Deleted File Recovery Tool Testing Results

Jim Lyle

NIST

CFTT

- Develop specifications for testing forensic tools
  - Disk Imaging
  - Write Blocking
  - Drive erase for reuse
  - Metadata based deleted file recovery
  - Other specs in development
- Submit test reports to NIJ for publication ~90

Deleted File Recovery

- Deleted file recovery (DFR)
  - Metadata based (from directory, i-node, MFT, etc.) – now
  - Signature based (aka file carving) – next
- Tested six popular tools
- Test reports are being drafted for publication later this year

Talk Goals

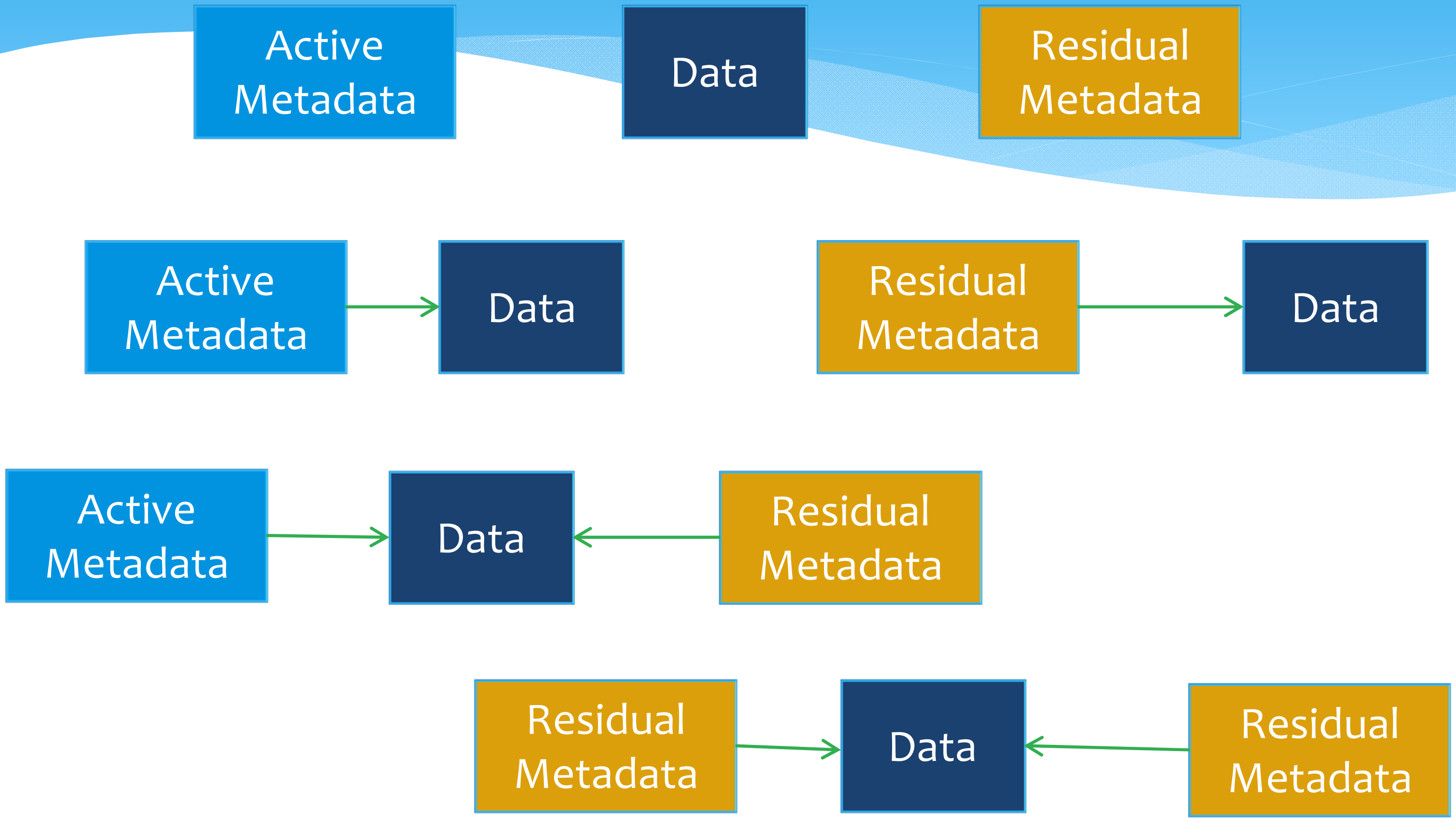
The presentation will impact the forensic community by:

- increase awareness in the community of ability of tool testing to reveal anomalies in tool behavior
- help the forensic practitioner recognize tool limitations

Remainder of Talk

- Metadata relationships
- Test suite
- Identifying Supported file systems
- Consider if there is fragmentation, but intact
- Overwriting
- Chaos
- Summary

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 BaseTest 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 object.

