외장형 저장장치의 파일유출에 관한 연구

(A Study of External Storage Device File Outflow)

송 유 진*, 이 재 용**

(Yu Jin Song and Jae Yong Lee)

요 약 외장형저장장치의 다양한 종류와 대용량화로 인해 대다수의 컴퓨터 사용자들이 사용하고 있다. 그러나 외장형 저장장치의 사용이 증가하면서 파일 유출사고도 늘고 있다. 이러한 파일 유출은 컴퓨터에서 파일을 실행하여 확인한 후 이동시키는 것과 파일명으로만 확인하고 이동시키는 경우로 나뉜다. 파일의 실행하여 확인하는 경우는 응용프로그램의 실행정보를 통해 흔적을 확인할 수 있으나 파일의 실행 없이 외장형 장치로 이동되는 경우 응용프로그램의 실행흔적이 남지 않아 포렌식 조사에 어려움이 많았다. 본 논문에서는 외장형 저장장치의 인식방법과 연결정보를 통하여 외장형 저장장치의 볼륨정보, 시간정보를 획득하는 방법과 링크파일의 분석을 통해 외장형 저장장치의 볼륨정보를 획득하여 서로 비교하고 링크파일의 생성시간정보, 접근시간 정보 등을 획득하여 파일의 실행 없이 외장형 장치로 이동되는 경우의 포렌식 조사에 도움을 줄 수 있는 방법을 제시한다.

핵심주제어 : File Outflow, Portable Storage Device, Key/Thumb Drive, Drive Enclosure

Abstract A lot of computer users use external memory device. But, same time file efflux incidents are also increasing. There are two ways people use for efflux file. One is moving it after checking file which is running on computer and the other is checking file name only. Checking from running file case, we can identify vestige with running information of applied program but, the case of moving as external device without running file there is no evidence running applied program. So there are a lot of difficulty with forensic investigation. In this paper we suggest the way to help forensic investigation which is method of getting external memory device information of volume and time through its awareness method and connection information and moving to external device without running file after compare the external memory device volume information through link file analysis and getting information of link file formation & access time from link file.

Key Words : File Outflow, Key/Thumb Drive, Drive Enclosure, Forensic Investigation

1. 서 론

컴퓨터 사용자들은 다양한 형태의 외장형 저장장치를 사용하고 있으며 여러 가지 형태의 파일을 저장하여 편리하게 사용하고 있다. 그러나 최근 외장형 저장장치를 컴퓨터에 접속하여 중요한 파일을 이동시키거

나 또는 외장형 저장장치로부터 악의적인 파일을 컴퓨터에 저장함으로써 많은 문제가 발생되고 있다. 외장형장치는 Thumb drive와 Drive Enclosure 타입으로 나누어 사용되고 있으며, 파일을 유출하거나 삽입하는 경우는 해당 컴퓨터에서 파일을 실행하여 확인하고 이동하는 경우와 실행하지 않고 이동하는 경우로 나누어 볼 수 있다. 파일을 실행하여 확인하는 경우는 최근 실행된 응용프로그램 또는 최근 실행된 파

* 한서대학교 전자·컴퓨터·통신학부, 제1저자

** 한서대학교 전자·컴퓨터·통신학부, 교신저자

일에서 그 흔적을 찾을 수 있으나 파일을 실행하지 않고 이동시켰다면 최근 실행된 응용프로그램이나 최근실행파일에 그 흔적이 남지 않게 된다. 그러나 파일을 실행하지 않았더라도 링크파일(Shell Link)에는 그 정보가 남아있게 된다. 본 논문에서는 외장형 저장장치의 연결정보를 분석하여 어떠한 종류의 저장장치가 연결되었는지를 구분하고 외장형 저장장치의 연결이 후 파일의 실행 없이 이동된 정보를 확인할 수 있는 방법을 제시 한다.

