제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

HPA/DCO 영역의 데이터 수집 기법 연구

박민수*, 손남흔*, 이상진*
*고려대학교 정보보호연구원
e-mail:minsoon2@korea.ac.kr, pida2@korea.ac.kr, sangjin@korea.ac.kr

A Study on Data Acquisition Technique for HPA/DCO

Min-su Park*, Nam-heun Son*, Sang-jin Lee*
*Center for Information Security Technologies, Korea University.

요 약

HPA(Host Protected Area) 영역과 DCO(Device Configuration Overlay) 영역은 사용자가 일반적으로 접근할 수 없는 영역이며 이 위치에 데이터를 저장하거나 은닉할 수 있다. HPA/DCO 영역은 저장 장치와의 통신을 위해 만들어진 규약인 ATA-4와 ATA-6에서 제시되었다. 디지털 포렌식 조사시 HPA/DCO 영역을 고려하지 않은 디스크 이미징 및 데이터 추출 방법은 해당 영역에 숨겨진 유용한 정보를 획득할 수 없다. 따라서 디지털 포렌식 관점에서 HPA/DCO 영역은 중요한 의미를 가지고 있으며, 해당 영역에 존재하는 데이터를 인식하여 획득하는 절차를 통해 디스크 이미징 또는 데이터 추출이 이루어져야 한다. 본 논문은 HPA/DCO 영역에 관한 기존 연구를 활용하여 포렌식 조사에서 해당 영역을 확인하고 접근할 수 있는 방법을 제시하며, HPA/DCO 영역에 저장되어 있는 데이터를 획득하여 디지털 포렌식 조사시 활용할 수 있도록 한다.

1. 서론

HPA는 Host Protected Area 또는 Hidden Protected Area라고 부르며 저장 장치와의 통신을 위한 규약인 ATA-4에서 제시되었다. 해당 영역은 HDD(Hard Disk Drive)에 의해 미리 예약된 영역으로 일반적으로 OS에서 확인할 수 없는 영역이다[3].

HPA 영역은 시스템 부팅이나 진단 유틸리티, 시스템 복구, 보안 유틸리티 저장 등에서 사용되지만 루트킷을 통한 악의적인 용도 및 데이터 은닉 등의 악의적인 용도로도 사용될 수 있다[3].

DCO는 Device Configuration Overlay라고 부르며 ATA-6에서 제시되었다. DCO 영역은 중간 벤더들 또는 필요에 의해 벤더로부터 구입한 HDD를 임의의 고정된 크기의 HDD로 변환할 때 사용된다[3].

이러한 HPA, DCO 영역은 일반적으로 OS 및 BIOS에서 확인 및 접근할 수 없기 때문에 사용자가 의도적으로 데이터를 숨기기 위한 목적으로 사용될 수 있다. 따라서 디지털 포렌식 조사 과정에서 해당 영역에 대한 추가적인 조사가 이루어지지 않는다면 해당 영역에 저장되어 있는 데이터를 획득할 수 없다. 또 디스크 이미징 과정에서 HPA, DCO 영역을 고려하지 않는다면 해당 영역이 제외되고 수집될 수 있다.

따라서 HPA, DCO 영역을 확인하고 해당 영역을 고려한 디스크 이미징 및 디지털 조사 방법이 필요하며 이를 위한 방법으로 다양한 도구를 이용한 영역 확인 및 데이터 획득 방법을 조사하였다.

* 본 연구는 한국연구재단을 통해 교육과학기술부의 바이오연구개발사업으로부터 지원받아 수행되었습니다.(20100020634)

2. HPA & DCO

HPA와 DCO는 일반적으로 OS나 BIOS에서 접근할 수 없고 ATA 명령을 이용하여 접근 및 확인이 가능하다.

