파티시스템 분석 복습
(MBR, EBR)

디지털포렌식 7기 김종훈
강대명 멘토님
파일시스템 분석 과목

목차

파일시스템 분석 복습

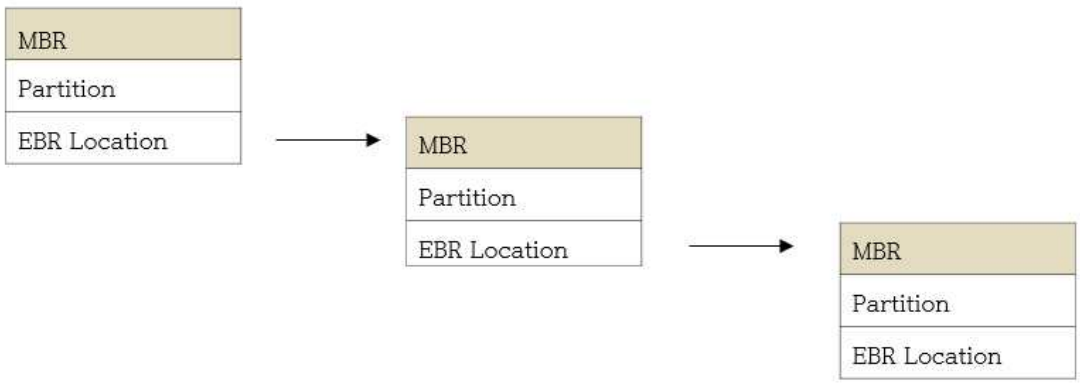
1. 이론

sha1: 6efc9ec1a9893fcf28fc708cc7181c19f27d5cce
size : 134,217,728(byte)

0번 sector에는 MBR(Master Boot Record)이 위치하며 디스크의 파티션테이블과 부트 로더를 포함하고 있다
부팅 순서는 다음과 같다.
1. POST(Power On Self-Test) 동작
2. BIOS에서 부팅 매체 읽음
3. 부팅 매체의 MBR을 읽음
4. 해당 내용을 메모리에 7C00h 에 복사
5. EIP(다음 인스트럭션)을 7C00h로 바꾸어 내용 시작
(부트로더가 MBR에 위치)

