

8장. 디지털 증거

박종현

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech.ac.kr

개 요

- 학습목표

- 디지털 포렌식의 의미와 전반적인 내용을 이해하고 조사과정에서의 일반 원칙 및 수행과정에 대해서 학습한다.
- 디지털 증거에 대해 이해한다.

- 학습 내용

- 디지털 포렌식
- 디지털 포렌식의 일반 원칙
- 디지털 포렌식의 수행과정
- 디지털 증거의 종류 및 특징

1. 디지털 증거의 개념 및 특성
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

7-1. 디지털 증거의 개념 및 특징

디지털 증거의 개념

- 디지털 증거 관련 용어

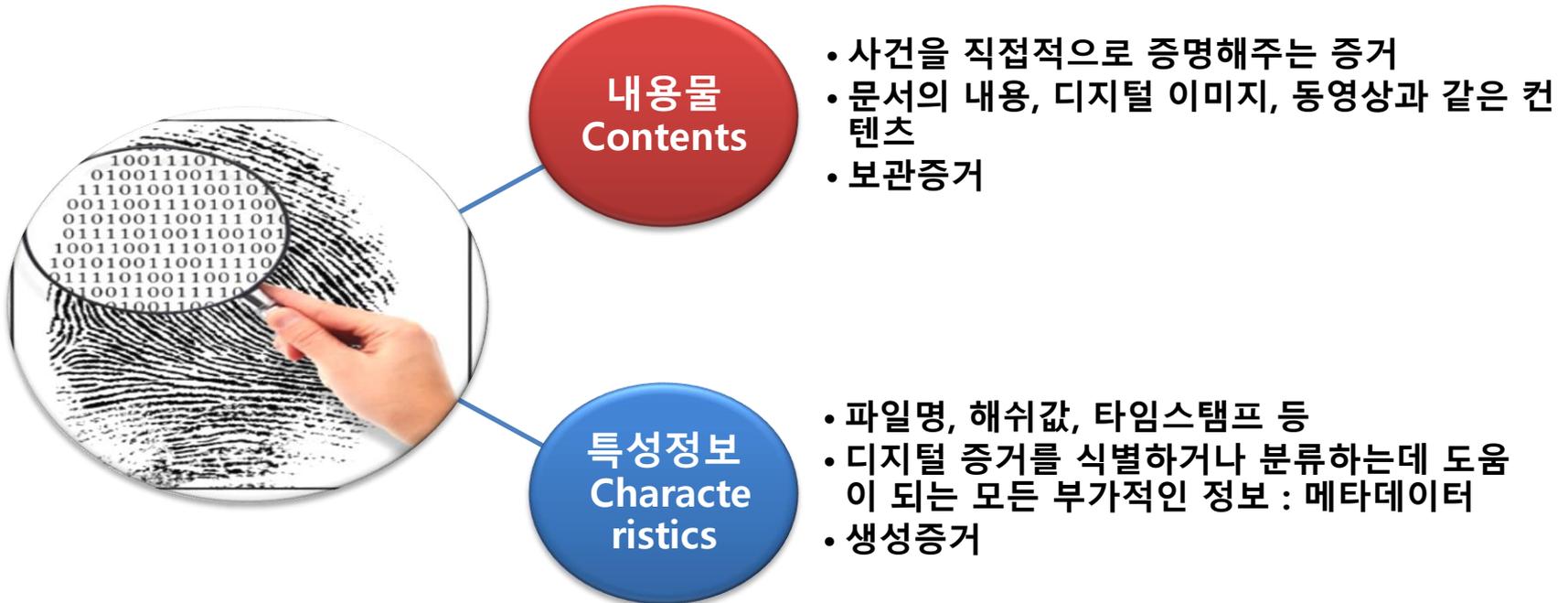
- 전자 증거(Electronic Evidence)
 - 전자기기에 저장되어 있거나 전자기기에 의해 전송되며, 증거로써 가치가 있는 정보와 데이터를 의미
- 전자 정보(ESI: Electronically Stored Information)
 - 미국에서는 전자정보 혹은 전자적으로 저장된 정보(Electronically Stored Information)라는 의미의 ESI라는 용어를 주로 사용

- 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



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

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 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 테러바이트에 이를 만큼 양이 방대함

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 데이터의 특성

- 비가시성(非可視性), 비가독성(非可讀性)

