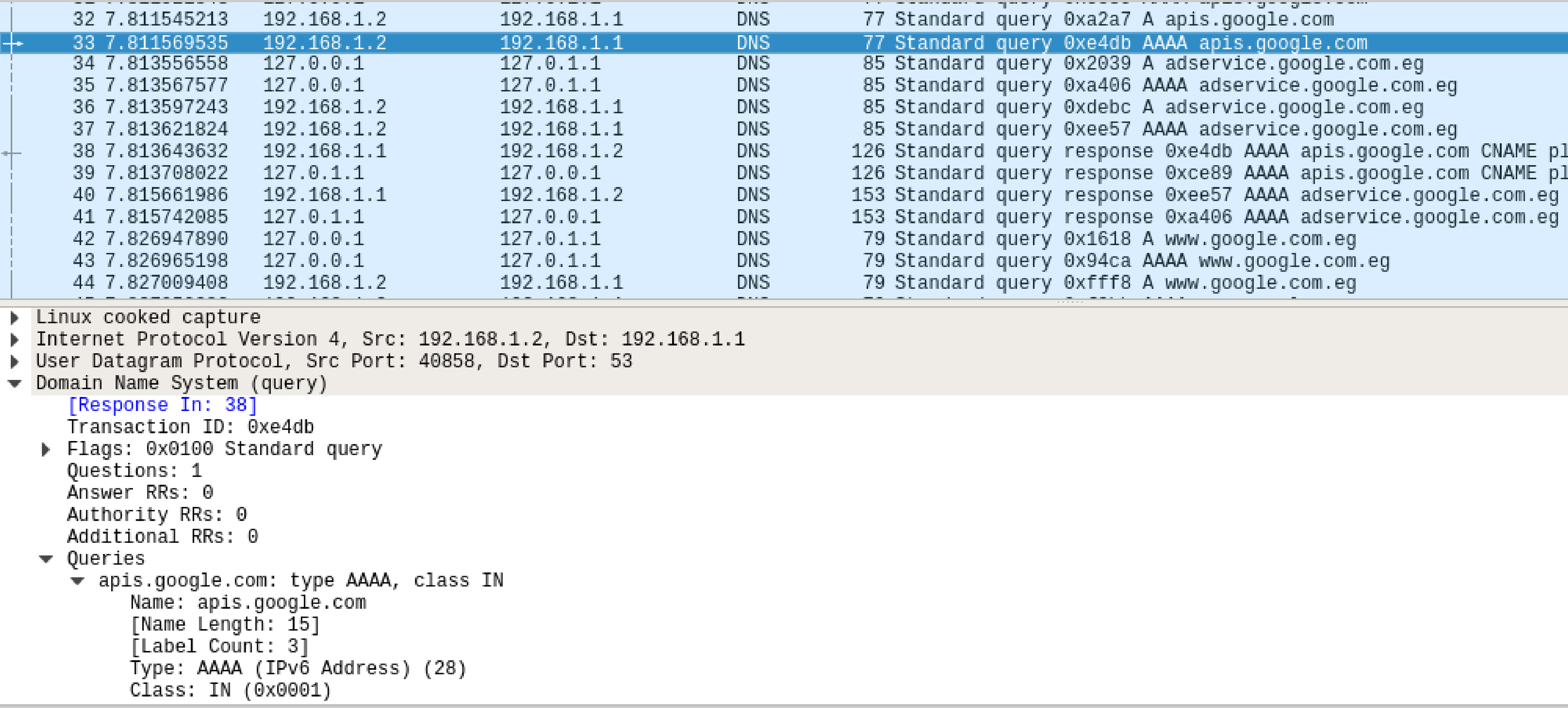
→ Transction ID
- Match replys to queries

→ Flags
- Specifies the operation (query)

→ Questions
- Number of entries in Questions section

→ Answer RRs
- Number of entries in Answer section
- always set to Zero in Query

→ Queries
- **query domain name** for which the query is send
- **query type** that define type of question A, AAAA, MX, CNAME
- **query class**



