NAME

logksi extract - Extracts log records and corresponding hash chains from the log files protected by KSI signatures.

SYNOPSIS

logksi extract <*logfile*> [<*logfile.logsig*>] [**-o** <*outfile*>] **-r** *records*... [*more_options*]

logksi extract --log-from-stdin <*logfile.logsig*> **-o** <*outfile*> **-r** *records*... [*more_options*]

logksi extract --sig-from-stdin <*logfile*> [**-o** <*outfile*>] **-r** *records*... [*more_options*]

DESCRIPTION

Extracts the specified record(s) from the given <*logfile*> and their KSI signature(s) from the respective log signature file <*logfile*>*.logsig* or <*logfile*>*.gtsig*. If the log signature file <*logfile.logsig*> is not specified, its name is derived from <*logfile*> by adding the *.logsig* suffix.

logksi extract outputs the requested log record(s) to the file <*logfile*>*.excerpt* and creates the record integrity proof file <*logfile*>*.excerpt.logsig* for these records. If the files already exist, they will be overwritten.

The extracted log records' KSI signatures can be verified independently, thus individual log records can be presented and their integrity proven regardless the state or content of other log records saved in the same <*logfile*>. See **logksi-verify**(1) for verification details.

OPTIONS

<*logfile*>

Log file from which the specified log records will be extracted. **--log-from-stdin** Read the log file from *stdin*. If **--log-from-stdin** is used, the log signature file <*logfile.logsig*> must be specified and **--sig-from-stdin** cannot be used.

--sig-from-stdin

Read the log signature file from *stdin*. If **--sig-from-stdin** is specified, the log file <*logfile*> must be specified and **--log-from-stdin** cannot be used.

-o <*outfile*>

Names of output files will be derived from <*outfile*> by adding the appropriate suffixes. Name of the log records file will be <*outfile*>*.excerpt*. Name of the integrity proof file will be <*outfile*>*.excerpt.logsig*. If <*outfile*> is not specified, names of output files will be derived from <*logfile*> by adding the same suffixes. If **--log-from-stdin** is specified, <*outfile*> must also be specified.

--out-log <*log.records*>

Specify the name of the log records file. The log records file can be redirected to *stdout* by using '-' as the file name. If the log records file name is not specified with **--out-log**, its name will be derived from either <*outfile*> or <*logfile*> by adding the *.excerpt* suffix.

--out-proof <*integrity.proof*>

Specify the name of the integrity proof file. The integrity proof file can be redirected to *stdout* (unless the log records file is also redirected to *stdout*) by using '-' as the file name. If the integrity proof file name is not specified with **--out-proof**, its name will be derived from either <*outfile*> or <*logfile*> by adding the *.excerpt.logsig* suffix.

-r *records*

Specify the position(s) of record(s) to be extracted. Position of the first record is 1 and all positions must be defined in a strictly ascending order, using positive decimal numbers. Positions to be extracted can be defined either:

- Individually: 1,2,3,4,8,9,10
- In ranges: 1-4,8-10
- Mixed: 1-4,8,9,10

-d Print detailed information about processes and errors to *stderr*. To make output more verbose increase debug level with **-dd** or **-ddd**. With debug level 1 a summary of log file is displayed. With debug level 2 a summary of each block and the log file is displayed. Debug level 3 will display the whole parsing of the log signature file. The parsing of *record hashes (r)*, *tree hashes (.)*, *final tree hashes (:)* and *meta-records (M)* is displayed inside curly brackets in following manner *{r.Mr..:}*. In case of a failure *(X)* is displayed and closing curly bracket is omitted.

--log *file*

Write *libksi* log to the given file. Use ’-’ as file name to redirect the log to *stdout*.

EXIT STATUS

See **logksi**(1) for more information.

EXAMPLES

1 To extract the records 1 to 200 and 250 to 260 from the log file */var/log/secure*. The extracted records will be written to */var/log/secure.excerpt*, the corresponding integrity proof file will be */var/log/secure.excerpt.logsig*:

```
logksi extract /var/log/secure -r 1-200,250-260
```

2 To extract the records 4, 25 and 121 from the log file */var/log/secure*. The extracted records will be written to */var/log/proof.excerpt*, the corresponding integrity proof file will be */var/log/proof.excerpt.logsig*:

```
logksi extract /var/log/secure -o /var/log/proof -r 4,25,121
```

3 To extract the records 1-3 from the log file that is read from *stdin*. The KSI signature(s) will be read from */var/log/messages.logsig*. The extracted records will be written to */var/log/log.records*, the corresponding integrity proof will be directed to *stdout*:

```
logksi extract --log-from-stdin /var/log/messages.logsig --out-log /var/log/log.records
--out-proof - -r 1-3
```

AUTHOR

Guardtime AS, http://www.guardtime.com/

SEE ALSO

logksi(1), **logksi-extend**(1), **logksi-integrate**(1), **logksi-sign**(1), **logksi-verify**(1), **logksi-conf**(5)