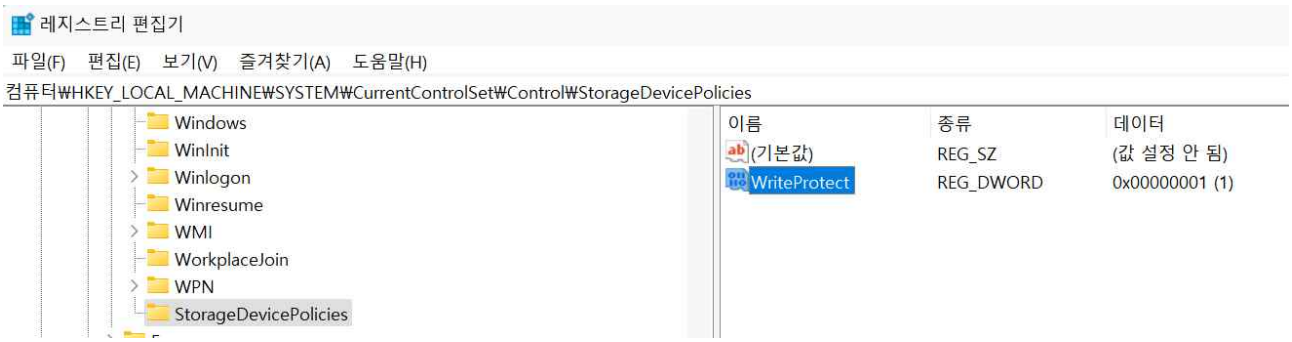
문제 1

1. 다음 요구 항목에 맞추어 증거물 사본을 생성하고, 각 문제 항목의 답안을 작성하시오.

1. USB 증거 사본을 생성하는 과정과 결과를 각 단계별로 기술하시오.(증거사본은 첨부하지 말 것.)

- 무결성 유지 및 원본과 사본과의 동일성 유지를 위해 전 과정을 영상촬영하고, 현장통제한다.
- 원본 usb 무결성 유지를 위해 논리적쓰기방지를 다음과 같이 수행한다.

'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies' 키 생성 후 'WriteProtect DWORD(32비트)' 값을 생성하여 1로 수정하여 논리적 쓰기 방지 수행



- 이후 원본 USB 무결성 유지를 위해 다음과 같이 [제어판]-[하드웨어 및 소리]-[자동 실행]에서 모든 미디어 및 장치에 자동 실행 사용을 체크해제 한다

- FTK Imager를 이용하여 이미지 사본을 생성하고, 생성된 사본에 대해 해시값을 기록한다. 다음은 FTK Imager를 활용하여 이미지 사본을 생성할 때 남겨진 로그파일 '이미지 Log.txt'이다.

```
Created By AccessData® FTK® Imager 4.2.0.13

Case Information:
Acquired using: ADI4.2.0.13
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

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

Information for D:\Test\이미지:

Physical Evidentiary Item (Source) Information:
[Device Info]
  Source Type: Physical
[Drive Geometry]
  Cylinders: 101
  Tracks per Cylinder: 255
  Sectors per Track: 63
  Bytes per Sector: 512
  Sector Count: 1,638,400
[Physical Drive Information]
  Drive Model: SanDisk Cruzer Blade USB Device
  Drive Serial Number: 4C530001040725104371
  Drive Interface Type: USB
  Removable drive: True
  Source data size: 800 MB
  Sector count:     1638400
  Removable drive: True
[Computed Hashes]
  MD5 checksum:
  SHA1 checksum:

Image Information:
  Acquisition started:    Sat Jun 15 12:56:50 2019
```

Acquisition finished: Sat Jun 15 12:56:55 2019
Segment list:
D:\Test\이미지.001

사본 이미지 경로(파일명)	C:\-\Bitnang_시나리오\문제1
MD5 해시값	1b421bafac99a606bc6bd61711edb8b7
SHA-1 해시값	f295ab387ec7cbfeb41a8bd1f327ea6e080b607d

- 사본 생성 후 해시값을 기록하고, 이에 대한 피압수자, 입회인 등의 서명날인을 받음.

