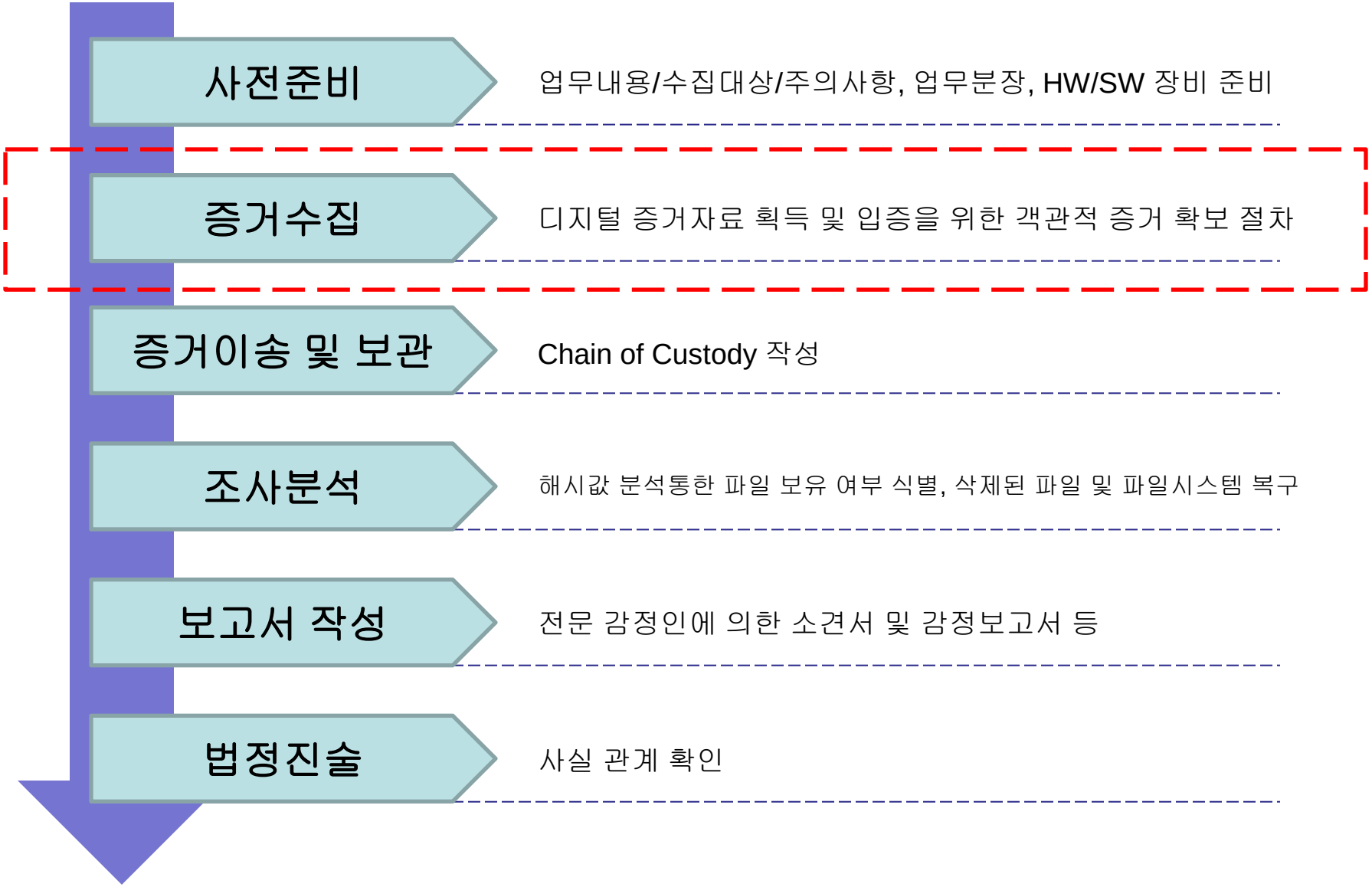
컴퓨터보안 실습

포렌식 실습

논리적 쓰기방지 및 이미지 생성

디지털포렌식 절차

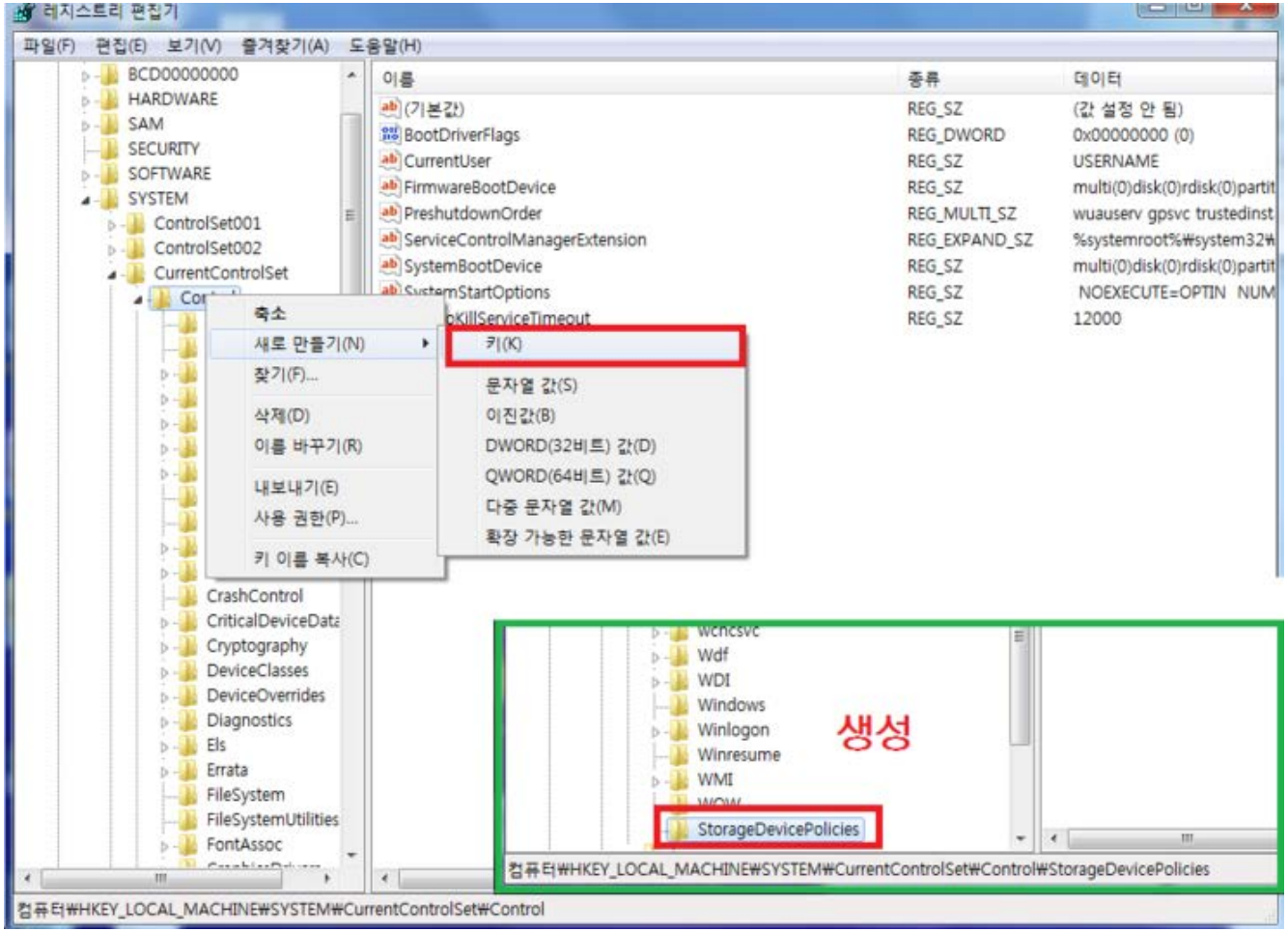

사전준비
업무내용/수집대상/주의사항, 업무분장, HW/SW 장비 준비
증거수집
디지털 증거자료 획득 및 입증을 위한 객관적 증거 확보 절차
증거이송 및 보관
Chain of Custody 작성
조사분석
해시값 분석통한 파일 보유 여부 식별, 삭제된 파일 및 파일시스템 복구
보고서 작성
전문 감정인에 의한 소견서 및 감정보고서 등
법정진술
사실 관계 확인

논리적 쓰기 방지

1. 레지스트리 수정을 통한 쓰기 방지

레지스트리 수정 - NTFS파일시스템(Win7) 레지스트리 수정 [오타나면 안됨]
Key: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies
Name : WriteProtect
Value : 0x00000000(쓰기방지 해제), 0x00000001(쓰기방지 설정) Dword 생성

