Computer Networks Assignment 1
19110207
Vishal Soni

Question 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.

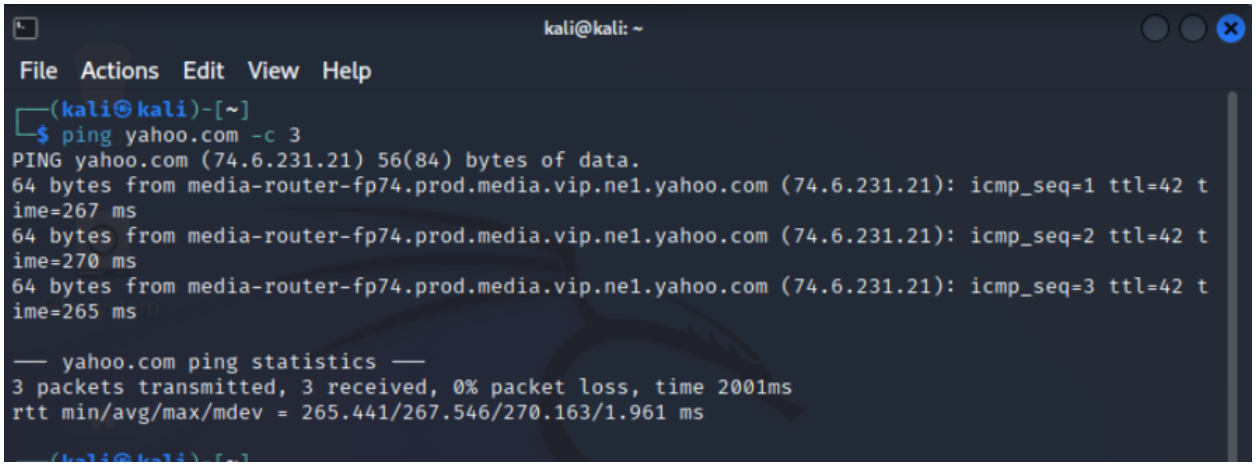
WireShark dump file **link**

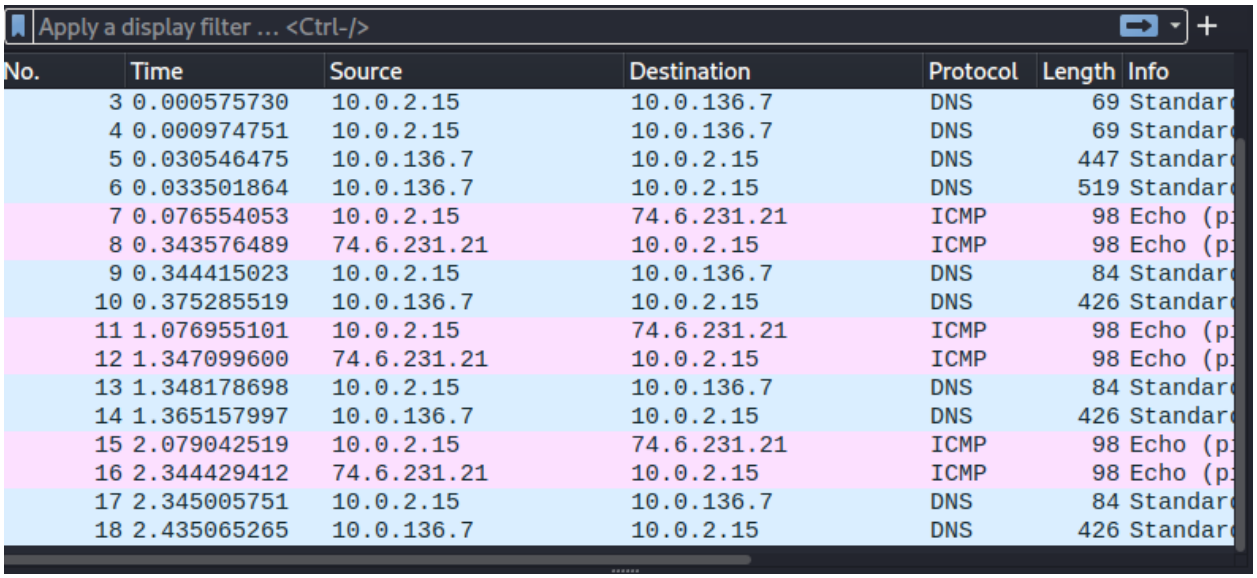
a. List at least 5 different network protocols that we have not discussed so far in the classroom and describe in 1-2 sentences the operation/usage of protocol and its layer of operation and indicate the associated RFC number if any

