KIPS Tr. Comp. and Comm. Sys.
Vol.6, No.1 pp.17~24 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2017.6.1.17

Process of Collection for a Removable Storage Device Image Using a Software

Baek Hyun Woo† · Jeon Sang Jun†† · Sang Jin Lee†††

ABSTRACT

As the prevalence of removable device, critical intelligences are often stored in the removable device. For that reason, in seizure and search, the removable device became a important evidence of while it could be has a salient key for prove a crime. When we acquired a removable device for proof, we image it by a imaging device or software with a write protection. However, these are high-priced exclusive equipments and sometimes it could be out of order. In addition, we found that some secure USB and inbuilt vaccine USB are failed to connect to the imaging device. Therefore, in this paper, we provide a suitable digital evidence collection procedure for real.

Keywords : Removable Storage Device, Imaging, Secure USB, Write Blocker, Imaging Device

소프트웨어를 이용한 이동식 저장매체 이미지 수집 절차

백 현 우† · 전 상 준†† · 이 상 진†††

요 약

이동식 저장매체가 널리 보급됨에 따라 중요한 정보가 이동식 저장매체에 보관되는 경우가 많아지고 있다. 따라서 핵심적인 범죄 증거 역시 이동식 저장 매체에 존재할 가능성이 커지고 있으며 압수·수색 현장에서 이동식 저장 매체는 반드시 수집해야 할 대상이 되었다. 이동식 저장매체를 증거물로 획득한 경우 하드웨어 기반의 이미징 장비나 쓰기방지장치를 동반한 포렌식 소프트웨어를 통해 이미징 작업을 진행한다. 하지만 이런 장비의 경우 고가일 뿐만 아니라 현장에서 고장으로 인해 급하게 사용할 수 없는 경우를 배제할 수 없다. 또한 실험을 통해 확인한 결과 보안 USB 혹은 백신 USB의 경우 하드웨어 기반의 이미징 장비나 쓰기방지장치에서 인식을 할 수 없는 경우를 발견하였다. 따라서 본 논문에서는 현재의 이동식 저장매체에 맞는 디지털 증거 수집절차를 제안한다.

키워드 : 이동식저장매체, 이미징, 보안USB, 쓰기방지장치, 이미징장비

1. 서 론

이동식 저장매체는 대용량화와 소형화가 많이 진행되었다. 다양한 이동식 저장매체 중 USB는 크기가 매우 작아 높은 휴대성을 제공하면서도 용량 대비 가격이 저렴하여 많은 사용자를 확보하고 있다. 최근 대용량을 필요로 하는 사용자를 위하여 대용량 USB도 개발되었고 사용자들은 더욱 많은 자료들을 이동식 저장매체에 저장할 수 있게 되었다. 반면 이동식 저장매체의 휴대성으로 인하여 분실 및 도난 사고의 발생빈도가 증가하였고 그로 인한 개인정보 및 기업의 주요정보 유출 사고에 대한 문제점이 발생되었다[1].

이러한 사고를 방지하기 위하여 제조사는 보안 솔루션을 내장한 이동식 저장매체를 개발하였다. 지문을 이용하여 사용자 인증을 하거나 패스워드를 통한 인증 등 다양한 솔루션이 개발되었다. 이동식 저장매체에서 보안 기능을 이용하는 경우 다른 사용자들이 인증과정을 거치지 못한다면 내부 데이터에 대해서 확인이 불가능하기 때문에 범죄자들은 이를 악용하여 데이터 은닉 용도로 사용하는 사례 또한 증가하고 있다. 실제 2006년 발생한 일심회 사건에서는 용의자들이 국가 기밀 정보를 보안 USB에 저장하고 있는데 압수수색과정에서 발견되었다.

수사관은 현장에서 이동식 저장매체를 증거물로 획득하였

† 준 회 원 : 고려대학교 정보보호대학원 정보보호학과 석사과정
†† 비 회 원 : 프리랜서
††† 종신회원 : 고려대학교 정보보호대학원 교수
Manuscript Received : June 15, 2016
First Revision : August 2, 2016
Second Revision : August 30, 2016
Third Revision : October 24, 2016
Accepted : October 25, 2016
* Corresponding Author : Sang Jin Lee(sangjin@korea.ac.kr)

을 경우 디지털 증거처리절차에 따라서 쓰기방지장치 혹은 하드웨어 기반 이미징 장비를 사용하여 이미지파일을 생성하고 원본 증거물과 이미지 파일의 해쉬값을 비교하여 복제된 이미지 파일에 대한 무결성을 유지한다. 하지만 실험을 통해 확인한 결과 자체적으로 보안 또는 백신 기능을 내장하고 있는 특수 USB 중 일부 제품들은 쓰기방지장치 혹은 하드웨어 기반의 이미징 장비를 통해서는 인식되지 않는 경우를 확인하였다. 또한 하드웨어 기반 이미징 장비의 경우 고가이고, 현장에서 쓰기방지장치가 고장이 나는 경우도 배제할 수 없다.

