

8장. 디지털 증거

박종현

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech.ac.kr

1. 디지털 증거의 개념
2. 디지털 증거의 법적 허용성
 - 위법수집증거배제의 원칙
(Exclusionary Rule of the Illegally Collected Evidence)
 - 전문법칙 (傳聞法則, Hearsay Rule)
3. 디지털 증거의 법적 허용성 요건
 - 디지털 증거의 증거 능력을 보장하기 위한 특성
 - 디지털 증거의 법적 허용성 보장을 위한 장치
4. 디지털 데이터의 증거 능력 관련 판례
5. 디지털 포렌식 조사 모델이란?
6. 디지털 포렌식 조사 모델
7. 디지털 포렌식 조사 모델 비교

8-1. 디지털 증거의 개념

디지털 증거의 개념

• 디지털 증거 관련 용어

- 전자 증거(Electronic Evidence)
 - 전자기기에 저장되어 있거나 전자기기에 의해 전송되며, 증거로써 가치가 있는 정보와 데이터를 의미
- 전자 정보(ESI: Electronically Stored Information)
 - 미국에서는 전자정보 혹은 전자적으로 저장된 정보(Electronically Stored Information)라는 의미의 ESI라는 용어를 주로 사용

• 디지털 증거(Digital Evidence) 정의

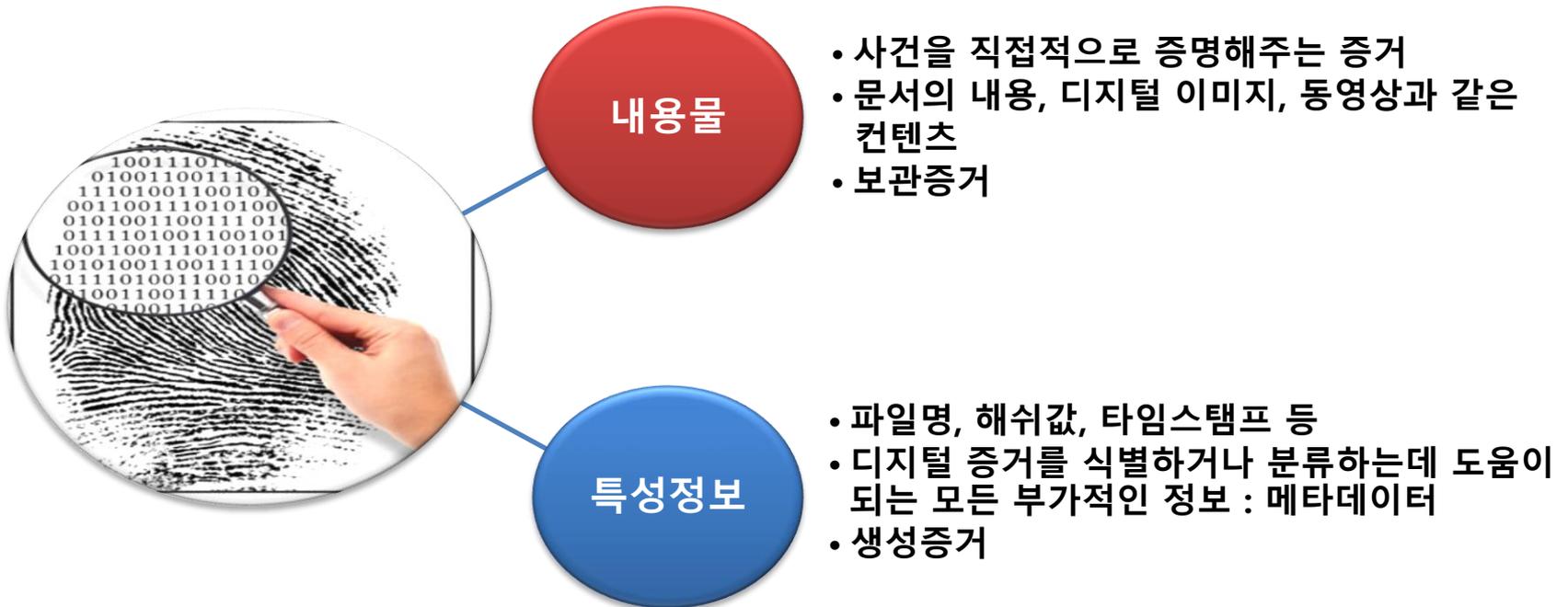
- 컴퓨터 또는 기타 디지털 저장 매체에 저장되거나 네트워크를 통해 전송 중인 자료로서 법정에서 신뢰할 수 있으며 증거 가치가 있는 정보
- IOCE(International Organization on Computer Evidence) 정의
 - 이진수 형태로 저장 혹은 전송되는 것으로 법정에서 신뢰할 수 있는 정보
- 미국 SWGDE(Scientific Working Group on Digital Evidence) 정의
 - 디지털 형태로 저장되거나 전송되는 증거가치가 있는 정보

디지털 증거의 종류

• 디지털 증거의 종류를 구분하는 방법

- 저장 매체의 종류, 증거의 내용, 법적 효력 또는 디지털 정보의 휘발성 정도
- 디지털 증거의 진정성과 무결성을 만족시켜 주는 속성에 따라 구분

• 디지털 증거의 속성에 따른 분류



8-2. 디지털 증거의 법적 허용성

디지털 증거의 증거 능력

- 법정에서 유효한 증거가 되기 위해서는 증거능력 관점에서 유의하여 증거를 수집/분석/제출해야 함



※ 자유심증 주의

증거의 증명력을 평가할 때 아무런 제한이나 구속력을 두지 않고 오로지 법관의 자유로운 판단에 맡기는 주의

위법수집증거능력배제원칙

- **위법수집증거능력배제원칙** (Exclusionary Rule of the Illegally Collected Evidence)
 - 위법한 절차에 의하여 수집된 증거, 즉 **위법 수집 증거는 증거능력을 부정하는 원칙**
 - 미국 연방대법원의 판례를 통하여 형성된 이론으로 미국 헌법에서 보장하고 있는 절차를 보장하고 인권을 보호하기 위한 목적
- **국내법에서 위법수집증거능력배제원칙**
 - 진술증거 특히 자백에 대하여 증거능력을 제한하는 명문 규정을 두었으나, 비진술증거인 증거물과 관련하여 그 증거능력에 아무런 규정이 없었음
 - 기존의 판례는 위법행위 여부와 상관없이 비진술증거에 대해서는 증거능력이 인정되었지만, 근래 형사소송법 내 308의2조에 **"적법한 절차에 따르지 아니하고 수집된 증거는 증거로 할 수 없다"**라고 명확히 위법수집증거배제원칙을 규정하고 있음

전문법칙

- 전문 (傳聞, Hearsay)

- 사실의 진위여부는 알지 못한 상태에서 전해들은 말을 의미
- 진실을 입증하기 위해 법정 밖에서 진술된 것

- 전문 법칙(Hearsay Rule)

- 전문법칙(전문증거배제법칙)은 전문증거의 증거능력을 배제하는 증거 법상의 원칙
- 원진술자가 말한 진술상의 취약점을 파악할 방법이 없음
- 현행 형사소송법 제310조의2에서는 이러한 전문증거의 증거능력을 원칙적으로 부인
- 전문이 아닌 예
 - 진술이 진실을 입증하려고 제출하는 것이 아닌 경우
 - 상대방에게 영향을 준 것을 보여주기 위해 제출하는 경우
 - 서로 관련 있다는 것을 보이기 위한 경우
 - 진술자의 동기에 관한 정황 증거인 경우
 - 진위 여부와 상관없이 진술되었다는 것에 관한 경우
 - 의문문 또는 명령문 인 경우
 - 동물과 기계로부터 획득된 정보

전문법칙의 예외

• 전문법칙의 예외

- 진술이 진실일 가능성이 큰 경우
- 잘못된 의미를 전달할 가능성 보다 다른 요소가 더 큰 경우
- 전문가 증언의 경우 전문가들이 근거로 하는 자료
- 원진술자가 법정에서 증언할 수 없다는 것을 입증할 경우

• 일반적인 전문법칙의 예외들

- 법원 또는 법관의 면전조서, 피의자신문조서, 진술조서 및 진술 기재서, 진술서, 검증조서, 감정서, 당연히 증거능력이 있는 서류 등

• 전문법칙의 예외 기준

- 신용성의 정황적 보장

- 해당 진술의 진실성을 담보할 수 있는 구체적이고 외부적인 정황이 있음을 의미

- 필요성의 원리

- 원진술과 동일한 내용의 진술을 구하는 것이 불가능하거나
- 현저히 곤란하기 때문에 비록 전문증거라고 하더라도 이를 사용하여 실제적 진실을 규명할 필요가 있을 경우

• 디지털 증거와 관련된 예외

- [형사소송법 315조] 신용성의 정황적 보장과 필요성 원리를 적용하여 당연히 증거능력이 있는 서류를 전문법칙의 예외로 둠
- 따라서, 315조에 해당되는 디지털 증거의 출력 물건 → 무결성, 신뢰성이 인정된다면 증거능력이 인정됨

형사소송법 제315조 (증거능력이 있는 서류)

다음에 게시한 서류는 증거로 할 수 있다.

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

디지털 증거와 전문법칙의 관계

• 디지털 증거와 전문법칙

- 디지털 증거는 직접적으로 사람의 지각·기억·표현·서술이라는 진술과정을 거치지 않고 그것이 기계적으로 처리되어 작성된 것
- **전문법칙에 근거하여 컴퓨터에 저장되어 있는 디지털 자료는 전문증거로 판단되어 증거능력을 인정하지 않을 수 있음**
 - 압수한 디지털 증거가 무결성의 문제, 신뢰성의 문제 및 원본성의 문제를 모두 통과하였다고 하더라도
 - 디지털 증거가 진술증거로 인정되는 경우에는 전문법칙이 적용되어 증거능력이 부정될 수 있음

• 전문법칙 예외 조항에 디지털 증거 적용

- 디지털 증거는 특정 프로그램을 이용, 사람이 표현하고자 하는 내용의 자료를 입력하여 처리·생성된 부분이 존재
- **내용의 진실성을 입증하기 위해서는 전문법칙의 관계에 유의하여 증거능력에 대한 검토가 필요**
- 디지털 증거도 적절한 조건을 갖추어 전문법칙의 예외로 적용됨

전문법칙의 예외 조항으로 디지털 증거

• 비진술 증거로서의 디지털 증거 (전문 아님)

- 주로 컴퓨터에 의해 생성된 증거(Computer-generated Evidence)
- 컴퓨터 시스템이 작동하면서 자동적으로 기록·저장되는 디지털 증거들
 - 시스템 로그파일, 이벤트 기록 및 인터넷 웹 히스토리 파일 등
 - 디지털 데이터 자체가 증거로서 제출되는 경우에는 진술증거가 아니므로 전문법칙이 적용될 여지가 없음
 - 진정성, 무결성, 신뢰성 등이 인정된다면 일반적으로 증거능력이 인정됨

• 진술 증거로서의 디지털 증거 (전문 여부 판단 필요)

- 주로 컴퓨터에 저장된 증거(Computer Stored Evidence)
- 대부분 진술증거로서 전문법칙이 적용됨
- 전자문서로 된 비즈니스 기록은 진술증거임에도 일정 요건이 만족되는 경우 전문법칙의 예외로 인정
 - **비즈니스 기록**: 기업의 일상적인 비즈니스 과정에서 비즈니스와 관련된 어떤 사실을 기록하기 위해 준비되거나 이용되는 모든 회계장부나 기타 문서들
 - 많은 국가에서 비즈니스 기록은 전문증거 규칙의 예외로 적용

8-3. 디지털 증거의 법적 허용성 요건

디지털 증거의 증거 능력 요건

진정성(Authenticity)

- 증거 데이터의 저장, 수집 과정에서 오류가 없으며, 의도된 결과가 정확히 획득되었고, 그로 인해 생성된 자료임이 인정됨

무결성(Integrity)

- 증거 데이터가 수집 및 분석과정을 거쳐 법정에 제출되기까지 변경이나 훼손 없이 안전하게 보호되는 것

신뢰성(Reliability)

- 증거 데이터의 분석 등 처리 과정에서 디지털 증거가 위·변조되지 않았고 의도되거나 의도되지 않은 오류를 포함하지 않음

원본성(Originality)

- 자체적으로 가시성과 가독성이 없는 디지털 증거를 변환하여 제출하는 과정에서 제출되는 증거 데이터가 원 매체에 있는 데이터와 동일함

디지털 증거가 법적 효력을 가지고 증거능력을 인정받기 위해서는 **디지털 증거의 진정성, 무결성, 신뢰성, 원본성이 기본적으로 보장되어야 함**

진정성과 무결성

• 진정성 (Authenticity)

