디지털 포렌식 이란?

PRESENTER: 박 명 찬

www.happy-maru.com
www.hmconsulting.co.kr

Thinking from your side
행복마루

2017.02.08

❖ 강사소개

이 름	박 명 찬 본부장/공학박사
학 위	2005. 공학박사 취득(정보보안 전공)
경 력	현)행복마루 컨설팅(주) 전략기획본부장 현)한국디지털포렌식 전문가협회 이사 현)한국저작권보호원 디지털과학수사 전문위원 현)행복마루 법무법인 디지털포렌식 자문위원 한국저작권위원회(감정포렌식팀 과장) 프롬투정보통신(정보보안팀 선임연구원)
자 격 증	CISSP, ACE, 디지털포렌식 전문가 2급
수행 경험	A사 협력업체 부정·비리 감사 B사 개인정보 관리실태 진단 C사 인수기업 PMI 감사 G사 기업정보유출 감사 A은행 정보보안 상시 점검 C그룹 정보보안 관리 체계 수립 J사 개인정보 관리실태 진단 문화부, 검찰 합동 저작권위반 OSP 수사지원

❖ 행복마루 컨설팅 소개(1/2)

- ✓ 2011년 대한민국 최초로 고객사에 감사전문가를 상주시키며 **독립적인 내부감사 수행**
- ✓ **디지털 포렌식 기반 부정 · 비리 감사를** 주된 업무영역으로 삼아 성장

2011년 10월

국내 최초로 기업 내 상주형
부정·비리 감사 계약 체결

회사 설립	금융회사 포렌식 전문감사 실시 개인정보보호 관리실태 점검 시작
업무범위 확대	정보보안 감사 Compliance 감사 부정·비리 수사 및 감사
고객사 확대	은행, 보험, 제조, 유통, 에너지, 방송, IT 등
지속적인 성장	외부신고채널 제공 **법무법인, 사모펀드 등과 연계한 서비스 도입**

현재

국내 유일의 디지털 포렌식 전문감사 기업
(Digital Forensic based Audit and Investigation)

❖ 행복마루 컨설팅 소개(2/2)

●●●●○ KT 오전 9:57 70%
news.naver.com

매경이코노미

[PEOPLE] 내부감사 아웃소싱 특화 행복마루컨설팅 조근호 대표 | 감사팀도 못 잡는 내부비리 족집게 적발

본문듣기 | 설정

기사입력 2016.01.18 오후 12:42

0 4

가 가

●●●○○ KT 오전 9:58 70%
news.naver.com

한국경제

[Law&Biz] "검찰 수사하듯 사내 비리 적발"…로펌컨설팅 '현미경 감사'

본문듣기 | 설정

기사입력 2015.03.25 오전 3:31
최종수정 2015.03.25 오전 9:24

0 2

가 가

조근호 변호사가 행복마루컨설팅 직원들의 업무 방식에 대해 설명하고 있다. 김병일 기자

행복마루, 협력업체 샅샅이 조사

●●●○○ KT 오전 10:06 68%
blog.naver.com

blog 고객을 위한 행... MY

포렌식지원서비스

디지털 포렌식팀 박명찬 부장님, 박재현 차장님 인터뷰 :)

2

행복이 +♣ | 2015. 12. 8. 10:50

앱으로 보기 >

목차

❶ 디지털 포렌식 이란?

❶ 디지털 포렌식 이란?

✓ Digital Forensics 美DFRWS(Digital Forensic Research Workshop)

- 범죄현장에서 확보한 개인 컴퓨터, 서버 등의 시스템이나 전자장비에서 수집 할 수 있는 **디지털 증거물에 대해 수집, 보존, 확인, 식별, 분석, 기록, 재현, 보고 등을** 과학적으로 도출하고 증명 가능한 방법으로 수행하는 것

✓ 컴퓨터범죄 수사에 입각한 정의

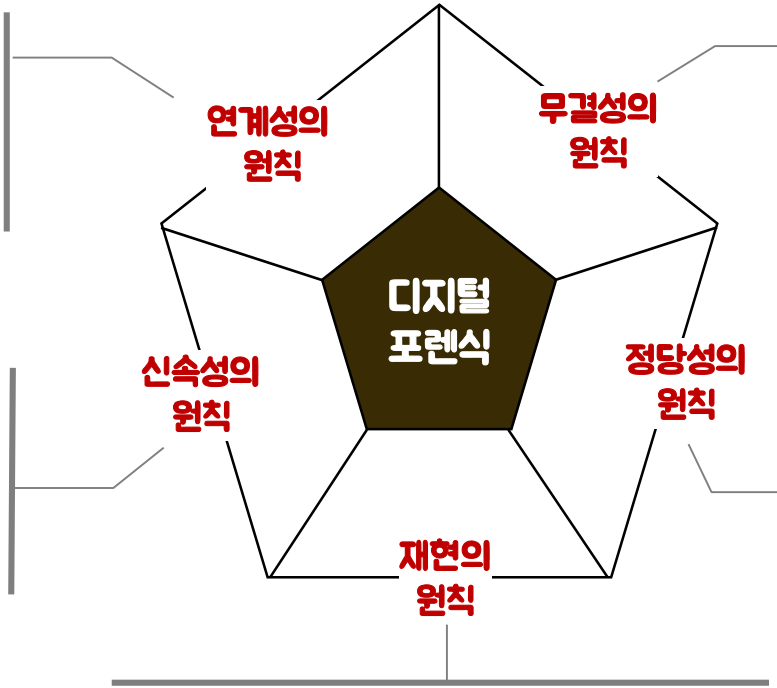
- 컴퓨터 관련 조사·수사를 지원하며 **디지털 자료가 법적 효력을 갖도록 하는 과학적이고 논리적 절차와 방법을 연구하는 학문**

- 디지털자료 : 컴퓨터에만 국한 되지 않음
- 법적 효력 : 법 규범에 합치되는 논리성을 가져야 함
- 과학적/논리적 : 보편성과 객관성이 필요한 지식체계
- 절차와 방법 : 목표달성을 위한 과정이 결과만큼 중요

❶ 디지털 포렌식 이란?

✓ 디지털 포렌식의 기본 원칙

증거물 획득,이송,분석,보관, 법정 제출의 **담당자 및 책임자 명확**



수집 증거가 **위/변조** 되지 않았음을 증명 (Hash값 검증 이용)

시스템의 휘발성 정보 수집을 비롯한 모든 과정은 **지체 없이 신속**하게 진행

입수 증거가 **적법절차**를 거쳐 얻어져야 함

피해 직전과 같은 조건에서 검증 시, 피해 당시와 **동일한 결과가 도출**되어야 함

❶ 디지털 포렌식 이란?

✓ 디지털 포렌식 절차

- 디지털 포렌식을 통한 증거수집 및 분석은 사전 준비 단계에서부터 보고서 작성에 이르기까지 총 5단계로 진행됨

사전 준비 [Preparation]	증거물 수집 [Acquisition]	이송 및 보관 [Preservation]	증거 분석 [Examination]	보고서 작성 [Reporting]
▪ 수집대상 및 범위 검토 ▪ 포렌식 툴 준비 및 검증 ▪ 장비 확보 등	▪ 수집대상 파악 ▪ 현장 보존 ▪ 하드디스크 이미징 (복제) ▪ 증거 수집물 목록 작성 등	▪ 증거물 포장 및 운반 ▪ 원본 디스크 이미지 복사 및 보관 등	▪ 데이터 복구, 추출, 분류, 검색, 분석 ▪ 관련 대상자 인터뷰 수행 등	▪ 용어 설명 ▪ 객관적 설명 ▪ Fact 기반 보고서 작성 등

❶ 디지털 포렌식 이란?

✓ 디지털 포렌식 분류

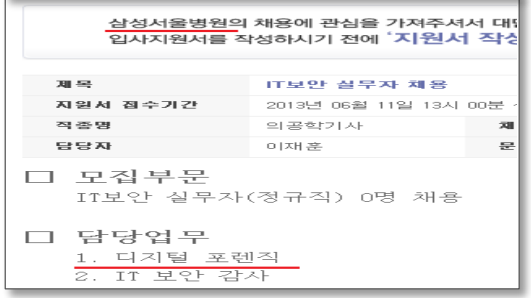
디스크 포렌식	물리적인 저장장치인 하드디스크 플로피디스크, CO ROM, DVD 등 각종 보조기억장치에서 증거를 수집하고 분석하는 포렌식 분야 디스크 파일 시스템 분석, 디스크 검색, 복구, 키워드 검색
시스템 포렌식	컴퓨터의 운영체제, 응용프로그램 및 프로세스를 분석하여 증거를 확보하는 포렌식 분야 시스템 데이터 및 로그분석
네트워크 포렌식	네트워크를 통하여 전송되는 데이터나 암호 등을 특정 도구를 이용하여 가로채거나 서버에 로그형태로 저장된 것을 접근하여 분석하거나 에러로그, 네트워크 형태 등을 조사하여 단서를 찾아내는 분야
인터넷 포렌식	인터넷으로 서비스되는 월드와이드웹(WWW), FTP, USENET 등 인터넷 응용프로토콜을 사용하는 분야에서 증거를 수집하는 포렌식 분야
모바일 포렌식	휴대폰, PDA, 전자수첩, 디지털 카메라, MP3, 캠코더, 휴대용 메모리카드 등 휴대용 기기에서 필요한 정보를 입수하여 분석하는 포렌식 분야 휴대용 기기 데이터 은닉 용이성으로 세심한 분석 필요
데이터베이스 포렌식	데이터베이스로부터 데이터를 추출 분석하여 증거를 획득하는 포렌식 분야 기업의 분식 회계, 횡령, 탈세 수사 시 필수

❶ 디지털 포렌식 이란?

