

# FOREMOST INSTALLATION & USE

Taken From the Foremost Documentation (Kendall & Kornblum)

## Introduction

Foremost is a Linux program to recover files based on their headers and footers. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers are specified by a configuration file, so you can pick and choose which headers you want to look for.

## Installation

To run foremost, you must:

- uncompress the archive
- compile
- install

Here's how to do it:

```
$ tar zxvf foremost-xx.tar.gz
$ cd foremost-xx
$ make
$ make install
```

On systems with older versions of glibc (earlier than 2.2.0), you will get some harmless warnings about ftello and fseeko not being defined. You can ignore these.

If you ever need to remove foremost from your system, you can do this: **make uninstall**

## Usage

A description of the command line arguments can be found in the man page. To view it:

```
$ man foremost
```

The configuration file is used to control what types of files foremost searches for. A sample configuration file, foremost.conf, is included with this distribution. For each file type, the configuration file describes the file's extension, whether the header and footer are case sensitive, the maximum file size, and the header and footer for the file. The footer field is optional, but header, size, case sensitivity, and extension are not!

Any line that begins with a '#' is considered a comment and ignored. Thus, to skip a file type just put a '#' at the beginning of that line

Headers and footers are decoded before use. To specify a value in hexadecimal use `\x[0-f][0-f]`, and for octal use `\[1-9][1-9][1-9]`. Spaces can be represented by `\s`. Example: `"\x4F\123\sCCI"` decodes to "OSI CCI".

To match any single character (aka a wildcard) use a '?'. If you need to search for the '?' character, you will need to change the 'wildcard' line *\*and\** every occurrence of the old

# FOREMOST INSTALLATION & USE

Taken From the Foremost Documentation (Kendall & Kornblum)

wildcard character in the configuration file. Don't forget those hex and octal values! '?' is equal to 0x3f and \063.

Here's a sample set of headers and footers:

```
# extension case-sens max-size header footer (option)
#
# GIF and JPG files (very common)
gif y 155000 \x47\x49\x46\x38\x37\x61 \x00\x3b
gif y 155000 \x47\x49\x46\x38\x39\x61 \x00\x00\x3b
jpg y 200000 \xff\xd8\xff \xff\xd9
```

Note: the option is a method of specifying additional options. Current the following options exist:

**FORWARD:** Specify to search from the header to the footer (optional) up to the max-size.

**REVERSE:** Specify to search from the footer to the header up to the max-size.

**NEXT:** Specify to search from the header to the data just past the footer. This allows you to specify data that you know is 'NOT' in the data you are looking for and should terminated the search, up to the max-size.