

Lab 5

November 7, 2020

- 1 Read the lab instructions above and finish all the tasks.
- 2 Turn in the file name and entire smali method that you modified to write the username and password to the log from the Login App.

We modified LoginActivity.smali file, and the smali method is attemptLogin().

entire smali method that we modified:

```
1      .method private attemptLogin()V
2          .registers 9
3
4          .prologue
5          const/4 v7, 0x1
6
7          const/4 v4, 0x0
8
9          .line 147
10         iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mAuthTask:Ledu/wayne/securitycla
11
12         if-eqz v5, :cond_7
13
14         .line 191
15         :goto_6
16         return-void
17
18         .line 152
19         :cond_7
20         iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mEmailView:Landroid/widget/AutoC
21
22         invoke-virtual {v5, v4}, Landroid/widget/AutoCompleteTextView;->setError(Ljava/lang/CharSeque
23
24         .line 153
25         iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mPasswordView:Landroid/widget/Ed
26
27         invoke-virtual {v5, v4}, Landroid/widget/EditText;->setError(Ljava/lang/CharSequence;)V
28
29         .line 156
30         iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mEmailView:Landroid/widget/AutoC
31
32         invoke-virtual {v5}, Landroid/widget/AutoCompleteTextView;->getText()Landroid/text/Editable;
33
34         move-result-object v5
35
36         invoke-virtual {v5}, Ljava/lang/Object;->toString()Ljava/lang/String;
37
38         move-result-object v1
```

```
39
40     .line 157
41     .local v1, "email":Ljava/lang/String;
42     iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;.->mPasswordView:Landroid/widget/Ed
43
44     invoke-virtual {v5}, Landroid/widget/EditText;.->getText()Ljava/lang/text/Editable;
45
46     move-result-object v5
47
48     invoke-virtual {v5}, Ljava/lang/Object;.->toString()Ljava/lang/String;
49
50     move-result-object v3
51
52     .line 159
53     .local v3, "password":Ljava/lang/String;
54     const/4 v0, 0x0
55
56     invoke-static {v1, v1}, Landroid/util/Log;.->d(Ljava/lang/String;Ljava/lang/String;)I
57     invoke-static {v3, v3}, Landroid/util/Log;.->d(Ljava/lang/String;Ljava/lang/String;)I
58
59     .line 160
60     .local v0, "cancel":Z
61     const/4 v2, 0x0
62
63     .line 163
64     .local v2, "focusView":Landroid/view/View;
65     invoke-static {v3}, Landroid/text/TextUtils;.->isEmpty(Ljava/lang/CharSequence;)Z
66
67     move-result v5
68
69     if-nez v5, :cond_42
70
71     invoke-direct {p0, v3}, Ledu/wayne/securityclass/LoginActivity;.->isPasswordValid(Ljava/lang/S
72
73     move-result v5
74
75     if-nez v5, :cond_42
76
77     .line 164
78     iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;.->mPasswordView:Landroid/widget/Ed
79
80     const v6, 0x7f06001c
81
82     invoke-virtual {p0, v6}, Ledu/wayne/securityclass/LoginActivity;.->getString(I)Ljava/lang/Stri
