Malicious APK File Creation

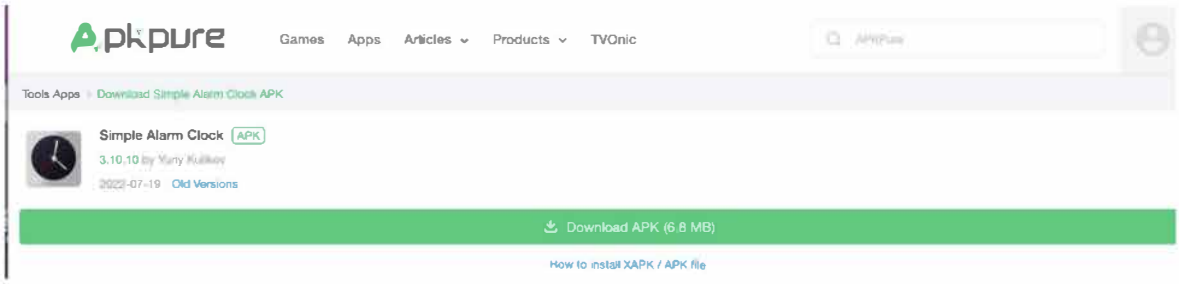
No. 18

Steps of the process:

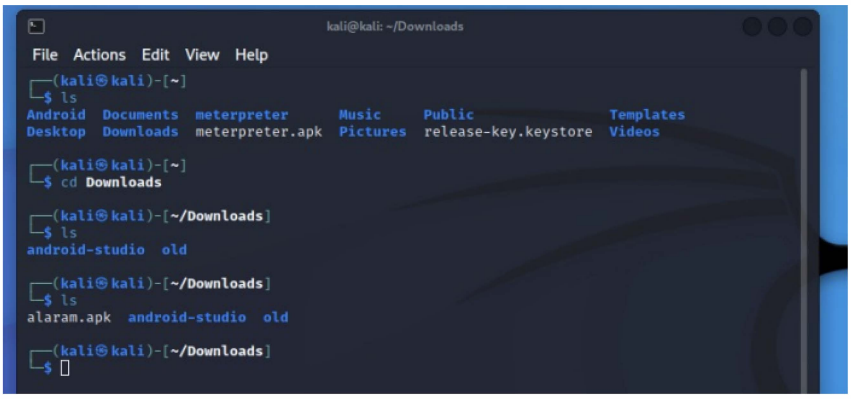
Following are the steps we took for the application.

Initially we Got an apk file from the internet. The file is of an alarm clock. The link is as follows:

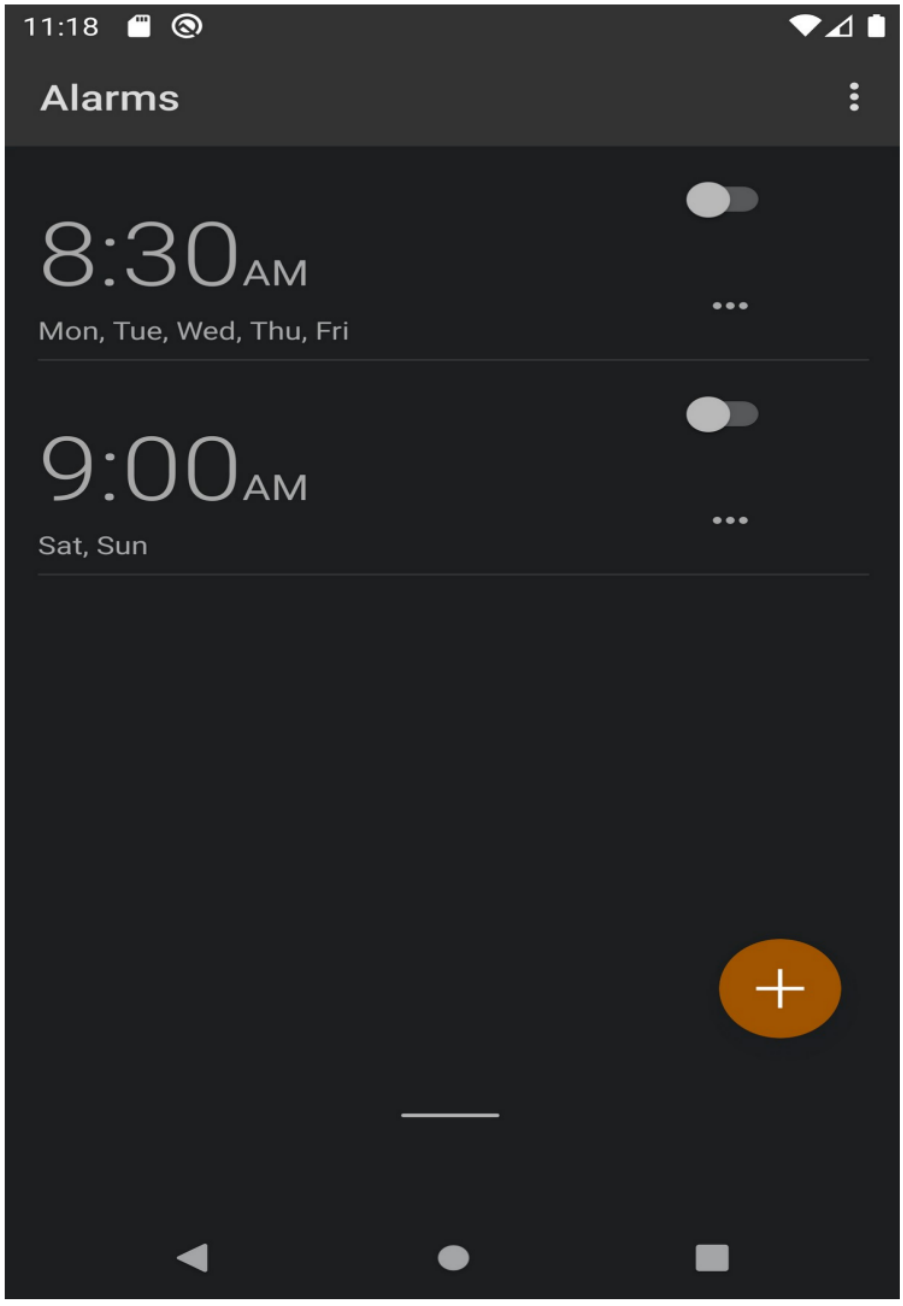
https://m.apkpure.com/simple-alarm-clock/com.better.alarm/download?from=details



2 Here is the apk file after download



3 Using the Emulator the view the application it is an alarm clock as show in the screen shot below :



4 : Next we decompiled the app using apk tool

Command: apktool d d alaram.apk (file name)

```
┌──(kali㉿kali)-[~/Downloads]
└─$ apktool d alaram.apk
I: Using Apktool 2.6.1 on alaram.apk
I: Loading resource table ...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package ...
I: Decoding file-resources ...
I: Decoding values */* XMLs ...
I: Baksmaling classes.dex ...
I: Baksmaling classes2.dex ...
I: Copying assets and libs ...
I: Copying unknown files ...
I: Copying original files ...
I: Copying META-INF/services directory

┌──(kali㉿kali)-[~/Downloads]
└─$
```

5 Add the secret code to the main UI file.

The folder res -> values - > strings.xml contains the string's value.

```
File  Actions  Edit  View  Help
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="add_alarm">Add alarm</string>
    <string name="alarm_alert_alert_silenced">Alarm silenced after %d minutes.</string>
    <string name="alarm_alert_dismiss_text">Dismiss</string>
    <string name="alarm_alert_hold_the_button_text">Hold the button!</string>
    <string name="alarm_alert_reschedule_text">Reschedule</string>
    <string name="alarm_alert_snooze_set">Snoozing for %d minutes.</string>
    <string name="alarm_alert_snooze_text">Snooze</string>
    <string name="alarm_in_silent_mode_summary">Play alarm even when the phone is in silent mode</string>
    <string name="alarm_in_silent_mode_title">Alarm in silent mode</string>
    <string name="alarm_klaxon_service_desc">Sound playback service for alarms set in Clock.</string>
    <string name="alarm_list_title">Secret Code is Digit</string>
    <string name="alarm_notify_snooze_label">%s (snoozed)</string>
    <string name="alarm_notify_snooze_text">Alarm set for %s. Touch to cancel.</string>
    <string name="alarm_notify_text">Snooze or dismiss alarm.</string>
    <string name="alarm_prealarm">Gentle pre-alarm</string>
    <string name="alarm_repeat">Repeat</string>
    <string name="alarm_vibrate">Vibrate</string>
    <string name="alarm_volume_summary">Set the volume of alarms</st
        ring>
    <string name="alarm_volume_title">Alarm volume</string>
    <string name="alert">Ringtone</string>
    <string name="alert_notifications_default_prio_text">" Secondary notifications are disabled.

It happens if you have disabled and enabled notifications again or changed settings manually.

Click OK to jump to system settings and select the second highest priority for this notification (Make sound).

Ironically, you should set the sound to none in advanced settings."</string>
    <string name="alert_notifications_high_prio_text">" Priority of for the big popup with snooze and dismiss buttons is too low
n!

It happens if you have disabled and enabled notifications again or changed settings manually.

Click OK to jump to system settings and select the highest priority for this notification (Make sound and pop up on screen).

-- INSERT --
```

