6장. 디지털 포렌식 개관

박종혁

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech.ac.kr

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

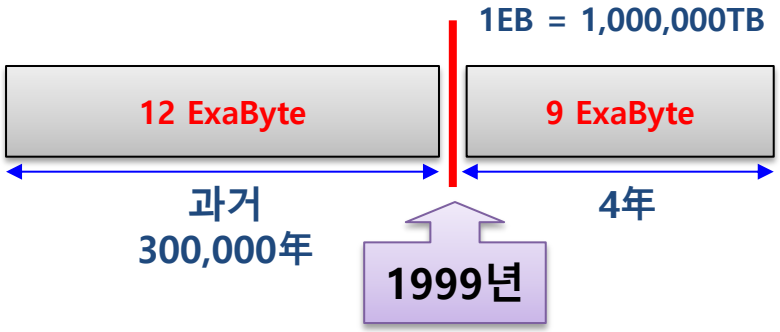
6-1. 디지털포렌식 개관

디지털 포렌식 개관

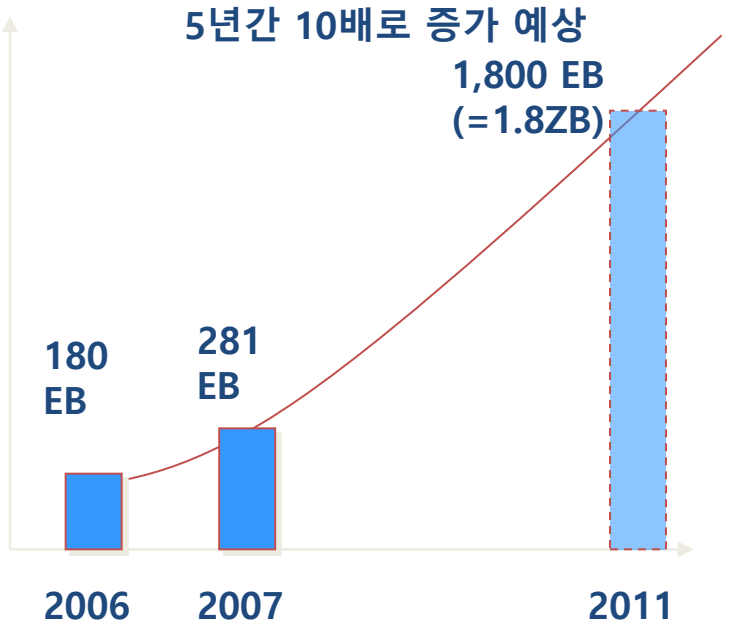
- **법과학(forensic science)**
  - 범죄 사실을 규명하기 위해 각종 증거를 과학적으로 분석하는 분야
- **Digital Forensics** 美 DFRWS(Digital Forensic Research Workshop)
  - 범죄 현장에서 확보한 개인 컴퓨터, 서버 등의 시스템이나 전자 장비에서 수집할 수 있는 디지털 증거물에 대해 보존, 수집, 확인, 식별, 분석, 기록, 재현, 현출 등을 과학적으로 도출되고 증명 가능한 방법으로 수행하는 것
- **컴퓨터 범죄 수사에 입각한 정의**
  - 컴퓨터 관련 조사·수사를 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

