CS359 Computer Networks

Assignment 1
Indian Institute of Technology, Patna

January 13, 2021

Instructions: Download Wireshark and install it on your computer.

Install Wireshark 2.2.5 via PPA:- (Note:- Run in administrator mode)

Steps:- **1.** To add the PPA, open terminal from Unity Dash / App Launcher, or via Ctrl+Alt+T shortcut keys, and then run command:

sudo add-apt-repository ppa:wireshark-dev/stable

Steps:- **2.** For those who have a previous release installed, launch Software Updater (or Update Manager) to upgrade it to the latest:

sudo apt-get update

sudo apt-get install wireshark

Steps:- **3.** Start wireshark

wireshark

Note:- Wireshark can be used to sniff wireless traffic.

Problem1: Writing Wireshark filter expressions for packet capture

Write the exact packet capture filter expressions to accomplish the following:

1. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account
2. Capture all HTTP traffic to/from Facebook, when you log in to your Facebook account
3. Find a popular YouTube video and play it while capturing all traffic to/from YouTube

After you run Wireshark with the above capture filters and collect the data, do the following:

1. Write a DISPLAY filter expression to count all TCP packets (captured under item #1) that have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set.
2. Use a DISPLAY filter expression to separate the packets sent by your computer vs. received from Facebook and YouTube in items #2 and #3 above. Show the fractions for each type.

Note:-

- When sniffing out TCP packets, you will be receiving TCP packets, SSL packets, and HTTP packets. This is because HTTP/SSL run on top of TCP and you capture their packets by default because they are subclasses of TCP packets.

- Then use display filters to separate the subset of TCP packets that are also HTTP packets. (You can do this by filtering only packets on port 80).
- Note that some of your sessions, e.g., Facebook, may be using secure HTTP (HTTP/SSL or HTTPS), which uses the port number 443.

Problem2:- Captured Data Analysis

a. Count how many TCP packets you received from / sent to Facebook or YouTube, and how many of each were also HTTP packets.

b. Determine if any TCP packets with SYN or PSH flags set were sent from your host or received from Facebook/Youtube.

c. Go flag-by-flag and count how many packets have `tcp.flags.push` set, then how many have `tcp.flags.syn` set, and finally, how many have `tcp.flags.reset` set.