File System Forensics

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

1. File System Forensic Analysis

- ✓ (FAT/NTFS) Recovery for Deleted Files
- ✓ (FAT/NTFS) Unallocated Cluster Analysis
- ✓ (FAT/NTFS) Slack Space Analysis
- ✓ (FAT/NTFS) Timestamp Analysis
- ✓ (FAT/NTFS) Signature Analysis
- ✓ (FAT/NTFS) Hidden/Encrypted File Analysis
- ✓ (FAT/NTFS) Boot Sector Analysis
- ✓ (FAT/NTFS) Wasted Area Analysis
- ✓ (NTFS) Metadata File Analysis
- ✓ (NTFS) Log Data Analysis
- ✓ (NTFS) $DATA Analysis

Recovery for Deleted Files

- 최근 삭제된 파일이나 사건이 일어난 시점에 삭제된 파일은 우선 분석 대상
- 파일시스템에서 파일 삭제 시 실제 데이터 삭제 없이 메타정보만 수정
- 따라서, 삭제된 파일의 메타정보 구조가 덮어써지지 않았다면 거의 완벽하게 파일 복구
- **NTFS** : 비연속적/연속적으로 할당된 파일 모두 완벽하게 복구 가능
- **FAT** : 비연속적으로 할당된 파일은 부분적인 복구만 가능 (FAT 테이블의 초기화로 연결정보가 사라짐)

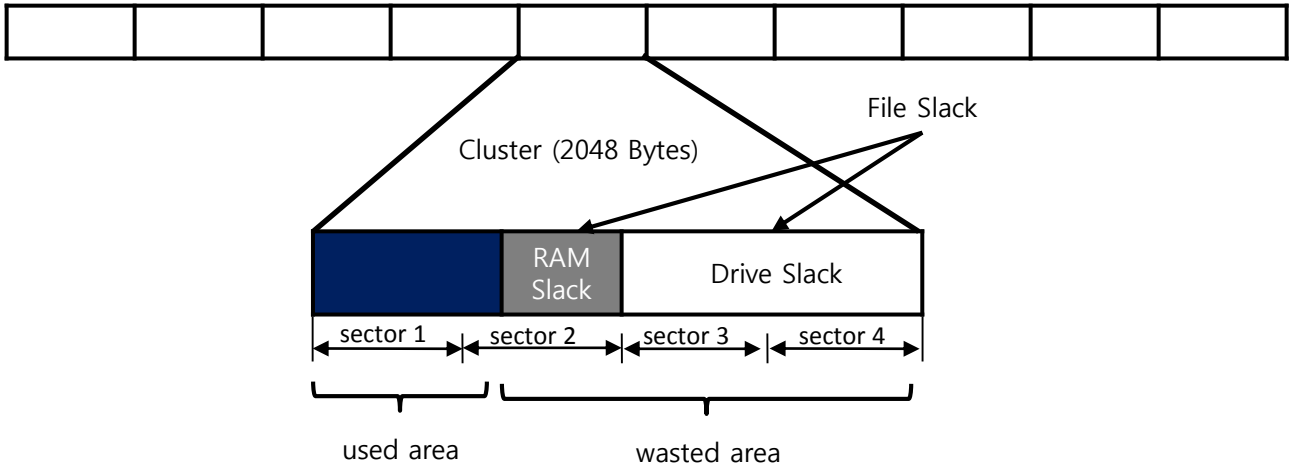
- **삭제된 파일 탐색**
  - **FAT12/16/32** : 루트 디렉터리부터 탐색하면서 디렉터리 엔트리(Directory Entry) 첫 바이트가 0xE5인 엔트리 수집
  - **exFAT** : 파일 디렉터리 엔트리(File Directory Entry) 값이 0x05인 엔트리 수집
  - **NTFS** : $MFT 의 $BITMAP 속성에서 0x00 값을 가지는 MFT 엔트리 조사 /
  - MFT 엔트리 헤더 Flags 값이 0x00인 MFT 엔트리 수집

Unallocated Cluster Analysis

- 대용량 저장매체의 일반적인 사용으로 많은 공간이 비할당 영역일 가능성
- 비할당 클러스터에는 이전 데이터가 남아 있을 가능성
  - 포맷하기 이전 데이터
  - 삭제된 이후 메타정보가 삭제된 파일
- 비할당 영역이 판별될 경우 해당 영역을 대상으로 문자열 추출 및 데이터 카빙 수행

- **비할당 클러스터 영역 수집**
  - **FAT12/16/32** : FAT 영역에서 0x00 값을 가지는 클러스터를 순차적으로 연결
  - **exFAT** : 할당 비트맵 테이블(Allocation Bitmap Table)에서 0x00 값을 가지는 클러스터를 순차적으로 연결
  - **NTFS** : $Bitmap 메타데이터 파일에서 0x00 값을 가지는 클러스터를 순차적으로 연결

Slack Space Analysis



- 슬랙 공간에는 의도적으로 삽입한 데이터나 이전 파일의 데이터가 남아 있을 가능성
- 저장매체 용량과 각 파티션 크기의 차이가 존재하는지 확인 ➔ 볼륨 슬랙
- **슬랙 공간**
  - 램 슬랙 (RAM Slack)
  - 드라이브 슬랙 (Drive Slack)
  - 파일시스템 슬랙 (File-System Slack)
  - 볼륨 슬랙 (Volume Slack)