- 디지털 저장매체에 저장된 디지털 증거 그 자체는 사람의 시각으로 바로 인식이 불가능
- 따라서 일정한 변환절차를 거쳐 모니터 화면으로 출력되거나 프린터를 통하여 인쇄된 형태로 출력되었을 때 가시성과 가독성을 가짐
- 따라서 디지털 증거와 출력된 자료와의 동일성 여부가 중요

- 취약성

- 디지털 증거는 삭제·변경 등이 용이
- 하나의 명령만으로 하드디스크 전체를 포맷하거나 파일 삭제가 가능하며, 파일을 열어보는 것만으로 파일 속성이 변경됨
- 수사기관에 의한 증거조작의 가능성도 배제할 수 없으므로 디지털 증거에 대한 무결성 문제가 대두

비가시성(非可視性), 비가독성(非可讀性)

```

7A83 9175 708D 6C73 8465 6B7E 6165 785E z..u|.l$.ek~aex"
6477 6064 775D 6475 5E82 7558 6273 5F63 dw|dw|du"bu[bs_c
755C 6374 5060 7258 5F8E 5A5E 705A 6170 u|wct# rX_nz~pzap
5E62 745F 6473 5A60 6D72 7881 4548 5600 "bt_dsZ~mrv.EHV.
010C 5A5D 6B63 6976 5C5F 6D58 616E 5B60 .Z|kciV~mLan[
6F58 616E 5061 705A 6170 5061 705A 6170 o|an#apZap#apZap
5060 7259 606F 5B64 6E5A 656D 5B64 6E59 #~rY o|dnZem|dnY
636D 5A63 6D57 616B 575F 6C56 5F6C 5961 cmZcmWakW~lV~lYa
6E57 606D 585F 6E57 606E 585F 7057 5F70 nW~mX_nW~nX_pW~p
5960 7158 6071 565D 6E55 5E8C 565D 6E55 Y~qX~q|nU~lV~nU
5E8C 565D 6E55 5E8C 565D 6E55 5E8C 555C "lV~nU~lV~nU~lU#
6D54 5D6B 555C 6D56 5F6D 575E 6F55 5E6C m|]kLWmV~mW~oU~l
555C 6D55 5C6B 6F72 801A 1E29 181B 295F U#mL#k#or...).).)
6572 5061 704D 5A63 585F 7054 5C6D 545B er#apMTCX~pT#mT[
6C53 5B6C 555C 6D55 5C6D 555C 6D55 5C6B IS[|U#mL#mL#mL#k
5B5B 6A54 5B6C 595D 7056 5C6F 585C 6F56 V|]T[|Y|pV#oX#oV
5C6F 595D 7057 5D70 585C 6F55 5B6E 585C #oY|pW|~pX#oU|nX#
6E58 5F70 5A5E 7055 5C6D 565A 6C56 5D6E nX~pz~pU#mVZ|V|n
595D 6F58 5D6C 6E6E 7022 2831 1315 2061 Y|oX|]kn|"&l...a
6472 6263 715C 5F6E 5A5C 6E5A 5E70 5A5C dr|bcd#~nz#Wnz~pzW
6E59 5D6F 5C5E 7059 5D6F 585C 6E58 5D6C nY|o#~pY|oX#mX|]
585D 6C39 5E6D 5A5F 6E3A 5F8E 5B6D 6F59 X|Y~mZ~nz~n[|oY
5E6D 5B6D 6F39 5E6D 5C5E 705A 5F6E 5C5E "m|]oY~m#~pz~n#~
705A 5F6E 5B6D 6F58 5D6C 5A5C 6E56 606F pz~n|]oX|]Z#n|]o
    
```



```

FABA 42B8 F702 817D A0A6 A8D8 4A7A 0225 .B...).}~Jz.%
511F 73CA 5D88 7F94 2938 C090 6480 DA34 Q..s|)...8...d..4
EBD1 9F96 493D C6CD E536 3BAF AE62 7B82 .|...|=...}.b{.
6F33 58E5 8EAB 16ED E49D 6DF7 BDC6 6095 o3X...}.m...}.
E4D5 7D03 6BF1 EC5F D6C7 7D4B 728B 8B57 ..}....}.}Kr..W
65FA AF71 D955 7CDB E476 B72C C9A6 3F18 e..q.U|...v...?.
ACBE 0693 E416 27EF 9E89 3317 2C30 F05D .}....}.i3..0.]
3605 F34E 455C 9DE7 A037 4283 CFA9 C76B 6..NEW...7B...k
AB63 ADA7 DF18 82DA 6413 71DB 5EB0 A438 ..}....}.d.q...8
D94E 8752 924B 8DDB 7A77 83A1 9E2A 70CB .N.R.K..zw...*p.
DD92 BC73 AC4C EAD2 FE66 3AAF 13EC 24A9 .S..L...f:...$.
4360 0015 74D0 7585 20A7 84E5 F451 80AB C~.t.u...}.0..
2B18 F9DE 1AFA FC72 207D 37AD 7988 3E4C +.....r }7.y>L
EB47 1AF2 CBAB 841A 708C 23CD 731F 6BF9 .G.....|]#s.k.
E768 4B87 5A5C FF8E 0A8E 4788 E6B2 AE9B .hK.ZW...G...
0856 5DEB 8175 81D2 651E B263 F446 49FE .V|...u...c..C.
3B5E 1136 ADBF 0E64 5632 BE9B 0309 34AF .}6...dV...4.
AC03 48BF D4D1 824F BARD 7932 77B1 CCEC .H...0..y2w...
23F4 3901 F917 94AC A3B4 7E31 9079 9FD6 #.9.....1.y.
5289 7525 35AB 2EE4 97BA D263 AC2B 054A R.u%5...c..t..J
0710 EA92 AE74 E0D3 F935 C7C3 8008 06D8 .}.t...5...
9ECC 695E B317 78CD 5F51 B7F0 0085 4FF0 .}.x..0...0.
3599 5DC7 6BFE 6975 6DBE CE8B 6650 E13F 5..k..um..kfp.?
55FB C80A FFB3 C2B7 F234 955D C866 FE71 U.....4..k.
    
```



