DOI: 10.3745/KIPSTC.2010.17C.2.159

완전삭제 도구 사용 흔적에 관한 연구

김 연 수[†] · 방 제 완[††] · 김 진 국[†] · 이 상 진[†††]

요 약

완전삭제 기술은 저장장치 내 데이터를 복구가 불가능하도록 흔적 없이 완벽하게 삭제하는 기술이다. 최근 개인정보 유출 사고가 급증함에 따라 저장된 데이터의 관리가 중요해지고 있다. 특히 개인정보가 포함된 데이터를 폐기해야 하는 경우, 데이터를 영구적으로 삭제하는 완전삭제 도구를 사용함으로써 개인정보에 대한 불필요한 유출을 막을 수 있다. 또한 완전삭제 기술은 데이터 보안 및 프라이버시 보호 측면으로 활용 가능하다. 그러나 완전삭제 기술은 의도적으로 사건과 관련된 증거를 인멸하기 위해 사용될 수도 있다. 이러한 의도적인 증거 인멸은 사건 수사에 있어서 중요한 실마리가 될 수 있다. 본 논문에서는 디지털 포렌식 수사 과정에서 완전삭제 도구의 사용 흔적을 확인할 수 있는 방안을 제시한다.

키워드 : 디지털 포렌식, 완전삭제, 데이터 복구

A Study of Trace for Data Wiping Tools

Yeonsoo Kim[†] · Jewan Bang[††] · Jinkook Kim[†] · Sangjin Lee[†††]

ABSTRACT

The data wiping is a technique which perfectly deletes data in a storage to prevent data recovery. Currently, management of stored data is important because of increasing an accident of personal information leakage. Especially, if you need to discard data contained personal information, using a wiping tool which permanently deletes data to prevent unnecessary personal information leakage. The data wiping is also used for data security and privacy protection. However the data wiping can be used intentionally destruction of evidence. This intentionally destruction of evidence is important clues of forensic investigation. This paper demonstrates the methods for detecting the usage of wiping tools in digital forensic investigation.

Keywords : Forensic Investigation, Data Wiping, Data Recovery

1. 서 론

최근 정보보호에 대한 사회적인 관심이 높아지면서 개인, 기업, 단체의 기밀정보에 대한 관리가 중요해지고 있다. 일반적으로 이러한 기밀정보는 하드디스크, USB와 같은 저장매체에 저장되어 관리된다. 저장매체는 저장된 정보를 효과적으로 관리하기 위해 운영체제별로 고유한 파일시스템을 사용하게 된다. 하지만 운영체제에서 지원하는 데이터 삭제 기능을 사용하여 데이터를 삭제할 경우 파일시스템의 특성을 이용하여 쉽게 복구할 수 있다. 따라서 최근 저장매체에 저장된 기밀정보를 완벽하게 삭제하기 위한 완전삭제 기술이 많이 활용되고 있다.

완전삭제 기술은 크게 하드웨어 측면과 소프트웨어 측면으로 나눌 수 있다. 전자는 저장매체에 강력한 자기장을 가하여 손상시키거나 전기적인 방식을 통하여 물리적인 손상을 일으키는 것을 의미한다[1]. 이 경우에는 저장매체의 재사용이 불가능하기 때문에 저장매체를 폐기할 때 주로 이용된다. 후자는 저장매체의 물리적인 손상 없이 논리적으로 삭제하는 방법으로 데이터가 저장된 저장매체의 영역을 반복적으로 덮어씀으로써 데이터를 복구할 수 없도록 만든다[2].

현재 소프트웨어적인 완전삭제 방법은 완전삭제 도구로 구현되어 활용되고 있다. 완전삭제 기술을 사용한다면 개인정보를 보호하고, 기밀 자료의 노출을 방지할 수 있다. 하지만 이러한 기술을 악용하여 사건과 관련된 증거를 은폐하기 위해 사용될 수도 있기 때문에 수사에 많은 어려움이 생기게 된다. 완전삭제 도구를 의도적으로 사용한 흔적을 발견할 경우 사건을 해결하는데 중요한 실마리가 될 수 있기 때문에 본 논문에서는 완전삭제 기술을 사용하는 23개 도구

※ 본 연구는 한국과학재단을 통해 교육과학기술부의 바이오연구개발사업으로부터 지원받아 수행되었습니다. (M10640030004-08N4003-00410)
† 준 회 원 : 고려대학교 정보경영공학전문대학원 석사과정
†† 준 회 원 : 고려대학교 정보경영공학전문대학원 석박사통합과정
††† 종신회원 : 고려대학교 정보경영공학전문대학원 교수
논문접수 : 2009년 9월 23일
수 정 일 : 1차 2009년 12월 3일
심사완료 : 2009년 12월 3일

중 우수한 것으로 판단되는 6개의 도구를 대상으로 사용 흔적을 조사하였다.

