

# 6장 디지털 증거 수집 기술

**박종혁 교수**

**UCS Lab**

Tel: 970-6702

Email: [jhpark1@seoultech.ac.kr](mailto:jhpark1@seoultech.ac.kr)



- 학습 목표

- 디지털 증거 수집을 위한 활성시스템 조사, 디스크 이미징, 임베디드 시스템 조사와 관련한 기술을 살펴본다.
- 실제 간단한 실습을 통해 디지털 증거 수집에 대한 학습의 이해와 경험을 획득한다.

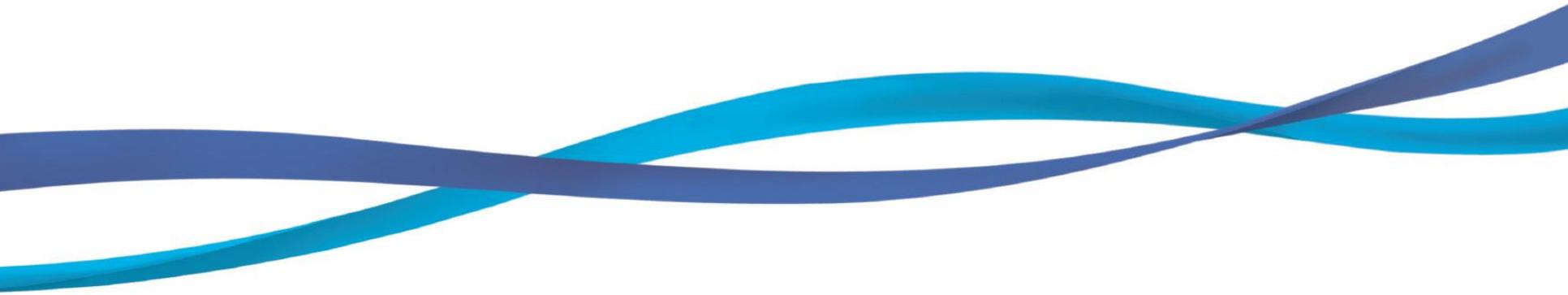
- 학습 내용

- 활성 시스템 조사
- 디스크 이미징 기술
- 임베디드 시스템 증거 확보 방법

# 목 차

1. 조사대상 매체 파악
2. 활성 시스템 조사
3. 디스크 이미징
4. 임베디드 시스템 증거 확보

# 1. 조사 대상 매체 파악



# 디지털 증거 조사 과정에서 사용되는 포렌식 장비들



디스크 복제 장치  
(ICS ImageMasster Solo4)



디스크 복제 장치  
(Logicube Dossier)



HDD 쓰기 방지 장치  
(ICS Super DriveLock)



휴대용 포렌식 도구  
(EnCase Portable)



USB 쓰기 방지 장치  
(Wiebetech USB WriteBlocker)



이동형 포렌식 워크스테이션  
(Forensic Air-Lite V MK III)



이동형 포렌식 워크스테이션  
(ICS RoadMasster 3)

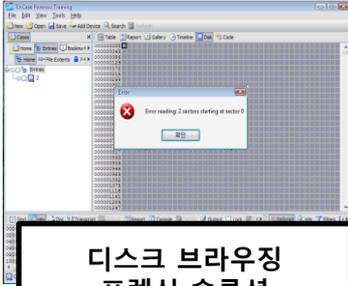
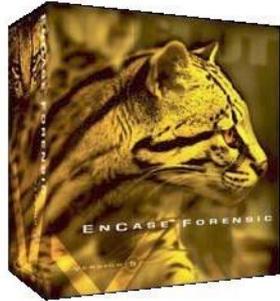


이동형 포렌식 워크스테이션  
(Forensic Air-Lite M-15-SR)

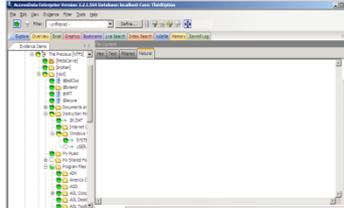


메모리카드 쓰기 방지 장치  
(ICS Write Protect Card Reader)

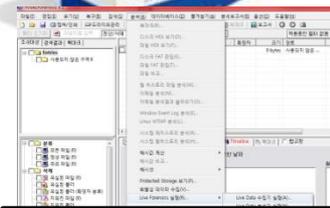
# 디지털 증거 조사 과정에서 사용되는 포렌식 SW



디스크 브라우징  
포렌식 솔루션  
(Guidance Encase v6)



디스크 브라우징  
포렌식 솔루션  
(AccessData Forensic  
Toolkit v3.0)



디스크 브라우징  
포렌식 솔루션  
(파일데이터  
Final Forensics v2.0)

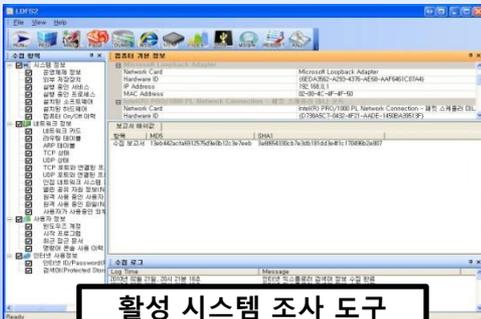


라이브 포렌식 도구  
(Helix 3)

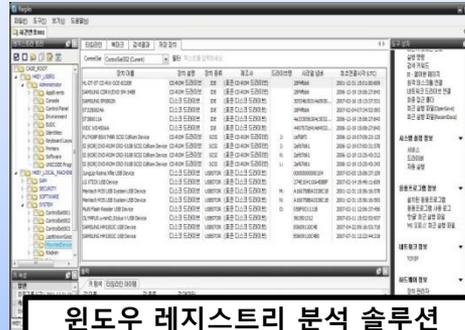
paraben's  
device  
seizure



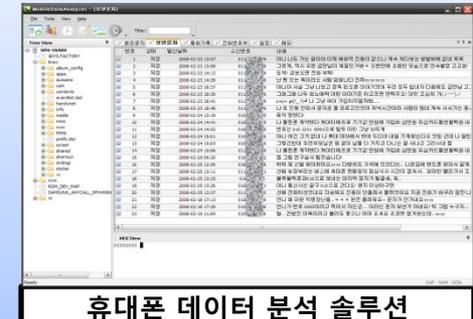
휴대폰 포렌식 솔루션  
(Paraben Device Seizure v3.3)



활성 시스템 조사 도구  
(고려대 LDFS)

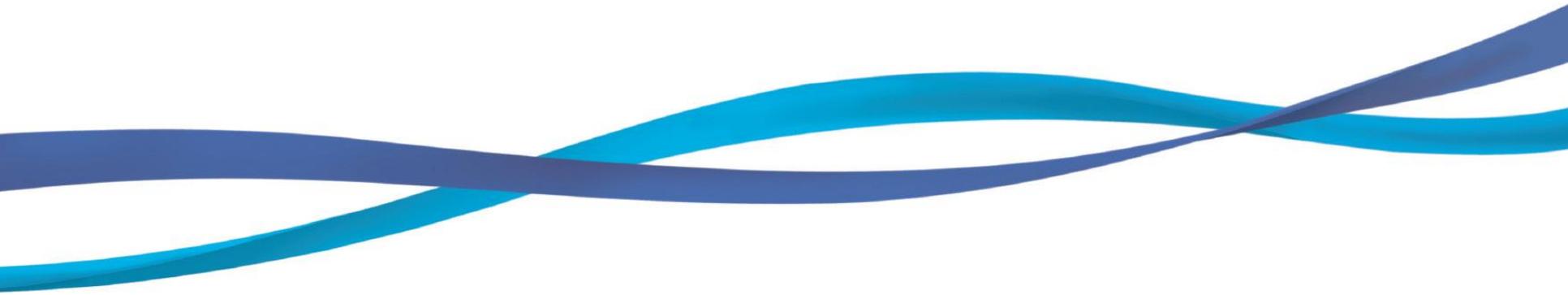


윈도우 레지스트리 분석 솔루션  
(고려대 RegAn)



휴대폰 데이터 분석 솔루션  
(고려대 Mobile Data Analyzer)

## 2. 활성 시스템 조사



# 활성 시스템 조사

## 활성 시스템 (Live System)

- 운영 중인 시스템
- 휘발성 데이터(Live Data, Volatile Data)  
: 시스템의 RAM에 저장되어 있어 전원을 차단하면 수집할 수 없는 데이터
- 활성 시스템 정보: "사건 현장에서 촬영한 증식 사진" 과 같이 당시 **시스템의 동작 상태를 그대로 나타내는 시스템 사용 정보**

## 활성 시스템 조사란(Live Forensics)?

- Live Forensics: 활성 상태의 시스템에서 증거 수집 및 분석을 수행하는 일련의 조사 과정
- 디스크 이미지 조사 기반의 일반적 디지털 포렌식 과정과는 다르게 **시스템이 구동 중인 상태에서 데이터를 선별 수집 및 조사를 진행함**
- 시스템의 전원을 차단하면 수집할 수 없는 **휘발성 데이터**와 신속한 조사에 필요한 **비휘발성 데이터**를 선별해서 수집

# 활성 시스템 조사의 중요성

## 포렌식 패러다임의 변화

- 하드디스크 용량이 급격하게 증가함에 따라 **디스크 이미지 기반의 증거 조사가 어려워짐**
- 현장에서 증거의 선별 수집 및 즉각적인 분석이 이루어지는 **현장 중심의 포렌식 조사에 대한 관심 증대**

## 시스템의 현재 상태가 중요한 경우

- **침해 사고 조사의 경우, 시스템의 현재 상태가 매우 중요**
- 시스템의 당시 상황이 쟁점인 경우, 이를 증명할 수 있는 증거 수집 과정이 필요

## 이미지 획득이 불가능한 시스템의 경우

- 서버와 같이 시스템을 압수하기가 용이하지 않은 경우, **시스템을 끄지 않고 조사를 수행할 수 있어야 함**
- **법 집행기관이 아닌 기관에서 조사할 경우, 디스크 이미징을 수행할 수 없는 경우가 발생**
  - 디스크 이미지 기반의 조사는 기업 비밀 노출 및 프라이버시 침해 문제 발생

# 활성 데이터의 개념

- 활성 데이터

- 활성 시스템에서 수집할 수 있는 휘발성 데이터와 조사에 필요한 비휘발성 데이터를 포괄하는 개념



# 활성 시스템 조사에서 수집 데이터의 분류

## 비휘발성 데이터 수집의 필요성

- 하드디스크 용량이 급격하게 증가함에 따라 디스크 이미지 기반의 증거 조사가 어려워지고, 현장에서 증거의 선별 수집 및 즉각적인 분석이 이루어져 하는 상황 발생
- 서버와 같이 시스템을 압수하기가 용이하지 않은 경우, 시스템을 끄지 않고 조사를 수행할 수 있어야 함
- 법 집행기관이 아닌 단체에서 조사할 경우, 디스크 이미징을 수행할 수 없는 경우가 발생
  - 사건에 연관된 파일만 압수하는 선택적 압수 수색 영장에 대한 필요성이 제기됨

## 수집 정보 분류

- 휘발성 데이터, 실행 중인 프로세스 덤프, 물리 메모리 이미지
- 데이터 선별을 통한 최소한의 비휘발성 데이터 수집
  - 파일시스템 메타데이터: NTFS의 \$MFT 파일, FAT 의 File Allocation Table 등
  - 운영체제 설정 정보: 시스템 이벤트 로그, 레지스트리 파일 등
  - 사용자 정보: 윈도우 계정, 시작 프로그램, 최근 접근 문서 등
  - 응용프로그램 정보: 인터넷 히스토리, 검색어, 웹 계정(ID/Password) 등

# 취발성 데이터의 종류

## 시스템 정보

- 시스템 시간
- 열려 있는 파일 정보
- 현재 실행 중인 프로세스 리스트
- 현재 실행 중인 서비스 리스트
- 현재 로그인한 사용자 계정
- 클립보드 내용
- 명령어 콘솔 사용 정보

## 네트워크 정보

- 네트워크 카드 정보
- 라우팅 테이블
- ARP 테이블
- TCP 연결 상태
- UDP 연결 상태
- 열린 TCP 포트와 연결된 프로세스 정보
- 열린 UDP 포트와 연결된 프로세스 정보
- 인접 네트워크 시스템 정보
- 열린 공유 자원 정보
- 원격 사용자 정보
- 원격 접근 파일
- 사용 중인 외부 자원

## 프로세스 세부 정보

- 프로세스 실행파일의 전체 경로
- 프로세스를 실행한 계정
- 부모/자식 프로세스
- 프로세스가 로드한 라이브러리
- 사용 중인 네트워크 연결 정보 (TCP/UDP)
- 실행 시작 시간

# 활성 시스템에서 수집하는 비휘발성 데이터

## 파일시스템 메타데이터

- 메타데이터 정보를 이용, 조사에 필요한 파일을 선별하여 최소한의 파일 수집
- 파일이름, 확장자, 시간 정보 별로 필요한 파일만을 선택하여 조사

## 운영체제 설정 정보

- 레지스트리는 시스템 사용과 관련해 다양한 정보 제공
- 디스크/파티션 정보
- 각종 이벤트들은 유용한 정보를 제공 (이벤트 로그)

## 사용자 정보

- 사용자 계정 리스트
- 최근 접근 문서
- 최근 실행 명령어
- 사용자 계정 패스워드 검색을 위한 데이터 수집 (LM Hash, NT Hash)

## 응용프로그램 정보

- 인터넷 사용 기록
- 웹 사이트 계정
- 검색어
- 메신저 사용 기록
- 대화 상대 및 내용
- 받은 파일

# 활성 시스템 조사 기법 -1

## 취발성 데이터 분석

- 수집한 다양한 취발성 데이터에 대한 상관 분석을 통해 의미있는 결과 도출
- 네트워크 데이터 분석 기술
  - 인가되지 않은 프로세스의 네트워크 연결 조사
  - 공유 자원 정보 획득 → 정보 유출 증거 수집
- 물리 메모리 및 가상 메모리 이미지에 대한 분석 기술
  - 덤프한 프로세스 이미지에서 유용한 정보 추출
  - 각 메모리 이미지에 대한 특정 키워드 검색 기술 및 유용한 텍스트 추출 기능

## 운영체제 사용 흔적 조사

- 운영체제 사용과 관련된 정보 수집 (시스템 기본 설정, 레지스트리 등)
- 운영체제 설정 파일 분석을 통한 사용 패턴 분석
- 포렌식 관점에서 유용한 데이터에 대한 연관 분석

# 활성 시스템 조사 기법 -2

## 파일시스템 메타데이터

- 키워드 검색 등을 통한 수사 대상 선별
- 수집이 필요한 특정 파일(한글, 오피스 문서 등) 선택적 증거 수집
- 확장자 별 통계 분석을 통한 해당 컴퓨터의 용도 및 사용자 패턴 분석
- 타임라인 분석을 통한 사용자 행위 추적

## 응용 프로그램 분석

- 웹 브라우저, 전자메일, 메신저 관련 파일 분석을 통한 사용자의 관심사 파악
- 응용프로그램 캐쉬(Prefatch) 분석을 통한 사용 이력 조사

