B1 A Forensic Comparison of NTFS and FAT32 File Systems

Kelsey L. Rusbarsky, MS, 2007 7th Ave, Apt 815, Huntington, WV 25703; Cynthia Smith, MS, 4150 N. Mulberry Dr, Ste 250, Kansas City, MO 64116-1696; and Joshua L. Brunty, MS, and Terry Fenger, PhD, 1401 Forensic Science Dr, Huntington, WV 25701*

After attending this presentation, attendees will: (1) understand the fundamental differences between the New Technology File System (NTFS) and the file allocation table 32-bit file system (FAT32); (2) gain an understanding of basic digital forensic knowledge of these file systems and the complications and advantages of each.

This presentation will impact the forensic science community by recognizing the importance of understanding the foundation of a science before anything more can be studied, stressing that the organization and processes of file systems must be understood. This research works to bring foundational data into one coherent discussion so that one can accurately assess advantages and disadvantages of specific file system forensic analysis.

The file system in any storage device is essential to the overall organization, storage mechanisms, and data control of the device. A file system can be thought of as an index in a book, where the book can be broken down into sections and chapters. Without this breakdown of sections and chapters in a book, it would be harder to find the information that is being searched for.

The same principles apply to file systems on a computer or storage device.[1] File systems utilize hierarchical structures to organize files and file directories into useable formats. This formatting is accomplished through the use of clusters, sectors, and data entries located on a hard disk. Within data entries are located metadata files, which store user and application data about file dates and times, length, file size, file names, and more.[2] 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 focus of this research is to differentiate and compare the two file systems, New Technology File System (NTFS) and File Allocation Table (FAT32), in eight areas. The eight areas are: key structures, storage mechanisms, file names, directories, file date and time, file deletion, encryption, and forensic implications.

NTFS is a newer file system, beginning with Windows® NT and 2000, and has brought in a lot of new features, including better metadata support and advanced data structures.[3] FAT systems were originally used in DOS and Windows versions prior to Windows XP. The 32 in FAT refers to the 32-bit numbers that represent the cluster values. Even though the FAT operating system is not utilized in many newer hard drives, it is still often used as a default file system in removable media and storage devices, as well as computers with multiple operating systems.[4]

One of the major differences between the NTFS and FAT32 file systems is that NTFS uses a Master File Table (MFT) and FAT32 uses a File Allocation Table (FAT).[4,5] The MFT table houses data entries for all files. Even metadata files have an entry in the MFT table. NTFS stores all of its data in attributes, which are simply data files. One attribute will house metadata, one will house file data, like size, and one will store the actual file content.[5,6]

There are many more attributes than this. The FAT table simply points to where the file is housed within the file system. Any metadata is stored in the header at the beginning of the file.[1] Some other noted differences are the process of file naming, where FAT utilizes both long and short (8.3) names (8.3 filename, or 255 UTF-16 characters when using LFN) and that NTFS uses long file names (255 UTF-16 code units).[4] Other differences noted are with the file deletion and encryption processes. NTFS was designed with fairly advanced security, whereas FAT32 has little to no encryption capability and was not designed with security in mind.[7,8]

References:

1. Carrier, Brian. File System Forensic Analysis. Pearson Education. 2005.
2. 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 19, 2012]
3. NTFS. Last updated July 2012. http://en.wikipedia.org/wiki/Ntfs [accessed June 9, 2012]
4. Windows Server. File System Technologies, FAT Technical Reference. http://technet.microsoft.com/en-us/library/cc758586(v=ws. 10). [accessed June 14, 2012]
5. Windows Server. File System Technologies, NTFS Technical Reference. http://technet.microsoft.com/en-us/library/cc778296(v= ws.10) [accessed June 14, 2012]
6. 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 10, 2012]
7. 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 12, 2012]
8. Microsoft Windows. BitLocker Drive Encryption. Copyright 2012 http://windows.microsoft.com/en-us/windows-vista/Bitlocker-Drive- Encryption-Overview [accessed July 25, 2012]

NTFS, FAT32, File Systems

Copyright 2013 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS. ** Presenting Author*