Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1059

하드디스크 드라이브 ATA 패스워드에 관한 연구

이 주 영,† 이 상 진‡
고려대학교 정보보호대학원

A Study on Hard Disk Drive ATA Passwords

Ju-young Lee,† Sang-jin Lee‡
Graduate School of Information Security, Korea University

요 약

하드디스크에 설정되는 패스워드는 일반적으로 잘 알려지지 않았을 뿐만 아니라, 설정되면 데이터에 접근이 불가능하기 때문에 포렌식 조사를 방해하는 목적으로 사용될 수 있다. 하드디스크의 패스워드를 해제하기 위해서는 PC-3000과 같은 고가의 도구가 필요한데 이는 조직에 비용 부담을 주며, 해당 도구에 익숙지 않은 조사관에게는 조사 시 어려움을 준다. 본 논문에서는 하드디스크 패스워드를 해제하기 위해 필요한 내용을 정리하고 고가의 도구 없이 하드디스크에 설정된 패스워드를 해제하는 방법들을 제안한다. 그리고 이 중 특정 제조사에 특화된 방법을 이용하여 패스워드를 획득하고 하드디스크의 잠금을 해제하는 절차를 제시한다.

ABSTRACT

Hard disk passwords are commonly not well known. If the passwords are set, forensic investigators are not allowed to access data on hard disks, so they can be used to obstruct investigations. Expensive tools such as PC-3000 are necessary for unlocking such hard disk passwords. But it would be a burden on both organizations that should pay for these tools and forensic investigators that are unfamiliar with these tools. This paper discusses knowledge required for unlocking hard disk passwords and proposes methods for unlocking the passwords without high-priced tools. And with a vendor-specific method, this paper provides procedures for acquiring passwords and unlocking hard disk drives.

Keywords: ATA Password, Unlock Hard Disk Drive, System Area, Anti-anti Forensics

I. 서 론

삼성 BIOS와 같은 일부 BIOS는 하드디스크 드라이브에 패스워드를 설정할 수 있는 기능이 있다. 이는 ATA 장치에 설정되는 패스워드인데 패스워드가 설정된 하드디스크는 잠금 상태가 되어 패스워드를 알지 못하면 데이터 영역에 접근이 불가능해진다. 또한 잠금 상태의 하드디스크는 이미징 장비로도 이미징을 할 수 없다. 때문에 하드디스크 패스워드는 포렌식 조사를 방해하는 안티-포렌식 목적으로 사용될 수 있다.

ATA 패스워드를 이용한 안티-포렌식 기법에 대응하기 위해서는 하드디스크 잠금을 해제할 수 있는 방법에 대한 연구가 필요하다. 본 논문에서는 하드디스크 드라이브에 설정된 ATA 패스워드의 메커니즘과 이를 해제하는 방법을 설명한다.

또한 Western Digital 하드디스크 드라이브의 패스워드를 추출하는 프로그램을 작성하여 본 논문에서 제시한 방법이 실제로 적용 가능함을 증명한다.

접수일(2015년 6월 3일), 수정일(2015년 9월 1일),
게재확정일(2015년 9월 14일)
† 주저자, rnajylee@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

II. 관련 연구

하드디스크 드라이브 보안에 대한 연구는 하드디스크의 특정 공간에 데이터를 숨기는 방법에 대한 연구가 주를 이루었다. Huw Read 등[1]은 하드디스크 펌웨어를 다른 펌웨어로 바꿈으로써 하드디스크 드라이브의 종류와 크기를 속여 데이터를 숨기는 방법을 연구했다. Mayank R. Gupta 등[2]은 HPA(Host Protected Area)와 DCO(Device Configuration Overlay)를 조작한 데이터 은닉 가능성을 제시했으며 Harald Baier 등[3]은 DCO 영역을 줄여서 줄인 만큼의 공간에 데이터를 숨길 수 있음을 보였다. Iain Sutherland 등[4]과 Gareth Davies 등[5]은 하드디스크의 결함 섹터를 관리하는 리스트를 조작하여 데이터를 숨기는 방법을 제시했다.

