dongguk UNIVERSITY

# 정보보호 개론 "10주차 강의"

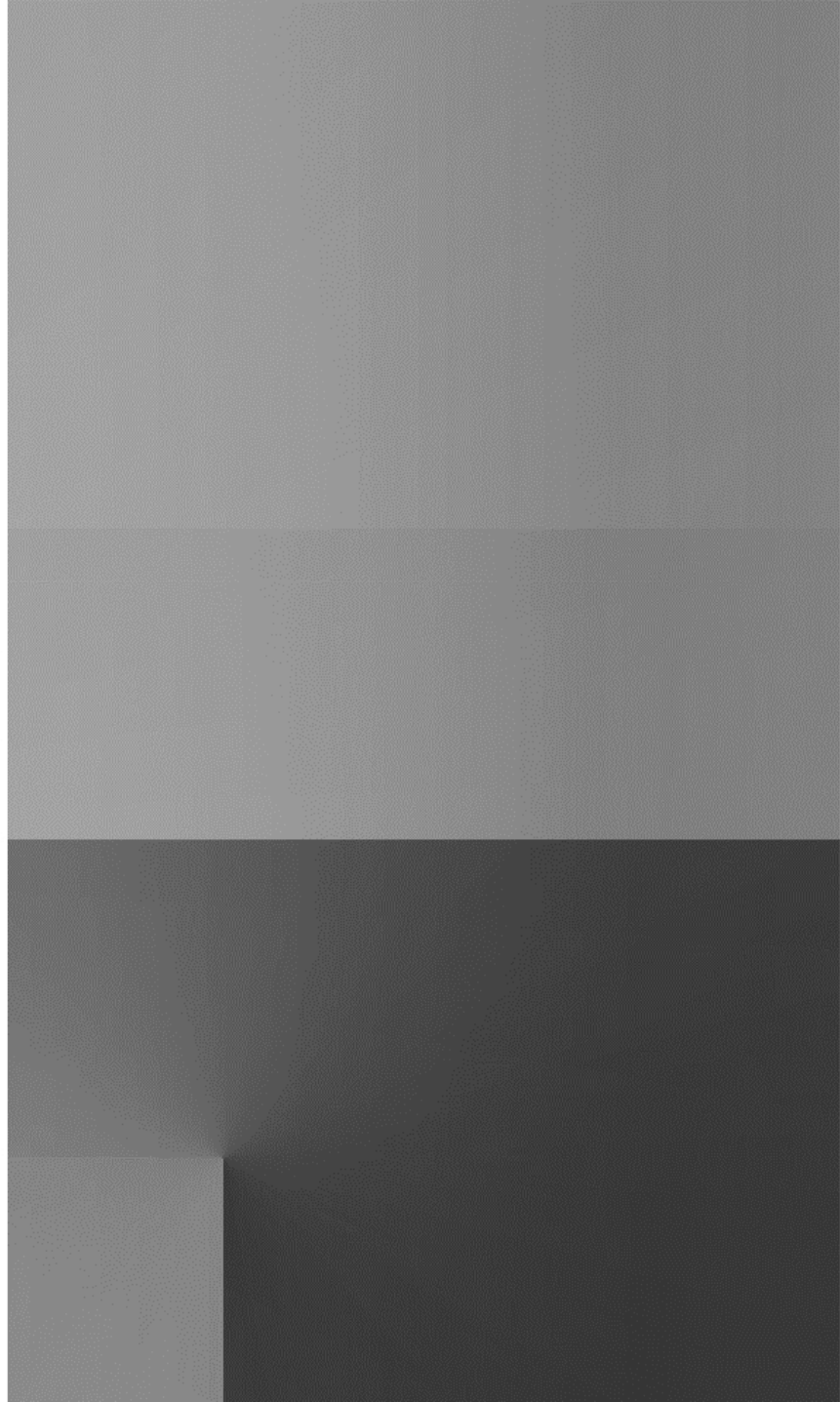
윤홍수

2025. 05. 08

# Table of Contents


I. **2025년 1학기 10주차 강의 계획**

- 과제 설명
- 인증시스템 : 인증수단
- 방화벽
- 데이터 복구 : FTK Imager

# 과제 설명(중요)

"이번 과제는 단순한 요약이 아니라,

여러분이 실제로 관심을 가지고 탐색해볼 수 있는 주제 선정

각 주제는 지금 우리가 배우는 '정보보호'가 어디에, 어떻게 적용되는지 직접 확인해볼 수 있는 기회"

**과제 주제 : 3개중 택 1**

**제출 방식 : PPT 혹은 PDF**

**마감일 : ~ 5/26(월) 23:59분까지**

**13주차 : 각자 발표 예정 (5 ~ 10분 할당)**

**제출 방법 : eclass 업로드 (eclass 시스템에 에러가 있을 경우, 별도 제출 이메일 공유 예정)**

# 과제 설명(중요)

**과제 주제**

**1. 내가 사용하는 서비스는 어떤 보안 기술이 적용되어 있는가? (예: 카카오톡, 네이버, 쿠팡 등)**

- 이 서비스에서 어떤 보안 기술이 사용되고 있는지 조사
- 나의 개인 정보는 어떻게 보호되고 있을까
- 기타…..

**2. 국내외 해킹 사건 중 하나 선택 (예 : 최근 SKT, LGU+)**

- 어떤 공격이었는가?
- 어떤 취약점이 있었는가?
- 피해는 어땠고, 이후 어떤 대응이 있었는가?
- 기타…..

# 과제 설명(중요)

**과제 주제**

**3. AI 시대에 새롭게 떠오르는 보안 위협과 대응 기술**

- AI가 만드는 새로운 위협 사례 (예: 딥페이크, 자동화된 피싱, AI 해킹 도구 등)
- 이에 대응하는 최신 보안 기술 또는 제도 조사
- 미래의 보안 전문가로서 내가 생각하는 대응 전략 제안
- 기타 …..

# 인증 시스템

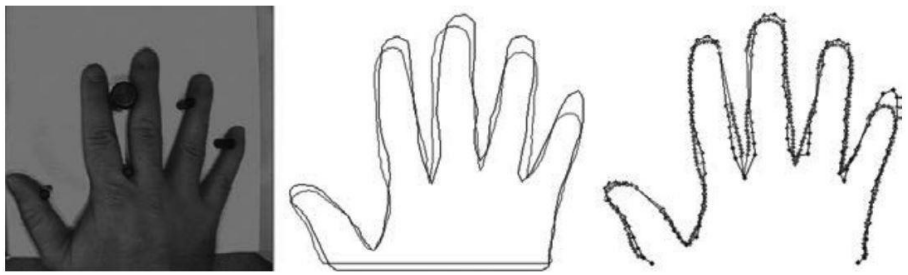
## 인증 수단

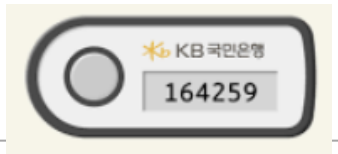
- 사용자가 나라는 것을 증명하는 방법
- 컴퓨터나 시스템이 **사용가 누구인지 확인하기 위해 사용하는 신분 확인 도구**

- 인증 수단의 3가지 방법
  - 알고 있는 것
  - 가지고 있는 것
  - 자신의 정보

# 인증 시스템

- 인증 수단의 3가지 방법
  - 알고 있는 것
    - 아이디/비밀번호, PIN, 보안 질문 등
  - 가지고 있는 것
    - OTP(One-Time Password) 토큰, 스마트폰, 인증서
  - 자신의 정보
    - 지문, 얼굴, 홍채, 손 모양, 목소리 등

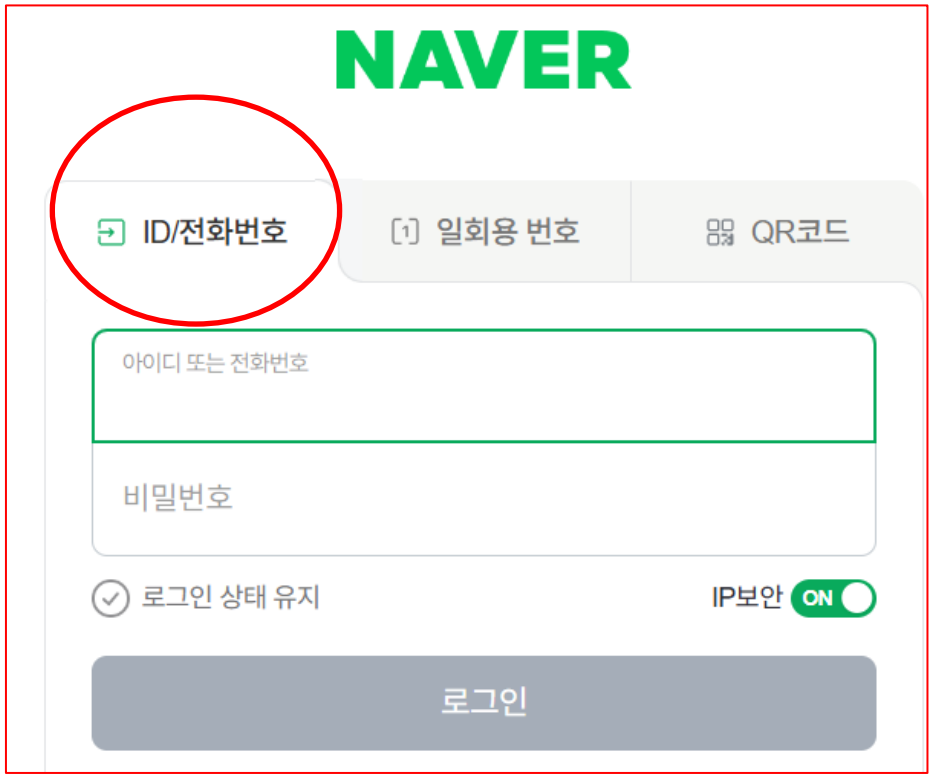




# 인증 시스템

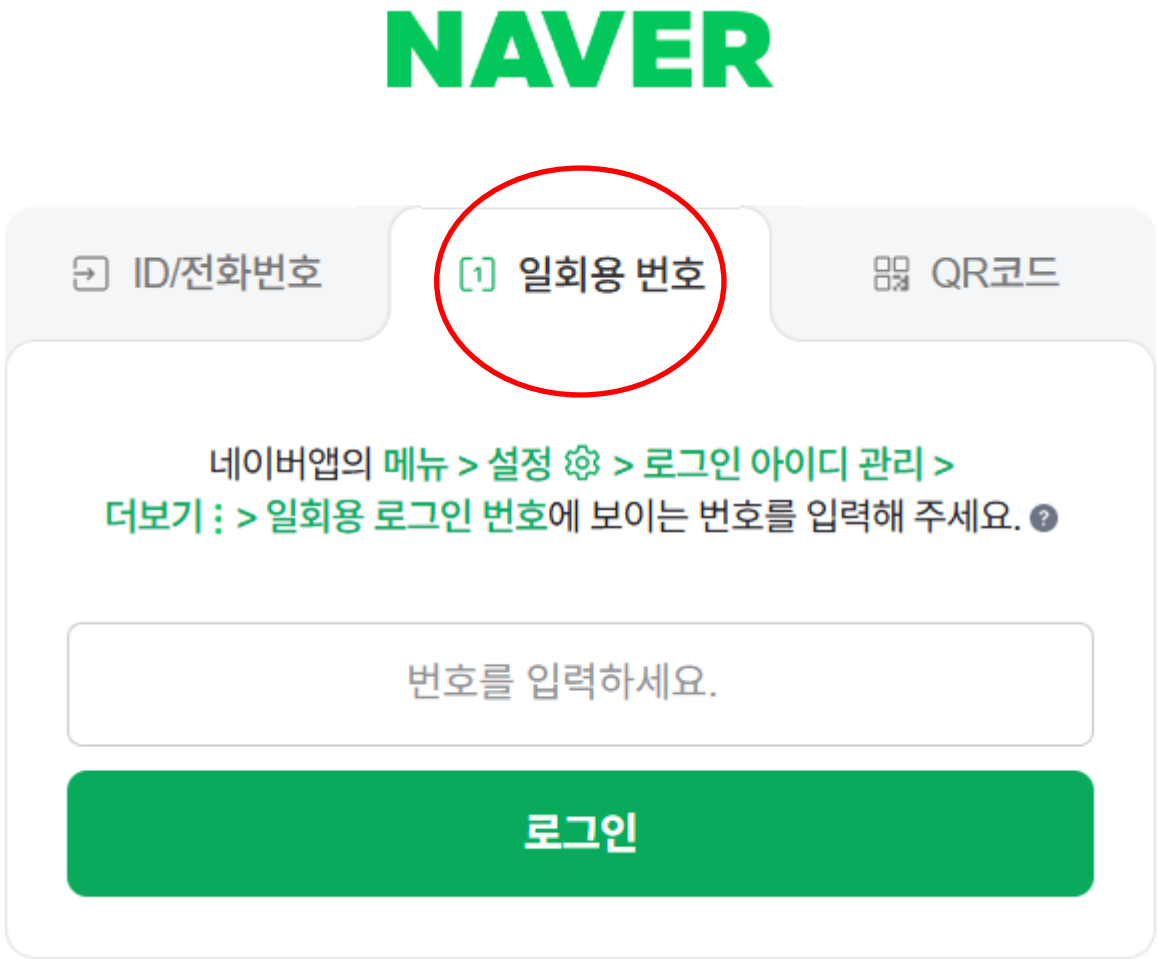
## 알고 있는 것

- 대표 예 : 아이디 + 비밀번호
  - 가장 널리 쓰이는 인증 수단
  - **장점 : 비용이 없고 설정이 쉽다**
  - **단점 : 쉽게 추측되거나 유출될 수 있다**
- 보안 팁
  - 8자 이상, 숫자+영문+특수문자 조합 사용
  - 사이트마다 다른 비밀번호 사용
  - 정기적으로 변경하기



# 인증 시스템

- **알고 있는 것**
  - 대표 예 : 일회용 번호(변화-1)
    - 일회용으로 생성되는 숫자 조합을 PC 화면에
    - 입력하여 로그인하는 방식
    - 스마트 폰의 앱, 로그인 관리에서 번호 체크
    - **장점 : 보안성 강화, 간편함**
    - **기타 : 스마트폰 보유 및 앱 설치 되어 있어야 함**

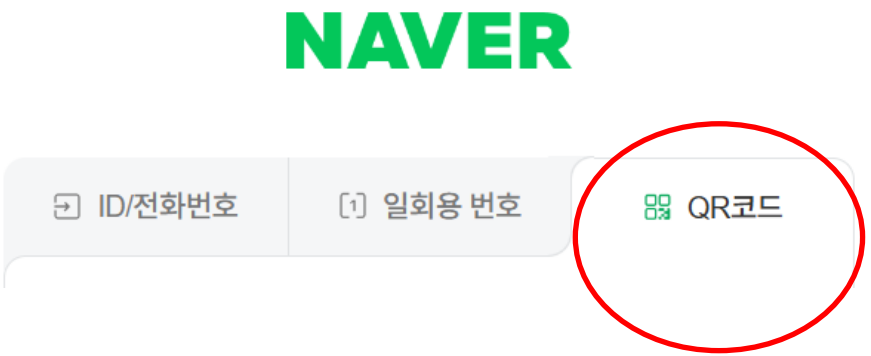


# 인증 시스템

## 알고 있는 것

- 대표 예 : QR 코드 (변화-2)
  - 일회용으로 생성되는 숫자 QR 코드 입력 + 숫자 입력
  - 스마트 렌즈로 QR코드를 입력하고, 인식이 되면

    보안 숫자를 선택을 하여, 로그인 한다
  - **장점 : 보안성 강화, 매우 간편함**
  - **기타 : 스마트폰 보유 및 앱 설치 되어 있어야 함**




QR 코드

# 인증 시스템

- **가지고 있는 것 : 소지 기반 인증**
  - OTP 토큰: 시간 기반으로 숫자가 계속 바뀜 (대부분 30초 간격으로 변경 됨)
  - 스마트폰 인증: 문자 인증, 카카오페이 인증
  - 공동 인증서: 공공기관이나 은행에서 사용
  - 특징
    - 이중 인증으로 많이 사용됨
    - 기기 분실 시 대체 어려움

# 인증 시스템

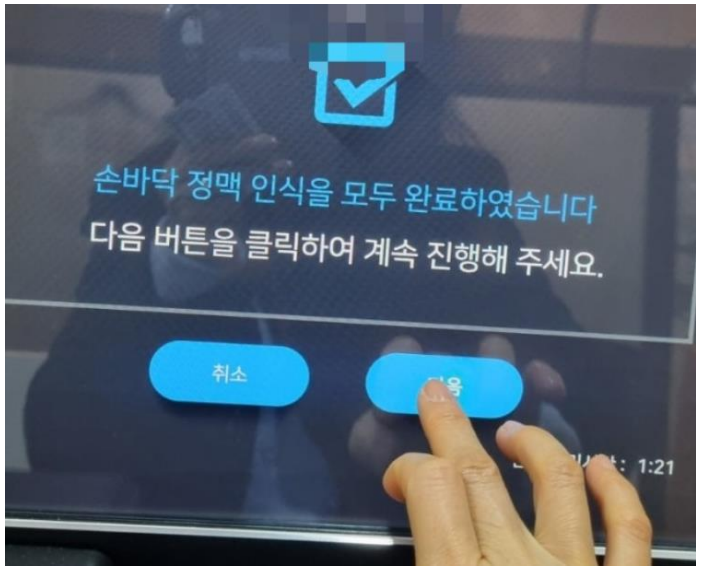
## 자신의 정보 : 생체 정보

- 지문 인식
  - **장점: 간편하고 빠르며 스마트폰에 흔히 탑재**
  - **단점: 손에 상처나 땀 등으로 인식률 저하 가능**
- 얼굴 인식
  - **스마트폰의 페이스ID, 카메라로 얼굴 비교**
  - **장점: 비접촉, 빠른 인증**
  - **단점: 마스크나 조명에 따라 인식 실패 가능**
- 홍채, 음성(ok 구글, 지니, 알렉사, 시리), 정맥
  - **고급 생체 인증 방식**
  - **병원, 군사 보안 등에서 사용**
  - **비싸고 전문 장비 필요하지만 보안성 우수**
- 손 모양
  - 손가락 길이, 두께로 인증
  - 장점: 빠르고 간편
  - **단점: 유사한 손 모양이면 오류, 위조 가능성 있음**

# 인증 시스템

## ▪ 자신의 정보 : 생체 정보

- 정맥 (바이오 정보)
  - 신속한 신원 확인: 국내선 보안 검색대에서 신분증 없이 통과 가능
  - 간편한 이용: 손바닥을 스캐너에 올려놓는 것만으로 인증 완료
  - 높은 보안성: 지문보다 위변조가 어려운 정맥 패턴을 활용



# 인증 시스템

## 타임 테이블

- 1960년대
  - 아이디 + 비밀번호
    - 배경 : 초창기 컴퓨터에서 사용자가 누구인지 구별하기 위해 도입
      - 초기 : 보안 인식 부족, 편의성, 기술적 한계????

- 1990년대
  - OTP
    - 배경 : 비밀번호 유출/중복 사용 문제를 해결하려고 도입
    - ? 우리 나라 ? 어떤 시스템? 언제 부터 도입 본격화 되었을까?

# 인증 시스템

## 타임 테이블

- 1990년대
  - OTP
    - 배경 : 비밀번호 유출/중복 사용 문제를 해결하려고 도입
    - ? 우리 나라 ? 어떤 시스템? 언제 부터 도입 본격화 되었을까?
      - 2005년 인터넷 뱅킹 보편화 시기
      - **외환은행 이용 고객의 계좌에서 5,000만원이 사라짐 (인터넷 뱅킹 시스템 불신, 충격)**
        - **악성 프로그램 유포 -> 피해자 감염 -> 정보 탈취 -> 로그인 우회 -> 자금 이체**
        - **보안 프로그램 설치 의무화**
        - **OTP 도입 활성화**
        - **공인 인증서 보안 강화**

# 인증 시스템

https://imnews.imbc.com/replay/2005/nwdesk/article/1924846_30781.html

입력 2005-06-03 | 수정 2005-06-03

# 인증 시스템

https://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0000260365

05.06.07 18:56 | 최종 업데이트 05.06.07 18:59

## 외환은행, 인터넷뱅킹 해킹피해 전액 보상

7일 보상위원회서 결정, 김아무개씨에 5000만원 지급

김영균 (gevara)

가+ 원고료로 응원하기 2 0 공유

사상 처음으로 인터넷뱅킹 해킹 피해를 당한 외환은행이 또 다른 피해자인 김아무개(42)씨의 피해 금액 5000만원을 전액 보상키로 결정했다. 외환은행은 7일 오후 보상위원회를 통해 이같이 결정했다고 밝혔다.

애초 외환은행은 해킹 피해자인 김씨에 대한 보상이나 배상책임이 없다는 입장이었다. 외환은행은 지난 3일 경찰 조사결과 발표 직후 "은행의 귀책사유가 드러나지 않은 이상 약관에 따라 은행이 책임져야 할 부분은 없다"고 밝힌 바 있다.

하지만 7일 외환은행은 김씨에 대한 전액 보상으로 입장을 선회했다. 이는 대내외적 이미지와 고객 관리 차원에서 내린 결정으로 보인다.

# 인증 시스템

- 타임 테이블
  - 2000년대 초
    - 공동 인증서 (구 공인인증서)
      - 배경 : 금융거래/정부 사이트에서 법적 본인 확인을 위해 도입
  - 2000년대 중반
    - 스마트폰 인증 (SMS, App 인증)
      - 배경 : OTP 불편함과 인증서 설치 어려움을 해결하려고 등장

# 인증 시스템

- 타임 테이블
  - 2010년대 초
    - 지문 인식
      - 배경 : 스마트폰 보급 → 간편하면서도 높은 보안 필요성 증가
  - 2010년대 중후반
    - 얼굴 인식
      - 배경 : 비접촉, 빠른 인증 수단 요구 증가

# 인증 시스템

- 타임 테이블
  - 2010년대 후반
    - 홍채 인식
      - 배경 : 높은 보안성과 위조 방지 필요성에서 발전
  - 2010년대 후반
    - 음성 인식
      - 배경 : 비접촉, 음성 기반 스마트 디바이스 증가에 따라 등장
  - 2020년대
    - 정맥 인식
      - 배경 : 지문/얼굴 위조 가능성을 극복하려는 시도

# 인증 시스템

- 지문 인식

1. 지문 스캔
   - 사용자가 지문 인식기에 손가락을 올린다
   - 지문 센서가 손끝의 골무늬(능선과 골짜기 패턴)를 스캔

2. 이미지 변환
   - 스캔된 지문 이미지를 디지털 정보로 변환

3. 특징 추출
   - 지문 속에서 분기점, 끝점, 교차점 등 고유한 특징을 찾아냄
   - 예: 어떤 위치에 몇 개의 갈라지는 무늬가 있는지 등.

# 인증 시스템

- 지문 인식

4. 데이터 비교

  - 등록된 지문 정보와 스캔된 정보의 특징을 비교

5. 인증 성공 여부 판단

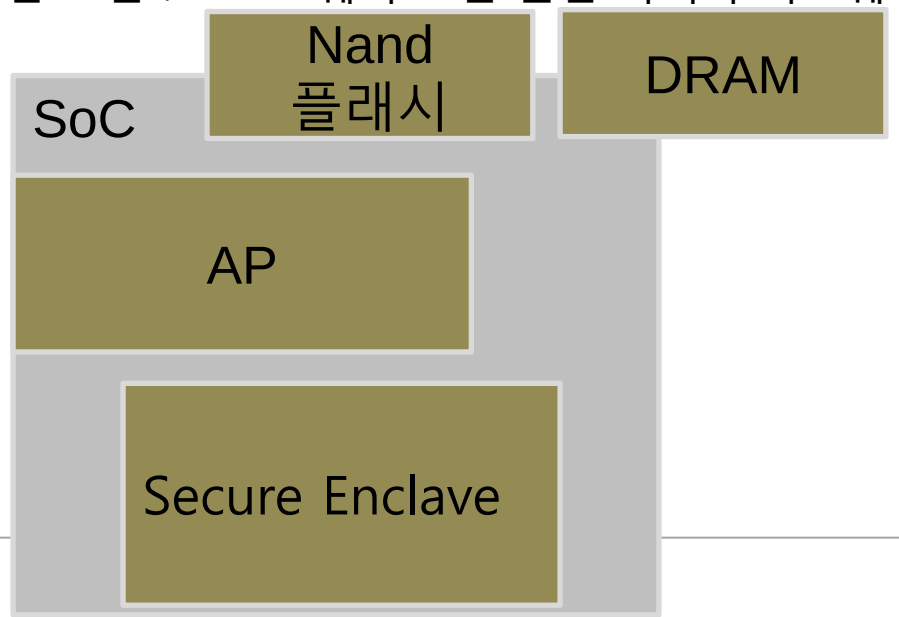
  - 비교 결과가 일정 기준 이상 일치하면 본인 인증 성공, 그렇지 않으면 실패
  - ? 지문데이터? 어디에? 저장이 될까요? 안전 할까요?

