# Dreamhack-chrome artifacts(level1)

## [forensics]

### Description

**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.** (2024.10.02)

#### Info

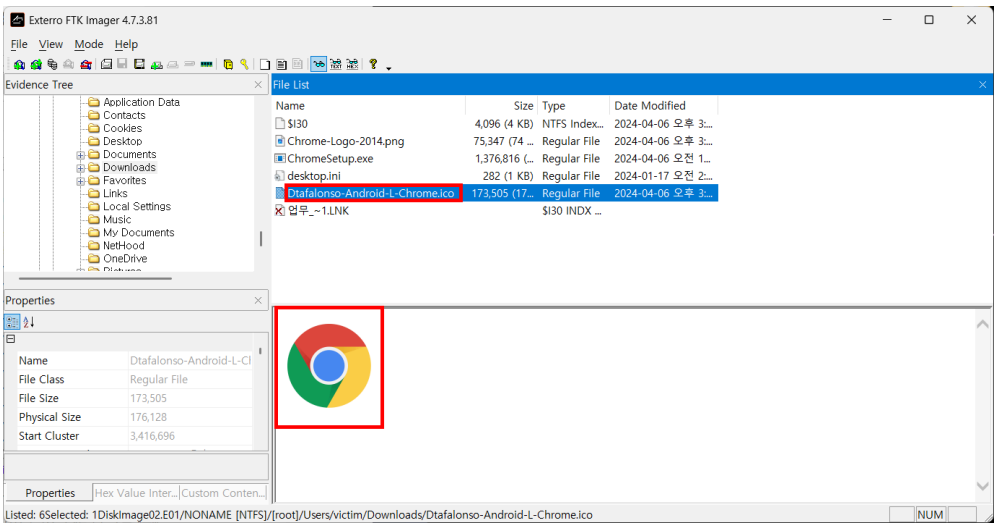
- FLAG = `DH{A_B_C}`
  - ◦ A: 파일의 이름 (경로 제외, 확장자 제외)
  - ◦ B: 파일 다운로드를 시작한 시간 (**Unix Timestamp**, seconds 단위)
  - ◦ C: 파일의 MIME type
- 예를 들어 A가 `dream`, B가 `1712154549`, 그리고 C가 `text/plain`이라면 FLAG는 `DH{dream_1712154549_text/plain}` 입니다.

