forensic-proof.com

디지털 포렌식 개요 및 절차

Twitter : @pr0neer

Blog : forensic-proof.com

Email : proneer@gmail.com

Kim Jinkook

개요

1. 디지털 포렌식 개요
2. 디지털 포렌식 기술
3. 디지털 포렌식 절차

디지털 포렌식 개요

Security is a people problem…

디지털 포렌식 개요

포렌식 vs 디지털 포렌식

디지털 포렌식 개요

전통적인 증거

디지털 포렌식 개요

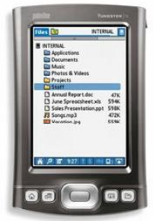
디지털 증거














디지털 포렌식 개요

디지털 포렌식 정의

- **컴퓨터 포렌식(computer forensics), WIKIPEDIA**
  - "Computer forensics is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media."

- **디지털 포렌식(digital forensics), WIKIPEDIA**
  - "Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term was originally used as a synonym for computer forensics but has expanded to cover other devices capable of storing digital data."

- **포렌식(forensic science), WIKIPEDIA**
  - "Forensic is the application of a broad spectrum of sciences to answer questions of interested to a legal system. The word forensic comes from the Latin adjective forensics, meaning 'of or before the forum'."

디지털 포렌식 개요

디지털 포렌식이란?

- **과학 수사**
  - 사건의 정확한 진상 규명을 위해 현대적 기술·시설 ·장비와 과학적 기술 ·지식을 활용하는 수사
  - 군, 검찰, 경찰 등 수사권자
- **수사과학**
  - 수사 활동에 필요한 지식을 객관적 및 계통적으로 연구하는 활동
  - 전문가, 감정가, 감식가 등
- **디지털 포렌식 (컴퓨터 포렌식, 사이버포렌식, e-Discovery)**
  - 디지털 데이터를 근거로 삼아 해당 디지털 기기를 매개체로 하여 발생한 특정 행위의 사실 관계를 법정에서 규명하고 증명하기 위한 절차와 방법
  - 정보화가 고도화되면서 과학수사, 수사과학 분야에서 디지털 기기를 매개체로 한 기술이 요구됨

디지털 포렌식 개요

디지털 포렌식 발전

- **1822 – 1911**
  - 살인 등의 범죄 사건에서 처음으로 지문(fingerprint) 정보 기록 – Francis Galton
- **1887 – 1954**
  - 범죄 사건에서 처음으로 혈액형을 사용 – Leone Latters
  - 란트슈타이너(Karl Landsteiner, 1868-1943, 오스트리아) - ABO식 혈액형 발명
- **1891 – 1955**
  - 총기와 총알의 비교를 통해 처음으로 사건을 해결 – Calvin Goddard
- **1858 – 1946**
  - 사건 조사 절차 동안 증거를 문서화하기 위한 형식을 개발 – Albert Osborn

디지털 포렌식 개요

디지털 포렌식 발전

- **1847 – 1915**
  - 사건 수사에 과학 연구를 최초로 사용 – Hans Gross
- **1932**
  - 포렌식 서비스를 제공하기 위해 연구소 개설 – FBI (The Federal Bureau of Investigation)
- **1984**
  - 컴퓨터 증거를 찾기 위해 FBI의 지원을 받아 CART(Computer Analysis and Response Teram) 구성
- **1993**
  - 컴퓨터 증거에 관한 첫 번째 국제 컨퍼런스가 미국에서 개최

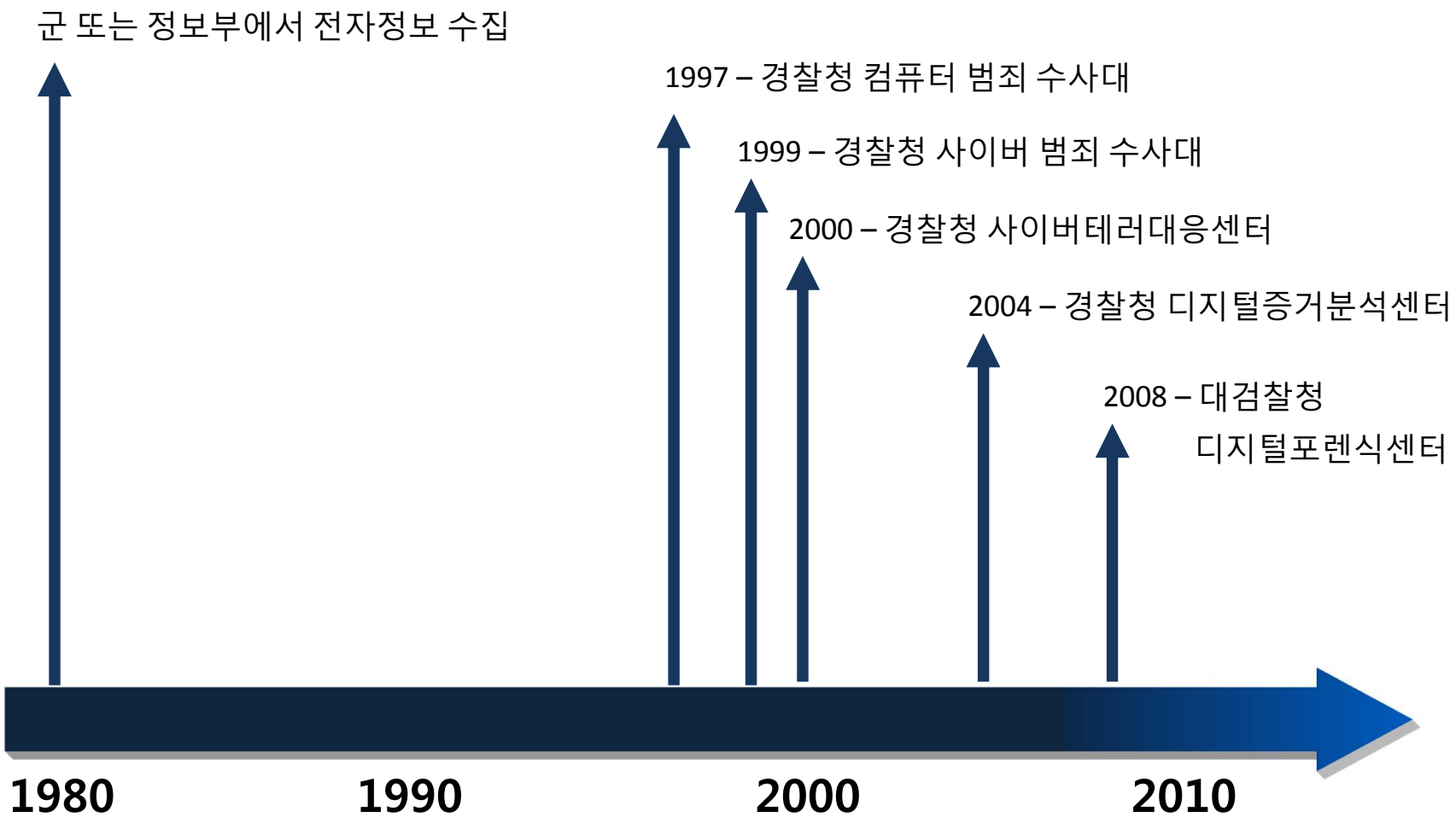
디지털 포렌식 개요

디지털 포렌식 발전

- **1995**
  - 사이버범죄 수사와 컴퓨터 포렌식과 관련된 문제에 관한 정보를 교환하기 위한 기구 설치
  - IOCE (International Organization on Computer Evidence)
- **1998**
  - 국제 포렌식 과학 심포지엄 개최
- **2000**
  - FBI에서 신원 확인, 해킹, 컴퓨터 바이러스, 테러리즘, 투자 사기, 사이버 스토킹, 마약 밀매, 피싱/스푸핑, 불법 프로그램, 신용 카드 사기, 온라인 경매 사기, 스팸, 지적재산권 등의 범죄 수사를 지원하기 위해 디지털 증거를 조사하는 전문 연구기관 설립
  - RCFL – First FBI Regional Computer Forensic Laboratory

디지털 포렌식 개요

국내 디지털 포렌식 발전



디지털 포렌식 개요

디지털 포렌식 목적

- 법정에서 증거로서 인정받을 수 있도록 디지털 매체와 관련된 데이터를 보존, 복구, 분석하기 위한 활동 – 디지털 증거

- 짧은 시간 내에 증거를 확인하기 위해 가해자의 신원을 의도와 신원을 확인하고, 악의적인 행위로 인해 일어난 잠재적인 영향을 확인하기 위한 활동

디지털 포렌식 개요

디지털 증거란?

