SeoulTech

6장 디지털 증거 수집 기술

박 종 혁 교수

UCS Lab

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

개요

- 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. 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)

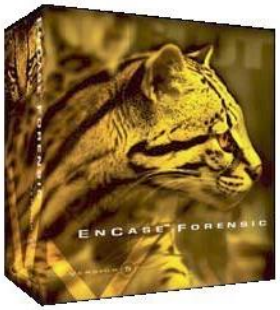
이동형 포렌식 워크스테이션
(Forensic Air-Lite V MK III)

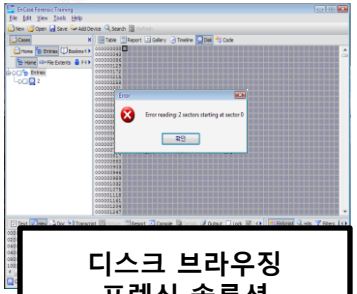
이동형 포렌식 워크스테이션
(ICS RoadMasster 3)

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

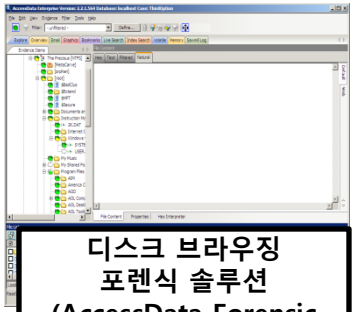
메모리카드 쓰기 방지 장치
(ICS Write Protect Card Reader)

디지털 증거 조사 과정에서 사용되는 포렌식 SW

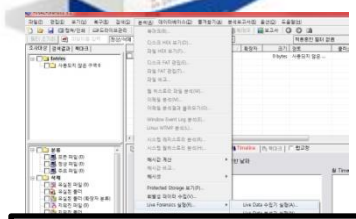




디스크 브라우징
포렌식 솔루션
(Guidance Encase v6)



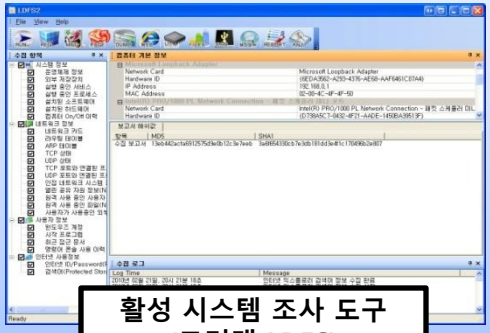
디스크 브라우징
포렌식 솔루션
(AccessData Forensic
Toolkit v3.0)



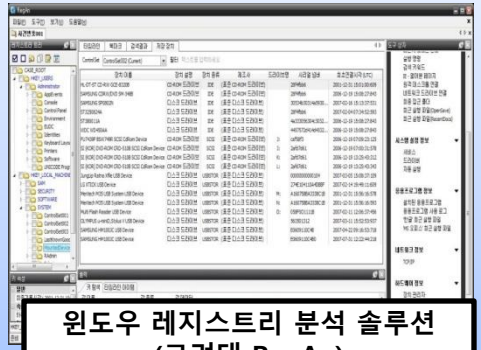
디스크 브라우징
포렌식 솔루션
(파이널데이터
Final Forensics v2.0)

라이브 포렌식 도구
(Helix 3)

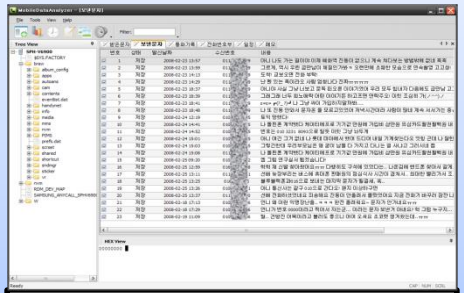
휴대폰 포렌식 솔루션
(Paraben Device Seizure v3.3)



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 즉석 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

휘발성 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	운영체제 설정 정보	사용자 정보	응용프로그램 정보

• 메타데이터 정보를 이용, 조사에 필요한 파일을 선별하여 최소한의 파일 수집
• 파일이름, 확장자, 시간 정보 별로 필요한 파일만을 선택하여 조사
	• 레지스트리는 시스템 사용과 관련해 다양한 정보 제공
	• 디스크/파티션 정보
	• 각종 이벤트들은 유용한 정보를 제공 (이벤트 로그)
		• 사용자 계정 리스트
		• 최근 접근 문서
		• 최근 실행 명령어
		• 사용자 계정 패스워드 검색를 위한 데이터 수집 (LM Hash, NT Hash)
			• 인터넷 사용 기록
			  • 웹 사이트 계정
			  • 검색어
			• 메신저 사용 기록
			  • 대화 상대 및 내용
			  • 받은 파일

활성 시스템 조사 기법 -1

휘발성 데이터 분석

- 수집한 다양한 **휘발성 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

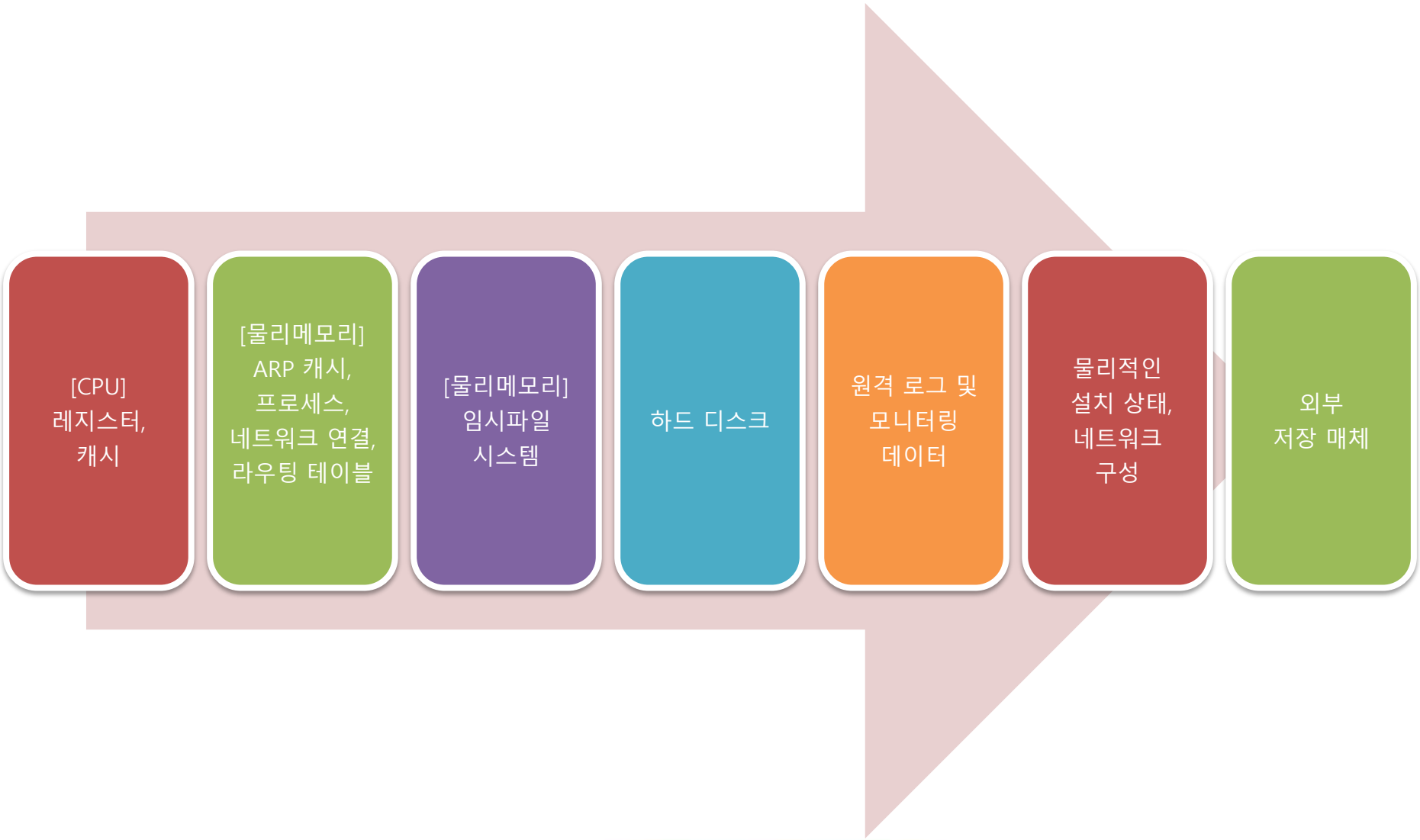
파일시스템 메타데이터

- 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

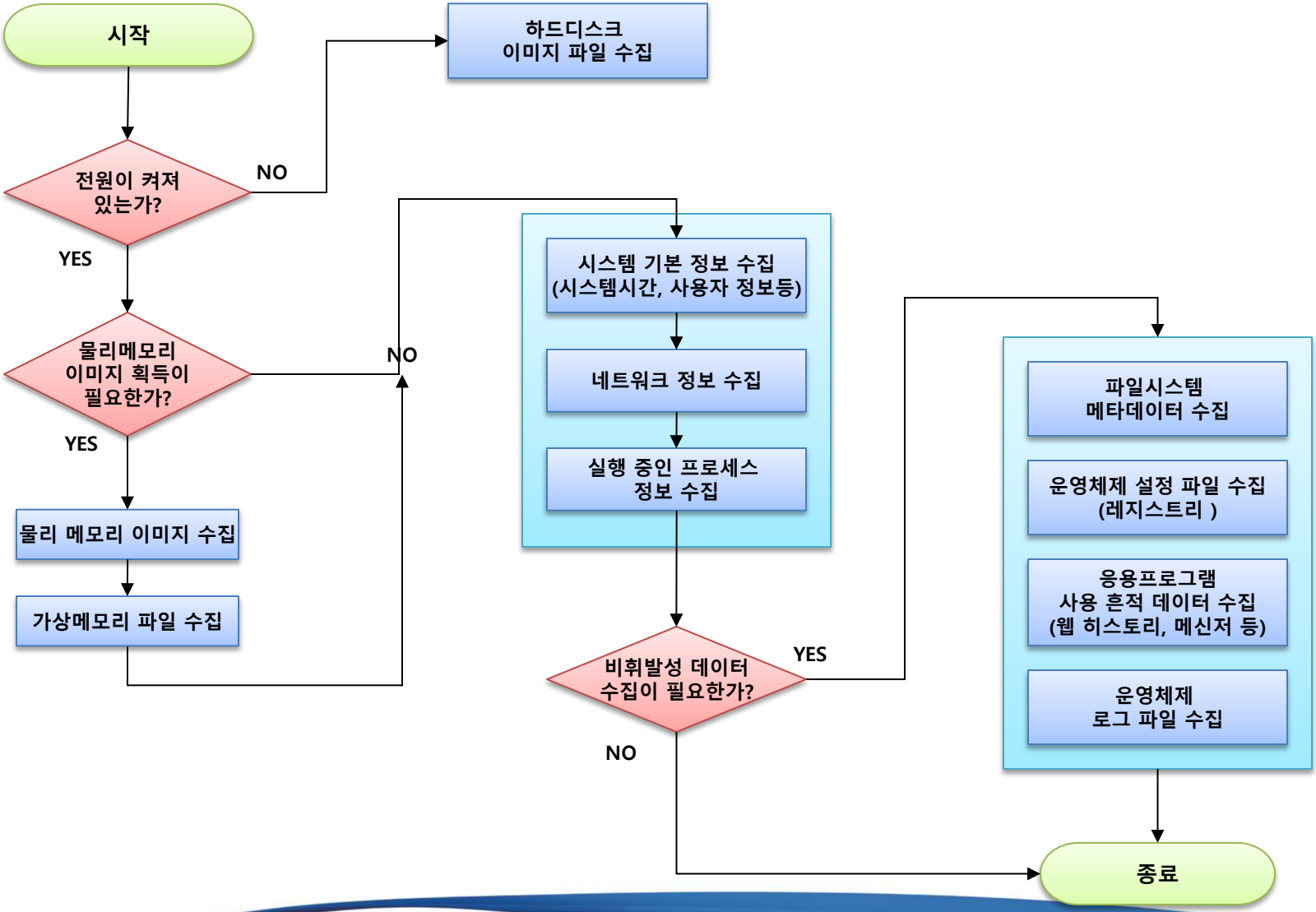
응용 프로그램 분석

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

휘발성 정도에 따른 수집 절차 (RFC 3227)



활성 시스템 조사 절차


시작
전원이 켜져 있는가?
NO
하드디스크 이미지 파일 수집
YES
물리메모리 이미지 획득이 필요한가?
NO
YES
물리 메모리 이미지 수집
가상메모리 파일 수집
시스템 기본 정보 수집 (시스템시간, 사용자 정보등)
네트워크 정보 수집
실행 중인 프로세스 정보 수집
비휘발성 데이터 수집이 필요한가?
YES
NO
파일시스템 메타데이터 수집
운영체제 설정 파일 수집 (레지스트리)
응용프로그램 사용 흔적 데이터 수집 (웹 히스토리, 메신저 등)
운영체제 로그 파일 수집
종료

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

휘발성 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 휘발성 데이터에서 의미 있는 결과를 도출할 수 있는 능력 필요