2. 관련 연구

초기의 데이터 완전삭제는 저장매체에 저장된 파일의 데이터 영역을 '0x00'으로 초기화하거나 임의의 값으로 데이터를 덮어씌우는 방식이었다[3]. 그러나 이와 같은 완전삭제 방법은 물리학적인 방법으로 복구가 가능하다는 것을 Peter Gutmann(1996)이 증명하였으며, 그는 이러한 복구를 방지할 수 있는 안전한 완전삭제 알고리즘을 소개하였다[4]. 각 나라의 주요 기관에서도 안전하게 데이터를 삭제하기 위한 완전삭제 알고리즘을 개발하고 있다. 대표적으로 미국 국방성에서 배포한 U.S. Department of Defense(DoD) 5220.22-M(1995)[5]이 있으며, 이 알고리즘은 현재까지도 대부분의 완전삭제 도구에서 기본적으로 제공하고 있다.

데이터 완전삭제 도구와 관련된 연구로는 Simon Innes (2005)[6]와 Matthew Geiger(2005)[7]의 연구가 있다. Simon Innes는 인터넷 익스플로러 사용 시 생성되는 파일 및 레지스트리 키 값을 삭제하는 3개의 완전삭제 도구를 대상으로 성능을 비교, 조사하였다. Matthew Geiger는 총 6개 완전삭제 도구를 대상으로 파일 완전삭제 시 데이터 영역에 고유하게 남아있는 패턴과 별도로 생성된 파일만을 정리하였다.

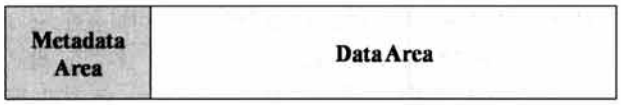
본 논문에서는 기존에 발표된 완전삭제 도구 연구결과에서 더 나아가 메타 영역의 완전삭제 여부 및 생성된 Prefetch 파일, 레지스트리 키 값을 조사하였다.

3. 완전삭제 도구

소프트웨어적인 완전삭제 방법을 수행하는 완전삭제 도구는 제공하는 기능과 실행 환경에 따라 다양하게 존재한다. 본 논문에서는 윈도우 환경에서의 FAT 파일시스템과 NTFS에서 실행이 가능한 완전삭제 도구를 대상으로 조사하였다.

3.1 완전삭제 도구 조사 및 검증

대부분의 파일시스템에서는 파일을 효율적으로 관리하기 위해 (그림 1)과 같이 메타 영역과 데이터 영역으로 나누어 관리한다. 메타 영역에는 파일 메타 정보인 파일의 이름, 시간 정보, 크기, 삭제 플래그 등의 정보가 저장된다. 이러한 메타 정보는 FAT 파일시스템의 디렉터리 엔트리, NTFS의 MFT 엔트리라는 구조로 관리되고, 데이터 영역에는 실제 파일 데이터가 저장된다[8].



(그림 1) 추상화한 파일시스템

〈표 1〉 완전삭제 검증 기준

번호	검증 항목
1	메타 영역에서 파일의 정보를 복구할 수 없는가?
2	데이터 영역에서 파일데이터를 복구할 수 없는가?