✓ 디지털 포렌식 전문인력 부족

- 디지털 포렌식 인력을 채용하고 있으나, 대부분 정보보안 부서에서 채용

삼성서울병원



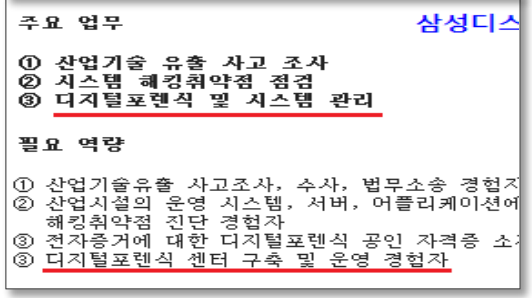
삼성서울병원의 채용에 관심을 가져주셔서 대
입사지원서를 작성하시기 전에 '지원서 작

제목	IT보안 실무자 채용
지원서 접수기간	2013년 06월 11일 13시 00분
직종명	의공학기사
담당자	이재훈

□ 모집부문
IT보안 실무자(정규직) 0명 채용

□ 담당업무
1. 디지털 포렌직
2. IT 보안 감사

삼성디스플레이



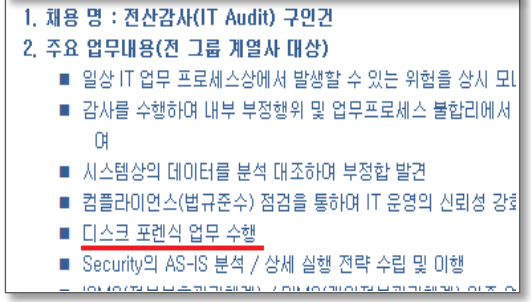
주요 업무 삼성디스

① 산업기술 유출 사고 조사
② 시스템 해킹취약점 점검
③ 디지털포렌식 및 시스템 관리

필요 역량

① 산업기술유출 사고조사, 수사, 법무소송 경험자
② 산업시설의 운영 시스템, 서버, 어플리케이션에
해킹취약점 진단 경험자
③ 전자증거에 대한 디지털포렌식 공인 자격증 소
③ 디지털포렌식 센터 구축 및 운영 경험자

코오롱베니트



1. 채용 명 : 전산감사(IT Audit) 구인건
2. 주요 업무내용(전 그룹 계열사 대상)
   - 일상 IT 업무 프로세스상에서 발생할 수 있는 위험을 상시 모니
   - 감사를 수행하여 내부 부정행위 및 업무프로세스 불합리에서
     여
   - 시스템상의 데이터를 분석 대조하여 부정합 발견
   - 컴플라이언스(법규준수) 점검을 통하여 IT 운영의 신뢰성 강화
   - 디스크 포렌식 업무 수행
   - Security의 AS-IS 분석 / 상세 실행 전략 수립 및 이행

삼성중공업

2. 모집분야: 조선해양/IT보안

3. 근무지: 거제

4. 세부 모집분야
1) 시스템,네트워크,웹 서비스 等의 보안진단
2) 모의해킹 및 침해사고 대응 업무
3) 디지털 포렌식 업무 (실무 경험자 우대)

현대카드/캐피탈

1) 정보보안감사팀
(1) 담당 업무_사원_사원~과장급
-디지털 포렌식
-IT감사
(2) 자격요건
-정보보안 관련 경력 3년 이상
-금융권 시스템 개발 및 설계 경험자 우대
-CISA, CISSP, CISM, CIA, CCFP 자격증 소지자 우대

삼정 KPMG

Job Description

1. 업무 내용
1) 디지털포렌식 업무 수행
-증거 수집, 증거 분석
-Disk Imaging, E-Discovery, Forensic Data Analysis
2) 부정 감사 업무 지원
3) 디지털포렌식 컨설팅
4) 디지털포렌식 비즈니스 발굴 (마케팅)

❶ 디지털 포렌식 이란?

✓ 디지털 포렌식 전문인력 채용(기업)

객관적 고려사항

- 디지털 포렌식 전문가 1급/2급 – 국가공인
- CCFP(Certified Cyber Forensic Professional) [국제공인]
- EnCE(Encase Certified Examiner)
  - Guidance
- ACE(Accessdata Certified Examiner)
  - Accessdata
- CHFI(Computer Hacking Forensic Investigator)
  - EC-Council
- CISA, CISSP 등 정보보안 자격증 + CIA

주관적 고려사항

- 검찰/경찰 등 수사기관에서 디지털포렌식 업무경험자
- 정보보안 또는 IT 부서에 근무한 경험이 있고 디지털 포렌식에 대한 이해가 있는 자
- 대학교, 대학원에서 디지털 포렌식 관련 전공을 한 후 실무 경력이 있는 자
- 디지털 포렌식 기술과 디지털 증거와 관련된 법률에 대한 이해가 있는 자

❶ 디지털 포렌식 이란?

✓ 디지털 포렌식 전용 도구 도입

증거수집(이미징)	쓰기방지	증거분석
디지털 증거(HDD, USB 등) 복제를 위한 장비	디지털 증거의 손상방지를 위해 물리적 장비를 이용하여 쓰기 차단	국내/외 수사기관 및 기업에서 사용하고 있는 증거분석 도구
• 로드마스터(RoadMaster) • 도시어(Dossier) • 솔로4(Solo4) • 팔콘(Falcon) • TD3 등 • 슈퍼이미저(SuperImager)	• Tableau • FastBlock • UltraDock 등	• Encase • FTK • Xray(모바일) • Finaldata Forensic 등

❶ 디지털 포렌식 전용 도구

✓ 증거수집 - 팔콘

- Falcon은 미국 Logicube사에서 새롭게 출시한 제품으로써 고속으로 데이터의 수집 및 삭제가 가능하도록 제작 되었으며, 이미지 작업 시 복제와 사본 해시 계산을 동시에 작업하는 것이 가능, 사본 하드디스크의 성능에 따라 속도가 향상

주요 기능

- 최대 11GB의 전송속도로 복제, 이미징, 삭제작업 가능(SATA기준)
- 원본 포트에 총 4개의 장치 연결이 가능하며, 각기 다른 작업 동시 가능
- 하나의 원본 저장 매체를 사용하여 복제 및 이미지 작업 동시가능
- 이미지 작업시 복제와 사본 Hash 계산을 동시에 하는것이 가능하며 사본 하드디스크의 속도에 비례하여 Hash 계산 속도 향상도 가능
- EnCase 전용 포멧인 E01과 Ex01 이미지 파일 생성가능
- 컴퓨터 또는 아이폰/아이패드의 웹브라우저 (크롬,사파리,오페라)를 사용하여 Falcon에 원격 접속 가능
- 데이터를 복구할 수 없도록 삭제가 가능하며, DoD 방식 지원
- 모든 작업에 대한 로그 파일 저장 및 전용 프린터를 사용하여 출력 가능
- 7" 터치스크린에 직관적인 GUI를 제공하여 사용이 용이

❶ 디지털 포렌식 전용 도구

✓ 증거수집 - 도시어

- 사용하기 쉬운 인터페이스와 최첨단의 기술을 제공하며, **소형으로 가볍게 디자인되어 현장 적용이 가능한 필드 이미징 장비로** eDiscovery 데이터 수집, 디지털 포렌식 수사, 법 집행 기관과 기업의 포렌식 수사에 적합

주요 기능

- 최대 분당 7GB의 전송 속도로 복제 및 삭제 작업 가능
- 고성능 내장엔진으로 고속 이미지 복제(7GB/분)
- EnCase에서 바로 조사/분석 가능한 E01이미지 생성
- 터치스크린, 자체 키보드 내장으로 손쉬운 사용
- 전용 운영체제를 통한 빠른 부팅 및 안정적인 동작
- 이미지 복제 시 무결성 보장을 위한 MD5, SHA256 해쉬값 계산 지원
- 다양한 드라이브와 호환될 수 있는 다중 인터페이스 지원
- IDE, SATA, SAS, SCSI, eSATA, MicroSATA 지원
- 미디어 리더기 내장으로 플래쉬 메모리에 대한 이미지 복제 지원
- CF, SD, SM, MS, MMC 지원/RAID로 구성된 드라이브 캡처 지원
- 자체 원본 HDD 쓰기 방지/Audit Trail Log 로그 저장

