



## 디지털 포렌식 (Digital Forensic)

보안프로젝트 이 별 강사  
(by1.joker@gmail.com)

## 강사소개

- 이 별(JOK3R)
- - 現 보안프로젝트 대표 강사 이별
- - 現 한국포렌식학회 총무이사 // 現 Gflow 과장
- - 現 한양사이버대학교 특강 교수(2017.11 ~ )
- - 現 대덕마이스터소프트웨어 고등학교 포렌식 멘토
- - StartUP 디스크 포렌식 저술(2017.04)
- - 문제로 배우는 디지털 포렌식 공저(2017.11.)
- **자격 및 수상 현황**
- - EnCE [Guidance Software/2016. 9.]
- - 국가공인 디지털포렌식전문가2급 [한국포렌식학회/2016. 7.]
- - CISSP / CISA/ CIA
- - 국방해킹방어대회 3위, KISA원장상 수상 [2015.07.]

# 1. 디지털포렌식 개요

## ▶▶ 디지털포렌식 개요

- 포렌식(Forensic)이란 법의학 등을 이용한 범죄에 관한 과학수사 정도로 말할 수 있으며, 디지털 포렌식(Digital Forensic)은 컴퓨터를 통해 발생한 범죄에 대한 과학 수사를 의미.

## ▶▶ 디지털포렌식 개요

- 포렌식의 기원

- 1980년대 중반부터 디지털 증거의 보존, 신원확인, 증거확보 등에 관한 기술을 다루기 시작
- 디지털포렌식 용어는 1991년 미국 포틀랜드에서 열렸던 International Association of Computer Specialists(IACIS)에서 처음 사용

- 정의

- 컴퓨터를 매개로 이루어지는 범죄에 대한 법적 증거자료 확보를 위해 컴퓨터 저장매체와 네트워크로부터 자료를 수집, 분석 및 보존하여 법정 증거물로서 제출할 수 있도록 하는 일련의 절차와 행위

## ▶ 디지털포렌식 목적

- 디지털포렌식은 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

## ▶ 디지털포렌식 필요성

- 컴퓨터 관련 범죄 증가 및 증거자료의 디지털화

- 정보화에 따른 컴퓨터 관련 범죄 뿐만 아니라 일반 범죄에서도 중요 증거 또는 단서가 컴퓨터를 포함한 전자매체 내에 보관되어 있는 경우가 가히 급수적으로 증가

- 디지털자료는 복사가 쉬울 뿐만 아니라 원본과 사본의 구분이 어렵고 조작 및 생성, 전송, 삭제가 매우 용이

- 범죄 관련 증거 자료가 디지털화 되어감에 따라 증거 수집, 분석을 위한 전문적인 디지털 포렌식 기술 개발이 필요

- 디지털포렌식 기술의 활용도 증가

- 국가기관에서 컴퓨터 범죄 뿐만 아니라 일반 범죄 수사에서의 활용 빈도가 증가

- 일반 기업체 및 금융회사 등의 민간분야에서도 디지털 포렌식 기술의 수요가 급증

- 내부정보유출, 회계감사, 보험사기 등에 활용

## ▶ 디지털포렌식 5대 원칙

### 정당성의 원칙

획득한 증거 자료가 적법한 절차를 준수해야 하며,  
위법한 방법으로 수집된 증거는 법적 효력을 상실함

### 신속성의 원칙

시스템의 휘발성 정보수집 여부는 신속한 조치에 의해  
결정되므로 모든 과정은 지체 없이 신속하게 진행되어야 함

### 무결성의 원칙

수집한 증거가 위·변조되지 않았음을  
증명할 수 있어야 함

법적  
증거로서의  
효력

### 재현의 원칙

피해 직전과 같은 조건에서 현장 검증을 실시하였다면,  
피해 당시와 동일한 결과가 나와야 함

### 연계 보관성의 원칙

증거물 획득, 이송, 분석, 보관, 법정 제출의 각 단계에서  
담당자 및 책임자를 명확하게 해야 함

## 2.디지털포렌식 유형



▶ 디지털포렌식의 분석 목적은 크게 두 가지로 나뉘며, 사고대응 포렌식과, 증거(정보) 추출 포렌식으로 나뉨.

