Lab 03

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?

```
C:\Users\DELL>nslookup tuoitre.vn
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    tuoitre.vn
Address:  14.225.199.147
```

The IP address of this server: 14.225.199.147

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

```
C:\Users\DELL>nslookup -type=NS www.rca.ac.uk
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
www.rca.ac.uk   canonical name = www.rca.ac.uk.cdn.cloudflare.net

cloudflare.net
        primary name server = ns1.cloudflare.net
        responsible mail addr = dns.cloudflare.com
        serial  = 2323811511
        refresh = 10000 (2 hours 46 mins 40 secs)
        retry   = 2400 (40 mins)
        expire  = 604800 (7 days)
        default TTL = 1800 (30 mins)
```

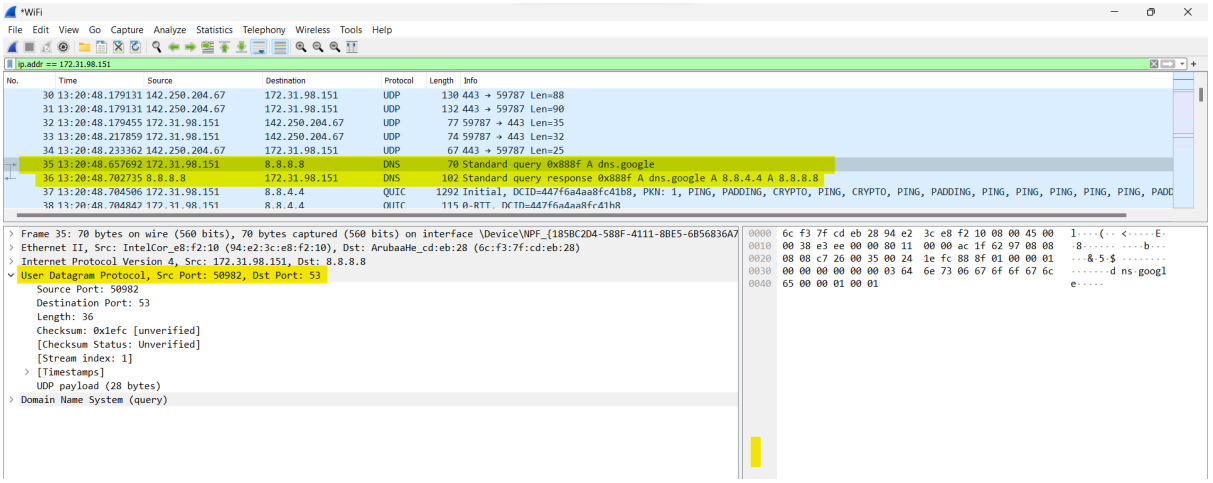
the authoritative DNS servers: ns1.cloudflare.net

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

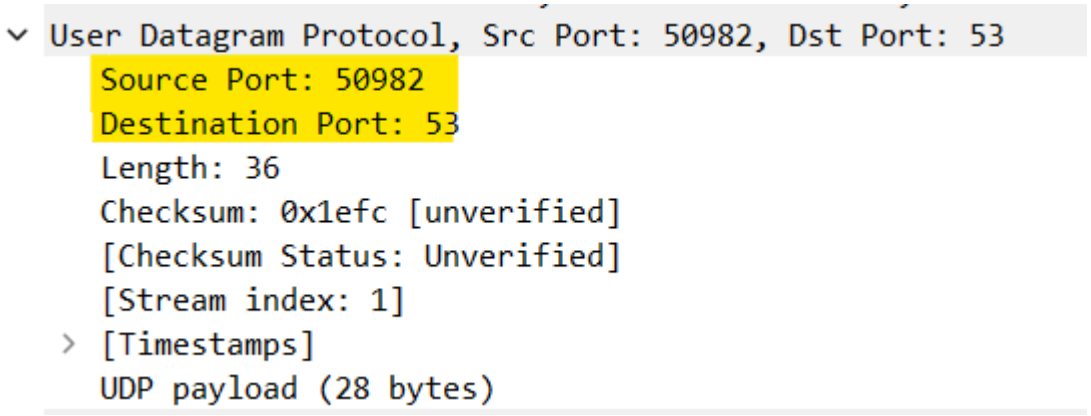
```
C:\Users\DELL>nslookup rca.ac.uk mail.yahoo.com
Server:  e2.ycpi.vip.hkb.yahoo.com
Address:  180.222.116.12

Non-authoritative answer:
Name:    rca.ac.uk
Address:  89.106.200.1
```

It's IP address: 89.106.200.1

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
UDP



