




작성자	김경민
분석 일자	2024.05.21
작성 일자	2024.05.25
분석 대상	102.ad1
문서 버전	1.0
작성자 E-mail	rlarudals877@gamil.com

0. 목차

- 1. 문제3
- 2. 분석 도구3
- 3. 환경3
- 4. Write-Up.....4
- 5. Flag.....5
- 6. 별도 첨부6
- 7. Reference7



1. 문제

URL	
문제 내용	<p>As a forensic expert, you must identify all graphics in the target image.</p> <p>Find all visual images and fill out the 102.csv.</p>
문제 파일	<div> 102ad1.zip</div>
문제 유형	디스크 포렌식
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version
Python	https://www.python.org/downloads/	3.12.0
DB Browser for SQLite	https://sqlitebrowser.org/	3.12.2
FTK Imager	https://accessdata.com/product-download	4.7

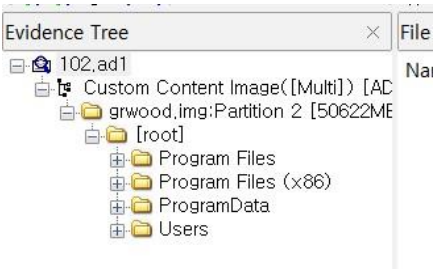
3. 환경

OS
Window 11 64-bit

4. Write-Up

파일명	102.ad1
용량	1,884,884 KB
SHA256	996d4a53947afe89c202af0887bf3ad3
Timestamp	2021-05-25 15:17:24

1. 제공받은 이미지 파일 내부를 확인해보았다.



[사진 1] .ad1 내부 확인

2. 문제에서 제공한 디스크 이미지의 내부를 확인한 결과, Windows 운영체제에 대한 파일 일부가 (Program Files) 덤프 되어 있었다.



[사진 2] 덤프된 파일

5. Flag

6. 별도 첨부

7. Reference

- [URL]