1. 디지털 포렌식 종류

1) 디스크 포렌식
디스크 포렌식은 물리적인 저장장치 즉, 외부적으로 충격을 가하면 쉽게 손상될 수 있는 하드디스크, 플로피디스크, CD-ROM 등 각종 보조 기억장치를 통해 삭제된 데이터를 가지고 증거를 수집하고 분석하는 포렌식 하는 것을 말한다.

디스크 포렌식을 하기 위해서 범죄자의 컴퓨터에서 물리적인 저장장치를 압수 한후에 훼손, 손상을 방지하기 위해서 사본을 만들고 사본을 가지고 분석을 실시해야 하며 사본이 원본과 동일하다는 사실을 증명하기 위해서 해쉬값을 통해서 동일하다는 검증을 하고 무결성을 입증해야한다.

2) 시스템 포렌식
시스템 포렌식은 서버, PC, 운영체제, 응용 프로그램 및 프로세스를 분석하여 증거를 확보하는 포렌식이다. 서버나 PC의 환경은 하드웨어적으로 호환성 측면에서 비슷하거나 조금은 다르지만, 운영체제에 따라서는 소프트웨어적 환경이 크게 차이가 난다. 컴퓨터 시스템은 Windows, Linux, Mac OS 등 여러 가지 운영체제를 사용한다.

시스템 포렌식의 중요한 단서가 되는 아티팩트(증거, 흔적)는 시스템이나 애플리케이션이 자동으로 생성한 데이터인 "생성 증거"이다. 아티팩트가 소프트웨어적 환경에서 크게 좌우된다면 각 운영체제에 대한 응용프로그램이나 파일시스템의 이해도가 높고 경험이 많은 디지털 포렌식 전문가가 수행하는 것이 효과적이다.

3) 네트워크 포렌식
네트워크 포렌식은 네트워크를 통하여 전송되는 데이터나 암호 등을 분석하거나 네트워크의 형태를 조사하여 단서를 찾아내는 포렌식입니다. 네트워크에서 전송되는 데이터를 패킷이라고 하는데, 패킷은 보내는 출발지와, 받는 도착지 간에 통신을 하고 패킷을 들여다 보면 어떤 내용의 데이터가 오고 가는지 파악이 가능하다.

대부분 네트워크는 사용자를 감시하기 위해 데이터 추적이 가능한 기능을 지원하게 된다. IP 헤더는 발신지(Source Address)IP와 목적지(Destination Address)IP를 포함하고 있으며, 데이터 링크 헤더(계층)는 MAC주소를 포함하고 있다.

4) 인터넷 포렌식
인터넷 포렌식은 인터넷으로 서비스되는 WWW(World Wide Web), FTP(File Transfer Protocol) 등 인터넷을 이용해서 응용 프토로콜을 사용하는 증거를 수집하는 포렌식이다. 인터넷은 포렌식 관점에서 볼 때 상당한 양의 증거가 저장되어 있는 저장소이다. 인터넷 포렌식은 부도덕적인 행동을 하는 범죄자들을 추적하기 위해 웹브라우저 히스토리 분석, 전자우편 헤더분석, IP추적 등 기술들을 이용하여 증거를 수집하게 된다.

5) 모바일 포렌식

모바일 포렌식은 우리가 일상생활에서 없으면 안되는 스마트폰, 태블릿PC, PDA(단말기), 디지털 카메라, IoT(사물인터넷) 기기 등과 같은 모바일 장비들을 통해서 데이터를 수집하고 분석하는 포렌식 기술이다.

모바일 포렌식은 스마트폰 포렌식이라고 생각할 수 있지만 큰 범주에 모바일 포렌식이 있고, 안에 스마트폰 포렌식이 존재한다. 스마트폰 포렌식은 모바일 포렌식 분석으로 얻을 수 있는 통화내역, 문자 내역, 카메라 등 기본정보를 추출하여 복원, 복구하여 증거로 이용하고, 이 뿐만 아니라 GPS, 메신저 앱, SNS앱, 인터넷 사용내역 등 다양한 디지털 정보를 얻을 수 있다.

6) 데이터베이스 포렌식
데이터베이스(DB)는 쉽게 설명하자면 데이터들이 통합하여 관리되는 집합체라고 설명할 수 있다. 중복된 데이터를 없애고, 자료를 구조화 하며, 효율적인 데이터 처리를 할 수 있도록 관리하게 된다. DB포렌식은 DB로부터 데이터를 추출, 분석하여 증거를 획득하게 되는 포렌식이다.

7) 암호 포렌식
암호 포렌식은 사용자가 이용하는 모든 파일에 암호를 걸어놨을 때 암호를 해독하기 위한 포렌식 분야이다.

2. 디지털 포렌식 대상물의 특징

1) 매체 독립성

- 디지털 증거는 유체물이 아닌 각종 디지털 저장매체에 저장되어 있거나 네트워크를 통하여 전송 중인 정보 그 자체
- 정보는 값이 같다면 어느 매체에 저장되어 있든지 동일한 가치

2) 비가시성, 비가독성
- 디지털 증거 그 자체는 사람의 지각으로 바로 인식이 불가능
- 일정한 변환절차를 거쳐 모니터 화면으로 출력되거나 프린터를 통하여 인쇄된 형태로 출력되었을 때 가시성과 가독성을 가짐

3) 취약성
- 삭제, 변경 등이 용이
- 하나의 명령으로 하드디스크 전체를 포맥하거나 파일 삭제가 가능
- 파일을 열어보는 것만으로 파일 속성이 변경됨

4) 대량성
- 방대한 분량의 정보를 하나의 저장매체에 저장가능함

5) 전문성

- 디지털 증거의 수집과 분석에 전문적인 기술이 사용되므로, 디지털 증거의 압수, 분석 등에 있어 디지털 포렌식 전문가가 필수적임

6) 네트워크 관련성
- 네트워크를 통해 서로 연결되어 있기 때문에, 디지털 증거의 관할권을 어느 정도까지 인정할 것인지 문제 발생.

3. 디지털 포렌식 5대 원칙

1) 정당성의 원칙
- 획득한 증거 자료가 적법한 절차를 준수해야 하며, 위법한 방법으로 수집된 증거는 법적 효력을 상실한다.

2) 무결성의 원칙
- 수집 증거가 위,변조되지 않았음을 증멸할 수 있어야 한다.

3) 재현의 원칙
- 피해 직전과 같은 조건에서 현장 검증을 실시하거나, 재판이나 법정의 검증과정에서도 동일한 결과가 나와야한다.

4) 신속성의 원칙
- 휘발성 증거의 수집 여부는 신속한 조치에 의해 결정되므로 모든 과정은 지체없이 진행되야 한다.

5) 절차 연속성의 원칙
- 증거물 획득 -> 이송 -> 분석 -> 보관 -> 법정 제출의 각 단계에서 담당자 및 책임자를 명확히 해야한다.