**App Name :** Elector

**Package Name :** com.bosonet.elector

**Version Code :** 4195088

**Version Name :** 7.31.136

**Compile SDK version : 29**

**Build version code : 29**

**Minimum SDK version : 16**

**Target SDK version : 29**

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

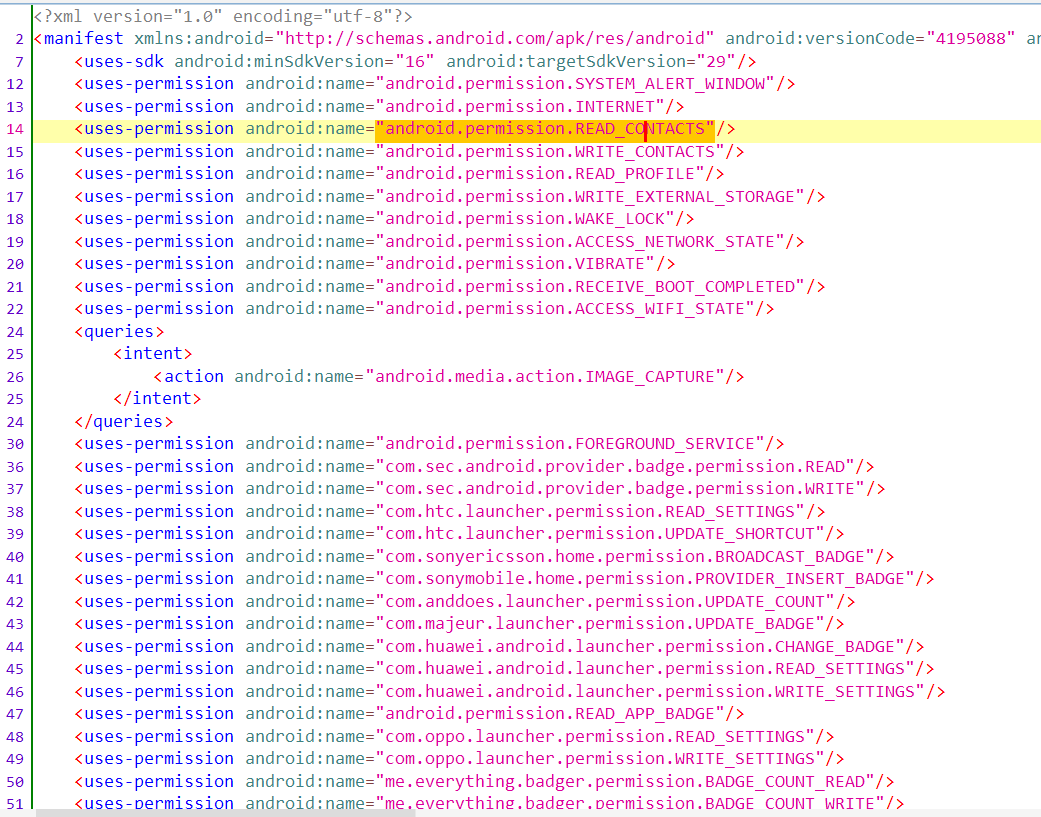
Spyware track the activities of user’s mobile phone and collects the data like contacts, sms, call logs, history, files, audio etc and send it to the third parties or hacker without user consent.

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.



