7장. 디지털 포렌식 개관

박종혁
서울과학기술대학교 컴퓨터공학과
jhpark1@seoultech.ac.kr

디지털포렌식 관련 영상

- [사이언스 CSI] 보이지 않는 흔적까지 찾는다! 디지털 포렌식 / YTN 사이언스
https://www.youtube.com/watch?v=tQxW-iS6YIE

- [IT 정보] 요즘 big news 많죠? 그전에 모바일 포렌식? 디지털 포렌식? 무엇일까요?
https://www.youtube.com/watch?v=f67sGhHhvRs

- 무한 매력의 소유자, 사이버 포렌식 전문가 / YTN 사이언스
https://www.youtube.com/watch?v=PIGPaRVEwe0

- 20년간 디지털포렌식만 해온 포렌직 전문가에게 물었습니다!
https://www.youtube.com/watch?v=zX-wuyzDsYI

개 요

- 학습목표
  - 디지털 포렌식의 의미와 전반적인 내용을 이해하고 조사과정에서의 일반 원칙 및 수행과정에 대해서 학습한다.
  - 디지털 증거에 대해 이해한다.

- 학습 내용
  - 디지털 포렌식
  - 디지털 포렌식의 일반 원칙
  - 디지털 포렌식의 수행과정
  - 디지털 증거의 종류 및 특징

목 차

6-1. 디지털포렌식 개관

디지털 포렌식 개관

- **법과학(forensic science)**
  - 범죄 사실을 규명하기 위해 각종 증거를 과학적으로 분석하는 분야
- **Digital Forensics** 美 DFRWS(Digital Forensic Research Workshop)
  - 범죄 현장에서 확보한 개인 컴퓨터, 서버 등의 시스템이나 전자 장비에서 수집할 수 있는 디지털 증거물에 대해 보존, 수집, 확인, 식별, 분석, 기록, 재현, 현출 등을 과학적으로 도출되고 증명 가능한 방법으로 수행하는 것
- **컴퓨터 범죄 수사에 입각한 정의**
  - 컴퓨터 관련 조사·수사를 지원하며, 디지털 자료가 법적 효력을 갖도록 하는 과학적·논리적 절차와 방법을 연구하는 학문
    - 전자적 자료: 컴퓨터에만 국한되지 않음
    - 법적 효력: 법규범에 합치되는 논리성을 가져야 함
    - 과학적/논리적: 보편성과 객관성이 필요한 지식 체계
    - 절차와 방법: 목표 달성을 위한 과정이 결과만큼 중요

디지털 포렌식 개념도


국가기관
디지털 증거 채택
사법기관
민간기업
컴퓨터 과학수사
법 · 제도 마련
증거 채택
증거 인증
디지털 포렌식
시스템
회계감사
인증기관
절차 및
기능 인증
기밀정보유출 탐지
모바일 범죄 증가
포렌식 시스템 검증
모바일 업체
검증기관

등장배경

- **디지털 포렌식의 등장 배경**
  - 정보화 사회가 고도화됨에 따라 사이버 범죄가 증가하고 있으며, 이에 대처하기 위해 과학수사와 수사과학 분야에서 새로운 형태의 조사 기술이 필요하게 됨
  - 생성되는 자료의 95% 이상이 전자 형태로 존재, 매년 2배씩 증가

