Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.39

Full Disk Encryption 환경에서 디지털 증거 수집 절차에 관한 연구*

장 성 민,† 박 정 흠, 박 찬 웅, 이 상 진‡
고려대학교 정보보호대학원

The Research for Digital Evidence Acquisition Procedure within a Full Disk Encryption Environment*

Sung-min Jang,† Jung-heum Park, Chan-ung Pak, Sang-jin Lee‡
Center for Information Security Technologies, Korea University

요 약

최근 개인정보보호에 관심이 증대되면서 암호화 솔루션 사용이 증가하고 있다. 또한, Windows XP 서비스 지원 종료와 함께 사용자의 운영체제 사양이 향상되면서, Bitlocker와 같은 Full Disk Encryption 솔루션의 활용도가 높아질 것으로 예상된다. 따라서 앞으로의 디지털 포렌식 조사는 Full Disk Encryption 환경에 대한 대응이 필요하다. 본 논문에서는 Full Disk Encryption 환경에 대응하는 디지털 증거 수집 절차를 제안하고 Full Disk Encryption 솔루션 중 사용률이 높은 제품들의 대응 방법 및 탐지 도구를 소개한다.

ABSTRACT

As a growing number of people are concerned about the protection of personal information, the use of encryption solution has been increased. In addition, with the end of support for Windows XP and the improvement of operating system, the use of the Full Disk Encryption solution like Bitlocker will be increased. Therefore, it is necessary to consider countermeasures against Full Disk Encryption for the future digital forensic investigation. This paper provides the digital evidence acquisition procedure that responds to the Full Disk Encryption environment and introduces the countermeasures and detection tool against Full Disk Encryption solutions that are widely used.

Keywords: Full Disk Encryption, Whole Disk Encryption, Evidence acquisition procedure.

I. 서 론

최근 국내에서 대형 개인정보 유출 사고와 기업 기밀 유출 사고 발생이 빈번해 지면서 데이터 암호화에 대한 관심이 증가하고 있다. 특히 데이터 암호화 방법 중 저장 매체 전체를 암호화하는 FDE(Full Disk Encryption) 솔루션에 대한 관심이 크게 증가하고 있다. 이를 반영하듯 최근 출시되는 노트북들은 FDE 솔루션 사용에 필요한 TPM(Trusted Platform Module)을 기본 장착하여 출시하고 있다. FDE 사용 환경이 개선되어 사용률이 증가함에 따라 수사관이 FDE 환경을 조사하는 경우는 증가할 것이다.

그러나 기존의 디지털 증거 수집 절차는 FDE환경을 고려하지 않고 있는 실정이다. 특히 FDE 환경 대

접수일(2014년 9월 24일), 수정일(1차: 2014년 11월 13일, 2차: 2014년 12월 12일), 게재확정일(2015년 1월 5일)
* 본 연구는 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임(2012M3A2A1051106)
† 주저자, sh2rkz@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

응은 수사관의 초동 조치가 증거 수집에 큰 영향을 미칠 수 있기 때문에 FDE 환경을 고려한 데이터 수집 절차의 연구가 필요하다. FDE 환경에 대응하는 방법은 크게 활성 상태 유무에 따라 구분되어야 하며, 각 FDE 솔루션마다 접근 방식이 다르므로 주의해야 한다.

본 논문에서는 디지털 포렌식 수사 시 FDE 환경을 고려한 증거 수집 절차를 제안한다. 4절에서는 FDE 솔루션 중 사용률이 높은 Bitlocker, Truecrypt, Symantec PGP Desktop의 Drive Encryption에 대한 탐지 및 대응방법을 기술한다. 5절에서는 3절과 4절의 내용을 적용할 수 있는 케이스를 분석한다. 6절에서는 FDE 환경 유무를 탐지하는 도구를 구현한 결과를 기술한다.

II. 관련 연구

2.1 FDE 동향

현재까지 디지털 포렌식 조사 시 FDE가 적용된 매체 조사는 수요가 적은 실정이다. 그러나 Windows XP 서비스 지원 종료와 함께 다수의 사용자가 운영체제의 사양을 향상시켰으며, 특히 암호화 솔루션 중 FDE 제품 사용 환경이 개선되었다. Windows 운영체제의 경우 Windows Vista Ultimate 버전 이후 제품부터 FDE 프로그램인 Bitlocker를 기본 제공한다. Table 1.에서는 FDE 솔루션들의 순위를 나타낸다[1].

Windows Vista Ultimate부터 지원하는 FDE 솔루션인 Bitlocker의 경우 기존 Windows 점유율로 인해 최고 순위를 가진다. 이후 Symantec의 Whole disk encryption과 오픈소스 FDE 솔루션인 Truecrypt의 경우 차례대로 다음 순위를 차지한다. 순위는 사용자들의 인기 순위에 의한 순서이다.

Table 1. The Worldwide Market Share of Full Disk Encryption Solutions

Rank	Manufacturer	Solution name
1	Microsoft	Microsoft Bitlocker
2	Symantec	Symantec Whole Disk Encryption
3	Symantec	Symantec Encryption
4	Wave Systems	Wave Encryptor
5	TrueCrypt Foundation	TrueCrypt

Wave Systems의 경우 자체 Drive Encryption 기능은 향후 제공 예정이며 현재는 Bitlocker의 키 관리 시스템 솔루션으로서 서비스 중이다[1].