쓰기방지를 통해 해쉬값의 변화를 방지하는 것은 디지털 포렌식에서 매우 중요한 절차 중 하나이다. 본 논문에서는 기존의 소프트웨어를 이용하여 하드웨어기반의 장비나 쓰기방지장치 없이 수사관의 PC를 이용하여 안전하게 이미징할 수 있음을 보이고, 기존의 이동식 저장매체를 수집하는 절차에 추가적인 방법을 제안한다.

2. 관련 연구

디지털 증거물은 데이터의 위, 변조가 쉽다. 따라서 디지털 증거를 수집할 경우 원본의 변경이 없도록 각별히 주의해야 하며, 이를 확인할 수 있는 암호학적 해쉬 함수를 이용하여 무결성을 확보해야 한다. 이 때, 입회인의 서명 날인 등을 이용하여 객관적인 자료를 확보해야 한다. 표준 가이드라인에 따르면 1)네트워크 접속은 금지하며 2)데이터 복제 과정에서 원본을 안전하게 보존하고 무결성을 확보해야 하고 3)획득된 디지털 증거에 대해 인증기관에서 데이터의 해쉬값을 비교하여 디지털 증거의 무결성을 검증한다[2]. 국내 절차에 대해 살펴보면 수사기관에서 수집한 디지털 증거에 대해 인증기관에서 데이터의 해쉬값을 비교하여 디지털 증거의 무결성을 검증한다.

현재 시중에 판매되고 있는 보안 USB는 분실, 도난 시 타인의 사용을 금지하기 위하여 사용자 인증 기능을 비롯한 위치정보를 추측할 수 있는 IP 주소 추적 기능과 지정된 PC에서만 사용하도록 하는 기능 등을 제공하고, 사용자의 편의를 위하여 접근이 허용된 사용자만 사용할 수 있는 보안영역과 누구나 접근이 가능한 일반영역으로 나누어서 사용할 수 있다[3].

보안 USB에 대한 발달은 점차 가속화되고 있고 국가에서도 이에 대한 세부 내용으로 1)사용자 식별/인증 기능 2)지정데이터 암/복호화 3)저장된 자료의 임의 복제 방지기능 4)분실 시 저장데이터의 보호를 위한 삭제 기능 등을 정확히 명시하고 평가하고 있다[4]. 이러한 보안 USB를 증거물로 수집하였을 경우 보안영역에 접근할 수 없다면 수사관은 내부 데이터를 확인할 수 없다. 이를 해결하기 위하여 Truecrypt 등의 소프트웨어를 기반으로 이동식저장매체를 암호화하는 FDE (Full Disk Encryption)을 해결하기 위한 연구[5]가 계속해서 진행되고 있다. 또한 USB에서 사용하는 컨트롤러를 분석하여 사용자 인증 절차를 우회할 수 있는 연구가 있다[6]. 그 밖에도 보안 USB에 대한 취약점 분석으로 메모리상에 남아있는 패스워드를 추출[7]하거나 소프트웨어 구현상의 취약점을 공격하여 패스워드 인증 알고리즘을 무력화하는 연구[8] 등 다양한 연구가 진행되고 있다.

수사기관에서는 이런 방법을 사용하기 이전에 현장에서 증거물을 압수하였을 경우 이미징 작업을 최우선으로 하고 분석실에서 분석을 진행하게 된다. 이미징 작업을 위해서 수사관은 정해진 절차에 의해서 이미지 파일을 생성하게 되는데, 실험을 통해 확인한 결과 일부 보안 USB 혹은 백신 USB의 경우 쓰기방지장치와 하드웨어 기반의 이미징 장비에서 인식하지 못하는 것을 확인하였다. 따라서 기존의 연구 내용을 반영하여 실무에서 반영할 수 있는 절차가 필요한 상황이다.

3. 디지털 증거 수집절차 및 문제점

디지털 증거 수집은 디지털 증거를 포함한 디지털 증거물을 획득하고 해당 매체 내의 데이터를 분석하여 사건과 관련된 디지털 증거를 추출하는 과정을 의미한다.

각 수사기관에서는 상황에 맞는 디지털 증거 수집절차를 가이드라인으로 제시하고 있고 새로운 이슈가 생길 경우 이에 대한 수정을 진행하고 있다.

