[2020 SWLUG 종강 세미나]

디지털포렌식을 활용한 다양한 사례와 도구 및 과정 살펴보기

-정보보호학과 20 김수현-

[차례]

CONTENTS 1

디지털 포렌식 사례 살펴보기 (2가지)

CONTENTS 2

디지털 포렌식에서 사용되는 도구 살펴보기

CONTENTS 3

디지털 포렌식 과정 살펴보기

[디지털 포렌식이 활용된 사례 2가지]

1. 피의자의 자택에서 압수한 스마트폰의 소유자 추정 사례

2. PC를 이용하여 영업 비밀을 유출한 사례

[1. 피의자의 자택에서 압수한 스마트폰의 소유자 추정

<상황 설명>

1) 해당 스마트폰은 해당 피의자 명의로 개통된 것이 아니며 피의자도 자신의 것이 아니라고 주장함

2) 로그인 되어 있는 계정이 여러 개

3) 실제로 피의자는 자신은 모르는 문건이고 왜 저장되어 있는지 모른다고 진술

Q1. 그러면 해당 스마트폰의 소유자나 사용자가 피의자라고 하는 근거가 무엇일까?

Q2. 로그인 되어 있는 계정이 여러 개인데, 이 경우 다른 사람의 소유이거나 피의자가 잠깐 사용했을 가능성이 존재할까?

Q3. 그 외에 소유자 또는 주 사용자라고 할 만한 근거가 존재하는가?

Q4. 스마트폰의 주 사용자가 피의자라고 할지라도 사용한 사람이 여러 명이라면, 피의자가 아닌 다른 사람이 작성하였을 경우도 존재하는가?

[1. 피의자의 자택에서 압수한 스마트폰의 소유자 추정 사례]

Q1. 그러면 해당 스마트폰의 소유자나 사용자가 피의자라고 하는 근거가 무엇일까?

일단, 스마트폰에 로그인 되어있는 여러 이메일 계정 중 피의자와 피의자의 배우자의 계정이 먼저 있었다.

또한, 어플리케이션에서 사용한 ID, 닉네임 등이 피의자가 주로 사용하는 ID 및 닉네임과 일치하는 점에서 피의자가 소유 또는 사용하는 것이 맞다고 추정된다.

[1. 피의자의 자택에서 압수한 스마트폰의 소유자 추정 사례]

Q2. 로그인 되어 있는 계정이 여러 개인데, 이 경우 다른 사람의 소유이거나 피의자가 잠깐 사용했을 가능성이 존재할까?

해당 스마트폰에 저장되어 있던 사진 중 피의자 본인 사진이 존재

해당 기기로 사진을 찍을 경우 사진을 생성한 기기의 정보와 위치정보 및 시간정보가 함께 저장됨

그리고 찍힌 사진이 자동으로 저장되는 폴더가 존재

국과수 디지털포렌식 결과 이 사진은 다운로드 받거나 외부에서 삽입된 파일이 아니며, 해당 스마트폰으로 생성된 것으로 보아 피의자 소유이거나 피의자가 주로 사용하는 것으로 추정함.

[1. 피의자의 자택에서 압수한 스마트폰의 소유자 추정 사례]

Q3. 그 외에 소유자 또는 주 사용자라고 할 만한 근거가 존재하는가?

해당 사진의 위치정보의 경우 피의자의 동선과 일치했음

이메일에 로그인 & 특정 포털 어플리케이션을 이용하는 경우 자동으로 시간정보와 위치정보가 저장되는 '캐시정보' 로 미루어 보았을 때 해당 스마트폰의 시간 및 위치정보와 피의자의 동선과 일치했음

[1. 피의자의 자택에서 압수한 스마트폰의 소유자 추정 사례]

Q4. 스마트폰의 주 사용자가 피의자라고 할지라도 사용한 사람이 여러 명이라면, 피의자가 아닌 다른 사람이 작성하였을 경우도 존재하는가?

해당 유출자료 문서파일이 스마트폰에서 작성되고 생성된 것이 아님은 맞았음

국과수의 디지털포렌식 결과 이 문서파일은 이메일을 통해 다운로드 받았는데, 피의자의 계정을 통해 다운로드 받은 사실이 확인되었으며, 보낸 이의 이메일 계정은 해당 스마트폰을 개통한 기업 내부직원의 ID로 확인되었음

[2. PC를 이용하여 영업 비밀을 유출

<상황 설명>

1) 피의자가 00시간대에 PC를 사용함.
2) 피의자가 이메일을 통해 공모자에게 자료를 전달함.

