디지털 포렌식 개요

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 디지털 포렌식 소개
2. 디지털 포렌식 기술
3. 디지털 포렌식 절차
4. 디지털 포렌식 법률

디지털 포렌식 소개

Security is a people problem…

디지털 포렌식 소개

포렌식 vs 디지털 포렌식

디지털 포렌식 소개

아날로그 증거

디지털 포렌식 소개

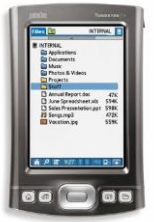
디지털 증거












디지털 포렌식 정의 cont'd

- **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'.

- **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.

디지털 포렌식 소개

디지털 포렌식 정의

- **디지털 포렌식 (컴퓨터포렌식, 사이버포렌식)**
  - 디지털 기기를 매개체로 하여 발생한 특정 행위의 사실 관계를 법정에서(?) 규명하고 증명하기 위한 절차와 방법

- **과학 수사**
  - 사건의 정확한 진상 규명을 위해 현대적 기술·시설 ·장비와 과학적 기술 ·지식을 활용하는 수사
  - 원래 포렌식(법의학)을 기반으로 했지만 최근에는 디지털 포렌식까지 영역 확장

디지털 포렌식 역사 cont'd

- **도입기** – (1970년대 후반 ~ 1980년대 초반)
  - 미국을 중심으로 컴퓨터 관련 범죄가 법으로 만들어짐
  - 저작권, 개인정보보호, 사이버 스토킹, 아동 포르노 등을 대처하기 위해 관련 법안 통과

- **성장기** – (1980년대 ~ 1990년대)
  - 법 집행 기관을 중심으로 디지털 포렌식 관련 기관 설립
  - 서로 간의 커뮤니티를 위해 관련 기구를 조직하거나 심포지엄 개최

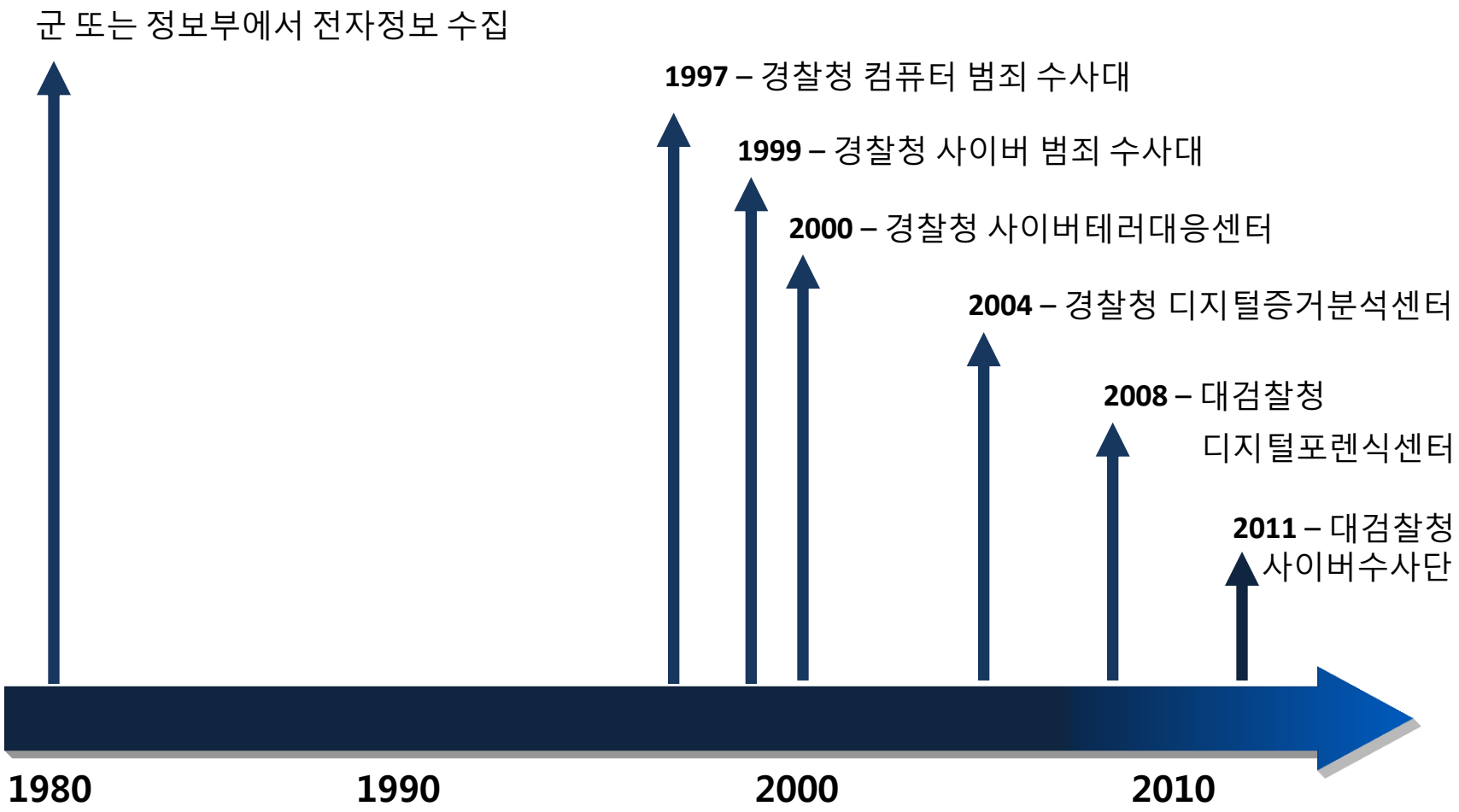
- **표준기** – (2000년대 ~ 2010년대)
  - 국가별로 디지털 포렌식 표준 수립
  - 국가기관을 중심으로 디지털 포렌식 정책, 기술 연구

디지털 포렌식 역사

- **암흑기** – (2010년대 ~ 현재)
  - 클라우드 기술을 이용하여 증거 수집의 어려움
  - 빅데이터로 분석의 어려움
  - 분석 대상 디지털 기기가 매우 다양함
  - 안티포렌식 기법의 증가
  - 고급 은닉 기법의 증가
  - 관련 법제도로 인해 적용 범위가 제한됨

디지털 포렌식 소개

국내 디지털 수사기관의 변천



디지털 포렌식 소개

디지털 증거 정의

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

- **디지털 증거**
  - **디지털 포렌식 절차**에 맞게 수집된 디지털 데이터(저장매체에 저장, 네트워크 전송)로 법정에서 증거능력을 갖는 디지털 데이터
    - ✓ **전자증거** (Electronic Evidence)
    - ✓ **전자정보** (ESI; Electronically Stored Information)

디지털 포렌식 소개

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 데이터 특성을 보완할 수 있는 절차와 방법 ➔ **디지털 포렌식**

디지털 포렌식 적용 분야 cont'd

- **수사 분야**
  - **사이버 및 지능 범죄**
    - ✓ 해킹, 바이러스 및 악성 코드 피해 조사, 사이버 테러, 정보 은닉, 암호화
  - **일반 및 강력 범죄**
    - ✓ 공갈, 사기, 위조, 협박, 횡령, 배임, 명예훼손 등의 일반 범죄
    - ✓ 회계부정, 세금포탈, 기업 비밀 유출
    - ✓ 살인, 강도, 강간, 폭행 등의 강력 범죄

디지털 포렌식 적용 분야

- **디지털 포렌식 응용 분야**
  - 침해사고 대응
  - 민사소송 대응
  - 이디스커버리
  - 포렌식 증거 분석
  - 포렌식 회계 감사
  - 포렌식 컨설팅
  - 내부 감사

디지털 포렌식 소개

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, 블랙박스
- 네트워크 장비(라우터, 스위치 등)
- 디지털 증거가 남을 수 있는 모든 디지털 장치

디지털 포렌식 소개

디지털 포렌식 유형

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

디지털 포렌식 소개

디지털 포렌식 유형

- **모바일/임베디드 포렌식**
  - 휴대폰, 스마트폰, PDA, 네비게이션, 라우터 등의 모바일 기기를 대상으로 증거 획득 및 분석
- **멀티미디어 포렌식**
  - 디지털 비디오, 오디오, 이미지 등의 멀티미디어 데이터에서 증거 획득 및 분석
- **소스코드 포렌식**
  - 프로그램 실행 코드와 소스 코드의 상관관계 분석, 악성코드 분석
- **데이터베이스 포렌식**
  - 방대한 데이터베이스로부터 유효한 증거 획득 및 분석
- **안티포렌식, 안티안티포렌식**
  - 데이터 완전 삭제, 암호화, 스테가노그래피

