forensic-proof.com

exFAT (Extended FAT) File System

Twitter : @pr0neer

Blog : forensic-proof.com

Email : proneer@gmail.com

Kim Jinkook

Outline

1. exFAT File System

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

exFAT Introduction

Security is a people problem…

exFAT Introduction

Introduction

- exFAT (Extended FAT) : 확장 파일 할당 테이블
- 마이크로소프트에서 새롭게 발표한 파일시스템 (FAT64라고도 불림)
- 등장 배경
  - 외장형 장치
  - 대용량 멀티미디어 파일
  - 오버헤드의 최소화
  - TFAT (Transactional FAT) 과의 호환성

exFAT Introduction

Timeline (Key Dates)

- **2006년 11월** : 윈도우 CE 6.0 에서 소개
- **2008년 03월** : exFAT 호환성을 가진 비스타 서비스팩 1 출시
- **2009년 01월** : SDXC (Secure Digital eXtended Capacity) 메모리카드 명세 발표, 파일시스템으로 exFAT 채택
- **2009년 01월** : exFAT을 지원하는 윈도우 XP 드라이버 발표
- **2009년 03월** : Pretec에서 최초로 SDXC 카드 출시
- **2009년 12월** : exFAT 라이선스 프로그램 발표
- **2009년 12월** : Diskinternals에서 exFAT 복구 프로그램 발표

exFAT Introduction

SDXC?

- 다양한 플래시 메모리 카드 모델 (SD vs. CF)
- SD와 SDHC 카드의 후속 모델
- 크기는 기존 제품과 동일하지만 용량(최대 2 TB)과 성능 면에서 강점

exFAT Introduction

Supported Operating Systems

- Windows Vista SP1
- Windows XP SP 2 (with updates)
- Windows XP SP 3 (with updates)
- Windows Server 2003
- Windows Server 2008
- Windows 7
- Windows CE 6.0

exFAT Introduction

Getting the drives put onto Windows XP

- KB955704 업데이트 패치를 통해 가능

  http://www.microsoft.com/downloads/en/details.aspx?FamilyID=1cbe3906-ddd1-4ca2-b727-c2dff5e30f61&displaylang=en

exFAT Introduction

Summary of exFAT Features

- 가변형 섹터 크기 (512 ~ 4096 바이트)
- 최대 클러스터 크기 (32 MB)
- 하위 디렉터리 (256 MB)
- NTFS의 특징을 가지지만 NTFS보다 낮은 오버헤드
- TexFAT (Transactional exFAT) 호환
- ACL (Access Control List), UTC (Universal Time, Coordinated) Timestamp 지원
- OEM 파라미터 섹터
- 9섹터 크기의 VBR (Volume Boot Record) 영역 (대용량 부트 프로그램 가능)
- 하위 디렉터리 파일 개수 증가 (최대 2,796,202개)

exFAT Introduction

Scalability and Limitations

- 파일 크기 : 128 PB (이론적으로 64 ZB, 마이크로소프트는 512 TB 권장)
- 디렉터리 당 최대 파일 개수 : 2,796,202
- 파일 이름 최대 길이 : 255 문자
- 볼륨 크기 : 16 EB (이론적으로는 64 ZB, 마이크로소프트는 512 TB 권장)

단위			바이트
KB	Kilobyte	2^{10}	1024
MB	Megabyte	2^{20}	1024 KB
GB	Gigabyte	2^{30}	1024 MB
TB	Terabyte	2^{40}	1024 GB
PB	Petabyte	2^{50}	1024 TB
EB	Exabyte	2^{60}	1024 PB
ZB	Zetabyte	2^{70}	1024 EB

exFAT Introduction

Maximum Volume and File Limitations

	FAT 12	FAT 16	FAT 32	NTFS	UDF	exFAT
최대 볼륨 크기	32 MB	2 GB	2 TB	16 TB	2 TB	128 PB
최대 파일 크기	4 GB	4 GB	4 GB	16 EB	16 EB	16 EB
복잡성 / 성능	Low	Low	Low	High	Low	Low
고장 저항력 (Fault Tolerance)	No	No	No	Yes	No	Yes
객체 권한 (Object Permissions)	No	No	No	Yes	No	Yes
파일 이름 최대 길이	255	255	256	256	127 Unicode 254 ASCII	255 Unicode

How to Identify exFAT Capability

- 시스템 파일
  - exfat.sys – %SystemRoot%₩System32₩Drivers₩
  - format.com – "exFAT" 옵션 포함 여부
  - uexfat.dll – %SystemRoot%₩System32₩

- 수정된 파일
  - fmifs.dll
  - fs_rec.sys
  - ifutil.dll
  - Shell32.dll
  - ulib.dll
  - xpsp3res.dll

exFAT Introduction

How to Identify exFAT Capability

- XP 레지스트리 키
  - SOFTWARE₩Microsoft₩Updates₩Windows XP₩SP4₩KB955704
  - SYSTEM₩%Current Control Set%₩Enum₩Root₩LEGACY_EXFAT
  - SYSTEM₩%Current Control Set%₩Services₩exFAT
  - 그 밖에 "exFAT"을 가지는 키

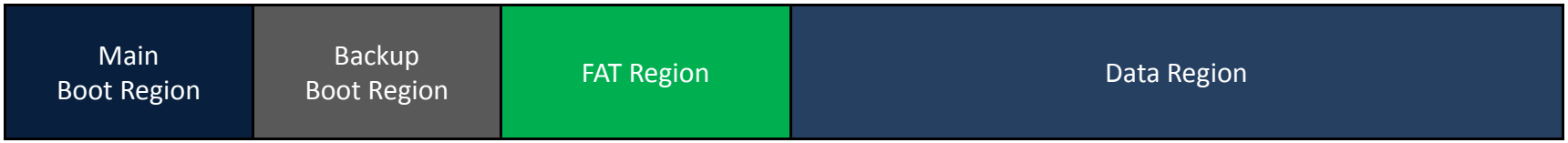
- Vista 레지스트리 키
  - SYSTEM₩%Current Control Set%₩Enum₩Root₩LEGACY_EXFAT
  - SYSTEM₩%Current Control Set%₩Services₩Eventlog₩System₩exFat
  - SYSTEM₩%Current Control Set%₩Services₩exFAT
  - 그 밖에 "exFAT"을 가지는 키

exFAT Internals

Security is a people problem…

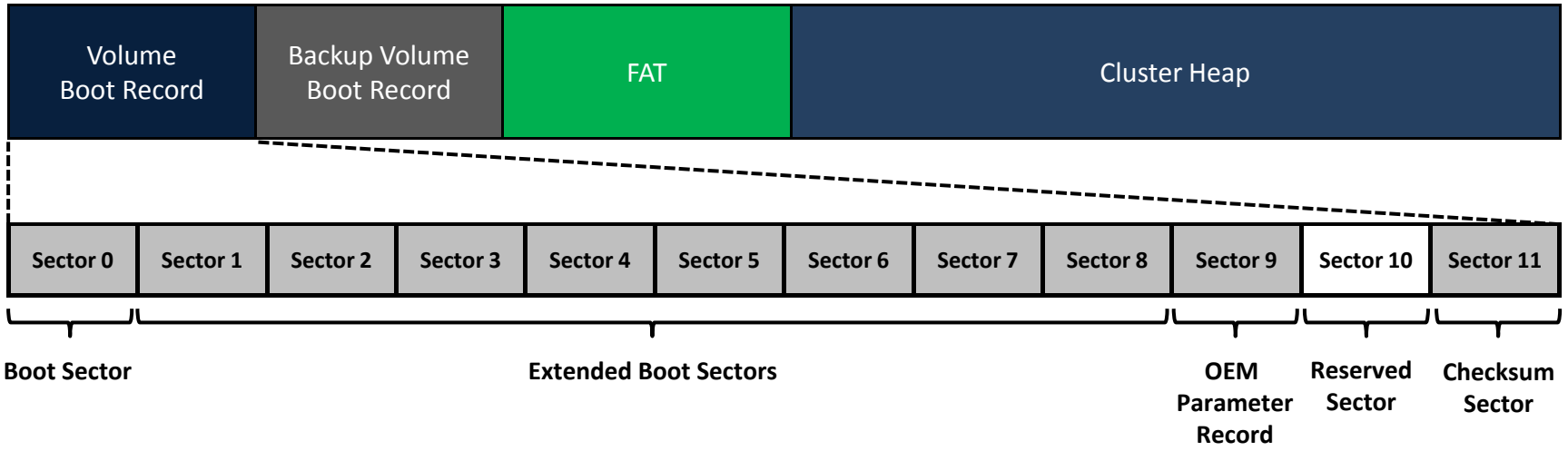
exFAT Internals

Volume Structure



exFAT Internals

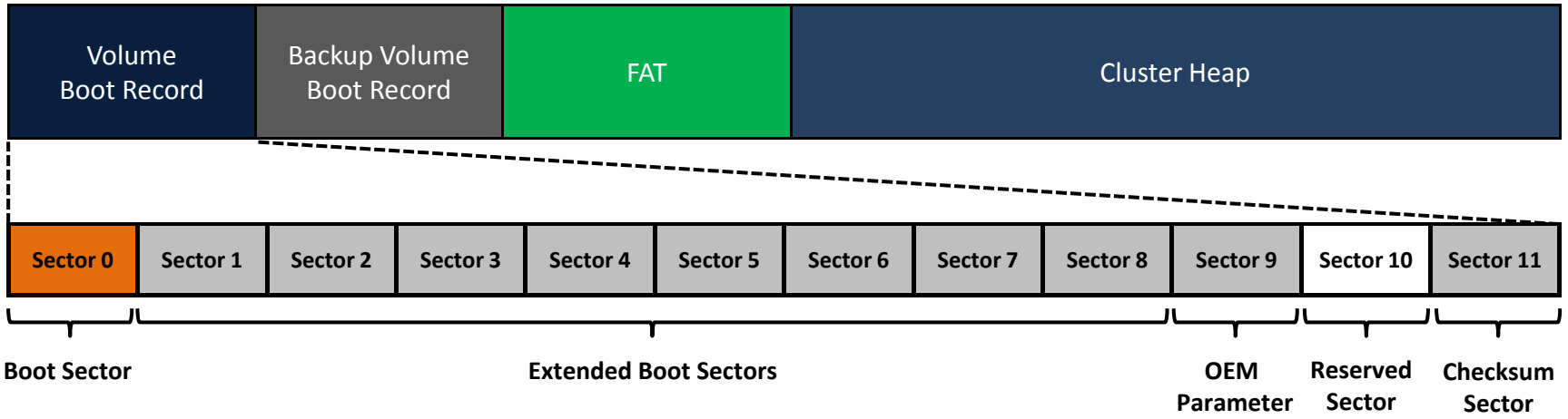
Volume Structure



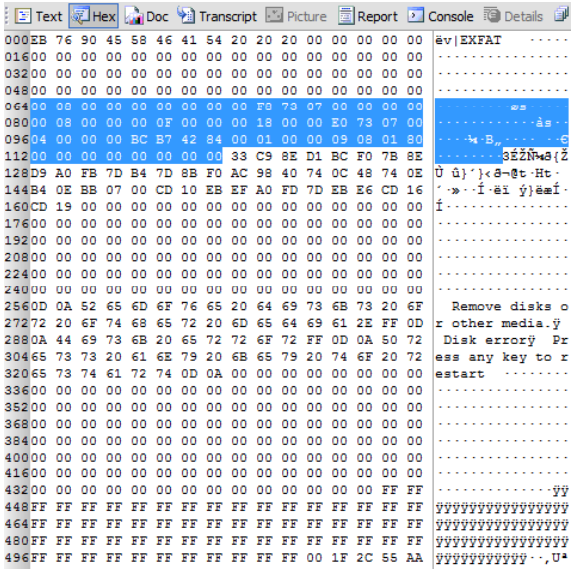
- **Boot Sector** : BIOS Parameter Block (BPB), 부트 코드, 시그니처
- **Extended Boot Sectors** : 추가적인 부트 코드 ➔ 대용량 부트 프로그램
- **OEM Parameter Record** : 공장에서 매체 제조사에 의해 기록된 내용
- **Reserved Sector** : 현재 정의되어 있지 않음
- **Checksum Sector** : 이전 11 섹터에 대한 체크섬 값
- VBR의 마지막 3 섹터는 부트 시그니처(0x55AA)가 존재하지 않음

exFAT Internals

VBR – Boot Sector



범 위	설 명
0 – 2	Jump Command to boot code
3 – 10	File System Name
11 – 63	Previously FAT Compatible
64 – 119	BIOS Parameter Block
120 – 509	Boot Program
510 – 511	Signature (0xAA55)