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

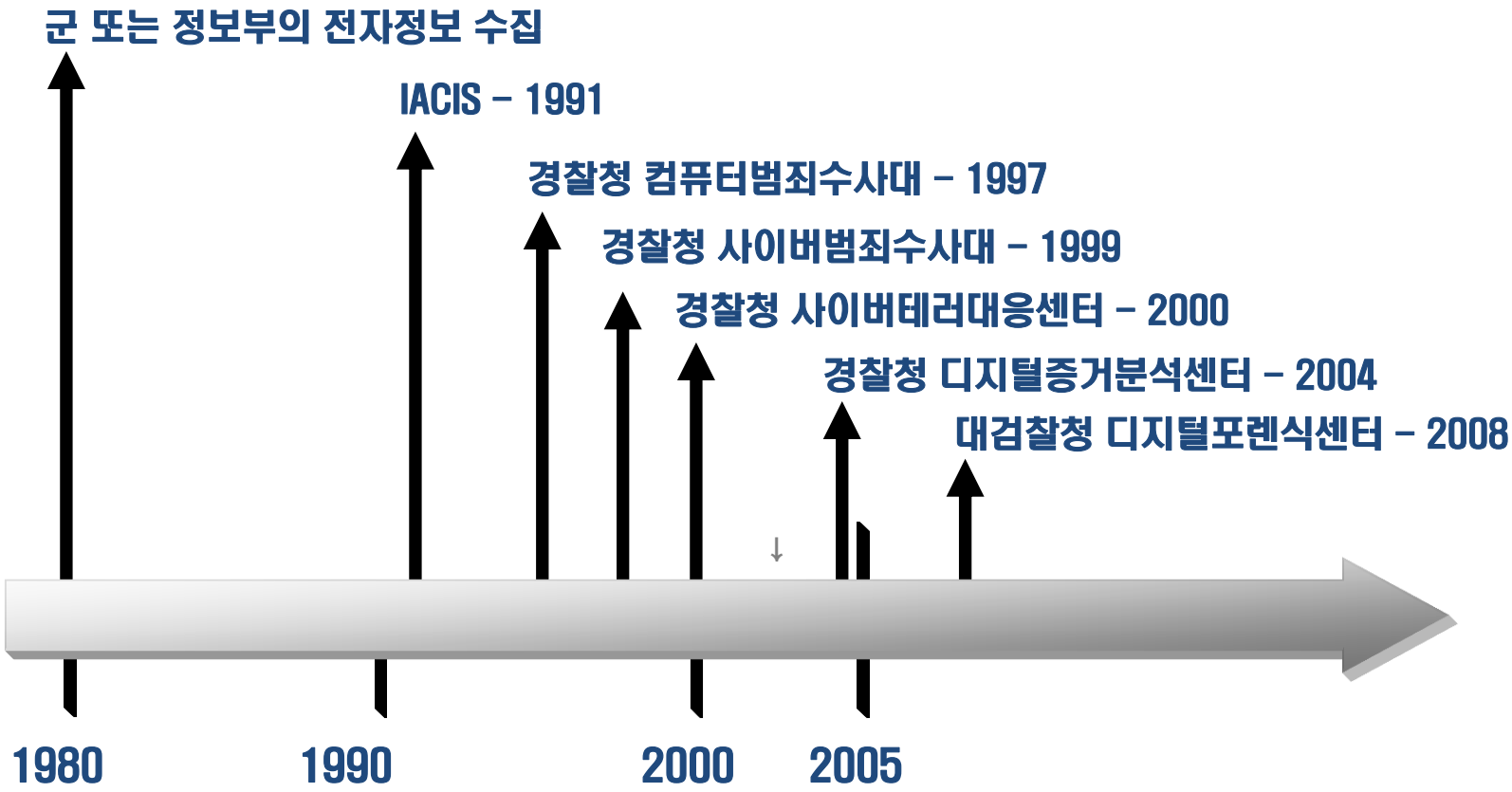


출처 버클리 大



출처
IDC

디지털 포렌식 흐름

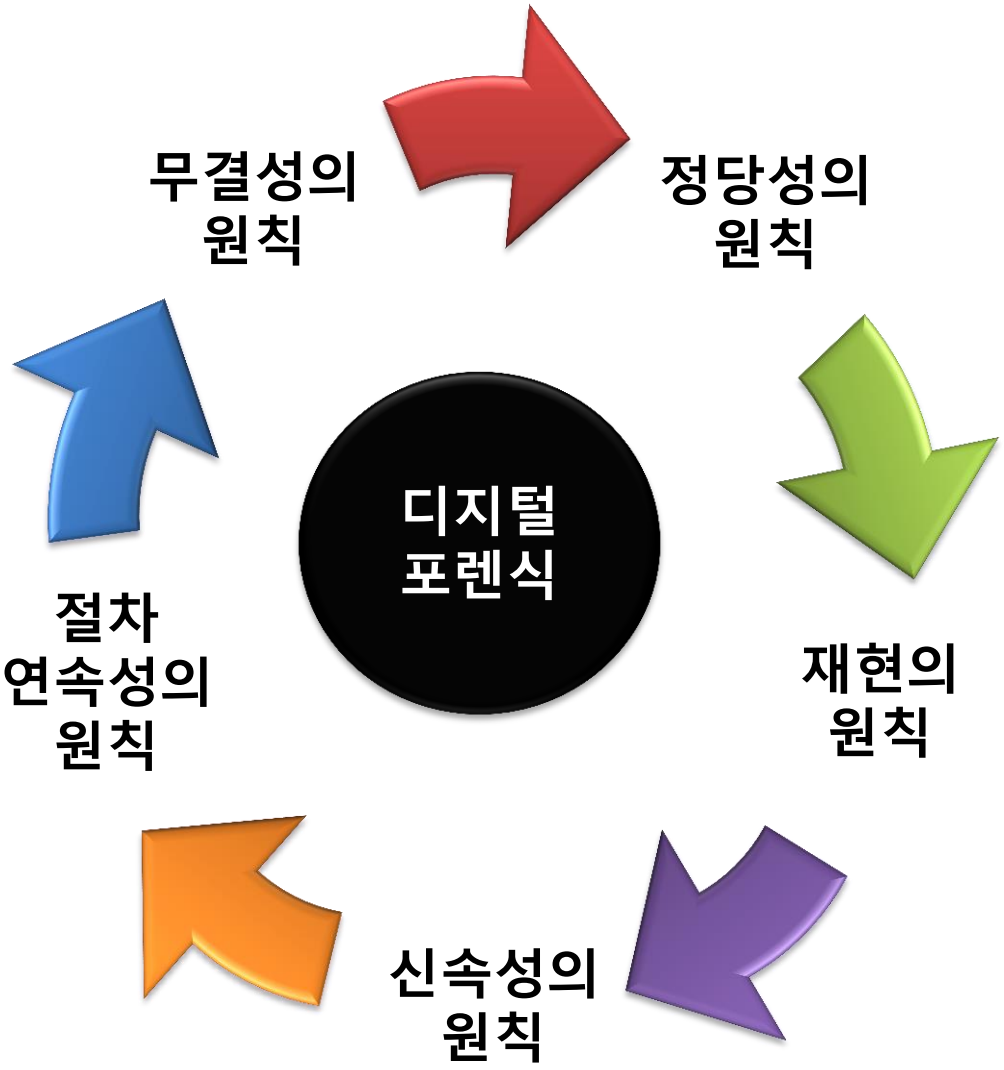

군 또는 정보부의 전자정보 수집
IACIS – 1991
경찰청 컴퓨터범죄수사대 – 1997
경찰청 사이버범죄수사대 – 1999
경찰청 사이버테러대응센터 – 2000
경찰청 디지털증거분석센터 – 2004
대검찰청 디지털포렌식센터 – 2008
1980
1990
2000
2005

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		

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

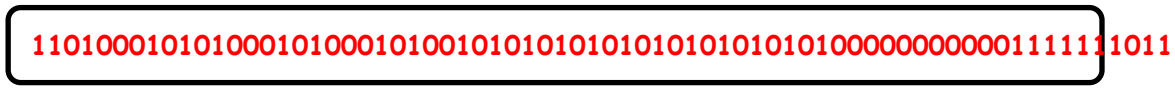
- **연계보관성(Chain of Custody)의 원칙**
  - 증거물 획득 – 이송 – 분석 – 보관 – 법정 제출의 각 단계에서 담당자 및 책임자를 명확히 해야 함
  - 수집된 하드 디스크가 이송단계에서 물리적 손상이 있었다면 이송 담당자는 이를 확인하고 해당 내용을 인수인계, 이후 과정에서 복구 및 보고서 작성 등 적절한 조치를 취할 수 있어야 함
- **무결성의 원칙**
  - 수집 증거가 위·변조 되지 않았음을 증명
    - 수집 당시의 데이터 hash 값과 법정 제출 시점 데이터의 hash 값이 같다면 hash 함수의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