❶ 디지털 포렌식 전용 도구

✓ 증거수집 - 솔로4

- Solo4 Forensic은 고속으로 데이터의 수집 및 삭제가 가능하도록 제작
- 휴대가 간편한 현장 증거 수집 장비

주요 기능

- 최대 분당 7GB의 전송 속도로 복제 및 삭제 작업 가능
- 1:2 또는 2:2의 방식으로 복제 작업이 가능하며, 복제 작업 시 해시값 생성이나 데이터 삭제 작업을 동시에 수행 가능
- FireWire 1394B 와 USB2.0 내장으로 노트북 및 일반 컴퓨터의 HDD분리 없이 capture가능
- IDE, SATA, SAS, USB, SCSI 지원
- 네트워크를 통한 증거 업로드
- 증거의 암호화(AES256) 저장

❶ 디지털 포렌식 전용 도구

✓ 증거수집 - 로드마스터

- RoadMASSter3는 고속으로 데이터의 수집 및 분석이 가능하도록 제작 되었으며, 외부에서도 사용이 가능한 종합 포렌식 장비

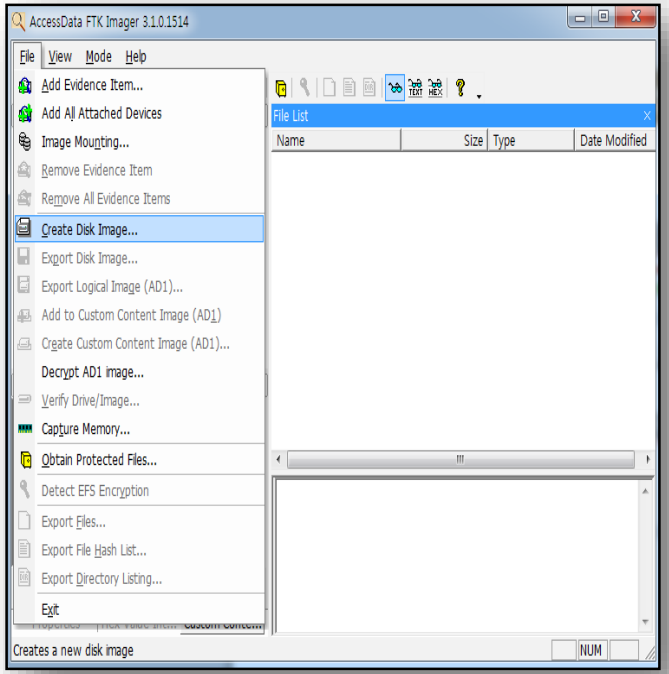
주요 기능

- 최대 분당 8GB의 전송 속도로 복제 및 삭제 작업 가능
- 현장 수사 시 증거자료 보존을 위한 원본 하드 디스크의 고속 복사 기능
- 1:2, 1:3 또는 2:2의 방식으로 복제 작업이 가능하며, 복제 작업 시 해시 값 생성이나 데이터 삭제 작업을 동시에 수행 가능
- 신속한 분석이 필요한 경우 현장에서 증거 수집과 동시에 분석 가능
- 하드웨어 및 소프트웨어 일체형
- USB Port를 통한 외장 드라이브 지원으로 대용량 백업 가능
- 현존하는 모든 OS 캡쳐

❶ 디지털 포렌식 전용 도구

✓ 증거수집 - FTK Imager

- 소프트웨어 기반으로 하드디스크 복제 수행



주요 기능

- E01, DD 등의 파일 형태로 하드디스크 이미징 가능
- 이미지 파일 생성시 압축률 조정 가능
- 해시값 생성
- 생성된 이미지 파일 읽기 가능
- 무료 SW

❶ 디지털 포렌식 전용 도구

✓ 쓰기방지 - 타블류

- Tableau Forensic Bridges는 하드 디스크, 외장형 스토리지, USB 메모리, FlashCard와 같은 디지털 저장 장치를 분석하고자 할 때 원본 데이터가 수정 및 삭제되지 않도록 해주는 **쓰기방지 기능을 지원하는 휴대장치**

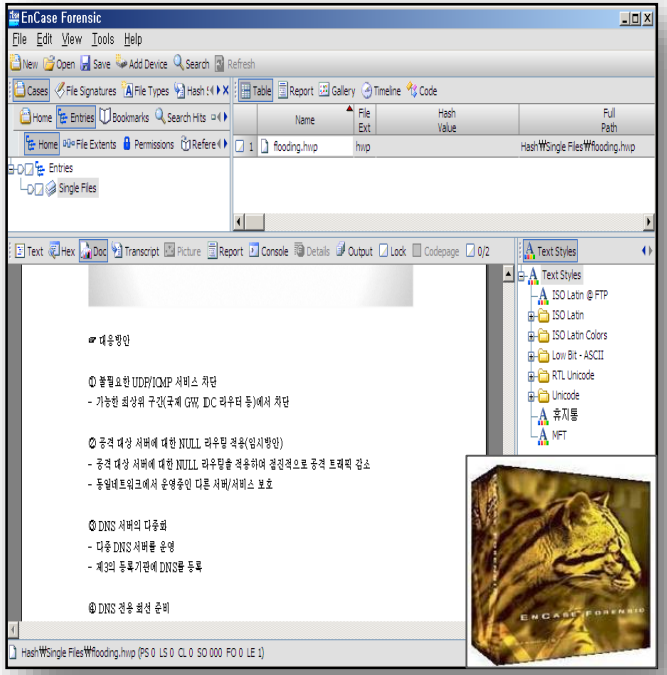
주요 기능

- P-ATA, S-ATA, SAS, USB, FireWire 장치 지원
- 모든 포트들이 **데이터 무결성을 위해 쓰기방지 기능 내장**
- 호스트 장비와 FireWire 및 eSATA 방식으로 연결 가능, 빠른 속도
- EnCase의 Write Blocked 표시
- T35u : USB3.0포트를 통해 IDE/SATA 방식의 하드디스크 지원 장치
- T4es : SCSI 방식의 하드 디스크 지원 장치
- T6es : SAS 방식의 하드 디스크 지원 장치
- T8-R2 : USB 방식의 저장 매체 지원 장치
- T9 : FireWire1394B 방식의 저장 매체 지원 장치

❶ 디지털 포렌식 전용 도구

✓ 증거분석 - EnCase

- 전세계적으로 가장 많이 사용되고 있는 업계 표준의 대표적인 컴퓨터 포렌식 조사 및 분석 소프트웨어
- 포렌식 전문가들을 위한 툴로 전 세계 법정에서 증거물로 인정 받고 있음



주요 기능

- 고속 Search Engine (검색시간 단축)
- Enhanced E-mail support
- Outlook PST 파일 빠른 분석, DBX 지원 (삭제 E-mail등)
- Base64 와 UUE encoded e-mail 의 자동 디코딩. Unicode 지원
- 가능 지원 File System : FAT,NTFS,HFS,HFS+,UFS,SUN,Solaris,EXT2,Palm,CDFS,UDF,ISO9660등
- 최적화 된 보고서 작성 (증거,작업자 설명,북마크,검색결과 등의 RTF와 HTML생성 가능)

❶ 디지털 포렌식 전용 도구

✓ 증거분석 - Forensic Toolkit

- 전세계적으로 가장 많이 사용되고 있는 디지털 포렌식 분석 소프트웨어 중 하나로 사용하기 편리한 인터페이스, 이메일 분석기능, 분산 프로세싱 능력 및 싱글 노드에 대한 원격 조사기능을 가진 엔터프라이즈급 제품

주요 기능

- 클라우드 컴퓨팅 시대에 최적화된 분산처리 지원
- 메모리 덤프 분석 (RAM Dump Analysis) 및 비교분석 기능
- 강력한 인덱스 검색(비할당영역지원), 정규 표현식(GREP) 검색 지원
- OCR분석을 통한 이미지 파일 내 문자열 분석
- Fuzzy Hash 분석기능을 통한 파일 유사도 검사 지원
- Data 카빙을 통한 다양한 파일복구 기능 지원
- 암호해독 솔루션 PRTK를 제공
- Tacc1441 H/W Accelerator와 결합하여 강력한 암호 해독 지원
- PORT의 Rainbow Table을 이용한 사전 계산된 전사적 공격 지원
- 네트워크를 통한 원격시스템의 메모리와 디스크에 대한 증거수집/분석

목차

❷ 디지털 증거

❷ 디지털 증거

✓ 로카르 법칙(Locard's Exchange Principle)

