Creating Deleted File Recovery Tool Testing Images

Jim Lyle

National Institute of Standards and Technology

Outline

- Introduction
- What should a DFR tool do
- Creating test images
  - Relationships between data blocks and metadata
  - Tools to create test images
  - Using the tools to create test images
- Some results
- Conclusions

Introduction

- Computer Forensic Tool Testing (NIST/CFTT)
  - Disk imaging
  - Write blocking
  - Drive erasing for reuse
  - Mobile device forensics
- Deleted file recovery (DFR)
  - Metadata based (from directory, i-node, MFT, etc.) – now
  - Signature based (aka file carving) – not now

Background

- File systems keep track of files with metadata – i-nodes, Master File Table, File Allocation Tables, etc.
- Some file systems do the minimum amount of work to delete a file
  - Mark metadata as deleted, and
  - Mark data blocks as available for reuse
- File systems are designed for performance in data access; try to keep file data blocks contiguous or at least near to each other
- Metadata based deleted file recovery uses the residual metadata after a file is deleted to reconstruct deleted files

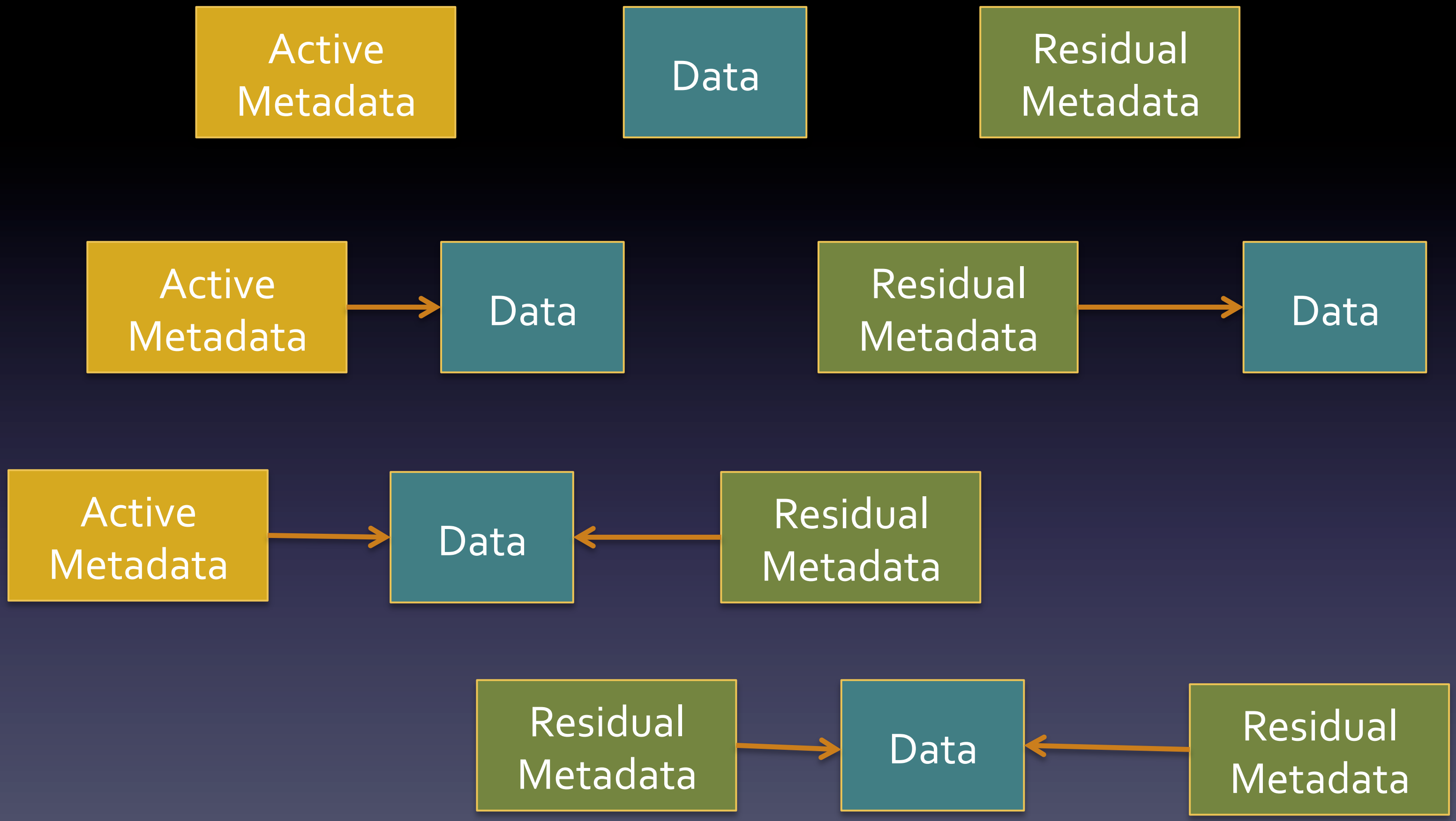
What to Recover

- File contents
- File name (**8.3 & long name)**
- MAC times (semantics differ) Birth time
- File attributes (Varies with file system)