---

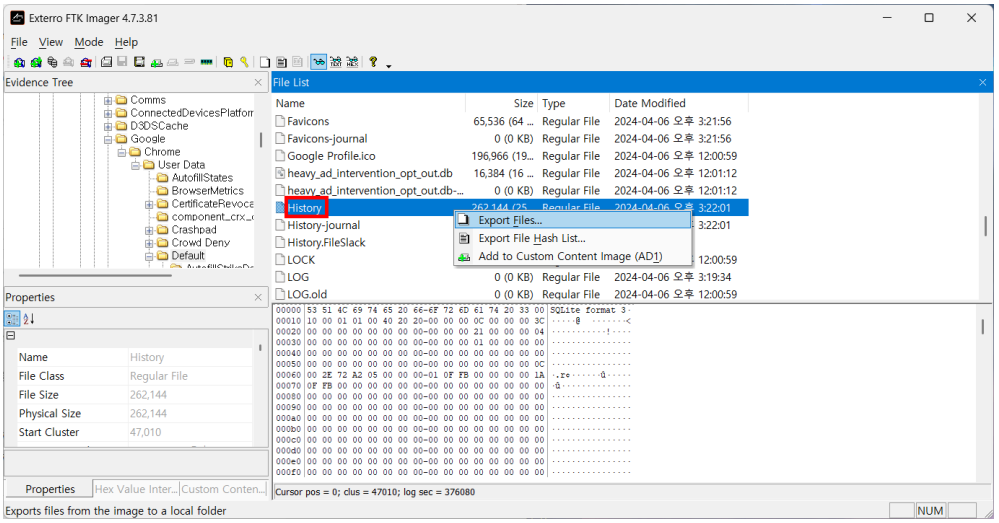
## Write up

- 사용 도구: FTK Imager, DB Browser for SQLite

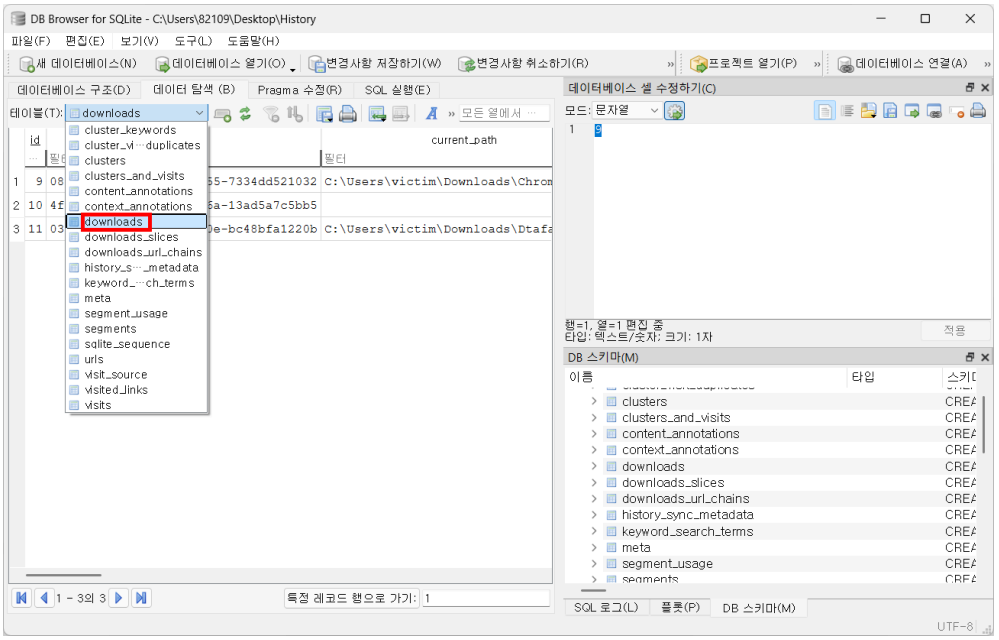
- `C:\Users\victim\Downloads` 경로의 `.ico` 파일 확인
  - `Dtafalonso-Android-L-Chrome.ico`
  - **2024-04-06 15:16:48**



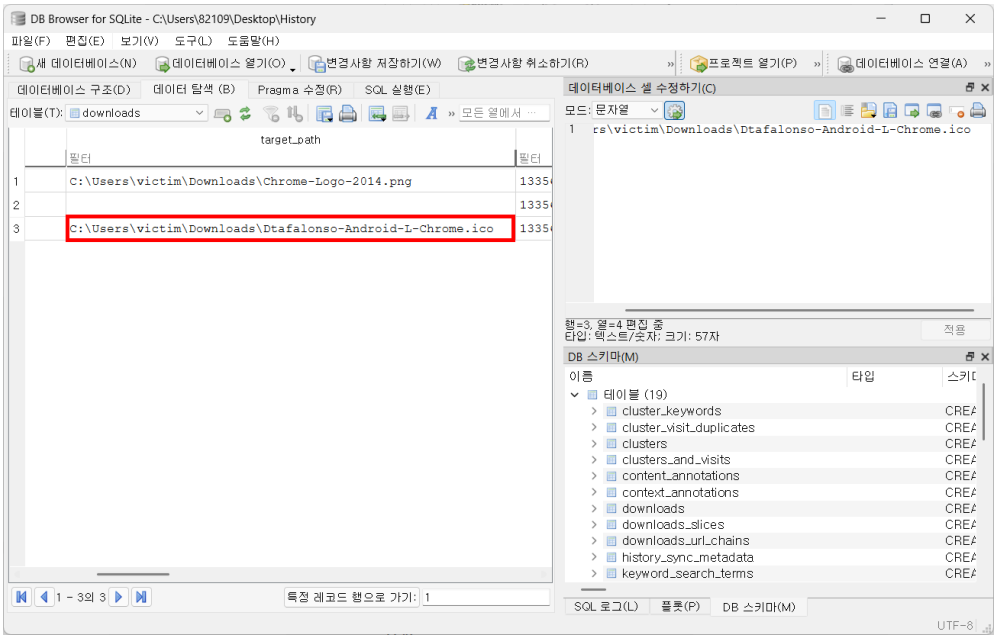

- FTK Imager를 통해 `C:\Users\victim\AppData\Local\Google\Chrome\User Data\Default\History` 추출



