

Notifications disabled (click to enable)

What's new! More

### Working iPhone recovery ramdisk with SSH (Discussion wave 3)

# Yes, this is the comment wave!

Discussion archive:

- [Discussion wave 1 \(slow, read-only\)](#)
- [Slow Discussion wave 2 \(WAS: Working iPhone recovery ramdisk with SSH\)](#)

## >> Up to date instructions HERE <<

Davelee1097@googlewave.com: Hi, Jun 16

I bought an iPhone 2g from ebay a couple of days ago, I don't know the history of it but it's stuck in recovery mode. I can get it to boot to the Apple logo but that's where it hangs, I have also enabled verbos ,ode on it and it seems to hang around where is gets MAC addresses. I have tried doing a restore through iTunes with no success and in every which way possible. I think it seems to be a problem with the kernel but no too sure, I came across the SSH'ing into the phone but have come stuck!

When opening RamDiskBuilder.exe and selecting "018-6136-014.dmg" my computer just freezes and it comes up saying the program has stopped working. I was wondering if someone could please upload or email me a copy of this file that has been run through ramdiskbuilder? My email address is davelee1097@ntlworld.com

I also can't find the keys for a 2g iPhone on 3.1.2 FW.

Thanks a lot for your time.

Dave

iPhone 2g running 3.1.2 FW  
O/S: Windows 7 Ultimate

Msft.guy@googlewave.com: Just use DFU restore, you have no business restoring data from phones bought on eBay. Jun 20

Tunnelcoder@googlewave.com: Aug 11

1:03 pm

Hi,  
Top tutorial - thank you! Wondered if you could assist with a problem im having when trying to image my device. I upload the dmg.ssh without issues, but when I issue the command 'ramdisk' as you do in your video it just moves to the next line and does nothing. I have managed to issue this command 'ramdisk' exactly like your video and receive the reply 'filesize variable invalid or not set, aborting' but not get any further.  
Any thoughts or ideas?  
Thank you

Msft.guy@googlewave.com: Please read the updated tutorial that describes uploading ramdisk using itunnel\_mux tool. Aug 11

Tunnelcoder@googlewave.com: thank you for your reply, I have found the tutorial and issued the 'itunnel\_mux\_r61.exe followed by ibss ibec ramdisk devicetree kernelcache commands (all with firmware and files filled in). The program runs the device turns white, then late black during the process gets to 'Kernelcache kernelcache.release.n88' and then just sits there doing nothing. Any thoughts? Thank you Aug 12

Tunnelcoder@googlewave.com: may be important for me to add. When i quit from stuck process and issue reboot command the phone restarts correctly. I have tried using a combination of techniques to get an image from device, including running itunnel\_mux\_rev4. Once I open putty to connect to port 22 the itunnel shows 'error: device service' and network is refused - im guesing this is because I havent loaded the ramdisk correctly. Thanks Aug 12

Msft.guy@googlewave.com: I'm not quite sure what exactly you're trying to do - can you maybe please post details about your device and exact command line you are running? Aug 12

Tunnelcoder@googlewave.com: would any of this work on an ipod touch 2g? does the device have to be jailbroken? thanks Aug 16

Msft.guy@googlewave.com: Yep; you'll need to use iReb first if not jailbroken. Aug 16

Tunnelcoder@googlewave.com: Thank you for your responce. The following is the log and details of device, do you have a direct e-mail rather than good reader? I am using a Windows XP SP3 machine with iTunes 9.2 Installed: Aug 23

The device is an iPhone 3gs running v4.0.1

I also place the device in recovery mode as it is not recognised in DFU mode.

After downloading your tools and creating + extracting the custom firmware I run the following:

```
itunnel_mux_r61.exe --ibec iBEC.n88ap.RELEASE.dfu --ramdisk 018-8234-001.dmg.ssh --devicetree DeviceTree.n88ap.img3 --kernelcache kernelcache.release.n88 --ramdisk-delay 5
```

I have also tried:

```
itunnel_mux_r61.exe --ibec iBEC.n88ap.RELEASE.dfu --ramdisk 018-8234-001.dmg.ssh --devicetree DeviceTree.n88ap.img3 --kernelcache kernelcache.release.n88 --ramdisk-delay 5 --ramdisk-command "ramdisk 0x90000000"
```

The result: Once the iBEC uploads the script stops at callback and I am forced to unplug and replug the device before it continues. The same happens at the Kernelcache. Once all have been uploaded it then does the same again (loops) starting with the iBEC etc etc. I have also tried using the same method on an iPod Touch running v2.2.1 which results in the same (even after using iReb).

I have also tried running the second method suggested:

```
irecovery -f 018-8231-001.dmg.ssh
irecovery -c "ramdisk"
irecovery -f kernelcache.release.n88
irecovery -c bootx
```

and

```
irecovery -f 018-8231-001.dmg.ssh
irecovery -c "ramdisk 0x90000000"
irecovery -f kernelcache.release.n88
irecovery -c bootx
```

where in both cases after entering the ramdisk command, nothing appears as if the command was ignored - it doesn't show anything such as creating ramdisk etc. When issuing the extra parameters '0x90000000' it sometimes shows 'ramdisk too big'. I have also tried going into irecovery -s and issuing ramdisk on its own.

I would be very grateful for any help,

Thank you so much



Msft.guy@googlewave.com: **Won't work** on a non-jailbroken 4.x 3GS without saved 3.1.2 SHSH (use FW Umbrella to check).

Aug 31 ▾



Wisehassaan@googlewave.com and Nguyenbakim@googlewave.com: i was listening music on my 2g fw 3.0.0 and suddenly it crashed, now when i start it apple logo shows and then it shuts down. Now i have to copy data so that i can restore. i am having same problem as Tariman21@googlewave.com. When i run ramdisk cmd it reboots. also RamDisk.exe crashes when pwn 018-5305-002.dmg is used. Using restore keys from [http://theiphonewiki.com/wiki/index.php?title=Kirkwood\\_7A341\\_%28iPhone%29](http://theiphonewiki.com/wiki/index.php?title=Kirkwood_7A341_%28iPhone%29) So i used original 018-5305-002.dmg and pwn kernelcache.release.s5l8900x. But no success. Then i tried the itunnel\_mux\_rev6.exe --ibec iBEC.pwned.dfu --ramdisk xxxx.dmg.ssh --devicetree DeviceTree.xxxxx.img3 --kernelcache kernelcache.pwned but having the following error <http://pastie.org/1042332>  
Please any help

Jul 28 ▾



Msft.guy@googlewave.com:

Try using 'ramdisk 0x90000000' or 'ramdisk 0x09000000'  
Also be sure to use correct keys and ramdisk file from original FW with RamdiskBuilder.

Jul 13 ▾



Wisehassaan@googlewave.com: i am using the correct keys. RamdiskBuilder only crashes when i use 018-5305-002.dmg from fw created by pwnageTool. Now i have tried the ramdisk 0x90000000 see the pastie

<http://pastie.org/1042436>  
iPhone hangs after that and after 15 min it restarts.

Jul 13 ▾



Wisehassaan@googlewave.com: now tried bootx cmd in irecovery -s

```
C:\irecovery>irecovery -s
iRecovery - Recovery Utility
by westbaer
Thanks to pod2g, tom3q, planetbeing, geohot and posixninja.
```

```
Found iPhone/iPod in Recovery mode
] bootx
Attempting to validate kernelcache @ 0x09000000
Loading kernel cache at 0xb000000...data starts at 0xb000180
done
gBootArgs.commandLine = [rd=md0 nand-enable-reformat=1 -progress ]
Installing WIFI Calibration
]
```

but same iPhone hangs in recovery mode and restarts after 15 min

full log  
<http://pastie.org/1042460>

Jul 13 ▾



Msft.guy@googlewave.com: Looks like it starts booting, but fails at some point.. not sure if this can be easily fixed. Using verbose iBEC may help figure out what happens on boot. Do you see Apple logo on the screen during those 15 minutes?

Jul 13 ▾



Wisehassaan@googlewave.com: not the apple logo but the iPhone displays a rotating progress indicator in recovery mode just like the screenshot DSC\_0491 above. The indicator spins for 15 min then iPhone restarts. The progress indicator shows up when i enter bootx cmd.

Jul 14 ▾



Msft.guy@googlewave.com: Try 3.1.2 fw

Jul 14 ▾



Wisehassaan@googlewave.com: ok i am trying on 3.1.2 ramdisk

Jul 14 ▾

```
Wisehassaan@googlewave.com: ok i tried on 3.1.2
now RamdiskBuilder does'nt crash with custom 018-6136-014.dmg
keys used http://theiphonewiki.com/wiki/index.php?title=Northstar_7D11_%28iPhone%29
first i tried in recovery mode. i got error on bootx
Found iPhone/iPod in Recovery mode
] bootx
Attempting to validate kernelcache @ 0x09000000
error loading kernelcache
```

```
then i tried in dfu mode
itunnel_mux_r6.exe --ibec iBEC.m68ap.RELEASE.dfu --ramdisk 018-6136-014.dmg.ssh --devicetree DeviceTree.m68ap.img3 --kernelcache kernelcache.release.s5l8900x
```

but same iPhone restarted

full log  
<http://pastie.org/1045226>

Jul 15 ▾



Msft.guy@googlewave.com: use version r61 and add `--ramdisk-delay 5` parameter.

Jul 15



Wisehassaan@googlewave.com: tried on r61

Jul 15

iPhone restarts after line

178 WinDFU::FinalizeDfuUpdate: success

full log

<http://pastie.org/1045250>

thanks buddy for your hard work.....



Msft.guy@googlewave.com: Hmm.. try also adding

Jul 15

`--ramdisk-command "ramdisk 0x9000000"`

Note only 6 zeroes and also quotes ..

if still doesn't work, install TeamViewer and email id/pw to msft.guy@gmail.com



Wisehassaan@googlewave.com: finally it worked after adding

Jul 15

`--ramdisk-command "ramdisk 0x9000000"`

but can't copy user data part

putty error

```
-sh-4.0# mount_hfs /dev/disk0s2s1 /mnt2
```

```
mount_hfs: No such file or directory
```

winscp shows mnt2 directory but its' empty



Msft.guy@googlewave.com: You need **disk0s2**; disk0s2s1 is ip4, 3GS and ipt3 only

Jul 15



Wisehassaan@googlewave.com: putty error

Jul 15

```
-sh-4.0# mount_hfs /dev/disk0s2 /mnt2
```

```
mount_hfs: Invalid argument
```



Msft.guy@googlewave.com: did fsck\_hfs run ok?

Jul 15



Wisehassaan@googlewave.com and Msft.guy@googlewave.com: see it

Jul 15

```
-sh-4.0# fsck_hfs /dev/disk0s2
```

```
** /dev/disk0s2
```

```
** Checking Non-joumaled HFS Plus volume.
```

```
** Detected a case-sensitive catalog.
```

```
** Checking Extents Overflow file.
```

```
** Checking Catalog file.
```

```
Invalid node structure
```

```
(4, 246)
```

```
** Volume check failed.
```

```
-sh-4.0# fsck_hfs /dev/disk0s1
```

```
** /dev/disk0s1
```

```
** Verifying volume when it is mounted with write access.
```

```
** Checking Non-joumaled HFS Plus volume.
```

```
** Detected a case-sensitive catalog.
```

```
** Checking Extents Overflow file.
```

```
** Checking Catalog file.
```

```
** Checking multi-linked files.
```

```
** Checking Catalog hierarchy.
```

```
** Checking Extended Attributes file.
```

```
** Checking volume bitmap.
```

```
** Checking volume information.
```

```
** The volume Kirkwood7A341.iPhoneOS appears to be OK.
```

```
-sh-4.0# /mnt/bin/ls /mnt1
```

```
-sh: /mnt/bin/ls: No such file or directory
```

```
-sh-4.0# /mnt1/bin/ls /mnt1
```

```
Applications Library User boot dev lib private tmp var
```

```
Developer System bin cores etc mnt sbin usr
```

```
-sh-4.0#
```



Msft.guy@googlewave.com: Looks like user volume is corrupted..

Jul 15

Copy /dev/disk0s2 using PsFtp or winscp in sftp mode (or cyberduck); then rename to .dmg and use HFS+ recovery software.

You can also try adding '-r' flag to fsck\_hfs, maybe that helps



Wisehassaan@googlewave.com: like

Jul 15

```
fsck_hfs -r /dev/disk0s2
```

?



Wisehassaan@googlewave.com: error copying with winscp in sftp mode

Jul 15

Bad message (badly formatted packet or protocol incompatibility).

Error code: 5

Error message from server: Bad message

Request code: 5



Msft.guy@googlewave.com: psftp does copy that, I think winscp fails because this is a special device and its size is unknown.

Jul 15

Use the

```
get /dev/disk0s2
```

command in psftp.



Wisehassaan@googlewave.com: get /dev/disk0s2

Jul 15

where will be the file downloaded to?

log:

```
psftp> get /dev/disk0s2
```

```
remote:/dev/disk0s2 => local:rdisk0s2
```



Msft.guy@googlewave.com: current dir, you will have to wait a while..

Jul 15

 Wisehassaan@googlewave.com: ok i see it copying now. Are there anymore files which i should copy that contain my data. Like songs, pictures, contacts etc. or this single file contains everything. Because i am not sure whether i could get another chance to copy. Can you specify good hfs+ recovery software? Jul 15 ▾

 Wisehassaan@googlewave.com: i was able to recover my data from rdisk0s2.dmg thanks a lot for the support. Jul 17 ▾

 + ▾  
Oct 29 ▾

 Me: .. Oct 30 ▾

 Sssteven15@googlewave.com: hey buddy, Everything goes according to plan when i run through ur tutorial on my iphone 3gs older bootrom but once i launch iphone\_tunnel, the putty ssh thing doesnt turn up :( any ideas? Jun 16 ▾

 Msft.guy@googlewave.com: Paste the output of itunnel; make sure you are running iTunes 9.1 + Jun 20 ▾

 Sssteven15@googlewave.com: thanks mate, this is what i get. Ive used the kernalcache from pwnagetool from a mac 3.1.2 as well. Jun 22 ▾  
iphone\_tunnel v2.0 for Mac  
created by novi. (novi.mad@gmail.com)  
Restore mode hack by msft.guy((rev 4))

```
Usage: iphone_tunnel [<iPhone port> <Local port> [Device ID, 40 digit]]
Example: iphone_tunnel 22 9876 0123456...abcdef
Default ports are 22 22
Waiting for device...
Device connected: f65eac36e934af4cad187ebb12662a8097e7b4a1
Info: Waiting for new TCP connection on port 22
```

The iphone goes to the apple with the progress bar underneath but then it just sits here for ages and the iphone tunnel does nothing after that. Any advice? thanks buddy.

