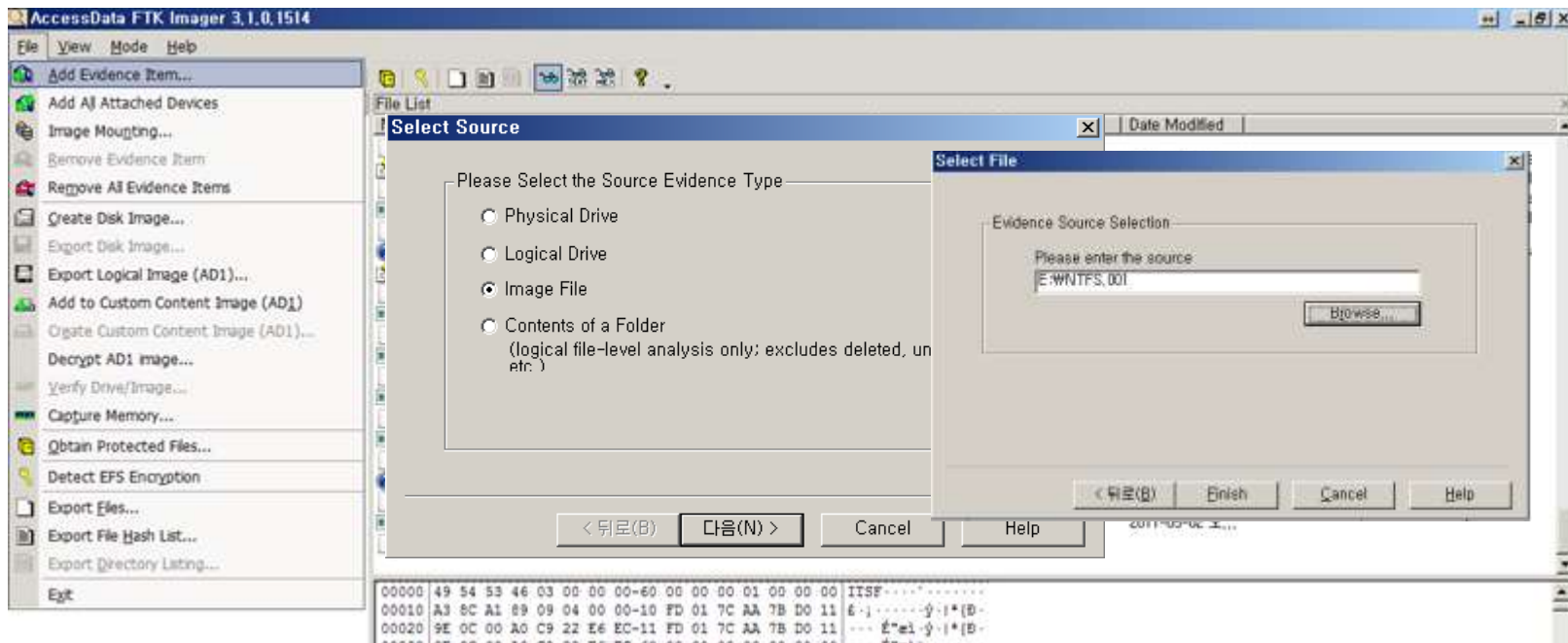


보안실습 7-1

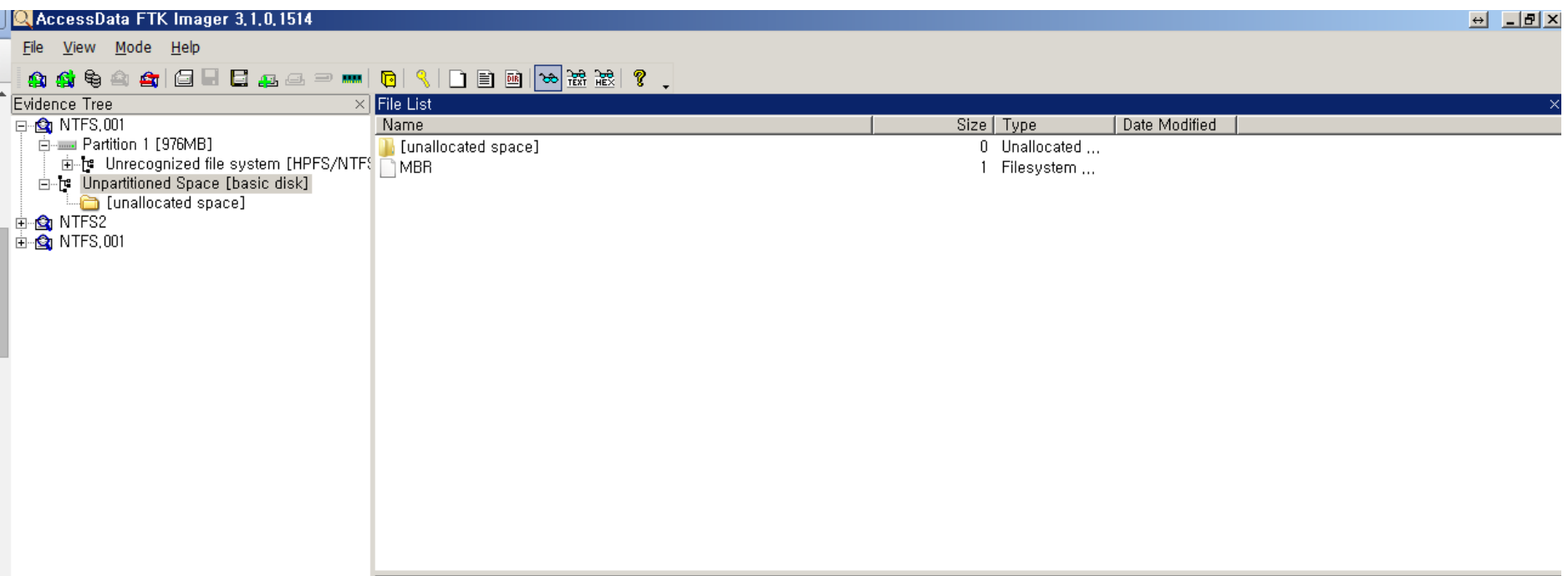
[NTFS 파티션 헤더 복구하기]

