Time Rules for NTFS File System for Digital Investigation

Tejpal Sharma[1], Manjot Kaur[2]

[1] Assitant Professsor,Deptt. of Computer science and Engg.
CGC-College of Engg. , Landran Mohali (Punjab), India
[2] Assitant Professsor,Deptt. of Computer science and Engg.
Khalsa College for Women, Amritsar,(Punajb), India

Abstract— Computer forensics (also known as cyber forensics) is a branch of forensic science that employs various analysis techniques to verify the facts and obtain the evidence related to computer crimes. The aim of computer forensics is to prevent computer related crimes by acquiring, analyzing and presenting the facts related to the crime. Computer forensics has been an extremely useful in solving various crimes related to cyber world. The main focus of research in this paper is time analysis of files used in windows system. The creation time, last written time, last accessed time and MFT modification time of a file are an important factor that indicates the events that have affected a computer system. The form of the time information varies with the file system and the information changes the features, depending on the user's actions such as copy, transfer or rename of files.

Keywords— : time analysis, MAC times, File system, NTFS, Digital Investigation.

I. INTRODUCTION

Computer forensic process is the process which is used to analyse the digital media like hard disk for the forensic process and then acquire the evidences from that media that may be helpful to solve the cyber crime case in which that hard disk involves.

A. NTFS File System:

NTFS is New Technology File System that determines naming, storing and organizing of data on a hard disk drive. This file system comes under window operating system which an upgrade from FAT file system and offers better performance and reliability such as file encryption, disk quota and also provide higher level security to the user [2,9].

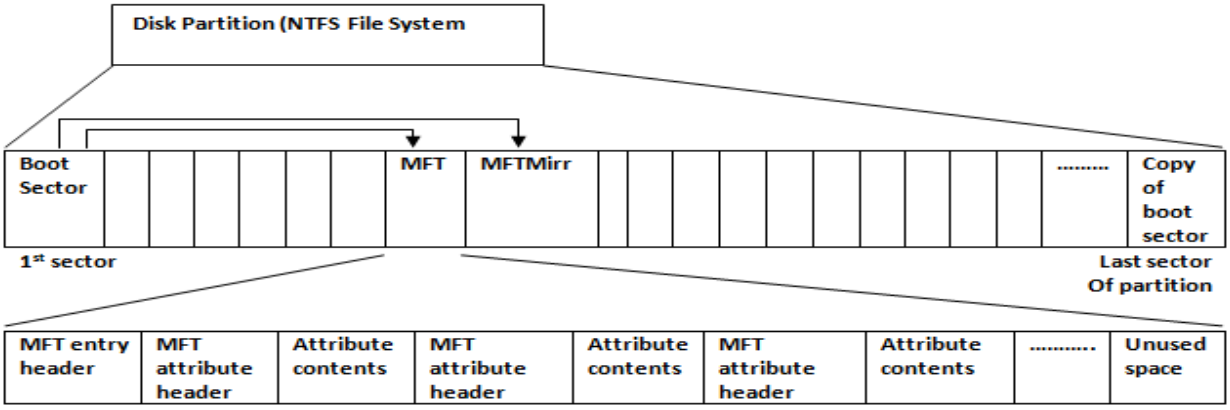

Figure 1. Basic organization of NTFS file system

The above figure describes that each NTFS partition has its first sector as the boot sector that contains the important information about the data and metadata stored on the disk. It contains information about the file system, version of the file system, boot code, starting cluster of MFT, MirrMFT, number of bytes

***Tejpal Sharma**, Assitant Professsor, Deptt. of Computer science and Engg., CGC-College of Engg. , Landran Mohali (Punjab), India*
***Manjot Kaur**, Assitant Professsor, Deptt. of Computer science and Engg. Khalsa College for Women, Amritsar,(Punajb), India.,*

ISSN: 2278 – 1323

in a sector and number of sectors in a cluster and some other information [2]. As said earlier we can get starting cluster of MFT from the boot sector and at that starting cluster we get 12 MFT entries reserved. These entries starts from 0 and end with 11.Each MFT entry is of 1024 bytes (size is given in the boot sector of partition).First entry is MFT entry ($MFT) itself. Each MFT entry contains header and attribute part. Its header is of 42 bytes and remaining part contains the attributes [2]. And the remaining part contains the attributes of MFT that describe about the file name, status of file, timing information of file, data of file etc. These attributes are listed in the table with their hex values [2].

