SeoulTech

제5장 디지털 포렌식 수행 절차

박 종 혁 교수

UCS Lab

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

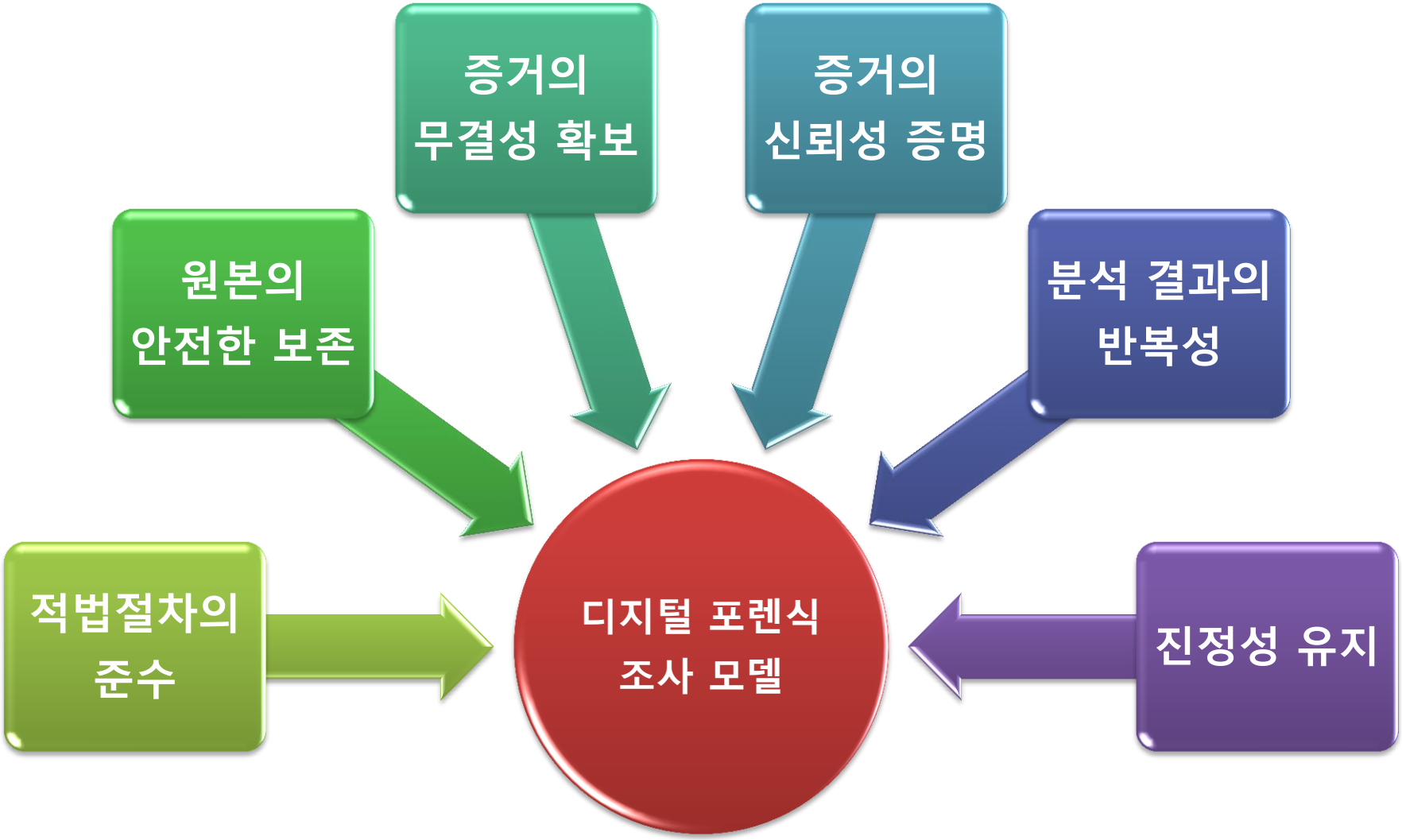
개요

- 학습목표
  - 디지털 포렌식 조사 모델을 통해 디지털 포렌식 수행 절차를 알아보고 수행시 유의 사항과 디지털 데이터가 법적인 증거로 사용되기까지의 과정을 학습한다.

- 학습 내용
  - 디지털 포렌식 수행시 유의 사항
  - 디지털 포렌식 조사 모델의 조사 준비
  - 디지털 포렌식 조사 모델의 현장대응
  - 디지털 포렌식 조사 모델의 증거 확보 및 수집
  - 디지털 포렌식 조사 모델의 증거 운반 및 확인
  - 디지털 포렌식 조사 모델의 조사 및 분석
  - 디지털 포렌식 조사 모델의 보고 및 증언

목 차

포렌식 조사 모델 수행 시 유의 사항



조사 모델 수행 시 유의 사항

- 적법 절차의 준수
  - 피조사자 개인의 인권을 보장해야 하고, 피조사 기관은 기업의 영업 비밀이나 중요 자료의 노출이 발생하지 않도록 적법 절차를 준수
  - 특히 디지털 포렌식 조사의 대상이 되는 저장 매체는 개인의 사생활과 관련된 많은 정보가 저장
  - 따라서 조사자가 이를 열람할 수 있는 권한을 확보하지 않은 상태에서 조사할 경우 추후 문제가 발생
  - **준수 방안**
    - 수사 기관인 경우, 압수・수색 권한 혹은 영장이 한정하는 영역 내에서만 조사를 진행
    - 민간 기관인 경우, 조사를 수행할 때 발생할 수 있는 책임 여부를 사전에 상호 확인하고, 의뢰인이 위임한 부분에 대해서만 조사를 수행

조사 모델 수행 시 유의 사항

- 원본의 안전한 보존
  - 디지털 데이터는 쉽게 훼손될 수 있기 때문에 데이터를 안전하게 보존할 수 있는 수단을 강구해야 함
  - 특히 물리적인 충격이나 전자기파에 의해 손상을 입지 않도록 포장에 주의
  - 증거 분석은 원본의 손상을 막기 위해 반드시 사본에서 수행
  - 또한 생성한 사본이 원본과 동일하다는 것을 증명할 수 있는 절차적, 기술적 절차가 수반

- 증거의 무결성 확보
  - 디지털 데이터는 완벽히 조작할 수 있기 때문에 데이터 확보 이후에는 어떠한 변경도 없었다는 것을 입증하기 위한 기술적, 절차적 수단을 확보해야 함
  - 법정에서 무결성을 증명할 수 있는 방법을 준비

조사 모델 수행 시 유의 사항

- 증거의 신뢰성 증명
  - 증거 분석은 과학적인 방법을 사용해야 하고, 해당 분야 전문가들에 의해 충분히 검토되어 신뢰할 수 있는 기술적 절차로 수행되어야 함
  - 도출된 결과는 신뢰성을 검증할 수 있어야 함

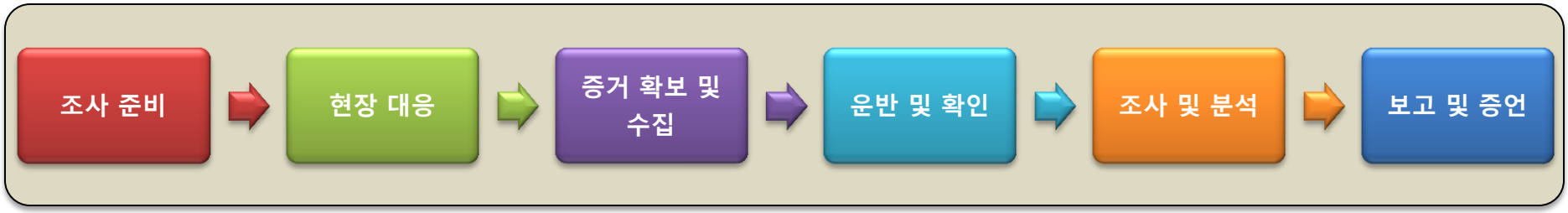
- 분석 결과의 반복성
  - 도출된 분석 결과는 동일한 실험 조건이 주어진다면, 오차 범위 내에서 항상 동일한 결과가 나올 수 있도록 재현할 수 있어야 함

- 진정성 유지를 위한 모든 과정의 기록
  - 디지털 증거 수집·분석을 비롯한 모든 과정을 기록함으로써 사후 검증할 수 있는 수단을 제공
  - 디지털 증거의 진정성은 수집 이후부터 법정까지 진행된 증거 처리에 관한 내용을 기록한 문서를 통해 입증

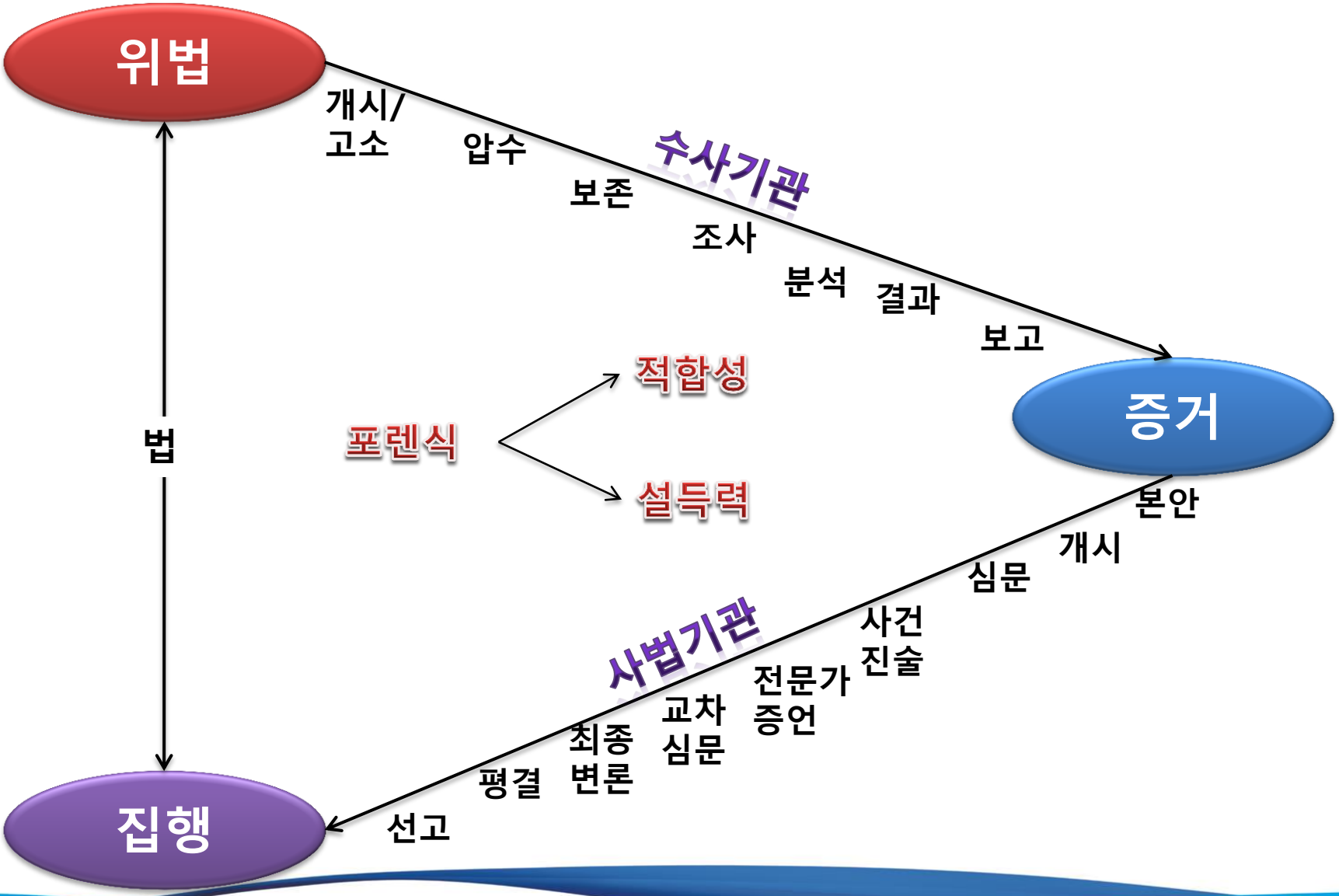
디지털 포렌식 조사 모델의 정의

- 디지털 포렌식 조사 모델의 정의
  - 디지털 정보를 포함하고 있는 매체를 증거로서 확보하여, 디지털 증거의 법적 가치가 훼손되지 않도록 수집 • 보관 • 이송 • 분석 • 보고하는 일련의 수행 절차
  - 이러한 과정은 분석된 결과가 법적인 증거로 허용될 수 있도록 법적 절차를 준수해야 하며, 신뢰성 있는 결과의 산출, 분석 결과의 정확성, 오류 발생의 최소화 등에 기초해야 함

•디지털 포렌식 조사 모델



일반적인 사법 처리 과정


위법
개시/
고소
압수
보존
수사기관
조사
분석
결과
보고
증거
적합성
포렌식
설득력
법
본안
개시
심문
사건
진술
사법기관
전문가
증언
교차
심문
최종
변론
평결
선고
집행

