NAME

sdjournal − Provide an interface to capture systemd journal entries.

SYNOPSIS

sdjournal [**−−help**] [**−−version**] [**−−extcap−interfaces**] [**−−extcap−dlts**]
[**−−extcap−interface**=<interface>] [**−−extcap−config**] [**−−capture**] [**−−fifo**=<path to file or pipe>]
[**−−start−from**=<entry count>]

DESCRIPTION

sdjournal is an extcap tool that allows one to capture systemd journal entries. It can be used to correlate system events with network traffic.

Supported interfaces:

1. sdjournal

OPTIONS

−−help

Print program arguments.

−−version

Print program version.

−−extcap−interfaces

List available interfaces.

−−extcap−interface=<interface>

Use specified interfaces.

−−extcap−dlts

List DLTs of specified interface.

−−extcap−config

List configuration options of specified interface.

−−capture

Start capturing from specified interface and write raw packet data to the location specified by −−fifo.

−−fifo=<path to file or pipe>

Save captured packet to file or send it through pipe.

−−start−from=<entry count>

Start from the last <entry count> entries, similar to the "−n" or "−−lines" argument for the tail(1) command. Values prefixed with a **+** sign start from the beginning of the journal, otherwise the count starts from the end. The default value is 10. To include all entries use **+0**.

EXAMPLES

To see program arguments:

```
sdjournal --help
```

To see program version:

```
sdjournal --version
```

To see interfaces:

```
sdjournal --extcap-interfaces
```

Only one interface (sdjournal) is supported.

Example output

```
interface {value=sdjournal}{display=systemd journal capture}
```

To see interface DLTs:

```
sdjournal --extcap-interface=sdjournal --extcap-dlts
```

Example output

```
dlt {number=147}{name=sdjournal}{display=USER0}
```

To see interface configuration options:

```
sdjournal --extcap-interface=sdjournal --extcap-config
```

Example output

```
arg {number=0}{call=--start-from}{display=Starting position}{type=string}
    {tooltip=The journal starting position. Values with a leading "+" start from
```

To capture:

```
sdjournal --extcap-interface=sdjournal --fifo=/tmp/sdjournal.pcap --capture
```

To capture all entries since the system was booted:

```
sdjournal --extcap-interface=sdjournal --fifo=/tmp/sdjournal.pcap --capture --sta
```

Note

To stop capturing CTRL+C/kill/terminate application.

SEE ALSO

wireshark(1), tshark(1), dumpcap(1), extcap(4), tcpdump(1)

NOTES

sdjournal 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

Gerald Combs <gerald[AT]wireshark.org>