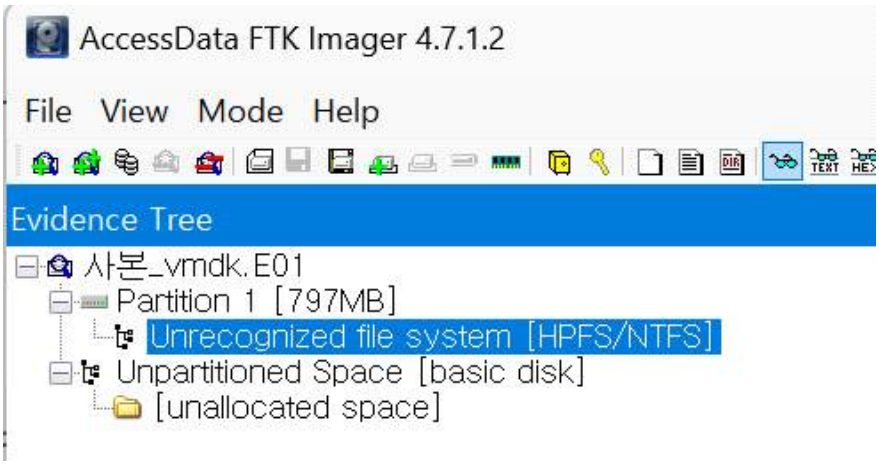
- 이후 정전기방지봉투, 충격보호케이스에 봉인하여 입회인 등의 서명날인을 받는다.

- 증거물 분석을 위해 이동 시 연계보관성 유지를 위해 관련인 등의 서명날인을 받고, 모든 과정을 문서화하여 증명할 수 있도록 한다.

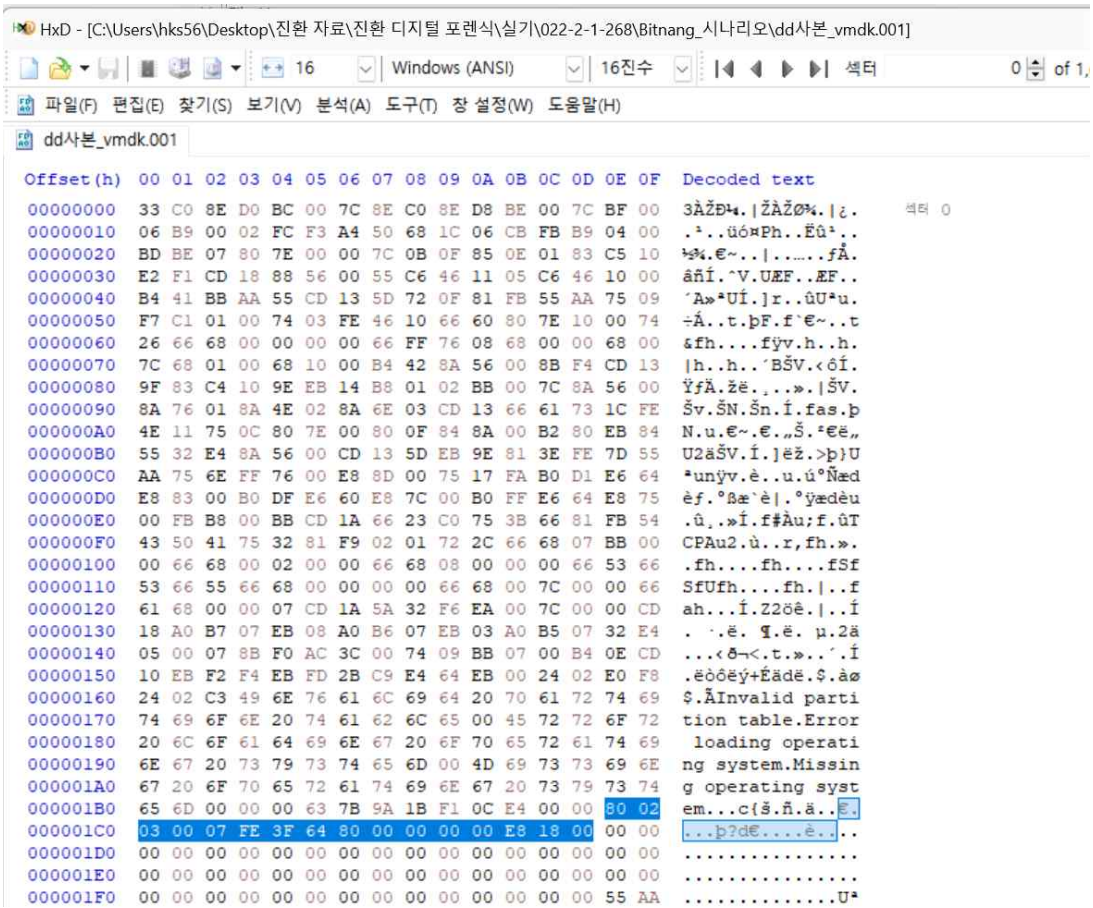
2. 파일 시스템이 훼손 되어 있다, 파일시스템 복구 후 증거사본의 매체 정보 중 아래 항목을 찾아 기술하시오.