디지털 포렌식 조사 모델


조사 준비
•사건 발생 및 확인
•조사 권한 획득 준비
•조사 팀 구성
•장비/도구 준비
현장 대응
•현장 통제와 보존
•접근 권한과 협조 획득
•조사 대상 매체의 확보
증거 확보 및 수집
•시스템 확보
•저장 매체 확보(하드디스크 등)
•증거물 포장과 봉인
운반 및 확인
•증거물 운반
•증거물 등록 및 확인
•원본 보관
조사 및 분석
•사본 생성
•데이터 추출
•데이터 분류
•상세 분석
보고 및 증언
•분석 보고서 작성
•증거 관련 문서 보관
•법정 증언

조사 준비 – Overview

- 조사 준비 단계
  - 위법 행위, IT 보안 시스템의 경보 등과 같이 사건이 발생하면, 본격적인 수사에 앞서 필요한 준비 과정을 수행하는 단계
  - 신뢰할 수 있는 디지털 증거를 확보하기 위해서는 조사 준비 과정에서 세밀한 준비가 절실히 요구됨
  - 현장 출동 시, 필요한 장비를 준비하지 못하거나, 인원이 부족하는 등의 문제가 발생하면 원활한 조사 진행이 불가능함
  - 오랜 조사 경험이나 전문지식이 있는 책임자의 지휘 아래 철저한 조사 준비를 해야 함

- 조사 준비 과정의 세부 절차
  - 사건 발생 및 확인
  - 조사 권한 획득
  - 인원 구성
  - 장비・도구 준비 단계

- 사건 발생 및 확인
  - 사건이 발생 시, 이에 대한 조사를 수행할 필요성이 있는 지에 확인 필요
  - 일반 범죄 수사의 경우
    - 최근 컴퓨터 및 디지털 기기의 사용이 일반화됨에 따라 일반적인 민사·형사 사건의 경우에도 범죄 현장의 디지털 포렌식 조사를 수행
    - 피해자의 신고를 통한 사건 발생, 내부 조사를 통해 위법 행위 등이 발견되면 본격적인 조사가 시작
  - 사이버 범죄 조사의 경우
    - 비정상적 경고의 발생
      - 침입 탐지 시스템의 경고 발생, 네트워크 방화벽 로그의 비정상적인 징후, 기타 보안 장비의 경고 신호 등
      - 네트워크 트래픽이 급증하였다면, 발생한 경보가 단순히 비정상적으로 방문자가 급증한 것이 원인인지, 내부 네트워크에서 실수로 패킷을 과다 발생시킨 것인지, DDos 공격에 의한 것인지 확인이 필요
    - 이러한 확인 과정은 특정 사건에 대한 조사를 진행할 것인지를 결정하는 첫 번째 단계이므로 신뢰성 있는 분석과 확실한 판단이 필요

- 주요 조사 대상의 선정 (조사 대상의 가치 평가)
  - 확인 과정은 나아가 주요 조사 대상이 무엇인지를 결정하고 전반적인 수사 계획을 설정하는 과정을 포함
  - 현대의 디지털 포렌식 수사는 엄청난 양의 데이터를 조사해야 하므로, 수많은 잠재적인 증거 자료로부터 사건 해결에 실마리를 제공해 줄 수 있고 중요한 결과를 얻을 수 있는 자료를 우선적으로 수집・분석할 수 있도록 선정하는 과정이 필요

- 사전 조사
  - 조사 대상을 선정하기 위해서는 피조사 기관의 전산 환경, 접근 대상 시스템의 유형, 규모, 운영체제, 네트워크 구성 등을 파악하여 증거 수집이 가능한 지를 판별
  - 특히 자체 보안 솔루션 등으로 외부 저장장치를 통한 데이터 접근이 제한되는지, DRM 시스템과 같이 접근 제어형 보안 소프트웨어가 사용되고 있는 지 확인이 필요

- 권한 획득의 필요성
  - 조사에 필요한 자료이지만 별도의 접근 권한이 필요한 경우는 그에 적합한 권한 확보 과정이 선행되어야 함
  - 수사 기관의 경우, 영장 신청 과정에서 조사가 필요한 대상과 권한 등의 내용을 상세히 기재해서 법적인 문제가 발생하지 않도록 주의
  - 차후 조사하는 과정에서, 사건과 관련 없는 정보를 열람할 경우가 분쟁이 발생할 수 있으므로 이에 대한 접근 권한을 명확히 설정해야 함

구분	확인 사항	설명
권한의 유무	• 당사자의 동의 • 권한 있는 자의 승인	당사자의 동의를 얻지 않을 경우, 영장을 발부 받아 조사 권한을 획득해야 함
영장 등 기재내용	• 사건 개요 • 압수 수색 장소 • 압수 대상 • 압수 범위	영장의 내용에서 기재된 범위를 확인해야 하며, 특히 압수수색의 주요 대상 증거물(특정 파일, 사진, 회계데이터 등) 이 무엇인지 확인해야 함
증거 수집 대상의 관련 정보	• 정보처리 시스템의 유형 • 규모 • 운영체제 • 네트워크 구성 등	DRM과 같이 자체 보안 등으로 외장저장장치를 통한 데이터 저장 제한, 특이한 컴퓨터 소프트웨어 사용 등을 확인해야 함

- 인원 구성
  - 사건의 유형, 조사자의 전문성, 압수 대상 장소의 수 등을 고려하여 조사팀의 인원을 구성
  - 추가적으로 현장 출동 후 수색 절차, 증거 수집 방법과 범위, 각 조사자의 역할 등을 분담

- 사전 교육
  - 조사 책임자는 현장 조사에 참여할 인원들에게 담당할 업무와 유의사항에 대한 사전 교육을 실시
  - 각 압수 장소에 대한 인원 배분, 시스템의 예상 수량과 장비의 배분, 또한 조사자의 전문성을 고려하여 적절한 배분과 역할을 분담

- 공증 인원 추가
  - 전체 현장 조사 과정을 검증할 자격이 있는 제3의 입회인을 참석시켜 증거 획득・포장・봉인・이송 과정을 확인하도록 할 수 있음
  - 이는 현장 대응 과정이 공정하고 무결하다는 것을 보여줄 수 있는 효과적인 증명 방법

- 증거 수집 장비
  - 소프트웨어 장비
    - 이미지 작성용 프로그램, 데이터 수집 프로그램, 현장 초동 분석용 프로그램 등이 포함
  - 하드웨어 장비
    - 현장에서 분석할 경우를 대비하기 위한 휴대용 컴퓨터(분석 소프트웨어 포함)
    - 하드디스크 이미징 장치, 쓰기 방지 장치, 대용량 저장 매체, 광학디스크 매체
    - 다양한 규격의 연결 케이블 및 어댑터, 시스템 분해와 해체를 위한 공구 일체
  - 기타 장비
    - 현장 촬영을 위한 카메라 및 녹화를 위한 캠코더 등이 포함
    - 서류 작성을 위한 각종 서식과 휴대용 프린터 등을 확보

- 증거 봉인 및 포장 장비
  - 충격 완화용 보호 박스 (증거 운반용 박스), 증거를 포장할 각종 봉투와 충격흡수 소재, 밀봉된 증거물의 무결성을 증명할 특수테이프 (Evidence Tape)와 봉인지 (Seal), 압수물 라벨, 정전기 차단 봉투, CD 케이스 등

- 운반 장비
  - 증거 운반용 전문 케이스나 운반 차량이 포함

- 포렌식 하드웨어

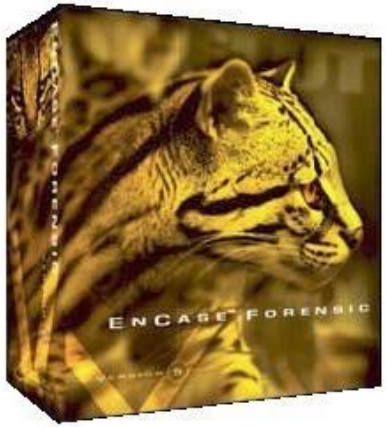








- 포렌식 소프트웨어

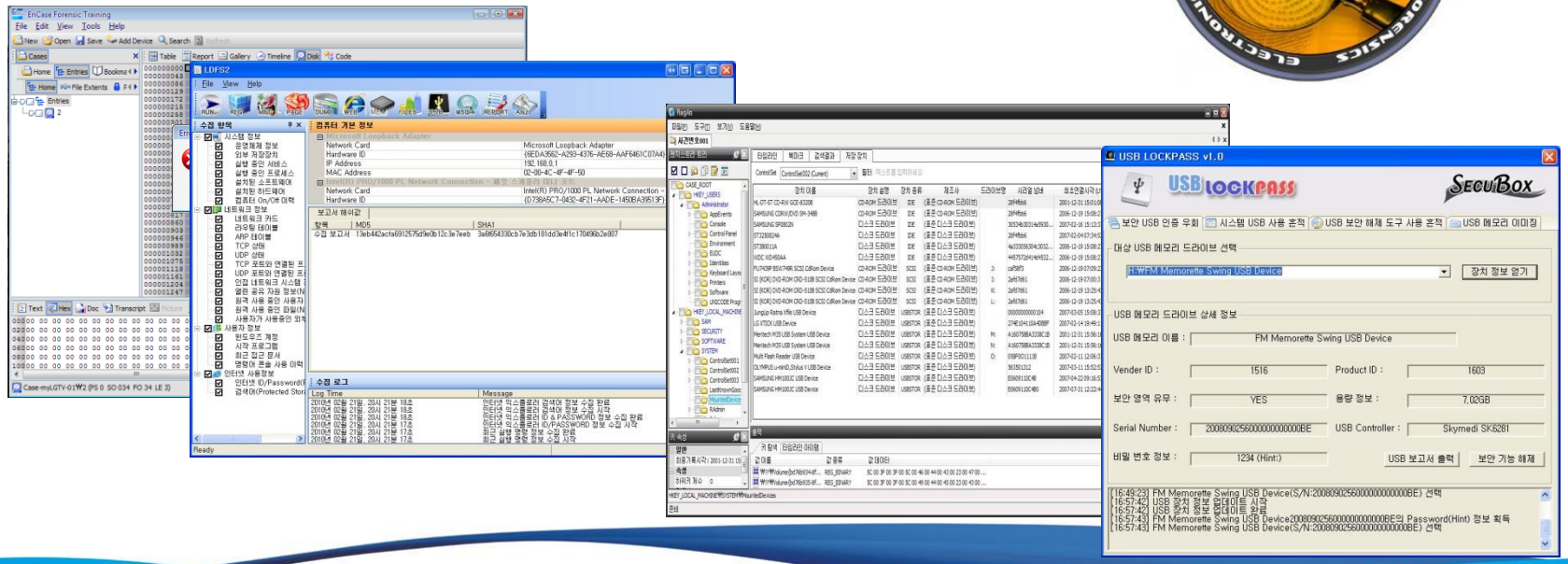

ENCASE FORENSIC


Final Forensics


Find, Organize, & Analyze Computer Evidence
ACCESSDATA
FTK 2.0
FORENSIC TOOLKIT
Install Forensic Toolkit 2.0
View User Guide
Install Registry Viewer
View Release Notes
Install FTK Imager
Install Adobe Reader


paraben's
e-mail
examiner


INCIDENT RESPONSE
HELIX 3
COMPUTER FORENSICS
ELECTRONIC DISCOVERY


EnCase Forensic Training
LDFS2
USB LOCKPASS v1.0
USB LOCKPASS
SECUBOX

- 장비/도구 종류별 일람

분류	세부 장비
분해와 해체를 위한 공구세트	컴퓨터 등 분해를 위한 사이즈 별 +/- 드라이버, 케이블 절단을 위한 니퍼, 플라이어 등
디스크 복제 장치	현장에서 디스크 복제 업무를 수행할 때 사용
쓰기 방지 장치	현장에서 사본 이미지 작성, 분석 업무 등을 수행할 때 원본 디스크의 데이터 훼손을 방지하기 위해 사용
증거 사본 보관용 대용량 저장장치	현장에서 디스크 복제 또는 사본 이미지를 작성하는 경우 사용할 대용량 HDD, 다양한 유형의 HDD를 연결할 수 있는 인터페이스 장비, 휴대용 RAID 저장 장치 등
외장형 저장 매체	데이터 검색 • 수집을 위한 USB 메모리 또는 휴대용 디스크, CD-R, DVD-R 등
분석용 소프트웨어	휘발성 데이터 수집 프로그램, 이미지 작성 프로그램, 해쉬 프로그램, 압축 프로그램, 기타 분석에 필요한 프로그램
다양한 규격의 연결 케이블 및 어댑터	멀티 플러그, 전원 케이블과 어댑터, 네트워크 케이블, 각종 데이터 전송 케이블과 어댑터 등
증거 포장 운반용 세트	충격 완화용 보호 박스, 정전기 차단용 백, 전차파 차폐용 팩, 운반용 하드케이스 등
증거수집 및 분석용 모바일 컴퓨터	현장에서 증거 수집 및 초동 분석 업무 등을 수행할 때 사용
기타 장비	카메라, 캠코더, 금속 스캐너, 모바일 프린터 등

현장 대응 –Overview

- 현장 도착 시 조치 과정
  - 사건 준비과정이 완료되면 현장에 출동하여 조사에 필요한 조치를 수행하며, 향후 증거 수집 과정을 시작하기 앞서 모든 준비과정을 수행하는 단계
  - 현장을 통제하고 이를 보존하며, 관계자와의 협조를 얻어 주요 조사 대상 시스템과 매체를 확보함.
  - 또한 조사 과정의 신뢰성 확보를 위해 카메라나 캠코더로 이를 촬영하여 기록

