

**NAME**

sigfind – Find a binary signature in a file

**SYNOPSIS**

**sigfind** [-b *bsize* ] [-o *offset* ] [-t *template* ] [-lV] [ *hex\_signature* ] *file*

**DESCRIPTION**

**sigfind** searches through a file and looks for the *hex\_signature* at a given offset. This can be used to search for lost boot sectors, superblocks, and partition tables.

**ARGUMENTS**

-b *bsize*

Specify the block size in which to search. The default is 512 and the value must be a multiple of 512.

-o *offset*

Specify the offset in a block in which the signature must exist. The default is 0.

-t *template*

Specify a template name that defines the signature value and offset. Run with no options to get a list of supported templates.

-l The signature is stored in little-endian ordering and must therefore be reversed.

-V Display version

[*hex\_signature*]

The binary signature that you are searching for. It must be given in hexadecimal format. This argument must exist if -t is not used.

*file* Any raw data.

**EXAMPLES**

sigfind -o 510 -l AA55 disk.dd

sigfind -t fat disk.dd

**AUTHOR**

Brian Carrier <carrier at sleuthkit dot org>

Send documentation updates to <doc-updates at sleuthkit dot org>