1. 디지털 포렌식

* 정의 : 디지털 디바이스에 저장된 데이터를 적법한 권원에 의해 획득하고 분석해 법정에서 유효한 증거로 사용될 수 있도록 보고하는 일련의 절차와 기술
* 물리적인 매체에 대해 독립적으로 존재하는 디지털 증거를 다루기 때문에 비디오 테이프나 전송 중인 신호를 대상으로 하는 전통적인 과학 수사와 구별됨
* 적법한 권원에 의해 수행될 것을 요구
  + 법 집행 기관에선 압수 수색영장과 같은 엄격한 법적인 권원 요구
  + 민간기업에선 조사 대상자가 입사 할 때 작성한 ‘비밀유지 서약서(Non-Disclosure Agreement)’의 존재 여부와 디지털 포렌식 조사에 대한 동의서 요구

등 조사의 적법성을 도러낼 수 있는 문서화된 근거 필요

* 단계 구분

한국에선 획득 단계와 분석 단계의 구별이 다소 모호한 편

1. 디지털 증거를 획득하는 단계
   * + 디지털 증거 분석을 위한 선행 절차
     + 데이터 검색, 선별, 변환, 복원 기술 주로 활용
     + 기술의 자동화에 연구 개발이 집중
     + 수사기관의 압수수색 상황에선 획득의 전 단계인 선별 과정에서 더욱 엄격한 법적인 제한이 뒤따름
2. 디지털 증거를 분석하는 단계
   * + 디지털 포렌식 분석관의 경험과 논리적 사고 과정에 관심
     + 분석관은 사건의 전반적인 내용을 이해하는 가운데 분석 과정에선 비판적 사고와 평가, 실험, 융합, 연관성 검증을 기반으로 육하원칙에 따라 사건 현장인 디지털 디바이스에 남겨진 증거에 대해 무엇, 언제, 어디서, 어떻게 생성되고, 누가, 무슨 이유에 의한 결과인지 물음
     + 디지털 증거 분석 결과
       - 최종적으로 문서로 만드는 과정을 거쳐 법정으로 제출되어야 함

|  |  |
| --- | --- |
| 데이터 복구 | 데이터 분석 |
| 단순한 기술적 처리에 대한 결과물만 전달 | 디지털 증거를 분석해 문서로 만들어 법정 제출 |

1. 디지털 포렌식과 고고학

|  |  |
| --- | --- |
| 디지털 포렌식 | 고고학(Archaeology) |
| 디지털 디바이스에서 데이터 복원 | 유적지에서 토기 비롯해 각종 유물 발굴 |
| 삭제된 데이터를 복원해 범죄가 발생한  시점의 상황을 재구성 | 발굴 작업 통해 과거 생활방식 알아냄 |

1. 디지털 포렌식과 데이터 복구

|  |  |
| --- | --- |
| 디지털 포렌식 | 데이터 복구 |
| 사건 또는 사고와 관련된 혐의자가 숨기거나 삭제한 정보를 복구 | 고의적 또는 실수 간에 사용자가 어떤 사고로 인해 삭제하거나 훼손된 정보를 단순히 복구만 하는 것 |
| 복구 대상 정보는 이미 특정되거나 특정되지 않는 경우가 대부분 | 복구해야 할 대상 정보는 이미 그것을 수행하기 이전에 특정됨 |
| 복구된 데이터는 반드시 법정에서 유효한 증거로 사용할 수 있도록 ‘절차의 완전성’  강조 | 단순 데이터 복구 |

1. 디지털 포렌식과 전통적 과학수사 , 디지털 포렌식과 정보보안과 각 유사해 보이지만 차이점 존재
2. 디지털 포렌식 종류

* 주로 디지털 디바이스에 맞춰 ‘(디지털 디바이스 이름) 포렌식’ 이라고 명함

1. 컴퓨터 포렌식 (computer Forensics)
   * + 컴퓨터, 노트북 , USB 메모리, CD/DVD, 외장 하드 드라이브 등
     + 2000년대 중반 : 현장에서 컴퓨터 자체를 획득하거나 하드디스크 드라이브만 분리해 획득해 수사기관의 분석실로 운반해 증거분석을 한 후 보고서를 제출하거나 원본을 반환하는 일련의 절차 거침
     + 2010년대 : 형사소송법 개정(2011.07.18)을 정점으로 디지털 증거의 포괄적인 획득에 대한 규제 시작, 법원이 압수수색영장에 디지털 증거의 압수 방법을 제한하는 별지 문서를 추가해 발부하는 관행이 정착되는 계기가 됨, 이후 ‘검사와 사법경찰관의 상호 협력과 일반적 수사 준칙에 관한 규정(이하 수사 준칙)’에서 명문화 되어 선별 압수 위주의 새로운 수사 기법이 완전히 정착하게 됨
     + 컴퓨터, 컴퓨터 시스템과 연결된 저장매체도 모두 포괄해 통합 포렌식이란 분야 만들어내고 있음
2. 모바일 포렌식 (mobile Forensics)
   * + 모바일 디바이스 대상으로 하는 포렌식, 스마트폰, 피처폰, 안드로이드, iOS기반 태블릿 컴퓨터 등
     + 분석을 위해 데이터 추출하기 전 모바일 디바이스의 칩을 제거 또는 Bootloader를 설치 요구
     + 모바일 디바이스에 대해 디바이스 자체의 설정을 바꾸지 않는다면 데이터에 대한 획득 자체가 불가능한 경우도 많음
     + 전통적인 포렌식의 제1원칙인 ‘원본에 대한 쓰기 방지’ 적용이 어려움, 모바일 포렌식은 동적인 시스템인 모바일 디바이스를 대상으로 해 디지털 증거를 추출하고 분석하는데 많은 어려움이 따름
3. 데이터베이스 포렌식 (Database Forensics)
   * + 기업의 대형 전산 시스템에서 사건/사고와 관련된 데이터를 식별하고 추출해 무결하게 획득
     + 공용 시스템이라 할 수 있는 기업 전산 시스템을 구성하는 그룹웨어(Groupware), ERP(Enterprise Resource Planning) 시스템, 데이터베이스 시스템, 이메일 시스템 등 대상
     + 기업 활동의 연속성을 유지할 수 있도록 보장하기 위해, 조사 대상 기업의 시스템 관리자를 통한 간접적인 방식의 데이터 획득을 선호
     + 조사 대상자나 제3자와의 원만한 의사소통 능력은 증거분석에 필요한 데이터를 빠르게 확보할 수 있는 중요한 역량 가운데 하나
     + 분석과정 : 데이터 검색과 선별작업, 추출과정
     + 점차 클라우드 포렌식 (Cloud Forensics)쪽으로 영역 넓어지고 있음
4. 파일시스템 포렌식 (File system Forensics)
5. 윈도우 포렌식 (Windows Forensics)
6. 맥 포렌식 (Mac OS Forensics)
7. 인터넷 포렌식 (Internet Forensics)
8. 악성코드 포렌식 (Malware Forensics)
9. 가나