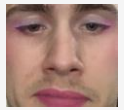
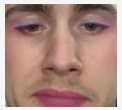
Welcome to My Presentation on Frida

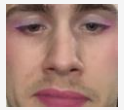
Which is just a list of poorly arranged screenshots 

Patching with Objection 

```
PS C:\Users\OwaisMehtab> objection patchapk --source .\kiosk.apk -D
The --ignore-nativelibs flag is required with the --skip-resources flag.
PS C:\Users\OwaisMehtab> objection patchapk --source .\kiosk.apk --skip-resources --ignore-nativelibs
No architecture specified. Determining it using `adb`...
Detected target device architecture as: arm64-v8a
Using latest Github gadget version: 16.0.3
Patcher will be using Gadget version: 16.0.3
Detected apktool version as: 2.6.1
Running apktool empty-framework-dir...
I: Removing 1.apk framework file...
Press any key to continue . . .
Unpacking .\kiosk.apk
App already has android.permission.INTERNET
Target class not specified, searching for launchable activity instead...
Reading smali from: C:\Users\OWAISM~1\AppData\Local\Temp\tmpkq4y9o85.apktemp\smali\com/doddle/kiosk/remotekiosk/ui/splash/SplashActivity.smali
Injecting loadLibrary call at line: 41
Attempting to fix the constructors .locals count
Current locals value is 0, updating to 1:
Writing patched smali back to: C:\Users\OWAISM~1\AppData\Local\Temp\tmpkq4y9o85.apktemp\smali\com/doddle/kiosk/remotekiosk/ui/splash/SplashActivity.smali
Creating library path: C:\Users\OWAISM~1\AppData\Local\Temp\tmpkq4y9o85.apktemp\lib\arm64-v8a
Copying Frida gadget to libs path...
Rebuilding the APK with the frida-gadget loaded...
Built new APK with injected loadLibrary and frida-gadget
Performing zipalign
Zipalign completed
Signing new APK.
Signed the new APK
Copying final apk from C:\Users\OWAISM~1\AppData\Local\Temp\tmpkq4y9o85.apktemp.aligned.objection.apk to .\kiosk.objection.apk in current directory...
Cleaning up temp files...
```

Running Patched Applications 

```
PS C:\Users\OwaisMehtab> frida-ps -Uai
  PID  Name                             Identifier
-----  -------------------------------  -----------------------------------------
 8016  Chrome                           com.android.chrome
12645  Gadget                           re.frida.Gadget
 7134  Google                           com.google.android.googlequicksearchbox
 6967  Google Play Store                com.android.vending
11226  Maps                             com.google.android.apps.maps
12463  Messages                         com.google.android.apps.messaging
11778  Photos                           com.google.android.apps.photos
12645  RemoteKiosk                      com.doddle.kiosk.simulator
  609  SIM Tool Kit                     com.android.stk
```

Running Patched Applications 

```
┌──(ggwp㉿DESKTOP-CQHU9T2)-[/mnt/c/Users/User/Downloads]
└─$ adb shell
Note_7P:/ $ ps -A | grep -i frida
1|Note_7P:/ $ netstat -tuplan | grep 27042
1|Note_7P:/ $ netstat -tuplan
Active Internet connections (established and servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program Name
tcp      130      0 192.168.114.211:51420   142.250.187.246:443     CLOSE_WAIT  -
tcp      130      0 192.168.114.211:50060   216.58.213.1:443        CLOSE_WAIT  -
tcp      130      0 192.168.114.211:54680   172.217.169.35:443      CLOSE_WAIT  -
tcp      130      0 192.168.114.211:42398   142.250.180.10:443      CLOSE_WAIT  -
tcp      130      0 192.168.114.211:47592   216.58.212.234:443      CLOSE_WAIT  -
tcp      130      0 192.168.114.211:36280   142.250.178.10:443      CLOSE_WAIT  -
tcp6       0      0 2a03:dd00:1112:4e3:5060 :::*                    LISTEN      -
tcp6       0      0 2a03:dd00:1112:4e:50001 :::*                    LISTEN      -
tcp6       0      0 ::ffff:127.0.0.1:42075  :::*                    LISTEN      -
tcp6       0      0 ::ffff:192.168.11:50744 ::ffff:74.125.133.:5228 ESTABLISHED -
tcp6       0      0 ::ffff:192.168.11:35756 ::ffff:216.58.212.2:443 ESTABLISHED -
tcp6       0      0 2a03:dd00:1112:4e:50000 2a03:dd00:1f80:280:5063 ESTABLISHED -
tcp6       0      0 ::ffff:192.168.11:57160 ::ffff:194.116.168.:443 ESTABLISHED -
udp     4352      0 192.168.114.211:68      192.168.114.1:67        ESTABLISHED -
udp6       0      0 2a03:dd00:1112:4e:50000 :::*                                -
udp6       0      0 2a03:dd00:1112:4e:50001 :::*                                -
udp6       0      0 2a03:dd00:1112:4e3:5060 :::*                                -
Note_7P:/ $
```

