forensic-proof.com

FAT12/16/32 File System

Twitter : @pr0neer

Blog : forensic-proof.com

Email : proneer@gmail.com

Kim Jinkook

Outline

1. FAT12/16/32

- ✓ Introduction
- ✓ Internals
- ✓ Directory Structure
- ✓ Example

FAT12/16/32 Introduction

Security is a people problem…

FAT12/16/32 Introduction

FAT (File Allocation Table)

- MS-DOS 시절부터 사용
- 간단한 구조로 메모리카드, 디지털카메라, 플래시메모리 등에 널리 사용
- FAT12, FAT16, FAT32, (exFAT)
  - FAT 뒤의 숫자는 표현 가능한 최대 클러스터 수
  - 000h, 001h, FF6h~FF로 는 예약된 값 (12개)

FAT 형식	최대 표현 가능한 클러스터 수
FAT12	4,084 (2^{12} - 12)
FAT16	65,524 (2^{16} - 12)
FAT32	268,435,444 (2^{28} - 12)

FAT 형식에 따른 최대 표현 가능한 클러스터 수

볼륨 크기	클러스터 크기
32MB – 8GB	4 KB
8GB – 16GB	8 KB
16GB – 32GB	16 KB
32GB -	32 KB

FAT32에서 볼륨 크기에 따른 클러스터 크기

FAT12/16/32 Introduction

FAT (File Allocation Table)

- **FAT32 용량 제한 (268,435,444 클러스터)**
  - 4 KB의 경우 1 TB 까지 표현
  - 32 KB의 경우 8 TB 까지 표현 ➔ MBR 구조의 제한으로 2 TB 까지만 표현 가능

- **exFAT (extended FAT)**
  - 윈도우 Embedded CE 6.0 부터 사용 (Vista 이상은 기본 지원, XP는 패치 설치)
  - 클러스터 표현 비트를 64 비트로 확장
  - 비트맵 사용
  - TFAT 지원
  - UTC (Universal Time, Coordinated) 지원 ➔ 시간 정밀도 10 ms (NTFS : 100 ns)

FAT12/16/32 Internals

Security is a people problem…

FAT12/16/32 Internals

Structure

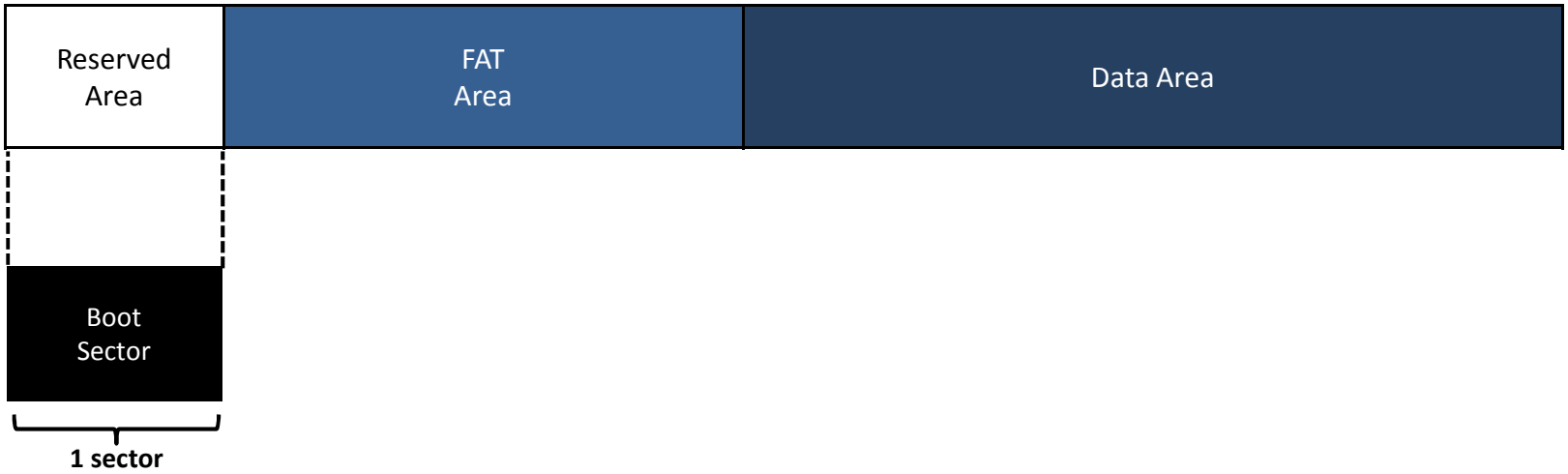
- 예약된 영역, FAT 영역, 데이터 영역

FAT 형식	예약된 영역 크기 (섹터)
FAT12	1
FAT16	1
FAT32	32

FAT 형식에 따른 예약된 영역의 섹터 수

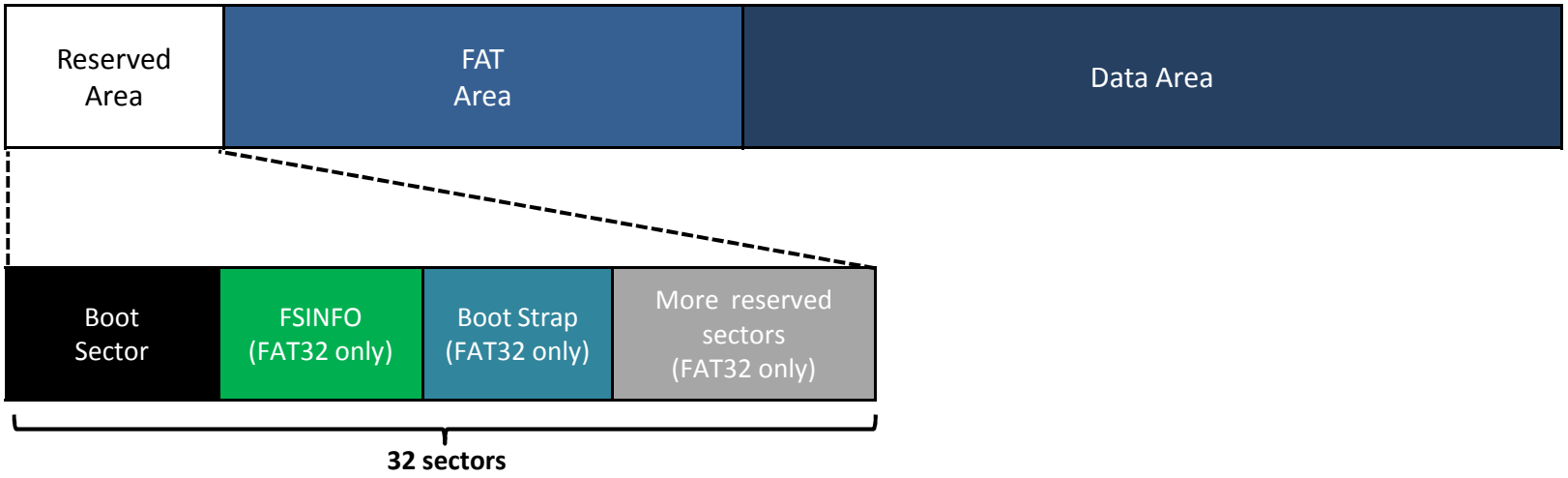
FAT12/16/32 Internals

Reserved Area (FAT12/16)



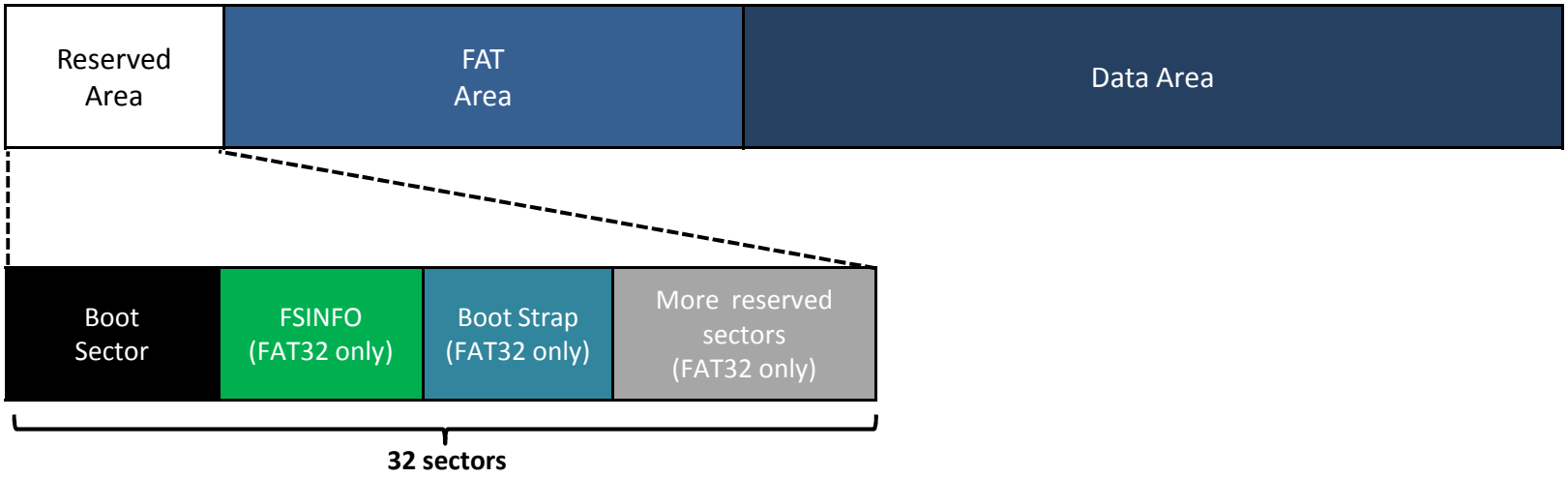
FAT12/16/32 Internals

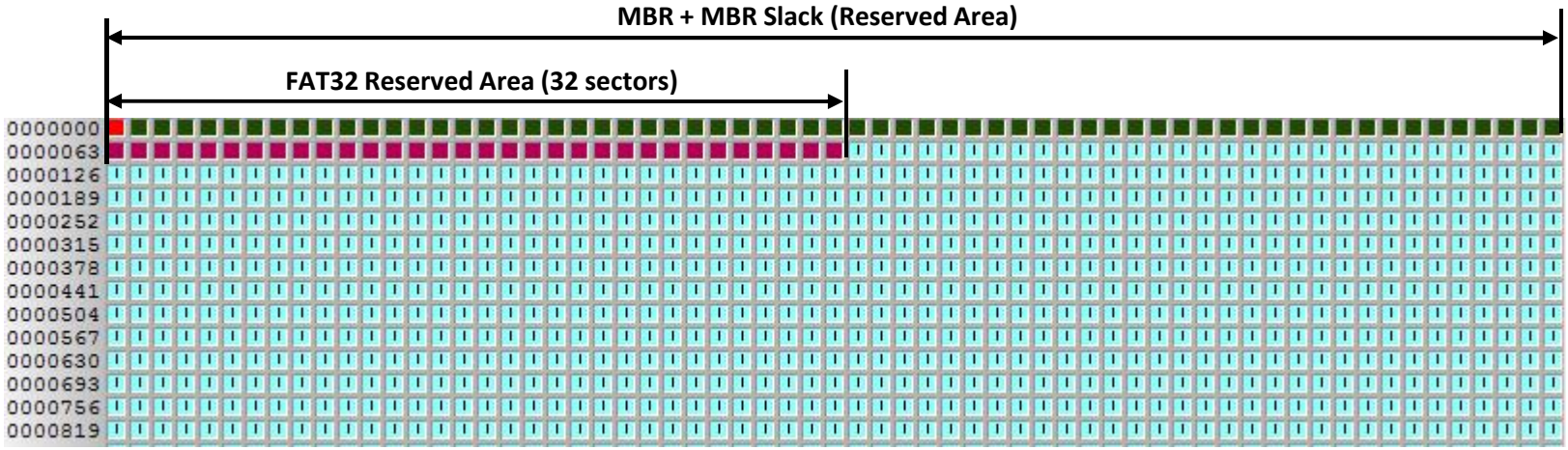
Reserved Area (FAT32)



FAT12/16/32 Internals

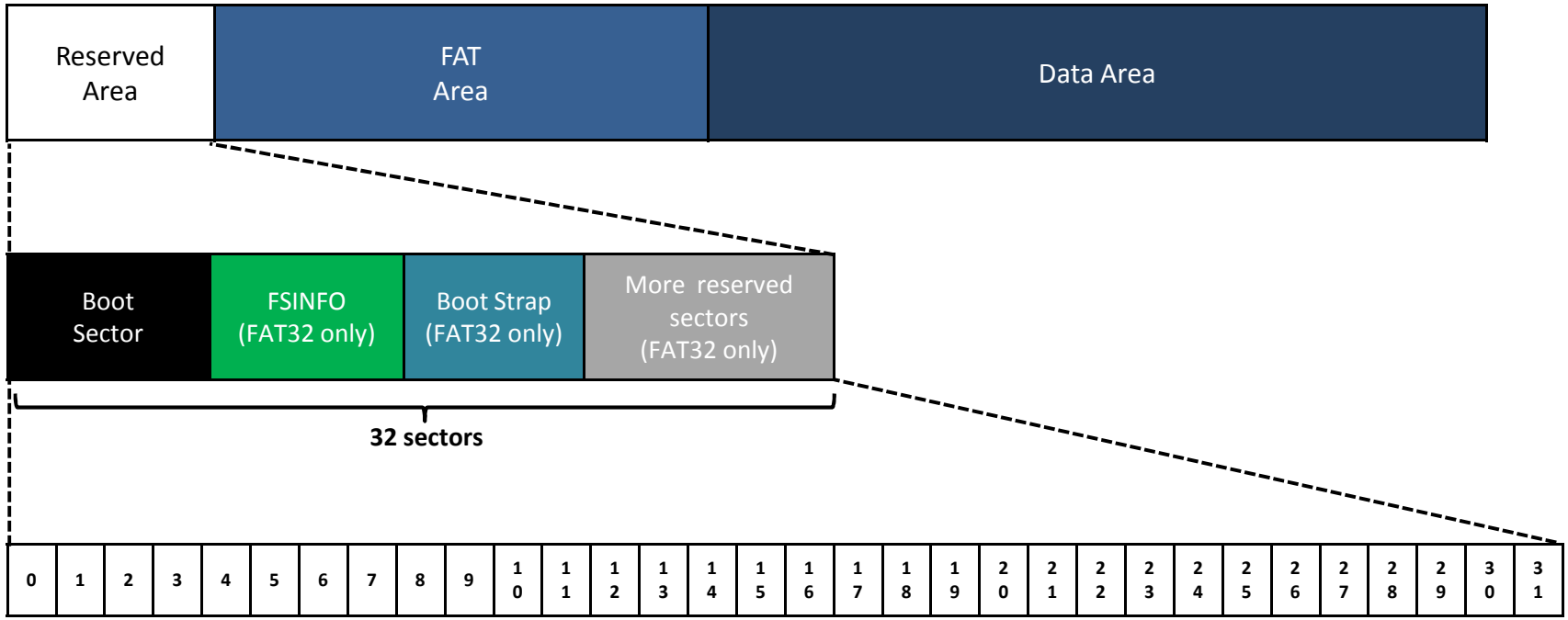
Reserved Area (FAT32)





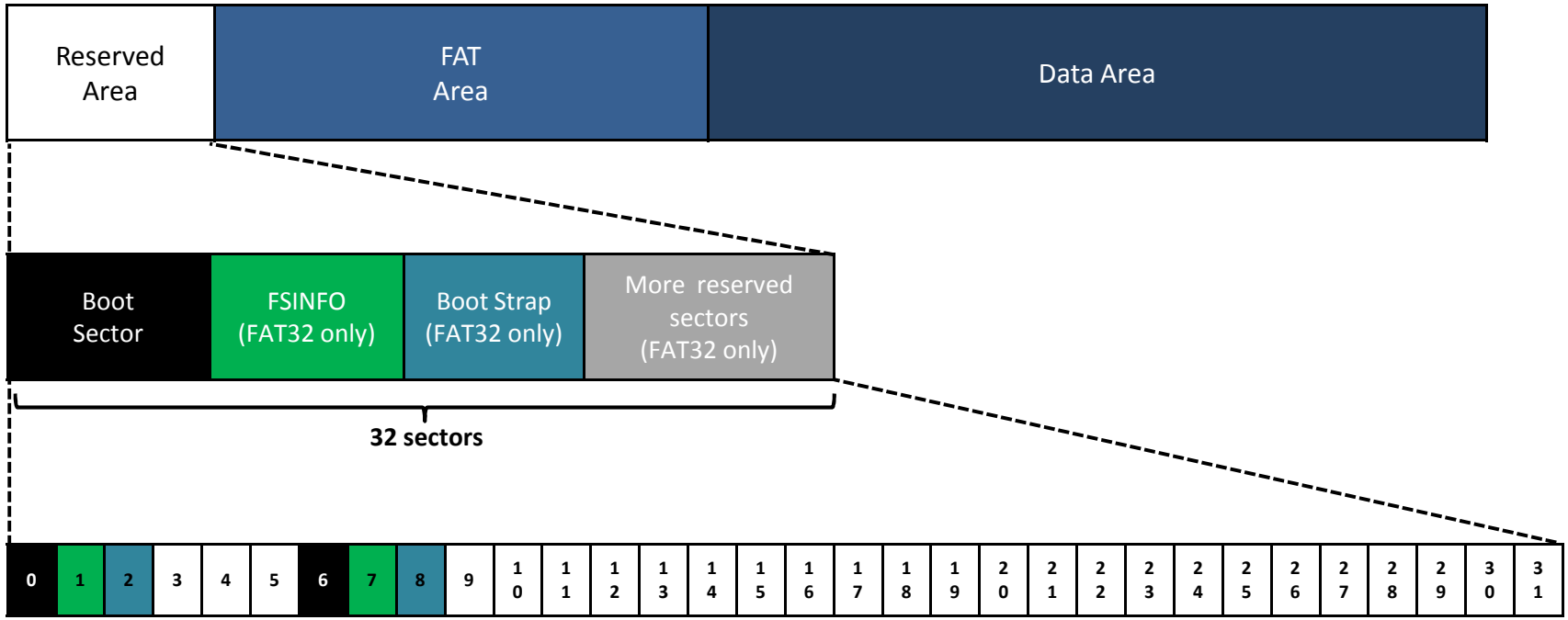
FAT12/16/32 Internals

Reserved Area (FAT32)