 Msft.guy@googlewave.com: have you tried connecting to localhost with putty ? .. Jun 22 ▾

 Sssteven15@googlewave.com: No i havent tried that program, can you send me the link please? I'm a noob at this stuff lol thanks for your help Jun 22 ▾

 Msft.guy@googlewave.com: UGH. Google it. Jun 22 ▾

 Sssteven15@googlewave.com: Hey buddy, so i connected using putty and then and then when i try to insert the mount\_hfs /dev/diskOs1 /mnt1, it says no such file or directory and also with Jun 27 ▾  
i tried the fsck\_hfs /dev/diskOs1 and it says no such file or directory as well. Any ideas on this problem?  
Also, when I input mount\_hfs /dev/diskOs1 and this is what comes up:  
usage: mount\_hfs [-xw] [-u user] [-g group] [-m mask] [-e encoding] [-t tbuffer-size] [-j] [-c] [-o options] special-device filesystem-node  
-j disables journaling; -c disables group-commit for journaling <t tbuffer-size> [-j] [-c] [-o options] special-device filesystem-node  
Any ideas what these mean?

 Msft.guy@googlewave.com: Means you can't read. Just paste the commands, don't try to type them in if you cannot do it correctly. O != 0 Jun 29 ▾

 Sssteven15@googlewave.com: ok so this is what i get in putty Jun 29 ▾  
-sh-4.0# mount  
/dev/md0 on / (hfs, local, read-only)  
devfs on /dev (devfs, local)  
-sh-4.0# mount /dev/diskOs1 /mnt1  
/dev/diskOs1 on /mnt1: Operation not supported by device  
-sh-4.0# mount\_hfs /dev/diskOs1 /mnt1  
mount\_hfs: No such file or directory  
-sh-4.0# mount\_hfs /dev/diskOs1 /mnt1  
mount\_hfs: No such file or directory  
-sh-4.0# mount\_hfs /dev/diskOs1 /mnt1  
mount\_hfs: No such file or directory  
-sh-4.0# fsck\_hfs /dev/diskOs1  
/dev/diskOs1: No such file or directory  
Can't stat /dev/diskOs1  
Can't stat /dev/diskOs1: No such file or directory  
Im not sure why it does this.

 Msft.guy@googlewave.com: Use WinSCP or CyberDuck to list the contents of /dev/ directory, list the devices starting with 'disk' Jun 29 ▾

 Trvnut1@googlewave.com: I'm having the same problem and I have an updated version of Itunes 9.1. Any other ideas? Putty pops up but there is no login and I'm unable to type anything. Jun 21 ▾  
Also I am using kernalcache file Iphone 2.1\_3.1.2\_7d11\_restore that was on my computer from either a previous restore or the original Blackrain.

 Msft.guy@googlewave.com: You aren't using the right kernalcache, please reread the instructions. Jun 21 ▾

 Daniel.mcgeary@googlewave.com: What steps should I take a jailbroken 3GS with 3.1.3? When I select the dmg in RamDisk Builder, it crashes. Jun 19 ▾

 Msft.guy@googlewave.com: You are not using correct key/IV. Jun 20 ▾

Daniel.mcgeary@googlewave.com: NVM, I didnt read the readme. im such a douche.

Jun 21

Daniel.mcgeary@googlewave.com: Where do I get the right Key/IV?

Jun 21

Elias.eldabbagh@googlewave.com: could you provide a more detailed way of making a custom IPSW file. I have an iPhone 3G 3.1.2 and I get the automatic reboot after the "ramdisk" cmd.

Jun 19

I have also tried iRecovery -f iBEC.n88ap.RELEASE.dfu - however the file name present in my PWND ipsw file is iBEC.m68ap.RELEASE.dfu - went ahead anyway and tried again, no avail.

Elias.eldabbagh@googlewave.com: the instruction of making an IPSW file from the other wave gave me an error in iTunes because of incompatibility. Im going to start over with a fresh firmware file and PWN it an go through the process again, This is turning out to be quite tedious.

Jun 20

-> It still dosent work... Im still stuck at ramdisk

Msf.guy@googlewave.com: If you've bothered to read the instructions, you might have noticed that 3G iPhones need 'ramdisk 0x90000000' command.

Jun 20

Elias.eldabbagh@googlewave.com: I did read, and and enter ramdisk 0x90000000

Jun 22

Elias.eldabbagh@googlewave.com: the cmd does nothing - I even used iReb and got the white screen - tried -f BEC.n82ap.RELEASE.dfu ; -c go ;; th meaning i can copy files right?

Jun 22

yes - i can upload the files fine it says "Successfully uploaded file!" after the cmd  
one moment

iRecovery -c returns "iRecovery - Recovery utility..."

so if my version dosent support -c where should I go?

ok - let me get your version - I restarted from scratch on a new computer and just downloaded it off of google

should I be trying all of this on the white screen? (caused via ireb)

ok

yes - custom 3.1.2 ipsw for iPhone 3G

just resent .dmg.ssh

done

-c ramdisk 0x90000000

that cmd returns "iRecovery - Recovery utility for 0x1281 and WTF by..." wait - used the rong iRecover again

ok starting with new iRecovery

copying the file now

ok now irecover -s Entering recovery mode, starting CMD prompt

how do I know when I can enter cmds? ok entering -c cmd now

-c ramdisk 0x90000000

i hit enter and it returned

]

im on mac BTW

should I try the cmd again, doing it again just returns to the next line with a new ]

this is where I got stuck last time as well on that next prompt place -f kernelcache and then -c bootx

ok i exited

now i need to do the -s before i can do the -c

im sorry - i know im a total noob aat this and no matter how many times I read and read the forum the details get lost on me

now after copying the kernel - i did /irecovery -s

and It wont got to the prompt - it is just stuck two lines down with a grey cursor

no it dosent

the last line it prints is Thanks to pod2g...

ok copying

-s

nope - stuck in the same place again :/

resending again stuck at that second line...

while waiting at that line - the iphone turned off

repeated all the steps again - and still got the cursor on the second line after copying the kernel

are there any other ways to go about this? what about the itunes restore method?

thats the thing - there is no consol output other then the automotatic print text from iRecover ok let me start over - the iphone rebooted just now

ok

1. iphone in restore mode

2 quit itunes

3. open termial

drag and drop irecover -f 018-6136-014.dmg.ssh

sending bytes

closing usb connection

irecover -s

Msf.guy@googlewave.com: post **everything on the terminal from the beginning of the latest attempt** to current state.

Jun 22

including your commands

open new cmd window then use edit - copy all

you are probably doing something wrong

post your console output here.

it's expected on 3g

just go to the next step

kemelcache etc

Ctrl+c or /exit before you do that..

Elias.eldabbagh@googlewave.com: Last login: Tue Jun 22 21:55:05 on ttys000

Jun 22

Elias-MacBook:~ Elias\$ /Users/Elias/Downloads/irecovery/irecovery -f /Users/Elias/Desktop/iPhone1,2\_3.1.2\_7D11\_Custom\_Restore/018-6136-014.dmg.ssh

iRecovery - Recovery Utility

by westbaer

Thanks to pod2g, tom3q, planetbeing and geohot.

Found iPhone/iPod in Recovery mode

Loaded image file (len: 0xff7974, packets: 8176, last: 0x174).  
Sending 0xff7974 bytes  
Sending 0x800 bytes in packet 0... OK

'..... 6000 lines later"

Sending 0x800 bytes in packet 8174... OK  
00 01 00 00 05 00  
Sending 0x174 bytes in packet 8175... OK  
00 01 00 00 05 00  
Successfully uploaded file!  
Executing it...  
00 01 00 00 06 00  
00 FFFFFFFB8 0B 00 07 00  
00 01 00 00 08 00  
Closing USB connection...  
Elias-MacBook:~ Elias\$ /Users/Elias/Downloads/irecovery/irecovery -siRecovery - Recovery Utility  
by westbaer  
Thanks to pod2g, tom3q, planetbeing and geohot.

```
=====
::
:: iRain for n82ap, Copyright 2009, Apple Inc.
::
:: BUILD_TAG: iBoot-636.65
::
:: BUILD_STYLE: RELEASE
::
:: USB_SERIAL_NUMBER: CPID:8900 CPRV:30 CPMF:03 SCEP:05 BDID:04 ECID:0000307DC014DAC IBFL:01 SRNM:[868409SXY7H]
::
=====
```

```
[FTL:MSG] Apple NAND Driver (AND) RO
[NAND] Device ID      0xba94d598
[NAND] BANKS_TOTAL   4
[NAND] BLOCKS_PER_BANK 4096
[NAND] SECTORS_PER_PAGE 824288
[NAND] BYTES_PER_SPARE 216
[FTL:MSG] FIL_Init    [OK]
[FTL:MSG] BUF_Init    [OK]
[FTL:MSG] FPart Init  [OK]
read old style signature 0x43303035 (line:371)
[FTL:MSG] VFL Register [OK]
[FTL:MSG] VFL Init     [OK]
[FTL:MSG] VFL_Open     [OK]
[FTL:MSG] FTL Register [OK]
[FTL:WRN] Failure running _LoadFTLCxt!
[FTL:WRN] Recovering NAND Data Structures - this will take some time!
[FTL:WRN] _FTLRestore OK!
[FTL:MG] FTL_Open     [OK]
Boot Failure Count: 15 Panic Fail Count: 0
Entering recovery mode, starting command prompt
```

```
w
] w
] -c ramdisk 0x90000000
]
```

 Elias.eldabbagh@googlewave.com: and i stoped proceding forward because I suspect this is where the first error is

Jun 22 ▼

 Msft.guy@googlewave.com: Either type iRecovery -c COMMAND in terminal  
or just COMMAND in interactive prompt.  
also in case you used -f command inside of the iRecovery interactive prompt, that doesn't work either.  
Start iRecovery -s, type JUST THE COMMAND, look at the result, then press Ctrl+C to go BACK to the terminal ;)

Jun 23 ▼

 Msft.guy@googlewave.com: hmm?  
does it say iphone found?  
reconnect usb  
then repeat from -f kernelcache step

Jun 22 ▼

 Msft.guy@googlewave.com: check if your irecovery even supports the -f command )  
-f = upload  
-c supported as well?  
what's the output without parameters?  
i have all links to the tools in the main wave -)  
won't hurt .  
is the ibec you are uploading from a custom ipsw?  
there is no response to -c, you should use -s mode to see the response ;)

Jun 22 ▼

 Msft.guy@googlewave.com: use -f to upload, only use -s for commands that you entered using -c

Jun 22 ▼

 Ayeayre@googlewave.com: I'm having a problem,  
I'm at the point where I type 'ramdisk 0x90000000' ("zero-x-nine-(7x zero's)") in iRecovery, but then I get 'Permission Denied'  
Any ideas?  
Really desperate, any help will be much appreciated.  
Thanks..

Jun 21 ▼

device:  
WinXP (access to Win7 64bit & Mac OS 10.4.11)  
iPhone 3G on 3.0 (cydia/rock update problem, reboot loop, iBeej's fixes don't work, tried on Win & Mac)  
Just updated libusb from 0.1.12.2 to 1.1.14.3 and iRecovery to 0.3.2, still the same..

 Ayeayre@googlewave.com: I tried using irecovery -c "ramdisk 0x90000000" with quotes and it just went to next line with a ] so now it looks like (last 3 lines):

Jun 21 ▼

```
Entering recovery mode, starting command prompt
←[m] ] irecovery -c "ramdisk 0x90000000"
]
```

ok i tried just using ramdisk only and I got:  
creating ramdisk at 0xc000000 of size 0xf68c00, from image at 0x9000000

should I proceed to next step? I don't want to loose any data, im scared :( lol

well I'm not even sure how to proceed anyway, it followws with a ] on the next line, then if i try and type anything it comes up as ^@ for each character I type..

I'm off to bed, ill check back after work tomorrow, thanks for anyone that can help me, really need stuff off this phone.  
thanks

 Msft.guy@googlewave.com: Use Ctrl+C or /exit command to close iRecovery, then proceed to the next step (iRecovery -f kernelcache). Good luck!

Jun 21 ▼

 Daniel.mcgeary@googlewave.com: Ok, now I'm sure I got the right key/IV for iPhone 3GS 7E18 3.1.3 ramdisk restore. I put the keys in and select the dmg, then....program crashes. Any ideas? Is it bcause I'm using Win7?

Jun 21 ▼

 Msft.guy@googlewave.com: [http://theiphonewiki.com/wiki/index.php?title=SUNorthstarTwo\\_7E18\\_\(iPhone\\_3GS\)#Restore\\_Ramdisk\\_28018-6495-022.dmg.29](http://theiphonewiki.com/wiki/index.php?title=SUNorthstarTwo_7E18_(iPhone_3GS)#Restore_Ramdisk_28018-6495-022.dmg.29) - those?

Jun 21 ▼

### Restore Ramdisk (018-6495-022.dmg)

- IV: 50a5d7418e3091a2c1d878495a6dbc6a
- Key: 217c7c38387264f2a2fef7a661d1bbeb705e7c90581c5b73055fe44f5bbc0498

Works fine for me on win7, doubt that's the problem

 Daniel.mcgeary@googlewave.com: hmmm...weird. thats the key im using. and i used sn0wbreeze to create the custom ipsw. and i extracted those two files that you did in the video.

