

### 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<br>filesize:<num> - stop file after <num> KB<br>files:<num> - stop after <num> files |

### Capture output

|                     |                                                                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -b <ringbuffer opt> | <b>duration:&lt;num&gt;</b> - switch to next file after <num> seconds<br><b>filesize:&lt;num&gt;</b> - switch to next file after <num> KB<br><b>files:&lt;num&gt;</b> - 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: "mnN-tCd"                                                          |
| -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                | display 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<br>default report="fields"<br>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 standard output file for -)   |
| -C <config profile>   | start with specified configuration profile                                               |
| -F <output file type> | set the output file type (def. is pcapng)<br>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                                          |



By **mbwalker**  
[cheatography.com/mbwalker/](https://cheatography.com/mbwalker/)

Not published yet.  
Last updated 8th December, 2020.  
Page 1 of 2.

Sponsored by **ApolloPad.com**  
Everyone has a novel in them. Finish Yours!  
<https://apollopad.com>

### 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 p-smll text fields | format of text output (def: text)                                                                                                                                                                                                                                                                                                                                                                                                                 |
| -e <field>                    | field to print if -Tfields selected (tcp.port, ws.col.info)<br>this option can be repeated to print multiple fields                                                                                                                                                                                                                                                                                                                               |
| -E <fieldsoption>=<value>     | set options for output when -Tfields selected:<br><b>header=y n</b> - switch headers on and off<br><b>separator=t /s &lt;char&gt;</b> - select tab, space, printable character as separator<br><b>occurrence=f l a</b> - print first, last or all occurrences of each field<br><b>aggregator=,/s /&lt;char&gt;</b> - select comma, space, printable character as aggregator<br><b>quote=d s n</b> - 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 than -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<br>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 ( <b>only for pcapng format</b> ) |



By **mbwalker**  
[cheatography.com/mbwalker/](https://cheatography.com/mbwalker/)

Not published yet.  
Last updated 8th December, 2020.  
Page 2 of 2.

Sponsored by **ApolloPad.com**  
Everyone has a novel in them. Finish Yours!  
<https://apollopad.com>