

# 디지털 증거 수집 방안



*JK Kim*

*@pr0neer*

*forensic-proof.com*

*proneer@gmail.com*

# 개요

1. 온라인 수집
2. 오프라인 수집

# 온라인 수집

- 온라인이란?

- 시스템 전원이 켜져 있는 상태

- 온라인 수집 데이터

1. 라이브 데이터
2. 저장장치 복사
3. 저장장치 이미징

## 1. 라이브 데이터 (계속)

- 시스템 전원이 켜져 있는 상태에서 수집할 수 있는 데이터
- 휘발성 데이터인 메모리 데이터와 비휘발성 주요 데이터 포함
- 이벤트의 원인을 가장 잘 알려줄 수 있는 데이터

- 라이브 데이터와 증거 능력

- ✓ 엄격한 사건의 경우 증거 능력의 논란이 있음
- ✓ 증거 능력을 갖추기 위한 절차나 연구가 부족한 상황

- 침해사고와 라이브 데이터

- ✓ 침해사고는 라이브 데이터를 최대한 활용!!
- ✓ 분석에 도움이 되는 정보는 최대한 수집!!

## 1. 라이브 데이터 (계속)

- 라이브 데이터 대상

- ✓ 물리메모리

- ✓ 활성데이터

- 네트워크 정보
    - 프로세스 정보
    - 사용자 로그인 정보
    - 시스템 정보
    - 네트워크 인터페이스 정보
    - 작업스케줄러 정보
    - 클립보드 정보
    - 자동실행 정보
    - ... ..

- ✓ 비활성 주요 데이터

- ✓ 네트워크 패킷

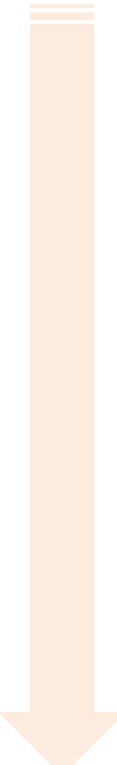
## 1. 라이브 데이터 (계속)

- 라이브 데이터 수집 시 고려 사항

- ✓ 시스템 흔적이 최소한으로 남도록 시스템 스크립트나 커맨드라인 명령 사용
  - 윈도우 → 배치 스크립트
  - 리눅스/유닉스 → 셸 스크립트
- ✓ 수집 대상 시스템의 명령을 사용하지 않고 직접 준비해간 명령 사용 → 사전 준비
- ✓ 중복체크가 가능하도록 명령 중복 실행
- ✓ 스크립트 동작 과정에 대한 로그 수집
- ✓ 다양한 환경에서 명령 혹은 모듈 안전성의 반복적인 테스트
- ✓ 휘발성 민감도(OOV, Order Of Volatility)를 반영한 수집???

## 1. 라이브 데이터 (계속)

- 휘발성 민감도 (OOV)



실전 포렌식	RFC 3227	NIST SP 800-86
네트워크 연결 정보	레지스터, 캐시	네트워크 연결 정보
물리메모리	라우팅 테이블, ARP 캐시	로그온 세션
프로세스 정보	프로세스 정보	물리 메모리
사용자 로그인 정보	물리 메모리	프로세스 정보
시스템 정보	임시 파일 시스템	열린 파일
네트워크 인터페이스 정보	디스크	네트워크 설정 경보
작업스케줄러	원격 로그인과 모니터링 데이터	시스템 시간
클립보드, 자동실행	물리적 설정, 네트워크 토폴로지	N/A
네트워크 패킷	기타 저장장치	N/A



## 1. 라이브 데이터 (계속)

- 활성 데이터 뿐만 아니라 비활성 주요 데이터도 수집 필요!!
- 비활성 주요 데이터만으로 포렌식 분석의 80% 이상 수행
- ???) 비활성 주요 데이터 수집 시간 + 대상 시스템 손상률 **vs.** 분석의 효율성
- **비활성 주요 데이터**
  - ✓ 파일시스템 메타데이터
  - ✓ 레지스트리
  - ✓ 프리패치
  - ✓ 이벤트 로그
  - ✓ 웹 브라우저 메타데이터
  - ✓ %SystemRoot%\system32\drivers\etc 폴더
  - ✓ %SystemRoot%\system32\config\systemprofile 폴더
  - ✓ ... ..

## 1. 라이브 데이터 (계속)

- 비활성 주요 데이터 수집 시 고려 사항
  - ✓ 수집 효율을 위해 라이브 데이터 수집 스크립트에 포함
  - ✓ 커맨드라인 명령으로 수집이 가능해야 함
  - ✓ 운영체제가 점유하고 있는 파일의 수집 방안 마련
  - ✓ 수집 시간을 고려하여 수집 데이터 선별
  - ✓ 조사관에게 수집 여부 옵션을 제공해야 함

## 1. 라이브 데이터 (계속)

- 라이브 데이터

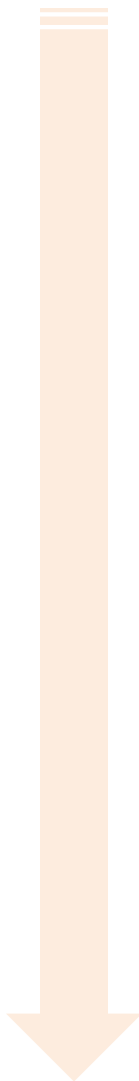
- ✓ 네트워크 정보
- ✓ 프로세스 정보
- ✓ 사용자 로그인 정보
- ✓ 시스템 정보
- ✓ 네트워크 인터페이스 정보
- ✓ 작업스케줄러 정보
- ✓ 클립보드 정보
- ✓ 자동실행 정보
- ✓ ... ..

- 비활성 주요 데이터

- ✓ 파일시스템 메타데이터
- ✓ 레지스트리
- ✓ 프리패치
- ✓ 이벤트 로그
- ✓ 웹 브라우저 메타데이터
- ✓ %SystemRoot%\system32\drivers\etc 폴더
- ✓ %SystemRoot%\system32\config\systemprofile 폴더
- ✓ ... ..

