Hrushti Naik
19110088

Computer Networks
Assignment 1: Part 3

5. Networking Tools

Run the Wireshark tool and capture the trace of the network packets on your host device. I expect you would be connected to the Internet and perform regular network activities.
The Wireshark dump can be found here: link

a. List at least 5 different network protocols that we have not discussed so far in the classroom and describe in 1-2 sentences the operation/usage of protocol and its layer of operation and indicate the associated RFC number if any.

1. **NTP (Network Time Protocol)** - internet protocol used to synchronise with computer clock time sources in a network. Used to ensure proper sequences by coordinated times, and for updates that require synchronised clock times.
   Works over the application layer.
   RFC 5905 (source: https://en.wikipedia.org/wiki/Network_Time_Protocol)
2. **ICMPv6 (Internet Control Message Protocol for IPv6)** - implementation of ICMP for IPv6, used for error reporting and diagnostic functions.
   Works over Network Layer in the Open Systems Interconnection (OSI) protocol stack.
   RFC 4443 (source: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol_for_IPv6)
3. **TLSv1.3 (Transport Layer Security v1.3)** - provides encryption and integrity for data being transmitted over HTTPS. TLSv1.3 is faster, more secure, and simpler compared to earlier versions of TLS.
   Works over Layers 4 through 7 of the OSI model.
   RFC 8446 (source: https://datatracker.ietf.org/doc/rfc8446/)
4. **QUIC (Quick UDP Internet Connections)** - QUIC transport protocol provides applications with flow-controlled streams for structured communication, low-latency connection establishment, and network path migration. QUIC includes security measures that ensure confidentiality, integrity, and availability in various deployment circumstances. Accompanying documents describe the integration of TLS for key negotiation, loss detection, and an exemplary congestion control algorithm. QUIC is an experimental transport layer network protocol designed by Google. The overall goal is to reduce latency compared to that of TCP.

RFC 9000 (source: https://datatracker.ietf.org/doc/html/rfc9000#:~:text=RFC%209000%20%2D%20QUIC%3A%20A%20UDP%2DBased%20Multiplexed%20and%20Secure%20Transport)

5. **OCSP (Online Certificate Status Protocol)** - an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
   RFC 6960 (source: https://www.rfc-editor.org/rfc/rfc6960)

b. Identify any one connection and try to estimate the RTT of that connection.

