PC 카카오톡 데이터 복호화 및 포렌식 분석

KakaoTalk for PC Data Decryption and Forensic Analysis

디지털포렌식 기술을 기반으로 PC 카카오톡 대화 데이터를
복호화하고 분석하는 전문 프로그램 **Walnut**

HM COMPANY™

1. 카카오톡 대화, 왜 별도의 복호화·분석이 필요한가

업무와 일상에서 오간 카카오톡 대화는 사실관계 확인, 내부조사, 분쟁 대응 과정에서 **핵심 자료로 활용**되는 경우가 많습니다.
그러나 PC에 저장된 카카오톡 대화 데이터는 암호화된 형태로 보관되어 일반적인 방법으로는 내용을 확인하기 어렵습니다.

4,900만
국내 카카오톡
월간 활성 이용자 수
카카오 2025년 3분기

94%
국내 모바일
메신저 이용률 1위
와이즈앱·리테일(2025)

8.3만 건
연간 디지털 증거분석 건수
(최근 5년 30%↑)
경찰청(2025)

카카오톡 PC 대화 분석 시 주요 이슈

암호화된 저장 구조
대화 데이터가 암호화된 상태로 저장되어
일반적인 방식으로는 내용 확인이 어렵습니다

시간이 지날수록 감소하는 대화 흔적
PC 사용이 계속되면 일부 흔적이 덮어써질 수 있어
확보 가능한 데이터가 줄어들 수 있습니다

삭제·은폐된 대화 정황
삭제되거나 사라진 대화방은
일반적인 방식으로는 분석이 제한될 수 있습니다

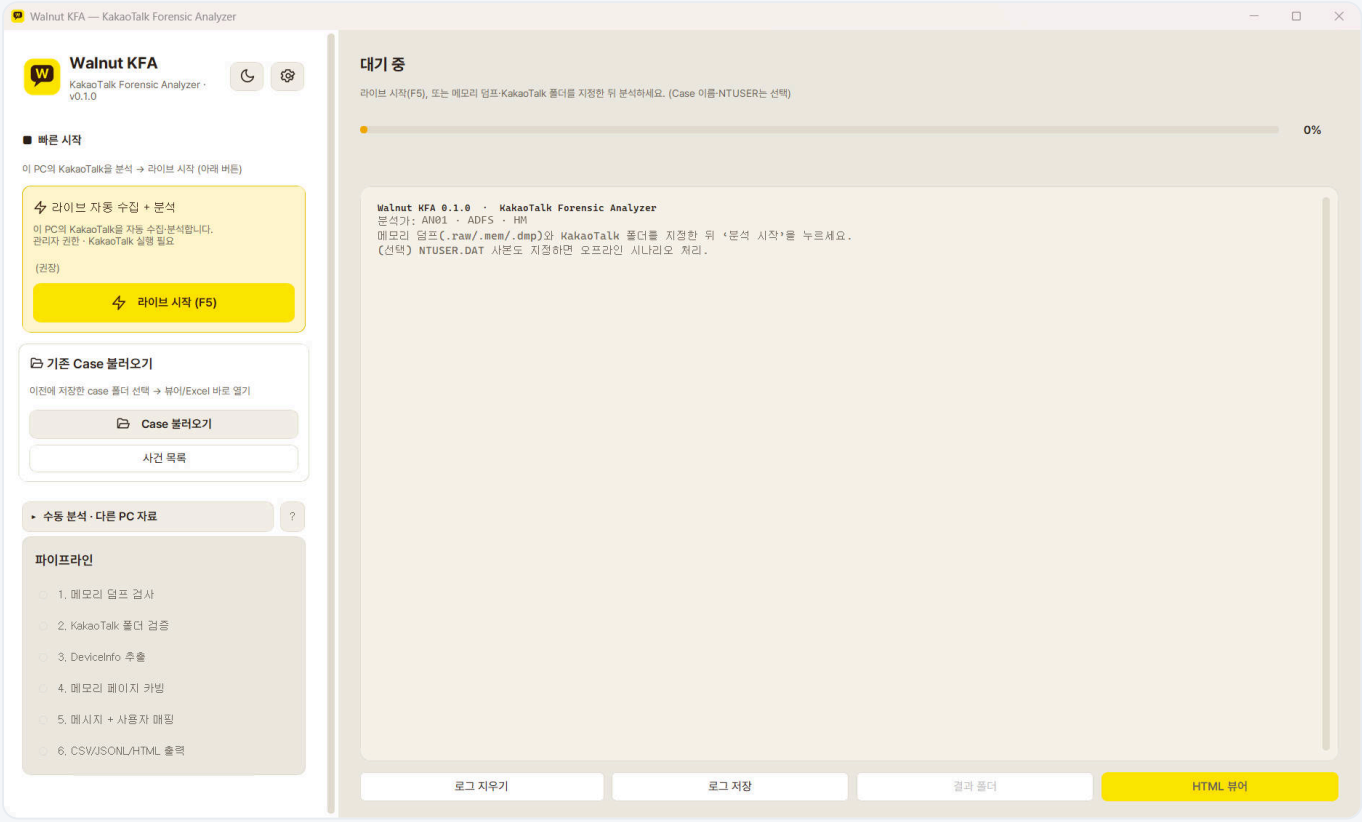
증거 자료로서의 신뢰성 확보
수집·복호화·분석 과정이 기록되지 않으면
분석 결과의 산출 근거를 설명하기 어렵습니다