## ▶ 분석 목적

### ● 사고대응 포렌식(침해사고)

-해킹 등 침해 시스템의 로그, 파일 등을 조사하여 침입자의 신원, 피해내용, 침입경로 등을 파악

-네트워크 기술과 서버의 로그분석 기술, 유닉스, 리눅스, 윈도우 서버 등 운영체제에 대한 기술 등이 필요

### ● 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-Mail 등의 데이터를 복구 및 검색하여 증거를 찾아내는 것이 목적

▶ 디지털포렌식 분석 대상에 따라서는 디스크, 시스템, 네트워크, 인터넷, 모바일, DB, 암호학, 메모리, 회계 포렌식 등으로 나눌 수 있음.

## ▶ 분석대상[1/4]

### ● 디스크포렌식

- 대용량의 비휘발성 저장매체로부터 자료를 획득, 분석,검색,삭제된 파일 복구하는 기능 등이 주로 활용
- 삭제된 파일을 복구하고, 여러 가지 종류의 파일을 파일명, 확장자, 작성자, 작성 일시 등을 기준으로 분류하고(타임라인), 키워드 검색을 통하여 수사의 단서를 추출하는 작업
- 디스크포렌식 과정에서는 증거의 손상이나 훼손을 방지하기 위해 2개의 사본을 만들어 하나는 증거로 보존하고 나머지 하나는 분석이 이루어져야 함

## ▶ 분석대상[2/4]

### ● 네트워크 포렌식

-네트워크를 통하여 전송되는 데이터, 암호 등을 특정도구를 이용하여 가로채거나 서버에 로그 형태로 저장된 것을 접근하여 분석하거나 네트워크 형태 등을 조사하여 단서를 찾아내는 분야

### ● 인터넷포렌식

-인터넷으로 서비스되는 WWW, FTP등 인터넷 응용 프로토콜을 사용하는 분야

-게시판에 불법 정보를 업로드 하거나 명예훼손과 관련된 글을 올린 용의자 추적, 전자메일발신 추적, 인터넷 서핑내역 추적 등을 위하여 웹 서버나 메일서버, WAS등의 서버를 분석

### ● 모바일포렌식

-휴대폰,PDA, 전자수첩, 디지털카메라, MP3, 캠코더, 휴대용 메모리카드, USB저장장치 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 분야

## ▶ 분석대상[3/4]

### ● 데이터베이스포렌식

-DB로부터 데이터를 추출/분석 하여 증거를 획득하는 분야

-방대한 양의 데이터로부터 증거 수집 및 분석을 위한 기술, ERP 기반에서 개발된 회계시스템 등의 대형 시스템을 위한 하드웨어 및 소프트웨어 기술, 다양한 DB관리 시스템에 대한 제어 기술 등이 필요

### ● 암호학포렌식

-문서나 시스템에서 암호를 찾아내는 분야

-암호가 될 수 있는 숫자나 문자를 고속으로 대입하여 비교하는 크랙 프로그램을 개발하여 무차별 대입 공격 기법이나 사전대입 공격 기법을 빠른 속도로 실

## ▶ 분석대상[4/4]

### ● 회계포렌식

- 기업의 부정과 관련된 수사를 할 때 저장된 회계 데이터를 추출하고 회계사 등 회계 전문가가 분석할 수 있도록 데이터를 정제하는 분야
- 회계 시스템에 대한 프로그램을 개발한 경험이 있거나 회계 시스템을 운영해 본 경험이 있는 전문가가 필요

### ● 메모리 포렌식

- 메모리에 로드 되는 정보들을 분석 할때 활용하며, 사고대응포렌식 분야에서 빠르게 시스템의 정보를 분석 할 때 유용하게 활용 할 수 있으며, 휘발성 정보(프로세스, 네트워크 등)를 한번에 분석 할 수 있음
- 하지만 증거추출 포렌식 분야에서는 법정 증거로 채택이 안됨. 사고대응포렌식 분야에서만 활용하고 있음

### 3.Digital Forensic 절차

▶ 컴퓨터 범죄수사나 민사소송 또는 침해사고 대응을 위하여 디지털 포렌식을 적용하는데 이 때, 일반적인 수행 절차로 준비, 수집, 이송, 분석, 보고서 작성의 순서로 수사가 이루어짐.

## ● 방법론



## ▶ 수사준비

- 관리적/기술적으로 준비를 하는 과정으로 컴퓨터포렌식에 사용되는 각종 소프트웨어 또는 하드웨어를 준비하고 점검 하는 단계.

