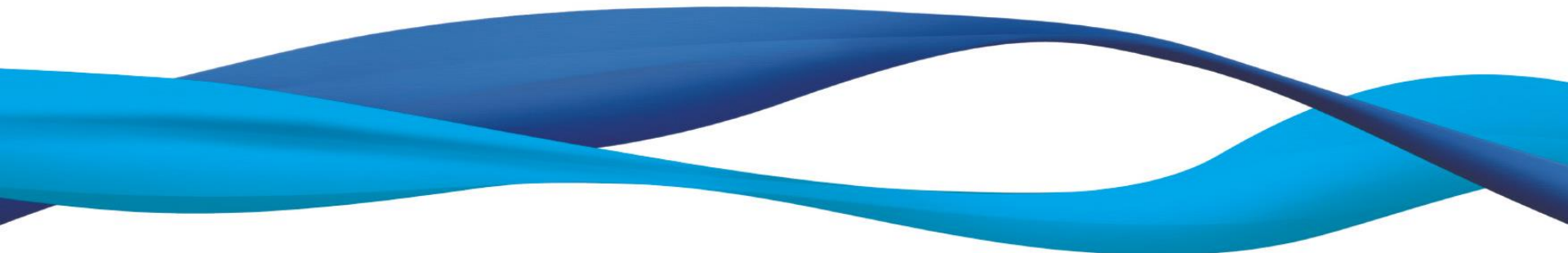


디지털 증거

김종성
국민대학교

Email: jskim@kookmin.ac.kr



목 차

1. 개 요

2. 디지털 증거의 개념 및 특성

3. 디지털 증거의 관련 법 규정

- 위법수집증거배제의 원칙
(Exclusionary Rule of the Illegally Collected Evidence)
- 전문법칙 (傳聞法則, Hearsay Rule)

4. 디지털 증거의 증거능력 요건

- 디지털 증거의 증거 능력을 보장하기 위한 특성
- 디지털 증거의 법적 허용성 보장을 위한 장치

5. 디지털 데이터의 증거 능력 관련 판례

개요

• 학습 목표

- 디지털 증거의 개념과 특성을 살펴보고, 법적 증거로서 허용 받기 위한 기본적인 원칙, 절차, 요건 등에 대해 학습한다.
- 실제 디지털 데이터가 증거가 쟁점이었던 판례를 살펴보고, 이를 통해 법적인 배경지식과 이해를 넓힌다.

• 학습 내용

- 디지털 증거의 개념과 특성
- 디지털 증거의 법적 허용성을 위한 원칙
- 디지털 증거의 법적인 보장을 위한 장치
- 디지털 데이터의 증거능력 관련 판례