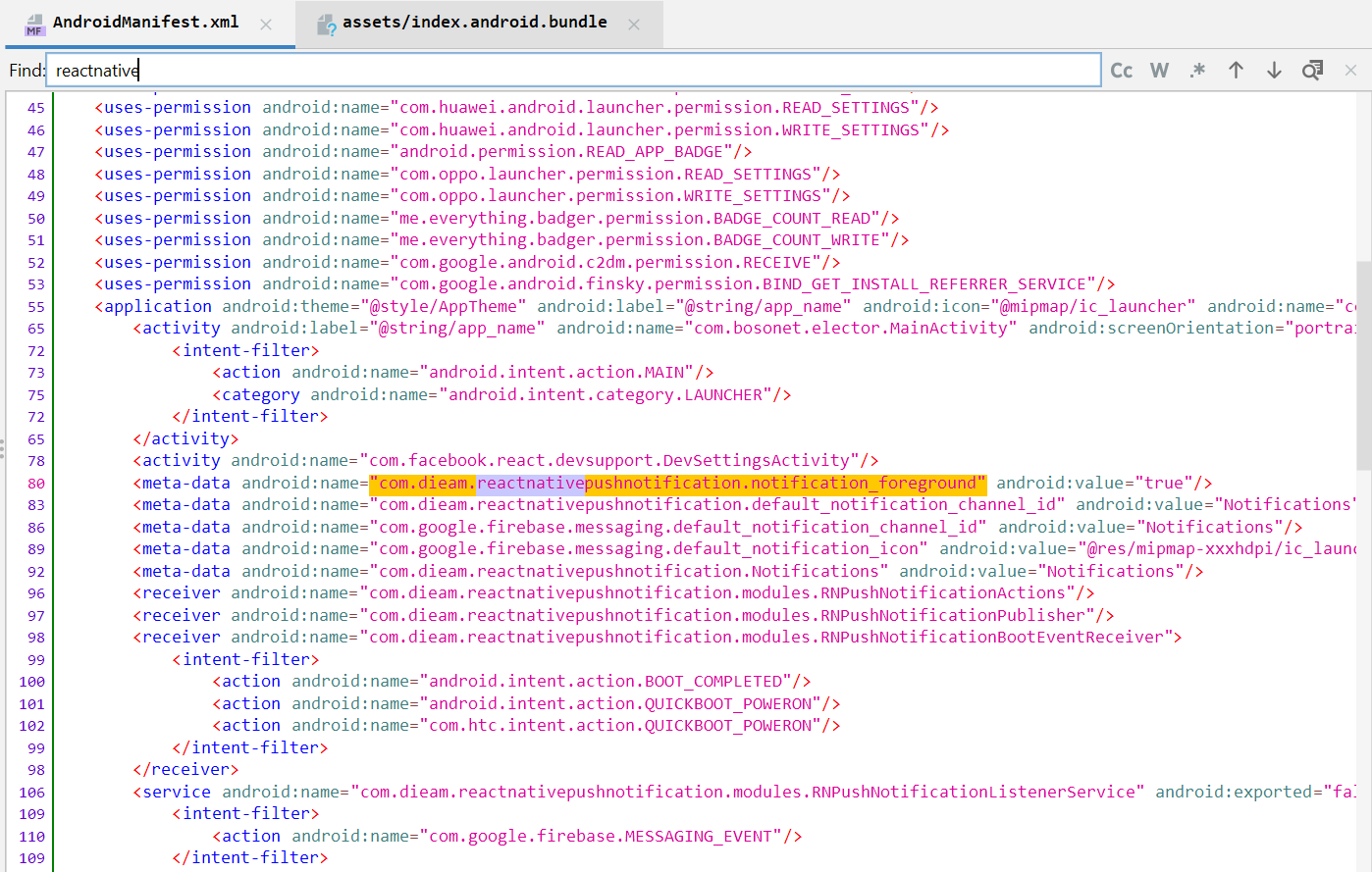
Here we can see READ\_CONTACTS permission which is related to spyware.

Now we will check for spyware in this app.

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

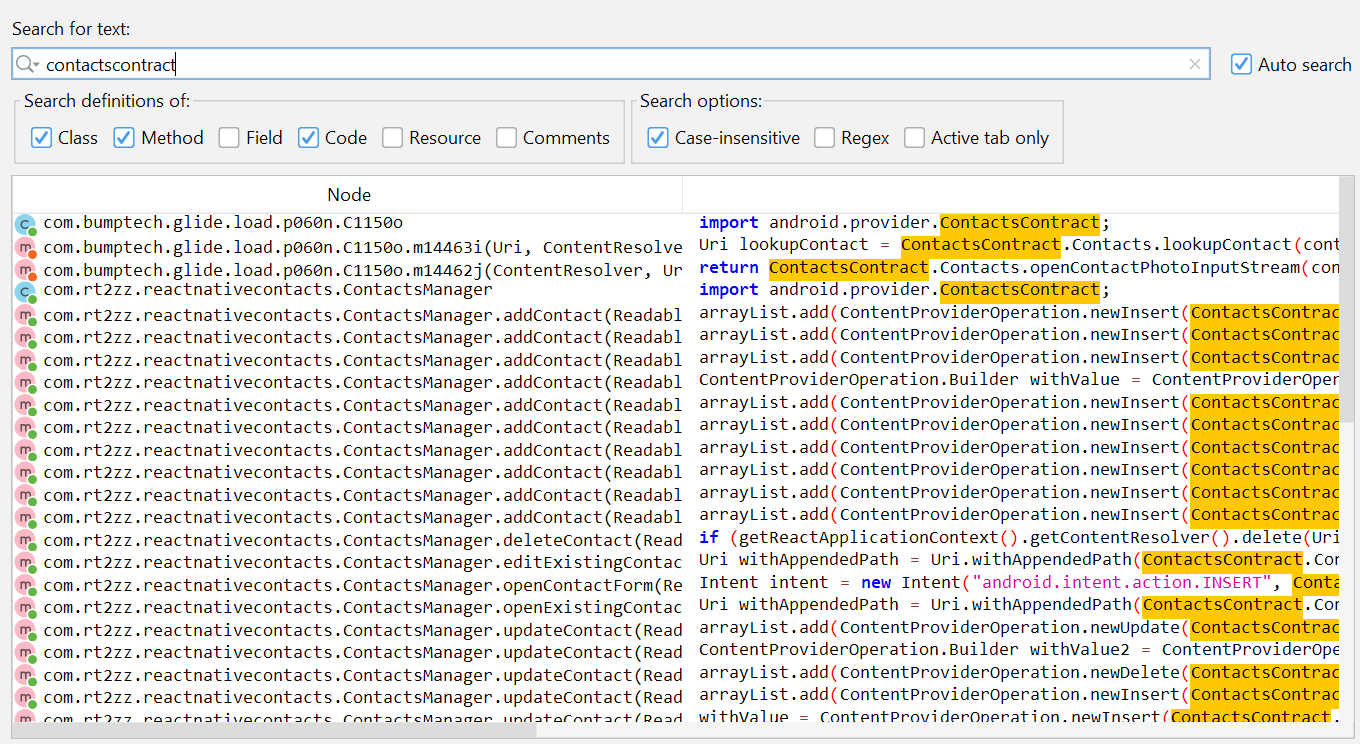
Here we are going to check whether this app is react native or not.

