문제1.

1. 증거사본 이미지를 생성하고 무결성을 입증하시오.

1) 사본 이미지 정보

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

------------------------------------------------------------

Information for E:\022-2-1-268\시나리오1\문제1\Scenario1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3,740
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60,088,320
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Glide USB Device
 Drive Serial Number: 4C530000261228113331
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 29340 MB
 Sector count:    60088320
[Computed Hashes]
 MD5 checksum:    cd075702a6fddd0023373020dbd30472
 SHA1 checksum:   ab2cd2e5dfcfe5e8ac9065c04c758ff51ad7737d

Image Information:
 Acquisition started:   Wed Jun 12 16:24:01 2024
 Acquisition finished:  Wed Jun 12 16:43:39 2024
 Segment list:
  E:\022-2-1-268\시나리오1\문제1\Scenario1.E01
```

- FTK Imager 이미징 로그 이용, 생성한 사본 이미지 정보에 대한 해시값 확인

파일명		E:\022-2-1-268\시나리오1\문제1\Scenario1
해시값	MD5	cd075702a6fddd0023373020dbd30472
	SHA1	ab2cd2e5dfcfe5e8ac9065c04c758ff51ad7737d

2) 무결성 유지를 위한 이미지 생성 절차

가. 이미지 생성 이전 행동요령

- 증거 수집절차 전 과정에 대한 영상촬영으로 기록하여 적법한 절차에 의해 이미지를 생성하고 분석하였음을 증명.
- 신분증 및 영장/동의서 제시하여 적법하게 분석 절차를 시행하고 있음을 증명.
- 현장을 통제하여 무결성 유지 / 해당 현장 기록하여 문서화
- 피압수자의 참여권 보장하여 적법한 절차에 의해 이미지 생성 및 분석

나. (논리적) 쓰기방지 설정(윈도우 레지스트리 편집기 이용 / Encase Fastbloc SE 사용)

- 레지스트리 편집기 이용, HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\하위에 'StorageDevicePolicies' 키 생성. 이후 DWORD(32bit) 값 'WriteProtect 생성' 후 값 1로 설정하여 쓰기방지(0: 쓰기방지설정 x, 1: 쓰기방지설정o)
- Encase Fastbloc SE 사용, WriteProtected 설정하여 쓰기방지

다. 자동실행 방지 설정

- 제어판 - 자동실행 탭에서 모든 미디어 및 장치에 자동실행 사용 체크 해제

라. 이미지 생성

- (나.단에서) 논리적 쓰기방지 설정 이후 FTK Imager 이용하여 해당 이미지 파일 생성

마. Hash값 및 로그파일 확인

- 이미지 생성 완료 후 FTK Imager에서 불러오거나 로그파일을 확인하여 해시값을 확인하고, 이에 대해 입회인/참관인에게 서명날인을 받는다.

바. 봉인 및 확인

- 이미지 생성 이후 증거원본usb를 훼손방지/무결성 유지를 위해 충격보호케이스에 포장하여 상세정보(사건번호, 수집자, 입회인, 수집환경 등)를 기록한다. 이후 입회인/참관인 등의 서명 날인을 받아 연계보관성이 유지되도록 한다.