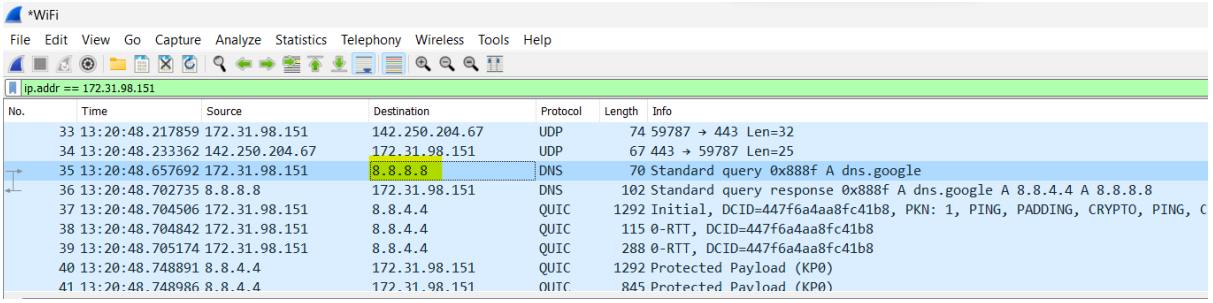
5. What is the destination port for the DNS query message? What is the source port of DNS response message?



Destination Port: 53
Source Port: 50982

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

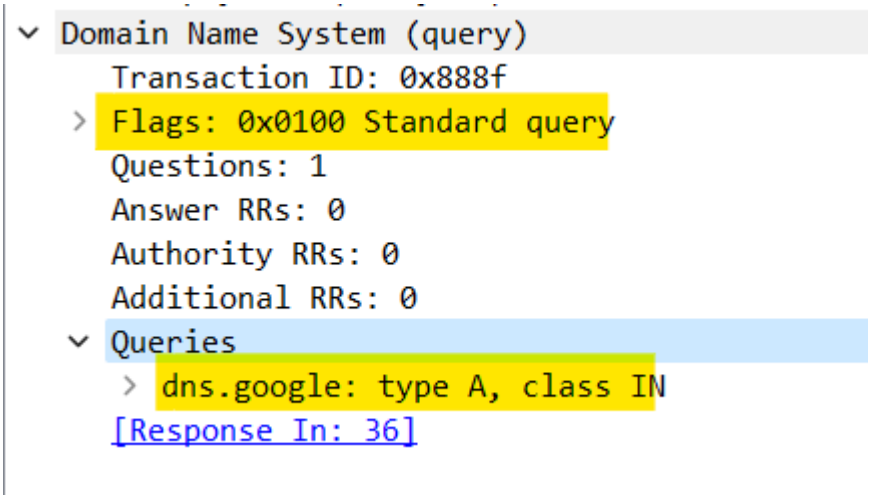
The DNS query was sent to IP address: 8.8.8.8
IP address of my local DNS server: 8.8.8.8
These two IP addresses are the same.




```
Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   Physical Address. . . . . . . . . : 94-E2-3C-E8-F2-10
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6895:54fc:4298:ee12%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.31.98.151(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Lease Obtained. . . . . . . . . . : 31 October 2023 09:09:24
   Lease Expires . . . . . . . . . . : 02 November 2023 01:04:48
   Default Gateway . . . . . . . . . : 172.31.98.1
   DHCP Server . . . . . . . . . . . : 172.31.98.1
   DHCPv6 IAID . . . . . . . . . . . : 76866108
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-90-9C-92-60-18-95-4B-C7-D1
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

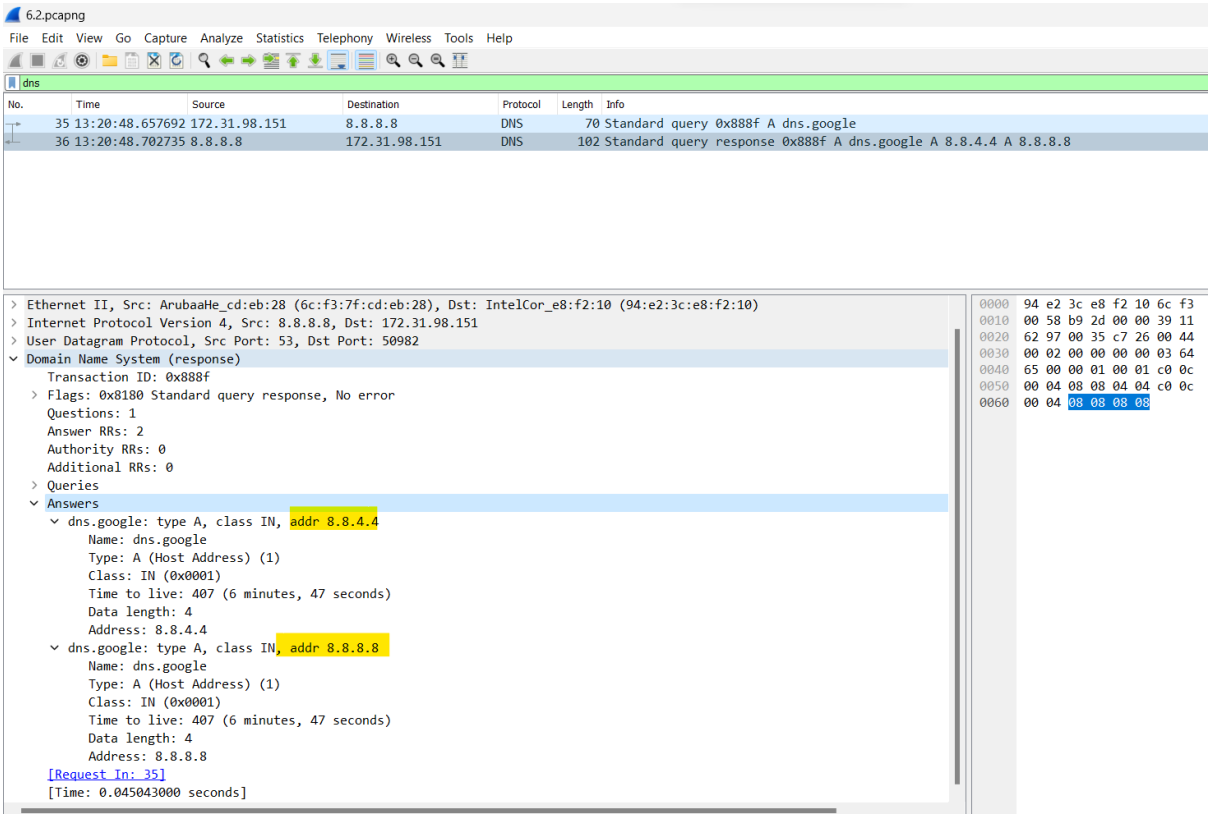
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Type" of DNS query was A.
The query message did not contain any "answers".



