

Introduction to Wireshark

CS3C03/SE4C03

Jason Jaskolka

Department of Computing and Software
Faculty of Engineering
McMaster University
Hamilton, Ontario, Canada
jaskolj@mcmaster.ca

Winter 2013

Outline

- 1 What is Wireshark?
- 2 Getting Started with Wireshark
- 3 Capturing Live Network Data
- 4 Working with Captured Packets
- 5 References

Outline

- 1 What is Wireshark?
- 2 Getting Started with Wireshark
- 3 Capturing Live Network Data
- 4 Working with Captured Packets
- 5 References

Introduction

- One's understanding of network protocols can often be greatly deepened by:
 - Observing the sequence of messages exchanged between two protocol entities
 - Delving down into the details of protocol operation
 - Causing protocols to perform certain actions and then observing these actions and their consequences
- This can be done in simulated scenarios or in a real network environment
- The Wireshark labs are designed to take the latter approach; *you will learn by doing*

Packet Sniffers

- The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**
- A packet sniffer captures messages being sent from or received by your computer
- A packet sniffer will also typically store and/or display the contents of the various protocol fields in these captured messages
- Packet sniffers themselves are **passive**; they *cannot* explicitly send or receive packets

Packet Sniffers

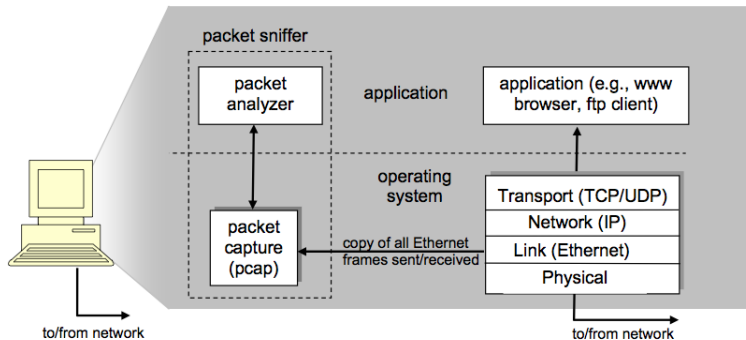


Figure : The structure of a packet sniffer

Packet Capture Library

- The **packet capture library (pcap)** receives a copy of every link-layer frame that is sent from or received by your computer
- Recall that messages exchanged by higher layer protocols such as HTTP, TCP, UDP, IP, etc. are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable
- Capturing all link-layer frames thus gives you all messages sent from or received by all protocols and applications

Packet Analyzer

- The **packet analyzer** is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network
- It understands the structure of different networking protocols
 - Displays the encapsulation and the fields along with their meanings of different packets specified by different networking protocols

What is Wireshark?

- Technically speaking, **Wireshark** is a network packet analyzer that uses the pcap library on your computer
 - It can only capture the packets on the types of networks that pcap supports
- Wireshark is very similar to **tcpdump**, but has a graphical front-end, plus some integrated sorting and filtering options

Intended Purposes

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn the internals of network protocols
- ... and many more

Some Features of Wireshark

- **Capture** live packet data from a network interface
- **Display** packets with very detailed protocol information
- **Open** and **Save** packet data captured
- **Import** and **Export** packet data from and to a lot of other capture programs
- **Filter** packets on many criteria
- **Search** for packets on many criteria
- **Colorize** packet display based on filters
- Create various **statistics**
- ... and many more

What Wireshark is Not

- Wireshark *is not* an intrusion detection system; it *will not* warn you when someone does strange things on your network
- Wireshark *will not* manipulate things on the network; it will only *measure* things from it
- Wireshark *does not* send packets on the network or do other active things

Outline

- 1 What is Wireshark?
- 2 Getting Started with Wireshark**
- 3 Capturing Live Network Data
- 4 Working with Captured Packets
- 5 References

Installing Wireshark

- Download the relevant package for your needs, i.e., source or binary distribution
- Build the source into a binary, if you have downloaded the source.
 - This may involve building and/or installing other necessary packages, including but not limited to:
 - GTK+
 - libpcap
 - X11
- Install the binaries into their final destinations