디지털 포렌식 연구 분야

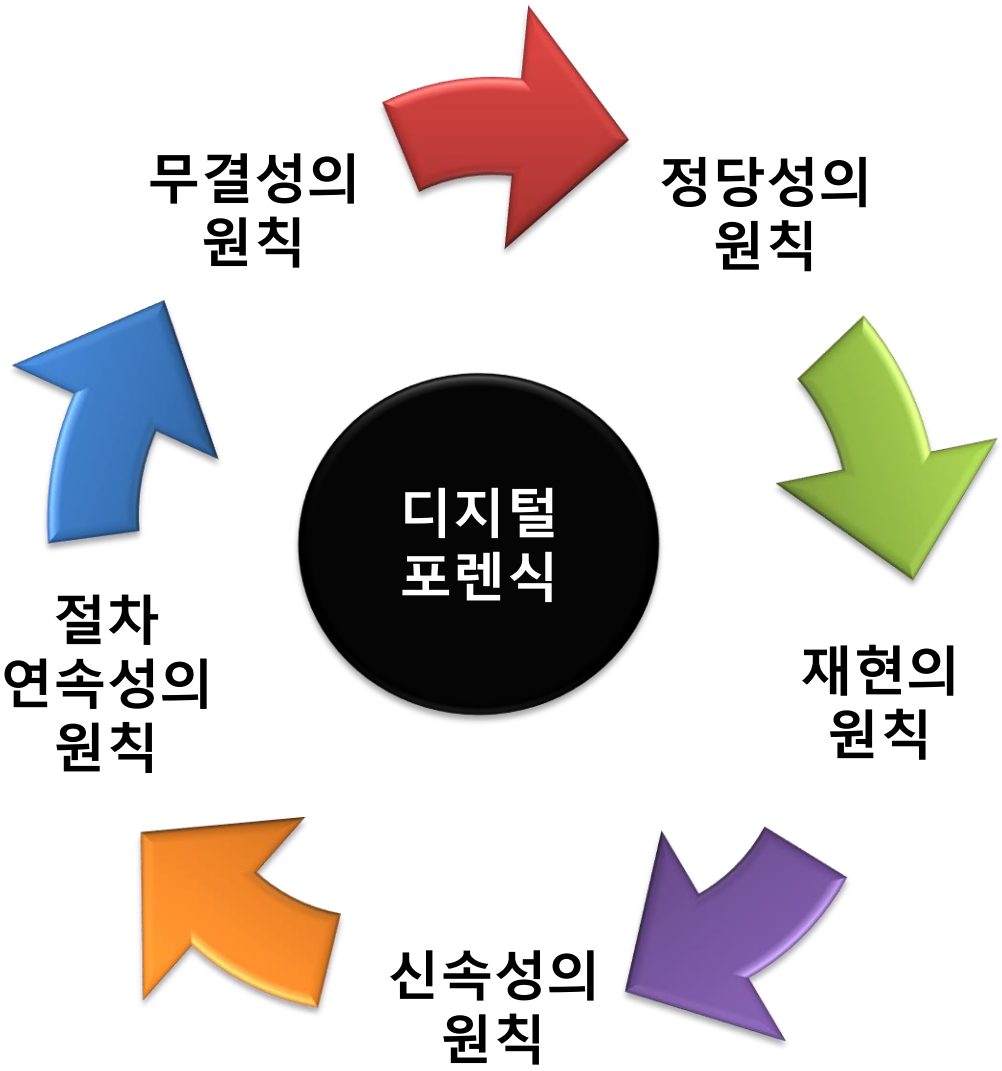
	증거 복구	증거 수집 및 보관	증거 분석
디지털 매체	하드디스크 복구 메모리 복구	하드디스크/전자매체 복제 기술 네트워크 장비 정보수집 하드디스크 복제 장비	전자 매체 사용이력 분석 메모리 정보 분석
시스템	삭제파일 복구 파일 시스템 복구 시스템 로그온 우회기법	휘발성 데이터 수집 시스템 초기 접근 Forensic Live CD	윈도우 레지스트리 분석 시스템 로그 분석
데이터 처리	언어통계 기반 파일복구 암호 해독 / 패스워드 / DB 분석 스태가노그래피 파일 파편 분석	디지털 저장 데이터 추출 디지털 증거 보존 디지털 증거 공증/인증	데이터 포멧별 Viewer 영상 정보 분석 DB 정보 분석 데이터 마이닝
응용 프로그램 및 네트워크	파일포맷 기반 파일복구 프로그램 로그온 우회기법 암호 통신 내용 해독	네트워크 정보 수집 네트워크 역추적 DB 정보 수집 Honey Pot/Net	네트워크 로그 분석 해쉬 DB(시스템, S/W, 악성파일) 웜/바이러스/해킹툴 분석 Network Visualization 기법 네트워크 프로토콜 분석기
기타 기술	프라이버시 보호, 포렌식 수사 절차 정립, 범죄 유형 프로파일링 연구 외산/국산 포렌식 S/W 비교 분석, 하드웨어/소프트웨어 역공학 기술, 회계부정탐지 기술		