8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

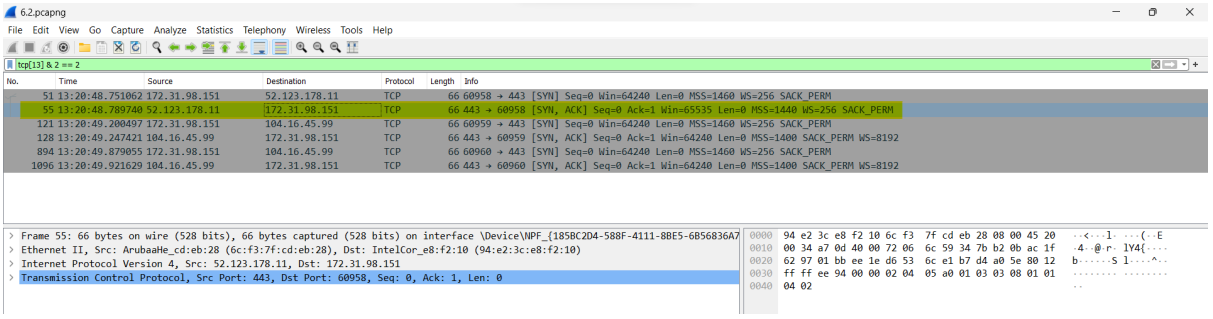
Two answers are provided. They contain the information for www.ietf.org:



9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The destination IP address of the SYN packet correspond is 172.31.98.151

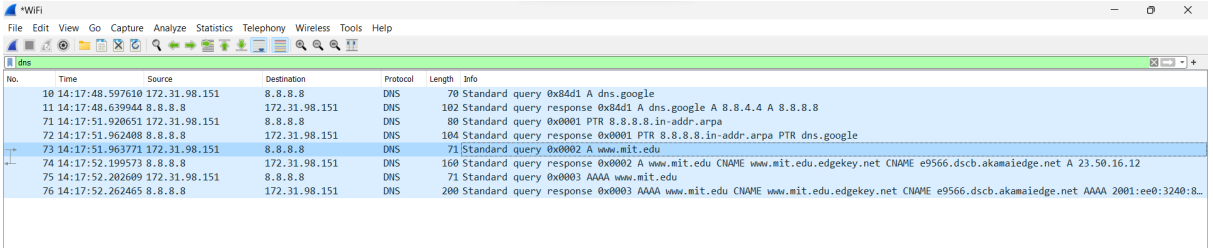
Yes, it is the IP address for www.ielf.org



10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

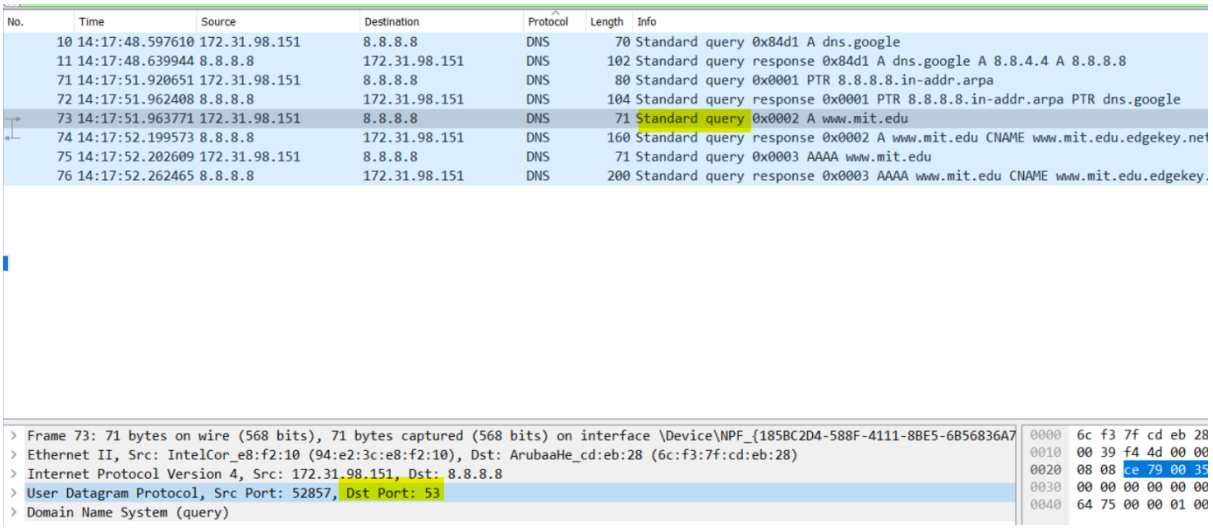
No. It uses the answer from the DNS response

ignore the first two sets of queries/responses.

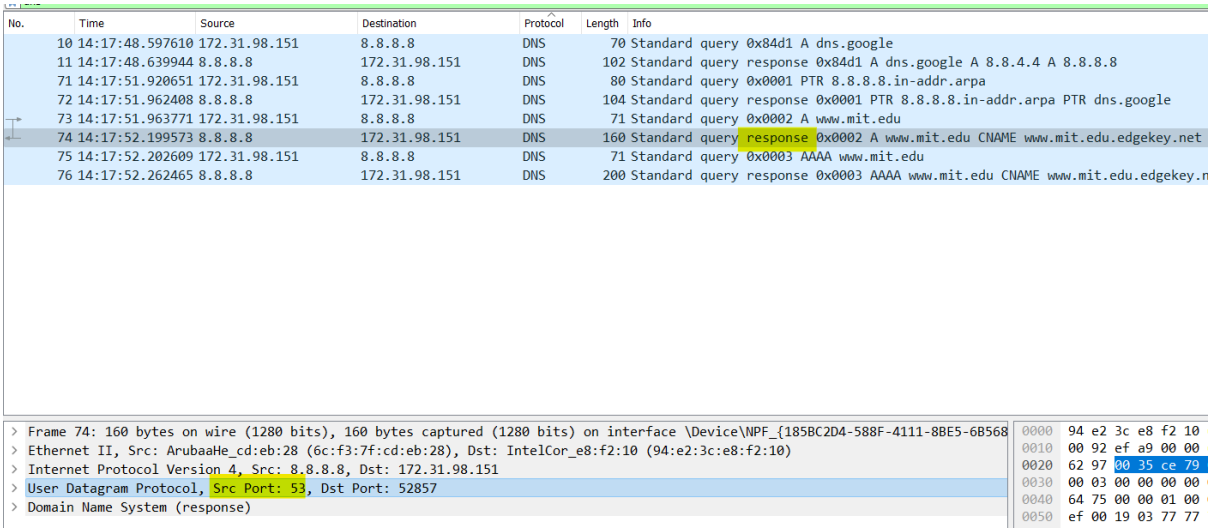


11. What is the destination port for the DNS query message? What is the source port of DNS response messages?

The destination port for the DNS query message is 53.



