사물인터넷융복합논문지 Vol. 11, No. 2, pp. 83-88, 2025 https://doi.org/10.20465/KIOTS.2025.11.2.083

# 자기 암호화 저장장치의 은닉 영역에 대한 포렌식 분석

김병국[1], 류갑상[2*]
[1]동신대학교 컴퓨터학과 박사과정, [2]동신대학교 컴퓨터학과 교수

# Forensic Analysis of Hidden Areas in Self-Encrypting Storage Devices

Byung-Gook Kim[1], Gab-Sang Ryu[2*]
[1]Doctor's Course, Student, Dept. of Computer Science, Dongshin University
[2]Professor, Dept. of Computer Science, Dongshin University

**요 약** 본 논문은 TCG 스토리지 표준 규약을 준수하는 자기 암호화 저장장치의 은닉 영역에 집중한다. 일반적으로 데이터 저장장치는 최종 사용자에게 제공되는 읽기, 쓰기 명령어로 접근 가능한 영역 외에도, HPA, DCO 등 읽기, 쓰기 명령으로 접근 불가능한 은닉 영역이 존재한다. 이러한 은닉 영역은 일반적인 산업용 도구에 의해 감지되지 않을 수 있으며, 이는 디지털 포렌식 조사자나 기업 보안 관리자에게 잠재적인 보안 위협이 될 수 있다. 은닉 영역은 데이터 저장장치에 대한 이미지 획득이 물리적인 드라이브의 실제 복사본이 아닐 위험을 크게 증가시키고 데이터 은닉으로 인해 불완전하거나 오류가 있는 조사 결과를 초래할 수 있다. 또한 일반적인 산업 도구를 이용한 삭제 절차에서는 이 영역의 데이터가 제거되지 않아, 민감한 정보가 유지되는 문제가 발생할 수 있다. 본 논문에서는 TCG 스토리지 표준 규약을 준수하는 자기 암호화 저장장치에 존재하는 고유한 은닉 영역에 대한 소개를 제공한다. 다음으로 오픈 소스 및 무료 도구를 사용하여 사용자가 해당 은닉 영역에 접근, 수정 및 기록할 수 있음을 확인한다. 마지막으로 이러한 은닉 영역이 디지털 포렌식 조사 과정에 미치는 잠재적 영향과 이에 대응하기 위한 방안을 논의한다.

**주제어 :** 저장시스템, 데이터 은닉, 자기 암호화 드라이브, 디지털 포렌식

**Abstract** This paper focuses on the hidden areas of self-encrypting drives (SEDs) that comply with the Trusted Computing Group (TCG) storage specification. In general, data storage devices include not only areas accessible via standard read and write commands provided to end-users but also hidden areas such as the Host Protected Area (HPA) and Device Configuration Overlay (DCO), which are inaccessible through conventional commands. These hidden areas may not be detectable by standard industrial tools, posing potential security risks to digital forensic investigators and corporate security administrators. The existence of such hidden areas significantly increases the risk that a forensic image of the storage device may not represent a true physical copy, potentially leading to incomplete or inaccurate investigative results due to concealed data. Moreover, data residing in these areas may persist despite deletion procedures carried out using typical industrial tools, resulting in the retention of sensitive information. This paper introduces the unique hidden areas present in self-encrypting drives compliant with the TCG storage specification. It further demonstrates, through the use of open-source and freely available tools, that users can access, modify, and write data within these hidden regions. Finally, the paper discusses the potential implications of these hidden areas in digital forensic investigations and proposes corresponding countermeasures.

