2021-09-30

디지털 포렌식 개요와 관련 도구

201812745 김종원

A Table of Contents.

“Forensic” 은 법의학 등을 이용한 범죄에 관한 과학수사이며,

“Digital Forensic” 은 컴퓨터를 통해 발생한 범죄에 대한 과학 수사를 의미한다.

Part 1,

디지털 포렌식이란?

컴퓨터를 매개로 이루어지는 범죄에 대한 법적 증거자료 확보를 위해 컴퓨터 저장 매체와 네트워크로부터 자료를 수집, 분석 및 보존하여 법정 증거물로써 제출할 수 있도록 하는 일련의 절차와 행위.

목적

- 컴퓨터 범죄 수사를 목적으로 사용됨
- 컴퓨터 범죄를 행하는 범죄자를 빠른 시간 안에 정확하게 찾아내서 범죄 행위에 이용된 증거를 확보하고, 이를 통하여 법적 대응이 가능하도록 해야 함.
- 정보통신 침해사고 분석 및 대응이 가능해야 함.
- 컴퓨터 시스템 및 네트워크 데이터를 분석함으로써 컴퓨터 범죄를 최소화 해야 함.

필요성

- 컴퓨터 관련 범죄 증가 및 증거자료의 디지털화
- 디지털 포렌식 기술의 활용도 증가

Part 2,

디지털 포렌식 개요

디지털 포렌식 5대 원칙

정당성의 원칙	신속성의 원칙	무결성의 원칙	연계 보관성의 원칙	재현의 원칙
획득한 증거 자료가 적법한 절차를 준수해야하며, 위법한 방법으로 수집된 증거는 법적 효력을 상실함.	시스템의 휘발성 정보수집 여부는 신속한 조치에 의해 결정되므로 모든 과정은 지체 없이 신속하게 진행되어야 함.	수집한 증거가 위변조 되지 않았음을 증명할 수 있어야 함.	증거물 획득, 이송, 분석, 보관, 법정 제출의 각 단계에서 담당자 및 책임자를 명확하게 해야 함.	피해 직전과 같은 조건에서 현장 검증을 실시하였다면, 피해 당시와 동일한 결과가 나와야 함.

Part 2,

디지털 포렌식 개요

분석 목적에 따른 분류

사고대응 포렌식(침해사고)

- 해킹 등 침해 시스템의 로그, 파일 등을 조사하여 침입자의 신원, 피해 내용, 침입 경로 등을 파악.
- 사고 내용을 분석하여 조치를 취해 추가적인 피해를 막고, 서비스를 재개하는 데에 목적.

증거(정보)추출 포렌식

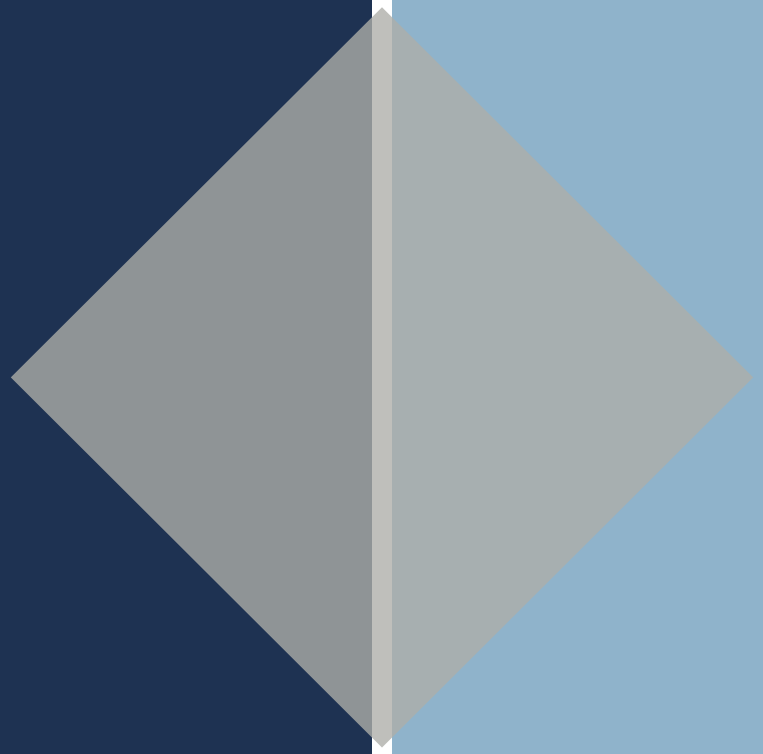
- 범행 입증에 필요한 증거를 얻기 위하여 디지털 저장매체에 기록되어 있는 데이터를 복구 하거나 검색하여 찾아냄.
- 회계 시스템에서 필요한 계정을 찾아 범행을 입증할 수 있는 수치 데이터를 분석하거나, E-Mail등의 데이터를 복구 및 검색하여 증거를 찾아내는 것이 목적.

