

<디지털 포렌식 A팀 발표> -4주차CTF문제 풀이-

김수현 조소영 조예원 홍정민

CONTENTS



써니나타
스 21번
문제 설명

-JPG 파일
관련-

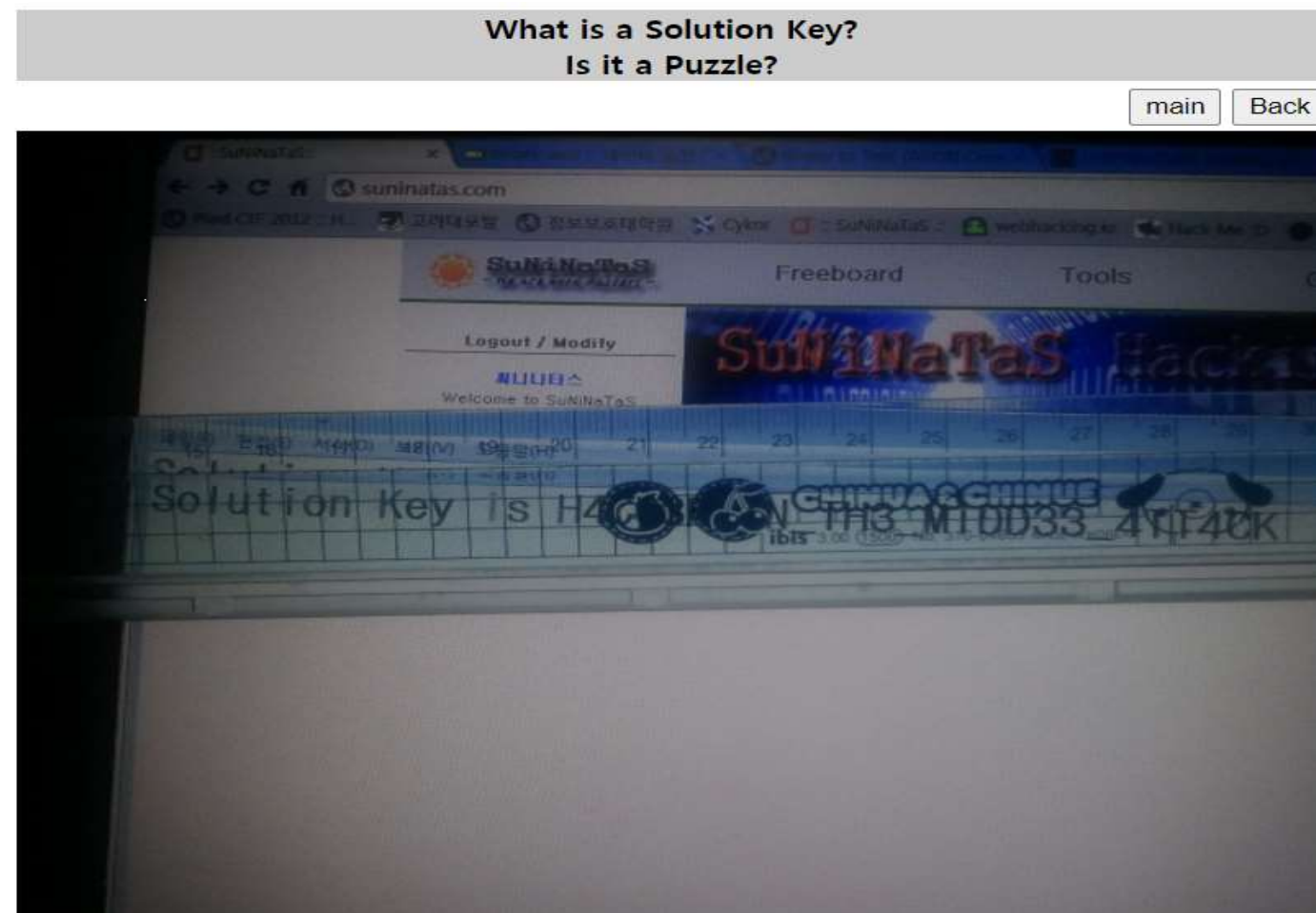


써니나타스
26번 문제
설명

-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...!!

