파일 시스템

김 종 성

국민대학교

파일시스템 소개

- 파일 시스템이 필요한 이유?
  - 저장 매체의 용량이 증가함에 따라 저장되는 파일의 수도 급격히 증가
  - 원하는 파일을 읽고 쓰는 기본적인 기능부터 데이터를 검색, 저장, 관리하기 위한 규약이 필요

- 파일시스템 이란?
  - 디지털 데이터를 효과적으로 관리하기 위해 파일을 체계적으로 기록하는 방식
  - 사용자에게 파일과 디렉터리를 계층 구조로 데이터를 저장하도록 하는 메커니즘
  - 파일이 어디에 저장되어 있는지 조직화하고, 사용자의 데이터를 구조적으로 정의함

파일 시스템

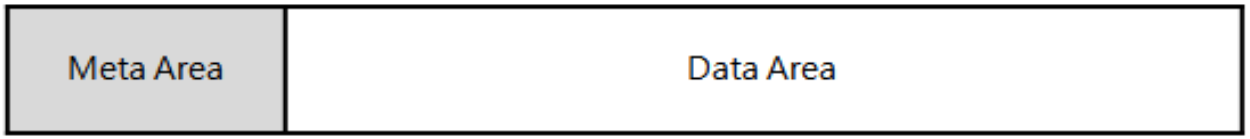
- ✓ 파일 시스템
  - 저장장치 내 데이터를 읽고 쓰기 위해 미리 정해진 규약
- ✓ 파일 시스템의 종류
  - **Windows System**
    - **FAT (File Allocation Table)**
    - **NTFS (New Technology File System)**
  - **Unix/Linux**
    - **UFS (Unix File System)**
    - **Ext2/3 (Extended File system)**
  - **CD-ROM, Network**
    - **ISO 9660 (International Organization for Standardization)**
    - **NFS (Network File System)**

파일시스템의 구조

✓ 파일시스템의 구조

- 파일시스템의 기본적인 동작은 운영체제가 각 파일을 사용하기 위해 저장되어 있는 위치로 접근하여 해당 데이터를 읽도록 함
- 또한 데이터의 위치를 파악하기 위하여 사용자가 저장된 파일의 목록을 확인할 수 있도록 지원함

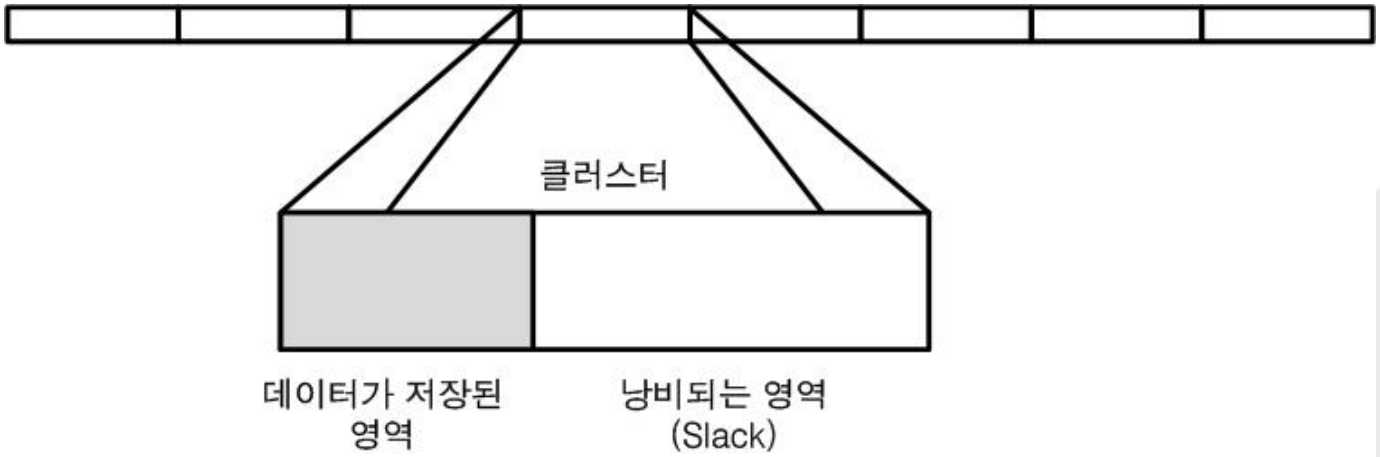
✓ 파일시스템의 추상화 구조



- 사용자가 생성한 파일의 내용은 데이터 영역에 기록
- 메타 영역에는 파일 관리를 위한 파일의 이름, 위치, 크기, 시간 정보 등이 기록
- 파일 시스템은 이러한 메타 정보를 유지 관리함으로써 파일 시스템을 효과적으로 관리

파일 시스템의 구성 요소

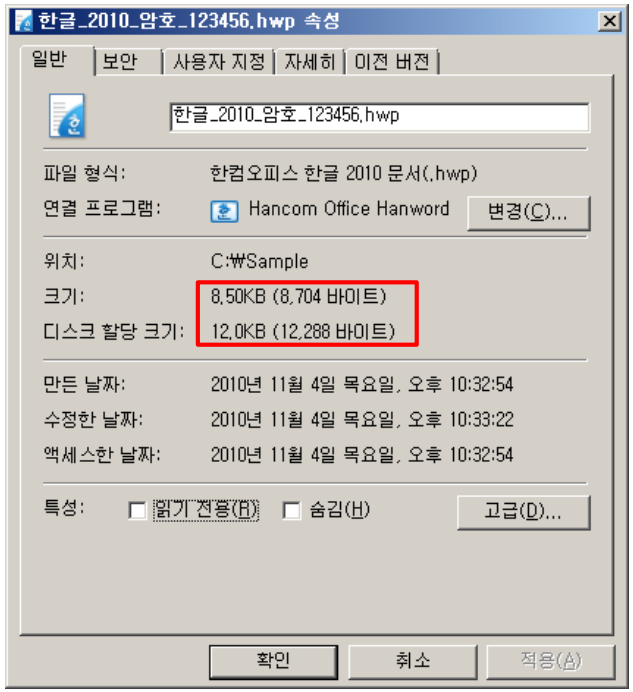
- ✓ 물리적 측면 : 섹터의 나열
- ✓ 논리적 측면 : 클러스터, 파일, 폴더
  - 클러스터
    - 파일 시스템에서 저장 장치에 데이터를 읽고 쓰는 논리적인 기본 단위
      - NTFS에서는 기본적으로 4,096bytes의 크기를 가짐



클러스터 크기

✓ 클러스터의 크기에 따른 장단점

구분	장점	단점
클러스터 크기가 작을 때	낭비되는 영역(Slack)이 적다.	파일 정보 관리 영역이 커진다.
클러스터 크기가 클 때	클러스터 처리 부담이 적다.	낭비되는 영역(Slack)이 많다.