현장 통제와 보존

- 조사를 수행하기에 앞서 최대한 현장을 보존하며, 증거 인멸 시도의 가능성을 고려하여 이를 보존하고 통제

조사 권한 획득과 협조 요청

- 사건 책임자가 용의자 또는 피조사 기관의 관리자와 면담을 통해 조사 협조를 구하고 관련 서류를 제시하여 접근 권한을 획득

조사 대상 시스템 및 저장 매체 확보

- 조사가 필요한 시스템, 물리적 증거들을 피조사자와 협조를 통해 확인
- 확보된 시스템은 사용자를 격리하여 이를 통제함
- 또한 전체적인 현장의 시스템 및 네트워크 상황을 파악해야 함

- 현장 통제와 보존의 필요성
  - 현장의 통제는 증거물을 최대한 원본 상태로 보존할 수 있고, 이를 통해 사건이 발생한 원인을 파악함으로써 본격적인 조사를 시작할 것인지를 판단할 수 있는 근거가 됨
  - 또한 증거 훼손을 막아 예기하지 못한 실수로 인해 중요한 증거 자료가 손실되지 않게 막을 수 있음

- 수사 기관의 현장 조치 요령

영장 제시
- 관리자에게 압수 수색 취지 설명
- 규정된 현장 조사 절차를 준수
- 팀 인원과 장비 배분

현장통제
- 전체 조직도, 직원 명부 활용 압수수색 대상 결정
- 현장으로부터 직원 격리
- 소지품 검사 (USB, 플래쉬 메모리) 확보

현장 분석
- 전산 관리자 신병 확보, 현장 분석에 활용
- 시스템 상황, 네트워크 상황 등 파악
- 현장의 전체적 구조를 촬영 및 스케치

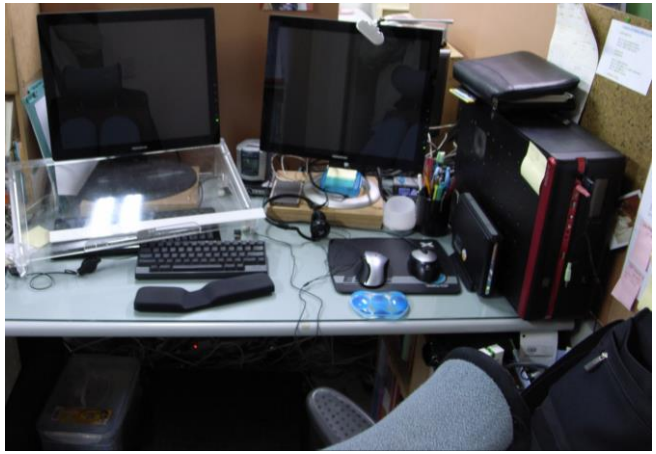
시스템 등 통제
- 시스템 on/off 유지
- 네트워크 연결 차단 등 조치
- 지문 채취 등 조치

- 조사 권한 획득
  - 수사 기관은 영장을 제시하여 주요 대상에 대한 접근 권한을 받음
  - 민간 기관은 의뢰기관이 허가한 시스템에 대해서만 조사를 진행

- 조사 대상자 참여 유도
  - 일반 사용자
    - 조사 과정에 직접 참관하고, 조사 과정을 공개적으로 설명하여 참여 유도
    - 수집된 증거물에 대한 확인, 서명을 받음으로써 수집 과정과 증거물의 객관성, 신뢰성, 증거물 출처와 데이터의 동일성을 주장할 수 있도록 함
  - 시스템 관리자 (기업 등 대규모 조사)
    - 현장 상황을 가장 잘 알고 있는 대상자의 협조를 통해 압수 수색의 효율성을 재고

- 다양한 시스템 및 저장 매체를 조사
  - 이동식 저장 매체 조사 (USB 드라이브, 플래쉬 메모리 등)
    - 최근 대용량・소형 저장 매체가 대중화되어 있으므로 이를 철저히 조사
  - 백업, 교체, 은닉 시스템이나 저장매체 수색 철저
    - 조사 과정에서 하드디스크 교체 흔적 등이 있는 경우 숨겨진 하드디스크나 백업용 저장 매체를 찾아야 함
    - 백업, 스토리지, 데이터베이스 서버 등 유용한 자료가 저장되어 있는 시스템을 은닉할 수 있으므로 시스템 구성을 파악하여 은닉 여부를 탐지
  - 재래식 증거물 수집
    - 다이어리 노트, 일지, 포스트-잇 메모지, 컴퓨터 출력물 등에서 비밀번호 등 함께 수집

- 조사 과정의 사진 촬영(녹화)을 통환 신뢰성 확보



- 디지털 포렌식에서 다양한 컴퓨터 확보
  - 대부분의 조사 대상은 데스크탑 컴퓨터와 다수의 사용자가 접속해서 사용하는 서버 컴퓨터로 구분
  - 두 종류의 컴퓨터 모두 다수의 하드디스크가 내장될 수 있으며, 주로 하드디스크가 압수 수색에서 가장 중요한 대상

- 컴퓨터 조사 시 유의 사항
  - 일반적으로 컴퓨터 본체를 압수하거나 하드디스크를 분리하여 디스크만 압수
  - 레이드(Raid) 시스템을 운영하는 환경의 컴퓨터 또는 서버 시스템의 경우, 환경이 특수하므로 전체를 압수하지 못하고 사건에 연관된 일부 데이터만을 확보
  - 하드디스크를 분리할 때, 보안 시스템 또는 자동으로 파괴하는 특수한 컴퓨터도 고려해야 하기 때문에 가능한 컴퓨터 그 자체를 압수하는 것이 바람직
  - 컴퓨터와 이동식 저장 매체는 각각 다른 증거물로 관리되기 때문에 ODD 내부에 CD나 DVD가 들어있을 수 있으므로 이를 주의해야 함

- 휴대폰
  - 휴대폰은 대부분의 사용 기록이 내부에 탑재된 플래시 메모리에 저장
  - 따라서 휴대폰을 조사할 때에는 기기 자체를 확보해야 하며, SIM 혹은 USIM 메모리 카드를 장착하고 있으므로 기기와 메모리 카드 각각을 분류해서 수집
  - 휴대폰은 전화 수신이 가능하므로 반드시 전자파를 차단해서 현재 상태를 보존

- 개인 휴대용 정보 단말기 (PDA, Smart Phone)
  - PDA는 내부 저장 장치로 플래시 메모리를 장착하고 있는 작은 컴퓨터
  - 또한 내장된 플래시 메모리 외에 소형 메모리 카드를 삽입해서 사용할 수 있으므로 이를 확인 후 각각을 압수
  - 스마트 폰의 경우에는 휴대폰과 같은 속성을 가지기 때문에 반드시 전자파를 차단함




휴대폰과 PDA



전파 차단 봉투와 차단 장치

- 디지털 캠코더 및 카메라
  - 영상 및 사진 정보를 담는 기기로서 포렌식 수사 관점에서 볼 때 컴퓨터의 하드디스크만큼이나 중요한 증거 대상임
  - 대부분 내부적으로 소형의 플래시 메모리를 장착하고 있으며, 실제 영상이나 사진 데이터는 메모리 카드를 통해 저장하므로 기기 안에 삽입되어 있는 메모리 카드는 반드시 분리하여 따로 확보

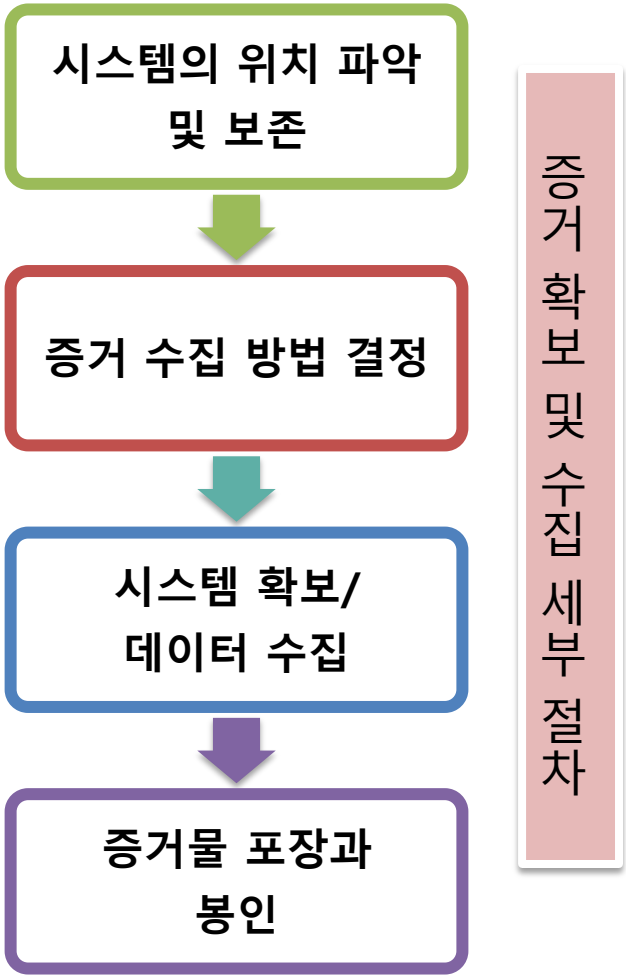
- 임베디드 시스템
  - 최근 MP3, PMP, 휴대용 게임기, 네비게이션, 비디오 게임기 등 다양한 디지털 기기에 대한 사용이 증가하고 있음
  - 이러한 기기들은 내부/외부에 플래시 메모리나 하드디스크 같은 저장 매체를 이용하므로 포렌식 조사의 대상으로 인식하고, 데이터를 수집할 수 있도록 이를 확보해야 함

- 컴퓨터에서 주로 사용하는 저장 매체의 종류
  - 플로피 디스크
  - 하드 디스크
  - 플래시메모리 기반 저장 매체 (USB 메모리, 메모리카드, SSD)
  - 광학 매체: CD-ROM, DVD-ROM, Blu-Ray, HD-DVD 등이 존재

- 디지털 포렌식 관점에서 저장 매체
  - 범죄 현장의 조사자는 다양한 디지털 저장 매체를 파악하고 이를 현장에서 확보할 수 있도록 배경 지식을 갖추어야 함
  - 대부분의 저장 매체는 메인보드에 직접 연결되어 사용되거나 USB 등과 같은 외부 연결 인터페이스를 사용
  - 이러한 연결 정보가 시스템에 저장되므로 사용자가 은닉한 매체가 있는지 확인하고 확보해야 함

증거 확보 및 수집–Overview

- 증거 확보 및 수집을 위한 준비
  - 조사 대상자의 증거물을 확보(압수)한 뒤 어떤 종류의 데이터를 어떤 방법으로 수집할 것인지를 결정
  - 수사 기관은 영장의 기재 내용에 의거하여 필요한 증거물을 압수하는 과정
  - 포렌식 서비스 업체는 현장에서 데이터를 수집 및 분석할 것인지, 시스템이나 중요 자료에 대해 사본을 생성하여 이를 확보할 것인지 등 협의



시스템 확보

•하드디스크에 저장된 데이터 및 시스템 전체에 대한 정밀분석이 요구될 때 실시

• 부득이한 경우 컴퓨터 본체를 비롯한 모니터, 프린터, 케이블 등 주변 장치도 확보

원본 하드디스크 확보

•하드디스크에 저장된 데이터의 복구 및 분석이 필요하고 원본의 필요성이 중요하여 확보할 필요가 있는 경우

사본 하드디스크 확보

•하드디스크에 저장된 데이터를 복구하고 분석할 필요가 있지만 굳이 원본을 확보할 필요가 없는 경우

선별 데이터 수집

•위 세 가지 방법에 의한 압수가 불가능하거나 영장의 허용 범위가 특정 데이터에만 국한된 경우

사진 촬영	• 사용자를 파악할 수 있도록 표시하고 모니터의 현재 화면, 시스템의 앞뒷면과 주변 장치 등을 촬영 • 필요한 경우 대상물의 위치와 상태를 스케치하여 기록
이동형 저장 매체 조사	• 플로피 드라이브와 CD・DVD 등을 확인하여 삽입된 것이 있으면 이를 제거하고 필요한 경우는 별도 압수물로 처리
컴퓨터 전원 상태 확인	• 비활성 시스템의 경우는 전원이 꺼진 상태 그대로 확보 • 전원이 켜져 있는 경우를 활성 시스템의 경우, 전원을 차단하기 전에 휘발성 데이터의 수집 필요성을 판단한 후 결정
휘발성 데이터 수집	• 시스템의 현재 상태가 중요한 경우는 휘발성 데이터를 수집 • 휘발성 데이터는 현재 실행 중인 프로세스 정보, 네트워크 연결 정보 등 다양한 정보를 포함하며 최근에는 필수적으로 수집함
시스템 종료 (전원 차단)	• Windows 제품 군을 사용하는 데스크탑 시스템은 정상 종료 과정에서 다양한 데이터를 삭제하거나 정리하여 데이터가 삭제될 수 있음 • 전원이 켜진 상태에서 전원공급장치에 연결된 전원 코드를 분리

- 활성 시스템 조사

활성 시스템 (Live System)

- 현장에서 조사관이 접근할 수 있는 전원이 켜져 운영 중인 시스템
- **휘발성 데이터**: 시스템의 RAM에 저장되어 있어 전원을 내리면 수집할 수 없는 데이터
- "사건 현장에서 촬영한 즉석 사진" 과 같이 당시 **시스템의 동작 상태를 그대로 나타내는 시스템 사용 정보**