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



Here we can see that reactnative is being used.

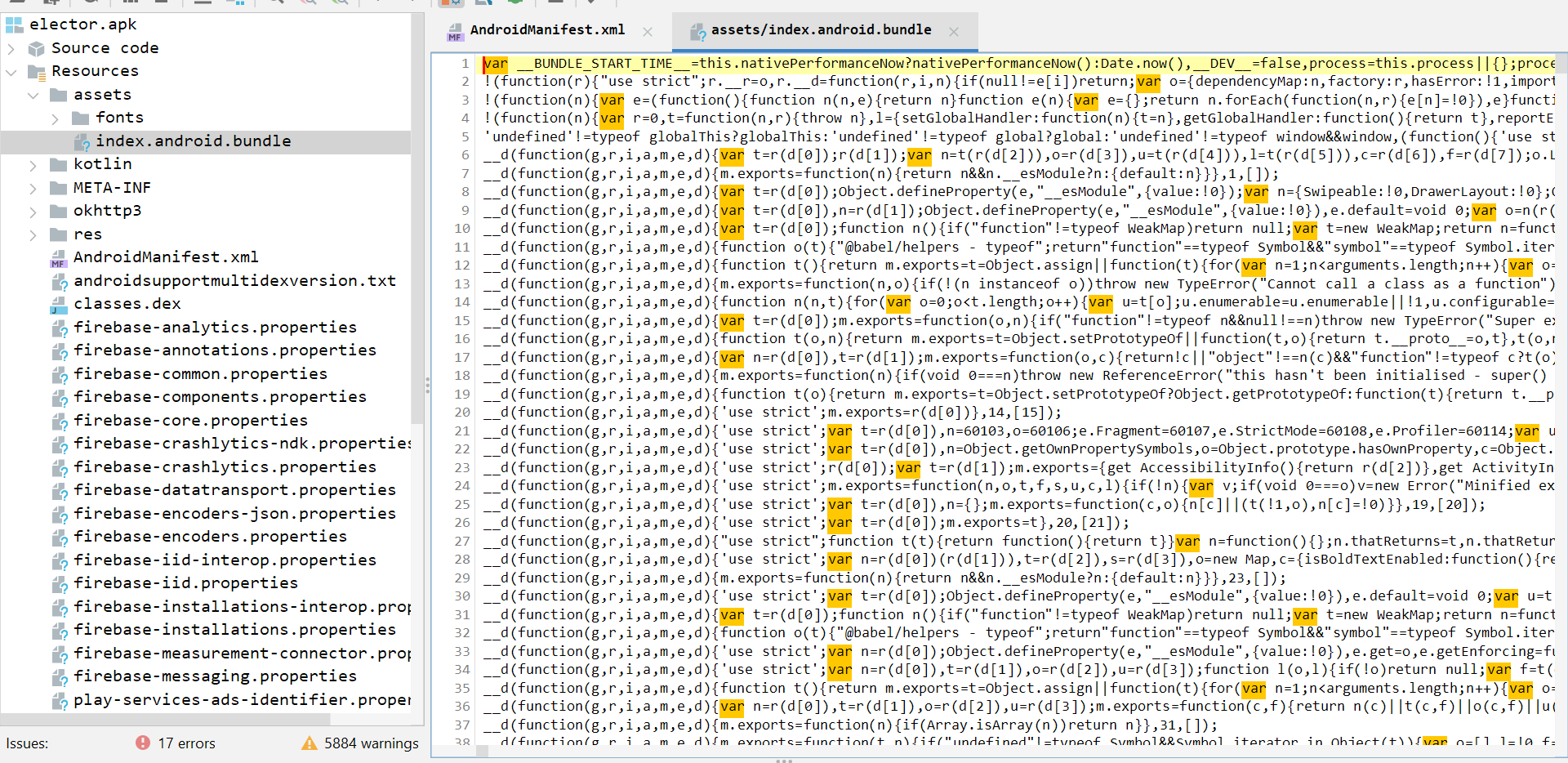
1. Again we will search “contactscontract” keyword using lens icon as shown in below screenshot.





