**CS 444/544 Spring 2018 Lab 1**

Lab 1 is due by 11:59pm on Tuesday, February 6th, 2018.

Send your answers to the following questions in the body of an email with no attachments to crandall@cs.unm.edu. Failure to follow these instructions will result in a zero on the assignment, so DO NOT DO YOUR LAB AS A PDF OR OTHER TYPE OF DOCUMENT AND SEND IT AS AN ATTACHEMENT. Submit your lab in the text body of the email, which should have no attachments at all (I won't knock you for, *e.g.*, a PGP signature block, but I definitely won't open any attachments to grade).

Lab 1 is worth 100 points, split per question as indicated below. I may give partial credit, or in some cases full credit if you made an honest attempt to answer the question. Your answers should be as concise as possible, feel free to stop by office hours to check them.

I will provide three packet captures *via* the course web site. Using wireshark, tshark, Python dpkt, chaosreader, and/or any other tools you wish to use, answer all of the questions below. One packet capture is a scan of T-Mobile's network, another is a web browsing session that includes non-Tor and Tor traffic, and the third is a test of a VPN kill switch.

You are expected to do your own work. From analyzing the packet captures to researching tools (*e.g.*, nmap) to writing the answers, for all phases of this project you should do your own work. Any instance of not doing your own work will be considered cheating. For your submission, if you copy even a single question from a classmate that will be considered cheating. If you're not sure whether something will be considered cheating or not, ask me before you do it. You are encouraged to discuss the assignment with your classmates at a high level. Exchanging tools, source code that existed before the assignment was assigned, and general thoughts about approaches to specific problems is okay. As a reminder of the course policy, if you cheat on any assignment in this class including this assignment (cheating includes, but is not limited to, representing somebody else's work as your own or having someone else do the assignment for you) you will receive an F in the class. If you want to share source code written for the assignment with a classmate, you should get my permission first and share it with the whole class.

Your answers to the below questions should be as concise as possible. Try to limit your answers to one or two sentences at the most. If you have something interesting to tell me (about a technique you used, something interesting you found, *etc.*) please stop by my office hours. For me to grade 70-ish of there the answers can't be very long, just say what you know and how you know it. Here are the questions you should answer about the three packet captures:

1. (30 points) For the VPN kill switch test, did the VPN kill switch work properly? In one or two sentences, explain your answer.
2. (30 points) For the scan of T-Mobile's network, approximately how many machines appeared to be on the scanned network?
3. (5 points) For the scan of T-Mobile's network, did the majority of machines that responded appear to be cell phones, servers, or something else?
4. (30 points) For the web browsing pcap, make two separate lists: websites that were visited that did a good job of hiding the content, and websites visited that didn't do a good job of hiding the content. Just list major websites visited (*e.g.*, nfl.com), not every little ad server or content distribution request.
5. (5 points) For the web browsing pcap, what website(s) was/were visited using Tor?