3.1 TTA 표준 가이드라인

한국정보통신기술협회에서 제안하고 있는 표준가이드라인에서는 컴퓨터 포렌식과 관련된 내용이 명시되어 있다. 하지만 이동식 저장매체에 대해서는 주변 장치 수집과 관련된 설명만 있을 뿐 해당 저장매체에 대하여 어떻게 디지털 증거를 수집해야 하는지는 명시되어 있지 않다. 다만 표준 컴퓨터 포렌식 가이드라인에서는 사건 현장에서 획득한 디스크에 대한 디지털 증거 수집 절차를 제시하고 있다. 가이드라인에서 제시하고 있는 수집 절차는 Fig. 1과 같다. 1)먼저 분석관은 증거물의 형태 및 인터페이스를 확인하고, 종류 및 특징에 따라 분석에 필요한 정보 및 기법을 사전에 숙지할 것을 명시하고 있다. 2)디스크의 타입 확인 과정이 끝난 뒤에 가이드라인에서는 디지털 증거물에 대한 복제 여부를 결정하도록 한다. 물리적인 복제를 할 경우 쓰기방지장치를 이용하되 원본의 디스크 크기보다 동일하거나 혹은 더 큰 하드디스크를 준비할 것을 설명하고 있다. 복제 작업이 완료된 뒤에는 동일성 및 무결성을 입증하기 위하여 원본 및 복사본의 해쉬값을 수집, 비교해야 한다. 3)복제 여부를 확인 후 디스크에 대한 이미지 파일을 생성할 것인지를 결정한다. 디스크에 대한 이미지 파일을 생성할 경우 복제와 동일하게 쓰기방지장치를 연결한 후 이미징을 해야 한다. 4)생성한 디스크 복제본 혹은 이미지 파일을 이용하여 디지털 증거 분석을 수행하고 분석에 대한 보고서 작성 및 전달하여야 한다.

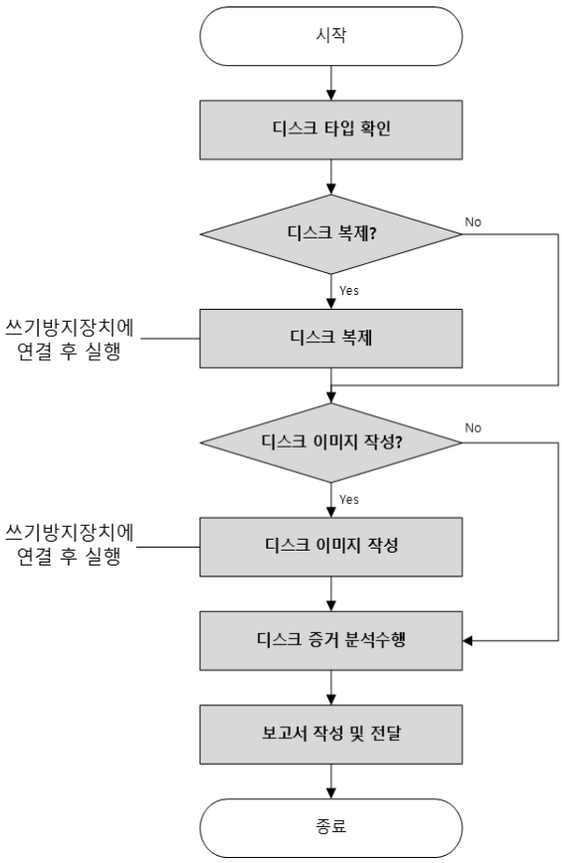

Fig. 1. TTA - Digital Evidence Acquisition Process

3.2 경찰청, 검찰청에서의 디지털 증거의 수집

경찰청에서는 디지털 증거를 수집[9]할 경우 경찰청 디지털포렌식센터장에게 지원을 요청할 수 있도록 되어있다. 디지털 데이터를 압수, 수색, 검증하고자 할 경우 준비 물품으로 디지털 증거분석 전용 노트북, 쓰기방지장치 및 하드디스크 복제장치, 복제용 하드디스크, 하드디스크 운반용 박스, 정전기 방지 장치 등 압수, 수색, 검증에 필요한 장비라고 설명하고 있다.

대검찰청에서도 디지털 증거의 압수, 수색[10]에 대하여 압수 대상자에 대한 파악 이후 정보저장매체만을 분리하여 압수하는 것을 원칙으로 하고 있고 부득이할 경우 전체를 압수하도록 하고 있다. 다만 정보처리시스템 자체를 압수하기 힘들 경우에는 사본을 생성하여 압수하도록 하고 있다. 이러한 과정을 진행하는 동안 쓰기방지장치를 사용하여 자료가 변경 또는 훼손되지 않도록 하여야 한다고 강조하고 있다.