ATA 패스워드 메커니즘에 대한 연구 중에서 Julian Knauer 등[6]은 ATA 패스워드에 대한 무차별 대입 공격이나 펌웨어를 조작하여 잠금을 해제할 수 있다는 것을 언급했다.

한편, HDDGURU는 하드디스크와 관련된 포럼으로 MHDD라는 하드디스크 진단 도구를 무료로 제공한다. MHDD에는 스크립트를 추가할 수 있는데, 이 포럼에서 작성된 스크립트[7][8]를 실행하면 Western Digital의 구모델 하드디스크의 패스워드가 저장된 모듈을 추출할 수 있으나 최신 모델 하드디스크에 대해서는 오류가 발생한다.

III. ATA 메커니즘과 ATA 패스워드

3.1 ATA 명령어 세트

ATA 명령어 세트는 ATA 장치와 통신하기 위한 인터페이스를 제공한다. 이 명령어들은 AT Attachment ATA/ATAPI Command Set (ATA ACS) 표준 문서[9][10]에 정의되어 있다. 이외에도 하드디스크 제조사별 고유의 명령어도 존재한다. ATA 명령어는 하드디스크 내의 레지스터에 특정한 값을 설정해줌으로써 사용 가능하다.

ATA/ATAPI-7 에서는 Feature, Count, LBA Low/Mid/High, Device, Command 레지스터가 사용되고, ATA-8 ACS 이상부터는 Feature, Count, LBA, Device, Command 레지스터가 사용된다. ATA/ATAPI-7의 LBA Low/Mid/High 레지스터는 ATA-8 ACS에서 하나의 LBA 레지스터로 통합되었다.

예를 들어 ATA 장치의 정보(모델명, 펌웨어 버전, 용량 등)를 확인하는 IDENTIFY DEVICE 명령어를 장치에 보내려면 command 레지스터를 ECh로 설정해야 한다. 이 명령어를 받은 ATA 장치는 장치 정보가 담긴 512바이트를 돌려준다.

3.2 ATA 보안 상태

ATA 장치는 SEC0부터 SEC6까지 보안 상태가 변할 수 있으며 이는 ATA ACS 표준 문서에 정의되어 있다. Fig. 1은 ATA 보안 상태를 나타낸 도식이다[9]. 각 상태에서 다른 상태로의 전환은 Fig. 1에 표시된 ATA 명령어를 통해 일어나거나 장치의 전원을 켜고 끔으로써 일어난다.

SEC1이 일반적인 하드디스크 상태이며 SEC4가 하드디스크에 패스워드가 설정된 상태다. SEC1에서 SECURITY SET PASSWORD 명령어로 패스워드를 설정하면 SEC5 상태가 되며 하드웨어 리셋을 통해 하드디스크가 SEC4 상태가 된다.

이처럼 설정된 하드디스크 패스워드를 해제하려면 SECURITY UNLOCK 명령어로 SEC5 상태로

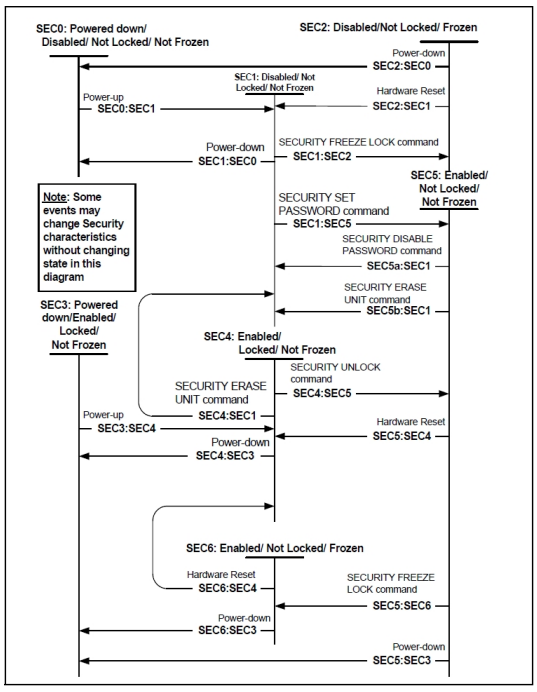

Fig. 1. Security State Diagram

전환한 뒤 SECURITY DISABLE PASSWORD 명령어로 SEC1 상태로 만들어야 한다.