# 인증 시스템

- 지문 인식
  - 지문 인식 데이터는 어디에 저장이 될까요?
    - 스마트폰에서는 지문 정보가 클라우드나 외부 서버에 저장되지 않는다
    - 스마트폰 내부의 보안 영역(Secure Enclave 또는 TrustZone)에 저장
      - iPhone: Secure Enclave (독립적인 보안 칩)
      - 갤럭시 등 안드로이드 폰: TrustZone
      - 위 데이터는 암호화 되어, 오직 지문/페이스.. 인증용으로만 사용 됨

# 인증 시스템

- 지문 인식
  - iPhone: Secure Enclave (독립적인 보안 칩)
    - 완전한 독립 : IOS나 다른 APP들과 완전한 격리(보안)
    - 암호화 : 지문 센서에서 읽어 들인 데이터는 즉시 암호화
    - 안전한처리 : 지문인식 작업은 오직 Secure Enclave 내부에서만 안전하게 처리
    - 고유한 키 : 고유키를 가지고 있어서, 다른 아이폰에서는 복호화 할 수 없음
    - 하드웨어 기반 보안 : 소프트웨어 보안 뿐만 아니라 하드웨어 기반이어서 물리적 보안까지 갖춤



# 인증 시스템

- 얼굴 인식

1. 얼굴 감지
   - 카메라로 입력된 이미지나 영상에서 얼굴을 찾아 냄
   - 스마트폰 카메라로 사진을 찍을 때 얼굴에 네모난 박스가 표시
     이것이 얼굴 감지 기술이 작동하는 것

2. 얼굴 분석
   - **얼굴의 특징적인 부분들을 찾고 분석**
   - **주요 분석 대상은 눈, 코, 입, 턱 등의 위치와 윤곽, 그리고 각 부분 사이의 거리나 각도 등**

3. 얼굴 인식
   - 디지털 얼굴 서명을 스마트폰에 이미 저장된 사용자의 얼굴 데이터와 비교

4. 얼굴 인식 데이터 저장

# 방화벽

- 방화벽 개념
  - 방화벽(Firewall)은 허용된 통신만 통과시키고, 위험하거나 불필요한 통신은 차단하는 보안 시스템

- 방화벽 설치
  - 개인용 컴퓨터: 윈도우 방화벽, macOS 방화벽 등 기본적으로 내장됨
    - 개인 컴퓨터 내부로 들어오거나 외부로 나가는 네트워크 트래픽을 감시
  - **기업: 네트워크에(라우터나 게이트웨이)설치하여 내부망을 보호**
  - 스마트폰에도 기본적으로 간단한 방화벽 기능이 탑재되어 있음
    - 앱 기반 접근 제어 및 권한 제어
    - 개인용 컴퓨터에 비해 더 제한적 임

# 방화벽

- 방화벽 기능
  - 정상적인 웹사이트 허용
    - 사용자가 www.naver.com에 접속
    - 웹 접속은 일반적으로 포트 80, 8080(HTTP) 또는 443(HTTPS)를 사용
    - 방화벽 동작:
      - 요청 포트와 IP가 정상 → 허용
      - 방화벽은 포트 번호를 보고 "정상적인 웹 접속 " 판단해서 통과

# 방화벽

- 방화벽 기능
  - 해커의 원격 접속 시도 차단
    - 외부 해커가 내 컴퓨터에 접속하려고 함 (예: 원격 데스크톱 접속)
    - 해커는 포트 3389(RDP) 또는 다른 비정상적인 포트를 사용
    - 방화벽 동작:
      - 기본 설정으로 막혀 있는 포트에 대한 외부로부터의 접근 → 차단
      - 방화벽은 외부에서 들어오는 허용되지 않은 포트로의 연결 시도를 감지하고 차단
  - 파일 자동 다운로드 차단
  - 불법 프로그램이나 악성코드가 서버에 연결하려 할 때 차단

# 다양한 기능을 설정 및 분석

## 전체 트래픽에 대한 세부 분석

### Top 공격자

Top Attackers

| Source IP | Count |
|---|---|
| 10.200.1.9 | 197 |
| 10.200.1.17 | 161 |
| 192.168.3.7 | 79 |
| 10.131.10.1 | 78 |
| 10.200.1.166 | 71 |
| 10.112.10.21 | 58 |
| 216.58.219.110 | 46 |
| 10.131.12.204 | 34 |
| 69.244.85.47 | 31 |
| 10.200.1.15 | 23 |

Last updated less than a minute ago

### Top 타켓

Top Targets

| Destination IP | Count |
|---|---|
| 10.200.1.2 | 61 |
| 10.200.1.3 | 61 |
| 10.200.1.5 | 59 |
| 10.200.1.86 | 49 |
| 10.131.10.121 | 37 |
| 10.200.1.17 | 36 |
| 10.200.1.18 | 36 |
| 10.131.10.120 | 35 |
| 10.200.1.169 | 33 |
| 10.200.1.74 | 31 |

Last updated 3 minutes ago

### 애플리케이션 총 이벤트

Total Events by Application Protocol

| Application | Total Events |
|---|---|
| HTTP | 1,474 |
| DNS | 620 |
| HTTPS | 352 |
| Google | 300 |
| VMware Server Console | 176 |
| Gmail | 26 |
| Google APIs | 18 |
| Google Analytics | 10 |
| NetBIOS-ssn (SMB) | 10 |
| Dropbox | 8 |

Last updated 2 minutes ago

### 등급별 위협 이벤트

Intrusion Events

| | Last 6 hours | Total |
|---|---|---|
| | | 1,432 |
| 0 | | 39 |
| 1 | | 63 |
| 2 | | 706 |
| 3 | | 569 |
| 4 | | 57 |
| All | | 1,434 |

### Top 악성코드

Malware Threats

| Detection Name | Count |
|---|---|
| Win.Trojan.StartPage-36 | 43 |
| Win.Adware.Mycentria-9 | 29 |
| Win.Trojan.Trafox-3 | 26 |
| Trojan.Generic.FakeAV | 24 |
| Trojan.Mycentria | 24 |
| Trojan.Clicker.Small | 15 |
| Trojan.Bifrose.NSP | 12 |
| Trojan.Generic.Fakesec | 12 |
| Win.Trojan.Trojan-533 | 8 |
| W32.Auto.6870a1.191464.in01 | 6 |

### 카테코리별 트래픽

Traffic by Security Intelligence Category

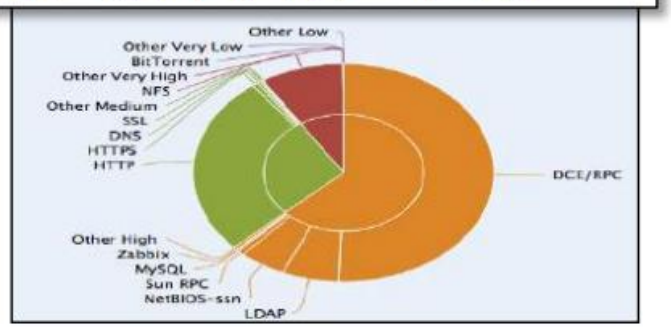
| Security Intelligence Category | Total Bytes (KB) |
|---|---|
| Network_Intelligence-Open_Relay | 203,831.79 |
| Network_Intelligence-Phishing | 51,971.37 |
| Network_Intelligence-CnC | 36,826.17 |
| Network_Intelligence-Tor_exit_node | 34,099.77 |
| Network_Intelligence-Suspicious | 32,455.18 |
| Network_Intelligence-Malware | 22,924.35 |
| Network_Intelligence-Attackers | 21,811.96 |
| Network_Intelligence-Spam | 21,786.07 |
| Network_Intelligence-Open_Proxy | 8,817.72 |
| Network_Intelligence-Bogon | 8,708.13 |

# 방화벽

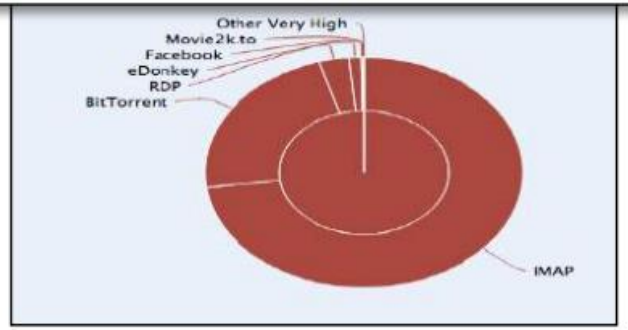
## 다양한 각도로 분석

### 관리 Tool을 통한 다양한 뷰

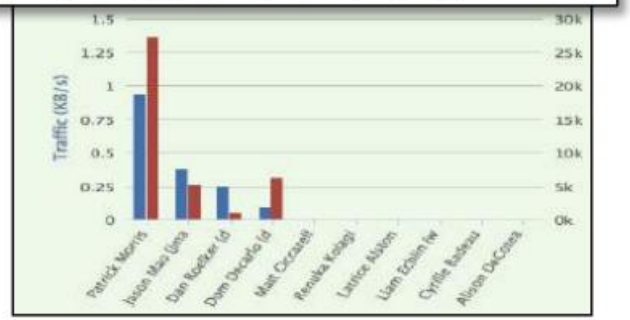
모든 애플리케이션 트래픽 뷰...



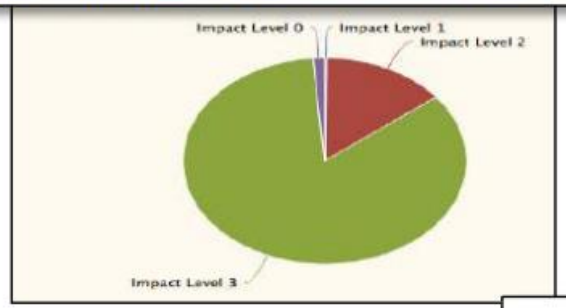

위험성 있는 애플리케이션 뷰...



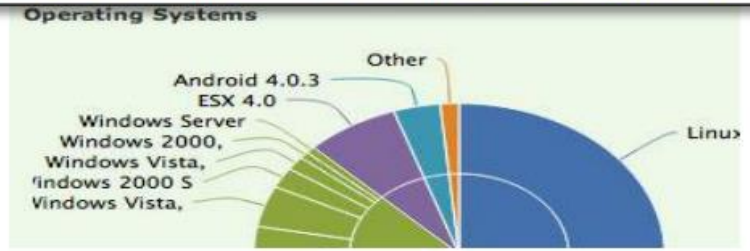

누가 그것을 사용하지 있는지?




그들은 어떠한 위험 요소가 있는지?




그들은 어떤한 OS를 사용하고 있는지?




그들의 이벤트 트래픽은 어떠한지?

# FTK Imager

➢ 프로그램 설명

- FTK Imager (Forensic Toolkit Imager)는 디지털 데이터 복구 전문가들이 사용하는 무료 도구
- 컴퓨터나 기타 저장장치에서 증거 데이터를 복사(이미징) 하고, 분석(미리보기, 검색) 할 수 있는 툴
- **➔ 누군가의 컴퓨터나 USB에서 파일을 복사하고, 삭제된 파일이나 숨겨진 정보를 복구하는 프로그램**

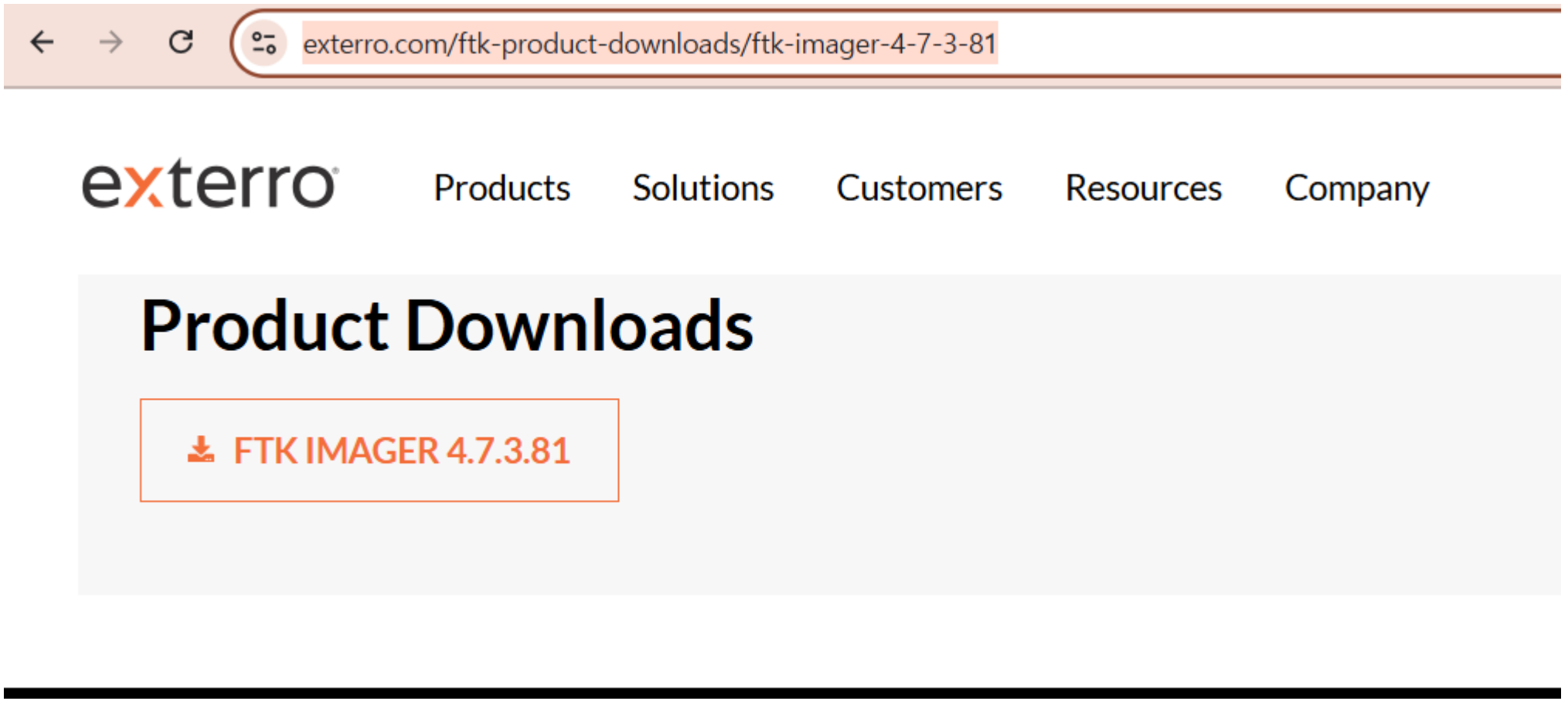
# FTK Imager

- 주요 기능

1. **디스크 이미지 생성 : 실제 저장장치(HDD, USB 등)를 복사해 E01 등의 이미지 파일로 저장**
2. **이미지 마운트 : 만들어진 이미지 파일을 불러와 내부 파일 구조 확인**
3. **삭제 파일 복구 보기 : 삭제된 파일 목록 확인**
4. 파일/폴더 구조 탐색 : 이미지 또는 실장치를 폴더 구조로 보여줌
5. 메타데이터 보기 : 파일 속성, 생성/수정/접근 시간 등 확인
6. 해시값 계산 : 파일이나 드라이브의 해시(MD5, SHA1 등) 생성
7. 문자열 검색 : 키워드 검색 기능으로 이미지 내 텍스트 탐색
8. 파일 내 Hex 보기 : 파일의 16진수 내용을 보여줌
9. E01, DD 등 다양한 포맷 지원 : EnCase, RAW 등 다양한 이미지 파일 포맷 지원

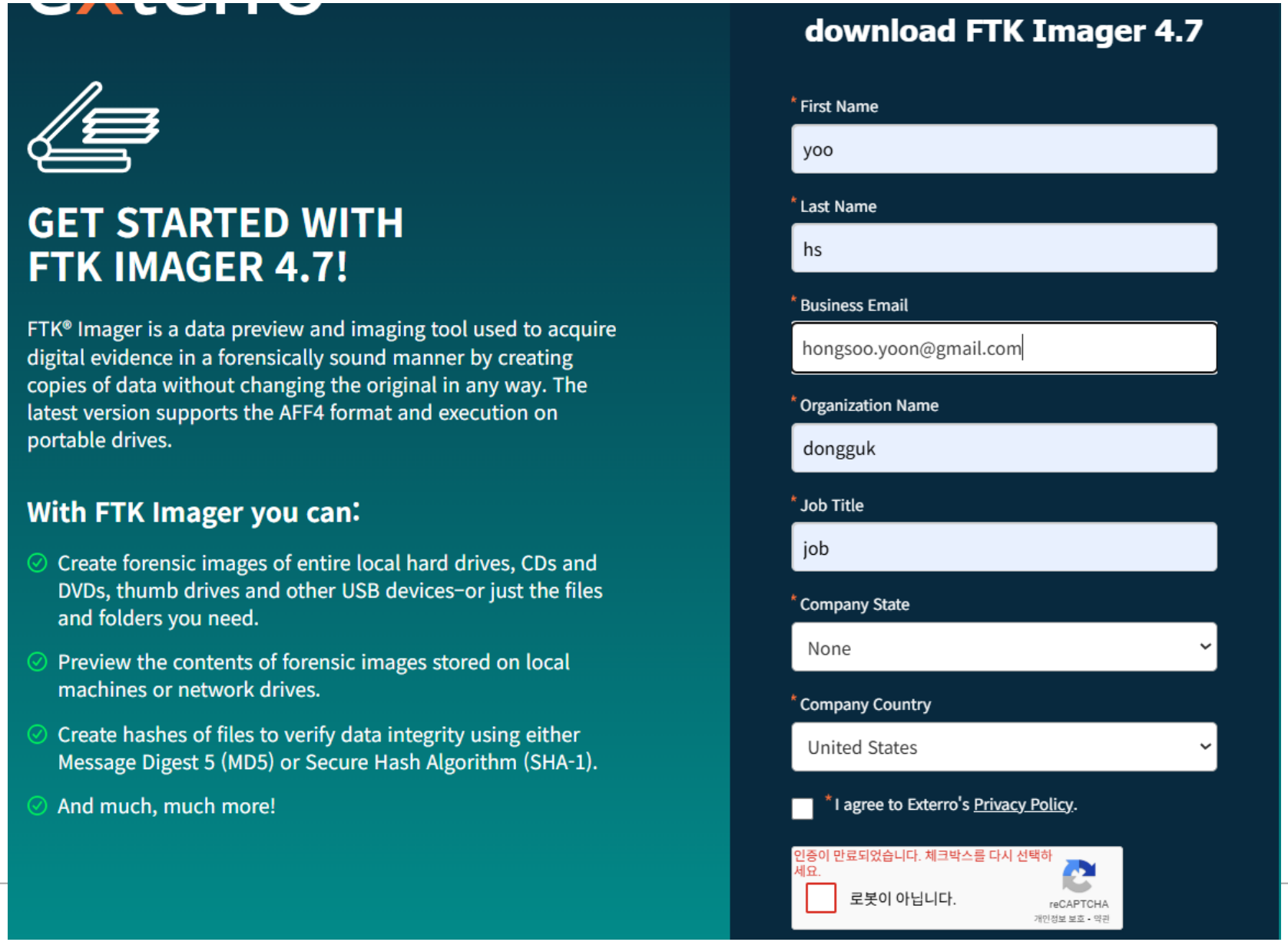
# FTK Imager - 설치

https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81

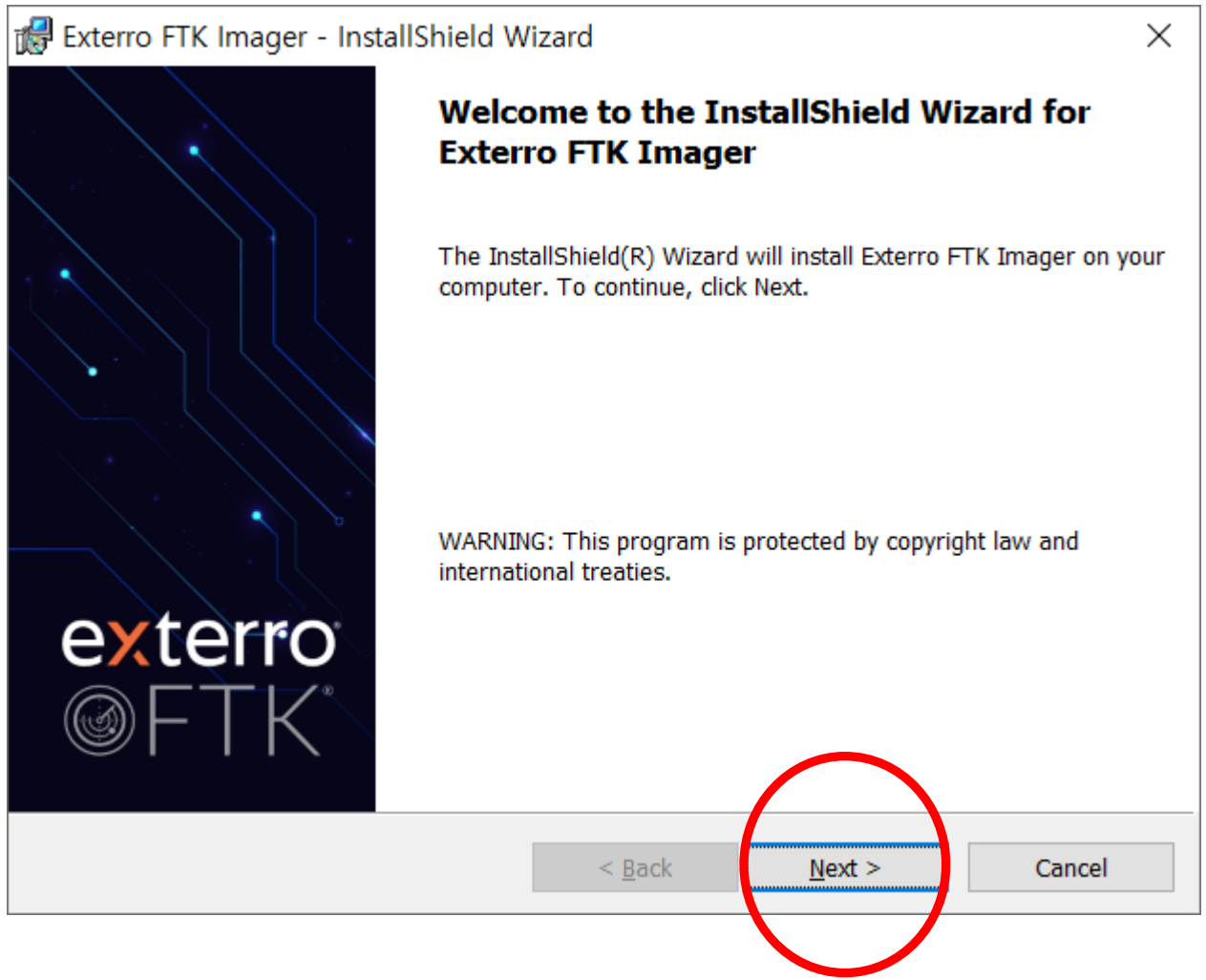


# FTK Imager - 설치

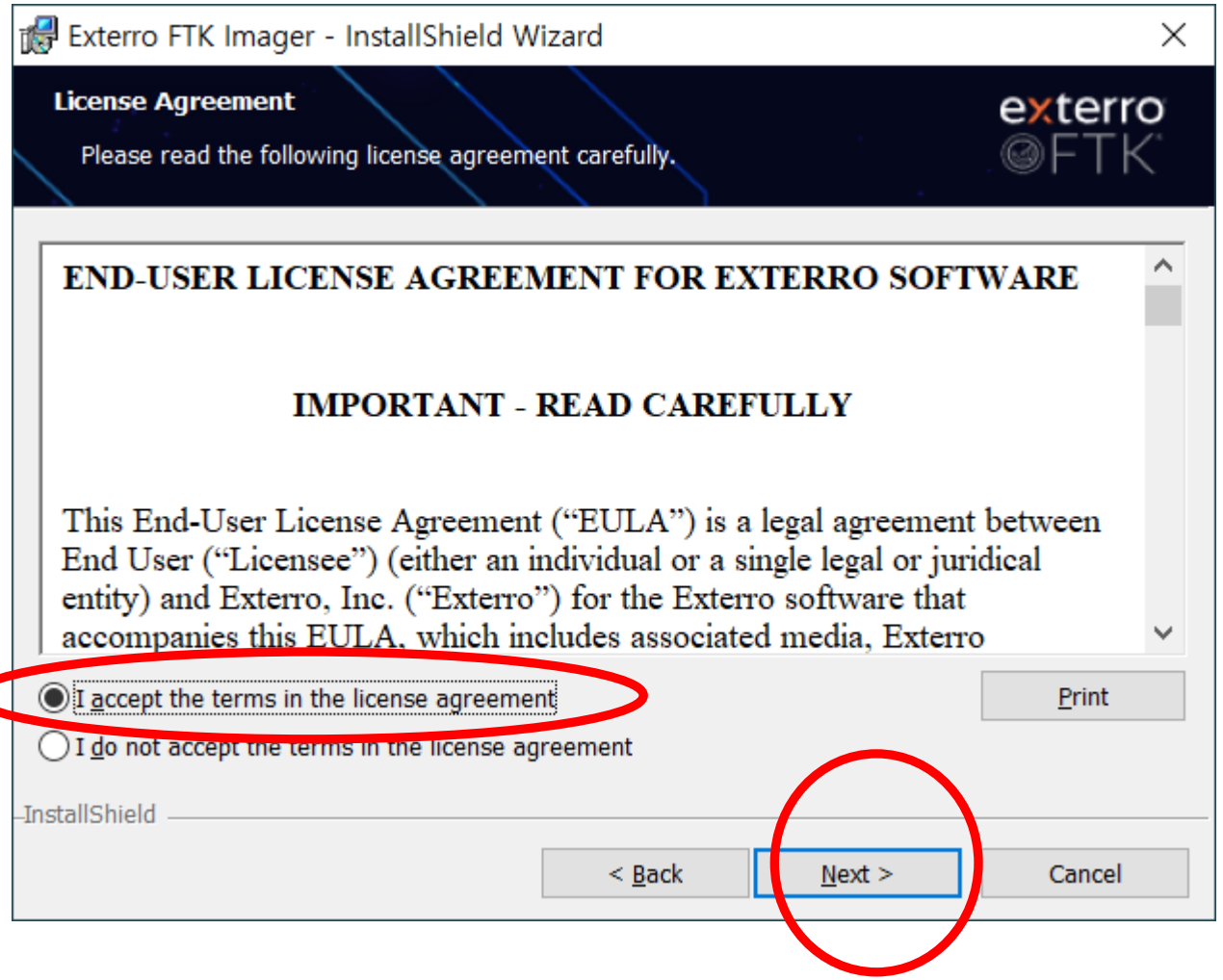
| 이름 | 수정한 날짜 | 유형 | 크기 |
|---|---|---|---|
| Exterro_FTK_Imager_(x64)-4.7.3.81.exe | 2025-04-22 오후 10:13 | 응용 프로그램 | 59,242KB |



