CS447-002: Lecture Note (Lecture #14, March 11, 2024)

1. **Pick up:**

   - Attendance card
   - Project #2 handout

2. **Announcements:**

   - Next quiz (Quiz #6) is scheduled on 3/18 (postponed from 3/13 to 3/18)

3. **Project #1 grades**: I received Project #1 grades from the TA this morning. Your Project #1 grad will be posted to the course website soon. If you have any question/problem, report your problem (or ask your question(s)) in the next 14 calendar days.

4. **Project #2 introduction** (only the highlights – for more details about the project, each of you is expected to carefully read the project handout):

   - Wireshark: Packet-capturing tool that "captures" any physical-layer packet locally observed at a local NIC (physical-layer packets that are destined to a host computer and that are "broad-casted" to a host computer).

   - Since the physical layer is the bottom (the lowest) layer in any protocol suite (including TCP/IP protocol suite), Wireshark captures all the packets from the physical-layer up to the application-layer in every packet it "captures".

   - Wireshark has many built-in functions, such as:

     (a) Automatically recognizes all the packet-encapsulation structure in every protocol layer (from the physical to the application layers).

     (b) Recognizes all the (existing) network protocols being used in each packet it captures:

     - Application layer: HTTP, FTP, telnet, DHCP, DNS, and etc.
     - Transport layer: TCP, UDP, ARP,
     - Network layer: IP,
     - Physical layer: those for Ethernet, Token-Ring, FDDI, ATM, frame-relays, and etc.

     (c) Offers many tools that summarize:

     - Captured-packet counts (for each protocol group)
     - Aggregated transmitted/received bytes (also as in the bps format)
     - The list of unique origin hosts (senders)
     - The list of unique destination hosts (receivers)
     - The number (count) of the detected packet collisions
     - Timestamps for each packet received/transmitted at the host computer Wireshark captured those packets
     - And more

- There are many websites in the Internet that explain/describe the built-in tools (it is strongly suggested that each of you conducts own research on "Wireshark"):

  (a) What tools are available
  (b) How those built-in tools can be used
  (c) What conclusions you can draw by using those built-in tools

- Although each of you is expected to study the tool (Wireshark) for network traffic analyses:

  (a) Each of you will earn credit by drawing logical conclusion(s) for each project question.

  (b) Each of you will earn credit by explaining your strategies for drawing you conclusion(s) for each project question.

  As the result, this project is not a cook-book project. Especially for Category III and IV questions, each of you is expected to develop own methods for drawing your conclusions.

- Each of you will receive a unique dataset (through email).

- The necessary knowledge to complete Project #2 will be continuously covered to the end of this month (February 2024).

5. **Project #3 will be introduced on 3/13** (only to the graduate students)

6. **Review midterm exam**

   QUESTION #3, #4, and #5