FTK Imager를 이용하여 주어진 NTFS 이미지를 열어보자



보안실습 7-1

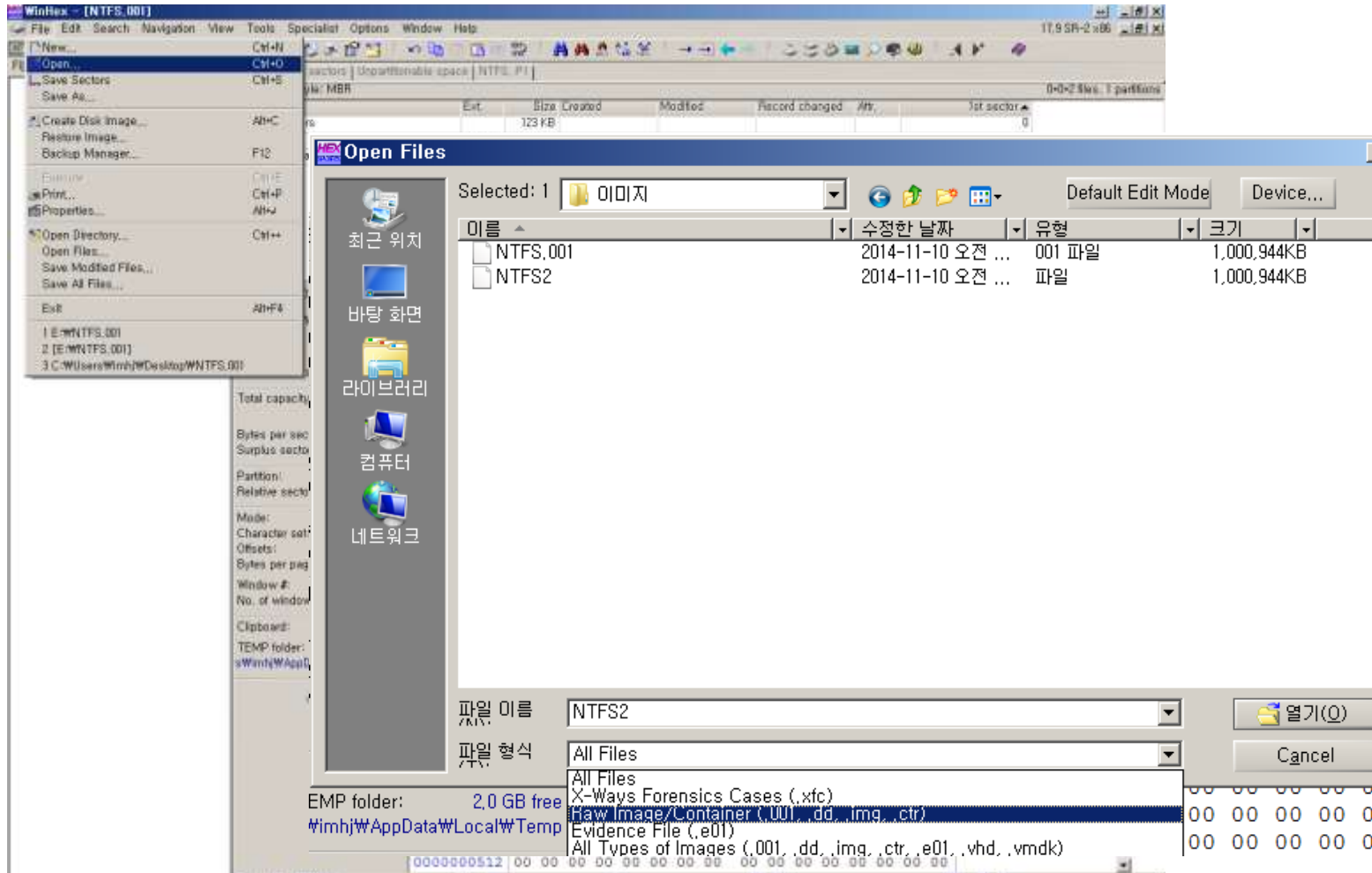
[NTFS 파티션 헤더 복구하기]



