HELLO.

HELLO.

scpCTF{hello}

Problem

2020.10.06

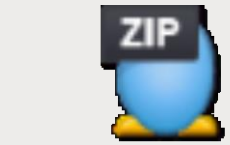
INDEX.

TITLE

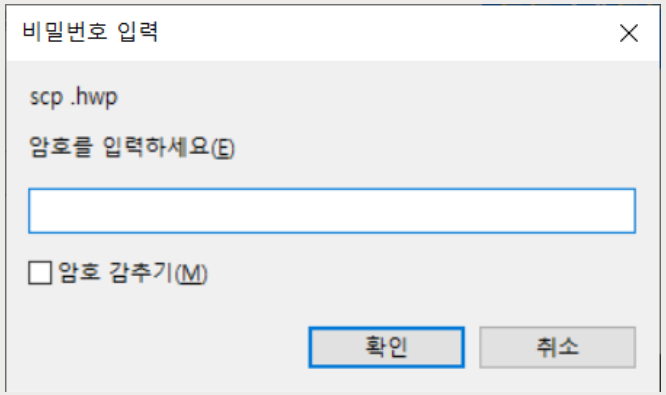

1
Fake pwd

Fake pwd

Forensic



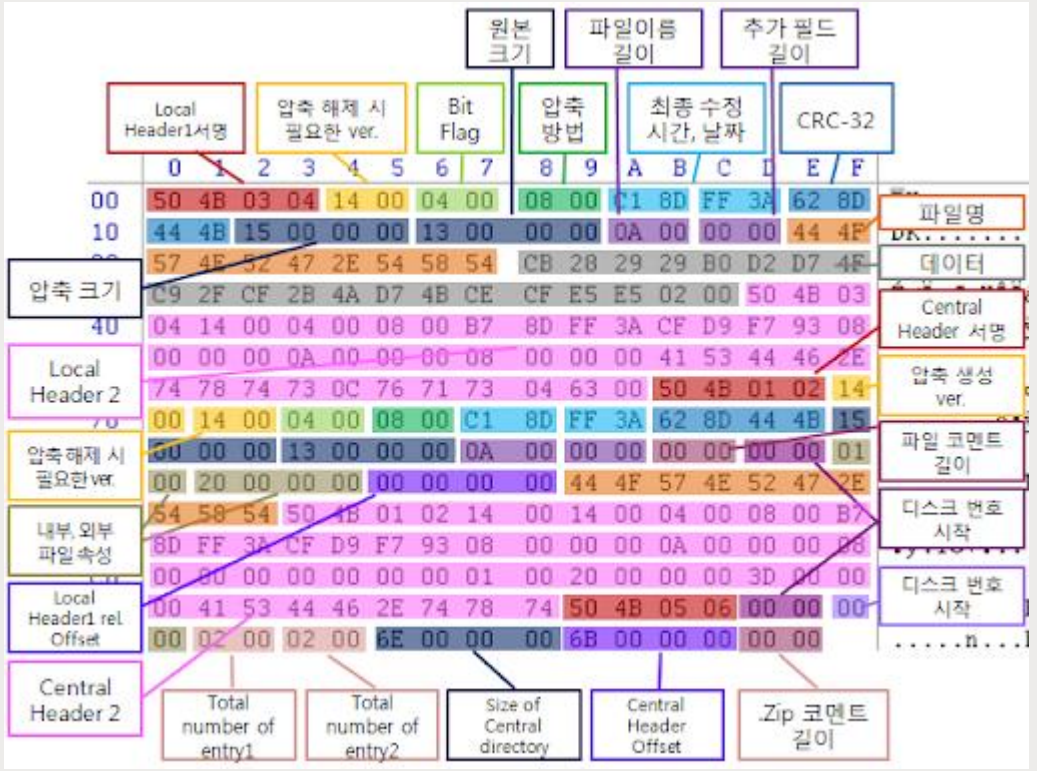
TOP Secret.zip



Fake pwd

Forensic

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	4B	03	04	14	00	00	00	09	08	46	72	42	51	C0	91	PK.....FrBQÀ'
00000010	5D	C4	C9	1C	01	00	FA	5D	01	00	08	00	00	00	73	63	]ÄÉ...ú].....sc
00000020	70	20	2E	68	77	70	EC	9A	07	58	53	4B	16	80	71	2D	p .hwpìš.XSK.€q-
00000030	AC	AB	80	AE	D2	9B	8A	82	4F	9A	48	09	1D	95	27	A8	¬«€®Ò›Š‚OšH..•'¨
00000040	34	15	05	E9	42	E8	10	5A	A8	01	82	8A	82	0A	88	2E	4..éBè.Z¨.‚Š‚.ˆ.
00000050	D2	A4	44	44	9A	74	24	A1	07	95	2A	BD	97	04	88	94	Ò¤DDštš$¡.•*½—.ˆ”
00000060	D0	03	42	08	81	84	B2	13	F4	6D	6F	6E	FB	76	BF	DD	Ð.B..„².ômonûv¿Ý
00000070	C3	F7	E7	CE	9D	19	66	E6	4C	BD	E7	DC	DB	D1	7E	F8	Ã÷çÎ..fæL½çÜÛÑ~ø