- **디지털 데이터**
  - 컴퓨터, 휴대폰 등의 디지털 기기에 존재하는 데이터

- **디지털 증거**
  - 디지털 포렌식 기법을 활용하여 수집된 디지털 데이터(저장매체에 저장, 네트워크 전송)로 법정에서 증거 능력을 갖는 디지털 데이터
  - ESI : Electronically Stored Information

디지털 포렌식 개요

디지털 데이터 특성

- **비가시성** – 눈으로 확인하기 어렵기 때문에 별도의 장치가 필요
- **변조 가능성** – 0과 1로 이루어진 데이터로 쉽게 변조가 될 수 있음
- **복제 용이성** – 0과 1의 특성 상 쉽게 복제할 수 있음
- **대규모성** – 디지털 데이터는 매우 방대하므로 고급 검색 및 필터가 필요
- **휘발성** – 내, 외부의 영향으로 쉽게 사라질 수 있음
- **초국경성** – 인터넷의 발달로 인해 데이터의 영향 범위가 국경을 초월함

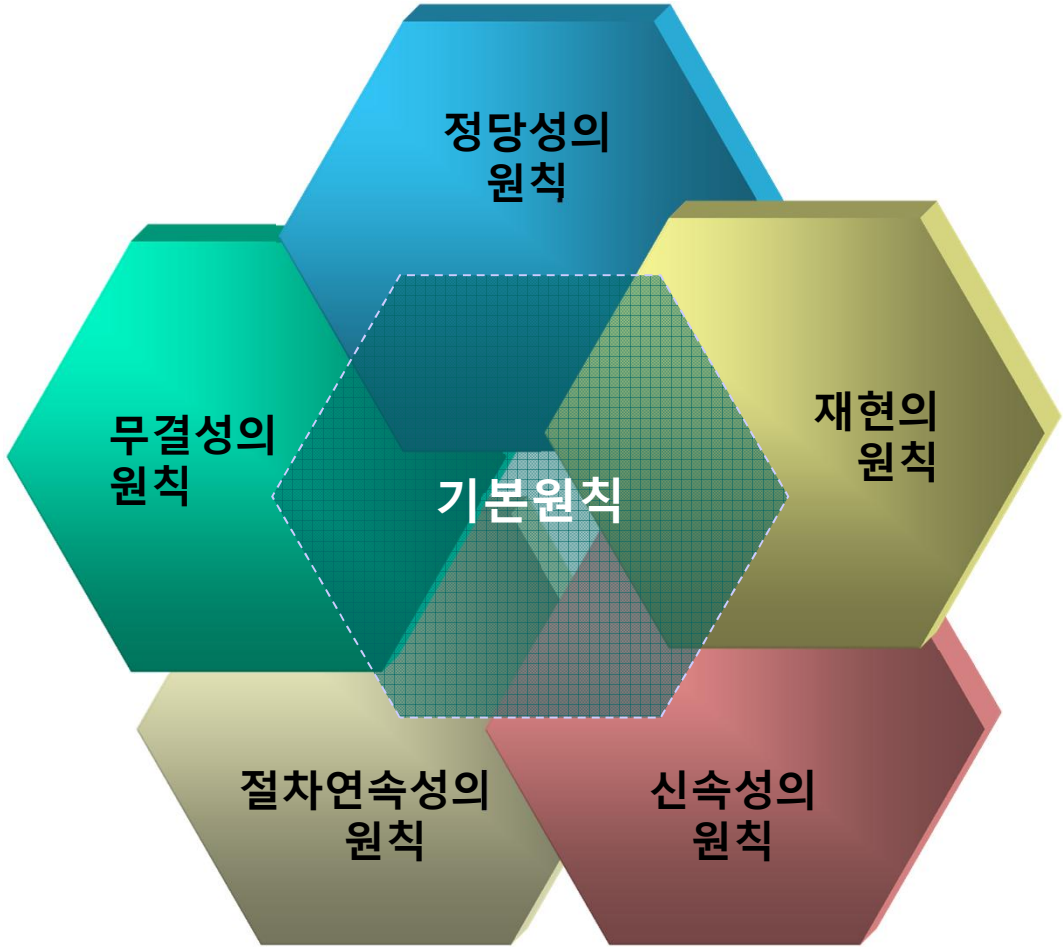
디지털 포렌식 개요

디지털 데이터의 증거능력 요건

- **디지털 데이터가 증거 능력을 보장하기 위한 특성**
  - 진정성 (Authenticity)
    - 해당 증거가 특정인이 특정 시간에 생성한 파일이 맞는지 여부
  - 무결성 (Integrity)
    - 원본으로부터 증거 처리절차 과정 동안 수정, 변경, 손상이 없어야 함
  - 원본성 (Originality)
    - 실제 법정에 제출되는 원본과 다른 사본 증거에 대한 증거 능력을 부여할 수 있는가?
  - 신뢰성 (Reliability)
    - 증거의 분석 과정에서 증거가 위,변조 되거나 의도하지 않은 오류를 포함해서는 안됨

디지털 포렌식 개요

디지털 포렌식 기본 원칙



디지털 포렌식 개요

디지털 포렌식 기본 원칙

- **정당성의 원칙**
  - 증거가 적법절차에 의해 수집되었는가?
  - **위법수집증거배제법칙**
    - 위법절차를 통해 수집된 증거는 증거능력이 없음 (불법적인 해킹을 통해 수집한 증거)
  - **독수 독과(과실)이론**
    - 위법하게 수집된 증거에서 얻어진 2차 증거도 증거능력이 없음
    - (불법적인 해킹을 통해 얻은 패스워드로 특정 파일을 복호화하여 얻은 증거)

디지털 포렌식 개요

디지털 포렌식 기본 원칙

- **재현의 원칙**
  - 같은 조건과 상황하에서 항상 같은 결과가 나오는가?
    - 불법 해킹 용의자의 해킹 툴이 증거능력을 가지기 위해서는 같은 상황의 피해시스템에 툴을 적용할 경우 피해 결과와 일치하는 결과가 나와야 함

- **신속성의 원칙**
  - 디지털 포렌식의 전 과정이 신속하게 진행되었는가?
    - 휘발성 데이터의 특성 상 수사 진행의 신속성에 따라 증거 수집 가능 여부가 달라짐

디지털 포렌식 개요

디지털 포렌식 기본 원칙

- **절차 연속성(Chain of Custody)의 원칙**
  - 증거물의 수집, 이동, 보관, 분석, 법정 제출의 각 단계에서 담당자 및 책임자가 명확해야 함
    - 수집된 저장매체가 이동 단계에서 물리적 손상이 발생하였다면, 이동 담당자는 이를 확인하고 해당 내용을 정확히 인수 인계하여 이후의 단계에서 적절한 조치가 취해지도록 해야함

- **무결성의 원칙**
  - 수집된 증거가 위·변조 되지 않았는가?
    - 일반적으로 해쉬값을 이용하여 수집 당시 저장매체의 해쉬값과 법정 제출 시 저장매체의 해쉬값을 비교하여 무결성 입증

디지털 포렌식 개요

사이버범죄

- **정의**
  - “any illegal act that involves a computer, its systems or its applications.”
  - 사이버 공간인 인터넷 환경 및 컴퓨터와 관련된 모든 범죄
  - 1969년 처음으로 컴퓨터 관련 범죄 발생
- **특징**
  - 속도가 빠름 (Speed)
  - 익명성 (Anonymity)
  - 증거의 생명 주기가 짧음 (Fleeting nature of evidence)

디지털 포렌식 개요

사이버범죄

- **분류**
  - 내부자 공격 (Insider attacks)
    - 조직 내에 고용인으로부터 발생되는 악의적인 행위
  - 외부자 공격 (External attacks)
    - 내부자에 의해 고용되거나 경쟁자의 명성에 해를 입히기 위한 외부자 공격

