## NAME

dumpcap − Dump network traffic

## SYNOPSIS

**dumpcap** [ **−a**|**−−autostop** <capture autostop condition> ] ...
[ **−b**|**−−ring−buffer** <capture ring buffer option> ] ... [ **−B**|**−−buffer−size** <capture buffer size> ]
[ **−c** <capture packet count> ] [ **−C** <byte limit> ] [ **−d** ] [ **−D**|**−−list−interfaces** ] [ **−f** <capture filter> ]
[ **−g** ] [ **−h**|**−−help** ]
[ **−i**|**−−interface** <capture interface>|rpcap://<host>:<port>/<capture interface>|TCP@<host>:<port>|− ]
[ **−I**|**−−monitor−mode** ] [ **−k** <freq>,[<type>],[<center_freq1>],[<center_freq2>] ]
[ **−L**|**−−list−data−link−types** ] [ **−M** ] [ **−n** ] [ **−N** <packet limit> ] [ **−p**|**−−no−promiscuous−mode** ]
[ **−−ifdescr** <description> ] [ **−−ifname** <name> ] [ **−P** ] [ **−q** ]
[ **−s**|**−−snapshot−length** <capture snaplen> ] [ **−S** ] [ **−t** ] [ **−v**|**−−version** ] [ **−w** <outfile> ]
[ **−y**|**−−linktype** <capture link type> ] [ **−−capture−comment** <comment> ] [ **−−list−time−stamp−types** ]
[ **−−time−stamp−type** <type> ]

## DESCRIPTION

**Dumpcap** is a network traffic dump tool. It lets you capture packet data from a live network and write the packets to a file. **Dumpcap**'s default capture file format is **pcapng** format. When the **−P** option is specified, the output file is written in the **pcap** format.

Without any options set it will use the libpcap, Npcap, or WinPcap library to capture traffic from the first available network interface and writes the received raw packet data, along with the packets' time stamps into a pcap file.

If the **−w** option is not specified, **Dumpcap** writes to a newly created pcap file with a randomly chosen name. If the **−w** option is specified, **Dumpcap** writes to the file specified by that option.

Packet capturing is performed with the pcap library. The capture filter syntax follows the rules of the pcap library.

## OPTIONS

−a|−−autostop <capture autostop condition>

Specify a criterion that specifies when **Dumpcap** is to stop writing to a capture file. The criterion is of the form *test:value*, where *test* is one of:

**duration**:*value* Stop writing to a capture file after *value* seconds have elapsed. Floating point values (e.g. 0.5) are allowed.

**files**:*value* Stop writing to capture files after *value* number of files were written.

**filesize**:*value* Stop writing to a capture file after it reaches a size of *value* kB. If this option is used together with the −b option, dumpcap will stop writing to the current capture file and switch to the next one if filesize is reached. Note that the filesize is limited to a maximum value of 2 GiB.

**packets**:*value* Stop writing to a capture file after *value* packets have been written. Same as **−c** <capture packet count>.

−b|−−ring−buffer <capture ring buffer option>

Cause **Dumpcap** to run in "multiple files" mode. In "multiple files" mode, **Dumpcap** will write to several capture files. When the first capture file fills up, **Dumpcap** will switch writing to the next file and so on.

The created filenames are based on the filename given with the **−w** option, the number of the file and on the creation date and time, e.g. outfile_00001_20220714120117.pcap, outfile_00002_20220714120523.pcap, ...

With the *files* option it's also possible to form a "ring buffer". This will fill up new files until the number of files specified, at which point **Dumpcap** will discard the data in the first file and start writing to that file and so on. If the *files* option is not set, new files filled up until one of the capture stop conditions match (or until the disk is full).

The criterion is of the form *key:value*, where *key* is one of:

**duration**:*value* switch to the next file after *value* seconds have elapsed, even if the current file is not completely filled up. Floating point values (e.g. 0.5) are allowed.

**files**:*value* begin again with the first file after *value* number of files were written (form a ring buffer). This value must be less than 100000. Caution should be used when using large numbers of files: some filesystems do not handle many files in a single directory well. The **files** criterion requires either **duration**, **interval** or **filesize** to be specified to control when to go to the next file. It should be noted that each **−b** parameter takes exactly one criterion; to specify two criterion, each must be preceded by the **−b** option.

**filesize**:*value* switch to the next file after it reaches a size of *value* kB. Note that the filesize is limited to a maximum value of 2 GiB.

**interval**:*value* switch to the next file when the time is an exact multiple of *value* seconds. For example, use 3600 to switch to a new file every hour on the hour.

**packets**:*value* switch to the next file after it contains *value* packets.

**printname**:*filename* print the name of the most recently written file to *filename* after the file is closed. *filename* can be `stdout` or − for standard output, or `stderr` for standard error.