Jun 21 ▼

 Daniel.mcgeary@googlewave.com: nvm

Jun 21 ▼

 Daniel.mcgeary@googlewave.com: OK not exactly sure where I messed up, but now I'm getting iPhone not found. Is there a way to start over?

Jun 21 ▼

 Daniel.mcgeary@googlewave.com: when i get to this point "iRecovery -f kernelcache.release.s518920x" this is when I get th no iPhone found. I see that for a 3G something different needs to be entered for ramdisk. should there b something different for th 3GS?

Jun 21 ▼

 Msft.guy@googlewave.com: reconnect USB after sending 'ramdisk 0x900...' command, then proceed with uploading kernelcache. Apparently this tool doesn't like snowbreeze-created ipsw, original should work ok though.

Jun 21 ▼

 Daniel.mcgeary@googlewave.com: yeah thats howi got pass the crashing. so should i just put ramdisk 0x900?

Jun 21 ▼

 Msft.guy@googlewave.com: Again, after you get the 'iPod not found', reconnect the USB cable, then retry the failed step.

Jun 21 ▼

 Daniel.mcgeary@googlewave.com: ahhh ok.

Jun 21 ▼

 Daniel.mcgeary@googlewave.com: Would the tunnel software work with the most recent release of itunes? I'm on 9.0 and i get the error could not load itunesmobiledevice.dll

Jun 21 ▼

 Jcutrone@googlewave.com: Having trouble getting this to work on a 3G (A1241) using a pwnagetool'd 3.1.2 FW (iBoot-596.24)

Jun 21 ▼

'ramdisk 0x90000000' always gives Permission Denied. 'ramdisk' always puts me back to the prompt.  
both the 018-6136-014.dmg.ssh and kernelcache.release.s518900x seem to upload fine. but then bootx does nothing (itunes + USB logo sits there)

also tried loading iBEC.n82ap.RELEASE.dfu and then -c go, just sits in restore mode.  
I had Wifi sync installed but removed it. Any suggestions?

 Msft.guy@googlewave.com: use iReb then all iRecovery steps (ramdisk etc)

Jun 22 ▼

 Jcutrone@googlewave.com: iH8sn0w - iREB V3.1.2 For Windows-English.exe doesnt give a white screen when I select 3G. The phone sits there in DFU mode and does nothing. I first tried with iTunes 9.2, then downgraded iTunes to 9.0.3. I'm not sure which FW is on the phone because its passcoded, would 3.1.3 on the phone make iReb not work? Any alternative?

Jun 22 ▼

 Msft.guy@googlewave.com: fw doesn't matter as long as the phone is in dfu

Jun 22 ▼

 Jcutrone@googlewave.com: Is there anything else I could try? iReb never turns the screen white like it says it should. I tried multiple combinations of DFU and restore mode. Still getting 'Permission Denied' when I do 'ramdisk 0x90000000'

Jun 22 ▼

I also notice this error in irecovery:  
Attempting to validate kernelcache @ 0x09000000  
error loading kernelcache

As if I were typing a zero between the 0x and the 9, but I'm not.

 Daniel.mcgeary@googlewave.com: Hey msft.guy,  
Thanks a bunch. I was able to get all the files I needed off.  
You're the man.

Jun 21 ▼

 Msft.guy@googlewave.com: Congrats :-)

Jun 22 ▼



Ayeayre@googlewave.com: thanks Msft.guy, everything seems ok, after i use bootx it says:

Jun 22 ▾

Attempting to validate kernelcache @ 0x90000000

Loading kernel cache at 0xb000000...data starts at 0xb000180

done

gBootArgs.commandLine = [rd=md0 nand-enable-reformat=1 -progress ]

Installing WIFI Calibration

]

now my iPhone is still at the recovery mode screen with usb to itunes logo but it has the spinning thing at the bottom and that's it..is that what it's supposed to do?

do I /exit out of of irecovery and close command prompt and follow next step?

thanks again, much appreciated..

Edit: the phone restarted itself anyway and then started the reboot loop again..

but when i try again, do I /exit and continue to next step?

sorry if I'm breaking your b4lls, just want it to work (phone's been down for about a month now, maybe more) and secondly don't want to do any damage that can't be undone..

thanks again for your help..



Msft.guy@googlewave.com: is iTunnel running? it should not show the spinning wheel until you connect to the phone using ssh/putty.

Jun 22 ▾

otherwise you seem on the right track, iRecovery steps-wise



Ayeayre@googlewave.com: iTunnel isn't running, I restarted the computer and tried again to make sure, same thing..

Jun 22 ▾

should have the progress bar at this stage right?

Any ideas?

Ill check back after work tomorrow..

Thanks again anyway..



Msft.guy@googlewave.com: since you are on 3.0 and trying to load 3.1.3 it might make sense to upload and use devicetree as well (after ramdisk).

Jun 22 ▾

File is DeviceTree.something.img3 , the command after upload is iRec -c devicetree

If that doesn't work then try also loading ibec file from pwned ipsw (the n82 version) and then executing 'go' command before running all other irecovery commands.



Ayeayre@googlewave.com: sorry if this is dumb, but what do you mean load 3.1.3? all the files im using come from 3.0 fw

Jun 22 ▾

thanks



Msft.guy@googlewave.com: yep, try with 3.1.2 or 3.1.3 now

Jun 22 ▾



Ayeayre@googlewave.com: ok, i tried 3.1.2 but now after i type the bootx command i get:

Jun 23 ▾

Attempting to validate kernelcache @ 0x09000000

error loading kernelcache

]

I am using pwnage tool to create custom fw if that makes any difference, i dunno, any ideas?

thanks



Msft.guy@googlewave.com: Please post full console output..

Jun 23 ▾



Ayeayre@googlewave.com: sure here, <http://www.pastie.org/1015711>

Jun 23 ▾



Ayeayre@googlewave.com: any ideas by any chance?

Jun 24 ▾



Msft.guy@googlewave.com: since you have a 3G, try using iReb, it uploads a newer version of iBSS than what you have. Also upload devicetree and use 'devicetree' command after ramdisk and before kernelcache.

Jun 29 ▾



Ayeayre@googlewave.com: thanks, i'm dling ireb now, is devicetree in the custom fw?

Jun 30 ▾



Msft.guy@googlewave.com: You can use either; it's not patched.

Jun 30 ▾



Ayeayre@googlewave.com: sorry if this is a dumb question, but when do i use iReb?

Jun 30 ▾



Msft.guy@googlewave.com: You put the phone in DFU, use iReb in order to get the phone to show the white screen, then you can proceed with the instructions (irec -f ramdisk, etc)

Jun 30 ▾



Ayeayre@googlewave.com: sweet ill give it a try n let u know how i go, thanks a lot..

Jun 30 ▾



Jcutrone@googlewave.com: Ayeayre, i'd be curious to know if it works for you. I was having the same issues as you, I tried iReb as per Msft.guys suggestion but can never get it to go white screen.

Jun 30 ▾



Ayeayre@googlewave.com: ill let u know as soon as i get time to give it a try..hopefully it's good news..

Jul 2 ▾



Jcutrone@googlewave.com: Finally got iReb to give me the white screen. Had to completely uninstall all Apple/iTunes related software. Then I reinstalled iTunes 9.0.2.25.

Jul 2 ▾



Jcutrone@googlewave.com: Just to recap:

Jul 2 ▾

1) I run iReb and get the white screen after installing iTunes version above.

2) With the white screen up I run 'irecovery -f 018-6136-014.dmg.ssh' it uploads fine

3) White screen still up, i run 'irecovery -s' and then 'ramdisk 0x90000000' and see no output. I /exit

4) I run 'irecovery -f DeviceTree.n82ap.img3' and then 'irecovery -s' then 'devicetree'. no output. /exit

5) I run 'irecovery -f kernelcache.release.s518900x' it uploads fine.

6) I run 'irecovery -c bootx' and the white screen goes away and gives me a dark (backlit) screen. But i'm not getting the Apple logo with progress bar.

I'm going to try a few different ways (using files from pwned 3.1.2 and 3.1.3 FW, also trying just 'ramdisk' as opposed to 'ramdisk 0x90000000'. Also will try fsboot instead of bootx



Jcutrone@googlewave.com: fsboot just seems to boot the device back to the regular lockscreen.

Jul 2 ▼

bootx in irecovery gives this output:

```
] bootx
Attempting to validate kernelcache @ 0x09000000
Loading kernel cache at 0xb000000...data starts at 0xb000180
done
gBootArgs.commandLine = [ ]
Installing WIFI Calibration
```

But im not getting the Apple logo. Trying to run itunnel\_mux anyway. Was failing with an error saying it needed iTunesMobileDevice.dll. Copied that file from iTunes setup.exe to C:\Program Files\Common Files\Apple\Mobile Device Support\



Jcutrone@googlewave.com: I get "Memory image not valid" if I do "go" after uploading the iBEC.n82ap.RELEASE.dfu

Jul 2 ▼

I can get the white screen in DFU mode. But I do the following commands while still in the white screen/DFU mode and it just turns either backlight or will eventually reboot. I pasted all the steps I took: <http://pastie.org/1028885>

See anything wrong?



Msft.guy@googlewave.com: Means iReb didn't work for you..

Jul 2 ▼



Jcutrone@googlewave.com: Hmm, I figured iReb was working because the screen goes white and I stopped getting "Permission denied" when i do ramdisk 0x90000000

Jul 2 ▼



Ayeayre@googlewave.com: ok, which devicetree do I use? I found 2..

Jul 4 ▼

Firmware\all\_flash\all\_flash.m68ap.production\DeviceTree.m68ap.img3

Firmware\all\_flash\all\_flash.n82ap.production\DeviceTree.n82ap.img3

note that it's a 3G and on 3.0 but I'm using this from 3.1.2 fw..



Ayeayre@googlewave.com: ireb isn't doing anything..

Jul 4 ▼



Ayeayre@googlewave.com: tried downgrading iTunes like Jay Cutrone did but still no go..

Jul 5 ▼



Jcutrone@googlewave.com: i think you use n82ap.img3 as per [http://theiphonewiki.com/wiki/index.php?title=Northstar\\_7D11\\_%28iPhone\\_3G%29#Restore\\_Ramdisk\\_.28018-6136-014.dmg.29](http://theiphonewiki.com/wiki/index.php?title=Northstar_7D11_%28iPhone_3G%29#Restore_Ramdisk_.28018-6136-014.dmg.29) you uninstalled itunes (see: <http://support.apple.com/kb/ht1925>) and installed 9.0.2.25?



Ayeayre@googlewave.com: ok sweet I managed to get a white screen thanks to your help, but now when I type the ramdisk command I don't get back what it usually did.. eg. it used to give me: creating ramdisk at 0xc00000 of size 0xff6c00, from image at 0x9000000

Jul 11 ▼

now it just goes to the next line without saying anything as if I just pressed enter



Msft.guy@googlewave.com: does it show an error **when you use ramdisk command without actually uploading ramdisk file first?** maybe you should try that before replying? ;) ugh, the .dmg.ssh one

Jul 11 ▼



Ayeayre@googlewave.com: sorry.. what is the ramdisk file?

Jul 11 ▼



Ayeayre@googlewave.com: ok i turned the phone off and got back to white screen, i then used irecovery -s then ramdisk command, it restarted the phone and it just went to the next line again without giving me any errors or anything.. now its just looping again..

Jul 11 ▼



Ayeayre@googlewave.com: this is doing my head in..everything i do except uploading 018-6136-014.dmg.ssh gives me nothing back and restarts the phone..

Jul 11 ▼



Msft.guy@googlewave.com: TeamViewer?

Jul 11 ▼



Ayeayre@googlewave.com: ill download it now do I need to use the VPN feature? nevermind

Jul 11 ▼

im ready when u are..

ill get back to u tomoro if your available, need to crash atm.. thanks



Msft.guy@googlewave.com: OK, gn8

Jul 11 ▼



Tariman21@googlewave.com: I seem to be having the exact same problem as Ayeayre. I have an iPhone 2G running firmware 3.0.1. My phone used to give the response: "creating ramdisk at 0xc00000 of size 0xf68c00, from image at 0x9000000", but now it restarts when I do anything other than upload. Please help.

Jul 11 ▼



Msft.guy@googlewave.com: For iPhone 2g, put it into DFU, use iReb with iTunes 9.0, then try the instructions after you get a white screen.

Jul 11 ▼



Tariman21@googlewave.com: Already tried it. Uploading ramdisk works fine, but after I enter the ramdisk command my iPhone just reboots.

Jul 11 ▼



Msft.guy@googlewave.com: OK, try itunnel\_mux\_rev6 tool .. itunnel\_mux\_rev6.exe --ibec iBEC.pwned.dfu --ramdisk xxxxx.dmg.ssh --devicetree DeviceTree.xxxxx.img3 --kernelcache kernelcache.pwned the 'pwned' files are from custom ipsw, run this after iReb gets your iPhone to show the white screen.

Jul 11 ▼



Tariman21@googlewave.com: Should I get the pwned devicetree as well?

Jul 11 ▼



Msft.guy@googlewave.com: I don't think it's patched by PwnageTool, but it won't hurt to use a pwned one.