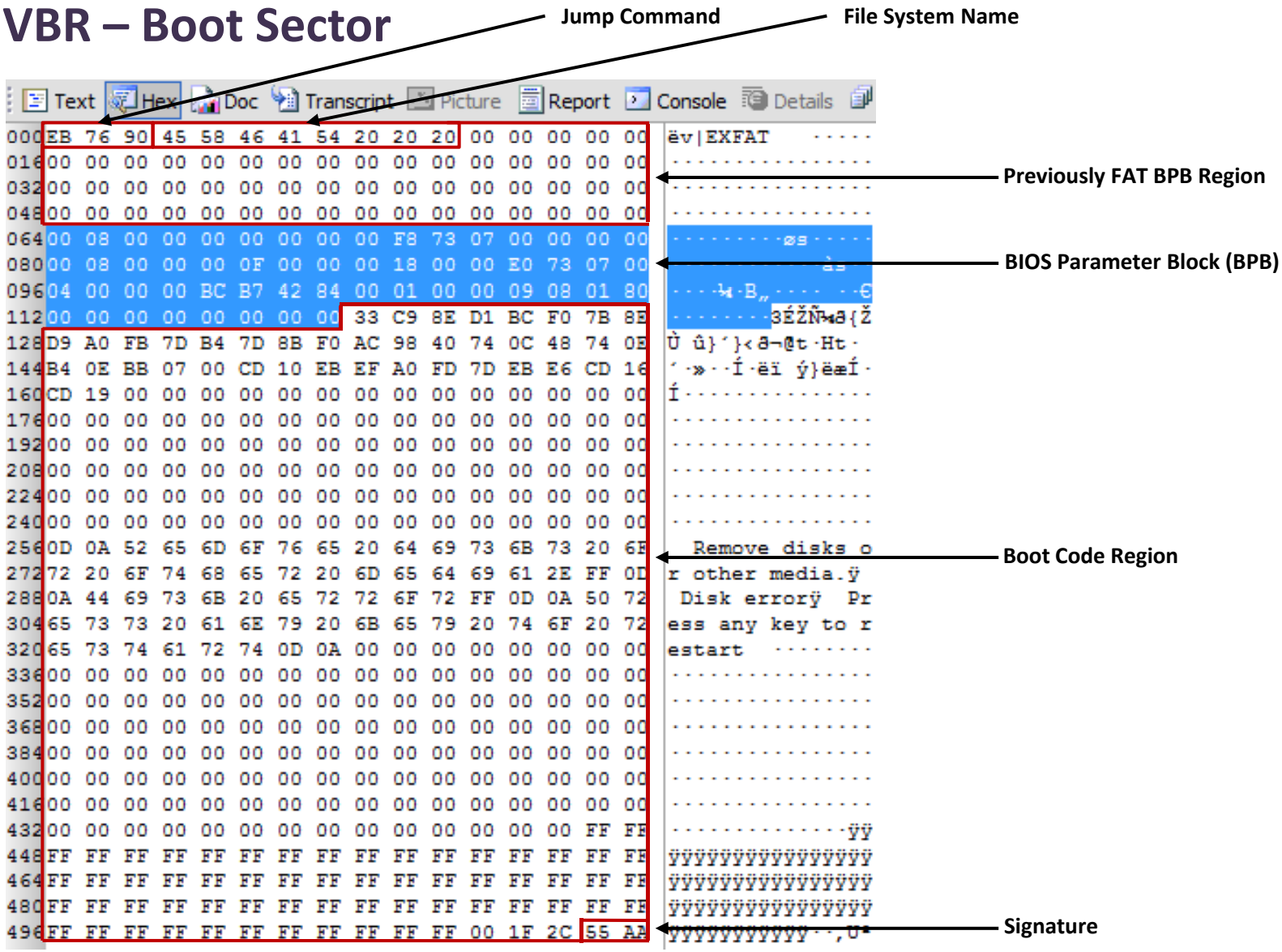


VBR – Boot Sector

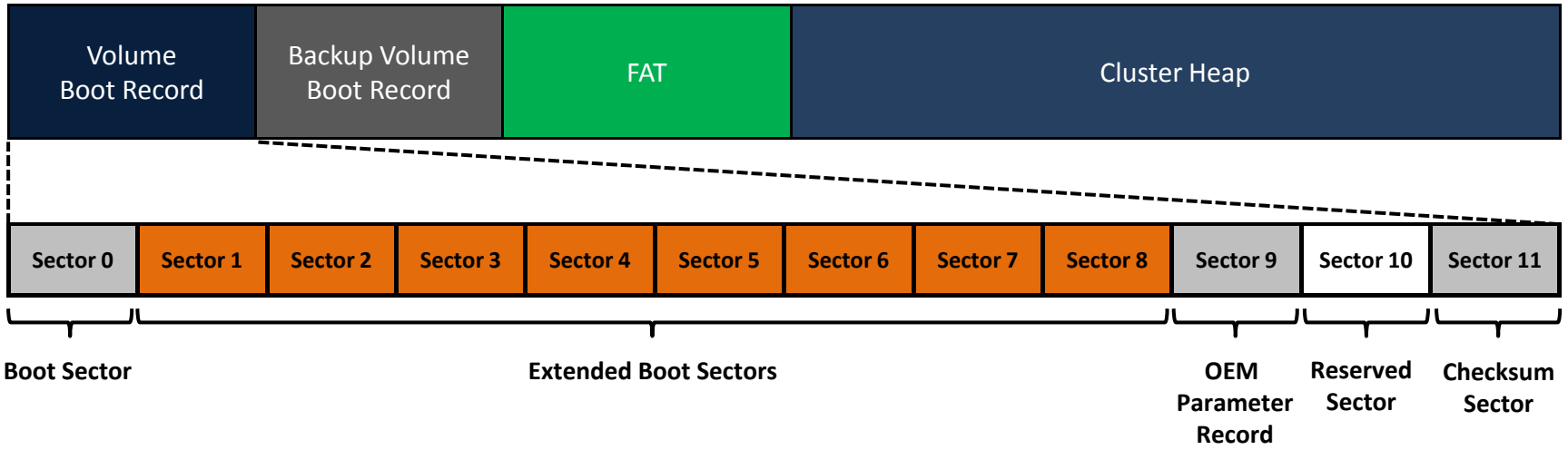
필드명	위치 (바이트)	크기 (바이트)	설명/값
Jump Boot	0	3	0xEB7690
File System Name	3	8	“EXFAT “
Must Be Zero	11	53	반드시 0x00 (기존 FAT 간의 오류를 막기 위해 존재)
Partition Offset	64	8	파티션 위치 섹터 주소
Volume Length	72	8	볼륨에 할당된 총 섹터 수
FAT Offset	80	4	1st FAT의 섹터 주소
FAT Length	84	4	FAT에 할당된 총 섹터 수
Cluster Heap offset	88	4	데이터 영역의 섹터 주소
Cluster Count	92	4	데이터 영역의 총 클러스터 수
Root Directory First Cluster	96	4	루트 디렉터리의 클러스터 주소
Volume Serial Number	100	4	볼륨 시리얼 번호
File System Revision	104	2	파일시스템 변경 사항
Volume Flags	106	2	볼륨 플래그
Bytes Per Sector	108	1	섹터 당 바이트 수
Sectors Per Cluster	109	1	클러스터 당 섹터 수
Number of FATs	110	1	FAT 개수
Drive Select	111	1	INT 13h 사용을 위해 존재
Percent In Use	112	1	데이터 영역의 사용 량
Reserved	113	7	
Boot Code	120	390	부트 프로그램
Boot Signature	510	2	0xAA55

exFAT Internals

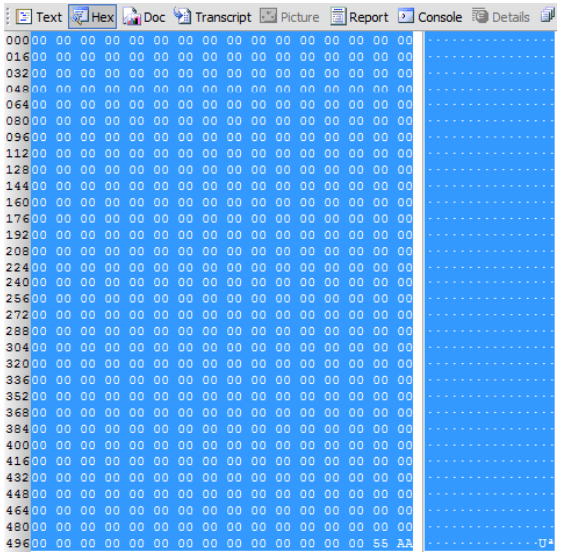
VBR – Boot Sector



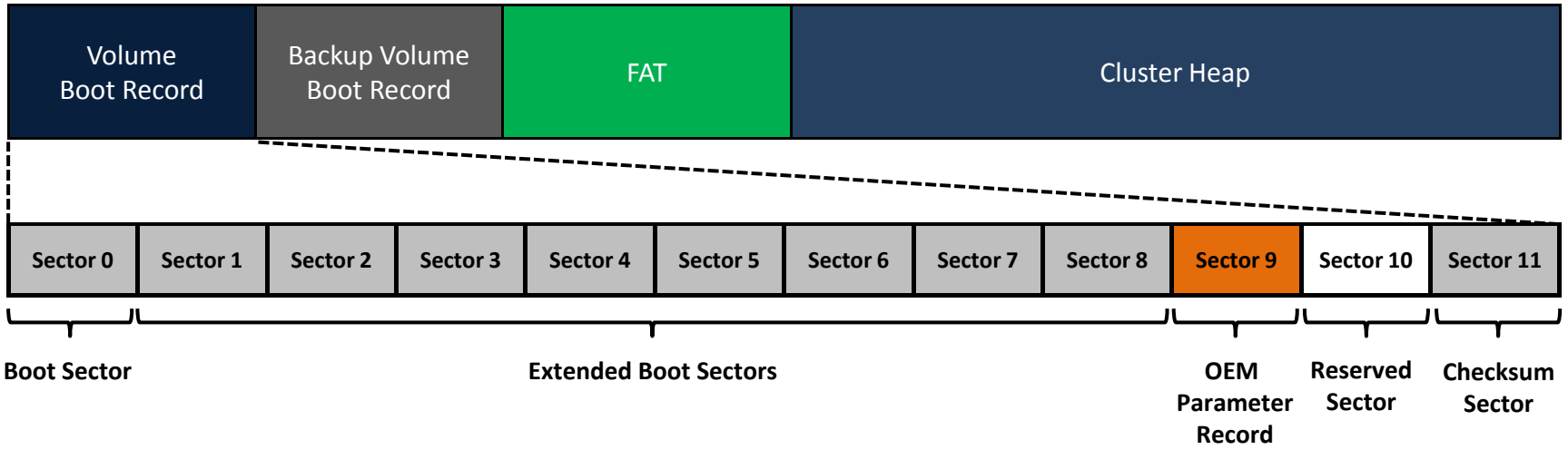
VBR – Extended Boot Sector



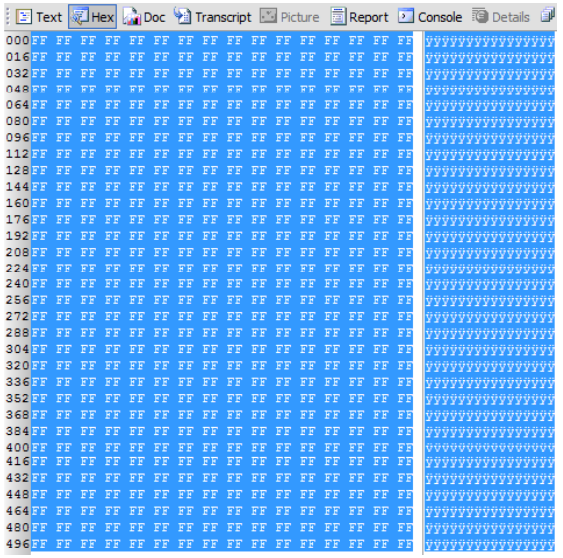
- **Extended Boot Sectors** : 추가적인 부트 코드 ➔ 대용량 부트 프로그램
- 별도의 부트 코드가 기록되지 않을 경우 0x00으로 채워짐
- 시그니처는 0xAA55



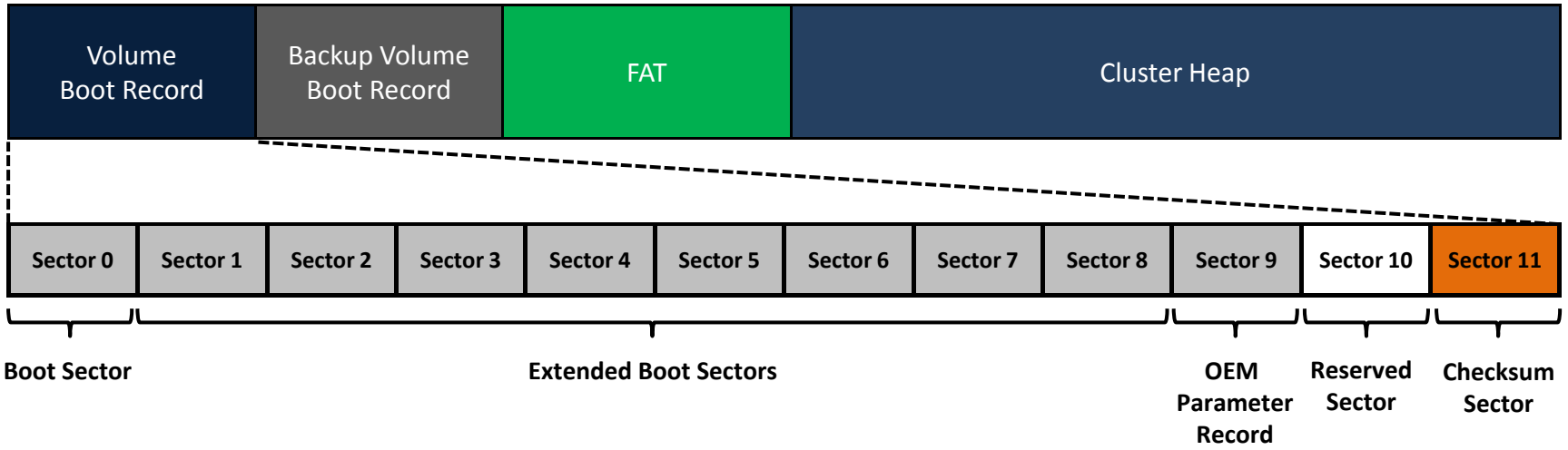
VBR – Extended Boot Sector



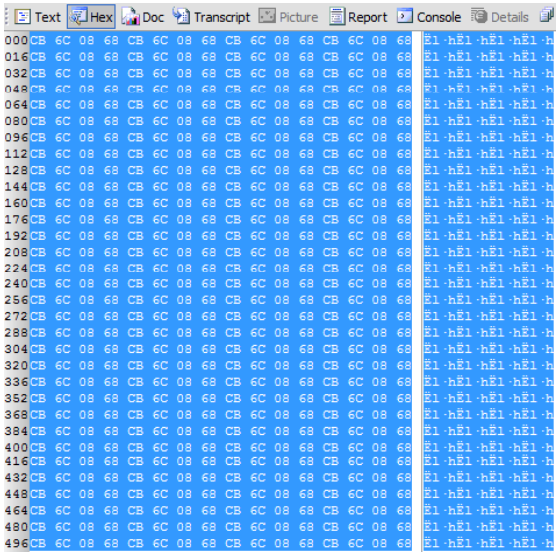
- **OEM Parameter Record** : 공장에서 매체 제조사에 의해 기록된 내용
  - HDD에서는 현재 사용되고 있지는 않음
  - 포맷 시 지워지지 않음 (완전삭제는 예외)
- **Parameter Field**
  - 48 바이트의 10개 필드
  - 16 바이트 GUID + 32 바이트 파라미터