Hash 함수

- **Hash**
  - 임의의 비트열을 고정된 짧은 길이로 변환

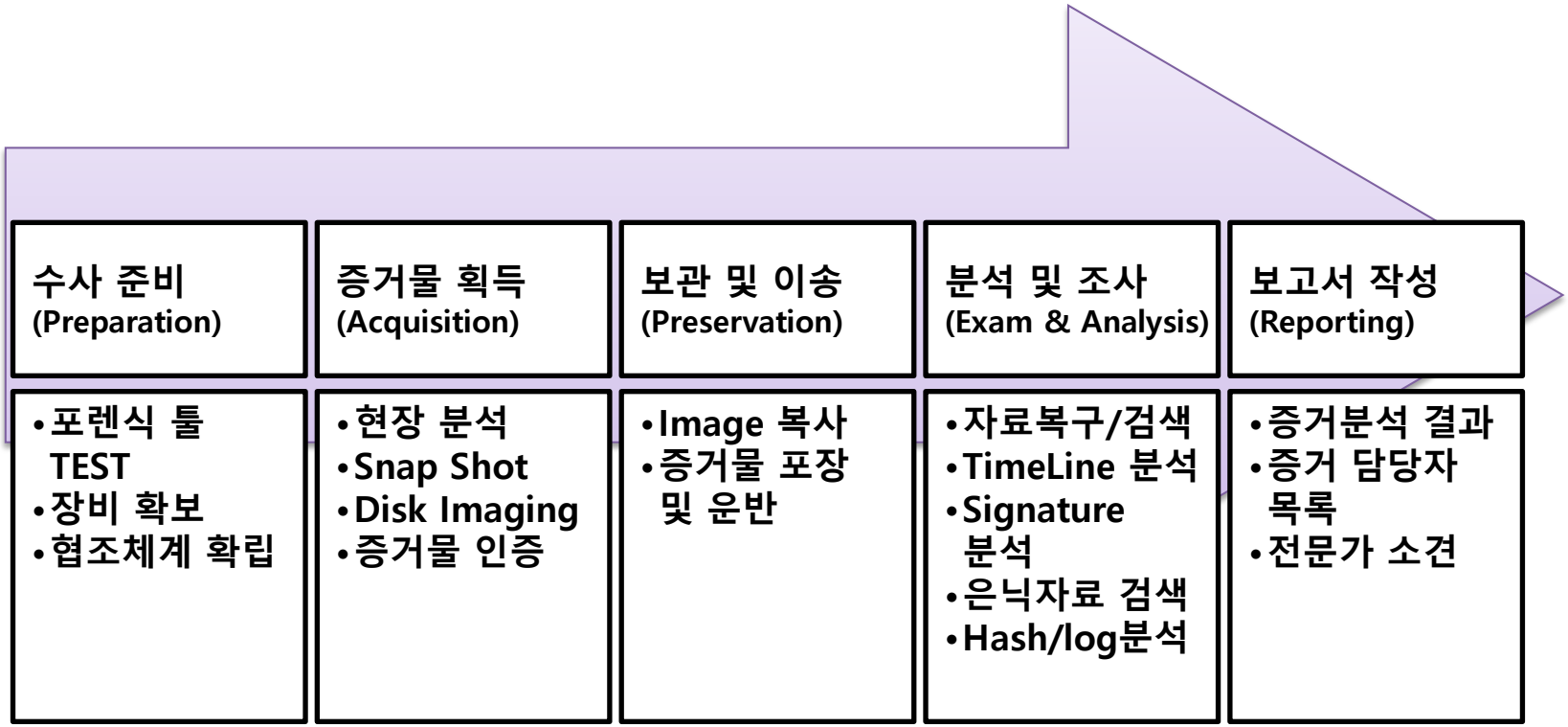
MD5의 경우 128bit 출력

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 알리바이외 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
Solid State Drive
128 GB