## 1. 라이브 데이터 (계속)

- 수집 순서



구분	수집 항목
비활성	프리패치
활성	네트워크 정보
활성	물리메모리
활성	프로세스 정보
활성	사용자 로그인 정보
활성	시스템 정보
활성	네트워크 인터페이스 정보
활성	작업스케줄러, 클립보드, 자동실행 정보
비활성	파일시스템 메타데이터
비활성	레지스트리
비활성	이벤트 로그
비활성	%SystemRoot% 하위 주요 파일
비활성	웹브라우저 아티팩트
활성	네트워크 패킷

## 1. 라이브 데이터 (계속)

- FPLive\_win.bat – <http://forensic-proof.com/resources/>

 **FORENSIC-PROOF** | Incident Investigation  
and Response

BLOGABOUTSTORYTOOLS  
SLIDESRESOURCES

Resources

**FP LIVE FORENSICS**  
FPLive\_win- FPLive\_win is script to acquire windows live data including memory dump, non-volatile data, packets.

## 1. 라이브 데이터 (계속)

- FPLive\_win.bat – NETWORK INFORMATION

<b>arp -a</b>	ARP 테이블 정보
<b>netstat -nao</b>	네트워크 상태 정보
<b>route PRINT</b>	라우팅 테이블 정보
<b>cports /stext</b>	TCP/IP 네트워크 열린 포트 정보
<b>urlprotocolview /stext</b>	URL 프로토콜 정보
<b>net session</b>	로컬 컴퓨터와의 모든 세션 정보
<b>net file</b>	서버 상에 열린 파일 목록
<b>net share</b>	로컬 컴퓨터에서 공유되고 있는 모든 리소스 정보
<b>nbtstat -c</b>	NetBIOS 캐시 내용
<b>tcpvcon -a -c</b>	모든 TCP 종단간 연결 목록

## 1. 라이브 데이터 (계속)

- FPLive\_win.bat – **PROCESS INFORMATION**

<b>pslist</b> /accepteula	동작 중인 프로세스 정보
<b>cprocess</b> /stext	동작 중인 프로세스 정보
<b>procinterrogate</b> -ps	동작 중인 프로세스 정보
<b>tasklist</b> -V	동작 중인 프로세스 정보
<b>tlist</b> (-c   -t   -s)	동작 중인 프로세스 정보
<b>listdlls</b> /accepteula	로드된 DLL 정보
<b>dllexp</b> /stext	DLL의 모든 익스포트 함수 목록과 가상 메모리 주소 정보
<b>injecteddll</b> /stext	프로세스에 인젝션된 DLL 목록
<b>handle</b> /accepteula	프로세스가 열고 있는 핸들 목록
<b>openfilesview</b> /stext	프로세스가 열고 있는 파일 목록

## 1. 라이브 데이터 (계속)

- **FPLive\_win.bat – LOGON USER INFORMATION**

<b>psloggedon</b> /accepteula	로컬과 리소스 공유 로그인 사용자 정보
<b>logonsessions</b> /accepteula	활성화된 로그인 세션 정보
<b>netusers</b> /local /history	로컬 사용자 로그인 기록
<b>net user</b>	사용자 계정 정보

- **FPLive\_win.bat – SYSTEM INFORMATION**

<b>psinfo</b> /accepteula	로컬 혹은 원격 시스템의 주요 정보
<b>psinfo</b> (-d   -s   -h)	디스크 볼륨(-d), 설치된 애플리케이션(-s), 설치된 핫픽스
<b>wul</b> /stext	설치된 윈도우 업데이트 목록
<b>gplist</b>	적용된 그룹 정책 정보
<b>gpresult</b> /Z	그룹 정책에 관한 모든 정보
<b>psservice</b> /accepteula	시스템 서비스 정보



## 1. 라이브 데이터 (계속)

- FPLive\_win.bat – NETWORK INTERFACE INFORMATION

<b>promiscdetect</b>	promiscuous 모드 탐지
<b>ipconfig /all</b>	NIC 전체 구성 정보
<b>ipconfig /displaydns</b>	DNS 캐시 정보
<b>getmac</b>	NIC 맥 정보

- FPLive\_win.bat – MISCS

<b>schtasks /query /fo list /v</b>	작업 스케줄러 정보
<b>pclip</b>	클립보드 정보
<b>autorunsc /accepteula</b>	자동 실행 정보

## 1. 라이브 데이터 (계속)

- FPLive\_win.bat – **PHYSICAL MEMORY**

<b>Fdpro</b>		<b>win(32 64)dd /m /0 /r /f</b>		<b>memorize</b> (configure XML)
--------------	--	---------------------------------	--	---------------------------------

- FPLive\_win.bat – **NON-VOLATILE DATA**

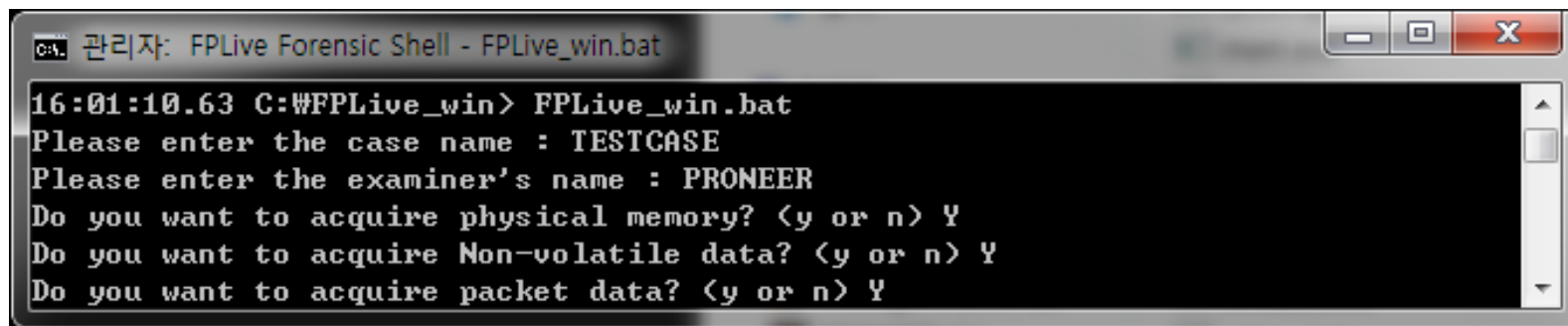
<b>forecopy_handy -m   --mft</b>	\$MFT 수집
<b>forecopy_handy -p   --prefetch</b>	프리패치 파일 수집
<b>forecopy_handy -g   --registry</b>	레지스트리 하이버 파일 수집
<b>forecopy_handy -t   --etc</b>	System32\drivers\etc 폴더 수집
<b>forecopy_handy -e   --evtlog</b>	이벤트 로그 수집
<b>forecopy_handy -i   -x   -c</b>	IE Firefox Chrome 아티팩트 수집

