**App Name :** Mobile Monitor App

**Package Name :** com.android.mms

**Version Code :** 13150000

**Version Name :** 13

**Compile SDK version : 33**

**Build version code : 33**

**Minimum SDK version : 29**

**Target SDK version : 33**

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.

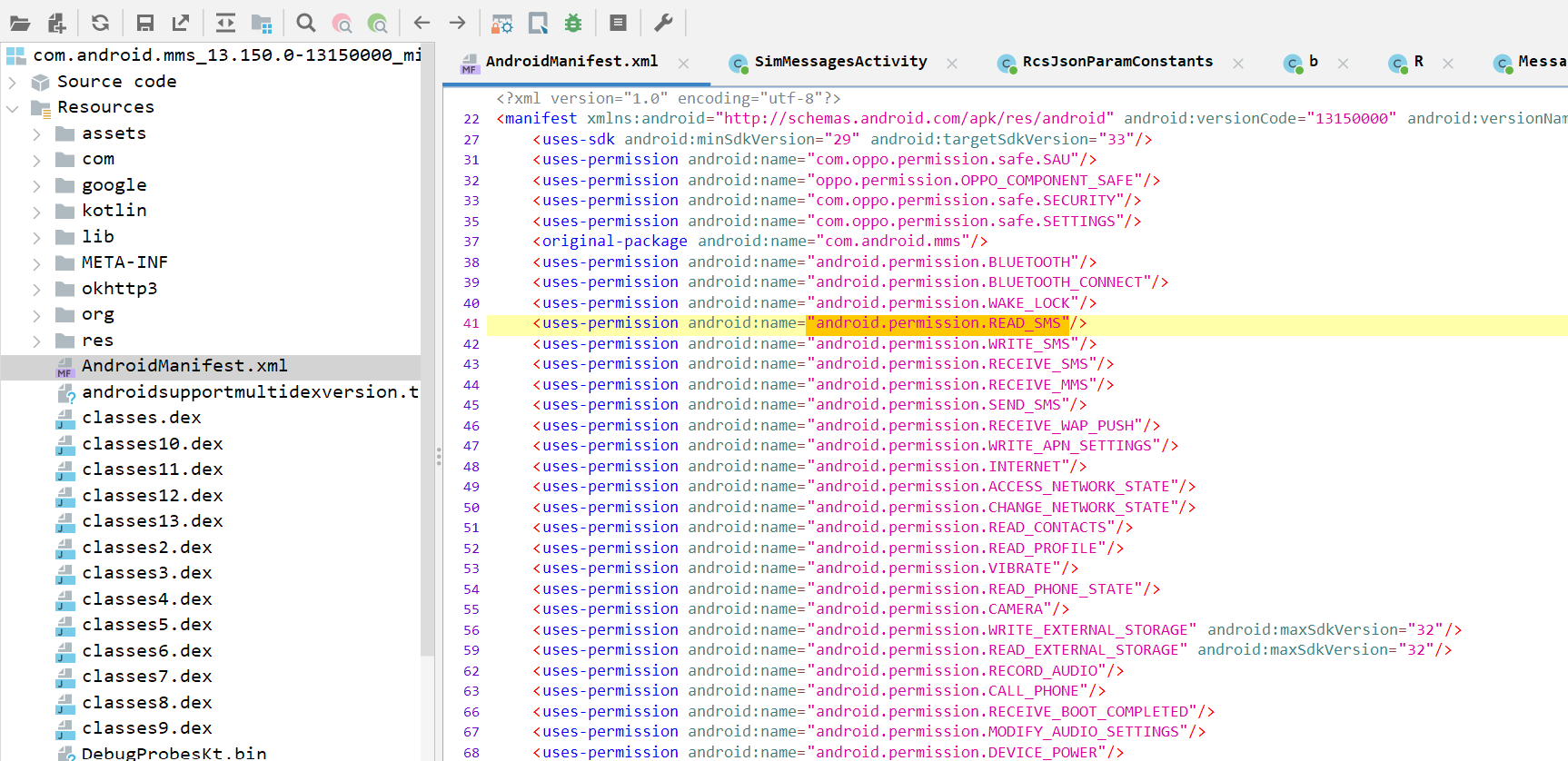
1. Permissions responsible for spyware :

* 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 doing RE.
2. Open the application in the JADX .