디지털 포렌식 분류

디스크 포렌식	물리적인 저장장치인 하드디스크 플로피디스크, CO ROM, DVD 등 각종 보조기억장치에서 증거를 수집하고 분석하는 포렌식 분야 디스크 파일 시스템 분석, 디스크 검색, 복구, 키워드 검색
시스템 포렌식	컴퓨터의 운영체제, 응용프로그램 및 프로세스를 분석하여 증거를 확보하는 포렌식 분야 시스템 데이터 및 로그분석
네트워크 포렌식	네트워크를 통하여 전송되는 데이터나 암호 등을 특정 도구를 이용하여 가로채거나 서버에 로그형태로 저장된 것을 접근하여 분석하거나 에러로그, 네트워크 형태 등을 조사하여 단서를 찾아내는 분야
인터넷 포렌식	인터넷으로 서비스되는 월드와이드웹(WWW), FTP, USENET 등 인터넷 응용프로토콜을 사용하는 분야에서 증거를 수집하는 포렌식 분야
모바일 포렌식	휴대폰, PDA, 전자수첩, 디지털 카메라, MP3, 캠코더, 휴대용 메모리카드 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야 휴대용 기기 데이터 은닉 용이성으로 세심한 분석 필요
데이터베이스 포렌식	데이터베이스로부터 데이터를 추출 분석하여 증거를 획득하는 포렌식 분야 기업의 분식 회계, 횡령, 탈세 수사 시 필수
클라우드 컴퓨팅 포렌식	클라우드 컴퓨팅 환경에서의 사고발생시 사고를 추적하고 증명할수 있는 포렌식 분야 Iaas, PaaS, SaaS 클라우드 서비스 모델에 따른 포렌식 특성 발생

6-2. 디지털포렌식 조사의 일반원칙

디지털 포렌식 조사의 일반 원칙



- **정당성의 원칙**
  - 입수 증거가 적법절차를 거쳐 얻어져야 함
    - 위법수집증거배제법칙
      - 위법절차를 통해 수집된 증거의 증거능력 부정
    - 독수의 과실이론
      - 위법하게 수집된 증거에서 얻어진 2차 증거도 증거능력이 없음
- **재현의 원칙**
  - 같은 조건에서 항상 같은 결과가 나와야 함
- **신속성의 원칙**
  - 전 과정은 지체 없이 신속하게 진행되어야 함

- **연계보관성(Chain of Custody)의 원칙**
  - 증거물 획득 – 이송 – 분석 – 보관 – 법정 제출의 각 단계에서 담당자 및 책임자를 명확히 해야 함
  - 수집된 하드 디스크가 이송단계에서 물리적 손상이 있었다면 이송 담당자는 이를 확인하고 해당 내용을 인수인계, 이후 과정에서 복구 및 보고서 작성 등 적절한 조치를 취할 수 있어야 함
- **무결성의 원칙**
  - 수집 증거가 위·변조 되지 않았음을 증명
    - 수집 당시의 데이터 hash 값과 법정 제출 시점 데이터의 hash 값이 같다면 hash 함수의 특성에 따라 무결성을 입증