Here we can see that reactnative library is being used.

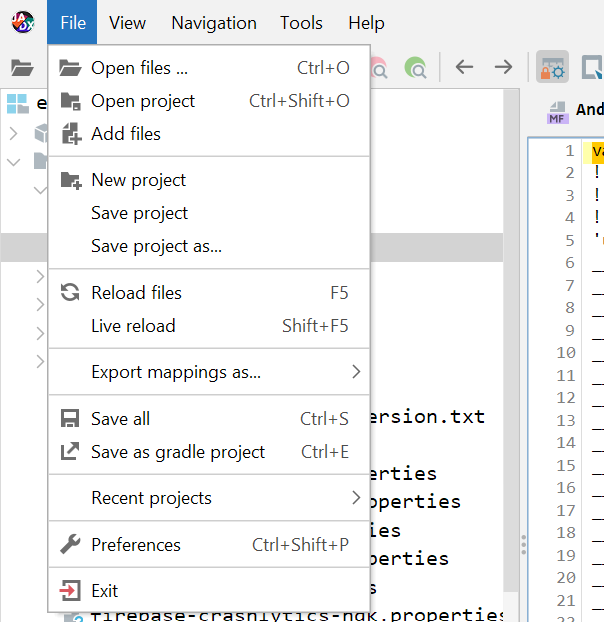
1. Now we will check the bundle file in asset folder ( Resources -> assets -> index.android.bundle )



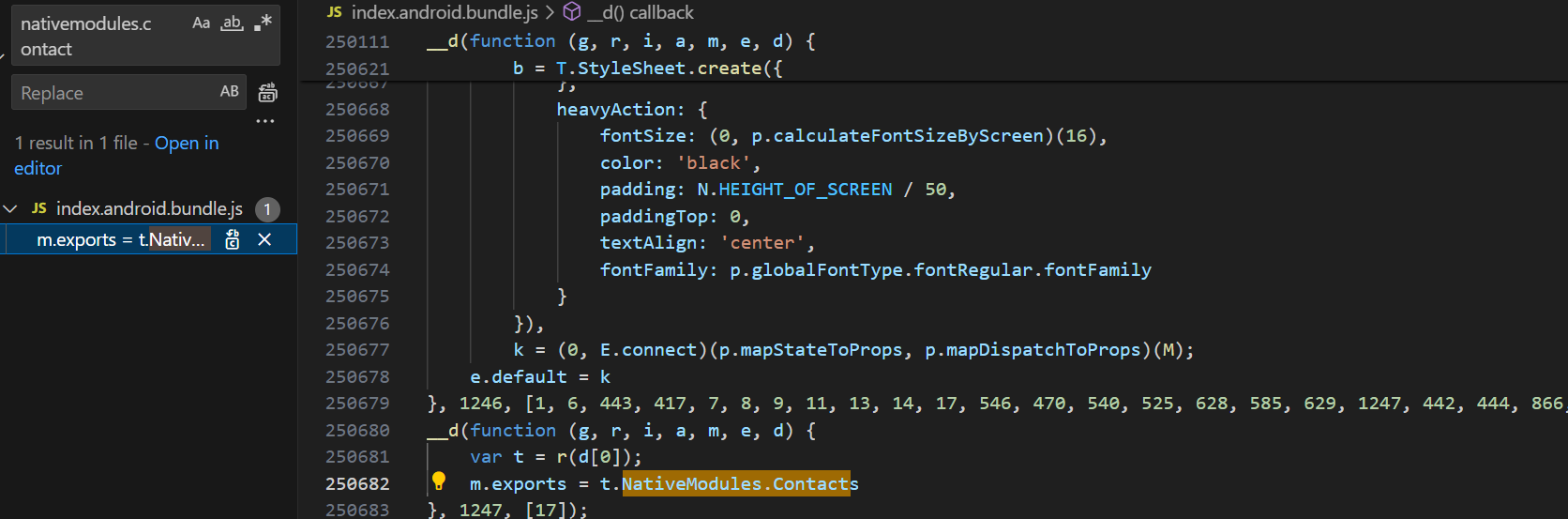
Here we can see index.android.bundle file and also it is human readable.