디지털 포렌식 소개

디지털 포렌식 국내 산업 현황

디지털 포렌식 국내 산업 현황 – 수사기관

- **검찰**
  - **대검찰청 디지털 포렌식 센터(DFC, Digital Forensic Center) ,** 약 100여명
    - ✓ 사이버범죄수사단
    - ✓ 디지털수사담당관실 – 디스크 분석팀, DB 분석팀, 모바일 분석팀, 통화/계좌 분석팀, 사이버팀, 교육연구팀
    - ✓ 과학수사담당관실
    - ✓ DNA 담당관실
  - **대전/대구/부산/광주고등검찰청, 서울 중앙/인천/수원지방검찰청,** 각 3~4명
    - ✓ 디지털포렌식 수사팀

디지털 포렌식 국내 산업 현황 – 수사기관

- **경찰**
  - **경찰청 사이버안전국(Cyber Bureau),** 약 120여명
    - ✓ 사이버안전과, 사이버범죄대응과, 디지털포렌식센터
  - **지방경찰청,** 약 1,000 여명 (경찰서 포함)
    - ✓ 사이버수사대, 사이버수사팀
  - **해양경찰청**
    - ✓ 과학수사팀

디지털 포렌식 국내 산업 현황 – 수사기관

- **국방부**
  - **국방부조사본부**
    - ✓ 수사단 내 사이버범죄수사대
  - **기무사령부**
    - ✓ 군사보안, 군 방첩, 군 관련 첩보 수집, 특정범죄 수사, 매년 국방해킹방어대회 개최
  - **헌병 수사기관**
    - ✓ 육군 중앙수사대, 해군 헌병단, 공군 헌병단
  - **군 검찰**
    - ✓ 육군/해군/공군 고등검찰부 디지털 포렌식팀
  - **국군사이버사령부**
    - ✓ 군사망 침해사고 예방, 조사, 대응 업무

디지털 포렌식 국내 산업 현황 – 수사기관

- **국가정보원**
  - **국가사이버안전센터**
    - ✓ 국가사이버안전 정책 총괄
    - ✓ 사이버위치 예방활동
    - ✓ 사이버공격 탐지활동
    - ✓ 사고조사 및 복구지원

디지털 포렌식 소개

디지털 포렌식 국내 산업 현황 – 준수사기관 (특별사법경찰관)

- 국세청
- 관세청
- 금융감독원
- 공정거래위원회
- 저작권위원회
- 방송통신위원회
- 선거관리위원회
- 한국마사회
- 식약청

디지털 포렌식 국내 산업 현황 – 법률, 회계 관련

- **회계관련**
  - **4대 회계법인 중심**
    - ✓ 안진 딜로이트, 삼일 PwC, 삼정 KPMG, 언스트앤영 한영

- **법률관련**
  - **대형로펌**
    - ✓ 김앤장, 율촌, 태평양, 세종, 화우
  - **IT 전문로펌**
    - ✓ 행복마루, 테크앤로, 민후, 평강

디지털 포렌식 국내 산업 현황 – 이디스커버리

- **이디스커버리 절차 지원**
  - 4대 회계법인
  - 유빅 (UBIC), 콜랩스리걸 (Kollabs Legal), 카탈리스트(Catalyst), 더존정보보호서비스

- **이디스커버리 관련 솔루션**
  - **이메일 아카이빙**
    - ✓ 시만텍 볼트(Vault), EMC 소스원(SourceOne), 다우기술 테라스(Terrace), ARTEC EMA 등
  - **리뷰 솔루션**
    - ✓ Clearwell, Guidance Software, ZyLAB, UBIC, Case Central, Nuix 등
  - **정보 저장소**

디지털 포렌식 국내 산업 현황 – 침해사고

- **KISA 인터넷침해대응센터**
  - 인터넷 침해대응 본부 – 침해사고 대응단, 침해사고 분석단

- **안랩**
  - 클라우드분석팀 – A-FIRST 파트

- **인포섹**
  - 탑서트(Top-CERT)

디지털 포렌식 소개

디지털 포렌식 국내 산업 현황 – 서비스 및 솔루션

- **장비/솔루션 리셀링**
  - 제트코, 더존정보보호서비스, 에이블시큐, 징코스테크놀로지, 유앤아이, 인섹시큐리티, 엔써클시스템즈, 쿠퍼스시스템즈, 레드아이포렌식, 벨정보
- **디지털포렌식 솔루션**
  - 더존정보보호서비스, 지엠디시스템, 파이널데이터, 포앤식스테크, 이스턴웨어, 모바일캅스
- **디지털 증거 분석**
  - 플레인비트, 더존정보보호서비스, 지엠디시스템, 레드아이포렌식, KDL컴퓨터포렌식, 비트포렌식
- **데이터 복구**
  - 명정보기술, 데이터닥터, 모바일탐정

디지털 포렌식 국내 산업 현황 – 교육

- **대학**
  - 경기대학교, 호원대학교, 광주대학교, 군산대학교, 영산대학교, 한국IT전문대학
- **대학원**
  - 고려대학교 정보보호대학원, 동국대 국제정보대학원, 순천향대 법과학대학원, 서울대 계약학과
- **민간교육기관**
  - SDS 멀티캠퍼스, 제트코, 더존정보보호서비스, 코어시큐리티, 한국정보보호교육센터, 아이제론
- **정기교육**
  - KITRI 지식정보보안양성과정, KISA 아카데미 디지털포렌식 시니어/주니어 과정, 고려대 정보보호교육지역센터 침해사고대응 및 디지털포렌식 과정

디지털 포렌식 국내 산업 현황 – 학회/협회

- **한국포렌식학회**
  - 대검찰청, 성균관대 주도로 처음 만듦
  - [디지털포렌식 전문가] 자격 운영

- **한국디지털포렌식학회**
  - 경찰청, 고려대 주도로 처음 만듦
  - [디지털포렌식 연구] 발간

- **사이버포렌식전문가협회**
  - 동국대 주도로 만듦
  - CFPA 자격 운영

디지털 포렌식 국내 산업 현황 – 보안/감사

- **기업 보안/감사팀**
  - 대기업을 중심으로 보안팀, 감사팀에서 포렌식 교육 이수, 인력 채용
  - 전문 포렌식 관련 팀 구성

디지털 포렌식 기술

Security is a people problem…

디지털 포렌식 기술

디지털 포렌식 관련 기술

	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		

기술 전망 – 표준 및 인증 방안

- **디지털포렌식 표준 마련 (NIST와 같은)**
  - 민.형사 소송에서 CoC를 보장할 수 있는 합리적인 절차 마련
  - 디지털 증거의 무결성을 인정받을 수 있는 데이터 수집, 처리, 분석 방법
- **포렌식 장비/솔루션 인증**
  - 어느 기관이 맡을 것인가? 어떤 기준으로?
- **포렌식 자격 인증**
  - (사) 한국포렌식학회 디지털포렌식전문가자격?
- **포렌식 분석 인증**
  - 국과수와 같은 모델이 필요한가?

기술 전망 – 연구 시장 마련

- **연구 발표 및 토론의 장 부족**
  - 논문/학회지?
  - 컨퍼런스/세미나?
- **이분화된 학회 운용**
  - 한국포렌식학회
  - 한국디지털포렌식학회

기술 전망 – 수집 방안

- **논리적 볼륨 & 엔터프라이즈 저장소 수집 방안**
  - RAID(0, 1, 2, 3, 4, 5, Hybrid), LVM, JBOD, Dynamic Disk
  - NAD, DAS, SAN, iSCSI
- **암호화 디스크 수집 기술**
  - SafeBoot Device Encryption, HP ProtectTools 2009, Bitlocker, PointSec, Truecrypt, GuardianEdge, Symantec Endpoint Encryption, SafeGuardEasy & PGP Whole Disk Encryption, Lenovo FDE
- **논리적 증거 (선별) 수집 방안**
  - DRM, DLP, FDE, 소극적 영장 등
- **원격 수집 방안**

