Dreamhack- chrome_artifacts(level1)

문제

Description

[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.

Info

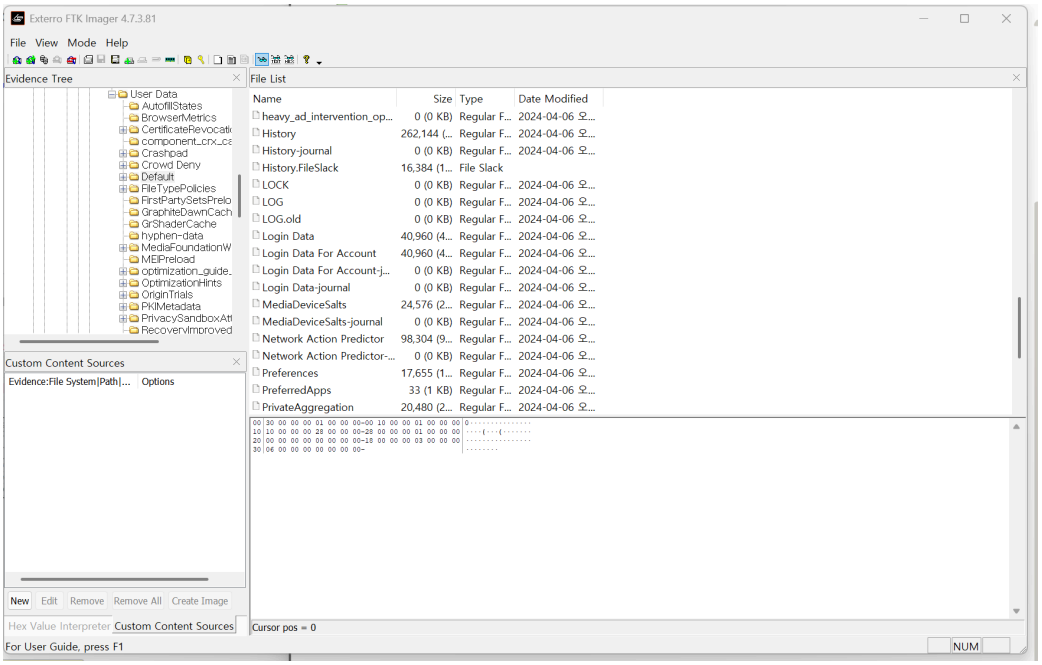
- FLAG = `DH{A_B_C}`
  - A: 파일의 이름 (경로 제외, 확장자 제외)
  - B: 파일 다운로드를 시작한 시간 (**Unix Timestamp**, seconds 단위)
  - C: 파일의 MIME type
- 예를 들어 A가 `dream`, B가 `1712154549`, 그리고 C가 `text/plain`이라면 FLAG는 `DH{dream_1712154549_text/plain}`입니다.

