Hey guys, just thought i would make this little Guide sheet for methods to hacking, their difficulty, and include some tutorials on them. Im making this so when people ask me how apps are hacked, i have an easy way to provide them with a link including all my methods I've learned people use to hack apps.

If you would like to download this tutorial as a Word file, please click HERE (this file is actually an outdated file of the tutorial because I cant post this tutorial to mediafire, then reedit the document and put the download link it it. So if you want the updated link, go to http://www.iapphacks.com/posting.php?mode=edit&f=8&t=20762&p=180423 , then click on the link provided there.

*Please note that this guide is mainly for beginners to the app hacking world who are striving to learn how to secure their own apps in development, however there may be much to learn in the more advanced hacking methods. a FAQ about hacking apps is located at the bottom of this tutorial.

ALSO TAKE PRECAUTION: This tutorial is for educational purposes only! Some things in this tutorial could be used to do illegal acts. Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for fair use for purposes such as criticism, comment, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use."

Table of Contents:

----IAPFree
----FLEX
7. IDA Hacking- Difficult
----Decrypting
----Dubugging

1. Pre-made Hacks

-Obviously, the easiest way hackers get into your apps is to download other people's hacks and use them. I included this so people have a good reference of where to get hacks if they aren't interested in creating their own.
Installing someone else's hack isn't a universal process. In order to install their hack into your game, it depends what method they used to hack the game. Typically people provide a tutorial/explaination of how to install their hack, but sometimes they don't. Usually, however, if you download a file, you just replace your file with theirs in your device. This can be done a few different ways with file managers. I disucuss this later-on in the tutorial.

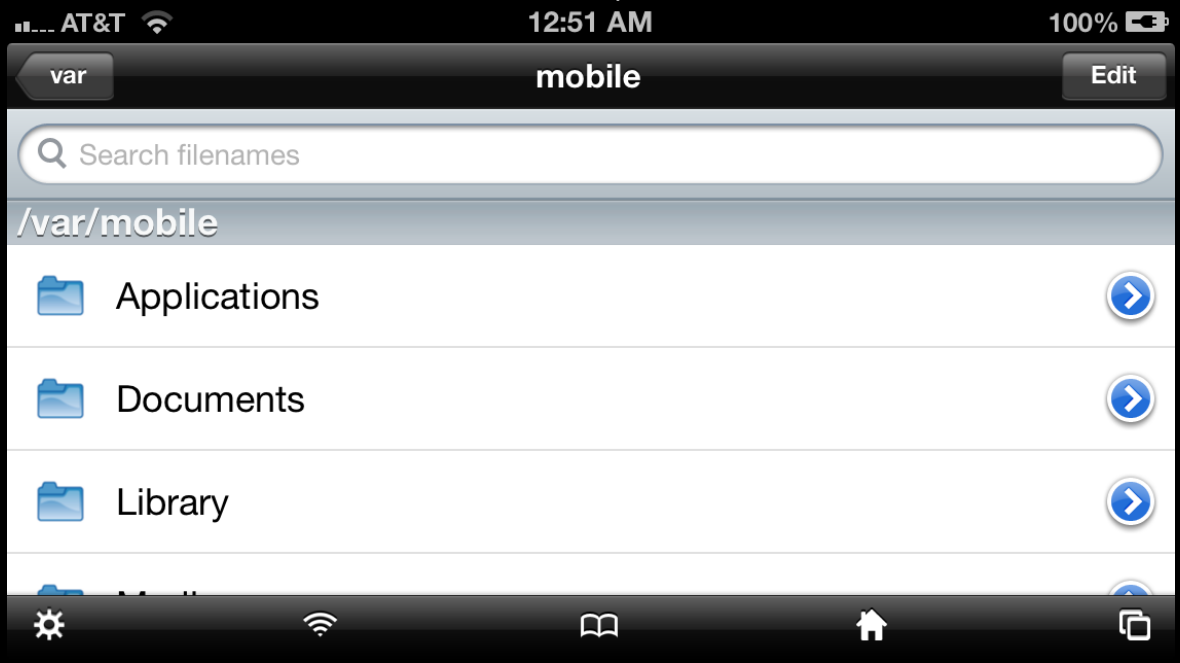
Where to find hacks.
1. Iapphacks-http://www.iapphacks.com/ios-free-hacks-f3/ Obviously, you can get hacks here, on Iapphacks.
2. Cydia- Try adding the repo "http://ihacksrepo.com/" in Cydia! Search for the app you would like to hack there.
3. Google- Did you try googling it? Sometimes a good, ol' google search does the trick!
4. Youtube- Make sure you tried youtube! I always try youtube first. Youtube is a jackpot for app hacks, but make sure to watch out for the scams! Ive seen MANY posts of fake hacks recently where you download a program to hack your device, sort of like this one: www.youtube.com/watch?v=E4Culy5xtpg

2. Text Editing- Basic

Description: The most basic way to hack your apps, involving using file managers such as Ifile, Ifunbox, and Iexplorer to text edit .txt, .plist, and .xml files.

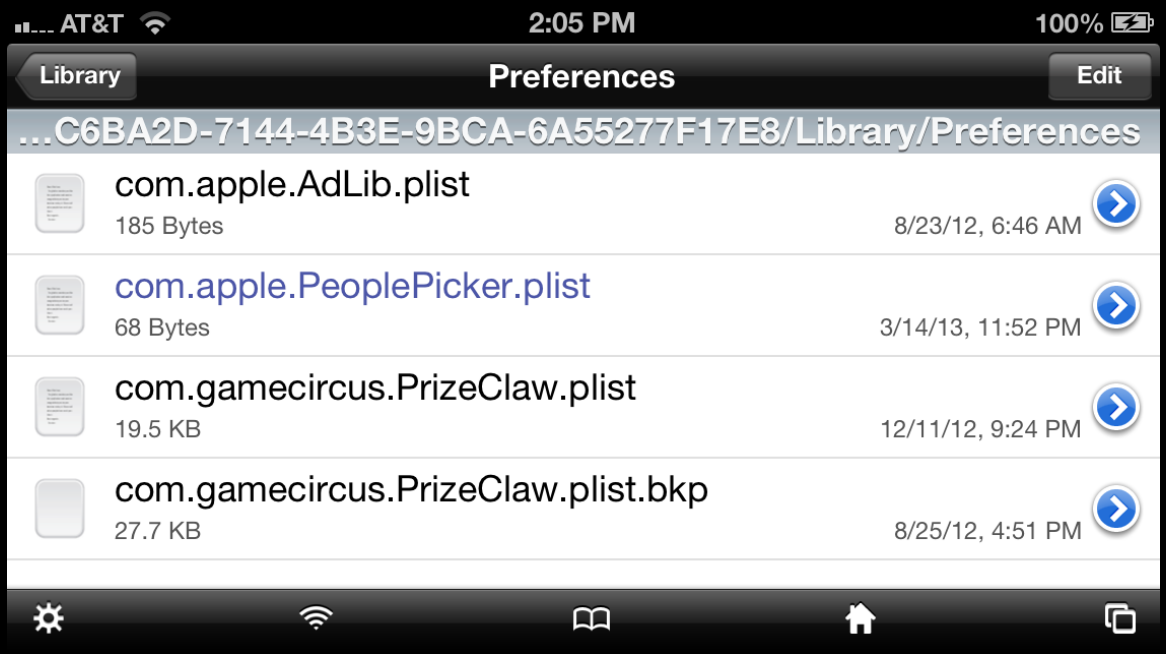
What you Need: File manager, app to hack

To begin learning to app hack, I would strongly suggest you jailbreak NOW, especially if you are on IOS 6.0+. (If you are one IOS 6.1.3+ and you have an iPhone 4s or 5, you cannot Jailbreak at this time; however, if you are on IOS 6.1.3+ and have an iPhone 4 or below, you can do a tethered jailbreak) I don't want to go into why i suggest this, but just take my word for it, its worth it. Once jailbroken, were going to download the most well-known hacking tool to app hackers, Ifile. *If you cannot jailbreak, don't freak out, ill provide another method to do basic hacks without a jailbreak later in this tutorial.* Go to Cydia and search "Ifile" in the search bar, then install Ifile.



