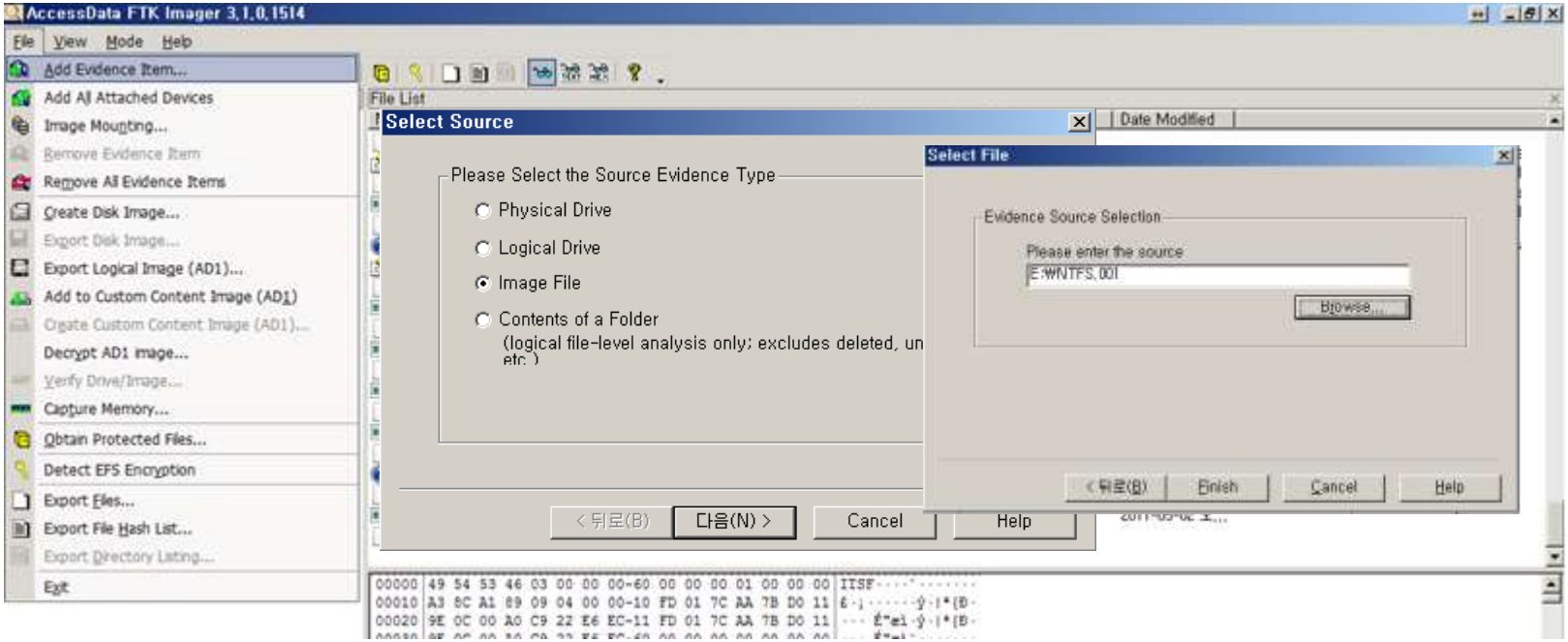
보안실습 7-1