Q1. 피의자가 00시간대에 PC를 사용했다는 자료는 무엇일까?

Q2. 위의 근거를 조사한 결과는?

Q3. 피의자가 이메일을 통해 공모자에게 중요자료를 전달했다는 사실을 어떻게 알 수 있는가?

Q4. 위의 근거를 조사한 결과는?

[2. PC를 이용하여 영업 비밀을 유출한 사례]

Q1. 피의자가 oo시간대에 PC를 사용했다는 자료는 무엇일까?

<이벤트 로그(event log)란..?>

감사 추적 제공을 위해 시스템 실행 시 발생하는 이벤트를 기록하며, 시스템 활동을 이해하고 문제를 진단하는 데 사용되는 것

PC가 부팅되어 작업들이 이루어지고 종료되기까지의 기록은 "이벤트 로그"에 저장된다.

그리고 이벤트 로그 중 하나인 "시스템 이벤트"에는 부팅 기록 정보와 계정 로그인, 로그아웃 정보가 존재한다.

[2. PC를 이용하여 영업 비밀을 유출한 사례]

Q2. 위의 근거를 조사한 결과는?

디지털 포렌식 분석 결과, 해당 PC는 00시00분에 부팅되었고 관리자 계정의 로그온이 00시00분에 이루어졌음을 확인.

PC가 위치한 사무실의 내부 CCTV에 저장된 영상을 확인할 결과, PC의 부팅 시간과 일치하는 시간에 피의자가 PC를 사용한 정황이 포착됨.

[2. PC를 이용하여 영업 비밀을 유출한 사례]

Q3. 피의자가 이메일을 통해 공모자에게 중요자료를 전달했다는 사실을 어떻게 알 수 있는가?

이메일 클라이언트 프로그램을 사용해서 이메일을 주고 받으면 PC에 이메일 데이터가 저장됨.

저장경로는 클라이언트 프로그램마다 다르지만 이메일 데이터를 분석하면 송*수신자 메일 주소, 시간, 메일의 본문내용, 첨부 파일 등을 알 수 있음.

[2. PC를 이용하여 영업 비밀을 유출한 사례]

Q4. 위의 근거를 조사한 결과는?

디지털 포렌식 분석 결과,
피의자가 사용한 PC의
C:\Users\Administrator\AppData\Local\Microsoft\Outlook
경로에 ost, pst 확장자 파일이 존재함.

이 파일들은 Outlook Express 프로그램으로 이메일을 송*수신 할 때 저장되는 파일들이며 송*수신자 이메일 주소와 피의자, 공모자 이메일이 일치함.

첨부파일의 Hash값과 중요자료의 Hash값이 동일했음.

[디지털 포렌식에서 사용되는 도구 살펴보기]

01 공개용 디지털포렌식 도구

·디스크 분석 도구

· 이메일 분석 도구

· 파일 및 데이터 분석 도구

· 인터넷 히스토리 분석 도구

· 레지스트리 분석 도구

· FTK Imager(AccessData사)

· EnCase Forensic Imager(Guidance Software)

02 상용 디지털포렌식 도구

· ★ FTK(AccessData사)

· Encase(Guidence Software)

· X-Ways Forensic(X-Ways 사)

· MAGNET AXIOM(Magnet Forensic)

· CTF

03 기타 디지털포렌식 도구

Autopsy

· ★ Volatility

· ★ HxD

[1. FTK Imager & FTK]

조사하고자 하는
디지털 데이터의 사본을
생성!

FTK Imager

VS

FTK

1) 대상 시스템에서 포렌식 도구를 실행하여 사본을 생성

2) 원본 저장매체를 분리하여 사본을 생성하는 경우

1) 원본 저장매체를 분리하여 사본을 생성하는 경우

2) 네트워크를 통해 사본을 생성하는 경우

[1. FTK]

FTK

[데이터 획득]
[데이터 분석]
[데이터·분석 결과 기록]