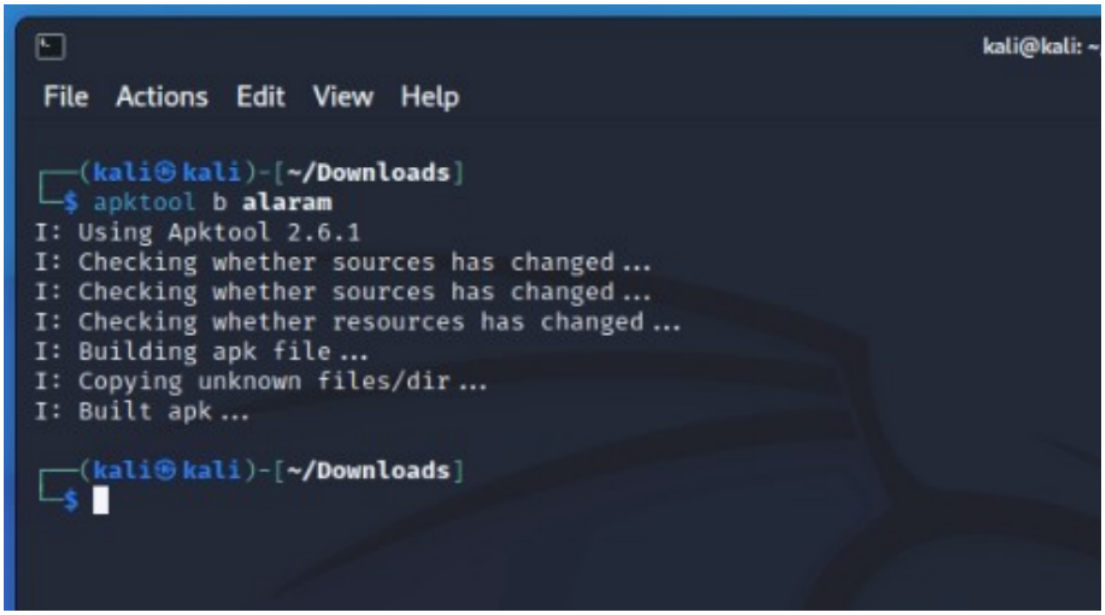
6 Here we set the code

Secret code is Digit

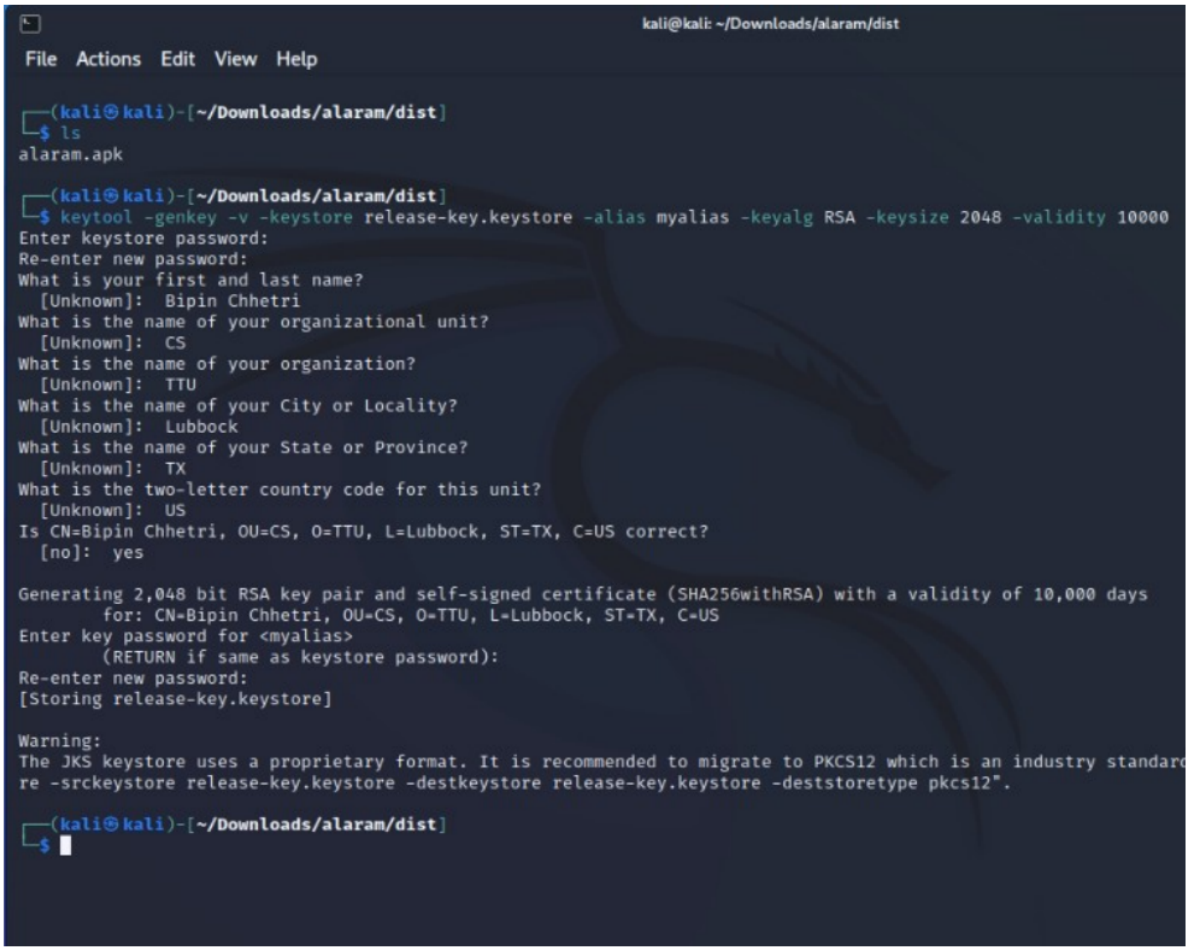
```
<string name="alarm_alert_reschedule_text">Reschedule</string>
<string name="alarm_alert_snooze_set">Snoozing for %d minutes.</string>
<string name="alarm_alert_snooze_text">Snooze</string>
<string name="alarm_in_silent_mode_summary">Play alarm even when the phone is in silent
<string name="alarm_in_silent_mode_title">Alarm in silent mode</string>