- 프랑스의 법의학자 로카르
- "접촉하는 두 개체는 서로의 흔적을 주고 받는다"
- 사용자 또는 조사자 그 누구든 간에 동작중인 시스템을 다루게 되면 해당 시스템은 변화가 발생한다
  - 프로세스 활동
  - 데이터 저장/삭제
  - 네트워크 상의 데이터 흐름
  - 웹 사이트 접속(캐시 데이터, 접속 목록, 방문 URL 등)

※ 충남 서산 경창서 증거분석실

❷ 디지털 증거

✓ 디지털 증거란, 저장 매체 또는 네트워크를 통해 전송 중인 자료 중 **법적 증거능력**을 가진 정보

디지털 증거의 종류

디지털 증거의 특징

비가시성	**눈에 보이지 않는 0과 1의 조합**인 디지털 형태로 저장되어 적발과 증명이 곤란
취약성 (변조가능성)	**변조나 손상이 쉽고 변조 사실을 찾아내기 어렵기** 때문에 사후에 법정에서 조작 여부, 증거 획득 절차의 적정성이 문제
매체독립성 (복제용이성)	0과 1의 디지털 신호로 되어 있어 **원본과 동일한 내용으로 쉽게 복제** 할 수 있으며 원본과 복제본의 구별이 쉽지 않음
대량성	기업의 전산 회계자료 등 **데이터 양이 수 백기가 바이트에 이를 만큼 방대**하여 특별한 도구나 전문인력이 없인 증거를 찾는데 어려움이 있음
초국경성	**인터넷을 통하여 전송**되거나 저장, 장소적 제한 없이 원거리 또는 타국의 서버나 컴퓨터에 존재
휘발성	**컴퓨터 메모리나 네트워크 상에서만 일시적으로 존재**하는 휘발성 데이터가 존재하며, 디지털 증거 압수과정에서 사라지지 않도록 각별히 주의해야 함
전문성	디지털 증거의 **수집과 분석은 전문적인 기술이 사용**되므로, 디지털 증거의 압수/분석 등에 있어 포렌식 전문가가 필수적임

❷ 디지털 증거

✓ 디지털 증거의 증거능력 요건

- **진정성 (Authenticity)**
  - 법정에 제출할 증거가 요증 사실을 설명하기 위한 바로 그 증거라는 사실을 증명
  - 특정인이 특정 시간에 생성한, 요증 사실의 증거가 맞는가?
- **무결성 (Integrity)**
  - 원본으로부터 수집되어 보관/분석 되는 과정에서 부당한 수정, 변경, 손상이 없어야 함.
- **원본성 (Originality)**
  - 디지털 증거는 자체로서 가독성이 없으므로 가시성이 있는 인쇄물로 출력하여 제출해야 함.
  - 증거원본이 제출되어야 하는 증거법상 사본증거, 가시성, 가독성있는 형태로 변환된 증거를 인정할 수 있는가?
- **신뢰성 (Reliability)**
  - 증거 데이터의 분석 등 처리과정에서 위/변조되거나 오류를 포함하지 않았다는 것을 의미
  - 증거 자체의 특성이 아닌 증거를 취급하는 정차, 도구, 인력 등과 같은 요소가 영향

※ 요증: 증명을 필요로 하는 일

❷ 디지털 증거

✓ 디지털 증거의 분류

생성증거(자동으로 생성되는 디지털 증거)

- 인터넷 사용기록
- 방화벽 로그
- 운영체제 이벤트 로그 등
- 각종 메타 데이터

보관증거(인위적으로 생성되는 디지털 증거)

- 문서파일
- 전자메일
- 동영상 및 사진
- 소프트웨어
- 암호 데이터

※ 일반적인 경우 보관증거는 법적 증거로 인정되지 않음.
단) 예외사항의 경우 증거로 인정됨

휘발성 증거

- 프로세스
- 예약작업
- 인터넷 연결 정보
- 네트워크 공유 정보
- 메모리 정보 등

비휘발성 증거

- 파일 및 파일 시스템
- 운영체제
- 로그 데이터
- 설치된 소프트웨어

목차

❸ 민간 영역에서의 디지털 포렌식 기술

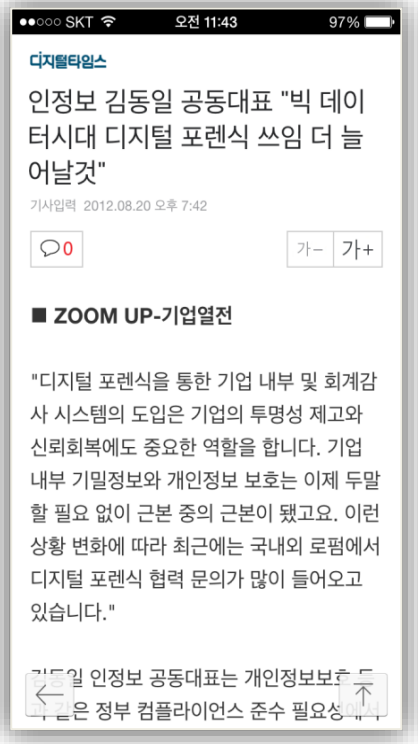
✓ 기업에서 디지털 포렌식 활용 분야

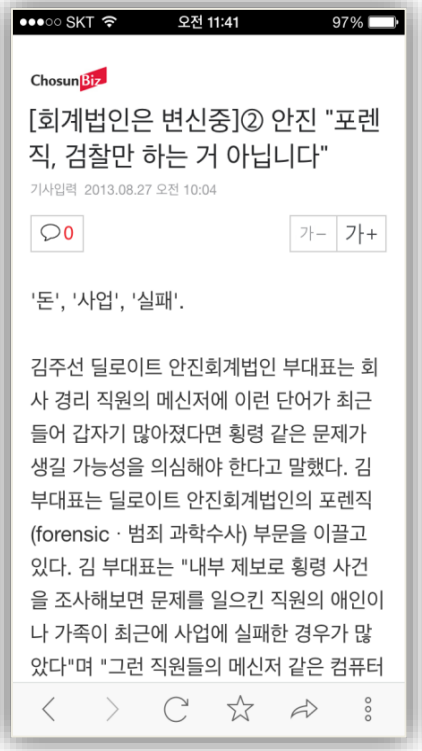
1	자금 횡령·배임 등 조사	▪ 지점, 대리점 근무자의 자금 횡령·배임 ▪ 불법적인 방법으로 영업활동 수행(차명계좌 사용 등)
2	협력업체 거래부정 조사	▪ 친인척 등 특수관계인 회사와 계약 체결 및 거래 발생 ▪ 과도한 선물 접대 등
3	경영실태 진단	▪ 기업 M&A로 인하여 DD 실사 참여 ▪ 점검대상자 PC 정밀 분석하여 기존 경영실태 파악
4	영업비밀 등 기업정보 유출 조사	▪ 경쟁사로 다수의 직원이 이직하여 설계도면 유출 ▪ 협력업체 직원 소스코드 유출
5	사내·협력업체 등 정보보안 감사	▪ 내부규정 우회하여 자료 보관(파일 암호화, 확장자 변경 등) ▪ 내부 사이트 취약점 점검
6	개인정보보호 관리실태 점검	▪ 협력업체에서 영업활동 목적으로 데이터 가공 ▪ 협력업체에서 보유기간 초과 개인정보 보관

❸ 민간 영역에서의 디지털 포렌식 기술

✓ 디지털 포렌식 서비스

- 디지털 포렌식 수요 증가로 인하여 **법무법인, 회계법인, 전문감사 기업** 등에서 디지털 포렌식 서비스 제공





❸ 민간 영역에서의 디지털 포렌식 기술

✓ 기업에서 수집 가능한 디지털 증거

물리적 증거	정보보안 시스템	업무용 시스템
• 사용자의 PC 및 노트북 • 법인 휴대폰 및 스마트패드 • 법인차 블랙박스 및 네비게이션 • CCTV 기록	• 매체제어 시스템 • 문서보안 시스템 • 방화벽 로그 • 출력물 관리 시스템 • 보안토큰 시스템 • 출입기록 시스템	• 전자결제 시스템 • ERP • 법인카드 사용 내역 • 이메일

