NTFS File System

Recover Data in $MFT

91416428 지창환

91514828 염정현

Contents

프로젝트 개요

팀원소개

정보보호학과

91416428 지창환

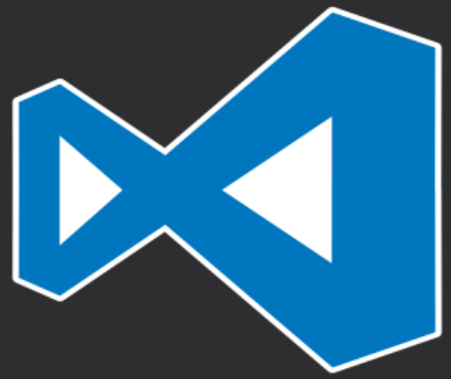
정보보호학과

91514828 염정현

프로젝트 개요

개발환경

Python



VScode

Pycharm

프로젝트 개요

목적

CONTENTS A

컨텐츠에 대한 내용을 적어요

Enjoy your stylish business and campus life with BIZCAM

CONTENTS A

컨텐츠에 대한 내용을 적어요

Enjoy your stylish business and campus life with BIZCAM

CONTENTS A

컨텐츠에 대한 내용을 적어요

Enjoy your stylish business and campus life with BIZCAM

CONTENTS A

컨텐츠에 대한 내용을 적어요

Enjoy your stylish business and campus life with BIZCAM

파일시스템 개념

NTFS File System

NTFS File System 이란?

(New Technology File System)

FAT32 File System의 한계점을 개선하기 위해 개발되었고. Windows NT 부터 현재 Windows 10까지 사용되고 있다. 또한 VBR 영역 다음에 나오는 MFT(Master File Table) 이라는 부분이 FAT File System과는 다른 NTFS File System의 핵심이다. 별도의 영역에 클러스터 할당 및 파일정보를 저장하던 FAT File System과는 다르게, NTFS는 이 MFT 파일에 모든 데이터들이 저장되는 구조이다.

파일시스템 개념

NTFS File System 구조

NTFS File System 구조

- Boot Record

NTFS의 부트레코드 구조는 FAT 파일시스템의 부트레코드 구조가 비슷하다. Windows를 부팅시키기 위한 코드와 설정 값이 있으며, 볼륨의 크기, 클러스터의 크기, MFT의 시작주소와 같은 중요한 정보를 알 수 있다.

- MFT

NTFS에서 가장 핵심적인 MFT는 모든 파일과 디렉터리의 정보를 담고 있는 테이블이며, 파일 디렉터리 수의 비례한 크기를 갖는다. 각각의 정보들은 MFT Entry라는 특별한 구조로 저장이 되며, 또한 MFT도 데이터 영역에 존재하는 파일로 관리되므로 볼륨의 어디에 위치하든 상관 없게 된다.

- Data Area

파일과 디렉터리를 담는 영역으로 FAT 파일 시스템과 마찬가지로 클러스터 단위로 읽기/쓰기가 이루어 지며, NTFS는 영역이 분할되어 있지 않고, 볼륨 전체를 데이터 영역으로 사용한다.

MFT 구조

MFT Entry

MFT Entry 구조

$STANDARD_INFORMATION

Type Number: 0x10(16)

$DATA

Type Number: 0x80(128)

$FILE_NAME

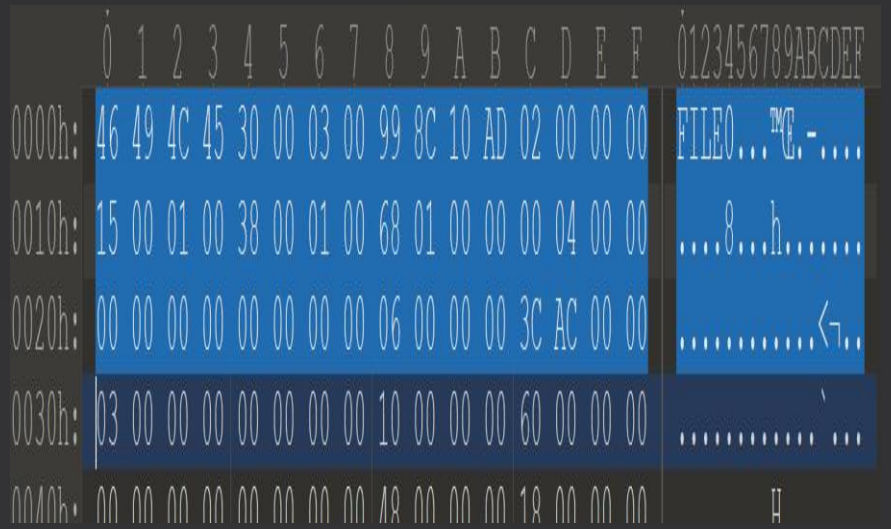
Type Number: 0x30(48)

