ARGOS 하계 정보보호 교육

Digital Forensic

2회차 – 디스크 포렌식

발 표 자 | 23학번 나소진

E-Mail | sjna@o.cnu.ac.kr

2024.08.22

CONTENTS

목차

01 강의 개요

02 Disk Image

03 File System

04 Windows 주요 아티팩트

05 과제 안내

CHAPTER
01

강의 개요

강의 구성 및 계획

강의 개요

- 강의 구성

  - 2~3회차 사전 준비 필수 → 카카오톡으로 안내 예정
  - 질문은 떠오르는 즉시 해주기
  - 과제는 필수는 아니지만, 제출 시 발표자 행복

강의 개요

- 주차별 계획

Week 1 (8/16)
숨겨진 데이터 찾기와 손상된 파일 복구

- Digital Forensic 개요
- File Format
- Steganography

Week 2 (8/22)
디스크 포렌식

- Disk Image
- File System
- Windows 주요 아티팩트

Week 3 (8/29)
메모리 포렌식

- 휘발성 데이터
- Volatility

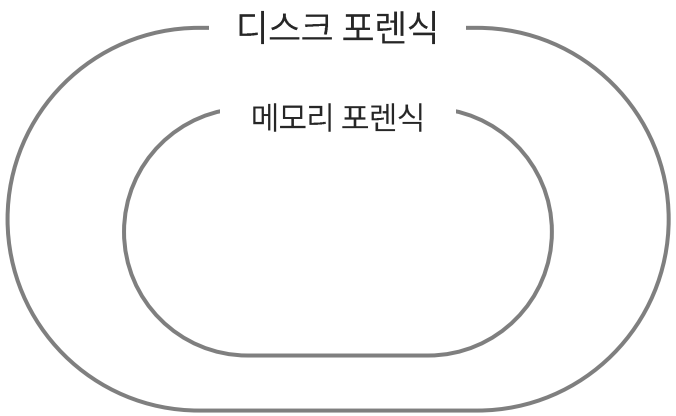
강의 개요

- 디스크 포렌식 개요
  - 정의
    - 저장매체에 대한 디지털 포렌식
  - 대상
    - 데스크탑, 노트북, 외장형 HDD, SSD, USB 등