00000080	73	4A	21	CF	28	D3	1F	88	2A	D3	6E	A6	AD	ED	FD	4C	sJ!Ï(Ó.ˆ*Ón¦.íýL
00000090	FB	7E	27	EE	67	3B	7C	93	43	4C	3B	69	BB	00	5B	DB	û~'îg;|"CL;i».[Û
000000A0	DB	DB	8C	A8	DD	80	03	80	ED	FF	CB	7F	8D	6C	02	B6	ÛÛŒ¨Ý€.€íÿË..l.¶
000000B0	B6	FF	2F	FF	AB	72	83	C9	15	FC	79	32	1D	63	BA	C4	¶ÿ/ÿ«rƒÉ.üy2.c°Ä
000000C0	E4	02	AE	1E	4C	7E	4C	DF	23	1C	4C	7B	7F	6F	BD	33	ä.®.L~Lß#.L{.o½3
000000D0	FD	0D	B2	F5	37	E6	FB	5B	E5	7B	EB	FF	67	CB	7F	73	ý.²õ7æû[å{ëÿgË.s
000000E0	FD	FF	CC	F1	DF	C5	F4	97	E5	D8	FE	3B	8A	FE	71	7D	ýÿÌñßÅô—åØþ;Šþq}
000000F0	BB	98	41	F8	2E	E7	D7	38	0D	26	07	26	67	26	1B	A6	»˜Aø.ç×8.&.&g&.¦
00000100	CB	00	4B	26	6B	F0	EB	C1	F4	3D	C2	C1	F4	B3	5D	7B	Ë.K&kðëÁô=ÂÁô³]{
00000110	BE	9D	3D	7F	AB	FE	E7	19	3F	DF	1A	FB	23	D0	1E	CA	¾.=.«þç.?ß.û#Ð.Ê
00000120	74	05	E8	6E	0B	42	DF	2F	87	98	7E	F6	DD	FD	7F	1A	t.èn.Bß/‡˜~öÝý..
00000130	B0	B4	F7	6B	78	2F	D0	DC	87	C9	8D	49	9F	C9	8B	09	°´÷kx/ÐÜ‡É.IŸÉ‹.
00000140	06	FE	2C	19	23	F0	9B	F6	78	EC	C4	78	82	3E	72	05	.þ,.#ð›öxìÄx‚>r.