파일 크기

8,704 바이트

클러스터 할당 크기

4096 * 3 = 12,288 바이트

클러스터 Slack

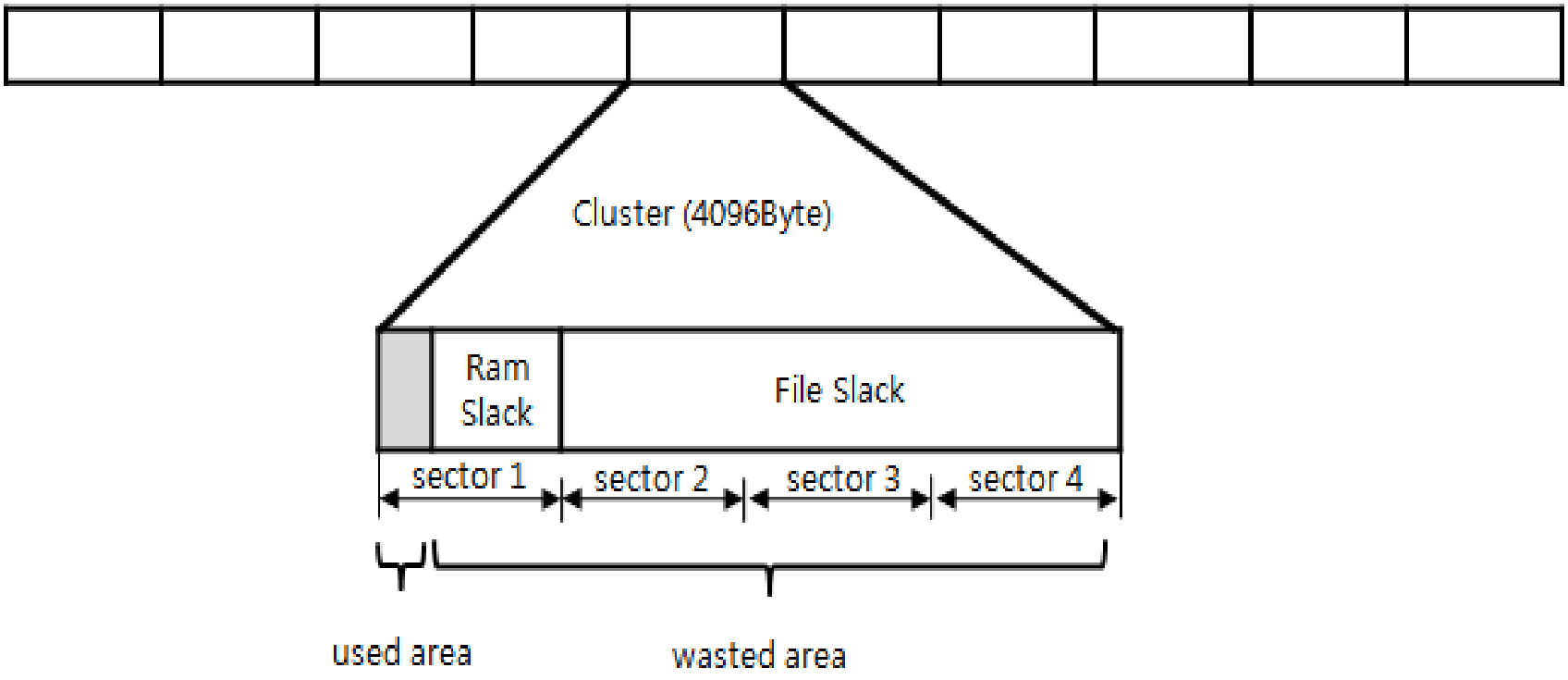
12,288 - 8,704 = 3,584 바이트

File System

- Slack Space
  - ✓ 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간
  - ✓ 파일에 할당된 공간이지만 사용되지 않는 낭비 공간
    - RAM Slack (Sector Slack) / File Slack (Drive Slack)
      - 파일 카빙에 활용
      - 이전에 사용한 데이터가 존재, 흔적 조사에 활용

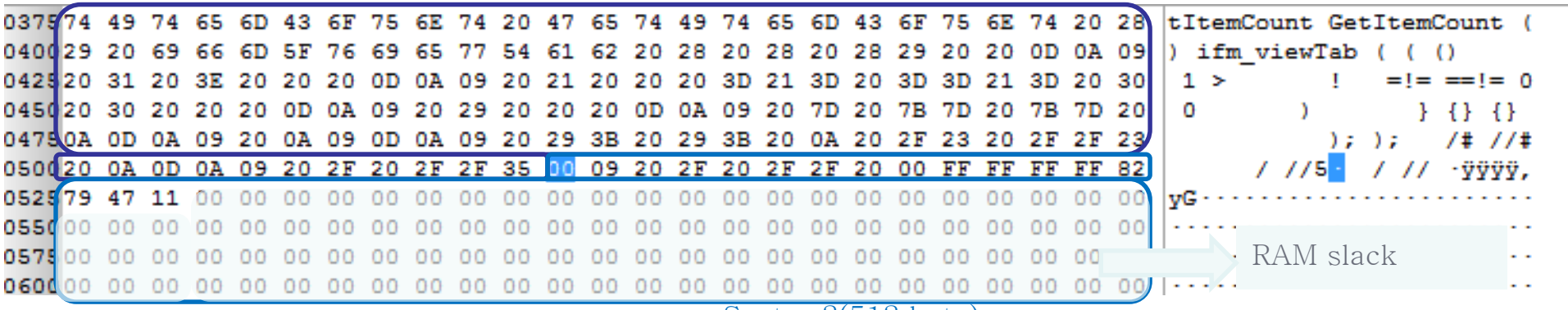
File System

- Slack Space (RAM Slack & File Slack)

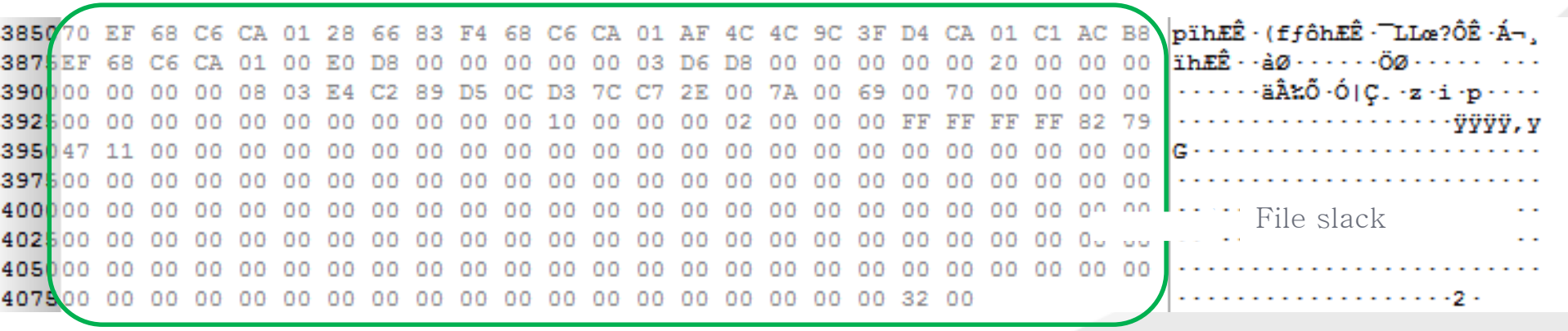


Slack Space (RAM Slack & File Slack)

Sector 1(512 byte)



Sector 2(512 byte)

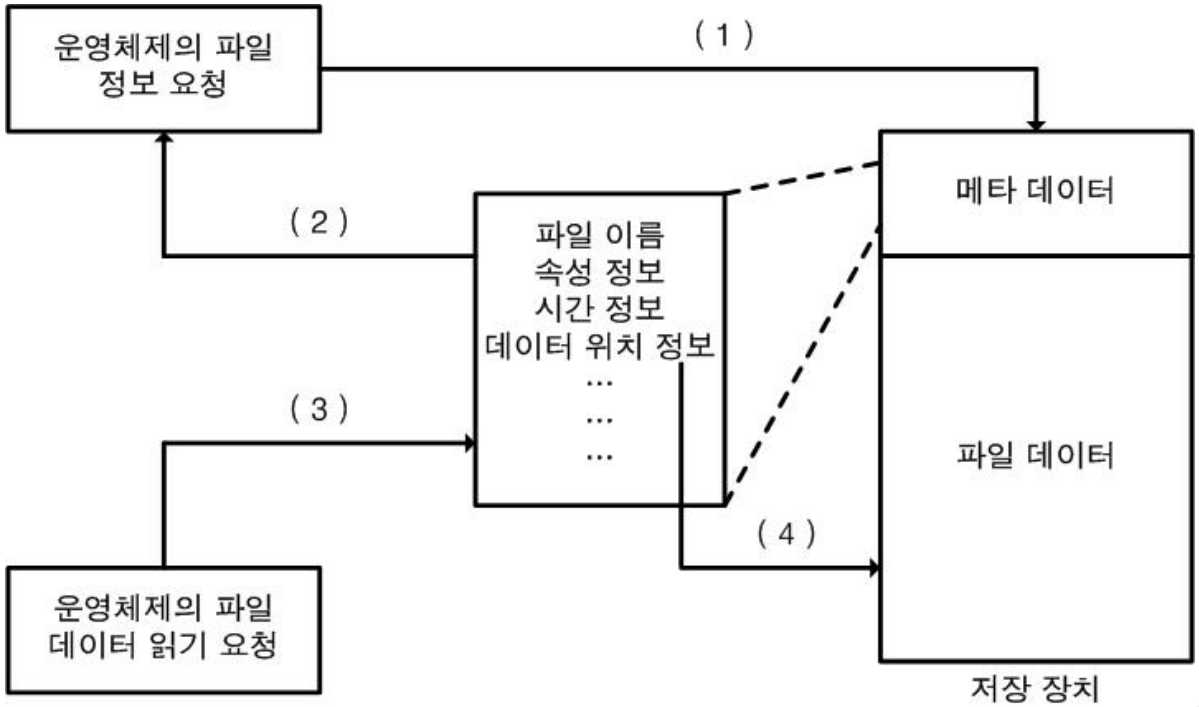


Sector 8(512 byte)

파일

- ✓ 파일
  - 속성을 기록하는 메타 데이터 영역
    - 파일 시스템에서 파일을 관리할 수 있는 정보
      - 파일 이름, 시간 정보, 크기, 속성, 클러스터 위치 등
  - 실제 데이터를 기록하는 영역
    - 클러스터 단위의 실제 데이터