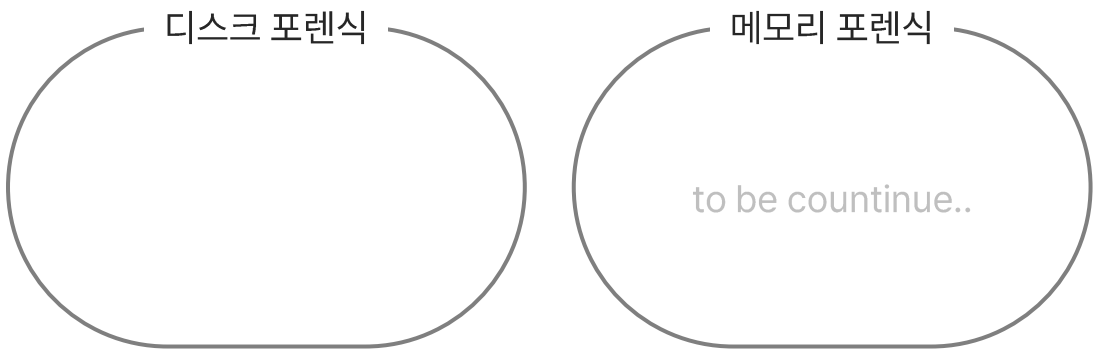
강의 개요

- 디스크 포렌식 개요
  - 일반적으로 활성 데이터 포렌식 포함하여 지칭

  → 메모리 포렌식을 포함하는 개념



일반적인 개념



강의를 위해 분리된 개념

CHAPTER

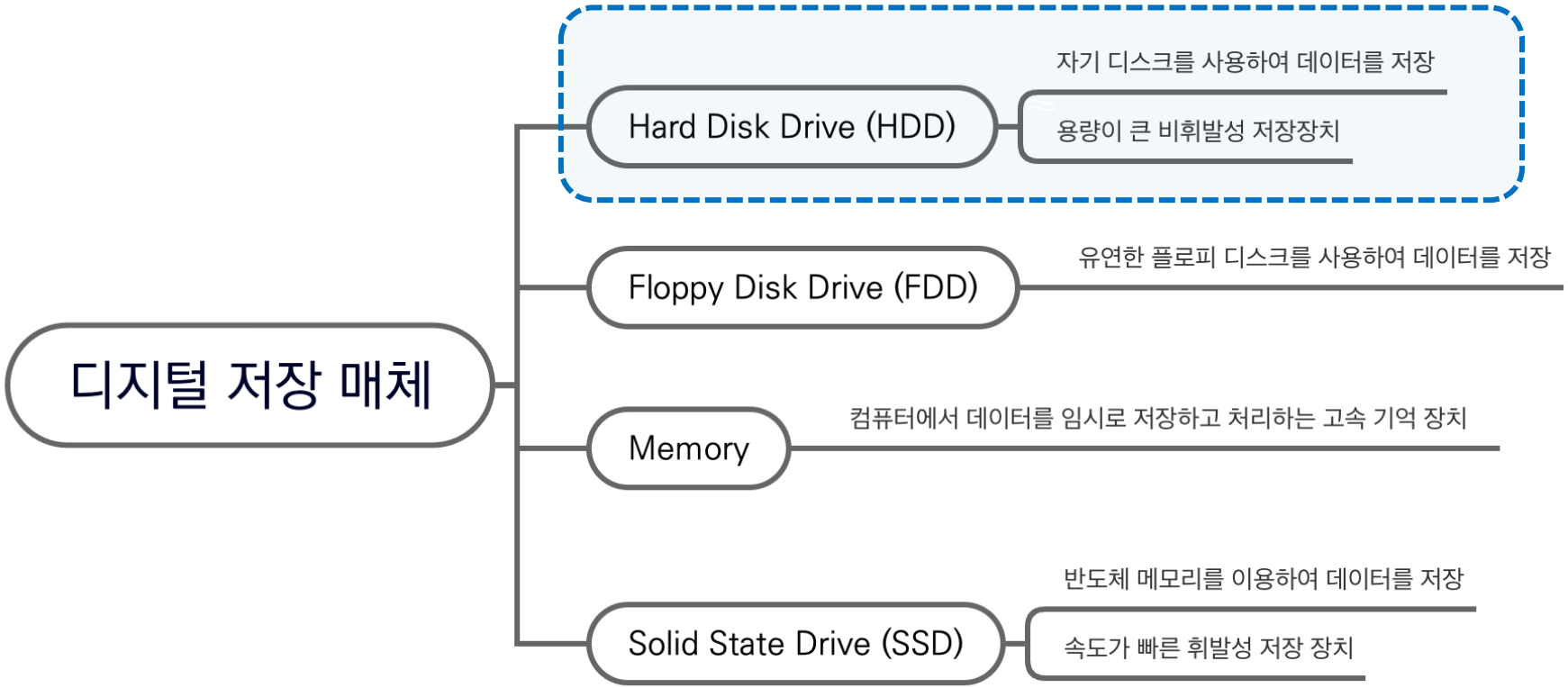
02

Disk Image

저장 매체의 분류와 디스크 이미지의 이해

Disk Image

- Disk Image 개요



Disk Image

- Disk Image 개요
  - 정의
    - 데이터를 수집 시, 원본 보존과 분석을 위해 모든 데이터를 복제하는 행위
  - 목적
    - 특정 시점의 데이터를 보존
    - 이미지의 해쉬값을 부여 → 디지털 증거 데이터의 무결성을 보장

Disk Image

- Disk Image 개요
  - 대상
    - 물리 드라이브
      - 디스크 전체, MBR 정보와 논리적으로 파티셔닝된 다른 불륨까지 포함
    - 논리 드라이브
      - 파티셔닝된 불륨 (C 드라이브, D 드라이브 등)

Disk Image

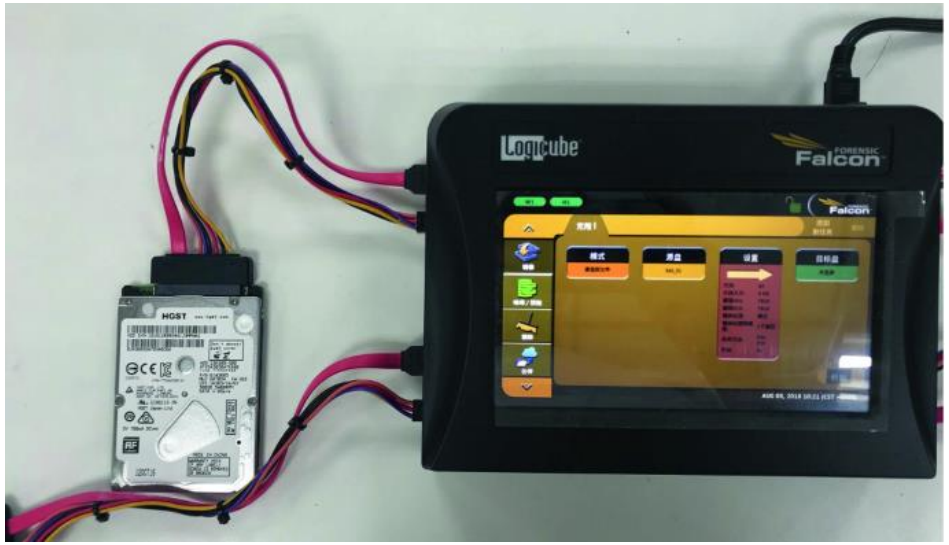
- File Format
  - RAW
    - 원본과 완전히 동일한 형태의 이미지 파일 생성
    - 이미징에 오랜 시간 소요
    - RAW 이미지 형식을 변형한 확장자

