

# MCAST

## Computer Security Laboratory Project

### Project #2—Packet Capture and Analysis

The objective of this project is to understand the methods of packet capturing over a network using an open source packet capture program such as Wireshark. Network packet capturing is used by both legitimate users and illegitimate (hackers) users of the system to gather system activity information. You are required to capture raw packets that are moved in and out of the network interface card on a system and to perform a thorough analysis of the captured packets.

**Goal: Produce a plan to perform packet capture and analysis**

**Task 1: Read the documentation on Wireshark.**

**Task 2: Install Wireshark.**

**Task 3: Implement a packet capturing procedure using Wireshark. Perform an analysis of captured packets.**

**Assessment and Grading Criteria:**

**Task 1: (20%)**

- **What is the primary function of Wireshark?**
- **Describe the main fields in a typical output of a Wireshark capture.**

**Task 2: (20%)**

**Successful installation of Wireshark.**

**Task 3: (60%)**

- Completion of the following subtasks:
  - 1) Start capturing packets on your machine. Open your browser and go to the URL address [www.google.com](http://www.google.com). Describe the color coding scheme of the captured packets.
  - 2) Configure Wireshark to monitor any Telnet or FTP activity. Set the coloring scheme of those protocols to a unique color (say violet). Start packet capturing. Perform a telnet or FTP to remote host. Stop capturing packets. Sort the output by protocols. Describe the acquired sensitive information (login name, password, IP numbers, etc.)