Fake pwd

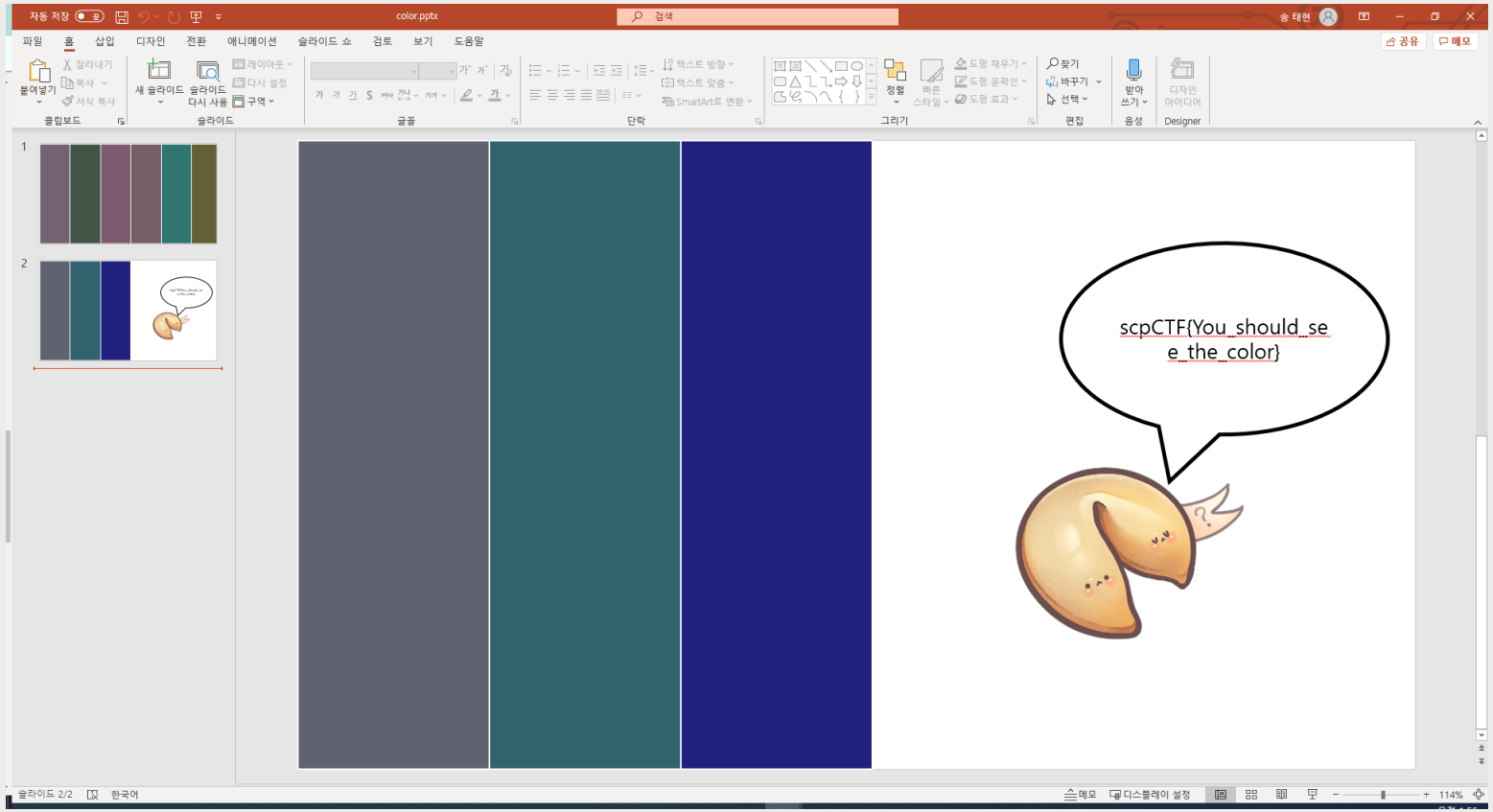
Forensic

```
00000A90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000AA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000AB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000AC0  12 00 02 01 FF FF FF FF 07 00 00 00 FF FF FF FF  ....ÿÿÿÿ....ÿÿÿÿ
00000AD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000AE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000AF0  00 00 00 00 0C 00 00 00 8B 31 01 00 00 00 00 00  ........‹1......
00000B00  50 00 72 00 76 00 54 00 65 00 78 00 74 00 00 00  P.r.v.T.e.x.t...
00000B10  73 63 70 43 54 46 7B 79 6F 75 5F 63 61 6E 5F 75  scpCTF{you_can_u
00000B20  6E 6C 6F 63 6B 5F 74 68 69 73 7D 00 00 00 00 00  nlock_this}.....
