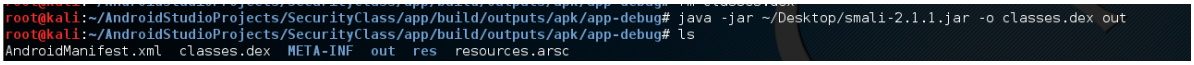
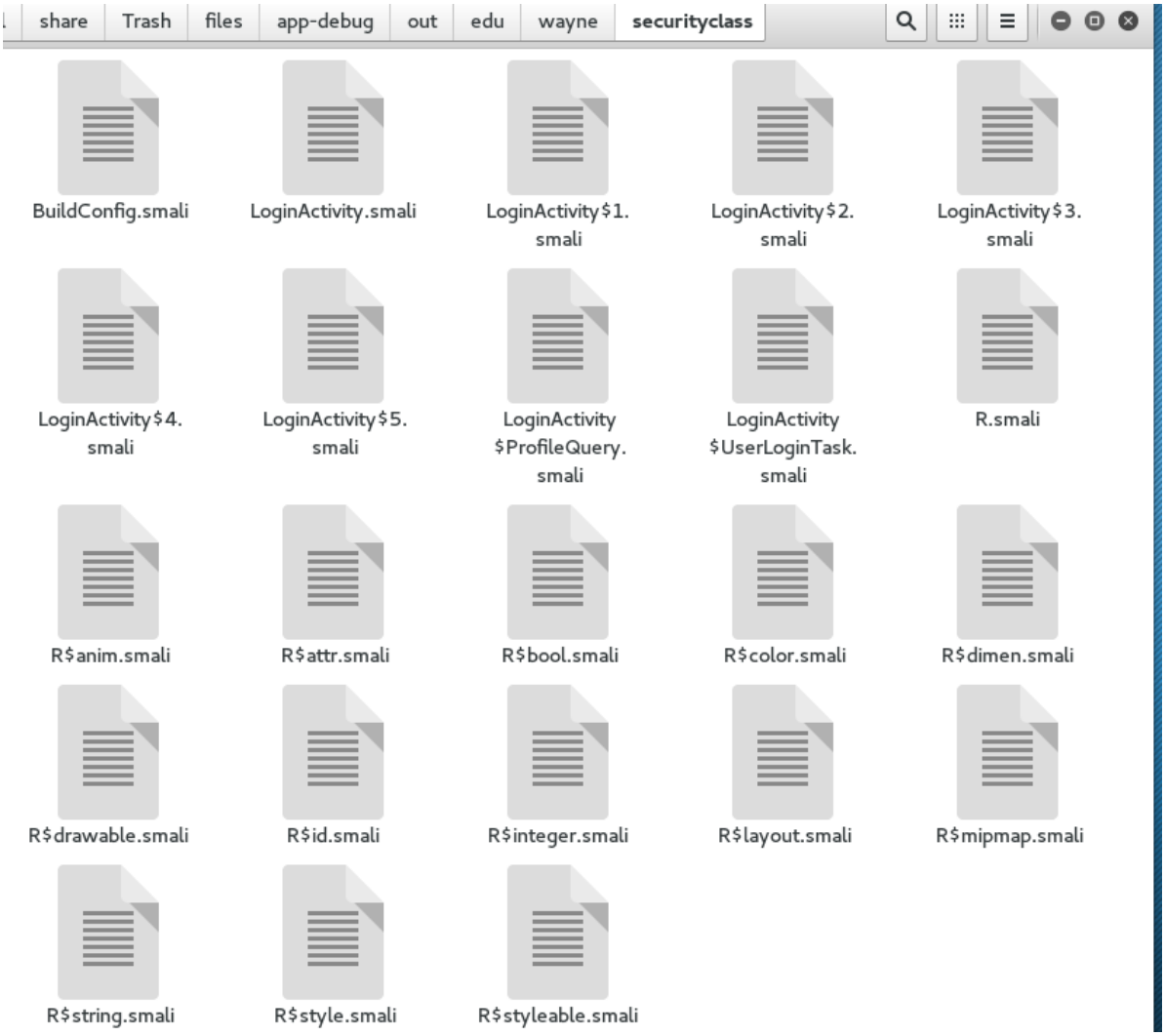
1.Get familiar with the process:

