

평—화로운
FAT 포렌식 분석
JWMSG

이름 : 정재완

KITRI BoB 6 DF 수료생
광운대학교 입학을 앞두고 있다.

요즘 안드로이드 외주를 한다.

명예 고3 이었고,
(수능 7일 남겨두고 POC 컨퍼런스 갔다고 한다.)

드디어 (2019 1월) 봉인해제 하였다.



이름 : 정재완

나이 : 0x14
성별 : XY
잘하는 것(?) : 보안/개발
좋아하는 것 : 보안/개발
취미/여가 : 보안/개발
여자친구 : (드디어 솔로 4년차)
소개 시켜주시면 감사하겠습니다.
(딥러닝 읍읍!!)



“ 4’s ”
“핫식스, 박카스, 리눅스, 이클립스”

-JWMSG

오늘 뭐 할까요?

1. 파일시스템을 알아봅시다.
2. FAT? 그게 뭉니까? (~~비만??~~)
3. FAT32 삽질하기 (~~삽질의 시작...~~)
4. 파일을 복구해 봅시다.

잡담) FAT32툴 을 만들어 보다...

“어디서 사골 곰국 냄새가 나!”

–죄송합니다. 제가 좀 많이 우려먹었습니다.

“I love 간단히.”

-진짜 전문적이고 깊은 내용을 다루지는 않습니다!

파일을 저장하다?

이걸



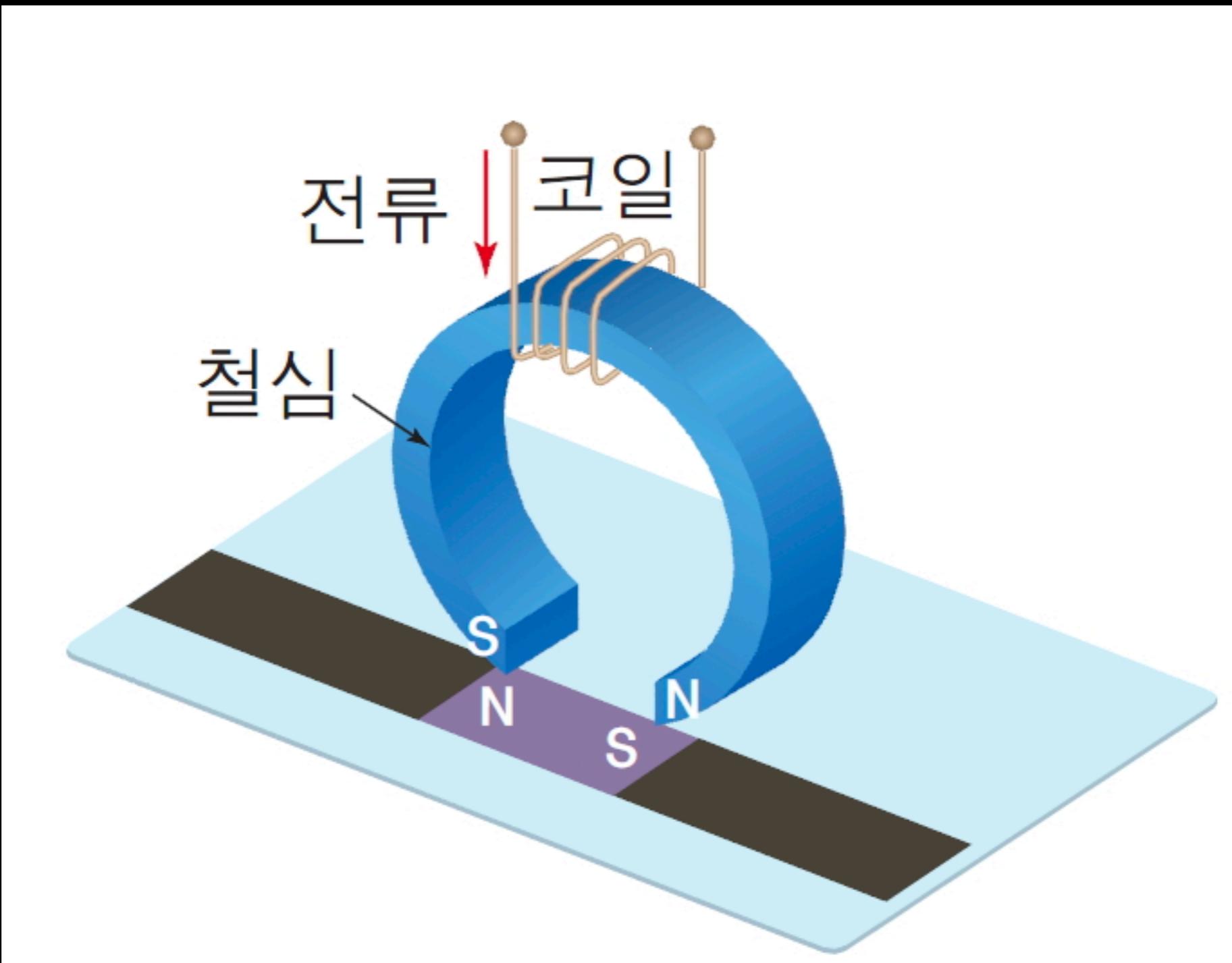
여기에??



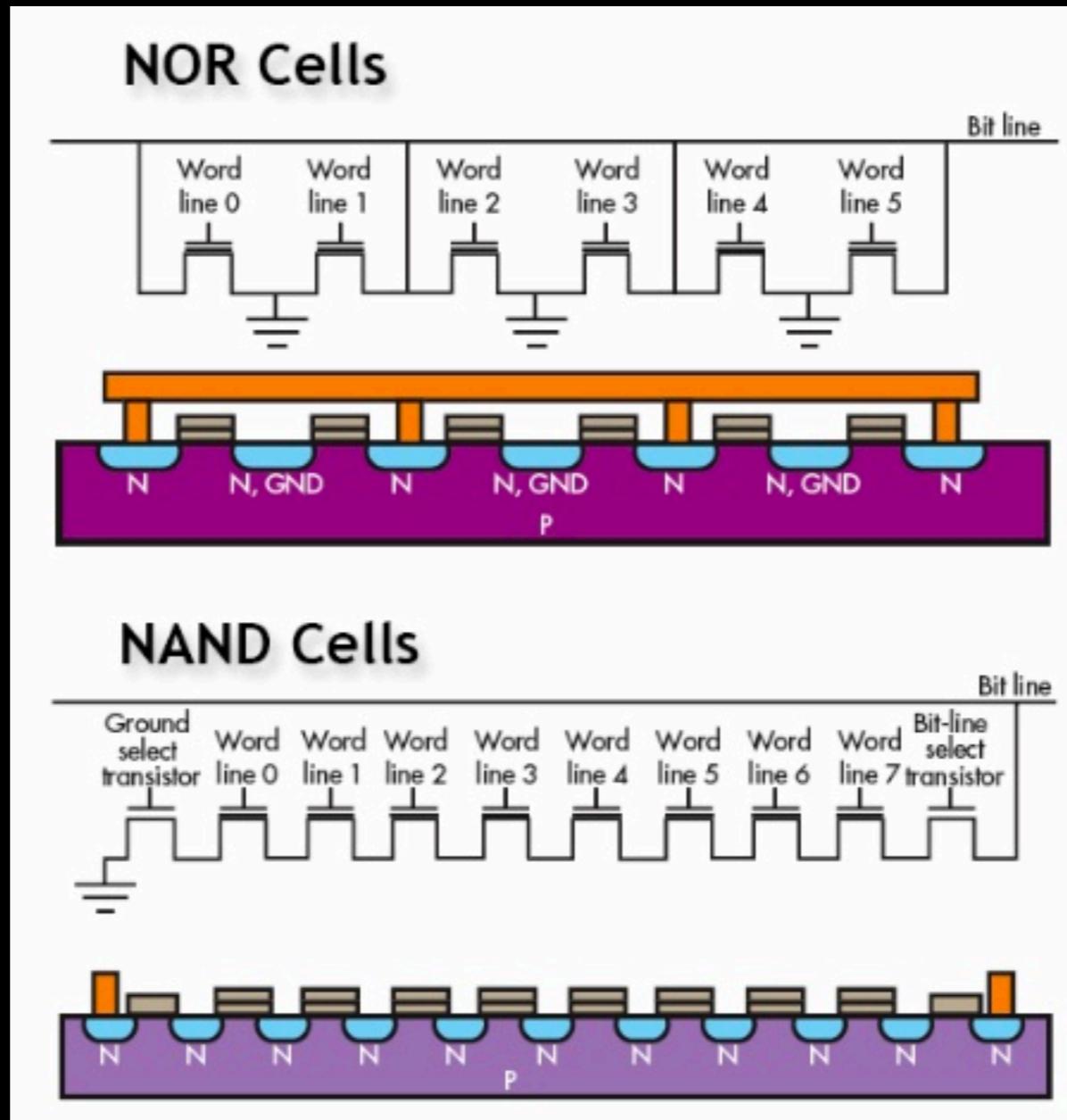
HDD

SSD

흔히 고등학교때 배우는



고등학교?????????????