PC 카카오톡 저장·보호 방식의 변화

PC 카카오톡의 저장·보호 방식은 지속적으로 변경되고 있습니다. 과거 버전 기준의 복호화 방식만으로는 최신 데이터 분석이 제한될 수 있으므로, 현행 버전까지 대응 가능한 복호화·분석 역량이 중요합니다.

2. 수집 화면 — 분석 시작 조건과 입력 자료

분석에 앞서 대상 PC에서 카카오톡 관련 데이터를 수집하고, 암호화된 대화 DB를 복호화합니다.
확보한 자료 유형에 따라 적합한 시작 방식을 선택합니다.



분석 시작 방식

실행 중인 PC에서 직접 수집
메모리와 카카오톡 폴더를
직접 확보

카카오톡 데이터 폴더
전달받은 폴더와
메모리 사본을 입력

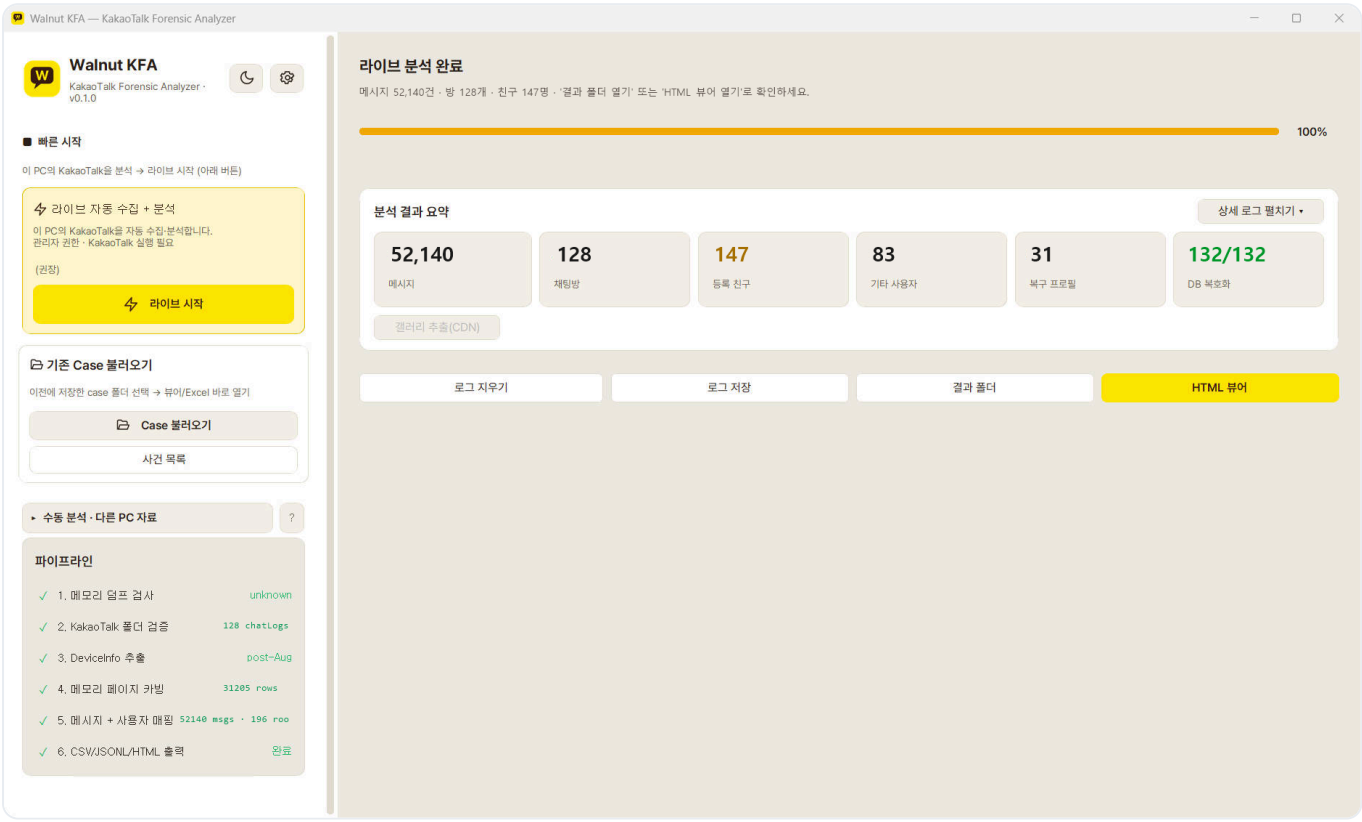
디스크 이미지
디스크 이미지에서 자료를 추출
메모리 사본 필요

분석 시작 전 준비사항

대상 PC	수집 시점에 카카오톡이 실행 중이어야 복호화 키 확보가 가능합니다.
메모리 사본	복호화 키는 메모리에서 확보되므로, 전달받은 카카오톡 폴더나 디스크 이미지를 분석하는 경우에도 메모리 사본이 함께 있어야 합니다.
권한	실행 중인 PC에서 직접 수집하는 경우 관리자 권한이 필요합니다.

3. 수집 화면 — 복호화 처리 단계와 결과

분석을 시작하면 6단계 절차가 순차적으로 진행되며, 진행률과 단계별 처리 결과가 화면에 표시됩니다.
분석이 완료되면 메시지 수, 채팅방 수, 친구 수, 복호화 범위가 요약되어 표시됩니다.