ATA는 Advanced Technology Attachment의 약자로 ANSI의 X3T10 그룹이 사용하는 공식 명칭으로서 디스크 드라이브 그 자체 내에 컨트롤러를 통합시켜 구현한 것이다. ATA는 통신 방식이 서로 다른 HDD, CD-ROM 등과 같은 기억 장치를 연결하는 표준 인터페이스이다. ATA는 흔히 IDE라는 용어와 혼재되어 사용된다.

HPA, DCO에서 사용되는 주요 Command Set은 IDENTIFY DEVICE, SET MAX ADDRESS(EXT), READ NATIVE MAX ADDRESS(EXT), DEVICE CONFIGURATION SET, DEVICE CONFIGURATION IDENTITY, DEVICE CONFIGURATION RESTORE 등이 있다[1].

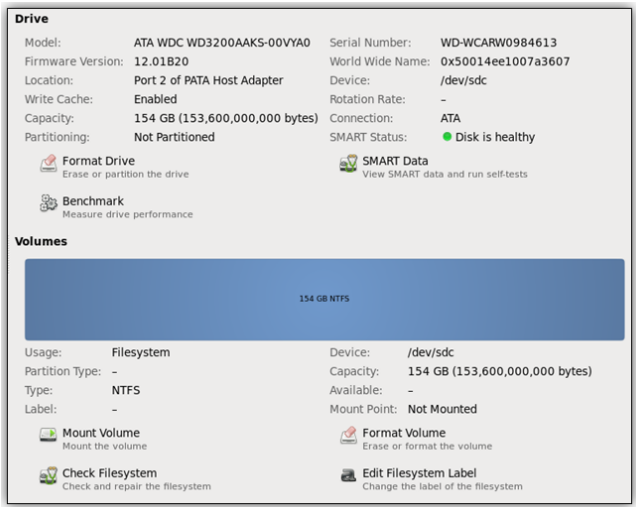
IDENTIFY DEVICE 명령을 통해 현재 BIOS를 통해 접근 가능한 영역을 확인할 수 있다. SET MAX ADDRESS 명령은 BIOS를 통해 접근 가능한 영역을 설정할 수 있으며, HPA 영역을 생성할 수 있다. READ NATIVE MAX ADDRESS는 HPA 영역을 포함한 디스크 크기를 확인할 수 있다[1].

DEVICE CONFIGURATION SET은 DCO영역을 설정

하고 DEVICE CONFIGURATION IDENTIFY는 DCO 영역을 포함한 디스크 크기를 확인할 수 있다. DEVICE CONFIGURATION RESTORE 명령은 DCO 영역을 제거할 수 있다[1].

<표 1> HPA&DCO 주요 ATA 명령어

명령어	기능
IDENTIFY DEVICE	BIOS를 통해 접근 가능한 영역 확인
SET MAX ADDRESS	HPA 생성
READ NATIVE MAX ADDRESS	HPA 영역 확인
DEVICE CONFIGURATION SET	DCO 설정
DEVICE CONFIGURATION IDENTITY	DCO 영역 확인
DEVICE CONFIGURATION RESTORE	DCO 제거



