

# 디지털 포렌식 수행 절차

**김종성**  
**국민대학교**

**Email: [jskim@kookmin.ac.kr](mailto:jskim@kookmin.ac.kr)**



# 디지털 포렌식 수행 절차

1

개 요

2

디지털 포렌식 조사 모델

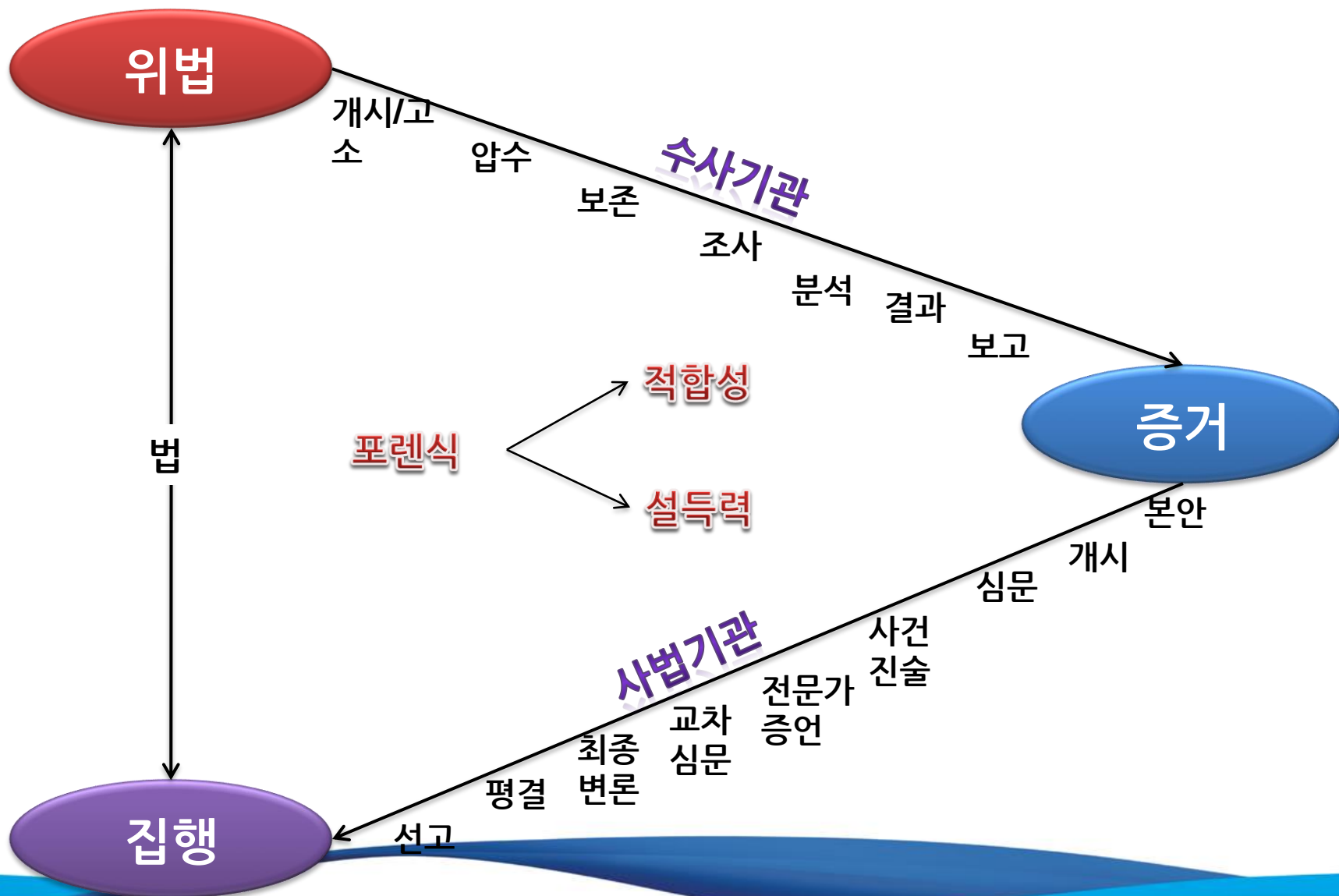
# 1.개요



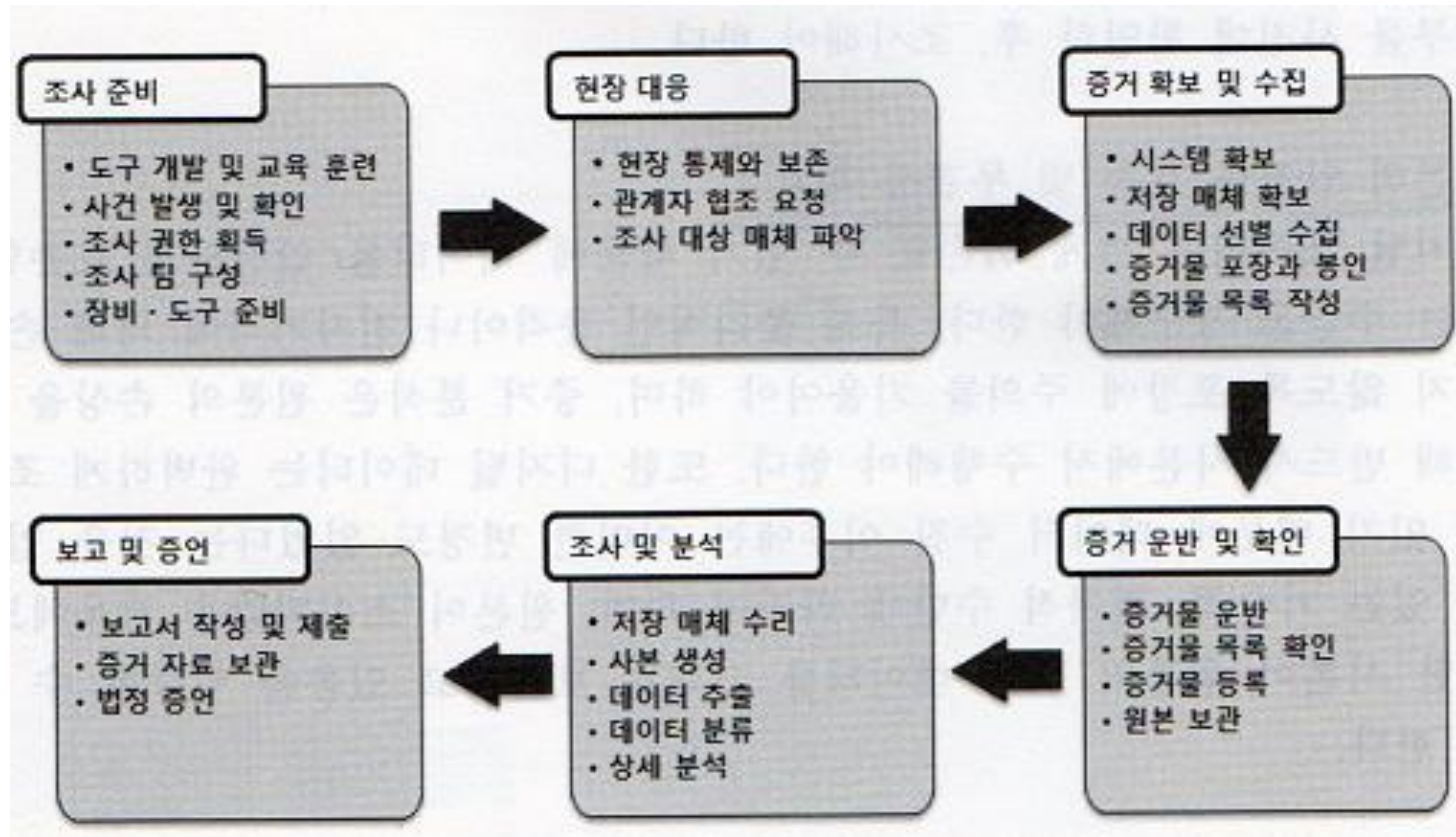
# 1.개요

- **적법절차의 준수**
  - 사건을 조사할 때 가장 우선해야 할 것은 피조사자의 인권을 보장하는 것이다.
- **원본의 안전한 보존 및 무결성 확보**
  - 디지털 데이터는 쉽게 훼손될 수 있기 때문에 데이터를 안전하게 보존할 수 있는 수단을 강구해야 한다.
- **분석 방법의 신뢰성 확보**
  - 증거 분석은 과학적인 방법을 사용해야 하고, 해당 분야 전문가들에 의해 충분히 검토되어 신뢰할 수 있는 기술적 절차로 수행해야 하며, 도출된 결과는 검증할 수 있어야 한다.
- **분석 결과의 반복성**
  - 동일한 환경에서 재분석한다면, 오차 범위 내에서 항상 동일한 결과가 도출되어야 한다.
- **진정성 유지를 위한 모든 과정의 기록**