〈표 2〉 상위 6개 완전삭제 도구 목록

도구명	버전	제조사	기타
DataEraser[9]	2.0	HAURI, Inc.	상용
East-Tec Eraser[10]	2008(8.9)	EAST Technologies	상용
Eraser[11]	5.86.1	Heidi Computers Ltd.	프리웨어
FINALeRASER[12]	4.0.6.0220	FINALDATA	상용
QuickClean[13]	6.01.0003	McAfee, Inc.	상용
SecureClean[14]	4.0	WhiteCanyon, Inc.	상용

운영체제에서 지원하는 파일 삭제 기능을 사용하여 파일을 삭제할 경우, 메타 영역의 삭제 플래그 값을 변경하여 파일이 삭제된 것처럼 인식하게 만든다. 이 경우 메타 영역의 파일 메타 정보와 데이터 영역의 실제 파일 데이터는 그대로 남아있기 때문에 비교적 쉽게 파일을 복구할 수 있다. 이러한 이유로 복구가 불가능하게 삭제해야 하는 파일들은 완전삭제도구라고 알려진 별도의 소프트웨어를 이용한다. <표 1>은 앞서 살펴본 파일시스템의 특징을 기반으로 완전삭제도구가 갖추어야 할 검증기준을 나타낸 것이다.

현재 많이 사용되고 있는 23개의 완전삭제 도구(상용 소프트웨어 19개, 프리웨어 4개)를 대상으로 위의 검증 기준을 적용해본 결과, 모든 검증 기준을 만족하는 도구는 단 6개였다. 하나의 검증 기준만을 만족하는 17개 도구의 경우, 메타 영역을 완전삭제하지 못해 파일의 메타정보인 파일 이름, 시간정보, 크기 등이 확인 가능했다. <표 2>는 모든 검증 기준을 만족하는 6개의 완전삭제 도구 목록이다.

3.2 완전삭제 도구 사용 여부 판별 기준

본 절에서는 앞서 조사한 23개의 완전삭제 도구를 대상으로 도구의 사용 여부를 판별할 수 있는 기준을 살펴본다.

메타 영역을 완전삭제하는 도구의 경우, '0x00'으로 초기화하거나 별도의 파일을 생성하여 생성한 파일의 메타 정보를 덮어쓰는 방식으로 삭제한다. 그리고 대부분의 완전삭제 도구는 데이터 영역을 완전삭제하기 위해 '0x00'으로 초기화하거나 임의의 값으로 채우는 방법을 이용한다.

메타 영역과 데이터 영역 이외에도 윈도우 환경에서 완전삭제 도구를 사용할 경우 Prefetch 파일, 프로그램 폴더, 레지스트리 키와 같이 시스템 내 다양한 흔적이 남게 된다.

Prefetch 파일은 소프트웨어의 성능 향상을 위해 소프트웨어 구동에 필요한 데이터를 미리 메모리에 올리기 위해 사용한다[15, 16]. 이 파일은 윈도우 XP 이상의 환경에서 소프트웨어를 실행하면 기본 윈도우 설치폴더인 %SYSTEMROOT%\Prefetch\ 폴더 내에 생성된다. Prefetch 파일에는 소프트웨어의 최종 실행시간 및 총 실행 횟수, 참조하는 라이브러리 정보 등이 저장되어 있다[17]. 소프트웨어를 설치하거나 제거할 경우에

〈표 3〉 완전삭제 도구 사용 여부 판별 기준

번호	확인항목
1	파일시스템에서의 메타 영역 흔적
2	파일시스템에서의 데이터 영역 흔적
3	도구 설치 및 제거, 실행 시 생성된 Prefetch 파일 흔적
4	도구 설치 시 생성된 프로그램 폴더 흔적
5	레지스트리 키 등록 흔적

도 Prefetch 파일이 생성되기 때문에 이를 통해 완전삭제 도구의 사용 시도를 판별하는 것이 가능하다.

프로그램 폴더는 소프트웨어 설치 시 기본 경로인 %PROGRAMFILES% 혹은 사용자가 선택한 경로에 생성되며, 이 폴더에는 소프트웨어를 실행하기 위해 필요한 파일이 저장된다. 프로그램 폴더의 존재 여부로 현재 조사 중인 시스템에 완전삭제 도구가 설치되어 있는지 확인할 수 있다.

레지스트리는 설치된 소프트웨어의 설정 값을 저장하는 데이터베이스로[18], 소프트웨어를 설치하면 파일, 폴더 생성뿐만 아니라 관련 레지스트리 키 값이 등록된다. 프로그램을 제거하게 되면 관련 파일은 대부분 삭제하나 레지스트리 키는 일부 남아있는 경우가 발생한다[19]. 특히 이러한 레지스트리 키는 도구명 혹은 제조사명으로 등록되기 때문에 특정 도구의 설치여부를 알 수 있다.

