NAME

log2pcap - Extract network traces from Samba log files

SYNOPSIS

log2pcap [-h] [-q] [logfile] [pcap_file]

DESCRIPTION

This tool is part of the **samba**(7) suite.

log2pcap reads in a samba log file and generates a pcap file (readable by most sniffers, such as ethereal or tcpdump) based on the packet dumps in the log file.

The log file must have a *log level* of at least **5** to get the SMB header/parameters right, **10** to get the first 512 data bytes of the packet and **50** to get the whole packet.

OPTIONS

-h

If this parameter is specified the output file will be a hex dump, in a format that is readable by the text2pcap utility.

-q

Be quiet. No warning messages about missing or incomplete data will be given.

logfile

Samba log file. log2pcap will try to read the log from stdin if the log file is not specified.

pcap_file

Name of the output file to write the pcap (or hexdump) data to. If this argument is not specified, output data will be written to stdout.

-?|--help

Print a summary of command line options.

EXAMPLES

Extract all network traffic from all samba log files:

```
$ log2pcap < /var/log/* > trace.pcap
```

Convert to pcap using text2pcap:

```
$ log2pcap -h samba.log | text2pcap -T 139,139 - trace.pcap
```

VERSION

This man page is part of version 4.13.17 of the Samba suite.

BUGS

Only SMB data is extracted from the samba logs, no LDAP, NetBIOS lookup or other data.

The generated TCP and IP headers don’t contain a valid checksum.

SEE ALSO

text2pcap(1), **ethereal**(1)

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.

This manpage was written by Jelmer Vernooij.