Communication Networks Laboratory
The University of Kansas EECS 780
Introduction to Protocol Analysis with Wireshark

Trúc Anh N. Nguyên,
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

jgps@eecs.ku.edu

https://www.ittc.ku.edu/~jgps/courses/nets
EECS Laboratories

Outline

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

- Wireshark labs
  - throughout semester, intuitive, based on textbook
- Wiki and web authoring
  - requires KU, or ITTC account
- Socket programming
  - relatively simple lab to demonstrate socket concepts
- Network simulation
  - lab to introduce network simulation
Protocol Analysis with Wireshark
Motivation and Overview

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

Introduction

• Wireshark is a *network protocol analyzer*
  – captures network packets
  – displays packet data in details
  – 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

Purpose

• Powerful tool for
  – troubleshooting network problems
  – examining security problems
  – debugging protocol implementations
  – learning network protocol internals

• Used in industry and academia
Protocol Analysis with Wireshark

Wireshark Installation and Use

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

Highlights

• Wireshark can be installed on various platforms
  – UNIX, MS, Linux, Mac OS, etc.
• Most recent release is v.2.6.3, 29 August 2018
• 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
Wireshark Installation
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 10 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 4.1.3
Wireshark Installation

Windows 10 Installation
Wireshark Usage

Main Features

- Capture live traffic
  - data can be captured on wired or wireless medium
  - numerous protocols can be captured and analyzed
- Display packet in details
- Open files containing packet data captured
  - from other programs (tcpdump/WinDump)
- 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 field
- packet list pane
- packet details pane
- packet bytes pane
- status bar
Wireshark Usage

Starting Capture

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

Start capturing on interface that has IP address

Other ways of capturing possible
Wireshark Usage

Capturing

Once the capturing starts, main window will be blank until the data is exchanged on network interface (NIC)
Wireshark Usage

Capturing

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 or field name in Apply a display filter and enter

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

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

Protocol Analysis

- Packets and protocols can be analysed after capture
- 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
Protocol Analysis and Examples

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 Statistics menu.
Protocol Analysis with Wireshark

Getting Started

WS.0 EECS 780 laboratory outline
WS.1 Motivation and overview
WS.2 Wireshark installation and use
WS.3 Protocol analysis and examples
WS.4 Getting started
Getting Started
Installation and First Lab Exercise

• Install Wireshark and familiarise
• Download first Getting Started v7.0 exercise
  http://www-net.cs.umass.edu/wireshark-labs/
• Complete first Wireshark Lab – *Getting Started*
Getting Started
First Lab Exercise Submission

• Complete first Wireshark Lab – *Getting Started*
  – follow EECS 780 submission instructions and email report
    • to grader cc to professor
  – Subject: EECE780 - wireshark getting started
  – attach file `<lastname>`-wireshark-getting-started.pdf
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/