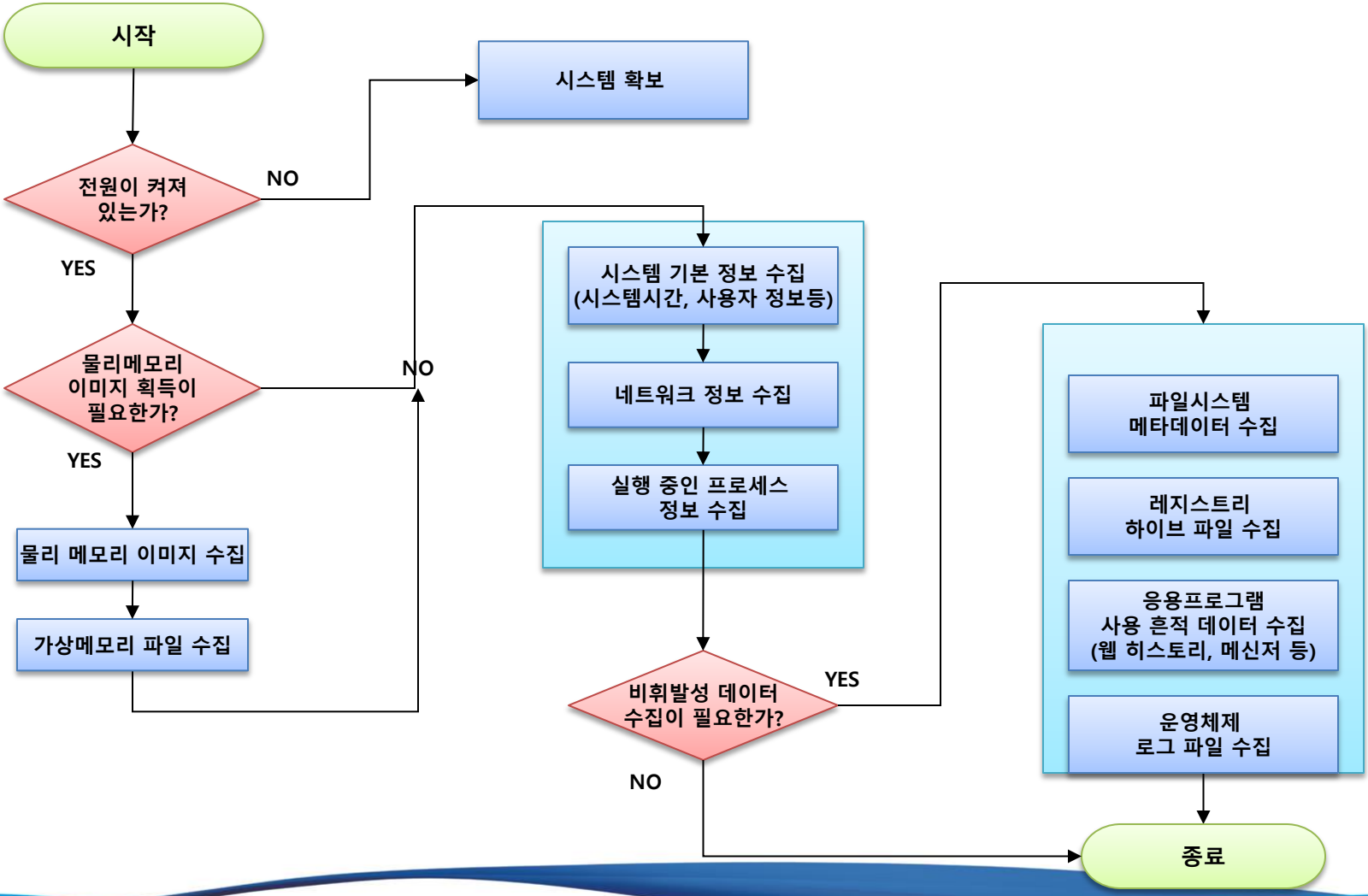
활성 시스템 포렌식 조사

- 디스크 이미지 조사 기반의 일반적 디지털 포렌식 과정과는 다르게 시스템이 켜져 있는 상태에서 데이터를 선별 수집 및 조사를 진행함
- 시스템의 전원을 내리면 수집할 수 없는 휘발성 데이터(Volatile Data)와 신속한 조사에 필요한 비휘발성 데이터를 선별해서 수집

• 휘발성 데이터의 종류

시스템 정보	네트워크 정보	프로세스 세부 정보
• 시스템 시간 • 열려 있는 파일 정보 • 현재 실행 중인 프로세스 리스트 • 현재 실행 중인 서비스 리스트 • 현재 로그인한 사용자 계정 • 클립보드 내용 • 명령어 콘솔 사용 정보	• 네트워크 카드 정보 • 라우팅 테이블 • ARP 테이블 • TCP 연결 상태 • UDP 연결 상태 • 열린 TCP 포트와 연결된 프로세스 정보 • 열린 UDP 포트와 연결된 프로세스 정보 • 인접 네트워크 시스템 정보 • 열린 공유 자원 정보 • 원격 사용자 정보 • 원격 접근 파일 • 사용 중인 외부 자원	• 프로세스 실행파일의 전체 경로 • 프로세스를 실행한 계정 • 부모/자식 프로세스 • 프로세스가 로드한 라이브러리 • 사용 중인 네트워크 연결 정보 (TCP/UDP) • 실행 시작 시간

- 휘발성 데이터 수집 시 조사 절차



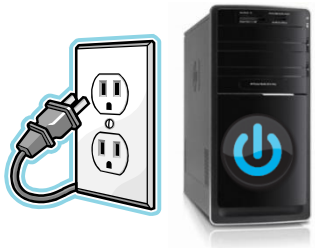
- 전원 차단 시 유의 사항
  - 전원 코드 강제 분리 종료
    - 전원이 끊김과 동시에 하드디스크에 쓰기 방지되어 하드디스크의 데이터를 동결시키는 효과를 얻을 수 있음
    - 갑작스런 전원 차단으로 시스템에 치명적인 손상이 가해질 수도 있음
    - Dos, Windows 3.1/NT/95/98/ME/2000/XP/Vista/7 Series
  - 정상적인 종료
    - 시스템이 종료되는 과정에서 운영체제가 각종 임시 파일들을 삭제하고 일부 시스템 파일을 수정하는 등 작업을 수정
    - Windows NT/2000/2003 Server, Linux/Unix, Macintosh

- 주변 기기와 케이블 분리
  - 시스템 혹은 하드디스크에 연결되어있는 주변기기와 케이블을 분리
  - 이때 시스템의 연결 포트와 케이블들을 차후에 재연결 할 수 있도록 꼬리표(라벨) 부착

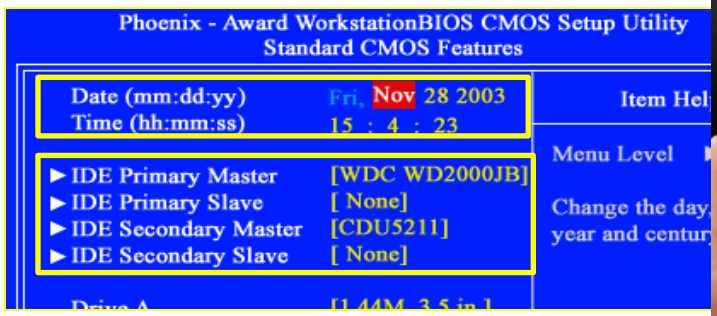
- 원본/사본 디스크 확보를 위한 준비 과정
  - 하드디스크만 확보할 경우, 시스템 시간 설정을 획득할 수 없으므로 현장에서 BIOS에 기록된 시간정보를 획득함
  - 시스템 전체를 확보하는 경우에는 조사기관의 증거 분석실에서 확인

- BIOS 시스템 시간 정보 확인 방법
  1. 시스템의 전원을 종료하고 본체를 분해
  2. 시스템에 연결된 모든 하드디스크를 분리
  3. 다시 전원을 연결하여 BIOS 셋업 화면으로 진입
  4. BIOS에 설정되어 있는 시스템 날짜와 시간 정보를 확인
  5. 증거물 라벨지에 획득한 시간 정보를 기록
     - 증거물 라벨지에 표준 시간을 동시에 기록하여 오차 확인

- 시스템 시간 정보 확인 (BIOS 설정 정보 활용)



시스템 전원 OFF



BIOS 에서시간 정보 비교
및 표준 시간과 확인

하드디스크 분해

시스템 전원 ON

부팅 시 BIOS 진입
(F2, Del 키 등)

- 사본 디스크 확보
  - 하드디스크에 저장된 데이터를 복구하고 분석할 필요가 있지만 굳이 원본을 확보할 필요가 없는 경우 수행
  - 입수된 하드디스크를 분석 시스템에 연결 하여 조사/분석 과정을 수행하면, 증거물이 손상되므로 복제(사본) 디스크를 생성

- 디스크 이미징(Disk Imaging)을 이용한 사본 생성
  - 원본 디스크를 복제(Bit by Bit Copy)하여 사본 디스크를 생성
  - 디스크 이미징 H/W 장비를 이용하여 다른 하드디스크에 이를 복제
  - 또는 디스크 이미징 S/W를 사용하여 디스크 이미지 파일을 생성
    - 디스크 이미지 파일 (Disk Image or Forensic Image)
      - 원본 디스크를 복제하여 이미지 파일을 생성하여 사본 디스크를 대신함
      - 원본 디스크와 동일함을 증명하기 위해 검증 과정이 필요 (해쉬함수로 무결성 검증)

- 디스크 이미징 장비 (Disk Imaging Hardware)
  - 단독으로 복제 디스크를 생성 가능한 포렌식 장비
  - 디스크를 컴퓨터에 연결하지 않고 다른 하드디스크에 사본을 생성
  - LogiCube Talon ,Dossier
  - ICS ImageMasster Solo 3 & 4 등

Logicube Talon

Logicube Dossier

ICS Image Masster Solo3

ICS Image Masster Solo4

- 디스크 이미징 장비를 이용한 사본 생성 절차

[조사 대상 시스템]

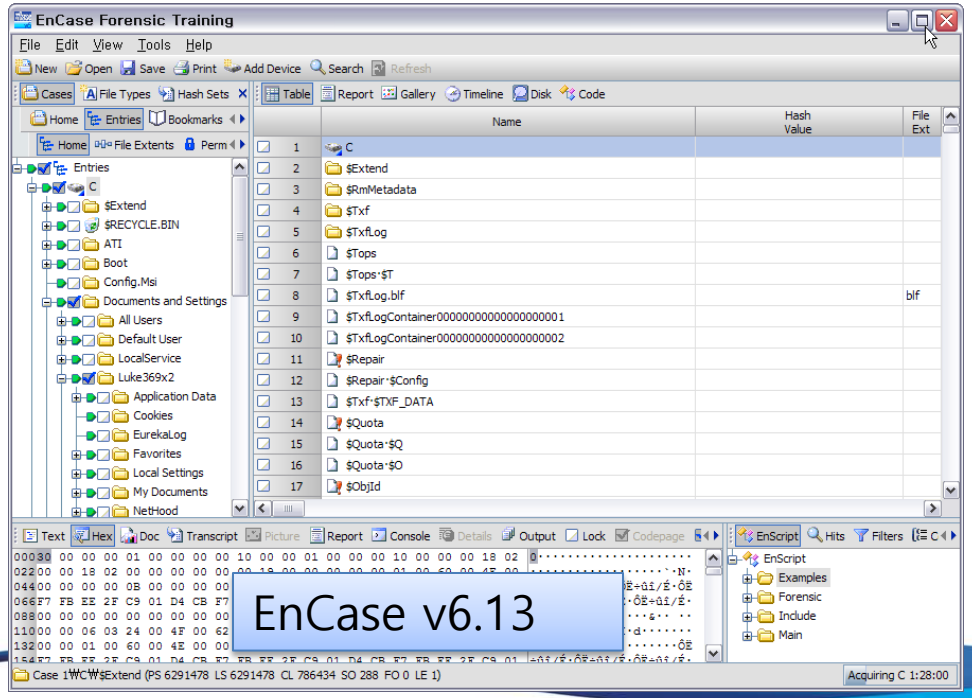
[조사 대상 시스템]
하드디스크 분해

[수집 대상 디스크]

원본 디스크에 대하여
사본 디스크를 복제
(사본 2개까지 생성)

[이미징 장치]

- 디스크 이미징 소프트웨어 (Disk Imaging Software)
  - **EnCase Forensic**
    - 디스크 이미징, 브라우징 기능 제공
    - 그래픽 인터페이스 제공
    - 증거 미리보기 및 데이터 검색/분석 기능 제공
    - 윈도우, Palm OS등의 플랫폼과 RAID 방식 지원

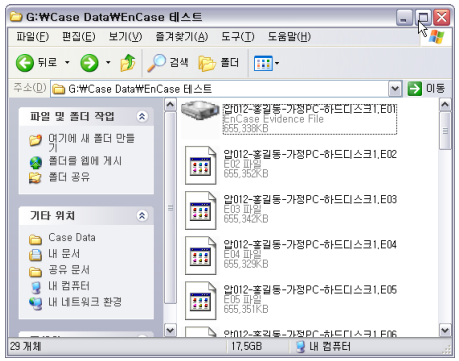


- 디스크 이미징 소프트웨어를 이용한 사본 생성 절차

[조사 대상 시스템]

