

과정명	
12차시	디지털 포렌식

<1> 증거자료 수집

[1] 디지털 포렌식의 개요

(1) 디지털 포렌식 등장배경

- 포렌식은 증거물을 과학적으로 조사하여 찾아내기 위한 일련의 과정을 말함
- 초기의 포렌식은 주로 법의학 분야의 지문, 모발, DNA 감식 등에 주로 사용함
- 최근의 포렌식은 물리적 형태의 증거뿐만이 아닌 디지털 포렌식 분야로 확대되고 있음
- 디지털 포렌식의 기본 원칙

(2) 디지털 포렌식의 필요성

- 컴퓨터 관련 범죄 증가 및 증거 자료의 디지털화
- 디지털 포렌식 기술의 활용도 증가

(3) 디지털 포렌식의 기본 원칙

- 적법성의 원칙, 재현의 원칙, 절차 연속성의 원칙, 무결성의 원칙

적법성의 원칙	- 표준 방법에 의한 증거 수집만이 법적으로 유효하며 엄격한 절차를 준수해야 함
재현의 원칙	- 디지털 데이터를 처리할 때 같은 조건에서 같은 데이터 처리를 수행한 결과는 항상 동일하도록 검증이 가능해야 함 - 조사 각 단계별로 전문가들에 의한 기술적 절차에 따라 조사가 수행되어야 하며, 결과는 오차 범위 내에서 항상 동일한 결과여야 함
절차 연속성의 원칙	- 현장에서 디지털 증거를 수집한 후~법정 제출까지 모든 과정이 상세히 기록되어야 함 - 각 단계별로 해당 업무를 수행하는 책임자 및 담당자를 명확히 함
무결성의 원칙	- 디지털 증거는 변조가 용이한 특성을 가지고 있기 때문에 수집된 증거가 원본 그 자체로서 변경되지 않았음을 보장할 수 있어야 함 - 디지털 증거의 훼손 여부는 원본과 복제본의 해시값을 비교하여, 값의 변경이 발생하지 않았음을 통해 입증 가능
신속성의 원칙	- 같은 조건에서 처리한 수행 결과가 항상 동일한 결과가 나와야 신뢰성을 보장받을 수 있음 - 조사 전 과정의 각 단계별로 외부 요인이 개입되지 않도록 주의

(4) 디지털 포렌식의 유형

- 디스크 포렌식, 시스템 포렌식, 네트워크 포렌식, 사물인터넷 포렌식, 데이터베이스 포렌식, 모바일 포렌식

디스크 포렌식	- 보조기억장치에서 디지털 증거를 수집하고 분석하는 분야
시스템 포렌식	- 컴퓨터 운영체제, 응용 프로그램, 프로세스를 분석하여 디지털 증거를 수집하고 분석하는 분야
네트워크 포렌식	- 네트워크를 통해 전송/저장되는 데이터를 분석하거나, 네트워크 상에서 디지털 증거를 수집하고 분석하는 분야
모바일 포렌식	- 휴대용 기기(휴대폰, 스마트 기기, 디지털 카메라 등)에서 디지털 증거를 수집하고 분석하는 분야
사물인터넷 포렌식	- 디지털 기기(스마트폰, 스마트 워치 등)의 저장 매체나 네트워크를 통해 전송되는 데이터를 디지털 증거로 사용해 수집하고 분석하는 분야
데이터베이스 포렌식	- 데이터베이스에 저장되어 있는 데이터로부터 증거를 수집하고 분석하는 분야

[2] 디지털 증거 파악

(1) 디지털 증거

- 디지털 증거는 디지털 포렌식을 위해 디지털 기기에 존재하는 정보를 매개로 하여 과거 어떤 행위의 인과 관계 또는 사실 관계를 증명 하는 절차의 중요한 요소임
- 디지털 증거는 컴퓨터에 의해 생성되어 디지털 기기에 저장되거나 네트워크를 통해 전송 중인 자료로서 법정에서 신뢰할 수 있으며, 증거로서 가치있는 정보

