✅ [WHS-3기][디지털포렌식 기초]-33반-김신아(9502)

🦹 범죄 시나리오 작성

범죄 배경

- 화이트은행에 다니던 A씨는 퇴직 후 부동산 개발업체를 설립하였습니다
- A씨는 은행에 재직할 당시 친분이 있던 동료 B씨와 친분을 유지하며, 내부 정보를 공유받았습니다.

범행 수법

- A씨는 B씨의 도움을 받아 허위의 부동산 담보자료를 제출하고, 차명으로 여러 건의 대출을 신청합니다.
- B씨는 내부 심사 과정을 조작하여 대출을 승인하게됩니다.
- 이러한 방식으로 A씨는 총 50건, 약 900억 원의 부당대출을 실행합니다.

은폐 시도

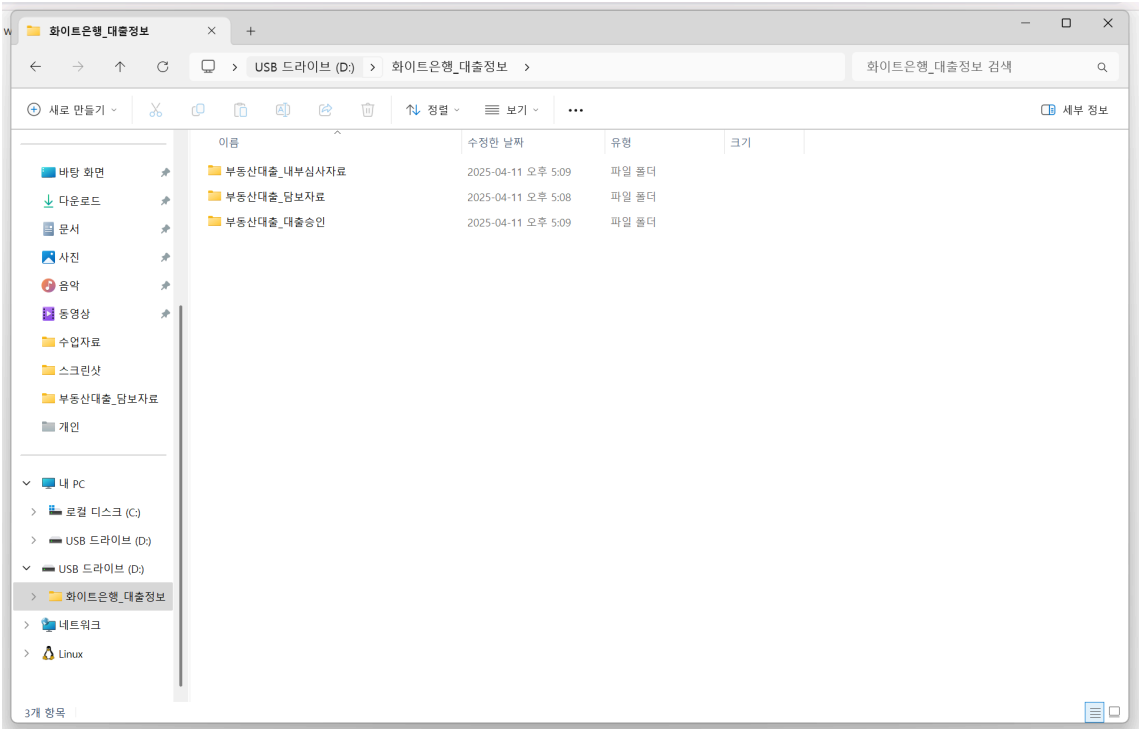
- 은행 내부 감사팀이 이상 징후를 발견하자, B씨는 관련 자료를 삭제 후, A씨와의 연관성을 숨기기 위해 보고서를 조작하게 됩니다.

