SIGPwny

SP2025 Week 05 • 2025-03-06

Forensics I: File Recovery Tools (SIFT)

Michael Khalaf

Agenda

1. Introduction to File Recovery Tools
2. Plaso Framework (Digital Forensics II (next Thursday)
3. dc3dd
4. photorec
5. foremost
6. scalpel

File Recovery

- *Definition:* A broader process that involves restoring lost, damaged, or deleted files from a storage medium using various techniques.

- *When to Use:* Applies both to situations where file carving is needed (when metadata is missing) and when file system structures are intact enough to use standard recovery methods.

- *Scope:* May involve repairing corrupted files, restoring partitions, or recovering files with intact metadata.

File Carving

Definition: Extracting files solely based on known file signatures or patterns rather than relying on file system metadata.

When to Use: Particularly useful when the file system is damaged, deleted files have lost their directory entries, or when file headers/footers are intact in raw disk sectors.

Imaging

Definition: The process of creating a bit-for-bit copy (forensic image) of a storage device.

When to Use: Essential for preserving the original state of data, allowing forensic analysts to work on a duplicate without risking alteration of evidence.

Purpose: Serves as a safeguard against data tampering and provides a reliable backup for further analysis, including file carving and data recovery.

Imaging: dc3dd

→ https://www.kali.org/tools/dc3dd/ ←

dc3dd is developed by the US Department of Defense Computer Forensic Laboratory. Made for improved logging, hashing, and error handling to ensure reliable disk imaging for investigations.

scalpel

What is Scalpel?

Scalpel is an open-source file carving tool designed to recover files from disk images or raw data. It focuses on extracting files based on their unique header and footer signatures rather than relying on file system metadata.

Origin & Development:
Scalpel was originally derived from the well-known tool Foremost. The developers aimed to improve performance and configurability, resulting in a tool that is both faster and more efficient in carving files.

Features

Configurable Carving: Uses a configuration file to define custom carving parameters, allowing you to specify which file types to target and the patterns to look for.

Header and Footer Recognition: Searches for specific byte patterns that mark the beginning and end of a file, making it useful for recovering files when directory information is missing or damaged.

Efficient Processing: Written in C, Scalpel is optimized for high performance, which is particularly important when working with large data sets.

foremost

What is Foremost?

Foremost is an open-source file carving tool designed to recover files from disk images and raw data. It was originally developed by the United States Air Force Office of Special Investigations and The Center for Information Systems Security Studies and Research.

Key Features:

- **File Carving Based on Headers, Footers, and Data Structures**: Foremost identifies files by scanning for known header and footer patterns, allowing it to recover data even when file system structures are damaged or missing.
- **Versatile File Type Recovery**: It supports a wide range of file formats (images, documents, archives, etc.) by leveraging pre-defined or custom carving rules.
- **Ease of Use**: The tool can be run from the command line with options to specify the input image and desired output, making it accessible for both beginners and experienced forensic examiners.

photorec

What is PhotoRec?

PhotoRec is an open-source file recovery tool designed to recover lost files, even when the file system structure has been severely damaged or reformatted. Despite its name, it recovers a wide array of file types beyond just photos.

Key Features:

- **File Carving Based on Signatures**: Uses file signature analysis to locate and recover files from raw disk sectors, bypassing the need for intact file system metadata.
- **Wide Range of File Support**: Capable of recovering various file formats including documents, archives, videos, and images.
- **Cross-Platform Compatibility**: Runs on multiple operating systems, making it a versatile choice for forensic investigations.

Let’s try it.

1. Download the following:

   dc3dd from https://www.kali.org/tools/dc3dd/

→
```
sudo apt-get install dc3dd
```

2. Retrieve the forensic disk drive I provide (SIGPwny Purple Team Box channel)

→ https://uofi.app.box.com/folder/310508629572?s=v4ia1oznl1xmtw36hblt9u707rq2a0o8