International Journal of Digital Evidence (Fall 2006)

Hidden Disk Areas : HPA and DCO

forensic-proof.com

proneer

Outline

1. *Introduction*
2. *Host Protected Area*
3. *Device Configuration Overlays*
4. *Host Protected Area*
5. *Co-existence of HAP and DCO*
6. *Investigative Significance*

HPA and DCO

Standard	Other Names	Transfer Modes (MB/s)	Maximum disk size	Other New Features
pre-ATA	IDE	PIO 0	2.1 GB	22-bit LBA
ATA-1	ATA, IDE	Single-word DMA	137 GB	28-bit LBA
ATA-2	EIDE, Fast ATA, Fast IDE, Ultra ATA	Multi-word DMA		PCMCIA connector
ATA-3	EIDE	Single-word DMA		S.M.A.R.T
ATA/ATAPI-4	ATA-4, Ultra ATA/33	Ultra DMA 0, 1, 2		AT Attachment Packet Interface(ATAPI), Host Protected Area(HPA), CompactFlash Association(CPA)
ATA/ATAPI-5	ATA-5 Ultra ATA/66	Ultra DMA 3, 4		80-wire cables; CompactFlash connector
ATA/ATAPI-6	ATA-6, Ultra ATA/100	Ultra DMA 5	144 PB	48-bit LBA, Device Configuration Overlay(DCO), Automatic Acoustic Management
ATA/ATAPI-7	ATA-7, Ultra ATA/133	Ultra DMA 6 aka SATA/150		SATA 1.0
ATA/ATAPI-8	ATA-8	-		Hybrid drive

Introduction

HPA and DCO

- ✓ **Host Protected Area(Hidden Protected Area)**
- ✓ HDD(Hard Disk Drive)에 의해 예약된 영역
- ✓ OS, BIOS 에 의해 보이지 않는 영역
- ✓ ATA(Advanced Technology Attachment)-4 부터 등장
- ✓ 사용자, BIOS, OS가 쉽게 수정하거나 변경할 수 없는 영역의 필요
- ✓ 일반적으로 HDD utilities, diagnostic tools, boot sector code 저장

Introduction

HPA and DCO

- ✓ **Device Configuration Overlay**
- ✓ HDD 제조사로부터 구입한 HDD를 모두 같은 섹터로 만드는 것이 가능
- ✓ 80 GB HDD를 BIOS, OS 모두 60 GB 의 HDD로 보이도록 구성 가능