기술 전망 – 분석 방안

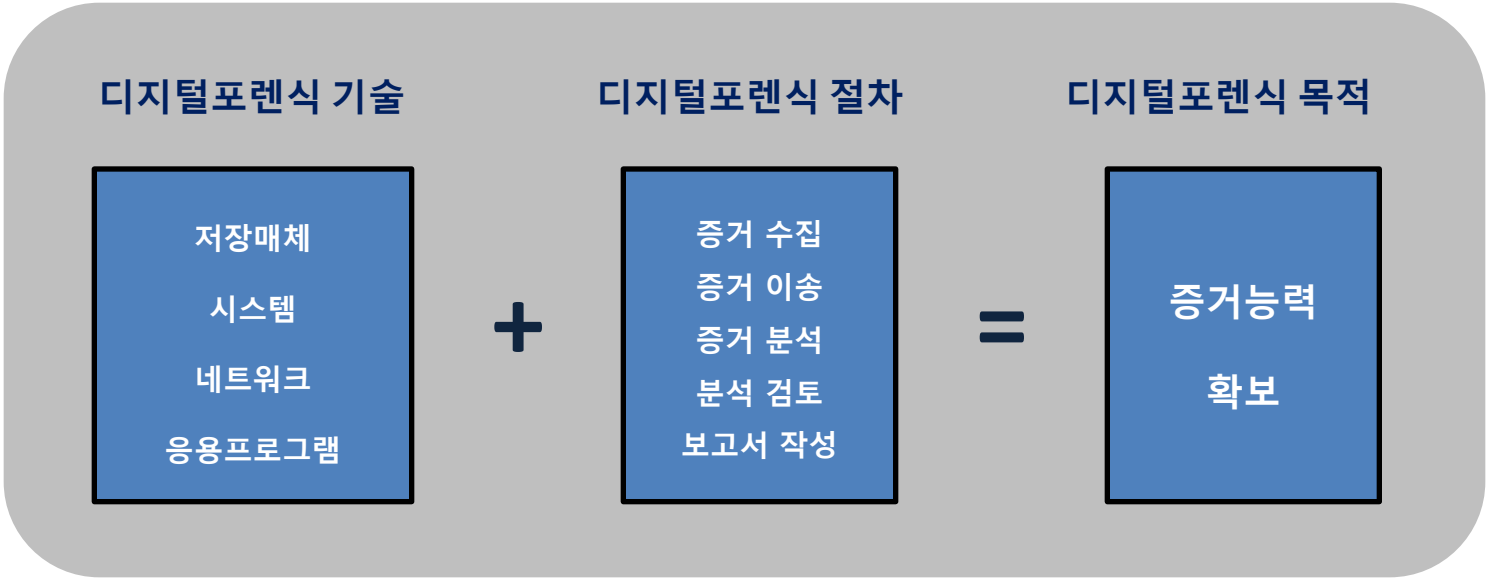
- **업무별 자동화된 프레임워크 개발**
  - 사용자 행위, 기밀 유출, 침해사고 등
- **대용량 데이터 검색, 인덱싱 방안**
- **데이터 별 다양한 시각화 연구**
- **안티안티포렌식 기법 연구**
- **가상화 포렌식 연구**
- **데이터 정규화, 마이닝 연구**
- **엔터프라이즈 포렌식 연구**
- **융합 연구 필요**
  - 자연어 처리, 신호 처리, 마이닝, 시각화 등

디지털 포렌식 절차

Security is a people problem…

디지털 포렌식 절차

디지털 포렌식 기술 + 절차 = 목적



디지털 포렌식 절차

디지털 포렌식 기본 원칙 ➔ 절차와 방법으로…

- **정당성의 원칙**
  - 증거가 적법절차에 의해 수집되었는가?
- **무결성의 원칙**
  - 증거가 수집, 이송, 분석, 제출 과정에서 위.변조 되지 않았는가?
- **연계보관성의 원칙**
  - 수집, 이동, 보관, 분석, 법정 제출의 각 단계에서 증거가 명확히 관리되었는가?
- **신속성의 원칙**
  - 디지털 포렌식의 전 과정이 신속하게 진행되었는가?
- **재현의 원칙**
  - 같은 조건과 상황하에서 항상 같은 결과가 나오는가?

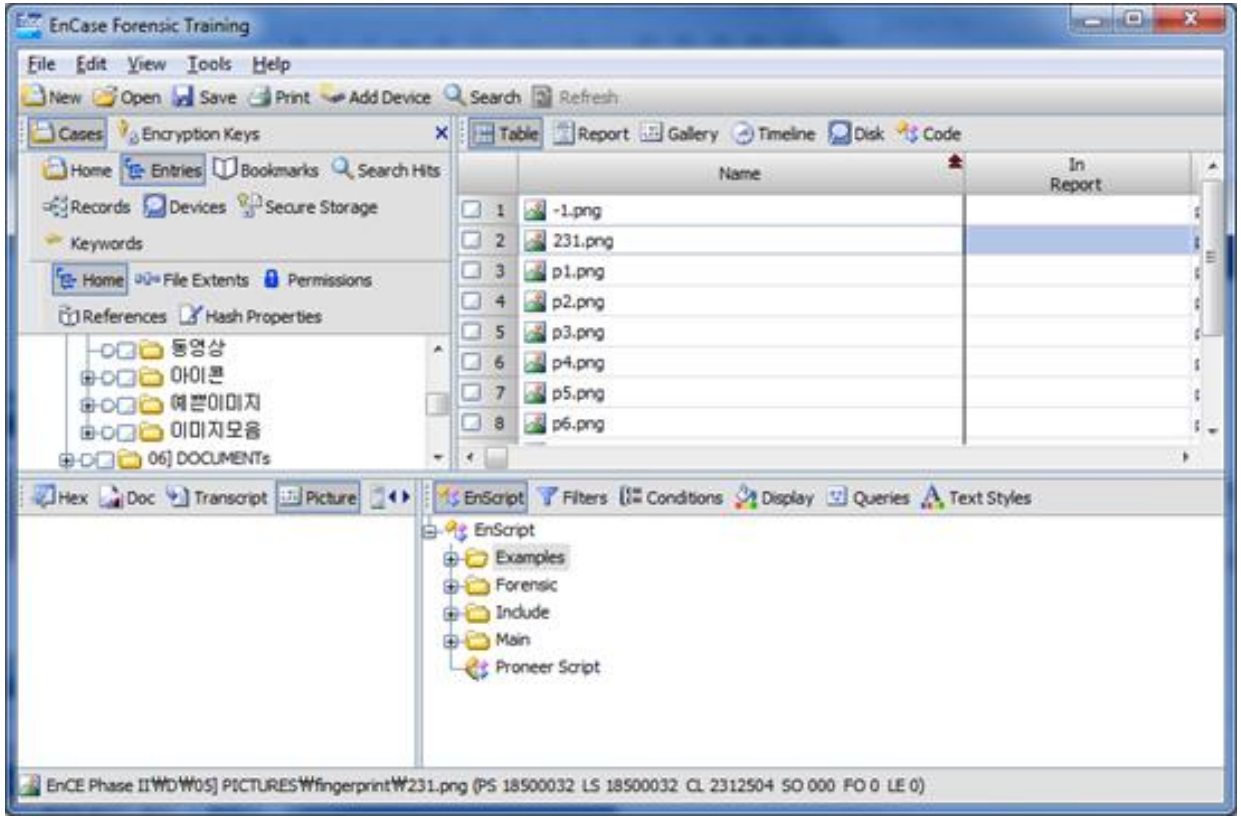
디지털 포렌식 절차

디지털 포렌식 절차 (6단계)

디지털 포렌식 절차

1단계 – 사전 준비

- **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

1단계 – 사전 준비

- **디지털 포렌식 도구**

구 분	종 류
쓰기 방지 도구	ICS Drive Lock, MyKey Technology, Inc. NoWrite FPU/FlashBlock II Tableau write blocker, WiebeTech write blocker, SAFE Block, FastBlock
복제/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/파일 도구	Conversions Plus, Quick View Plus, Thumbs Plus, WinHex, Ultra Edit, EditPlus 010Editor, FileInsight, Hex Editor Neo, FlexHex, Radare, Hiew, Hex Workshop
분석/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, log2timeline, X-Way Forensics

디지털 포렌식 절차

1단계 – 사전 준비

- **디지털 포렌식 도구 검증**
  - NIST의 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
  - 국내에서도 검증을 통한 인증 필요

