보안실습 6

[첫번째] FTK Imager 및 설치

- FTK Imager는 이미징을 위한 전문화된 도구
- 또한 파일 복원 및 무결성 검증 등 다양한 기능 제공
- 디지털 증거 분석을 위해 사본(이미지)을 생성하여 법적 증거 제출 시 사용

[정리] 이미징이란

- 컴퓨터 하드디스크의 각종 정보를 압축된 파일 또는 이미지로 변경해 사용자가 원하는 다른 하드디스크와 PC, 노트북 PC 등에 복사하고 저장하는 것

- 하드디스크의 각종 데이터뿐 아니라 부팅 시스템까지 포함해 모든 기록을 통째로 하드디스크에 복사, 저장하므로 하나의 하드디스크에 문제가 발생하더라도 정보를 보존할 수 있음

- 특히 하드디스크를 포맷하고 프로그램을 다시 설치해야 할 때 유용

보안실습 6

[두번째] FTK Imager 파악 및 이미지 생성

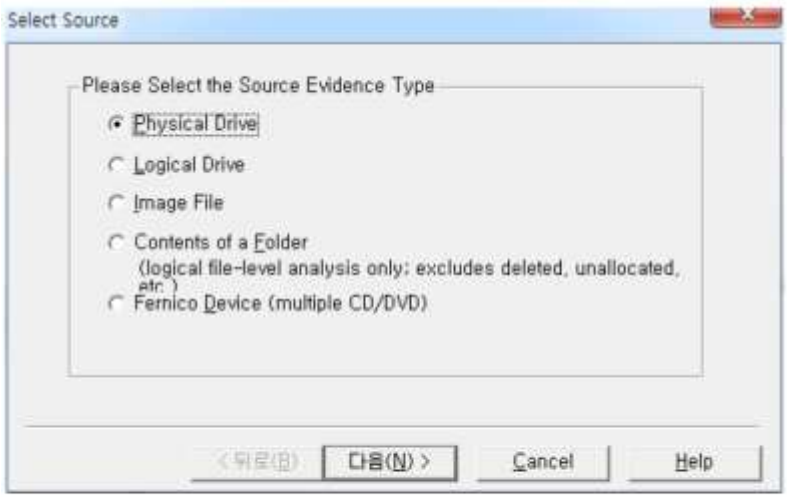

그림 2. 이미지를 생성할 위치

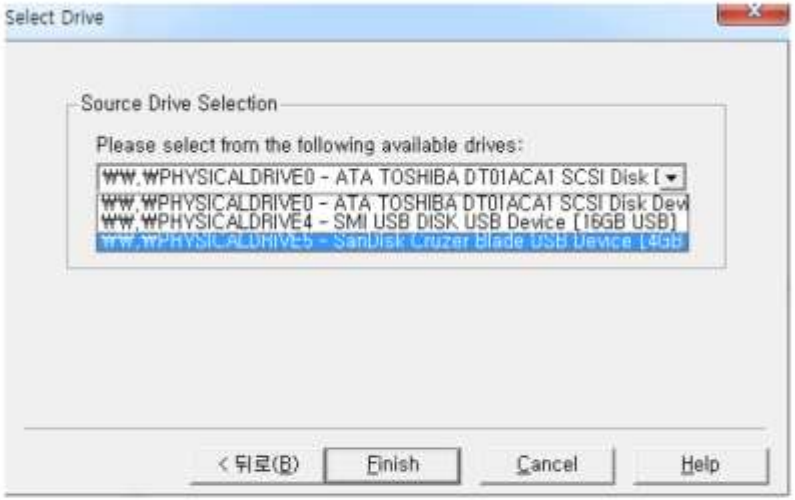

그림 3. 이미지 대상