# 취발성 정도에 따른 수집 절차 (RFC 3227)

[CPU]  
레지스터,  
캐시

[물리메모리]  
ARP 캐시,  
프로세스,  
네트워크 연결,  
라우팅 테이블

[물리메모리]  
임시파일  
시스템

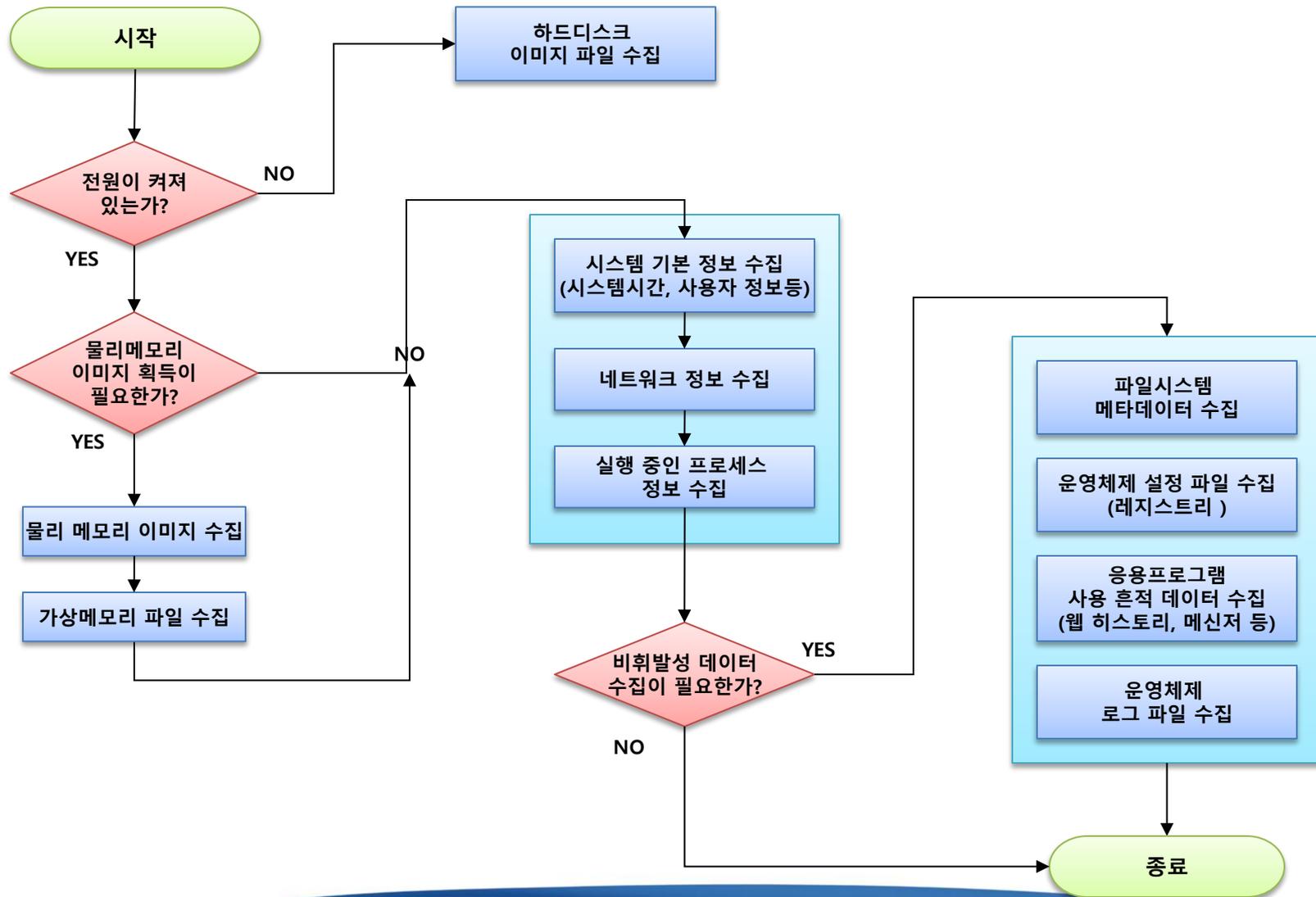
하드 디스크

원격 로그 및  
모니터링  
데이터

물리적인  
설치 상태,  
네트워크  
구성

외부  
저장 매체

# 활성 시스템 조사 절차



# 활성 시스템 조사의 한계성

활성 시스템에서 조사를 위한 도구를 실행할 경우, 시스템에 불가피한 데이터 변형을 유발함

- Ex) 파일 접근 시간 변경, 메모리 데이터 무결성 훼손

DLL 후킹 기법 등을 사용하는 악성코드에 의해서 변조된 데이터를 수집할 가능성이 있음

- 메모리 분석을 통한 악성 코드 존재여부 파악이 필요함

삭제 파일에 대한 복구 불가능

- 이미지 분석과정에서 파일 복구를 시도해야 함

# 활성 데이터 조사 고려사항 (1/2)

## 조사 대상 시스템의 무결성 보장

- 이론적으로는 수집 데이터의 내용은 물론 메타 데이터까지 변경되지 않아야 함
- **휘발성 데이터 수집 및 분석은 필연적으로 대상 시스템에 영향을 미침**
- 휘발성 저장 장치에서 수집한 증거의 법적 효력에 관한 연구 필요
  - 절차적 방법 : 입회인의 서명
  - 기술적 방법 : 메타데이터 변경의 최소화, 수집 데이터의 위조 불가능성

## 데이터 수집의 용이성

- 이미지 생성 없이 필요한 데이터만 선별적으로 수집 가능

## 인증 절차 우회

- 사용자 인증이 불필요하며, 자동 암호화 솔루션 우회 가능

# 활성 데이터 조사 고려사항 (2/2)

## 활성 시스템 조사 시 주의사항

- 시스템에 주는 영향을 최소화
- 신뢰성 있는 도구 사용
- 신중한 조사
  - 한번 변경되면 원래 상태로 되돌릴 수 없음
- 조사과정의 기록
  - 조사 시각, 수집 데이터 명시 및 변경 데이터 명시



# 활성 데이터의 저장

## CD를 이용하는 방법

- 활성 포렌식 도구를 CD에 저장하고 수집한 데이터는 USB 저장 장치에 저장하거나 네트워크를 이용하여 증거 수집 서버에 전송함
- 포렌식 도구의 신뢰성을 향상시킬 수 있음

## USB Thumb Drive 이용하는 방법

- 대용량의 데이터를 저장할 수 있어 최근 많이 사용됨
- Windows의 Plug and Play 기능 활성화로 어려움 없이 사용 가능
  - Windows 시스템에 로그 정보 남음(setuplog.txt, setupapi.log)
- USB 저장 장치의 일부 영역을 제조사에서 제공하는 고유 도구를 이용하여 CDFS(CD File System)로 설정한 후 도구를 저장하고, 수집한 데이터는 데이터 영역에 저장하는 방식을 이용

# 취발성 데이터 수집 및 분석

## 수집 목적

### • 프로세스 정보

- 시스템에 악영향을 미치는 악성 프로그램, 이상 프로세스 판별

### • 네트워크 정보

- 허가되지 않은 네트워크 연결 정보 확인
- 실행 중인 프로세스의 네트워크 연결 정보 비교/분석

### • 사용자 정보

- 대상 시스템에 대한 사용자의 흔적 정보들을 바탕으로 정황 증거 확보

## 분석 방법

### • 상관 관계 분석

- 수집 결과에서 서로 관계 있는 정보들을 추출하여 상관 분석을 시행
- 예) 실행 중인 프로세스 리스트, 열린 TCP 포트와 연결된 프로세스 정보, 네트워크 접속 정보 등을 비교 분석하여 비정상적 행위 분석(악성코드 감염 판별)

### • 활성 정보를 분석할 수 있는 능력 필요

- 각각의 수많은 취발성 데이터에서 의미 있는 결과를 도출할 수 있는 능력 필요

# 시스템 기본 정보 - 시스템 시간

## System Time

- 증거 수집 시, 시간 기준이 됨
- 그 외 중요 요소들
  - Real time
  - 시스템의 구동시간(Up time)

## 수집 방법

- date, API를 이용한 Perl script
- date (/t : 현재 시간 바로 출력)
  - 휴대전화 시각 등 정확한 시간과 비교하여 시간차를 기록함

# 시스템 기본 정보 - 시스템 시간

```
C:\> C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\menba169>date /t & time /t
:008-01-14
오후 01:33
```

Console Command  
- date /t & time /t

LDFS - [20090202]

파일(F) 보기(V) 창(W) 도움말(H)

RUN REG MFT PAGE DUMP WEB MEM REPORT ANZ

20090202

수집 항목

- 시스템 정보
  - 운영체제 정보
  - 외부 저장장치
  - 실행 중인 프로세스
  - 실행 중인 서비스
  - 설치된 소프트웨어
  - 설치된 하드웨어
- 네트워크 정보
  - 네트워크 카드
  - 라우팅 테이블
  - ARP 테이블
  - TCP 상태
  - UDP 상태
  - TCP 포트와 연결된 프로세스
  - UDP 포트와 연결된 프로세스
  - 인접 네트워크 시스템 정보(NETVIEW)
  - 열린 공유 자원 정보(NETSHARE)
  - 원격 사용 중인 사용자 정보(NETSESS)
  - 원격 사용 중인 파일(NETFILE)
  - 사용자가 사용 중인 외부 자원(NETUSE)
- 사용자 정보
  - 윈도우즈 계정
  - 시작 프로그램
  - 최근 접근 문서
  - 명령어 콘솔 사용 이력
- 인터넷 사용 정보
  - 인터넷 ID/Password(Protected Storage)

기본 컴퓨터 정보

Basic Information

System Time	2009년 02월 23일, 04시 28분 19초
-------------	----------------------------

IP Configuration

Disk Information

Partition Information

Logged-on Account Information

Win32 Account Information

수집 파일 해쉬값

항목	MD5	SHA1
수집 보고서	3a44fa91ffe0282c64718f6a94846e9f	710e2469cbf830c391e83b0ff235f4b5aafb4be8

로그

Log Time	Message
2009년 02월 23일, 04시 29분 24초	인터넷 익스플로러 검색어 정보 수집 완료
2009년 02월 23일, 04시 29분 24초	인터넷 익스플로러 검색어 정보 수집 시작
2009년 02월 23일, 04시 29분 23초	인터넷 익스플로러 ID & PASSWORD 정보 수집 완료
2009년 02월 23일, 04시 29분 18초	인터넷 익스플로러 ID/PASSWORD 정보 수집 시작
2009년 02월 23일, 04시 29분 18초	최근 실행 명령어 정보 수집 완료

LDFS  
-Win API 이용

# 시스템 기본 정보 - 현재 로그인 계정

## 현재 로그인 계정(Logged-on user)

- 수집 시스템의 현재 계정 정보 확보
- 정보의 주체가 누구인지 알아야 함

## 수집방법

- net users : netbios 명령어
- psloggedon : Sysinternals 사에서 제공하는 공개프로그램
- net sessions : netbios 명령어

# 현재 로그인 계정 (Windows)

The image shows a Windows command prompt window running the Psloggedon utility. The output lists users logged on locally and via resource shares. A red box highlights the command used to run the utility, and another red box highlights the output for users logged on via resource shares. A pink callout box points to the command, and a blue callout box points to the LDFS interface.

```
C:\WINDOWS\system32\cmd.exe
Sysinternals - www.sysinternals.com

Users logged on locally:
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
KTS\computer
NT AUTHORITY\SYSTEM

C:\Documents and Settings\computer>"C:\Documents and Settings\computer\바탕 화면
\Tools\Tools\Pstools\psloggedon.exe" -x

loggedon v1.33 - See who's logged on
Copyright ?2000-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
KTS\computer
NT AUTHORITY\SYSTEM

Users logged on via resource shares:
<null>\WBROMPTON

C:\Documents and Settings\computer>
```

Psloggedon  
-현재 로그인한 사용자  
정보

LDFS  
-Win API 이용

Win32 Account Information

항목	MD5	SHA1
수집 보고서	3a44fa91ffe0282c64718f6a94846e9f	710e2469cbf830c391e83b0ff235f4b5aafb4be8

로그

Log Time	Message
2009년 02월 23일, 04시 29분 24초	인터넷 익스플로러 검색어 정보 수집 완료
2009년 02월 23일, 04시 29분 24초	인터넷 익스플로러 검색어 정보 수집 시작
2009년 02월 23일, 04시 29분 23초	인터넷 익스플로러 ID & PASSWORD 정보 수집 완료
2009년 02월 23일, 04시 29분 18초	인터넷 익스플로러 ID & PASSWORD 정보 수집 시작

# 현재 로그인계정 (UNIX)

- USER INFORMATION – 사용자정보 – w, finger -lmsp, who -r

```
1 HP-UX  2 HP-UX  3 Ubuntu
# w
 2:02am  up  6:06,  4 users,  load average: 0.00, 0.00, 0.00
User      tty          login@  idle   JCPU   PCPU   what
root      console     8:02pm  2:47
proneer   pts/0       8:14pm  5:48
proneer   pts/1       11:21pm
root      pts/2       10:03pm  10
# finger -lmsp
Login name: root
Directory: /                Shell: /sbin/sh
On since Mar 25 20:02:12 on console from rx2600
2 hours 49 minutes Idle Time
New mail received Sat Jan 31 16:26:51 2009;
unread since Thu Mar 26 00:54:57 2009

Login name: proneer
Directory: /home/proneer    Shell: /sbin/sh
On since Mar 25 20:14:38 on pts/0 from 163.152.165.111
5 hours 49 minutes Idle Time
No unread mail
```