<string name="alarm_klaxon_service_desc">Sound playback service for alarms set in Clock.
<string name="alarm_list_title">Secret Code is Digit</string>
<string name="alarm_notify_snooze_label">%s (snoozed)</string>
<string name="alarm_notify_snooze_text">Alarm set for %s. Touch to cancel.</string>
<string name="alarm_notify_text">Snooze or dismiss alarm.</string>
<string name="alarm_prealarm">Gentle pre-alarm</string>
```

6

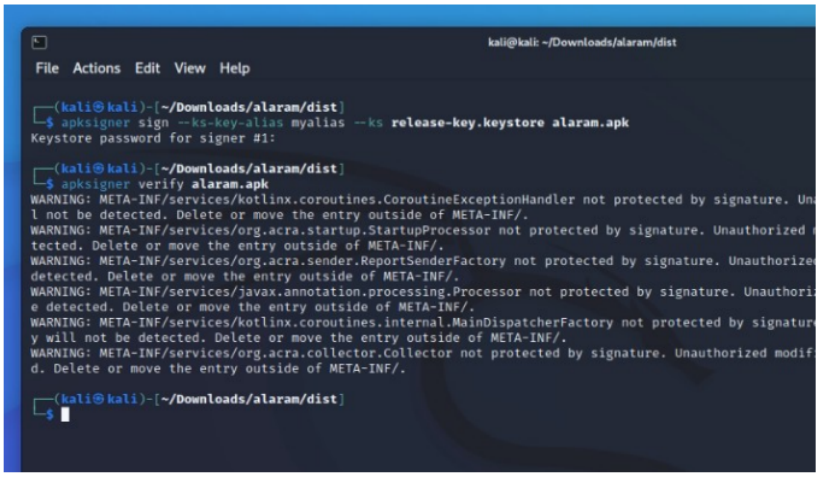
Using apktool, create an apk file from the calculator folder.
Run the apktool b alaram command.