참고 사례 : https://news.kbs.co.kr/news/pc/view/view.do?ncd=8209732&ref=A

분석 항목

- USB안 삭제된 파일 내용
- 부당대출 고객 정보 확인

— 범죄 은폐 실습 —

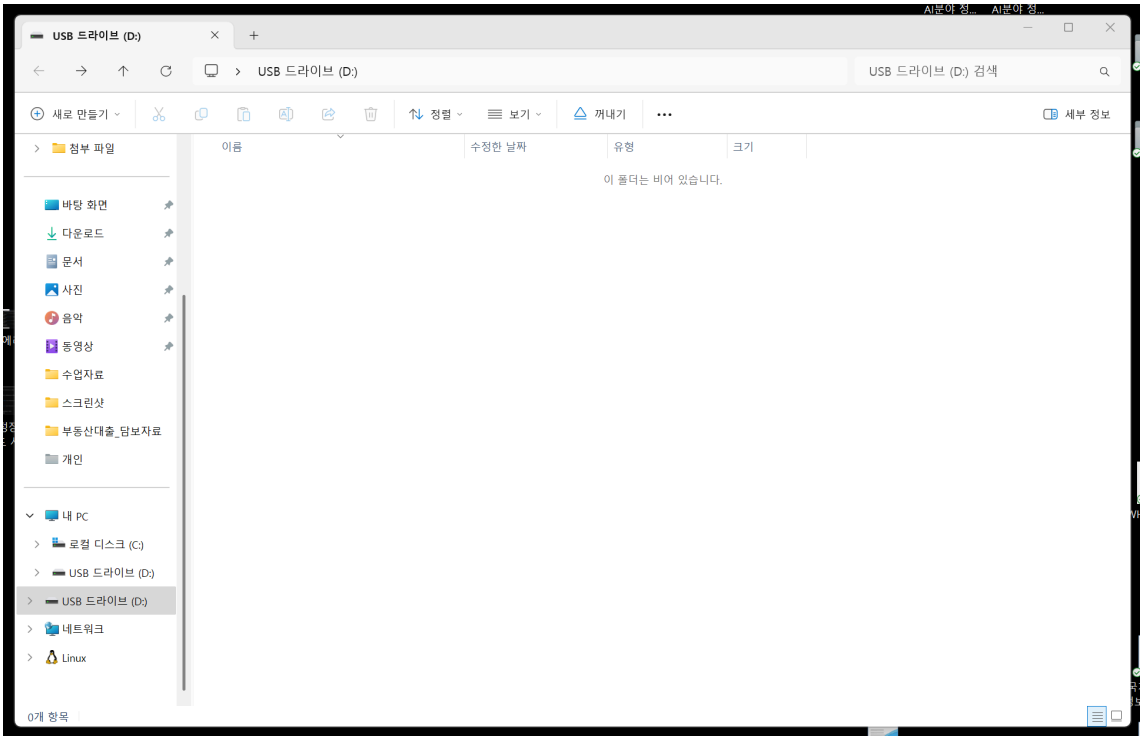


1. USB안에 파일 생성

각 파일 안에

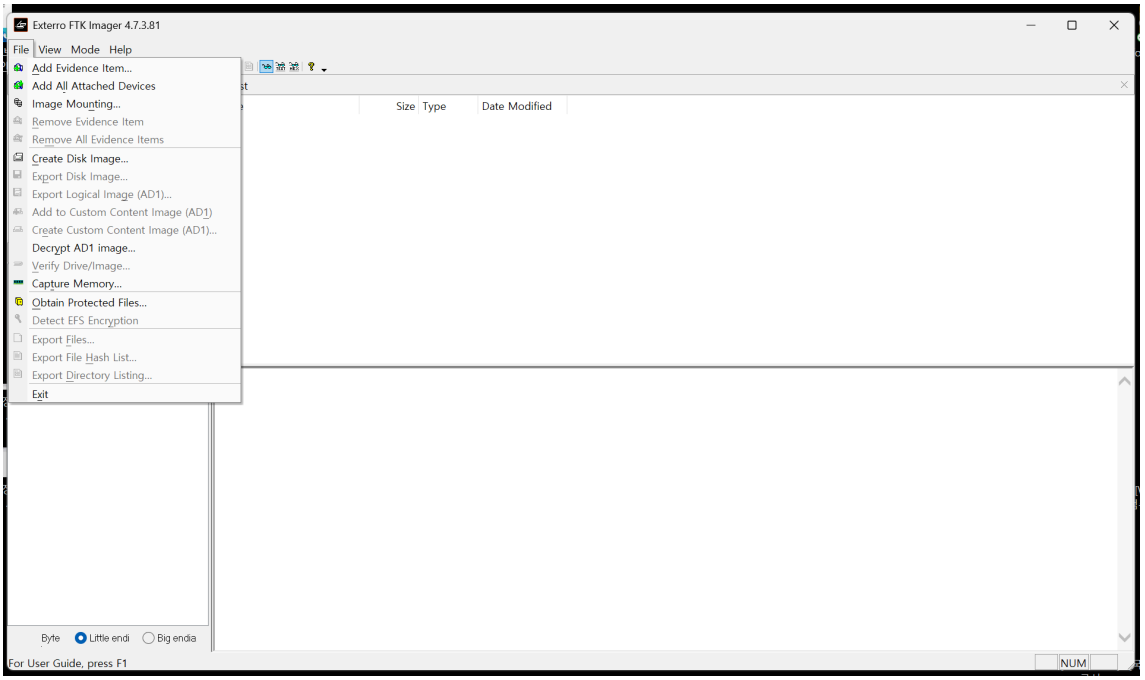
> 고객명: 차명 김OO
>
> 대출번호: 2024-0111
>
> 담보정보: 서울시 강남구 XX동 허위 건물
>
> 대출금액: 21억
>
> 담당자: B씨