00000B30  00 00 00 00 00 00 00 00 00 00 10 00 02 01 02 00  ................
00000B40  00 00 08 00 00 00 FF FF FF FF 00 00 00 00 00 00  ......ÿÿÿÿ......
00000B50  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000B60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000B70  00 00 FC 07 00 00 00 00 00 00 44 00 6F 00 63 00  ..ü.......D.o.c.
00000B80  4F 00 70 00 74 00 69 00 6F 00 6E 00 73 00 00 00  O.p.t.i.o.n.s...
00000B90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

2
Color

color

Misc

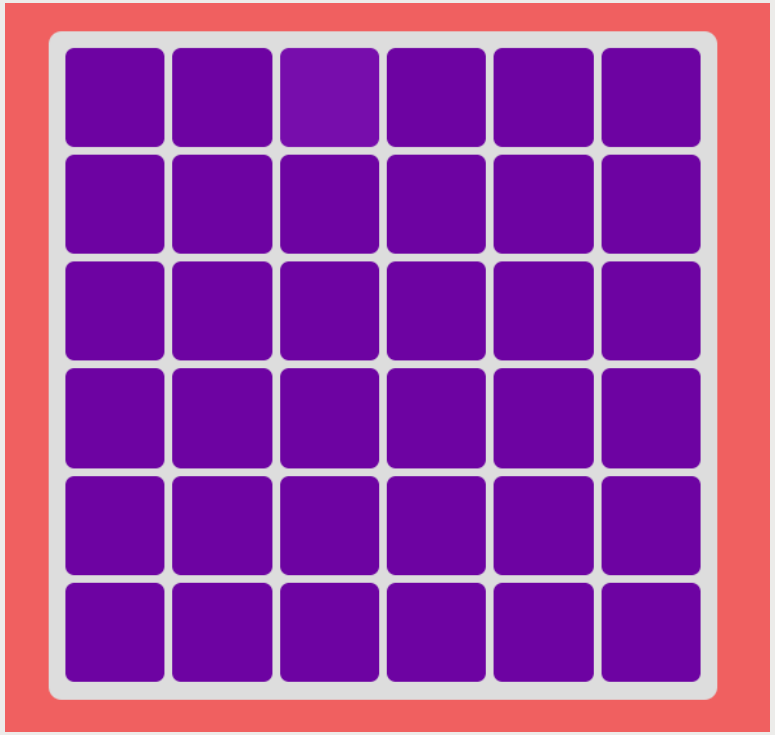


color

Misc

scpCTF{You_f0und_4_co1or!!}

736370 435446 7B596F 755F66 30756E 645F34 5F636F 31636F 21217D



3
더빨리

더 빨리

Reversing