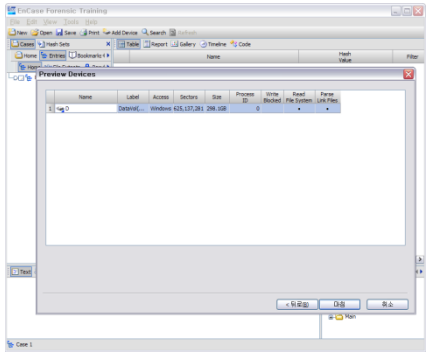
분해

[이미지 파일]



획득

[디스크 이미징 도구]



수집

[수집 대상 디스크]
쓰기 방지 장치에 연결

[쓰기방지 장치]
분석 시스템과 쓰기 방지 장치 연결

[분석 시스템]

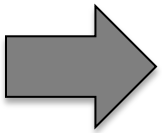
디스크 이미지의 무결성 검증

디스크 이미지

- **비트 스트림 복제(Bit Stream Clone) 방식으로 저장매체를 전체 복사해서 이미지를 생성**

해쉬 및 오류 검증 알고리즘을 저장매체와 이미지에 적용

- **해쉬 알고리즘**
  - 해쉬 : 데이터의 일부분에 알고리즘을 적용하여 고정된 크기의 유일한 디지털 지문을 생성
  - 원본 데이터를 1bit만 바꾸어도 해쉬 함수는 전혀 다른 출력 값을 생성하기 때문에 데이터 변조 여부 확인 방법으로 사용됨
- **오류 검증 알고리즘**
  - CRC(Cyclic Redundancy Check) : 전송 데이터 내에 에러가 있는지 확인하기 위한 방법 중의 하나
  - 검증 값이 불일치하면 데이터에 오류가 존재함



- **해쉬 및 오류 검증 알고리즘을 원본 Disk와 Disk image에 적용하여 보관**
- **차후 법정 증거 제출 시에 무결성 확보 여부를 주장할 수 있음**

- 증거물 포장
  - 물리적 충격이나 정전기/자기장의 영향을 받지 않도록 세심히 포장
  - 완충용 보호박스나 정전기/자기장 방지 봉투를 사용
  - 밀봉전용 특수 테이프(evidence tape)와 봉인지(seal)를 이용해 증거물 훼손을 막도록 마감 처리

- 증거물 인증
  - 증거물 라벨를 작성하여 참관인으로부터 확인을 받고 서명을 필하여 증거물에 부착
  - 증거물 라벨과는 별도로 전체 증거물에 대한 압수목록을 작성
  - 증거 확보 절차 모두가 완료되면, 획득한 증거물 목록을 완성하여 조사자로부터 확인, 서명을 받고, 사건 책임자가 서명을 함

증거물 라벨(시스템 용)					
사건번호		압수 번호			
담당부서/ 조사 책임자					
제조사/모델명					
제품번호					
압수 장소					
압수 일시	년	월	일	시	분
시스템 시간	년	월	일	시	분
시스템 사용자					
조사관	(서명)	참관인	(서명)		
피조사자	(서명)				
비 고 (특이사항)					

증거물 운반 및 확인

- 증거물 운반
  - 운반 과정의 최우선 사항은 증거물의 무결성 유지와 훼손 방지
  - 증거물의 누락 및 도난이 없도록 연계보관 원칙을 면밀히 수행하고, 철저한 확인 과정을 거쳐야 함

- 증거물 인수인계
  - 증거물 인수인계 시 반드시 증거 목록을 함께 전달하고 이를 비교하여 누락된 증거물이 없는지 확인
  - 증거물을 인수할 때는 각 증거물의 밀봉전용 특수 테이프(evidence tape)와 봉인지(seal)의 상태가 이상 없는지 확인
  - 만약 특수테이프나 봉인지가 훼손되었다면 해당 증거물은 증거물 목록에서 제외하고 기록에 남김
  - 모든 증거물의 무결성에 문제가 없다고 판단될 경우 운반 책임자는 증거물 목록에 무결한 상태로 전달했다는 서명을 함

- 분석실에 도착한 증거물 확인
  - 조사 대상자나 참관인도 운반 과정에 동행하여, 분석실에 도착 후 자신이 서명한 목록과 이상이 없는지를 확인

조사 및 분석

- 조사 및 분석 과정
  - 조사 및 분석 과정에서 처리해야 할 데이터의 양이 많고, 범죄 유형에 따라 조사해야 할 데이터가 서로 다르므로 많은 시간이 소요
  - 따라서 어떠한 방법으로 분석을 수행할 것인지 전략을 수립하여 분석할 전체 데이터를 유형에 따라 분류하고, 그 결과를 검토하여 분석을 수행

데이터 추출

- 조사가 필요한 데이터를 추출할 수 있도록 사본을 생성해서 수행
- 응용 프로그램 파일, 운영체제 사용 정보 등 분석에 유용한 데이터를 추출

데이터 분류

- 효과적인 분석과 소요 시간을 줄이기 위해 데이터를 특정 기준으로 분류
- 시간 흐름, 응용 프로그램 종류 등에 따라 데이터를 분류하고 결과 검토

상세 분석

- 분류된 데이터를 바탕으로 사건 유형에 맞게 본격적인 분석을 수행
- 인터넷 사용 흔적 분석, 사용자 활동 정보 분석, 시스템 사용 정보 분석, 응용 프로그램 사용 흔적 분석, 파일 분석 등

- 증거물 보존을 위한 사본 생성
  - 증거물 원본에 대하여 바로 분석을 수행할 경우, 무결성에 손상을 줄 수 있으므로 원본과 동일한 저장 매체나 이미징 기술로 사본 생성
  - 일반적으로 2개의 사본을 생성하며, 하나는 분석용으로 사용하고 나머지는 만일의 사태에 대비하여 보관

- 디지털 저장 매체에 대한 사본 생성
  - 하드디스크의 보존은 증거 확보 단계에서 수행한 디스크 이미징을 통하여 사본 디스크나 이미지를 생성
  - 현장에서 확보한 USB 메모리, 메모리 카드, 광학 매체와 같은 휴대용 저장 매체는 디스크 이미징 기술을 활용하여 이미지 파일을 생성하여 분석을 수행

- 데이터 추출
  - 데이터 분류를 위해서는 먼저 조사가 필요한 데이터 추출을 먼저 수행
  - 데이터 추출은 원본 증거물에 대한 무결성을 유지하면서 수행

- 데이터 추출 기법의 구분
  - **물리적 추출**: 파일 시스템과 무관하게 물리적인 매체에서 데이터를 복구하고 식별하여 데이터 추출
  - **논리적 추출**: 설치된 운영체제, 파일 시스템, 응용 프로그램에 기반하여 파일과 데이터를 복구하고 식별하여 데이터 추출

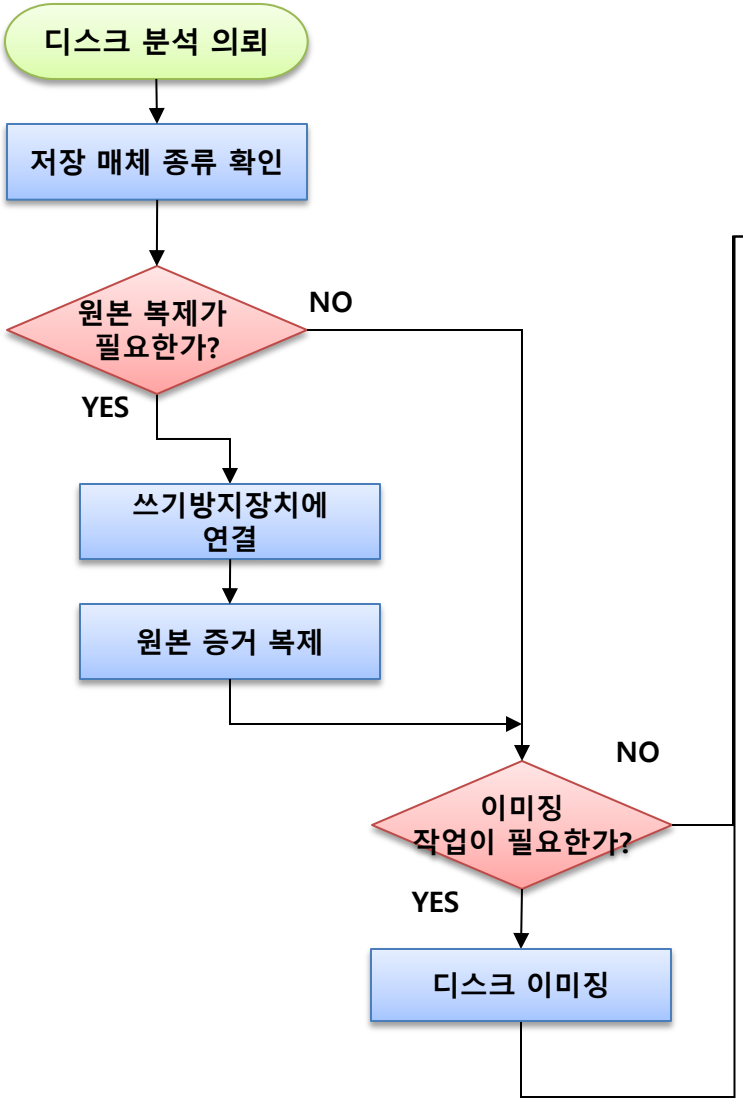
물리적 추출
- 키워드 검색
- 파일 카빙
- 파티션 테이블 추출
- 미할당 영역에서 삭제된 파일 복구
- 조각난 데이터 복구 등

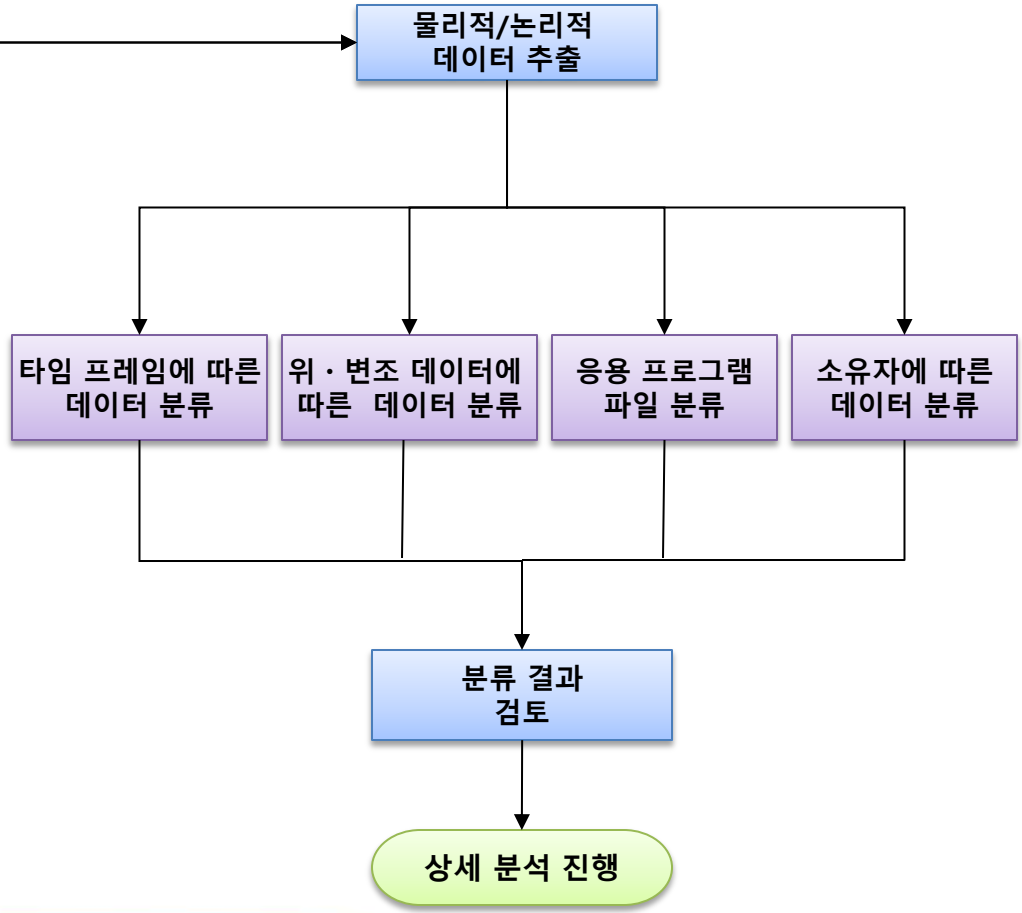
논리적 추출
- 정상 파일 추출
- 응용프로그램별 파일 추출
- 파일시스템에서 삭제된 파일 복구
- 파일 슬랙 데이터 추출 등

- 데이터 분류의 목적
  - 조사에 필요한 데이터를 선별함으로써 분석할 데이터의 양을 줄여, 효율적이고 신속한 분석을 가능하도록 함
  - 분류된 결과를 검토하여 상세 분석 단계로 진행할지 결정
  - 다양한 분류 방법이 존재하며, 분류된 결과는 서로 데이터가 중복될 수 있음

- 일반적인 데이터 분류 방법
  - 시간 정보(timeframe: 타임프레임)에 따른 분류
  - 위・변조 데이터 분류
  - 응용 프로그램 파일 별 분류
  - 소유자에 따른 분류

