

Table of Contents



- 1 FAT 기본 정보
- 파일시스템 분석 이론
- 3 FAT 구조 분석 및 실습

Objectives



- ✓ FAT의 일반적인 정보에 대해 이해한다.
- ✓ FAT의 구조에 대해 이해한다.
- ✓ FAT 이미지를 Hex 뷰어를 이용하여 분석한다.





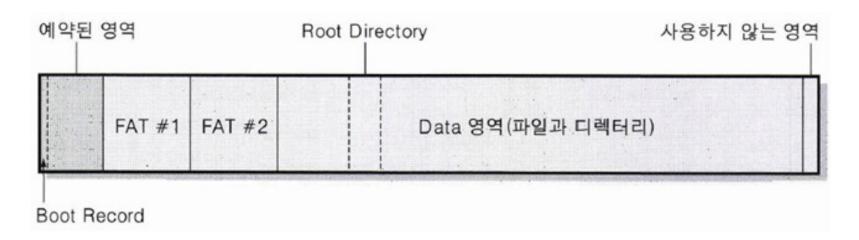
FAT

■ File Allocation Table



FAT

- File Allocation Table
- 구조가 간단하다는 장점





FAT

- File Allocation Table
- 구조가 간단하다는 장점
- 일반 시스템 외에도 이동식 저장장치에서 많이 사용







FAT

- File Allocation Table
- 구조가 간단하다는 장점
- 일반 시스템 외에도 이동식 저장장치에서 많이 사용
- FAT12, FAT16, FAT32, exFAT 등

Attribute	FAT12	FAT16	FAT32
Used For	Floppies; small hard drives	Small to large hard drives	Large to very large hard drives
Size of Each FAT Entry	12 bits	16 bits	28 bits
Maximum Number of Clusters	~4,096	~65,536	~268,435,456
Supported Cluster Sizes	512 B to 4 KB	2 KB to 32 KB	4 KB to 32 KB
Maximum Volume Size	16,736,256 B (16 MB)	2,147,123,200 B (2 GB)	~2 ⁴¹ B (2 TB)



파일시스템 분석 개론



파일시스템

■ 정의

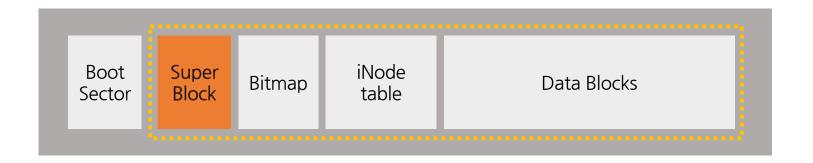
The <u>structure and logic rules</u> used to manage the groups of information
 and their names

- Wikipedia

■ 종류

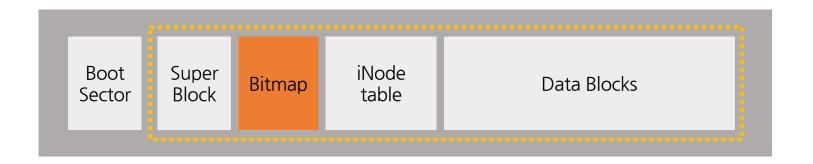
- Ext 2 / 3 / 4, NTFS
- FAT 12 / 16 / 32, exFAT (or FAT 64)
- EFS2, TFS5, YAFFS
- F2FS, APFS, VDFS





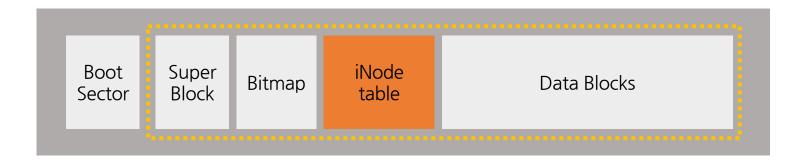
- 수퍼 블록
 - 파일 시스템의 가장 기본이 되는 정보 저장
 - 전체 크기, 블록 크기, 루트 아이노드 번호, 저널 번호





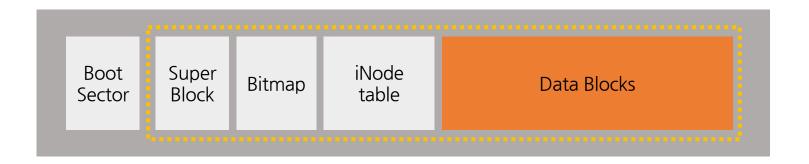
- 비트맵
 - 데이터 영역의 각 블록의 사용 여부를 비트로 표현한 자료구조





- 아이노드
 - 파일 / 디렉토리의 메타 데이터(시각, 크기, 속성, 이름 등)
 - 데이터 혹은 데이터가 저장되어 있는 위치





- 데이터 영역
 - 실제 데이터가 존재하는 영역
 (아이노드, 비트맵, 수퍼블록을 제외한 전체 데이터)

파일시스템 분석 개론



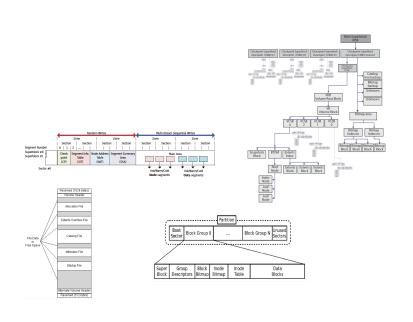
파일시스템 복원

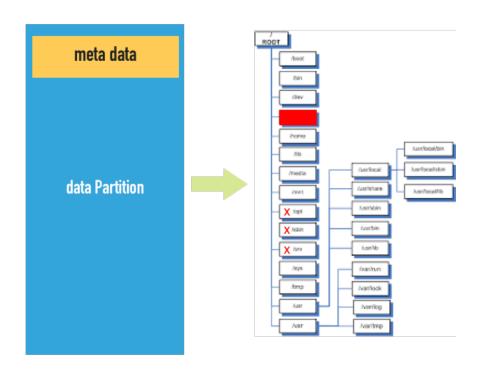
- 파일시스템 복원
 - 획득 이미지에서 활성과 삭제 영역을 식별
 - 파일시스템 복호화(iPhone physical)



