



2022 국민대학교 정보보안암호수학과 학술동아리 주관 경진대회

4번 문제 - 디지털 포렌식 (출제: 동아리 FaS)

[시나리오]

정보보안암호수학과 학부생 A는 메일로 온 'FaS 동아리 가입 신청서.zip' 파일 압축을 풀고 다음 그림과 같이 FaS 동아리에 가입하기 위해 한글 파일을 열었다.

 FaS 동아리 가입 신청서.hwp	...	2022-10-17 오후 1...	응용 프로그램
 FaS 동아리 가입 신청서.zip		2022-10-17 오후 1...	압축(ZIP) 파일

한글 파일을 연 순간 학부생 A가 사용하고 있는 PC에 랜섬웨어가 감염되면서 모든 파일이 암호화되었다. 가입 신청서 한글 파일을 다시 확인해보니 실행파일이었으며, hwp 파일로 위장한 랜섬웨어 실행파일이었다.

 FaS 동아리 가입 신청서.hwp		.exe	2022-10-17 오후 1...	응용 프로그램
--	---	------	--------------------	---------

학부생 A는 감염된 PC를 복구하기 위해 해당 랜섬웨어 복구툴이 담긴 USB를 연결하였다. USB를 꽂자 USB 전체가 또한 감염되었고, 학부생 A는 급한 대로 USB 전체를 덤프 뜬 이미지를 국민대학교 정보보안암호수학과 포렌식 수사관에게 전달하였다.

전달받은 이미지에서 감염시킨 실행파일을 추출하여 해당 파일을 분석하시오. 분석한 내용은 다음 문제에 따라 순차적으로 풀이과정을 작성하여 보고서 형식으로 제출하시오.

[문제]

1. 덤프 뜬 'FaS_USB.img' 이미지에서 모든 파일을 추출하시오 (5점)
2. 추출한 모든 파일이 각각 몇 번째 섹터에 있는지 풀이과정을 상세히 작성하시오 (20점)
3. 감염된 파일의 감염시간을 초 단위까지 작성하시오 (10점)
4. 실행파일이 어떠한 방식으로 암호화하였는지 사용 알고리즘과 분석 과정을 상세히 작성하시오 (30점)
5. 분석한 내용을 바탕으로 복호툴을 만들어 암호화된 모든 파일을 복호화하고, 제작한 복호툴의 과정을 상세히 설명하시오 (30점)
6. 복호화한 파일들과 문제의 정답들을 zip으로 압축하여 다음 email로 보내세요 (5점)

email : sae61597@naver.com (문제 관련 문의도 해당 이메일로 보내주세요.)

[검색어 hint]

무료 디버깅 프로그램, HxD에서 디스크 이미지로 열기(2번 문제)

[참고]

덤프 뜯은 이미지 내에 있는 분석 대상인 실행파일은 실행시켜도 아무 이상 없습니다.

(문제 제작용으로 만든 실행 파일이라 백신 경고문 메시지가 뜰 수 있지만, 입력된 파일만 암호화 하기 때문에 PC에 영향은 없으니 참고해주세요.)

(-> 실행파일을 통해 파일 암호화 가능하며, 암호화된 파일 구조 파악 가능)