Save onboard SHSH Blobs for 32-bit device

Note:

- Device needed to be jailbroken, if you are not, use 3utools (3u.com) to do it
- In Cydia, install OpenSSH and Core Utilities if you didn't install it yet

Odyseus - save onboard SHSH Blobs
————————————————————

1. Get Baseband:

./sshtool -s baseband.tar -p 22 deviceIP

2. Build Custom IPSW

./ipsw downloaded.ipsw custom.ipsw -memory baseband.tar
If "error: /tmp/xpwn/hfs/rawfile.c:233 allocate"
.ipsw normal.ipsw custom.ipsw -S 20 baseband.tar
Still error - try -S 50

3. Extract iBSS

./xpwntool `unzip -j custom.ipsw 'Firmware/dfu/iBSS*' | awk '/inflating/{print $2}'` pwnediBSS

4. Extract iBEC

mv `unzip -j custom.ipsw 'Firmware/dfu/iBEC*' | awk '/inflating/{print $2}'` pwnediBEC

5. Boot PWNed

./sshtool -k ../kloader -b pwnediBSS -p 22 deviceIP
./irecovery -f pwnediBEC

6. Extract onboard SHSH Blobs

./irecovery -s
/send ../payload
go blobs
/exit
./irecovery -g myblob.dump
./irecovery -s
reboot

7. Validating Blobs

./ticket myblob.dump myblob.plist custom.ipsw -z - copy ECID in output

./validate myblob.plist downloaded.ipsw -z - Should say: “myblobs.plist seems usable for ECID 0x0000000000000000”

8. Make Blobs usable

Rename the “myblob.plist” file to “ECID-iPhoneX,X-X.X(.X).shsh”

^ | ^

iPhone model | iOS version

Restore device with Future Restore to same iOS while lose jailbreak

———————————————————————————————————

1. Add following Repo on Cydia on iOS: http://repo.tihmstar.net
2. Go to System -> kDFUApp on newly added repo
3. Slide all slider until they are green, then click on “Enter kDFU” to enter kDFU mode
4. Open Terminal, and type “cd “ and insert the Future Restore folder to the terminal window and press Enter
5. ./futurerestore_macos -t SHSH.shsh --latest-baseband --use-pwndfu IPSW.ipsw

- Replace SHSH.shsh with the name of your .shsh file.
- Replace IPSW.ipsw with the name of your .ipsw file.
- If you are using a non-cellular device, like a WiFi-only iPad or an iPod touch, replace –latest-baseband with –no-baseband.

6. Hit Enter, and do not disconnect device while it’s restoring, and look out for errors. If your iOS device flash green, and an Apple logo appear, that mean the restore is processing.
7. The device should boot into the setup screen, and you are done!