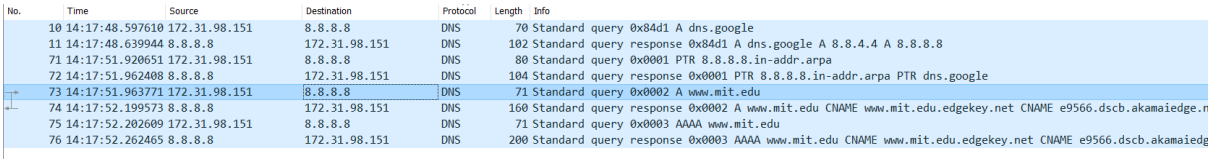
The source port of DNS response messages is 53.



12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The DNS query message sent to IP address: 8.8.8.8

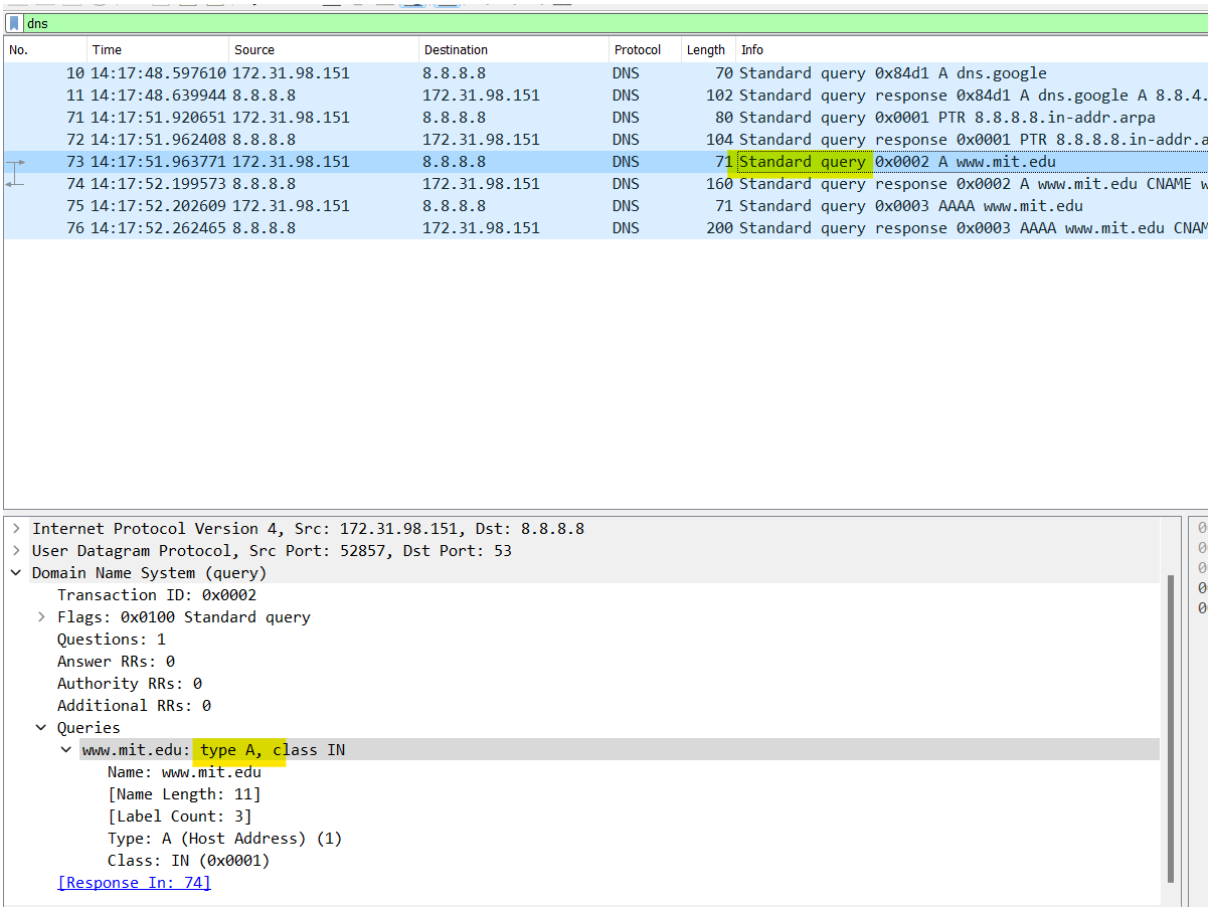
Yes. The IP address of my default local DNS server also is 8.8.8.8



13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

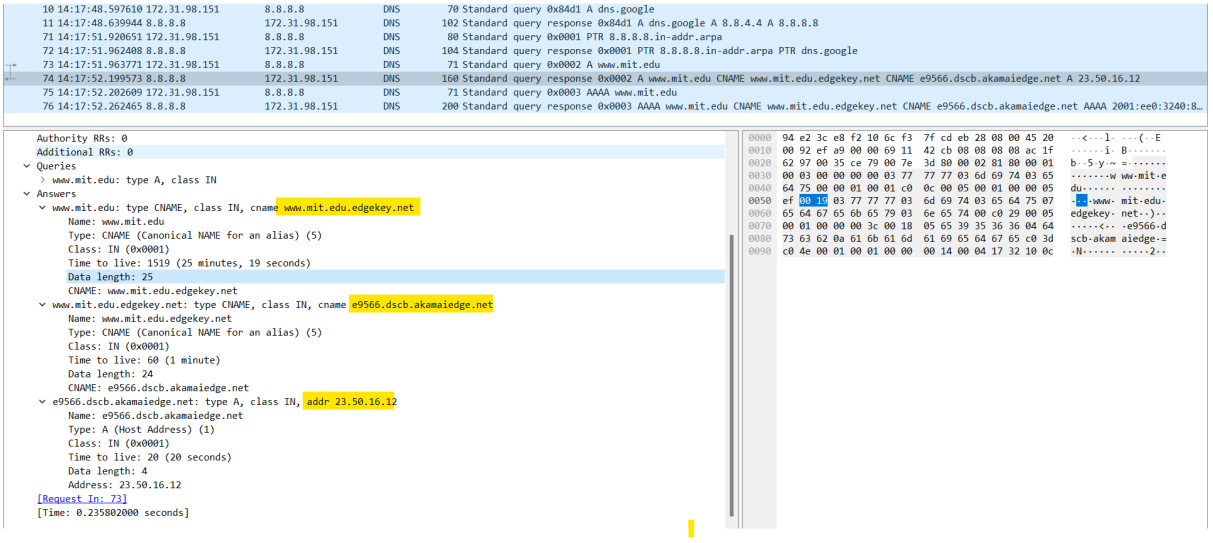
Type" of DNS query was A.