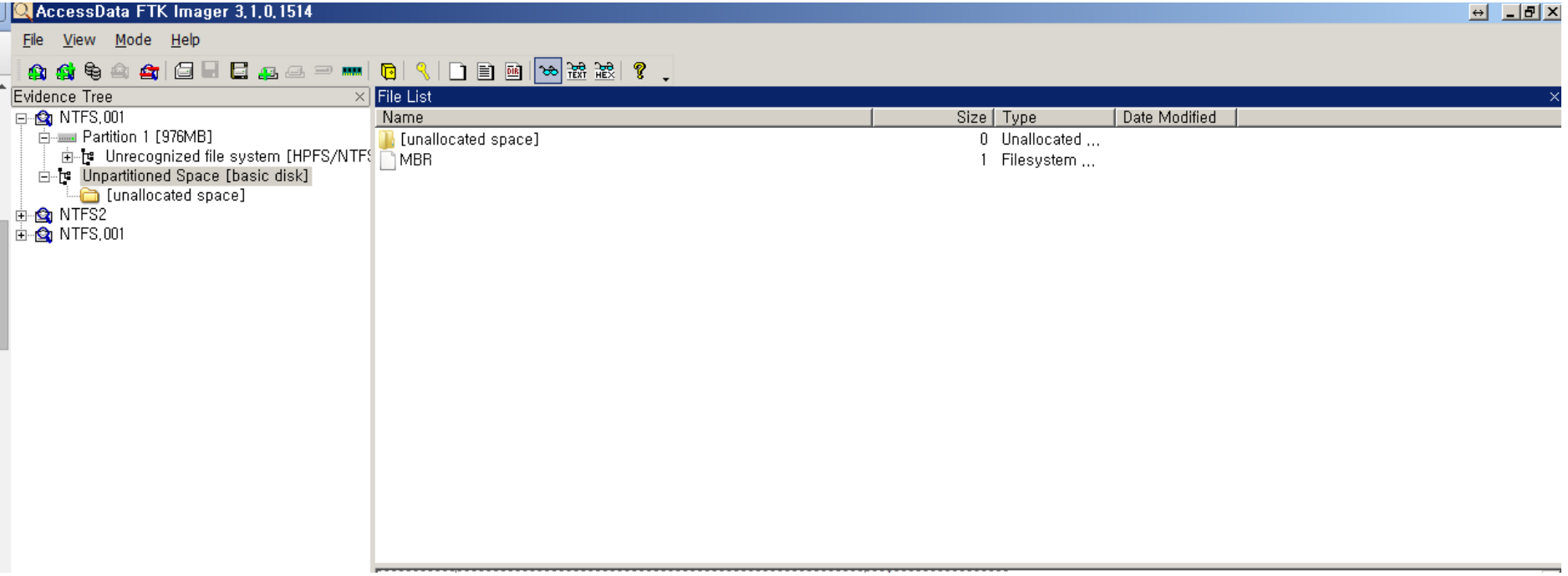
[NTFS 파티션 헤더 복구하기]