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

1단계 – 사전 준비

- **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

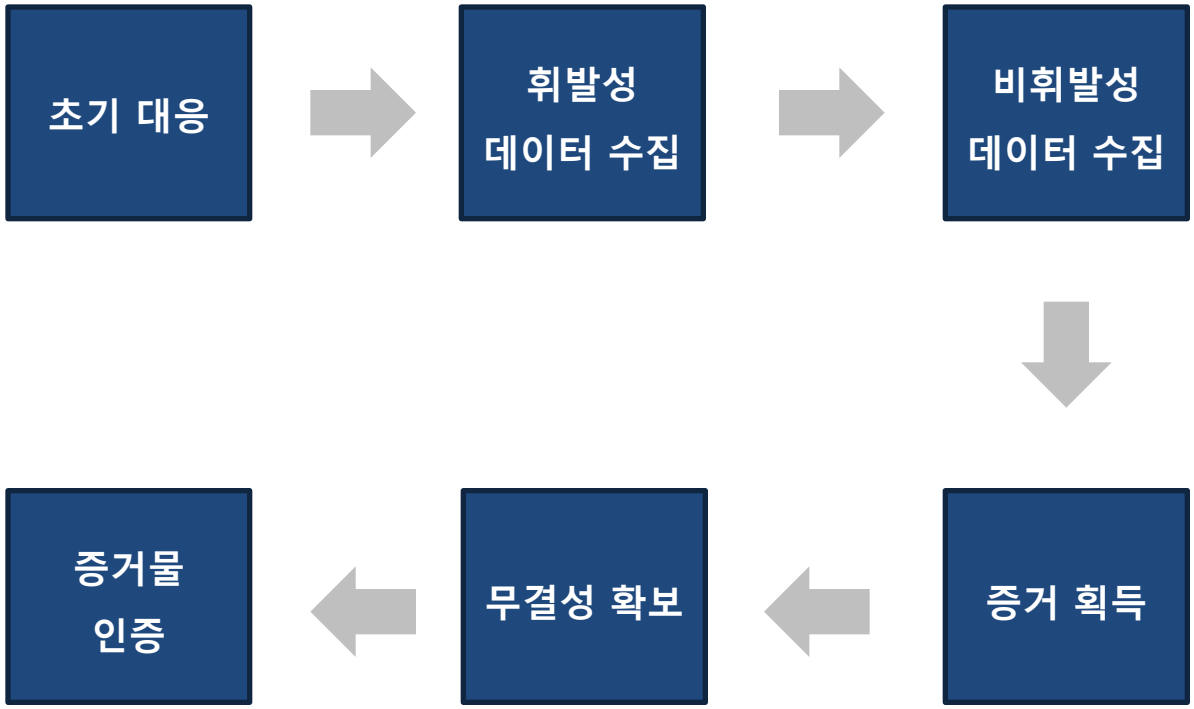
1단계 – 사전 준비

- **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

2단계 – 증거 수집

- 일반적인 디지털 증거물 획득 절차



디지털 포렌식 절차

2단계 – 증거 수집

- **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

2단계 – 증거 수집

- **휘발성 데이터 수집**

실전 포렌식	RFC 3227	NIST SP 800-86
네트워크 연결 정보	레지스터, 캐시	네트워크 연결 정보
물리메모리	라우팅 테이블, ARP 캐시	로그온 세션
프로세스 정보	프로세스 정보	**물리 메모리**
열린 파일 목록	**물리 메모리**	프로세스 정보
로그온 사용자(세션)	임시 파일 시스템	열린 파일
열린 TCP/UDP 포트 정보	디스크	네트워크 설정 경보
프로세스와 포트 맵핑	원격 로그온과 모니터링 데이터	시스템 시간
라우팅 테이블	물리적 설정, 네트워크 토폴로지	N/A
네트워크 인터페이스	기타 저장장치	N/A

- 휘발성 데이터 수집은 **커맨드라인 방식**(보통 스크립트)를 활용

디지털 포렌식 절차

2단계 – 증거 수집

- **비휘발성 데이터 수집**
  - 저장매체의 대용량화 ➔ 비휘발성 데이터 우선 수집 ➔ 전처리로 분석 시간 단축

- **비휘발성 우선 수집 대상**
  - 파일시스템 메타데이터
  - 레지스트리 하이브 파일
  - 프리패치/슈퍼패치
  - 웹 브라우저 사용흔적
  - 시스템 설정 파일
  - 다양한 시스템/응용프로그램 로그

2단계 – 증거 수집

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

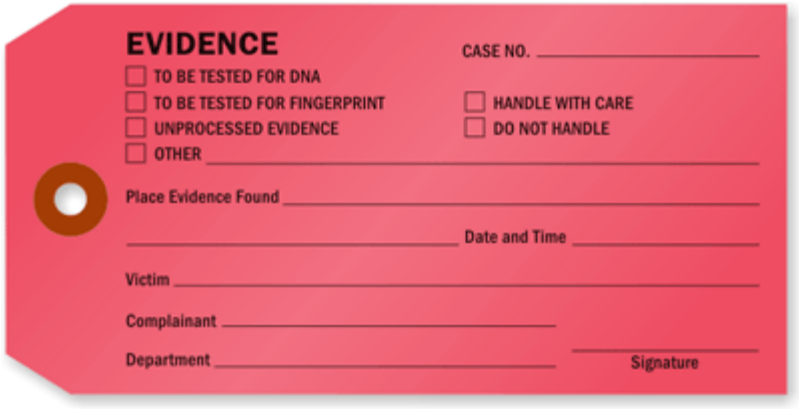
구분	저장매체 복사	저장매체 이미징	저장매체 복제
저장 방식	원본 읽기 / 사본 쓰기	비트 스트림 이미징	비트 스트림 복제
저장 대상	파일과 디렉터리 단위의 정보	원본의 모든 물리적 섹터	원본의 모든 물리적 섹터
데이터 손실	정보 손실 발생	원본의 모든 정보 포함	원본의 모든 정보 포함
파일 복구	복구 불가	삭제된 파일 복구 가능	삭제된 파일 복구 가능

디지털 포렌식 절차

2단계 – 증거 수집

- **무결성 확보**
  - 해시 알고리즘 사용 (MD5, SHA1 등)

- **봉인**
  - 증거물 이동 과정에서 연계 보관성(Chain of Custody)을 보장하기 위해 봉인



디지털 포렌식 절차

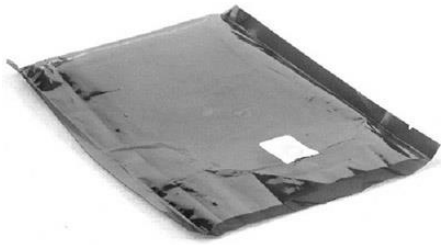
2단계 – 증거 수집

- **수집된 증거물에 대한 인증**
  - 용의자의 서명
  - 제 3자의 서명
  - 증거 수집 과정 촬영 및 녹화
  - 디지털 공증

디지털 포렌식 절차

3단계 – 증거 포장 및 이송

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



Antistatic Bag

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

3단계 – 증거 포장 및 이송

- **연계 보관**
  - 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

3단계 – 증거 포장 및 이송

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

4단계 – 조사 분석

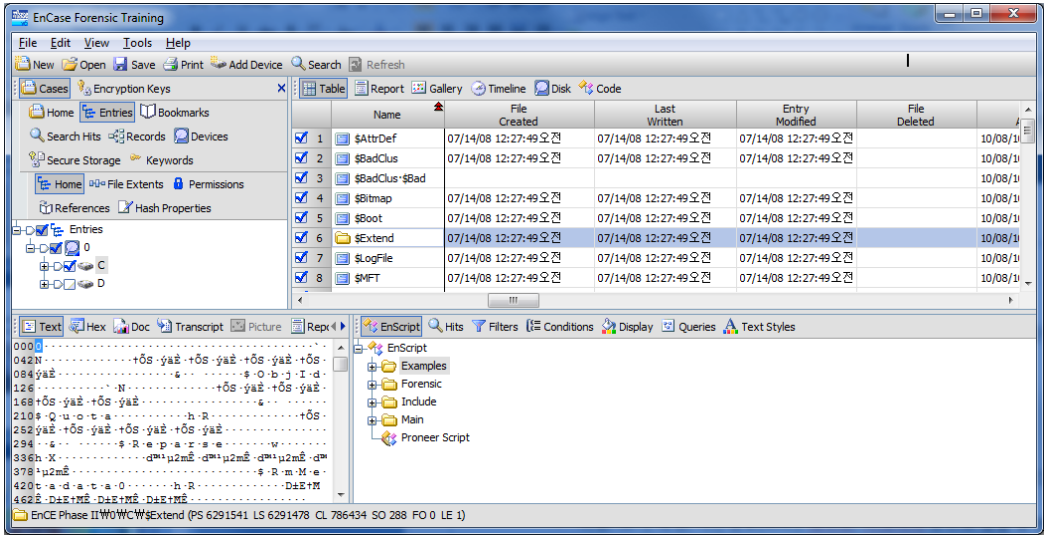
- **타임라인 분석**
  - 시간정보가 포함된 시스템 아티팩트를 대상으로 타임라인 정렬
  - 사건 발생 시간을 기준으로 전, 후 맥락 비교
  - 사건의 원인과 결과를 한눈에 확인 가능