The Main Window

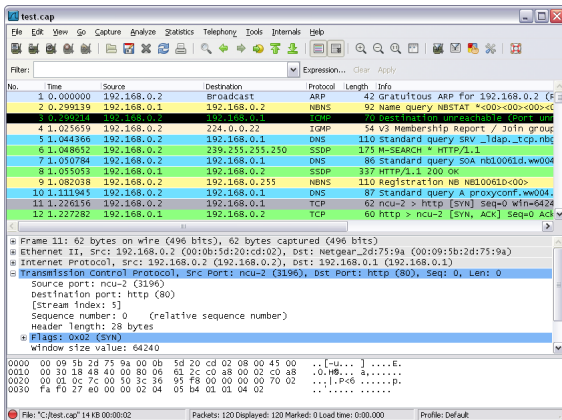


Figure : The Wireshark Main Window

The Main Toolbar



Figure : The Wireshark Main Toolbar

- Provides quick access to frequently used items from the menu
- Only the items useful in the current program state will be available; others will be greyed out

The Filter Toolbar

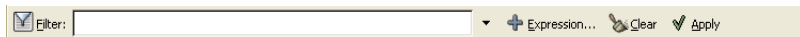
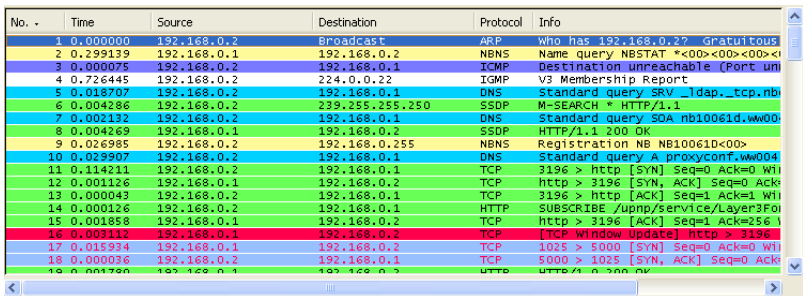


Figure : The Wireshark Filter Toolbar

- Allows you to quickly edit and apply display filters
- Entering a protocol name or other information can filter the information displayed in the Packet List Pane
- **Note:** This is also called the **display-filter-specification**

The Packet List Pane



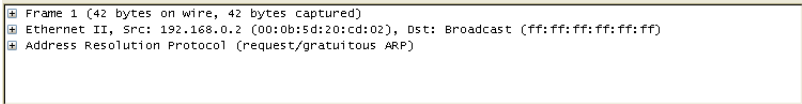
No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.2	Broadcast	ARP	Who has 192.168.0.2? Gratuitous
2	0.299139	192.168.0.1	192.168.0.2	NBNS	Name query NBSTAT *<00><00><00><0
3	0.000075	192.168.0.2	192.168.0.1	ICMP	Destination unreachable (Port un
4	0.726445	192.168.0.2	224.0.0.22	IGMP	V3 Membership Report
5	0.018707	192.168.0.2	192.168.0.1	DNS	Standard query SRV _ldap._tcp.nbi
6	0.004286	192.168.0.2	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
7	0.002132	192.168.0.2	192.168.0.1	DNS	Standard query SOA nb10061d.ww00
8	0.004269	192.168.0.1	192.168.0.2	SSDP	HTTP/1.1 200 OK
9	0.026985	192.168.0.2	192.168.0.255	NBNS	Registration NB NB10061D<00>
10	0.029907	192.168.0.2	192.168.0.1	DNS	Standard query A proxyconf.ww004
11	0.114211	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Ack=0 Win
12	0.001126	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack
13	0.000043	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Win
14	0.000126	192.168.0.2	192.168.0.1	HTTP	SUBSCRIBE /upnp/service/Layer3Foi
15	0.001858	192.168.0.1	192.168.0.2	TCP	http > 3196 [ACK] Seq=1 Ack=256
16	0.003112	192.168.0.1	192.168.0.2	TCP	[TCP window update] http > 3196
17	0.015934	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [SYN] Seq=0 Ack=0 Win
18	0.000036	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [SYN, ACK] Seq=0 Ack
19	0.001760	192.168.0.1	192.168.0.2	HTTP	HTTP/1.1 200 OK

