외장형 USB 저장장치의 포렌식 조사방법

(Forensic Investigation of External USB Drive)

송 유 진*, 이 재 용**
(Yu-Jin Song and Jae-Yong Lee)

요 약 휴대용 저장장치의 기술 발달로 저장장치의 대용량화가 가속화 되고 많은 데이터들의 이동 및 보관이 편리해 졌다. 휴대용 저장장치로는 USB 저장장치가 보편화 되어 사용되고 있으며, 포렌식 측면에서 이러한 USB 저장장치의 사용흔적 확보는 휴대용 저장장치를 통한 중요데이터 유출에 관한 조사를 가능하게 한다. 부트영역에 남아있는 USB 저장장치의 사용흔적을 확보하게 된다면 데이터 유출 및 범죄 행위 입증에 관한 조사가 가능하게 된다. 본 논문에서는 Disk Signature의 분석을 통한 USB Key/Thumb drive, USB Drive Enclosure 사용여부의 확인과 구분방법을 제시한다.

핵심주제어 : Disk Signature, Portable storage device, Key/Thumb drive, Drive Enclosure

Abstract Because of portable storage device's technical improvement, it's speeding up the conversion of mass storage. It means it's easier to move and save data. Generally, USB is using for portable storage device and forensic perspective, it's possible us to study data drain through portable storage device under securement of using vestige of USB. If we can secure using vestige of USB from boot domain it's possible to investigate data drain & prove criminal act. This thesis is suggesting Key/Thumb drive & USB Drive Enclosure's confirmation of using or not and division way though Disk Signature analysis.

Key Words : Disk Signature, USB Key/Thumb drive, USB Drive Enclosure

1. 서 론

외장형 USB 저장장치는 사용편의성과 다른 저장매체(CD, DVD, 플로피디스켓)보다 우수한 저장능력으로 사용자 수가 증가했다. USB 저장장치는 대용량, 소형화에 따른 사용자수의 급증으로 여러 가지 문제점 또한 발생되고 있다. USB 저장장치의 분실로 인한 정보유출, 장치 소형화에 따른 소지 여부의 확인이 어려워지는 등 기밀정보의 유출사고가 발생되고 있다. 이러한 사고의 수사를 위해 USB 저장장치의 사용에 관한 조사를 필요로 하고 있으며 어떤 종류의 USB 저장장치가 사용되었는지를 확인하는 것은 사고조사의 가장 중요한 부분을 차지한다. 수사관이 범죄에 사용 된 USB 저장장치의 사용흔적을 찾아내어 USB 저장장치의 증거물 획득에 성공한다면 사건 해결에 많은 도움을 줄 것이다. 그러나 최근 USB를 통한 외장하드디스크의 연결이 증가함에 따라 Thumb drive 형태인지, Drive Enclosure 형태인지를 파악하고 증거확보에 임한다면 보다 정확한 증거확보에 도움이 될 것이다. 이에 본 논문에서는 Signature 분석을 통한 Thumb drive, Drive Enclosure의 구분을 보임으로써 정확한 증거확보를 가능하게 할 수 있다.

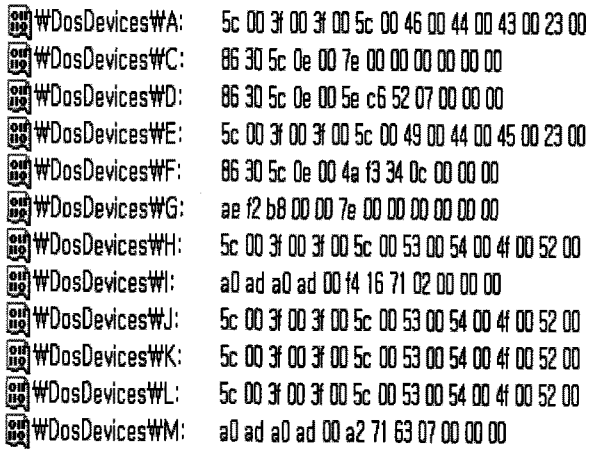
* 한서대학교 전자·컴퓨터·통신학부, 제1저자
** 한서대학교 전자·컴퓨터·통신학부, 교신저자

2. 저장매체 관리방법

2.1 MBR Signature를 이용한 관리방법

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.

