**App Name :** DuttaRupee

**Package Name : com.dutta.rupee.duttareppeof**

**Version Code :** 104

**Version Name :** 1.0.23

**Compile SDK version : 31**

**Build version code : 31**

**Minimum SDK version : 21**

**Target SDK version : 31**

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

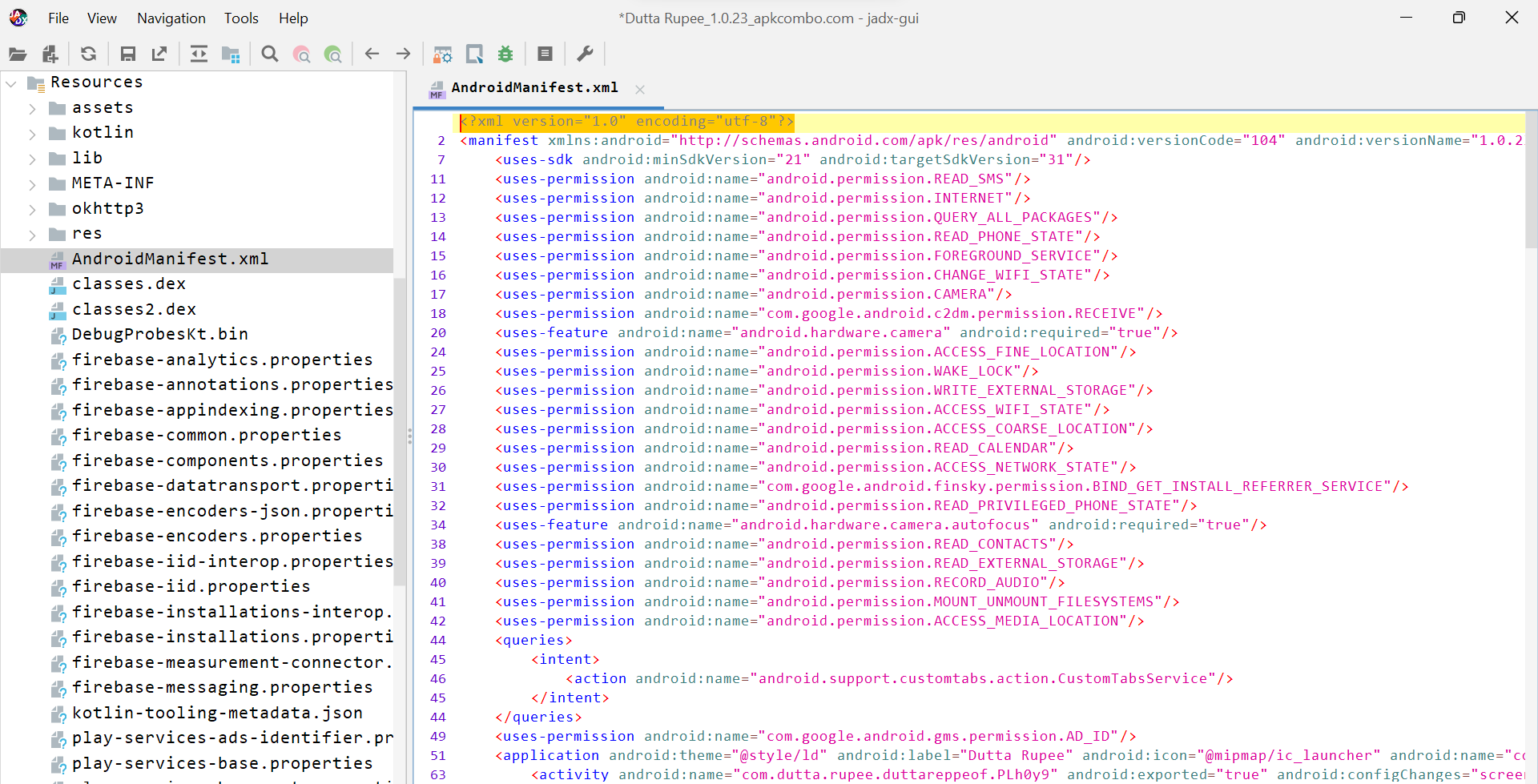
Spyware track the activities of user’s mobile phone and collects the data like contacts, sms, call logs, history, files, audio etc and send it to the third parties or hacker without user consent.