위에서 언급한 완전삭제 도구의 사용 여부를 판별할 수 있는 기준을 정리하면 <표 3>과 같다. 이는 시스템에서 완전삭제 도구를 사용하기 위한 시도가 있었는지 짐작해볼 수 있는 흔적들로 확인해야 할 항목은 총 5개이다.

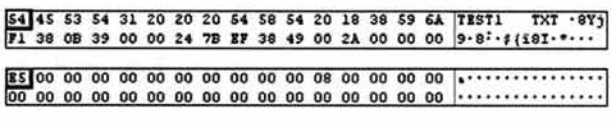
4. 완전삭제 도구 사용 흔적 확인

앞서 살펴본 완전삭제 도구의 사용 여부를 판별하기 위한 기준은 총 5가지로 메타 영역, 데이터 영역, Prefetch 파일, 프로그램 폴더, 레지스트리이다. 이 기준에 따라 상위 6개 도구의 설치 및 제거, 실행 후 어떠한 흔적이 남는지 확인한 결과는 다음과 같다.

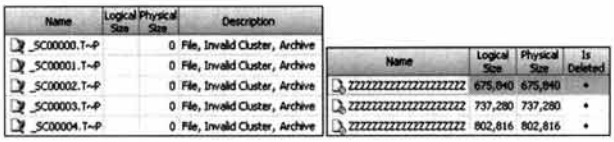
4.1 메타 영역 흔적

FAT 파일시스템과 NTFS에서는 파일을 관리하는 방식에 차이가 있기 때문에 메타 영역의 흔적 또한 다르게 남는다. 따라서 각 파일시스템 별로 완전삭제 도구를 이용하여 파일을 삭제한 뒤, 메타 영역을 확인해야 한다. 6개의 완전삭제 도구가 메타 영역을 삭제한 흔적은 크게 세 가지로 나누어볼 수 있다.

*DataEraser 2.0, FINALeRASER4.0.6.0220*을 사용했을 경우, FAT 파일시스템에서는 디렉터리 엔트리의 삭제 Flag와 속성 항목만 각각 '0xE5', '0x08'로 설정하고 나머지를 '0x00'으로 채운다. NTFS에서는 MFT 엔트리를 모두 '0x00'으로 변경한다.



(그림 2) DataEraser-파일 완전삭제 실행 전후 디렉터리 엔트리 비교



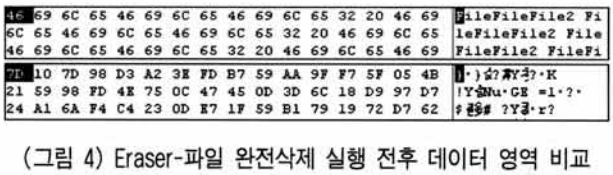
(그림 3) SecureClean-파일 완전삭제 실행 후 흔적 확인

*Eraser 5.86.1, QuickClean6.01.0003*은 원래의 파일명과 확장자를 일정한 패턴이 존재하지 않는 임의의 문자로 변경하는데, 이 때 그 길이는 그대로 유지한다. 이러한 결과는 FAT 파일시스템뿐만 아니라 NTFS에서도 동일하다.

*East-Tec Eraser 2008(8.9), SecureClean 4.0*은 특정 패턴을 이용하여 삭제한 파일의 이름과 확장자를 덮어씌우는 방식이다. East-Tec Eraser의 경우 FAT 파일시스템에서는 임의의 문자를 이용하는 반면, NTFS에서는 확장자를 항상 'wip'로 변경한다. SecureClean의 경우 FAT 파일시스템에서는 '_SC*****.T~P' 형태의 패턴을 이용하는데, *로 표시한 부분은 0부터 순차적으로 증가하는 숫자를 의미한다. 그러나 NTFS에서는 알파벳 'Z' 문자를 이용하여 덮어씌운다.

4.2 데이터 영역 흔적

6개의 완전삭제 도구 모두 '0x00'로 초기화하거나 사용자가 선택한 완전삭제 알고리즘에 따라 임의의 값으로 데이터 영역을 덮어씌웠다. 이때 사용한 도구를 판별할 수 있는 별도의 패턴은 사용하지 않는다.