```
C:₩Users₩qkdrn₩OneDrive₩바탕 화면₩jbctf₩reverse₩Release>2.exe
준비됐으면 엔터를 눌러주세요(구구단 0.5초안에입력해야합니다)

★☆100문 100답 시작이다☆★

5 X 5 = ?
시간을 초과했거나 틀렸어요
```

더 빨리

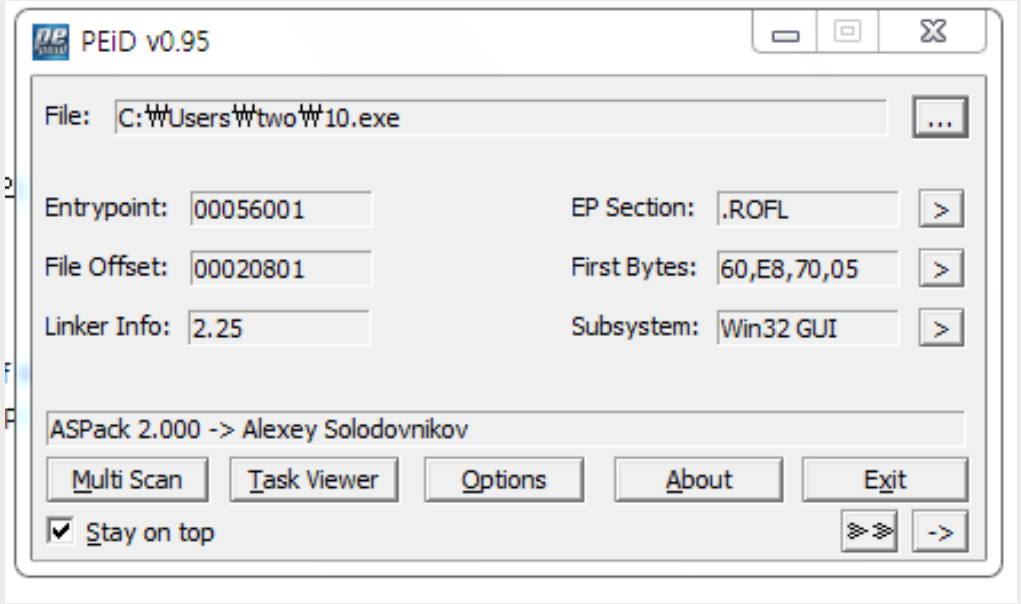
Reversing

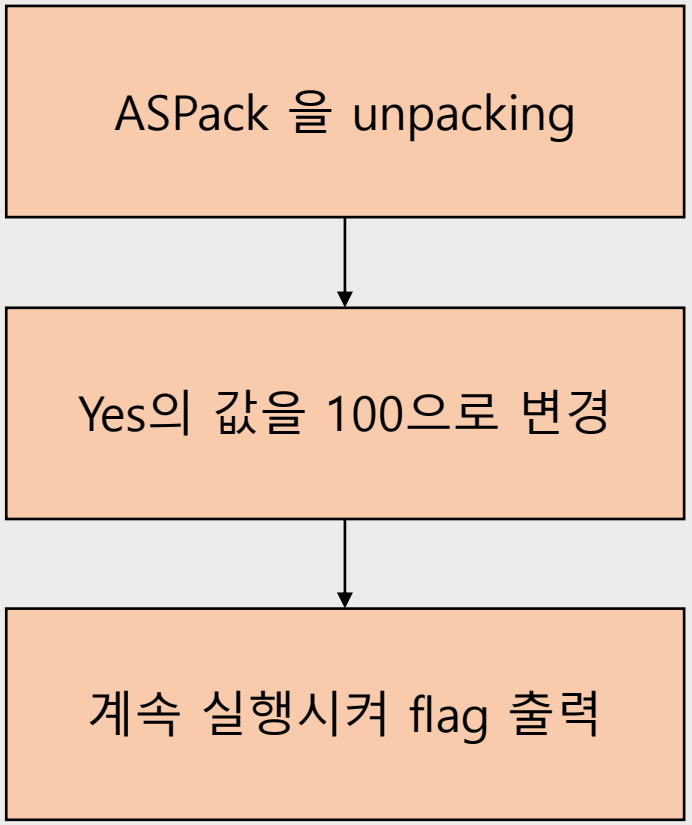
```c
int main(void)
{
    int x, y, answer, sum;
    int yes = 0;                // 정답 수
    time_t new_time, old_time;    // 경과 시간
    int keyin;                    // 답 입력 여부

    srand((unsigned)time(NULL));        // 시작할 때마다 값이 달라지도록 함

    printf("준비됐으면 엔터를 눌러주세요(구구단 0.5초안에입력해야합니다)₩n");
    getchar();

    printf("★☆100문 100답 시작이다☆★₩n₩n");


    while (1) {
        x = rand() % 9 + 1; y = rand() % 9 + 1; sum = x * y;    // 1 ~ 9

        old_time = clock();        // 시작 시간
        keyin = 1;                // 키입력 초기값

        printf("%d X %d = ?₩n", x, y);

        do {
            new_time = clock();    // 현재 시간
            if (difftime(new_time, old_time) > DELAY) {    // 시간 초과 검사
                answer = 0;        // 답이 없음
                keyin = 0;        // 키입력이 없음
                break;
            }
        } while (!kbhit());        // 키가 안 눌린 동안