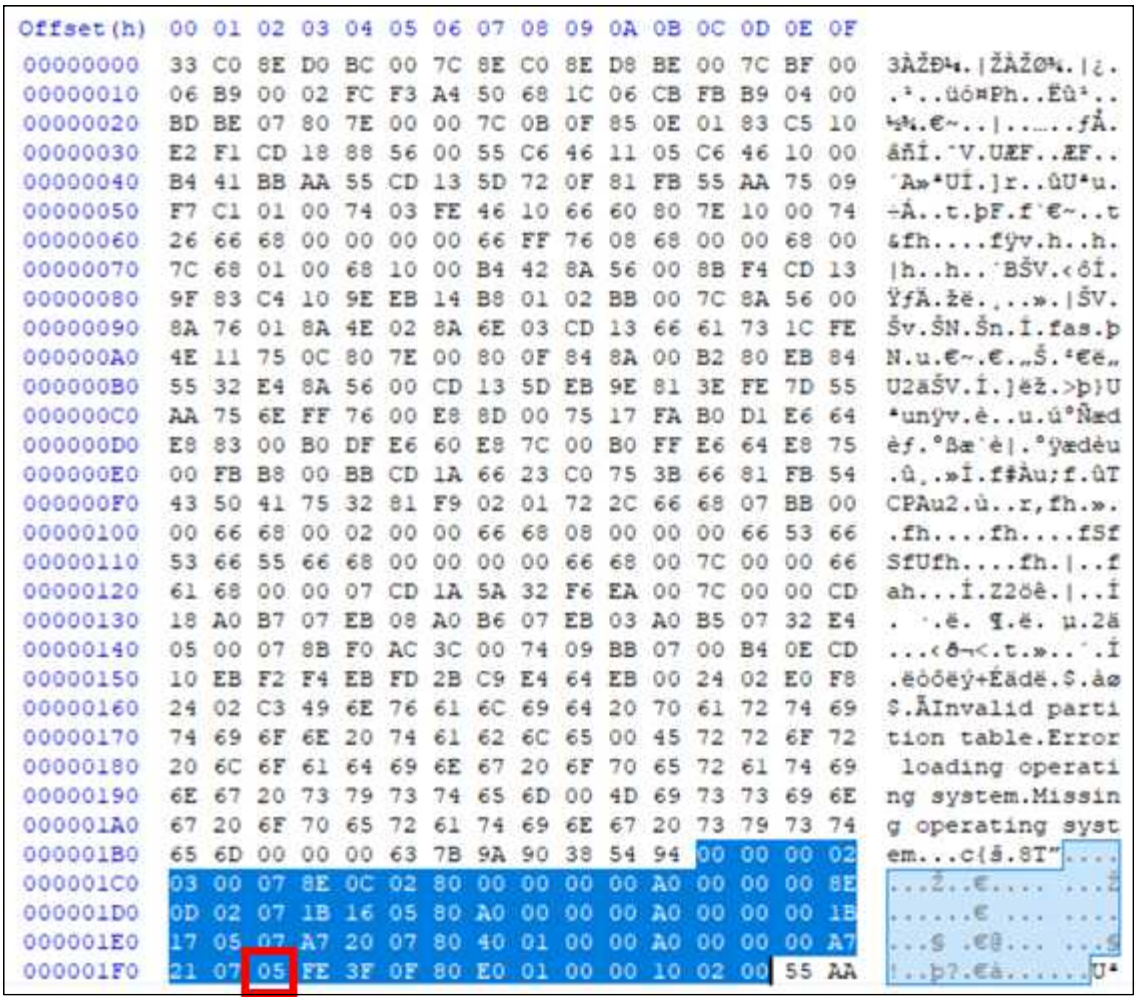
섹터는 512Bytes가 일반적이며 실습 과정에서도 512Bytes로 섹터를 구분한다.
512 bytes = 446Bytes(부트 코드) + 16(파티션 테이블 엔트리)*4 + 2(Signature(0x55AA))
파티션 테이블 엔트리에 처음 1바이트로 부팅이 가능한지 아닌지 확인할 수 있다.
0x80 : 부팅가능 , 0x00 : 부팅 불가능
5바이트 위치를 가리키는 곳에서 파티션 타입을 확인할 수 있다.
0x0b : FAT32, 0x07 : NTFS, 0x05 : EBR(다중 파티션)

다중 파티션의 경우 파티션 테이블 엔트리에서 파티션 타입이 05로 이루어져 있다면 0x05 값을 가리키며 이는 확장 파티션이 있다는 뜻이고 CHS Address를 통해 다음 확장 파티션의 주소로 넘어가면 파티션의 테이블 엔트리와 추가적인 확장파티션 정보를 확인할 수 있다.



2. 실습과정

[0 sector]

