한국컴퓨터정보학회 하계학술대회 논문집 제27권 제2호 (2019. 7)

안티포렌식을 위한 타임스탬프 변경도구들에 대한 디지털포렌식 관점에서의 기능의 분석

조규상O
동양대학교 컴퓨터학과O
e-mail: cho@dyu.ac.krO

Digital Forensic Analysis of Timestamp Change Tools: An Anti-Forensics Perspective

Gyu-Sang ChoO
Dept. of Computer, Dongyang UniversityO

● 요 약 ●

본 논문에서는 타임스탬프의 위변조를 위한 안티포렌식의 도구로 사용되는 타임스탬프 변경도구들에 기능에 대하여 디지털 포렌식 관점에서 분석을 수행한다. 타임스탬프 변경도구들로써 수행할 수 있는 타임스탬프 변경작업의 범위와 특징을 찾아본다. NTFS파일시스템에서 사용하는 타임스탬프 변경도구들의 기능상의 분류는 그것들이 변경할 수 있는 타임스탬프 종류와 정밀도를 기준으로 정하고 그 도구들을 사용한 후에 기록된 타임스탬프의 특징들을 디지털 포렌식 관점에서 분석을 수행하기로 한다. 이 연구에서의 분류 형태 중 타입 I은 FileTouch.exe, SKTimeStamp, BulkFileChanger류의 도구들과 타입 II는 timestomp, 타입 III은 SetMACE로 분류하고 각 도구들을 사용한 후에 변경된 타임스탬프들의 특징을 살펴보기로 한다.

키워드: 타임스탬프 변경도구(timestamp change tools), 디지털포렌식(digital forensics), NTFS 파일시스템(NTFS filesystem)

I. Introduction

타임스탬프는 디지털 포렌식 분석에 있어서 가장 기본적이면서도 가장 중요한 정보이다. 이벤트들을 시간대별로 분석할 수 있는 근거가 되기 때문이다. 타임스탬프의 시간을 위변조하여 포렌식 분석을 어렵게 만들기 위한 안티-포렌식(anti-forensic)을 하기 위한 도구들도 많이 사용되고 있다[1,2].

이 논문에서는 타임스탬프 변경툴들이 수행할 수 있는 기능을 중심으로 NTFS 파일시스템의 타임스탬프 정보인 $STANDARAD_INFORMATION($SI)속성과 $FILE_NAME($FN)속성에 각각 4개씩 들어 있는 생성시간, 수정시간, MFT 엔트리 수정시간, 접근시간 등의 전체 8개의 타임스탬프 중에서 변경가능한 타임스탬프의 범위와 시간의 정밀도를 기준으로 분류하기로 한다. 타임스탬프 변경툴은 타임스탬프를 임의로 변경할 수 있지만 툴의 기능들이 제한적으로 제공되고 있기 때문에 그에 맞게 기능을 이용해야 한다. 3가지 타입으로 분류할 수 있는데 타입 I은 생성시간, 수정시간, 접근시간의 3가지 타임스탬프만 수정이 가능한 경우이다. 타입 II는 "년-월-일 시:분:초"까지 수정이 가능한 경우이다. 타입 III은 "년-월-일 시:분:초.0000000" 100나노초까지 수정가능한 경우이다. 이런 타입에 따라 각 항목에 해당하는 대표적인 타임스탬프 변경툴에 대하여 2장에서 소개하기로 한다.

II. Timestamp Change Tools

1. Type I: FileTouch NewFileTime, Chtime etc.

타입 1에 속한 타임스탬프 변경도구들은 생성시간, 수정시간, 접근시간을 변경할 수 있는 기능을 갖고 있다. MFT엔트리 수정시간에 대해서는 변경할 수 있는 기능을 갖추고 있지 않다. 여기에 해당하는 도구들은 FileTouch, NewFileTime, Chtime, SKTimeStamp, BulkFileChanger, ChangeTimestamp, Filechtime.exe, XTST등 다수의 도구들이 존재한다.

