NTFS파일시스템 내 데이터 복구

염정현, 지창환*

*중부대학교 (대학생)

NTFS File System Recover in Data

Yeom Jeong Hyun, Ji Chang Hwan*

*Joongbu University(Graduate student)

요 약

컴퓨터 환경이 지속적으로 발전함에 따라 사용되는 데이터의 양이 증가하게 되고 그에 따른 저장장치의 크기도 함께 증가해왔다. 그러나 타인에 의한 바이러스 감염이나 예상치 못한 상황으로 인해 파일 시스템이 손상되는 경우가 빈번하게 발생한다. 또한 손상된 파일 시스템을 복구하기 위해서는 많은 시간이 걸리고, 상황에 따라서 복구하지 못하는 경우도 발생한다. 따라서 파일 시스템의 복구는 중요한 이슈이며, 이와 관련한 해결 방안들이 연구되어 왔다. 본 논문에서는 NTFS 파일시스템 내에 $MFT 내 $Standard_Information, $Filename, $DATA 속성을 통해 MFT내에 resident 속성의 모든 파일에 대한 MACtime, 파일명, 데이터까지 복구하는 과정을 나타낸다.

I. 서론

1.1 배경

컴퓨터 환경이 지속적으로 발전함에 따라 사용되는 데이터의 양이 증가하게 되었고 그에 따른 저장장치의 크기도 함께 증가해왔다. 그러나 타인의 의한 바이러스 감염이나 예상치 못한 상황으로 인해 파일 시스템이 손상되는 경우가 빈번하게 발생한다. 또한 손상된 파일 시스템을 복구하기 위해서는 많은 시간에 걸리고, 상황에 따라서 복구하지 못하는 경우도 발생한다. 따라서 파일 시스템의 복구가 중요한 이슈가 되어 왔으며, 이와 관련한 해결 방안들이 연구되어 왔다. 그래서 우리는 파일 시스템 백업 및 복구를 구현하고 파일 시스템의 핵심적인 부분인 $MFT내에서 데이터를 복구를 직접 구현해 보고자 한다.

1.2 관련 연구

1.2.1 NTFS(New Technology File System)

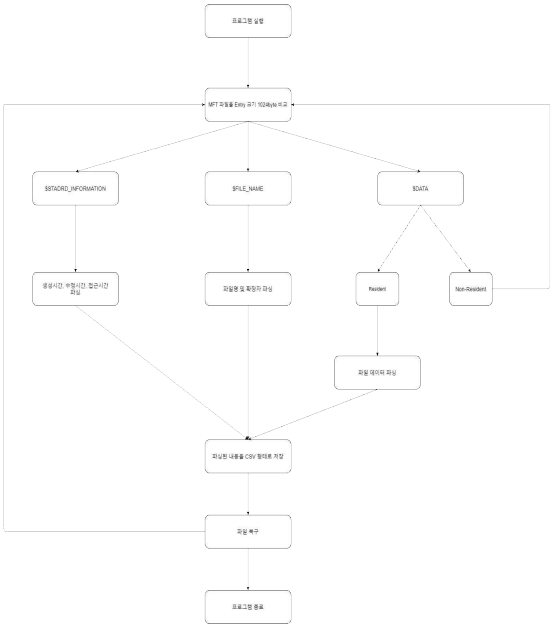
NTFS는 FAT파일시스템의 한계를 개선한 윈도우 NT 계열 파일시스템이다. NTFS 파일 시스템은 디스크 손상과 시스템 고장을 복구하는 능력과 하나의 파일을 열면 파일의 보안 속성을 관장하는 보안 속성을 관장하는 보안 서술자를 가진 파일 객체로 구현된다.[1]

1.2.2 MFT(Master File Table)

MFT는 NTFS파일시스템의 핵심적인 역할로서 볼륨에 존재하는 모든 파일과 디렉터리에 대한 정보를 가진 테이블이다. 파일과 디렉터리와 관련된 대부분의 정보가 MFT에 저장되고 파일과 디렉터리의 개수와 MFT Entry의 수는 비례한다.

MFT Entry는 NTFS 파일시스템에서 하나의 파일 또는 폴더를 하나의 MFT Entry가 할당된다. MFT Entry크기는 1024바이트로 고정, 처음 48바이트 헤더 필드 후 속성의 헤더와 속성의 컨텐츠들이 따라온다.[2][3]

1.3 제안 방법



$MFT 파일을 추출하면 해당 파일 내부에는 많은 파일들의 대한 컨텐츠들을 담고 있다. 내부의 각각의 파일들은 파일 시그니처를 지니고 있는데 먼저 파일 시그니처를 찾아준 후 필수적으로 존재하는 $Standard_Information, $Filename, $Data 속성들의 속성 식별값을 이용하여 해당 속성들이 존재하는지 확인한다. 그리고 $Data 속성에서는 resident or non-resident 속성인지 구분한다.

본 논문에서는 별도의 클러스터를 할당한 non-resident 속성이 아닌 resident 속성의 데이터를 복구하는 것을 목적으로 하기 때문에 resident 속성의 데이터 정보만을 저장한다.

$Standard_Information 속성에서는 파일의 대한 MACtime 정보, $Filename 속성에서는 파일 이름, 파일 확장자 정보, $Data 속성에서는 앞에서 언급했던 것과 같이 resident 속성의 데이터 값을 정보를 저장한다. 다음과 같이 저장한 정보들을 바탕으로 파일을 복구, csv파일로 문서화하였다.

II. 결론

본 논문에서는 NTFS File system, MFT, MFT 속성에 대한 정보를 이용하여 MFT내에 저장되어 있는 삭제된 데이터의 대한 복구 과정을 다뤘다. 또한 Python을 통해 구현하여 실험 하였고, 그 결과 MFT내에 데이터가 저장되는 방식인 Resident 방식의 파일들은 삭제된 파일이나 존재하는 파일 모두 복구가 되는 것을 확인하였고, 포렌식 측면에서 파싱된 MFT내에 존재하는 데이터들에 대한 수집이 원활하게 이뤄졌다.

향후 연구에서는 MFT에 하나의 Entry내에 $DATA 속성이 두 개가 존재하는 파일에 대한 복구가 필요하고, 성능 개선을 통해 시간을 더욱 단축할 수 있는 연구가 필요하다.

[참고문헌]

[1] https://ko.wikipedia.org/wiki/NTFS

[2] 김용식, 최명렬, 장태주, 류재철 하드디스크의 물리적 섹터 접근 방법을 이용한 MFT 기반 증거 파일 탐색 기법, 정보보안 논문지 제8권 제 4호 pp66-68

[3] Rincy Roy Oommen, Princy Sugathan,(저자) 'Recovering Deleted Files from NTFS'(논문제목), International Journal of Science and Research(논문지), Volume 5, Issue 5(논문 권, 호), pp.205-208(페이지)/ p.205, 2016

[4] Suleyman Gokhan TASKIN, Ecir Ugur KUCUKSILLE 'Recovering Ddata Using MFT Records in NTFS File System, International Symposium on Innovative Technologies in Engineering and Science, S.G.TASKIN et al./ ISITES2018 Alanya-Antalya, pp448-456