FDE의 사용 환경 개선과 관련 솔루션 증가로 수사관이 FDE 환경을 조사해야 하는 경우가 늘어날 것이다. 그러나 현재 디지털 포렌식 증거 수집 방법으로는 FDE 환경에 대응하기 어렵다. 따라서 FDE 환경을 고려한 새로운 디지털 증거 수집 절차가 필요하다.

2.2 FDE 환경 대응 연구

디지털 포렌식 수사 시 FDE가 적용된 저장매체는 데이터가 암호화되어 있어 일반적인 수집방법 적용이 어렵다. FDE 환경 대응 시 복호화된 데이터 획득을 위해 암호키나 패스워드 획득이 중요하다. 그러나 조사할 컴퓨터가 활성 상태라면 FDE가 적용된 매체일지라도 복호화된 데이터 상태이므로 데이터 수집이 가능하다[2].

FDE가 적용된 매체 사용 시 입력된 패스워드는 운영체제 물리 메모리 상에 존재할 수 있다. 또한, 암호화된 데이터일지라도 물리 메모리 상에는 복호화된 상태로 존재한다. FDE 솔루션 중 오픈소스 FDE 솔루션인 Truecrypt의 경우 물리 메모리 상에 암호키의 정보를 남긴다. 이 암호키 정보를 사용하여 암호화된 가상 디스크를 복호화할 수 있다[2]. 따라서 활성 상태에서 물리 메모리 수집 절차가 필요하다.

FDE가 적용된 저장매체 대응 시 활성 상태 유무를 확인하여 대응한다. 활성 상태의 시스템인 경우 조사 대상의 물리 메모리 수집 및 분석으로 FDE 탐지를 수행한다. 로그인되지 않은 경우 피압수자 인터뷰를 통해 로그인 정보 획득 후 로그인하여 대응한다. FDE가 탐지되었다면 솔루션에 맞는 대응 방법으로 매체에 접근한다. 비활성 상태의 경우 사용자의 인터뷰를 토대로 접근하고 주변 장치나 메모 흔적, 패스워드로 예상되는 증거 수집이 필요하다[2].

FDE가 적용된 저장매체는 활성 상태 유무 확인 후 솔루션에 맞게 대응하여야 한다. 따라서 기존의 증거 수집 절차에서 추가적인 대응 방안이 필요하다.

III. FDE 환경을 고려한 디지털 증거 수집 절차 및 대응 방안

현재 디지털 포렌식 수사 시 증거 수집 절차는 활성 데이터의 수집을 고려한 증거 수집 절차를 따른다[3].

Fig.1.과 같이 휘발성 데이터 수집을 고려한 증거 수집 절차의 경우 전원 차단 여부 파악 후 휘발성 증거를 수집하고 전원 플러그를 제거한다. 그러나 이 절차는 FDE 환경을 고려하지 않기 때문에 수사관이 디지털 증거 수집 후 암호화된 데이터가 있으면 분석이 어려워진다. 또한, 휘발성 증거 수집 시 FDE 환경을 고려하지 않은 경우 FDE 환경을 탐지하여 대응할 수 있는 라이브 이미징 기회를 놓칠 수 있다. 따라서 디지털 증거 수집 시 FDE 환경 탐지가 필요하다. 또한, FDE 환경이 탐지되었을 경우 조사 대상의 활성 상태 유무와 FDE 솔루션에 따라 대응하는 방법이 다르므로 상황에 맞는 대응 방법이 필요하다.

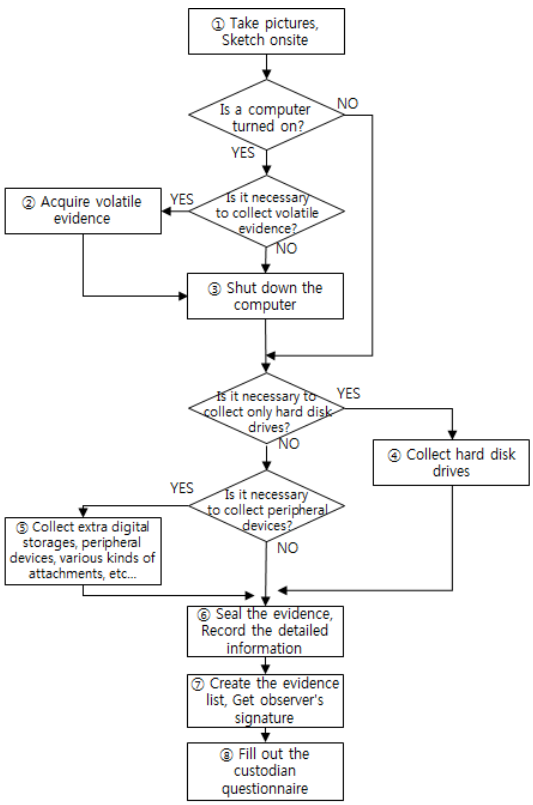

Fig. 1. Digital Evidence Acquisition Procedure for Volatile Data.

3.1 FDE 환경을 고려한 디지털 증거 수집 절차

현재의 디지털 증거 수집 절차는 영장 기재 내용에 따른 선별 압수를 지향하고 있다. 그러나 FDE 환경의 보급이 증가함에 따라 영장에 기재되지 않은 암호키나, 저장매체의 추가 압수가 필요한 상황이 발생할 수 있다. FDE 환경에서는 데이터 암호화로 인해 원활한 증거 수집이 어려울 수 있으므로 저장매체를 압수하거나 전체 데이터의 복제 또는 이미징을 고려해야 한다[4,5].