2008 Anti Forensic Template.hwp [D:\#재판 논문W2008년 언더포렌식대응기술연구소 논문] - 한글과컴퓨터 한글

2. 소스단원 작성 기법

소스단원의 번호(예 1.1.1)는 후면고적 9pts, 강령 95%, 자간-5%로 작성한다.

(예) 계속하여 논문을 작성한다.)

4. 그림과 표

이 장에서는 그림과 표의 형식에 대하여 설명하겠습니다. 그림과 표의 제목/설명은 국문으로 설명하도록 하고, 글자모양은 신명궁고적 8pt, 강령 95%, 자간 -5%, 줄간격은 130%이며, 포인트의 내용은 신명궁명고 8pt, 강령 95%, 자간 -5%, 줄간 130%로 한다.

1. 그림의 사용 예

그림 1은 사용 예로서 한글 코딩에서 제공하는 정선편집 기능을 이용하여 작성합니다. 그림과 표는 가능한 한 육안으로 분명히 식별할 수 있을 정도로 크기가 적당하여야 하며, 육안으로 식별되지 않을

그림 1. 그림에 대한 설명이 들어갑니다. 그림제목과 표제 목은 신명궁고적 8포인트, 강령 95%, 자간-4% 줄간격 130% 한다. (예)이러는 그림 자리를 공간으로 비어 놓으십시오.)

표의 사용도 그림과 동일한 형식을 이용합니다. 표의 장선은 표의 상단(좌측)에 위치합니다. 아래의 표 1(예)과 같이 표는 논문 상단에 위치하고 있기 때문에 위와 0mm와 아래에서 5mm 정도의 여백을 줍니다. 한데로 논문 하단에 위치하고 있다면 아래에 0mm 위와 5mm의 여백을 주어야 합니다.

2. 표의 사용 예

표 1. 시뮬레이션 파라미터

Item	Value
Terminal data rate	20 kbps
Packet arrival rate	

- 복제 용이성(매체독립성)

- 디지털 증거는 '유체물'이 아니고 각종 디지털저장매체에 저장되어 있거나 네트워크를 통하여 전송 중인 정보 그 자체
- 정보는 값이 같다면 어느 매체에 저장되어 있든지 동일한 가치를 가지며, **디지털 증거는 사본과 원본의 구별이 불가능함**

- 대량성

- 저장 기술의 발전으로 방대한 분량의 정보를 하나의 저장 매체에 모두 저장할 수 있게 되었으며, 회사의 업무처리에 있어 컴퓨터의 사용은 필수적이고, 모든 업무 자료는 컴퓨터에 저장됨
- 또한 **대형 서버 시스템이나 파일 서버가 수사 대상일 경우, 수집할 데이터 양이 방대하며, 압수 대상일 경우 업무수행에 지장을 줄 수 있어 업무 연속성에 지장을 주는 경우**