- 디지털 증거의 저장, 수집 과정에서 오류가 없었으며, 의도된 결과가 정확하고 그로 인해 생성된 자료임이 인정되어야 함
- 디지털 증거는 다른 증거와 달리 훼손, 변경이 용이한 특성으로 인하여 최초 증거가 저장된 매체에서 법정에 제출되기까지 확실한 인수인계를 통해 변경이나 훼손이 없어야 함
(연계 보관성- Chain of Custody)

• 무결성 (Integrity)

- 디지털 증거가 원본 소스로부터 수집되어 보관, 분석되는 과정에서 부당한 수정, 변경, 손상이 없도록 유지해야 하며 이를 검증(보장) 할 수 있어야 함
- 법정 제출 시 디지털 증거를 검증하여 위조 여부를 판별해야 함
- 고소인 측에서 연계 보관성을 통한 무결성을 증명하더라도, 피고소인이 디지털 증거의 위조 가능성을 이유로 증거효력을 무력화 할 경우, 디지털 증거의 신뢰성을 입증할 수 있어야 함

- 디지털 증거의 원본성 (Originality)

- 디지털 증거 자체로는 가시성, 가독성이 없으므로
→ 가시성 있는 인쇄물로 출력하여 법원에 제출

- 원본성과 디지털 증거 사본

- 대용량 시스템에서의 증거 수집은 원본 매체 자체를 다른 저장 매체에 복제 혹은 기타 방법으로 이동시켜 수집함
- 실제 법정에서 제출되는 증거들은 원본 증거와는 다른 형태를 취하게 되며, 증거 원본이 제출되어야 함
- 증거법 원칙상,
“제출되는 사본 증거, 그리고 가시성, 가독성 있는 형태로 변환된 증거를 원본으로 인정할 수 있는가?”라는 법적 문제가 제기될 수 있음

• 최량증거규칙 (The Best Evidence Rule)

- 영미권에서 증거원칙으로 문서의 원본증거가 증거로서 그 내용을 증명하기 위해 원본이 제출되어야 한다는 것
- 미국 최량증거규칙은 연방증거규칙(Federal Rules of Evidence)에서 명시
 - "서류, 기록물 또는 사진의 내용을 증명하기 위하여 문서, 기록물, 사진의 원본이 요구된다."
 - 디지털 증거는 자기적 혹은 전기적 방식에 의한 기록물로서 서류, 기록물 등에 포함되므로, 디지털 증거도 기본적으로 당연히 원본으로 제출될 것을 요구 받음
 - 그러나, 다음과 같은 경우에는 복제물도 Best Evidence로 법정 증거로 허용된다고 명시

FRE 1004 (Federal Rules of Evidence)

- ① 원본이 삭제되거나 멸실된 경우 : 해쉬 함수와 적절한 이미지로 검증된 복제본임을 쉽게 입증할 수 있음
- ② 원본을 획득하기 힘들 경우 : 상대방에게 장비를 돌려줘야 하거나 상대방이 원본을 파괴한 경우
- ③ 상대방이 원본을 소유하고 있는 경우 : 상대방이 해당 원본증거에 접근하는 것을 거부한 경우

신뢰성

• 디지털 증거의 신뢰성

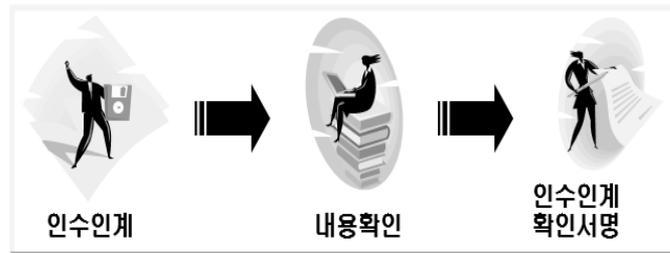
- 증거 데이터의 분석 등 처리 과정에서 디지털 증거가 위·변조되거나 의도되지 않은 오류를 포함하지 않았음을 의미
- 디지털 증거의 신뢰성은 디지털 증거 자체의 특성이 아닌 디지털 증거를 취급하는 인력, 도구, 분석 절차 등과 같은 주·객관적인 요소들의 신뢰성 증명을 통해 간접적으로 증명 가능

• 신뢰성 관점에서 디지털 증거의 법적 활용

- 행위자에 의한 원본 생성부터 조사 과정에서의 수집, 분석, 법정 제출까지의 신뢰성 확보를 위한 관리가 필요
- 신뢰성 확보를 위한 제도적, 과학적 절차의 마련이 필요하며, 이는 곧 디지털 포렌식 연구 목표와 동일

1) 디지털 증거의 진정성 / 무결성 보장 장치

- 디지털 증거는 진정성과 무결성을 유지하기 어려움
- 저장매체의 내부 정보는 외관 확인으로 증거물의 상태를 확인불가
- 각 인수인계 단계마다 진정성과 무결성을 검증할 수 있는 절차로서 **연계 보관성 (Chain of Custody)** 유지가 필요



• 연계 보관성 (Chain of Custody)

- 디지털 증거의 발견방법과 처리방법을 비롯하여 증거와 관련된 모든 사항을 명확히 기술하고 보관·이송 과정에서 인수인계 과정에 대한 기록과 검증이 필요
- 대검찰청의 디지털증거수집 및 분석규정의 2조
 - "디지털기기를 압수·수색·검증하거나 디지털 자료를 수집·분석할 때에는 디지털기기 또는 디지털 자료를 수집한 때로부터 법정에 증거로 제출할 때까지 변경 또는 훼손되지 않도록 절차의 연속성을 유지하여야 하며 그 과정을 기록하여야 한다."라고 연계보관성원칙을 가장 먼저 명시

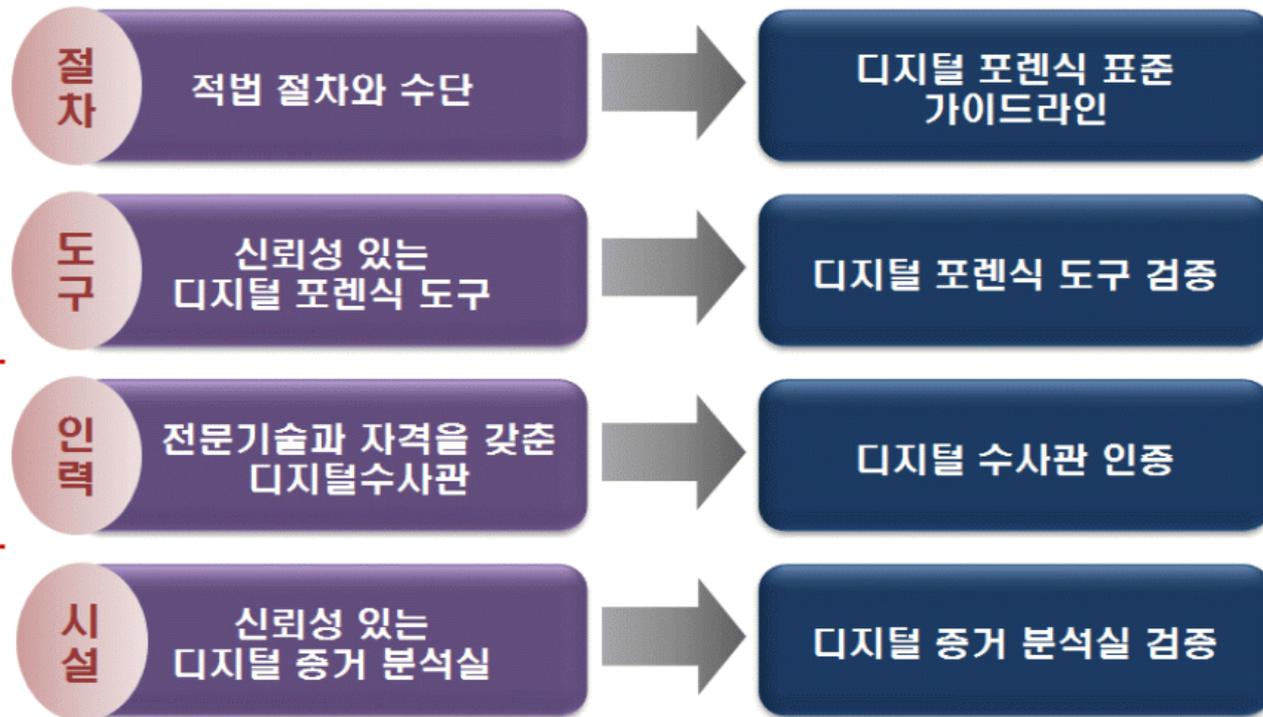
• 연계 보관성 유지를 위해 기록할 정보

- 증거를 발견하고 수집한 사람, 장소, 시간
- 증거를 취급하고 조사한 사람, 장소, 시간
- 증거를 보관하는 사람, 보관 기간, 보관 방식
- 증거 관리가 변경되었을 때의 이송 방법과 날짜 (선적 번호 포함)

2) 디지털 증거의 신뢰성 보장 장치

• 디지털 증거의 법적 허용성 보장을 위한 제도적 장치

- 국가차원의 제도화를 통해 법 집행력을 높이고 법 정의를 실현하는데 도움을 제공

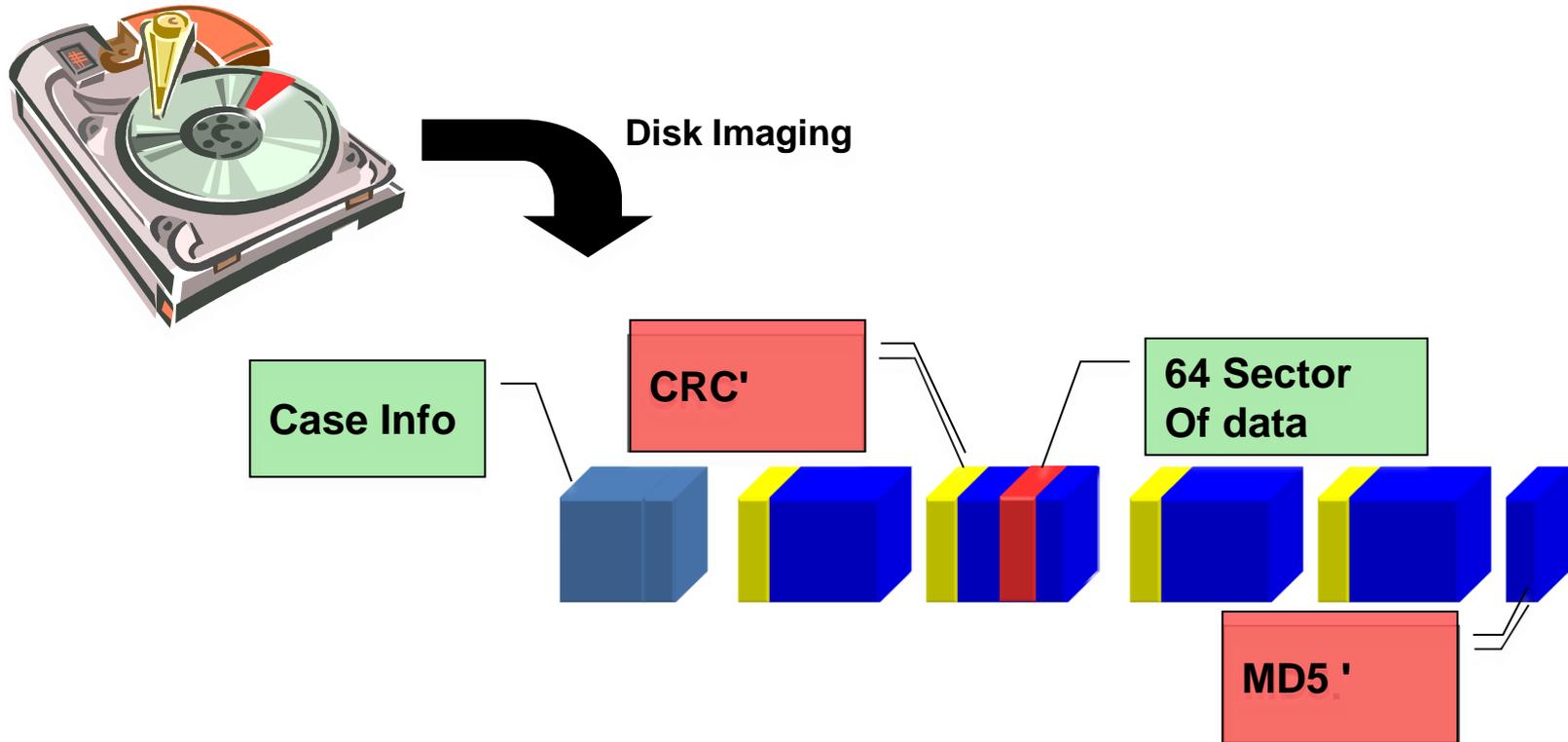


- 2007년 일심회에 대한 대법원 판례
디지털 증거가 법적 효력을 갖기 위한 요건들이 제시

현재의 디지털 증거의 무결성 입증 방법

- 암호학적 해시함수를 이용하여 디지털 증거의 무결성 입증
- 암호학적 해시함수
 - 임의의 긴 입력 값을 적절하게 처리하여 고정된 길이의 값을 출력
 - 해시 함수의 출력 값을 이용하여 역으로 입력 값을 유추할 수 없음
 - 같은 출력 값을 갖는 임의의 입력 값 2개를 찾는 것은 계산상 불가능
- 디지털 증거의 무결성 입증을 위한 해시함수 사용
 - 디지털 증거를 획득(하드디스크 이미지)
 - 획득한 증거에 대한 해시함수 적용
 - 해시함수의 출력 값을 별도 보관
 - 이 후 법정에서 디지털 증거의 해시 값을 계산하여 별도 보관된 해시 값과 비교하여 일치하면 무결성이 입증됨

