디스크 섹터 직접 접근을 통한 파일시스템 구조 시각화 및 파일 복원

File System Hierarchy Visualization and File Recovery by Direct Access to Disk Sectors

연제성 · 한유일 · 전병준 · 이건명
Jeseong Yeon, Yuil Han, Byungjun Jeon, Keon Myung Lee

충북대학교 전자정보대학 소프트웨어 학과
Dept. of Computer Science, Chungbuk National University

요 약

최근 많은 운영체제의 저장장치를 공격하는 범죄가 늘어나고 있다. 저장매체는 손상되거나 고의적으로 삭제된 파일은 복구가 어려운 것으로 알려져 있다. 이에 삭제된 파일 복구 및 손상된 정보를 추출하고 수정하기 위해 파일시스템 메타데이터를 활용할 수 있다. 본 논문에서는 FAT32를 이용하여 손상된 파일의 복원 및 복원을 하면서 발생하는 로그정보에 대해 수집하는 방법을 제시한다. FAT32의 메타데이터를 활용하기 위해 저장장치를 직접 접근하고, 읽어온 메타데이터를 활용하여 데이터를 복원할 수 있다. 또한, 이러한 복원과정에서 발생되는 로그를 수집한다.

키워드 : FAT32, 메타데이터 파일복원, 파일시스템

1. 서 론

최근 CCTV, 차량 블랙박스, 촬영장비에는 영상 정보를 저장하기 위해서 플래시 메모리 등을 사용한다. 그러나 장치에서 사용되는 저장매체가 사용 중인 용량이 한계에 도달하면 기존의 영상을 삭제함으로써 사용 가능한 용량을 확보한다. 이 때, 중요하게 쓰일 수 있는 영상도 삭제될 수 있다.

대표적으로 FAT32의 경우 파일삭제 시 기존의 데이터는 남겨두고 메타데이터만 삭제를 한다. 만약 이 파일을 다시 복원할 수 있다면 중요한 자료가 될 것이며, 혹시나 모를 조작을 대비해 복원과정에 파일에 접근하는 로그로 기록한다면 증거자료로 채택될 수 있다. 이에 본 논문에서는 FAT32 파일 시스템에서 메타데이터를 이용하여 파일 복원 및 복원 과정에서 발생되는 로그를 기록하여 증거자료를 획득하는 방법을 제시한다.

2. POSIX 표준을 이용한 디스크 섹터 접근

저장장치와 통신하기 위해서 POSIX 표준 인터페이스와 시스템 콜을 사용하였다. 시스템 콜은 저장장치의 디바이스 드라이버를 통하여 저장장치의 컨트롤러와 통신한다. 저장장치의 디바이스 드라이버는 시스템 콜의 명령어를 컨트롤러에 보내 섹터에 대한 데이터를 얻어온다. 시스템 콜의 명령어는 POSIX 표준 인터페이스에 정의된 명령어를 사용하여 저장장치에 접근하였다. 저장장치의 섹터에 대한 바이트스트림을 기반으로 파일시스템을 시각화한다.

3. 파일시스템 구조 시각화

해당 파티션의 파일시스템의 구조를 시각화하기 위해서는 현재 물리 디스크의 MBR(Master Boot Record)을 읽어 현재 디스크의 파티션에 대한 정보를 확인한다. MBR에는 현재 설치된 파티션들의 크기 및 파일시스템 정보, 파티션 시작 섹터 등 다양한 정보를 가지고 있다. 이것을 이용하여 FAT32에 해당하는 파일시스템을 찾아내고 파티션의 첫 번째 섹터를 알 수 있다. 첫 번째 섹터에는 FAT32에 대한 파일시스템 정보가 담겨져 있고, 클러스터 크기, Data Area 시작 섹터 등 다양한 정보를 비트스트림으로 파싱하여 원하는 정보를 알아낸다. (그림 1)은 FAT32의 대략적인 구조 보여준다. Boot Record 영역은 파일시스템 정보를 가지고 있다. FAT 영역은 클러스터를 관리하기 위한 테이블이 있는 영역으로 연결된 클러스터에 대한 정보를 가지고 있다. Data 영역은 파일 및 디렉토리 엔트리가 저장되어 있는 영역이다.

그림 1. FAT32 구조

FAT32 파일시스템의 정보를 이용하여 실제 데이터가 저장된 Data Area의 Root Directory에 접근하면, 모든 데이터가 비트스트림으로 되어있다. 이 비트들을 파싱하여 파일시스템의 디렉토리 엔트리로 변환하기 위해서는 디렉토리 엔트리의 파싱 순서 및 엔트리의 크기 등을 알아야 한다. (그림 2)은 FAT32 파일시스템의 디렉토리 엔트리의 구조를 보여준다.

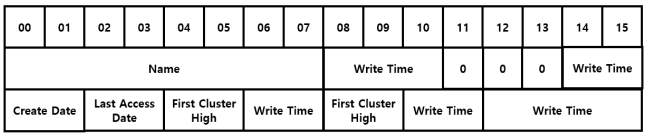

그림 2. FAT32 디렉토리 엔트리 구조

파일의 디렉토리 엔트리를 활용하여 실제 데이터가 저장되어 있는 섹터에 대한 섹터 주소를 알 수 있다. 파일의 실제 데이터와 파일의 디렉토리 엔트리 정보를 이용하여 사용자에게 파일시스템의 구조를 시각화 할 수 있다. (그림 3)는 실제 구현한 프로그램이 섹터를 파싱하여 사용자에게 폴더와 파일형태로 파일시스템을 시각화한 그림이다.