date	time	MACB	sourcetype	desc
09/19/2012	22:39:44	M.C.	NTFS $MFT	/Windows/Inf/WmiApRpl/WmiApRpl.h
09/19/2012	22:39:48	M.C.	NTFS $MFT	**/Windows/Prefetch/WMIADAP.EXE-F8DFDFA2.pf**
09/19/2012	22:40:03	..C.	NTFS $MFT	**/$Recycle.Bin/x.exe**
09/19/2012	22:40:03	MAC.	NTFS $MFT	/Users/JK/Desktop
09/19/2012	22:40:03	MACB	NTUSER key	Key name: HKEY_USER/CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Software/Microsoft/Windows/CurrentVersion/Explorer
09/19/2012	22:40:03	MACB	NTUSER key	Key name: HKEY_USER/CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Software/Microsoft/Windows/CurrentVersion/Explorer/OperationStatusManager
09/19/2012	22:40:09	MACB	NTFS $MFT	**/Windows/Prefetch/DLLHOST.EXE-6A473D35.pf**
09/19/2012	22:40:12	..C.	NTFS $MFT	/Users/JK/AppData/Local/Microsoft/Sqm/WindowsLL
09/19/2012	22:40:12	M.C.	NTFS $MFT	/Users/JK/AppData/Local/Microsoft/Sqm/WindowsLL/WindowsLL.wns.14.sqm
09/19/2012	22:40:13	MACB	SOFTWARE k	Key name: HKLM/SoftwareCsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Wow6432Node/Microsoft/Windows/**Windows Error Reporting**
09/19/2012	22:40:13	MACB	SOFTWARE k	Key name: HKLM/SoftwareCsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Wow6432Node/Microsoft/Windows/Windows Error Reporting/Debug
09/19/2012	22:40:13	M.C.	NTFS $MFT	/Windows/System32/LogFiles/Scm/1db7c2f1-876c-4f24-ad17-8428211113f9
09/19/2012	22:40:14	.A.B	NTFS $MFT	/Windows/System32/winevt/Logs/**Microsoft-Windows-WER-Diag%4Operational.evtx**
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6B90.tmp.dmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6BEE.tmp.cab (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6B70.tmp.appcompat.txt (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C02.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C14.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C15.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C13.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C27.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	**/Windows/Prefetch/X.EXE-CB615E65.pf**
09/19/2012	22:40:16	MACB	NTUSER key	Key name: HKEY_USER/CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Software/Microsoft/Windows/WindowsErrorReporting
09/19/2012	22:40:16	MAC.	NTFS $MFT	/ProgramData/Microsoft/Windows/WER/ReportArchive
09/19/2012	22:40:16	MACB	NTFS $MFT	/ProgramData/Microsoft/Windows/WER/ReportArchive/**AppCrash_x.exe_c598da784abfeeaa78a28a697595ebb2f4f7a43_cab_095c6e9a/Report.wer**
09/19/2012	22:40:16	MACB	NTFS $MFT	/ProgramData/Microsoft/Windows/WER/ReportArchive/AppCrash_x.exe_c598da784abfeeaa78a28a697595ebb2f4f7a43_cab_095c6e9a
09/19/2012	22:40:16	MACB	NTFS $MFT	**/Windows/Prefetch/WERFAULT.EXE-37549B7E.pf**
09/19/2012	22:40:16	MAC.	NTFS $MFT	/Windows/Prefetch
09/19/2012	22:40:16	MAC.	NTFS $MFT	/Users/JK/AppData/Local/Temp
09/19/2012	22:40:23	M.C.	NTFS $MFT	**/Windows/Prefetch/SVCHOST.EXE-80F4A784.pf**
09/19/2012	22:40:41	M.C.	NTFS $MFT	/Windows/System32/wbem/Repository/OBJECT~1.DAT
09/19/2012	22:40:41	M.C.	NTFS $MFT	/Windows/System32/wbem/Repository/INDEX.BTR

디지털 포렌식 절차

4단계 – 조사 분석

- **데이터 브라우징**
  - 획득한 저장매체 내부의 정보를 가독성 있는 형태로 변환하여 출력
  - **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, 해시값, 시그니처 등으로 정렬이나 분류 가능



디지털 포렌식 절차

4단계 – 조사 분석

- **데이터 복구**
  - 기본적인 파일 삭제는 메타 정보와 데이터의 링크만 사라짐
  - 대부분의 파일시스템에서 삭제된 파일 복구 가능
  - 삭제 후 덮어써졌다면 파일 카빙 기법을 이용해 복구
  - **파일 카빙 기법**
    - ✓ 시그니처 카빙
    - ✓ 램 슬랙 카빙
    - ✓ 파일 크기 획득
    - ✓ 파일 구조 검증
    - ✓ 스마트 카빙 기법

디지털 포렌식 절차

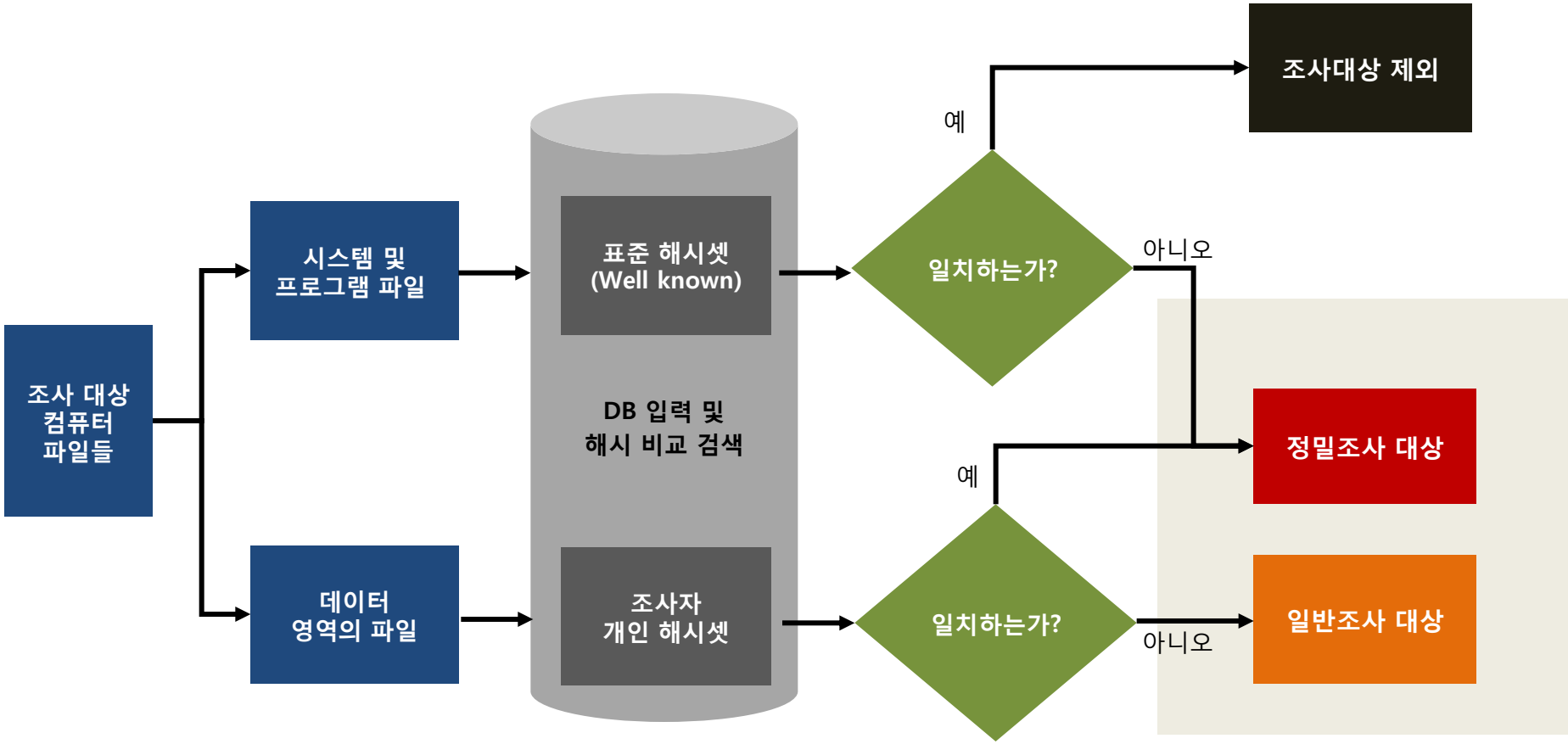
4단계 – 조사 분석

- **저장매체 수리/복원**
  - 화재, 침수와 같은 자연재해로 인해 손상도 상황에 따라 복구 가능
  - 하드웨어, 파일시스템이 손상된 경우에도 상황에 따라 복구 가능
  - 손상된 저장매체를 어떻게 취급, 관리하느냐에 따라 복구율이 달라짐