• 데이터 추출 및 분류 절차도



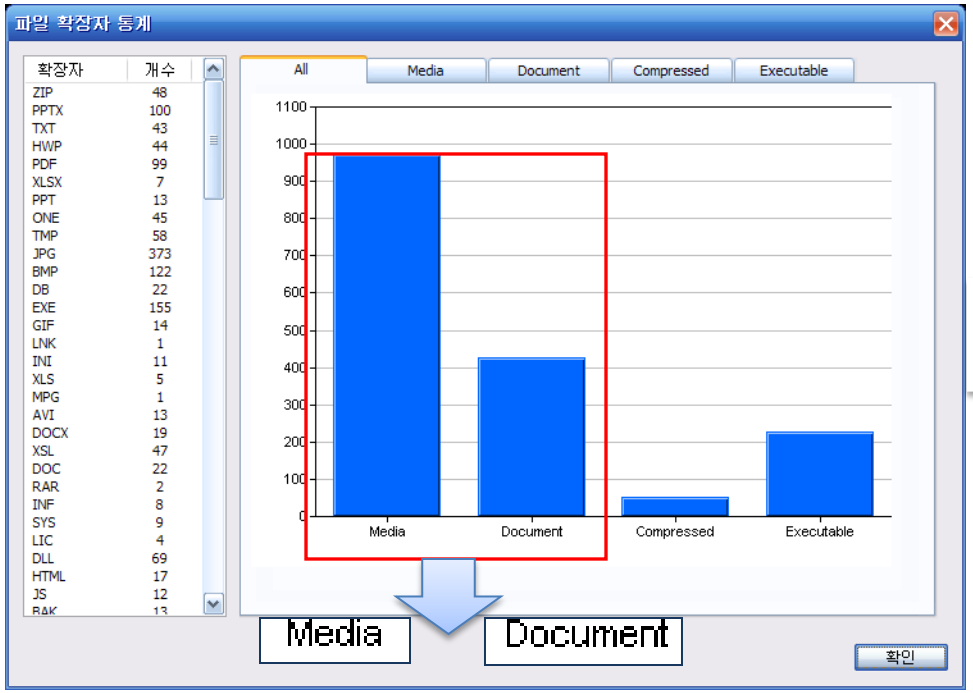


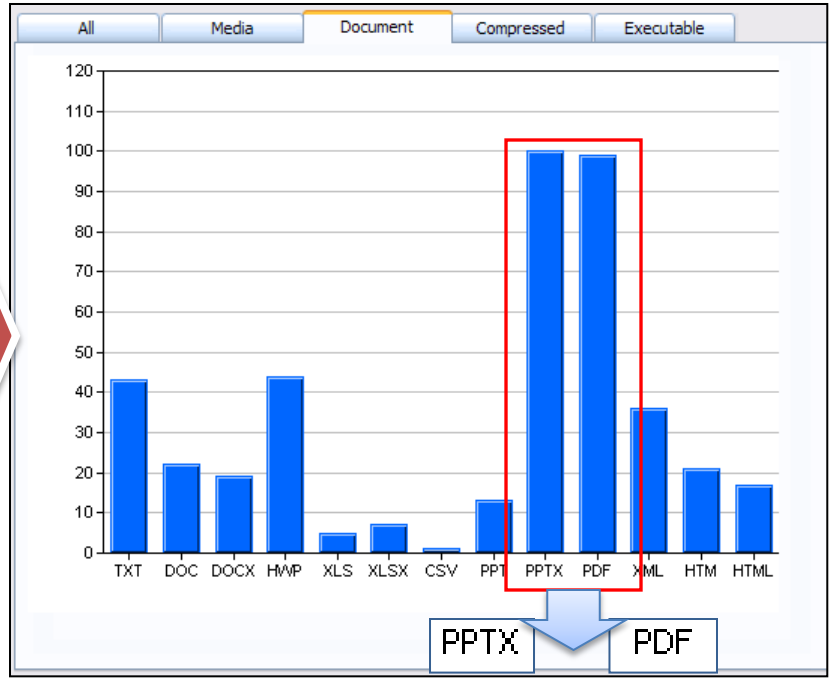
- 시간 정보에 따른 분류
  - 사건이 발생한 시점이나 주변 시간대에서 컴퓨터의 사용 흔적을 조사하여 사용자, 작업한 내용 등을 선별하여 조사하는데 유용
  - 파일 시스템의 메타정보(마지막 수정 시간, 마지막 접근 시간, 생성 시간, 변경 상태 등)와 파일 내부에 저장된 시간과 날짜 정보를 검토
  - 사건 발생 시간대에서 작업한 파일들의 리스트를 확인하고, 범죄 행위와 관련된 파일이 없는지 키워드 검색 등을 활용하여 분석

이름	File Type	만든 날짜	수정한 날짜	액세스한 날짜
Session 1-디지털포렌식 개론.pptx	Powerpoint Docume...	2010-04-01 17:30:48	2010-02-10 04:31:12	2010-04-02 01:26:04
Session 2-활성시스템 조사 방법.pptx	Powerpoint Docume...	2010-04-01 17:30:50	2010-02-10 04:26:28	2010-04-02 01:26:08
Session 3-윈도우 사용흔적 분석.pptx	Powerpoint Docume...	2010-04-01 17:30:51	2010-02-10 04:27:34	2010-04-02 01:26:22
Session 4-응용프로그램 사용 흔적 조사 방법.pptx	Powerpoint Docume...	2010-04-01 17:30:52	2010-02-10 04:28:24	2010-04-02 01:26:23

시간 역전 현상: 파일을 수정한 날짜가 만든 날짜보다 과거 시간
→ 파일을 원래 매체에서 다른 저장 매체에서 옮길 경우 주로 발생

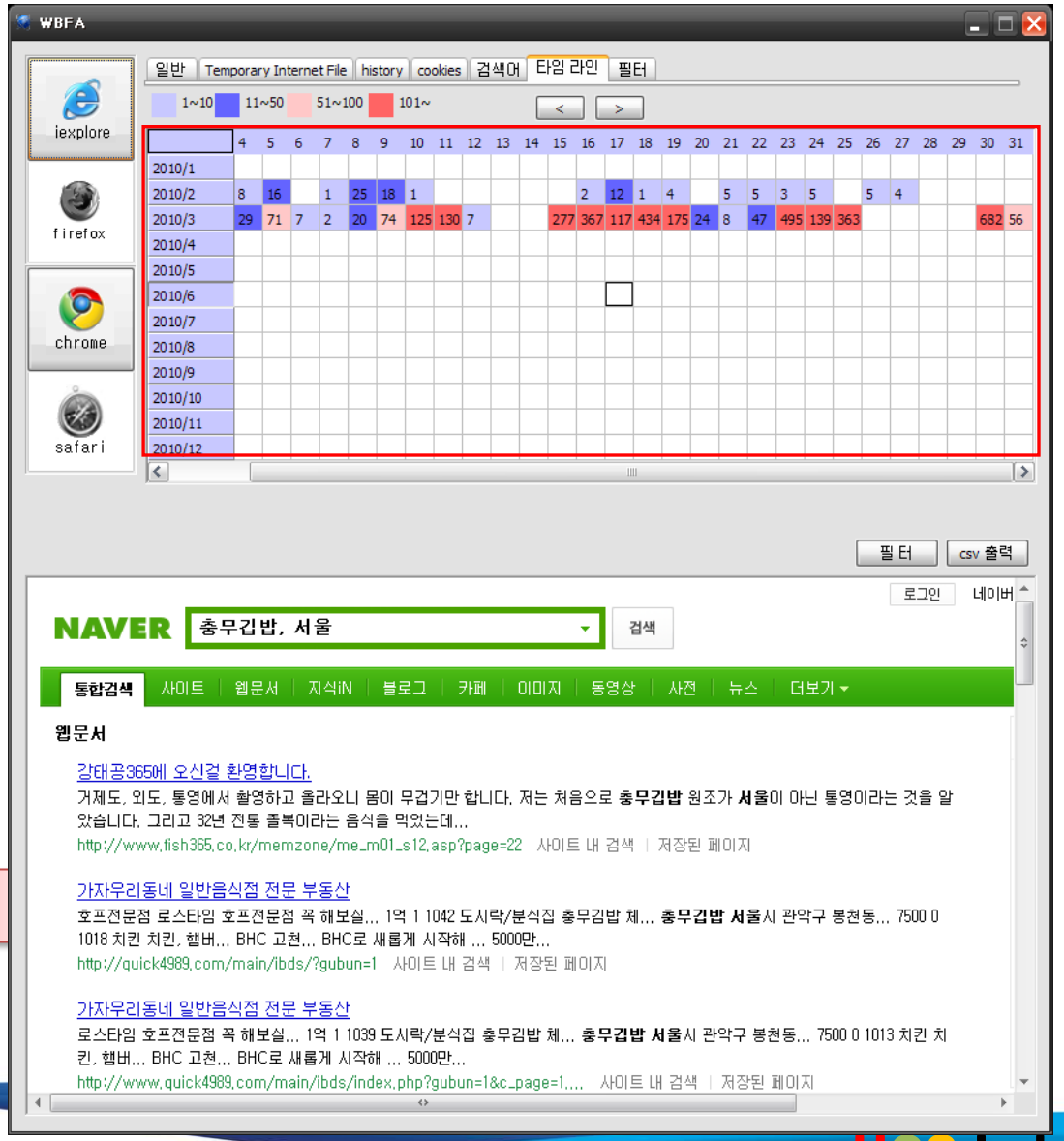
- 응용 프로그램과 파일 유형에 따른 분류
  - 사건과 관련된 정보를 효과적으로 검색하는데 도움을 줄 수 있음
  - 파일 종류 별 통계 분석으로 사용자의 컴퓨터 사용 수준을 파악할 수 있으며 시스템의 주요 사용 목적을 추측할 수 있음



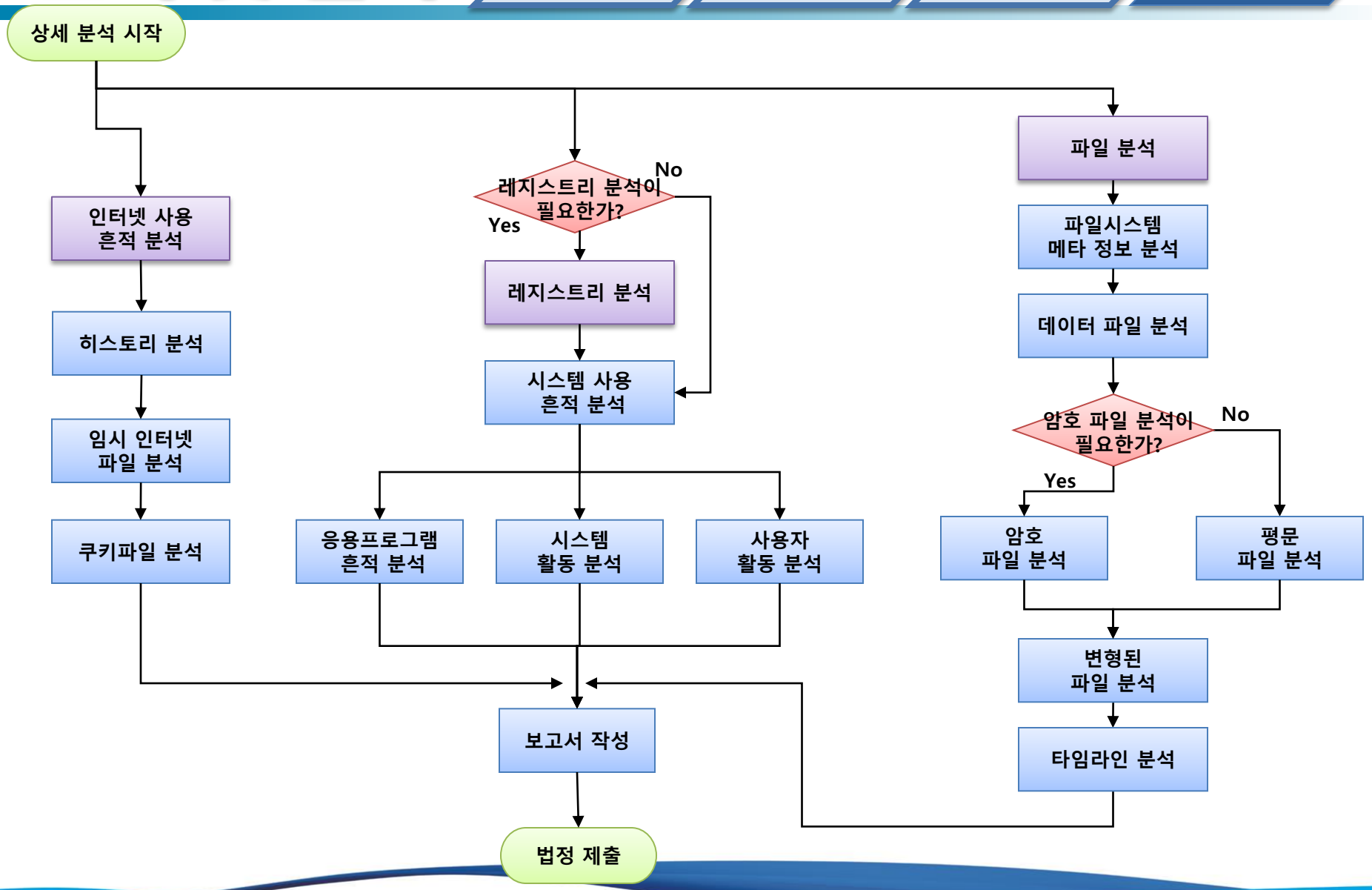


- 특정 시간대에 있는 파일을 분류
  - 시스템 로그 데이터와 응용 프로그램의 로그에서 특정 타임프레임 내에서 수사와 관계된 이벤트가 없는지 확인
  - 사건이 발생한 특정 시점의 전후 시간대를 기준으로 파일의 접근 및 변경 시간을 조사