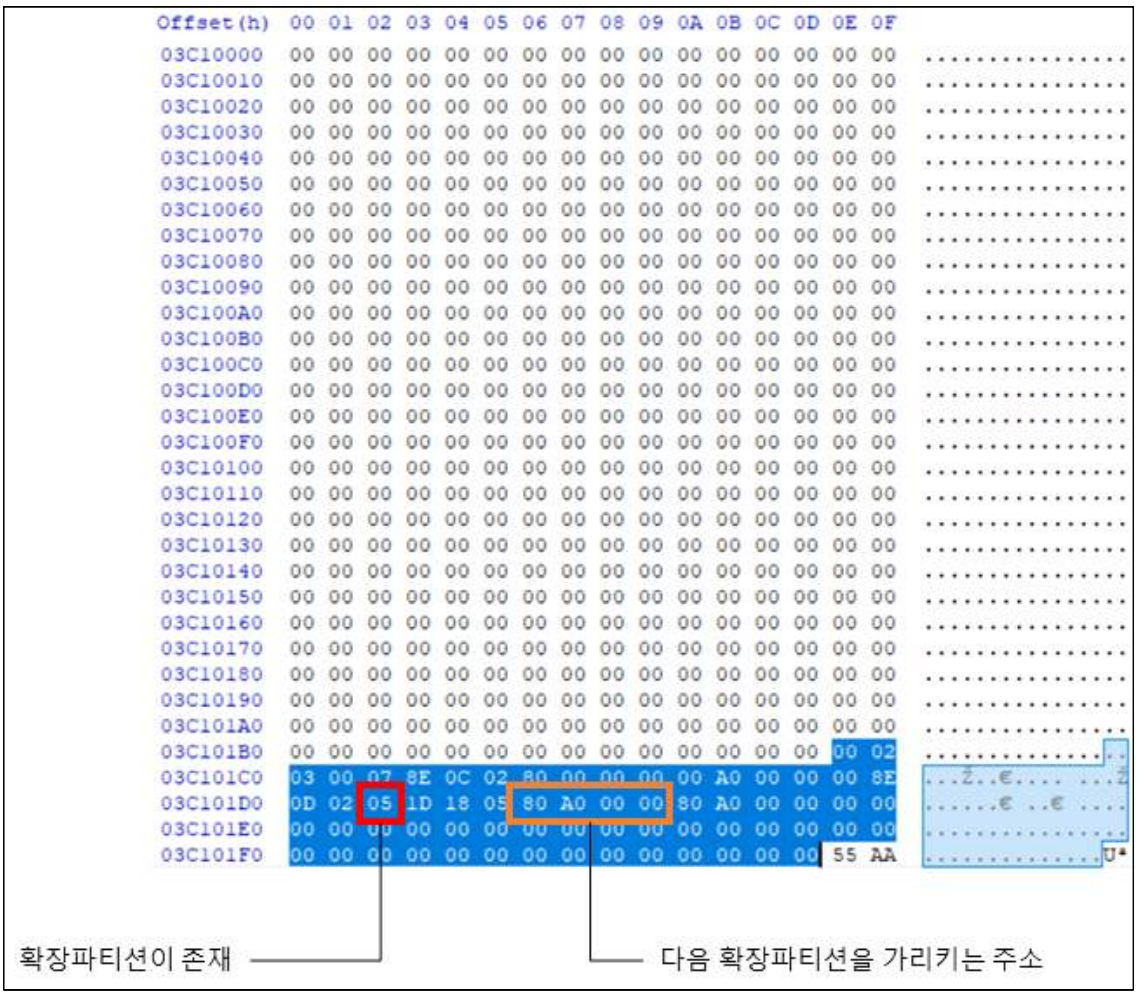


Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00
00000010	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00
00000020	BD	BE	07	80	7E	00	00	7C	0B	0F	85	0E	01	83	C5	10
00000030	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00
00000040	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09
00000050	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74
00000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00
00000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13
00000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00
00000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE
000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84
000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55
000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64
000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75
000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54
000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00
00000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66
00000110	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66
00000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD
00000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4
00000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD
00000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8
00000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69
00000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72
00000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69
00000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E
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	90	38	54	94	00	00	00	02
000001C0	03	00	07	8E	0C	02	80	00	00	00	00	A0	00	00	00	8E
000001D0	0D	02	07	1B	16	05	80	A0	00	00	00	A0	00	00	00	1B
000001E0	17	05	07	A7	20	07	80	40	01	00	00	A0	00	00	00	A7
000001F0	21	07	05	FE	3F	0F	80	E0	01	00	00	10	02	00	55	AA

	부팅	타입	주소	크기
1	00(불가)	NTFS	128(80)	20MB
2	00(불가)	NTFS	41088(A080)	20MB
3	00(불가)	NTFS	82048(14080)	20MB
4	00(불가)	EBR	123008(1E080)	?

4번째 파티션의 위치값을 확인하면 0x01E080이며 10진수로 123008섹터에 위치한다.