What Might Help a Tool Do Something Interesting

- File system type: FAT, NTFS, EXT, …
- Allocation unit size
- File size
- File layout: fragmentation, block order, …
- Overwritten files

Metadata relationships with data



Active Metadata

Data

Residual Metadata

Active Metadata → Data

Residual Metadata → Data

Active Metadata → Data ← Residual Metadata

Residual Metadata → Data ← Residual Metadata

17 Basic Test Cases

DFR-01. Recover one non-fragmented file.
DFR-02. Recover file with two fragments.
DFR-03. Recover file with multiple frags.
DFR-04. Recover files with non-ASCII names.
DFR-05. Recover several fragmented files.
DFR-06. Recover one large file.
DFR-07. Recover one overwritten file.
DFR-08. Recover several overwritten files.
DFR-09. Recover 1000 files no overwrite.

DFR-10. Recover 1000 files, overwritten.
DFR-11. Recover one directory.
DFR-12. Recover multiple directories.
DFR-13. Recover random activity.
DFR-14. Recover other file system objects.
DFR-15. List one of each object.
DFR-16. List a large number of files.
DFR-17. List deep file paths.

At least 4 images per case:

1. FAT: FAT12, FAT16 & FAT32
2. ExFAT
3. NTFS
4. EXT: ext2, ext3 & ext4

Some one-off images:

- NTFS compressed
- NTFS file in MFT
- HFS+ file listing
- Recycle bin/trash can

What Does a Test Image Need

- Initialize each and every sector uniquely
- Each sector of created file should uniquely identify the file and block within the file
- Tool to summarize data in each recovered file
- Tool to document file system layout
- Document each step of creating image

Creating Test Images (tools)

- not-used – tag each sector of a device with the string “not used,”
- mk-file – create a file of tagged blocks (file name & block #),
- ap-file – append more tagged blocks to an existing file,
- fill-fs – allocate all free blocks to a single file,
- layout – categorize all blocks in the image of a file system as: file, unused, fill or metadata, and
- fana – file analysis (characterize and summarize file content to simplify comparison of a recovered file to the original file).

Wipe Test Drive

- Start by filling every sector like this:

```
00001000  45 6d 70 74 79 20 53 65  63 74 6f 72 20 30 30 30  |Empty Sector 000|
00001010  30 30 30 30 30 30 30 30  38 20 6e 6f 74 20 75 73  |000000008 not us|
00001020  65 64 0a 00 5a 5a 5a 5a  5a 5a 5a 5a 5a 5a 5a 5a  |ed..ZZZZZZZZZZZZ|
00001030  5a 5a 5a 5a 5a 5a 5a 5a  5a 5a 5a 5a 5a 5a 5a 5a  |ZZZZZZZZZZZZZZZZ|
*
00001200  45 6d 70 74 79 20 53 65  63 74 6f 72 20 30 30 30  |Empty Sector 000|
00001210  30 30 30 30 30 30 30 30  39 20 6e 6f 74 20 75 73  |000000009 not us|
00001220  65 64 0a 00 5a 5a 5a 5a  5a 5a 5a 5a 5a 5a 5a 5a  |ed..ZZZZZZZZZZZZ|
00001230  5a 5a 5a 5a 5a 5a 5a 5a  5a 5a 5a 5a 5a 5a 5a 5a  |ZZZZZZZZZZZZZZZZ|
```