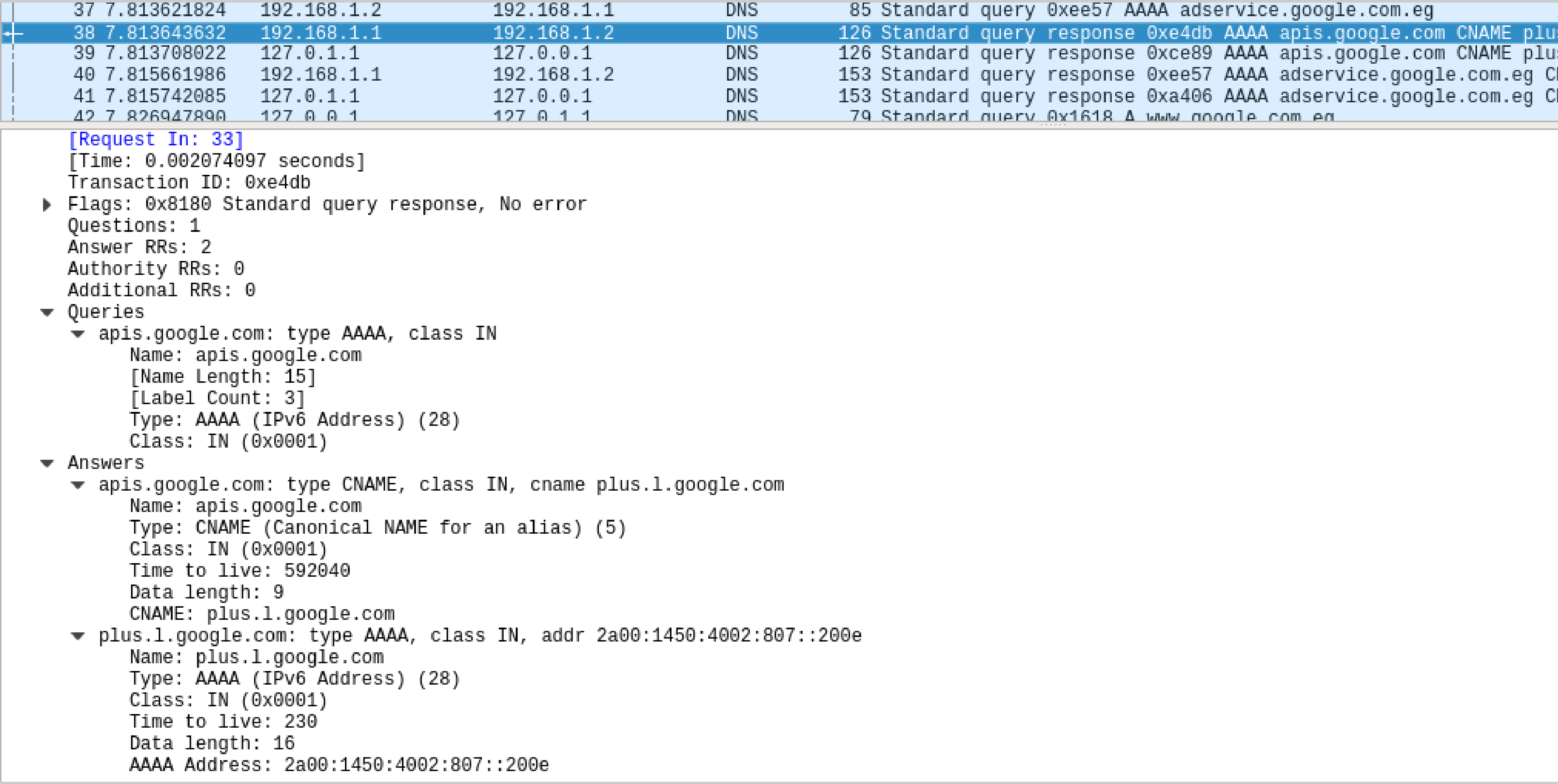
```
32 7.811545213   192.168.1.2    192.168.1.1    DNS     77 Standard query 0xa2a7 A apis.google.com
33 7.811569535   192.168.1.2    192.168.1.1    DNS     77 Standard query 0xe4db AAAA apis.google.com
34 7.813556558   127.0.0.1      127.0.1.1      DNS     85 Standard query 0x2039 A adservice.google.com.eg
35 7.813567577   127.0.0.1      127.0.1.1      DNS     85 Standard query 0xa406 AAAA adservice.google.com.eg
36 7.813597243   192.168.1.2    192.168.1.1    DNS     85 Standard query 0xdebc A adservice.google.com.eg
37 7.813621824   192.168.1.2    192.168.1.1    DNS     85 Standard query 0xee57 AAAA adservice.google.com.eg
38 7.813643632   192.168.1.1    192.168.1.2    DNS    126 Standard query response 0xe4db AAAA apis.google.com CNAME pl
39 7.813708022   127.0.1.1      127.0.0.1      DNS    126 Standard query response 0xce89 AAAA apis.google.com CNAME pl
40 7.815661986   192.168.1.1    192.168.1.2    DNS    153 Standard query response 0xee57 AAAA adservice.google.com.eg
41 7.815742085   127.0.1.1      127.0.0.1      DNS    153 Standard query response 0xa406 AAAA adservice.google.com.eg
42 7.826947890   127.0.0.1      127.0.1.1      DNS     79 Standard query 0x1618 A www.google.com.eg
43 7.826965198   127.0.0.1      127.0.1.1      DNS     79 Standard query 0x94ca AAAA www.google.com.eg
44 7.827009408   192.168.1.2    192.168.1.1    DNS     79 Standard query 0xfff8 A www.google.com.eg
```

```
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 40858, Dst Port: 53
Domain Name System (query)
    [Response In: 38]
    Transaction ID: 0xe4db
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        apis.google.com: type AAAA, class IN
            Name: apis.google.com
            [Name Length: 15]
            [Label Count: 3]
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
```