고객 정보 입력



2. 범죄 행위를 은폐하기 위해 파일 삭제

— 삭제된 USB안의 내용 복구 실습 —

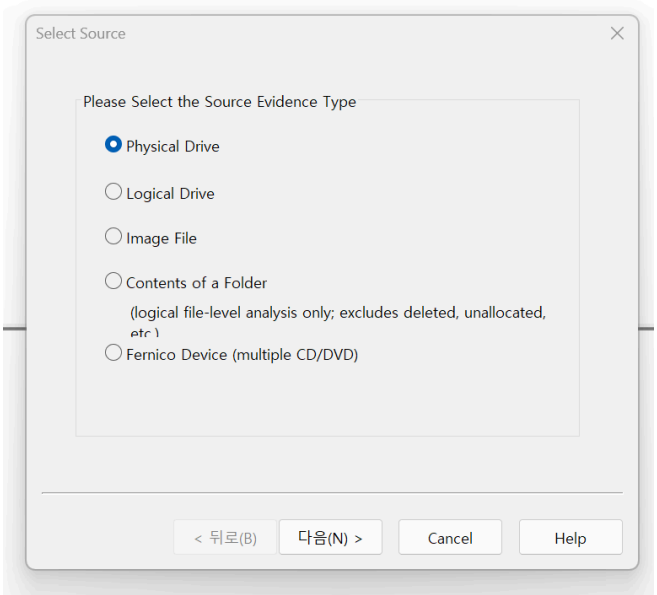


1. FTK를 활용해 복구 시도

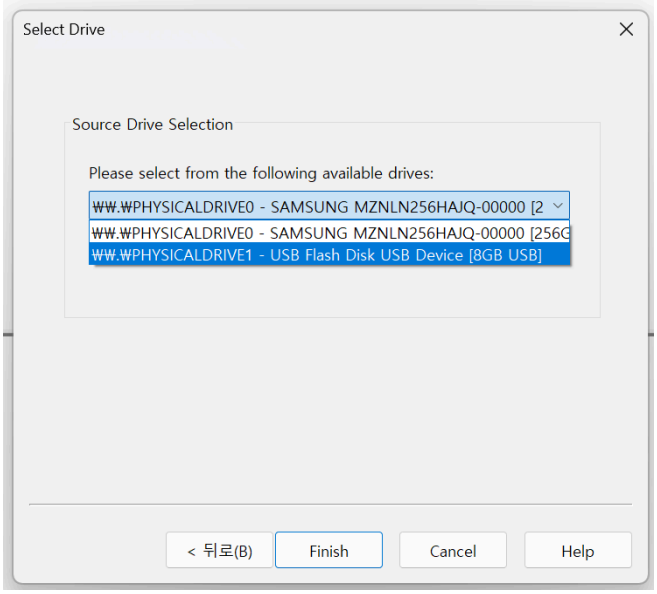
Create Disk Image 선택

- Create Disk Image란?

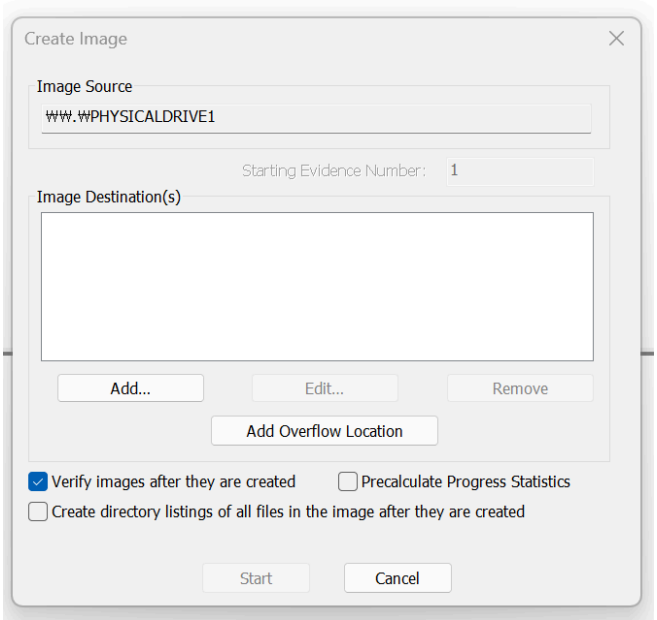
디스크 전체를 하나의 이미지 파일로 만들어 백업 또는 분석용으로 저장하는 것