시스템 기본 정보-시스템 시간

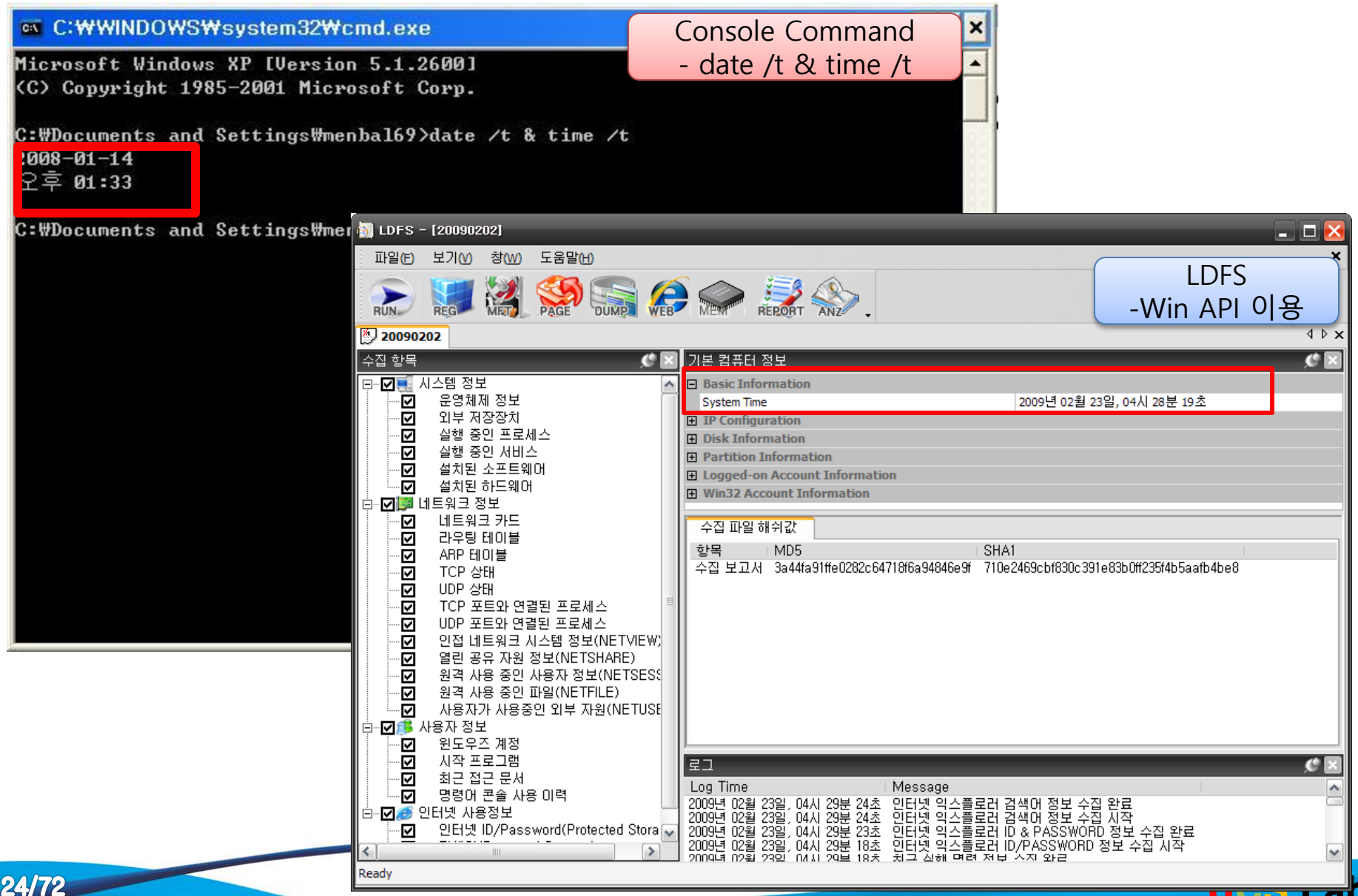
System Time

- 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



시스템 기본 정보– 현재 로그온계정

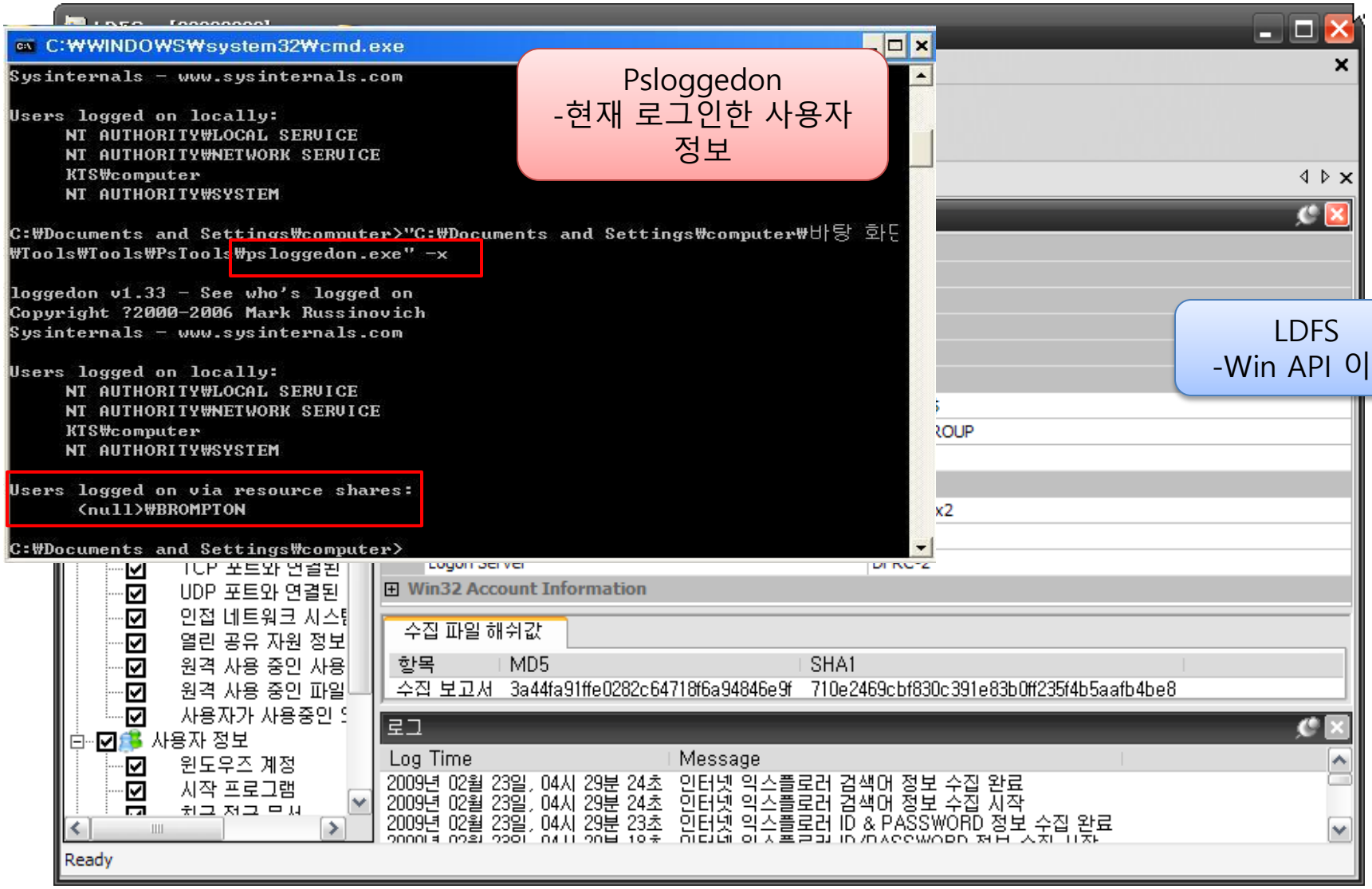
현재 로그온 계정(Logged-on user)

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

수집방법

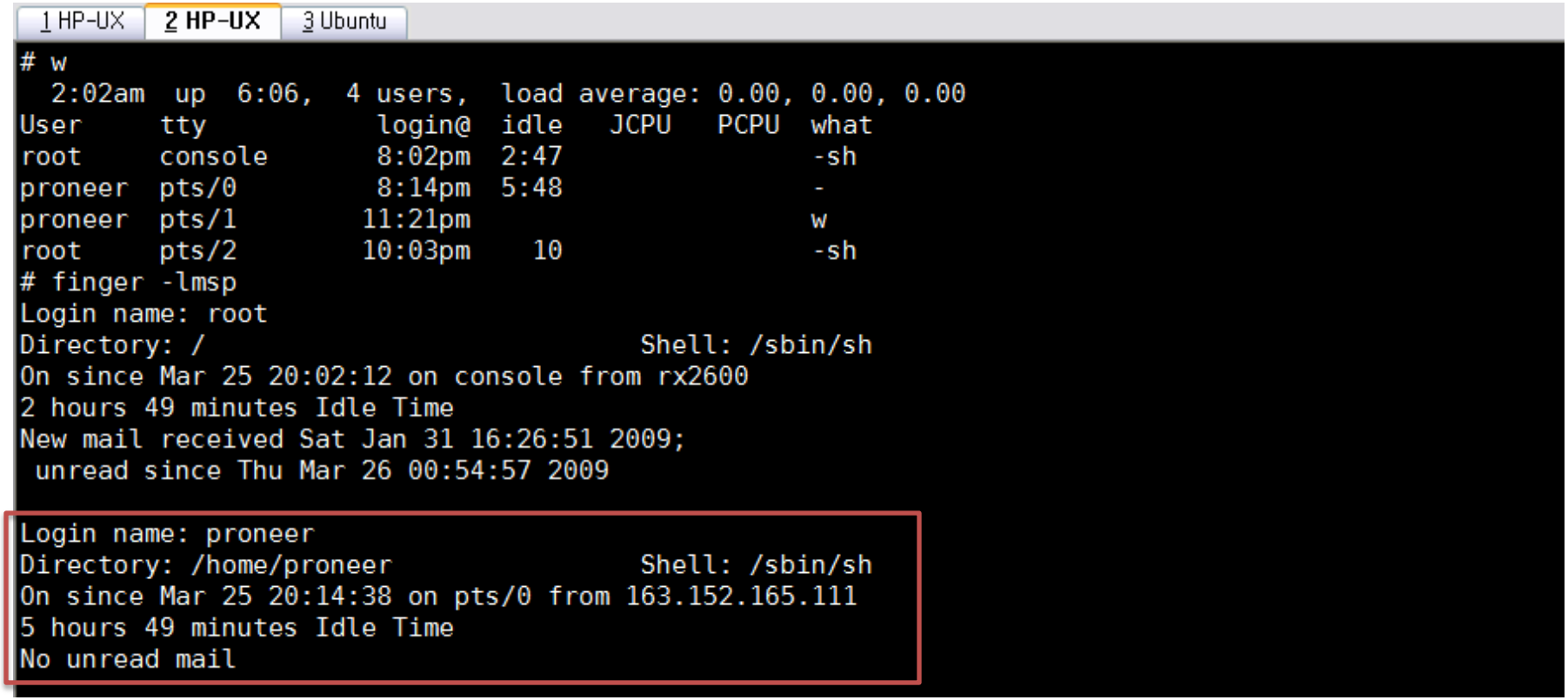
- net users : netbios 명령어
- psloggedon : Sysinternals 사에서 제공하는 공개프로그램
- net sessions : netbios 명령어

현재 로그온계정 (Windows)



현재 로그온계정 (UNIX)

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



시스템 기본 정보– 디스크 정보

디스크 정보

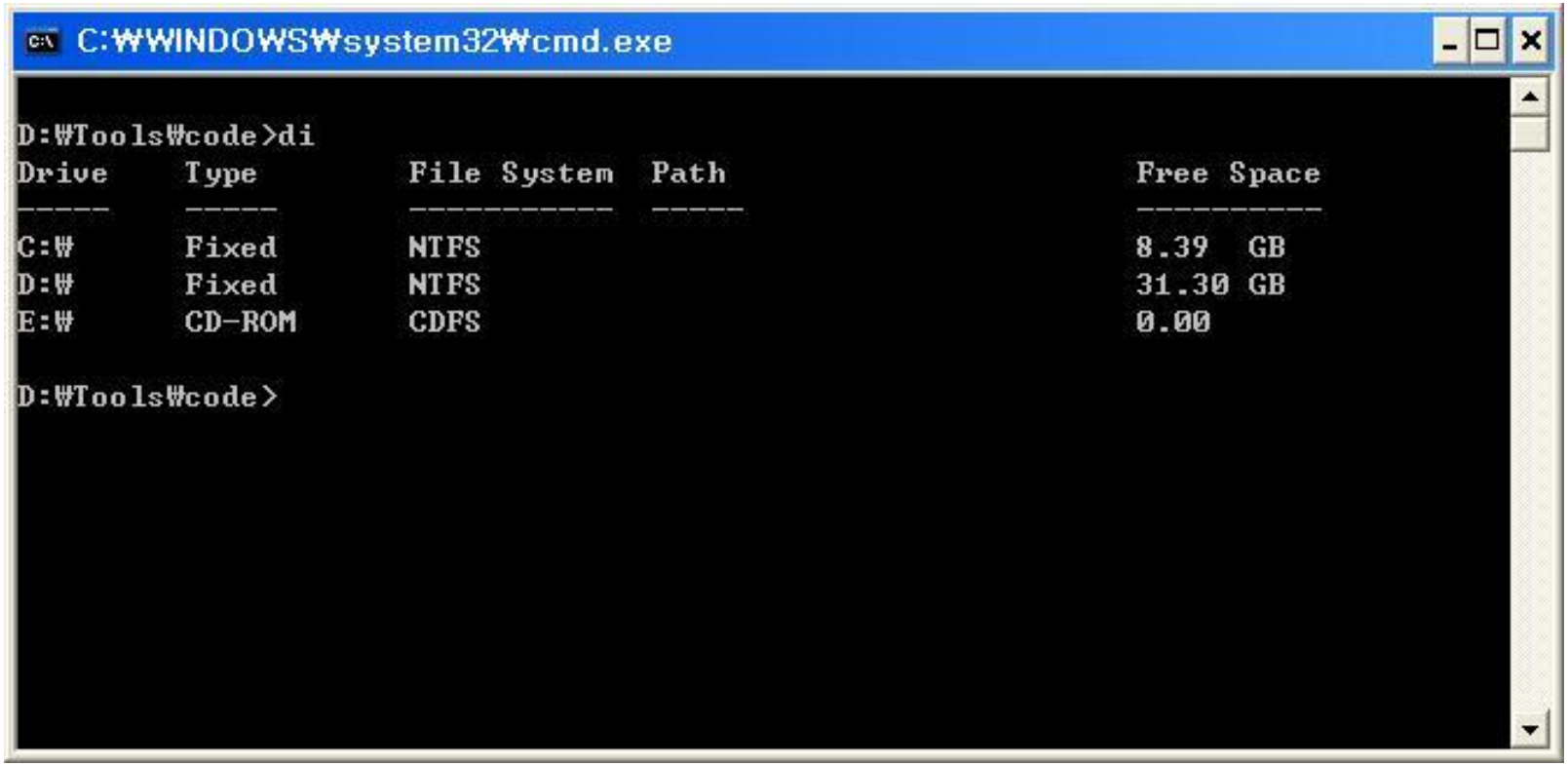
- 수집해야 하는 디스크 목록 확인

수집방법

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

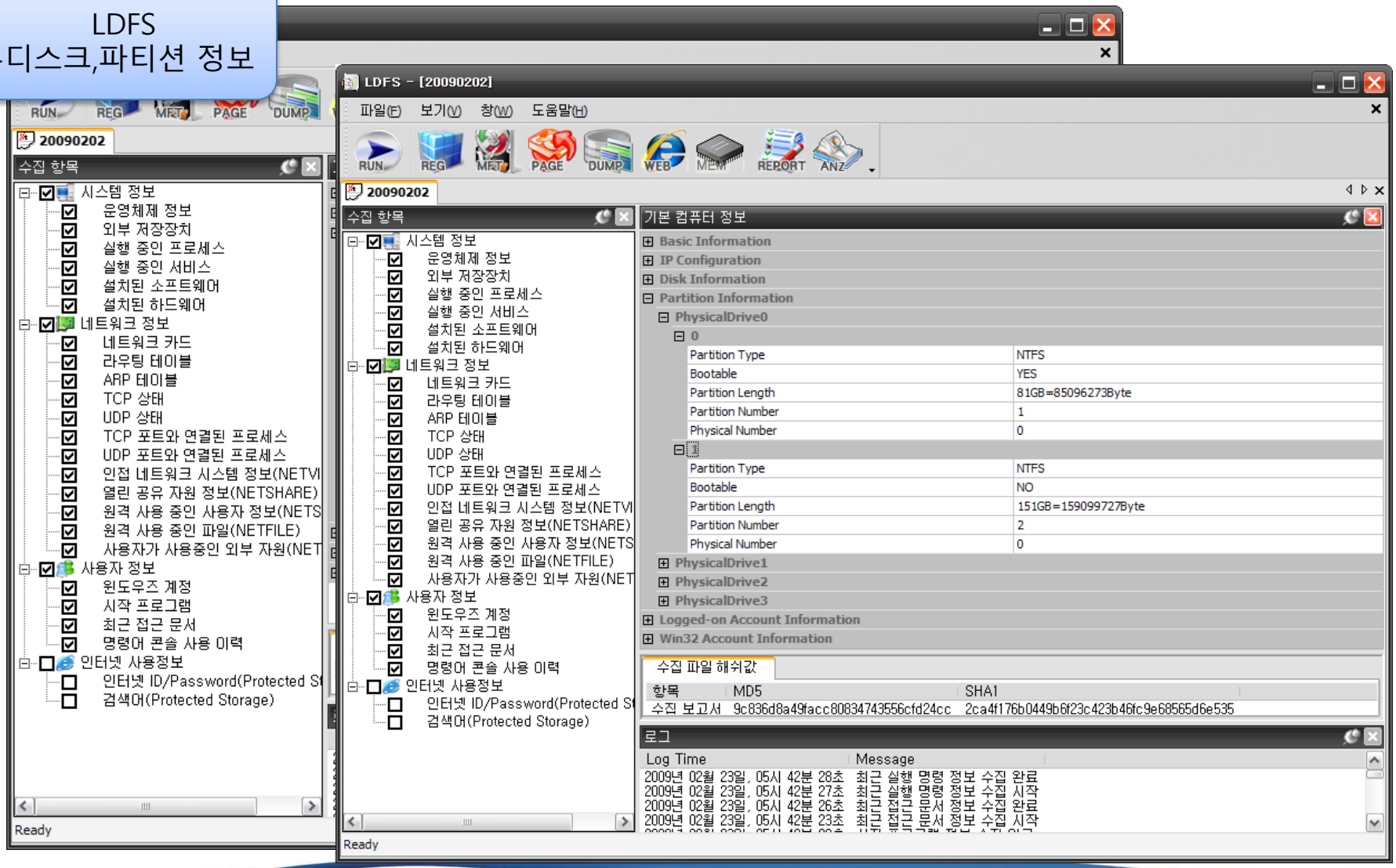
디스크, 파티션 정보(Windows)

- **di (각 Driver의 정보)**



디스크, 파티션 정보(Windows)

LDFS
-디스크,파티션 정보



디스크, 파티션 정보(Unix)