  - 디지털 증거의 수집, 분석 도중 불가피하게 발생한 증거의 변형을 비롯한 모든 과정을 기록함으로써 사후 검증할 수 있는 수단을 제공해야 한다.

## 2.디지털 포렌식 조사 모델



## 2.디지털 포렌식 조사 모델



## 2.디지털 포렌식 조사 모델

### 가. 조사 준비

#### 1)도구 개발 및 교육 훈련

- 디지털 기기는 계속해서 신제품이 출시되고, 지속적으로 개량되고 있다. 따라서 해당 기기에 대한 연구가 선행 되어 있지 못하면 조사 자체가 어려울 수 있다.

# 2.디지털 포렌식 조사 모델

## 가. 조사 준비

### 2)사건 발생 및 확인

- 사건 발생을 인지하고, 조사할 필요가 있는지 확인해야 한다.
- 확인 과정을 거쳐 주요 조사 대상을 결정하고 전반적인 수사 계획을 수립한다.
- 주요 조사 대상은 사건마다 달라진다.
- 나아가 증거 수집 대상을 확보하기 위한 사전 조사가 필요하다.



## 2.디지털 포렌식 조사 모델

### 가. 조사 준비

#### 3) 조사 권한 획득

- 보통 사건을 조사하는 과정에서 불가피하게 알게 되는 정도가 있다.특히 기업비밀이나 프라이버시 관련 사항 등 외부에 노출되지 않아야 할 정보가 포함될 수 있다. 따라서 해당 정보에 접근할 권한이 없다면 관련 내용에 대한 조사를 하지 말아야 하며, 조사가 꼭 필요하다면 그에 적합한 권한 확보가 선행 되어야 한다.