USB 시리얼 넘버 / 파일 시스템 종류 / 총 섹터 수 / 전체용량 / 가용용량 / 볼륨 시리얼 번호 / 단위 클러스터 크기

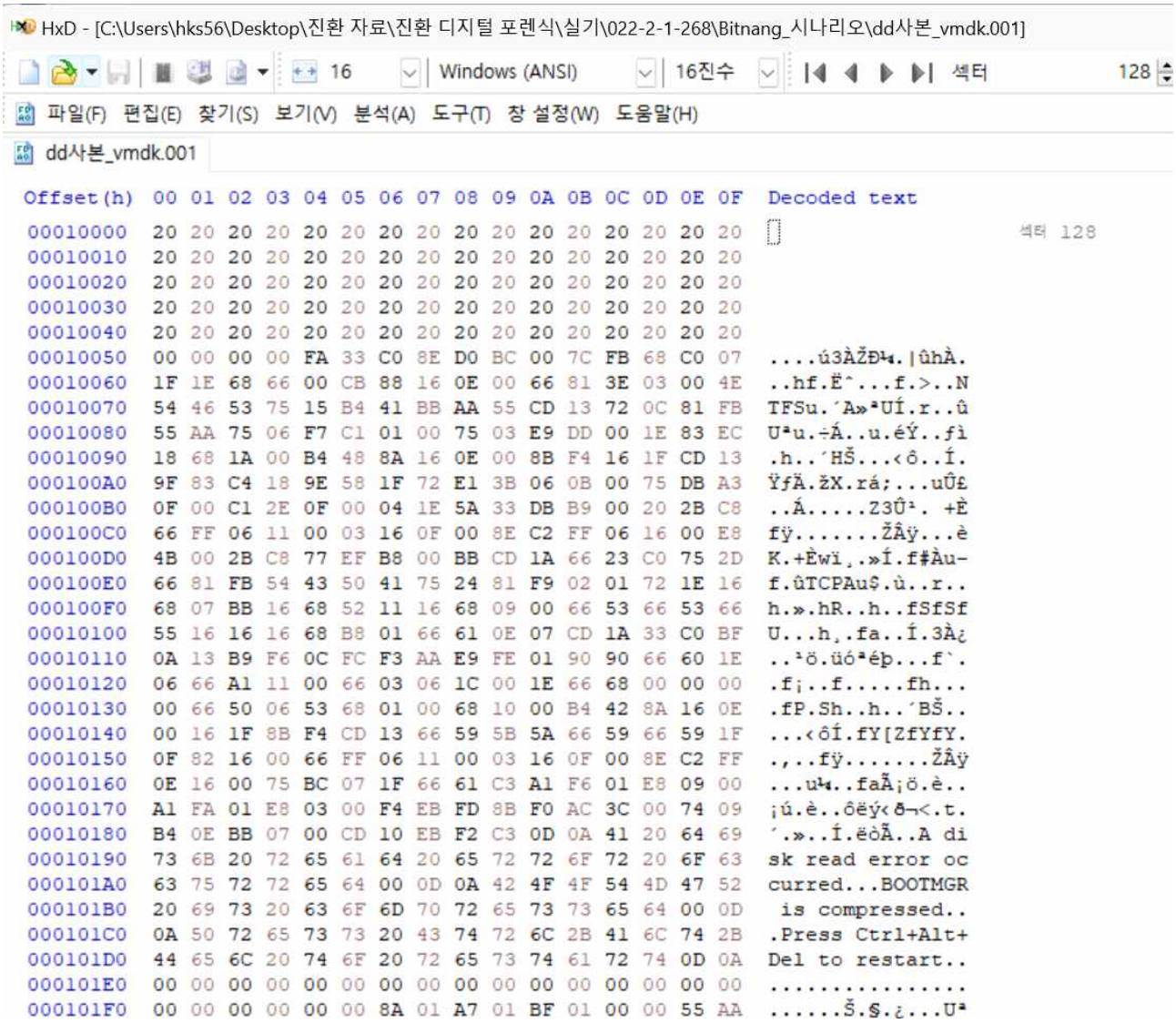
- USB 시리얼 넘버는 “이미지 Log.txt” 참고