흠... 그렇게 많은 데이터를?

그렇게 시스템이 필요해 졌다.

Partition & Volume

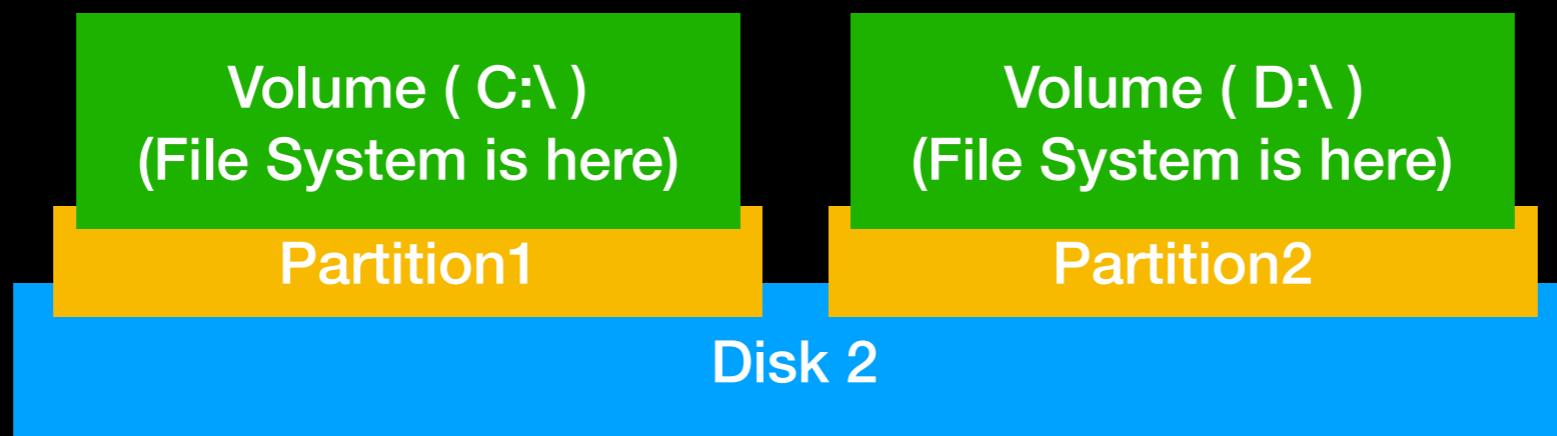
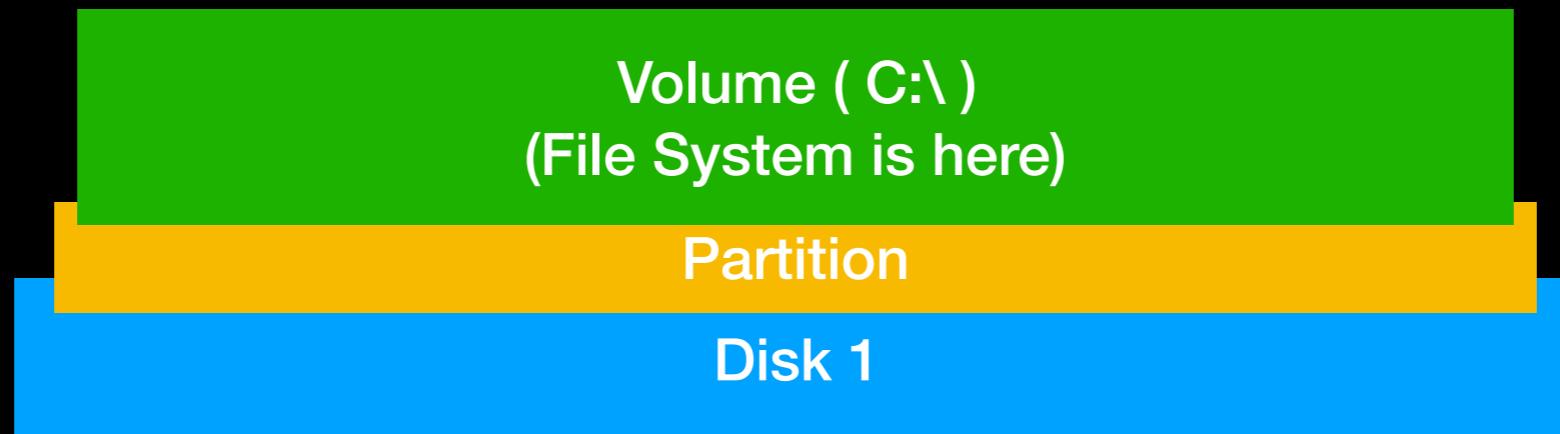
Partition

- Disk partitioning or Disk slicing is Creation of one or more regions on a hard disk or other secondary storage, so that an operating system can manage information in each region separately.
- 디스크파티션 작업은 하드디스크의 기억공간을 “파티션”이라는 별도의 데이터 영역으로 분할하는것을 말한다.

Volume

- In computer data storage, a volume or logical drive is a single accessible storage area with a single filesystem, typically(though not necessarily) resident on a single petition of a hard disk.
- 볼륨 또는 논리드라이브는 하나의 파일시스템을 갖춘 하나의 접근 가능한 저장공간 영역으로, 일반적으로 하드디스크의 단일 파티션에 상주한다.

