tshark Reference Guide

General

Getting Help

Usage: -h

Example: `tshark -h`

Note: if you use the -h option anywhere in the command line, it overrides other options and just displays the help page.

More detailed information on tshark can be found online at:
https://www.wireshark.org/docs/man-pages/tshark.html

Manual pages for other Wireshark-related command-line tools can be found at:
https://www.wireshark.org/docs/man-pages/

Capturing Traffic

List Interfaces

Usage: -D

Example: `tshark -D`

Capture from an Interface

Usage: -i <namelindex>

Example: `tshark -i eth0`

Note: default is to capture from the first non-loopback interface in the list.

Using a Capture Filter

Usage: -f

Example: `tshark -i eth0 -f "host 10.1.2.3"`

Note: for more info on capture filters, see https://wiki.wireshark.org/CaptureFilters.

Output to a File

Usage: -w

Example: `tshark -i eth0 -w my_capture.pcap`

FOCAL POINT ACADEMY

Viewing and Filtering Traffic

Reading from a Capture File

Usage: -r <filename>

Example: `tshark -r example.pcap`

(Unfiltered) output:

- Packet number
- Time (seconds since beginning of capture is the default format)
- Source IP address
- Destination IP address
- Protocol
- Frame length
- Information (this is an aggregated field where Wireshark/tshark provides summary information for the packet, depending on the protocol in use)

Filtering Using a Display Filter

Usage: -Y "<display filter>"

Example: `tshark -r example.pcap -Y "ip.addr == 192.168.1.1"`

Note: can be used with a capture file or during live capture. For more info on display filters, see https://wiki.wireshark.org/DisplayFilters.

Filtering Using a Read Filter

Usage: -2 -R "<read filter>"

Example: `tshark -r example.pcap -2 -R "ip.addr == 192.168.1.1"`

Note: must include the -2 option to perform two-pass analysis. Read filters can be used before additional filtering or processing (e.g., statistics) is done. Otherwise, they behave the same as display filters.

Time Display Format

Usage: -t <option>

Example: `tshark -r example.pcap -t ad`

Note: use the option "-t help" to get the full list of time display options.

Capture File Information

To obtain summary info about a capture file, use the command-line tool *capinfos* that comes bundled with Wireshark/tshark. This utility outputs the same information that is available from the 'Capture File Properties' option in the Statistics menu of Wireshark.

Usage: capinfos <filename>

Example: `capinfos example.pcap`

Guide created by Focal Point – https://www.focal-point.com

Using Streams

Usage: -z follow,<protocol>,<format>,<filter>
Examples:

```
tshark -r example.pcap -q -z follow,tcp,hex,10.1.2.3:34856,10.10.0.4:80
tshark -r example.pcap -q -z follow,http,ascii,0
```

Note: use the option "-z help" to get the full list of available protocols. The filter value can be a socket pair (IP address and port number) or a stream number.

Statistics

In general, the -z option is used with a two-part argument to provide statistical information from a live capture or capture file. It is commonly combined with the -q option for quiet output as the desired result is usually just the statistics and not packet details.

Details of the -z options are not included in the regular help page. Use the -z option with the value "help" to get a full list.

Important note: using a display filter does not affect the output of the statistics options. They will still produce output for the entire capture or file. Use a read filter to filter out packets before the statistical analysis is performed.

Protocol Hierarchy

Usage: -z io,phs
Examples:

```
tshark -r example.pcap -q -z io,phs
tshark -r example.pcap -2 -R "ip.addr == 209.85.239.20" -q -z io,phs
```

Hosts

Usage: -z hosts
Example: `tshark -r example.pcap -q -z hosts`
Note: outputs IP addresses with related host names. Can specify IPv4 or IPv6 if desired. Both are dumped by default.

Endpoints

Usage: -z endpoints,<protocol>
Example: `tshark -r example.pcap -q -z endpoints,tcp`
Note: use the option "-z help" to get the full list of available protocols.

Conversations

Usage: -z conv,<protocol>
Example: `tshark -r example.pcap -q -z conv,ip`
Note: use the option "-z help" to get the full list of available protocols.

Percentage Trees

There are various options for showing packet counts and percentages for different types of objects, such as HTTP requests. The following are some useful examples.

IP addresses with usage percentages (IP | Number of Packets | Percent):

```
tshark -r example.pcap -q -z ip_hosts,tree
```

List of HTTP transactions with percentages (type (Request | Response) | percentage):

```
tshark -r example.pcap -q -z http,tree
```

HTTP requests broken down by HTTP host with percentages:

```
tshark -r example.pcap -q -z http_req,tree
```

Packet lengths with percentages:

```
tshark -r example.pcap -q -z plen,tree
```

Destination port by source IP address:

```
tshark -r example.pcap -q -z dests,tree
```

Specifying Output Fields

Usage: -T fields -e <value>
Example: `tshark -r example.pcap -T fields -e ip.src -e ip.dst`
Note: using fields restricts the output to only the field(s) you specify. (Multiple fields can be specified if desired.) Fields can be combined with display or read filters to narrow down the results.
Example:

```
tshark -r example.pcap -Y "http.user_agent" -T fields -e ip.src -e http.user_agent
```

Exporting Objects

Usage: --export-objects <protocol>,<dest_dir>
Example: `tshark -r example.pcap --export-objects http,http_objects`
Note: if dest_dir does not exist, tshark will create it. Use the option "--export-objects help" to get a list of available protocols.

Expert Info

Usage: -z expert
Example: `tshark -r example.pcap -q -z expert`
Note: outputs a list of errors, warnings, and analytic notes.