파일시스템 복원

■ 파일시스템 복원

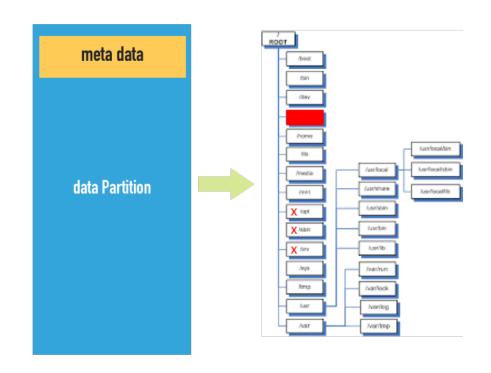






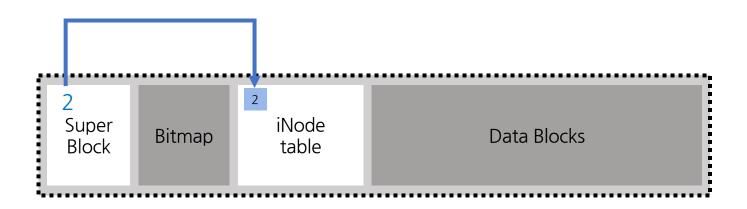
파일시스템 복원

- 파일시스템 복원
 - 디렉토리와 파일
 - 심볼릭 링크 / 하드 링크
 - 비할당 영역
 - 복원된 디렉토리 엔트리



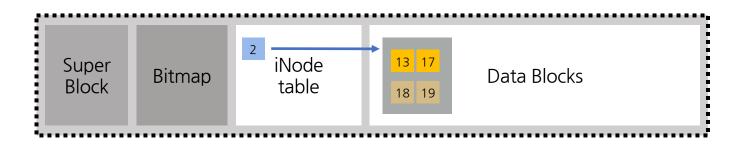


■ 루트 아이노드 읽기





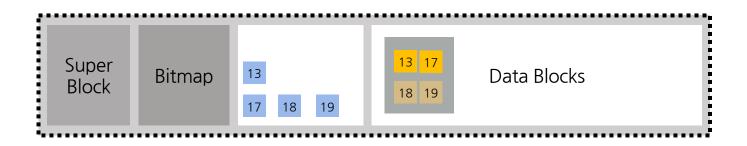
■ 루트 아이노드 데이터 읽기



파일 노드



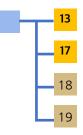
■ 각 디렉토리 엔트리에서 아이노드 식별

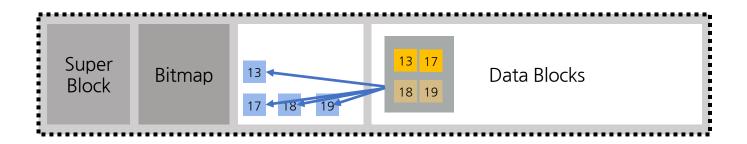


파일 노드



■ 각 디렉토리 엔트리에서 식별한 아이노드 읽기



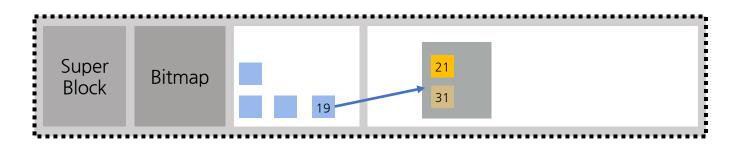


파일 노드



■ 자식 아이노드 데이터 읽기

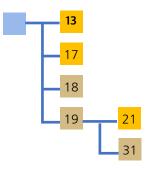


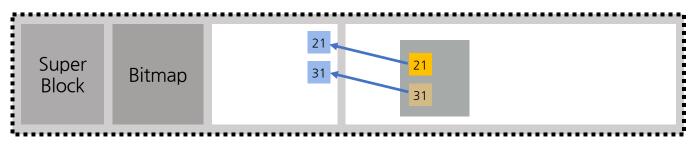


파일 노드



■ 자식 아이노드 읽기

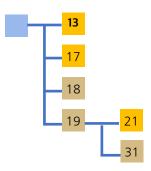


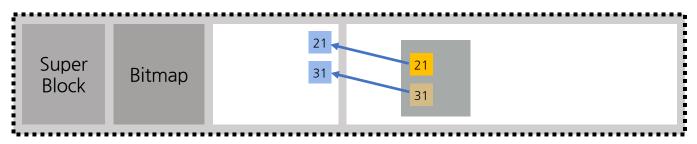


파일 노드



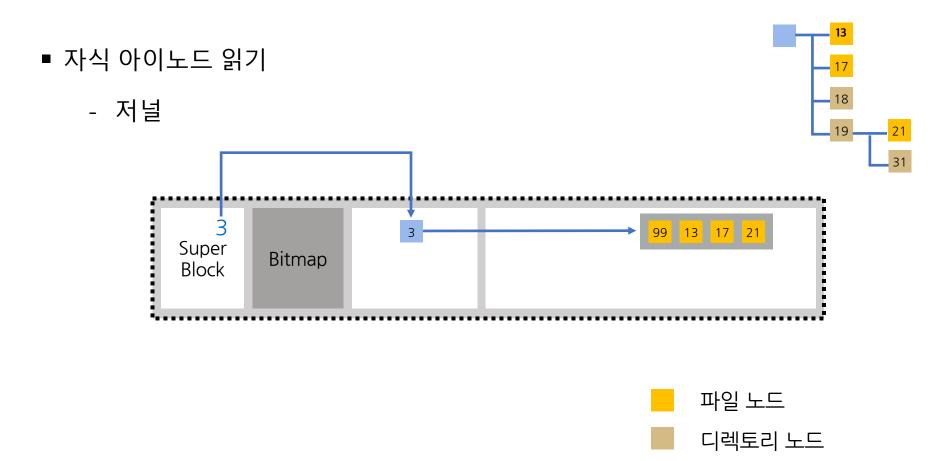
- 자식 아이노드 읽기
 - 반복



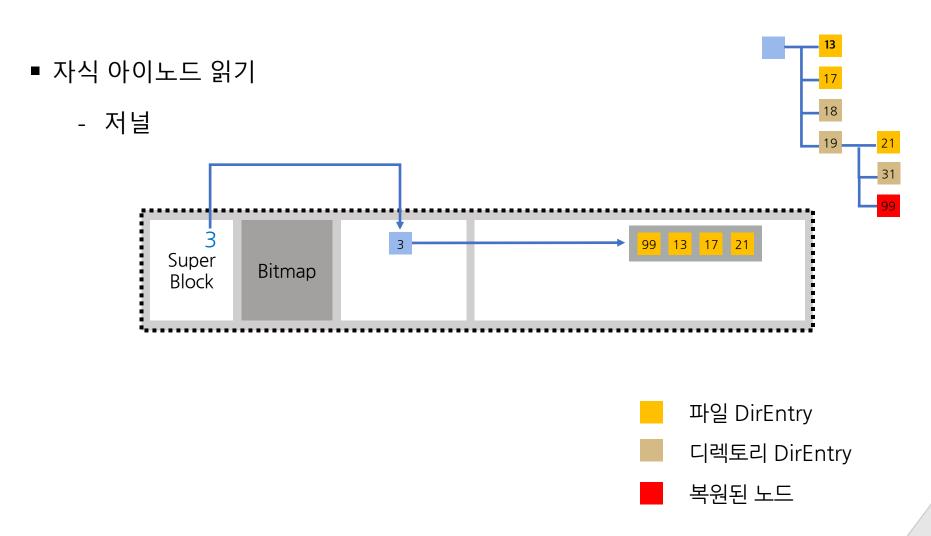


파일 노드



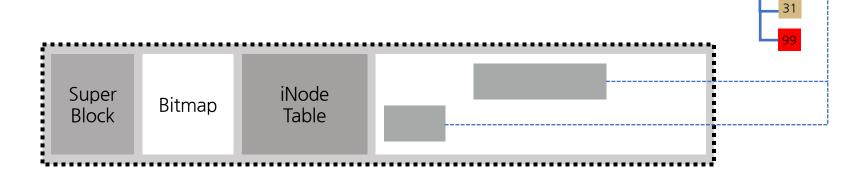








- 비할당 영역 계산
 - 두 가지 방법



파일 노드

디렉토리 노드

복원된 노드

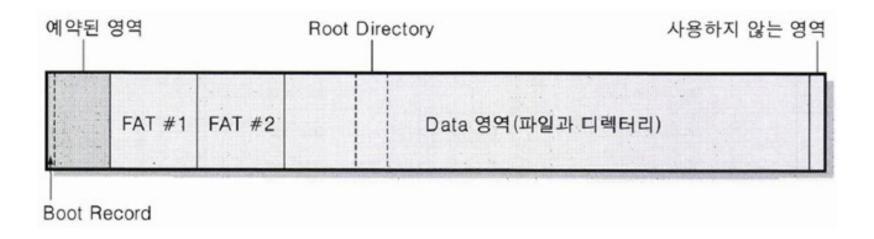
비할당 영역 노드





파일시스템 레이아웃

■ 레이아웃





부트 레코드

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
Jump Boot Code OEM Name											s Per tor	Sec P Clust	Reserved Sector Count			
Num of FAT									r per ick	Numb He		Hidden Sector				
	Total Sector 32 FAT Size 32 Ext Flags									File System Version			Root Directory Cluster			
File S) Int	ystem fo	Boot R Backup							Rese	rved						
Drive Num ber	Rese rved 1	Boot Sign ature		Volume ID Volume Label												
Volume Label File System Type																



부트 레코드

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00													s Per tor	S.Per C.		vd ount
0x10	#FAT															
0x20					#sector of FAT Area								F	Root Dir	r Cluste	er
0x30																
0x40																
0x50																·



부트 레코드

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00													s Per tor	S.Per C.	Rs S. Co	vd ount
0x10	#FAT															
0x20	#sector of FAT A												F	Root Dir	Cluste	er
0x30																
0x40																
0x50																



부트 레코드

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00												_	s Per ctor	S.Per C.	Rs S. Co	
0x10	#FAT															
0x20					#se	ector of	f FAT A	rea					F	Root Dir	Cluste	er
0x30																
0x40																
0x50																



부트 레코드

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00												_	s Per ctor	S.Per C.	Rs S. Co	
0x10	#FAT															
0x20					#se	ector of	f FAT A	rea					F	Root Dir	Cluste	er
0x30																
0x40																
0x50																

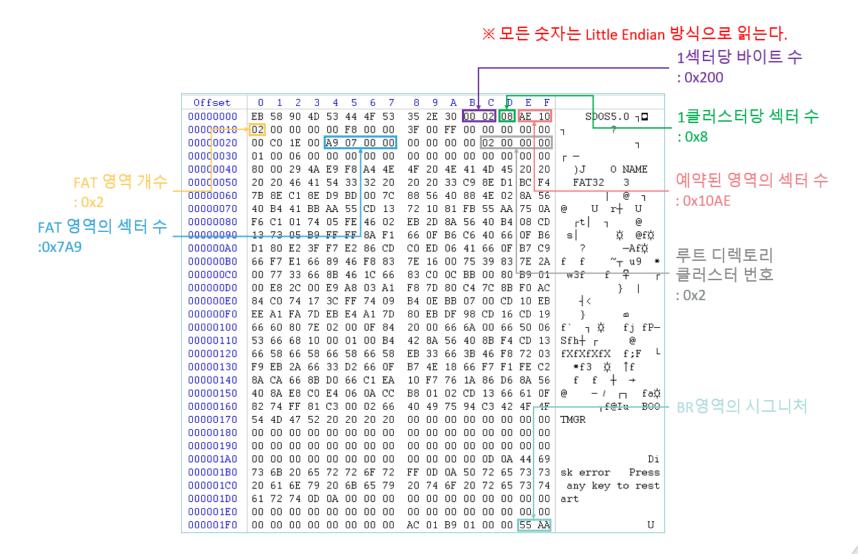


부트 레코드

	00	01	02	03	04	05	06	07	08	09	10	-11	12	13	14	15
0x00													s Per ctor	S.Per C.		vd ount
0x10	#FAT															
0x20					#se	ector of	f FAT A	rea					F	Root Dir	r Cluste	er
0x30																
0x40																
0x50																-



Boot Record 해석





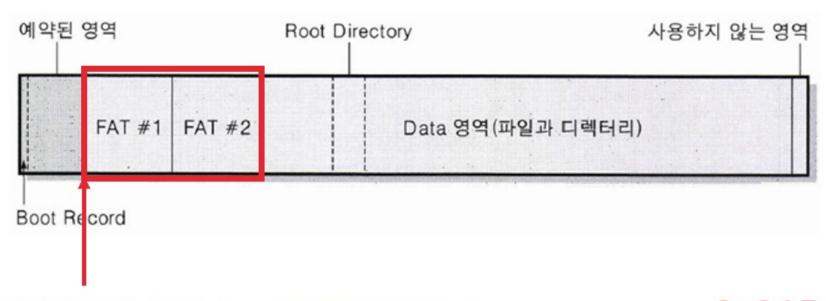
디렉토리 엔트리

Directory Entry

0x0 0x1	0x2 0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
	Na	ime				Е	xtensio	n	Attr	Rese	erved		ntion me
Created Date	Last Access Date	Starti Clust Hig	ter	Wri	ist tten ne	Wri	st tten ite	Star Cluste	ting r Low		File	Size	