The query message did not contain any “answers”.



14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Three answers are provided. They contain the information for www.mit.edu:

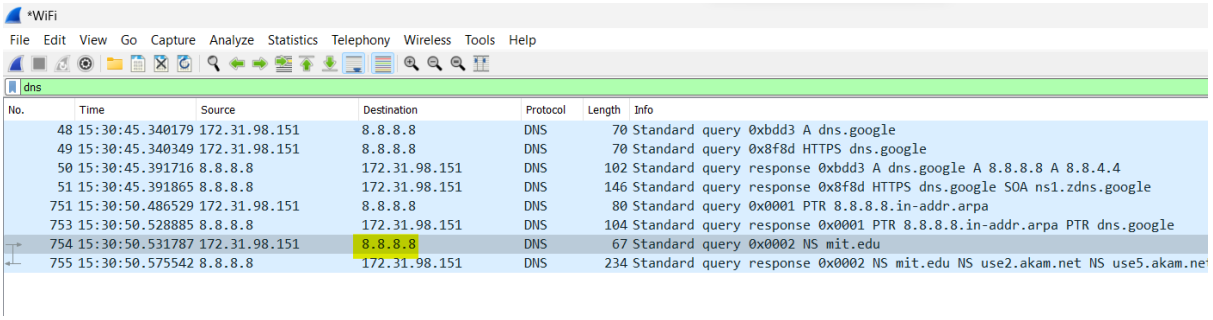


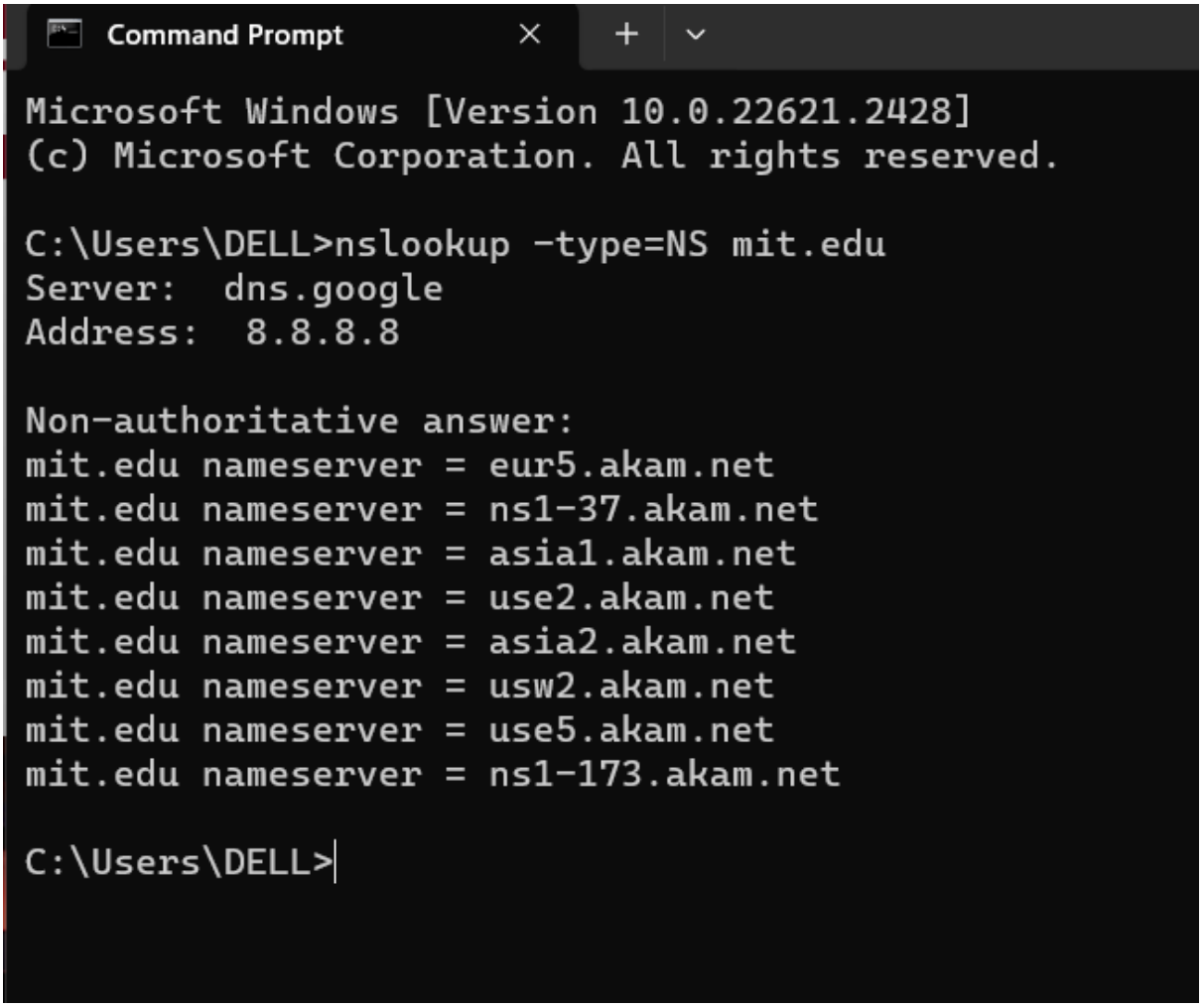
15. Screenshot

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The DNS query was sent to IP address: 8.8.8.8

IP address of my local DNS server: 8.8.8.8





17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Type" of DNS query was NS.