## 2.디지털 포렌식 조사 모델

### 가. 조사 준비

#### 4) 조사 팀 구성

- 사건의 유형, 조사자의 전문성, 압수 대상 장소를 고려하여 조사 팀을 구성하고, 현장 도착 후 수색 절차, 증거 수집 방법과 범위, 각 조사자의 역할 등을 분담한다.

## 2.디지털 포렌식 조사 모델

### 가. 조사 준비

#### 5) 장비 도구 준비

- 장비 및 도구 준비는 크게 증거 수집 장비, 증거 봉인 및 포장 장비, 운반 장비로 나눌 수 있다.
- 증거 수집 장비는 소프트웨어, 하드웨어 모두를 포함한다.
- 소프트웨어:이미지 작성용 프로그램, 데이터 수집 프로그램
- 하드웨어 장비:휴대용 컴퓨터,카메라, 캠코더 시스템 분해 및 해체 도구 등

## 2.디지털 포렌식 조사 모델

### 장비 분류 및 세부 장비

분류	설명 및 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 플래시 드라이브 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, 전차과 차폐용 팩, 운반용 하드케이스 등
증거수집 및 분석용 포렌식 컴퓨터	현장에서 증거 수집 및 초동 분석 업무 등을 수행할 때 사용
기타 장비	카메라, 캠코더, 금속 스캐너, 모바일 프린터 등

