Introduction to Packet Analyzer (Software)

Dr. Xiaohai Li

Dept. of Computer Engineering Technology
New York City College of Technology

Fall 2014

Objectives

- To help you gain a better understanding of the fundamentals of data communications and computer networks.
- To help you learn the most up-to-date technologies.
- To help you have an enhanced learning experience.

Tools

- Real-world application tools are introduced.
- NOT just use simulation software.
- Some free, open-source software are available.
- A grant has been successfully granted for this course. Tools will be provided.

Packet/Protocol Analyzer

- A packet or protocol analyzer is basically a piece of software or a piece of hardware (with software), which can intercept and log data traffic passing over a digital network or part of a network.
- Also called "packet analyzer", "packet sniffer", "protocol analyzer", or for particular types of networks, "Ethernet sniffer" or "Wi-Fi sniffer".
- Allows networking professionals or network administrators to monitor, analyze and troubleshoot wired & wireless computer networks.

Some Popular Packet/Protocol Analyzers

Software Analyzers:

- Capsa from ColaSoft
- Observer from Network Instruments
- CommView from TamoSoft
- WANGUARD from AndriSoft
- Wireshark (Free and open-source)
- Ettercap (A popular free and open-source network security tool which can be used as packet sniffer.)

Some Popular PacketProtocol Analyzers

Hardware Analyzers:

- Ethertest from Frontline
- OptiView from Fluke.

Free Packet Analyzers

- Capsa Free: www.colasoft.com/capsa-free
- Wireshark: www.wireshark.org
- Ettercap: http://ettercap.github.com/ettercap/

Demonstration

The instructor demonstrates the use of Capsa.

Lab #2

Today's experiment:

- Learn to use Capsa, get familiar with it.
- Use Capsa to monitor data traffic and identify the source address of a large inbound data traffic.