가장 기본적인 구조

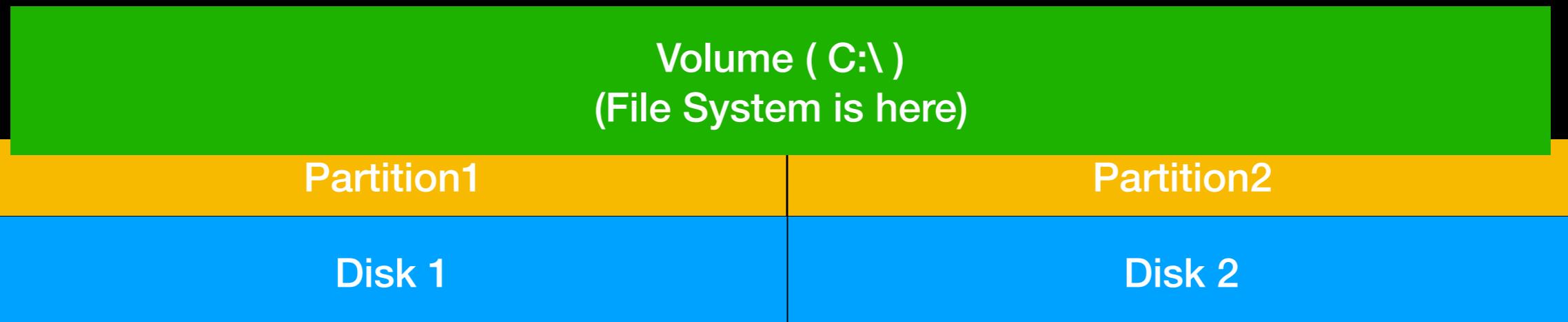


Volume

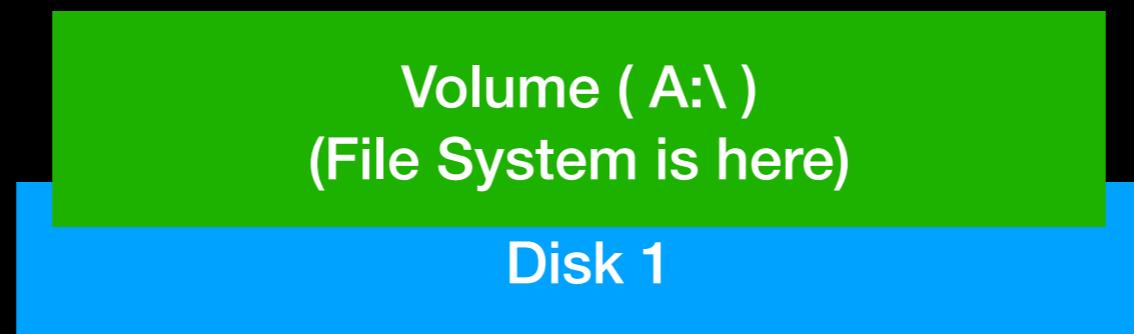
- In computer data storage, a volume or logical drive is a single accessible storage area with a single filesystem, typically **(though not necessarily)** resident on a single partition of a hard disk.

드디어 혼종이 생기기 시작합니다.

예시) RAID



조금 더 특이한 종
예시) Floppy Disk



아 근데 잠만..
RAID 는 어떻게 증거수집 해요?

RAID

제가 아는 방식은 크게 3가지 입니다.

만약 10개의 하드디스크가 묶여있는 10TB의 RAID 일경우

1. 하드 10개를 순서대로 다 이미지 뜨고 들고가서 순서대로
다 꽂은 다음 같은방식으로 RAID 를 올린다.
(매우 귀찮음, 오래걸림)
2. 10TB 혹은 20TB 짜리 하드에 그대로 이미지를 떠버린다
(MBR 영역부터 숨겨진 영역까지 모으기엔 무리)
3. 네트워크 열어서 NAS 에 이미지를 보내버린다
(이게 원본이랑 같다는 걸 어케 보장할꺼임?)

Partition & Volume 를 정리하면

- Partition 은 물리적 저장소를 논리적으로 쪼개는 행위
- Volume 은 접근하여 데이터를 저장하고 빼는 영역
- 보통 1Volume 1Partition 인데,, 혼종은 늘 존재한다.

File System

Definition/Describes

- 파일시스템은 자료를 보관하기 위한 하드웨어 장치를 사용하여 파일의 물리적인 정보를 관리하는 것이다.
- 최근, 네트워크를 통하여 서버상의 파일에 접근하고 관리하는 NFS,SMB 등도 파일시스템에 포함하기도 한다.
- The structure and logic rules used to manage the groups of information and their names is called a “File system”
- In computing, a File-System controls how data is stored or retrieved.

다양한 종류의 파일시스템

FAT
NTFS
HFS
APFS
NNFS
Ext2
Ext3
Ext4
ISO 9660

...