Disk Image

- File Format
  - EWF(Expert Witness Compression Format)
    - 생성일, 생성자, 해시 등 메타데이터를 포함하여 압축 기능 및 암호화 기능 제공
    - 종류
      - .E01
        - EWF 포맷의 기본 파일 형식
      - .Ex01
        - EWF 포맷의 확장 파일 형식
        - 특정 도구에서만 사용 (ex. Encase v7 이상)

Disk Image

- 이미징 방법
  - 하드웨어를 이용한 방법
    - Forensic Falcon, Tableau Forensic Imager 등



[Forensic Falcon을 사용하는 모습]

이미지 출처. “Forensic Analysis of Play Station 4”, SPRINGER LINK

Disk Image

- 이미징 방법
  - 소프트웨어를 이용한 방법
    - Encase, FTK Imager 등

장점 : 다양한 기능을 제공

단점 : 비싼 가격, 개인이 구매 불가

장점 : 오픈 소스

단점 : 다른 SW에 비해 자동 분석 기능이 부족

Disk Image

- 실습
  - 로컬에서 파티션 나누기
  - 분리된 파티션의 불륨에 파일 생성 및 삭제
  - 파티션 이미징
  - 이미지 마운트

CHAPTER

03

File System

파일 시스템 및 삭제된 파일 복구 방법의 이해

- Why do we study "File System"?
  - 손상된 디스크 이미지 파일 복구 가능

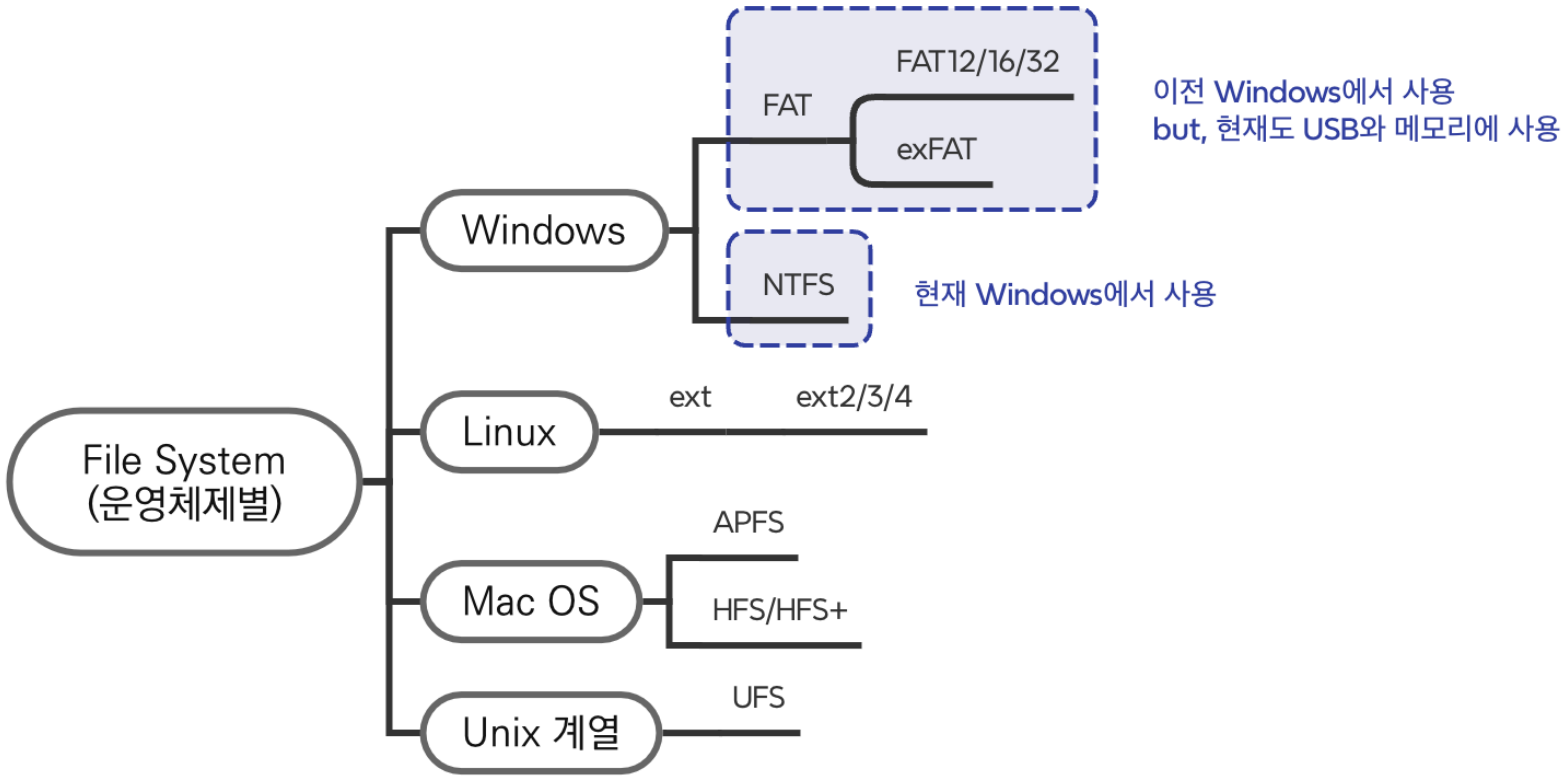
    → File System의 구조 학습 필요
  - 디스크 내에 존재하는 삭제된 파일 복구 가능