**Key Words :** Storage System, Data Hiding, Self-Encrypting Drive, Digital Forensic

*교신저자 : 류갑상(gsryu@dsu.ac.kr)
접수일: 2025년 03월 14일 수정일: 2025년 04월 01일 심사완료일 2025년 04월 16일

## 1. 서론

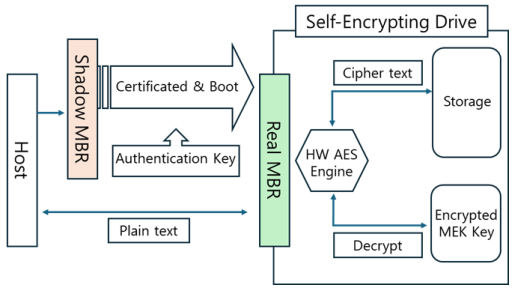
TCG 스토리지 SSC(Security Subsystem Class)는 신뢰 컴퓨팅 그룹이 정의한 디스크 암호화 표준이다. 주로 자기 암호화 드라이브(Self-Encrypting Drive)와 관련된 기술로, 보안성이 강화된 저장장치의 관리 및 보호를 위한 표준을 제공하고, 데이터를 저장하는 하드 디스크 드라이브 또는 SSD에서 데이터를 보호하고, 암호화 키 관리, 데이터 무결성 및 액세스 제어를 개선하기 위한 기술적 방법을 제공한다[1]. Shadow MBR(Master Boot Record) 영역과 DataStore 영역은 TCG 표준을 준수하는 SSD나 하드 디스크 드라이브에 존재하는 은닉 영역으로, 일반적으로 사용자나 바이오스, 운영체제에서 접근하거나 수정할 수 없도록 설계되어 있다. 이 영역은 자기 암호화 드라이브에서 부팅 전 인증을 위한 프로그램, 진단 도구, 시스템 설정값 등 중요한 정보를 저장하는 데 사용될 수 있지만, 데이터 은닉 등 다른 목적으로 활용될 가능성 또한 존재한다. 따라서 데이터 은닉 관점에서 디지털 포렌식 조사의 중요한 고려 사항이 된다[2,3]. 본 논문에서는 Shadow MBR 영역 및 DataStore 영역의 특성, 포렌식 분석에 미치는 영향, 그리고 전통적인 방식으로 저장장치의 데이터를 관리하는 과정에서 발생할 수 있는 취약점들에 대하여 실험을 통해 분석한다[4,5].

## 2. 배경 및 취약점

### 2.1 자기 암호화 저장장치의 구조와 특징

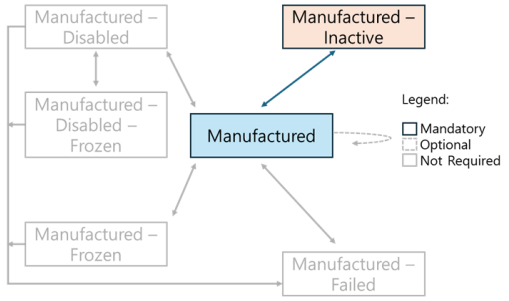
신뢰 컴퓨팅 그룹(Trusted Computing Group)은 컴퓨팅 장치의 신뢰성과 안전성을 제고시키기 위한 산업 표준을 수립하고 공표하는 단체로서, 공표된 표준은 업계에서 널리 사용된다. 신뢰 컴퓨팅 그룹 산하 워크 그룹 중 스토리지 워크 그룹(SWG)은 Opal SSC 등 다양한 하위 시스템 클래스를, 저장장치를 위한 보안 관리 프로토콜을 위한 규약으로 제정하였으며, 이러한 규약을 준수하는 자기 암호화 저장장치는 개인용 컴퓨터와 노트북에 사용되는 장치에 주로 적용된다[6]. 자기 암호화 저장장치의 데이터 암호화는 호스트의 도움 없이 저장장치 자체적으로 수행하며, 데이터 암호화 키는 장치 내부의 안전한 영역에 저장하여 관리한다.[7-10].

Fig. 1은 자기 암호화 저장장치의 구조를 보여주고 있다. 자기 암호화 저장장치는 전체 디스크 암호화를 수행




[Fig. 1] Architecture of Self-Encrypting Drive

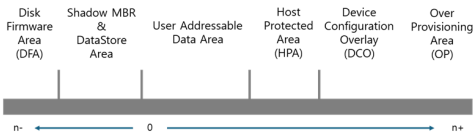
하여 저장된 데이터를 보호한다. 따라서 저장시스템의 부팅 과정에 앞서 사전 부트 인증 과정(Pre-Boot Authentication)을 통해 암호화된 데이터의 암호 해독키에 접근할 수 있도록 하는 접근 제어 과정이 선행되어야 한다[11]. 사전 부트 인증을 수행하기 위한 프로그램을 저장하기 위하여 Shadow MBR로 불리는 은닉 영역이 제공된다. 또한 ATA 표준 사양에 명시된 TRUSTED SEND 및 TRUSTED RECEIVE 명령을 지원한다. 이를 통해 바이오스, 운영체제 혹은 응용 프로그램에서 자기 암호화 기능의 설정 및 제어가 가능하다[12-14].