Introduction

Issue for forensic investigators

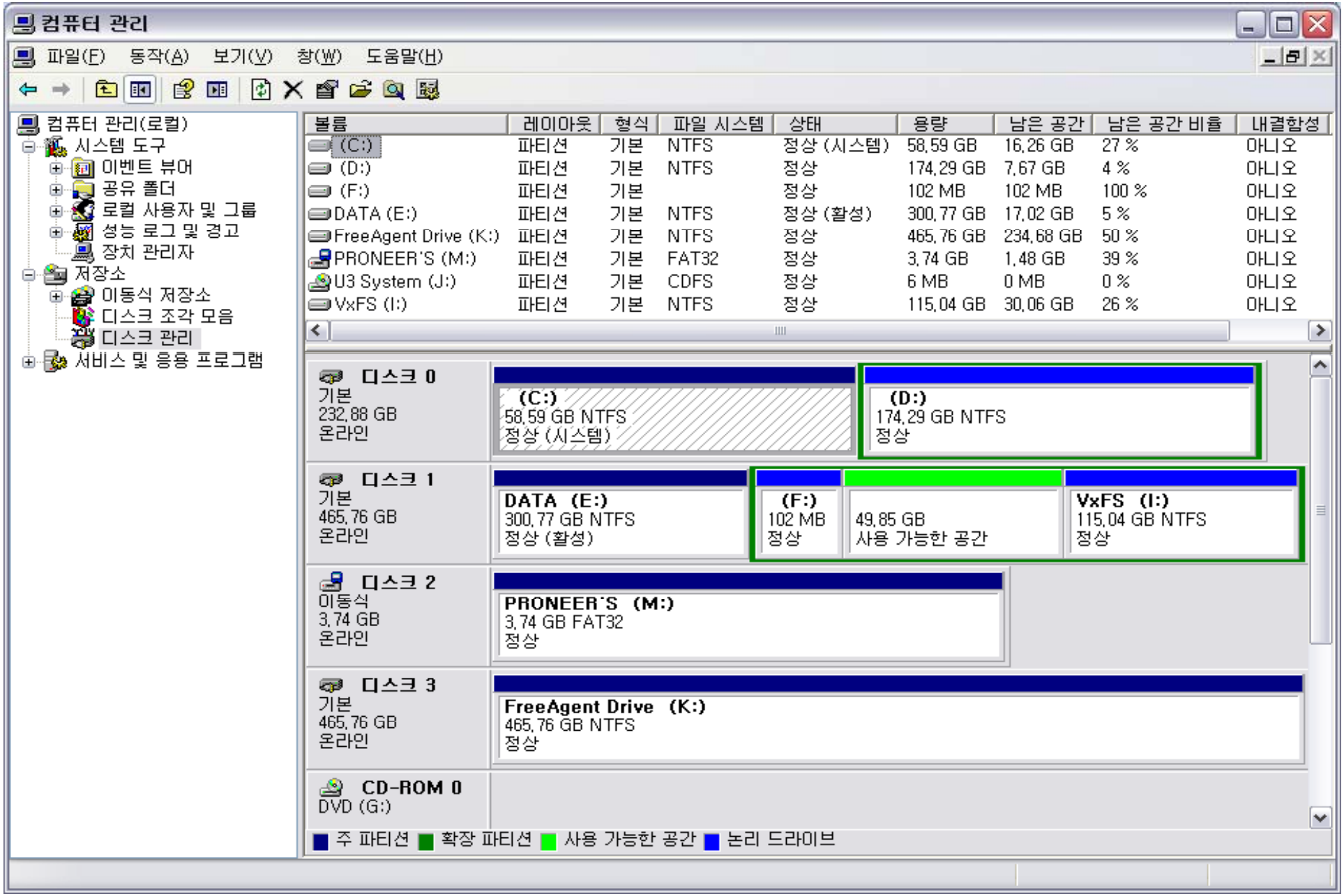
- ✓ HPA와 DCO에 정보가 저장된 경우 일반적으로 BIOS, OS, 사용자는 접근 불가
- ✓ 포렌식 수사관들에게는 해당 영역 파악 필요
- ✓ HDD 이미지의 경우에도 HPA와 DCO를 고려하여 이미징 해야 함
- ✓ HPA 영역에서 탐지를 피하는 ROOTKIT 존재

Introduction

Why?

- ✓ HDD는 출시전 품질 테스트
- ✓ 250 GB HDD는 물리적으로 500 GB의 HDD와 같을 수 있음
- ✓ 단, 120 GB 품질 테스트만 통과했기 때문에 120 GB로 판매
- ✓ HDD 관리를 위해 포맷을 해도 지워지지 않는 영역이 필요