FAT12/16/32 Internals

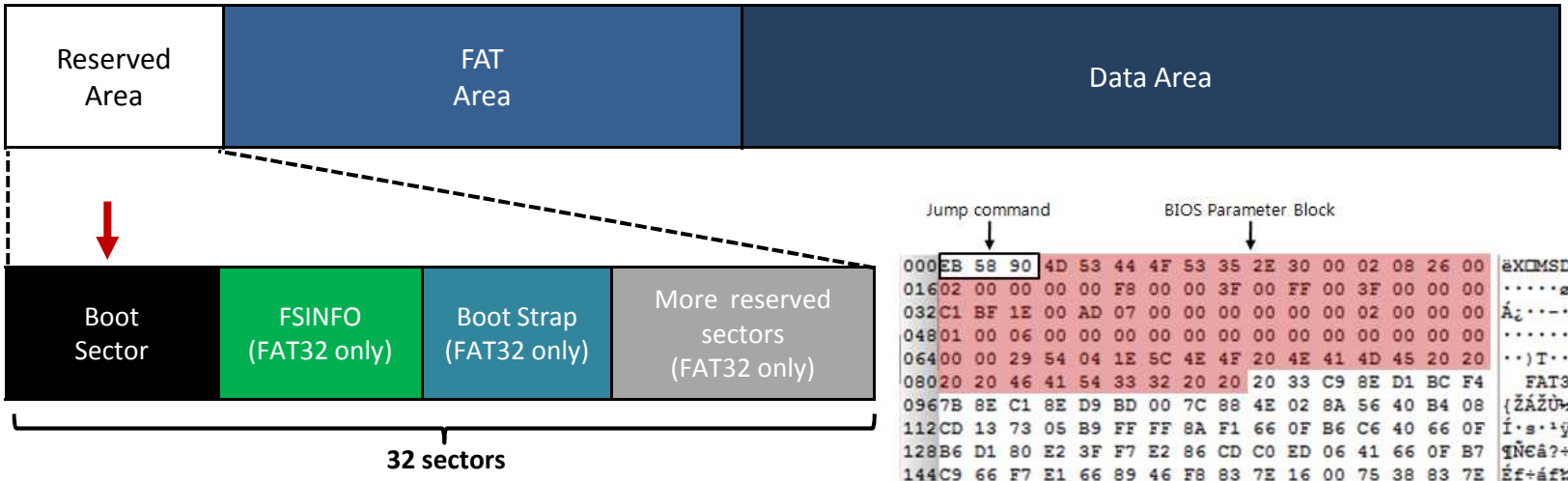
Reserved Area (FAT32)



- **0, 6 번 섹터** : 볼륨 부트 섹터 (Volume Boot Sector)
- **1, 7 번 섹터** : File System Information (FSINFO) 구조체
- **2, 8 번 섹터** : 부트스트랩 코드 (Boot Strap Code)

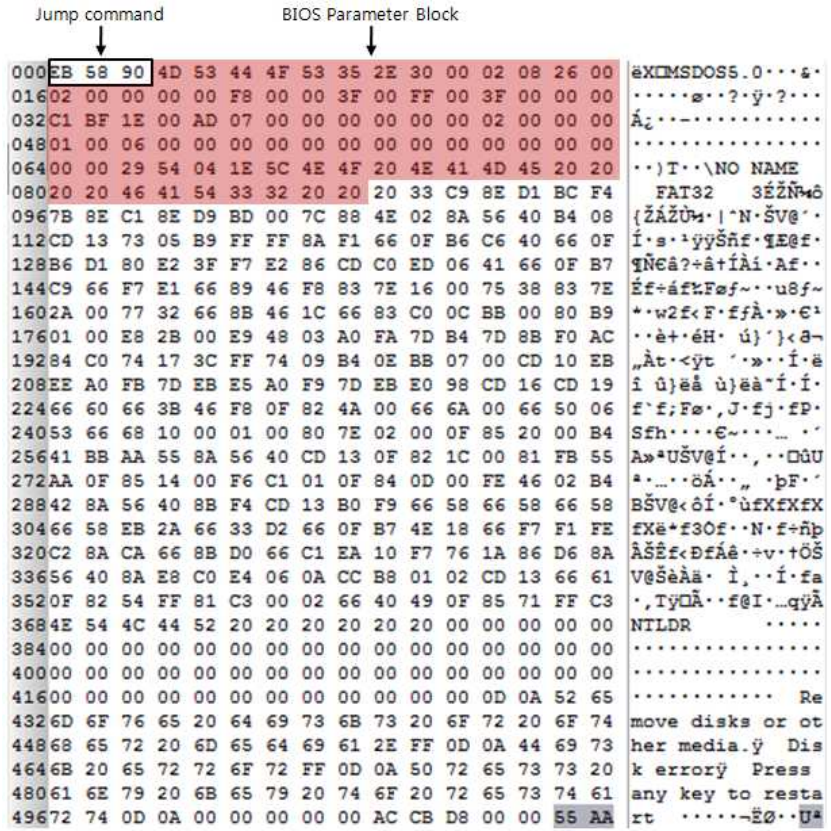
FAT12/16/32 Internals

Reserved Area (FAT32)



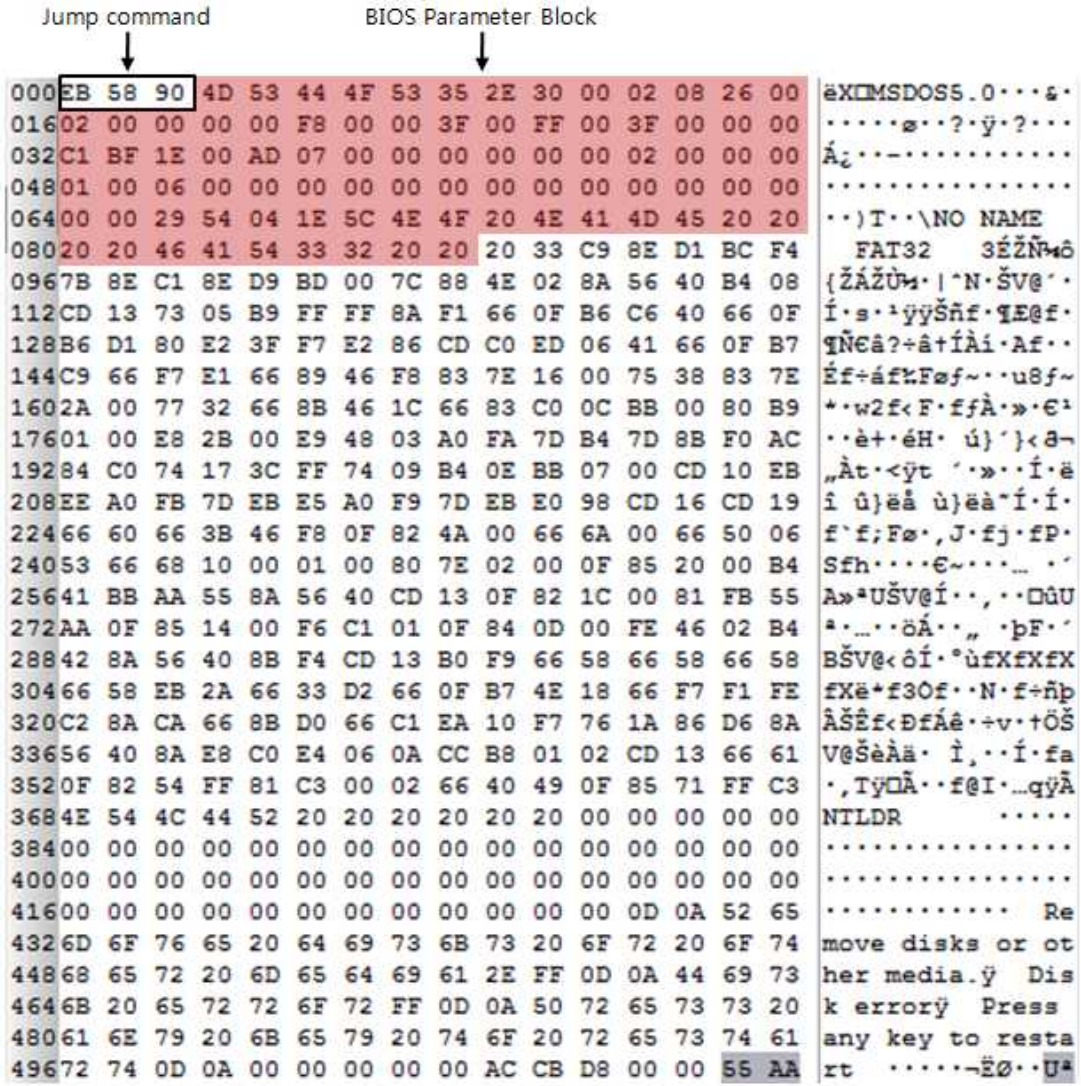
FAT 형식	범위	설명
FAT12/16	0 – 2	Jump command to boot code
FAT32		
FAT12/16	3 – 61	BIOS Parameter Block(BPB)
FAT32	3 – 89	
FAT12/16	62 – 509	Boot code Error message
FAT32	90 – 509	
FAT12/16	510 - 511	Signature (0x55AA)
FAT32		

부트 섹터 데이터 구조



FAT12/16/32 Internals

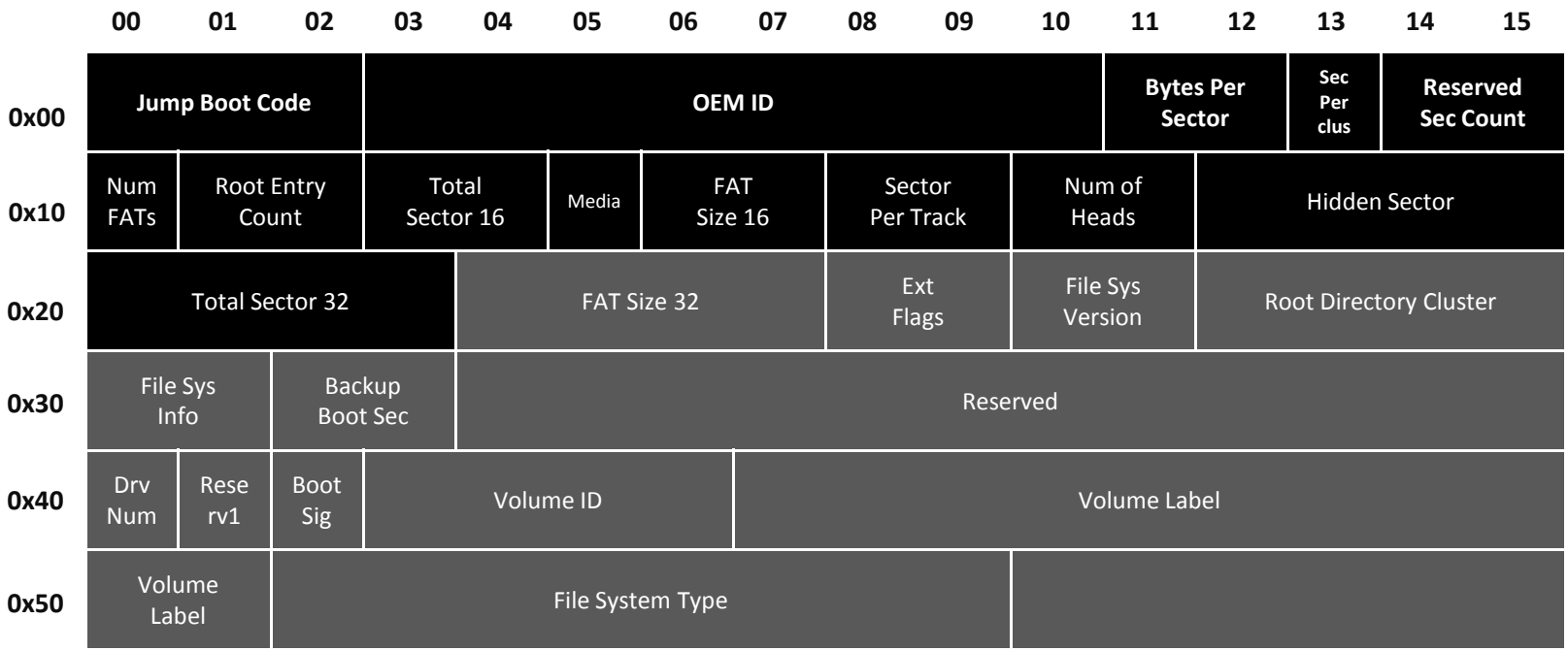
Reserved Area (FAT32) ➔ BIOS Parameter Block




```
000 EB 58 90 4D 53 44 4F 53 35 2E 30 00 02 08 26 00  ëXMSDOS5.0···&·
016 02 00 00 00 00 F8 00 00 3F 00 FF 00 3F 00 00 00  ·····ø··?·ÿ·?···
032 C1 BF 1E 00 AD 07 00 00 00 00 00 00 02 00 00 00  Á¿··-···········
048 01 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00  ················
064 00 00 29 54 04 1E 5C 4E 4F 20 4E 41 4D 45 20 20  ··)T··\NO NAME
080 20 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4    FAT32   3ÉŽÑ¼ô
096 7B 8E C1 8E D9 BD 00 7C 88 4E 02 8A 56 40 B4 08  {ŽÁŽÙ½·|ˆN·ŠV@´·
112 CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66 0F  Í·s·¹ÿÿŠñf·¶E@f·
128 B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7  ¶Ñ€â?÷â†ÍÀí·Af··
144 C9 66 F7 E1 66 89 46 F8 83 7E 16 00 75 38 83 7E  Éf÷áf‰Føƒ~··u8ƒ~
160 2A 00 77 32 66 8B 46 1C 66 83 C0 0C BB 00 80 B9  *·w2f‹F·fƒÀ·»·€¹
176 01 00 E8 2B 00 E9 48 03 A0 FA 7D B4 7D 8B F0 AC  ··è+·éH· ú}´}‹ð¬
192 84 C0 74 17 3C FF 74 09 B4 0E BB 07 00 CD 10 EB  „Àt·<ÿt ´·»··Í·ë
208 EE A0 FB 7D EB E5 A0 F9 7D EB E0 98 CD 16 CD 19  î û}ëå ù}ëà˜Í·Í·
224 66 60 66 3B 46 F8 0F 82 4A 00 66 6A 00 66 50 06  f`f;Fø·‚J·fj·fP·
240 53 66 68 10 00 01 00 80 7E 02 00 0F 85 20 00 B4  Sfh····€~···… ·´
256 41 BB AA 55 8A 56 40 CD 13 0F 82 1C 00 81 FB 55  A»ªUŠV@Í··‚··□ûU
272 AA 0F 85 14 00 F6 C1 01 0F 84 0D 00 FE 46 02 B4  ª·…··öÁ··„ ·þF·´
288 42 8A 56 40 8B F4 CD 13 B0 F9 66 58 66 58 66 58  BŠV@‹ôÍ·°ùfXfXfX
304 66 58 EB 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE  fXë*f3Òf··N·f÷ñþ
320 C2 8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A  ÂŠÊf‹ÐfÁê·÷v·†ÖŠ
336 56 40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61  V@ŠèÀä· Ì¸··Í·fa
352 0F 82 54 FF 81 C3 00 02 66 40 49 0F 85 71 FF C3  ·‚Tÿ□Ã··f@I·…qÿÃ
368 4E 54 4C 44 52 20 20 20 20 20 20 00 00 00 00 00  NTLDR      ·····
384 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ················
400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ················
416 00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 52 65  ·············· Re
432 6D 6F 76 65 20 64 69 73 6B 73 20 6F 72 20 6F 74  move disks or ot
448 68 65 72 20 6D 65 64 69 61 2E FF 0D 0A 44 69 73  her media.ÿ  Dis
464 6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73 20  k errorÿ  Press
480 61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 61  any key to resta
496 72 74 0D 0A 00 00 00 00 00 AC CB D8 00 00 55 AA  rt  ·····¬ËØ··Uª
```

