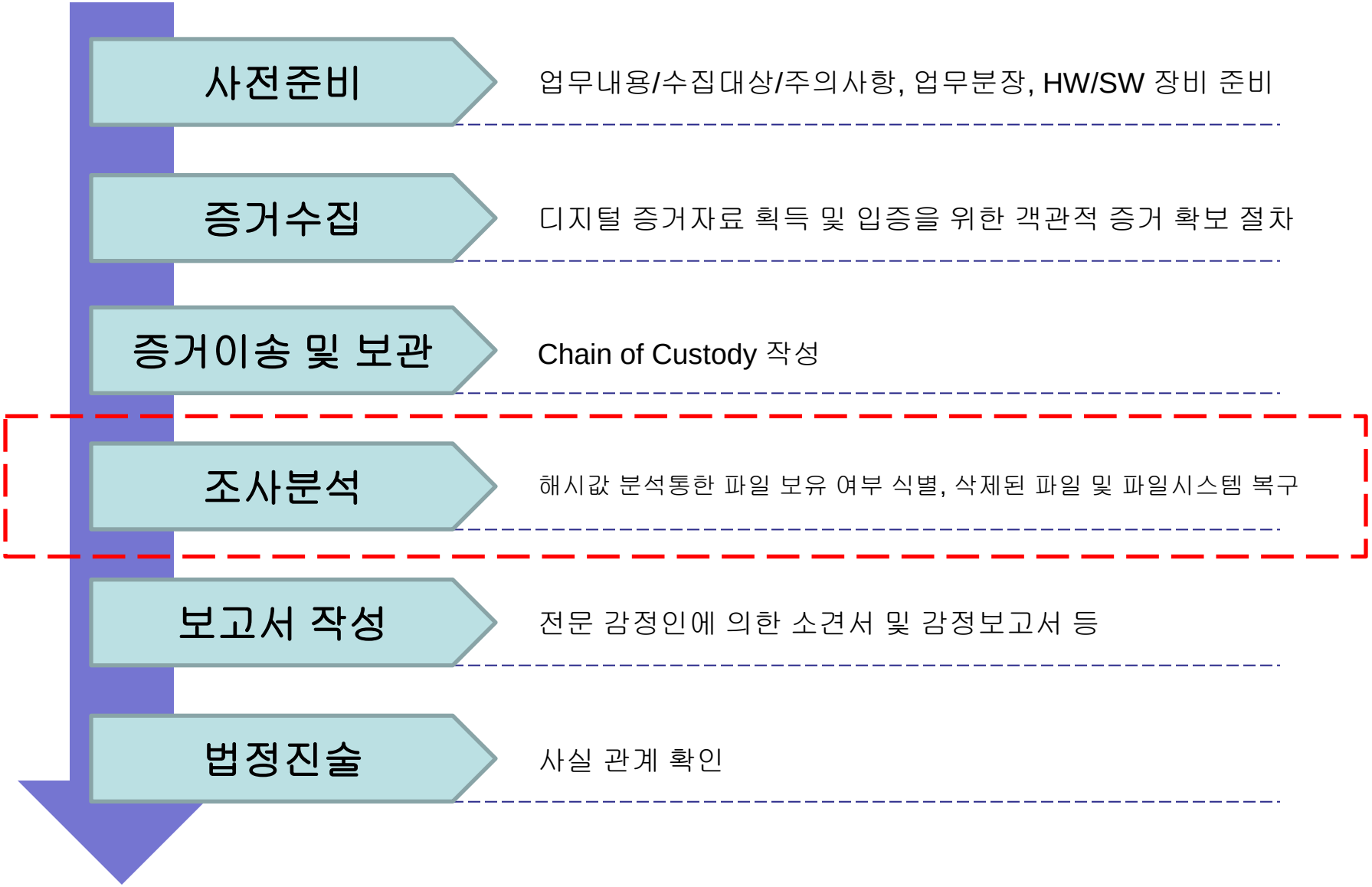
컴퓨터보안 실습

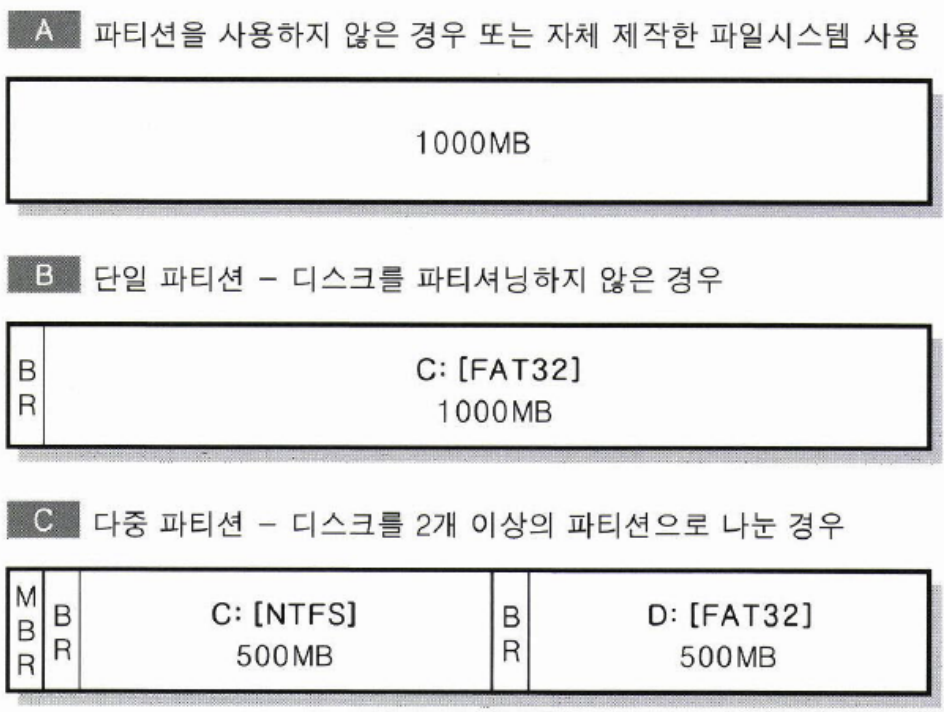
포렌식 실습(실습9)

조사 분석 – 손상 파티션 복구

디지털포렌식 절차

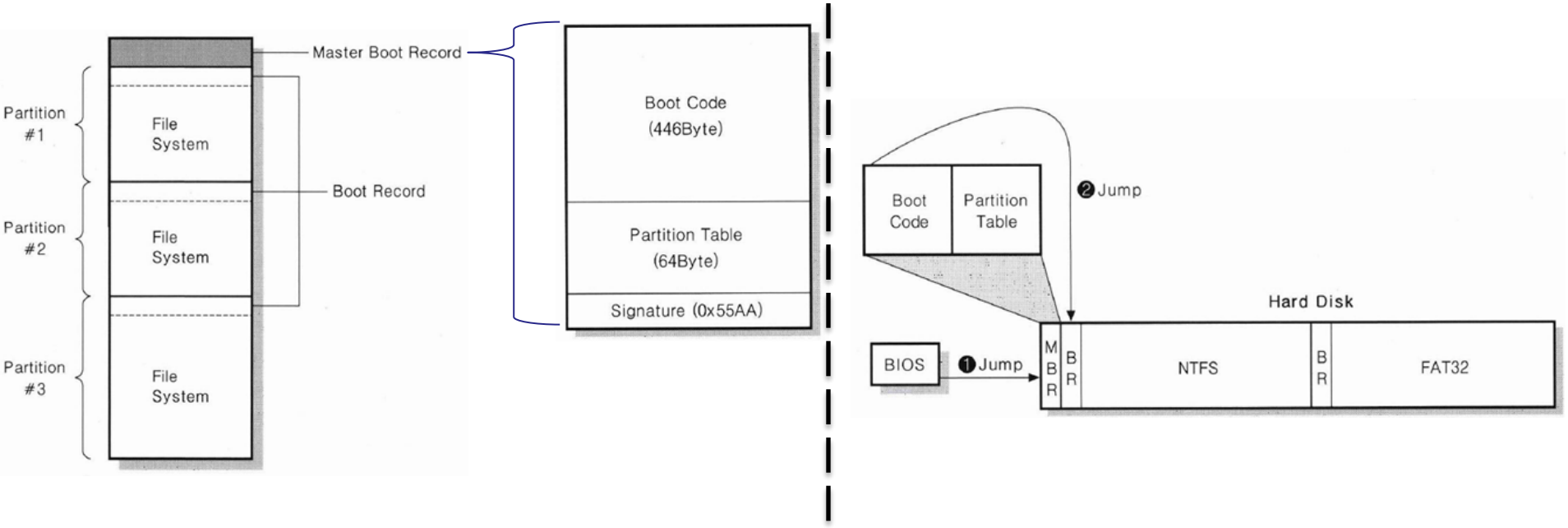

사전준비
업무내용/수집대상/주의사항, 업무분장, HW/SW 장비 준비
증거수집
디지털 증거자료 획득 및 입증을 위한 객관적 증거 확보 절차
증거이송 및 보관
Chain of Custody 작성
조사분석
해시값 분석통한 파일 보유 여부 식별, 삭제된 파일 및 파일시스템 복구
보고서 작성
전문 감정인에 의한 소견서 및 감정보고서 등
법정진술
사실 관계 확인

파티션 정의



- 저장 공간을 하나 이상의 연속되고 독립된 영역으로 나누어 사용할 수 있도록 한 규약

MBR(Master Boot Record)