Jul 11 ▼

 Tariman21@googlewave.com: I'm not sure if I'm doing this right, but I keep getting an "Error 0x7E (126): 'Unknown error'. I'm not too sure as to how to use itunnel. Am I supposed to enter that in exactly as shown? Jul 11 ▼

 Msft.guy@googlewave.com: Can you post full output to [pastie.org](http://pastie.org) and link it here? Jul 11 ▼

 Tariman21@googlewave.com: This is all it says, "Error 0x7E (126): 'Unknown error'  
Could not load C:\Program Files\Common Files\Apple\Mobile Device Support\iTunesMobileDevice.dll: ABORTING" Jul 11 ▼

 Msft.guy@googlewave.com: Can you install iTunes 9.2 or 9.1 on another computer and run itunnel\_mux.. there? Jul 11 ▼

 Tariman21@googlewave.com: Sure, I'll do that. I'll get back to you tomorrow though. Have to go to my friend's wedding reception. Thanks for the help. What time will you be available tom? Jul 11 ▼

 Msft.guy@googlewave.com: approx. the same time Jul 11 ▼

 Tariman21@googlewave.com: I tried out what you told me to do and it didn't work. Here's what happened: <http://pastie.org/1040615> and the iPhone restarted. Jul 12 ▼

 Msft.guy@googlewave.com: TeamViewer? Looks like it still reboots after the ramdisk command.. Jul 12 ▼

 Tariman21@googlewave.com: Alright, but I have two computers. One with iTunes 9.0 and one with iTunes 9.2. Should I use the one with the newer iTunes? Jul 12 ▼

 Tariman21@googlewave.com: Are you available to use TeamViewer right now? Jul 12 ▼

 Ayeayre@googlewave.com: hey msft.guy, are u available to give TeamViewer a try atm? Jul 12 ▼

 Msft.guy@googlewave.com: yep, email id/pass already Jul 12 ▼

 Ayeayre@googlewave.com: should be in Jul 12 ▼

 Msft.guy@googlewave.com: msft.guy@gmail.com .. nothing yet Jul 12 ▼

 Ayeayre@googlewave.com: sorry hang on sent Jul 12 ▼

 Ayeayre@googlewave.com: ey msft.guy are u available to give it another try with TeamViewer? I am on another computer with iTunes 9.2..thanks Jul 14 ▼

 Msft.guy@googlewave.com: ok Jul 14 ▼

 Ayeayre@googlewave.com: email sent Jul 14 ▼

 Ayeayre@googlewave.com: thanks a lot, MUCH appreciated, are u in the U.S? Jul 14 ▼

 Msft.guy@googlewave.com: Yeah Jul 14 ▼

 Ayeayre@googlewave.com: sorry i know im a ball breaker..but i accedently disscnected and now now it wont reconnect..do i need to do anything special? Jul 14 ▼

 Msft.guy@googlewave.com: same command line .. did you close itunnel\_mux ? Jul 14 ▼

 Ayeayre@googlewave.com: nope Jul 14 ▼

 Ayeayre@googlewave.com: dunno if this is a dumb question, but do I need to do anything special before/after I copy files? eg. permissions or something, I'm just going to copy over the whole mnt2 dir..everything is in there right? just in case I forget something and when I restore it will b too late..any options i need to make sure are enabled/disabled/checked/unchecked? thanks again Jul 14 ▼

 Ayeayre@googlewave.com: keep getting errors in WinSCP wen transfering /mnt2 i dont think there important but maybe u could shed some light? Jul 15 ▼

Cannot open remote file '/mnt2/mobile/ap blah blah /Library/Preferences/.GlobalPreferences.plist' (which is only 1 of about 20 so far)

No such file or directory.  
Error code: 2  
Error message from server: No such file  
Request code: 3

have to skip all or it will never finish

 Msft.guy@googlewave.com: Probably symlinks are broken because actual file locations are different when mounted to mnt1 and mnt2 than when on live OS. Jul 15 ▼

 Ayeayre@googlewave.com: is it serious? now it says error 141..out of memory.. Jul 15 ▼

 Msft.guy@googlewave.com: not really. You can always copy the whole /dev/rdisk0s2 disk image so that you won't forget anything! Jul 15 ▼

 Ayeayre@googlewave.com: hmmm..soon as i tried doing that i got: Jul 15 ▼

Error

Copying files from remote side failed.

Bad message (badly formatted packet or protocol incompatibility).

Error code: 5

Error message from server: Bad message

Request code: 5

not sure if it means anything but everything in /dev including rdisk0s2 has 0 under 'size'..

 Ayeayre@googlewave.com: ok something went wrong..my comp fukd up..I had to system restore back to before I installed iTunes..everything seems ok now, i also have a macbook, would I have less problems copying using a mac? or should I use PuTTY instead of WinSCP? if its not one thing its another..fukn computers...is it too much to ask for shit to just work?..lol Jul 16 ▼

 Msft.guy@googlewave.com: You can connect to a Mac after getting Apple+progress bar display, then just use CyberDuck to copy the file (/dev/disk0s2). Jul 16 ▼

 Ayeayre@googlewave.com: sweet, will i need anything else installed on the mac? Jul 17 ▼

 Ayeayre@googlewave.com: sorry to b a ballbreaker, but at wat stage do I continue from? Jul 19 ▼

 Msft.guy@googlewave.com: Hmm? You have to repeat the steps to load the ramdisk, then connect your phone to a Mac, then use OS X version of iphone\_tunnel and CyberDuck to copy the volume (disk0s2). If you have difficulties, just email me TeamViewer id again! Jul 19 ▼

 Ayeayre@googlewave.com: sweet im just upgrading to snow leopard so ill giv it a try tmoro..thanks..should b it now Jul 19 ▼

 Ayeayre@googlewave.com: ey, will I need to reinstall Lib-USB on here? (windows 7 64bit comp with older iTunes), i think that's wat fukd things up abit last time so if i dont have to.. Jul 20 ▼

 Msft.guy@googlewave.com: Nope, itunnel thingie doesn't need libUSB. Jul 20 ▼

 Ayeayre@googlewave.com: wait a sec i need newest itunes right? 9.2+ is this the command i need?..after i use ireb to get white screen?  
itunnel\_mux\_r61.exe --ibec iBEC.n82ap.RELEASE.dfu --ramdisk 018-6136-014.dmg.ssh --devicetree DeviceTree.n82ap.img3 --kernelcache kernelcache.release.s518900x  
yes u r right, include that all at once?  
sweet, then in cyberduck i still have to mount n all that? think u helped someone else with it so ill just give it a read above..i hope dont have a lot of time right now, ill give it a go tomoro..thanks again.. Jul 20 ▼

 Msft.guy@googlewave.com: yeah Looks right to me. I think there was also --ramdisk-delay and --ramdisk-command "ramdisk 0x9000000" 6 zeroes on iPhone2g, 7 on iPhone3g yep, on the same command line Jul 20 ▼

 Ayeayre@googlewave.com: u around msft.guy? Jul 23 ▼

 Msft.guy@googlewave.com: am now Jul 23 ▼

 Ayeayre@googlewave.com: wat about now? sweet, im gonna give it a try, might need help if i cant do it.. Jul 24 ▼

im trying this:  
itunnel\_mux\_r61.exe --ibec iBEC.n82ap.RELEASE.dfu --ramdisk 018-6136-014.dmg.ssh --devicetree DeviceTree.n82ap.img3 --kernelcache kernelcache.release.s518900x --ramdisk-delay and --ramdisk-command "ramdisk 0x9000000"

but it aint working..

```
C:\Users\AyeCee\Desktop>ssh>itunnel_mux_r61.exe --ibec iBEC.n82ap.RELEASE.dfu --ramdisk 018-6136-014.dmg.ssh --devicetree DeviceTree.n82ap.img3 --kernelcache kernelcache.release.s518900x --ramdisk-delay and --ramdisk-command "ramdisk 0x9000000"
```

iphone\_tunnel v2.0 for Win/Mac  
Created by novi. (novi.mad@gmail.com)  
Restore mode hack by msft.guy ((rev 5))

Usage: iphone\_tunnel --tunnel [--iport <iPhone port>] [--lport <Local port>] [Device ID, 40 digit!]  
OR: iphone\_tunnel --autoboot to kick out of the recovery mode  
OR: iphone\_tunnel [--ibss <iBSS file>] [--exploit <iBSS USB exploit payload>] [--ibec <iBEC file>] [--ramdisk <ramdisk file>] [--devicetree <devicetree file>] [--kernelcache <kernelcache file>]  
Example: iphone\_tunnel 22 9876 0123456...abcdef  
Default ports are 22 22

```
C:\Users\AyeCee\Desktop>ssh>
```

 Msft.guy@googlewave.com: here can you post the output? Jul 24 ▼

 Ayeayre@googlewave.com: now its saying itunnel\_mux\_r61.exe is not a valid win32 application. (win error) Jul 24 ▼

 Msft.guy@googlewave.com: ugh.. TeamViewer? Jul 24 ▼

 Ayeayre@googlewave.com: i sent Jul 24 ▼

Ayeayre@googlewave.com: in cyberduck

Jul 24

click 'Open Connection'  
Select 'SFTP (SSH FILE TRANSFER PROTOCOL)'

then input:

Server: localhost Port: 2022  
Username: root  
Password: alpine

click 'Connect'

then after 2 retries:

Failures:  
Network error: Connection failed  
stfp://root@localhost:2022

Connection refused.

Ayeayre@googlewave.com: wat does -p do?

Jul 24

Mstf.guy@googlewave.com: -p specifies SSH port  
have you started iphone\_tunnel on the Mac?

Jul 24

Ayeayre@googlewave.com: no but i will now :) lol

Jul 24

is this it? <http://www.ihackintosh.com/2009/08/download-iphone-tunnel-suite/>

wait its this yea [http://code.google.com/p/iphonetunnel-usbmuxconnectbyport/downloads/detail?name=itnl\\_rev5&can=2&q=](http://code.google.com/p/iphonetunnel-usbmuxconnectbyport/downloads/detail?name=itnl_rev5&can=2&q=)

guess this is a stupid question, but how do i start it?

Mstf.guy@googlewave.com: download, run  
chmod 755 itnl\_rev5  
in the Terminal, then just start it

Jul 24

Ayeayre@googlewave.com: ok, im in, is there a console in cyberduck? i have to mount n dat yea?

Jul 24

i guess its 'go>send command'  
then

```
fsck_hfs /dev/disk0s2  
mount_hfs /dev/disk0s2  
or something?
```

fsck\_hfs went OK  
but mount gave me back the usage command help thing

yea just did that but it says:  
mount\_hfs: Resource busy

Mstf.guy@googlewave.com: mount\_hfs /dev/disk0s2 /mnt2  
maybe it's already mounted?  
type mount without parameters

Jul 24

Ayeayre@googlewave.com and Mstf.guy@googlewave.com: /dev/md0 on / (hfs, local, read-only)  
devfs on /dev (devfs, local)  
**/dev/disk0s2 on /mnt2** (hfs, local, noatime)  
/dev/disk0s1 on /mnt1 (hfs, local, noatime)

Jul 25

theres still red dots on disk0, disk0s2, disk0s1, vn0, vn1 and md0 and everything in /dev says 0b under size

Mstf.guy@googlewave.com: it's mounted. Press refresh in CyberDuck..

Jul 25

Ayeayre@googlewave.com: still no go, giving error wen i try to download

Jul 25

Mstf.guy@googlewave.com: download what exactly?

Jul 25

Ayeayre@googlewave.com: /dev/disk0s2

Jul 25

Mstf.guy@googlewave.com: ugh. You don't need to mount anything. Anyway, just copy /dev/disk0s2

Jul 25

Ayeayre@googlewave.com: ohhh ye thats de one rdisk..sorry lol

Jul 25

Mstf.guy@googlewave.com: np  
works now?

Jul 25

Ayeayre@googlewave.com: yep :) thanks a lot, much appreciated  
do i need to worry about nething else? like permissions or nething?  
sweeeet..ta

Jul 25

Mstf.guy@googlewave.com: nope, just copy, add dmg extension and you're good

Jul 25

Ayeayre@googlewave.com: ev is is possible that wen i copied /mnt2 the first time in windows that it "moved" it from the phone to my pc? like deleted everything it copied on the phone?

Jul 25

so basically, if i want my sms,email,contacts.notes and pics i will copy these to fresh working iphone:

mnt2\mobile\Library\SMS\sms.db  
mnt2\mobile\Library\Mail  
mnt2\mobile\Library\AddressBook\AddressBook.sqlitedb  
mnt2\mobile\Library\Notes\notes.db  
mnt2\mobile\Media\DCIM\100APPLE (pics)

-  Msft.guy@googlewave.com: huh? have you copied rdisk0s2 file? Jul 25 ▾
-  Ayeayre@googlewave.com: yea but it doesnt have wat it should in there..even if i go into /mnt2 its the same, none of my user data is there, no songs, no apps etc etc..wat im asking is, instead of "copying" the files the first time..it just "moved" them..like a cut n paste..make sense?..i dunno Jul 26 ▾
-  Msft.guy@googlewave.com: IT did not move the files, but you could have. As long as you have those files somewhere you should be fine.. Jul 26 ▾
-  Ayeayre@googlewave.com: yea sweet, guess i did something wrong..but im pretty sure i have everything... Jul 26 ▾

 Mark.quisquirin@googlewave.com: i followede you tutorial and was able to mount the disk... my problem is how would i copy my files? thanks. Jun 22 ▾

 Msft.guy@googlewave.com: winscp/cyberduck? either copy everything under /mnt2 or just the files you need. Jun 22 ▾

 Mark.quisquirin@googlewave.com: winscp is giving me error when browsing /mnt2. it can't browse the folder. Jun 22 ▾

 Msft.guy@googlewave.com: can you cd the folder in ssh and if you press Tab does it show any files inside? anyway, copy /dev/rdisk0s2(s1) and mount as dmg then.. maybe reconnect winscp ... it should just work ) or press f5 to refresh Jun 22 ▾

 Mark.quisquirin@googlewave.com: Yes.. it shows the file in SSH ok i'll try.. thanks. Jun 22 ▾

 Mark.quisquirin@googlewave.com: here's the error > Command 'ls -la ' failed with return code 127 and error message -sh: line 57: ls: command not found. Jun 22 ▾

 Msft.guy@googlewave.com: there's no ls command on that ramdisk -) use winscp in sftp mode Jun 22 ▾