# 시스템 기본 정보 - 디스크 정보

## 디스크 정보

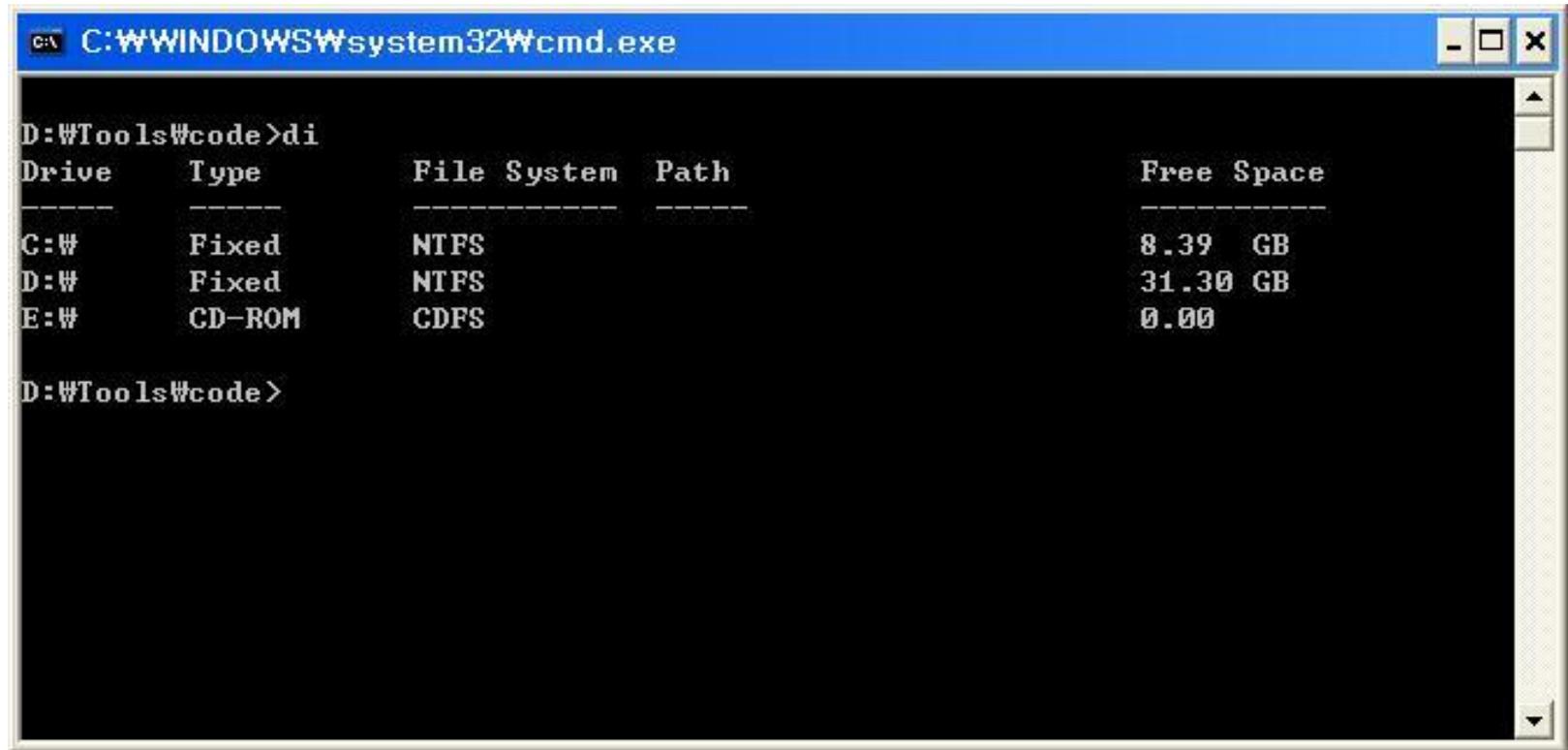
- 수집해야 하는 디스크 목록 확인

## 수집방법

- Di 명령어(Windows) - 파티션 구성 정보 확인 가능
- Unix
  - iostat -fC disk
  - 디스크상태 - (cat /proc/diskstats)
  - 파티션정보 - (cat /proc/partitions)

# 디스크, 파티션 정보(Windows)

- di (각 Driver의 정보)



```
C:\WINDOWS\system32\cmd.exe
D:\Tools\code>di
Drive      Type      File System  Path      Free Space
-----
C:\       Fixed    NTFS
D:\       Fixed    NTFS
E:\       CD-ROM   CDFS
          8.39 GB
          31.30 GB
          0.00

D:\Tools\code>
```

Drive	Type	File System	Path	Free Space
C:\	Fixed	NTFS		8.39 GB
D:\	Fixed	NTFS		31.30 GB
E:\	CD-ROM	CDFS		0.00

# 디스크, 파티션 정보(Windows)

LDFS  
-디스크,파티션 정보

The screenshot displays the LDFS utility interface. On the left, a tree view shows system and network information. The main window is divided into two panes: '기본 컴퓨터 정보' (Basic Computer Information) and '수집 항목' (Collected Items).

**기본 컴퓨터 정보 (Basic Computer Information):**

- Basic Information
- IP Configuration
- Disk Information
- Partition Information

**Physical Drive 0:**

Partition Type	NTFS
Bootable	YES
Partition Length	81GB=850962738Byte
Partition Number	1
Physical Number	0

**Physical Drive 1:**

Partition Type	NTFS
Bootable	NO
Partition Length	151GB=1590997278Byte
Partition Number	2
Physical Number	0

**수집 항목 (Collected Items):**

항목	MD5	SHA1
수집 보고서	9c836d8a49facc80834743556cfd24cc	2ca4f176b0449b6f23c423b46fc9e68565d6e535

**로그 (Log):**

Log Time	Message
2009년 02월 23일 05시 42분 28초	수집 시작
2009년 02월 23일 05시 42분 27초	수집 완료
2009년 02월 23일 05시 42분 26초	수집 시작
2009년 02월 23일 05시 42분 25초	수집 완료
2009년 02월 23일 05시 42분 24초	수집 시작
2009년 02월 23일 05시 42분 23초	수집 완료

# 디스크, 파티션 정보(Unix)

- SYSTEM INFORMATION – 저장장치 - `ioscan -fC disk`

```
1 HP-UX 2 HP-UX 3 Ubuntu
# ioscan -fC disk
Class      I  H/W Path          Driver      S/W State   H/W Type    Description
=====
disk      0  0/0/2/0.0.0.0    sdisk       CLAIMED     DEVICE      TEAC      DV-28E-N
disk      1  0/1/1/0.0.0      sdisk       CLAIMED     DEVICE      SEAGATE   ST373405LC
disk      2  0/1/1/0.1.0      sdisk       CLAIMED     DEVICE      SEAGATE   ST373405LC
#
```

- ✓ -f : full listing
- ✓ -C class : Restrict the output listing to those devices belonging to the specified class

# 프로세스 정보 분석

- **목적:** 실행 중인 프로세스 정보 수집 및 분석을 통한 비정상 프로세스 판별 악성코드 탐지
- **방법:**
  - 기존 프로세스 정보들과 비교 분석하여 참조 DLL
  - 실행 경로 등이 이상이 없는지 점검, 또한 각 프로세스의 자식 프로세스의 활동 정보 비교/분석
  - 물리 메모리에서 프로세스 구조체를 추출하여 숨겨진 프로세스 탐지 등
- **도구:** 윈도우 작업 관리자(Windows), Process Explorer(Windows), top(Unix)

Process Explorer - Sysinternals: www.sysinternals.com

Process	PID	C.	Description	Company Name
explorer.exe	2972		Windows Explorer	Microsoft Corporation
acasp.exe	3528		AhnLab Common Architecture	AhnLab, Inc.
AhnSD.exe	4064		AhnSD	AhnLab, Inc.
RTHDCPL.exe	3872		Realtek HD Audio Control Panel	Realtek Semiconductor Corp.
GrooveMonitor.exe	3324		GrooveMonitor Utility	Microsoft Corporation
AcroTray.exe	2220		AcroTray	Adobe Systems Inc.
rundll32.exe	308		Run a DLL as an App	Microsoft Corporation
VolPanel.exe	660		VolPanel.exe	Creative Technology Ltd
CTHELPER.EXE	3912		CTHelper Application	Creative Technology Ltd
CTXFIHLP.EXE	4012		CTXfiHlp MFC Application	Creative Technology Ltd
Scheduler.exe	1420		Scheduler Application	SIGMACOM Co.,Ltd
SMPManager.exe	2088		SMPPlayer TrayIcon Application	SIGMACOM Co.,Ltd
rundll32.exe	2156		Run a DLL as an App	Microsoft Corporation
AIINap.exe	3808			
ctfmon.exe	2332		CTF Loader	Microsoft Corporation
LClock.exe	1980		LClock Application	
NMBgMonitor.exe	2300		Nero Home	Nero AG
googletalk.exe	3344		Google 토크	Google
CTCMSGo.exe	976		Creative MediaSource Gol	Creative Technology Ltd
SetPoint.exe	2616		Logitech SetPoint Event Manager (UNICODE)	Logitech, Inc.
KHALMNPX.exe	2744		Logitech KHAL Main Process	Logitech, Inc.
PowerMate.exe	1948		PowerMate 2.0	Griffin Technology
WindowsSearch.exe	2808		Windows Search System Tray	Microsoft Corporation
ONENOTEM.EXE	3960		Microsoft Office OneNote Quick Launcher	Microsoft Corporation
DriveXpert.exe	1588		Drive Xpert Volume Manager	Silicon Image, Inc.
AIISuite.exe	816			
WINWORD.EXE	2696	1	Microsoft Office Word	Microsoft Corporation

Type	Name
Desktop	WDefault
Directory	WWindows
Directory	WBaseNamedObjects
Directory	WKnownDis
Event	WBaseNamedObjectsWUserenv: User Profile setup event
Event	WBaseNamedObjectsWmixercallback

CPU Usage: 2% Commit Charge: 29,76% Processes: 82

1 HP-UX 2 HP-UX 3 Ubuntu

System: rx2600 Thu Mar 26 01:42:45 2009

Load averages: 0.00, 0.00, 0.00

129 processes: 111 sleeping, 18 running

Cpu states:

LOAD	USER	NICE	SYS	IDLE	BLOCK	SWAIT	INTR	SSYS
0.00	0.0%	0.0%	0.0%	100.0%	0.0%	0.0%	0.0%	0.0%

Memory: 265964K (182648K) real, 488368K (318384K) virtual, 991992K free Page# 1/3

TTY	PID	USERNAME	PRI	NI	SIZE	RES	STATE	TIME	%WCPU	%CPU	COMMAND
? 48	root	152	20	2232K	1984K	run	0:18	0.31	0.31	vxfsd	
? 10	root	152	20	864K	768K	run	0:00	0.18	0.18	ObjectThreadPool	
? 2186	root	152	20	163M	56872K	run	0:05	0.18	0.18	cimserver	
? 2773	root	152	20	113M	14420K	run	0:05	0.14	0.14	vxsvc	
? 551	root	152	20	7844K	1880K	run	0:00	0.10	0.10	utmpd	
? 38	root	152	20	216K	192K	run	0:01	0.06	0.06	schedcpu	
? 20	root	191	20	144K	128K	run	0:00	0.04	0.04	ksyncer_daemon	
? 2173	root	152	20	25528K	3616K	run	0:00	0.04	0.04	rpcd	
? 2492	root	152	20	23728K	2840K	run	0:00	0.04	0.04	swagentd	
? 0	root	127	20	72K	64K	sleep	0:14	0.02	0.02	swapper	
? 1	root	152	20	1868K	436K	run	0:00	0.02	0.02	init	
? 2	root	128	20	72K	64K	sleep	0:00	0.02	0.02	vhand	
? 3	root	128	20	72K	64K	sleep	0:00	0.02	0.02	statdaemon	
? 4	root	128	20	72K	64K	sleep	0:00	0.02	0.02	unhashdaemon	
? 11	root	152	20	72K	64K	sleep	0:00	0.02	0.02	nfsktcpd	
? 13	root	147	20	72K	64K	sleep	0:00	0.02	0.02	lvmkd	
? 14	root	147	20	72K	64K	sleep	0:00	0.02	0.02	lvmkd	
? 15	root	147	20	72K	64K	sleep	0:00	0.02	0.02	lvmkd	

# 프로세스 정보 - GUI 분석 도구

- Process Explorer(Active)-Systinternals

Process Explorer - Sysinternals: www.sysinternals.com

Process	PID	C..	Description	Company Name
explorer.exe	2972		Windows Explorer	Microsoft Corporation
acasp.exe	3528		AhnLab Common Architecture	AhnLab, Inc.
AhnSD.exe	4064		AhnSD	AhnLab, Inc.
RTHDCPL.exe	3872		Realtek HD Audio Control Panel	Realtek Semiconductor Corp.
GrooveMonitor.exe	3324		GrooveMonitor Utility	Microsoft Corporation
Acrotray.exe	2220		AcroTray	Adobe Systems Inc.
rundll32.exe	308		Run a DLL as an App	Microsoft Corporation
VolPanel.exe	660		VolPanel.exe	Creative Technology Ltd
CTHELPER.EXE	3912		CTHelper Application	Creative Technology Ltd
CTXFIHLP.EXE	4012		CTXfiHlp MFC Application	Creative Technology Ltd
Scheduler.exe	1420		Scheduler Application	SIGMACOM Co.,Ltd
SMPManager.exe	2088		SMPPlayer TrayIcon Application	SIGMACOM Co.,Ltd
rundll32.exe	2156		Run a DLL as an App	Microsoft Corporation
AiNap.exe	3808			
ctfmon.exe	2332		CTF Loader	Microsoft Corporation
LClock.exe	1980		LClock Application	
NMBgMonitor.exe	2300		Nero Home	Nero AG
googletalk.exe	3844		Google 토크	Google
CTCMSGo.exe	976		Creative MediaSource Go!	Creative Technology Ltd
SetPoint.exe	2616		Logitech SetPoint Event Manager (UNICODE)	Logitech, Inc.
KHALMNPR.exe	2744		Logitech KHAL Main Process	Logitech, Inc.
PowerMate.exe	1948		PowerMate 2.0	Griffin Technology
WindowsSearch.exe	2808		Windows Search System Tray	Microsoft Corporation
ONENOTEM.EXE	3360		Microsoft Office OneNote Quick Launcher	Microsoft Corporation
DriveXpert.exe	1588		Drive Xpert Volume Manager	Silicon Image, Inc.
AiSuite.exe	816			
WINWORD.EXE	2896	1	Microsoft Office Word	Microsoft Corporation

Type	Name
Desktop	\\Default
Directory	\\Windows
Directory	\\BaseNamedObjects
Directory	\\KnownDlls
Event	\\BaseNamedObjects\\Userenv: User Profile setup event
Event	\\BaseNamedObjects\\mixercallback

CPU Usage: 2% | Commit Charge: 29,76% | Processes: 82

# 프로세스 정보 - GUI 수집 및 분석 도구

- LDFS - 실행 중인 프로세스 뷰어(Static)

The screenshot displays the 'Process Information' window. On the left, a tree view lists running processes, with 'nateonmain.exe(3924)' selected. The main area shows details for 'nateonmain.exe', including its description as 'NateOn Messenger' and its full path. Below this, 'Process Basic Information' and 'Listening Information' (TCP and UDP) are shown. Three blue callout boxes highlight key features: 'PROCESS 설명' (Process Description), 'Process 정보' (Process Information), and 'UDP 열린 포트 정보' (UDP Open Port Information). A fourth callout box at the bottom left highlights the '실행 중인 프로세스 목록' (Running Process List).