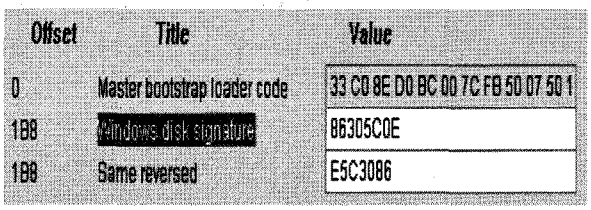
마운트된 장치 GUID는 윈도우 레지스트리 "HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices" 에 저장된다. 볼륨의 GUID 외에 드라이브 문자를 기준으로 한 GUID가 존재하는 것도 확인할 수 있다. 드라이브 문자로 지원하는 것은 현재 또는 가장 최근에 각 드라이브에 마운트 되었던 장치의 정보이다.



<그림 1> 드라이브에 따른 GUID

해당 값의 데이터에는 12바이트의 값이나 12바이트 이상의 값들이 존재하는데, 12바이트의 값이 존재하는 것은 해당 장치의 MBR(Master Boot Record)이 존재하는 경우이고 나머지는 CD-ROM, USB 저장장치 등을 나타낸다. 12바이트의 문자는 MBR의 정보를 이용해 생성하지만 그보다 긴 값들은 운영체제가 임의로 생성하게 된다[2][3].

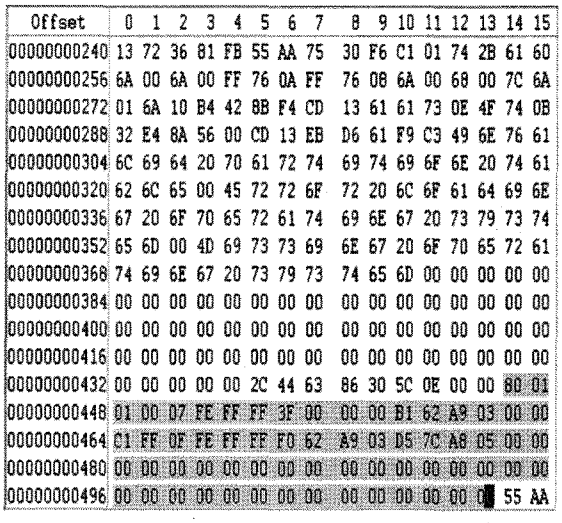
MBR은 저장매체의 LBA 0번 섹터에 존재하는 영역으로 해당 볼륨의 파티션 정보와 각 파티션의 부트 섹터(Boot Sector)의 부트코드(Boot Code)를 실행하기 위한 MBR 부트코드가 저장된다.



<그림 2> MBR

MBR(LBA 0 Sector) 512 바이트의 내용은, 처음 446 바이트는 부트코드 영역으로 ROM(Read Only Memory) BIOS(Basic Input/Output System)에 의해 POST(Power On Self-Test)과정을 마친 후 실행되는 코드이다.

부트 코드의 주 역할은 파티션 테이블에서 부팅 가능한 파티션을 찾아 해당 파티션의 부트 섹터를 호출해 주는 역할을 수행한다. 이어 나오는 64바이트의 파티션테이블은 해당 볼륨의 파티션정보를 저장한다. 각 파티션은 16바이트로 정보가 표현되기 때문에 총 4개의 파티션 정보가 저장 가능하다. 따라서 기본적으로 한 장치 당 주 파티션이 4개 까지만 생성이 가능하다. 더 많은 파티션을 생성하기 위해서는 확장 파티션을 통해 논리 파티션을 생성하고 사용해야 한다. 하지만 논리 파티션의 경우에는 부팅이 불가능하기 때문에 부팅 가능한 파티션은 각 장치 당 4개로 MBR의 설계 당시 정해진 값이다[1].