디지털 포렌식 개요

사이버범죄

- **사이버(컴퓨터) 범죄의 유형**

신원 도용	이메일 폭탄/스팸
해킹	지적재산권 도용
컴퓨터 바이러스	서비스 거부 공격
사이버 스토킹	인터넷 금전 사기
마약 밀매	투자 사기
피싱/스푸핑	사이버 명예 훼손
불법 프로그램	소프트웨어 저작권
신용카드 사기	금전 위조
온라인 경매 사기	음란/성인물

디지털 포렌식 개요

디지털 포렌식 적용 분야

- **사이버 및 지능 범죄**
  - 해킹, 바이러스 및 악성 코드 피해 시스템 조사, 사이버 테러, 정보 은닉, 암호화, 침해 사고 대응

- **일반 및 강력 범죄**
  - 공갈, 사기, 위조, 협박, 횡령, 명예훼손 등의 일반 범죄
  - 회계부정, 세금포탈, 기업 비밀 유출(내부감사)
  - 살인, 강도, 강간, 폭행 등의 강력 범죄

- **민사 소송 분쟁**
  - 명예훼손, 업무상 과실 재해, 내부 감사

디지털 포렌식 개요

디지털 포렌식 적용 대상

- 개인용 및 서버용 컴퓨터, 노트북
- 이동형 저장 매체(CD, DVD, USB, 외장하드 등)
- 휴대폰, 스마트폰
- 데이터베이스
- 디지털 카메라, PDA, 녹음기, 캠코더, MP3, PMP
- CCTV, GPS 네비게이션, 블랙 박스
- 네트워크 장비(라우터, 스위치 등)
- 디지털 증거가 남을 수 있는 모든 디지털 장치

디지털 포렌식 개요

디지털 포렌식 유형

- **디스크 포렌식 (Disk Forensics)**
  - 비휘발성 저장매체(하드디스크, SSD, USB, CD 등)를 대상으로 증거 획득 및 분석
- **활성데이터 포렌식 (Volatile data Forensics)**
  - 휘발성 데이터를 대상으로 증거 획득 및 분석
- **네트워크 포렌식 (Network Forensics)**
  - 네트워크로 전송되는 데이터를 대상으로 증거 획득 및 분석
- **이메일 포렌식 (Email Forensics)**
  - 이메일 데이터로부터 송.수신자, 보낸.받은 시간, 내용 등의 증거 획득 및 분석
- **웹 포렌식 (Web Forensics)**
  - 웹 브라우저를 통한 쿠키, 히스토리, 임시파일, 설정 정보 등을 통해 사용 흔적 분석

디지털 포렌식 개요

디지털 포렌식 유형

- **모바일/임베디드 포렌식 (Mobile/Embedded Forensics)**
  - 휴대폰, 스마트폰, PDA, 네비게이션, 라우터 등의 모바일 기기를 대상으로 증거 획득 및 분석
- **멀티미디어 포렌식 (Multimedia Forensics)**
  - 디지털 비디오, 오디오, 이미지 등의 멀티미디어 데이터에서 증거 획득 및 분석
- **소스코드 포렌식 (Source code Forensics)**
  - 프로그램 실행 코드와 소스 코드의 상관관계 분석, 악성코드 분석
- **데이터베이스 포렌식 (Database Forensics)**
  - 방대한 데이터베이스로부터 유효한 증거 획득 및 분석
- **안티포렌식 (Anti-Forensics)**
  - 데이터 완전 삭제, 암호화, 심층암호 (Steganography)

디지털 포렌식 개요

디지털 포렌식 분야의 확장

- 전자증거개시 (E-discovery)
- 포렌식 어카운팅 (Forensic Accounting)
- 내부 감사 (Internal Audit)

디지털 포렌식 기술

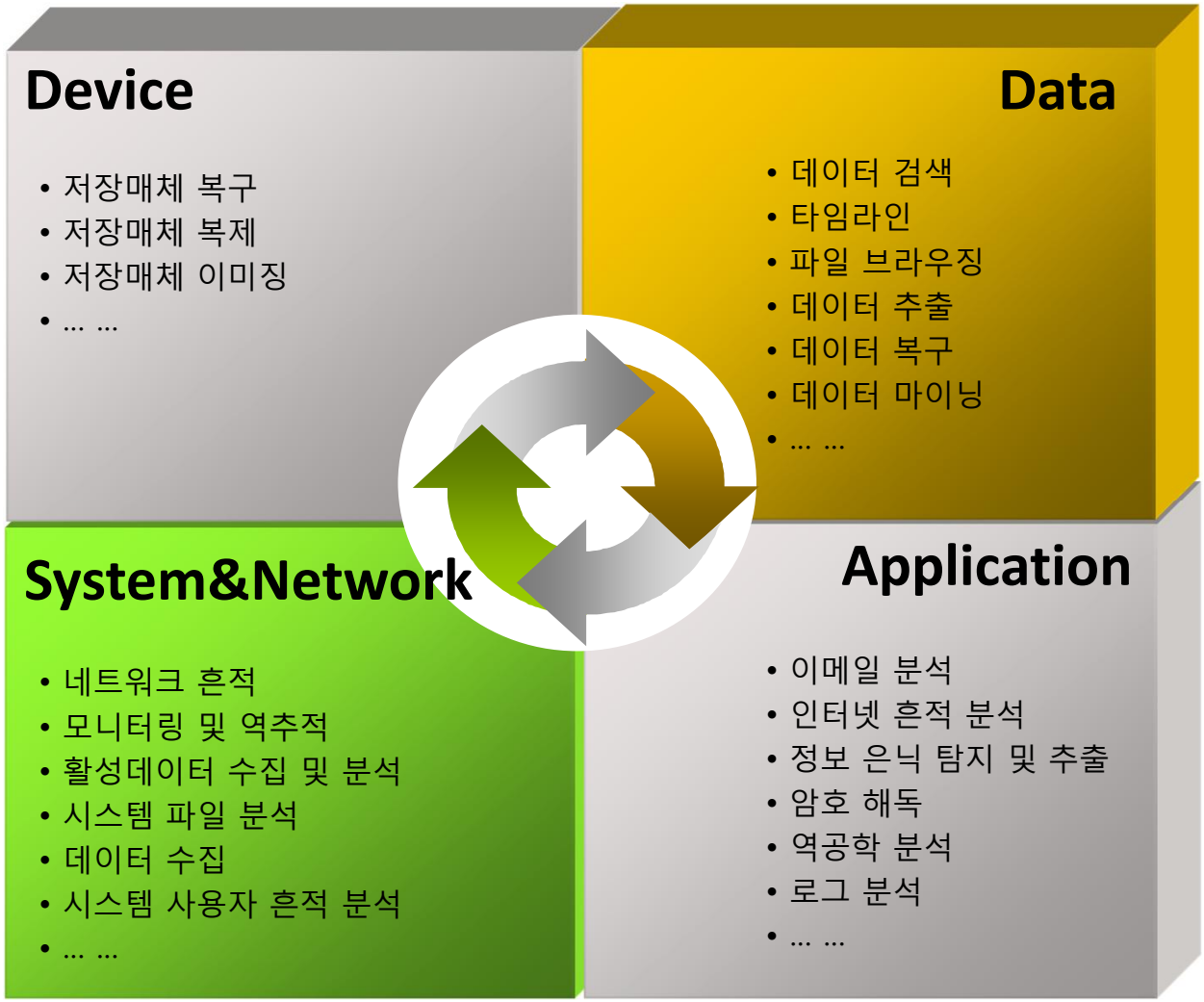
Security is a people problem…

디지털 포렌식 기술

디지털 포렌식 기술 (1)