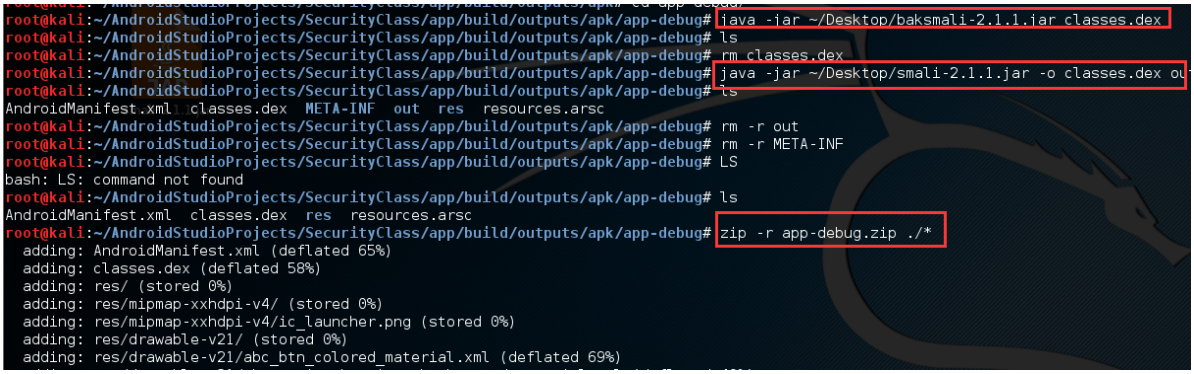
Convert dex to smail Format:



Examine the smail file:



Repackage the file:

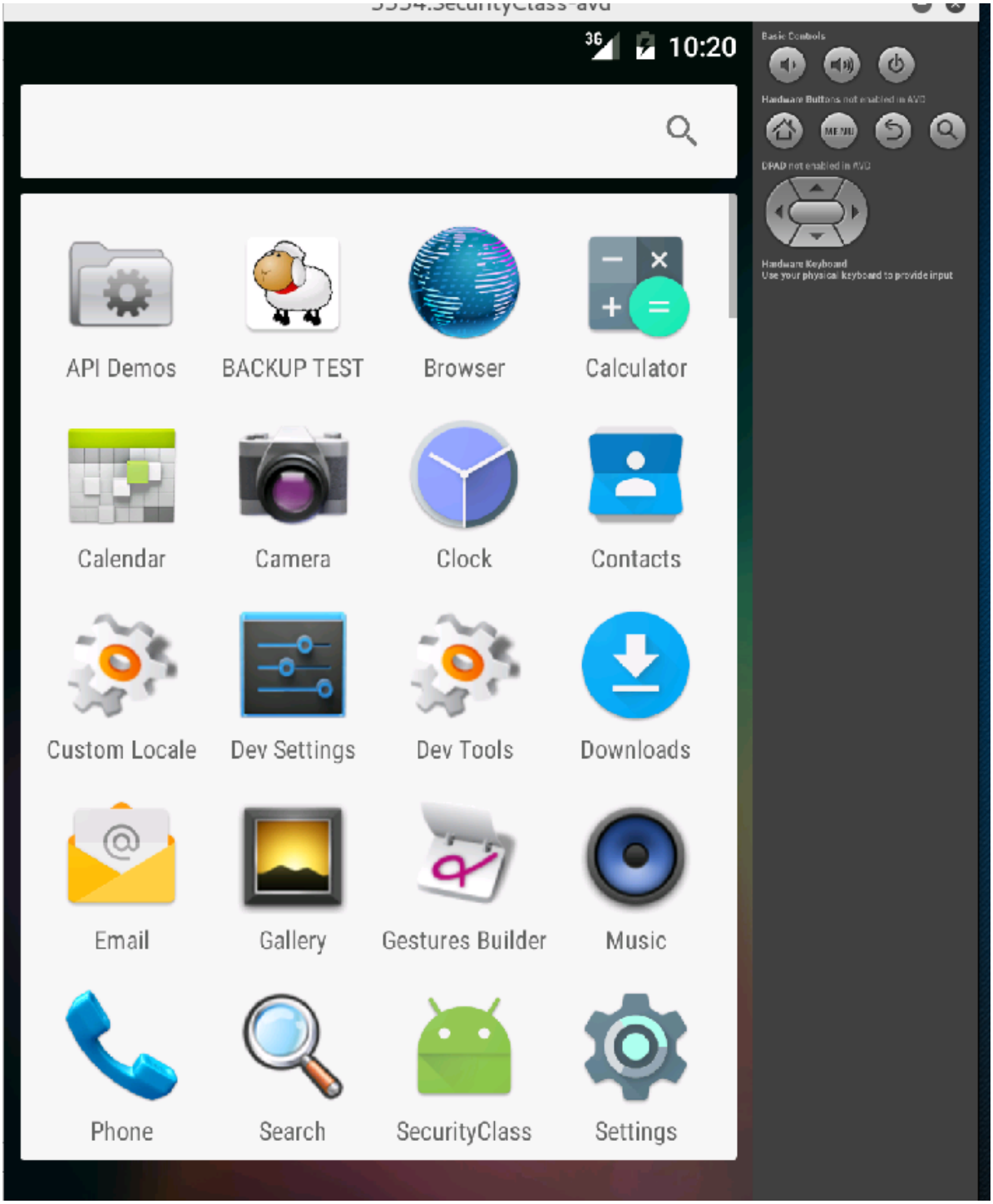


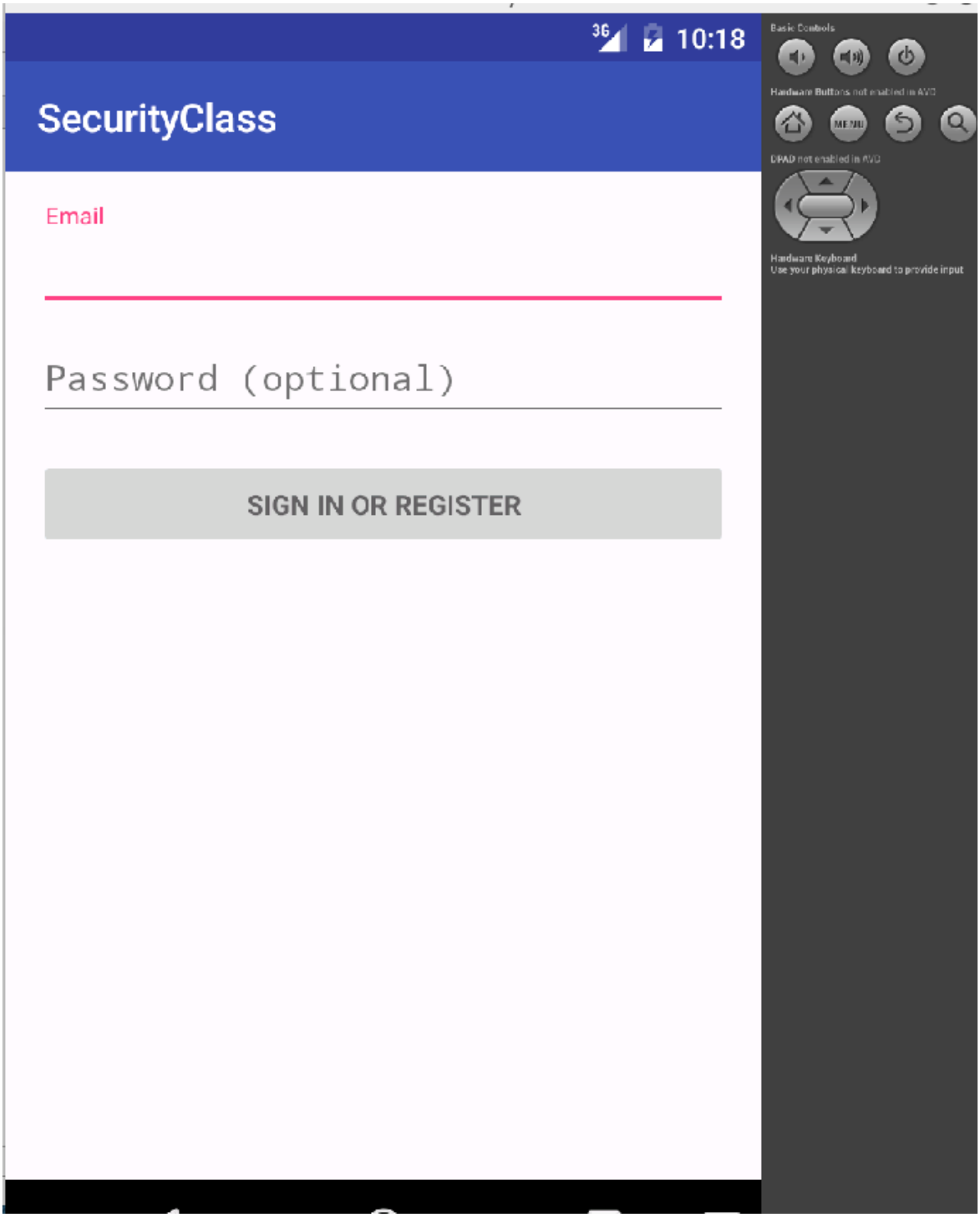
Sign the package:

```
root@kali:~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug# keytool -genkey -keystore xinying.keystore -alias xinying-key -keyalg RSA -keysize 2048 -validity 10000
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
  [no]:  y

Enter key password for <xinying-key>
        (RETURN if same as keystore password):
Re-enter new password:
root@kali:~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug# jarsigner -sigalg SHA1withRSA -digestalg SHA1 -keystore xinying.keystore app-debug.apk xinying-key
\Enter Passphrase for keystore:
jarsigner error: java.lang.RuntimeException: keystore load: Keystore was tampered with, or password was incorrect
root@kali:~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug# jarsigner -sigalg SHA1withRSA -digestalg SHA1 -keystore xinying.keystore app-debug.apk xinying-key
Enter Passphrase for keystore:
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate this jar after the signer certificate's expiration date (2049-03-10) o
vocation date.
root@kali:~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug# /root/Android/Sdk/build-tools/23.0.2/zipalign -v 4 app-debug.apk app-debug-aligned.apk
Verifying alignment of app-debug-aligned.apk (4)...
     50 META-INF/MANIFEST.MF (OK - compressed)
  10200 META-INF/XINYING-.SF (OK - compressed)
  20490 META-INF/XINYING-.RSA (OK - compressed)
  21630 AndroidManifest.xml (OK - compressed)
  22571 classes.dex (OK - compressed)
```

```
1154116 resources.arsc (OK - co
Verification succesful
root@kali:~/AndroidStudioProject
```

install it and run it on avd:


10:20
API Demos
BACKUP TEST
Browser
Calculator
Calendar
Camera
Clock
Contacts
Custom Locale
Dev Settings
Dev Tools
Downloads
Email
Gallery
Gestures Builder
Music
Phone