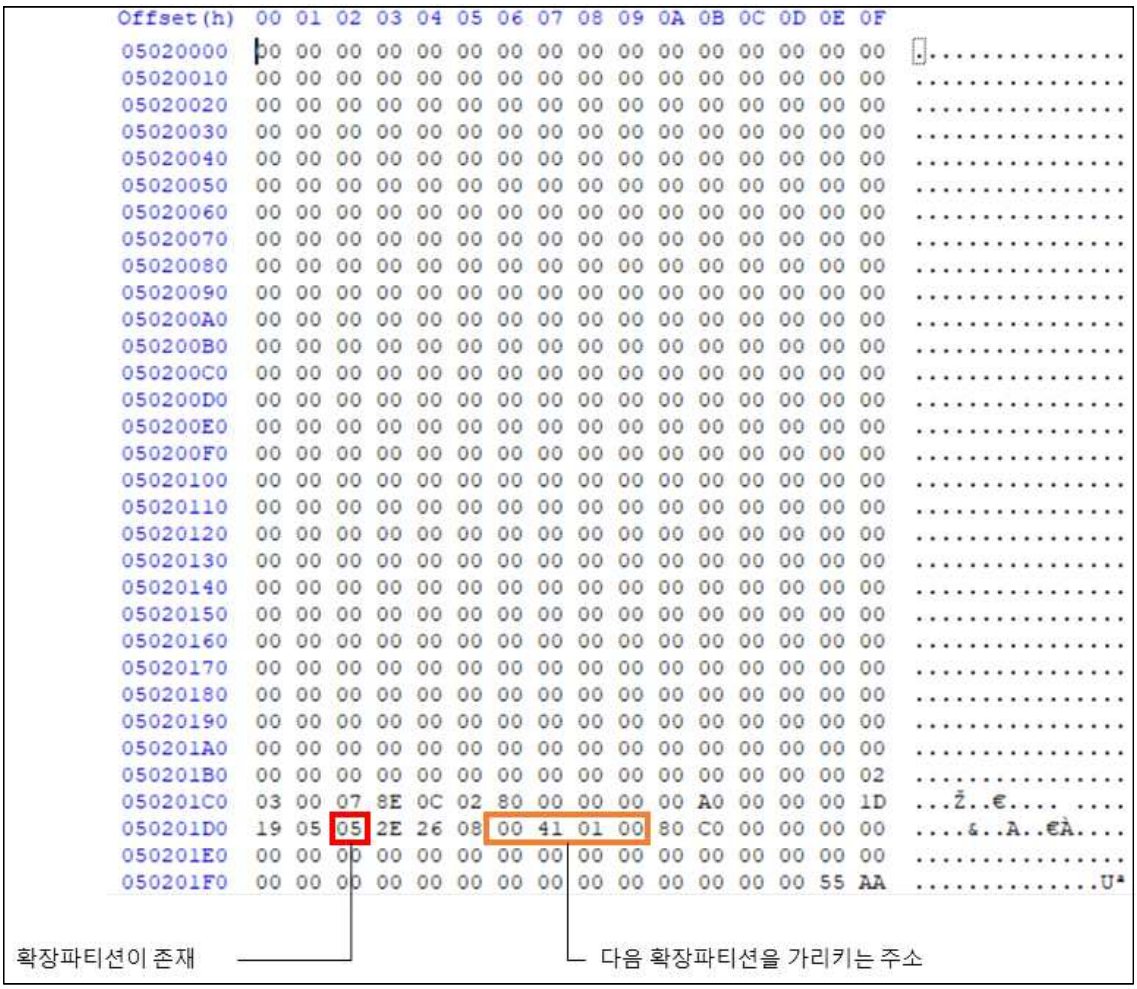
[123008 sector]



123008섹터의 위치로 가면 첫 번째 테이블 엔트리에는 파티션타입이 [0x07]로 NTFS파일임을 확인할 수 있다. 그리는 A000으로 섹터의 크기(512bytes)를 곱해주면 20971520(bytes)로 대략 20Mb의 파티션 크기임을 확인할 수 있다. 다음 엔트리에는 5번째 확장파티션의 존재여부와 주소를 확인할 수 있다. 여기서 혼동하면 안되는 점은 0섹터에 있는 4번째 파티션의 위치를 가리키는 섹터 값에 다음 확장파티션 주소를 합해서 다음 EBR의 주소로 접근할 수 있다.

