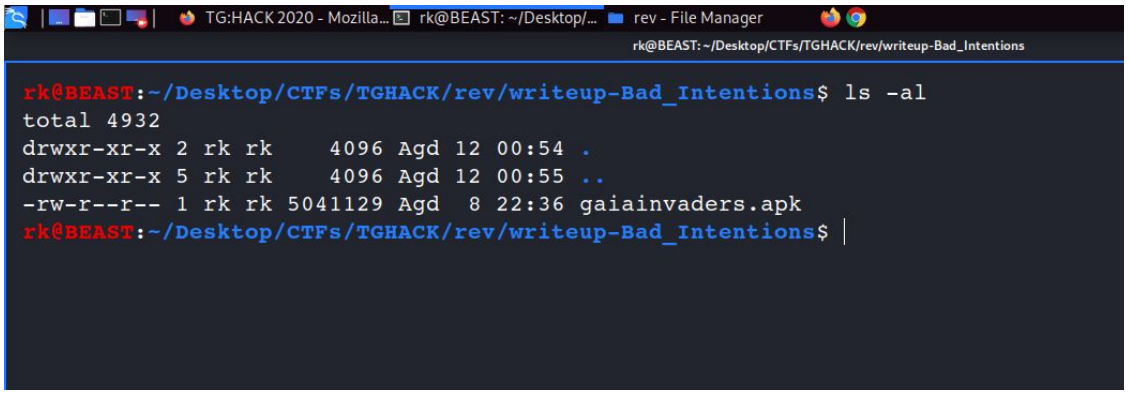
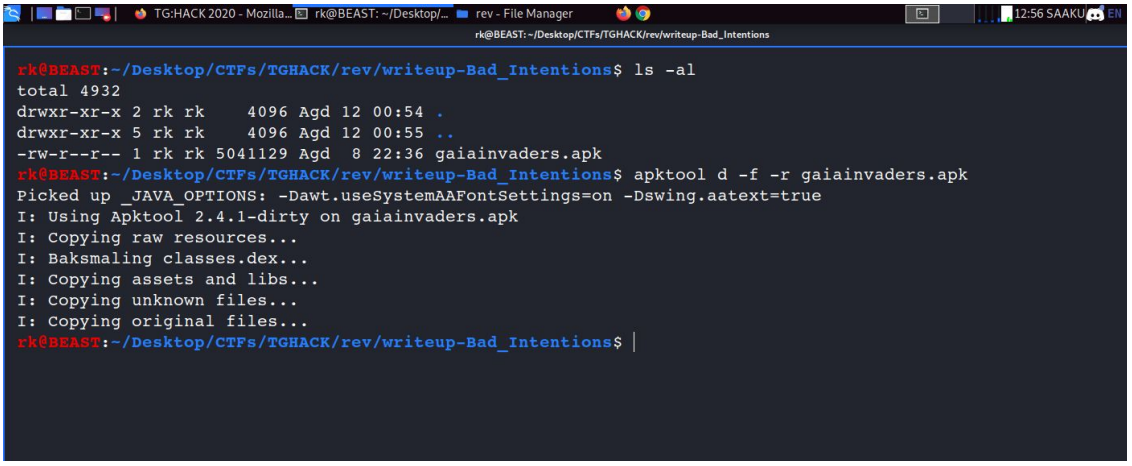
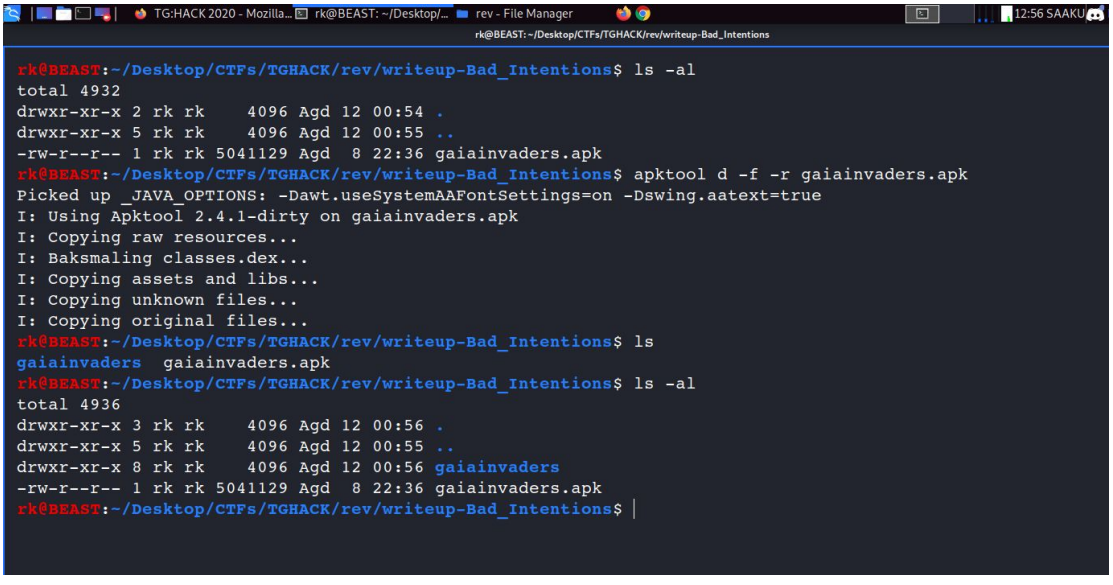
