증거 획득

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

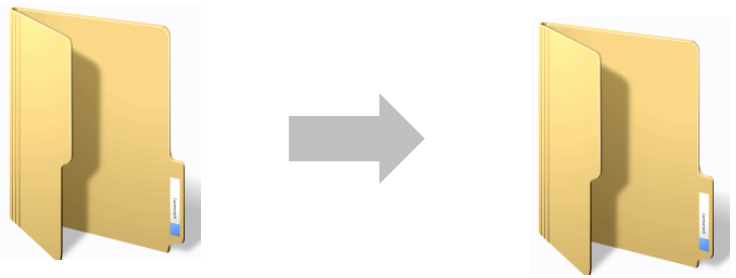
1. 증거 획득 방식
2. 증거 획득 장비
3. 증거 획득 도구

증거 획득 방식

Security is a people problem…

증거 획득 방식

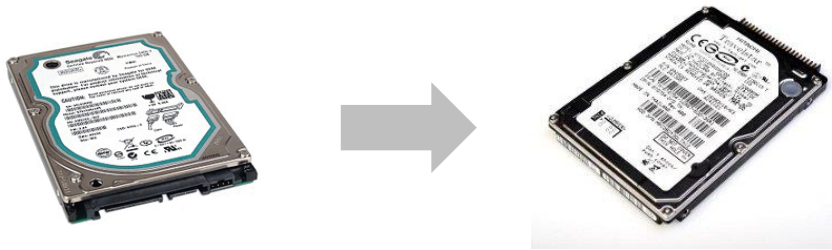
저장매체 복사



- **원본 읽기 ➔ 사본 쓰기**
- **장점**
  - 비교적 손쉬운 방법(?)으로 증거 수집 가능
  - 필요한 데이터만 빠르게 수집이 가능 ➔ 신속한 분석
  - 활성 시스템(시스템 전원을 내릴 수 없는 경우)에서 유용하게 활용
- **단점**
  - 활성 시스템의 무결성 훼손 (?) ➔ 무결성 훼손을 최소화하는 방안이 필요 (**fcopy**)
  - 파일과 디렉터리 단위의 정보만 획득 (일반적인 복사 작업)
  - 삭제된 파일이나 은닉된 데이터를 확인하기 어려움

증거 획득 방식

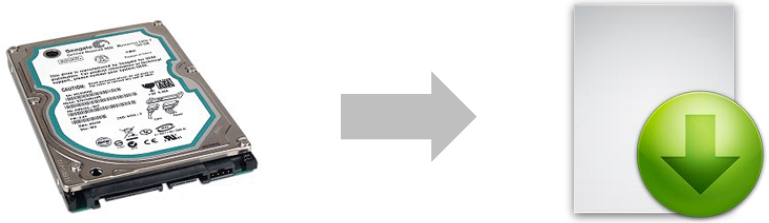
저장매체 복제



- **원본의 모든 물리적 섹터 ➔ 사본 저장매체**
- **비트스트림 복제**
- **장점**
  - 무결성 유지
  - 원본의 모든 정보를 획득 ➔ 삭제된 파일 복구 가능
- **단점**
  - 원본보다 크거나 동일한 사본 저장매체가 필요 ➔ 사본 저장매체의 낭비
  - 사본 저장매체(기기) 특성에 종속 (저장매체 오류 및 물리적 배드섹터)
  - 복제 전 사본 저장매체의 완전삭제(wiping)가 필요

증거 획득 방식

저장매체 이미징



- **원본의 모든 물리적 섹터 ➔ 이미지 파일**
- **비트스트림 이미징**
- **장점**
  - 무결성 유지
  - 원본의 모든 정보를 획득 ➔ 삭제된 파일 복구 가능
  - 사본 저장매체의 완전삭제(wiping)가 필요 없음
  - 쉽게 저장매체 이미지를 복사 가능 (여러 명이 작업할 경우)
  - 사본 이미지를 저장할 저장매체의 용량 제약이 없음 (압축 사용 가능)
- **단점**
  - 2TB 원본 저장매체의 이미지를 압축 없이 이미징하려면 2TB보다 큰 저장매체 필요