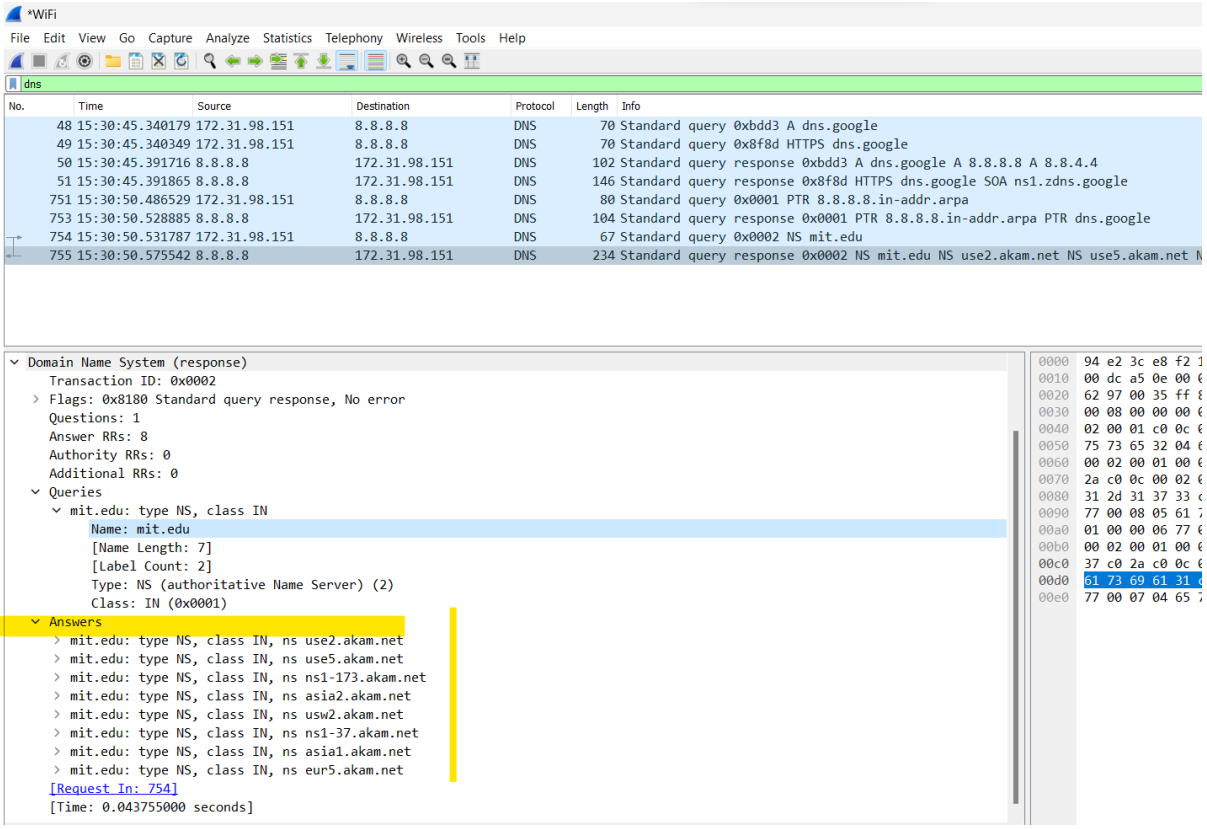
The query message did not contain any "answers".

```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 755]
```

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

The response message provides 8 MIT nameservers.

The response message does not also provide the IP address of the nameservers.