디지털 증거의 정의

• 디지털 증거 관련 용어

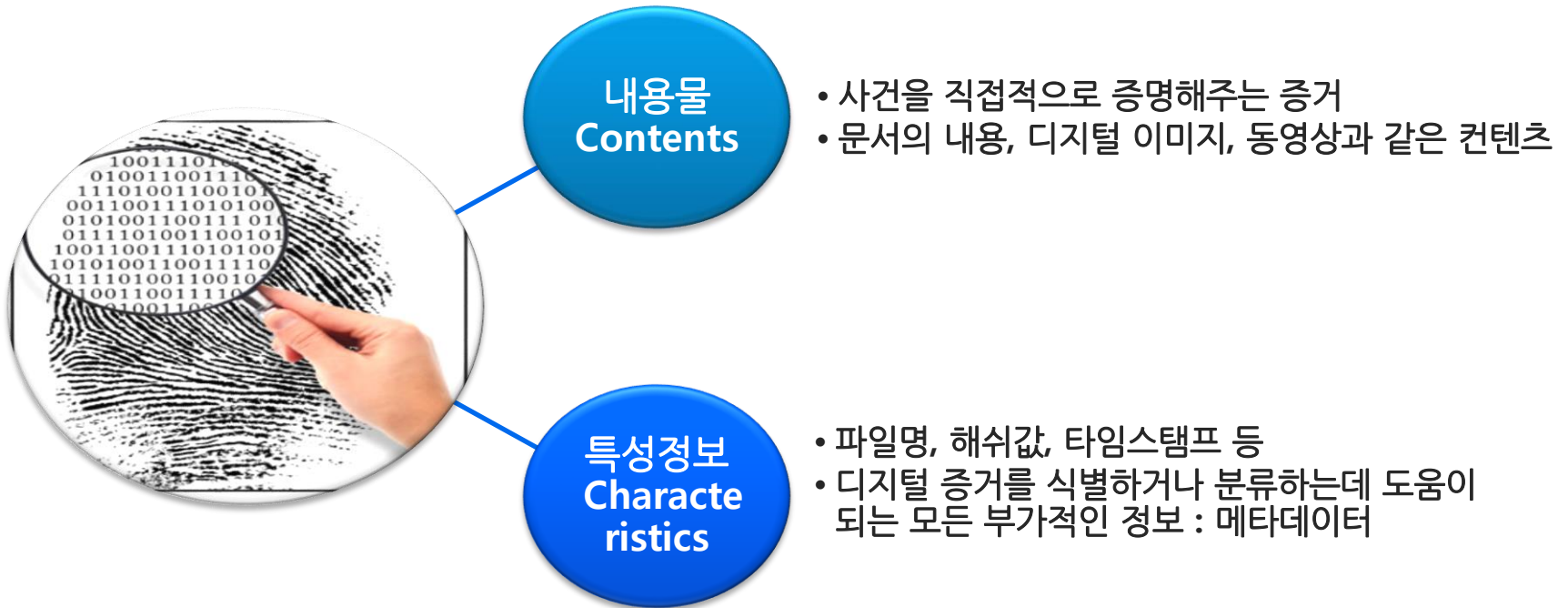
- 전자 증거(Electronic Evidence)
 - 전자기기에 저장되어 있거나 전자기기에 의해 전송되며, 증거로써 가치가 있는 정보와 데이터를 의미
- 전자 정보(ESI: Electronically Stored Information)
 - 미국에서는 전자정보 혹은 전자적으로 저장된 정보(Electronically Stored Information)라는 의미의 ESI라는 용어를 주로 사용

• 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 (1/3)

- 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



디지털 증거의 종류 (2/3)

자동으로 생성되는 디지털 증거

- ❖ 인터넷 사용기록
- ❖ 방화벽 로그
- ❖ 운영체제 이벤트 로그
등
- ❖ 각종 메타 데이터

인위적으로 생성되는 디지털 증거

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

디지털 증거의 종류 (3/3)

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 증거의 유형

디지털 증거의 유형

1) 내용물과 특성정보

내용물 : 사건을 직접적으로 증명해주는 증거.

특성정보 : 파일명 , 해쉬값 , 타임스탬프 등 디지털 정보를 식별하거나 분류하는데 도움이 되는 모든 부가적인 정보인 메타데이터를 말함.

2) 보관증거와 생성증거

보관증거 : 사람의 사상이나 감정을 표현하기 위하여 사람이 직접 작성한 증거.

생성증거 : 인간의 개입 없이 디지털 기기가 동작하는 과정 중에 자동으로 생성된 증거.

-일반적으로 내용물은 보관증거 , 특성정보는 생성증거로 볼 수 있다.

(내용물 = 보관증거 , 특성정보 = 생성증거)

-보관증거인 내용물은 작성자의 동의가 없는 한 그 자체로는 법적증거로 인정될 수 없다. 작성자가 부인한 경우 생성증거로서의 특성정보에 의해 증명되어야 디지털 증거로서 법정에서 인정 될 수 있다.

디지털 데이터의 특징 개관

비가시성, 비가독성

- 눈에 보이지 않는 0과 1의 조합인 디지털 형태로 저장되어 있어 그 자체는 육안 식별이 불가능한 잠재성, 은닉성, 불가시성, 불가독성을 갖는 무체물이므로 그 발견과 증명이 어려움

취약성 (변조 가능성)

- 오류에 의한 손상이나 의도적인 변조가 쉬우며, 변조 사실을 찾아내기 어려운 취약성 존재
- 사후에 법정에서 증거의 조작여부, 증거 획득 절차의 적정성 등을 고려해야 함

복제 용이성 (매체 독립성)

