Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.839

하드웨어 고유 정보 수집에 대한 디지털 증거 수집 절차

박 찬 웅,† 이 상 진‡
고려대학교 정보보호대학원

Digital Evidence Collection Procedure for Hardware Unique Information Collection

Chan-ung Pak,† Sang-jin Lee‡
Center for Information Security Technologies, Korea University

요 약

빈번한 개인정보 유출 사고를 통해 프라이버시 정책이 강화됨에 따라 민감한 데이터는 암호화하여 저장한다. 이런 이유로 피조사자 소유의 암호화 된 데이터는 디지털 포렌식 관점에서 중요한 분석대상이다. 현재까지 디지털 증거 수집 절차에서는 이미징만 고려하고 있으며, 하드웨어 고유 정보는 수집하지 않는다. 디스크 이미지에 남지 않는 정보를 통해 암호 키를 생성한다면 암호화 된 데이터를 복호화 할 수 없다. 최근 하드웨어 고유 정보를 이용하여 암호화를 수행하는 어플리케이션이 등장하였다. 따라서 본 논문에서는 보조기억장치에 남지 않는 하드웨어 고유 정보에 대해 연구하였으며, 하드웨어 고유 정보 수집 방안을 소개한다.

ABSTRACT

Sensitive data is encrypted and stored as privacy policy is strengthened through frequent leakage of personal information. For this reason, the cryptographically owned encrypted data is a very important analysis from the viewpoint of digital forensics. Until now, the digital evidence collection procedure only considers imaging, so hardware specific information is not collected. If the encryption key is generated by information that is not left in the disk image, the encrypted data can not be decrypted. Recently, an application for performing encryption using hardware specific information has appeared. Therefore, in this paper, hardware specific information which does not remain in file form in auxiliary storage device is studied, and hardware specific information collection method is introduced.

Keywords: Encryption, Database, Hardware information, Digital evidence

I. 서 론

디지털 포렌식은 운영체제와 응용 소프트웨어가 생성한 데이터를 분석하여 어떤 일이 발생했는지를 규명한다.

기존에는 사건 이전에 널리 사용되고 있는 소프트웨어들을 사전에 분석하여 자동으로 생성되는 아티팩트(Artifact)를 사건 규명에 사용하였다.

그러나 매번 새로운 프로그램의 출시, 소프트웨어의 업데이트 등으로 인해 사건 이전에 소프트웨어를 미리 분석할 수 없어 사후 분석을 고려해야 한다.

대부분 개인 정보와 같이 민감한 데이터들을 보호하기 위해 기술적·관리적 보호 조치 기술들을 적용하고 있으며 사용이 간편하다.

이러한 사례로 PC에서 사용하는 FDE(Full Disk Encryption)의 암호화 키는 TPM(Trusted Platform Module)에 저장하고 Android에서 사용하는 FDE의 키는 TrustZone에 저장[1]하여 매

Received(01. 29. 2018), Modified(1st: 05. 21. 2018, 2nd: 06. 25. 2018), Accepted(06. 25. 2018)
† 주저자, koha@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

번 부팅 시 사용자가 암호를 입력할 필요가 없다.

개정 형사소송법 제106조 제3항으로 범죄와 관련 정보만 출력·복제 압수원칙이 명문화 되어 파일·디스크만 복제가 많아지고, 메신저에서와 같이 프라이버시 보호를 위한 암호화 기능이 보편화되면서 하드웨어 고유정보 수집이 중요해지고 있다.

본 논문에서는 하드웨어 고유 정보에 대해 구분하고, 보조기억장치에 저장되지 않는 하드웨어 고유 정보를 식별함으로써 디지털 증거 수집 절차에서 하드웨어 고유 정보 수집의 필요성을 제시하며 이에 따른 수집 절차의 개선 방법을 제안한다.