    → File System 중 MTF, unallocated space에 대한 학습 필요

- File System 개요
  - 정의
    - 컴퓨터에서 파일이나 자료를 쉽게 발견 및 접근할 수 있도록 보관 또는 조직하는 체제
  - 사용 목적 및 기능
    - 데이터는 '파일' 형태로 저장 장치에 저장 → 증가하는 파일을 관리하는 시스템 필요
    - 압축, 암호화, 동적 할당 등의 추가기능을 지원
  - 분류

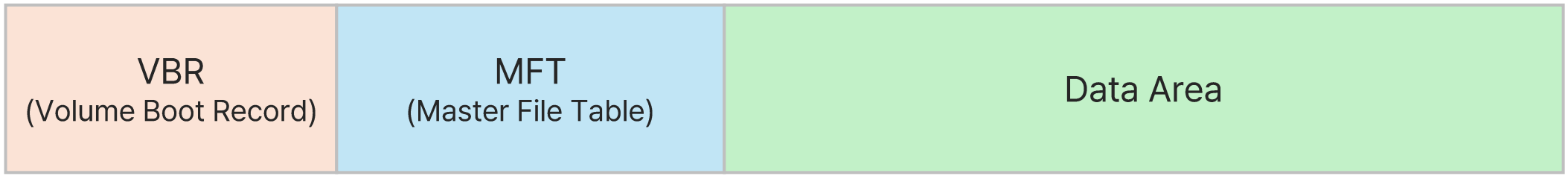
Disk | Flash | CD-ROM | Network | Virtual File

- Disk file system 분류



File System

- NTFS 개요
  - 등장배경
    - 윈도우 NT 운영체제의 등장으로 서버용 운영체제에서 사용하기 위한 새로운 기능을 추가한 파일시스템 필요
  - 구조