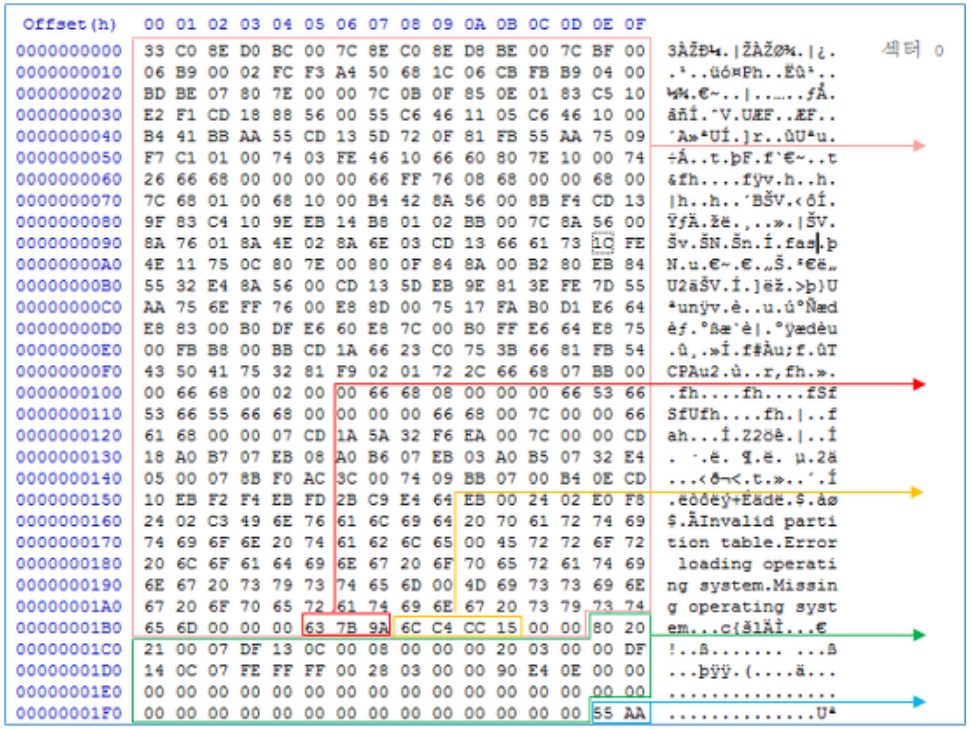


[MBR의 구조]

- 디스크 0번 섹터에 위치하며 부팅에 필요한 부트 코드와 파티션 테이블을 포함(512바이트)
- BR 호출과정 포함, 파티션 테이블을 읽고, 각각의 파티션이 부팅 가능한지 확인하며, 파티션이 정상적이지 않거나 부팅 가능한 파티션이 없는 경우 예외 처리
- 해당 파티션의 Boot Record를 호출하는 것이 주요 목적

MBR(Master Boot Record)

✓ Boot Code = 446 Byte Partition Table = 64 Byte Magic Number = 2 Byte



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0000000000	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00
0000000010	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00
0000000020	BD	BE	07	80	7E	00	00	7C	0B	0F	85	0E	01	83	C5	10
0000000030	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00
0000000040	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09
0000000050	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74
0000000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00
0000000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13
0000000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00
0000000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE
00000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84
00000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55
00000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64
00000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75
00000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54
00000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00
0000000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66
0000000110	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66
0000000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD
0000000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4
0000000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD
0000000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8
0000000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69
0000000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72
0000000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69
0000000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E
00000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
00000001B0	65	6D	00	00	00	63	7B	9A	6C	C4	CC	15	00	00	80	20
00000001C0	21	00	07	DF	13	0C	00	08	00	00	00	20	03	00	00	DF
00000001D0	14	0C	07	FE	FF	FF	00	28	03	00	00	90	E4	0E	00	00
00000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

Boot Code

Error message Offset

Signature

Partition Table

[MBR Partition Table Entry]

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0x00															Boot Flag	
0x10	Starting CHS Address		Part Type	Ending CHS Address			Starting LBA Address				Size in Sector					