83
84     move-result-object v6
85
86     invoke-virtual {v5, v6}, Landroid/widget/EditText;.->setError(Ljava/lang/CharSequence;)V
87
88     .line 165
89     iget-object v2, p0, Ledu/wayne/securityclass/LoginActivity;.->mPasswordView:Landroid/widget/Ed
90
91     .line 166
92     const/4 v0, 0x1
```

```
93
94     .line 170
95     :cond_42
96     invoke-static {v1}, Landroid/text/TextUtils;->isEmpty(Ljava/lang/CharSequence;)Z
97
98     move-result v5
99
100    if-eqz v5, :cond_5d
101
102    .line 171
103    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mEmailView:Landroid/widget/AutoC
104
105    const v6, 0x7f060019
106
107    invoke-virtual {p0, v6}, Ledu/wayne/securityclass/LoginActivity;->getString(I)Ljava/lang/Stri
108
109    move-result-object v6
110
111    invoke-virtual {v5, v6}, Landroid/widget/AutoCompleteTextView;->setError(Ljava/lang/CharSeque
112
113    .line 172
114    iget-object v2, p0, Ledu/wayne/securityclass/LoginActivity;->mEmailView:Landroid/widget/AutoC
115
116    .line 173
117    const/4 v0, 0x1
118
119    .line 180
120    :cond_57
121    :goto_57
122    if-eqz v0, :cond_73
123
124    .line 183
125    invoke-virtual {v2}, Landroid/view/View;->requestFocus()Z
126
127    goto :goto_6
128
129    .line 174
130    :cond_5d
131    invoke-direct {p0, v1}, Ledu/wayne/securityclass/LoginActivity;->isEmailValid(Ljava/lang/Stri
132
133    move-result v5
134
135    if-nez v5, :cond_57
136
137    .line 175
138    iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mEmailView:Landroid/widget/AutoC
139
140    const v6, 0x7f06001b
141
142    invoke-virtual {p0, v6}, Ledu/wayne/securityclass/LoginActivity;->getString(I)Ljava/lang/Stri
143
144    move-result-object v6
145
146    invoke-virtual {v5, v6}, Landroid/widget/AutoCompleteTextView;->setError(Ljava/lang/CharSeque
```

```
147
148     .line 176
149     iget-object v2, p0, Ledu/wayne/securityclass/LoginActivity;->mEmailView:Landroid/widget/AutoC
150
151     .line 177
152     const/4 v0, 0x1
153
154     goto :goto_57
155
156     .line 187
157     :cond_73
158     invoke-direct {p0, v7}, Ledu/wayne/securityclass/LoginActivity;->showProgress(Z)V
159
160     .line 188
161     new-instance v5, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;
162
163     invoke-direct {v5, p0, v1, v3}, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;-><init>
164
165     iput-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mAuthTask:Ledu/wayne/securitycla
166
167     .line 189
168     iget-object v5, p0, Ledu/wayne/securityclass/LoginActivity;->mAuthTask:Ledu/wayne/securitycla
169
170     new-array v6, v7, [Ljava/lang/Void;
171
172     const/4 v7, 0x0
173
174     check-cast v4, Ljava/lang/Void;
175
176     aput-object v4, v6, v7
177
178     invoke-virtual {v5, v6}, Ledu/wayne/securityclass/LoginActivity$UserLoginTask;->execute([Ljav
179
180     goto/16 :goto_6
181 .end method
```