- 전문성

- 디지털 방식으로 자료를 저장하고 이를 출력하는데 컴퓨터 기술과 프로그래밍이 사용됨
- 디지털 증거의 수집과 분석에도 전문적인 기술이 사용되므로, 디지털 증거의 압수·분석 등에 있어 포렌식 전문가가 필수적임
- 전문성의 부재는 디지털 증거에 대한 신뢰성 문제가 대두됨

- 휘발성

- 디지털 증거에는 컴퓨터 메모리나 네트워크 상에서만 일시적으로 존재
- 휘발성 데이터는 사건이 발생한 시점의 상태를 파악할 수 있는 중요한 정보이므로, 디지털 증거 압수과정에서 사라지지 않도록 각별히 주의해야 함

- 초국경성(네트워크 관련성)

- 디지털 환경은 각각의 컴퓨터가 고립되어 있는 것이 아니라 인터넷을 비롯한 각종 네트워크를 통하여 서로 연결되어 있음
- 따라서 디지털 증거는 공간의 벽을 넘어 전송되고 있으며, 그 결과 재판관할권을 어느 정도까지 인정할 것인지 국경을 넘는 경우 국가의 주권문제까지도 연관됨

7-2. 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, 최근에는 형사소송법 내 308의2조에 **"적법한 절차에 따르지 아니하고 수집된 증거는 증거로 할 수 없다"**라고 명확히 위법수집증거배제원칙을 규정하고 있음

- 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**
 - 원 진술과 동일한 내용의 진술을 구하는 것이 불가능하거나 현저히 곤란하기 때문에 비록 전문증거라고 하더라도 이를 사용하여 실체적 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 문건 → 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 갖출 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
 - 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

7-3. 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 인정됨을 뜻함

무결성(Integrity)

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

신뢰성(Reliability)

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

원본성(Originality)

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

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 무력화할 경우, 디지털 증거의 신뢰성을 입증할 수 있어야 함

- 디지털 증거의 원본성 (Originality)
 - 디지털 증거 자체로는 가시성, 가독성이 없으므로 가시성 있는 인쇄물로 출력하여 법원에 제출할 수밖에 없음
- 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 하는 증거법상의 원칙상 제출되는 사본 증거, 그리고 가시성, 가독성 있는 형태로 변환된 증거를 원본으로 인정할 수 있는가라는 법적 문제가 제기될 수 있음

- **최량증거규칙 (The Best Evidence Rule)**

- 영미권에서 발달한 증거원칙으로 **문서의 원본증거가 증거로서 그 내용을 증명하기 위해 제출되어야 한다는 것**
- 미국 최량증거규칙은 연방증거규칙(Federal Rules of Evidence)에서 명시
- 연방증거규칙 1002조는 "서류, 기록물 또는 사진의 내용을 증명하기 위하여 문서, 기록물, 사진의 원본이 요구된다."고 최량증거원칙을 규정
- 1001조 1호에 의하면 디지털 증거는 자기적 혹은 전기적 방식에 의한 기록물로서 1002조의 서류, 기록물 등에 포함되므로, 디지털 증거도 기본적으로 당연히 원본으로 제출될 것을 요구받음
- 1004조에는 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

- 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



- 대검찰청의 디지털 증거수집 및 분석규정의 2조
 - "디지털 기기를 압수·수색·검증하거나 디지털 자료를 수집·분석할 때에는 디지털 기기 또는 디지털 자료를 수집한 때로부터 법정에 증거로 제출할 때까지 변경 또는 훼손되지 않도록 절차의 연속성을 유지하여야 하며 그 과정을 기록하여야 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