Part 2,

디지털 포렌식 개요

분석 대상에 따른 분류

- 디스크 포렌식
- 시스템 포렌식
- 네트워크 포렌식
- 인터넷 포렌식
- 모바일 포렌식
- 데이터베이스 포렌식
- 암호학 포렌식
- 사물인터넷 포렌식



Part 2,

디지털 포렌식 개요

디지털 포렌식 수행 과정

수사 준비

관리적/기술적 준비를 하는 과정으로 컴퓨터 포렌식에 사용되는 각종 소프트웨어 또는 하드웨어를 준비하고 점검하는 단계

>>

증거물 획득

피해 사고 발생 장소 또는 용의자 컴퓨터를 압수하는 현장에서 각종 저장매체와 시스템에 남아있는 디지털 증거를 획득하는 단계.

>>

이송 및 보관

수집된 증거물을 안전한 방법으로 분석실 또는 보관소로 옮기는 과정. 그리고 증거물의 무결성을 보증할 수 있는 환경에서 보관 및 관리하는 단계.

>>

분석 및 조사

증거물 분석단계는 증거물의 내부를 확인하고 범죄에 관련된 파일 또는 정보를 획득하는 과정.

>>

보고서 작성

디지털 증거수집, 운송 및 보관, 조사/분석 단계의 모든 내용을 문서화하여 법정에 제출하는 단계.

Part 2,

디지털 포렌식 개요

증거물 획득 단계

1. 휘발성 증거 우선 수집

- 증거수집 시 메모리나 프로세스, 화면에 있는 정보 등 소멸 가능성이 많은 증거부터 우선 확보
- 일반적으로 레지스트리 / 캐쉬 / 라우팅 테이블 / ARP 캐쉬 / 프로세스 테이블 / 커널 정보와 모듈 / 메인 메모리 / 임시파일 / 보조메모리 / 라우터 설정 순으로 소멸

2. 전원차단 여부 결정

- 서버의 경우는 전원을 차단하기 전에 프로세스 정보가 유실되지 않도록 종료.
- 네트워크에 연결되어 있는 경우에는 수시로 원격으로 접속하여 데이터 삭제가 가능하므로 이에 대비하여 사전에 네트워크 단자를 제거.

3. 증거수집 대상에 따른 대응

- 개인용 컴퓨터인 경우 본체 그대로 증거로 채택하거나 하드디스크를 분리하여 복제
- 데이터가 대기업의 회계관련 DB 또는 ERP 등 대형 컴퓨터에 저장되어 있는 경우 전문가의 도움을 받아 상황에 따른 적절한 증거 수집 수행

디지털 포렌식 개요

운영체제	전원차단 방법	비고
윈도우(개인PC)	전원 플러그 바로 분리	정상 종료 절차를 수행하면 임시데이터가 삭제됨
윈도우(서버)	정상 종료 후 분리	
Linux	정상 종료 후 분리	
Unix	정상 종료 후 분리	
Macintosh	전원 플러그 바로 분리	정상 종료 절차를 수행하면 임시데이터가 삭제됨

Part 2,

디지털 포렌식 개요

증거물 획득 단계

1. 휘발성 증거 우선 수집

- 증거수집 시 메모리나 프로세스, 화면에 있는 정보 등 소멸 가능성이 많은 증거부터 우선 확보
- 일반적으로 레지스트리 / 캐쉬 / 라우팅 테이블 / ARP 캐쉬 / 프로세스 테이블 / 커널 정보와 모듈 / 메인 메모리 / 임시파일 / 보조메모리 / 라우터 설정 순으로 소멸