복호화·분석 6단계

1 메모리 덤프 검증
수집한 메모리 덤프의 유효성을 확인합니다

2 카카오톡 데이터 폴더 검증
카카오톡 데이터 폴더의 구조와 필수 파일을 확인합니다

3 복호화 기기 정보 추출
복호화에 필요한 기기 식별 정보를 추출합니다

4 대화 기록 복호화 및 복원
복호화된 대화 데이터와 메모리에 남은 기록을 함께 반영합니다

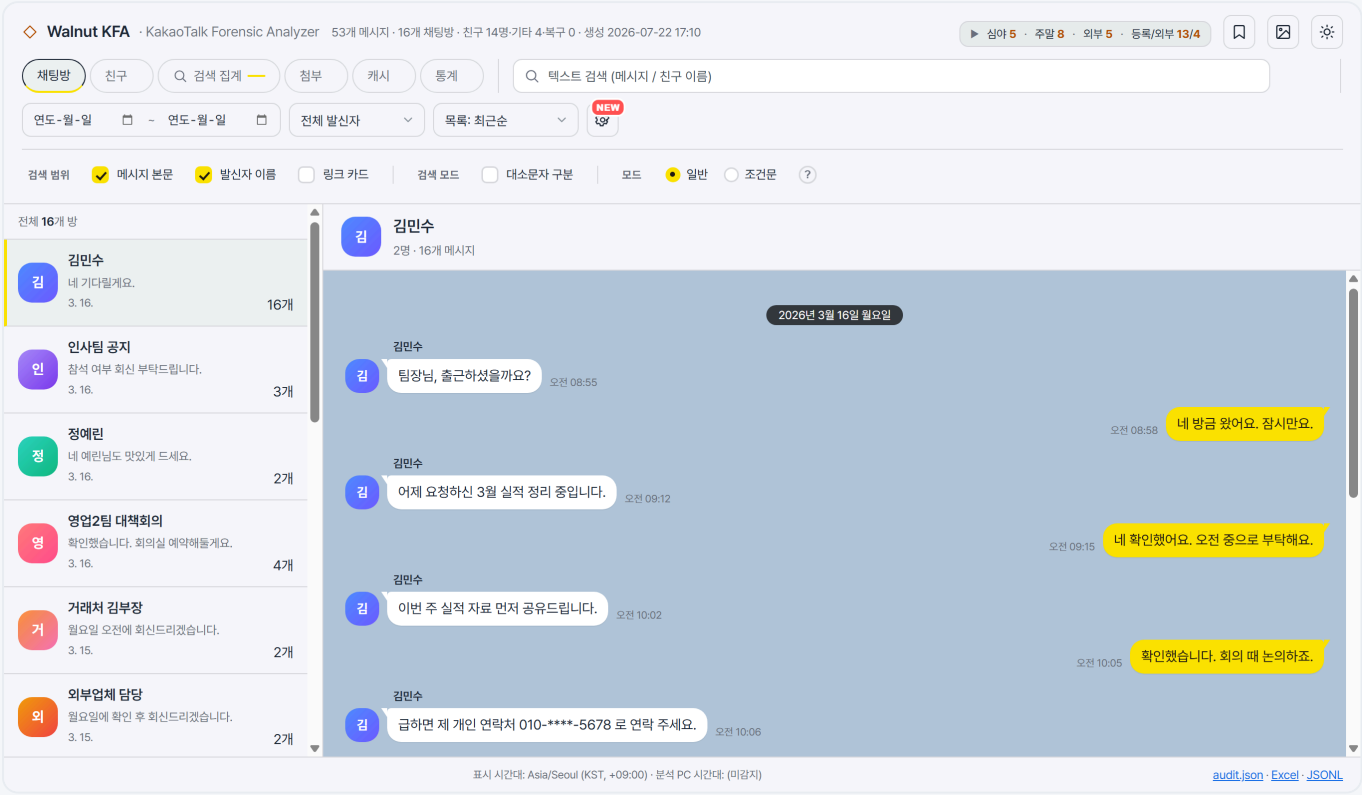
5 채팅방·발신자 매핑
메시지를 채팅방 및 발신자 정보와 연결합니다

6 분석 결과 생성
HTML 열람 화면과 표 형식 데이터를 생성합니다

오프라인 기반 처리
수집부터 결과 생성까지 대상 PC 또는 분석 환경 내에서 처리되며, 대화 내용은 외부로 전송되지 않습니다.

4. 분석 화면 — 채팅방 열람 및 검색

분석 결과는 HTML 파일로 생성되어, 별도 프로그램이 없는 PC에서도 웹 브라우저로 열람할 수 있습니다.
결과 화면은 채팅방, 친구, 검색 집계, 첨부, 캐시, 통계 탭으로 구성됩니다.



기능

채팅방 목록 정렬

방 이름, 마지막 메시지, 메시지 수를 기준으로 최근순·이름순 등 정렬하여 확인할 수 있습니다.

대화 내용 열람

카카오톡 화면처럼 말풍선·발신자·시각을 보여주고, 답장 인용·통화 기록도 함께 표시합니다.