- 부팅가능여부, 읽기 모드, 시작과 끝 위치, 타입, 섹터 수 기록

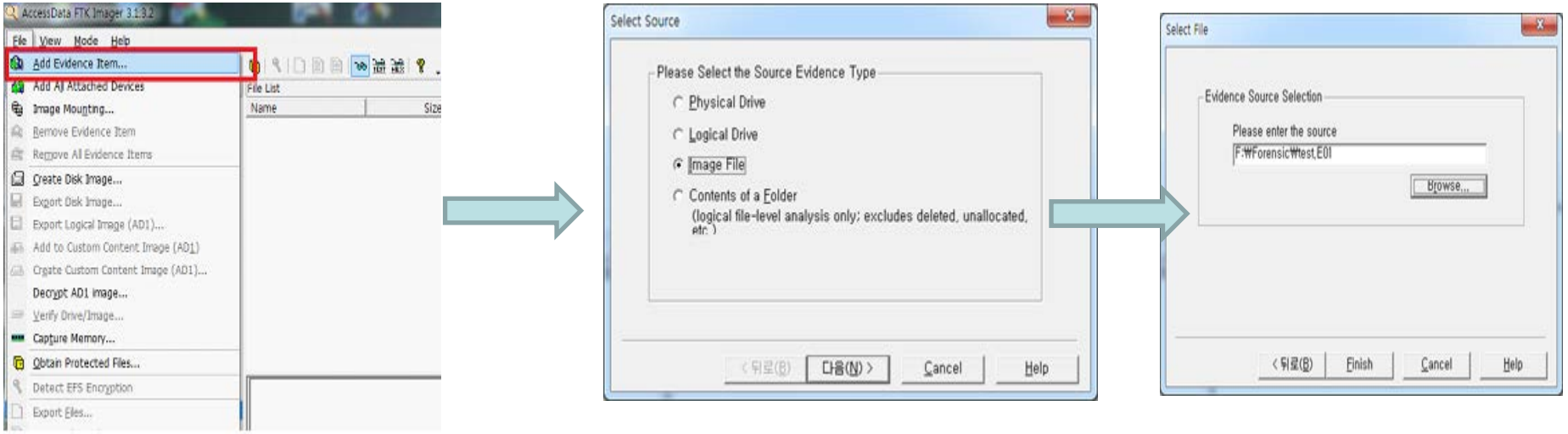
(실습) 파티션 복구

1. 실습준비

1). http://www.parkjonghyuk.net/lecture/2019-1st-lecture/2019-1st-lecture.htm

→FAT32.001 증거 이미지 파일

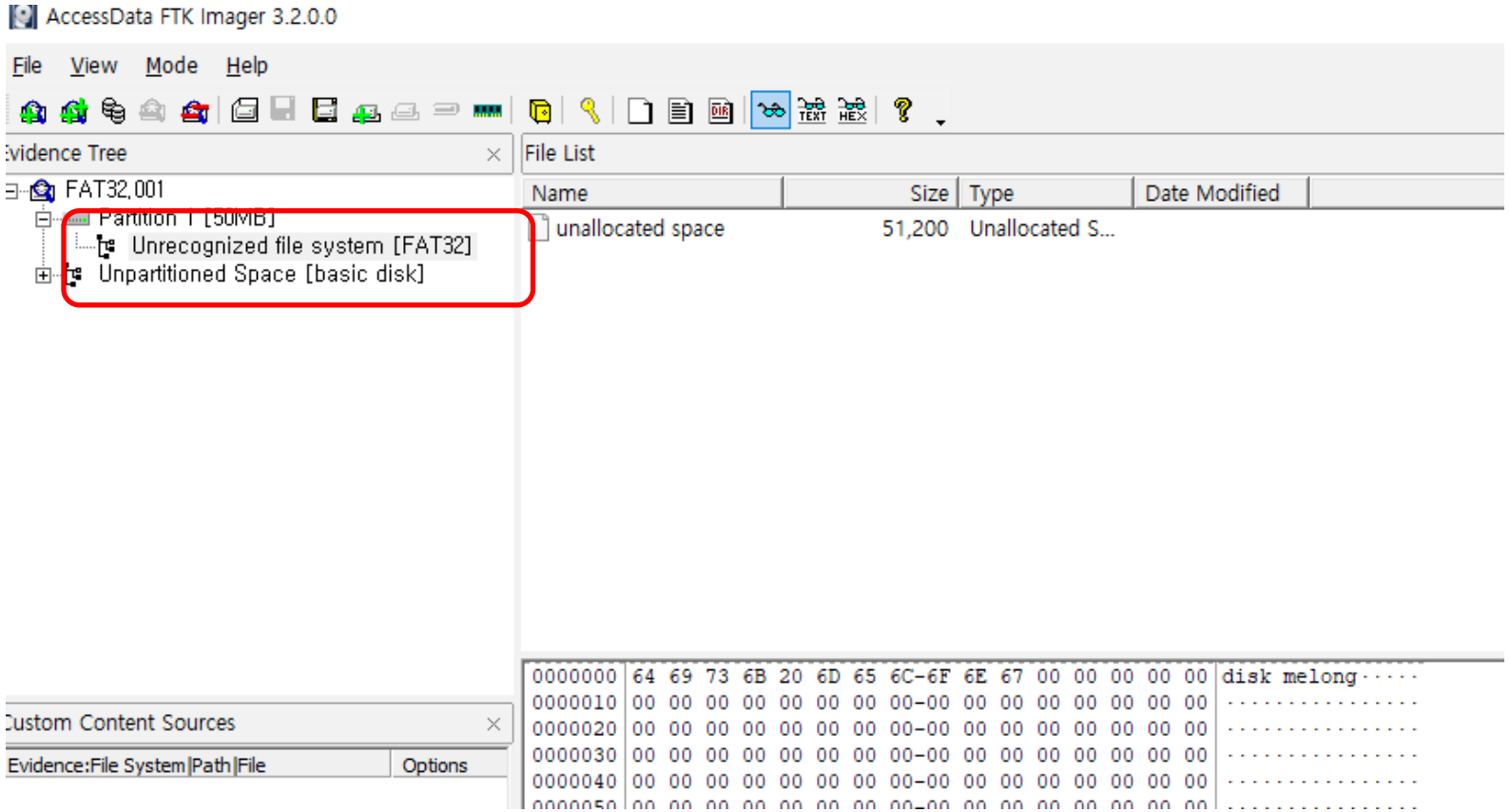
→HxDSetup.zip 파일 다운로드 및 설치



- 증거 이미지 파일 불러오기

(실습) 파티션 복구

1. 이미지 파일 불러오기

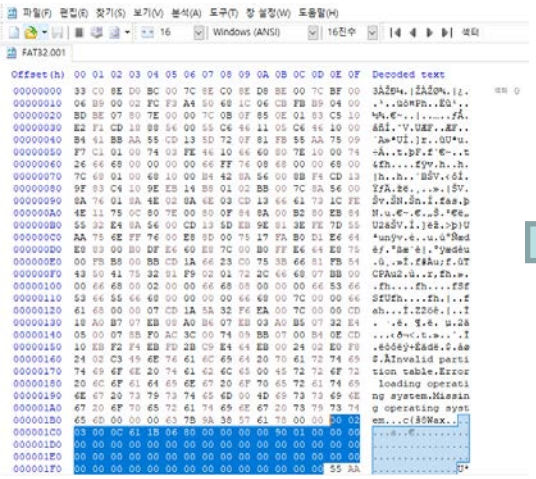


- 손상된 이미지 파일임을 확인
- 파일시스템 확인과 복구 위해 HxD(HexEditor) 실행

(실습) 파티션 복구

2. HexEditor, MBR 확인

*리틀 엔디언 방식



[MBR Partition Table Entry]

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0x00															Boot Flag	
0x10	Starting CHS Address		Part Type	Ending CHS Address			Starting LBA Address				Size in Sector					