[Fig. 2] Life cycle state diagram of manufactured SPs

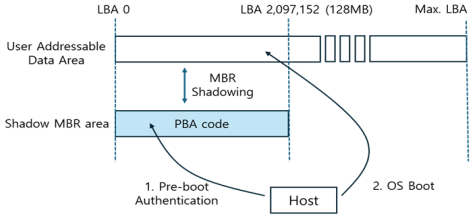
Fig. 2는 TCG 저장장치의 접근 제어를 위한 Locking SP의 생애 주기를 보여주고 있다. TCG Opal SSC를 지원하는 저장장치는 활성화(Manufactured) 혹은 비활성화(Manufactured-Inactive)로 구분하여 전환할 수 있다. 저장장치가 제조된 초기 상태에서의 Locking SP는 비활성화 상태이며, 저장장치의 소유자가 보안 관리 권한을 획득(Take Ownership)하는 과정을 통하여 Locking SP를 활성화하여 핀 설정 및 사용자 접근 영역에 대한 읽기 쓰기 접근 권한을 설정할 수 있다. 저장장치의 Locking SP가 활성화된 자기 암호화 저장장치는 DataStore로 불리는 은닉 영역을 호스트에게 제공하여, 호스트가 저장장치의 관리를 위해 생성한 정보를 저장할 수 있도록 한다.

## 2.2 자기 암호화 저장장치의 은닉 영역




[Fig. 3] Overview of the disk areas

Fig. 3은 자기 암호화 드라이브의 데이터 저장 영역을 구분하여 표현하고 있다. 저장장치에는 다양한 은닉 영역이 존재한다[15,16]. HPA(Host Protected Area)는 하드 디스크 드라이브나 SSD의 특정 영역으로, 사용자에게 보이지 않는 은닉 영역이다. ATA-4 표준에서 추가된 이 기능은 장치 제조사나 시스템 관리자가 설정할 수 있으며, 사용자가 접근할 수 없도록 보호된다. 이 영역은 일반적으로 바이오스, 시스템 복구 도구, 펌웨어 업데이트, 복구 파티션 또는 특정 시스템 정보를 저장하기 위한 용도로 사용된다. 사용자는 기본적으로 이 영역에 접근할 수 없으며, 특수한 명령어나 펌웨어를 통해서만 접근이 가능하다. 일반적인 운영체제나 사용자 인터페이스에서는 이 영역을 볼 수 없다. 다음으로 DCO(Device Configuration Overlay)는 디스크의 설정을 변경하기 위한 은닉 영역이다. ATA-6 표준에서 추가된 이 기능은 논리 블록 주소를 원하는 값으로 설정하여 저장장치의 용량을 줄이는 기능을 수행한다. 이러한 기능은 장치 제조사가 한 가지 용량의 저장장치를 제작하여 고객사의 다양한 요청에 대응할 수 있도록 유연성을 제공한다. OP(Over Provisioning)은 저장장치에서 사용 가능한 용량보다 더 많은 물리적 용량을 할당하여, 장치의 성능과 내구성을 향상시키는 기술이다. 주로 SSD에서 사용되며, OP 영역으로 할당된 여유 블록을 사용하여 SSD의 수명 연장, 성능 향상, 가비지 컬렉션 및 웨어 레벨링의 최적화를 수행한다. Shadow MBR 영역은 TCG 스토리지 표준 규약을 준수하는 자기 암호화 저장장치에서 제공하는 은닉 영역으로, 사전 부트 인증을 수행하기 위한 프로그램을 저장하기 위한 용도로 사용된다. 이 영역은 바이트 단위로 접근 및 읽기, 쓰기가 가능하며 최소한 128MB (0x08000000) 이상의 공간을 제공해야 하며, 관리자 권한의 계정으로 읽기 및 쓰기가 가능하다. DataStore 영역 또한 TCG 스토리지 표준을 준수하는 자기 암호화 저장장치에서 제공하는 은닉 영역으로, 호스트가 저장장치의 관리를 위해 생성한 정보를 저장하는 용도로 사용된다. 이 영역 또한 바이트 단위로 읽기 및 쓰기가 가능하며 최소한 10MB (0x00A00000) 이상의 공간을 제공해야 하며, 접근을 위해 기본적으로 관리자 권한의 계정이 필요하지만, 접근 권한 변경을 통하여 일반 사용자 계정의 접근이 가능하다. 사용자가 접근 가능한 LBA(Logical Block Addressing) 영역 및 HPA 영역을 제외한 나머지 영역은 일반적인 읽기, 쓰기 명령으로 접근이 불가능하며, Shadow MBR 영역과 DataStore 영역은 TRUSTED SEND 및 TRUSTED RECEIVE 명령으로 접근이 가능하다. 그 외의 영역에 접근하려면 프로그래머블 입출력을 사용하여 저장장치의 입출력 포트로 명령을 직접 전송하여 제어해야 한다. 이 명령은 저장장치 제조사 고유의 명령으로, 일반적으로 공개되지 않는다.