FTK Imager를 이용하여 주어진 NTFS 이미지를 열어보자



보안실습 7-1

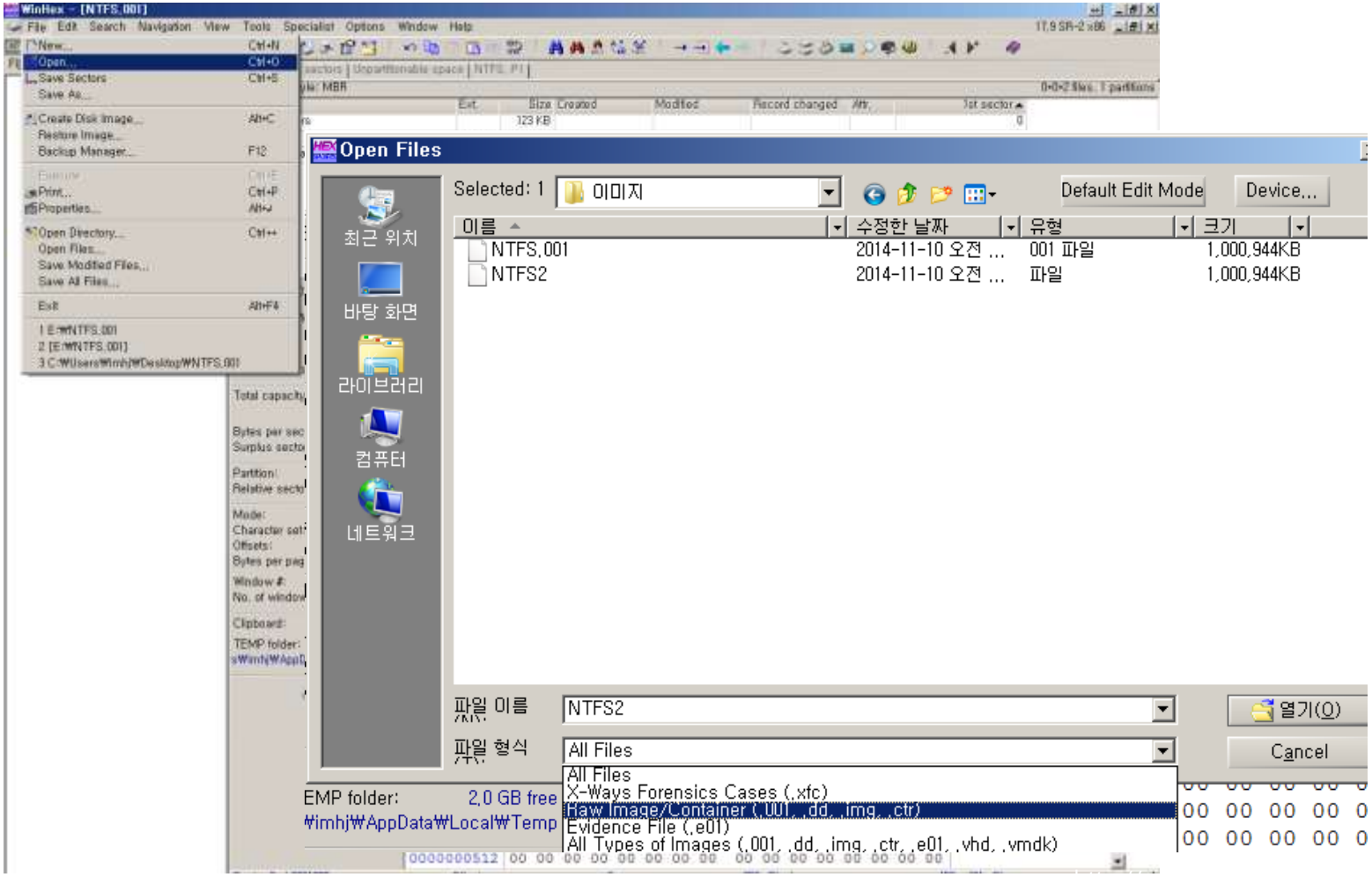
[NTFS 파티션 헤더 복구하기]



아무런 내용을 볼 수 없다는 것을 확인할 수 있다.