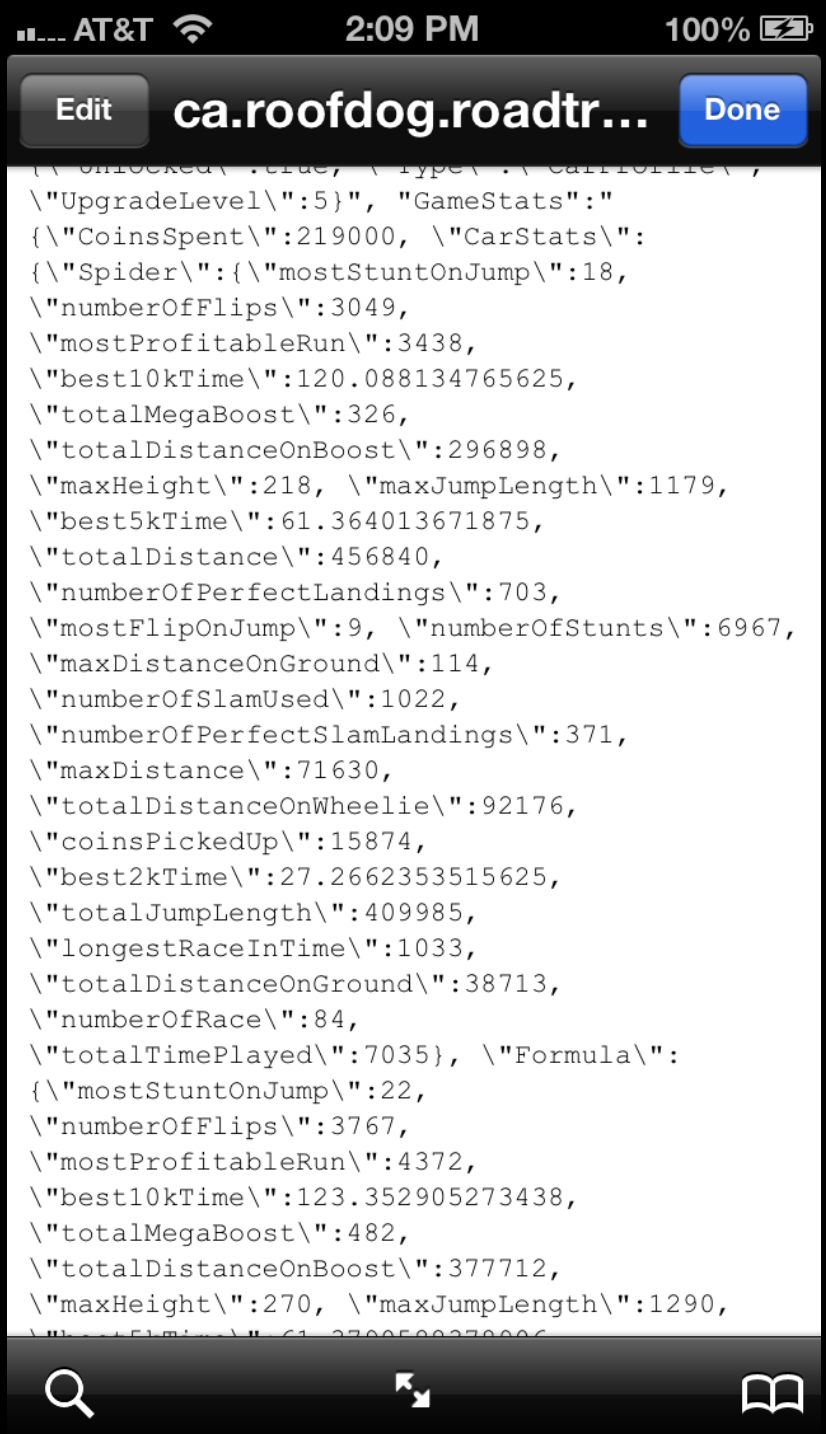
(Ifile- var/mobile/)

This is whats called a file manager. You can view nearly all of the files on your Idevice. Now navigate your way to var>mobile>Applications in Ifile.
Now go to settings (bottom left) and click on "File Viewers", then make sure "Application Names" is turned on. Click done.
See all your apps? Go on, explore. click through your favorite app and view the file contents. search around a little. Once ready, go to the app you would like to hack, navigate your way to "app you want to hack">Library>Preferences. Now, click on the .plist file without "apple" in the name.



(very bottom file)

This file (or files) should hold valuable data for relatively insecure apps.
However, a LOT of the time, you will find your high scores and things of that sort in this file. This is not valuable if your looking to modify your leader board scores (usually) because most games will update the scores online, then update your scores on your game; basically, the scores in the game are usually just for the users purpose.
However, if your only purpose is to decieve your friends on your highest score, you can modify your number here and it will appear in the game



(an example of what you would usually find in this file. The game is Extreme Road Trip 2)

Tap "text editor". If you would like to try to hack a game that works with this method, download "coin dozer" or "Prize Claw". In the .plist file for Prize Claw "com.gamecircus.PrizeClaw.plist" find where it says:

(near the bottom of the file)
"<key>scene0: :m_current_level</key>
<integer>1<integer>"

(if your having difficulty finding it, use my side-scroller bar as a reference to how far down the page it is)

Pretty easy, right? Can you take a guess what you do to hack this? i

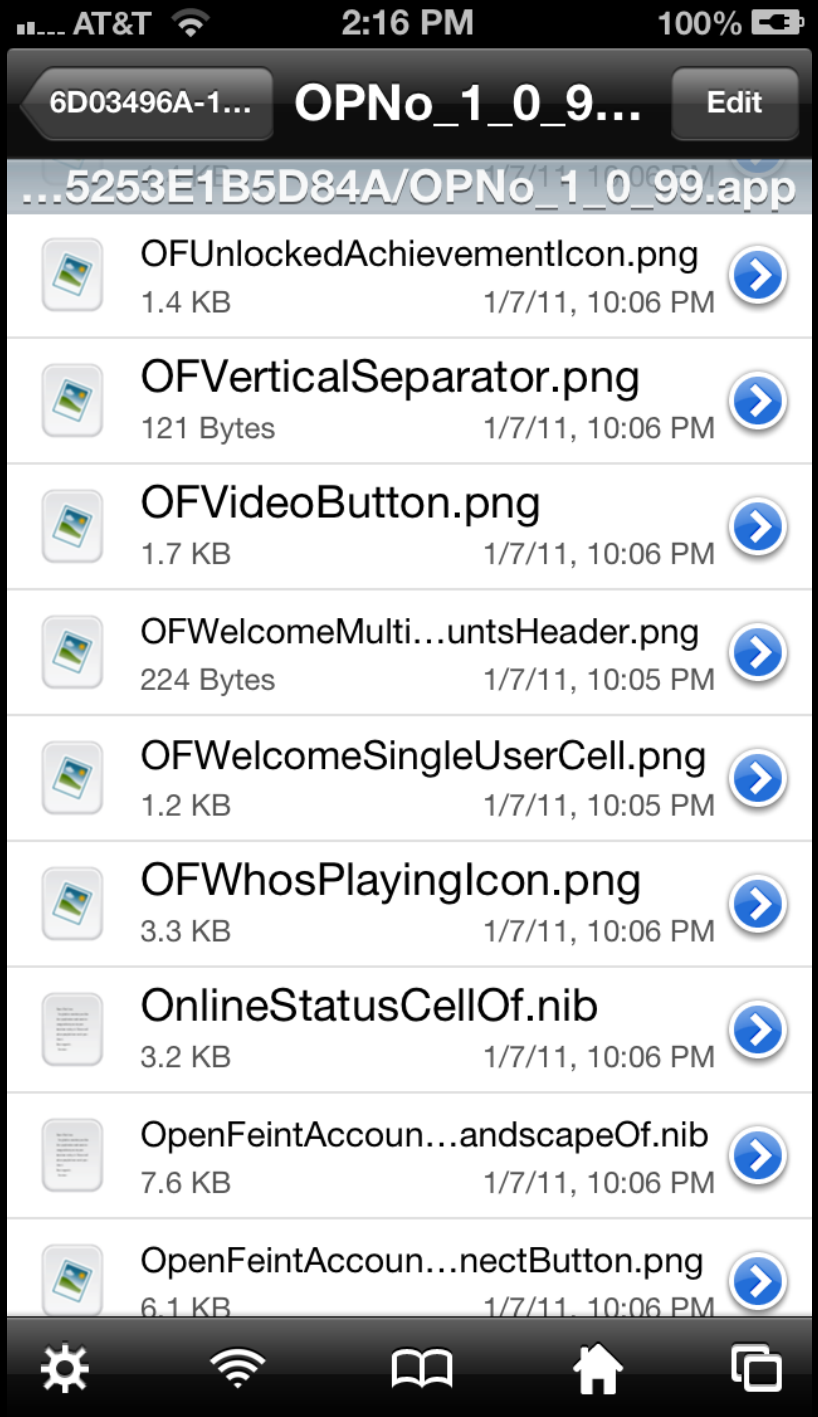
bet you can if you passed 7th grade math! Edit the integer (number) to a higher number. So change it to:
"<integer>999<integer>"
If your looking to hack for more coins, well ill leave you hanging! figure it out! Its fairly simple to do, its found in this file. You can even hack your prizes in this file, mana amount, etc. Many things! good luck! When your finished, click done, then exit out of Ifile, go to your backgrounding apps and *make sure the app you edited is deleted from your backgrounding before testing your tweaks.

Now, if you DONT have a jailbroken device, download ifunbox at :http://www.i-funbox.com
install this file manager and do the same thing as described above. Im not going to go through the process of how to find the file and all in Ifunbox, Im sure your able. Once you find it, change the name of the file to make it a ".txt" file instead of ".plist" in order to edit the file. Make sure to change it back when your done, then drag and drop the file over the old one to sync your hack to your device.