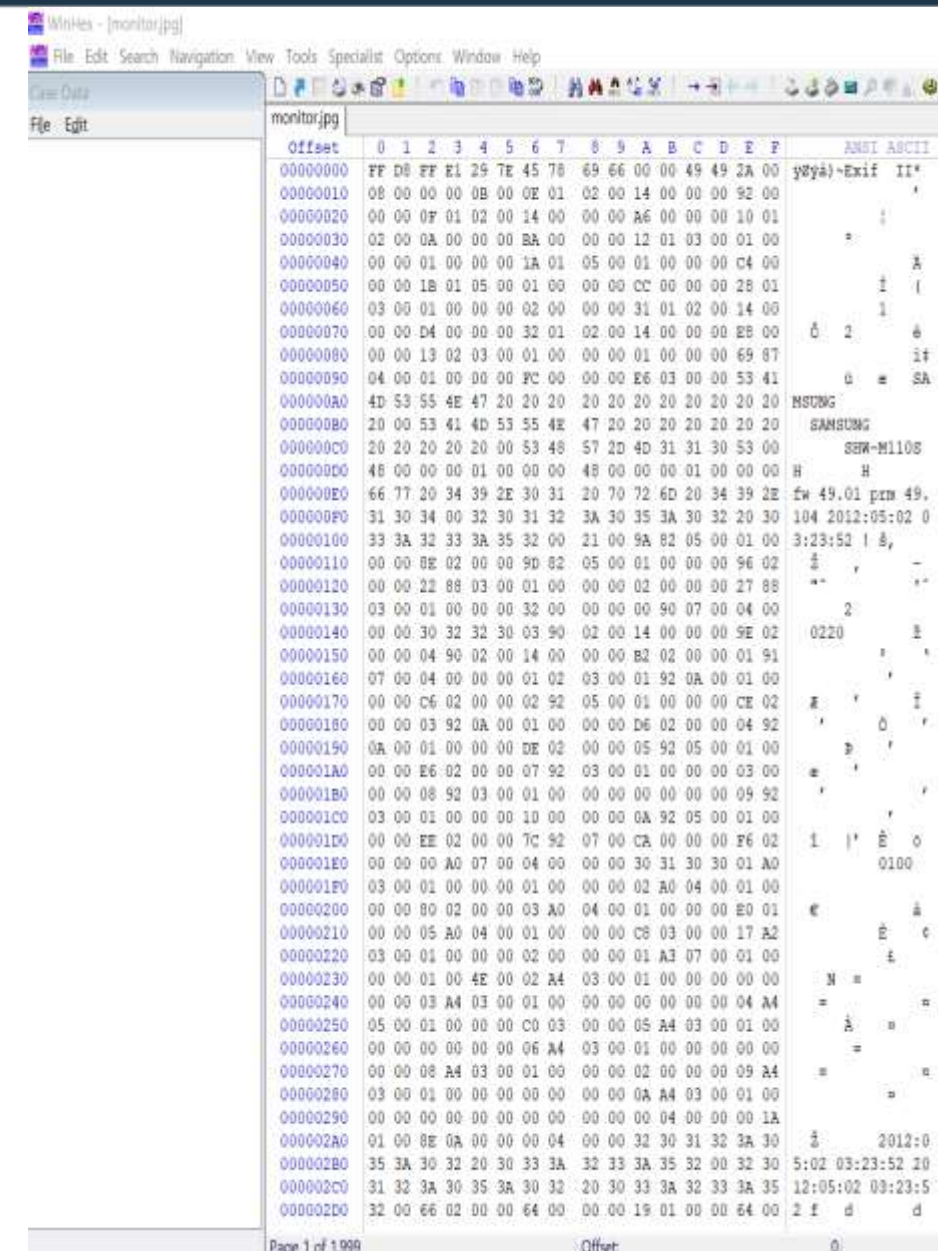
<써니나타스 CTF 21번 문제 풀이>

여러장의
사진파일을 한장의
파일로 겹쳐

편집을 시도할
수도 있다는 추측
가능

파일 형식: 알씨 JPG 파일(.jpg)
연결 프로그램: ALSee (데스크톱) 변경(C)...
위치: C:\Users\Wuser\Desktop
크기: 1.40MB (1,470,667 바이트)
디스크 할당 크기: 1.40MB (1,474,560 바이트)
만든 날짜: 2020년 10월 1일 목요일, 오후 1:23:02
수정한 날짜: 2020년 10월 1일 목요일, 오후 1:23:03
액세스한 날짜: 2020년 10월 1일 오늘, 오후 1:23:03
특성: ☐ 읽기 전용(R) ☐ 숨김(H) 고급(D)...
보안: 이 파일은 다른 컴퓨터로부터 왔으며 사용자의 컴퓨터를 보호하기 위해 차단되었습니다. ☐ 차단 해제(K)
확인 취소 적용(A)