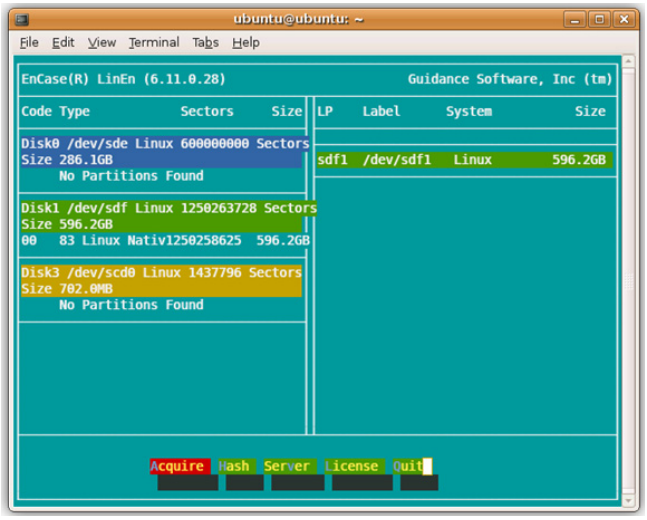
(그림 1) HPA&DCO 영역이 설정된 디스크 드라이브

3. HPA & DCO 영역 접근 및 확인

HPA&DCO 영역을 확인하고 해당 영역을 이미징하기 위해서는 추가적인 방법이 필요하다. HPA, DCO 영역을 이미징하기 위해 ATA 명령을 이용하여 해당 영역을 삭제하거나 재설정하는 방법 등이 필요하며 해당 영역을 이미징 하기 위한 일련의 과정이 필요하다. 이러한 일련의 과정을 간단하게 확인하고 이미징을 하기 위해 사용할 수 있는 도구들이 제공되고 있다.

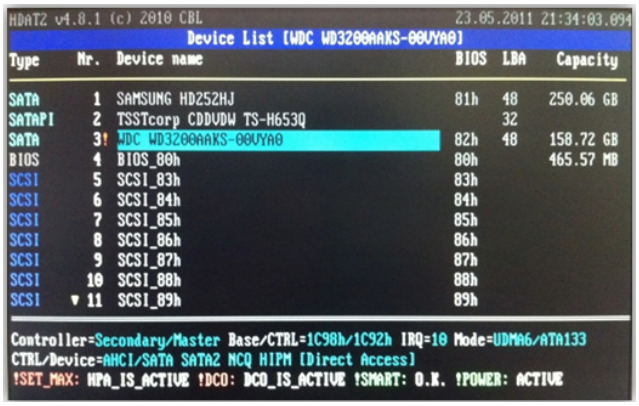
HPA, DCO 영역을 확인하고 접근, 해제 및 재설정할 수 있는 대표적인 도구로는 Helix, HDAT2, SAFE BLOCK, hdparm 등이 있다.

Helix는 Live CD 형태로 제공되며 다양한 포렌식 관련 도구가 내장되어 있다. HPA, DCO 영역이 설정되어 있는 디스크 드라이브를 설치하고 Helix를 구동하면 추가적인 과정 없이 HPA 영역을 자동으로 해제하여 해당 영역을 확인 및 접근할 수 있다 하지만 DCO 영역 확인, 접근 및 해제는 제공하지 않는다. Helix 내부에 설치되어 있는 EnCase를 통해 디스크 이미징도 함께 수행할 수 있다.



(그림 2) Helix에 설치된 EnCase

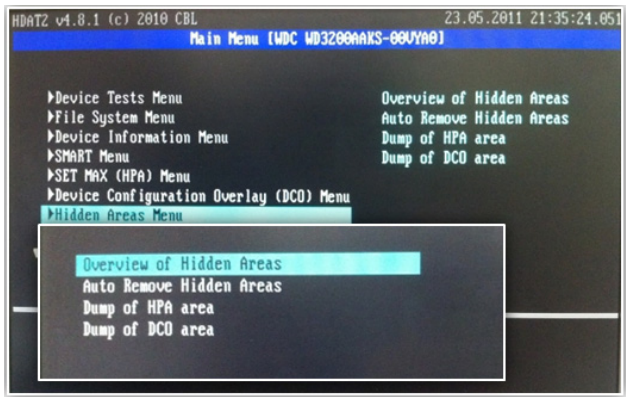
DOS 환경에서 실행되는 HDAT2는 HPA 영역의 확인, 접근 및 영역 설정이 가능하고 Helix에서는 지원하지 않는 DCO 영역에 대한 확인 및 삭제, 접근, 설정 등의 기능을 제공한다.