디지털 포렌식 절차

4단계 – 조사 분석

- **해시 검색** – NSRL, Bit9 등의 화이트리스트 해시 사용

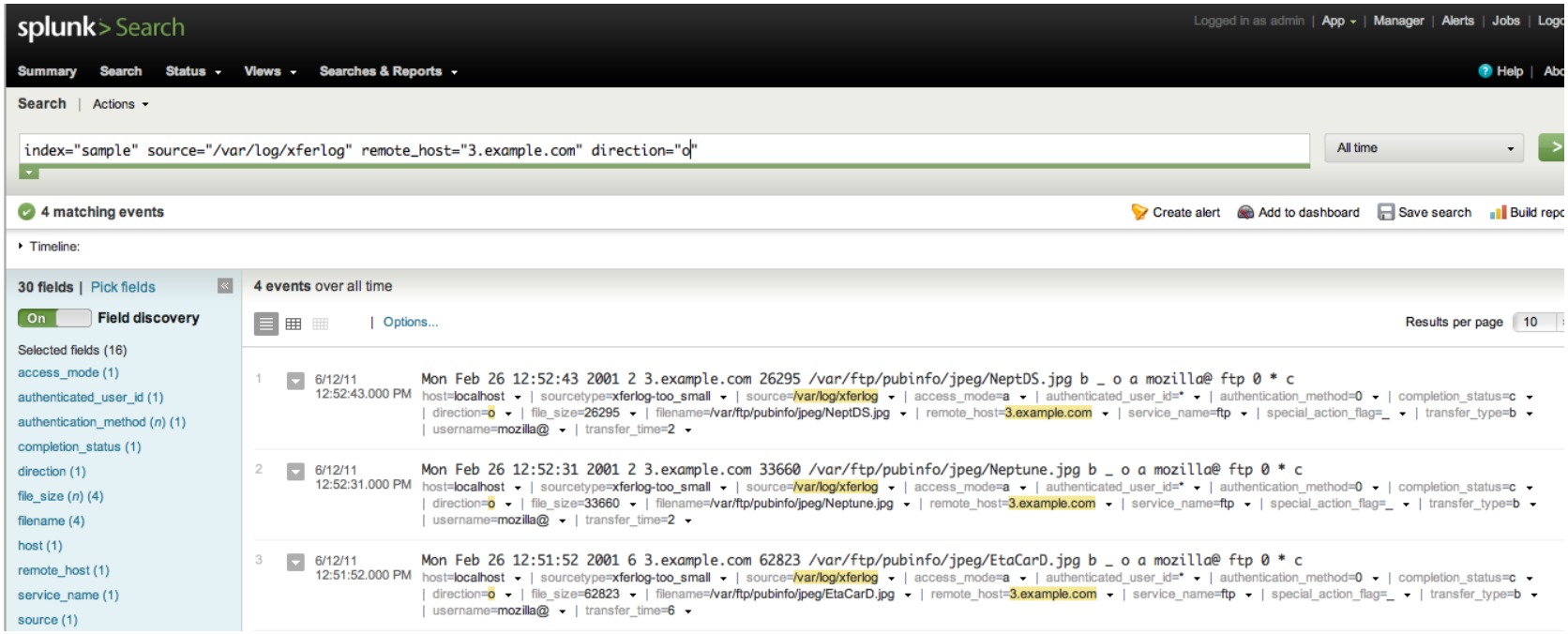


정상 파일의 해시셋 VS 악의적인 파일의 해시셋

디지털 포렌식 절차

4단계 – 조사 분석

- **파일 검색**
  - 연속 검색을 위해 인덱싱 필요
  - 통합 분석도구에서 인덱싱 지원
  - 검색 전용 도구 – Splunk



디지털 포렌식 절차

4단계 – 조사 분석

- **데이터 탐색**
  - 용의자의 은닉 정보를 식별
  - 스테가노그래피 탐색
  - 슬랙 공간 탐색 (램 슬랙, 파일 슬랙, 볼륨 슬랙, 파일시스템 슬랙 등)
  - NTFS ADS (Alternated Data Stream) 탐색
  - HPA(Host Protected Area), DCO(Device Configuration Overlay) 탐색

4단계 – 조사 분석

- **암호 복호화/패스워드 크랙**
  - 용의자는 자신에게 불리한 증언을 하지 않을 권리 ➔ 패스워드 노코멘트
  - 권고 이상의 키를 이용해 TDES, AES, RSA 등의 관용 암호를 사용할 경우 복호화 어려움
  - 하지만, 사회공학적 방법, 사전공격 등을 통하여 패스워드를 얻어낼 가능성이 높음
  - **패스워드 공격**
    - ✓ 상용 및 무료 소프트웨어를 이용한 공격
    - ✓ GPGPU를 활용한 패스워드 복호화
    - ✓ 대규모 분산 시스템을 이용하여 패스워드 복호화
    - ✓ 검색용 데이터베이스(TMTO, 한국형 패스워드 사전)를 이용한 복호화

디지털 포렌식 절차

4단계 – 조사 분석

- **그 외 다양한 데이터 분석**
  - 통합 로그 분석
  - 시스템 아티팩트 정밀 분석
  - 악성코드 역공학

디지털 포렌식 절차

5단계 – 정밀 검토

- 분석 결과는 법정에 증거로 사용될 수 있으므로 보고서 제출 전 정밀 검토가 필요
- 사본을 대상으로 동일한 과정을 반복하여 결과와 일치하는지
- 분석 내용과 사건과 논리적으로 잘 연결이 되는지

디지털 포렌식 절차

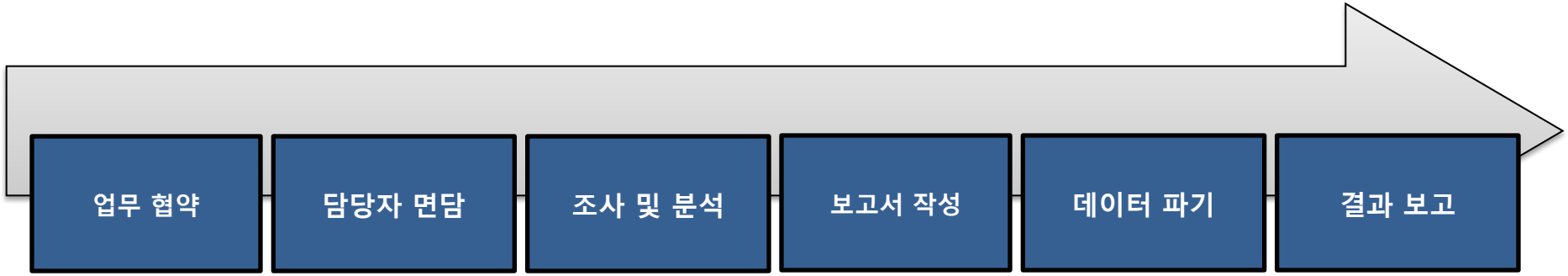
6단계 – 보고서 작성

- 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 알기 쉬운 형태로 작성
- 전문가 증언을 대비해 비전문가를 대상으로 논리의 타당성이 있는지 연습이 필요

디지털 포렌식 절차

침해사고 대응 절차 (1/2)

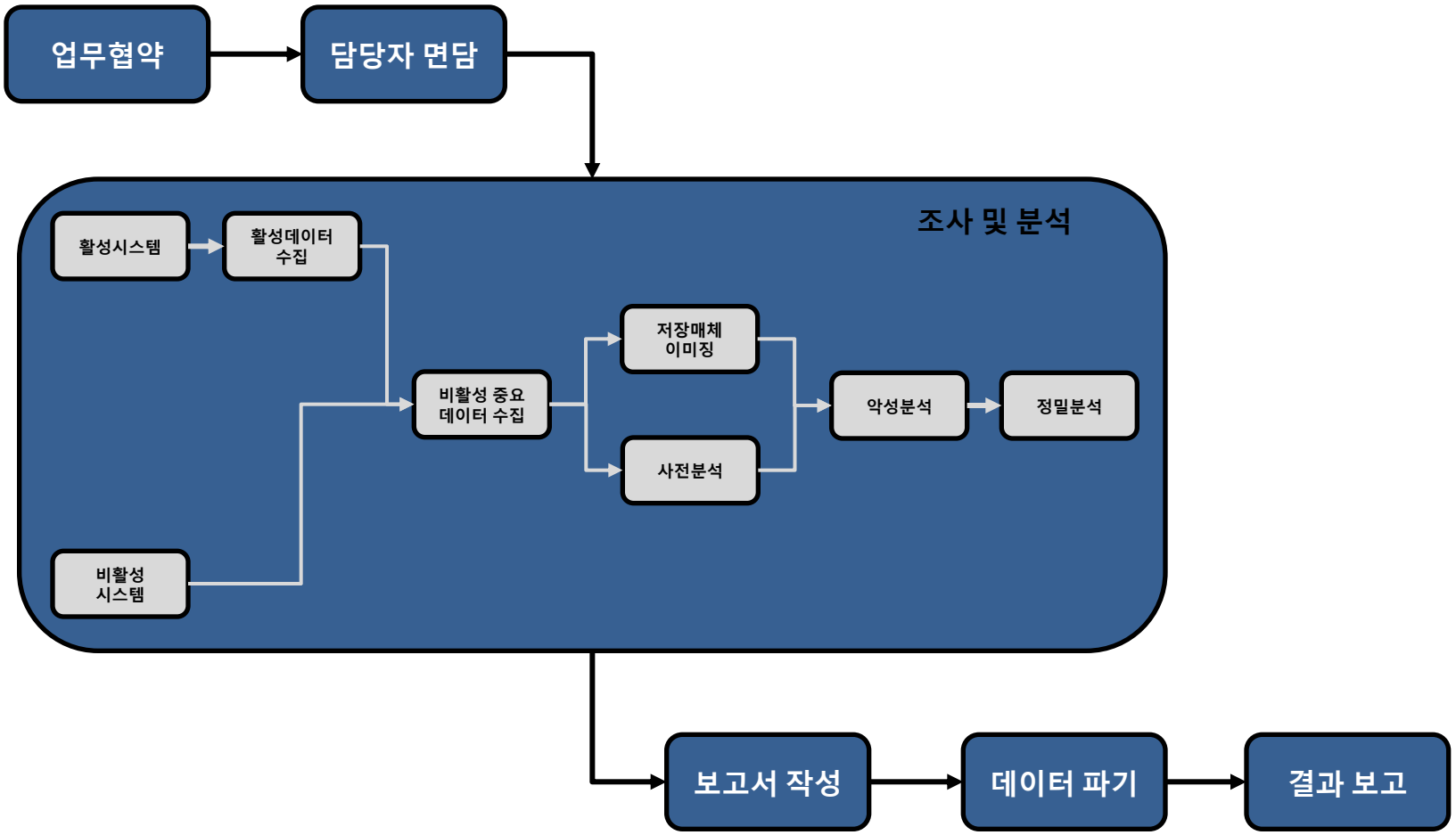
디지털포렌식 절차



침해사고 대응 절차

디지털 포렌식 절차

침해사고 대응 절차 (2/2)