❸ 민간 영역에서의 디지털 포렌식 기술

✓ 기업의 디지털 포렌식 절차

- 수사기관에서 사용하는 절차와 기업에서 사용하는 절차 비교

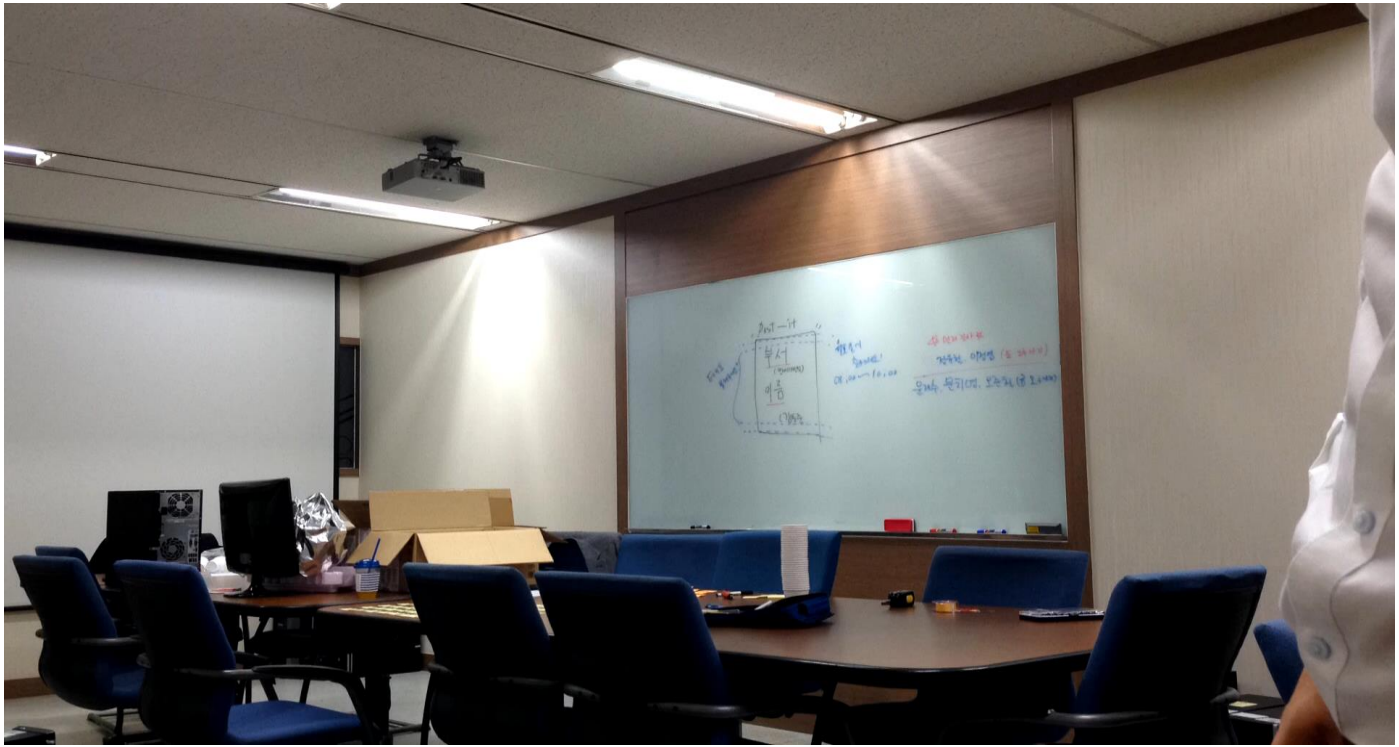
사전 준비 [Preparation]	증거물 수집 [Acquisition]	이송 및 보관 [Preservation]	증거 분석 [Examination]	보고서 작성 [Reporting]
▪ 사건파악 ▪ 포렌식 도구 검증 ▪ 장비 확보 ▪ 이미징 대상 선정 ▪ 동의서 준비(법률적 검토 필수) ▪ 특별감사 통보	~~(영장제시)~~ • 현장분석 • 동의서 징구 • 디스크 이미징 • 해시값 확인서 서명 (사안의 중요성에 따라서 결정)	• 증거물 포장 및 운반 • 이미지 복사 • 사본 생성	• 타임라인 분석 • 시그니처 분석 • 레지스트리 분석 • 웹히스토리 분석 • 데이터복구 • 키워드 검색 • 패스워드 및 암호 복구	• 증거 분석 결과 • 전문가 소견

❸ 민간 영역에서의 디지털 포렌식 기술

1)사전 준비 단계

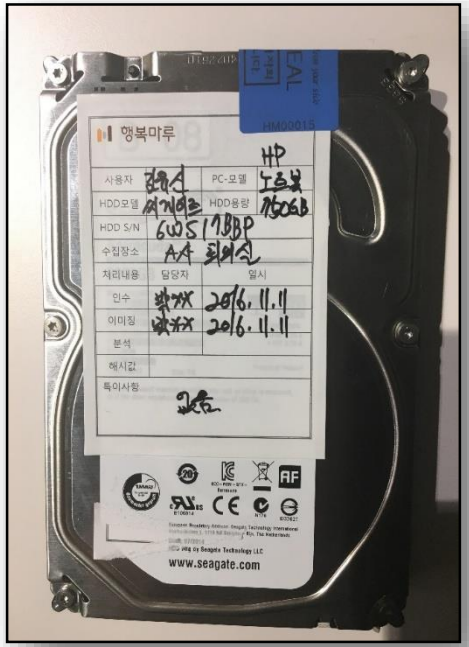
- 증거 수집 시 필요한 장비 점검(카메라, 캠코더, 멀티탭, 드라이버 등)
- 포렌식 H/W 점검(Dossier 등 이미징 장비, Tableau 등 쓰기방지 장치)
- **포렌식 대상자 PC 정보 확인**(IP, 하드디스크 용량, 자산관리 번호 등)
- 필요 시, 포렌식 대상자 업무현황 파악 및 기타 인적 정보 확인
- 임직원 하드디스크 이미징(복제) **동의서 및 확인서** 준비
- 포렌식 S/W 점검(Encase, FTK, FTK Imager 등)
- 보안씰(Security Seal) 준비
- 안전봉투, 정전기 방지 봉투

3 민간 영역에서의 디지털 포렌식 기술



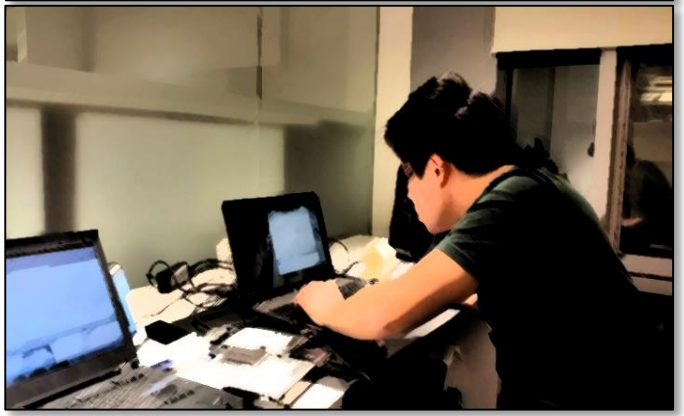
3)디지털 증거 이송 단계

- 수집된 디지털 증거물(보안씰 부착)
- 증거 분석실 이송을 위해 정전기 봉투에 넣고, 최종 안전봉투에 넣어 이송



4)디지털 증거 분석 단계

- 타임라인 분석을 통한 사용자의 PC 사용 패턴 분석
- 인터넷 히스토리 분석을 통해 최근 인터넷 검색 내용 및 접근한 사이트 분석
- 레지스트리 분석을 통하여 최근 열람 문서 및 이동식 저장장치 등 사용 흔적 분석
- 시그니처 분석을 통하여 사용자가 은닉을 목적으로 파일 확장자를 변경한 흔적 분석
- 회사 내부 메신저 대화 내역 분석 - 부정행위 입증에 결정적 증거 제공
- 문서 파일 키워드 분석을 통하여 결정적 입증자료 증명
- 삭제파일 복원하여 최근에 삭제한 내역 중심으로 분석 실시
- 이메일 분석 등 실시

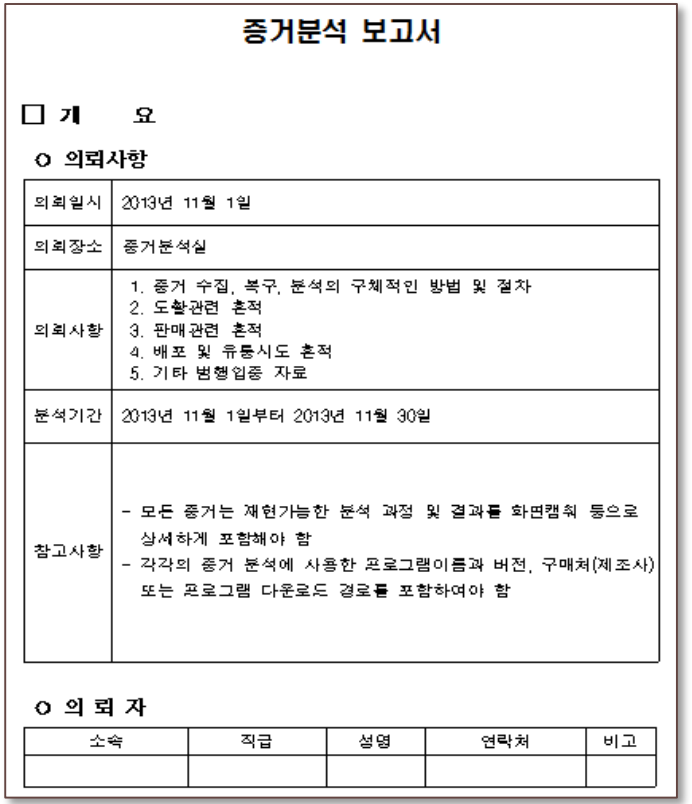


4)디지털 증거 분석 단계

1. 환경구축	✓ 증거물 이상유무 확인 및 사본 생성 ✓ 삭제파일 복구(할당 영역, 비할당 영역) ✓ 각종 문서파일 추출(doc, hwp, ppt, pdf 등) ✓ 레지스트리 정보 추출 ✓ 웹 접속 정보 추출 ✓ 시스템 로그 추출 ✓ 문서, 메일 등 키워드 분석을 위한 Indexing
2. 증거분석	✓ 레지스트리 분석 ✓ 웹 접속 분석 ✓ 키워드 분석 ✓ 메신져 분석 ✓ 시그니처 분석 ✓ 타임라인 분석

