

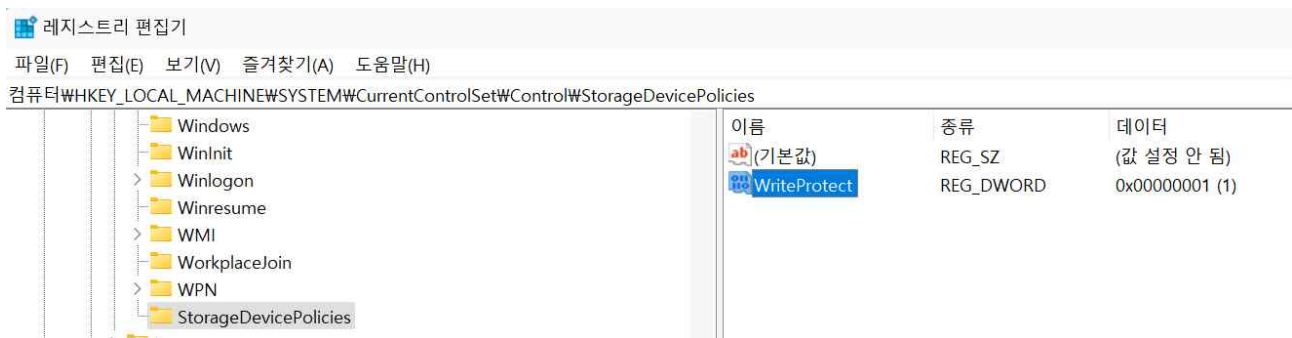
## 문제 1

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

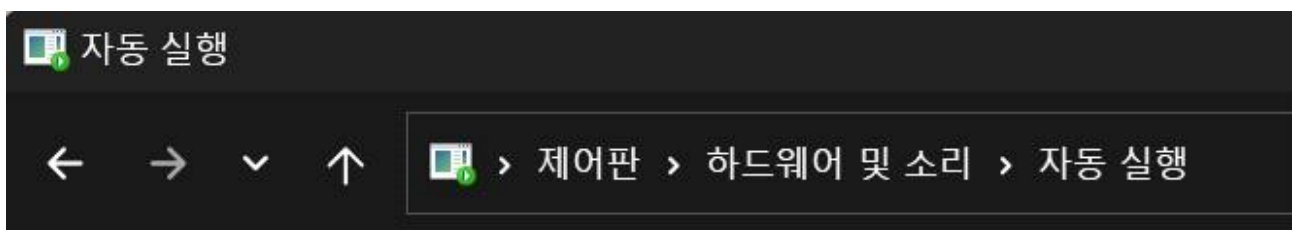
1. USB 증거 사본을 생성하는 과정과 결과를 각 단계별로 기술하시오.(증거사본은 첨부하지 말 것.)

- 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



각 미디어나 장치를 삽입하여 할 작업 선택

☐ 모든 미디어 및 장치에 자동 실행 사용(U)

- 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:

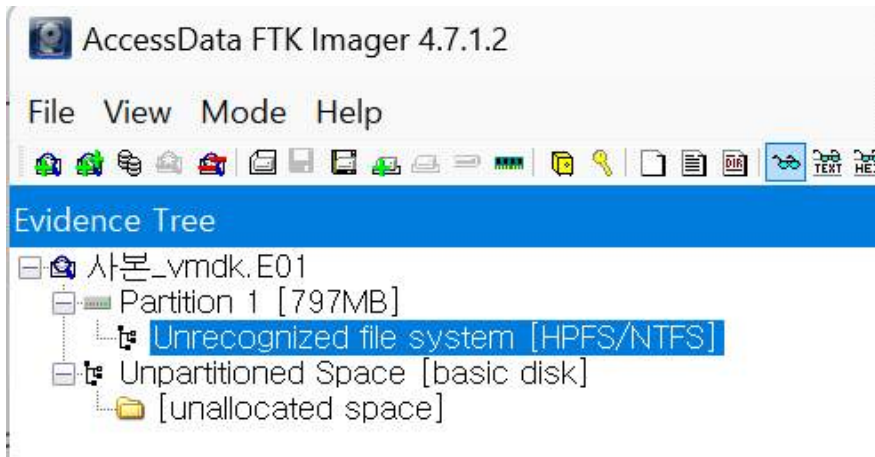
D:\Test\이미지.001

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

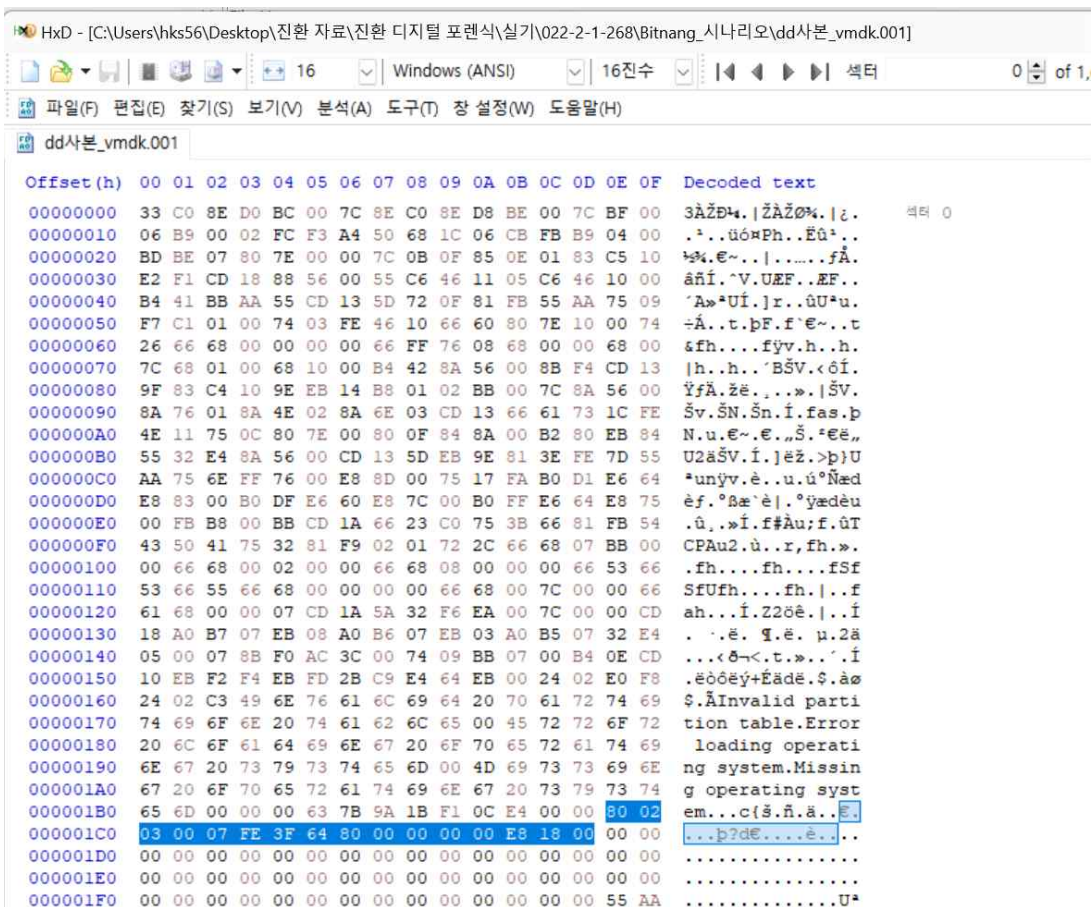
- 사본 생성 후 해시값을 기록하고, 이에 대한 피압수자, 입회인 등의 서명날인을 받음.
- 이후 정전기방지봉투, 충격보호케이스에 봉인하여 입회인 등의 서명날인을 받는다.
- 증거물 분석을 위해 이동 시 연계보관성 유지를 위해 관련인 등의 서명날인을 받고, 모든 과정을 문서화하여 증명할 수 있도록 한다.