3.3 현 디지털 증거 수집절차의 문제점 및 대응 방안

디지털 증거를 수집하였을 경우 쓰기방지장치를 이용하거나 하드웨어 기반의 이미징 장비를 이용하여 사본을 생성하는 것은 학계 혹은 현업에서도 이미 정론이다. 하지만 최근에 출시된 보안 USB 혹은 백신을 내장하고 있는 USB의 경우 Fig. 2와 같이 쓰기방지장치와 하드웨어 기반 이미징 장비에서는 인식하지 못하는 것을 확인하였다.

Fig. 2. WirteBlocker, Imaging Device

이러한 특수 USB의 경우 수사관의 PC를 이용하여 이미지 파일을 생성하는 방법 외에는 증거를 수집할 수 있는 방법이 존재하지 않는다. 패스워드를 파악하여 특수목적의 USB를 이미징 할 경우 해쉬값이 변경되는 경우를 확인하였다. Table 1은 네트워크 연결이 해제되어 있는 PC에서 패스워드 인증 이후 보안 USB를 이미징한 결과이다. 임의적인 작업 없이 이미징을 수행한 결과 해쉬값이 변경되는 것을 확인할 수 있다.

Table 1. Images of Specific USB Generated Hash Value Changes

	MD5		
	Test 1	Test 2	Test 3
SecuDrive	3953bcce33b050c0 bbd7c6cf1b90f3d3	888462a8121752d1 406da43ddeddebae	ede5158e84328582 794ccf8c3cbc9c11
SaferZone	765adbe9d7041e0 eb86f18faf3433aba	765adbe9d7041e0 eb86f18faf3433aba	765adbe9d7041e0 eb86f18faf3433aba
Turbo Vaccine	fb60fa73a034c06b d90ed87a492aedbf	b84956b46655fd40 bd4cce5f7963e121	cc67129123e8fa27 fed40cf9710504cb

따라서 하드웨어 이미징 장비 혹은 쓰기방지장치를 사용하지 않고 안전하게 이미징을 수행하기 위해서는 소프트웨어적인 대응책이 필요하다. 이동식 저장매체의 경우 내부 로직에 따라서 Windows OS에서는 이동식 드라이브 혹은 하드디스크 드라이버로 인식한다. 이동식 저장매체가 이동식 드라이브로 인식하는 경우 Windows에서 제공하는 WriteProtect 레지스트리키를 이용하여 쓰기방지장치를 연결한 것과 동일한 효과를 볼 수 있다. 만일 이동식 저장매체가 하드디스크 드라이브로 인식되는 경우 Windows 8 버전 이후로는 WriteProtect 레지스트리키를 사용하여도 쓰기방지 효과를 확인할 수 없다. 따라서 이러한 경우에는 Mount Volume Utility를 이용하여 논리적으로 드라이브를 마운트하지 않고 이미징 작업을 수행한다면 쓰기방지효과를 볼 수 있다[11].

4. 실험 및 결과

이동식 저장매체를 이미징할 경우, 하드웨어 기반 이미징 장비를 사용하는 것은 이미 정론화 되어있다. 하지만 본 실험에서는 보안 USB, 백신 USB 등의 특수 USB에 대해서도 하드웨어 기반의 이미징 장비가 사용 가능한지를 실험하고 Windows에서 제공하는 레지스트리키와 옵션을 변경[11]하여 이미징할 경우에도 무결성을 유지할 수 있는지에 대해 실험하였다.

실험에 사용한 보안 USB 및 백신 USB와 실험 환경은 Table 2와 같다.

Table 2. Secure USB, Test environment

OS	- Windows XP Professional Service Pack 2 - Windows 7 Home Premium
Device	- Forensic Falcon - Tableau TD3 - Tableau Forensic USB Bridge (Model T8-R2) - SecuDrive 4GB - SaferZone 8GB - TurboVaccine 8GB
Tools	- AccessData FTK Imager 3.1.1.8

실험 방법으로는 보안 USB로 사용한 Secu Drive[12], SaferZone[13]와 백신 기능을 내장하고 있는 USB인 TurboVaccine[14] 총 3 제품을 하드웨어 기반의 이미징장비와 쓰기방지장치를 이용하여 이미징을 수행한 뒤 해쉬값을 확인하고 수사관의 PC를 이용하여 이미징한 뒤 해쉬값을 통하여 무결성을 입증할 수 있는지에 대한 실험을 진행하였다. 실험 방법은 Fig. 3과 같다.