(그림 4) Eraser-파일 완전삭제 실행 전후 데이터 영역 비교

4.3 생성된 Prefetch 파일 흔적

대부분의 완전삭제 도구는 설치 후 사용이 가능하다. 프로그램을 설치하거나 제거하는 것은 실행파일을 통해 수행하기 때문에 Prefetch 파일이 생성된다. 이러한 Prefetch 파일을 통해 완전삭제 도구를 사용하기 위한 시도가 있었는지 판별할 수 있다. <표 4>는 도구 설치 및 제거 시 생성된 Prefetch 파일 흔적을 조사한 결과이다.

만약 시스템 내에서 완전삭제 도구가 설치되었던 흔적이 발견되더라도 용의자는 실제 도구를 실행한 적이 없다고 주장할 수 있다. 따라서 도구를 실행한 이력이 기록되어있는 Prefetch 파일이 남아있는지 확인해 보아야 한다. 특히 Prefetch 파일에는 마지막으로 프로그램을 실행한 시간정보와 총 실행 횟수가 포함되어 있기 때문에 유심히 살펴보아야 하는 항목이다. <표 5>는 도구를 실행했을 때 생성되는 Prefetch 파일을 조사한 결과이다.

〈표 4〉 도구 설치 및 제거 시 생성된 Prefetch 파일 흔적

도구명	구분	도구 설치 및 제거 흔적
DataEraser 2.0	설치	%SYSTEMROOT%\Prefetch\HAURI_VRDE_2[1].0.5.4B_REL.EX-[HASH].pf
	제거	%SYSTEMROOT%\Prefetch\SET11.TMP-[HASH].pf
East-Tec Eraser 2008(8.9)	설치	%SYSTEMROOT%\Prefetch\ETERASER_LICENSED.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\ETERASER_LICENSED.TMP-[HASH].pf
		%SYSTEMROOT%\Prefetch\ETRISKMON.EXE-[HASH].pf
	제거	%SYSTEMROOT%\Prefetch\UNINS000.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch_IU14D2N.TMP-[HASH].pf
Eraser 5.86.1	설치	%SYSTEMROOT%\Prefetch\ERASERSETUP32.EXE-[HASH].pf
	제거	
FINALeRASER 4.0.6.0220	설치	%SYSTEMROOT%\Prefetch\WPMDEMO.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\SETUP.EXE-[HASH].pf
	제거	%SYSTEMROOT%\Prefetch\SETC.TMP-[HASH].pf
		%SYSTEMROOT%\Prefetch\FDSCHEDULE.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\WPM.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\FDWIPEFILE.EXE-[HASH].pf
QuickClean 6.01.0003	설치	%SYSTEMROOT%\Prefetch\EULA.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MCAGENT.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MCAPPINS.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MCDETECT.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MCINFO.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MCREGWIZ.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MCTSKSHD.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MCUPDATE.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MCUPDMGR.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MGHTML.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\MQCH_6011_ENGB.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\SETUP.EXE-[HASH].pf
	제거	%SYSTEMROOT%\Prefetch\PLGUNI.EXE-[HASH].pf
SecureClean 4.0	설치	%SYSTEMROOT%\Prefetch\SECURECLEAN.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\SCWATCH4.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\SCTRAY4.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\SCWELCOME.EXE-[HASH].pf
	제거	%SYSTEMROOT%\Prefetch\SCUNINSTALL4.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\UNINSTALL.EXE-[HASH].pf

