

chrome_artifacts

Description

[함께실습] **chrome_artifacts**에서 실습하는 문제입니다.

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.

Info

FLAG = **DH{A_B_C}**

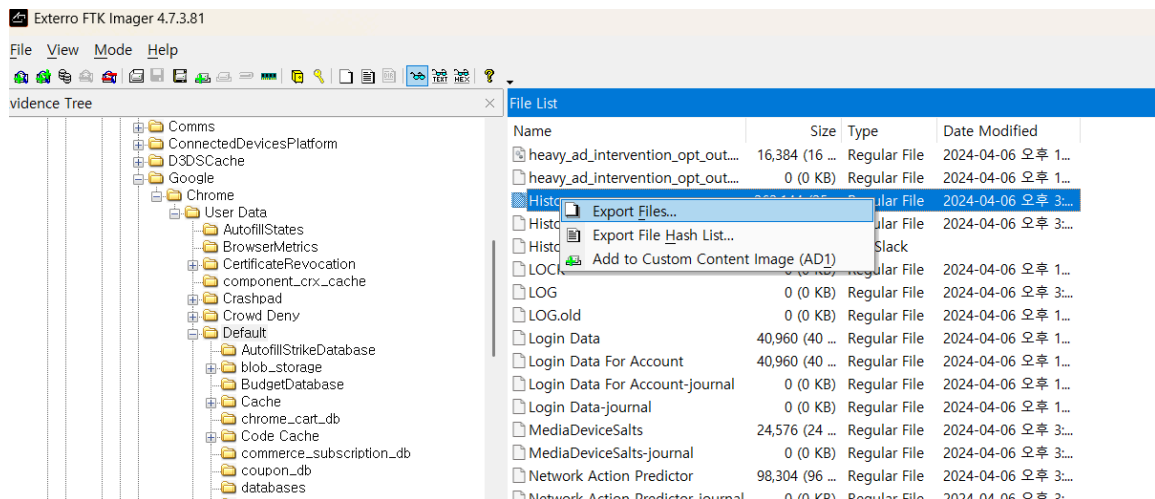
- A: 파일의 이름 (경로 제외, 확장자 제외)
- B: 파일 다운로드를 시작한 시간 (Unix Timestamp, seconds 단위)
- C: 파일의 MIME type 예를 들어 A가

dream , B가 **1712154549** , 그리고 C가 **text/plain** 이라면 FLAG 는 **DH{dream_1712154549_text/plain}** 입니다.

- 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 FLAG 는 **DH{dream_1712154549_text/plain}** 입니다.

1. 크롬의 아티팩트 기본 경로인 아래 경로 접속

C:\Users\victim\AppData\Local\Google\Chrome\User Data\Default\History



2. DB Browser for SQLite를 통해 다운로드 기록 확인

target_path	start_time	reci
	필터	필터
is\Chrome-Logo-2014.png	13356890126521330	
	13356890160260093	
is\Dtafalonso-Android-L-Chrome.ico	13356890201309017	

3. DH 값 확인

축하합니다!

1 LEVEL 1 chrome_artifacts 문제를 해결했습니다.

대단해요. 문제를 어떻게 해결하셨나요?
풀이를 작성하면 포인트까지 받을 수 있어요.