디지털 증거 수집 시 Fig.1.과 같이 휘발성 데이터를 고려한 증거 수집절차나 저장 매체만을 수집하는 기존의 증거 수집절차는 FDE 환경에 적합하지 않다. 따라서 Fig.2.에서 제안된 절차를 적용해야 증거 수집 기회를 증대시킬 수 있을 것이다.

FDE 환경을 고려한 디지털 증거 수집절차는 수집 대상의 활성 상태 유무에 따라 대응한다. 수집 대상이 활성 상태이나 운영체제가 잠겨있을 경우 피압수자 인터뷰를 통해 잠금을 해제한다. 이후 활성 데이터 수집에서 FDE 환경을 탐지한다. 또한, 활성 상태에서는 수집할 데이터가 복호화된 상태이거나, 물리 메모리 수집을 통해 암호키 획득이 가능할 수 있기 때문에 전원 차단에 유의하여야 한다. 그리고 활성데이터 수집 이후 논리 디스크 라이브 이미징을 통해 복호화된 데이터를 수집한다.

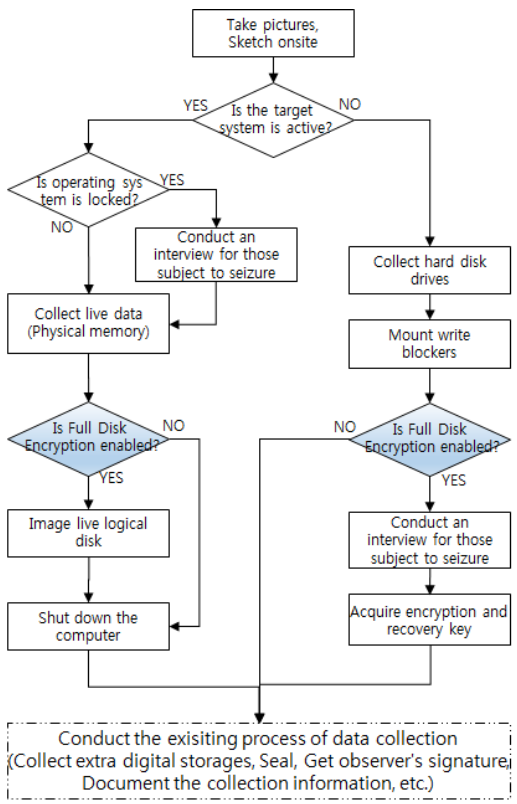

Fig. 2. Digital Evidence Acquisition Procedure within Full Disk Encryption Environment.

수집 대상이 비활성 상태인 경우 기존 증거 수집 절차에 의한 저장매체 수집 시 분석 단계에서 FDE 환경을 인지할 때 사전 대응을 통한 증거 수집 기회를 잃을 수 있다. 따라서 디지털 증거 수집 시 FDE 환경 탐지가 먼저 수행되어야 한다. FDE 환경 탐지는 수집 대상 매체를 쓰기방지장치에 연결 후 FDE가 사용하는 시그니처를 검색하여 탐지한다[2]. FDE 환경이 탐지되면 피압수자 인터뷰를 통해 키 정보를 획득하여 분석 시 대응한다.

기존의 증거 수집 절차는 휘발성 증거 수집 여부에 따라 물리 메모리를 수집한 후 전원을 차단하고 저장매체 사본이나 이미지를 생성한다. 이 경우 조사대상이 FDE 환경이면 증거 수집 이후 분석실에서 분석이 어려워진다. 그러나 FDE 환경을 고려한 증거 수집절차의 경우 현장에서 FDE 환경을 탐지하고 활성 상태 유무에 따라 암호키 획득이나 라이브 이미징, 피압수자 인터뷰를 통해 대응하기 때문에 증거 수집 및 분석이 원활히 할 수 있다.

3.2 FDE 솔루션에 따른 대응 방안

FDE 환경 대응 시 FDE 솔루션에 따라 대응 방법에 차이가 존재한다. 본 논문에서 다루는 FDE 솔루션은 현재 시장점유율이 가장 높은 Bitlocker와 점유율 대비 사용률이 높은 Truecrypt, Symantec사의 PGP Desktop 솔루션 내 Drive Encryption 솔루션의 대응방법을 Table 2.와 같이 제안한다.

Table 2. Countermeasures against each FDE solution

FDE Solutions	Active state	Inactive state
Bitlocker	Key management change	User interview, Acquiring other media
	Disable Bitlocker	
	Live imaging	
Truecrypt	Searching passphrase in physical memory	
	Exploiting vulnerability	
Drive Encryption	Live imaging	

Bitlocker의 경우 암호키로 쓸 수 있는 수단은 외부저장매체, 패스워드 입력, TPM(Trusted Platform Module)칩이 사용된다. 저장매체 접근 시 암호키를 사용할 수 없는 경우 복구키를 이용하여 저장매체에 접근할 수 있다. 저장매체가 활성 상태인 경우 Bitlocker를 해제하거나 복구키 백업을 통해 암호화된 저장 매체를 복호화할 수 있다. 운영체제 접근 권한문제로 인해 Bitlocker 해제나 복구키 백업이 어려운 경우 라이브 이미징을 통해 복호화된 논리 볼륨을 이미징한다.