〈표 5〉 도구 실행 시 생성된 Prefetch 파일 흔적

도구명	도구 실행 흔적	
DataEraser 2.0	%SYSTEMROOT%\Prefetch\DATAERASER.EXE-[HASH].pf	
	%SYSTEMROOT%\Prefetch\DATAMON.EXE-[HASH].pf	
East-Tec Eraser 2008(8.9)	%SYSTEMROOT%\Prefetch\ETERASER.EXE-[HASH].pf	
	%SYSTEMROOT%\Prefetch\ETSECUREERASE.EXE-[HASH].pf	
Eraser 5.86.1	%SYSTEMROOT%\Prefetch\ERASER.EXE-[HASH].pf	
FINALeRASER 4.0.6.0220	%SYSTEMROOT%\Prefetch\WPM.EXE-[HASH].pf	
	File Wiping	%SYSTEMROOT%\Prefetch\FDWIPEFILE.EXE-[HASH].pf
	Free Space Wiping	%SYSTEMROOT%\Prefetch\FDWIPEFREESPACE.EXE-[HASH].pf
QuickClean 6.01.0003	%SYSTEMROOT%\Prefetch\UNI.EXE-[HASH].pf	
	%SYSTEMROOT%\Prefetch\QCLEAN.EXE-[HASH].pf	
	%SYSTEMROOT%\Prefetch\SHRED32.EXE-[HASH].pf	
SecureClean 4.0	Clean My Computer	%SYSTEMROOT%\Prefetch\SCLAUNCHER4.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\SCBASE4.EXE-[HASH].pf
	SecureClean File Zapper	%SYSTEMROOT%\Prefetch\SCDRAGDROP4.EXE-[HASH].pf
		%SYSTEMROOT%\Prefetch\SCZAP4.EXE-[HASH].pf

4.4 생성된 프로그램 폴더 흔적

프로그램을 설치하면 기본적으로 실행에 필요한 파일을 지정한 경로 하위에 새로운 폴더를 생성하여 저장한다. 이때 폴더는 '\프로그램명' 혹은 '\제조사명\프로그램명' 형태로 생성된다. 프로그램 폴더는 대부분 프로그램 제거 과정에서 삭제되지만 일부 프로그램의 경우, 폴더 내 파일만 삭제한다. 따라서 프로그램 설치 시 기본 경로로 지정된 %PROGRAMFILES%의 하위 폴더를 살펴보거나 완전삭제

〈표 6〉 도구 설치 시 생성된 프로그램 폴더 흔적

도구명	프로그램 폴더 흔적
DataEraser 2.0	{사용자 지정 경로}\ViRobot DataEraser 2.0
East-Tec Eraser 2008(8.9)	{사용자 지정 경로}\East-Tec Eraser 2008
Eraser 5.86.1	{사용자 지정 경로}\Eraser
FINALeRASER 4.0.6.0220	{사용자 지정 경로}\FinalData\WPM Demo
QuickClean 6.01.0003	{사용자 지정 경로}\McAfee.com\Shared
SecureClean 4.0	{사용자 지정 경로}\WhiteCanyon\SecureClean 4

도구 이름, 제조사명 등 특정 키워드를 검색하는 방법으로 확인할 수 있다. <표 6>은 각 도구가 설치될 때 생성된 프로그램 폴더 목록이다.

4.5 레지스트리 흔적

윈도우 환경에서는 사용자의 다양한 행위 흔적과 설정정보를 효과적으로 관리하기 위해 레지스트리를 사용하며, 소프트웨어 설치 시 관련 레지스트리 키를 등록하여 관리한다[19]. 레지스트리 키에는 설치된 소프트웨어의 실행과 관련된 환경설정 정보가 저장되어 있다.

<표 7>은 6개 도구를 설치하는 과정에서 등록된 레지스트리 키 중 도구 제거 후에도 남아있는 항목을 확인한 결과이다.

5. 결론 및 향후 연구 방향

완전삭제 도구는 저장장치 내 기록된 데이터를 완벽하게 삭제하기 위한 기능을 제공한다. 이는 데이터 폐기 시 개인정보 및 기밀정보 유출을 방지하고자 할 경우 유용하게 사용될 수 있다. 하지만 다른 측면에서 사건과 관련된 증거 데이터를 은폐하기 위한 목적으로 악용될 가능성이 있다. 이러한 경우 용의자의 시스템 내에 데이터 완전삭제를 의심할 수 있는 흔적이 남아있는지 확인해야 한다.