증거 획득 방식

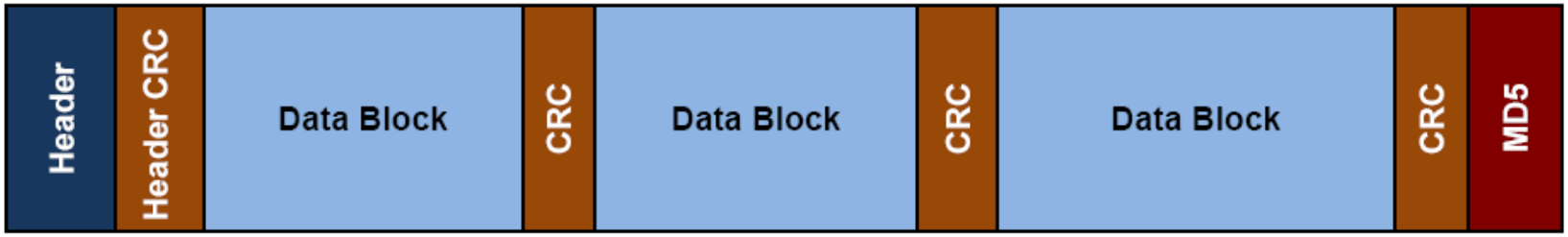
저장매체 이미지 종류

- **RAW(dd) 이미지**
  - 원본 저장매체의 비트스트림 이미지
  - 이미지 파일 자체의 무결성 훼손 우려 (?)
  - dd, dc3dd, dcfldd
- **E01(Ex01) 이미지**
  - EnCase에서 지원하는 이미지 파일
  - CRC, MD5를 이용하여 이미지 파일의 무결성 유지
  - EnCase, FTK Imager, Tableau Imager
- **AFF, SMART, IDIF, IRBF, IEIF, ProDiscover IF, SDi32's Format**

