Learn how Wireshark Captures Traffic

The following has been taken from "*Wireshark 101 Essential Skills for Network Analysis, by Laura Chappell, Protocol Analysis Institute, 2013"*

Understanding how Wireshark captures traffic will affect how you use Wireshark's features. In this section we refer to the elements depicted in Figure 1.

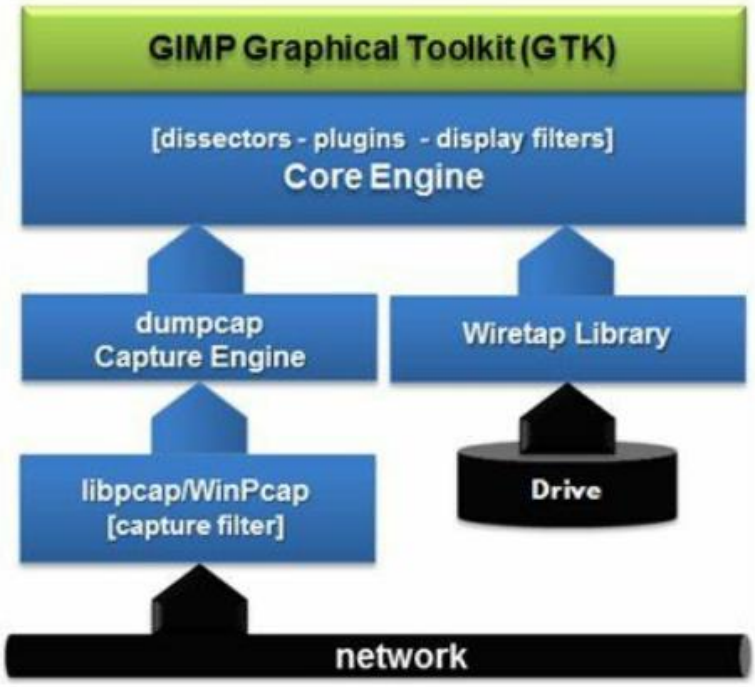

Figure 1. How Wireshark handles traffic from a live capture or from a saved trace file.

The Capture Process Relies on Special Link-Layer Drivers

When your computer connects to a network, it relies on a network interface card (such as an Ethernet card) and link-layer driver (such as an Atheros PCI-E Ethernet driver) to send and receive packets.

Wireshark also relies on network interface cards and link-layer drivers to pass up traffic for capture and analysis. Although the network interface cards are the same in both situations, when you use Wireshark, two special link-layer drivers are commonly used: WinPcap and libpcap. These special drivers provide access to raw data on the network.

WinPcap is the special link-layer driver used on a Windows host. Libpcap is the special link-layer driver used on *NIX hosts and OS X.

When you start capturing traffic with Wireshark, a tool called dumpcap is launched to do the actual capturing. Frames are passed up from the network, through one of these special link-layer drivers directly into Wireshark's Capture Engine. If you applied a capture filter (only capturing broadcast traffic for example), the frames that pass through the capture filter are passed up to the Capture Engine. Capture filters use Berkeley Packet Filtering (BPF) syntax.

The Dumpcap Capture Engine Defines Stop Conditions

The Dumpcap capture engine defines how the capture process runs and the stop conditions. For example, you can set up a capture to save frames to a set of 50 MB files and automatically stop after 6 files have been written. We refer to these files as trace files.

The current default trace file format is .pcapng (packet capture, next generation).

The Core Engine is the Goldmine

The Capture Engine passes frames up to the Core Engine. This is where Wireshark's power becomes evident. Wireshark supports thousands of dissectors that translate the incoming bytes into human readable format frames. The dissectors break apart the fields in the frames and often perform analysis on the content of those fields.

The Graphical Toolkit Provides the User Interface

The GIMP (GNU Image Manipulation Program) graphical toolkit provides the cross-platform interface for Wireshark. With very few exceptions, you can move seamlessly from a Wireshark system running on one platform to a Wireshark system running on another platform with no problems. The basic interface elements are the same.

The Wiretap Library is Used to Open Saved Trace Files

The Wiretap Library is used for the input/output functions for saved trace files. When you open a trace file (whether captured with Wireshark or another analysis tool), the Wiretap Library delivers the frames to the Core Engine.