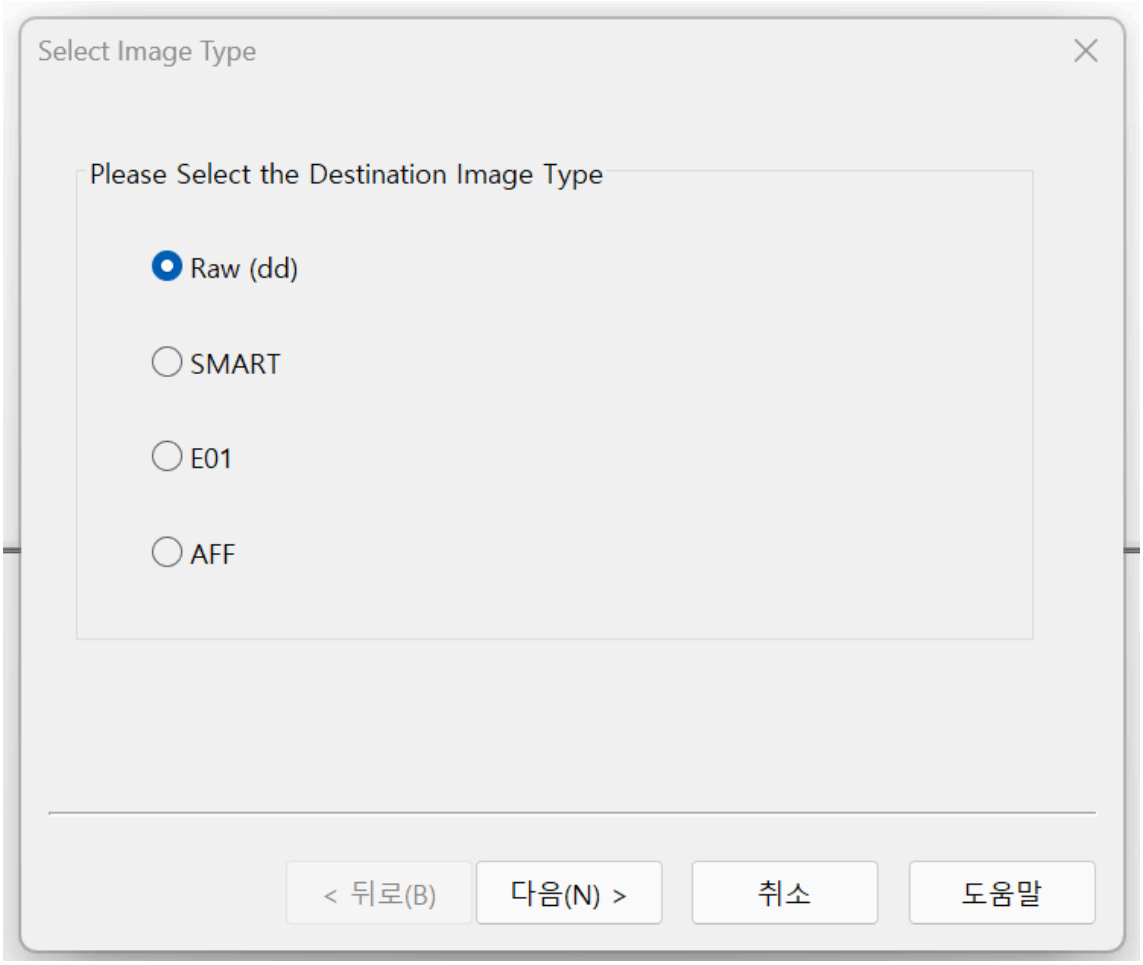
2. Physical Drive 선택



3. 복구할 USB선택



4. Add 선택



5. Raw 선택

이미지 형식

- Raw(dd)