증거 획득 방식

저장매체 이미지 포맷

- **E01 이미지**



- **E01 vs Ex01**

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

증거 획득 장비

Security is a people problem…

증거 획득 장비

Rapid Image 7020CS

- **₩ 20,000,000 (1EA)** – US $ 11,500

증거 획득 장비

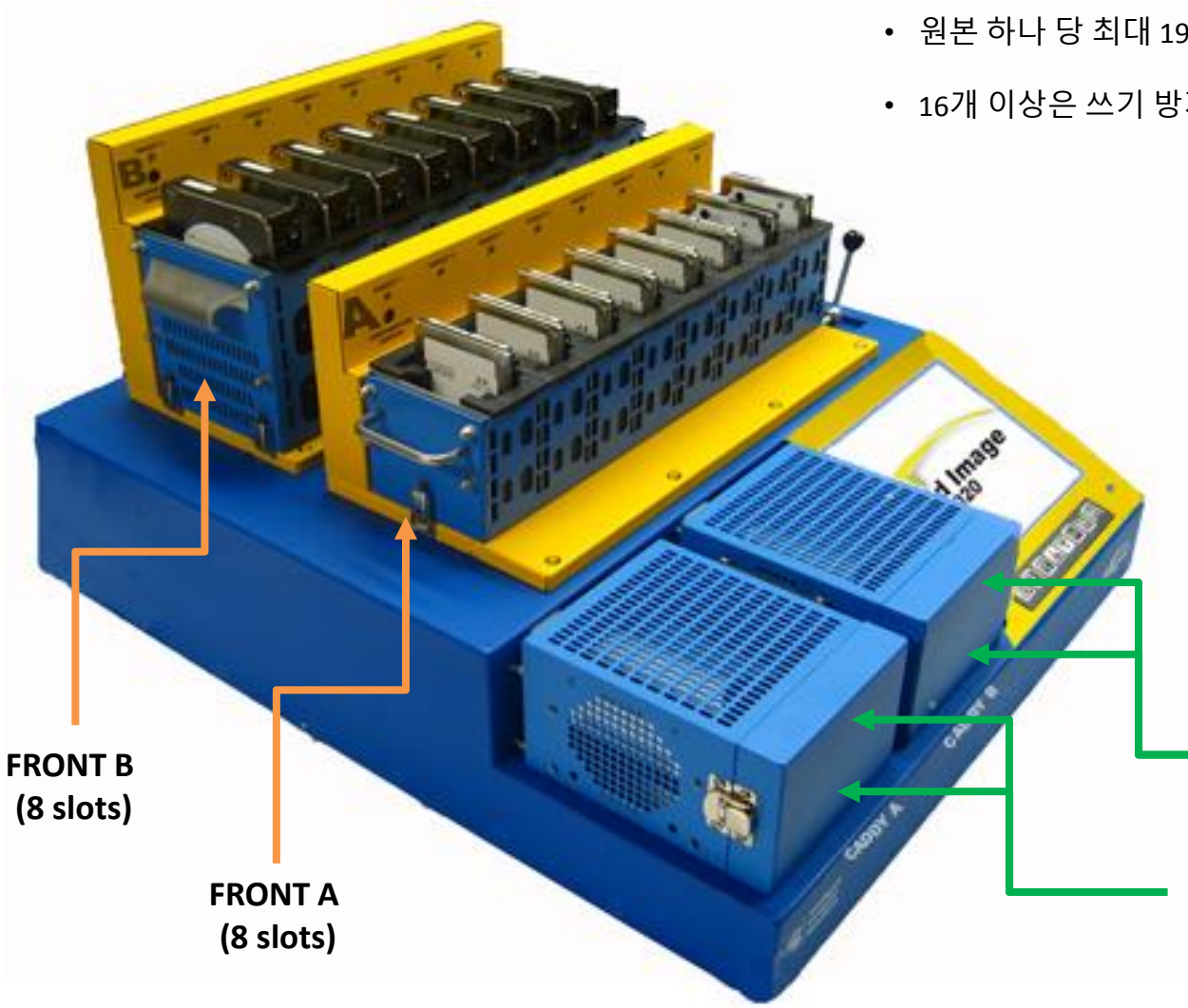
Rapid Image 7020CS

- **기능**
  - **속도** : 6GB/Min (100 MBps)
  - **지원 인터페이스** : SAS/SATA/IDE* (* optional)
  - **운영체제** : Windows Embedded Standard 7
  - **추가 기능**
    - HPA/DCO 지원
    - CRC32, MD5, SHA-1, SHA-2 지원
    - 저장매체 복제, 이미징(RAW, E01) 지원
    - 저장매체 완전삭제 기능

증거 획득 장비

Rapid Image 7020CS

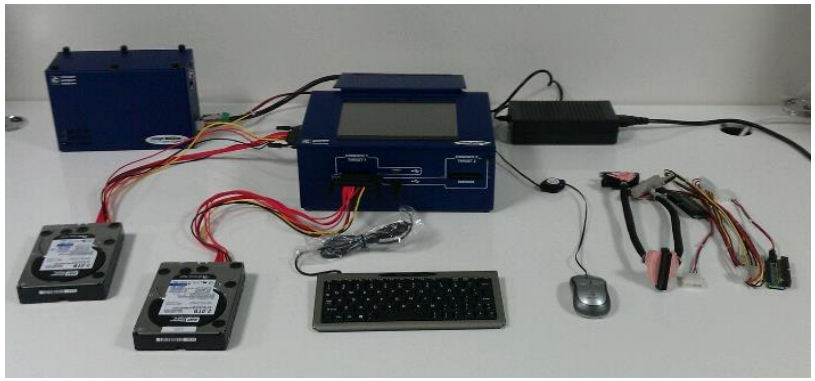
- 각각의 원본(CADDY) 마다 동시 4개의 사본 생성 가능
- 원본 하나 당 최대 19개 사본 동시 생성 가능
- 16개 이상은 쓰기 방지 설정 해제가 필요하므로 비추천



