<디지털 포렌식 A팀 발표>

-4주차 CTF 문제 풀이-

김수현 조소영 조예원 홍정민

CONTENTS

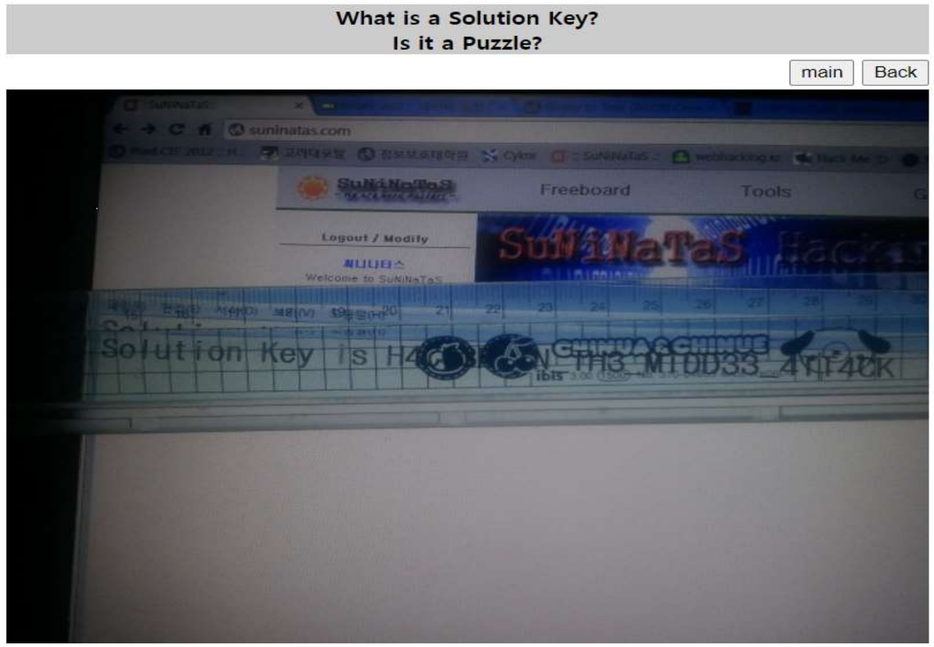
써니나타스 21번 문제 설명

-JPG 파일 관련-

써니나타스 26번 문제 설명

-빈도 분석 관련-

<써니나타스 CTF 21번 문제 풀이>



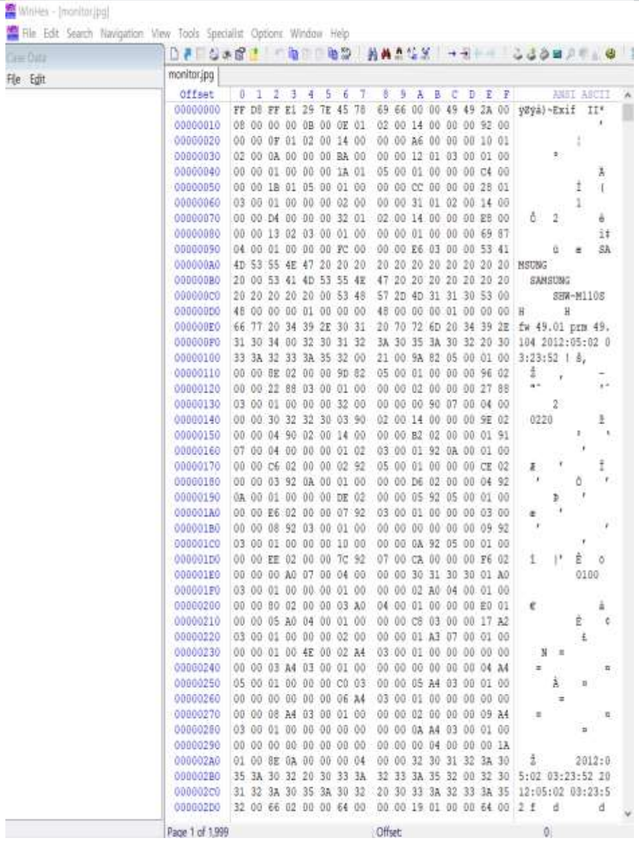
What is a Solution Key? is it a Puzzle? 이라는 지문과 함께 한 장의 사진이 기재되어 있음!