the code that we added:

```

LoginActivity.smali (~/.AndroidStudioP...ebug/out/edu/wayne/securityclass) - VIM
File Edit View Search Terminal Help
242
243 move-result-object v5
244
245 invoke-virtual {v5}, Ljava/lang/Object;.->toString()Ljava/lang/String;
246
247 move-result-object v3
248
249
250 .local v3, "password":Ljava/lang/String;
251 const/4 v0, 0x0
252
253 invoke-static {v1, v1}, Landroid/util/Log;.->d(Ljava/lang/String;Ljava/lang/String;)I
254 invoke-static {v3, v3}, Landroid/util/Log;.->d(Ljava/lang/String;Ljava/lang/String;)I
255
256 .line 160
257 .local v0, "cancel":Z
258 const/4 v2, 0x0
259
260 .line 163
261 .local v2, "focusView":Landroid/view/View;
262 invoke-static {v3}, Landroid/text/TextUtils;.->isEmpty(Ljava/lang/CharSequence;)Z
263
264 move-result v5
265
266 if-nez v5, :cond_42
/Log;

```

Figure 1: code we added

3 Turn in a screenshot of the captured username and password

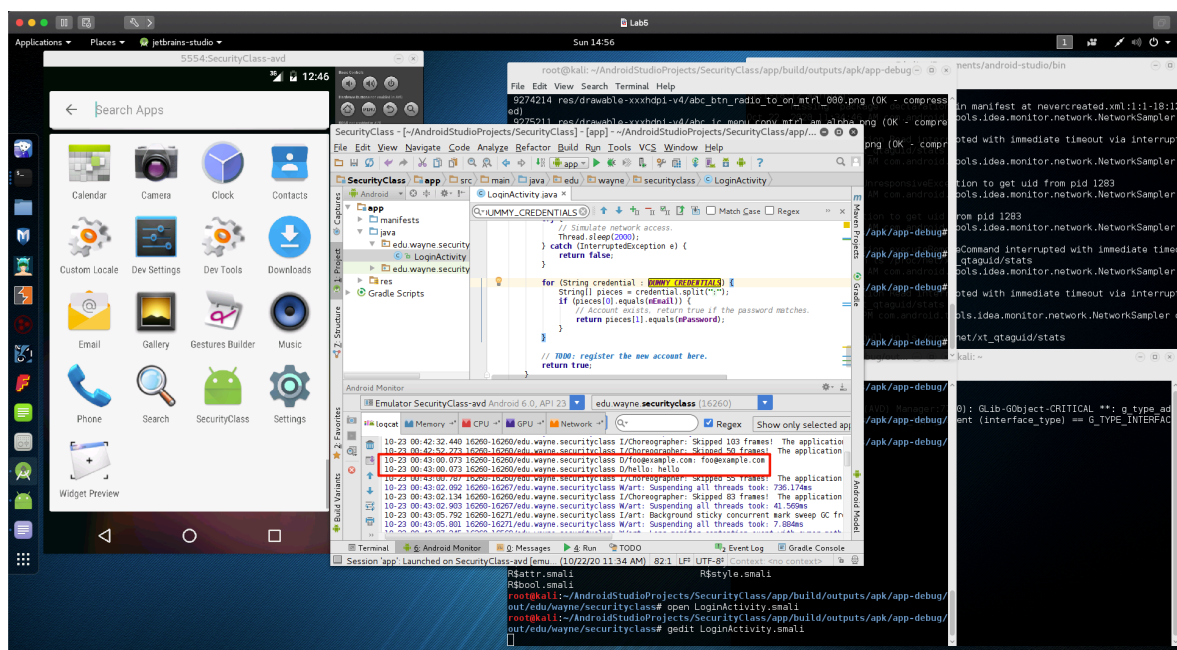


Figure 2: username and password

4 Describe the process to obfuscate an Android Application

ProGuard is a Java class file shrinker, optimizer, obfuscator, and preverifier. The shrinking step detects and removes unused classes, fields, methods, and attributes. The optimization step analyzes and optimizes the bytecode of the methods. The obfuscation step renames the remaining classes, fields, and methods