파일 정보 요청 과정


운영체제의 파일
정보 요청
(1)
(2)
파일 이름
속성 정보
시간 정보
데이터 위치 정보
…
…
…
메타 데이터
(3)
파일 데이터
(4)
운영체제의 파일
데이터 읽기 요청
저장 장치

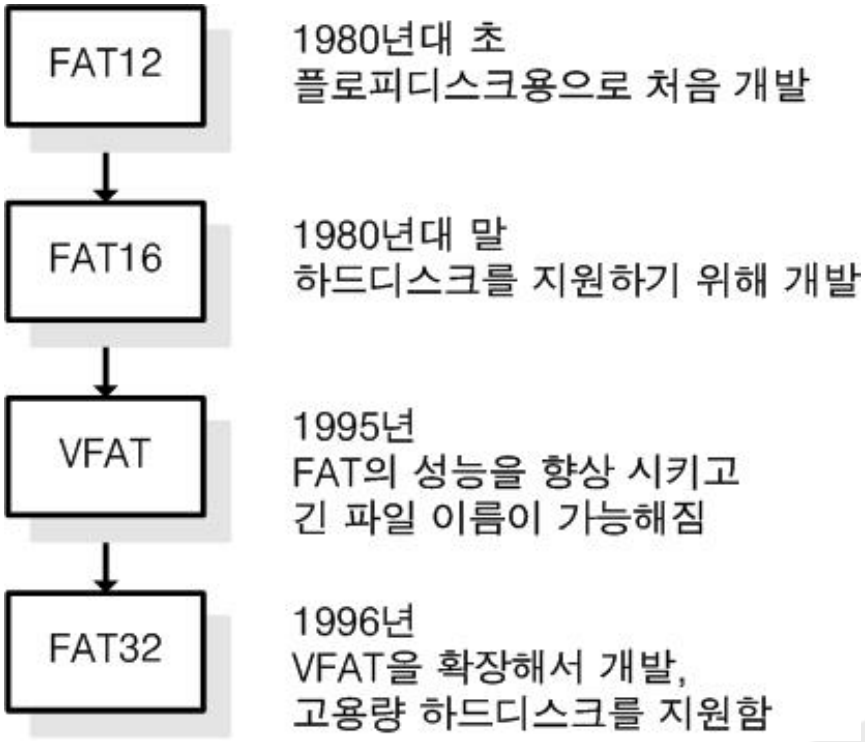
폴더

- 폴더 (디렉토리)
  - 파일들을 계층화 하고 그룹화 하기 위한 개념
  - 파일과 폴더는 파일 시스템 관점에서 크게 다르지 않음
    - 폴더의 데이터 영역은 하위에 존재하는 폴더 및 파일 리스트를 포함

- 모든 파일 시스템은 파일 정보를 관리하는 자료 구조를 가짐
  - **FAT: Linked List**
  - **NTFS: B-Tree**

FAT

- FAT (File Allocation Table)
  - BASIC에서 플로피 디스크를 관리하기 위해 구현
    - MS-DOS와 함께 보급
  - FAT 파일 시스템의 변화 과정



✓ FAT 파일 시스템 비교

구분	FAT12	FAT16	FAT32
사용 용도	플로피 디스크	저용량 하드디스크	하드디스크
클러스터 표현 비트 수	12bit	16bit	32bit(28bit만 사용)
최대 클러스터 개수	4,084개	65,524개	약 2^{28}개
최대 볼륨 크기	16MB	2GB	2TB (이론상, 실제 32GB)
파일의 최대 크기	볼륨 크기 만큼	볼륨 크기만큼	4GB
디렉토리당 최대 파일 개수	디렉토리 개념 없음	65,535개	65,535개

File Allocation Table

- Structure – FAT Area

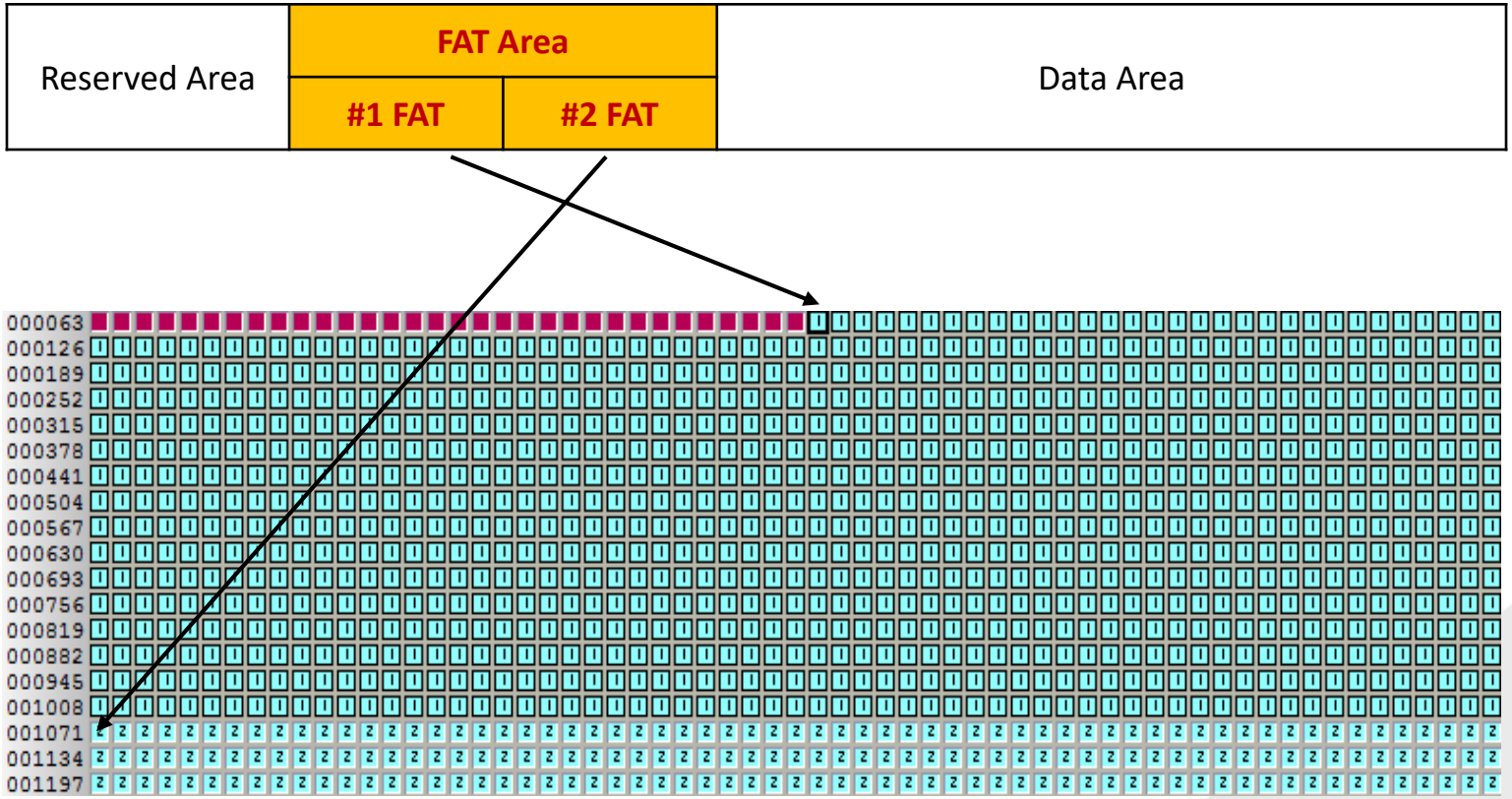
✓ Reserved Area: 섹터 당 바이트 수, 클러스트 당 섹터 수 등 파일시스템 정보 포함, 또한 비할당 클러스터의 첫 위치 및 전체 비할당 클러스터 수를 알려 줌

✓ FAT (File Allocation Table) Area - #1 FAT, #2 FAT(Backup)

✓ 저장된 파일의 클러스터 할당 관계를 표현 - FAT 12/16 (2 bytes), FAT 32 (4 bytes)