	증거 복구	증거 수집 및 보관	증거 분석
저장매체	• 하드디스크 복구 • 메모리 복구	• 하드디스크 복제 기술 • 메모리기반 장치 복제 기술 • 네트워크 정보 수집 • 저장매체 복제 장비	• 저장매체 사용 흔적 분석 • 메모리 정보 분석
시스템	• 삭제된 파일 복구 • 파일시스템 복구 • 시스템 로그온 우회기법	• 휘발성 데이터 수집 • 시스템 초기 대응 • 포렌식 라이브 CD/USB	• 윈도우 레지스트리 분석 • 시스템 로그 분석 • 프리패치 분석 • 백업 데이터 분석
데이터 처리	• 언어통계 기반 복구 • 암호 해독 / DB 구축 • 스테가노그래피 • 파일 조각 분석	• 디지털 저장 데이터 추출 • 디지털 증거 보존 • 디지털 증거 공증/인증	• 데이터 포맷 별 분석 • 영상 정보 분석 • 데이터베이스 정보 분석 • 데이터 마이닝
응용/네트워크	• 파일 포맷 기반 복구 • 프로그램 로그온 우회기법 • 암호 통신 내용 해독	• 네트워크 정보 수집 • 네트워크 역추적 • 데이터베이스 정보 수집 • 허니넷	• 네트워크 로그 분석 • 해쉬 데이터베이스 • 바이러스/해킹 분석 • 네트워크 시각화
기타 기술	• 개인정보보호 기술, 디지털포렌식 수사 절차 정립, 범죄 유형 프로파일링 연구, 통합 타임라인 분석 • 디지털포렌식 도구 비교 분석, 하드웨어/소프트웨어 역공학 기술, 회계부정탐지 기술		

디지털 포렌식 기술 (2)

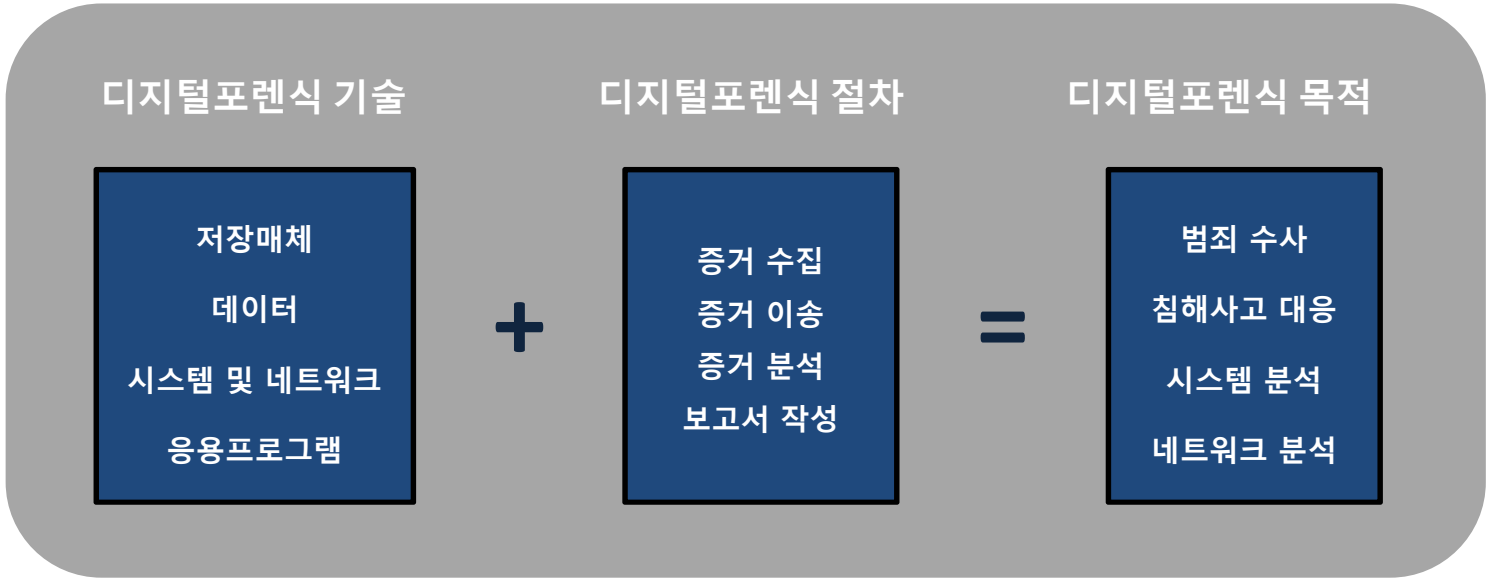

Device
• 저장매체 복구
• 저장매체 복제
• 저장매체 이미징
• … …
Data
• 데이터 검색
• 타임라인
• 파일 브라우징
• 데이터 추출
• 데이터 복구
• 데이터 마이닝
• … …
System&Network
• 네트워크 흔적
• 모니터링 및 역추적
• 활성데이터 수집 및 분석
• 시스템 파일 분석
• 데이터 수집
• 시스템 사용자 흔적 분석
• … …
Application
• 이메일 분석
• 인터넷 흔적 분석
• 정보 은닉 탐지 및 추출
• 암호 해독
• 역공학 분석
• 로그 분석
• … …

디지털 포렌식 절차

Security is a people problem…

디지털 포렌식 절차

디지털 포렌식 기술 + 절차 = 목적



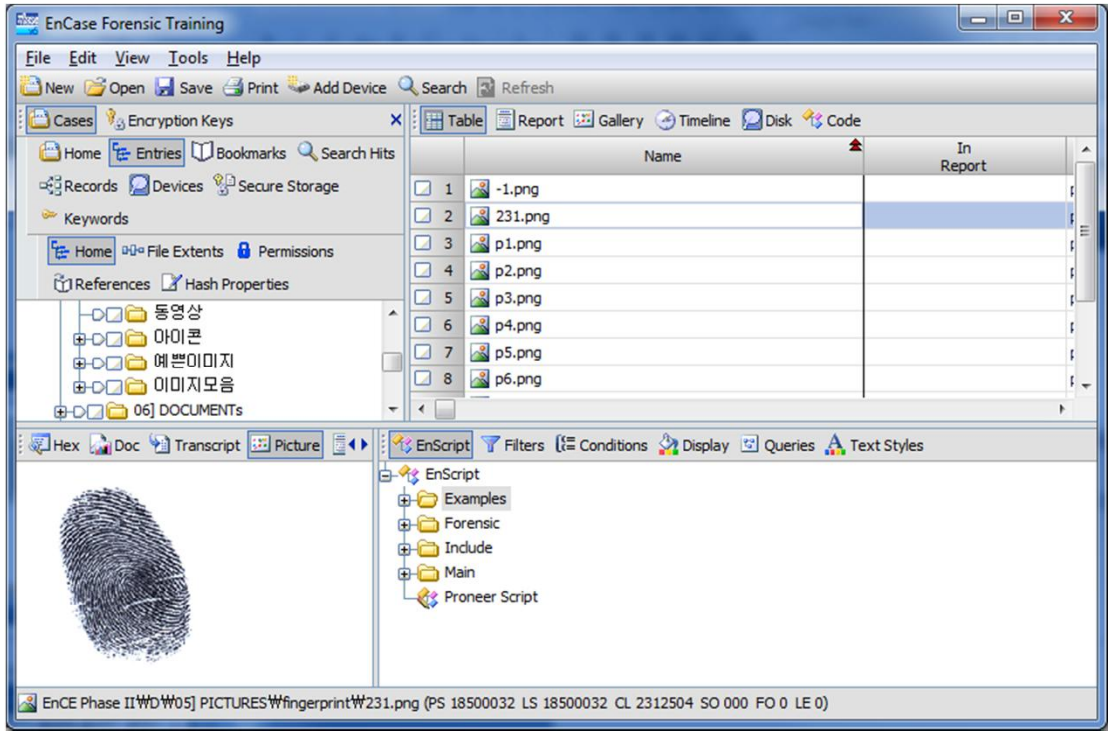
디지털 포렌식 절차

디지털 포렌식 증거 처리 절차 (6단계)

디지털 포렌식 절차

사전 준비 단계

- **디지털 포렌식 도구**
  - 디지털 포렌식 절차를 신뢰적, 효율적, 체계적으로 실시할 수 있는 독립 또는 통합 도구 준비
  - 평소에 포렌식 도구가 올바르게 동작하여, 무결성을 보장하는지 검증해야 함