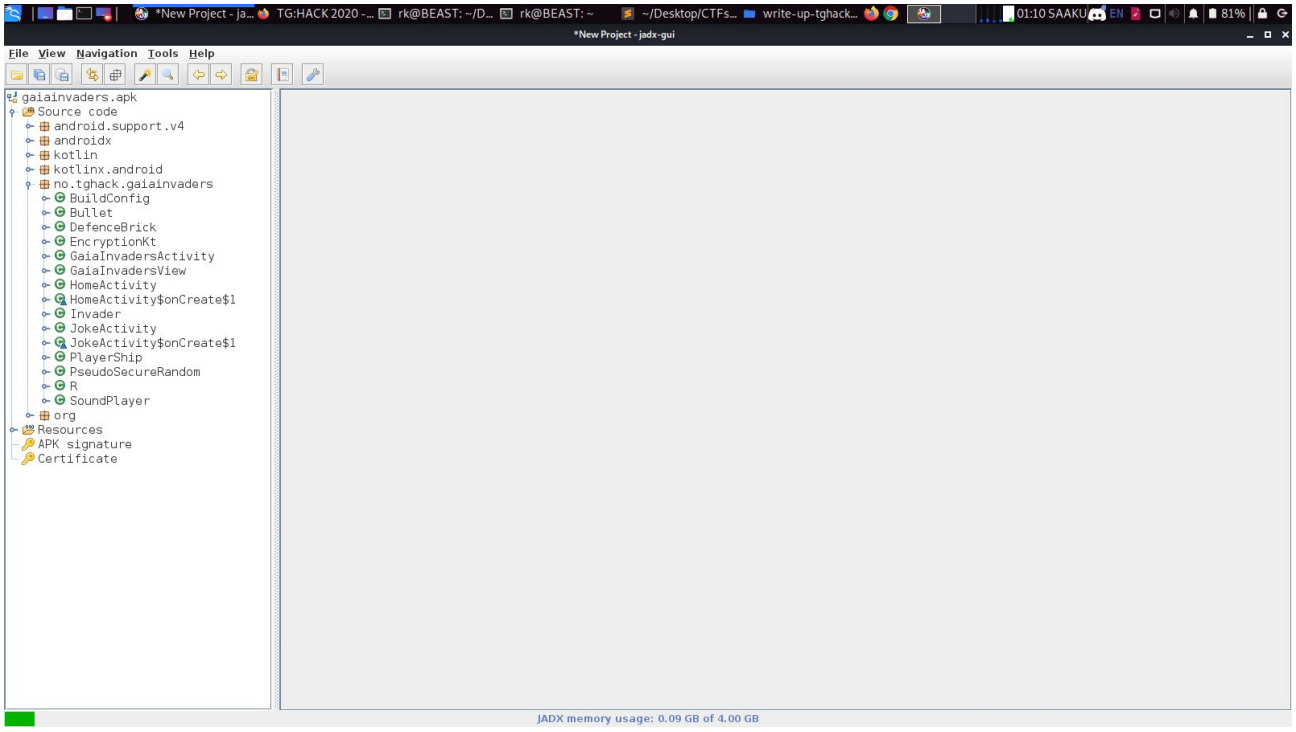
TGHACK/ReverseEngineering/BAD-INTENTIONS