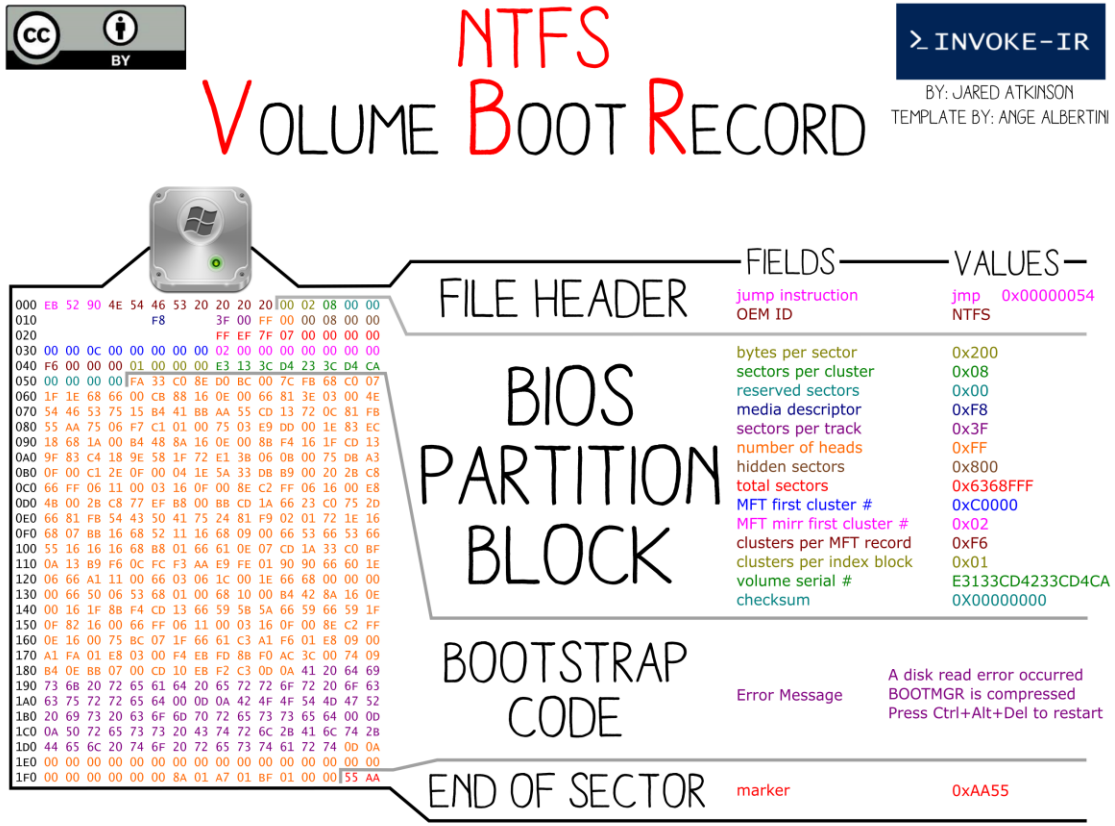
File System

- VBR(Volume Boot Record)
  - NTFS로 포맷된 파티션의 첫 번째 섹터에 위치하는 영역
  - 해당 볼륨의 여러가지 설정 값, 부팅을 위한 실행 코드 포함
  - 부팅 시 POST(Power On Self-Test) 과정 후 VBR 호출
  - 2개 이상의 파티션이 존재할 경우 MBR이 존재 (Master+VBR)

File System

- VBR(Volume Boot Record)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS ....
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	90	BD	1D	.....ø..?.ÿ...½.
00000020	00	00	00	00	80	00	80	00	FF	8F	11	00	00	00	00	00	....€.€.ÿ.....
00000030	55	BB	00	00	00	00	00	00	02	00	00	00	00	00	00	00	U»..............
00000040	F6	00	00	00	01	00	00	00	99	46	6B	54	65	6B	54	16	ö.......™FkTekT.
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	....ú3ÀŽÐ¼.|ûhÀ.
00000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ë^...f.>..N
00000070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.´A»ªUÍ.r..û
00000080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uªu.÷Á..u.éÝ..ƒì
00000090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..´HŠ...‹ô..Í.
000000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸƒÄ.žX.rá;...uÛ£
000000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Û¹. +È
000000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.......ŽÂÿ...è
000000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Èwï¸.»Í.f#Àu-
000000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ûTCPAu$.ù..r..
000000F0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.».hR..h..fSfSf
00000100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h¸.fa..Í.3À¿
00000110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..¹ö.üó ªéþ...f`.
00000120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f¡..f.....fh...
00000130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..´BŠ..
00000140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...‹ôÍ.fY[ZfYfY.
00000150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	.‚..fÿ.......ŽÂÿ
00000160	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u¼..faÃ¡ö.è..
00000170	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	¡ú.è..ôëý‹ð¬<.t.
00000180	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	´.»..Í.ëòÃ..A di
00000190	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc
000001A0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	curred...BOOTMGR
000001B0	20	69	73	20	63	6F	6D	70	72	65	73	73	65	64	00	0D	is compressed..
000001C0	0A	50	72	65	73	73	20	43	74	72	6C	2B	41	6C	74	2B	.Press Ctrl+Alt+
000001D0	44	65	6C	20	74	6F	20	72	65	73	74	61	72	74	0D	0A	Del to restart..
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001F0	00	00	00	00	00	00	8A	01	A7	01	BF	01	00	00	55	AA	......Š.§.¿...Uª

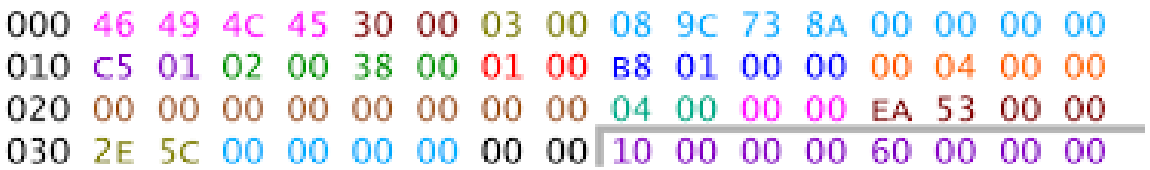


File System

- MFT(Master File Table)
  - NTFS의 핵심으로 파일의 Meta Data를 저장하는 영역
  - 파일이나 디렉토리가 생성될 때마다 MFT 엔트리가 생성
  - 구성
    - MFT Entry Header - Fixup Array – Attributes - End Marker - Unused Space