So, now I know how to hack the most basic .plist file in an app... what about all the other files??
Well, we will get into other files! However, this method only focuses on .plist, .txt, xml files.
".txt" stands for "text", the most basic file format there is.
.xml stands for “Extensible markup language”, which “was created to structure, store, and transport information.” According to w3schools.com.
".plist" stands for "property list", so in .plist files you'll find many things that have true/false values. Some of these can lead to valuable hacks by simply deleting "false" and making it "true"! or vis versa. For example, I have found code in the past that is about an achievement or an unlock, it'll say something like:
<key/>Car_upgrade_unlocked<key/>
<false/>
So, take your knowledge and run with it! See if you can't find .plist or .txt files in the game that have these traits. Once trying the library>preferences method, attempt editing files in the "name of app".app file. Some games there are many .txt files, and some there aren't! NOTE** if you are using a non-jailbroken iphone to test these mods and are on ios 6.0+ you will NOT be able to modify any files in the ".app" folder. Apple added this restriction into ios 6.0 to prevent

hackers.

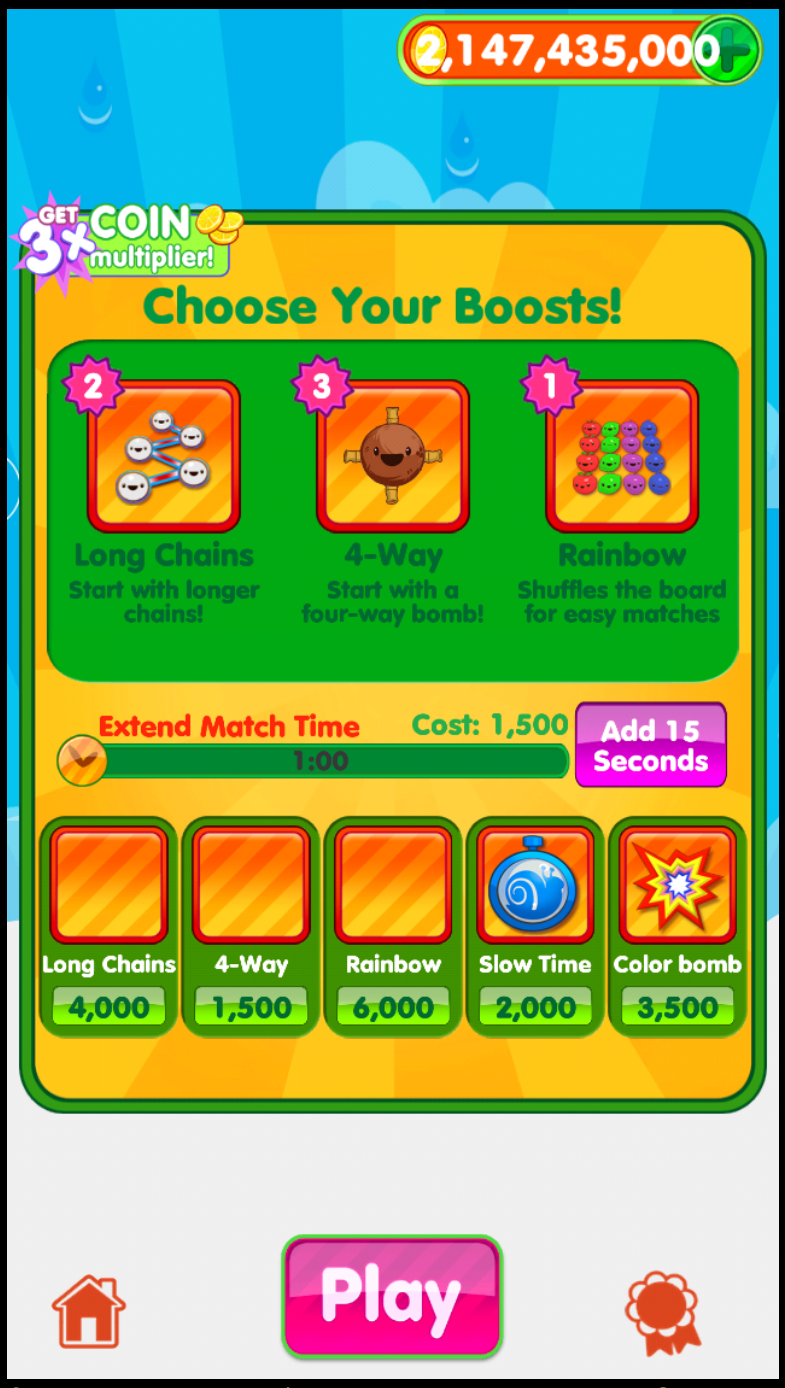
A good skill to learn is being able to find the files with valuable data and the ones without. For example, games with Open Feint have a LOT of files in them with "OF" or "OFF" before them. I don't care WHAT the extension of the file is, its not valuable to you. These aren't actual game files, they are strictly for Open Feint.



(Open Feint files in the game "Defence Line")

So if you know of some files that hold information that could potentially be exploited, make sure to use these methods on that file! I guarantee if you use all my methods on one file and cannot find a way to get into it, that your app is HIGHLY secure and has a low chance of being modified.

Because theres so many examples of ignorant developers out there that don't bother to secure their data in their apps, i wanted to provide another more major example of what could happen if you don't keep simple data from ending up in this .plist file.
For this tutorial, you will need to download the app "Fruit Pop". My friend showed me this simple connect the fruits for points app earlier today and i got bored quickly, so i do what i always do, check the apps security. It didn't end well for the app.



(Fruit Pop app. *Notice my amount of coins at the top right)

Ah, yes. A good, ol' coins hack done simply by editing the .plist file in the library of the app. This is common for the more insecure apps. Not only that, but you can hack your highscore in the game in this file.

(my "highscore")

However, what i did not expect was that the leaderboards of the game would also be run off this data.

(My game center after hacking my score and my coins. *Notice my ranking)

NOTE** When a hacker's goal is to leaderboard hack, typically they will enter the score "2,147,483,647" because it is the highest possible number in a 32bit game. However, some hackers will manage to enter "92233720368547758O7". This number is the highest number in a 64bit game. I am unsure as to how some hackers are able to enter this number, however i think it is done by editing a gamecenter file in

the game and telling the game to enter 64 bit scores.

(an example of a hacked leader board)

Back to Fruit Pop.
This actually may be one of the lowest security games I have EVER seen. Reason being:
1. There was valuable data in the .plist file
2. The data was the same data that syncs to the leader boards

3. The app simply reuploaded the high-score and money every time to the leaderboards! How ridiculous!
The reason this is so ridiculous is TYPICALLY, apps, like extreme road trip 2 (photo above), your only able to find old high scores in the .plist file; but that data isn't what is used to upload to the leaderboards. Most apps upload the players score after the player gets the score in the game, then thats IT. This score is saved on to the game, just so the player can view their score from before; the old score is uploaded and finished. This is to prevent people from editing old high-scores and having them upload. Typically, to hack games that upload the scores once and once only, the hacker must edit the score in the game so that when the level is finished, the modified score is uploaded.
Please don't create an app that has this level of security unless you plan on having a leaderboard where the top 200 people have hacked their score.

3.Mobile Substrate Hacking- Mediocre

Honestly, i had no clue that Mobile Substrate hacking EXISTED until i was making this tutorial and searching around the forum at other tutorials. So i thought i would include it in here, however, since i do not know much about it other than what i have read, i am unable to make a tutorial on it.
Here are four links to other, great tutorials on Mobile Substrate Hacking. Good Luck!

Mobile Substrate and It's Dynamic Libraries
Mobile Substrate Symbol Hooking
Mobile Substrate Code Injection
Extended Tips for MobileSubstrate Hacking

4. Hacking Encrypted Files- Easy/Mediocre

Description: Editing files that are encrypted in games under any extension with file managers
What you Need: file manager, an encrypted file from an app
Ever came across/ made a file that looks like this?:

° O V 9-ã K*»…,.10∏»» XºÑôïùc!ãG? ,dÛËÖ2
,‰ÙËÉ≤9∏yÖDdÂ54µ!|FF® *0 wÅ˜^° O 1
¬ã Ì–]L

p ΔÒfl€üRQáJE•¢RqJE•¢Tá“
E•
•:t8'ääc¢®(o[6Y1léac√ΔÜç
Û≤ÿÿ∞±ac„Çç

Well, I have! I actually took this encrypted code straight out of a file that I ended up making my "The Blockheads Hack" (viewtopic.php?f=3&t=7796) to hack your inventory.
This is the third time I have managed to modify a game involving encrypted code. First you must ask yourself, is this encrypted? Or am i just using the wrong file editor? (for example, try editing a .jpg with the text editor or editing the IDA (file with no extension in an app) with a text editor)
With encrypted files, the cool thing is, sometimes you don't even need to decrypt it! I wouldn't know where to start if I did. Now, the chances of this working for you are slim, but keep it in mind if your trying to modify your app in the future. This is a method I made up that is really simple and most people don't think of.
What your going to want to do is use this method when you find a file that clearly holds A SINGLE piece of data. This file I took the code out of was named "blockhead_111_inventory", therefore I knew that file held the inventory of the blockhead character labeled as "111". This code may also represent a single number.
What you can do in this situation is copy the code, and because you now know for a fact what that code is, you can use that for your advantage. When creating the inventory hack, I realized that the code I had equaled my inventory, right? so all I have to do is go back into the game, store all the things in my inventory, then paste my OLD inventory (by pasting in the encrypted code) over the new one and BOOM. You've duplicated your inventory!
So if you find a file with a number, maybe your number of gold, you can copy that code, spend all your gold, then paste that code back into the file and wallah. Your gold is back.
I also managed to make a hack that got me to the top of the leader boards by taking a very large encrypted number and pasting it in an encrypted number that represented my score on the leader boards. If you ever make a hack like this in someone else’s app, please delete the code and re-sync the file so your score doesn’t stay at the top of the leaderboards as I did for this hack.

