Q1. *Load balancing* refers to distributing incoming network traffic across multiple compute resources. How can DNS be used to load balance services? Give a concrete explanation for google.com.

A domain can correspond to a website, a mail system likewise that is made accessible via internet. It helps faster access to a domain by providing several IP addresses for a single host or domain name which routes traffic between two or more servers.

For google clients are located in the different locations and while accessing it search for the packets to the closest web service, providing low latency to users while using a single virtual IP . Using a single virtual IP means we can increase the time to live (TTL) of our DNS records, which further reduces latency. In this way the load of the traffice is balanced by google.

```
Abhinav Kumar@LAPTOP-HPO3CB59 MINGW64 ~
$ nslookup google.com
Non-authoritative answer:
Server:  dsldevice6.attlocal.net
Address:  2600:1700:1658:4070::1

Name:    google.com
Addresses:  2607:f8b0:4009:806::200e
          142.250.190.142
```

Q2. DNS has been around since 1985 and the core protocol is still being used today. What is the inherent weakness of DNS (as of RFC1035; excluding DNSSEC)? Give an example of how an attacker might utilize it.

Some of the threats against the DNS are various forms of packet interception like monkey in the middle attacks, eavesdropping on requests combined with spoofed responses that beat the real responses back to the resolver. the attacker can simply tell either party (usually the resolver) whatever it wants that party to believe. While packet interception attacks are far from unique to DNS, DNS's usual behavior of sending an entire query or response in a single unsigned, unencrypted UDP packet makes these attacks particularly easy for any bad guy with the ability to intercept packets on a shared or transit network. Other weakness is betrayal by trusted server. Trusted server that turns out not to be so trustworthy, whether by accident or by intent. In many cases the trusted server is furnished by the user's ISP and advertised to the client which help the attacker .

Q3. Perform a manual iterative DNS query for mail-relay.iu.edu with dig starting from the root servers. List all commands and their outputs and explain why you issued every command. Do not use tracing features (`dig +trace`) for your final write-down.

I will first connect to root server using below command

dig @b.root-servers.net edu q-A

```
; <<>> DiG 9.16.1-Ubuntu <<>> @b.root-servers.net edu q-A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10552
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8327db0e4da7d1fe0100000061451dedecce5fac3f172511 (good)
;; QUESTION SECTION:
;edu.                           IN      A

;; AUTHORITY SECTION:
edu.                    172800  IN      NS      a.edu-servers.net.
edu.                    172800  IN      NS      b.edu-servers.net.
edu.                    172800  IN      NS      c.edu-servers.net.
edu.                    172800  IN      NS      d.edu-servers.net.
edu.                    172800  IN      NS      e.edu-servers.net.
edu.                    172800  IN      NS      f.edu-servers.net.
edu.                    172800  IN      NS      g.edu-servers.net.
edu.                    172800  IN      NS      h.edu-servers.net.
edu.                    172800  IN      NS      i.edu-servers.net.
edu.                    172800  IN      NS      j.edu-servers.net.
edu.                    172800  IN      NS      k.edu-servers.net.
edu.                    172800  IN      NS      l.edu-servers.net.
edu.                    172800  IN      NS      m.edu-servers.net.

;; ADDITIONAL SECTION:
a.edu-servers.net.      172800  IN      A       192.5.6.30
a.edu-servers.net.      172800  IN      AAAA    2001:503:a83e::2:30
b.edu-servers.net.      172800  IN      A       192.33.14.30
b.edu-servers.net.      172800  IN      AAAA    2001:503:231d::2:30
c.edu-servers.net.      172800  IN      A       192.26.92.30
c.edu-servers.net.      172800  IN      AAAA    2001:503:83eb::30
d.edu-servers.net.      172800  IN      A       192.31.80.30
d.edu-servers.net.      172800  IN      AAAA    2001:500:856e::30
e.edu-servers.net.      172800  IN      A       192.12.94.30
e.edu-servers.net.      172800  IN      AAAA    2001:502:1ca1::30
f.edu-servers.net.      172800  IN      A       192.35.51.30
f.edu-servers.net.      172800  IN      AAAA    2001:503:d414::30
g.edu-servers.net.      172800  IN      A       192.42.93.30
g.edu-servers.net.      172800  IN      AAAA    2001:503:eea3::30
h.edu-servers.net.      172800  IN      A       192.54.112.30
h.edu-servers.net.      172800  IN      AAAA    2001:502:8cc::30
i.edu-servers.net.      172800  IN      A       192.43.172.30
i.edu-servers.net.      172800  IN      AAAA    2001:503:39c1::30
j.edu-servers.net.      172800  IN      A       192.48.79.30
j.edu-servers.net.      172800  IN      AAAA    2001:502:7094::30
k.edu-servers.net.      172800  IN      A       192.52.178.30
k.edu-servers.net.      172800  IN      AAAA    2001:503:d2d::30
l.edu-servers.net.      172800  IN      A       192.41.162.30
l.edu-servers.net.      172800  IN      AAAA    2001:500:d937::30
m.edu-servers.net.      172800  IN      A       192.55.83.30
m.edu-servers.net.      172800  IN      AAAA    2001:501:b1f9::30

;; Query time: 44 msec
```

```
;; SERVER: 199.9.14.201#53(199.9.14.201)
;; WHEN: Fri Sep 17 18:59:57 EDT 2021
;; MSG SIZE  rcvd: 855

;; BADCOOKIE, retrying.
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31153
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8327db0e4da7d1fe0100000061451dedecce5fac3f172511 (good)
;; QUESTION SECTION:
;q-A.                           IN      A

;; AUTHORITY SECTION:
.                       86400   IN      SOA     a.root-servers.net. nstld.verisign-
grs.com. 2021091702 1800 900 604800 86400

;; Query time: 44 msec
;; SERVER: 199.9.14.201#53(199.9.14.201)
;; WHEN: Fri Sep 17 18:59:57 EDT 2021
;; MSG SIZE  rcvd: 135
```