5)보고서 작성 단계

- 보고서에 기술되는 **모든 내용은 사실(Fact) 기반으로 작성**되어야 함
- 보고서를 받아보는 사람이 **쉽게 이해할 수 있는 용어**들을 사용해야 하며, 이해하기 어려운 용어에 대해서는 각주로 표기해야 함
- **추정 또는 가능성 등 개인적인 소견을** 나타내는 용어들은 **가급적 사용 금지**
- **어떤 방법과 절차**로 증거분석 결과가 도출되었는지 상세히 기술
- 법적인 이슈와 관련이 있을 경우 **사내 변호사의 보고서 검토 작업 필요**



증거분석 보고서

□ 개 요

○ 의뢰사항

의뢰일시	2013년 11월 1일
의뢰장소	증거분석실
의뢰사항	1. 증거 수집, 복구, 분석의 구체적인 방법 및 절차 2. 도촬관련 흔적 3. 판매관련 흔적 4. 배포 및 유통시도 흔적 5. 기타 범행입증 자료
분석기간	2013년 11월 1일부터 2013년 11월 30일
참고사항	- 모든 증거는 재현가능한 분석 과정 및 결과를 화면캡쳐 등으로 상세하게 포함해야 함 - 각각의 증거 분석에 사용한 프로그램이름과 버전, 구매처(제조사) 또는 프로그램 다운로드 경로를 포함하여야 함

○ 의 뢰 자

소속	직급	성명	연락처	비고

목차

✓ 디지털 포렌식 적용 사례

활용 사례	세부내용
반도체 개발 업체 기술유출 사건	▪ 최근 1년간 10여명의 개발자가 외국계 기업으로 이직이 빈번하여 기술유출 여부 디지털 포렌식 조사
개발회사 소스코드 유출 사건	▪ 외주업체 직원이 이미지파일에 소스코드 숨겨서 외부 유출한 사건
대리점 자금 횡령 사건	▪ 대리점에서 판촉비 명목으로 내린 현금을 지점장이 자금을 유용·횡령하였는지 디지털 포렌식 조사
협력업체 거래부정 사건	▪ 내부직원이 친구이름으로 차명회사를 설립한 후 다수의 프로젝트를 아웃소싱한 협력업체 거래부정 사건
개인정보 유출 사건	▪ 디지털 포렌식 방법론을 적용하여 내부통제를 우회하여 회사 기밀 정보, 개인정보 등 보유 실태 점검

✓ 반도체 개발 업체 기술유출 조사

① 개요

- 최근 1년간 반도체 설계부서 직원 10여명이 경쟁사로 이직
- 회사 매출이 감소하기 시작하고 기술유출이 되었다는 소문이 들리기 시작
- 경쟁사로 이직을 결정한 A대리에 대한 조사 요청

② 점검방법

- 대상 PC에 대해 디지털 포렌식 정밀 진단 수행

③ 발견사항

- 파일 접근권한이 없는 K과장에게 반도체 관련 파일 전송 정황 확인(메신저)
- 개인 USB에 회사 업무관련 파일 복사된 흔적 확인
- 한달 후 K과장 경쟁사로 이직

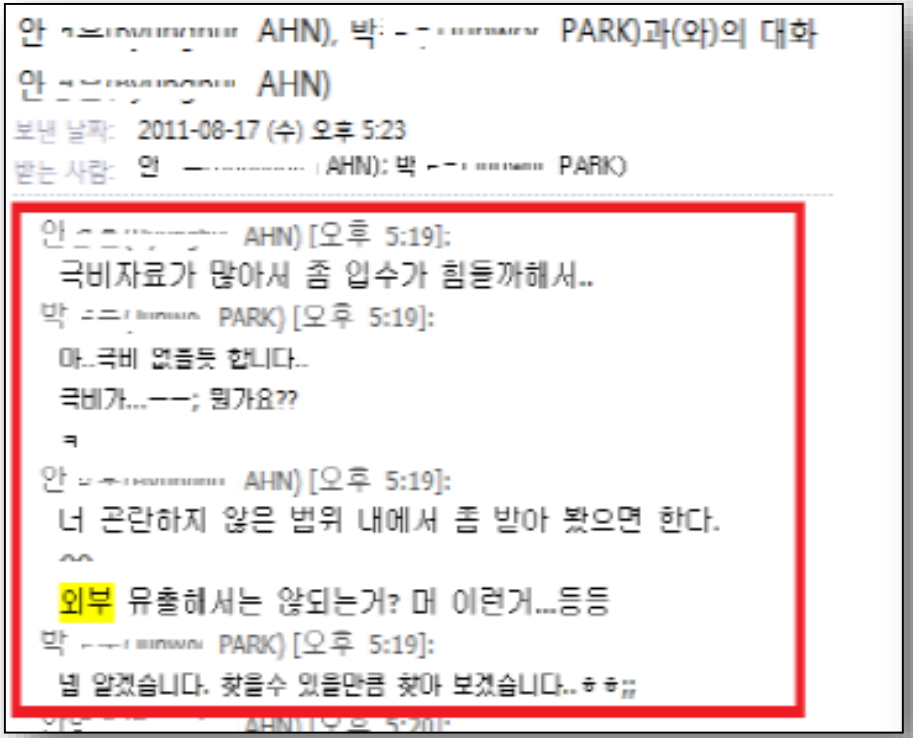
④ 결과

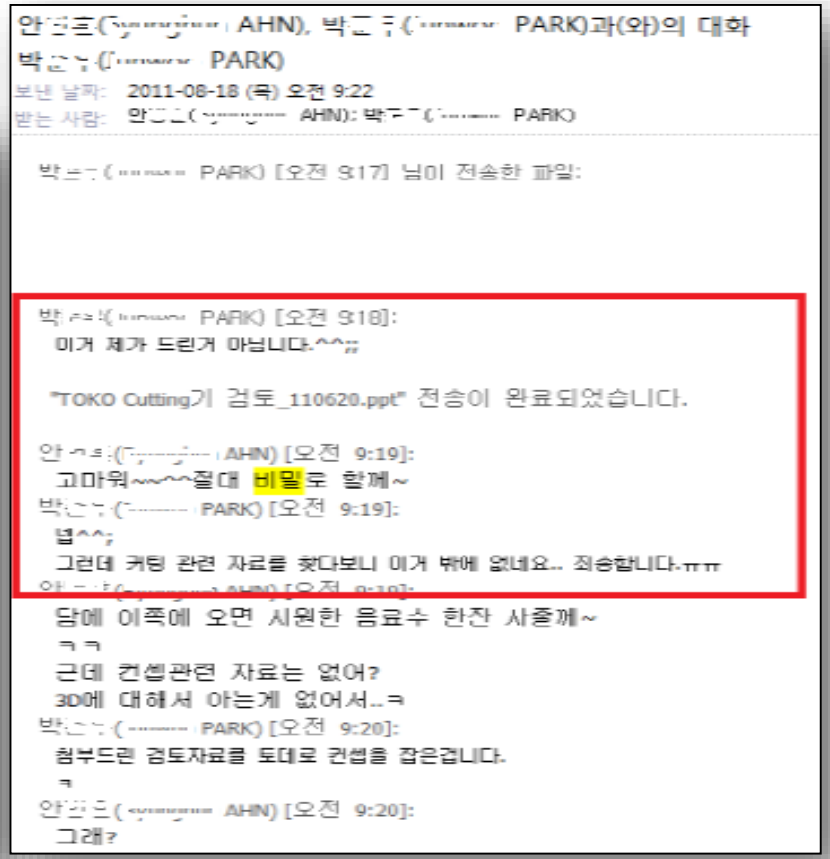
- K과장이 경쟁사 이직을 위해 A대리로 부터 기업비밀 자료 확보 후 이직