5. Hex Editing-Mediocre/Difficult

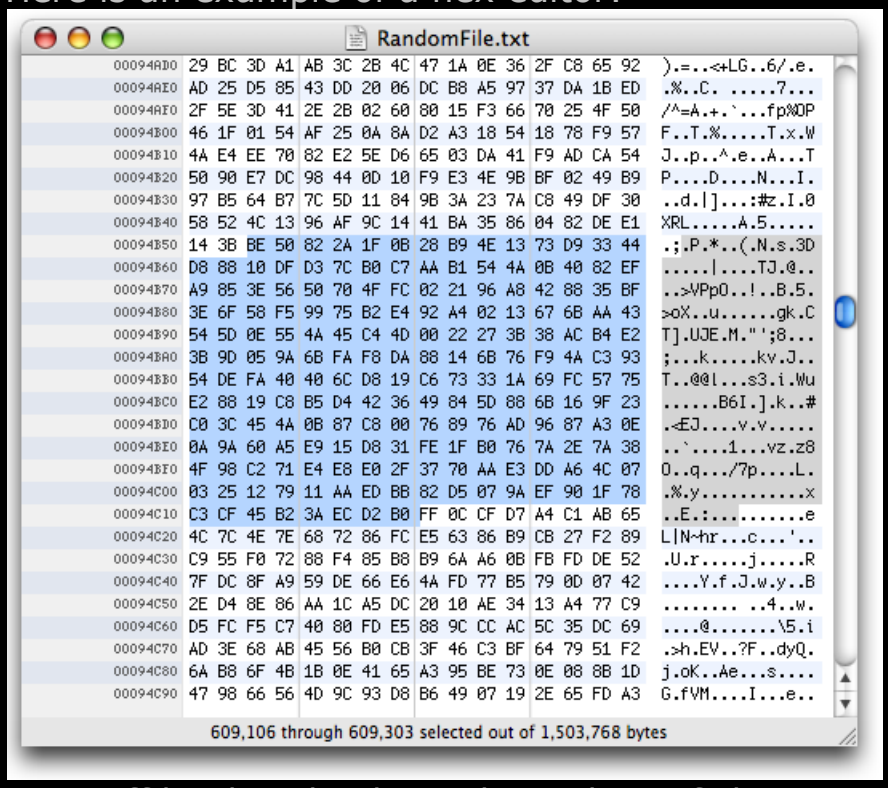
Description: Using a Hex editor to modify files in the game, particularly the files in the documents file within a game (.bin .dat .sav files work best).

What you Need: File manager, good hex editor

I will start this tutorial by admitting that I am NOT very skilled with hex editors. I have only successfully created a couple hacks using hex editors, mainly because I don't try it very often.

A Hex editor is a type of editor for binary files.

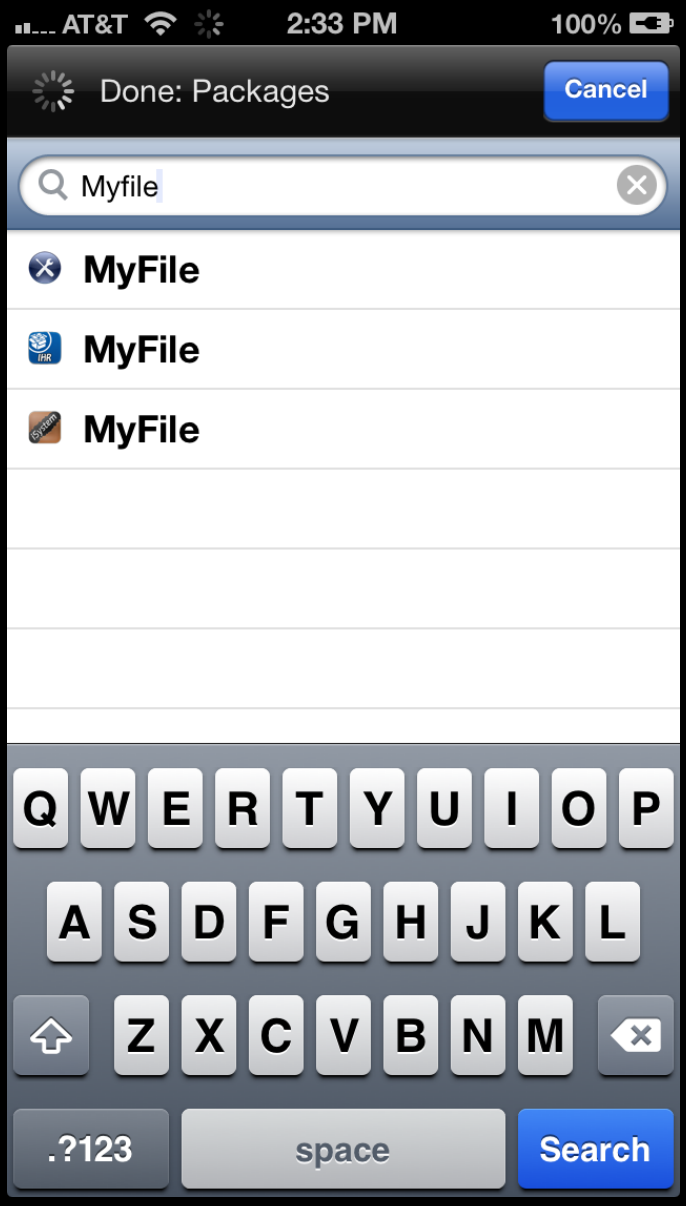
Here is an example of a hex editor:



Start off by downloading a hex editor of choice, or I have one here that I use for my mac: http://ridiculousfish.com/hexfiend/

or, you can even get one right on your jailbroken Idevice! Just search "Myfile" in Cydia. Its on numerous repos, I'm sure you'll find it.

**NOTE-Ifile now supports a hex editor too! Yay!



(Searching "Myfile" in Cydia)

To use Myfile, when you click edit on the file of choice (just like in Ifile), "hex editor" will pop up as an option.
Alright, so now lets talk about HOW a hex editor is used. When using a hex editor, information will come up in two areas. If you refer to the photo above, you can see that there is encrypted information on the right (this info is not always encrypted) and in the middle is series of letters and numbers separated into groups of two. When highlighting something on one side, the hex editor should highlight the translated data on the other side. There is a couple ways to figure out what is going on in hex and figure out where and what to edit to achieve the

happiness of a hacked app;

