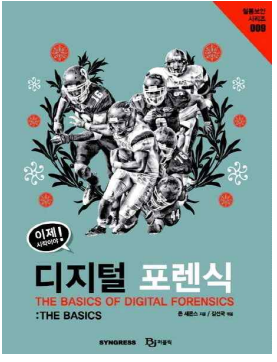
윈도우 시스템에서의 증거 수집

IT융합공학부 윤세영

유투브 주소: https://youtu.be/GKLHgWG_tb4

- 이제 시작이야! 디지털 포렌식
- 존 새몬스 저 / 김선국 역
- 디지털 포렌식 입문용 도서로 좋음



목차

목차

Introduction

- 윈도우(Windows)
- 마이크로소프트가 개발한 컴퓨터 운영 체제
- 데스크톱 시장의 약 70퍼센트 차지

삭제된 데이터 찾기 – File Carving

- 파일 카빙(File Carving)

- 저장 매체의 **비할당 영역**에서 이전에 저장되어 있었던 파일을 복구하는 기법

- 파일 시스템의 파일 메타 정보에 의존하지 않기 때문에 파일 시스템이 존재하지 않거나 고장 난 경우에도 파일 복구가 가능함

김진국 외 4명. (2008). 파일카빙 기법에 관한 연구. *디지털포렌식연구*,(2), 19-31.

최대 절전모드 파일(HIBERFIL.SYS)

- 대기모드

- 데이터가 RAM에 존재, 전력이 없으면 사라지는 휘발성 메모리

  포렌식적으로 도움이 되지 않음

- 최대 절전모드 / 하이브리드 절전모드

- 데이터가 hiberfil.sys 파일에 저장됨

최대 절전모드 파일(HIBERFIL.SYS)

- hiberfil.sys 파일은 Windows 운영체제에서 사용되는 Hibernate 기능에 대한 파일로, 시스템의 현재 상태를 저장함

〈Table 1〉 Comparison of memory storage state and default activation by options

옵션		hiberfil.sys 파일로의 메모리 데이터 저장 여부	저장되는 메모리 영역	기본 활성화 여부
시스템 종료	빠른 시작 ON	O	커널	O
	빠른 시작 OFF	X	-	X
다시 시작		X	-	O
절전 모드		X	-	X
최대 절전 모드		O	커널 + 사용자	O
하이브리드 절전 모드		O	커널	O

방수민 외 7명. (2021). Windows 10 내의 hiberfil.sys 파일에 대한 포렌식 활용 방안. 디지털포렌식연구, 15(1), 125-136.

윈도우 레지스트리

- 레지스트리

- 설정파일을 위한 데이터베이스
- 사용자와 시스템 구성의 설정을 관리
- 레지스트리를 이용하여
  검색어, 실행된 프로그램, 설치된 프로그램, 웹 주소, 최근 실행한 파일 등을 찾아낼 수 있음

윈도우 레지스트리

EnCase 실행화면

FTK

http://forensic.korea.ac.kr/DFWIKI/index.php/EnCase
https://en.wikipedia.org/wiki/Forensic_Toolkit

프린터 스풀링

- 프린터 스풀링(Printer Spooling)

- (PC에서 프린트를 진행할 경우)
  PC 내 임시파일 형태로 프린트와 관련된 데이터를 저장하고 이를 프린터기에 전송함
- 데이터는 .SHD, .SPL 형태로 저장되며, 이들을 **스풀 파일(Spool File)**이라고 부름

메타데이터

- 메타데이터

- 데이터를 설명해주는 데이터

  (ex: 사진의 메타데이터 – 찍은 시간, 이미지 크기, 파일 크기 등)

- 만든 날짜, 수정된 날짜, 액세스한 날짜 등의 정보를 가지고 있음

썸네일 캐시

- 썸네일(thumbnail)

- 컴퓨터에 있는 사진을 좀 더 쉽게 볼 수 있도록 미리보기 형태로 사진을 작게 만든 것
- 썸네일 파일은 사용자가 "미리보기"를 윈도우 탐색기에서 선택하면 윈도우가 자동으로 생성함
- 윈도우 버전에 따라 thumbds.db 혹은 thumbcache.db 라는 이름으로 파일을 생성함

- 썸네일 파일의 존재 자체가 시스템에서 특정 시점에 사진이 존재했다는 것을 보여줌

복원 지점과 섀도우 복사

- 복원 지점

- 정상적으로 동작하던 컴퓨터에 미리 복원 지점을 생성하여
  오류가 생겼을 때, 문제 발생 이전으로 복원하는 기능

- 복원 지점의 생성 시기를 이용하여
  특정 데이터가 시스템에 언제부터 존재하였는지를 판단할 수 있음

복원 지점과 섀도우 복사

- 섀도우(shadow) 복사

- 복원 지점의 소스 데이터

- 섀도우 파일을 사용하여 특정 파일이 시간 경과에 따라 어떻게 변화하였는지 증명할 수 있음

링크 파일

- 링크 파일

- 연결로 지정된 파일 및 디렉터리에 접근하여 읽고 쓰는 프로그램
  (ex: 바로가기)
- 링크 파일 자체에도 날짜와 시간 정보가 저장되어 있음


Q&A