Search
SecurityClass
Settings
Basic Controls
Hardware Keyboard
Use your physical keyboard to provide input



2.Leak the username and password:

```
//The file I modify: LoginActivity.smail
//The method I modified :

.method private attemptLogin()V
    .registers 9

    .prologue
    const/4 v7, 0x1

    const/4 v4, 0x0

    .line 147
```

```
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;-
>mAuthTask:Ledu/wayne/securityclass/LoginActivity$UserLoginTask;

    if-eqz v5, :cond_7

    .line 191
    :goto_6
    return-void

    .line 152
    :cond_7
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;-
>mEmailView:Landroid/widget/AutoCompleteTextView;

    invoke-virtual {v5, v4}, Landroid/widget/AutoCompleteTextView;-
>setError(Ljava/lang/CharSequence;)V

    .line 153
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;-
>mPasswordView:Landroid/widget/EditText;

    invoke-virtual {v5, v4}, Landroid/widget/EditText;-
>setError(Ljava/lang/CharSequence;)V

    .line 156
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;-
>mEmailView:Landroid/widget/AutoCompleteTextView;

    invoke-virtual {v5}, Landroid/widget/AutoCompleteTextView;-
>getText()Landroid/text/Editable;

    move-result-object v5

    invoke-virtual {v5}, Ljava/lang/Object;->toString()Ljava/lang/String;

    move-result-object v1

    .line 157
    .local v1, "email":Ljava/lang/String;
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;-
>mPasswordView:Landroid/widget/EditText;

    invoke-virtual {v5}, Landroid/widget/EditText;-
>getText()Landroid/text/Editable;

    move-result-object v5

    invoke-virtual {v5}, Ljava/lang/Object;->toString()Ljava/lang/String;

    move-result-object v3

    .line 159
    .local v3, "password":Ljava/lang/String;
    const/4 v0, 0x0

    .line 160
    .local v0, "cancel":Z
    const/4 v2, 0x0
```