<그림 3> MBR(LBA 0 Sector)

마지막 2바이트는 해당 MBR의 Signature를 나타낸다. 섹터 시그니쳐(Sector Signature)로 부르기도 하며, 각 파티션의 부트섹터에도 섹터 마지막 2바이트에 동일한 Signature가 기록된다[5].

2.2 Disk Signature를 이용한 관리방법

부트코드 영역으로 사용하는 446 바이트의 영역의 Offset 440 부터 4바이트가 해당 디스크의 Signature를 나타낸다. <그림 2> MBR에서 고유ID는 "86 30 5C 0E" 이다. 따라서 해당 디스크가 마운트될 경우 이 ID 값을 사용하여 장치의 GUID를 생성한다. <그림 1> 레지스트리의 내용을 보면 C, D, F 드라이브가 같은 고유의 ID를 사용하고 있음을 알 수 있다.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000240	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60
00000000256	6A	00	6A	00	FF	76	0A	FF	76	08	6A	00	68	00	7C	6A
00000000272	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B
00000000288	32	E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	6E	76	61
00000000304	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61
00000000320	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E
00000000336	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
00000000352	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61
00000000368	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00
00000000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000432	00	00	00	00	00	2C	44	63	86	30	5C	0E	00	00	80	01
00000000448	01	00	07	FE	FF	FF	3F	00	00	00	B1	62	A9	03	00	00
00000000464	C1	FF	0F	FE	FF	FF	F0	62	A9	03	D5	7C	A8	05	00	00
00000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

<그림 4> Windows disk signature

분석대상 디스크는 파티션이 두 개로 나눠져 있다. C: 는 주 파티션 D:, F: 는 확장파티션으로 구성되어 있다. 레지스트리 내용을 보면 앞의 4바이트는 각 장치의 MBR ID 값을 사용하는데 뒤의 8바이트는 서로 다른 것을 확인할 수 있다. 나머지 8바이트는 각 파티션의 시작 위치(바이트)를 나타낸다. MBR 이미지에서 파티션 테이블을 살펴보면 각 파티션의 정보는 16바이트로 구성된다[1][5].

<표 1> 파티션의 정보

0 - 0	Bootable Flag
1 - 3	Starting CHS Address
4 - 4	Partition Type
5 - 7	Ending CHS Address
8 - 11	Starting LBA Address
12 - 15	Size in Sectors

파티션의 시작주소를 나타내는 값은 8-11의 영역인 "Starting LBA Address" 이다. 대부분의 저장매체는 용량의 한계로 CHS 대신 LBA 주소표현방식을 사용한다.

<표 2> 각 파티션의 시작위치정보

C:\ : 0x0000003F (63)
D:\ : 0x03A962F0 (61432560)

C:의 경우 파티션의 시작이 디스크의 63번째 섹터부터라는 의미이며, 섹터의 위치를 나타낸다.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000240	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60
00000000256	6A	00	6A	00	FF	76	0A	FF	76	08	6A	00	68	00	7C	6A
00000000272	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B
00000000288	32	E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	6E	76	61
00000000304	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61
00000000320	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E
00000000336	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
00000000352	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61
00000000368	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00
00000000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000432	00	00	00	00	00	2C	44	63	86	30	5C	0E	00	00	80	01
00000000448	01	00	07	FE	FF	FF	3F	00	00	00	B1	62	A9	03	00	00
00000000464	C1	FF	0F	FE	FF	FF	F0	62	A9	03	D5	7C	A8	05	00	00
00000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