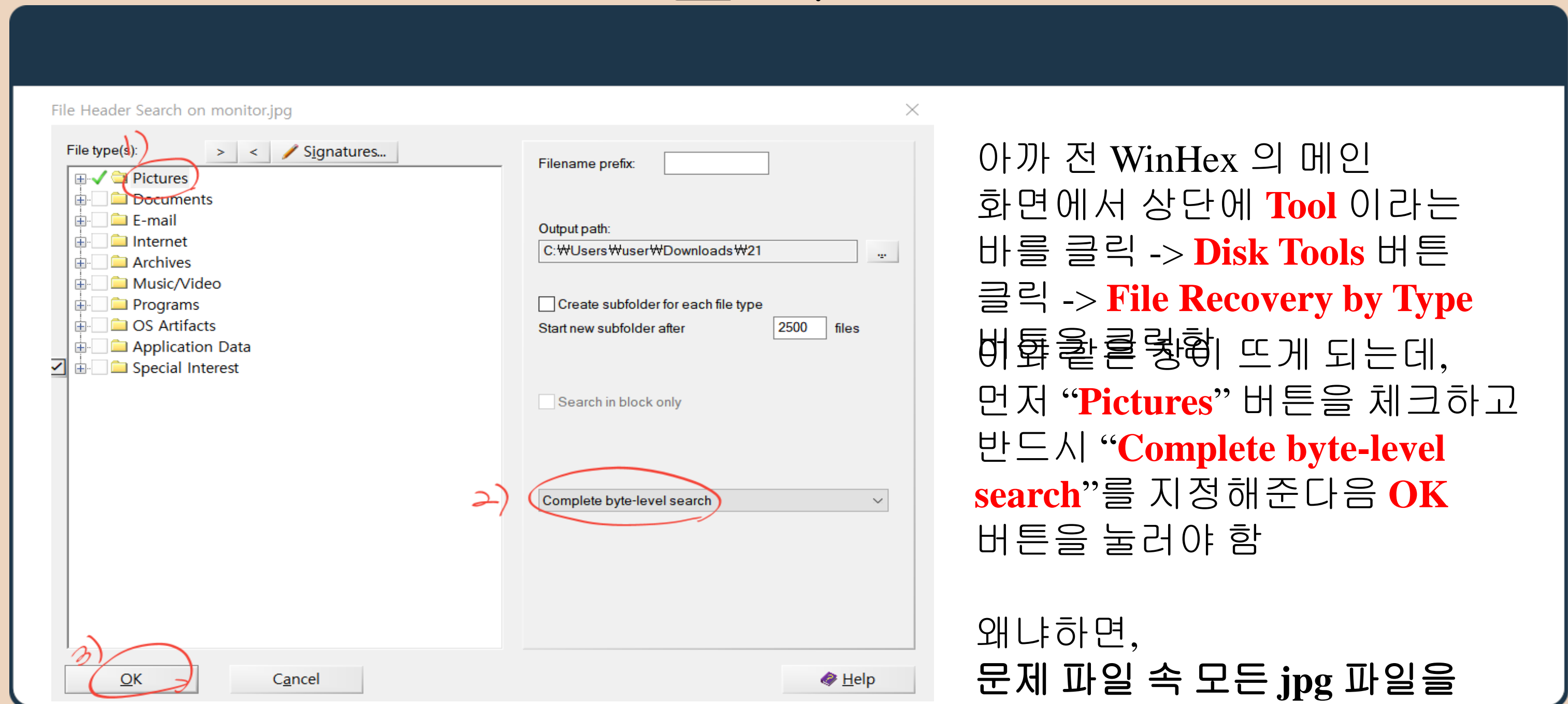
사진을
다운로드 한 후
속성을
들어가서 보니
사진 한장의
크기가 매우 큰
용량을
차지하고
있음을 확인



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 뜨게 되는데, 먼저 “**Pictures**” 버튼을 체크하고 반드시 “**Complete byte-level search**”를 지정해준다음 **OK** 버튼을 눌러야 함