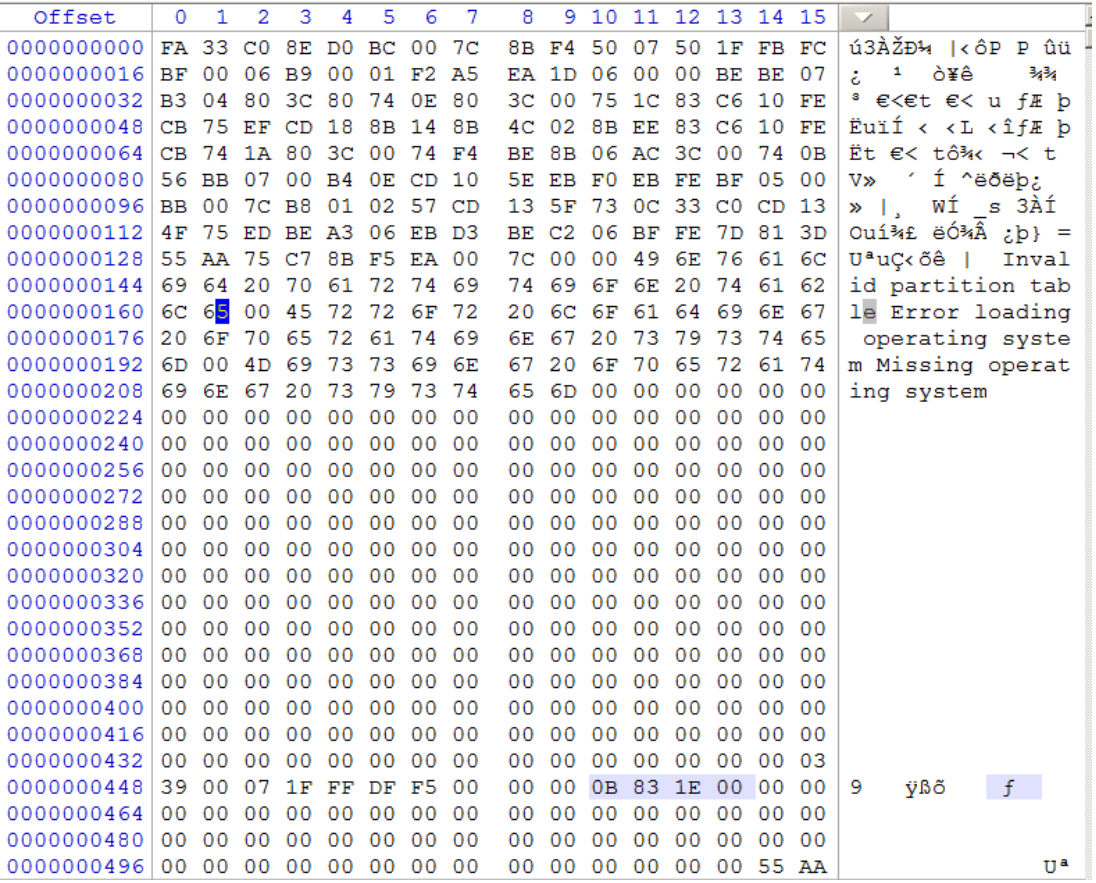
보안실습 7-1

X-Ways WinHex 실행 및 파일 이미지 불러오기



보안실습 7-1

X-Ways WinHex 를 통한 MBR 확인



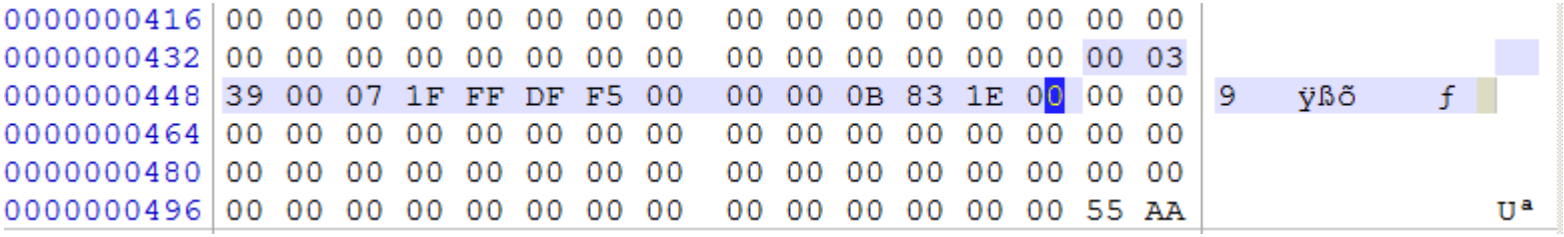
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000000000	FA	33	C0	8E	D0	BC	00	7C	8B	F4	50	07	50	1F	FB	FC
0000000016	BF	00	06	B9	00	01	F2	A5	EA	1D	06	00	00	BE	BE	07
0000000032	B3	04	80	3C	80	74	0E	80	3C	00	75	1C	83	C6	10	FE
0000000048	CB	75	EF	CD	18	8B	14	8B	4C	02	8B	EE	83	C6	10	FE
0000000064	CB	74	1A	80	3C	00	74	F4	BE	8B	06	AC	3C	00	74	0B
0000000080	56	BB	07	00	B4	0E	CD	10	5E	EB	F0	EB	FE	BF	05	00
0000000096	BB	00	7C	B8	01	02	57	CD	13	5F	73	0C	33	C0	CD	13
0000000112	4F	75	ED	BE	A3	06	EB	D3	BE	C2	06	BF	FE	7D	81	3D
0000000128	55	AA	75	C7	8B	F5	EA	00	7C	00	00	49	6E	76	61	6C
0000000144	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61	62
0000000160	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	67
0000000176	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	65
0000000192	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61	74
0000000208	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00	00
0000000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	03
0000000448	39	00	07	1F	FF	DF	F5	00	00	00	0B	83	1E	00	00	00
0000000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

MBR (Master Boot Record)를 확인할 수 있음.