MFT 구조

MFT Entry

MFT Entry Header

MFT Entry Header는 모든 MFT Entry의 앞 부분에 위치하는 48byte 정보이며, 0x46 0x49 0x4C 0x45 로 시작하는 FILE Signature를 가지고 있다.
다음 MFT Entry Header의 데이터 구조이다.



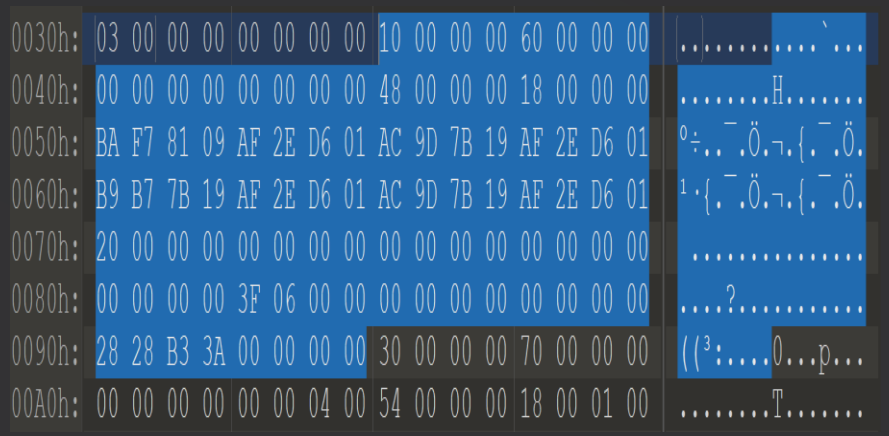
범위(Dec)	설명
0 – 3	Signature (“FILE”)
4 – 5	Offset to fixup array
6 – 7	Number of entries in fixup array
8 – 15	$LogFile Sequence Number (LSN)
16 – 17	Sequence Number
18 – 19	Link count
20 – 21	Offset to first attribute
22 – 23	Flags (in-use and directory)
24 – 27	Used size of MFT Entry
28 – 31	Allocated size of MFT Entry
32 – 39	File reference to base record
40 – 41	Next attribute ID
42 – 43	Align to 4B boundary
44 - 47	Number of this MFT Entry

MFT 구조

MFT Entry 속성

MFT Entry $STANDARD_INFORMATION 속성

$STANDARD_INFORMATION 속성은 NTFS의 모든 파일에 기본적으로 존재하는 속성이며, 파일의 시간정보, 파일특성, 등 기본적인 속성 정보를 가지고 있다. 또한 속성들 중 타입번호가 가장 낮기 때문에 MFT Entry 내의 속성들 중 가장 처음에 위치 한다.



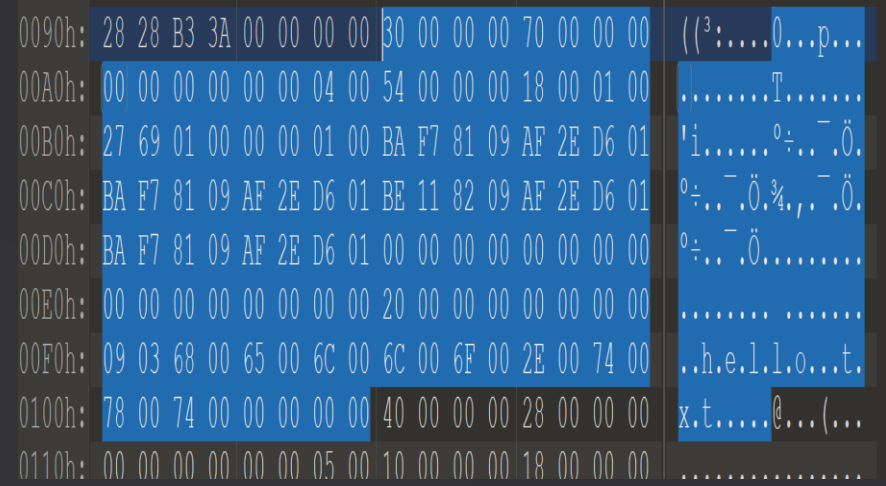
범위(Dec)	설명
-	속성 헤더 (Attribute header)
0 – 7	생성 시간 (Creation time)
8 – 15	수정 시간 (Modified time)
16 – 23	MFT 수정 시간 (MFT modified time)
24 – 31	접근 시간 (Last accessed time)
32 – 35	속성 플래그 (Flags)
36 – 39	버전 최대값 (Maximum number of versions)
40 – 43	버전 번호 (Version number)
44 – 47	클래스 ID (Class ID)
48 – 51	소유자 ID (version 3.0 +)
52 – 55	보안 ID (version 3.0 +)
56 – 63	Quota Charged (version 3.0 +)
64 - 71	USN (Update Sequence Number) (version 3.0 +)