So from the above steps it is confirmed that this app is react native application.

1. Now we will check NativeModules.Contacts in index.android.bundle for that do saveAll in jadx.



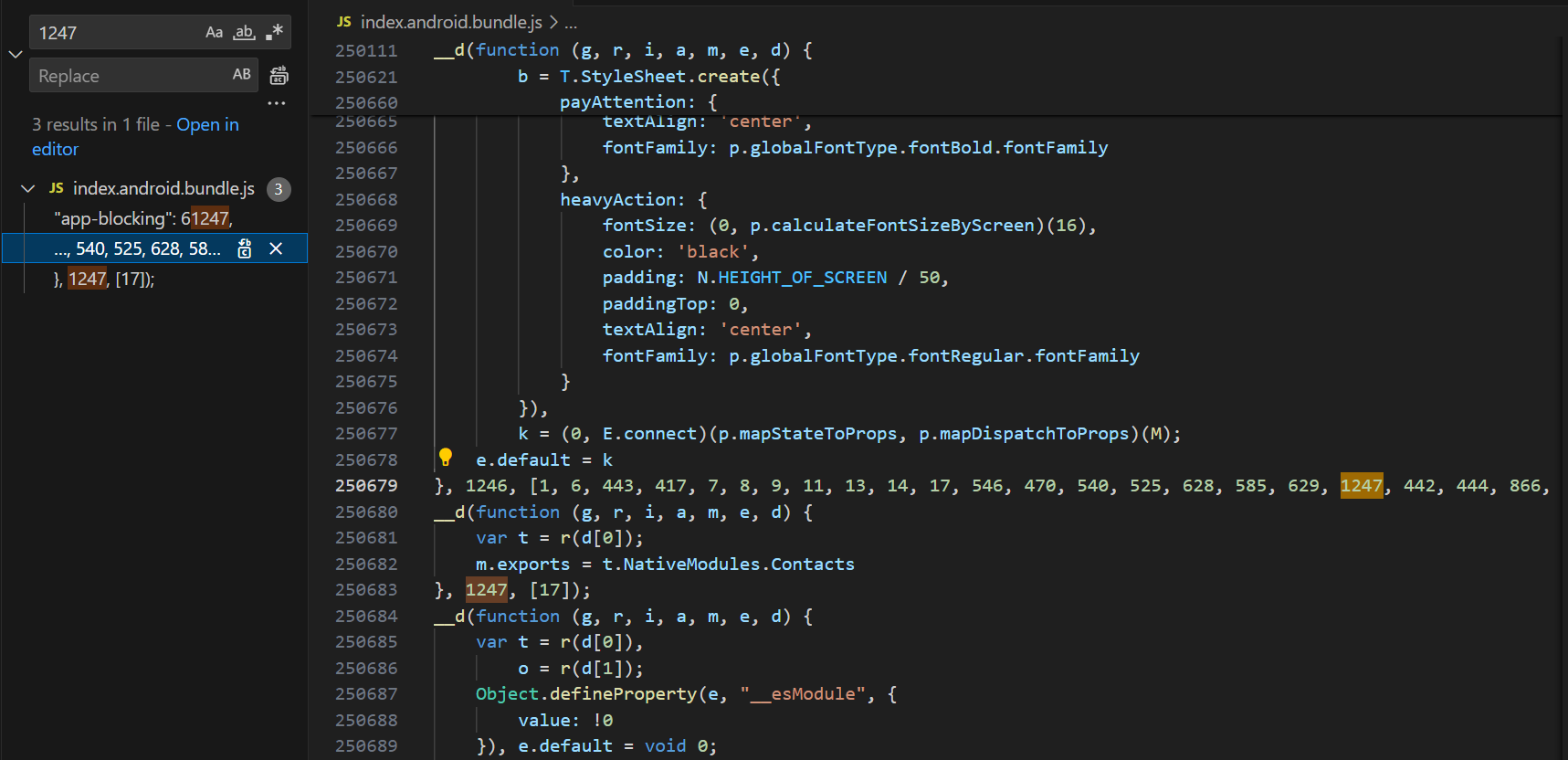
1. Open the saved file in vs code and search NativeModules.Contacts