삭제·회수 메시지 표시

삭제 또는 회수된 것으로 확인된 메시지는 해당 위치에 배지로 표시됩니다.

개인정보 선택 마스킹

전화번호, 계좌번호, 주민등록번호 등 개인정보 유형을 선택하여 일부 값을 마스킹할 수 있습니다.

고급 검색

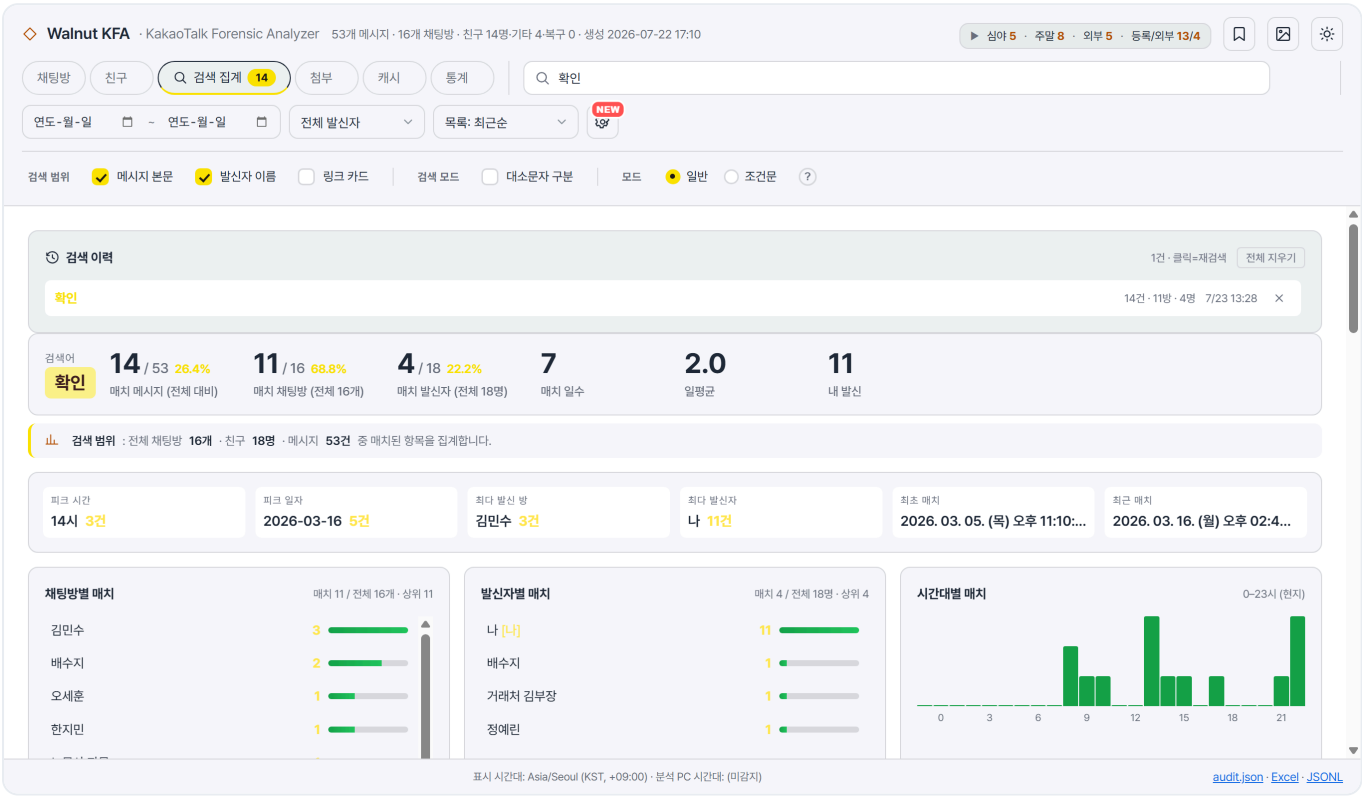
본문·발신자·링크 카드를 대상으로 AND·OR·NOT 조건식·와일드카드·정규식 검색을 지원합니다.