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

Supported File Systems

Determine supported file systems by trying a simple case –

Delete a single file, see if the six tools recovers anything

FS	1	2	3	4	5	6
ext2	✔	✔	✔	✔	✔	✔
ext3						
ext4						
FAT	✔	✔	✔	✔	✔	✔
NTFS	✔	✔	✔	✔	✔	✔
ExFAT	✔	✔	✔			✔
HFS+						

FAT Fragmentation

Case FAT-03 -- Recover a file in 4 fragments

Layout: A, C, D & E are active files; B is deleted

A	B1	C	B2	D	B3	E	B4

Results:

- Three tools recovered entire file
- One tool stopped after first cluster
- One tool included part of an active file
- One tool recovered two fragments and two clusters from active files

Tool	Recovered File			
1	B1	B2	B3	B4
2	B1			
3	B1	C(1)		
4	B1	B2	B3	B4
5	B1	B2	B3	B4
6	B1	C	B2	D

Fragmentation – Other File Systems

- NTFS – Well behaved
- Ext2 – recovered where supported
- One tool had trouble with ext2

FS	1	2	3	4	5	6
FAT	✔	1	1A	✔	✔	2AM
ExFAT	✔	✗	✗	□	□	✔
NTFS	✔	✔	✔	✔	✔	✔
ext2	2	✔	✔	✔	✔	✔

□ -- not supported
✗ -- not recovered
✔ -- recovered
Other – partial recovery

Summary for non-overwriting Cases

# recovered / # deleted						
FS	1	2	3	4	5	6
FAT	807/819	792/819	792/819	807/819	807/819	792/819
ExFAT	270/273	254/273	265/273	□	□	270/273
NTFS	273/273	273/273	273/273	273/273	273/273	273/273
ext	264/273	273/273	273/273	255/273	273/273	271/273

- Best results on NTFS, all files recovered by all tools
- Some tools miss a few files from ext2
- All tools miss a few files from ExFAT

Anomalies for non-overwriting Cases by data source

# multi-src / # other src / # Active file						
FS	1	2	3	4	5	6
FAT	9/0/0	6/0/0	27/3/18	9/0/0	12/0/3	24/0/18
ExFAT	0/0/1	10/0/10	8/0/8	□	□	0/0/0
NTFS	0/0/1	0/0/0	23/0/23	0/0/0	0/1/0	0/0/0
ext2	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0

- Except for one file recovered by tool #5, and 3 recovered by tool #3, all recovered content came for current or previous files
- Tool #3 recovered 296 of 273 deleted NTFS files

Overwrite Cases: Data & Metadata

Available Metadata and File Block Summary

		Metadata Exists			Metadata Overwritten		
Case	**Deleted**	**Intact**	**Partial**	**None**	**Intact**	**Partial**	**None**
FAT	2894	1118	2	100	7	10	1657
ExFAT	965	376	3	28	1	3	554
NTFS	965	371	3	560	0	3	28
EXT	2869	1225	21	969	17	8	629

Summary for Overwriting Cases

# intact files with metadata / # deleted						
FS	1	2	3	4	5	6
FAT (1118/2894)	885	885	885	885	885	885
ExFAT (376/965)	369	275	305	□	□	370
NTFS (371/965)	374	374	353	374	374	374
Ext (408/956)	292	372	372	14	372	372

- Best results on FAT & NTFS
- One tool showed poor results for ext2
- Results for ExFAT vary

Anomalies for overwriting Cases by data source

# multi-src / # other src / # Active file						
FS	1	2	3	4	5	6
FAT	304/4/41	183/3/41	309/66/170	269/3/0	269/3/40	297/81/197
ExFAT	18/14/16	95/7/94	89/10/88	---	---	18/18/16
NTFS	24/2/24	21/24/0	29/0/29	21/14/6	24/2/24	24/0/24
ext2	107/52/9	25/26/0	431/17/426	16/8/17	29/56/162	29/17/24

- Lots of recovered files include data from more than one source
- NTFS seems best behaved

Summary

- The residual metadata varies with the file system. For example, file names may be completely or partially lost, pointers to file blocks may be overwritten.
- Only the first block of a deleted file is identified for FAT file systems. Some tools guess the location of the remainder of the deleted file; this strategy often leads to recovered files that are mixed from several original files.
- The tools sometimes include blocks from active files in a recovered file.
- The tools rarely include blocks that have never been allocated to the current file system, i.e., it is not likely that a block from a recovered file was not a part of some file.
- Some tools attempt to identify overwritten files. The tools often identify (incorrectly) intact files as overwritten.
- Support for ExFAT, ext3 and ext4 is sometimes lacking.

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