Figure : The Wireshark Packet List Pane

The Packet List Pane

- Displays a one-line summary for each packet captured, including:
 - Packet number (assigned by Wireshark)
 - Time at which the packet was captured
 - Source and destination addresses
 - Protocol type
 - Other protocol-specific information contained in the packet
- The protocol type field lists the highest level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet
- **Note:** This is also called the **packet-listings window**

The Packet Details Pane



```
⊕ Frame 1 (42 bytes on wire, 42 bytes captured)
⊕ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊕ Address Resolution Protocol (request/gratuitous ARP)
```

Figure : The Wireshark Packet Details Pane

- Shows the protocols and protocol fields of the packet selected in the Packet List Pane
- The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed

The Packet Bytes Pane

```
0000  ff ff ff ff ff ff 00 0b 5d 20 cd 02 08 06 00 01  ..... } .....  
0010  08 00 06 04 00 01 00 0b 5d 20 cd 02 c0 a8 00 02  ..... } .....  
0020  00 00 00 00 00 00 c0 a8 00 02  ..... }
```

Figure : The Wireshark Packet Bytes Pane

- Shows the data of the current packet (selected in the Packet List Pane) in both ASCII and hexadecimal format
- **Note:** This is also called the **packet-contents window**

Outline

- 1 What is Wireshark?
- 2 Getting Started with Wireshark
- 3 Capturing Live Network Data**
- 4 Working with Captured Packets
- 5 References

Prerequisites

- Setting up Wireshark to capture packets for the first time can be tricky
- Some of the most common pitfalls include failures to:
 - Have root/Administrator privileges required to start a live capture
 - Choose the right network interface to capture packet data from
 - Capture at the right place in the network to see the traffic you want to see
 - ... and many more

Starting a Live Capture

- In order to begin a live capture, you must select an appropriate interface to capture on
- The choices vary by computer, but typically include:
 - **en0** or **eth0**: wired ethernet
 - **en1** or **eth1**: wireless ethernet
 - **lo0**: loopback
- Other choices may include firewire adapters, etc.
- Once you have selected the interface, you can start the packet capture

While a Live Capture is Running ...

- While a capture is running, the Capture Info Dialog Box is shown
- This dialog box will inform you about the number of captured packets and the time since the capture was started

While a Live Capture is Running ...

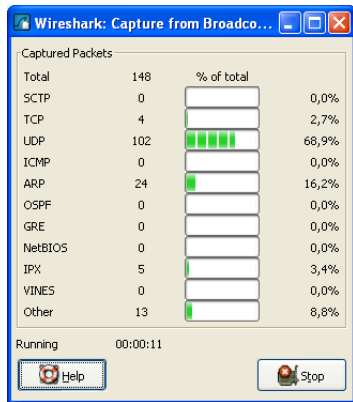


Figure : The Wireshark Capture Info Dialog Box

Outline

- 1 What is Wireshark?
- 2 Getting Started with Wireshark
- 3 Capturing Live Network Data
- 4 Working with Captured Packets**
- 5 References

Viewing Packets You Have Captured

- Once you have captured some packets, or you have opened a previously saved capture file, you can view the packets that are displayed in the Packet List Pane
- Simply clicking on a packet in the Packet List Pane, will bring up the selected packet in the Packet Details Pane and Packet Bytes Pane

Finding and Filtering Packets

- Wireshark provides a simple but powerful display filter language that allows you to build quite complex filter expressions
- You can compare values in packets as well as combine expressions into more specific expressions
- Familiarity with filtering will also help in finding packets that you have captured

Demonstration

- Demonstration

Outline

- 1 What is Wireshark?
- 2 Getting Started with Wireshark
- 3 Capturing Live Network Data
- 4 Working with Captured Packets
- 5 References**

References



Wireshark Foundation

Wireshark

Available: <http://www.wireshark.org>



Wireshark Foundation

Wireshark User's Guide

Available: http://www.wireshark.org/docs/wsug_html_chunked/



Wireshark Foundation

The Wireshark Wiki

Available: <http://wiki.wireshark.org>