분석 보고서

사이버보안학과 10170546 김유진 10170890 정선영

# 개요

납치된 아이(채영)의 위치가 범인의 컴퓨터에 저장되어 있다는 사실을 알아내어 범인의 컴퓨터에서 수집한 레지스트리 파일을 분석함으로써 잠겨진 파일을 풀어내, 아이(채영)의 위치를 찾아 내야한다.

# 사용한 TOOL 및 SITE

## REGA Registry Analyzer (1.5.2.2)

## HxD Hex Editor (2.1.0.0)

## Base64 DCODING SITE (<https://www.base64decode.org/>)

* FILE SIGNATURE (<https://www.garykessler.net/library/file_sigs.html>)

# 분석 자료

# 스크린샷이(가) 표시된 사진 자동 생성된 설명

## 납치계획.zip : 레지스트리 파일에서 찾아낸 암호를 입력하면 풀 수 있음

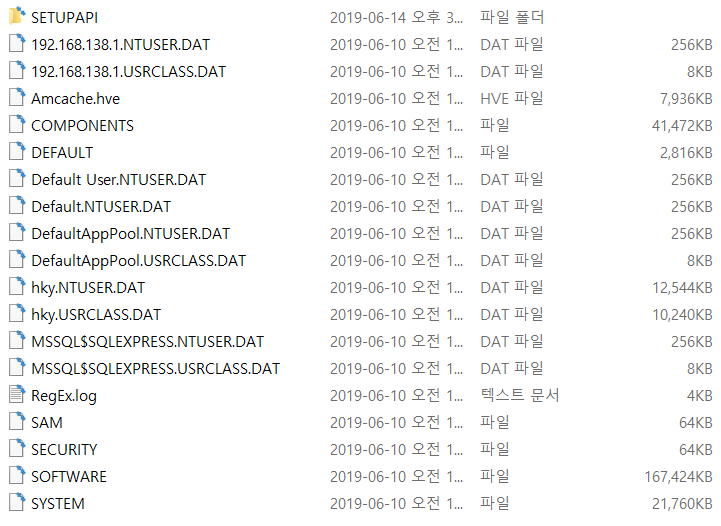
## 디지털 포렌식 문제.pdf : 문제가 적혀 있는 pdf 파일

## 범인 컴퓨터.zip : 범인 컴퓨터에서 수집한 레지스트리 파일

# 분석 과정

# 스크린샷이(가) 표시된 사진 자동 생성된 설명

납치계획.zip 파일은 암호가 걸려져 있는 상황.



범인 컴퓨터.zip 파일의 압축을 푸니 범인 컴퓨터에서 수집한 레지스트리 파일이 들어있었다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

REGA를 사용해 범인 컴퓨터에서 수집한 레지스트리 분석을 한다.

***분석 결과, 이상한 점을 하나 발견했다.***

스크린샷이(가) 표시된 사진

자동 생성된 설명

사용자 계정 정보를 분석해보면 로그인 횟수가 가장 많은 default 계정은 **‘hky’**라고 알 수 있다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

하지만 열어본 페이지 목록의 계정명을 보면 ‘192’로 default 계정이 아닌 걸 확인할 수 있다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

그래서 위에서 찾아낸 default 계정인 **‘hky’**으로 바꿔주었다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

열어본 페이지 목록에서 수상해보이는 URL을 하나 발견했다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

찾은 URL로 들어가보자 범인의 블로그로 추정되는 사이트가 나왔고, 거기서 암호로 보이는 단어를 발견했다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

찾은 암호를 입력하자 잠금이 해제됐다.

동물, 포유류이(가) 표시된 사진

자동 생성된 설명

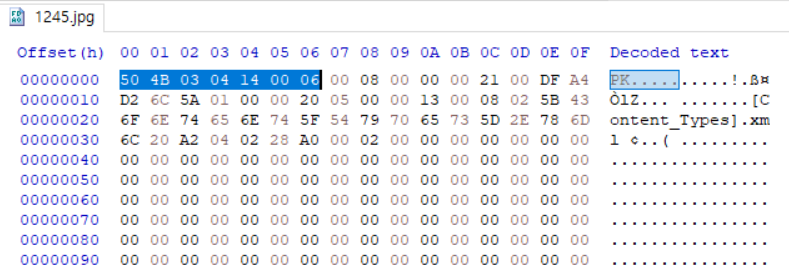
찾은 범인의 납치 계획서.