논리적 쓰기 방지



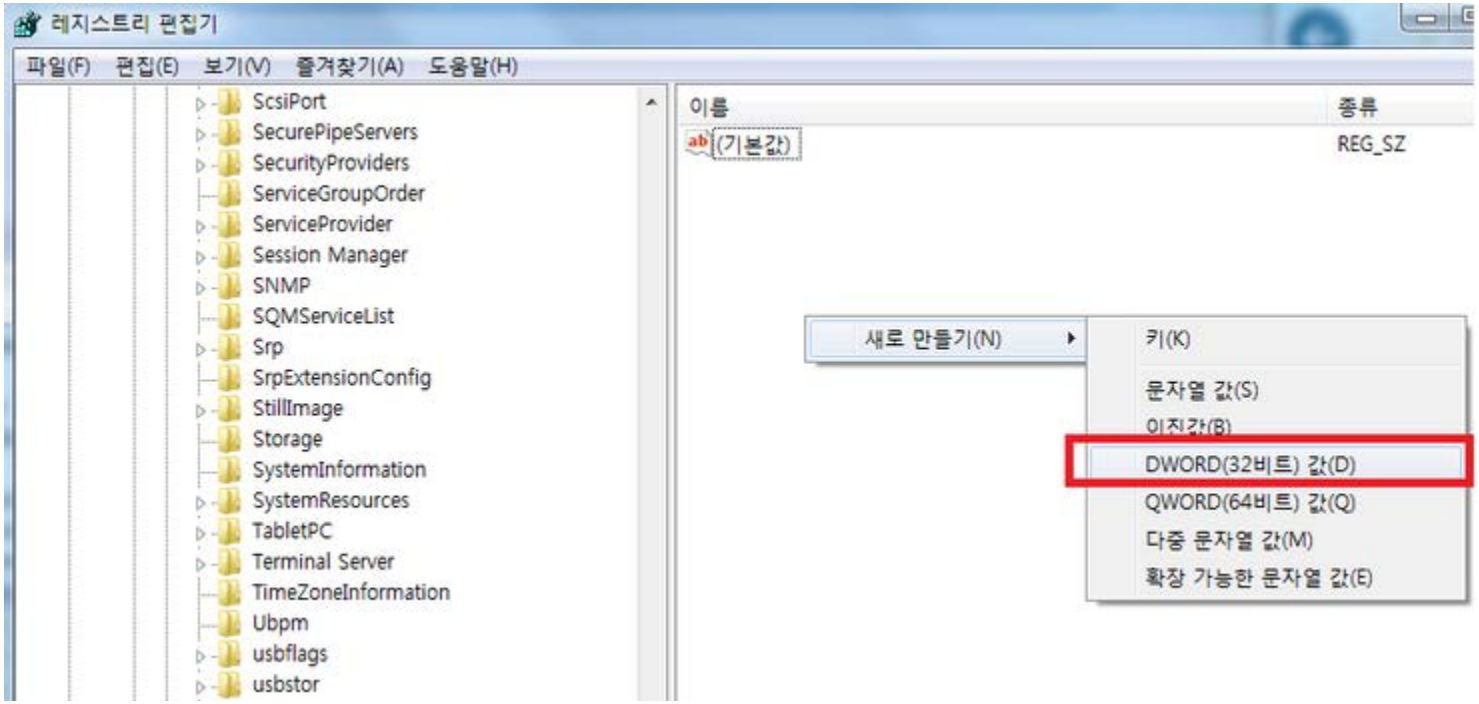
레지스트리 수정 - NTFS파일시스템(Win7) 레지스트리 수정 [오타나면 안됨]

Key: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies

Name : WriteProtect

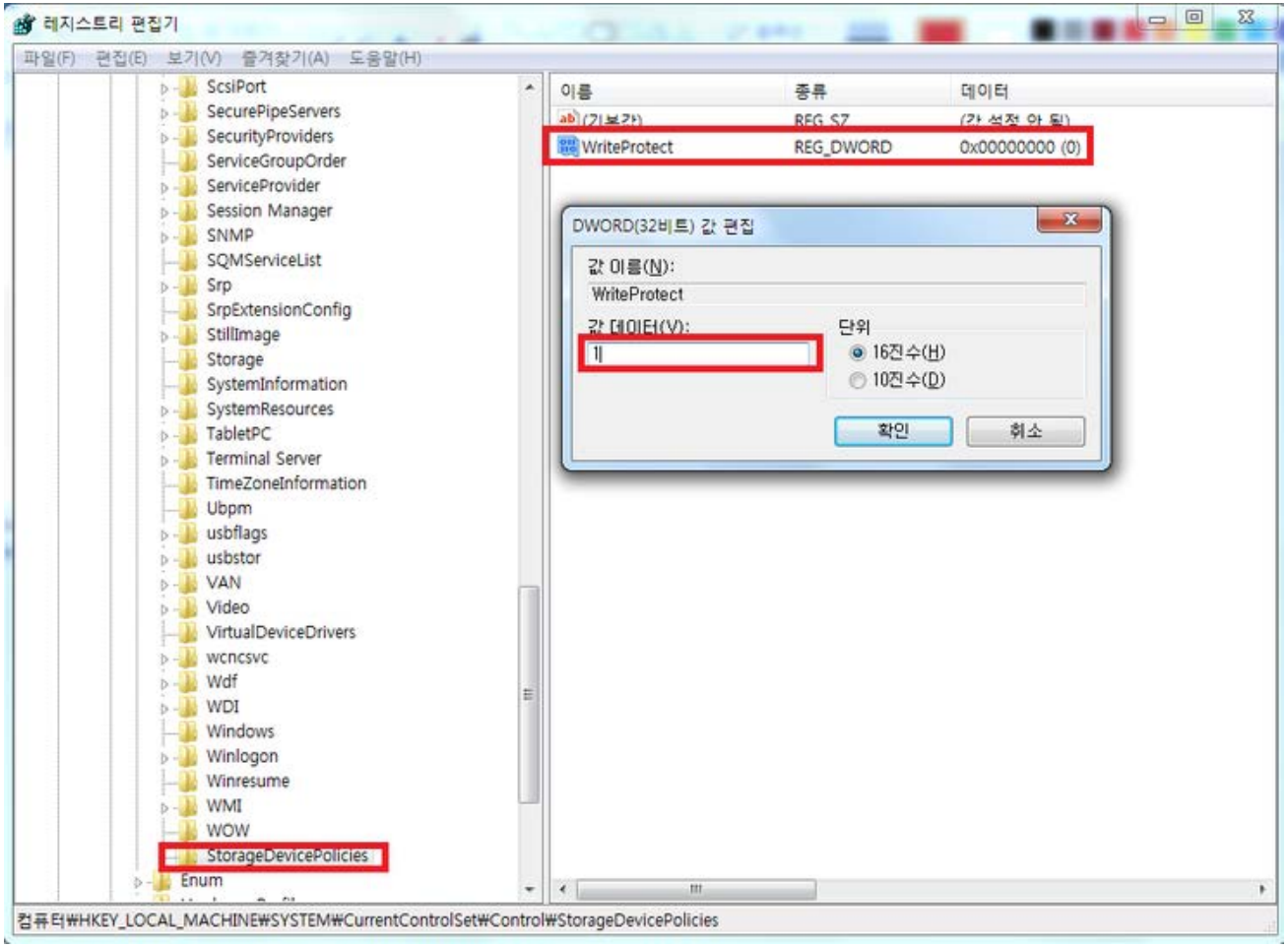
Value : 0x00000000(쓰기방지 해제), 0x00000001(쓰기방지 설정) Dword 생성