(2) 디지털 증거의 특성

- 비가시성, 위변조성, 자료의 대용량성, 복제 용이성, 휘발성, 네트워크성, 전문성

비가시성	- 디지털 기기, 저장 매체에 저장되는 디지털 데이터는 사람이 인지할 수 없는 0과 1의 일련의 2진수의 조합으로 이루어짐 - 디지털 증거는 하드 디스크, 보조 기억장치, 메모리 등을 제시하는 것만으로는 증거로 인정되지 않음
위변조성	- 외부 침입이나 의도치 않은 시스템적인 오류에 의한 손상 등에 의해 내용이 거짓된 내용으로 쉽게 바뀔 수 있음 - 증거가 위변조되면 쉽게 알아내기 어렵기 때문에 증거 조작 여부와 증거 획득 절차의 적합성을 판단하는 것이 중요 피의자의 고의적인 중요 정보 삭제 가능성이 있기 때문에 신속한 대응 필요
자료의 대용량성	- 최근에는 대용량 데이터를 파일서버나 데이터베이스에 저장하고 있어 대용량 데이터를 수집하고 분석하는 도구를 사용해야 함
복제 용이성	- 컴퓨터 메모리에 저장된 데이터는 쉽게 복제가 가능해 원본과 복제본 구별이 쉽지 않음 → 데이터 내용이 동일하다면 원본과 복제본은 모두 동일한 가치를 가지며, 어떤 매체에 저장되어 있는지는 중요하지 않음
휘발성	- 휘발성 데이터는 오류 발생이나 의도적인 누군가의 시도에 의해 쉽게 지워질 수 있기 때문에 증거로 수집하기 위해서는 주의를 기울여야 함
네트워크성	- 디지털 데이터는 인터넷을 통해 전 세계의 다양한 장소, 사람 등과 연결되어 공유되고 있으며, 네트워크를 통해 누구나 원격으로 접근할 수 있고 저장이나 수정, 삭제 뿐만 아니라 위변조가 가능함 - 디지털 데이터가 원거리 또는 국외에 존재하는 경우, 법 집행이나 국내외의 법 관할권을 어느 정도까지 인정할 것인지의 국가 주권 문제가 거론될 수 있음
전문성	디지털 증거를 수집하고 분석하는 과정에서는 전문적인 기술, 도구 등이 사용됨 → 디지털 증거의 압수/수색에는 포렌식 전문가의 전문적 지식이 필요 디지털 포렌식 전문가에 의해 데이터를 수집하고 분석하는 행위가 이루어져야 정확한 증거 능력 확보가 가능

(3) 디지털 증거의 종류

- 디지털 증거의 종류는 저장매체의 종류, 디지털 데이터의 휘발성 여부, 디지털 데이터의 생성원인, 디지털 데이터의 속성에 따라 구분할 수 있음
- 1) 저장매체의 종류에 따른 구분
 - 디지털 데이터는 컴퓨터 하드 디스크, USB, 원격 네트워크, 클라우드 등 다양한 저장매체를 통해 저장 가능
 - 2) 디지털 데이터의 휘발성 여부에 따른 구분
 - 전원을 켜 이후 생성 되어 종료 시 사라지는 휘발성 데이터(인터넷 연결 정보 등)
 - 전원이 꺼져도 그대로 저장되는 비휘발성 데이터(운영체제, 파일 시스템과 파일 등)
 - 3) 디지털 데이터의 생성 원인에 따른 구분
 - 사람이 직접 작성하거나 생성한 데이터인 인위적 생성 데이터(문서파일, 동영상, 기록물 등)
 - 자동 생성 데이터(인터넷 사용 기록, 시스템 접속 기록, 로그인 정보 등)
 - 4) 디지털 데이터의 속성에 따른 구분
 - 실제 증거로서 증명해주는 내용인 콘텐츠(문서 자체, 동영상/사진, 디지털 이미지 등)
 - 디지털 증거 식별에 부가적인 정보 구분에 도움이 되는 메타데이터(파일명, 확장자 등)

(4) 디지털 증거의 증거 능력

- 디지털 증거의 사용을 위해서는 디지털 증거 자체의 특성 뿐만 아니라, 수집/분석하는 절차의 적법성 여부와 함께 무결성, 진정성, 신뢰성, 원본성과 같은 문제가 해결되어야 함

무결성	<ul style="list-style-type: none"> - 최초 수집한 증거가 제출되는 과정까지 훼손되지 않고 원본 그 자체로 유지되고 있음을 보증 - 원본 자체의 훼손이 전혀 없어야 함 - 해시값 변경이 없는 경우 무결성 유지로 판단
진정성	<ul style="list-style-type: none"> - 특정한 사람에 의해 특정 시점에 생성된 데이터임을 입증하는 것 - 메타데이터만이 아닌 연계 보관 로그도 함께 기록하고 보관
신뢰성	<ul style="list-style-type: none"> - 위변조, 의도/비의도적 변경이 없는지 확인 - 증거 자체보다는 디지털 증거를 취급하는 과정에서 보장되어야 하는 특성으로 조사자, 도구, 절차 등에도 신뢰성 등이 보장되는지 확인
원본성	<ul style="list-style-type: none"> - 디지털 증거가 원본 증거와 다른 형태로 제출되는 경우가 많음 <ul style="list-style-type: none"> → 증거 원본이 제출되었는지 확인 → 가시성있게 제출된 증거를 원본 증거로 인정할 수 있는지 확인

