TV 4K Jailbreak Guide

@J_Duffy01 + ElcomSoft

An Introduction

There's a limited amount of information on the web around installing the new unc0ver jailbreak on tvOS 13.5. With this in mind, myself and ElcomSoft collaborated in order to release this guide showing the entire process in detail.

Requirements

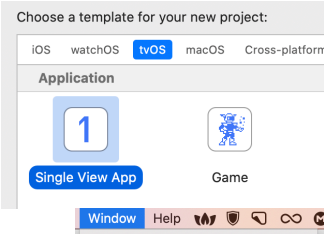
There are a couple of requirements which we'll need to fufill before we get started! I'll list them here:

- Xcode
- Apple Developer Account
- Mac (connected to the same network as Apple TV)
- iOS App Signer (https://dantheman827.github.io/ios-app-signer)
- Unc0verTV IPA (https://unc0ver.dev/tvos)

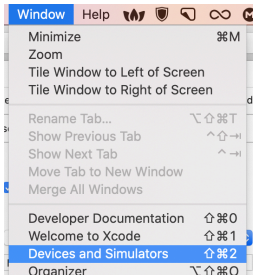
So, let's begin!

1) Setup your **Apple TV** if you haven't already, and maybe start a little **Chilled Jazz** on **Spotify** (sorry Apple Music) in the background (https://open.spotify.com/playlist/37i9dQZF1DX2vYju3i0lNX?si=1GJZcOufRRCNKQs00SzWrA).

2) On our **Apple TV**, launch the **Settings** app. Scroll to '**Remotes and Devices**'. Select this menu and scroll again, this time to '**Remote App and Devices**'. You should see '**Devices**' on the right side of your Apple TV display at this point, although it's probably not populated.

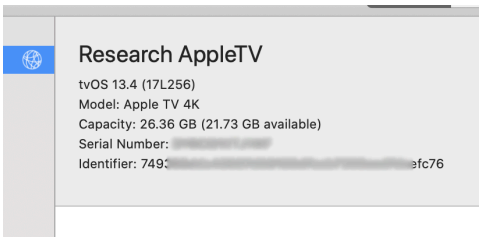


3) Let's head back to the **Mac**. Launch **Xcode** and select '**Create a new Xcode project**'. Select **tvOS**, '**Single View App**', and then hit '**Next**'. For our project name, we can type absolutely anything! Maybe type **unc0ver**. Your team should display your **Apple ID**. Leave all the other settings as default, and finally, hit '**Finish**'!



4) **Xcode** should be showing the '**General**' tab by default. This is designed to show some basic information about our application but isn't required for our task, so we can ignore the information here in this case. Select '**Window**' from the menu bar, and select '**Devices and Simulators**'.

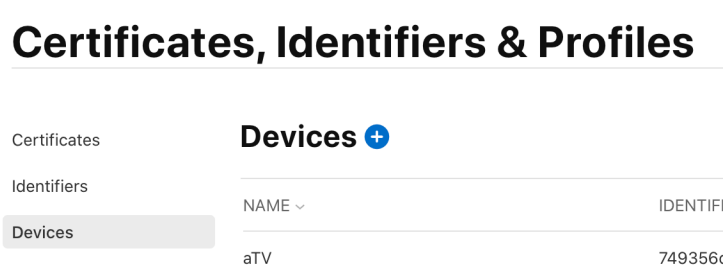
5) Your **Apple TV** should show immediately on the new window, with the option to '**Pair**' the Apple TV. If it doesn't, make sure you completed **Step 2**. You should now be prompted to enter the **pairing code** displayed on the Apple TV. This allows the **Mac** and **Apple TV** to communicate and install applications **over-the-air**.



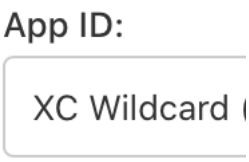
6) While we have '**Devices and Simulators**' open, and our Apple TV successfully paired, copy the '**Identifier**' of our Apple TV. It's a pretty long alphanumeric string! You could add it to a virtual sticky-note for a few minutes, we'll need it soon!

5) We can now close the the '**Devices and Simulators**' window and return to our main Xcode window. Select the '**Signing & Capabilities**' tab and tick '**Automatically manage signing**'. If you see an error, don't worry (yet)!