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.

```

HxD - [C:\Users\hks56\Desktop\진환 자료\진환 디지털 포렌식\실기\022-2-1-268\Bitnang_시나리오\dd사본_vmdk.001]
16 Windows (ANSI) 16진수 섹터 128
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)
dd사본_vmdk.001

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00010000 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 
00010010 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 
00010020 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 
00010030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 
00010040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 
00010050 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07 ....ú3ÀŽĐµ. |ûhÀ.
00010060 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E ..hf.Ē`...f.>..N
00010070 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB TFSu.´A»²Uí.r..û
00010080 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC U²u.÷Ã..u.éÝ..fì
00010090 18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13 .h...´HŠ...<ó...í.
000100A0 9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3 ŸfÃ.žX.rá;...uŮž
000100B0 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8 ..Á.....23Ů². +È
000100C0 66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8 fy.....ŽÄÿ...è
000100D0 4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D K.+Èwi,»Í.f#Àu-
000100E0 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16 f.ûTCPAu$.ù...r..
000100F0 68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66 h.».hR..h..fSfSf
00010100 55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF U...h,fa.Í.3Äž
00010110 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E ..²ó.úó²ép...f`.
00010120 06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00 .f;...f.....fh...
00010130 00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E .fP.Sh..h...´BŠ..
00010140 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F ...<óÍ.fY[ZfYfY.
00010150 0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF ,...fy.....ŽÄÿ
00010160 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00 ...u²...faÃ;ö.è..
00010170 A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09 ;ú.è...óëý<ð¬<.t.
00010180 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69 ´.»...Í.èòÃ..A di
00010190 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63 sk read error oc
000101A0 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52 curred...BOOTMGR
000101B0 20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D is compressed..
000101C0 0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B .Press Ctrl+Alt+
000101D0 44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A Del to restart..
000101E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000101F0 00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA .....Š.$.¿...U²

```



- 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

```
HxD - [C:\Users\hks56\Desktop\진환 자료\진환 디지털 포렌식\실기\022-2-1-268\Bitnang_시나리오\dd사본_vmdk.001]
16 Windows (ANSI) 16진수 섹터 1632383 of 1,638
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)
dd사본_vmdk.001

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
31D0FE00 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 ER.NTFS .....
31D0FE10 00 00 00 00 00 F8 00 00 3F 00 FF 00 80 00 00 00 .....ø...?.ý.é...
31D0FE20 00 00 00 00 80 00 80 00 FF E7 18 00 00 00 00 00 .....é.ÿç.....
31D0FE30 AA 09 01 00 00 00 00 00 02 00 00 00 00 00 00 00 ^.....
31D0FE40 F6 00 00 00 01 00 00 00 1D 0C 7F 04 49 7F 04 B6 ö.....I..g
31D0FE50 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07 ....ú3ÄŽĐ*.|ùhÀ.
31D0FE60 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E ..hf.Ē^...f.>..N
31D0FE70 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB TFSu.'A»²Uí.r..û
31D0FE80 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC U*u.÷À..u.éÝ..fì
31D0FE90 18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13 .h..'HŠ...<ô..í.
31D0FEA0 9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3 ŸfÀ.žX.rá;...uÜĖ
31D0FEB0 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8 ..Á.....Z3Ů¹. +Ē
31D0FEC0 66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8 fy.....ŽÄÿ...è
31D0FED0 4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D K.+Ēwi,»í.f#Au-
31D0FEE0 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16 f.ûTCPAu$.ù..r..
31D0FEF0 68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66 h.».hR..h...fSfSf
31D0FF00 55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF U...h,fa..í.3Äĵ
31D0FF10 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E ...²ô.üó²ép...f^
31D0FF20 06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00 .fì...f.....fh...
31D0FF30 00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E .fP.Sh..h..'BŠ..
31D0FF40 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F ...<ôí.fY[ZfYfY.
31D0FF50 0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF ...fy.....ŽÄÿ
31D0FF60 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00 ...u*.faÄĵö.è..
31D0FF70 A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09 ĵú.è..ôëý<ô-<.t.
31D0FF80 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69 '.»...í.ëòÄ..A di
31D0FF90 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63 sk read error oc
31D0FFA0 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52 curred...BOOTMGR
31D0FFB0 20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D is compressed..
31D0FFC0 0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B .Press Ctrl+Alt+
31D0FFD0 44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A Del to restart..
31D0FFE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
31D0FFF0 00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA .....Š.Š.ċ...U²
```