[Fig. 4] Pre-boot Authentication with a SMBR

Fig. 4는 자기 암호화 저장장치의 사전 부트 인증과정을 표현하고 있다. 사전 부트 인증과정은 저장시스템이 부팅되기 전에 사용자 인증을 수행하여, 저장시스템에 대한 무단 접근을 방지한다. 이를 통해 해커나 악의적인 사용자가 시스템에 접근하여 중요한 데이터를 조작하거나 탈취하는 것을 막을 수 있다. 자기 암호화 저장장치는 전체 디스크 암호화(Full Disk Encryption)를 사용하여 저장된 데이터를 보호한다. 따라서 운영체제를 포함한 전체 데이터가 암호화 되어 있으므로 사전 부트 인증과정을 통해 접근 권한을 획득한 후 데이터 암호화 키를 생성하고 데이터를 복호화하는 과정을 마쳐야 운영체제를 부팅 할 수 있다. Shadow MBR 영역에 사전 부트 인증을 수행하기 위한 프로그램을 저장하기 위해서는 접근 제어를 위한 Locking SP를 활성화해야 한다. 프로그램의 저장 및 정상적인 설정이 완료된 자기 암호화 저장장치에 전원을 인가하여 시큐어 부트 프로세스가 시작되면, 0번 LBA부터 시작하여 총 128MB 영역에 해당하는 데이터 영역을 Shadow MBR 영역으로 섀도잉하여, 바이오스는 사전 부트 인증 프로그램을 실행하고 자기 암호화 저장장치의 인증과정을 수행할 수 있다. 하지만 이러한 은닉 영역은 데이터 은닉과 같은 다른 목적을 위한 공간으로 사용될 가능성이 존재한다. 이 영역에 은닉을 위한 데이터를 저장한 후 Shadow MBR 영역의 섀도잉 기능을 비활성화하면, 저장장치에 새로운 전원 사이클을

발생시켜도 MBR 섀도잉 과정이 발생하지 않는다. 즉 호스트는 일반적인 읽기, 쓰기 명령어로는 Shadow MBR 영역에 은닉된 데이터를 확인할 수 없는 상태가 된다. 만약 사전 부트 인증과정 없이도 운영체제가 부팅 가능한 상태로 설정한다면, Shadow MBR 영역이 사용자 영역에 노출되지 않으므로 은닉된 데이터의 존재 여부에 대한 인지를 어렵게 만들 수 있다.