## 2.디지털 포렌식 조사 모델

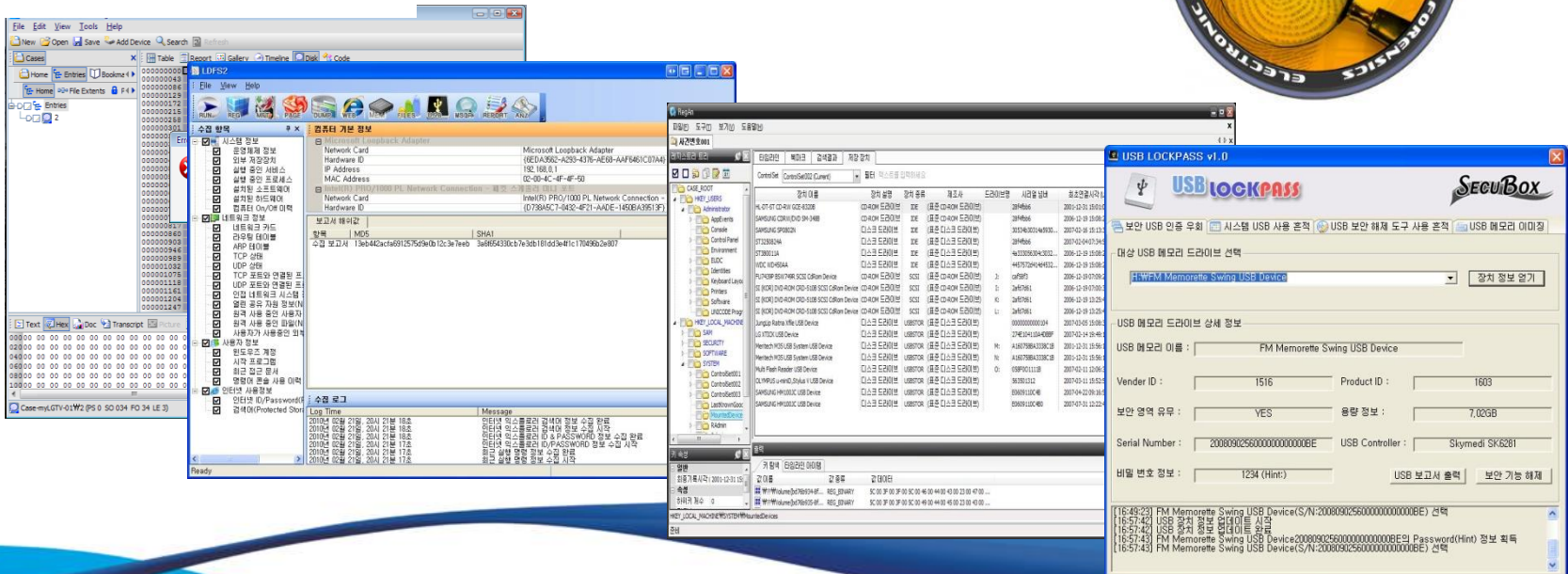
- 포렌식 하드웨어





# 2.디지털 포렌식 조사 모델

## • 포렌식 소프트웨어



# 2.디지털 포렌식 조사 모델

## 나. 현장 대응

### 1) 현장 통제와 보존

- 현장에 도착하여 피조사자에게 부여된 권한의 범위를 명확히 설명하고 조사할 대상을 신속히 파악한 후, 현장 보존과 통제를 실시함으로써 현장 조사가 시작된다.
- 현장 대응 과정에서 가장 기본이 되는 과정이 현장보존이다.
- 현장 보존을 위해서는 외부인의 접근 통제가 있어야 한다.

# 2.디지털 포렌식 조사 모델

## 나. 현장 대응

### 2) 관계자 협조 요청

- 피조사자가 협조하면 상당히 쉽게 증거를 수집할 수 있다.
- 증거 수집 과정의 객관성과 신뢰성을 확보하기 위하여 현장 조사 과정에 조사 대상자가 직접 참관토록 하여 수집하는 증거를 확인시키고, 현장에서 발견된 증거물에 대한 확인 서명을 받는다.
- 기업 조사의 경우는 복잡한 전산 환경으로 인해 주요 대상 시스템의 확보가 어려울 수 있고, 자체 보안 솔루션으로 인해 일반적인 방법으로 증거 수집이 어려울 수 있다.



