

/ramdisk/restore.external.c

- iPod Touch 3G: http://appldnld.apple.com/iPhone4/061-8360.20111012.New3w/iPod3,1_5.0_9A334_Restore.ipsw n18
- iPod Touch 4G: http://appldnld.apple.com/iPhone4/061-9622.20111012.Evry3/iPod4,1_5.0_9A334_Restore.ipsw n81
- iPhone 3GS: http://appldnld.apple.com/iPhone4/041-8356.20111012.SQRDT/iPhone2,1_5.0_9A334_Restore.ipsw n88
- iPhone 4 (GSM - AT&T): http://appldnld.apple.com/iPhone4/041-8358.20111012.FFc34/iPhone3,1_5.0_9A334_Restore.ipsw n90
- iPhone 4 (CDMA - Verizon): http://appldnld.apple.com/iPhone4/041-9743.20111012.vjhfp/iPhone3,3_5.0_9A334_Restore.ipsw n92
- iPad 1: http://appldnld.apple.com/iPhone4/041-8357.20111012.DTOrM/iPad1,1_5.0_9A334_Restore.ipsw k48

iphone 3 n82

???IOS ????

??? <http://yogeshd.blog.com/2011/04/10/v...sqlitedb-file/>

SMS <http://riactant.wordpress.com/2009/0...y-for-windows/>

<http://isohunt.com/torrents/?iht=-1&ihq=xcode+4.2?>

???KEYChian ??? (??UID + time + ??????????) =???? ????????

???? ?? UID ,??, ??:

deeper undelte anaylzer

????? ???? About

??? ?

1.?JB exploit ??bootloader ????ramdisk

2.????IOS ??

3.????keychain ????????

4.????IOS

5.? HFS ??image

6.??HFS ??

?code ??

<http://code.google.com/p/iphone-data...on/wiki/README>

????OS X VM ?????

<http://kuai.xunlei.com/d/WMSBPYFNTZVX>

?? HELLOWORLD

user ?root password ??9?s

ios ipsw?????opensources???????

<https://github.com/KatanaForensics/LanternLite>

??

????IOS ?? (??GUI??)

????IOS

??check usb python ?????? ??

?????????optoion

python python_scripts/emf_decrypter.py image.img ?py ??????????? print out ??

??????UID ??

1.????

2. Jailbreak ??

3. ????

?:demo_bruteforce.py

???? "?????: ?? "

(????????)

4. ????

?:

IOS 4 /dev/rdisk0s2s1

ssh -p 2222 root@localhost dd if=/dev/rdisk0s2s1 bs=8192 | dd of=image.img

IOS 5

ssh -p 2222 root@localhost dd if=/dev/rdisk0s1s2 bs=8192 | dd of=image.img

????

"ios 4 or ios5"

"?????????:alpine"

"?? 100%"

"???? ????encrypted.img ??" "

5.

?: ??? image ? ,image ??? ??UID??

???? "????keychian ????? ??" "

6. IOS ???? emf_decrypter ?image file ??????

??? "???"

"????IOS ????? ?image ??encrypted.img, ?????decrypted.img ??"

7 .?????? EMF undelter

"???"

" ?????? \UID\junk and \UID\undeltere ????? ??"

8.???????? EMF undelte (??catving empty space)

" ?????? \UID\junk and \UID\advance undeltere ????? ??"

9. USB SSH mount??

"????ios ?? SSH Port ,????? port :2222 ?? ??"

????

1.?????

2.????? ?????

3.?

?OS X ???xcode ??

??????? <http://mercurial.berkwood.com/>

10.7 ?? <http://mercurial.berkwood.com/binari...macosx10.7.zip>

10.6 ?? <http://mercurial.berkwood.com/binari...macosx10.6.zip>

?????????????? .

