**App Name :** Calculator

**Package Name :** calccalculator.calccalculator

**Version Code :** 5

**Version Name :** 1.0.1

**Compile SDK version :**

**Build version code :**

**Minimum SDK version : 16**

**Target SDK version : 27**

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

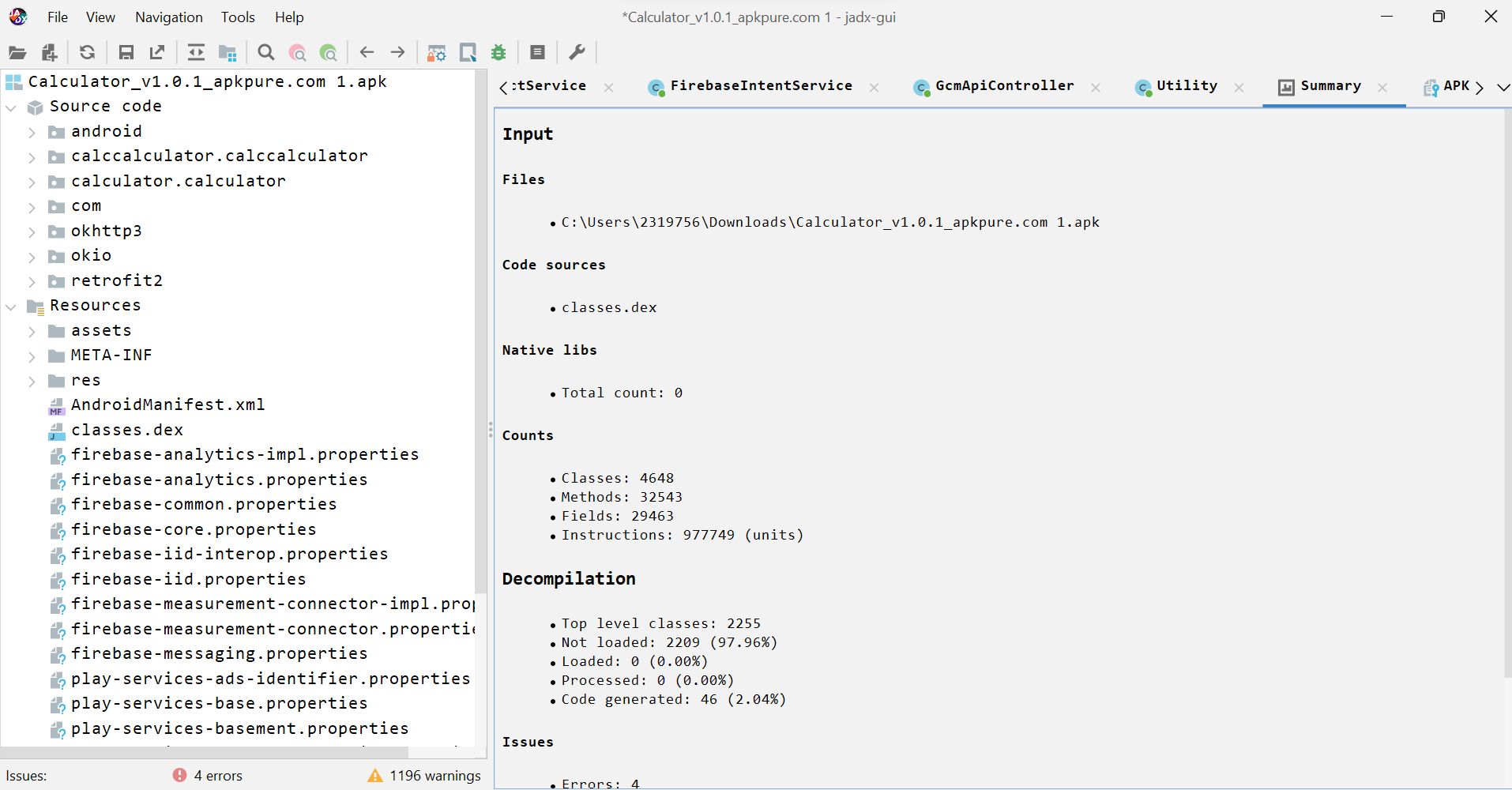
Spyware track the activities of user’s mobile phone and collects the data like contacts, sms, call logs, history, files, audio etc and send it to the third parties or hacker without user consent.