- 원본과 동일한 내용으로 쉽게 복제할 수 있으며, 원본과 복제본의 구별 어려움

대량성

- 기업 전산 회계자료, 데이터베이스 자료나 파일 서버 문서자료 등은 데이터 양이 수십 테라바이트에 이를 만큼 양이 방대함

디지털 데이터의 특징 개관

전문성

- 디지털 방식으로 자료를 저장하고 이를 출력하는데 컴퓨터 기술과 프로그램이 사용됨
- 디지털 증거의 수집과 분석은 전문적인 기술이 사용되므로, 디지털 증거의 압수·분석 등에 있어 포렌식 전문가가 필수적임

휘발성

- 컴퓨터 메모리나 네트워크 상에서만 일시적으로 존재하는 휘발성 데이터가 존재하며, 디지털 증거 압수과정에서 사라지지 않도록 각별히 주의해야 함

초국경성 (네트워크 관련성)

- 디지털 증거는 네트워크로 상호 연결되어 있을 수 있으며, 장소에 구애 받지 않아 원거리 또는 타국 소재로 인한 문제가 발생할 수 있음

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
 - 기존의 판례는 위법행위 여부와 상관없이 비진술증거에 대해서는 증거능력이 인정되었지만, 최근에는 형사소송법 내 308의2조에 **"적법한 절차에 따르지 아니하고 수집된 증거는 증거로 할 수 없다"**라고 명확히 위법수집증거배제원칙을 규정하고 있음
 - ✓ 증거자료 수집 과정에서 엄정한 적법절차 준수
 - ✓ 당사자의 기본권을 보호하면서 수사에 필요한 최소한도 범위 내에서 증거 수집.
 - ✓ 자료손상 최소화, 증거의 무결성을 확보하면서 수집 해야 함.

위법수집증거능력배제원칙

- ✓ 압수, 수색 영장이 한정하는 영역 내에서 조사 진행. (선별수집 관련)

형사소송법 제215조 제1항

검사는 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한하여 지방법원판사에게 청구하여 발부 받은 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.

형사소송법 제106조 제3항

법원은 압수의 목적물이 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체인 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.

위법수집증거능력배제원칙

- ✓ 압수, 수색 영장이 한정하는 영역 내에서 조사 진행. (참여권 관련)

형사소송법 제121조(영장집행과 당사자의 참여)

검사, 피고인 또는 변호인은 압수수색영장의 집행에 참여할 수 있다.

형사소송법 제122조(영장집행과 참여권자への 通知)

압수수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다.

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 증거법상의 원칙
- 원진술자가 말한 진술상의 취약점을 파악할 방법이 없음
- 현행 형사소송법 제310조의2에서는 이러한 전문증거의 증거능력을 원칙적으로 부인

전문법칙의 예외

- 전문법칙의 예외 기준

- 신용성의 정황적 보장

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

- 필요성의 원리

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

전문법칙의 예외

• 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
- 따라서 내용의 진실성을 입증하기 위해서는 전문법칙의 관계에 유의하여 증거능력에 대한 검토가 필요
- 디지털 증거도 적절한 조건을 갖추어 경우 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
 - 이러한 디지털 데이터 자체가 증거로서 제출되는 경우에는 진술증거가 아니므로 전문법칙이 적용될 여지가 없음
 - 또한 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

전문법칙의 예외 조항으로 디지털 증거

형사소송법 제 313조

① 전2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것 (피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보로서 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다. 이하 이 조에서 같다)은 공판준비나 공판 기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판 기일에서의 그 작성자의 진술에 의하여 그 성립의 진정함이 증명되고 **그 진술이 특히 신빙할 수 있는 상태에서 행하여진 때에 한하여 피고인의 공판준비 또는 공판 기일에서의 진술에 불구하고 증거로 할 수 있다.** <개정 2016.5.29.>

