디지털 포렌식 종류

· 컴퓨터 법과학: USB 드라이브, SD 드라이브 등 복원

· 모바일 장치 법과학: 내장된 GPS/ 위치추적 또는 셀 사이트로그 범위 추적, 내장된 통신 시스템(예:GSM)

· 네트워크 법과학: 정보수집 및 로컬 및 WAN/인터넷의 네트워크 트래픽을 모니터링 하고 분석하는 패킷 레벨 분석법

· 데이터 분석 법과학: 금융 범죄로 인한 사기 행위 패턴을 발견 및 분석, 구조화된 데이터 조사

· 데이터베이스 법과학: 데이터베이스와 관련된 포렌식 / 인로그, 데이터베이스 내용, RAM의 타임라인 구축 및 복구

디지털 포렌식 대상물의 특징

· 컴퓨터에서 압수되는 디지털 증거물은 생성/복사/변경/삭제가 용이한 특징을 가지고 있음

- 디지털 증거물의 삭제 및 위조/변조 용이

▶ 디지털 증거물은 압수하기 이전에 삭제 및 위/변조를 하는 경우 이를 복구하거나 위조 및 변조되었다는 것을 확인할 수 있어야 함

▶ 또한 파일의 확장자 등을 변경한 경우를 찾아 다시 복구할 수 있어야 함

- 디지털 증거물의 방대성

▶ 디지털 증거물을 검색 도구 없이 일일이 확인하는 것은 어려움

▶ 검색을 통해 혹은 특정한 파일만을 찾아내는 기술을 적용할 수 있음

- 컴퓨터의 휘발성 메모리

▶ 휘발성 메모리의 내용이 사라지기 전에 수집하는 방안 필요

▶ 범죄 대상의 컴퓨터 화면이나 압수 당시의 실행되는 프로세스를 검출하여 증거 확보

디지털 포렌식 5대 원칙

3. 재현의 원칙

· 피해 직전과 같은 조건에서 현장 검증을 실시하거나, 재판이나 법정의 검증과정에서도 동일한 결과가 나와야 함

- 불법 해킹 용의자의 해킹 툴이 증거능력을 가지기 위해서는 같은 상황의 피해시스템에 툴을 적용할 경우 피해 결과와 일치하는 결과가 나와야 함

4. 신속성의 원칙

· 휘발성 증거의 수집 여부는 신속한 조치에 의해 결정되므로 모든 과정은 지체없이 진행되야 함

5. 연계 보관성의 원칙

· 증거물 획득 ≫ 이송 ≫ 분석 ≫ 보관 ≫ 법정 제출의 각 단계에서 담당자 및 책임자를 명확히 해야 함

· 수집된 저장매체가 이동단계에서 물리적 손상이 발생하였다면, 이동 담당자는 이를 확인하고 해당 내용을 정확히 인수 인계하여 이후의 단계에서 적절한 조치가 취해지도록 해야 함