**PROCESS 설명**

**Process 정보**

**실행 중인 프로세스 목록**

**TCP 열린 포트 정보**

**UDP 열린 포트 정보**

# 물리메모리에서 프로세스 정보 추출

- 덤프한 물리메모리에서 프로세스 구조체 (eProcess) 추출
  - 프로세스 구조체는 포렌식 관점에서 유용한 정보가 다수 존재
- 은닉 프로세스 탐지 및 이전에 실행한 프로세스 목록 추출 가능
  - 전원을 차단하지 않을 경우 메모리에 프로세스 목록이 일주일 이상 잔류

물리메모리 Win32 eProcess 분석기

C:\Documents and Settings\Administrator\바탕 화면\XNETBLUE- 1023 MB 종료

No.	Type	Status	PID	PPID	Process	Create Time
00000000	Process		920	680	VMUpgradeHelper	2010년 03월 24일 05시 30분 01초
00000001	Process		0	0	Idle	Unknown
00000002	Process		1156	680	svchost.exe	2010년 03월 24일 05시 29분 35초
00000003	Process		1288	680	spoolsv.exe	2010년 03월 24일 05시 29분 35초
00000004	Process		1356	1580	cmd.exe	2010년 03월 24일 05시 35분 12초
00000005	Process		996	680	svchost.exe	2010년 03월 24일 05시 29분 35초
00000006	Process		1060	388	Miranda.exe	2010년 03월 24일 05시 37분 13초
00000007	Process		1764	1580	VMwareTray.exe	2010년 03월 24일 05시 29분 42초
00000008	Process		200	1580	cmd.exe	2010년 03월 24일 05시 36분 04초
00000009	Process		692	636	lsass.exe	2010년 03월 24일 05시 29분 34초
00000010	Process	--Hidden--	2012	1740	vanquish.exe	2010년 03월 24일 05시 54분 47초
00000011	Process		224	680	ExpressService.	2010년 03월 24일 05시 29분 33초
00000012	Process		1372	1580	DIFront.exe	2010년 03월 24일 05시 49분 46초
00000013	Process		280	680	Nsavsvc.npc	2010년 03월 24일 05시 29분 53초
00000014	Process		580	680	vmtoolsd.exe	2010년 03월 24일 05시 30분 00초
00000015	Process		328	680	nsvmon.npc	2010년 03월 24일 05시 29분 53초
00000016	Process		680	636	services.exe	2010년 03월 24일 05시 29분 34초
00000017	Process		1096	1372	mdd_1.3.exe	2010년 03월 24일 05시 49분 55초
00000018	Process		564	4	smss.exe	2010년 03월 24일 05시 29분 33초
00000019	Process		612	564	csrss.exe	2010년 03월 24일 05시 29분 34초
00000020	Process		636	564	winlogon.exe	2010년 03월 24일 05시 29분 34초
00000021	Process		1404	1372	mdd_1.3.exe	2010년 03월 24일 05시 50분 25초
00000022	Process		896	680	svchost.exe	2010년 03월 24일 05시 29분 35초
00000023	Process		1740	1580	cmd.exe	2010년 03월 24일 05시 54분 35초
00000024	Process		1808	1580	msmsgs.exe	2010년 03월 24일 05시 29분 42초
00000025	Process		1800	1580	ctfmon.exe	2010년 03월 24일 05시 29분 42초
00000026	Process		1580	1520	explorer.exe	2010년 03월 24일 05시 29분 42초

OS: XP

덤프 파일 열기

eProcess 분석

중지

csv로 결과 저장

# 취발성 데이터 수집 및 분석 - 네트워크 정보

- **목적:** 현재 네트워크 연결 및 사용정보를 바탕으로 비인가 접속 판별
- **방법:** 현재 연결된 IP 주소와 포트 등에 대한 점검, 연결 상태와 프로세스 별 연결 포트를 확인하여 허가되지 않은 사용 정보를 판별
- **도구:** netstat, netbios (Windows), Fport (Windows), netstat -an

```
C:\WINDOWS\system32\cmd.exe

K:\Tools\ForensicTools\Open Forensic Tools\Foundstone ForensicTools\Fport\Fport-2.0
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid Process Port Proto Path
1296 -> 135 TCP
4 System -> 139 TCP
4 System -> 445 TCP
1280 rapmgr -> 990 TCP C:\PROGRAM~1\MI3AA1~1\rapmgr
3052 -> 1028 TCP
3328 BateryApp -> 1040 TCP C:\Program Files\Batery\Bate
3328 BateryApp -> 1057 TCP C:\Program Files\Batery\Bate
0 System -> 1178 TCP
0 System -> 1185 TCP
```

Fport (Windows)

Netstat (Unix)

```
1 HP-UX 2 HP-UX 3 Ubuntu
# netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp 0 0 *.49173 * * * * LISTEN
tcp 0 0 *.2301 * * * * LISTEN
tcp 0 0 *.22 * * * * LISTEN
tcp 0 0 *.6010 * * * * LISTEN
tcp 0 0 127.0.0.1.49444 * * * * LISTEN
tcp 0 0 *.2148 * * * * LISTEN
tcp 0 0 *.515 * * * * LISTEN
tcp 0 0 *.49152 * * * * LISTEN
tcp 0 0 *.111 * * * * LISTEN
tcp 0 0 *.49157 * * * * LISTEN
tcp 0 0 *.901 * * * * LISTEN
tcp 0 0 *.6112 * * * * LISTEN
tcp 0 0 *.7815 * * * * LISTEN
tcp 0 0 *.543 * * * * LISTEN
tcp 0 0 127.0.0.1.7161 * * * * LISTEN
tcp 0 0 *.10864 * * * * LISTEN
tcp 0 0 *.135 * * * * LISTEN
tcp 0 0 *.5989 * * * * LISTEN
tcp 0 0 *.49168 * * * * LISTEN
tcp 0 0 *.25 * * * * LISTEN
tcp 0 0 *.587 * * * * LISTEN
tcp 0 0 *.6897 * * * * LISTEN
tcp 52 0 163.152.165.119.22 163.152.165.111.2622 ESTABLISHED
tcp 0 0 163.152.165.119.22 163.152.165.111.2127 ESTABLISHED
tcp 0 0 *.49263 * * * * LISTEN
```

# 네트워크 정보 - 현재 네트워크 연결 정보

## 현재 네트워크 연결 정보

- 호스트로 들어온 연결
- 호스트에서 나가는 연결
- 침입 흔적 정보 획득

## 수집방법 (netstat)

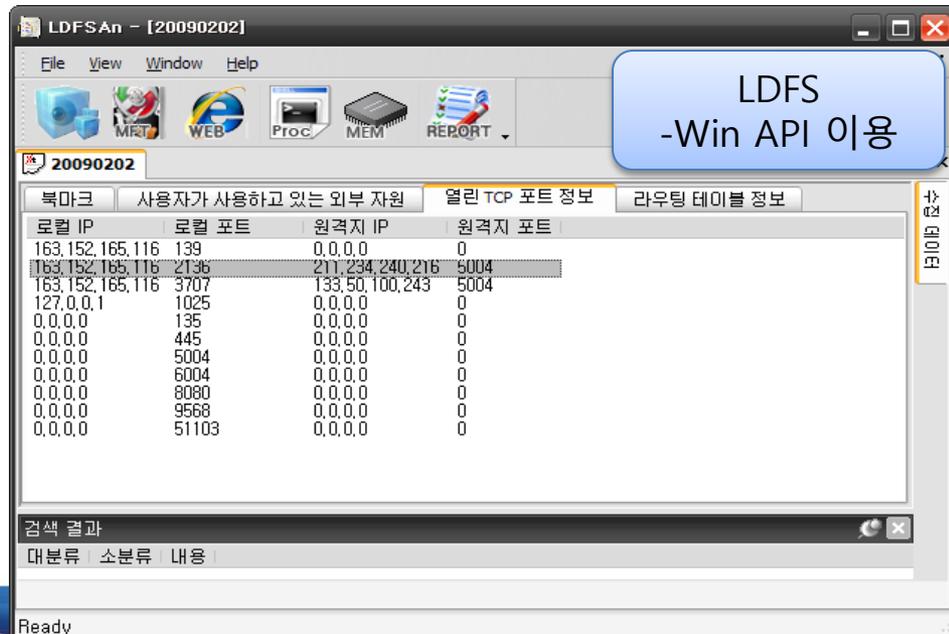
- netstat -ano
  - a:모든 연결, n:IP로 표시
  - o:Process ID
- 모든 네트워크 연결 정보 획득

```
D:\Tools\code>netstat -ano
```

netstat -ano

```
Active Connections
```

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1568
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5004	0.0.0.0:0	LISTENING	508
TCP	0.0.0.0:6004	0.0.0.0:0	LISTENING	508
TCP	127.0.0.1:1035	0.0.0.0:0	LISTENING	2764
TCP	163.152.146.233:139	0.0.0.0:0	LISTENING	4
TCP	163.152.146.233:1041	207.46.111.65:1863	ESTABLISHED	1080
TCP	163.152.146.233:1050	211.234.239.138:5004	ESTABLISHED	508
TCP	163.152.146.233:1842	220.69.247.1:80	CLOSE_WAIT	2772
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:500	*:*		1284
UDP	0.0.0.0:1025	*:*		1744
UDP	0.0.0.0:1031	*:*		472
UDP	0.0.0.0:1063	*:*		1744
UDP	0.0.0.0:4500	*:*		1284



# 네트워크 정보 - 열린 네트워크 포트와 프로세스 정보

## 열린 네트워크 포트와 연결된 프로세스 정보

- 특정 활성 포트와 매핑된 프로세스 정보
- 의심 가는 프로세스가 포트를 열고 데이터를 주고 받는다면 악성 코드 의심

## 수집방법

- Fport
- Foundstone사에서 제공하는 공개 버전의 콘솔 명령어

```
C:\Documents and Settings\Luke369x2>"H:\Tools\Live Forensics\Fport-2.0\Fport.exe"
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
```

Pid	Process	Port	Proto	Path
1172		-> 135	TCP	
4	System	-> 139	TCP	
4	System	-> 445	TCP	
2056		-> 1025	TCP	
3924	NATEONMain	-> 2136	TCP	C:\Program Files\NATEON\BIN\NATEONMain.exe
5232	MelOn	-> 3330	TCP	C:\Program Files\MelOn\Player\MelOn.exe
3924	NATEONMain	-> 3707	TCP	C:\Program Files\NATEON\BIN\NATEONMain.exe
3924	NATEONMain	-> 5004	TCP	C:\Program Files\NATEON\BIN\NATEONMain.exe
3924	NATEONMain	-> 6004	TCP	C:\Program Files\NATEON\BIN\NATEONMain.exe
1104	svchost	-> 8080	TCP	C:\WINDOWS\system32\svchost.exe
6596	P3MELO~1	-> 9568	TCP	C:\WINDOWS\system32\P3MELO~1.EXE
536	MSProxy	-> 51103	TCP	C:\Program Files\AhnLab\W3IS2007\MSProxy.ah

fport

LDFSAn - [20090202]

File View Window Help

20090202

북마크 UDP 열린 포트와 연결된 프로세스 정보 TCP 열린 포트와 연결된 프로세스 정보

로컬 IP	로컬 포트	원격지 IP	원...	프로세스 이름	PID	프로세스
0.0.0.0	135	0.0.0.0	0	N/A	1172	N/A
0.0.0.0	445	0.0.0.0	0	N/A	4	N/A
0.0.0.0	5004	0.0.0.0	0	NATEONMain.exe	3924	C:\Program Files\NATEON\BIN\NATEONMain.exe
0.0.0.0	6004	0.0.0.0	0	NATEONMain.exe	3924	C:\Program Files\NATEON\BIN\NATEONMain.exe
0.0.0.0	8080	0.0.0.0	0	svchost.exe	1104	C:\WINDOWS\system32\svchost.exe
0.0.0.0	9568	0.0.0.0	0	P3MELO~1.EXE	6596	C:\WINDOWS\system32\P3MELO~1.EXE
0.0.0.0	51103	0.0.0.0	0	MSProxy.ahn	536	C:\Program Files\AhnLab\W3IS2007\MSProxy.ahn
127.0.0.1	1025	0.0.0.0	0	N/A	2056	N/A
163.152.165.116	139	0.0.0.0	0	N/A	4	N/A
163.152.165.116	2136	211.234.240.216	5004	NATEONMain.exe	3924	C:\Program Files\NATEON\BIN\NATEONMain.exe
163.152.165.116	3707	133.50.100.243	5004	NATEONMain.exe	3924	C:\Program Files\NATEON\BIN\NATEONMain.exe

Ready

LDFS  
-Win API 이용

# 네트워크 정보 - 공유 파일

## Open Files

- 외부에서 원격으로 열려있는 파일 획득
- 허가 받지 않은 사용자가 접근해서 자원을 사용하는지 확인 필요

## 수집방법

- net file : 공유 파일 정보 출력 명령어
- psfile : sysinternal 사에서 제공하는 콘솔 명령어
- openfiles : 콘솔 명령어

# 네트워크 정보 - 공유 파일

- openfiles

- 열린 파일 조사

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\computer>openfiles

정보: 로컬에서 열린 파일을 보려면 시스템 글로벌 플래그 'maintain objects list' 를
사용하도록 설정해야 합니다. 자세한 내용은 Openfiles /? 를 확인하십시오.

로컬 공유 지점을 통해 원격으로 열린 파일:
-----
ID      액세스한 사용자      종류      열린 파일 <경로#실행 파일>
-----
22      BROMPTON              Windows   C:\kwon
44      BROMPTON              Windows   C:\kwon\네오플러스1_분석_권태석.ppt
C:\Documents and Settings\computer>
```

- psfile

- 원격에서 접근한 파일 정보 획득

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\computer>"C:\Documents and Settings\computer\바탕 화면
\Tools\Tools\PsTools\Psfile.exe"

psfile v1.02 - psfile
Copyright ?2001 Mark Russinovich
Sysinternals

Files opened remotely on KTS:

[22] C:\kwon
      User: BROMPTON
      Locks: 0
      Access: Read

[44] C:\kwon\??????.??_???.ppt
      User: BROMPTON
      Locks: 0
      Access: Read

C:\Documents and Settings\computer>
```

# 네트워크 정보 - 외부 시스템 연결 정보

## 외부 시스템 연결 정보

- 사용자가 원격으로 사용하고 있는 공유 자원 정보 획득
- 허가 받지 않은 외부 자원 → 정보 유출

## 수집방법

- nbtstat -c (c : Cached NetBIOS Name Table)
- IP, 네트워크에 연결된 후 현재까지의 시간 등의 정보 조사

```
C:\Documents and Settings\computer>nbtstat -c
```

```
로컬 영역 연결:
```

```
Node IpAddress: [163.152.146.203] Scope Id: []
```

### NetBIOS Remote Cache Name Table

Name	Type	Host Address	Life [sec]
163.152.146.233<20>	UNIQUE	163.152.146.233	295
DONCOM <20>	UNIQUE	163.152.146.194	422

```
C:\Documents and Settings\computer>_
```

