NAME

capinfos − Prints information about capture files

SYNOPSIS

capinfos [**−a**] [**−A**] [**−b**] [**−B**] [**−c**] [**−C**] [**−d**] [**−D**] [**−e**] [**−E**] [**−F**] [**−h**] [**−H**] [**−i**] [**−I**] [**−k**] [**−K**] [**−l**] [**−L**] [**−m**] [**−M**] [**−n**] [**−N**] [**−o**] [**−q**] [**−Q**] [**−r**] [**−R**] [**−s**] [**−S**] [**−t**] [**−T**] [**−u**] [**−v**] [**−x**] [**−y**] [**−z**] <*infile*> ...

DESCRIPTION

Capinfos is a program that reads one or more capture files and returns some or all available statistics (infos) of each <*infile*> in one of two types of output formats: long or table.

The long output is suitable for a human to read. The table output is useful for generating a report that can be easily imported into a spreadsheet or database.

The user specifies what type of output (long or table) and which statistics to display by specifying flags (options) that corresponding to the report type and desired infos. If no options are specified, **Capinfos** will report all statistics available in "long" format.

Options are processed from left to right order with later options superseding or adding to earlier options.

Capinfos is able to detect and read the same capture files that are supported by **Wireshark**. The input files don’t need a specific filename extension; the file format and an optional gzip, zstd or lz4 compression will be automatically detected. Near the beginning of the DESCRIPTION section of wireshark(1) or https://www.wireshark.org/docs/man−pages/wireshark.html is a detailed description of the way **Wireshark** handles this, which is the same way **Capinfos** handles this.

OPTIONS

−a

Displays the start time of the capture. **Capinfos** considers the earliest timestamp seen to be the start time, so the first packet in the capture is not necessarily the earliest − if packets exist "out−of−order", time−wise, in the capture, **Capinfos** detects this.

−A

Generate all infos. By default **Capinfos** will display all infos values for each input file, but enabling any of the individual display infos options will disable the generate all option.

−b

Separate infos with ASCII SPACE (0x20) characters. This option is only useful when generating a table style report (−T). The various info values will be separated (delimited) from one another with a single ASCII SPACE character.

Note

Since some of the header labels as well as some of the value fields contain SPACE characters. This option is of limited value unless one of the quoting options (−q or −Q) is also specified.

−B

Separate the infos with ASCII TAB characters. This option is only useful when generating a table style report (−T). The various info values will be separated (delimited) from one another with a single ASCII TAB character. The TAB character is the default delimiter when −T style report is enabled.

−c

Displays the number of packets in the capture file.

−C

Cancel processing any additional files if and when **Capinfos** fails to open an input file or gets an error reading an input file. By default **Capinfos** will continue processing files even if it gets an error opening or reading a file.

Note: An error message will be written to stderr whenever **Capinfos** fails to open a file or gets an error reading from a file regardless whether the −C option is specified or not. Upon exit, **Capinfos** will return an error status if any errors occurred during processing.

−d

Displays the total length of all packets in the file, in bytes. This counts the size of the packets as they appeared in their original form, not as they appear in this file. For example, if a packet was originally 1514 bytes and only 256 of those bytes were saved to the capture file (if packets were captured with a snaplen or other slicing option), **Capinfos** will consider the packet to have been 1514 bytes.

−D

Displays a count of the number of decryption secrets in the file. This information is not available in table format.

−e

Displays the end time of the capture. **Capinfos** considers the latest timestamp seen to be the end time, so the last packet in the capture is not necessarily the latest − if packets exist "out−of−order", time−wise, in the capture, **Capinfos** detects this.

−E

Displays the per−file encapsulation of the capture file.

−F

Displays additional capture file information.

−h|−−help

Prints the help listing and exits.

−H

Displays the SHA256, RIPEMD160, and SHA1 hashes for the file. SHA1 output may be removed in the future.

−i

Displays the average data rate, in bits/sec

−I

Displays detailed capture file interface information. This information is not available in table format.

−k

Displays the capture comment. For pcapng files, this is the comment from the section header block.