- FPLive\_win.bat – **NETWORK PACKETS**

<b>dumpcap -i %_NIC% -a duration:180 -w %_PACKET_DIR%\NIC_%_NIC%.pcap</b>
---

## ➔ 실습

- FPLive\_win.bat을 이용해 윈도우 라이브 데이터 수집하기!!
  - 1) 대상 윈도우 시스템의 버전을 확인한 후, 해당 버전 폴더의 cmd.exe 실행
  - 2) setenv.bat를 실행하여 환경 변수 변경
  - 3) FPLive\_win.bat를 실행



```
C:\> 관리자: FPLive Forensic Shell - FPLive_win.bat
16:01:10.63 C:\#FPLive_win> FPLive_win.bat
Please enter the case name : TESTCASE
Please enter the examiner's name : PRONEER
Do you want to acquire physical memory? <y or n> Y
Do you want to acquire Non-volatile data? <y or n> Y
Do you want to acquire packet data? <y or n> Y
```

## ➔ 실습

- FPLive\_win.bat로 침해 시스템에서 수집한 라이브 데이터 분석하기!! (CASE #1)
  - 1) 감염 시스템의 운영체제는 무엇인가?
  - 2) 악성 프로세스의 이름과 PID는 무엇인가?
  - 3) 악성 프로세스를 실행시킨 사용자는 누구인가?
  - 4) 악성 프로세스는 언제 실행되었는가?
  - 5) 악성 프로세스가 열고 있는 파일은 몇 개인가?
  - 6) 악성 프로세스가 작업 스케줄러에 등록한 작업은 몇 개인가?
  - 7) 드롭퍼(최초 실행된 악성코드)는 시스템의 어디에 위치하고 있는가?
  - 8) 자동 실행 위치에 등록된 악성코드는 무엇인가? (전체 경로)
  - 9) 드롭퍼가 생성한 것으로 보이는 악성코드를 모두 나열하라. (전체 경로)

## ➔ 실습

- FPLive\_win.bat로 침해 시스템에서 수집한 라이브 데이터 분석하기!! (CASE #2)

## 2. 저장장치 복사

- 압수수색 대상이 특정 폴더나 파일로 제한될 경우

- ✓ 라이브 상태에서 특정 시간 대역이나 사용자 행위를 중심으로 파일 검색 후 추출
- ✓ 라이브 상태에서 특정 키워드를 기준으로 검색 후 추출

- 저장장치 이미징이 불가능하거나 빠른 분석이 필요한 경우

- ✓ 라이브 상태에서 주요 분석 데이터 수집
- ✓ 리눅스 시스템의 경우, "/var/log" 폴더
- ✓ 윈도우 시스템의 경우,
  - 웹 브라우저 데이터 수집
  - 이메일 스토리지 파일 수집
  - 볼륨 샷도 복사본 수집
  - 대용량 로그(웹 로그, 애플리케이션 로그 등) 수집
  - 데이터 베이스 파일 수집
  - 특정 시간을 기준으로 생성/수정/접근된 파일 수집
  - ... ..

## 2. 저장장치 복사

- 복사 도구

- ✓ **ROBOCOPY** – Microsoft

- <http://technet.microsoft.com/en-us/library/cc733145.aspx>

- ✓ **XCOPY** – Microsoft

- <http://technet.microsoft.com/en-us/library/bb491035.aspx>

- ✓ **RichCopy** – Microsoft

- <http://technet.microsoft.com/en-us/magazine/2009.04.utilityspotlight.aspx>

- ✓ **FORECOPY** – FORENSIC-PROOF

- <https://code.google.com/p/proneer/downloads/list>

- ✓ **GImageX** – Autoit

- <http://www.autoitscript.com/site/autoit-tools/gimagex/>

## 2. 저장장치 복사

- **ROBOCOPY (Robust File Copy)**, <http://technet.microsoft.com/en-us/library/cc733145.aspx>

- ✓ 복사 주요 옵션

- **/S** : 비어 있는 디렉터리를 제외하고 하위 디렉터리 복사
- **/E** : 비어 있는 디렉터리를 포함하여 하위 디렉터리를 복사
- **/MIR** : 디렉터리 트리를 미러링
- **/COPY:FLAG** : 파일 정보를 복사 (기본값은 /COPY:DAT)  
D = 데이터, A = 특성, T = 타임스탬프, S = 보안 = NTFS ACL, O = 소유자, U = 감사 정보)
- **/COPYALL** : 모든 파일 정보를 복사 (COPY:DATSOU)

- ✓ 파일 선택 주요 옵션

- **/IA:[RASHCNETO]** : 지정된 특성을 가진 파일만 포함
- **/MAXAGE:yyyymmdd** : yyyymmdd 보다 최신 파일만 복사
- **/MINAGE:yyyymmdd** : yyyymmdd 보다 이전 파일만 복사
- **/XJ** : 연결지점(JUNCTION) 제외 (일반적으로 기본값)



## 2. 저장장치 복사

- **ROBOCOPY (Robust File Copy)**, <http://technet.microsoft.com/en-us/library/cc733145.aspx>
  - ✓ 다시 시도 주요 옵션
    - **/R:n** : 실패한 복사본 다시 시도 횟수 (기본값은 백만번)
    - **/W:n** : 다시 시도 대기 시간 (기본값은 30초)
  - ✓ 로깅 주요 옵션
    - **/TS** : 출력에 원본 파일 타임스탬프를 포함
    - **/FP** : 출력에 파일의 전체 경로 이름을 포함
    - **/ETA** : 복사하는 파일의 예상 도착시간을 표시
    - **/TEE** : 로그 파일과 콘솔 창에 출력
    - **/LOG:FILE** : 상태를 로그 파일에 출력 (기존 파일을 덮어씀)