웹 브라우저 사용기록을 연/월/일 단위로 구분하여 특정 시간 내에 방문한 웹사이트, 검색어 등을 분석

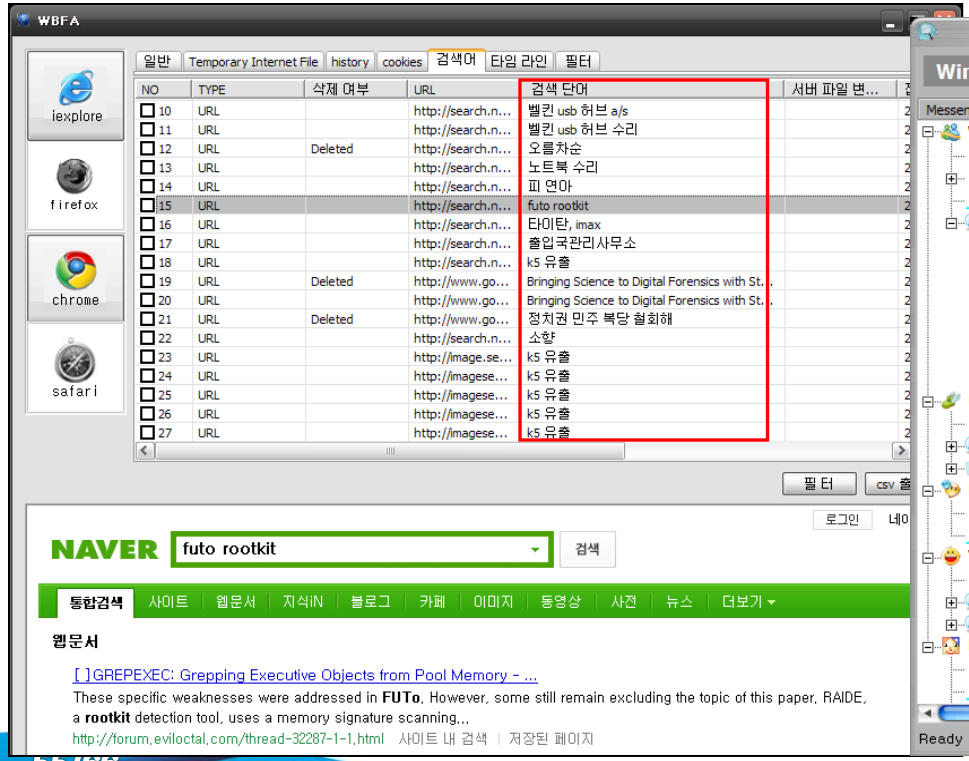


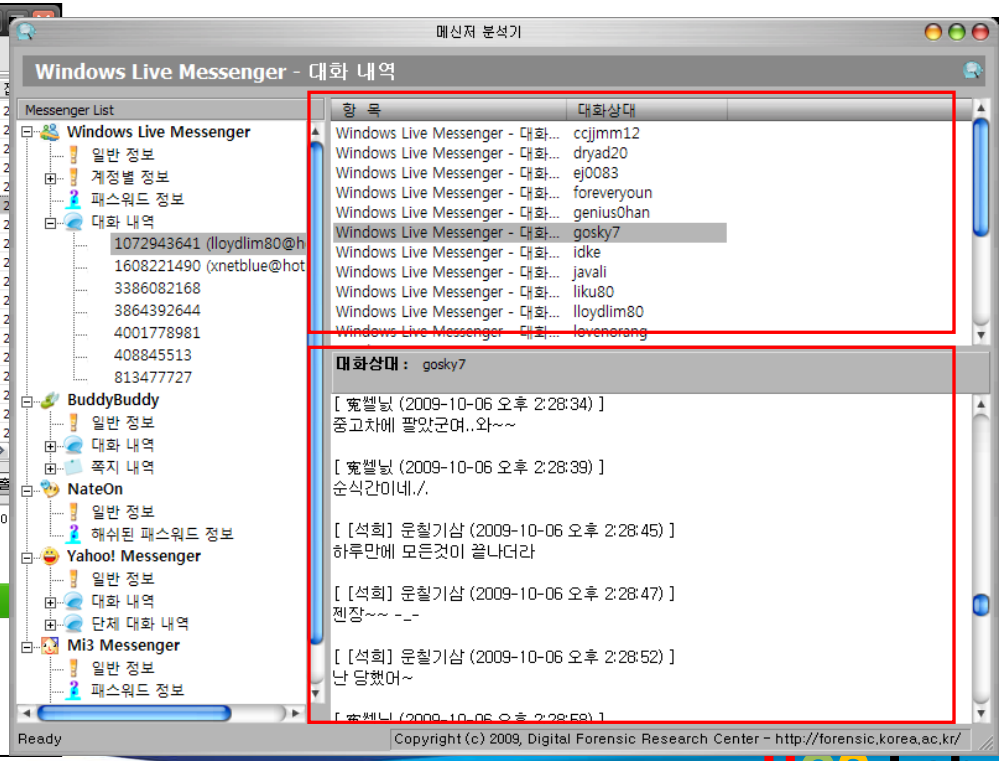
조사 및 분석


상세 분석 시작
인터넷 사용 흔적 분석
히스토리 분석
임시 인터넷 파일 분석
쿠키파일 분석
레지스트리 분석이 필요한가?
No
Yes
레지스트리 분석
시스템 사용 흔적 분석
응용프로그램 흔적 분석
시스템 활동 분석
사용자 활동 분석
파일 분석
파일시스템 메타 정보 분석
데이터 파일 분석
암호 파일 분석이 필요한가?
No
Yes
암호 파일 분석
평문 파일 분석
변형된 파일 분석
타임라인 분석
보고서 작성
법정 제출

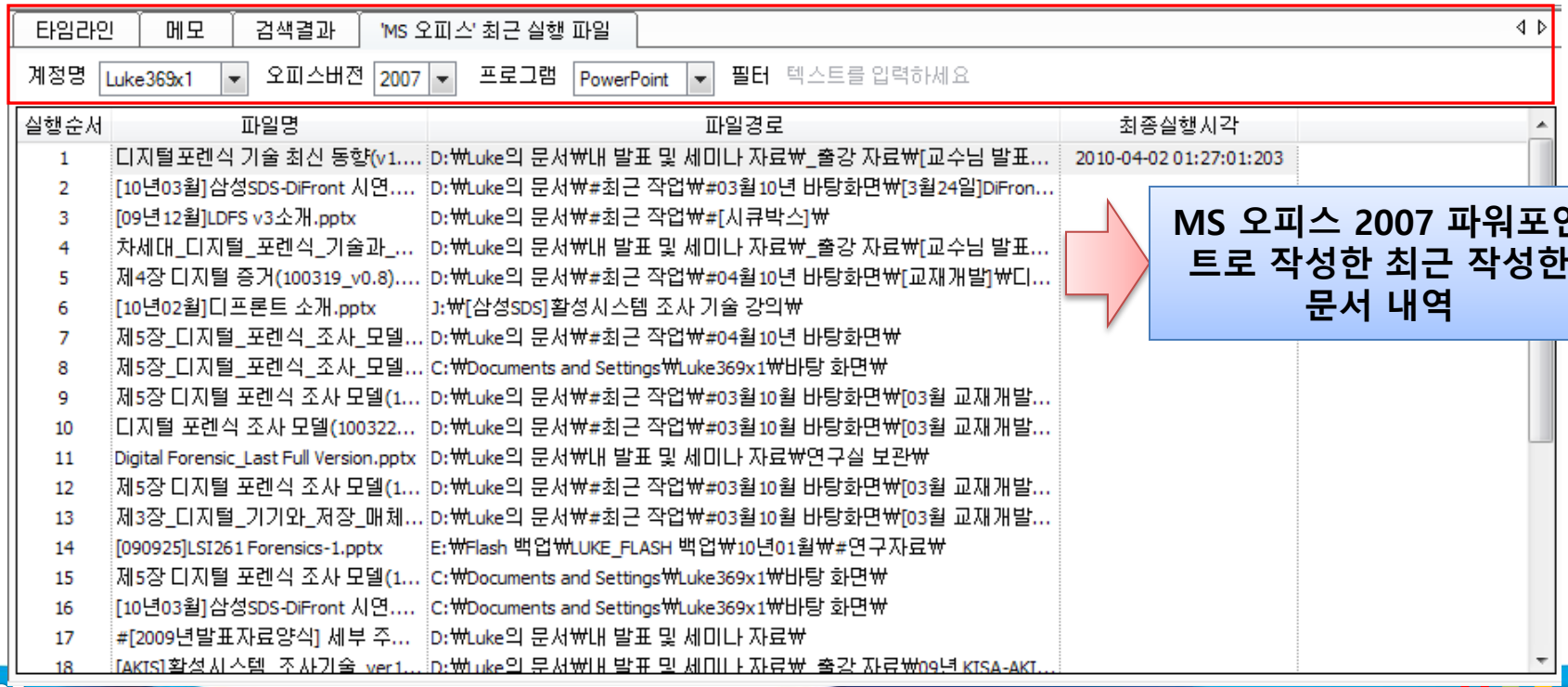
- 파일 분석
  - 상세 분석 과정의 핵심으로, 사용자가 범죄에 이용하였거나 작업한 데이터는 사건 해결에 결정적 단서를 제공
  - 데이터 분류 기법과 응용프로그램 사용 흔적 분석과 연계하여 중요 파일들을 선별하여 분석을 수행

- 인터넷 서비스 사용 흔적 분석
  - 인터넷 사용 흔적은 사용자의 최근 관심사, 취미 생활, 생활 습관 등 행동 패턴까지 분석이 가능
  - 용의자의 인터넷 사용 정보를 조사하면 범죄 행위에 대한 다양한 직·간접적 증거 자료를 획득할 수 있음
  - 전자메일, 메신저 사용 흔적은 사용자의 친구, 인맥, 최근 송수신 자료 또는 대화 내용 등을 획득할 수 있으므로, 범죄 공모 사실, 개인의 비밀 정보 등 유용한 정보를 파악할 수 있음





- 시스템 사용 정보 분석(레지스트리 분석)
  - 사용자 정보, 응용 프로그램 및 하드웨어 설치 정보 등의 유용한 정보를 획득하여 분석
  - Windows 운영체제의 레지스트리는 시스템의 사용 정보를 저장하는 일종의 데이터베이스로, 포렌식 관점에서 유용한 정보가 존재
  - 사용자의 프로필, 컴퓨터에 설치된 응용 프로그램, 최근에 작성한 문서, 사용한 이동형 저장 매체, 폴더 및 응용 프로그램 정보 등을 획득 가능



- 위·변조 데이터 분석
  - 위·변조 데이터가 발견되면 고의적으로 데이터를 은닉한 것으로 볼 수 있으므로, 여기에서 유용한 정보를 취득할 가능성이 높음
  - 위·변조 데이터 분류 방법
    - 파일 확장자의 불일치
      - 해당 파일 구조를 비교하여 파일 확장자의 이상 유무를 판별, 불일치하는 경우 사용자가 고의적으로 은닉할 수 있으므로 실제 파일을 추출하여 분석
    - 패스워드로 접근이 제어되거나 암호화된 파일의 획득
      - 사용자가 데이터를 숨기려고 시도한 것을 판별할 수 있음
      - 또한 복구한 패스워드 자체는 다른 암호화 파일의 복구에 도움을 줌

이름	크기	속성	File Type	Signature Verification	Extension Verification
프로젝트 진행보고(pptx-아래한글 확장자로 변경).hwp	3160374		MS Office (2007)	Signature Miss Match	Extension Miss Match
프로젝트 진행보고(pptx 확장자 그대로).pptx	3160374		Powerpoint Docume...	Compound Document	Compound Document
보고서 포맷(확장자 그대로).hwp	9216		HWP Document	Compound Document	Compound Document
보고서 포맷(아래한글파일-JPG 확장자로 변경).jpeg	9216		Compound Document	Signature Miss Match	Extension Miss Match
논문 A(PDF 파일 PPT 파일로 변경).ppt	175156		Adobe PDF	Signature Miss Match	Extension Miss Match
논문 A (확장자 그대로).pdf	175156		Adobe PDF	Match	Match
jpeg 이미지(확장자 그대로).jpg	34700		JPEG	Match	Match
jpeg 이미지(JPG이미지-아래한글 확장자로 변경).hwp	34700		JPEG	Signature Miss Match	Extension Miss Match

파일 확장자 불일치 여부 확인

보고 및 증언

결과 보고서

- 조사・분석자의 모든 행동과 관찰 내역, 분석 과정 등의 내용을 객관적이고 명확하게 기록
- 분석 결과를 증거 자료로 인정받기 위해 분석 결과를 재현하였을 경우에도 완벽히 일치해야 함
- 보고서의 내용은 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리 정연하게 작성
- 작성자는 결과 보고서에 서명하고 작성 내용에 대해 책임짐