        if (keyin == 1){
            scanf_s("%d", &answer);        // 답을 받음

        }

        if (sum == answer) {
            printf("₩n");
        }
```

```c
yes++;    // 정답수
if (yes == 100) {
    char down[68] = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ{}[]_-0123456789";
    char key[34] = "";
    key[0] = down[18]; //s
    key[1] = down[2]; //c
    key[2] = down[15]; //p
    key[3] = down[28]; //C
    key[4] = down[45]; //T
    key[5] = down[31]; //F
    key[6] = down[62]; //{
    key[7] = down[22]; //w
    key[8] = down[14]; //o
    key[9] = down[22]; //w
    key[10] = down[66]; //_
    key[11] = down[24]; //y
    key[12] = down[68]; //0
    key[13] = down[20]; //u
    key[14] = down[66]; //_
    key[15] = down[62]; //4
    key[16] = down[17]; //r
    key[17] = down[61]; //3
    key[18] = down[66]; //_
    key[19] = down[12]; //m
    key[20] = down[0]; //a
    key[21] = down[18]; //s
    key[22] = down[19]; //t
    key[23] = down[4]; //e
    key[24] = down[17]; //r
    key[25] = down[66]; //_
    key[26] = down[14]; //o
    key[27] = down[5]; //f
    key[28] = down[66]; //_
    key[29] = down[6]; //g
    key[30] = down[20]; //u
    key[31] = down[6]; //g
    key[32] = down[20]; //u
    key[33] = down[63]; //}


    for (int i = 0; i < 34; i++) {
        printf("%c", key[i]);
    }
    break;
}
```

더 빨리

Reversing

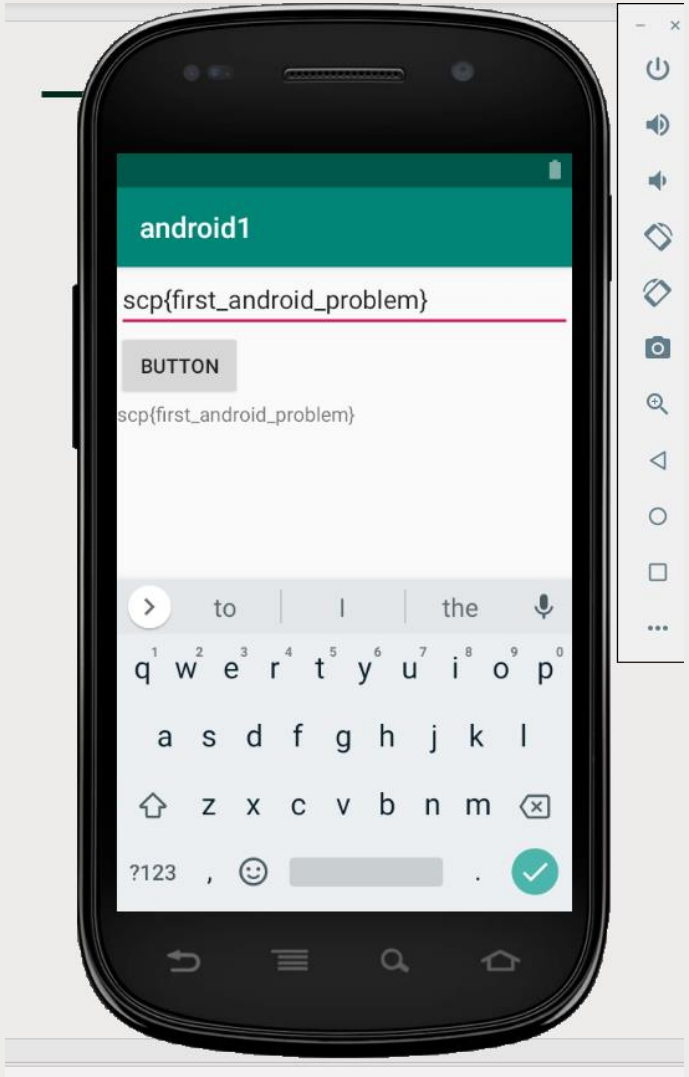


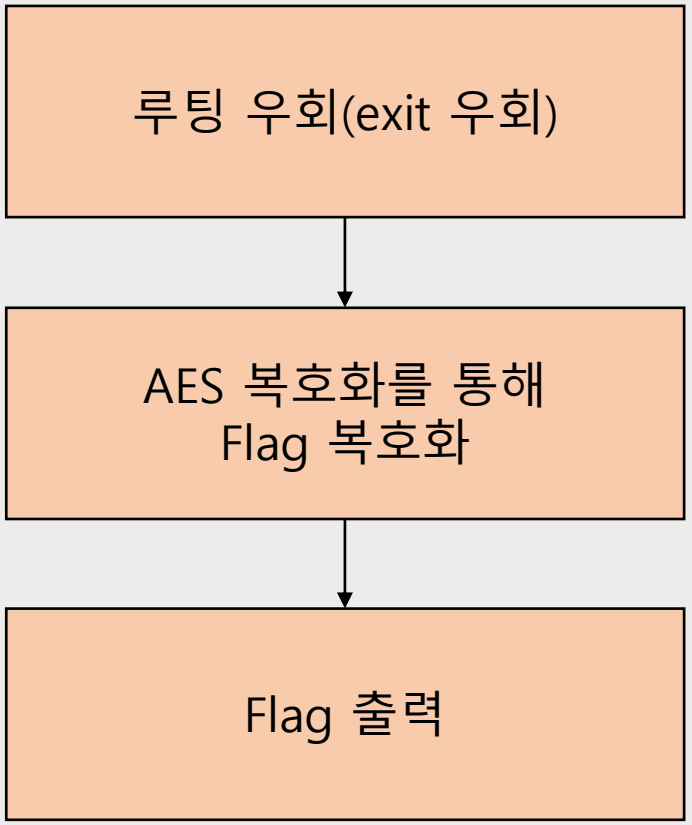


4
Android

Android

Reversing





Android

Reversing

