**App Name :** mpocket

**Package Name :** com.mpokket.app

**Version Code :** 100160

**Version Name :** 2.1.6

**Compile SDK version :** 28

**Build version code :** 28

**Minimum SDK version : 19**

**Target SDK version : 28**

1. This application is being validated for **spyware PHA**
2. Let us understand the definition of spyware again

Spyware track the activities of user’s mobile phone and collects the data like contacts, sms, call logs, history, files, audio etc and send it to the third parties or hacker without user consent.

1. Permissions responsible for spyware :

* android.permission.READ\_CONTACTS
* android.permission.RECEIVE\_SMS
* android.permission.READ\_SMS
* android.permission.READ\_EXTERNAL\_STORAGE
* android.permission.READ\_CALL\_LOG
* android.permission.RECORD\_AUDIO
* android.permission.READ\_CALENDER
* android.permission.ACCESS\_COARSE\_LOCATION
* android.permission.ACCESS\_FINE\_LOCATION
* com.android.browser.permission.READ\_HISTORY\_BOOKMARKS

1. Lets start reversing it.
2. Open the application in the JADX .

After opening, you can see the whole list of class files as mentioned in the screenshot below.

A screenshot of a computer

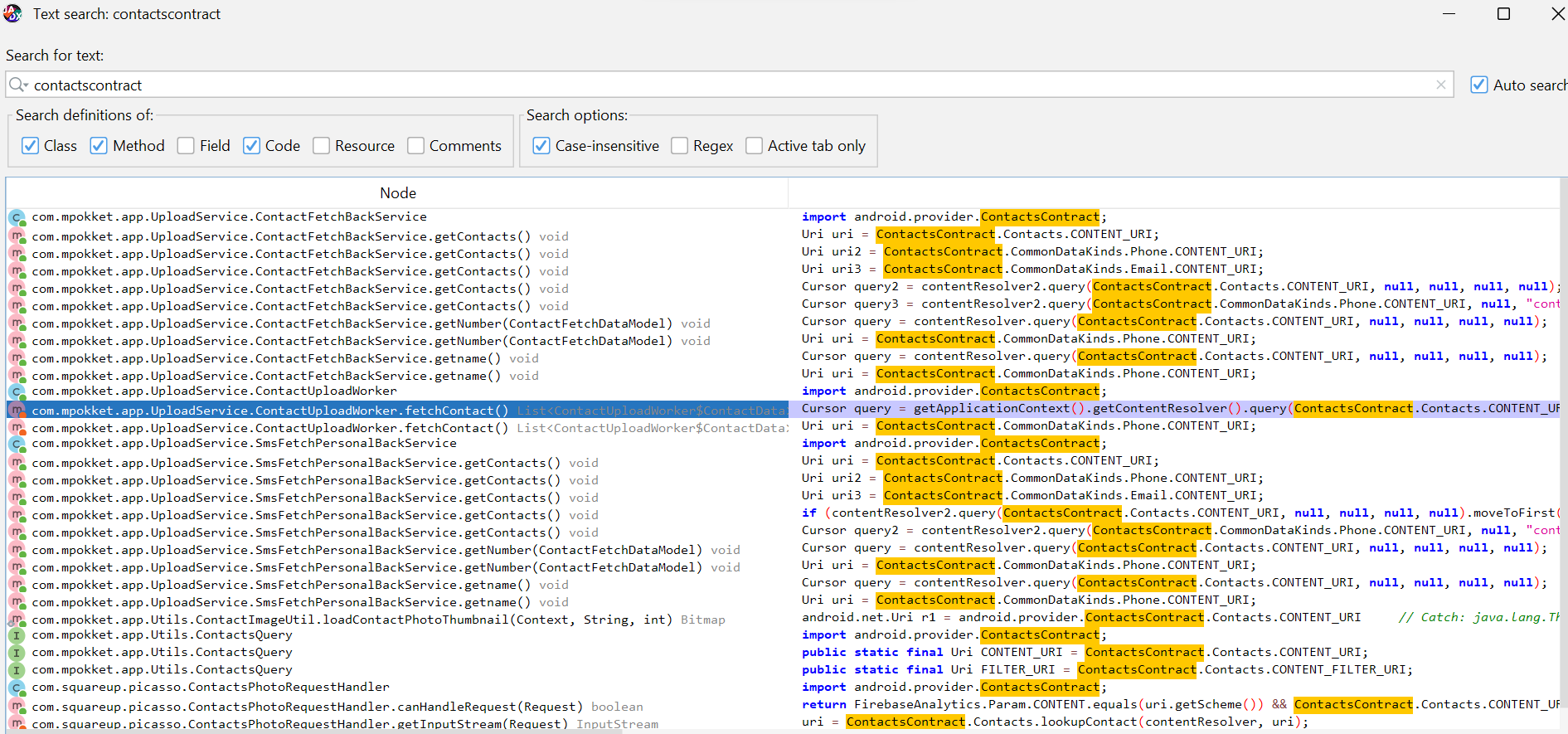
Description automatically generated

1. You can find READ\_CONTACTS permission at **line 22** which is suspicious relating to spyware

A screen shot of a computer

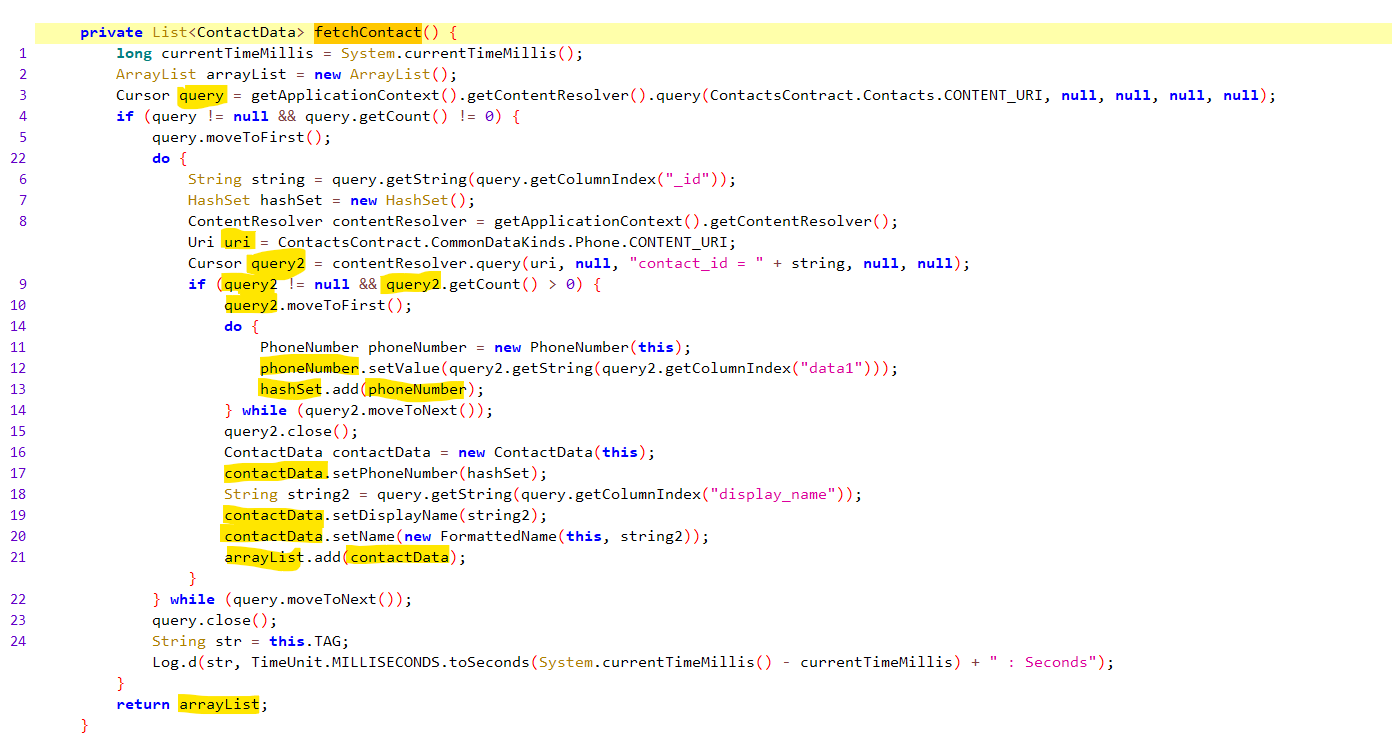
Description automatically generated

1. Search contactscontract in search bar and click on query which is being highlighted in the given below screenshot.



1. Here contact is added to arraylist and return by fetchContact( ).

So check for usage of fetchContact( ) method.



1. Here fetchContact( ) is assigned to fetchContact and baseurl is located.





A yellow and black text

Description automatically generated