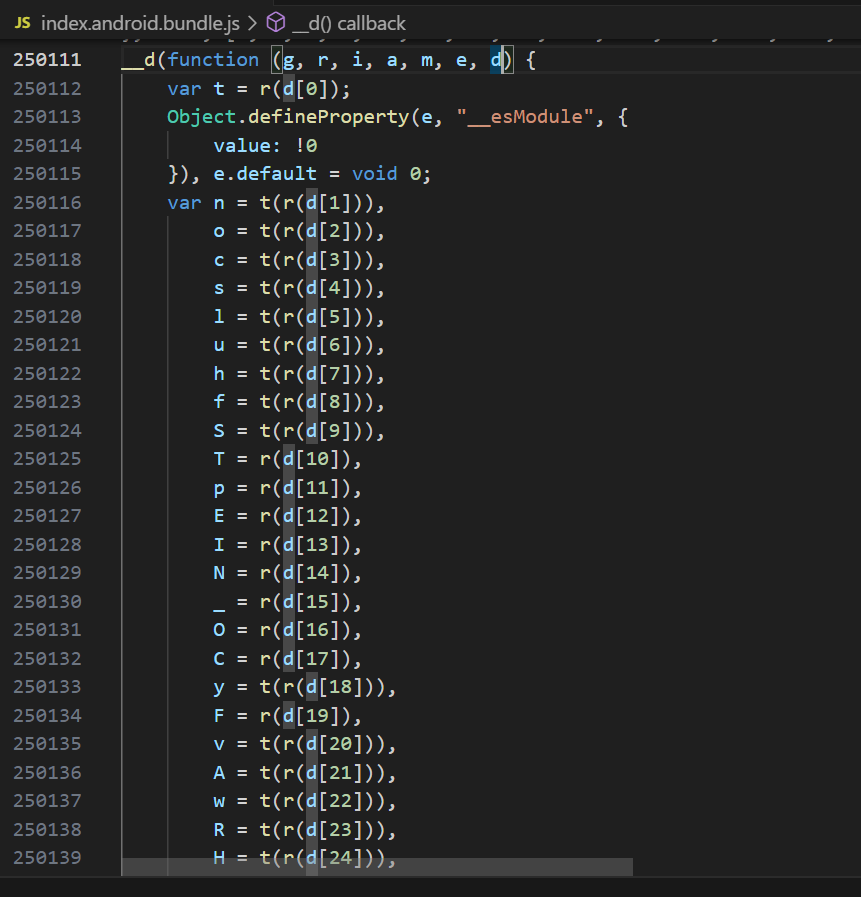
Here nativemodules.contact is searched

Here we will follow 1247 variable.

1. Now we will search 1247 go with that option which is used in array.



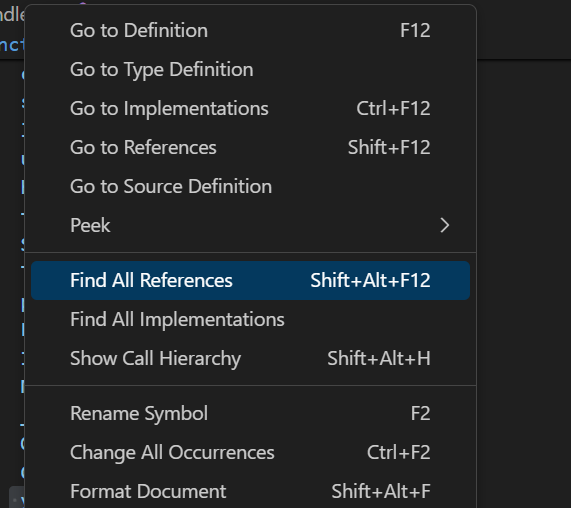
1. Now we will check position of 1247 in function and check that variable as shown in below screenshot.