```java
@Override
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);


    //xml에 배치한 버튼의 속성을 가져다 쓰기위한 구문
    Button bt1 = (Button) findViewById(R.id.button1);

    //버튼을 클릭했을때 이벤트가 일어나도록 처리
    bt1.setOnClickListener(new Button.OnClickListener() {

        //OnClickListener에 필요한 메소드 처리
        @Override
        public void onClick(View arg0) {

            if (c.a() || c.b() || c.c()) {
                System.exit( status: 0);
            }

            // TODO Auto-generated method stub
            //xml에 배치한 에디트텍스트의 속성을 가져다 쓰기 위한 구문
            EditText ed1 = (EditText) findViewById(R.id.editText1);
            //에디터박스에 입력받은 문자열을 저장할 공간할당
            String str;
            //str에 에디트텍스트의 문자열을 저장
            str = ed1.getText().toString();

            //xml에 배치한 텍스트뷰의 속성을 가져다 쓰기위한 구문
            TextView tv1 = (TextView) findViewById(R.id.textView1);
            //str에 저장된 문자열을 텍스트뷰에 출력
            tv1.setText(str);
```

```java
package com.test.android1;

import android.os.Build;
import java.io.File;


public class c {
    public static boolean a() {
        for (String file : System.getenv( name: "PATH").split( regex: ":")) {
            if (new File(file, child: "su").exists()) {
                return true;
            }
        }
        return false;
    }

    public static boolean b() {
        String str = Build.TAGS;
        return str != null && str.contains("test-keys");
    }

    public static boolean c() {
        for (String file : new String[]{"/system/app/Superuser.apk", "/system/xbin/daemonsu", "/system/etc/init.d/99SuperSUDaemon", "/system/bin/.ext/.su", "/system/etc/.has_su_daemon", "/system/etc/.installed_su_daemo
            if (new File(file).exists()) {
                return true;
            }
        }
        return false;
    }

}
```

1. 암호화 작업

2. 반드시 후킹을 이용 하도록 변경

5
To be Continue

만들 예정

FIRST

포스터

평양에서 온 편지

SECOND

어셈블리

어셈블리어만 보고 값 유추

THIRD

Eps이용

Eps 를 이용한 한글 문서

FOURTH

Android hooking

Gps 값을 후킹하여 변조 후 flag 출력

BYE.

좀 더 좋은 문제를 만들고 싶다

E.N.D