

**NAME**

utmpdump – dump UTMP and WTMP files in raw format

**SYNOPSIS**

**utmpdump** [options] [*filename*]

**DESCRIPTION**

**utmpdump** is a simple program to dump UTMP and WTMP files in raw format, so they can be examined. **utmpdump** reads from stdin unless a *filename* is passed.

**OPTIONS**

**-f, --follow**

Output appended data as the file grows.

**-o, --output *file***

Write command output to *file* instead of standard output.

**-r, --reverse**

Undump, write back edited login information into the utmp or wtmp files.

**-V, --version**

Display version information and exit.

**-h, --help**

Display help text and exit.

**NOTES**

**utmpdump** can be useful in cases of corrupted utmp or wtmp entries. It can dump out utmp/wtmp to an ASCII file, which can then be edited to remove bogus entries, and reintegrated using:

**utmpdump -r < ascii\_file > wtmp**

But be warned, **utmpdump** was written for debugging purposes only.

**File formats**

Only the binary version of the **utmp(5)** is standardised. Textual dumps may become incompatible in future.

The version 2.28 was the last one that printed text output using **ctime(3)** timestamp format. Newer dumps use millisecond precision ISO-8601 timestamp format in UTC-0 timezone. Conversion from former timestamp format can be made to binary, although attempt to do so can lead the timestamps to drift amount of timezone offset.

**BUGS**

You may **not** use the **-r** option, as the format for the utmp/wtmp files strongly depends on the input format. This tool was **not** written for normal use, but for debugging only.

**AUTHOR**

Michael Krapp

**SEE ALSO**

**last(1)**, **w(1)**, **who(1)**, **utmp(5)**

**AVAILABILITY**

The utmpdump command is part of the util-linux package and is available from Linux Kernel Archive (<https://www.kernel.org/pub/linux/utils/util-linux/>).