VBR – Extended Boot Sector

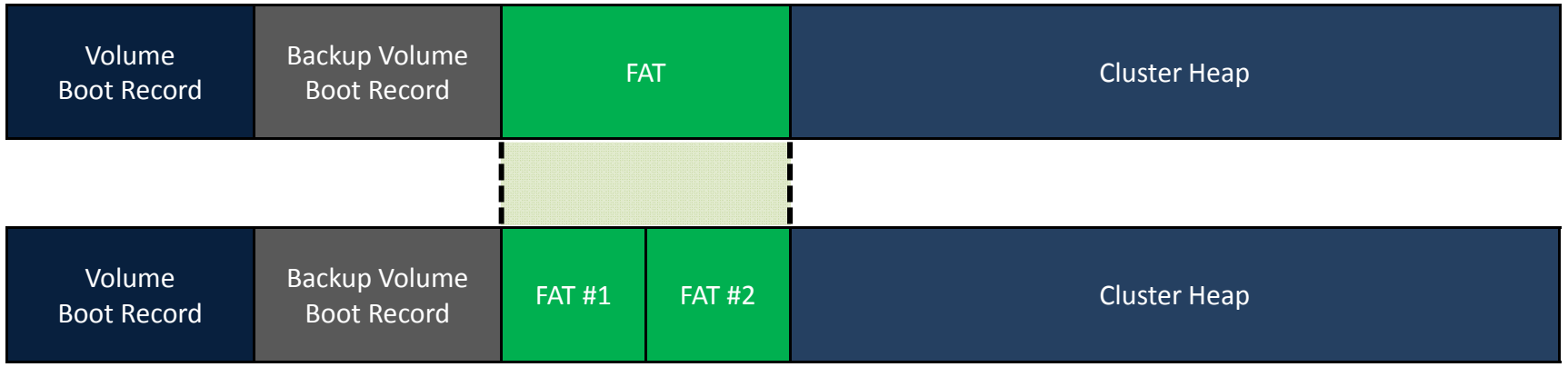


- **Checksum Sector** : 이전 11 섹터에 대한 체크섬 값
  - 0x68086CCB
  - 4 바이트 체크섬 값 반복



exFAT Internals

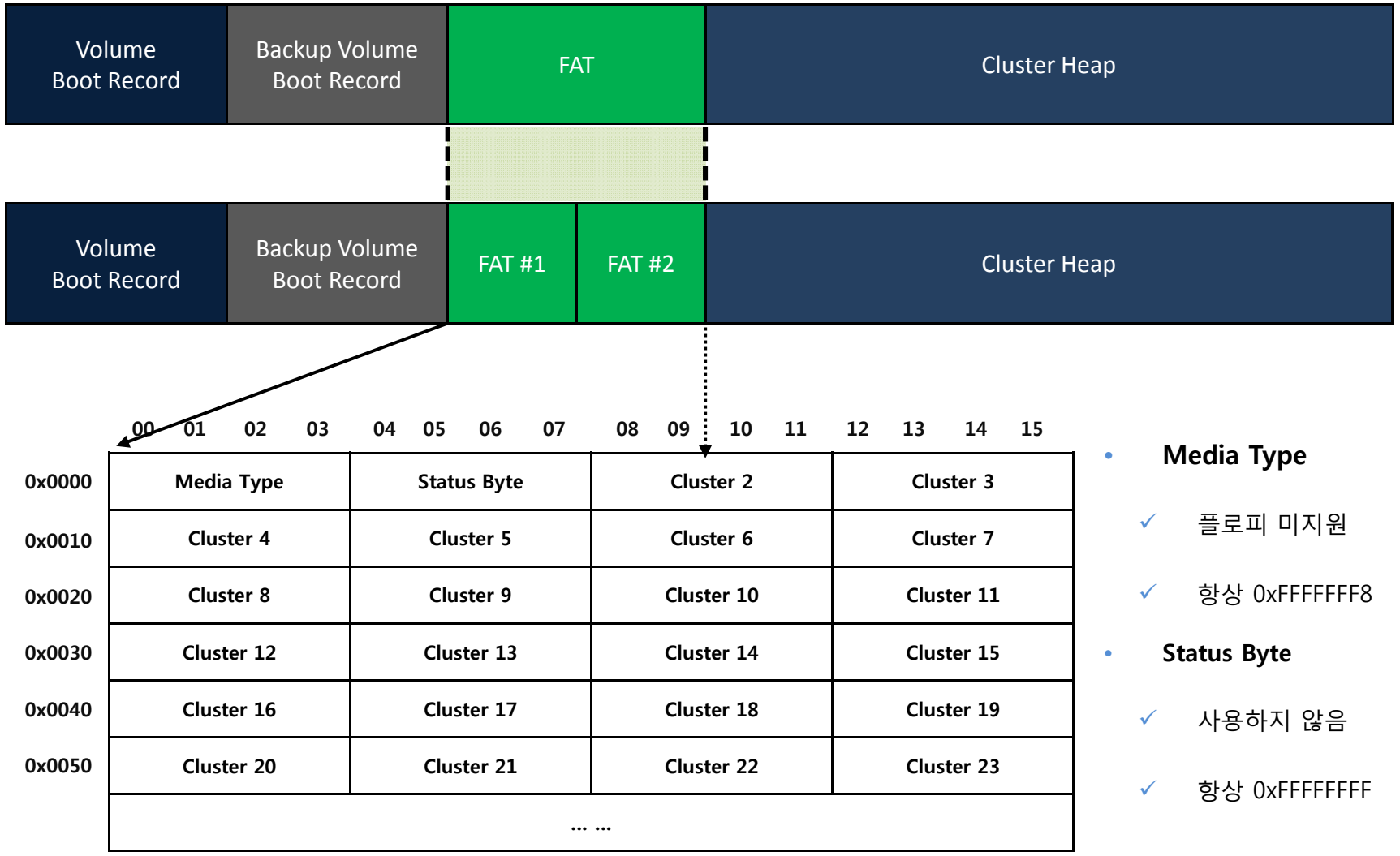
File Allocation Table (FAT)



- FAT #2 : TexFAT 에서만 지원
  - 버전 1.0에서는 Transactional exFAT (TexFAT) 미지원
- FAT #2는 FAT #1과 항상 다음에 존재하며 동일한 크기
- FAT12/16/32에서 FAT의 역할은 클러스터 체인과 할당 상태
- exFAT에서는 할당 상태 역할은 제외 ➔ 비트맵을 통해 관리 ➔ I/O 성능 향상
- 연속적인 클러스터 할당일 경우 FAT 사용 X, 비연속적일 경우에 클러스터 체인으로만 활용

exFAT Internals

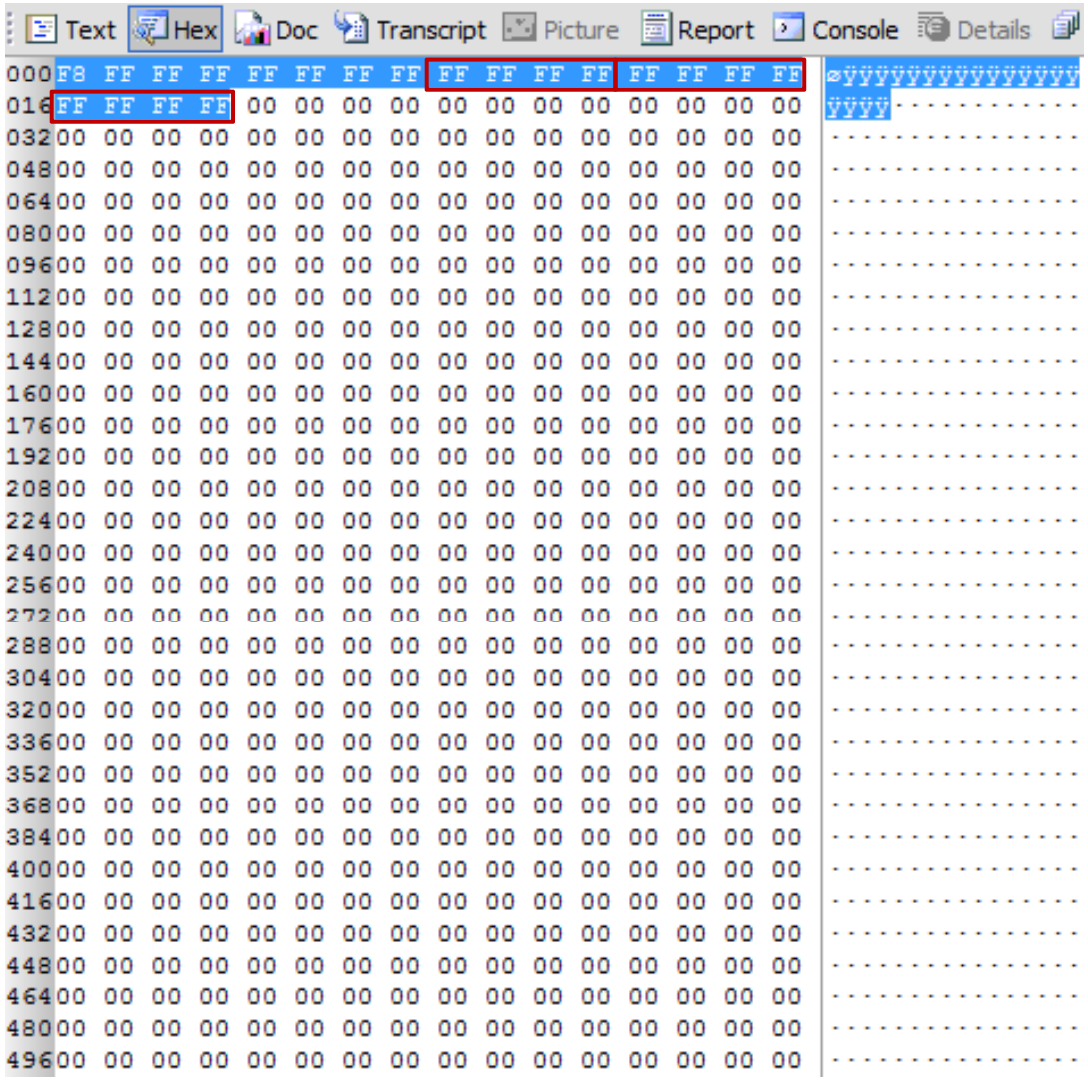
File Allocation Table (FAT)



- **Media Type**
  - ✓ 플로피 미지원
  - ✓ 항상 0xFFFFFFF8
- **Status Byte**
  - ✓ 사용하지 않음
  - ✓ 항상 0xFFFFFFFF

exFAT Internals

File Allocation Table (FAT) ➔ As soon as media is formatted

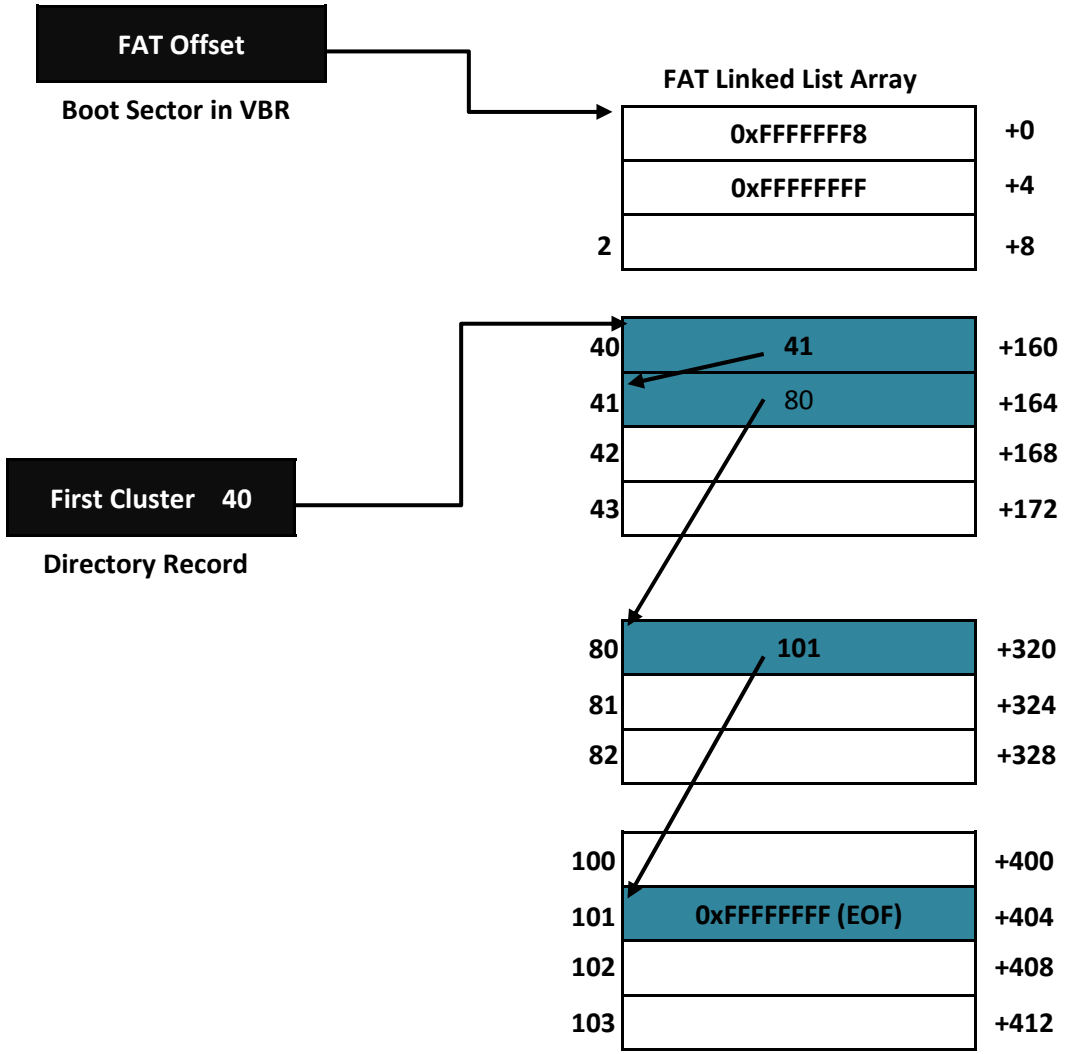


- **0x00000000** : No significant meaning
- **0x00000001** : Not a valid cell value
- **0xFFFFFFF6** : Largest Value
- **0xFFFFFFF7** : Bad Block
- **0xFFFFFFF8** : Media Descriptor
- **0xFFFFFFF9 ~ E** : Not Defined
- **0xFFFFFFFF** : End of File (EOF)