File System

- MFT(Master File Table)
  - MFT Entry Header 분석



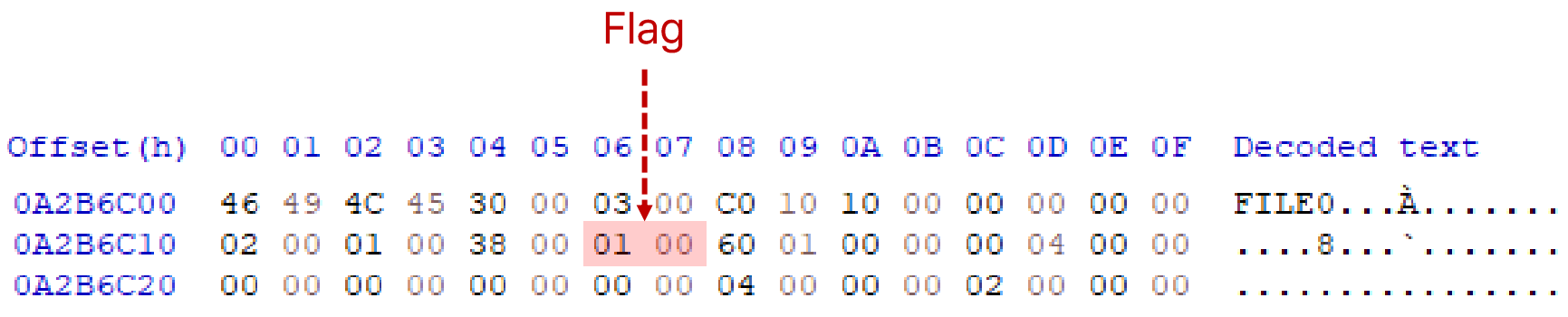
FIELDS	VALUES
magic	FILE
offset to us	0x30
size of us	0x03
logical sequence number	8A739C08
sequence number	0x1C5
hardlinks	0x02
offset to attributes	0x38
flags	0x01
real size	0x1B8
allocated size	0x400
reference to base	0x0000000000000000
next attribute id	0x04
alignment bytes	0x00
record numbers	0x53EA
update sequence	0x02 0x00
update sequence array	0x00 0x00 0x00 0x00

File System

- 삭제된 파일 복구
  - 파일 삭제 = File system에서 해당 파일의 Flag를 변경

  → 파일이 차지하고 있는 공간은 할당해제 상태로 변경 (unallocated space)

  - 실제 파일 삭제는 다른 데이터로 덮어 써졌을 때 발생



사용 가능한 Flag 값

0x01 : in use

0x02 : directory

0x03은?

File System

- 실습
  - NTFS.001 이미지 복구
    - Q. 복구된 이미지에서 확인할 수 있는 “컴퓨터 포렌식 가이드라인”의 제정일은?
    - Hint. Not VBR! It’s MBR

- 실습 해설 및 향후 활용 방향

CHAPTER

04

Windows 주요 아티팩트

윈도우 레지스트리와 이벤트 로그의 이해

Windows 주요 아티팩트

- 아티팩트 개요
  - 의미
    - 시스템의 흔적 (by. me0w2en)
    - 디지털 포렌식 과정에서 증거로 사용할 수 있는 모든 데이터
  - 특징
    - 사용자의 행위 및 여러 정보를 담고 있음
    - 사용자의 의지와 상관없이 시스템이나 프로그램에 의해 생성될 수 있음

Windows 주요 아티팩트

- 아티팩트 개요
  - 분석 대상
    - 레지스트리
    - ≈
    - 이벤트 로그
    - 프리패치
    - 웹 브라우저
    - 외부매체 및 기기 연결 흔적 (ex. USB, Printer 등)
    - ...