## 2.디지털 포렌식 조사 모델

### 나. 현장 대응

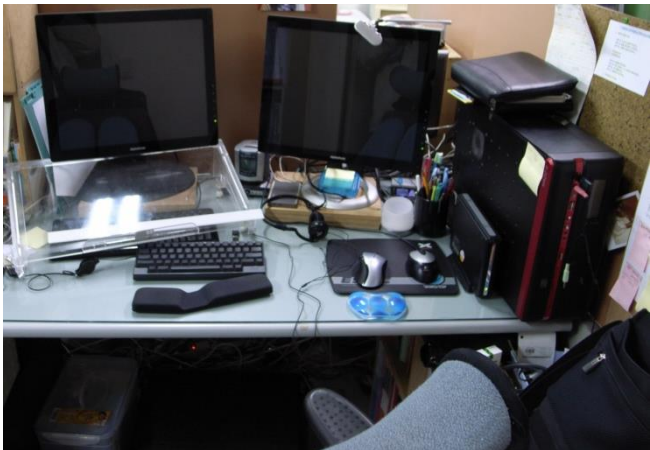
#### 3) 조사 대상 매체 파악

- 현장에 있는 모든 것이 조사 대상이라고 할 수 있다. 물리적인 증거와 디지털 기기, 저장매체, 네트워크 구성을 파악한다.



## 2.디지털 포렌식 조사 모델


- 조사 과정의 사진 촬영(녹화)을 통한 신뢰성 확보



# 2.디지털 포렌식 조사 모델

## 다. 증거 확보 및 수집

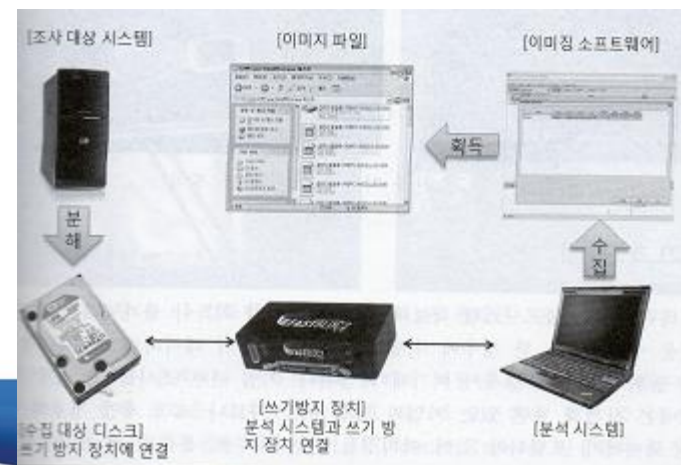
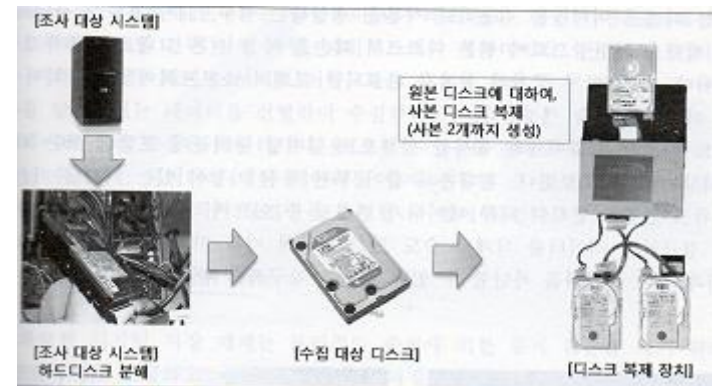
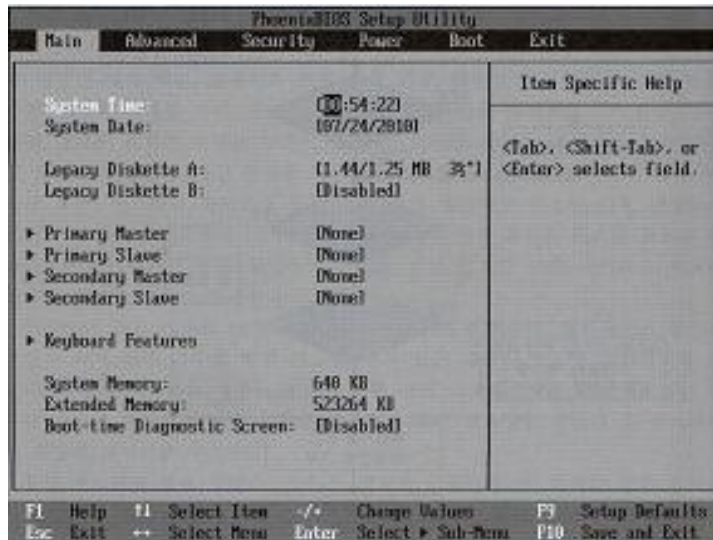
### 1) 시스템 확보