### -전문인력과 포렌식 도구의 활용방안 수립

▶ 다양한 운영체제 및 파일 시스템, 네트워크,DB,회계 시스템 등의 기술을 가진 전문가들이 조사관으로 참여하여 각종 전문적인 도구를 이용하여 신속 정확하게 증거를 수집

### -보관의 연속성 방안 수립

▶ 증거를 가져간 시간, 돌려준 시간, 소지한 이유 등을 정확히 기록함으로써 증거가 훼손되지 않았음을 보여주고 무결성을 입증하기 위한 구체적인 방안을 수립

### -데이터의 무결성 유지방안 수립

▶ 확보된 데이터의 증거능력을 확보하고 공판과정에서 공소사실을 입증하는 증거로써 가치를 부여하기 위해 무결성을 입증할 수 있는 여러 가지 방법을 결정

-추가로 압수수색영장,진술서 양식, 자문가 연락처, 관리자 승인, 현장 채증 준비, 증거분석 툴 등을 준비함



## ▶ 증거물 획득

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

### -휘발성 정보수집

>시스템을 종료하거나 전원을 차단할 경우 휘발성 데이터가 손실되므로 현재의 상태가 유지되는 상태에서 프로세스, 메모리, 자원 사용정보 등의 휘발성 정보를 수집

### -디스크 이미징

>증거대상 디스크와 정확히 같은 사본을 만드는 과정을 말함. 압수된 디스크를 조사/분석하게 되면 증거가 손상될 우려가 있으므로, 이미지를 가지고 조사/분석을 진행해야 함.

### -증거의 무결성

>해쉬 및 검증 알고리즘을 원본 디스크와 디스크 이미지에 적용하여 보관한 뒤, 법정 증거 제출시 무결성 확보 여부를 주장할 수 있음.

## ▶ 디지털증거 수집단계[1/3]

- 피해 사고 발생 장소 또는 용의자 컴퓨터를 압수하는 현장에서 각종 저장매체와 시스템에 남아 있는 디지털 증거를 획득하는 단계.
- 휘발성 증거우선 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
- 전원차단 여부 결정
  - 서버의 경우는 전원을 차단하기 전에 프로세스 정보가 유실되지 않도록 Shutdown
  - 네트워크에 연결되어 있는 경우에는 수시로 원격으로 접속하여 데이터 삭제가 가능하므로 이에 대비하여 사전에 네트워크 단자를 제거