MFT 구조

MFT Entry 속성

MFT Entry $FILE_NAME 속성

이전 속성과 함께 NTFS 의 모든 파일에 기본적으로 존재하는 속성이며, 속성 이름에서 알 수 있듯이 파일의 이름을 저장하기 위해 존재한다. 하지만 파일의 이름 외에도 다양한 정보를 저장하고 있다.



범위(Dec)	설명
-	속성 헤더 (Attribute header)
0 – 7	부모 디렉터리의 파일 참조 주소
8 – 15	생성 시간 (Creation time)
16 – 23	수정 시간 (Modified time)
24 – 31	MFT 수정 시간 (MFT modified time)
32 – 39	접근 시간 (Last accessed time)
40 – 47	파일 할당 크기 (Allocated size of file)
48 – 55	파일 실제 크기 (Real size of file)
56 – 59	속성 플래그 (Flags)
60 – 63	Reparse 값
64 – 64	이름 길이 (Length of name)
65 – 65	이름 형식 (Namespace)
66 -	이름 (Name)

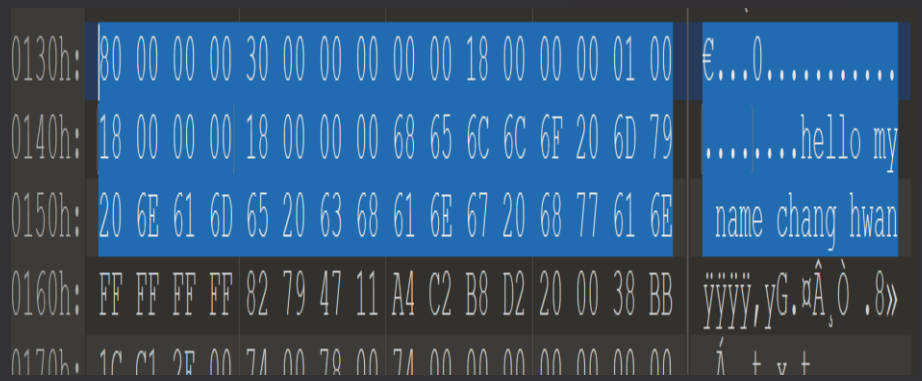
MFT 구조

MFT Entry 속성

MFT Entry $DATA 속성

$DATA 속성은 이름에서도 알 수 있듯이 파일의 데이터를 저장하는 속성이다. 물론 데이터 저장되는 방식은 데이터의 크기(약 700 바이트)에 따라 Resident 속성 또는 Non- Resident 속성으로 저장이 되며, Non- Resident 속성의 경우 MFT Entry 가 아닌 별도의 클러스터를 할당 받아 저장하게 된다. 데이터의 크기가 적을 경우 Resident 속성이 되어 MFT Entry 내부에 데이터가 저장된다.