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

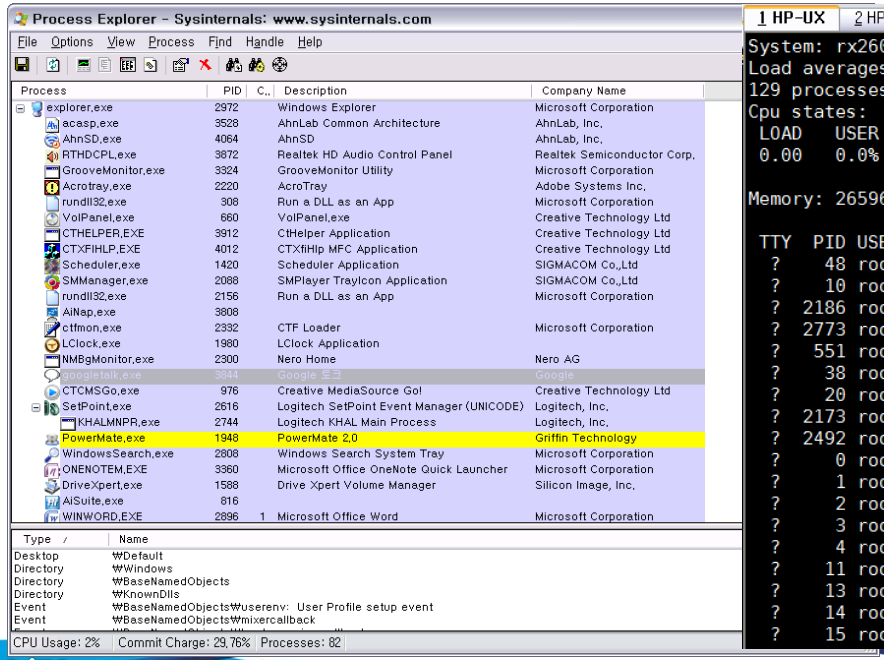
1 HP-UX | 2 HP-UX | 3 Ubuntu

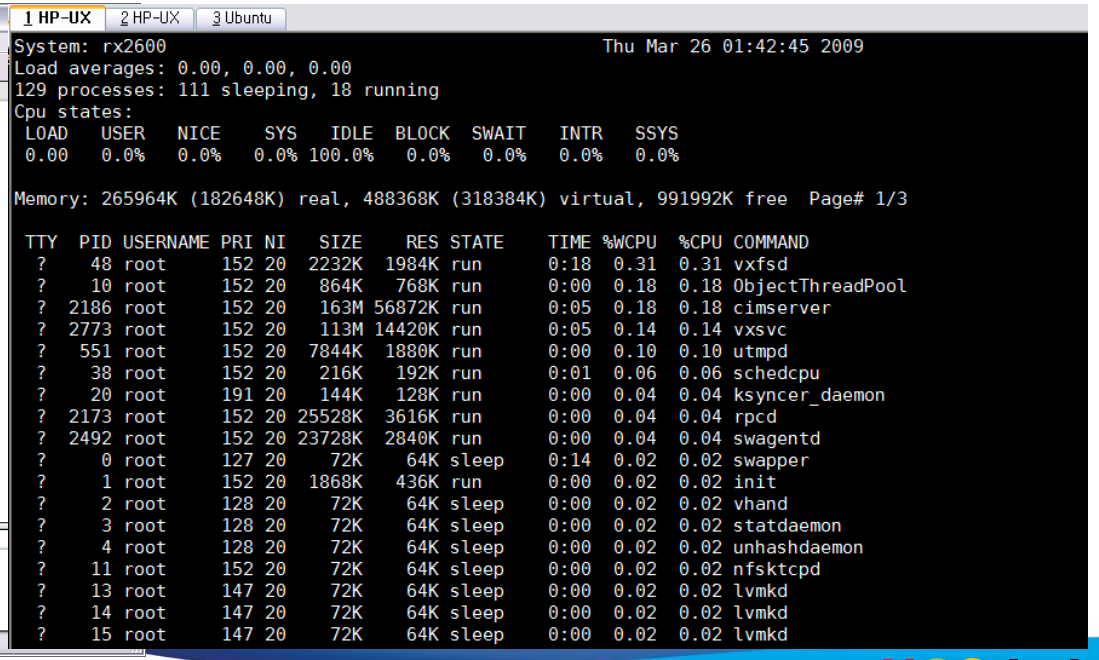
```
# ioscan -fC disk
Class     I  H/W Path        Driver     S/W State   H/W Type     Description
=============================================================================
disk      0  0/0/2/0.0.0.0   sdisk      CLAIMED     DEVICE       TEAC    DV-28E-N
disk      1  0/1/1/0.0.0     sdisk      CLAIMED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

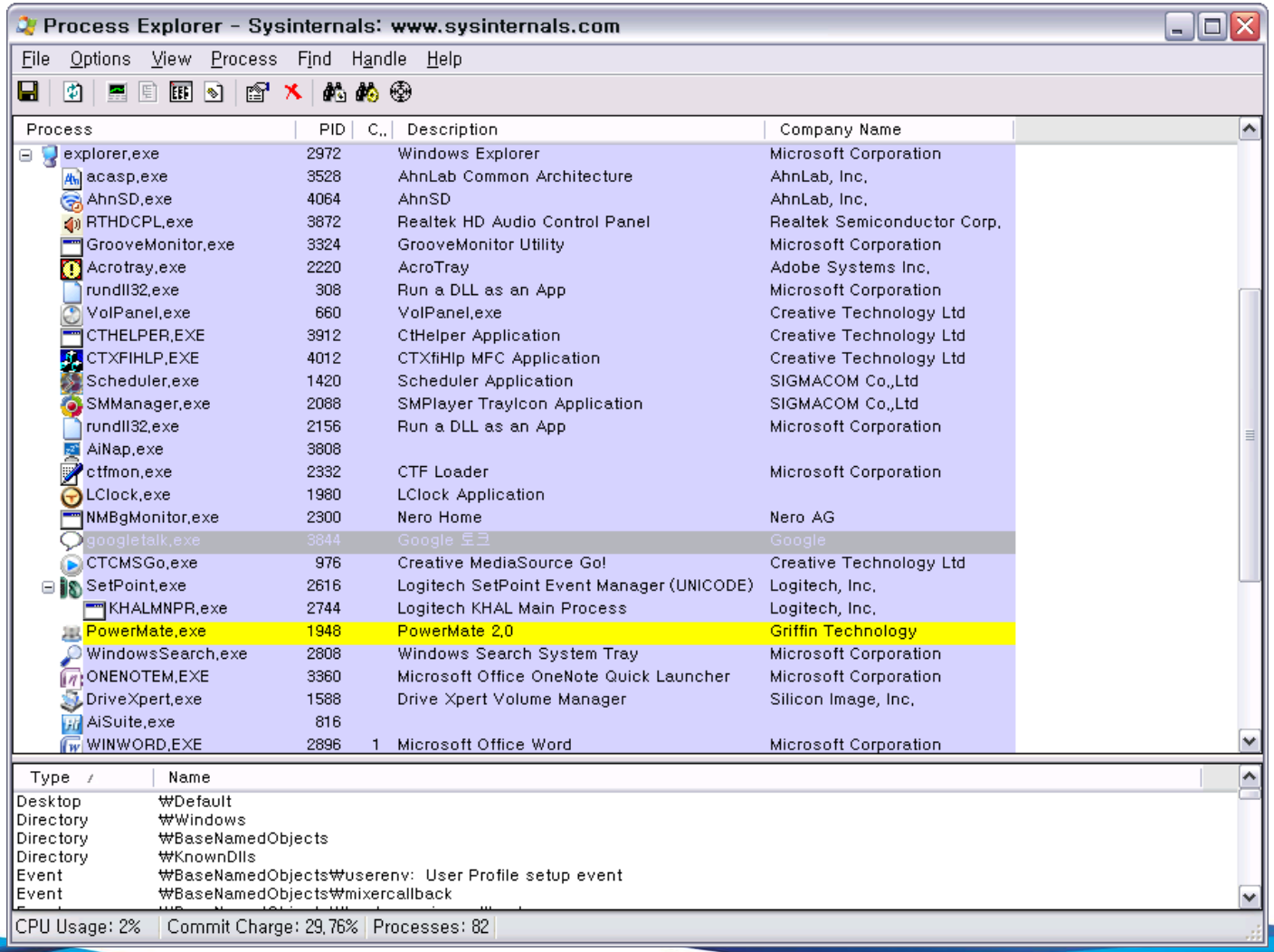
- **목적**: 실행 중인 프로세스 정보 수집 및 분석을 통한 비정상 프로세스 판별 악성코드 탐지
- **방법**:
  - 기존 프로세스 정보들과 비교 분석하여 참조 DLL
  - 실행 경로 등이 이상이 없는지 점검, 또한 각 프로세스의 자식 프로세스의 활동 정보 비교/분석
  - 물리 메모리에서 프로세스 구조체를 추출하여 숨겨진 프로세스 탐지 등
- **도구**: 윈도우 작업 관리자(Windows), Process Explorer(Windows), top(Unix)





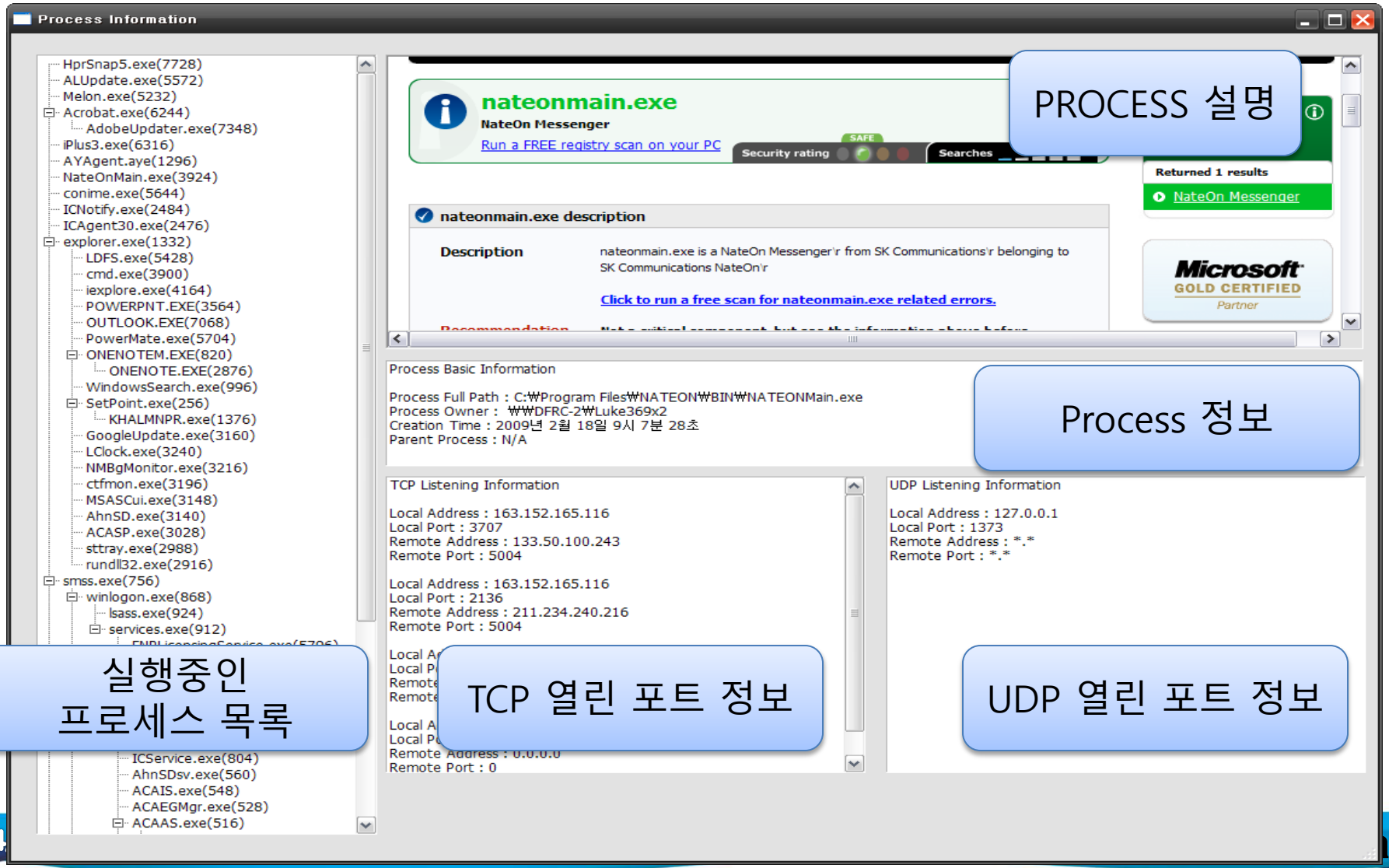
프로세스 정보 –GUI 분석 도구

- **Process Explorer(Active)-Systinternals**



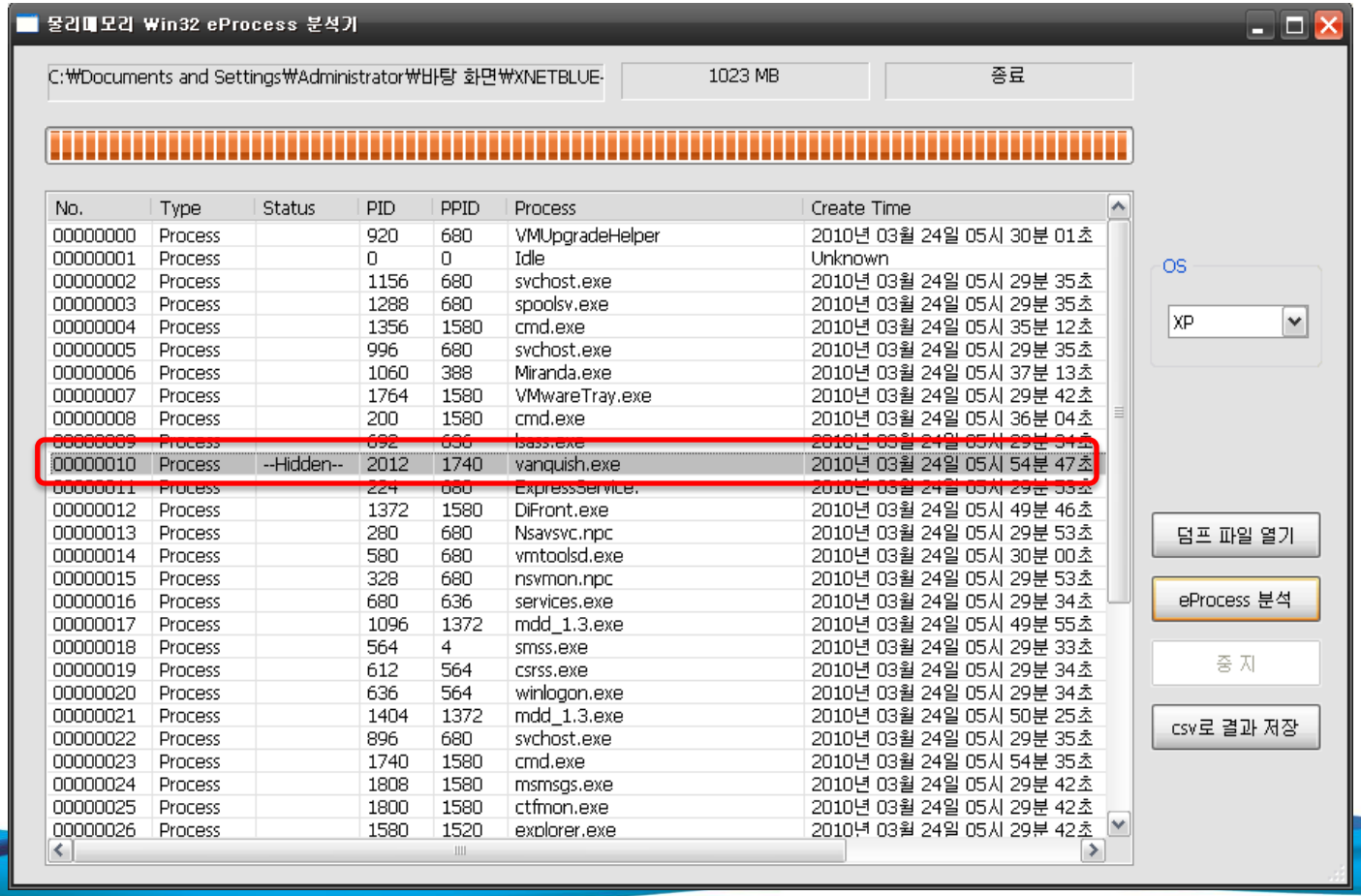
프로세스 정보 – GUI 수집 및 분석 도구

- **LDFS – 실행 중인 프로세스 뷰어(Static)**



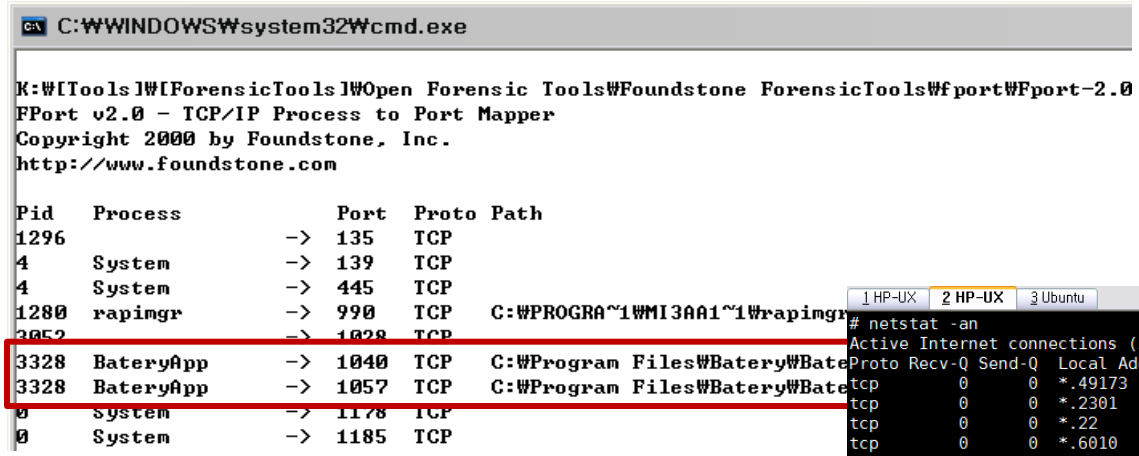
물리메모리에서 프로세스 정보 추출

- 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



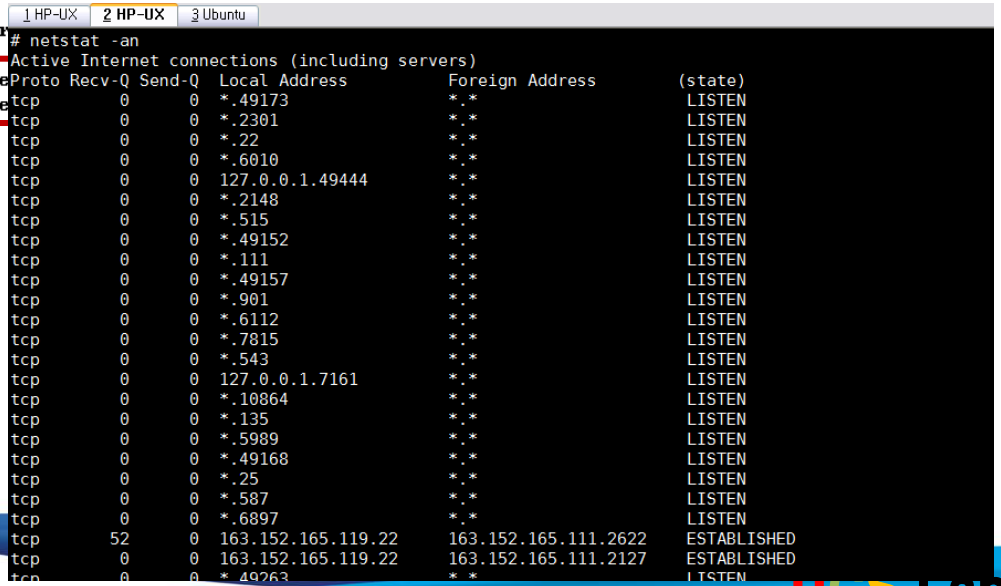
휘발성 데이터 수집 및 분석 –네트워크 정보

- **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



Fport (Windows)

Netstat (Unix)



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

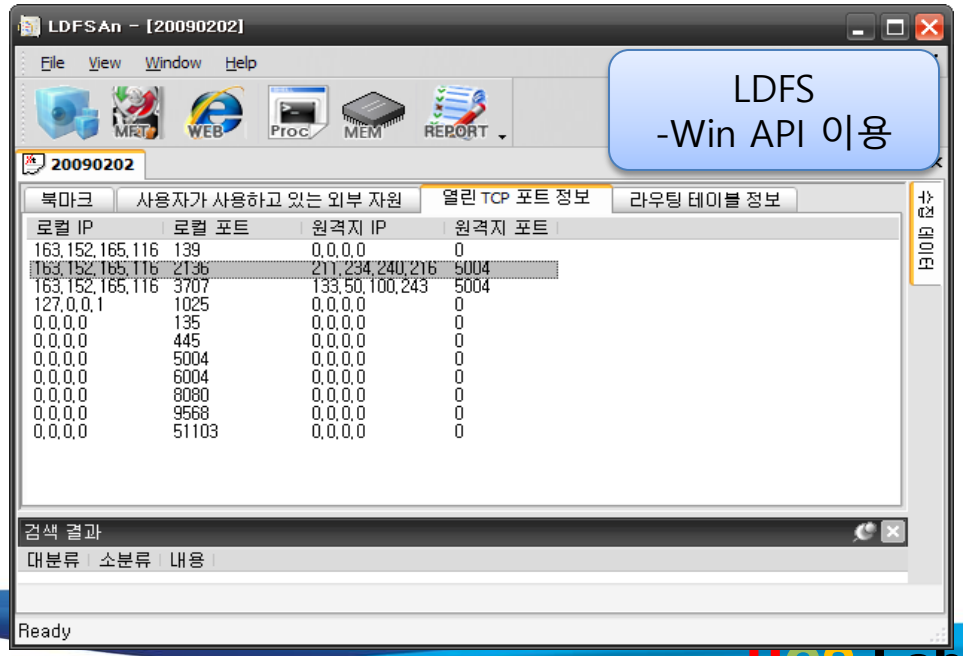
netstat –ano

