Write-up: chrome_artifacts (level1)

https://dreamhack.io/wargame/challenges/1328

1. Challenge Info

- **Challenge Name:** chrome_artifacts
- **Category:** Forensics
- **Difficulty Level:** Level 1
- **Platform:** DreamHack Wargame
- **Objective:**

  고객의 해킹 사고를 분석해 Chrome 부라우저 아티팩트를 분석해 파일의 이름, 파일 다운로드를 시작한 시간, 파일의 MIME type를 분석하여 플래그를 완성하다.

> 플래그 형식: **DH{A_B_C}**
>
> - A: 파일의 이름 (경로 제외, 확장자 제외)
> - B: 파일 다운로드를 시작한 시간 (Unix Timestamp, seconds 단위)
> - C: 파일의 MIME type

2. Problem Description

> “당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.
>
> 범행에 사용된 것으로 보이는 아이콘 이미지(`.ico`)가 외부 인터넷 사이트에서 다운로드 된 것으로 보입니다.
>
> Chrome 브라우저 아티팩트를 분석해 플래그를 구해주세요.”

- 제공된 디스크 이미지: `DiskImage02.E01`
- 이 파일은 `boot_time` , `nikonikoni` 문제와 동일

---

3. Provided Files

- `DiskImage02.E01` (Windows 시스템의 디스크 이미지 파일, E01 포맷)

---

4. Tools Used

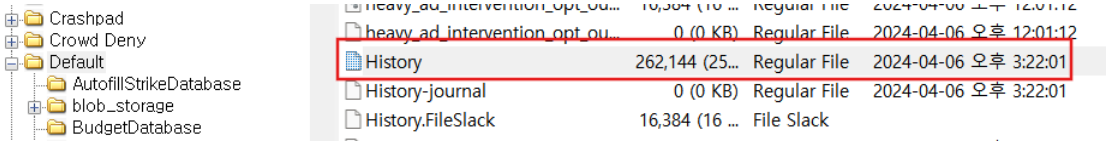
Tool	Version
FTK Imager	v4.7.8.31
DB Browser for SQLite	v3.13.1