- **Cluster 2** : Allocation Bitmap
- **Cluster 3** : UP-Case Table
- **Cluster 4** : Root Directory

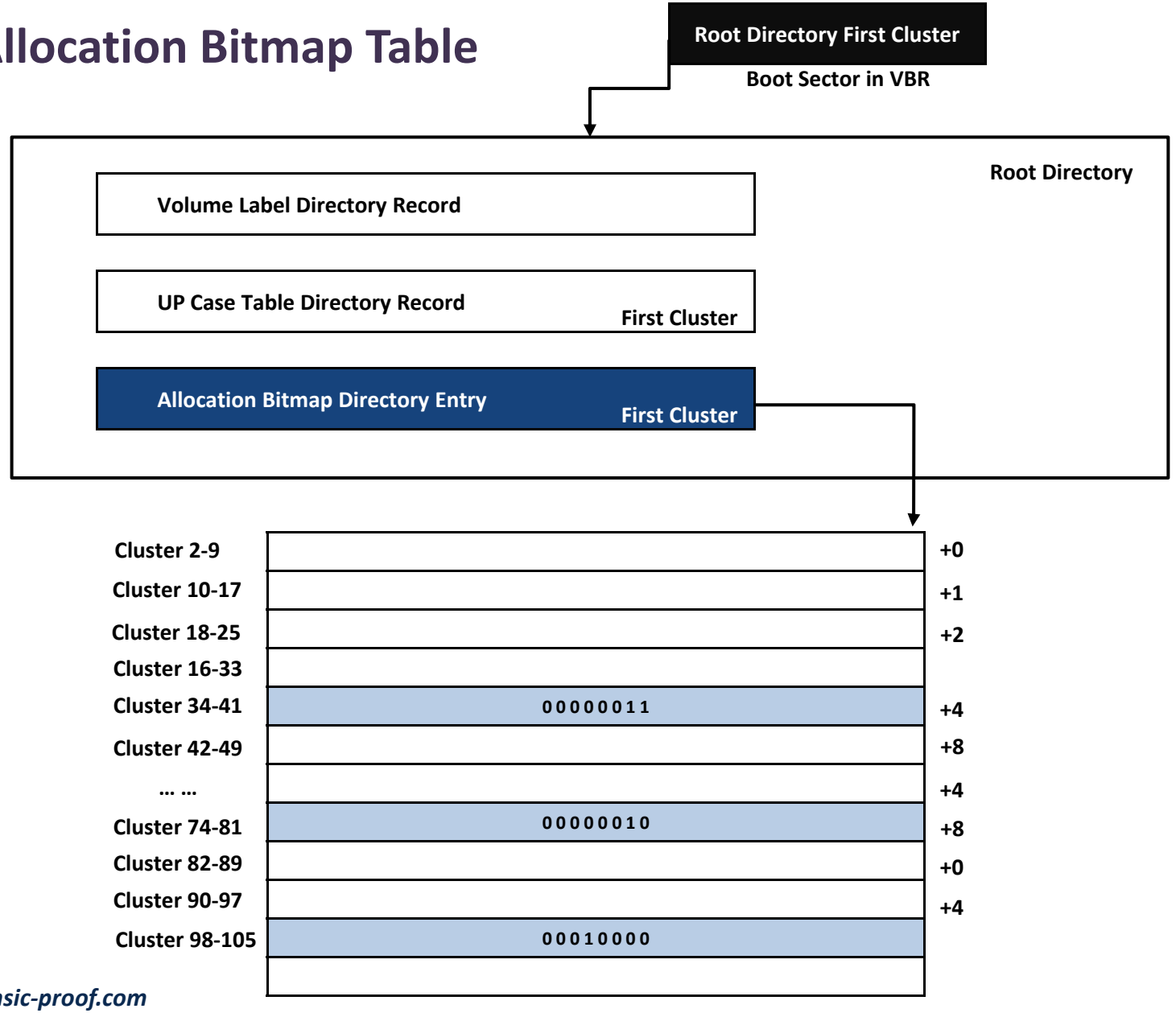
exFAT Internals

File Allocation Table (FAT) ➔ FAT Example

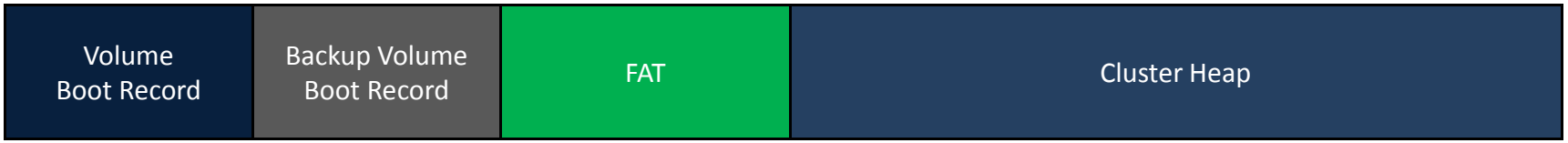


exFAT Internals

Allocation Bitmap Table



Cluster Heap



- **Cluster Heap**
  - exFAT 파일시스템의 데이터 영역
  - 루트 디렉터리
  - 하위 디렉터리
  - UP-Case 테이블
  - Allocation Bitmap
  - 파일

exFAT Directory Structure

Security is a people problem…

exFAT Directory Structure

Root Directory

- 하위 디렉터리, 파일, 볼륨 레이블, UP-Case 테이블 위치, 할당 비트맵(Allocation Bitmap) 위치 등으로 사용
- TexFAT (Transactional FAT), ACL (Access Control List)은 현재 윈도우 CE 버전에서만 지원
- 각 파일 및 디렉터리는 3 ~ 19 개의 엔트리 사용
- 디렉터리 엔트리
  - 32 바이트 크기
  - 첫 바이트 형식 코드 (Type Code)를 통해 해당 엔트리의 상태 및 목적을 나타냄

exFAT Directory Structure

Root Directory ➔ Type Code

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		4.0 KB					672
proDIR		4.0 KB	2010-10-22 20:2...	2010-10-22 20:2...	2010-10-22 20:2...		680
$Bitmap		7.6 KB					640
$UpCase		5.7 KB					656
forensic_example.txt	txt	188 B	2010-10-22 20:2...	2010-10-06 19:1...	2010-10-22 20:2...	A	688

File system: exFAT

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:

Cluster No.: 6
(Root directory)
\

Snapshot taken 17 min. ago

Used space: 0.9 MB
950,272 bytes

Free space: 244 MB
255,619,072 bytes

Total capacity: 245 MB
256,900,608 bytes

Bytes per cluster: 4,096
Free clusters: 62,407
Total clusters: 62,639

Bytes per sector: 512
Sector count: 501,759

Physical disk: 3

Display time zone: UTC +09:00
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 30x16=600

Window #: 2
No. of windows: 2

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00054000	03	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00054010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00054020	81	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00054030	00	00	00	00	02	00	00	00	96	1E	00	00	00	00	00	00
00054040	82	00	00	00	0D	D3	19	E6	00	00	00	00	00	00	00	00
00054050	00	00	00	00	04	00	00	00	CC	16	00	00	00	00	00	00
00054060	85	02	16	B8	10	00	00	00	23	A3	56	3D	23	A3	56	3D
00054070	23	A3	56	3D	29	29	A4	A4	A4	00	00	00	00	00	00	00
00054080	C0	03	00	06	35	11	00	00	00	10	00	00	00	00	00	00
00054090	00	00	00	00	07	00	00	00	00	10	00	00	00	00	00	00
000540A0	C1	00	70	00	72	00	6F	00	44	00	49	00	52	00	00	00
000540B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000540C0	85	03	AF	91	20	00	00	00	39	A3	56	3D	4D	99	46	3D
000540D0	39	A3	56	3D	6A	00	A4	A4	A4	00	00	00	00	00	00	00
000540E0	C0	03	00	14	84	83	00	00	BC	00	00	00	00	00	00	00
000540F0	00	00	00	00	08	00	00	00	BC	00	00	00	00	00	00	00
00054100	C1	00	66	00	6F	00	72	00	65	00	6E	00	73	00	69	00
00054110	63	00	5F	00	65	00	78	00	61	00	6D	00	70	00	6C	00
00054120	C1	00	65	00	2E	00	74	00	78	00	74	00	00	00	00	00
00054130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00054140	85	02	E0	BC	20	00	00	00	39	A3	56	3D	19	83	4B	3D
00054150	39	A3	56	3D	80	00	A4	A4	A4	00	00	00	00	00	00	00
00054160	C0	03	00	0B	C6	D0	00	00	41	5B	02	00	00	00	00	00
00054170	00	00	00	00	09	00	00	00	41	5B	02	00	00	00	00	00
00054180	C1	00	70	00	72	00	6F	00	6E	00	65	00	65	00	72	00
00054190	2E	00	70	00	64	00	66	00	00	00	00	00	00	00	00	00
000541A0	85	06	FD	A5	20	00	00	00	39	A3	56	3D	EC	88	55	3D
000541B0	39	A3	56	3D	95	00	A4	A4	A4	00	00	00	00	00	00	00
000541C0	C0	03	00	46	D1	80	00	00	8E	87	05	00	00	00	00	00
000541D0	00	00	00	00	2F	00	00	00	8E	87	05	00	00	00	00	00
000541E0	C1	00	52	00	65	00	76	00	65	00	72	00	73	00	65	00
000541F0	20	00	45	00	6E	00	67	00	69	00	6E	00	65	00	65	00

형식 코드	위치	크기
In Use	7	1
Category	6	1
Importance	5	1
Code	0	5

- **In Use**
  - ✓ 0 : Not In Use
  - ✓ 1 : In Use
- **Category**
  - ✓ 0 : Primary Entry
  - ✓ 1 : Secondary Entry
- **Importance**
  - ✓ 0 : Critical Entry
  - ✓ 1 : Benign Entry
- **Code**
  - ✓ Identifiers the entry

exFAT Directory Structure

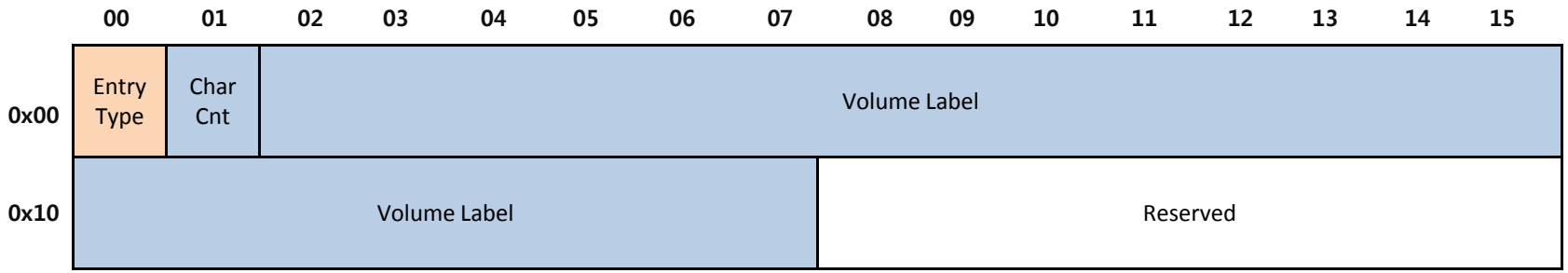
Root Directory

- 총 10 개의 디렉터리 엔트리 사용
  - 볼륨 레이블 디렉터리 엔트리 (Volume Label Directory Entry)
  - 할당 비트맵 디렉터리 엔트리 (Allocation Bitmap Directory Entry)
  - 대문자 테이블 디렉터리 엔트리 (UP-Case Directory Entry)
  - 볼륨 GUID 디렉터리 엔트리 (Volume GUID Directory Entry)
  - TexFAT 패딩 디렉터리 엔트리 (TexFAT Padding Directory Entry)
  - 윈도우 CE 접근 제어 테이블 디렉터리 엔트리 (Windows CE Access Control Table Directory Entry)
  - 파일 디렉터리 엔트리 (File Directory Entry)
  - 스트림 확장 디렉터리 엔트리 (Stream Extension Directory Entry)
  - 파일 이름 확장 디렉터리 엔트리 (File Name Extension Directory Entry)

각 파일 및 디렉터리 당 3 개의 엔트리 구성

exFAT Directory Structure

Volume Label Directory Entry



데이터 구조

필드명	위치	크기	설명/값
Entry Type	0	1	0x83
Character Count	1	1	레이블 문자열 길이
Volume Label	2	22	볼륨 레이블 (유니코드)
Reserved	24	8	-

