디지털 포렌식 관점에서 이동식 저장매체의 은닉영역 분석 연구

홍표길 · 이대성· 김도현*

부산가톨릭대학교

A Study on Analysis of Hidden Areas of Removable Storage Device from a Digital Forensics Point of View

Pyo-gil Hong · Dae-sung Lee · Dohyun Kim*

Catholic University of Pusan

E-mail : kinvyrlfl744@gmail.com / dslee@cup.ac.kr / dohyun@cup.ac.kr

요 약

이동식 저장매체로 대표되는 USB 저장장치는 클라우드 서비스가 일상화된 요즘에도 널리 사용되고 있다. 하지만 USB 저장장치에 은닉영역을 생성하여 악용하는 경우가 있기 때문에 안티 포렌식 관점에서도 이를 탐지하고 분석하는 연구가 필요하다. 본 논문에서는 은닉 파티션을 생성하고 이곳에 파일을 저장할 수 있어 안티 포렌식으로 악용 될 수 있는 프로그램과 이것으로 만들어진 파일 시스템을 디지털 포렌식 관점에서 분석한다.

ABSTRACT

USB storage devices, which are represented by removable storage media, are widely used even nowadays when cloud services are common. However, since they are cases where hidden areas are created and exploited in USB storage devices. This research is needed to detect and analyze them from an Anti-forensic point of view. In this paper, we analyze a program that can be exploited as Anti-forensic because it can create a hidden partition and store files there, and the file system created by it from a digital forensic point of view.

키워드

Digital Forensics, Counter Anti-Forensics, Hidden Area Detection, Data Hiding, Removable Storage Deivce

Ⅰ. 서 론

USB 저장장치의 용량과 속도는 플래시 메모리의 발전으로 인해 널리 사용되고 있다. 하지만 USB에 은닉 파티션을 생성하는 등의 안티 포렌식의 발전과 대중화로 일반인들이 데이터를 은닉하거나 암호화하기 쉬워지면서 디지털 포렌식 조사를 어렵게 하고 있다. 본 연구를 통해 은닉 파티션을 생성하는 프로그램과 그로 인해 생성된 파일 시스템을 분석하여 은닉영역을 탐지하는 방법과 메타데이터 구조 및 파일 저장 방식을 분석한다. 본 논문은 은닉 영역을 탐지하는 방안을 제시하며, 은닉영역의 메타데이터 영역을 분석하여 이를 통한 안티 포렌식 대응 기술로 활용 가능하다.

* corresponding author

Ⅱ. 관련연구

김소희는 하드웨어 방식의 보안 USB 저장장치에 CD 영역을 생성하는 도구를 이용하여 은닉영역을 생성하는 방법과 그리고 그에 대한 탐지방안에 대해 논하였다[1]. Nir는 USB 저장장치에 기반을 둔 공격에 대한 동향을 연구했다. Nir의 Data hiding과 Hidden Partition의 연구는 본 논문과

관련이 있다[2]. Davis는 일부 Linux에서 은닉 파티션을 탐지할 수 있는 가능성과 은닉 파티션 생성하는 방법을 제시했다[3]. David는 Linux에서 은닉 파티션을 생성하는 방법과 은닉된 파티션에 데이터를 숨기는 방법에 대해 제시했다[4]. Mohamad는 파일 시스템과 관련된 안티 포렌식 기술의 동향을 연구를 했다[5].

III. 은닉 영역 탐지 및 메타데이터 분석 방법

3.1 MBR(Master Boot Record) 영역

본 논문에서는 은닉 영역을 생성하기 위해 부팅 USB를 제작하는 프로그램 Fbinst tool 1.6 version[6, 7]과 이것의 기반인 Fbinst[8] 오픈소스를 분석했다. [그림 1]은 은닉 영역이 생성된 이동식 저장매체의 MBR 영역이며 크기는 1섹터(512Byte)이다.

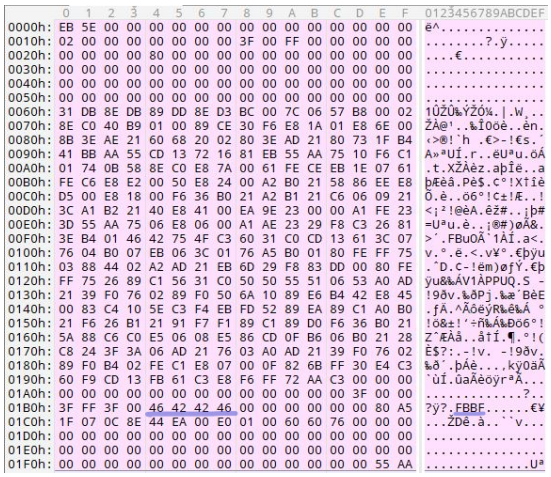

그림 1. MBR section

이 MBR 영역의 0x1B4~0x1B8은 Fbinst Signature이다. MBR 영역에 이 Signature가 있다면 은닉된 파티션이 존재할 수 있다. Fbinst는 은닉 영역을 생성하면서 이 MBR을 64개 연속적으로 쓴다. 이런 특징으로도 은닉된 파티션의 존재여부를 의심할 수 있다.