증거 획득 장비

SOLO 4 Forensic Super Kit (Expansion Box + SCSI to SCSI Card)

- **₩ 10,000,000 (3EA) – US $ 5,500**



증거 획득 장비

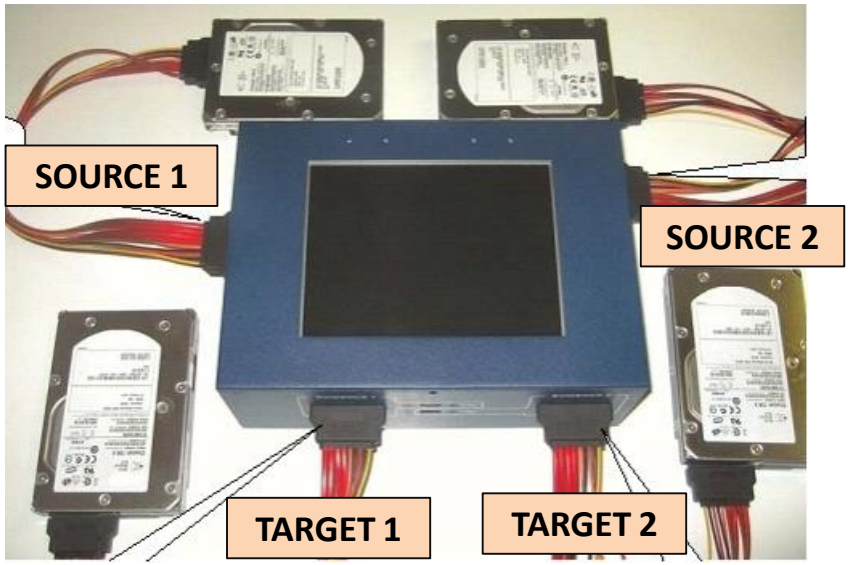
SOLO 4 Forensic Super Kit (Expansion Box + SCSI to SCSI Card)

- **기능**
  - **속도** : 6GB/Min (?)
  - **지원 인터페이스** : SATA/SAS(SATA2 speed), USB
  - **운영체제** : Windows Embedded Standard 7
  - **추가 기능**
    - SHA-1, SHA-2, MD5 지원
    - IDE, RAID, e-SATA, SD Card, CF Card 등 지원(컨버터), SCSI(Expansion Box) 등 지원
    - 저장매체 복제, 이미징(RAW, E01) 지원
    - 저장매체 완전삭제 기능
    - 네트워크 스토리지(SAN)에 업로드 기능

증거 획득 장비

SOLO 4 Forensic Super Kit (Expansion Box + SCSI to SCSI Card)

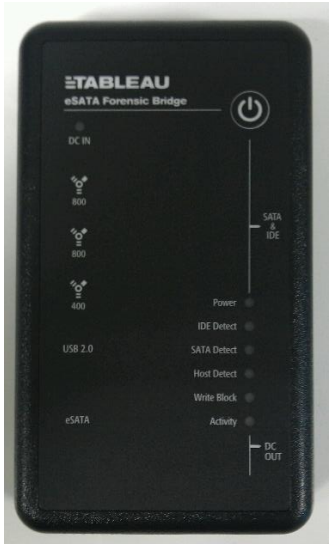
- 각각의 원본(SOURCE) 마다 동시 1개의 사본 생성 가능
- 원본 하나 당 최대 3개 사본 동시 생성 가능
- 2개 이상은 쓰기 방지 설정 해제가 필요하므로 비추천



증거 획득 장비

Super Tableau Kit

- ₩ 3,500,000 (3EA)