<데이터 분석>

1) 라이브 서치 & 인덱스 서치 - 키워드 및 특정 패턴을 알고 있는 경우에 사용

2) KFF를 이용한 해시 분석 - 알려진 해시 값을 오해 불필요한 파일을 제외 또는 특정 파일만 찾아내고자 할 경우에 사용

3) 퍼지 해시 분석 - 문서를 비교하여 두 문서 간의 유사성을 비교할 수 있음

4)OS Artifacts Analysis - 윈도우 운영체제의 구성성 특징을 이용하여 여러 가지 데이터를 분석

<데이터·분석 결과 기록>

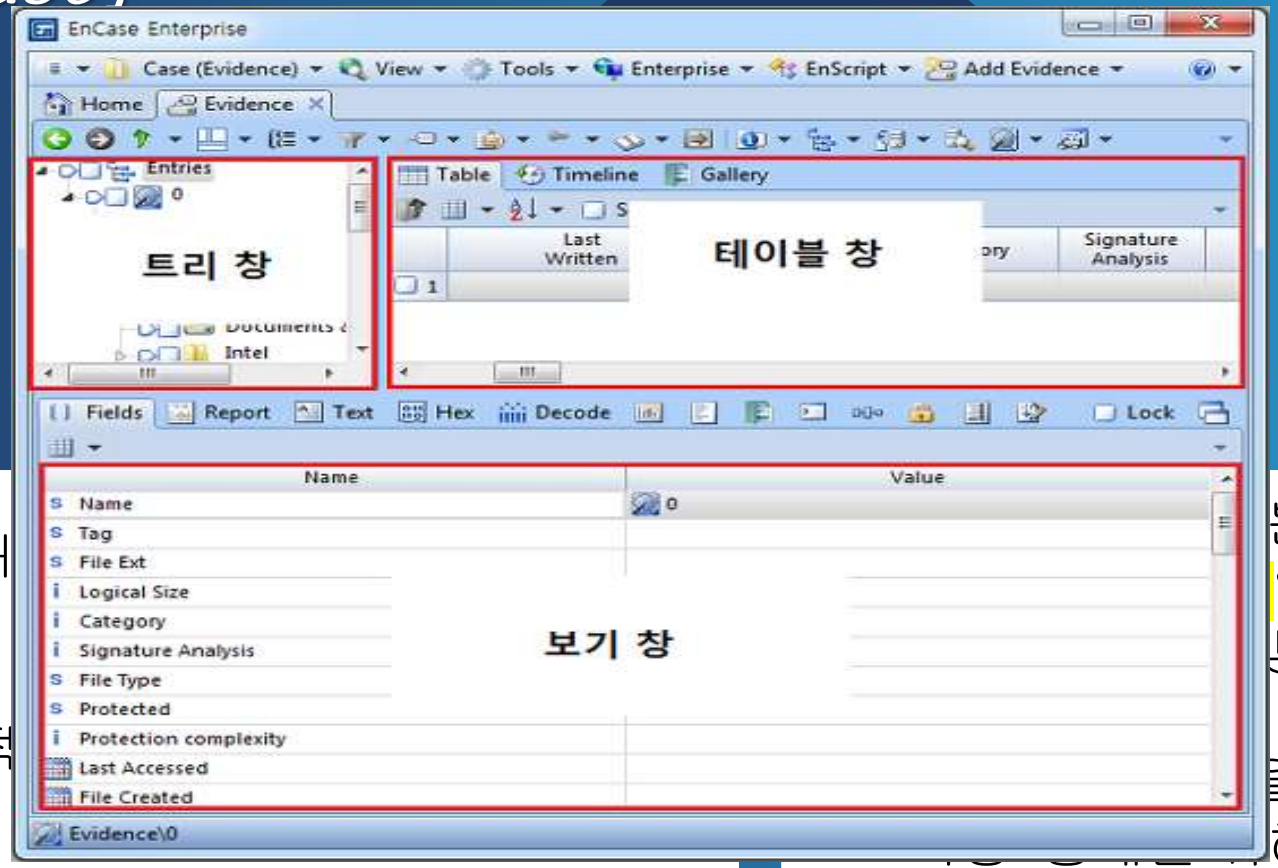
1) 북마크 & 라벨 기능 - 의심 가는 파일과 분석을 통해 얻은 결과를 체계적으로 기록할 수 있는 기능을 제공

2) 보고서 생성 기능 - 분류된 데이터들을 보고서로 작성할 수 있는 기능을 제공

3) 실시간 데이터 베이스에 저장하는 기능 - 분석 도중 시스템의 전원이 꺼지거나, 시스템이 중단되어 프로그램이 다운되더라도 그때까지 분석된 데이터들을 그대로 보존

[2. EnCase]

https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r#lifecycle



[디지털포렌식 전문가들을 위한 표준 도구로 사용되고 있음!]