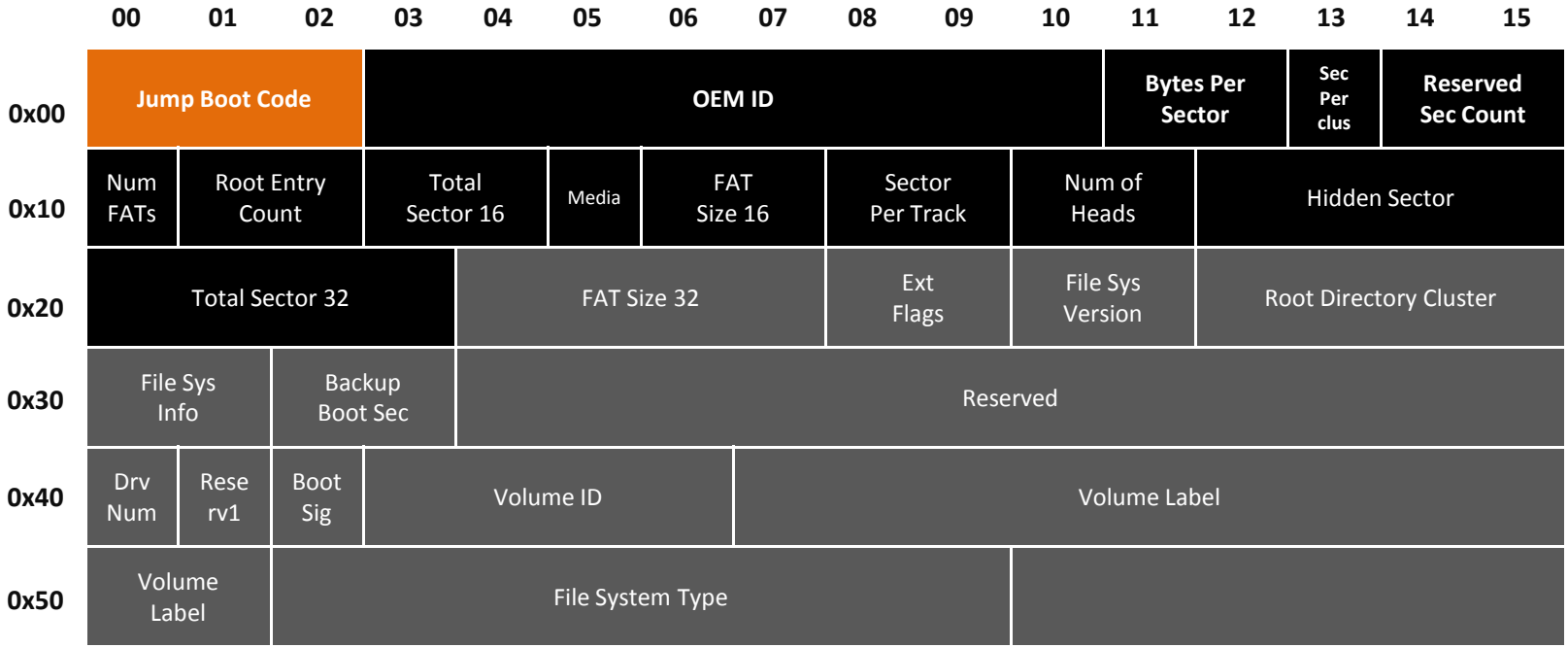
FAT12/16/32 Internals

Reserved Area (FAT32) ➔ BIOS Parameter Block



FAT12/16/32 Internals

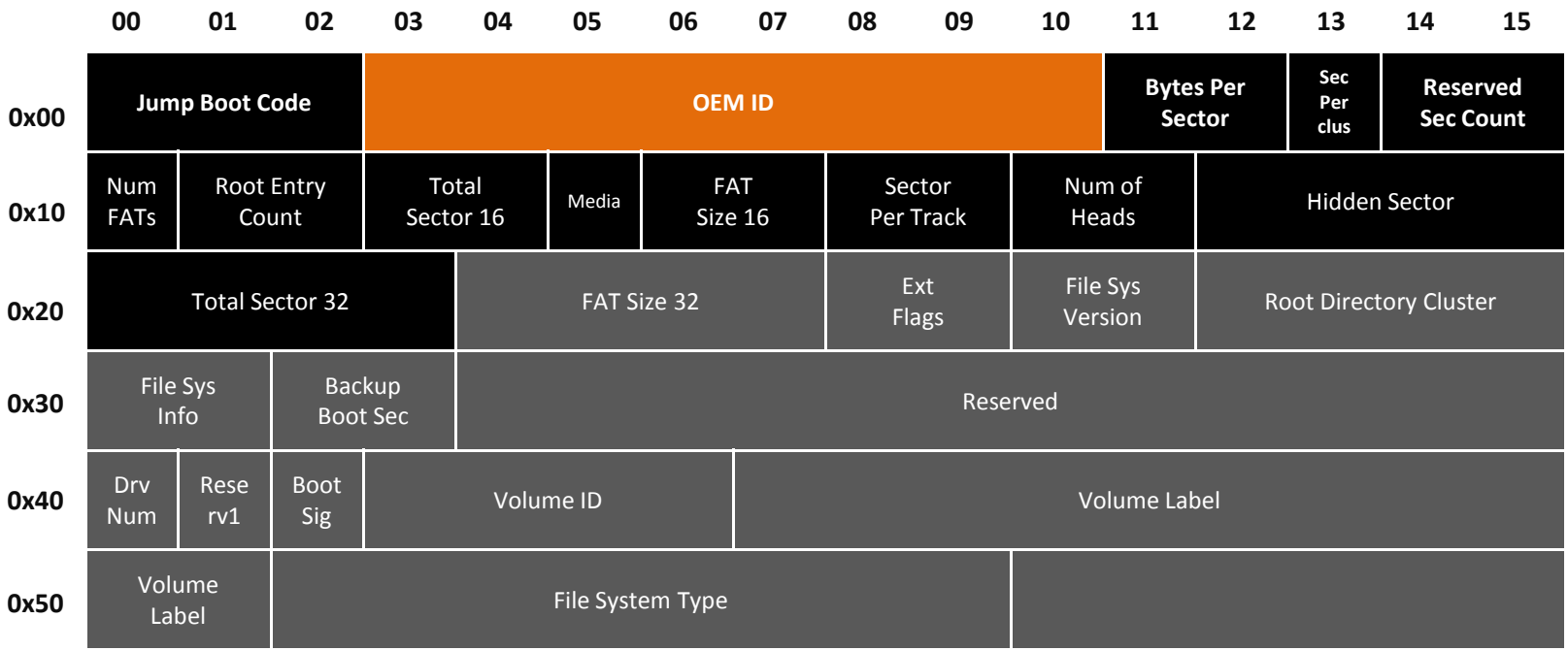
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **Jump Boot Code** : 부트 코드로 점프하기 위한 명령어 (0xEB5890)
  - EB58 : jmp 0000005A
  - 90 : nop

FAT12/16/32 Internals

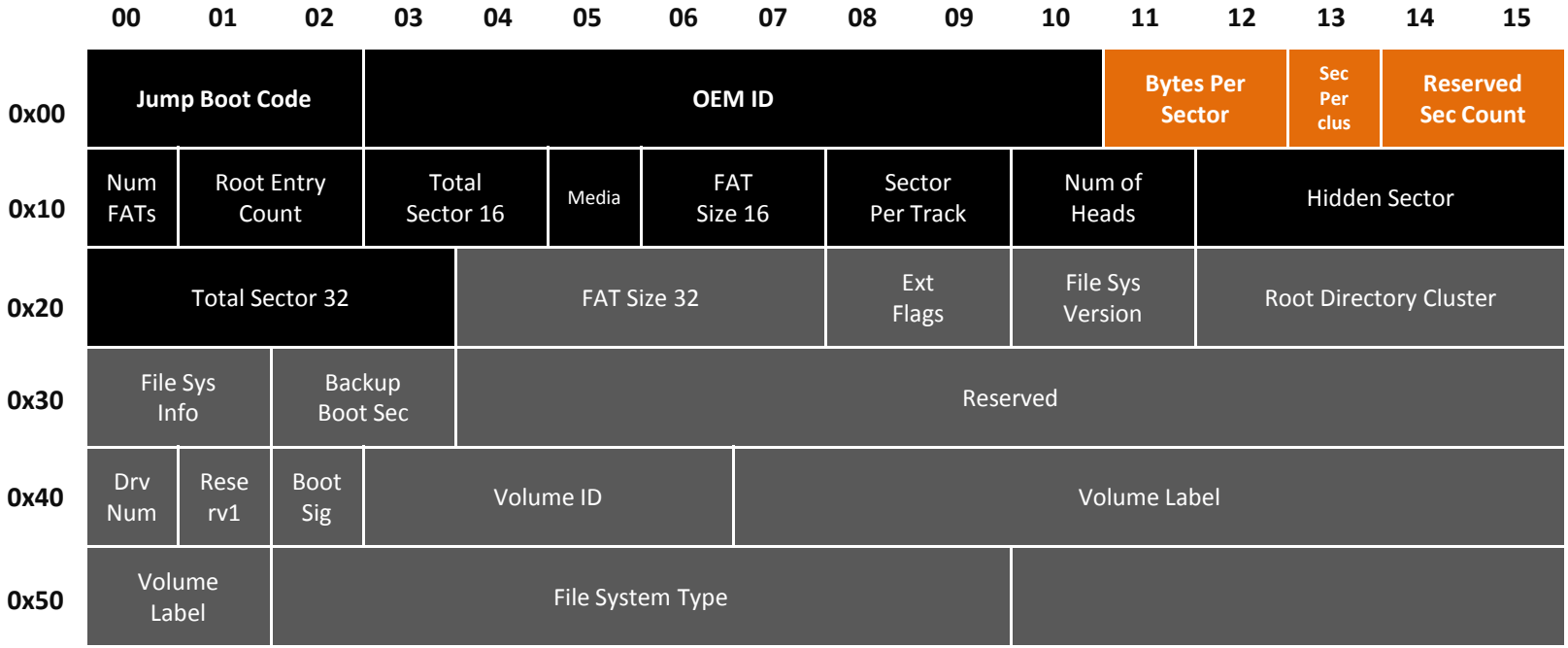
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **OEM ID** : 운영체제 버전별 ID
  - Win95 : MSWIN4.0
  - Win98 : MSWIN4.1
  - Win2K/XP/Vista : MSDOS5.0
  - Linux : mkdosfs

FAT12/16/32 Internals

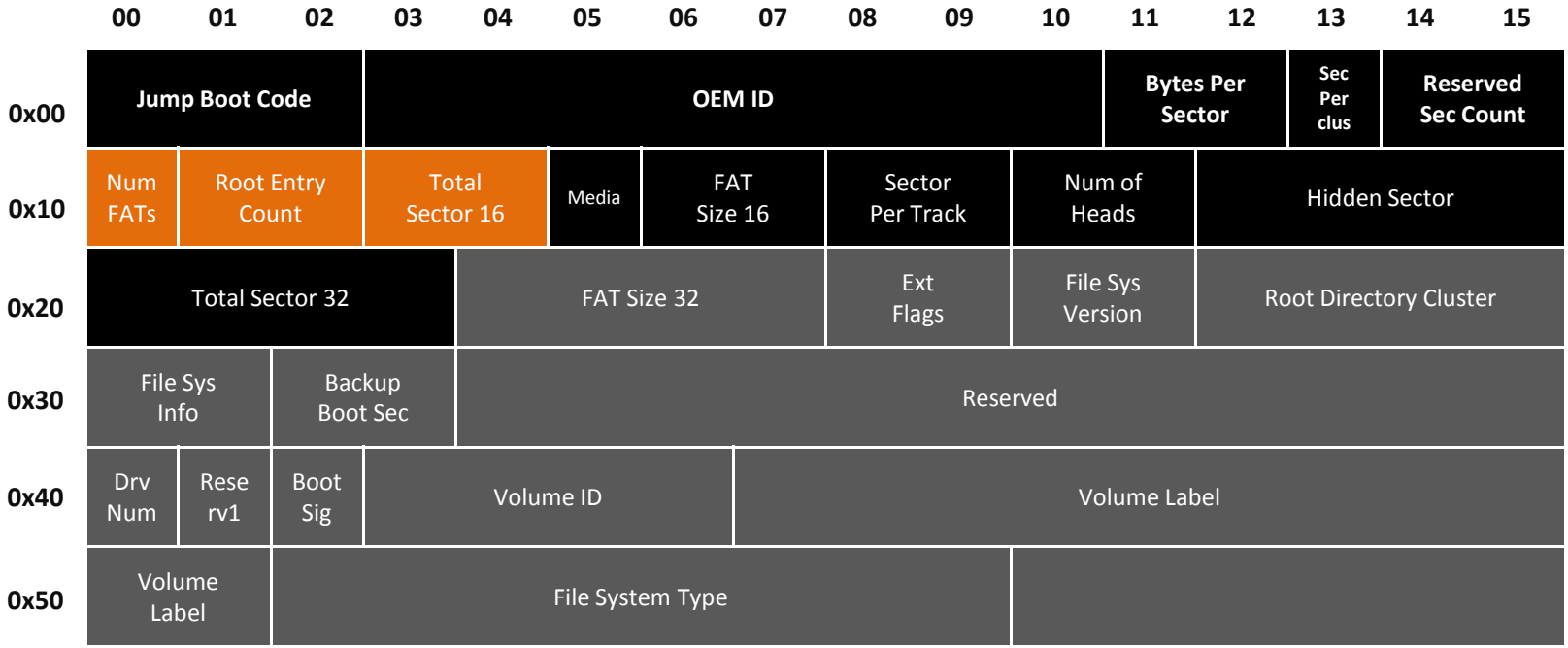
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **Bytes Per Sector** : 섹터 당 바이트 수
- **Sector Per Cluster** : 클러스터 당 섹터 수
- **Reserved Sector Count** : 예약된 영역 섹터 수 (FAT12/16 = 1, FAT32 = 32, 가변형)

FAT12/16/32 Internals

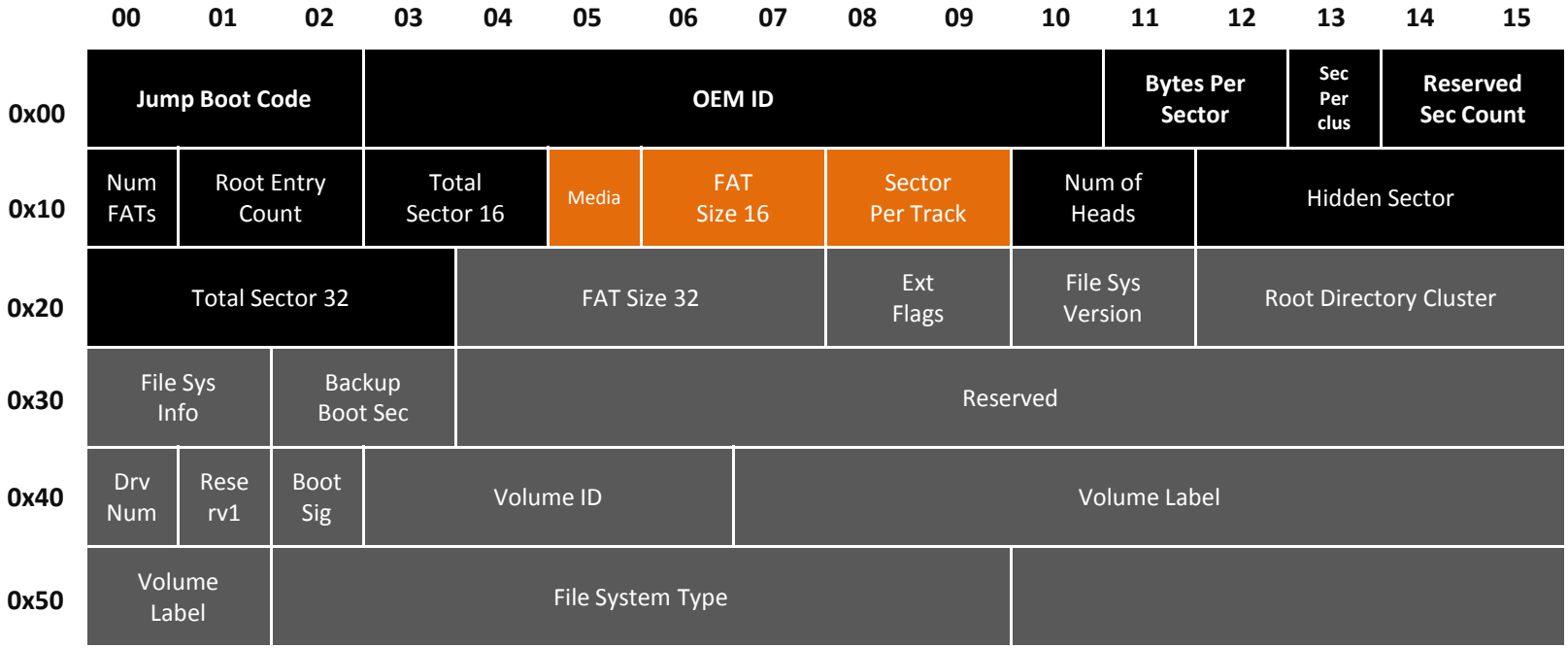
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **Number of FAT Tables** : FAT 테이블 수 (보통 0x02)
- **Root Directory Entry Count** : FAT12/16에서 루트디렉터리가 포함하는 최대 파일 수(FAT12/16=512,FAT32=0)
- **Total Sector 16** : 2 바이트 크기의 파티션 총 섹터 수 (2 바이트로 부족할 경우 Total Sector 32 사용)

FAT12/16/32 Internals

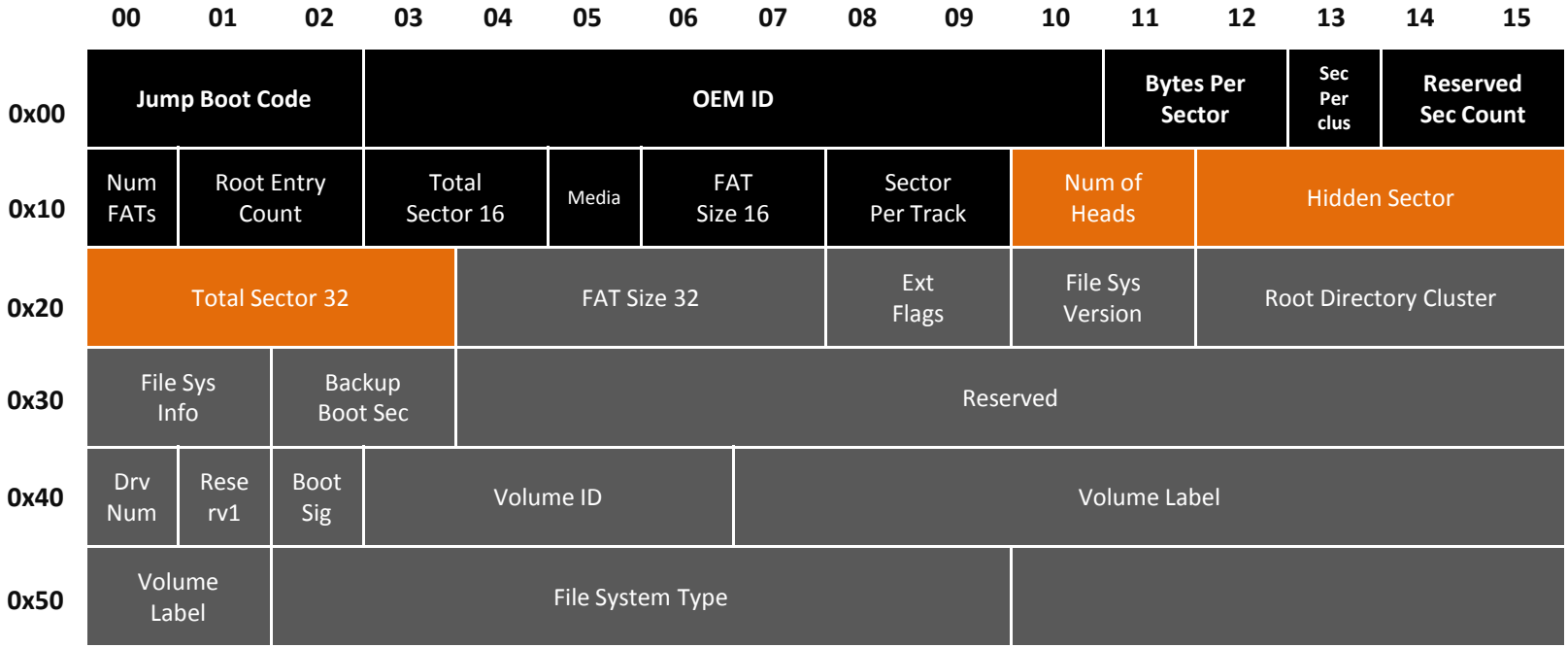
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **Media Type** : 0xF8=fixed disk, 0xF0/F9/FD/FF/FC/FE=floppy, removable
- **FAT Size 16** : FAT12/16에서 FAT 영역이 가지는 2 바이트 크기의 섹터 수 (FAT32=0)
- **Sectors Per Track** : 장치의 트랙 당 섹터 수 (보통 0x3F=63)