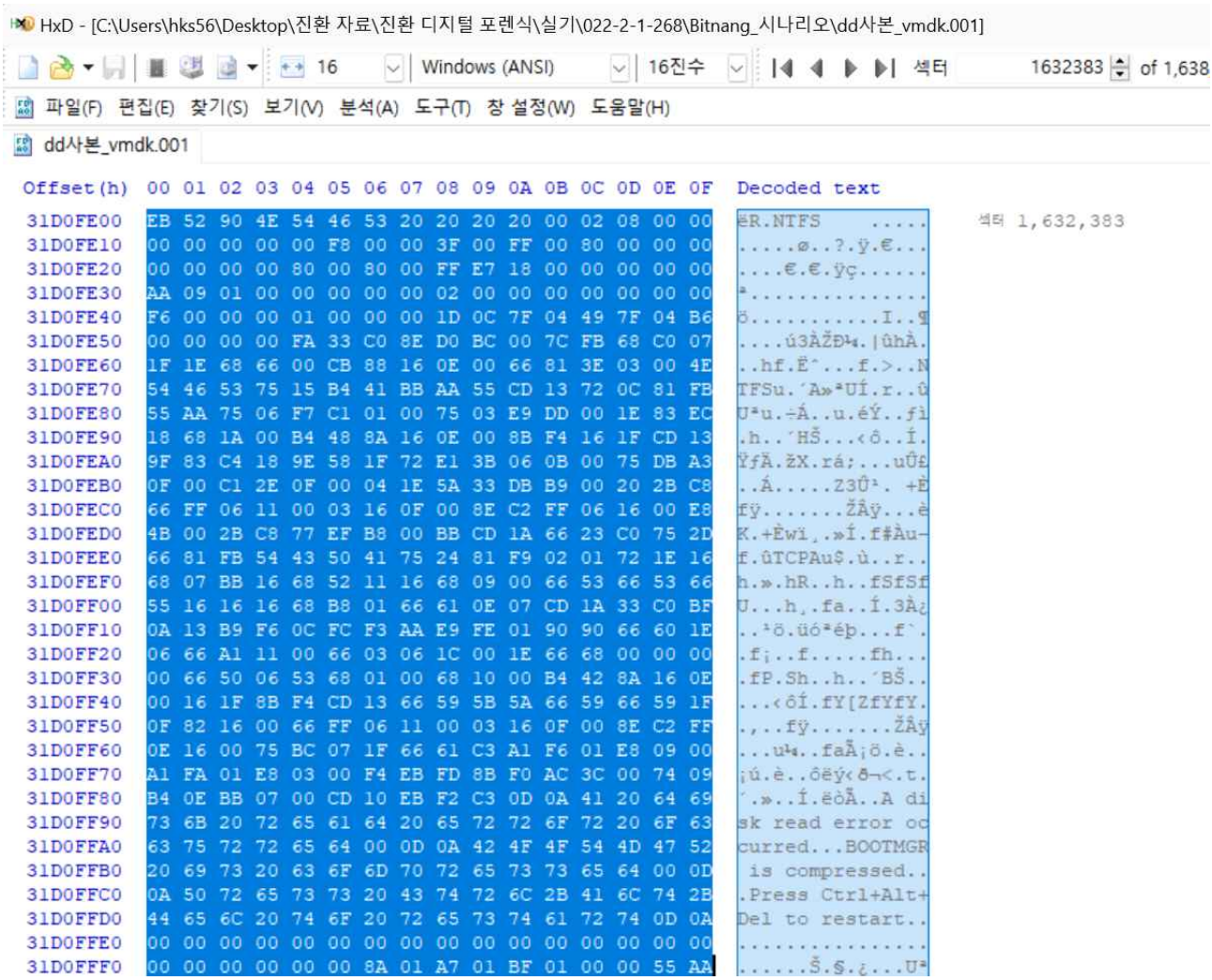
- 최초 확인시 Partition 1이 Unrecognized file system으로 복원해야하므로 .001파일로 재이미징 하여 HxD에서 다음과 같이 불러온 결과 MBR에서 Partition Table 정보를 다음과 같이 확인함.



