



Digital Forensics

Beyond Digital Forensics!

과학과 사실이 지배하는 세상을 향해

KDI

Korea Digital Intelligence



“과학과 사실이 지배하는 세상을 향해”

RULE OF FACT



What is Digital Forensics?

디지털 포렌식이란?

PC나 노트북, 휴대폰 등 각종 저장매체 또는 네트워크 상에 남아 있는 디지털 정보를 분석하여 범죄의 증거를 확보하는 과학수사기법을 말한다.

현재는 수사 뿐 아니라 기업의 감사 및 정보보안 등의 영역으로 확대되어 지적재산권 분야와 민사소송에서 역할 비중이 증가하고 있다.

LEVEL & PROCEDURE

KDI 디지털 포렌식은 단순 데이터 복구가 아닙니다!

실체적 진실 발견을 위해 법정이나 공공 기관에 제출하는 디지털 증거의 확보와 보고서 작성(Documentation & Reporting)은 수사기관 출신 포렌식 전문요원의 조사분석을 필요로 합니다.

KDI 디지털 포렌식은 검찰 출신 디지털 포렌식 전문 요원과 고문 변호사의 팀워크로 구성됩니다.

레벨 1 | 단순 데이터 복구

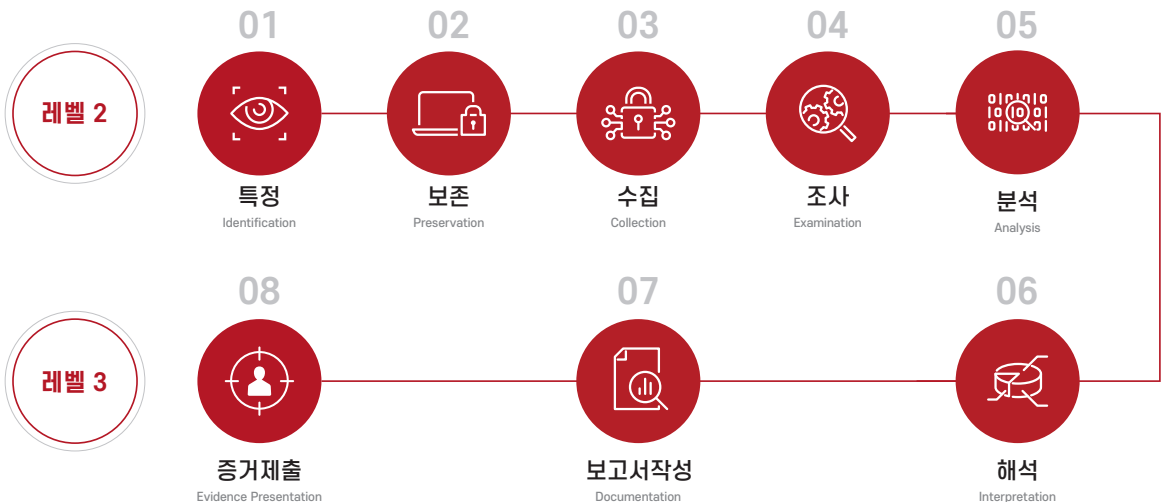
단순 데이터 복구는 포렌식 도구 운용 능력만으로 가능한 기본적 서비스임. 그러나 디지털 증거 확보를 위한 전문 디지털 포렌식의 데이터 복구는 단순 복구와 달리 증거의 무결성 (Digital Chain of Custody)을 위해 이미지를 통한 데이터의 보존 수집이 필요하므로 단순 복구와는 전혀 차원이 다른 과정임

레벨 2 | 전문기술 디지털 포렌식

고가의 최신 장비와 수사 경험 있는 전문 디지털 포렌식 요원 필요

레벨 3 | 증거 전문 디지털 포렌식

민/형사 사건 대응과 공공기관 감사 등 정식 증거제출을 위한 디지털 포렌식은 수사기관 출신의 전문 분석요원에 의해서 가능



KDI DIGITAL FORENSICS KDI 디지털 포렌식

대검찰청 과학수사부장 출신의 총괄 자문 하에 서울고검, 인천지검, 고위공직자범죄수사처(공수처)의 디지털 포렌식 팀장 출신 전문가의 조사분석 및 보고서 작성, 디지털 포렌식 전 과정의 적법한 진행을 관리할 법률고문 변호사들의 법률자문, 그리고 R&D 와 보안점검을 책임질 전문인력이 KDI 디지털 포렌식의 팀워크를 이룹니다.



개인정보 보안
디지털 포렌식



기술 및 기업정보
유출 대응



기업 내부감사
포렌식



회계감사 및
M&A 실사 포렌식



소송 대응
디지털 포렌식



e-DISCOVERY
디지털 포렌식

DIGITAL FORENSICS SCOPE 디지털 포렌식 범위

PC나 노트북, 휴대폰 등 각종 저장매체 또는 네트워크 상에 남아 있는 각종 디지털 정보를 분석해 범죄 증거를 확보하는 과학수사기법을 말한다. 현재는 수사 뿐 아니라 기업의 감사 및 정보보안 등의 영역으로 확대되어 지적재산권 분야와 민사소송에서의 역할 비중이 증가하고 있다.