메시지 북마크 및 사건별 정리

여러 채팅방의 메시지를 북마크해 사건별 묶음으로 모으고, 메모를 달아 CSV로 내보냅니다.

5. 분석 화면 — 대화 통계 및 패턴 분석

전체 대화를 숫자와 그래프로 정리하여 대화 흐름과 주요 패턴을 확인할 수 있습니다.
검색 결과에 대해서도 동일한 방식으로 통계를 산출할 수 있습니다.



기능

검색 결과 통계

검색어와 일치하는 메시지 건수, 비율, 채팅방별·발신자별·시간대별 분포를 그래프로 확인할 수 있습니다.

기간·발신자 필터

기간과 발신자를 지정하여 조건에 맞는 대화만 통계에 반영할 수 있습니다.

전체 대화 통계

총 메시지 수, 채팅방 수, 발신자 수, 첨부파일 수, 오픈채팅 현황, 외부 사용자 수 등을 요약합니다.

이상 대화 패턴 지표

심야(밤 10시~새벽 6시)·주말·외부 연락처 메시지 건수를 화면 상단에 표시합니다.

첨부파일 분석

주고받은 사진, 동영상, 파일을 한 화면에 모아 파일 종류, 크기, 해시값, 원본 링크를 함께 표시합니다.

분석 결과 내보내기

열람 화면(HTML), 분석 보고서(PDF), 표 형식 데이터(Excel·CSV), 처리 이력을 파일로 저장할 수 있습니다.

6. 디지털 증거로서의 신뢰성 관리

분석 결과가 실제 조사·분쟁·소송 대응에 활용되기 위해서는 원본 데이터와의 동일성 및 분석 과정의 무결성을 설명할 수 있어야 합니다. 본 프로그램은 수집, 복호화, 분석, 보고까지의 처리 과정을 기록하고, 그 근거를 산출물에 함께 남깁니다.

01 원본 데이터 보존

입력 원본 데이터는 수정하지 않으며, 복호화 결과는 별도 영역에 기록됩니다.

02 해시 검증

입력 데이터와 산출물의 SHA-256 해시값을 기록하여 원본 동일성과 이후 변경 여부를 확인할 수 있습니다.

03 처리 이력 기록

수집, 복호화, 분석, 보고 각 단계의 수행 시각과 처리 내용이 감사 기록으로 남습니다.

04 분석자 및 생성 시점 기록

분석자 정보와 결과 생성 시점이 산출물에 포함되며, 필요 시 시점 확인 자료로 활용할 수 있습니다.

05 분석 재현성

동일한 입력 자료를 기준으로 다시 분석할 경우, 동일한 복호화 결과가 재현되도록 설계되어 있습니다.

정당한 권한과 동의를 전제로 분석합니다

본인 데이터	본인이 사용하거나 소유한 PC의 카카오톡 데이터 분석
소지자·당사자 동의	기기 소지자 또는 대화 당사자의 명시적 동의에 따른 분석
정당한 위탁	기업이 소유·관리하는 기기에 대해 사전 고지, 동의 및 내부 규정에 근거한 내부조사 위탁

본 분석은 수사기관의 강제수사 권한이 아니라, 소지자·당사자의 동의 또는 기업의 정당한 권한을 전제로 수행됩니다.
통신비밀보호법, 개인정보보호법 등 관계 법령과 적법 절차를 준수하며, 제3자의 개인정보는 필요한 경우 마스킹하여 보호합니다.

7. 제품 구성 및 주요 활용 사례

제품 구성

카카오톡 PC 데이터 복호화·분석 프로그램 Walnut은 다음 구성으로 제공됩니다.

실행 파일(EXE)
단일 실행 파일 형태로 제공
Windows 환경 지원

기간제 USB 동글키
USB 라이선스 키 제공
동글 1개당 1대 사용

사용 안내 및 기술지원
사용 설명서 제공
도입 및 기술 문의 대응

도입 방식

제품 도입 USB 동글키를 받아 대상 PC에서 직접 수집·분석합니다.