## 2. 저장장치 복사

- ROBOCOPY 예제

- ✓ 프리패치 파일 수집

```
#> ROBOCOPY C:\Windows\Prefetch F:\Prefetch /MIR /R:10 /W:10 /LOG:"F:\prefetch.log"
```

- ✓ 바로가기 파일 수집

```
#> ROBOCOPY C:\ F:\LNKs /MIR /R:10 /S /TS /FP /R:0 /W:0 /TEE /LOG:"F:\lnk_copy.log"
```

- ✓ 휴지통 하위 모든 파일 수집

```
#> ROBOCOPY C:\$Recycle.Bin F:\Recycle /S /MIR /COPYALL /TS /FP /LOG:"F:\recycle.log"
```

- ✓ 로그 파일 원격 백업

```
#> ROBOCOPY D:\LOG \\192.168.10.24\F$\LOG /E /MIR /R:1 /W:1
```

## 2. 저장장치 복사

- **ROBOCOPY 예제**

- ✓ ROBOCOPY를 이용한 수집 스크립트

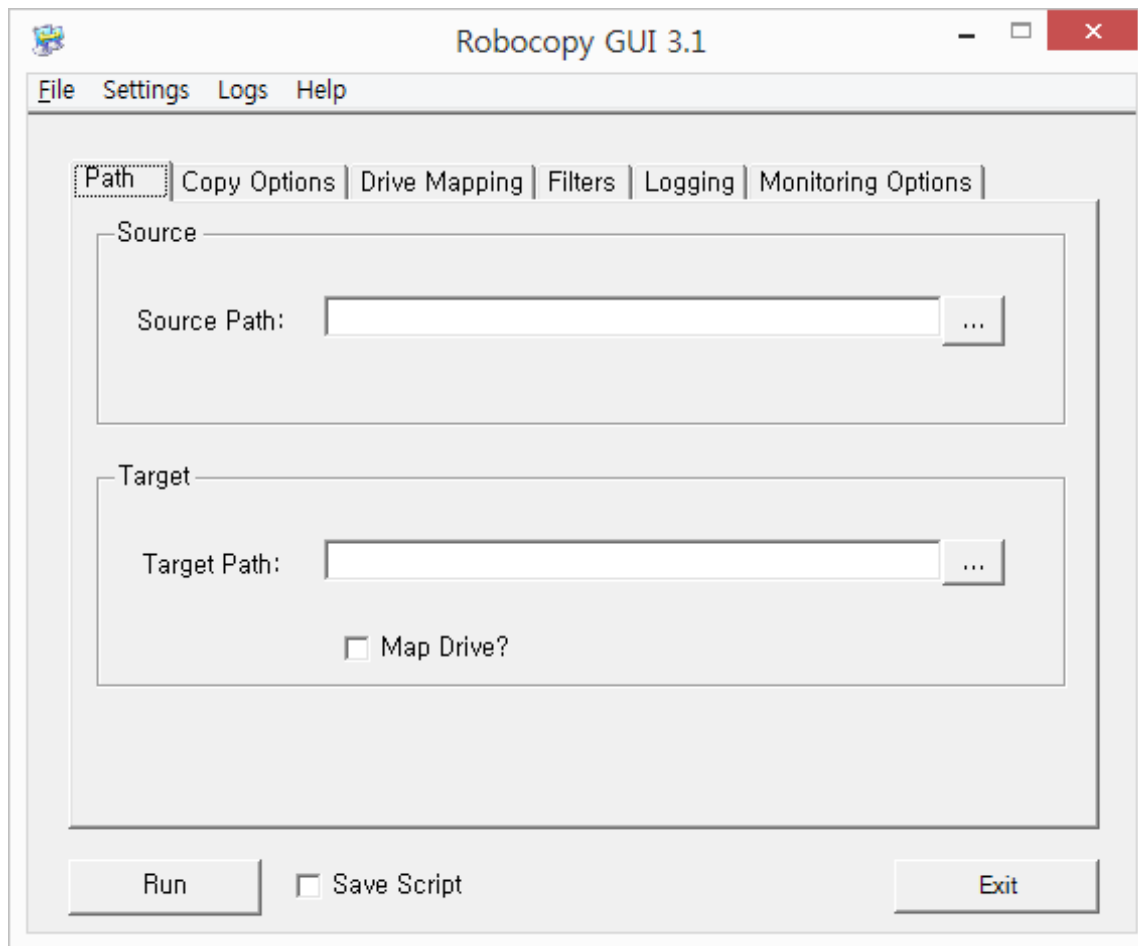
<http://computer-forensics.sans.org/blog/2009/01/08/robocopy-a-computer-forensics-tool/comment-page-1>

```
echo off
echo About to copy files from %1: to %computername%-%1 on portable drive.
... ..
cd
attrib -h -s %computername%-%1
ver | find "Microsoft" > %computername%-%1Version.txt
type %computername%-%1Version.txt
find "XP" %computername%-%1Version.txt
if "%errorlevel%" == "0" goto XPCommand
echo.
echo Error Level not equal to 0
echo VISTA System....
rem Call the Vista version of Robocopy for the XJ parm. Note no path to robocopy provided.
pause
robocopy %1: %computername%-%1 *.pst *.ost *.out *.xls* *.txt *.doc* *.zip *.csv *.mdb *.ldif *.rtf
*.dbf *.prt *.pdf *.tif* /S /COPY:DAT /IA:RASHCNETO /MAXAGE:%2 /TS /FP /XJ /NC /NS /NP /W:0 /R:0
/TEE /LOG:%computername%-%1ROBOLOG.TXT
goto VistaCommand
```