Master Boot Code(446 byte)
(01BE) 첫번째 프리머리 파티션 테이블(16 byte)
(01CE)두번째 프리머리 파티션 테이블(16 byte)
(01DE)세번째 프리머리 파티션 테이블(16 byte)
(01EE)네번째 프리머리 파티션 테이블(16 byte)
시그니처 0x55 AA(2 byte)

보안실습 7-1

[파티션 테이블 확인]



0000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	03
0000000448	39	00	07	1F	FF	DF	F5	00	00	00	0B	83	1E	00	00	00
0000000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

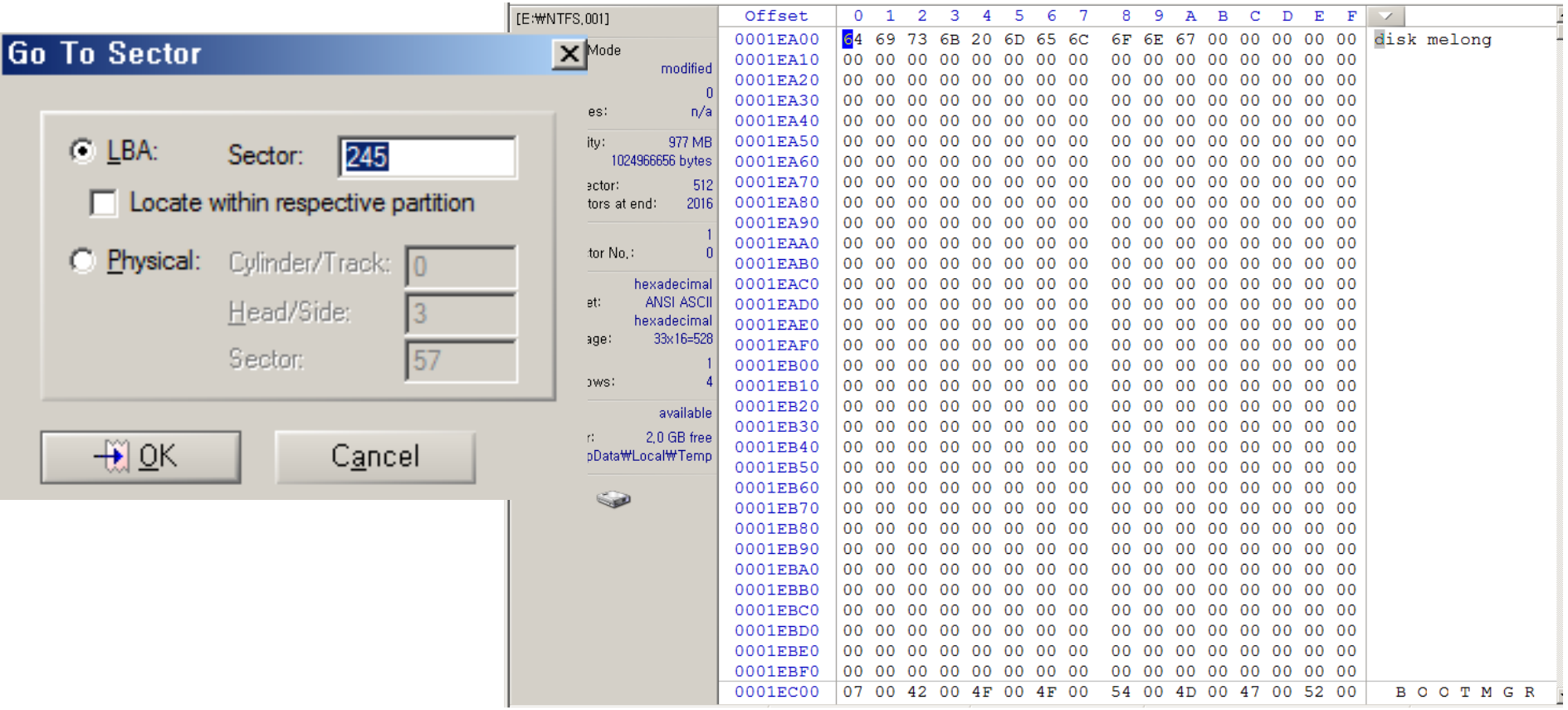
※ 리틀 엔디언 방식으로 표기되어 있으므로 거꾸로 읽어야함

1 바이트 -> 부팅 활성화 [00 : 부팅 안함]
3 바이트 -> 파티션의 위치를 CHS로 표시 [00 39 03]
1 바이트 -> NTFS [07 : NTFS]
3 바이트 -> 파티션의 마지막 위치를 CHS로 표시[DF FF 1F]
4 바이트 -> 파티션 시작 위치를 LBA 방식으로 표기 함
[00 00 00 F5 : F5섹터부터 파티션이 시작됨]
4 바이트 -> 파티션의 크기 [00 1E 83 0B]

보안실습 7-1

[파티션 이동]

Ctrl+g 단축키를 이용한 섹터 이동



보안실습 7-1

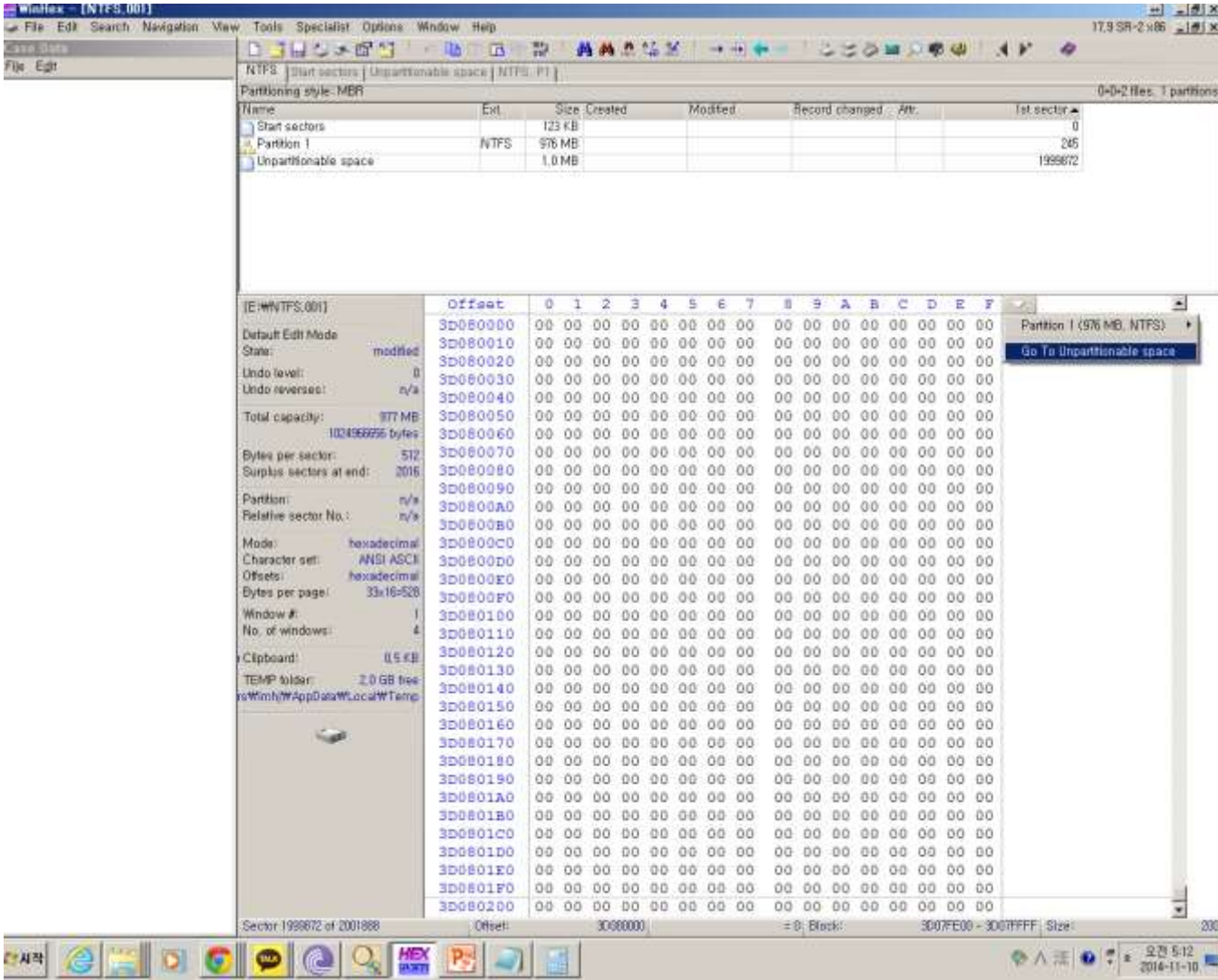
[파티션 이동]