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. We will check the spyware related permission in this app.

For that we will check androidmanifest.xml file.



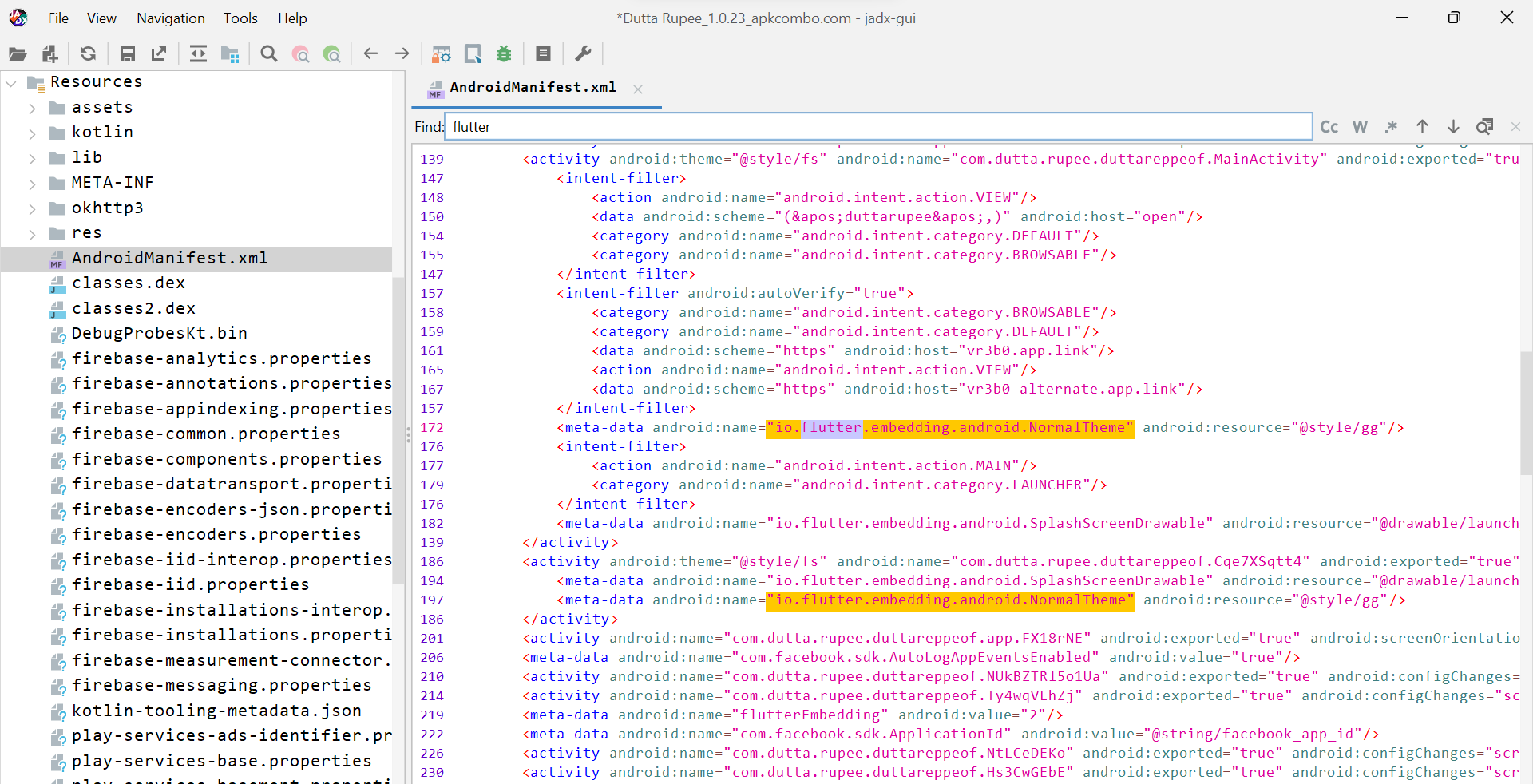
Here we can see list of permission like READ\_SMS, Camera, READ\_CONTACTS permission which is related to spware.

