Rubrics for Assignment 1:

1) **Measurement Tools (30 marks) [TA-1]**

1.1) Ping

A [2].
Correct Answer : Google Datacenter is geographically closer in comparison to Sigcom servers therefore less number of hops in google case.

B [5].
DNS - If hostname is given as input **[0.5],** Network Layer - ICMP **[1]**, IP**[0.5]**
Theoretical upper limit is 65536 bytes**[1].**
Not Always, Sometimes, firewalls can reject your packet if the size is very large**[2].**

C [2].
Use -6 flag
In some-cases, even after using the flag you receive ipv4 echo messages, this is because the device might not have an ipv6 address.

1.2) Traceroute

A [3]. Check the traceroute output, the ip addresses will belong to some network. It is Expected in this part to map those ip addresses with their network using some online tool.

B [4].
Ask them why * is observed.
They should give following type of explanations :

Traceroute works using ping. It sends three TTL messages by setting ttl=1. Each router will Forward the ping message if ttl is greater than 0. When ttl is 0, it will discard the message and send time exceeded icmp message to source. Repeat the process until source receives final destination ip address in its response. **[1]**

"*" is observed when a router do not reply when ttl expires**[1]**
If you see continuous "*", this means neither router is replying nor forwarding your packet.**[2]**

C [4]. As traceroute send multiple TTL packets with same value of TTL field in each iteration, each packet can take different route, and respond with different ip address even when the hop count is same.

D [4]. The ip address received will start from 10.x.x.x. This is a private ip address is not valid outside a network. For example, each ip address based device inside iit delhi is given a private network, but the network has only single valid ip address from outside network. You can check that globally valid ip address of iit delhi by pinging by mobile data.**[2]**

When you ping with mobile data, it will be invalid because routers will echo their private ip address as they do not know that the ip address assigned to them is private.**[2]**

E [3]. Look at their output and mapped autonomous network names. They should give a case where it is 2-tier or 3-tier architecture and one where it is not **[1.5].** They will not observe these ISPs if source LAN has direct agreement with destination LAN. Like in case of IIT Delhi as a source and Google as a destination, IIT Delhi has direct connection with Google Data Center Network, therefore they will not observe any architecture in this case **[1.5].**

F [3]. If destinations are really far, the packet will travel more which will cause propagation delay. Sometimes, we can also observe opposite results. This can happen if you send a packet to a congested network where queueing time at routers and transmission delay can overcome propagation delays.
Check their outputs, they should able to make arguments like above using their data

2) Network Data Collection and Header Analysis (35 marks) [TA-2]

A. (6 marks)

- Identified correct Network layer protocols **(1 mark)**
- Mentioned number of packets for NL protocol as a percentage of total packets **(1 mark)**
- Identified correct Transport Layer protocols **(1 mark)**
- Mentioned number of packets for TL protocol as a percentage of total packets **(1 mark)**
- Identified correct Application Layer protocols **(1 mark)**
- Mentioned number of packets for AL protocol as a percentage of total packets **(1 mark)**
- Wrong categorization of protocols in NL **(-1 mark)**
- Wrong categorization of protocols in TL **(-1 mark)**
- Wrong categorization of protocols in AL **(-1 mark)**
- Just pasted screenshot of the Protocol Hierarchy window of Wireshark **(-1 mark)**

B. (12 marks)

- Mentioned direct connection, stated a concrete reason and mentioned possible reasons for an indirect connection **(10 marks)**

- Mentioned if they did multiple attempts (tried mobile network vs. IITD Network, over VPNs, etc.) **(2 marks)**

Or,

- Mentioned indirect connection **(2 marks)**
- Mentioned correct endpoints and IPs **(2 marks)**
- Mentioned if it is the same endpoint or, not **(3 marks)**
- Explained correctly about the relay server **(5 marks)**

C. (17 marks)

- Mentioned the correct number of audio and video packets from the traffic capture **(3 marks)**
- Explained the correct logic (Port no./ Codec Type (RTP Payload Type) / Packet len.) used to separate audio and video packets **(6 marks)**
- Plotted a correct time-series diagram showing the bandwidth utilization **(8 marks)**

3) Traffic Analysis and Network Performance (35 marks) [TA-3]

A. 7 marks- mentioned the correct logic to find the IP of speedtest server.**(4 marks)**
Correctly estimate the speedtest traffic percentage**(3 marks)**

B. 13 marks- Correct plot of uplink and downlink speed**(10 marks)**
correct unit of throughput.**(3 marks)**
Or. 8 marks for port based segregated traffic plot.

C. 15 marks- for 27.5 < download speed < 31 and 8.5 < upload speed < 11.
Or •12 marks for 26 < download speed < 27.5 and 7.5 < upload speed < 8.5.
Or • 10 marks for 24 < download speed < 26 and 5.5 < upload speed < 7.5.
Or • 6 marks for 10 < download speed < 24 and 2.5 < upload speed < 5.5.
• 0 otherwise
Marks deducted for incorrect approach.