3.3 ATA 패스워드

ATA 패스워드는 사용자 패스워드와 마스터 패스워드가 있다. 사용자 패스워드는 일반적으로 BIOS 상에서 사용자가 설정한 패스워드이고, 마스터 패스워드는 제조사에서 하드디스크에 기본적으로 설정해 놓은 패스워드이다.

BIOS에 하드디스크 패스워드를 설정하는 기능이 있는 컴퓨터와, BIOS에 이러한 기능이 없는 컴퓨터에 각각 잠긴 하드디스크를 추가적으로 연결하고 부팅을 할 때에는 차이가 있다.

먼저 BIOS에 하드디스크 패스워드를 설정하는 기능이 있는 경우, 잠긴 하드디스크를 연결하고 부팅하면 Fig. 2처럼 패스워드를 묻는 과정을 거쳐야 운영체제가 부팅된다.

반면 BIOS에 하드디스크 패스워드를 설정하는 기능이 없는 경우, 잠긴 하드디스크를 연결하더라도 패스워드를 묻는 과정을 거치지 않고 부팅이 된다. 그러나 운영체제는 잠긴 하드디스크를 물리적으로 인식할 뿐 실제 데이터를 가져오지 못한다.

또한 패스워드가 설정된 하드디스크는 이미징 장치로 이미징을 할 수 없다. Fig. 3은 Tableau TD3 Imager에서 이미징을 시도했을 때 나타나는

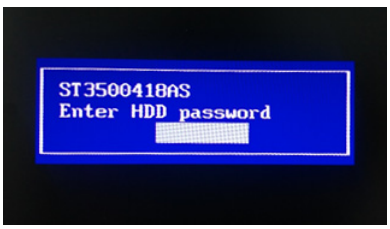

Fig. 2. HDD Password Verification

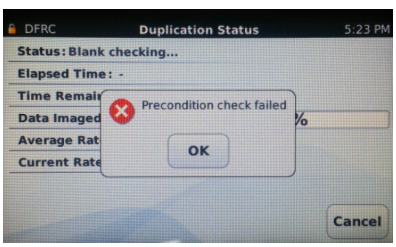

Fig. 3. TD3 Imager Error

오류 화면이다.

ATA 패스워드는 하드디스크 내 SA 모듈에 저장된다. SA란 HDD 논리기판에 있는 CPU가 드라이브를 구동하기 위해 사용하는 정보로, Fig. 4처럼 모듈화되어 있다[11].

IV. ATA 패스워드 해제 방법

ATA 패스워드를 해제하는 방법은 펌웨어를 플래싱하는 방법, 마스터 패스워드를 이용하는 방법, 제조사 고유의 방법을 이용하여 사용자 패스워드와 마스터 패스워드를 추출하여 해제하는 방법이 있다.

4.1 펌웨어 플래싱

하드디스크 펌웨어를 조작하는 도구를 이용하여 펌웨어를 플래싱하면 하드디스크 패스워드가 해제된다. 대표적인 펌웨어 조작 도구가 HDDHACKR다.

HDDHACKR는 일반 하드디스크를 Xbox 360에서 사용할 수 있도록 하드디스크의 펌웨어를 조작하는 도구이다. HDDHACKR는, 패스워드가 설정되지 않은 하드디스크에서 추출한 SA 모듈 파일을 이용하여 패스워드가 설정된 하드디스크의 SA 모듈을 덮어쓰는 방식을 사용한다.

그러나 이 도구는 일부 Western Digital 하드디스크만 지원한다[12]. 또한 펌웨어를 플래싱하기 위해서는 하드디스크 모델에 맞는 SA 모듈을 저장한 파일이 필요한데, 이 파일이 없을 경우에는 하드디스크 패스워드를 해제하지 못한다.

4.2 마스터 패스워드

마스터 패스워드를 이용하는 방법은 하드디스크에 설정된 보안 수준이 High일 때와 Maximum일 때로 나뉜다. 이 보안 수준은 하드디스크 패스워드를 설정할 때 결정되는데 BIOS에서 하드디스크 패스워드를 설정하면 보안 수준이 일반적으로 High로 설정된다. 보안 수준은 IDENTIFY DEVICE 명령으로 확인이 가능하다.