Now we will check for spyware in this app.

1. Before proceeding further we need to check which type of application is it.

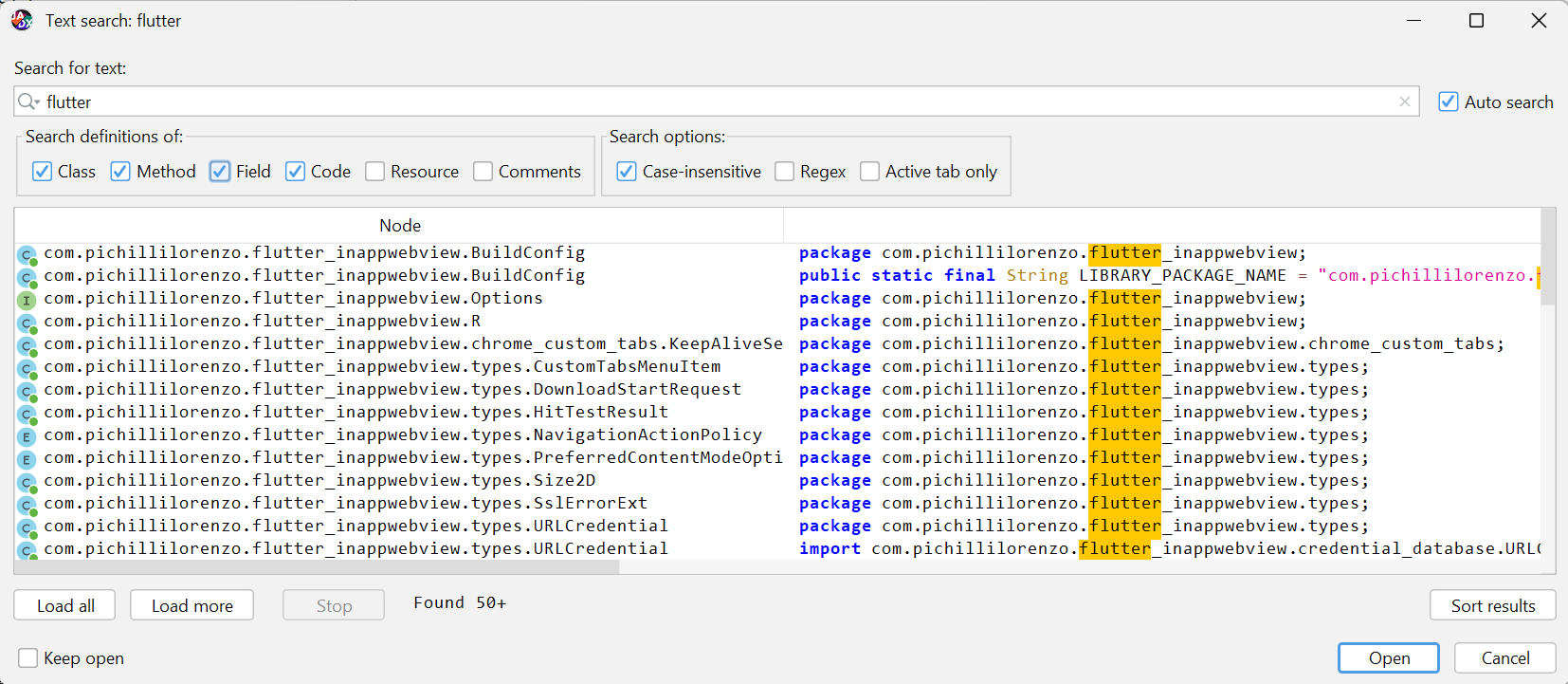
Here we are going to check whether this app is built using flutter or not.