논리적 쓰기 방지



레지스트리 수정 - NTFS파일시스템(Win7) 레지스트리 수정 [오타나면 안됨]
Key: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies
Name : WriteProtect
Value : 0x00000000(쓰기방지 해제), 0x00000001(쓰기방지 설정) Dword 생성

논리적 쓰기 방지



레지스트리 수정 - NTFS파일시스템(Win7) 레지스트리 수정 [오타나면 안됨]

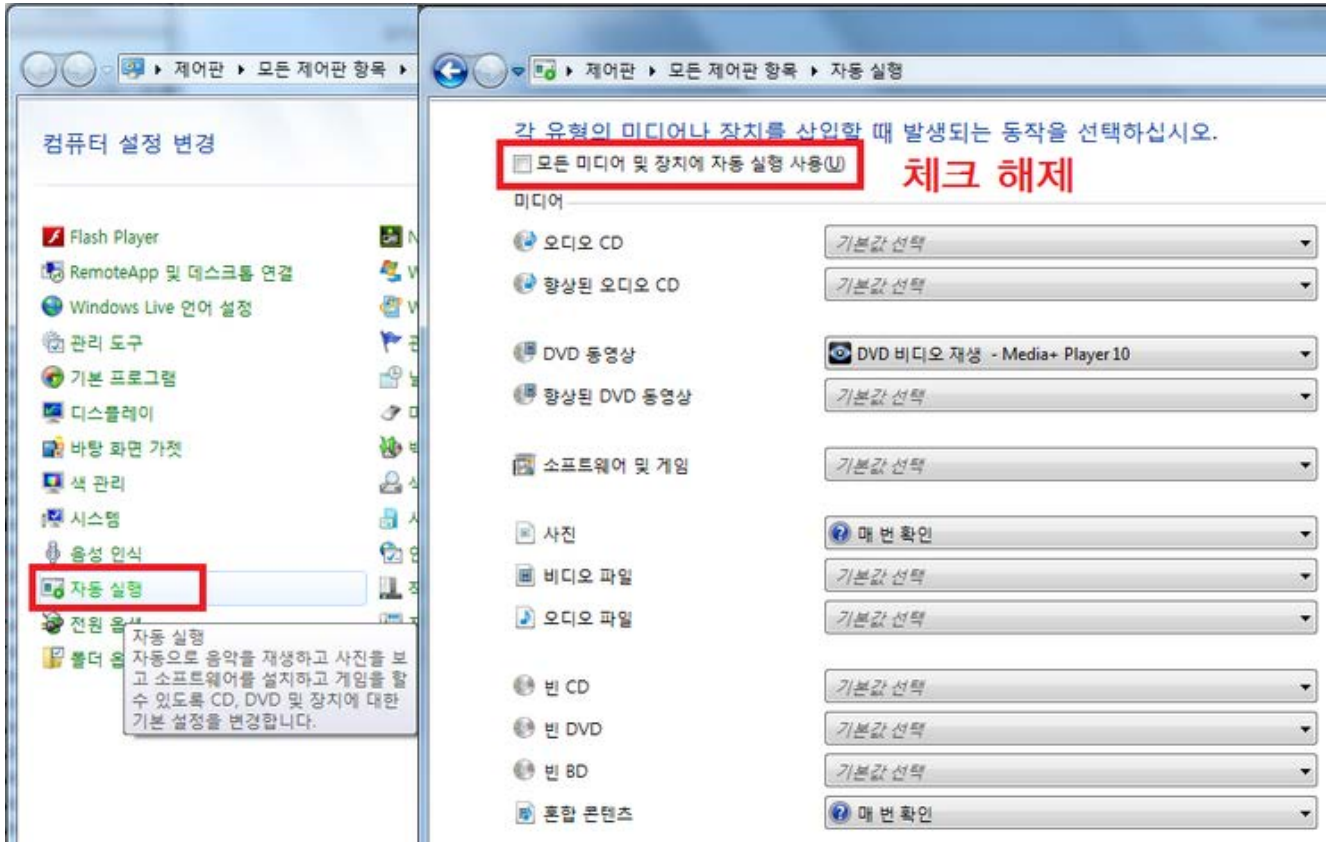
Key: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies

Name : WriteProtect

Value : 0x00000000(쓰기방지 해제), 0x00000001(쓰기방지 설정) Dword 생성

논리적 쓰기 방지

2. 자동 실행 방지

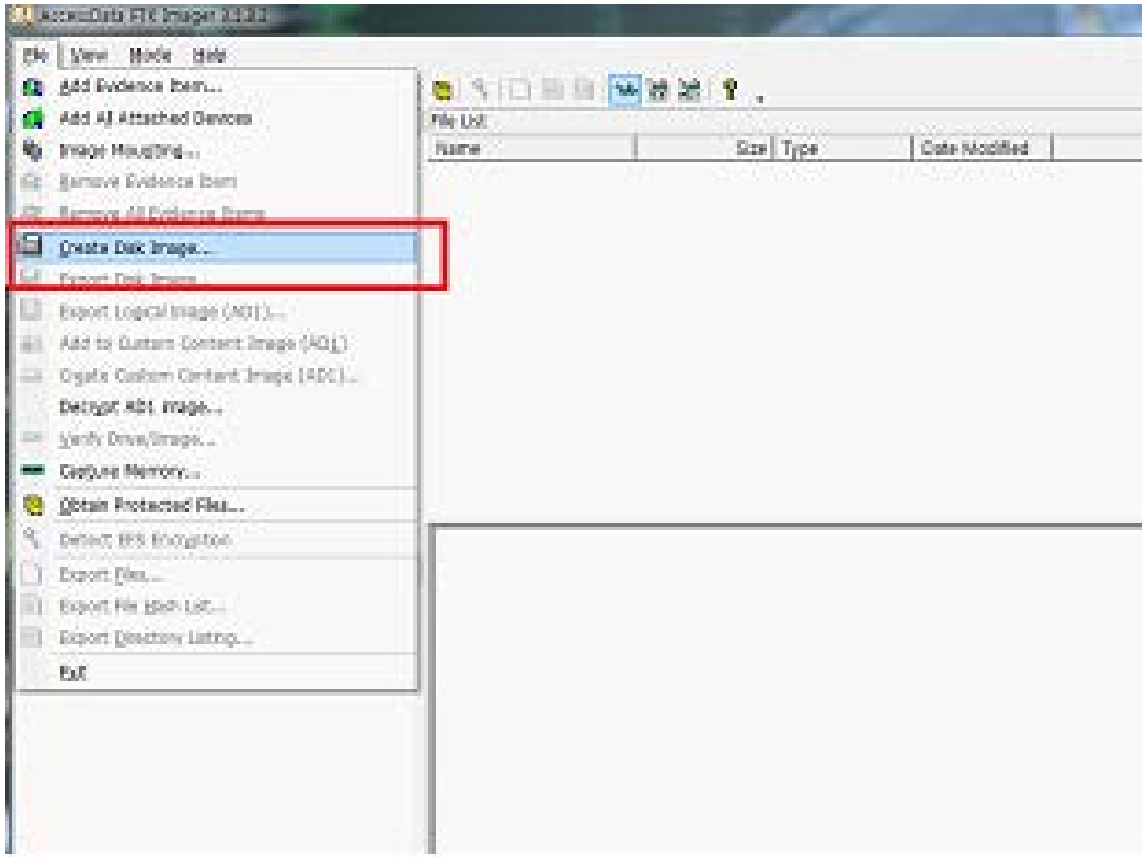


제어판 - 자동실행

모든 미디어 및 장치에 자동 실행 사용 체크 해제

이미지 생성 작업

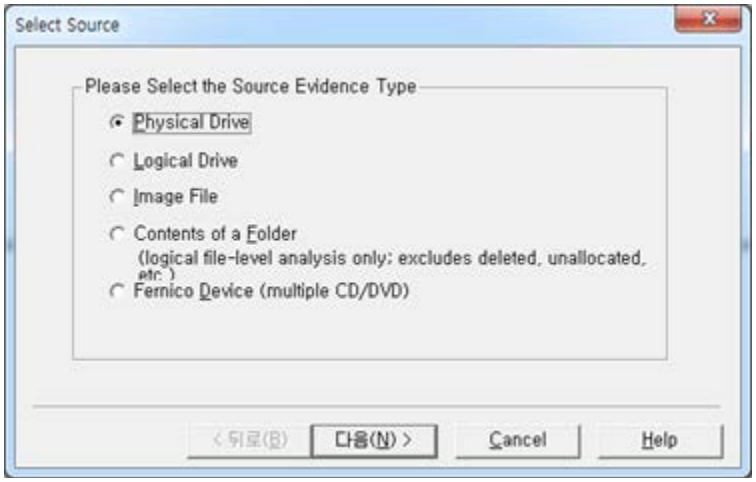
1. 이미징 도구 AccessData FTK Imager 3.1.3 설치 및 실행