2. 윈도우에서의 외장형저장장치 구분 방법

윈도우(Windows)는 부트영역에 저장되는 고유의 ID (Disk Signature)를 통해 장치의 GUID(Globally Unique Identification Number)를 생성한다. 윈도우의 경우 시스템에 어떤 장치가 마운트 되면 레지스트리에 해당 장치의 GUID 값을 생성하고 이 값을 통하여 장치를 다루게 된다. 마운트된 장치 GUID는 윈도우 레지스트리 "HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices"에 저장된다. 볼륨의 GUID 외에 드라이브 문자를 기준으로 한 GUID가 존재하는 것도 확인할 수 있다. 드라이브 문자로 지원하는 것은 현재 또는 가장 최근에 각 드라이브에 마운트 되었던 장치의 정보이다[1][2][3][4].

```

[[[
HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices
    \DosDevices\A: 5c 00 3f 00 3f 00 5c 00 46 00 44 00 43 00 23 00
    \DosDevices\C: 86 30 5c 0e 00 7e 00 00 00 00 00 00
    \DosDevices\D: 86 30 5c 0e 00 5e c6 52 07 00 00 00
    \DosDevices\E: 5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00
    \DosDevices\F: 86 30 5c 0e 00 4a f3 34 0c 00 00 00
    \DosDevices\G: ae f2 b8 00 00 7e 00 00 00 00 00 00
    \DosDevices\H: 5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00
    \DosDevices\I: a0 ad a0 ad 00 16 71 02 00 00 00
    \DosDevices\J: 5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00
    \DosDevices\K: 5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00
    \DosDevices\L: 5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00
    \DosDevices\M: a0 ad a0 ad 00 a2 71 63 07 00 00 00
]]]

```

<그림 1> 드라이브에 따른 GUID

2.1 Thumb drive

USB 저장장치의 경우는 형태에 따라 다른 GUID 형식을 가지고 있으며, 일반적으로 Thumb drive, Drive Enclosure의 형태로 나뉜다. Thumb drive는 고유의 ID값을 갖고 있지 않고, Drive Enclosure 형태의 드라이브 장치는 케이블로 IDE(Integrated Drive

Electronics)와 SATA(Serial Advanced Technology Attachment)방식을 통해 BIOS(Basic Input Output System)가 해당 드라이브를 인식하게 된다. 외장형 저장장치의 방식에 따라 생성되는 ID를 통하여 Thumb drive와 Drive Enclosure의 형태를 구분할 수 있다.

Offset	Title	Value
0	Master bootstrap loader code	FA B8 00 00 8E D0 BC 00 7C 8B F4 5
440	Windows disk signature	0
440	Same reversed	0

<그림 2> Thumb drive Disk Signature

<그림 2>는 Thumb drive가 연결된 값을 보여주고 있으며 고유의 ID 값이 존재하지 않는 것을 확인할 수 있다.

```

[[[
HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices
    \DosDevices\A: 5c 00 3f 00 3f 00 5c 00 46 00 44 00 43 00 23 00 47 00
    \DosDevices\C: 86 30 5c 0e 00 7e 00 00 00 00 00 00
    \DosDevices\D: 86 30 5c 0e 00 5e c6 52 07 00 00 00
    \DosDevices\E: 5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00
    \DosDevices\F: 86 30 5c 0e 00 4a f3 34 0c 00 00 00
    \DosDevices\G: ae f2 b8 00 00 7e 00 00 00 00 00 00
    \DosDevices\H: 5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00
    \DosDevices\I: a0 ad a0 ad 00 16 71 02 00 00 00
    \DosDevices\J: 5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00
    \DosDevices\K: 5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00
    \DosDevices\L: 5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00
    \DosDevices\M: a0 ad a0 ad 00 a2 71 63 07 00 00 00
]]]

```

<그림 3> Thumb drive Mounted Device GUID

<그림 3>은 J, K, L, 파티션에 Thumb drive가 마운트된 것을 확인할 수 있는 내용이다.

2.2 Drive Enclosure

Drive Enclosure는 고유의 ID값을 갖고 있으며 이는 시스템에 장치가 마운트 되면 레지스트리에 해당 장치의 GUID 값을 생성하고 후에 이 값을 사용해 장치를 다루게 되는 과정에서 같은 외장형 저장장치라고 할지라도 구분되어 다른 GUID를 갖게 되는 것이다[5].

