The goal of this project is to use a packet sniffer tool to eavesdrop communications in your local area network. The desired environment is a **wired network** with a few other computers in the same subnet.

This is an open-end project. I will only guide you through the first few steps.

Wireshark is one of the most popular open-source packet sniffer tools. In this project, you are asked to install and use Winshark to sniff your local network. Wireshark is very powerful, we will only use some basic functions.

1. Download Wireshark from: http://www.wireshark.org/download.html. Install it on your computer.

2. Start sniffing: capture -> options; select the correct interface (i.e. the correct Ethernet device). Slick start, and you will see packets been captured.

Task I:

1. Add a filter to only include your IP (`ip.addr==YourIP`). Open a browser to visit Google, return to Wireshark, and stop sniffing.

2. Now, it's time to analyze sniffed packets. You should first see DNS requests to your DNS server, and then HTTP traffic. If you maintain logged-in with Google, you will see HTTPS instead of HTTP.

Task II (You cannot use KU's Jayhawk network for this task**):**

1. Add a filter to exclude your own mac address (`!(eth.addr==YourMAC)`). Let WireShark capture for a while, and stop sniffing.
2. You should be able to see broadcast packets (ARP, DHCP, etc) from other devices that are connected to the same WiFi network. Examine the packets. Can you identify the make/model of the devices? What else can you learn?

3. Save the packets in a pcapng file using: File -> Export Specified Packets -> Choose "All Packets" and "Displayed" (so that you don't save your own packets).

You are required to submit a short report, together with your pcapng file, to describe what you have done in the project.

Due: April 10, End of day