출처: https://k-dfc.tistory.com/39

1) 미국
개발 및 판매

2) 전 세계적

3) 미국 NIST의 CFTT 검증 또한 받았기 때문에, 수사기관 및 조사기관에서 가장 선호하는 분석 도구 중 하나

분석 도구가 갖추어야 할
" 과 "분석 기능 " 을 모두
갖추고 있음

을 출시하면서 , 조사의 편
해서 Pathway기능을 추가,
해시 분석의 편의성 증대를 위해 Project VIC를 통합(다른 기능들도 추가적으로 포함)

[3. Volatility]

https://github.com/volatilityfoundation

Volatility

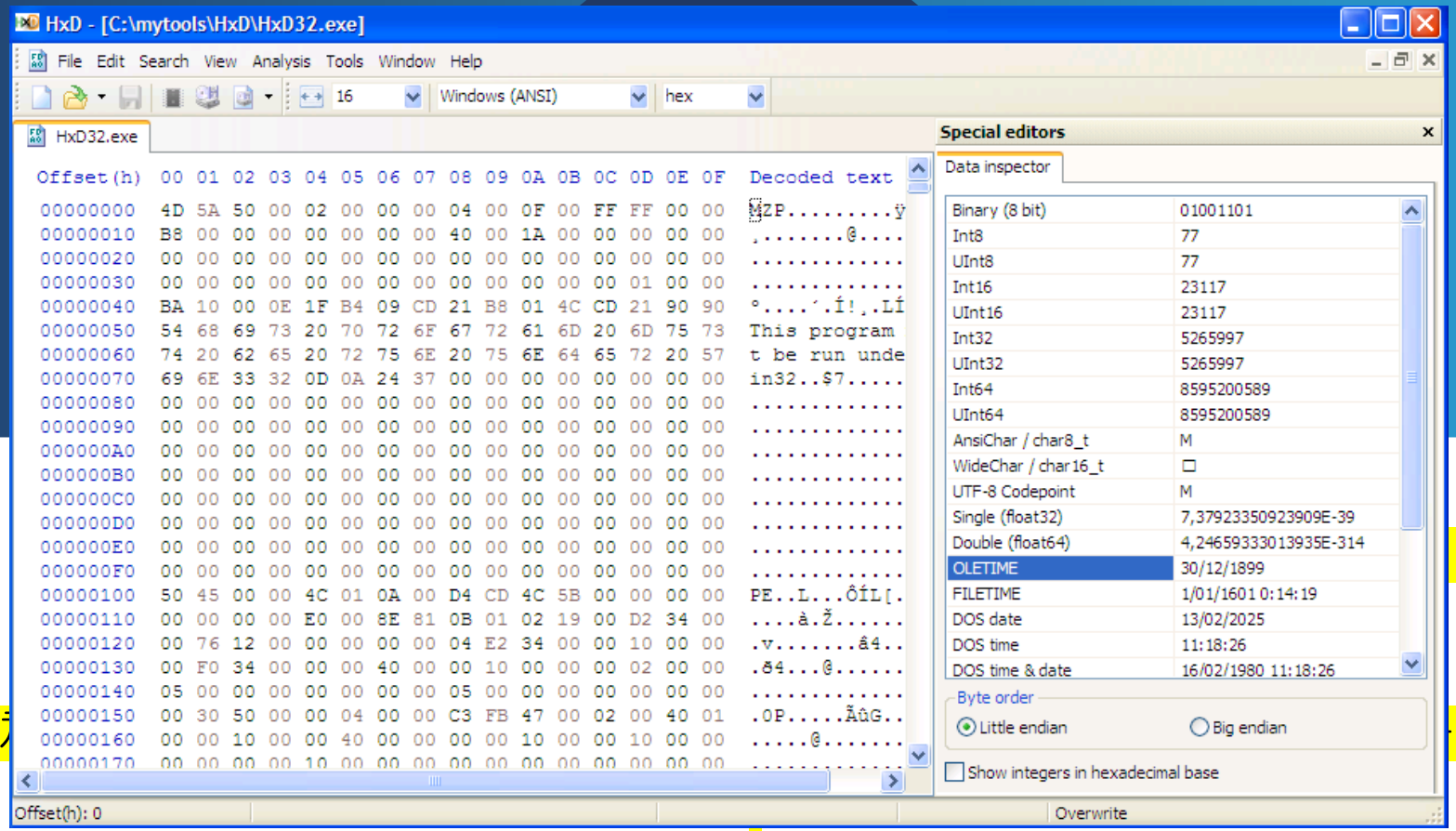
1) 메모리를 덤프 및 분석을 위해 가장 많이 사용되는“파이썬 기반 오픈소스 디지털 포렌식 도구”