대부분의 완전삭제 도구는 그 동작 여부를 판단할 수 있는 고유한 흔적을 남긴다. 이에 본 논문에서는 총 23개의 완전삭제 도구를 대상으로 완전삭제 검증 기준을 적용하여 모든 검증 기준을 만족하는 상위 6개 도구를 선별하였다. 그리고 선별된 도구 6개의 완전삭제 기능을 완전삭제 도구 사용 여부 판별 기준에 따라 확인하였다. 그 결과 각 도구의 설치 및 제거, 실행 과정에서 생성된 Prefetch 파일과 등

〈표 7〉 레지스트리 등록 흔적

도구명	레지스트리 키
DataEraser 2.0	HKU\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\ViRobot Data Eraser 2.0
	HKU\{SID}\Software\Microsoft\Windows\ShellNoRoam\MUICache - {User defined path}\ViRobot DataEraser 2.0\{DataEraser.exe, DataMon.exe}
	HKU\{SID}\Software\ViRobot DataEraser20\{CleanWnd, DriveWnd, FileWnd, MainWnd, SearchWnd}
East-Tec Eraser 2008(8.9)	HKLM\SOFTWARE\EAST Technologies
	HKLM\SOFTWARE\EAST_Technologies\East-Tec_Eraser
	HKU\{SID}\Software\EAST Technologies
	HKU\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\East-Tec Eraser 2008
	HKU\{SID}\Software\Microsoft\Windows\ShellNoRoam\MUICache - {User defined path}\East-Tec Eraser 2008\unins000.exe
Eraser 5.86.1	HKU\.DEFAULT\Software\Heidi Computers Ltd\Eraser
	HKU\{SID}\Software\Heidi Computers Ltd\Eraser
	HKU\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\Eraser
	HKU\{SID}\Software\Microsoft\Windows\ShellNoRoam\MUICache - %ALLUSERSPROFILE%\Local Settings\Temp\mia10.tmp\EraserSetup32.exe - %ALLUSERSPROFILE%\Application Data\{SID}\EraserSetup32.exe - {User defined path}\Eraser\{Eraser.exe, ErsChk.exe}
FINALeRASER 4.0.6.0220	HKU\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\WPM Demo
	HKU\{SID}\Software\Microsoft\Windows\ShellNoRoam\MUICache - {User defined path}\FinalData\WPM Demo\{FdWipeEmail.exe, FdWipeFile.exe, FdWipeFreeSpace.exe, wpm.exe}
QuickClean 6.01.0003	HKCR\{.q1a, .q1b, .qb6, .u4a, .u4b, .uar, .ub6, .UDL, .uff}
	HKCR\CLSID\{GUID}\InProcServer32
	HKCR\{QuickClean.Archive, QuickClean.Backup}
	HKLM\SOFTWARE\Classes\{.q1a, .q1b, .qb6, .u4a, .u4b, .uar, .ub6, .UDL, .uff}
	HKLM\SOFTWARE\Classes\CLSID{GUID}\InProcServer32
	HKLM\SOFTWARE\Classes\{QuickClean.Archive, QuickClean.Backup}
	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\QuickClean files
	HKU\{SID}\Software\Microsoft\Windows\ShellNoRoam\MUICache - {User defined path}\McAfee\McAfee QuickClean\{Plguni.exe, Uni.exe}
SecureClean 4.0	HKEY_CLASSES_ROOT\CLSID\{SID}\Shell\SecureClean Recycle Bin
	HKU\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\WhiteCanyon\SecureClean 4
	HKU\{SID}\Software\Microsoft\Windows\ShellNoRoam\MUICache - %ALLUSERSPROFILE%\Local Settings\Temp\uninstall.exe - {User defined path}\WhiteCanyon\SecureClean 4\{scbase4.exe, SCDragDrop4.exe, SCLauncher4.exe, scliveupdate.exe, scregmanager4.exe, scscanner4.exe, SCWelcome.exe, sczap4.exe}
	HKLM\SOFTWARE\Classes\SecureClean4
	HKLM\SYSTEM\ControlSet002\Services\SCWatch 4.0

록한 레지스트리 키를 통해 특정 완전삭제 도구의 이름이나 제조사를 파악할 수 있었다.

향후에는 본 논문 결과를 통해 조사 시스템으로부터 완전삭제 도구 실행 여부를 판별하는 탐지도구를 개발 중에 있다. 그리고 완전삭제 기술 이외에 사건을 은폐하고자 증거를 조작하는 데이터 암호화 및 은닉 기술을 제공하는 도구의 흔적을 조사하여 증거 은닉을 위한 행위 조사 시 활용할 수 있도록 하고자 한다.