FAT 영역 찾아가기



예약된 영역의 섹터 수 X 1섹터당 바이트 수 = 0x10AE X 0x200 = 0x215c00

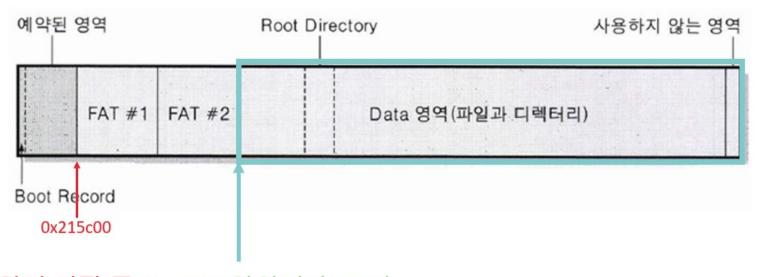


FAT 영역 찾아가기

```
Offset
           0
                     3
                        4
                           5
                              6
                                        9
                                              В
                                                  С
00215C00
          🖪8 FF FF OF FF FF FF
                                    FF FF FF OF FF FF OF
00215C10
          FF FF FF OF
                      FF FF FF OF
                                    FF FF FF
                                                08
                                                                          00215C20
          09 00 00 00 0A 00 00 00
                                    OB 00
                                          00
                                                OC 00
                                             00
00215C30
          OD 00 00 00 OE 00 00 00
                                    OF 00 00 00 10 00 00 00
00215C40
          11 00 00 00 12 00 00 00
                                    13 00 00 00 14 00 00
00215C50
          15 00 00 00 16 00 00 00
                                    17 00 00 00 18 00
00215060
          19 00 00 00 1A 00 00 00
                                    1B 00 00 00 1C 00 00 00
00215C70
          1D 00 00 00 1E 00 00 00
                                    1F 00 00 00 20 00 00 00
                                    23 00 00 00 24 00
00215C80
          21 00 00 00 22 00 00 00
00215090
                                    27 00 00 00 28 00 00
          25 00 00 00 26 00 00 00
                                                          00
00215CA0
          29 00 00 00 2A 00 00 00
                                    2B 00 00 00 2C 00 00 00
00215CB0
          2D 00 00 00 2E 00 00 00
                                    2F 00 00 00 30 00
00215CC0
          31 00 00 00 32 00 00 00
                                    33 00 00 00 34 00 00 00
00215CD0
          35 00 00 00 36 00 00 00
                                    37 00 00 00 38 00 00
00215CE0
          39 00 00 00 3A 00 00 00
                                    3B 00 00 00 3C 00
00215CF0
          3D 00 00 00 3E 00 00 00
                                    3F 00 00 00 40 00
00215D00
          41 00 00 00 42 00 00 00
                                    43 00 00 00 44 00 00
00215D10
          45 00 00 00 46 00 00 00
                                    47 00 00
                                             00 48 00
                                                                          Η
00215D20
                                                                          L
          49 00 00 00 4A 00 00 00
                                    4B 00 00 00 4C 00
00215D30
          4D 00 00 00 4E 00 00 00
                                    4F 00 00 00 50 00
00215D40
          51 00 00 00 52 00 00 00
                                    53 00 00 00 54 00 00 00
                                                                          Τ
00215D50
          55 00 00 00 56 00 00 00
                                    57 00 00 00 58 00
                                                                          Χ
00215D60
          59 00 00 00 5A 00 00 00
                                    5B 00 00
                                             00 5C 00
00215D70
          5D 00 00 00 5E 00 00 00
                                    5F 00 00 00 60 00 00 00
00215D80
          61 00 00 00 62 00 00 00
                                    63 00 00 00 64 00
                                                                          d
                                                                      С
00215D90
          65 00 00 00 66 00 00 00
                                    67 00 00 00 68 00
00215DA0
          69 00 00 00 6A 00 00 00
                                    6B 00 00 00 6C 00 00 00
                                                                          1
00215DB0
          6D 00 00 00 6E 00 00 00
                                    6F 00 00 00 70 00 00
                                                                  n
                                                                      О
00215DC0
          71 00 00 00 72 00 00 00
                                    73 00 00 00 74 00
00215DD0
          75 00 00 00 76 00 00 00
                                    77 00 00 00 78 00 00 00
                                                                  V
                                                                          Х
00215DE0
          79 00 00 00 7A 00 00 00
                                    7B 00 00 00 7C 00 00
                                                                  Z
00215DF0
          7D 00 00 00 7E 00 00 00
                                    7F 00
                                          00
                                             00
00215E00
          81 00 00 00 82 00 00 00
                                    83 00 00
                                             00 84 00
00215F10
          85 00 00 00 86 00 00 00
                                    87 00 00 00 88 00 00 00
```



DATA 영역 찾아가기



FAT 영역의 시작 주소 + FAT 영역의 총 크기

= FAT 영역의 시작 주소 + (FAT 영역 개수 X FAT 영역의 섹터 수 X 1섹터당 바이트 수)

= 0x215c00 + (0x2 X 0x7A9 X 0x200) = 0x400000



DATA 영역 찾아가기

```
Offset
00400000
                                                          TEST
                                                                     00400010
                                  A3 4C 00 00 00 00 00 00
          00 00 00 00 00 00 B4 71
00400020
          42 20 00 49 00 6E 00 66
                                  00 6F 00 0F 00 72 72 00
00400030
          6D 00 61 00 74 00 69 00
                                  6F 00 00 00 6E 00 00 00
          01 53 00 79 00 73 00 74
00400040
                                  00 65 00 OF 00 72 6D 00
00400050
          20 00 56 00 6F 00 6C 00
                                  75 00 00 00 6D 00 65 00
                                                            Volu
                                                                      m e
00400060
          53 59 53 54 45 4D 7E 31
                                  20 20 20 16 00 09 B3 71
                                                          SYSTEM~1
                                                                     Т
00400070
          A3 4C A3 4C 00 00 B4 71
                                  A3 4C 03 00 00 00 00 00
00400080
          44 49 52 31 20 20 20 20
                                  20 20 20 10 08 7F C9 71
                                                          DIR1
                                                                     +01
00400090
          A3 4C A3 4C 00 00 91 71
                                  A3 4C 06
                                          00 00 00 00 00
          E5 49 47 45 52 20 20 20
                                  4A 50 47 20 18 5B F0 71
004000A0
                                                            GER
                                                                  JPG ↑[
         A3 4C A3 4C 00 00 EA 71
004000B0
                                  A3 4C 02 01 22 C5 01 00
                                                                    л г"
004000C0
          00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00 00
004000D0
          00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00
004000E0
          00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00
         nn nn nn nn nn nn nn
                                  004000F0
```

- FAT에서 클러스터의 시작 번호는 2번
- Root directory가 2번 클러스터였으므로 Data 영역의 가장 앞에 존재



Root directory entry 분석

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0:	9	0xA	0xB	0xC	0xD	0xE	0xF
0xE5				Name				E	xtei	ısio	n	Attr	Rese	rved	Crea tir	
Crea Da	ated ate		Access		ting ster gh	Writ	ist tten me	Writ	st tten ite			ting er Low		File	Size	

	Attribute
0x02	Hidden
80x0	Volume Label
0x10	Directory
0x0F	LFN

												П							
Offset	0	1	2	3	4	5	6	- 7	8	9	Α	В	C	D	Ε	F			
00400000	54	45	53	54	20	20	20	20	20	20	20	08	00	00	00	00	TEST		
00400010	00	00	00	00	00	00	В4	71	АЗ	4C	00	00	00	00	00	00			
00400020	42	20	00	49	00	6E	00	66	00	6F	00	OF	00	72	72	00	B I n	fо	¤ rr
00400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	mati	iο	n
00400040	01	53	00	79	00	73	00	74	00	65	00	OF	00	72	6D	00	гЅуѕ	t e	🌣 rm
00400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	V o 1	l u	m e
00400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	09	ВЗ	71	SYSTEM	~1	Т
00400070	АЗ	4C	ΑЗ	4C	00	00	В4	71	АЗ	4C	03	00	00	00	00	00			L
00400080	44	49	52	31	20	20	20	20	20	20	20	10	08	7F	С9	71	DIR1		 □।
00400090	АЗ	4C	ΑЗ	4C	00	00	91	71	АЗ	4C	06	00	00	00	00	00			-
004000A0	E5	49	47	45	52	20	20	20	4A	50	47	20	18	5B	FΟ	71	GER	JP	
004000B0	А3	4C	АЗ	4C	00	00	EΑ	71	АЗ	4C	02	01	22	С5	01	00			ור"
004000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
004000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
004000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
NN4NNNFN	nn	ΠN	ΠN	ΠN	ΠN	ΠN	ΠN	ΠN	ΠN	ΠN									



Root directory entry 분석

OxE5 Name Extension Attr Reserved Creat tim Created Last Access Clast Written Starting Start	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
Created Last Access	0xE5				Name				E	xtensio	n	Attr	Rese	erved		
Created Last Access Charter Waiter Starting File Circ					Star	ting	La	ast	La	ist						
Date Date Cluster Written Written Date File Size														File	Size	

	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN

Offset	0	1	2	3	4	- 5	-6	7	8	9	Α	В	C	D	E	F			
00400000	5 4	45	53	54	20	20	20	20	20	20	20	08	00	00	00	00	TEST		
00400010	00	00	00	00	00	00	В4	71	АЗ	4C	00	0	00	00	00	00			
00400020	42	20	00	49	00	6E	00	66	00	6F	00	OF	00	72	72	00	B I n	fо	¢ rr
00400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	m a t i	О	n
00400040	01	53	00	79	00	73	00	74	00	65	00	OF	00	72	6D	00	гЅуз	t e	₿ rm
00400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	V o 1	u	m e
00400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	09	ВЗ	71	SYSTEM~	1	Т
00400070	АЗ	4C	ΑЗ	4C	00	00	В4	71	АЗ	4C	03	00	00	00	00	00		l	-
00400080	44	49	52	31	20	20	20	20	20	20	20	10	08	7F	С9	71	DIR1		∔□ ।
00400090	АЗ	4C	ΑЗ	4C	00	00	91	71	АЗ	4C	06	00	00	00	00	00		-	-
004000A0	E5	49	47	45	52	20	20	20	4A	50	47	20	18	5B	F0	71	GER	JPG	} ↑[
004000B0	АЗ	4C	АЗ	4C	00	00	EΑ	71	АЗ	4C	02	01	22	C5	01	00		٦	Γ"
004000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
004000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			