- NTFS 마지막 섹터로 이동

MBR에서 확인한 파티션
크기를 이용해
직접 Sector로 이동

OR

오른쪽 그림과 같이
툴을 이용한 이동

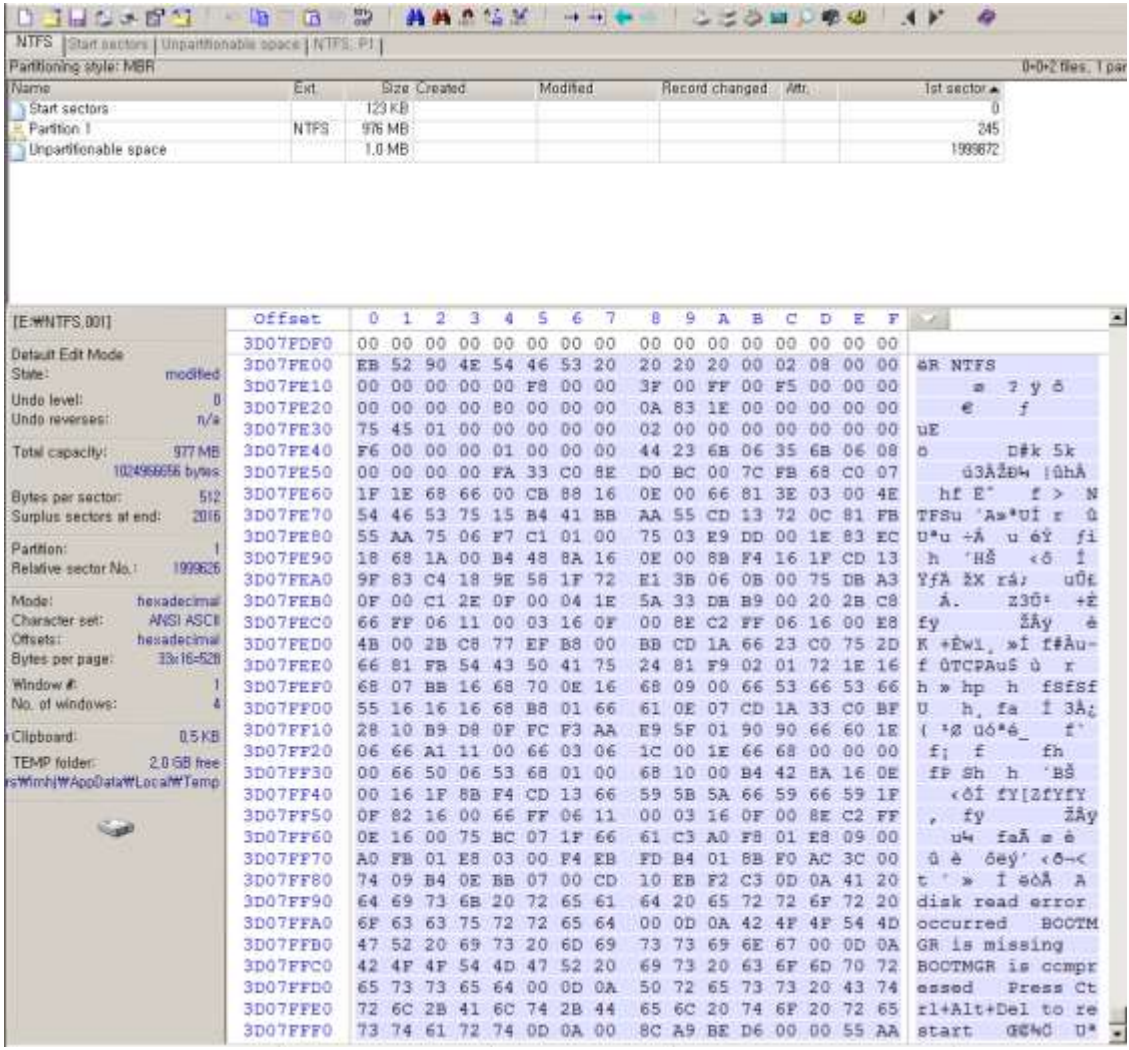


보안실습 7-1

[파티션 이동]

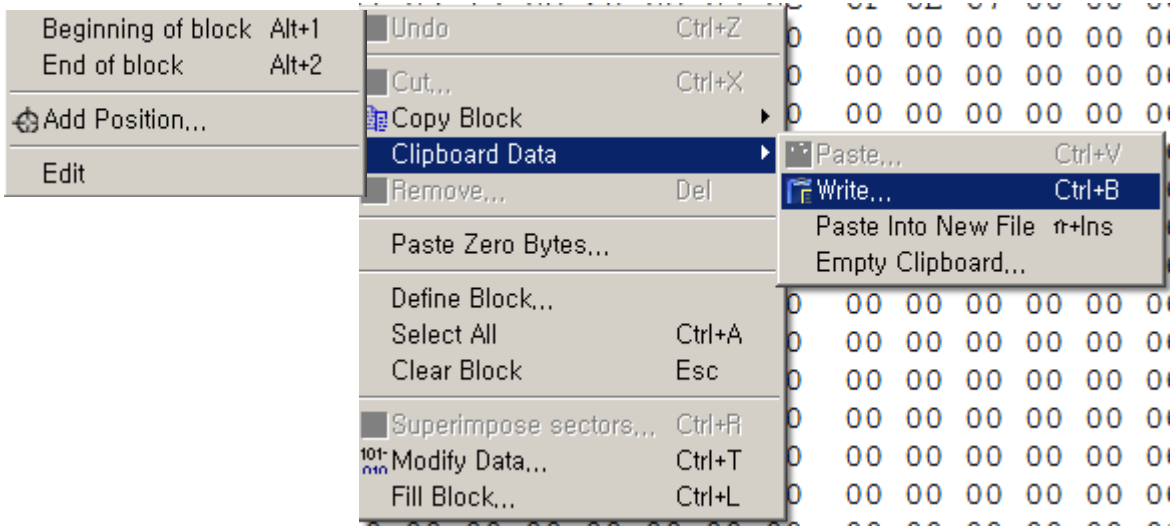
NTFS 의 마지막 섹터에 복사본이 위치한 걸 알 수 있습니다.

이를 복사하여 파티션 헤더 부분에 복사
우클릭 - edit - Copy Block - Hex Values



보안실습 7-1

[파티션 헤더 복구]



보안실습 7-1

[새로 저장하기]

본 파일을 다시 FTK로 열어보면 파티션이 복구되어 보이지 않던 파일이 보이는 것을 확인 할 수 있음.