A Comparison among FDRecovery and TestDisk, Foremost and PhotoRec

MTU Security and Privacy (SnP) lab

FDRecovery is an open-sourced forensic tool developed by the NTU Security and Privacy (SnP) lab. The tool can be used to restore the files deleted by users accidentally. The core idea is to perform forensic analysis over the file system metadata and the journals. Compared to other free forensic data recovery tools for Linux (e.g., TestDisk, PhotoRec, Foremost), FDRecovery can provide to the user a candidate list of the potential files to be recovered, and can store the specific file selected by user. In addition, the recovery process is much more efficient.

FDRecovery vs. TestDisk

Link to tool: https://www.cgsecurity.org/wiki/TestDisk
How it works:
—
TestDisk is meant primarily to recover full lost partitions, and repairing disks which are no longer bootable. It does have a undelete feature though this only works in FAT, exFAT, NTFS and ext2 filesystem. TestDisk uses the directory entries of the file to get their location on disk.

Does not use journal for recovery.

Functional differences between TestDisk and FDRecovery:
—
testDisk works on FAT, exFAT, NTFS and ext2 filesystems, whereas FDRecovery works on ext3, ext4, and ext2 (on older linux distributions)

TestDisk is not primarily for file recovery - this makes it more complicated to use specifically for file recovery.

TestDisk displays the directory that the file was deleted from.

TestDisk can take significantly longer than FDRecovery.

FDRecovery vs. Foremost

Link to tool: https://sourceforge.net/projects/foremost/
How it works:
—
Foremost is provided a disk image as input, and the user specifies a file type that it wishes to recover as well as an output directory for recovered files. There are a few other input options, but these are the ones essential to recovery.

Given this disk image, foremost searches the entire provided disk image for files of the specified type. It detects the file type based on file headers, footers, and internal data structures.

Does not use journal for recovery

Functional differences between foremost and FDRecovery:
—
Foremost only has support for limited file types (jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, and cpp) whereas FDRecovery can recover any file type.

Foremost is orders of magnitude slower than FDRecovery as it manually looks through data blocks for specific file type indicators.

Foremost is filesystem type agnostic while FDRecovery exploits different filesystem features for recovery.

Foremost recovers all deleted files of the specified type; does not allow the user to pick and choose.

Foremost is more difficult for the user to use - it is purely a CLI application.

Foremost is unaware of when the files were deleted (or other specific file identification) - this makes it harder for the user to identify which file they wanted.

Foremost can recover files from specific directories.

Foremost does not have some of the same limitations that FDRecovery has due to its reliance on the journal.

FDRecovery vs. PhotoRec

Link to tool: https://www.cgsecurity.org/wiki/PhotoRec

How it works:
—
It first tries to find out what the block size is (much like FDRecovery, using the super block to do this). To perform actual data recovery, PhotoRec works much like Foremost, where it searches block by block in order to find recognizable file headers and footers in order to reconstruct files of specific filetypes. QPhotorec is simply a GUI for PhotoRec

Does not use journal for recovery

Functional Differences between PhotoRec and FDRecovery:
—

PhotoRec simply recovers all deleted files, rather than allowing the user to choose which ones to recover. This makes it a lot harder to find the file you wanted when there are so many being recovered.

PhotoRec takes significantly longer than FDRecovery (hours rather than seconds).

PhotoRec is unaware of when the files were deleted (or other specific file identification) - this makes it harder for the user to identify which file they wanted.

Can recover hundreds of different file formats. This is better than Foremost, but not fully comprehensive as FDRecovery recovers all files regardless of format.

PhotoRec does not autodetect filesystem type, while FDRecovery does.

PhotoRec does not have some of the same limitations that FDRecovery has due to its reliance on the journal.

PhotoRec supports FAT, NTFS, exFAT, ext2/ext3/ext4, HFS while FDRecovery only supports ext2(in older linux distros)/ext3/ext4 (so far).