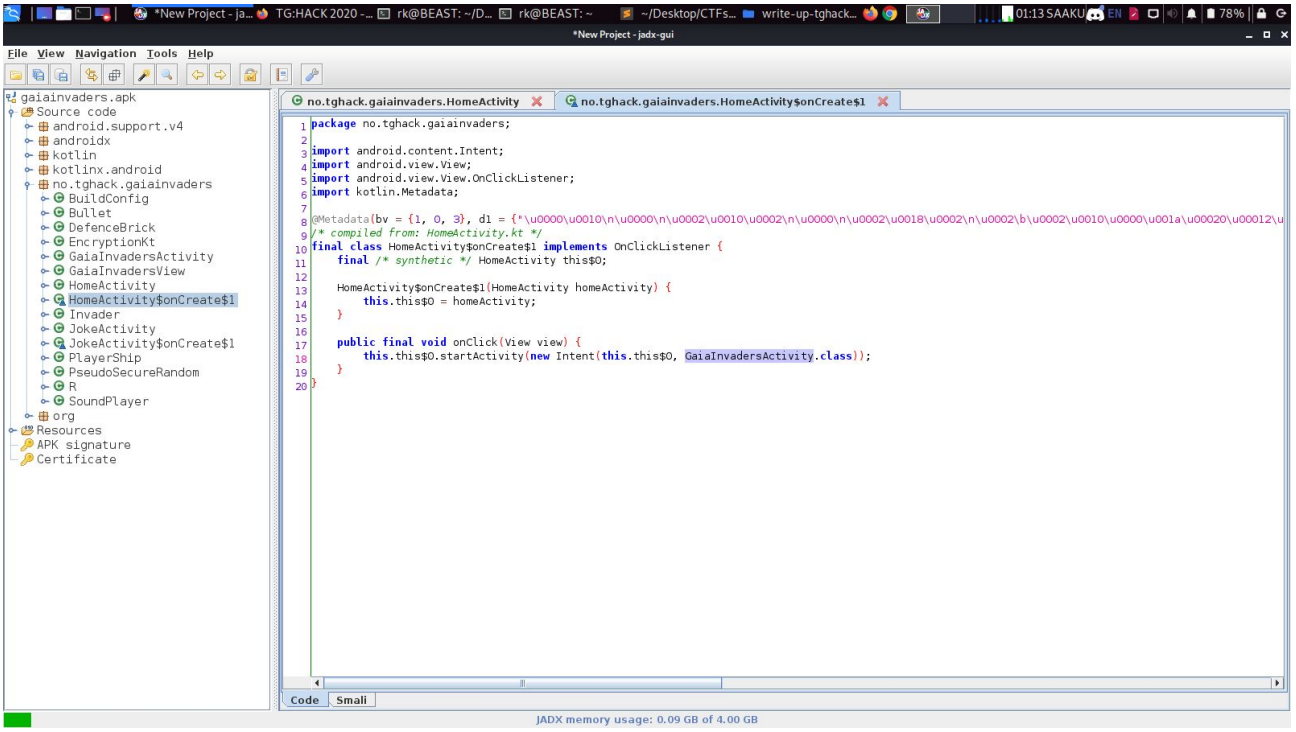




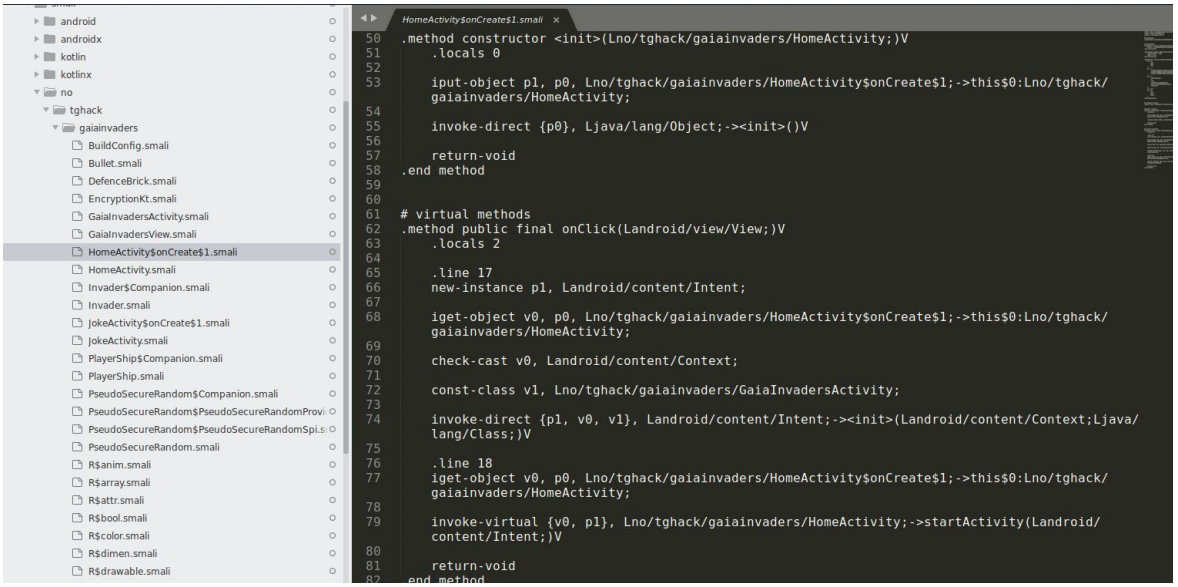