Hash 함수

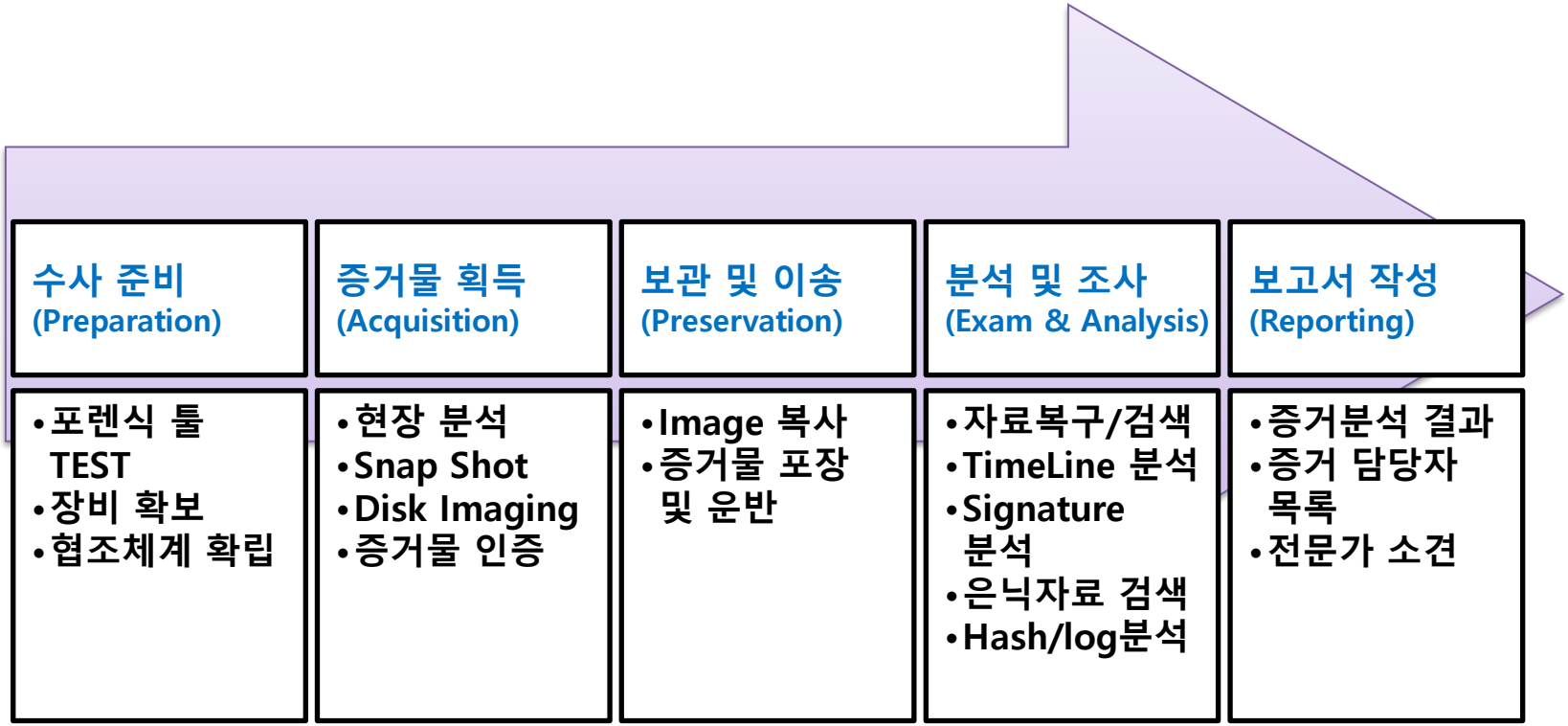
- **Hash**
  - 임의의 비트열을 고정된 짧은 길이로 변환

MD5의 경우 128bit 출력

SHA-1 의 경우 160bit 출력

6-3. 디지털포렌식 수행과정

디지털 포렌식 수행 과정


수사 준비
(Preparation)
증거물 획득
(Acquisition)
보관 및 이송
(Preservation)
분석 및 조사
(Exam & Analysis)
보고서 작성
(Reporting)
•포렌식 툴 TEST
•장비 확보
•협조체계 확립
•현장 분석
•Snap Shot
•Disk Imaging
•증거물 인증
•Image 복사
•증거물 포장 및 운반
•자료복구/검색
•TimeLine 분석
•Signature 분석
•은닉자료 검색
•Hash/log분석
•증거분석 결과
•증거 담당자 목록
•전문가 소견