(그림 3) HDAT2 초기화면

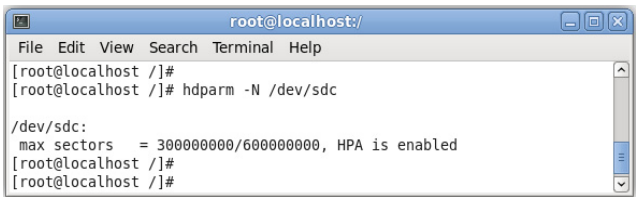
<표 2> HPA/DCO 지원 도구

도구명	HPA	DCO	공식 사이트
Helix	확인 및 해제 가능	확인 및 해제 불가	http://www.e-fense.com/products.php
HDAT2	확인 및 해제 영역 설정 가능	확인 및 해제 영역 설정 가능	http://www.hdat2.com/
hdparm	확인 및 해제 영역 설정 가능	확인만 가능	http://sourceforge.net/projects/hdparm/
SAFE Block	확인 및 해제 가능	확인 및 해제 가능	http://www.forensicsoft.com/

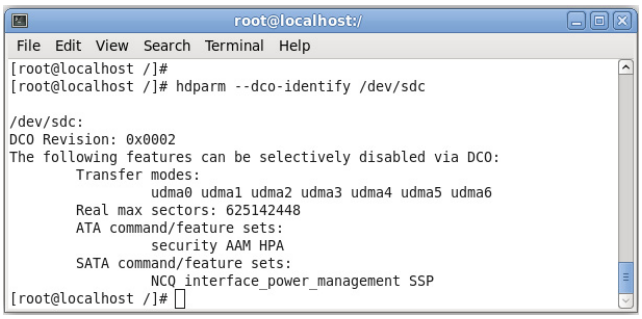


(그림 4) HDAT2 메뉴

리눅스 환경에서 사용할 수 있는 도구로는 hdparm이 있다. hdparm에서 제공하는 다양한 명령어 및 옵션을 이용하여 HPA, DCO 영역의 확인 및 접근이 가능하고, HPA 영역의 삭제 및 설정도 가능하다. 하지만 DCO 영역은 해제가 불가능 하다.



(그림 5) hdparm을 이용한 HPA 영역 확인



(그림 6) hdparm을 이용한 DCO 영역 확인

윈도우 환경에서는 ForensicSoft의 SAFE Block이라는 도구를 이용하여 HPA, DCO 영역을 확인 및 삭제, 설정이 가능하다. SAFE Block은 현재 윈도우 XP에서만 HPA, DCO 영역 확인 및 삭제 기능을 지원하고 VISTA 이후의 버전에서는 제공하지 않는다.

(그림 7) SAFE Block

4. 결론 및 향후 과제

HPA, DCO 영역은 BIOS 및 OS를 이용하여 접근하거나 확인할 수 없으며 이 영역에 악의적인 프로그램이나 데이터를 은닉하여 포렌식 조사에 유용하게 사용될 수 있는 정보를 숨길 수 있다. 디지털 포렌식 조사시 HPA, DCO 영역의 확인 및 이 영역을 고려한 디스크 이미징이 이루어지지 않는다면 해당 영역에 숨겨진 유용한 정보를 획득할 수 없다.

따라서 HPA, DCO 영역을 확인 및 해제하고 이 영역을 포함한 디스크 이미징을 제공하는 자동화된 도구가 필요하다. 향후 윈도우 및 리눅스와 같은 다양한 OS 환경에서 해당 영역을 포함한 디스크 이미징 기능을 제공하는

자동화된 도구를 구현할 것이다. 구현된 도구를 이용하면 분석관이 해당 디스크 드라이브에 숨겨진 데이터를 확인 및 획득하여 범죄 행위를 밝히는데 유용하게 사용될 수 있다.

참고문헌

[1] Mayank R. Gupta, Michael D. Hoeschele, Marcus K. Rogers, "Hidden Disk Areas: HPA and DCO" International Journal of Digital Evidence

[2] Hal Berghel, "Hiding Data, Forensics, and Anti-Forensics", Communications of the ACM

[3] 이상진, " 디지털 포렌식 개론", 이룬, 2010