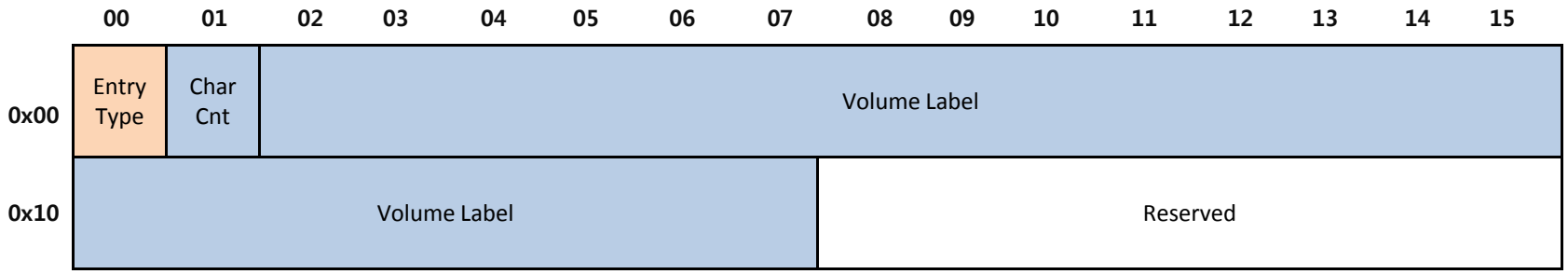
형식 코드 표현

형식 코드	위치	크기	값
In Use	7	1	1
Category	6	1	0
Importance	5	1	0
Code	0	5	00001

- 볼륨 레이블 최대 길이 : 11 글자
- 볼륨 레이블을 할당하지 않을 경우 (포맷 시), 형식 코드 값은 0x03
  - In Use 비트가 0이 되지만, 삭제된 것이 아니라 단지 사용하지 않음을 의미

exFAT Directory Structure

Volume Label Directory Entry



볼륨 레이블을 지정 안 한 경우

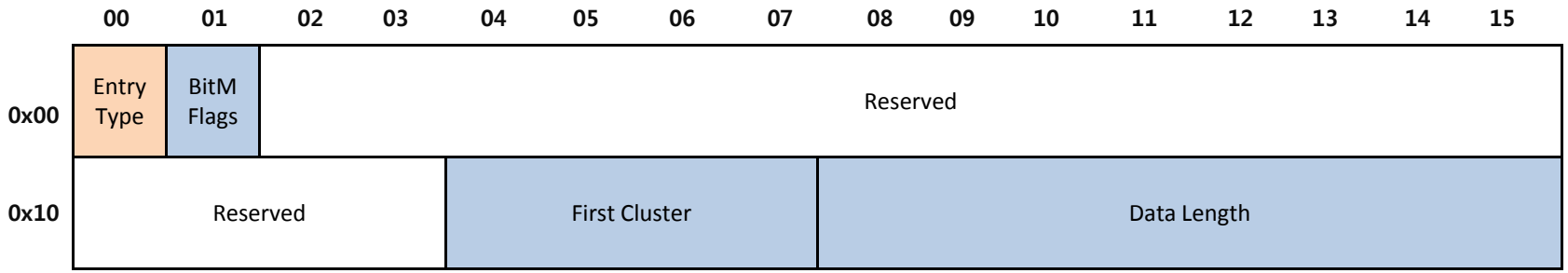
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
03	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

볼륨레이블을 지정한 경우

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
83	09	65	00	78	00	46	00	41	00	54	00	5F	00	55	00	▌ e x F A T _ U
53	00	42	00	00	00	00	00	00	00	00	00	00	00	00	00	S B

exFAT Directory Structure

Allocation Bitmap Directory Entry



데이터 구조

필드명	위치	크기	설명/값
Entry Type	0	1	0x81
Bitmap Flags	1	1	비트맵 플래그
Reserved	2	18	
First Cluster	20	4	시작 클러스터 주소
Data Length	24	8	데이터 길이

형식 코드 표현

형식 코드	위치	크기	값
In Use	7	1	1
Category	6	1	0
Importance	5	1	0
Code	0	5	00011

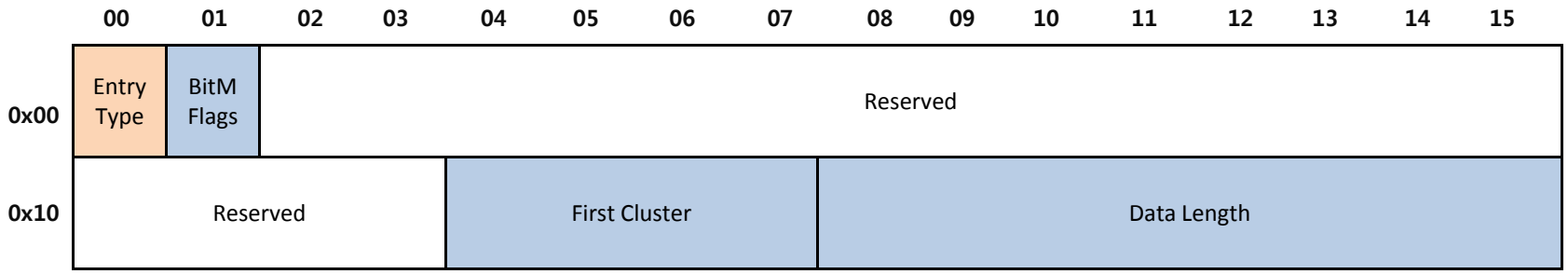
비트맵 플래그 표현

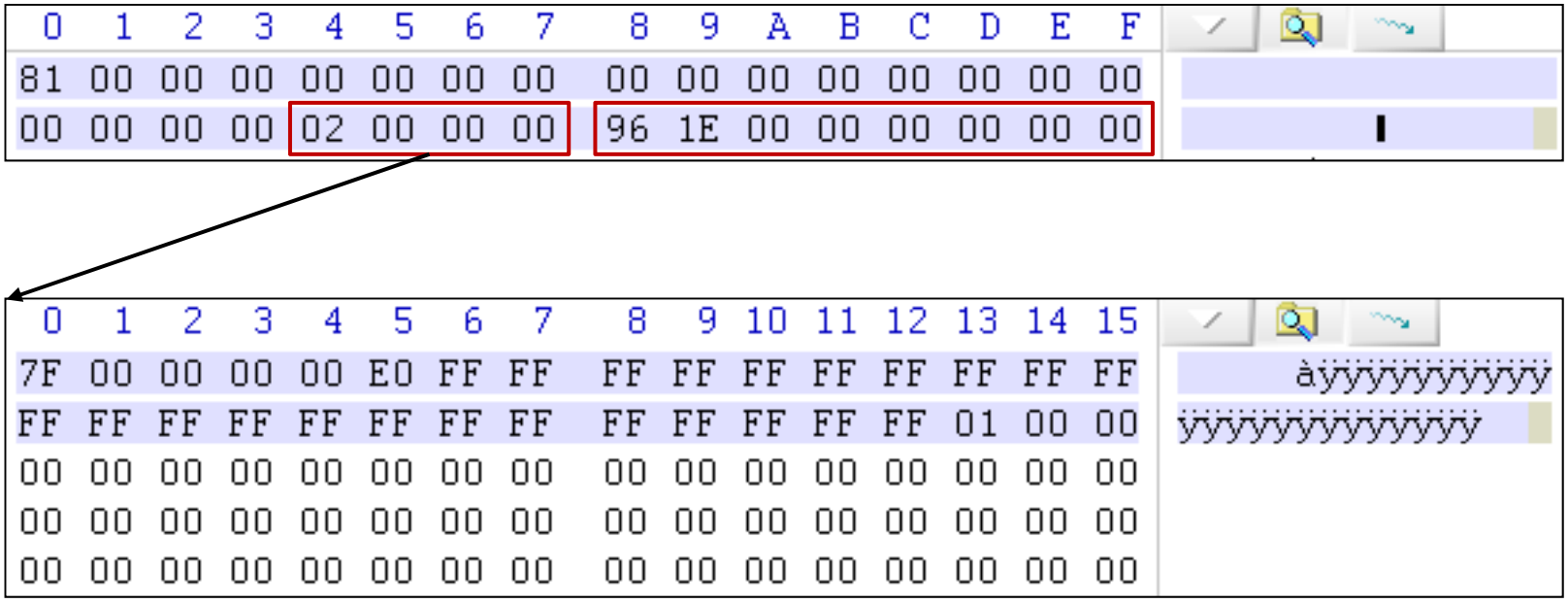
비트	크기	값	의미
7-1			Reserved
0	1	0	1st Bitmap
0	1	1	2nd Bitmap

- 할당 비트맵 테이블은 최대 2개 (TexFAT 사용 시)
- 보통 클러스터 2 번에 위치 (가변적)
- 데이터 길이는 바이트 길이

exFAT Directory Structure

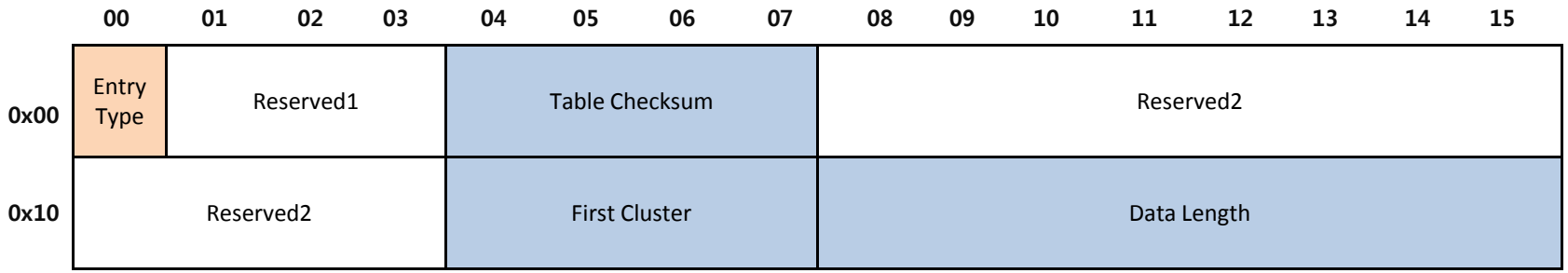
Allocation Bitmap Directory Entry





exFAT Directory Structure

UP-Case Table Directory Entry



데이터 구조

필드명	위치	크기	설명/값
Entry Type	0	1	0x82
Reserved1	1	3	
Table Checksum	4	4	테이블 체크섬
Reserved2	8	12	
First Cluster	20	4	시작 클러스터 주소
Data Length	24	8	데이터 길이

형식 코드 표현

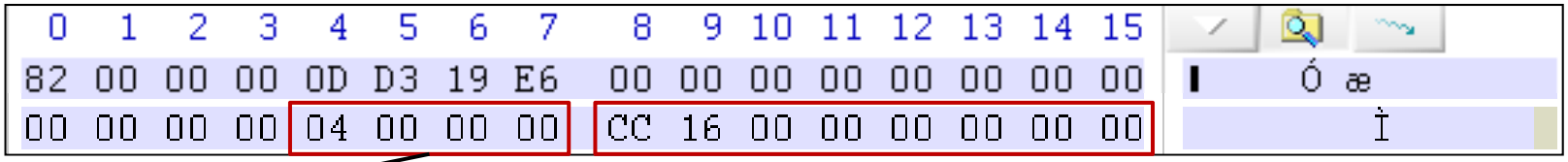
형식 코드	위치	크기	값
In Use	7	1	1
Category	6	1	0
Importance	5	1	0
Code	0	5	00010

- 파일명을 대문자로 변환할 때 사용 (파일이름과 검색 문자열의 비교)
- 테이블 사용 이전에 체크섬 계산 필요

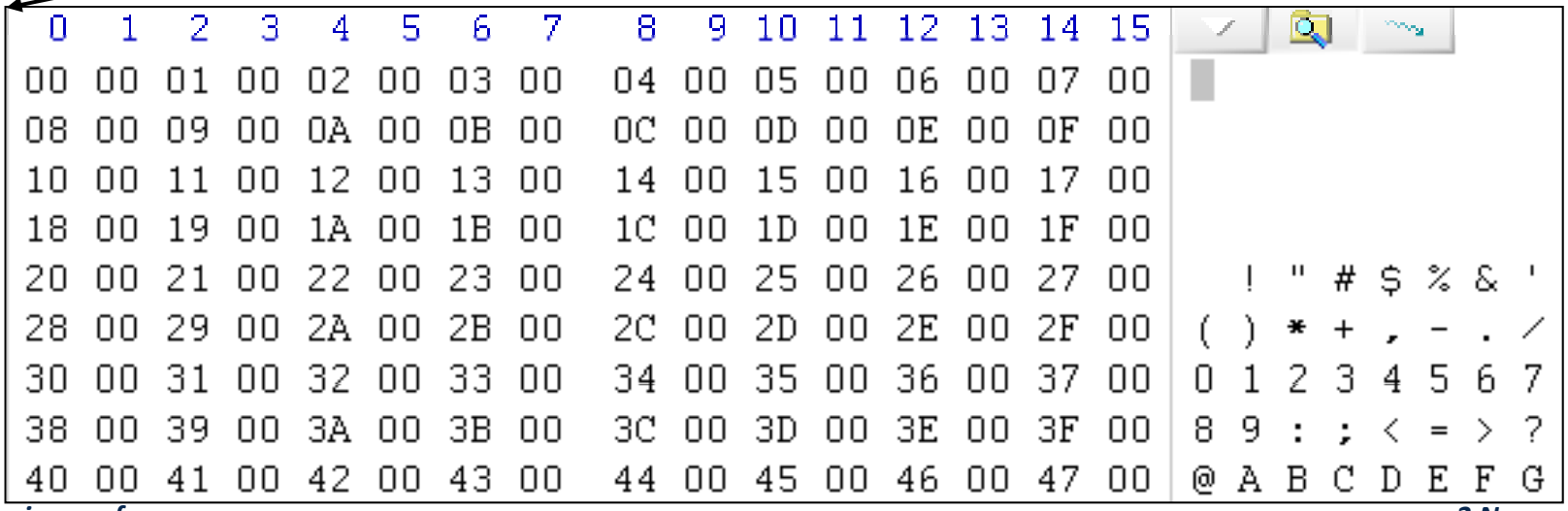
exFAT Directory Structure

UP-Case Table Directory Entry

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00	Entry Type	Reserved1			Table Checksum				Reserved2							
0x10	Reserved2				First Cluster				Data Length							