확장자: `.dd` 또는 `.img`

설명: 디스크의 바이트 단위 복사. 가장 기본적인 형태의 이미지

장점: 호환성이 매우 높고 다양한 도구에서 사용 가능

단점: 압축이 안 되어 용량이 큼, 메타데이터 없음

- SMART

확장자: `.s01`, `.s02` ,

설명: AccessData의 SMART 도구에서 사용되는 형식

장점: 세분화된 파일로 저장되어 일부 복구나 보관에 유리함

단점: 일부 툴에서만 호환 가능

- E01

확장자: `.E01`

설명: 법적 증거 수집에서 자주 쓰이는 포맷

장점: 압축 가능, 해시값, 사건 정보 등 메타데이터 포함

단점: 포렌식 도구에서만 열 수 있음. 조금 복잡함

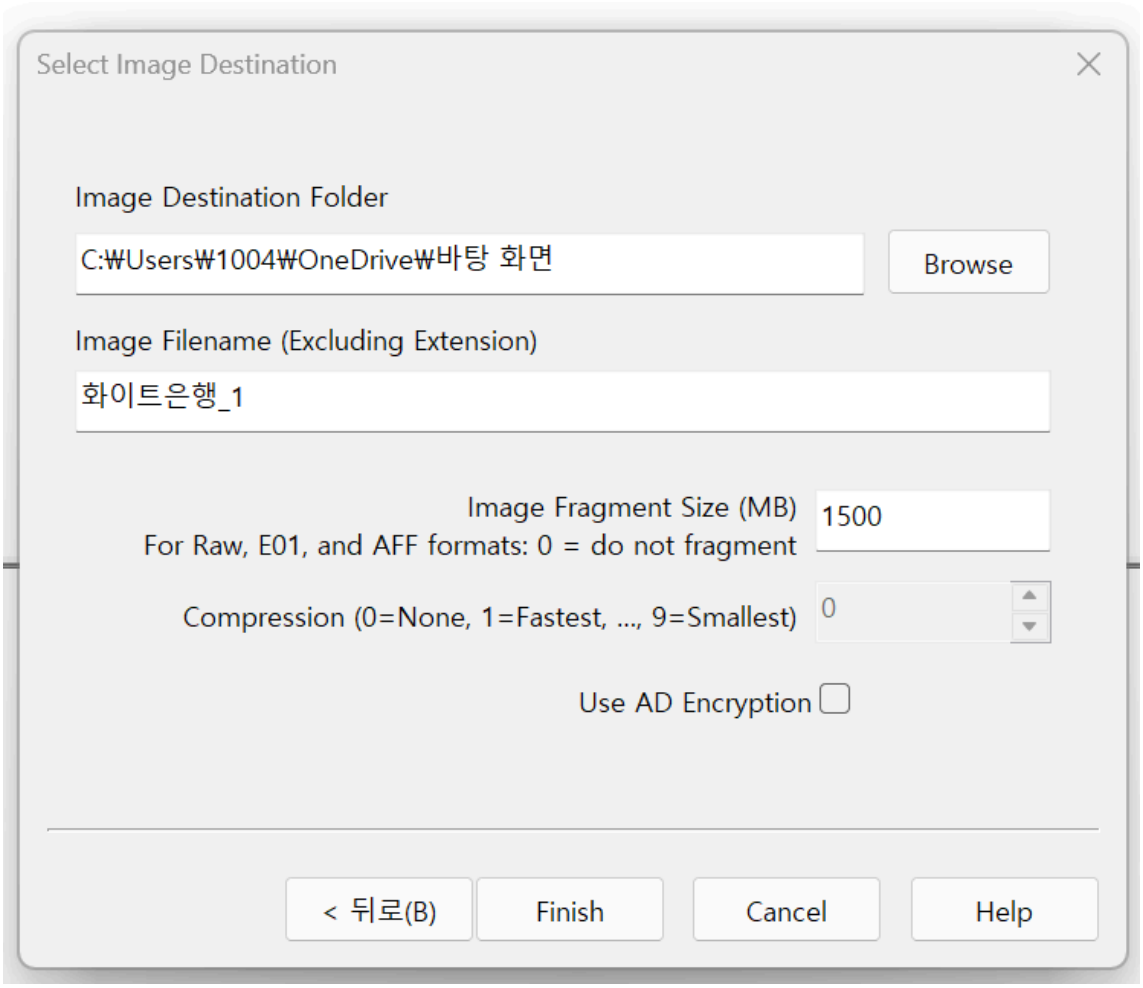
- AFF

확장자: `.aff`

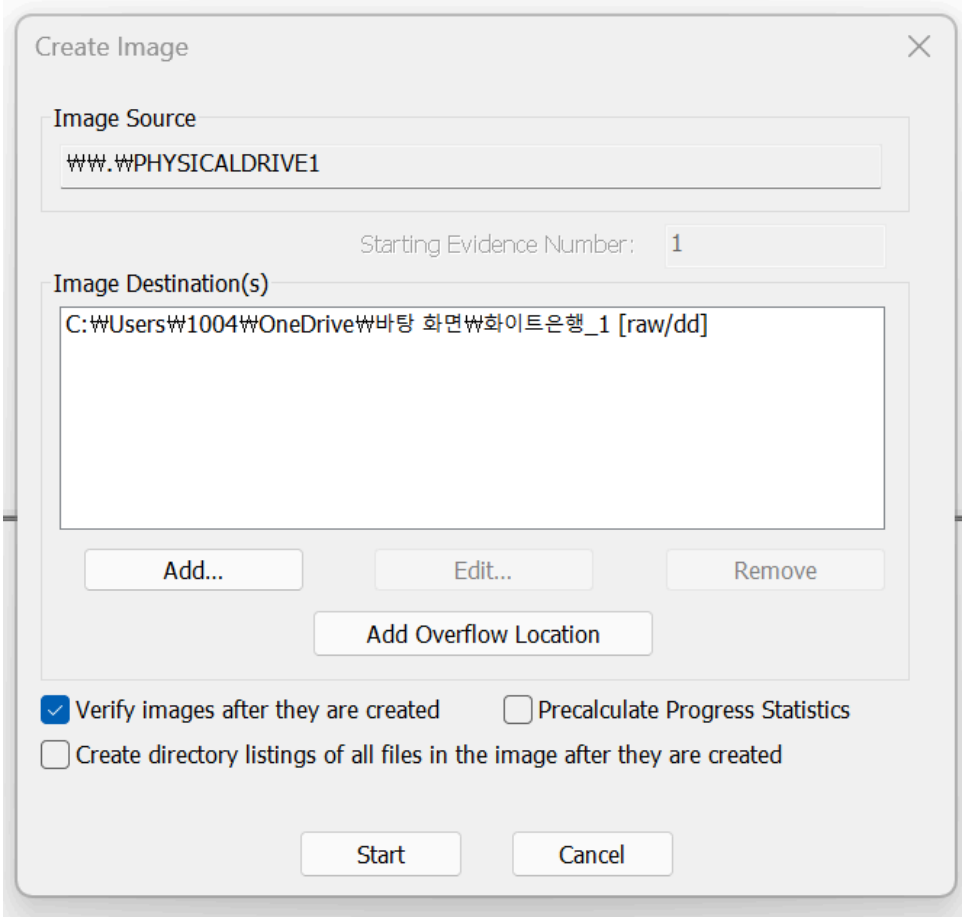
설명: Open-source 기반 포맷. 디지털 증거의 효율적 저장을 위해 설계됨