Offset	Title	Value
32256	Master bootstrap loader code	EB 52 90 4E 54 46 53 20 20 20 20 00
32696	Windows disk signature	44522069
32696	Same reversed	69205244

<그림 4> Drive Enclosure Disk Signature

이름	데이터
W??Volume{8f...	a0 ad a0 ad 00 a2 71 53 07 00 00 00
W??Volume{8f...	86 30 5c 0e 00 5e c6 52 07 00 00 00
W??Volume{8f...	86 30 5c 0e 00 4a f3 34 0c 00 00 00
W??Volume{8f...	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00
W??Volume{8f...	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00
W??Volume{aa...	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00
W??Volume{b1...	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00
WdosDevicesWA...	5c 00 3f 00 3f 00 5c 00 46 00 44 00 43 00 23 00 47 00 45 0c
WdosDevicesWC...	86 30 5c 0e 00 7e 00 00 00 00 00 00
WdosDevicesWD...	86 30 5c 0e 00 5e c6 52 07 00 00 00
WdosDevicesWE...	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 64 0c
WdosDevicesWF...	86 30 5c 0e 00 4a f3 34 0c 00 00 00
WdosDevicesWG...	5b 0b 47 b1 00 7e 00 00 00 00 00 00
WdosDevicesWH...	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00
WdosDevicesWI...	a0 ad a0 ad 00 14 16 71 52 00 00 00
WdosDevicesWJ...	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00
WdosDevicesWK...	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00
WdosDevicesWL...	5c 00 3f 00 3f 00 5c 00 53 00 54 00 4f 00 52 00 41 00 47 00
WdosDevicesWM...	a0 ad a0 ad 00 a2 71 53 07 00 00 00

<그림 5> Enclosure Mounted Device GUID

<그림 5>에서 C:, D:, F: 파티션은 같은 디스크를 사용하고 있으며, I:, M: 파티션도 같은 디스크를 사용한다. 현재 시스템 하드디스크의 경우 C: 파티션은 주 파티션으로 사용 중이며, D:, F:는 확장파티션으로 사용 중이다. G: 파티션은 Drive Enclosure 형태의 외장형 저장장치가 마운트된 정보이다[5].

2.3 Thumb drive와 Drive Enclosure의 로그

외장형 저장장치의 설치 로그의 첫 부분에는 장치 타입(USBSTOR), 제조사, 제품명, 펌웨어버전 등을 저장하고 있는 Device Class ID와 Device Instance ID를 확인할 수 있다. Device Instance ID는 장치 고유의 식별자로서 장치의 serial number가 기록되어, <그림 6>의 [2011/04/07 13:05:47]과 같이 연결정보를 확인할 수 있다. 장치에 고유 식별자가 존재하지 않는 경우엔 운영체제는 GUID를 할당한다.

```
[2011/04/07 13:05:47 556.3 Driver Install]
#-019 usb#vid_8564&pid_1000&rev_1100,usb#vid_8564&pid_1000 하드웨어 ID를
검색 중
#-018
usb#class_08&subclass_06&prot_50,usb#class_08&subclass_06,usb#class_08
호환 ID를 검색 중
#-198 명령줄 처리됨: C:\WINDOWS\system32\services.exe
#1022 "USB#Class_08&SubClass_06&Prot_50"(C:\WINDOWS\inf\usbstor.inf) 발
견: 장치: "USB 대용량 저장소 장치"; 드라이버: "USB 대용량 저장소 장치"; 공급자:
"Microsoft"; Mfg: "Compatible USB storage device"; 구역 이름: "USBSTOR_BULK".
#1023 실제 설치 구역: [USBSTOR_BULK.NT]. 링크: 0x00002000. 드라이버 유효 날
짜: 07/01/2001.
#-166 장치 설치 기능: DIF_SELECTBESTCOMPATDRV.
#1063 선택한 드라이버는 [USBSTOR_BULK] 구역("c:\windows\inf\usbstor.inf")
에서 설치됩니다.
#320 장치의 클래스 GUID: {36FC9E60-C465-11CF-8056-444553540000}
#1060 선택한 드라이버를 설정했습니다.
```