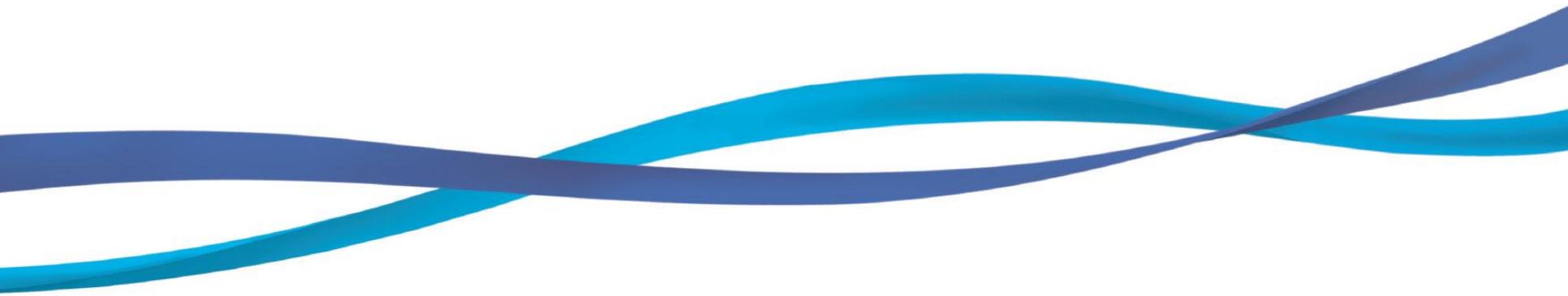
# 비휘발성 데이터

- 전원을 차단해도 사라지지 않는 데이터
- 쓰기방지 장치를 부착하여 수집하는 것이 원칙
- 시스템을 종료시키지 못하는 환경에서는 활성 시스템에서 직접 데이터 수집 및 분석이 필요
- 데이터 선별을 통해 사건과 관련된 비휘발성 데이터만을 수집하는 경우도 있음

# 활성 시스템 데이터 수집

- 운영체제 종류별로 수집에 사용할 수 있는 도구 및 시스템 API가 다름
  - 활성 시스템 데이터 수집도구는 이러한 특성을 고려하여 개발
- 시스템 상태의 변경을 최소화 해야 하므로 **CLI(Command Line Interface)**의 사용을 권장
- 시스템 명령어, 라이브러리를 정적으로 포함하고 있는 도구를 사용, 읽기만 가능한 매체에서 실행할 것을 권장

# 3. 디스크 이미징



- 디스크 이미징 장비 (**Disk Imaging Hardware**)

- 단독으로 복제 디스크를 생성할 수 있는 포렌식 장비
- 디스크를 컴퓨터에 연결하지 않고 다른 하드디스크에 사본을 생성
- LogiCube Talon, Dossier
- ICS ImageMasster Solo 3 & 4 등



Logicube Talon



Logicube Dossier

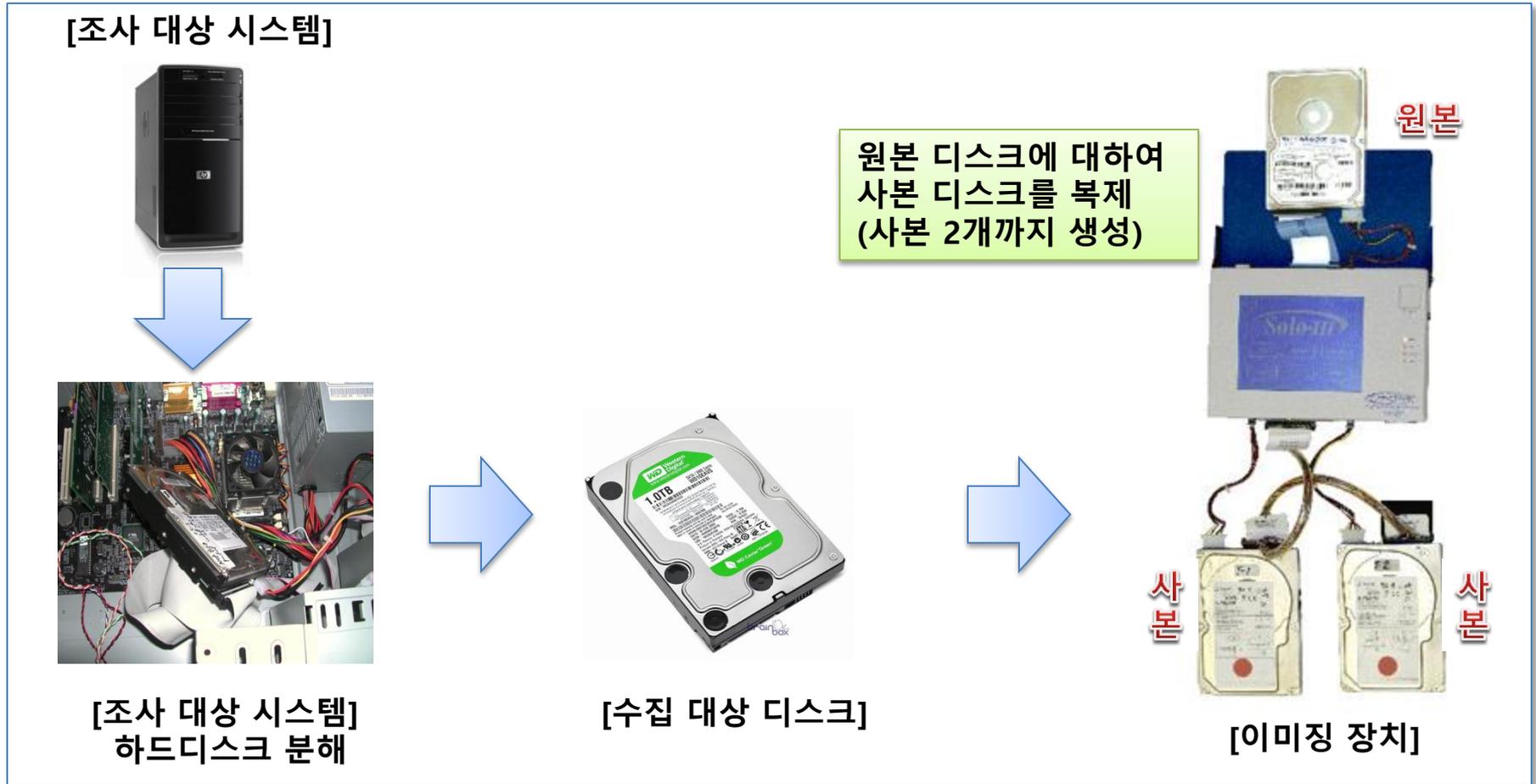


ICS Image Masster Solo3



ICS Image Masster Solo4

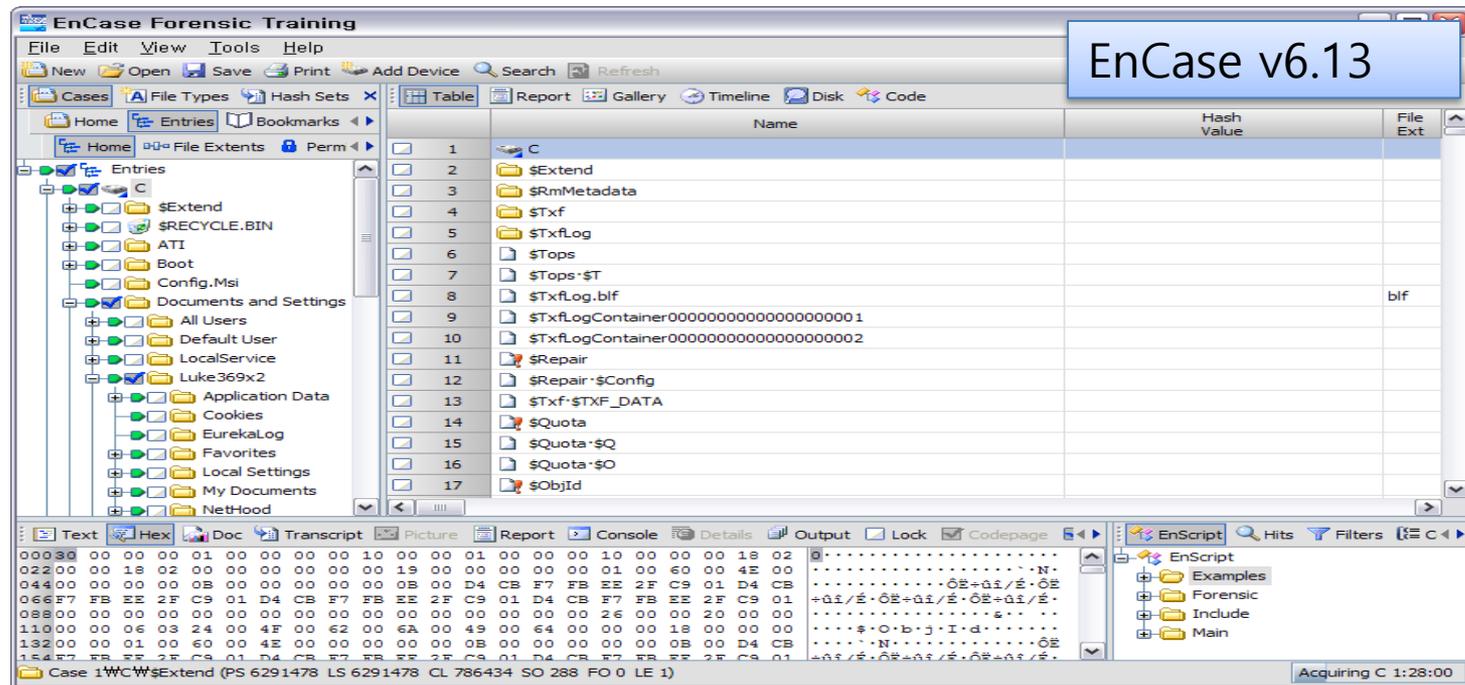
# 디스크 이미징 장비를 이용한 사본 생성 절차



# 디스크 이미징 및 분석

## • EnCase

- Guidance Software 에서 개발한 세계에서 가장 널리 쓰이는 포렌식 S/W
- 그래픽 인터페이스 바탕으로 디스크 이미징, 디스크 브라우징 기능 제공
- 증거 미리보기 및 데이터 검색/분석 기능 제공
- 윈도우, Palm OS 등의 플랫폼과 RAID 방식 지원



# 디스크 이미징 S/W를 이용한 사본 생성 절차

[조사 대상 시스템]

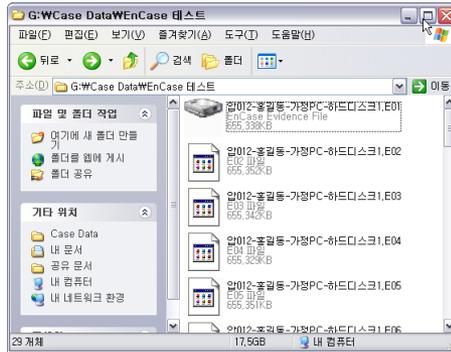


분해



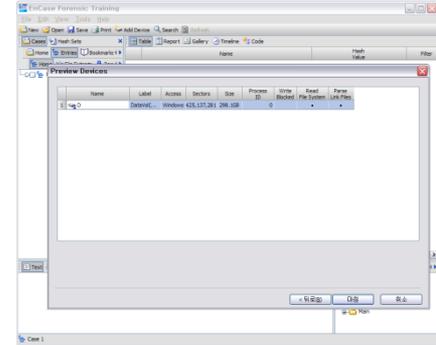
[수집 대상 디스크]  
쓰기 방지 장치에 연결

[이미지 파일]



획득

[디스크 이미징 도구]



수집



[쓰기방지 장치]  
분석 시스템과 쓰기 방  
지 장치 연결



[분석 시스템]

# EnCase를 이용한 디스크 이미징

The image displays two overlapping screenshots of the EnCase Forensic Training software. The top-left screenshot shows the 'Case Options' dialog box with the following fields: Name (Case-Test-1), Examiner Name (임경수), Default Export Folder (C:\Program Files\EnCase\Export), Temporary Folder (C:\Program Files\EnCase\Temp), and Index Folder (C:\Program Files\EnCase\Index). A blue callout box below this dialog reads '기본 창에서 사건 파일 생성' (Generate case file from basic window). The bottom-right screenshot shows the main software interface with the 'Add Device' button highlighted by a red box and a white arrow. A blue callout box below this button reads '사건 파일에 저장 매체 추가' (Add storage media to case file). A large black curved arrow points from the 'Add Device' button back to the 'Case Options' dialog box.

# EnCase를 이용한 디스크 이미징

마운트할 논리 드라이브를 선택

	Label	Access	Sectors	Size	Process ID	Write Blocked	Read File System	Parse Link Files
<input checked="" type="checkbox"/>	1 WinXP(WD320B)	Windows	206,483,381	98.5GB	0		•	•
<input type="checkbox"/>	2 DataVol(WD320A)	Windows	625,137,281	298.1GB	0		•	•
<input type="checkbox"/>	3 Down(WD320B)	Windows	418,637,834	199.6GB	0		•	•
<input type="checkbox"/>	4 HL-DT-ST	ASPI	356,880	697MB	0		•	•
<input type="checkbox"/>	5 Backup(BC500)	Windows	351,277,226	167.5GB	0		•	•
<input type="checkbox"/>	6 Contents(BC500)	Windows	625,474,709	298.2GB	0		•	•
<input type="checkbox"/>	7 W							
<input type="checkbox"/>	8 S							
<input type="checkbox"/>	9 W							

Preview Devices

Name	Label	Access	Sectors	Size	Process ID	Write Blocked	Read File System	Parse Link Files
1 C	WinXP(W...	Windows	206,483,381	98.5GB	0		•	•

디스크 마운트 중 -파일 시스템을 읽는 과정

Parsing MFT

< 뒤로(←)    마침    취소

# EnCase를 이용한 디스크 이미징

- 윈도우 운영체제가 설치된 C 드라이브를 마운트한 상태

The screenshot displays the EnCase Forensic Training interface. The main window shows a file explorer view of a mounted C drive. The left pane shows a tree view of the drive's contents, including folders like .zenmap, Application Data, Cookies, EurekaLog, Favorites, IECompatCache, IETldCache, Local Settings, NetHood, PrintHood, PrivaCI, Recent, SendTo, Templates, Tracing, UserData, 바탕 화면 (Desktop), 시작 메뉴 (Start Menu), and NetworkService. The right pane shows a table of files and folders with columns for Name, Filter, In Report, File Ext, File Type, File Category, and Signat. The table lists 20 items, including folders like DFRC-116 and evidenceBag, and files like Helix2009R1.iso, [Luke의 논문연구]..., and QOOK 아이디스크... The bottom pane shows a hex editor view of the selected file, displaying hexadecimal data. The status bar at the bottom indicates the current file path: Case-Test-01\WC\Documents and Settings\Luke369x1\바탕 화면\DFRC-116 (PS 6352302 LS 6352302 CL 794037 SO 296 FO 0 LE 1).