하드웨어 장비와 쓰기방지장치로 이미지 파일 생성을 시도한 결과 앞서 언급한 바와 같이 정상적인 이미지 파일 생성이 불가능한 것을 확인하였다. 보안 USB인 SecuDrive 제품과 SaferZ one 제품의 경우 Falcon을 통해서만 이동식 저장매체 인식이 가능하였다. 하지만 사용자 인증 과정을 거치기 전으로 보안영역은 접근이 불가능하였고 일반 영역에 대해서만 이미지 파일을 생성할 수 있었다. 백신 USB는 이동식 저장매체로 인식하지 못하였기 때문에 이미지 파일 생

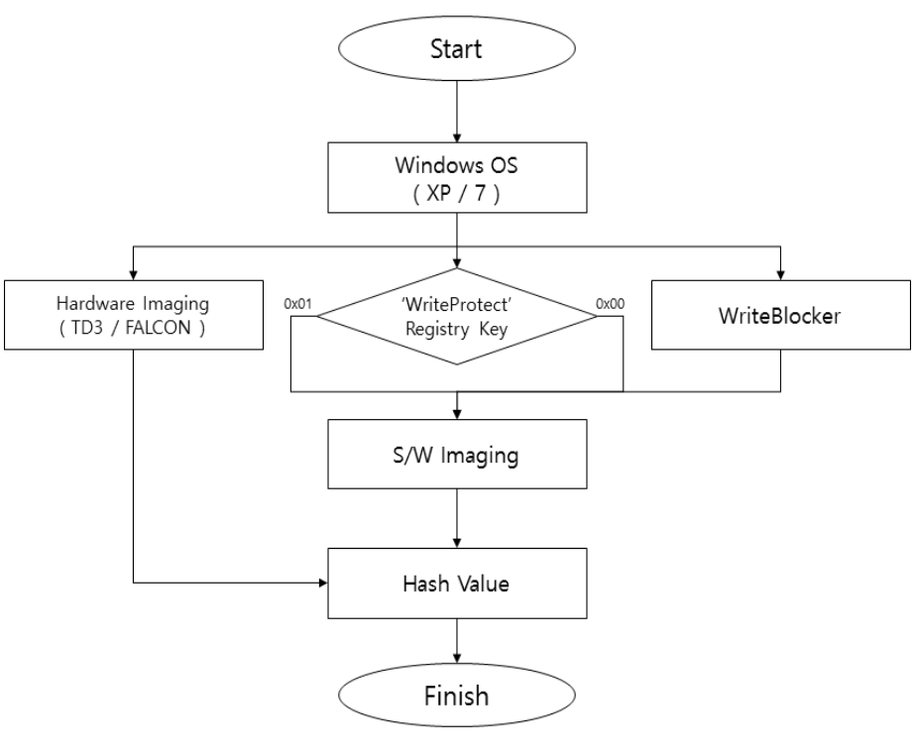

Fig. 3. Experiment Procedure

Table 3. Result of removable device with Hardware Device experiment

Device	HW	Hash (MD5)
SecuDrive	FALCON	add278a238985a8b440e55293f6aca5b (CD-ROM)
	TD3	No Supported
	WriteBlocker	No Supported
SaferZone	FALCON	a2c0fac213c16c329ed9c867bc1da332 (CD-ROM)
	TD3	No Supported
	WriteBlocker	No Supported
TurboVaccine	FALCON	No Supported
	TD3	No Supported
	WriteBlocker	No Supported

성이 불가능하였다. 또한 쓰기방지장치에서는 세 제품 모두 “USB Device, Not Supported”라는 문구와 함께 인식되지 않는 것을 확인하였다. Table 3은 하드웨어 기반 이미징 장비 및 쓰기방지장치를 이용하여 이미지 파일을 생성한 결과이다.

다음으로 Windows XP, 7 환경에서 Windows 레지스트리키를 변경한 경우 사용자 인증과정을 거쳐 소프트웨어를 이용하여 이미지파일을 생성한 경우에 대해서 실험을 진행하였다. 실험에 대한 결과는 Table 4와 같다. 실험의 결과와 같이 WriteProtect 레지스트리키를 사용하는 경우 생성된 이미지 파일의 해쉬값이 유지되는 것을 알 수 있으며 레지스트리키를 활성화하지 않을 경우 해쉬값이 변경되는 것을 알 수 있다. 따라서 쓰기방지장치 혹은 하드웨어 기반의 이미징 장비를 사용할 수 없는 경우 레지스트리키 설정을 통해서 수사관의 PC에서 생성하는 이미지 파일의 무결성을 유지할 수 있음을 확인하였다.