이 도구들은 타임스탬프 관련 API들 중에서 SetFileTime()을 타임스탬프 변경에 사용하여 제작된 것이다[3]. 이 기능을 사용하면 프로그램을 쉽고 빠르게 제작할 수 있는 장점이 있지만 이 것은 생성시간, 접근시간, 수정시간만을 인수로 설정할 수 있는 제약이 있다. MFT 엔트리 수정시간은 이 도구를 사용하여 타임스탬프 변경작업을 수행한 순간의 기록되므로 이것을 근거로 언제 타임스탬프를 변경하였는지 알 수 있다.

```
BOOL SetFileTime(
      HANDLE hFile,
      CONST FILETIME *lpCreationTime,
      CONST FILETIME *lpLastAccessTime,
      CONST FILETIME *lpLastWriteTime
);
```

Fig. 1. SetFileTime() function prototype

2. Type II: Timestomp

Timestomp는 James C. Foster and Vincent Lie가 제작한 도구로써 MFT 엔트리 수정시간도 변경할 수 있는 기능을 갖고 있는 도구이다. 그러나. $FN 속성의 타임스탬프를 직접 변경시킬 수 있는 기능을 갖고 있지 않기 때문에 $SI 속성의 타임스탬프를 변경한 후에 파일의 이동명령을 수행하면 $SI 속성 타임스탬프가 $FN의 속성으로 복사되는 기능을 이용하여 $SI 속성과 $FN 속성을 의도한 대로 바꿀 수 있다[2,4]. 나노초의 설정기능이 없어서 100나노초까지의 십진수 7자리는 0000000으로 설정된다. 나노초 표시부분이 0000000으로 되어있다는 근거로 이 도구가 사용된 것을 추정할 수 있다.

3. Type III: SetMace

SetMACE(2014, Ver. 1.0.0.16)는 디스크를 직접 접근하여 타임스탬프에 쓰기 작업을 수행하는 도구이다. timestomp의 기능에서 구현되지 않은 $FILE_NAME 속성에 직접 쓰기 기능을 수행할 수 있다. 또한 시간을 YYYY:MM:DD:HH:MM:SS:MSMSMS:NSNSNSNS로 입력하여 년:월:일:시:분:초:밀리초:나노초 단위까지 입력할 수 있다. 타임스탬프 변조도구로는 유일하게 밀리초:나노초를 설정할 수 있다[5]. 이 도구가 가장 정밀하게 타임스탬프를 변경할 수 있는 기능을 갖고 있다.

III. Conclusions

이 논문에서는 NTFS의 $SI속성과 $FN속성의 생성시간, 수정시간, MFT엔트리 수정시간, 접근시간 등의 전체 8개의 타임스탬프 중에서 변경가능한 타임스탬프의 종류와 정밀도를 기준으로 툴들을 분류하였다. 생성시간, 수정시간, 접근시간 등의 3가지 타임스탬프만 수정이 가능한 경우(타입 I), “년-월-일 시:분:초”까지 수정이 가능한 경우(타입 II), “년-월-일 시:분:초.0000000” 100나노초까지 수정가능한 경우(타입 III)로 분류하였다. 안티포렌식 수행을 위하여 각 타입의 툴들이 사용되고 난 후에 나타나는 타임스탬프 변경의 특징들에 대하여 살펴보았다.

Table 1. Timestamp change tools and the characteristics

Type	Timestamp change tools	Creation time	Modified time	MFT entry modified time	Access time	Remarks
Type I	FileTouch, NewFileTime, SKTimeStamp등	y/m/d h:m:s 변경 가능	y/m/d h:m:s 변경 가능	변경 불가능 (변경작업 수행시간기록)	y/m/d h:m:s 변경 가능	초미만의 시간은 0000000 설정
Type II	Timestomp	y/m/d h:m:s 변경 가능	y/m/d h:m:s 변경 가능	y/m/d h:m:s 변경 가능	y/m/d h:m:s 변경 가능	초미만의 시간은 0000000으로 설정
Type III	SetMace	y/m/d h:m:s .0000000 까지 변경가능	y/m/d h:m:s .0000000 까지 변경가능	y/m/d h:m:s .0000000 까지 변경가능	y/m/d h:m:s .0000000 까지 변경가능	초미만시간을 100나노초(ns)정밀도로 설정가능

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (NRF-2016 R1D1A1B03935646)

REFERENCES

[1] Gyu-Sang Cho, “A Computer Forensic Method for Detecting Timestamp Forgery in NTFS”, Computer & Security, Vol. 34, 2013, pp. 36-46.

[2] Wicher Minnaard, "Timestomping NTFS," IMSc final research project report, Univ. of Amsterdam, Faculty of Natural Sci., Math. and Comp. Sci., Jul. 2014.

[3] https://docs.microsoft.com/en-us/windows/desktop/api /fileapi/nf-fileapi-setfiletime

[4] Metasploit Anti Forensics Projecthttp://www.metas ploit.com/research/projects/antiforensics/

[5] SetMace, “https://github.com/jschicht/SetMace”