A Forensic Comparison of NTFS and FAT32 File Systems

*Kelsey L. Rusbarsky, BS *, Marshall University Forensic Science Center; Special Agent Cynthia Smith, MLA, BA AOJ, Kansas Bureau of Investigation, Heart of America Regional Computer Forensics Laboratory; Joshua Brunty, MS, CHFI, SCERS, FTK/ACE-AME, Marshall University Forensic Science Center; Dr. Terry Fenger, PhD, Marshall University Forensic Science Center* *Primary Investigator

Marshall University Forensic Science Program, 1401 Forensic Science Dr., Huntington, WV 25701; HARCFL, 4150 N. Mulberry Drive, Suite 250, Kansas City, MO 64116-1696

ABSTRACT

The file system on any storage device is essential to the overall organization, storage mechanisms, and data control of the device. Knowing how these file systems work and the layout of key structures, storage mechanisms, associated metadata, and file system characteristics is essential to being able to forensically investigate a computer or other device. The New Technology File System (NTFS) and File Allocation Table (FAT32) are two key file systems that will be compared and contrasted, since both are still actively used and encountered often. Both systems offer forensic evidence that is significant and mandatory in an investigation.

INTRODUCTION

- File systems are essential for any storage device:
  - Overall organization
  - Storage mechanisms
  - Data control of device
- Hierarchal Structures through files and directories
- Computers, flash memory, optical disks, floppy disks, and hard disk drives are examples of devices that use file systems
- Without file systems there would be no order to an operating system.
  - Organization
  - Evidence potential
- Understanding this foundation is essential to being able to find evidence in a computer
  - Metadata is essential – human or computer
  - Mistake, misunderstanding, or purposeful
  - Investigate fraud, abuse, system failures
  - Establish causation, timing, extent of knowledge
  - Reveal creation, authorship, history, and intent of documents and files
- The focus of this research was to differentiate and compare New Technology File System (NTFS) and File Allocation Table, 32-bit version (FAT32).
- The seven key areas that are being focused on are:
  - Key Structures
  - Storage Mechanisms
  - File Names
  - Directories
  - File Date and Time
  - File Deletion
  - Encryption

MATERIALS AND METHODS

- AccessData Forensic Toolkit (FTK) Imager, Version 3.1.0.1514, © 2011 AccessData Group, LLC
- Toshiba Satellite Intel Celeron M Laptop
- 2 PNY 4GB Thumb Drives
  - One formatted for NTFS, the other for FAT32 Imaged on FTK Imager
- Literature Search
  - Internet, Technical reference books and journals, and related Sources

RESULTS

KEY STRUCTURES

- NTFS organizational structure
  - MFT metadata files
    - Attribute locations
    - Less "Slack Space"
- FAT32 organizational structure
  - File Allocation Table (FAT)
  - Yields same data, with more possible complications

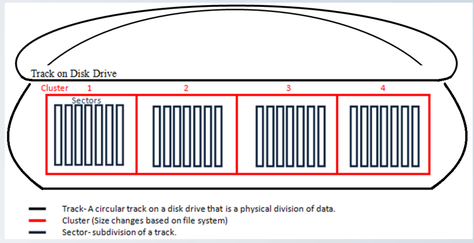

Figure 3: Example of a Disk Drive

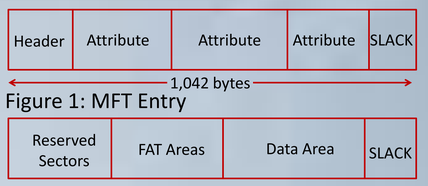

Figure 1: MFT Entry

Figure 2: FAT Structure

STORAGE MECHANISMS

- NTFS has reduced slack space
  - Size control of clusters
- FAT cannot locate files as easily as NTFS
  - Cluster addresses do not start at beginning of sector
    - Sector Addresses needed
  - Data size does not always match cluster size
    - Larger "Slack Space"
    - Forensic Potential here
  - Fracturing of large files in FAT
  - Mirrored copy of FAT