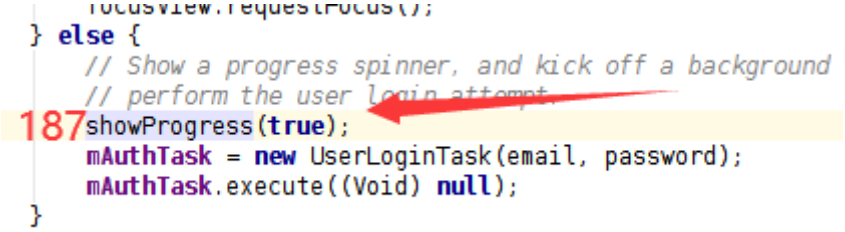
```
    .line 163
    .local v2, "focusView":Landroid/view/View;
    invoke-static {v3}, Landroid/text/TextUtils;->isEmpty(Ljava/lang/CharSequence;)Z

    move-result v5

    if-nez v5, :cond_42

    invoke-direct {p0, v3}, Ledu/wayne/securityclass/LoginActivity;->isPasswordValid(Ljava/lang/String;)Z

    move-result v5

    if-nez v5, :cond_42

    .line 164
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mPasswordView:Landroid/widget/EditText;

    const v6, 0x7f06001c

    invoke-virtual {p0, v6}, Ledu/wayne/securityclass/LoginActivity;->getString(I)Ljava/lang/String;

    move-result-object v6

    invoke-virtual {v5, v6}, Landroid/widget/EditText;->setError(Ljava/lang/CharSequence;)V

    .line 165
    iget-object v2, p0, Ledu/wayne/securityclass/LoginActivity;->mPasswordView:Landroid/widget/EditText;

    .line 166
    const/4 v0, 0x1

    .line 170
    :cond_42
    invoke-static {v1}, Landroid/text/TextUtils;->isEmpty(Ljava/lang/CharSequence;)Z

    move-result v5

    if-eqz v5, :cond_5d

    .line 171
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mEmailView:Landroid/widget/AutoCompleteTextView;

    const v6, 0x7f060019

    invoke-virtual {p0, v6}, Ledu/wayne/securityclass/LoginActivity;->getString(I)Ljava/lang/String;

    move-result-object v6
```

```
    invoke-virtual {v5, v6}, Landroid/widget/AutoCompleteTextView;-
>setError(Ljava/lang/CharSequence;)V

    .line 172
    iget-object v2, p0, Ledu/wayne/securityclass/LoginActivity;-
>mEmailView:Landroid/widget/AutoCompleteTextView;

    .line 173
    const/4 v0, 0x1

    .line 180
    :cond_57
    :goto_57
    if-eqz v0, :cond_73

    .line 183
    invoke-virtual {v2}, Landroid/view/View;->requestFocus()Z

    goto :goto_6

    .line 174
    :cond_5d
    invoke-direct {p0, v1}, Ledu/wayne/securityclass/LoginActivity;-
>isEmailValid(Ljava/lang/String;)Z

    move-result v5

    if-nez v5, :cond_57

    .line 175
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;-
>mEmailView:Landroid/widget/AutoCompleteTextView;

    const v6, 0x7f06001b

    invoke-virtual {p0, v6}, Ledu/wayne/securityclass/LoginActivity;-
>getString(I)Ljava/lang/String;

    move-result-object v6

    invoke-virtual {v5, v6}, Landroid/widget/AutoCompleteTextView;-
>setError(Ljava/lang/CharSequence;)V

    .line 176
    iget-object v2, p0, Ledu/wayne/securityclass/LoginActivity;-
>mEmailView:Landroid/widget/AutoCompleteTextView;

    .line 177
    const/4 v0, 0x1

    goto :goto_57

//modify here!
    .line 187
    :cond_73
    const-string v5, "email:"
```

```
    invoke-static {v5, v1}, Landroid/util/Log;-
>d(Ljava/lang/String;Ljava/lang/String;)I

    .line 188
    const-string v5, "password:"
    invoke-static {v5, v3}, Landroid/util/Log;-
>d(Ljava/lang/String;Ljava/lang/String;)I
//
    .line 189
    invoke-direct {p0, v7}, Ledu/wayne/securityclass/LoginActivity;-
>showProgress(Z)V

    .line 190
    new-instance v5, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;

    invoke-direct {v5, p0, v1, v3},
Ledu/wayne/securityclass/LoginActivity$UserLoginTask;-><init>
(Ledu/wayne/securityclass/LoginActivity;Ljava/lang/String;Ljava/lang/String;)V

    iput-object v5, p0, Ledu/wayne/securityclass/LoginActivity;-
>mAuthTask:Ledu/wayne/securityclass/LoginActivity$UserLoginTask;

    .line 191
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;-
>mAuthTask:Ledu/wayne/securityclass/LoginActivity$UserLoginTask;

    new-array v6, v7, [Ljava/lang/Void;

    const/4 v7, 0x0

    check-cast v4, Ljava/lang/Void;

    aput-object v4, v6, v7

    invoke-virtual {v5, v6},
Ledu/wayne/securityclass/LoginActivity$UserLoginTask;-
>execute([Ljava/lang/Object;)Landroid/os/AsyncTask;

    goto/16 :goto_6
.end method
```

