Step 0: What's This All About?

DFU nonce collision downgrade is a downgrade method that doesn't need a jailbreak or already set generator to restore your device. You can restore from any firmware you want as long as latest SEP and baseband are compatible with destination firmware.

Step 1: Requirements

1) You need to have a 4K device.

This includes:
-> iPhone 5s/6/6+
-> iPad Air 1
-> iPad Mini 2/3
-> iPod touch 6

2) Your blobs should be saved with colliding apnonces. If you don't want to save every blob for every apnonce manually, check nudaoaddu for A7 by Dora and A8/A8x update by me.

Step 2: Creating Downgrade Folder

1) Create a folder on your Mac and name it whatever you want. I'll name it as 'downgrade' in this example.
2) **Put the destination ipsw file to the folder.**
3) Put the shsh blob(s) that has colliding apnonces for your device to the downgrade folder.
4) Put the latest futurerestore by s0uthwest to the downgrade folder.

Step 3: Preparing Futurerestore

1) Launch terminal
2) cd to your downgrade folder
3) Write this command (if you're on Mac): ./futurerestore -t [your blob here] --latest-sep --latest-baseband [ipsw file here]

Step 4: Preparing The Device

The shsh blob you saved earlier has a custom apnonce and it needs to match the device's apnonce to start restoring. Let's match them then!

1) Put your device in DFU mode
2) Run igetnonce (download here:) to see which apnonce your device has generated
3) If you got the nonce you need, you can proceed over to step 5, otherwise keep putting your device to DFU Mode over and over again until you get the announce your blob has.

Step 5: Restoring The Device

Nice! You got your device's apnonce match with blob's apnonce. But still, there is a problem.

Futurerestore can only restore devices that are on Recovery or normal mode. But nonce collision only exist in DFU Mode! So, how do we start the restore process?

You can sign iBSS and iBEC and upload it to your device using irecovery and *hopefully* it will jump into recovery mode. Well, this has never worked for me. So we found a workaround. We call this 'static nonce method'.

To do this you'll need latest signing ipsw from apple and iTunes.

1) Keep your device connected in DFU mode with the desired apnonce and launch iTunes.
2) Click 'restore device' in iTunes with alt-option key.
3) Select the latest ipsw that you have downloaded earlier (don't worry we won't restore to it)
4) Start the restore process in iTunes. When it says 'waiting for device', wait for the backlight to turn on on your device and then plug the usb cable out of the Mac, close iTunes and plug the cable back again.

YOU'RE NOW IN RECOVERY MODE AND YOUR DESIRED APNONCE REMAINS THE SAME!

Step 6: Starting Futurerestore

Return back to the terminal window that you prepared in STEP 3 and press enter. Restore will start and your device will be downgraded to the destination firmware!