6-4. 디지털 증거

디지털 증거

- **전자적 형태로 유통되거나 저장되어 있는 데이터로 사건의 발생 사실을 입증하거나 반박하는 정보 또는 범행 의도나 알리바이와 같은 범죄의 핵심 요소를 알 수 있는 정보**
- **컴퓨터 시스템**
  - 하드디스크, USB와 같은 휴대용 저장장치
- **통신 시스템**
  - 네트워크 정보
  - 인터넷, 방화벽, IDS 등의 로그 데이터
- **임베디드 시스템**
  - 휴대폰, PDA, 네비게이터, MP3 플레이어

디지털 증거의 종류

- 문서 파일 : 한글, 훈민정음, MS 워드 등
- 멀티미디어 데이터 : 동영상, 사진, MP3
- 전자메일(email)
- 네트워크 데이터
- 소프트웨어 : 바이러스 제작 도구, 안티 포렌식 도구
- 로그 데이터 : 인터넷, 방화벽, IDS 등의 로그 데이터
- CCTV 영상 데이터
- 임베디드 시스템의 저장 정보
- 교통카드, 신용카드, 휴대폰 사용 기록 등

자동으로 생성되는 디지털 증거

- 인터넷 사용기록
- 방화벽 로그
- 운영체제 이벤트 로그 등
- 최근 사용한 파일

인위적으로 생성되는 디지털 증거

- 문서 파일
- 전자 메일
- 동영상
- 사진
- 소프트웨어
- 암호 데이터

휘발성 증거

- 프로세스
- 예약작업
- 인터넷 연결 정보
- 네트워크 공유 정보
- 메모리 정보 등

비휘발성 증거

- 파일 및 파일 시스템
- 운영체제
- 로그 데이터
- 설치된 소프트웨어

디지털 저장 매체

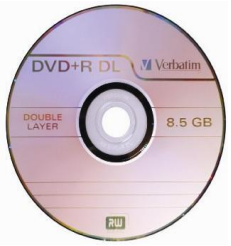




TOSHIBA
SD
Solid State Drive
128GB

Data
Digital Media




DVD+R DL
Verbatim
DOUBLE LAYER
8.5 GB
RW


SanDisk
MEMORY STICK PRO DUO
8GB
MAGICGATE

SanDisk
8GB
micro SD HC



MERCURY


Macintosh

2.0GB


FUJIFILM
xD
xD-Picture Card
512MB



Xacti

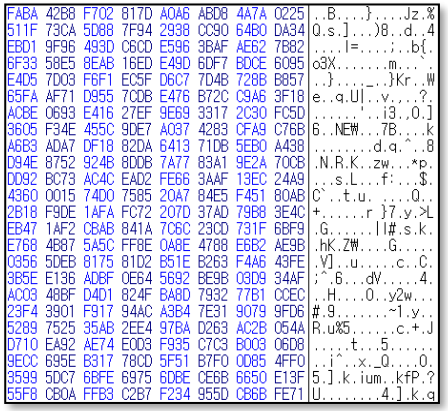

디지털 증거의 특징

- **매체독립성**
  - 디지털 증거는 '유체물'이 아니고 각종 디지털저장매체에 저장되어 있거나 네트워크를 통하여 전송 중인 정보 그 자체
  - 정보는 값이 같다면 어느 매체에 저장되어 있든지 동일한 가치임
  - 따라서 디지털증거는 사본과 원본의 구별이 불가능함

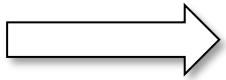
- **비가시성(非可視性), 비가독성(非可讀性)**
  - 디지털 저장매체에 저장된 디지털증거 그 자체는 사람의 지각으로 바로 인식이 불가능하며 일정한 변환절차를 거쳐 모니터 화면으로 출력되거나 프린터를 통하여 인쇄된 형태로 출력되었을 때 가시성과 가독성을 가짐, 따라서 디지털 증거와 출력된 자료와의 동일성 여부가 중요