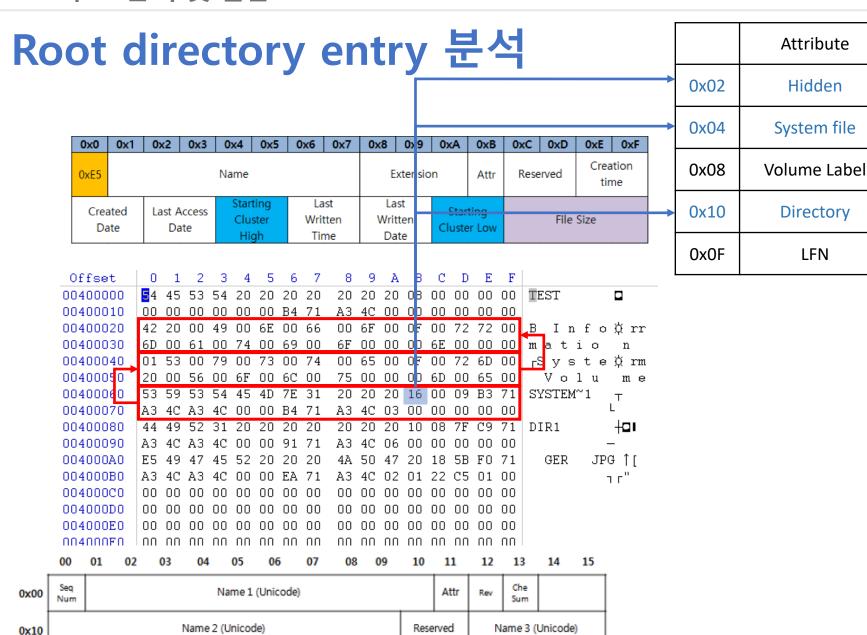
Root directory entry 분석

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0xE5				Name				E	xtensio	n	Attr	Rese	erved		ntion ne
C		1 /		Star	ting	La	ist	La	st						
	ated ate	l	Access ate		ster		tten		tten		ting er Low		File	Size	
				Hi	gh	Lir	me	Da	te						

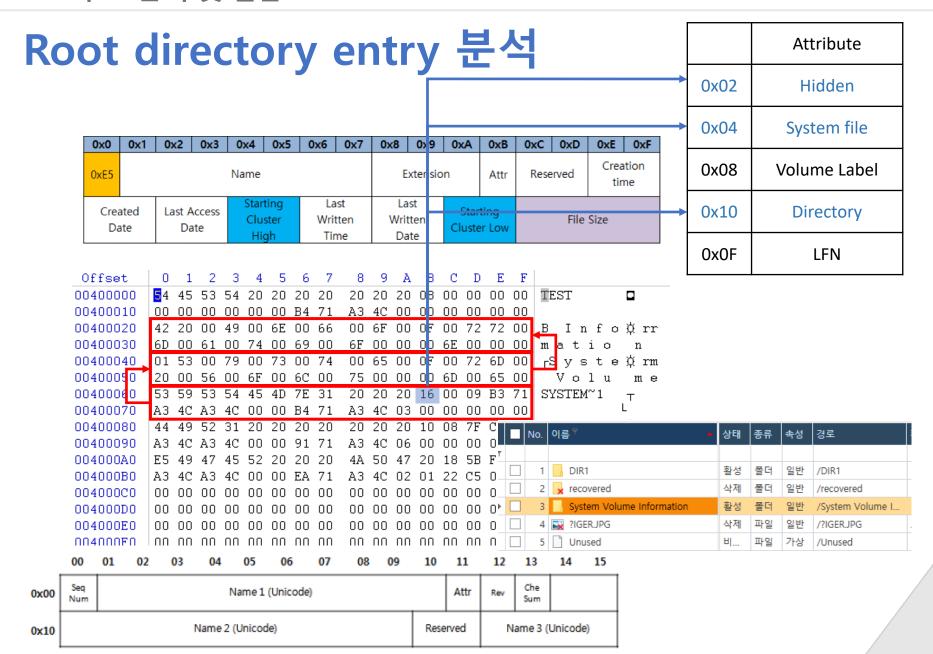
	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN

Offset	0	1	2	3	4	- 5	6	7	8	9	Α	В	C	D	E	F				
00400000	54	45	53	54	20	20	20	20	20	20	20	08	00	00	00	00	TEST			
00400010	00	00	00	00	00	00	В4	71	АЗ	4C	00	00	00	00	00	00				
00400020	42	20	00	49	00	6E	00	66	00	6F	00	0F	00	72	72	00	B In	f o	prr	
00400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	m a ti	. 0	n	
00400040	01	53	00	79	00	73	00	74	00	65	00	OF	00	72	6D	00	гS уз	t e	🌣 rm	
00400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	Vol	u	m e	
00400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	09	ВЗ	71	SYSTEM^	1	Т	
00400070	АЗ	4C	АЗ	4C	00	00	В4	71	АЗ	4C	03	00	00	00	00	00			L	
00400080	44	49	52	31	20	20	20	20	20	20	20	10	08	7F	С9	71	DIR1		 	
00400090	АЗ	4C	АЗ	4C	00	00	91	71	АЗ	4C	06	00	00	00	00	00		-	_	
004000A0	E5	49	47	45	52	20	20	20	4A	50	47	20	18	5B	F0	71	GER	JP(3 ↑[
004000B0	АЗ	4C	АЗ	4C	00	00	EΑ	71	АЗ	4C	02	01	22	C5	01	00		-	ı r"	
004000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
004000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
004000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				











Root directory entry 분석

OxE5 Name Exter sion Attr Reserved Creation time Created Date Date Name Exter sion Attr Reserved Creation time Creation time Starting Cluster Written Date Cluster High Time Date Cluster Low File Size	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0x	Α	0xB	0xC	0xD	0xE	0xF
Created Last Access Date Date Cluster Written Written Starting Cluster Low File Size	0xE5				Name				E	xtersi	on		Attr	Rese	erved		
Title Bate					Clu	ster	Wri	tten	Writ	tten					File	Size	

	Date		Dat	te		Litte			T:-		'	D-4		CI	uster	Low		1110	5120
						Hig	jn		Tin	ne		Date	e						
	Offset	- 0	1	2	3	4	- 5	- 6	7	8	9	A	В	C	D	E	F		
0	0400000	5 4	45	53	54	20	20	20	20	20	20	20	03	00	00	00	00	TEST	
0	0400010	00	00	00	00	00	00	В4	71	АЗ	4C	00	00	00	00	00	00		
0	0400020	42	20	00	49	00	6E	00	66	00	6F	00	07	00	72	72	00	B I n	fo¤rr
0	0400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	mat	io n
0	0400040	01	53	00	79	00	73	00	74	00	65	00	07	00	72	6D	00	гЅуз	te¤rm
0	0400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	Vο	lu me
0	0400060	53	59	53	54	45	4D	7E	31	20	20	20	15	00	09	ВЗ	71	SYSTEM	~1 _T
0	0400070	АЗ	4C	АЗ	4C	00	00	В4	71	АЗ	4C	03	00	00	00	00	00		L
0	0400080	44	49	52	31	20	20	20	20	20	20	20	10	08	7F	С9	71	DIR1	+□•
0	0400090	ΑЗ	4C	АЗ	4C	00	00	91	71	АЗ	4C	06	00	00	00	00	00		_
0	04000A0	E5	49	47	45	52	20	20	20	4A	50	47	20	18	5B	FΟ	71	GER	JPG ↑[
0	04000B0	АЗ	4C	АЗ	4C	00	00	EΑ	71	АЗ	4C	02	01	22	C5	01	00		ר"
0	04000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
0	04000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
0	04000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		

NOTATION OF THE OWNER O

	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN



Root directory entry 분석

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
														Cros	tion
0xE5				Name				E	xter sid	on	Attr	Rese	erved	tir	ne
Cre	ated	lact /	Access	Star	ting	La	ist	La	st	Star	ting				
	ate		ate	Clu	ster	Wri	tten	Wri	tten		er Low		File	Size	
	ate	D 6	ate	Hi	gh	Tir	me	Da	te	Cluste	er Low				
				- 111	911	- "	110								

	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN

Offset	0	1	2	3	4	5	- 6	7	8	9	A	В	C	D	Ε	F						
00400000	54	45	53	54	20	20	20	20	20	20	20	08	00	00	00	00	TEST					
00400010	00	00	00	00	00	00	В4	71	АЗ	4C	00	00	00	00	00	00						
00400020	42	20	00	49	00	6E	00	66	00	6F	00	0.7	00	72	72	00	В І	n f	ο¤	rr		
00400030	6D	00	61	00	74	00	69	00	6F	00	00	0	6E	00	00	00	m a	ti	o n			
00400040	01	53	00	79	00	73	00	74	00	65	00	0.7	00	72	6D	00	гSу	rs t	е≬	rm		
00400050	20	00	56	00	6F	00	6C	00	75	00	00	0	6D	00	65	00	V	0 1	ı m	ı e		
00400060	53	59	53	54	45	4D	7E	31	20	20	20	15	00	09	ВЗ	71	SYST	EM~1	Т			
00400070	АЗ	4C	ΑЗ	4C	00	00	В4	71	А3	4C	03	00	00	00	00	00			L			
00400080	44	49	52	31	20	20	20	20	20	20	20	10	08	7F	С9	71	DIR1	L	+0	I		
00400090	АЗ	4C	ΑЗ	4C	00	00	91	71	А3	4C	06	00	00	00	00	00			_			
004000A0	E5	49	47	45	52	20	20	20	4A	50	47	20	18	5B	FΟ	71	GE	ER (JPG ↑	[
004000B0	АЗ	4C	АЗ	4C	00	00	EΑ	7:	No	0	르						_	상태	종류	속성	경로	확장지
004000C0	00	00	00	00	00	00	00	0(140									01	оπ	70	8-	700
004000D0	00	00	00	00	00	00	00	0(
004000E0	00	00	00	00	00			0([1	DII	R1						활성	폴더	일반	/DIR1	
NN4NNNFN	nn	ΠΠ	ΠΠ	ΠΠ	ΠΠ	ΠΠ	ΠΠ	Ut [2	rec	cove	red					삭제	폴더	일반	/recovered	
								[3	Sy	stem	Volu	me li	nforn	natior	n	활성	폴더	일반	/System Volume I	
								[4	?10	SER.J	PG					삭제	파일	일반	/?IGERJPG	JPG
								[5] Un	usec	i					비	파일	가상	/Unused	