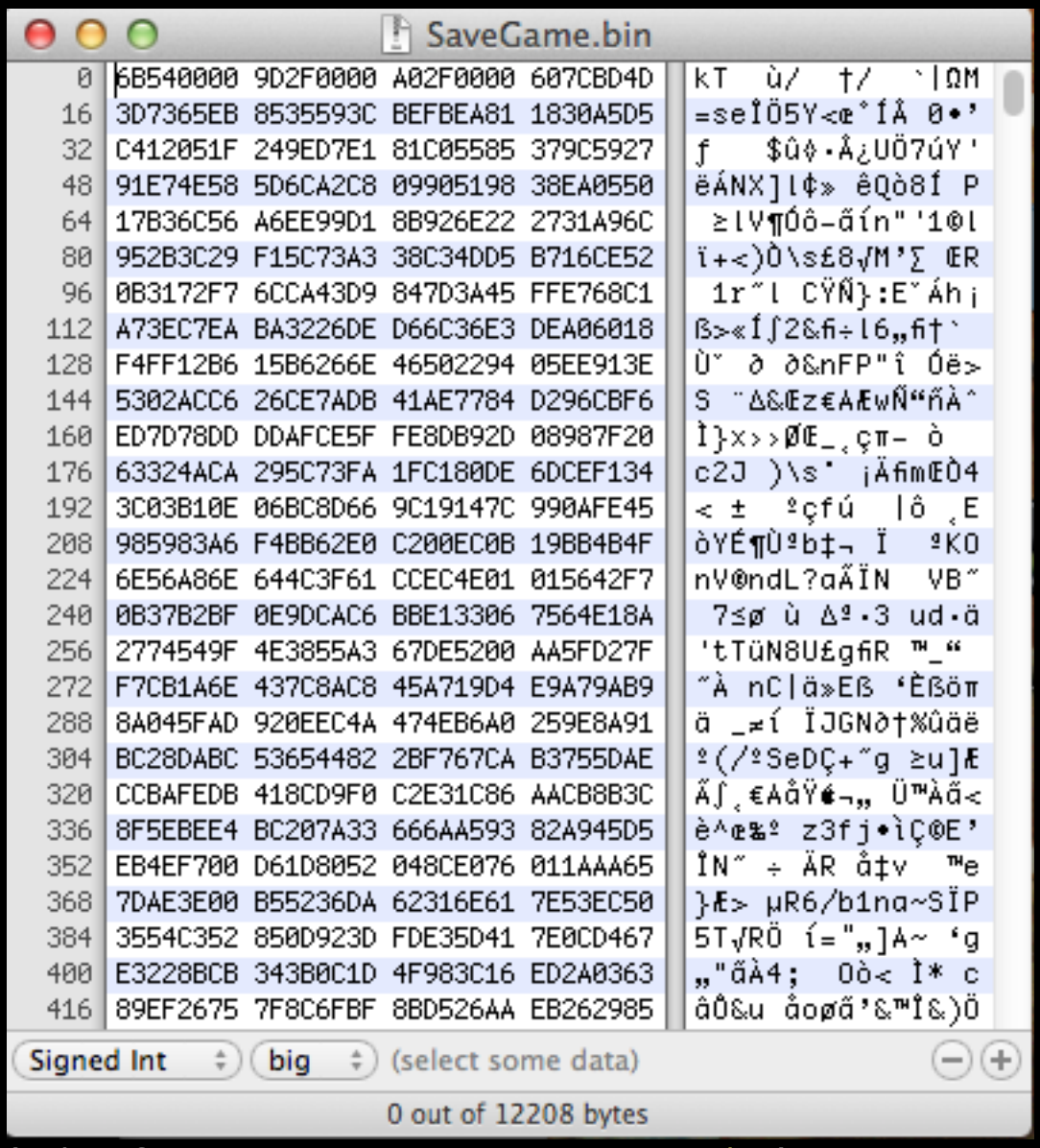
1. Intuitive Method- Easy

2.Additional Programs Method- Difficult

This very helpful tutorial covers one intuitive method of realizing what info means in hex:
http://www.iapphacks.com/post56628.html#p56628
Please read this tutorial, it is very informative and I will assume you have read it in my additional intuitive tutorial.
Here is another tutorial for an intuitive Hex hack that is very commonly done for the app "Minecraft PE"
http://www.minecraftforum.net/topic/1056486-tutorial-hex-editing-on-ios-not-jailbroken/

Intuitive Method-

I will also cover another file I hacked using the "intuitive" method.
First off, in order to use the intuitive method, you have to have some basic knowledge on Hex. If you open up a file that you hope to be able to use the intuitive method on, and it looks like this:



(Taken from MC4, Documents>SaveGame.bin)

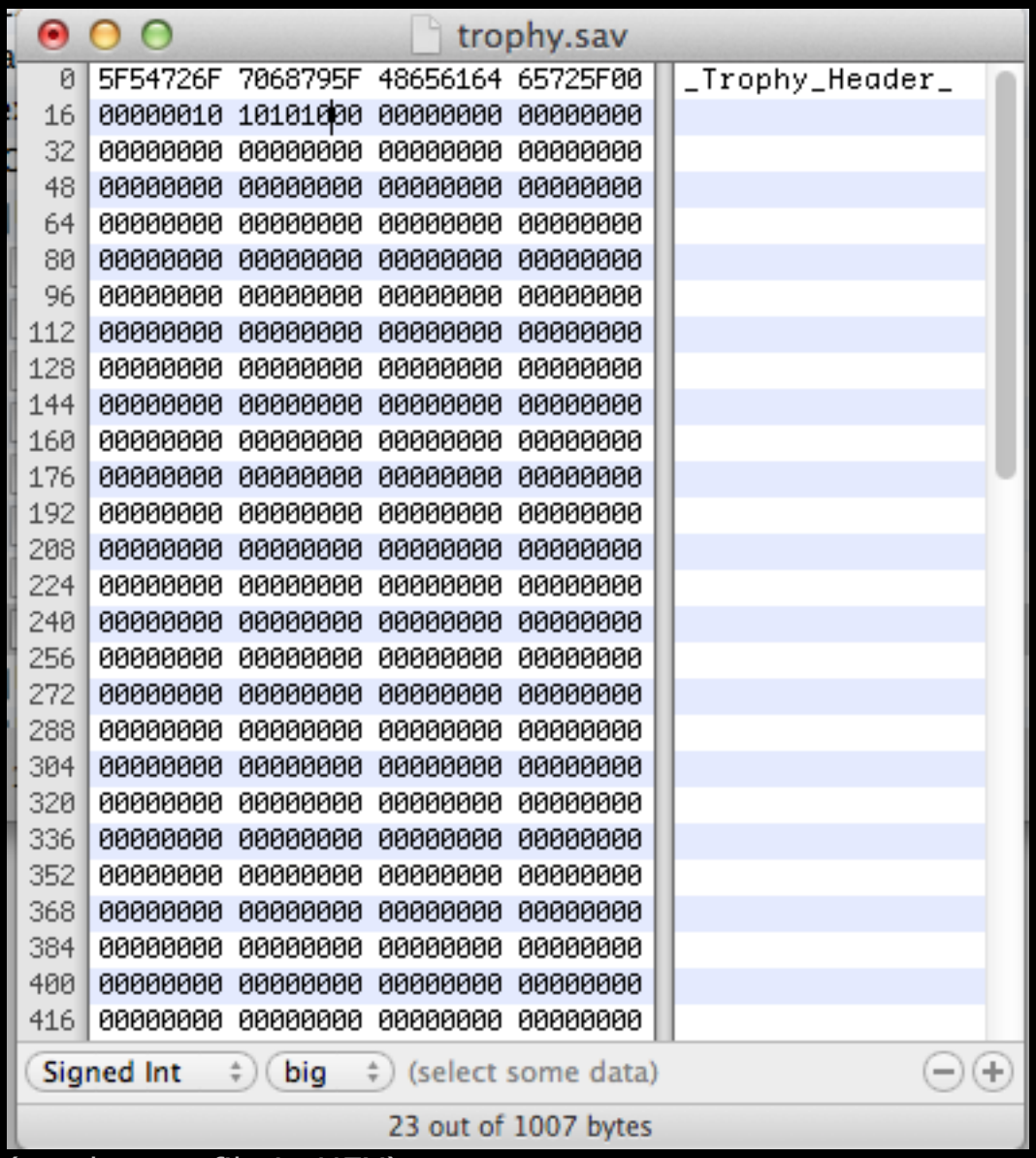
Chances are, you should give up right there on the intuitive method and fall back on another method to hack the file.
A couple common traits of files that are modified via hex edit:
1. a BASIC app is used.
2. The file being edited is very specific.
I used Modern Combat 4 for this example because I KNEW that the game's file would be complex. In the Air Penguin file, the game is BASED around the idea "level one. Three stars, level two, fours stars. etc". what is MC4 based around? Something like: "Current ammo:XXX, Current position in game:XX, YY, angle turned: XXXX, etc.". In other words, it's not going to come out very smoothly in hex and your going

to have no clue whatsoever is going on. Maybe you're a hex genius. If you are, I have no clue why you are reading this tutorial.

This leads me to how I discovered a hack for the trophies on all Gameloft live games. NOTE: This no longer works with newer games I think they figured out how insecure their method of uploading trophies was and patched it, so in this tutorial I will use an older game, N.O.V.A

For this tutorial you will need a very old game with trophies for GameLoft Live. Honestly, I would suggest simply reading this tutorial and not attempting it because I have various outcomes with different apps and it simply is not a reliable hack anymore due to the fact there is a lot of different versions of GameLoft Live and also different versions of the file I'm about to modify.

Lets begin.
Go to your file manager and go to "var>mobile>applications>NOVA>Documents>trophy.sav. Now edit this file in a hex editor. Wallah.