보안 수준이 High인 경우, 마스터 패스워드를 알고 있으면 SECURITY UNLOCK과 SECURITY DISABLE PASSWORD 명령어를 통해 하드디스크의 사용자 패스워드를 제거하여 잠금을 해제할 수 있다.

반면 보안 수준이 Maximum인 경우에는 마스터 패스워드를 알고 있더라도 SECURITY ERASE UNIT 명령어를 통해 사용자 데이터를 모두 삭제한 후 잠금을 해제할 수 있다. 따라서 이 경우는 포렌식 조사에 도움이 되지 않는다.

마스터 패스워드는 제조사마다, 하드디스크 모델마다 다르다. 알려진 마스터 패스워드는 Table 1과 같다[13].

마스터 패스워드를 이용하는 방법은 마스터 패스워드를 알지 못하는 경우와 보안 수준이 Maximum인 경우에는 사용할 수 없다.

Table 1. Master Passwords

Vendor	Master Password
Western Digital	- WSDAMMWS - WSDACMWS - WDCWDCWDCWDCWDCWDC WDCWDCWDCWDCW[1)] - WDCWDCWDCWDCWDCWDC WDCWDCWDCWDCWD[2)]
Seagate	- Seagate + 25 spaces - SeaGate + 25 periods - amim
Fujitsu	- 32 spaces
Samsung	- ttttttttttttttttttttttttttttttt[3)]
Toshiba	- 32 spaces

4.3 제조사 고유의 방법

패스워드를 확인하기 위한 제조사 고유의 방법은 다양하다. 예를 들어 제조사만의 ATA 명령어를 이용하여 패스워드가 저장된 영역에 접근하는 방법, 하드디스크 진단 기능을 이용해 메모리를 덤프해서 패스워드를 찾는 방법[14][15] 등이 있다. 제조사는 고유의 ATA 명령어 등 패스워드를 찾는 법을 공개하지 않기 때문에 이러한 방법은 역공학을 통해 알아내야 한다.

이 방법을 이용하면 사용자 패스워드와 마스터 패스워드를 모두 확인할 수 있으며, 두 패스워드 중 하나를 이용하여 SECURITY UNLOCK과 SECURITY DISABLE 명령어를 통해 잠금을 해제할 수 있다

1) (10 WDC) + W
2) (10 WDC) + WD
3) 32 t

다음 장에서는 제조사 고유의 ATA 명령어를 이용하는 방법을 통해 Western Digital 하드디스크 패스워드를 알아내고 이를 해제하는 방법에 대해 논한다.

V. Western Digital SA 모듈 추출

Western Digital 하드디스크 드라이브는 ID가 2인 SA 모듈에 사용자 패스워드와 마스터 패스워드를 저장한다. 따라서 이 SA 모듈을 추출하면 사용자 패스워드와 마스터 패스워드를 획득할 수 있다.

5.1 SA 모듈 추출을 위한 ATA 명령어

FIRMWARE MODE(가칭)는 ATA 표준에는 없는 제조사 고유의 명령어로, 각 레지스터에는 (45h, 0Bh, 00h, 44h, 57h, A0h, 80h) 값이 들어간다. 이 명령어는 이후 SA 모듈에 접근하는 명령어를 실행하기 위해 실행된다[8].

SMART WRITE LOG와 SMART READ LOG는 SA 모듈을 읽어오기 위한 명령어로 각각 레지스터는 (D6h, 01h, BEh, 4Fh, C2h, A0h, B0h) 값과 (D5h, 05h, BFh, 4Fh, C2h, A0h, B0h) 값을 가진다.

특히 SMART WRITE LOG 명령어는 키 섹터(key sector)라는 512바이트 값을 장치에 전달하는데 이를 통해 어떤 모듈을 읽어올지 결정된다. 패스워드 정보가 저장된 모듈을 불러오기 위해서는 키 섹터 (0Bh, 00h, 04h, 00h, 02h, 00h, 00h, 00h, …)를 사용한다. 생략된 뒷부분은 512번째 바이트까지 00h 값으로 채워진다.

