ICSI416/516 Project 3 – Network traffic analysis
Due May 2nd at 11:59PM

Objectives

Your day-to-day online interactions generate large volumes of packets that are carefully hidden from the end user and from the application. The TCP/IP model enables this abstraction. The goal of homework 1 is for you to familiarize yourself with the underlying network activity as several day-to-day online activities are carried out. To complete this assignment you will use Wireshark. You already have some basic experience with Wireshark from your homework assignment.

Note: This is an individual assignment. Each student is requested to submit an individually-completed report.

Assignment details

The goal of this assignment is to explore the network packets associated with several typical online activities. You will have the chance to analyze bit-by-bit the flows associated with these services and evaluate different application and protocol parameters across the entire TCP/IP stack including Data Link Layer/Medium Access Control (L2), Network Layer (a.k.a. IP or L3), Transport Layer and Application Layer.

To carry out this analysis, you will use Wireshark. (If you haven't already) you will need to install Wireshark on your own computer. For more information and installation instructions visit https://www.wireshark.org/. Part of finishing this assignment will be learning how to use Wireshark effectively. To do this, you can refer to the User's Guide available here https://www.wireshark.org/docs/wsug_html_chunked/.

While Wireshark allows you to capture packets on a network interface it can also be used to read previously collected packet traces. For this assignment you will be analyzing a trace that I have already captured. ***You can download the trace from Blackboard or the course website at*** `http://www.cs.albany.edu/~mariya/courses/csi416516S16/projects/p3_wireshark_trace.pcapng`. Some of the activity in this trace contains protocols we have not gone over (or will not be going over). Other protocols, we have studied extensively in this class. In either case, there is an abundance of information online and I encourage you to read up if you are not sure what a protocol is dedicated for.

The deliverable of this assignment is a report in which you will explain what you saw in this trace. In order to complete the assignment you need to do two things: (i) make sense of the trace and (ii) write the report. The remainder of this assignment provides details on how to approach these two tasks.

1. Making sense of the trace. Begin your analysis by considering the following questions:
   a. How many packets are in the trace?
   b. What types of packets are these?
   c. What DLL/MAC addresses can you see in the trace?

    d. What IP addresses can you see in the trace?
    e. How do IP and MAC addresses map to each other?
    f. Can you tell by the trace what kind of network card was used to capture the trace: an Ethernet adapter or a 802.11 wireless card?
    g. Can you conclude anything about the network topology on which the trace was collected? Which was the machine (IP and MAC address) on which the trace was collected? What is the network mask? What is the default gateway? What is the DNS server? What is the DHCP server? Which hosts are on the local network? How many hosts are there on the local network? Can you determine some of the applications these hosts are running? Which hosts are remote?
    h. How many hops away are the remote hosts? Which is the most "remote" host?
    i. What services were accessed?
    j. Did any IP fragmentation occur? Were there any packets in which the "Don't fragment" bit was set?

2. Writing your report. Being able to convey what you have learned from the trace is equally important to understanding what is going on in the trace. This section provides you with guidelines on how to organize your understanding of the trace in a nice, coherent story, so your reader can also learn from your knowledge.
    a. Paper format: your submission will be a single PDF file.
    b. Paper content. Your paper will need to answer the questions above plus any other interesting things you have found in the trace. While the above questions provide a nice framework to analyze the trace, answering them one by one in the report will not lead to a nice coherent story; instead it will produce a hard to read and hard to understand bucket list. When writing your report consider presenting your findings in multiple levels of detail. For example, you can first provide a summary of the trace including number of packets, number of hosts and a high-level idea of what these hosts are up to. Then describe the different services/applications you see. For each service dive in details about the packet trace associated with this service. What transport layer protocol did it use? Did you see anything unexpected? Describe the packets you see in the flow associated with this service. Include diagrams where appropriate. You can then conclude your report with a brief summary of what you learned from this trace.

Turnin: You will need to submit your report via blackboard.

Cheating policy: This assignment is to be done individually. Cheating is not tolerated. Please, read the university Community Rights and Responsibilities for more information on cheating. Students caught cheating will receive 0 points for this assignment. More serious consequences are possible as well.