TShark Cheat Sheet v1.4

Key Points:

- “ **-t ad** ” will show absolute time. Default is “**-t r**”, time relative to start of file.
- “ **-T fields** “ must precede the usage of “ **-e** “ when displaying columns, and must include “**-R**” or “**-Y**” (depending on version)
- “ **tshark -h** “ will show a condensed version of the Manual page, and entering blank flags should produce a list of options

View Number of Available Streams:
tshark -r (file) **-T fields -e tcp.stream | sort -nu** (mind that the **stream index starts at zero**)

Follow a TCP stream:
tshark -r (file) **-qz follow,tcp,ascii,#** (replace # with desired stream index number)

Follow TCP streams where IP1:Port1 talk to IP2:Port2:
tshark -r (file) **-qz follow,tcp,ascii,IP1:PORT1,IP2:PORT2**

View Frame Summaries:
tshark -r (file) **-nSR (display filter)** (display filters what you want to see, i.e. “ -R ‘http && ip.src=1.2.3.4’ ”)

View Verbose Frame Information:
tshark -r (file) **-nVR (display filter)**

Decode As…:
tshark -r (file) -d **layerType==specifiedValue,desiredProtocol** (i.e. “ -d tcp.port==8888,http” will decode TCP 8888 traffic as http)

Display Column Data in Desired Format:
tshark -r (file) **-T fields -e (COLUMN) -e (COLUMN) -R (display filter)** (“ -e “ can be used once or many times)

View Packet Bytes:
tshark -r (file) **-O dns,http** (note -O is the filter that invokes Bytes view and is a comma-separated list of services to view)

Export Specific Information to File:
tshark **-r (INFILE) -R (display filter) -w (OUTFILE) -F (FORMAT)** (give -F no arguments and it will present a list of options)

Statistics Usage:
tshark -r (file) **-qz http,stat,** (the last comma needs to be there)
tshark -r (file) **-qz http,tree**
tshark -r (file) **-qz http_req,tree**
tshark -r (file) **-qz http_srv,tree**
tshark -r (file) **-qz conv,tcp,[filter]** (can omit filter / displays conversations in a file by transport/filter)
tshark -r (file) **-qz expert,[error/warn/note/chat][filter]** (can omit bracketed items to display all expert warning levels)
tshark -r (file) **-qz io,phs,[filter]** (can omit filter / protocol hierarchy, i.e. “ io,phs ” or “ io,phs,tcp.stream==1 ”)

Examples:
tshark -r Bad.pcap -qz follow,tcp,ascii,2 (will show stream 2 of a PCAP file)
tshark -r Bad.pcap -T fields -e tcp.stream -e http.request.method -e http.host -R http.request (prints specified columns)
tshark -r Bad.pcap -R dns -w BadDNS.pcap -F pcapng (copies all DNS to a new PCAP file)

Commonly-Used Display Filters:
(note that ‘ referrer ’ is supposed to only have one ‘ r ’ due to a misspelling in the RFC)
Use “ && ”, “ || ”, “ == “, and/or “(filter) contains x” to form your arguments

http
http.user_agent
http.referer
http.content_type

http.request
http.request.method
http.request.uri
http.request.full_uri

http.response
http.response.code
http.response.phrase
ftp-data

http.host
dns
rdp
tcp.srcport

udp.dstport
ip.dst
tcp.flags.syn
ssl.handshake.extensions_server_name

Last Updated: 17 Aug 2016 // JB