## 2. 저장장치 복사

- **ROBOCOPY GUI**

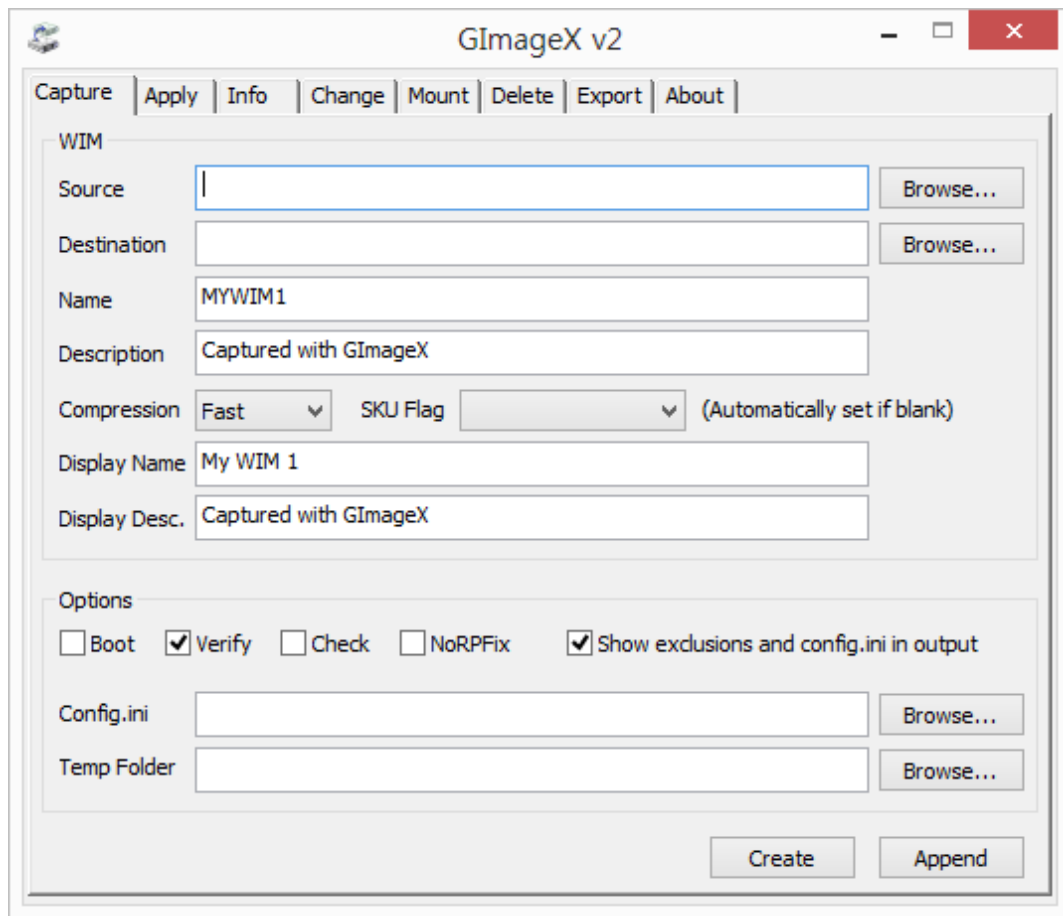
<http://technet.microsoft.com/en-us/magazine/2006.11.utilityspotlight.aspx>



## 2. 저장장치 복사

- GImageX

- ✓ Windows Imaging Format(WIM) 형식의 파일 획득



## ➔ 실습

- ROBOCOPY를 이용해 파일 선별 수집하기!!
  - 1) 시스템 이벤트 로그 수집하기!!
  - 2) %SystemRoot%\system32\config 폴더 하위 모든 파일 수집하기!!

## 3. 저장장치 이미징

- 컴퓨터 전원을 끌 수 없는 경우 라이브 상태에서 저장장치 이미징
- 논리적인 구성(RAID, LVM 등)의 경우에도 라이브 저장장치 이미징 수행!!
- 주로 소프트웨어를 사용해 이미징
- **로컬 이미징**
  - ✓ 로컬에 직접 연결하여 이미징 수행
  - ✓ 여분의 저장장치 슬롯을 이용하거나 외부 인터페이스(USB/IEEE 1394/eSATA 등) 이용
- **원격 이미징**
  - ✓ 네트워크 케이블을 이용해 이미징 수행
  - ✓ 여분의 네트워크 포트를 이용하거나 서비스 포트를 사용
  - ✓ 서비스 가용성을 고려하여 여유 시간대나 트래픽을 제한하여 이미징