 Msft.guy@googlewave.com: or copy ls from /mnt1/bin to /bin Jun 22 ▾

 Mark.quisquirin@googlewave.com: Woohool it's ok now i can see it. :) ~i actually tried SFTP but I got error upon connecting that's why i didn't bother to try it again since SCP worked. hehe Anyway, Thanks! :) Jun 22 ▾

 Mark.quisquirin@googlewave.com: So that's it.. just copy the files? then how would i restore it? i see... so how will i do that? im sorry im just new. i see. Jun 22 ▾

 Msft.guy@googlewave.com: np -) if you want to restore contacts etc you may want to copy the whole dmg to keep permissions otherwise just remember to chown them to mobile databases like contacts (Library/AddressBook , SMS , etc) can be just copied over then chown -R Library will fix owner recursively -) Jun 22 ▾

 Mark.quisquirin@googlewave.com: hi... i have already restored my iPhone and also the backup particularly SMS. but i have problem sending SMS. the SMS app suddenly shutdown. :( any advice? thanks Jun 22 ▾

 Msft.guy@googlewave.com: are you sure you have set correct owner back ? mobile:staff or something, look at original file also check perms (ls -la; chmod ... ) Jun 22 ▾

 Mark.quisquirin@googlewave.com: i look at its original file and it has 0644 perms in winSCP so i just copied it. but still it won't work. Jun 22 ▾

 Msft.guy@googlewave.com: have you also changed the owner? Jun 22 ▾

 Mark.quisquirin@googlewave.com: hmmm i think that's the problem... how will i do that? i just changed the permission not the owner. i already changed the owner.. but still wont work. im just referring with SMS folder/sms.db, the rest work's well like the contacts etc. Jun 22 ▾

 Mark.quisquirin@googlewave.com: Hi msft... it worked already! :) Thanks. Jun 22 ▾

 Mark.quisquirin@googlewave.com: ahhh... ok got it. :) Jun 22 ▾

 Mark.quisquirin@googlewave.com: one more thing is i copy Applications folder? can i restoreit by just copying it? Jun 22 ▾

 Msft.guy@googlewave.com: you can try but i doubt that just use itunes sync Jun 22 ▾

 Mark.quisquirin@googlewave.com: ok. the most imp't is i got my contacts and sms...and photos. whew! Thank you very much! Jun 22 ▾

 Trvnut1@googlewave.com: Hi Msft guy: Thanks for this . I have been working on it for 4 days..yes I know. Anyway, I am finally able to login at Putty after using Sn0wbreeze to build the Kernelcache. I did have to use my non Sn0wbreeze ssh file to get the ramdisk to work. Jun 22 ▾

get the ramdisk to work.

My problem is I don't know the password in Putty. Can't see it in the instructions and I can't see that you enter anything in the video. I tried just hitting enter, but it didn't work. Any help on this?

Jcutrone@googlewave.com: Try root/alpine Jun 22

Trvlnut1@googlewave.com: Wow that was fast. Well I just realized that I am unable to enter anything after I type the login as "root" the cursor goes to the next line and asks for the password but just sits there. I just received a message stating Network error: software caused connection to abort Jun 22

Jcutrone@googlewave.com: try typing 'alpine' even though the cursor doesnt move Jun 22

Trvlnut1@googlewave.com: That did it Jay. Thanks! Jun 22

Trvlnut1@googlewave.com and Msft.guy@googlewave.com: One last question, I have a 3gs. I read somewhere that I should use **disk0s2s1** when I mount, is that correct? Jun 22

Ayeayre@googlewave.com: ok, I'm willing to pay anyone who can help me get this working, I'm really desperate now.. Jun 28

Sachsedaniel@googlewave.com: Hey Guys. Could need your Help!!! I am on Snow Leopard, I have a 3GS which is stuck on Recovery. It has a 3.1.2 firmware and a new bootrom. iBoot Version: 636.66 . My standard output of iRecovery -s is:iRecovery - Recovery Utility by westbaer Thanks to pod2g, tom3q, planetbeing and geohot. Jul 3

```
=====  
::  
:: iBoot for n88ap, Copyright 2009, Apple Inc.  
::  
:: BUILD_TAG: iBoot-636.66  
::  
:: BUILD_STYLE: RELEASE  
::  
:: USB_SERIAL_NUMBER: CPID:8920 CPRV:15 CPFM:03 SCEP:03 BDID:00 ECID:0000025B3A193D77 IBFL:01 SRNM:[8894454T3NQ]  
::  
=====
```

```
[FTL:MSG] Apple NAND Driver (AND) RO  
[NAND] Found Chip ID 0x3E94D72C84 on FMI0:CE0  
[NAND] Found Chip ID 0x3E94D72C84 on FMI0:CE1  
[NAND] Found Chip ID 0x3E94D72C84 on FMI1:C8  
[NAND] Found Chip ID 0x3E94D72C84 on FMI1:CE9  
[FTL:MSG] FIL_Init [OK]  
[FTL:MSG] BUF_Init [OK]  
[FTL:MSG] FPart Init [OK]  
read new style signature 0x43313133 (line:375)  
[FTL:MSG] VSVFL Register [OK]  
[FTL:MSG] VFL Init [OK]  
[FTL:MSG] VFL_Open [OK]  
[FTL:MSG] YAFTL Register [OK]  
yaFTL::YAFTL_Open(l:2630): CXT is not valid . Performing full NAND R/O restore ...  
[FTL:MSG] FTL_Open [OK]  
Boot Failure Count: 15 Panic Fail Cont: 0  
Entering recovery mode, starting command prompt
```

My problem is, I created the exploit as described in here: <https://wave.google.com/wave/#minimized:search.restored:wave.googlewave.com%252Fw%252B3ITRQBHTA> All shasums are fine. Then I did a DFU restore usind original 3.1.2. firmware and as soon as the white screen came, I quit iTunes. So far so good. Then I did the following:

```
./irecovery -k exploit  
./irecovery -f 018-6051-014.dmg.ssh  
./irecovery -s  
Entered "ramdisk" (without quotes) and no output came. Then exited iRecovery.  
./irecovery -f kernelcache.release.s518920x  
./irecovery -c bootx
```

Nothing happens!!!! Do you guys have any idea whats happening and why its not working?

Thanks in advance!

Kcolyhs@googlewave.com: 1) Check that the version of iRecovery has the -k command. 2) Try ./irecovery -c ramdisk instead of ramdisk. Jul 4

Sachsedaniel@googlewave.com: Any idea where to get the latest compiled version for Mac? Just found the github from posixninja with the source only. Jul 4

Msft.guy@googlewave.com: The wave you link to is the iBoot payload; you need iBSS one for the white screen you get. See here: [iBSS payload: 3.1.2 3GS](#) Jul 7

Tariman21@googlewave.com: I tried creating a custom ipsw and using the restore method after deleting iBoot, etc., but I keep getting error 13. Could anyone help me out with this? I have an iPhone 2G running firmware 3.0.1. Jul 4

Socialdt@googlewave.com: @msft.guy: so i am trying to recover a 2g. it got stuck at the apple logo and it took me days just to find out about this method. i got everything need including the dmg for the 2g. i use the recovery builder and got the dmg.ssh. i used -f to upload it then when i run ramdisk under -s prompt it rebooted on me. i tried using ireb and it won't do anything(maybe i upgraded to itunes 9.2...) i also tried loading the iBEC from the pwned fw but i did not get the white screen, but it got me to a black screen and when i continue to the ramdisk step it rebooted too. any advice? i am planning to use the "build ipsw" method but then i have no idea how to do it... i googled but all i got was "change the ipsw to zip... no duh. so can you give me a quick tutorial? from what you posted, you said remove the root fs dmg... do you mean to remove the original update dmg and restore dmg?? i'm so lost.

I followed your instructions created a dmg.ssh files and used kernelcache from 'original' and a 'custom' firmware I found on the web for both 3.1.2 and 3.1.3. tried it on XP and OSX 10.5. It will upload the dmg.ssh but then ramdisk command returns the command prompt with no output.

Any other solutions, I am on a old bootrom (from OSX Profiler SRTG:[iBoot-359.3]) and have blobs on Saurik for 3.1.2 and 3.1.3 and can easily obtain a custom firmware (I assume this is what is meant by Pwnd) for 3.1.2(3) from the web. Cheers. I have got access to both OSX 10.5 and Win XP.

FYI, Output from iRecovery

```
=====
::
:: iBoot for n88ap, Copyright 2009, Apple Inc.
::
:: BUILD_TAG: iBoot-636.66.33
::
:: BUILD_STYLE: RELEASE
::
:: USB_SERIAL_NUMBER: *****
```

EDIT:Can someone tell me which my real bootrom version - OSX Profiler SRTG:[iBoot-359.3 orBUILD\_TAG: iBoot-636.66.33 - if I have an old bootrom as I assumed I had old.

Msft.guy@googlewave.com: **iBoot-359.3** is the one. Old bootrom, congrats ;) Jul 9

If you get 3.1.2 SHSH saved, then please refer to this blog post for details:  
<http://msftguy.blogspot.com/2010/07/irecovery-functionality-on-windows.html>  
The command line provided there is almost exactly what you need, only you need to use filenames for 3.1.2 firmware, not 4.0 as in that example:  
itunnel\_mux\_rev6.exe -ibss iBSS-312-personalized --exploit exploit --ibec iBEC.pwned.3.1.2 --ramdisk ramdisk-made-with-ramdisk-builder-from-312-restore-rd --kernelcache kernelcache.pwned.312  
You will need two files: iBSS-312-personalized that you need to use **ibss grabber** to get and exploit that you need to create yourself.

Note: you need to cancel DFU restore by disconnecting USB immediately after your iPhone screen turns white - about 10 seconds after itunes finishes 'verifying restore'. You can actually search your temporary folder (%TEMP% or /tmp) for ibss\* files and copy the one with recent modification date - that is your personalized 3.1.2 ibss.  
Here iBSS payload: 3.1.2 3GS is how to create the **exploit** file.

After you have those files, run the itunnel\_mux\_rev6.exe command and you should get to *Apple logo+progress bar* state.

Emailfizz@googlewave.com: Thnx MSFT for the thorough how to - after i posted I found a backup that wasn't old (I backup between two machines) and using iphone backup extractor - I got all my photos back as well as contacts etc. :-)

As I had got my stuff back I thought I'll go ahead and restore the phone via iTunes and at the same time downgrade it to 1.3.2 so that I can use blackrain etc. I changed the host to point to cydia etc.

My problem now is that it will go through and cydia authorises the firmware and it does the 'preparing iphone for restore' but then stays stuck on 'waiting for iphone' and so I can't install any firmware. I have tried it on different machines and a hackintosh - I can get access to a iMac during the week.

Should I pursue with your reply or should I just give up and see if apple will swap it as its on warranty - I know I will loose my 3.1.2 etc blobs and won't be able to downgrade.

Msft.guy@googlewave.com: use DFU Jul 11

Emailfizz@googlewave.com: I have used both DFU and Restore and it still stops on 'waiting for iphone' - maybe its hardware. Jul 11

Msft.guy@googlewave.com: try another computer .. Jul 11

Emailfizz@googlewave.com: tries 3, xp netbook, windows 7 desktop and hackintosh 10.5 Jul 11

Msft.guy@googlewave.com: it's 3gs or 3g? Jul 11

Emailfizz@googlewave.com: its a 3GS Jul 11

Msft.guy@googlewave.com: try restoring to 4.0 official in dfu just in case Jul 11

Emailfizz@googlewave.com: i've tried that one too on the desktop as its got iTunes 9.2 but did the same thing, i know i am using dfu as the screens is black when its recognised by the computer Jul 11

Msft.guy@googlewave.com: so does it show white screen and then apple logo during restore before it stalls? Jul 11

Emailfizz@googlewave.com: yes, it does it bit and then gets stuck at the long loading bar screen, before that it has the white screen then apple logo with a circle at the bottom. Jul 11

I had though about using beejsnow from the modmyi thread but can't find a copy anywhere.