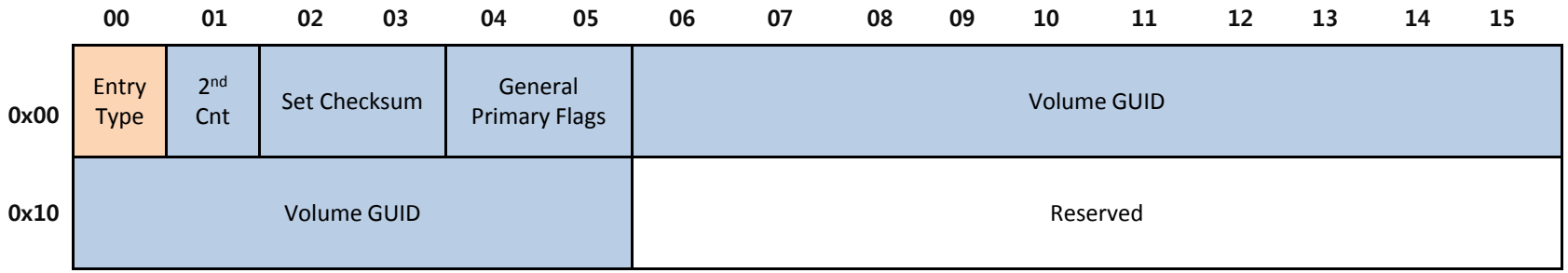
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
82	00	00	00	0D	D3	19	E6	00	00	00	00	00	00	00	00	
00	00	00	00	04	00	00	00	CC	16	00	00	00	00	00	00	



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	01	00	02	00	03	00	04	00	05	00	06	00	07	00	
08	00	09	00	0A	00	0B	00	0C	00	0D	00	0E	00	0F	00	
10	00	11	00	12	00	13	00	14	00	15	00	16	00	17	00	
18	00	19	00	1A	00	1B	00	1C	00	1D	00	1E	00	1F	00	
20	00	21	00	22	00	23	00	24	00	25	00	26	00	27	00	! " # $ % & '
28	00	29	00	2A	00	2B	00	2C	00	2D	00	2E	00	2F	00	( ) * + , - . /
30	00	31	00	32	00	33	00	34	00	35	00	36	00	37	00	0 1 2 3 4 5 6 7
38	00	39	00	3A	00	3B	00	3C	00	3D	00	3E	00	3F	00	8 9 : ; < = > ?
40	00	41	00	42	00	43	00	44	00	45	00	46	00	47	00	@ A B C D E F G

exFAT Directory Structure

Volume GUID Directory Entry



데이터 구조

필드명	위치	크기	설명/값
Entry Type	0	1	0xA0
Secondary Count	1	1	항상 0x00
Set Checksum	2	2	
General Primary Flags	4	2	주요 플래그
Volume GUID	6	16	볼륨 GUID
Reserved	22	10	

형식 코드 표현

형식 코드	위치	크기	값
In Use	7	1	1
Category	6	1	0
Importance	5	1	1
Code	0	5	00000

주요 플래그 표현

필드	위치	크기	값
Allocation Prossible	0	1	0 – No
No FAT Chain	1	1	0 – Valid 1 – Invalid
Custom	2	14	

- Benign Primary 엔트리
- 하나만 존재하고 없을 수도 있음

exFAT Directory Structure

Windows CE Access Control Table Directory Entry

데이터 구조

필드명	위치	크기	설명/값
Entry Type	0	1	0xE2
Reserved	1	31	

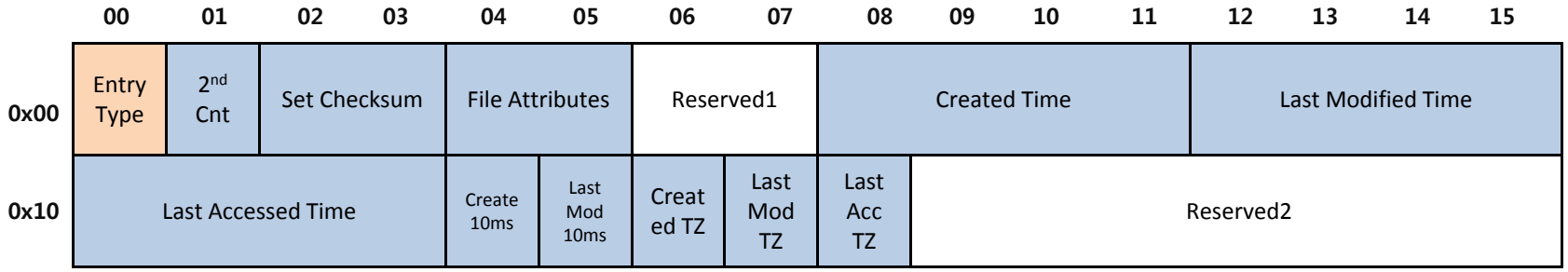
형식 코드 표현

형식 코드	위치	크기	값
In Use	7	1	1
Category	6	1	0
Importance	5	1	0
Code	0	5	00010

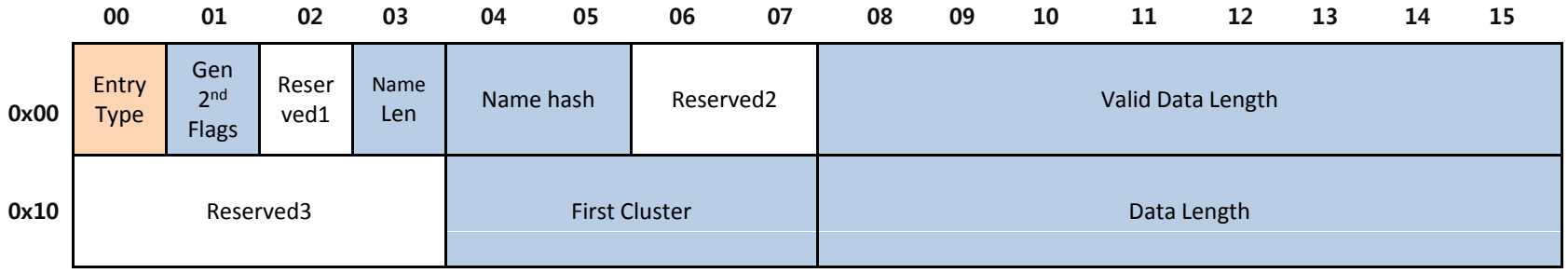
- Benign Secondary 엔트리
- 버전 1.0 에서는 지원하지 않음 (윈도우 CE만 지원)

exFAT Directory Structure

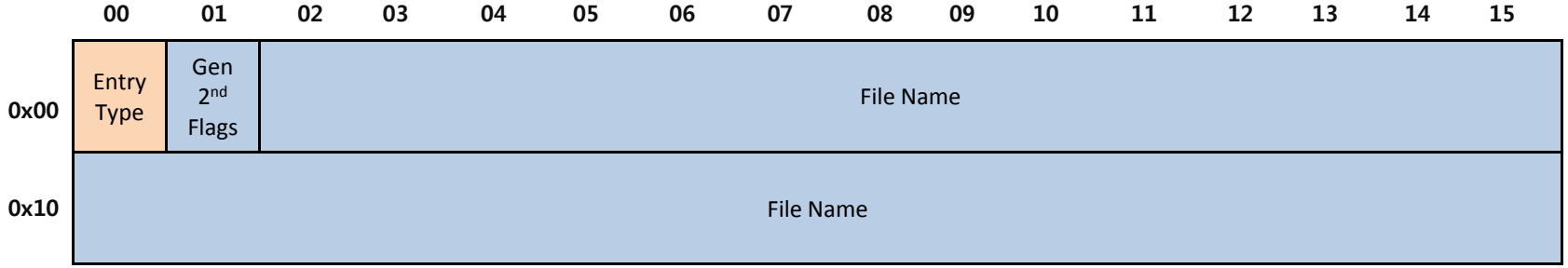
File + Stream Extension + File Name Extension Entry



File Directory Entry



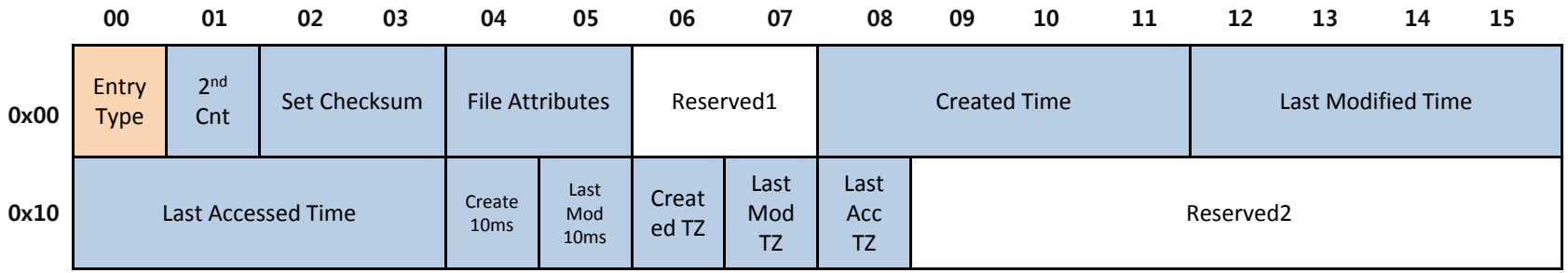
Stream Extension Entry



File Name Extension Entry

exFAT Directory Structure

File Directory Entry



데이터 구조

필드명	위치	크기	설명/값
Entry Type	0	1	0x85
Secondary Count	1	1	
Set Checksum	2	2	
File Attributes	4	2	파일 속성
Reserved1	6	2	
Created Time	8	4	DOS Timestamp 형식
Last Modified Time	12	4	DOS Timestamp 형식
Last Accessed Time	16	4	DOS Timestamp 형식
Created 10ms	20	1	생성시간 10ms 증가값
Last Modified 10ms	21	1	마지막 수정시간 10ms 증가값
Created TZ Offset	22	1	생성시간 Timezone 위치
Last Modified TZ Offset	23	1	마지막 수정시간 Timezone 위치
Last Accessed TZ Offset	24	1	마지막 접근시간 Timezone 위치
Reserved2	25	7	

형식 코드 표현

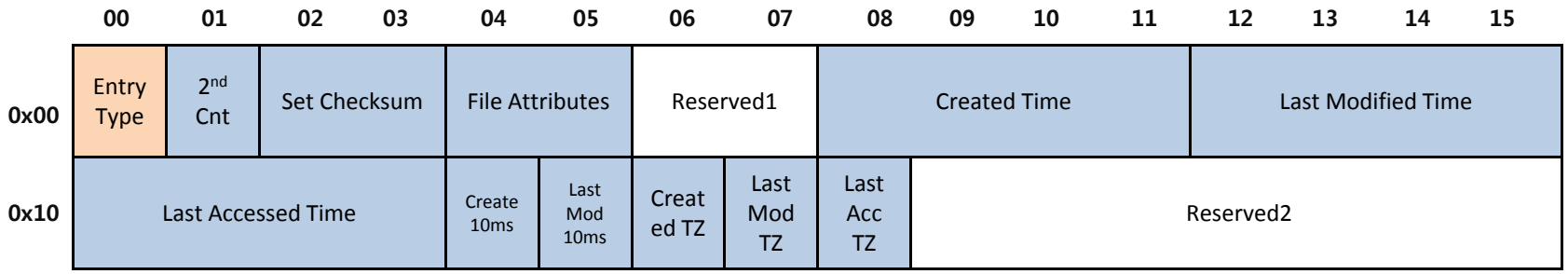
형식 코드	위치	크기	값
In Use	7	1	1
Category	6	1	0
Importance	5	1	0
Code	0	5	00101

파일 속성 표현

속성	위치	크기	마스크
Reserved2	6	10	
Archive	5	1	0x20
Directory	4	1	0x10
Reserved1	3	1	
System	2	1	0x04
Hidden	1	1	0x02
Read-Only	0	1	0x01

exFAT Directory Structure

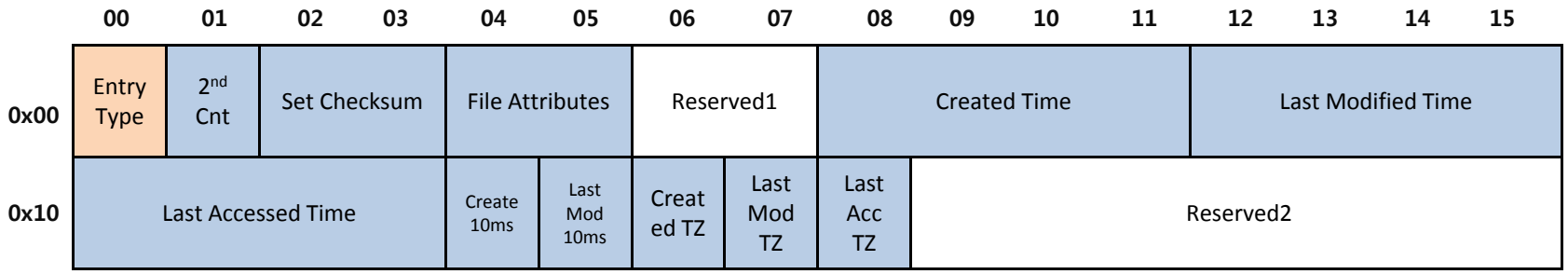
File Directory Entry



- 생성시간, 마지막 수정시간, 마지막 접근시간 저장
- 10ms 단위의 생성 및 마지막 수정시간 저장
- 각 시간 별 타임존(Time Zone) 저장
- 윈도우 XP 환경에서 10ms 단위의 시간 필드 이상 동작 (확인 필요)

exFAT Directory Structure

File Directory Entry ➔ File Deletion



삭제 전

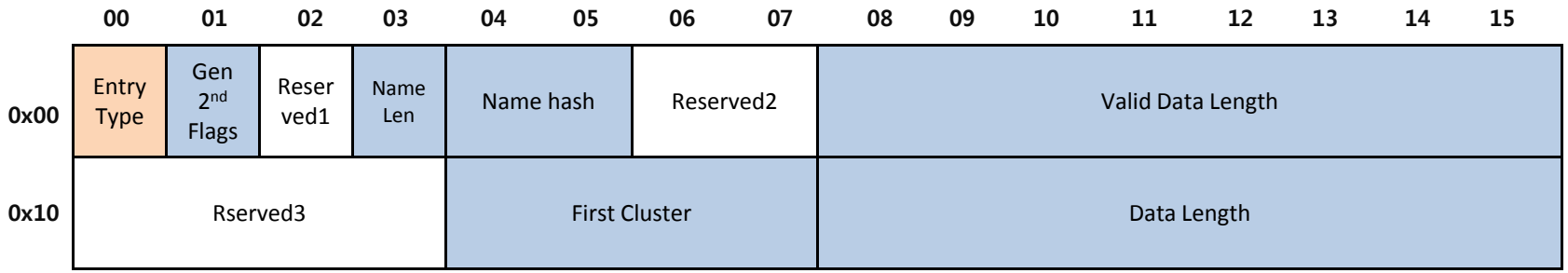
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
85	02	E0	BC	20	00	00	00	39	A3	56	3D	19	83	4B	3D
39	A3	56	3D	80	00	A4	A4	A4	00	00	00	00	00	00	00