## 3. 저장장치 이미징

- 로컬 이미징 도구

- ✓ **FTK Imager (Lite)** – AccessData

<http://www.accessdata.com/support/product-downloads>

- ✓ **Tableau Imager (with Tableau W/B)** – Guidance Software

<http://www.tableau.com/index.php?pageid=products&category=software>

- ✓ **EnCase Forensic Imager** – Guidance Software

<http://www.guidancesoftware.com/Document.aspx?did=1000021905>

- ✓ **포렌식 이미징 도구 비교 (FTK vs Tableau vs EnCase Imager)**

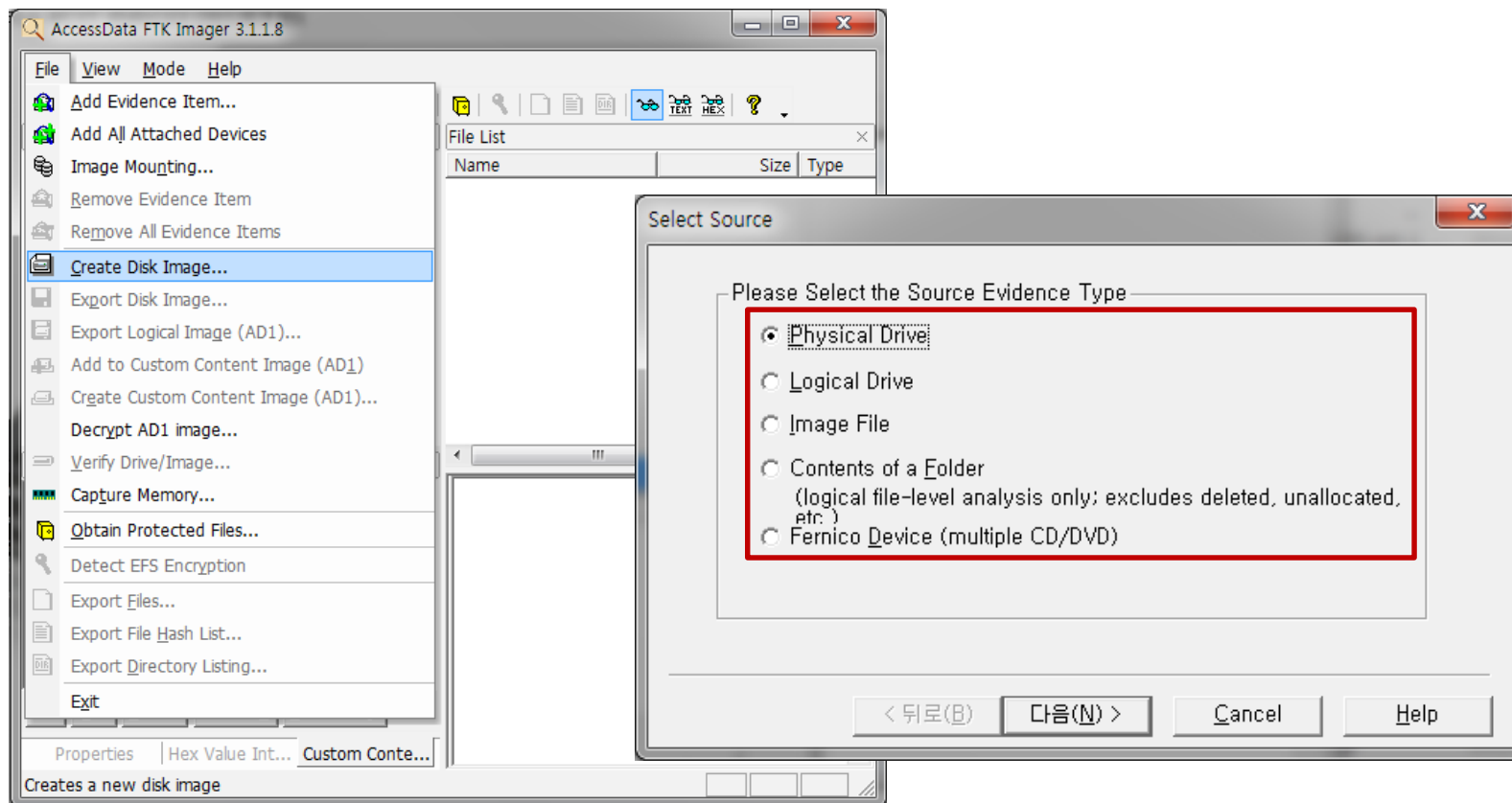
<http://forensic-proof.com/archives/4871>



## 3. 저장장치 이미징

- 로컬 이미징 도구

✓ FTK Imager (Lite) – AccessData



## ➔ 실습

- FTK Imager로 라이브 시스템의 저장장치 이미징하기!!
- FTK Imager로 이미지 파일 마운트하기!!

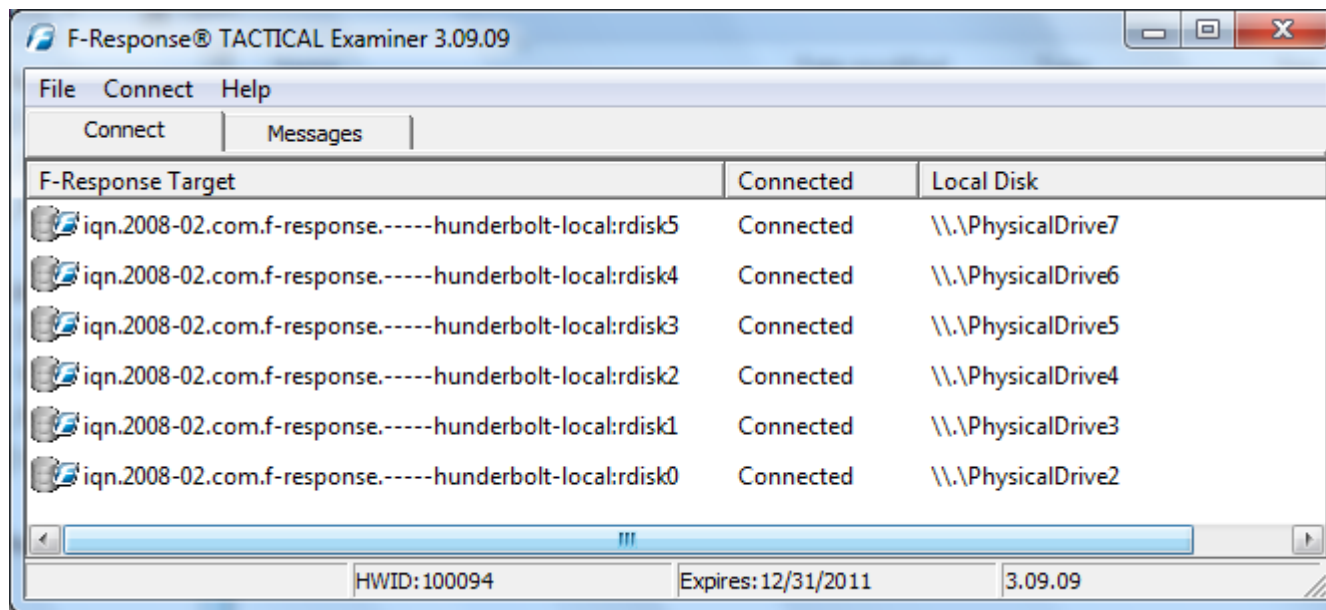
## 3. 저장장치 이미징

- 원격 이미징 도구
  - ✓ **F-Response Series** – F-Response  
<https://www.f-response.com/software>
  - ✓ **DD(Disk Dumper) + NetCat**

## 3. 저장장치 이미징

- 원격 이미징 도구

✓ **F-Response Series** – F-Response



## ➔ 실습

- F-Response TACTICAL로 원격 시스템의 저장장치 이미징하기!!

# 오프라인 수집

- 오프라인이란?