Host Protected Area



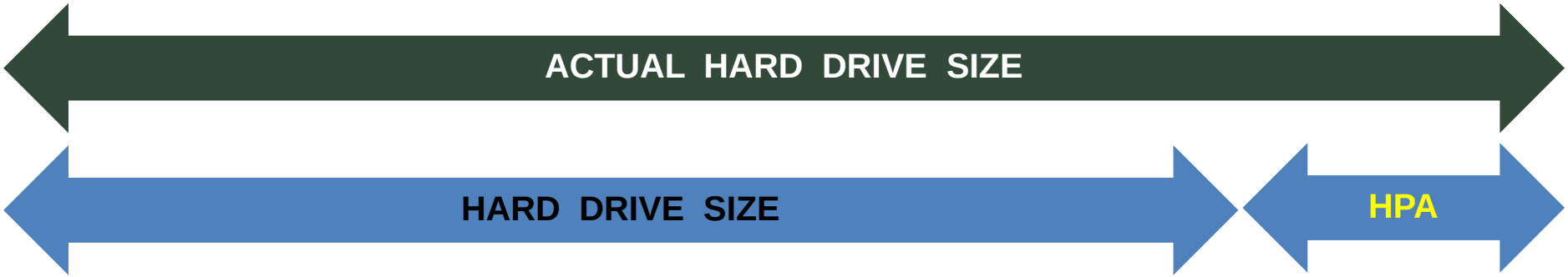
Host Protected Area

Use

- ✓ BIOS와 함께 HPA에 접근하기 위한 유틸리티 존재
- ✓ Phoenix FirstBIOS
  - BEER(Boot Engineering Extension Record)
  - PARTIES(Protected Area Run-Time Interface Extension Services)
- ✓ CD or DVD 없이 OS가 로드되기 전에 시스템 복구 목적으로 활용
- ✓ IBM, LG 노트북 등에서는 복구 소프트웨어 저장 용도로 사용