장점: 압축 가능, 메타데이터 저장 가능

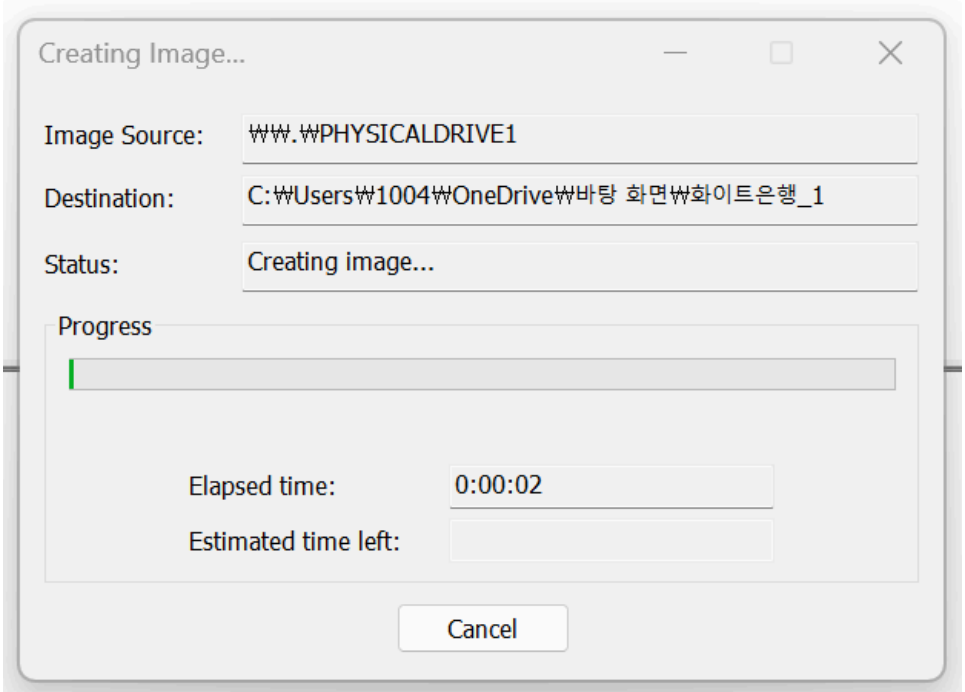
단점: 일부 툴에서만 호환

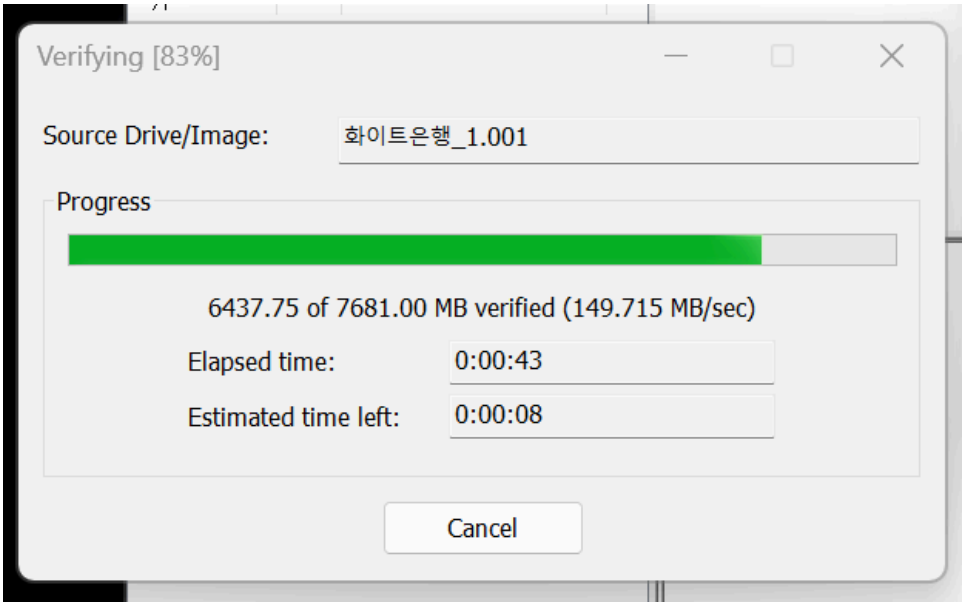


6. 이미징 저장 위치와 파일 이름 설정

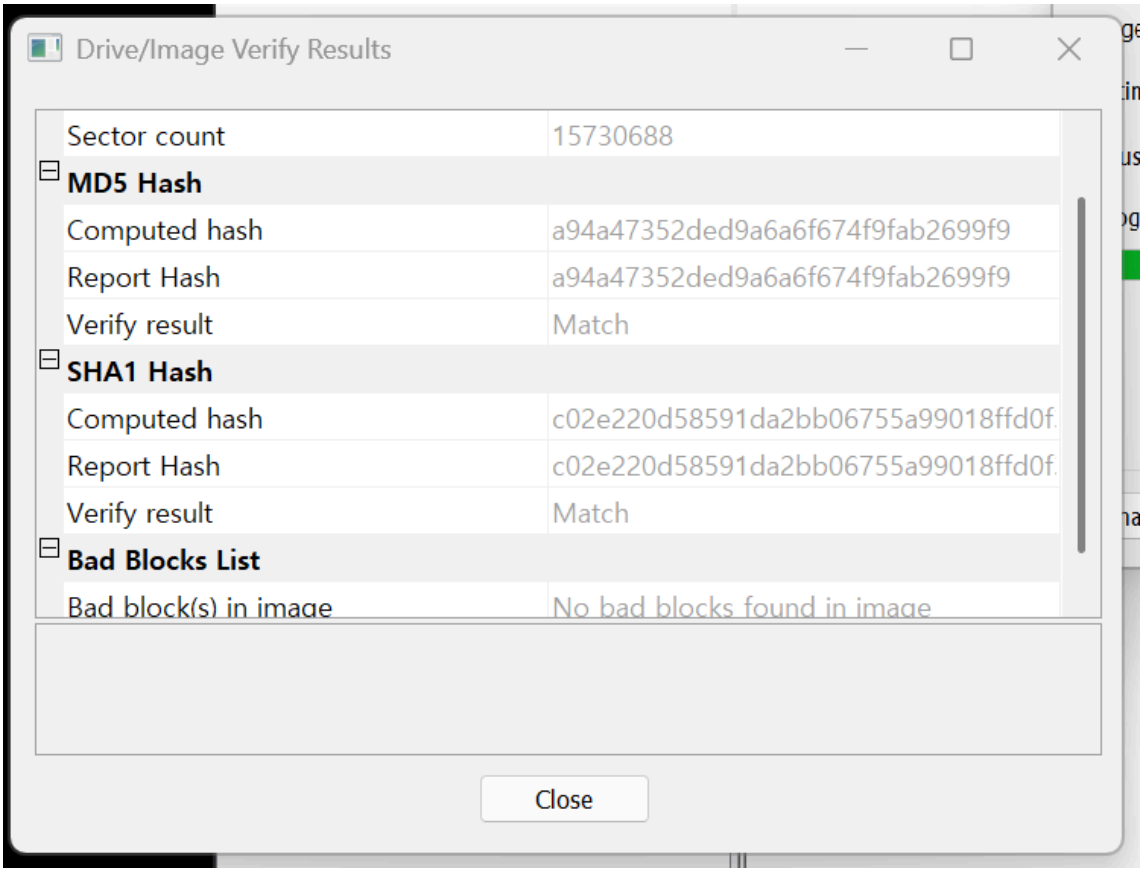


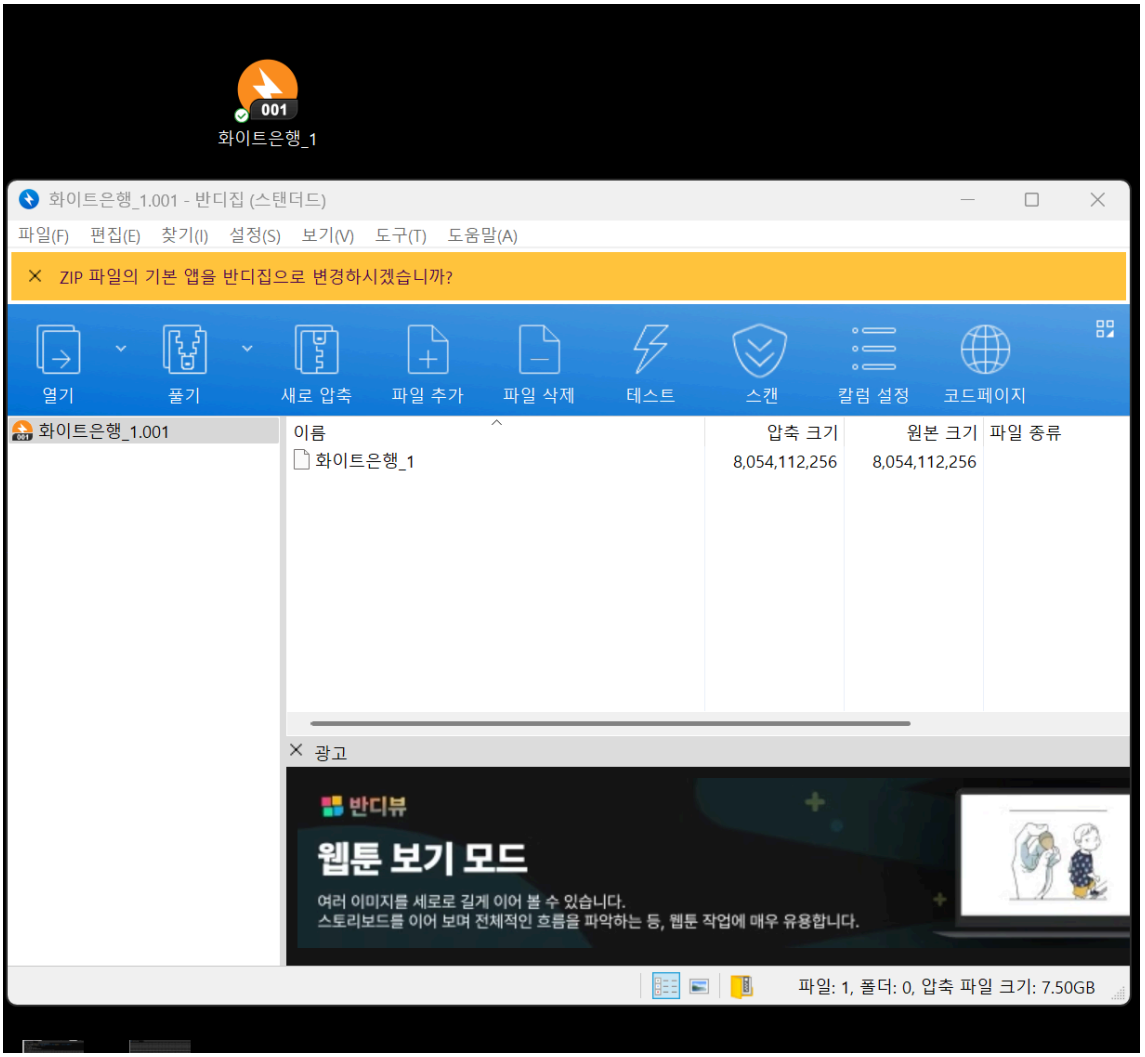
7. 모든 설정이 끝난 후 Start 클릭




Verifying [83%]
Source Drive/Image:
화이트은행_1.001
Progress
6437.75 of 7681.00 MB verified (149.715 MB/sec)
Elapsed time:
0:00:43