- USB를 이용한 이미지 생성이므로 Physical Drive 선택

-포렌식 법적 증거 자료로 사용될 Drive 선택
-복구할 Drive 선택

보안실습 6

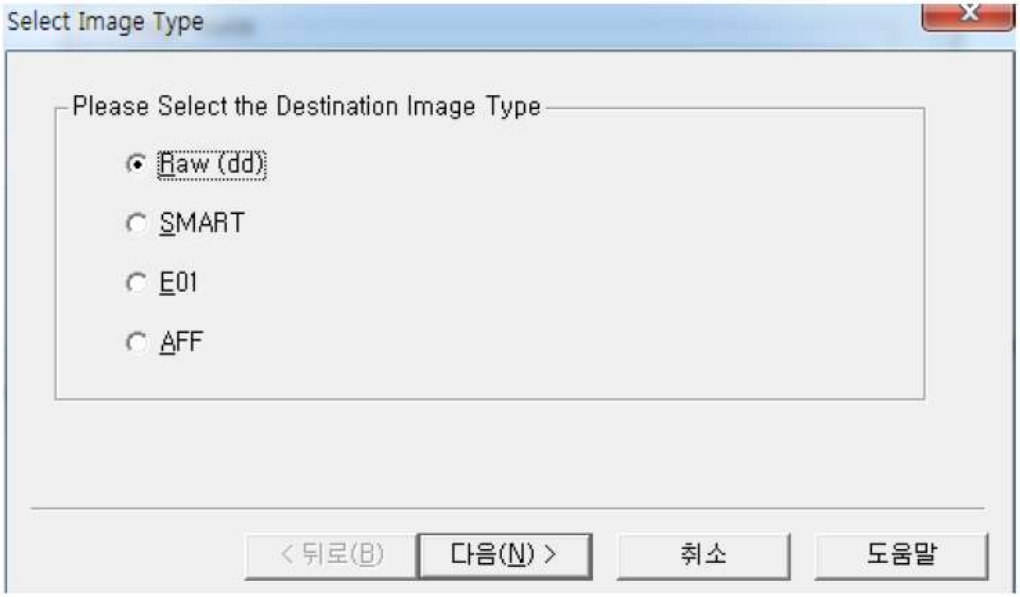

그림 4. 이미지 유형

- 저장매체 이미징은 원본 저장매체의 모든 물리적인 섹터를 파일 형태로 만드는 방식
- 초기에는 Disk Dump 방식을 많이 사용
- 최근에는 이미지 파일의 손상을 보호하기 위해 별도의 포렌식 이미지 포맷 사용

보안실습 6

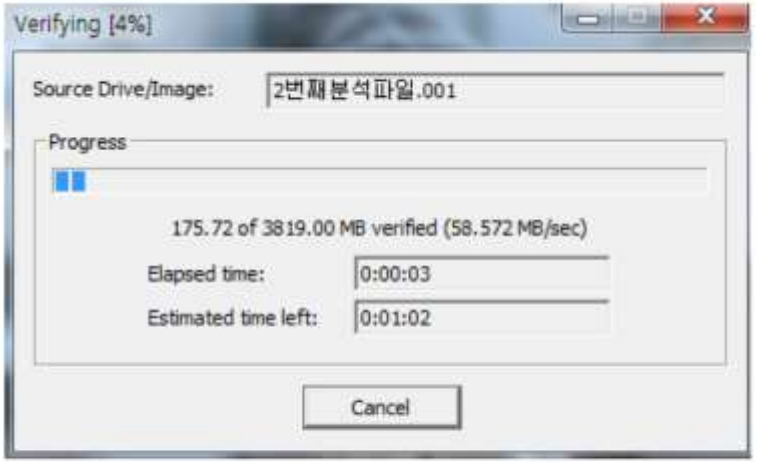

그림 5. Verifying(검증) 수행

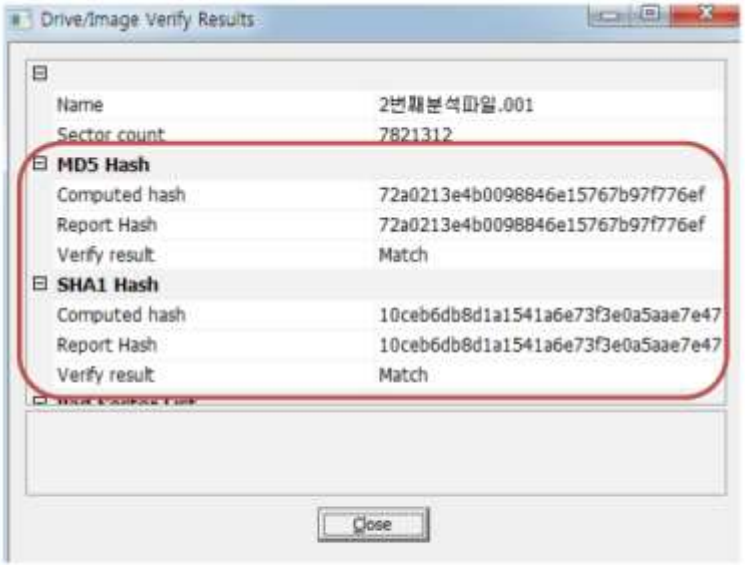

그림 6. 무결성 검증

- 검증이 수행되면서 Elapsed time(경과 시간) 과 Estimated time left(잔여 시간), 진행상황 파일 크기 등을 제공
- 원본 데이터와 이미지(사본)파일 간의 해쉬 값 일치 여부로 무결성을 검증