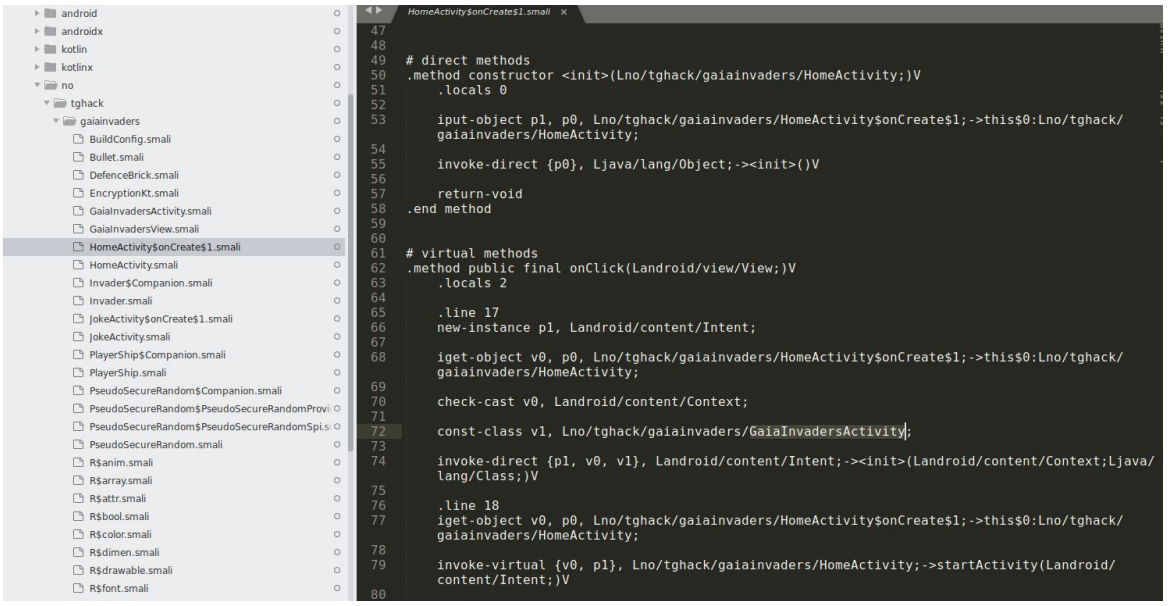
open jadx-gui in terminal
open gaiainvaders/ in jdax-gui