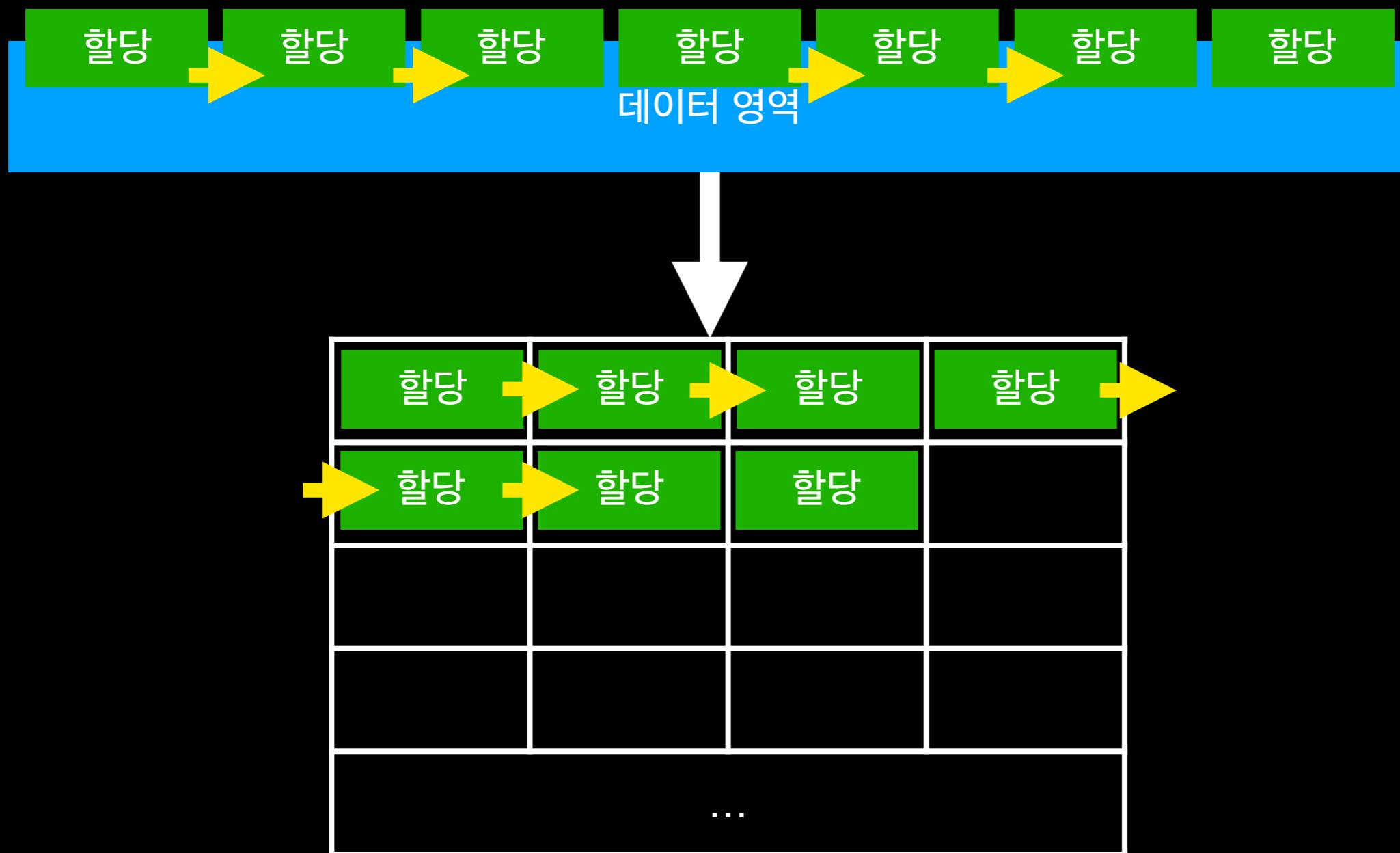
Let's Start FAT

File Allocation Table

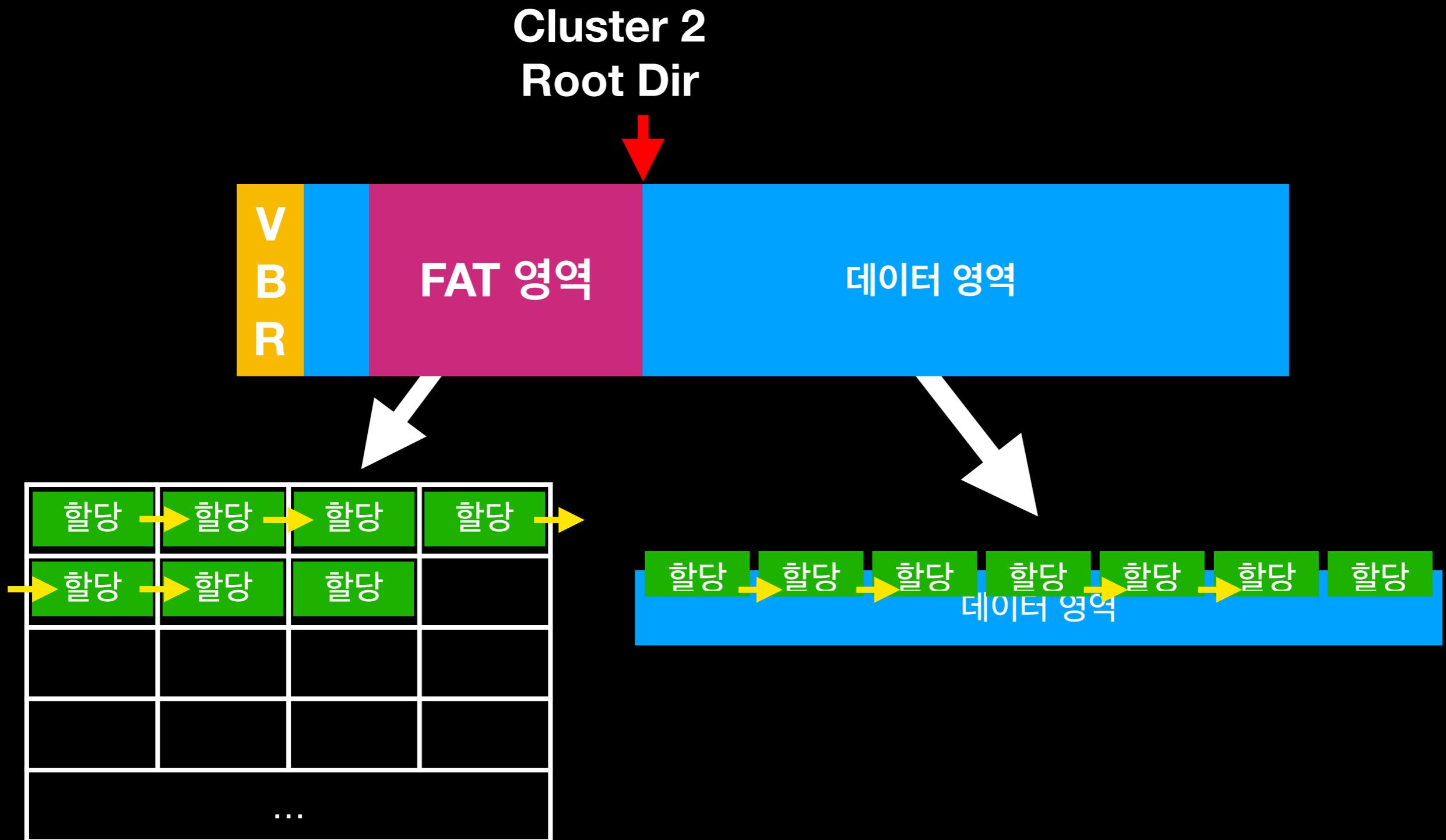
- FAT is a computer file system architecture and a family of industry-standard file systems utilizing it.
- 간단한/보편적인 운영체제에서 볼 수 있는 가장 간단한 파일 시스템 중 하나.

File Allocation Table

파일 할당 표(식탁)?



FAT32 기본구조



Volume Boot Record

해당하는 볼륨의 기초 정보들이 들어있다.

```
uint8_t bootcode[3];
char OEMname[8];
uint16_t bytePerSector;
uint8_t sectorPercluster;
uint16_t sizeOfReservedSec;
uint8_t cntOfFAT;
uint16_t maxFileOfRoot;
uint16_t totalSec2;
uint8_t mediaTyp;
uint16_t cntOfFATSec;
uint16_t secOfTrack;
uint16_t headOnStor;
uint32_t secOfPrePart;
uint32_t totalSec4;
uint32_t secOfFAT;
uint16_t HowToAlloc;
uint8_t minorVersion;
uint8_t majorVersion;
uint32_t OffOfRootClust;
uint16_t OffOfFsinfo;
uint16_t OffOfCopyBootSector;
char reserved[12];
uint8_t driveNum;
uint8_t unused;
uint8_t extendSignature;
uint32_t volSereal;
char vollabel[11];
char sysType[8];
char padding[420];
char signautre[2];
```

Volume Boot Record

주요 정보들?

OEM 이름

1 Sector 당 차지하는 Byte

1 Cluster 당 차지하는 Sector

예약된 영역이 차지하는 Sector

존재하는 FAT 영역 개수

FAT영역 1개당 차지하는 Sector

루트디렉터리의 클러스터 번호

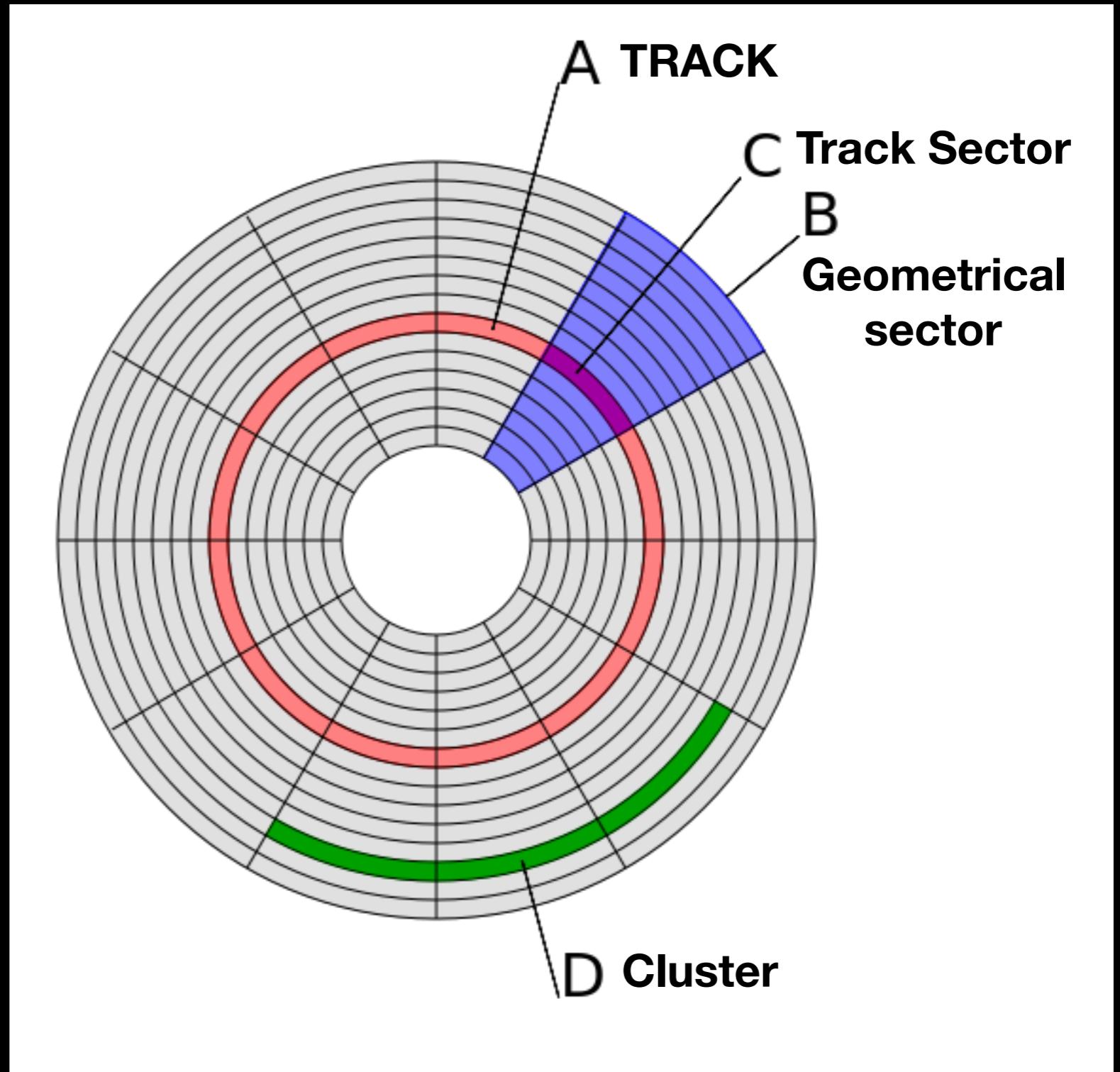
Sector?