<그림 5> 주 파티션 정보

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000192	0A	77	23	72	05	39	46	08	73	1C	B8	01	02	BB	00	7C
00000000208	8B	4E	02	8B	56	00	CD	13	73	51	4F	74	4E	32	E4	8A
00000000224	56	00	CD	13	EB	E4	8A	56	00	60	BB	AA	55	B4	41	CD
00000000240	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60
00000000256	6A	00	6A	00	FF	76	0A	FF	76	08	6A	00	68	00	7C	6A
00000000272	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B
00000000288	32	E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	6E	76	61
00000000304	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61
00000000320	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E
00000000336	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
00000000352	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61
00000000368	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00
00000000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000432	00	00	00	00	00	2C	44	63	86	30	5C	0E	00	00	80	01
00000000448	01	00	07	FE	FF	FF	3F	00	00	00	B1	62	A9	03	00	00
00000000464	C1	FF	0F	FE	FF	FF	F0	62	A9	03	D5	7C	A8	05	00	00
00000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

<그림 6> 확장파티션 정보

<그림 1>과 <표 3>의 C:, D:, E:의 데이터를 살펴보면 MBR ID 값과 시작 위치를 조합한 것이 GUID라는 것을 확인할 수 있다.

<표 3> 섹터의 바이트 변환

C:\ : 0x3F(63) * 0x200(512) = 0x00007E00 (32256)
D:\ : 0x03A962F0 (61432560) * 0x200(512) =0x0752C5E000 (31453470720) + 0x00007E00 (32256) = 0x0752C65E00 (31453502976)

포렌식 조사자의 관점에서 MBR이 존재하는 디스크의 경우 사용자가 임의적으로 해당 레지스트리 값을 지우지 않는다면 Mounted Device에 GUID 값이 저장된다. 용의자가 외장하드나 포터블 저장매체의 사용을 통한 범죄에 대하여 증거인멸을 시도할 경우 이 부분에서 증거의 인멸이 가능해진다. 포렌식 조사자는 Mounted Device의 정보를 확인하여 가장 최근에 마운트된 장치나 이전에 마운트된 장치의 정보를 기반으로 관련 장치를 획득할 수 있어야 한다.

3. 외장형 USB 저장장치 구분과 증거획득

3.1 USB Thumb drive 사용증거

USB 장치의 경우는 형태에 따라 다른 GUID 형식을 가진다. 일반적으로 USB는 Thumb drive, Drive Enclosure 형태로 나눠진다. USB Drive Enclosure 형태의 드라이브 장치는 케이블로 IDE 또는 SATA 방식을 통해 BIOS가 해당 드라이브를 인식한다. 따라서 고유 ID를 통하여 Thumb drive, Drive Enclosure 형태를 구분할 수 있다[2][3].

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 7> USB Thumb drive Disk Signature

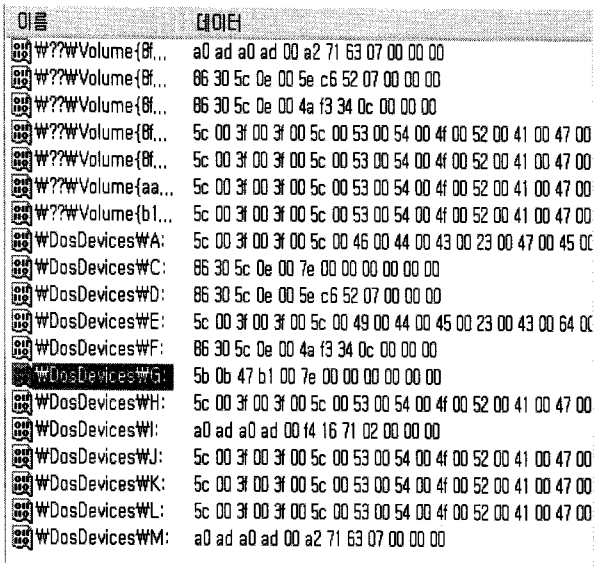
<그림 7>에서 보는 것과 같이, USB Thumb drive는 고유의 ID 값이 존재하지 않는다.