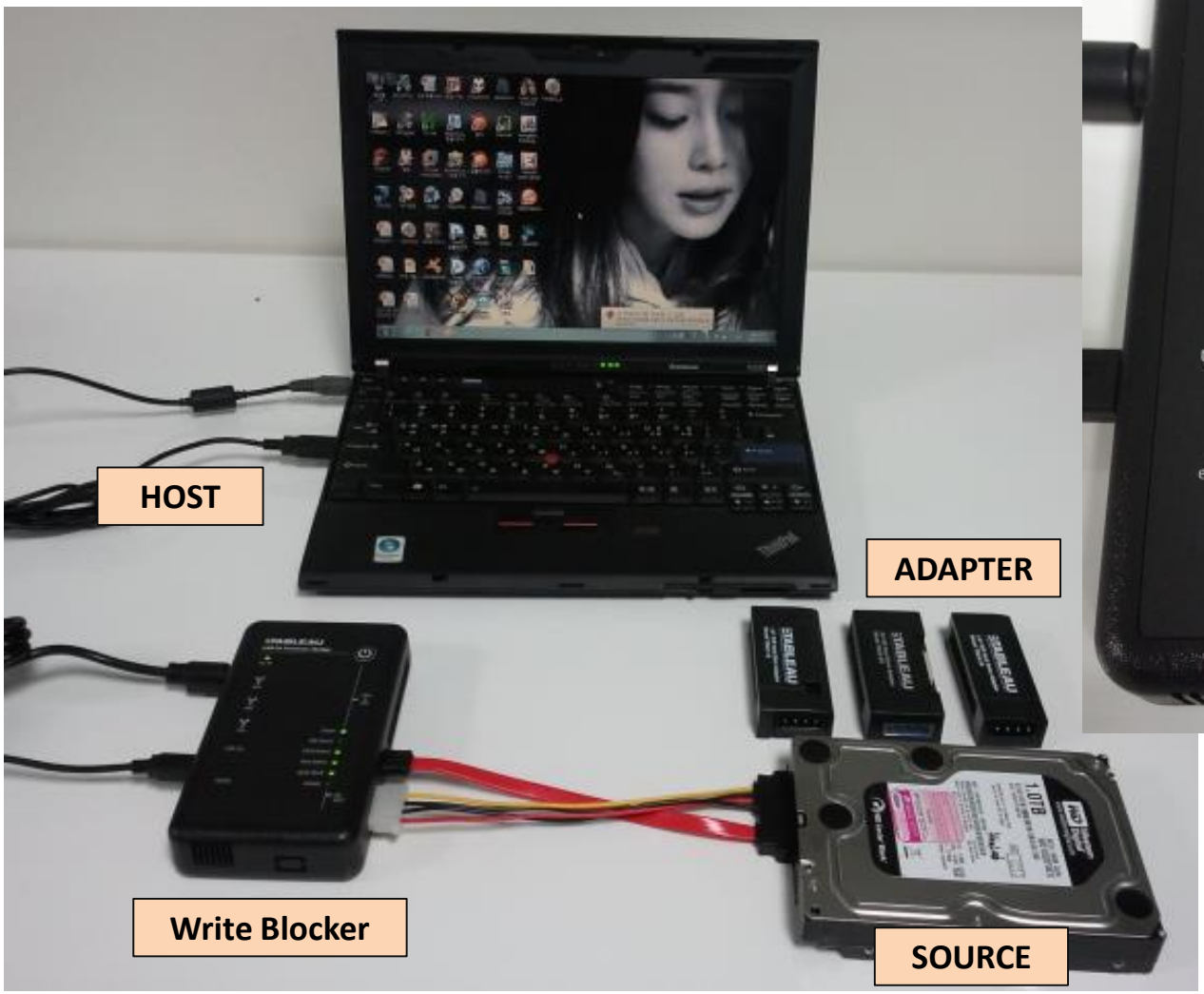
증거 획득 장비

Tableau Set

- **구성**
  - 1 x T35es S-ATA bridge
  - 1 x T4 SCSI bridge
  - 1 x T8 USB bridge
  - 2 x TP2 power supplies with power lead
  - 2 x Portable Hard Drive Coolers
  - FireWire 9 to 9, 9 to 6, 6 to 6 and 6 to 4 cables
  - 2 x USB cables
  - 1 x SCSI 68 pin to 50 pin and SCA adaptor
  - 1 x Tableau 2.5" Adaptor
  - 1 x Tableau 1.8" Adaptor
  - 1 x Tableau ZIF Adaptor
  - 1 x Tableau Utilities disk
  - 1 x Addonics Write Protected Smart Card Read