```
D:₩Tools₩code>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
```

LDFS
-Win API 이용



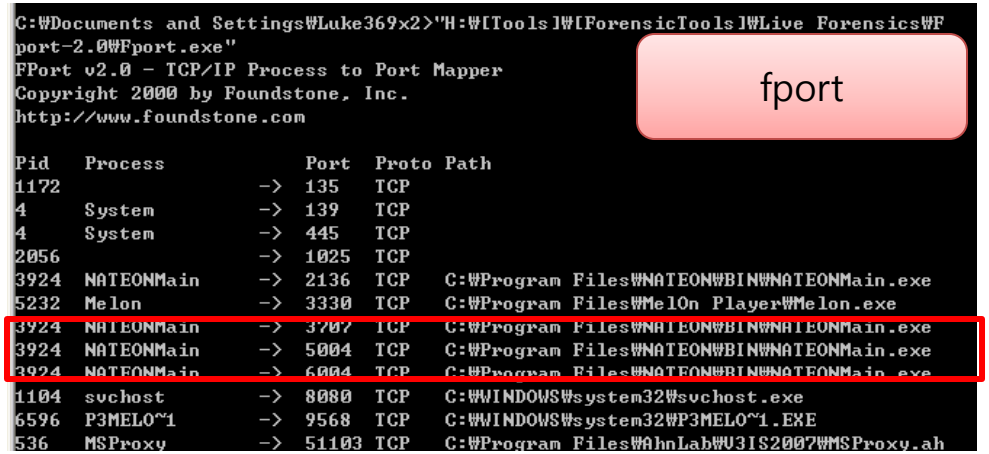
네트워크 정보 –열린 네트워크 포트와 프로세스 정보

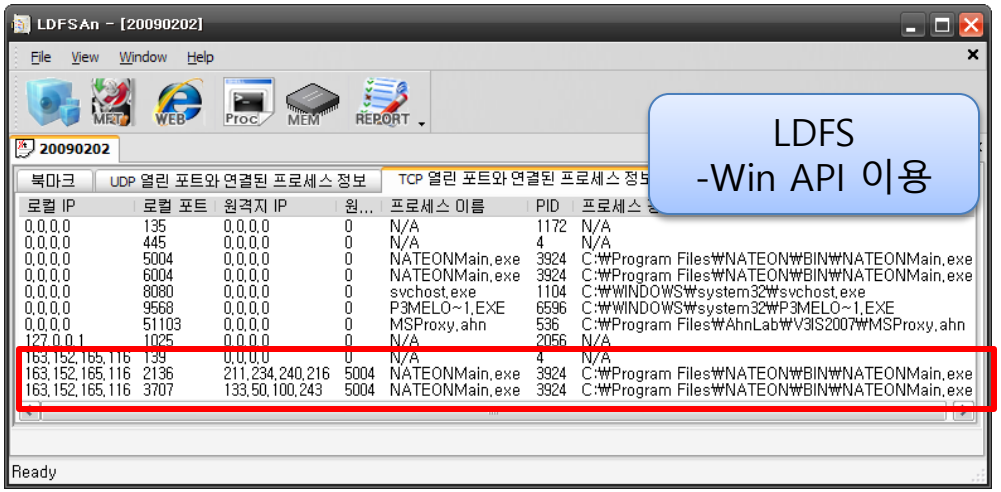
열린 네트워크 포트와 연결된 프로세스 정보

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

수집방법

- Fport
  - Foundstone 사에서 제공하는 공개 버전의 콘솔 명령어





네트워크 정보 – 공유 파일

Open Files

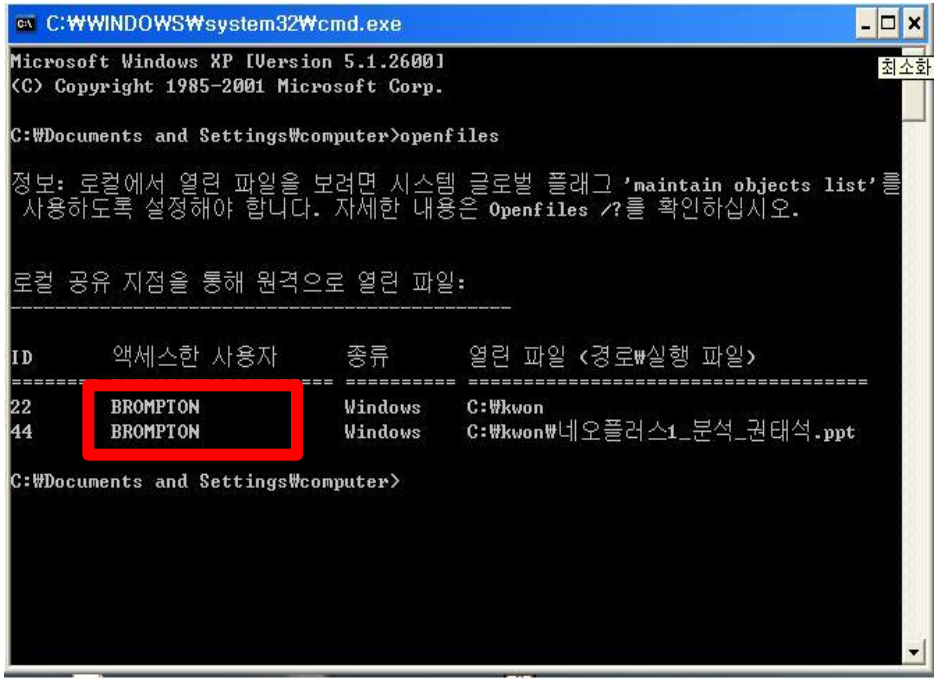
- 외부에서 원격으로 열려있는 파일 획득
- 허가 받지 않은 사용자가 접근해서 자원을 사용하는지 확인 필요

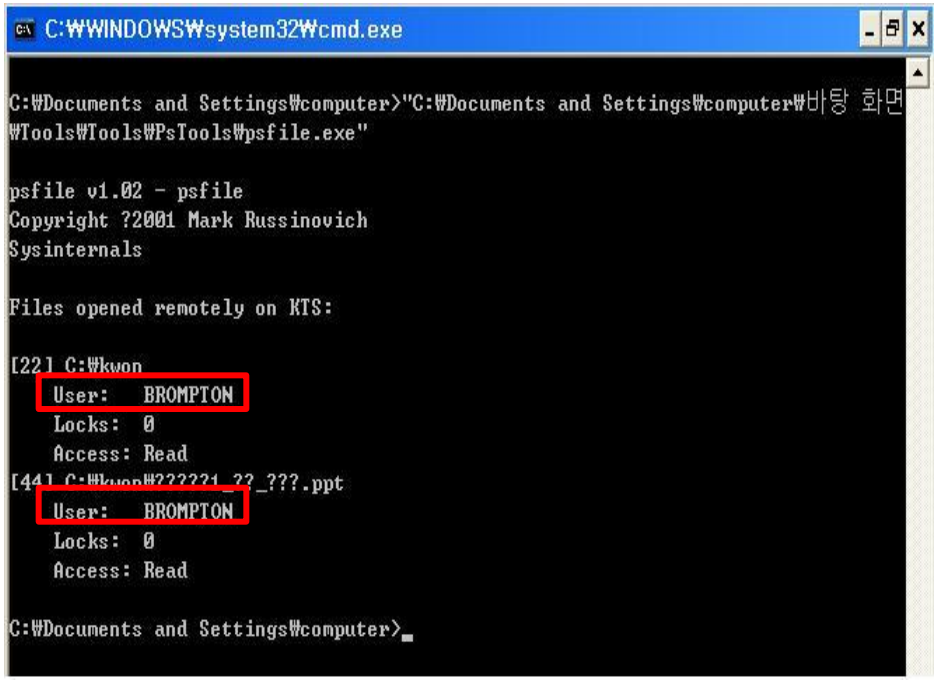
수집방법

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

네트워크 정보 – 공유 파일

- openfiles
  - 열린 파일 조사
- psfile
  - 원격에서 접근한 파일 정보 획득





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 **API**가 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

[조사 대상 시스템]

[조사 대상 시스템]
하드디스크 분해

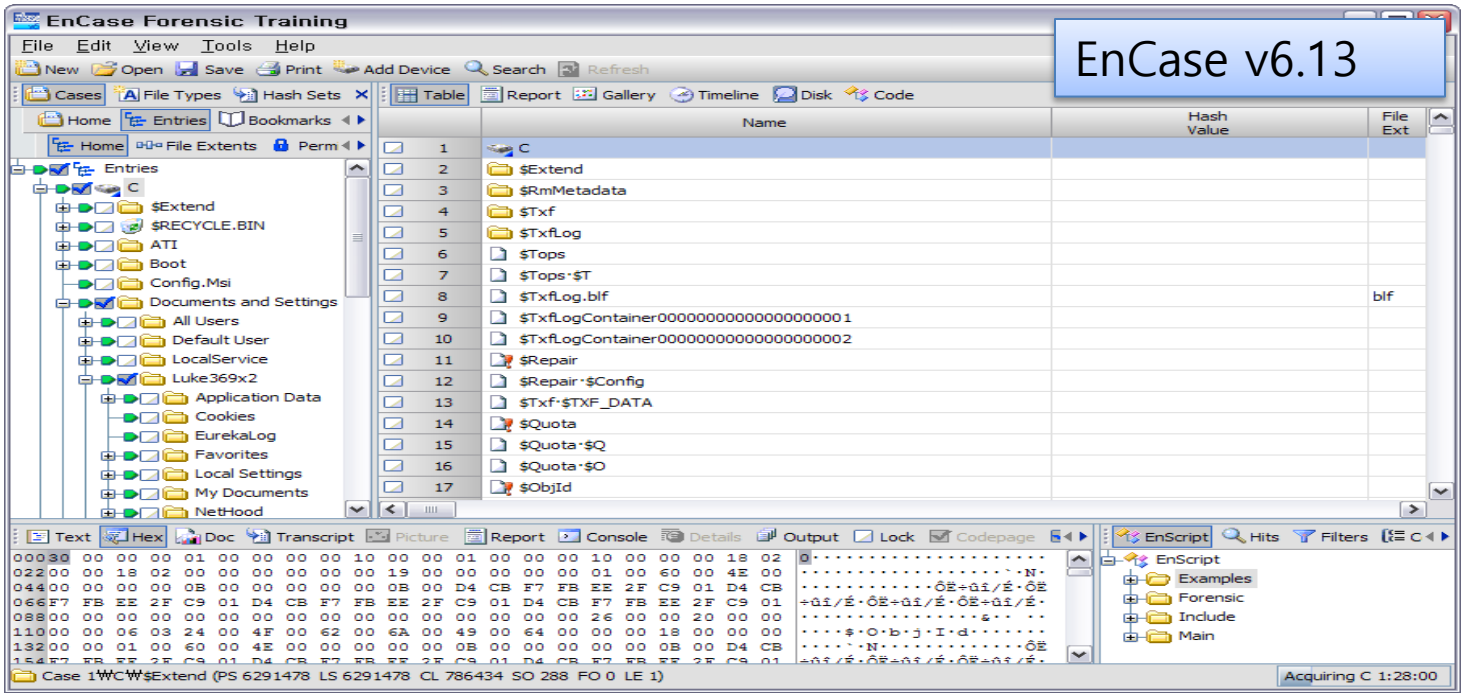
[수집 대상 디스크]

원본 디스크에 대하여
사본 디스크를 복제
(사본 2개까지 생성)

[이미징 장치]

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 OS등의 플랫폼과 RAID 방식 지원