How it works? 

```
┌──(ggwp㉿DESKTOP-CQHU9T2)-[/mnt/c/Users/User/Downloads/kiosk.objection]
└─$ tree lib/
lib/
└── arm64-v8a
    └── libfrida-gadget.so

1 directory, 1 file
```

SplashActivity.smali

C: > Users > User > Downloads > kiosk.objection > smali > com > doddle > kiosk > remotekiosk > ui > splash > SplashActivity.smali

```
47      return-void
48  .end method
49
50  .method static constructor <clinit>()V
51      .locals 1
52
53      .prologue
54      const-string v0, "frida-gadget"
55
56      invoke-static {v0}, Ljava/lang/System;->loadLibrary(Ljava/lang/String;)V
57
58      return-void
```

Issues with embedded mode 

```
┌──(ggwp㉿DESKTOP-CQHU9T2)-[/mnt/c/Users/User/Downloads]
└─$ adb install kiosk.flawed.apk
Performing Streamed Install
adb: failed to install kiosk.flawed.apk: Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES: Failed to collect certificates from /data/app/vmdl1663977953.
e.apk: Attempt to get length of null array]
```

```
┌──(ggwp㉿DESKTOP-CQHU9T2)-[/mnt/c/Users/User/Downloads]
└─$ keytool -genkey -v -keystore my-release-key.keystore -alias alias_name -keyalg RSA -keysize 2048 -validity 10000 ^C

┌──(ggwp㉿DESKTOP-CQHU9T2)-[/mnt/c/Users/User/Downloads]
└─$ jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore my-release-key.keystore kiosk.objection.apk alias_name
Enter Passphrase for keystore:
 updating: META-INF/MANIFEST.MF
   adding: META-INF/ALIAS_NA.SF
   adding: META-INF/ALIAS_NA.RSA
  signing: META-INF/services/io.grpc.LoadBalancerProvider
  signing: META-INF/services/io.grpc.ManagedChannelProvider
  signing: META-INF/services/io.grpc.NameResolverProvider
  signing: META-INF/services/kotlinx.coroutines.CoroutineExceptionHandler
  signing: META-INF/services/kotlinx.coroutines.internal.MainDispatcherFactory
   adding: META-INF/OBJECTIO.SF
   adding: META-INF/OBJECTIO.RSA
  signing: AndroidManifest.xml
  signing: classes.dex
  signing: classes2.dex
  signing: kotlin/annotation/annotation.kotlin_builtins
  signing: kotlin/collections/collections.kotlin_builtins
  signing: kotlin/coroutines/coroutines.kotlin_builtins
  signing: kotlin/internal/internal.kotlin_builtins
  signing: kotlin/kotlin.kotlin_builtins
  signing: kotlin/ranges/ranges.kotlin_builtins
  signing: kotlin/reflect/reflect.kotlin_builtins
  signing: lib/arm64-v8a/libfrida-gadget.so
```

Issues with embedded mode 

```
└─$ jarsigner -verify kiosk.apk -verbose | tail -n 20

  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore

- Signed by "O=Doddle"
    Digest algorithm: SHA-256
    Signature algorithm: SHA256withRSA, 2048-bit key

jar verified.
```

```
└─$ jarsigner -verify kiosk.objection.apk -verbose | tail -n 20
s      73164 Thu Nov 24 10:41:26 GMT 2022 META-INF/MANIFEST.MF

  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore

- Signed by "CN=Unknown, OU=objection, O=SensePost, L=Unknown, ST=Unknown, C=Unknown"
    Digest algorithm: SHA-256
    Signature algorithm: SHA256withRSA, 2048-bit key
```

Preloaded Injection 

```
Note_7P:/data # setenforce 0
Note_7P:/data # getenforce
Permissive
Note_7P:/data # setprop wrap.com.doddle.kiosk.simulator LD_PRELOAD=/data/local/tmp/frida.
frida.config  frida.so
Note_7P:/data # setprop wrap.com.doddle.kiosk.simulator LD_PRELOAD=/data/local/tmp/frida.so
Note_7P:/data # getprop | tail -n 5
[wifi.interface]: [wlan0]
[wifi.tethering.interface]: [ap0]
[wlan.driver.status]: [ok]
[wlan.wfd.security.image]: [1]
[wrap.com.doddle.kiosk.simulator]: [LD_PRELOAD=/data/local/tmp/frida.so]
Note_7P:/data #
```

```
C:\Users\User\Downloads>adb shell am start -n com.doddle.kiosk.simulator/.SplashActivity
Starting: Intent { cmp=com.doddle.kiosk.simulator/.SplashActivity }
```