Host Protected Area

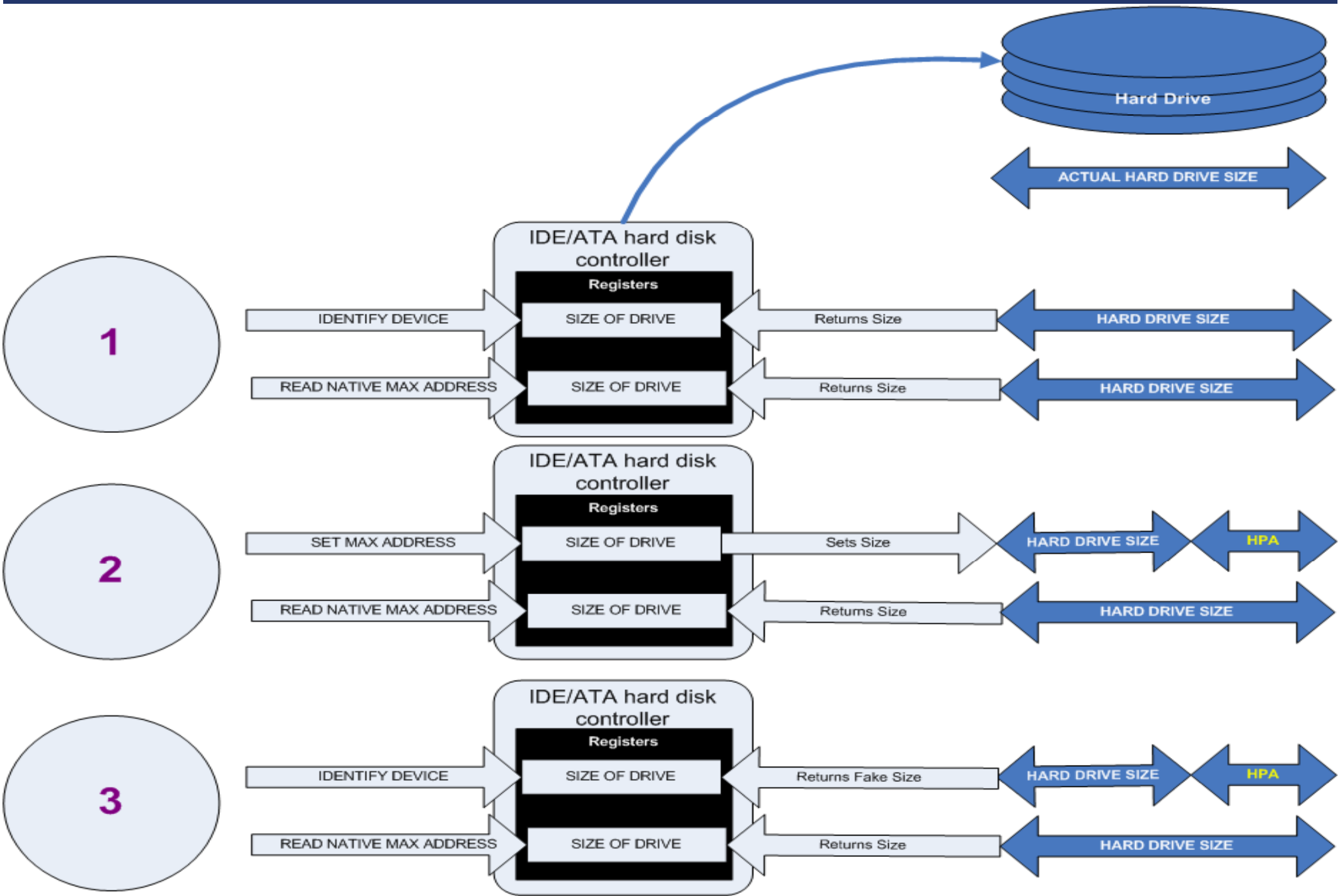
ATA Command



✓ HPA 접근하기 위한 ATA 컨트롤러 명령어 :

- IDENTIFY DEVICE
- SET MAX ADDRESS (EXT)
- READ NATIVE MAX ADDRESS (EXT)

Host Protected Area



Device Configuration Overlays

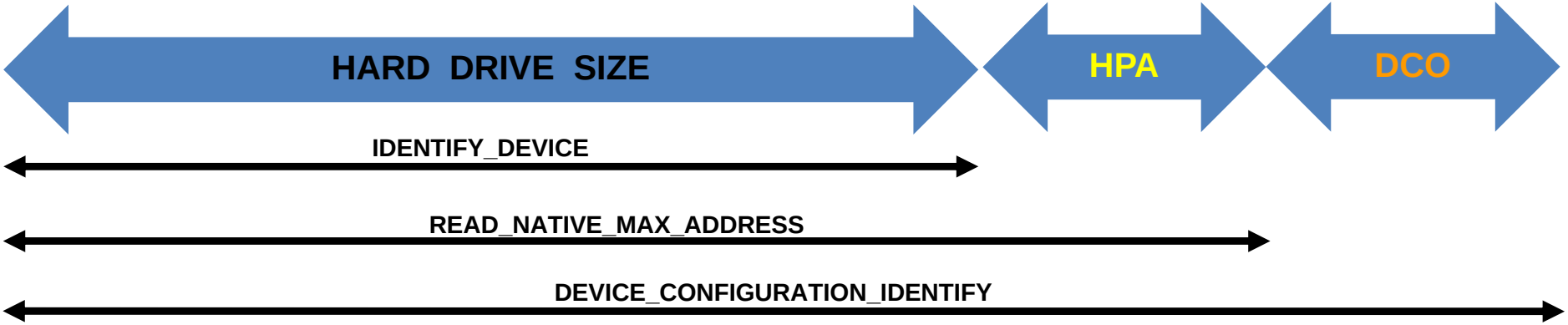
Introduction

- ✓ ATA-6 표준에서 처음 소개
- ✓ PC 제조사들은 서로 다른 HDD를 구입하여 같은 용량으로 만듦
- ✓ DCO 접근하기 위한 ATA 컨트롤러 명령어 :
  - DEVICE CONFIGURATION SET : DCO 설정
  - DEVICE CONFIGURATION IDENTITY : DCO 접근
  - DEVICE CONFIGURATION RESTORE : DCO 제거

Co-existence of HPA and DCO

Collision?

- ✓ HPA와 DCO는 동일한 HDD에 존재 가능
  - DEVICE CONFIGURATION SET을 통해 DCO 설정 후
  - SET MAX ADDRESS (EXT) 를 통해 HPA 구성
- ✓ READ NATIVE MAX ADDRESS (EXT)와 DEVICE CONFIGURATION IDENTIFY 의 비교를 통해 DCO 적용 여부 확인



Identification & Manipulation

Identification Tools

- ✓ The Sleuth Kit (free, open software) by Brian Carrier. (HPA Linux-only)
- ✓ The ATA Forensic Tool(TAFT) by Arne Vidstrom
- ✓ EnCase for DOS by Guidance Software
- ✓ Access Data's Forensic Toolkit
- ✓ HD Tune Pro