SMART READ LOG 명령어를 실행하면 하드디스크는 SA 모듈의 처음부터 512바이트의 값(오프셋 0h~1FFh)을 반환한다. SMART READ LOG 명령어를 다시 실행하면 그 이후의 512바이트 값(오프셋 200h~3FFh)을 반환한다. 패스워드가 저장되는 SA 모듈의 크기는 하드디스크마다 다르므로 하드디스크가 더 이상 읽을 내용이 없다는 에러를 반환할 때까지 SMART READ LOG 명령어를 실행하여 해당 SA 모듈 전체를 획득한다.

5.2 구현과 추출 결과

윈도우에서 ATA 명령어를 사용하기 위해

DeviceIoControl API를 사용해 2번 SA 모듈을 추출하는 프로그램을 구현하였다.

분석 컴퓨터에 패스워드가 설정된 하드디스크를 연결해서 부팅한 후 구현 프로그램을 실행하면 Fig. 5처럼 연결된 물리 디스크의 목록이 출력된다. SA 모듈을 추출하고자 하는 Western Digital 하드디스크의 물리 드라이브 번호를 입력한다.

이후 FIRMWARE MODE, SMART WRITE LOG, SMART READ LOG 명령어가 순차적으로 실행되며 2번 SA 모듈이 파일로 저장된다. 해당 파일에는 Fig. 6처럼 사용자 패스워드와 마스터 패스워드가 존재한다.

이 파일에서는 '123123'이 사용자가 설정한 패스워드이고, 'WSDACMWS'가 마스터 패스워드이다.

패스워드를 알고 있으므로 MHDD와 같은 하드디스크 진단 도구를 이용하여 SECURITY UNLOCK과 SECURITY DISABLE PASSWORD 명령어를 실행하면 하드디스크의 잠금이 해제된다. 이 두 명령어를 실행하려면 마스터 패스워드 또는 사용자 패스워드가 필요하다. Table 2는 사용자 패스워드를 이용하여 하드디스크 잠금을 해제하는 과정이다.

Id	Deskription	Cr.level	Cyl	Sector	Size
01	Modules directory	B	-1	0	2
31	Translator	Ad	-1	6	176
17	Loaded part of microprogram code	B	-1	192	30
41	Adaptive data	As	-1	232	19
34	G-List (Grown defect list)	C	-1	255	12
29	Loaded part of microprogram code	B	-1	271	5
51	Parameters table 2	As	-1	280	2
35	SA Defects	Dd	-2	0	1
02	Configuration (HDD ID)	B	-2	5	2
33	P-List (Primary defect list)	Dd	-2	11	290
26			-2	305	129
1C	Loaded part of microprogram code	B	-2	438	27
06	Family models configuration (Alt2)	B	-2	475	10
2D	Debug Log	Dr	-3	0	283
1B	Loaded part of microprogram code	B	-3	293	94
19	Loaded part of microprogram code	B	-3	397	25
4C	Loaded part of microprogram code	B	-3	432	13
07	Family models configuration (Alt3)	B	-3	455	9
2F	Loaded part of microprogram code	B	-3	468	5
52	Parameters table 3	As	-3	477	2
2E	Loaded part of microprogram code	B	-8	0	283
23	S.M.A.R.T. Log (reserved)	B	-8	293	64
1E	Loaded part of microprogram code	B	-8	361	23
40	Adaptive data	As	-8	394	19
05	Family models configuration (Alt1)	B	-8	417	9
4A	Adaptive data	As	-8	430	4
53	Parameters table 4	As	-8	438	2

Fig. 4. SA Modules (PC-3000)

```
G:₩>Get_WD_PWD_Module.exe
Your Drive(s) :
DeviceID            Model                   Size
₩₩.₩PHYSICALDRIVE1  ST3250410AS            250056737280
₩₩.₩PHYSICALDRIVE0  WDC WD10EURX-63C57Y0    1000202273280

Select Physical Drive Number : 0
₩₩.₩PhysicalDrive0 is selected.
```