### 2.3 데이터 삭제 명령과 정책

ATA 표준에서 지원하는 SECURITY ERASE 명령은 사용자가 접근 가능한 LBA 영역을 삭제 대상으로 한정한다. 따라서 Shadow MBR 영역, DataStore 영역 등 자기 암호화 저장장치에서 제공하는 추가적인 은닉 영역은 삭제 대상에서 제외된다. 이 명령은 일반 모드와 향상된 삭제 모드를 제공하며, 일반 모드에서는 현재 할당된 사용자 데이터 영역에 대한 삭제만을 수행하고, 강화 모드에서는 이전에 할당되었으나 현재는 액세스할 수 없게 된 물리적 섹터까지 삭제를 수행한다. 자기 암호화 저장장치의 경우 일부 제조사에서는 강화 모드에서 암호화 삭제(Cryptographic Erase) 명령을 수행하도록 구현되어있다. 또한 데이터 삭제 관점에서의 실제 동작은 제조사 정책에 따라 다르며, 논리 블록과 물리 블록 사이의 매핑만을 삭제하고 데이터 블록의 삭제를 보장하지 않을 수 있다. ATA 표준에서 지원하는 SANITIZE 명령 또한 사용자가 접근 가능한 논리 블록 주소 영역을 삭제 대상으로 한정하지만, 이전에 할당되었으나 현재는 접근할 수 없게 된 물리적 섹터까지 삭제를 수행하며 데이터 블록의 삭제를 보장한다는 점이 다르다. 그러나 Locking SP가 활성화된 상태에서는 SECURITY ERASE 명령과 SANITIZE 명령은 비활성화되어 실행 불가능한 상태가 된다. 따라서 Locking SP가 제공하는 Revert 명령을 사용하여 데이터를 삭제해야 한다. 이 명령은 데이터 블록을 물리적으로 삭제하지 않고 데이터 블록의 암호화 키를 삭제하는 암호화 삭제를 수행한다. 자기 암호화 저장장치에서는 일부 메타 영역을 제외한 모든 영역이 암호화 키로 암호화되어 있으므로, Shadow MBR 영역과 DataStore 영역의 암호화 삭제를 보장한다.

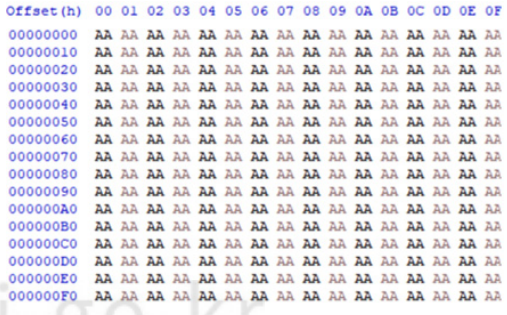
## 3. 실험 및 분석

실험에 사용된 Samsung 870 EVO SSD는 TCG Opal SSC를 지원하는 자기 암호화 저장장치이다. Table 1에 TCG Opal SSC를 지원하는 주요 제조사의 SSD 제품을 나열하였다.

〈Table 1〉 Shortlist of disks that are compatible with TCG Opal SSC

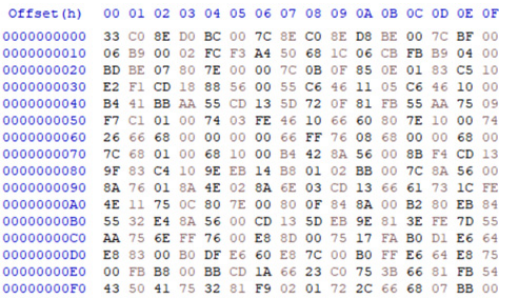
| Make | Model | Bus |
|---|---|---|
| Samsung | 870 EVO | SATA |
| SKHynix | HFS001TDE9X081N | NVMe |
| WDC | SANDISK SSD G5 BICS4 | SATA |
| Kingston | SUV500M8/120G | NVMe |
| Segate | SEAGATE FIRECUDA 520 | NVMe |
| Intel | SSDPEKKF256G8 | NVMe |
| Crucial | CT1000T700SSD3 | NVMe |