For this, we will use Wireshark and use the terminal to ping yahoo.com thrice:

```
┌──(kali㉿kali)-[~]
└─$ ping yahoo.com -c 3
PING yahoo.com (74.6.143.25) 56(84) bytes of data.
64 bytes from media-router-fp73.prod.media.vip.bf1.yahoo.com (74.6.143.25): i
cmp_seq=1 ttl=43 time=219 ms
64 bytes from media-router-fp73.prod.media.vip.bf1.yahoo.com (74.6.143.25): i
cmp_seq=2 ttl=43 time=218 ms
64 bytes from media-router-fp73.prod.media.vip.bf1.yahoo.com (74.6.143.25): i
cmp_seq=3 ttl=42 time=223 ms

── yahoo.com ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 217.915/220.004/222.618/1.955 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.136.7	DNS	69	Standard query 0x87dc A
2	0.000027742	10.0.2.15	10.0.136.7	DNS	69	Standard query 0xe4da A
3	0.032289417	10.0.136.7	10.0.2.15	DNS	447	Standard query response
4	0.054688414	10.0.136.7	10.0.2.15	DNS	519	Standard query response
5	0.055848970	10.0.2.15	74.6.143.25	ICMP	98	Echo (ping) request id=
6	0.275320676	74.6.143.25	10.0.2.15	ICMP	98	Echo (ping) reply id=
7	0.275527754	10.0.2.15	10.0.136.7	DNS	84	Standard query 0x904c P
8	0.405750496	10.0.136.7	10.0.2.15	DNS	426	Standard query response
9	1.055845693	10.0.2.15	74.6.143.25	ICMP	98	Echo (ping) request id=
10	1.273722242	74.6.143.25	10.0.2.15	ICMP	98	Echo (ping) reply id=
11	1.274027160	10.0.2.15	10.0.136.7	DNS	84	Standard query 0xa066 P
12	1.277293098	10.0.136.7	10.0.2.15	DNS	426	Standard query response
13	2.057598914	10.0.2.15	74.6.143.25	ICMP	98	Echo (ping) request id=
14	2.280174255	74.6.143.25	10.0.2.15	ICMP	98	Echo (ping) reply id=
15	2.280481501	10.0.2.15	10.0.136.7	DNS	84	Standard query 0xacda P
16	2.342275564	10.0.136.7	10.0.2.15	DNS	426	Standard query response

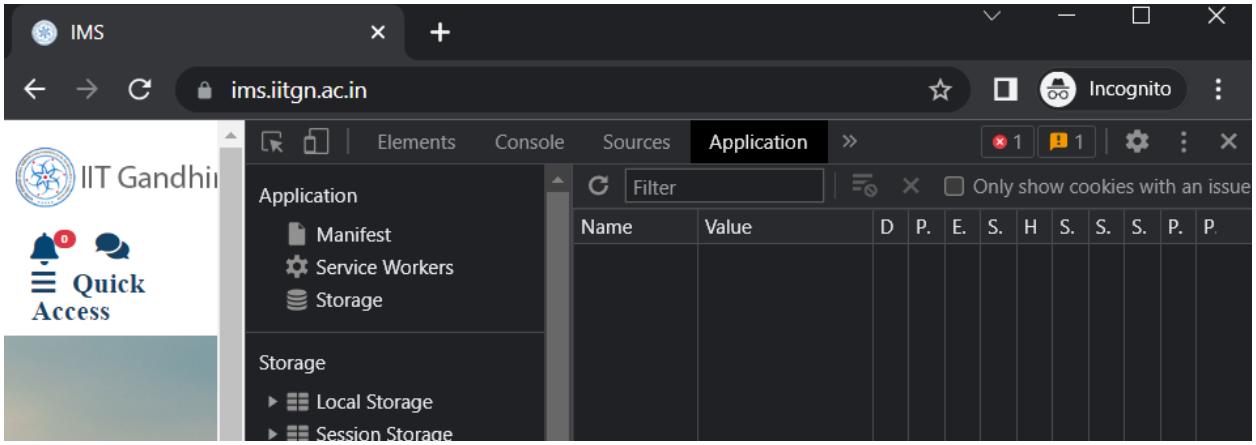
As seen in the terminal screenshot, the min/avg/max RTT is mentioned. The average RTT is 220.004 ms. This can also be seen in Wireshark, where the difference timestamps of the three pings (highlighted in pink) give the RTT (time difference between request and reply).

1st ping RTT: 0.275320 - 0.055848 = 0.219472 microseconds
2nd ping RTT: 1.273722 - 1.055845 = 0.217877 microseconds
3rd ping RTT: 2.280174 - 2.057598 = 0.222576 microseconds

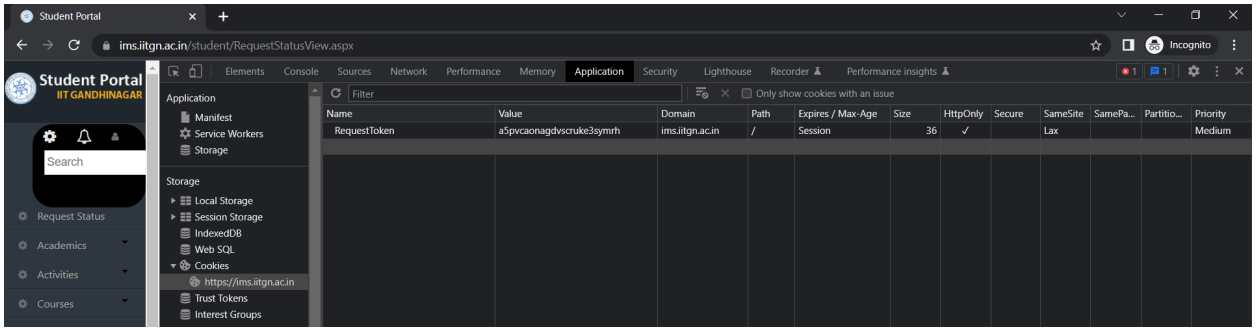
The average RTT from Wireshark is 0.219975 microseconds = 219.975 ms, which is very close to that seen in the terminal.

c. ***List the cookies and identify the characteristics of the cookies setup when you visit ims.iitgn.ac.in and also when you login to the student portal.***

When ims.iitgn.ac.in is opened for the first time, no cookies are present:



After logging in, we see one entry in the cookies:



Name: RequestToken
Value: a5pvcaonagdvscruke3symrh
Domain: ims.iitgn.ac.in
Path: /
Expires: Session → it will expire as soon as the session is closed/expires.
Size: 36 → in bytes
HttpOnly: ✅ → denotes cookie should only be used over HTTP (prevents client access to cookie data)
Secure: → not checked implies it is not encrypted
SameSite: Lax → denotes relaxed form of protection for cross-site requests
SameParty:
Partition Key:
Priority: Medium