123008 + 41088(0xA080) = 164096

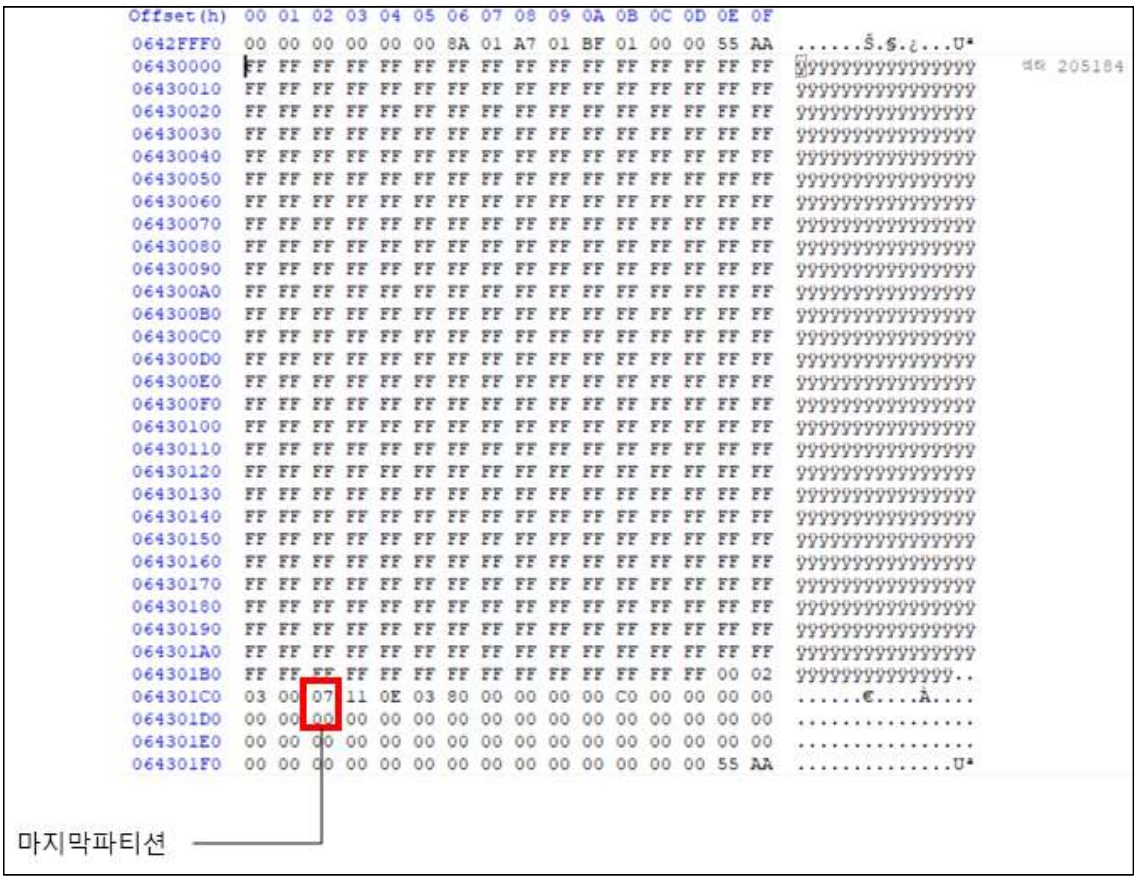
[164096 sector]



6번째 섹터의 정보는 [0x07] 타입이므로 NTFS이며 20MB의 크기를 가진다.

다음 섹터의 위치는 123008 + 82176(0x14100) = 205184

[205184 sector]



7번째 파티션의 크기는 C000*200h = 25165824(0x1800000) = 약 25Mb

3. 결론

전체 파티션의 정보를 정리한 결과이다.

	부팅	타입	주소	크기
1	00(불가)	NTFS	128(80)	20MB
2	00(불가)	NTFS	41088(A080)	20MB
3	00(불가)	NTFS	82048(14080)	20MB
5	00(불가)	NTFS	123008(1E080)	20MB
6	00(불가)	NTFS	164096(28100)	20MB
7	00(불가)	NTFS	205184(32180)	24MB

FTK Imager로 확인한 값과 비슷하다