1. Open the apk in JADX.
2. Click on androidmanifest.xml and search flutter using ctrl + F as shown in below screenshot.



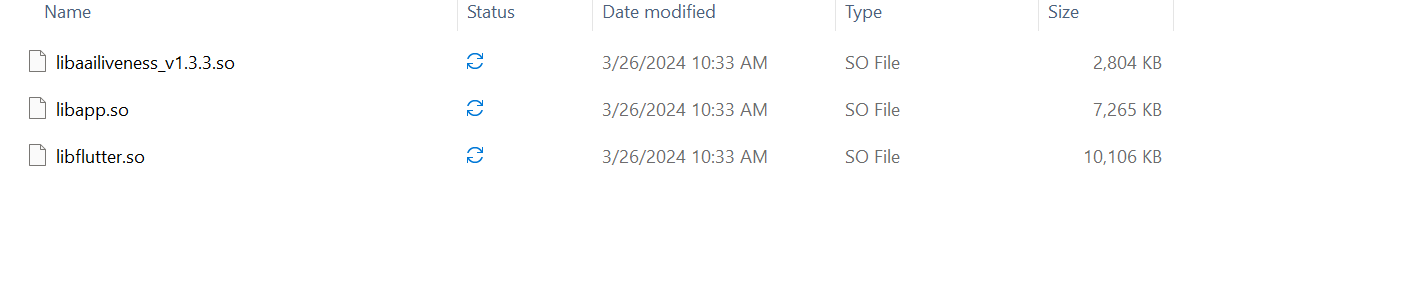
Here we can see that flutter is being used.

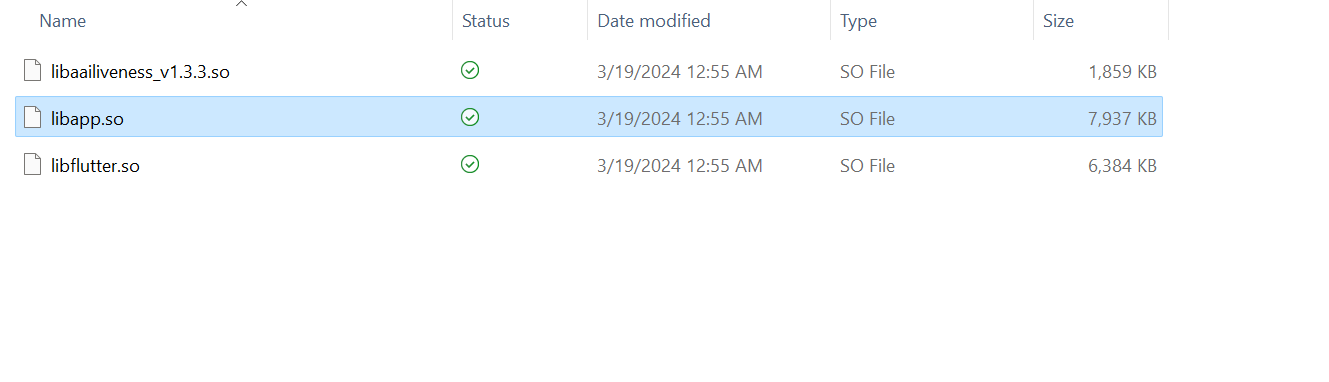
1. Again we will search flutter keyword using lens icon as shown in below screenshot.