EnCase의 디지털 증거 무결성 확보 방법



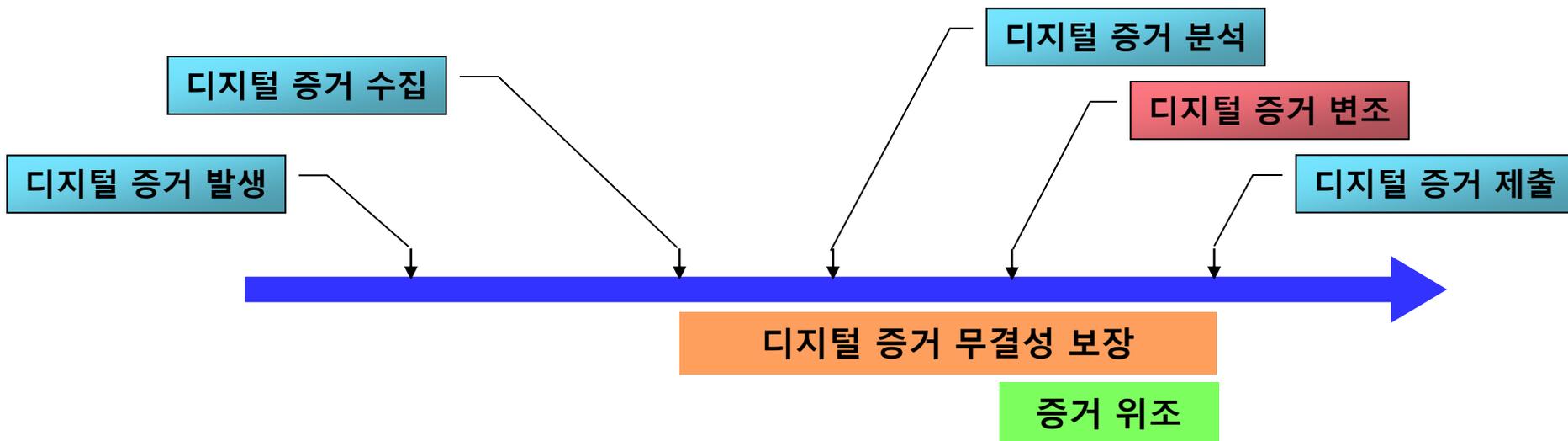
$$V = h(H) = h(I)$$

$$V' = h(H') = h(I')$$

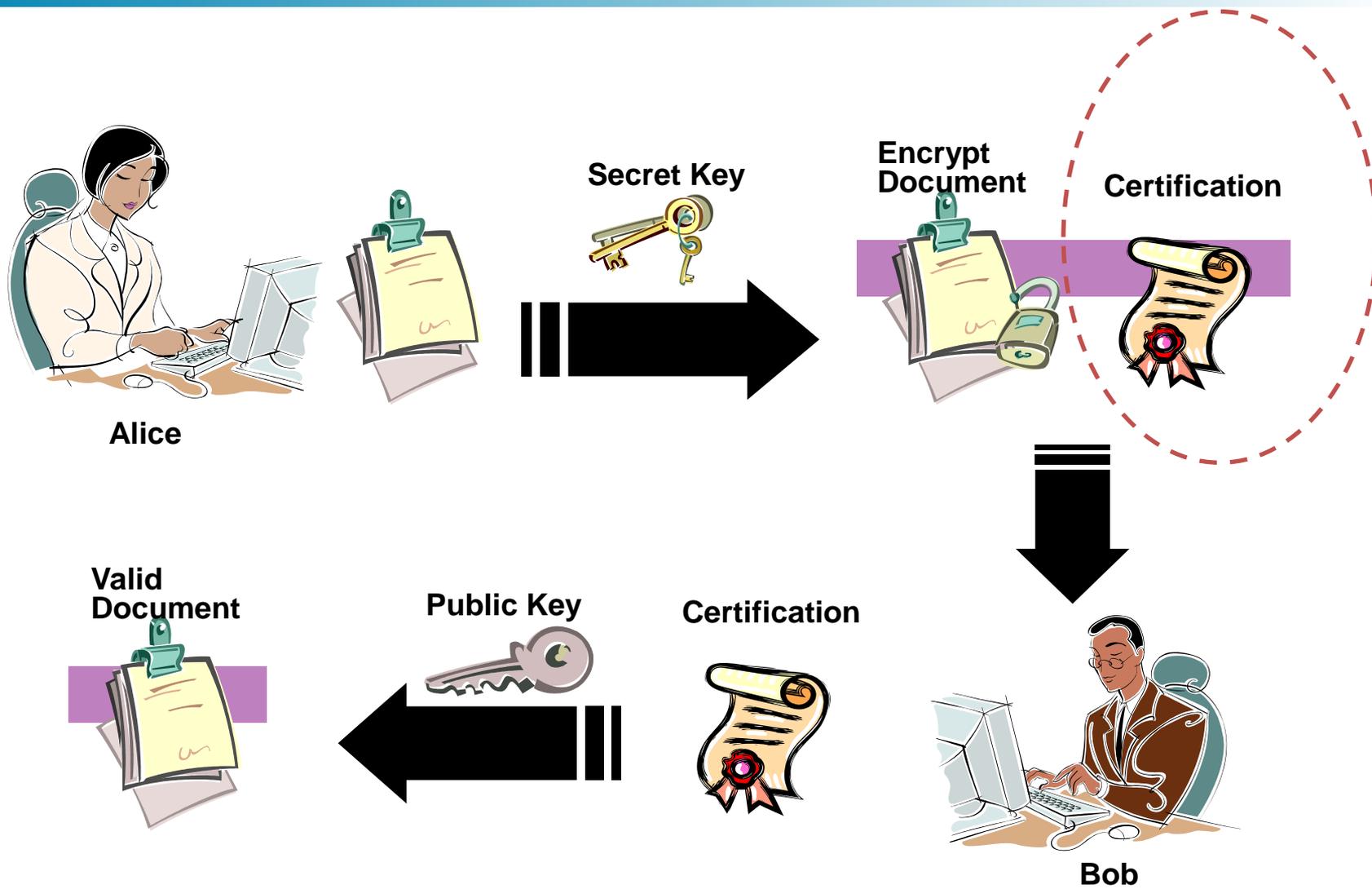
현재 디지털 증거 무결성 확보의 문제점

• 디지털 증거의 신뢰성

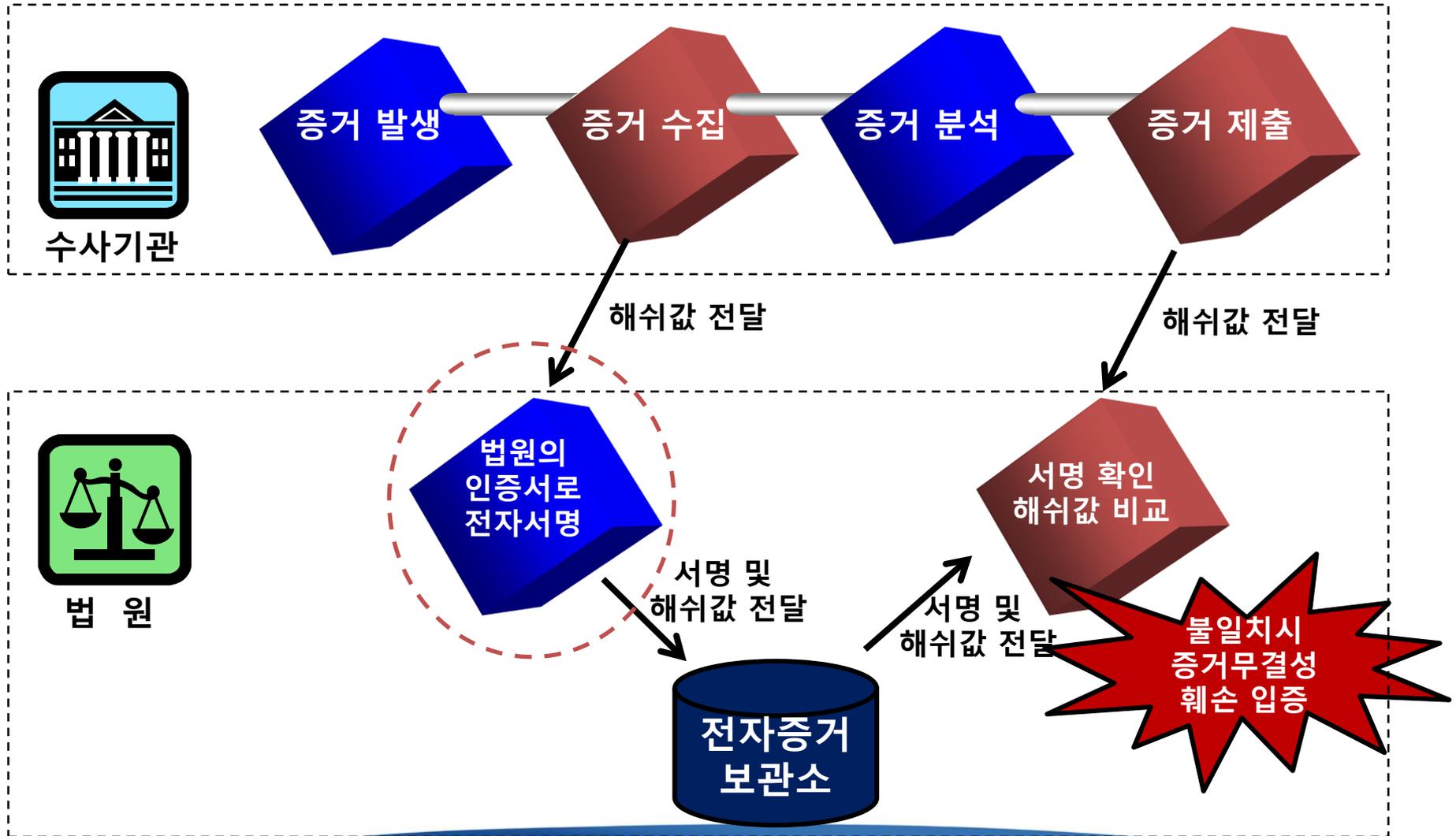
- 디지털 증거가 위조되어 법정에 제출되는 경우
- 디지털 증거가 위조되지 않았음에도 불구하고
.용의자 또는 피고소인이 디지털 증거가 위조되었을 가능성을 이유로,
증거 효력을 무력화 시키려 하는 경우



인증서를 사용한 전자서명



디지털 증거의 인증 방안



디지털 증거의 증거능력

• 디지털 증거의 복사본

- 디지털 증거의 특성상 원본과 사본의 데이터는 완벽히 일치
- 장기간 보관 또는 취급 부주의로 인한 고장 등으로 데이터 훼손 가능
- 제 3자의 입회 하에 해쉬 값에 대한 공증 필요
- 해쉬 값이 동일한 경우 사본에 대한 증거력 인정 필요

• 네트워크 정보의 증거력

- 네트워크 데이터는 실시간으로 변화
- 데이터의 수집기간에 따라 해쉬값이 바뀔 수 있음
- 제 3자의 입회 하에 수집 및 해쉬 값 계산, 공증
- 이후 동일 해쉬 값을 갖는 데이터를 원본으로 인정



• 대형 시스템에서의 디지털 증거

- 대형 시스템의 경우 이미징이 현실적으로 불가능
- 이미징을 위해 시스템을 정지시킬 수 없음
- 기업의 업무에 피해를 미침
- 모든 데이터를 출력물로 생성하는 것은 현실적으로 불가능
- 논리적 파일로 수집해야 할 필요성 존재
- 제 3자의 입회 하에 파일로 수집하고 이에 대한 해시 값을 공증
- 이 후 동일한 해시 값을 갖는 파일에 대해 증거력 부여



• 임베디드 시스템에서의 디지털 증거

- 핸드폰, PDA, 게임기, PMP 등 다양한 임베디드 시스템 존재
- 데이터의 수집 자체가 어려운 경우가 존재
- 다양한 수집기법 존재 : 물리적 수집 및 논리적 수집
- 따라서 물리적 수집과 논리적 수집된 각 디지털 증거에 대해 증거력 부여가 필요





