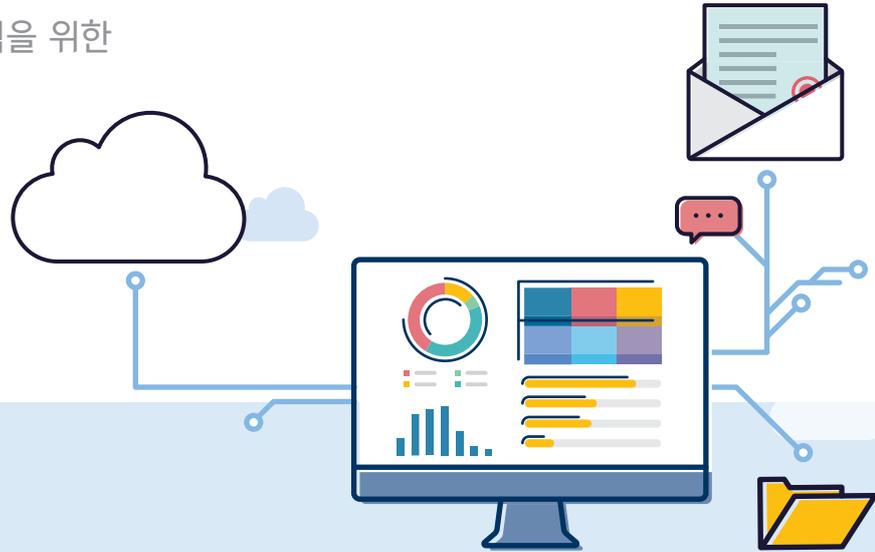


DFAS Cloud

이메일 및 클라우드 분석을 위한
디지털포렌식 솔루션



DFAS CLOUD는 클라우드 컴퓨팅 환경과 email (웹, 로컬) 데이터를 수집 · 분석하는 포렌식 솔루션입니다.

클라우드 및 이메일에 저장되는 데이터는 날이 갈수록 증대되고 있으며, 이러한 데이터는 사용자의 행위를 분석하는데 있어 매우 중요한 가치를 가지고 있습니다.

DFAS CLOUD는 사용자의 클라우드 또는 메일 계정을 통하여 획득한 데이터를 통하여 부정행위자의 디지털 증거 자료에 대한 자동 수집 및 분석·관리를 수행합니다.

주요 기능



자동 계정
유효성 검사

- 클라우드 및 email 계정을 사용하여 액세스 가능한 정보 자동 검색



검색

- 제목, 발신자/수신자, 날짜, 내용, 첨부 파일 등에 대한 검색 기



데이터 분석

- 원본 보기 (메일 소스, 본문, 첨부 파일, 헤더 등 정보 확인)
- 북마크 및 메모 기능



시각화

- 타임라인 분석, 상관관계 및 첨부파일 분석



분석 결과 보고서
자동 생성

- 분석 결과 통계화 표시
- 비정상적 정보 통지



케이스 관리

- 여러 메시지를 단일 증거 컨테이너로 추출
- 파일 저장 및 CD 레코딩 제공
- 수집된 데이터 파일 생성 및 해시 값 (MD5, SHA-1) 계산



- 클라우드 및 메일 데이터의 디지털 포렌식 분석 수행
- 이상 사용 징후 및 사용자 사전 탐지 효과
- 허가되지 않은 정보에 대한 접근 차단
- 즉각적인 사고 대응
- 현장 및 Lab에서 신속하게 분석 결과 확인
- 외부 전문가나 수사기관 의뢰 전 충분한 사전 내부 조사 기회 제공

주요 기능



웹 메일



로컬 메일



클라우드 환경

수집

웹 메일 및 로컬 메일

- 동일 사용자 계정에 대한 타 사이트 접속 가능 여부 지원 (계정 액세스 테스트)
- 여러 유형의 email 데이터 획득 (Outlook, Outlook Express, Gmail, MSN, etc.)
- 북마크, 검색엔진, 미리보기 및 내보내기 기능 지원

로컬 메일 복구

- PST, OST, DBX 복구
- 복구 전용 별도의 사서함 제공

클라우드

- 클라우드 기반 데이터 수집 및 분석
- 다양한 종류의 클라우드 서비스 지원 (Facebook, Instagram, Google Drive, Google Contacts, Dropbox, Twitter 등)
- 정보 유출 용의자의 온라인 행위 데이터 수집

데이터 분석

분석 결과 보고서 자동 생성

- 웹 메일 및 PC에 저장된 로컬 메일의 데이터까지 디지털 포렌식 분석
- 클라우드 환경에 저장된 온라인 행위 데이터 분석
- 고급 링크 분석을 통해 사용자 및 도메인 간의 커뮤니케이션 및 상관관계 분석
- 짧은 시간에 대량의 데이터를 스캔, 조회, 검색, 조사, 분석부터 보고서 생성까지 사용자에게 제공
- 데이터 분석 결과 타임라인 및 시각화 자료 제공

보고서 내보내기

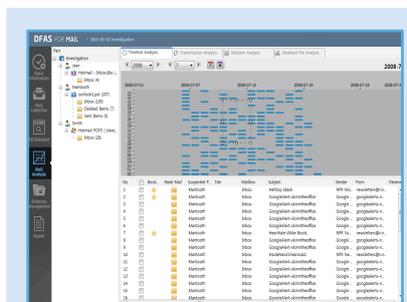
- 분석 결과 자동 보고서 생성 (첨네일 제공)
- JPG, HTML 형식의 보고서 제공



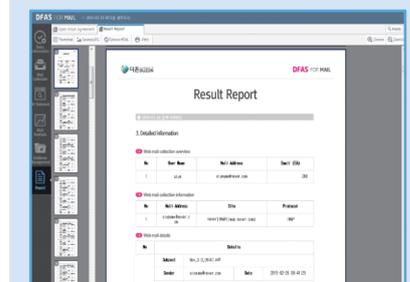
스크린샷



직관적인 UI와 대시보드



타임라인 분석



자동 보고서 생성