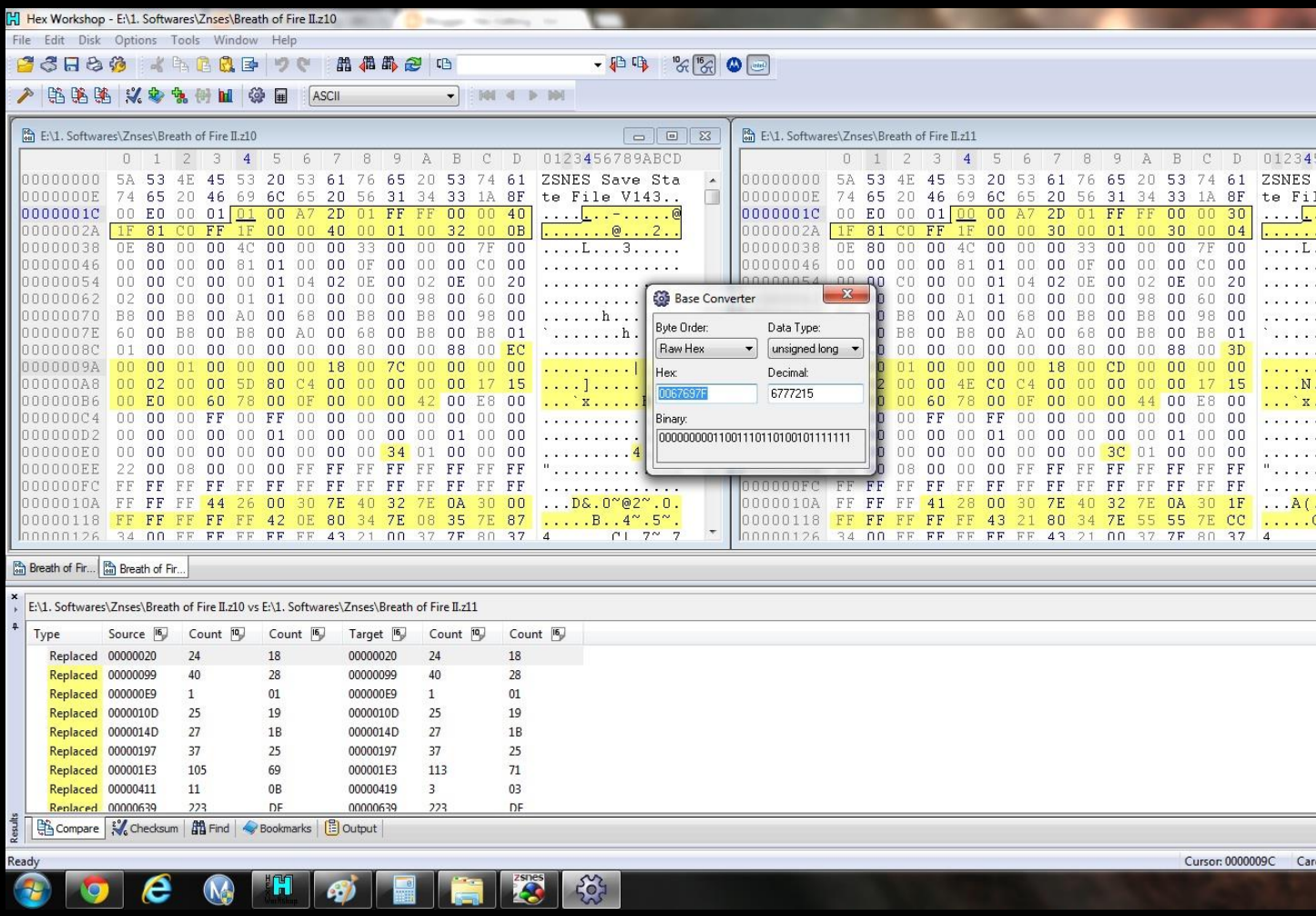


(trophy.sav file in HEX)

This looks confusing to a beginner of hex, but later on you will see the simplicity of this file. So, one thing to note is that i knew that i had four trophies to begin with. See any relation? If you actually read the Air Penguin tutorial like I suggested, well, you PROBABLY will see a relation.
First off, lets notice that
"5F 54 72 6F 70 68 79 5F 48 65 61 64 65 72 5F 00" = "_Trophy_Header_"
This is just another example of how one side is translated into the other side, this time, however, not encrypted.
Alright, lets get down and dirty here. So whats the relation? Hmmm....

"00 00 00 10 10 10 10 00 00 00 00 00 00 00 00 00" Well, how many trophies did I have? Four. How many "1"s are there? Four. Last time I checked the stupidest property in math, the Reflexive Property, 4=4. So all i have to do is change the hex from above so that it gives me 14 trophies (the total amount of trophies for NOVA). It should look like this:
"00 00 00 10 10 10 10 10 10 10 10 10 10 10 10 10"
Now just save and overwrite the file into your game with a file manager. Boom.

Basically to intuitively mod a file with hex, you want to use your pattern recognition skills along with a lot of common sense and puzzle-piecing skills. If your file your editing is “PlayerInventory”, and you know in your inventory you have 6 grenades, 12 bullets and a handgun, look up what “6” and “12” are in hex with this link:
http://easycalculation.com/decimal-converter.php
Turns out that 6=6 in Hex and 12=c in Hex. So now you want to search around your file until you find those numbers/letters and see if you can pin-point exactly what you want to edit, then change it to a higher value. Boom. This is also where the simplicity of a file benefits a hacker to coming to the conclusion of what is what in Hex. If this file looked like the MC4 one, and i held 6 grenades and 12 bullets in my inventory, who knows where I would find these values?? Well, we can always use the "find" function in the "edit" tab. However, then we come across a LOT of "c"s and it is going to be hard to determine which is which. As always, theres a way around this. Some Hex editors have the ability to compare two Hex files. What a hacker would do is save a save file from one point in the game, lets say they had 4440 gold in this save game, then buy or sell something so the money value changes, lets say 4440 drops to 4230, then save this save file. Now the the hacker can search for both 4440 and 4230 (converted into hex) in hex fiend, then view all that is highlighted in the file until they come across 4440 on one side and 4230 on the other (converted into hex, of course). These will be the values your looking for.



(Two Hex files being compared in Hex Workshop)

Unfortunately, i do not think that HexFiend has the ability to compare two files.

Additional Programs-

The second method to using hex involves using additional programs with hex. This will be explained more in depth later in the tutorial, however, for now, I will provide a quick summary.
A hacker can use another program, typically IDA Pro, to determine certain values/commands in the file and then use the HEX editor to change them.
For example, in IDA Pro, a hacker could come across a command that sends information to tell the character to lose health when a bullet collides with the character. They could then determine what a code translated into hex is that basically says "do nothing" and implant this code into the hex of the file in order to change it.

Once again, this will all be described more in-depth later on in the IDA hacking method.

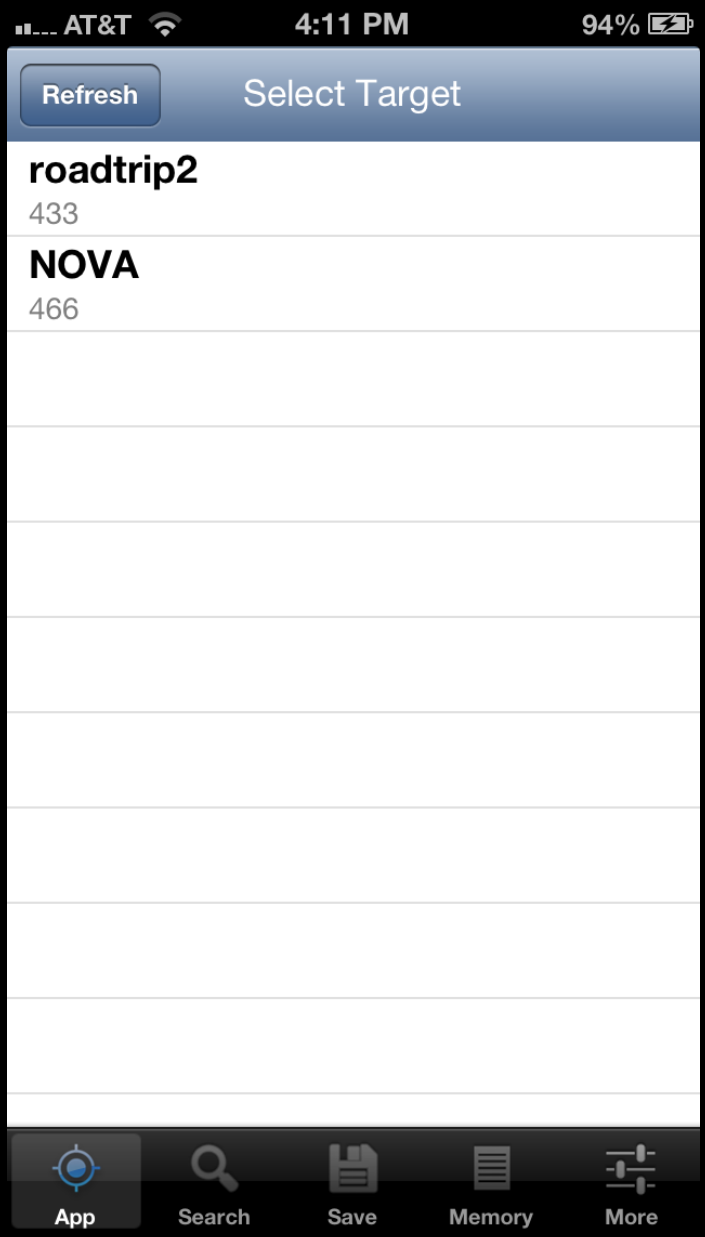
6. Universal Hacking Programs- Easy/Mediocre

Description: Using programs made by others that were created to help simplify hacking apps and to work on the largest amount of apps possible.

This method is merely a simple way to hack many apps that takes very little time, however it only works for certain apps.
Three programs that can be installed to simplify hacking are:

1. Igameguardian
2. IAP cracker
3. Flex

These three programs are all examples of software that you can download to simplify hacking, however I'm sure that there are more out there.
Lets take a look at how these programs are obtained and how they work.