Secondly connect with the Indiana.edu to get the different dns.

dig @a.edu-servers.net www.indiana.edu q-A

```
abkuma@silo:~$ dig @a.edu-servers.net www.indiana.edu q-A

; <<>> DiG 9.16.1-Ubuntu <<>> @a.edu-servers.net www.indiana.edu q-A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44620
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.indiana.edu.               IN      A

;; AUTHORITY SECTION:
indiana.edu.            172800  IN      NS      dns1.iu.edu.
indiana.edu.            172800  IN      NS      dns2.iu.edu.
indiana.edu.            172800  IN      NS      dns3.iu.edu.

;; ADDITIONAL SECTION:
dns1.iu.edu.            172800  IN      A       134.68.220.8
dns1.iu.edu.            172800  IN      AAAA    2001:18e8:3:220::10
dns2.iu.edu.            172800  IN      A       129.79.1.8
dns2.iu.edu.            172800  IN      AAAA    2001:18e8:2:8::10
dns3.iu.edu.            172800  IN      A       52.23.85.80

;; Query time: 28 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Fri Sep 17 19:01:30 EDT 2021
;; MSG SIZE  rcvd: 208

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43552
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;q-A.                           IN      A

;; AUTHORITY SECTION:
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.

;; Query time: 24 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Fri Sep 17 19:01:30 EDT 2021
;; MSG SIZE  rcvd: 243
```

Finally, will connect with mail service using one of the dns we got

dig @dns1.iu.edu mail-relay.iu.edu q-A

```
abkuma@silo:~$ dig @dns1.iu.edu mail-relay.iu.edu q-A

; <<>> DiG 9.16.1-Ubuntu <<>> @dns1.iu.edu mail-relay.iu.edu q-A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44119
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: dff84540087fb4394f02b02661451e87c246e4210e3cb670 (good)
;; QUESTION SECTION:
;mail-relay.iu.edu.             IN      A

;; ANSWER SECTION:
mail-relay.iu.edu.      300     IN      A       134.68.220.47
mail-relay.iu.edu.      300     IN      A       129.79.1.38

;; AUTHORITY SECTION:
iu.edu.                 3600    IN      NS      dns3.iu.edu.
iu.edu.                 3600    IN      NS      dns2.iu.edu.
iu.edu.                 3600    IN      NS      dns1.iu.edu.

;; ADDITIONAL SECTION:
dns1.iu.edu.            3600    IN      A       134.68.220.8
dns2.iu.edu.            3600    IN      A       129.79.1.8
dns3.iu.edu.            3600    IN      A       52.23.85.80
dns1.iu.edu.            3600    IN      AAAA    2001:18e8:3:220::10
dns2.iu.edu.            3600    IN      AAAA    2001:18e8:2:8::10

;; Query time: 4 msec
;; SERVER: 134.68.220.8#53(134.68.220.8)
;; WHEN: Fri Sep 17 19:02:31 EDT 2021
;; MSG SIZE  rcvd: 267

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23155
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
```