풀이

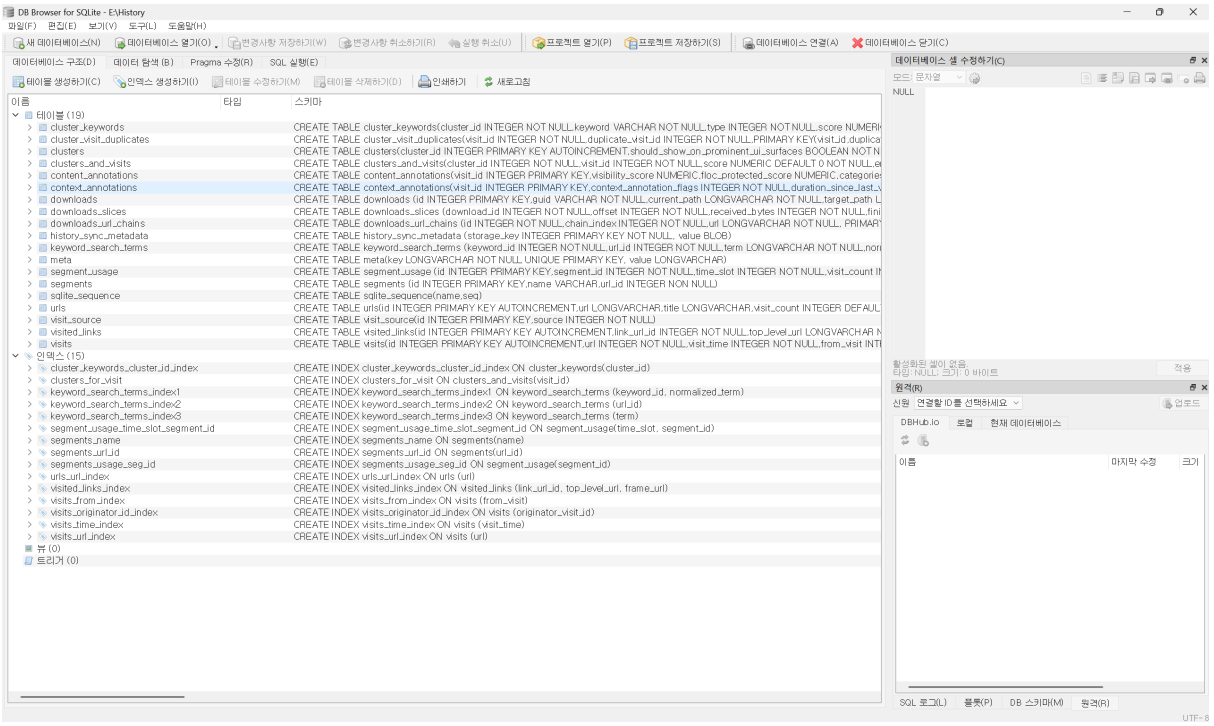
1. 문제 파악

   외부 인터넷 사이트에서 `.ico` 확장자의 이미지 파일을 다운로드 ~>
   Chrome 브라우저의 아티팩트를 분석 진행

2. 문제 풀이



브라우저 아티팩트 분석을 위해 FTK에서 History 파일을 추출한다.



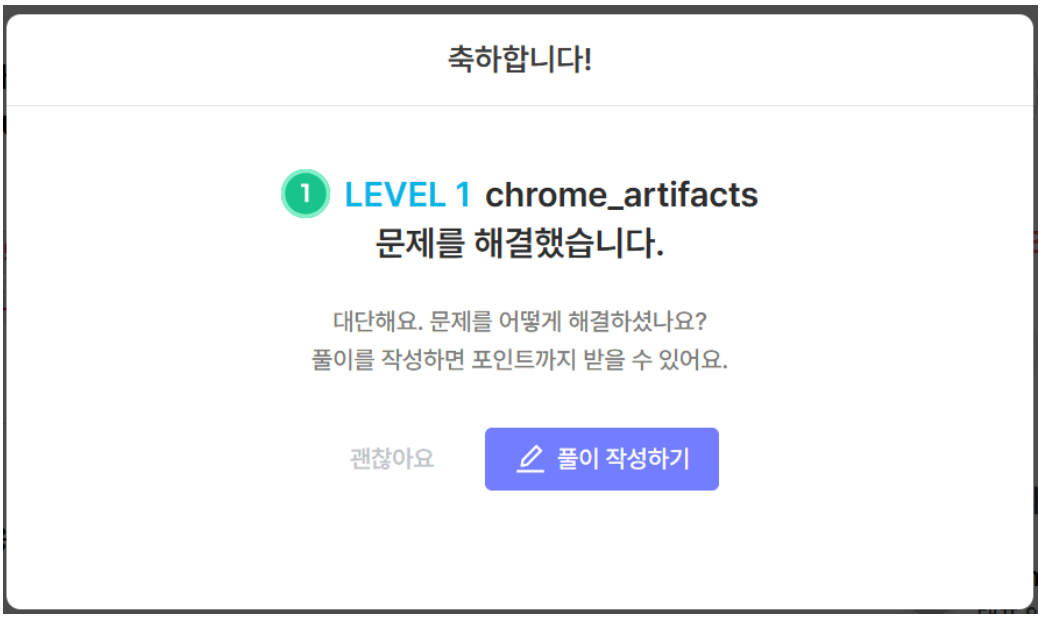
DB Browser for SQLite로 오픈하여 데이터 탐색 → downloads 테이블 선택

파일의 이름 : Dtafalonso-Android-L-Chrome.ico

파일 다운로드를 시작한 시간 : 13356890201309017 ⇒ 1712416601

파일의 MIME type : image/x-icon

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



참고 자료

https://shsh010914.tistory.com/69