TABLE 1

ATTRIBUTES OF MFT WITH THEIR HEX VALUES

ATTRIBUTE NAME	HEXADECIMAL VALUE
STANDARD_INFORMATION	0x10
FILE_NAME	0x30
OBJECT_ID	0x40
SECURITY_DESCRIPTOR	0x50
VOLUME_NAME	0x60
VOLUME_INFORMATION	0x70
DATA	0x80
INDEX_ROOT	0x90
INDEX_ALLOCATION	0xA0
BITMAP	0xB0
EA_INFORMATION	0xD0
EA	0xE0
LOG_UTILITY_STREAM	0x100

B. Description of attributes:

1. STANDARD_INFORMATION: It is the attribute that contains information about the creation time, last modification time, entry modification time and about the last access time of file and also provided ownership and security information of the file [2].

2. ATTRIBUTE_LIST: It gives the information about all the attributes in the MFT.

3. FILE_NAME: This attribute provides information about the four timing fields as given in the first attribute. It also contains information about the name of file, size allocated to file and actual size of file.

4. VOLUME_VERSION: It contains information about the volumes of file system. Version is divided into two parts major version and minor version. It exists in window NT.

5. VOLUME_NAME: It contains the name of volume.

6. VOLUME_INFORMATION: It contains information about file system version.

7. DATA: It the main attribute of the file MFT that contains information about the data or if file size is very small then data of file is stored in data attribute of file. When size is large does not fit in attribute then data is stored on the external clusters [2].

8. INDEX_ROOT: it contains information about the root directory of the file system.

9. INDEX_ALLOCATION: Large entries does not fit in the root directories then they need non-resident attributes to store their directory structure so this attribute is used to large directory structures.

10. EA_INFORMATION: information about the backward compatibility of operating system applications [2]

C. Time Analysis:

The file system is organized into a stream data and a metadata. The metadata is controlled by the different structures of the file system. The analysis of files can be performed from the timing information of the files that may lead to solve various cyber crime cases. When user executes any action on the files then its creation, modification and access time changes, which are helpful for computer forensic analysis of file system. There, are two attribute used in time analysis of NTFS file system and these are: $STANDARD_INFORMATION and $FILE_NAME. These attribute are useful for time analysis of NTFS file system [1]. These contain information about:

-CREATION TIME

-LAST ACCESS TIME

ISSN: 2278 – 1323

-MODIFICATION TIME

-ENTRY MODIFICATION TIME

II. LITERATURE SURVEY

The temporal analysis is also very useful in digital forensics. Chow et al. [3] suggested a technique that is useful for time analysis of files in NTFS. They first make their observation on the change of timing parameters when actions are performed on the data. Then they created their rule according to their observation and rules are checked on different scenarios. They created 10 scenarios for the files and folders for examining them. In this way they concentrated on the modification access and creation time of the files. And then these are compared with the created scenario and evidences are collected based on their search.

Timestamp forgery in NTFS file system is performed by Gyu-Sang Cho. In which they worked on the three different document files, txt, docx and pdf file for their time analysis and produced various rules [8].

III. RESEARCH ANALYSIS

Timing analysis of files:

We made our observation on the basis of actions performed on the file system. We concentrate on the timing information of the files those are very helpful to track user action on the files. Mainly two attributes are analyzed in this observation one is $STANDARD_INFORMATION and second is $FILE_NAME attribute. The changes in these two attributes are observed and rules are created according to them. We analyze the changes and then perform the actions on the files [3, 8].

The analysis is performed by using two tools: Disk Explorer 4.25 and DMDE 2.4.2.