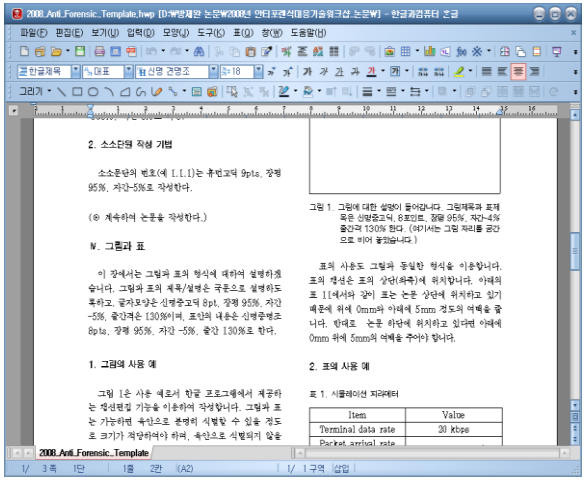
- 비가시성(非可視性), 비가독성(非可讀性)

untitled.bmp
320 x 307
BMP 파일



2008_Anti_Forensic_Template...
한글과컴퓨터 한글 문서
20KB





- **취약성**
  - 디지털 증거는 삭제·변경 등이 용이
  - 하나의 명령만으로 하드디스크 전체를 포맷하거나 파일 삭제가 가능함, 또한 파일을 열어보는 것만으로 파일 속성이 변경됨
  - 수사기관에 의한 증거조작의 가능성도 배제할 수 없으므로 디지털 증거에 대한 무결성 문제가 대두
- **대량성**
  - 저장 기술의 발전으로 방대한 분량의 정보를 하나의 저장 매체에 모두 저장할 수 있게 됨, 회사의 업무처리에 있어 컴퓨터의 사용은 필수적이고, 회사의 모든 자료가 컴퓨터에 저장됨
  - 그 결과 수사기관에 의하여 컴퓨터 등이 압수되는 경우, 업무수행에 지장을 줄 수 있음

- **전문성**
  - 디지털 방식으로 자료를 저장하고 이를 출력하는데 컴퓨터 기술과 프로그램이 사용됨
  - 디지털증거의 수집과 분석에도 전문적인 기술이 사용되므로, 디지털 증거의 압수·분석 등에 있어 디지털 포렌식 전문가가 필수적임
  - 여기에서 디지털 증거에 대한 신뢰성 문제가 대두됨
- **네트워크 관련성**
  - 디지털 환경은 각각의 컴퓨터가 고립되어 있는 것이 아니라 인터넷을 비롯한 각종 네트워크를 통하여 서로 연결되어 있음
  - 디지털 증거는 공간의 벽을 넘어 전송되고 있으며, 그 결과 관할권을 어느 정도까지 인정할 것인지 국경을 넘는 경우 국가의 주권문제까지도 연관됨

참고문헌

- 대검찰정 과학수사본부 : 디지털포렌식센터
  - https://www.spo.go.kr/spo/major/forensics/forensics01.jsp
- 경찰청 사이버 안전국 : 디지털포렌식센터
  - http://cyber.go.kr/bureau/sub4.jsp?mid=040401
- 사이버포렌식협회
  - http://www.cfpa.or.kr/intro2.htm
- 한국포렌식학회
  - https://kdfs.jams.or.kr/co/main/jmMain.kci
- 한국디지털포렌식전문가협회
  - http://fka.kr/
- KISTI 마켓 리포트, 디지털포렌식, 38, 2016
- 최우용, 은성경, “스마트포렌식 기술 동향”, ETRI, 2015
- UK parliment, “Digital Forensics and Crim”, POST-pn-520, 2016
- 이상진, “디지털포렌식기술동향 및 발전전망”, 고려대학교 Digital Forensic Research Center, 2016
- 박명찬, " 디지털 포렌식 이란?”, 행복마루, 2017
- 더존 정보보호서비스, “산업기술유출 방지 및 정보감사를 위한 디지털포렌식의 이해와 적용“, 더존포렌식센터
- 김인순, “디지털 포렌식 개념도”, 전자신문, 2011
- HM Knowledge, “클라우드 포렌식”, 2021

Q & A