- 증거 확보
  - 시스템 확보
  - 원본 하드 디스크 드라이브  
확보
  - 하드 디스크 복제
  - 선별 데이터 수집
- 

# 2.디지털 포렌식 조사 모델

## 다. 증거 확보 및 수집

### 2) 저장 매체 확보



## 2.디지털 포렌식 조사 모델

### 다. 증거 확보 및 수집

#### 3) 데이터 선별 수집

- 데이터 선별 수집은 시스템 확보나 디스크 이미지 획득이 불가능하여 특정 데이터만을 수집하도록 한 경우에 수행되며, 의뢰 내용이 데이터에 한정된 경우나 영장의 범위가 제한된 경우가 여기에 해당된다.

## 2.디지털 포렌식 조사 모델

### 다. 증거 확보 및 수집

#### 4) 증거물 포장과 봉인

- 확보한 디지털 저장 매체는 물리적인 충격에 의한 증거 훼손을 막기 위해 충격 방지제로 포장하고, 증거 획득과 이송과정에서 증거물에 대한 위 변조가 없었음을 증명하기 위해서 봉인한다.
- 대형 디지털 기기(컴퓨터,비디오 게임 콘솔 등)
- 소형 디지털 기기(이동전화,PDA,디지털 캠코더 등)
- 휴대용 저장장치(외장 하드 디스크 ,CD/DVD,USB등)



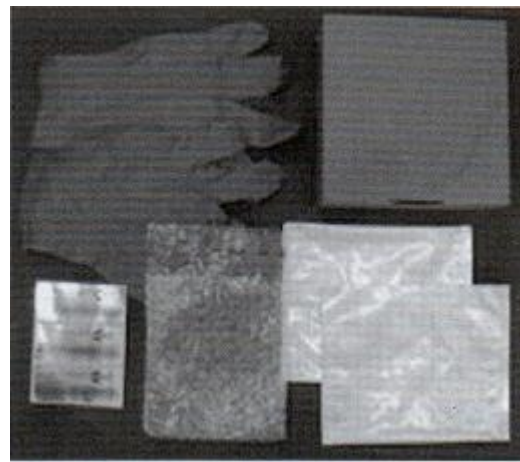
## 2.디지털 포렌식 조사 모델

### 다. 증거 확보 및 수집

#### 4) 증거물 포장과 봉인



컴퓨터 포장용 봉투



휴대폰 포장용 봉투

## 2.디지털 포렌식 조사 모델

### 다. 증거 확보 및 수집

#### 4) 증거물 포장과 봉인



밀봉 전용 특수 테이프



## 2.디지털 포렌식 조사 모델

### 다. 증거 확보 및 수집

#### 5) 증거물 목록 작성

증거물 라벨(시스템 용)			
사건번호	서울-가-100312-134	압수번호	100312-013-010
담당부서/ 조사 책임자	서울 경찰청 사이버수사대/김철수		
제조사/모델명	삼성/DB-P60(코어2듀오 E6600)		
제품 번호	KDDA10301AB		
압수 장소	서울시 성북구 안암 5가		
압수 일시	2010 년 3 월 12 일 11시 30분		
시스템 시간	2010 년 3 월 12 일 11시 28분		
시스템 사용자	홍 길 동		
조사관	김 철 수(서명)	참관인	강 영 희(서명)
피조사자	홍 길 동		
비 고(특이사항)	컴퓨터에 부착된 포스트잇 2장 보존된 채로 압수, 훼손되지 않도록 주의 요망		

## 2.디지털 포렌식 조사 모델

### 라. 증거 운반 및 확인

- 디지털 증거 운반에서 가장 주의해야 할 사항은 획득한 증거물의 진정성 유지와 훼손 방지이다.
- 증거물을 인수할 때는 각 증거물의 밀봉전용 특수 테이프에 이상이 없는지 확인해야 한다.
- 획득한 증거물을 분석할 수 있는 장소로 이송한 후, 가장 먼저 수행해야 할 일은 운반하기 전 과정과 동일하게 증거물 목록을 이용하여 증거물을 대조하면서 훼손 여부를 확인하는 것이다.
- 이송 전과 같이 각 증거물들의 밀봉전용 특수 테이프의 상태를 확인하는 과정 역시 거쳐야 한다.