II. 기존 디지털 증거의 수집 체계

범죄수사에서 디지털 증거의 중요성이 증가함에 따라 각 수사기관에서는 디지털 증거 처리에 관한 가이드라인 및 내규를 정하여 운영하고 있다. 그러나 현재 디지털 증거의 수집 체계에서는 이미지 수집에 집중하고 있으며 하드웨어 고유 정보 수집에 대해서는 고려하지 않는다.

대검찰청의 '디지털 증거의 수집·분석 및 관리 규정' 〔시행 2017.3.1.〕 〔대검찰청예규 제876호, 2016.12.26., 일부개정〕 에서 디지털 증거의 수집과 관련하여 디지털 기기의 메모리에 기록된 데이터 및 키보드와 마우스 등에 남은 지문을 채취하거나, 네트워크 또는 케이블의 연결 상태를 기록하는 것까지 명시되어 있지만, 수집 대상 PC의 하드웨어 정보는 기술하지 않았다[2].

경찰의 '디지털증거 처리 표준 가이드북'인 '디지털 증거수집 절차'와 '디지털 증거 수집 및 처리 등에 관한 규칙' 〔시행 2017.9.1.〕 〔경찰청훈령 제845호, 2017.8.28., 일부개정〕 둘 다 수집 대상 PC의 하드웨어 정보는 고려하지 않고 있다[3][4].

증거유형별 분석절차에서 평문 상태가 아닌 파일에 대한 분석 절차에 대해 일부 언급하고 있다. 암호파일에서 증거자료를 추출하기 위한 방법으로 해독 프로그램을 이용하거나 역공학 등의 방법으로 분석한다는 내용이 포함되어 있으나, 최초 압수 시 PC의 하드웨어 고유 정보를 함께 수집하는 것에 대한 구체적인 지침이 규정되어 있지 않다.

지금까지의 디지털 증거 수집 절차에서는 디스크 또는 물리 메모리에 저장된 데이터에 대한 이미징만 고려하고 있기 때문에 하드웨어 고유 정보에 대한 수집은 실시하고 있지 않다.

III. 하드웨어 고유 정보 수집의 필요성

3.1 하드웨어 고유 정보 부재 시 문제점

USB 연결 여부 판별이 중요했던 사례가 있다. 호텔에 술 취한 사람이 알몸으로 돌아다닌다는 신고를 받아 출동하였다. 다른 사람과 함께 있었으며, 빔 프로젝터를 통해 아동 포르노 사진이 나오고 있었다. 외장하드에서 아동포르노가 발견되었는데, 노트북은 본인 기기가 맞으나 외장하드는 본인 소유가 아니며, 본인과 관련 없다고 주장하였다. 노트북의 레지스트리에 있는 USBStor 키 항목에서 외장하드 시리얼 번호와 모델명을 찾았고 특정 시점에 연결됨을 증명하여 이를 근거로 아동 포르노 보유로 유죄가 선고되었다[5].

이 사건의 경우 외장하드 인터페이스는 USB이기 때문에 PC에 연결 시 레지스트리에 외장하드의 고유 정보가 모두 기록되는 특징을 가지고 있어, 레지스트리를 분석하면 외장하드 연결 유무를 입증할 수 있다.

그러나 보조기억장치의 인터페이스는 IDE (Integrated Drive Electronics)와 SATA (Serial Advanced Technology Attachment)이기 때문에 보조기억장치의 모델명만 레지스트리에 저장한다. 그리고 현재 대부분 메인보드에서는 핫스왑(HotSwap)기능을 지원하기 때문에 재부팅 없이 연결 및 제거를 할 수 있어 보조기억장치를 외장하드처럼 사용할 수 있다.

TTA의 '디지털 증거 수집 보존 가이드라인'에서는 유형별 디지털 증거 수집에서 카메라 또는 캠코더를 통해 증거 수집 시 수집 대상의 모델번호를 포함하는 제원 촬영을 명시하고 있다[6].