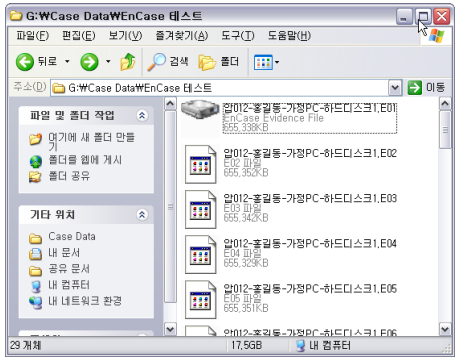


디스크 이미징 S/W를 이용한 사본 생성 절차

[조사 대상 시스템]

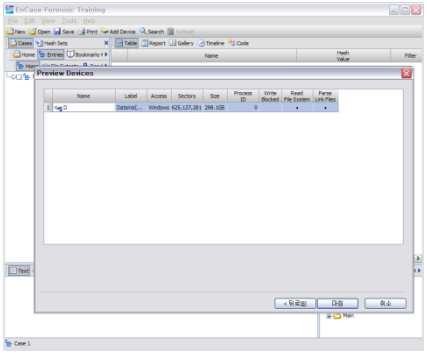
분해

[이미지 파일]



획득

[디스크 이미징 도구]



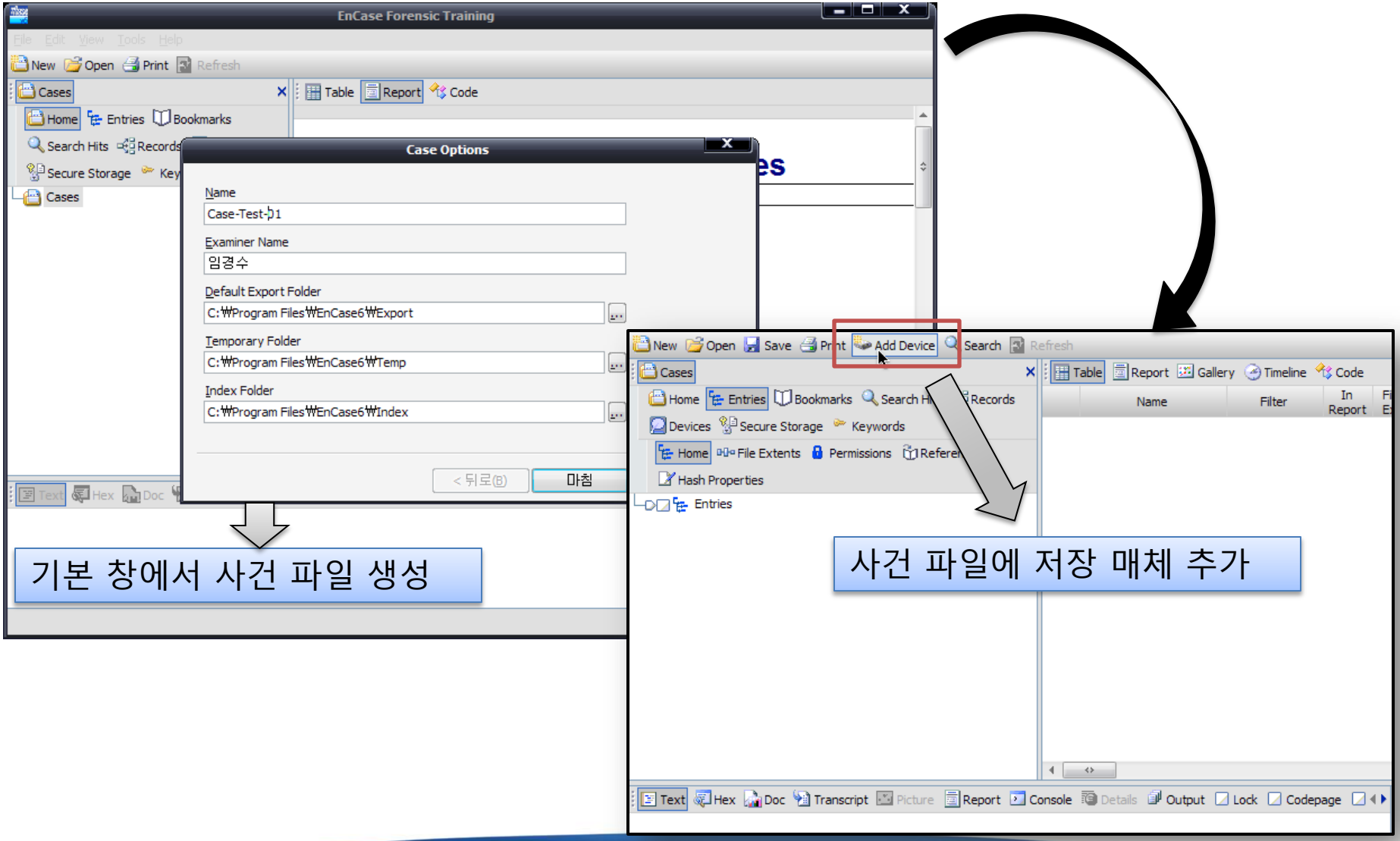
수집

[수집 대상 디스크]
쓰기 방지 장치에 연결

[쓰기방지 장치]
분석 시스템과 쓰기 방지 장치 연결

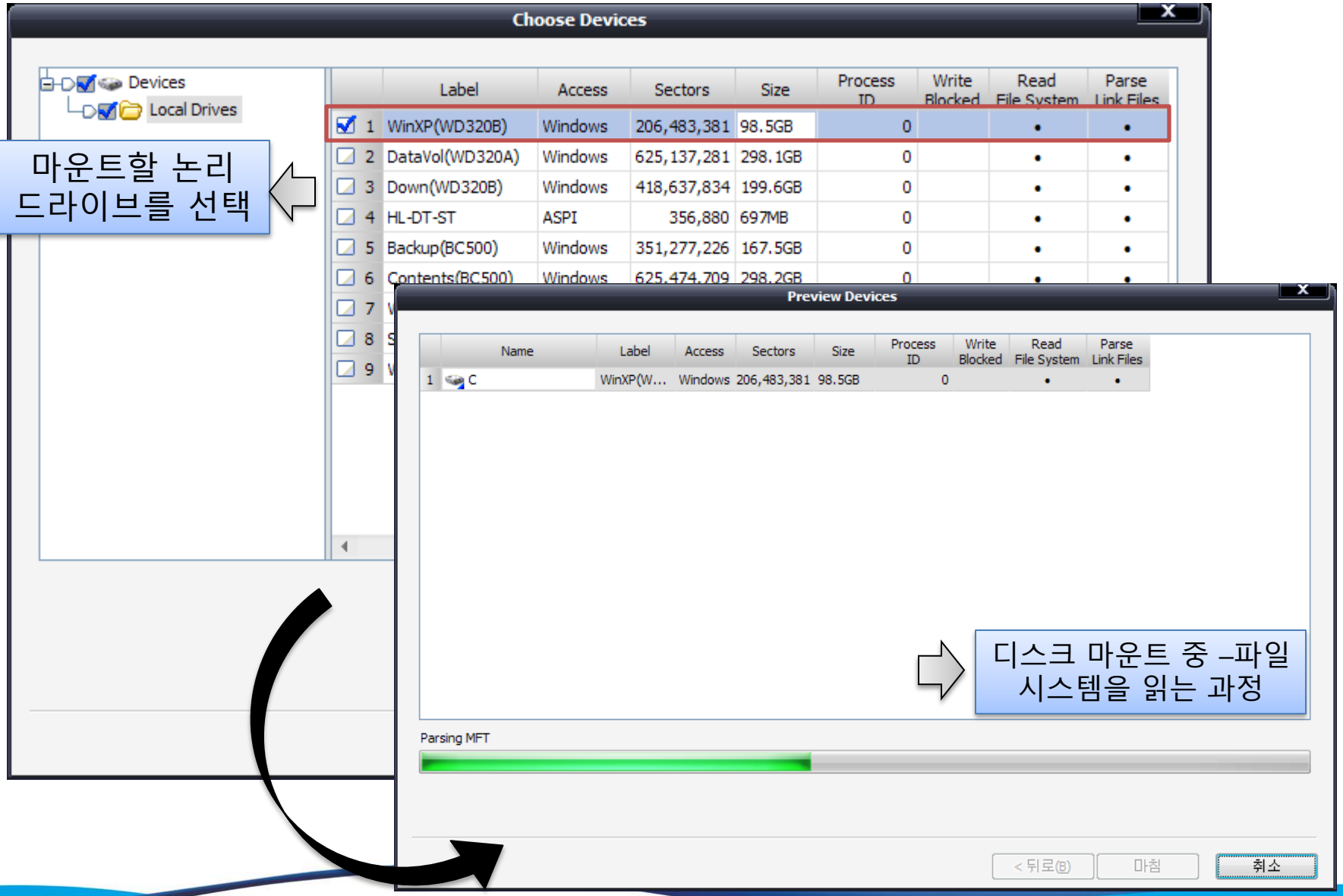
[분석 시스템]

EnCase를 이용한 디스크 이미징



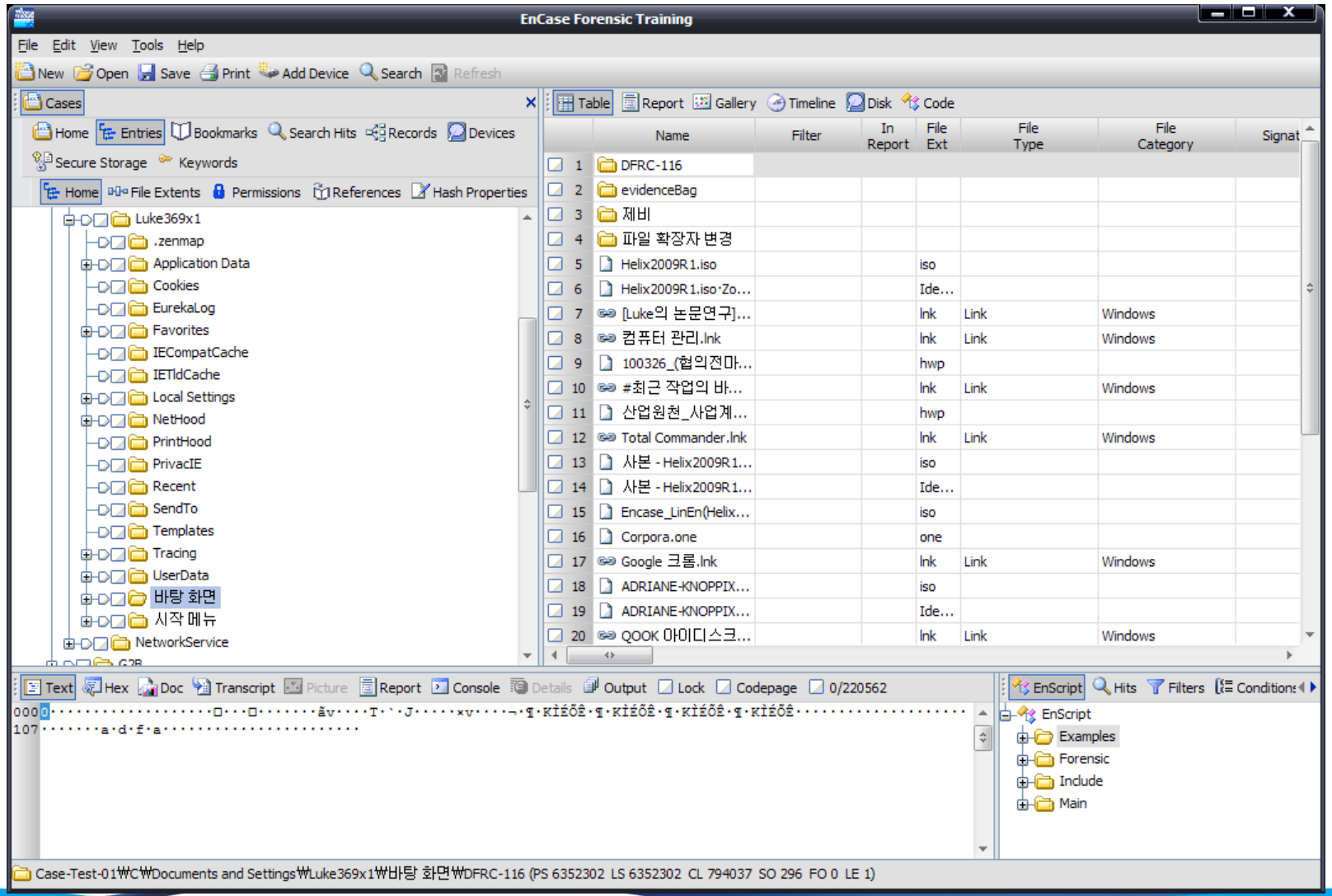
UCS Lab

EnCase를 이용한 디스크 이미징



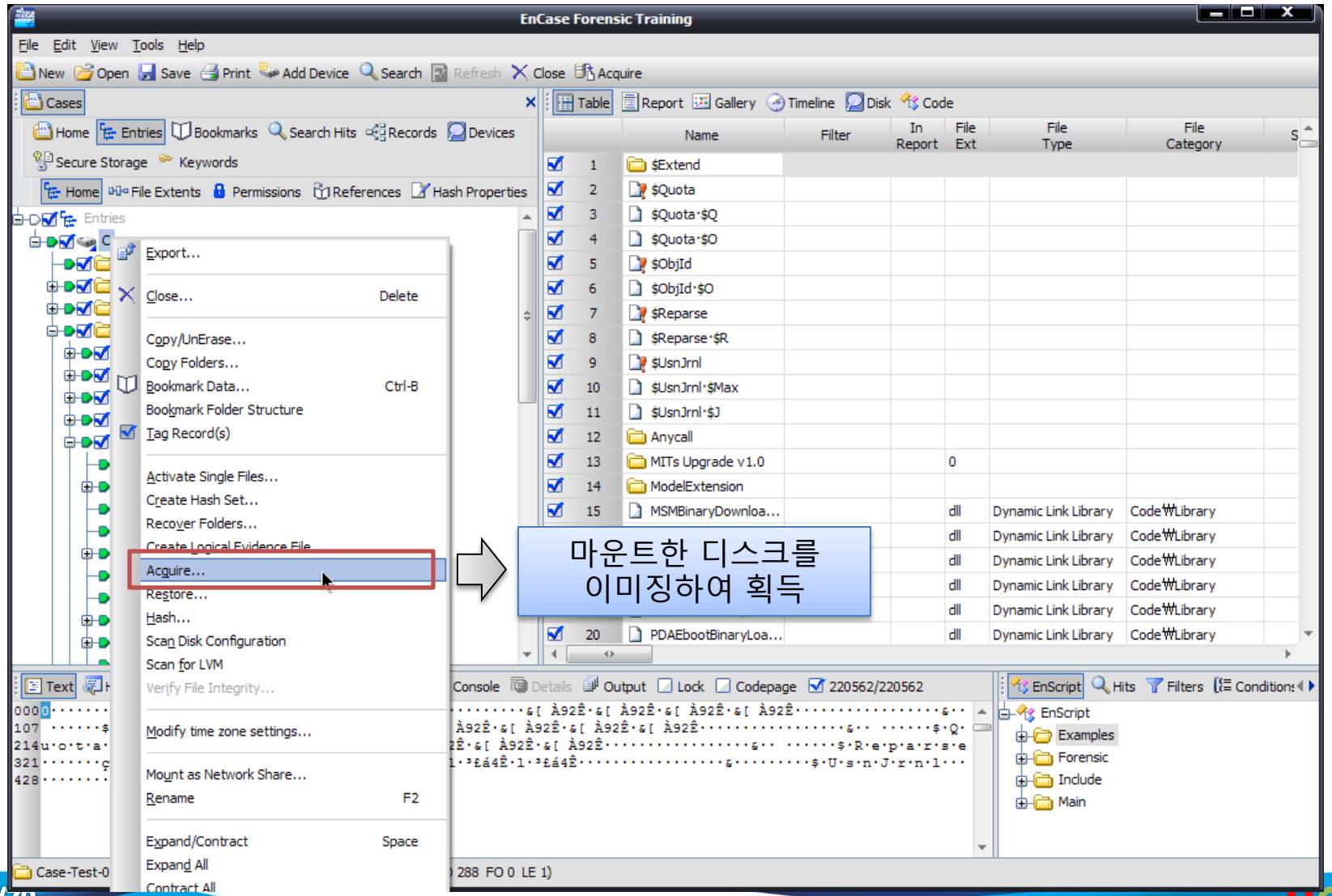
EnCase를 이용한 디스크 이미징

- 윈도우 운영체제가 설치된 **C** 드라이브를 마운트한 상태

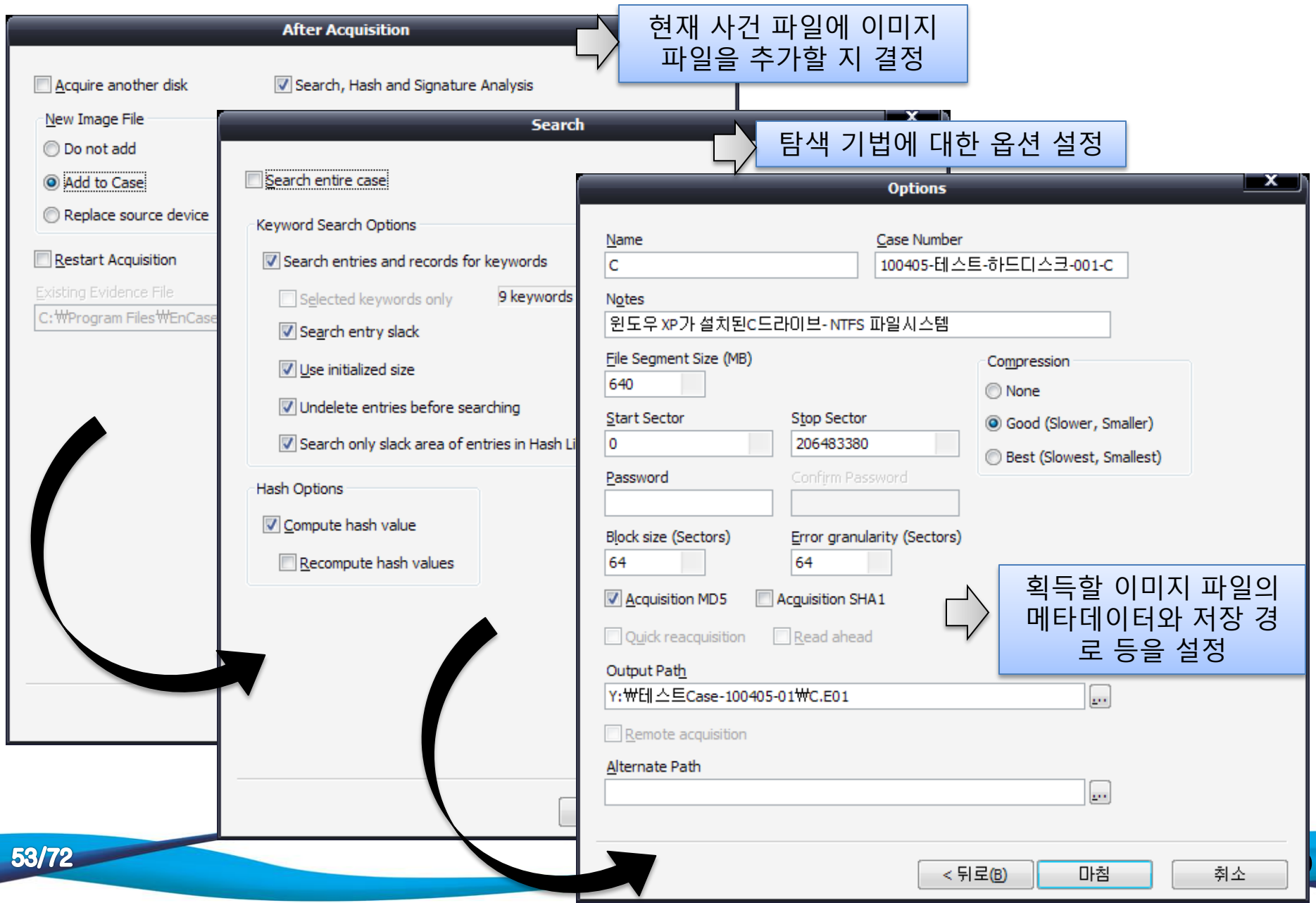


EnCase를 이용한 디스크 이미징

- 윈도우 운영체제가 설치된 **C** 드라이브를 마운트한 상태

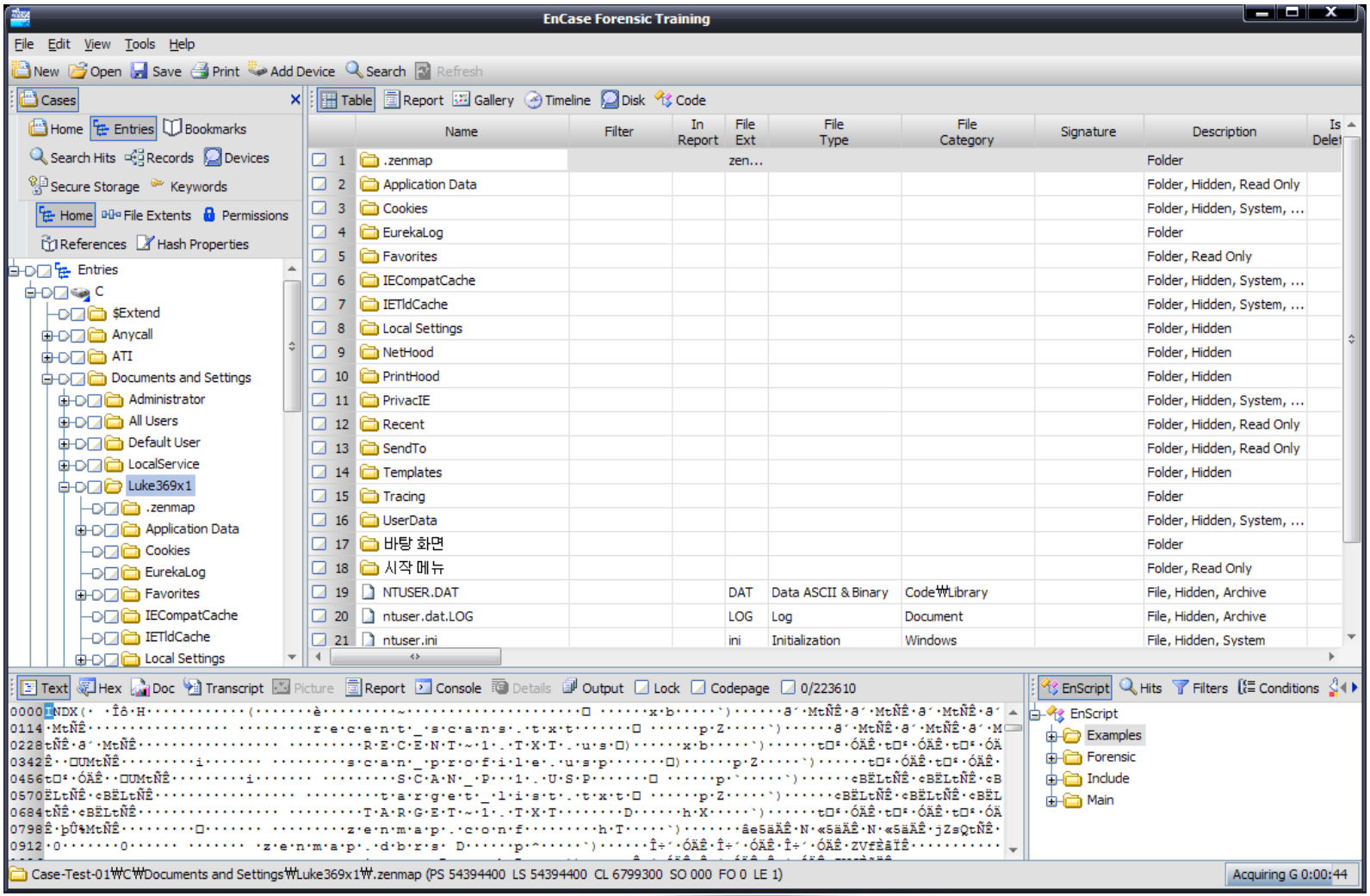


EnCase를 이용한 디스크 이미징



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

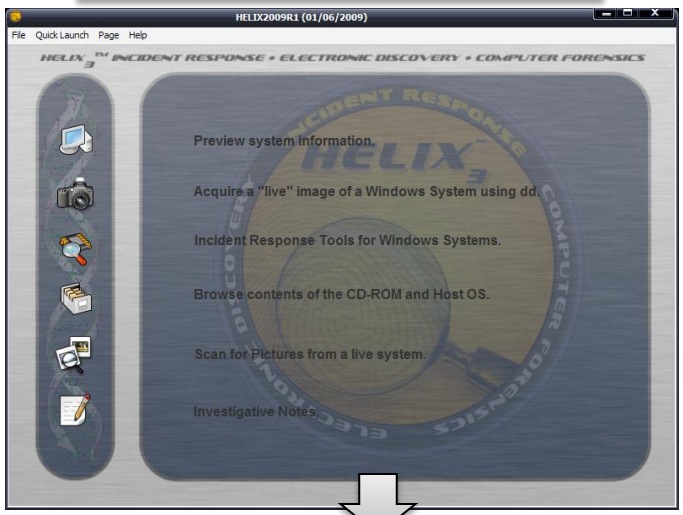
Live-Analysis CD (ex. Helix)

- 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

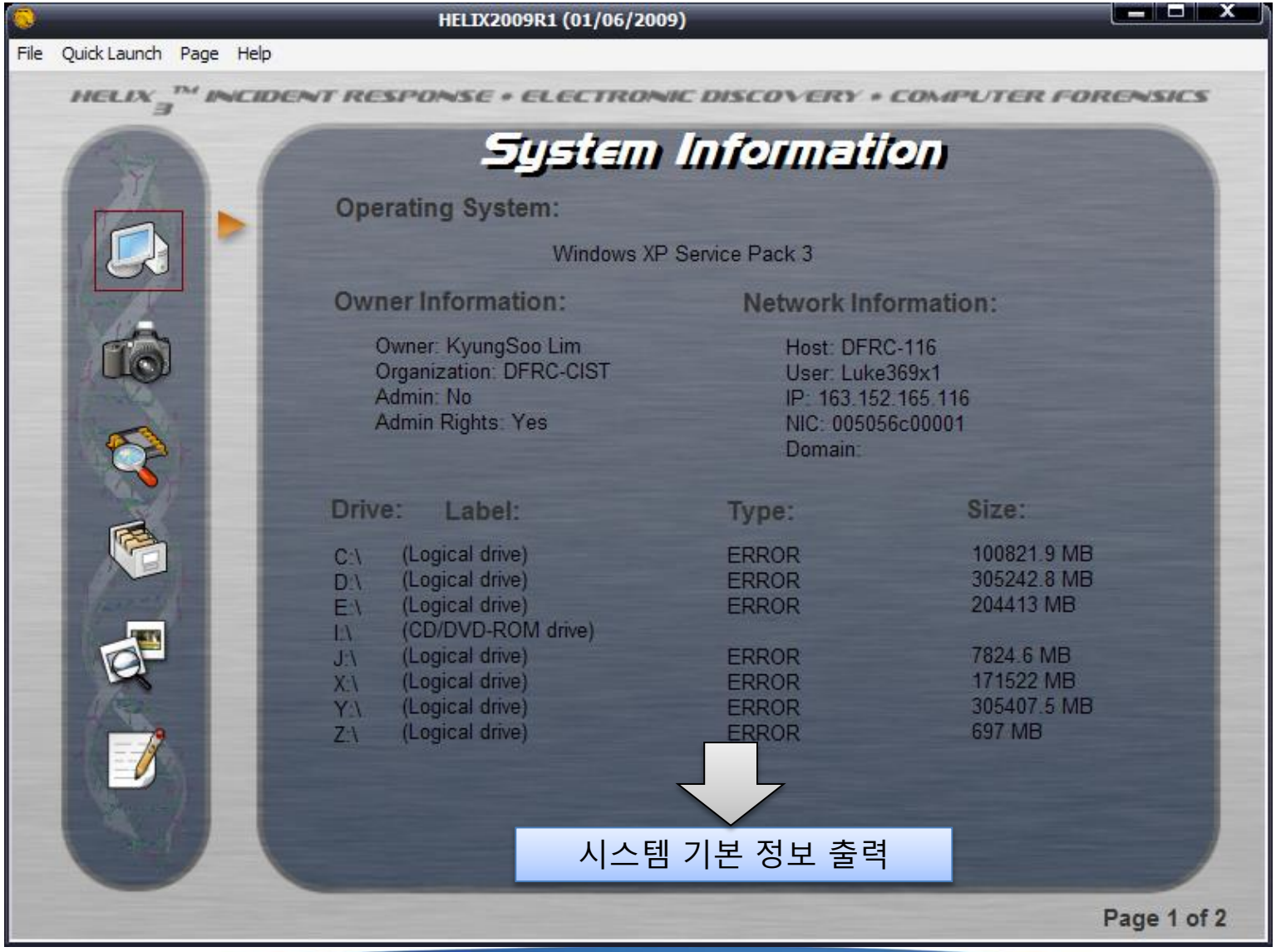
- **Helix 3 소개**
  - 라이브 포렌식을 위한 Bootable 도구
  - 우분투 기반의 포렌식 분석용 Bootable 도구
