# CS-349 Networks Lab

## Assignment-2: Analysing network packets using Wireshark

**Submission deadline: 11th February 2015**

Wireshark is a packet sniffer and network protocol analyzer tool. It helps to capture network packets and understands the structure of different networking protocols.

**Instructions need to be followed by each group:**

1. Install wireshark (www.wireshark.org).
2. Learn how to capture packets and filter the required content.
3. Each group is assigned an application for which traces needs to be collected using wireshark.
4. To answer each question provide snapshots of traces in the report and highlight the content as and when needed.
5. Carry out your experiments across different network conditions such as different time of the day and locations.
6. No need to describe about the tool or application or protocol in general. Only trace based description should given for each question.

**Questions:**

1. List out all the protocols used by the application at different layers (only those which you can figure out from traces) and study their packet formats.
2. Highlight and explain the values of various fields of the protocols which you can see in the traces. Example, Source or destination IP address and port no., Ethernet address, protocol number, etc.
3. Explain the sequence of messages exchanged by the application for using several functionalities available in the application. For example, upload, download, play, pause, stop and so on. Check and explain if any handshaking sequence occurs or not.
4. Explain how a particular protocol is relevant for functioning of the application.
5. Calculate the following statistics from your traces when you perform experiment at different times of the day: Throughput, RTT, Packet size, No. of packets lost, number of UDP & TCP packets, number of responses received with respect to one request sent.
6. Check if the whole content is being sent from same location/source. List out the IP addresses of content providers if there exist multiple sources and explain the reason behind it.

| **Application** | **Group Numbers** |
|---|---|
| Skype | 1,11,21,31,41,51,61,71 |
| Live Streaming | 2,12,22,32,42,52,62 |
| Vimeo – uploading and downloading video | 3,13,23,33,43,53,63 |
| Dailymotion - uploading and downloading video | 4,14,24,34,44,54,64 |
| NPTEL video lectures | 5,15,25,35,45,55,65 |
| Gtalk- Audio and video chats / Google Hangout | 6,16,26,36,46,56,66 |
| P2P connectivity using Remote desktop and softwares like Team Viewer | 7,17,27,37,47,57,67 |
| DC++ | 8,18,28,38,48,58,68 |
| Online games | 9,19,29,39,,49,59,69 |
| Dropbox | 10,20,30,40,50,60,70 |

**Submit a soft copy of the report and your traces in a zipped form on moodle. The name of the zipped file should be like rollno1_rollno2.zip. Example 120101001_120101002.zip. Note: Report should not contain more than 5-6 pages. Copy cases will be strictly punished by giving 'F' grades.**