Fig. 5. SA Module Extraction Program

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
04C0h: 57 44 43 20 57 44 31 30 45 55 52 58 2D 36 33 43  WDC WD10EURX-63C
04D0h: 35 37 59 30 20 20 20 20 20 20 20 20 20 20 20 20  57Y0
04E0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
04F0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0500h: 01 00 00 01 53 7C 42 46 4C 4B 50 44 4D 5A 48 59  ....S|BFLKPDMZHY
0510h: 43 4E 52 47 56 41 4B 57 55 47 00 20 20 20 20 20  CNRGVAKWUG.
0520h: 20 20 20 20 20 20 20 20 30 33 2D 31 39 2D 32 30          03-19-20
0530h: 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00  14..............
0540h: 00 00 00 00 00 00 00 00 00 01 07 00 31 32 33 31  ............1231
0550h: 32 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00  23..............
0560h: 00 00 00 00 00 00 00 00 00 00 00 00 57 53 44 41  ............WSDA
0570h: 43 4D 57 53 00 00 00 00 00 00 00 00 00 00 00 00  CMWS............
0580h: 00 00 00 00 00 00 00 00 00 00 00 00 08 40 FE FF  .............@þÿ
```

Fig. 6. Passwords in Extracted File

Table 2. Password Removal with MHDD

```
MHDD>unlock
WDC WD10EURX-63C57Y0  LBA:1,953,525,168
SN:WD-WCC4J3833881    FW:01.01A01    Size = 953869MB

WARNING: THIS DRIVE IS LOCKED BY ATA PASSWORD

What kind of password will you use?
For master, type "1". For user, type "0" > 0
Type password max 32sym (empty line for cancel):
123123
Done
```

```
MHDD>dispwd
WDC WD10EURX-63C57Y0  LBA:1,953,525,168
SN:WD-WCC4J3833881    FW:01.01A01    Size = 953869MB

WARNING: THIS DRIVE IS LOCKED BY ATA PASSWORD

Disable password works only when drive has been unlocked.

