WMLUG March 2017

Intro to Wireshark

Patrick TenHoopen

Wireshark

Wireshark is a multi-platform network protocol analyzer.

It was started by Gerald Combs in 1998 and was originally named Ethereal.

Riverbed is Wireshark's primary funding sponsor.

https://www.wireshark.org/

What Does a Protocol Analyzer Do?

It intercepts and logs traffic (consisting of packets) on a digital network for live or offline inspection.

The packets and data in the packets can be decoded and analyzed for anomalies or to diagnose problems.

Notes on Capturing Data

A switched network prevents traffic snooping by routing the traffic from the source to the destination only and not broadcasting to every connected device.

A monitoring port a.k.a. Switch Port Analyzer (SPAN) port can be set up to mirror traffic to the sniffing device but it can drop packets in a high-traffic network.

A network TAP (Test Access Point) is a passive splitter that can be used instead of a mirror port in high-traffic networks.

In addition, promiscuous mode needs to be enabled on the capturing device's NIC to gather all traffic and not just the traffic destined for the device.

Why Do Packet Analysis?

- Analyze network problems
- Detect network intrusion attempts
- Gather network statistics
- Monitor bandwidth utilization
- Debug client/server communications

User Interface Layout

The default layout consists of three panes, arranged vertically:

1. Packet List
   - Shows list of captured packets
2. Packet Details
   - Shows details of a selected packet
3. Packet Bytes
   - Shows raw packet data of the selected packet

Packet List Pane

The default displayed fields for a packet are:

- Number (No.)
- Time
- Source
- Destination
- Protocol
- Length
- Info

The packets are color coded by default. You can double-click a packet to view it in a new window.

Packet Details Pane
(for a TCP packet)

The packet data is presented in several groups of data in a collapsible tree layout.

Frame

Provides an overview of the highlighted packet. It shows the frame number, time related information regarding the packet, frame length, protocols within the frame, and the Wireshark coloring rule.

Ethernet II

Indicates the packet's source and destination.

(Layer 2 - Data Link layer - Frame)

Packet Details Pane, Cont.

Internet Protocol

Contains the source and destination information along with version, header details, and lifetime. The source and destination IP addresses are listed here.

(Layer 3 - Network layer - Packet)

Packet Details Pane, Cont.

TCP

Shows information about source and destination ports involved in the communication, sequence number, and different flags (along with their values).

(Layer 4 - Transport layer - Segment)

Protocol Info (label varies)

Shows information on application data (HTTP, FTP, DNS, etc.)

(Layer 5 - Application layer - Data)

Demo

Demo

- Interface
- Capturing data
- Inspecting data

Useful Videos

Optimal Wireshark Setup | Enhance Your Wireshark Experience

https://www.youtube.com/watch?v=F4l3CedRlJc&list=PLnKJHZhW_BuCPcIg6Ja2boDeHIRwoHMT-&index=2

Free Wireshark Courses by Laura Chappell, a Wireshark expert

https://www.lcuportal2.com/wireshark101.html