증거 획득 장비

Tableau Set (SATA/IDE)



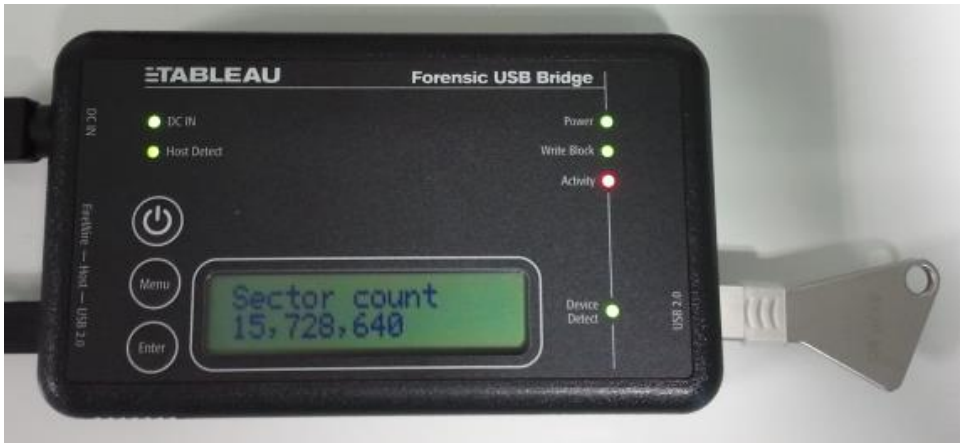
증거 획득 장비

Tableau Set (USB)