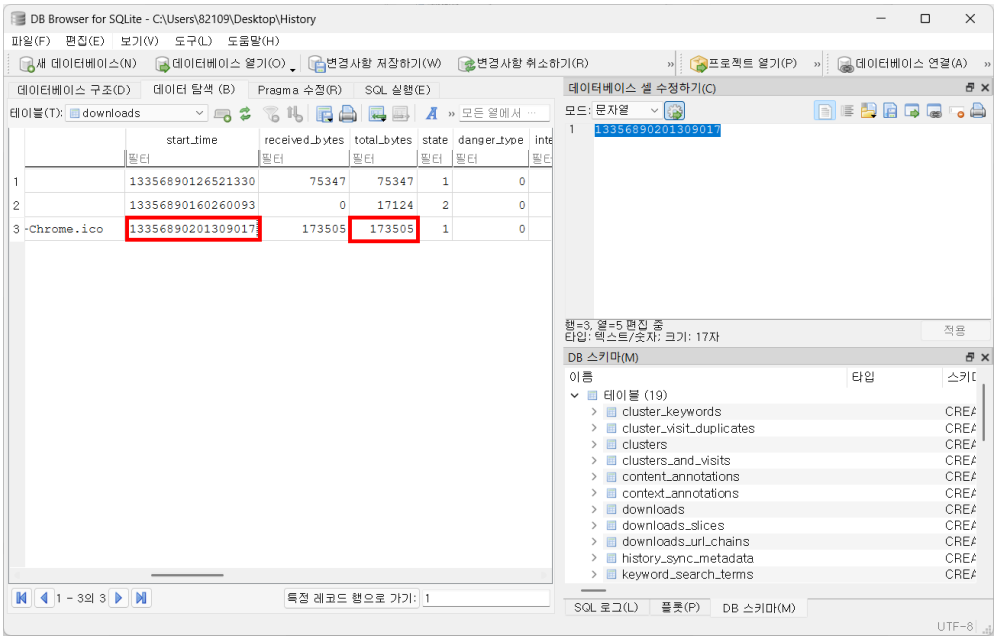

- DB Browser for SQLite를 통해 downloads 기록 확인

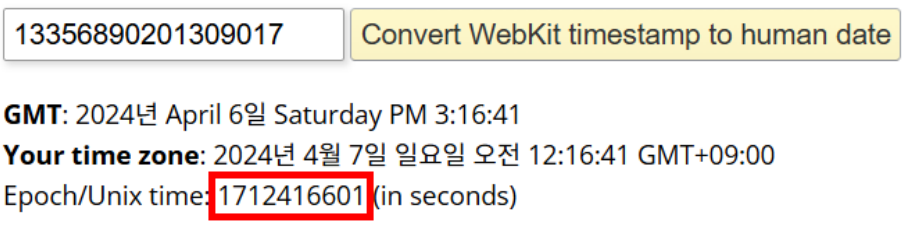



- `Dtafalonso-Android-L-Chrome.ico` 파일 다운로드 확인

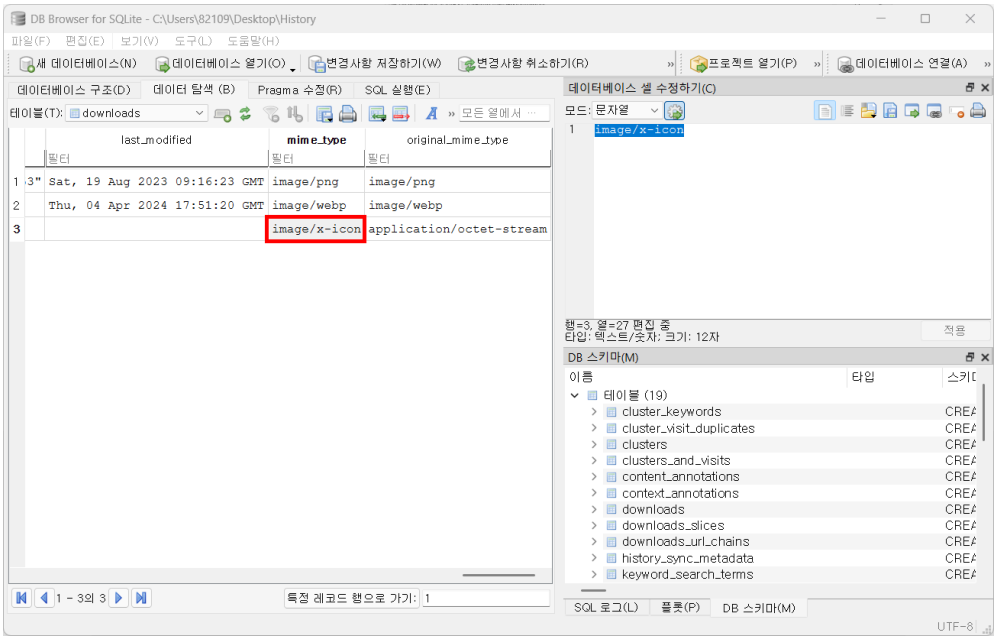



- 다운로드 시작 시간과 파일 크기 확인
  - `C:\Users\victim\Downloads` 파일 크기(173,505)와 일치함 확인
  - WebKit을 통해 Unix TimeStamp로 변환, `13356890201309017`



- MIME TYPE 확인 ⇒ `image/x-icon`




| current_path | target_path | start_time | total_bytes | mime_type |
|---|---|---|---|---|
| C:\Users\victim\Downloads\Dtafalonso-Android-L-Chrome.ico | C:\Users\victim\Downloads\Dtafalonso-Android-L-Chrome.ico | 13356890201309017 | 173505 | image/x-icon |

- A: **Dtafalonso-Android-L-Chrome**
- B: **1712416601**
- C: **image/x-icon**
- FLAG 형식으로는, DH{Dtafalonso-Android-L-Chrome_1712416601_image/x-icon}

---

## FLAG

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