Example: **−b filesize:1000 −b files:5** results in a ring buffer of five files of size one megabyte each.

−B|−−buffer−size <capture buffer size>

Set capture buffer size (in MiB, default is 2 MiB). This is used by the capture driver to buffer packet data until that data can be written to disk. If you encounter packet drops while capturing, try to increase this size. Note that, while **Dumpcap** attempts to set the buffer size to 2 MiB by default, and can be told to set it to a larger value, the system or interface on which you're capturing might silently limit the capture buffer size to a lower value or raise it to a higher value.

This is available on UNIX systems with libpcap 1.0.0 or later and on Windows. It is not available on UNIX systems with earlier versions of libpcap.

This option can occur multiple times. If used before the first occurrence of the **−i** option, it sets the default capture buffer size. If used after an **−i** option, it sets the capture buffer size for the interface specified by the last **−i** option occurring before this option. If the capture buffer size is not set specifically, the default capture buffer size is used instead.

−c <capture packet count>

Set the maximum number of packets to read when capturing live data. Same as **−a packets:**<capture packet count>.

−C <byte limit>

Limit the amount of memory in bytes used for storing captured packets in memory while processing it. If used in combination with the **−N** option, both limits will apply. Setting this limit will enable the usage of the separate thread per interface.

−d

Dump the code generated for the capture filter in a human−readable form, and exit.

−D|−−list−interfaces

Print a list of the interfaces on which **Dumpcap** can capture, and exit. For each network interface, a number and an interface name, possibly followed by a text description of the interface, is printed. The interface name or the number can be supplied to the **−i** option to specify an interface on which to capture.

This can be useful on systems that don’t have a command to list them (UNIX systems lacking **ifconfig −a** or Linux systems lacking **ip link show**). The number can be useful on Windows systems, where the interface name might be a long name or a GUID.

Note that "can capture" means that **Dumpcap** was able to open that device to do a live capture. Depending on your system you may need to run dumpcap from an account with special privileges (for example, as root) to be able to capture network traffic. If "**dumpcap −D**" is not run from such an account, it will not list any interfaces.

−f <capture filter>

Set the capture filter expression.

The entire filter expression must be specified as a single argument (which means that if it contains spaces, it must be quoted).

This option can occur multiple times. If used before the first occurrence of the **−i** option, it sets the default capture filter expression. If used after an **−i** option, it sets the capture filter expression for the interface specified by the last **−i** option occurring before this option. If the capture filter expression is not set specifically, the default capture filter expression is used if provided.

Pre−defined capture filter names, as shown in the GUI menu item Capture→Capture Filters, can be used by prefixing the argument with "predef:". Example: **−f "predef:MyPredefinedHostOnlyFilter"**

−g

This option causes the output file(s) to be created with group−read permission (meaning that the output file(s) can be read by other members of the calling user’s group).

−h|−−help

Print the version and options and exits.

−i|−−interface <capture interface>|rpcap://<host>:<port>/<capture interface>|TCP@<host>:<port>|−

Set the name of the network interface or pipe to use for live packet capture.

Network interface names should match one of the names listed in "**dumpcap −D**" (described above); a number, as reported by "**dumpcap −D**", can also be used. If you’re using UNIX, "**netstat −i**", "**ifconfig −a**" or "**ip link**" might also work to list interface names, although not all versions of UNIX support the **−a** option to **ifconfig**.

If no interface is specified, **Dumpcap** searches the list of interfaces, choosing the first non−loopback interface if there are any non−loopback interfaces, and choosing the first loopback interface if there are no non−loopback interfaces. If there are no interfaces at all, **Dumpcap** reports an error and doesn’t start the capture.

Pipe names should be either the name of a FIFO (named pipe) or "−" to read data from the standard input. On Windows systems, pipe names must be of the form "\\pipe\.*pipename*". Data read from pipes must be in standard pcapng or pcap format. Pcapng data must have the same endianness as the capturing host.

"TCP@<host>:<port>" causes **Dumpcap** to attempt to connect to the specified port on the specified host and read pcapng or pcap data.

This option can occur multiple times. When capturing from multiple interfaces, the capture file will be saved in pcapng format.

−−ifdescr> <description>

Use *description* as the description in the capture file for the interface or pipe specified before it with **−i**.

−−ifname> <name>

Use *name* as the name in the capture file for the the interface or pipe specified before it with **−i**.

−I|−−monitor−mode

Put the interface in "monitor mode"; this is supported only on IEEE 802.11 Wi−Fi interfaces, and supported only on some operating systems.

Note that in monitor mode the adapter might disassociate from the network with which it’s associated, so that you will not be able to use any wireless networks with that adapter. This could prevent accessing files on a network server, or resolving host names or network addresses, if you are capturing in monitor mode and are not connected to another network with another adapter.