- 시스템 전원이 꺼져 있는 상태

- 오프라인 수집 데이터

1. 저장장치 복사
2. 저장장치 복제
3. 저장장치 이미징

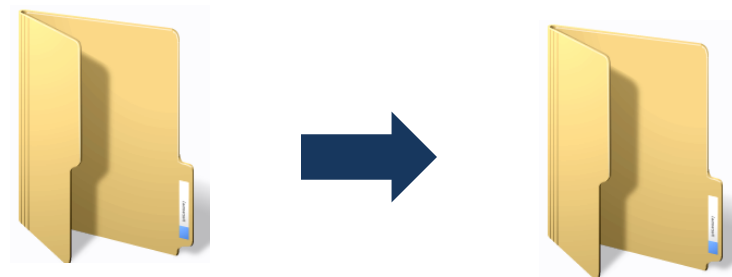
## 1. 저장장치 복사

- 압수수색 대상이 특정 폴더나 파일로 제한될 경우
  - ✓ 라이브 상태에서 특정 시간 대역이나 사용자 행위를 중심으로 파일 검색 후 추출
  - ✓ 라이브 상태에서 특정 키워드를 기준으로 검색 후 추출
- 저장장치 복제/이미징 작업 동안 사전 분석을 위한 데이터
  - ✓ 쓰기방지장치를 장착(???)한 상태에서 사전 분석 데이터 추출
  - ✓ 비활성 데이터 수집 시간 VS. 사전 분석 효율
  - ✓ 파일시스템 메타데이터, 레지스트리, 프리패치, 바로가기 파일, 이벤트 로그 등



## 1. 저장장치 복사

- 원본 읽기 → 사본 쓰기
- 상황에 따라 쓰기방지장치 장착 후 복사



- **장점**

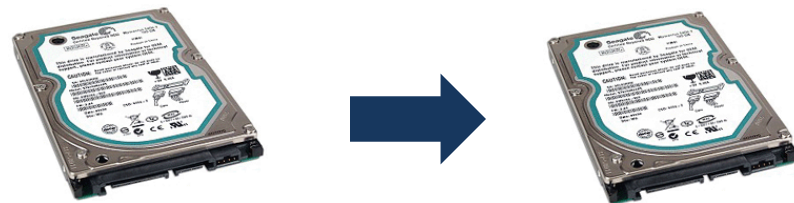
- ✓ 필요한 데이터만 비교적 손쉽게 수집 가능 → 신속한 분석

- **단점**

- ✓ 파일과 디렉터리 단위의 정보만 획득하는 일반적인 복사
- ✓ 원본의 메타 정보를 별도로 관리해야 함
- ✓ 삭제된 파일이나 슬랙에 은닉된 데이터는 확인할 수 없음

## 2. 저장장치 복제

- 원본 모든 섹터 → 사본 저장장치
- 비트스트림 복제



- **장점**

- ✓ 원본과 동일하기 때문에 삭제된 파일 복구 가능
- ✓ 일반적으로 이미징보다 속도가 빠름
- ✓ 현장 대응 방식으로 주로 사용

- **단점**

- ✓ 매 복제마다 원본보다 크거나 동일한 사본 저장장치 필요 → 사본 저장장치의 부담
- ✓ 사본 저장장치 특성에 의존 (저장장치 오류 및 배드섹터)
- ✓ 복제 전 사본 저장장치의 완전삭제 필요

## 3. 저장장치 이미징

- 원본 모든 섹터 → 이미지 파일
- 비트스트림 이미징



- **장점**

- ✓ 원본과 동일하기 때문에 삭제된 파일 복구 가능
- ✓ 사본 저장장치의 완전삭제가 필요 없음
- ✓ 여러 명이 분석할 경우 증거를 쉽게 분배/공유 가능
- ✓ 압축 기능을 이용해 분배 및 저장 효율 증대
- ✓ 암호화 기능을 이용해 안전성 강화

- **단점**

- ✓ 압축을 하지 않을 경우, 원본 저장장치보다 더 큰 저장장치 필요

## 3. 저장장치 이미징

- 원본 모든 섹터 → 이미지 파일
- 비트스트림 이미징



- **장점**

- ✓ 원본과 동일하기 때문에 삭제된 파일 복구 가능
- ✓ 사본 저장장치의 완전삭제가 필요 없음
- ✓ 여러 명이 분석할 경우 증거를 쉽게 분배/공유 가능
- ✓ 압축 기능을 이용해 분배 및 저장 효율 증대
- ✓ 암호화 기능을 이용해 안전성 강화

- **단점**

- ✓ 압축을 하지 않을 경우, 원본 저장장치보다 더 큰 저장장치 필요

## 3. 저장장치 이미징

- 포렌식 이미지 형식

- ✓ **RAW(dd)**

- 원본 저장장치의 순수 비트스트림 이미지
    - 별도의 이미지 파일 처리/보호 매커니즘 X

- ✓ **Expert Witness E01(Ex01)**

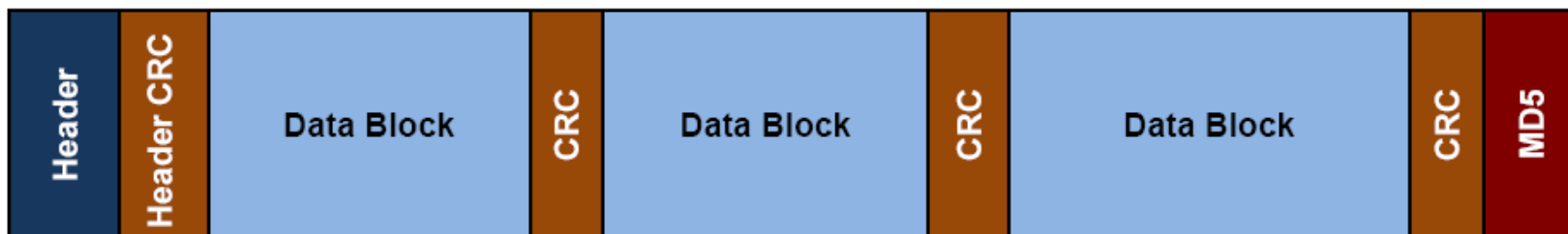
- 엔케이스(EnCase)에서 지원하는 이미지 형식
    - CRC, MD5를 이용하여 이미지 파일의 무결성 보장
    - 압축, 암호화 지원

- ✓ **기타 이미지 형식**

- AFF, SMART, IDIF, IRBF, IEIF, ProDiscover IF, SDi32's Format

## 3. 저장장치 이미징

- Expert Witness E01(Ex01) 형식



- E01 vs. Ex01

구분	E01	Ex01
압축 방식	DEFLATE	BZIP2
해쉬 알고리즘	MD5, SHA1	MD5, SHA1
보안기능	Password	AES256

- 오프라인 수집 도구

- 쓰기방지장치(Write Blocker/Protector, WB)