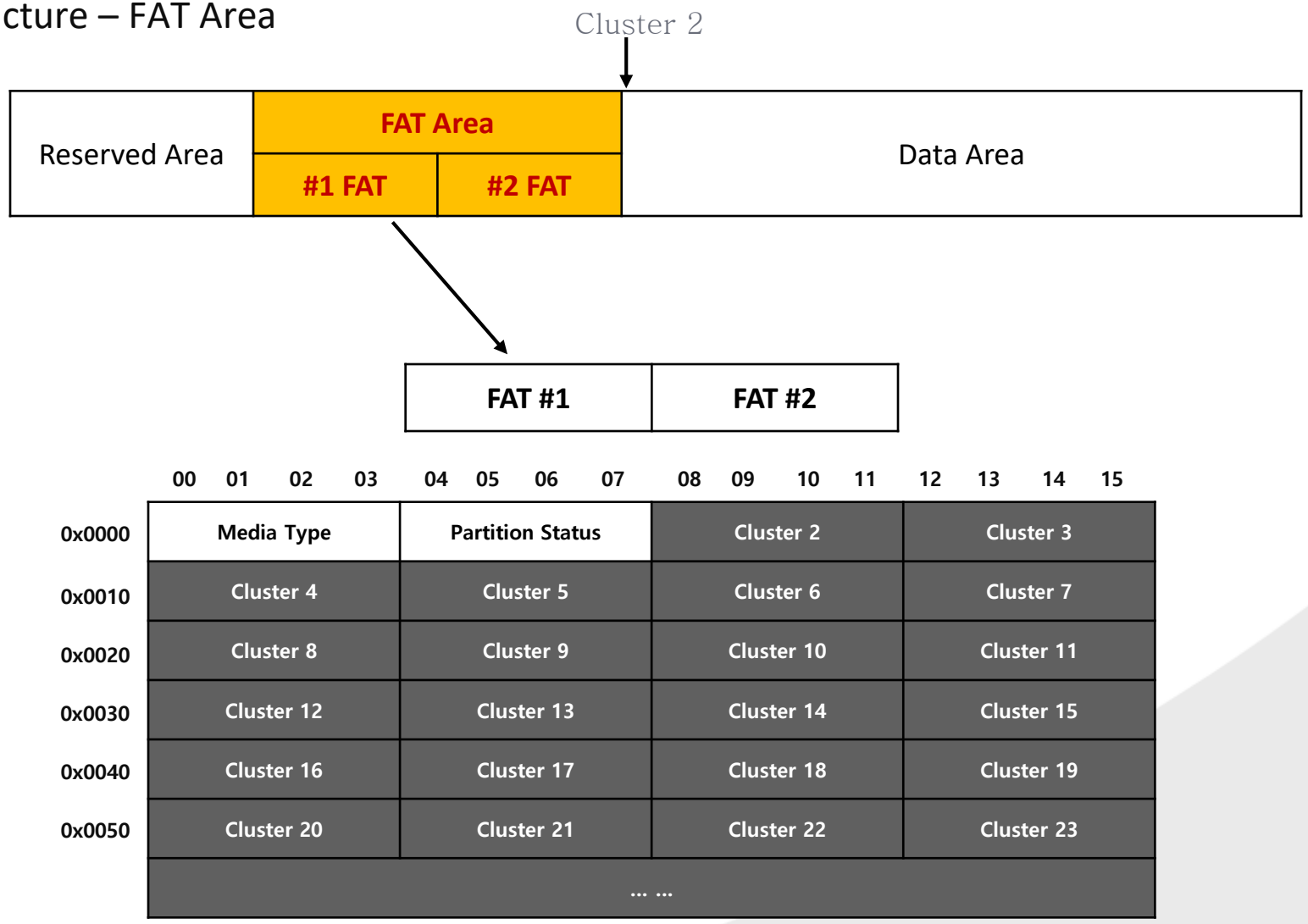
File Allocation Table

- Structure – FAT Area



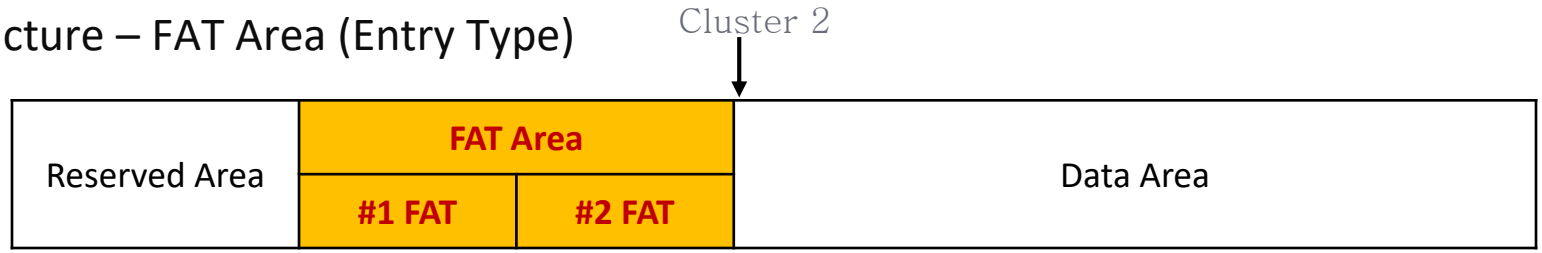
File Allocation Table

- Structure – FAT Area

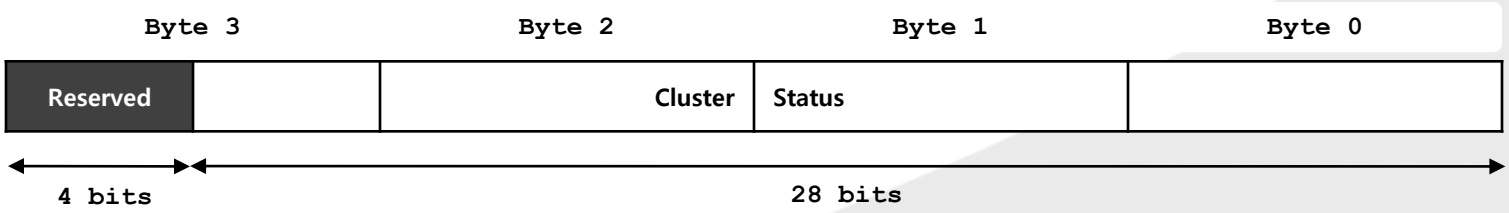


File Allocation Table

- Structure – FAT Area (Entry Type)