Truecrypt의 경우 암호키는 사용자가 입력한 패스워드이다. Truecrypt의 데이터 암·복호화는 전용 프로그램으로 수행된다. 저장매체 접근 시 활성 상태인 경우 물리 메모리 수집 후 평문 상태의 패스워드 검색이나 암호키 검색으로 대응한다. 암호키가 검색된 경우 암호화된 매체의 헤더 섹터 영역을 패치 하는 취약점으로 복호화 가능하다.

Drive Encryption의 경우 암호키는 사용자가 입력한 패스워드, 보안토큰, 외부 저장매체이다. 저장매체 접근 시 활성 상태인 경우 라이브 이미징을 통해 복호화된 논리 볼륨을 이미징 한다. 복구키가 존재하는 경우 입력 패스워드 변경이나 Drive Encryption 해제를 수행한다.

저장 매체가 비활성 상태일 때 대응 방법은 FDE 솔루션마다 비슷하다. 솔루션에 맞는 복구키를 조사하거나 피압수자 인터뷰를 통한 정보 획득 및 암호키로 사용될 수 있는 주변 매체를 활용한다.

IV. FDE 환경 탐지 및 상세 대응 방안

FDE 환경 탐지 방법으로 활성 상태의 경우 물리 메모리 수집 후 프로세스 목록이나 DLL 목록을 확인하여 탐지할 수 있다.

비활성 상태의 경우 논리 레벨의 첫 번째 섹터인 VBR(Volume Boot Record)영역에서 FDE 솔루션의 시그니처가 존재한다. 따라서 저장 매체에 쓰기방지장치를 연결 후 시그니처를 탐지한다. 이후 탐지된 결과를 바탕으로 FDE 솔루션에 맞는 대응을 한다.

4.1 Bitlocker 대응 방안

Bitlocker는 Microsoft 사에서 제작한 FDE 솔루션으로써 Windows Vista Ultimate 버전 이상에서 동작한다. Bitlocker 활성화 시 해당 볼륨은 부

팅 영역과 암호화 데이터 영역으로 구분된다. 부팅 시에는 부팅 파일의 무결성이 유지되었는지 확인하여 정상적인 동작을 검사한다. 부팅 이후 데이터 영역을 암·복호화할 때 사용되는 암호키는 TPM, USB, 패스워드이다.

Fig.3.는 Bitlocker에서 암호화된 데이터를 복호화하는 과정이다[6]. 복호화 과정에서 사용자가 사용하는 암호키 외에 VMK(Volume Master Key)를 복호화하는 복구키가 별도로 존재한다. 따라서 복구키를 사용하여 Bitlocker 대응에 활용할 수 있다.

Bitlocker는 svchost.exe에 의해 활성화되며 bdesvc.dll을 사용한다. 이를 통해 운영체제 사용 시 데이터 암·복호화를 수행한다. 따라서 Fig.4.와 같이 물리 메모리 수집 후 분석을 통해 svchost 프로세스에 사용된 "bdesvc.dll"을 확인하여 Bitlocker 적용 여부를 탐지할 수 있다.

Bitlocker는 운영체제의 가상메모리파일(pagefile.sys) 관리에서도 데이터 기밀성을 보장한다. 레지스트리 내의 "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PagefileOnOSVolume" 키는 Bitlocker가 활성화된 경우에만 존재한다. 따라서 이 정보를 통해 Bitlocker 적용 여부를 탐지할 수 있다. "PagefileOnOSVolume" 키는 윈도우에서 가상메모리 관리 시 Bitlocker가 활성화된 볼륨에만 관리하는 설정으로써, Bitlocker가 활성화되지 않은 볼륨에 가상메모리를 할당하여 데이터

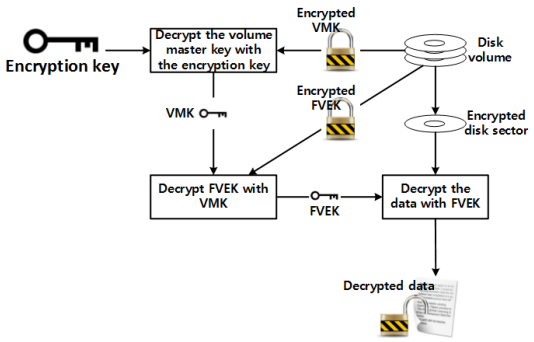

Fig. 3. Bitlocker Decryption Process

```
root@sh2rkz:~# vol -f /root/Desktop/SH2RKZ-PC-20140918-195336.raw
 --profile=Win7SP0x86 dlllist -p 908 | grep bdesvc.dll
Volatility Foundation Volatility Framework 2.3.1
0x701d0000    0x16000         0x1 c:\windows\system32\bdesvc.dll
```

Fig. 4. bdesvc.dll in the dll list used by svchost.exe

가 유출되는 것을 방지한다.

비활성 상태의 저장매체는 VBR에서 시그니처를 탐지할 수 있다. 저장매체의 첫 번째 섹터를 기준으로 0x03 번째 오프셋에서 "-FVE-FS" 문자열이 존재한다. 0xA0 번째 오프셋의 16바이트는 Bitlocker 적용 여부를 확인할 수 있는 시그니처이다. 4967d63b-2e29-4ad8-8399-f6a339e3d01 값을 가지며 Fig.5.의 값을 리틀 엔디안으로 해석한 값과 같다.