3.2 SubMBR 영역

SubMBR 영역은 [그림 1]의 MBR이 64번 반복된 후 65번 섹터이후에 존재하는 영역이다. Fbinst tool에서 생성하는 추가 MBR 코드를 다루고 있다. [표 1]은 SubMBR 영역의 오프셋에 해당하는 값이다.

표 1. SubMBR 구조

Byte Offset (Hex)	Size (Byte)	Meaning
0x8000~0x8001	2 Byte	Boot_Size
0x8002~0x8003	2 Byte	offset_flags
0x8004~0x8005	2 Byte	Fbinst Version
0x8006~0x8007	2 Byte	List_Used
0x8008~0x8009	2 Byte	List_Size
0x800A~0x800B	2 Byte	Primary_Size
0x800C~0x800F	4 Byte	Extend_Size
0x8010~0x868F	680 Byte	Sub Boot Code

은닉 영역에 저장할 수 있는 구역은 2가지로 나눠지는데, Primary 영역과 Extend 영역이다. Primary 영역은 8MB~30MB 크기이며, Extend 영역은 전체 은닉 영역의 나머지 부분이다. List Size는 메타데이터의 최대 크기를 의미한다.

3.3 File Metadata 영역

이 영역은 SubMBR이 끝나는 영역의 다음 섹터에 존재하며 파일의 이름, 크기, 수정시각, 데이터 시작위치 등이 저장된 영역이다. [그림 2]는 파일 메타데이터이다.

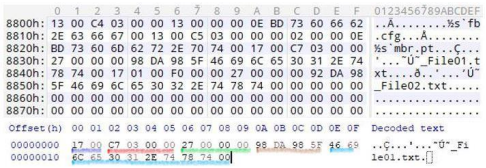

그림 2. File Metadata

표 2. File Metadata 구조

Byte Offset (Hex)	Size(Byte)	Meaning
0x00	1 Byte	Number of metadata chracters in file from 0x02
0x01	1 Byte	0 = Primary section, 1 = Extend section
0x02~0x05	4 Byte	File_start_Sector (Sector)
0x06~0x09	4 Byte	File_Size (Byte)
0x0C~0x0F	4 Byte	Modified time(UnixTime)
0x0E~0x17	10 Byte	File_Name (dynamic)
0x18	1 Byte	End Signature (00)

[표 2]는 파일 메타데이터 구조이다. 0x00은 0x02부터 파일 메타데이터의 길이다. 0x01은 저장할 영역을 의미한다. 파일 이름의 길이는 가변 길이이며 파일 이름이 변경되면 같이 변한다. 그 대

신 End Signature로 파일 메타데이터의 끝을 구분한다.

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 USB 저장장치에 도구를 이용해 특수한 파일 시스템이 존재하는 은닉 영역을 만들어 데이터를 체계적으로 은닉하는 방법에 대해 논하였다. 이러한 체계적인 방법은 사용자에게 더 손쉽게 파일을 은닉할 수 있게 도움을 줄 것이며, 나날이 조사해야할 데이터가 늘어가고 있는 디지털 포렌식 조사에 영향을 미칠 것으로 예상된다. 이 미징을 이용해 탐지가 가능하나 이러한 사전 지식 없이 찾기에는 매우 많은 시간을 소비할 것이다. 향후 연구는 디지털 포렌식 조사에서 이러한 은닉 영역을 조사하는 시간을 줄이기 위한 은닉 영역 탐지 기법과 본 논문에서 논한 은닉 방법과 유사하거나 더 효과적으로 은닉하는 방법에 대해 연구를 진행해 분석하고 탐지하는 방안을 연구할 예정이다.

Acknowledgement

This paper was supported by RESEARCH FUND offerd from Catholic University of Pusan.

References

[1] 김소희, 한재혁, 이상진. “플래시 메모리 기반 이동식 저장장치의 데이터 은닉 영역 탐지 방안에 대한 연구.” 디지털포렌식연구, 12(2), 21-29. 2018

[2] Nir Nissim, Ran Yahalom, Yuval Elovici, "USB-based attacks", Computers &Security, Volume 70, Pages 675-688, 2017.

[3] Davis, Jeremy & MacLean, Joe & Dampier, David, “Methods of Information Hiding and Detection in File Systems.” 10.1109/SADFE ,66-69. .2010.

[4] David Verhasselt, Hide Data in Invisible Partitions [Internet]. Available : https://davidverhasselt.com/hide-data-in-invisible-partitions/

[5] Mohamad Ahtisham Wani, Ali AlZahrani, Wasim Ahmad Bhat, "File system anti-forensics – types, techniques and tools", Computer Fraud & Security, Volume 2020, Issue 3, Pages 14-19, 2020.

[6] Fbinsttool 1.6 version [Internet] Available : http://bbs.wuyou.net/forum.php?mod=viewthread&tid=169595&highlight=

[7] Fbinsttool 1.7 version [Internet] Available : http://bbs.wuyou.net/forum.php?mod=viewthread&tid=189221&extra=page%3D1

[8] Chenall, Github Fbinst[Internet] Available : https://github.com/chenall/grubutils/tree/master/grubutils/fbinst/