- In computer disk storage, a sector is a subdivision of a track on a magnetic disk or optical disc.
- The Sector is the minimum storage unit of a hard drive.
- Operating System typically operate on blocks of data, which may span multiple sectors.

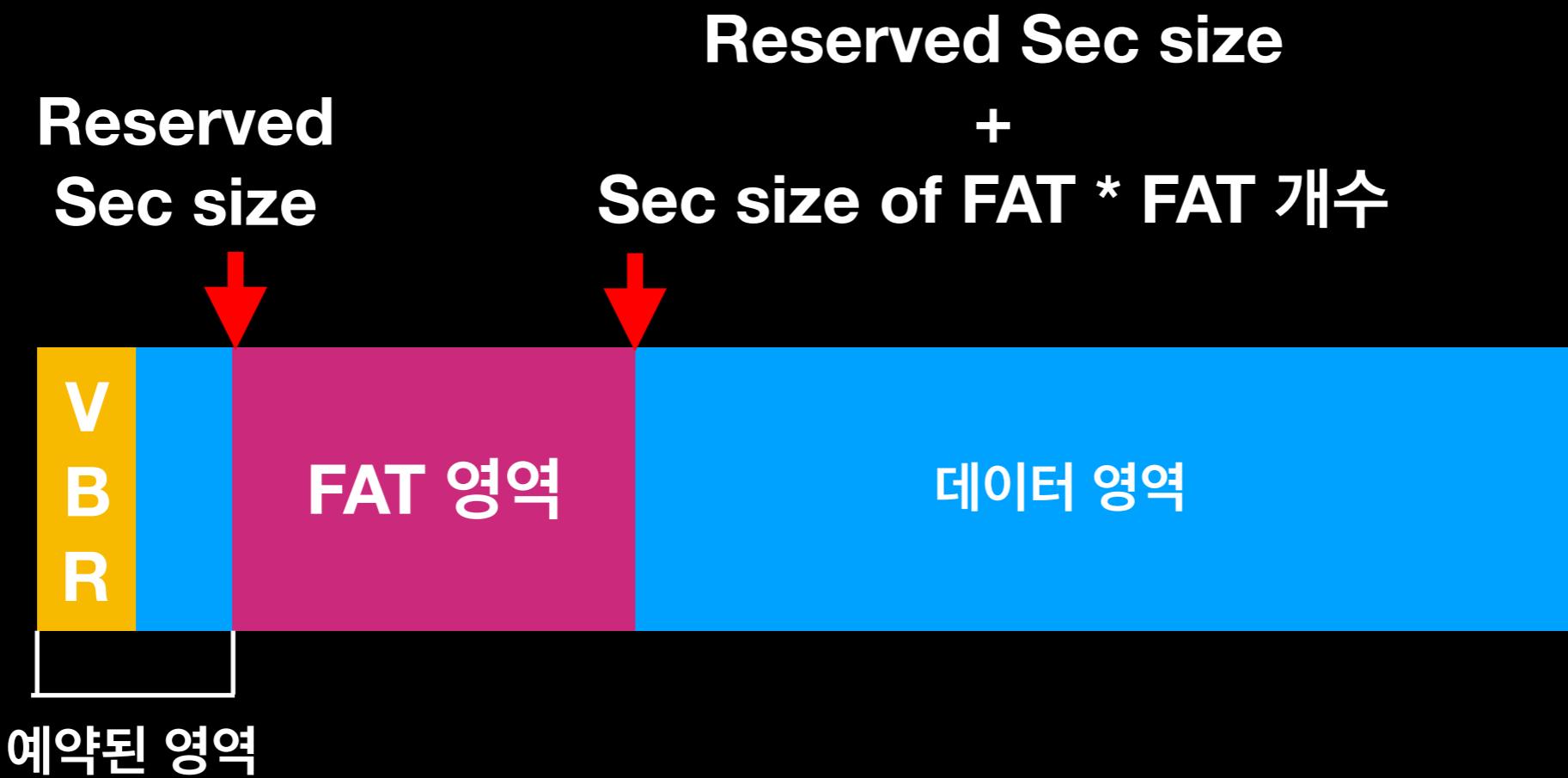
Cluster?

- In computer file systems, a cluster of allocation unit is a unit of disk space allocation for files and directories.
- A cluster is the smallest logical amount of disk space that can be allocated to hold a file.
- The filesystem does not allocate individual disk sectors by default, but contiguous groups of sectors, called clusters

Disk structure



Find offset



FAT

한칸당 4바이트

2	EOF	3	0	4	0	5	0
6	EOF	7	8	8	9	9	EOF
A	EOF		0		0		0
0	0	0	0	0	0	0	0
...							

FAT32 DATA Area

Cluster 2

Volume Name	
Dir 1	0x6
File 1	0x7

Cluster 6

.	0x6
..	0x2
Dir 2	0xA

Cluster 7 ~

Entry

```
char FirstSig;
char filename[10];
uint8_t filetype;
uint8_t reserved;
uint8_t createTime;
uint16_t createTimeD;
uint16_t createDate;
uint16_t accessDate;
uint16_t parentTopClu;
uint16_t modifyTime;
uint16_t modifyDate;
uint16_t parentBotClu;
uint32_t filesize;
```

총 32바이트의 크기의 구조체이다.

심지어 긴이름의 파일을 저장하기 위해
특수한 구조가 또 있는데,,,,

긴이름 Entry

자료형	설명
uint8_t	순서번호(0x40 과 Xor 되어있음.) 비활당일경우 0xe5
char[10]	파일 이름 문자 (unicode)
uint8_t	파일 속성 (0x0f)
uint8_t	?
uint8_t	체크섬
char[12]	파일 이름 문자 (unicode)
uint8_t	?
char[4]	파일 이름 문자 (unicode)

총 32바이트의 크기의 구조체

긴이름 Entry 에
총 13글자가 들어간다.

이 아이들 모으면
더 긴 이름도 가능

FAT32 DATA Area

Cluster 2

Volume Name	
Dir 1	0x6
File 1	0x7

Cluster 6

.	0x6
..	0x2
Dir 2	0xA

Cluster 7 ~

이 파일의 끝을 찾아보려해.MP3



이 파일의 끝을 찾아보려해.MP3

2	EOF	3	0	4	0	5	0
6	EOF	7	8	9	9	9	EOF
A	EOF		0	0	0	0	
0	0	0	0	0	0	0	
			...				

여기서 질문?
클러스터의 남은 부분은
너무 낭비 아닌가?

Let's Go HEX!

아 일단,
제가 따로 어디서 구한 샘플을
기준으로 발표자료가 만들어졌습니다.

VBR

OEM name

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	3E	18	ëX.MSDOS5.0....>.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	A8	0F	00ø...?..ÿ...“..
00000020	00	A0	0F	00	E1	03	00	00	00	00	00	02	00	00	00	00	. . . á.
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	80	00	29	A1	0B	39	C4	4E	4F	20	4E	41	4D	45	20	20	€.) ;. 9ÄNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽŇ&ó
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽÙ‰. ^N.ŠV@^A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»^UI.r..ûU^u.öÁ.
00000080	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	13	73	05	t.pF.ë-ŠV@^I.s.
00000090	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	D1	80	E2	¹ÿÿŠñf.¶E@f.¶Ñeå
000000A0	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	66	F7	E1	?÷â†ÍÀí.Af. ·Éf÷á

FAT32 의 OEM은
보통 MSDOS5.0

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000170	20	20	20	20	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	0D	0A	52	65	Re
000001B0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74	move disks or ot
000001C0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73	her media.ÿ..Dis
000001D0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20	k errorÿ..Press
000001E0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61	any key to resta
000001F0	72	74	0D	0A	00	00	00	00	AC	CB	D8	00	00	55	AA	rt.....→ÈØ..U^	

VBR

1sector 당 바이트 수 (512)

VBR

1cluster 당 sector 수 (8sectors == 1cluster)