2. 전원차단 여부 결정

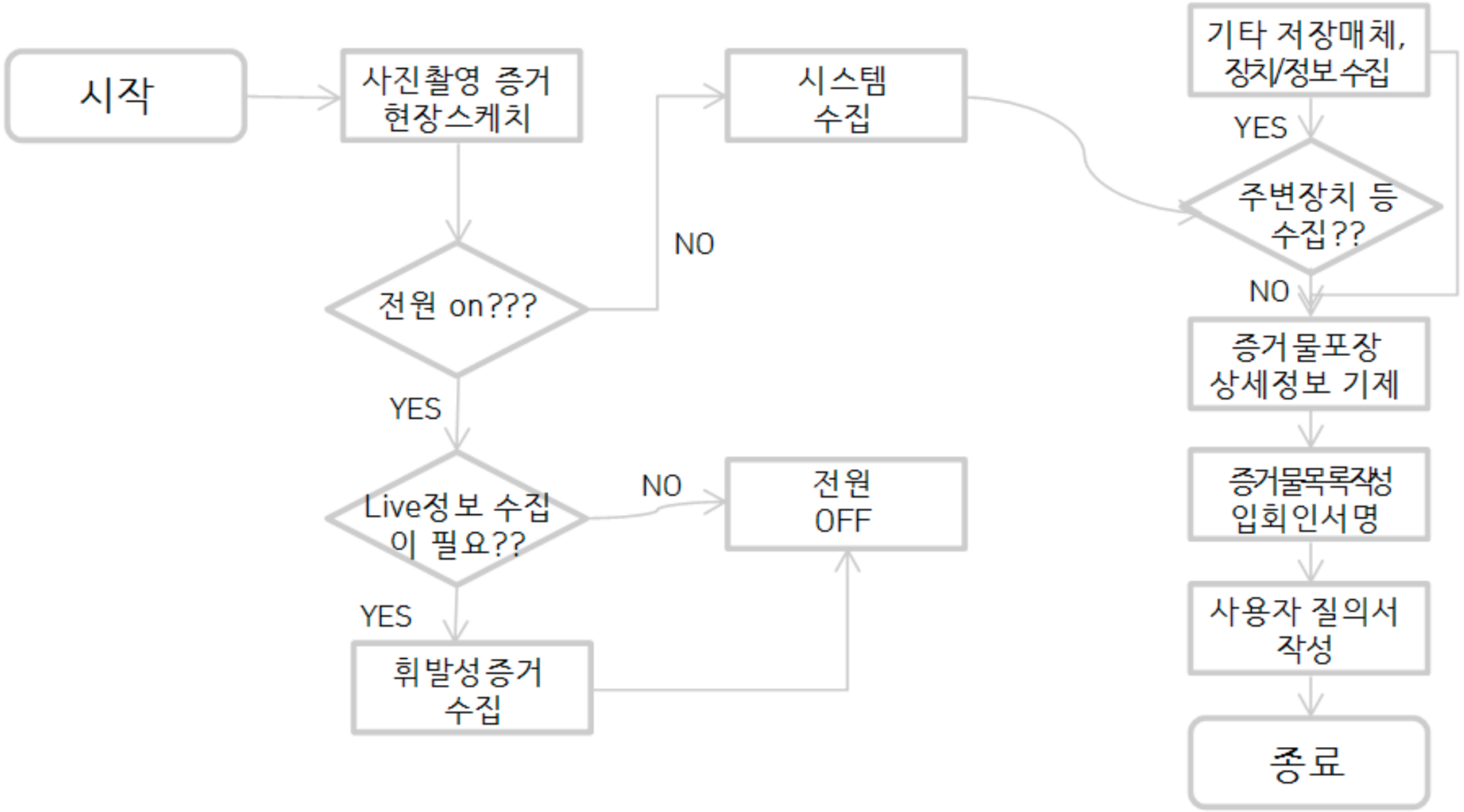
- 서버의 경우는 전원을 차단하기 전에 프로세스 정보가 유실되지 않도록 종료.
- 네트워크에 연결되어 있는 경우에는 수시로 원격으로 접속하여 데이터 삭제가 가능하므로 이에 대비하여 사전에 네트워크 단자를 제거.