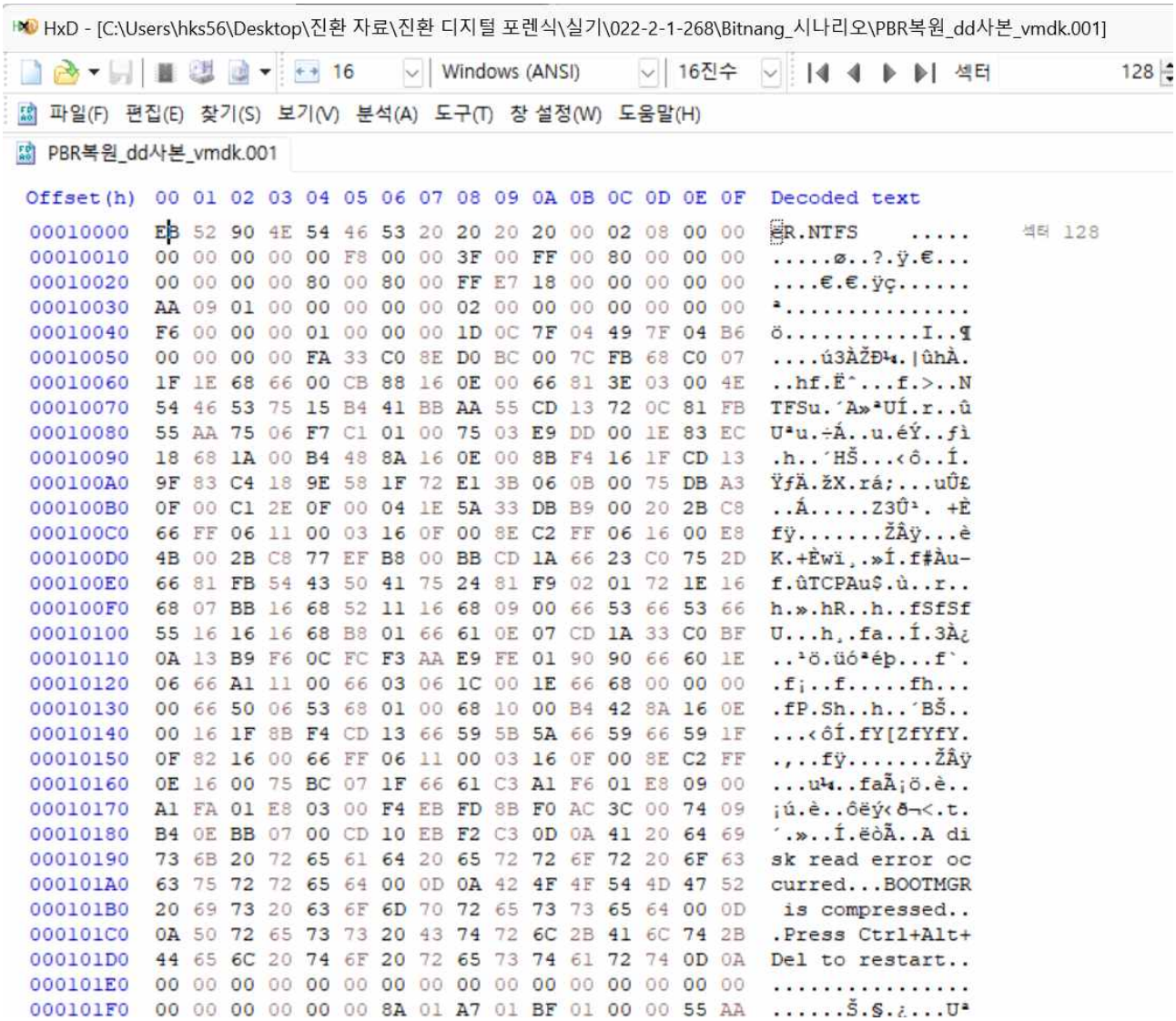
- MBR의 파티션 테이블 정보를 확인하여 00 00 00 80(Little Endian 변환)의 위치로 섹터 128이 훼손된 파티션의 시작 섹터임을 확인. 이후 이동하였더니 다음과 같이 PBR 훼손되었음.