분석을 위해 사본생성



증거분석

분석 보고서 제출

장기보관 등으로 인한
데이터 변조



해취값이 동일한 경우
사본의 증거력 인정 필요

해취값이 바뀜
→ 증거 인정 불가



법원

8-4. 디지털 데이터의 증거 능력 관련 판례

국내사례 (1)-영남위 사건

• 부산고등법원 선고 99노123 [국가보안법위반]

- 수사도중 디스켓에서 북한을 찬양한 문서 파일이 발견됨
 - 이를 국가 보안법 위반 찬양 고무등의 혐의로 기소한 사건
 - 대법원 판례 요지
 - "컴퓨터 디스켓이 들어 있는 문건이 증거로 사용되는 경우
 - 그 컴퓨터 디스켓은 그 기제의 매체가 다를 뿐 실질에 있어서는 피고인 또는 피고인 아닌 자의 진술을 기재한 서류와 크게 다를 바 없고,
 - 압수 후의 보관 및 출력과정에 조작의 가능성이 있으며,
 - 기본적으로 반대신문의 기회가 보장되지 않는 점 등에 비추어
 - 그 기재내용의 진실성에 관하여는 **전문법칙이 적용**된다고 할 것이고,
 - 따라서 형사소송법 제313조 제1항에 의하여
 - "그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다"
- 증거능력 부정

국내사례 (2)-일심회 사건

• 대법원 2007.12.13선고 207도 7257판결 [국가보안법 위반]

- 반국가단체 구성원으로부터 플로피 디스켓을 전달
- PC방에서 북한공작원과 e-mail 송수신 및 게시판 글 대북보고
- 3.5" 디스켓과 USB, 노트북PC, CD, e-mail 출력물 등 압수

- 대법원 판례 요지

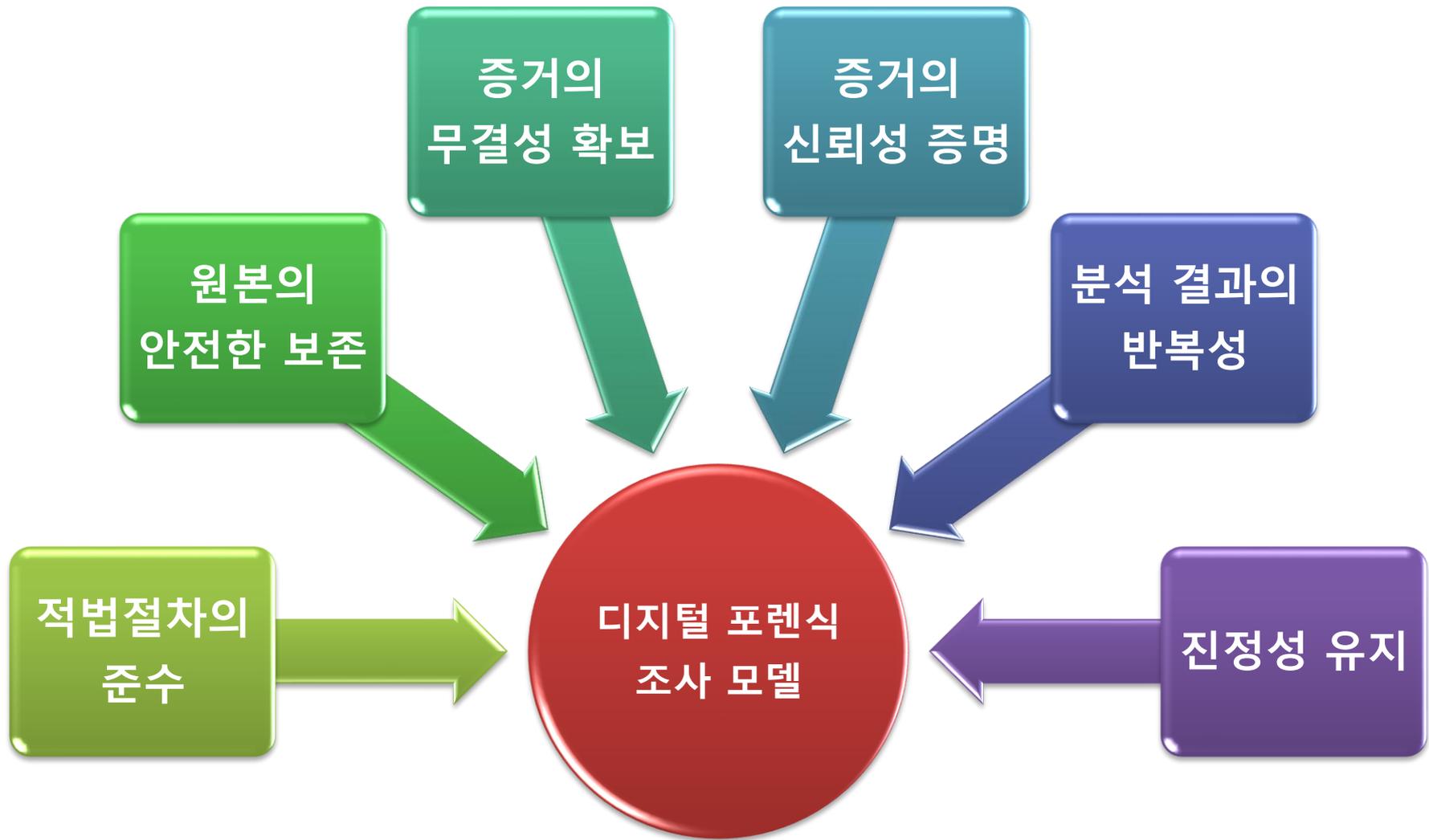
압수물인 디지털 저장매체로부터 출력한 문건을 증거로 사용하기 위해,

- 디지털 저장매체 원본과 출력한 문서의 동일성이 인정되어야 하며,
- 이를 위해 **디지털 저장매체 원본이 문서 출력시까지 변경되지 않았음이 담보되어야 함**
- 하드카피나 이미징으로부터 출력된 문서라면,
 - 원본과 이들 사이의 동일성도 인정되어야 하고
 - 이를 확인하는 컴퓨터의 정확성과 조작자의 전문성도 담보되어야 함
- 압수된 디지털 저장매체로부터 출력된 문건을 진술증거로 사용하려면 기재내용의 진실성에 관해 **전문법칙**이 적용되므로,
- 형사소송법 제313조 제1항에 따라

"그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다"

8-5. 디지털 포렌식 조사 모델이란?

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

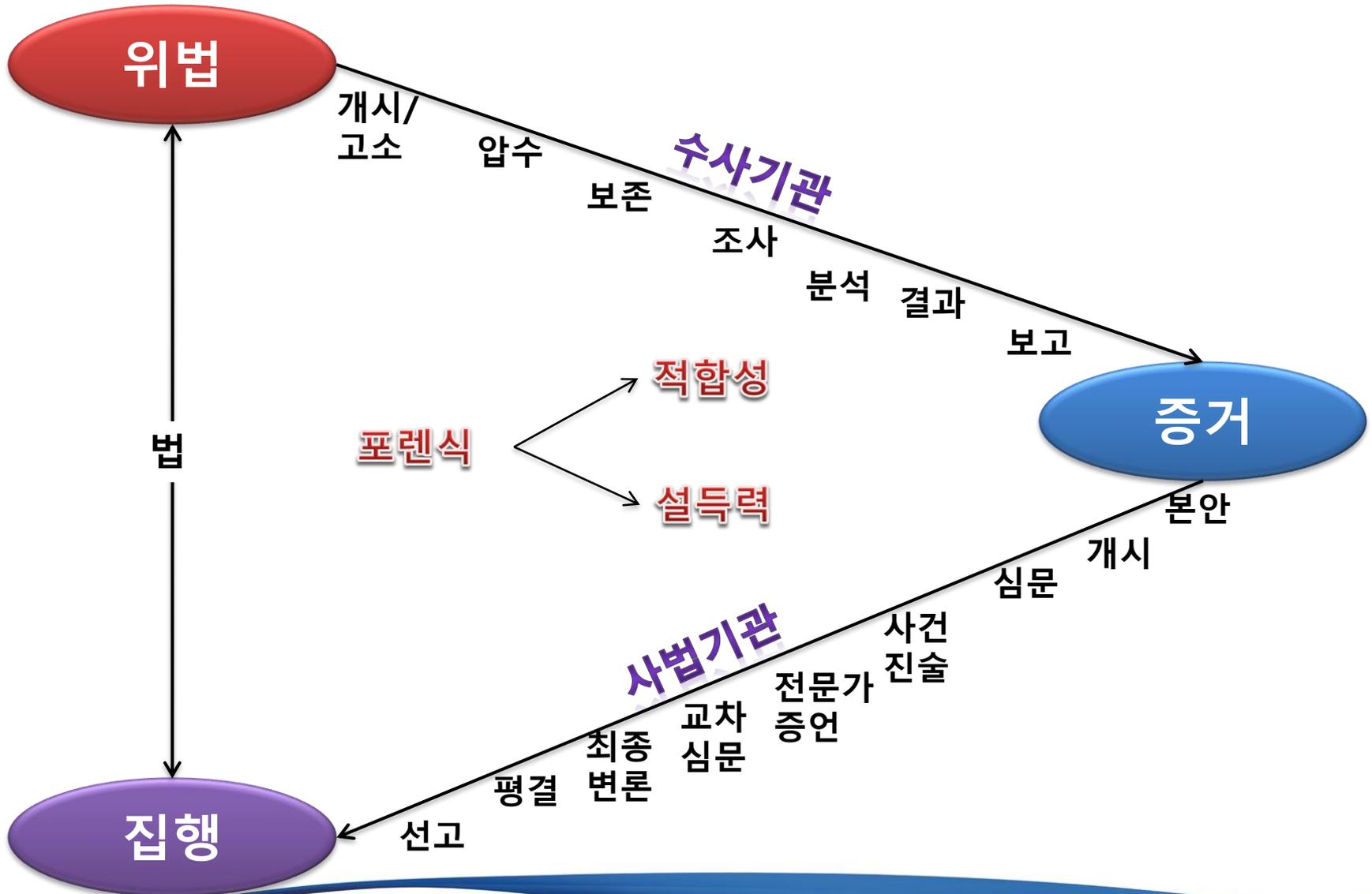
• 디지털 포렌식 조사 모델의 정의

- 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



8-6. 디지털 포렌식 조사 모델

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

보고 및 증언

- 분석 보고서 작성
- 증거 관련 문서 보관
- 법정 증언

조사 및 분석

- 사본 생성
- 데이터 추출
- 데이터 분류
- 상세 분석

운반 및 확인

- 증거물 운반
- 증거물 등록 및 확인
- 원본 보관

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 부족한 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 발견 되면 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 선행**되어야 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	<ul style="list-style-type: none"> • 당사자의 동의 • 권한 있는 자의 승인 	당사자의 동의를 얻지 않을 경우, 영장을 발부 받아 조사 권한을 획득해야 함
영장 등 기재내용	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 조사 팀의 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

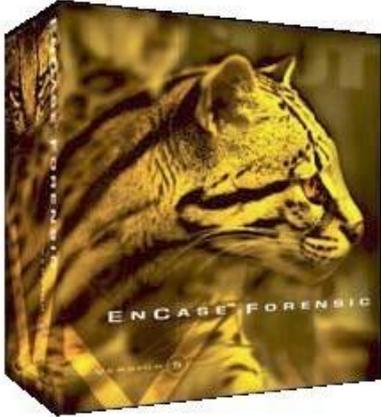
• 운반 장비

- 증거 운반용 전문 케이스나 운반 차량이 포함

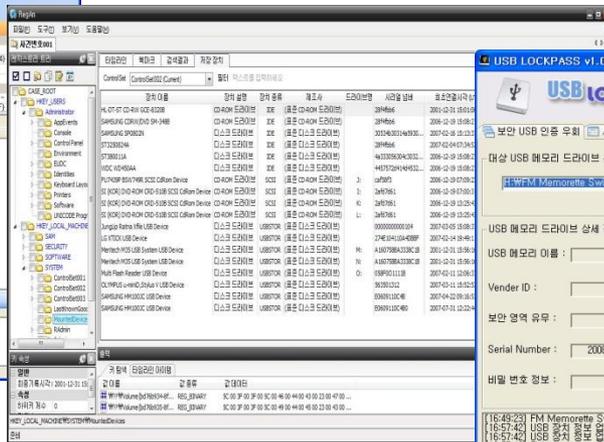
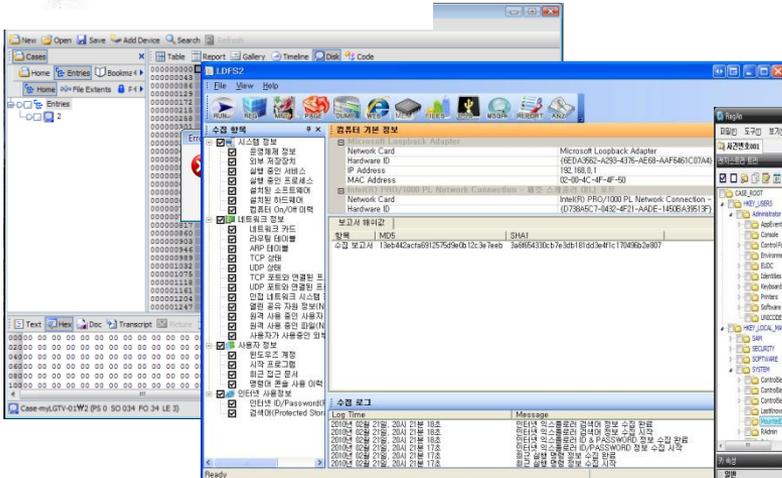
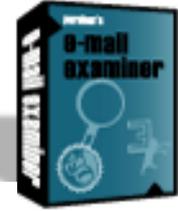
• 포렌식 하드웨어