(5) 디지털 증거의 수집 절차

1) 조사 대상 파악

- 저장 매체와 디지털 증거물인 조사 대상의 목록과 위치를 명확히 파악
- 디지털 포렌식 조사 대상 및 해당 사건과 무관한 개인적 데이터는 조사 대상 제외

2) 활성 시스템 조사

- 활성 시스템 : 현재 서비스 제공을 위해 가동 중인 시스템
- 휘발성 데이터, 비휘발성 데이터 모두 조사대상에 포함
- 활성 시스템 조사는 시스템 및 서비스에 영향을 미치기 때문에 여러 상황을 고려하여 조사

3) 디스크 이미징 등의 기술 활용

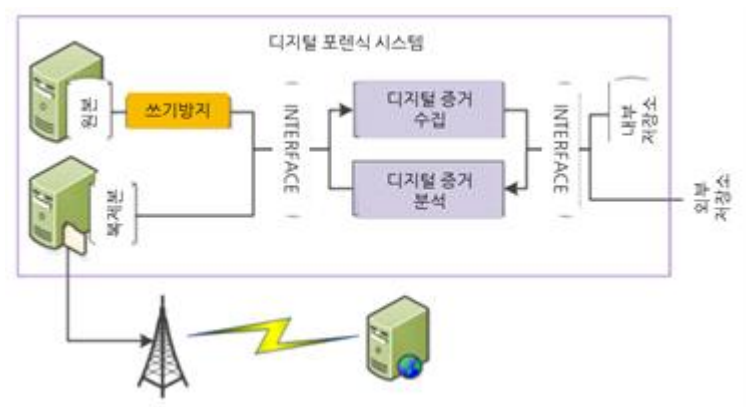
- 디지털 증거물의 조사, 분석 과정에는 원본과 완벽하게 동일한 복제본을 사용(훼손 방지)

4) 임베디드 시스템 증거 확보

<2> 디지털 포렌식 분석

[1] 디지털 포렌식 절차 수립

(1) 디지털 포렌식 시스템의 구성



1) 직접 원본 데이터 분석을 위한 장치 이용

- 원본 데이터 훼손 우려가 있어 부득이한 경우에만 사용
- 분석 전, 무결성 훼손 방지를 위해 쓰기 방지 장치 부착
- 추출된 데이터는 내/외부 저장소에 저장

2) 시스템 내에 복제본을 저장하여 데이터 분석

- 원본 데이터 훼손 방지를 위해 복제본을 만들어 저장 후 별도의 데이터 분석 과정 수행

(2) 안티 포렌식

- 디지털 포렌식 기술에 대응하여 불리한 진술로 작용할 수 있는
디지털 증거물을 차단하려는 일련의 활동
- 탐지 회피, 정보 수집 방해, 디지털 포렌식 도구 동작 방해 및 오류 발생 유발,
증거로서의 가치가 없어지도록 훼손하는 것이 목적
- 데이터 암호화, 데이터 영구 삭제, 데이터 은닉 기법이 존재

1) 데이터 암호화

- 압축 파일, 일반 문서 파일, 로그 파일 등의 암호화
- 운영체제 자체 지원 암호화 기능이나 별도의 암호화 자동 도구 사용

2) 데이터 영구 삭제(폐기)

- 데이터를 복구 불가능한 수준으로 완전히 삭제하거나, 저장매체를 물리적으로 완전히 파기
- 디스크 와이핑, 디가우저, 데이터 자동 삭제 등의 기법이 존재

3) 데이터 은닉

- 스테가노그래피, 여유 공간

[2] 디지털 포렌식 분석

(1) 디지털 포렌식 분석 절차

- 디지털 포렌식 준비 → 증거 수집 → 운반 및 이송 → 디지털 증거 조사 → 디지털 증거 분석
→ 증거 분석 및 보고서 작성

디지털 포렌식 준비	- 조사 준비 단계는 침해 탐지, 보안 시스템 경보 등을 통해 문제점을 인식하는 것에서부터 시작 - 다양하고 복잡한 디지털 정보 기기 등의 특성으로 인해 조사 전 철저한 준비과정이 필요
증거 수집	- 현장에서 사용할 디지털 증거의 수집 대상과 방법 결정 - 증거 수집 방법은 시스템의 연관 관계, 네트워크 상태를 고려하여 디지털 증거 능력을 갖춘 상태로 증거를 수집할 수 있는 방법이어야 함
운반 및 이송	- 증거의 무결성과 연결 - 증거물의 훼손, 누락, 도난이 없도록 철저히 확인
디지털 증거 조사 디지털 증거 분석	- 증거물 분석 전 체계적으로 분류하여 각 유형별 데이터를 분류하는 선행 과정 필요 - 디지털 증거물은 훼손, 변형되기 매우 쉬우므로, 각각에 대한 복제본을 만들어 원본은 보관용, 복제본은 분석용 자료로 사용 - 복제본으로 디지털 증거물을 분석하기 위해서는 파일 시스템에서 각 데이터의 특성을 조사대상에 포함
증거 분석 및 보고서 작성	- 사실 관계를 기술, 객관적 사실과 의견을 구분 - 증거 수집 과정 및 증거물에 대한 조사 분석 단계별 기록을 모두 포함

