Dreamhack-chrome_artifacts (level1)

👉 **[함께실습] chrome_artifacts에서 실습하는 문제입니다.**

당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.

범행에 사용된 것으로 보이는 아이콘 이미지(`.ico`)가 외부 인터넷 사이트에서 다운로드된 것으로 보입니다.

Chrome 브라우저 아티팩트를 분석해 플래그를 구해주세요.

사용 툴 - FTK Imager, DB Browser for SQLite

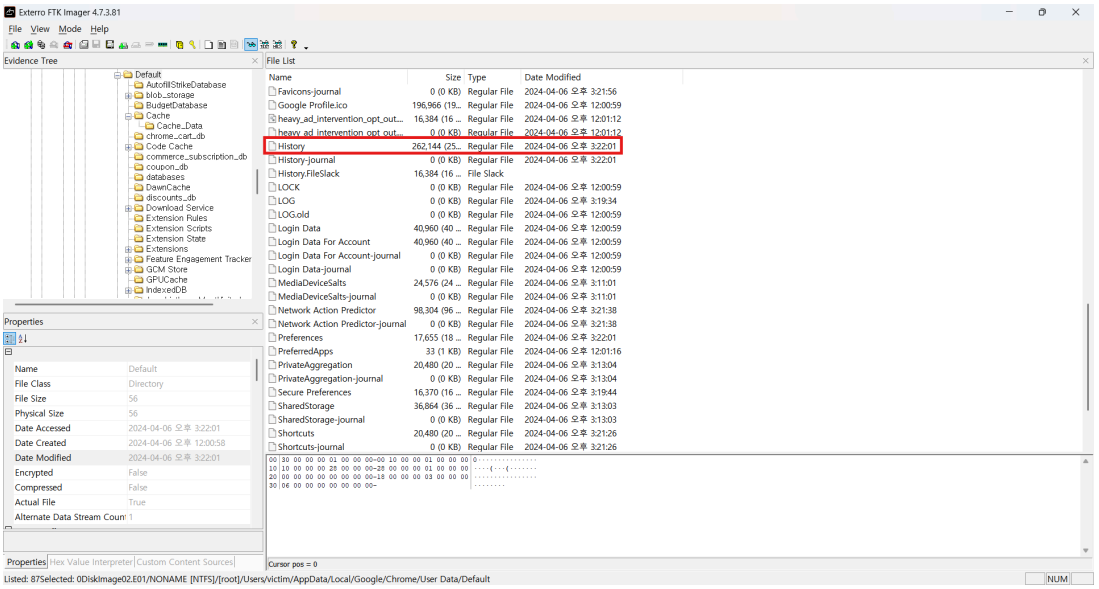
1. Web Browser Artifacts

   Web Browser는 Chrome, Edge, Whale 등과 같이 인터넷을 이용하기 위해 실행하는 응용 프로그램을 말한다. Web Browser Artifacts에서 Web Browser의 데이터를 확인할 수 있는데 확인할 수 있는 데이터의 종류는 아래와 같다.

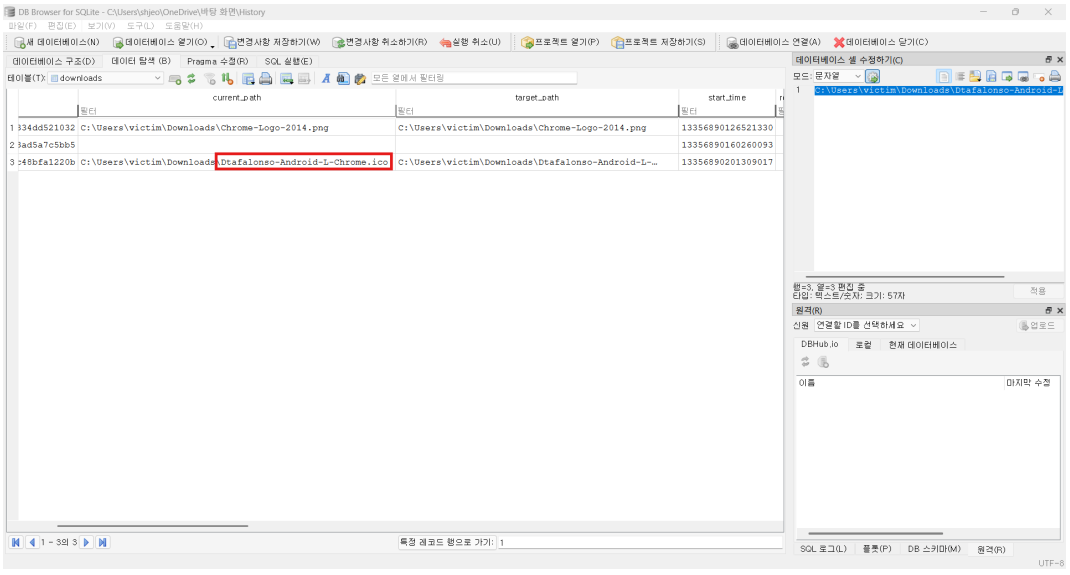
   - History: 방문한 URL, 방문 횟수, 방문 시각 등
   - Cache: 캐시로 저장되는 이미지, 텍스트, 스크립트, 아이콘, 시간, 크기
   - Cookie: 사용자 데이터, 자동 로그인 등
   - Download list: 저장 경로, URL, 크기, 시간, 성공 여부 등

2. FTK Imager 를 통하여 아래 경로에서 다운로드한 파일을 확인하기 위하여 History 파일을 추출

   - 경로 : `C:\User\victim\AppData\Local\Google\Chrome\User Data\Default`



3. DB Browser for SQLite 를 통하여 History 에서 downloads 를 확인한 결과, .ico 확장자를 갖는 파일은 하나 밖에 없음을 확인
    - 분석 내용 : 타임스탬프는 Chrome 형식의 타임스탬프이므로 이를 Unix Timestamp로 변환 必



👉 DH{Dtafalonso-Android-L-Chrome_1712416601_image/x-icon}