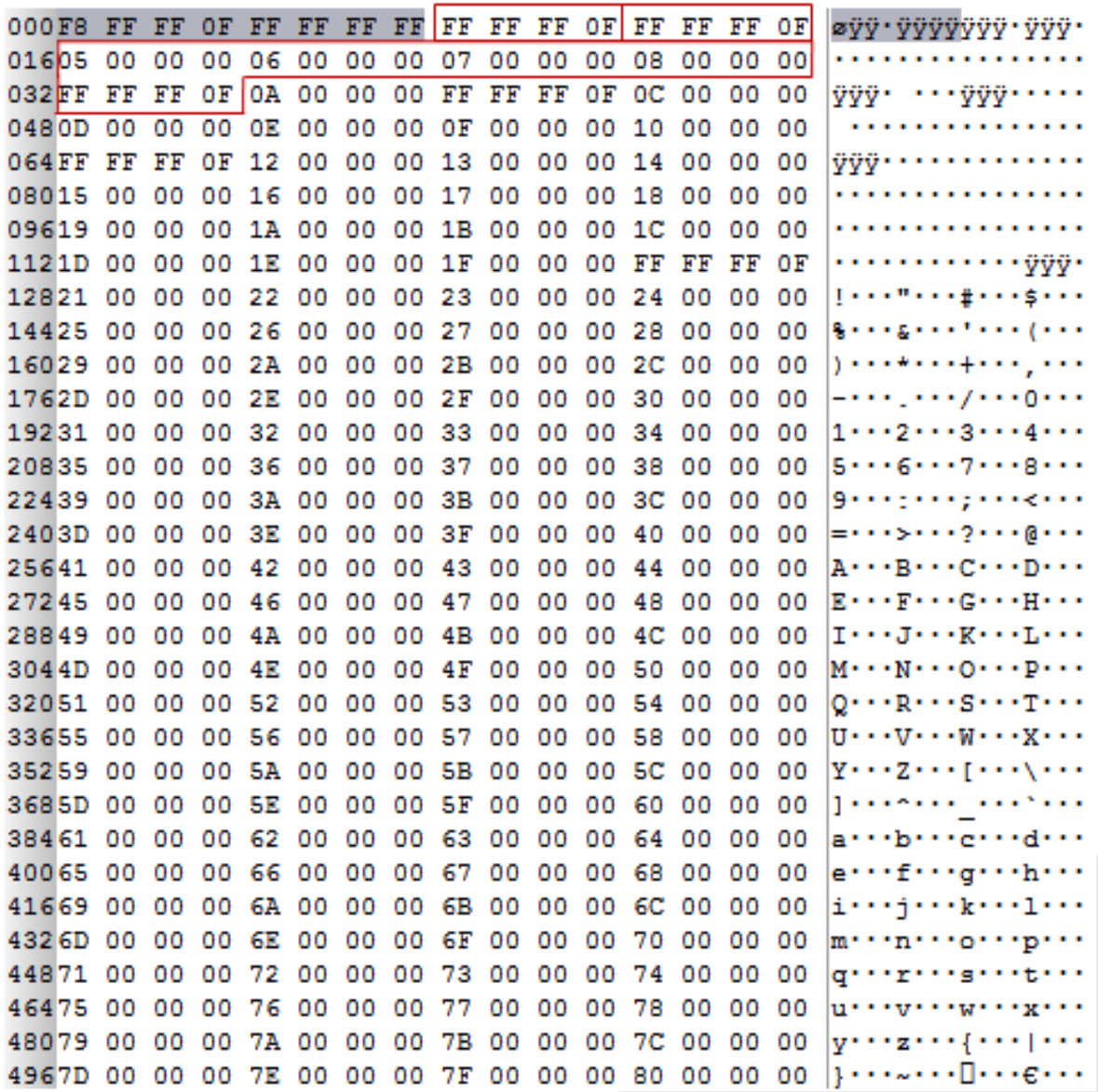


FAT 12	FAT 16	FAT 32	설명
0x000	0x0000	0x00000000	Unallocated (Free) cluster
0x001	0x0001	0x00000001	Reserved cluster
0x002	0x0002 ~ 0xEFFF	0x00000002 ~ 0x0FFFFFEF	Allocated cluster
0xFF0 ~ 0xFF6	0xFFF0 ~ 0xFFF6	0x0FFFFFF0 ~ 0x0FFFFFF6	Reserved cluster
0xFF7	0xFFF7	0x0FFFFFF7	Bad cluster
0xFF8	0xFFF8 ~ 0xFFFF	0x0FFFFFF8 ~ 0x0FFFFFFF	End-of-file marker



File Allocation Table

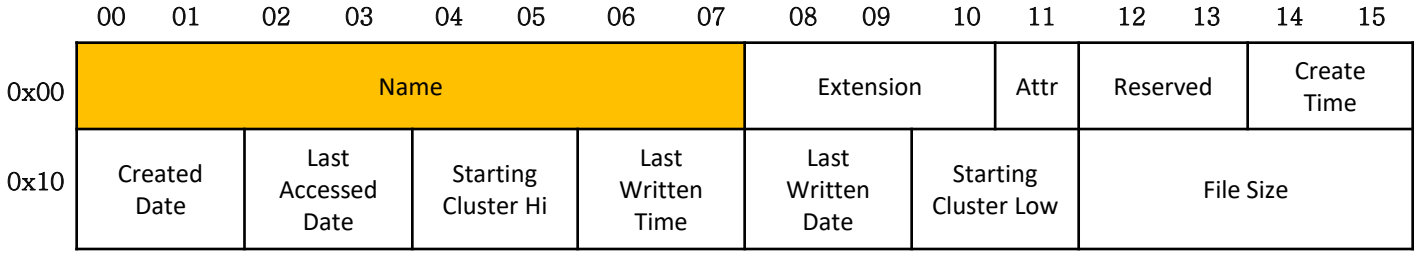
- FAT Dump



```
000 F8 FF FF 0F FF FF FF FF FF FF FF 0F FF FF FF 0F  øÿÿ·ÿÿÿÿÿÿÿ·ÿÿÿ·
016 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00  ················
032 FF FF FF 0F 0A 00 00 00 FF FF FF 0F 0C 00 00 00  ÿÿÿ· ···ÿÿÿ·····
048 0D 00 00 00 0E 00 00 00 0F 00 00 00 10 00 00 00   ···············
064 FF FF FF 0F 12 00 00 00 13 00 00 00 14 00 00 00  ÿÿÿ·············
080 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00  ················
096 19 00 00 00 1A 00 00 00 1B 00 00 00 1C 00 00 00  ················
112 1D 00 00 00 1E 00 00 00 1F 00 00 00 FF FF FF 0F  ············ÿÿÿ·
128 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00  !···"···#···$···
144 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00  %···&···'···(···
160 29 00 00 00 2A 00 00 00 2B 00 00 00 2C 00 00 00  )···*···+···,···
176 2D 00 00 00 2E 00 00 00 2F 00 00 00 30 00 00 00  -···.···/···0···
192 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00  1···2···3···4···
208 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00  5···6···7···8···
224 39 00 00 00 3A 00 00 00 3B 00 00 00 3C 00 00 00  9···:···;···<···
240 3D 00 00 00 3E 00 00 00 3F 00 00 00 40 00 00 00  =···>···?···@···
256 41 00 00 00 42 00 00 00 43 00 00 00 44 00 00 00  A···B···C···D···
272 45 00 00 00 46 00 00 00 47 00 00 00 48 00 00 00  E···F···G···H···
288 49 00 00 00 4A 00 00 00 4B 00 00 00 4C 00 00 00  I···J···K···L···
304 4D 00 00 00 4E 00 00 00 4F 00 00 00 50 00 00 00  M···N···O···P···
320 51 00 00 00 52 00 00 00 53 00 00 00 54 00 00 00  Q···R···S···T···
336 55 00 00 00 56 00 00 00 57 00 00 00 58 00 00 00  U···V···W···X···
352 59 00 00 00 5A 00 00 00 5B 00 00 00 5C 00 00 00  Y···Z···[···\···
368 5D 00 00 00 5E 00 00 00 5F 00 00 00 60 00 00 00  ]···^···_···`···
384 61 00 00 00 62 00 00 00 63 00 00 00 64 00 00 00  a···b···c···d···
400 65 00 00 00 66 00 00 00 67 00 00 00 68 00 00 00  e···f···g···h···
416 69 00 00 00 6A 00 00 00 6B 00 00 00 6C 00 00 00  i···j···k···l···
432 6D 00 00 00 6E 00 00 00 6F 00 00 00 70 00 00 00  m···n···o···p···
448 71 00 00 00 72 00 00 00 73 00 00 00 74 00 00 00  q···r···s···t···
464 75 00 00 00 76 00 00 00 77 00 00 00 78 00 00 00  u···v···w···x···
480 79 00 00 00 7A 00 00 00 7B 00 00 00 7C 00 00 00  y···z···{···|···
496 7D 00 00 00 7E 00 00 00 7F 00 00 00 80 00 00 00  }···~···□···€···
```

File Allocation Table

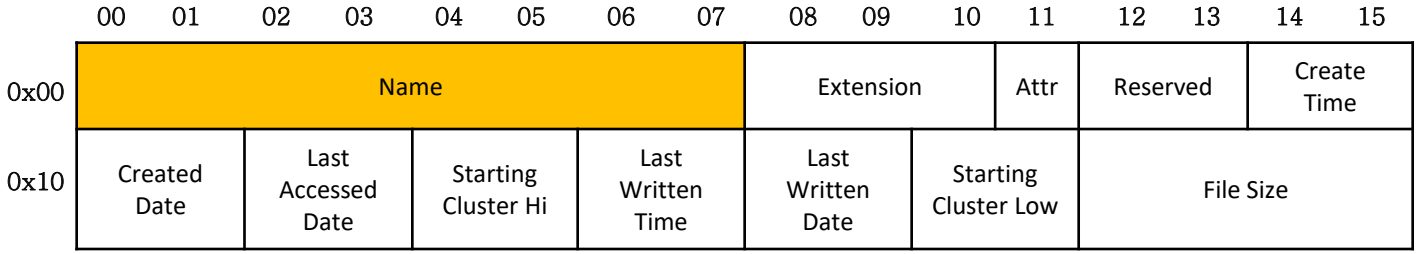
- Structure – FAT Data Area (Directory Entry – Name)



- ✓ 첫번째 바이트 파일 이름 또는 파일의 상태를 나타냄: 0xE5는 삭제된 파일 등
- ✓ 파일 이름 또는 디렉토리 이름의 문자 제한
  - 영어 대문자 : A ~ Z (소문자는 대문자로 변환)
  - 특수 문자 : $ % ` - _ @ ~ ! ( ) { } ^ # &

File Allocation Table

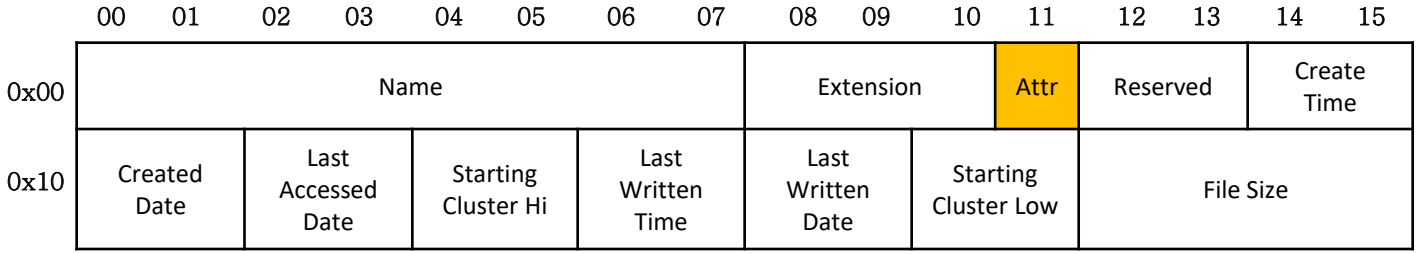
- Structure – FAT Data Area (Directory Entry – Name)