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	ú3ÀŽĐ¼ <ôP P ûú
0000000016	BF	00	06	B9	00	01	F2	A5	EA	1D	06	00	00	BE	BE	07	¿ ¹ ò¥è ¾¾
0000000032	B3	04	80	3C	80	74	0E	80	3C	00	75	1C	83	C6	10	FE	* €<et €< u fÆ þ
0000000048	CB	75	EF	CD	18	8B	14	8B	4C	02	8B	EE	83	C6	10	FE	ÈuíÍ < <L <íÆ þ
0000000064	CB	74	1A	80	3C	00	74	F4	BE	8B	06	AC	3C	00	74	0B	Èt €< tð¾< -< t
0000000080	56	BB	07	00	B4	0E	CD	10	5E	EB	F0	EB	FE	BF	05	00	V» ' í ^èðèþ¿
0000000096	BB	00	7C	B8	01	02	57	CD	13	5F	73	0C	33	C0	CD	13	» , WÍ _s 3ÀÍ
0000000112	4F	75	ED	BE	A3	06	EB	D3	BE	C2	06	BF	FE	7D	81	3D	Ouí¾ èÓ¾À ¿þ} =
0000000128	55	AA	75	C7	8B	F5	EA	00	7C	00	00	49	6E	76	61	6C	UªuÇ<ðè Inval
0000000144	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61	62	id partition tab
0000000160	6C	6E	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	67	l Error loading
0000000176	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	65	operating syste
0000000192	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61	74	m Missing operat
0000000208	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00	00	ing system
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	00	
0000000448	39	00	07	1F	FF	DF	F5	00	00	00	0B	83	1E	00	00	00	9 yRð f
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	Uª

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	9 ÿßð f U ^a
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

Go To Sector

☒ **LBA:** Sector:

☐ Locate within respective partition

☐ **Physical:** Cylinder/Track:
Head/Side:
Sector:

[E:\WNTFS,001]

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0001EA00	4	69	73	6B	20	6D	65	6C	6F	6E	67	00	00	00	00	00
0001EA10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EA20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EA30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EA40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EA50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EA60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EA70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EA80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EA90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EAA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EAB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EAC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EAD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EAE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EAF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EB90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EBA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EBB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EBC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EBD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EBE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EBF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0001EC00	07	00	42	00	4F	00	4F	00	54	00	4D	00	47	00	52	00