process

Examine the source code, I want to add log here:



Then I explore the smali file and locate it:

```
    .line 187
    :cond_73
    invoke-direct {p0, v7}, Ledu/wayne/securityclass/LoginActivity;->showProgress(Z)V

    .line 188

    new-instance v5, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;

    invoke-direct {v5, p0, v1, v3}, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;-
><init>(Ledu/wayne/securityclass/LoginActivity;Ljava/lang/String;Ljava/lang/String;)V

    iput-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mAuthTask:Ledu/wayne/
securityclass/LoginActivity$UserLoginTask;

    .line 189
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mAuthTask:Ledu/wayne/
securityclass/LoginActivity$UserLoginTask;

    new-array v6, v7, [Ljava/lang/Void;

    const/4 v7, 0x0

    check-cast v4, Ljava/lang/Void;

    aput-object v4, v6, v7

    invoke-virtual {v5, v6}, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;->execute
([Ljava/lang/Object;)Landroid/os/AsyncTask;

    goto/16 :goto_6
.end method
```

Then I modify it :

```
    .line 187
    :cond_73
    const-string v5, "email:"

    invoke-static {v5, v1}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

    .line 188
    const-string v5, "password:"

    invoke-static {v5, v3}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

    .line 189   +2
    invoke-direct {p0, v7}, Ledu/wayne/securityclass/LoginActivity;->showProgress(Z)V

    .line 190
    new-instance v5, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;

    invoke-direct {v5, p0, v1, v3}, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;-><init>(Ledu/wayne/securityclass/Logir

    iput-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mAuthTask:Ledu/wayne/securityclass/LoginActivity$UserLoginTask;

    .line 191
    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mAuthTask:Ledu/wayne/securityclass/LoginActivity$UserLoginTask;

    new-array v6, v7, [Ljava/lang/Void;
```

Repackage it and install it, then I find the log in the logcat

3.The result

```
10-23 00:14:17.266 684-684/? D/gralloc_goldfish: Emulator without GPU emulation detected.
10-23 00:14:35.260 684-684/? I/LatinIME: Starting input. Cursor position = 0,0
10-23 00:14:39.858 1068-1068/? D/email:: foo@example.com
10-23 00:14:39.858 1068-1068/? D/password:: hello
10-23 00:14:39.926 1068-1068/? I/Choreographer: Skipped 30 frames!  The application may be
10-23 00:14:43.274 55-55/? D/gralloc: Registering a buffer in the process that created it.
```

4.obfuscation

a. What tools did you use?