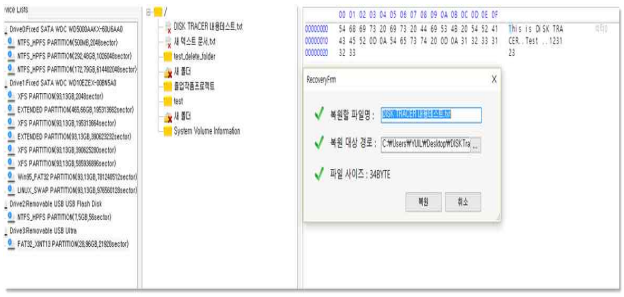

그림 3. 파일시스템 시각화

4. 파일 복원

파일의 디렉토리 엔트리는 파일의 데이터가 삭제되어도 계속 남아 있어 현재 디렉토리에 어떤 파일이나 디렉토리가 있었는지를 알 수 있다. 이 부분을 활용하여 데이터를 삭제해도 파일을 복원할 수 있다.

파일 복원 시 파일의 디렉토리 엔트리를 이용하여 해당 파일의 데이터가 존재하는 지 확인하다. 파일의 데이터가 남아 있다면 파일을 복원 할 수 있다. 파일의 메타데이터는 파일 삭제 시 최상위 바이트만 바뀌었기 때문에, 파일 데이터가 저장된 섹터 번호에 대한 정보는 남아있다. 이것을 이용하여 데이터를 다른 곳에 저장한 후 새로운 파일을 새로 만들면 해당 파일이 복원이 완료된다.

만약 파일의 크기가 클러스터의 크기를 넘어가면 FAT32는 여러 개의 클러스터를 파일에 할당한다. 할당한 클러스터에 대한 정보는 FAT영역에서 관리를 하며, 삭제 시 모든 정보가 초기화 된다. 그러므로 여러 개의 클러스터가 할당된 파일은 복구하기 힘들며, 복구 할 경우 모든 클러스터를 뒤져서 파일을 연결하여 복구해야 한다. 현재는 한 개의 클러스터만 할당된 파일만 복구하며, 여러 개의 클러스터가 할당된 파일의 경우 계속 연구 진행 중이다.

5. 파일 접근 로그 수집

파일을 탐색하고 복원하는 과정에서 수집될 수 있는 기록은 아래와 같다.

- 연결된 저장장치들의 정보
- 저장장치들의 논리적 파티션 정보
- 장치내의 논리적 파일에 대한 접근 정보
- 파일 복원 기록에 관한 정보

위 로그 정보에 대해서는 모두 타임스탬프를 남겨서 탐색 및 복원이 이뤄진 시점에 저장장치에 대한 모든 기록을 저장하고 확인할 수 있다.

6. 시스템 구성

본 논문에서 제안하는 시스템은 저장장치, 윈도우 커널, 응용프로그램으로 구성되어 있다. 저장장치는 윈도우 커널의 디바이스 드라이버와 연결되어 있다. 응용프로그램은 디바이스 드라이버의 인터페이스를 사용하여 저장장치에 명령을 내린다. 응용프로그램에서는 byte단위의 데이터를 파싱하여 사용자에게 파일과 디렉토리 형태로 데이터를 보여준다. (그림 4)는 현재 구현한 시스템 구성도이다.

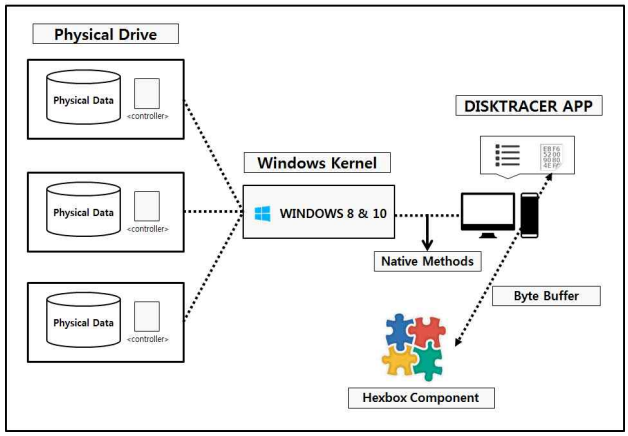

그림 4. 시스템 구성도

7. 결론

본 논문에서는 다양한 파일시스템 중에서도 현재 각종 촬영장비의 저장장치에서 많이 사용되고 있는 FAT32를 디스크 섹터에 직접 접근하여 파일시스템 구조 시각화 및 파일 복원에 대한 연구를 하였다. 파일의 디렉토리 엔트리를 이용하여 데이터를 복원하고 그 과정에 대한 로그를 기록할 수 있도록 했다. 파일 복원의 경우 아직 시작 단계이지만 계속 연구하여 파일을 대부분 복원할 수 있는 기능을 추가할 것이다.

8. 감사의 말

본 연구는 미래창조과학부 및 정보통신기술진흥센터(IITP)의 서울어코드활성화지원사업(IITP-2016-R0613-16-1093)의 연구결과로 수행되었음.

참 고 문 헌

[1] N.R. Poole, Q. Zhou, P. Abatis, “Analysis of CCTV digital video recorder hard disk storage system”, Digital Investigation, Vol. 5, pp. 85-92, 2009

[2] A., Arffin, j., Slay, K-K,. Choo, “Data Recovery from Proprietary Formatted CCTV Hard Disks Digital Forensics”, Chapter in Advances in Digital Forensics IX, Volume 410 of the series IFIP Advances in Information and Communication Technology pp. 213-223, 2013