디지털 포렌식 절차

사전 준비 단계

- **디지털 포렌식 도구 종류**

구 분	종 류
저장매체 쓰기 방지 도구	ICS Drive Lock, MyKey Technology, Inc. NoWrite FPU/FlashBlock II Tableau write blocker, WiebeTech write blocker, SAFE Block, FastBlock
저장매체 복제 및 이미징 도구	Data Compass, DeepSpar Disk Imager, ICS Solo3, PSIClone, Voom HardCopy III Dd, dcfldd, LinEn, dd_rescue, rdd, sdd, aimage, Adepto, FTK Imager
검색 도구	Grep, dtSearch, Text Search Plus(NTI), Afind, Hfind, Sfind
문서 및 파일 보기 도구	Conversions Plus, Quick View Plus, Thumbs Plus, WinHex, Ultra Edit, EditPlus 010Editor, FileInsight, Hex Editor Neo, FlexHex, Radare, Hiew, Hex Workshop
분석 및 복구 도구	Hash Keeper, TCT, Easy Recovery, Recovery My Files, R-Tools Final Data, Advanced Password Recovvery
통합 분석 도구	EnCase, Forensic Toolkit(FTK), Autopsy, F.I.R.E, Final Forensics X-Way Forensics

디지털 포렌식 절차

사전 준비 단계

- **디지털 포렌식 도구 검증**
  - 미 국립표준기술연구소(NIST)의 CFTT (Computer Forensics Tool Testing) - http://www.cftt.nist.gov/
  - 디지털 포렌식 도구의 검증 및 평가 방안 제시
  - 테스트 결과를 문서화하여 공개, 포렌식 도구의 객관성 강화

평가 요소	평가 결과
기능	복제, 이미징, 검증
대상 매체	BIOS to IDE, BIOS to SCSI, ATA, ASPI, Legacy BIOS, SATA, SAS
결과물의 크기	원본 = 사본, 원본 < 사본, 원본 > 사본
오류	없음, 읽기 에러, 쓰기 에러, 이미지 R/W/C
대상 형식	볼륨, 파티션
원격 접속	가능, 불가능

디지털 포렌식 절차

사전 준비 단계

- **디지털 포렌식 매뉴얼**
  - 증거 수집 및 보관에 관한 지침 – **RFC2828**
  - 디지털 증거 수집 및 획득에 대한 가이드라인 – **RFC3227**
  - 컴퓨터 포렌식 가이드라인 – **한국정보통신기술협회**
  - 휴대폰 포렌식 가이드라인 – **한국정보통신기술협회**
  - 컴퓨터 포렌식을 위한 디지털 데이터 수집 도구 요구사항 – **한국정보통신기술협회**
  - 사이버 범죄 수사 : 초동 수사를 위한 지침 – **U.S. Department of Justice**
  - 법 집행과 검시를 위한 지침 – **U.S. Department of Justice**
  - 디지털 증거의 포렌식 조사 – **U.S. Department of Justice**
  - … …

디지털 포렌식 절차

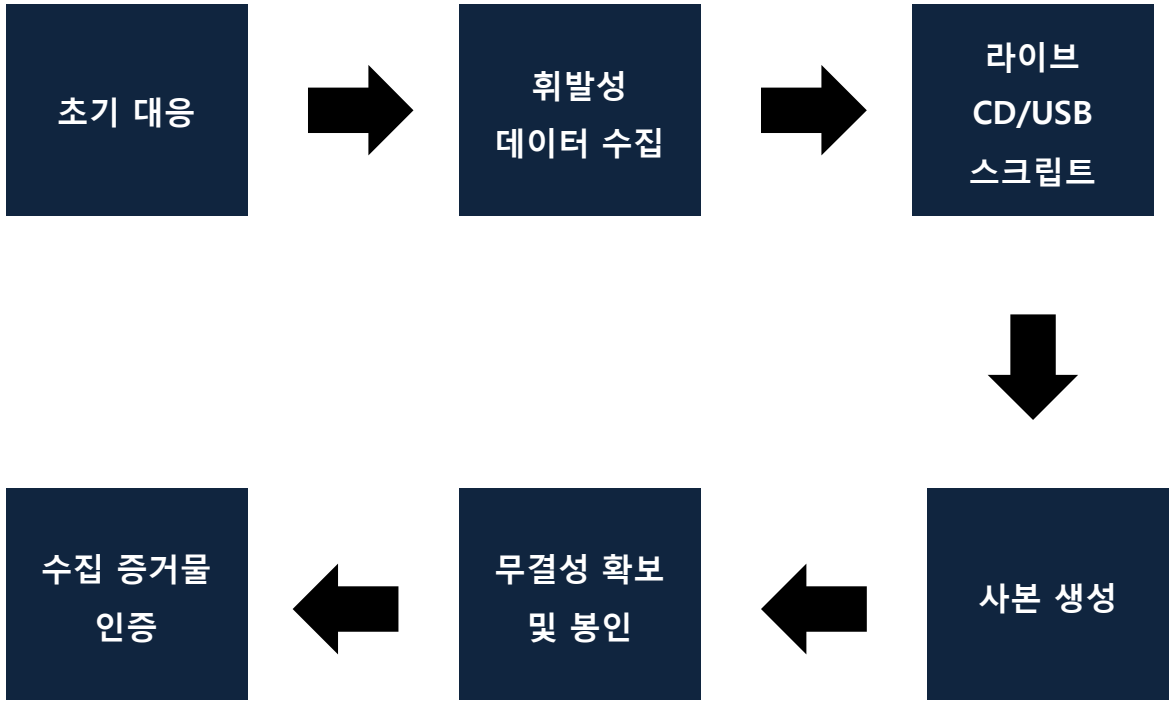
사전 준비 단계

- **저장매체 준비**
  - 증거물 수집을 위한 저장매체의 조건
    - 충분한 용량
    - 편리한 확장성
    - 무결성을 제공해야 함
  - 저장매체 완전삭제(Wiping)를 통해 기존 데이터를 완벽히 제거해야 함

디지털 포렌식 절차

사전 수집 단계

- **일반적인 디지털 증거물 획득 절차**



디지털 포렌식 절차

사전 수집 단계

- **초기 대응**
  - **현장 도착 및 보호**
    - 현장의 안전 확보, 1차 대응자는 증거 자료의 삭제/파괴 행위 방지
    - 범죄 현장 범위를 구분하고 경계선 수립 (Police Line)
  - **현장 수색 및 시스템 파악**
    - 시스템과 관련 증거에 대한 수집 목록 작성
    - 현장에 훼손되거나 사라질 가능성이 있는 증거가 있다면 카메라나 메모를 통해 현장 기록
  - **현장 정밀 수색**
    - 수색 영장이 허용하는 범위에서 모든 H/W, S/W, 메모, 로그, 저장매체 등을 수색

디지털 포렌식 절차

사전 수집 단계

- **휘발성 데이터 수집**
  - **휘발성 순서 – RFC 3227 2.1절**
  - **휘발성 정보**
    - 시스템 시간
    - 로그온 사용자
    - 열린 파일
    - 네트워크 연결 정보
    - 프로세스 정보 및 포트 맵
    - 프로세스 메모리
    - 클립보드
    - 서비스/드라이버 정보

디지털 포렌식 절차

사전 수집 단계

- **디지털 포렌식 라이브 CD/USB**
  - 휘발성 증거 수집 과정은 시스템 상태를 변경시킬 수 있으므로, 라이브 CD/USB 환경 하에서 수행
  - 라이브 CD/USB 기능
    - 활성 시스템 : 포렌식 스크립트 수행
    - 비활성 시스템 : Bootable CD에 의핸 포렌식 도구 수행
  - 수집 결과는 네트워크를 통해 서버에 전송하거나 보조 저장매체에 기록

- **디지털 포렌식 스크립트**
  - 휘발성 및 시스템 주요 데이터 수집을 위한 일련의 명령어 집합 (배치 및 쉘 스크립트)
  - 시스템 내부 도움 없이 실행될 수 있도록 정적 라이브러리 사용

디지털 포렌식 절차

사전 수집 단계

- **사본 생성**
  - 메모리 덤프
  - 저장매체 복사, 이미징, 복제
  - 생성 과정에서 오류 검출 알고리즘 사용 (CRC : Cyclic Redundancy Check)