??????

sudo -s

?OS X VM root??9?s

curl -O http://networkpx.googlecode.com/files/ldid

chmod +x ldid

sudo mv ldid /usr/bin/

#install OSXFuse for img3fs ??osxfuse ??

curl -O -L https://github.com/downloads/osxfuse/osxfuse/OSXFUSE-2.3.4.dmg

hdiutil mount OSXFUSE-2.3.4.dmg

sudo installer -pkg /Volumes/FUSE\for\ OS\ X\Install\ OSXFUSE\2.3.pkg -target /

hdiutil eject /Volumes/FUSE\for\ OS\ X/

??python ?????

sudo ARCHFLAGS='-arch i386 -arch x86_64' easy_install pycrypto

sudo easy_install M2crypto construct progressbar

##?RAM disk ??

hg clone https://code.google.com/p/iphone-dataprotection/

cd iphone-dataprotection

make -C img3fs/

curl -O -L https://sites.google.com/a/iphone-dev.com/files/home/redsn0w_mac_0.9.9b8.zip

unzip redsn0w_mac_0.9.9b8.zip

cp redsn0w_mac_0.9.9b8/redsn0w.app/Contents/MacOS/Keys.plist .

python python_scripts/kernel_patcher.py **IOS5_IPSW_FOR_YOUR_DEVICE**

sh ./make_ramdisk_n88ap.sh

(????? ????? ram disk ?????make ramdisk?.sh

?? kernelcache.release.nxx.patched ???)

redsn0w -i **IOS5_IPSW_FOR_YOUR_DEVICE** -r myramdisk.dmg -k kernelcache.release.n88.patched

#?usb port iphone ?????port

python usbmuxd-python-client/tcprelay.py -t 22:2222 1999:1999

????????

##?ios ?? SSH ? localhost:2222. ??ios????????

ssh -p 2222 root@localhost

???????alpine
 ????????ctrl-z ??

#????????
 python python_scripts/demo_bruteforce.py

#?keychain?? ??????? UDID ?????
 python python_scripts/keychain_tool.py -d UDID/keychain-2.db UDID/DATAVOLUMEID.plist

#????
 ssh -p 2222 -oStrictHostKeyChecking=no -oUserKnownHostsFile=/dev/null root@localhost "dd if=/dev/
 rdisk0s2s1 bs=8192 || dd if=/dev/rdisk0s1s2 bs=8192" >image.img

#???HFS System??
 python python_scripts/emf_decrypter.py image.img
 #?????
 python python_scripts/emf_undelete.py image.img

Windows ?????

?????ituens ???????

32 ??? applemobiledevicesupport

64???applemoviledvicesupport64

??python2.7 ??
<http://www.python.org/ftp/python/2.7/python-2.7.msi>

?????
http://www.slproweb.com/download/Win...SSL-0_9_8t.exe
<http://www.voidspace.org.uk/download...in32-py2.7.zip>

QT (?????)
<http://www.riverbankcomputing.co.uk/...-gpl-4.9-1.exe>

python ????
<http://www.osslab.com.tw/@api/deki/f...e-packages.rar>
 ?????? /python27/lib/site-packages

??hack ios python code
<http://www.osslab.com.tw/@api/deki/f...0/=hackios.rar>

??? hack ios python code
 ???

tcprelay.py -t 22:2222 1999:1999

??

?? cygwin +ssh ??

ssh -p 2222 root@localhost dd if=/dev/rdisk0s2s1 bs=8192 | dd of=iphone-root.img
 ??cygwin home???.

ssh -p 2222 root@localhost dd if=/dev/rdisk0s2s1 bs=8192 | dd of=iphone-user.img

putty -ssh -P 2222 root@localhost -pw alpine dd if=/dev/rdisk0s2s1 bs=8192 | dd of=iphone-user.img

dd of=/HardDriveBackup.img | putty -ssh -P 2222 root@localhost -pw alpine dd if=/dev/rdisk0s2s1

dd if=/dev/rdisk0s2s1 bs=8192 | ssh root@localhost 'dd of=iphone-dump.img'

iphone 4s , ipad2 ????
 1.???cyndia ?????sshd
 (???????)
 2.??usb port
 3.??

tcprelay.py -t 22:2222 1999:1999

4.?ssh ?putty ??

ssh -p 2222 root@localhost
 ???????alpine

#?????????
 demo_bruteforce.py

#?keychain?? ??????? UDID ??????

```
keychain_tool.py -d UDID/keychain-2.db UDID/DATAVOLUMEID.plist
```

??

?? cygwin +ssh ??

ios 3 /dev/rdisk0s2.

IOS 4 /dev/rdisk0s2s1

```
ssh -p 2222 root@localhost dd if=/dev/rdisk0s2s1 bs=8192 | dd of=image.img
```

IOS 5

```
ssh -p 2222 root@localhost dd if=/dev/rdisk0s1s2 bs=8192 | dd of=image.img
```

??cygwin home???..??iphone4s ??