# 2.디지털 포렌식 조사 모델

## 마. 조사 및 분석

### 1) 저장 매체 수리

- 저장 매체의 데이터를 분석하기 위해서는 데이터에 접근할 수 있어야 한다. 고장이 있거나 증거 인멸을 위해 인위적으로 파괴한 경우는 수리 과정을 거친다.

### 2) 사본 생성

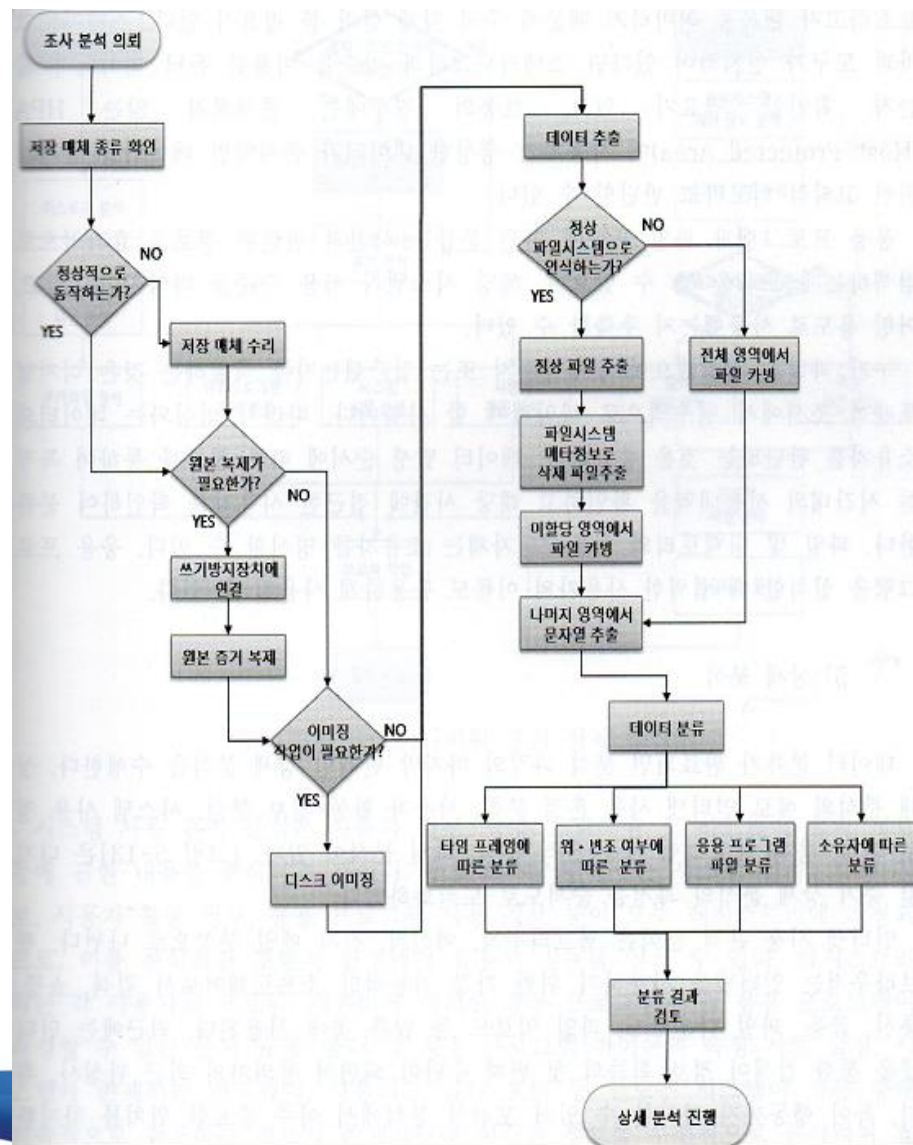
- 분석을 시작하기 전에 수집한 디지털 증거물을 복제한다.