삭제 후

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
05	02	E0	BC	20	00	00	00	39	A3	56	3D	19	83	4B	3D
39	A3	56	3D	80	00	A4	A4	A4	00	00	00	00	00	00	00

exFAT Directory Structure

Stream Extension Directory Entry



데이터 구조

필드명	위치	크기	설명/값
Entry Type	0	1	0xC0
General Secondary Flags	1	1	
Reserved1	2	1	
Name Length	3	1	이름 길이
Name hash	4	2	이름 해쉬 (디렉터리 검색에 사용)
Reserved2	6	2	
Valid Data Length	8	8	유효한 데이터 길이
Reserved3	16	4	
First Cluster	20	4	시작 클러스터
Data Length	24	8	데이터 길이

형식 코드 표현

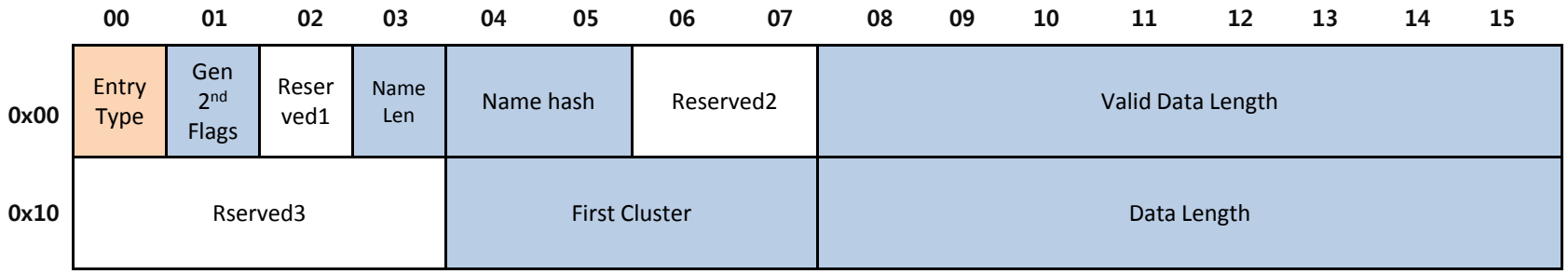
형식 코드	위치	크기	값
In Use	7	1	1
Category	6	1	1
Importance	5	1	0
Code	0	5	00000

2차 플래그 표현

필드	위치	크기	값
Allocation Possible	0	1	0 – No 1 – Yes
No FAT Chain	1	1	0 – Valid 1 – Invalid
Custom	2	14	

exFAT Directory Structure

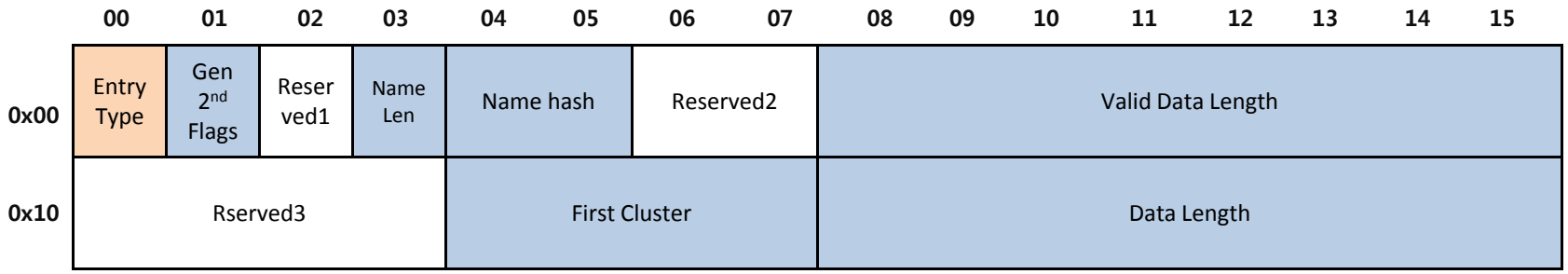
Stream Extension Directory Entry



- 파일의 크기 및 위치 정보 저장
- 파일 이름 해쉬 ➔ 디렉터리 검색 속도 향상
- No FAT Chain 플래그 : 1
  - 클러스터가 연속적으로 할당되어 있음을 의미
  - 시작 클러스터부터 파일 용량만큼 획득

exFAT Directory Structure

Stream Extension Directory Entry ➔ File Deletion



삭제 전

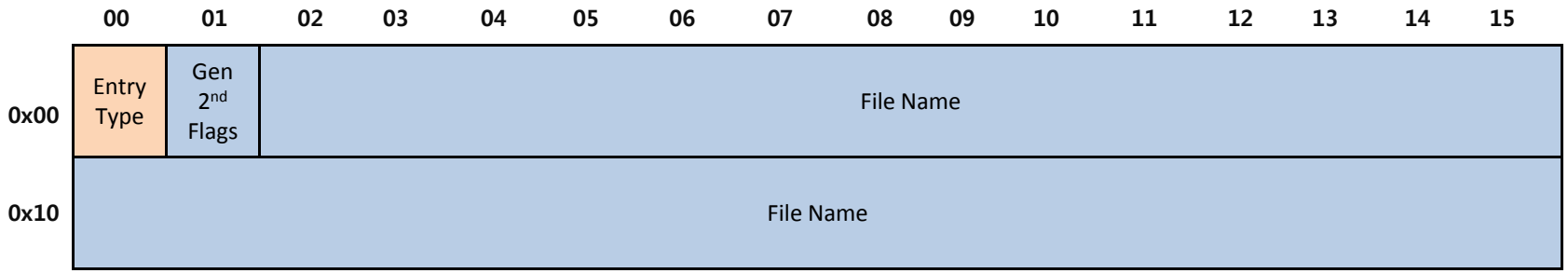
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
C0	03	00	0B	C6	D0	00	00	41	5B	02	00	00	00	00	00
00	00	00	00	09	00	00	00	41	5B	02	00	00	00	00	00

삭제 후

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
40	03	00	0B	C6	D0	00	00	41	5B	02	00	00	00	00	00
00	00	00	00	09	00	00	00	41	5B	02	00	00	00	00	00

exFAT Directory Structure

File Name Extension Directory Entry



데이터 구조

필드명	위치	크기	설명/값
Entry Type	0	1	0xC1
General Secondary Flags	1	1	0x00
File Name	2	30	파일명 15 글자 (유니코드)

- 할당이 가능하지 않음
  - 시작 클러스터 및 데이터 길이 필드가 없음
- 최대 255 글자의 파일명 가능
  - 17개 파일 이름 확장 디렉터리 엔트리 필요

형식 코드 표현

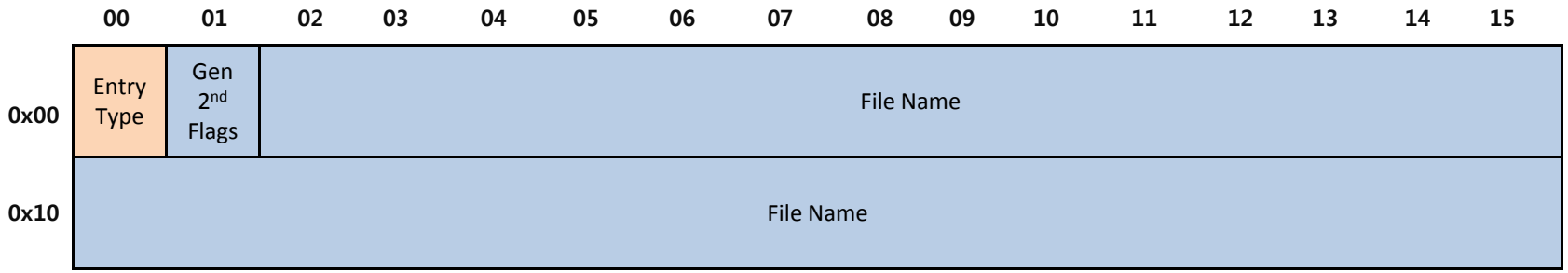
형식 코드	위치	크기	값
In Use	7	1	1
Category	6	1	1
Importance	5	1	0
Code	0	5	00001

이차 플래그 표현

필드	위치	크기	값
Allocation Possible	0	1	0 – No 1 – Yes
No FAT Chain	1	1	0 – Valid 1 - Invalid
Custom	2	14	

exFAT Directory Structure

File Name Extension Directory Entry ➔ Multiple Entry

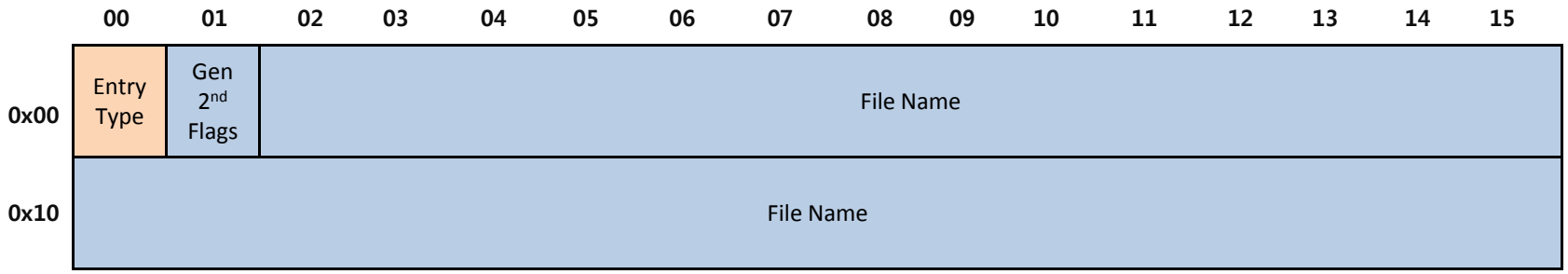


Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000541E0	C1	00	52	00	65	00	76	00	65	00	72	00	73	00	65	00	Á R e v e r s e
000541F0	20	00	45	00	6E	00	67	00	69	00	6E	00	65	00	65	00	E n g i n e e
00054200	C1	00	72	00	69	00	6E	00	67	00	20	00	74	00	68	00	Á r i n g t h
00054210	65	00	20	00	4D	00	69	00	63	00	72	00	6F	00	73	00	e M i c r o s
00054220	C1	00	6F	00	66	00	74	00	20	00	45	00	78	00	74	00	Á o f t E x t
00054230	65	00	6E	00	64	00	65	00	64	00	20	00	46	00	41	00	e n d e d F A
00054240	C1	00	54	00	20	00	46	00	69	00	6C	00	65	00	20	00	Á T F i l e
00054250	53	00	79	00	73	00	74	00	65	00	6D	00	20	00	28	00	S y s t e m (
00054260	C1	00	65	00	78	00	46	00	41	00	54	00	29	00	2E	00	Á e x F A T) .
00054270	70	00	64	00	66	00	00	00	00	00	00	00	00	00	00	00	p d f

Reverse Engineering the Microsoft Extended FAT File System (exFAT).pdf

exFAT Directory Structure

File Name Extension Directory Entry ➔ File Deletion



삭제 전

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
C1	00	70	00	72	00	6F	00	6E	00	65	00	65	00	72	00
2E	00	70	00	64	00	66	00	00	00	00	00	00	00	00	00

삭제 후

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
41	00	70	00	72	00	6F	00	6E	00	65	00	65	00	72	00
2E	00	70	00	64	00	66	00	00	00	00	00	00	00	00	00