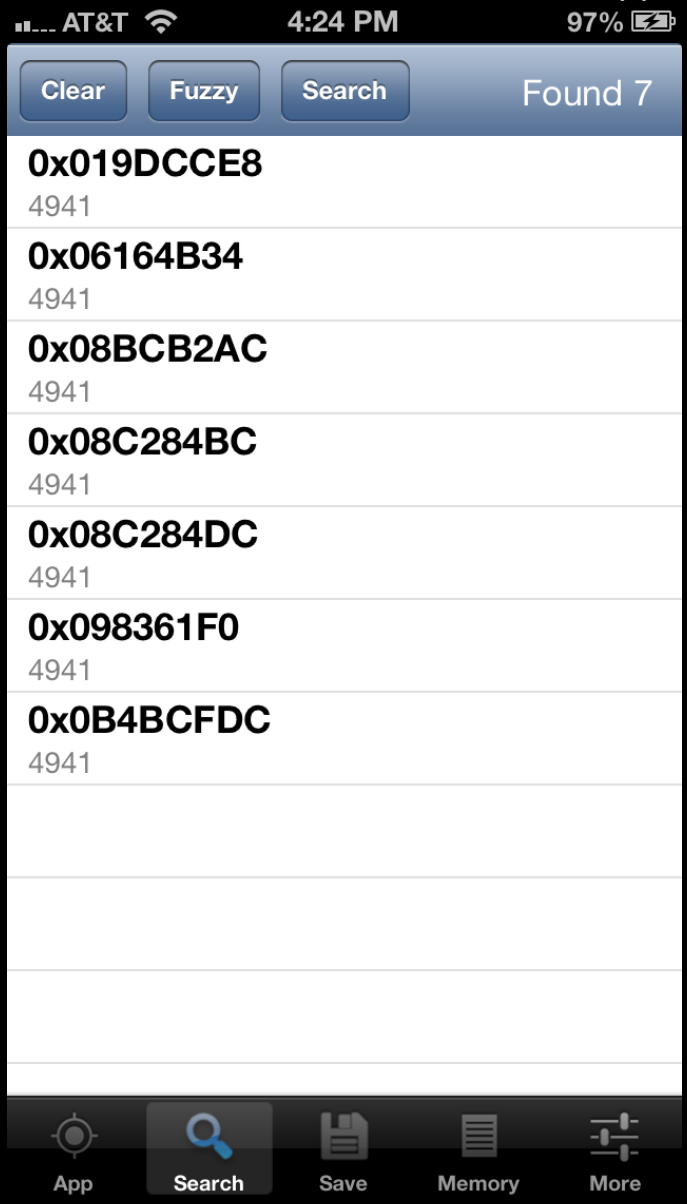


(IGameGuardian screenshot)

1. This is Igameguardian. What does it do? Well, its made to modify any number value in an app. It does this by basically what we did in the Hex tutorial; it searches for a given number in all the files of the game, if it finds them, they appear on a list of numbers. You can then modify these values in Igameguardian, all right on your jailbroken device.

To get Igameguardian, go to Cydia, make sure you've added the repo "http://ihacksrepo.com/", then search for the Program in the search

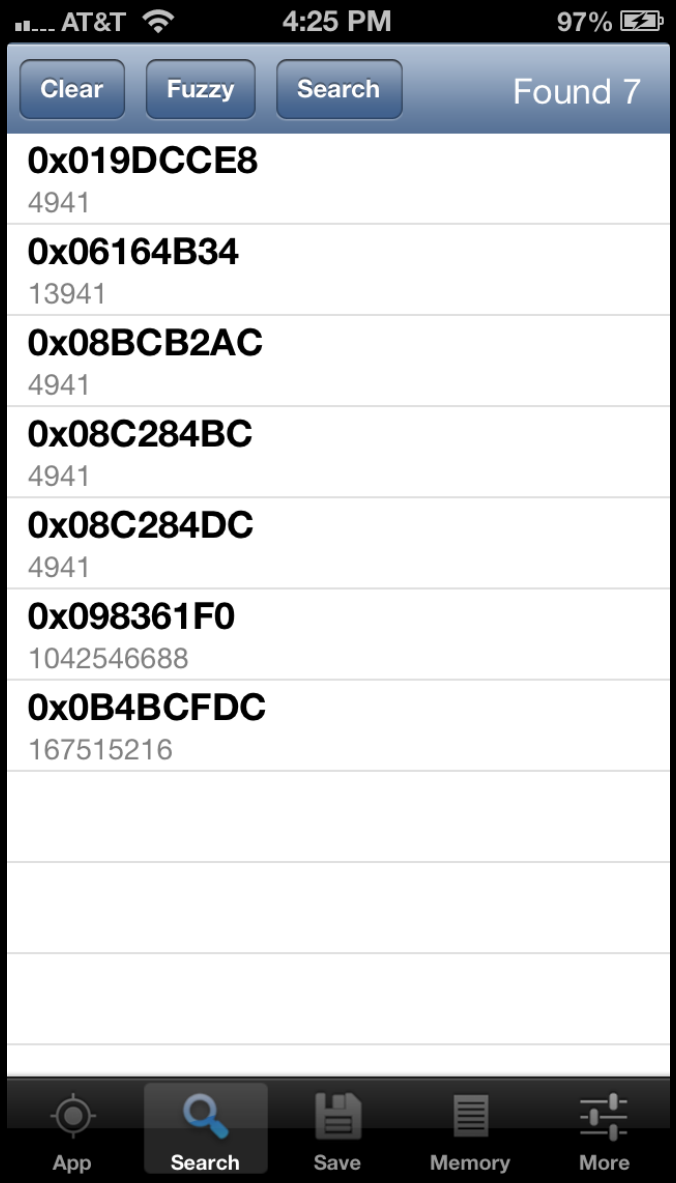
bar. Download. Install.
Lets take the app Extreme Road Trip 2 for example. In ERT2, i have 4941 gold. Open up ERT2, then open up igameguardian. Now click on roadtrip2 as shown in the previous image. Go to search, search for "4941" and wait for the values to appear.



(searching for 4941 in Igameguardian)

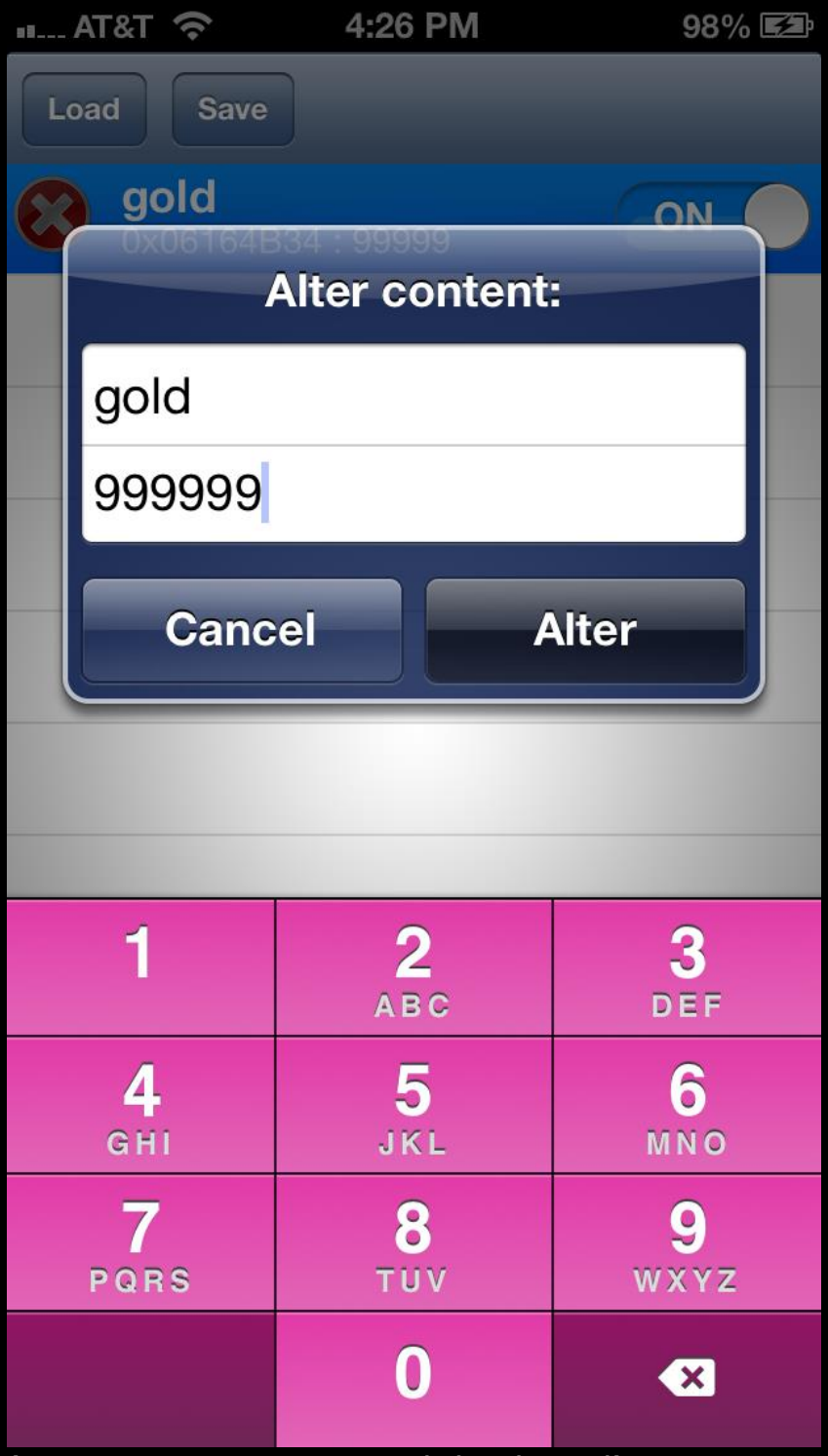
Alright. Now that these values have appeared, we need to determine which of these numbers is the number of gold. Don't go changing them all, this could cause a potential crash because you may edit vital information for the app to run. So all we have to do is change the amount of gold in the game, then come back to Igameguardian and

see which one changed to our number.
I went ahead and went into ERT2 and bought 9,000 gold (you can do anything you want, as long as the amount of gold increases or decreases).
so now we go into Igameguardian and search for out new number, 13941.



(searching for 13941 in Igameguardian)

Well look at that! See which one changed? Now click on the value, click "save", then go to saves, turn on the save, then edit the value.