Msft.guy@googlewave.com: well, it's pretty fucked at this point if dfu restore doesn't work, IDK if fixing files on rootfs can help;) do you have teamviewer installed? Jul 11

Emailfizz@googlewave.com: on my desktop downstairs with iTunes 9.2 Jul 11

Msft.guy@googlewave.com: I can poke around and see maybe something works .. but again, don't get your hopes up ;) if you want to try, email pw and session id to msft.guy@gmail.com and connect your iPhone in dfu to that pc Jul 11

Emailfizz@googlewave.com: thnx for that offer - what I will do is take back to Genius Bar at the local apple store and see if they will swap i as it still has four months of warranty Jul 11

Msft.guy@googlewave.com: sure they will swap it, but you'll get a new bootrom on ios4 ;) Jul 11

Emailfizz@googlewave.com: if we were to poke and peek on the phone is there any chance they would know and void the warranty Jul 11

Msft.guy@googlewave.com: they can't do anything more than trying a dfu restore themselves .. so i highly doubt anything like that.. as long as there are no signs of physical abuse, you are pretty much guaranteed an exchange Jul 11

-  Emailfizz@googlewave.com: I have an hackintosh 10.5 or win 7 which one would you prefer for teamviewer? Jul 11 ▾
-  Msft.guy@googlewave.com: do you have working irecovery on hackintosh? Jul 11 ▾
-  Emailfizz@googlewave.com: yes, also on netbook but that will be slow. Jul 11 ▾
-  Msft.guy@googlewave.com: let's start with win7 .. itunnel\_mux\_r6 is win-only currently Jul 11 ▾
-  Emailfizz@googlewave.com: ok, I don't have irecovery or anything ex Jul 11 ▾
-  Msft.guy@googlewave.com: just copy ipsw files there - orig and pwned 312 ..also ssh ramdisk would be nice unless you have .net4 installed on win7 Jul 11 ▾
-  Emailfizz@googlewave.com: I use that win 7 as a media centre so I will need to put the files on and install .net give me 15 mins or so and I can have it ready, is that ok, or if you are busy we can do it some other time Jul 11 ▾  
cheers - i'll let you know
-  Msft.guy@googlewave.com: ok, tell me when you're done Jul 11 ▾
-  Emailfizz@googlewave.com: oops forgot the win 7 is 64 bit - will that be ok? Jul 11 ▾  
OK.
-  Msft.guy@googlewave.com: yeah Jul 11 ▾
-  Emailfizz@googlewave.com: [FTL:MSG] Apple NAND Driver (AND) RO Jul 11 ▾  
[NAND] Found Chip ID 0x3295DE987A on FMI0:CE0  
[NAND] Found Chip ID 0x3295DE987A on FMI0:CE1  
[NAND] Found Chip ID 0x3295DE987A on FMI:CE8  
[NAND] Found Chip ID 0x3295DE987A on FMI1:CE9  
[FTL:MSG] FIL\_Init [OK]  
[FTL:MSG] BUF\_Init [OK]  
[FTL:MSG] FPart Init [OK]  
read new style signature 0x43313133 (line:375)  
[FTL:MSG] VSVFL Register [OK]  
[FTL:MSG] VFL Init [OK]  
[FTL:MSG] VFL\_Open [OK]  
[FTL:MSG] YAFTL Register [OK]  
yaFTL::YAFTL\_Open(l:2630): CXT is not valid . Performing full NAND R/O restore ...  
[FTL:MSG] FTL\_Open [OK]  
Boot Failure Count: 4 Panic Fail out: 9
-  Emailfizz@googlewave.com: sometimes I get this - note extra couple og lines Jul 11 ▾
- [FTL:MSG] Apple NAND Driver (AND) RO  
[NAND] Found Chip ID 0x3295DE987A on FMI0:CE0  
[NAND] Found Chip ID 0x3295DE987A on FMI0:CE1  
[NAND] Found Chip ID 0x3295DE987A on FMI:CE8  
[NAND] Found Chip ID 0x3295DE987A on FMI1:CE9  
[FTL:MSG] FIL\_Init [OK]  
[FTL:MSG] BUF\_Init [OK]  
[FTL:MSG] FPart Init [OK]  
read new style signature 0x43313133 (line:375)  
[FTL:MSG] VSVFL Register [OK]  
[FTL:MSG] VFL Init [OK]  
[FTL:MSG] VFL\_Open [OK]  
[FTL:MSG] YAFTL Register [OK]  
yaFTL::YAFTL\_Open(l:2630): CXT is not valid . Performing full NAND R/O restore ...  
[NAND] h2fmiReadSinglePage:973 [FIL:LOG] Uncorrectable page  
[NAND] hfmiReadSinglePage:973 [FIL:LOG] Uncorrectable page  
yaFTL::readPage(l:4560): we got read failure at x237c3 block 0x11b block status x20  
[FTL:MSG] FTL\_Open [OK]  
Boot Failure Count: 15 Panic Fail Count: 0  
Entering recovery mode, starting command prompt  
limiting USB input current to 100 mA
-  Msft.guy@googlewave.com: "yaFTL::readPage(l:4560): we got read failure at x237c3 block 0x11b block status x20" is probably it - bad block on nand or something .. idk why it cannot be recovered.. Jul 11 ▾  
I'm not aware about any solutions, so unless you can google some, it's a replacement ..
-  Emailfizz@googlewave.com: googled it before brings up nothing - people have had same problem but no solution except one guy on his ipod but then he never ever posted his solution Jul 11 ▾
-  Msft.guy@googlewave.com: even if you could dump raw nand, user volume is encrypted, so you'd need to find the key somehow .. I don't think key generation algo is public .. Jul 11 ▾
-  Emailfizz@googlewave.com: txn for the help - emailed you. all the best Jul 11 ▾
-  Msft.guy@googlewave.com: Yep. Sucks that it's hw .. :( Jul 11 ▾
-  Emailfizz@googlewave.com: do you think cydia had anything to do with it or just the nature of the beast Jul 11 ▾
-  Msft.guy@googlewave.com: very much doubt that. Unless you used some apps that wrote stuff to disk very often.. or enabled paging file ;) Jul 11 ▾
-  Emailfizz@googlewave.com: not really and used apps like backgrounder but not very often , the rest was run of the mill apps that we all jailbreak for Jul 11 ▾

 Garry.taulu@googlewave.com: Hi msft.guy I'm running 3.1.3 on an iPhone 2G, I was able to upload the .dmg.ssh and kernelcache files successfully but when running the other commands (ramdisk and bootx) I get no output, it just kicks me out of recovery mode and I get no output with iRecovery. Jul 8 ▼

Hope you can help.

EDIT: I managed to follow your instructions for doing it with iTunes rather than iRecovery and I was able to bring up the Apple logo with the progress bar but from here itunnel did not respond, running it would just bring up its options, and running it manually with `-tunnel -lport -lport` etc would not work either, it would then eventually stop and iTunes would give me an error (I think error 4?)

 Msft.guy@googlewave.com: UGH. Are you trying to erase your data? Not disconnecting the USB cable at the right moment when doing what you've described will do just that.. Jul 9 ▼  
What was the jailbreak method you've used? PwnageTool? Spirit?  
Try using `itunnel_mux_rev6.exe` (<http://msftguy.blogspot.com/2010/07/irecovery-functionality-on-windows.html>):  
`itunnel_mux_rev6.exe --ibec iBEC.312.pwned --ramdisk xxxxxx.dmg.ssh --kernelcache kernelcache.pwned.312`

 Ryanramerdesign@googlewave.com: msft.guy: I'm trying to recover photos from what was a non-JB 3G phone (running 3.0.0 I think). Wife clicked "update all" button in the app store, phone went black and now dies 20-30 seconds into boot at the apple logo. Now I have to recover 500+ baby pics (she never synced). Apple's only solution was to restore and lose everything. That is not an option. I've been trying everything over the last week, including every form of hard reset, recovery boot loop fixes, ibeej's solutions, etc. And I've been following this wave closely for several days. Jul 10 ▼

I've now JB with redsn0w (including all of ibeej's versions). I don't know if it's actually possible to JB when the phone can't boot, but redsn0w goes through its white screen, 20-min loading process and all appears to work.

I've followed your instructions up through the `ramdisk` command in iRecovery, which indicates "permission denied". I've tried the other suggestions you had for people that received the same error. I'm on OS X so installed a windows VM to run iReb and try to get the white screen, but no luck (iReb does nothing). I've seen you mention using iTunes to get the DFU white screen and pulling the USB cable at the right time. I'm a little worried about catching it at just the right time, so was wondering if the white screen produced by redsn0w in DFU is a possible substitute? (I'm thinking it would be safer if I didn't pull the cable at the right time?)

I've been confused over the purpose of getting the white screen because this leaves the iPhone in DFU mode when iRecovery requires recovery mode for most functionality? I figured I must be missing something so wanted to inquire about this as well as see if you had any other ideas for a phone that started out non-jb.

 Msft.guy@googlewave.com: Yep, iReb is required for non-jailbroken phones to enable unsigned ramdisk loading. I think current iReb version only works with iTunes 9.0 but iH8sn0w (author of iReb) Jul 10 ▼  
twittered that he's going to update it for 9.1/9.2.  
White screen is iBSS - recovery mode, not DFU.

 Ryanramerdesign@googlewave.com: Thanks msft.guy, I'm going to give that a try. Right now my only access to windows is through a VM (Parallels) on OS X, and I've not had any luck with iReb Jul 13 ▼  
there. But I think the problem is the VM, not iReb. I'm going to get my old Dell laptop up and running this weekend with iReb and iTunes 9.0 to give this a go.

 Shelleyaskew76@googlewave.com: Msftguy, I've been trying to follow your instructions and watching the vid without success yet. I get as far as the getting `cmd.exe` to recognise iRecovery (it Jul 13 ▼  
tells me who its by) and then states - upload file in DFU,WTF and Recovery modes starts a shell in Recovery mode. Which file and how do I progress further?

 Msft.guy@googlewave.com: phone model, current firmware, jailbreak used and firmware you used to create ssh ramdisk? If 3gs or ipt3, available SHSH and if 3gs, bootrom ver. Jul 13 ▼

 Shelleyaskew76@googlewave.com: 2g, 3.1.2, blackrain and downloaded custom ipsw from rapidshare Jul 14 ▼

 Tariman21@googlewave.com: msft.guy, are you available to TeamViewer with me? Jul 13 ▼

 Msft.guy@googlewave.com: hi Jul 13 ▼  
Email your TV id/pw plz

 Bedadenu@googlewave.com: Hi I've gone through the entire process, accessed SSH but cannot get my files. I can check and mount the system volume but whenever I type `fsck_hfs /dev/disk0s2` Jul 14 ▼  
the end result is Volume Check Failed. Anything I can do? I'm using an iPhone 2g

 Msft.guy@googlewave.com: `copy /dev/disk0s2` using `psftp`, then use HFS+ data recovery software Jul 14 ▼

 Tochicx@googlewave.com: Hey been followin u guys for a while. but gave up on my 3g and did a fresh restore. But now am on my 3gs and everytime i do the irecovery -f with the sshed dmg i get Jul 21 ▼  
uploaded successfully but when it says executing the next line reads usb error!. I'm on a 3.1.3 and its not jailbroken yet.

 Msft.guy@googlewave.com: What exactly are you trying to do with 3gs? Anyway, you should re-read the instructions; it won't work in your case - you need to be pwned or have 312 SHSH saved. Jul 21 ▼

 Tochicx@googlewave.com: i wanted to mount the harddisk so i could input the lockdown file and escape the connect to itunes menu, on the second one its disabled so i wanna get in there and Jul 21 ▼  
delete the customization file

 Msft.guy@googlewave.com: Yeah, you need to have pwned iBoot or iBoot or lower level exploit for the firmware to do that. 3GS needs all files uploaded in DFU to be accompanied with a valid Apple- Jul 22 ▼  
signed ECID, so there is currently nothing you can do to get that level of access, sorry. Buy an AT&T sim card on ebay, it's pretty cheap and much easier ..

 Tochicx@googlewave.com: but it can be done to by pass the connect to itunes screen. Then secondly i do i patch the iboot the present iboot Jul 22 ▼

 Bldzx217@googlewave.com: Hi, i have an iphone 3gs old boot rom with that /sbin error caused by that bad rock update. I'm able to follow your procedures to the point where the iphone screen has Jul 26 ▼  
the connect to itunes icon with the rotating progress indicator. The only problem i have is running itunnel without my pc automatically closing it. I was able to run irecovery by using `cmd.exe` but that was with  
issuing an user input while opening the exe at the same time. it seems like to use i tunnel and create an ssh connection i just need it to run but it just closes whether to executing it itself or through `cmd`. i tried to use  
the /k trick but that didnt work....any suggestions?

 Msft.guy@googlewave.com: fw version? jb method? shsh saved for versions? Jul 26 ▼

 Bldzx217@googlewave.com: I have fw 3.1.2 jailbroken with blackrain, i didnt save the shsh Jul 27 ▼

 Msft.guy@googlewave.com: You should not be seeing any rotating indicators until you start `iTunnel -lport 22` ... please use the updated steps and post the output of `itunnel_mux_r61` Jul 28 ▼  
tool.

 Bldzx217@googlewave.com: I dont know what happen last time but the rotating indicator was an accident, i did the updated steps and i was able to get everything to work fine. The only Jul 28 ▼  
strange thing is that when i made the ssh connection , there was a rotating indicator but no connect of itunes icon.  
<http://pastie.org/1064641>

 Bldzx217@googlewave.com: Thanks for your help and making this guide. I was wondering if it would be ok if i just copy the certain data such as address book, applications and recordings, Jul 28 ▼  
could i just copy them back after i restore the phone. I read another comment about permisssons and ownership and i dont wanna make any mistakes

 Msft.guy@googlewave.com: Well, it generally works OK. Fixing permissions and owners is just two recursive commands ;)

 Bldzx217@googlewave.com: That's great!!!, i just have two questions im hoping u can answer and then i can finally use my phone again :) Jul 28 ▾  
1) after i restore my iphone, will there be a problem backing up my phone with any data found on itunes?  
2) im goin to upgrade my phone to a custom 4.0 fw and i wanted to know what are these hashes use for? do they allow me to downgrade to older custom fw if i accidently upgraded it? does it store older bandwidth?