Data
Digital Media




DVD+R DL
Verbatim
DOUBLE LAYER
8.5 GB


SanDisk
MEMORY STICK PRO DUO
8GB
MAGICGATE

SanDisk
8GB
micro SD HC



MERCURY


Macintosh

2.0GB


FUJIFILM
xD
xD-Picture Card
512MB



Xacti

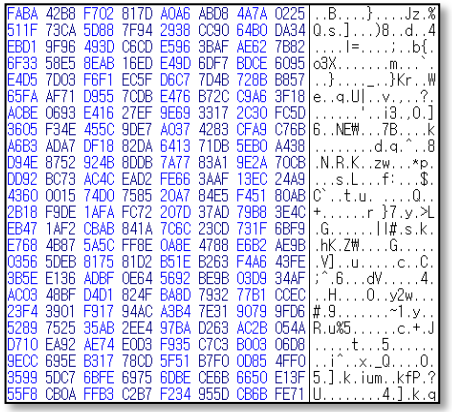

디지털 증거의 특징

- **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

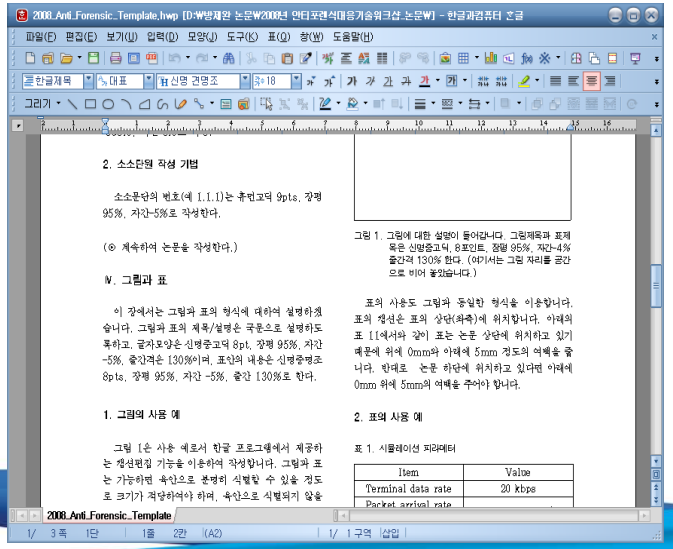
- **비가시성(非可視性), 비가독성(非可讀性)**
  - 디지털 저장매체에 저장된 디지털증거 그 자체는 사람의 지각으로 바로 인식이 불가능하며 일정한 변환절차를 거쳐 모니터 화면으로 출력되거나 프린터를 통하여 인쇄된 형태로 출력되었을 때 가시성과 가독성을 가짐, 따라서 디지털 증거와 출력된 자료와의 동일성 여부가 중요

- 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



UCS Lab

- **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

디지털포렌식 동향

- 글로벌 디지털 포렌식 시장은 2014년 20억 달러에서 연평균 12.5%씩 성장하여, 2020년에는 40억 달러로 전망되며, 국내 시장은 2020년에는 400억 원 규모로 성장 할 것으로 전망됨

(단위 : 억 달러, 억 원)

구분	2014년	2015년	2016년	2017년	2018년	2019년	2020년	CAGR(%)
세계 시장	20.0	22.5	25.3	28.4	32.0	36.0	40.5	12.5
국내 시장	200	225	253	285	320	360	405	

자료: Digital Forensic Market(GSGTF) 2015-2021, 2016 국내외 지식정보보안 산업동향보고서

- 최근 법적 증거제출 목적외에 보안이 중요한 국방 과 금융, 의료, 정보기술, 교육, 물류 등 다양한 분야에서도 디지털 포렌식 기술이 요구되고 있음

- 기술발전에 따라 디지털 매체에 대한 증거의 효율적 수납과 보존, 분석 기술인 디지털 포렌식 기술은 산업 전 분야에 걸쳐 지속적으로 성장할 것으로 기대
  - 기술의 급발달로 인해 모바일과 클라우드 컴퓨팅, 사물인터넷(Internet of Things, IoT) 분야의 폭발적인 성장이 예측되고 있음

- 스마트폰에는 통화기록, 문자 메시지, 이메일, 아이디, 패스워드, GPS 데이터, 신용카드 등 수많은 개인정보가 저장되기 때문에 개인 사이버범죄 수사에서 모바일 포렌식 활용이 증가함

