Do Metadata-Based Deleted File Recovery Tools Meet the NIST Guidelines?

Andrew Meyer, Quinton Currier
Department of Computer Science, BGSU

Objective

Perform a comparative analysis of metadata-based deleted file recovery (DFR) tools according to guidelines set by the National Institute for Standards and Technology (NIST)'s Computer Forensics Tool Testing (CFTT) Program.

Background

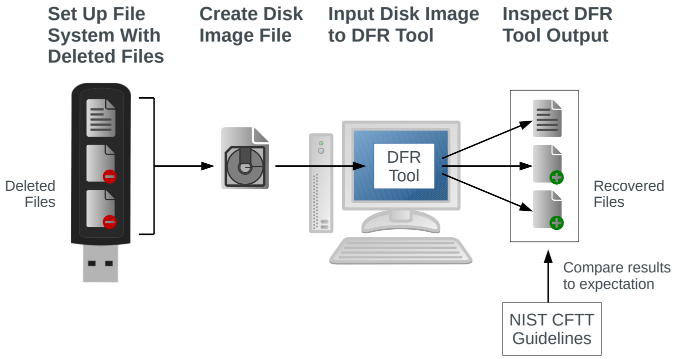
Deleted file recovery is possible due to how most computers handle file deletion. Fully erasing a file would use valuable time the computer could spend working on something else. Instead, only the file's metadata is modified, communicating to the operating system that the file should be ignored and can be overwritten if space is needed. Metadata-based DFR tools are a class of DFR tools that scan for those "marked-as-deleted" metadata entries, which may still point to file data.

NIST Core Features

1) The tool must identify to the user each file system metadata entry that is marked as deleted.
2) The tool must produce an output (the "recovered file") for each deleted metadata entry it identifies.
3) The recovered file must contain the data from all parts of the disk listed in the metadata entry, except those which have been reused.
4) All data making up the recovered file must have originated from the deleted file.

Methodology

- We designed a set of test cases to represent common file deletion scenarios.
- By writing and deleting files in a deliberate sequence, we created each test case in a real file system and recorded it as a read-only "disk image."
- Each disk image was used as input to the DFR tools to evaluate them for a corresponding test case.



Set Up File System With Deleted Files

Create Disk Image File

Input Disk Image to DFR Tool

Inspect DFR Tool Output

Deleted Files

DFR Tool

Recovered Files

Compare results to expectation

NIST CFTT Guidelines

Our test cases are all composed of variations and combinations of two situations:

- *Fragmentation* – when the space a file's data occupies is not contiguous
- *Overwriting* – when the space occupied by a deleted file's data is reused for another file

We made a total of 16 test images for the FAT file system and 11 test images for the NTFS file system.

DFR tools tested:

- Autopsy
- Recuva
- FTK Imager
- TestDisk
- Magnet Axiom

Results

- A DFR tool is considered passing if it meets all four core features for a given test case.
- The DFR tools we tested did not pass for the majority of test cases.
- Most failures were because of the fourth core feature, so tools which were more conservative in what they attempted to recover tended to pass in more cases.

Conclusions

- The DFR tools we tested generally do not meet the guidelines set by NIST.
- The NIST guidelines aim to be as general as possible, which causes ambiguity in cases involving certain file systems. So, some results depend on our interpretation.

For more information please see our article in *EAI Endorsed Transactions on Security and Safety*, Volume 6 Issue 21.

http://dx.doi.org/10.4108/eai.13-7-2018.163091

Acknowledgements

This work was supported by a grant from BGSU's Center for Undergraduate Research and Scholarship, and by the guidance and expertise of Dr. Sankardas Roy. Any opinions or findings are those of the authors and do not necessarily reflect the views of the funding agency.