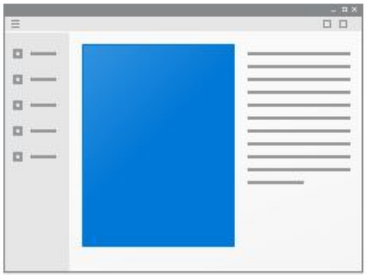
2024 암호분석경진대회

3번 문제

암호 포렌식은 디지털포렌식의 한 분야로 디지털 데이터와 시스템에서 암호화된 정보를 분석하고 복구하는 프로세스를 의미한다. 여기에는 암호화된 데이터를 해독하고, 암호 관련 문제를 해결하기 위해 디지털 증거 수집, 프로그램 분석, 복구 기술 시도 등의 다양한 과정이 포함된다.

Q. 한 회사에서 주요 정보가 유출되는 정황이 발견되어 수사가 시작되었다. 유력한 용의자 A씨의 PC를 분석해본 결과 최근 삭제된 응용프로그램과 이미지 파일을 각각 하나씩 획득할 수 있었다. 정황상 cryptocontest.exe는 c_contest_2024.jpg를 암호화하는 프로그램으로 보인다. 해당 프로그램에 역공학을 수행하여 c_contest_2024_out.jpg 파일의 원본을 획득하시오. 그리고 원본 획득이 가능하였던 이유를 상세히 설명하시오.

c_contest_2024_out.jpg



cryptocontest.exe

주의사항 및 힌트

1) cryptocontest.exe 파일은 c_contest_2024.jpg 파일이 같은 경로에 존재하는 경우에만 실행할 수 있다.

2) cryptocontest.exe 파일 내에는 Cryptographically Secure Pseudo-Random Number Generator(ChaCha20 활용)가 한 번 이상 사용된다.

3) 역공학 도구는 x64dbg, IDA, Ghidra 등을 모두 허용한다. 단, 사용한 도구는 모두 보고서에 기재하여야 한다.

4) 원본 데이터 획득 방식은 코드 재현, 코드 패치 등 모든 방식을 허용한다. 단, 사용한 방식을 모두 보고서에 기재하여야 한다.

5) 결과물은 다음 2종 이상을 포함해야 한다. (이 외 결과물은 함께 업로드 또는 보고서에 기재해도 된다.)
- 복호화된 원본 이미지
- 문서

6) 평가방법은 다음과 같다.
- 암호기(암호화 프로그램) 구조 파악(40점, 절대평가)
- 암호키 재현 방법 파악(20점, 절대평가)
- 데이터 복호화(20점, 복호화를 위한 쿼리 횟수에 따른 절대평가)
- 결과 문서화(20점, 절대평가)