[증거 이미지 MBR PartitionTable Entry]

```
000001A0  67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74
000001B0  65 6D 00 00 00 63 7B 9A 38 57 61 78 00 00 00 02
000001C0  03 00 0C 61 1B 06 80 00 00 00 00 90 01 00 00 00
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA
00000200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

파티션의 시작 섹터(16진수) : 0x00000080
총 섹터 수(16진수) : 0x00019000

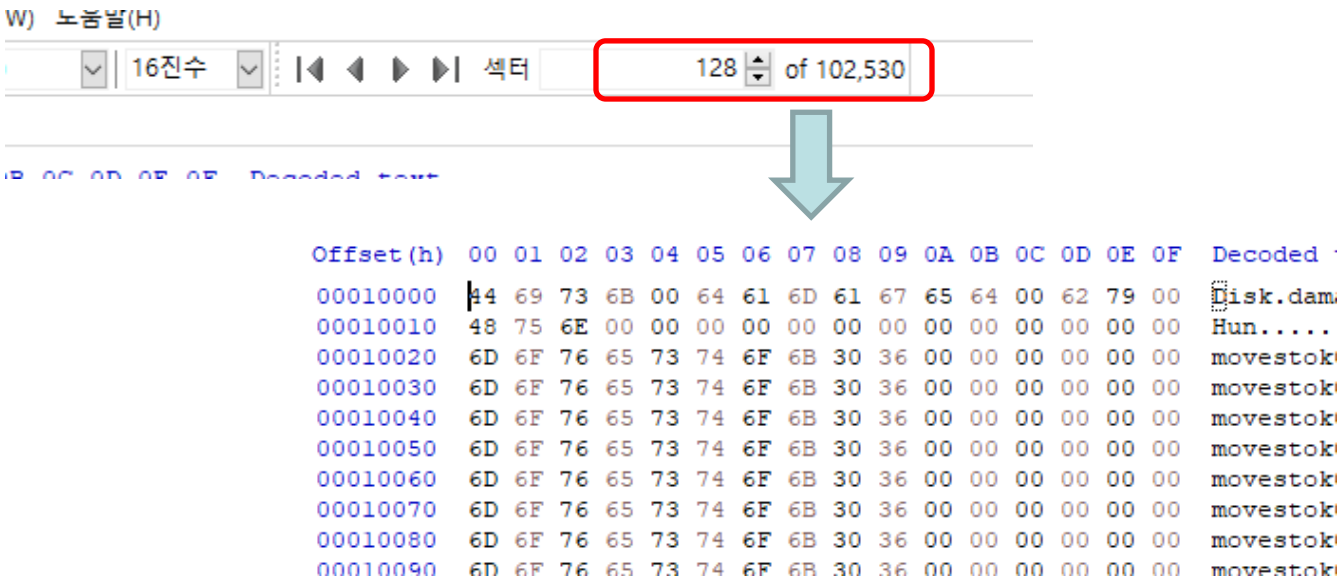
- 파티션 정보를 찾기 위해 MBR부터 조사
- 512바이트 구성 MBR의 파티션 테이블 확인

(실습) 파티션 복구

3. HexEditor, BR0이동

HEX	80
DEC	128

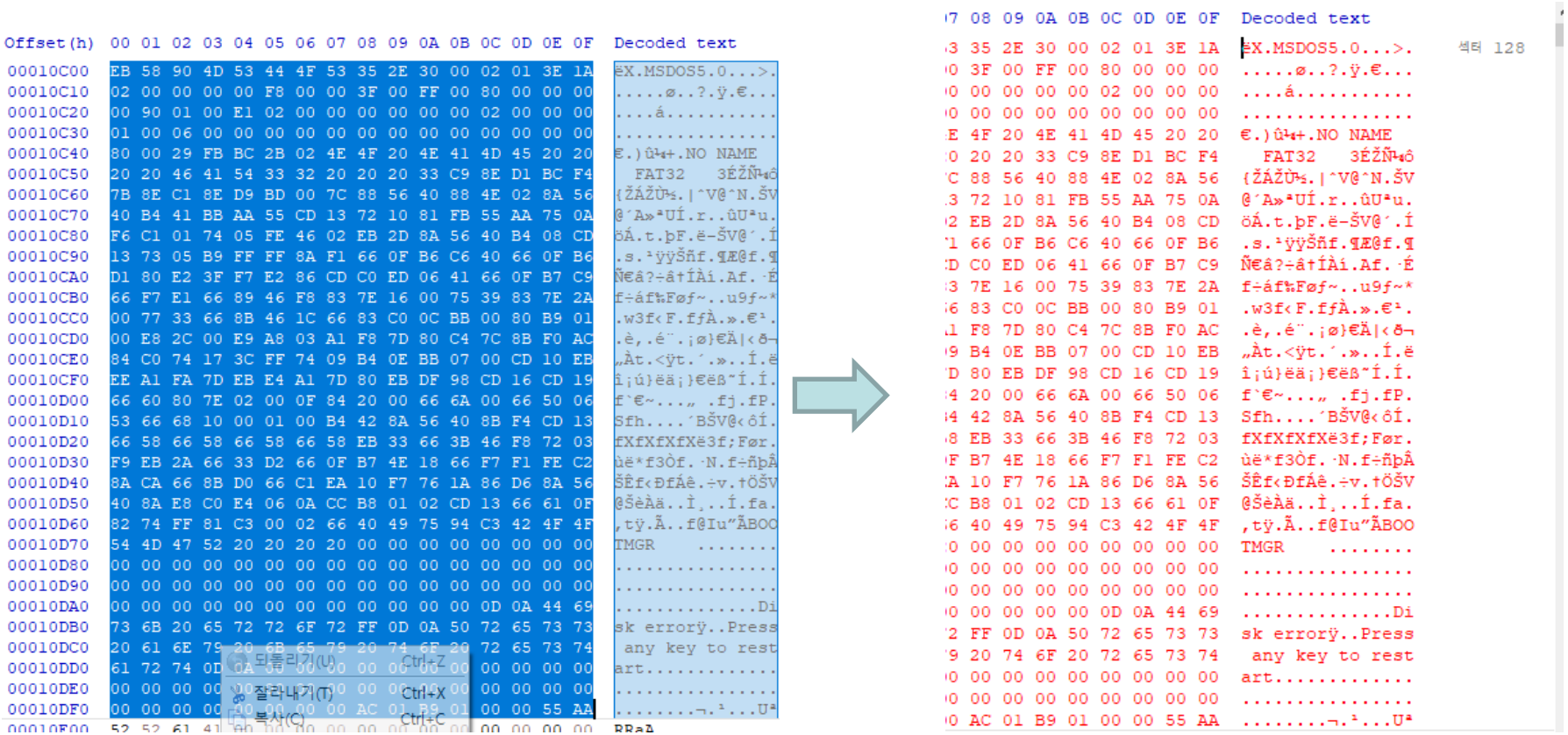
- 파티션의 시작 섹터(16진수) : 0x00000080 ➔ 첫 파티션 128섹터에 위치
- 총 섹터 수(16진수) : 0x00019000 ➔ 섹터 수 계산으로 총 용량 계산 가능



- 부트 레코드 삭제되어 있음
- FAT32는 BR 백업본을 파티션의 시작위치에서 6번째 섹터에 저장

(실습) 파티션 복구

3. HexEditor, BR 백업본으로 원본 BR복구



Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

00010C00 EB 58 90 4D 53 44 4F 53 35 2E 30 00 02 01 3E 1A ëX.MSDOS5.0...>.
00010C10 02 00 00 00 00 F8 00 00 3F 00 FF 00 80 00 00 00 .....ø..?.ÿ.€...
00010C20 00 90 01 00 E1 02 00 00 00 00 00 00 02 00 00 00 ....á...........
00010C30 01 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010C40 80 00 29 FB BC 2B 02 4E 4F 20 4E 41 4D 45 20 20 €.)û¼+.NO NAME
00010C50 20 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4 FAT32 3ÉŽÑ¼ô