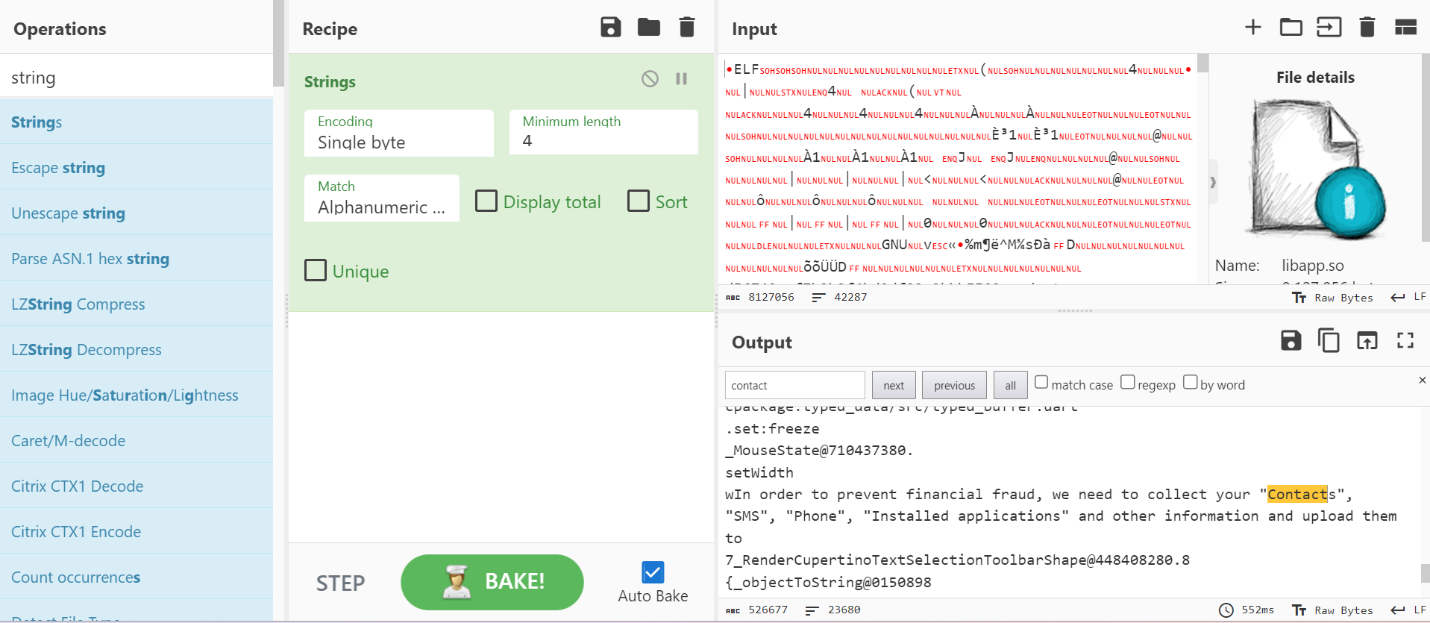
Here we can see that flutter library is being used.