	Name	Filter	In Report	File Ext	File Type	File Category	Signat
<input checked="" type="checkbox"/>	1	DFRC-116					
<input checked="" type="checkbox"/>	2	evidenceBag					
<input checked="" type="checkbox"/>	3	제비					
<input checked="" type="checkbox"/>	4	파일 확장자 변경					
<input checked="" type="checkbox"/>	5	Helix2009R1.iso		iso			
<input checked="" type="checkbox"/>	6	Helix2009R1.iso-Zo...		Ide...			
<input checked="" type="checkbox"/>	7	[Luke의 논문연구]...		Ink	Link	Windows	
<input checked="" type="checkbox"/>	8	컴퓨터 관리.lnk		Ink	Link	Windows	
<input checked="" type="checkbox"/>	9	100326_(협의전마...		hwp			
<input checked="" type="checkbox"/>	10	#최근 작업의 바...		Ink	Link	Windows	
<input checked="" type="checkbox"/>	11	산업원천_사업계...		hwp			
<input checked="" type="checkbox"/>	12	Total Commander.lnk		Ink	Link	Windows	
<input checked="" type="checkbox"/>	13	사본 - Helix2009R1...		iso			
<input checked="" type="checkbox"/>	14	사본 - Helix2009R1...		Ide...			
<input checked="" type="checkbox"/>	15	Encase_LinEn(Helix...		iso			
<input checked="" type="checkbox"/>	16	Corpora.one		one			
<input checked="" type="checkbox"/>	17	Google 크롬.lnk		Ink	Link	Windows	
<input checked="" type="checkbox"/>	18	ADRIANE-KNOPPIX...		iso			
<input checked="" type="checkbox"/>	19	ADRIANE-KNOPPIX...		Ide...			
<input checked="" type="checkbox"/>	20	QOOK 아이디스크...		Ink	Link	Windows	

# EnCase를 이용한 디스크 이미징

- 원도우 운영체제가 설치된 C 드라이브를 마운트한 상태

The screenshot shows the EnCase Forensic Training interface. On the left, a tree view shows the 'C' drive mounted. A context menu is open over the drive, with 'Acquire...' highlighted. A blue callout box with an arrow points to this menu item, containing the text '마운트한 디스크를 이미징하여 획득' (Acquire the mounted disk for imaging). The main window displays a table of files and folders on the C drive.

	Name	Filter	In Report	File Ext	File Type	File Category
<input checked="" type="checkbox"/>	1	Folder				
<input checked="" type="checkbox"/>	2	File				
<input checked="" type="checkbox"/>	3	File				
<input checked="" type="checkbox"/>	4	File				
<input checked="" type="checkbox"/>	5	File				
<input checked="" type="checkbox"/>	6	File				
<input checked="" type="checkbox"/>	7	File				
<input checked="" type="checkbox"/>	8	File				
<input checked="" type="checkbox"/>	9	File				
<input checked="" type="checkbox"/>	10	File				
<input checked="" type="checkbox"/>	11	File				
<input checked="" type="checkbox"/>	12	Folder				
<input checked="" type="checkbox"/>	13	Folder		0		
<input checked="" type="checkbox"/>	14	Folder				
<input checked="" type="checkbox"/>	15	File		dll	Dynamic Link Library	Code Library
<input checked="" type="checkbox"/>	16	File		dll	Dynamic Link Library	Code Library
<input checked="" type="checkbox"/>	17	File		dll	Dynamic Link Library	Code Library
<input checked="" type="checkbox"/>	18	File		dll	Dynamic Link Library	Code Library
<input checked="" type="checkbox"/>	19	File		dll	Dynamic Link Library	Code Library
<input checked="" type="checkbox"/>	20	File		dll	Dynamic Link Library	Code Library

# EnCase를 이용한 디스크 이미징

The image shows a screenshot of the EnCase software interface during the disk imaging process. It features three overlapping windows: 'After Acquisition', 'Search', and 'Options'. The 'After Acquisition' window is in the background, the 'Search' window is in the middle, and the 'Options' window is in the foreground. Three blue callout boxes with white text and arrows point to specific settings in each window. A large black curved arrow on the left side of the 'After Acquisition' window points towards the 'Options' window. At the bottom left, there is a blue banner with the text '53/72'. At the bottom right, there are three buttons: '< 뒤로(B)', '마침', and '취소'.

**After Acquisition**

- Acquire another disk
- Search, Hash and Signature Analysis
- New Image File
  - Do not add
  - Add to Case
  - Replace source device
- Restart Acquisition
- Existing Evidence File
  - C:\Program Files\EnCase

**Search**

- Search entire case
- Keyword Search Options
  - Search entries and records for keywords
    - Selected keywords only 9 keywords
  - Search entry slack
  - Use initialized size
  - Undelete entries before searching
  - Search only slack area of entries in Hash List
- Hash Options
  - Compute hash value
  - Recompute hash values

**Options**

- Name: C
- Case Number: 100405-테스트-하드디스크-001-C
- Notes: 윈도우 XP가 설치된 C 드라이브 - NTFS 파일 시스템
- File Segment Size (MB): 640
- Compression:
  - None
  - Good (Slower, Smaller)
  - Best (Slowest, Smallest)
- Start Sector: 0
- Stop Sector: 206483380
- Password:
- Confirm Password:
- Block size (Sectors): 64
- Error granularity (Sectors): 64
- Acquisition MD5  Acquisition SHA1
- Quick reacquisition  Read ahead
- Output Path: Y:\테스트\Case-100405-01\C.E01
- Remote acquisition
- Alternate Path:

< 뒤로(B)    마침    취소

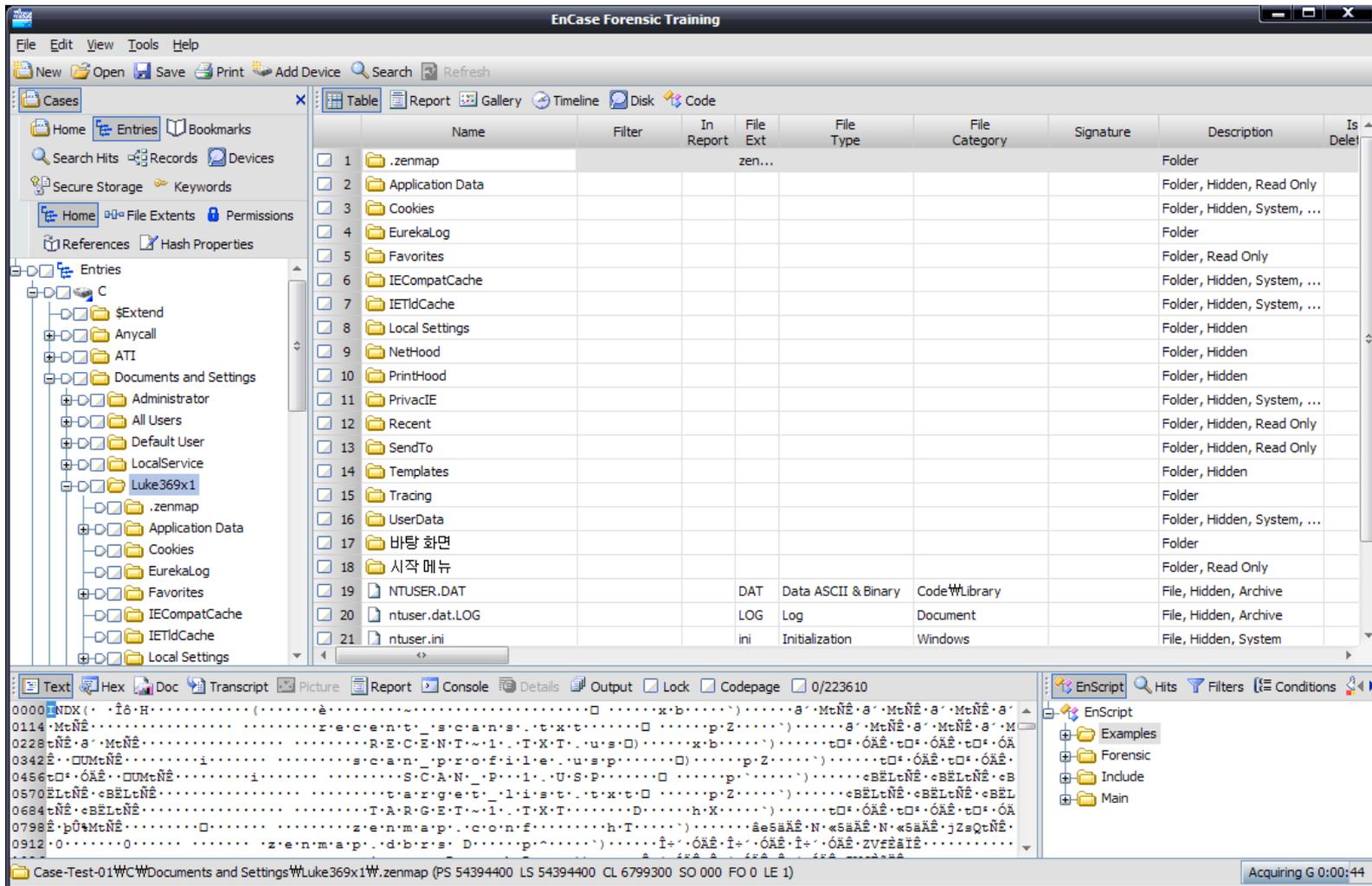
현재 사건 파일에 이미지 파일을 추가할 지 결정

탐색 기법에 대한 옵션 설정

획득할 이미지 파일의 메타데이터와 저장 경로 등을 설정

# EnCase를 이용한 디스크 이미징

- 디스크 이미징 완료 후, 이미지 파일에서 조사 수행



# Live CD와 Live Analysis CD

## Live CD (ex. Knoppix)

- Live CD는 Bootable CD로, 전원이 꺼져있는 오프라인 시스템을 조사할 때 사용
- 원본 OS에 영향을 끼치지 않으려는 목적으로 제작해서 사용
- 디스크 이미징, 데이터 열람 등이 가능하나, 활성 데이터 분석에는 맞지 않음



## Live-Analysis CD (ex. Helix)

- 대부분의 라이브 분석 CD 는 Live CD 의 기능을 내장하고 있음
- 활성 시스템 조사나 활성 시스템에서 디스크 이미징을 수행하려는 목적으로 사용
  - 원본 OS의 영향을 최소화하기 위해 도구뿐만 아니라 사용하는 DLL도 내장하여야 함
  - 프로세스 수집, 네트워크 정보 수집 등과 같이 활성 시스템 조사 기능이 탑재



# Helix 3 라이브 분석 CD 소개

- Helix 3 소개
  - 라이브 포렌식을 위한 Bootable 도구
  - 우분투 기반의 포렌식 분석용 Bootable 도구
- 3개의 Helix 버전
  - Helix 3 (Live Response)
    - 휘발성 데이터 수집 및 디스크 이미징
    - 사건 발생 시, 즉각적인 조사 대응을 위한 도구
  - Helix 3 Pro
    - 기본 버전에 파일 카빙, 모바일 데이터 수집 도구 등을 추가
  - Helix 3 Enterprise
    - E-Discovery 중점의 침해사고 대응
- Helix 3 기본 버전기능
  - 시스템 기본 정보
  - 하드웨어 장치 정보
  - 디스크 구성 정보
  - 디스크 이미징
  - 휘발성 데이터 수집, 파일시스템 데이터 열람 등



Helix 3 로 부팅 시



활성 시스템에서 Helix 3  
실행 시 기본 화면

# Helix 3 실행 화면

HELIX2009R1 (01/06/2009)

File Quick Launch Page Help

HELIX™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS

## System Information

**Operating System:**  
Windows XP Service Pack 3

**Owner Information:**  
Owner: KyungSoo Lim  
Organization: DFRC-CIST  
Admin: No  
Admin Rights: Yes

**Network Information:**  
Host: DFRC-116  
User: Luke369x1  
IP: 163.152.165.116  
NIC: 005056c00001  
Domain:

Drive:	Label:	Type:	Size:
C:\	(Logical drive)	ERROR	100821.9 MB
D:\	(Logical drive)	ERROR	305242.8 MB
E:\	(Logical drive)	ERROR	204413 MB
I:\	(CD/DVD-ROM drive)		
J:\	(Logical drive)	ERROR	7824.6 MB
X:\	(Logical drive)	ERROR	171522 MB
Y:\	(Logical drive)	ERROR	305407.5 MB
Z:\	(Logical drive)	ERROR	697 MB