FAT12/16/32 Internals

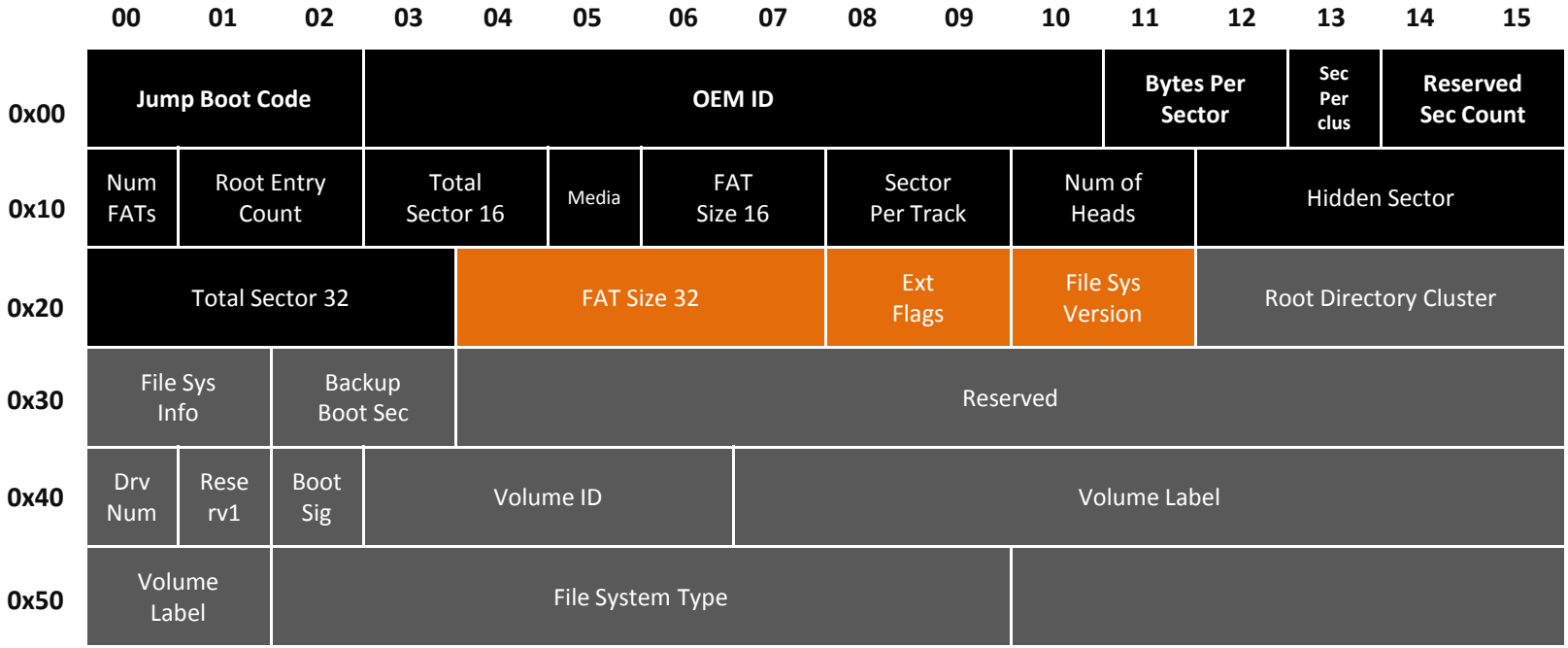
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **Number of Heads** : 장치의 헤더 수
- **Hidden Sectors** : 파티션 시작 전 섹터의 수
- **Total Sector 32** : 4 바이트 크기의 파티션 총 섹터 수

FAT12/16/32 Internals

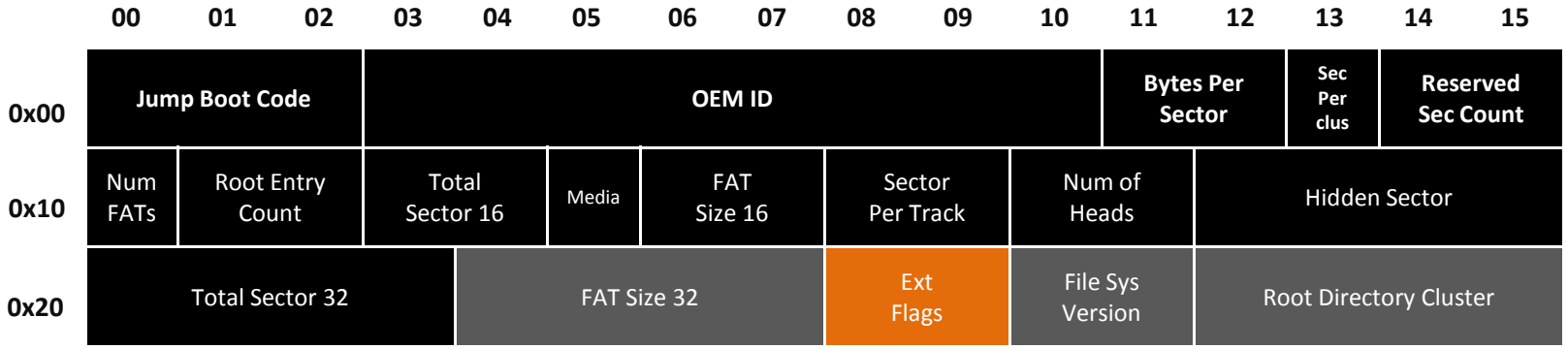
Reserved Area (FAT32) ➔ BIOS Parameter Block

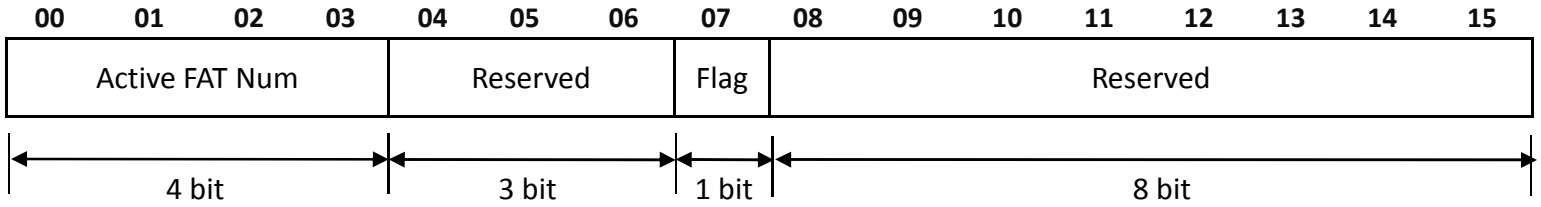


- **FAT Size 32** : FAT 하나의 영역이 가지는 4 바이트 크기의 섹터 수
- **Ext Flags** : 여러 개의 FAT 영역을 사용할 경우 설정 값
- **File System Version** : 파일시스템의 주 버전(major)과 하위 버전(minor)

FAT12/16/32 Internals

Reserved Area (FAT32) ➔ BIOS Parameter Block

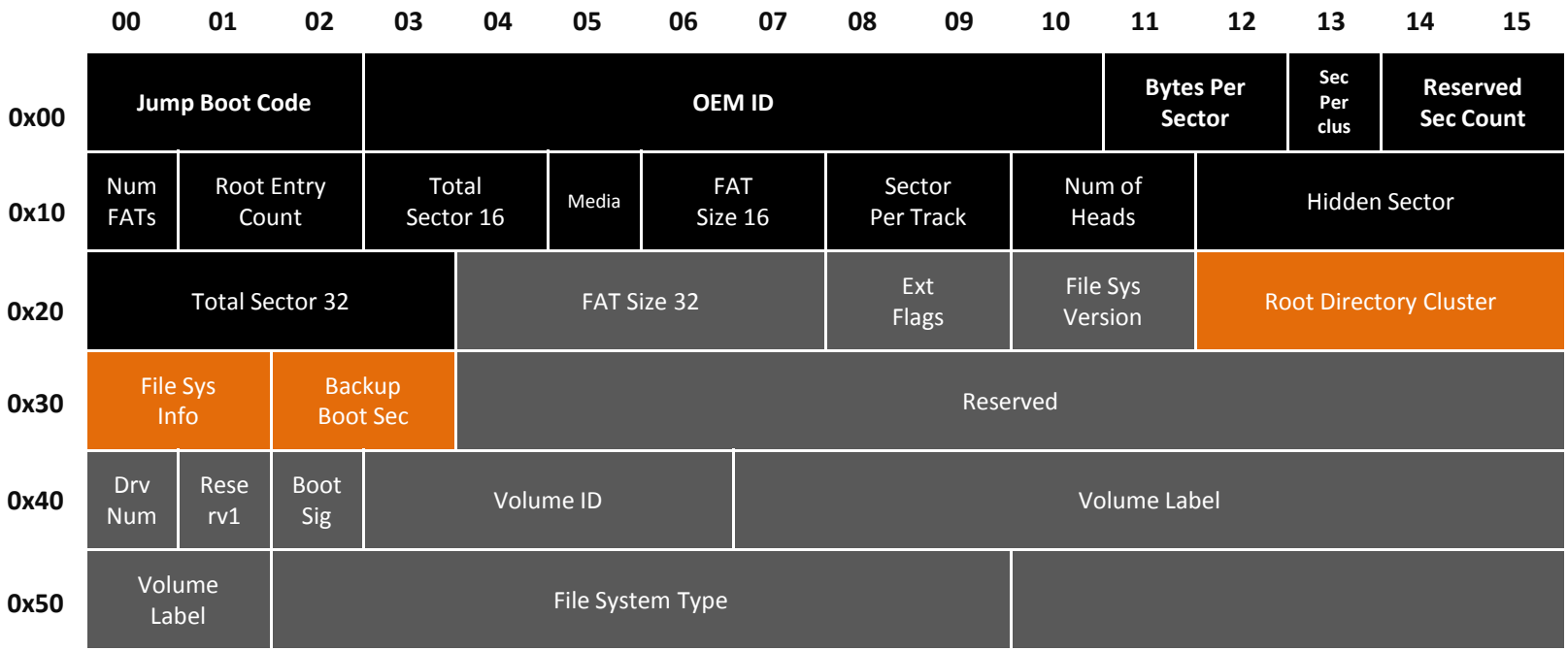




속성 이름	크기	설명
Active FAT Number	4 bit	활성화시킬 FAT 번호로 0부터 시작 (Flag 값이 “1”인 경우에만)
Reserved	3 bit	미래를 위해 예약된 영역
Flag	1 bit	0 : 변경 내용을 모든 FAT 영역에 반영 1 : 변경 내용을 Active FAT Number이 설정된 FAT 영역에만 반영
Reserved	8 bit	미래를 위해 예약된 영역

FAT12/16/32 Internals

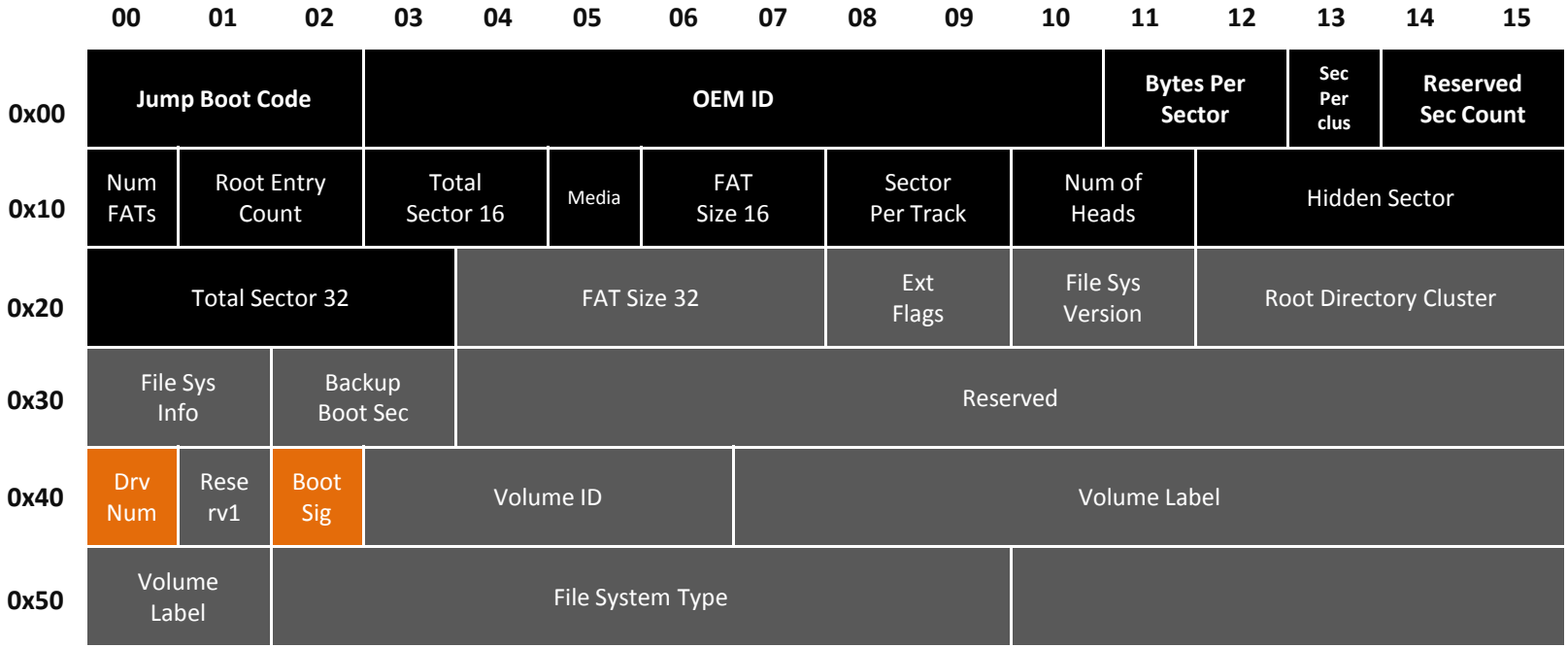
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **Root Directory Cluster** : 루트 디렉터리가 위치한 클러스터 값
  - FAT12/16은 고정된 위치에 루트 디렉터리가 오지만, FAT32의 경우에는 정해져 있지 않음 (보통 클러스터 2번 사용)
- **File System Information** : FSINFO 구조체가 저장된 섹터 번호 (보통 0x01)
- **Backup Boot Record** : 백업된 부트 섹터의 위치 (보통 0x06)

FAT12/16/32 Internals

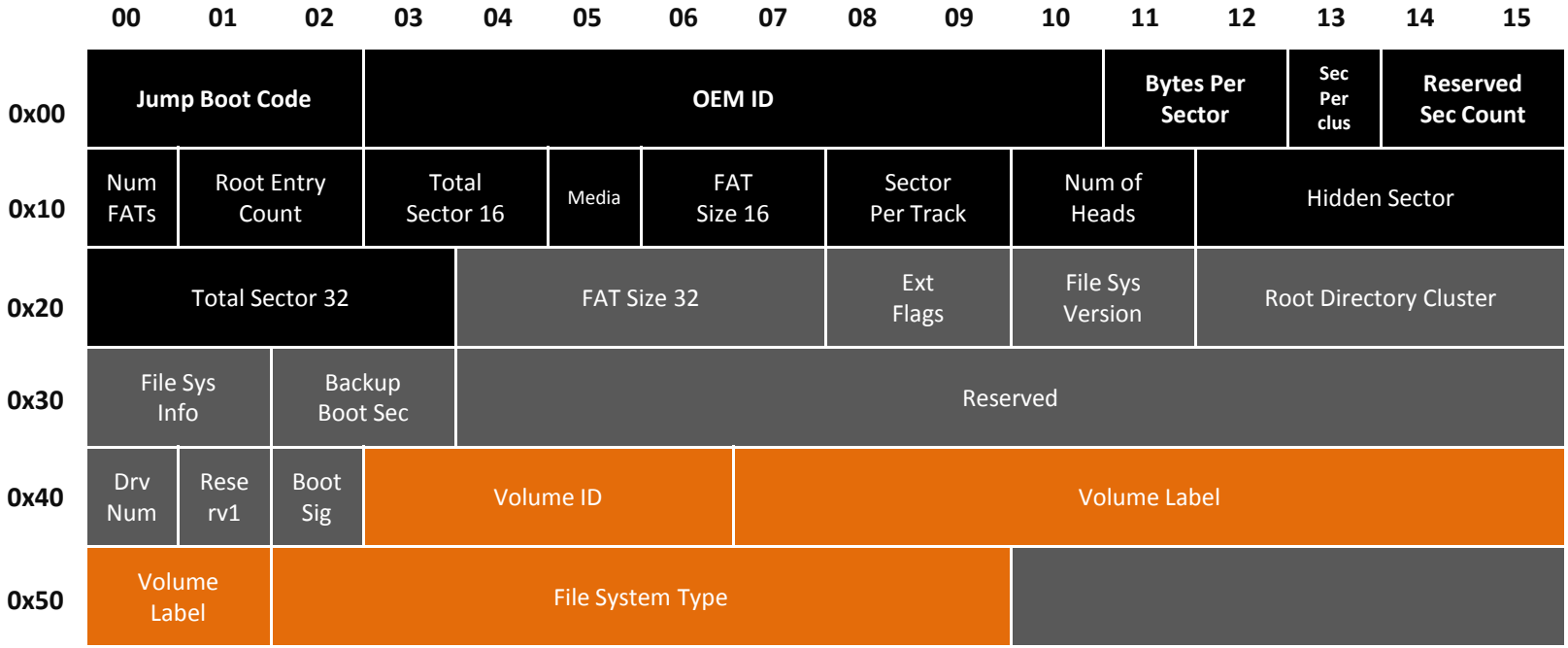
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **Drive Number** : BIOS INT13h 드라이브 번호
- **Boot Signature** : 확장 부트 시그니처 (보통 0x29)
  - 확장 부트 시그니처가 존재할 경우, 시그니처 이후에 3개의 부가 정보(볼륨 ID, 레이블, 타입)가 존재한다는 의미

FAT12/16/32 Internals

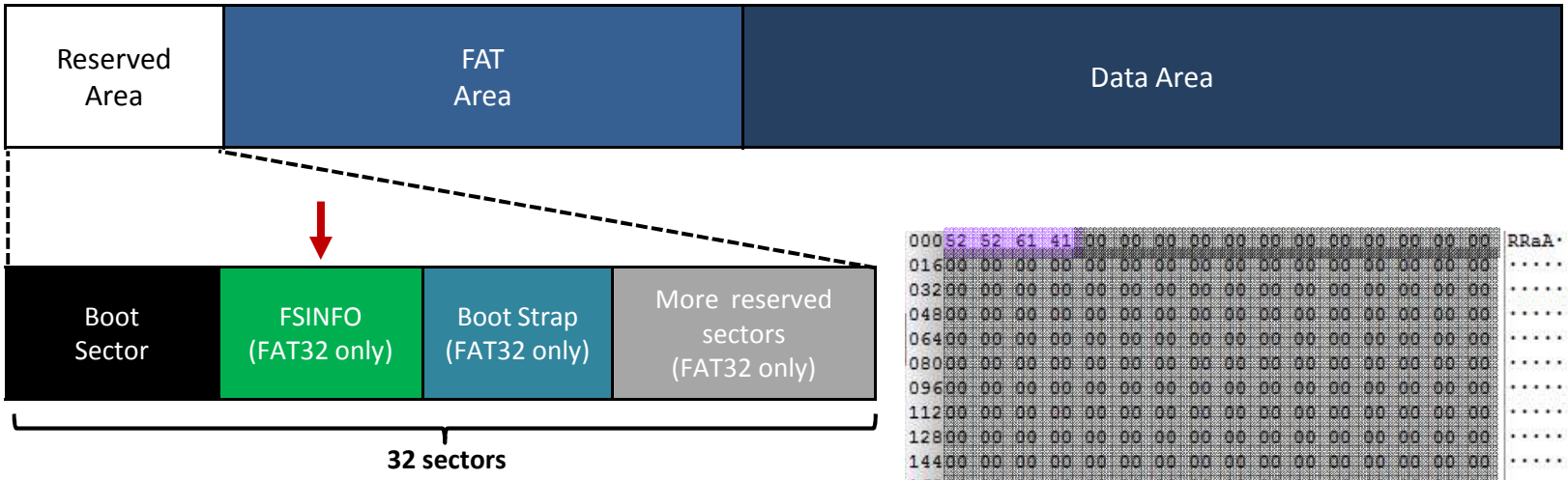
Reserved Area (FAT32) ➔ BIOS Parameter Block