## ▶ 디지털증거 수집단계[2/3]

- 전원차단 방법

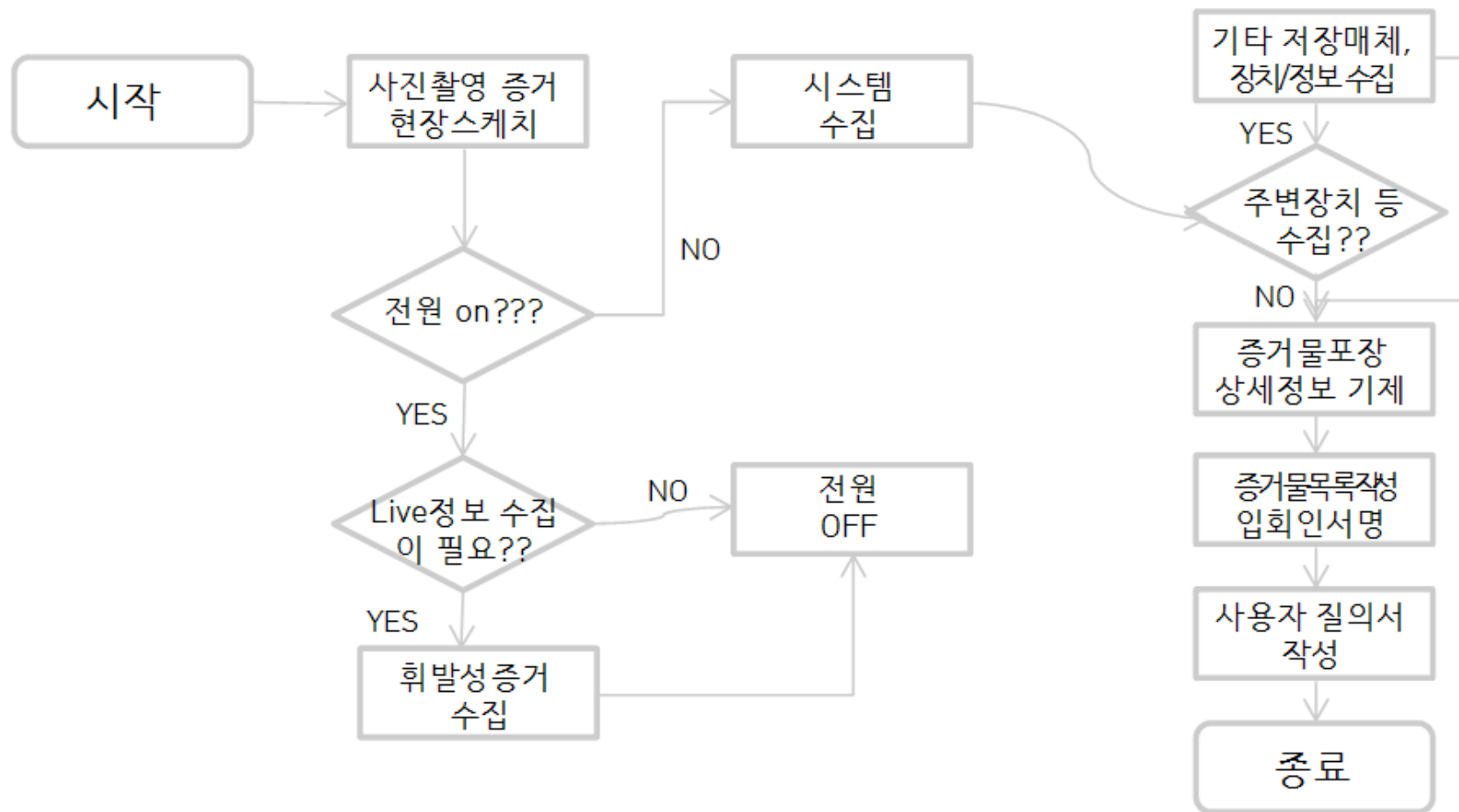
운영체제	전원차단 방법	비고
윈도우(개인PC)	전원 플러그 바로 분리	정상 종료 절차를 수행하면 임시데이터가 삭제됨
윈도우(서버)	정상 종료 후 분리	
Linux	정상 종료 후 분리	
Unix	정상 종료 후 분리	
Macintosh	전원 플러그 바로 분리	정상 종료 절차를 수행하면 임시데이터가 삭제됨

## ▶ 디지털증거 수집단계[3/3]

### ● 증거수집 대상에 따른 대응

- 개인용컴퓨터인 경우 본체를 그대로 증거로 채택하거나 하드디스크를 분리하여 복제하고, 데이터가 대기업의 회계관련 DB 또는 ERP 등 대형 컴퓨터에 저장되어 있는 경우에는 전문가의 도움을 받아 상황에 따른 적절한 증거 수집이 수행 되어야 함
- 증거의 위치나 수집순서가 결정되면 증거 수집 프로그램 및 도구를 사용하여 사건과 관련 성이 있는 데이터를 중심으로 증거 수집
- 수집한 매체의 종류에 따라 PC, 서버, 이동형 저장매체 등의 출처, 사용자, 관련부서, 연락처 등을 정확히 기재하여 나중에 혼동되는 일이 없도록 해야 하며 라벨을 부착
- 증거 수집과정에서 사용한 도구의 이름, 버전, 분석과정, 시간, 산출 결과 등 전 과정도 기록

## ▶ 디지털 증거물 획득 절차



## ▶ 디지털증거물 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 한의 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 것 만으로도 데이터 변조가 있으므로 각별히 주의

## 이송 및 보관

- 디지털증거의 경우 전자기파(EMP)에 노출되면 저장된 내용이 훼손되기 때문에 수집된 증거물을 안전한 방법으로 분석실 또는 보관소로 옮겨야 함.

### -증거자료는 반드시 이중으로 확보

- >디스크이미지 사본확보로 우발 상황 대비

- >쓰기 방지 조치 및 봉인, 증거물 담당자 목록 유지

### -증거물 이송

- >Bubble Wrap, 정전기 방지용 팩, 하드케이스를 이용하여 이송하고 접근통제가 가능한 공간 확보

### -연계보관

- >현장에서 증거가 법정에 제출될 시점까지 거쳐간 경로, 담당자, 장소 시간을 기록

- >증거의 무결성 증명을 위하여 담당자 목록을 통해 최초 수집자로부터 법정제출까지 담당자가 유지되어야 하며, 인수인계과정에서 상호 증거를 확인하는 절차가 필요

## ▶ 분석 및 조사

- 증거물 분석단계는 증거물의 내부를 확인하고 범죄에 관련된 파일 또는 정보를 획득하는 과정.  
조사/분석 기술 중 필수적인 요소로 데이터 복구, 은닉정보 검색, 암호파일 해독 등이 있음.