This option can occur multiple times. If used before the first occurrence of the **−i** option, it enables the monitor mode for all interfaces. If used after an **−i** option, it enables the monitor mode for the interface specified by the last **−i** option occurring before this option.

−k <freq>,[<type>],[<center_freq1>],[<center_freq2>>

Set the channel on the interface; this is supported only on IEEE 802.11 Wi−Fi interfaces, and supported only on some operating systems.

*freq* is the frequency of the channel. *type* is the type of the channel, for 802.11n and 802.11ac. The values for *type* are

NOHT

Used for non−802.11n/non−802.1ac channels

HT20

20 MHz channel

HT40−

40 MHz primary channel and a lower secondary channel

HT40+

40 MHz primary channel and a higher secondary channel

HT80

80 MHz channel, with *centerfreq1* as its center frequency

VHT80+80

two 80 MHz channels combined, with *centerfreq1* and *centerfreq2* as the center frequencies of the two channels

VHT160

160 MHz channel, with *centerfreq1* as its center frequency

−L|−−list−data−link−types

List the data link types supported by the interface and exit. The reported link types can be used for the **−y** option.

−M

When used with **−D**, **−L**, **−S** or **−−list−time−stamp−types** print machine−readable output. The machine−readable output is intended to be read by **Wireshark** and **TShark**; its format is subject to change from release to release.

−n

Save files as pcapng. This is the default.

−N <packet limit>

Limit the number of packets used for storing captured packets in memory while processing it. If used in combination with the **−C** option, both limits will apply. Setting this limit will enable the usage of the separate thread per interface.

−p|−−no−promiscuous−mode

*Don't* put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, **−p** cannot be used to ensure that the only traffic that is captured is traffic sent to or from the machine on which **Dumpcap** is running, broadcast traffic, and multicast traffic to addresses received by that machine.

This option can occur multiple times. If used before the first occurrence of the **−i** option, no interface will be put into the promiscuous mode. If used after an **−i** option, the interface specified by the last **−i** option occurring before this option will not be put into the promiscuous mode.

−P

Save files as pcap instead of the default pcapng. In situations that require pcapng, such as capturing from multiple interfaces, this option will be overridden.

−q

When capturing packets, don’t display the continuous count of packets captured that is normally shown when saving a capture to a file; instead, just display, at the end of the capture, a count of packets captured. On systems that support the SIGINFO signal, such as various BSDs, you can cause the current count to be displayed by typing your "status" character (typically control−T, although it might be set to "disabled" by default on at least some BSDs, so you’d have to explicitly set it to use it).

−s|−−snapshot−length <capture snaplen>

Set the default snapshot length to use when capturing live data. No more than *snaplen* bytes of each network packet will be read into memory, or saved to disk. A value of 0 specifies a snapshot length of 262144, so that the full packet is captured; this is the default.

This option can occur multiple times. If used before the first occurrence of the **−i** option, it sets the default snapshot length. If used after an **−i** option, it sets the snapshot length for the interface specified by the last **−i** option occurring before this option. If the snapshot length is not set specifically, the default snapshot length is used if provided.

−S

Print statistics for each interface once every second.

−t

Use a separate thread per interface.

−v|−−version

Print the version and exit.

−w <outfile>

Write raw packet data to *outfile*. Use "−" for stdout.

−y|−−linktype <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.

This option can occur multiple times. If used before the first occurrence of the **−i** option, it sets the default capture link type. If used after an **−i** option, it sets the capture link type for the interface specified by the last **−i** option occurring before this option. If the capture link type is not set specifically, the default capture link type is used if provided.

−−capture−comment <comment>

Add a capture comment to the output file, if supported by the output file format.

This option is only available if we output the captured packets to a single file.

This option may be specified multiple times. Note that Wireshark currently only displays the first comment of a capture file.

−−list−time−stamp−types

List time stamp types supported for the interface. If no time stamp type can be set, no time stamp types are listed.

−−time−stamp−type <type>

Change the interface’s timestamp method.

## CAPTURE FILTER SYNTAX

See the manual page of pcap−filter(7) or, if that doesn’t exist, tcpdump(8), or, if that doesn’t exist, https://gitlab.com/wireshark/wireshark/−/wikis/CaptureFilters.

## SEE ALSO

wireshark(1), tshark(1), editcap(1), mergecap(1), capinfos(1), pcap(3), pcap−filter(7) or tcpdump(8)

## NOTES

This is the manual page for **Dumpcap** 3.6.2. **Dumpcap** is part of the **Wireshark** distribution. The latest version of **Wireshark** can be found at https://www.wireshark.org.

HTML versions of the Wireshark project man pages are available at https://www.wireshark.org/docs/man−pages.

## AUTHORS

**Dumpcap** is derived from the **Wireshark** capturing engine code; see the list of authors in the **Wireshark** man page for a list of authors of that code.