- **Volume ID** : 볼륨 시리얼 번호
- **Volume Label** : 볼륨 레이블 (없을 경우 "NO NAME ")
  - 볼륨 레이블 위치 : 부트 섹터, 루트 디렉터리
- **File System Type** : 파일시스템 형식 ("FAT32 ")

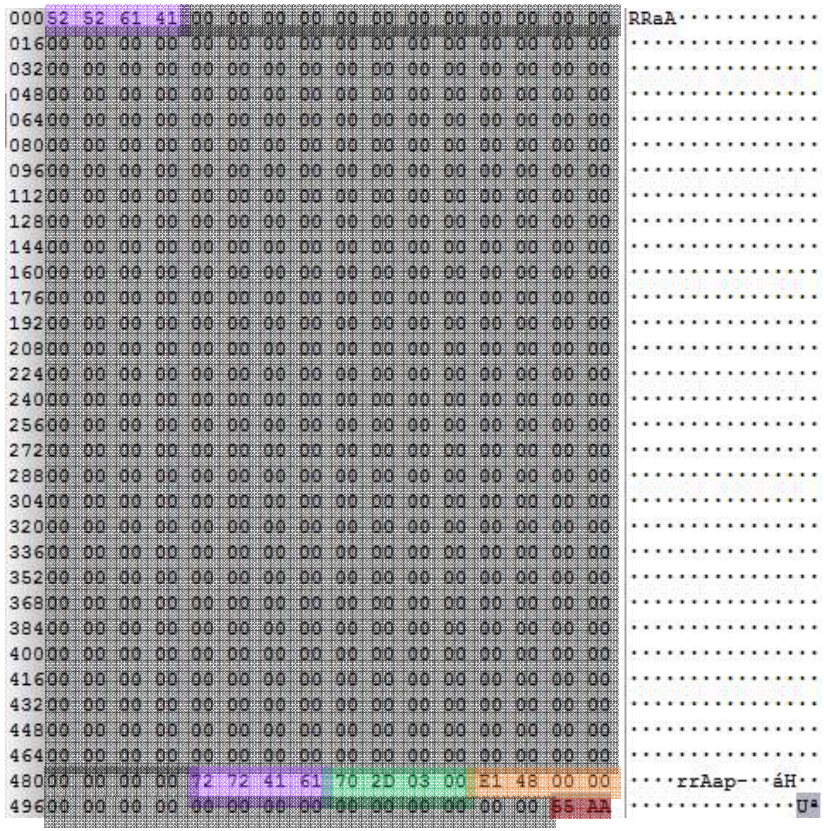
FAT12/16/32 Internals

Reserved Area (FAT32)



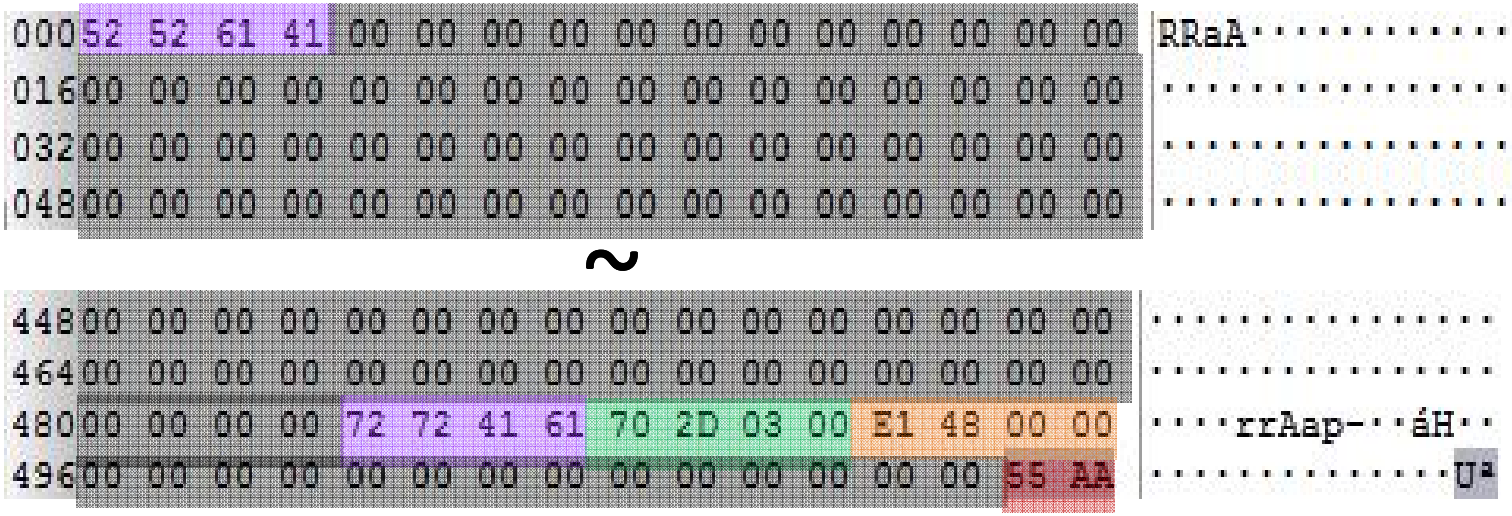
범 위	설 명
0 – 3	Signature (0x41615252)
4 – 483	Not used
484 – 487	Signature (0x61417272)
488 – 491	Number of free clusters
492 – 495	Next free cluster
496 – 508	Not used
510 - 511	Signature (0x55AA)

FSINFO (File System Information)



FAT12/16/32 Internals

Reserved Area (FAT32) ➔ FSINFO Structure

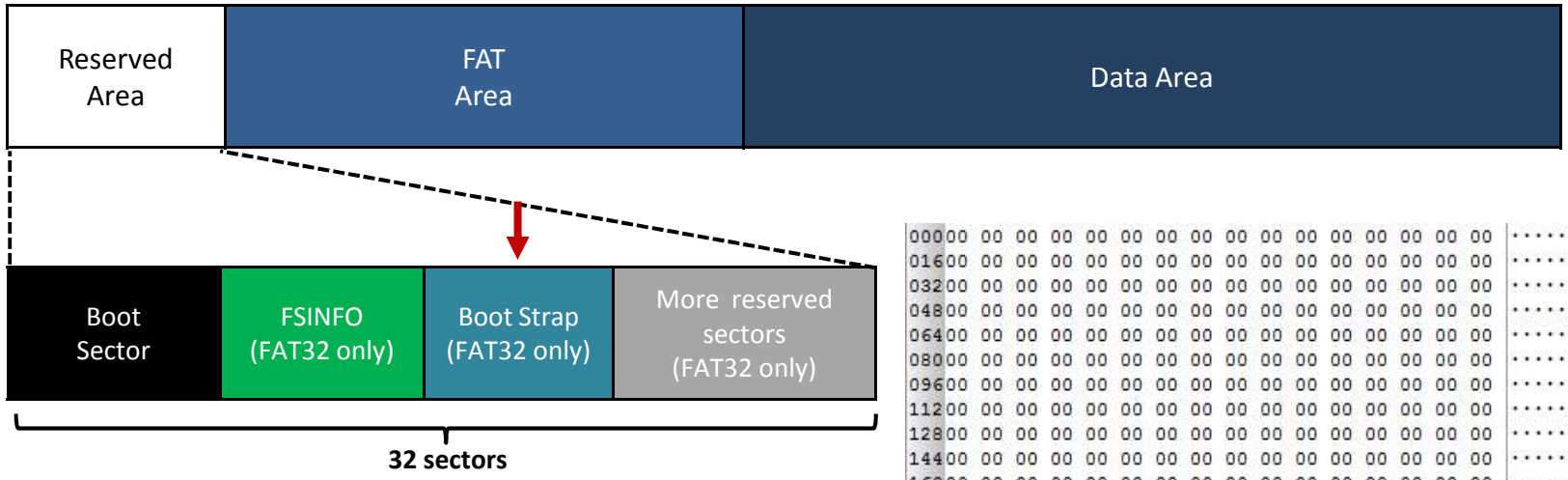


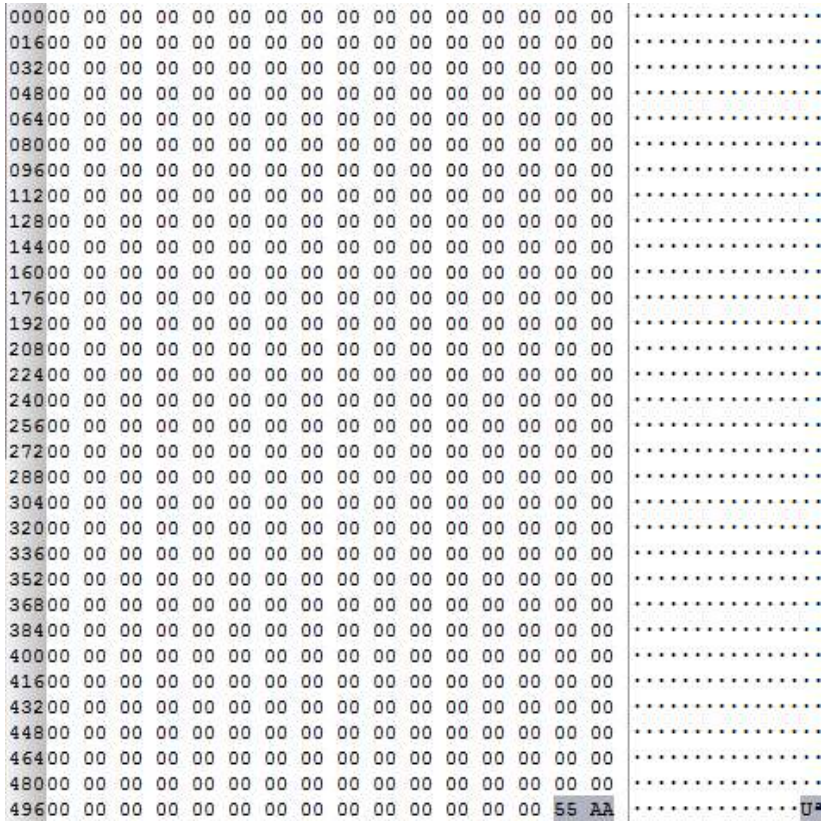
범 위	설 명	값
0 – 3	Signature (0x41615252)	0x41615252
4 – 483	Not used	-
484 – 487	Signature (0x61417272)	0x61417272
488 – 491	Number of free clusters	0x00032D70 (208240)
492 – 495	Next free cluster	0x000048E1 (18657)
496 – 508	Not used	-
510 - 511	Signature (0x55AA)	0x55AA

FSINFO (File System Information)

FAT12/16/32 Internals

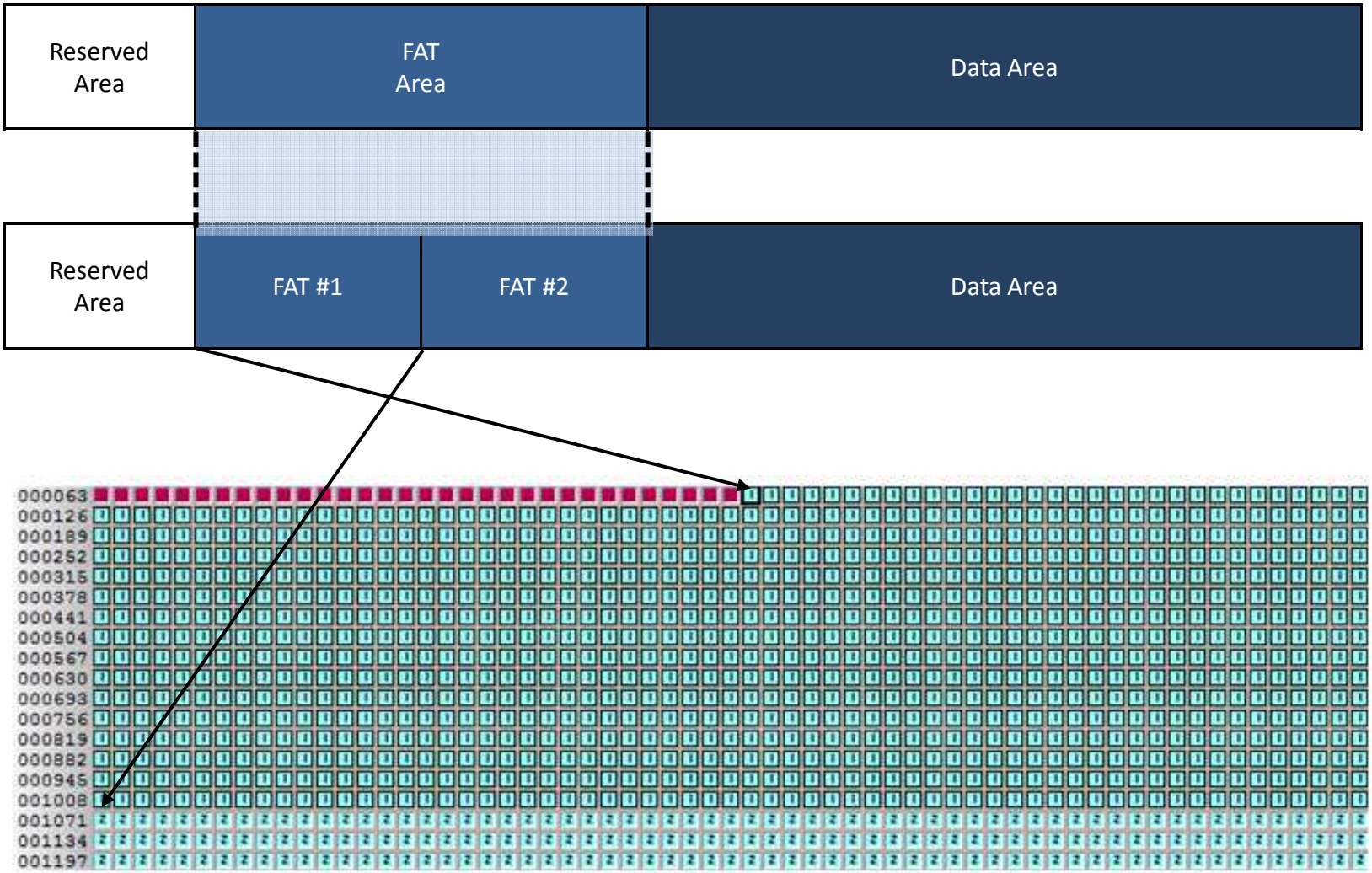
Reserved Area (FAT32)





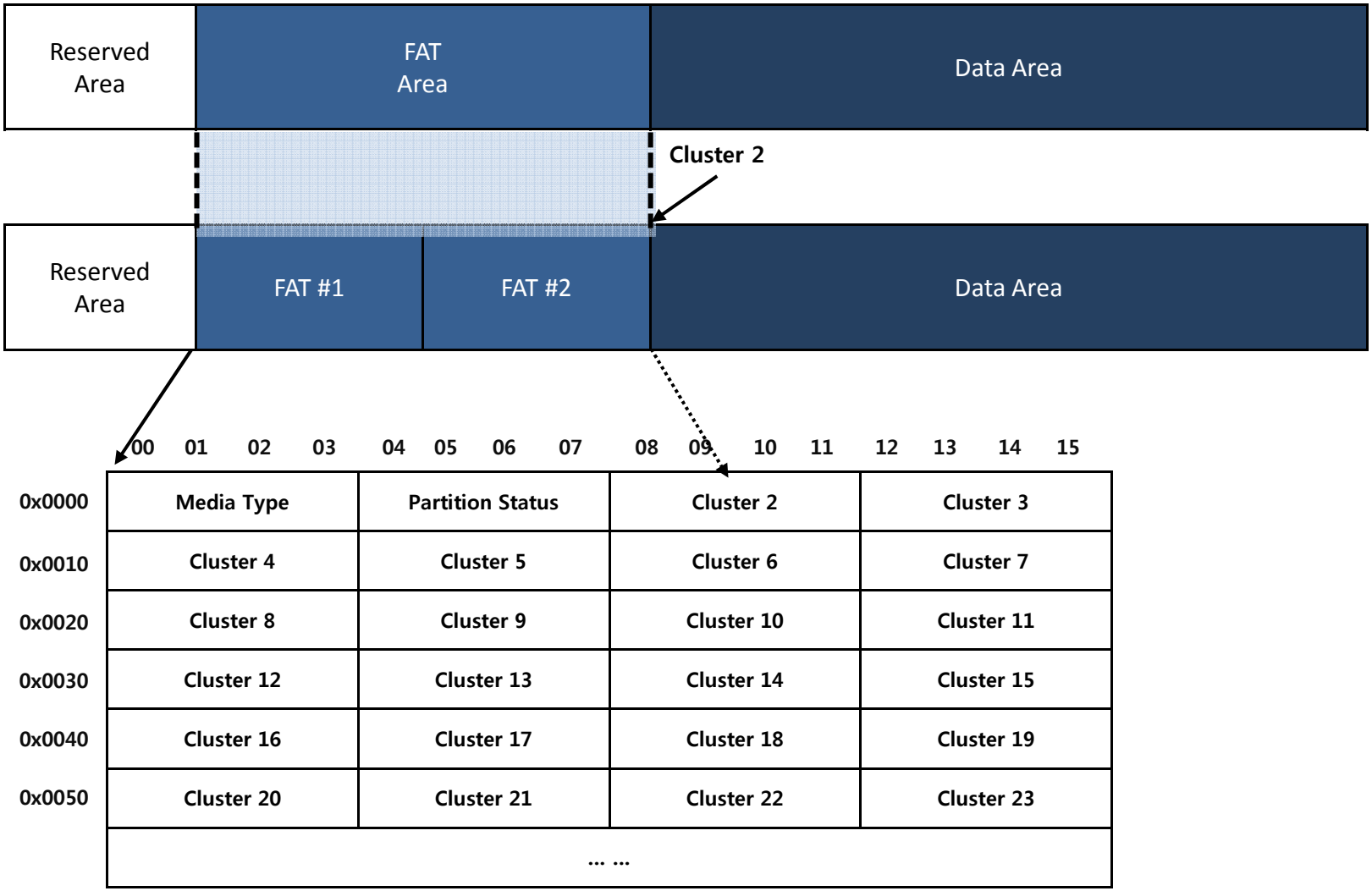
FAT12/16/32 Internals

FAT Area (FAT32)



