4a) Analysis of quiescent traffic captured via wireshark.

Significant traffic can be observed even when all user programs are closed (on Microsoft Windows 10)

Type of traffic:

- DNS lookups and HTTP requests for several windows/microsoft domains
- ARP (Address Resolution Protocol), LLMNR (Link-Local Multicast Name Resolution) and NBNS (NetBIOS Name Service) packets to discover devices on local wireless network
- SSDP over HTTP to connect to windows/microsoft servers.
- HTTP CONNECT requests to IITD proxy server from windows services using secure connection (SSL), causing upgradation to TCP connection.

Applications Causing this traffic:

- Windows Update
- Windows live storage
- Windows service to discover systems on local network.
- Other windows services to report to microsoft

4_a_idle: Screenshot of wireshark capture.

4b) Analysis of packets when opening IITD homepage.

I. DNS query was launched for **www.iitd.ernet.in** to *10.10.1.2* (DNS server)
II. 64 HTTP requests were sent.
Filtered using *ip.src==10.205.157.116 and http*
III. Number of tcp connections made were **6**.
Filtered using *tcp.flags.syn==1 && tcp.flags.ack==0*
IV. **1.5 sec**, checked using chrome
V. **Yes**, packets were lost.
Wireshark reported *"TCP ACKed unseen segment"* many times.

List of figures:

4_b_1: DNS packet
4_b_2: Number of http request generated.
4_b_3: Number of TCP connections opened.
4_b_3_1: Verification on number of TCP connection by going to statitics->conversation.
4_b_3_1_a to 4_b_3_1_f: TCP Headers
4_b_4: Webpage loading time.
4_b_5: TCP Losses
4_b_6: IP Headers