- **3개의 Helix 버전**
  - Helix 3 (Live Response)
    - 휘발성 데이터 수집 및 디스크 이미징
    - 사건 발생 시, 즉각적인 조사 대응을 위한 도구
  - Helix 3 Pro
    - 기본 버전에 파일 카빙, 모바일 데이터 수집 도구 등을 추가
  - Helix 3 Enterprise
    - E-Discovery 중점의 침해사고 대응
- **Helix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

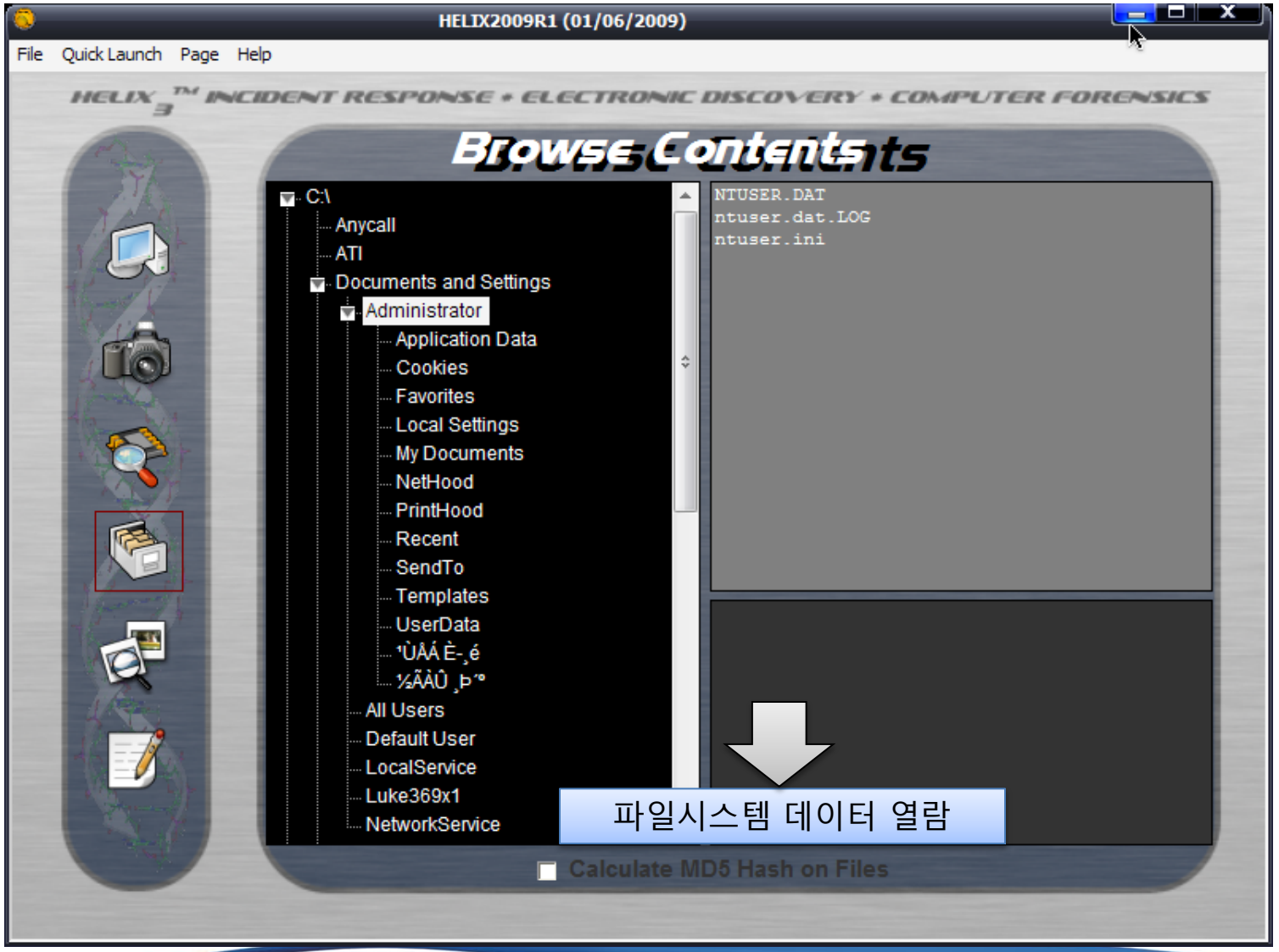
Helix 3 실행 화면


HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
HELIX 3 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


HELIX2009R1 (01/06/2009)
File
Quick Launch
Page
Help
HELIX 3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Incident Response
Windows Forensic Toolchest (WFT)
First Responder Utility (FRU)
Incident Response Collection Report (IRCR2)
Agile Risk Management's Nigilant32
Start a NetCat Listener
활성 시스템 수집
Page 1 of 3

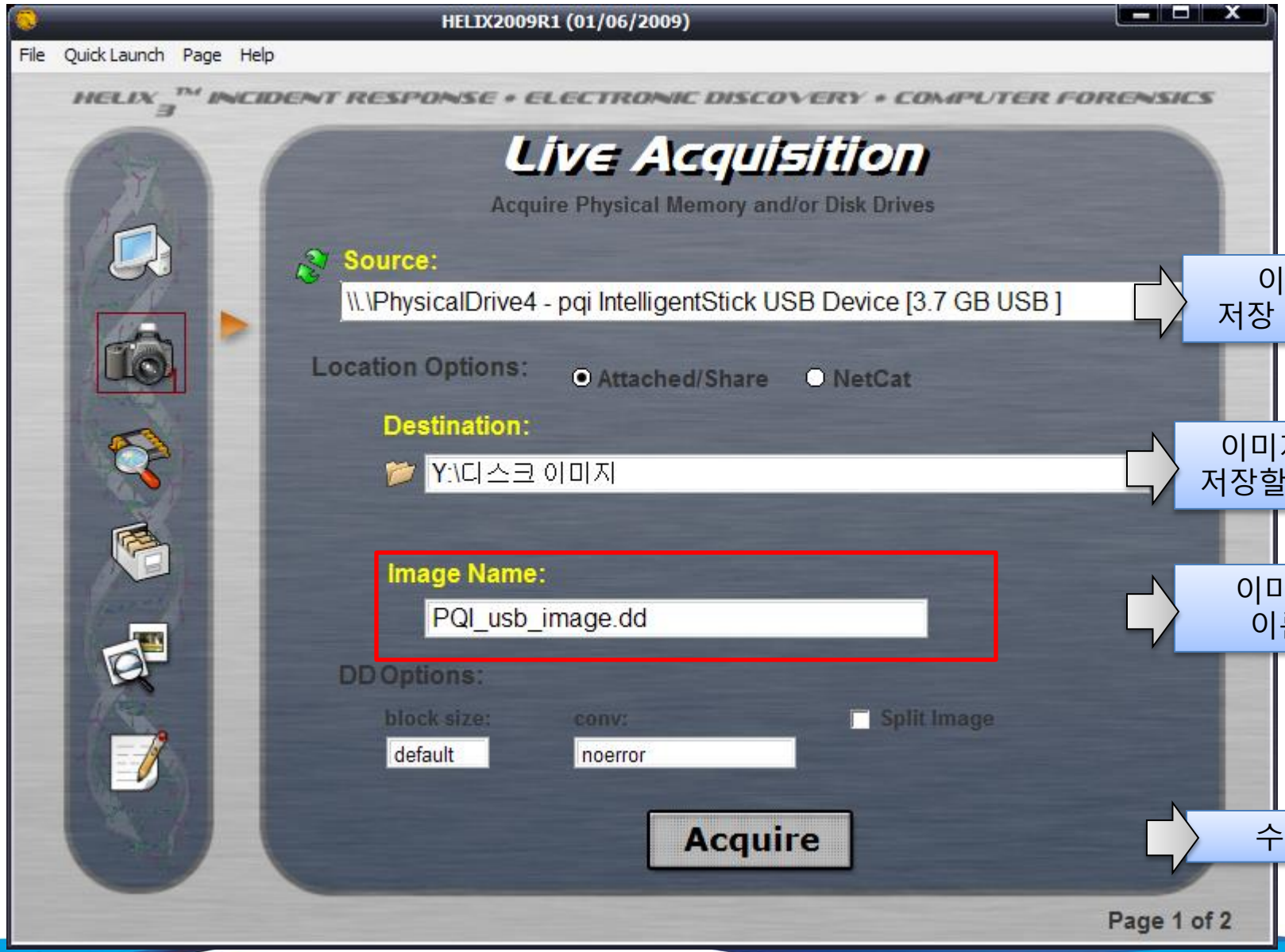
Helix 3 실행 화면


HELIX2009R1 (01/06/2009)
File
Quick Launch
Page
Help
HELIX 3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Browse Contents
C:\
Anycall