따라서 수사관이 보안 USB 혹은 백신 USB를 증거물로 획득하였을 경우 수사관의 PC에서 레지스트리키를 변경한 뒤 이미지파일 생성을 수행하여야만 한다.

Table 4. Secure, Vaccine USB Hash Value test result

OS	Device	WriteProtect	Certification	Hash (MD5)
Windows 7	SecuDrive	0x01	On	ede5158e84328582794ccf8c3cbc9c11
				ede5158e84328582794ccf8c3cbc9c11
	SaferZone	0x01	On	765adbe9d7041e0eb86f18faf3433aba
				765adbe9d7041e0eb86f18faf3433aba
	TurboVaccine	0x01	-	fb1da213582537baab06b58025b4be67
				fb1da213582537baab06b58025b4be67
Windows XP	SecuDrive	0x01	On	ede5158e84328582794ccf8c3cbc9c11
				ede5158e84328582794ccf8c3cbc9c11
	SaferZone	0x01	On	765adbe9d7041e0eb86f18faf3433aba
				765adbe9d7041e0eb86f18faf3433aba
	TurboVaccine	0x01	-	fb1da213582537baab06b58025b4be67
				fb1da213582537baab06b58025b4be67
Windows 7	SecuDrive	0x00	On	d8b28db4b0ab2fc6cc9e50ab7c833a2e
				62e0bcd82bcb6ed03019dd352b33663e
	SaferZone	0x00	On	765adbe9d7041e0eb86f18faf3433aba
				765adbe9d7041e0eb86f18faf3433aba
	TurboVaccine	0x00	-	ac698832f51bae910aca60057530e778
				ff38fa0494e05dd601d995d6578ee15b
Windows XP	SecuDrive	0x00	On	96dbad39733c76c53737c455ee290de8
				763b8990188a45b505f86fae0438feda
	SaferZone	0x00	On	765adbe9d7041e0eb86f18faf3433aba
				765adbe9d7041e0eb86f18faf3433aba
	TurboVaccine	0x00	-	63012ff745f9b3a5bf89f69dbc2c6e2d
				adf3152bb9a401a77c57260ecd947938

5. 이동식 저장매체에 대한 안전한 이미징 절차

이동식 저장매체에 대해서 하드웨어 기반의 이미징 장비나 쓰기방지장치를 이용하여 이미지 파일을 생성하는 것은 일반적인 방법이다. 하지만 위의 실험을 통해서 특수 USB의 경우 하드웨어 이미징 장비가 인식하지 못하는 것을 확인하였다. 또한, USB의 인증과정 이후 아무런 쓰기방지 대책 없이 이미징을 할 경우 이미지 파일에 대한 해쉬값이 계속 변경되는 것을 확인할 수 있었다. 이는 디지털 포렌식에서 무결성을 입증하지 못하는 상황으로 연결될 수 있고 수사 과정에서 증거물에 대한 입증으로 인해 더욱 많은 시간이 소요될 수 있으며 증거물로 인정받지 못할 수 있는 상황이 발생할 수 있다. 따라서 이동식 저장매체에 대한 안전한 증거 수집 절차로 Fig. 4와 같이 제안한다.

5.1 준비 단계

수사관은 디지털 증거 수집 PC에서 쓰기방지장치를 사용할 수 없는 상황에 대비하여 레지스트리 및 Mount Volume Utility의 변경을 위해 준비를 해두어야 한다. 보안 USB 등의 특수 USB 이외에도 현장에서 쓰기방지장치를 갑작스럽게 사용할 수 없는 경우가 발생할 수 있기 때문에 이에 대한 대비가 필요하다. 또한, PC에 생성한 USB를 저장할 수 있도록 충분한 용량 확보가 필요하다.

5.2 디스크 타입 확인

수사관은 현장에서 이동식 저장매체를 디지털 증거로 획득하였을 경우 해당 저장장치에 대한 식별이 필요하다. 획득한 이동식 저장매체에 대한 종류 및 특징에 따라서 필요한 정보 및 기법을 사전에 숙지해야 한다.

수사관은 확인된 디스크 타입에 따라서 디스크 복제 혹은 이미징을 하기 이전에 쓰기방지장치 연결 혹은 레지스트리키 수정 및 Mount Volume Utility를 변경하여 사전에 준비하여야 한다.