Windows 주요 아티팩트

- 레지스트리
  - 의미
    - Windows 운영체제에서 작동하는 모든 하드웨어, 소프트웨어, 사용자 정보 및 시스템 구성 요소 등을 담고 있는 계층형 데이터베이스
    - 부팅부터 로그인, 응용프로그램 실행, 사용자 행위 등 모든 활동에 관여
  - 분석 Tool
    - 윈도우 탐색기 – '레지스트리 편집기' 검색
    - 실행(Win+R) – 'regedit.exe' 입력

Windows 주요 아티팩트

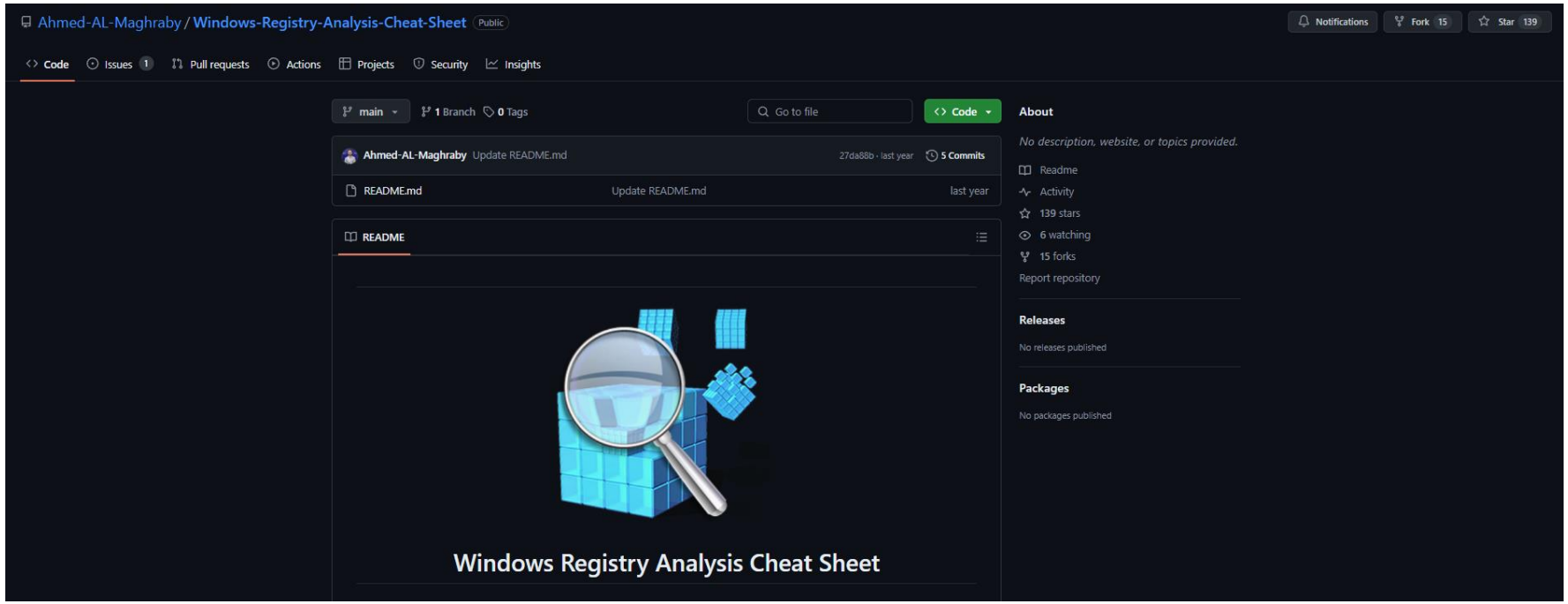
- 레지스트리
  - 분석을 통해 얻을 수 있는 정보
    - 운영체제, 사용자 계정, 시스템 정보
    - 네트워크 연결 목록
    - 응용프로그램 실행 시간, 횟수 등의 이용 기록
    - 자동 시작 프로그램(Autoruns)의 설치/삭제 여부
    - 저장매체 사용 흔적 분석
    - 최근 열람/저장한 문서
  - 사용자/시스템/저장매체 사용 흔적 분석 → 추가적인 포렌식 분석 대상 선별

Windows 주요 아티팩트

- 레지스트리
  - 경로별로 획득 가능한 정보
    - 운영체제 정보 : HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
    - 컴퓨터 이름 : HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
    - 시스템 표준 시간 : HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
    - 컴퓨터 종료 시간 : HKLM\SYSTEM\CurrentControlSet\Control\Windows
    - ...

Windows 주요 아티팩트

- 레지스트리
  - 수많은 레지스트리 경로를 외우는 것은 어려움 → 정리된 자료를 적극 활용!