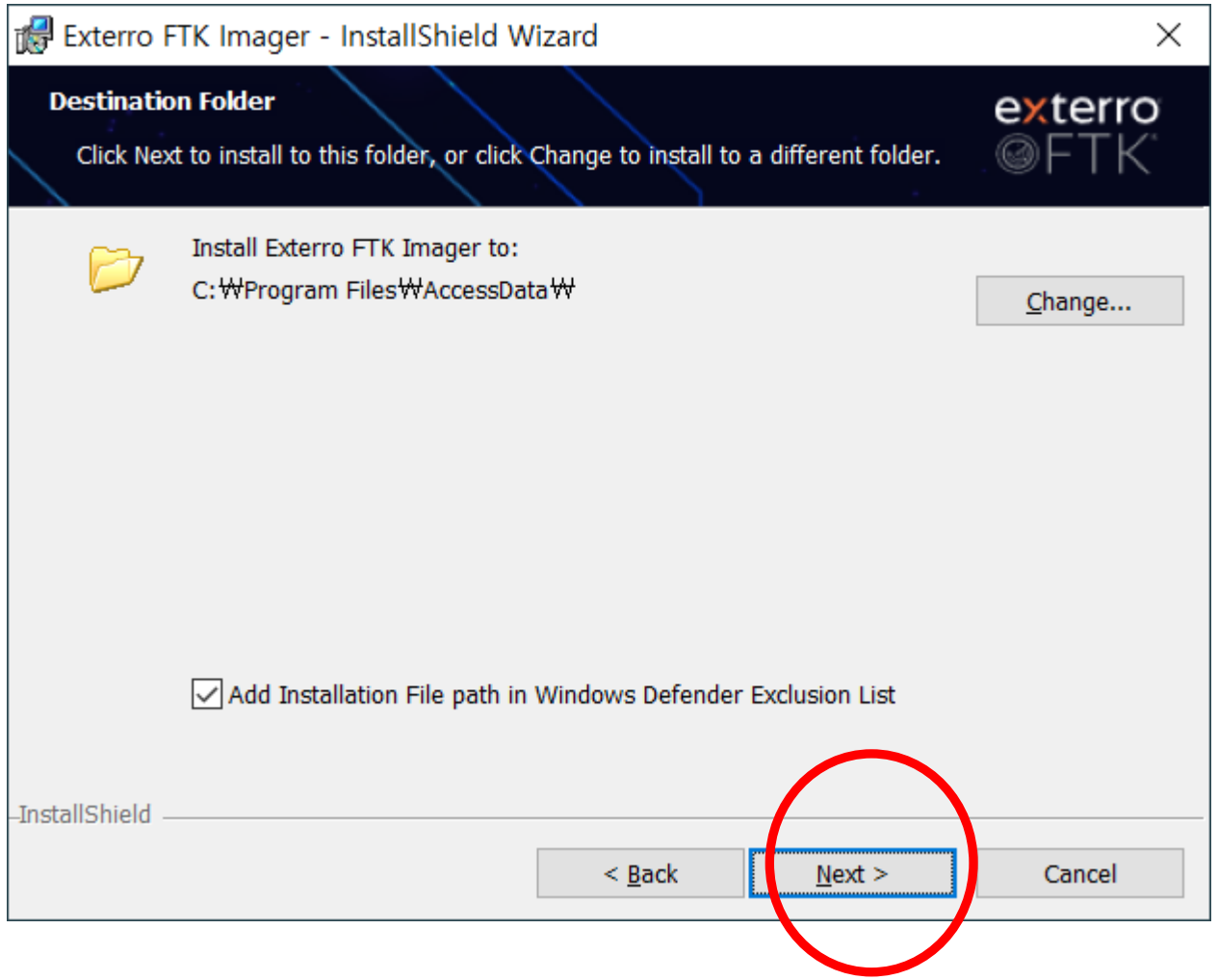
# FTK Imager - 설치



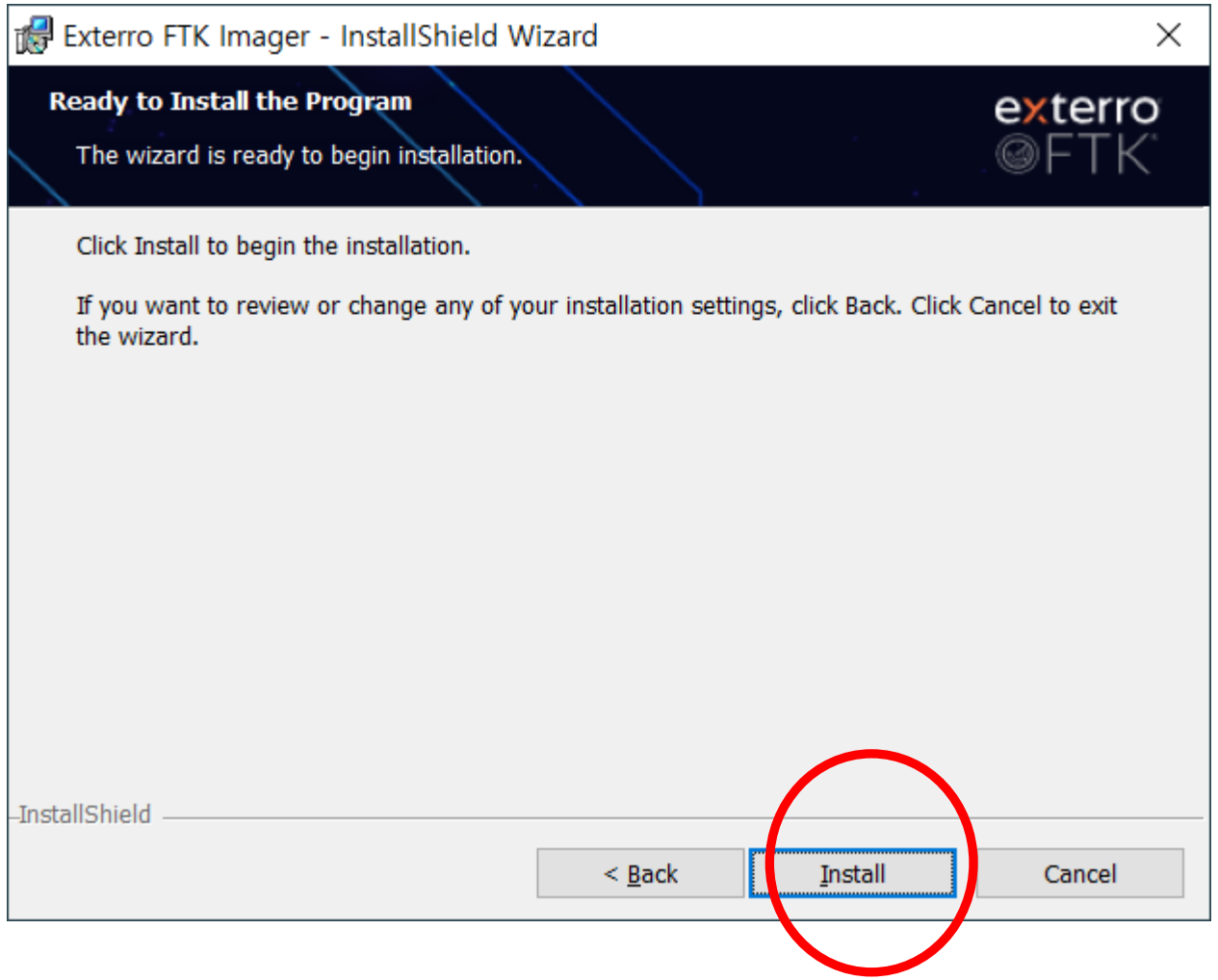
# FTK Imager - 설치



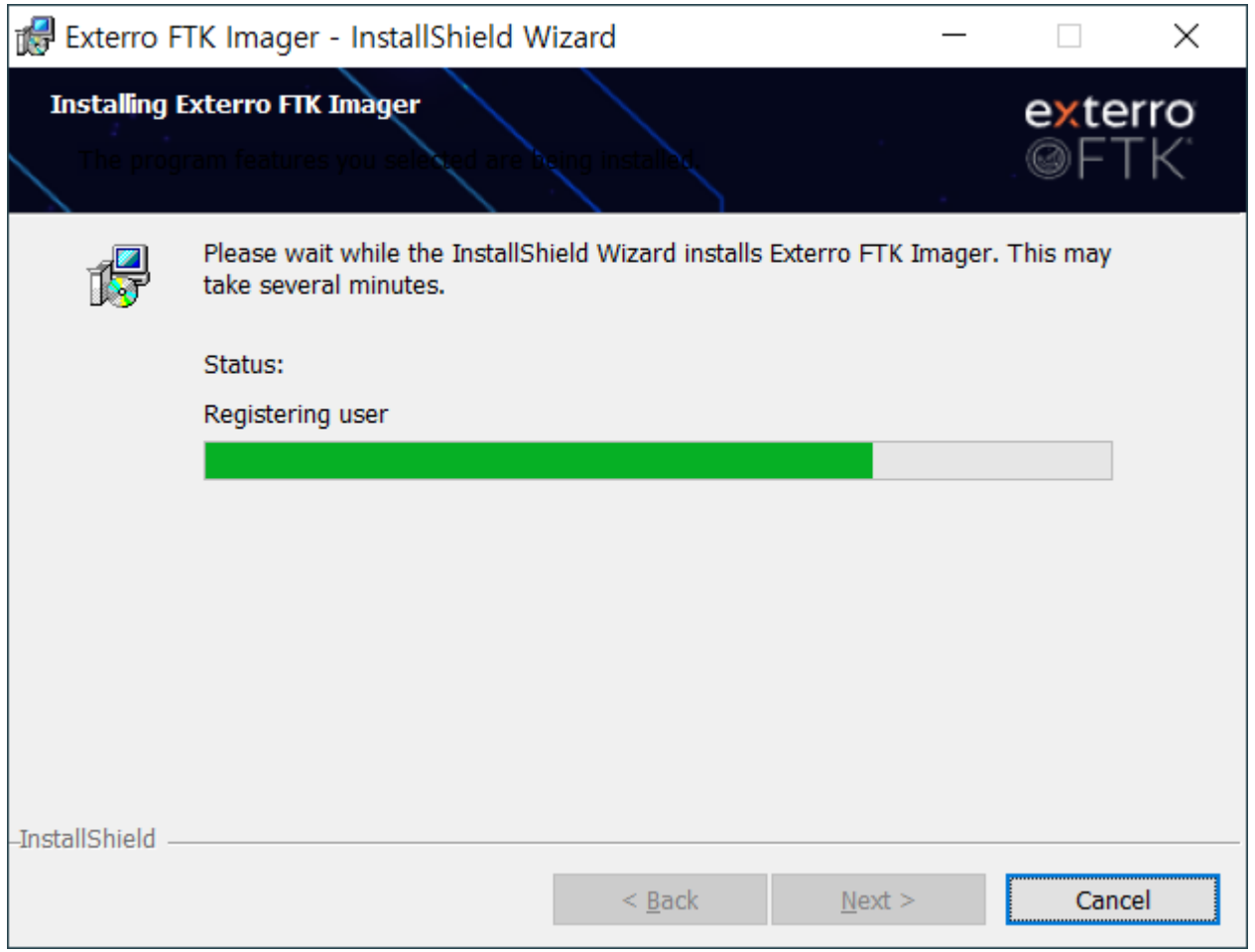
# FTK Imager - 설치



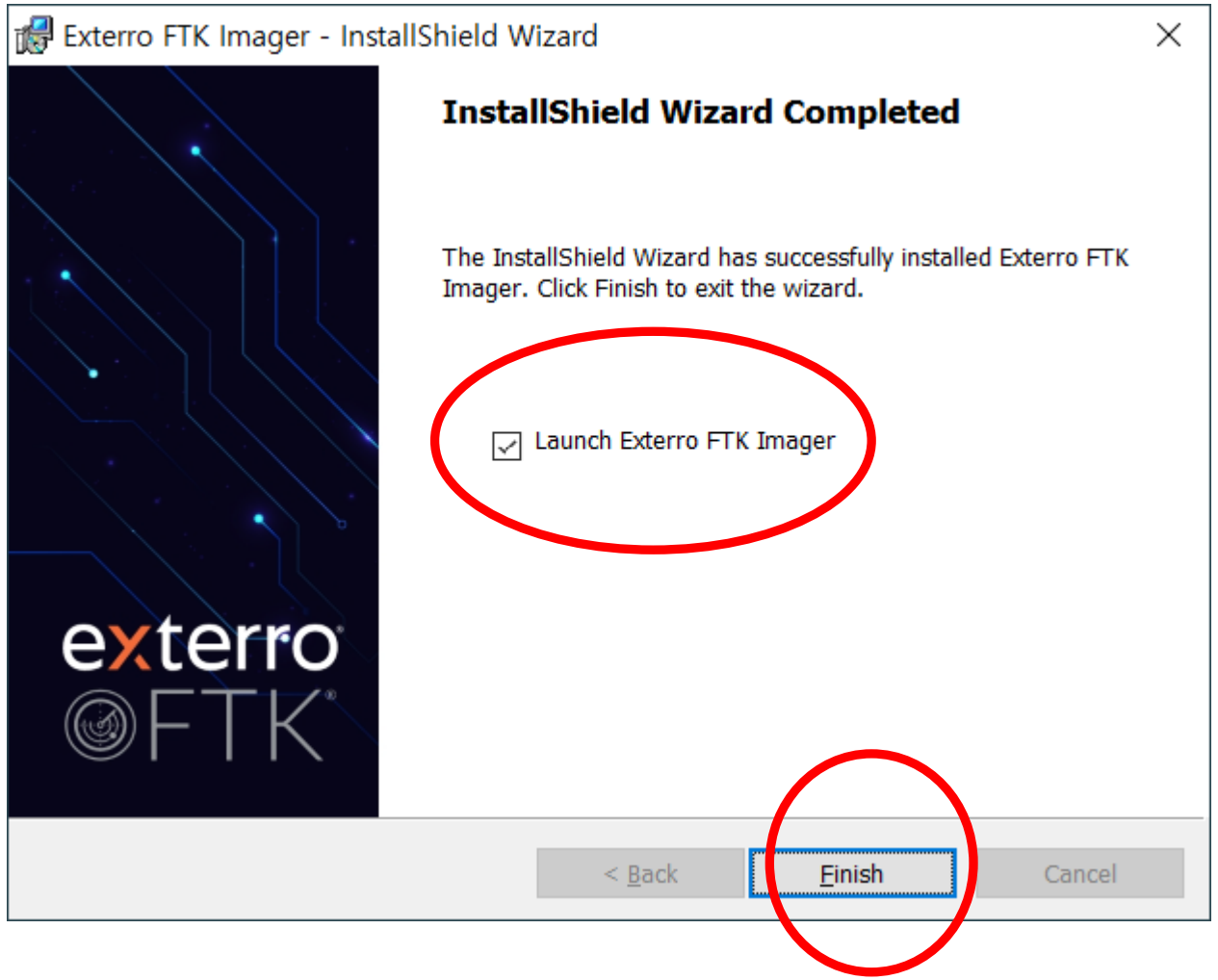
# FTK Imager - 설치



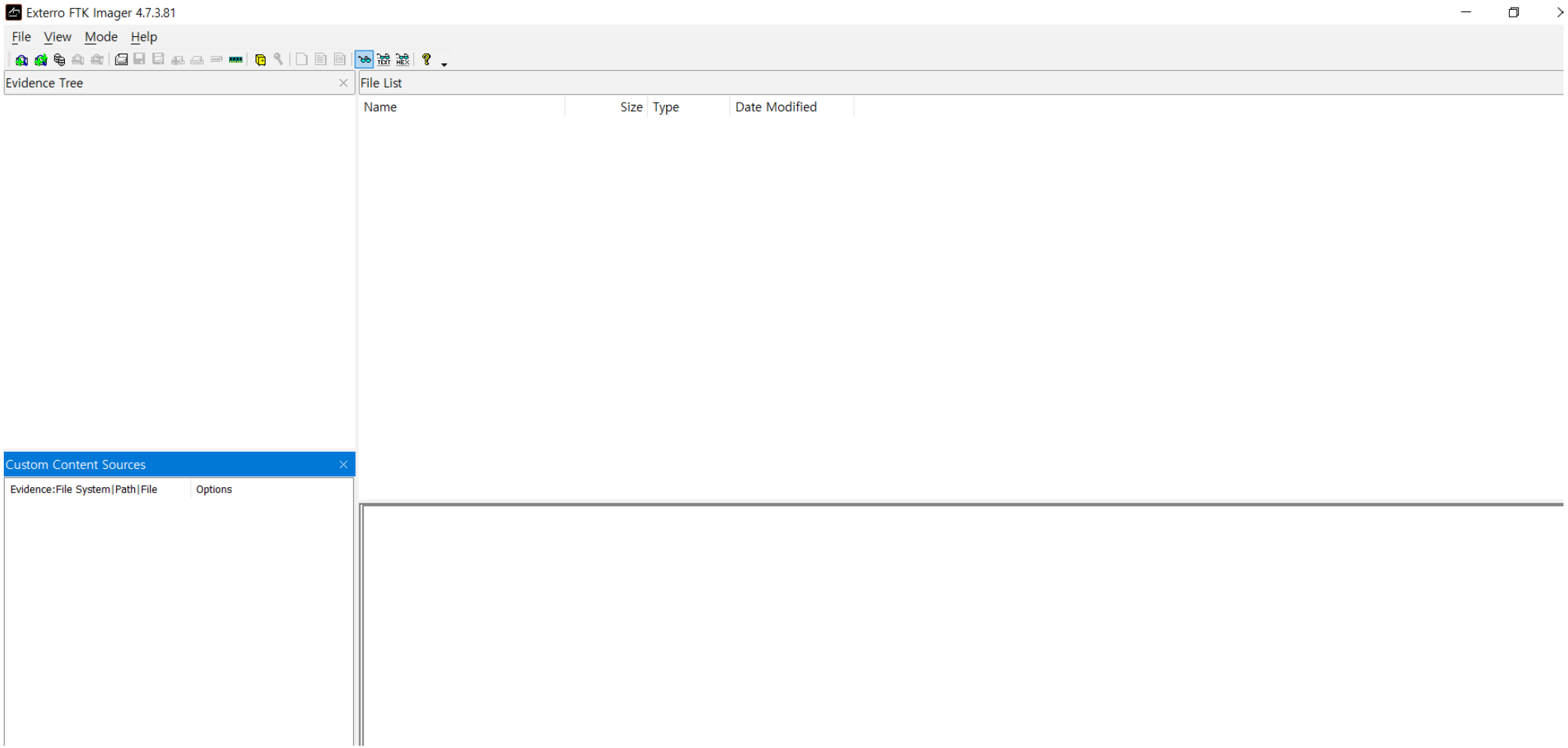
# FTK Imager - 설치



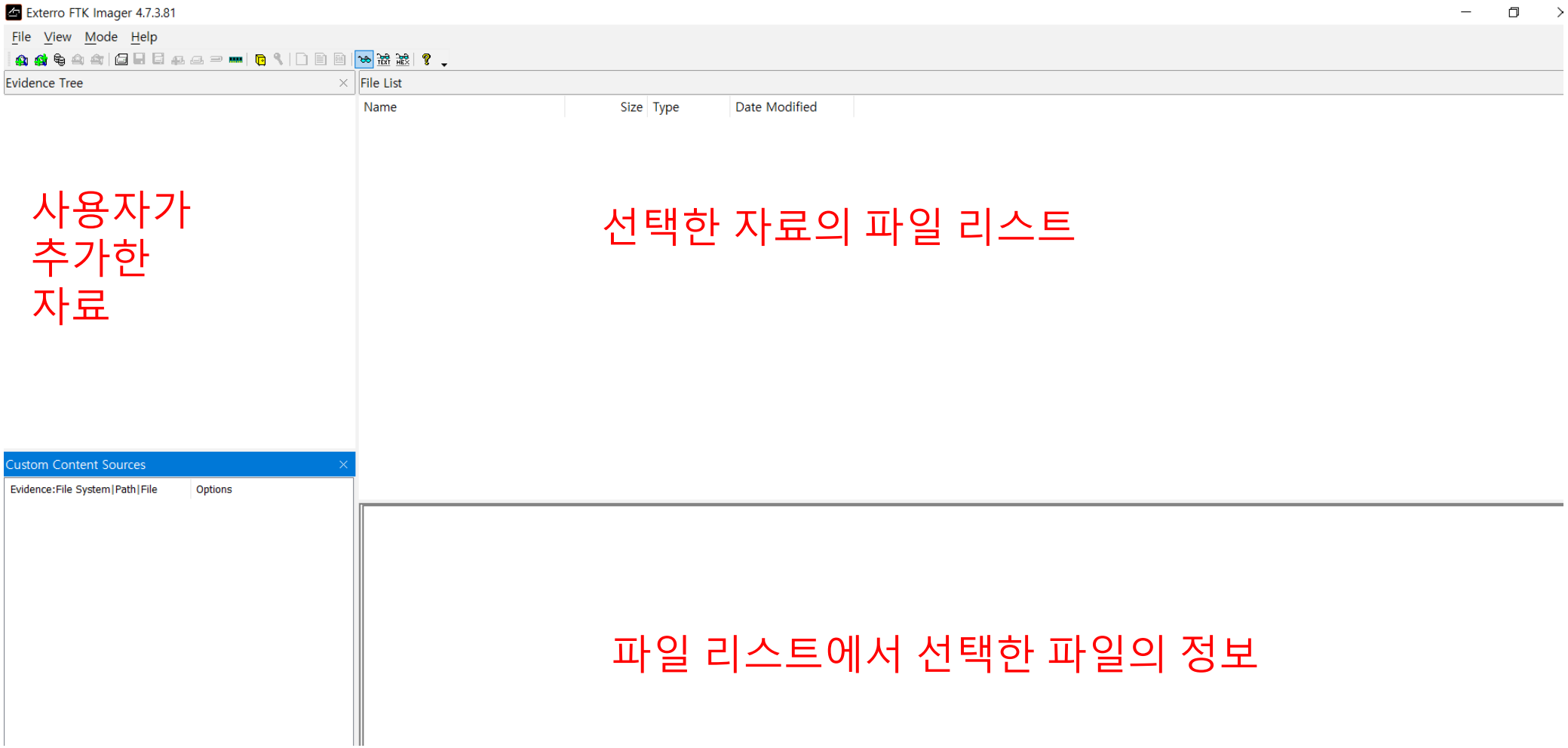
# FTK Imager - 설치



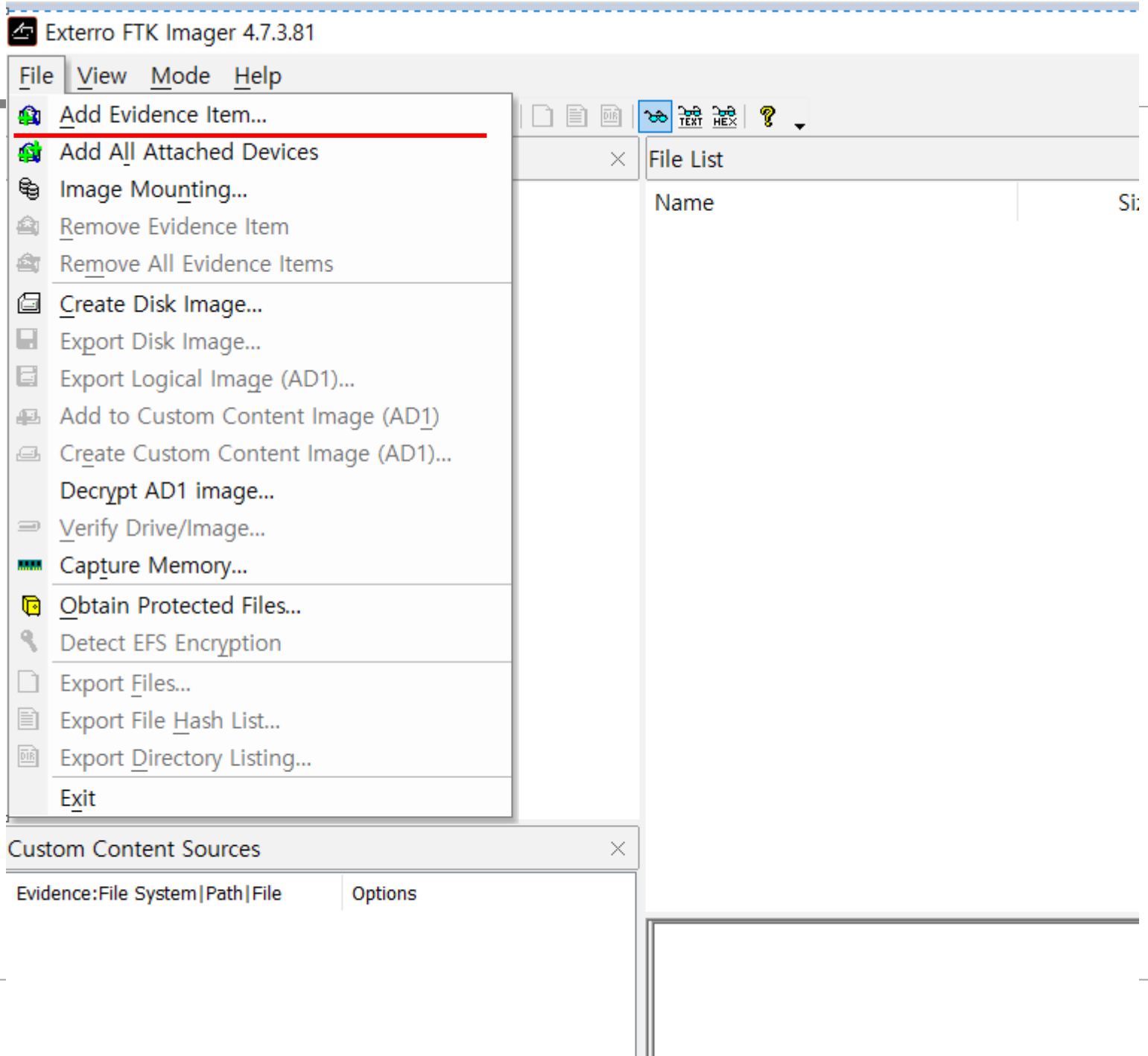
# FTK Imager – 설치 완료



# FTK Imager


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
사용자가 추가한 자료
선택한 자료의 파일 리스트
Custom Content Sources
Evidence:File System|Path|File Options
파일 리스트에서 선택한 파일의 정보

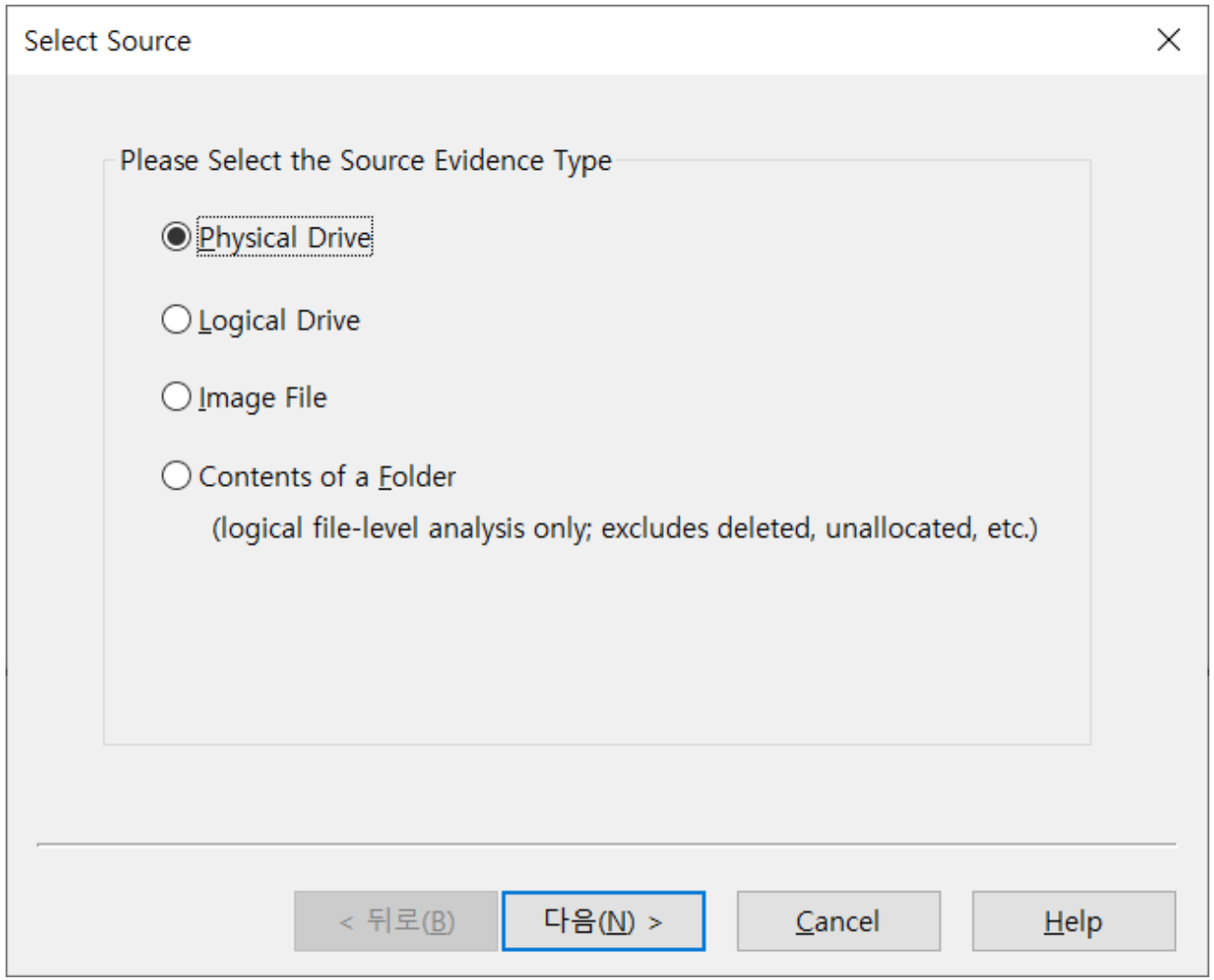
# FTK Imager


Exterro FTK Imager 4.7.3.81
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name
Custom Content Sources
Evidence:File System|Path|File
Options

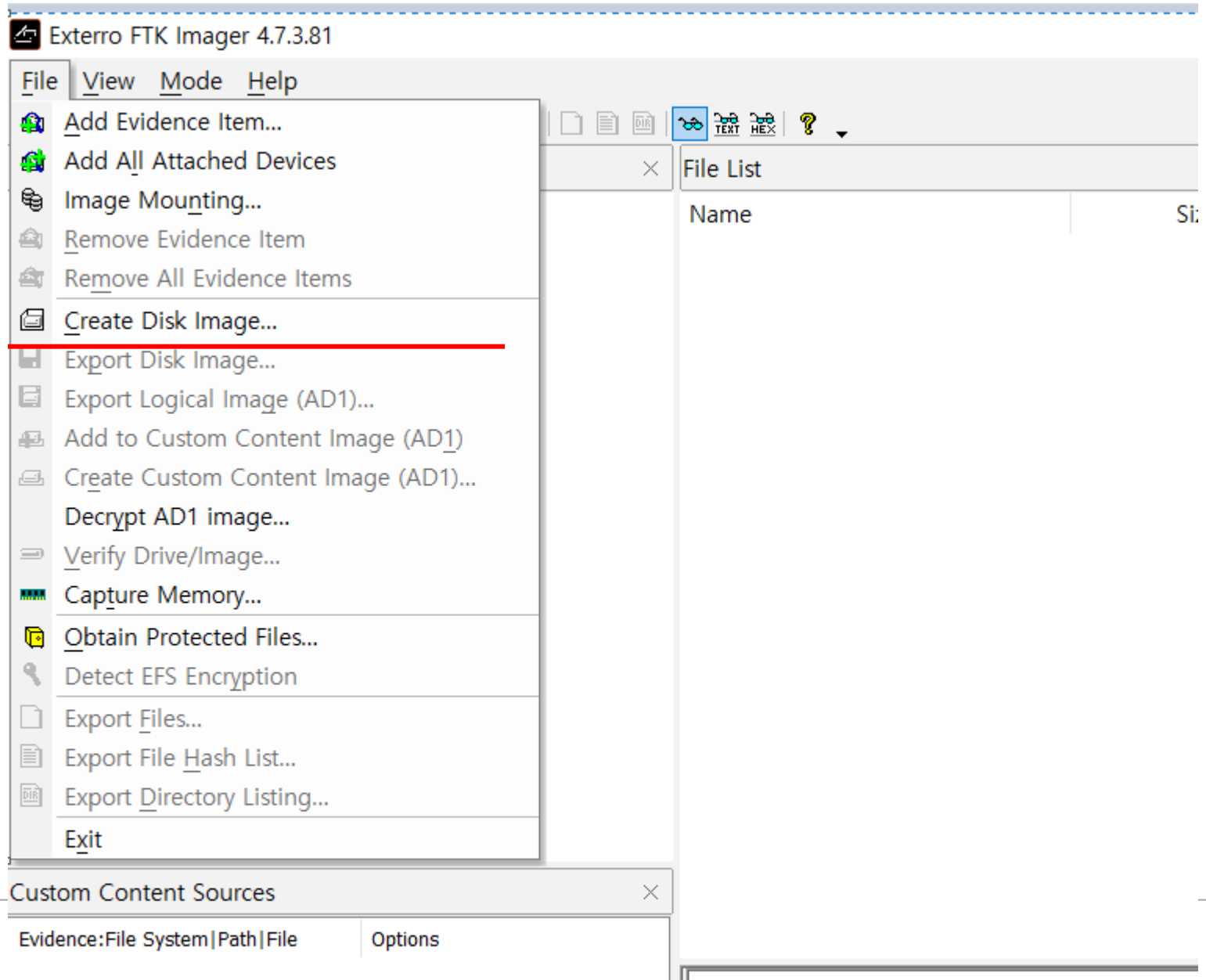
# FTK Imager - Add Evidence Item

- 기능
  - 말 그대로 증거 자료를 Evidence Tree 에 추가
  - 선택하면 Source 종류를 선택할 수 있다
    - Physical Drive : 물리적 드라이브 (HDD 전체를 지정)
    - Logical Drive : 논리적 드라이브 (HDD 를 C, D 등으로 분할하여 사용할 경우 이 옵션 선택)
    - Image File : 이미징 파일
    - Contents of a Folder : 특정 폴더의 콘텐츠
  - 자신의 상황에 맞게 추가하면 됨.