00010C60 7B 8E C1 8E D9 BD 00 7C 88 56 40 88 4E 02 8A 56 {ŽÁŽÙ½.|ˆV@ˆN.ŠV
00010C70 40 B4 41 BB AA 55 CD 13 72 10 81 FB 55 AA 75 0A @´A»ªUÍ.r..ûUªu.
00010C80 F6 C1 01 74 05 FE 46 02 EB 2D 8A 56 40 B4 08 CD öÁ.t.þF.ë-ŠV@´.Í
00010C90 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66 0F B6 .s.¹ÿÿŠñf.¶Æ@f.¶
00010CA0 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7 C9 Ñ€â?÷â†ÍÀí.Af.·É
00010CB0 66 F7 E1 66 89 46 F8 83 7E 16 00 75 39 83 7E 2A f÷áf‰Føƒ~..u9ƒ~*
00010CC0 00 77 33 66 8B 46 1C 66 83 C0 0C BB 00 80 B9 01 .w3f‹F.fƒÀ.».€¹.
00010CD0 00 E8 2C 00 E9 A8 03 A1 F8 7D 80 C4 7C 8B F0 AC .è,.é¨.¡ø}€Ä|‹ð¬
00010CE0 84 C0 74 17 3C FF 74 09 B4 0E BB 07 00 CD 10 EB „Àt.<ÿt.´.».Í.ë
00010CF0 EE A1 FA 7D EB E4 A1 7D 80 EB DF 98 CD 16 CD 19 î¡ú}ëä¡}€ëß˜Í.Í.
00010D00 66 60 80 7E 02 00 0F 84 20 00 66 6A 00 66 50 06 f`€~...„ .fj.fP.
00010D10 53 66 68 10 00 01 00 B4 42 8A 56 40 8B F4 CD 13 Sfh....´BŠV@‹ôÍ.
00010D20 66 58 66 58 66 58 66 58 EB 33 66 3B 46 F8 72 03 fXfXfXfXë3f;Førˆ.
00010D30 F9 EB 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE C2 ùë*f3Òf.·N.f÷ñþÂ
00010D40 8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A 56 ŠÊf‹ÐfÁê.÷v.†ÖŠV
00010D50 40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61 0F @ŠèÀä..Ì¸..Í.fa.
00010D60 82 74 FF 81 C3 00 02 66 40 49 75 94 C3 42 4F 4F ‚tÿ.Ã..f@Iu”ÃBOO