4 적용사례

✓ 반도체 개발 업체 기술유출 조사

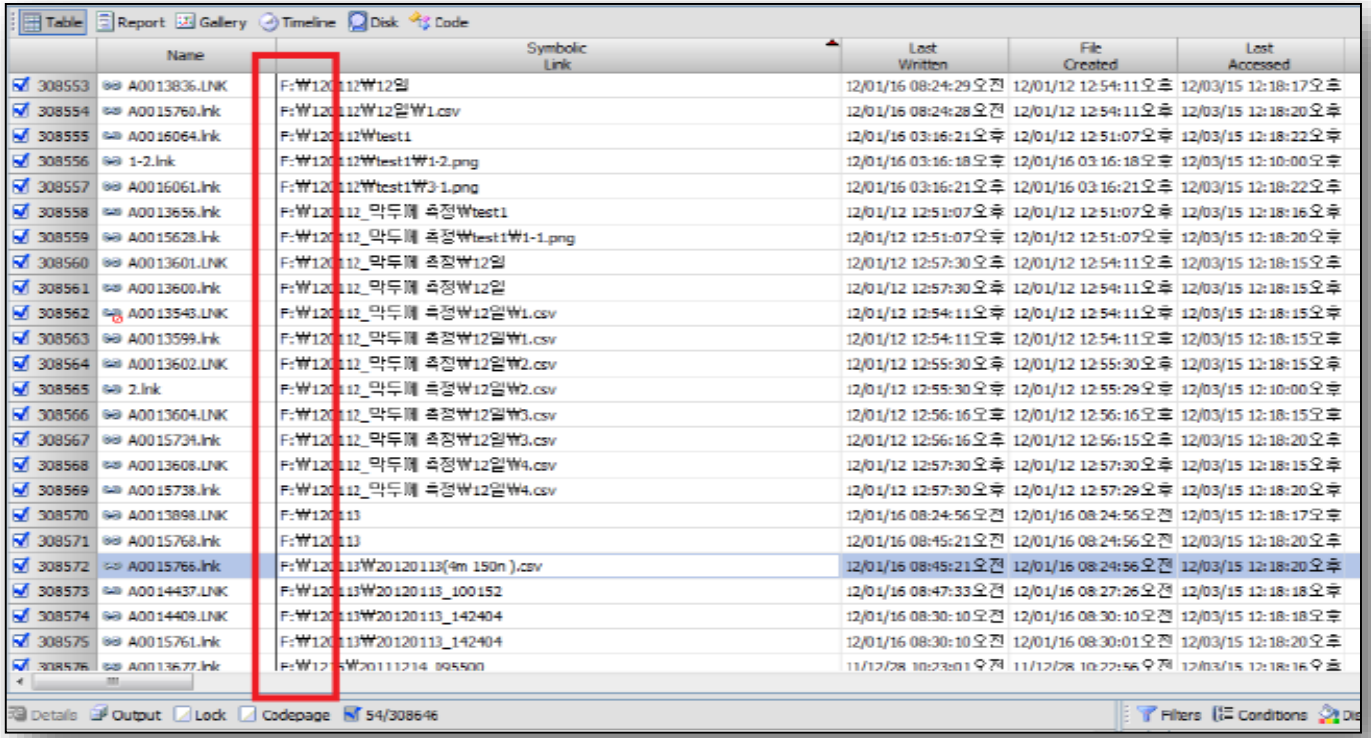
- 메신저 대화에서 이상징후 확인





✓ 반도체 개발 업체 기술유출 조사

- USB를 통해 회사 기밀자료 전송 정황 확인(링크파일 분석)



✓ 개인정보 유출 조사

① 개요

- A기업 인수합병과정 실사 중 정보유출 관련 내부 문서 발견 후 조사 요청

② 점검방법

- 대상 PC에 대해 디지털 포렌식 정밀 진단 수행

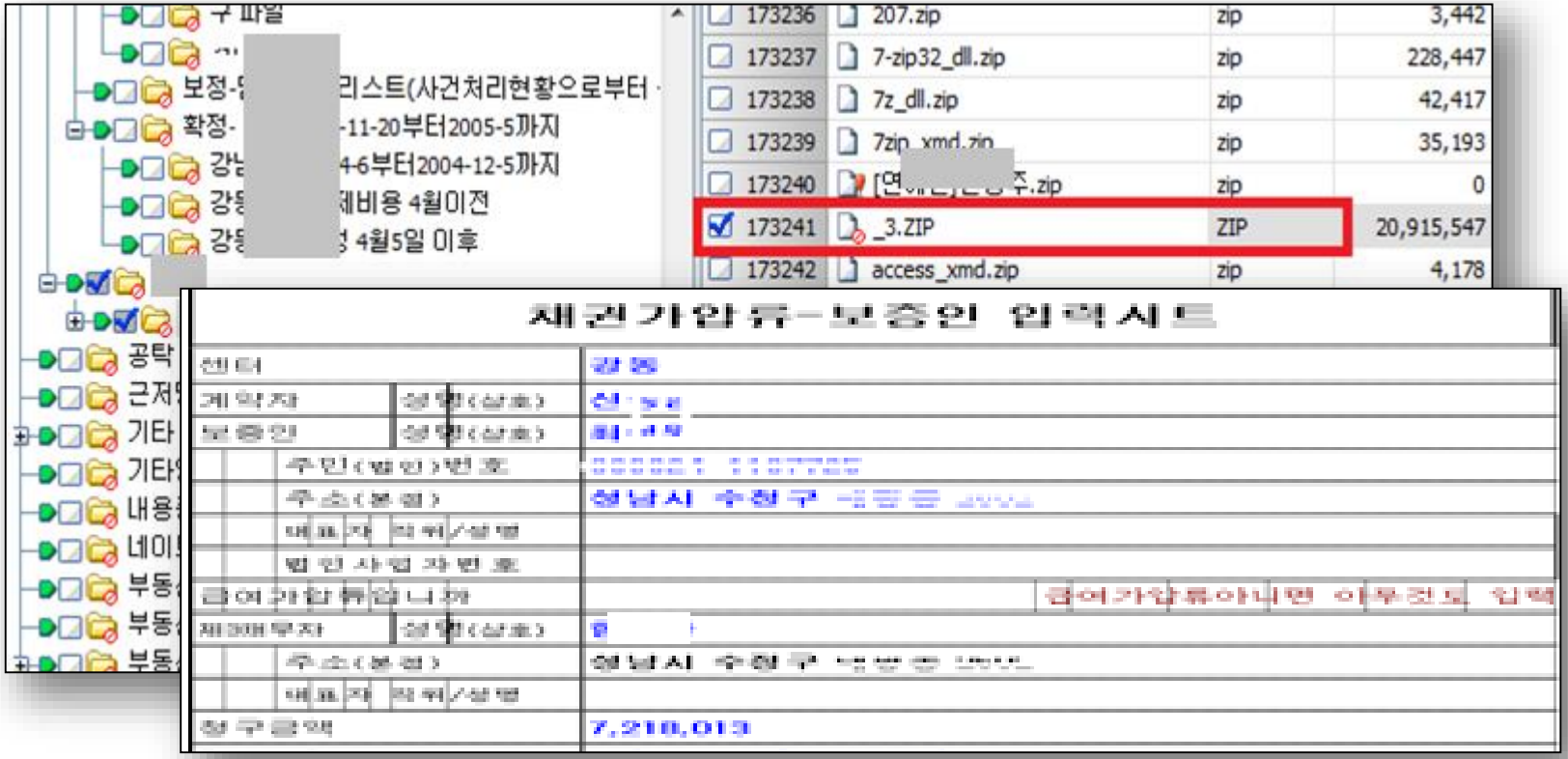
③ 발견사항

- 삭제파일 복구 과정에서 시그니처가 다른 이상 파일 확인
- 복구 확인결과 엑셀파일로 확인

④ 결과

- 압축파일 해제 결과 다량의 개인정보 자료 확인
- 고객정보 보관을 위해 저장(개인정보 관리 위반)

✓ 개인정보 유출 조사


173236 207.zip zip 3,442
173237 7-zip32_dll.zip zip 228,447
173238 7z_dll.zip zip 42,417
173239 7zip_xmd.zip zip 35,193
173240 [연[redacted]주.zip zip 0
173241 _3.ZIP ZIP 20,915,547
173242 access_xmd.zip zip 4,178
보정-[redacted]리스트(사건처리현황으로부터
확정-[redacted]-11-20부터2005-5까지
[redacted]4-6부터2004-12-5까지
[redacted]제비용 4월이전
[redacted]4월5일 이후
공탁
근저
기타
기타
내용
네이
부동
부동
부동
7,218,013