Root directory entry 분석

00 00 00 00 00 00 00

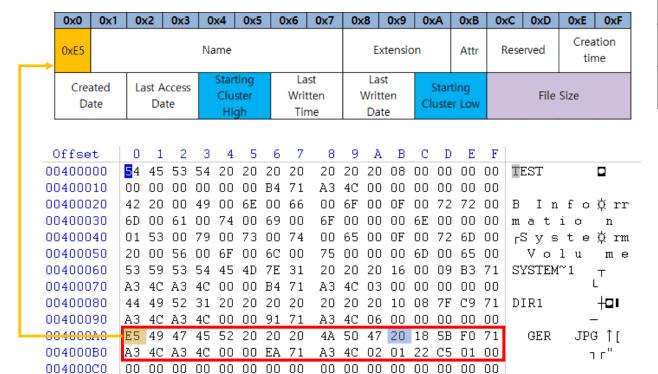
00 00 00 00 00 00 00 00

"삭제 파일"

004000D0

004000E0

004000F0



00 00 00 00 00

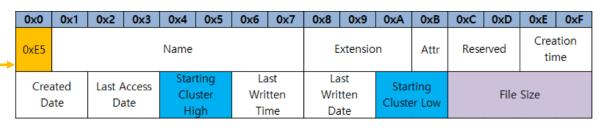
00 00 00 00 00 00 00 00

	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN



Root directory entry 분석

"삭제 파일"



	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN

Offset	0	1	2	3	4	- 5	- 6	7	8	9	A	В	C	D	E	F					
00400000	54	45	53	54	20	20	20	20	20	20	20	08	00	00	00	00	TES	ST			
00400010	00	00	00	00	00	00	В4	71	АЗ	4C	00	00	00	00	00	00					
00400020	42	20	00	49	00	6E	00	66	00	6F	00	OF	00	72	72	00	В	I n	f o	¤ rr	
00400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	m a	a t i	io	n	
00400040	01	53	00	79	00	73	00	74	00	65	00	OF	00	72	6D	00	гS	уѕ	t e	₿ rm	l
00400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	1	/ o]	l u	m e	!
00400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	09	ВЗ	71	SYS	STEM^	1	Т	
00400070	АЗ	4C	АЗ	4C	00	00	В4	71	АЗ	4C	03	00	00	00	00	00			L	-	
00400080	44	49	52	31	20	20	20	20	20	20	20	10	08	7F	С9	71	DIE	₹1		∔ □।	
00400090	АЗ	4C	АЗ	4C	00	00	91	71	АЗ	4C	06	00	00	00	00	00			-	-	
004000A0	E5	49	47	45	52	20	20	20	4A	50	47	20	18	5B	FΟ	71		3ER	JPG	;	
004000B0	ΑЗ	4C	АЗ	4C	00	00	EΑ	71	АЗ	4C	02	01	22	C5	01	00			٦	Γ"	
004000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
004000D0	00	00	00	00	00	00	00	0	No	. OJ.							_	상태	종류	속성	경
004000F0	nn	nn	nn	nn	nπ	nn	nn			Τ.	_							-"			_

004000C0	00 00	00 (00	00	00	00	00	(00 (00 00 00 00 00 00					
004000D0	00 00	00 (00	00	00	00	0	П	No.	이름	상태	종류	속성	경로	확장자
004000E0	00 00	00 (00	00	00	00	0,				- "			_	
004000F0	nn nn	00.1	nn	nπ	nn	nn	\cap								
									1	☐ DIR1	활성	폴더	일반	/DIR1	
									2	x recovered	삭제	폴더	일반	/recovered	
									3	System Volume Information	활성	폴더	일반	/System Volume I	
									4	🙀 ?IGERJPG	삭제	파일	일반	/?IGERJPG	JPG
									5	Unused	비	파일	가상	/Unused	



Dir1 분석

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0xE5				Name				E	xtensio	n	Attr	Rese	erved	Crea tin	
	ated ate		Access		ting ster gh	Wri	ist tten me	Writ	st tten ite		ting er Low		File	Size	

	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN

Offset	0	1	2	3	4	- 5	- 6	7	8	9	A	В	C	D	E	F		
00400000	54	45	53	54	20	20	20	20	20	20	20	08	00	00	00	00	TEST	
00400010	00	00	00	00	00	00	В4	71	АЗ	4C	00	00	00	00	00	00		
00400020	42	20	00	49	00	6E	00	66	00	6F	00	OF	00	72	72	00	B I n	fo¤rr
00400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	mat:	io n
00400040	01	53	00	79	00	73	00	74	00	65	00	OF	00	72	6D	00	гЅуз	te¤rm
00400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	V o S	lu me
00400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	09	ВЗ	71	SYSTEM'	~1 _T
00400070	АЗ	4C	ΑЗ	4C	00	00	В4	71	АЗ	4C	03	00	00	00	00	00		L
00400080	44	49	52	31	20	20	20	20	20	20	20	10	08	7F	С9	71	DIR1	+01
00400090	ΑЗ	4C	ΑЗ	4C	00	00	91	71	АЗ	4C	06	00	00	00	00	00		_
004000A0	E5	49	47	45	52	80	20	20	4A	50	47	20	18	5B	FO	71	GER	JPG ↑[
004000B0	АЗ	4C	АЗ	4C	00	00	EΑ	71	АЗ	4C	D 2	01	22	С5	01	00		ר"
004000C0	00	00	00	00	00	00	00	00	00	00/	00	00	00	00	00	00		
004000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
004000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
NN4NNNFN	nn	ΠN	ΠN	ΠN	ΠN	ΠN	ΠN	ΠN	nn	ΠN	ΠN	ΠN	ΠN	ΠN	ΠN	ΠN		

0x0000006



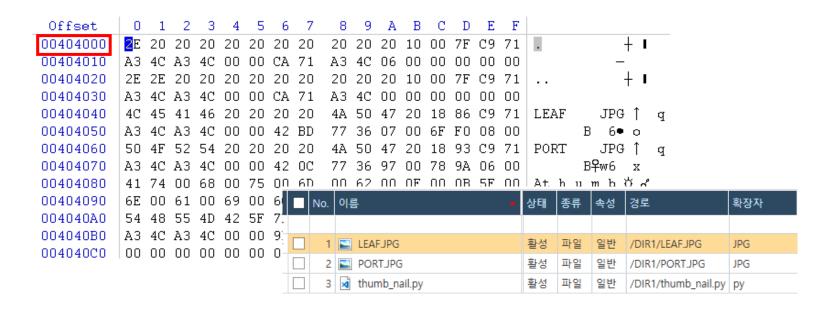
Dir1 분석

0x6 "6번째 클러스터 1개로 이루어진 디렉토리"

```
Offset
                         5 6
         00215C00
00215C10
                              OF
                                     FF FF OF 08 00 00 00
00215C20
          09 00 00 00 0A 00 00 00 0B 00 00 00 0C 68 00 00
          OD 00 00 00 OE 00 00 00
00215C30
                                  OF 00 00 00 10 00 00 00
00215C40
         11 00 00 00 12 00 00 00
                                  13 00 00 00 14 00 00 00
                                                                        OxOFFFFFF
00215C50
         15 00 00 00 16 00 00 00
                                  17 00 00 00 18 00 00 00
                                                                        = 이어지는 클러스터 없음
00215060
         | 19 00 00 00 1A 00 00 00
                                  1B 00 00 00 1C 00 00 00
00215C70
         1D 00 00 00 1E 00 00 00
                                  1F 00 00 00 20 00 00 00
00215080
          21 00 00 00 22 00 00 00
                                  23 00 00 00 24 00 00 00
00215090
          25 00 00 00 26 00 00 00
                                  27 00 00 00 28 00 00 00
00215CA0
          29 00 00 00 2A 00 00 00
                                  2B 00 00 00 2C 00 00 00
00215CB0
          2D 00 00 00 2E 00 00 00
                                  2F 00 00 00 30 00 00 00
00215CC0
          31 00 00 00 32 00 00 00
                                  33 00 00 00 34 00 00 00
00215CD0
          35 00 00 00 36 00 00 00
                                  37 00 00 00 38 00 00 00
00215CE0
          39 00 00 00 3A 00 00 00
                                  3B 00 00 00 3C 00 00 00
00215CF0
          3D 00 00 00 3E 00 00 00
                                  3F 00 00 00 40 00 00 00
00215D00
          41 00 00 00 42 00 00 00
                                  43 00 00 00 44 00 00 00
00215D10
          45 00 00 00 46 00 00 00
                                  47 00 00 00 48 00 00
00215D20
          49 00 00 00 4A 00 00 00
                                  4B 00 00 00 4C 00 00 00
00215D30
          4D 00 00 00 4E 00 00 00
                                  4F 00 00 00 50 00 00 00
00215D40
          51 00 00 00 52 00 00 00
                                  53 00 00 00 54 00 00 00
                                                                       Х
00215D50
          55 00 00 00 56 00 00 00
                                  57 00 00 00 58 00 00 00 U
00215D60
          59 00 00 00 5A 00 00 00
                                  5B 00 00 00 5C 00 00 00
00215D70
          5D 00 00 00 5E 00 00 00
                                  5F 00 00 00 60 00 00 00
00215D80
          61 00 00 00 62 00 00 00
                                  63 00 00 00 64 00 00 00
00215D90
          65 00 00 00 66 00 00 00
                                  67 00 00 00 68 00 00 00
00215DA0
          69 00 00 00 6A 00 00 00
                                  6B 00 00 00 6C 00 00 00
00215DB0
          6D 00 00 00 6E 00 00 00
                                  6F 00 00 00 70 00 00 00
00215DC0
          71 00 00 00 72 00 00 00
                                  73 00 00 00 74 00 00 00
00215DD0
          75 00 00 00 76 00 00 00
                                  77 00 00 00 78 00 00 00
00215DE0
          79 00 00 00 7A 00 00 00
                                  7B 00 00 00 7C 00 00 00 y
00215DF0
          7D 00 00 00 7E 00 00 00
                                  7F 00 00 00 80 00 00 00
          81 00 00 00 82 00 00 00
                                  83 00 00 00 84 00 00 00
00215E00
          85 NO NO NO 86 NO NO NO
                                 87 00 00 00 88 00 00 00
```