2) 주로 사용되는 경우: 실행파일 또는 프로그램이 실행 중인 경우 & 종료 후에 메모리상에 남아 있는 정보를 추출하는 경우 & 프로세스 관련 모듈과 라이브러리 정보 추출 & 악성코드가 감염된 피해시스템에서 외부 네트워크 접속 시도 정보 및 공격자가 접속한 원격시스템 확인

→ 메모리 상에서만 존재하는 운영체제나 소프트웨어 및 파일과 관련된 다양한 데이터의 정보를 추출하여 분석

→ 현재 CTF 문제를 풀 때 자주 사용되는 디지털 포렌식 도구 중 하나

[4.HxD]



1) 단위

2) 자분

3) Volatility와 마찬가지로 CTF문제를 풀 때 자주 사용되는 디지털포렌식 도구 중 하나

출처: https://www.portablefreeware.com/index.php?id=1454

[디지털포렌식 수행과정 살펴보기]

01 증거의 획득

1) 조사할 디지털 저장매체와 기록정보를 식별, 이를 증거로서 수집하는 절차

2) 디지털포렌식 수행과정 중에 가장 중요한 과정

3) 가장 먼저 수행되는 디지털 포렌식 과정이기 때문에 정당성의 원칙을 위반하였을 경우, 모든 증거의 증거능력이 부정됨

02 증거 분석

1) 획득 과정에서 생성한 증거분석용 이미지. 파일을 이용하여 실제 원본증거물에 존재하던 내용을 조사

2) 범죄 증거를 발견하면 파일의 분석과 확인 과정이 어떻게 되었는지 문서화가 필요

3) 원본 데이터의 무결성을 유지 & 분석 결과물의 신뢰성 보장 필요

03 증거 보관

1) 전자적 증거물도 보관 도중 물리적으로 훼손이 되거나 바이러스에 의한 파괴되는 경우가 발생하여 무결성을 유지하지 못하면 조작의 의심 등을 받을 수 있음

2) 증거물의 보관을 위해 반하는 경우 충격이나 물리적인 공격에 안전한 케이스를 이용해야 하며, 보관할 때는 적합한 보관 장소에 보관 하여야 함

04 증거 제출과 증거조사

1) 증거물의 획득과정을 알 수 있도록 하여 증거물로 채택되었을 때 증거물로서의 타당성을 제공하는 문서화 작업이 필요

2) 일련의 과정이 명백히 확인되어야 하며, 제 3자의 전문가가 검증했을 때도 신뢰성을 보장할 수 있는 문서화 작업은 꼭 필요

05 제3자의 검증

1) 포렌식 전문가 또는 한국포렌식 학회의 감정 또는 법원의 검증과정에서의 제3자의 재생 재현이 필요

[기타 – 분석방법에 관한 보고서 기재요령 예시]

출처: https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000073689

디지털증거 분석보고서

접수일자	2010. 5. 25
분석번호	Case 1
관리번호	20100525_KMJ
분 석 자	OOO대 OO대학원 정보보호전공 OOO 전화 OOO-OOO-OOOO 핸드폰 OOO-OOO-OOOO
분석일시	2010. 5. 25 ~ 2010. 5. 27
장 소	OOOOOO
분석대상	CFPA20-2.E01 파일
수 량	1본
요청기관	OO대 OO대학원 사이버포렌식 과정
요청사항	피의자 노트북 하드디스크에 저장된 범죄 증거물 분석
분석결과	Encase Image File을 분석 수행하였으며 분석도구는 Encase 4.2로 분석하였음 의심 파일 5개 발견

(별지 제3호 서식) <개정 2016. 12. 26.>

분석보고서

접 수 일 자
지 원 번 호
증 거 번 호

분 석 일 자
장 소

분 석 대 상

요 청 기 관

요 청 사 항

종합분석결과 ○
-
-
-
○
-
-

20 . . .

