문제 1.

1. 증거 USB의 사본 이미지를 생성하고 무결성을 입증하시오

1) 참여권 보장, 사본 이미지 생성 및 분석 등 전 과정 사진/영상 촬영한 후 신분증, 영장 제시

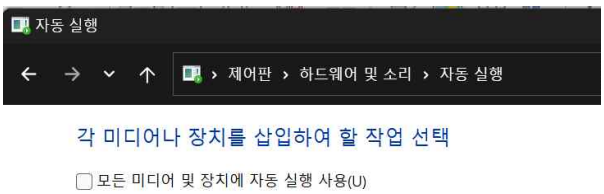
2) 현장통제하여 현장 훼손 방지 및 현장 상황 상세 기록하여 문서화

3) (논리적) 쓰기 방지 설정

증거 USB 무결성 유지를 위해 위와 같이 레지스트리 편집기를 이용하여 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
하위에 StorageDevicePolicies 키를 생성하고, DWORD(32비트)의 WriteProtect 값을 생성하여 해당 데이터를 1로 수정하여 논리적쓰기방지함. (0으로 설정 시 쓰기방지 적용안됨)

또한, Encase Fastbloc SE에서 Write Protected로 설정하여 논리적쓰기방지함.
(Encase Fastbloc SE에서 Write Protected로 설정화면 캡처)

4) 자동실행 방지 설정



제어판 - 하드웨어 및 소리 - 자동실행 탭에서 모든 미디어 및 장치에 자동 실행 사용 체크 해제하여 자동 실행 방지

5) 이미지 생성

무결성 유지를 위해 논리적 쓰기 방지 설정 후, 증거 USB를 연결하고 FTK Imager를 활용하여 e01 파일로 다음과 같이 이미징하였음. 해당 이미징에 대한 로그는 아래와 같음.

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

파일경로(파일명)	E:\022-2-1-268\시나리오2\문제1\Scenario2.E01
MD5 Hash	cd075702a6fddd0023373020dbd30472
SHA1 Hash	ab2cd2e5dfcfe5e8ac9065c04c758ff51ad7737d

원본 USB, 사본 이미지 파일의 동일성 유지를 위해 해시값을 위와 같이 기록함. 해당 해시값은 입회인에게 확인 후 서명날인을 받는다.

6) 봉인 및 확인

이미지 생성 이후 증거 원본 usb를 훼손방지/무결성 유지를 위해 충격보호케이스에 포장하여 상세정보(사건번호, 수집자, 입회인, 수집환경) 등을 기록하고, 해시값 또한 기록하여 입회인에게 확인 후 서명날인받아 봉인하여 연계보관성이 유지되도록 한다.