File Name	Name + Extender (11 bytes)										
FOO.BAR	F	O	O						B	A	R
FILEDATA.DOC	F	I	L	E	D	A	T	A	D	O	C
foo	F	O	O								
foo.bar	F	O	O						B	A	R
Pickle.A	P	I	C	K	L	E			A		
.BIG	□≈ ∴ . Name[0]∠ 0x20τ , ∅Λ										
HELLO!.JPG	□≈ ∴ . ≠ (“!”) 8□ ◡♥ H(										

File Allocation Table

- Structure – FAT Data Area (Directory Entry – Attribute)



Attribute	설명
0x0000 0001	Read only
0x0000 0010	Hidden file
0x0000 0100	System file
0x0000 1000	Volume label
0x0000 1111	Long file name (LFN)
0x0001 0000	Directory
0x0010 0000	Archive

파일 시스템의 시간 정보

✓ FAT의 시간 정보

- 생성 시간, 수정 시간, 접근 날짜

Name	File Created	Last Written	Last Accessed
091030_전체세미나 발표	2009/10/30 18:23:28	2009/10/30 18:23:30	2009/10/30
100121	2010/02/25 05:20:50	2010/02/25 05:20:52	2010/02/25
100121_정진형, 이진경	2010/01/21 15:44:07	2010/01/21 15:44:08	2010/01/21
100224 포렌식 전체세미나	2010/02/24 20:00:16	2010/02/24 20:00:18	2010/02/24
100305_이동찬, 최용석	2010/03/05 21:00:07	2010/03/05 21:00:08	2010/03/05
100518_정진형, 이진경	2010/05/18 14:28:29	2010/05/18 14:28:30	2010/05/18
100903_Live memory forensics of mob...	2010/09/03 18:24:46	2010/09/03 18:24:48	2010/09/03
_00305	2010/03/05 21:00:07	2010/03/05 21:00:08	2010/03/05
딱따구리	2010/01/21 15:44:07	2010/01/21 15:44:08	2010/01/21
매	2010/05/18 14:28:29	2010/05/18 14:28:30	2010/05/18
병아리	2010/03/05 21:00:07	2010/03/05 21:00:08	2010/03/05
새 폴더	2010/09/03 18:24:46	2010/09/03 18:24:48	2010/09/03
솔개	2010/02/25 05:20:50	2010/02/25 05:20:52	2010/02/25
100121_김태수_All-IP 네트워크에서...	2010/01/26 01:42:40	2010/01/26 01:42:42	2010/01/26
100121_이진경_A novel time memory...	2010/01/21 18:51:39	2010/01/21 17:26:02	2010/02/25
100121_정진형_Recovering Deleted ...	2010/01/21 19:34:37	2010/01/21 18:45:10	2010/02/25
._100518_Network forensic framewor...	2010/05/18 18:51:47	2010/05/18 18:51:46	2010/05/18
~$All-IP 네트워크에서의.pptx	2010/01/26 01:42:20	2010/01/26 01:43:20	2010/01/26
~$100305_시큐박스 하드 복구서비...	2010/03/05 20:35:27	2010/03/05 21:00:38	2010/03/05
100518_Network forensic frameworks...	2010/05/18 18:01:25	2010/05/18 18:01:24	2010/11/02
100121_김태수_All-IP 네트워크에서...	2010/01/21 18:52:35	2010/01/21 18:11:22	2010/02/25

FAT 파일 시스템의 행위에 따른 시간 정보 변화

✓ 파일 생성 및 접근

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
☐ 1	TEST2.TXT			TXT	Text	Document		File, Archive		07/16/08	07/15/08 01:19:46오전	07/15/08 01:19:48오전
☐ 2	TEST1.TXT			TXT	Text	Document		File, Archive		07/16/08	07/15/08 01:19:20오전	07/15/08 01:19:22오전
☐ 3	TEST3.TXT			TXT	Text	Document		File, Archive		07/17/08	07/15/08 01:22:02오전	07/15/08 01:22:04오전

- 파일 생성(M = A = C time) 후 접근 시 접근 시간 변경
  - 단, A time이 날짜만 존재하기 때문에 같은 날 다른 시간에 접근하더라도 이를 파악하기 어려움

FAT 파일 시스템의 행위에 따른 시간 정보 변화

✓ 파일 복사

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
1	TEST.TXT			TXT	Text	Document		File, Archive		07/16/08	07/16/08 02:44:44오후	07/11/08 05:17:54오후
2	TEST1.TXT			TXT	Text	Document		File, Archive		07/16/08	07/16/08 02:44:44오후	07/15/08 02:04:16오전
3	TEST2.TXT			TXT	Text	Document		File, Archive		07/16/08	07/16/08 02:44:44오후	07/15/08 02:04:38오전
4	TEST3.TXT			TXT	Text	Document		File, Archive		07/16/08	07/16/08 02:44:44오후	07/15/08 02:05:00오전

- 생성 시간과 접근 시간이 복사 실행 시간으로 변경
  - 수정 시간은 원본 파일의 수정 시간 그대로 유지
  - 개별 복사와 일괄 복사의 결과가 동일
    - 일괄 복사의 경우, 생성 시간이 모두 동일한 시간

FAT 파일 시스템의 행위에 따른 시간 정보 변화

✓ 파일 이동

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
1	dragmove1.txt			txt	Text	Document		File, Archive		07/15/08	07/15/08 11:31:20오전	07/15/08 11:31:22오전
2	dragmove2.txt			txt	Text	Document		File, Archive		07/15/08	07/15/08 11:31:38오전	07/15/08 11:31:40오전

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
1	dragmove1.txt			txt	Text	Document		File, Archive		07/16/08	07/16/08 03:34:20오후	07/15/08 01:32:46오후
2	dragmove2.txt			txt	Text	Document		File, Archive		07/16/08	07/16/08 03:35:56오후	07/15/08 01:33:06오후

✓ '이동' 명령 사용 및 Drag & Drop 결과 확인

- 생성 시간과 접근 시간이 실제 파일 이동 시간으로 변경

FAT 파일 시스템의 행위에 따른 시간 정보 변화

✓ 압축된 파일로부터 추출

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
1	TEST1.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 02:58:26오후	07/15/08 02:58:26오후
2	TEST2.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 02:58:38오후	07/15/08 02:58:38오후
3	TEST3.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 02:58:52오후	07/15/08 02:58:52오후
4	TEST4.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 02:59:06오후	07/15/08 02:59:06오후
5	TEST5.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 02:59:18오후	07/15/08 02:59:18오후

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
1	TEST1.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 03:05:30오후	07/15/08 02:58:26오후
2	TEST2.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 03:05:30오후	07/15/08 02:58:38오후
3	TEST3.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 03:05:30오후	07/15/08 02:58:52오후
4	TEST4.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 03:05:30오후	07/15/08 02:59:06오후
5	TEST5.TXT			TXT	Text	Document		File, Archive		07/15/08	07/15/08 03:05:30오후	07/15/08 02:59:18오후

- 생성 시간이 압축해제 시간으로 동일하게 변경
  - 하지만 수정 시간이 압축된 원본 파일의 수정 시간으로 설정

FAT 파일 시스템의 행위에 따른 시간 정보 변화

✓ 파일 내용 수정

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
1	TEST1.TXT			TXT	Text	Document		File, Archive		07/16/08	07/16/08 10:39:48오전	07/16/08 10:39:50오전
2	TEST2.TXT			TXT	Text	Document		File, Archive		07/16/08	07/16/08 10:40:10오전	07/16/08 10:40:12오전

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
1	TEST1.TXT			TXT	Text	Document		File, Archive		07/16/08	07/16/08 10:39:48오전	07/16/08 10:41:16오전
2	TEST2.TXT			TXT	Text	Document		File, Archive		07/16/08	07/16/08 10:40:10오전	07/16/08 10:40:12오전

– 수정 시간과 접근 시간이 내용 수정 시간으로 변경

✓ FAT 파일시스템의 시간 정보 분석의 한계

– 접근 시간 정보에 날짜만 존재하여 시간 정보 분석에 한계가 있음

NTFS

✓ NTFS (New Technology File System)