00010D70 54 4D 47 52 20 20 20 20 00 00 00 00 00 00 00 00 TMGR ....
00010D80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010D90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010DA0 00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 44 69 ....Di
00010DB0 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73 sk errorÿ..Press
00010DC0 20 61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 any key to rest
00010DD0 61 72 74 0D 0A 00 00 00 00 00 00 00 00 00 00 00 art.............
00010DE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010DF0 00 00 00 00 00 00 00 00 AC 01 B9 01 00 00 55 AA ....¬.¹...Uª
00010E00 52 52 61 41 00 00 00 00 00 00 00 00 00 00 00 00 RRaA

되돌리기(U) Ctrl+Z
잘라내기(T) Ctrl+X
복사(C) Ctrl+C

[백업 BR섹터 134]

7 08 09 0A 0B 0C 0D 0E 0F Decoded text

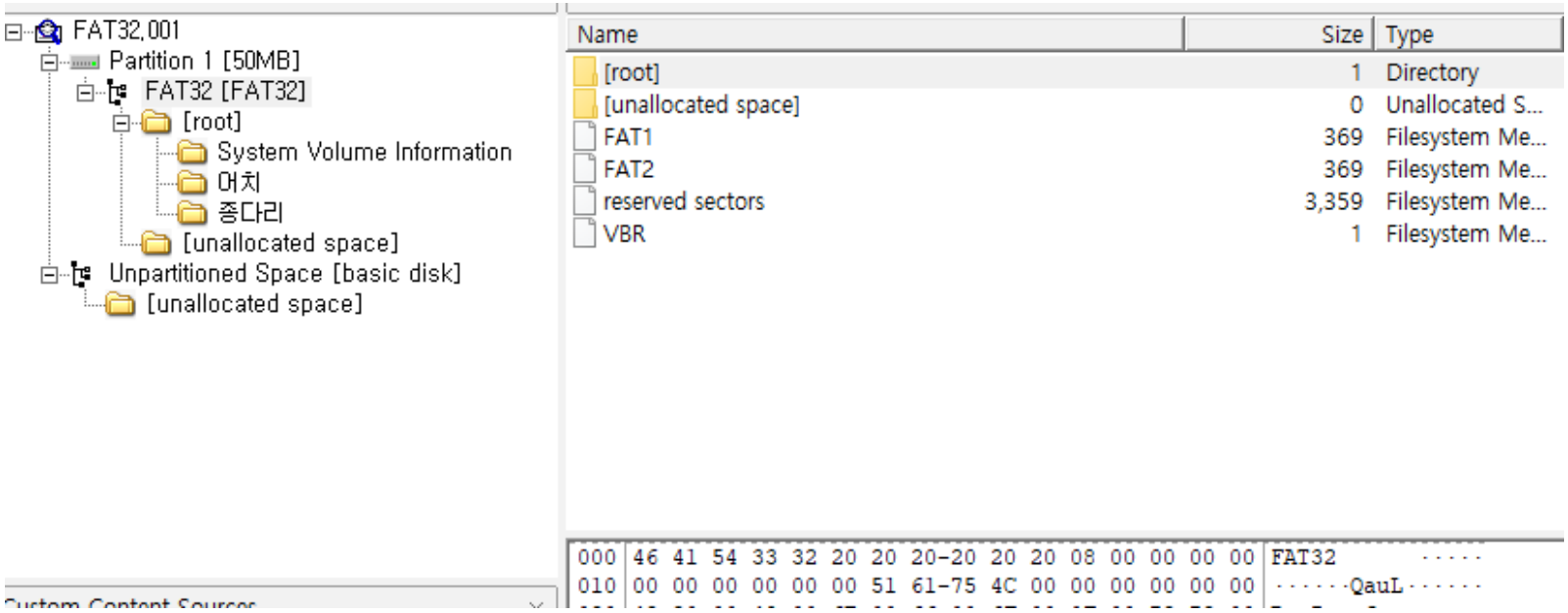
3 35 2E 30 00 02 01 3E 1A ëX.MSDOS5.0...>. 섹터 128
0 3F 00 FF 00 80 00 00 00 .....ø..?.ÿ.€...
0 00 00 00 00 02 00 00 00 ....á...........
0 00 00 00 00 00 00 00 00 ....
E 4F 20 4E 41 4D 45 20 20 €.)û¼+.NO NAME
0 20 20 33 C9 8E D1 BC F4 FAT32 3ÉŽÑ¼ô
C 88 56 40 88 4E 02 8A 56 {ŽÁŽÙ½.|ˆV@ˆN.ŠV
3 72 10 81 FB 55 AA 75 0A @´A»ªUÍ.r..ûUªu.
2 EB 2D 8A 56 40 B4 08 CD öÁ.t.þF.ë-ŠV@´.Í
1 66 0F B6 C6 40 66 0F B6 .s.¹ÿÿŠñf.¶Æ@f.¶