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

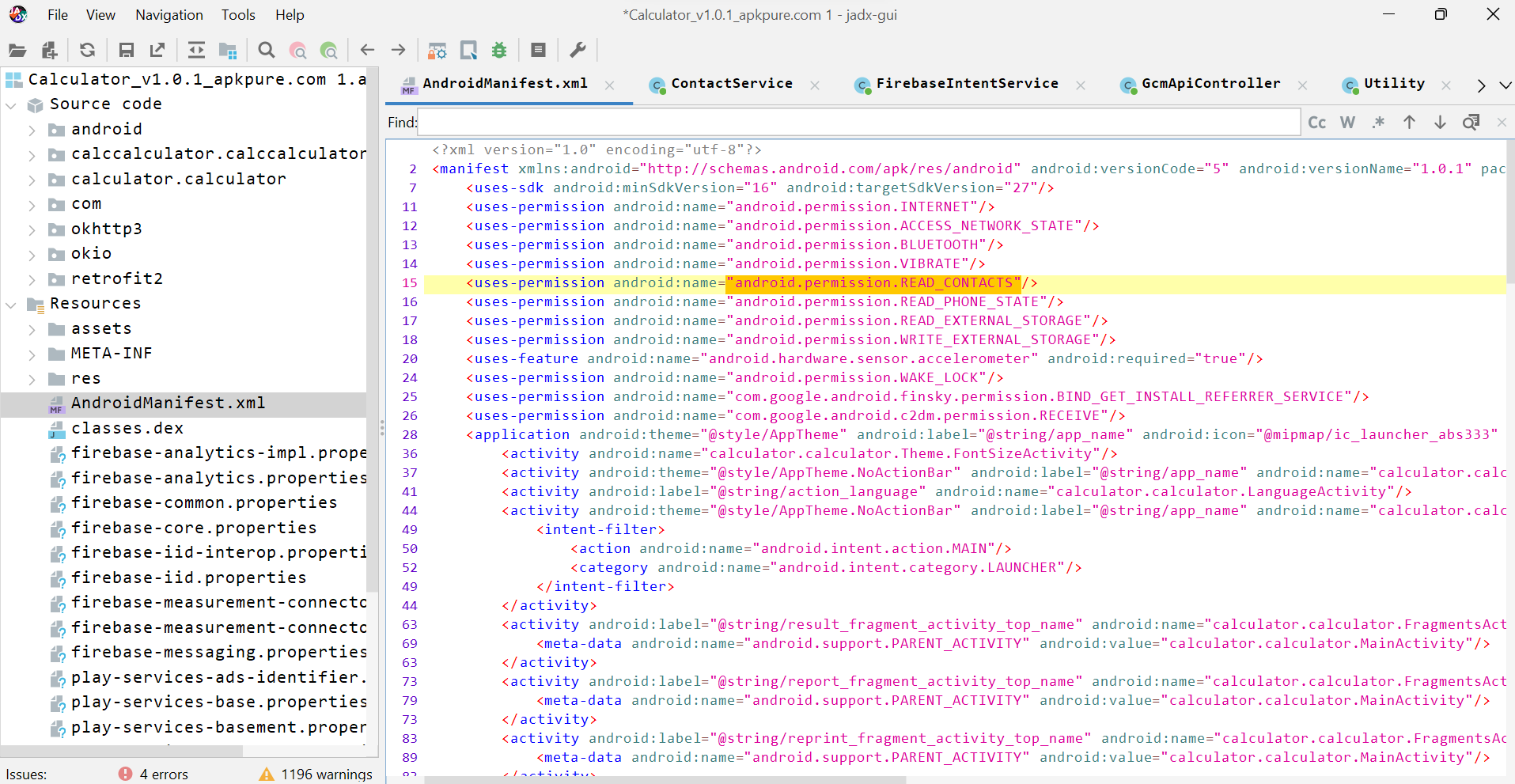
1. Lets start reversing it.
2. Open the application in the JADX .

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



1. Double click the androidmanifest.xml

After opening the androidmanifest.xml file in JADX you can find READ\_CONTACTS permission in androidmanifest.xml at **line 15**



A screen shot of a computer

Description automatically generated

so here you can see the READ\_CONTACTS permission which is suspicious relating to spyware.

1. Now click on  button in JADX to find for Contacts usage.
2. Search for ContactsContract as mentioned in below screenshot .

ContactsContract defines an extensible database of contact related information. The contact between the contents provider and the applications.

A screenshot of a computer

Description automatically generated

Make sure class, method, code, field and case-insensitive field is checked.

1. Go for **query** since you can find CommonDataKinds.Phone.CONTENT\_URI,new String[]{“data1”}.

Here data1 means it contains phone no.

