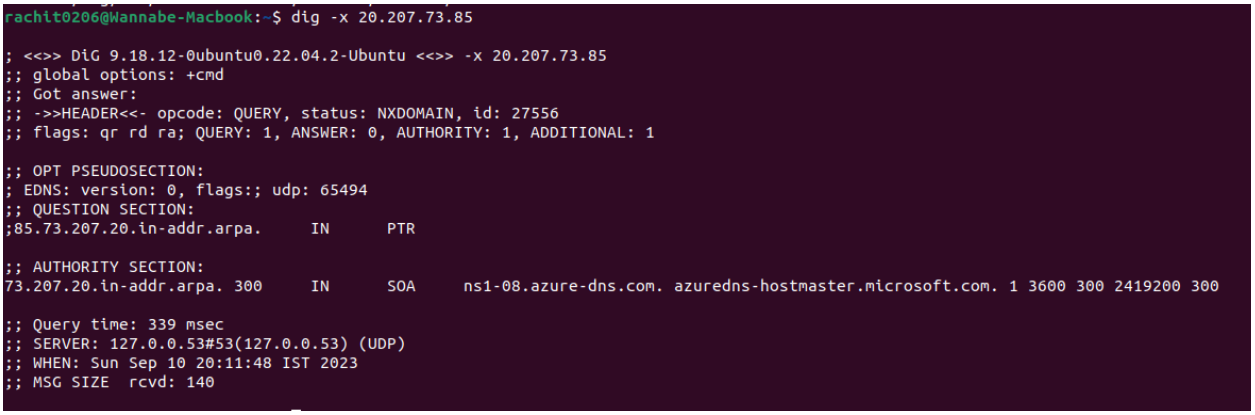
Protocols:

- **QUIC** - QUIC is a transport layer protocol which was built by Google over the UDP protocol. It is designed to reduce latency and is closely associated with HTTP/3. It supports multiplexed data streams. RFC - 9000
- **ARP -** ARP is an internet layer protocol used to map an internet layer address like IP address to a link layer address like MAC address on a local network. ARP accomplishes this by broadcasting an ARP request, and the device with the corresponding IP address responds with its MAC address. RFC - 826
- **TLS** - TLS is a cryptographic protocol located between the application protocol layer and the TCP/IP layer, where it can encrypt and send application data to the transport layer. RFC - 5246 for TLS version 1.2 , RFC - 4346(for TLS version 1.1), RFC - 8446(for TLS version 1.3)
- **SSDP -** SSDP is a UDP and HTTP based network protocol used for discovering and advertising services and devices on a local network. SSDP is intended for use in small environments like offices and institutions. RFC - Not available
- **WLCCP** - WLCCP is a proprietary protocol developed by Cisco used for managing and controlling LAN devices in Cisco wireless LAN deployment. The WLCCP registration protocol can automatically create and delete links in the network, securely distribute operational context, and reliably establish Layer 2 forwarding paths on wireless links. RFC - Not available since it is a proprietary protocol by Cisco.

RTT of a connection

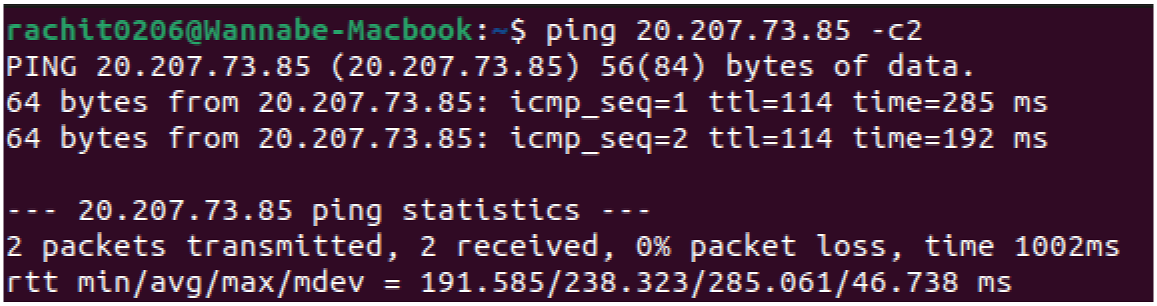
Connection used for sampling - Packets to IP address 20.207.73.85

Reverse DNS lookup result:



```
rachit0206@Wannabe-Macbook:~$ dig -x 20.207.73.85

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> -x 20.207.73.85
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 27556
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
73.207.20.in-addr.arpa. 300     IN      SOA     ns1-08.azure-dns.com. azuredns-hostmaster.microsoft.com. 1 3600 300 2419200 300

;; Query time: 339 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Sep 10 20:11:48 IST 2023
;; MSG SIZE  rcvd: 140
```

We estimated the RTT of this connection using the ‘ping’ command. The results indicating the average, minimum and maximum values of the RTT are indicated in the picture below:



```
rachit0206@Wannabe-Macbook:~$ ping 20.207.73.85 -c2
PING 20.207.73.85 (20.207.73.85) 56(84) bytes of data.
64 bytes from 20.207.73.85: icmp_seq=1 ttl=114 time=285 ms
64 bytes from 20.207.73.85: icmp_seq=2 ttl=114 time=192 ms

--- 20.207.73.85 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 191.585/238.323/285.061/46.738 ms
```

Protocols used by websites:

- **Github.com:** h2: h2(or HTTP/2) is an application-level protocol that operates over a TLS connection. With h1(or HTTP/1), a separate TCP/IP connection is established for each object request. In contrast, h2 uses persistent TCP connections. In addition, these requests can be multiplexed to handle multiple requests concurrently.

- **Google.com:** h3: h3(or HTTP/3) is an application-level protocol that is built over the QUIC protocol. The QUIC protocol was developed for mobile devices which would switch between networks frequently. UDP is a connectionless and unreliable protocol that is not as reliable as TCP, but is faster and more flexible than it. h3 inherits features from h2 like multiplexing, header compression, server push, and prioritization, while introducing new features like Connection migration (which allows clients and servers to switch between different network interfaces or IP addresses without interruption), while 0-RTT enables clients and servers to resume previous connections without performing a full handshake. HTTP/3 is more flexible than HTTP/2, while being more complex and having lesser compatibility.

- **netflix.com :** http/1.1 , h2, h3: HTTP/1.1, created in 1997, was the first usable version of HTTP. It suffers from head-of-line blocking, which occurs when a large object blocks the transfer of other smaller objects. This issue was resolved in HTTP/2 using prioritization and pipelining of the requested objects. To speed up web performance, both HTTP/1.1 and HTTP/2 compress HTTP messages. However, HTTP/2 uses a more advanced compression method called HPACK to eliminate redundant information in HTTP header packets.

Cookies set up by eoffice.iitgn.ac.in

Name of the cookies setup: PHPSSID, AIT

The PHPSSID is a session specific cookie(based on its session expiry) while AIT is presumably collecting more longer information(based on its longer expiry). Moreover, AIT is a secure cookie while the PHPSSID is not. This indicates the AIT contains more sensitive information for improving the user experience while PHPSSID might be collecting statistics and more general information. Both are of the same size(35). Both of the cookies are of medium priority. This is because I have never visited the website before and hence the browser does not have any relevant information to give to the website. AIT is a http only cookie while PHPSSID is not.