**251 – Find the suspect**

|  |
| --- |
| **Team Information** |

**Team Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Team Member \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Email Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |
| --- |
| **Instructions** |

**Description** Investigators impound a MacBook believed to have been used in the crime at the crime scene. However, it is difficult to solve the case because the suspect of the crime is not specified. Analyze the evidence file to identity of the criminal.

|  |  |
| --- | --- |
| Target | Hash (MD5) |
| Users.zip | 56E3072B8D12D449B57E47A90BB35CAF |

**Questions**

1. Find all files that appear to be related to the crime, and identify the file name and upload or download time (UTC+9) (20 points)
2. Identify suspect's name and email address. (80 points)
3. Submit the tool to decrypt the dbx. (150 points)

Teams must:

* Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
* Specify all tools used in deriving the conclusion(s).

|  |
| --- |
| **Tools used:** |

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | Publisher**:** |  |
| Version: |  | | |
| URL: |  | | |

|  |
| --- |
| **Step-by-step methodology:** |

1. Find all files that appear to be related to the crime, and identify the file name and upload or download time (UTC+9) (20 points)

Users\dfc2023\.dropbox\instance1로 들어간다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

3개의 DB가 존재한다. 각각의 특징을 서술해보았다.

avatarache: 채팅 애플리케이션, 소셜 미디어 플랫폼, 이메일 혹은 게임 클라이언트 등 사용자 아바타 정보를 캐시하는데 사용되는 데이터베이스 파일이다.

preview\_cache: 애플리케이션에서 미리보기 이미지를 캐시하는데 사용되는 데이터베이스 파일이다. 문서, 사진, 비디오 등의 미리보기 이미지를 저장하여 애플리케이션이 더 빠르게 미리보기를 로드할 수 있도록 돕는다.

sync\_history: 모바일 기기 혹은 데스크탑 환경에서 동기화 서비스와 관련된 데이터를 저장하는 SQLite 데이터베이스 파일이다. 다양한 애플리케이션에서 동기화 기록, 상태, 메타데이터 등을 저장하기 위해 사용될 수 있다.

문제가 범죄와 관련된 파일 이름과 업로드/다운로드 시간을 찾는 것이므로 sync\_history.db에 접근해보았다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

DB Browser SQLite에 파일을 업로드하고 데이터 보기를 클릭하면 문제와 관련된 정보를 얻을 수 있다.

|  |  |  |  |
| --- | --- | --- | --- |
| download | 입금주소(XMR).txt | 1681081949 | 2023-04-09 23:12:29.0000000 Z |
| download | 1월\_메스암페타민\_판매\_장부.xlsx | 1681081949 | 2023-04-09 23:12:29.0000000 Z |
| download | 1월\_대마\_판매\_장부.xlsx | 1681081949 | 2023-04-09 23:12:29.0000000 Z |
| download | 고객\_정보.xlsx | 1681081949 | 2023-04-09 23:12:29.0000000 Z |
| upload | 메스암페타민\_샘플용.jpg | 1676623739 | 2023-02-17 08:48:59.0000000 Z |
| upload | 던지기장소2.png | 1676622947 | 2023-02-17 08:35:47.0000000 Z |
| upload | 던지기장소1.png | 1676622938 | 2023-02-17 08:35:38.0000000 Z |

2. Identify suspect's name and email address. (80 points)

3. Submit the tool to decrypt the dbx. (150 points)

**The deadline for this problem is June 30.**

**Please do not post your write-up before the deadline for fair competition!**

**\* Delete this box when submitting your answer.**