사진을 다운로드 후 살펴보도록...!!

<써니나타스 CTF 21번 문제 풀이>

여러장의 사진파일을 한장의 파일로 겹쳐 편집을 시도할 수도있다는 추측 가능

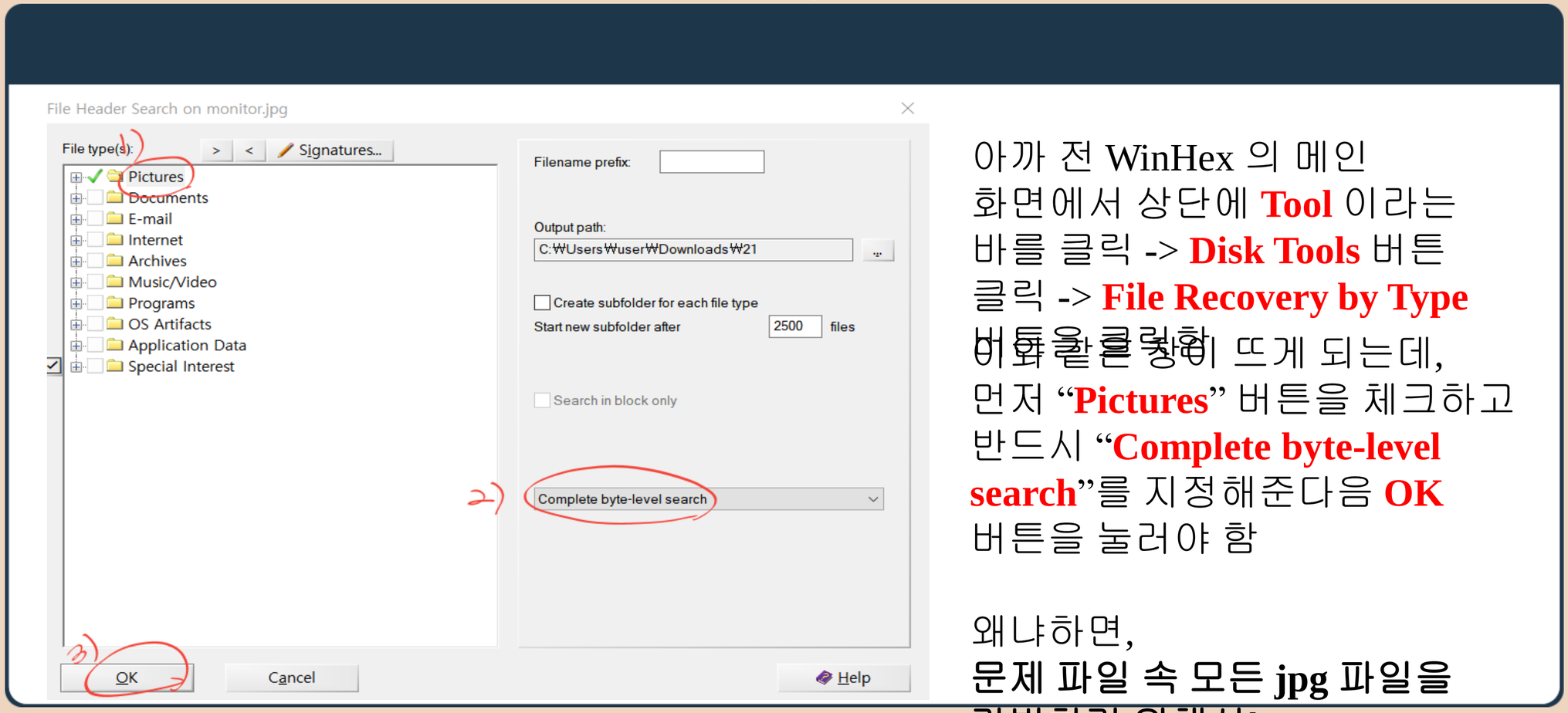
사진을 다운로드 한 후 속성을 들어가서 보니 사진 한장의 크기가 매우 큰 용량을 차지하고 있음을 확인



X-Ways hex editor 도구인 WinHex 도구를 이용하여 파일을 카빙함

의심지점!!