• 포렌식 소프트웨어



paraben's e-mail examiner



• 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

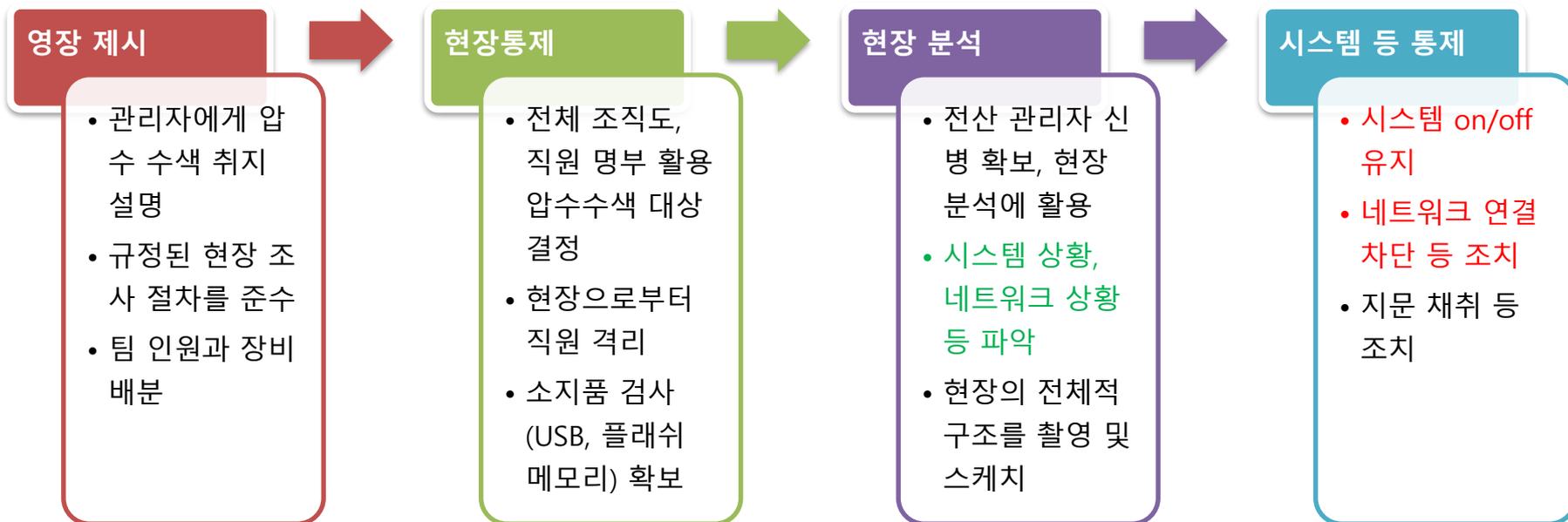
조사 대상 시스템 및 저장 매체 확보

- 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 판단**할 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



• 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, 플래시 메모리 등)
 - 최근 용량 · 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 통한 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
 - *RAID: 여러 개의 디스크를 배열하여 속도의 증대, 안정성의 증대, 효율성, 가용성의 증대를 하는데 쓰이는 기술
 - 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**

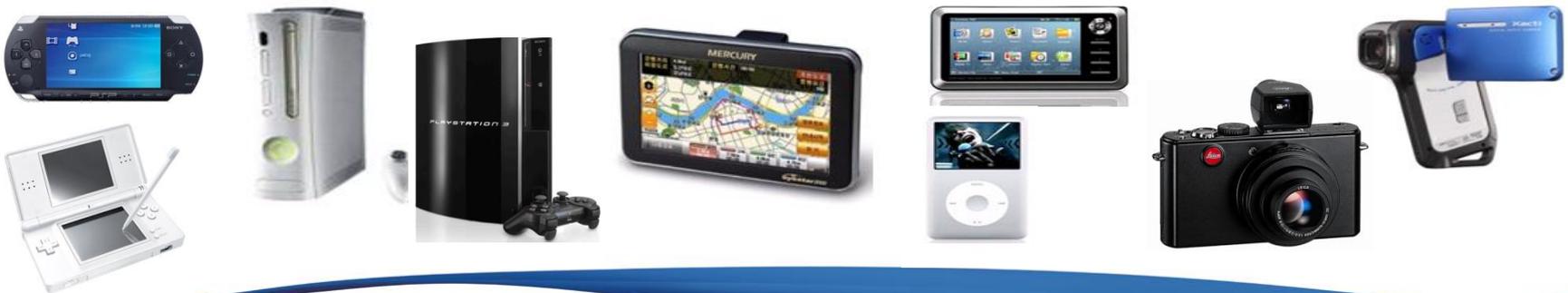


• 디지털 캠코더 및 카메라

- 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

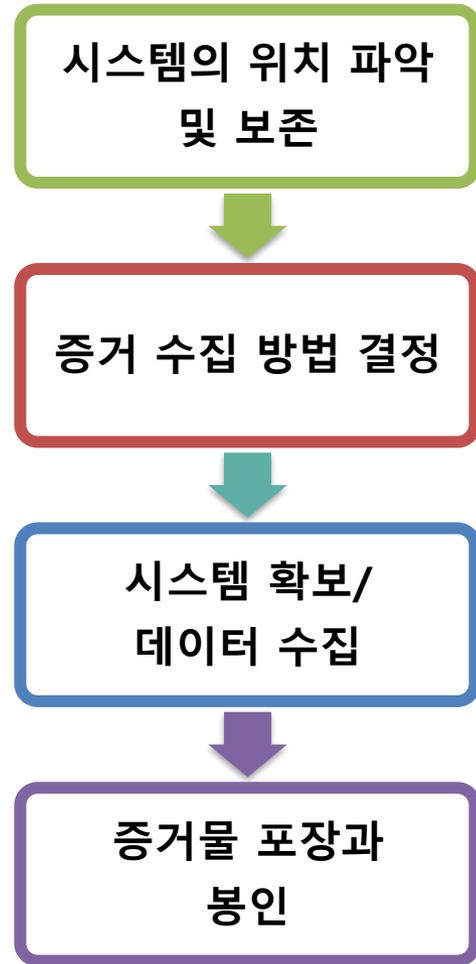
- 범죄 현장의 조사자는 다양한 디지털 저장 매체를 파악하고 이를 현장에서 확보할 수 있도록 배경 지식을 갖추어야 함
- 대부분의 저장 매체는 메인보드에 직접 연결되어 사용되거나 USB 등과 같은 외부 연결 인터페이스를 사용
- 이러한 연결 정보가 시스템에 저장되므로 사용자가 은닉한 매체가 있는지 확인하고 확보해야 함



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



증거 확보 및 수집 세부 절차



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 데이터**를 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

- 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

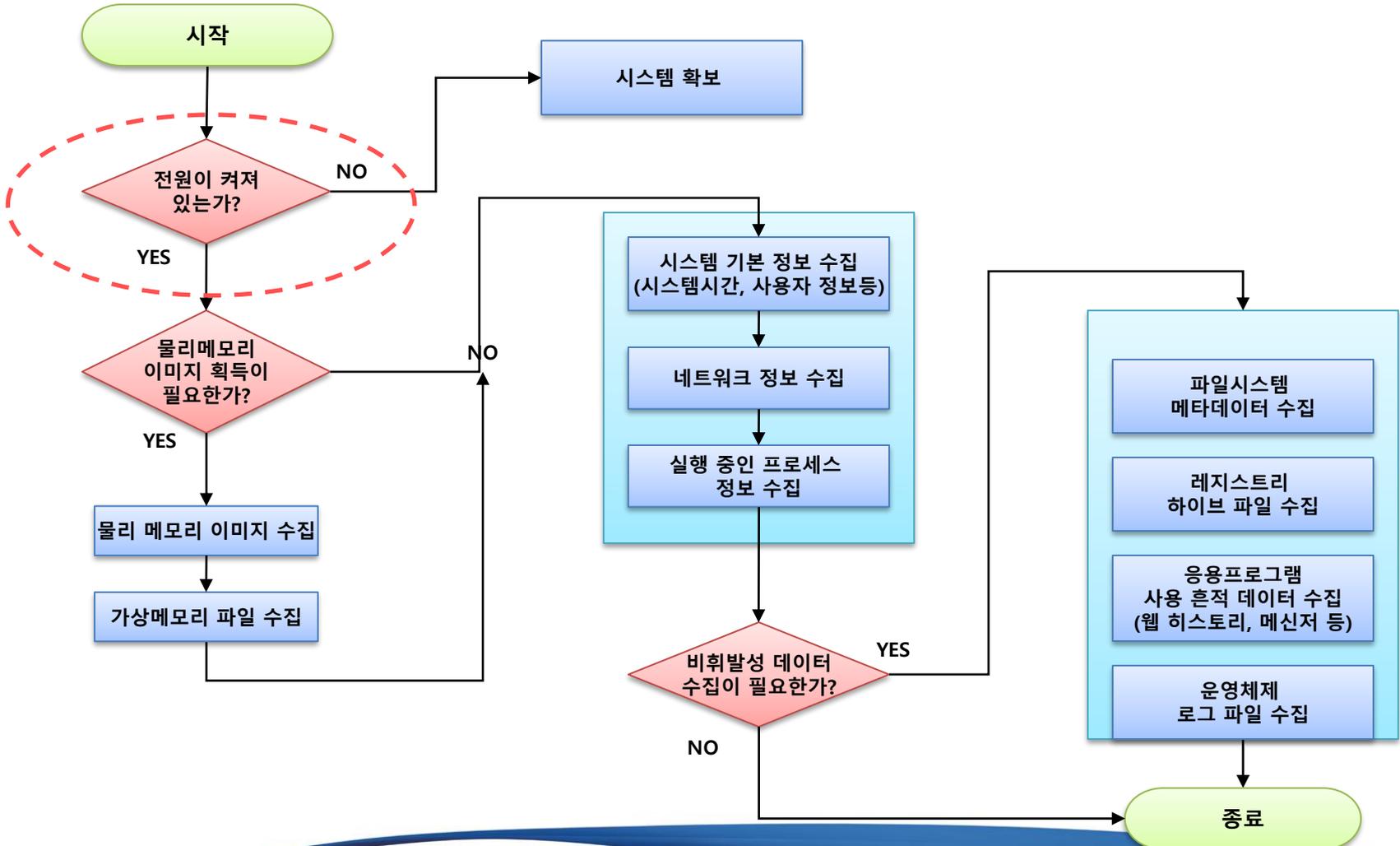
네트워크 정보

- 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 세부 정보

- 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

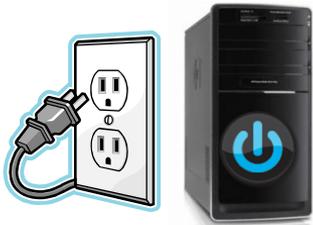
• 원본/사본 디스크 확보를 위한 준비 과정

- 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)



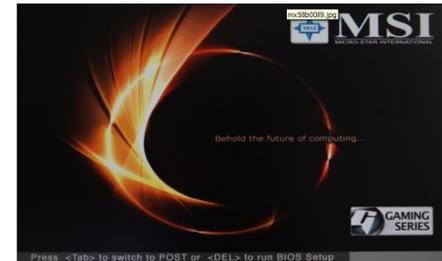
시스템 전원 OFF



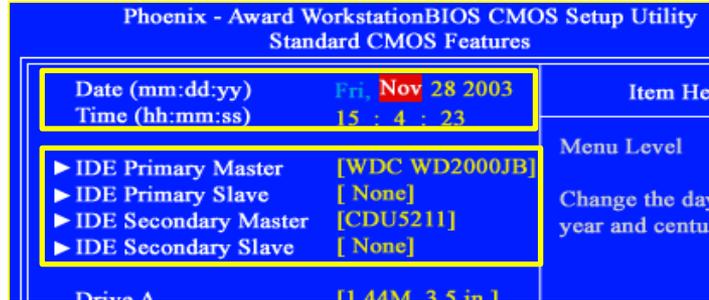
하드디스크 분해



시스템 전원 ON



부팅 시 BIOS 진입 (F2, Del 키 등)