- DNS Reply

→ Transction ID
→ Flags
- Specifies the operation (query response)
- response status code

→ Questions
→ Answer RRs
→ Queries
→ Answers
- **domain name**
- **type**
- **class**
- **TTL :**how long this record can be cached



```
 37 7.813621824   192.168.1.2          192.168.1.1          DNS          85 Standard query 0xee57 AAAA adservice.google.com.eg
 38 7.813643632   192.168.1.1          192.168.1.2          DNS         126 Standard query response 0xe4db AAAA apis.google.com CNAME plu
 39 7.813708022   127.0.1.1            127.0.0.1            DNS         126 Standard query response 0xce89 AAAA apis.google.com CNAME plu
 40 7.815661986   192.168.1.1          192.168.1.2          DNS         153 Standard query response 0xee57 AAAA adservice.google.com.eg C
 41 7.815742085   127.0.1.1            127.0.0.1            DNS         153 Standard query response 0xa406 AAAA adservice.google.com.eg C
 42 7.826947890   127.0.0.1            127.0.1.1            DNS          79 Standard query 0x1618 A www.google.com.eg
```

```
    [Request In: 33]
    [Time: 0.002074097 seconds]
    Transaction ID: 0xe4db
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ apis.google.com: type AAAA, class IN
        Name: apis.google.com
        [Name Length: 15]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  ▼ Answers
    ▼ apis.google.com: type CNAME, class IN, cname plus.l.google.com
        Name: apis.google.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 592040
        Data length: 9
        CNAME: plus.l.google.com
    ▼ plus.l.google.com: type AAAA, class IN, addr 2a00:1450:4002:807::200e
        Name: plus.l.google.com
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 230
        Data length: 16
        AAAA Address: 2a00:1450:4002:807::200e
```

Let’s have fun

1. How to use **nslookup** command to resolve a hostname or IP address?
   - Find IP address of “wireshark.com”
   - Find hostname of “108.174.10.10”

   Hint :
   ```
   $ nslookup DOMAIN  # returns IP address
   $ nslookup IPADDRESS  # returns domain name
   ```
2. what is the IP address of your local DNS server?
3. Can you resolve a hostname from a specific DNS server?(ex: ns1.sprintlink.net)

   Hint :
   ```
   $nslookup DOMAIN DNSSERVER
   ```
4. Capture some DNS packets using wireshark. find DNS query and reply messages. Are them sent over UDP or TCP?
5. What is the default port number for the DNS service ?
6. From DNS packets identify the following:
   a. Destination port for the DNS query.
   b. Source port of the DNS reply. (what this port represent?)
   c. Examine the DNS query message.
   d. Examine the DNS reply message.

Bonus !

# Why nslookup command result comes from server IP 127.0.0.1? How You can change this behavior to use your DNS IP ?

# what is DNS query Class ?