- **연계 보관성 (Chain of Custody)**

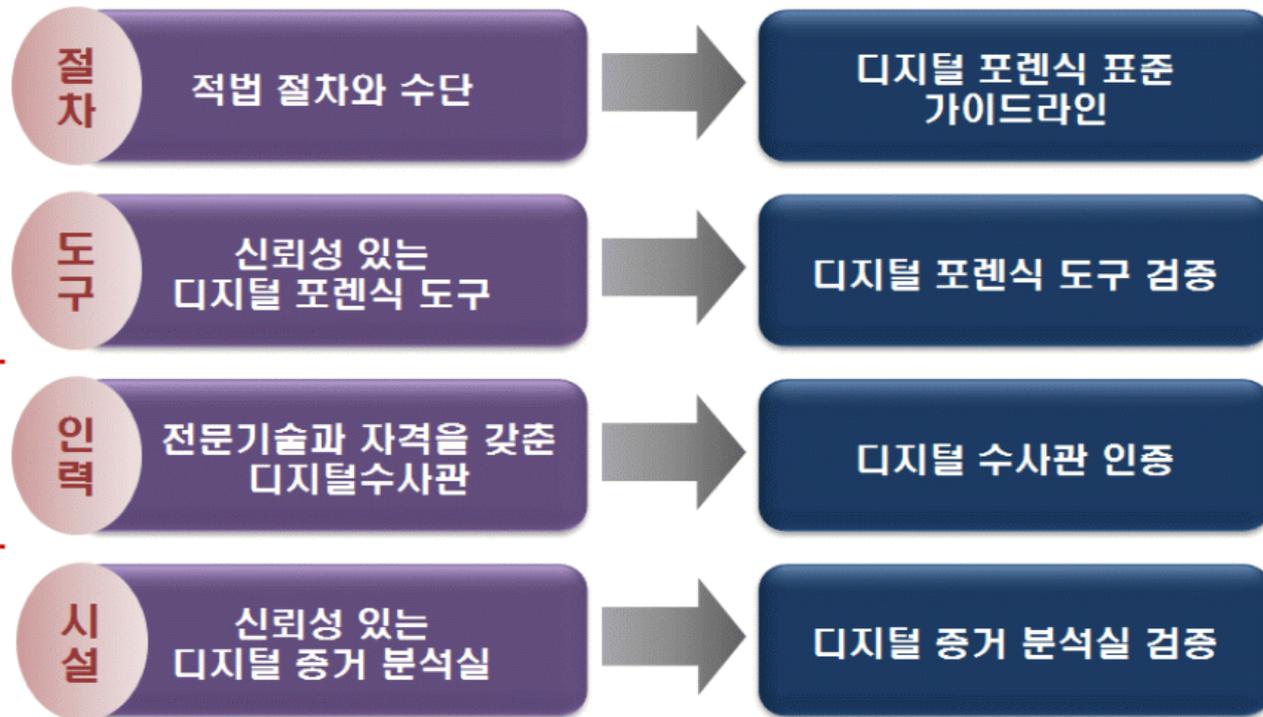
- 디지털 증거의 발견방법과 처리방법을 비롯하여 증거와 관련된 모든 사항을 명확히 기술하고 보관 · 이송 과정에서 인수인계 과정에 대한 기록과 검증이 필요
- 대검찰청의 디지털증거수집 및 분석규정의 2조
 - "디지털기기를 압수 · 수색 · 검증하거나 디지털 자료를 수집 · 분석할 때에는 디지털기기 또는 디지털 자료를 수집한 때로부터 법정에 증거로 제출할 때까지 변경 또는 훼손되지 않도록 절차의 연속성을 유지하여야 하며 그 과정을 기록하여야 한다."라고 연계보관성원칙을 가장 먼저 명시