3. 증거수집 대상에 따른 대응

- 개인용 컴퓨터인 경우 본체 그대로 증거로 채택하거나 하드디스크를 분리하여 복제
- 데이터가 대기업의 회계관련 DB 또는 ERP 등 대형 컴퓨터에 저장되어 있는 경우 전문가의 도움을 받아 상황에 따른 적절한 증거 수집 수행

Part 2,

디지털 포렌식 개요



Part 2,

디지털 포렌식 개요

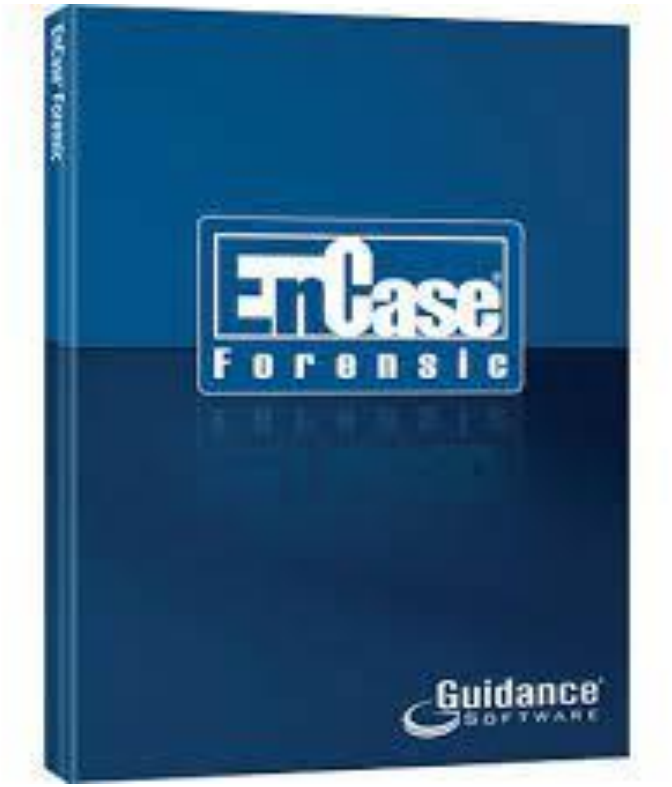
증거물 수집 시 주의사항

- 어떤 시스템을 수집할 것인지를 목록에서 확인하여 신속 정확하게 수집
- HDD만 수집할 경우 충격 및 자기장 등으로 인해 증거 손상이 가지 않도록 주의
- 시스템 하드웨어나 네트워크를 파악하고 원본의 손상을 방지
- 시스템의 전원 차단 여부를 먼저 파악하고, 전원이 꺼져 있다고 판단되더라도 화면보호기 작동여부, HDD 및 모니터 작동 여부 등을 파악하여 전원 유무를 재확인
- 전원이 켜져 있는 시스템에서 수집 해야 할 휘발성 자료가 있을 때 시스템에 피해가 가지 않는 한 최소한의 범위 내에서 작업 수행
- 시스템 시간을 확인 하는 과정에서 표준시간 정보와 비교해서 정확하게 기록
- 전원이 켜져 있을 경우 부주의에 의해 시스템 내의 프로그램을 실행시키지 않도록 주의
- 기타 장치 종류를 확인하고, 알 수 없는 장치가 있는 경우 사진촬영 등 자료를 확보하고 전문가와 상의
- 취급 미숙으로 인해 시스템을 켜는 것만으로도 데이터 변조가 있으므로 각별히 주의

Part 3,

디지털 포렌식 관련 도구

EnCase



- 증거수집
- 쓰기 방지 기능
- 파일 시그니처 분류 기능
- 그림 파일 해석
- 압축 파일 해석
- 레지스트리 분석
- 시간 정보 해석
- 삭제된 파일 카빙

Part 3,

디지털 포렌식 관련 도구

Autopsy

- 타임라인 분석
- 키워드 검색
- 썸네일 보기
- 이메일 분석
- 레지스트리 분석
- 파일 타입 정렬