

브라우저 기반 AI Assistant Extension Program 아티팩트 분석

2025-1 **AJOU**
SOFTCON

팀 명 회장모이조

팀 원 한주현, 이상민, 한창민

지도교수 손태식

멘 토 최 욱

개발동기 및 목적

! Problem

AI를 활용한 범죄 가능성 및 포렌식 수요 증가

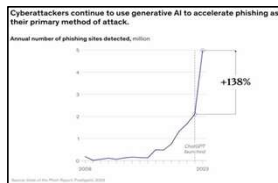
AI 어시스턴트 확장 프로그램에 대한 포렌식 연구 미비.

! Solution

Top3(Monica, Sider, MaxAI) AI 확장 프로그램 대상.

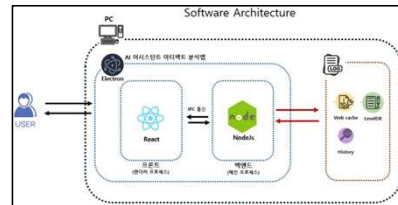
AI 확장 프로그램의 프롬프트, 응답, 업로드 파일, 쿠키 등의 아티팩트 연구

연구 결과 기반 수집/분석 도구 제공



주요기술

분석 도구 Architecture



JSON 변환 및 키값 추출

RAW 데이터를 JSON 형태로 변환.

데이터 내 주요 Key값 추출.

```

[{"id": 1, "name": "John", "age": 30, "email": "john@example.com"}, {"id": 2, "name": "Jane", "age": 25, "email": "jane@example.com"}, {"id": 3, "name": "Bob", "age": 35, "email": "bob@example.com"}]
    
```

TreeView 및 검색 기능

트리 구조로 시각화하여, 중첩된 구조를 계층적으로 탐색.

키워드 기반 검색을 통해 특정 대화 내용, 키, 값 등을 빠르게 검색.



대화 흐름 시각화

사용자 프롬프트와 AI 응답 데이터를 시간순 대화 흐름으로 재구성.

질문-응답 형태로 대화정렬 및 업로드한 파일 다운 기능 제공.



결과 및 분석

Program	유저 정보	채팅 정보	업로드 파일 정보	파일 획득 가능 여부 (유효기간 존재)	아티팩트 추출 가능
Monica	○	○(삭제, 임시)	○	○(14일)	○
Sider	○	△	○	△(23일)	○
MaxAI	○	○(삭제)	○	○(7일)	△

획득 가능한 데이터 종류에 대한 최종 분석 표

활용방안 및 기대효과

브라우저 확장형 AI 서비스에 대한 포렌식연구 기초 성립

실제 사건 대응 시 삭제된 대화 기록, 사용자 입력/응답, 업로드 파일 획득

악성 사용자 식별, 비인가자 정보 유출 탐지 등에 실무 적용

분석을 통해 도출한 취약점(예: 잔존 데이터, Signed URL 접근)을 바탕으로 보안 기능 강화 기능 설계에 기여

오픈소스 URL

https://github.com/hcmhcs/AI_extension_forensic_tool



저장 구조 분석



확장 프로그램 데이터 저장 위치 분석

LevelDB, IndexedDB 구조 분석 및 JSON 형식 파일 변환 (디코딩 진행)

채팅 내용 및 업로드 파일 분석



AI와 상호작용한 발생한 대화내역(삭제/임시) 구조 분석
사용한 AI 모델, 채팅 시간 기록 확인

AI모델에 업로드한 이미지, 파일에 대한 데이터 추출 원본 확보