By modify the build.gradle

add:

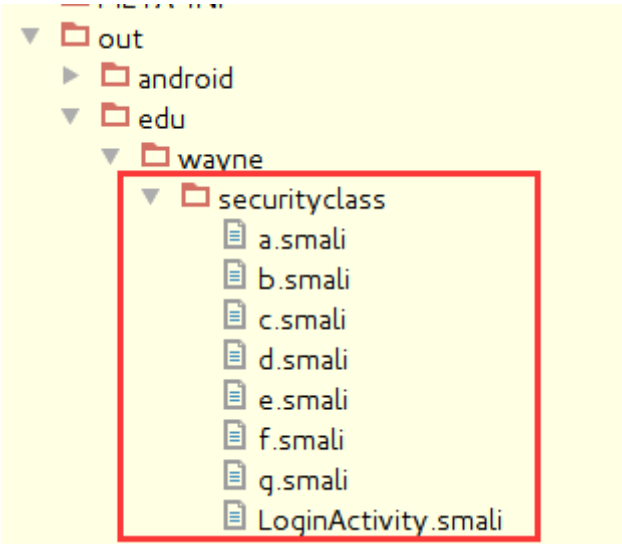
```
 minifyEnabled true
 shrinkResources true
```

```
apply plugin: 'com.android.application'

android {
    compileSdkVersion 23
    buildToolsVersion "23.0.2"

    defaultConfig {
        applicationId "edu.wayne.securityclass"
        minSdkVersion 19
        targetSdkVersion 23
        versionCode 1
        versionName "1.0"
    }
    buildTypes {
        debug {
           // Enables code shrinking, obfuscation, and optimization for only
           // your project's release build type.
            minifyEnabled true

           // Enables resource shrinking, which is performed by the
           // Android Gradle plugin.
            shrinkResources true
            proguardFiles getDefaultProguardFile('proguard-android.txt'),
'proguard-rules.pro'
        }

        release {
           // Enables code shrinking, obfuscation, and optimization for only
           // your project's release build type.
            minifyEnabled true

           // Enables resource shrinking, which is performed by the
           // Android Gradle plugin.
            shrinkResources true
            proguardFiles getDefaultProguardFile('proguard-android.txt'),
'proguard-rules.pro'
        }
    }
}

dependencies {
    compile fileTree(dir: 'libs', include: ['*.jar'])
    testCompile 'junit:junit:4.12'
    compile 'com.android.support:appcompat-v7:23.1.1'
    compile 'com.android.support:design:23.1.1'
}
```

b. Can you still repackage the application using baksmali or smali tool? Justify your answer

I can still repackage the application using baksmali or smali tool, but the smail code become harder to understand.

The content:



And there is no method name and attribute name anymore:

```
.method private m()V
    .registers 9
```

```
:cond_72
invoke-direct {p0, v3}, Ledu/wayne/securityclass/LoginActivity;->b(Z)V
```

no line order anymore.

But carefully, we can still find the place where log in happended.

```
const-string v8, "email:"
invoke-static {v8, v5}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I
const-string v8, "password:"
invoke-static {v8, v6}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I
invoke-direct {p0, v3}, Ledu/wayne/securityclass/LoginActivity;->b(Z)V
new-instance v1, Ledu/wayne/securityclass/g;
invoke-direct {v1, p0, v5, v6}, Ledu/wayne/securityclass/g;-><init>(Ledu/wayne/securityclass/LoginActivity;Ljava/lang/String;L
iput-object v1, p0, Ledu/wayne/securityclass/LoginActivity;->j:Ledu/wayne/securityclass/g;
iget-object v1, p0, Ledu/wayne/securityclass/LoginActivity;->j:Ledu/wayne/securityclass/g;
new-array v2, v3, [Ljava/lang/Void;
check-cast v0, Ljava/lang/Void;
aput-object v0, v2, v4
```