3.2 USB Drive Enclosure 사용증거

<그림 7>에서 USB Drive Enclosure는 고유의 ID 값을 갖고 있으며 이는 시스템에 장치가 마운트 되면 레지스트리에 해당 장치의 GUID 값을 생성하고 후에 이 값을 사용해 장치를 다루게 되는 과정에서 같은 외장형 USB 저장장치라고 할지라도 구분되어 다른 GUID를 갖게 되는 것이다.

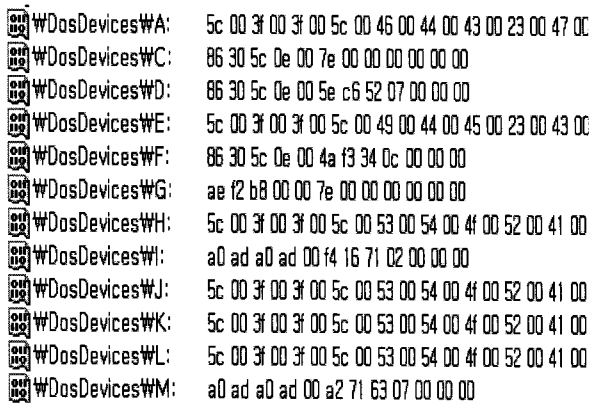
Offset	Title	Value
32256	Master bootstrap loader code	EB 52 90 4E 54 46 53 20 20 20 20 00
32696	Windows disk signature	44522069
32695	Same reversed	69205244

<그림 8> USB Drive Enclosure Disk Signature



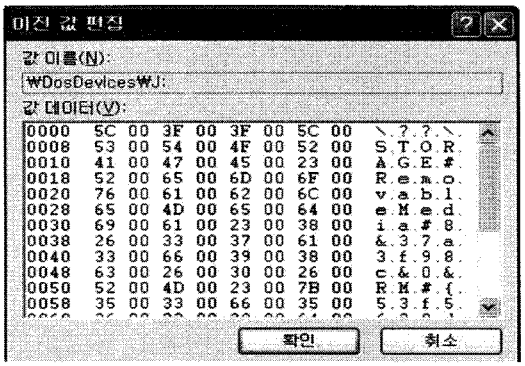
<그림 9> USB Drive Enclosure Mounted Device GUID

<그림 9>에서 추가적으로 확인할 수 있는 정보는 C:, D:, F: 파티션은 같은 디스크를 사용하고 있으며, I:, M: 파티션도 같은 디스크를 사용한다. 현재 시스템 하드디스크의 경우 C: 파티션은 주 파티션으로 사용중이며, D:, F:는 확장파티션으로 사용 중이다. G: 파티션은 USB Drive Enclosure 형태의 외장하드가 마운트된 정보이다.

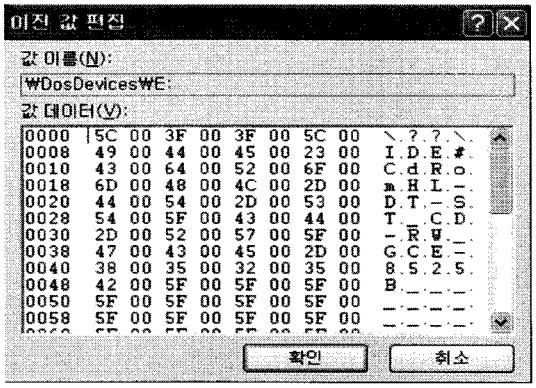


<그림 10> USB Thumb drive Mounted Device GUID

<그림 10>에서 J:, K:, L:, 파티션은 USB Key/ Thumb drive가 마운트된 정보이다.



<그림 11> USB Thumb Drive GUID Data



<그림 12> CD-ROM/RW GUID Data

USB Thumb Drive와 USB Drive Enclosure는 서로 다른 Mounted Device GUID를 갖게 된다. 이것은 어떤 USB Drive를 사용했는지에 대한 명확한 구분을 가능하게 한다.