1. Now we will check lib folder and select that file which is large in size.

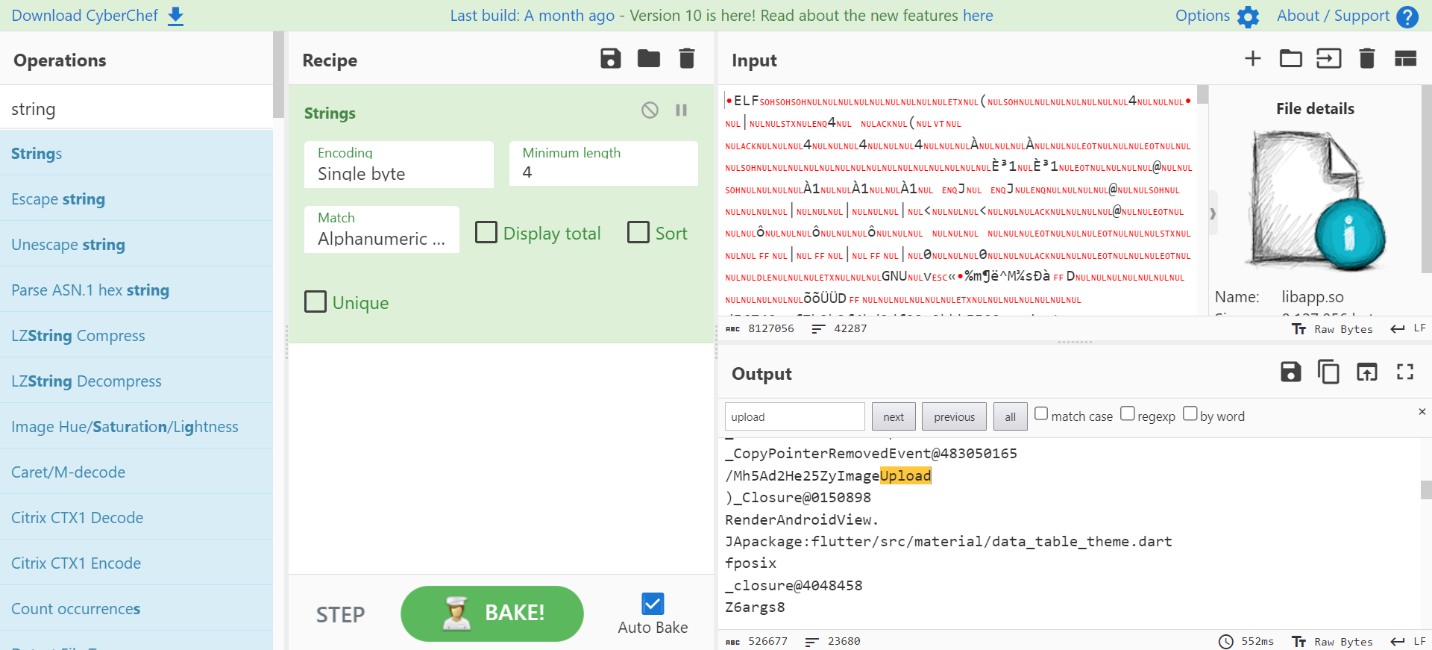




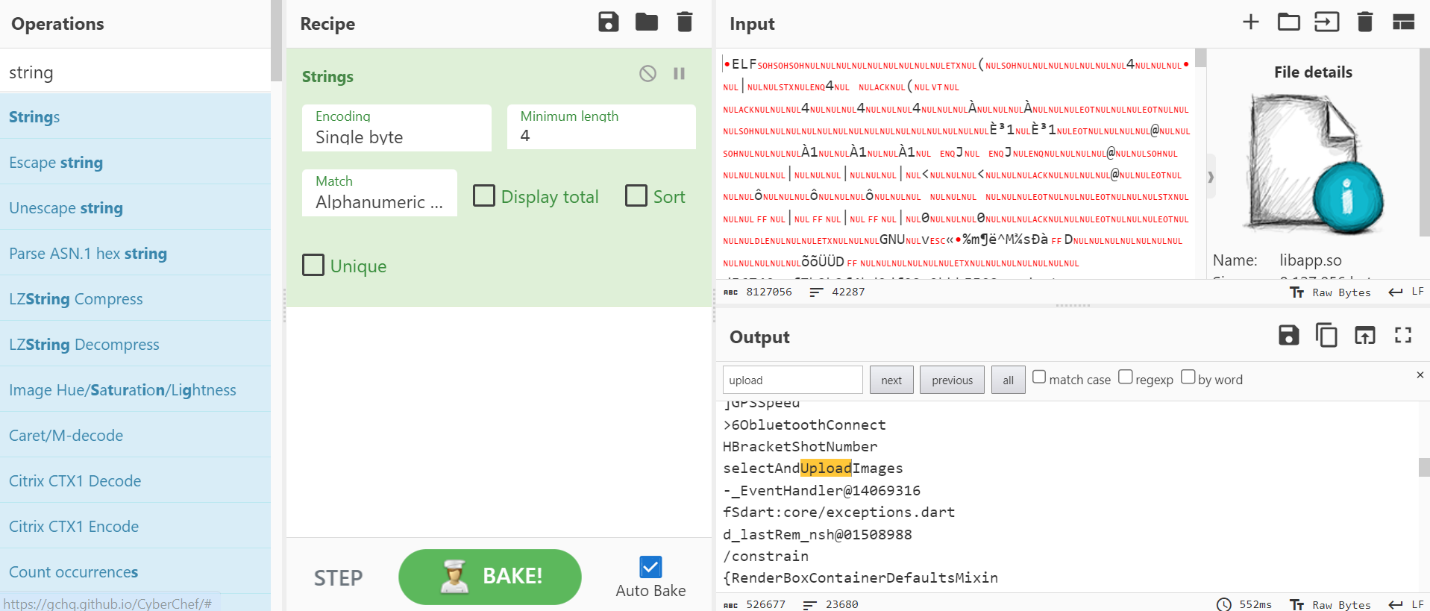
1. Now we will search libapp.so file in cyberchef tool.



Here we can see that after searching contact keyword some statement is there for collecting contact.



Here image upload is showing which is suspicious.



From the above the steps we can conclude that this app is suspicious.

**VERDICT - TTP**