- **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

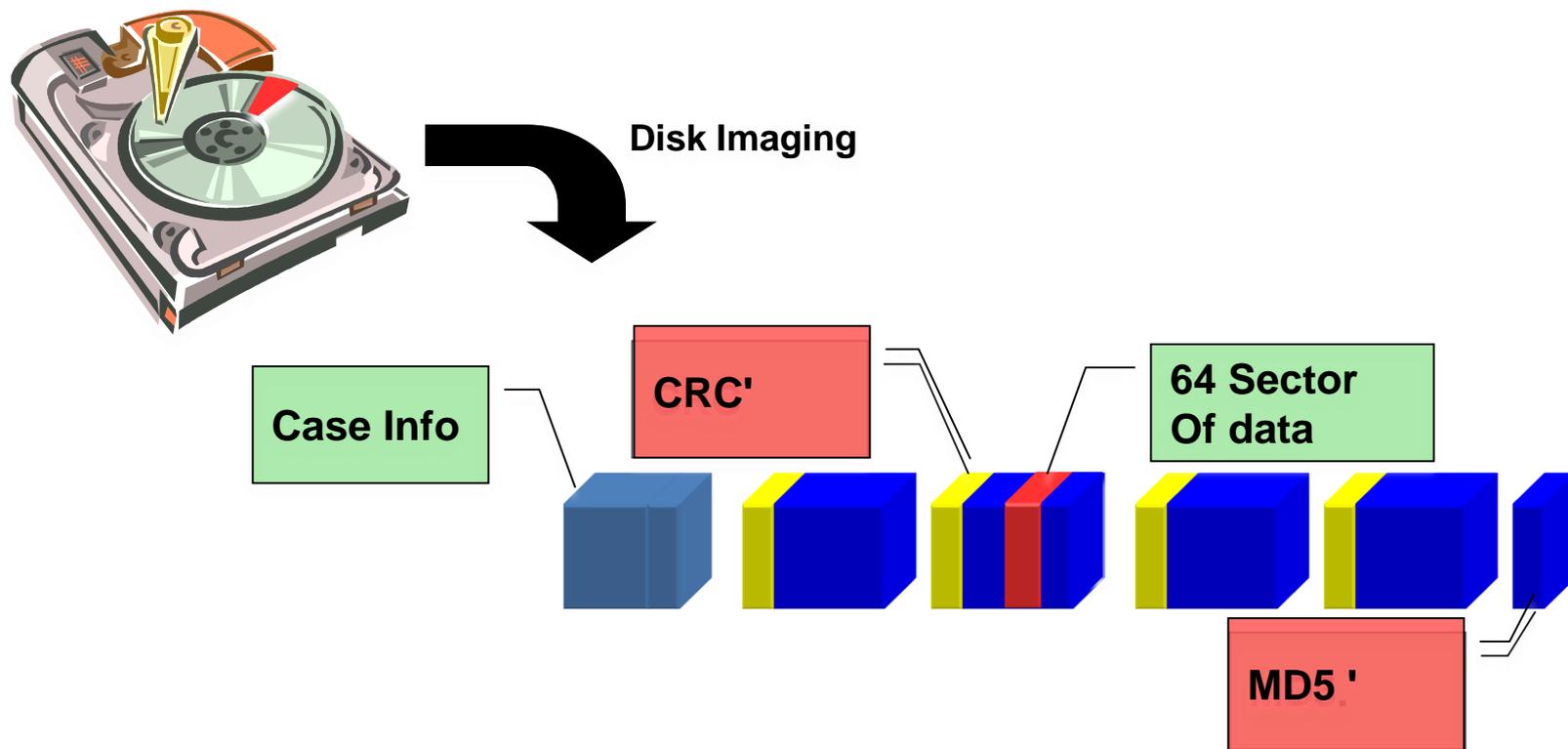


- 2007년 일심회에 대한 대법원 판례
디지털 증거가 법적 효력을 갖기 위한 요건들이 제시

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



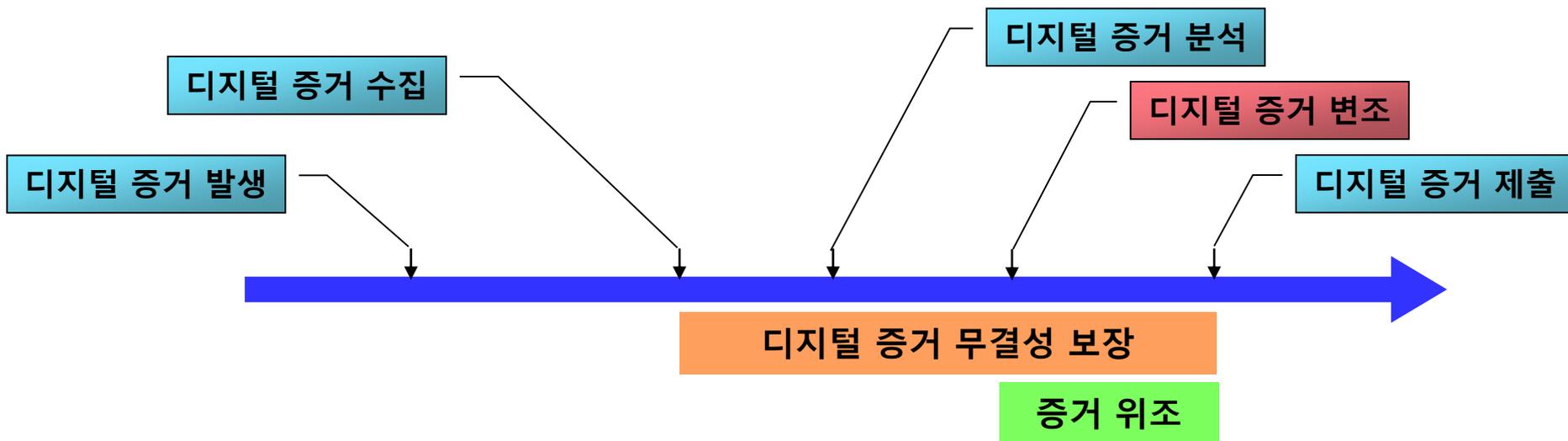
$$V = h(H) = h(I)$$

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