구분	저장매체 복사	저장매체 이미징	저장매체 복제
저장 방식	원본 읽기 / 사본 쓰기	비트 스트림 이미징	비트 스트림 복제
저장 대상	파일과 디렉터리 단위의 정보	원본의 모든 물리적 섹터	원본의 모든 물리적 섹터
데이터 손실	정보 손실 발생	원본의 모든 정보 포함	원본의 모든 정보 포함
파일 복구	삭제된 파일이 제외되어 복구 불가	삭제된 파일 복구 가능	삭제된 파일 복구 가능

디지털 포렌식 절차

사전 수집 단계

- **무결성 확보**
  - 해쉬 알고리즘 사용 (MD5, SHA1 등)
- **봉인**
  - 증거물 이동 과정에서 절차연속성을 보장하기 위해 봉인

디지털 포렌식 절차

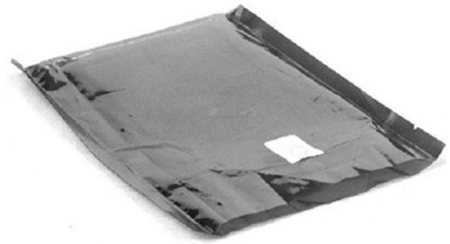
사전 수집 단계

- **수집된 증거물에 대한 인증 (현장에서)**
  - 용의자의 서명
  - 제 3자의 서명
  - 증거 수집 과정 촬영 및 녹화

디지털 포렌식 절차

증거 포장 및 이송 단계

- **전자기(EMP) 폭탄 방지**
  - 순간적으로 매우 강한 전자기파 발생 ➔ 전자기기 및 저장매체 파괴
  - 일반 폭탄과 달리 무소음 폭발이 가능하여 사용의 은밀성 제공
  - 이송 중인 디지털 증거물에 전자기 폭탄 사용시 증거물 무력화 가능성



Antistatic Bag

- **증거물 포장**
  - 충격 방지 랩, 정전기 방지용 팩, 하드케이스 등을 사용하여 포장
  - 접근 통제가 가능한 공간에 보관

디지털 포렌식 절차

증거 포장 및 이송 단계

- **연계 보관**
  - 증거 담당자 목록 : 현장에서 법정에 제출될 때까지 거쳐간 경로, 담당자, 장소, 시간 기록
  - 증거의 무결성 증명을 위해 담당자 목록 유지
  - 디지털 증거의 특성 상 인수 인계 과정에서 상호 증거를 확인하는 절차 필요

Maine Dept. of Inland Fisheries & Wildlife
Warden Service

CHAIN OF CUSTODY RECORD

CASE NO.

DATE AND TIME OF SEIZURE:	DISTRICT:	EVIDENCE/PROPERTY SEIZED BY:

SOURCE OF EVIDENCE/PROPERTY (person and/or location):
- ❑ TAKEN FROM:
- ❑ RECEIVED FROM:
- ❑ FOUND AT:

CASE TITLE AND REMARKS:

ITEM NO.	DESCRIPTION OF EVIDENCE/PROPERTY (include Seizure Tag Numbers and any serial numbers):

ITEM NO.	FROM: (PRINT NAME, AGENCY)	RELEASE SIGNATURE:	RELEASE DATE	DELIVERED VIA: ❑ U.S. MAIL ❑ IN PERSON ❑ OTHER:
	TO: (PRINT NAME, AGENCY)	RECEIPT SIGNATURE:	RECEIPT DATE	

❑ ADDITIONAL TRANSFERS ON REVERSE SIDE

디지털 포렌식 절차

증거 포장 및 이송 단계

- **이송**
  - 이송 과정에서 증거물 훼손을 방지
  - 안전한 이송을 위한 포렌식 차량 사용

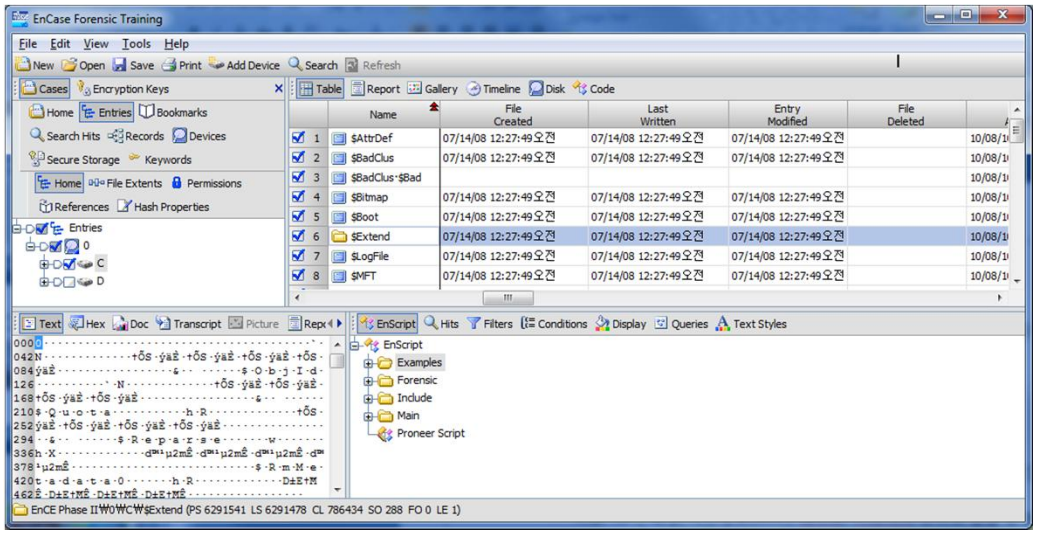
디지털 포렌식 절차

조사 분석 단계

디지털 포렌식 절차

조사 분석 단계

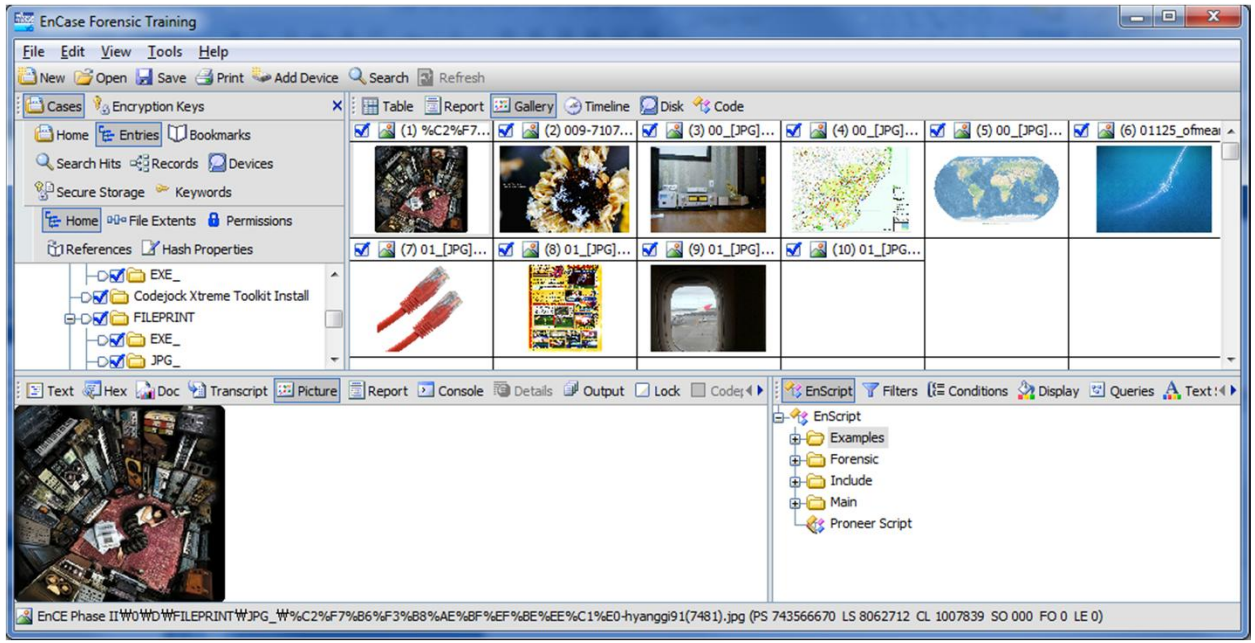
- **데이터 브라우징 (Browsing)**
  - 획득한 저장매체 내부의 정보를 가독성 있는 형태로 변환하여 출력 (윈도우 탐색기, ls/dir 명령어 등)
  - 포렌식 관점의 브라우징
    - 기억장치의 이진 데이터를 폴더/파일 단위로 출력
    - 저장매체 또는 이미지에 존재하는 파일들을 CLI/GUI 환경에서 쉽게 다룰 수 있어야 함
    - 이름, 크기, 속성, 시간정보(MAC), 해쉬(hash)값, 시그니처(signature) 등으로 정렬 및 분류



