مراحل کار جلبریک کردن :

مرحله اول :ابتدا جدیدترین نسخه برنامه evasionکه همان evasi0n7است را از دانلود نمایید و آن را داخل پوشه‌ای تحت عنوان "evasi0n"روی دسکتاپ خود ذخیره نمایید.

مرحله دوم :روی فایل دانلود شده دبل کلیک نمایید و فولدر آن را اکسترکت یا استخراج نمایید. از داخل فولدر یاد شده برنامه evasionرا پیدا کرده و راه‌اندازی نمایید.

کاربران ویندوز: لطفا با یوزر Administratorاین برنامه را اجرا نمایید. برای این منظور روی فولدر برنامه راست کلیک نمایید و گزینه "Run as Administrator"را انتخاب کنید.

مرحله سوم :پس از اجرای برنامه، از شما خواسته می‌شود تا آی‌پد خود را به سیستم متصل نمایید.

مرحله ۴ :در این مرحله لازم است که پسورد گوشی یا تبلت خود را غیرفعال نمایید چراکه در غیر اینصورت نمی‌توانید

ن را جیلبریک نمایید، برای این منظور کافی است به ترتیب این مسیر را دنبال نمایید

: Settings -> General -> Passcode Lock On -> Turn Passcode Off

مرحله ۵ :پس از این مرحله آی‌پد یا گوشی خود را به سیستم متصل نمایید تا برنامه evasi0nابزار شما را شناسایی نموده و نام میان‌افزاری که روی آن در حال اجراست را ذکر کند. پس از این مرحله باید روی دکمه Jailbreakکلیک نمایید .

مرحله ۶ :پس از کلیک نمودن روی دکمهJailbreak، نرم‌افزار مراحل پیشرفت فرایند جیلبریک را به شما نشان می‌دهد که به شرح زیر می‌باشد:

- دریافت بسته نرم‌افزاری
- آپلود نمودن داده‌های جیلبریک
- وارد نمودن برنامه
- پیکره‌بندی سیستم
- ری‌بوت کردن سیستم

که معادل انگلیسی آنها به شرح زیر می‌باشد:

- Retrieving remote package

- Uploading jailbreak data
- Injecting evasion app (1/2)
- Injecting evasion app (2/2)
- Configuring system (1/2)
- Configuring system (2/2)
- Rebooting device

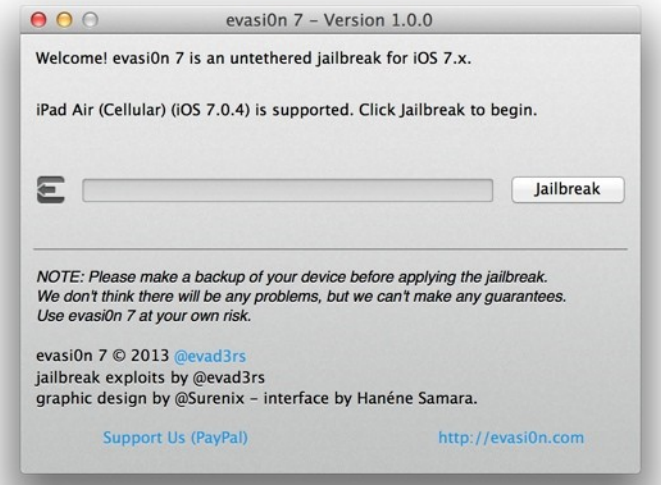
در زمان انجام این فرایند باید کاملا صبور باشید و برنامه‌های iTunesیا Xcodeرا اجرا نکنید.

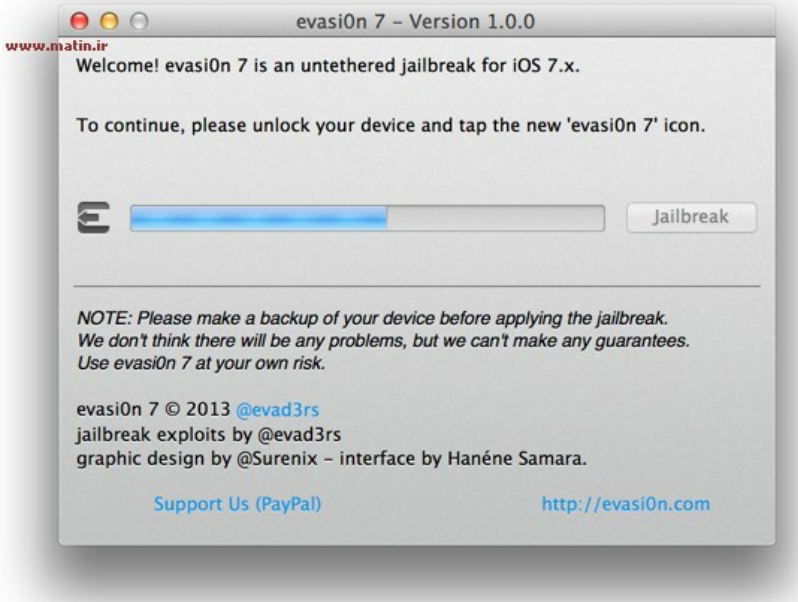
مرحله ۷ :پس از اتمام این فرایند، ابزار شما از نو بوت می‌شود و سیستم از شما می‌خواهد تا آی‌پد خود را قفل‌گشایی یا اصطلاحا آنلاک نمایید. به خاطر داشته باشید که پنجره برنامه را نبندید.