A screenshot of a computer

Description automatically generated

1. Double click the query2 line. Here you can see contactInfo is being added to the arraylist and that arraylist is returned to the getContacts( ) method

A screenshot of a computer code

Description automatically generated

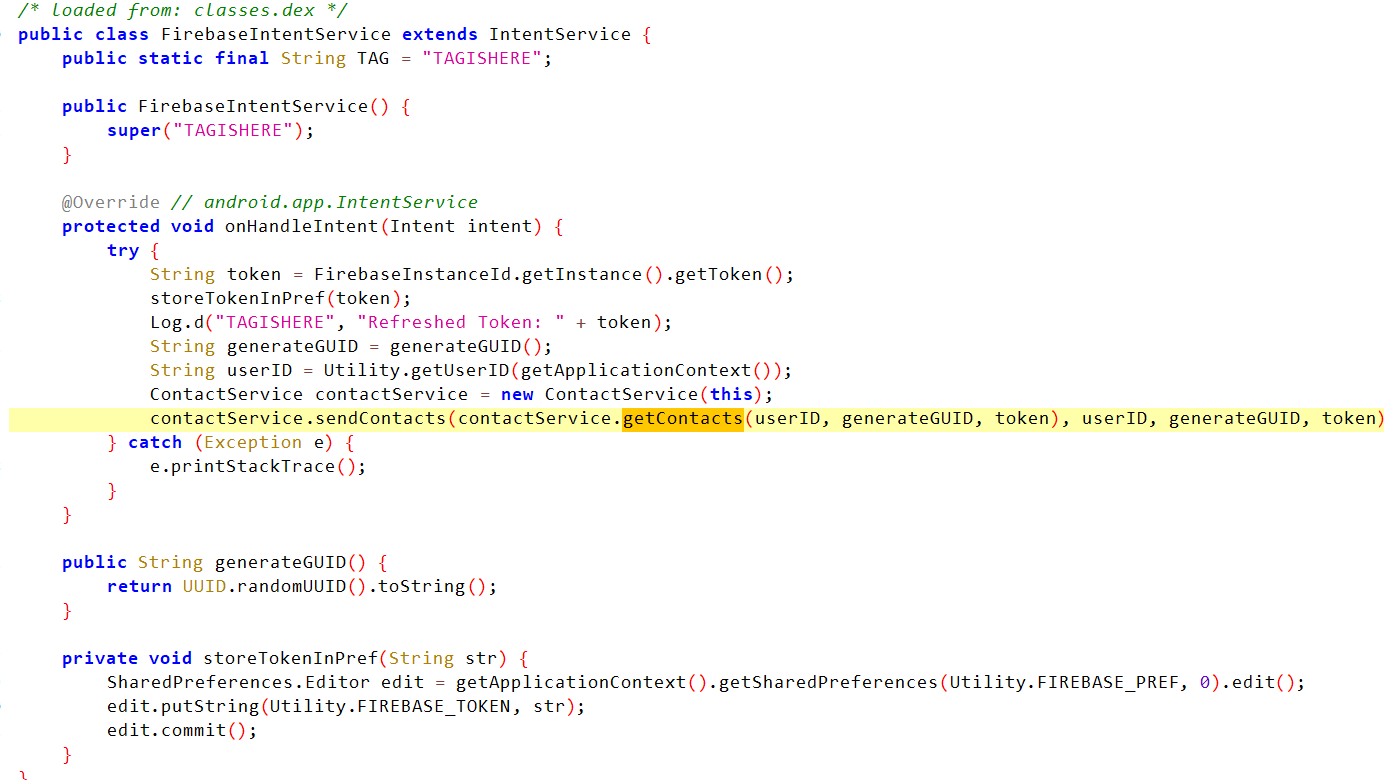
g. Right click on getContacts( ) method and select find usage(x) to know where the getContacts( ) method is being used.

A screenshot of a computer

Description automatically generated

1. getContacts( ) is being passed in sendContacts( ) of contactService object.

Right click on sendContacts( ) and click on go to the declaration(d) to know the functionalities of sendContacts( ) method.



1. ContactInfo is passed in the createSyncContactsRequest( ) in the form of arrayList.

Go to declaration of this method to know the functionalities of the method.

A screenshot of a computer code

Description automatically generated

1. base\_url\_post\_contact is concatenated with params.

So go to declaration of base\_url\_post\_contact

A screen shot of a computer code

Description automatically generated

1. Here we can find that contact is being sent to some external server i.e. http: // mpaaap.com/app/u.php which confirms that this app is a spyware.