그러나 지문을 남기지 않기 위해 장갑 사용과 범죄에 사용할 차량의 번호판을 제거하듯 제품 정보가 기록된 스티커 등을 하드웨어에서 제거 또는 위조할 수 있기 때문에 실제 제품에 기록된 데이터와 교차검증이 필요하다.

3.2 하드웨어 정보를 통한 데이터 암호 키 생성 사례

국내에서 가장 많이 사용하는 카카오톡 PC 버전은 자동로그인 기능을 설정하면 PC가 켜져있는 상태에서는 모든 대화 내역이 PC에 저장된다.

카카오톡 메신저의 대화 내용은 '%LOCALAPP

DATA%\Kakao\KakaoTalk\users′ 경로에서 사용자 ID 값을 암호화 후 해시 함수로 계산한 값을 디렉토리명으로 갖는다.

대화 내역 파일명은 ′〈chatLogs_chatID〉.edb′으로 구성되어 있으며 메시지 내용과 메시지를 받은 시간, 그리고 메시지의 송신자 등에 대한 데이터가 저장되어 있으나, Fig.1과 같이 대화 내용을 저장한 데이터베이스 파일 전체를 암호화 한다.

메신저 프로그램을 실행하면 디스크의 시리얼 번호, 디스크 모델명, SMBIOS UUID(4장 하드웨어 고유 정보에서 설명)을 사용하여 Fig.2와 같은 알고리즘을 통해 고유한 암/복호화 키를 생성한다.

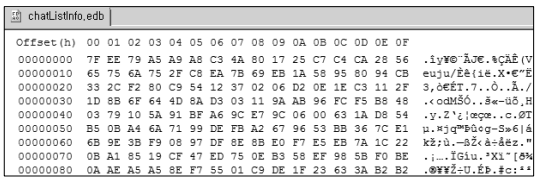

Fig. 1. Chat Database Files

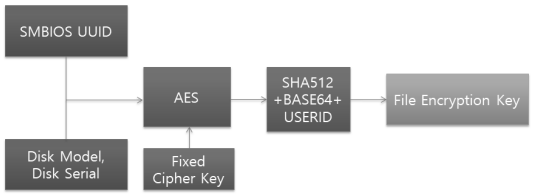

Fig. 2. Encryption key

하드웨어 고유 정보를 사용하여 암호 키를 생성하기 때문에 분석 대상 PC에 장착된 하드웨어 고유 정보가 있어야만 대화내역을 확인할 수 있다.

3.3 하드웨어 정보를 통한 통신 암호 키 생성 사례

불법 프로그램 중 사람이 플레이하지 않고 자동으로 사냥과 아이템을 획득하는 게임 매크로가 있다. 이 프로그램은 클라이언트와 서버로 분리하여 사용자를 인증하며 통신 내역을 보호하기 위해 암호화 통신을 한다.

여러 PC에서 공동으로 사용하지 못하도록 불법 프로그램은 로그인 시 사용자 PC의 하드웨어 고유 정보를 전송하며 하드웨어 고유 정보를 통해 암호 키를 생성한다.

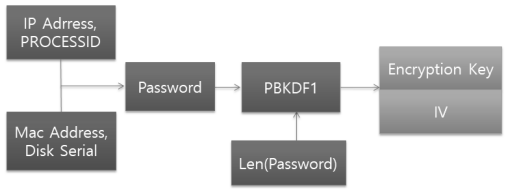

Fig. 3. Encryption Key

생성한 암호키를 통해 서버와 통신하며 매크로의 핵심 기능의 명령을 받아 기능을 수행한다.

따라서 이 불법 프로그램의 서버 압수 후 통신 내역을 분석하여 불법 프로그램 사용자의 IP와 Mac Address, Disk Seiral 번호를 특정할 수 있으며, 이를 통해 이 프로그램이 설치된 PC의 하드웨어 고유정보를 확인하면 사용자를 특정할 수 있다.