6) Head to **'https://developer.apple.com'** and select '**Account**'. Head to '**Devices**' and hit the '**+**'. Name your Apple TV, and in the **Device ID** we can now paste the '**Identifier**' we saved earlier in our virtual sticky-note!
Now that our Apple TV is registered in our account, we may continue on this journey!

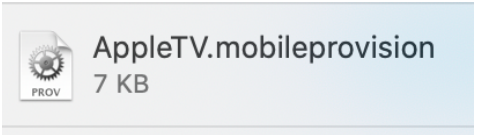


7) Head to '**Certificates, Identifiers & Profiles**' and select '**Profiles**'. Hit the '**+**' and select '**tvOS App Development**'.
Continue, and for our '**Application ID**' we can simply select the **XC Wildcard**. Again, hit the lovely, too-well-known Continue button!
Your Mac should now be shown in the list of **Certificates**. For example, '**James's Macbook Pro**'. Tick your mac and hit Continue.
Select your Apple TV in the list, and as always, hit Continue. Give your **certificate** a name, anything you like!

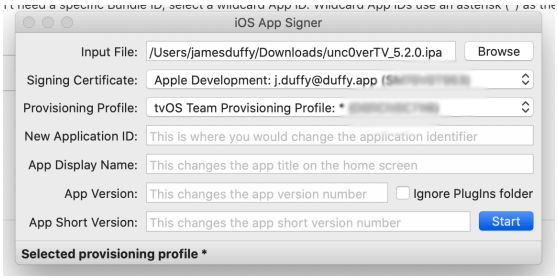


Now, hit '**Generate**'.

8) We can how hit the '**Download**' button to download our **Mobile Provisioning Profile**! This is a profile that allows **unc0ver** to be signed and installed on our specific **Apple TV**!

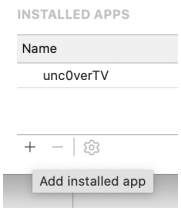


9) Now, that most of the hard-work done. Congratulations! We can now launch 'iOS App Signer' (The application from the prerequisites).
Our Input File is our **unc0verTV IPA**. The signing certificate should be pre-populated with '**Apple Development: APPLEIDHERE!**'.
Now, for the Provisioning Profile, select '**Choose Custom File**' and select the **Provisioning Profile** we downloaded and generated in the **Apple Developer Portal**!



10) Hit **Start**! You may name the output file anything you like...
I'm going to presume everything processed successfully, and we have our final, signed **IPA**! (If something went wrong, please do **@** me on **Twitter** or leave a comment!)

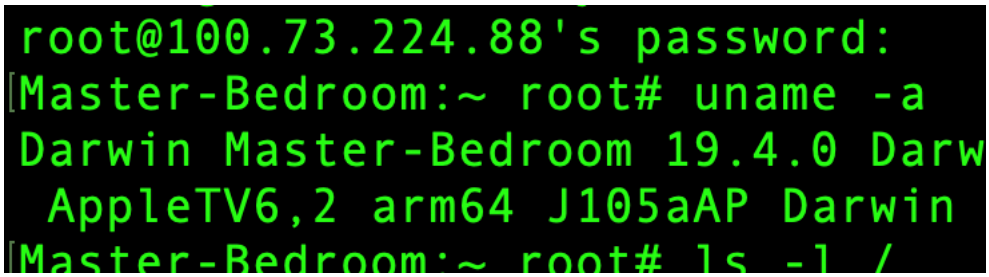
11) We're almost there... Hopefully the **Chilled Jazz** music is keeping you going! Head back too **Xcode**, and open '**Devices and Simulators**' once more. Under '**Installed Apps**' for our Apple ID, hit the '**+**'.
You may now select our **Signed IPA** we created using '**iOS App Signer**'!



12) If all is well... the **unc0ver** should now be installed on the **Apple TV 4K**! (But we're not done yet (sorry!))...

13) Let's launch the **unc0ver** application on your Apple TV and hit **Jailbreak**. Following a successful execution, the **nitoTV** launcher should appear! Let's head to the Settings app on your Apple TV. Open the **Network** tab, and take note of the '**IP Address**' of your Apple TV.

14) On the mac, head over to the Terminal! Type the following '**ssh root@IPADDRESS**' (For me, the command would be '**ssh root@100.73.224.88**'). You'll now have one last prompt asking you to confirm the **identity** of the remote server (which is the **Apple TV**). Confirm the prompt, and type '**alpine**' as the password.



15) You're in, congratulations and enjoy your jailbroken **Apple TV 4K**! Woohoo!