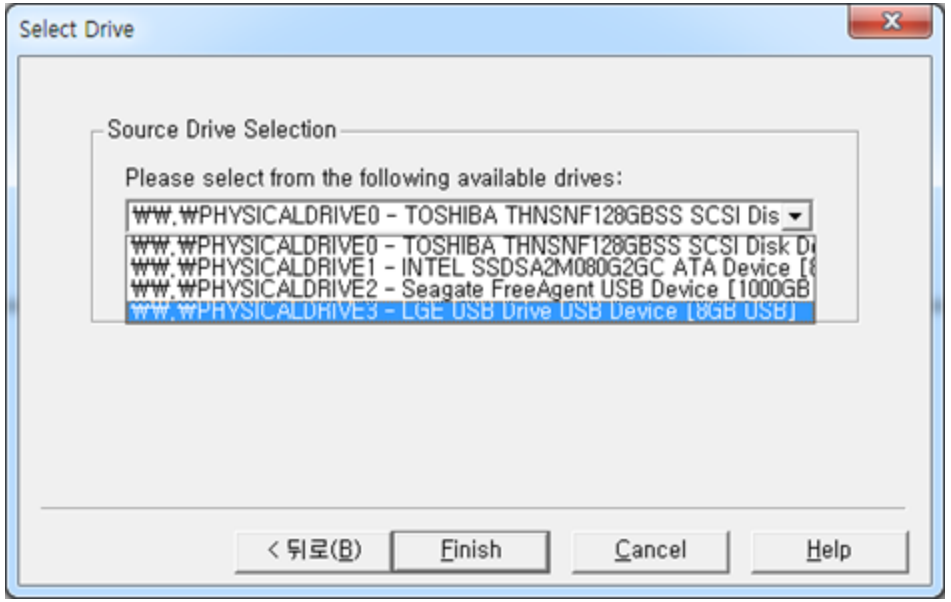


1) 파일 - Create Disk Image

이미지 생성 작업

2. 원본 이미지 선택

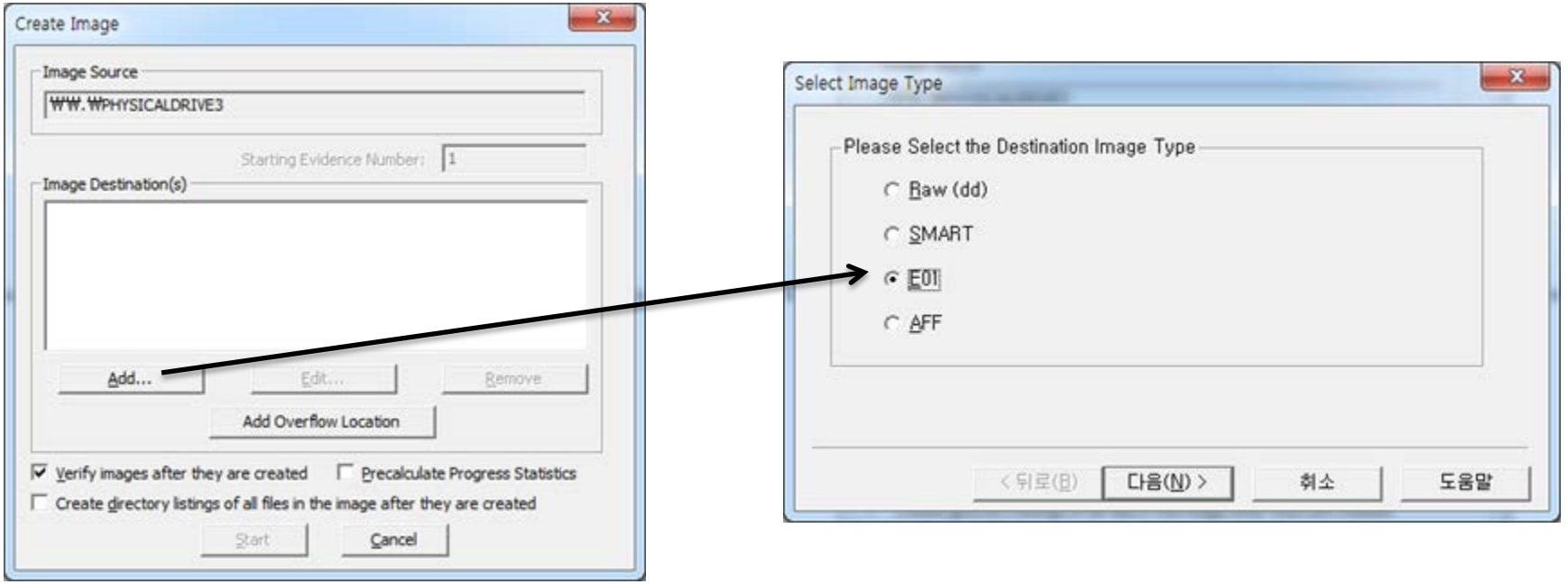




1) 파일 - Create Disk Image
2) Physical Dirve 선택
3) 증거 드라이브 선택

이미지 생성 작업

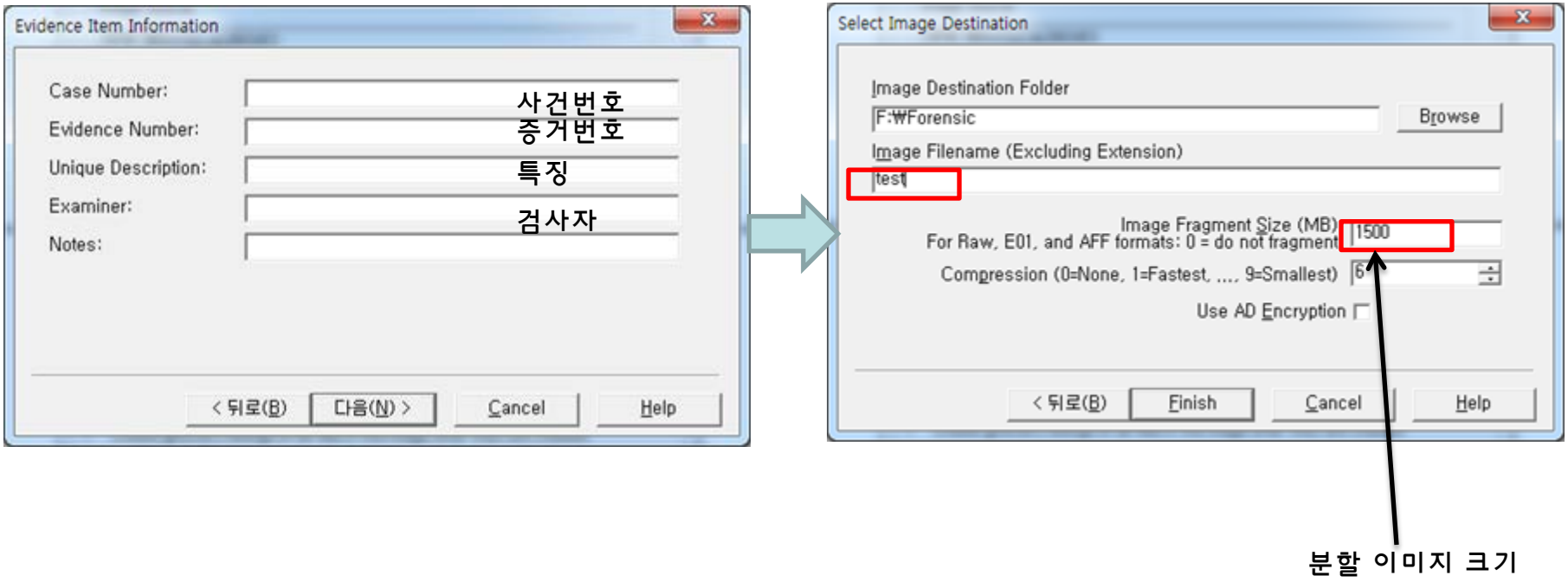
3. 이미지 포맷 설정



1) 파일 - Create Disk Image