3.3 외장형 USB 저장장치의 설치 증거

Windows는 부트영역에 저장되는 고유의 ID를 통해 장치 관리 정책에 따라 설치 로그를 저장한다. 저장된 정보는 USB 저장매체의 사용 흔적을 확인할 수 있게 한다. XP의 경우 C:\WINDOWS\Setupapi.log에 Vista와 Win7은 C:\WINDOWS\inf\Setupapi.dev.log에 장치 설치 과정에 대한 로그가 저장된다.

<그림 13> 장치설치 로그

<그림 13>의 장치설치 로그에서 설치 로그의 첫 부분에는 장치 타입(USB STOR), 제조사, 제품명, 펌웨어버전 등을 저장하고 있는 Device Class ID와 Device Instance ID를 확인할 수 있다. Device Instance ID는 장치의 고유의 식별자로써 장치의 serial number가 기록된다. 또한 [2010/11/03 10:08:26 552.3 Driver Install]과 같은 항목을 통해 장치의 연결 시간정보를 확인할 수 있다. 이것은 다른 장치에 연결되더라도 같은 값으로 기록되기 때문에 사용에 관한 기록을 획득할 수 있다. 장치에 고유 식별자가 존재하지 않는 경우에 운영체제는 GUID를 할당한다[2][4].

<그림 11>에서 운영체제가 할당한 값을 확인할 수 있다. 운영체제가 Signature를 통해 할당한 GUID 정보는 관련 윈도우 레지스트리"HKLM\SYSTEM\MountedDevices"에 저장되어 있으므로 <그림 1> 드라이브에 따른 GUID의 내용에서 장치의 사용여부를 정확히 확인하고 외장형 USB 저장장치의 사용 구분을 확인 할 수 있다.

4. 결 론

최근 휴대용 대용량 USB 저장장치의 급속한 증가로 인한 많은 정보 유출의 피해가 보고되고 있다. 정보 유출에 관한 조사가 다양한 USB 저장장치들에 대하여 이루어지고 있지만 3장에서 분석한 고유 ID 분석을 통한 외장형 USB 저장장치의 구분이 선행된다면 사건해결에 많은 도움이 될 것이다. 본 논문에서 제시한 외장형 USB 저장장치의 구분방법과 사용 흔적에 관한 조사방법은 다양한 USB 저장장치가 증거로 제출되었다 하더라도 정확한 증거물 채택으로 인한 빠른 수사결론에 도움을 줄 수 있다. 앞으로 더욱 다양해질 휴대용 USB 저장장치의 사용에 관한 조사는 수사관의 사건해결에 많은 어려움을 줄 수 있다. 이에 다양한 휴대용 저장장치에 알맞은 증거수집 확보에 관한 연구가 있어야 할 것이다.

참 고 문 헌

[1] Harlan Carvey, "Windows Forensic Analysis, 2nd Edition," June, 2009.

[2] Rob Lee, "Profile Windows XP USB Drive Enclosures," SANS, Sep, 2009.

[3] Rob Lee, "Profile Windows XP USB Keys/ Thumb drives," SANS, Sept, 2009.

[4] J. Axelson, *USB Mass Storage: Designing and Programming Devices and Embedded Hosts*, Lakeview Research, 2006.

[5] 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 공학석사
- 한서대학교 디지털포렌직학과 박사과정
- 한서대학교 전자·컴퓨터·통신학부 겸임
- 관심분야 : 정보보호, 디지털포렌식

이 재 용 (Jae-Yong Lee)

- 인하대학교 전자계산학과 이학사
- 인하대학교 전자계산학과 이학석사
- 인하대학교 전자계산공학과 공학박사
- 한서대학교 전자·컴퓨터·통신학부 교수
- 관심분야 : 인터넷관리, 디지털포렌직, Neuro Linguistic Human Computer Interaction

논 문 접 수 일 : 2010년 11월 01일
1차수정완료일 : 2010년 11월 22일
게 재 확 정 일 : 2010년 11월 29일