# FTK Imager - Add Evidence Item



# FTK Imager - Create Disk Image



# FTK Imager - Create Disk Image

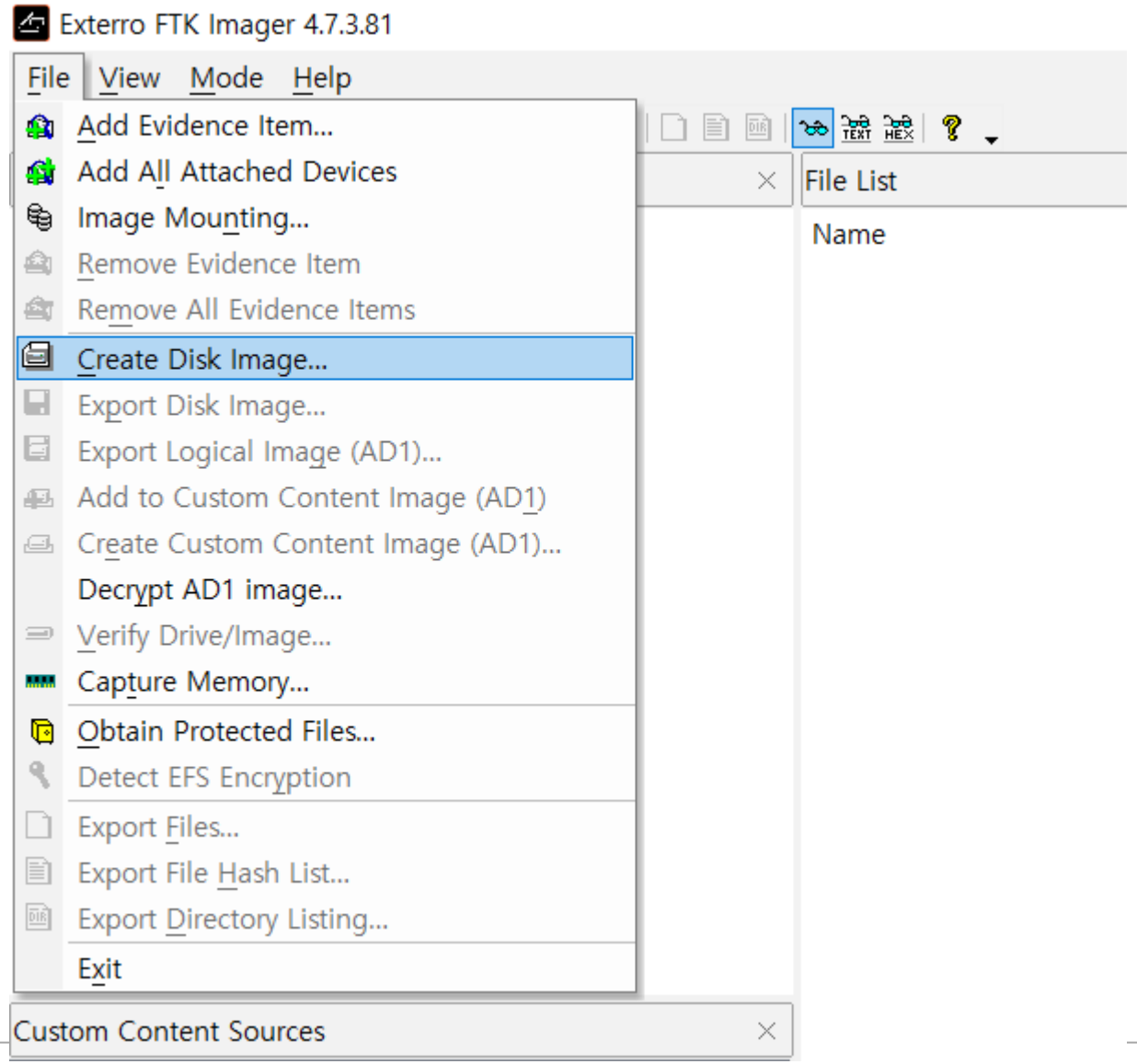
- 기능
  - 디스크 이미지 만드는 기능
  - 내 디스크 이미지 덤프 하기

디스크 이미징 하는 이유?

현재 상태를 이미징 파일로 현재 상태를 보존

# FTK Imager - Create Disk Image

- 기능
  - 디스크 이미지 만드는 기능
  - 내 디스크 이미지 덤프 하기

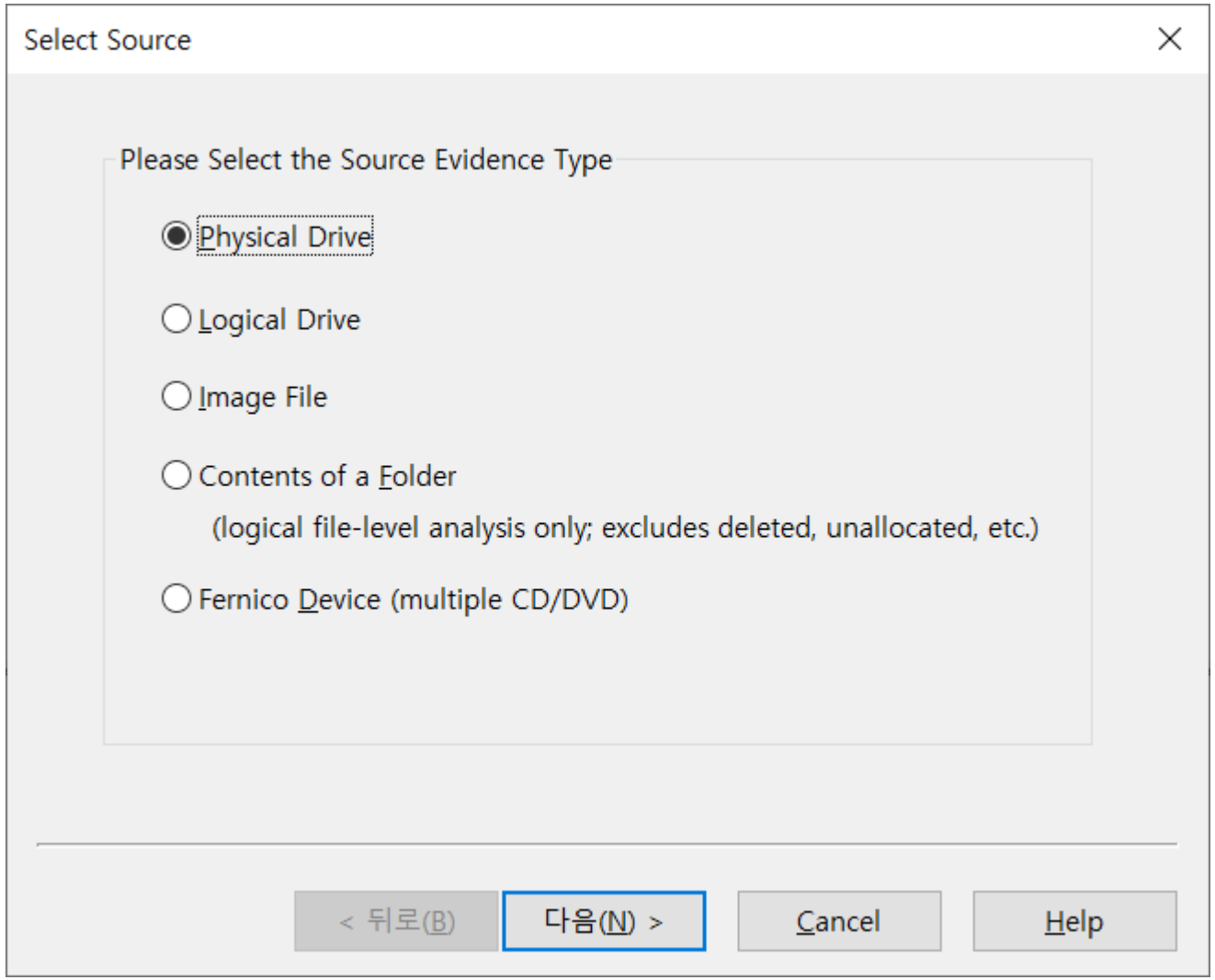


# FTK Imager - Create Disk Image

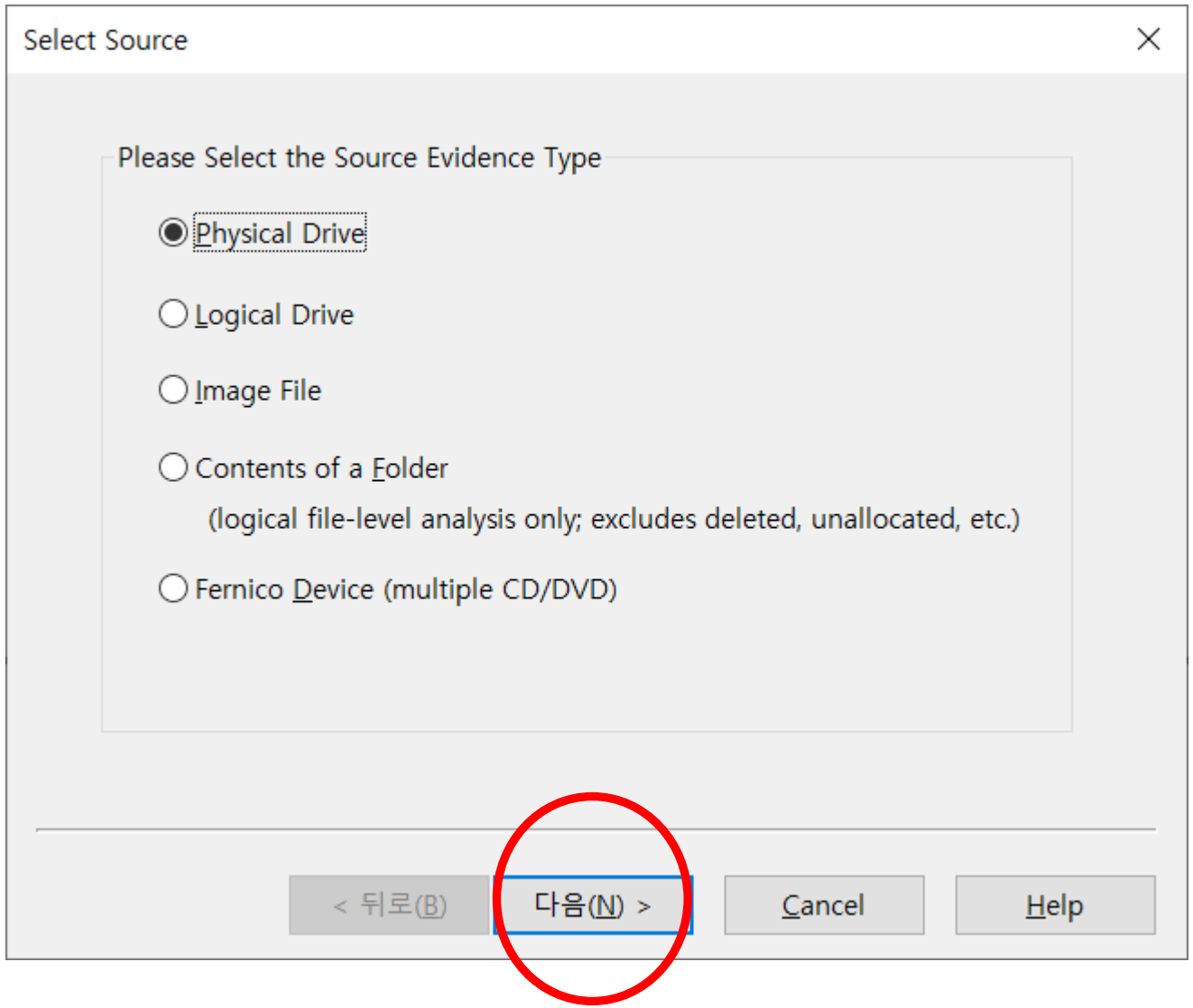
Physical Drive 선택

- Physical Drive : 물리적 드라이브 (HDD 전체를 지정)
- Logical Drive : 논리적 드라이브

  (HDD 를 C, D 등으로 분할하여 사용할 경우 이 옵션 선택)
- Image File : 이미징 파일
- Contents of a Folder : 특정 폴더의 콘텐츠

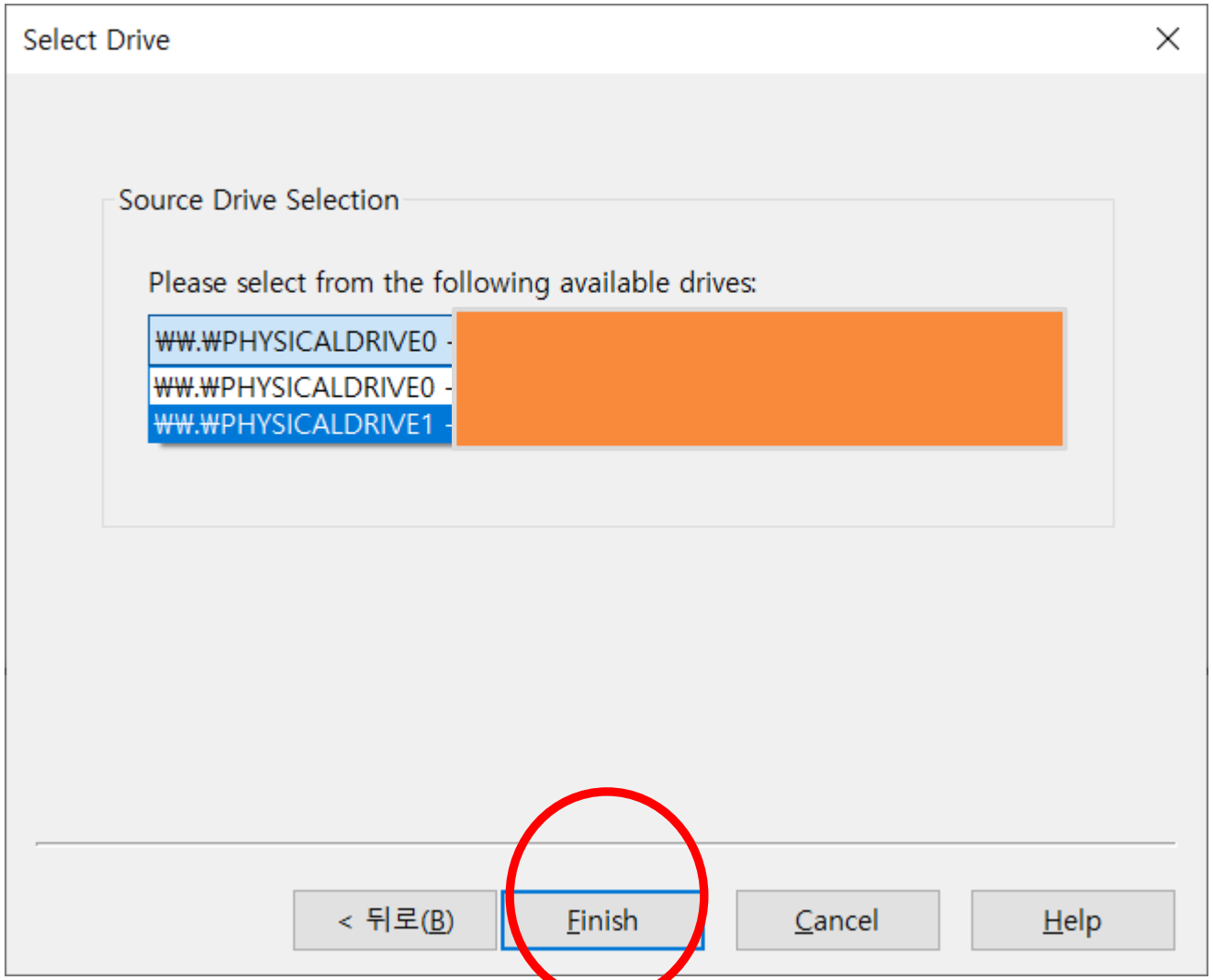


# FTK Imager - Create Disk Image

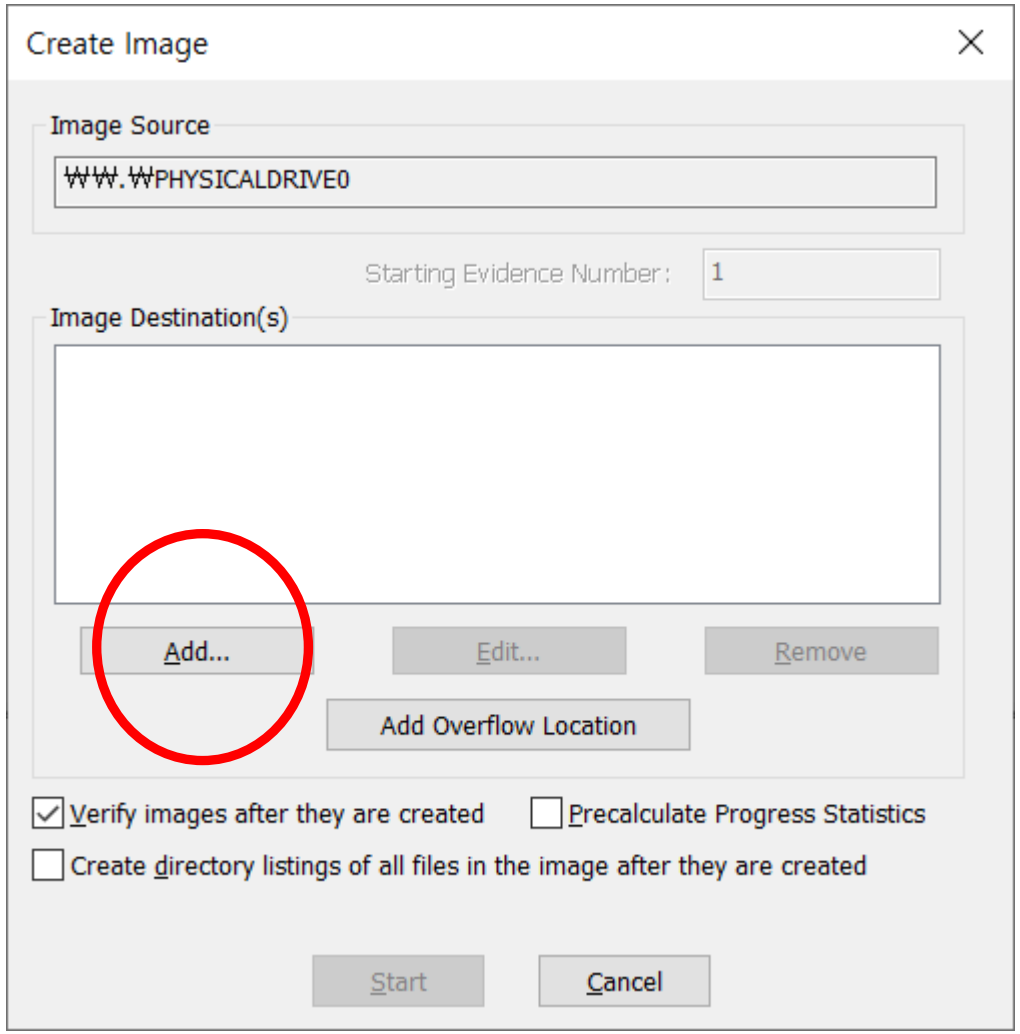


# FTK Imager - Create Disk Image

디스크 선택 후 Finish



# FTK Imager - Create Disk Image

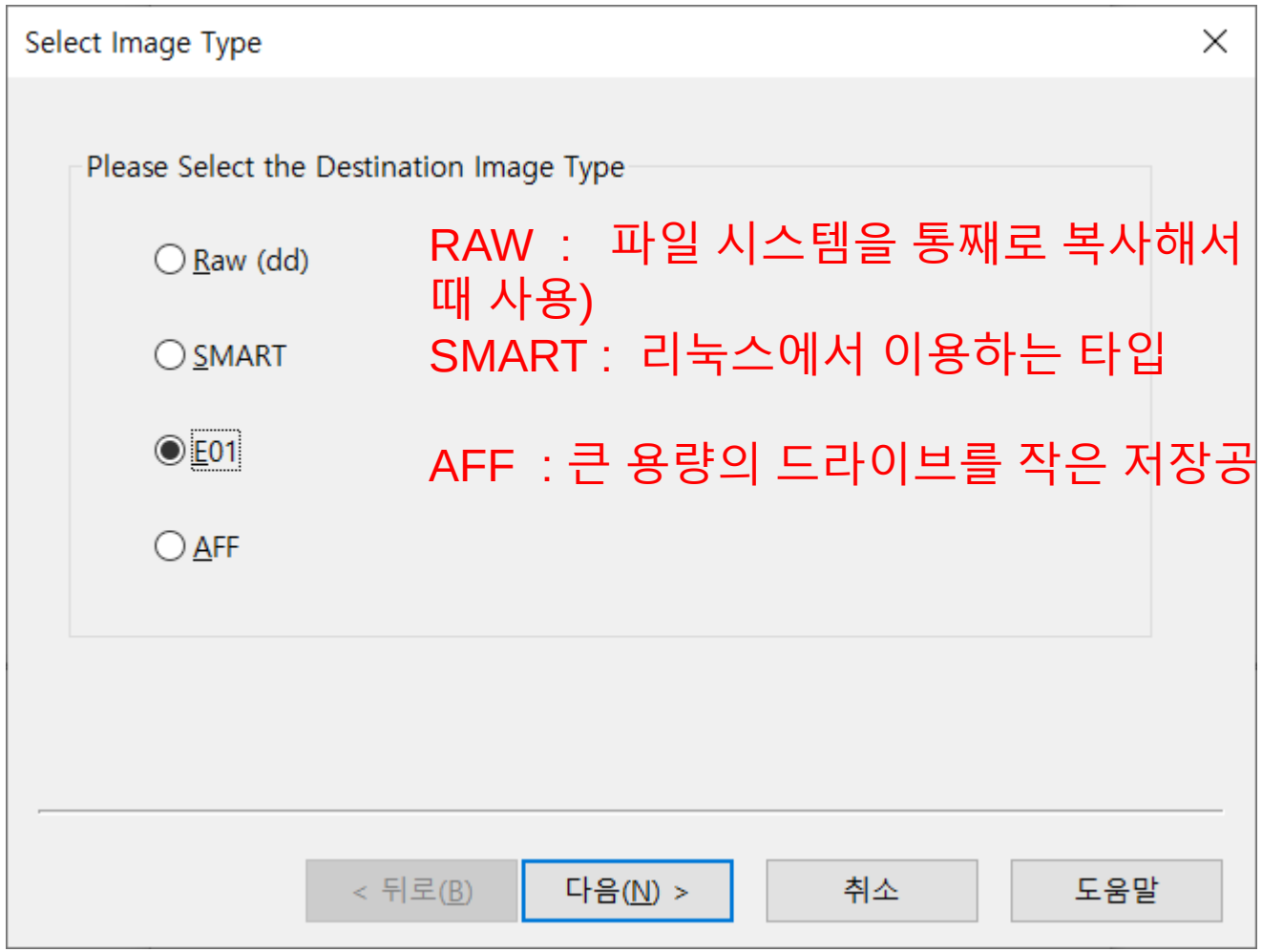



검증, 확인 하는 것으로 시간이 약 30%정도 더 걸릴 수 있음. (Verify images after they are created)

Precalculate Progress Statistics를 선택하면 남은 시간을 보여줌

Add click

# FTK Imager - Create Disk Image

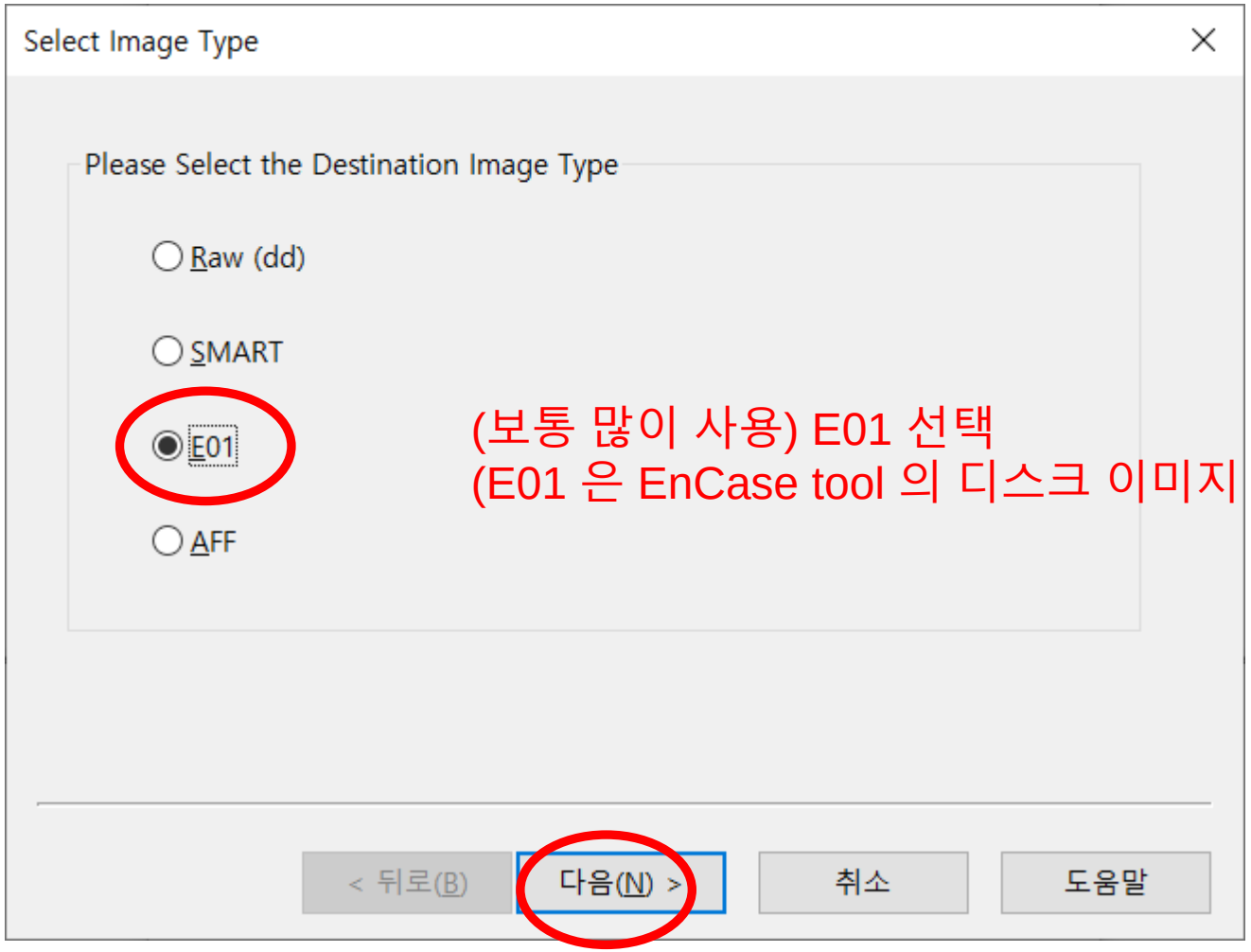



RAW : 파일 시스템을 통째로 복사해서 이미지를 만듬 (디스크의 파일시스템 전체를 복제할 때 사용)