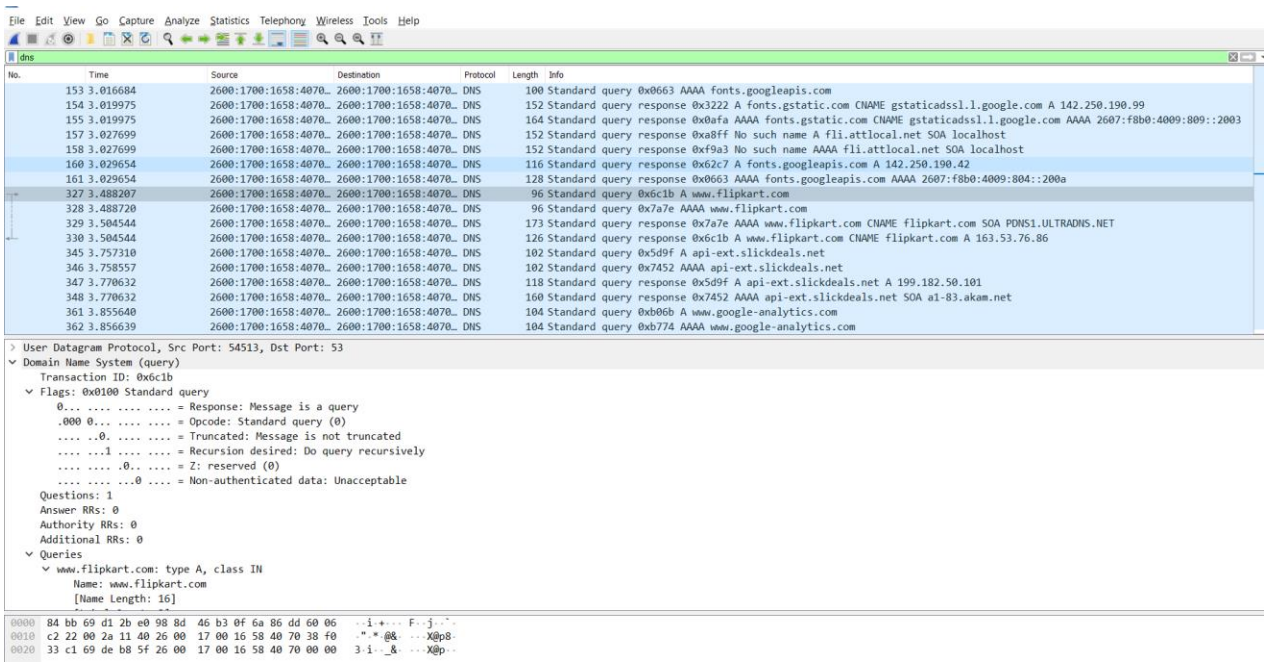
```
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: dff84540087fb43912c6382961451e8799b0acb25f1c9ccb (good)
;; QUESTION SECTION:
;q-A.                           IN      A

;; AUTHORITY SECTION:
.                       10318   IN      SOA     a.root-servers.net. nstld.verisign-
grs.com. 2021091702 1800 900 604800 86400

;; Query time: 4 msec
;; SERVER: 134.68.220.8#53(134.68.220.8)
;; WHEN: Fri Sep 17 19:02:31 EDT 2021
;; MSG SIZE  rcvd: 135
```

Q4. You are sitting in a coffee shop and are connected to a public WLAN. You fire up wireshark and start sniffing the traffic of other customers. You notice that all their traffic is over https so you cannot simply read it. You also notice something striking about the DNS traffic, what is it and what are the implications?

While checking the dns traffic we can get information under queries about the website name. Also, the information of the class can be found under dns. Moreover, the type of the DNS record can be found. Here in the given exam type A is there. The A stands for address and this is the most fundamental type of DNS record which indicates the IP address of a given domain. So we can get these information by using the DNS traffic.



Q5. Suppose that IU has an internal DNS cache. You are an ordinary user (no network admin). Can you determine (and if yes, how) if a given external website was recently accessed?

Yes, we can check if the external website was recently access by using the Query Time.

So, in the below example I tried to access flipkart.com using dig flipkart.com. Now the query time is 28 msec. Now again I tried to access the same website and the query time is 0 this time which shows this website was access before.

```
Last login: Fri Sep 17 16:38:07 2021 from 69.223.63.2
abkuma@silo:~$ dig flipkart.com

; <<>> DiG 9.16.1-Ubuntu <<>> flipkart.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28821
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
flipkart.com.           30      IN      A       163.53.78.110

;; Query time: 28 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Sep 17 17:25:15 EDT 2021
;; MSG SIZE  rcvd: 57

abkuma@silo:~$ dig flipkart.com

; <<>> DiG 9.16.1-Ubuntu <<>> flipkart.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8648
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
flipkart.com.           18      IN      A       163.53.78.110

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Sep 17 17:25:26 EDT 2021
;; MSG SIZE  rcvd: 57
```