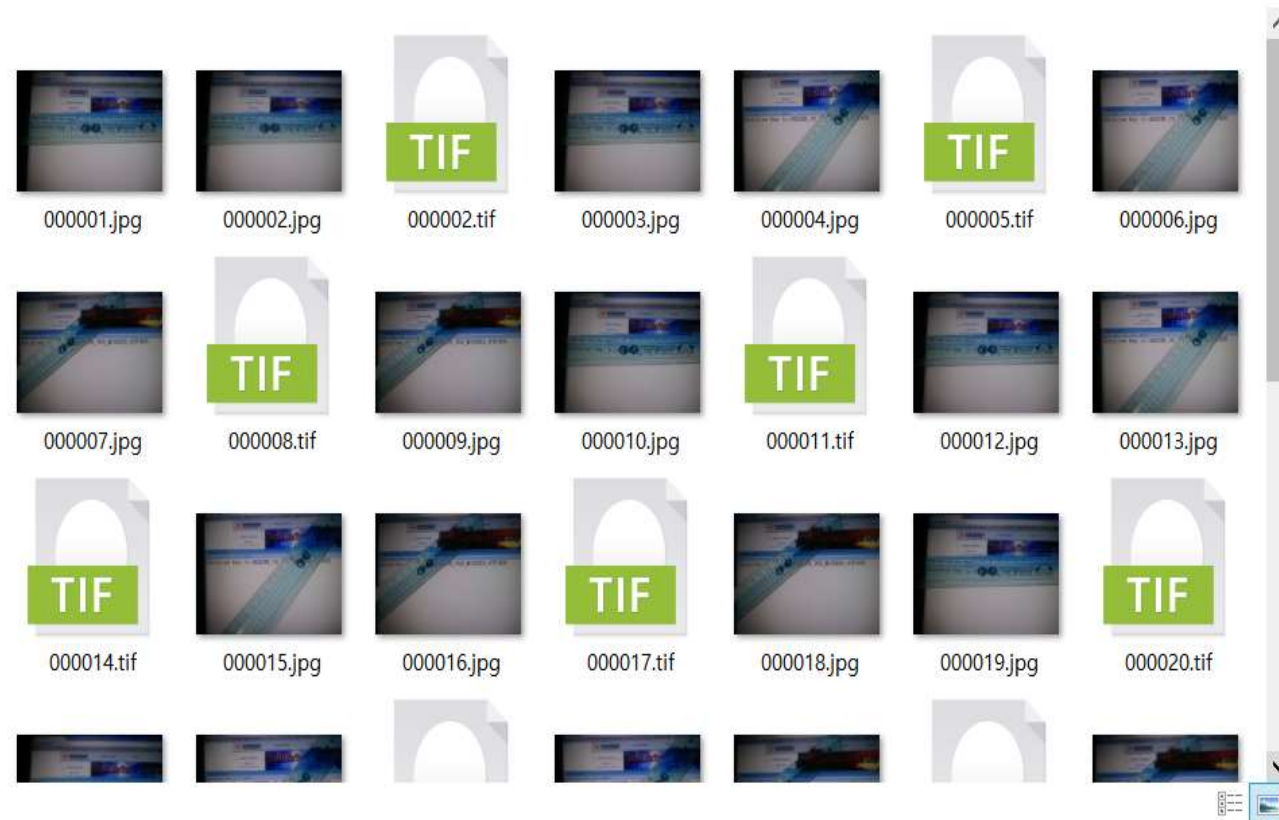
왜냐하면,
문제 파일 속 모든 jpg 파일을 카빙하기 위해서!

<써니나타스 CTF 21번 문제 풀이>

suninatas.com 내용:

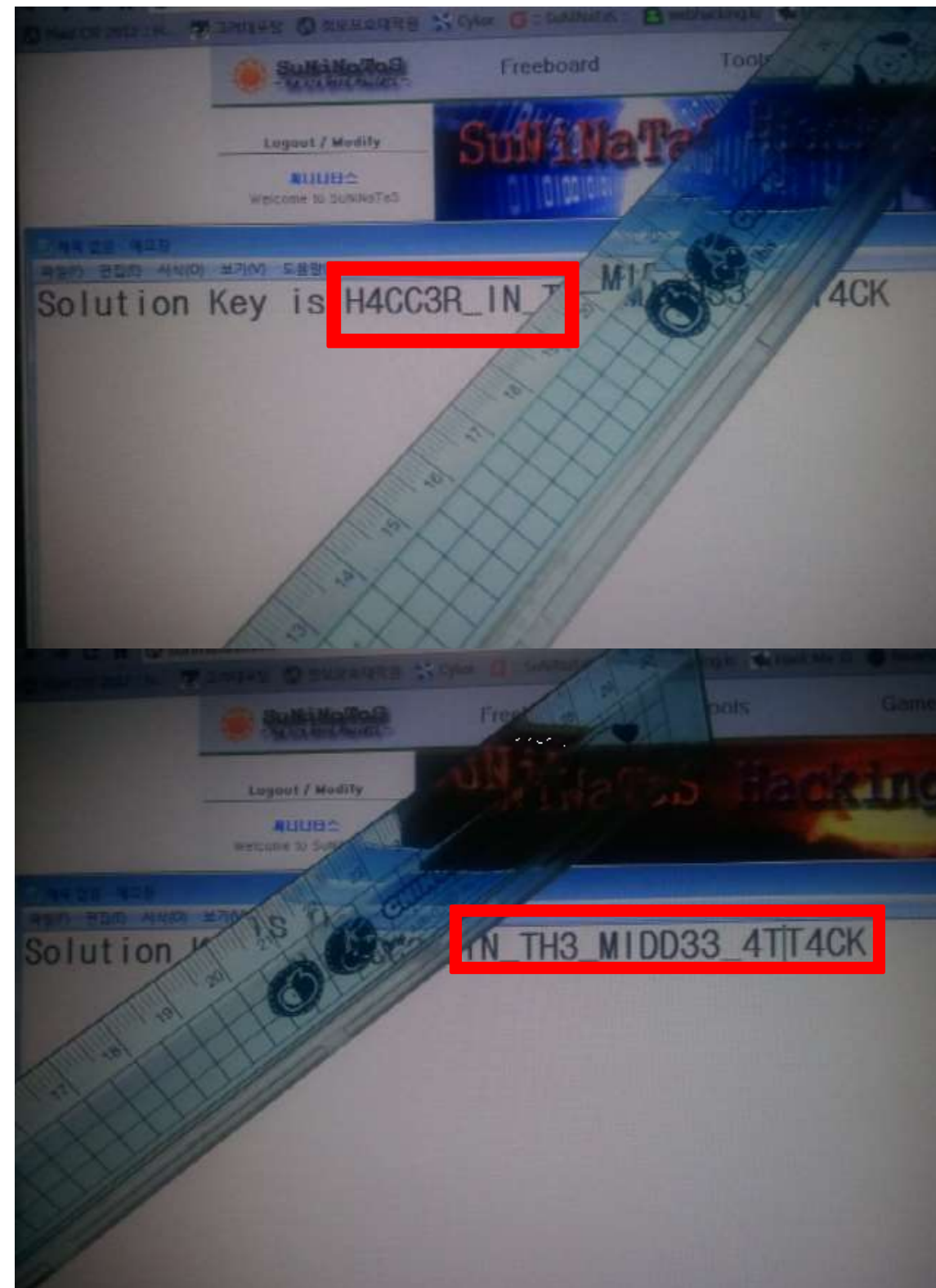
Congratulation, You have solved Challenge 21!

확인



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_MIDD3
3_4TT4CK**”

<써니나타스 CTF 26번 문제 파일>

Cipher III : Frequency analysis

[main](#) [Back](#)

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

```
szqkagczvcvyabpsyincgozdainvscbnivpnzvpnyfkqhzmmmpcqhyzgfcxznvvzgdfnvbpnjyifxmpcqhygbpnoyaimy  
gbzgngbvmmpcqhygcbpinnbzqndicgxhiztozgcfmmpcqhygbpnjyifxeagzyimpcqhygbpneagzyidicgxhiztozgcfmmpc  
qhzygcgxcoyaibzqnvyabpsyincggcbzygcfmpcqhyzgszqzvpnozibvyabpsyincgozdainvscbnibyzgcqnxcfcbcgzva  
eagzyiyivngzyidicgxhiztnungbzvampcqhygvpzhcgxbpnyfkqhzmdcqnvvpnzvpnozibonqcfvscbnibyzgpbnyfk  
qhzmdcqnvbpnjyifxmpcqhygvpzhvbpnoyaimygbzgngbvmmpcqhygvpzhvcgxbpndicgxhiztozgcfpnzvygnyobpn  
qyvpzdpfkinmydgzlnxcbpfnbvvcgxqnxzcozdainvzgyabpsyinccvyochizfbpzvkncivpnzvicgsnxvnmygxzgbnpjyifx  
rkbpnzgbnigcbzygcfvscbzgdagzygvpnzvpbnmaingbinmyixpyfxnioyifcxznvzgbpnvpyibhiydicqbpnoinnvscbzgdc  
gxbpnmyqrzgnxbybcfagxnibpnzvaeaxdzgdvkvbnqvpnzvcfybpnozibonqcfvscbnibyvaihcvbpbnpjypaxincxhyzg  
bqcisagxnibpnzvaeaxdzgdvkvbnqvpnpvcgnunirnghfcmnxyoobpnhyxzaqzgpninbzinmcinni
```

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

딱 보기에 눈이
아픈 암호문이 있음

빈도분석을 통해
복호화를 해야 하는
문제!

