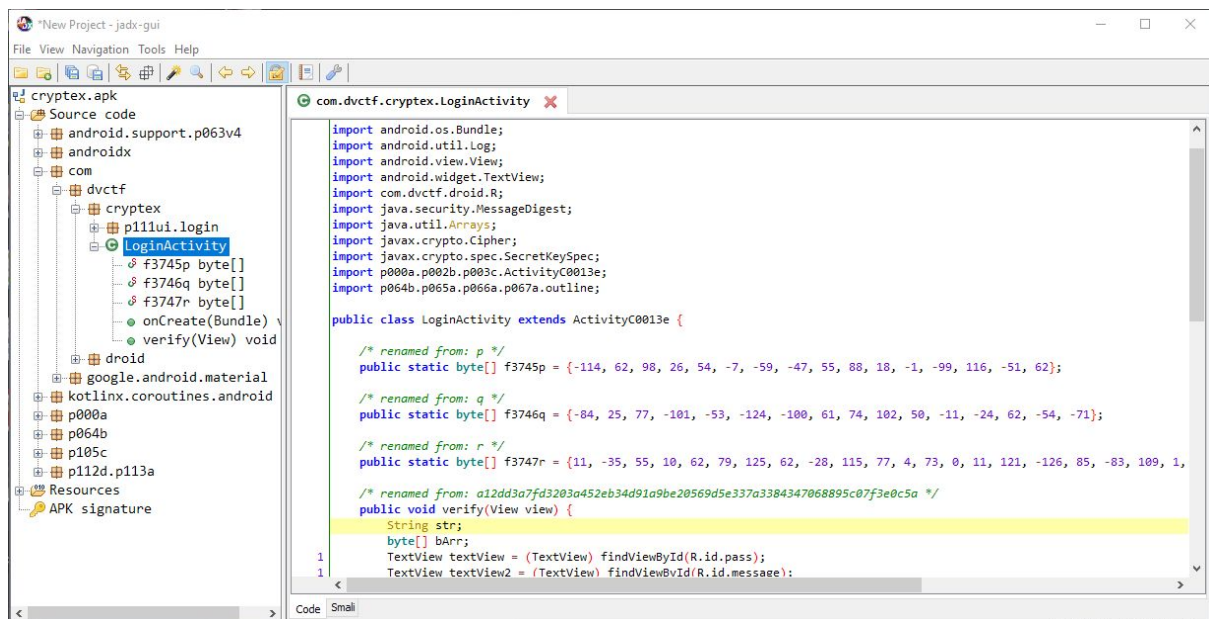


Cryptex Apk

Tools used for this challenge:

- jadx-gui
- Sublime text

For solving this challenge, I tried to unpack the apk with 7zip and convert the classes.dex to classes.jar, but it didn't work, the text was unreadable. So, I used **jadx-gui**:



The main class is **LoginActivity**. Copying, renaming and adapting the code, the class results in this file: [github](#)

To summarize the comparison process:

- The password entered by us is encrypted in a hash
- The password is then encrypted in aes. The aes key is created from a value stored
- At the end, a comparison is performed between our password and a stored password, the original password to guess.

So, to retrieve the right password, we have to:

- Take the password stored, used to perform the comparison
- Generate the aes key with the value stored
- Decrypt the password
- Show the hash
- Break the hash

The code used to do that is [here](#)