## 2.디지털 포렌식 조사 모델

### 아.조사 및 분석

#### 3) 데이터 추출

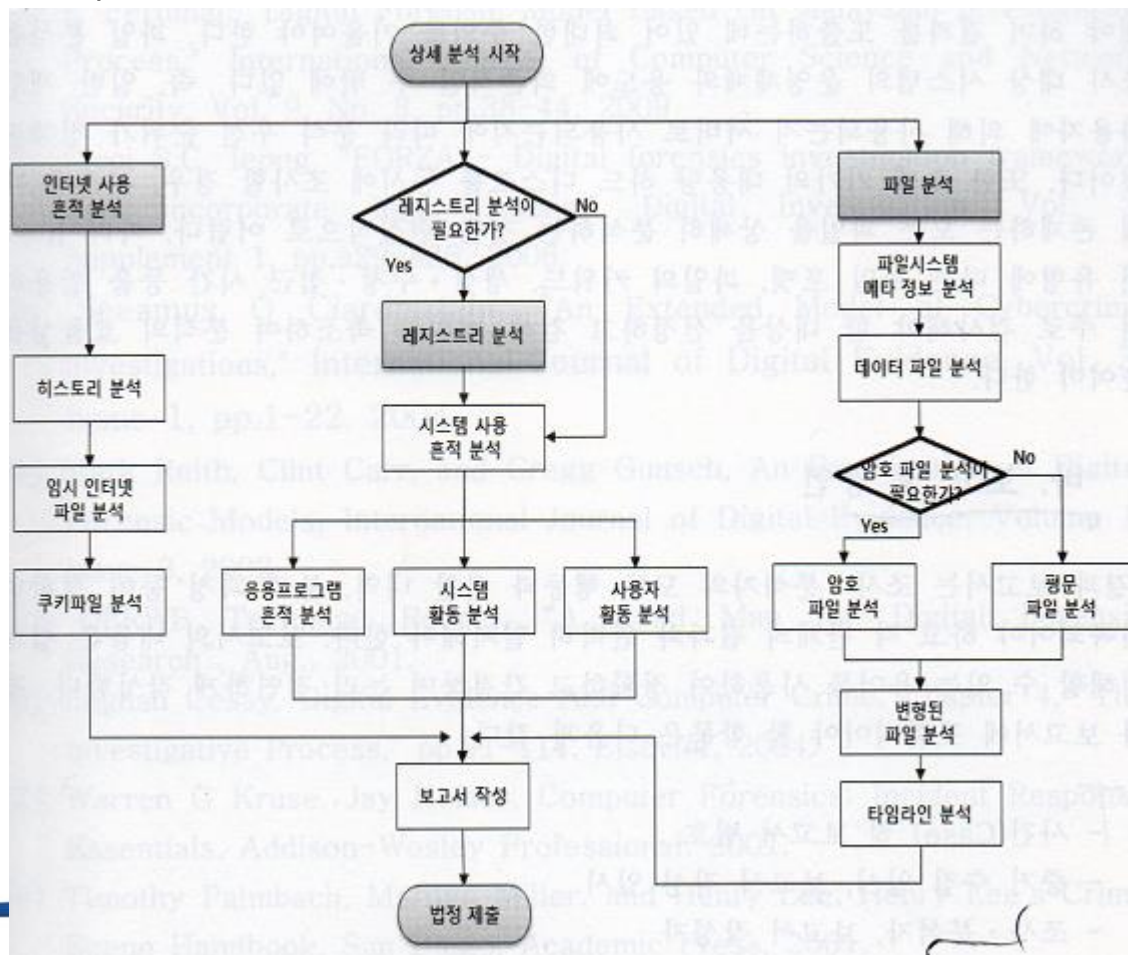
#### 4) 데이터 분류



## 2.디지털 포렌식 조사 모델

### 아.조사 및 분석

#### 5) 상세 분석



## 2.디지털 포렌식 조사 모델

### 바. 보고 및 증언

- 결과 보고서는 조사 분석자의 모든 행동과 관찰 내역, 분석 과정 등이 정확히 기록되어야 하고 각 단계의 결과와 완벽히 일치해야 한다.보고서의 내용은 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리 정연하게 작성한다.
- 사건 및 보고서 번호
- 증거 수집 일시, 보고서 작성 일시
- 조사 분석자, 보고서 작성자
- 조사 분석에 사용된 장비 및 환경
- 각 절차에 대한 개략적 설명
- 사진 및 인쇄물 등과 같은 첨부 자료
- 추출 및 분석된 증거 데이터의 상세 설명
- 분석 결과 및 결론