BIOS 에서 시간 정보 비교 및 표준 시간과 확인



• 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
- 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



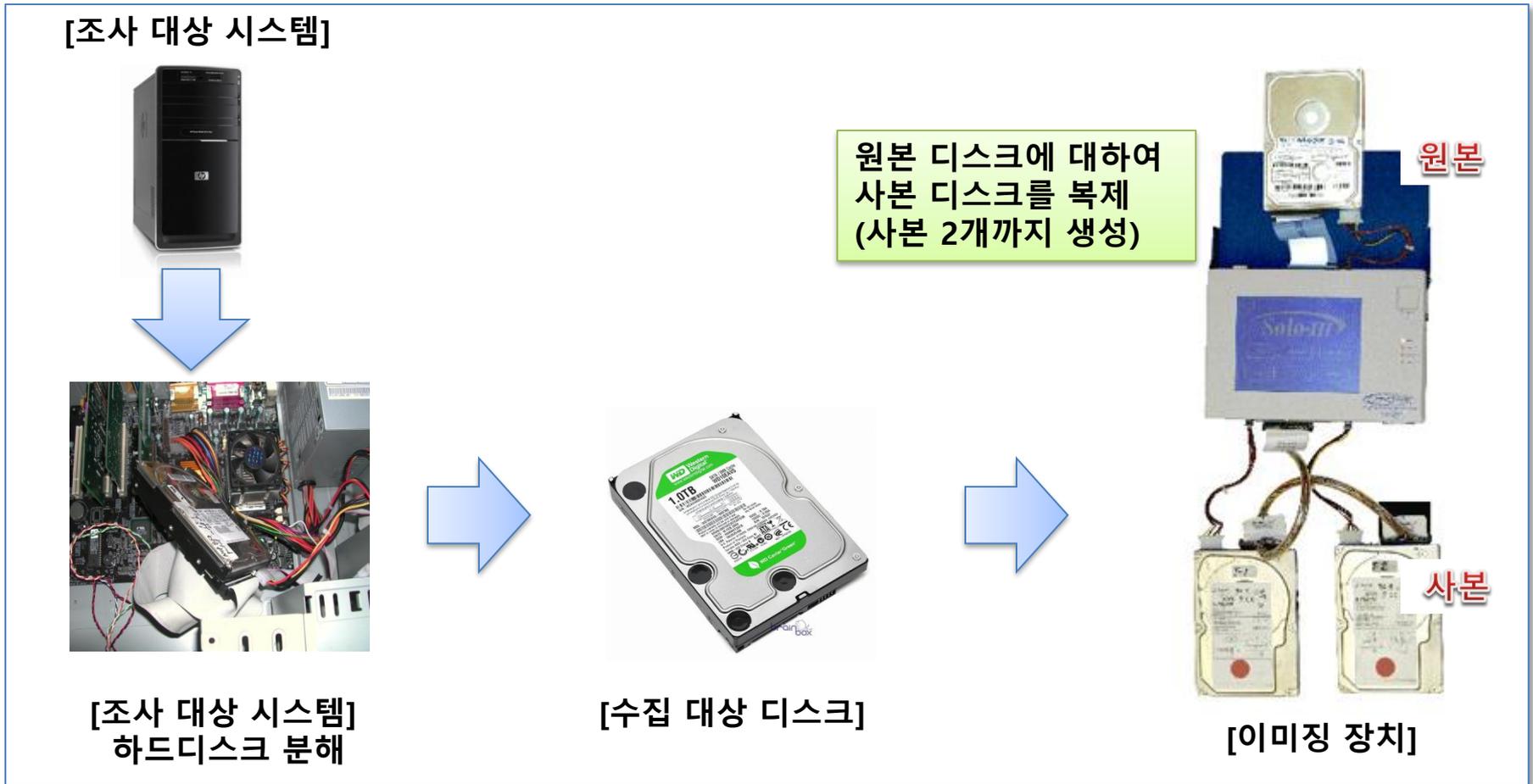
Logicube Talon

Logicube Dossier

ICS Image Masster
Solo3

ICS Image Masster
Solo4

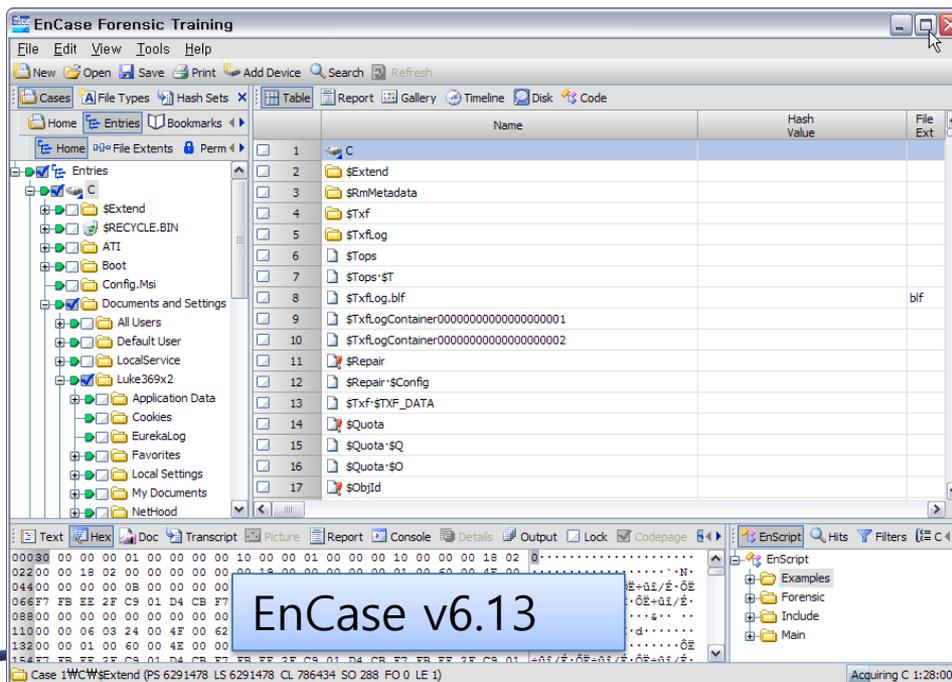
• 디스크 이미징 장비를 이용한 사본 생성 절차



• 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 OS 등의 플랫폼과 RAID 방식 지원



• 디스크 이미징 소프트웨어를 이용한 사본 생성 절차

[조사 대상 시스템]

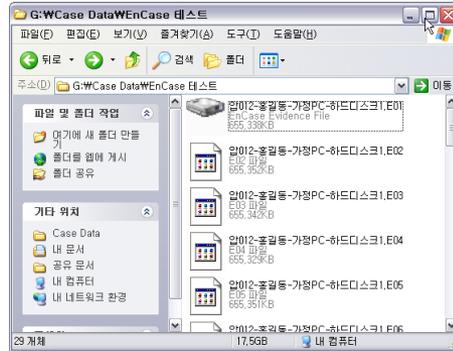


분해



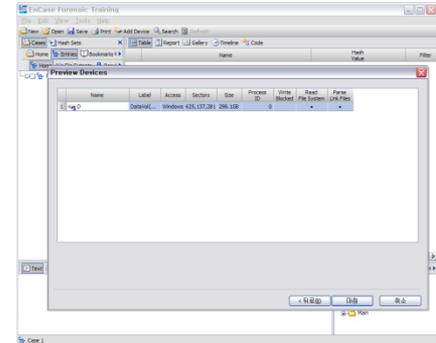
[수집 대상 디스크]
쓰기 방지 장치에 연결

[이미지 파일]



획득

[디스크 이미징 도구]



수집



[분석 시스템]

[쓰기방지 장치]
분석 시스템과 쓰기 방
지 장치 연결

디스크 이미지의 무결성 검증

디스크 이미지

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

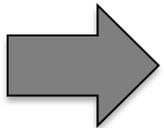
해쉬 및 오류 검증 알고리즘을 저장매체와 이미지에 적용

• 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 라벨을 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

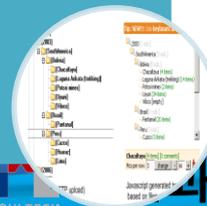
- 키워드 검색
- 파일 카빙
- 파티션 테이블 추출
- 미할당 영역에서 삭제된 파일 복구
- 조각난 데이터 복구 등

물리적 추출



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

논리적 추출



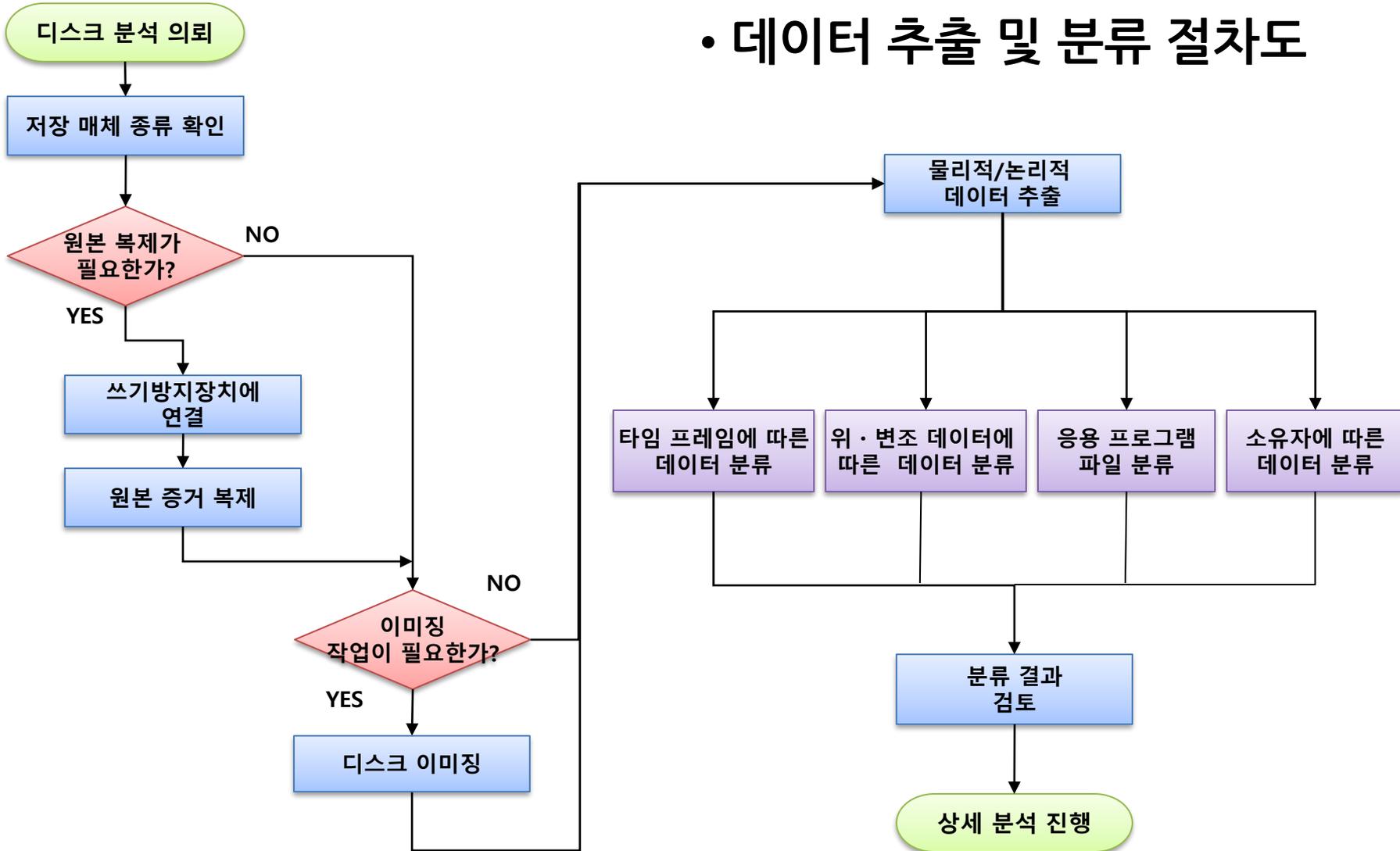
• 데이터 분류의 목적

- 조사에 필요한 데이터를 선별함으로써
.분석할 데이터의 양을 줄여, **효율적이고 신속한 분석**을 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