(2) 디지털 포렌식 분석 기술

- 포렌식을 통해 획득한 증거가 법적인 효력을 가지려면 증거를 발견, 기록, 획득, 보관하는 절차가 적절해야 하며, 분석에 적합한 장비와 프로그램을 사용하여 수행해야 함
- 디지털 포렌식 분석 기술로는 디스크 브라우징, 데이터 뷰잉, 검색, 타임라인 분석, 통계 분석, 로그 분석, 시각화 기술 등이 있음

디스크 브라우징	- 저장매체나 하드디스크 복제본의 이미지 구조 및 파일 시스템 구조를 파악하는 방법으로 쉽고 빠르게 분석 가능 - 복제한 디스크, 디스크 이미지 파일이나 USB 드라이브, CD와 같은 저장매체에서 생성한 이미지 파일이 대상 - 복제한 이미지 파일 사본을 분석자가 수동으로 확인할 필요가 없어 분석 시간 최소화가 가능
데이터 뷰잉	- 이진화된 파일의 데이터를 시각적으로 쉽게 확인할 수 있어 디지털

	증거 데이터의 내부 구조를 시각적인 정보로 보여주는 기술 - 다양한 형태의 파일을 개별적인 실행 프로그램 사용 없이 데이터 분석 도구를 사용하여 쉽게 데이터 확인이 가능
검색	- 대용량 저장매체, 하드디스크로부터 증거로서 의미가 있는 데이터를 찾는 기술 - 사고와 관련된 자료를 쉽게 찾기 위해 키워드, 해시, 시그니처 검색 등의 반복적인 검색을 통해 검색 범위를 축소해 나가는 방법 - 다른 데이터 분석 기술을 조합하여 사고의 증거물 조사나 분석 시간을 최소화 시킬 수 있음
타임라인 분석	- 파일 시스템 상의 파일의 생성, 변경, 접근, 삭제 시간 정보를 이용하여 사용자 행위를 추적하는 기술
통계 분석	- 시스템의 사용 목적이나 사용자의 행위 기록을 통해 성향을 파악하는 기술 - 파일, 응용 프로그램, 이벤트 종류별로 사용자의 행위를 분석하고 해당 파일, 서비스, 이벤트를 사용하는 목적을 알아내는데 유용한 기술
로그 분석	- 파일 시스템, 인터넷 접속 정보, 네트워크 연결 정보, 모바일 앱 사용 기록에 관한 로그 기록을 분석하여 사고와 관련한 용의자의 행위 파악 가능 - 운영체제별 로그 분석, 네트워크 로그 분석, 정보보호 시스템 로그 분석, 서비스 로그 분석 등
시각화	- 시스템 내부에 저장되어 있는 데이터를 일정 형태로 보여지도록 하여 분석자가 알아볼 수 있는 형태로 시각화하는 기술 - 표, 트리, 그래프를 활용

[3] 보고서 작성

(1) 보고서 작성 시 기재사항

- 사건 개요, 분석 대상, 요청 사항, 분석 방법, 분석 결과
- 1) 사건 개요
 - 해당 디지털 포렌식 분석의 전반적인 사건에 대한 설명 및 개요
- 2) 분석 대상
 - 분석 기간, 분석 장소, 분석에 참여한 전문가 정보, 분석 대상과 대상의 특징
- 3) 요청 사항
 - 디지털 포렌식 요청기관명, 담당자 성명
- 4) 분석 방법
 - 사용한 디지털 포렌식 도구 및 지원 도구의 버전 정보 등 구체적인 설명, 사본 작성 시각과 해당 해시값 정보, 분석 방법에 대한 구체적인 정보
- 5) 분석 결과
 - 원본, 사본 이미지의 전체 또는 일부 등 실제 분석이 필요한 대상
 - 상세 분석 결과는 별도 첨부

(2) 보고서 작성 절차

- 디지털 증거 목록 확인 → 디지털 증거 분석 의뢰서 내용 파악 → 증거 분석 도구의 분석 결과 취합 → 분석 결과의 증거로서 유효성 여부 판단