IV. 하드웨어 고유 정보

하드웨어 정보를 수집하지 않으면 이미지만 있는 증거물에서는 데이터 분석을 실패할 수 있다. 따라서 보조기억장치에 하드웨어 고유 정보가 기록되는지 확인하기 위해 Table 1.과 같은 PC를 대상으로 조사하였으며, 제조사가 다른 2개의 SSD로 실험을 진행하였다.

실험 대상 OS는 Table 2.와 같이 Windows 7 버전별과 Windows 10 버전별로 진행하였으며 지원이 중단된 Windows XP와 점유율이 낮은 Windows 8은 실험 대상 OS에서 제외하였다.

하드웨어 고유 정보가 보조기억장치에 잔존하는지 확인하기 위해 하드웨어 고유 정보들을 먼저 선별하였다. 이후 SSD(Solid State Drive)에 실험 대상 OS를 설치하고 이미징 작업 이후 이미지 파일에 하드웨어 고유 정보가 저장되어 있는지 전수 조사를 진

Table 1. System Information

Classify	Model
CPU	Intel(R) Core(TM) i7-4770
Board	ASUSTeK Z87-PRO
Ram	M378B5173QH0-CK0
ODD	HL-DT-ST DVDRAM GH24NSB0
HDD	INTEL SSDSC2BW120A4
	SanDisk SD8SBAT128G1122
Monitor	SAMSUNG SyncMaster B2240

Table 2. OS List

OS	Windows 7 Ultimate K with Service Pack 1
	Windows 7 Home Premium K with Service Pack 1
	Windows 7 Professional K with Service Pack 1
	Windows 10 Enterprise, Version 1703
	Windows 10 Education KN
	Windows 10 (Multiple Editions)

행하였다.

분석한 결과 Table 3.과 같이 Ram의 Part Number와 Serial, HDD의 Serial과 WWN 등은 보조기억장치에 저장되지 않았다.

Table 4.와 같이 메인보드, ODD, 모니터 , NIC의 모델명 정보들은 레지스트리에 기록되어 있다.

System Management BIOS (SMBIOS)의 UUID(Universally Unique IDentifier)는 128bit로 RFC4122 표준으로 시간, 공간 모두 고려하여 고유한 값으로 설계한 식별자[7]이며 해당 정보도 보조기억장치에 저장되지 않는다.

예외 사항으로 어플리케이션에서 하드웨어 고유 정보를 요청했다면 다음과 같이 3개의 파일들에서 잔존할 가능성이 있다.

1. hiberfil.sys : 최대 절전 모드를 수행하기 위해 ram의 크기만큼 생성하는 파일
2. pagefile.sys : 메모리가 더 필요할 경우 보조기억장치 자원을 사용하는 파일
3. "%windir%\LiveKernelReports\win32kbase.sys-%d-%d.dump" : 충돌 발생 시 Windows에서 생성한 Dump 파일

dump 파일들은 충돌 발생 시 상황을 저장한다. 응용 프로그램에서 하드웨어 고유 정보 요청 이후 충돌이 발생하였다면 이 파일에 저장될 가능성이 있다.

dump 파일의 기록시간과 dump 파일 분석을 통해 해당 시점에서 어떤 하드웨어 고유 정보를 가지고 있는지 확인할 수 있다.

Linux는 데이터 파일, 하드웨어, 프로세스 등 모든 것을 파일로 인식되어 보조기억장치 이미징 이후 확인한 결과 하드웨어 정보를 확인할 수 있다.