1. **Network Time Protocol (NTP):** IP to synchronize with computer clock time sources in a network.
   Used for updates that call for synchronised clock times and to assure accurate sequences by coordinated times. Works over the application layer.
   RFC 5905 (source)
2. **Online Certificate Status Protocol (OCSP):** IP used to obtain revocation status of an X.509 digital certificate.
   RFC 6960 (source)
3. **Transport Level Security (TLSv1.3):** provides data integrity and encryption for HTTPS transmission. Comparing TLSv1.3 to prior TLS versions, the latter is quicker, safer, and easier to use. Works over layers 4 through 7 of the OSI model.
   RFC 8446 (source)
4. **Internet Control Management Protocol (ICMP):** ICMP, a protocol that supports the network layer, is used by network devices to transmit error signals and operational information. ICMP messages, which are sent in IP packets, are used to transmit out-of-band messages about how the network is functioning or not. ICMP is used to announce network errors, congestion, and timeouts. It also aids in debugging. Works over network layer in OSI model.
   RFC 792 for IPv4 (source).
5. **Serial Line IP (SLIP):** TCP/IP point-to-point serial connections are made via SLIP. On dedicated serial links and sporadically for dial-up applications, SLIP is employed. Only a packet framing protocol, It specifies a string of characters used to serially frame IP packets.
   RFC 1055 (source)

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:





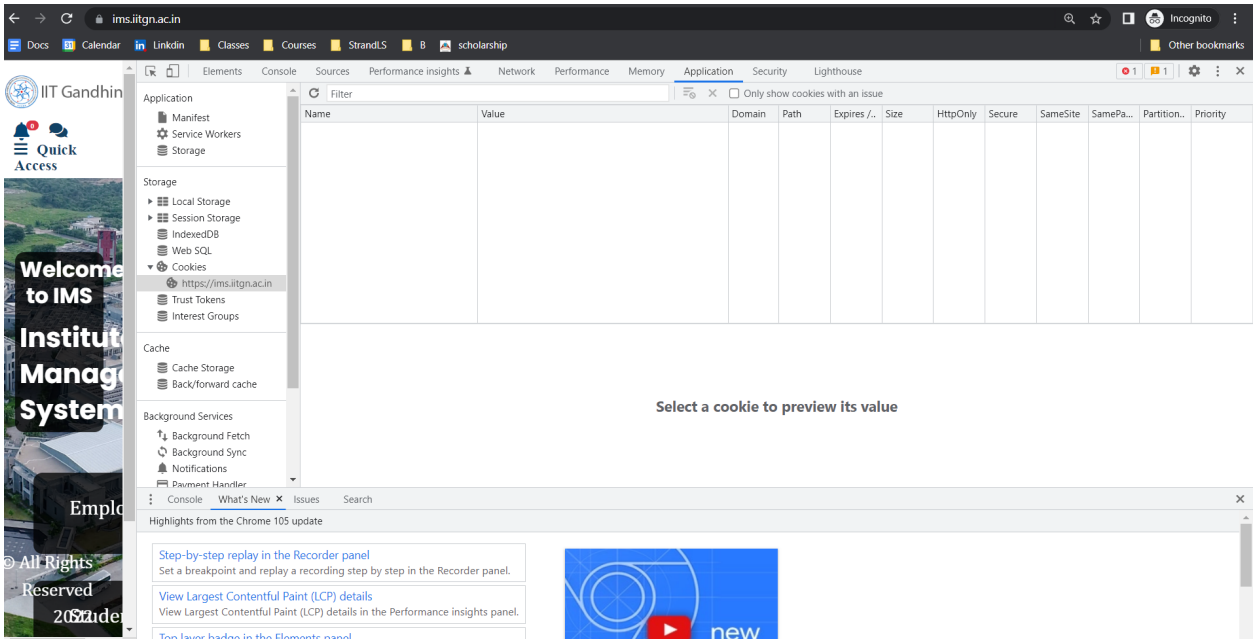
As seen in the terminal screenshot, the min/avg/max RTT is mentioned.
The average RTT is 267.546 ms.
This can also be seen in Wireshark, where the difference timestamps of the three pings (highlighted in pink) give the RTT (time difference between request and reply).