<그림 6> Thumb drive/ Drive Enclosure 설치로그

3. 실행된 파일과 실행되지 않은 파일정보

3.1 실행된 파일의 정보

컴퓨터내의 응용프로그램을 통하여 작업을 한다면 시스템 레지스트리의 최근 사용한 응용프로그램 정보와 최근에 접근한 폴더, 확장자 연결정보에 그 내용이 남게 된다. 최근 사용된 폴더와 파일의 정보는 시스템 레지스트리의 다음위치 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU를 통해 최근 접근한 폴더의 순서를 확인할 수 있다. <그림 7>의 MRU List를 통해 최근 접근한 폴더를 확인할 수 있다.

파일(F)	편집(E)	보기(V)	출력하기(S)	도움말(H)	이름	데이터
App Paths					(21) 숨은 항목	
Applets					컴퓨터	45 00 45 00 50 00 50 00 4c 00 4f 00 52 00 45 00 2e 00
CINTLGN					컴퓨터	53 00 47 00 44 00 5e 00 5c 00 64 00 72 00 2e 00 65 00
Control Folder					컴퓨터	47 00 4f 00 44 00 2e 00 55 00 76 00 55 00 00 45 00
Explorer					컴퓨터	6d 00 73 00 70 00 61 00 69 00 6e 00 74 00 2e 00 65 00
Advanced					컴퓨터	65 00 54 00 69 00 74 00 70 00 6c 00 75 00 73 00 2e 00
AutoComplete					컴퓨터	40 00 56 00 69 00 65 00 77 00 32 00 30 00 30 00 30 00
AutoPlayHandlers					컴퓨터	73 00 69 00 6d 00 63 00 6f 00 5e 00 2e 00 65 00 76 00
BitBucket					컴퓨터	52 00 46 00 5f 00 4e 00 56 00 5f 00 4d 00 61 00 6e 00
BrowseNewProcess					컴퓨터	51 00 43 00 4e 00 56 00 69 00 65 00 77 00 2e 00 65 00
CabinetState					컴퓨터	45 00 46 00 53 00 45 00 76 00 70 00 6c 00 6f 00 72 00
CD Burning					컴퓨터	42 00 75 00 69 00 6c 00 64 00 47 00 61 00 6e 00 67 00
CLSID					컴퓨터	50 00 52 00 47 00 65 00 49 00 2a 00 65 00 78 00 65 00
ComDlg32					컴퓨터	6e 00 6f 00 74 00 65 00 70 00 61 00 64 00 2e 00 65 00
LastVisitedMRU					컴퓨터	amtdcsbrnqpoelkijghf
OpenSaveMRU						
ComputerDescriptions						

<그림 7> MRU List

만약 최근 접근한 폴더의 순서상에 기록된 내용이 없다면 해당 프로그램에 대하여 작업한 기록이 남게 되는 확장자 연결정보 레지스트리인 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts의 하위키를 확인한다. 각각의 하위키를 확인해 보면 각 확장자마다 연결된 프로그램의 정보가 최신 순으로 저장되어 있다[6][7].

3.2 실행되지 않은 파일의 정보

컴퓨터에서 실행되지 않은 파일들은 응용프로그램 사용흔적에서 찾을 수 없지만 파일이 이동되어진 정보는 링크파일에 남아있게 된다. 링크파일은 타겟 파일(Target File)에 대한 정보를 갖고 있으며 어플리케이션, 디렉터리, 데이터 파일, 프린터 등에 대한 정보를 가지고 있다. 링크파일은 응용프로그램, 디렉터리, 파일 등의 객체를 참조하는 파일로써 하나의 완벽한 파일형식을 갖고 있기 때문에 이를 분석하여 필요한 정보를 얻을 수 있다. <그림 8>은 링크파일생성 당시의 타겟파일 Time 정보를 보여주고 있다[6][8].

<그림 12>는 타겟 파일이 들어있는 파일시스템의 볼륨시리얼넘버가 링크파일에 그대로 부여되는 것을 보이고 있다.