Rules and observation result according to user actions on the files:

This analysis process is performed on Microsoft windows 7 ultimate, vista home premium and windows XP service pack 2.

1. Rules for Changes in time fields with various user actions on files windows 7

TABLE 2

CHANGES IN TIME FIELDS WITH VARIOUS USER ACTIONS ON FILES (RULES FOR WINDOWS 7)

Rule	**$SI# creation time**	**$SI# Last Modification time**	**$SI# Entry modification time**	**$SI# Last Access time**
	$FN* creation time	**$FN* last Modification time**	**$FN* Entry modification time**	**$FN* last Access time**
1. File creation	Creation time	Creation time	Creation time	Creation time
	Creation time	Creation time	Creation time	Creation time
2. File transfer in same volume	No change	No change	Transfer time	No change
	No change	No change	No change	No change
3. File transfer in different volume	Original file creation time	Original file modification time	Copy time	Copy time
	Copy time	Copy time	Copy time	Copy time
4. File copy in same volume	Copy time	Modification time of original file	Copy time	Copy time
	Copy time	Copy time	Copy time	Copy time

ISSN: 2278 – 1323

5. File copy in different volume	Copy time	Last Modification time of original file	Copy time	Copy time
	Copy time	Copy time	Copy time	Copy time
6. Editing in file	No change	Modification time	Modification time	No change
	No change	No change	No change	No change
7. Access to file	No change	No change	Last access time	No change
	No change	No change	No change	No change
8. Renaming file	No change	No change	Name change time	No change
	$SI Creation time before name change	$SI modification time before the name change	$SI entry modification time before name change	$SI Last access time before name change
9. Extraction of file from compressed zipped file	Extraction time	Creation time	Extraction time	Extraction time
	Extraction time	Extraction time	Extraction time	Extraction time
10. Restoration of file from recycle bin	No change	No change	Restoration time	No change
	$SI Creation time before deletion	$SI modification time before deletion	Deletion time	$SI Last access time before deletion
11. File replace	Old file creation time	Replacement time	Replacement time	Old file creation time
	Old file creation time	Old file creation time	Old file creation time	Old file creation time
12. Attachment of file to email	No change	No change	No change	No change
	No change	No change	No change	No change
13. Property change of file	No change	No change	Property change time	No change
	No change	No change	No change	No change
14. Download file	Download time	Download time	Download time	Download time
	Download time	Download time	Download time	Download time

Note: #:-$STANDARD_INFORMATION attribute and *:- FILE_NAME attribute

ISSN: 2278 – 1323

2. Rules for Changes in time fields with various user actions on files in windows vista (All other rules are same as window 7 table)

TABLE 3

CHANGES IN TIME FIELDS WITH VARIOUS USER ACTIONS ON FILES (RULES FOR WINDOWS XP)

Rule	**$SI[#] creation time**	**$SI[#] Last Modification time**	**$SI[#] Entry modification time**	**$SI[#] Last Access time**
	$FN[*] creation time	**$FN[*] last Modification time**	**$FN[*] Entry modification time**	**$FN[*] last Access time**
6.Editing in file	No change	No change	Edit time	No change
	No change	No change	No change	No change
9.Extraction of file from compressed zipped file	No change	No change	Extraction time	No change
	Extraction time	Extraction time	Extraction time	Extraction time

3. Rules for Changes in time fields with various user actions on files in windows Xp (Other rules are same as windows 7 table)

TABLE 4.

CHANGES IN TIME FIELDS WITH VARIOUS USER ACTIONS ON FILES (RULES FOR WINDOWS XP)

Rule	**$SI[#] creation time**	**$SI[#] Last Modification time**	**$SI[#] Entry modification time**	**$SI[#] Last Access time**
	$FN[*] creation time	**$FN[*] last Modification time**	**$FN[*] Entry modification time**	**$FN[*] last Access time**
3.File transfer in different volume	No change	No change	No change	Copy time
	Copy time	Copy time	Copy time	Copy time
4.File copy in same volume	Copy time	No change	No change	Copy time
	Copy time	Copy time	Copy time	Copy time
5.File copy in different volume	Copy time	No change	No change	Copy time
	Copy time	Copy time	Copy time	Copy time
6.Editing in file	No change	Edit time	Edit time	Edit time
	No change	No change	No change	No change
9.Extraction of file from compressed zipped file	No change	No change	Extraction time	No change
	Extraction time	Extraction time	Extraction time	Extraction time