범위(Dec)	설명
-	속성 헤더 (Attribute header)
0 – (가변적)	데이터



MFT 구조

MFT Entry 속성의 종류

속성 타입 번호	속성 이름	설명
0x10	$STANDARD_INFORMATION	생성, 수정, 접근 시간, 소유자와 보안 ID와 같은 정보
0x20	$ATTRIBUTE_LIST	다른 속성 정보들이 어디에 있는지 찾을 수 있는 속성 리스트
0x30	$FILE_NAME	파일 이름(유니코드) 및 생성, 접근, 수정 시간에 대한 정보
0x40	$VOLUME_VERSION	볼륨 정보를 담고 있다. (버전1.2에만 존재)
0x40	$OBJECT_ID	파일이나 디렉터리를 위한 고유 값 16바이트로 표현(버전3.0 이상에만 존재)
0x50	$SECURITY_DESCRIPTOR	파일의 접근 제어와 보안 속성을 담고 있다.
0x60	$VOLUME_NAME	볼륨 이름과 관련된 정보를 가지고 있다.
0x70	$VOLUME_INFORMATION	파일시스템의 버전과 여러 Flag들을 담고 있다.
0x80	$DATA	파일 내용을 담고 있다.
0x90	$INDEX_ROOT	인덱스 트리의 루트 노드를 담고 있다.
0xA0	$INDEX_ALLOCATION	$INDEX_ROOT 속성에 연결되어 있는 인덱스 노드들의 정보
0xB0	$BITMAP	$MFT 파일과 인덱스의 할당 정보
0xC0	$SYMBOLIC_LINK	Soft Link의 정보 (버전1.2에만 존재)
0xC0	$REPARSE_POINT	Soft Link가 사용하는 reparse 위치 정보(버전3.0이상에 존재)
0xD0	$EA_INFORMATION	OS/2 응용 프로그램과 호환성을 위해 사용
0xE0	$EA	
0x100	$LOGGED_UTILITY_STEAM	암호화된 속성에 대한 키들과 정보를 담고 있다.

Q&A

PPT PRESENTATION

Enjoy your stylish business and campus life with BIZCAM

Product A

68%

Product A

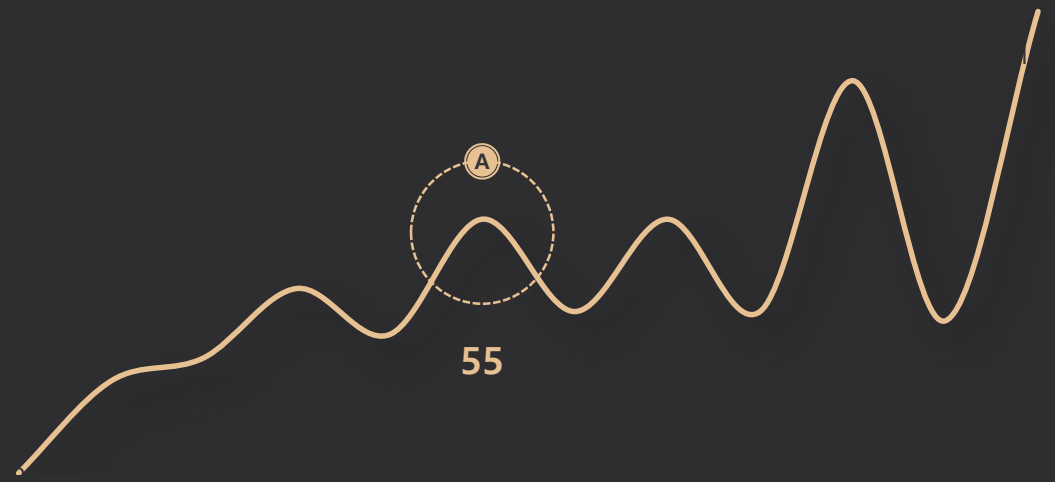
68%

Product A

68%

Product A

68%



CONTENTS A

You can use a software program such as Microsoft Power Point to provide the audience with slides that contains your major points or essential information.

PPT PRESENTATION

Enjoy your stylish business and campus life with BIZCAM

CONTENTS

TEXT A

Enjoy your stylish business and campus life with BIZCAM

TEXT B

Enjoy your stylish business and campus life with BIZCAM

TEXT C

Enjoy your stylish business and campus life with BIZCAM

CONTENTS

TEXT A

Enjoy your stylish business and campus life with BIZCAM

TEXT B

Enjoy your stylish business and campus life with BIZCAM

TEXT C

Enjoy your stylish business and campus life with BIZCAM

CONTENTS

TEXT A

Enjoy your stylish business and campus life with BIZCAM

TEXT B

Enjoy your stylish business and campus life with BIZCAM

TEXT C

Enjoy your stylish business and campus life with BIZCAM