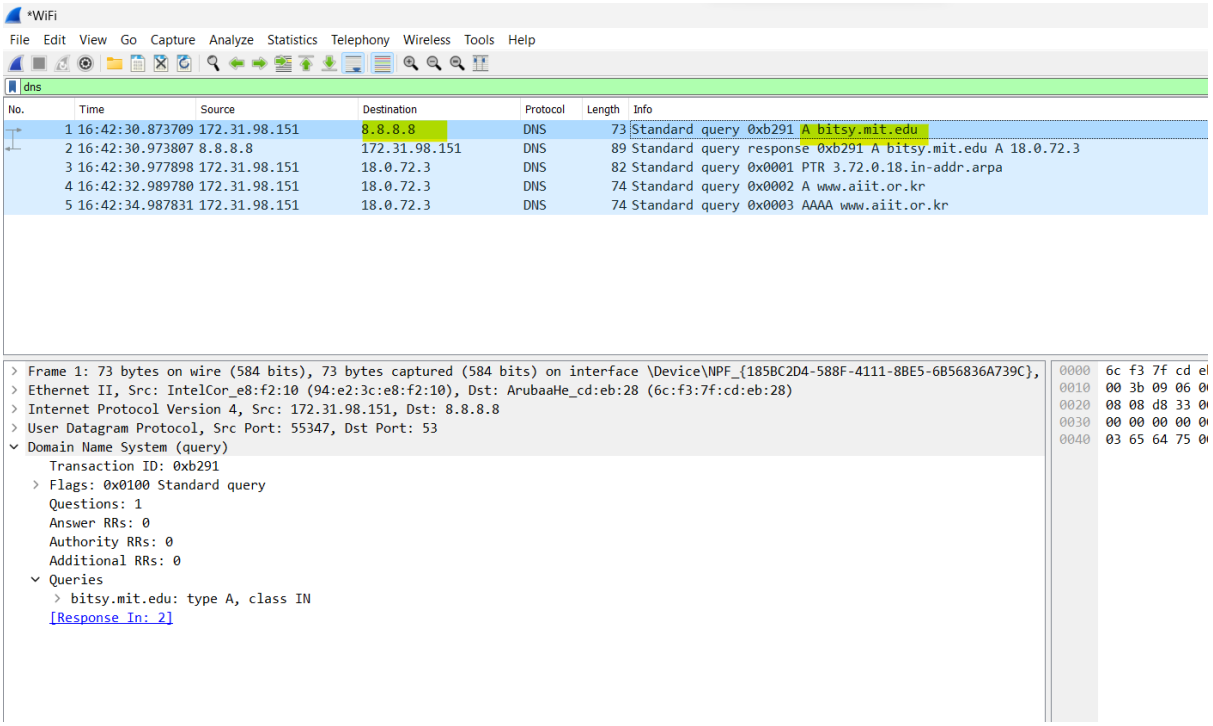


19. Screenshot

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

The DNS query was sent to IP address: 8.8.8.8

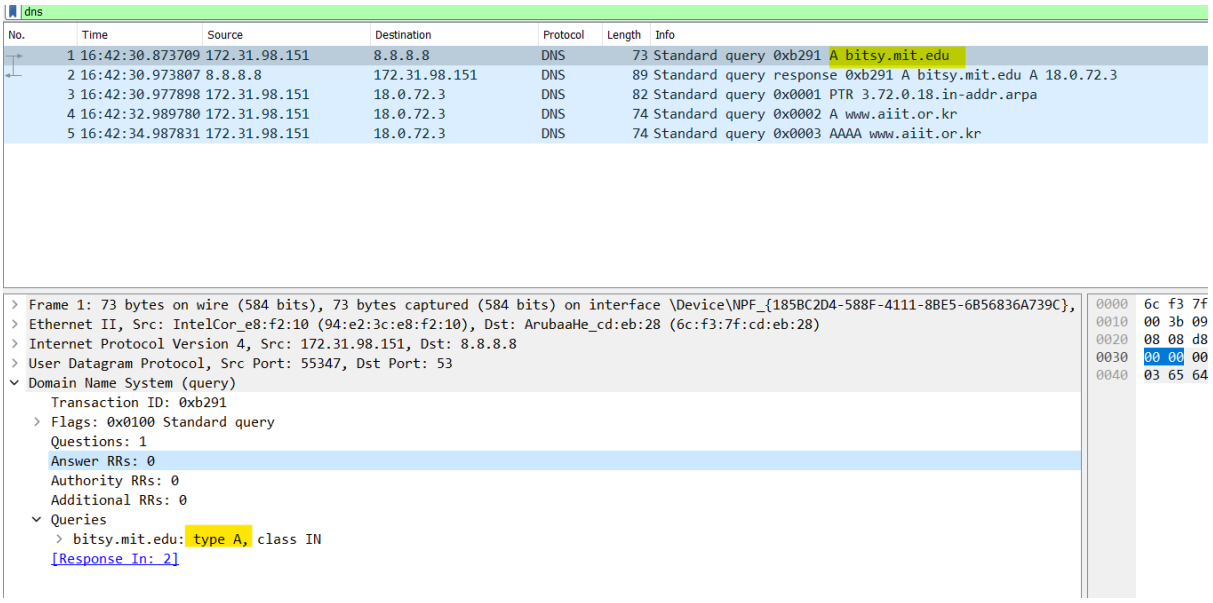
IP address of my local DNS server: 8.8.8.8



21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

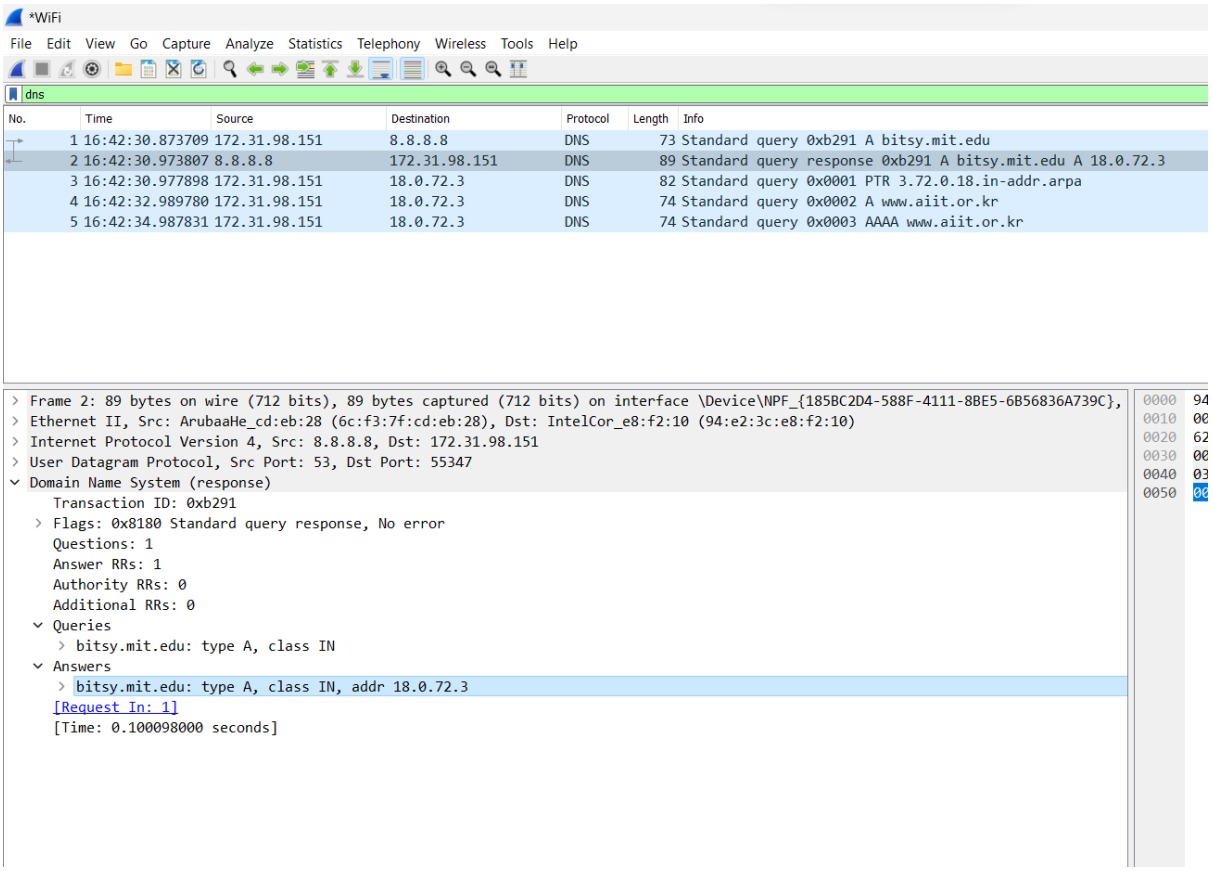
Type" of DNS query was A.