Bitlocker 탐지 후 대응 방안은 활성 상태와 비활성 상태 대응으로 구분한다. 활성 상태인 경우 해당 볼륨에서 "Bitlocker 관리" 클릭 시 Fig.6.와 같이 확인된다. Fig.6.의 대화상자에서 Bitlocker를 해제하거나 복구키 백업으로 대응한다. 그리고 비 할당영역 조사 시 삭제된 데이터는 Bitlocker를 해제하여도 존재하지 않는다. 따라서 저장매체 이미징 시 활성 상태에서 논리 볼륨의 라이브 이미징을 수행하여 대응한다.

비활성 상태의 경우 저장매체 수집 후 이외의 저장매체에서 복구키를 검색하거나 사용자 인터뷰를 통해 얻은 정보로 암호키 매체나 운영체제 로그온 정보를 수집하여 대응한다.

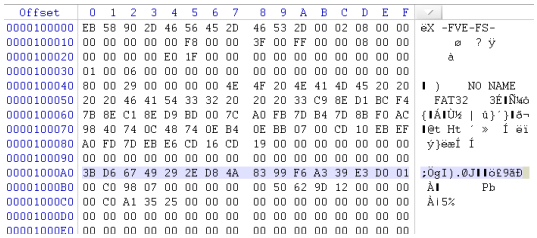

Fig. 5. Bitlocker Signature in VBR

Fig. 6. Bitlocker Management Options

4.2 Truecrypt 대응 방안

Truecrypt는 오픈소스로 개발된 FDE 솔루션으로써 Windows XP 이상의 Windows 운영체제와 Unix 운영체제를 지원한다. 사용법은 가상 디스크 볼륨을 생성하고 자체 프로그램에서 마운트하여 실행된다.

데이터 암호화는 Fig.7.과 같이 AES를 기본 알고

리즘으로 사용하며 다른 암호 알고리즘을 선택할 수 있다. 그리고 사용자가 입력한 패스워드를 암호키로 사용하며 지원 파일시스템은 FAT과 NTFS이다.

암호화 과정은 암호화할 가상 디스크를 임의로 생성한 마스터키로 암호화한다. 그리고 암호화된 가상 디스크 파일 512byte 헤더에 마스터키 정보를 저장하는데, 이때 사용자가 입력한 패스워드와 가상 디스크 헤더의 0x00~0x40의 Salt 값을 사용하여 마스터키를 암호화한다. 복호화는 사용자가 입력한 패스워드와 가상 디스크 헤더의 Salt 값을 이용하여 마스터키를 복호화하고 복호화된 마스터키는 다시 암호화된 데이터를 복호화한다.

Truecrypt는 암호화된 가상디스크를 자체 프로그램을 통해 마운트 하여 사용한다. 따라서 활성 상태일 때 가상 디스크가 존재하면 Fig.8.과 같이 Truecrypt 프로세스를 확인하여 탐지할 수 있다. 또한, 가상디스크의 고유 확장자인 "TC" 파일을 검색하여 파일 존재 여부를 파악할 수 있다. 비활성 상태 저장 매체의 경우 MBR 영역 0x06 오프셋에서 "TrueCrypt" 문자 유무 확인으로 탐지할 수 있다.

탐지 후 대응 방안은 활성 상태와 비활성 상태 대응으로 구분한다. 활성 상태인 경우 해당 논리 볼륨의 라이브 이미징을 수행하여 대응한다. 또는 시스템은

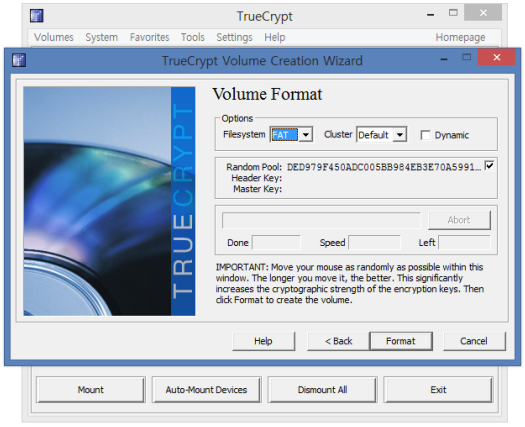

Fig. 7. Creating File System by Truecrypt

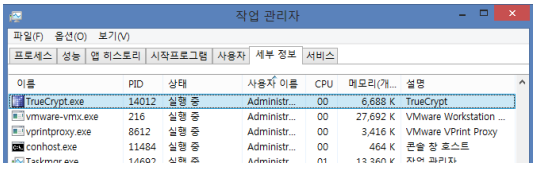

Fig. 8. Truecrypt Process in a Task Manager

활성 상태이나 마운트 되지 않은 가상디스크의 경우 헤더 패치 취약점으로 대응한다. 참고로 TrueCrypt는 현재 개발이 중단된 상태이며 헤더 패치 취약점에 대한 대응은 다른 솔루션을 사용할 것을 권장하고 있다. TrueCrypt를 사용하는 환경 대응은 헤더 패치 취약점을 적용할 수 있다.

취약점 적용 시 Fig.10.과 같이 조사 대상 시스템에서 물리 메모리 내에 마스터키가 존재할 수 있으며, Fig.9.와 같이 해당 시스템에서 사용되었던 마스터키가 탐지되면 이를 데이터 복호화에 활용할 수 있다 [7,8].