- 1993년 Microsoft Windows NT 3.1에 포함되어 발표
- 현재 윈도우 운영체제 환경에서 널리 사용되고 있음

Version	OS	Features
v1.0	Windows NT 3.1	N/A
v1.1 (3.5)	Windows NT 3.5	N/A
v1.2 (4.0)	Windows 3.51	Compressed files
v3 (5.0)	Windows 2000	Disk Quotas
v3.1 (5.1)	Windows XP	Encryption
v3.1 (5.2)	Windows Server 2003	N/A
v3.1 (6.0)	Windows Vista	Transactional
v3.1	Windows Server 2008	N/A

NTFS Concepts

✓ Features

특 징	설 명
Update Sequence Number Journal	파일의 모든 변경 내용을 기록하여 시스템 오류 발생으로 재부팅 될 경우 잘못된 처리 작업을 롤백(Rollback)
ADS (Alternate Data Stream)	파일 이름은 하나인 다중 데이터 스트림 지원
Sparse 파일	파일 데이터가 대부분 0일 경우 실제 데이터는 기록하지 않고 정보만 기록
파일 압축	LZ77의 변형된 알고리즘을 사용하여 파일 데이터 압축
EFS (Encrypting File System)	파일을 암호화 하는 기능으로 빠른 암,복호화를 위해 FEK(File Encryption Key)를 통한 대칭키 방식의 암호화 수행
Quotas	사용자 별 디스크 사용량 제한
유니코드 지원	다국어 지원 (파일, 디렉터리, 볼륨 이름 모두 유니코드로 저장)
대용량 지원	이론상 Exa Byte(2^{64}), 실제로는 약 16 TB (2^{44})

NTFS Concepts

Master File Table

- NTFS는 파일, 디렉터리 및 메타 정보까지 파일 형태로 관리
- 각 파일은 위치, 시간 정보, 크기, 파일 이름 등을 MFT Entry라는 특별한 구조로 저장
- MFT(Master File Table)은 NTFS 상의 모든 MFT Entry들의 배열
- MFT Entry 0 ~ 15번은 파일 시스템 생성시 함께 생성되어 특별한 용도로 사용

파일 시스템 분석

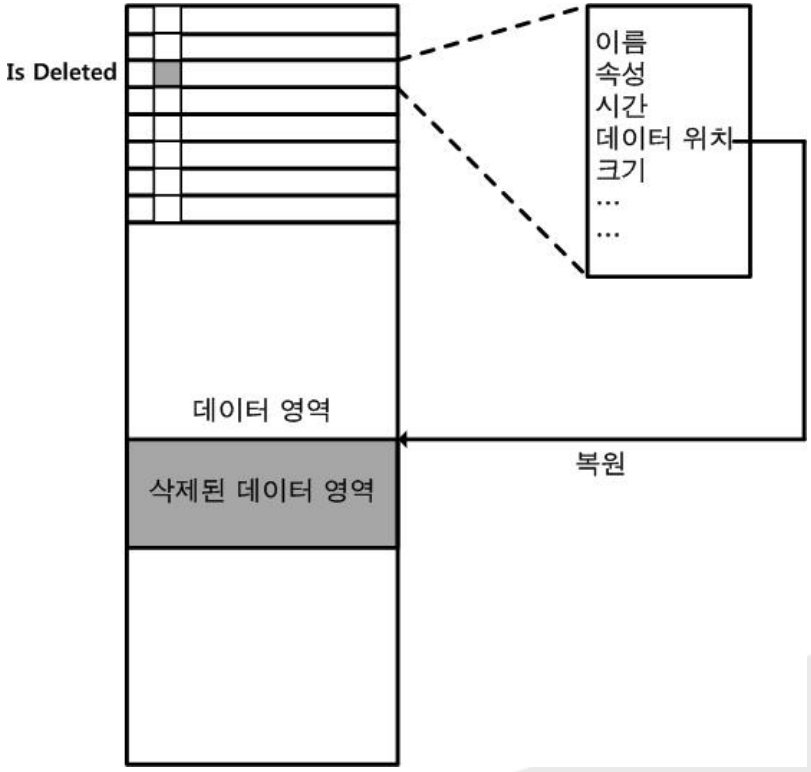
- **Timestamp Analysis**
  - ✓ 사건이 발생한 시점을 중심으로 데이터 분석
  - ✓ 시간의 흐름 파악이 중요
  - ✓ 시간의 역전 및 의도적인 조작이 발생했는지 파악
  - ✓ 시간 정보 위치
    - ✓ FAT : 해당 파일, 디렉터리의 Directory Entry
      (create time, last written time, created date,
      last accessed date, last written date)
    - ✓ NTFS : 해당 파일의 속성
      ($STANDARD_INFORMATION, $FILE_NAME)

파일 시스템 분석

- **Signature Analysis**
  - ✓ 파일 시그니처와 확장자가 일치하는지 검사
  - ✓ 확장자 변경을 통해 의도적으로 파일을 은폐할 가능성
  - ✓ 확장자 위치
    - ✓ FAT : 해당 파일의 Directory Entry
    - ✓ NTFS : 해당 파일의 $FILE_NAME 속성

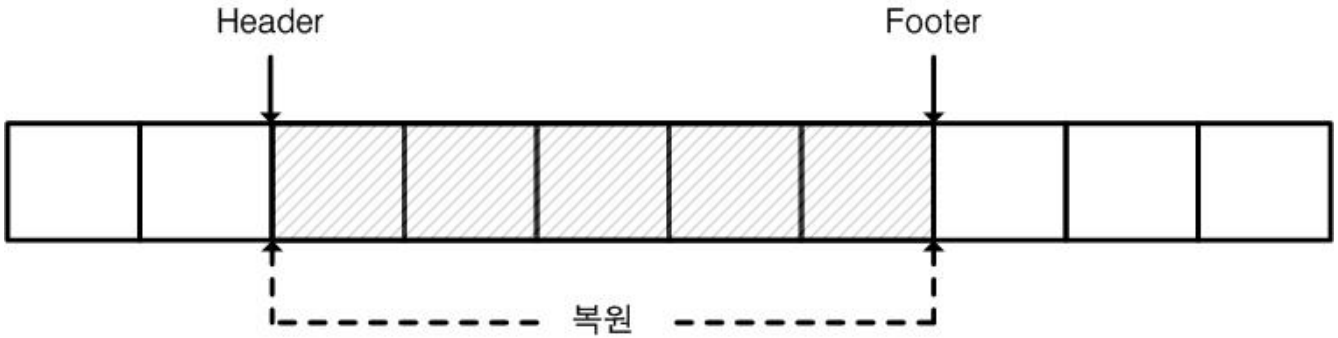
파일 복원 기법

- ✓ 파일 시스템 정보 기반 복구
  - 파일의 메타 데이터의 삭제 Flag 기반 복구
    - 파일 삭제시 데이터/메타데이터 영역을 덮어쓰지 않기 때문에 가능
    - 다른 파일로 덮이지 않았다면 복구 가능



파일 복원 기법

- ✓ 파일 시스템 정보를 얻을 수 없는 경우의 복구
  - **File Carving**
    - 파일 시스템에서 얻을 수 있는 정보 없이 '파일 자체 정보' 기반 복구
    - 즉, 파일의 고유한 특성이 있는 파일만 복구 가능