증언

- 분석 보고서에 최종 날인하고 확인한 조사 책임자는 향후 법정에 출두할 가능성이 높음
- 법정에서 전문가 증언 시, 전문가로서 경력에 따라 분석 결과의 신뢰성이 판단될 수 있으므로 사건 책임자나 분석팀장 등이 증언
- 증언 시에는 객관적이고 분명한 어조로 설명해야 하며, 조사 및 분석 내용은 비전문가도 이해할 수 있도록 쉽게 설명해야 함

국외 포렌식 조사 모델 비교

	Lee et al.(2001)	DFRWS(2001)	Reith et al. (2002)	Séamus 확장 모델 (2004)	Casey (2004)
사건 준비 및 대응	인지, 확인 (Recognition, Identification) 수집과 보존 (Collection and Preservation)	확인(Identification) 보존(Preservation) 수집(Collection)	확인(Identification) 준비(Preparation) 보존(Preservation) 수집(Collection)	인식(Awareness) 허가(Authorization) 계획(Planning) 고지(Notification) 탐색/확인 (Search/Identification) 수집(Collection)	인지(Recognition) 보존(Preservation) 수집(Collection) 문서화(Documentation)
이송 및 보관				이송(Transport) 보관(Storage)	
조사	구별(Individualization)	조사(Examination)	조사(Examination)	조사(Examination)	분류(Classification) 비교(Comparison) 구별(Individualization)
분석 및 보고	재구성(Reconstruction) 보고 및 제출 (Reporting and Presentation)	분석(Analysis) 제출(Presentation) 결정(Decision)	분석(Analysis) 제출(Presentation)	가설(Hypothesis) 제출(Presentation) 증명(Proof/Defense) 보고(Dissemination)	재구성(Reconstruction)

국외 포렌식 조사 모델 비교

- DFRWS 모델
  - 디지털 포렌식 수사 모델은 단순히 증거 처리에만 중점
  - 증거 수집, 증거 조사, 증거 분석 단계로 구분

- Henry LEE 의 모델
  - 전체 수사 절차에 중심을 둔 것이 아니라, 범죄 현장에서 어떻게 대응할 것인지를 위주로 제안한 현장 수사 모델 (일반적인 물리 증거 조사까지 포함)
  - 구체적 절차
    - 인지(recognition)
      - 어떤 대상을 잠재적 증거 자료로 삼을 것인지를 파악하여 "무엇을(What), "어디서(Where)" 찾을 것인지를 결정하고, 이를 기록・수집・보존
    - 식별(identification)
      - 물리적・생물학적・화학적 및 그 이외의 증거들을 분류하여 기존 실험 결과와 비교
    - 특정(individualization)
      - 가능성 있는 증거 자료에서 특정인이나 이벤트를 실험과 해석을 통해 유일한 대상으로 선정
    - 재현(reconstruction)
      - 도출된 결과를 종합하여 사건을 재현하고 이를 보고・현출

국외 포렌식 조사 모델 비교

- DFRWS 모델
  - 2001년에 디지털 포렌식 분야의 국제 학술 대회인 DFRWS (Digital Forensic Research Workshop)에서 디지털 포렌식을 중심으로 한 새로운 조사 모델이 발표
  - 특징: 디지털 증거 법적 효력을 갖도록 하기 위해 각 단계 별로 필요한 요소 또는 기술들을 소개하고, 앞으로 어떠한 연구를 수행해야 할 것인가를 제안

확인	보존	수집	조사	분석	제출
사건/범죄 탐지	사건 관리	보존	보존	보존	문서화
고소/고발	이미징 기술	증명된 하드웨어	추적성	추적성	전문가 증언
악성코드 발견	연계 보관	증명된 소프트웨어	유효성 기술	통계 분석	설명
비정상 탐지	시간 정보 확인	법적 권한	필터링 기술	프로토콜 분석	요점 중심 진술
프로파일링		비손실 압축	패턴 매칭	데이터 마이닝	대응책
시스템 모니터링		데이터 샘플링	은닉 데이터 조사	타임라인 분석	통계 해석
감정 분석		데이터 복구	은닉 데이터 추출	상관 분석	

국외 포렌식 조사 모델 비교(Casey 모델)

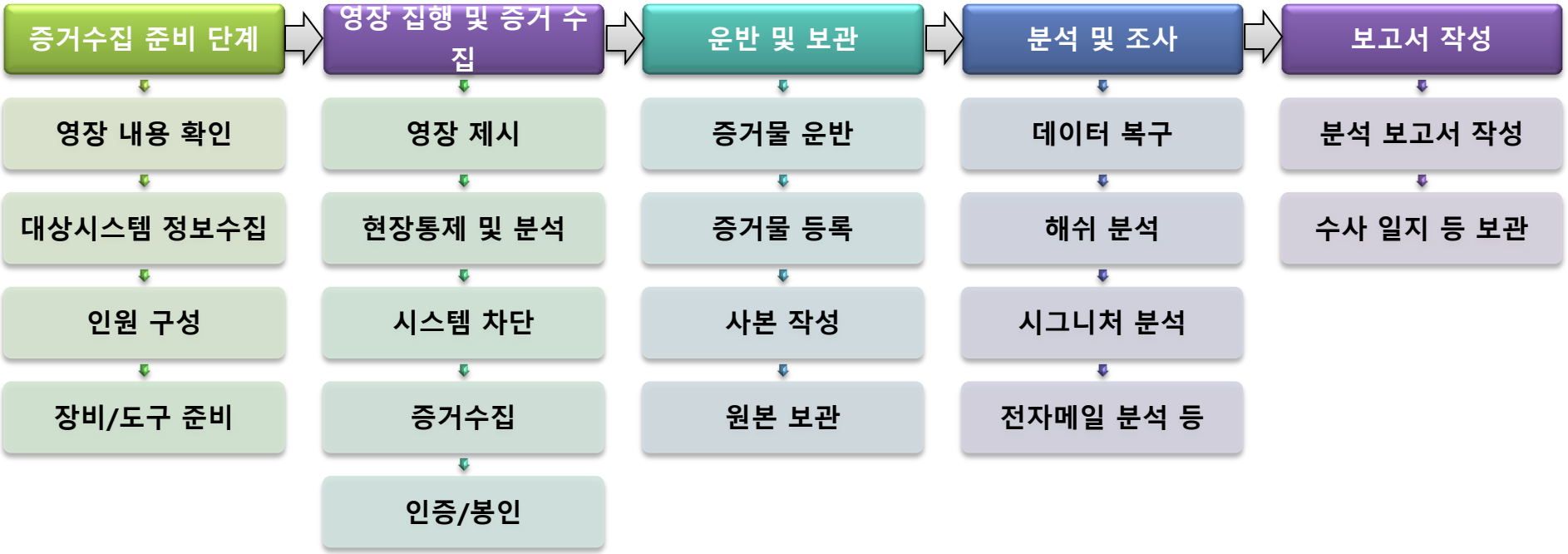
사건 발생	• 범죄가 신고 되거나 위법 행위가 감지되어 수사를 시작하는 단계
가치 평가	• 전반적인 수사 과정에서 어떤 대상이 우선적으로 조사할 가치가 있는지를 평가하여 순위를 선정
현장 대응	• 수사를 진행하는 기관의 입장에서 자체적으로 수립한 규칙・절차에 따라 조사를 진행
확인・압수	• 수립한 가치 평가와 현장 대응 절차를 바탕으로 수사 대상을 확인하고 이를 압수, 포장하는 과정
보존	• 무결성을 유지하기 위해 사본을 생성하고 압수한 원본을 적절한 보관시설에 보존
복구	• 삭제되거나 은닉된 데이터를 복구하여 가능한 모든 데이터를 추출

국외 포렌식 조사 모델 비교(Casey 모델)

조사	• 복구된 데이터를 비롯하여 사건 해결에 필요한 데이터를 수집
분류	• 수집한 데이터를 특정 기준으로 분류하여 분석 과정에 필요 없는 데이터를 삭제하여 조사 대상을 줄이는 과정
재구성 및 검색	• 사건과 관련된 정보를 이용하여 수집한 데이터를 재구성하여 필요한 정보를 검색
분석	• 조사 결과를 바탕으로 평가, 실험, 종합, 상관 분석, 유효성 판단 과정을 거쳐 법정에 제출할 증거 자료를 생성하는 과정
보고	• 생성한 증거 자료가 법정에서 받아들여질 수 있도록 상세히 기록하고 그 과정들을 문서화
진술 및 증언	• 증거 자료, 기록, 관련 조서들을 법정에서 활용할 수 있도록 알기 쉽게 해석하고 이를 진술・증언

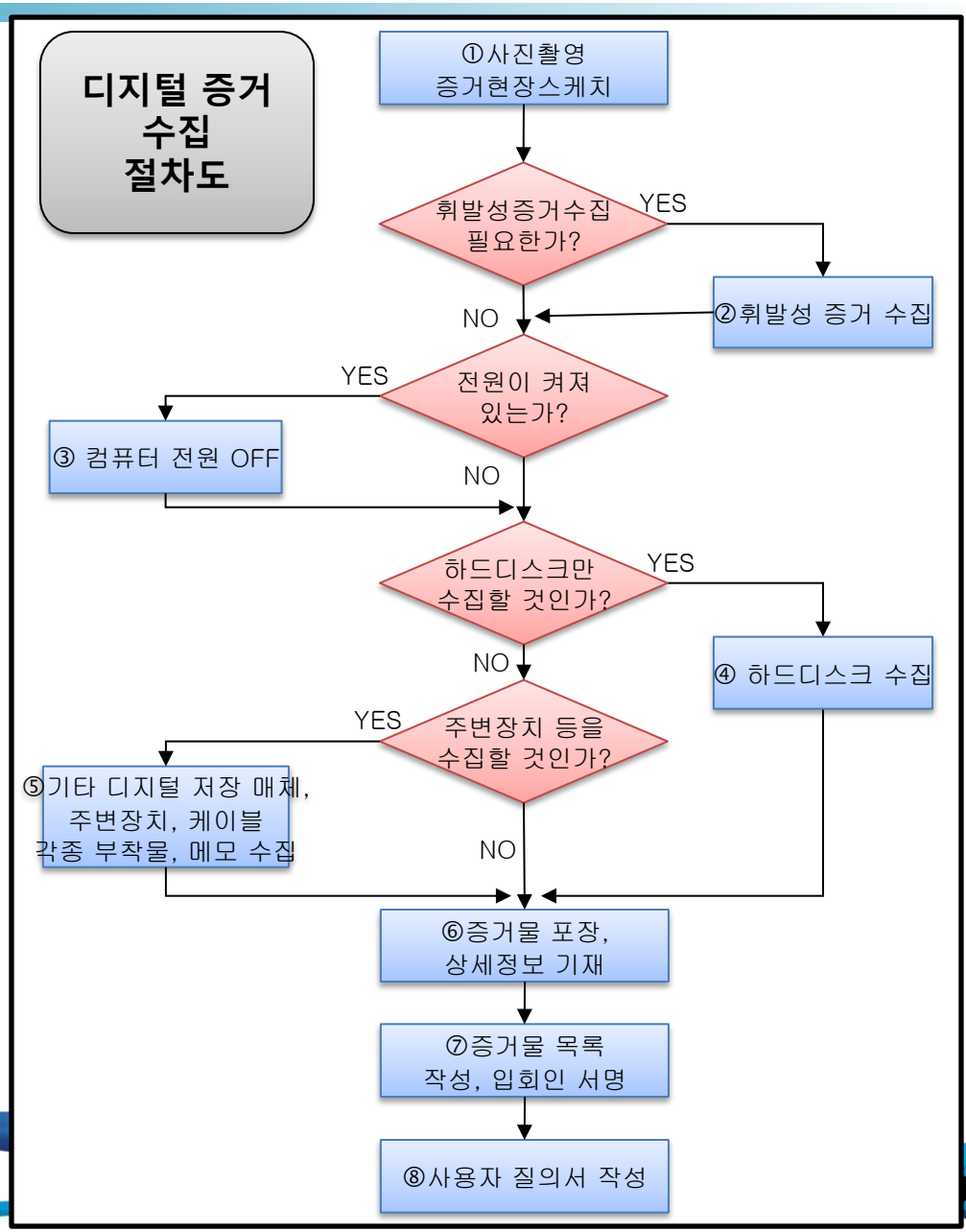
(국내)대검찰청 디지털증거 압수수색 모델

- 대검찰청 압수수색 모델은 수사기관인 점을 감안하여 영장 발부,집행, 압수 수색과 같은 부분이 강조됨



(국내)경찰청 디지털 증거 압수 절차

- 전체 수사 모델에 대해 공개된 자료는 없음
- 경찰청에서 발간한 디지털 증거처리가이드라인에서 증거 수집, 증거 분석, 보고서 작성으로 나누어 상세히 설명하고 있음



디지털 포렌식 조사 모델의 변천

- 각 모델의 초점에 따라 다양
  - 과학적 체계, 기술적인 방법, 조사 절차, 법적 절차 등, 각 모델이 추구하는 초점에 따라 다양한 조사 모델이 존재
  - 디지털 포렌식 연구가 시작된 2000년 초반은 디지털 증거의 취약성에 주의하여 디지털 증거의 보존을 중심으로 발전
  - 최근에는 디지털 포렌식 조사가 일반 민사·형사 사건에 모두 활용되면서 디지털 증거 처리만이 아닌 사건 발생부터 법정 증언까지 고려한 전체 조사 과정을 다루는 모델로 발전

Q & A