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

Click on AndroidManifest.xml to check the permissions.

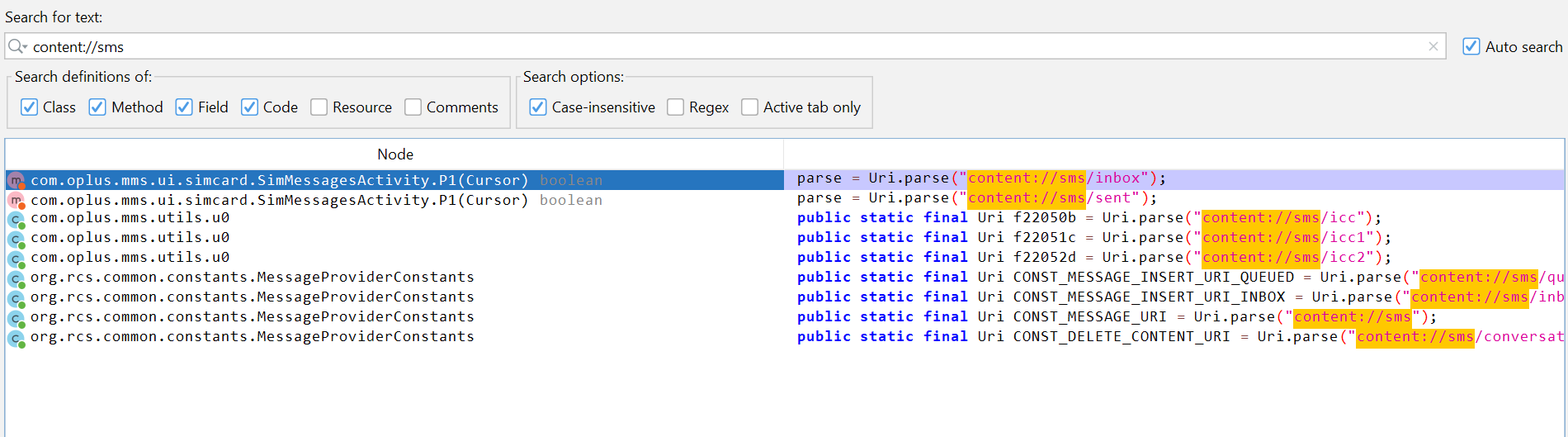




Here we can see that READ\_SMS and READ\_CONTACTS permission is there at line 41 and 51.

We will check for read\_sms then we will check read\_contacts.

1. Now click on  button in JADX to find for sms usage.
2. Now search content://sms as shown in below screenshot.



From the list we check the first one as it is defining uri of sms.

1. Double click the first list



We will check the declaration of this method



1. Here we can see that H1( ) method is defined.

We will check the declaration of this method.