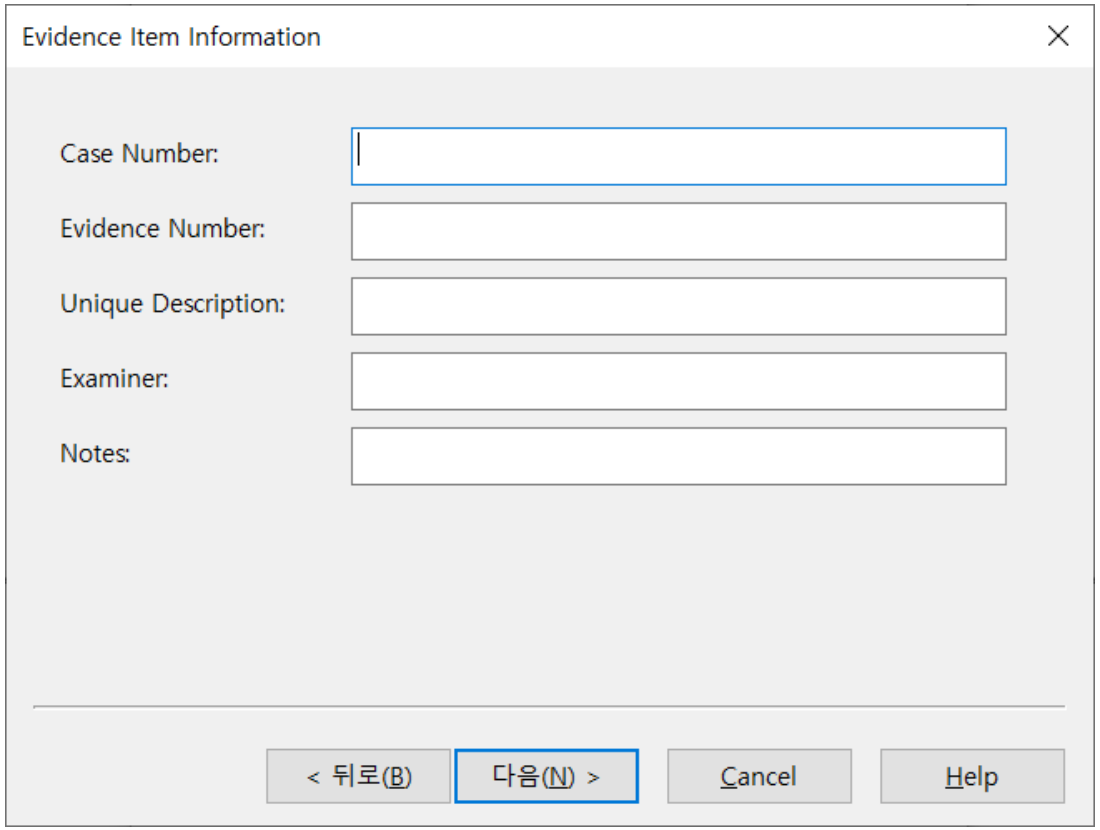
SMART : 리눅스에서 이용하는 타입

AFF : 큰 용량의 드라이브를 작은 저장공간에 저장하기 위해 많이 사용하는 방법

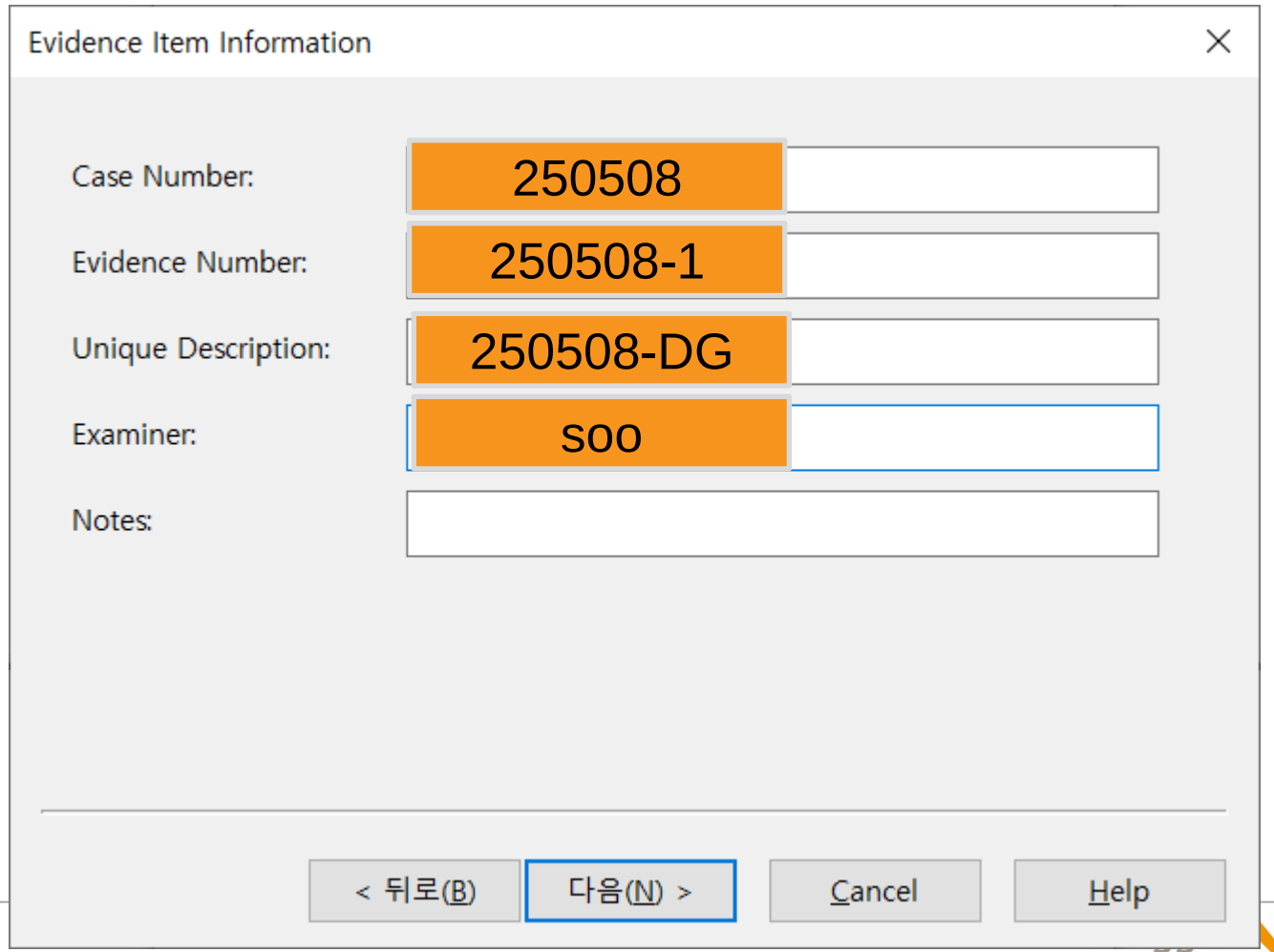
# FTK Imager - Create Disk Image



# FTK Imager - Create Disk Image



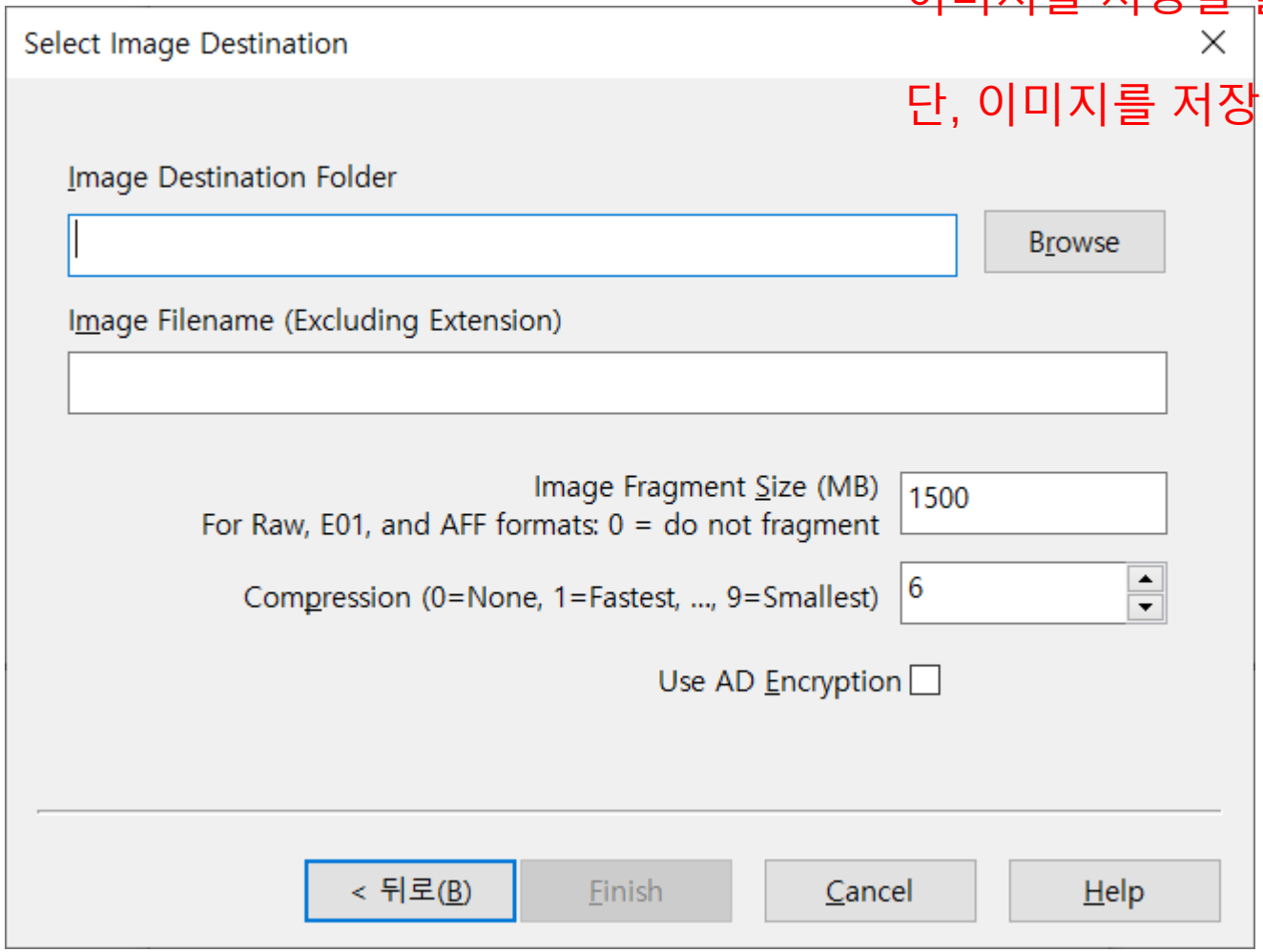

본인들의 케이스 내용에 맞게 작성



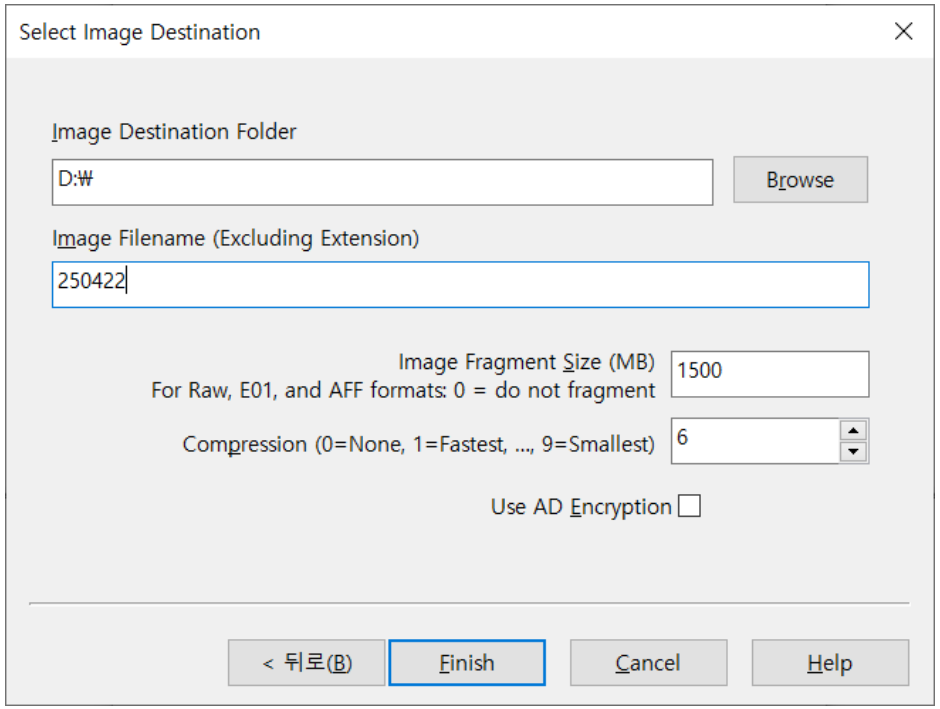
# FTK Imager - Create Disk Image

이미지를 저장할 폴더 와 이미지 파일 이름(확장자 제외) 작성

단, 이미지를 저장할 폴더는 덤프 할 디스크와 같은 곳에 존재하면 안된다.



# FTK Imager - Create Disk Image

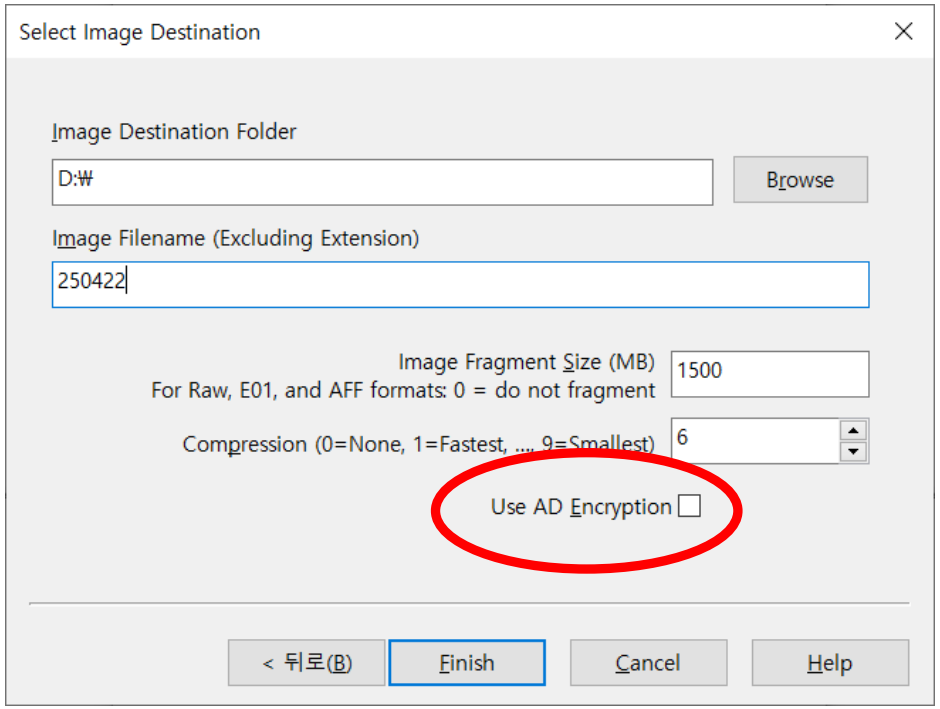


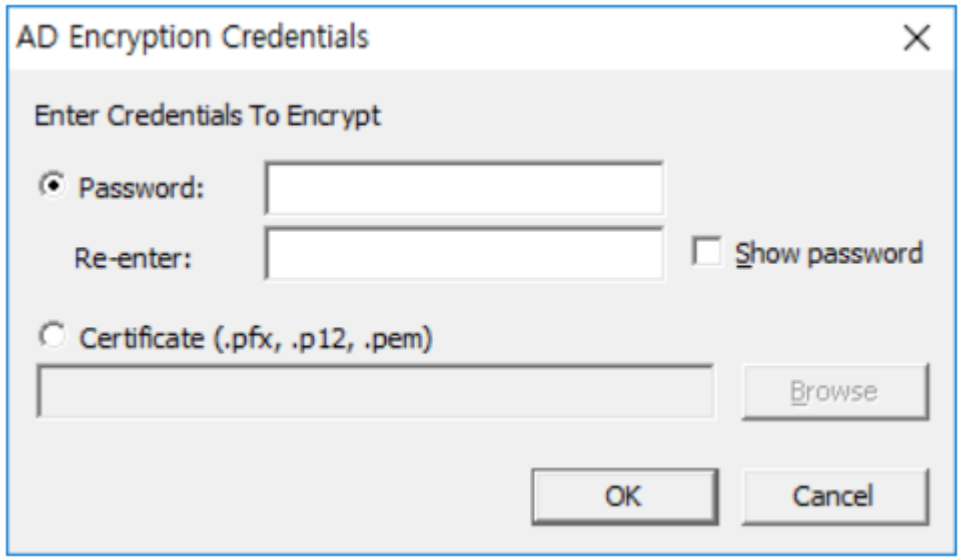

이미지 만들 디스크를 처음에 : C 드라이브를 선택을 했었음
그래서 저장할 위치를 D로 다른 저장장치로 설정 함.

Image Fragment Size 는 Image 파일을 분할하여 저장하는 경우, 어느 크기로 분할할지 지정
0 으로 설정하면 한 파일에 디스크 이미지를 생성하도록 하는 것 (4000으로 하면 4GB로 적당 함)

Compression 은 압축 정도인데, 9에 가까울수록 용량은 적어지겠지만 이미지 파일을 만드는 시간은 오래 걸림 (6이 적당)