D C0 ED 06 41 66 0F B7 C9 Ñ€â?÷â†ÍÀí.Af.·É
3 7E 16 00 75 39 83 7E 2A f÷áf‰Føƒ~..u9ƒ~*
6 83 C0 0C BB 00 80 B9 01 .w3f‹F.fƒÀ.».€¹.
1 F8 7D 80 C4 7C 8B F0 AC .è,.é¨.¡ø}€Ä|‹ð¬
9 B4 0E BB 07 00 CD 10 EB „Àt.<ÿt.´.».Í.ë
D 80 EB DF 98 CD 16 CD 19 î¡ú}ëä¡}€ëß˜Í.Í.
4 20 00 66 6A 00 66 50 06 f`€~...„ .fj.fP.
4 42 8A 56 40 8B F4 CD 13 Sfh....´BŠV@‹ôÍ.
8 EB 33 66 3B 46 F8 72 03 fXfXfXfXë3f;Førˆ.
F B7 4E 18 66 F7 F1 FE C2 ùë*f3Òf.·N.f÷ñþÂ
A 10 F7 76 1A 86 D6 8A 56 ŠÊf‹ÐfÁê.÷v.†ÖŠV
C B8 01 02 CD 13 66 61 0F @ŠèÀä..Ì¸..Í.fa.
6 40 49 75 94 C3 42 4F 4F ‚tÿ.Ã..f@Iu”ÃBOO
0 00 00 00 00 00 00 00 00 TMGR ....
0 00 00 00 00 00 00 00 00 ....
0 00 00 00 00 00 00 00 00 ....
0 00 00 00 00 0D 0A 44 69 ....Di
2 FF 0D 0A 50 72 65 73 73 sk errorÿ..Press
9 20 74 6F 20 72 65 73 74 any key to rest
0 00 00 00 00 00 00 00 00 art.............
0 00 00 00 00 00 00 00 00 ....
0 AC 01 B9 01 00 00 55 AA ....¬.¹...Uª

[원본 BR섹터 128]

- 백업된 BR 섹터(134)를 복사하여 원래의 BR 섹터(128)로 '붙여넣기 쓰기'
- 저장

(실습) 파티션 복구

4. 복구 파일 확인



- FTK Imager에서 파티션이 정상적으로 복구되었는지 확인
- '어치' 에 있는 파일목록 캡처하여 bgwon214@gmail.com로 제출

참고문헌

- 정보 보안 개론[개정3판], 양대일 저, 한빛미디어, 2018, 1.
- 디지털 포렌식 개론(2판), 이상진 저, 이룬 출판사, 2015. 5.
- 파티션 설명 및 복구이미지 파일 naver.blog/bitnang, 2014.11
- 컴퓨터보안, William Stalling 저, 한티미디어, 2016. 8
- 정보보안과 사이버 해킹의 기초, 김경신 저, 2016. 8

Q & A