

chrome_artifacts

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.

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/plain이라면 FLAG는 DH{dr

사용한 도구

FTK Imager, DB Browser for SQLite

Background

Web 브라우저 아티팩트

History: 방문한 URL, 방문 횟수, 방문 시각 등

Cache: 캐시로 저장되는 이미지, 텍스트, 스크립트, 아이콘, 시간, 크기 등

Cookie: 사용자 데이터, 자동 로그인 등

Download list: 저장 경로, URL, 크기, 시간, 성공 여부 등

<https://shsh010914.tistory.com/69>

Chrome 브라우저 아티팩트

기본 경로: `UserProfile%\AppData\Local\Google\Chrome\User Data\Default`

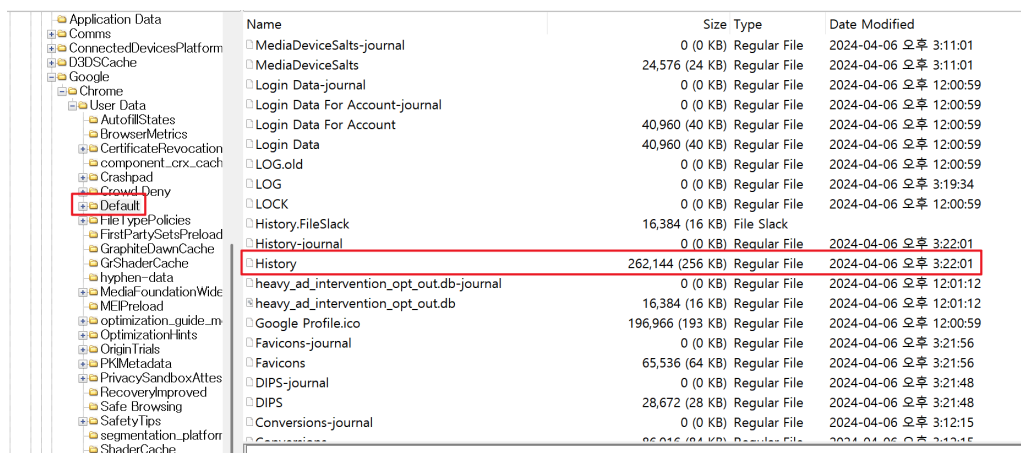
History 정보 분석

- 파일 형식: SQLite DB 파일 형식
- 주요 테이블

downloads 테이블	언제 다운로드 했는지, 다운로드 후 어디에 저장되었는지, 언제 접근했는지 등
urls 테이블	방문한 url 정보 저장, 같은 url은 중복 저장 X, 중복 방문 시 마지막 접속 시간 저장
visits 테이블	실제 방문 정보 저장, 실제 방문 시 저장되는 url정보는 urls 테이블에서 참조