ISSN: 2278 – 1323

11.File replace	Old file creation time	Last modification time of Replacement file	Last entry modification time of Replacement file	Replacement time
	Old file creation time	Old file modification time	Old file entry modification time	Old file access time

IV. CONCLUSION AND FUTURE SCOPE

From the research work it is concluded that, doubtful files are analysed according to their timing fields. User actions on the files are detected according to their creation, modification, entry modification and access time of the files. Analysis is performed on window's 7, window's vista and window's xp. 14 rules are created for the analysis purpose of NTFS files that can be used to detect user action on files. Window's 7 and Window's vista has maximum same rules but windows xp have some difference. For future work time analysis of files of various Linux based operating systems can be performed to detect actions performed on files.

REFERENCES

[1] Bang, J., Yoo, B., Kim, J. and Lee S., 2009. "Analysis of time information for digital investigation", Fifth international joint conference on In, IMS and IDC, IEEE conference 2009, pp 1858-1864.
[2] Carrier, B., 2005. "File system forensic analysis "Publishers: Addison Wesley Professional, March 17, 2005, ISBN: 0-32-126812-2.
[3] Chow, K.P., Kawan, M.Y. K., Law, F. Y. W. and Lai, K.Y., 2007. " The rules of time on NTFS system", In Proceedings of Systematic Approaches to Digital Forensic Engineering, Department of computer Science, The university of Hong Kong.
[4] Davis, J., MacLean, J. and Dampier, D., 2010. "Methods of information hiding and detection in file systems", Fifth international workshop on systematic approaches to digital forensic engineering, IEEE conference, pp 66-69.
[5] "DEFINING ISSUES: FORENSIC TECHNOLOGY, Proactive Forensics", KPMG cutting through complexity 2013, pp 1-2.
[6] DMDE 2.4.2. Free Edition- Disk Editor, Dmitry Sidorov, last accessed march, 2015, http://softdm.com/
[7] Disk Explorer 4.25 for NTFS file system, Runtime software, Laser accessed March, 2015, http://www.runtime.org/
[8] Gyu-Sang Cho, 2013. "A computer forensic method for detecting timestamp forgery in NTFS", computers and security 2013, pp 36-46.
[9] Kai, Z., En, C. and Qinquan, G., 2010. "Analysis and Implementation of NTFS file system based on computer forensics", Second international workshop on education technology and computer science, IEEE conference, pp 325-328.
[10] Naiqi, Lu. Zhongshan, W., Yujie, H. and Qunke,2008. "Computer forensics research and implementation based on NTFS file system",2008 ISECS International colloquium on computing, communication, control and management, IEEE conference, pp 519-523.
[11] Patel, Pratik. And Mishra, Shailendra. "Detecting timestamp forgery in NTFS file system using log file ", International Journal of Engineering Development and Research 2014, Vol. 2, Issue 3 ISSN: 2321-9939, pp 3224-3227.
[12] Pollitt, M., 1995. "Computer Forensics: an Approach to Evidence in Cyberspace", Proceedings of the National Information Systems Security Conference, Baltimore, Vol. 2, pp 487-491.

Tejpal Sharma received the B.Tech degree in Computer Science and Engineering and M.Tech degree in E-Security from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (Punjab). Presently working as Assistant Professor in Chandigarh Group of Colleges Landran, Mohali (Punjab). India.

Manjot Kaur received the B.Tech.degree in Computer Science from Rayat Institute of Engineering and Technology and M.Tech. degree in E-Security from Baba Banda Singh Bahadur Engineering College, respectively. Presently working as Assistant Professor in Khalsa College for Women Amritsar(Punjab), India.

ISSN: 2278 – 1323