2) Physical Dirve 선택
3) 증거 드라이브 선택
4) Add 선택, 파일 포맷 E01으로 설정

이미지 생성 작업

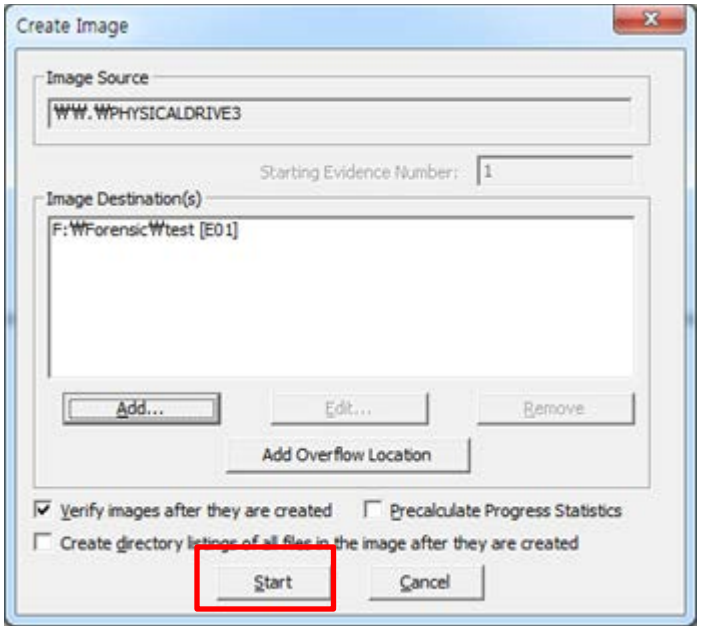
4. 증거 정보 입력

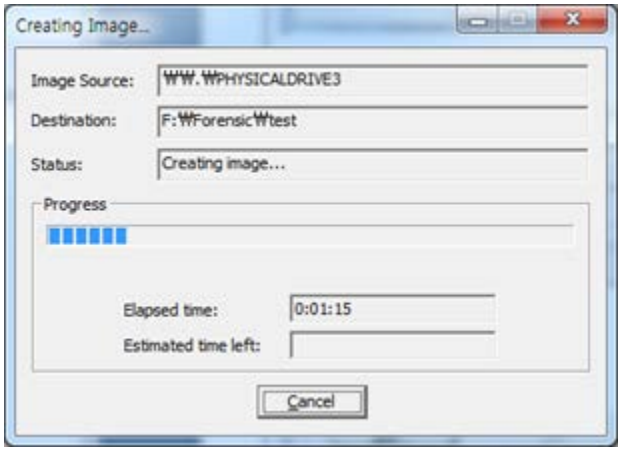


1) 파일 - Create Disk Image
2) Physical Dirve 선택
3) 증거 드라이브 선택
4) Add 선택, 파일 포맷 E01으로 설정
5) 증거 정보입력, 파일 위치 설정