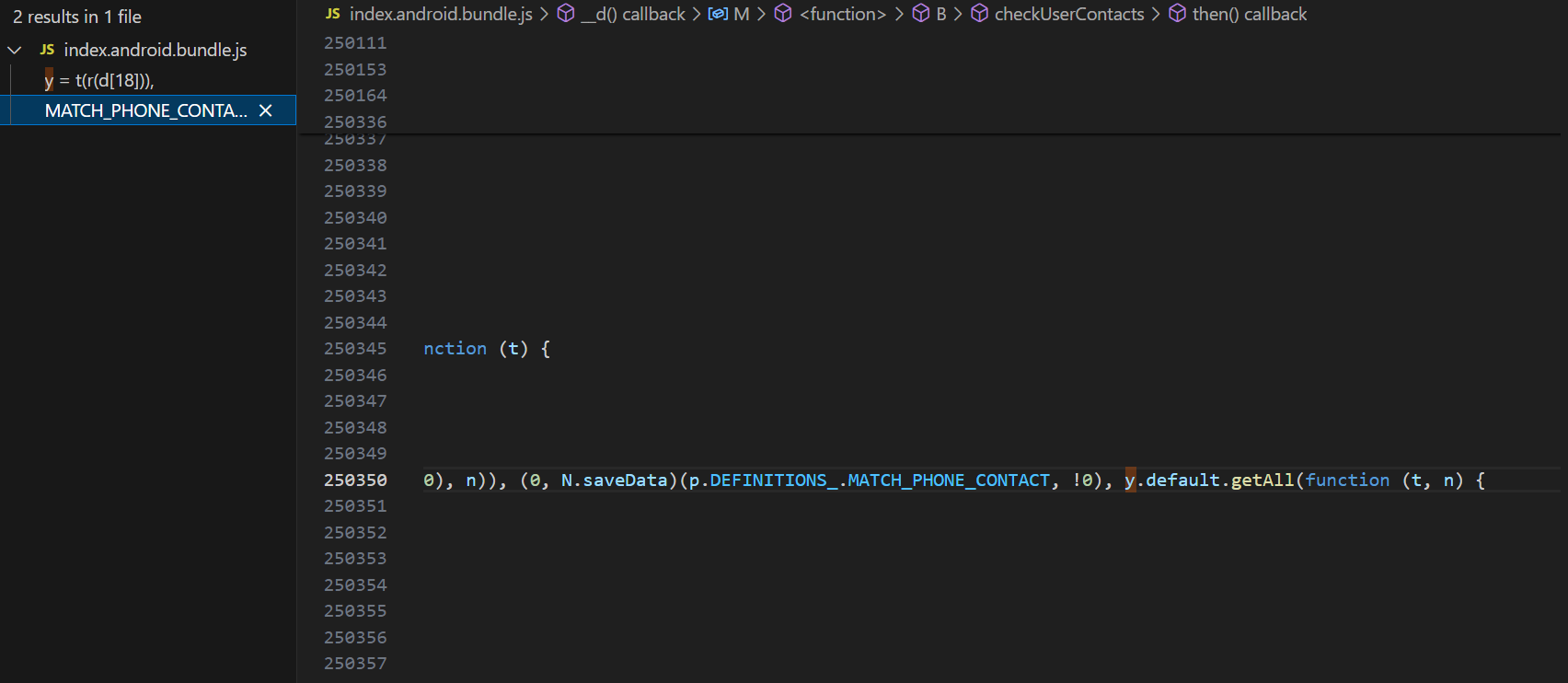


Since the position of 1247 in array is 18 here we will check 18th position variable and we will get y.

1. Right click the y variable and check Find all references as shown in below screenshot.



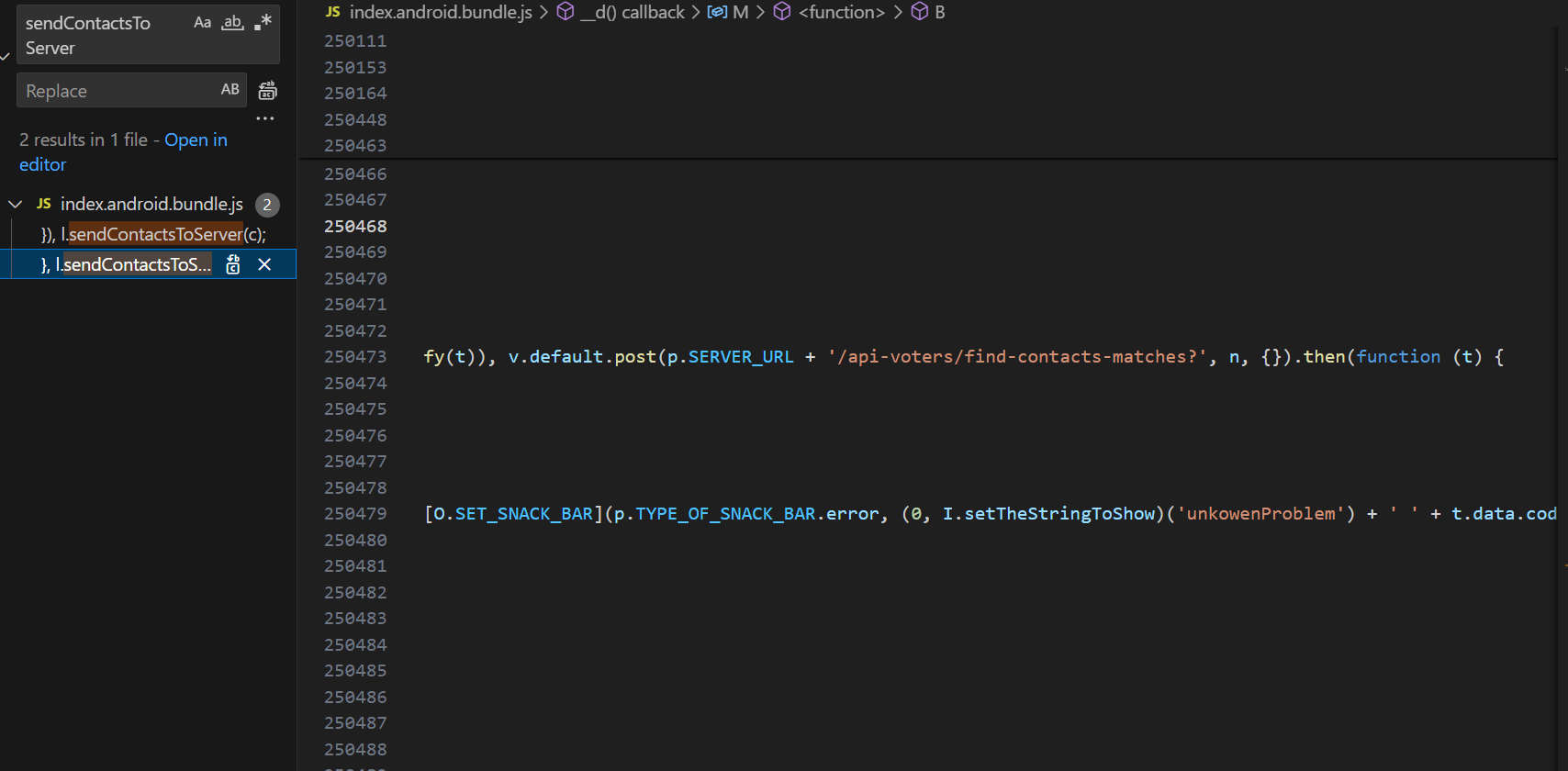
1. We will go with MATCH\_PHONE\_CONTACT