- Format a file system – then everything not empty is metadata

Metadata

```
dd bs=512 count=8 skip=98430 if=dfr-05-braid-fat.dd | hexdump -C | more
00000400  46 41 54 33 32 20 20 20  20 20 20 08 00 00 00 00  |FAT32      .....|
00000410  00 00 00 00 00 00 9c 9c  4b 3f 00 00 00 00 00 00  |........K?......|
00000420  41 41 00 6c 00 67 00 6f  00 6c 00 0f 00 27 2e 00  |AA.l.g.o.l...'..|
00000430  74 00 78 00 74 00 00 00  ff ff 00 00 ff ff ff ff  |t.x.t...........|
00000440  41 4c 47 4f 4c 20 20 20  54 58 54 20 00 00 99 9d  |ALGOL   TXT ....|
00000450  4b 3f 21 26 00 00 20 10  21 26 04 00 00 04 00 00  |K?!&.. .!&......|
00000460  e5 42 00 65 00 6c 00 6c  00 61 00 0f 00 10 74 00  |.B.e.l.l.a....t.|
00000470  72 00 69 00 78 00 2e 00  74 00 00 00 78 00 74 00  |r.i.x...t...x.t.|
00000480  e5 45 4c 4c 41 54 7e 31  54 58 54 20 00 00 99 9d  |.ELLAT~1TXT ....|
00000490  4b 3f 22 26 00 00 a0 69  e4 38 05 00 00 08 00 00  |K?"&...i.8......|
000004a0  e5 43 00 61 00 6e 00 6f  00 70 00 0f 00 ce 75 00  |.C.a.n.o.p....u.|
000004b0  73 00 2e 00 74 00 78 00  74 00 00 00 00 00 ff ff  |s...t.x.t.......|
000004c0  e5 41 4e 4f 50 55 53 20  54 58 54 20 00 00 99 9d  |.ANOPUS TXT ....|
000004d0  4b 3f 22 24 00 00 a0 71  5d 28 06 00 00 08 00 00  |K?"$...q](......|
000004e0  41 44 00 65 00 6e 00 65  00 62 00 0f 00 4c 6f 00  |AD.e.n.e.b...Lo.|
000004f0  6c 00 61 00 2e 00 54 00  58 00 00 00 54 00 00 00  |l.a...T.X...T...|
00000500  44 45 4e 45 42 4f 4c 41  54 58 54 20 00 00 99 9d  |DENEBOLATXT ....|
00000510  4b 3f 21 26 00 00 20 10  21 26 09 00 00 04 00 00  |K?!&.. .!&......|
00000520  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

Create a File

```
*
00000200  0a 44 46 52 0a 46 69 6c  65 20 41 6c 67 6f 6c 2e  |.DFR.File Algol.|
00000210  74 78 74 20 70 61 74 68  20 72 6f 6f 74 0a 00 2b  |txt path root..+|
00000220  2b 2b 2b 2b 2b 2b 2b 2b  2b 2b 2b 2b 2b 2b 2b 2b  |++++++++++++++++|
*
000003f0  2b 2b 2b 2b 0a 41 6c 67  6f 6c 2e 74 78 74 0a 00  |++++.Algol.txt..|

00000400  0a 44 46 52 0a 42 6c 6f  63 6b 20 30 30 30 30 31  |.DFR.Block 00001|
00000410  20 53 65 67 6d 65 6e 74  20 30 30 31 20 66 69 6c  | Segment 001 fil|
00000420  65 20 41 6c 67 6f 6c 2e  74 78 74 20 70 61 74 68  |e Algol.txt path|
00000430  20 72 6f 6f 74 0a 00 2b  2b 2b 2b 2b 2b 2b 2b 2b  | root..+++++++++|
00000440  2b 2b 2b 2b 2b 2b 2b 2b  2b 2b 2b 2b 2b 2b 2b 2b  |++++++++++++++++|
*
000005f0  2b 2b 2b 2b 0a 41 6c 67  6f 6c 2e 74 78 74 0a 00  |++++.Algol.txt..|
```

Append to a File

```
00000600  0a 44 46 52 0a 46 69 6c  65 20 42 65 6c 6c 61 74  |.DFR.File Bellat|
00000610  72 69 78 2e 74 78 74 20  70 61 74 68 20 72 6f 6f  |rix.txt path roo|
00000800  0a 44 46 52 0a 42 6c 6f  63 6b 20 30 30 30 30 31  |.DFR.Block 00001|
00000810  20 53 65 67 6d 65 6e 74  20 30 30 31 20 66 69 6c  | Segment 001 fil|
o o o
00000e00  0a 44 46 52 0a 42 6c 6f  63 6b 20 30 30 30 30 32  |.DFR.Block 00002|
00000e10  20 53 65 67 6d 65 6e 74  20 30 30 32 20 66 69 6c  | Segment 002 fil|
00000e20  65 20 42 65 6c 6c 61 74  72 69 78 2e 74 78 74 20  |e Bellatrix.txt |
00000e30  70 61 74 68 20 72 6f 6f  74 0a 00 2b 2b 2b 2b 2b  |path root..+++++|
00000e40  2b 2b 2b 2b 2b 2b 2b 2b  2b 2b 2b 2b 2b 2b 2b 2b  |++++++++++++++++|
```

Process to Create Test images

1. Mark each sector of a device as “not used”, then format file system.
2. Image the drive to capture the base state of the formatted file system.
3. Use the mk-file program to create some files.
4. Do additional actions (create and append) to achieve the relationship between data blocks and metadata required for the specific test image.
5. Use the fana program to characterize every file to be deleted.
6. Set MAC times, Record MAC times, Delete files.
7. Un-mount and image the final state of the device. This final image is the test image.

Creating Fragmentation

- To create a two fragment file (for a FAT File System)
  1. Create files A, B1 & C
  2. Un-mount, image & remount
  3. Append B2 to B1
- This gives four data blocks ordered: A B1 C B2
- If file B is deleted, then B1 is referenced in residual metadata, and B2 is not referenced in metadata. (The link to B1 is in the directory entry, now flagged as deleted, the link to B2 in the FAT Table is set to free.
- Possible recovery results for file B:
  1. B1 B2 – guess, right by chance
  2. B1 – tool doesn't guess
  3. B1 C – guess, wrong

Steps in Creation of DFR-05-Braid

1. Create: Algol.txt Bellatrix.txt Canopus.txt
2. Append: Bellatrix.txt
3. Append: Canopus.txt
4. Create: Denebola.TXT
5. Set date/time: Algol.txt Bellatrix.txt Canopus.txt Denebola.TXT
6. Delete: Bellatrix.txt Canopus.txt
   Delete time: Tue Oct 11 19:46:34 EDT 2011

Drive Layout
DFR-05-braid

