Tshark Display Filters

(By : - Pratyush and Sreelakshmi)

Tshark - A network protocol analyzer

Installation

sudo apt-get install tshark	Install TShark on Ubuntu
tshark -i wlan0 -w capture-output.pcap	Basic Usage

Lower Case Options

-a <capture autostop condition>	Specify a criterion that specifies when TShark is to stop writing to a capture file
-b <capture ring buffer option>	Run Tshark in "multiple files" mode. Ex: -b filesize:1000 -b files:5 results in a ring buffer of five files of size one megabyte each
-c <capture packet count>	Set the maximum number of packets to read when capturing live data. If reading a capture file, set the maximum number of packets to read
-d <layer type>==<selector>,<decode-as protocol>	Specify how a layer type should be dissected. Ex: -d tcp.port==8888,http will decode any traffic running over TCP port 8888 as HTTP
-e <field>	Add a field to the list of fields to display if -T fields is selected
-f <capture filter>	Set the capture filter expression
-h	Print the version and options and exits

-i <capture interface> | -	Set the name of the network interface or pipe to use for live packet capture
-n	Disable network object name resolution (such as hostname, TCP and UDP port names); the -N flag might override this one
-p	Don't put the interface into promiscuous mode
-r <infile>	Read packet data from infile, can be any supported capture file format (including gzipped files)
-s <capture snaplen>	Set the default snapshot length to use when capturing live data
-u <seconds type>	Specifies the seconds type. Valid choices are: s for seconds hms for hours, minutes and seconds
-v	Print the version and exit
-w <outfile> | -	Write raw packet data to outfile or to the standard output if outfile is '-'
-x	Print a hex and ASCII dump of the packet data after printing the summary
-y <capture link type>	Set the data link type to use while capturing packets. The values reported by -L are the values that can be used

Upper Case Options

-B <capture buffer size>	Set capture buffer size (in MiB, default is 2 MiB)
-C <configuration profile>	Run with the given configuration profile
-D	Print a list of the interfaces on which TShark can capture, and exit
-E <field print option>	Set an option controlling the printing of fields when -T fields is selected
-F <file format>	Set the file format of the output capture file written using the -w option
-H <input hosts file>	Read a list of entries from a "hosts" file, which will then be written to a capture file

-I	Put the interface in "monitor mode"; this is supported only on IEEE 802.11 Wi-Fi interfaces, and supported only on some operating systems
-K <keytab>	Load kerberos crypto keys from the specified keytab file. Ex: -K krb5.keytab
-N <name resolving flags>	Turn on name resolving only for particular types of addresses and port numbers, with name resolving for other types of addresses and port numbers turned off
-Q	When capturing packets, only display true errors
-S <separator>	Set the line separator to be printed between packets
-V	Print a view of the packet details
-W <file format option>	Save extra information in the file if the format supports it

-X <eXtension options>	Specify an option to be passed to a TShark module. The eXtension option is in the form extension_key:value
-Y <displaY filter>	Applies specified filter before printing a decoded form of packets or writing packets to a file

Special Options

-2	Perform a two-pass analysis. Also permits reassembly frame dependencies to be calculated correctly
-G	A special mode to dump one of several types of internal glossaries and then exit
-z <statistics>	Collects various types of statistics and display the result after finishing reading the capture file