Table 3. Unsaved Hardware Information

Classify	Type	Result
Ram	Part Number	None
	Serial	"
HDD	Serial	"
	WWN	"
SMBIOS	UUID	"
NIC	MAC	"

Table 4. Saved Hardware Information

Classify	Type	Result
Board	Model	%system32%\config\SYSTEM
	Serial	%system32%\config\SOFTWARE
ODD	Model	%system32%\config\SYSTEM
	Serial	"
HDD	Model	"
Monitor	Model	"
	Serial	"
NIC	Model	"

Table 5. Hardware Information

Classify	Type	Result
Board	Model	%system32%\config\SYSTEM
	Serial	%system32%\config\SOFTWARE
Ram	Part Number	None
	Serial	None
ODD	Model	%system32%\config\SYSTEM
	Serial	%system32%\config\SYSTEM
HDD	Model	%system32%\config\SYSTEM
	Serial	None
	WWN	None
Monitor	Model	%system32%\config\SYSTEM
	Serial	%system32%\config\SYSTEM
SMBIOS	UUID	None
NIC	Model	%system32%\config\SYSTEM
	MAC	None

V. 디지털 증거 수집 체계 개선 방안

5.1 하드웨어 고유 정보 수집 절차

FDE(Full Disk Encryption) 환경을 고려한 수집[8]과 Bios 설정 정보 수집[9], 하드웨어 고유 정보 등을 수집하는 디지털 증거 수집 절차는 Fig 4과 같다.

증거수집은 크게 활성 상태와 비활성 상태로 나뉘며 자세한 내용은 하드웨어 고유 정보 수집방안에서 설명한다.

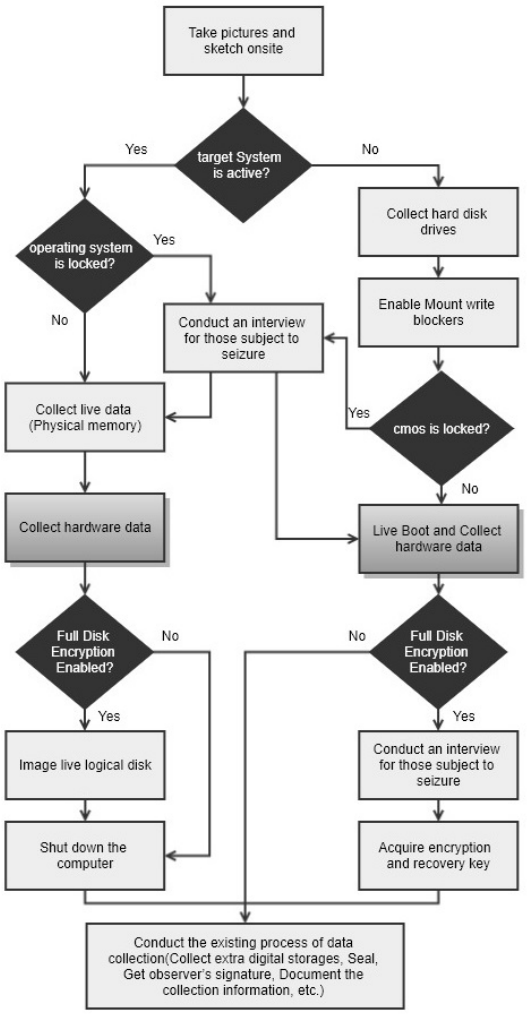

Fig. 4. Digital Evidence Acquisition Procedure

5.2 하드웨어 고유 정보 수집 방안

부팅 시 USB를 사용하거나 ODD를 통해서 부팅을 하면 Bios의 NVRAM에 부팅 정보가 저장되기 때문에 수집해야 한다[9].

조사 대상 PC가 활성 상태로 Window 시스템인 경우에는 Fig.5에서 보는 바와 같이 WMIC(Winodws Management Instrumentation Command-Line)를 사용하여 하드웨어 고유 정보를 수집할 수 있다.

그러나 저장 매체의 World Wide Name (WWN) 또는 World Wide Identifier (WWID)는 Window에서 제공하는 기능으로는 호출할 수 없다. 해당 정보를 수집하기 위해서는 디바이스 정보를 요청해야 한다. 장치를 컨트롤할 수 있는 DeviceIo Control을 호출하여 기기정보를 요청할 수 있다.