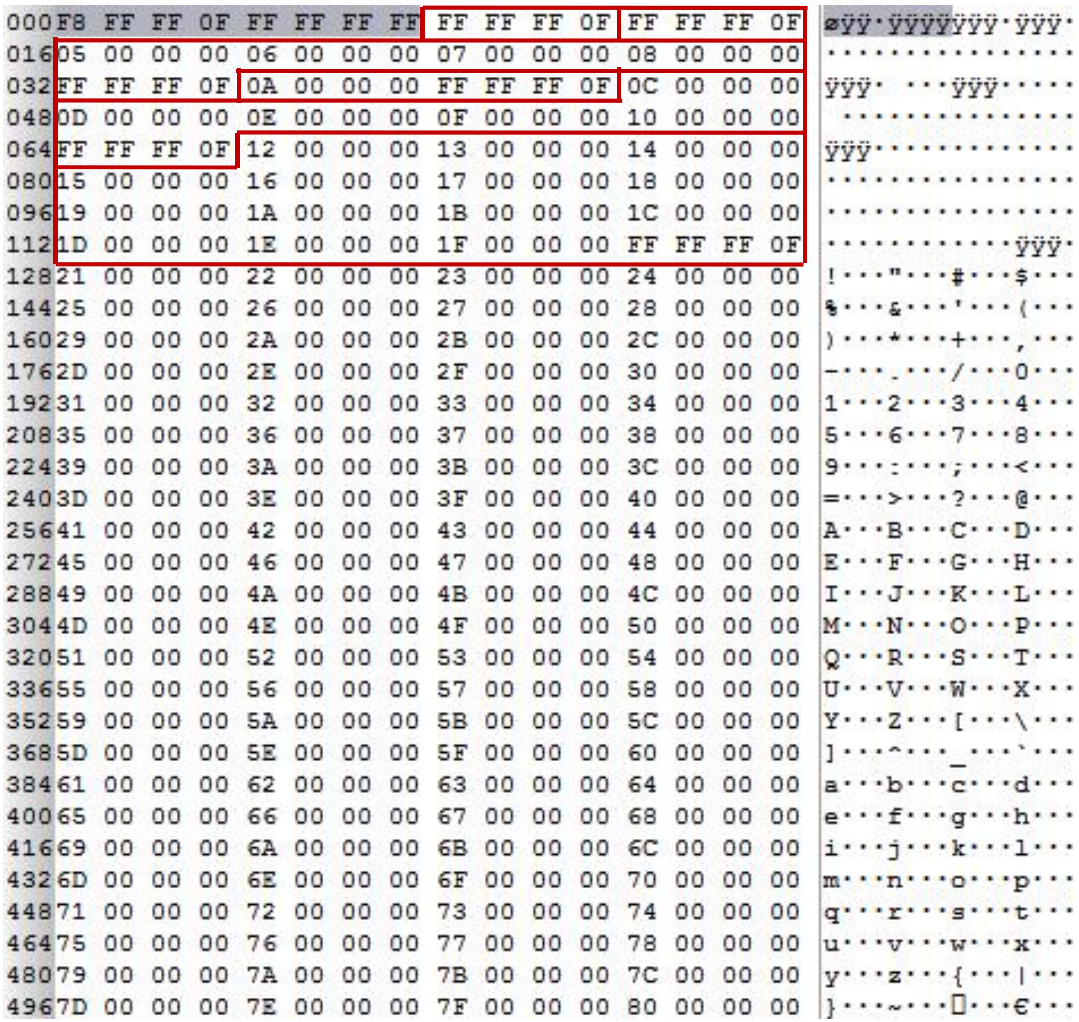
FAT12/16/32 Internals

FAT Area (FAT32)



FAT12/16/32 Internals

FAT Area (FAT32)



000	F8	FF	FF	0F	FF	FF	FF	FF	FF	FF	FF	0F	FF	FF	FF	0F
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
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
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
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
192	31	00	00	00	32	00	00	00	33	00	00	00	34	00	00	00
208	35	00	00	00	36	00	00	00	37	00	00	00	38	00	00	00
224	39	00	00	00	3A	00	00	00	3B	00	00	00	3C	00	00	00
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
272	45	00	00	00	46	00	00	00	47	00	00	00	48	00	00	00
288	49	00	00	00	4A	00	00	00	4B	00	00	00	4C	00	00	00
304	4D	00	00	00	4E	00	00	00	4F	00	00	00	50	00	00	00
320	51	00	00	00	52	00	00	00	53	00	00	00	54	00	00	00
336	55	00	00	00	56	00	00	00	57	00	00	00	58	00	00	00
352	59	00	00	00	5A	00	00	00	5B	00	00	00	5C	00	00	00
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
400	65	00	00	00	66	00	00	00	67	00	00	00	68	00	00	00
416	69	00	00	00	6A	00	00	00	6B	00	00	00	6C	00	00	00
432	6D	00	00	00	6E	00	00	00	6F	00	00	00	70	00	00	00
448	71	00	00	00	72	00	00	00	73	00	00	00	74	00	00	00
464	75	00	00	00	76	00	00	00	77	00	00	00	78	00	00	00
480	79	00	00	00	7A	00	00	00	7B	00	00	00	7C	00	00	00
496	7D	00	00	00	7E	00	00	00	7F	00	00	00	80	00	00	00

- **0x00000000** : Available
- **0x?FFFFFFF** : End-Of-Marker
- **0x?FFFFFF7** : Bad Cluster

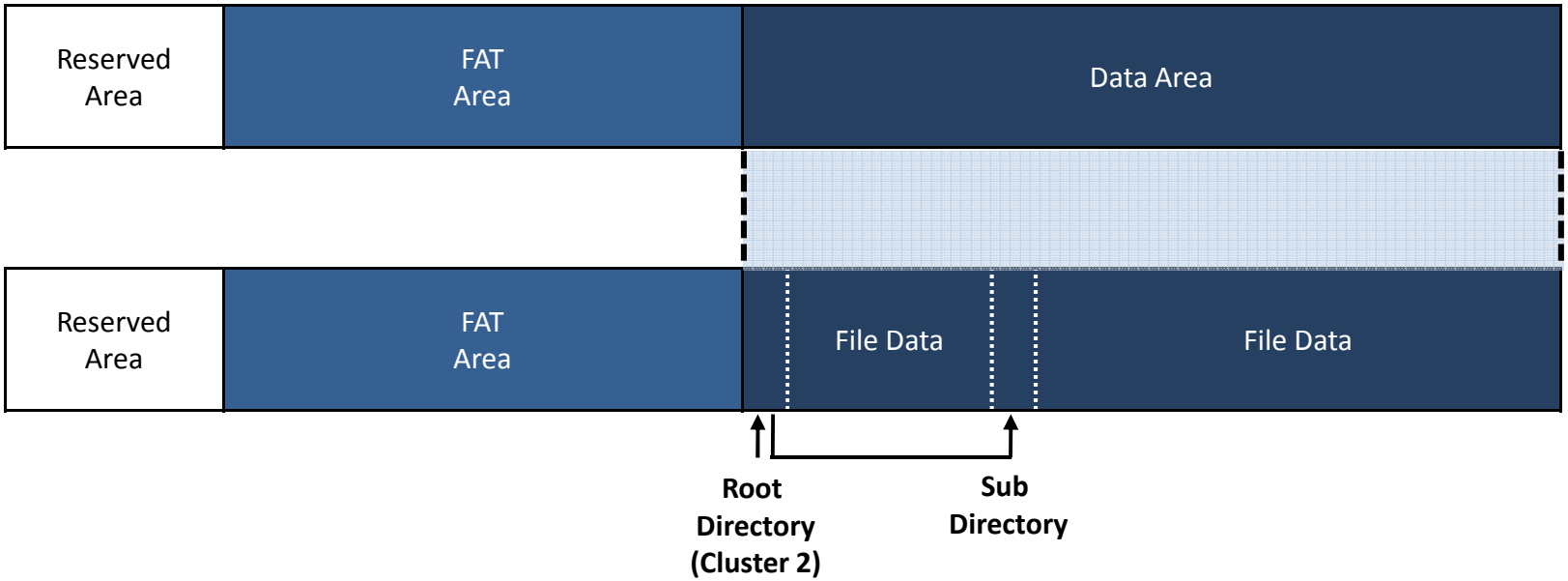
- **FAT Entry 크기**
  - ✓ **FAT12/16 :** 2 bytes (256개)
  - ✓ **FAT32 :** 4 bytes (128 개)

FAT12/16/32
Directory Structure

Security is a people problem…

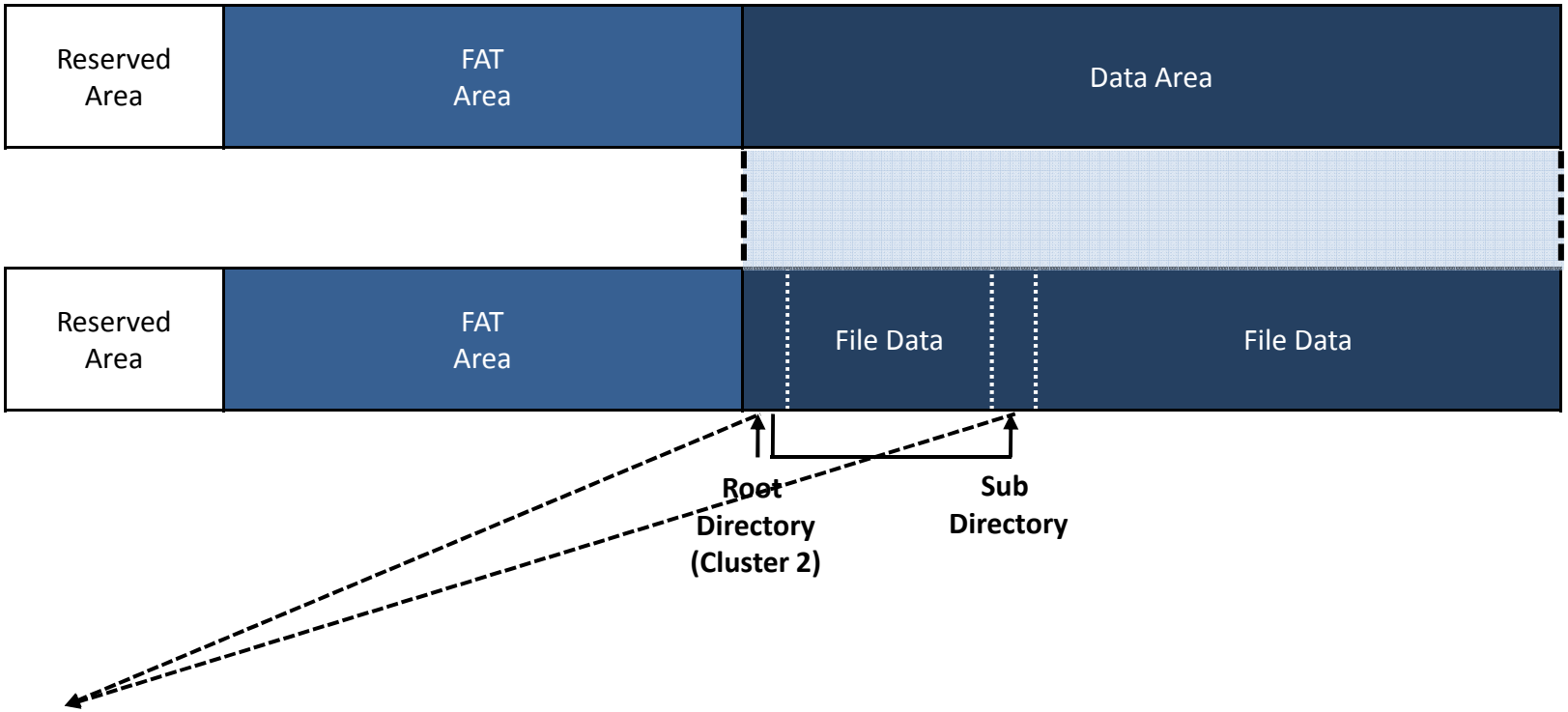
FAT12/16/32 Directory Structure

Data Area



FAT12/16/32 Directory Structure

Data Area



	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00	Name								Extension			Attr	Rese rved	Create Time Tenths	Created Time	
0x10	Created Date				Last Accessed Date				Starting Cluster Hi			Last Written Time			Last Written Date	
	Starting Cluster Low				File Size											

FAT12/16/32 Directory Structure

Data Area ➔ Directory Entry

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00	Name								Extension			Attr	Reserved	Create Time Tenths	Created Time	
0x10	Created Date				Last Accessed Date				Starting Cluster Hi			Last Written Time			Last Written Date	
0x20	Starting Cluster Low				File Size											

위치	설명
0 – 0	File Name or Status Byte
1 – 7	File Name
8 – 10	File Extension
11 – 11	Attributes
12	Reserved
13	Created Time (tenths of second)
14 – 15	Created Time
16 – 17	Created Date
18 – 19	Accessed Date
20 – 21	Starting Cluster High 2 Bytes
22 – 23	Written Time
24 – 25	Written Date
26 – 27	Starting Cluster Low 2 Byte
28 - 31	File Size

- **Status Byte**
  - **0xE5** : 삭제된 파일
  - **0x00** : 비어있는 파일
  - **0xE5** (일본 간지) ➔ **0x05** 대신 표현

FAT12/16/32 Directory Structure

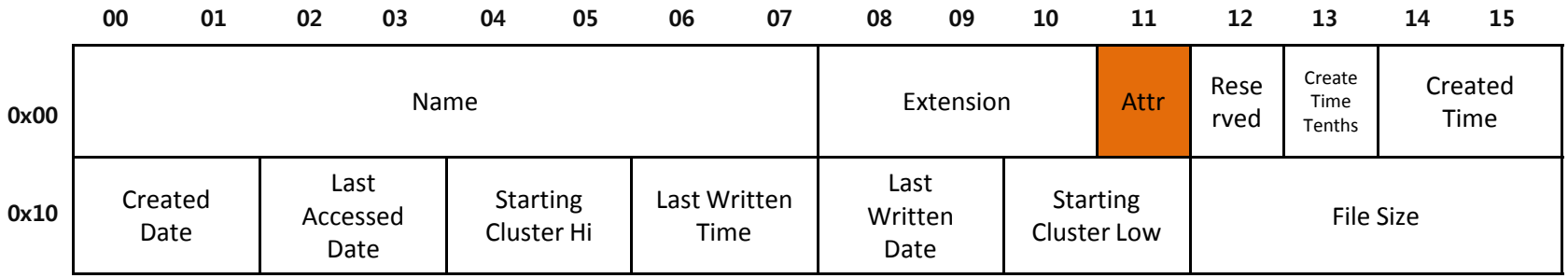
Data Area ➔ Directory Entry

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00	Name								Extension			Attr	Reserved	Create Time Tenths	Created Time	
0x10	Created Date		Last Accessed Date		Starting Cluster Hi		Last Written Time		Last Written Date		Starting Cluster Low		File Size			

- **Name** : 8 바이트의 파일 이름
  - 영문 : ASCII 로 표현
  - 한글 : 한글 완성형
  - 공백은 0x20 (ASCII, space)로 표현
- **Extension** : 3 바이트의 파일 확장자

FAT12/16/32 Directory Structure

Data Area ➔ Directory Entry

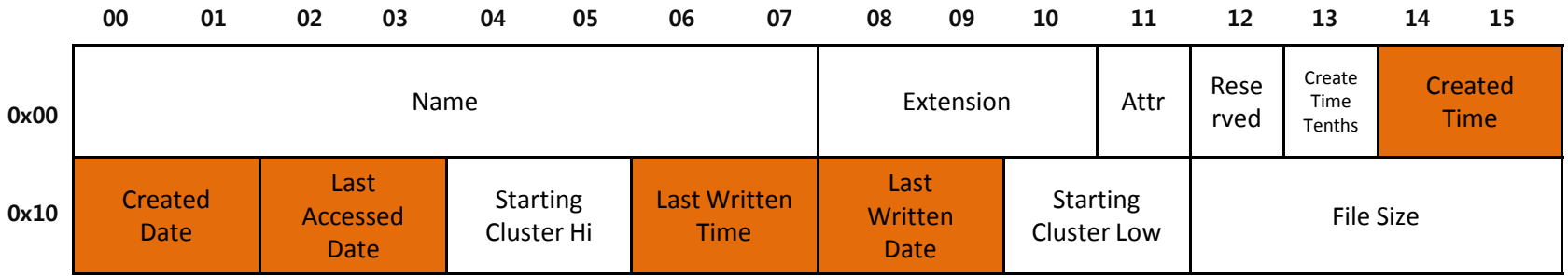


- **File Attributes** : 해당 파일의 형식

값	의미	설명
0000 0001 (0x01)	Read Only	읽기 전용 파일
0000 0010 (0x02)	Hidden File	숨긴 파일
0000 0100 (0x04)	System File	운영체제 시스템 파일
0000 1000 (0x08)	Volume Label	해당 파일의 이름이 곧 볼륨 이름 루트 디렉터리에 위치하며 시작 클러스터는 “0”
0000 1111 (0x0F)	Long File Name	긴 파일 이름 엔트리
0001 0000 (0x10)	Directory	디렉터리
0010 0000 (0x20)	Archive	일반 파일

FAT12/16/32 Directory Structure

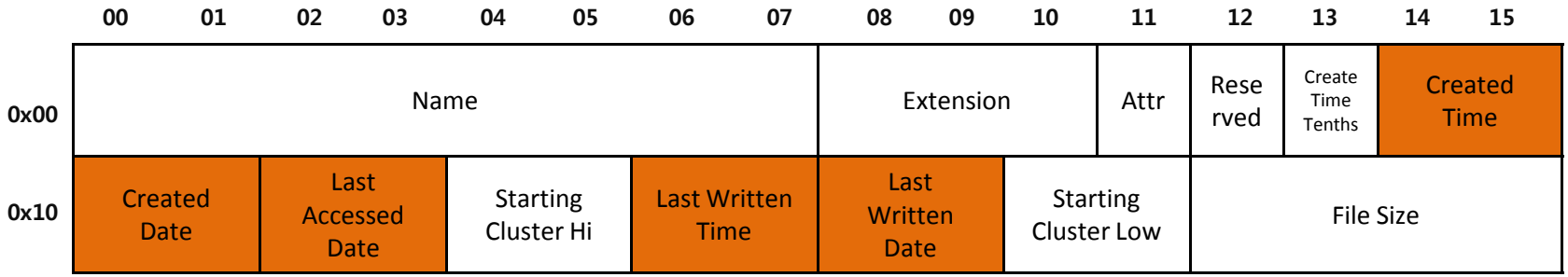
Data Area ➔ Directory Entry



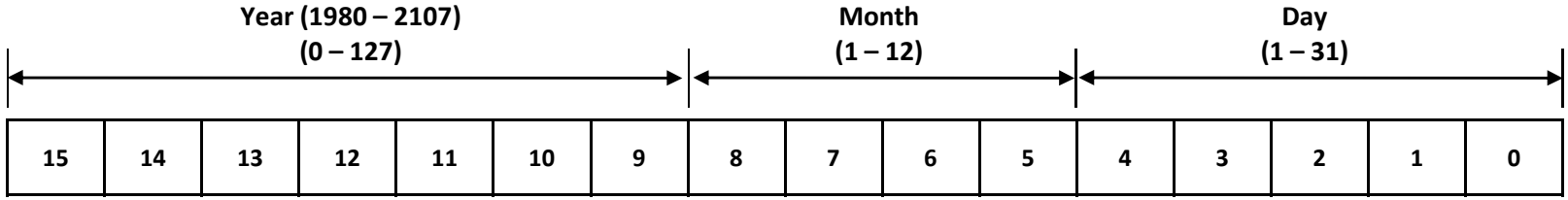
- **Create Time (tenths of second)** : 파일 생성 시간 (10분의 1초)
- **Created Time (hours, minutes, seconds)** : 파일 생성 시간 (시, 분, 초)
- **Created Date** : 파일 생성 날짜
- **Last Accessed Date** : 마지막 접근 날짜
- **Last Written Time (hours, minutes, seconds)** : 마지막 수정 시간 (시, 분, 초)
- **Last Written Date** : 마지막 수정 날짜