대상

컴퓨터 / 노트북

모바일 / 태블릿

이메일 / SNS

블랙박스 / CCTV

드론 / 자동차

기타

주요 제공 서비스

디지털 포렌식 도구를 이용하여 데이터 사본 생성

수집된 이미지(사본)에서 삭제된 파일 복구

복구된 파일 (문서 / 이메일 등) 검토

외장하드/이메일/메신저 등 여러 경로를 통해 파일의 이동 기록을 탐색하는 등 컴퓨터를 사용하여 파일 등을 전달하거나 다운로드 받은 기록을 추적하고 분석

분석결과(엑셀파일)제공

위 과정을 통해 확보된 증거를 기초로 기업비밀이나 개인정보 등이 유출된 경로와 책임자 등을 특정하거나 추론

위 내용의 분석 보고서 작성 및 제공

휴대전화, 태블릿의 메시지(문자, 카카오톡 등) 통화내역, 이메일 등 분석 작업



소송 대응 디지털 포렌식

☞KDI 디지털 포렌식은 실제 조사분석 전 과정을 수행합니다.

검찰 디지털포렌식 센터와 동일한 수준의 장비를 갖추고, 검찰 디지털 포렌식팀장 경력의 분석 요원과 군 000에서 군사기밀 유출 수사를 담당한 전문 포렌식 요원이 팀을 이루어 실제 조사분석을 수행하는 디지털 포렌식 전문 기업입니다.



형사사건 대응

수사기관에 대응하여 피의자 측 자체 포렌식이 필요
수사 이후 손해배상 상속 보험 등의 민사 문제로 파생



민사 · 상사 분쟁 대응

당사자 일방의 증거에 대한 진실성을 다투기 위해 디지털 포렌식중요성 증가.
특히 법원의 개입을 제도화하는 e-Discovery도입은 민사에서 디지털 포렌식 비중이 증가함을 의미 - 현재 지적재산권 중심으로 e-Discovery 도입 논의 중



e-DISCOVERY 대응

법원의 증거 보존 및 개시 절차에 따른 증거조사 과정
한국기업이 미국이나 EU 지역에서 소송당사자가 될 경우
e-Discovery 절차에서 디지털 포렌식의 중요성 증가



e-Discovery 디지털 포렌식 절차





사전 예방 디지털 포렌식

PREVENTIVE DIGITAL FORENSICS

개인 정보보안 디지털 포렌식

기술 및 기업정보 유출 대응

기업 Compliance Risk 대응

기업 내부감사 디지털 포렌식 지원

기업 회계감사 디지털 포렌식 지원

M&A 실사 디지털 포렌식 지원

나도 모르는 내 정보!

나도 모르게 휘말릴 수 있는 법적 책임으로부터 스스로를 보호할 디지털 방패, KDI 디지털 포렌식

CEO도 모르는 회사 정보!

정보유출과 잠재된 사고, 언제 터질지 모르는 법적 책임에 대비한 디지털 방패, KDI 디지털 포렌식

기업 기밀 및 산업기술 유출 예방

2017년부터 5년간 국가핵심기술 35건을 포함해 총 101건의 산업기술 해외 유출 적발
지난 5년간 약22조원에 달하는 산업기술 해외 유출! 특히 중소기업이 산업기술 유출에 취약



기업감사 디지털 포렌식

CORPORATE INVESTIGATION DIGITAL FORENSICS

KDI의 기업 감사 지원

기업의 준법경영 (compliance) 리스크 대응

상시적 준법 감시와 사고 발생 후 법적 분쟁을 회피하기 위한
기업 내부감사의 디지털 포렌식은 법적 리스크를 항상 안고
있는 기업경영에서 필수적인 예방 절차이다.

M&A 실사 디지털 포렌식 지원

M&A에 필수적인 정확한 valuation과 숨겨진 정보로 인한
법적 리스크 회피를 위해 M&A 실사는 필수적인 절차이고,
기업의 거의 모든 정보가 ESI(전자저장정보)인 현실에서
디지털 포렌식의 중요성은 계속 증가할 수 밖에 없다.

회계법인의 회계감사 포렌식 지원

기업의 투명경영을 위해 갈수록 엄격함과 신뢰성이 요구되는 회계감사
회계감사의 법적 책임과 리스크가 증가하는 상황에서 기업의
회계감사에 최첨단의 디지털 포렌식은 필수적 절차이다.





DIGITAL CHAIN OF CUSTODY

KDI만의 데이터 금고 서비스

디지털 포렌식의 생명은 기술과 보안!
KDI만의 자체 서버로 의뢰인 데이터의 안전한 보관

Chain of Custody 데이터의 무결성 절차

디지털 증거의 무결성(Digital Chain of Custody)이란 디지털 증거의 상태 변경이나 오염을 방지하고 증거의 온전함(integrity)을 유지하기 위해 증거의 수집부터 법정제출까지 전 과정에 걸쳐 디지털 증거의 보존과 관리를 기록함을 의미한다.



PROTECTIONS FOR CHAIN OF CUSTODY



Video Surveillance

비디오 감시 보안시스템
데이터 접수 개봉부터 분석 과정과 보관
밀봉까지 비디오 녹화 감시



Secure Evidence Vault

KDI만의 블록체인 데이터 서버 보유
의뢰인의 안전한 디지털 금고



24/7 Security Guard

포렌식 분석실 24시간 보안 시스템 작동



Tamper Evidence Casing

접촉한 데이터의 밀봉 보관 표시
무단 접촉 시 표시변경되는 특수 밀봉





주식회사 코리아디지털인텔리전스

서울 강남구 테헤란로 322 한신인터밸리 24빌딩 서관 1516호 / 분석실 : 서관 1115호

Tel. 대표 - 02. 556. 6968 / 분석실 - 02. 553. 4572

Fax. 02. 552. 4502

www.kdi.or.kr