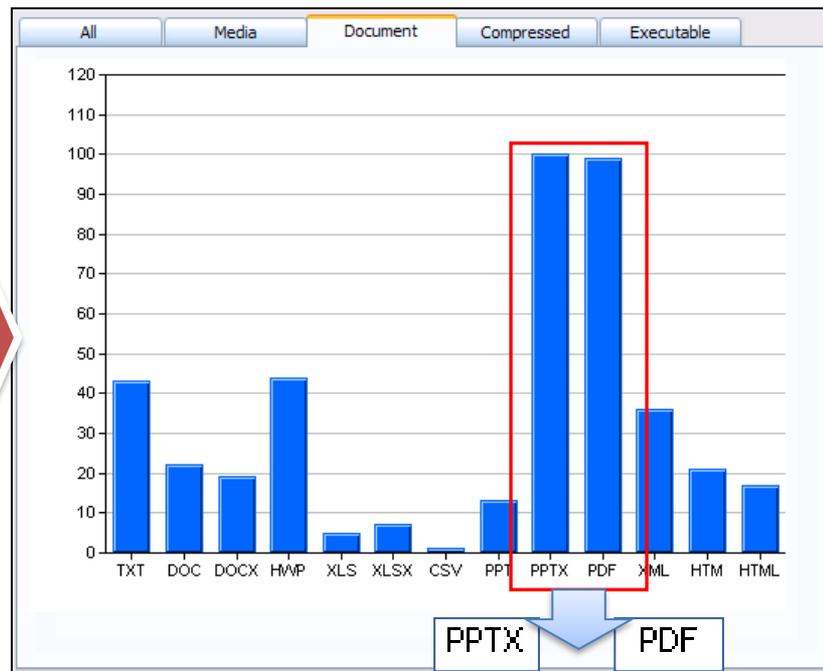
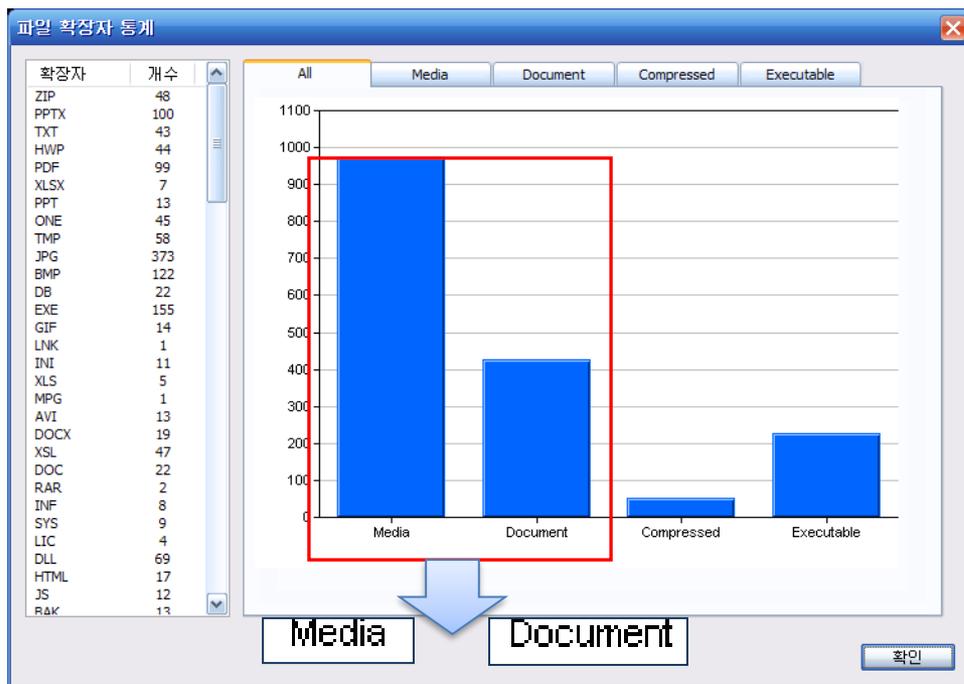
이름	File Type	만든 날짜	수정한 날짜	액세스한 날짜
Session 1-디지털포렌식 개론.pptx	Powerpoint Docume...	2010-04-01 17:30:48	2010-02-10 04:31:12	2010-04-02 01:26:04
Session 2-활성시스템 조사 방법.pptx	Powerpoint Docume...	2010-04-01 17:30:50	2010-02-10 04:26:28	2010-04-02 01:26:08
Session 3-윈도우 사용흔적 분석.pptx	Powerpoint Docume...	2010-04-01 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

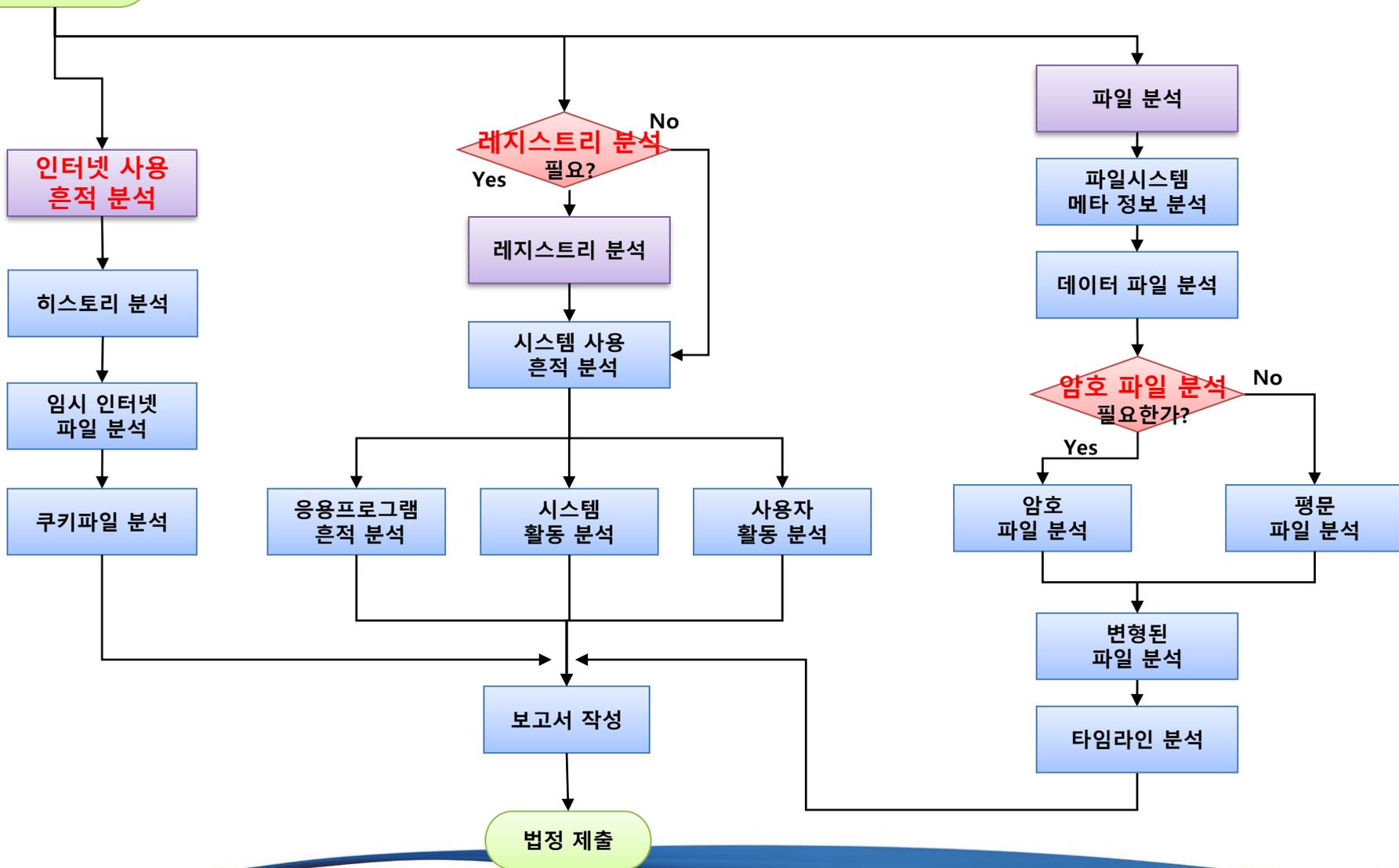
- 시스템 로그 데이터와 응용 프로그램의 로그에서 특정 타임프레임 내에서 수사와 관련된 이벤트가 있는지 확인
- 사건이 발생한 특정 시점의 전후 시간대를 기준으로 파일의 접근 및 변경 시간을 조사

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

The screenshot shows a Windows File History window titled 'WBFA'. It displays a grid of file access logs for various browsers: iexplore, firefox, chrome, and safari. The grid has columns for days of the month (4-31) and rows for dates from 2010/1 to 2010/12. A red box highlights the data for 2010/3. Below the grid is a search bar for '총무김밥, 서울' on Naver.

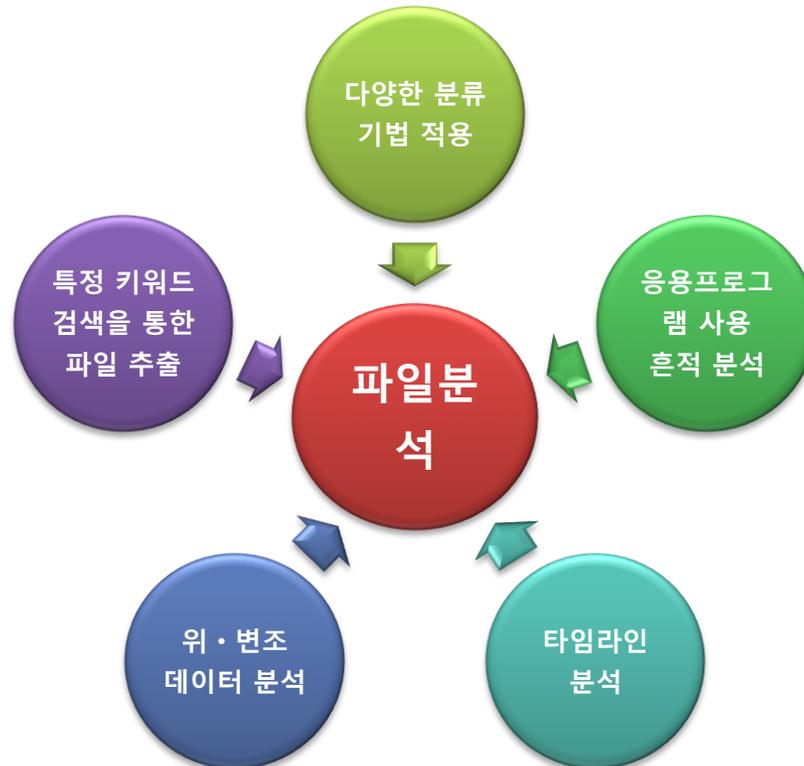
	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
2010/1																												
2010/2	8	16		1	25	18	1						2	12	1	4		5	5	3	5		5	4				
2010/3	29	71	7	2	20	74	125	130	7				277	367	117	434	175	24	8	47	495	139	363				682	56
2010/4																												
2010/5																												
2010/6																												
2010/7																												
2010/8																												
2010/9																												
2010/10																												
2010/11																												
2010/12																												