Estimated time left:
0:00:08
Cancel

8. 이미징 진행


Drive/Image Verify Results
Sector count
15730688
MD5 Hash
Computed hash
a94a47352ded9a6a6f674f9fab2699f9
Report Hash
a94a47352ded9a6a6f674f9fab2699f9
Verify result
Match
SHA1 Hash
Computed hash
c02e220d58591da2bb06755a99018ffd0f
Report Hash
c02e220d58591da2bb06755a99018ffd0f
Verify result
Match
Bad Blocks List
Bad block(s) in image
No bad blocks found in image
Close


001
화이트은행_1
화이트은행_1.001 - 반디집 (스탠더드)
파일(F) 편집(E) 찾기(I) 설정(S) 보기(V) 도구(T) 도움말(A)
ZIP 파일의 기본 앱을 반디집으로 변경하시겠습니까?
열기
풀기
새로 압축
파일 추가
파일 삭제
테스트
스캔
칼럼 설정
코드페이지
화이트은행_1.001
이름
압축 크기
원본 크기
파일 종류
화이트은행_1
8,054,112,256
8,054,112,256
광고
반디뷰
웹툰 보기 모드
여러 이미지를 세로로 길게 이어 볼 수 있습니다.
스토리보드를 이어 보며 전체적인 흐름을 파악하는 등, 웹툰 작업에 매우 유용합니다.
파일: 1, 폴더: 0, 압축 파일 크기: 7.50GB

9. 복구 된 파일 확인