참고로 발견된 마스터키를 활용하여 암호화된 데이터를 복호화하는 과정은 다음과 같다. 검색된 마스터키를 프로그램 코드 내 복호화 로직에 임의로 삽입하여 컴파일한다. 마스터키가 포함되어 컴파일된 TrueCrypt 프로그램은 취약점 적용 시 사용된다. TrueCrypt는 가상디스크 파일 마운트 시 해당 파일의 헤더에서 패스워드 관련 정보를 확인하여 패스워드를 요청한다. 그러나 수사관이 임의로 가상 디스크 파일을 생성한 후 헤더 영역을 조사 대상 가상디스크에 헤더 영역으로 덮어씌우는 경우 Fig.10.의 Encrypted Header가 수사관의 헤더 정보로 바뀌게 된다.

따라서 헤더 패치 이후 조사대상 가상디스크를 마운트 시 TrueCrypt에서 요청하는 패스워드는 조사관의 헤더 정보를 확인하여 요청된다. 조사관은 해당

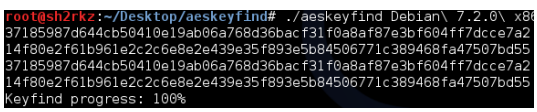

Fig. 9. Finding AES Key in Physical Memory

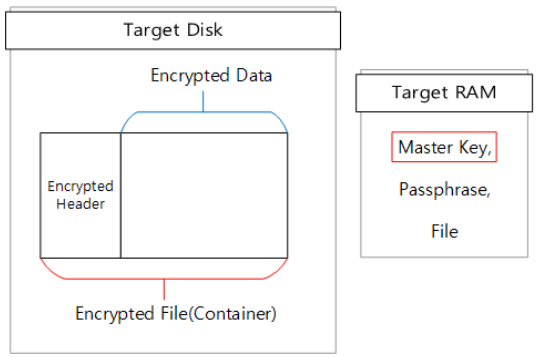

Fig. 10. The Structure of Truecrypt Virtual Disk and Physical Memory Status.

헤더의 패스워드를 알고 있기 때문에 TrueCrypt의 패스워드 요청단계를 통과할 수 있다. 이후 실제 암호화 데이터의 복호화 시 사용되는 마스터키는 앞서 컴파일한 프로그램 코드 내에 삽입한 조사 대상의 마스터키이므로 데이터는 정상적으로 복호화 된다. 위의 과정은 TrueCrypt 응용 프로그램을 이용한 복호화 방법의 한 가지 예제이며, 내부 알고리즘을 이용하여 별도의 도구를 개발하여 복호화를 시도할 수 있다.

비활성 상태의 경우 hibernate 파일에서 마스터키를 검색하여 취약점 공격을 수행하거나 피압수자 인터뷰를 통한 정보 획득으로 대응한다. 또는 가상디스크에 패스워드 무작위 대입 공격을 시도하여 대응할 수 있다.

4.3 Drive Encryption

Symantec 사의 PGP Desktop 솔루션 내 Drive Encryption은 해당 볼륨의 암호화를 수행한다. 지원하는 운영체제는 Windows 운영체제와 Mac OSX, Linux 운영체제이다. 볼륨 암호화 시 자체 부트로더를 사용하여 운영체제 파티션을 로드한다. 따라서 Fig.11.과 같은 부트로더가 활성화되며 사용자가 입력한 패스워드를 요구한다. 패스워드 분실 시에는 부트로더에서 패스워드 복구 질의문에 대한 답을 입력하거나 Drive Recovery Token을 사용하여 복구할 수 있다.

Drive Encryption은 암호화된 볼륨을 자체 부트로더를 통해 부팅하기 때문에 MBR 영역에 시그니처가 존재한다. 따라서 저장 매체의 MBR 영역 0x03 오프셋에서 Fig.12.와 같이 "PGPGUARD" 값을 검색하여 탐지한다[8]. 활성 상태의 경우 Drive Encryption 프로세스인 "PGPtray.exe"를 확인하여 탐지한다.

Fig. 11. Drive Encryption Bootloader.

탐지 후 대응 방안은 활성 상태와 비활성 상태 대응으로 구분한다. 활성 상태인 경우 해당 논리 볼륨을 라이브 이미징을 수행하여 대응한다.

비활성 상태의 경우 피압수자 인터뷰를 통해 복구 질의문에 대한 답이나 패스워드를 수집한다. 그리고 Drive Recovery Token 수집 및 주변 장치 수집으로 대응한다.

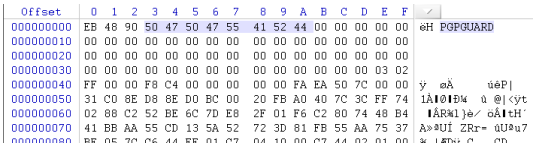

Fig. 12. Drive Encryption Signature in VBR

V. FDE 환경 사례 분석

FDE 환경은 기업에서 기밀 유출을 막기 위해 사용되거나 개인정보보호를 목적으로 개인이 사용한다. 그러나 범죄사건에서 디지털 포렌식 수사를 방해하기 위해 사용되기도 한다. 따라서 수사관의 치밀한 증거 수집 계획이 있어야 하며 대응 방법에 미숙한 경우 디지털 증거 수집 기회를 잃을 수 있다. 따라서 수사관의 역량이나 경험과 관계없이 대응 절차를 정립하여 수사에 적용함으로써 일정한 수사 효율을 유지해야 한다.

