Codeengn 스마트앱 2번문제 보고서

1. SmartApp L02.apk 를 디컴파일 후 자바소스를 통해 분석 중 키를 출력해주는 부분을 찾음.
   시간과 볼륨을 변조하면 될 것 같으나 조건문을 바꾸기로 함.
   == && == 을 != && != 로 변조하기로 함.

```
41      protected void onCreate(Bundle bundle)
42      {
43          super.onCreate(bundle);
44          setContentView(0x7f030000);
45          aView = (TextView)findViewById(0x7f080000);
46          if(makeDate() == "2013-11-02-12:35:03" && Volume() == 53)
47              aView.setText(keyString());
48      }
```

2. MainActivity.smali 파일에서 1번에서 발견한 조건문의 조건을 변조함.

```
83  .method protected onCreate(Landroid/os/Bundle;)V
84      .locals 2
85      .parameter "savedInstanceState"
86
87      .prologue
88      .line 21
89      invoke-super {p0, p1}, Landroid/app/Activity;->onCreate(Landroid/os/Bundle;)V
90
91      .line 22
92      const/high16 v0, 0x7f03
93
94      invoke-virtual {p0, v0}, Lcom/namdaehyeon/findkey2/MainActivity;->setContentView(I)V
95
96      .line 24
97      const/high16 v0, 0x7f08
98
99      invoke-virtual {p0, v0}, Lcom/namdaehyeon/findkey2/MainActivity;->findViewById(I)Landroid/view/View;
100
101     move-result-object v0
102
103     check-cast v0, Landroid/widget/TextView;
104
105     iput-object v0, p0, Lcom/namdaehyeon/findkey2/MainActivity;->aView:Landroid/widget/TextView;
106
107     .line 29
108     invoke-virtual {p0}, Lcom/namdaehyeon/findkey2/MainActivity;->makeDate()Ljava/lang/String;
109
110     move-result-object v0
111
112     const-string v1, "2013-11-02-12:35:03"
113
114     if-ne v0, v1, :cond_0
115
116     .line 30
117     invoke-virtual {p0}, Lcom/namdaehyeon/findkey2/M
118
119     move-result v0
120
121     const/16 v1, 0x35
122
123     if-ne v0, v1, :cond_0
124
```

if-ne 를 if-eq로 변조함.

3. 변조 후 왼쪽 화면이 우측 화면처럼 답을 출력함.