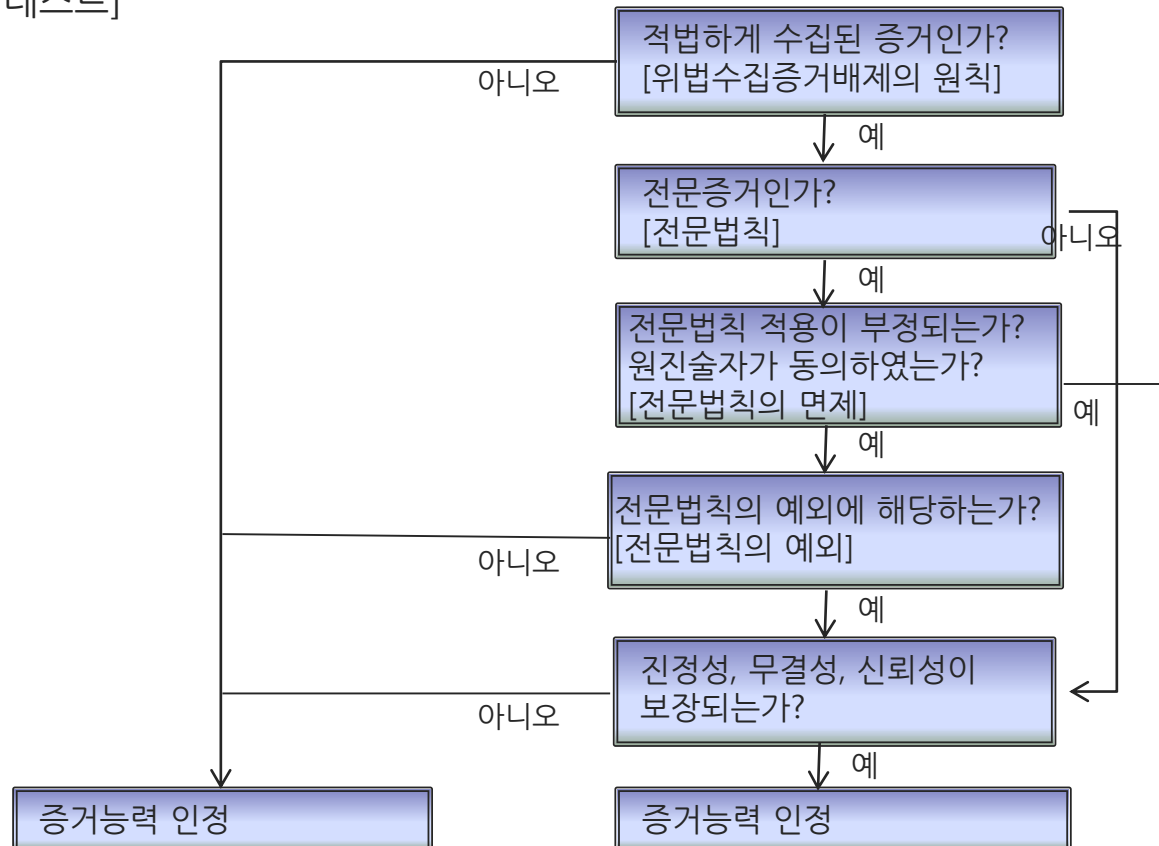
② 제1항 본문에도 불구하고 진술서의 작성자가 공판준비나 공판 기일에서 그 성립의 진정을 부인하는 경우에는 **과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다.** 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판 기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다. <개정 2016.5.29.>

③ 감정의 경과와 결과를 기재한 서류도 제1항 및 제2항과 같다. <신설 2016. 5. 29.>

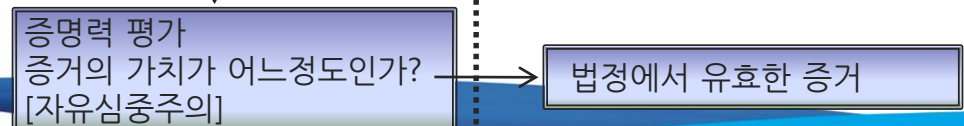
디지털 증거의 증거능력 과정

- 증거능력 : 법정에서 유효한 증거로 인정받는다.는 것은 해당 디지털증거가 증거능력을 갖고, 충분한 증명력을 갖는 다는 것이다.

[증거능력 테스트]



[증명력 테스트]



디지털 증거의 증거능력 (1)

디지털 증거의 증거능력 요건

-디지털 증거의 증거능력을 보장하기 위한 특성

(디지털 증거의 증거능력을 보장하기 위한 특성으로는 **진정성**, **무결성**, **신뢰성**, **원본성**이 있고 이 특성들이 기본적으로 보장되어야 한다)

디지털 증거의 증거능력 (2)

1) 디지털 증거의 진정성 (Authenticity)

증거의 진정성 증명이란 **법정에 제출할 증거가 요증 사실을 설명하기 위한 바로 그 증거**라는 사실을 말한다.