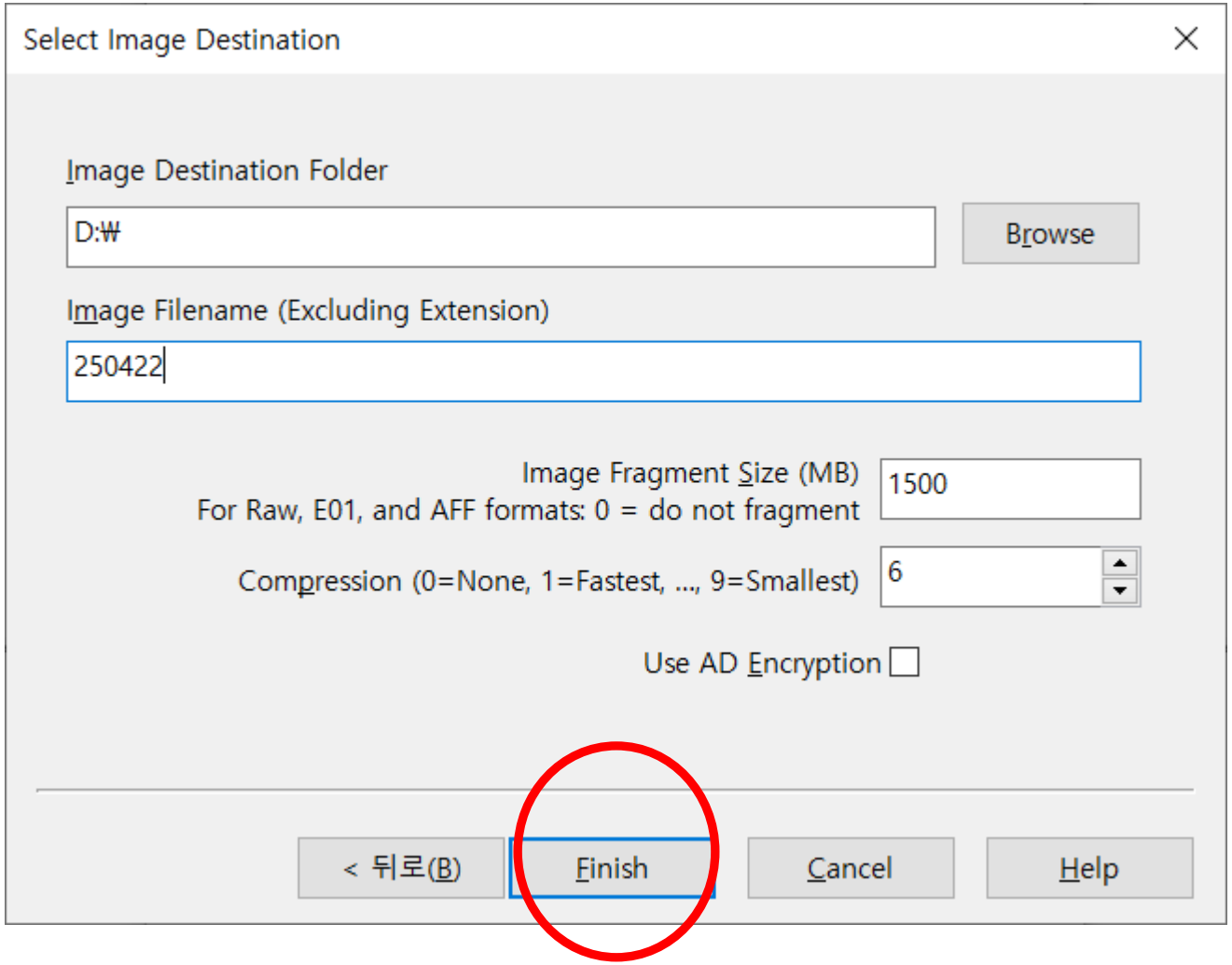
# FTK Imager - Create Disk Image



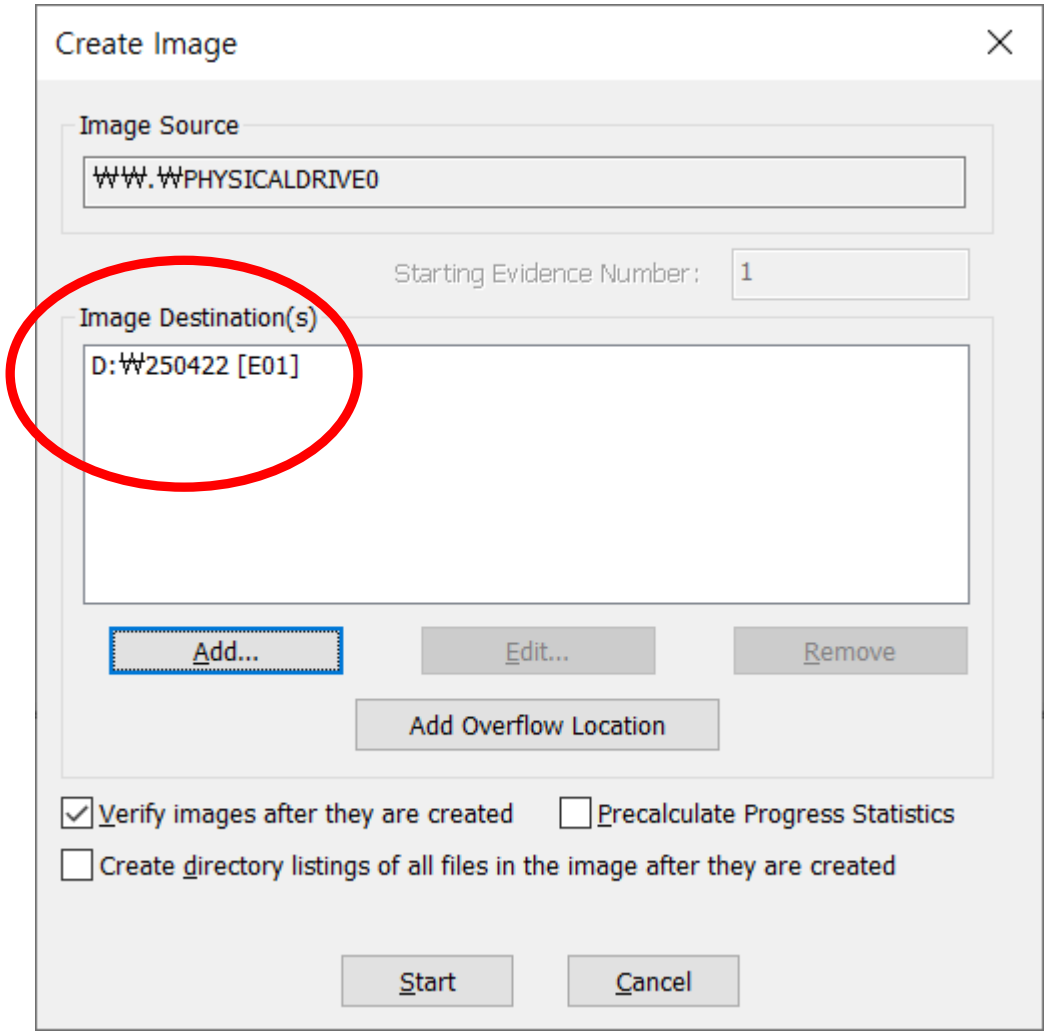




체크 박스는 이미지 파일에 대한 암호를 설정 하는 것임
설정을 하고 Finish를 하면 옆과 같은 창이 뜸

# FTK Imager - Create Disk Image



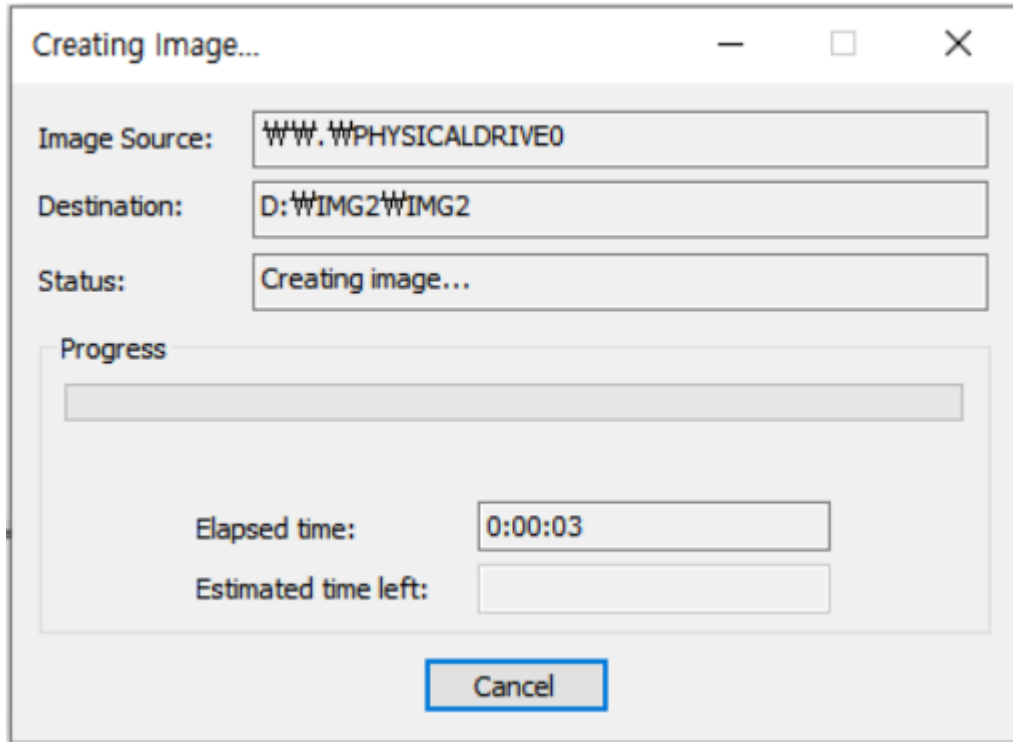
# FTK Imager - Create Disk Image

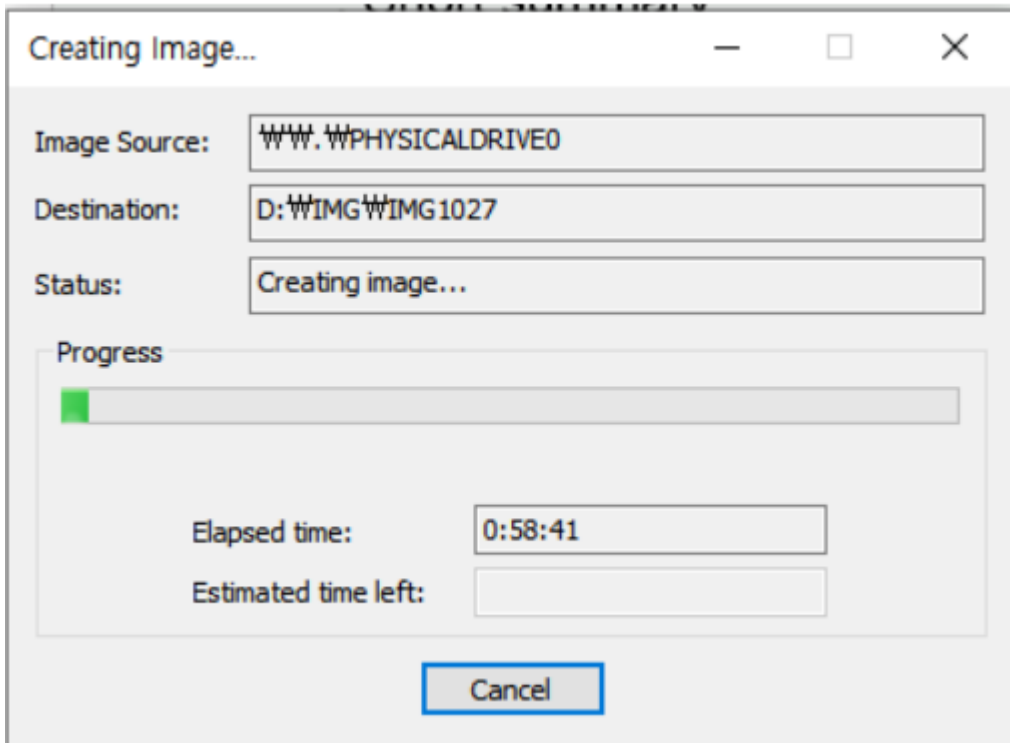



Start 누르면 이미지 덤프가 시작됨

컴퓨터와 디스크 용량에 따라 오래 걸릴 수 있다

# FTK Imager - Create Disk Image

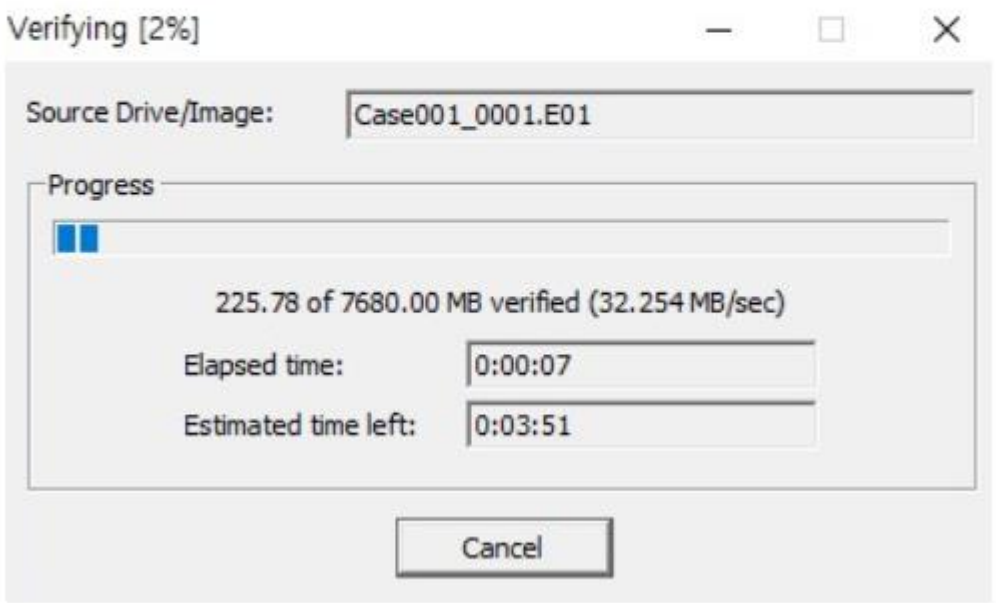


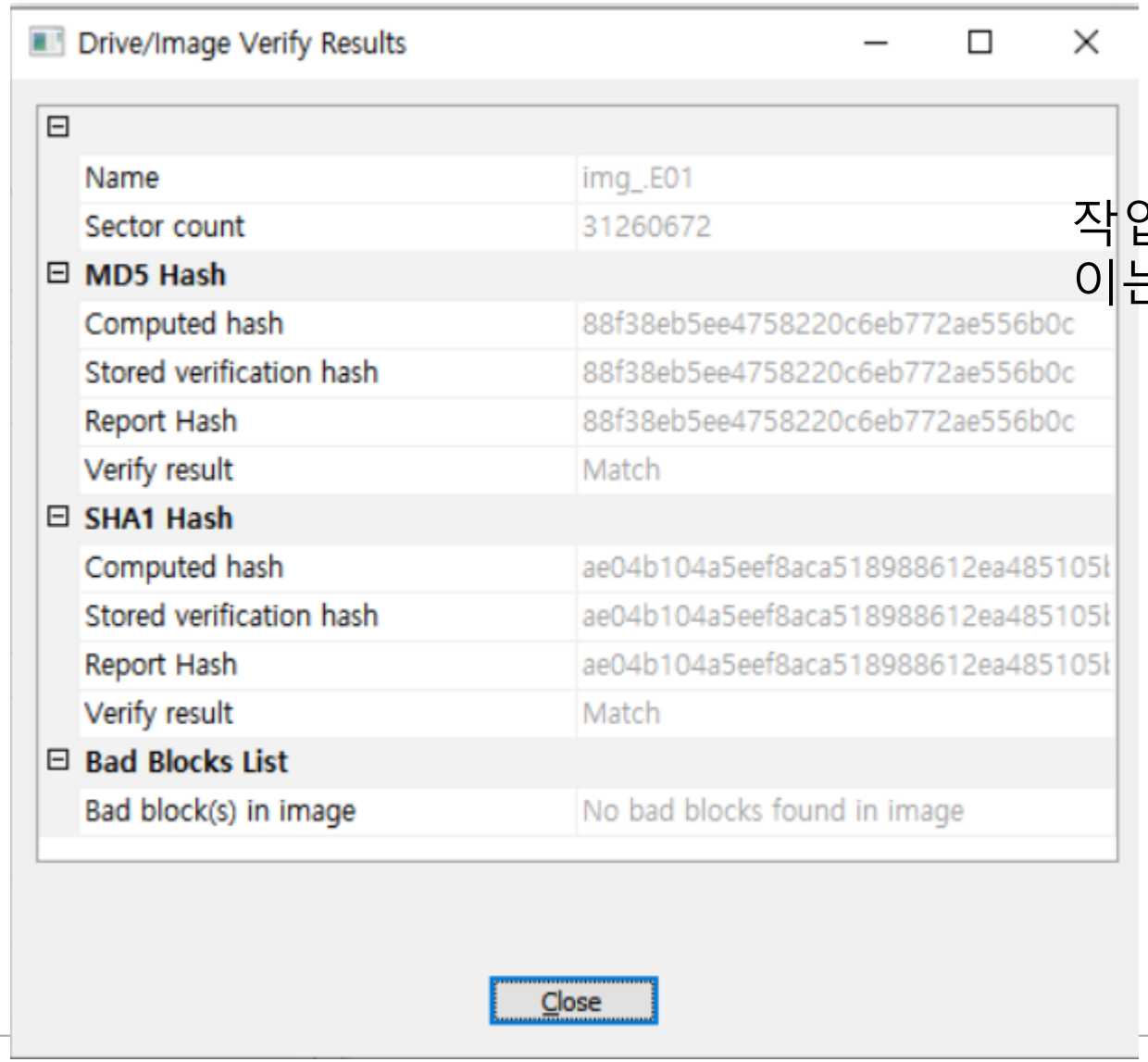
# FTK Imager - Create Disk Image

이미징이 완료되면 Successful 메시지가 나타나고

Verifying을 체크 하였다면 아래 그림과 같이 확인작업을 수행하게 됩니다.



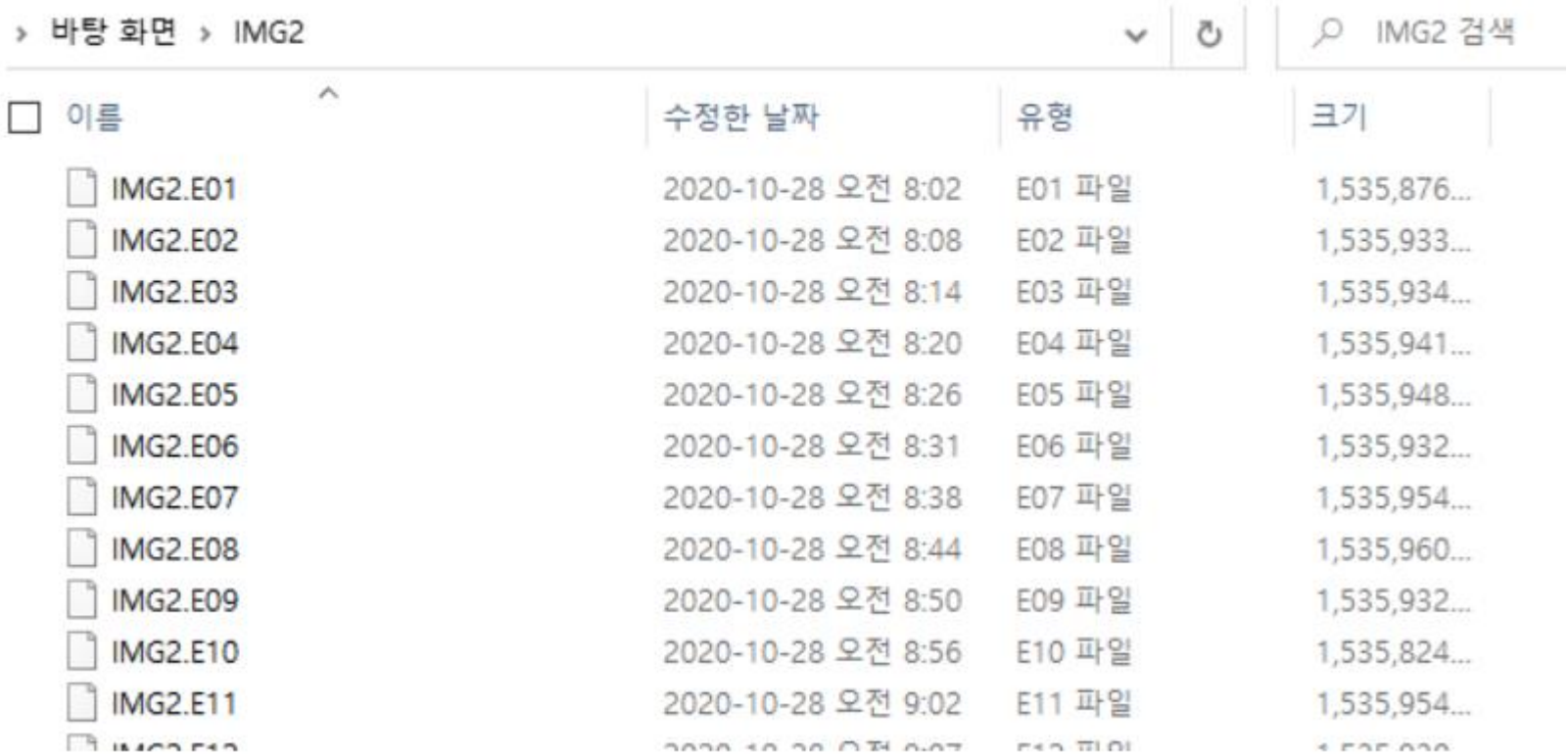
# FTK Imager - Create Disk Image




작업이 끝나면 Drive/Image Verify Results 가 나오고,
이는 증거의 무결성에 사용되는 해시값들을 보여줌

# FTK Imager - Create Disk Image

저장한 폴더에 가면 지정한 대로 1500MB 씩 끊어서 이미지가 저장된 것을 확인할 수 있다.



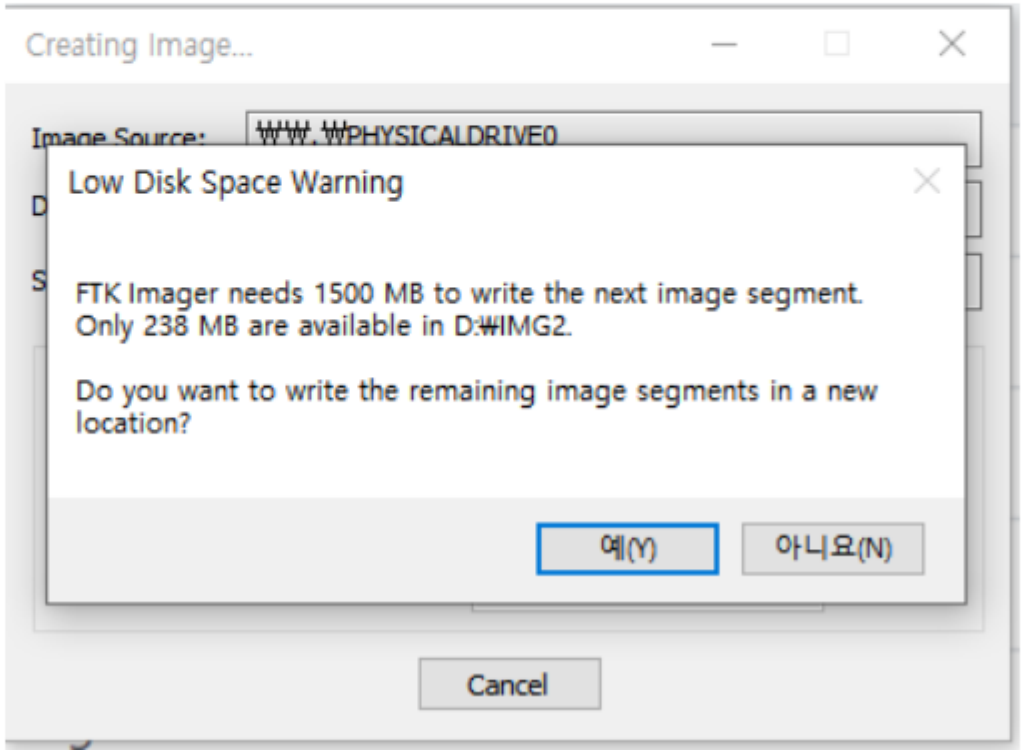

FTK Imager를 시용하여
증거 수집 대상 HDD에 대해 이미징을 수행하는 방법을 실습해 봤습니다.

# FTK Imager - Create Disk Image

+) 참고: **Low Disk Space Warning**

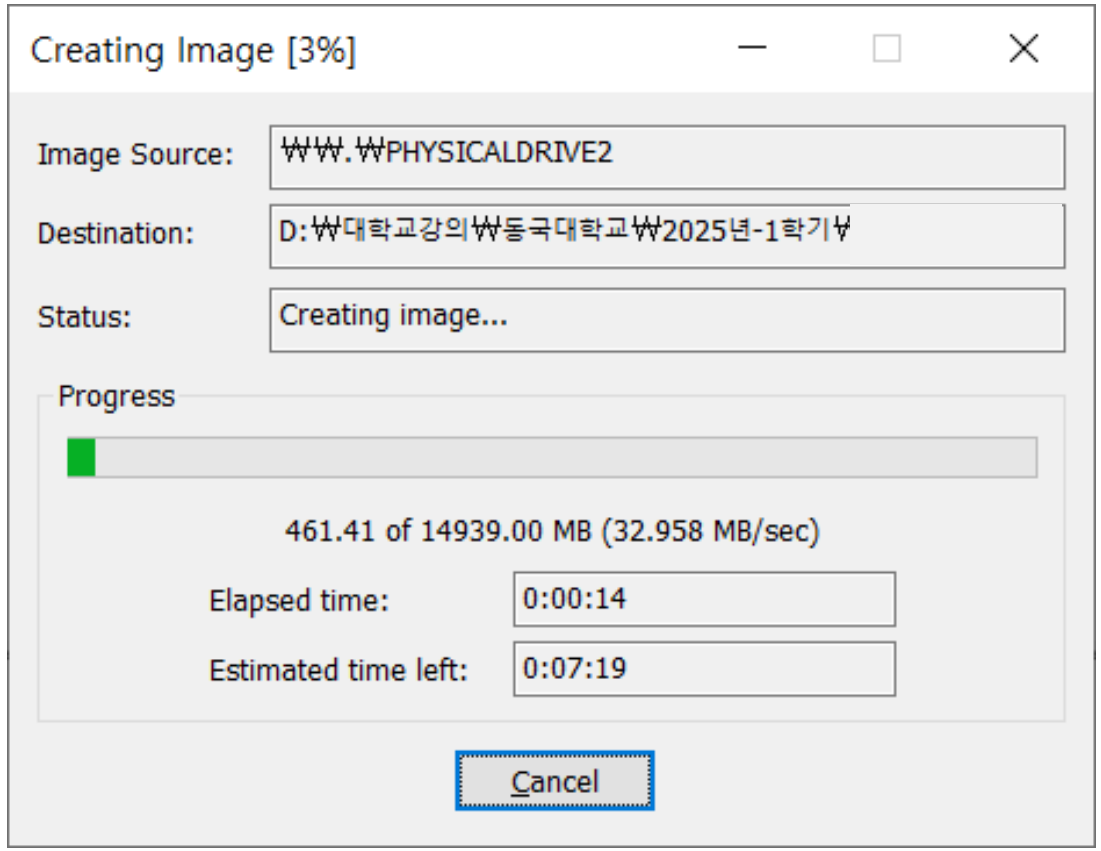
디스크 이미지 생성 중, 다음 화면이 뜨면 디스크 이미지를 저장할 공간이 부족하다는 것이다.

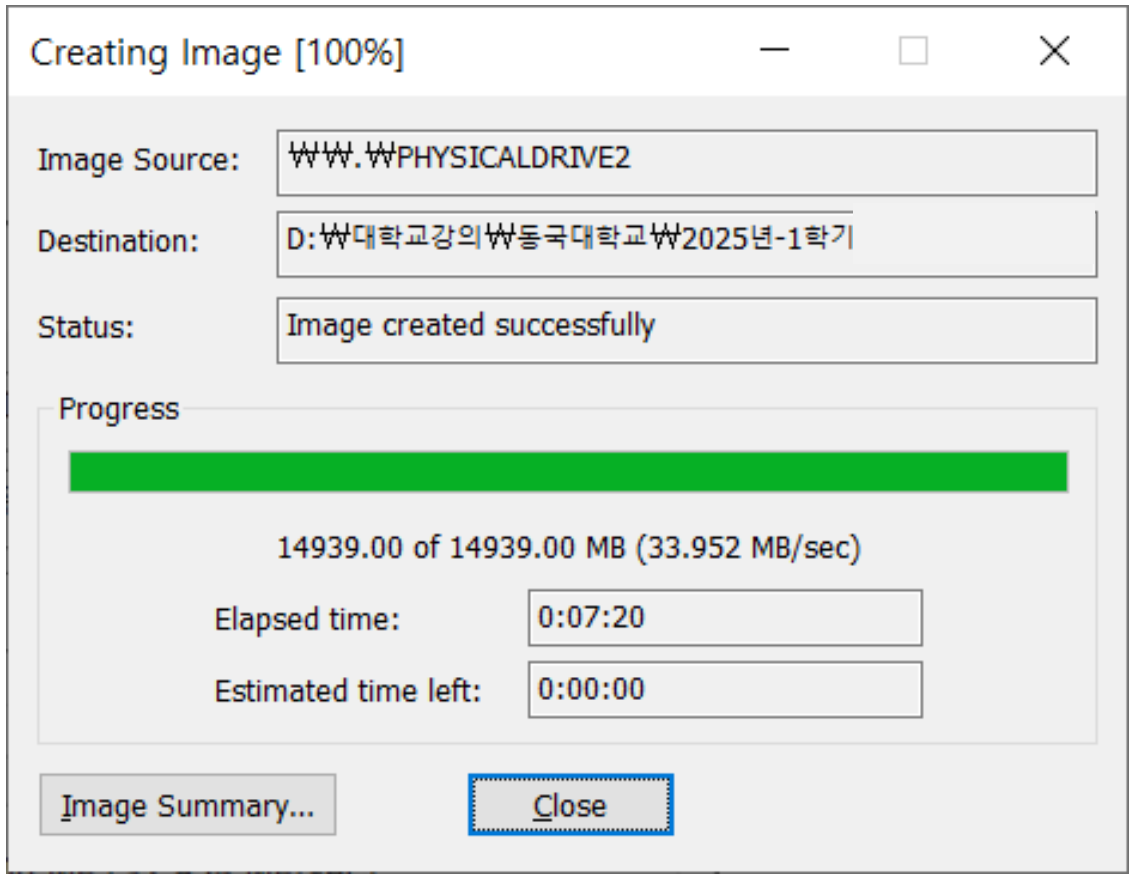
저장 공간을 더 만들어주거나, 다른 공간에다가 저장해주는 방법이 있다.