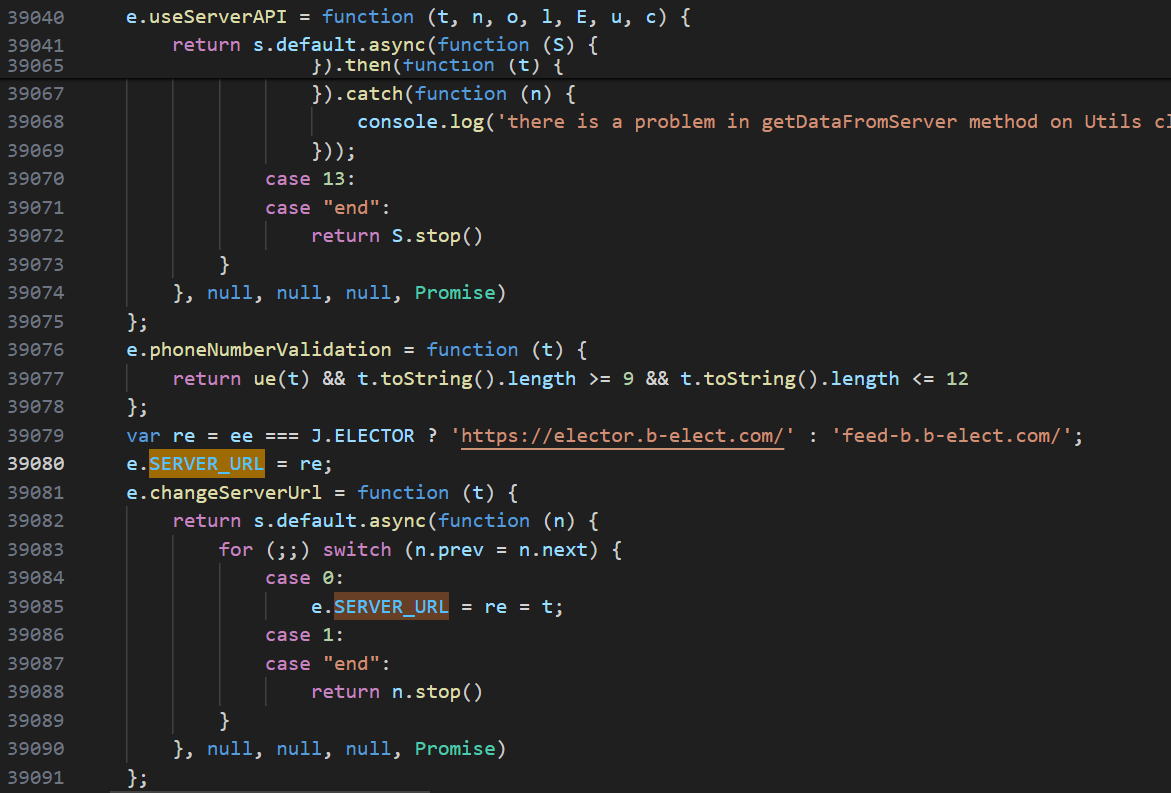
1. In the above function there is sendContactsToServer( ) we will search it.



1. In sendContactsToServer( ) ,there is SERVER\_URL as shown in below screenshot.



1. Now we will search SERVER\_URL as shown in below screenshot.



From here we can find base\_url on which contact is being sent.

So the verdict is TTP