disk melong

B O O T M G R

보안실습 7-1

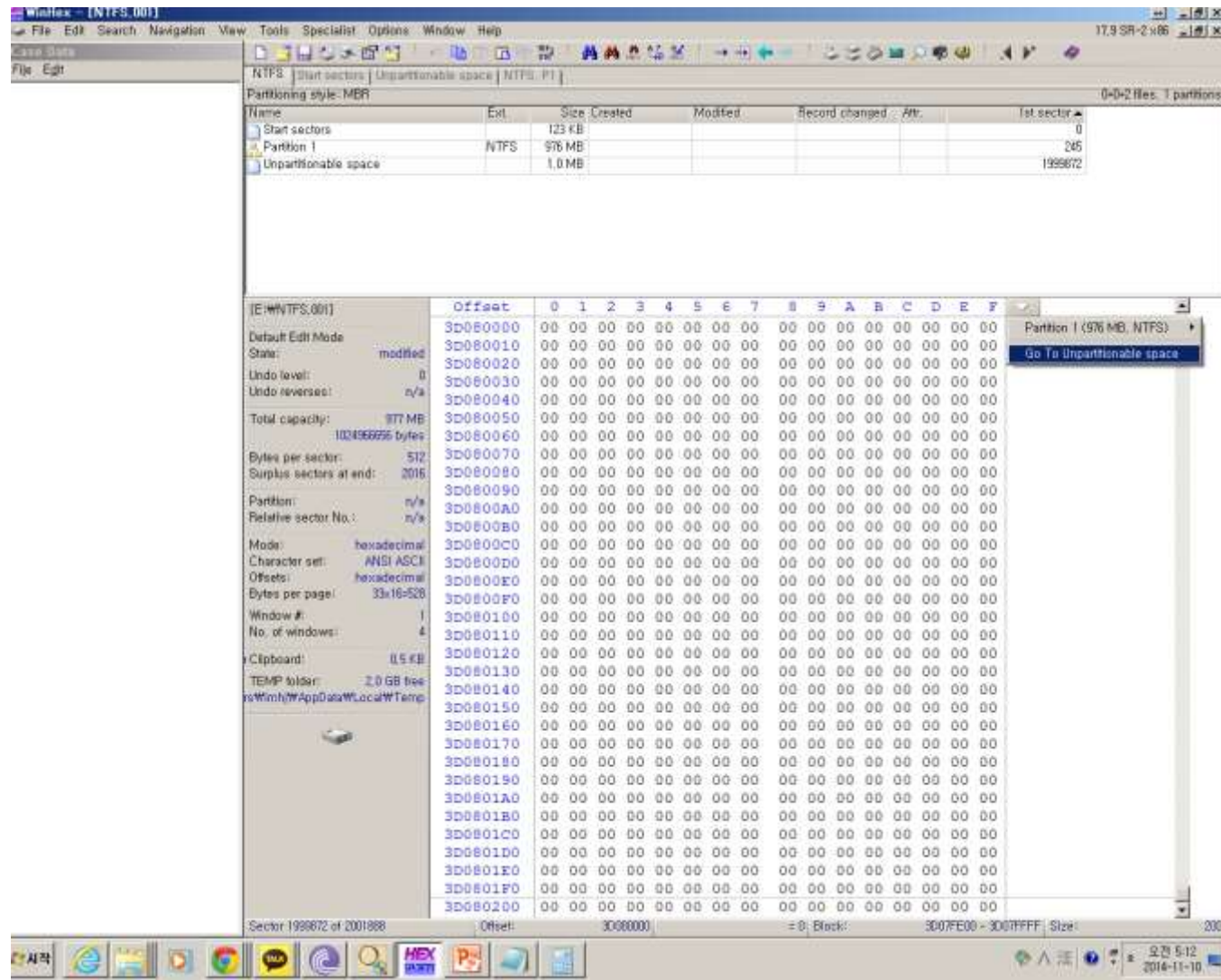
[파티션 이동]

- 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

The screenshot displays a disk partitioning tool interface. The top pane shows the partition table with the following details:

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Start sectors		123 KB					0
Partition 1	NTFS	976 MB					245
Unpartitionable space		1.0 MB					1999872

The bottom pane shows the hex editor view of the NTFS partition header. The left sidebar lists various fields and their values:

- Default Edit Mode: modified
- State: modified
- Undo level: 0
- Undo reverses: n/a
- Total capacity: 977 MB
- 102496656 bytes
- Bytes per sector: 512
- Surplus sectors at end: 2016
- Partition: 1
- Relative sector No.: 1999872
- Mode: hexadecimal
- Character set: ANSI ASCII
- Offsets: hexadecimal
- Bytes per page: 33x16-520
- Window #: 1
- No. of windows: 4
- Clipboard: 0.5 KB
- TEMP folder: 2.0 GB free
- rs\Winch\WAppData\Local\Temp