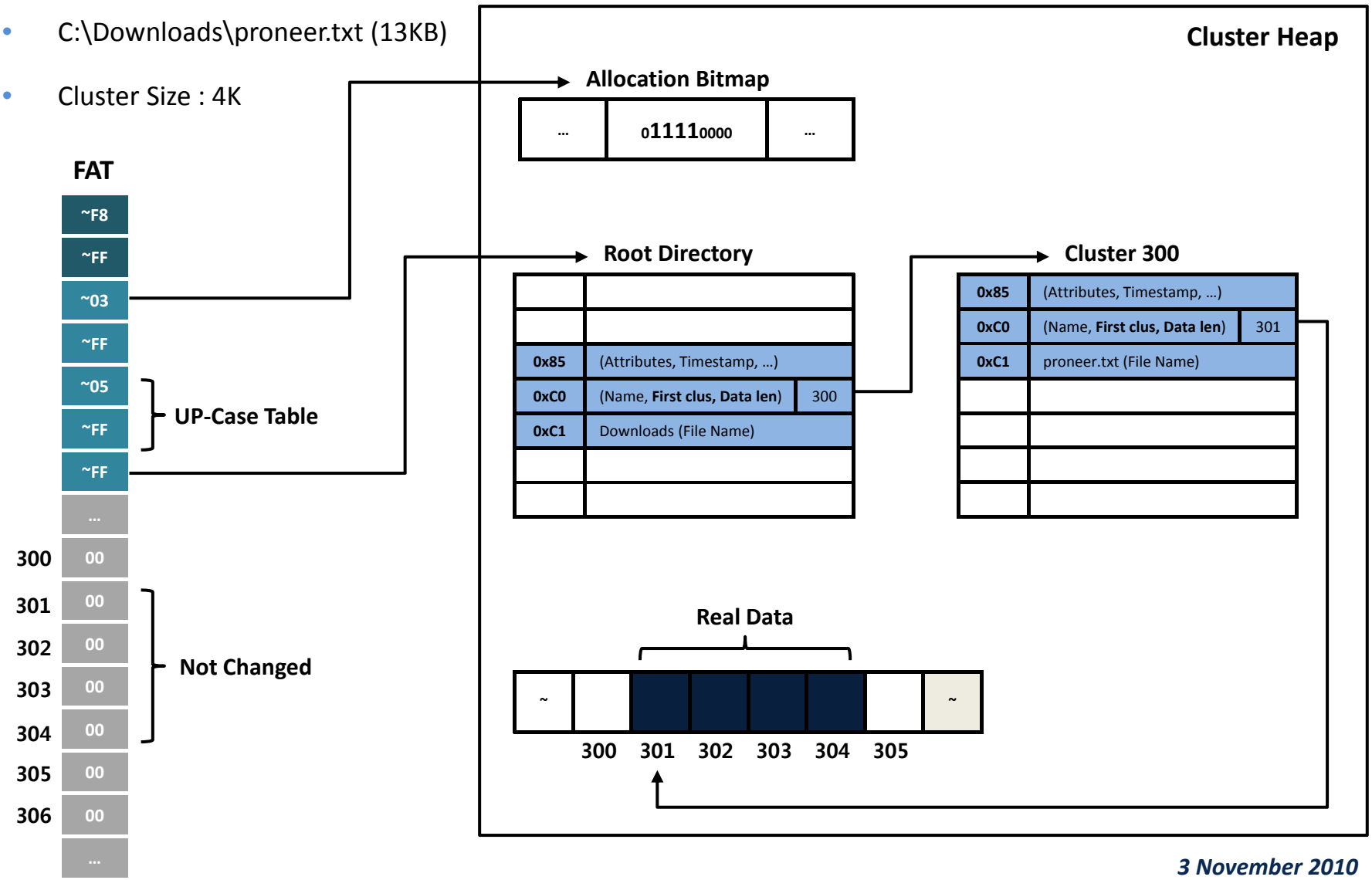
exFAT Example

Security is a people problem…

exFAT Example

File(Not fragmented) Allocation

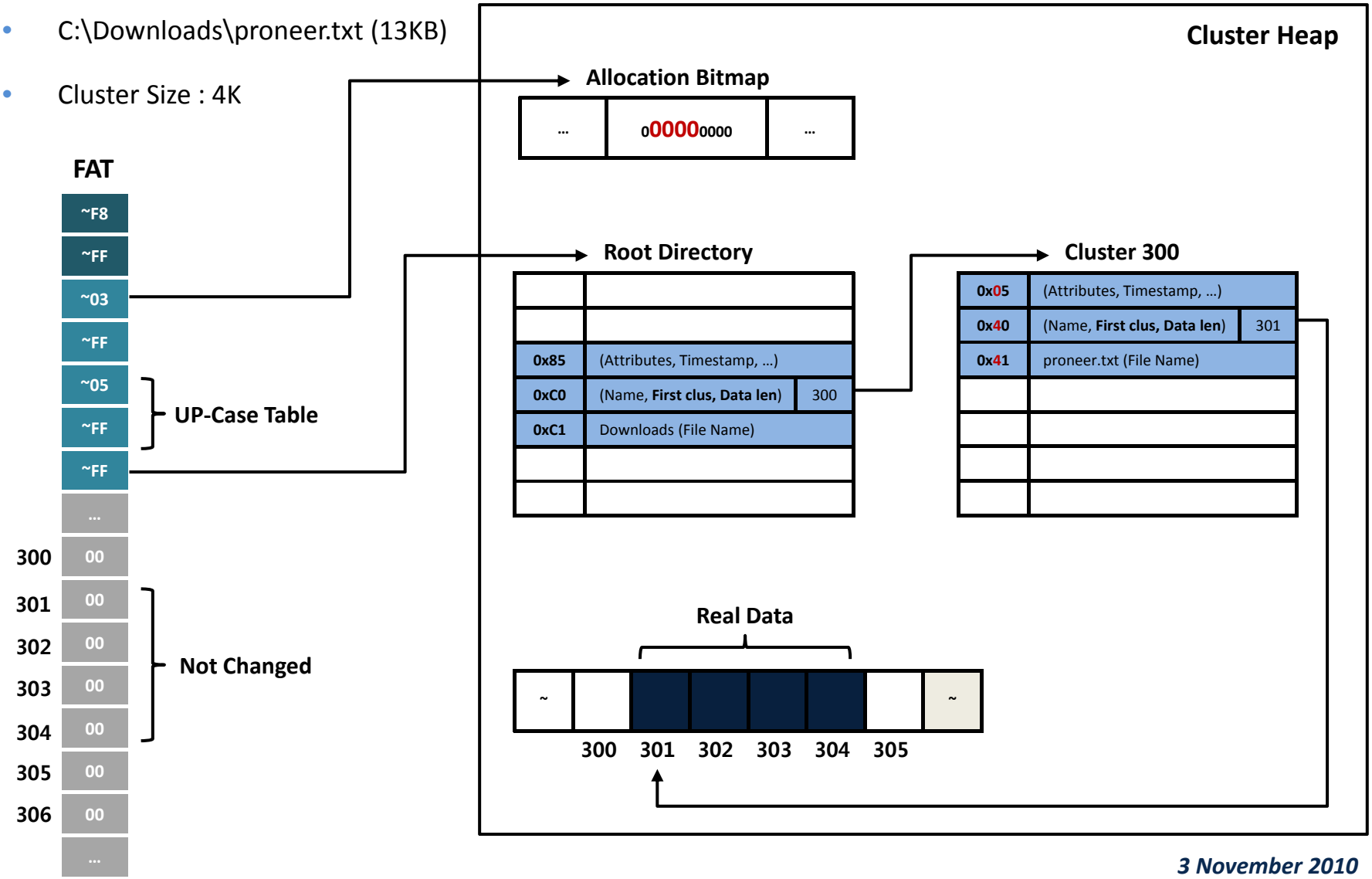
- C:\Downloads\proneer.txt (13KB)
- Cluster Size : 4K



exFAT Example

File(Not fragmented) Deletion

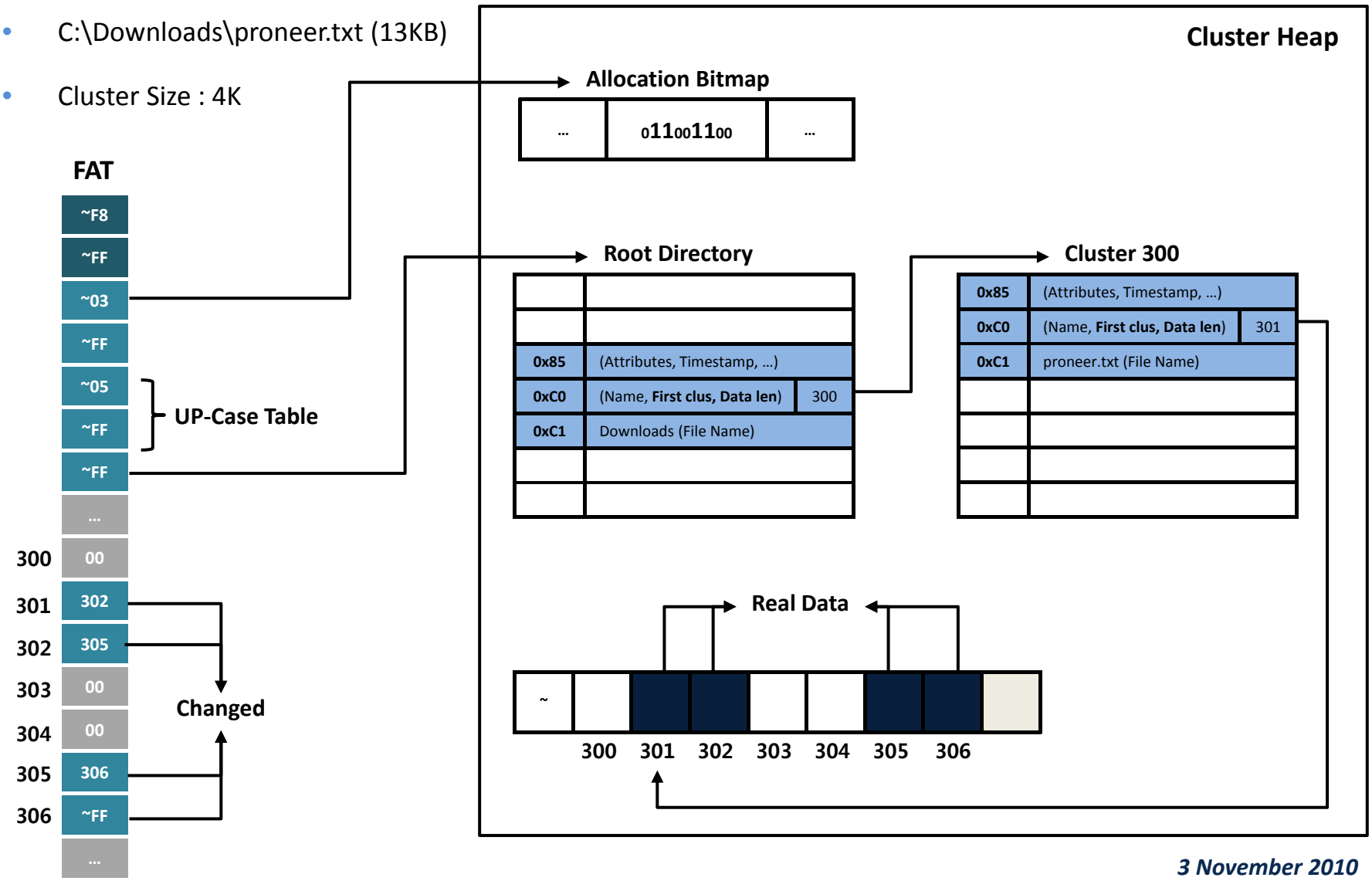
- C:\Downloads\proneer.txt (13KB)
- Cluster Size : 4K



exFAT Example

File(Fragmented) Allocation

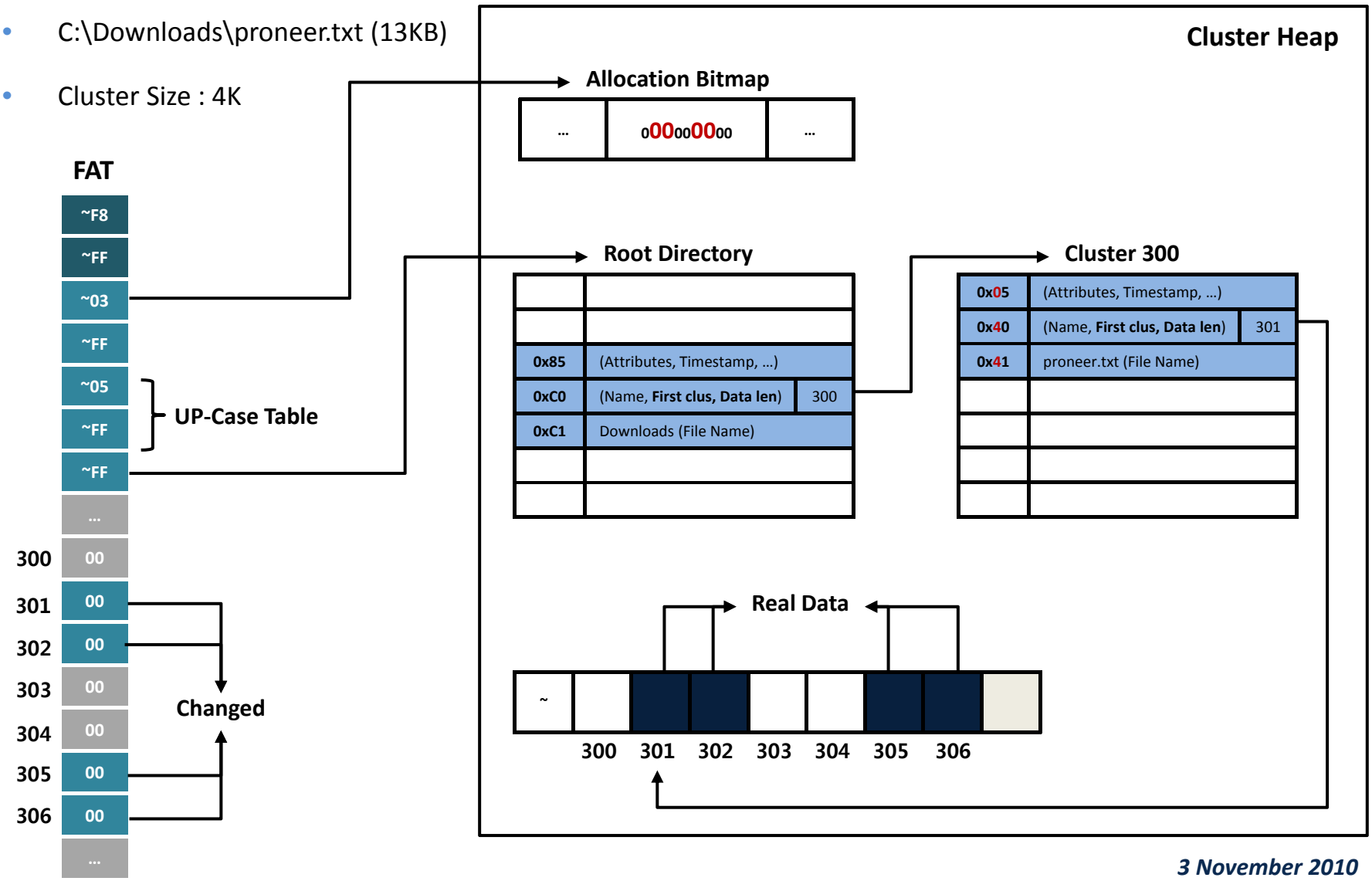
- C:\Downloads\proneer.txt (13KB)
- Cluster Size : 4K



exFAT Example

File(Fragmented) Allocation

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



Quiz !

Security is a people problem…

Quiz !

exFAT

- FAT32 과 다른 점은?
- VBR (Volume Boot Record)가 가지는 총 섹터 수는?
- Cluster Heap 영역에 존재하는 객체는?
- 한 파일이 가질 수 있는 최대 엔트리 개수는?
- 파일의 시간 정보가 저장되는 엔트리는?
- 10ms 단위의 시간이 저장되는 시간 필드는?
- 각 파일과 디렉터리마다 생성되는 디렉터리 엔트리의 개수 및 종류는?

Quiz !

exFAT

- 비할당 클러스터 판별법은?
- 삭제된 파일 판별법은?
- 덮어써진 파일 판별법은?

Question & Answer