<써니나타스 CTF 26번 문제 풀이>

Letter frequencies

n	: 92
e	: 78
g	: 69
c	: 65
b	: 65
v	: 62
i	: 60
y	: 59
p	: 58
x	: 31
q	: 30
a	: 27
h	: 26
f	: 25
m	: 22
o	: 20
d	: 19
s	: 14
k	: 9
j	: 7
l	: 5
t	: 4
r	: 3
u	: 2
w	: 0

3 letter sequences

bpn	=> 24
zne	=> 18
zyg	=> 13
pcq	=> 10
hzy	=> 10
cqh	=> 10
mpc	=> 10
vbp	=> 9
cgx	=> 9
pnz	=> 9
nzv	=> 8
vpn	=> 7
gbp	=> 6
pno	=> 6
vsc	=> 6
scb	=> 6
yif	=> 5
gcf	=> 5
gzy	=> 5
ygb	=> 5
dic	=> 5
icg	=> 5
hiz	=> 5
zgd	=> 5
ngb	=> 5
.	=> 1

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

위의 사이트에 접속하면
알파벳의 빈도를
분석해주는 것을 해 줄
수 있음

하지만, 이와 같은
과정으로는 힌트를 얻을
수 없었음

<써니나타스 CTF 26번 문제

풀이

suninatas.com 내용:

Congratulation, You have solved Challenge 26!

확인

quipqiup

BETA

quipqiup is a fast and automated cryptogram solver by [Edwin Olson](#). It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

szqkagczvcvyabpsyingozda invscbn ivpnzvpnyfkqhzmpcqhyzgfcxznvvzgdfnvbnjyifxmpcqhyzgbpnoya imygbzgngbvmpcqhyzgcbinnbzqndicgxhiztozgcfmqchzygpnjyifxeagzyimpcqhyzgbneagzyidicgxhiztozgcfmqchzygcgcxcoyaibzqnyabpsyinggcbzygcfmqchzygszqzvpnoz ivbvyabpsyingozda invscbn iby jzgcqncfcbcgzvaeagzyiivngzyidicgxhiztnungbzvampcqhyzgvz hcgxbpnyfkqhzmdcqnvvpnzvpnoz ivbonqcfnvscbn iby jzgbpnyfkqhzmdcqnvbnjyifxmpcqhyzgvpzhvbnoya imygbzgngbvmpcqhyzgvpzhvcgxbpndicgxhiztozgcfvpnzvygnyobpnqyvpzdpfk inmydgz l nxcbpfnbnvcgxnzcozda invzgyabpsyingccvyoch izfbpzykncivpnzvicgsnxvmygzgbpnjyifxrkbpnzgbn igcbzygcfvscbzgdagzygvpnzvpbnmai ingbinmyixpyfxnioyifcxznvzgbpnvpyibhiydicqbp noinnvscbzgdcgxbpnmyqrzgnxbybcfagxn ibpnzvaeaxdzgdvkvbnqvpnzvcfyvbnnoz ivbonqcfnvscbn ibyva ihcvvbnbjypax incxhyzgbqicisagxn ibpnzvaeaxdzgdvkvbnqvpncvgnunirnnghfcmnxyoobpn hyxzaqzgpnibz inmcinni

Clues: For example G=R QVW=THE

auto

Solve

0 -1.375 (kim yuna) is south korean figure skater she is the olympic champion in ladies singles the world champion the four continents champion a three time grand prix final champion the world junior champion the junior grand prix final champion and a four time south korean national champion kim is the first south korean figure skater to win a medal at an isu junior or senior grand prix event is u championship and the olympic games she is the first female skater to win the olympic games the world championships the four continents championships and the grand prix finals he is one of the most highly recognized athletes and media figures in south korea as of april this years he is ranked second in the world by the international skating union she is the current record holder for ladies in the short program the free skating and the combined total under the isu judging systems he is also the first female skater to surpass the two hud read point mark under the isu judging systems he has never been placed off the podium in her entire career

<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 ~