HOST

Write Blocker

SOURCE



증거 획득 장비

PRO'S Electronics Master Kit – Briefcase Style

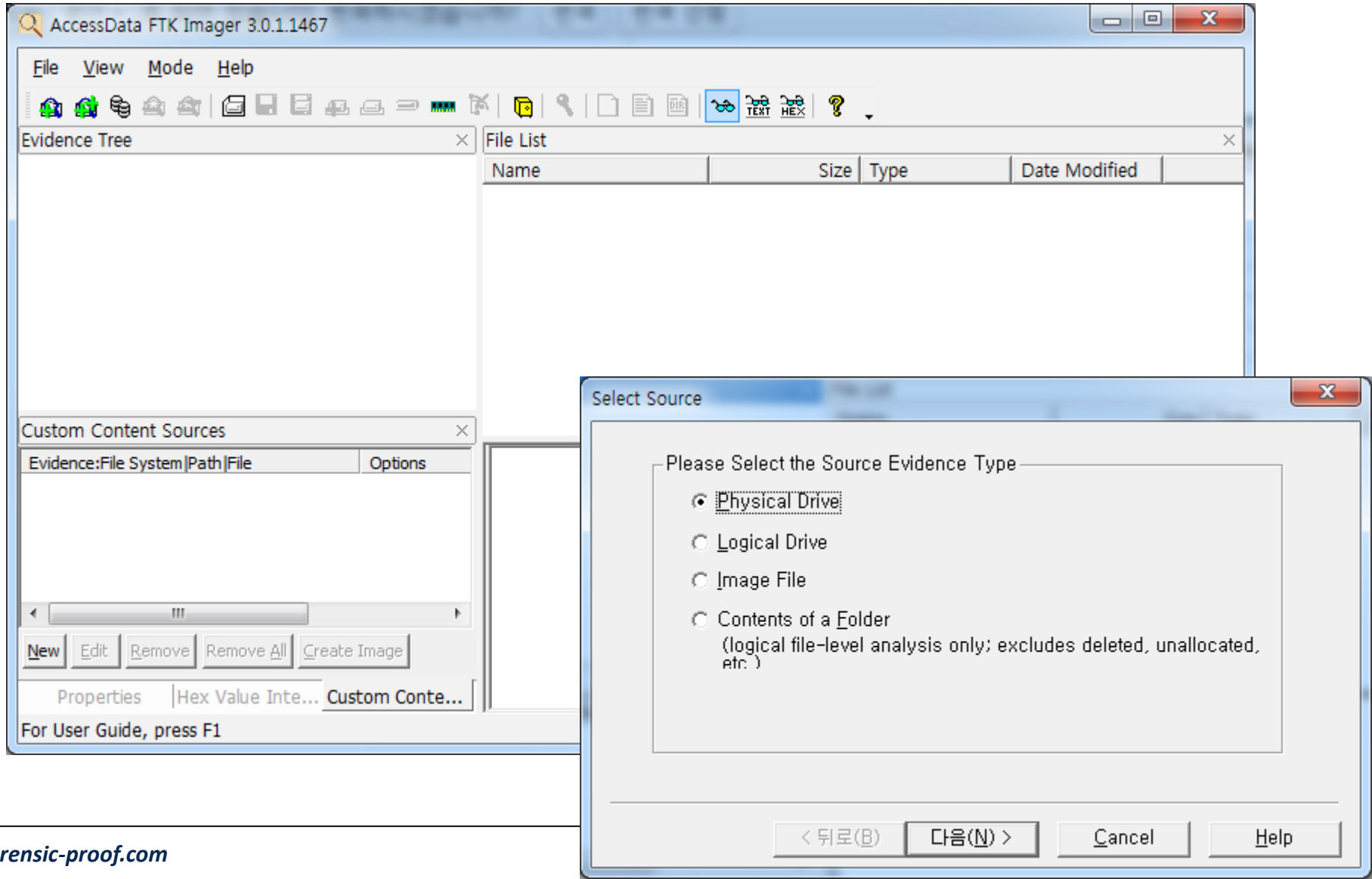
- **₩ 700,000 (2EA)** – US $ 240

증거 획득 도구

Security is a people problem…

증거 획득 도구

FTK Imager



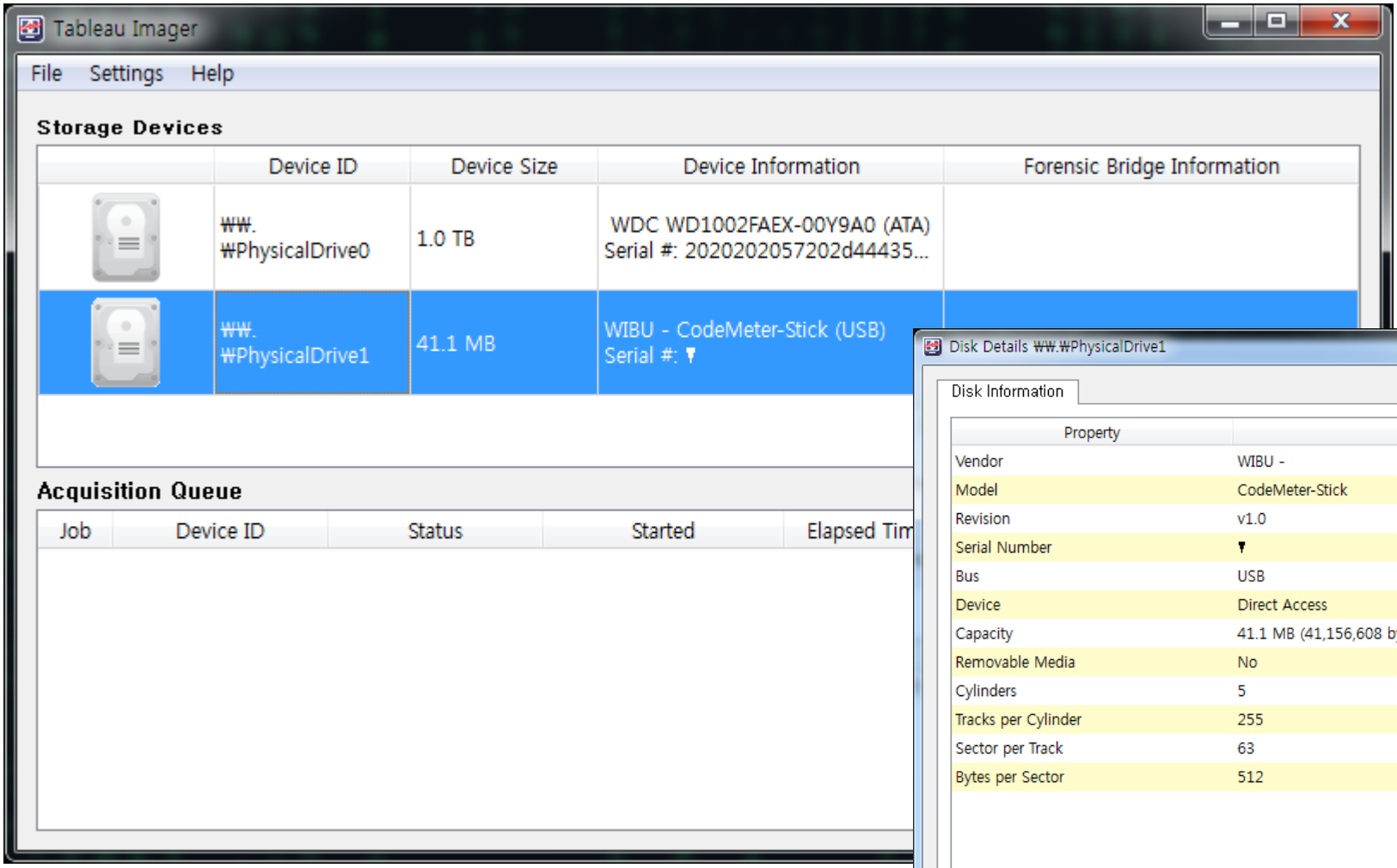
증거 획득 도구

FTK Imager

- **지원 파일 형식**
  - RAW/DD, SMART, EnCase E01, AFF
- **파일 크기**
  - User-defined
- **AD Encryption**
  - SHA-512
  - AES 128, 192, 256
  - Key materials (for AES) : pass phrases, raw key files, certificate

증거 획득 도구

Tableau Imager (with Tableau write-blockers)



증거 획득 도구

Tableau Imager (with Tableau write-blockers)

- **지원 파일 형식**
  - RAW/DD, EnCase E01, DMG
- **파일 크기**
  - 700MB, 1G, 2G, 4G, Unlimited
- **에러 복구**
  - Quick Recovery, Complete Recovery