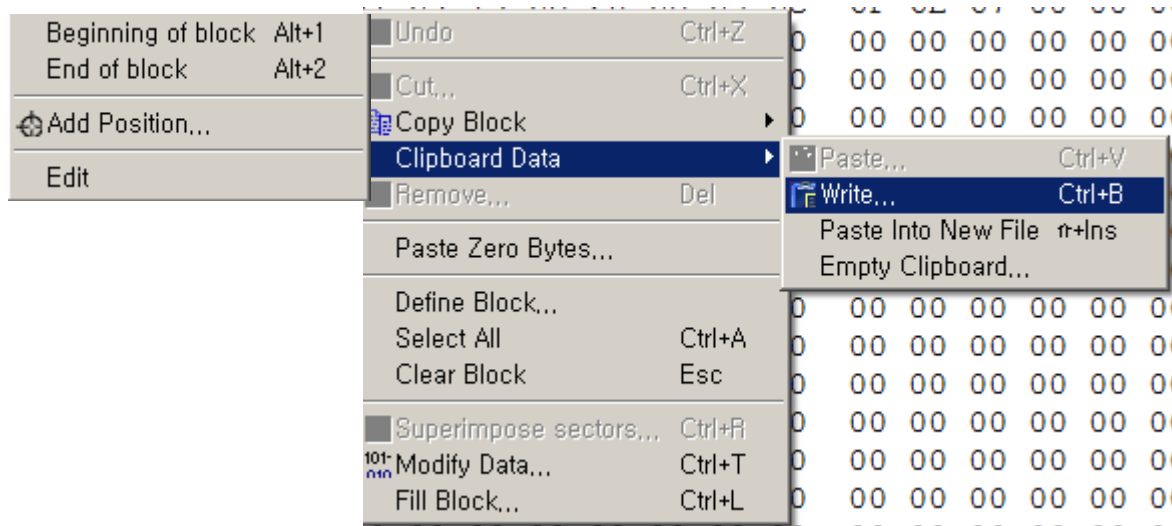
The main hex editor area shows the following data:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3D07FDF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
3D07FE00	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
3D07FE10	00	00	00	00	00	F8	00	00	3F	00	FF	00	F5	00	00	00
3D07FE20	00	00	00	00	80	00	00	00	0A	83	1E	00	00	00	00	00
3D07FE30	75	45	01	00	00	00	00	00	02	00	00	00	00	00	00	00
3D07FE40	F6	00	00	00	01	00	00	00	44	23	6B	06	35	6B	06	08
3D07FE50	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
3D07FE60	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E
3D07FE70	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB
3D07FE80	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC
3D07FE90	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13
3D07FEA0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3
3D07FEB0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8
3D07FEC0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8
3D07FED0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	0C	75	2D
3D07FEE0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16
3D07FEF0	68	07	BB	16	68	70	0E	16	68	09	00	66	53	66	53	66
3D07FFF0	55	16	16	16	68	BB	01	66	61	0E	07	CD	1A	33	C0	BF
3D07FF00	28	10	B9	D8	0F	FC	F3	AA	E9	5F	01	90	90	66	60	1E
3D07FF10	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00
3D07FF20	00	66	50	06	53	68	01	00	68	10	00	B4	42	BA	16	0E
3D07FF30	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F
3D07FF40	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF
3D07FF50	0E	16	00	75	BC	07	1F	66	61	C3	A0	F8	01	E8	09	00
3D07FF60	A0	FB	01	E8	03	00	F4	EB	FD	B4	01	8B	F0	AC	3C	00
3D07FF70	74	09	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20
3D07FF80	64	69	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20
3D07FF90	6F	63	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D
3D07FFA0	47	52	20	69	73	20	6D	69	73	73	69	6E	67	00	0D	0A
3D07FFB0	42	4F	4F	54	4D	47	52	20	69	73	20	63	6F	6D	70	72
3D07FFC0	65	73	73	65	64	00	0D	0A	50	72	65	73	73	20	43	74
3D07FFD0	72	6C	2B	41	6C	74	2B	44	65	6C	20	74	6F	20	72	65
3D07FFE0	73	74	61	72	74	0D	0A	00	8C	A9	BE	D6	00	00	55	AA

The right sidebar shows the ASCII representation of the hex data, which is mostly garbled text, indicating the start of an NTFS boot sector.

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.