이미지 생성 작업

5. 이미징

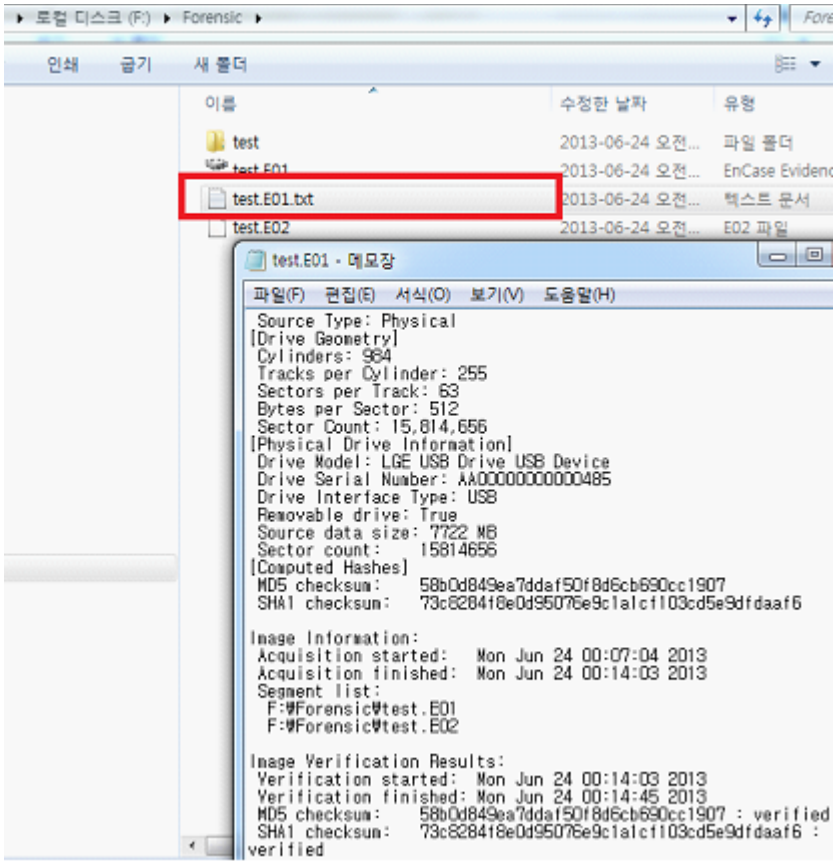




1) 파일 - Create Disk Image
2) Physical Dirve 선택
3) 증거 드라이브 선택
4) Add 선택, 파일 포맷 E01으로 설정
5) 증거 정보입력, 파일 위치 설정
6) 이미징 작업 진행

이미지 생성 작업

5. 정보 확인

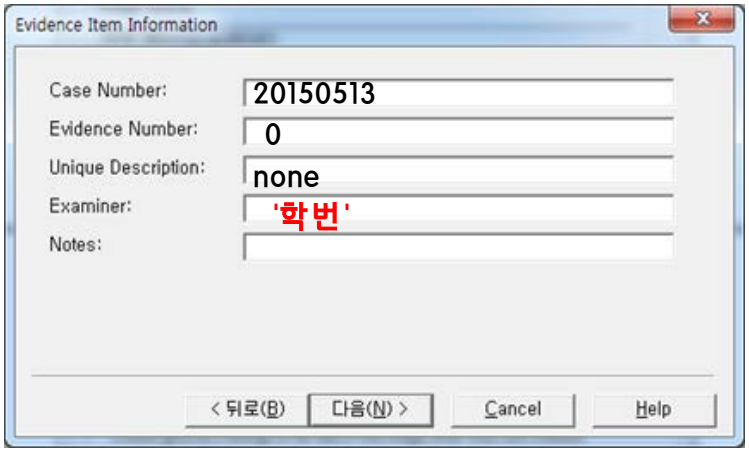


1) *.txt로 증거 이미지 정보 확인
2) 파일정보 중 MD5, SHA1 등 무결성을 확인할 수 있는 해시값 확인

실습 과제

증거물 USB에 대한 사본 이미지 생성 및 무결성 입증

1. 증거물 USB의 파일 변경, 훼손 없이 사본 이미징 작업이 완료되어야 함



2. 이미지 파일 포맷은 E01으로 설정

3. ‘USB 번호’,‘생성된 사본 이미지 파일 정보(.txt) 내용’을 복사하여 bgwon214@gmail.com로 제출

참고문헌

- 정보 보안 개론[개정3판], 양대일 저, 한빛미디어, 2018, 1.
- 디지털 포렌식 개론(2판), 이상진 저, 이룬 출판사, 2015. 5.
- 컴퓨터보안, William Stalling 저, 한티미디어, 2016. 8
- 정보보안과 사이버 해킹의 기초, 김경신 저, 2016. 8

Q & A