TShark

TSHARK is used to dump and analyze network traffic and comes included with Wireshark®. Wireshark's most powerful feature is its vast array of display filters (over 216000 fields in 2000 protocols as of version 2.4.5)

How to capture network traffic with TSHARK

$tshark –D will give you a list of interfaces, you can capture network traffic using tshark –i for example;

$tshark –I “eth0”

TSHARK capture interface behavior

Network interface names should match one of the names listed in "tshark -D" (described above); a number, as reported by "tshark -D", can also be used. If you're using UNIX, "netstat -i" or "ifconfig -a" might also work to list interface names, although not all versions of UNIX support the -a option to ifconfig. If no interface is specified, TShark searches the list of interfaces, choosing the first non-loopback interface if there are any non-loopback interfaces, and choosing the first loopback interface if there are no non-loopback interfaces. If there are no interfaces at all, TShark reports an error and doesn't start the capture. Pipe names should be either the name of a FIFO (named pipe) or ``-'' to read data from the standard input. Data read from pipes must be in standard pcap format. This option can occur multiple times. When capturing from multiple interfaces, the capture file will be saved in pcap-ng format. Note: the Win32 version of TShark doesn't support capturing from pipes!To see the full collection of styles in this template, display the “Styles task pane” by clicking in the lower-right corner of the Style Gallery above.

Reading network captures with TSHARK –r

The –r option will allow you to read packets contained within a .pcap .cap .pcapng file respectively.

TSHARK General Usage

Read packet data from infile, can be any supported capture file format (including gzipped files). It is possible to use named pipes or stdin (-) here but only with certain (not compressed) capture file formats (in particular: those that can be read without seeking backwards).

Examples

- $ tshark -r "filename"
    - To write raw packet data to file
        - **$ tshark -i "eth0" -w "filename"**
- NOTE: -w provides raw packet data, not text. If you want text output you need to redirect stdout (e.g. using '>'), don't use the -w option for this.