ATI
Documents and Settings
Administrator
Application Data
Cookies
Favorites
Local Settings
My Documents
NetHood
PrintHood
Recent
SendTo
Templates
UserData
All Users
Default User
LocalService
Luke369x1
NetworkService
NTUSER.DAT
ntuser.dat.LOG
ntuser.ini
파일시스템 데이터 열람
Calculate MD5 Hash on Files

Helix 3 실행 화면


HELIX2009R1 (01/06/2009)
File
Quick Launch
Page
Help
HELIX 3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Scan For Pictures
310.jpg
311.jpg
312.jpg
313.jpg
314.jpg
315.jpg
316.jpg
317.jpg
318.jpg
319.jpg
320.jpg
321.jpg
323.jpg
324.jpg
사진 데이터 열람
Load Folder
Clear All
Enlarge
Decrease

Helix 3를 이용한 디스크 이미징



이미징할 저장 매체 선택

이미지 파일을 저장할 매체 선택

이미지 파일 이름 설정

수집 실행

Helix 3를 이용한 디스크 이미징

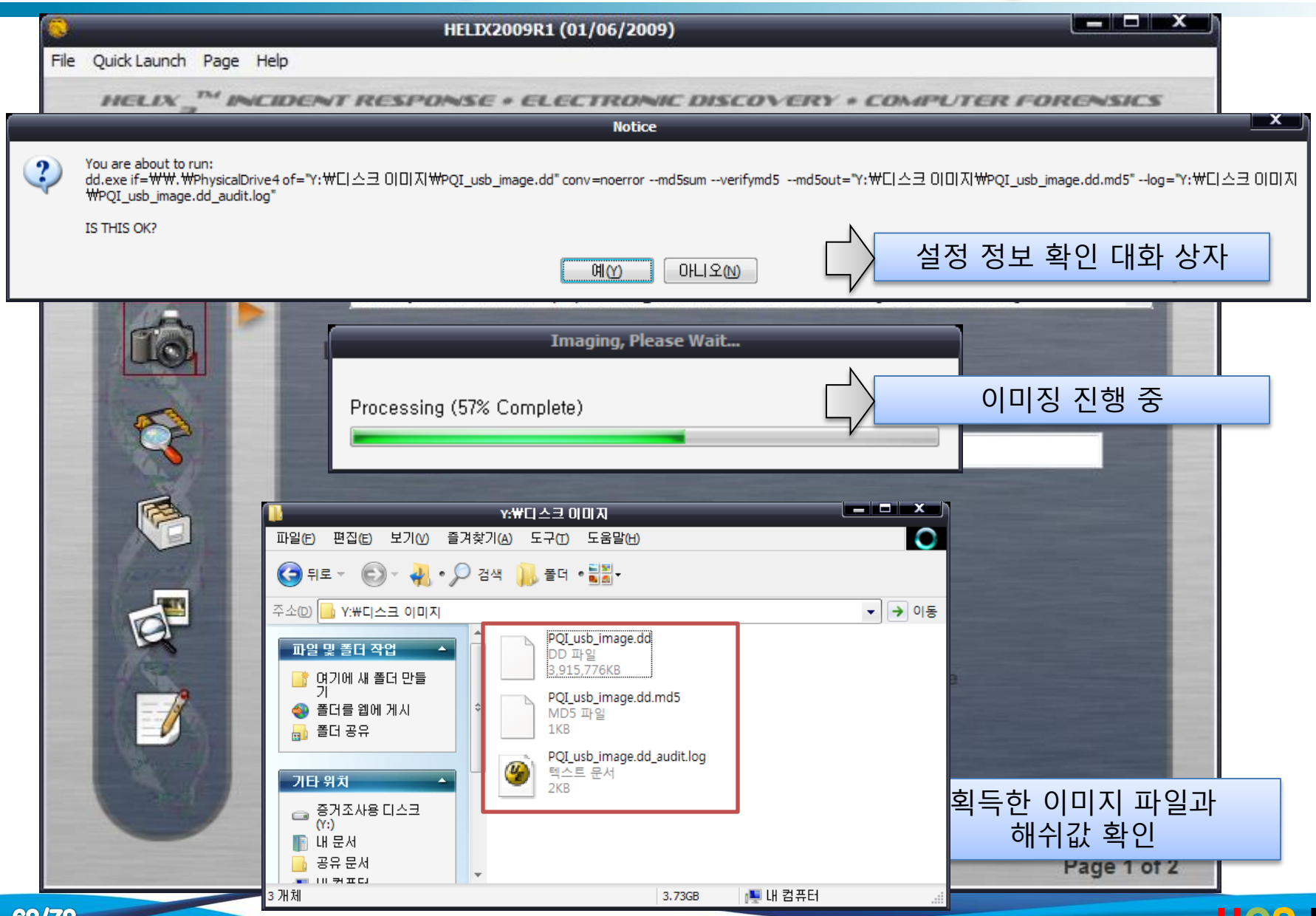


Image Mount Pro를 활용한 이미지 파일 열람

- **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

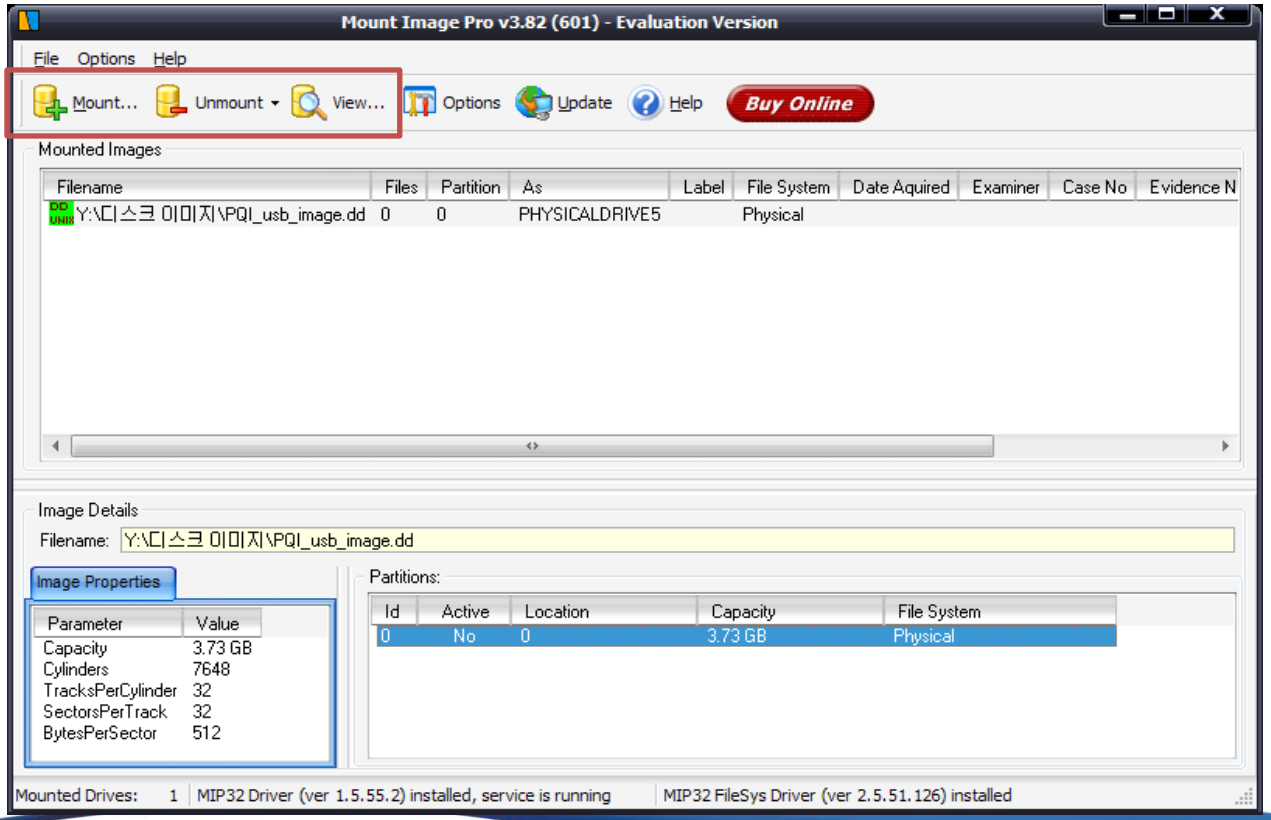


Image Mount Pro를 활용한 이미지 파일 열람

- **Mount** 실행 → 이미지 파일 선택 → 마운트 옵션 설정