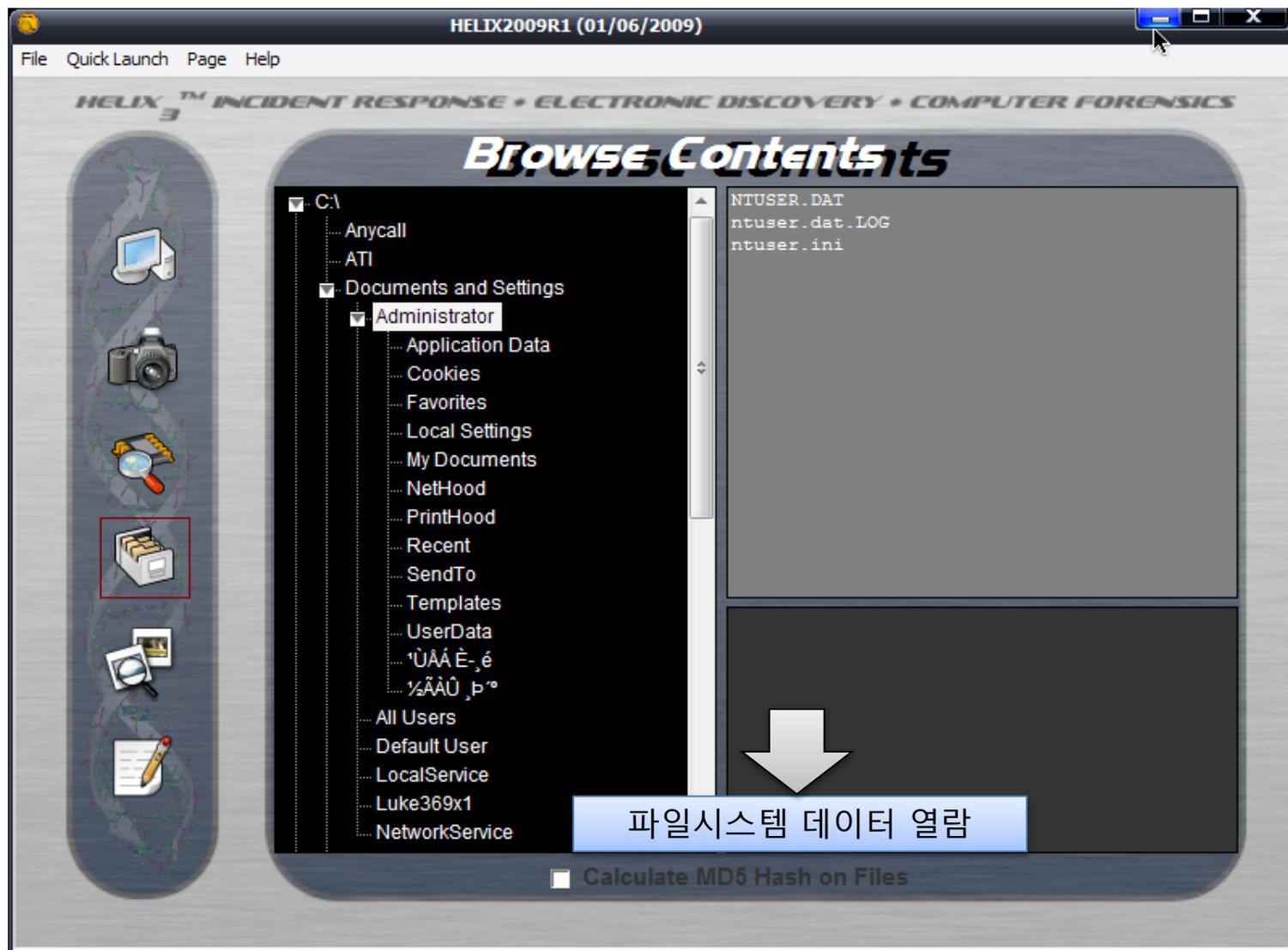
시스템 기본 정보 출력

Page 1 of 2

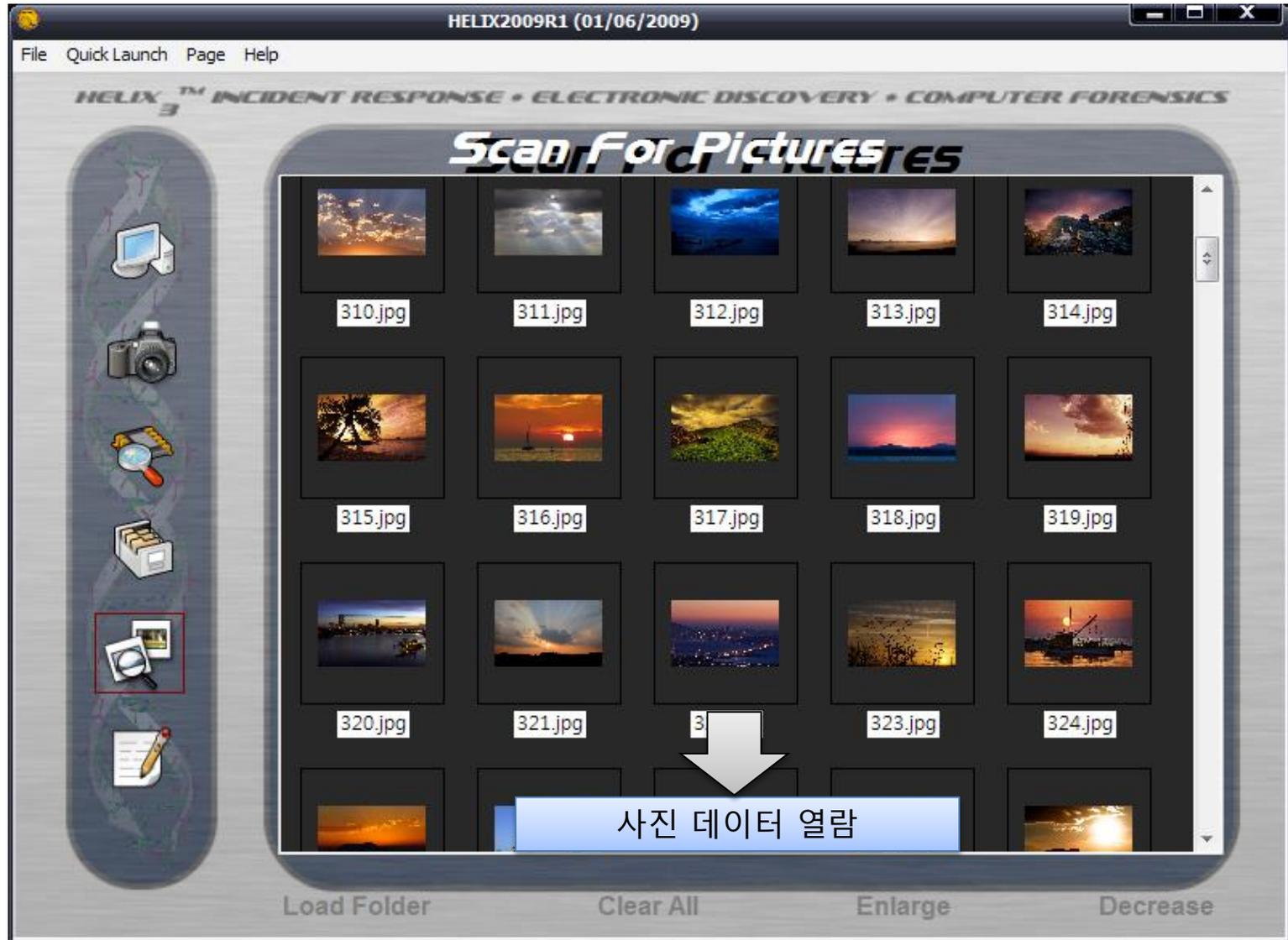
# Helix 3 실행 화면



# Helix 3 실행 화면



# Helix 3 실행 화면



# Helix 3를 이용한 디스크 이미징

The screenshot shows the Helix 3 Live Acquisition window. On the left is a vertical toolbar with icons for various acquisition methods. The main area is titled 'Live Acquisition' and 'Acquire Physical Memory and/or Disk Drives'. It contains several input fields and options:

- Source:** A text field containing '\\.\PhysicalDrive4 - pqi IntelligentStick USB Device [3.7 GB USB]'. An arrow points from this field to a blue callout box.
- Location Options:** Radio buttons for 'Attached/Share' (selected) and 'NetCat'.
- Destination:** A text field containing 'Y:\디스크 이미지'. An arrow points from this field to a blue callout box.
- Image Name:** A text field containing 'PQI\_usb\_image.dd', highlighted with a red border. An arrow points from this field to a blue callout box.
- DD Options:** Includes 'block size: default', 'conv: noerror', and a 'Split Image' checkbox.
- Acquire:** A large button at the bottom center. An arrow points from this button to a blue callout box.

At the bottom right of the window, it says 'Page 1 of 2'.

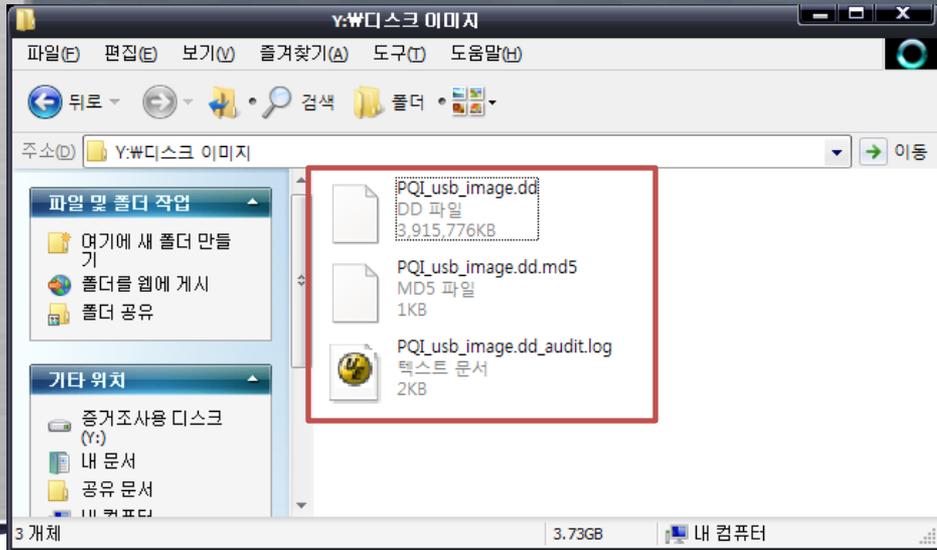
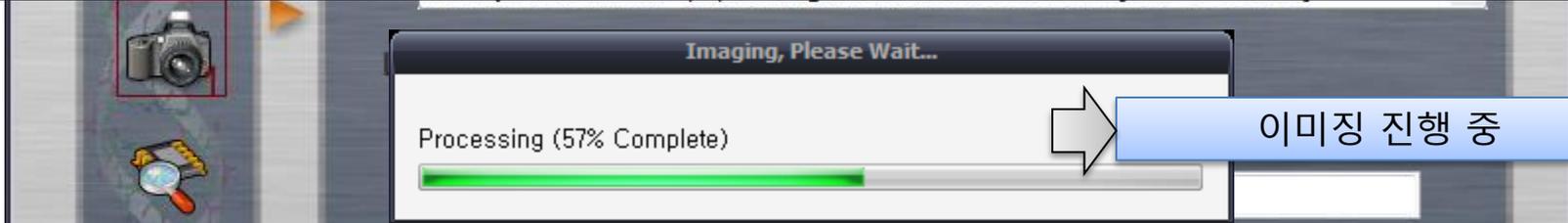
이미징할  
저장 매체 선택

이미지 파일을  
저장할 매체 선택

이미지 파일  
이름 설정

수집 실행

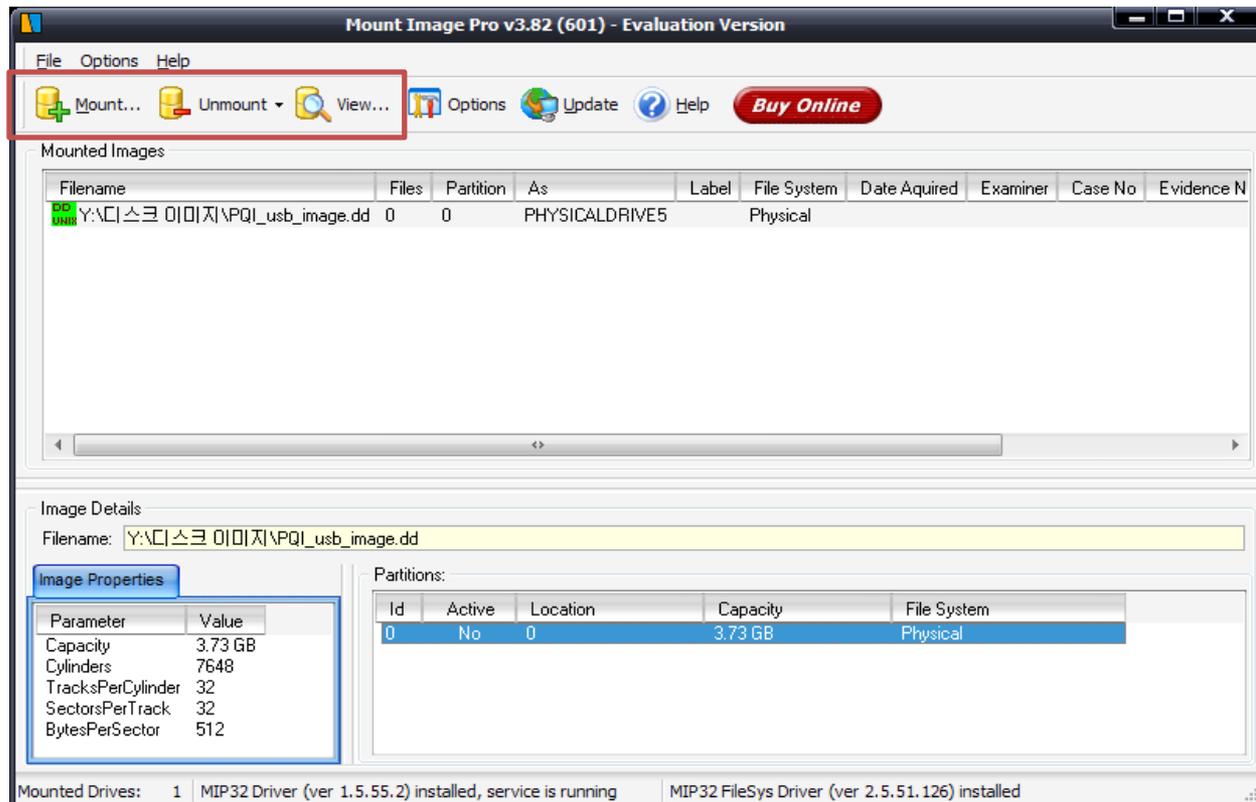
# Helix 3를 이용한 디스크 이미징



# Image Mount Pro를 활용한 이미지 파일 열람

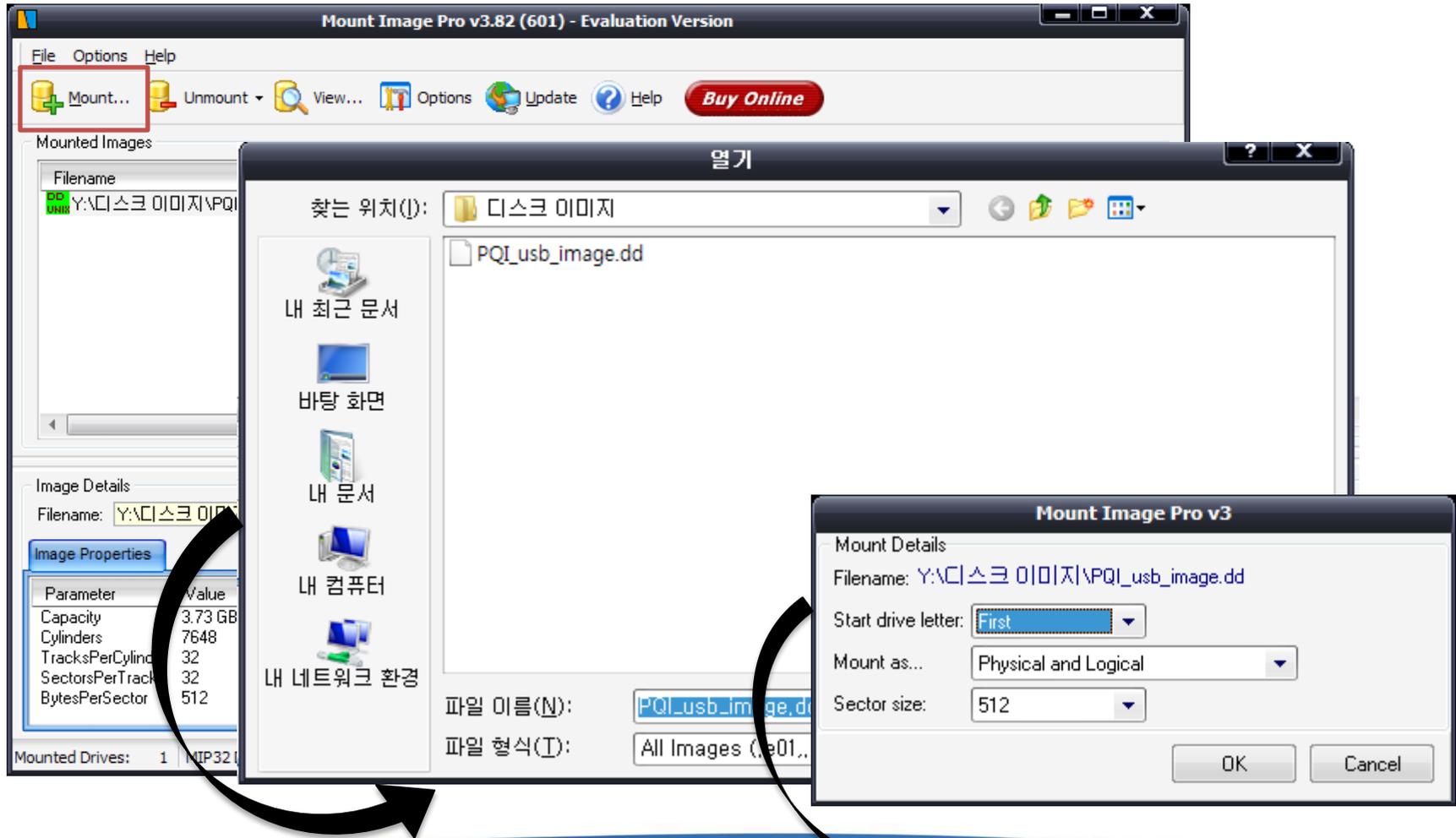
## • Image Mount Pro 소개

- 다양한 이미지 파일(DD, Encase, FTK 등)을 열람할 수 있도록 마운트 기능을 지원하는 도구
- 마운트한 이미지는 EnCase 등의 도구를 활용하여 해당 도구의 이미지로 재생성하거나 분석이 가능