디지털 포렌식 절차

조사 분석 단계

- **데이터 뷰잉 (Data Viewing)**
  - 최근 개인용 저장매체가 1TB를 넘어감에 따라 저장매체에 수많은 파일이 존재
  - 포렌식 조사 분석 과정에서 일일이 파일을 확인하기 어려우므로 자동으로 이미지, 텍스트, HEX 형식으로 볼 수 있는 기능이 필요



디지털 포렌식 절차

조사 분석 단계

- **데이터 복구 (Data Recovery)**
  - 파일이 삭제되어도 실제로 해당 데이터가 사라지는 것은 아님
  - FAT 12/15/32, exFAT, NTFS, ext2/3 등 대부분의 파일시스템에서 삭제된 파일 복구 가능
  - 삭제된 후 덮어써졌다면 파일 카빙 기법을 이용해 복구

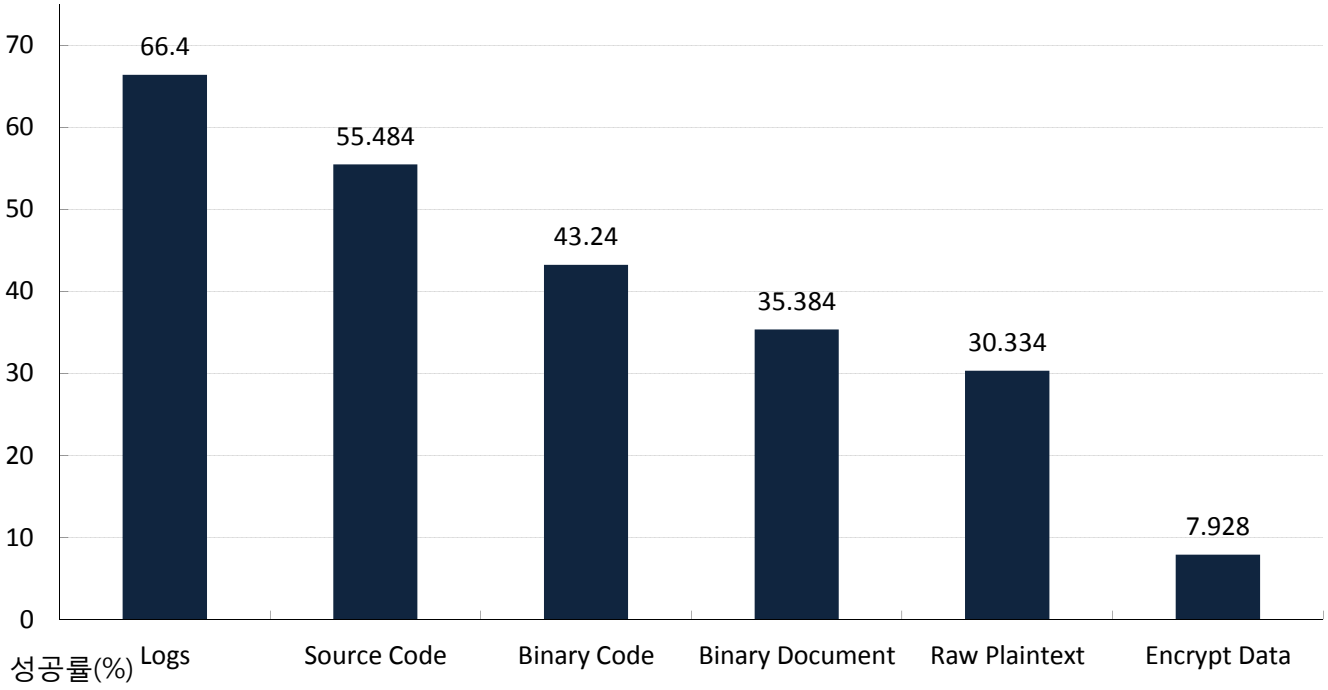
디지털 포렌식 절차

조사 분석 단계

- **수리 및 복원 (Repair)**
  - 하드웨어가 손상된 저장매체 수리
  - 파일시스템이 손상된 경우에도 파일시스템 수리(복구)

조사 분석 단계

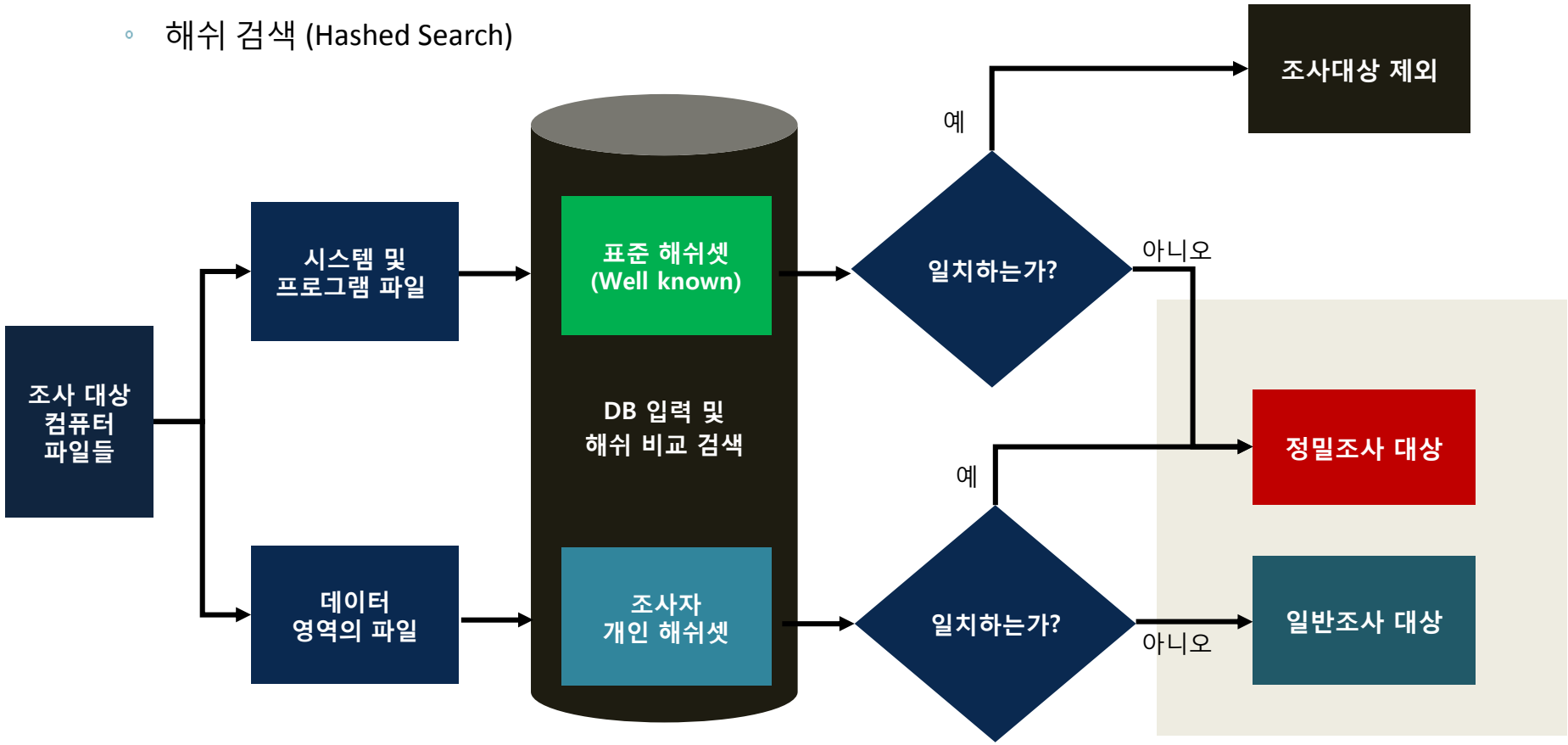
- **수리 및 복원 (Repair)**
  - 파일이 손상된 경우에도 조각난 파일 부분을 맞추거나 정렬하여 복원