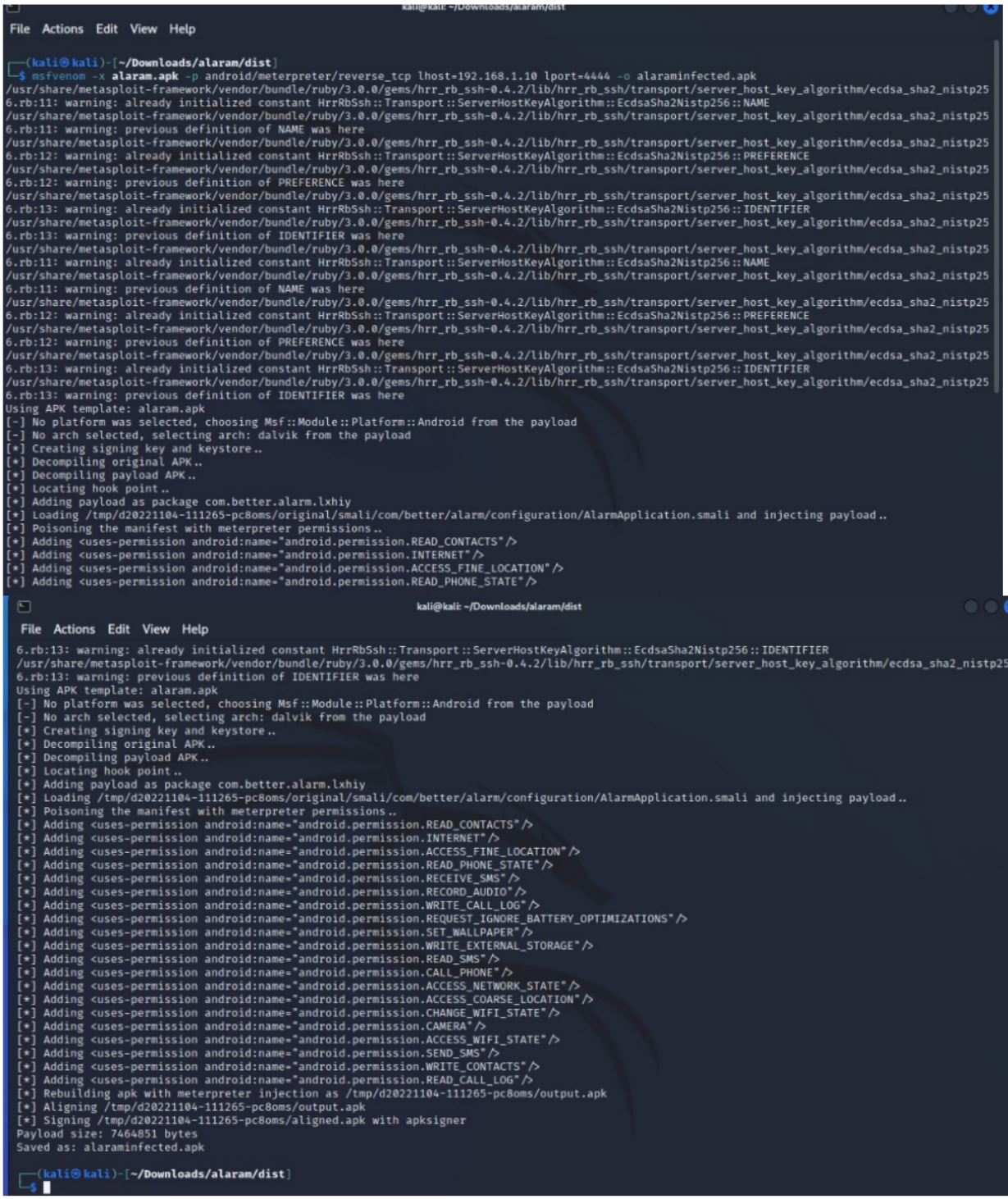
7 Sign the app tool.
Create the keystore file. Keytool -genkey -v Release-Key.Keystore -alias Myalias -Keyalg RSA -Keysize 2048 -Validity 10000