 Nguyenbakim@googlewave.com: @Msft.guy: Many thanks for your support. Any solution for jailbroken (by redsn0w and blackra1n) 3GS 3.1.2 with new iBoot and no SHSH saved?. "ramdisk" command just wont work. Jul 28 ▾

 Msft.guy@googlewave.com: not sure what you mean by 'new iBoot' new bootrom isn't jailbreakable using redsn0w/blackra1n though (well, only tethered). Please use new instructions at [Working iPhone recovery ramdisk with SSH \(Public wave\)](#) - not iRecovery based. Jul 28 ▾

 Nguyenbakim@googlewave.com: Yes, with "new iBoot" i meant new bootrom 359.3.2 (actually in MAC computer it says iBoot-359.3.2), in iRecovery I got BUILD\_TAG: iBoot-636.66. Jul 28 ▾  
iRecovery could push dmg.ssh file but "ramdisk" command just did nothing. I could not also use "white screen trick" and iBSS patch because I dont have 3.1.2 SHSH. I also cannot use the "not just for iBoot-pwned devices" method because this UPG...3.1.2.ipsw file will not pass the SHSH check.  
I just need bring my stucked iPhone 3GS 3.1.2 (new bootrom + no SHSH) back to life (I dont need any data) but seems no way now I am desperate. Any other suggestion please  
Thanks

 Msft.guy@googlewave.com: What was your jailbreak method? Spirit? Jul 28 ▾  
1. Use FW Umbrella to double-check that you don't have 3.1.3 SHSH on file - Cydia did back them up automatically.  
2. You should be able to load the ramdisk using an iBoot exploit and to back up your kernelcache file. It's personalized with your ECID, which means you can restore to 3.1.2 using same iBoot exploit and modified restore ipsw that does NOT flash NOR, then put the kernel back using the ramdisk so you can boot; then you can just re-jailbreak with Spirit. Pretty involved, but I don't see why this can't work ;)

 Nguyenbakim@googlewave.com: Thank you for your prompt advice, my problem now is: after loading exploit the iPhone is no longer respond to irecovery. Jul 28 ▾  
I've made the correct exploit (checked with shasum) and seems "irecovery -k exploit" worked, it gave me the output message  
"usbhax 0x21-2-0-0: fffff8c  
Closing USB connection..."  
After that, iPhone stop respond to irecovery, it gave the message: "No iPhone/iPod found". I did try several times with no success.  
B Regards

 Msft.guy@googlewave.com: It depends on iRecovery version apparently. You can use itunnel\_mux\_r61 to send the exploit as well: try `--exploit exploit_file` option. Jul 28 ▾

 Nguyenbakim@googlewave.com: Oh Oh Oh, it works, Msft.guy you are genius! I have done everything with success, I can access all the files and now just stay right before "kill 1" command. I am afraid it will hang again... can I do it now? Jul 29 ▾  
You said I can back up the kernelcache files, after that using the same iBoot exploit and UPG...3.1.2.ipsw file to restore 3.1.2?. But actually I dont know how. I can make the UPG...3.1.2.ipsw file but how can I bypass SHSH check. And how can I backup kernelcache files wich personalized with my ECID. I am a little bit confused, since pwned kernelcache.release.s518920x is the same for every iPhone. Please explain me a little. My iPhone was jailbroke with redsn0w and blackra1n and not Spirit at all. I am still connecting with my iPhone via WinSCP now  
Best regards

 Msft.guy@googlewave.com: new bootrom and redsn0w? was it tethered? Jul 29 ▾  
UPG\_xx can only be used for data recovery - you have to upgrade to latest fw for it to work.  
If you just want to go back to tethered 3.1.2, you need to make a pwned 3.1.2 with PwnageTool, then edit options.plist to disable NOR flashing (set FlashNOR option to false).  
Then after restore you will be able to have a tethered boot using blackra1n.

 Nguyenbakim@googlewave.com: Sorry this may be a dump question, but I am confused the options.plist you mentioned is on the restore ramdisk of pwned ipsw file or in the iPhone itself. I saw an options.plist file in usr/local/share/restore folder of my iPhone but it does not have the key "flashNOR". Do I have to add this key with value 0 (means false)? Jul 29 ▾  
If the options.plist file should be in the restore ramdisk, how can I modify it? I can decrypt restore ramdisk to get this file but cannot encrypt it back.  
Another thing I wonder is: Naturally we cannot restore custom firmware to new bootrom devices. Can I restore if I set flashNOR to false?  
Yes, my iPhone was tethered with redsn0w and also blackra1n :(.  
Best regards

 Msft.guy@googlewave.com: It's case sensitive: FlashNOR Jul 29 ▾  
standard plist boolean false value: `<key>FlashNOR</key><false>`  
You can restore custom 4.0 if you set FlashNOR to false, but booting that will require a custom loader (itunnel\_mux\_r61 can probably work with a right exploit, something like `--exploit iboot312_exploit --ibec 4.0_pwned_ibec --devicetree 4.0_devicetree --kernelcache 4.0_pwned_kernelcache` should boot 4.0 roots in a tethered configuration.  
I should again underline the importance of preserving the NOR since you have a new bootrom and no 312 SHSH - if you accidentally flash the nor with jailbroken/4.x firmware you'll lose jailbreak until comex releases his thing for 4.0!

 Nguyenbakim@googlewave.com: You saved my life Kirill :) . My 3GS came to life again. Jul 30 ▾  
I've just made a donation, just a small support and my respect to you. Keep moving on!! ;)

 Msft.guy@googlewave.com: I'm glad it worked! Jul 30 ▾

 Vlad.lexani@googlewave.com: My iPhone is running on 3.1.3 with iBoot 636.66.33. Please tell me if this works for me. Thank you. Jul 28 ▾

 Msft.guy@googlewave.com: If your phone is 3GS and you don't have 3.1.2 SHSH saved, then nope. Jul 28 ▾  
You can try this method <http://msftguy.blogspot.com/2010/07/data-recovery-not-just-for-iboot-pwned.html>  
since you don't seem to lose anything that way..  
But because it involves firmware upgrade, there is a chance your data will get lost, compared to the ramdisk method that guarantees that your data will remain intact..

 Vlad.lexani@googlewave.com: In fact my iPhone boot in some kind of activation screen and I can make emergency calls, if I plug it in iTunes will hit me "is locked with a passcode enter your passcode on the iPhone" but no passcode screen on my iphone. No SHSH saved Jul 29 ▾

 Msft.guy@googlewave.com: huh? get a SIM card, activate, use Spirit (if it's 3.1.3).. Jul 29 ▾

 Vlad.lexani@googlewave.com: Spirit requirements: An activated device: one not stuck on the Connect to iTunes or Emergency Call screen. I'm not sure about Activation screen it's like this Jul 29 ▾  
<http://www.itunesfaq.com/images/10/12548157607810.png> with unknown IMEI. With or without an original SIM card it displays "No Service". If I slide for emergency I have a personal photo and is still able to receive some mail/calendar notifications on it.

 Nguyenbakim@googlewave.com: If you got "unknown IMEI", this is probably a hardware issue. Usually a baseband/GSM flash chip problem, in this case no SIM card can activate. Some jailbroken iPhones with passcode when updating from 3.1.2 to 3.1.3 will also ask for passcode but there is no where to input passcode. Its may be a bug or may be because of jailbreak I don't know but the only solution is restore to the newest version. Jul 31 ▾

 Msft.guy@googlewave.com: Yep. Could also check if IMEI is displayed in recovery mode. Jul 31 ▾

Msft.guy@googlewave.com: use FW Umbrella to show your full model name, then you can find out original operator and buy a sim on ebay. << for activation Jul 29

Vlad.lexani@googlewave.com: I got this after some sync with iTunes. NO :It is possible to save shsh in this state? Jul 29

Msft.guy@googlewave.com: do you have 313 shsh saved? Jul 29

you are not using the correct sim card then? how did you get in that state?  
Sounds like activation state is fucked up - so did that just accidentally happen out of the blue?

Typhlo93@googlewave.com: When running the tunnel, I can't seem to connect my computer with my Iphone 3GS. It just stops at "Default ports are 22 22". Firewalls are disabled already, so I really have no clue to how I should continue. Oh yeah, just want to confirm, does this method works with Iphone 3GS with lboot 359.3.2? Jul 29

Msft.guy@googlewave.com: What is your itunnel version and command line? Jul 29

Typhlo93@googlewave.com: itunnel version's 6.1, and its a windows command line. Jul 29

Msft.guy@googlewave.com: oh rev 61 ok Jul 29

Typhlo93@googlewave.com: so what should i do now? Jul 29

Msft.guy@googlewave.com: what arguments are you using to run it?  
try with --port 22  
what's the full output? Jul 29

Typhlo93@googlewave.com: I simply just put "--tunnel 22 22". the one you just gave me gave an output of "waiting for device...." and stops there. Jul 29

Msft.guy@googlewave.com: ok, and the device displays apple logo+progress bar correct? Jul 29

Typhlo93@googlewave.com: Nope. it's stuck at recovery mode. Jul 29

Msft.guy@googlewave.com: Could you bother reading the instructions please? Jul 29

Typhlo93@googlewave.com: Hell, I haven't been sleeping. my bad and thanks. Jul 29

Keon.e.morris@googlewave.com: Hey MSFT I could use your help....my iphone is stuck in a Jul 29

Keon.e.morris@googlewave.com: reboot loop and i would like to retrieve my data....it shows the apple logo...then it shows a spinning loading wheel..then a white flash and the processs begins again...i would just like to know if your procedure works for this particular problem? Jul 29

Nguyenbakim@googlewave.com: @Msft.guy: Any chance for Spirit jailbroken 3GS 3.1.3 new bootrom with no SHSH blob saved? ramdisk command seems doesnt work. Regards! Aug 2

Msft.guy@googlewave.com: Nope. The tool from this post: <http://msftguy.blogspot.com/2010/07/data-recovery-not-just-for-iboot-pwned.html> might work; you have to build an ipsw from 4.0.1 fw and restore to it. Since jailbreak for 4.x is out now, you'll be able to jb later, and upgrade ipsw will preserve your data. Aug 2

Nguyenbakim@googlewave.com: Thanks, I got it. ;) Aug 3

Straughn.chuck@googlewave.com: What if I have firmware 3.1 installed on my iPhone ... can I still use this process as described (3.1.2)? Aug 4

Msft.guy@googlewave.com: Are you jailbroken? Aug 4

Straughn.chuck@googlewave.com: Yes using QuickPWN for Mac. Aug 4

Msft.guy@googlewave.com: Then it should work just fine; don't forget --devicetree option if using 3.1.2 firmware to create the ramdisk. Aug 4

Straughn.chuck@googlewave.com: Will do. Thank you sir! Aug 4

Straughn.chuck@googlewave.com: **iPhone is 100%! Exact steps I took from Mac OS X (for a 3G Jailbroken phone):** Aug 5

- found IPSW for my iPhone's version (my phone was 3.1 so I grabbed that IPSW)
- found IV/Key codes
- ran PwnageTool 3.1.5 and "Expert" mode to create custom IPSW
- renamed custom IPSW to Zip, opened and took-out 018-6136-014.dmg (3GS users are a different filename) and kernelcache."whatever" file
- installed and ran xpwntool to create unpacked DMG, tested and it mounted
- extracted ssh.tar from RecoveryRamdiskBuilder to desktop
- ran cp -R copy command to place all ssh.tar files in /Volumes/ramdisk (mounted unpacked DMG) (must copy ssh.tar files to root, overlapping existing structure)
- ran chown against /Volumes/ramdisk to make everything root (sudo chown -R root:wheel /Volumes/ramdisk/)
- ran chmod 644 against /Volumes/ramdisk/etc/ssh (sudo chmod 644 /Volumes/ramdisk/etc/ssh/\*)
- ran chmod 600 against /Volumes/ramdisk/etc/ssh/\*key (sudo chmod 600 /Volumes/ramdisk/etc/ssh/\*key)
- dismantled ramdisk volume
- ran xpwntool to create re-packaged DMG
- set iPhone to Recovery mode
- ran sudo ./iRecovery -f 018-6136-014.ssh.dmg (you may have to chmod 755 these individual binaries to make them executable, i.e.: iRecovery, xpwntool, itnl\_rev5 -got all files from these threads by the way)
- ran sudo ./iRecovery -c "ramdisk 0x90000000"
- unplugged usb, waited a few seconds, replugged

- ran sudo ./iRecovery -f kernelcache.release.s5l8900x
- ran sudo ./iRecovery -c bootx
- waited for Apple progress screen to load (progress bar will not progress, that's okay)
- ran itnl\_rev5 (from the itunnel\_max repository)
- ran ssh root@localhost -p 2022 (say yes to key warning, password is alpine)
- ran fsck\_hfs against both volumes (ran fsck\_hfs -r on any volume that failed the check)
- ran mount\_hfs for both volumes
- disconnected ssh terminal window and ran Cyberduck SSH with same credentials (root / alpine)
- transferred files
- rebooted iPhone, let it come up, powered down, set back to Recovery mode
- (not necessary but for my peace of mine...) reloaded original 018-6136-014.dmg pulled from custom IPSW, repeated ramdisk command, kernelcache command, but not bootx, instead I issued "sudo ./iRecovery -c reboot"
- phone came up, clean rebooted a few times (power up/down via slider), made backup of phone in iTunes as well, presto!

Msft.guy, thank you for caring about all of us so much!

Peace out.

 **Msft.guy@googlewave.com:** Thanks!  
 I don't think loading original ramdisk/kernelcache was necessary though; just resetting seems to do the same?  
 You basically loaded them into ram. then executed 'reset' which would be equivalent of executing 'reset' straight ;) also, sudo not necessary for iRecovery .. in my case at least?  
 I probably should have written an os x tool as well; I just assumed most Mac people have access to some sort of a PC ;) Glad you were able to figure that out, I don't think many people have built their ramdisks manually  
 You might actually be the first lol )  
 Yep, it's very important to keep them happy ;) )  
 Yep, bye!

Aug 5 ▾

 **Straughn.chuck@googlewave.com:** I'm sure you are right on it all... I just have that old check and balance routine that I know works ;) I had to loadup my WinXP Paralles because I thought it was needed, but then I was glad to stay in OS X. Bulding the ramdisk was actually really easy once I got the security right, that was messing me up. So I just read through ALL the entries to pull enough details out to get the "pictures off" to make "the wife happy". LOL Peace out bud.