1st ping RTT: 0.343576 - 0.076554 = 0.267022 microseconds
2nd ping RTT: 1.347099 - 1.076955 = 0.270144 microseconds
3rd ping RTT: 2.344429 - 2.079042 = 0.265387 microseconds

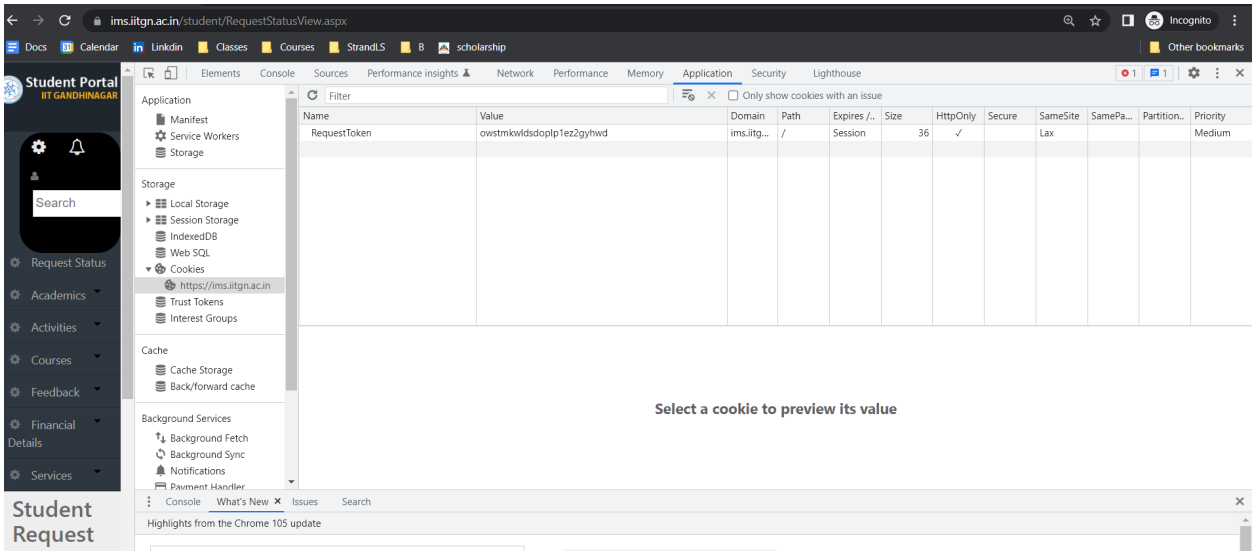
The average RTT from Wireshark is 0.267517 microseconds = 267.517 ms, which is very close to that seen in the terminal.

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.

Opening IMS initially



After logging into student portal, we see a single request token which must be the encryption token generated for logging in for my user credentials.



Name: RequestToken
Value: owstmkwldsdoplp1ez2gyhwd
Domain: ims.iitgn.ac.in
Path: /
Expires: Session
Size: 36
HttpOnly: ✅ -> denotes cookie should only be used over HTTP

Secure:
SameSite: Lax -> denotes that cookie is using same-site attribute
SameParty:
Partition Key:
Priority: Medium