Identification & Manipulation

Identification Methods to Linux

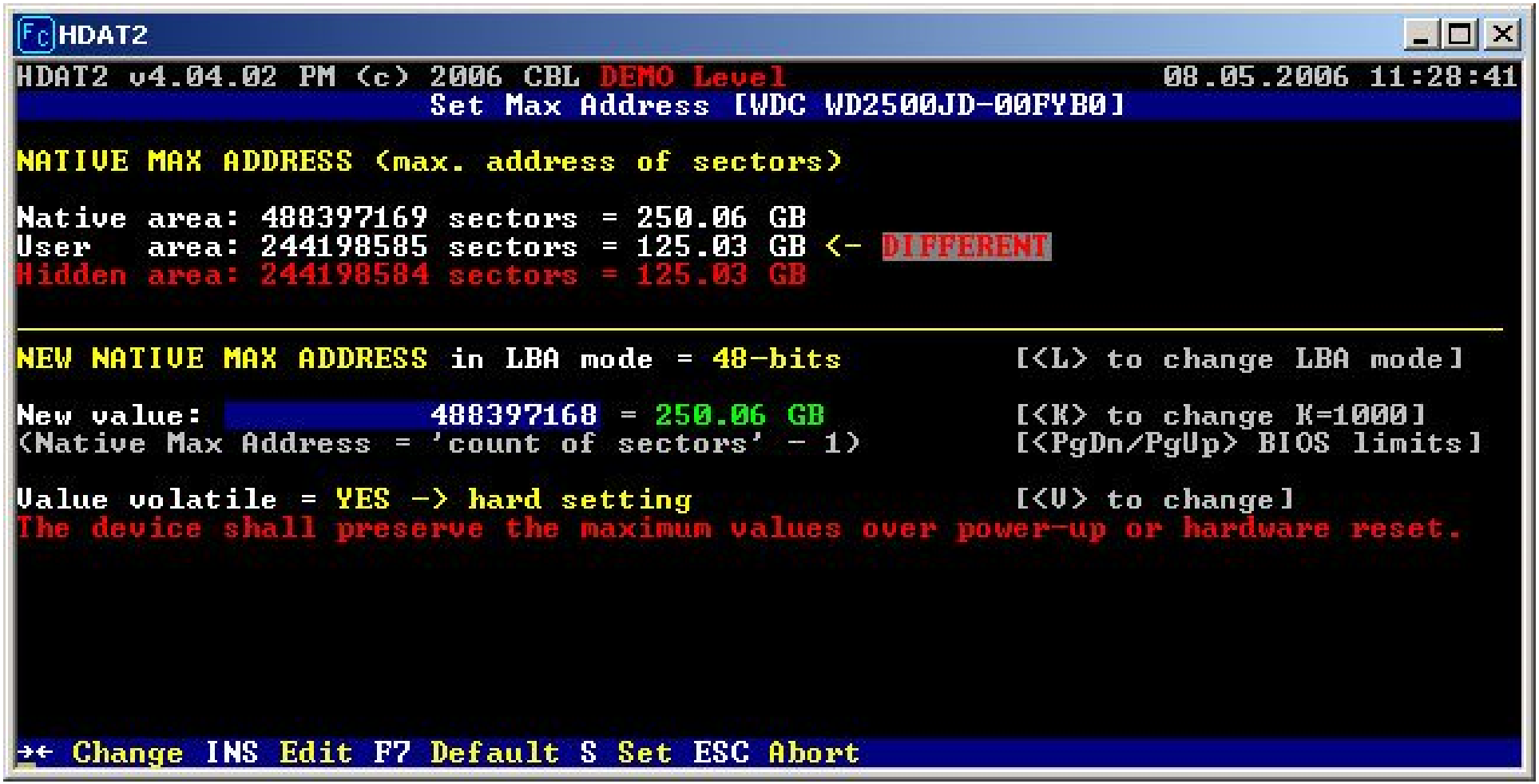
```
[webadmin@ime ~]$ dmesg | less
...skipping...
hda: Host Protected Area detected.
        current capacity is 156365903 sectors (80059 MB)
        native  capacity is 156368016 sectors (80060 MB)
hda: Host Protected Area disabled.
```

```
root@fse2010-desktop:~# hdparm -N /dev/sda

/dev/sda:
 max sectors   = 312500000/312500000, HPA is disabled
root@fse2010-desktop:~#
```