What kind of password will you use?
For master, type "1". For user, type "0" > 0
Type password max 32sym (empty line for cancel):
123123
Done
```

Table 3은 구현한 프로그램을 테스트한 Western Digital 하드디스크 목록이다.

비교적 옛날에 제조된 하드디스크뿐만 아니라 최근에 제조된 하드디스크의 SA 모듈도 제대로 추출

Table 3. Test Hard Disk Drives

Model	Size	Manufactured Date
WD800JD-55MUA1	80GB	14 JAN 2006
WD1600JS-00MHB0	160GB	27 OCT 2005
WD1600BEVS-000UST0	160GB	16 APR 2008
WD2000JS-55MHB0	200GB	13 JAN 2006
WD3200AAKS-00VYA0	320GB	31 OCT 2007
WD6401AALS-00E3A0	640GB	12 MAR 2010
WD10EURX-63C57Y0	1TB	19 MAR 2014
WD10EZEX-00RKKA0	1TB	25 OCT 2012
WD2003FZEX-00P8RA0	2TB	01 DEC 2013
WD20EZRX-00D8PB0	2TB	07 AUG 2014

했다. 이를 통해 하드디스크에 설정된 사용자 패스워드와 마스터 패스워드를 확인할 수 있었다.

본 논문에서 구현한 도구를 이용하면 MHDD 스크립트나 HDDHACKR가 지원하지 않는 최신 Western Digital 하드디스크의 패스워드까지 추출할 수 있다.

VI. 결 론

하드디스크 드라이브에 설정된 ATA 패스워드는 포렌식 조사를 방해하는 안티-포렌식 기법으로 사용될 수 있다. 따라서 본 논문에서는 ATA 패스워드에 초점을 두어 그 메커니즘과 패스워드를 해제하기 위해 필요한 방안을 연구하였다.

하드디스크 자체에 패스워드를 설정할 수 있다는 것은 일반적으로 널리 알려져 있지 않기 때문에 포렌식 조사관이 이에 대한 지식이 없으면 조사 시 패스워드가 걸린 하드디스크를 고장난 하드디스크로 간과할 위험이 있다.

조사관은 조사 대상 하드디스크의 데이터 영역에 접근이 안 된다면 패스워드가 걸려 있는지 확인한 후 조사를 수행해야 한다. 하드디스크에 패스워드가 걸려있는지 여부는 IDENTIFY DEVICE 명령어로 알 수 있다.

추후에는 본 논문에서 분석하여 패스워드를 해제한 Western Digital 하드디스크뿐만 아니라 다양한 제조사의 하드디스크에 대한 연구가 필요하다.

References

〔1〕 Huw Read, Konstantinos Xynos, Iain Sutherland, Gareth Davies, Tom Houiellebecq, Frode Roarson and Andrew Blyth, "Manipulation of hard drive firmware to conceal entire partitions," Digital Investigation, vol. 10, issue 4, pp. 281-286, Dec. 2013.

〔2〕 M. R. Gupta, M. D. Hoeschele, and M. K. Rogers, "Hidden Disk Areas: HPA and DCO," International Journal of Digital Evidence, vol. 5, issue 1, Fall 2006.

〔3〕 Harald Baier, Julian Knauer, "AFAUC - anti-forensics of storage devices by alternative use of communication channels," 2014 8th International Conference on IT Security Incident Management & IT Forensics, pp. 14-26, 2014.

〔4〕 Iain Sutherland, Gareth Davies, Andrew Blyth, "Malware and steganography in hard disk firmware," Journal in Computer Virology, vol. 7, issue 3, pp. 215-219, Aug. 2011.

〔5〕 Gareth Davies, Iain Sutherland, "Hard Disk Storage: Firmware Manipulation and Forensic Impact and Current Best Practice," ADFSL Conference on Digital Forensics, Security and Law, 2010.

〔6〕 Julian Knauer, Harald Baier, "Zur Sicherheit von ATA-Festplattenpasswörtern," Proceedings of D-A-CH Security 2012, pp. 26 - 37, Sep. 2012.

〔7〕 "ATA Passw0rd Unl0cking for all drives," http://forum.hddguru.com/viewtopic.php?f=1&t=16429&p=108750&hilit=dump+script+register#p108750

〔8〕 "Writing/reading a drive's firmware youuru.com/viewtopic.php?f=13&t=26971

〔9〕 T13, "AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS)," http://www.t13.org/documents/uploadeddocuments/docs2007/d1699r4a-ata8-acs.pdf, May 2007.

〔10〕 T13, "AT Attachment with Packet Interface - 7 Volume 1 - Register Delivered Command Set, Logical Register Set(ATA/ATAPI-7 V1)," http://www.t13.org/documents/uploadeddocuments/docs2007/d1532v1r4b-at_attachment_with_packet_interface_-_7_volume_1.pdf, Apr. 2004.

〔11〕 "newbie info, from and for newbies :) About firmware, SA, etc," http://forum.hddguru.com/viewtopic.php?f=16&t=6562

〔12〕 "Hddhackr V1.40 Build 20130303," http://forums.xbox-scene.com/index.php?/topic/746020-hddhackr-v140-build-20130303/, Mar. 2013.

〔13〕 "List of hard disk ata master passwords,"

https://ipv5.wordpress.com/2008/04/14/list-of-hard-disk-ata-master-passwords/
〔14〕 Thomas Schneider, "ATA security lock removal for seagate [Solved] :)," https://blacklotus89.wordpress.com/2013/11/27/ata-security-lock-2/
〔15〕 Thomas Schneider, "seaget," https://github.com/BlackLotus/seaget
〔16〕 "Sending ATA commands directly to device in Windows?," http://stackoverflow.com/questions/5070987/sending-ata-commands-directly-to-device-in-windows/5071027#5071027
〔17〕 "Estrarre le password ATA da un Hard Disk," http://elettrofreak.blogspot.kr/2011/02/estrarre-le-password-ata-da-un-hard.html
〔18〕 Dmitry Postrigan, "MHDD Documentation," http://hddguru.com/software/2005.10.02-MHDD/mhdd_manual.en.html
〔19〕 T13, "SMART Command Transport(SCT)," http://www.t13.org/Documents/UploadedDocuments/docs2005/DT1701r5-SCT.pdf, Feb. 2005.

〈저 자 소 개〉

이 주 영 (Ju-young Lee) 학생회원
2014년 2월: 동국대학교 국어국문학과 학사
2014년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 디지털 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