○○○○검찰청
디지털포렌식팀
디지털포렌식 수사관

[기타 – 분석방법에 관한 보고서 기재요령 예시]

출처: https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000073689

(별지 제7호 서식) <신설 2016. 12. 26.>

National Digital Forensic Center

디지털증거 폐기 확인서

피의자 에 대한 ○○○○검찰청 20__형제____(20__요청____) 사건에 관하여 20 . . . : 검사 의 폐기 지휘에 따라 대검찰청 국가디지털포렌식센터(NDFC)에서 폐기한 디지털증거는 다음과 같습니다.

순번	디지털증거명	보관 증거번호	용량	등록일시	폐기일시	폐기방법
1						

위와 같이 디지털증거를 폐기했음을 확인합니다.

20 . . .

디지털증거 관리책임자 (서명 또는 날인)

발급번호: 출력시간:

(별지 제4호 서식) <신설 2015.7.16.>

【정보저장매체 등 제출 확인서】

피압수자(임의제출자)	성명 : 생년월일 : 연락처(전화번호) :
압수(임의제출) 일시, 장소 등	
전원차단 일시, 장소 등	
기기의 종류, 제조사·모델명	기기의 종류 : 제조사 : 모델명(S/N) :
(모바일의 경우) 실사용자, 전화번호, 사용여부 등	실사용자 : 가입자명 : 전화번호, 통신사 : ☐ 현재 사용하고 있는 기기임 ☐ 사용하고 있지 않은 기기임
※ 피압수(임의제출) 기기에 패스워드, 잠금패턴 등이 설정되어 있을 경우 설정 해제된 상태로 송부하거나, 해제가 곤란하면 패스워드, 잠금해제패턴 등을 직접 기재하여 송부 ▣ 패스워드 : ▣ 잠금해제패턴 :	
· 작성일 : 20 . . . · 작성자 : 00검찰청 00부 검찰수사관 000 (서명) · 제출자 000 (서명)	

【이미징 등 참관 여부 확인】

위와 같이 압수 또는 임의제출된 정보저장매체 등에 대하여 이미징 등 과정에 (☐ 참관하겠음, ☐ 참관하지 않겠음) 을 확인합니다.

참관 예정자	성명 : 생년월일 : 연락처(전화번호) :
작성일 : 20 . . . 위 확인자(피압수자·임의제출자 등) : (서명)	

(별지 제4호 서식) <개정 2016. 12. 26.>

【정보저장매체 제출 및 이미징 참관여부 확인서】

피압수자(임의제출자)	성 명 : 생년월일 :	
기기의 종류 등	기기의 종류 : 제조사 및 모델(S/N) : (모바일의 경우) 전화번호 :	
이미징 등 참관	위와 같이 압수 또는 임의제출된 정보저장매체 등에 대하여 하드카피, 이미징, 전자정보의 탐색, 복제(이미징 포함) 또는 출력 등 증거를 확보 과정에 (☐ 참관하겠음, ☐ 참관하지 않겠음)	
	참관 시 참관 범위	하드카피·이미징 [ ] 전자정보탐색 [ ] 전자정보복제·출력 [ ]
	참관 예정자	성 명 : 생년월일 : 연락처(전화번호) :
	위 이미징 등 과정은 _____ 디지털포렌식팀에서 시행 예정임을 검찰수사관 _____으로부터 통지받음	

▣ (모바일 기기의 경우) 유의사항 등 :

- 기기의 이미징 과정에서 분해, 재조립, 내부해선, 펌웨어 체인지(루트권한 관리기관한 획득을 위한 펌웨어의 업로드 및 복제) 등 방법이 필요한 모델의 경우 **기기 손상 또는 데이터 초기화가 될 수 있음**
- 특히 **삼성전자의 일부 안드로이드 기기는** 이미징 과정에서 '녹스'(삼성의 모바일 기기에 탑재된 보안 솔루션)에 영향을 미쳐 이를 기반으로 동작하는 **앱(삼성페이 등)을 이후 사용할 수 없게 되고, 해당 앱의 기존 데이터는 유실됨**
- 녹스 관련 앱(삼성knox, 삼성페이 등)의 사용 여부 (*사용 시 체크 표시)

삼성knox ☐	삼성페이 ☐	기타 ( )

▣ 압수 및 임의제출 기기의 패스코드·잠금패턴, 암호 애플 아이튠스 백업암호 등는 해제 또는 아래 표기

▣ 패스코드·암호 : ▣ 잠금패턴 :

· 작성일 : 20 . . .