Thank You

Thinking from your side
행복마루

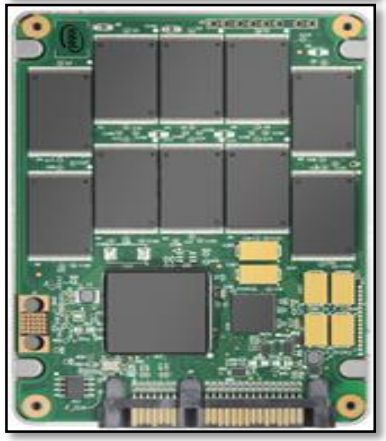
목차

5 모바일 포렌식

✓ HDD vs SSD

- HDD: 자기 디스크 방식으로 충격에 약하고, 발열량이 많음
- SSD(Solid Stata Drive): 반도체 방식으로 비활성 플래시 메모리 사용

	HDD	SSD
구동방식	자기디스크	반도체
반응/응답	낮음	높음
전송속도	낮음	높음
동작소음	있음	없음
소비전력	높음	낮음
물리적 내구성	약함	강함
대용량 접근성	높음	낮음
용량대비 가격	낮음	높음
손실 데이터 복구율	높음	낮음



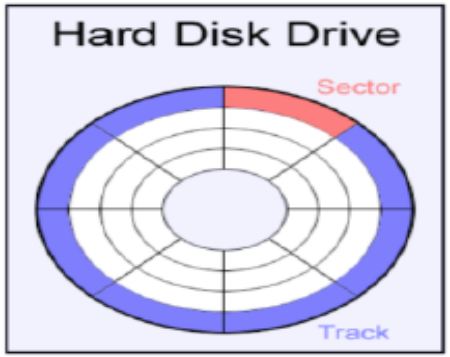
✓ SSD 종류

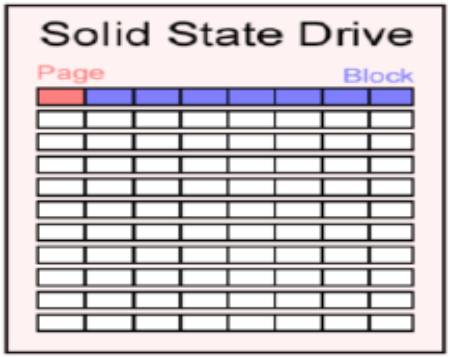
- 데이터 저장 방식에 따라 SLC, MLC, TLC로 구분
- SLC(Single Level Cell) - 하나의 셀이 1bit의 정보를 저장 {0,1}
- MLC(Multi Level Cell) - 하나의 셀에 2bit의 정보를 저장 {00,01,10,11}
- TLC(Triple Level Cell) - 하나의 셀에 3bit의 정보를 저장 {000,001, ... 110,111}

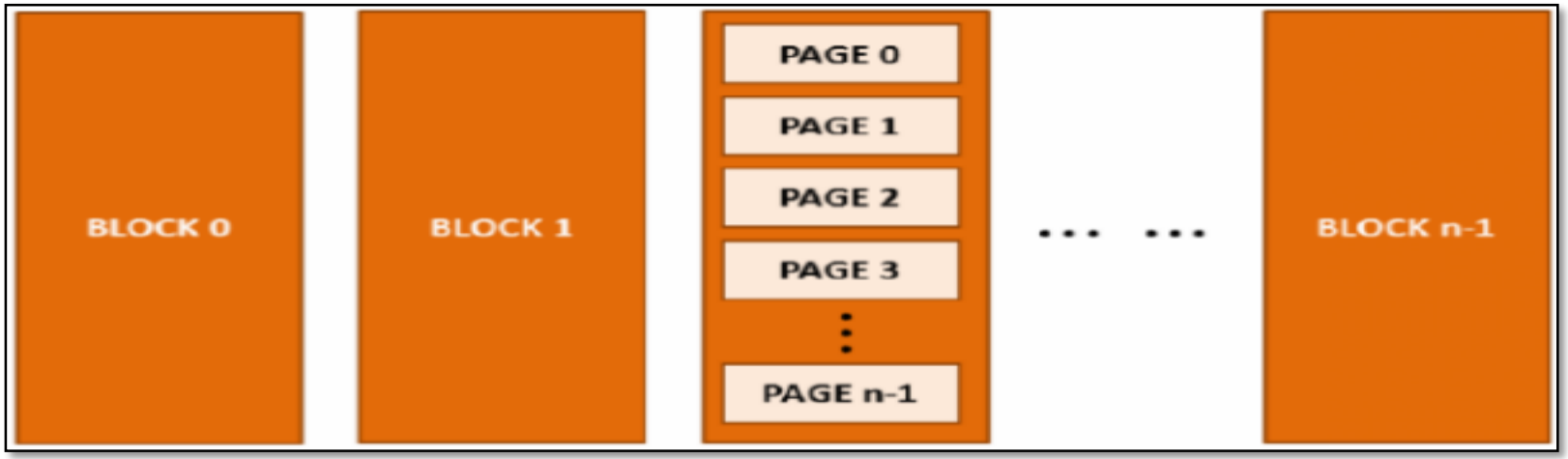
	SLC	MLC	TLC
BPC (bit/cell)	1	2	3
재기록 가능횟수(P/E Cycles)	100,000	10,000 ~ 3,000	1,000
읽기 성능(Read Time)	25㎲	50㎲	~75㎲
쓰기 성능(Write Time)	200㎲~300㎲	600㎲~900㎲	~900㎲~1350㎲
지우기 성능(Erase Time)	1.5ms~2ms	3ms	~4.5ms

✓ SSD 구조

- SSD 기본 단위 셀(Cell)
- 셀이 모여서 Page(4KB)
- Page가 모여서 Block(512KB)

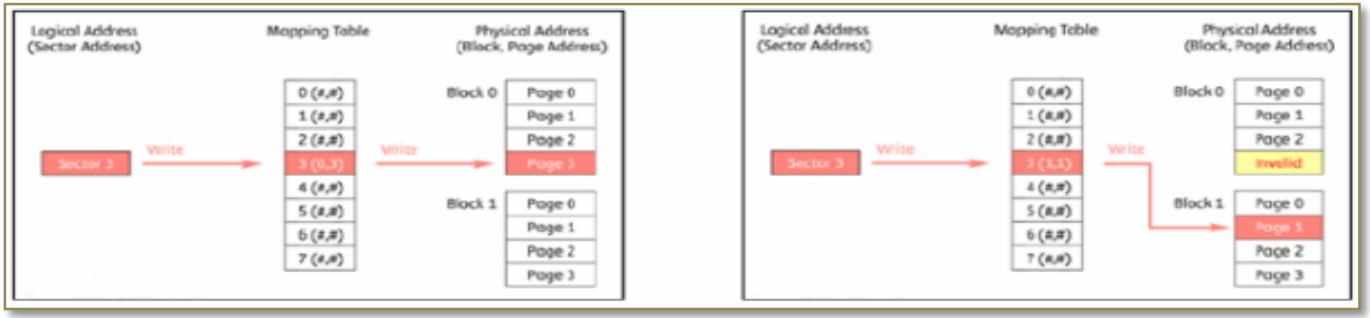




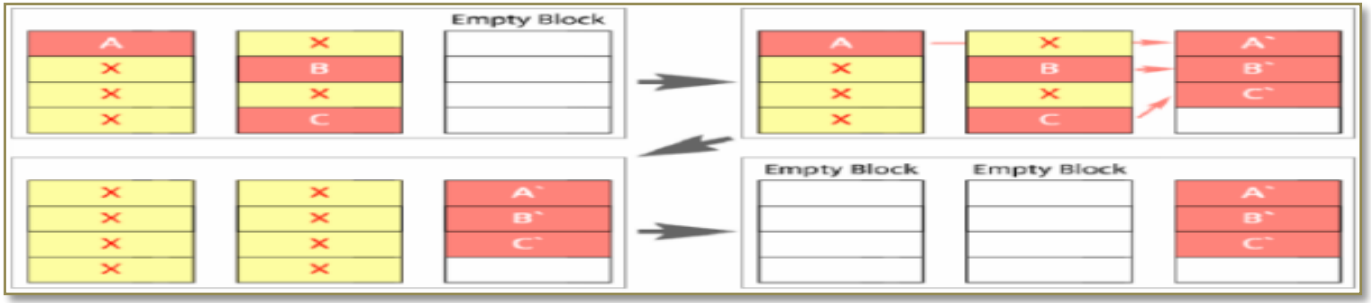


✓ SSD 구조

- **웨어 레벨링(Wear leveling)**: 셀마다 쓰기 횟수가 제한적. 모든 페이지에 골고루 쓰기가 가능하도록 관리(모든 페이지의 재기록 횟수 저장 관리)



- **가비지 콜렉션(Garbage Collection)**: 일정 수준의 Invalid가 모이면 한꺼번에 삭제 수행



END

Thinking from your side
행복마루