저장장치의 설정 상태를 확인할 수 있는 레벨 0 디스커버리 프로토콜을 수행한 후 응답 헤더의 내용을 확인하여 TCG Opal SSC의 접근 제어를 위한 Locking SP의 활성화 여부, Shadow MBR 기능이 활성화 여부 및 MBR 섀도잉 동작 상태를 파악할 수 있다. 저장장치의 초기 상태에서는 Locking Enabled 비트가 '0'이므로 Locking SP가 비활성화 상태임을 확인할 수 있다. SP를 활성화하면, 해당 비트가 '1'로 변경되므로 이를 통하여 SP의 활성화 여부를 확인할 수 있고, Shadow MBR 영역에는 128MB 크기의 데이터를 은닉할 수 있으며, DataStore 영역에는 10MB 크기의 데이터를 은닉할 수 있다. Shadow MBR 영역에 데이터를 은닉한 후 MBR Enabled 비트를 '1'로 설정하면 섀도잉 기능이 활성화되며, MBR Done 비트를 '0'으로 설정하거나 저장장치에 새로운 전원 사이클을 인가하면 MBR 영역이 Shadow MBR 영역으로 대체되고, '1'로 설정하면 복원된다. 따라서 MBR Enable 비트를 '0'으로 설정하면 섀도잉 기능이 활성화되지 않으므로, 사용자가 접근 가능한 LBA 영역에 노출되는 경우가 발생하지 않고, 데이터는 은닉된다.



[Fig. 5] Dump of LBA 0 when MBR Enabled = 1

반대로 MBR 영역이 섀도잉 상태로 전환하면 Fig. 5와 같이 호스트에서 읽기 명령어로 섀도잉된 MBR 데이터를 확인할 수 있다.




[Fig. 6] Dump of LBA 0 when MBR Enabled = 0

섀도잉 기능을 비활성화하면 Fig. 6와 같이 호스트에서 읽기 명령어로 운영체제의 실제 MBR 데이터를 확인할 수 있다. 실험의 마지막 과정으로 Revert 명령을 수행하였으며, Shadow MBR 영역의 데이터가 삭제되었음을 확인하였다. Revert 명령 수행 후 데이터의 패턴이 랜덤한 값으로 변경되었으며, 이는 데이터를 암호화하는 키가 삭제 후 재생성 되었음을 의미한다. 위 실험 과정은 TCG Opal SSC 기능을 제어할 수 있는 오픈 소스 및 무료 도구인 SEDutil을 사용하여 Tab1e 2에 기술된 절차로 수행하였다.

〈Table 2〉 Experimental Procedure

| Sequence & Details | Note |
|---|---|
| Level 0 Discovery | |
| Activate | |
| Injection of PBA Image | pattern = 0xAA |
| Set MBREnable to '1' | |
| Perform a power cycle | |
| Read LBA 0 | Fig. 5 |
| Set MBREnable to '0' | |
| Perform a power cycle | |
| Read LBA 0 | Fig. 6 |
| Revert | |

## 4. 결론

본 연구에서는 TCG 스토리지 표준 규격을 준수하는 자기 암호화 저장장치에 존재하는 고유한 은닉 영역의 특성을 확인하고, 이를 데이터 은닉 관점에서 분석하였다. 또한 Shadow MBR 영역에 데이터를 삽입한 후, MBR Enabled 비트를 '0'으로 설정 및 유지함으로써 해당 데이터를 은닉된 상태로 보존할 수 있음을 실험을 통해 확인하였다. 이는 정상적인 운영 시나리오에서, 사전 부트 인증을 위한 프로그램을 삽입한 후 MBR Enabled 비트를 '1'로 설정하여 영역의 접근을 허용하는 방식과는 상이한 결과이다. 이러한 잠재적 보안 취약점을 보완하기 위한 방안으로, MBR Enabled 비트가 '0'인 상태에서 데이터 삽입이 발생한 후 이를 '1'로 변경하기 전 새로운 전원 사이클이 인가되는 경우, 또는 MBR Enabled 비트가 '1'인 상태에서 '0'으로 전환되는 시점에 해당 영역의 데이터를 삭제하는 보안 정책의 적용이 효과적인 대응책이 될 수 있다.