Link Data	
Serial Number	730B-53E4
Drive Type	J
Base Name	C:\Documents and Settings\All Users\Document

<그림 12 >Link File의 Volume Serial Number

5. 결 론

최근 컴퓨터 사용자들은 외장형 저장장치의 사용편의성과 보편성이 증가함에 따라 외장형 저장장치를 많이 사용하고 있다. 그러나 외장형 저장장치의 사용이 증가하면서 파일 유출사고도 늘어나고 있다. 이러한 파일의 유출을 확인하는 과정에서 컴퓨터에서 파일의 실행이 없었다면 쉽게 확인할 수 없게 된다. 본 논문에서 제시한 외장형 저장장치의 인식방법과 연결정보를 통하여 외장형 저장장치의 볼륨정보 획득과 시간정보의 획득을 통해 컴퓨터의 링크파일에 볼륨정보를 확인하여 매칭하고 최근 링크 파일의 분석을 통하여 생성시간정보와 접근시간 정보를 획득한다면 외장형 저장장치로의 파일이동 흔적을 확보할 수 있을 것이다. 파일의 실행 없이 외장형 장치로 이동되는 경우 응용프로그램의 실행흔적이 남지 않아 포렌식 조사에 어려움이 많았다. 하지만 외장형 저장장치의 정보를 시스템 레지스트리 연결정보기록 분석으로 확인할 수 있고, 링크파일의 분석을 통해 파일의 이동정보를 확인할 수 있다. 앞으로 다양한 외장형 저장장치의 사용과 파일 유출 사고가 있을 것이다. 파일의 유출은 주로 외장형 저장장치를 통해 실행되는 경우가 많기 때문에 연계 조사를 반드시 하여야 하며, 실행되지 않은 파일은 흔적을 남기지 않는다고 대부분 알려져 있으나 조사자의 분석방법에 따라 이동증거의 획득이 가능하며 링크파일의 정보를 통해 그 기록이 남아있음을 확인할 수 있었다. 늘어나는 파일 유출사고와 다양한 외장형 저장장치의 등장에 따라 조사자의 증거확보 능력은 중요한 부분이며 지속적인 연구가 있어야 할 것이다.

참 고 문 헌

- [1] Rob Lee, "Profile Windows XP USB Drive Enclosures," SANS, Sept. 2009.
- [2] Rob Lee, "Profile Windows XP USB Keys/Thumbdrives," SANS, Sept. 2009.
- [3] J. Axelson, USB Mass Storage: Designing and Programming Devices and Embedded Hosts, Lakeview Research, 2006.
- [4] 최영희, 유재수, 오재철, "논리볼륨 관리자를 위한 매핑 관리자의 설계 및 구현", 한국산업정보학회 학술대회논문집, pp.350-362, 2002년 11월.
- [5] 송유진, 이재용, "외장형 USB 저장장치의 포렌식 조사방법", 한국산업정보학회 논문지, 제15권, 제4호, 2010.
- [6] Brian Carrier, "File System Forensic Analysis," Addison-Wesley, 2005.
- [7] Harlan Carvey, "Windows Forensic Analysis, 2nd Edition," June 2009.
- [8] Microsoft, FAT32 File System Specification, <http://www.microsoft.com/whdc/system/platform/firmware/fatgen.mspx>

송 유 진 (Yu Jin Song)

- 한서대학교 물리학과 이학사
- 한서대학교 정보보호공학과 공학 석사
- 한서대학교 디지털포렌식학과 박사수료
- 에이알모드커뮤니케이션(주) 웹/팀장
- 한서대학교 컴퓨터공학전공 겸임강사
- 관심분야 : 정보보호, 디지털포렌직

이 재 용 (Jae Yong Lee)

- 인하대학교 전자계산학과 이학사
- 인하대학교 전자계산학과 이학석사
- 인하대학교 전자계산공학과 공학박사
- KIST/SERI 연구원
- 수원여자대학 컴퓨터응용학부 조교수
- 한서대학교 컴퓨터공학전공 교수
- 관심분야 : 신경언어컴퓨팅(Neuro Linguistic Computing), 인터넷관리, 디지털포렌직

논문접수일 : 2011년 04월 15일

1차수정완료일 : 2011년 06월 01일

게재확정일 : 2011년 06월 23일