분석 의뢰 직접 수행이 어려운 경우, 디지털포렌식 전문 인력에게 수집·분석을 의뢰할 수 있습니다.

주요 활용 사례

동의 또는 정당한 권한 확인을 전제로, 다음과 같은 상황에서 활용할 수 있습니다.

유형	시나리오	프로그램 활용
기업 내부조사	임직원 부정행위 또는 정보유출 의심 상황에서 회사 소유 업무 PC 분석	업무 PC의 카카오톡 대화를 복호화하여 심야 대화, 외부 연락처, 첨부파일 등 관련 정황 확인
이혼·가사 분쟁	당사자가 본인 PC의 대화를 증거자료로 정리하려는 경우	닫힌 대화방을 포함한 대화를 복호화하여 타임라인과 참여자 정보를 정리
명예훼손·분쟁 대응	본인 대화를 근거로 사실관계를 소명해야 하는 경우	본인 데이터를 복호화하고 무결성 기록과 함께 보고서로 출력
퇴직자 영업비밀 유출 의심	반납된 회사 소유 PC에서 영업비밀 유출 정황 확인	카카오톡 대화와 첨부파일 흔적을 확인하여 반출 정황 정리

산출물 형식

HTML 뷰어
탭별 결과 열람 통계 및 행위 정황 포함

분석 보고서(PDF)
분석 결과 정리 제출 및 보고용

표 형식 데이터
Excel·CSV 필터 및 검색 용이

무결성 기록
감사 로그, 서명, 복호화 범위 포함

8. HM Company 주요 수행 역량 및 실적

HM Company는 2011년 설립 이후 디지털포렌식 전문성을 기반으로 정보유출 조사, 개인정보·정보보호 리스크 진단, IT 감사, 내부감사 등 기업 리스크 대응 서비스를 수행해 왔습니다.

ADFS 본부			RAS 본부		
디지털포렌식 서비스	정보유출 조사	IT 감사	컴플라이언스 리스크 진단	회계감사 외부전문가 조사	
정보보호 리스크 진단	KOLAS 공인시험성적서 발급		경영진단·내부감사	직장 내 괴롭힘 조사	PMA

Why HM COMPANY ADFS

15년+
디지털포렌식 기반
조사·진단 수행 경험

19,946+
누적 디지털포렌식
증거물 처리 경험

KOLAS
민간 최초 디지털포렌식 분야
KOLAS 공인시험기관 인정 보유

NDA
보안서약 체결 및
데이터 안전 폐기 체계 운영

주요 수행 실적

분야	주요 수행 실적
금융	내부감사 자료 검토 및 Co-Sourcing
금융	협력업체 개인정보 및 정보보안 리스크 진단
금융	법인카드 및 골프회원권 사용 적정성 조사
제조	임직원 부정행위 조사 및 사실관계 분석
제조	첨단기술 및 영업비밀 유출 리스크 진단
제조	제품 설계도 등 영업비밀 파일 유출 리스크 진단
제조	회계장부 등 영업비밀 유출 진단
제조	정보유출 및 부정위험 조사·진단
의료·헬스케어	임직원 개인정보 관리실태 진단
의료·헬스케어	임원 부정행위 의혹 조사 및 검토
유통	보유 고객정보 관리실태 진단
유통	협력업체 개인정보 관리실태 진단
법률 사건 지원	디지털 증거 확보, 선별 추출, 전처리, 검색 가능한 검토 환경 구성

HM COMPANY™

Digital Forensic Evidence Collection & Preservation Service

Contact Us

박 재 현 상무

jaehyun.park@hmcom.co.kr

이 정 훈 수석

jeonghoon.lee@hmcom.co.kr

전화

02-6237-6213

제품 도입 상담과 디지털포렌식 분석 의뢰를 지원합니다
도입 방식, 비용 등 상세 사항은 문의해 주시기 바랍니다

hmcom.co.kr
hmadfs.com
서울특별시 서초구 효령로70길 36-9, 와이엘타워 2층, 3층