문제 1.

1. 증거사본 이미지를 생성하고 무결성을 입증하시오.

1) 전 과정의 영상 촬영

- 이미지 생성, 분석 등 적법한 영장 집행과정에서의 전 과정 영상 촬영으로 적법한 절차에 의해 진행됨을 증명

2) (논리적) 쓰기 방지 설정

- 원본 증거 USB 연결 전 논리적으로 쓰기 방지를 수행

가. 레지스트리 편집기 이용

- 레지스트리 편집기 이용하여 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\' 하위에 StorageDevicePolicies 키 생성(없을 경우) 후 Dword(32비트 값) WriteProtect 생성하여 해당 값 1로 수정해 논리적 쓰기 방지 수행

나. Encase Fastbloc SE 이용

(Encase Fastbloc SE 이용하여 WriteProtect 설정한 화면 캡처)

- Encase Fastbloc SE이용하여 WriteProtect 항목 체크하여 논리적 쓰기 방지 수행

3) 자동실행 방지 설정

- [제어판]-[하드웨어 및 소리]-[자동 실행]에서 모든 미디어 및 장치에 자동 실행 사용 체크 해제하여 자동실행 방지

4) 이미지 생성

- FTK Imager 활용하여 사본 이미지 생성한 후 사본 이미지로만 분석 진행
- 사본 이미지와 증거 원본 USB 동일성 입증을 위해 해시값 생성 후 입회인의 서명 날인

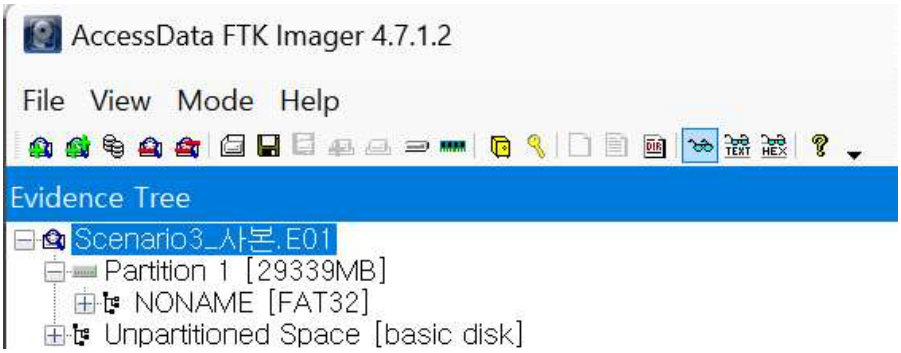
Created By AccessData® FTK® Imager 4.7.1.2

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

Information for C:\Users\-\시나리오3\문제1\Scenario3_사본:

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: d829f9fb2dad9a4772db1f5955003f96
 SHA1 checksum: cf6f5369f4be4eec83b3e894081745f46f160820

Image Information:
 Acquisition started: Tue Jun 18 00:19:50 2024
 Acquisition finished: Tue Jun 18 00:39:12 2024
 Segment list:
  C:\Users\-\시나리오3\문제1\Scenario3_사본.E01



파일 경로(파일명)	C:\Users\-\시나리오3\문제1\Scenario3_사본.E01
MD5 Hash	d829f9fb2dad9a4772db1f5955003f96
SHA-1 Hash	cf6f5369f4be4eec83b3e894081745f46f160820

5) 압수목록 교부 및 봉인

- 원본 USB 등 압수한 목록에 대해 피압수자에게 압수목록을 교부한다.
- 원본 USB 등 압수한 물품의 훼손방지(무결성 유지)를 위해 충격보호케이스 등에 봉인(무선송수신 장치의 경우 전자파 차단케이스 등 활용)하여 해당 물품명, 사건번호, 해시값 등을 기록하여 입회인의 서명날인을 받는다.

6) 연계보관성

- 증거물의 수집, 분석, 이동, 법정에서의 제출까지의 전 과정에 대해 연계보관성이 이루어지도록 피압수자, 변호인 등의 참여권을 보장하고, 인수인계 시 인수자/인계자 서명날인을 받는다.