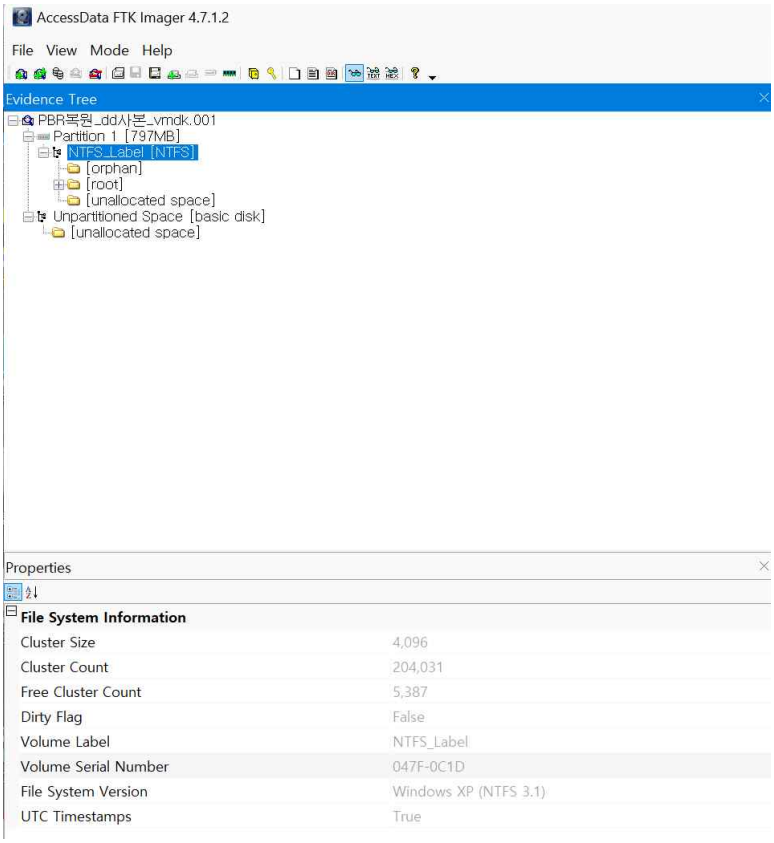
- NTFS PBR 백업본이 위치한 NTFS 파일시스템 마지막 섹터로 이동(시작섹터 + 섹터수 - 1)
(128 + 1,632,256(18 E8 00 ; Little Endian 변환) - 1 = 1,632,383 섹터로 이동.)
후 백업본 확인하여 복사



- PBR 복구를 위해 시작섹터인 128로 돌아와서 해당 백업본 붙여넣기 쓰기로 복원 후 다른이름으로 저장



- PBR 복원 이후 해당 파티션 내부구조 다음과 같이 확인 가능.



USB 시리얼 넘버	4C530001040725104371
파일 시스템 종류	NTFS (0X07)
총 섹터 수	1,632,256
전체용량	835,715,072 Bytes
가용용량	835,710,976 Bytes
볼륨 시리얼 번호	047F-0C1D
단위 클러스터 크기	4,096 Bytes