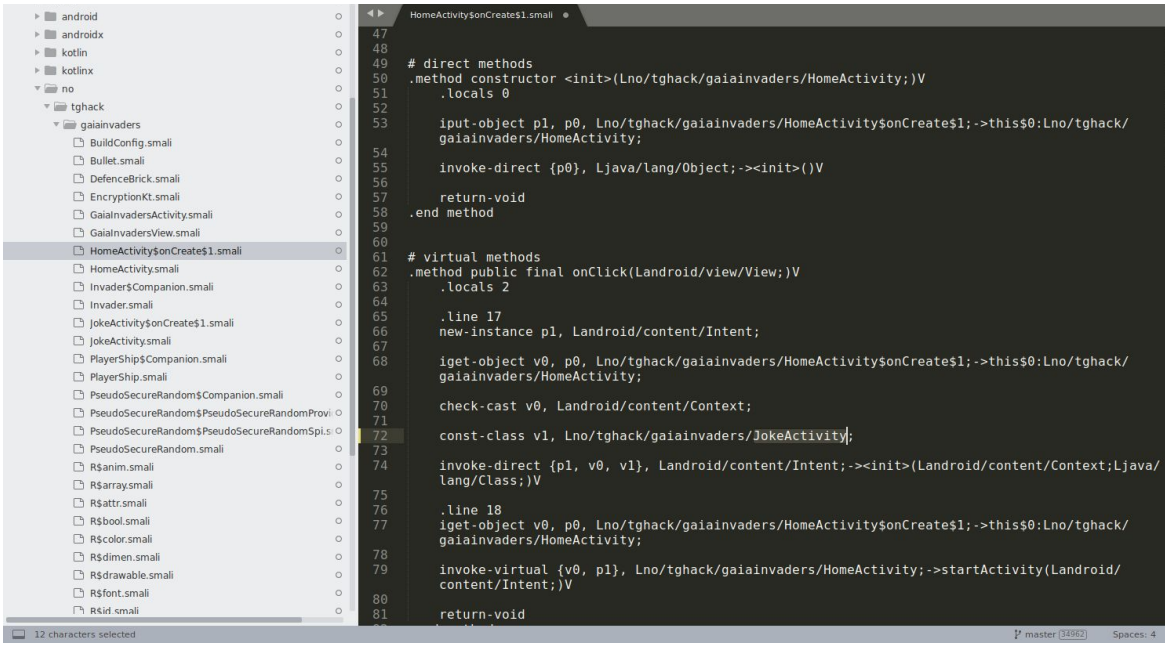





```
-rw-r--r-- 1 rk rk 5041129 Agd  8 22:36 gaiainvaders.apk
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ apktool d -f -r gaiainvaders.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1-dirty on gaiainvaders.apk
I: Copying raw resources...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ ls
gaiainvaders  gaiainvaders.apk
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ ls -al
total 4936
drwxr-xr-x 3 rk rk    4096 Agd 12 00:56 .
drwxr-xr-x 5 rk rk    4096 Agd 12 00:55 ..
drwxr-xr-x 8 rk rk    4096 Agd 12 00:56 gaiainvaders
-rw-r--r-- 1 rk rk 5041129 Agd  8 22:36 gaiainvaders.apk
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ subl gaiainvaders
```


android
androidx
kotlin
kotlinx
no
tghack
gaiainvaders
BuildConfig.smali
Bullet.smali
DefenceBrick.smali
EncryptionKt.smali
GaiaInvadersActivity.smali
GaiaInvadersView.smali
HomeActivity$onCreate$1.smali
HomeActivity.smali
Invader$Companion.smali
Invader.smali
JokeActivity$onCreate$1.smali
JokeActivity.smali
PlayerShip$Companion.smali
PlayerShip.smali
PseudoSecureRandom$Companion.smali
PseudoSecureRandom$PseudoSecureRandomProvi
PseudoSecureRandom$PseudoSecureRandomSpi.s
PseudoSecureRandom.smali
R$anim.smali
R$array.smali
R$attr.smali
R$bool.smali
R$color.smali
R$dimen.smali
R$drawable.smali
HomeActivity$onCreate$1.smali
.method constructor <init>(Lno/tghack/gaiainvaders/HomeActivity;)V
.locals 0
iput-object p1, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
invoke-direct {p0}, Ljava/lang/Object;-><init>()V
return-void
.end method
virtual methods
.method public final onClick(Landroid/view/View;)V
.locals 2
.line 17
new-instance p1, Landroid/content/Intent;
iget-object v0, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
check-cast v0, Landroid/content/Context;
const-class v1, Lno/tghack/gaiainvaders/GaiaInvadersActivity;
invoke-direct {p1, v0, v1}, Landroid/content/Intent;-><init>(Landroid/content/Context;Ljava/lang/Class;)V
.line 18
iget-object v0, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
invoke-virtual {v0, p1}, Lno/tghack/gaiainvaders/HomeActivity;->startActivity(Landroid/content/Intent;)V
return-void
.end method