디지털 포렌식 절차

조사 분석 단계

- **검색 (Searching)**
  - 해쉬 검색 (Hashed Search)

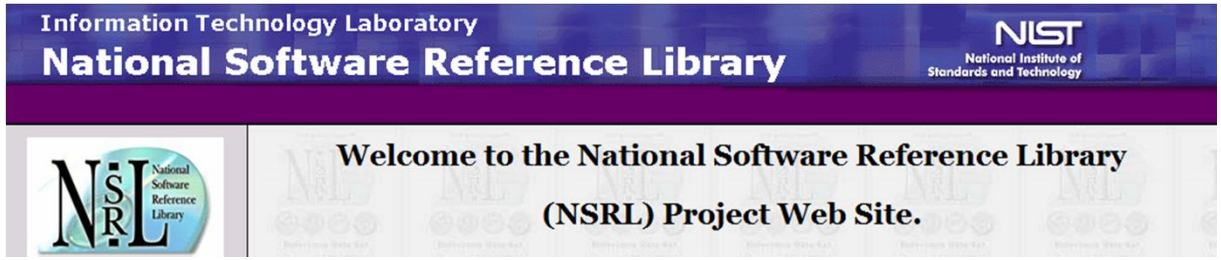


정상 파일의 해쉬셋 vs 악의적인 파일의 해쉬셋

디지털 포렌식 절차

조사 분석 단계

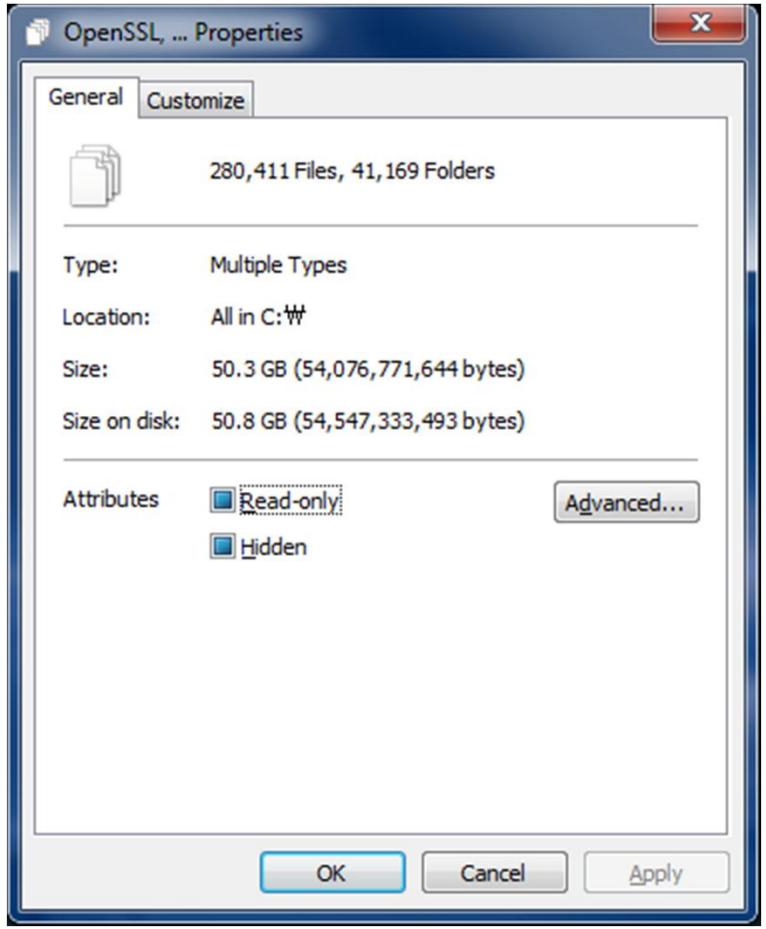
- **검색 (Searching) - http://www.nsrl.nist.gov/**
  - NSRL (National Software Reference Library)
    - 미국 국립표준기술연구소(NIST)에서 제공하는 국가 표준 참조 데이터
    - 범죄에 사용되는 파일의 식별 자동화하여 효율적인 조사를 지원
    - U.S. Department of Justice's NIJ (National Institute of Justice)의 지원을 받음
    - 수년간 각종 S/W 및 알려진 파일 수집, 각 파일의 해쉬값 데이터베이스화
    - 전세계 10,000 여개 소프트웨어,
    - 35개국 언어 운영체제 참조 데이터 셋 RDS(Reference Data Set) 구축



디지털 포렌식 절차

조사 분석 단계

- **검색 (Searching)**
  - 파일 및 문자열 검색
    - 지속적인 검색 작업을 위해 전문 검색 도구를 사용
    - Hurricane Search /WinGREP
    - dtSearch



디지털 포렌식 절차

조사 분석 단계

- **탐색 (Finding)**
  - 정보 은닉
    - 용의자의 은닉 정보를 식별하고 내용을 확인할 수 있는 기술
    - 스테가노그래피 탐색
    - 슬랙(slack) 공간 탐색 (램슬랙, 파일슬랙, 볼륨슬랙, 파일시스템슬랙 등)
    - NTFS ADS (Alternated Data Stream) 탐색
    - HPA(Host Protected Area), DCO(Device Configuration Overlay) 탐색

디지털 포렌식 절차

조사 분석 단계

- **암호 해독 및 패스워드 크랙 (Decryption)**
  - 용의자는 자신에게 불리한 증언을 하지 않을 권리가 있으므로, 암호화된 파일의 키/패스워드를 증언하지 않을 권리가 있음
  - 디지털 증거 분석 단계에서 해당 파일을 복호화하거나 크랙하여 데이터를 확인할 필요가 있음
  - TDES, ASE, RSA 등의 관용 암호를 사용하고 일정 길이 이상의 키를 사용한 경우 경우 전수 조사를 통해 키를 알아내는 것은 불가능
  - 하지만, 사회공학적 방법, 사전공격 등을 통하여 패스워드를 얻어낼 가능성이 높음

디지털 포렌식 절차

조사 분석 단계

- **암호 해독 및 패스워드 크랙 (Decryption)**
  - 상용 및 무료 소프트웨어를 이용한 복호화 (CPU)
    - ElcomSoft : Advanced Office Password Recovery, Phone Password breaker, …
    - Rixler Software : Office Password Recovery, Internet Password Recovery, Windows Password…
    - Passware : Windows Key, Passware Kit
  - GPGPU를 활용한 패스워드 복호화
  - 대규모 클러스터링 및 분산 시스템을 이용하여 패스워드 복호화
  - 검색용 데이터베이스를 이용한 복호화
    - TMTO (Time/Memory Trade Off)
    - 한국형 패스워드 사전

디지털 포렌식 절차

조사 분석 단계

- **데이터 분석 (Data Analysis)**
  - 시그니처 분석
  - 로그 및 히스토리 분석
  - 레지스트리 분석
  - 타임라인 분석
  - 역공학 분석

디지털 포렌식 절차

정밀 검토 단계

- 분석 결과는 법정에 증거로 사용될 수 있으므로 보고서 제출 전 정밀 검토가 필요
- 사본을 대상으로 동일한 과정을 반복하여 결과와 일치하는지 확인
- 무결성을 입증하기 위한 해쉬값 비교 검증

디지털 포렌식 절차

보고서 작성 단계

- 증거물 획득, 보관, 이송, 분석 등의 과정을 6하 원칙에 따라 명백하고 객관성 있게 기술
- 예상치 못한 사고 발생 시, 관련 내용 및 담당자 목록을 명확히 기재하고 범죄 혐의의 입증에 무리가 없는지 논리적으로 설득할 수 있어야 함
- 보고서의 대상이 되는 법관, 배심원, 변호사 등은 비전문가이므로 누구나 알기 쉬운 형태로 작성
- 법정에서 전문가 증언을 할 경우 사전에 비전문가를 대상으로 논리의 타당성이 있는지 연습이 필요

질문 및 답변