Preloaded Injection 

```
adb logcat -v color | grep -i frida
4 11:39:59.748 14549 14549 I app_process64: type=1400 audit(0.0:12296): avc: denied { execute } for path="/data/local/tmp/frida.so" dev="dm-1" ino=802
ontext=u:r:untrusted_app:s0:c128,c256,c512,c768 tcontext=u:object_r:shell_data_file:s0 tclass=file permissive=1
4 11:40:00.358 14549 14550 I Frida    : Listening on 127.0.0.1 TCP port 27042
4 11:40:01.396 14564 14564 I crash_dump64: type=1400 audit(0.0:12303): avc: denied { read } for name="frida.so" dev="dm-1" ino=802826 scontext=u:r:cra
p:s0:c128,c256,c512,c768 tcontext=u:object_r:shell_data_file:s0 tclass=file permissive=1
```

```
11-24 11:40:33.500 32308 32308 I zygote64: Ignoring open file descriptor 3
11-24 11:40:33.501 32308 32308 I zygote64: Ignoring open file descriptor 4
11-24 11:40:34.288 32308 32308 I Zygote   : Wrapped process has pid 14629
11-24 11:40:34.289 14629 14629 D Zygote   : begin preload
11-24 11:40:34.289 14629 14629 I Zygote   : Installing ICU cache reference pinning...
11-24 11:40:34.289 14629 14629 I Zygote   : Preloading ICU data...
11-24 11:40:34.296 14629 14629 I Zygote   : Preloading classes...
11-24 11:40:34.809 14629 14629 I Zygote   : ...preloaded 6535 classes in 513ms.
11-24 11:40:34.881 14629 14629 E BOOTPROF:      at com.android.internal.os.ZygoteInit.addBootEvent(ZygoteInit.java:126)
11-24 11:40:34.881 14629 14629 E BOOTPROF:      at com.android.internal.os.ZygoteInit.preloadClasses(ZygoteInit.java:376)
11-24 11:40:34.881 14629 14629 E BOOTPROF:      at com.android.internal.os.ZygoteInit.preload(ZygoteInit.java:159)
11-24 11:40:35.076 14644 14644 F DEBUG    :     #03 pc 00000000007cc0ec  /system/framework/arm64/boot-framework.oat (offset 0x3d800
setManager.createSystemAssetsInZygoteLocked+108)
11-24 11:40:35.076 14644 14644 F DEBUG    :     #07 pc 0000000000c059a0  /system/framework/arm64/boot-framework.oat (offset 0x3d800
s.ZygoteInit.preloadResources+80)
11-24 11:40:35.076 14644 14644 F DEBUG    :     #08 pc 0000000000c03f18  /system/framework/arm64/boot-framework.oat (offset 0x3d800
s.ZygoteInit.preload+280)
11-24 11:40:35.206 14629 14629 I Zygote   : Preloading resources...
11-24 11:40:35.232 14629 14629 I Zygote   : ...preloaded 64 resources in 25ms.
11-24 11:40:35.232 14629 14629 E BOOTPROF:      at com.android.internal.os.ZygoteInit.addBootEvent(ZygoteInit.java:126)
11-24 11:40:35.232 14629 14629 E BOOTPROF:      at com.android.internal.os.ZygoteInit.preloadResources(ZygoteInit.java:406)
11-24 11:40:35.232 14629 14629 E BOOTPROF:      at com.android.internal.os.ZygoteInit.preload(ZygoteInit.java:162)
11-24 11:40:35.237 14629 14629 I Zygote   : ...preloaded 41 resources in 5ms.
11-24 11:40:35.238 14629 14629 E BOOTPROF:      at com.android.internal.os.ZygoteInit.addBootEvent(ZygoteInit.java:126)
11-24 11:40:35.238 14629 14629 E BOOTPROF:      at com.android.internal.os.ZygoteInit.preloadResources(ZygoteInit.java:429)
```

Preloaded Injection 

```
(venv) C:\Users\User\Downloads>frida -U Gadget
     ____
    / _  |   Frida 15.0.0 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/

[Note 7P::Gadget]-> Process.id
15235
[Note 7P::Gadget]-> exit

Thank you for using Frida!

(venv) C:\Users\User\Downloads>frida -U Chrome
     ____
    / _  |   Frida 15.0.0 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
Failed to attach: unable to act on other processes when embedded
```

Scripting + LD_PRELOAD 

```
{
  "interaction": {
    "type": "script",
    "path": "/data/local/tmp/hookclasses.js"
  }
}
```

```
init(stage, parameters) {
    console.log('[init]', stage, JSON.stringify(parameters));

    Interceptor.attach(Module.getExportByName(null, 'open'), {
      onEnter(args) {
        const path = args[0].readUtf8String();
        console.log('open("' + path + '")');
      }
});
```

https://frida.re/docs/gadget/

Thank you


THANKS FOR
YOUR ATTENTION
CLAP AND DON'T ASK
ANY QUESTION, PLEASE
memegenerator.es