The query message did not contain any "answers".



22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

One answer is provided. They contain the information for bitsy.mit.edu:



23.Screenshot.

Additional:

24. What is Dynamic DNS? Give a brief introduction about Dynamic DNS? Why do we need Dynamic DNS?

- Dynamic DNS, also known as Dynamic Domain Name System (DDNS), is a system that enables devices with dynamic IP addresses to be accessed easily using a domain name.
- **A brief introduction about Dynamic DNS:**
  In a typical scenario, internet service providers (ISPs) assign dynamic IP addresses to their customers, which means that the IP address can change over time. However, most internet resources, such as websites or servers, are usually accessed using domain names.
- **We need Dynamic DNS because:**
  Dynamic DNS solves the problem of accessing devices with changing IP addresses by dynamically updating the IP address associated with a domain name. It works by running a piece of software or using a router that periodically communicates with a DDNS provider, notifying it of any IP address changes. The DDNS provider then updates the DNS records for the associated domain name, ensuring it points to the correct IP address.

25. List out some (at least 5) popular Dynamic DNS providers. Briefly compare them

Here are five popular Dynamic DNS providers:

1. **DynDNS:** DynDNS, now called Dyn, is one of the oldest and well-known dynamic DNS providers. It offers a range of services and features, including various DNS update methods, multiple domain support, and advanced security options. However, some of its services may require a paid subscription.

2. **No-IP:** No-IP provides a simple and user-friendly dynamic DNS service. It offers a free plan that allows users to manage up to three domain names and offers various update clients and integrations. No-IP also offers affordable paid plans with additional features and support.

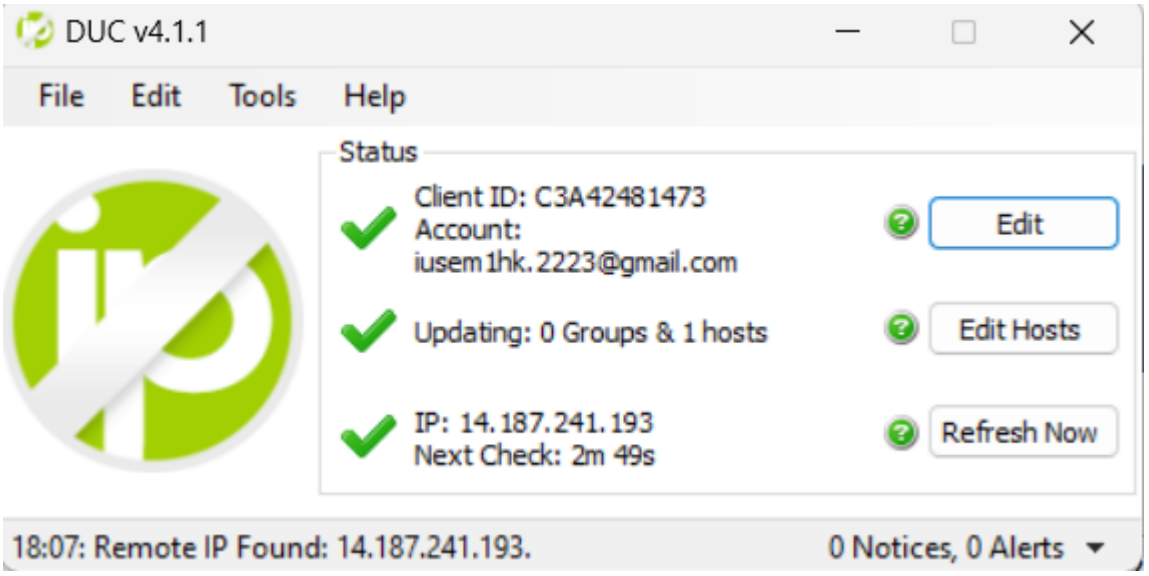
3. **DuckDNS:** DuckDNS is a free dynamic DNS service that focuses on simplicity and ease of use. It doesn't require any account registration and provides a straightforward API for updating DNS records. While it may lack some advanced features, it is a popular choice for basic DDNS needs**.**

4. **ChangeIP:** ChangeIP offers both free and paid dynamic DNS services. Its free plan includes five hostnames and supports various update protocols. The paid plans provide additional features such as email forwarding, SSL certificates, and extended customer support.

5. **afraid.org:** afraid.org, also known as FreeDNS, is a unique dynamic DNS provider that offers free DDNS services. It allows users to create unlimited subdomains under a wide selection of domain names provided by the service. Although it doesn't offer advanced features like some other providers, it remains popular due to its free and flexible nature.

26. Demonstrate how to use Dynamic DNS:

- **Setup a SIMPLE web server, ftp server or something similar on your machine (host A)**
- **Register and config Dynamic DNS for host A**
- **Use your partner’s machine (host B) to access the service running on host A**


DUC v4.1.1
File
Edit
Tools
Help
Status
Client ID: C3A42481473
Account:
iusem1hk.2223@gmail.com
Edit
Updating: 0 Groups & 1 hosts
Edit Hosts
IP: 14.187.241.193
Next Check: 2m 49s
Refresh Now
18:07: Remote IP Found: 14.187.241.193.
0 Notices, 0 Alerts