android
androidx
kotlin
kotlinx
no
tghack
gaiainvaders
BuildConfig.smali
Bullet.smali
DefenceBrick.smali
EncryptionKt.smali
GaiaInvadersActivity.smali
GaiaInvadersView.smali
HomeActivity$onCreate$1.smali
HomeActivity.smali
Invader$Companion.smali
Invader.smali
JokeActivity$onCreate$1.smali
JokeActivity.smali
PlayerShip$Companion.smali
PlayerShip.smali
PseudoSecureRandom$Companion.smali
PseudoSecureRandom$PseudoSecureRandomProvi
PseudoSecureRandom$PseudoSecureRandomSpi.s
PseudoSecureRandom.smali
R$anim.smali
R$array.smali
R$attr.smali
R$bool.smali
R$color.smali
R$dimen.smali
R$drawable.smali
R$font.smali
HomeActivity$onCreate$1.smali
direct methods
.method constructor <init>(Lno/tghack/gaiainvaders/HomeActivity;)V
.locals 0
iput-object p1, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
invoke-direct {p0}, Ljava/lang/Object;-><init>()V
return-void
.end method
virtual methods
.method public final onClick(Landroid/view/View;)V
.locals 2
.line 17
new-instance p1, Landroid/content/Intent;
iget-object v0, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
check-cast v0, Landroid/content/Context;
const-class v1, Lno/tghack/gaiainvaders/GaiaInvadersActivity;
invoke-direct {p1, v0, v1}, Landroid/content/Intent;-><init>(Landroid/content/Context;Ljava/lang/Class;)V
.line 18
iget-object v0, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
invoke-virtual {v0, p1}, Lno/tghack/gaiainvaders/HomeActivity;->startActivity(Landroid/content/Intent;)V


android
androidx
kotlin
kotlinx
no
tghack
gaiainvaders
BuildConfig.smali
Bullet.smali
DefenceBrick.smali
EncryptionKt.smali
GaiaInvadersActivity.smali
GaiaInvadersView.smali
HomeActivity$onCreate$1.smali
HomeActivity.smali
Invader$Companion.smali
Invader.smali
JokeActivity$onCreate$1.smali
JokeActivity.smali
PlayerShip$Companion.smali
PlayerShip.smali
PseudoSecureRandom$Companion.smali
PseudoSecureRandom$PseudoSecureRandomProvi
PseudoSecureRandom$PseudoSecureRandomSpi.s
PseudoSecureRandom.smali
R$anim.smali
R$array.smali
R$attr.smali
R$bool.smali
R$color.smali
R$dimen.smali
R$drawable.smali
R$font.smali
HomeActivity$onCreate$1.smali
direct methods
.method constructor <init>(Lno/tghack/gaiainvaders/HomeActivity;)V
.locals 0
iput-object p1, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
invoke-direct {p0}, Ljava/lang/Object;-><init>()V
return-void
.end method
virtual methods
.method public final onClick(Landroid/view/View;)V
.locals 2
.line 17
new-instance p1, Landroid/content/Intent;
iget-object v0, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
check-cast v0, Landroid/content/Context;
const-class v1, Lno/tghack/gaiainvaders/JokeActivity;
invoke-direct {p1, v0, v1}, Landroid/content/Intent;-><init>(Landroid/content/Context;Ljava/lang/Class;)V
.line 18
iget-object v0, p0, Lno/tghack/gaiainvaders/HomeActivity$onCreate$1;->this$0:Lno/tghack/gaiainvaders/HomeActivity;
invoke-virtual {v0, p1}, Lno/tghack/gaiainvaders/HomeActivity;->startActivity(Landroid/content/Intent;)V
return-void
12 characters selected
master
Spaces: 4

```
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ apktool b gaiainvaders
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1-dirty
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Copying raw resources...
I: Copying libs... (/kotlin)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ keytool -genkey -V -keystore key.keystore -alias gaia -keyal
g RSA -keysize 2048 -validity 1000
```

