Project 2: Wireshark Packet Capture and Analysis

1.1. Data Capture (10%)

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

1. Capture all TCP traffic to/from Youtube, during the time when you log in to your Youtube account
2. Capture all HTTP traffic to/from Youtube, when you log in to your Youtube 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 YouTube in items #2 and #3 above. Show the fractions for each type.

Note that 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.

So, capture them all and store in a local database.

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., Youtube, may be using secure HTTP (HTTP/SSL or HTTPS), which uses the port number 443.

1.2. Data Analytics (5%)

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

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

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.

Report all three counts in a table.

1.3. Additional Requirements (10%)

Draw a rough sketch with a timeline of your YouTube session (roughly 5 minutes, or whatever is the duration of your chosen video) and indicate approximately when during the session the packets with SYN or PSH flags occurred. Your timeline should start at the time when the first video packet is received and end when the last video packet is received. You don't need to draw a precise timeline—just illustrate the relationships.

Analyze if during the course of a video session your client connected to multiple Youtube servers. Indicate approximately on the timeline where this occurred. Did packets with SYN or PSH flags occur at about the same time when your server changed? Provide some explanation as to why SYN/PSH packets were sent at all and if they were correlated with the server switching.

Analyze the Youtube packet sizes. Draw a histogram showing how many packets were received within a range of sizes, e.g., how many packets had length 0 - 100 bytes, 100 - 200 bytes, 200 - 300 bytes, etc. Indicate the packet size units (in bytes) on the horizontal axis.

Report Preparation and Submission

The report should contain the following information:

1. Location where the experiments were run (University campus/lab, home, other) and the type of your computer.
2. Exact Wireshark filters used for capture and display.
   To improve the readability of your report, provide the filter expressions in separate lines.
3. Explanation for every component of your filter expressions.
4. The exact URL for all Youtube videos that you visited for this experiment.
5. A table of observed statistics for counting the set flags in captured TCP packets.
6. Histogram of the Youtube packet lengths.
7. Sketch of the timeline of your Youtube session.
8. The list of references used during the data analysis and report preparation, such as websites, blogs, books, etc.