### -데이터 복구 및 증거물 분석

- >디지털 증거를 추출하기 위해 암호 복구, 데이터 복구, 키워드 검색 및 정보 추출, MAC Time 분석 등 다양한 포렌식 도구를 사용하여 증거물을 과학적이고 기술적으로 분석
- >분석과정이 명확하고, 결과도출이 논리적으로 이루어져야 함
- >재현이 가능해야 하며, 증거물 훼손 및 내용변경이 금지되어야 함



## ▶ 보고서작성

- 컴퓨터포렌식 절차 중 마지막 단계로 디지털 증거수집, 운송 및 보관, 조사/분석 단계의 모든 내용을 문서화 하여 법정에 제출하는 단계.

-누구나 알기 쉬운 형태로 작성

-증거물 획득, 보관, 분석 등의 과정을 6하 원칙에 따라 명백하고 객관성 있게 설명해야 하며, 예상하지 못한 사고로 데이터가 유실되어 변경이 생겼을 경우 이를 명확히 기재하고 범죄 혐의 입증에 무리가 없음을 논리적으로 설득할 수 있어야 함

-수사 기관에서 조사 분석할 수 없어 외부에 이를 의뢰하였거나, 컴퓨터포렌식 서비스 또는 전문가에게 상담을 의뢰하였다면, 그 결과를 전문가 소견서 형태로 제출하고 전문가(Expert)를 법정에 참고인으로 출석할 수 있게 해야 하는 과정도 포함

## 결과 보고서 작성에 따른 주의사항

- 수사관이 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리 정연하게 작성
- 추정을 배제하고, 사실 관계를 중심으로 작성
- 객관적 사실, 설명내용, 분석관 의견을 구분하여 작성
- 증거 발견 방법 및 증거물에 대한 작업 내용은 명확하게 문서화
- 분석 및 처리과정을 사진 또는 영상 등으로 기록 유지
- 분석에 사용된 하드웨어와 소프트웨어의 정보를 반드시 기록
- 작성이 완료되면 분석담당관의 서명 후 원본 증거물과 함께 의뢰인에게 송부
- 수정이 불가능한 문서자료 형태로 작성하여, 관련 사건의 재판 종결 시, 또는 공소시효 만료시까지 증거 보관실에 보관

## ▶ 디지털포렌식 분석 보고서

### Digital Forensic REPORT

분석자 : 이 별

### 디지털증거 분석보고서

접수일자

분석번호

판리번호

분 석 자

분석일시

장 소

분석대상

수 량

요청기관

요청사항

분석결과

## 디지털포렌식 분석 보고서

6. 세부 내역(Encase)

가. 리피받은 케이스 오픈 상태

File Name	Size	File Type	File Category	File Location	File Hash	File Date	File Owner
Encase Case File	100,000,000	Encase Case File	Encase Case File	Encase Case File	Encase Case File	Encase Case File	Encase Case File
Encase Case File	100,000,000	Encase Case File	Encase Case File	Encase Case File	Encase Case File	Encase Case File	Encase Case File
Encase Case File	100,000,000	Encase Case File	Encase Case File	Encase Case File	Encase Case File	Encase Case File	Encase Case File

나. 의


- E

및

리

다. 증

증거1: Forensic\_Accuention.jpg 복원 결과



EO 00)인대

다. 증거2. forensic-heroes.doc

File Name	Size	File Type	File Category	File Location	File Hash	File Date	File Owner
forensic-heroes.doc	100,000,000	Word Document	Word Document	Word Document	Word Document	Word Document	Word Document
forensic-heroes.doc	100,000,000	Word Document	Word Document	Word Document	Word Document	Word Document	Word Document
forensic-heroes.doc	100,000,000	Word Document	Word Document	Word Document	Word Document	Word Document	Word Document

그림1

파일

확장

00)인대

다. 증거3.

