Chapter 7
Understanding File System Forensics:
FAT, NTFS, HFS, and EXT

Henil Sanjaykumar Gandhi
https://orcid.org/0009-0009-0121-3255
Illinois Institute of Technology, USA

Aryan Dinesh Deshmukh
Illinois Institute of Technology, USA

ABSTRACT

In the following paper, we look at file system forensics intricacies for four dominant ones: EXT, FAT, NTFS and HFS. In this book, each of the system is discussed with its structure, operational characteristics and forensic challenge to collect evidence against it. The EXT family (EXT2, EXT3, EXT4) gets its turn on being evolutionary and providing tons of improvements around journaling and data integrity. It describes the FAT file system for its simplicity and great acceptance, then it presents common forensic techniques such as metadata examination and cluster chain analysis. Although NTFS has some advanced features of its own, such as the Master File Table (MFT) and strong journaling system that it uses to recover both resident and non-resident files, it's really not too much different from other file systems. Now comes to its proprietary nature with the analysis of HFS file system including Catalog file corruption, encryption handling, and more details about the entire structure of its Cloud.

DOI: 10.4018/979-8-3373-0857-9.ch007

INTRODUCTION

File systems are fundamental operations of computers that govern how data is stored and retrieved from the computer. They manage attributes like file properties, including the date and time of creation, file type, name, and last modification. Over the years, numerous file systems have been developed, but some of the most widely used include NTFS, which is an appropriate file system for Windows (Sterniczuk (2022)), and Linux file systems like ext4, XFS, Btrfs, and ZFS (Sterniczuk (2022)). File system forensics is an essential branch of cyber forensics, particularly when dealing with recovering deleted files, corrupt files, hidden files, and metadata from disks during forensic investigations. NTFS (New Technology File System), HFS (Hierarchical File System), FAT (File Allocation Table), and Ext (Extended File System) are among the prominent file systems discussed in this paper. FAT and Ext cater to different types of computing environments, but NTFS remains the default file system for Windows, while HFS is primarily used in macOS (Craiger & Burke (2005)). FAT and NTFS have always been of major significance in forensic analysis and investigation over the years. Microsoft developed both of these systems during different eras of computing. NTFS stands for New Technology File System. NTFS was developed on the evolutionary basis from FAT, and it has more advanced features in comparison, with improvements in reliability, file system structure, and security combined with user-friendliness. Currently, the Windows operating system has over 90% market share, and FAT32 and NTFS are common file systems used on a variety of Windows operating systems (Zhang, N., Jiang, Y., & Wang, J.2020).

File Allocation Table [FAT] File System

One of the oldest file systems is known as File allocation table (FAT) which was developed by Microsoft to use in floppy disks. It got utilized in hard drives & other equipment. FAT filesystem gets its moniker from the structure (array) of indexes to clusters (groups of contiguous disk sectors) with annotations (Li, Q., Zhang, Q., Tan, Y. A., Li, Y., & Zheng, J. (2016)) FAT, which stands for File Allocation Table, was first implemented back in 1977 as the standard filesystem of MS-DOS and Windows 9x operating systems.