FAT32 파일 구조 발표 스크립트

[페이지1]

안녕하세요. FAT32 파일 구조 발표를 할 고은이 입니다.

[페이지2]

목차로는 FAT32파일 구조 설명과 FAT32 삭제 파일 분석 순으로 발표하겠습니다.

[페이지3]

FAT32 파일의 큰 구조는 클러스터, 파일 엔트리, 루트 디렉터리, 파일 할당 테이블, 클러스터 체인으로 이루어져 있습니다.

FAT32 파일 시스템은 디스크 공간을 여러 개의 클러스터로 나누고 저장합니다. 파일 엔트리는 파일과 디렉터리의 메타데이터 정보를 저장하는 테이블입니다. 각 파일과 디렉터리에는 하나의 파일 엔트리가 존재합니다. 파일 엔트리에는 파일 이름, 확장자, 파일 크기, 파일 생성 일시, 마지막 수정 일시 등의 정보가 저장됩니다. 루트 디렉터리는 디스크 섹터 단위로 구성됩니다. 파일 할당 테이블은 디스크의 클러스터 할당 정보를 저장하는 테이블입니다. 각각의 클러스터는 이전의 클러스터의 번호나 다음 클러스터의 번호를 기록하는 방식으로 파일의 연속성을 유지합니다. 파일 할당 테이블은 모든 클러스터의 할당 정보를 가지고 있고 이 정보를 통해 파일의 데이터가 어떻게 연결되었는지 알 수 있다. 파일은 여러 클러스터에 걸쳐 저장될 수 있고 이런 클러스터들의 연결을 클러스터 체인이라고 합니다. 클러스터 체인을 통해 파일 시스템은 파일의 시작 클러스터를 찾고 이후에 연속적으로 할당된 클러스터를 따라 파일의 모든 데이터를 읽거나 쓸 수 있습니다.

[페이지4]

마스터 부트 레코드 즉 MBR은 컴퓨터가 모든 하드웨어를 확인하고 소프트웨어 로딩을 제어한 후 실행되는 첫번째 코드입니다. MBR은 운영체제를 부팅 시키기 위한 파티션을 찾는 부분인 부트스트랩 코드(446바이트)와 파티션에 대한 정보가 들어있는 테이블인 파티션 테이블(64바이트), 시그니쳐 값으로 해당 섹터의 오류를 체크하는 시그니쳐(0x55AA)으로 이루어져 512바이트로 구성되어 있습니다.

[페이지5]

Reserved영역은 파일 시스템의 부팅과정 및 내부 동작에 사용되는 중요한 데이터를 저장하는 부분입니다. 이 영역은 파일 시스템의 내부적인 운영에 필요한 데이터를 포함하기 때문에 일반 사용자가 직접 접근하거나 수정하면 안 됩니다. 파일 시스템을 포맷하거나 파티션을 나눌 때 주의가 필요하고 해당 영역을 손상시키지 않도록 해야 합니다.

[페이지6]

FAT#1 영역과 FAT#2영역은 서로 동일한 정보를 가지고 있고, 파일 시스템의 모든 클러스터에 대한 할당 정보를 공유합니다. 일반적으로 이런 두 파일 할당 테이블이 완전히 동일한 정보를 가지고 있지만 하나의 테이블이 손상되었을 때 시스템이 더 안정적으로 작동하기 위해 다른 테이블로 전환하는데 사용됩니다.

두 파일 할당 테이블은 디스크의 다른 위치에 저장되어 파일 시스템의 신뢰성을 높일 수 있습니다.

[페이지7]

데이터 영역은 루트 디렉터리 이후에 위치하고 파일 할당 테이블에 의해 관리되는 클러스터로 구성됩니다. 파일 시스템의 중요한 부분으로 파일의 실제 데이터가 저장되는 공간입니다.

[페이지8]

이전에 FAT32 삭제 파일 복구 실습을 했던 파일을 살펴보면 노란색으로 표시된 00 02 부분이 부팅 가능여부를 확인할 수 있는 부분으로 부팅이 가능하면 80으로 표시가 되고 부팅이 가능하지 않으면 00으로 표시가 됩니다.

빨간색을 표시된 00 08 00 00 부분은 부트 섹터의 위치를 알 수 있는 부분입니다.

초록색으로 표시된 00 E8 FF 03 부분으로는 파티션 섹터의 수를 알 수 있습니다.

주황색 부분은 부트 시그니쳐입니다.

[페이지9]

화면을 보면 빨간색으로 표시된 곳이 부트 코드이고 초록색으로 표시된 부분이 BPB로 BPB는 FAT32 파일 시스템의 중요한 부분으로 파일 시스템을 초기화하고 사용하기 위해 필요한 정보를 저장합니다. 주황색으로 표시된 부분은 FAT32 섹션입니다.

[페이지10]

사진의 첫번쨰 줄에 00 02는 섹터당 바이트 값, 40은 클러스터 당 섹터, 06 20은 예약된 영역을 나타냅니다. 세번째 줄의 FD 1F 00 00은 FAT#1영역이고, 02 00 00 00은 루트 디렉터리 클러스터 시작 영역입니다. 네번째 줄의 01 00 06 00은 파티션 총 섹터이고, 여섯번째 줄의 46 41 54 33 32 20 20 20은 파일 시스템 타입을 나타냅니다. 해당부분을 잡으면 FAT32파일임을 알 수 있습니다.

[페이지11]

빨간색 E5 43 50 20 20 20 20 20 이 파일 이름입니다. 파일 이름이 E5로 시작하면 삭제된 파일 임으로 사진에 보이는 해당 파일은 삭제된 파일 인 것을 알 수 있습니다. 주황색 54 58 54는 확장자 정보, 노란색 20은 속성 정보, 초록색 20 76은 생성시간은 알 수 있습니다. 파란색의 F2 56은 만든 날짜 하늘색의 F2 56은 수정 날짜를 표시하는 부분으로 해당 파일은 만든 날짜와 마지막 수정 날짜가 동일한 것을 알 수 있습니다. 보라색 00 00 08 00은 파일 위치 클러스터를 알 수 있고 분홍색 07 00 00 00은 파일 크기를 알 수 있습니다.

[페이지12]

이상 발표를 마치겠습니다. 감사합니다.

Q&A