Timestamp Analysis

- 파일시스템은 파일의 생성/수정/접근 시간 정보 기록
- 사건 발생 시점을 중심으로 데이터 분석 가능
- 시간의 역전 및 의도적인 조작이 발생했는지 파악

- **시간 정보 위치**
  - **FAT12/16/32** : 파일의 디렉터리 엔트리 (DOS Timestamp)
    - Created Date/Time, Last Written Date/Time, Last Accessed Date
  - **exFAT** : 파일의 파일 디렉터리 엔트리 (DOS Timestamp + Time Zone Offset)
    - Created Date/Time, Last Date/Modified Time, Last Accessed Date/Time
  - **NTFS** : MFT 엔트리 및 $I30 인덱스의 속성 정보 (Windows 64-Bit Timestamp)
    - $STANDARD_INFORMATION, $FILE_NAME

Signature Analysis

- 파일 시그니처와 확장자가 일치하는지 검사
- 확장자 변경을 통해 의도적으로 파일을 은폐할 가능성

- **확장자 위치**
  - **FAT** : 파일의 디렉터리 엔트리
  - **exFAT** : 파일의 파일 이름 확장(File Name Extension) 디렉터리 엔트리
  - **NTFS** : 파일의 $FILE_NAME 속성

Hidden/Encrypted File Analysis

- **숨긴 파일(Hidden File) / 암호화된 파일**
  - 사용자의 의도적인 행위가 포함됐을 가능성

- **숨긴 파일 탐색**
  - **FAT** : 디렉터리 엔트리의 속성값이 0x02를 가지는 파일 탐색
  - **exFAT** : 파일 디렉터리 엔트리의 파일 속성값이 0x02를 가지는 파일 탐색
  - **NTFS** : $STANDARD_INFORMATION 속성의 플래그 값이 0x0002를 가지는 파일 탐색

- **암호화된 파일 탐색**
  - **NTFS** : $STANDARD_INFORMATION 속성의 플래그 값이 0x4000를 가지는 파일 탐색
    - 레지스트리의 암호화된 private key 복호화 (Brute Force)
    - EFS0.TMP 파일 조사

Boot Sector Analysis

- 부트 코드를 의도적으로 수정 가능성 ➔ 루트킷

- **방지 대책**
  - 부트 코드 분석을 통해 임의적인 흐름 변경이 있는지 분석

Wasted Area Analysis cont.

- 낭비되는 영역은 악의적인 데이터의 은폐 목적으로 사용될 가능성

- **공통된 낭비 영역**
  - MBR 사용으로 인해 62 섹터의 낭비되는 영역 (MBR Slack)

- **FAT12/16/32**
  - 예약된 영역(Reserved Area) 내의 낭비되는 섹터 (0,1,2,6,7,8 섹터 제외) 조사
  - FSINFO의 사용되지 않는 영역 (1,7 섹터) 조사
  - 예약된 영역 내의 추가적인 부트 코드 영역 (2,8 섹터) 조사

Wasted Area Analysis

- **exFAT**
  - VBR의 확장 부트 코드 영역(1~8 섹터) 및 예약된 영역(10 섹터) 분석 ➔ ???? 정말로?
  - 백업 VBR 영역 조사
- **NTFS**
  - VBR에서 부트 섹터와 부트 로더 위치 항목이 기록된 섹터를 제외한 영역 조사
  - MFT 엔트리 12-15번 영역 조사
- **HPA(Host Protected Area), DCO(Device Configuration Overlay)** ??

Metadata File Analysis

- **$Boot 메타데이터 파일 분석**
  - $Boot는 부트 섹터의 내용을 저장
  - $Boot 파일의 크기는 제한 없음 ➔ 크기를 늘려 데이터 은닉

- **$BadClus 메타데이터 파일 분석**
  - $BadClus 파일은 배드 섹터가 포함된 클러스터 관리
  - 정상적인 클러스터를 $BadClus에 등록 후 의도한 데이터 저장

Log Data Analysis

- **$LogFile 메타데이터 파일 분석**
  - $LogFile은 메타데이터 파일의 트랜잭션 정보를 로그로 저장
  - $LogFile 분석을 통해 최근 사용자의 행위 재구성

- **$UsnJrnl 메타데이터 파일 분석**
  - $UsnJrnl은 파일의 변경 정보를 기록
  - $UsnJrnl 분석을 통해 최근 사용자의 행위 재구성

$DATA Analysis

- **ADS (Alternate Data Stream)**
  - ADS를 데이터 은닉의 목적으로 이용할 가능성
  - $DATA 속성을 두 개 이상 가지는 MFT 엔트리 조사

- **디렉터리의 $DATA 속성**
  - 디렉터리의 $DATA 속성은 일반적으로 사용되지 않음
  - 임의의 데이터를 은닉할 가능성
  - 디렉터리의 MFT 엔트리를 검사하여 $DATA 속성이 존재하는지 조사

질문 및 답변