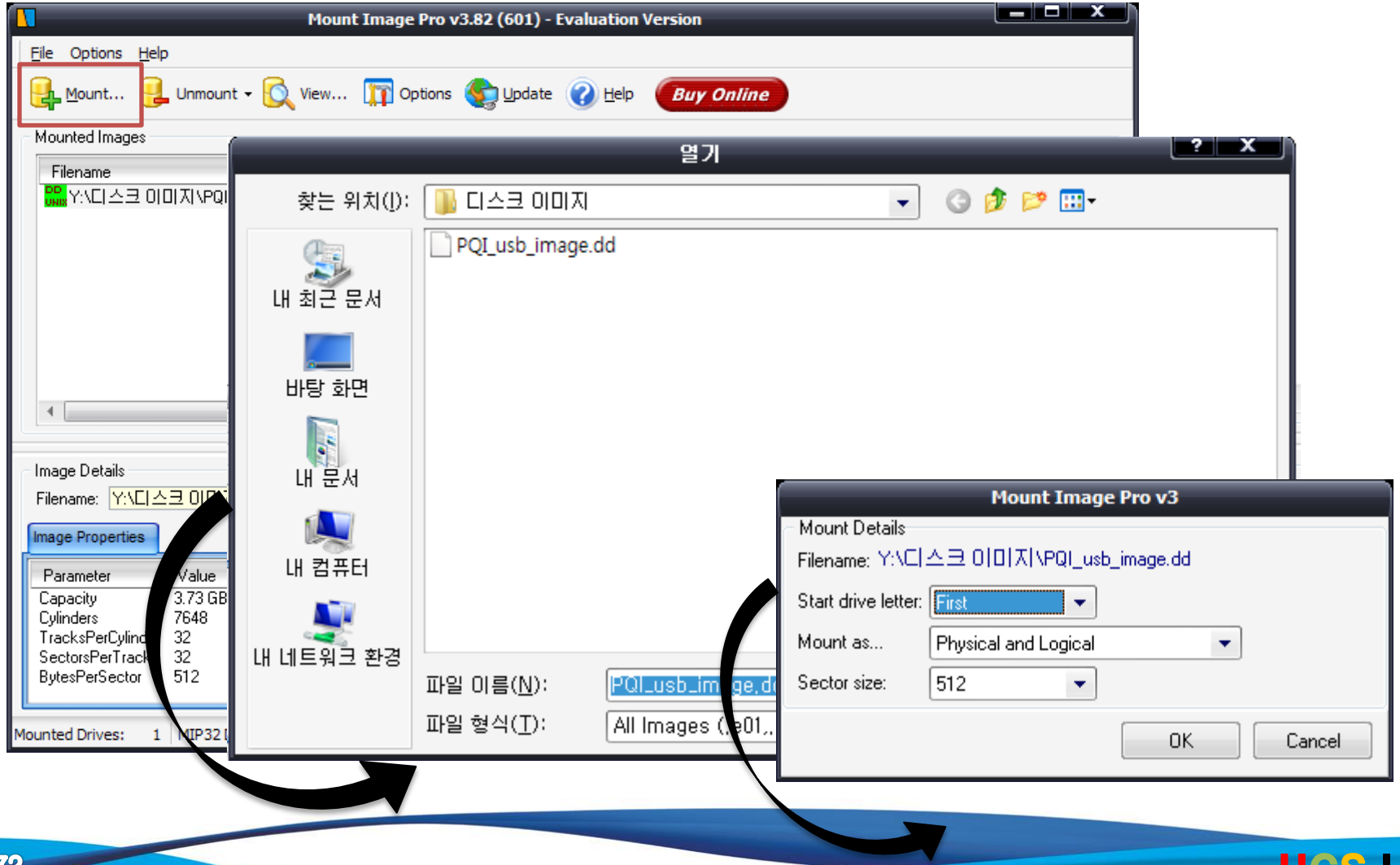


Image Mount Pro를 활용한 이미지 파일 열람

- 마운트가 완료되면 논리적으로 하나의 드라이브가 마운트됨

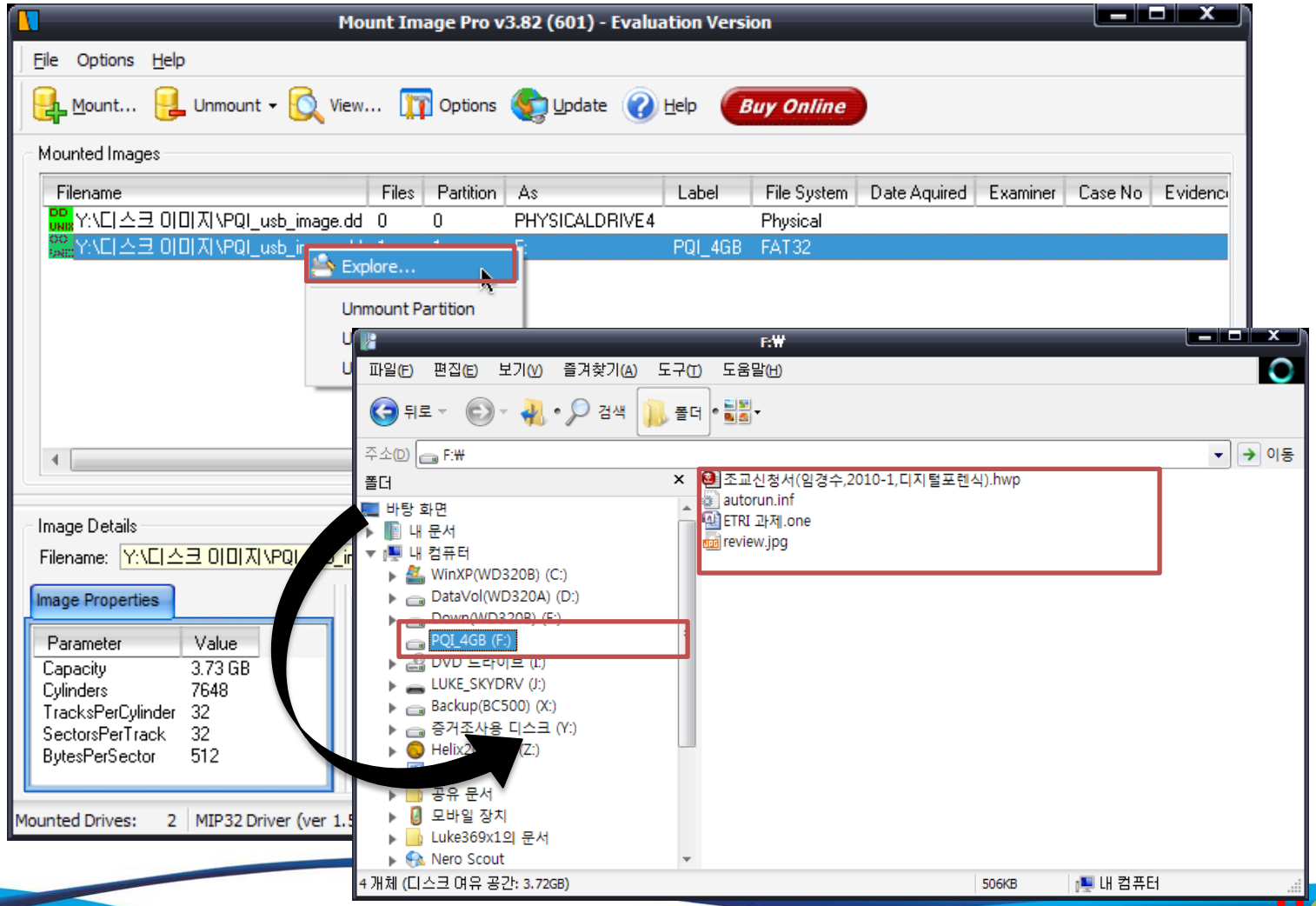
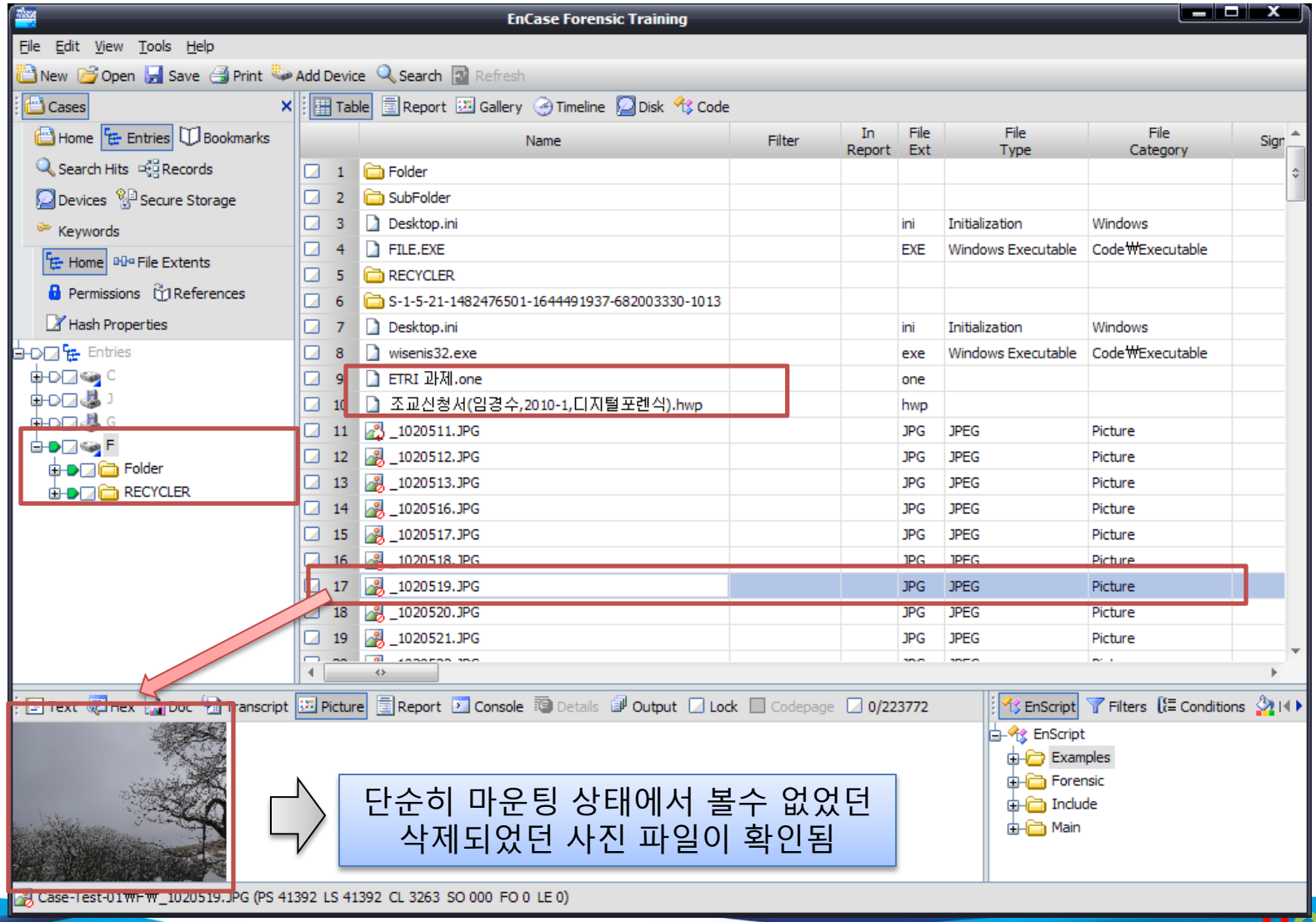


Image Mount Pro를 활용한 EnCase 분석

- **Image Mount Pro**로 마운트한 **DD** 이미지를 **EnCase**로 분석



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

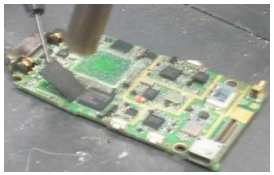
Request Files

Sending Files

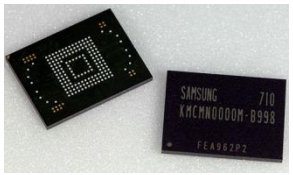
물리적 수집 방법

using JTAG Interface

or



using Flash Memory Reader



스마트폰 증거자료 추출 방법

- 스마트 폰 주요 데이터
  - 휴대폰 데이터 + **이메일, 아웃룩(MS), 인터넷 사용 기록, GPS 정보** 등

- 데이터 획득 방법

논리적 수집 방법

MS ActiveSync

or

Remote API

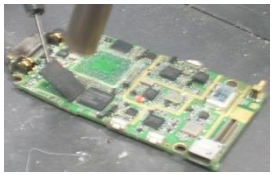
Request Files

Sending Files

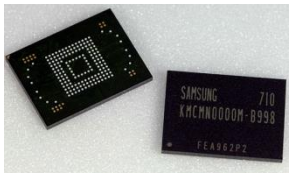
물리적 수집 방법

using JTAG Interface

or



using Flash Memory Reader

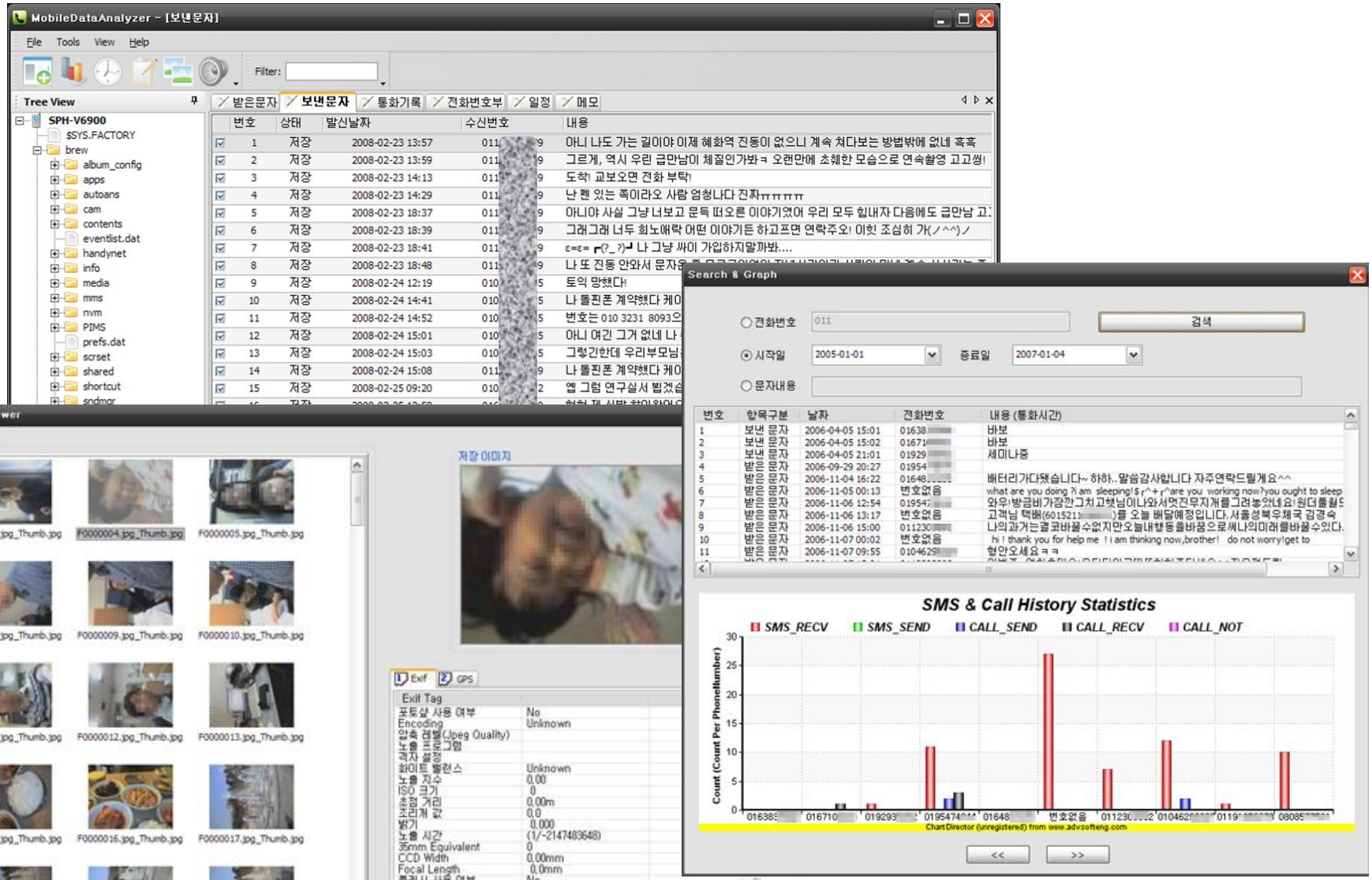


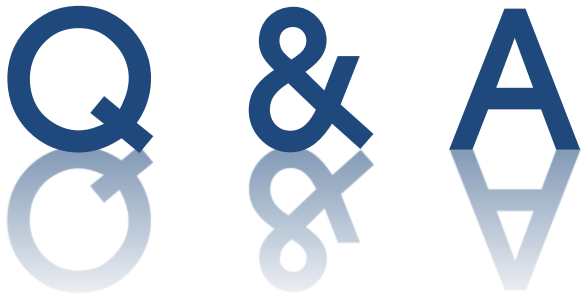
모바일 데이터의 분석

- 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




Q & A