5.1 OO사 기밀 유출 사건

OO사는 얼마전 다량의 고객 정보 유출로 인해 그 근원지를 찾는 중 내부자 유출 정황을 발견하고 수사를 의뢰하였다. 유출 시 사용했을 것으로 추정되는 노트북이 켜져 있었으며 웹브라우저 기록이 전부 삭제되어 있었다. 증거 수집을 위해 물리 메모리를 수집하고 분석하는 중 AES 암호키 스트림이 발견되었고 메모리상에 존재한 프로세스 리스트 중 Truecrypt 가 발견되었다. 다른 FDE 매체는 존재하지 않았으며 TrueCrypt 가상 디스크 확장자인 TC 파일을 검색하여 발견하였다. 그 후 물리 메모리 내부로부터 마스터키를 발견하여 복호화한 결과 대량의 고객 정보가 담긴 엑셀파일이 존재하였다. 웹브라우저 기록은 삭제되었지만 물리 메모리 상에서 노트북 사용자의 이메일 주소가 발견되어

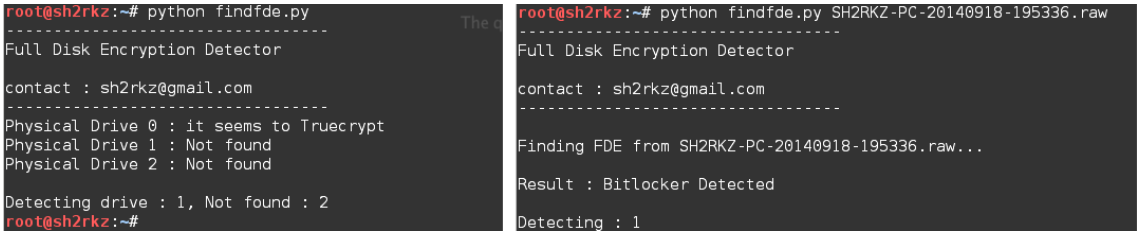

Fig. 13. Full Disk Encryption Detecting Tools with Python Script

유출자를 특정할 수 있었다.

이 사례는 운영체제가 활성 상태인 경우 물리 메모리 수집과 FDE 저장매체 확인이 중요한 사례이다. 기밀 유출 사건은 디지털 포렌식 수사를 방해하는 요소가 다수 존재하기 때문에 수사관의 경험과 역량에 의존하는 경우가 많다. 사례를 FDE환경을 고려한 증거 수집 절차를 적용하는 경우 조사 대상 시스템이 활성 상태임을 확인하고 물리 메모리를 수집한다. 수집된 물리 메모리는 FDE 환경 탐지 도구를 사용하여 적용된 솔루션을 확인한다. 사례에서 적용된 솔루션은 Truecrypt이므로 라이브 이미징이나 취약점 공격을 통해 증거 수집이 가능할 것이다.

본 논문에서 제안된 증거 수집 절차를 활용하여 FDE 환경에 대응하는 수사관의 역량과 관계없이 일정한 수사 효율을 유지하기 위해 FDE 환경을 고려한 증거 수집 절차를 적용하여야 한다.

5.2 OO 불법 도박 사이트 운영 사건

OO 불법 도박 사이트를 운영 중인 사업장 위치를 제보받아 현장을 급습하였다. 현장에서는 도박 사이트 서버와 관리자 컴퓨터를 강제로 종료한 상황이었다. 저장 매체를 먼저 확보하고 이미징 작업 중 매체 정보를 확인할 수 없는 문제가 발생하였다. 수집한 매체에 쓰기방지장치를 연결한 후 매체의 시그니쳐 확인 결과 Bitlocker가 활성화된 상태였다. Bitlocker 적용 확인 후에 피압수자와의 인터뷰를 통해 운영체제 로그온 정보를 알아냈으며, PC 주위에 구겨진 용지를 확인한 결과 Bitlocker의 복구키 정보를 출력한 용지임을 확인하고 추가 수집하였다.

이 사례는 비활성 상태에서 시그니쳐 확인을 통해 복구키 수집이 중요한 사례이다. Bitlocker가 적용된 매체 분석 시 TPM이 없는 수사관의 분석 환경에서 대응 가능한 방법은 복구키를 확보하는 것이다. Bitlocker는 구동 시스템 환경이 달라질 경우 복구키를 입력해야 저장 매체에 접근할 수 있기 때문이다.

디지털 포렌식 수사에서 비활성 상태의 매체를 수집해야 하는 경우 수사관의 사전 지식이 부족할 때 복구키와 같은 분석을 위한 정보를 획득하지 못하여 증거 수집 이후 분석이 불가능할 수 있다. 따라서 FDE 솔루션들의 대응 방법을 숙지하고 FDE 환경을 고려한 대응 절차를 적용하여 증거 수집 이후 분석이 불가능한 상황을 방지하여야 한다.

VI. FDE 환경 탐지 도구 구현

4절의 내용을 토대로 FDE 환경 탐지를 위한 도구를 개발하였으며 운영체제의 실행 의존성이 적은 Python 스크립트로 개발하였다. Fig.13.은 구현된 도구의 결과물이며 실행 시 FDE 환경을 탐지한다. 또한, 프로그램 실행 인자로 물리 메모리 덤프 파일을 사용하여 FDE 환경을 탐지할 수 있다.