섹터 1,632,383

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

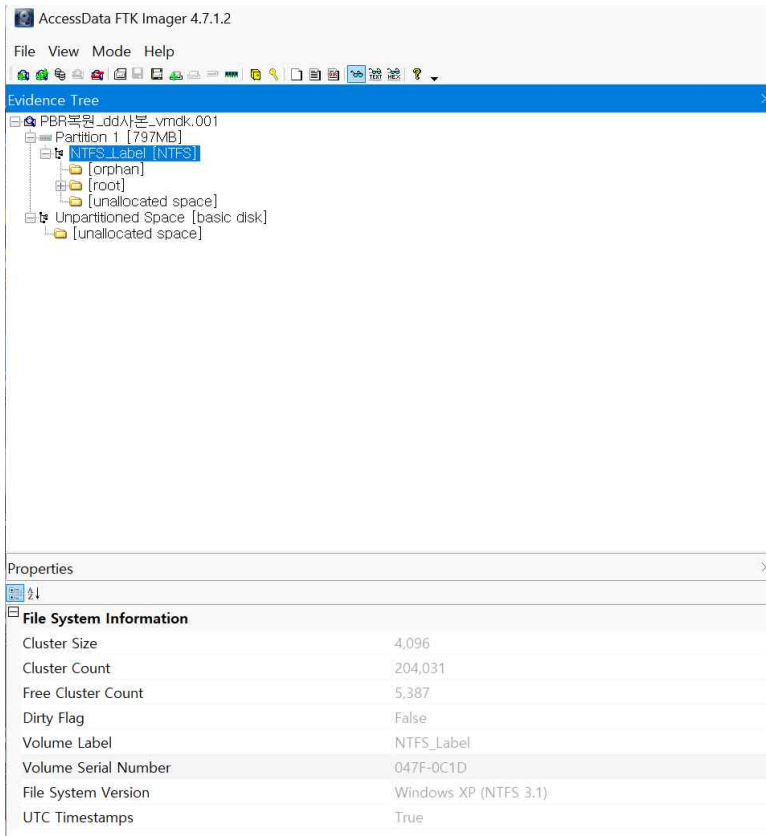
```

HxD - [C:\Users\hks56\Desktop\진환 자료\진환 디지털 포렌식\실기\022-2-1-268\Bitnang_시나리오\PBR복원_dd사본_vmdk.001]
Windows (ANSI) 16진수 섹터 128
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)
PBR복원_dd사본_vmdk.001

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00010000 E8 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 R.NTFS ..... 섹터 128
00010010 00 00 00 00 00 F8 00 00 3F 00 FF 00 80 00 00 00 .....ø...?.ÿ.€...
00010020 00 00 00 00 80 00 80 00 FF E7 18 00 00 00 00 00 ....€..ÿç.....
00010030 AA 09 01 00 00 00 00 00 02 00 00 00 00 00 00 00 ^.....
00010040 F6 00 00 00 01 00 00 00 1D 0C 7F 04 49 7F 04 B6 ö.....I..¶
00010050 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07 ....ú3ÄZB4. |ûhÄ.
00010060 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E ..hf.Ë^...f.>..N
00010070 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB TFSu.'A»*UÍ.r..û
00010080 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC U*u.÷Ä..u.éÝ..fi
00010090 18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13 .h..'HŠ...<ö..í.
000100A0 9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3 ŸfÄ.žX.rá;...uÜž
000100B0 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8 ..Á.....Z3Ů². +Ë
000100C0 66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8 fÿ.....ŽÄÿ...è
000100D0 4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D K.+Ëwì,.»í.f#Au-
000100E0 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16 f.ûTCPAu$.ù...r..
000100F0 68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66 h.».hR..h..fSfSf
00010100 55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF U...h, .fa..í.3Äž
00010110 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E ..²ö.úó*ép...f`.
00010120 06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00 .f;...f.....fh...
00010130 00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E .fP.Sh..h..'BŠ..
00010140 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F ...<óí.fY[ZfYfY.
00010150 0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF ,...fÿ.....ŽÄÿ
00010160 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00 ...u4...faÄ;ö.è..
00010170 A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09 ;ú.è..öëÿ<ö-<.t.
00010180 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69 `.»...í.ëöÄ..A di
00010190 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63 sk read error oc
000101A0 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52 curred...BOOTMGR
000101B0 20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D is compressed..
000101C0 0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B .Press Ctrl+Alt+
000101D0 44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A Del to restart..
000101E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000101F0 00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA .....Š.S.¿...U²

```

- 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