## REFERENCES

[1] "TCG Storage Architecture Core Specification," Trusted Computing Group, 2025.

[2] P.G.Hong, D.S.Lee and D.H.Kim "A Study on Analysis of Hidden Areas of Removable Storage Device from a Digital Forensics Point of View," Proceedings of the Korean Institute of Information and Commucation Sciences Conference, Vol.25, No.1, pp.111-113, 2021.

[3] N.Y.Ahn and D.H.Lee, "Forensic Issues and Techniques to Improve Security in SSD With Flex Capacity Feature," IEEE Access, Vol.9, pp.167067-167075, 2021.

[4] E.Akbal, O.F.Yakut, S.Dogan, T.Tuncer and F.Ertam, "A Digital Forensics Approach for Lost Secondary Partition Analysis using Master Boot Record Structured Hard Disk Drives," Sakarya University Journal of Computer and Information Sciences, Vol.4, No.3, pp.326-346, 2021.

[5] J.P.Mehta and D.Rathod, "Towards Enablement Of Efficient Forensics Of Encrypted Storage Devices Such As HDDs and SSDs," International Journal of Computer Sciences and Engineering, Vol.6, No.9, pp.467-473, 2018.

[6] "TCG Storage Security Subsystem Class: Opal Specification," Trusted Computing Group, 2025.

[7] E.Casey, G.Fellows, M.Geiger and G.Stellatos, "The growing impact of full disk encryption on digital forensics," Digital Investigation, Vol.8, No.2, pp.129-134, 2011.

[8] L.Khati, N.Mouha and D.Vergnaud "Full Disk Encryption: Bridging Theory and Practice," Topics in Cryptology–CT-RSA 2017, Vol.10159, No.1, pp.241-257, 2017.

[9] I.V.Kalutskiy, A.G.Spevakov and V.A.Shumaylova, "Method for Ensuring Data Privacy on the Computer's Internal Hard Disk," Advances in Automation II,

Vol.729, No.1, pp.543-549, 2022.

[10] J.S.Kim, M.G.Bae, Y.S.Chu, M.C.Park, D.W.Park, D.W.Jung and S.Y.Cho, "Self-Encrypting Drive Evolving Toward Multitenant Cloud Computing," Computer, Vol.57, No.2, pp.79-90, 2024.

[11] R.Benadjila, L.Khati and D.Vergnaud, "Secure storage—Confidentiality and authentication," Computer Science Review, Vol.44, No.100465, pp.1-36, 2022.

[12] "AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS)," International Committee for Information Technology Standards, 2025.

[13] "TCG Storage Interface Interactions Specification (SIIS)," Trusted Computing Group, 2023.

[14] P.Patil and B.Jagdale "Analyzing the Common Host Interfaces Used with SSDs," Applied GIS, Vol.4, No.3, pp.1-4, 2016.

[15] H.Suthar and P.Sharma "Method for Extracting Data from an Overprovisioned SSD," 2022 IEEE Pune Section International Conference, pp.1-6, 2022.

[16] H.S.Lee "Performance analysis and prediction through various over-provision on NAND flash memory based storage," Journal of Digital Convergence, Vol.20, No.3, pp.343-348, 2022.

김 병 국(Byung-Gook Kim) [종신회원]

■ 2006년 7월 ~ 2021년 4월 : 삼성전자 DS부문 책임연구원
■ 2022년 8월 ~ 현재 : 배화여자대학교 소프트웨어공학과 교수
■ 2025년 3월 ~ 현재 : 동신대학교 컴퓨터학과 박사과정

〈관심분야〉
사물인터넷, 스토리지 보안, 디지털 포렌식

류 갑 상(Gab-Sang Ryu) [종신회원]

■ 1985년 3월 ~ 1996년 2월 : 한국기계연구원, 선임연구원
■ 1996년 3월 ~ 현재 : 동신대학교 컴퓨터학과 교수
■ 2020년 1월 ~ 2021년 1월 : 한국소프트웨어품질안전포럼, 의장

〈관심분야〉
블록체인, SW품질, 정보처리