상세 분석 시작



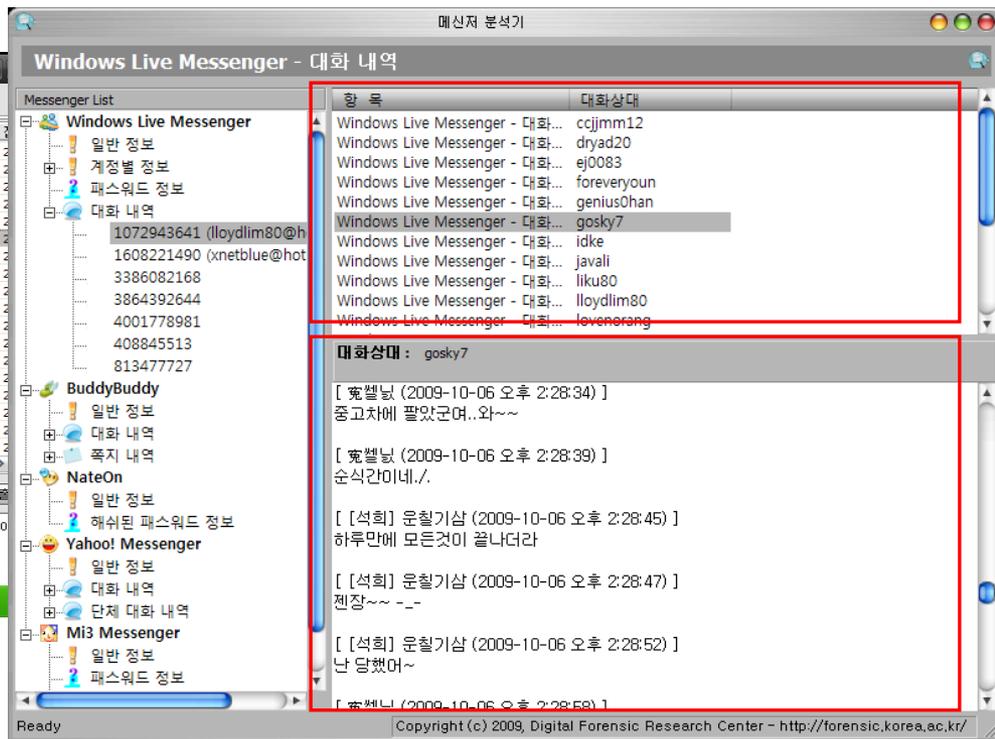
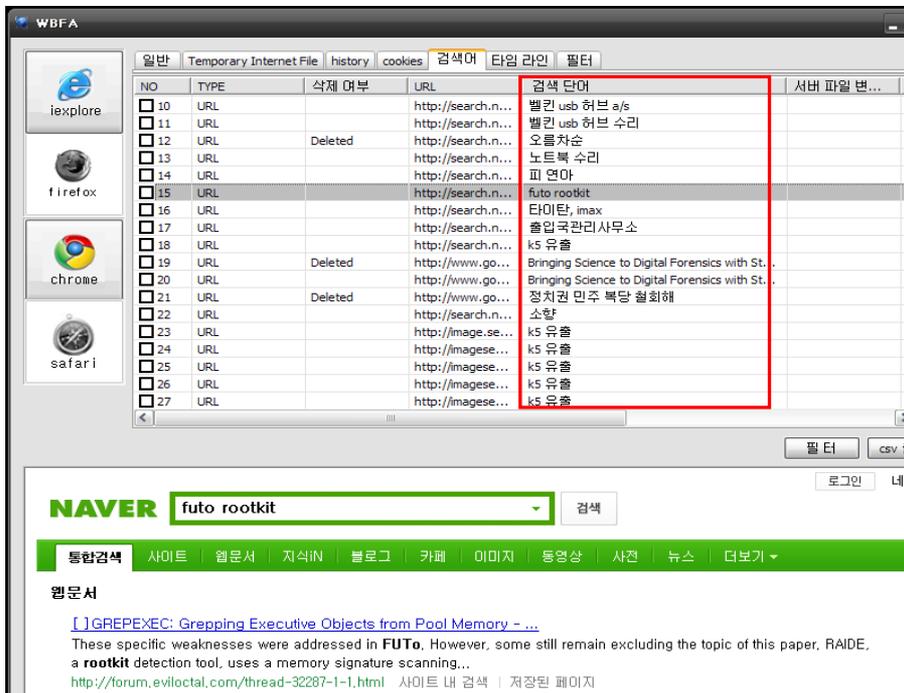
• 파일 분석

- 상세 분석 과정의 핵심으로, 사용자가 범위에 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**

실행순서	파일명	파일경로	최종실행시각
1	디지털포렌식 기술 최신 동향(v1...	D:\₩Luke의 문서₩내 발표 및 세미나 자료₩출강 자료₩[교수님 발표...	2010-04-02 01:27:01:203
2	[10년03월]삼성SDS-DiFront 시연...	D:\₩Luke의 문서₩#최근 작업₩#03월10년 바탕화면₩[3월24일]DiFron...	
3	[09년12월]LDFS v3소개.pptx	D:\₩Luke의 문서₩#최근 작업₩#[시큐박스]₩	
4	차세대_디지털_포렌식_기술과_...	D:\₩Luke의 문서₩내 발표 및 세미나 자료₩출강 자료₩[교수님 발표...	
5	제4장 디지털 증거(100319_v0.8)...	D:\₩Luke의 문서₩#최근 작업₩#04월10년 바탕화면₩[교재개발]₩디...	
6	[10년02월]디프론트 소개.pptx	J:\₩[삼성SDS]활성시스템 조사 기술 강의₩	
7	제5장_디지털_포렌식_조사_모델...	D:\₩Luke의 문서₩#최근 작업₩#04월10년 바탕화면₩	
8	제5장_디지털_포렌식_조사_모델...	C:\₩Documents and Settings₩₩Luke369x1₩₩바탕 화면₩	
9	제5장 디지털 포렌식 조사 모델(1...	D:\₩Luke의 문서₩#최근 작업₩#03월10월 바탕화면₩[03월 교재개발...	
10	디지털 포렌식 조사 모델(100322...	D:\₩Luke의 문서₩#최근 작업₩#03월10월 바탕화면₩[03월 교재개발...	
11	Digital Forensic_Last Full Version.pptx	D:\₩Luke의 문서₩내 발표 및 세미나 자료₩연구실 보관₩	
12	제5장 디지털 포렌식 조사 모델(1...	D:\₩Luke의 문서₩#최근 작업₩#03월10월 바탕화면₩[03월 교재개발...	
13	제3장_디지털_기기와_저장_매체...	D:\₩Luke의 문서₩#최근 작업₩#03월10월 바탕화면₩[03월 교재개발...	
14	[090925]LSI261 Forensics-1.pptx	E:\₩Flash 백업₩₩LUKE_FLASH 백업₩10년01월₩#연구자료₩	
15	제5장 디지털 포렌식 조사 모델(1...	C:\₩Documents and Settings₩₩Luke369x1₩₩바탕 화면₩	
16	[10년03월]삼성SDS-DiFront 시연...	C:\₩Documents and Settings₩₩Luke369x1₩₩바탕 화면₩	
17	#[2009년발표자료양식] 세부 주...	D:\₩Luke의 문서₩내 발표 및 세미나 자료₩	
18	[AKTS]활성시스템 조사기술 ver1...	D:\₩Luke의 문서₩내 발표 및 세미나 자료₩ 출강 자료₩09년 KISA-AKT...	

MS 오피스 2007 파워포인트로 작성한 최근 작성한 문서 내역

• 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

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 법정에서 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

8-7. 디지털 포렌식 조사 모델 비교

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 것 인지를 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 법정에서 제출할 증거 자료를 생성하는 과정

보고

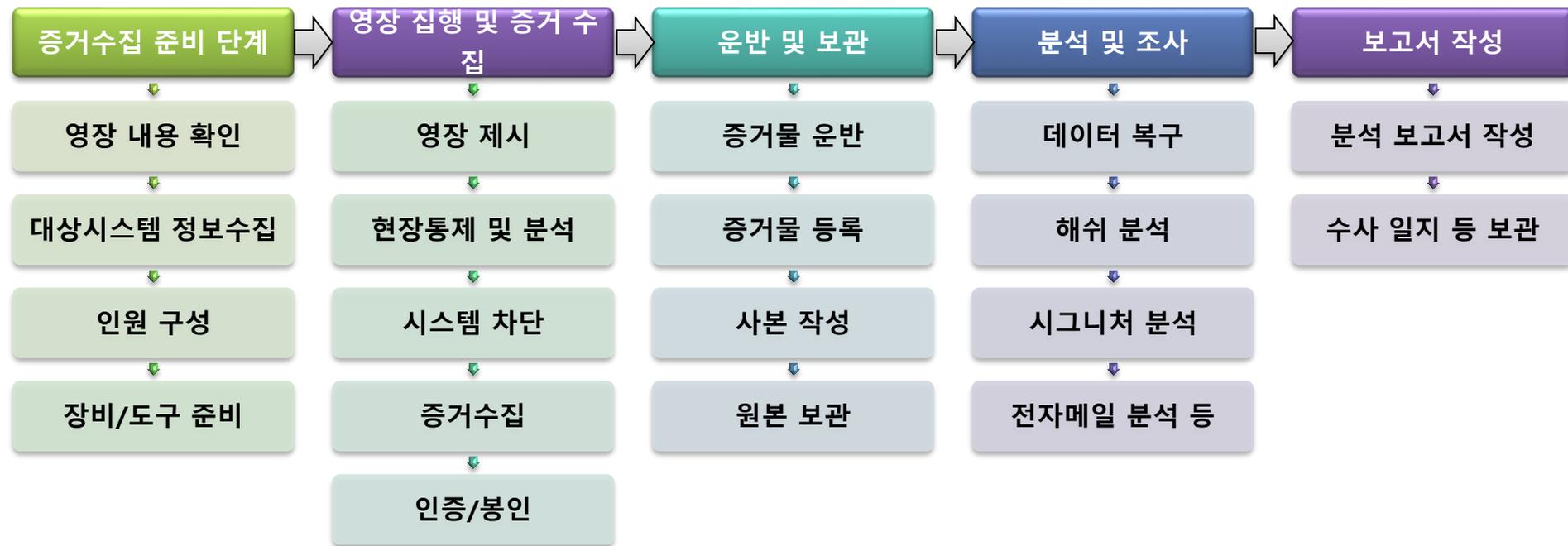
- 생성한 증거 자료가 법정에서 받아들여질 수 있도록 상세히 기록하고 그 과정들을 문서화

진술 및 증언

- 증거 자료, 기록, 관련 조서들을 법정에서 활용할 수 있도록 알기 쉽게 해석하고 이를 진술·증언

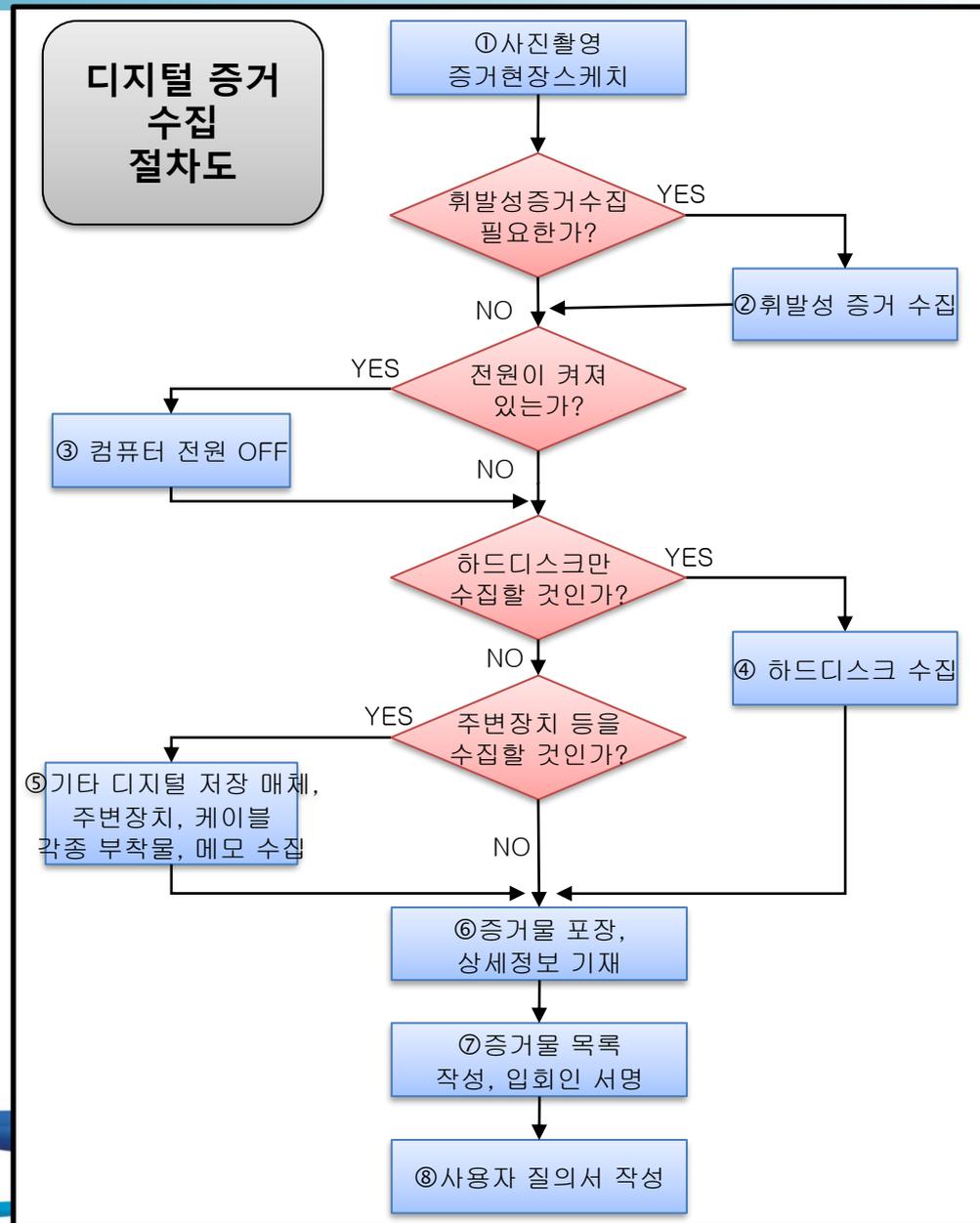
(국내)대검찰청 디지털증거 압수수색 모델

- 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 증거 처리가이드라인에서 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**

참고문헌

- 대검찰청 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
- 정익래, and 홍도원. "디지털 포렌식 기술 및 동향." (2007).
- 이상진, "디지털포렌식기술동향 및 발전전망", 고려대학교 Digital Forensic Research Center, 2016
- 곽병선. "디지털 포렌식 수사의 문제점과 개선방안." 법학연구 42 (2011): 171-191.

Q & A