FAT12/16/32 Directory Structure

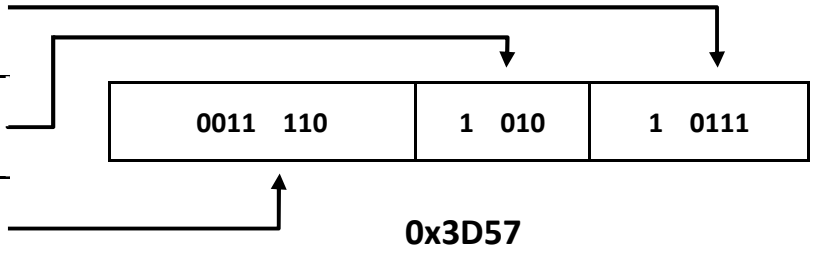
Data Area ➔ Directory Entry



- **날짜 표현 형식 (October 23, 2010)**

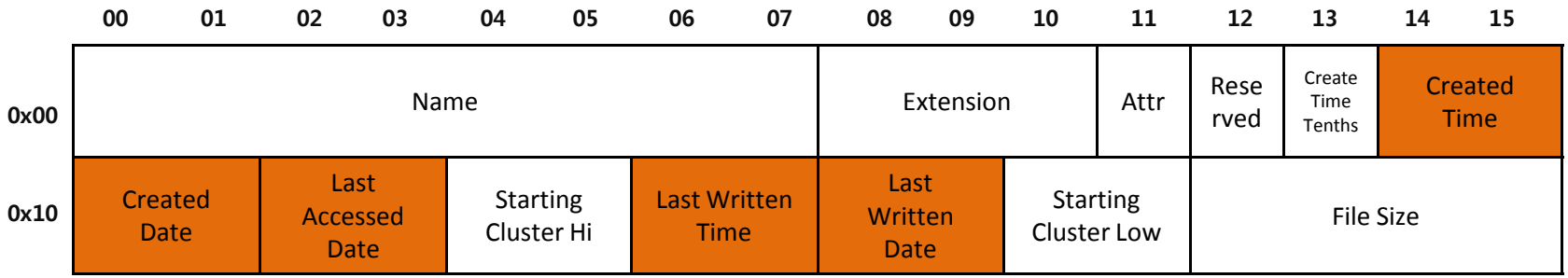


날 짜	10진수	16진수	바이너리
23	23	0x17	1 0111
October	10	0x0A	1010
2010	30	0x1E	001 1110

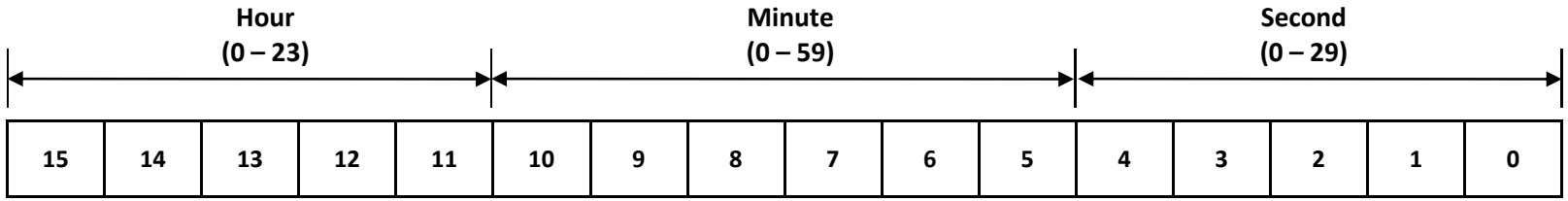


FAT12/16/32 Directory Structure

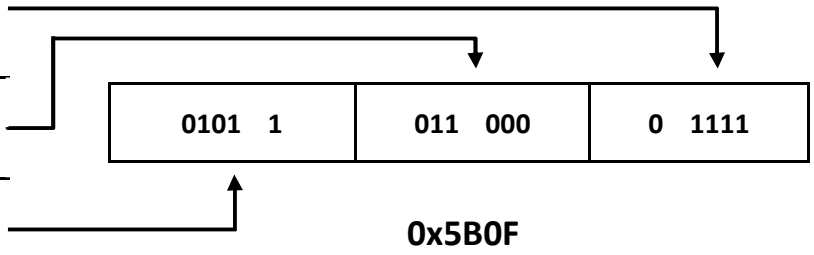
Data Area ➔ Directory Entry



- **시간 표현 형식 (11:24:30 AM)**

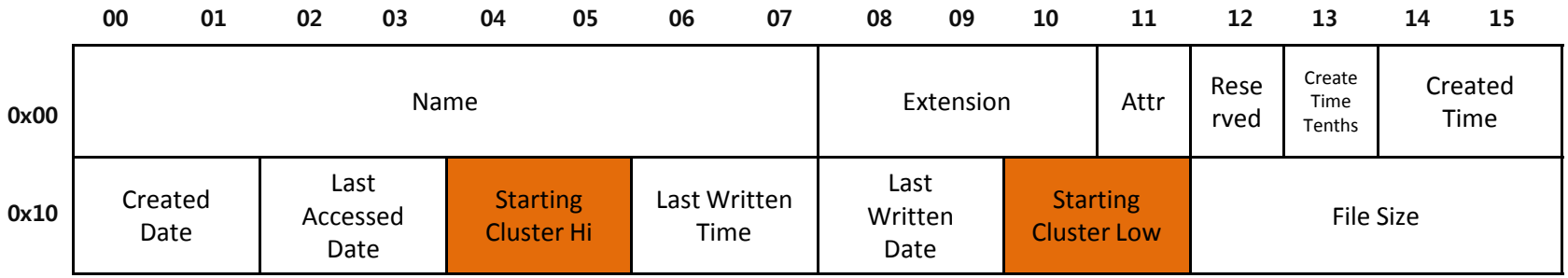


시 간	10진수	16진수	바이너리
30	15	0x0F	0 1111
24	24	0x18	01 1000
11	11	0x0B	0 1011



FAT12/16/32 Directory Structure

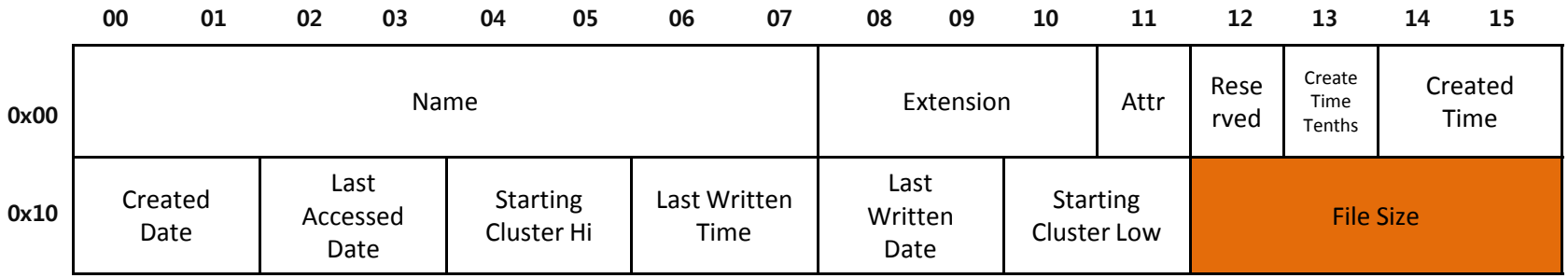
Data Area ➔ Directory Entry



- **Starting Cluster Hi (2 bytes)** : 파일이 위치한 시작 클러스터의 상위 2 바이트
- **Starting Cluster Low (2 bytes)** : 파일이 위치한 시작 클러스터의 하위 2 바이트

FAT12/16/32 Directory Structure

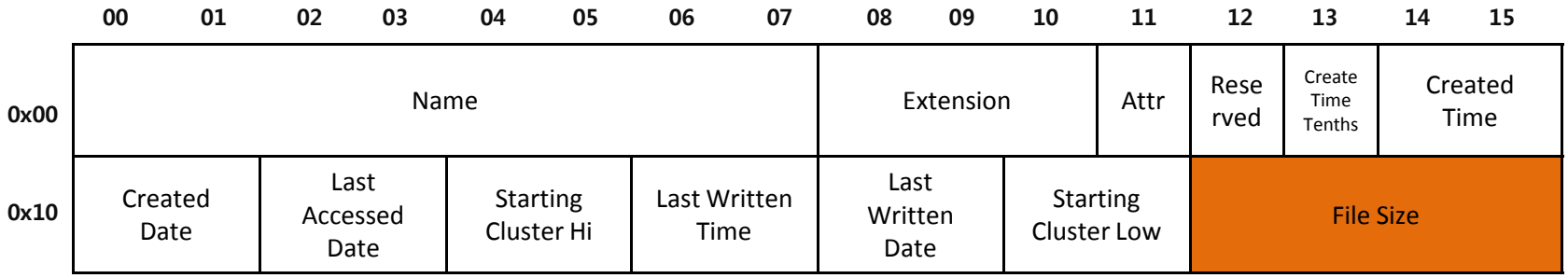
Data Area ➔ Directory Entry



- **File Size** : 바이트 단위의 파일 크기 (2^{32} = 4,294,967,296 = 4 GB)

FAT12/16/32 Directory Structure

Data Area ➔ Directory Entry

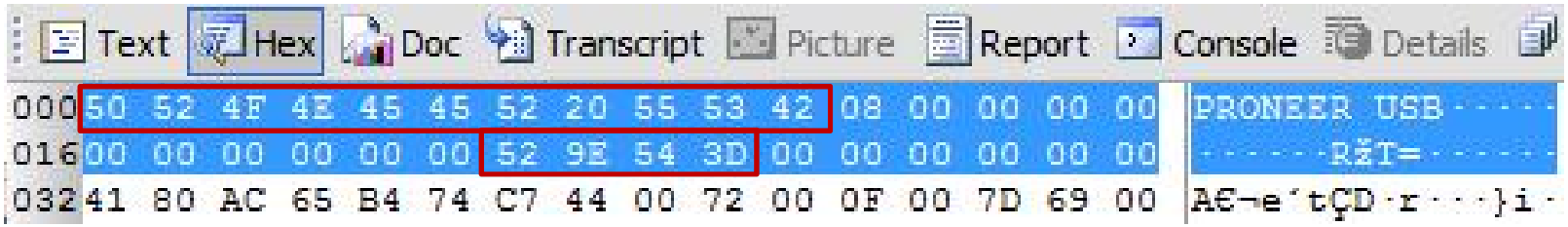


이 름	값
Name	PRONEER
Extension	TXT
Attribute	0x20 (Archive, 일반 파일)
Created Date/Time	2010년 10월 20일 04:17:10 PM
Last Accessed Date	2010년 10월 20일
Last Written Date/Time	2010년 9월 29일 05:37:16 PM
Starting Cluster	0x000064A5 (25,765)
Created Time	0x000000AA (170)

FAT12/16/32 Directory Structure

Data Area ➔ Directory Entry (볼륨이름)

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00	Name								Extension			Attr	Rese rved	Create Time Tenths	Created Time	
0x10	Created Date		Last Accessed Date		Starting Cluster Hi		Last Written Time		Last Written Date		Starting Cluster Low		File Size			



- **볼륨 이름 : "PRONEER USB"**
  - 루트 디렉터리 내 첫 번째 디렉터리 엔트리에 위치
  - 확장자 필드도 볼륨 이름으로 사용
  - 속성과 마지막 수정 시간 (볼륨 이름 설정 시간)만 빼고 나머지 필드는 사용 안함
    - 볼륨 이름 설정 시간을 알 수 있음

FAT12/16/32 Directory Structure

Data Area ➔ Directory Entry (한글이름)

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00	Name								Extension			Attr	Rese rved	Create Time Tenths	Created Time	
0x10	Created Date		Last Accessed Date		Starting Cluster Hi		Last Written Time		Last Written Date		Starting Cluster Low		File Size			

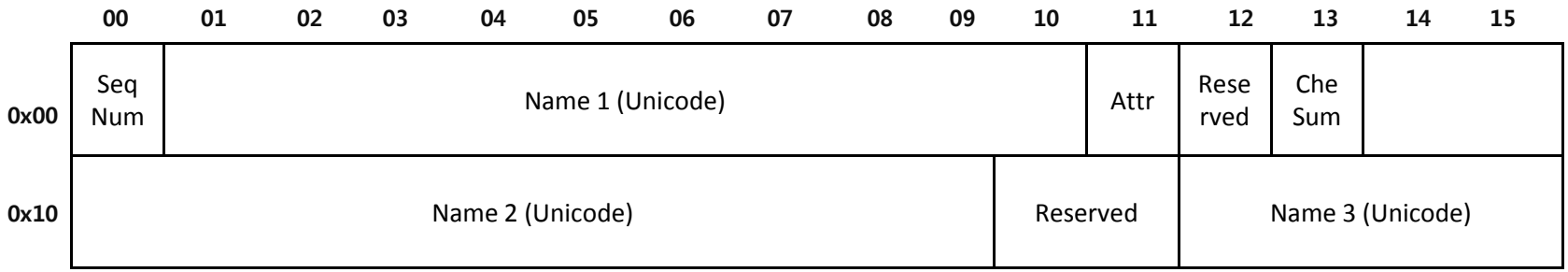
Text | Hex | Doc | Transcript | Picture | Report | Console | Details

```
320 C7 C1 B7 CE B4 CF BE EE 48 57 50 20 00 AB 29 8E  ÇÁ·Î´Ï¾îHWP ·«)Ž
336 54 3D 54 3D 00 00 FB 90 52 3D 77 6E 00 66 00 00  T=T=··û|R=wn·f··
352 E5 41 4D 50 4C 45 7E 31 44 4F 43 20 00 AD 97 99  åAMPLE~1DOC ·—™
```

- **한글 완성형 코드 값**
  - **프** : 0xC7C1
  - **로** : 0xB7CE
  - **니** : 0xB4CF
  - **어** : 0xBEEE

FAT12/16/32 Directory Structure

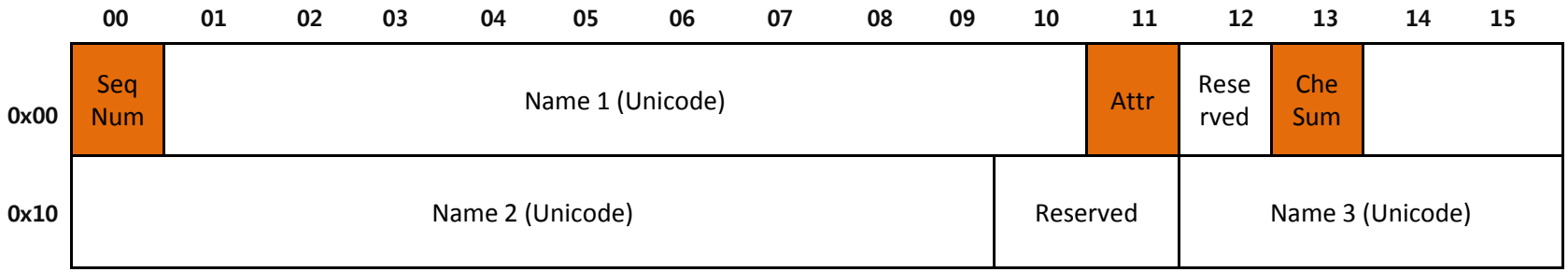
Data Area ➔ LFN (Long File Name) Entry



위 치	설 명
0 – 0	Sequence Number or Status Byte
1 – 10	LFN Character 1-5 (Unicode)
11 – 11	Attributes (0x0F)
12 – 12	Reserved
13 – 13	Checksum
14 – 25	LFN Character 6-11 (Unicode)
26 – 27	Reserved
28 – 31	LFN Character 12-13 (Unicode)

FAT12/16/32 Directory Structure

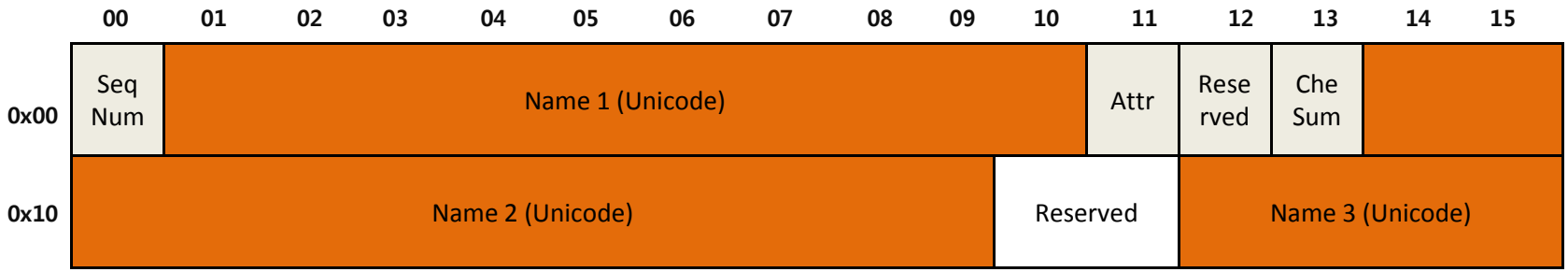
Data Area ➔ LFN (Long File Name) Entry



- **Sequence number / allocation status** :
  - 255 자 이하의 파일 이름 표현을 위해 하나 이상의 LFN 엔트리 사용
  - 1부터 시작하여 차례로 증가
  - 마지막 값은 "**증가값 | 0x40**" 으로 순서번호 생성
  - **0xE5** : 삭제된 LFN 엔트리
- **Attribute** : LFN 엔트리이므로 항상 0x0F 값
- **Checksum** : 파일 이름의 체크섬 값