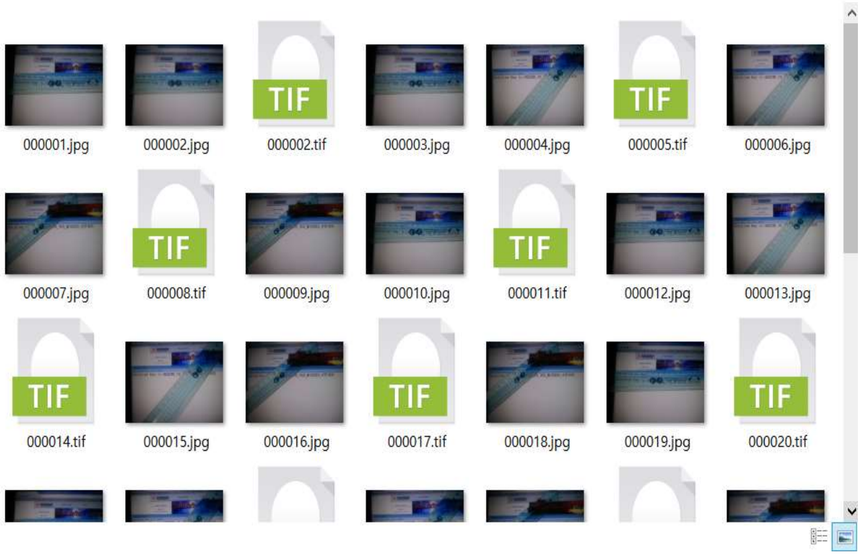
<써니나타스 CTF 21번 문제 풀이>



아까 전 WinHex 의 메인 화면에서 상단에 **Tool** 이라는 바를 클릭 -> **Disk Tools** 버튼 클릭 -> **File Recovery by Type** 버튼을 클릭하면 아래와 같은 창이 뜨게 되는데, 먼저 "**Pictures**" 버튼을 체크하고 반드시 "**Complete byte-level search**"를 지정해준다음 **OK** 버튼을 눌러야 함

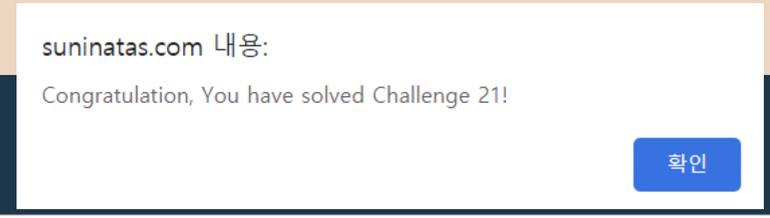
왜냐하면,
문제 파일 속 모든 jpg 파일을 카빙하기 위해서!