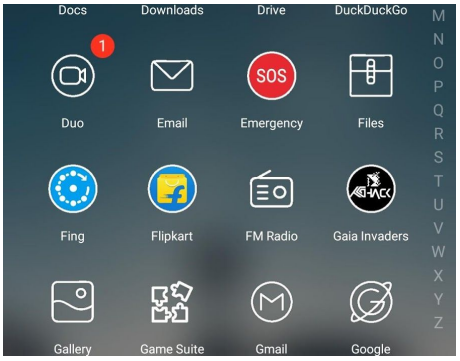
```
I: Using Apktool 2.4.1-dirty on gaiainvaders.apk
I: Copying raw resources...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ ls
gaiainvaders  gaiainvaders.apk
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ ls -al
total 4936
drwxr-xr-x 3 rk rk    4096 Agd 12 00:56 .
drwxr-xr-x 5 rk rk    4096 Agd 12 00:55 ..
drwxr-xr-x 8 rk rk    4096 Agd 12 00:56 gaiainvaders
-rw-r--r-- 1 rk rk 5041129 Agd  8 22:36 gaiainvaders.apk
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ subl gaiainvaders
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ apktool b gaiainvaders
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1-dirty
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Copying raw resources...
I: Copying libs... (/kotlin)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ keytool -genkey -V -keystore key.keystore -alias gaia -keyal
g RSA -keysize 2048 -validity 1000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
```

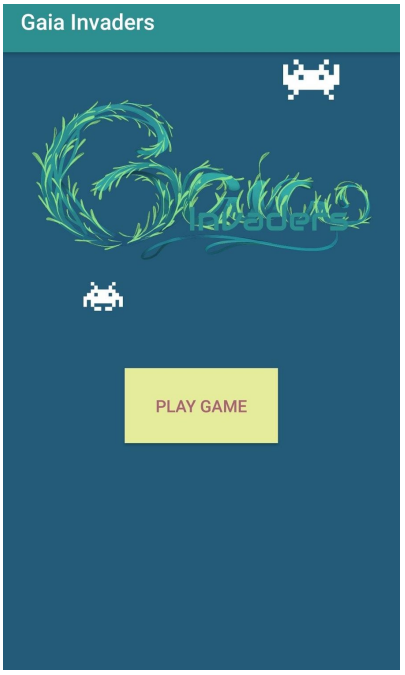
```
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ subl gaiainvaders
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ apktool b gaiainvaders
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1-dirty
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Copying raw resources...
I: Copying libs... (/kotlin)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ keytool -genkey -V -keystore key.keystore -alias gaia -keyal
g RSA -keysize 2048 -validity 1000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  test
What is the name of your organizational unit?
  [Unknown]:  test
What is the name of your organization?
  [Unknown]:  test
What is the name of your City or Locality?
  [Unknown]:  test
What is the name of your State or Province?
  [Unknown]:  test
What is the two-letter country code for this unit?
  [Unknown]:  te
Is CN=test, OU=test, O=test, L=test, ST=test, C=te correct?
  [no]:  yes
```

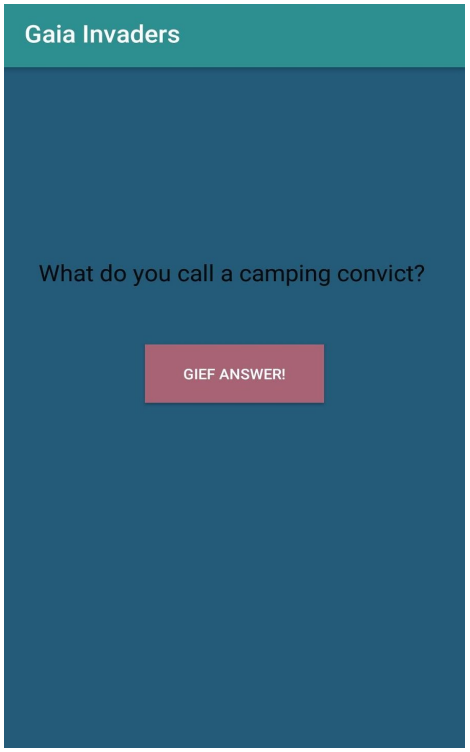
```
I: Copying unknown files/dir...
I: Built apk...
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ keytool -genkey -V -keystore key.keystore -alias gaia -keyal
g RSA -keysize 2048 -validity 1000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  test
What is the name of your organizational unit?
  [Unknown]:  test
What is the name of your organization?
  [Unknown]:  test
What is the name of your City or Locality?
  [Unknown]:  test
What is the name of your State or Province?
  [Unknown]:  test
What is the two-letter country code for this unit?
  [Unknown]:  te
Is CN=test, OU=test, O=test, L=test, ST=test, C=te correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 1,000 days
        for: CN=test, OU=test, O=test, L=test, ST=test, C=te
[Storing key.keystore]
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keys
tore key.keystore gaiainvaders/dist/gaiainvaders.apk gaia
```