진정성의 보증을 위해서는 작성자, 수신자 및 생성일시와 같은 디지털 증거의 생성 당시의 부가 정보는 물론 활용단계의 부가정보가 보존될 필요가 있으며 디지털 증거가 증거 수집 이후 보관 단계에서 위조되거나 다른 파일로 바뀌치기 될 가능성을 없애기 위해 디지털 증거 수집 단계에서 법원제출 단계에까지 연계 보관 로그를 기록해야 한다.

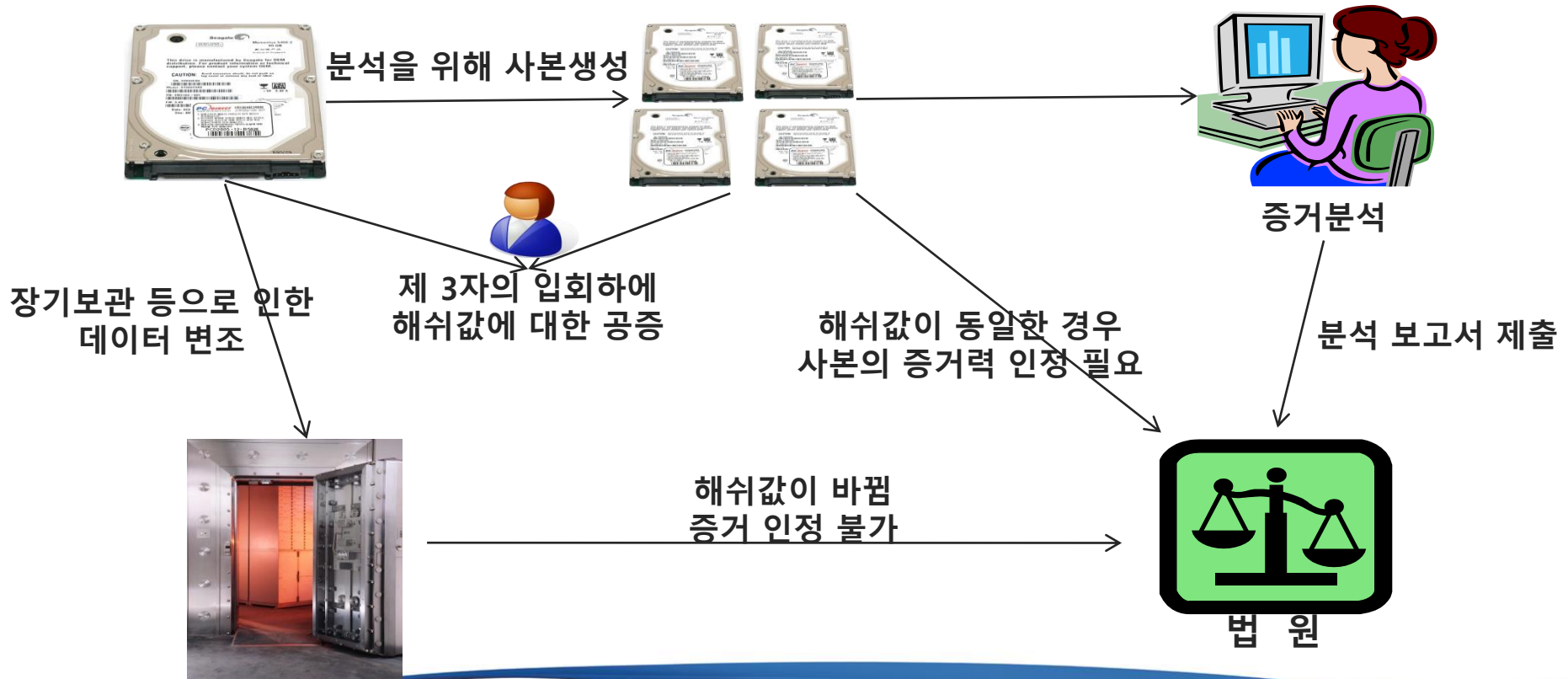
~ 연계 보관성 유지를 위한 문서에 기록되어야 할 정보 ~

- 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

디지털 증거의 증거능력 (3)

2) 디지털 증거의 무결성

-디지털증거가 원본으로부터 수집되어 보관, 분석되는 과정에서 부당한 수정, 변경, 손상이 없도록 유지되어야 하며, 이러한 수정, 변경, 손상이 발생하지 않았음을 검증할 수 있어야 한다는 것을 의미.



