Cheatography

tshark - Wireshark Command Line Cheat Sheet

by mbwalker via cheatography.com/26872/cs/7667/

Capture interface options

-i <interface>	name or index of interface (defaults to 1st non-loopback)
-f <capture filter>	packet filter in libpcap filter syntax
-p	disable capturing in promiscuous mode
-B <buffer size>	size of kernel buffer (def. 2MB)
-y <link type>	link layer type (def. first appropriate)
-D	print list of interfaces and exit
-L	print list of link layer types and exit

Capture stop conditions

-c <packet count>	stop after n packets (def. infinite)
-a <autostop condition>	duration:<num> - stop after <num> seconds filesize:<num> - stop file after <num> KB files:<num> - stop after <num> files

Capture output

-b <ringbuffer opt>	**duration:<num>** - switch to next file after <num> seconds **filesize:<num>** - switch to next file after <num> KB **files:<num>** - ringbuffer: replace after <num> files

Processing options

-2	perform a two-pass analysis
-R <read filter>	packet read filter in Wireshark display filter syntax
-Y <display filter>	packet display filter in Wireshark display filter syntax
-n	disable all name resolutions
-N <name resolve flags>	enable specific name resolutions: "mnNtCd"
-d <layer type>==<selector>,<decode_as_protocol>	decode as, see the tshark man page for details
-H <hosts file>	read a list of entries from a hosts file which will then be written to a capture file (implies -W n)
--disable-protocol <proto_name>	disable dissection of <proto_name>

Processing options (cont)

--enable-heuristic <short_name>	enable dissection of heuristic protocol
--disable-heuristic <short_name>	disable dissection of heuristic protocol

Micellaneous options

-h	display help and exit
-v	dispaly version info and exit
-o <name>:<value>	override preference setting
-K <keytab>	keytab file to use for Kerberos decryption
-G <report>	dump one of several available reports and exit default report="fields" use -G ? for more help

RPCAP options

-A <user>:<password>	use RPCAP password authentication

Input file options

-r <infile>	set the filename to read from (- to read from stdin)

Output file options

-w <outfile|->	write packets to a pcap-format file named "outfile" (or to stadard output file for -)
-C <config profile>	start with specified configuration profile
-F <output file type>	set the output file type (def. is pcapng) an empty -F option will list the file types
-V	add output of packet tree (Packet Details)
-O <protocols>	only show packet details of these protocols (comma separated)
-P	print packet summary even while writing to file

Output file options (cont)	
-S <separator>	the line separator to print between packets
-x	add output of hex and ASCII dump (Packet Bytes)
-T pdml|ps|psml|text|fields	format of text output (def: text
-e <field>	field to print if -Tfields selected (tcp.port, ws.col.info) this option can be repeated to print multiple fields
-E <fieldsoption>=<value>	set options for output when -Tfields selected: **header=y|n** - switch headers on and off **separator=/t|/s|<char>** - select tab, space, printable character as separator **occurence=f|L|a** - print first, last or all occurences of each field **aggregator=,|/s|/<char>** - select comma, space, printable character as aggregator **quote=d|s|n** - select double, single or no quotes for values
-t a|ad|d|dd|e|r|u|ud	output format of timestamps (def: r rel. to first)
-u s|hms|	output format of seconds (def: s - seconds)
-l	flush standard output after each packet
-q	be more quiet on stdout (when using statistics)
-Q	only log true errors to stderr (quieter that -q)

Output file options (cont)	
-g	enable group read access on the output file(s)
-W n	save extra info in the file, if supported n= write network address resolution info
-X <key>:<value>	eXtension options, see tshark man page for details
-z <statistics>	various statistics, see tshark man page for details
--capture-comment <comment>	add a capture comment to the newly created output file (**only for pcapng format**)