Aug 5 ▾

 **Hafidchraibi@googlewave.com:** hi everybody,  
 i have an iphone 3G 8Gb, jailbroken with 3.1.2 stuck in the apple, when starting when trying iRecovery i get  
**Boot Failure Count: 15 Panic Fail Count: 0**

when i try iRecovery -f 018-6051-014.dmg.ssh it seems to be executed correctly but as soon as i try  
 ramdisk or ramdisk 0x90000000

the iphone reboots and quit the recovery mode and start his looping process  
 when i put it back in recovery mode and try a iRecovery -f kernelcache.release.s5l8920x  
 i get a  
 Attempting to validate kernelcache @ 0x09000000  
 error loading kernelcache

please help

The full iRecovery log

```
Found iPhone/iPod in Recovery mode
=====
:: iRain for n82ap, Copyright 2009, Apple Inc.
::
:: BUILD_TAG: iBoot-636.66
:: BUILD_STYLE: RELEASE
:: USB_SERIAL_NUMBER: CPID:8900 CPRV:30 CPFM:03 S
=====
[FTL:MSG] Apple NAND Driver (AND) RO
[NAND] Device ID 0x-----
[NAND] BANKS_TOTAL 4
[NAND] BLOCKS_PER_BANK 4096
G] FTL_Open [OK]524288
Boot Failure Count: 15 Panic Fail Count: 0
Entering recovery mode, starting command prompt
[OK]
[FTL:MSG] FPart Init [OK]
read old style signature 0x43303035 (line:371)
[FTL:MSG] VFL Register [OK]
[FTL:MSG] VFL Init [OK]
[FTL:MSG] VFL_Open [OK]
[FTL:MSG] FTL Register [OK]
[FTL:WRN] Failure running _LoadFTLCxt!
[FTL:WRN] Recovering NAND Data Structures - this will
[FTL:WRN] _FTLRestore OK!
[FTL:MG] FTL_Open [OK]
Boot Failure Count: 15 Panic Fail Count: 0
Entering recovery mode, starting command prompt
```

 **Msft.guy@googlewave.com:** Try using itunnel\_mux - based steps if you have access to a Windows box.

Aug 31 ▾

 **Jonathannakandala@googlewave.com:** Hi, been trying to get this to work. I've got the original iPhone with 3.1.2 installed. I was able to get upto the step of connecting but then reached a problem. Sep 17 ▾  
 I kept getting the error with the USBMuxConnectByPort. However I used Sn0wbreeze to "pwn" the ipsw. And got the kernel cache from the root directory afterwards.  
 It seems like this should have worked but after a few tries and also finding a "pre-pwned" ipsw, I just kept getting this error on connect.  
 The pc is a Windows XP machine with iTunes 9.2 installed.  
 I did make the ramdisk by copying the files onto it using a pc using transmac don't think I edited the chmod values or was able to. Would have have made any difference?  
 I really want to run fsck -r on my iPhone's user partition =(  
 Also tried the iBoot method but everytime I type bootx. The iPhone just boots into iBoot normally and then fsck fails and it turns off

 **Msft.guy@googlewave.com:** Wtf? Just use the tool to build the ramdisk, why are you 'copying the files'? iv/key for your iPhone 2G ramdisk are on the iPhone Wiki..

Sep 17 ▾



Jonathannakandala@googlewave.com: For some reason the tool crashes every time I open the ramdisk on the wiki =/. Tried that on my Win7 pc and also in a Windows XP virtual machine both times it crashes. Had to download the .NET 4.0 both times so it could be a problem with the framework.

Sep 17 ▾



Jonathannakandala@googlewave.com: oh wow, I gave it another go but instead of using the ramdisk on the snowbreezed ipsw I used to original. Somehow it works!!!! Was able to fsck it and it worked. I cannot thank you enough. I really appreciate it  
You're the best! =D

Sep 17 ▾



Msft.guy@googlewave.com: iBEC.n82ap.RELEASE.dfu  
Your chances might improve if you stop trying to load 3GS firmware onto a 3G

Sep 20 ▾



Hafidchraibi@googlewave.com: THANK YOU msft.guy, it was all about using the right files , so for everybody who has a 3g use 82ap only

Oct 28 ▾



Shalomii@googlewave.com: After a bit of careful reading of the process and googling some things i got as far as the person who posted above me, and I'm stuck in the white screen as well, after the commands. Here is my log for reference.

Oct 3 ▾

Microsoft Windows [Version 6.1.7600]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>cd desktop

```
C:\Users\User\Desktop>itunnel_mux_r61 --ibec iBEC.n82ap.RELEASE.dfu --ramdisk 01
8-7079-079.dmg.ssh --devicetree DevicetreeXXX.img3 --kernelcache kernelcache.rel
ease.n82 --ramdisk-delay 5 --ramdisk-command "ramdisk 0x90000000"
Will try to kick connected devices out of the Recovery mode..
dfu_connect_callback
dfu_disconnect_callback
dfu_connect_callback
dfu_disconnect_callback
recovery_connect_callback
getUsbDeviceName: \\?\USB#VID_05AC&PID_1281#CPID:8900_CPRV:30_CPFM:03_SCEP:05_BD
ID:04_ECID:000003273C1075F7_IBFL:00_SRNM:[87848S1LY7H]_IMEI:[011773006224843]#(B
8085869-FEB9-404B-8CB1-1E5C14FA8C54)\0000
WinDFU::OpenDFUDevice: path: \\?\USB#VID_05AC&PID_1281#CPID:8900_CPRV:30_CPFM:03
_SCEP:05_BDID:04_ECID:000003273C1075F7_IBFL:00_SRNM:[87848S1LY7H]_IMEI:[01177300
6224843]#(B8085869-FEB9-404B-8CB1-1E5C14FA8C54)\0000
WinDFU::OpenDeviceByPath: \\?\USB#VID_05AC&PID_1281#CPID:8900_CPRV:30_CPFM:03_SC
EP:05_BDID:04_ECID:000003273C1075F7_IBFL:00_SRNM:[87848S1LY7H]_IMEI:[01177300622
4843]#(B8085869-FEB9-404B-8CB1-1E5C14FA8C54)\0000
operation 0 progress 3
operation 0 progress 7
operation 0 progress 11
operation 0 progress 15
operation 0 progress 19
operation 0 progress 23
operation 0 progress 27
operation 0 progress 30
operation 0 progress 34
operation 0 progress 38
operation 0 progress 42
operation 0 progress 46
operation 0 progress 50
operation 0 progress 54
operation 0 progress 58
operation 0 progress 61
operation 0 progress 65
operation 0 progress 69
operation 0 progress 73
operation 0 progress 77
operation 0 progress 81
operation 0 progress 85
operation 0 progress 89
operation 0 progress 92
operation 0 progress 96
WinDFU::UploadData: EOF, cbRead: -124
operation 0 progress 100
WinDFU::UploadData: ZLP
WinDFU::FinalizeDfuUpdate: GetStatus: status: 0, state: 6
WinDFU::ProcessUpdateState: status.bState == DFU_STATE_MANIFEST_SYNC
WinDFU::FinalizeDfuUpdate: GetStatus: status: 0, state: 7
WinDFU::ProcessUpdateState: status.bState == DFU_STATE_MANIFEST, PollTimeout: 30
00
WinDFU::FinalizeDfuUpdate: GetStatus: status: 0, state: 8
WinDFU::ProcessUpdateState: status.bState == DFU_STATE_MANIFEST_WAIT_RESET
WinDFU::ResetDevice: resetting...
WinDFU::FinalizeDfuUpdate: success
getUsbDeviceName: \\?\USB#VID_05AC&PID_1281#CPID:8900_CPRV:30_CPFM:03_SCEP:05_BD
ID:04_ECID:000003273C1075F7_IBFL:00_SRNM:[87848S1LY7H]_IMEI:[011773006224843]#(E
D82A167-D61A-4AF6-9AB6-11E52236C576)\0B0000
iBEC iBEC.n82ap.RELEASE.dfu loaded
```

I hope you guys can help us both :)



Msft.guy@googlewave.com: hafidchraibi: use n82ap files, not the n68.. ones.  
shalomii: use 4.0 FW to make CFW and ssh ramdisk, there are problems with sending files over 4.1+ protocol.

Oct 21 ▾



Shalomii@googlewave.com: Hi everyone, am very inexperienced with this situation, and not sure if this recovery method will even work for my situation.  
Well, the device is an iPhone 3G 8GB which was never jailbroken as far as i remember, and had a very early FW version, don't remember which. My mom claims she turned it off before a flight, turned it back on after and it went to the connect to itunes screen. I tried many methods to try and get it to function again without restoring. I tried using QuickPwn (cant get it to open on any of my computer for some reason) ZPhone (didnt work) irecovery (am able to send commands and they work, such as reboot but the process explained somewhere about trying to kick it out of recovery loop didnt work) I tried to use blackra1n and it detects it while in recovery mode and even says successfully jailbroken, but the screen with geohot's face doesn't come up and just reboots once into apple logo, and then reboots again into connect to itunes screen.  
So, is it even possible for me to do this type of recovery?

Oct 2 ▾

I'd really appreciate any and all help you all can give.

Thanks

 **Me:** Hi, this is what I have done until now, please correct me if something is wrong or explain to me the next step(s)... thanks! iPhone 3GS, 3.1.2, new bootrom, tethered JB (blackra1n), recovery boot-loop, trying to save the data, both MacOS X and WinXP available to work on this problem. Mac and PC both run iTunes 9.2. SHSH on file for 3.1.2 (among others) Oct 30 ▾

1. Downloaded "iPhone2,1\_3.1.2\_7D11\_Restore.ipsw" somewhere
2. Downloaded Pwnage Tool, version 3.1.4
3. Pwnage Tool: Expert Mode, Select iPhone 3gs, Select the ipsw file mentioned above, double-click on build, define output filename and location -> created: "iPhone2,1\_3.1.2\_7D11\_Custom\_Restore.ipsw" Are the specific options in the Pwnage Tool important? I think I checked "General" (a green check-mark appeared next to it) and then I hit the Build button in the red font... everything correct here?
4. Renamed custom ipsw to \*.zip
5. Extract "018-6051-014.dmg" from the root folder of this zip file (is this the right one? It's 13mb, but there's also a 307mb one in there)
6. Downloaded the "RamdiskBuilder" tool and extracted it, started the tool
7. RamdiskBuilder: Enter IV = fd19726dc6b555b6bb4dbbcd91d1e7c0, Key = fb2792b935fb9cd183341cb24539376556f8b7b8f887eb90fcebaa0daf2d6d9c
8. RamdiskBuilder: Select Ramdisk -> 018-6051-014.dmg
9. RamdiskBuilder: Got the following output -> <http://pastie.org/private/ie5ceb37ruuepmaz58g8a>
10. Two new files have been created in the RamdiskBuilder folder: 018-6051-014.dmg.dec (~16mb) and 018-6051-014.dmg.ssh (~16mb)
11. ?

There are several steps listed under "Tethered support", where Advanced skills and OS X are recommended... when in the process am I to do these steps? Are they to be done before the main instructions list, or somewhere in between or the very end?

Please give feedback if everything was done correctly so far and what the next step(s) would be... many thanks!

msft.guy's how-to seems great, but it's just a little bit above my IT skillset, so if someone could translate/transform into steps that are easier to follow, that would be awesome. Please help me out...

 **Msft.guy@googlewave.com:** So far seems fine. Note that there's an easier way now, using GreenPois0n exploit: <http://www.bingner.com/pwnstrap.html> Oct 30 ▾  
After you load 3.1.2 ibec using manual steps from this method, you can proceed loading ramdisk and kernelcache.

 **Me:** Thank you so much for your reply Msft.guy!  
Just to make sure that I don't do anything wrong: Oct 31 ▾

1. I will use the greenpois0n JB and then upload the iBSS from my 3.1.2 custom/pwned ipsw via irecovery, even though the site you linked to specifically says that it only works with ipsw 4.1 or higher?
2. "After you load 3.1.2 ibec using manual steps from this method" - does this mean I should do steps 1-5 from the manual procedure, or 1-6? [I assume step 7 would not be a good idea ;)]

Also: When I do irecovery -s, I have the feeling that my commands do not really have an effect. printenv for example doesn't do anything, I just get a new command line. "reboot" works though... I am just mentioning this because steps 2 and 6 include various commands that I am supposed to execute in iRecovery and I don't know whether this is a problem or if I should just go ahead with steps 3,4,5 and then proceed w/ loading ramdisk and the kernelcache.

Btw, the fact that printenv (for example) does not seem to "work" happens with iRecovery 1.3 and with the "unofficial iRecovery for new devices" by bingner... I have libusb v1.2.2.0 installed.

Thank you!

 **Tgerschman@googlewave.com:** Hi! I'm not sure if this wave is still alive - but was hoping for some help if anyone is still around. Nov 25 ▾  
My situation is as follows.

iPhone 3G 3.1.2 - Ultrasn0w unlocked

Was working all day, but battery seemed to be draining quite a bit (was using 3G heavily though). Reached about 10% and then the phone just shut-off completely. I thought that it was due to a dead battery so plugged it into the wall when I got home and that's when the real problem started.

When I push power or plug in the USB the device powers on to the Apple Logo. Then, after 24 seconds, it shuts off completely. This is consistent. I am able to enter to ?recovery mode, in which case it just stays there and is recognized by iTunes (10.1 PC) and offers to restore.

I have tried to kick it out of recovery mode with TinyUmbrella and then just back to shutting off after 24 seconds.

I have tried Redsn0w and iB33j's dcc version (does anyone have working link to the other ones??). It sends the file over to the iPhone which then processes it for several minutes (Jailbreaking Data with spinning wheel) and then reboots. That time the Apple logo stays for about 90 seconds before rebooting and then back to the 24 seconds.

I have tried to use iRecover and have had some difficulties in that step (and hence not been able to get to the Ramdisk solution to save my contacts, photos, sms, etc). I am running Windows 7. I installed libusb 0.1.12.1 using the "WinXP compatibility mode" (and subsequently have also tried v1.2.2.0) but iRecover always says "Got USB. No iPhone/iPod found." When running the libusb test utility I don't get a proper readout either. So does anyone have further tips on how to properly install libusb for Windows 7 (64bit) or to get iRecover working?

note - I think I switched off WiFi - does that mean SSH is impossible? will itunnel still work?

Thanks so much for the help!

I'd be so happy to be able to access my files on the iPhone and then do a fresh restore. It would be great if there was some way to just "fix it" with b33j's files if anyone has access to those (which dcc didn't work unfortunately). Any other suggestions??

 **Msft.guy@googlewave.com:** 1. Use iReb 4 from DFU mode to get a 'white screen'  
2. Use itunnel\_mux to load the ssh ramdisk, prepare files using the ssh ramdisk builder and Snowbreeze for 3.1.2. Nov 25 ▾

Tags: [iPhone](#) [SSH](#) [iRecovery](#) [ramdisk](#) [payload](#) [recovery](#) [3GS](#) [DISCUSSION WAVE](#) [iphone 2g](#) [iphone edge](#) [+](#)

[Next wave](#) ➔