



작성자	류나연
분석 일자	2024.05.28-30
작성 일자	2024.05.31
분석 대상	Windows11.dd.zip
문서 버전	1.0
작성자 E-mail	01star01ek@gmail.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>[번역본] (*원본 영문 문제는 별도 첨부에 작성되어 있음)</p> <p>경찰은 Z 우주의 새로운 엔진의 청사진을 유출한 혐의로 브로커를 체포했습니다. 그 브로커는 이메일을 통해 약속 시간과 장소가 포함된 문서 파일(R:Blue Moon(UP.pptx)에 대한 정보를 전달했다고 진술했습니다. 그 경찰관은 디지털 포렌식 분석을 위해 연구원의 컴퓨터를 압수했습니다.</p> <p># 시스템의 시간대를 기준으로 모든 문제를 해결해 주시기 바랍니다. # 영어 이외의 다른 언어로 된 데이터는 문제 해결과 관련이 없습니다.</p> <p>1) 연구자가 브로커로부터 받은 문서파일의 SHA1 해시값은? (20점) 2) 연구원이 브로커에게 받은 파일의 비밀번호는? (150점) 3) 연구자는 문서파일의 비밀번호가 포함된 이메일을 언제 읽었습니까? (UTC+9) (80점) 4) 연구원이 중개인을 만나기로 한 장소의 GPS 정보는? (50점)</p>
문제 파일	 Windows11.dd.zip
문제 유형	Disk forensic
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version

3. 환경

OS
Windows 11 Home

4. Write-Up

파일명	Windows11.dd.zip
용량	3.36GB
SHA256	13cab83a22fab571a6c8c102741a1b8e0a95a5334203bb91f0256992a966d424
Timestamp	2024-05-22 10:04:08

1. 압축을 해제하려니 200GB 파일을 열수가 없어서 막혔다.

주문 상품	외장HDD 1TB SLIM	
배송 정보	류나연	01030960288
할인 혜택	-27,000 원	
포인트 사용	1,291 P	
결제 정보	삼성페이 결제	106,709원

현재 배송중이다!

5. Flag

[작성 방법]

- 1. 문제의 Flag가 확인되는 내용을 [4. Write-Up]에 이어 작성한다.
- 2. 작성 규칙은 [4. Write-Up]과 같다.
- 3. 제출 시 해당 [작성 방법] 텍스트 상자를 삭제해야 한다.

6. 별도 첨부

- 원본 영문 문제

Description Police arrested a broker for leaking blueprints of Space Z's new engine. The broker stated that he passed on information about a document file (**R:Blue Moon(UP).pptx**) that includes the appointment time and place through e-mail. The officer confiscated the researcher's computer for digital forensic analysis.

Target	Hash (MD5)
Windows11.dd.zip	68b05a9c173c9d8d8ea679cbcca3df67

Questions

- # Please solve all problems based on the time zone of the system.
 - # Data in any language other than English is not relevant to problem-solving.
- 1) What is the SHA1 hash value of a document file that the researcher received from the broker? (20 points)
 - 2) What is the password of the file that the researcher received from the broker? (150 points)
 - 3) When did the researcher read the e-mail containing the password of the document file? (UTC+9) (80 points)
 - 4) What is the GPS information of the place where the researcher is supposed to meet the broker? (50 points)

7. Reference

- [URL]