Windows 주요 아티팩트

- 이벤트 로그
  - 의미
    - 시스템에 접속한 사용자들의 행위들을 저장해 놓은 기록
    - System, Security, Application 등 여러 종류의 파일이 존재
    - 각 파일은 Windows 버전에 따라 기록되는 위치와 형태가 변화
  - 분석 Tool
    - Microsoft사의 Windows Event Viwer
    - Nirsoft사의 FullEventLogView

Windows 주요 아티팩트

- 이벤트 로그
  - 분석을 통해 얻을 수 있는 정보
    - 사용자의 특정 파일에 대한 접근 정보
    - 사용자의 시스템 로그인 성공/실패 여부
    - 특정 어플리케이션 사용 여부
    - 감사 정책 변경 여부
    - 사용자 권한 변경 여부

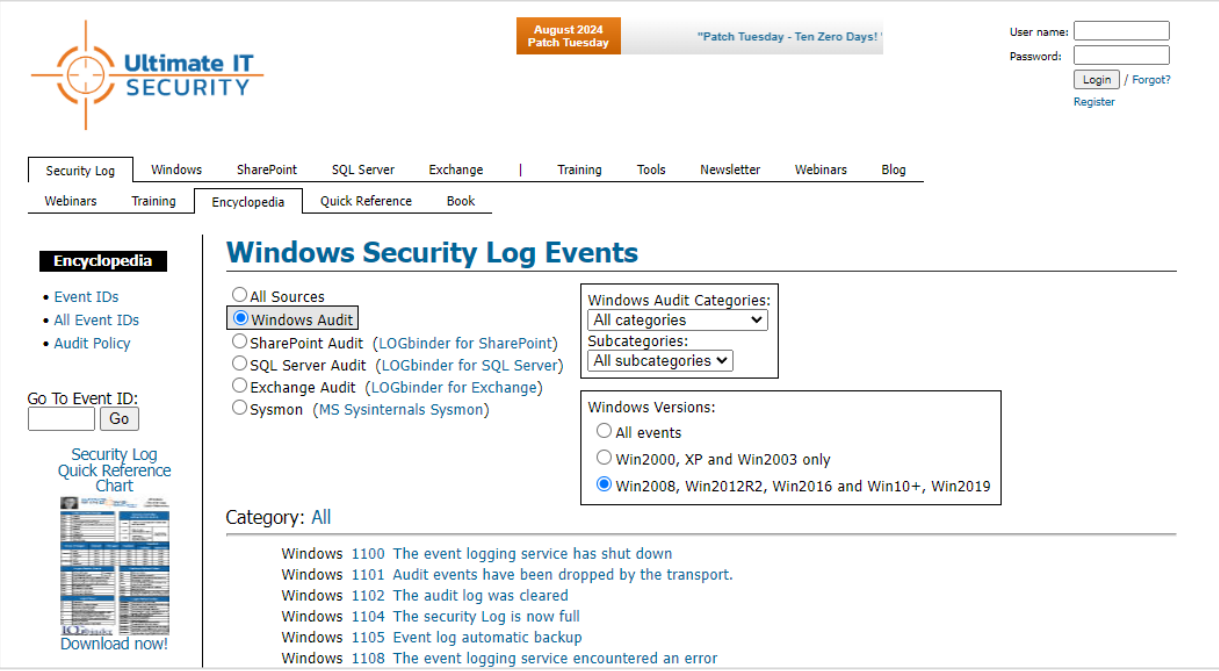
Windows 주요 아티팩트

- 이벤트 로그
  - 주요 이벤트 ID

이벤트 ID		내용
Type 1 (~ Windows 2003)	Type 2 (Windows Vista ~)	
528, 540	4624	로그온 실패 – 알 수 없는 사용자 이름 또는 암호
529	4625	로그온 실패- 시간 제한
530	4625	로그온 실패 – 현재 사용할 수 없는 계정
531	4625	로그온 실패 – 지정한 사용자 계정이 만료됨
532	4625	로그온 실패 – 사용자가 이 시스템에 로그온이 허용되지 않았음
533	4625	로그온 실패 – 허용되지 않은 로그온 유형
534	4625, 5461	로그온 실패 – 지정된 계정 암호가 만료됨
535	4625	로그온 실패- NetLogon 구성 요소가 활성화되어 있지 않음

Windows 주요 아티팩트

- 이벤트 로그
  - 수많은 이벤트 유형을 외우는 것은 어려움 → 정리된 자료를 적극 활용!



Windows 주요 아티팩트

- 실습
  1. REGA로 주어진 레지스트리 파일 분석
  2. 로컬 PC에서 이벤트 로그 확인하기
  3. 이벤트 로그 파일의 CTF 문제 풀이

Windows 주요 아티팩트

- 실습 해설 및 향후 활용 방향

CHAPTER

05

과제 안내

CHAPTER
05 과제 안내

- 과제
  1. RecoveryAndHide 문제 풀이
     → 절대 유출 금지!

- 제출 방법
  - 정답과 풀이 과정을 자유로운 양식으로 작성하여 카카오톡으로 전달

Reference

1. Forensic Proof, http://forensic-proof.com/
2. 디지털 포렌식 A-Z, 충남대학교