FAT12/16/32 Directory Structure

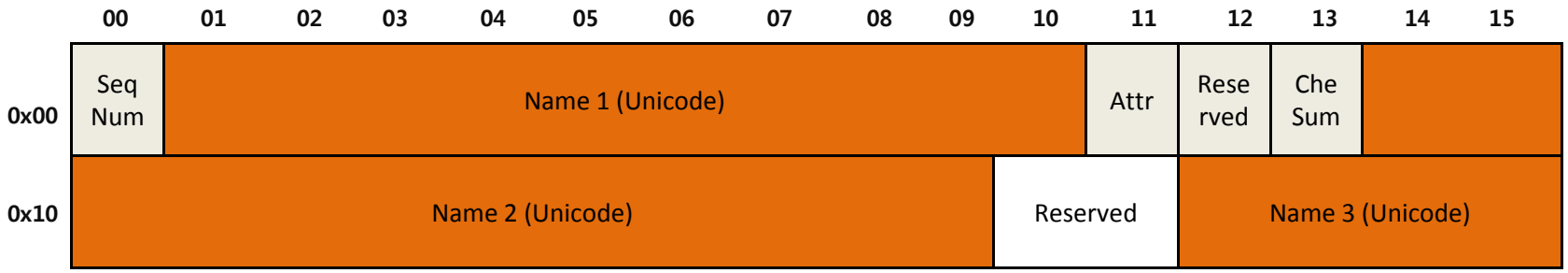
Data Area ➔ LFN (Long File Name) Entry

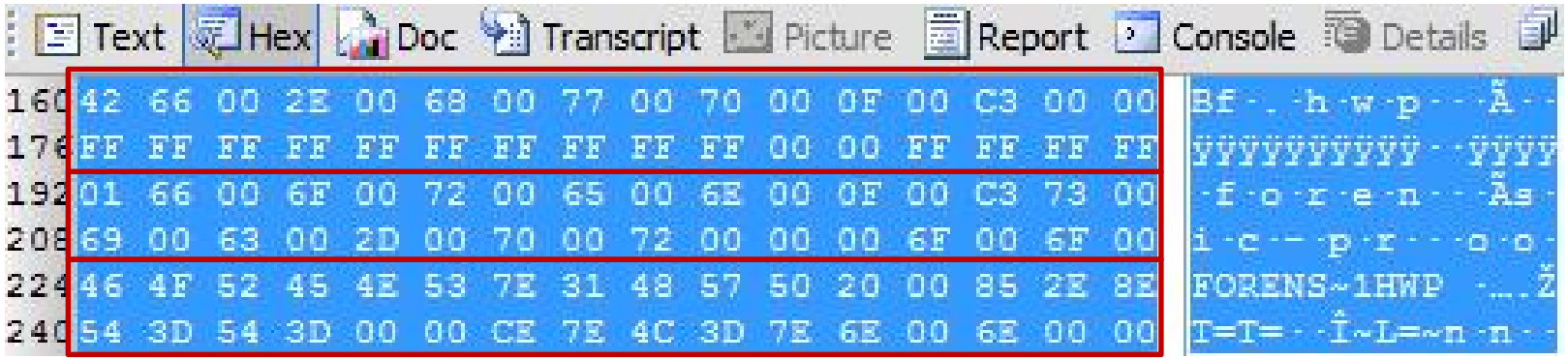


- **Name 1** : 유니코드 5 문자
- **Name 2** : 유니코드 6 문자
- **Name 3** : 유니코드 2 문자
- 하나의 LFN 엔트리는 총 유니코드 13 문자 표현 가능
- 최대 255 문자 할당 시 14개의 LFN 엔트리 필요
- 문자가 할당되지 않을 경우 0xFF로 패딩

FAT12/16/32 Directory Structure

Data Area ➔ LFN (Long File Name) Entry

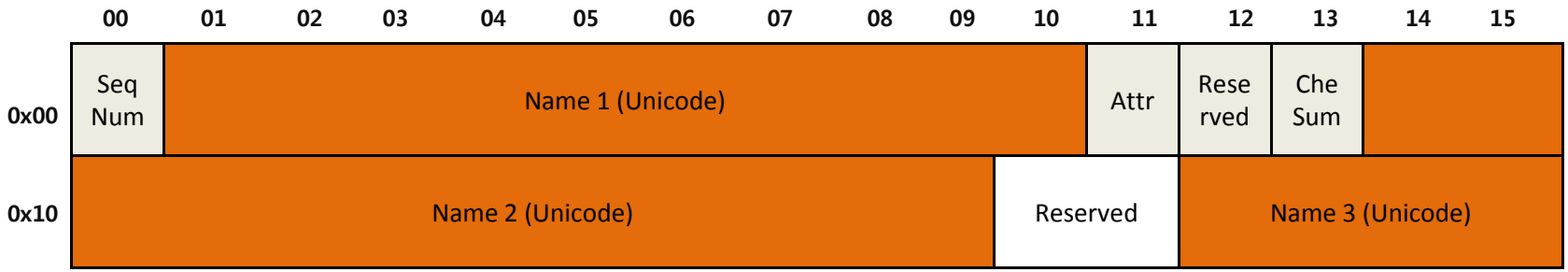


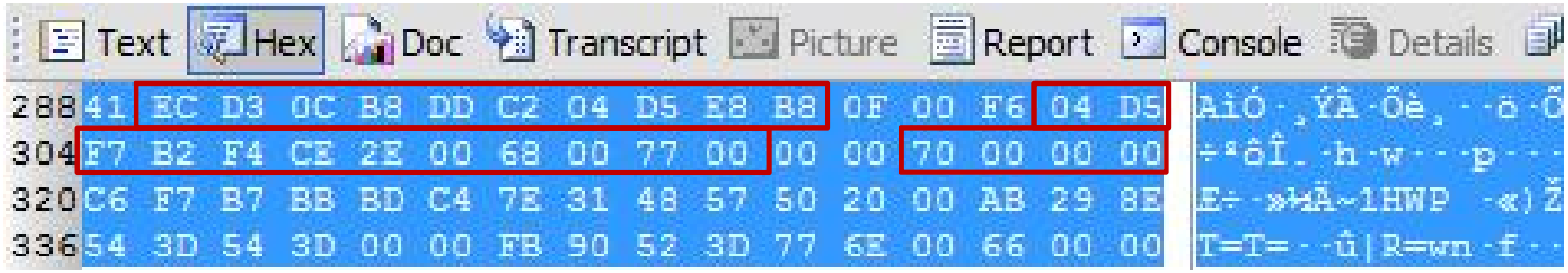


- **"forensic-proof.hwp" LFN 엔트리**
  - 짧은 이름 (Directory Entry)의 경우 짧은 이름 생성 규칙에 맞춰 8 바이트 이름 생성 "FORENS~1.HWP"
  - 순서 번호 증가 : 0x01 ➔ 0x42
  - 사용되지 않은 영역은 0xFF로 패딩

FAT12/16/32 Directory Structure

Data Area ➔ LFN (Long File Name) Entry (한글이름)





- **"포렌식프루프닷컴.hwp" 유니코드 값**
  - **포** : U+D3EC
  - **렌** : U+B80C
  - **식** : U+C2DD
  - **프** : U+D504
  - **루** : U+B8E8
  - **프** : U+D504
  - **닷** : U+B2F8
  - **컴** : U+CEF4

FAT12/16/32 Directory Structure

Data Area ➔ Example : Root Directory (Cluster 2)


```
000 43 4F 46 45 45 20 20 20 20 20 20 08 00 00 00 00   COFEE      ·····
016 00 00 00 00 00 00 0E 71 24 3B 00 00 00 00 00 00   ·······q$;······
032 E5 44 45 4C 54 45 4D 50 20 20 20 22 00 80 17 5A   åDELTEMP   "·€·Z
048 24 3B 24 3B 00 00 05 71 24 3B 03 00 00 70 60 3D   $;$;···q$;···p`=
064 E5 53 00 44 00 45 00 4C 00 54 00 0F 00 81 45 00   åS·D·E·L·T···□E·
080 4D 00 50 00 31 00 00 00 FF FF 00 00 FF FF FF FF   M·P·1···ÿÿ··ÿÿÿÿ
096 E5 44 45 4C 54 45 7E 31 20 20 20 22 00 17 04 71   åDELTE~1   "···q
112 24 3B 24 3B 00 00 05 71 24 3B 00 00 00 00 00 00   $;$;···q$;·····
128 E5 53 00 44 00 45 00 4C 00 4D 00 0F 00 5D 46 00   åS·D·E·L·M···]F·
144 54 00 30 00 30 00 30 00 30 00 00 00 30 00 30 00   T·0·0·0·0···0·0·
160 E5 44 45 4C 4D 46 7E 31 20 20 20 22 00 1A 04 71   åDELMF~1   "···q
176 24 3B 24 3B 00 00 05 71 24 3B 00 00 00 00 00 00   $;$;···q$;·····
192 42 49 4E 20 20 20 20 20 20 20 20 10 08 A0 0D 71   BIN        ··  q
208 24 3B 24 3B 03 00 0E 71 24 3B 02 00 00 00 00 00   $;$;···q$;·····
224 52 55 4E 4E 45 52 20 20 45 58 45 20 18 B2 15 71   RUNNER  EXE ·²·q
240 24 3B 2A 3B 03 00 AC 90 55 38 FE 00 69 60 0A 00   $;*;··¬□U8þ·i` ·
256 43 37 00 32 00 38 00 32 00 38 00 0F 00 CA 00 00   C7·2·8·2·8···Ê··
272 FF FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
288 02 45 00 45 00 52 00 2D 00 32 00 0F 00 CA 30 00   ·E·E·R·-·2···Ê0·
304 30 00 39 00 30 00 39 00 30 00 00 00 34 00 31 00   0·9·0·9·0···4·1·
320 01 6F 00 75 00 74 00 2D 00 43 00 0F 00 CA 49 00   ·o·u·t·-·C···ÊI·
336 53 00 54 00 2D 00 50 00 52 00 00 00 4F 00 4E 00   S·T·-·P·R···O·N·
352 4F 55 54 2D 43 49 7E 31 20 20 20 10 00 8B 8E 8B   OUT-CI~1   ··‹Ž‹
368 24 3B 24 3B 03 00 8F 8B 24 3B D8 0D 00 00 00 00   $;$;··□‹$;Ø ····
384 52 45 43 59 43 4C 45 52 20 20 20 17 00 BB 82 7E   RECYCLER   ··»‚~
400 28 3B 28 3B 00 00 83 7E 28 3B 7F 48 00 00 00 00   (;(;··ƒ~(;□H····
416 41 55 54 4F 52 55 4E 20 49 4E 46 27 18 A8 83 7E   AUTORUN INF'·¨ƒ~
432 28 3B 2B 3B 00 00 8B 7E 28 3B 85 48 1A 01 00 00   (;+;··‹~(;…H····
448 E5 49 00 6D 00 6A 00 69 00 6E 00 0F 00 BC 2E 00   åI·m·j·i·n···Œ.·
464 62 00 6D 00 70 00 00 00 FF FF 00 00 FF FF FF FF   b·m·p···ÿÿ··ÿÿÿÿ
480 E5 4D 4A 49 4E 20 20 20 42 4D 50 20 00 4E 86 7E   åMJIN   BMP ·N†~
496 28 3B 28 3B 00 00 6F 7E 28 3B 86 48 6F FA 0F 00   (;(;··o~(;†Hoú··
```

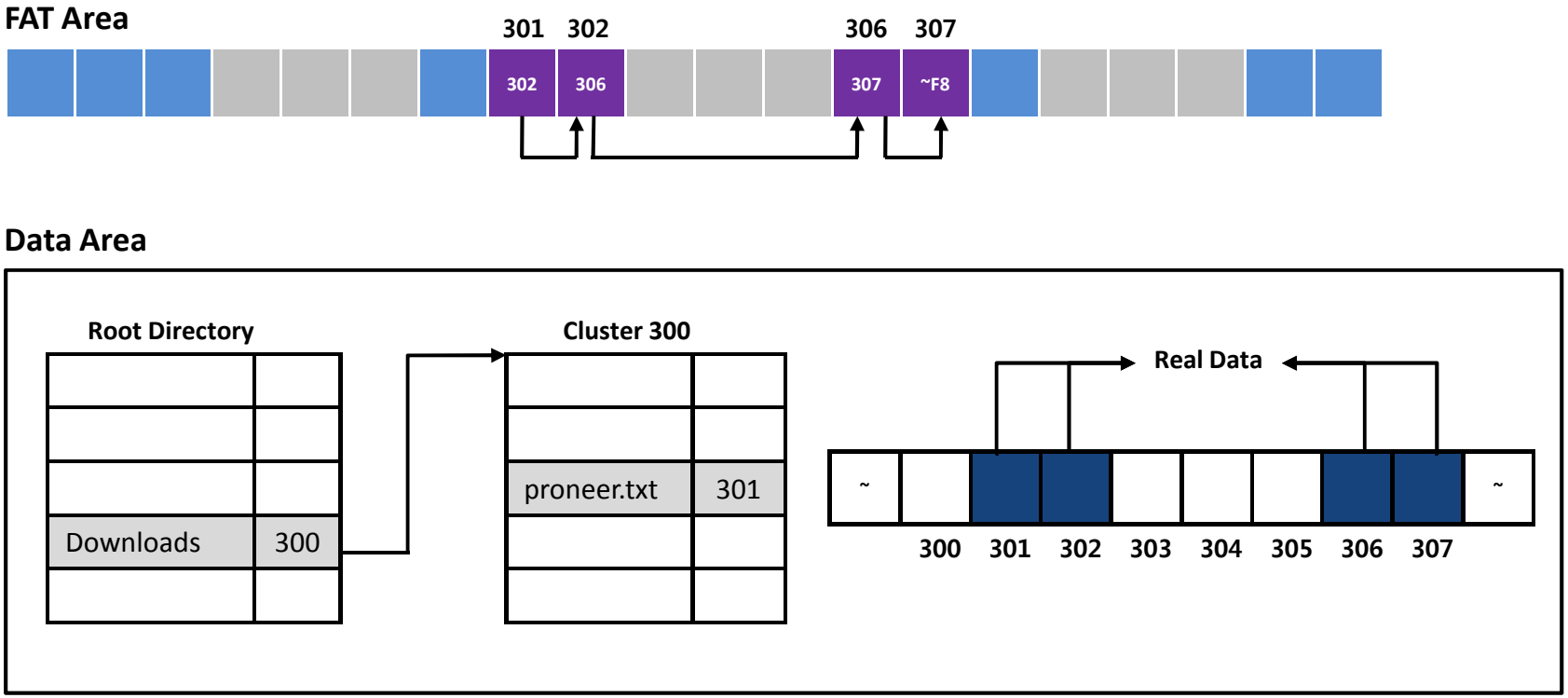
FAT12/16/32 Example

Security is a people problem…

FAT12/16/32 Example

File Allocation

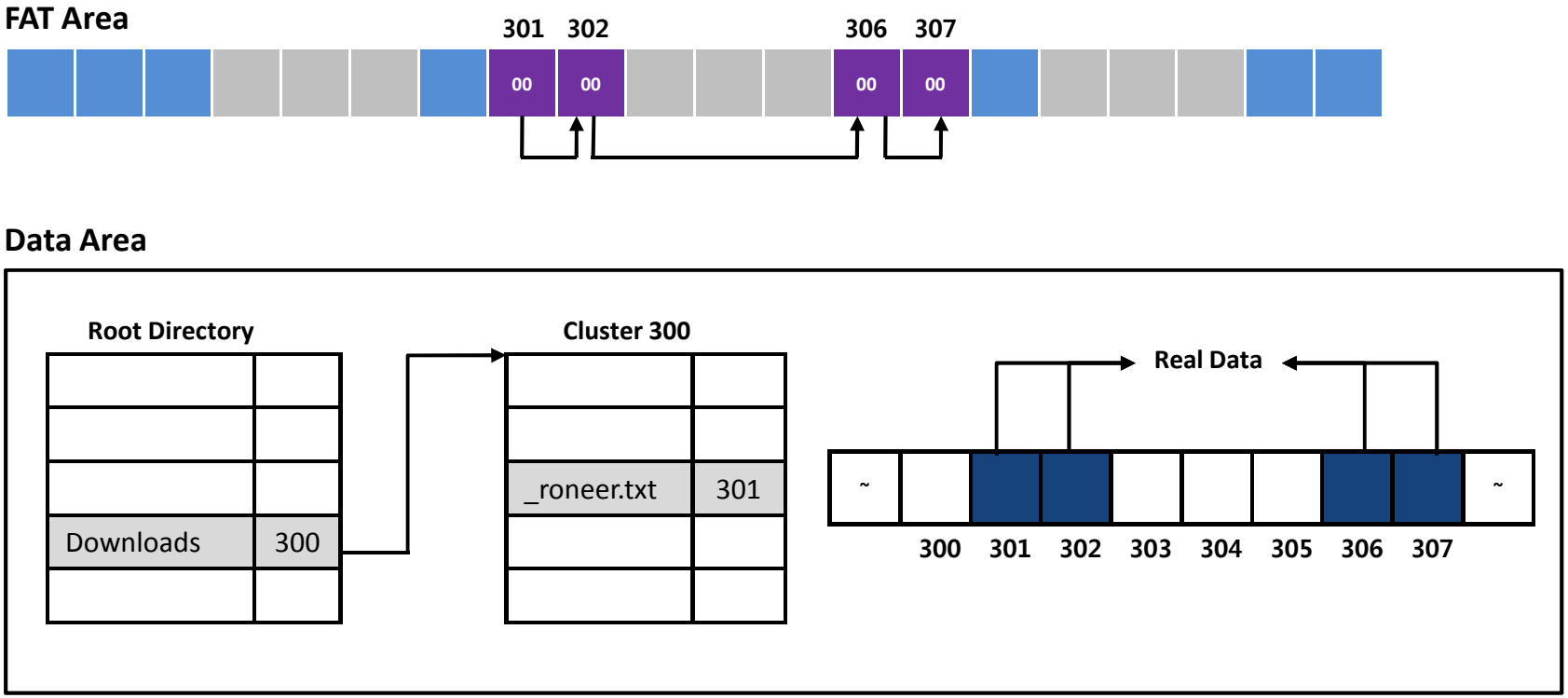
- C:\Downloads\proneer.txt (13KB)
- Cluster Size : 4K



FAT12/16/32 Example

File Deletion

- C:\Downloads\proneer.txt (13KB)
- Cluster Size : 4K



FAT12/16/32 Example

Wasted Area Analysis

- MBR 슬랙
- FAT32의 예약된 영역 내의 낭비되는 섹터 (1, 2, 3, 6, 7, 8 섹터 제외)
- FAT32의 예약된 영역의 추가적인 부트 코드 영역 (섹터 3, 8)
- FSINFO 구조체 영역 (섹터 2, 7)의 사용되지 않는 영역
- 파일 슬랙 (램 슬랙, 드라이브 슬랙), 파일시스템 슬랙, 볼륨 슬랙

Quiz !

Security is a people problem…

Quiz !

FAT12/16/32

- 디렉터리 엔트리의 크기는?
- FAT12/16/32에서 각 파티션의 예약된 영역 크기는?
- FAT32의 경우 예약된 영역에서 사용되지 않는 섹터 수는?
- 파일 시간 정보의 위치는?
- 파일 확장자의 위치는?
- FAT32의 최대 표현 가능한 클러스터 수는?

Quiz !

FAT12/16/32

- 예약된 영역의 부트 섹터 부트 코드의 역할은?
- FDISK를 사용하여 포맷할 경우의 상태 및 복구 방안은?
- 비할당 클러스터 판별법은?
- 삭제된 파일 및 디렉터리 판별법은?
- 덮어써진 파일 판별법은?

Question & Answer