조사 대상 시스템이 비활성 상태인 경우 저장매체 수집 이후 쓰기 방지 장치에 연결하고 탐지 도구를 실행한다. 탐지 도구는 저장 매체의 논리 볼륨에서 첫 번째 섹터나 MBR 영역 해석 후 FDE 솔루션별 시그니쳐를 검색하여 적용된 FDE 솔루션을 탐지한다,

조사 대상 시스템이 활성 상태인 경우 물리 메모리를 수집하고 덤프 파일을 탐지 도구 실행 인자로 사용한다. 이때 탐지 도구는 덤프 파일 내 프로세스 리스트를 해석하여 FDE 관련 프로세스를 검색하거나 프로세스들이 사용한 DLL 리스트에서 FDE가 사용한 특징적인 DLL을 검색하여 FDE 환경을 탐지한다.

VII. 결 론

FDE 환경의 대응 방법은 조사대상의 활성 상태 여부에 따라 구분된다. 활성 상태의 경우 메모리상의 암호키 정보 획득이 중요하고 불가능한 경우에는 암호화 저장 매체의 라이브 이미징을 통해 대응한다. 비활

성 상태의 경우 사용자 인터뷰 및 복구키 수집, 외부 매체 수집을 통해 대응한다.

향후 디지털 포렌식 수사에서 수사관이 대응하게 될 FDE 환경은 정립된 대응 절차에 의해 효율적으로 대응하여 일정한 수사 효율을 유지해야 할 것이다. 따라서 증거 수집단계에서 FDE 환경을 고려한 증거 수집 절차를 적용해야 할 것이다. 이로써 증거 수집이 가능한 기회를 최대한 확보하여 수사 효율을 높이고 원활한 증거 수집을 수행할 수 있을 것이다.

본 논문 이후의 연구에서는 논문에 기술된 대응 방법 이외의 FDE 솔루션 탐지 및 대응방안 연구와 개별 파일 보호를 위해 사용되는 DRM 솔루션 대응 방안을 연구할 것이다.

References

[1] G2Crowd, "https://www.g2crowd.com/products/microsoft-bitlocker/reviews", G2Crowd, Nov. 2014.

[2] E Casey, GJ Stellatos, "The Impact of Full Disk Encryption on Digital Forensics", ACM SIGOPS Operating Systems Review, Vol. 42, Issue. 3, pp. 93-98, Apr. 2008.

[3] Sangjin Lee, "Introduction of Digital Forensics", Digital Forensic Research Center, Mar. 2011.

[4] Ministry of Justice, "Criminal Procedure Law - Code 106, Seizure", Oct. 2014.

[5] Supreme Prosecutors' office, "Digital evidence acquiring and analysis provisions", Nov. 2012.

[6] Microsft, "http://technet.microsoft.com/ko-kr/library/cc162804.aspx", TechNet, Apr. 2007.

[7] Hargreaves, Christopher, Howard Chivers, "Recovery of encryption keys from memory using a linear scan.", Availability, Reliability and Security, 2008. ARES 08. Third International Conference on, pp. 1369-1376, Mar. 2008.

[8] SANS, "Encrypted Storage Incident Handling", SANS, Apr. 2009.

[9] Magnet Forensics "http://www.magnetforensics.com/encrypted-disk-detector-a-free-digital-forensics-tool/", Magnet Forensics, Apr. 2013.

[10] Forensic Wikipedia, "http://www.forensicswiki.org/wiki/BitLocker_Disk_Encryption", Forensic Wikipedia, Dec. 2014.

[11] Microsoft, "http://technet.microsoft.com/ko-kr/library/hh831507.aspx", TechNet, May. 2013.

[12] Symantec, "http://www.symantec.com/content/en/us/enterprise/white_papers/b-how-drive-encryption-works_WP_21275920.pdf", Symantec, Nov. 2012.

[13] Liang, Min, Chao-wen Chang, "Research and design of full disk encryption based on virtual machine.", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, Vol. 2, pp. 642-646, Jul. 2010.

[14] Halderman, J. Alex, et al, "Lest we remember: cold-boot attacks on encryption keys.", Communications of the ACM, Vol. 52, Issue. 5, pp. 91-98, May. 2009.

[15] Balogh, Stefan, Matej Pondelik, "Capturing encryption keys for digital analysis.", Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2011 IEEE 6th International Conference on, Vol. 2, pp. 759-763, Sep. 2011.

[16] Dietiker, Kristen, "PGP whole disk encryption: blazing trails in IT security at UW Medicine.", Proceedings of the 36th annual ACM SIGUCCS fall conference: moving mountains, blazing trails, pp. 17-20, Oct. 2008.

[17] Hargreaves, Christopher, Howard Chivers, "Detecting hidden encrypted volumes.", Communications and Multimedia Security, pp. 233-244, May. 2010.

〈저자소개〉

장 성 민 (Sung-min Jang) 학생회원
2013년 2월: 인제대학교 컴퓨터공학부 졸업
2013년 3월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 디지털 포렌식, 정보보호, 역공학

박 정 흠 (Jung-heum Park) 정회원
2007년 2월: 한양대학교 정보통신대학 컴퓨터전공 공학사
2009년 2월: 고려대학교 정보경영공학전문대학원 공학석사
2014년 2월: 고려대학교 정보경영공학전문대학원 박사
〈관심분야〉 디지털 포렌식, 안티-안티 포렌식

박 찬 웅 (Chan-ung Pak) 학생회원
2013년 2월: 건양대학교 정보보호학과 졸업
2013년 9월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 디지털 포렌식, 역공학, 모바일 포렌식

이 상 진 (Sang-jin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수