NAME

udpdump − Provide an UDP receiver that gets packets from network devices (like Aruba routers) and exports them in PCAP format.

SYNOPSIS

udpdump [**−−help**] [**−−version**] [**−−extcap−interfaces**] [**−−extcap−dlts**] [**−−extcap−interface**=<interface>] [**−−extcap−config**] [**−−capture**] [**−−fifo**=<path to file or pipe>] [**−−port**=<port>] [**−−payload**=<type>]

DESCRIPTION

udpdump is a extcap tool that provides an UDP receiver that listens for exported datagrams coming from any source (like Aruba routers) and exports them in PCAP format. This provides the user two basic functionalities: the first one is to have a listener that prevents the localhost to send back an ICMP port−unreachable packet. The second one is to strip out the lower layers (layer 2, IP, UDP) that are useless (are used just as export vector). The format of the exported datagrams are EXPORTED_PDU, as specified in https://gitlab.com/wireshark/wireshark/−/raw/master/epan/exported_pdu.h

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 save saved it in place specified by −−fifo.

−−fifo=<path to file or pipe>

Save captured packet to file or send it through pipe.

−−port=<port>

Set the listener port. Port 5555 is the default.

−−payload=<type>

Set the payload of the exported PDU. Default: data.

EXAMPLES

To see program arguments:

```
udpdump --help
```

To see program version:

```
udpdump --version
```

To see interfaces:

```
udpdump --extcap-interfaces
```

Example output

```
interface {value=udpdump}{display=UDP Listener remote capture}
```

To see interface DLTs:

```
udpdump --extcap-interface=udpdump --extcap-dlts
```

Example output

```
dlt {number=252}{name=udpdump}{display=Exported PDUs}
```

To see interface configuration options:

```
udpdump --extcap-interface=udpdump --extcap-config
```

Example output

```
arg {number=0}{call=--port}{display=Listen port}{type=unsigned}{range=1,65535}{de
```

To capture:

```
udpdump --extcap-interface=randpkt --fifo=/tmp/randpkt.pcapng --capture
```

Note

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

SEE ALSO

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

NOTES

udpdump 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

Dario Lombardo <lomato[AT]gmail.com>