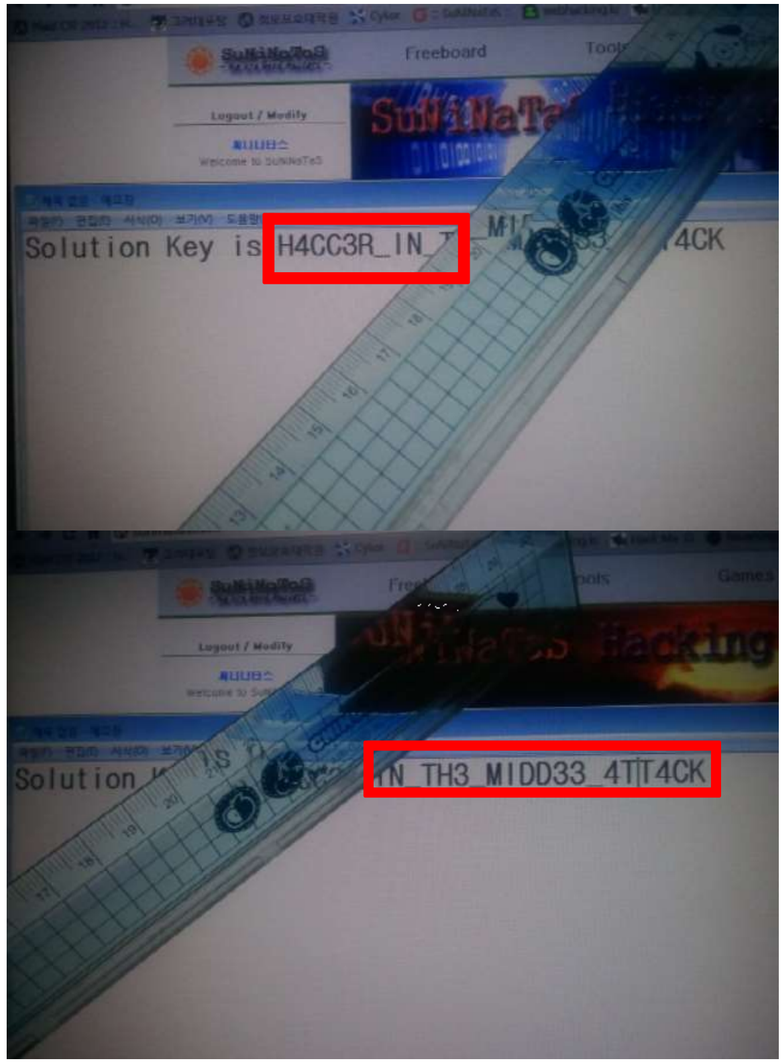
<써니나타스 CTF 21번 문제 풀이>



앞의 모든 과정을 거치면,
최종적으로 숨겨져 있던 모든 jpg 파일들을 볼 수 있음

그 중 몇 개의 사진을 찾아서





Solution Key에 대한 해답이 나와있는 것을 확인할 수 있음!!!!

Authkey는 “**H4CC3R_IN_TH3_MIDD33_4TT4CK**”

<써니나타스 CTF 26번 문제 풀이>

Cipher III : Frequency analysis

main Back

This challenge is to recover the plaintext from the following ciphertext using frequency analysis:

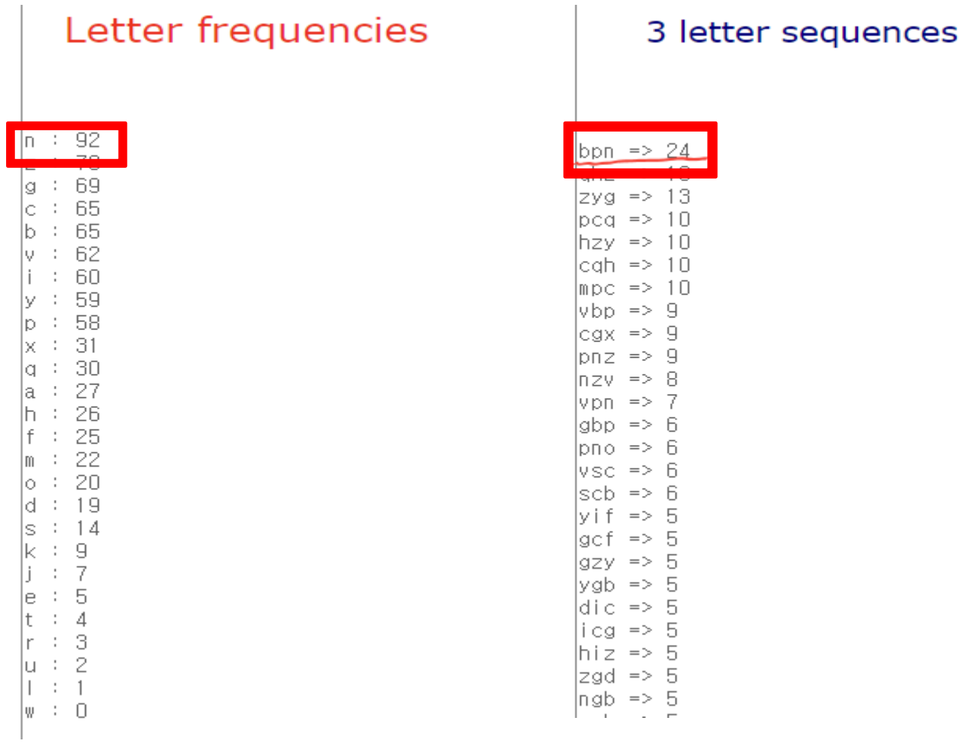
szqkagczvcvyabpsyincgozdainvscbnivpnzvbpnyfkqhzmmpcqhzygzgfcxznvvzgdfnvbpnjyifxmpcqhzygbpnoyaimy
gbzgngbvmpcqhzygcbpinnbzqndicgxhiztozgcfmpcqhzygbpnjyifxeagzyimpcqhzygbpneagzyidicgxhiztozgcfmpc
qhzygcgxcoyaibzqnvyabpsyincggcbzygcfmpcqhzygszqzvbpnozivbvyabpsyincgozdainvscbnibyjzgcqnxcfcbcgzva
eagzyiyivngzyidicgxhiztnungbzvampcqhzygvpzhcgxbpnyfkqhzmdcqnvvpnzvbpnozivbonqcfnvscbnibyjzgbpnyfk
qhzmdcqnvbpnjyifxmpcqhzygvpzhvbpnoyaimygbzgngbvmpcqhzygvpzhvcgxbpndicgxhiztozgcfvpnzvygnyobpn
qyvbpzdpfkinmydgzlnxcbpfnbnvcgxqnxzcozdainvzgvyabpsyinccvyochizfbpzvkncivpnzvicgsnxvnmygxzgbpnjyifx
rkbpnzgbnigcbzygcfvscbzgdagzygvpnzvbpnmaiingbinmyixpyfxnioyifcxznvzgbpnvpyibhiydicqbpnoinnvscbzgdc
gxbpnmyqrzgnxbybcfagxnibpnzvaeaxdzgdvkvbnqvpnzvcfvybpnozivbonqcfnvscbnibyvaihcvvbpnbjypaxincxhyzg
bqcisagxnibpnzvaeaxdzgdvkvbnqvpnpcvgnunirnnghfcmnxyoobpnhyxzaqzgpningbzinmcinni

Note that we have omitted the blank letters and punctuation marks of the plaintext.

딱 보기에도 눈이 아픈 암호문이 있음

빈도분석을 통해 **복호화**를 해야 하는 문제!

<써니나타스 CTF 26번 문제 풀이>



http://www.richkni.co.uk/php/crypta/freq.php

위의 사이트에 접속하면
알파벳의 빈도를
분석해주는 것을 해줄
수 있음

하지만, 이와 같은
과정으로는 힌트를 얻을
수 없었음

<써니나타스 CTF 26번 문제 풀이

https://quipqiup.com/

위의 사이트에 다시 접속해서 암호문을 복호화 해줬음

그 결과, Kim yuna(김연아)와 관련된 설명으로 해석된 것을 볼 수 있음

따라서 Authkey는 "**Kimyuna**"

<JPG 파일>

JPEG(Joint Photographic Experts Group)은 사진 이미지를 위해 개발된 형식으로 손실 압축 기법을 사용하며
JPEG로 된 파일은 JFIF(JPEG File Interchange Format)로 저장되는데, 이의 확장자로 JPG 또는 JPEG를 사용함.

손실 압축으로 압축률을 높일 경우 이미지의 상태가 떨어지는 단점이 있음. 그러나 일반 그래픽 프로그램에서 저장

<암호학에서 빈도분석이란?>

평문과 암호문에 사용되는 문자 또는 문자열의 출현빈도를 단서로 이용하는 암호해독법을 말함.
(출처: 위키백과)

문자의 출현빈도에 따라서 단어 또는 언어가 바뀌는 그런 것.

빈도분석을 자동으로 해주는 사이트를 이용할 수 있음.

감사합니다

~ THANK YOU ~