A computer code with text

Description automatically generated with medium confidence

1. Now, we will check declaration of c( ) method.

A screenshot of a computer

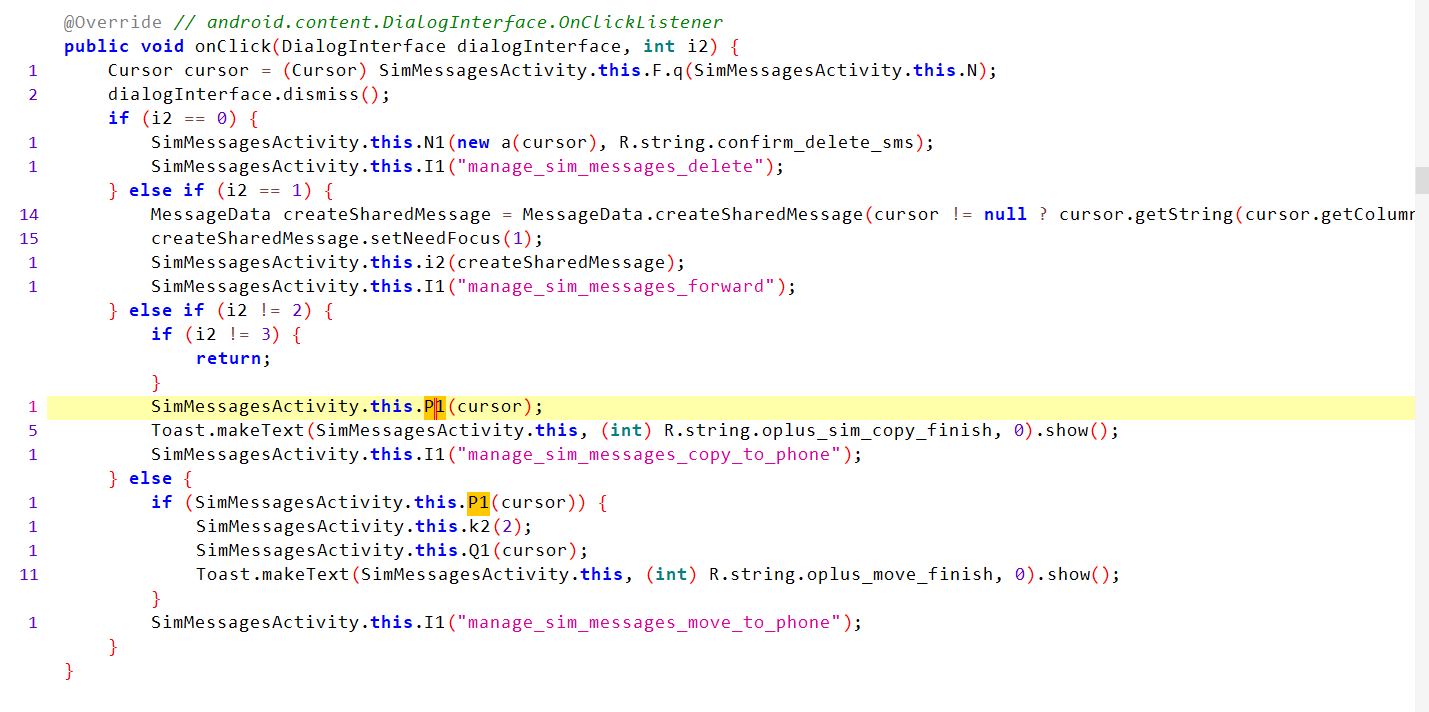
Description automatically generated

From here we can see that data is being inserted into sqlLiteDatabase.

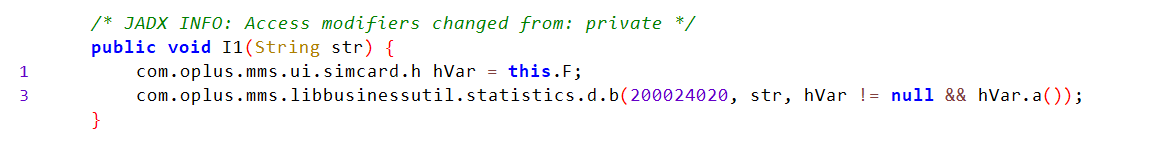
1. We will check the usage of P1( ) method



1. We will check SimMessagesActivity.



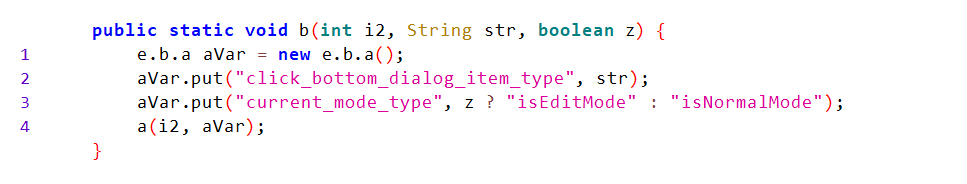
1. Now will check the I1( ) method.





