1. 디지털 포렌식 분석의 육하원칙

* 분석의 요구사항은 곧 분석의 목적

1. 디지털 포렌식 분석의 육하원칙은 비판적이고 논리 정연한 태도를 유지하기 위한 분석 기법 중 하나
2. Who

관련 데이터

1. 컴퓨터 이름, 컴퓨터 사용자 이름, 문서 작성자, 문서의 마지막 저장자, 이메일 주소, 메신저 아이디, 전화 번호 등
2. 운영체제 설치 일자, 컴퓨터 시동 및 종료 일자, 로그온 및 로그아웃 일자, 프로그램 실행 일자, 파일의 시간 정보 등
3. IP 주소, 네트워크 카드 주소, 공유기 이름, GPS 데이터, 파일의 경로 정보 등
4. 문서 파일, 사진 파일, 녹음 파일, 이메일 첨부파일, 문자 메시지 첨부파일 등
5. 컴퓨터 사용 흔적, 프로그램 실행 흔적, 파일 조작 흔적, 데이터 위변조 흔적, 인터넷 활동 흔적, 외부 장치 연결 흔적, 이메일 등 사용 흔적 등
6. 인터넷 검색어, 윈도우 검색어, 이메일 본문, 메신저 대화 등
   * 누가 관련 되었는가?
   * 누가 타깃 파일을 소유했는가?
   * 누가 그 파일을 그 볼륨에 두었는가?
   * 누가 그 파일을 열람 또는 실행 했는가?
   * 누가 그것을 삭제했는가?
   * 누가 그것을 전송 했는가?
   * 누가 그 컴퓨터를 사용했는가?
7. When
   * 언제 그것이 일어 났는가?
   * 언제 사진을 촬용한 것인가?
   * 언제 열람/삭제/수정/전송 되었는가?
   * 언제 실행되었는가?
   * 언제 마지막으로 접속 되었는가?
8. Where
   * 어디에서 그것이 일어났는가?
   * 어디에 파일이 위치하는가?
   * 어디에 파일이 저장/다운로드 되었는가?
   * 어디로 파일이 배포되었는가?
   * 어디에 로그가 위치하는가?
9. What
   * 발생한 일은 무엇인가?
   * 찾고자 하는/복구하고자 하는 파일은 무엇인가?
   * 관련된 파일은 무엇인가?
   * 해시값이 같은 파일은 무엇인가?
   * 연결된 정보는 무엇인가?
10. How
    * 그런 일이 어떻게 일어났나?
    * 이 파일이 어떻게 그 기기에 저장되었나?
    * 그 파일이 어떻게 다른 사람과 공유되었나?
    * 사용자는 어떻게 다른 사람과 소통하였나?
    * 그 파일이 어떻게 위조/유출/절취되었나?
11. Why
    * 왜 그런일이 일어났나?

2. 디지털 포렌식 분석의 종류

1. 일반적인 분석 형태 정적 분석(Static Analysisi) / 동적 분석(Dynamic Analysis)
2. 정적 분석(Static Analysisi) = Dead Forensics = 사후 포렌식(Post-mortem Forensics)
   * 분석 대상 시스템에서 저장 장치를 분리하고, 분리한 저장장치에 대한 논리적인 증거 이미지 사본을 작성한 후 이것을 대상으로 분석하는 Dead Acquistion에서 비롯된 개념
   * 디지털 디바이스를 범행의 현장으로 취급해야 하는 사안에선 정적 분석이 여전히 주된 분석 기법으로 자리
3. 동적 분석(Dynamic Analysis) = Live Foorensics
   * 트리아지 포렌식(Triage Forensics) : 동작 중인 컴퓨터를 대상으로 함, ‘선별’방식의 분석이 동적 분석의 전형을 이룸, 동적 분석의 한 예
   * 분석 대상 시스템이 동작하는 가운데 디지털 포렌식 분석관의 분석용 외장 하드 드라이브를 연결한 후 직접 조사하는 기법
   * 조사 대상 시스템의 운영체제를 그대로 이용

3. 디지털 포렌식 기술 – 증거 획득

1. 쓰기 방지 기술
   * 정적 분석 경우 필수
   * 쓰기 방지 장치를 사용하지 않을 경우 위험성
     1. 섬네일 이미지가 자동으로 생성될 우려
     2. 로컬 검색 데이터베이스에 색인이 자동으로 일어날 우려
     3. 안티바이러스 소프트웨어에 의한 스캔이 자동으로 일어날 우려
     4. 연결된 드라이브에 수정이 일어날 우려
     5. 타임 스탬프가 변경될 우려
     6. 손상된 파일시스템에 대한 자동 복구가 일어날 우려
   * 위와 같은 많은 위험이 있지만, 가장 조심 해야하는 것은 사람에 의한 실수가 일어날 가능성이 가장 큰 위험성이기 때문에 경각심을 가져야 함
   * 쓰기 방지 장치의 종류
     1. 하드웨어 기반 쓰기 방지 장치

* 운영체제의 종류와는 상관없이 독립적으로 사용 가능
* 가장 안정적으로 쓰기 방지 효과 가져오기 가능
* 별도의 하드웨어가 필요 없어 손쉽게 사용 가능
* 가장 안전한 방법이란 할 순 없음
  + 1. 소프트웨어 기반 쓰기 방지 장치
* 분석 대상 미디어 자체에 쓰기 방지 기능이 있는 경우, 별도의 쓰기 방지 장치가 필요 없을 수 있음

1. 이미징 기술
   * 이미징 = 포렌식 이미징(Forensics Imaging)
   * 이미징의 다른 호칭 : 비트스트림 카피(Bit-Stream Copy), 포렌식 카피(Forensic Copy)
   * 이미징 정의 : 원본인 저장 장치의 데이터를 무결하게 복제해 하나의 논리적인 파일로 만드는 기술
   * 물리적 이미징 (디바이스 전체 대상)
     1. HDD, SSD, USB 메모리 등 저장 장치 전체 대상으로 이미징
     2. 비할당 영역(Unallocated Area), 슬랙 공간(Slack Space), 시스템에서 예약한 영역(Reserved Area)까지 디스크의 첫 번째 섹터에서 마지막 섹터까지 모든 데이터가 이미징 대상
     3. 볼륨 단위의 이미징도 물리적 이미징이라고 부름
     4. 일정한 사유가 있는 경우 예외적으로 물리적 이미징 허용
     5. 포맷 유형 : EWF(Expert Witness Format), DD(Data Dump) 포멧이 유명
   * 논리적 이미징 (디바이스 일부만 대상)
     1. 저장 장치에서 선별된 데이터만을 대상
     2. 대부분 포렌식 이미징은 논리적 이미징 형식으로 이뤄짐
     3. 논리적 이미징 파일 포맷 : EnCase의 .L01 , .Lx01, FTK의 .ad1등
   * 포렌식 이미징 포맷 : 로우 포맷, 포렌식 전용 포맷
2. 디스크 복제 기술
   * 원본 디스크와 같은 물리적 사본 디스크를 만듬 (포렌식 이미징이 원본 디스크와 같은 내용을 갖는 논리적인 하나의 파일을 만드는 것)
   * 동적인 분석 환경이 있어야 하는 상황에 복제 기술 사용
3. 해시값 계산 기술 = 해싱기술
   * 메시지 다이제스트(Message Digest) = 가변 길이로 입력된 데이터 스트림을 일방향 수학적 알고리즘을 이용해 계산한 후, 고정된 길이의 16진수로 보여주는 값