스크린샷이(가) 표시된 사진

자동 생성된 설명

1245.jpg 라는 이미지 파일을 찾아서 열어보았지만, 열리지 않았다.

그래서 우리는 이 파일의 확장자가 바뀌었음을 추측하고 HxD를 사용해 확인해보았다.

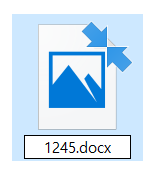


앞의 ***’50 4B 03 04 14 00 06’***을 사용해 파일 시그니쳐를 찾아보았다.

개체이(가) 표시된 사진

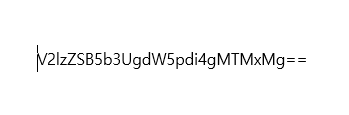
자동 생성된 설명

찾아본 결과, 1245.jpg 파일은 사실은 1245.docx 파일이었다는 사실을 알게 되었다.

 스크린샷이(가) 표시된 사진

자동 생성된 설명

1245.jpg 파일의 확장자를 1245.docx로 바꿔보았다.



파일을 열어보자 인코딩 되어 있는 문장을 발견할 수 있었다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

우리는 base64 디코딩 사이트로 들어가 발견한 문장을 디코딩 해보았다.



디코딩 하자 ‘Wise you univ. 1312’라는 문장이 나왔다.

***이로써 우리는 아이가 납치된 장소가 영산대학교 1312호 강의실이라는 사실을 알게 되었다.***

# 분석 결과 및 요약

범인의 컴퓨터 레지스트리 파일 분석으로 알아낸 암호로 잠긴 파일을 엶.

그 안에서 범인의 계획과 암호화된 아이의 위치를 알아냄.

암호화된 문장을 복호화하여 아이가 납치된 정확한 장소를 알아냄.

# 분석 후기

처음 문제를 받았을 땐, 레지스트리 분석만 하면 쉽게 풀릴 것 같아서 어렵게 생각하지 않고 시작했었는데, 막상 레지스트리 분석이 끝나고 나니 어디서부터 어떻게 분석을 해야할지 많이 헤맸다.

열어본 페이지 목록에서 블로그 주소를 찾아내기까지 꽤 많은 시간이 걸렸다. 겨우 찾아낸 암호로 잠긴 파일을 풀자 여러 개의 이미지 파일과 하나의 pdf 파일, 그리고 열리지 않는 jpg 파일이 있었는데, pdf 파일 안에 너구리 사진이 너무 수상해 보여서 HxD로 사진만 따로 분리하기도 했지만 알고보니 아무 의미 없는 사진이었다.

또한, 다른 근영.jpg나 채영.jpg 파일보다 지민.jpg와 하나.jpg 파일의 용량이 두 배 가량 더 크길래 그 사진들 안에 다른 것들이 숨겨져 있을 거라 생각하고 HxD로 열심히 분석해보았으나 그 사진들 또한 아무것도 아니었다.

게다가 1245.jpg 파일도 docx 파일이라는 것은 금방 알아차렸지만, docx의 파일 시그니쳐의 시작과 끝이 여러 번 반복되길래 그 파일안에 docx 파일이 여러 개 있을 줄 알았지만 알고보니 그것도 그냥 확장자만 바꾸면 되는 문제였다.

결과적으로는 어렵지 않은 문제였지만 모든 것이 수상해보이고 의심을 해서 작은 것 하나하나 전부 분석하느라 시간이 많이 걸렸다.

# \*\*\* 이채림, 하가영 팀에게 제공한 문제 \*\*\*

텍스트이(가) 표시된 사진

자동 생성된 설명

▲ 문제

스크린샷이(가) 표시된 사진

자동 생성된 설명

▲ 분석 자료