New Technology File System (NTFS)

From Forensics Wiki

The **New Technology File System** (**NTFS**) is a file system developed and introduced by Microsoft in 1995 with Windows NT. As a replacement for the FAT file system, it quickly became the standard for Windows 2000, Windows XP and Windows Server 2003.

The features of NTFS include:

- Hard-links
- Improved performance, reliability and disk space utilization
- Security access control lists
- File system journaling

Contents

Time Stamps

NTFS keeps track of lots of time stamps. Each file has a time stamp for 'Create', 'Modify', 'Access', and 'Entry Modified'. The latter refers to the time when the MFT entry itself was modified. These four values are commonly abbreviated as the 'MACE' values. Note that other attributes in each MFT record may also contain timestamps that are of forensic value.

Additional information on how NTFS timestamps work when files are moved or copied is available here: Microsoft KB 299648 (http://support.microsoft.com/kb/299648)

Changes in Windows Vista

In Windows Vista, NTFS no longer tracks the Last Access time of a file by default. This feature can be enabled by setting the NtfsDisableLastAccessUpdate value to '0' in the Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem
```

Note that this feature has been around since as early as Windows 2000 [1] (http://technet.microsoft.com/en-us/library/cc959914.aspx) .

Alternate Data Streams

The **NTFS** file system includes a feature referred to as Alternate Data Streams (ADSs). This feature has also been referred to as "multiple data streams", "alternative data streams", etc. ADSs were included in **NTFS** in order to support the resource forks employed by the Hierarchal File System (HFS) employed by Macintosh systems.

As of Windows XP SP2, files downloaded via Internet Explorer, Outlook, and Windows Messenger were automatically given specific "zoneid" ADSs. The Windows Explorer shell would then display a warning when the user attempted to execute these files (by double-clicking them).

Sysadmins should be aware that prior to Vista, there are no tools native to the Windows platform that would allow you to view the existence of arbitrary ADSs. While ADSs can be created and their contents executed or viewed, it wasn't until the "/r" switch was introduced with the "dir" command on Vista that arbitrary ADSs would be visible. Prior to this, tools such as LADS (http://www.heysoft.de/Frames/f_sw_la_en.htm) could be used to view the existence of these files.

Microsoft FSRM (File System Resource Manager) also uses ADS as part of 'file classification'.

Examiners should be aware that most forensic analysis applications, including EnCase and ProDiscover, will display ADSs found in acquired images in red.

Advanced Format (4KB Sector) Hard Drives

NTFS does not natively handle drives that use the new standard of 4KB sectors. For information on this, see Advanced Format.

Transactional NTFS (TxF)

According to MSDN Transactional NTFS (TxF) allows file operations on an NTFS file system volume to be performed in a transaction.

Several TxF related file-system-metadata files can be found in the file-system-metadata directory: \$Extend\$RmMetadata\. TxF also uses the MFT attribute $LOGGING_UTILITY_STREAM with the name $TXF_DATA.

TxF uses the Common Log File System (CLFS)

External links

- Technet: How NTFS Works (http://technet.microsoft.com/en-us/library/cc781134%28WS.10%29.aspx) , by Microsoft
- Wikipedia: NTFS (http://en.wikipedia.org/wiki/NTFS)
- MSDN: Transactional NTFS (http://msdn.microsoft.com/en-us/library/bb968806%28v=VS.85%29.aspx)

- Wikipedia: Transactional NTFS (http://en.wikipedia.org/wiki/Transactional_NTFS)
- Windows NTFS Metadata Extractor Utility (http://www.tzworks.net/prototype_page.php?proto_id=12) Free tool that can be run on Windows, Linux or Mac OS-X
- Graphic Engine for NTFS Analysis (gena) (http://www.tzworks.net/prototype_page.php?proto_id=28) (GUI to view NTFS internals/extract data on live systems)
- Linux-ntfs Documentation (http://sourceforge.net/projects/linux-ntfs/files/NTFS%20Documentation/) Detailed documentation of the NTFS format by the Linux-NTFS driver creators.
- Default cluster size for NTFS, FAT, and exFAT (http://support.microsoft.com/kb/140365)
- New Technologies File System (NTFS) (http://code.google.com/p/libfslibs/downloads/detail?name=New%20Technologies%20File%20System%20%28NTFS%29.pdf) , by the libfslibs project, August 2009
- Incident Response with NTFS INDX Buffers – Part 1: Extracting an INDX Attribute (https://www.mandiant.com/blog/striking-gold-incident-response-ntfs-indx-buffers-part-1-extracting-indx/) , by William Ballenthin, September 18, 2012
- Incident Response with NTFS INDX Buffers – Part 2: The Internal Structures of a File Name Attribute (https://www.mandiant.com/blog/incident-response-ntfs-indx-buffers-part-2-internal-structures-file-attribute/) , by Jeff Hamm, September 26, 2012

Retrieved from "http://www.forensicswiki.org/w/index.php?title=New_Technology_File_System_(NTFS)&oldid=13315"
Category: File Systems

- This page was last modified on 8 January 2014, at 14:53.
- This page has been accessed 11,405 times.
-