**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.**

1. DNS query was launched for **www.iitd.ernet.in** to *10.10.1.2* (DNS server)
2. 64 HTTP requests were sent.  
   Filtered using *ip.src==10.205.157.116 and http*
3. Number of tcp connections made were **6**.   
   Filtered using *tcp.flags.syn==1 && tcp.flags.ack==0*
4. **1.5 sec**, checked using chrome
5. **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