1. Since str is being passed into b( ) method.

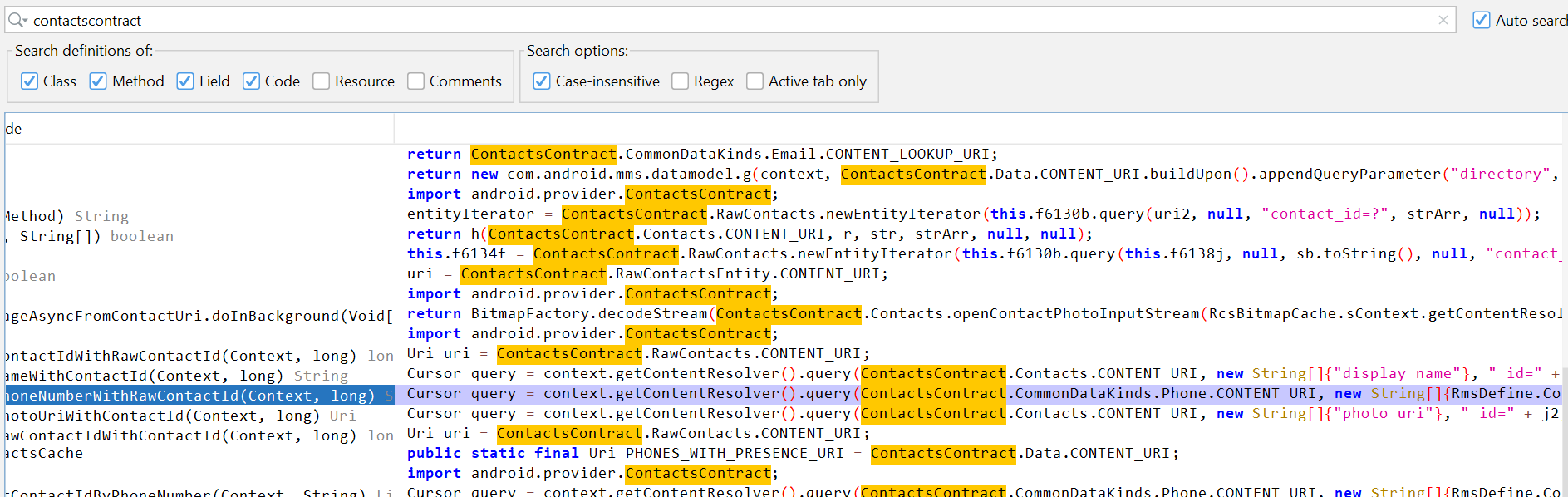
We will check declaration of b( ) method.



From here we can not derive any conclusion.

Now we will check READ\_CONTACTS permission.

1. Search contactscontract in the search bar



1. From the list we will select CommonDataKinds.Phone as it is returning cursor.

Here we can see that arrayList is being returned. So we will check the usage of getPhoneNumberWithRawContactId( )

1. Here we can see that arrayList is being returned. So we will check the usage of getPhoneNumberWithRawContactId( )

A screenshot of a computer code

Description automatically generated



1. Here we can see that getPhoneNumberWithRawContactId( ) is returned in getPhoneNumberWithRawContactId( ) method as shown in below screenshot.

A screenshot of a computer code

Description automatically generated



1. Now we will check usage of getPhoneNumberWithContactId( ) method.
2. The above method is not used .

So from here we are not able to reach any link on which contact is being sent.