Wireshark – Introduction

Wire 1

Due date: Friday, October 30th

Outline

- Overview
- Introduction
- Packet Sniffer
- Lab and Grading

Overview

- First of series of "sniffer" labs
  - This one designed to get you familiar with the Wireshark packet capture tool
- Work through a "cook-book" like set of instructions
  - Install Wireshark
  - Gather a trace
  - Basic investigation about performance
- Turn in
  - Trace
  - Answers to some questions

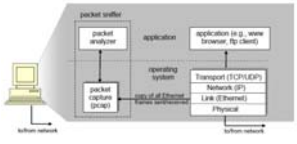
Motivation

"Tell me and I forget. Show me and I remember. Involve me and I understand."
Chinese proverb

- Better understanding by "seeing" network protocols in action
  - Seeing sequence of messages exchanged
  - Delving into details
- Can be done by simulation or observing real Internet data → we'll choose the latter
- Basic tool to do so is the **packet sniffer**

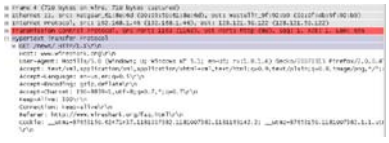
Packet Sniffer

- Captures ("sniffs") messages send/received by your computer
  - Also stores
- A passive application (does not send data itself)
  - Contrast that to active measurements
  - Gets a copy of all data send/received



Packet Sniffer w/Analyzer

- "Understand" format of the data
  - Layers of the network (e.g. HTTP, TCP, Ethernet …)
  - Within the layer (e.g. GET and POST in HTTP)



Wireshark

- One of the best open-source packet sniffers available today
- Mutiple platforms (Windows, Linux, Mac)
- Get it and install
- Note! You need your own computer
  - Capturing traffic requires root/administrator access
  - Or, borrow a friends for capture and can analyze on a public machine

The Lab

- Download and install Wireshark
  - http://www.wireshark.org
- Work through book lab
  - Wireshark Lab: Getting Started
- Answer questions in lab
  - Only a few on this one, more later

Submission

- Answers in text file
- Wireshark trace
- Zip up, submit
  - wire1 is lab name
- Web-based turnin
  - http://web.cs.wpi.edu/~kfisler/turnin.html
  - Should get password!
    - Email: cs3516-staff@cs.wpi.edu if not!

Grading Guidelines

- Wireshark 50% Answers 50%
- **90-100**: The Wireshark capture file is present, answers to the questions are thorough and accurate.
- **80-89**: The Wireshark capture file is present, all questions are answered and mostly accurate, but there are some minor errors.
- **70-79**: The Wireshark capture file is present, but an answer is missing or several answers are incomplete or inaccurate.
- **60-69**: The Wireshark capture file is present, but one or more answers are missing and/or most of the answers are incomplete or inaccurate.
- **0-50**: The Wireshark capture file is not present and the answers to the questions are incorrect or severely lacking.