- ✓ **Tableau Forensic Bridge** – Guidance Software

[http://www.tableau.com/index.php?pageid=products&category=forensic\\_bridges](http://www.tableau.com/index.php?pageid=products&category=forensic_bridges)

- ✓ **Forensic Dock Series** – WiebeTech

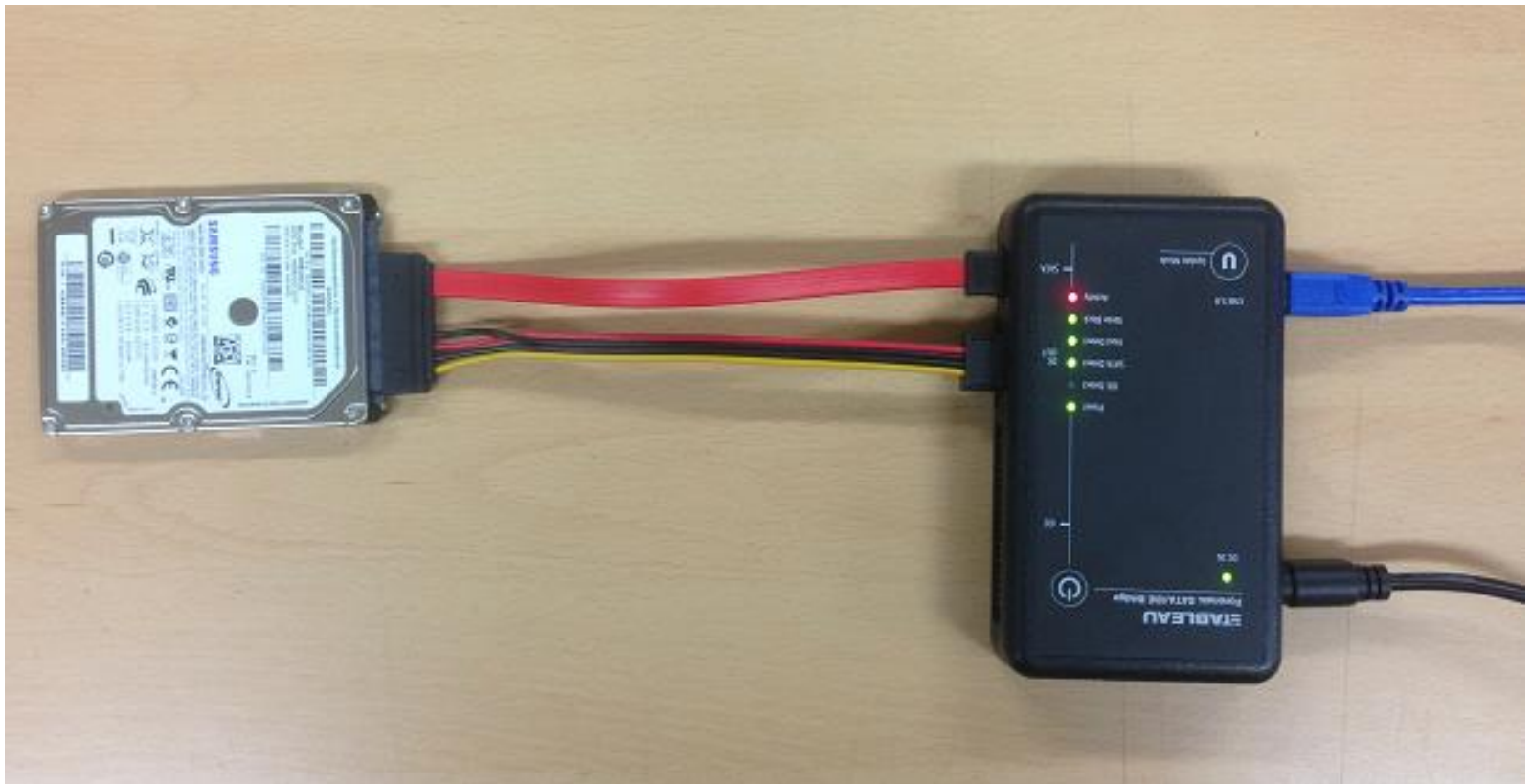
<http://www.wiebetech.com/home.php?home=5>

- ✓ **DriveLock** – ICS(Intelligent Computer Solutions)

<http://www.ics-iq.com/Super-DriveLock-Write-Blocker-Write-Protector-p/f.gr-0028-0000.htm>

# 오프라인 수집

- 오프라인 수집 도구
  - 쓰기방지장치(Write Blocker/Protector, WB)
    - ✓ Tableau Forensic Bridge – Guidance Software





- 오프라인 수집 도구

- 복제/이미징 도구

- ✓ **TD3** – Guidance Software

<http://www.tableau.com/index.php?pageid=products&model=TD3>

- ✓ **Falcon** – Logicube

<http://www.logicube.com/shop/falcon/>

- ✓ **MagiCube 2** – Data Expert

<http://www.dataexpert.com.hk/product/magicube%20%E2%80%93%202.htm>

- ✓ **Image MASter Solo-4** – ICS

<http://www.ics-iq.com/Image-MASter-Solo-4-RUGGEDIZED-p/f.gr-0055-000a.htm>

# 오프라인 수집

- 오프라인 수집 도구
  - 복제/이미징 도구
    - ✓ Image MASter Solo-4 – ICS



# 오프라인 수집

- 오프라인 수집 도구
  - 포렌식 하드웨어 장비가 너무 비싸다?!
  - 그렇다면, 이런 장비는?



## ■ 오프라인 수집 도구

### • 무결성 유지가 필요없다면

- ✓ 쓰기방지장치 없이 이미징 소프트웨어를 이용해 이미징
- ✓ 저렴한 저장장치 하드웨어 복제 도구를 이용해 복제

### • 무결성 유지가 필요하다면

- ✓ 쓰기방지장치 하에서 이미징 소프트웨어를 이용해 이미징
- ✓ 쓰기방지기능이 내장된 포렌식 하드웨어를 이용해 이미징

### • 전문 장비 사용의 이점

- ✓ 법적 소송을 대비해 저장물을 관리할 경우
- ✓ 복제 및 이미징 과정에서 대상 장치의 오류나 손상 가능성 최소화
- ✓ 압축, 암호화 기능을 통해 보관의 효율성과 기밀성을 높일 수 있음