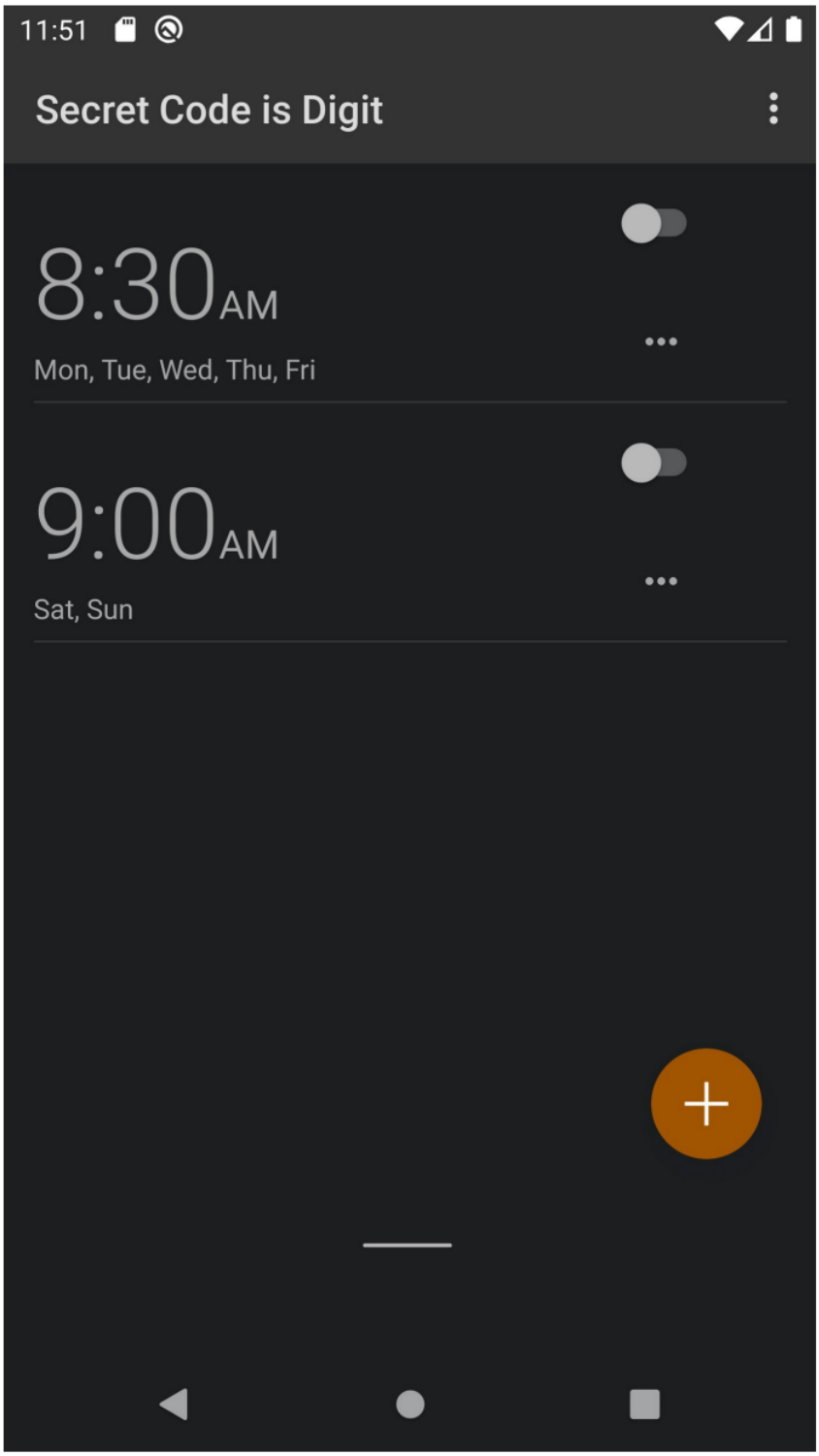
By using the command apksigner verify calculator.apk, we can confirm the signature.



8 Incorporate a payload into the apk file We utilized msfvenom and the standard reverse tcp payload for Android in order to embed the malicious payload in the apk file.



9 Launch the application in an emulator to look for the hidden code.
The screenshot below demonstrates how a calculator app requests various permissions.



10. Also you can check the apk in the virusl total (In 2004, VirusTotal was established as a free service that scans files and URLs for malware such as viruses, worms, and trojan horses.)