# Chapter 30
# A New Timestamp Digital Forensic Method Using a Modified Superincreasing Sequence

**Gyu-Sang Cho**
*Dongyang University, Youngju, Republic of Korea*

## ABSTRACT

*This paper proposes a new digital forensic method using a modified superincreasing sequence. Timestamp changes by file commands in Windows NTFS file system are used for identifying what commands were executed and are a useful and a logical way for performing digital forensics. A superincreasing sequence is modified for the timestamp change patterns to make each timestamp pattern have a distinct value. The method has two functions; one is a timestamp change check function and the other is a forensic evaluation function. The former checks differences of timestamps between before and after command execution, and the latter produces a characteristic output by applying ten kinds of timestamp change patterns. According to the characteristic output, the kind of command that is executed is identified. By virtue of adopting the modified superincreasing sequence, the evaluation function could produce distinct characteristic output values and thereby provides a way to reconstruct executed file commands.*

## INTRODUCTION

Timestamp evidence is a fundamental component of many forensic computing examinations to reconstruct events, and the determination of event times is an important and difficult task in computer forensics. Numerous studies on the timestamps of file systems have been reported. Casey (2002) indicated that a MAC time analysis is necessary for the reconstruction of digital events. MAC timestamps record a file's most recent modification, access, and creation times. By reconstructing this information on a timeline, forensic investigators can find filesystem activity and computer usage of a particular time. An

DOI: 10.4018/978-1-7998-3025-2.ch030

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

investigator can also draw a historical plot of filesystem activity per time period (Grier, 2011). Boyd and Forster discussed time structure and its use in Microsoft Internet Explorer with local and UTC time translation issues (Boyd & Forster, 2004). Chow et al. presented behavioral characteristics of MAC times on an NTFS file system so that a validation basis for a temporal analysis of event reconstruction models can be formulated (Chow et al., 2007). Stevens introduced a clock model that can account for the various factors that affect the behavior of digital clocks such as those used in computers and other digital electronic devices (Stevens, 2004). Willassen presented a hypothesis-based investigation method to solve the problems of timestamp manipulation and a clock that is erroneous or improperly adjusted (Willassen, 2008).

J. Olsson and M. Boldt (2009) developed a computer forensic timeline visualization tool that provides a way to visualize evidence and allows investigators to find related evidence in a fast and intuitive manner. C. Hargreaves and J. Patterson (2012) proposed a technique that can automatically reconstruct high-level events from set of low-level events, analyzing patterns automatically. They described a framework that extracts low-level events to a SQLite backing store; the provenance of any high-level events is also preserved and the raw data that caused the low-level event to be initially created can also be viewed.

Recently, Cho (2013) proposed a method for detecting timestamp forgery in an NTFS filesystem. Log records that operate on files leave large amounts of information in the $LogFile that is used to reconstruct operations on the files and is also used as forensic evidence. If the past timestamps can be found before any changes to the file are made, this could act as evidence of a file time forgery. Rule sets for detecting a timestamp forgery based on using a difference comparison between changes in timestamp patterns by the file time change tool and normal file commands is provided, and the forensic rule sets of .txt", ".docx", and ".pdf" file types are applied for detecting timestamp forgery cases.

Digital forensic research on file systems other than NTFS has also been reported. Kevin D. Fairbanks (2012) presented a research paper on a low-level study and analysis of Ext4 file system data structures. The paper provided a more comprehensive analysis of the file system behavior with respect to data recovery. Ming Xu et al. presented experimental results under a Linux operating system demonstrating that the proposed method can correctly reconstruct the file system and recover file and file traces from YAFFS2; experiments conducted on physical images of Android phones show that this method can be applied to real scenarios (Xu et.al, 2013). A. Marrington et al. developed a tool that implements techniques for detecting contradictory and missing events in the history of the computer system. Experiments with this software demonstrated that the proposed techniques can be used successfully (Marrington et al., 2011).

In this paper, a new forensic method using a modified superincreasing sequence based on timestamp change patterns of commands on files in a Windows NTFS file system is proposed. A superincreasing sequence is modified for the timestamp change patterns such that each timestamp pattern has a distinct value. In chapter 2, ten timestamps patterns classified by their timestamp changes are explained. In chapter 3, the basic idea of a superincreasing sequence is introduced and a modified sequence to be utilized for timestamp forensics is proposed. In chapter 4, a new method composed of a timestamp change check function and a forensic evaluation function is described. Using two commands, "Copy" and "Move to an Outside Volume", the usefulness of the proposed forensic method is tested in chapter 5. Finally, concluding remarks is presented in chapter 6.

28 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/a-new-timestamp-digital-forensic-method-using-a-modified-superincreasing-sequence/252705

## Related Content

The Impact of Social Engineer Attack Phases on Improved Security Countermeasures: Social Engineer Involvement as Mediating Variable
Louay Karadsheh, Haroun Alryalat, Ja'far Alqatawna, Samer Fawaz Alhawariand Mufleh Amin AL Jarrah (2022). *International Journal of Digital Crime and Forensics (pp. 1-26).*
www.irma-international.org/article/the-impact-of-social-engineer-attack-phases-on-improved-security-countermeasures/286762

Electricity Theft, Regulatory Quality, and the Rule of Law: A Cross-Country Analysis
Gamze Kargn-Akkoçand Fuat Ouz (2023). *Theory and Practice of Illegitimate Finance (pp. 148-164).*
www.irma-international.org/chapter/electricity-theft-regulatory-quality-and-the-rule-of-law/330629

On the Pixel Expansion of Visual Cryptography Scheme
Teng Guo, Jian Jiao, Feng Liuand Wen Wang (2017). *International Journal of Digital Crime and Forensics (pp. 38-44).*
www.irma-international.org/article/on-the-pixel-expansion-of-visual-cryptography-scheme/179280

Malware: Can Virus Writers be Psychologically Profiled?
Gráinne Kirwanand Andrew Power (2012). *The Psychology of Cyber Crime: Concepts and Principles (pp. 73-92).*
www.irma-international.org/chapter/malware-can-virus-writers-psychologically/60684

Difference Between the Real and Estimated Size of a Company: A Potential Cause of Tax Evasion
Gerardo Reyes Ruiz (2023). *Theory and Practice of Illegitimate Finance (pp. 301-332).*
www.irma-international.org/chapter/difference-between-the-real-and-estimated-size-of-a-company/330639