Fig.6.과 같이 디바이스 정보를 요청하여 기기 정보를 획득할 수 있다. 따라서 Serial Number, Model Name, WWN 정보의 수집이 가능하다.

조사 대상 PC가 비활성 상태일 경우에는 디지털

```
C:₩Users₩abc>wmic diskdrive get model
Model
SanDisk SD8SBAT128G1122
SanDisk Cruzer Blade USB Device


C:₩Users₩abc>wmic diskdrive get serialnumber
SerialNumber
160892400687
2005153573030E43460A


C:₩Users₩abc>wmic csproduct get uuid
UUID
2F58ED80-D7DA-11DD-A1C2-D850E655A5B3


C:₩Users₩abc>
```

Fig. 5. wmic

```
C:₩Users₩koha₩Desktop₩hanung₩ConsoleApplication1₩Debug>ConsoleApplicat
2C 00 00 00 00 00 0C 00  01 00 00 00 00 02 00 00  |  ................
02 00 00 00 50 00 00 00  30 00 00 00 A1 08 0E 00  |  ....P...0.......
01 00 00 00 A0 EC 00 00  00 00 00 00 00 00 00 00  |  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |  ................
40 00 FF 3F 37 C8 10 00  00 00 00 00 3F 00 00 00  |  @..?7.......?...
00 00 00 00 56 43 41 44  34 33 36 35 30 30 37 41  |  ....VCAD4365007A
32 31 37 30 4E 47 20 20  00 00 00 00 00 00 43 44  |  2170NG  ......CD
32 32 20 20 20 20 4E 49  45 54 20 4C 53 53 53 44  |  22    NIET LSSSD
32 43 57 42 32 31 41 30  20 34 20 20 20 20 20 20  |  2CWB21A0 4
20 20 20 20 20 20 20 20  20 20 20 20 20 20 10 80  |                ..
00 40 00 2F 00 40 00 00  00 00 07 00 FF 3F 10 00  |  .@./.@.......?..
3F 00 10 FC FB 00 10 01  B0 4B F9 0D 00 00 07 00  |  ?........K......
03 00 78 00 78 00 78 00  78 00 10 40 00 00 00 00  |  ..x.x.x.x..@....
00 00 00 00 00 00 1F 00  0E 07 84 00 4C 05 40 00  |  ............L.@.
FC 03 FF FF 6B 74 29 74  63 61 69 74 09 B4 63 61  |  ....kt)tcait..ca
7F 40 02 00 01 00 FE 00  FE FF 00 00 00 00 00 00  |  .@..............
00 00 00 00 00 00 00 00  B0 4B F9 0D 00 00 00 00  |  .........K......
00 00 01 00 00 40 00 00  CD 55 40 2E 89 4B FF 95  |  .....@...U@..K..
00 00 00 00 00 00 00 00  00 00 00 00 00 00 1C 40  |  ...............@
```

Fig. 6. DeviceIoControl

증거의 무결성을 입증하기 위해 디스크 이미징 이후 디스크에 Write Blocker를 설치한 뒤 Live CD 또는 Live USB를 통해 부팅하여 수집해야 한다.

증거 수집용 Live USB 생성 시 Persistence를 활성화 하여 USB에 저장 가능하게 한다.

생성된 USB를 통해 Live 부팅하여 하드웨어 고유 정보를 수집할 수 있다.