FILE NAMES AND DIRECTORIES

- NTFS attributes house:
  - Locations and sizes of data records
  - Recover deleted files
  - Data streams
    - $Logfile- records transactions and entries
- FAT
  - Tracks files by 8.3 filenames
  - This is usually not a disadvantage to long file names
  - Piece together large files

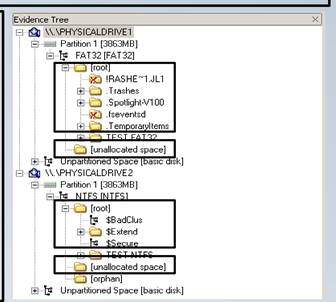

Figure 4: Root Directory File types

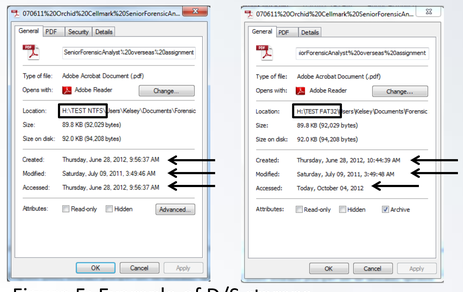

Figure 5: Example of D/S stamps

FILE DATES AND TIMES

- Date and time stamps
  - Both file systems have these
- NTFS
  - Attributes help with organization
  - Extra metadata: permissions, encryptions, $Mft entry location, and an extra time stamp
- FAT
  - Stamps are not always TRUE, but this is also exhibited in NTFS

ENCRYPTION

- NTFS
  - Protected files, locked
  - Preservation of evidence, prevents tampering
- FAT
  - Easily access data
  - Not tamper proof
- Encryption is not typically an issue

FILE DELETION

- Recovery after deletion, before reuse
- NTFS permissions
  - May block some deletions
- Examine carefully since these files are no longer addressed
  - Unallocated space can house data with forensic potential
  - Slack space can as well

DISCUSSION & CONCLUSION

Overall, each file system has it strengths and weaknesses.

- NTFS was designed as a robust file system
  - Highly organized
  - Priority of security and access control
  - Compatibility with other systems
- FAT32 was designed with compatibility and simplicity
  - Little to no security
  - Disk errors and recoverability is decent
  - Organization is good, but not as high as NTFS
  - Hidden files are not always recovered in full

When considering the FAT32 file system, it has many good qualities in areas other than the strong areas of NTFS. These qualities are such things as versatility and compatibility. FAT32 has very little security, and if one has access to the drive, can access any files or folders there. FAT32 is much more susceptible to disk errors and do not recover as readily as NTFS. FAT32 does not support file compression, which helps greatly with organization. Since NTFS allows smaller cluster sizes than FAT32, it wastes less disk space, and has less potential for hidden files. However, again FAT32 has its uses. It is compatible with any Windows Operating System, Apple's HFS file system, and many Linux file systems (ext 2/3/4)[22] and can be converted to NTFS without reformatting. If NTFS were to be converted to FAT32 for some reason, the NTFS would have to be reformatted.[17]

NTFS was designed to be a robust file system. With its added features, such as, data streams, hierarchical storage, file compression and encryption, plus a very high performance level, NTFS has proved to be a very capable system.[7] However, if an older Windows system, earlier than Windows NT (2003), is used, NTFS may not be compatible with it. Also, older software programs may not be able to function with NTFS. Permissions are allowed in NTFS to control file and folder access, but this puts the chance for errors in the system way up.