참 고 문 헌

[1] Peter F. Bennison and Philip J. Lasher, "Data security issues relating to end of life equipment," IEEE International Symposium on Electronics and the Environment, pp.317-320, 2004.

[2] Forte, D. and Power, R., "A tour through the realm of anti-forensics," Computer Fraud & Security, Vol.2007, Issue.6, pp.18-20, 2007.

[3] John R. Mallery, "Secure File Deletion: Fact or Fiction?," SANS GSEC Practical Assignment, Version 1.2e, 2006.

[4] Peter Gutmann, "Secure Deletion of Data from Magnetic and Solid-State Memory," Sixth USENIX Security Symposium, 1996.

[5] DoD 5220.22-M, "National Industrial Security Program Operating Manual(NISPOM)," 2006. (http://www.dtic.mil/whs/directives/corres/html/522022m.htm)

[6] Simon Innes, "Secure Deletion and the Effectiveness of Evidence Elimination Software," 3rd Australian Computer, Network & Information Forensics Conference, 2005.

[7] Matthew Geiger, "Evaluating Commercial Counter-Forensic Tools," the 5th Annual Digital Forensic Research Workshop, 2005.

[8] Brian Carrier, "File System Forensic Analysis," Addison-Wesly, 2005.

[9] DataEraser 2.0, HAURI, Inc. (http://www.hauri.co.kr/customer/product/product_view.html?product_uid=NDk=&prodcut_group=MTI=)

[10] East-Tec Eraser 2008(8.9), EAST Technologies (http://www.east-tec.com/consumer/eraser/index.htm)

[11] Eraser 5.86.1, Heidi Computers Ltd. (http://eraser.heidi.ie/)

[12] FINALeRASER 4.0.6.0220, FINALDATA (http://www.finaldata.co.kr/Products/?s=PRD&c=4)

[13] QuickClean 6.01.0003, McAfee, Inc. (http://www.mcafeestore.com/dr/sat4/ecMAIN.Entry10?SP=10023&PN=1&xid=50147&V1=797957&CUR=840&DSP=&PGRP=0&ABCODE=&CACHE ID=0)

[14] SecureClean 4.0, WhiteCanyon Inc. (http://www.whitecanyon.com/secureclean-clean-hard-drive.php)

[15] Steve Anson and Steve Bunting, "Mastering, Windows Network Forensics and Investigation," Wiley Publishing, Inc. 2007.

[16] T Bosschert, "Battling Anti-Forensics: Beating the U3 Stick," Journal of Digital Forensic Practice, 2006.

[17] Harlan Carvey, "Windows Forensic Analysis DVD Toolkit," SYNGRESS, pp.226-228, 2007.

[18] Harlan Carvey, "The Windows Registry as a forensic resource," Digital Investigation, Vol.2, Issue.3, pp.201-205, 2005.

[19] Harry Velupillai and Pontjho Mokhonoana, "Evaluation of Registry Data Removal by Shredder Programs," Advances in Digital Forensics IV, Springer Boston, pp.51-58, 2008.

김 연 수

e-mail : behappysoo@korea.ac.kr

2008년 서울여자대학교 정보보호공학과 (학사)

2008년~현 재 고려대학교 정보경영공학 전문대학원 석사과정

관심분야 : 디지털 포렌식, 모바일 포렌식

방 제 완

e-mail : jwbang@korea.ac.kr

2007년 한세대학교 정보통신공학과(학사)

2007년~현 재 고려대학교 정보경영공학 전문대학원 석박사통합과정

관심분야 : 디지털 포렌식, 소프트웨어 역공학 분석, 임베디드 시스템

김 진 국

e-mail : proneer@gmail.com

2008년 강원대학교 컴퓨터정보통신공학과 (학사)

2008년~현 재 고려대학교 정보경영공학 전문대학원 석사과정

관심분야 : 디지털 포렌식, 데이터 복구 및 분석

이 상 진

e-mail : sangjin@korea.ac.kr

1987년 고려대학교 수학과(학사)

1989년 고려대학교 수학과(이학석사)

1994년 고려대학교 수학과(이학박사)

1989년~1999년 ETRI 연구원

1999년~현 재 고려대학교 정보경영공학 전문대학원 교수

관심분야 : 디지털 포렌식, 모바일 포렌식, 심층 암호, 해쉬 함수