5.3 디스크 복제/이미징

수사관은 디지털 증거물의 복제/이미징 여부를결정하고 복제/이미징하여 분석하고자 할 경우 디스크 타입에 따라서 쓰기방지장치 연결 혹은 쓰기방지 대책 마련을 해두어야 한다. 일반 이동식 저장매체일 경우 쓰기방지장치에 연결하여 복제/이미징을 진행하고, 쓰기방지장치를 사용할 수 없을 경우 레지스트리키 변경 및 Mount Volume Utility에서 자동 마운트 옵션을 해제한 뒤에 수사관의 PC에 이동식 저장매체를 연결한다. 포렌식 도구를 이용하여 복제본/이미지 파일을 생성한 뒤 원본 디지털 증거물과의 동일성 및 무결성 입증을 위해 원본 및 생성본의 각 해쉬값을 수집, 비교한다. 마지막으로 비교한 해쉬값을 기록하고 입회인의 서명 날인을 받는다.

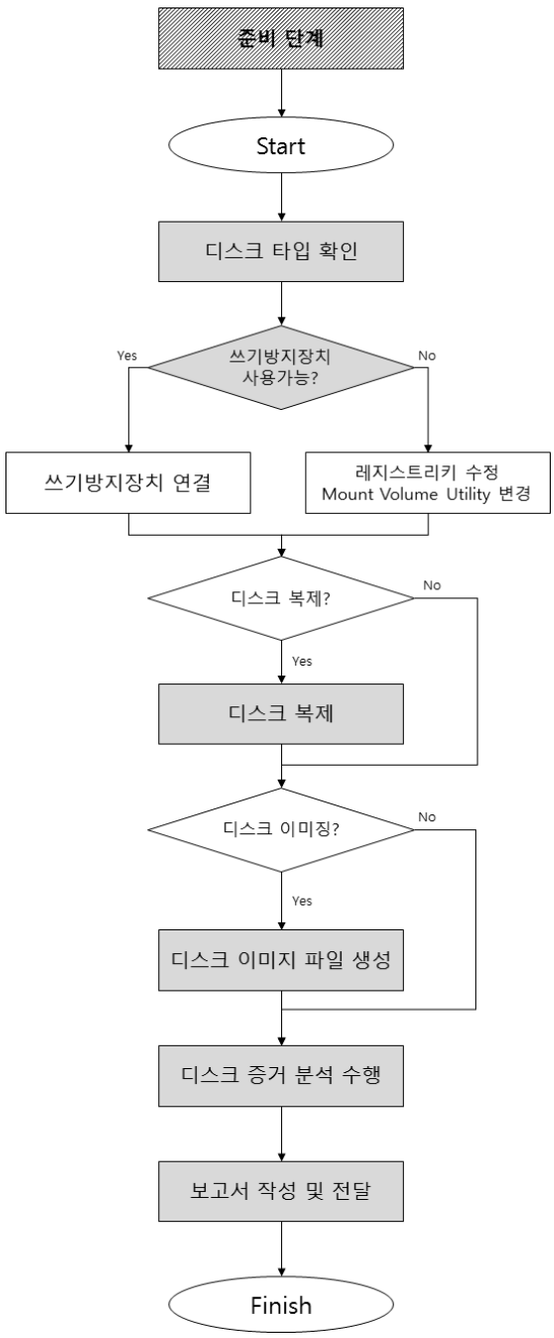

Fig. 4. Effective Imaging Method of Removable Storage Device

5.4 디지털 증거 분석 및 보고서 작성

수사관이 현장에서 초등 분석이 가능할 경우 디지털 증거에 대해서 분석을 진행한다. 디지털 증거 분석은 복제본 혹은 이미지 파일을 이용하여 분석을 진행하되 여의치 않을 경우 분석실에서 분석을 진행하도록 한다.

분석 완료 후 분석 결과 및 전반적인 절차와 정보를 기술한 보고서를 작성한다. 보고서는 사건 담당자에게 상세 설명 후 증거물과 함께 전달한다.

6. 결 론

본 논문은 이동식 저장매체를 이미징하는데 있어서 쓰기방지장치 혹은 하드웨어 기반의 이미징 장비를 사용하는 것에 대하여 개선된 절차를 제시하고 있다. 디지털 증거의 수집 절차는 향후 분석에 대해 법정에서 디지털 증거에 대한 효력을 인정받기 위한 중요한 절차 중 하나이다. 실제로 여러 판례들에서 적법하지 못한 수집 절차 혹은 수집한 디지털 증거에 대하여 무결성을 입증하지 못하여 증거로 인정되지 않는 사례가 발생하고 있다. 따라서 각각의 디지털 증거에 맞는 적절한 증거 수집 절차가 필요하다.