디지털 포렌식 법률

Security is a people problem…

디지털 증거의 특성

- **증거능력 (Admissibility)**
  - 증거가 엄격한 증명 자료로 사용될 수 있는 법률상의 자격
  - 미국에서는 법적 허용성(Legal Admissibility) 용어로 사용
  - 위법수집증거배제법칙, 전문법칙

- **증명력 (Weight)**
  - 증거의 실질적 가치, 신빙도 정도 ➔법관의 자유심증주의에 의해 판단

- 유효한 증거가 되기 위해서는 **증거능력**과 **증명력**이 있어야 함
- 디지털 증거의 **증거능력**과 **증명력**을 뒷받침하기 위한 과학수사 ➔ **디지털 포렌식**

증거법상 기본원칙 (형사소송법) cont'd

- 증거재판주의
- 자유심증주의
- 위법수집증거배제원칙
- 자백배제법칙
- 전문배제법칙

증거법상 기본원칙 (형사소송법) cont'd

- **증거재판주의**
  - 반드시 증거에 의해서만 사실인정을 허용한다는 원칙
  - 증거는 증거능력이 있고, 적법한 절차를 거쳐야 함

  - **형사소송법 제307조(증거재판주의)** [전문개정 2007.6.1]
    1. 사실의 인정은 증거에 의하여야 한다.
    2. 법죄사실의 인정은 합리적인 의심이 없는 정도의 증명에 이르러야 한다.

증거법상 기본원칙 (형사소송법) cont'd

- **자유심증주의**
  - 증거의 증명력을 법률로 규정하지 않고, 법관의 자유로운 판단에 맡기는 원칙

  - **형사소송법 제308조(자유심증주의)**

    1. 증거의 증명력은 법관의 자유판단에 의한다.

  - **민사소송법 제202조(자유심증주의)**

    1. 법원은 변론 전제의 취지와 증거조사의 결과를 참작하여 자유로운 심증으로 사회정의와 형평의 이념에 입각하여 논리와 경험의 법칙에 따라 사실주장이 진실한지 아닌지를 판단한다.

증거법상 기본원칙 (형사소송법) cont'd

- **자유심증주의 vs. 과학적 증거방법**
  - **대판 2007.5.10, 2007도 1950**

> 자유심증주의를 규정한 형사소송법 제308조가 증거의 증명력을 법관의 자유판단에 의하도록 한 것은 그것이 실체적 진실발견에 적합하기 때문이지 법관의 자의적인 판단을 인용한다는 것은 아니므로, 증거판단에 관한 전권을 가지고 있는 사실심 법관은 사실인정에 있어 공판절차에서 획득된 인식과 조사된 증거를 남김없이 고려하여야 한다. 그리고 증거의 증명력은 법관의 자유판단에 맡겨져 있으나 그 판단은 논리와 경험법칙에 합치하여야 하고, 형사재판에 있어서 유죄로 인정하기 위한 심증형성의 정도는 합리적인 의심을 할 여지가 없을 정도여야 한다(대법원 2004. 6. 25. 선고 2004도2221 판결 등 참조). 특히, 유전자검사나 혈액형검사 등 과학적 증거방법은 그 전제로 하는 사실이 모두 진실임이 입증되고 그 추론의 방법이 과학적으로 정당하여 오류의 가능성이 전무하거나 무시할 정도로 극소한 것으로 인정되는 경우에는 법관이 사실인정을 함에 있어 상당한 정도로 구속력을 가진다 할 것이므로, 비록 사실의 인정이 사실심의 전권이라 하더라도 아무런 합리적 근거 없이 함부로 이를 배척하는 것은 자유심증주의의 한계를 벗어나는 것으로서 허용될 수 없다.

증거법상 기본원칙 (형사소송법) cont'd

▪ 위법수집증거배제원칙 (1/2)

- 위법한 절차에 의해 수집된 증거는 증거능력을 배제하는 원칙

- **기존 판례**

  ✓ 영장주의에 위반하여 압수한 증거물의 경우 압수 절차가 위법이라 하더라도 물건 자체의 성질이나 형상에 변경을 가져오는 것은 아니므로 그 형상 등에 관한 증거가치에는 변함이 없다 할 것이므로 증거능력이 인정된다. [대법원 1968.9.17. 선고 68도932판결]

증거법상 기본원칙 (형사소송법) cont'd

▪ 위법수집증거배제원칙 (2/2)

- **형사소송법 제308조의2(위법수집증거의 배제)** [2007.6.1 신설], 2008년 시행

  1. 적법한 절차를 따르지 아니하고 수집한 증거는 증거로 할 수 없다.

- **판례의 변경** [대법원 2007.11.15.선고 2007도3061 전원합의체 판결]

  ✓ 헌법과 형사소송법이 정한 절차에 따르지 아니하고 수집한 증거는 기본적 인권 보장을 위해 마련된 적법한 절차에 따르지 않은 것으로서 원칙적으로 유죄 인정의 증거로 삼을 수 없다. 수사기관의 위법한 압수수색을 억제하고 재발을 방지하는 가장 효과적이고 확실한 대응책은 이를 통하여 수집한 증거는 물론 이를 기초로 하여 획득한 2차적 증거를 유죄 인정의 증거로 삼을 수 없도록 하는 것이다. [제주지사실 압수수색사건, 공직선거법위반]

  ✓ **독수독과이론**(Fruit of the poisonous tree)

증거법상 기본원칙 (형사소송법) cont'd

▪ 자백배제법칙

- 임의성이 의심되는 자백은 증거능력을 배제하는 원칙
- 자백일지라도 그 사실이 증거의 의하지 아니하면 인정될 수 없음
- 단, 민사소송에서는 당사자의 자백에 대한 다툼이 없을 때는 증거가 필요 없음
- **형사소송법 제309조(강제등 자백의 증거능력)** [제목개정 1963.12.13]

  1. 피고인의 자백이 고문, 폭행, 협박, 신체구속의 부당한 장기화 또는 기망 기타의 방법으로 임의로 진술한 것이 아니라고 의심할만한 이유가 있는 때에는 이를 유죄의 증거로 하지 못한다.

- **형사소송법 제310조(불이익한 자백의 증거능력)**

  1. 피고인의 자백이 그 피고인에게 불이익한 유일의 증거인 때에는 이를 유죄의 증거로 하지 못한다.

- **민사소송법 제288조(불요증사실)**

  1. 법원에서 당사자가 자백한 사실과 현저한 사실은 증명을 필요로 하지 아니한다.

증거법상 기본원칙 (형사소송법) cont'd

▪ 전문배제법칙

- 전문증거는 증거능력을 배제하는 원칙
- 자백배제법칙과 함께 배심원의 합리적 심증형성을 위해 발달한 증거법칙

- **전문(hearsay)**
  - ✓ 원 진술자가 공판기일 또는 심문 기일에 행한 진술 이외의 진술
  - ✓ 사실의 진위여부를 알지 못한 상태에서 전해들은 말

- **형사소송법 제310조의2(전문증거와 증거능력의 제한)** [본조신설 1961.9.1]

  1. **제311조** 내지 **제316조**에 규정한 것 이외에는 공판준비 또는 공판 기일에서의 진술에 대신하여 진술을 기재한 서류나 공판준비 또는 공판 기일 외에서의 타인의 진술을 내용으로 하는 진술은 이를 증거로 할 수 없다.