Dir1 분석



6번 클러스터의 주소

= DATA 영역의 시작 주소 + (클러스터 번호 – 2) X 클러스터 크기

 $= 0 \times 400000 + (6 - 2) \times 0 \times 1000 = 0 \times 404000$



LEAF.JPG 분석

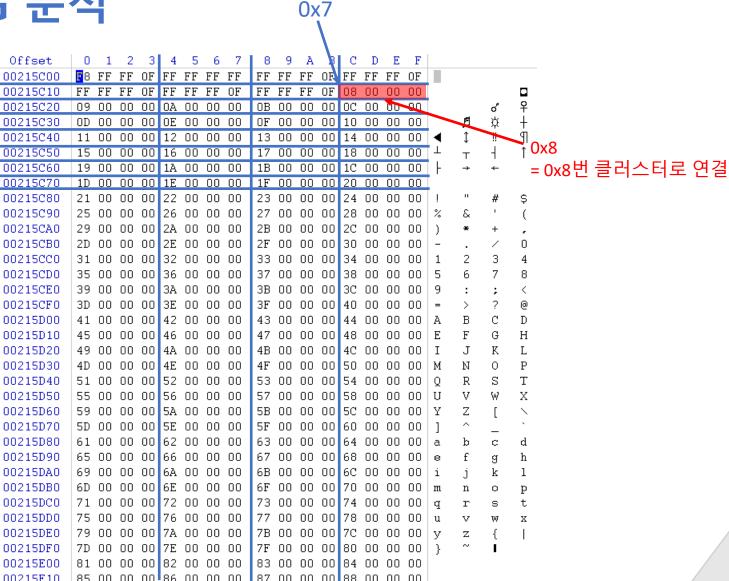
0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0xE5				Name				E	xtensio	n	Attr	Reserved		Creation time	
	ated ate		ccess		ting ster gh	La Wrii Tir		Writ	st tten ite	Star Cluste	ting er Low		File	Size	

	Attribute
0x02	Hidden
0x08	Volume Label
0x0F	LFN
0x10	Directory
0x20	Archive

Offset	- 0	- 1	2	- 3	4	- 5	- 6	7	- 8	- 9	A	В	- 0	_ D	F	F		<u> </u>	
Oliset								- 1							- 15		_		
00404000	2E	20	20	20	20	20	20	20	20	20	20	10	00	7F	С9	71		+ •	
00404010	АЗ	4C	ΑЗ	4C	00	00	CA	71	АЗ	4C	06	00	00	00	00	00		_	
00404020	2E	2E	20	20	20	20	20	20	20	20	20	10	00	7F	C9	71		+ •	
00404030	АЗ	4C	ΑЗ	4C	00	00	CA	71	АЗ	4C	00	00	00	00	00	00			
00404040	4C	45	41	46	20	20	20	20	4A	50	47	20	18	86	С9	71	LEAF J	JPG ↑	q
00404050	ΑЗ	4C	ΑЗ	4C	00	00	42	BD	77	36	07	00	6F	F0	08	00	В	6• o	
00404060	50	4F	52	54	20	20	20	20	4A	50	47	20	18	93	С9	71	PORT J	JPG ↑	q
00404070	АЗ	4C	ΑЗ	4C	00	00	42	0C	77	36	97	00	78	9A	06	00	B₽₩	76 x	
00404080	41	74	00	68	00	75	00	6D	00	62	00	OF	00	OB	5F	00	At h u m	ьфб	_
00404090	6E	00	61	00	69	00	6C	00	2E	00	00	00	70	00	79	00	nail.	. р	У
004040A0	54	48	55	4D	42	5F	7E	31	50	59	20	20	00	Α2	С9	71	THUMB_~1F	PΥ	q
004040B0	АЗ	4C	ΑЗ	4C	00	00	9B	8C	A2	4C	01	01	6C	03	00	00		rrl L	-
004040C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			



LEAF.JPG 분석





LEAF.JPG 분석

0x9

= 0x9번 클러스터로 연결

Offset	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	E	F				
00215C00	F 8	FF	FF	OF	FF	OF	FF	FF	FF	OF										
00215C10	FF	FF	FF	OF	FF	FF	FF	OF	FF	FF	FF	OF	08	00	00	00				
00215C20	09	00	00	00	91	88	80	00	UB	UU	00	00	0C	00	00	00			റ്	우
00215C30	OD	00	00	00	0E	00	00	00	OF	00	00	00	10	00	00	00		Ħ	₿	+
00215C40	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00	◀	1	ij	P
00215C50	15	00	00	00	16	00	00	00	17	00	00	00	18	00	00	00	Τ	Т	4	1
00215C60	19	00	00	00	1A	00	00	00	1B	00	00	00	1C	00	00	00	[\rightarrow	←	
00215C70	1D	00	00	00	1E	00	00	00	1F	00	00	00	20	00	00	00				
00215C80	21	00	00	00	22	00	00	00	23	00	00	00	24	00	00	00	ļ	11	#	\$
00215C90	25	00	00	00	26	00	00	00	27	00	00	00	28	00	00	00	%	&	1	(
00215CA0	29	00	00	00	2A	00	00	00	2B	00	00	00	2C	00	00	00)	*	+	,
00215CB0	2D	00	00	00	2E	00	00	00	2F	00	00	00	30	00	00	00	_		/	0
00215CC0	31	00	00	00	32	00	00	00	33	00	00	00	34	00	00	00	1	2	3	4
00215CD0	35	00	00	00	36	00	00	00	37	00	00	00	38	00	00	00	5	6	7	8
00215CE0	39	00	00	00	ЗΑ	00	00	00	ЗВ	00	00	00	3C	00	00	00	9	:	;	<
00215CF0	3D	00	00	00	ЗЕ	00	00	00	ЗF	00	00	00	40	00	00	00	=	>	?	@
00215D00	41	00	00	00	42	00	00	00	43	00	00	00	44	00	00	00	Α	В	С	D
00215D10	45	00	00	00	46	00	00	00	47	00	00	00	48	00	00	00	E	F	G	Н
00215D20	49	00	00	00	4A	00	00	00	4B	00	00	00	4C	00	00	00	Ι	J	K	L
00215D30	4D	00	00	00	4E	00	00	00	4F	00	00	00	50	00	00	00	M	N	0	Ρ
00215D40	51	00	00	00	52	00	00	00	53	00	00	00	54	00	00	00	Q	R	S	Τ
00215D50	55	00	00	00	56	00	00	00	57	00	00	00	58	00	00	00	U	V	₩	X
00215D60	59	00	00	00	5A	00	00	00	5B	00	00	00	5C	00	00	00	Y	Z	[\
00215D70	5D	00	00	00	5E	00	00	00	5F	00	00	00	60	00	00	00]	^	_	`
00215D80	61	00	00	00	62	00	00	00	63	00	00	00	64	00	00	00	a	b	С	d
00215D90	65	00	00	00	66	00	00	00	67	00	00	00	68	00	00	00	е	f	g	h
00215DA0	69	00	00	00	6A	00	00	00	6B	00	00	00	6C	00	00	00	i	j	k	1
00215DB0	6D	00	00	00	6E	00	00	00	6F	00	00	00	70	00	00	00	m	n	0	p
00215DC0	71	00	00	00	72	00	00	00	73	00	00	00	74	00	00	00	q	r	s	t
00215DD0	75	00	00	00	76	00	00	00	77	00	00	00	78	00	00	00	u	V	W	X
00215DE0	79	00	00	00	7A	00	00	00	7В	00	00	00	7C	00	00	00	У	Z	{	
00215DF0	7D	00	00	00	7E	00	00	00	7F	00	00	00	80	00	00	00	}	~	- 1	
00215E00	81	00	00	00	82	00	00	00	83	00	00	00	84	00	00	00				
00215F10	85	ΠN	ΠN	ΠN	86	ΠN	ΠN	ΠN	87	ΠN	ΠN	ΠN	88	ΠN	ΠN	ΠN				



LEAF.JPG 분석

0xA = 0xA번 클러스터로 연결

Offset	0	1	2	3	4	5	6	7	8	9	Α	В	C	D	E	F				
00215C00	F 8	FF	FF	OF	FF	OF	FF	FF	FF	OF										
00215C10	FF	FF	FF	0F	FF	FF	FF	OF	FF	FF	FF	OF	08	00	00	00				
00215C20	09	00	00	00	0A	00	00	00	0B	00	00	00	0C	00	00	00			റ്	우
00215C30	OD	00	00	00	0E	00	00	00	OF	00	00	00	10	00	00	00		Ħ	₿	+
00215C40	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00	◀	1	ii	P
00215C50	15	00	00	00	16	00	00	00	17	00	00	00	18	00	00	00	Τ	Т	4	1
00215060	19	00	00	00	1A	00	00	00	1B	00	00	00	1C	00	00	00	[\rightarrow	←	
00215C70	1D	00	00	00		00	00	00	1F	00	00	00		00	00	00				
00215C80	21	00	00	00	22	00	00	00	23	00	00	00	24	00	00	00	ļ	"	#	\$
00215C90	25	00	00	00	26	00	00	00	27	00	00	00	28	00	00	00	%	&	'	(
00215CA0	29	00	00	00	2A	00	00	00	2B	00	00	00	2C	00	00	00)	*	+	,
00215CB0	2D	00	00	00	2E	00	00	00	2F	00	00	00	30	00	00	00	-		/	0
00215CC0	31	00	00	00	32	00	00	00	33	00	00	00	34	00	00	00	1	2	3	4
00215CD0	35	00	00	00	36	00	00	00	37	00	00	00	38	00	00	00	5	6	7	8
00215CE0	39	00	00	00	ЗА	00	00	00	ЗВ	00	00	00	3C	00	00	00	9	:	;	<
00215CF0	3D	00	00	00	ЗЕ	00	00	00	ЗF	00	00	00	40	00	00	00	=	>	?	@
00215D00	41	00	00	00	42	00	00	00	43	00	00	00	44	00	00	00	Α	В	С	D
00215D10	45	00	00	00	46	00	00	00	47	00	00	00	48	00	00	00	Ε	F	G	Η
00215D20	49	00	00	00	4A	00	00	00	4B	00	00	00	4C	00	00	00	Ι	J	K	L
00215D30	4D	00	00	00	4E	00	00	00	4F	00	00	00	50	00	00	00	M	И	0	Ρ
00215D40	51	00	00	00	52	00	00	00	53	00	00	00	54	00	00	00	Q	R	S	Τ
00215D50	55	00	00	00	56	00	00	00	57	00	00	00	58	00	00	00	U	V	W	Χ
00215D60	59	00	00	00	5A	00	00	00	5B	00	00	00	5C	00	00	00	Y	Z	[\
00215D70	5D	00	00	00	5E	00	00	00	5F	00	00	00	60	00	00	00]	^	_	`
00215D80	61	00	00	00	62	00	00	00	63	00	00	00	64	00	00	00	a	b	С	d
00215D90	65	00	00	00	66	00	00	00	67	00	00	00	68	00	00	00	е	f	g	h
00215DA0	69	00	00	00	6A	00	00	00	6B	00	00	00	6C	00	00	00	i	j	k	1
00215DB0	6D	00	00	00	6E	00	00	00	6F	00	00	00	70	00	00	00	m	n	0	p
00215DC0	71	00	00	00	72	00	00	00	73	00	00	00	74	00	00	00	q	r	s	t
00215DD0	75	00	00	00	76	00	00	00	77	00	00	00	78	00	00	00	u	v	W	X
00215DE0	79	00	00	00	7A	00	00	00	7В	00	00	00	7C	00	00	00	У	Z	{	
00215DF0	7D	00	00	00	7E	00	00	00	7F	00	00	00	80	00	00	00	}	~	ı	
00215E00	81	00	00	00	82	00	00	00	83	00	00	00	84	00	00	00				
00215F10	85	ΠN	ΠN	ΠN	86	ΠN	ΠN	ΠN	87	ΠN	ΠN	ΠN	88	ΠN	ΠN	ΠN				