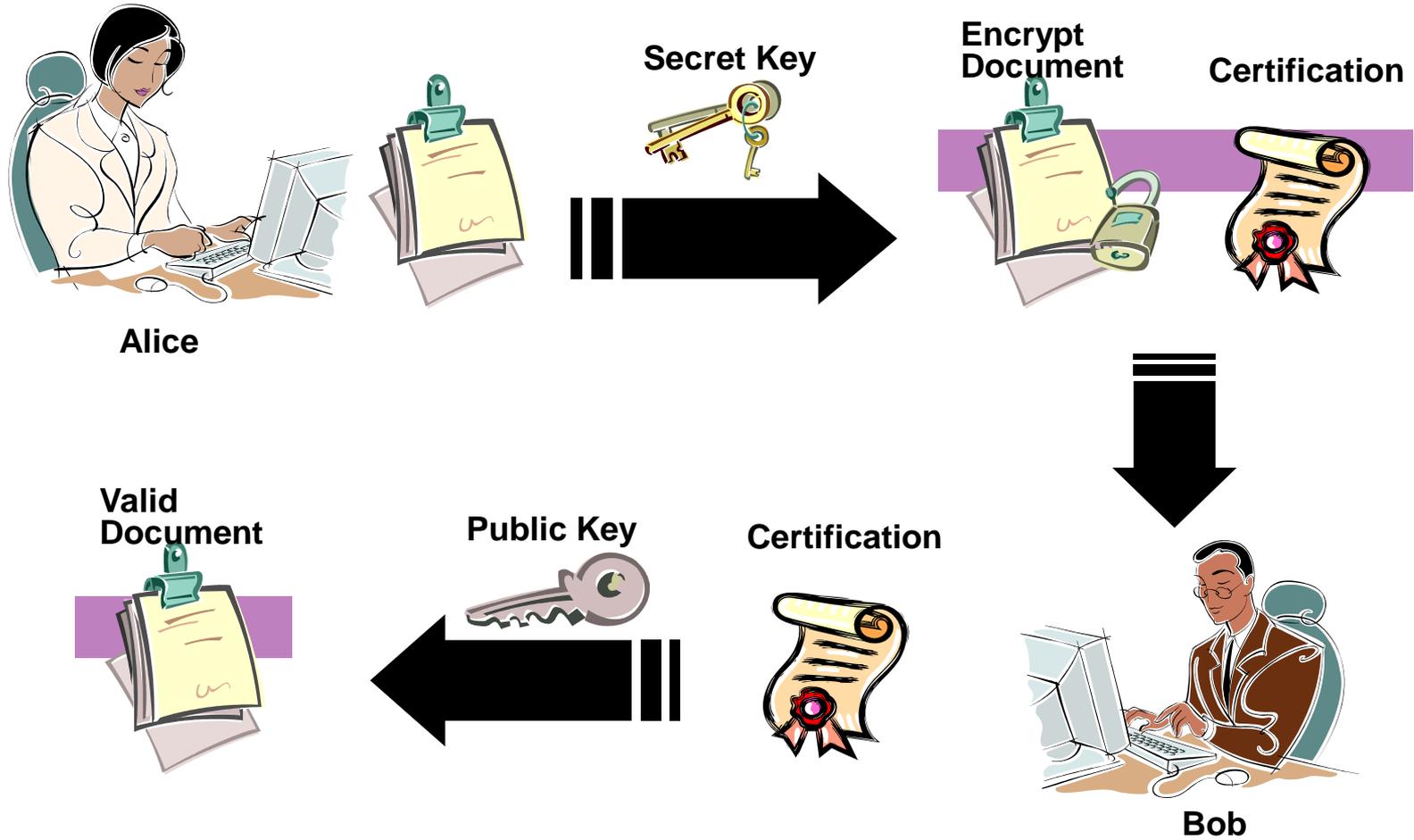
현재 디지털 증거 무결성 확보의 문제점

• 디지털 증거의 신뢰성

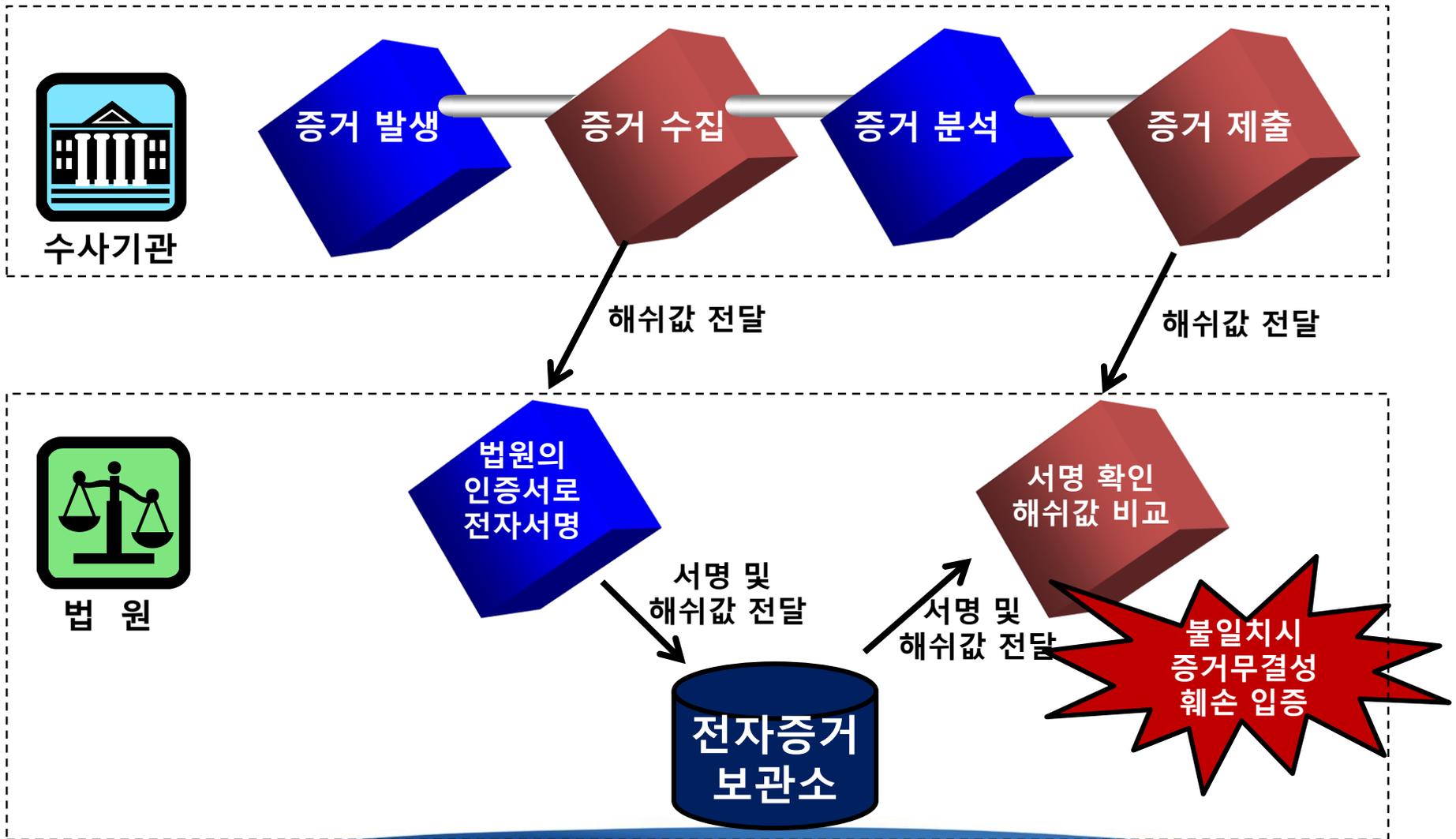
- 디지털 증거가 위조되어 법정에서 제출되는 경우
- 디지털 증거가 위조되지 않았음에도 불구하고, 용의자 또는 피고소인이 디지털 증거가 위조되었을 가능성을 이유로, 증거 효력을 무력화 시키려 하는 경우



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 해쉬 값을 공증
- 이 후 동일한 해쉬 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



법원

해쉬값이 동일한 경우
사본의 증거력 인정 필요

제 3자의 입회하에
해쉬값에 대한 공증

해쉬값이 바뀔
증거 인정 불가

장기보관 등으로 인한
데이터 변조



7-4. 디지털 데이터의 증거 능력 관련 판례

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 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 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 207도 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