---

5. Analysis Steps

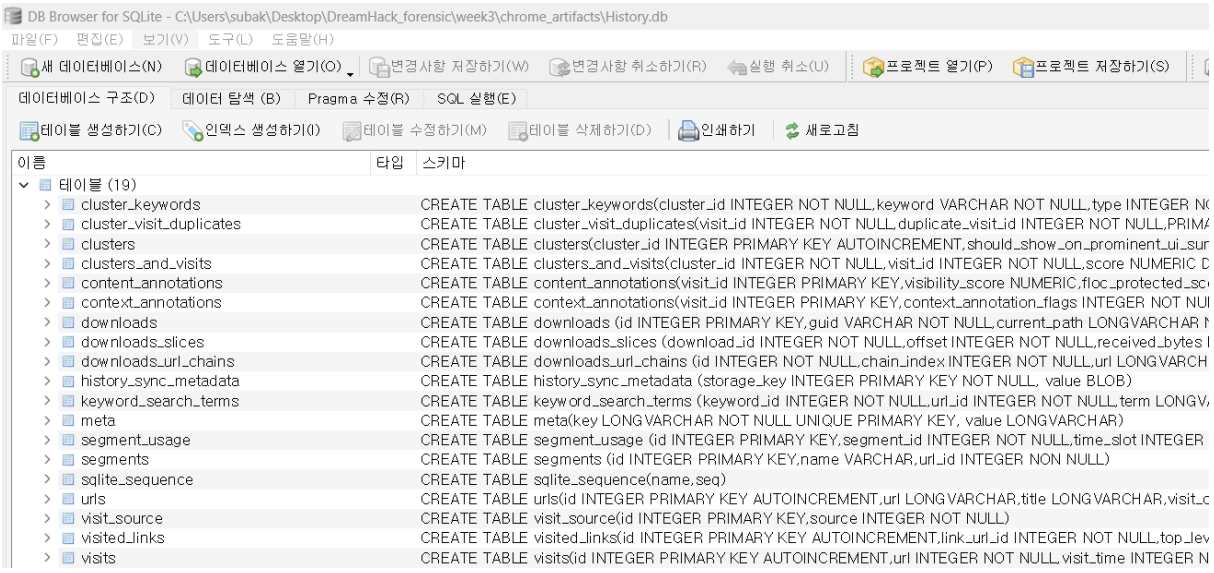
5.1 디스크 이미지 마운트

- **도구:** FTK Imager
- 제공된 `DiskImage02.E01` 파일을 FTK Imager로 열기
- `History` (다운로드 기록, 방문 기록) 파일 추출
  - **경로:** `C:\Users\victim\AppData\Local\Google\Chrome\User Data\Default\History`



5.2 History 파일 확인

- **도구:** DB Browser for SQLite
- 추출한 History 파일을 DB Browser for SQLite로 열기

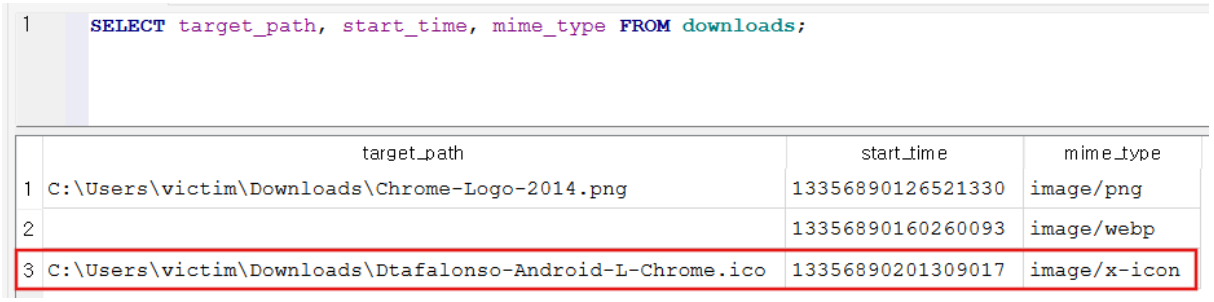


- 명령어를 사용하여 다운로드한 파일 중 확장자가 `.ico` 이고 외부 URL에서 내려받은 파일을 찾기 위해 파일 경로, 다운로드 시작 시간, MIME type을 검색함

- **명령어:**

```
SELECT target_path, start_time, mime_type FROM downloads;
```

- **target_path:** `C:\Users\victim\Downloads\Dtafalonso-Android-L-Chrome.ico`
- **start_time:** `13356890201309017`
- **mime_type:** `image/x-icon`



```
SELECT target_path, start_time, mime_type FROM downloads;
```

	target_path	start_time	mime_type
1	C:\Users\victim\Downloads\Chrome-Logo-2014.png	13356890126521330	image/png
2		13356890160260093	image/webp
3	C:\Users\victim\Downloads\Dtafalonso-Android-L-Chrome.ico	13356890201309017	image/x-icon

5.3 파일 다운로드를 시작한 시간 변환

- start_time: `13356890201309017`

- **변환 과정**
  1. 단위 변환 (초 단위로 변환)
     - 주어진 값은 Webkit/FILETIME 기준 마이크로초 단위.
     - 초 단위로 변환:

       ```
       13356890201309017 / 1,000,000 = 13356890201.309017 (초)
       ```

       - 이는 1601년 1월 1일부터 경과한 총 초(second)
  2. Epoch 차이 보정 (Unix epoch으로 변환)
     - Windows Epoch(1601년)과 Unix Epoch(1970년) 사이의 초 차이:

       ```
       11644473600초
       ```

     - 이를 빼서 Unix Timestamp로 변환:

```
13356890201.309017 - 11644473600 = 1702416601.309017
```

3. 결과 확인
    - 소수점 아래를 버리고 정수 부분만 사용:

```
Unix Timestamp = 1702416601
```

5.4 최종 정보 정리

- **파일의 이름:** `Dtafalonso-Android-L-Chrome`
- **파일 다운로드를 시작한 시간:** `1712416601`
- **파일의 MIME type:** `image/x-icon`

---

6. Flag

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