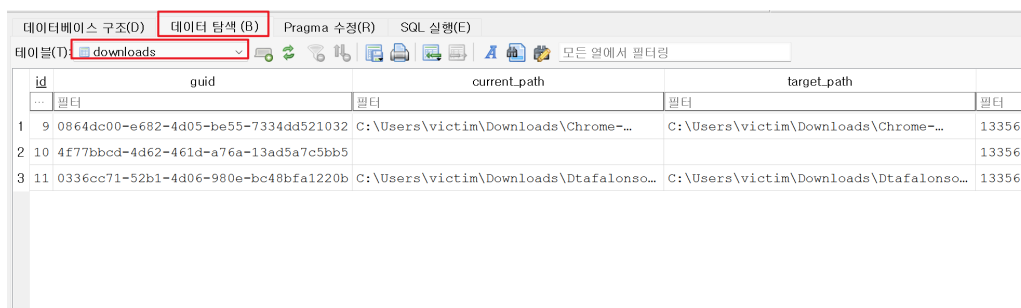
1. Chrome 기본 경로에서 History파일 추출

FTK Imager로 Chrome 기본 경로에서 History 파일 추출



Name	Size	Type	Date Modified
MediaDeviceSalts-journal	0 (0 KB)	Regular File	2024-04-06 오후 3:11:01
MediaDeviceSalts	24,576 (24 KB)	Regular File	2024-04-06 오후 3:11:01
Login Data-journal	0 (0 KB)	Regular File	2024-04-06 오후 12:00:59
Login Data For Account-journal	0 (0 KB)	Regular File	2024-04-06 오후 12:00:59
Login Data For Account	40,960 (40 KB)	Regular File	2024-04-06 오후 12:00:59
Login Data	40,960 (40 KB)	Regular File	2024-04-06 오후 12:00:59
LOG.old	0 (0 KB)	Regular File	2024-04-06 오후 12:00:59
LOG	0 (0 KB)	Regular File	2024-04-06 오후 3:19:34
LOCK	0 (0 KB)	Regular File	2024-04-06 오후 12:00:59
History.FileSlack	16,384 (16 KB)	File Slack	
History-journal	0 (0 KB)	Regular File	2024-04-06 오후 3:22:01
History	262,144 (256 KB)	Regular File	2024-04-06 오후 3:22:01
heavy_ad_intervention_opt_out.db-journal	0 (0 KB)	Regular File	2024-04-06 오후 12:01:12
heavy_ad_intervention_opt_out.db	16,384 (16 KB)	Regular File	2024-04-06 오후 12:01:12
Google Profile.ico	196,966 (193 KB)	Regular File	2024-04-06 오후 12:00:59
Favicons-journal	0 (0 KB)	Regular File	2024-04-06 오후 3:21:56
Favicons	65,536 (64 KB)	Regular File	2024-04-06 오후 3:21:56
DIPS-journal	0 (0 KB)	Regular File	2024-04-06 오후 3:21:48
DIPS	28,672 (28 KB)	Regular File	2024-04-06 오후 3:21:48
Conversions-journal	0 (0 KB)	Regular File	2024-04-06 오후 3:12:15
Conversions	86,016 (84 KB)	Regular File	2024-04-06 오후 3:12:15

2. DB Browser for SQLite로 downloads 테이블 확인



id	guid	current_path	target_path	s
1	0864dc00-e682-4d05-be55-7334dd521032	C:\Users\victim\Downloads\Chrome-...	C:\Users\victim\Downloads\Chrome-...	133566
2	10 4f77bbcd-4d62-461d-a76a-13ad5a7c5bb5			133566
3	11 0336cc71-52b1-4d06-980e-bc48bfa1220b	C:\Users\victim\Downloads\Dtafalonso...	C:\Users\victim\Downloads\Dtafalonso...	133566

새 데이터베이스(N) 데이터베이스 열기(O) 변경사항 저장하기(W) 변경사항 취소하기(R) 실행 취소(U) 프로젝트 열기(P) 프로젝트 저장하기(S)			
데이터베이스 구조(D) 데이터 탐색(B) Pragma 수정(R) SQL 실행(E)			
데이터베이스(T) downloads 모든 열에서 필터링			
id	guid	current_path	target_path
...	필터	필터	필터
1	9 0864dc00-e682-4d05-...	C:\Users\victim\Downloads\Chrome-Logo-2014.png	C:\Users\victim\Downloads\Chrome-Logo-2014.png
2	10 4f77bbcd-4d62-461d-...		
3	11 0336cc71-52b1-4d06-980...	C:\Users\victim\Downloads\Dtafalonso-Android-L-Chrome.ico	C:\Users\victim\Downloads\Dtafalonso-Android-L-Chrome.ico

- .ico 다운로드 기록은 C:\Users\victim\Downloads\Dtafalonso-Android-L-Chrome.ico 경로에 있는 Chrome.ico 하나만 존재

3. 파일 다운로드 시간과 MIME type 확인

- start time

start_time
필터
13356890126521330
13356890160260093
13356890201309017

13356890201309017 → unix timestamp로 변환 → 1712416601

- MIME type

mime_type
필터
image/png
image/webp
image/x-icon

FLAG

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