증거법상 기본원칙 (형사소송법) cont'd

▪ 전문법칙 예외 규정 (1/3)

- **형사소송법 제311조(법원 또는 법관의 조서)**

1. 공판준비 또는 공판 기일에 피고인이나 피고인 아닌 자의 진술을 기재한 조서와 법원 또는 법관의 검증의 결과를 기재한 조서는 증거로 할 수 있다. 제184조 및 제221조의2의 규정에 의하여 작성한 조서도 또한 같다. <개정 1973.1.25, 1995.12.29> [전문개정 1961.9.1]

- **형사소송법 제314조(증거능력에 대한 예외)**

✓ 제312조 또는 제313조의 경우에 공판준비 또는 공판 기일에 진술을 요하는 자가 사망·질병·외국거주·소재불명 그 밖에 이에 준하는 사유로 인하여 진술할 수 없는 때에는 그 조서 및 그 밖의 서류를 증거로 할 수 있다. 다만, 그 진술 또는 작성이 특히 신빙할 수 있는 상태하에서 행하여졌음이 증명된 때에 한한다. [전문개정 2007.6.1]

증거법상 기본원칙 (형사소송법) cont'd

- **전문법칙 예외 규정 (2/3)**

  - **형사소송법 제315조(당연히 증거능력이 있는 서류)**

    다음에 게기한 서류는 증거로 할 수 있다. <계정 2007.5.17>

    1.가족관계기록사항에 관한 증명서, 공정증서등본 기타 공무원 또는 외국공무원의 직무상 증명할 수 있는 사항에 관하여 작성한 문서

    2.상업장부, 항해일지 기타 업무상 필요로 작성한 통상문서

    3.기타 특히 신용할 만한 정황에 의하여 작성된 문서

증거법상 기본원칙 (형사소송법) cont'd

▪ 전문법칙 예외 규정 (3/3)

- **형사소송법 제316조(전문의 진술)**

1. 피고인이 아닌 자(공소제기 전에 피고인을 피의자로 조사하였거나 그 조사에 참여하였던 자를 포함한다. 이하 이 조에서 같다)의 공판준비 또는 공판기일에서의 진술이 피고인의 진술을 그 내용으로 하는 것인 때에는 그 진술이 특히 신빙할 수 있는 상태하에서 행하여졌음이 증명된 때에 한하여 이를 증거로 할 수 있다. <개정 2007.6.1>
2. 피고인 아닌 자의 공판준비 또는 공판기일에서의 진술이 피고인 아닌 타인의 진술을 그 내용으로 하는 것인 때에는 원진술자가 사망, 질병, 외국거주, 소재불명 그 밖에 이에 준하는 사유로 인하여 진술할 수 없고, 그 진술이 특히 신빙할 수 있는 상태하에서 행하여졌음이 증명된 때에 한하여 이를 증거로 할 수 있다. <개정 1995.12.29, 2007.6.1> [전문개정 1961.9.1]

증거법상 기본원칙 (형사소송법) cont'd

- **디지털 증거에서의 전문법칙**
  - 디지털 증거는 직접적으로 사람의 지각, 기억, 표현, 서술이라는 진술과정을 거치지 않고 기계적으로 처리되어 작성된 것
  - **생성 증거(Computer Generated Evidence) ➔ 전문법칙 미적용**
    - ✓ 시스템이 자동으로 생성한 증거, 시스템 아티팩트 (로그, 레지스트리, 프리패치, 브라우저 흔적 등)
    - ✓ 디지털 증거를 식별하거나 분류하는데 도움이 되는 부가 정보 (메타데이터)
    - ✓ 파일명, 해시값, 타임스탬프 등
  - **보관 증거(Computer Stored Evidence) ➔ 전문법칙 적용**
    - ✓ 사건을 직접적으로 증명해주는증거
    - ✓ 보통 사람의 사상이나 감정을 표현하기 위해 작성한 증거 (문서, 사진, 동영상 등)
  - 저장증거가 증거가 되기 위해서는 **전문법칙의 예외 규정**에 적용이 되야 함
    - ✓ 형사소송법 제311조, 제312조, 제313조, 제314조, 제315조, 제316조

증거법상 기본원칙 (형사소송법) cont'd

- **전문법칙 예외 규정**
  - **형사소송법 제311조**
    - ✓ 공판 기간 동안 진술을 기재한 조서와 법원 또는 법관의 검증의 결과를 기재한 조서
  - **형사소송법 제312조**
    - ✓ 검사 또는 사업경찰관의 조서 등
  - **형사소송법 제313조**
    - ✓ 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때, 진술서
  - **형사소송법 제314조**
    - ✓ 사망, 질병, 외국거주, 소재불명 등으로 진술할 수 없을 때, 그 조서 및 그 밖의 서류
  - **형사소송법 제315조**
    - ✓ 가족관계기록사항에 관한 증명서, 공정증서등본 등
    - ✓ 상업장부, 항해일지 기타 업무상 필요로 작성한 통산 문서 ➔ 비즈니스 기록 (회계 장부 등)
    - ✓ 기타 특히 신용할만한 정황에 의하여 작성된 문서 ➔ 신용할만한 정황을 입증
  - **형사소송법 제316조**
    - ✓ 피고인이 아니더라도 공판 기간 동안 진술이 피고인의 진술을 그 내용으로 하는 것인 경우

디지털 데이터와 증거능력

- **디지털 데이터의 증거능력 요건**
  - **진정성 (Authenticity)**
    - ✓ 증거 데이터 수집 과정에서 오류 없이 의도된 결과가 정확히 획득됐고, 그로 인해 생성된 자료임이 입증되어야 함
  - **무결성 (Integrity)**
    - ✓ 수집에서부터 법정에 제출되기까지 증거 데이터가 훼손 없이 보호되었음이 입증되어야 함
  - **신뢰성 (Reliability)**
    - ✓ 증거 데이터의 처리 과정에서 사용된 솔루션과 분석가의 자질에 신뢰성이 입증되어야 함
  - **원본성 (Originality)**
    - ✓ 원본 매체의 데이터와 실제 법정에 제출되는 데이터의 동일함이 입증되어야 함

디지털 데이터와 영장

- **영장의 방식**

  - **형사소송법 제114조(영장의 방식)**

    1. 압수·수색영장에는 피고인의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부년월일, 유효기간과 그 기간을 경과하면 집행에 착수하지 못하며 영장을 반환하여야 한다는 취지 기타 대법원규칙으로 정한 사항을 기재하고 재판장 또는 수명법관이 서명날인하여야 한다. 다만, 압수·수색할 물건이 전기통신에 관한 것인 경우에는 작성기간을 기재하여야 한다. <개정 2011.7.18.>
    2. 제75조제2항의 규정은 전항의 영장에 준용한다.

디지털 데이터와 압수

▪ 압수•수색 절차와 대상

- 형사소송법상 압수의 대상은 "**유체물**"만 가능
- 디지털 증거는 "**무체물**"이기 때문에 압수의 대상이 되지 못함 ➔ 유체물 대상으로 압수 수행

- 2007년 10월 개정된 형사소송규칙 제134조의7, 제134조의8
  - ✓ 읽을 수 있도록 출력하여 인증한 등본 제출
  - ✓ 녹음.녹음매체 등의 녹취서, 그 밖에 그 내용을 설명하는 서면을 제출, 재생하여 청취 또는 시청

- 형사소송규칙에 근거하여 저장매체의 사본을 만들어 기록하고, 디지털 정보를 출력하여 사용

디지털 데이터와 압수

- **압수•수색 대상**
  - **형사소송법 제106조(압수)**
    1. 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다. <개정 2011.7.18>
    2. 법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.
    3. 법원은 압수의 목적물이 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체 등"이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출 받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있다. <신설 2011.7.18>
    4. 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다. <신설 2011.7.18>

디지털 데이터와 압수

- **압수•수색 대상**
  - **형사소송법 제215조(압수, 수색, 검증)**
    1. 검사는 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 지방법원판사에게 청구하여 발부받은 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.
    2. 사법경찰관이 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 검사에게 신청하여 검사의 청구로 지방법원판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다. [전문개정 2011.7.18]

디지털 데이터와 압수

- **판례** – 2011. 5. 26. 대법원 재항고 기각
  - **전자정보에 대한 압수.수색영장의 집행이 그 적법성을 갖추기 위하여 필요한 조치** [2009모1190]

> 전자정보에 대한 압수·수색영장의 집행에 있어서는 원칙적으로 영장 발부의 사유로 된 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행현장의 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 그와 같은 경우에 그 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 예외적으로 허용될 수 있을 뿐이다. 나아가 이처럼 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보아야 한다. <생략>

- 2011년 7월 18일 **압수.수색에 관한 형사소송법 개정** ➔ 디지털 데이터 압수.수색 관련 조항 신설

디지털 포렌식 법률

국내 디지털 포렌식 관련 법률

- 형사소송법/규칙
- 디지털증거수집 및 분석규정 (대검찰청 예규)
- 정보통신망 이용 촉진 및 정보보호 등에 관한 법률
- 통신비밀보호법
- 부정경쟁방지 및 영업비밀보호에 관한 법률
- 산업기술의 유출방지 및 보호에 관한 법률
- 신용정보법 등 개인정보관련 규정 등

질문 및 답변