디지털 증거의 증거능력 (4)

3) 디지털 증거의 원본성

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

(1) 미국의 최량 증거 규칙 (Best Evidence Rules)

- 영미권에서 발달한 증거 원칙으로 **문서의 원본증거가 증거로서 그 내용을 증명하기 위해 제출되어야 한다는 것이다.**
- 미국 최량 증거 규칙은 연방증거규칙에서 명시 되어 있다.
- 서류, 기록물 또는 사진의 내용을 증명하기 위하여 문서, 기록물, 사진의 원본이 요구된다.

~ 복제물도 법정 증거로 허용되는 경우 ~

- **원본이 삭제되거나 멸실된 경우** : 해쉬 함수와 적절한 이미지로 검증된 복제본임을 쉽게 입증할 수 있음
- **원본을 획득하기 힘든 경우** : 상대방에게 돌려줘야 하거나 상대방이 원본을 파괴한 경우
- **상대편이 원본을 소유하고 있는 경우** : 상대방이 해당 원본증거에 접근하는 것을 거부한 경우

디지털 증거의 증거능력 (5)

(2) 국내의 원본성 규칙

- 국내 형사소송법은 미국과 달리 **최량증거원칙을 채택하지 않으며**, 단지 **압수한 하드 디스크 등 저장 매체의 원본에 저장된 내용과 출력한 문건이 동일한지 여부**가 문제 될 뿐이다.
- 출력물이 **원본인지 여부와 관계없이 동일성이 인정**되면 일단 증거 능력을 인정할 수 있다는 입장을 취하고 있음.

4) 디지털 증거의 신뢰성

- 증거 데이터의 분석 등 처리 과정에서 디지털 증거가 위, 변조 되거나 의도되지 않은 오류를 포함하지 않았다는 것을 의미한다.

~ 제도적 장치들과 디지털 증거의 신뢰성 요건의 관계 ~

-디지털 포렌식 표준 가이드 라인 수행

(디지털 증거가 법적 증거로서 허용 되려면 진정성과 무결성을 보증해줄 수 있는 표준화된 순서와 절차가 필요한데 공신력 있는 기관에서 논리적이고 체계화된 디지털 증거 처리 표준 가이드 라인 수행 필요)

-디지털 증거 수집 장비의 검증

(디지털 포렌식 도구들에 대한 검증을 수행해야 하며, 이를 위해서 검증 항목 및 절차 수립, 디지털 포렌식 도구 검증을 위한 테스트 베드 구축을 통하여 사용자로 하여금 신뢰 할 수 있는 도구를 선택할 수 있도록 해야 한다.)

디지털 증거의 증거능력 (6)

-디지털 포렌식 조사자의 인증

(포렌식 도구 사용능력 및 디지털 증거에 대한 이해와 그 수집 절차의 숙지 여부를 평가하는 조사자 인증 제도를 구축하여 일정 수준 이상의 조사자만이 디지털 증거 수집 작업에 관여할 수 있도록 해야한다)

-디지털 증거 분석 시설의 검증

(수집된 디지털 증거를 보관하고 분석하는 디지털 증거 분석실에 대한 검증과 인정이 수행 되어야 한다)

국내사례 (1)-영남위 사건

• 부산고등법원 선고 99노123 [국가보안법위반]

- 수사도중 디스켓에서 북한을 찬양한 문서 파일이 발견됨, 이를 국가보안법 위반 찬양 고무등의 혐의로 기소한 사건

- 대법원 판례 요지

- "컴퓨터 디스켓이 들어 있는 물건이 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 적용된다고 할 것이고, 따라서 형사소송법 제313조 제1항에 의하여 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다"

국내사례 (2)-일심회 사건

- 대법원 2007.12.13 선고 2007도 7257 판결 [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
 - 디지털 저장매체 원본과 출력한 문서의 동일성이 인정될 것
 - 디지털 저장매체 원본이 문서 출력시까지 변경되지 않았음이 담보될 것
 - 하드카피나 이미징으로부터 출력된 문서라면, 원본과 이들 사이의 동일성도 인정되어야 하고, 이를 확인하는 컴퓨터의 정확성과 조작자의 전문성도 담보될 것
 - 압수된 디지털 저장매체로부터 출력된 문건을 진술증거로 사용하려면 기재내용의 진실성에 관해 전문법칙이 적용됨

Q & A