Identification & Manipulation

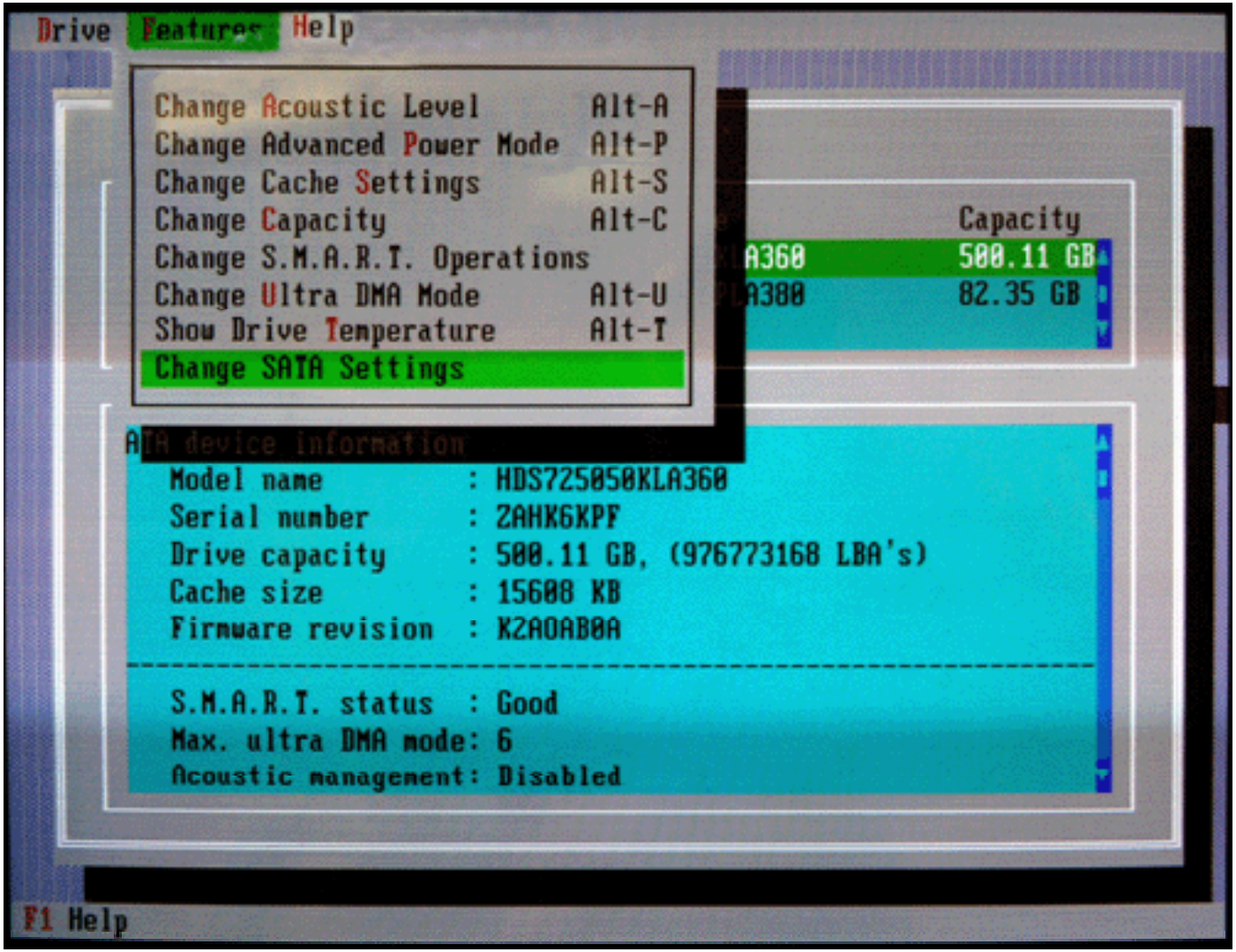
Manipulation tools – HDAT2



http://www.hdat2.com/

Identification & Manipulation

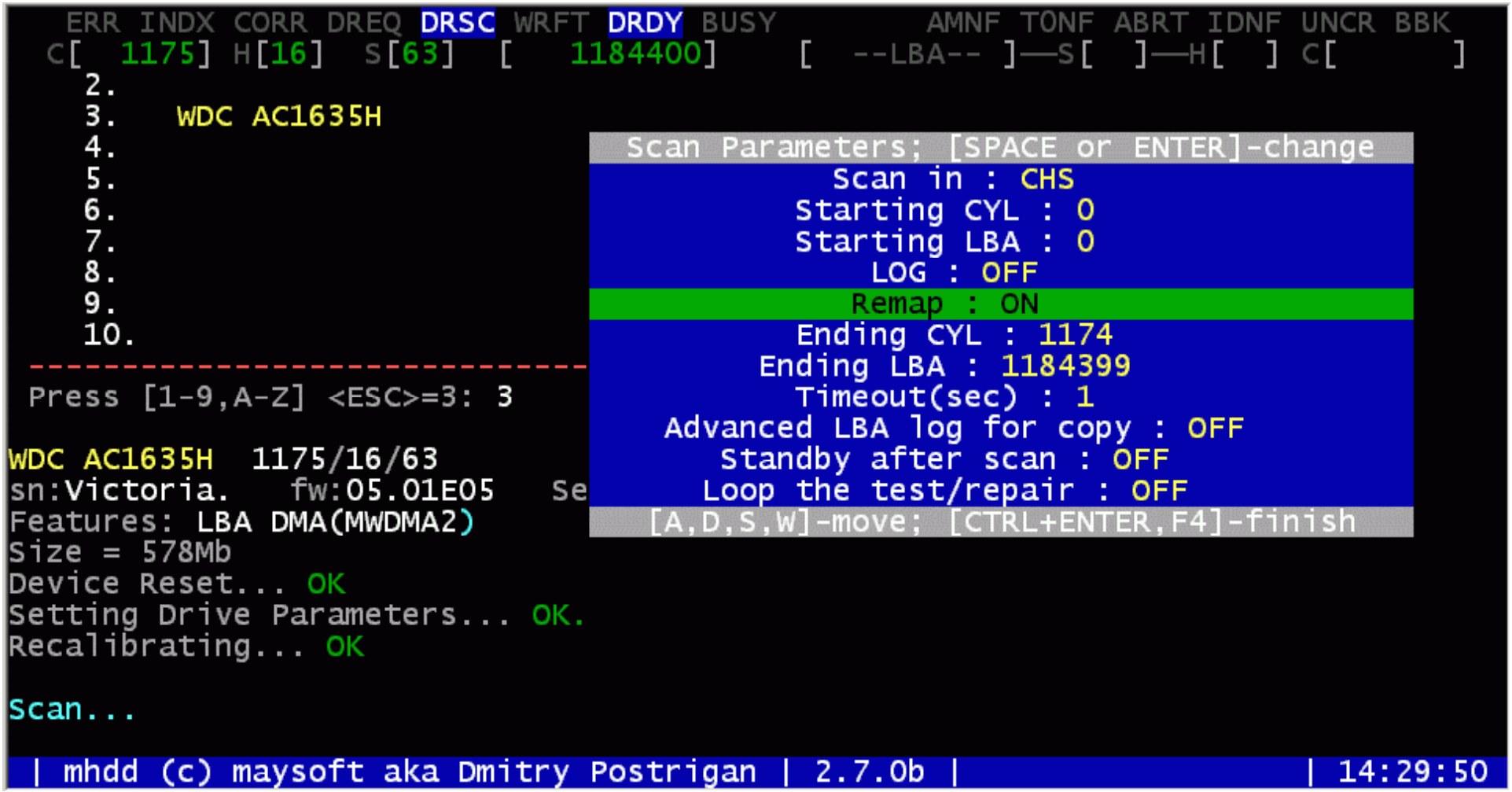
- Manipulation tools – Feature Tool by Hitachi Global Storage Technologies



http://www.hitachigst.com/hdd/support/download.htm#FeatureTool

Identification & Manipulation

Manipulation tools – MHDD by Dmitry Postrigan



http://hddguru.com/

Identification & Manipulation

- **Manipulation tools – hdparam(linux program) & setmax(by Andries E. Brouwer)**