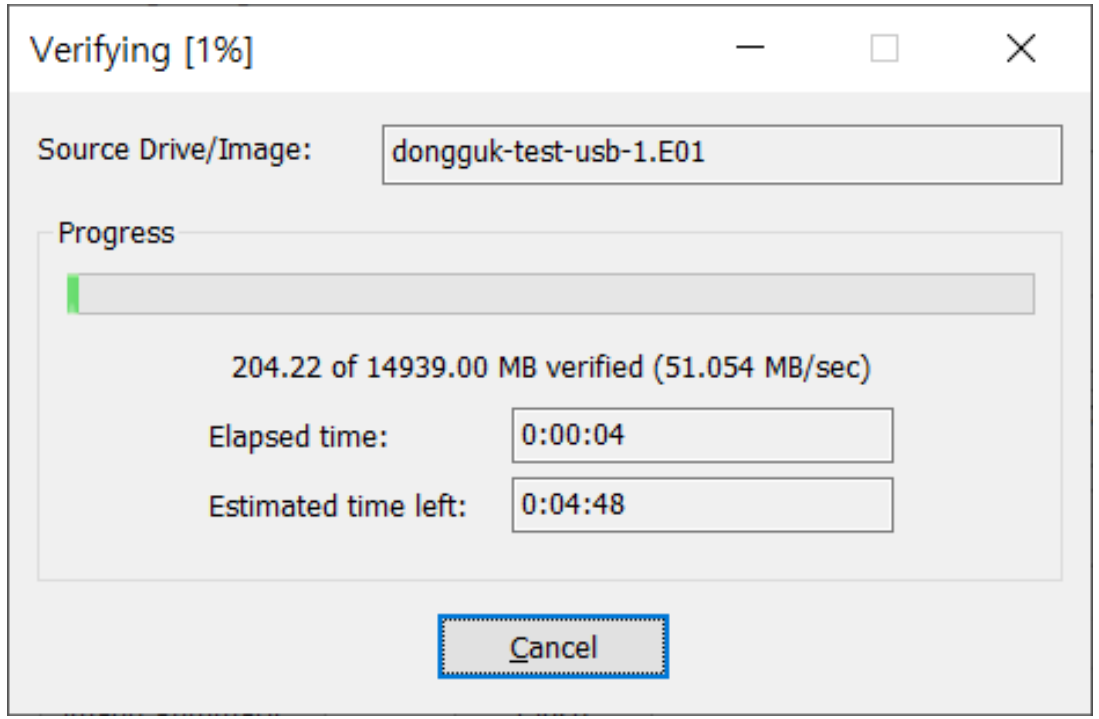
# FTK Imager - Create Disk Image - 실습

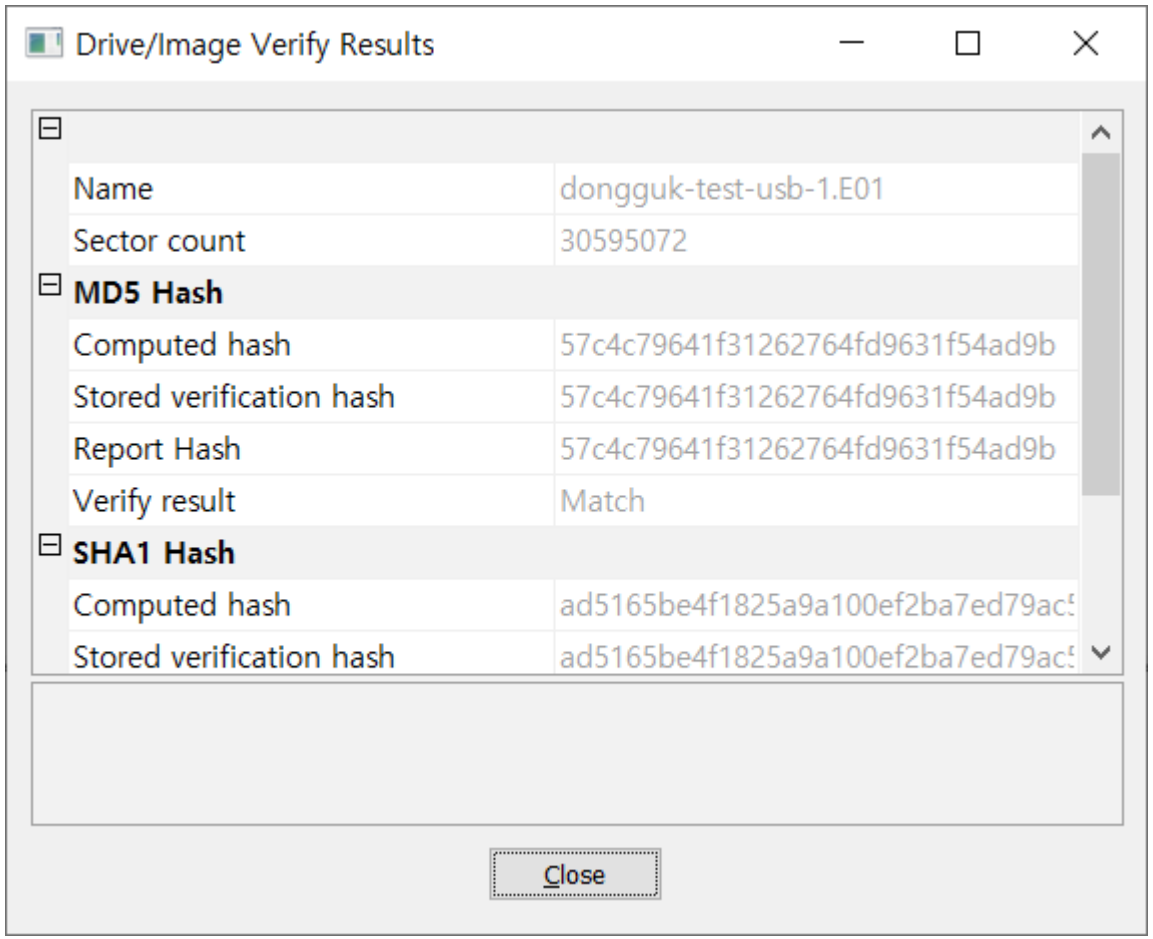
USB 1개를 IMG 만듬



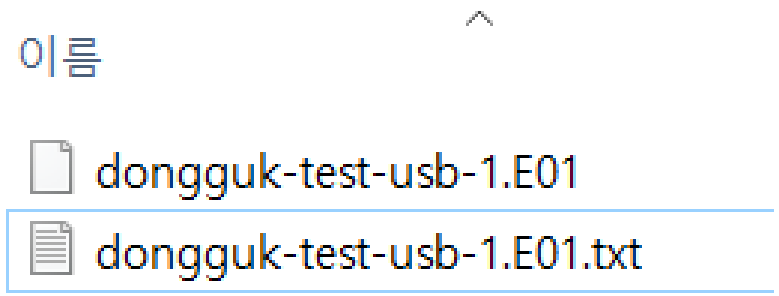



# FTK Imager - Create Disk Image - 실습

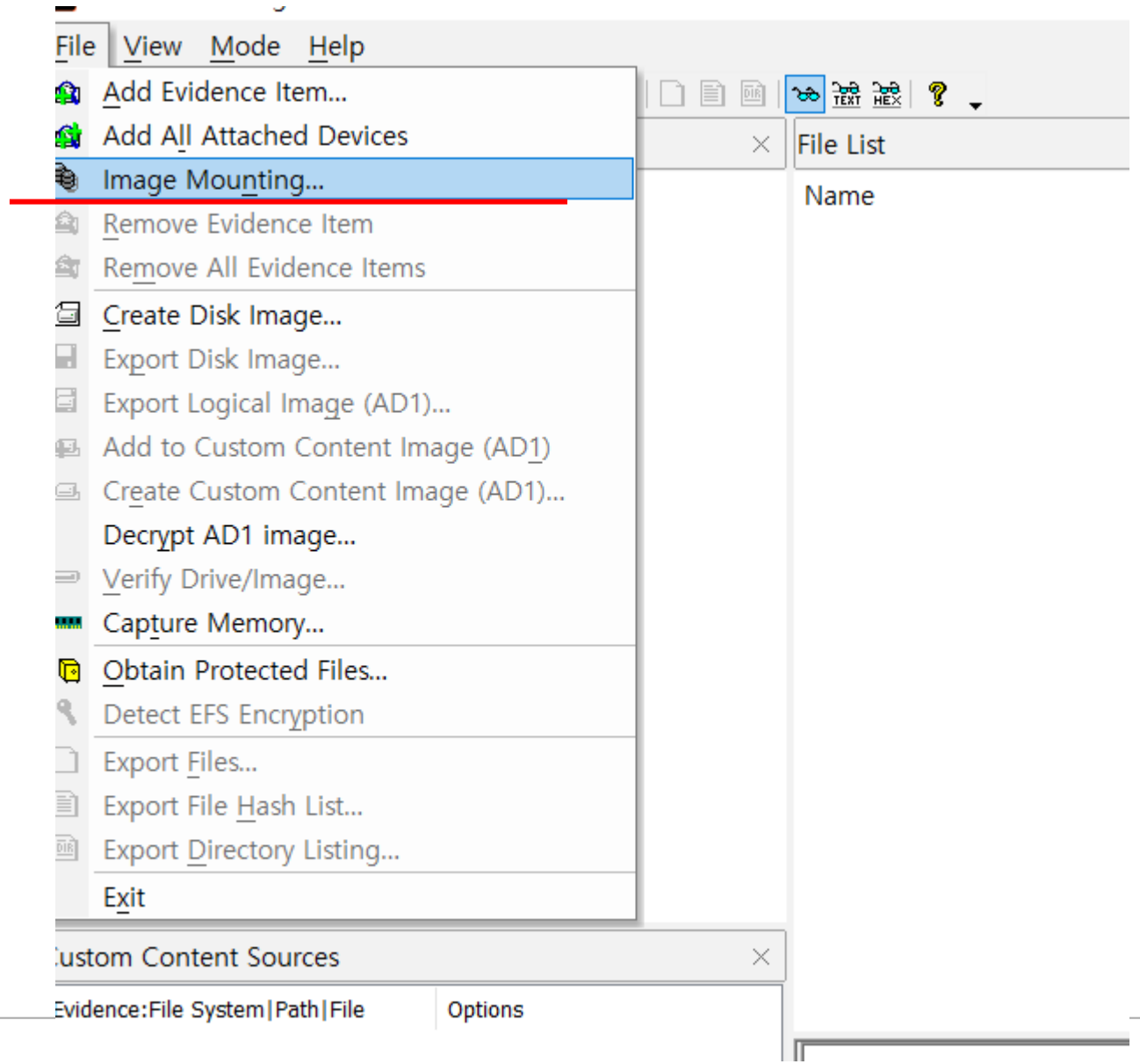


# FTK Imager - Create Disk Image - 실습

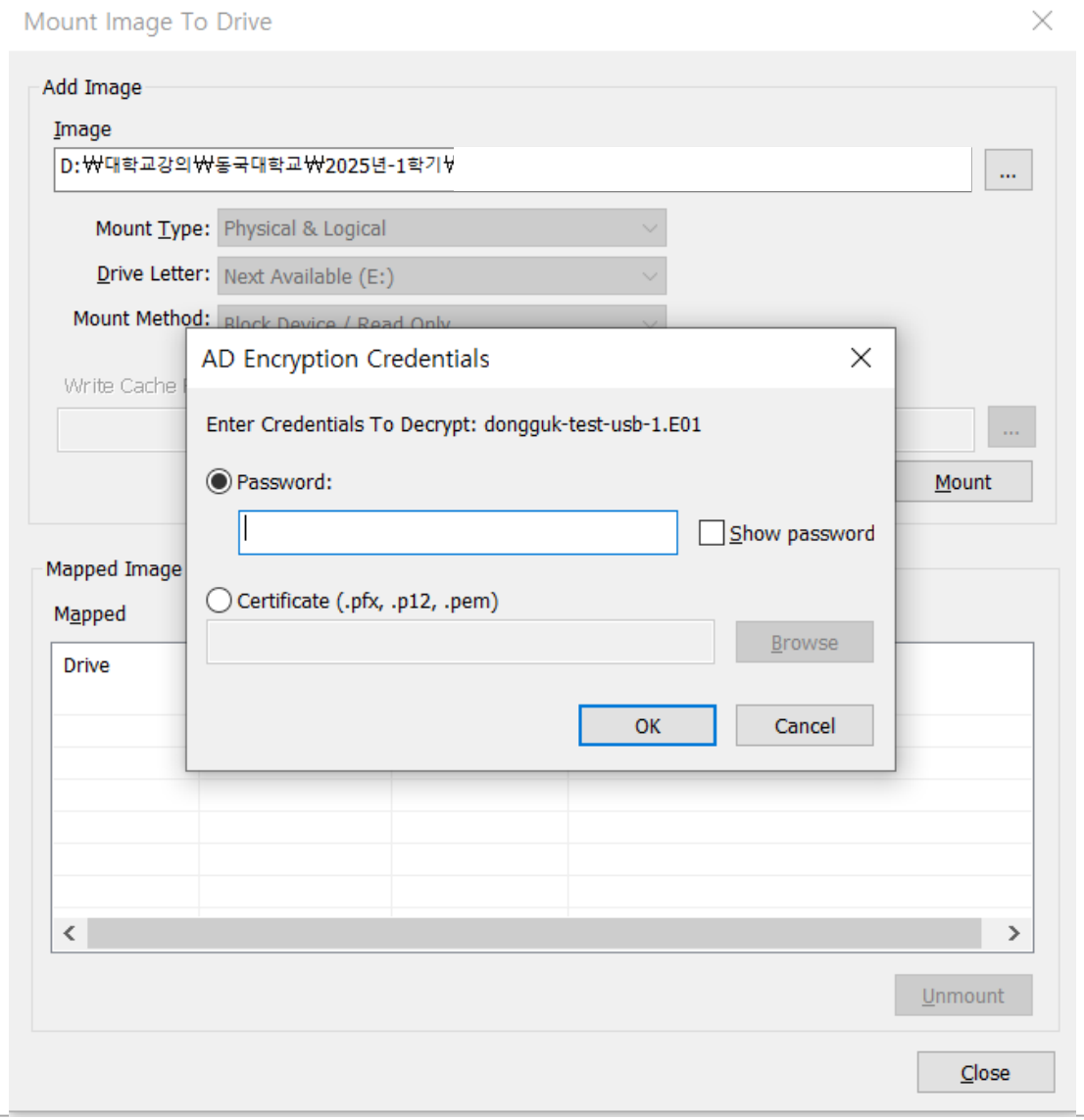


# FTK Imager - Create Disk Image - 실습

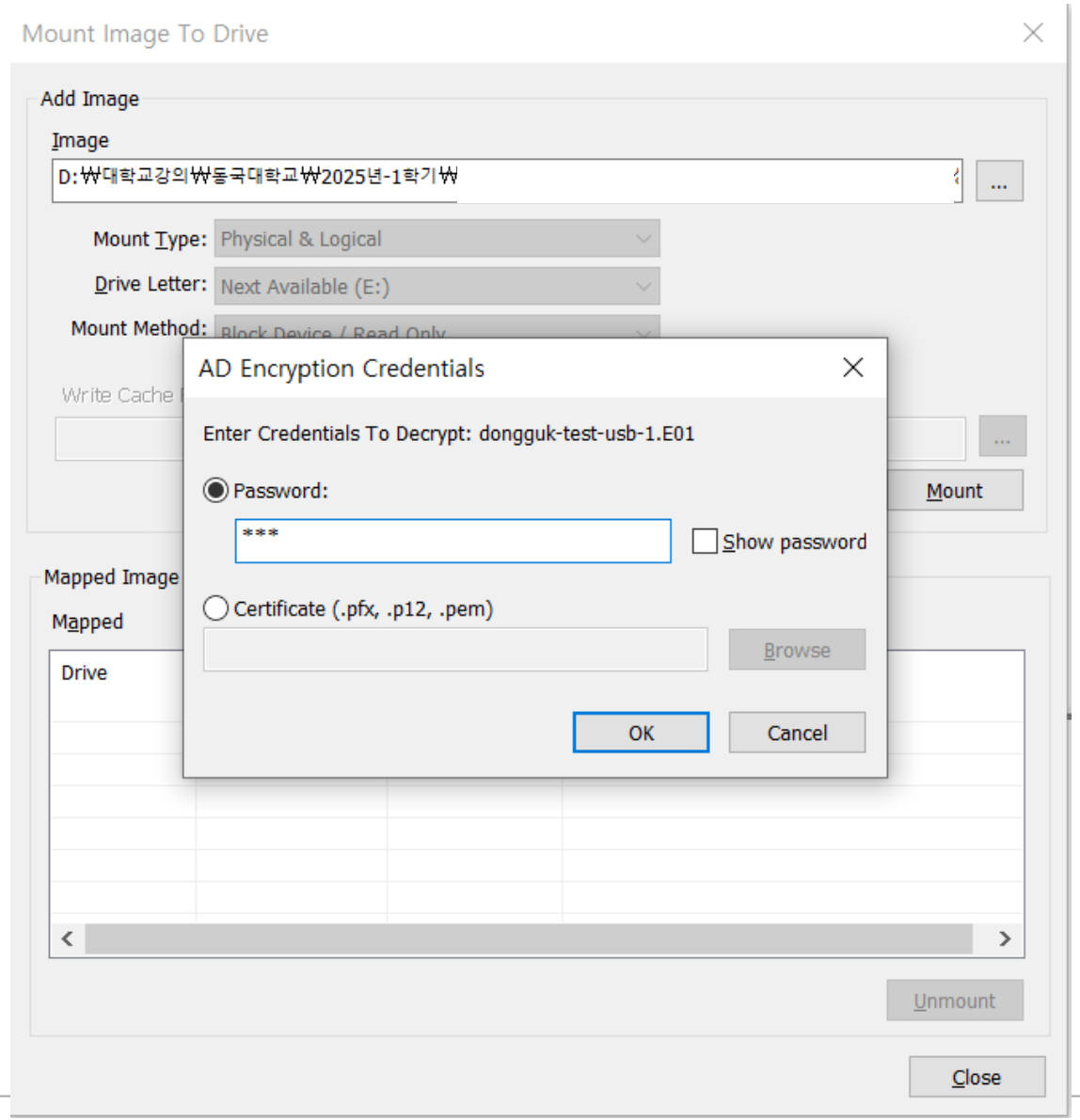


# FTK Imager - Create Disk Image - 실습

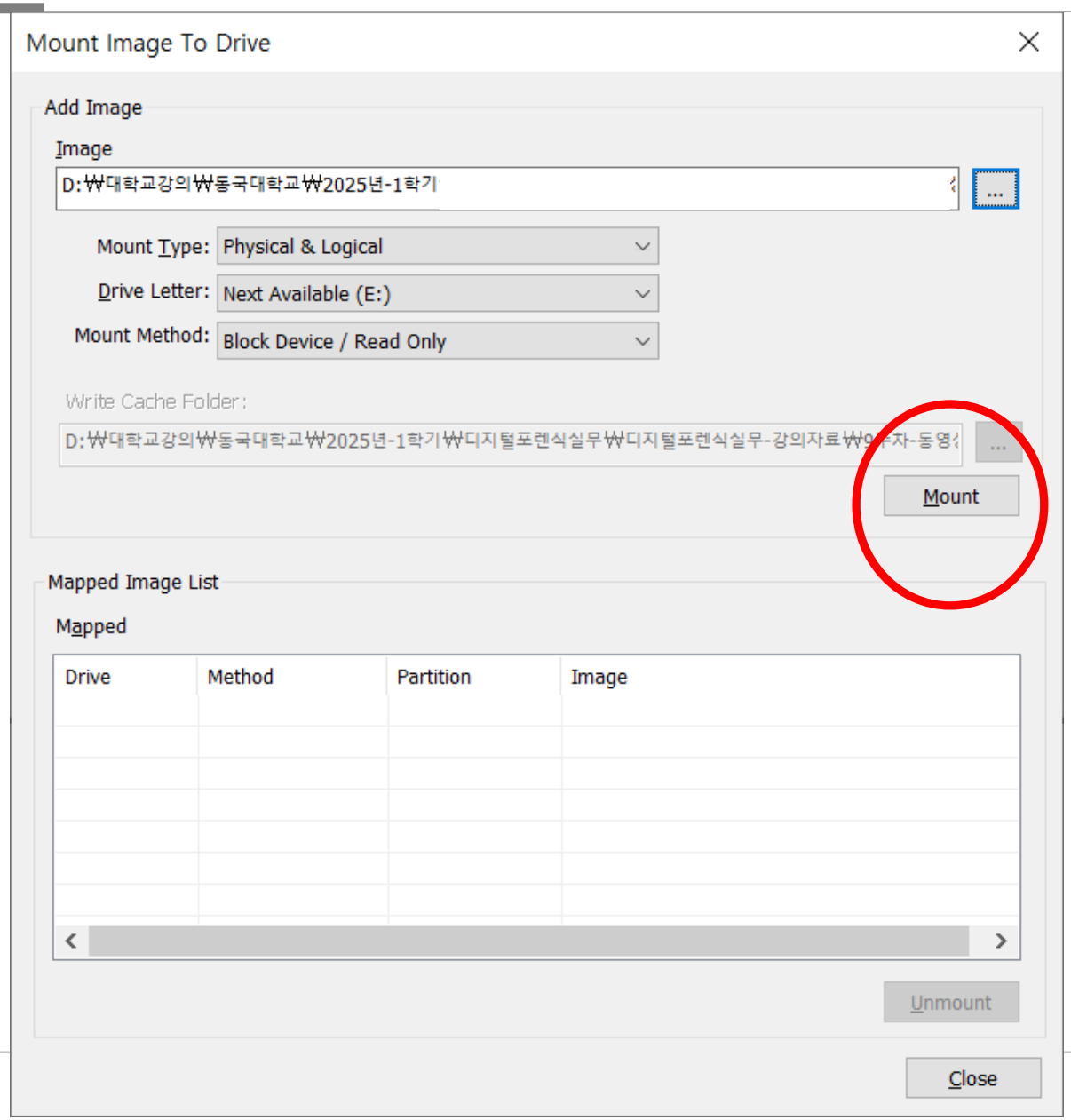
설정 했던
비번 입력



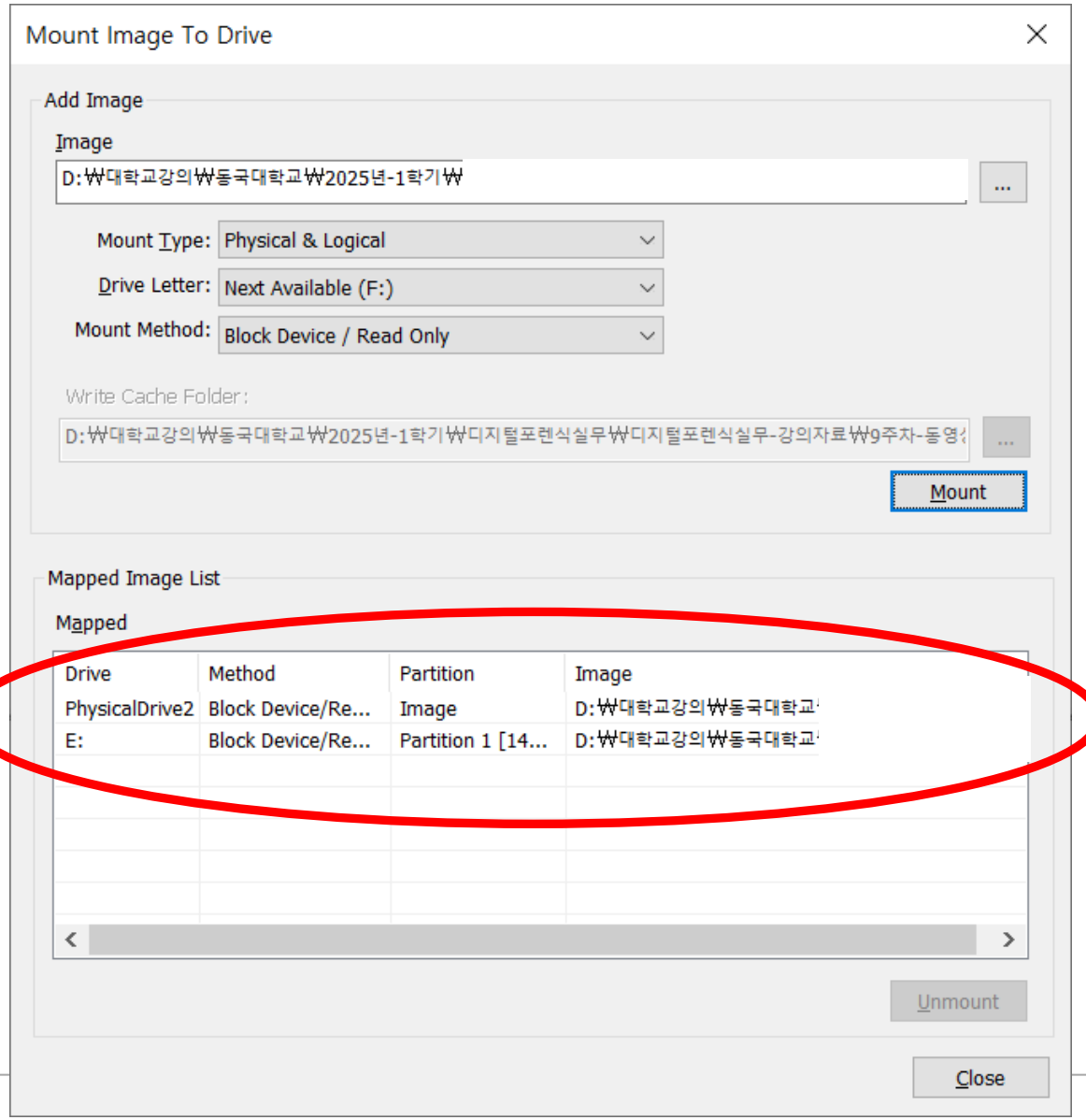
# FTK Imager - Create Disk Image - 실습



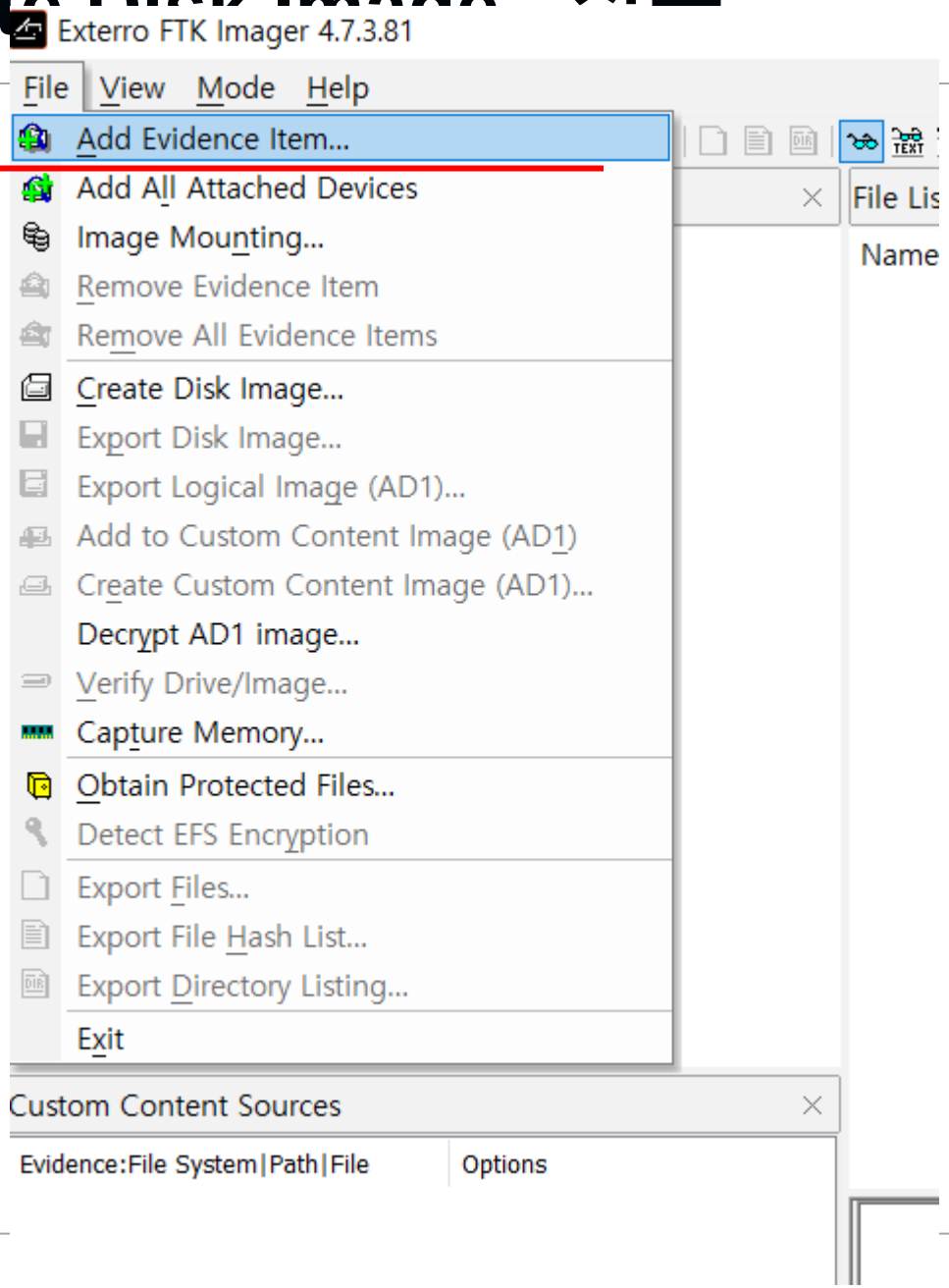
# FTK Imager - Create Disk Image - 실습



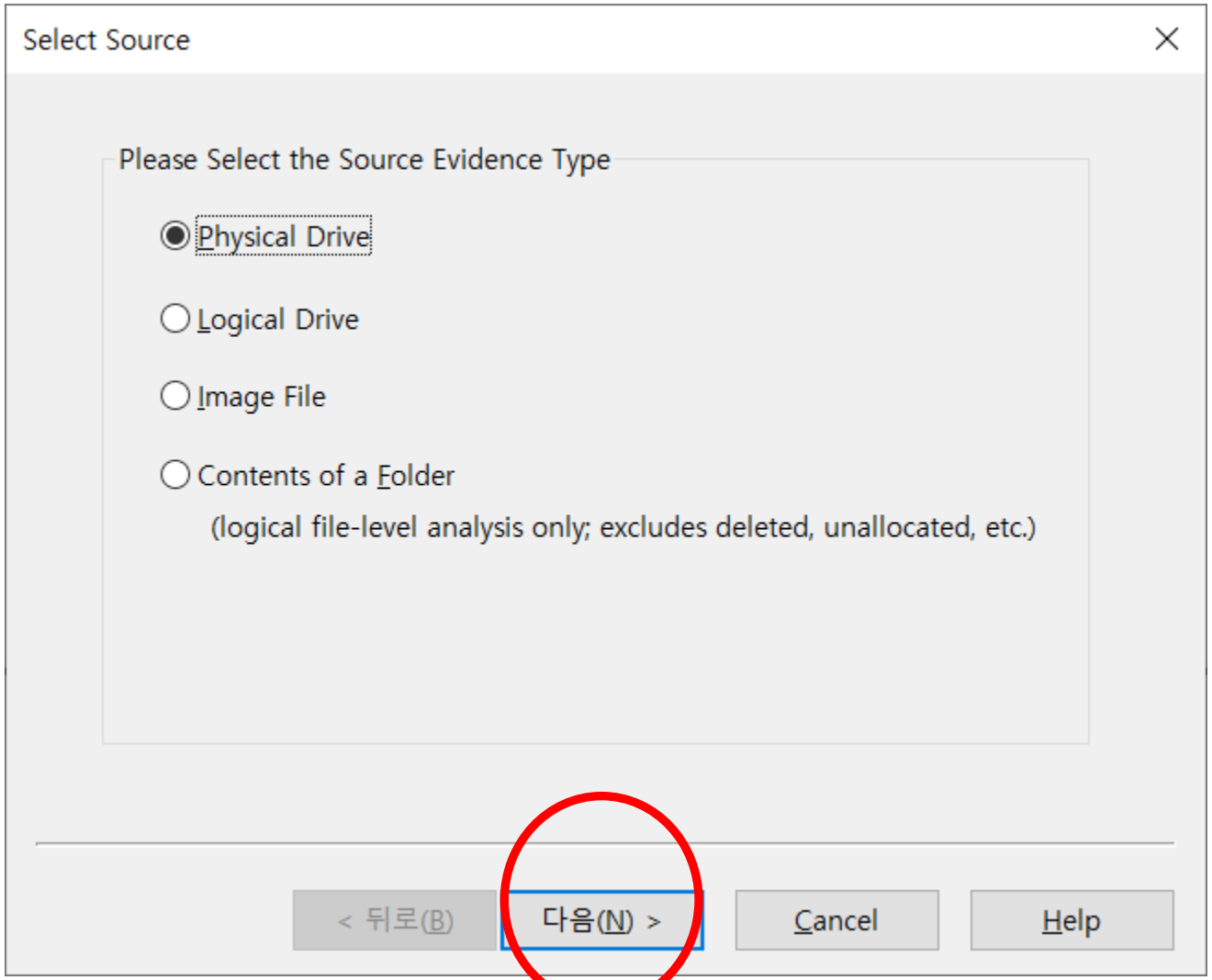
# FTK Imager - Create Disk Image - 실습



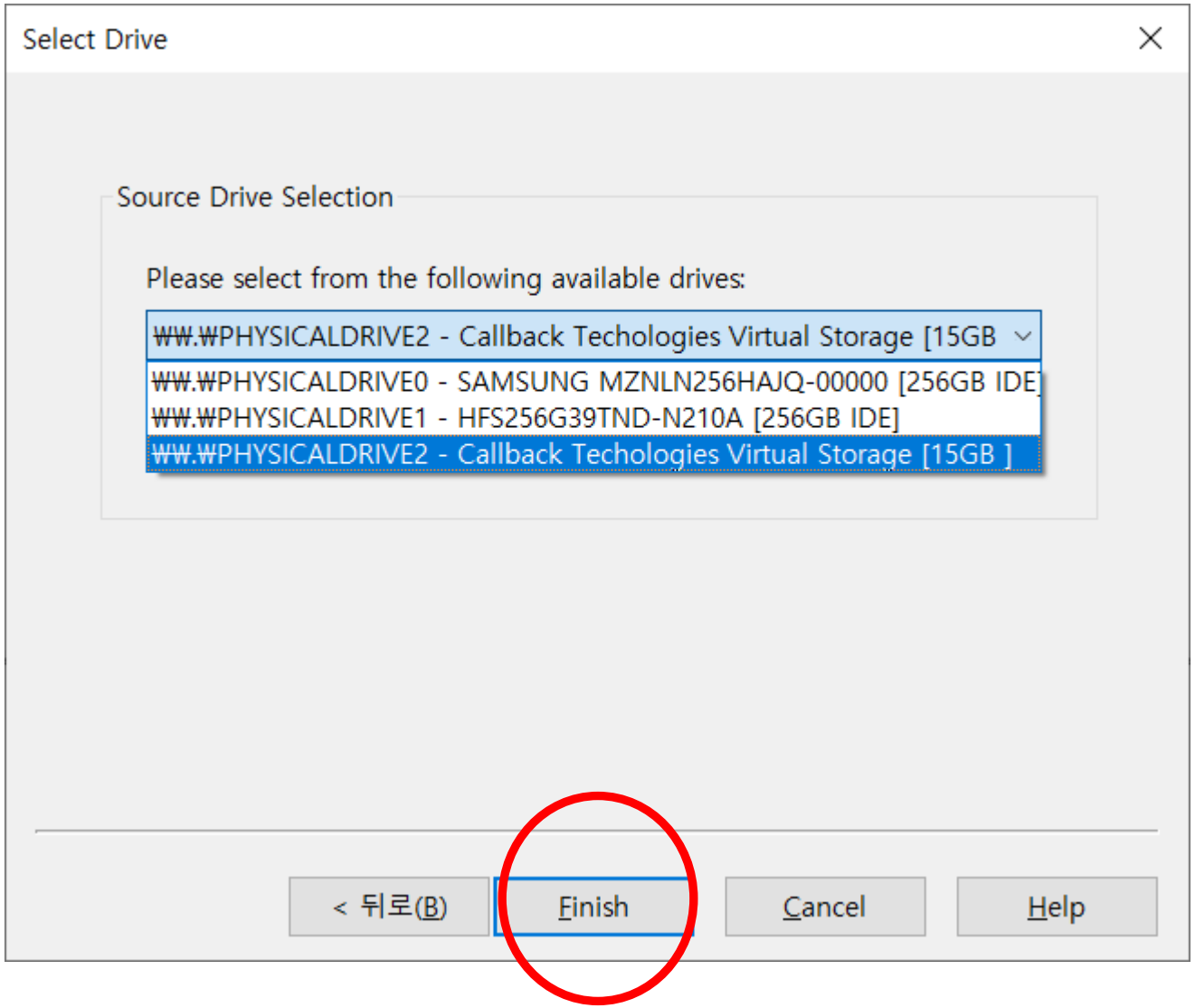
# FTK Imager - Create Disk Image 시스



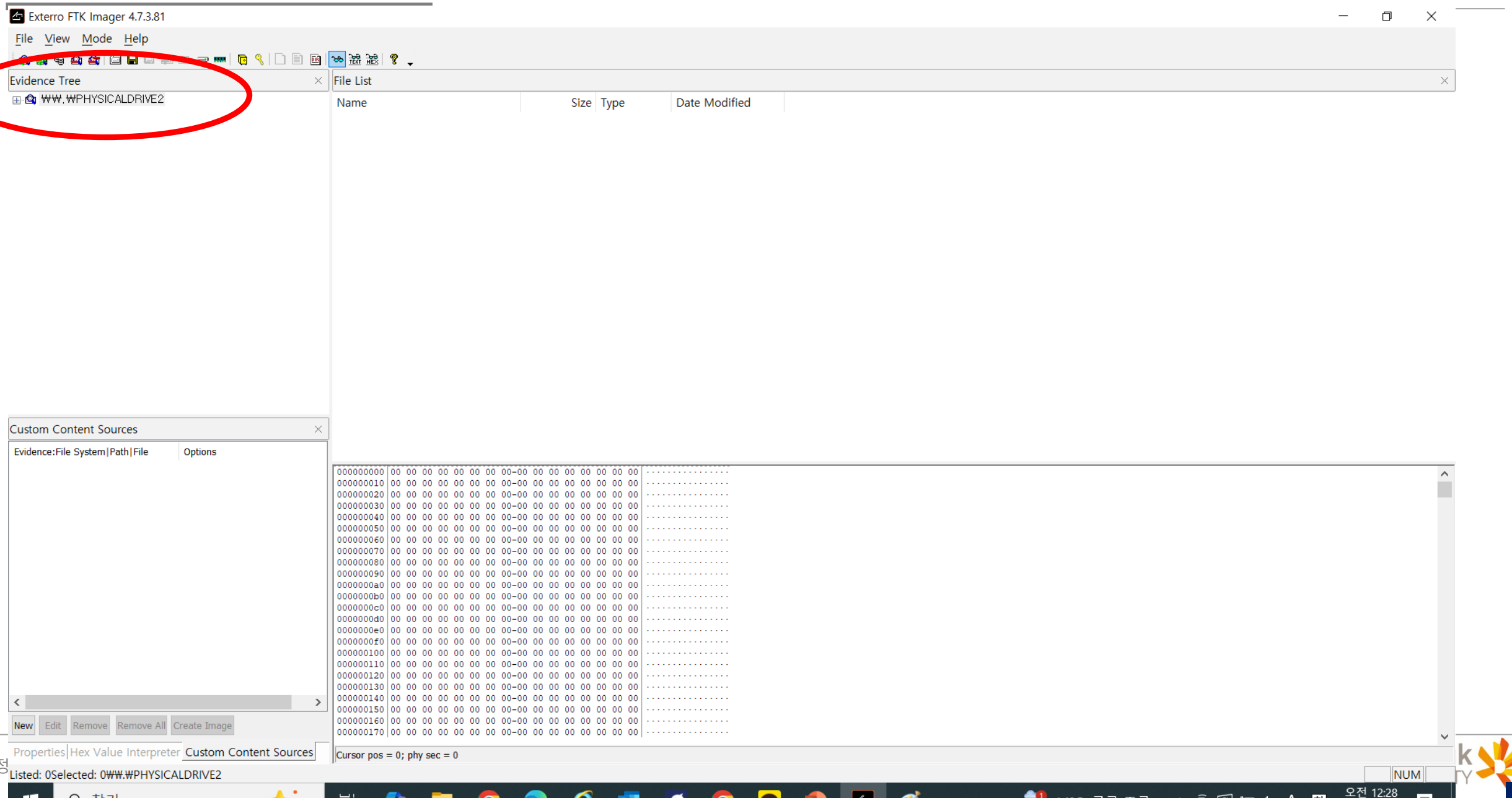
# FTK Imager - Create Disk Image - 실습



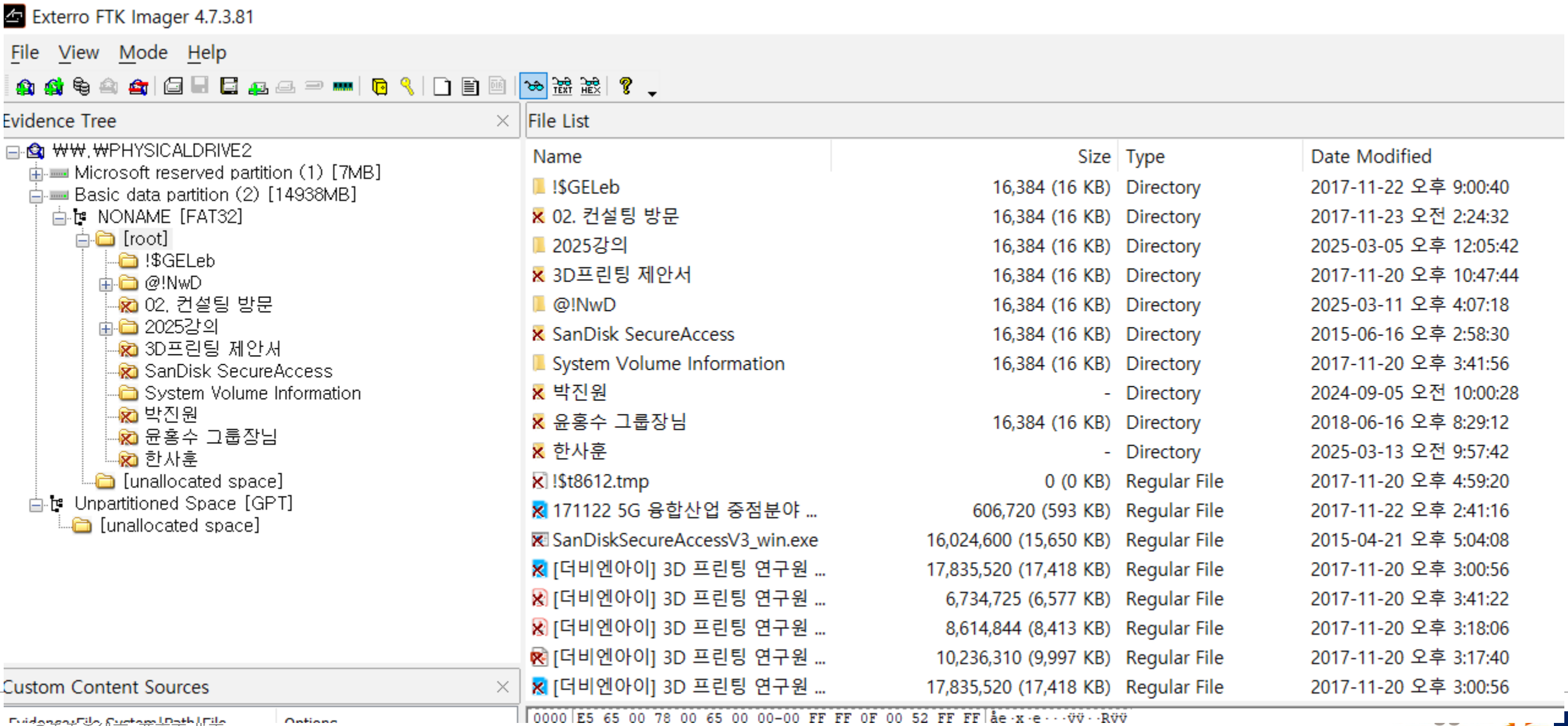
# FTK Imager - Create Disk Image - 실습



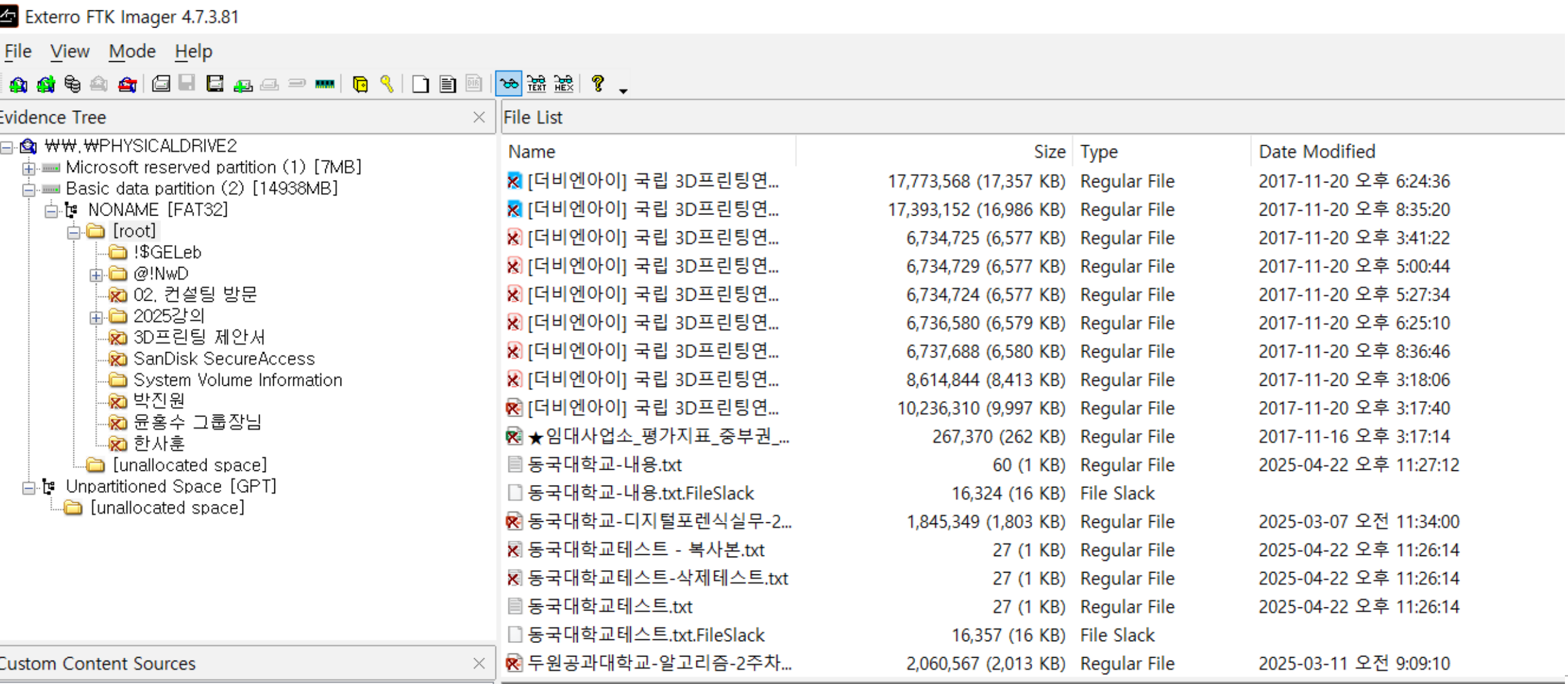
# FTK Imager - Create Disk Image - 실습



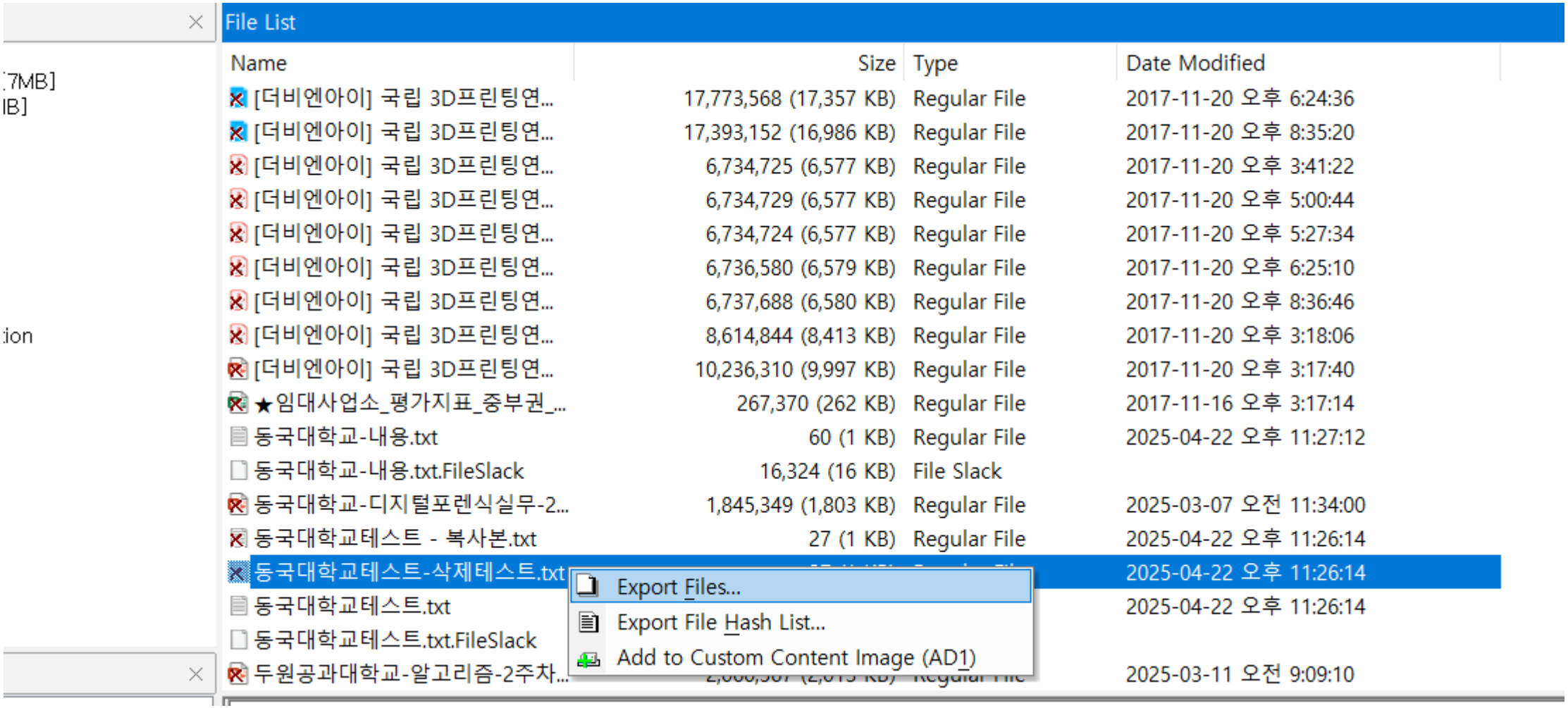
# FTK Imager - Create Disk Image - 실습



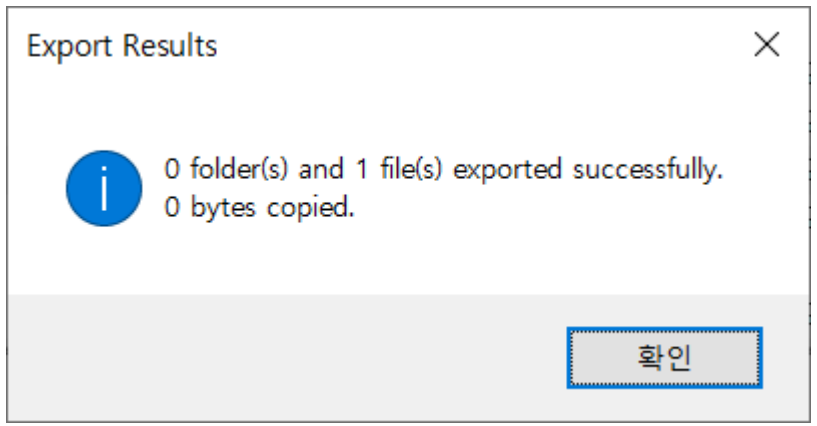
# FTK Imager - Create Disk Image - 실습

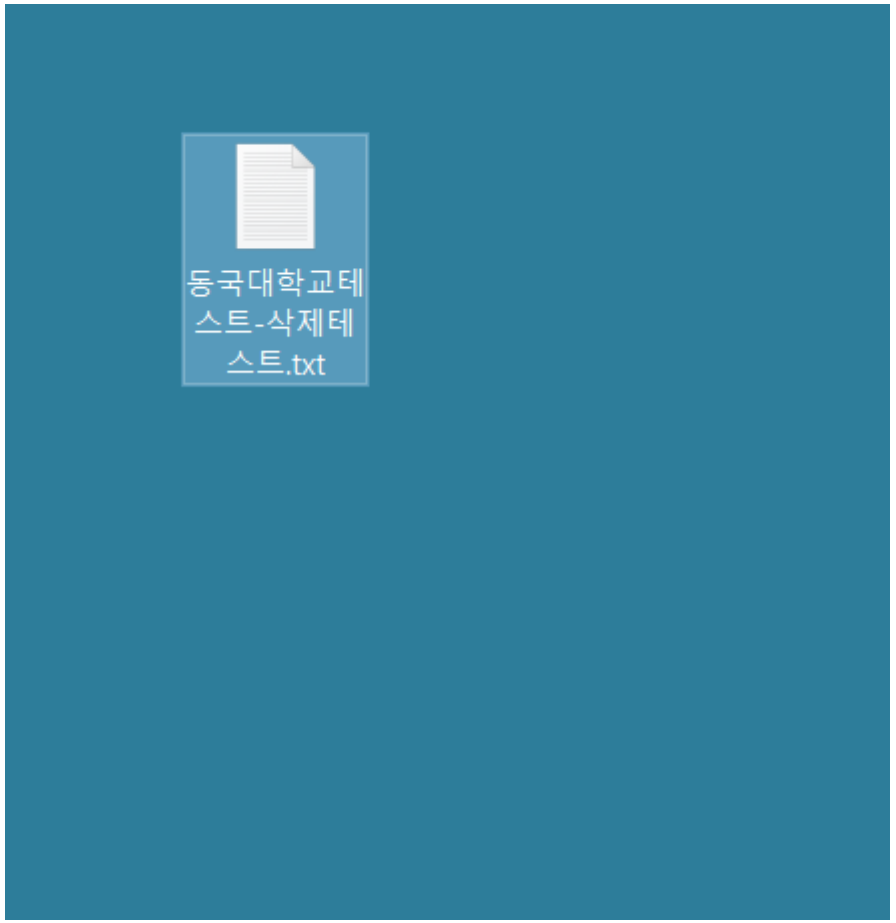


