Tips for Jailbreaking iOS Devices

Older iOS devices were able to hold an untethered jailbreak which means the user could turn their device off and on without losing the jailbreak. With later iOS versions, we rely on tethered jailbreaks which means the device may get stuck in Recovery Mode or not be able to boot if it loses a charge or reboots. It's important to keep tethered jailbreaks charged at all times to avoid this issue. There are also cases of semi-tethered and semi-untethered cases for older iOS versions.

CONS: Jailbreaking is not always simple and may brick the device, leaving it un-functional. The System and the Data partition will be modified in newer jailbreaks. Jailbreaks for iOS 10 and 11 REQUIRE an Internet connection (must be able to communicate with ppq.apple.com at a minimum). You WILL ALWAYS leave a trace when you jailbreak. Even a factory reset may leave traces behind.

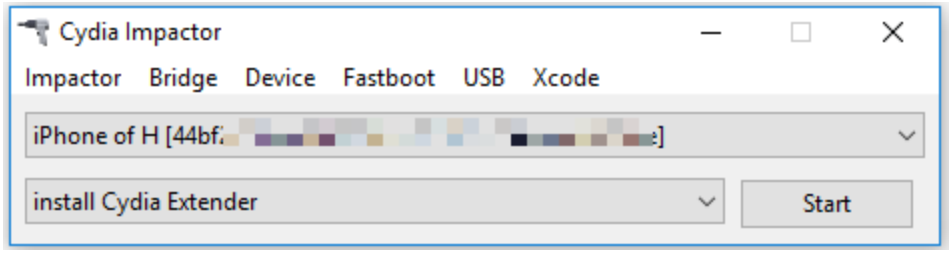
PROS: Jailbreaking, when successful, gives the examiner full access to the file system and its contents.

Common Mistakes:

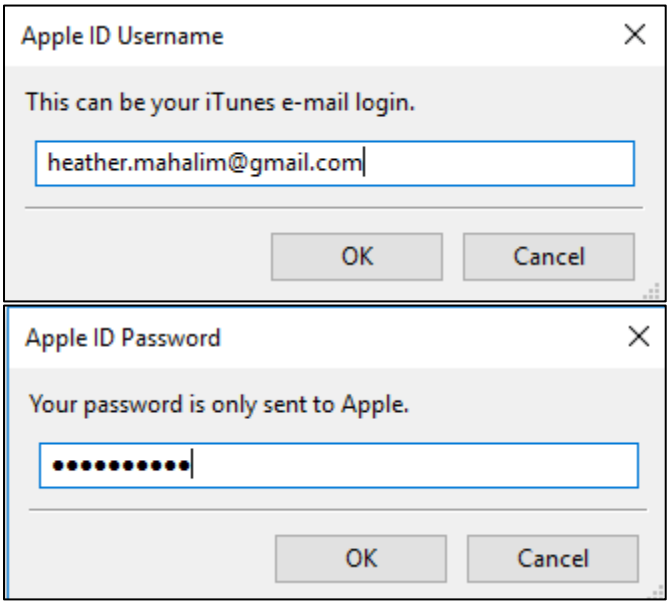
1. Do not run as Administrator on Windows – drag and drop will no longer work
2. Make sure you have to correct IPA for your iOS version
3. DO NOT let the iOS device update during the process or you may lose your jailbreak

For iOS 10 and 11 jailbreaks:

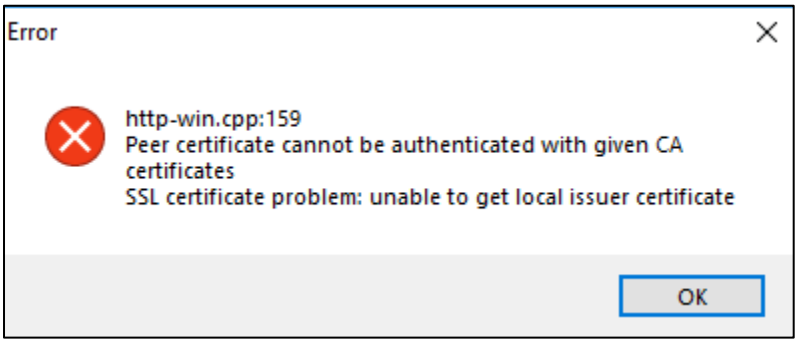
1. Backup with iTunes or create an acquisition to ensure you have all data possible prior to jailbreaking.
2. Remove the device passcode and turn off Find My iPhone, if possible (Settings > UserName > iCloud > Find My iPhone and Turn off – will require Apple ID and Password.
3. Research your iOS version and device type and download the IPA file from the following trusted site:
   https://www.theiphonewiki.com/wiki/Jailbreak
4. Download the Cydia Impactor from **http://www.cydiaimpactor.com/** (used to sign the IPA so it can be executed)
5. Connect the device to the forensic workstation and launch Cydia Impactor
6. Trust the computer on the iOS device
7. Drag the IPA into Cydia Impactor and click Start



8. You must provide an Apple ID and Password (Create a test one that is used for this purpose)



9. Cydia Impactor should sideload the IPA – should it fail and you see the error below, go to step 10



10. Make sure you watch the iOS device, as you may have to do the following:
    a. Go into Settings
    b. General
    c. Device Management
    d. Trust the X
11. On the iOS device, launch the jailbreak app and follow any onscreen instructions.
12. Ensure you are still connect to the Internet and Cellular, if relevant

Cydia is NO longer installed, but the jailbreak should have SSH access (port 22 or 2222), if not, try to install OpenSSH from Cydia. If this does not work, we need to find a way to transfer files of interest to and from the device.