증거 수집

1 온라인 수집

1.1 라이브데이터

구분	수집 항목
비활성	프리패치, 최근 파일 캐시
활성	네트워크 정보
활성	물리메모리
활성	프로세스 정보
활성	사용자 로그온 정보
활성	시스템 정보
활성	네트워크 인터페이스 정보
활성	작업스케줄러, 클립보드, 자동실행 정보
비활성	MBR, VBR, 파일시스템 메타데이터, 파일시스템 로그
비활성	레지스트리, 이벤트 로그
비활성	바로가기, 점프 목록
비활성	%SystemRoot% 하위 주요 파일
비활성	웹 브라우저 아티팩트
활성	네트워크 패킷

시스템 전원이 켜져 있는 상태에서 수집할 수 있는데이터를 말한다. 활성 데이터, 메모리 덤프, 비활성 주요 데이터를 포함한다. 이벤트의 원인을 가장 잘 알려줄 수 있는 데이터이다.

- 활성데이터
  - 네트워크 정보, 프로세스 정보, 사용자 로그온 정보, 시스템 정보, 네트워크 인터페이스 정보, 작업스케줄러 정보, 클립보드 정보, 자동실행 정보

- 물리메모리
    - 활성데이터에서 네트워크 정보 다음으로 수집해야한다.
- 비활성주요데이터
    - 파일시스템 메타데이터파일시스템, 이벤트로그
    - 레지스트리, 프리패치
    - 바로가기, 점프 목록
    - 웹브라우저 흔적
    - %SystemRoot@system32₩drivers₩etc
    - %SystemRoot@system32₩config₩systemprofile
- 네트워크 패킷

1.2 저장장치 복사

- 이미징 불가능 or 빠른 분석이 필요
- 라이브 상태에서 주요 분석 데이터 수집
  - 리눅스 시스템의 경우, "/var/log" 폴더
  - 윈도우 시스템의 경우,
    - 웹 브라우저 데이터 수집
    - 이메일 스토리지 파일 수집
    - 볼륨 섀도 복사본 수집
    - 대용량 로그(웹 로그, 애플리케이션 로그 등) 수집
    - 데이터 베이스 파일 수집
    - 특정 시간을 기준으로 생성/수정/접근된 파일 수집
- 특정 폴더나 파일로 제한
    - 라이브 환경에서 특정 시간 대역이나 사용자 행위를 중심으로 파일 검색 후 추출
    - 라이브 환경에서 특정 키워드를 중심으로 검색 후 추출

1.3 저장장치 이미징

- 컴퓨터 전원을 끌 수 없는 경우 라이브 상태에서 저장장치 이미징
- 논리적인 구성(RAID, LVM 등)의 경우에도 라이브 저장장치 이미징 수행!!
- 주로 소프트웨어를 사용해 이미징
- 로컬 이미징
  - 로컬에 직접 연결하여 이미징 수행
  - 여분의 저장장치 슬롯을 이용
  - 외부 인터페이스(USB/IEEE 1394/eSATA 등) 이용
- 원격이미징
  - 네트워크 케이블을 이용해 이미징 수행
  - 여분의 네트워크 포트를 이용하거나 서비스 포트를 사용
  - 서비스 가용성을 고려하여 여유 시간대나 트래픽을 제한하여 이미징

2 오프라인수집

2.1 저장장치 복사

- 원본읽기 -> 사본쓰기
- 장점
  - 필요한 데이터만 비교적 손쉽게 수집 가능 신속한 분석
- 단점
  - 파일과 디렉터리 단위의 정보만 획득하는 일반적인 복사
  - 원본의 메타 정보를 별도로 관리해야 함
  - 삭제된 파일이나 슬랙에 은닉된 데이터는 확인할 수 없음
- 압수수색 대상이 특정 폴더나 파일로 제한될 경우
  - 라이브 상태에서 특정 시간 대역이나 사용자 행위를 중심으로 파일 검색 후 추출
  - 라이브 상태에서 특정 키워드를 기준으로 검색 후 추출

- 저장장치 복제/이미징 작업 동안 사전 분석을 위한 데이터
  - 쓰기방지장치를 장착한 상태에서 사전 분석 데이터 추출
  - 비활성 데이터 수집 시간 VS. 사전 분석 효율
  - 파일시스템 메타데이터, 레지스트리, 프리패치, 바로가기 파일, 이벤트 로그 등

2.2 저장장치 복제

- 원본 모든 섹터 -> 사본 저장장치
- 비트스트림 복제
- 장점
  - 원본과 동일하기 때문에 삭제된 파일 복구 가능
  - 일반적으로 이미징보다 속도가 빠름
  - 현장 대응 방식으로 주로 사용
- 단점
  - 매 복제마다 원본보다 크거나 동일한 사본 저장장치 필요 사본 저장장치의 부담
  - 사본 저장장치 특성에 의존 (저장장치 오류 및 배드섹터)
  - 복제 전 사본 저장장치의 완전삭제 필요

2.3 저장장치 이미징

- 원본 모든 섹터 -> 이미지 파일
- 비트스트림 이미징
- 장점
  - 원본과 동일하기 때문에 삭제된 파일 복구 가능
  - 사본 저장장치의 완전삭제가 필요 없음
  - 여러 명이 분석할 경우 증거를 쉽게 분배/공유 가능
  - 압축 기능을 이용해 분배 및 저장 효율 증대
  - 암호화 기능을 이용해 안전성 강화
- 단점
  - 압축을 하지 않을 경우, 원본 저장장치보다 더 큰 저장장치 필요
- 포렌식 이미지 형식

- RAW(dd)
  - 원본 저장장치의 순수 비트스트림 이미지
  - 별도의 이미지 파일 처리/보호 매커니즘 X

- Expert Witness E01(Ex01)
  - 엔케이스(EnCase)에서 지원하는 이미지 형식
  - CRC, MD5를 이용하여 이미지 파일의 무결성 확인 가능
  - 압축, 암호화 지원

- 기타 이미지 형식
  - AFF, SMART, IDIF, IRBF, IEIF, ProDiscover IF, SDi32's Format

- **E01 vs. Ex01**

구분	E01	Ex01
압축 방식	DEFLATE	BZIP2
해쉬 알고리즘	MD5, SHA1	MD5, SHA1
보안기능	Password	AES256

2.4 오프라인 수집 도구

- 무결성 유지가 필요없다면
  - 쓰기방지장치 없이 이미징 소프트웨어를 이용해 이미징
  - 저렴한 저장장치 하드웨어 복제 도구를 이용해 복제

- 무결성 유지가 필요하다면
  - 쓰기방지장치 하에서 이미징 소프트웨어를 이용해 이미징
  - 쓰기방지기능이 내장된 포렌식 하드웨어를 이용해 이미징

- 전문 장비 사용의 이점
  - 법적 소송을 대비해 저장물을 관리할 경우
  - 복제 및 이미징 과정에서 대상 장치의 오류나 손상 가능성 최소화
  - 압축, 암호화 기능을 통해 보관의 효율성과 기밀성을 높일 수 있음