# FTK Imager - Create Disk Image - 실습

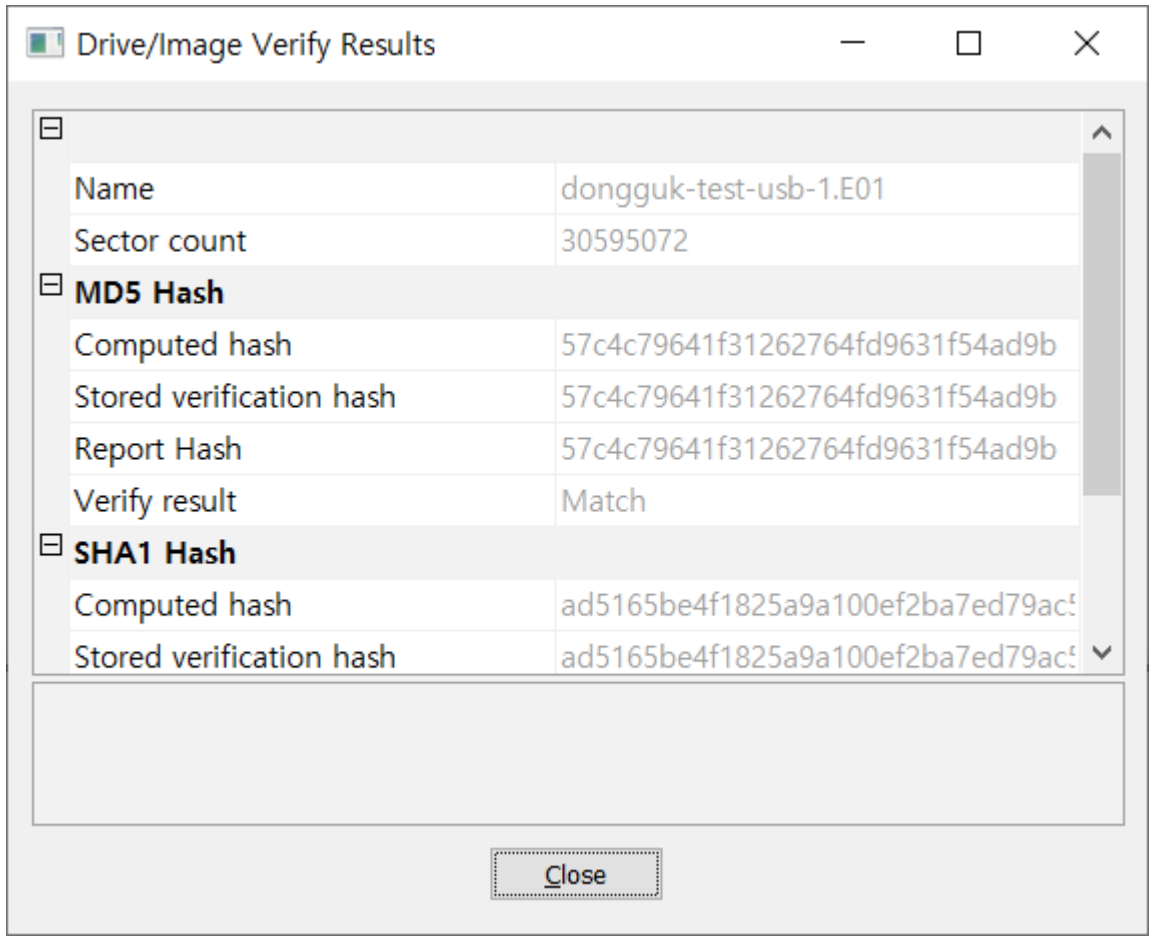


# FTK Imager - Create Disk Image - 실습

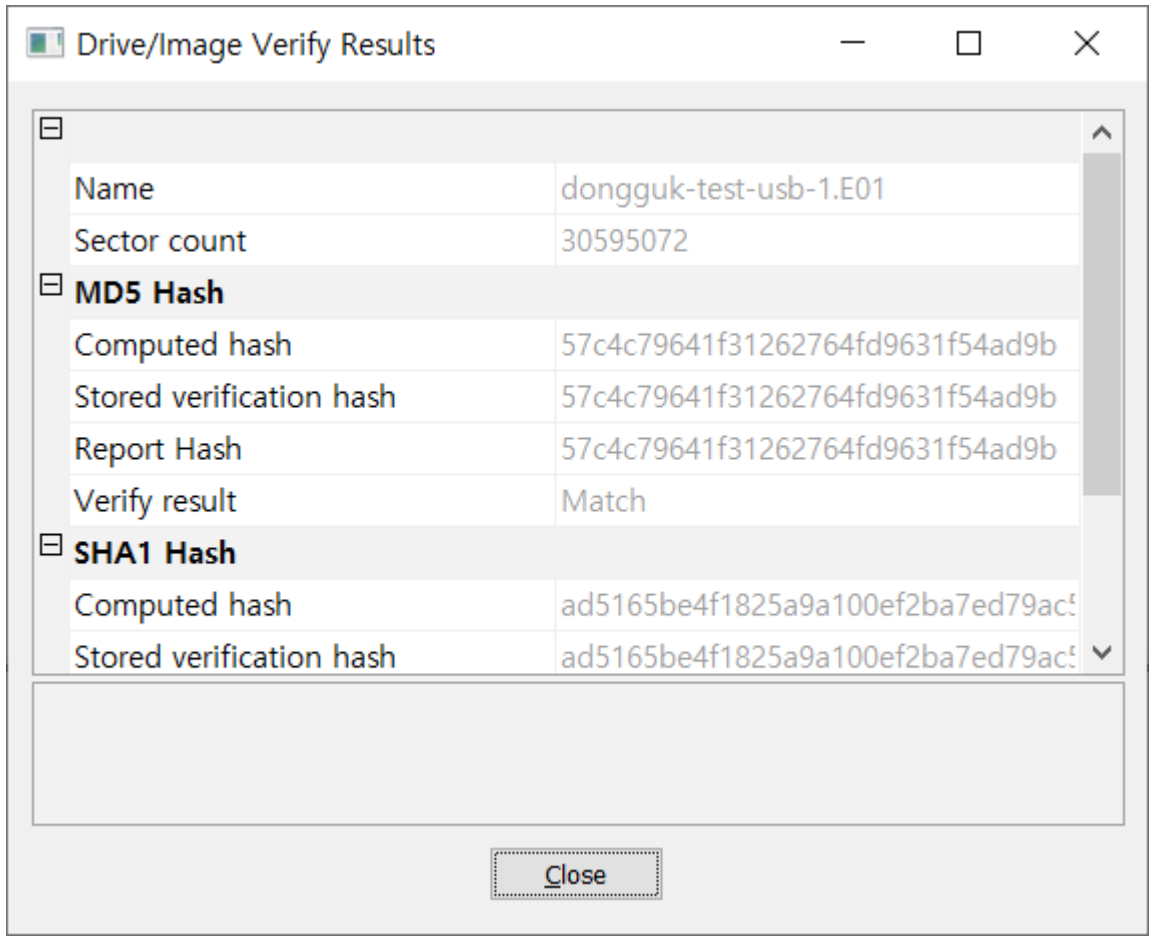


# FTK Imager - Create Disk Image – 실습- Hash값? 고민



# FTK Imager - Create Disk Image – 실습- Hash값? 고민




Computed Hash : 이미지 생성 끝난 후에 계산 (나중에 비교용)
Stored Verification Hash : 이미지 생성 당시에 저장된 값 (원본 무결성 기준값)

# FTK Imager - Create Disk Image – 실습- Hash값? 고민

FTK Imager는 이 둘을 비교 합니다

Stored Hash == Computed Hash

같으면 : “이미지가 완벽하게 만들어졌습니다.”
다르면 : “이미지 생성 중 오류 또는 변경이 발생했습니다.”

**“복사된 이미지가 원본과 완전히 동일하며, 과정 중 변경이 없었다”는 것을 입증합니다.**

# 퀴즈

Q1. FTK Imager에서 “Stored Verification Hash”는 언제 생성되는가?

A. 디스크 이미지를 열 때

**B**. 이미지 생성 도중 원본을 읽으면서 계산된 값

C. 이미지 생성 완료 후 다시 계산된 값

D. 사용자가 수동으로 입력하는 값

Stored Hash는 디스크를 복사하면서 동시에 계산되고, 이미지 파일 내에 저장

# 퀴즈

Q2. 다음 중 FTK Imager에서 "Computed Hash"의 용도는 무엇인가요?

A. 사용자의 암호를 복구하기 위해

B. 원본 파일 이름을 저장하기 위해

**C**. 이미지 생성 후 무결성을 확인하기 위해

D. 삭제된 파일을 복원하기 위해

이미지 생성 후 다시 계산하여 저장된 Hash 값과 일치하는지 비교

# 퀴즈

O, X

Q3. Computed Hash와 Stored Hash가 다르면, 디스크 이미지에 변경이 있었던 것으로 본다.

정답: O

정답: 두 값이 다르면 이미지 생성 과정에서 오류가 발생했거나, 이미지가 손상/조작되었을 가능성이 있다

# 퀴즈

O, X

Q4. FTK Imager는 이미지 생성 시 MD5 해시만 사용하고, SHA1은 선택 사항이다.

정답: X

FTK Imager는 기본적으로 MD5와 SHA1을 함께 계산
MD5/SHA1은 기본값

# Thank you for Listening

새로운 세상과 변화에 도전하는 동국대인이 되기를 바랍니다.