LEAF.JPG 분석

0x96번 클러스터가 0x0FFFFF0F이므로 마지막이다. 따라서 0x7번 클러스터로부터 0x96번 클러스터까지 거쳐온 모든 클러스터가 c LEAF.JPG을 이루는 클러스터이다.

Offset	0	1	2	3	4	- 5	6	7	8	9	Α	В	C	ЦĖ	A l	.J₽	ᅝᆯ	VΙ	干.	
00215C00	F8	FF	FF	0F	FF	FF	FF	FF	FF	FF	FF	0F	FF	FF	FF	OF				
00215C10	FF	${\tt FF}$	FF	OF	FF	FF	FF	OF	FF	FF	FF	OF	08	00	00	00				
00215C20	09	00	00	00	0A	00	00	00	0B	00	00	00	0C	00	00	00			ď	우
00215C30	OD	00	00	00	0E	00	00	00	OF	00	00	00	10	00	00	00		Ħ	₿	+
00215C40	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00	◀	1	ij	П
00215050	15	00	00	00	16	00	00	00	17	00	00	00	18	00	00	00	Τ	Т	4	1
00215060	19	00	00	00	1A	00	00	00	1B	00	00	00	1C	00	00	00	}	\rightarrow	←	
00215C70	1D	00	00	00	1E	00	00	00	1F	00	00	00	20	00	00	00				
00215C80	21	00	00	00	22	00	00	00	23	00	00	00	24	00	00	00	ļ	11	#	\$
00215C90	25	00	00	00	26	00	00	00	27	00	00	00	28	00	00	00	%	&	1	(
00215CA0	29	00	00	00	2A	00	00	00	2B	00	00	00	2C	00	00	00)	*	+	,
00215CB0	2D	00	00	00	2E	00	00	00	2F	00	00	00	30	00	00	00	-		/	0
00215CC0	31	00	00	00	32	00	00	00	33	00	00	00	34	00	00	00	1	2	3	4
00215CD0	35	00	00	00	36	00	00	00	37	00	00	00	38	00	00	00	5	6	7	8
00215CE0	39	00	00	00	ЗА	00	00	00	3B	00	00	00	3C	00	00	00	9	:	;	<
00215CF0	3D	00	00	00	ЗЕ	00	00	00	3F	00	00	00	40	00	00	00	=	>	?	@
00215D00	41	00	00	00	42	00	00	00	43	00	00	00	44	00	00	00	Α	В	С	D
00215D10	45	00	00	00	46	00	00	00	47	00	00	00	48	00	00	00	E	F	G	Н
00215D20	49	00	00	00	4A	00	00	00	4B	00	00	00	4C	00	00	00	Ι	J	K	L
00215D30	4D	00	00	00	4E	00	00	00	4F	00	00	00	50	00	00	00	М	И	0	P
00215D40	51	00	00	00	52	00	00	00	53	00	00	00	54	00	00	00	Q	R	S	T
00215D50	55	00	00	00	56	00	00	00	57	00	00	00	58	00	00	00	U	V	W	Χ
00215D60	59	00	00	00	5A	00	00	00	5B	00	00	00	5C	00	00	00	Y	Z	[`
00215D70	5D	00	00	00	5E	00	00	00	5F	00	00	00	60	00	00	00]	^	_	
00215D80	61	00	00	00	62	00	00	00	63	00	00	00	64	00	00	00	a	b	С	d
00215D90	65	00	00	00	66	00	00	00	67	00	00	00	68	00	00	00	e	f	a	h
00215DA0	69	00	00	00	6A 6E	00	00	00	6B	00	00	00	6C	00	00	00	i	j	k	1
00215DB0 00215DC0	6D 71	00	00	00	72	00	00	00	6F 73	00	00	00	70 74	00	00	00	m	n	0	р
00215DD0	75	00	00	00	76	00	00	00	77	00	00	00	78	00	00	00	ď	r	s	t
00215DE0	79	00	00	00	7A	00	00	00	77 7B	00	00	00	7C	00	00	00	u	v -	W	X
00215DE0 00215DF0	7D	00	00	00	7E	00	00	00	7F	00	00	00	80	00	00	00	у }	z ~	{ 	ı
00215DF0	81	00	00	00	82	00	00	00	83	00	00	00	84	00	00	00	ì		•	
00215E00	85	00	00	00	86	00	00	00	87	00	00	00	88	00	00	00				
00215E10 00215E20	89	00	00	00	8A	00	00	00	8B	00	00	00	8C	00	00	00				
00215E20 00215E30	8D	00	00	00	8E	00	00	00	8F	00	00	00	90	00	00	00				
00215E30 00215E40	91	00	00	00	92	00	00	00	93	00	00	00	94	00	00	00				
00215E40 00215E50	95	00	00	00	96	00	00	00	FF	FF	FF	OF	98	00	00	00				
00213630	193	00	00	00	50	00	00	-00	TT	II	LI	OF	50	00	00	00				



LEAF.JPG 분석

```
Offset
00405000
         FF D8 FF E1 O1 B6 45 78
                                69 66 00 00 4D 4D 00 2A
00405010
         00 00 00 08 00 0C 01 OF
                               00 02 00 00 00 07 00 00
00405020
         00 9E 01 10 00 02 00 00 00 07 00 00 00 A6 01 12
00405030
         00 03 00 00 00 01 00 01 00 00 01 12 00 03 00 00
00405040
         00405050
         00 AE 01 1B 00 05 00 00 00 01 00 00 00 B6 01 28
00405060
         00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00
00405070
         00 0E 00 00 00 BE 01 32 00 02 00 00 00 14 00 00
00405080 | 00 CC 01 3C 00 02 00 00 00 10 00 00 00 E0 02 13
00405090
         00 03 00 00 00 01 00 01 00 00 87 69 00 04 00 00
004050A0
         00 01 00 00 00 F0 00 00 00 00 4E 49 4B 4F 4E 00
                                                                 NIKON
004050B0
         00 00 45 35 37 30 30 00 00 00 00 F0 00 00 00 01
004050C0
         00 00 00 F0 00 00 00 01 00 00 51 75 69 63 6B 54
                                                              г QuickT
004050D0
         69 6D 65 20 37 2E 31 00 32 30 30 36 3A 30 35 3A ime 7.1 2006:05:
004050E0
         31 39 20 31 31 3A 33 34 3A 30 39 00 4D 61 63 20
                                                       19 11:34:09 Mac
004050F0
         4F 53 20 58 20 31 30 2E 34 2E 36 00 00 0B 82 9A
                                                       OS X 10.4.6 &
00405100
         00 05 00 00 00 01 00 00 01 7A 82 9D 00 05 00 00
00405110
         00 01 00 00 01 82 88 22 00 03 00 00 00 01 00 02
00405120
         00 00 90 00 00 07 00 00 00 04 30 32 32 30 90 03
00405130
         00 02 00 00 00 14 00 00 01 8A 92 04 00 0A 00 00
00405140 00 01 00 00 01 9E 92 07 00 03 00 00 00 01 00 05
00405150 00 00 92 09 00 03 00 00 00 01 00 10 00 00 92 0A
00405160
         00405170 00 01 00 00 07 80 A0 03 00 04 00 00 00 01 00 00
00405180
         04 B0 00 00 00 00 00 26 25 A0 00 98 96 80 00 36
00405190
         EE 80 00 OF 42 40 32 30 30 34 3A 31 30 3A 31 30
                                                          ₿B@2004:10:10
004051A0 | 20 31 35 3A 30 35 3A 34 36 00 00 00 00 00 77 35 | 15:05:46
```

시작 주소: 0x7번 클러스터의 주소

= DATA 영역의 시작 주소 + (클러스터 번호 – 2) X 클러스터 크기

 $= 0x400000 + (7 - 2) \times 0x1000 = 0x405000$



LEAF.JPG 분석

```
Offset | 0 1 2 3 4 5 6 7 8 9 A B C D E F
00494000 | 48 F9 17 A7 1D AB 67 48 27 ED 57 3C 9F BA 6B EB H
                                          H' < k
00494010
      E9 C6 3F D9 B0 76 D6 CF F2 3C 88 37 CE FD 4E 89
                                               Ν
00494020
      C9 F2 D8 E4 E7 23 F9 D5 99 4E 63 19 F4 AC 22 DA
00494030
      55 6C FA 2F DO DF FE 5E 19 B7 7C 45 6C 47 5C 37
                                           F E1G\7
00494040
      F4 AE 36 5E 65 19 F5 AF 37 19 FE F1 48 E9 7F 02
                                           7 H ¬
00494050
      35 50 01 34 38 03 9A 4D 53 FD 43 FF 00 BD 5E CD
                                      5P-48L
00494060
      04 A5 51 F3 2B FB AF F2 26 9F C0 FD 59 FF D9 00
00494070
      00494080
      00494090
      004940A0
      004940B0
      004940C0
      00 00 00 00 00 00 00 00
                      00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00
00494000
                      00404050
```