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	3E	18	ëX.MSDOS5.0...>.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	A8	0F	00ø...?..ý...“..
00000020	00	A0	0F	00	E1	03	00	00	00	00	00	00	02	00	00	00	. . . á.
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	80	00	29	A1	0B	39	C4	4E	4F	20	4E	41	4D	45	20	20	€.) ï. 9ÄNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽŇ&ó
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽÙ‰. ^N. ŠV@^A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»^UI.r..ûU^u.öÁ.
00000080	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	13	73	05	t.pF.ë-ŠV@^Í.s.
00000090	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	D1	80	E2	ÿyŠñf.¶E@f.¶Ñeâ
000000A0	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	66	F7	E1	?÷å†ÍÀí.Af. ·Éf÷á

그럼 1클러스터당 바이트 수는
 $8 * 512 == 4096$ Byte

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000170	20	20	20	20	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	0D	0A	52	65Re
000001B0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74	move disks or ot
000001C0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73	her media.ý..Dis
000001D0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20	k errorý..Press
000001E0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61	any key to resta
000001F0	72	74	0D	0A	00	00	00	00	AC	CB	D8	00	00	55	AA	rt.....¬ÉØ..U^	

VBR

예약된 영역의 cluster 수(6206)

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	3E	18	ëX.MSDOS5.0...>.
000000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	A8	0F	00ø..?..ý..`..
000000020	00	A0	0F	00	E1	03	00	00	00	00	00	02	00	00	00	00	. . . á
000000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
000000040	80	00	29	A1	0B	39	C4	4E	4F	20	4E	41	4D	45	20	20	€.) ¡. 9ÄNO NAME
000000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽŇčô
000000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽÙ‰. ^N.ŠV@'A
000000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»^UÍ.r..úU^u.öÁ.
000000080	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	13	73	05	t.þF.ě-ŠV@'.í.s.
000000090	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	D1	80	E2	^ýyŠñf.þE@f.þNéá
0000000A0	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	66	F7	E1	?÷åtíÀi.Af.-Éf÷á
0000000B0	66	89	46	F8	83	7E	16	00	75	38	83	7E	2A	00	77	32	f‰Føf~..u8f~*.w2
0000000C0	66	8B	46	1C	66	83	C0	0C	BB	00	80	B9	01	00	E8	2B	f«F.ffÀ».€¹..è+
0000000D0	00	E9	2C	03	A0	FA	7D	B4	7D	8B	F0	AC	84	C0	74	17	.é,. ú} ` } <ð„„Àt.
0000000E0	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB	EE	A0	FB	7D	<ýt.`..»..í.ëi ú}
0000000F0	EB	E5	A0	F9	7D	EB	E0	98	CD	16	CD	19	66	60	80	7E	ëå ú}ëà~í.í.f`€~
000000100	02	00	0F	84	20	00	66	6A	00	66	50	06	53	66	68	10fj.fP.Sfh.
000000110	00	01	00	B4	42	8A	56	40	8B	F4	CD	13	66	58	66	58	...`BŠV@`óí.fXfx
000000120	66	58	66	58	EB	33	66	3B	46	F8	72	03	F9	EB	2A	66	fXfxé3f; Før.ùë*f
000000130	33	D2	66	0F	B7	4E	18	66	F7	F1	FE	C2	8A	CA	66	8B	3òf. ·N.f÷ñpÅŠEf<
000000140	D0	66	C1	EA	10	F7	76	1A	86	D6	8A	56	40	8A	E8	C0	ĐfÁê.÷v.tÖŠV@ŠèÀ
000000150	E4	06	0A	CC	B8	01	02	CD	13	66	61	0F	82	75	FF	81	ä...ì...í.fa.,uý.
000000160	C3	00	02	66	40	49	75	94	C3	42	4F	4F	54	4D	47	52	Ä..f@Iu"ÄBOOTMGR
000000170	20	20	20	20	00	00	00	00	00	00	00	00	00	00	00	00
000000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	0D	0A	52	65 Re	
000001B0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74	move disks or ot
000001C0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73	her media.ý..Dis
000001D0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20	k errorý..Press
000001E0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61	any key to resta
000001F0	72	74	0D	0A	00	00	00	00	00	AC	CB	D8	00	00	55	AA	rt.....-ÉØ..U^

Find offset

**Reserved
Sec size**



V
B
R

FAT 영역

데이터 영역

예약된 영역은 6206 개의 sector로 이뤄져 있으니
 $6206 * 512$
총 3,177,472 Byte 이고
FAT영역 시작지점의 offset 은 당연히 3177472 이 된다.

FAT영역

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00307C00	F8	FF	FF	0F	FF	ÿÿ.ÿÿÿÿÿÿ.ÿÿÿ.											
00307C10	FF	FF	FF	0F	06	00	00	00	07	00	00	00	08	00	00	00	ÿÿÿ.....
00307C20	09	00	00	00	0A	00	00	00	0B	00	00	00	0C	00	00	00
00307C30	0D	00	00	00	0E	00	00	00	0F	00	00	00	10	00	00	00
00307C40	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00
00307C50	15	00	00	00	16	00	00	00	17	00	00	00	18	00	00	00
00307C60	19	00	00	00	1A	00	00	00	1B	00	00	00	1C	00	00	00
00307C70	1D	00	00	00	1E	00	00	00	1F	00	00	00	20	00	00	00
00307C80	21	00	00	00	22	00	00	00	23	00	00	00	24	00	00	00	!...".#.\$...
00307C90	25	00	00	00	26	00	00	00	27	00	00	00	28	00	00	00	%...&.'...(
00307CA0	29	00	00	00	2A	00	00	00	2B	00	00	00	2C	00	00	00)...*...+...,...
00307CB0	2D	00	00	00	2E	00	00	00	2F	00	00	00	30	00	00	00	-...../..0...
00307CC0	31	00	00	00	32	00	00	00	33	00	00	00	34	00	00	00	1...2...3...4...

VBR

존재하는 FAT 수

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	3E	18	ëX.MSDOS5.0....>.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	A8	0F	00ø...?..ÿ...“..
00000020	00	A0	0F	00	E1	03	00	00	00	00	00	00	02	00	00	00	. . . á.....
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	80	00	29	A1	0B	39	C4	4E	4F	20	4E	41	4D	45	20	20	€.) ï. 9ÄNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽŇ&ô
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽÙ‰. ^N.ŠV@`A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»^UI.r..ûU^u.öÁ.
00000080	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	13	73	05	t.pF.ë-ŠV@`í.s.
00000090	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	D1	80	E2	¹ÿyŠñf.¶E@f.¶Néá
000000A0	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	66	F7	E1	?÷å†ÍÀí.Af. ·Éf÷á
000000B0	66	89	46	F8	83	7E	16	00	75	38	83	7E	2A	00	77	32	f‰Føf~..u8f~*.w2
000000C0	66	8B	46	1C	66	83	C0	0C	BB	00	80	B9	01	00	E8	2B	f< F. ffÀ.»..€¹..è+
000000D0	00	E9	2C	03	A0	FA	7D	B4	7D	8B	F0	AC	84	C0	74	17	.é.,. ú} `} < ð„„Àt.
000000E0	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB	EE	A0	FB	7D	<ÿt. `..»..í.ëí û}
000000F0	EB	E5	A0	F9	7D	EB	E0	98	CD	16	CD	19	66	60	80	7E	ëå û}ëà~í.í.f`€~
00000100	02	00	0F	84	20	00	66	6A	00	66	50	06	53	66	68	10fj.fP.Sfh.
00000110	00	01	00	B4	42	8A	56	40	8B	F4	CD	13	66	58	66	58	...`BŠV@`óí.fXfx
00000120	66	58	66	58	EB	33	66	3B	46	F8	72	03	F9	EB	2A	66	fXfxë3f;Før.ùë*f
00000130	33	D2	66	0F	B7	4E	18	66	F7	F1	FE	C2	8A	CA	66	8B	3òf. ·N.f÷ñþÅŠÉf<
00000140	D0	66	C1	EA	10	F7	76	1A	86	D6	8A	56	40	8A	E8	C0	ĐfÀè.·v. tÖŠV@ŠéÀ
00000150	E4	06	0A	CC	B8	01	02	CD	13	66	61	0F	82	75	FF	81	ä..í...í.fa.,uÿ.
00000160	C3	00	02	66	40	49	75	94	C3	42	4F	4F	54	4D	47	52	Ã..f@Iu"ÅBOOTMGR
00000170	20	20	20	20	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	0D	0A	52	65	Re
000001B0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74	move disks or ot
000001C0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73	her media.ÿ..Dis
000001D0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20	k errorÿ..Press
000001E0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61	any key to resta
000001F0	72	74	0D	0A	00	00	00	00	00	AC	CB	D8	00	00	55	AA	rt.....¬ÈØ..U^