File Name	Size	File Type	File Category	File Location	File Hash	File Date	File Owner
증거3	100,000,000	Image File	Image File	Image File	Image File	Image File	Image File
증거3	100,000,000	Image File	Image File	Image File	Image File	Image File	Image File
증거3	100,000,000	Image File	Image File	Image File	Image File	Image File	Image File

그림 1-4

## ▶ 디지털포렌식 분석 보고서

- <그림 1-4>의 HEX 값을 바꾸어 볼때 JPG 파일헤더값(FF D8 FF E0 00)인데 파일의 확장자를 ZIP(압축파일)로 변조한 것으로 추정됨.  
확장자 JPG로 변경후 저장.

1. 증거물

다. 증거 4

이름: 4.jpg  
크기: 1.0MB  
형식: JPEG

이름: 4.jpg  
크기: 1.0MB  
형식: JPEG

- <그림 1-4>  
JPG 파일

이름: 4.jpg  
크기: 1.0MB  
형식: JPEG

```
00000000h: FF 10 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 77 3F IF .....
00000010h: 05 00 00 00 11 00 00 00 18 00 00 00 08 00 00 00 : .....
00000020h: 00 00 00 00 0A 00 00 00 08 00 00 00 0C 00 00 00 : .....
```

<그림 1-4 HEX 값 수정>

### 6. 분석결과

구분	상태	Before	After	결과
Forensic Analysis		Forensic Analysis	Forensic Analysis	정상복원
4.jpg				정상복원
forest				정상복원
cc				정상복원
출판사:				정상복원
책 175				정상복원
계 175				정상복원
책 175				정상복원
Book 175				정상복원

작성일: 2016. 7. 28

분석자: 이별 (인)

확인자: 홍길팔 (인)

## 4.Digital Forensic 도구(장비)

## ▶ 디지털포렌식 도구 H/W

구분	제품명
디스크 복제 장치	<ul style="list-style-type: none"> <li>ICS imagemasster Series</li> <li>Logicube Dossier &amp; Falcon</li> <li>Tableau TD3</li> <li>DataExpert Magicube</li> <li>RedEye Forensic Duplicator Kit II, III</li> </ul>
이동형 포렌식 워크스테이션	<ul style="list-style-type: none"> <li>Forensic Air-Lite MK III</li> <li>ICS RoadMasster 3</li> <li>Forensic Air-Lite M-15-SR</li> </ul>
휴대용 포렌식 도구	<ul style="list-style-type: none"> <li>Encase Portable</li> </ul>
HDD 쓰기 방지 장치	<ul style="list-style-type: none"> <li>ICS super DriverLock</li> <li>Tableau Tableau Forensic Bridge</li> <li>Wiebetech Wiebetech Dock</li> </ul>
USB 쓰기 방지 장치	<ul style="list-style-type: none"> <li>Wiebetech USB WriteBlocker</li> </ul>
메모리카드 쓰기 방지 장치	<ul style="list-style-type: none"> <li>Ics Write Protect Card Reader</li> </ul>

## ▶▶ 디지털포렌식 도구 S/W

구분	제품명
디스크 포렌식 솔루션	<ul style="list-style-type: none"> <li>• Guidance Encase</li> <li>• AccessData Forensic Toolkit</li> <li>• 파이널데이터 Final Forensics</li> <li>• Nuix</li> <li>• Autopsy</li> <li>• WinHex Forensic</li> </ul>
휴대폰 포렌식 솔루션	<ul style="list-style-type: none"> <li>• Paraben Device Seizure</li> </ul>
라이브 포렌식 도구	<ul style="list-style-type: none"> <li>• SIFT 3</li> <li>• Helix 3</li> </ul>
활성 시스템 조사 도구	<ul style="list-style-type: none"> <li>• LDFS</li> </ul>
윈도우 레지스트리 분석 솔루션	<ul style="list-style-type: none"> <li>• Rega</li> </ul>
휴대폰 데이터 분석 솔루션	<ul style="list-style-type: none"> <li>• 한컴 MD-NEXT</li> <li>• XRY</li> <li>• UFED</li> </ul>



## ▶ 디지털포렌식 도구 기타

- 데이터 복구를 위한 복구도구(R-Studio, Recover My File 등 )
- 현장 촬영용 카메라
- 현장 녹화용 캠코더
- 연계 보관성을 위한 서류 및 라벨
- 증거 보관을 위한 케이스
- 증거 손상을 막기 위한 충격흡수 봉투(케이스)
- 정전기 방지를 위한 정전기방지 봉투
- 증거운송을 위한 충격완화 증거 운반용 박스

## 5.디지털포렌식 실습 포렌식 도구 살펴보기

## 5.디지털포렌식 실습 이미징 수집 및 부팅



**Thank You !**