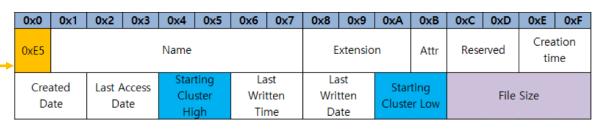
마지막 주소: 0x96번 클러스터의 주소

- = DATA 영역의 시작 주소 + (클러스터 번호 2) X 클러스터 크기
- $= 0x400000 + (0x96 0x2) \times 0x1000 = 0x494000$



삭제파일 복원

"삭제 파일"



	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN

0	1	2	3	4	5	6	7	8	9	Α	В	C	D	E	F				
54	45	53	54	20	20	20	20	20	20	20	08	00	00	00	00	TEST			
00	00	00	00	00	00	В4	71	АЗ	4C	00	00	00	00	00	00				
42	20	00	49	00	6E	00	66	00	6F	00	OF	00	72	72	00	B I n	f	: # c	rr
6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	mat	i o	n	
01	53	00	79	00	73	00	74	00	65	00	OF	00	72	6D	00	гЅуз	t	9 ∯ 1	m
20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	Vο	l u	m	е
53	59	53	54	45	4D	7E	31	20	20	20	16	00	09	ВЗ	71	SYSTEM	$^{\sim}1$	Т	
АЗ	4C	АЗ	4C	00	00	В4	71	АЗ	4C	03	00	00	00	00	00			L	
44	49	52	31	20	20	20	20	20	20	20	10	08	7F	C9	71	DIR1		+□।	l
АЗ	4C	АЗ	4C	00	00	91	71	АЗ	4C	06	00	00	00	00	00			_	
E5	49	47	45	52	20	20	20	4A	50	47	20	18	5B	FO	71	GER	J	PG ↑	[
АЗ	4C	АЗ	4C	00	00	EΑ	71	A3	4C	02	01	22	C5	01	00			٦г"	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	<u> </u>			
00	00	00	00	00	00	00	0	No.	. OJ.	름						▲ 상태	종류	속성	; 경
	00 42 6D 01 20 53 A3 44 A3 E5 A3	00 00 42 20 6D 00 01 53 20 00 53 59 A3 4C 44 49 A3 4C E5 49 A3 4C 00 00	00 00 00 42 20 00 6D 00 61 01 53 00 20 00 56 53 59 53 A3 4C A3 44 49 52 A3 4C A3 E5 49 47 A3 4C A3	54 45 53 54 00 00 00 00 42 20 00 49 6D 00 61 00 01 53 00 79 20 00 56 00 53 59 53 54 A3 4C A3 4C 44 49 52 31 A3 4C A3 4C E5 49 47 45 A3 4C A3 4C 00 00 00 00	\$\begin{array}{cccccccccccccccccccccccccccccccccccc	\$\begin{array}{cccccccccccccccccccccccccccccccccccc	54 45 53 54 20 20 20 00 00 00 00 00 00 00 00 6E 00 6D 00 56 00 6F 00 6C 53 59 53 54 45 4D 7E A3 4C A0 00 00 EA 00 00 00 00 00 00 00 00 00 00 00 00 00	\$\begin{array}{cccccccccccccccccccccccccccccccccccc	\$\begin{array}{c c c c c c c c c c c c c c c c c c c	\$\begin{array}{cccccccccccccccccccccccccccccccccccc	\$\begin{array}{cccccccccccccccccccccccccccccccccccc	\$\begin{array}{c c c c c c c c c c c c c c c c c c c	\$\begin{array}{c c c c c c c c c c c c c c c c c c c	\$\begin{array}{c c c c c c c c c c c c c c c c c c c	\$\begin{array}{cccccccccccccccccccccccccccccccccccc	\$\begin{array}{cccccccccccccccccccccccccccccccccccc	E4 45 53 54 20 20 20 20 20 20 20 08 00 00 00 00 00 00 00 00 00 00 00 00	E4 45 53 54 20 20 20 20 20 20 20 08 00 00 00 00 TEST 00 00 00 00 00 00 B4 71 A3 4C 00 00 00 00 00 00 42 20 00 49 00 6E 00 66 00 6F 00 0F 00 72 72 00 B Info 6D 00 61 00 74 00 69 00 6F 00 00 0F 00 72 6D 00 matio 01 53 00 79 00 73 00 74 00 65 00 0F 00 72 6D 00 rS yste 20 00 56 00 6F 00 6C 00 75 00 00 00 6D 00 65 00 Volu 53 59 53 54 45 4D 7E 31 20 20 20 16 00 09 B3 71 SYSTEM~1 A3 4C A3 4C 00 00 B4 71 A3 4C 03 00 00 00 00 00 44 49 52 31 20 20 20 20 20 20 10 08 7F C9 71 DIR1 A3 4C A3 4C 00 00 91 71 A3 4C 06 00 00 00 00 E5 49 47 45 52 20 20 20 4A 50 47 20 18 5B F0 71 GER JI A3 4C A3 4C 00 00 00 EA 71 A3 4C 02 01 22 C5 01 00 00 00 00 00 00 00 00 00 00 00 00 00	E4 45 53 54 20 20 20 20 20 20 20 08 00 00 00 00 00 00 00 00 00 00 00 00

004000C0 00 00 00 00 0			00 00 00 00 00 00					
004000D0 00 00 00 00 0	00 00 00	No.	이름	상태	종류	속성	경로	확장자
004000E0 00 00 00 00 0	00 00 00		.=				-	
	n oo oo o							
		1	DIR1	활성	폴더	일반	/DIR1	
		2	x recovered	삭제	폴더	일반	/recovered	
		3	System Volume Information	활성	폴더	일반	/System Volume I	
		4		삭제	파일	일반	/?IGERJPG	JPG
		5	Unused	비	파일	가상	/Unused	



삭제파일 복원

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0xE5				Name				E	xtensio	n	Attr	Rese	erved	Crea tin	
	ated ate		Access		ting ster gh	Wri	ist tten me	Writ	st tten ite		ting er Low		File	Size	

	Attribute
0x02	Hidden
0x08	Volume Label
0x10	Directory
0x0F	LFN

Offset	0	1	2	3	4	- 5	- 6	7	8	9	A	В	C	D	E	F		
00400000	54	45	53	54	20	20	20	20	20	20	20	08	00	00	00	00	TEST	
00400010	00	00	00	00	00	00	В4	71	АЗ	4C	00	00	00	00	00	00		
00400020	42	20	00	49	00	6E	00	66	00	6F	00	OF	00	72	72	00	B I n	fo¤rr
00400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	mat:	io n
00400040	01	53	00	79	00	73	00	74	00	65	00	OF	00	72	6D	00	гЅуз	te¤rm
00400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	V o :	lu me
00400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	09	ВЗ	71	SYSTEM	~1 T
00400070	АЗ	4C	АЗ	4C	00	00	В4	71	АЗ	4C	03	00	00	00	00	00		L
00400080	44	49	52	31	20	20	20	20	20	20	20	10	08	7F	С9	71	DIR1	+□•
00400090	АЗ	4C	ΑЗ	4C	00	00	91	71	АЗ	4C	06	00	00	00	00	00		_
004000A0	E5	49	47	45	52	20	20	20	4A	50	47	20	18	5B	FO	71	GER	JPG ↑[
004000B0	АЗ	4C	АЗ	4C	00	00	EΑ	71	АЗ	4C	02	01	22	C5	01	00		דר"
004000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
004000D0	00	00	00	00	00	00	00	00	00	00	ØO	00	00	00	00	00		
004000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
NN4NNNFN	nn	ΠN	ΠN	ΠN	ΠN	ΠN	ŊΠ	ΠΠ	ΠN	UN	ΠN	ΠN	ΠN	ΠN	ΠN	ΠΠ		



삭제파일 복원

```
Offset.
00500000
        FF D8 FF E0 00 10 4A 46
                              49 46 00 01 01 01 01 20
00500010
        01 2C 00 00 FF DB 00 43 00 08 06 06 07 06 05 08
00500020
         07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 •••
00500030 | 13 OF 14 1D 1A 1F 1E 1D 1A 1C 1C 2O 24 2E 27 20 | ₩XY →
00500040 22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27
00500050 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09
                                                   9=82<.342
00500060 09 00 0B 00 18 0D 0D 18 32 21 10 21 32 32 32 32
222222222222222
00500090
                                                    2222222222222
        32 32 32 32 32 32 32 32 32 32 32 32 32 FF CO
005000A0 00 11 08 02 58 03 E8 03 01 11 00 02 11 01 03 11
005000B0
        01 FF C4 00 1C 00 00 02 03 01 01 01 01 00 00 00
005000C0
        00 00 00 00 00 00 04 05 02 03 06 01 07 00 08 FF
005000D0 C4 00 4A 10 00 02 01 03 03 02 05 01 06 03 07 03
        02 03 05 09 01 02 03 00 04 11 05 12 21 31 41 06
005000E0
005000F0
        13 22 51 61 71 14 32 81 91 A1 B1 23 42 C1 07 15
00500100 | 52 62 D1 E1 F0 33 72 F1 24 82 43 63 92 16 25 34 | Rb
00500110 | 44 53 93 A2 C2 64 35 73 B2 D2 E2 FF C4 00 19 01 |
00500130 | 00 01 02 03 04 05 FF C4 00 31 11 00 02 02 03 00
00500140 02 01 04 02 01 02 06 03 01 01 00 00 01 02 11 03
00500150 21 31 12 41 04 13 22 32 51 61 71 91 42 B1 14 81
                                                              우니
00500160 A1 D1 F0 F1 23 33 52 E1 C1 FF DA 00 0C 03 01 00
00500170 | 02 11 03 11 00 3F 00 F1 32 2B 32 0E 62 98 11 A0 |
00500180 | 67 D9 A6 O4 81 A0 O9 O6 AO 44 83 50 32 41 A8 O2
00500190
         5E 61 14 OC 90 9B 1D E8 28 97 DA 31 DE 80 B2 B7
00500120 R8 CD 30 R2 96 97 34 28 20 2D 24 20 08 79 86 80
```

시작 주소: 0x102번 클러스터의 주소

= DATA 영역의 시작 주소 + (클러스터 번호 – 2) X 클러스터 크기

 $= 0x400000 + (0x102 - 0x2) \times 0x1000 = 0x500000$