VBR

1개의 FAT 당 sector 수(993)

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	3E	18	ëX.MSDOS5.0....>.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	A8	0F	00ø...?..ÿ...^..
00000020	00	A0	0F	00	E1	03	00	00	00	00	00	00	02	00	00	00	. . . á
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	80	00	29	A1	0B	39	C4	4E	4F	20	4E	41	4D	45	20	20	€.) j. 9ÄNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽŇ&ô
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽÙ‰. ^N.ŠV@`A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»²UIÍ.r..ûU²u.öÁ.
00000080	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	13	73	05	t.pF.ë-ŠV@`í.s.
00000090	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	D1	80	E2	¹ÿyŠñf.¶E@f.¶Néå
000000A0	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	66	F7	E1	?÷â†ÍÀí.Af. ·Éf÷á

두개의 FAT가 존재했고, 1개의 FAT당 가지는 sector 수는 993개, FAT는 2개다
 $993 * 512 * 2$

1,016,832 Byte

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000170	20	20	20	20	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	0D	0A	52	65Re
000001B0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74	move disks or ot
000001C0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73	her media.ÿ..Dis
000001D0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20	k errorÿ..Press
000001E0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61	any key to resta
000001F0	72	74	0D	0A	00	00	00	00	AC	CB	D8	00	00	55	AA	rt.....¬ÉØ..U²	

Find offset

$$3177472 + 1016832 = 4,194,304$$



VBR

Root cluster number

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	3E	18	ëX.MSDOS5.0....>.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	A8	0F	00ø...?..ý...^..
00000020	00	A0	0F	00	E1	03	00	00	00	00	00	00	02	00	00	00á.....
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	80	00	29	A1	0B	39	C4	4E	4F	20	4E	41	4D	45	20	20	€.)í.9ÄNO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽŇ&O
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41	{ŽÁŽÙ‰. ^N.ŠV@`A
00000070	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	F6	C1	01	»*UI.r..ûU <u>.öÁ.</u>
00000080	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	13	73	05	t.pF.ë-ŠV@`í.s.
00000090	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	D1	80	E2	¹ÿyŠñf.¶E@f.¶Néå
000000A0	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	66	F7	E1	?÷å†ÍÀí.Af.·Éf÷á
000000B0	66	89	46	F8	83	7E	16	00	75	38	83	7E	2A	00	77	32	f‰Føf~..u8f~*.w2
000000C0	66	8B	46	1C	66	83	C0	0C	BB	00	80	B9	01	00	E8	2B	f< F.ffff.»..€¹..è+
000000D0	00	E9	2C	03	A0	FA	7D	B4	7D	8B	F0	AC	84	C0	74	17	.é,. ú} `} < ð„„Àt.
000000E0	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB	EE	A0	FB	7D	<ÿt. `..í.ëí ú}
000000F0	EB	E5	A0	F9	7D	EB	E0	98	CD	16	CD	19	66	60	80	7E	ëå ú}ëà~í.í.f`€~
00000100	02	00	0F	84	20	00	66	6A	00	66	50	06	53	66	68	10fj.fP.Sfh.
00000110	00	01	00	B4	42	8A	56	40	8B	F4	CD	13	66	58	66	58	...`BŠV@`óí.fXfx
00000120	66	58	66	58	EB	33	66	3B	46	F8	72	03	F9	EB	2A	66	fXfxë3f;Før.ùë*f
00000130	33	D2	66	0F	B7	4E	18	66	F7	F1	FE	C2	8A	CA	66	8B	3òf.·N.f÷ñþÅŠEf<
00000140	D0	66	C1	EA	10	F7	76	1A	86	D6	8A	56	40	8A	E8	C0	ĐfÅè.÷v.tÖŠV@ŠeÅ
00000150	E4	06	0A	CC	B8	01	02	CD	13	66	61	0F	82	75	FF	81	ä..í...í.fa.,uý.
00000160	C3	00	02	66	40	49	75	94	C3	42	4F	4F	54	4D	47	52	Ã..f@Iu"ÅBOOTMGR
00000170	20	20	20	20	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	0D	0A	52	65	Re
000001B0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74	move disks or ot
000001C0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73	her media.ý..Dis
000001D0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20	k errorý..Press
000001E0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61	any key to resta
000001F0	72	74	0D	0A	00	00	00	00	00	AC	CB	D8	00	00	55	AA	rt.....→ÈØ..U²

Find offset

대부분 여기가 클러스터 2번



Root Cluster

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00400000	4E	45	57	20	56	4F	4C	55	4D	45	20	08	00	00	00	00	NEW VOLUME
00400010	00	00	00	00	00	00	02	0C	36	3E	00	00	00	00	00	006>.....
00400020	24	52	45	43	59	43	4C	45	42	49	4E	16	00	13	A7	0C	\$RECYCLEBIN...\$.
00400030	36	3E	36	3E	00	00	A8	0C	36	3E	03	00	00	00	00	00	6>6>..".6>.....
00400040	44	53	43	5F	31	33	32	30	4A	50	47	20	00	42	B0	0C	DSC_1320JPG .B°.
00400050	36	3E	36	3E	00	00	F5	A4	2E	3B	05	00	11	0D	07	00	6>6>..õ¤.;.....
00400060	44	53	43	5F	31	33	34	35	4A	50	47	20	00	45	B0	0C	DSC_1345JPG .E°.
00400070	36	3E	36	3E	00	00	09	A9	2E	3B	76	00	CB	F9	06	00	6>6>...©.;v.Ëù..
00400080	44	53	43	5F	31	32	37	39	4A	50	47	20	00	6B	B0	0C	DSC_1279JPG .k°.
00400090	36	3E	36	3E	00	00	79	7C	2E	3B	E6	00	F3	F7	08	00	6>6>..y .;æ.ó÷..
004000A0	44	53	43	5F	31	32	37	30	4A	50	47	20	00	6F	B0	0C	DSC_1270JPG .o°.
004000B0	36	3E	36	3E	00	00	6B	7A	2E	3B	76	01	96	A0	04	00	6>6>..kz.;v.- ..
004000C0	44	53	43	5F	31	32	38	34	4A	50	47	20	00	71	B0	0C	DSC_1284JPG .q°.
004000D0	36	3E	36	3E	00	00	8F	7C	2E	3B	C1	01	9E	46	06	00	6>6>... .;Á.žF..
004000E0	44	53	43	5F	31	32	38	31	4A	50	47	20	00	75	B0	0C	DSC_1281JPG .u°.
004000F0	36	3E	36	3E	00	00	85	7C	2E	3B	26	02	6E	67	06	00	6>6>.... .;&.ng..
00400100	44	53	43	5F	31	33	32	36	4A	50	47	20	00	7A	B0	0C	DSC_1326JPG .z°.
00400110	36	3E	36	3E	00	00	A8	A8	2E	3B	8D	02	11	29	07	00	6>6>.."".;....)
00400120	E5	4D	00	53	00	49	00	65	00	36	00	0F	00	83	37	00	åM.S.I.e.6....f7.
00400130	32	00	32	00	2E	00	74	00	6D	00	00	00	70	00	00	00	2.2....t.m....p...
00400140	E5	53	49	45	36	37	32	32	54	4D	50	10	00	B2	55	14	åSIE6722TMP...“U.
00400150	36	3E	36	3E	00	00	56	14	36	3E	00	03	00	10	00	00	6>6>..V.6>.....

파일 복구

내가 파일을 지웠는데?
그게 남아있다고???
어떻게 남아있는거지?

그냥 지우면...