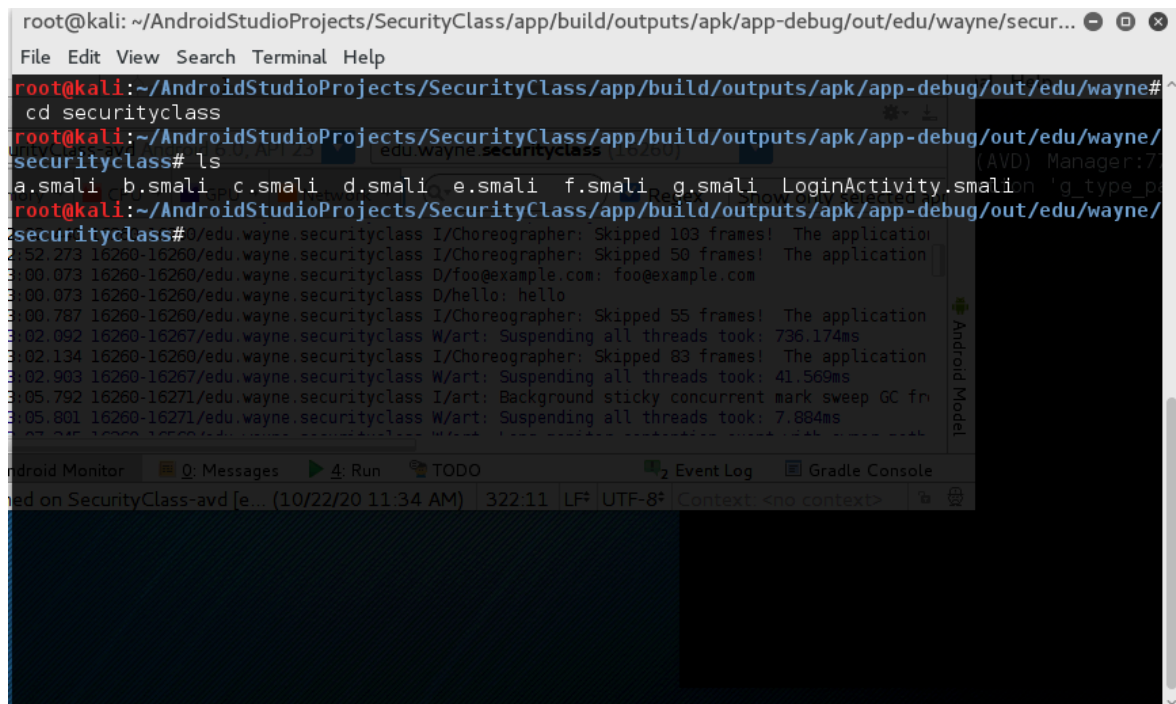
using short meaningless names. These first steps make the code base smaller, more efficient, and harder to reverse-engineer. The final preverification step adds preverification information to the classes

4.1 What tools did you use?

ProGuard.

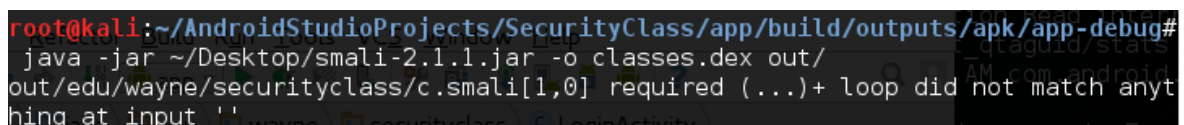
4.2 Can you still repackage the application using baksmali or smaltool? Justify your answer.

No, because we obfuscate the android application.



```
root@kali: ~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug/out/edu/wayne/secur...
File Edit View Search Terminal Help
root@kali:~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug/out/edu/wayne#
cd securityclass
root@kali:~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug/out/edu/wayne/
securityclass# ls
a.smali b.smali c.smali d.smali e.smali f.smali g.smali LoginActivity.smali
root@kali:~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug/out/edu/wayne/
securityclass# ./
2:52.273 16260-16260/edu.wayne.securityclass I/Choreographer: Skipped 103 frames! The application
3:00.073 16260-16260/edu.wayne.securityclass D/foo@example.com: foo@example.com
3:00.073 16260-16260/edu.wayne.securityclass D/hello: hello
3:00.787 16260-16260/edu.wayne.securityclass I/Choreographer: Skipped 55 frames! The application
3:02.092 16260-16267/edu.wayne.securityclass W/art: Suspending all threads took: 736.174ms
3:02.134 16260-16260/edu.wayne.securityclass I/Choreographer: Skipped 83 frames! The application
3:02.903 16260-16267/edu.wayne.securityclass W/art: Suspending all threads took: 41.569ms
3:05.792 16260-16271/edu.wayne.securityclass I/art: Background sticky concurrent mark sweep GC fr
3:05.801 16260-16271/edu.wayne.securityclass W/art: Suspending all threads took: 7.884ms
```

Figure 3: obfuscate



```
root@kali:~/AndroidStudioProjects/SecurityClass/app/build/outputs/apk/app-debug#
java -jar ~/Desktop/smali-2.1.1.jar -o classes.dex out/
out/edu/wayne/securityclass/c.smali[1,0] required (...) + loop did not match anyt
hing at input '
```

Figure 4: repackage fail