- 지속적으로 광범위하게 등장하는 모바일 기술, 다양한 펌웨어, 제조사의 각기 다른 하드웨어 및 소프트웨어 등이 현재 포렌식 수사 과제로 새롭게 대두되고 있음

- 보편적으로 사용되고 있는 클라우드 컴퓨팅은 기존의 컴퓨팅 환경과 다른 특징들을 가지기 때문에 새로운 형태의 디지털 포렌식 조사 절차 및 방법이 필요하며 연구기관 및 기업에서 활발히 연구 되고 있음

- 최근 빅데이터, 머신러닝 및 딥러닝, 유전자 알고리즘(Genetic Algorithm), 양자컴퓨터 등 다양한 미래IT 기술의 급격한 변화로 융합형 디지털포렌식 연구 및 인력 양성의 중요성이 강조되고 있음

- 영국의회(Parliament UK) **Digital Forensics and Crime** 보고서에서 발표된 2017 디지털 포렌식의 과제(Challenges)
  - 데이터 액세스
    - 범죄에 사용된 전자정보들은 암호화 및 범죄자만의 보안절차를 심어 놓거나 개인 클라우드에 저장되어 조사관이 접근할 때 액세스 및 가용하기가 쉽지 않음
  - 암호화
    - 범죄에 사용된 전자정보는 일반적으로 암호화 되어있기 때문에 암호 알고리즘, 키, 관련 함수를 분석하여 암호해독이 필요함
  - 클라우드 스토리지
    - 클라우드 컴퓨팅 (데이터 저장, 처리 및 소프트웨어와 같은 공유 컴퓨팅 리소스에 대한 온라인 액세스 포함)의 사용 증가는 클라우드 데이터가 빠르게 변경 될 수 있으며 한 사용자가 삭제 한 항목은 다른 사용자가 빠르게 덮어 쓸 수 있어 증거 데이터 수집에 어려움을 줌
  - 안티포렌식
    - 일부 범죄자는 법 집행에 사용되는 기술을 이미 알고 있으며 디지털 활동을 숨기려고 함
    - 안티포렌식 행위
      - 파일과 관련된 날짜와 시간을 변경
      - 파일을 덮어 써서 파일을 영구히 삭제
      - 암호화 된 디지털 스토리지를 사용하여 드라이브의 다른 섹션으로 연결되는 여러 개의 암호를 중첩하여 사용

디지털포렌식 관련 기관

- 정부기관
  - **대검찰청 과학수사부** : 국가디지털포렌식 센터
    - 범죄수사 증거물의신속·정확한감정 및 분석
    - 사이버범죄에 체계적인 대응으로 일선 검찰청 수사를 지원
  - **경찰청 사이버 안전국** : 디지털포렌식 센터
    - 디지털포렌식 정책 기획, 유관기관 협력, 장비보급
    - 디지털증거 수집·분석 기법 연구 개발
    - 포렌식 지원 시스템 관리, 중요사건 현장지원 및 지도
  - **중앙선거관리위원회** : 사이버선거범죄대응센터
    - 가짜뉴스 등 비방·흑색선전행위를 차단·대응을 위해 디지털증거 수집 및 분석
- 연구기관
  - **한국포렌식학회(KDFS)**
    - 포렌식전문가 자격시험제도 운영
    - 포렌식 전문가 양성 및 검증, 재교육 실시
  - **한국디지털포렌식전문가협회(KDFPA)**
    - 디지털포렌식 도구 개발 및 검증, 디지털 증거분석, 정보침해사고 조사 및 정보보안 컨설팅, 디지털포렌식 교육 및 전문가 양성, 디지털포렌식관련 세미나 개최
  - **사이버포렌식협회(CFPA)**
    - 사이버포렌식 분야에 종사하는 전문가들의 저변확대와 교육, 회원 간 정보교류, 친목도모 등을 목적으로 설립

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**
- **Parliament UK, “Digital Forensics and Crime”, POST-pn-520, 2016**

Q & A