00400120	E5 4D 00 53 00 49 00 65 00 36 00 0F 00 83 37 00	åM.S.I.e.6...f7.
00400130	32 00 32 00 2E 00 74 00 6D 00 00 00 70 00 00 00	2.2...t.m...p...
00400140	E5 53 49 45 36 37 32 32 54 4D 50 10 00 B2 55 14	åSIE6722TMP..^U.
00400150	36 3E 36 3E 00 00 56 14 36 3E 00 03 00 10 00 00	6>6>..V.6>.....

E5로 첫 시그니처가 생긴다.

이를 이용해서 지워진 데이터의 클러스터를 알아내고 해당 클러스터를 복구해 내면 된다.

해당 클러스터 영역에 파일 데이터가 그대로 남아 있기도 하지만, 해당 클러스터가 다른 파일로 할당 되면,,, 복구 못한다.

물론, 이때 FAT에는 0으로 덮어씌워진다.

엔트리가 없거나
덮어씌워 진 경우라면??

캬빙? Car 冰?



사진출처 :

[https://m.blog.naver.com/PostView.nhn?
blogId=cskuh&logNo=220923158105&categoryNo=67](https://m.blog.naver.com/PostView.nhn?blogId=cskuh&logNo=220923158105&categoryNo=67)

카빙 Carving

비 할당 영역을 복구합니다.

비 할당 영역

파일이 할당 되지 않은 영역!
파일이 지워지거나 하면 FAT 에는 0이다.

EOF	0	0	0
EOF	8	9	EOF
EOF	0	0	13
FAT 에 0으로 덮어씌워졌다고 해도,,, 해당 클러스터에 가보면, 데이터가 그대로 남아있는 경우가 많습니다.			

질문 !

파일의 시작과 끝을 어떻게 찾아요?



답은 파일 시그니처!

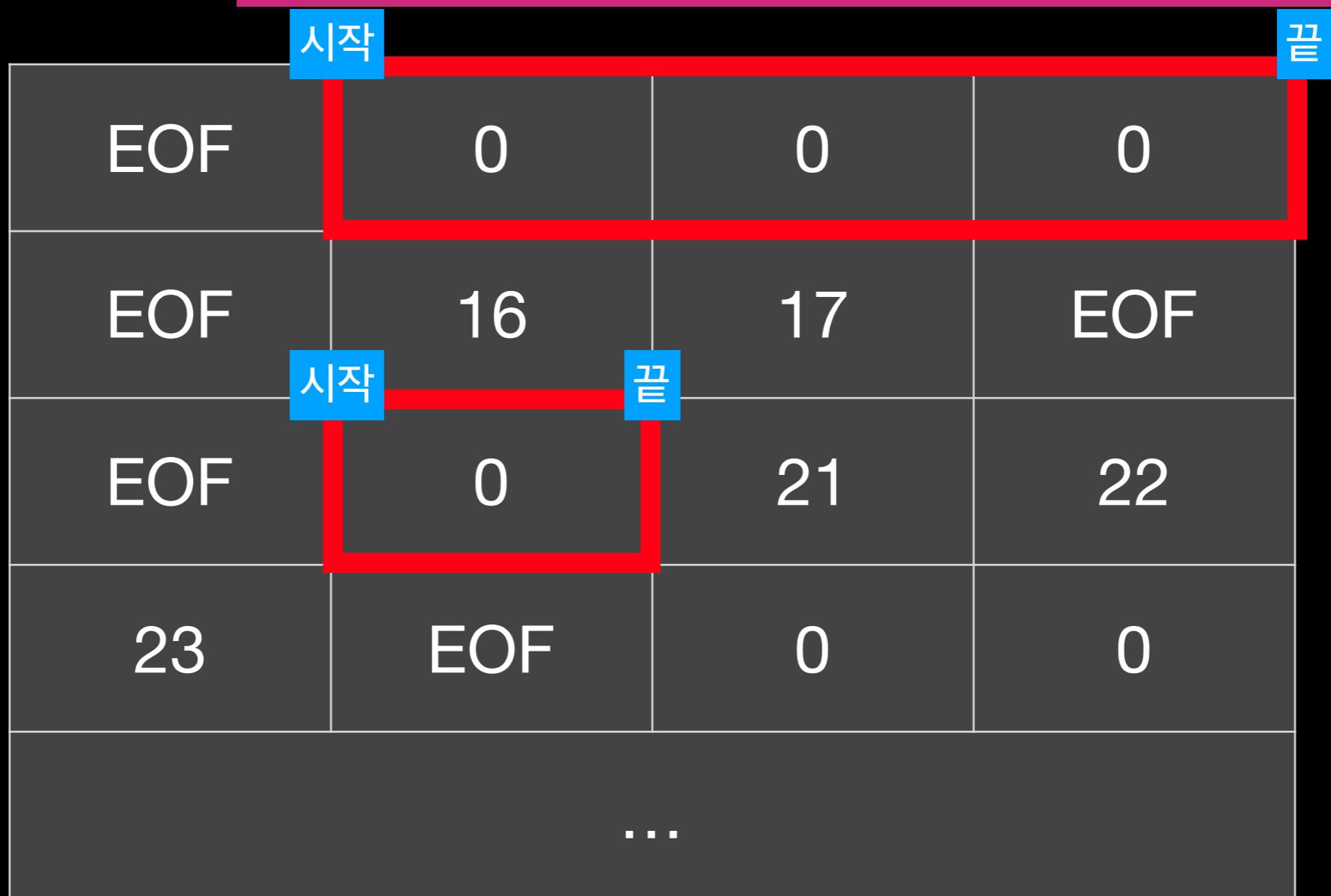
대부분 파일의 시작부분에는 파일 시그니처가 존재합니다.

확장자	시그니처
JPG	FF D8
PNG	89 50 4E 47
EXE (MS PE structure)	4D 5A
압축파일 (ZIP 등)	50 4B

질문 !

그럼 끝을 어떻게 찾아요?

끝을 정의 할 필요가 없는 경우가 많음.



질문 !

그럼 끝을 어떻게 찾아요?

중간에 푸터가 있다.
그럼 파일을 복구하고 읽어들일때
의미없는 데이터는 대부분 무시됩니다.

질문 !

그럼 끝을 어떻게 찾아요?

시그니처 데이터데이터데이터데이터

데이터데이터데이터데이터데이터

이터데이터데이터데이터데이터

터데이터데이터데이터데이터



|터가 잘렸을 경우.

, 잘린부분의 데이터는 못살리나
경우 시그니처와 상단부분 데이터만
있는 경우가 있습니다.

질문!

그럼 끌을 어떻게 찾아요?

중간에 데이터가 바뀌면???
답이 없을 수도 있으나
가끔씩 의외로 이런 경우도 생긴다고 합니다.



질문 !

그럼 끝을 어떻게 찾아요?

중간에 데이터가 바뀌면???
사실 이럴 일은 자주 발생하지는 않습니다.

카빙 Carving

신기하쥬?

잡담
(코드리뷰)

FAT Tool

영상으로 대체하겠습니다.

끝!
≡

Reference (en)

- https://en.wikipedia.org/wiki/Disk_partitioning
- [https://en.wikipedia.org/wiki/Volume_\(computing\)](https://en.wikipedia.org/wiki/Volume_(computing))
- https://en.wikipedia.org/wiki/File_system
- https://en.wikipedia.org/wiki/File_Allocation_Table
- https://en.wikipedia.org/wiki/Disk_sector
- https://en.wikipedia.org/wiki/Data_cluster

Reference (ko)

- https://ko.wikipedia.org/wiki/디스크_파티션
- [https://ko.wikipedia.org/wiki/볼륨_\(컴퓨팅\)](https://ko.wikipedia.org/wiki/볼륨_(컴퓨팅))
- https://ko.wikipedia.org/wiki/파일_시스템
- https://ko.wikipedia.org/wiki/파일_할당_테이블
- <http://jwmsg.kr/main/2018/09/21/fat32-분석기-1/>

Reference (Book)

- 파일시스템 포렌식 분석 (FILE SYSTEM FORENSIC ANALYSIS) - 브라이언 캐리어 지음, 주필환 옮김

jwmsg.kr

Q & A

진짜 끝!

감사합니다!