−K

Use this option to suppress printing capture comments. By default capture comments are enabled. Capture comments are relatively freeform and might contain embedded new−line characters and/or other delimiting characters making it harder for a human or machine to easily parse the **Capinfos** output. Excluding capture comments can aid in post−processing of output.

−l

Display the snaplen (if any) for a file. snaplen (if available) is determined from the capture file header and by looking for truncated records in the capture file.

−L

Generate long report. **Capinfos** can generate two different styles of reports. The "long" report is the default style of output and is suitable for a human to use.

−m

Separate the infos with comma (,) characters. This option is only useful when generating a table style report (−T). The various info values will be separated (delimited) from one another with a single comma "," character.

−M

Print raw (machine readable) values in long reports. By default **Capinfos** prints numeric values with human−readable SI suffixes, and shows human−readable file type and encapsulation. Table reports (−T) always print raw values.

−n

Displays a count of the number of resolved IPv4 addresses and a count of the number of resolved IPv6 addresses in the file. This information is not available in table format.

−N

Do not quote the infos. This option is only useful when generating a table style report (−T). Excluding any quoting characters around the various values and using a TAB delimiter produces a very "clean" table report that is easily parsed with CLI tools. By default infos are **NOT** quoted.

−o

Displays "True" if packets exist in strict chronological order or "False" if one or more packets in the capture exists "out−of−order" time−wise.

−q

Quote infos with single quotes ('). This option is only useful when generating a table style report (−T). When this option is enabled, each value will be encapsulated within a pair of single quote (') characters. This option (when used with the −m option) is useful for generating one type of CSV style file report.

−Q

Quote infos with double quotes ("). This option is only useful when generating a table style report (−T). When this option is enabled, each value will be encapsulated within a pair of double quote (") characters. This option (when used with the −m option) is useful for generating the most common type of CSV style file report.

−r

Do not generate header record. This option is only useful when generating a table style report (−T). If this option is specified then **no** header record will be generated within the table report.

−R

Generate header record. This option is only useful when generating a table style report (−T). A header is generated by default. A header record (if generated) is the first line of data reported and includes labels for all the columns included within the table report.

−s

Displays the size of the file, in bytes. This reports the size of the capture file itself.

−S

Display the start and end times as seconds since January 1, 1970. Handy for synchronizing dumps using **editcap −t**.

−t

Displays the capture type of the capture file.

−T

Generate a table report. A table report is a text file that is suitable for importing into a spreadsheet or database. **Capinfos** can build a tab delimited text file (the default) or several variations on Comma−separated values (CSV) files.

−u

Displays the capture duration, in seconds. This is the difference in time between the earliest packet seen and latest packet seen.

−v|−−version

Displays the tool’s version and exits.

−x

Displays the average packet rate, in packets/sec

−y

Displays the average data rate, in bytes/sec

−z

Displays the average packet size, in bytes

EXAMPLES

To see a description of the options use:

```
capinfos −h
```

To generate a long form report for the capture file mycapture.pcap use:

```
capinfos mycapture.pcap
```

To generate a TAB delimited table form report for the capture file mycapture.pcap use:

```
capinfos −T mycapture.pcap
```

To generate a CSV style table form report for the capture file mycapture.pcap use:

```
capinfos −T −m −Q mycapture.pcap
```

or

```
capinfos −TmQ mycapture.pcap
```

To generate a TAB delimited table style report with just the filenames, capture type, capture encapsulation type and packet count for all the pcap files in the current directory use:

```
capinfos −T −t −E −c *.pcap
```

or

```
capinfos −TtEc *.pcap
```

Note: The ability to use of filename globbing characters are a feature of *nix style command shells.

To generate a CSV delimited table style report of all infos for all pcap files in the current directory and write it to a text file called mycaptures.csv use:

```
capinfos −TmQ *.pcap >mycaptures.csv
```

The resulting mycaptures.csv file can be easily imported into spreadsheet applications.

SEE ALSO

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

NOTES

This is the manual page for **Capinfos** 3.6.2. **Capinfos** 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

Original Author

Ian Schorr <ian[AT]ianschorr.com>

Contributors

Gerald Combs <gerald[AT]wireshark.org>

Jim Young <jyoung[AT]gsu.edu>