보안 USB, 백신 USB와 같은 특수 USB의 경우 앞의 실험 결과와 같이 쓰기방지장치로는 인식이 되지 않으며, 쓰기방지 대책 없이 이미징할 경우 해쉬값이 변경되기 때문에 적법한 과정을 거쳐서 증거물을 획득하였더라도 증거로 인정받지 못하는 경우가 발생할 수 있다. 따라서 본 논문에서 제시하는 절차와 같이 이동식 저장매체에 대한 증거 수집 절차가 추가적으로 명시되어야 하며 수사관들은 이를 인지하고 현장에 적용할 수 있어야 한다.

향후 계획으로는 SSD(Solid State Disk)와 같이 Garbage Collection이나 Trim기능을 가지고 있는 저장매체에 대해서 안전하게 이미징할 수 있는 방법에 대해서 연구하고, 국내의 다른 보안 솔루션이 적용된 제품이나 외국의 보안 USB에 대해서도 적용이 가능한 안전한 이미징 절차에 대해서 연구하고자 한다.

References

[1] Lee, Sun-Ho and Im-Yeong Lee, "A study on security solution for USB flash drive," *Journal of Korea Multimed ia Society,* Vol.13, No.1, pp.93-101, 2010.

[2] "Computer Forensics Guideline," *Telecommunications Technology, Association*, 2007. 12. 26.

[3] Hye-Won Lee, Chang-Wook Park, Guen-Gi Lee, Kwon-YoupKim, and Sang-Jin Lee, "Secure USB Analysis in Forensic perspective," *The Korea Society of Broadcast Engineers Conference*, pp.63-65, 2008.

[4] "Removable Storage Device Security Manage ment Guidelines," National Intelligence Service, 2007.

[5] Sung-Min Jang, Jung-Heum Park, Chan-Ung Pak, and Sang-Jin Lee, "The Research for Digital Evidence Acquisition Procedure within a Full Disk Encryption Environment," *Journal of The Korea Institute of Information Security & Cryptology*, Vol.25, No.1, 2015.

[6] Keun-Gi Lee, Hye-Won Lee, Chang-Wook Park, Je-Wan Bang, Kwon-youp Kim, and Sangjin Lee, "USBPassOn: Secure USB Thumb Drive Forensic Toolkit," *2008 Second International Conference on Future Generation Communication and Networking*, Vol.2, IEEE 2008.

[7] C. Hargreaves and H. Chivers, "Recovery of Encryption Keys from Memory Using a Linear Scan," *The Third International Conference on Availability Reliability and Security*, pp. 1369-1376, Mar., 2008.

[8] Minho Kim, Hyunuk Hwang, Kibom Kim, Taejoo Chang, Minsu Kim, and Bongnam Noh, "Vulnerability Analysis Method of Software-based Secure USB," *Journal of The Korea Institute of Information Security & Cryptology,* Vol.22, No.6, pp.1345-1354, 2012.

[9] "Rules relating to the collection and processing of digital evidence," National Police Agency, Directive, No.766, 2015.05.22.

[10] "Study on the procedures and facilities for maintaining the integrity of digital evidence," Supreme Prosecutor's Office, 2006. 06.

[11] "Digital Forensics: How to configure Windows Investigative Workstations," S*ANS Digital Forensics and Incident Response Blog*, 2010. 12.

[12] SecuDrive [Internet], http://www.secudrive.co.kr/.

[13] SaferZone [Internet], http://www.saferzone.com/saferzone/sub01_02_ 01.asp.

[14] TurboVaccine [Internet], http://www.turbovaccine.com/sub/usb_otg2.asp.

백 현 우

e-mail : hyunwoob.24@gmail.com

2015년 경희대학교 전자전파공학과(공학사)

2015년~현 재 고려대학교 정보보호대학원 정보보호학과 석사과정

관심분야 : Digital Forensic, Reverse Engineering

전 상 준

e-mail : heros86@korea.ac.kr

2010년 고려대학교 산업시스템정보공학과(학사)

2010년~2013년 고려대학교 정보보호대학원 정보보호학과(박사수료)

2013년~2014년 ㈜안랩 A-First 연구원

2014년~2016년 고려대학교 정보보호대학원 디지털포렌식연구센터(강사 및 연구원)

2016년~현 재 프리랜서

관심분야 : Reverse Engineering, Digital Forensic

이 상 진

e-mail : sangjin@korea.ac.kr
1987년 고려대학교 수학과(학사)
1989년 고려대학교 수학과(석사)
1994년 고려대학교 수학과(박사)
1989년~1999년 ETRI 선임연구원
1999년~현 재 고려대학교 정보보호대학원 교수
2008년~현 재 고려대학교 디지털포렌식연구센터 센터장
관심분야 : Digital Forensic, Steganography, Hash Function