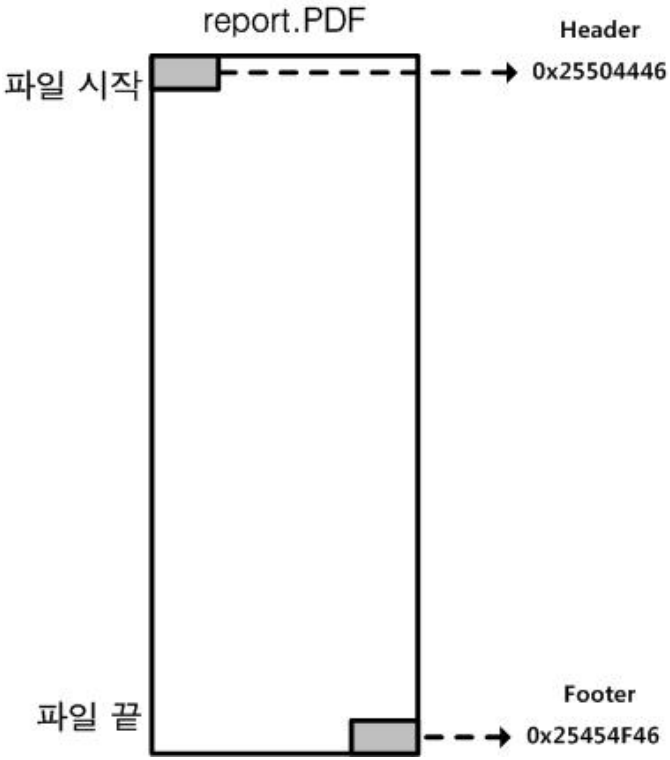


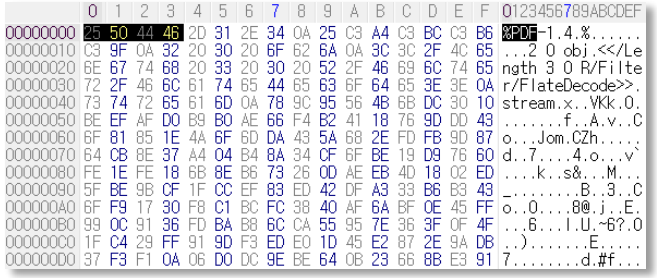
파일 복원 기법

File Carving

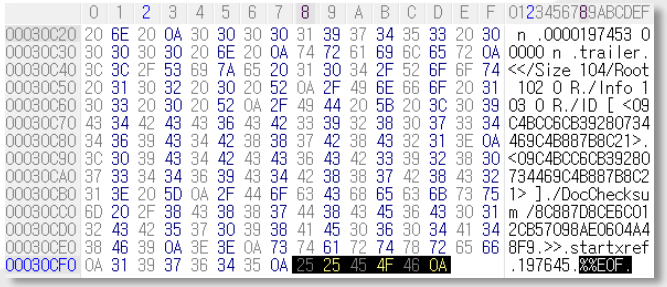
– 파일의 Header와 Footer 정보

- 일부 파일은 파일의 시작과 끝을 알 수 있는 고유한 값을 가짐
  - PDF, GIF. PNG, JPG, ALZ, ZIP, RAR, MPG …





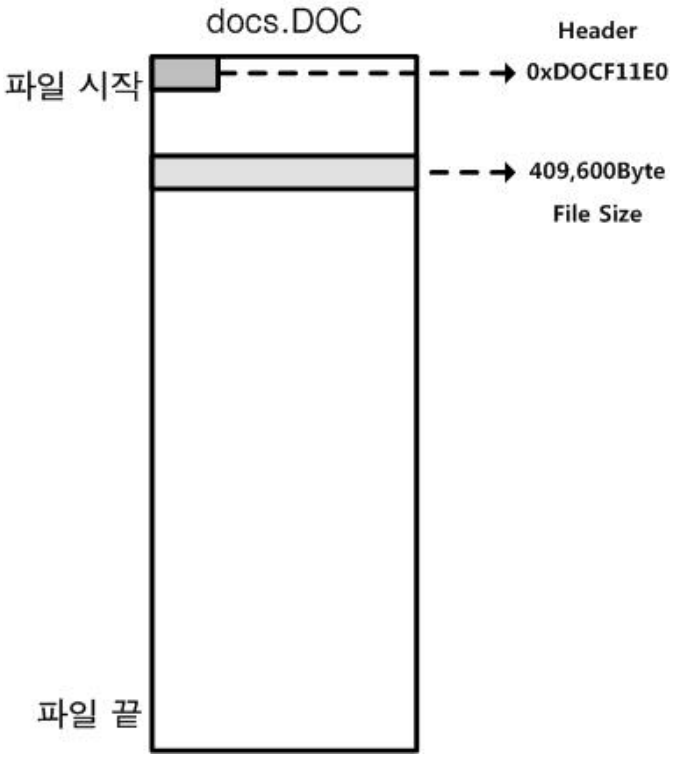
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	25	50	44	46	2D	31	2E	34	0A	25	C3	A4	C3	BC	C3	B6	%PDF-1.4.%.....
00000010	C3	9F	0A	32	20	30	20	6F	62	6A	0A	3C	3C	2F	4C	65	...2 0 obj.<</Le
00000020	6E	67	74	68	20	33	20	30	20	52	2F	46	69	6C	74	65	ngth 3 0 R/Filte
00000030	72	2F	46	6C	61	74	65	44	65	63	6F	64	65	3E	3E	0A	r/FlateDecode>>.
00000040	73	74	72	65	61	6D	0A	78	9C	95	56	4B	6B	DC	30	10	stream.x..VKk.0.
00000050	BE	EF	AF	D0	B9	B0	AE	66	F4	B2	41	18	76	9D	DD	43	.......f..A.v..C
00000060	6F	81	85	1E	4A	6F	6D	DA	43	5A	68	2E	FD	FB	9D	87	o...Jom.CZh.....`
00000070	64	CB	8E	37	A4	04	B4	8A	34	CF	6F	BE	19	D9	76	60	d..7....4.o...v`
00000080	FE	1E	FE	18	6B	8E	B6	73	26	0D	AE	EB	4D	18	02	ED	....k..s&...M...
00000090	5F	BE	9B	CF	1F	CC	EF	83	ED	42	DF	A3	33	B6	B3	43	_.......B..3..C
000000A0	6F	F9	17	30	F8	C1	BC	FC	38	40	AF	6A	BF	0E	45	FF	o..0....8@.j..E.
000000B0	99	0C	91	36	FD	BA	B8	6C	CA	55	95	7E	36	3F	0F	4F	...6...l.U.~6?.O
000000C0	1F	C4	29	FF	91	9D	F3	ED	E0	1D	45	E2	87	2E	9A	DB	..)........E.....
000000D0	37	F3	F1	0A	06	D0	DC	9E	BE	64	0B	23	66	8B	E3	91	7........d.#f...

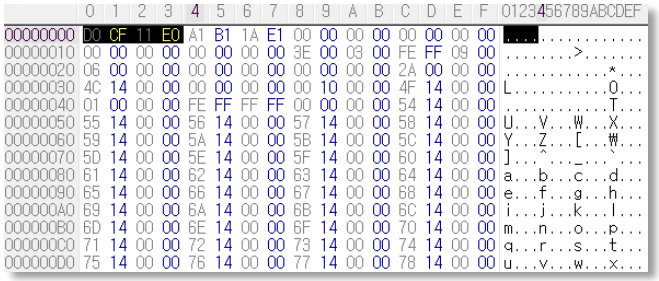


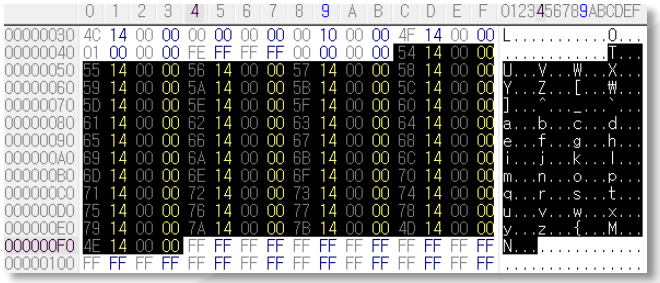
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00030C20	20	6E	20	0A	30	30	30	30	31	39	37	34	35	33	20	30	n .0000197453 0
00030C30	30	30	30	30	20	6E	20	0A	74	72	61	69	6C	65	72	0A	0000 n .trailer.
00030C40	3C	3C	2F	53	69	7A	65	20	31	30	34	2F	52	6F	6F	74	<</Size 104/Root
00030C50	20	31	30	32	20	30	20	52	0A	2F	49	6E	66	6F	20	31	102 0 R./Info 1
00030C60	30	33	20	30	20	52	0A	2F	49	44	20	5B	20	3C	30	39	03 0 R./ID [<09
00030C70	43	34	42	43	43	36	43	42	33	39	32	38	30	37	33	34	C4BCC6CB39280734
00030C80	34	36	39	43	34	42	38	38	37	42	38	43	32	31	3E	0A	469C4B887B8C21>.
00030C90	3C	30	39	43	34	42	43	43	36	43	42	33	39	32	38	30	<09C4BCC6CB39280
00030CA0	37	33	34	34	36	39	43	34	42	38	38	37	42	38	43	32	734469C4B887B8C2
00030CB0	31	3E	20	5D	0A	2F	44	6F	63	43	68	65	63	6B	73	75	1>]./DocChecksu
00030CC0	6D	20	2F	38	43	38	38	37	44	38	43	45	36	43	30	31	m /8C887D8CE6C01
00030CD0	32	43	42	35	37	30	39	38	41	45	30	36	30	34	41	34	2CB57098AE0604A4
00030CE0	38	46	39	0A	3E	3E	0A	73	74	61	72	74	78	72	65	66	8F9.>>.startxref
00030CF0	0A	31	39	37	36	34	35	0A	25	25	45	4F	46	0A			.197645.%%EOF.

파일 복원 기법

- File Carving
  - 파일의 Header와 File size 정보
    - 일부 파일은 파일의 시작과 크기를 알 수 있는 정보를 포함하고 있음
      - DOC, ODT, ODS, BMP, AVI, ASF, WAV …







감사합니다