```
File  98436 -  98436 (1) root Algol.txt
Block 98437 -  98437 (1) root Algol.txt
File  98438 -  98438 (1) root Bellatrix.txt
Block 98439 -  98439 (1) root Bellatrix.txt
File  98440 -  98440 (1) root Canopus.txt
Block 98441 -  98441 (1) root Canopus.txt
Block 98442 -  98443 (2) root Bellatrix.txt
Block 98444 -  98445 (2) root Canopus.txt
File  98446 -  98446 (1) root Denebola.TXT
Block 98447 -  98447 (1) root Denebola.TXT
```

Creating Test images (Full Process)

1. Mark each sector of a device as “not used”.
2. Format the device with one or more partitions of the same family.
3. Synchronize the drive state by un-mounting all partitions.
4. Image the drive to capture the base state of the formatted file system.
5. Mount the file systems.
6. Use the mk-file program to create some files.
7. Un-mount the file systems, image and remount.
8. Do additional actions (create and append) to achieve the relationship between data blocks and metadata required for the specific test image.
9. Use the fana program to characterize every file to be deleted.
10. Set MAC times for every file to be deleted.
11. Un-mount, image and remount.
12. Record MAC times for every file to be deleted.
13. Delete the files.
14. Un-mount and image the final state of the device. This final image is the test image.

Another Fragmented Layout FAT-05-nest

1. Create: Alcor.TXT Betelgeuse.txt Capella.txt Deneb.txt ElNath.TXT
2. Append: Deneb.txt
3. Create: Fomalhaut.TXT
4. Append: Betelgeuse.txt
5. Create: Gemma.TXT
6. Delete: Betelgeuse.txt Deneb.txt

Actual Results FAT-05-nest

- Layout: A B1 C D1 E D2 F B2 G
- Delete B & D
- Files A, C, E, F & G are still active

Tool	Recover B	Comment on File B Recovery	Recover D	Comment on file D Recovery
1	B1 D1	Two files mixed	D1 D2	OK
2	B1	Only first block	D1	Only first block
3	B1 C	Block C from active file	D1 E	Block E from active file
4	B1 C	Block C from active file	D1 E	Block E from active file

Forced Overwrite

- Overwritten files can be created as follows:

  1. Create a desired block layout.
  2. Allocate all remaining free file blocks to one large file.
  3. Delete one or more files.
  4. Create one or more files. Because the only free blocks are from the files just deleted in step 3, files created now overwrite those deleted files.

- By varying the file sizes and the number of files deleted in step 3 different relationships can be created between residual metadata and data blocks
- Some of the overwritten blocks are now referenced by metadata of both a deleted and an active file.
- By deleting the active file we now have a block referenced by two deleted files.

Other Results Seen

- Rendering issues with non-English file names
- Simple fragmentation matters for FAT file systems, but not for others (e.g., ext, NTFS)
- Deleting files from NTFS via Linux – file names lost
- Tool can't parse some partition types – e.g., case sensitive HFS+, ext4

Summary

- NIST/CFTT DFR tools & test images available on http://www.CFReDS.nist.gov
- Easy to produce a variety for metadata to data relationships
- Easy to identify source of data blocks within a recovered file
- OS and file system combination matters
- Relevance of a particular relationship between data & metadata depends on the file system

Project Sponsors (aka Steering Committee)

- National Institute of Justice (Major funding)
- Homeland Security (Major funding)
- FBI (Additional funding)
- Department of Defense, DCCI (Equipment and support)
- State & Local agencies (Technical input)
- Other federal agencies (Technical input)
- NIST/OLES (Program management)

Disclaimer

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

Contact Information

Jim Lyle
jlyle@nist.gov
http://www.cftt.nist.gov
http://www/cfreds.nist.gov

Sue Ballou, Office of Law Enforcement Standards
Steering Committee representative for State/Local Law Enforcement
Susan.ballou@nist.gov