  - ✓ hdparm - http://sourceforge.net/projects/hdparm/
  - ✓ setmax - http://www.win.tue.nl/~aeb/linux/setmax.c

Investigative Significance

Forensic Tools

Tool	*Programmer/Vendor*	*Version(Now)*
The Sleuth Kit	Brian Carrier	2.02 (3.01)
ATA Forensic Tool	Arne Vidstrom	1.1 (1.2)
EnCase	Guidance Software	4.20 (6.13)

Investigative Significance

EnCase for Windows vs The Sleuth Kit for Linux

- ✓ EnCase for Windows 의 경우 HPA/DCO를 지원하지 않음
- ✓ 동일한 HDD를 대상으로 EnCase for Windows와 The Sleuth Kit for Linux 이미징
- ✓ 두 이미지에 대한 MD5 checksum 값이 불일치

➔ **대상 HDD는 리눅스 시스템을 통해 HPA/DCO를 포함하여 수집해야 함**

Increase the Capacity of a HDD

✓ 준비물 : Ghost 2003 Build 2003.775 (not patched), HDD * 2 (둘다 OS 설치)

1. T를 마스터로 잡고 X를 슬레이브로 잡는다. 파일 시스템 타입이 양쪽 드라이브 모두 같아야 한다(NTFS 혹은 FAT32 등등)
2. Ghost 2003 build 2003.775 를 T 드라이브에 표준설정으로 설치한다. 필요하다면 재부팅한다.
3. Ghost를 열고 Ghost Basic을 선택한다. 옵션 리스트에서 Backup을 선택한다. C:\ (하드드라이브 T에서 파티션을 없애려는 드라이브)를 선택해 백업한다. second 드라이브를 타겟으로 선택한다. 아무 이름이나 입력하고 reboot이 나올 때까지 OK – Continue 혹은 Next를 클릭한다.
4. 재부팅이 시작되면 DOS나 드라이버가 로딩되기 전에 PC를 셧다운 시켜야 한다. 가장 좋은 방법은 BIOS가 뜨고 하드 디스크를 detect하는 순간 전원을 빼어 버리는 것이다.
5. Ghost가 백업하기 전에 셧다운 시켰다. 이제 마스터로 설치했던 하드 드라이브 T를 제거하고 드라이브 X를 설치한다. 하드 드라이브 T를 secondary 드라이브로 설치한다. X는 마스터가 되고 부팅이 가능하게 되었을 것이다. 컴퓨터 관리 – 디\스크 관리로 간다. T 드라이브에 VPSGHBOOT 혹은 비슷한 라벨이 붙은 9메가 파티션과 이전에는 보이지 않았던 스페이스가 보일 것이다. 아직은 VPSGHBOOT 를 제거해서는 안된다!
6. T 드라이브의 할당되지 않은 스페이스를 선택해 새로운 primary 혹은 extended 파티션을 생성한다. 좋아하는 파일 시스템 타입을 선택하고 quick format(만일 옵션이 있다면)으로 포맷한다. 포맷이 완성되면 드라이브에서 VPSGHBOOT 파티션을 제거한다.
7. T 드라이브에 다음과 같은 것이 보일 것이다:
   a. 드라이브에 숨겨진 파티션이 있었을 당시의 오리지널 파티션
   b. 방금 복구한 새로운 파티션 스페이스
   c. 8 메가의 할당되지 않은 파티션
8. T 드라이브를 primary 하드디스크로 잡고 싶으면 디스크 관리자로 가서 오리지널 파티션(위의 a)을 활성 파티션으로 설정

Conclusion

- ✓ OS, BIOS로부터 보이지 않는 HPA, DCO는 사용자에 의해 변경 가능
- ✓ HDD를 통한 증거 수집 시 ATA 버전과 HPA, DCO 지원 여부가 고려되어야 함

In My Opinion…

- ✓ HDD 복제나 이미징의 경우 미리 HPA, DCO 존재 여부 파악 필요
- ✓ EnCase 사용시 EnCase for DOS 를 통한 증거 수집 홍보
- ✓ DDI(DFRC Disk Imaging) for DOS 개발 필요

Question and Answer