مرحله ۸ :پس از قفل‌گشایی گوشی یا تبلت خود، روی آیکون برنامه evasi0n 7کلیک نمایید.

مرحله ۹ :در زمان اجرای برنامه، صفحه نمایش شما کاملا سفید شده و سپس مجددا بوت می‌شود.

مرحله ۱۰ :در این لحظه باقی مراحل جیلبریک شدن انجام می‌شود و پس از بون شدن مجدد، لوگوی بزرگی از evasi0nروی نمایشگر دیده می‌شود و پیغام‌های مختلفی در مورد فرایند جیلبریک شدن سیستم به کاربر داده میشود که به شرح زیر است:





- Reading kernel
- Calculating offsets
- Setting up packages
- Setting up Cydia
- Continuing with boot

مرحله ۱۱ :در این نقطه کار تمام است و آیکون مربوط به Cydiaروی نمایشگر نشان داده می‌شود. اگر در میانه راه مشکلی پیش‌آمد بهترین کاری که می‌توانید انجام دهید آن است که آی‌پد یا آی‌فون خود را ری‌ست نموده و مجددا فرایند را آغاز کنید.

چه کارهایی را می‌توان با ابزارهای جیل‌بریک شده انجام داد؟

- تغییر اینترفیس ابزارهای مبتنی بر iOS
- حذف برنامه‌های داخلی iOS
- نصب برنامه‌هایی که از سوی اپل مجوز نصب آنها وجود ندارد و یا در App Store موجود نمی‌باشند.
- دریافت و نصب برنامه‌های پولی به صورت رایگان (هرچند که این کار نوعی سرقت محسوب می‌شود).
- دانلود موسیقی، ویدئو، کتاب‌های الکترونیکی و انواع دیگر محتوی به صورت رایگان
- دسترسی به فایل سیستم iOS

اپل مخالف اصلی Jailbreak

مسلما این اقدام به هیچ وجه از سوی اپل حمایت نمی‌شود با این حال هکرها همواره به دنبال یافتن راهی برای نفوذ به سیستم عامل اپل می‌گردند تا امکان استفاده از برنامه‌های ساخته شده توسط توسعه‌دهندگان ثالث را برای کاربران این ابزارها فراهم نمایند. اما این مسأله از طرف دیگر اپل را وادار می‌کند تا به دنبال کشف آسیب‌پذیری‌های iOSو برطرف نمودن آن باشد.

در همین راستا نیز به محض آنکه یکی از انجمن‌های Jailbreakابزار جدیدی برای شکستن قفل iOSتولید میکند، اپل به این مسأله پی می‌برد و در نسخه جدید سیستم عامل خود اقدام به برطرف کردن آن می‌کند و در نتیجه استفاده از آن ابزار در نسخه جدید امکان‌پذیر نخواهد بود. هکرها که تنها به پشتوانه خلاقیت و ابتکار خود عمل می‌کنند، ممکن است تا مدتها نسخه جدیدی ارائه نکنند و این مسأله مدت زمان زیادی به طول بیانجامد. روشن است که بروز رسانی سیستم عامل گوشی به نسخه جدید به معنی برطرف شدن نقطه نفوذ و از کار افتادن Jailbreakاست و این بدان معناست که گوشی مجددا به وضعیت قفل شده سابق خود باز خواهد گشت. سیستم عامل iOS 7در ۲۲ سپتامبر ۲۰۱۳ منتشر شد و ابزار Jailbreakآن در ۱۶ دسامبر عرضه شد: یعنی حدود ۴ ماه زمان سپری شد تا هکرها نقطه ضعف آن را پیدا کنند. از سویی به زودی اپل این نقطه ضعف را در نسخه جدید سیستم عامل iOSبرطرف خواهد کرد و آن زمان است که کاربر باید میان انتخاب سیستم عامل جدید و امکان نفوذ به سیستم عامل یکی را انتخاب نماید.