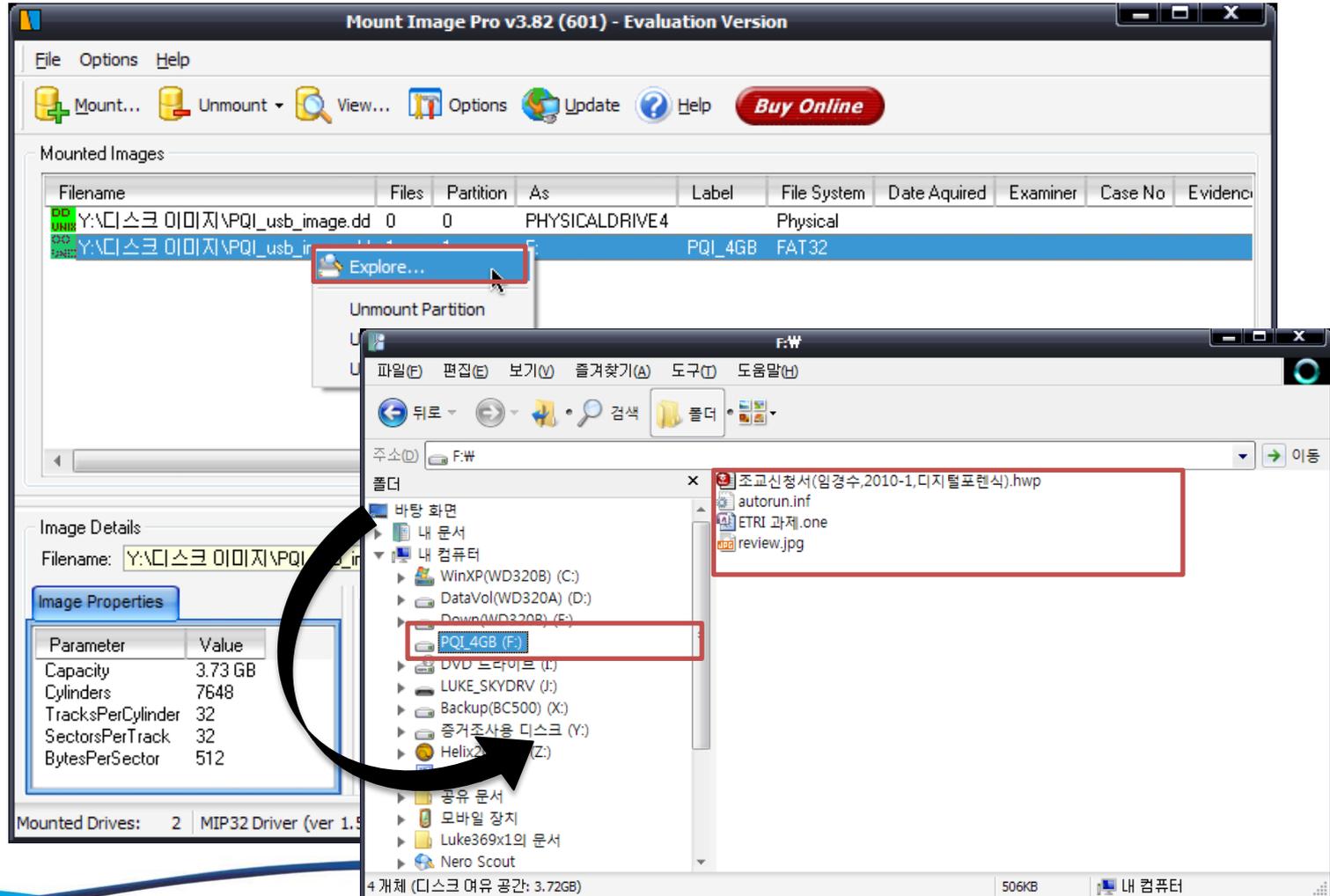
# Image Mount Pro를 활용한 이미지 파일 열람

- Mount 실행 → 이미지 파일 선택 → 마운트 옵션 설정



# Image Mount Pro를 활용한 이미지 파일 열람

- 마운트가 완료되면 논리적으로 하나의 드라이브가 마운트됨



# Image Mount Pro를 활용한 EnCase 분석

- Image Mount Pro로 마운트한 DD 이미지를 EnCase로 분석

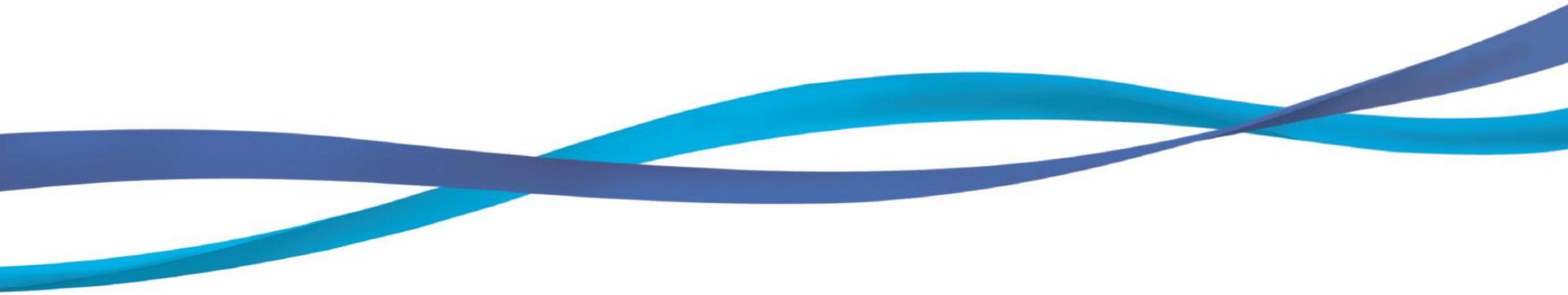
EnCase Forensic Training

	Name	Filter	In Report	File Ext	File Type	File Category	Sign
1	Folder						
2	SubFolder						
3	Desktop.ini			ini	Initialization	Windows	
4	FILE.EXE			EXE	Windows Executable	Code\Executable	
5	RECYCLER						
6	S-1-5-21-1482476501-1644491937-682003330-1013						
7	Desktop.ini			ini	Initialization	Windows	
8	wisenis32.exe			exe	Windows Executable	Code\Executable	
9	ETRI 과제.one			one			
10	조교신청서(임경수,2010-1,디지털포렌식).hwp			hwp			
11	_1020511.JPG			JPG	JPEG	Picture	
12	_1020512.JPG			JPG	JPEG	Picture	
13	_1020513.JPG			JPG	JPEG	Picture	
14	_1020516.JPG			JPG	JPEG	Picture	
15	_1020517.JPG			JPG	JPEG	Picture	
16	_1020518.JPG			JPG	JPEG	Picture	
17	_1020519.JPG			JPG	JPEG	Picture	
18	_1020520.JPG			JPG	JPEG	Picture	
19	_1020521.JPG			JPG	JPEG	Picture	
20	_1020522.JPG			JPG	JPEG	Picture	

Case-Test-01\F\F\F\\_1020519.JPG (PS 41392 LS 41392 CL 3263 SO 000 FO 0 LE 0)

단순히 마운팅 상태에서 볼수 없었던 삭제되었던 사진 파일이 확인됨

## 4. 임베디드 시스템의 증거 확보



# 모바일 기기 증거자료 추출 방법

- 휴대폰 주요 데이터
  - 최근 통화, 문자메시지, 전화번호부, 일정, 메모, 사진 및 동영상 등
- 데이터 획득 방법

## 논리적 수집 방법



or



Request Files

Sending Files



## 물리적 수집 방법

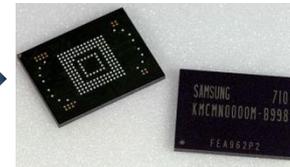
using JTAG Interface



or



using Flash Memory Reader



# 스마트폰 증거자료 추출 방법

- 스마트폰 주요 데이터
  - 휴대폰 데이터 + 이메일, 아웃룩(MS), 인터넷 사용 기록, GPS 정보 등
- 데이터 획득 방법

## 논리적 수집 방법



MS ActiveSync

or

Remote  
API



## 물리적 수집 방법

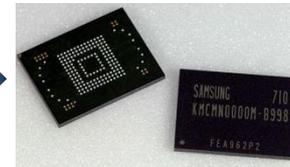
using JTAG Interface



or



using Flash Memory Reader



# 모바일 데이터의 분석

- 모바일 포렌식

- 휴대폰 데이터 분석 항목

데이터	항목
수신 문자메시지(SMS)	수신 일시, 송신자 전화번호, 문자내용
발신 문자메시지(SMS)	발신 일시, 수신자 전화번호, 문자내용
임시저장 문자메시지(SMS)	저장 일시, 수신자 전화번호, 문자내용
최근 통화 기록(Call History)	통화종류, 송수신자 전화번호, 통화시간
전화번호부(PhoneBook)	저장된 이름, 전화번호, 단축번호, 그룹
일정(Schedule)	일정 일시, 일정내용
메모(Memo)	메모 일시, 메모내용
사진(Photo)	사진 콘텐츠, 사진 촬영 정보
멀티미디어(Multimedia)	동영상, 음성 메모, 음악 등
휴대폰 전자일련번호(ESN)	제조사 식별 코드, 기기 일련 번호
휴대폰 비밀번호	※ 휴대폰 잠금 해제

# 모바일 데이터 분석 도구 실행화면

MobileDataAnalyzer - [보낸문자]

File Tools View Help

Filter:

Tree View

- SPH-V6900
  - \$SYS.FACTORY
  - brew
  - album\_config
  - apps
  - autoans
  - cam
  - contents
  - eventlist.dat
  - handynet
  - info
  - media
  - mms
  - nvm
  - PIMS
  - prefs.dat
  - scrsct
  - shared
  - shortcut
  - sndmcr

번호 상태 발신날짜 수신번호 내용

1	저장	2008-02-23 13:57	011	9	애니 나도 가는 길이야 이제 해화역 전동이 없으니 계속 쳐다보는 방법밖에 없네 ㅎㅎ
2	저장	2008-02-23 13:59	011	9	그르게, 역시 우리 급만남이 체질인가봐ㅋ 오랜만에 초채한 모습으로 연속촬영 고고생!
3	저장	2008-02-23 14:13	011	9	도학! 교보오면 전화 부탁!
4	저장	2008-02-23 14:29	011	9	난 썬 있는 쪽이랑도 사람 엄청나다 진짜!!!!
5	저장	2008-02-23 18:37	011	9	애니야 사실 그냥 너보고 문득 떠오른 이야기였어 우리 모두 힘내자 다음에도 급만남 고!
6	저장	2008-02-23 18:39	011	9	그래그래 너도 최노애락 어떤 이야기든 하고프면 연락주오! 미친 조심해 가(ノ^^)ノ
7	저장	2008-02-23 18:41	011	9	애니야 나 그날 사이 가입하지말까봐....
8	저장	2008-02-23 18:48	011	9	나 또 진동 안와서 문자를 올렸어ㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋ
9	저장	2008-02-24 12:19	010	5	토익 망했다
10	저장	2008-02-24 14:41	010	5	나 올린 폰 계약했다 케오
11	저장	2008-02-24 14:52	010	5	번호는 010 3231 8093
12	저장	2008-02-24 15:01	010	5	애니 여긴 그게 없네 나
13	저장	2008-02-24 15:03	010	5	그렇긴한데 우리부모님
14	저장	2008-02-24 15:08	011	9	나 올린 폰 계약했다 케오
15	저장	2008-02-25 09:20	010	2	엡 그림 연구실서 땀것습

Search & Graph

전화번호: 011 검색

시작일: 2005-01-01 종료일: 2007-01-04

문자내용

번호	항목구분	날짜	전화번호	내용 (통화시간)
1	보낸 문자	2006-04-05 15:01	01638	바분
2	보낸 문자	2006-04-05 15:02	01671	바분
3	보낸 문자	2006-04-05 21:01	01929	세미나중
4	보낸 문자	2006-09-29 20:27	01954	
5	보낸 문자	2006-09-29 20:27	01648	
6	보낸 문자	2006-11-05 00:13	번호없음	배터리가다웠습니다~ 하하, 말씀감사합니다. 자주연락드릴게요^^
7	보낸 문자	2006-11-06 12:54	01954	what are you doing? am sleeping!\$^*+*+* are you working now? you ought to sleep
8	보낸 문자	2006-11-06 13:17	번호없음	와우! 방금네 가장큰그치고했네!나와서엿전우지개를 그려놓았네요! 칭찬좀될드
9	보낸 문자	2006-11-06 15:00	011230	고객님 덕분에(601521)를 오늘 배달예정입니다. 서울성복우체국 검경속
10	보낸 문자	2006-11-07 00:02	번호없음	나의과거는결국바꿀수없지만오늘내행동을바꿈으로써나의의미라를바꿀수있다.
11	보낸 문자	2006-11-07 09:55	0104629	hi! thank you for help me! i am thinking now,brother! do not worry!get to

Image Viewer

미리 보기

자랑 이미지

Exit Tag

포도상 사용 여부 No

Encoding Unknown

압축 레벨 (Jpeg Quality) Unknown

노출 프로그램

각자 설정

화이트 밸런스 Unknown

노출 자수 0.00

ISO 크기 0

초점 거리 0.00mm

조리개 값 0.0

발기 0.000

노출 시간 (1/-2147483648)

35mm Equivalent 0

CCD Width 0.00mm

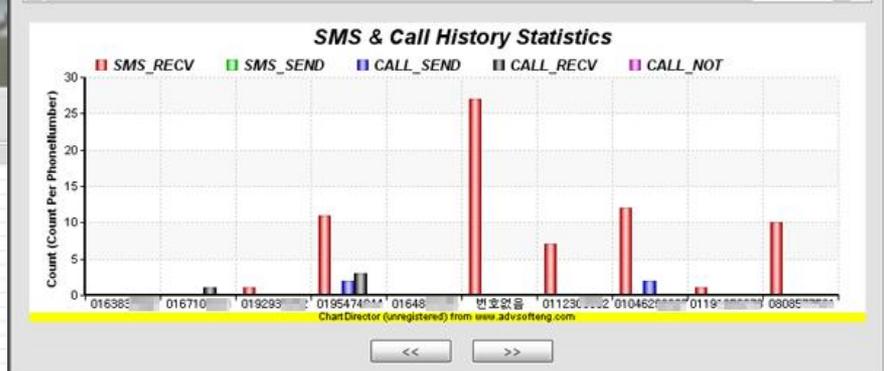
Focal Length 0.0mm

플래시 사용 여부 No

Is Color

방향 정위(Orientation) 0

Y방향 해상도(dpi) -1,\$



Q

&

A