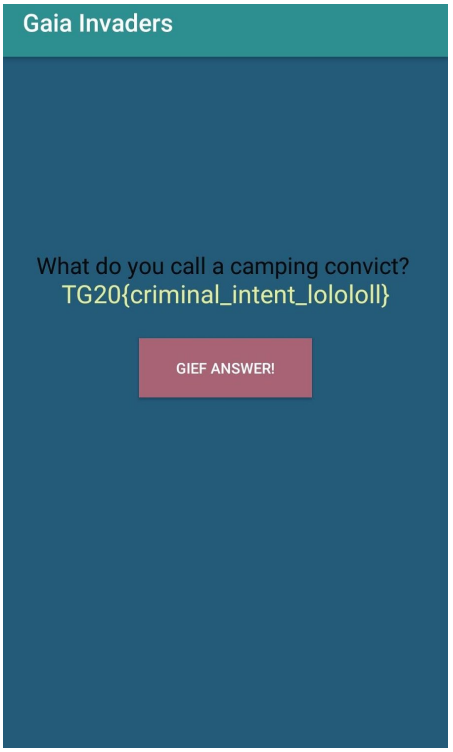
```
  signing: assets/archive.0962.dat
  signing: assets/archive.0567.dat
  signing: assets/archive.0481.dat
  signing: assets/archive.0918.dat
  signing: assets/archive.0047.dat
  signing: assets/archive.0290.dat
  signing: assets/archive.0537.dat
  signing: assets/archive.0365.dat
  signing: assets/archive.0260.dat
  signing: org/bouncycastle/x509/CertPathReviewerMessages.properties
  signing: org/bouncycastle/x509/CertPathReviewerMessages_de.properties

>>> Signer
    X.509, CN=test, OU=test, O=test, L=test, ST=test, C=te
    [trusted certificate]

jar signed.

Warning:
The signer's certificate is self-signed.
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ zipalign -v 4 gaiainvaders/dist/gaiainvaders.apk gaiainvader
s/dist/signed.apk
```

```
  4866562 assets/archive.0890.dat (OK - compressed)
  4866633 assets/archive.0979.dat (OK - compressed)
  4866704 assets/archive.0898.dat (OK - compressed)
  4866775 assets/archive.0494.dat (OK - compressed)
  4866846 assets/archive.0336.dat (OK - compressed)
  4866917 assets/archive.0965.dat (OK - compressed)
  4866988 assets/archive.0059.dat (OK - compressed)
  4867059 assets/archive.0447.dat (OK - compressed)
  4867130 assets/archive.0962.dat (OK - compressed)
  4867201 assets/archive.0567.dat (OK - compressed)
  4867272 assets/archive.0481.dat (OK - compressed)
  4867343 assets/archive.0918.dat (OK - compressed)
  4867414 assets/archive.0047.dat (OK - compressed)
  4867485 assets/archive.0290.dat (OK - compressed)
  4867556 assets/archive.0537.dat (OK - compressed)
  4867627 assets/archive.0365.dat (OK - compressed)
  4867698 assets/archive.0260.dat (OK - compressed)
  4867803 org/bouncycastle/x509/CertPathReviewerMessages.properties (OK - compressed)
  4873950 org/bouncycastle/x509/CertPathReviewerMessages_de.properties (OK - compressed)
Verification successful
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$ adb install gaiainvaders/dist/signed.apk
Success
rk@BEAST:~/Desktop/CTFs/TGHACK/rev/writeup-Bad_Intentions$
```


Docs
Downloads
Drive
DuckDuckGo
Duo
Email
Emergency
Files
Fing
Flipkart
FM Radio
Gaia Invaders
Gallery
Game Suite
Gmail
Google
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z


Gaia Invaders
PLAY GAME


Gaia Invaders
What do you call a camping convict?
GIEF ANSWER!


Gaia Invaders
What do you call a camping convict?
TG20{criminal_intent_lolololl}
GIEF ANSWER!