· 위 정보저장매체의 제출 및 참관 등 절차를 확인하고, 수사 또는 재판 목적 소멸시 전자정보는 폐기 예정임을 고지 받았으며 위와 같은 사실에 동의함

피압수자·임의제출자 등 : (서명)

검찰수사관 : (서명)

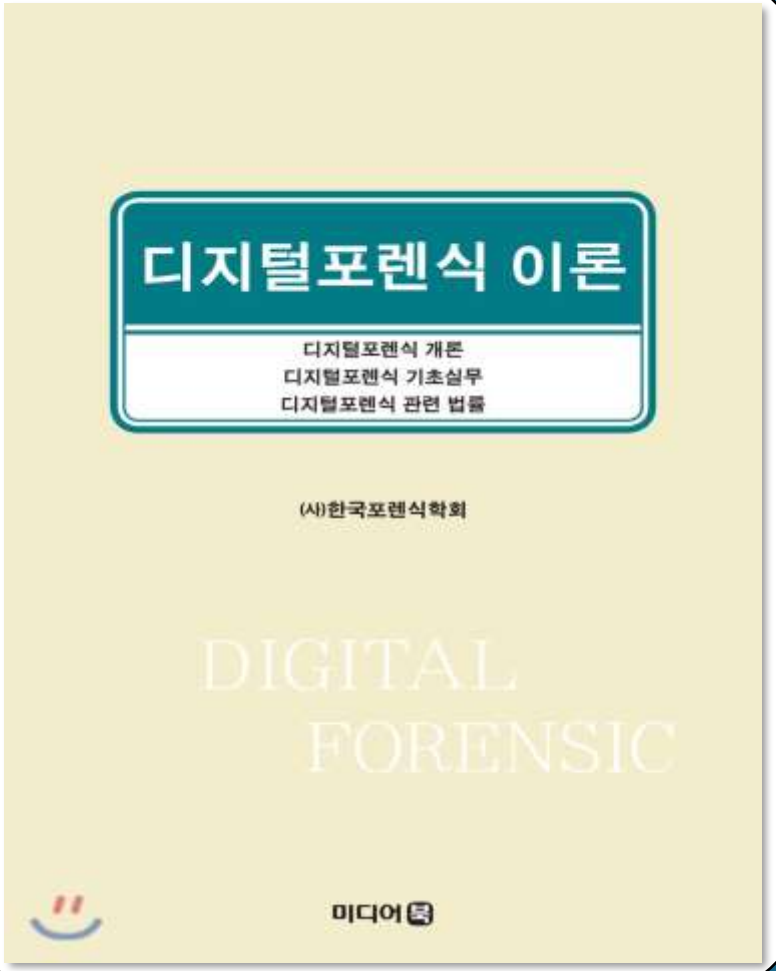
[기타 – 참고문헌]

출처: https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000073689

· 참고문헌 – 디지털포렌식 이론 / (사)한국포렌식학회

< Encase Forensic >
https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r#lifecycle

< Volatility >
https://github.com/volatilityfoundation



<감사합니다>

·PPT 디자인 출처 - http://pptbizcam.co.kr/?p=7234

최근 저의 자료를 카페 등에 무단으로 재배포 하는 일이 자주 발생하고 있습니다.

이에 대해 굉장히 심각한 문제로 받아 들이고 있으며,

해당 문제가 반복될 경우, 재배포한 자에 대해서는 그에 대한 책임을 반드시 물을 것입니다.

저작권을 존중하지 않는 극히 소수의 사용자로 인해 다수가 피해를 보지 않도록 주의해 주시면 감사하겠으며

제 자료가 업로드 된 곳이 있다면 저에게 알려주시면 감사하겠습니다.

제 자료를 소개하고자 할 경우에는

pptbizcam 사이트로의 링크 처리로만 가능하며

파일 자체를 업로드 하는 것은 불가한 점 유의해 주시면 감사하겠습니다.

홍보, 경제적 이익을 취하는 행위 또한 불가합니다.

※기타 활용 가능 범위는 공유 사이트 -> 수다방 게시판 공지사항 참고