REFERENCES

- AccessData. Forensic Toolkit: Sales and Promotional Summary. AccessData Corp. http://accessdata.com/media/en_us/print/techdocs/Forensic%20Toolkit.pdf [accessed July 12th, 2012]
- Brunty, Josh. NTFS Filesystem PowerPoint. Fall 2012.
- Carrier, Brian. File System Forensic Analysis. Chapters 8-13. Pearson Education. 2005.NTFS. Copyright 1998-2012. http://www.ntfs.com [accessed June 9th, 2012]
- Corbet, Jonathan. Barriers and Journaling Filesystems. Copyright 2008. http://lwn.net/Articles/283161/ [accessed June 9th, 2012]
- DIY DataRecovery. Undelete: deleted file recovery. Created 2006. http://www.diydatarecovery.nl/kb_undelete_article.htm [accessed July 16th, 2012] Fenger, Terry, Ph.D. NTFS (New Technology File System) Foundations and Fundamentals. Fall 2011.
- Foley, Jim. The Elder Geek. FAT32 or NTFS: Making the Choice. Copyright 2002-2011. http://www.theeldergeek.com/ntfs_or_fat32_file_system.htm [accessed July 24th, 2012]
- Forensic Data Recovery. Forensic Data Recovery vs Data Recovery. http://www.cnwrecovery.com/html/forensic_dr.html [accessed July 19th, 2012]
- Kozierok, Charles M. The PC Guide. NTFS Architecture and Structures. Copyright 1997-2004. http://www.PCGuide.com/ref/hdd/file/ntfs/arch.htm. [accessed July 10th, 2012]
- Kozierok, Charles M. The PC Guide. NTFS Directories and Files. Copyright 1997-2004. http://www.PCGuide.com/ref/hdd/file/ntfs/files.htm. [accessed July 12th, 2012]
- Kozierok, Charles M. The PC Guide. Other NTFS Features and Advantages, Encryption. Copyright 1997-2004. http://www.PCGuide.com/ref/hdd/file/ntfs/other.htm. [accessed July 12th, 2012]
- Medeiros, Jason. NTFS Forensics: A Programmers View of Raw Filesystem Data Extraction. Grayscale Research. 2008. http://grayscale-research.org/new/pdfs/NTFS%20forensics.pdf. [accessed June 7th, 2012]
- Microsoft Support. Description of the exFAT file system driver update package. http://support.microsoft.com/kb/955704 [accessed July 25th, 2012] Microsoft Support. You cannot delete a file or folder on an NTFS file system volume. http://support.microsoft.com/kb/320081 [accessed July 16th, 2012] Microsoft Windows. BitLocker Drive Encryption. Copyright 2012. http://windows.microsoft.com/en-us/windows-vista/Bitlocker-Drive-Encryption-Overview [accessed July 25th, 2012]
- MSDN Blogs. Building Windows 8: An Inside Look from the Windows Engineering Team. Building the next generation file system for Windows: ReFS. Pub. January 16th, 2012. http://blogs.msdn.com/b/b8/archive/2012/01/16/building-the-next-generation-file-system- for-windows-refs.aspx [accessed July 24th, 2012]
- Ruhnka, John; Bagby, John. The CPA Journal, Forensic Uses of Metadata. June 2008. http://www.nysscpa.org/cpajournal/2008/608/essentials/p68.htm [accessed July 19th, 2012]
- Where is Your Data?. Dates: NTFS Created, Modified, Accessed, Written. 2009. http://whereismydata.wordpress.com/2009/02/14/dates-ntfs-created-modified-accessed-written/. [accessed July 3rd, 2012]
- Windows Server. File System Technologies, FAT Technical Reference. http://technet.microsoft.com/en-us/library/cc758586(v=ws.10). [accessed June 14th, 2012]
- Windows Server. File System Technologies, NTFS Technical Reference. http://technet.microsoft.com/en-us/library/cc778296(v=ws.10) [accessed June 14th, 2012]
- Windows. File Times. http://msdn.microsoft.com/en-us/library/windows/desktop/ms724290(v=vs.85).aspx [accessed July 3rd, 2012]
- Yousef, Mohammad. Tech Junkeez. File Systems Exposed (Part 2). August 2004. http://www.techjunkeez.com/archive/general/file_systems_exposed_2.htm [accessed July 24th, 2012]