Introduction to Protocol Analysis with Wireshark

Egemen K. Çetinkaya, Mohammed Alenazi and James P.G. Sterbenz

Department of Electrical Engineering & Computer Science
Information Technology & Telecommunications Research Center
The University of Kansas

malenazi@ittc.ku.edu
jpgs@eecs.ku.edu

http://www.ittc.ku.edu/~jpgs/courses/nets

Protocol Analysis with Wireshark

Outline

L1.0  EECS 780 laboratory outline
L1.1  Motivation and overview
L1.2  Wireshark installation and use
L1.3  Protocol analysis examples
L1.4  Getting started
EECS 780 Laboratories

Outline

L1.0 EECS 780 laboratory outline
L1.1 Motivation and overview
L1.2 Wireshark installation and use
L1.3 Protocol analysis examples
L1.4 Getting started

Semester Outline

• Wireshark labs
  - throughout semester, intuitive, based on textbook
• Wiki and web authoring
  - requires EECS, KU, or ITTC account
• Socket programming
  - relatively simple lab to demonstrate socket concepts
• Network simulation
  - lab to introduce network simulation
• Hands-on network performance evaluation
  - configure Cisco router, utilise open source tools
• Others if time permits
  - programmable networks using GpENI testbed
Motivation and Overview

Introduction

- Wireshark is a network protocol analyzer
  - www.wireshark.org
- First released in 1998 by Gerald Combs as Ethereal
  - many contributors around the world
- Open source and free software
- Graphical alternative to tcpdump
Motivation and Overview

• Powerful tool for network troubleshooting
• Sniffs and captures live traffic
• Filters data for ease of analysis
• Statistics and graphs available
• Used in industry and academia

Protocol Analysis with Wireshark

Wireshark Installation and Use

L1.0 EECS 780 laboratory outline
L1.1 Motivation and overview
L1.2 Wireshark installation and use
L1.3 Protocol analysis examples
L1.4 Getting started
Wireshark Installation

**Highlights**

- Wireshark can be installed on various platforms
  - UNIX, MS, Linux, Mac OS, etc
- Most recent release is v.1.8.4, Nov. 2012
- System requirements
  - section 1.2 at http://www.wireshark.org/docs/wsug_html/
  - rule of thumb: fast CPU, more memory is better
- FAQs and Wiki pages provide more information

**Overview**

- Installation of Wireshark requires
  - downloading the relevant package
    - building the source into binary if the source is downloaded
  - install binaries to their destinations
  - section 2 provides detailed installation instructions http://www.wireshark.org/docs/wsug_html/
- Windows installation includes WinPcap
  - packet capture library (also needed for tcpdump)
- Installation easy and intuitive
Wireshark Usage

Windows XP Installation

Go to wireshark.org

Click on Download Wireshark

Save and run the executable (.exe) file

Installation wizard is intuitive

pcap library is required to capture low-level network messages

WinPcap for Windows, libpcap for UNIX/Linux

Latest WinPcap release 4.1.2
Wireshark Installation

Windows XP Installation

Wireshark Usage

Main Features

- Capturing live traffic
  - data can be captured on wired or wireless medium
- Numerous protocols can be captured and analyzed
- Filtering is essential when dealing with lots of packets
  - filters can be applied on protocols, fields, values, etc.
  - filtering while capturing packets is possible
Wireshark GUI

Main Window

Menu
Main toolbar
Filter toolbar
Packet list pane
Packet details pane
Packet bytes pane
Status bar

Wireshark Usage

Starting Capture

To capture:
go to Capture menu and select Interfaces...

Start capturing on interface that has IP address

Other ways of capturing possible
Wireshark Usage

Capturing 1

Once the capturing starts, until the data is exchanged on Network Interface Card (NIC), main window will be blank.

Capturing 2

When packets exchanged on NIC, the packets will be dumped to main window.
**Wireshark Usage**

**Stopping Capture**

Capturing can be stopped by clicking on “Stop the running capture” button on the main toolbar.

**Wireshark Usage**

**Filtering**

Filter by entering the “protocol name or field name” and click the apply button in the filter menu.

Detailed filters can be applied by creating expressions.
Protocol Analysis with Wireshark

Protocol Analysis

- Packets/protocols can be analyzed after capturing
- Individual fields in protocols can be easily seen
- Graphs and flow diagrams can be helpful in analysis
Protocol Analysis and Examples

Packet Details Pane

Analysis is performed manually.

Example shows TCP segment with SYN and ACK fields set to 1.

Packet Byte Pane

Zoom in or out is possible in main toolbar.

Packet Byte pane consists of offset, Hex, and ASCII fields.
Protocol Analysis and Examples

Statistics – Flow Graph Example

TCP plots and flow graphs are available in the Statistics menu.

Example shows a flow diagram of the ping utility.

Protocol Analysis with Wireshark

Getting Started

L1.0 EECS 780 laboratory outline
L1.1 Motivation and overview
L1.2 Wireshark installation and use
L1.3 Protocol analysis and examples
L1.4 Getting started
Getting Started

Installation and First Lab Exercise

- Install Wireshark
- Go to student resources web page at http://www.pearsonhighered.com/pearsonhigheredus/educator/product/products_detail.page?isbn=9780132856201
- Complete first Wireshark Lab - *Getting Started*
- Familiarize yourself with Wireshark

Protocol Analysis with Wireshark

Acknowledgements

Some material in these foils comes from the textbook supplementary materials:

  http://kuroseross.com
- http://www.wireshark.org/
- http://www.winpcap.org/