이에 기반을 하여 하드웨어 고유 정보 수집 스크립트를 개발하였다. Fig.7.은 개발된 스크립트이며 실행 시 장치의 고유 정보들을 출력하여 수집한다.

```
test@ubuntu:~$ python hwfinder.py
##################################
# Hardware Information Extractor #
#                                #
#                   kkoha@msn.com #
##################################

Physical Drive : 5
Drive Model: SanDisk SD7SB6S256G1122
Drive Serial Number: 151955401849
World Wide Name: 5001B44E6CD46879
Drive Model: Seagate ST3750528AS
Drive Serial Number: 5VN00VY8
World Wide Name: 5000C50013C4E014
Drive Model: INTEL SSDSC2BW120A4
Drive Serial Number: CVDA345600A71207GN
World Wide Name: 55CD2E404B8995FF
Drive Model: WDC WD2003FZEX-00Z4SA0
Drive Serial Number: WD-WMC1F1189178
World Wide Name: 50014EE0AE55B4B
Drive Model: SanDisk pSSD
Drive Serial Number: 007e33b03
World Wide Name: 5001B440E30733B

Physical RAM : 2
Part Number: M378B1G73BH0-CK0
Serial Number: 95AEF8A0
Part Number: M378B1G73BH0-CK0
Serial Number: 95AEF89A

Physical ODD : 0

Physical NIC : 1
product: 82545EM Gigabit Ethernet Controller (Copper)
MAC Address: 00:0c:29:c5:05:49
```

Fig. 7. Hardware Infomation

VI. 결 론

디지털 포렌식 관점에서 암호화된 데이터들은 중요한 분석 대상이다.

앞서 살펴본 바와 같이 현재 증거 수집 절차에서는 저장매체에 대해서만 초점을 맞추고 있으며 저장매체에 저장되지 않는 정보를 고려하지 않았다.

본 논문에서는 저장매체에 저장되지 않는 하드웨어의 고유 정보에 대해 실험하였으며 하드웨어 고유 정보 수집을 통한 증거 수집 절차를 제시하였다.

앞으로 기술적·관리적 보호조치의 암호화 기술사용은 증가할 것이며 이를 의무화 시키는 규제 또한 강화될 전망이다.

그러나 아직까지 사법기관이나 학계에서 하드웨어 고유 정보에 대한 수집에 대해서 고려하고 있지 않는 실정이다.

따라서 디지털 포렌식을 위한 데이터 수집 시에 하드웨어 고유 정보 수집도 반드시 병행하여 실시해야 한다.

References

[1] Gal Beniamini, "TrustZone TEEs - An Attacker's Perspective", BlueHat IL 2017, 2017.01.24.

[2] Supreme Prosecutor's Office, "Regulation for the collection, analysis and management of digital evidence" 2017. 3.1.

[3] National Police Agency, "Digital Evidence Processing Standards Guidelines", 2006.12.28.

[4] National Police Agency, "Rules for the collection and processing of digital evidence", 2017.09.01.

[5] Sammons, J, "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics "USA:Syngress, pp.70-71, 2012

[6] Telecommunications Technology Association, "Guidelines for Collection, Acquisition and Preservation of Digital-Evidence", TTAS.KO-12.0058/R1, 2017. 12.13.

[7] Distributed Management Task Force, Inc, "System Management BIOS (SMBIOS) Reference Specification", DSP0134, 2017.01.13

[8] Sung-min Jang, Jung-heum Park and Chan-ung Pak, "The Research for Digital Evidence Acquisition Procedure within a Full Disk Encryption Environment", KIISC, 25(1), pp. 39-48, Feb. 2015

[9] S. H. Jeong, Y. H. Lee, and S. J. Lee, "A Study of Acquisition and Analysis on the Bios Firmware Image File in the Digital Forensics," KIPS

Transactions on Computer and Communication Systems, Vol.5, No.12, pp.491-498, 2016, DOI: 10.3745/KTCCS.2016.5.12.491.

〈저자소개〉

박 찬 웅 (Chan-ung Pak) 학생회원
2013년 2월: 건양대학교 정보보호학과 졸업
2013년 8월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식, 역공학, 모바일 포렌식

이 상 진 (Sang-jin Lee) 종신회원
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
2017년 3월~현재: 고려대학교 정보보호대학원 원장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수