- **해쉬 지원**
  - MD5, SHA1, MD5+SHA1

증거 획득 도구

그밖에 도구

- **EnCase (Linen)**
- **DD (FAU DD)**

실험

- **8GB USB ➔ E01 Imaging (no compression)**

	Host Directly	With Tableau(T8R2) Forensic USB Bridge (Write Blocker)
Tableau Imager	-	**9min 14sec**
FTK Imager	13min 28sec	17min 55sec
EnCase 6.18	9min 59sec	12min 14sec

저장매체 인터페이스 속도

Interface	bps(bit/s)	Bps(Byte/s)	Practical
SATA1(SATA150)	1.5 Gbps	187.5 MBps	-
SATA2(SATA300)	3.0 Gbps	375 MBps	100 MBps (SSD 250 MBps)
SATA3(SATA600)	6.0 Gbps	750 MBps	250 MBps (SSD 520 MBps)
USB1.0	1.5 Mbps	187.5 KBps	-
USB1.1	12 Mbps	1.5 MBps	-
USB2.0	480 Mbps	60 MBps	30 MBps
USB3.0	5 Gbps	625 MBps	120 MBps
FireWire 400	400 Mbps	50 MBps	-
FireWire 800	800 Mbps	100 MBps	-
Thunderbolt	10 Gbps	1.25 GBps	-

질문 및 답변