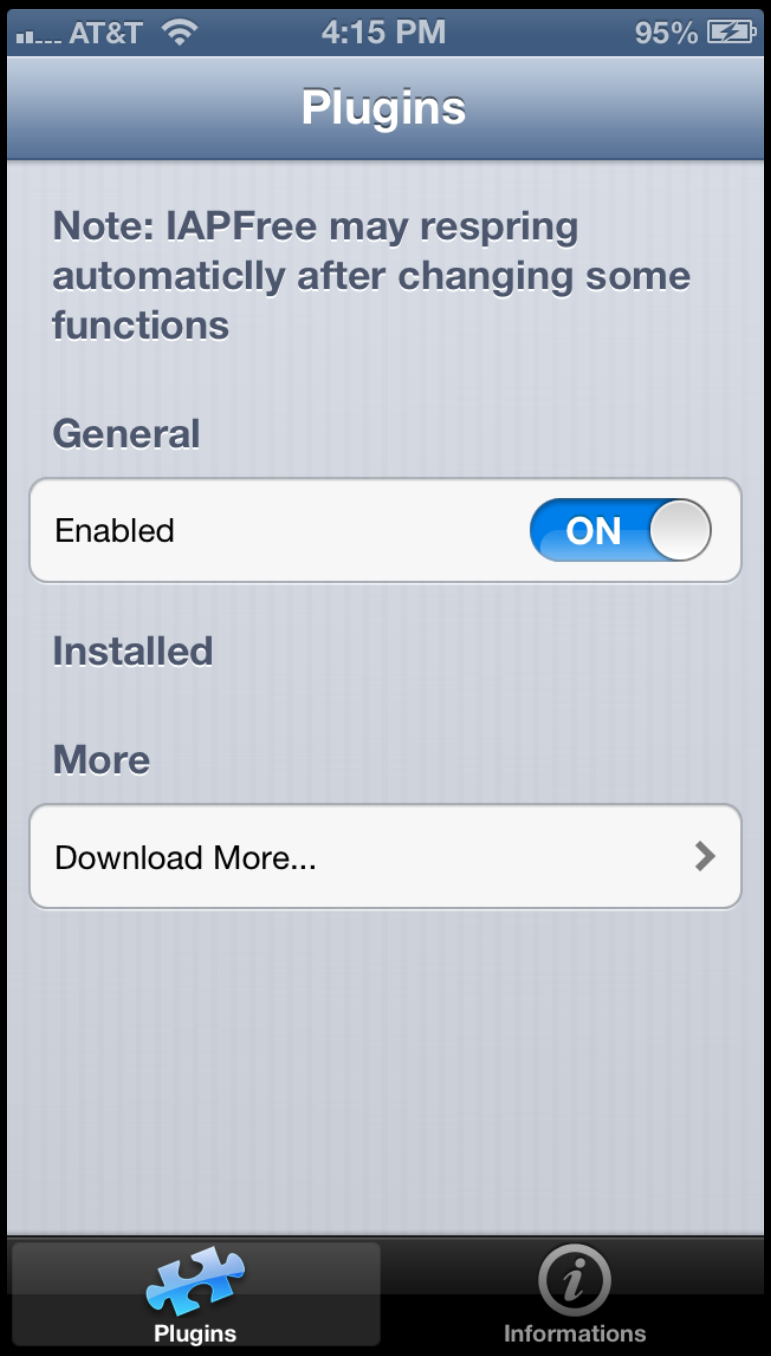


(inspecting my sexy, pink keyboard)

However i successfully found the value of gold in the game and edited it to a larger number, this doesn't mean it will work. I went back into the game and my gold did NOT change. So if your testing this on your

own app and it your able to find vital information in igameguardian, no big deal, as long as the value doesn't actually change. This will prevent many hackers since igameguardian is very popular to petty hackers who only know very basic methods to hacking like this.

Also, be ware that igameguardian is a common way (ok, well, its MY way) of hacking apps that submit their score to the leaderboards at the end of the level, game, world, etc. For example, the app "Line Surfer" submits its score after you fail at staying on top of your surf board, which ends the game. In order to hack this app so that you can achieve a maximum score of 2,147,483,647, you have to edit your score BEFORE it uploads to the leaderboards. Igameguardian is actually the ONLY way i know to hack your score like this, because it enables you to pause the game and edit your score. All you must do is pause the game, search for your distance traveled on Igameguardian, open the game again, go a few more feet, search the number again, determining which number is your distance traveled, then edit it to whatever number you would like. Now go back to the game, travel a bit further and you will notice your score change to whatever you entered. Boom. Now die and it will submit your score.
Aha!
I have successfully hacked many leader boards with this method. This works for many other apps, even temple run 2 (you would THINK that maybe they would have higher security than this, especially with the amount of money they made off their first game), which is funny because they stated
"Our goal is to build something that lasts for the long term."-
Developer of Imangi Studios.
It's hard to keep a game going "for the long term" when at least 100 people on each of your leader boards have hacked themselves to the top!



(IAPfree's home screen)

2. This is IAP Free.

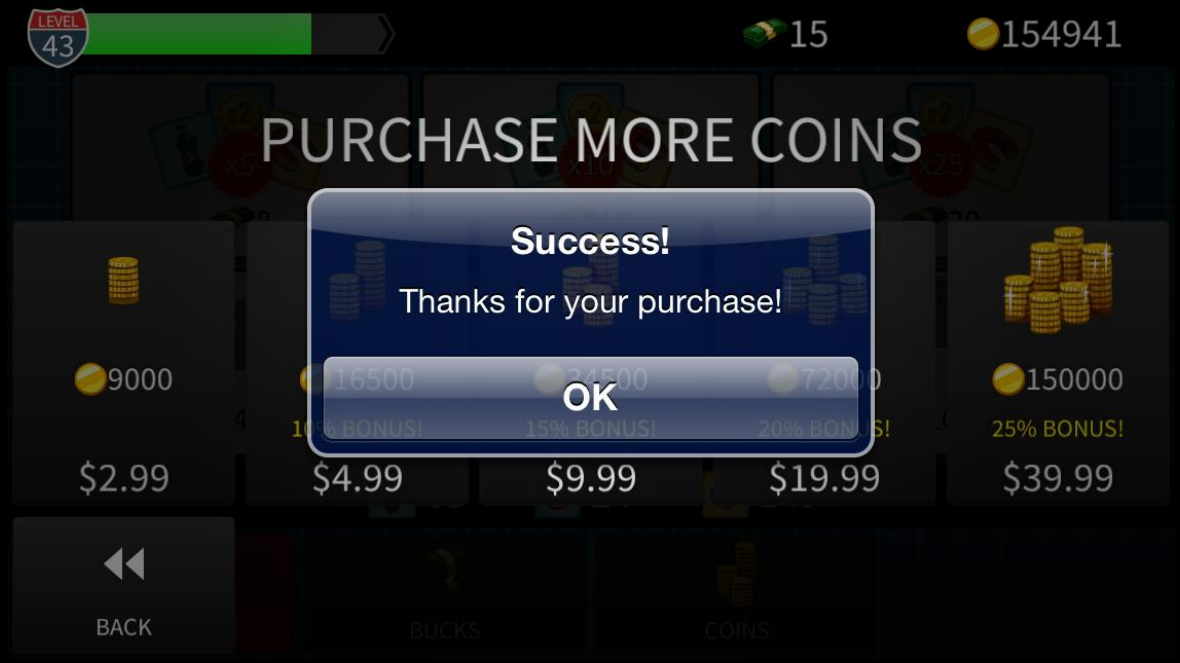
What does it do? Well, lets look at the name: I.A.P= In App Purchase free. So it "cracks" in app purchases. It steals them. Makes them Free.

Lets take a look at how to get IAP free.
Go to Cydia. add the repo "http://cydia.myrepospace.com/Alex793/"

once installed, Search "IAPFree (no space) core plugin 1 .9. 1". It should come up. Install it. Respring.
Now, we don't actually get an app on your home screen like i have, i provided this relatively unknown iap free plugin because it requires no effort and it works like all the others. If you would like the app that is in the photo above, search "IAPFree" in Cydia. It should come up, if not, add "http://ihacksrepo.com/". There is also "IAP Cracker" that does the same thing, however, the one i suggested you download is the only one i've gotten to work.

Alright, you have now installed iapfree. Go to an app and try buying an in-app-purchase. NOTE** if it prompts you for your apple password, IT DID NOT WORK. With IAPFree, no app will EVER ask you for your password when getting an IAP. If it prompts you, please try reinstalling IAPFree plugin. This does not work for ALL in app purchases, only ones that are not server sided. So if you have in-app-purchases in your game that simply give you more of an item and doesn't check online or refer back to anything else, chances are, this will work on your app. However, some apps have either purposely found a way around this, or their app simply does not work with IAPFree. For example, Fruit Pop doesn't work with iapfree, zombie road trip, Vector, Mad Skills BMX, and Line Runner 2. Ive actually came across MANY apps that this does not work with, simply because when you go to click on "purchase", it will just forever load, give an error, or can't connect to the Itunes store.
However, some apps are not so lucky. I like to use "Extreme Road Trip 2" as an example. So far it has passed all of the tests for a relatively secure app, however, it is about to fail.

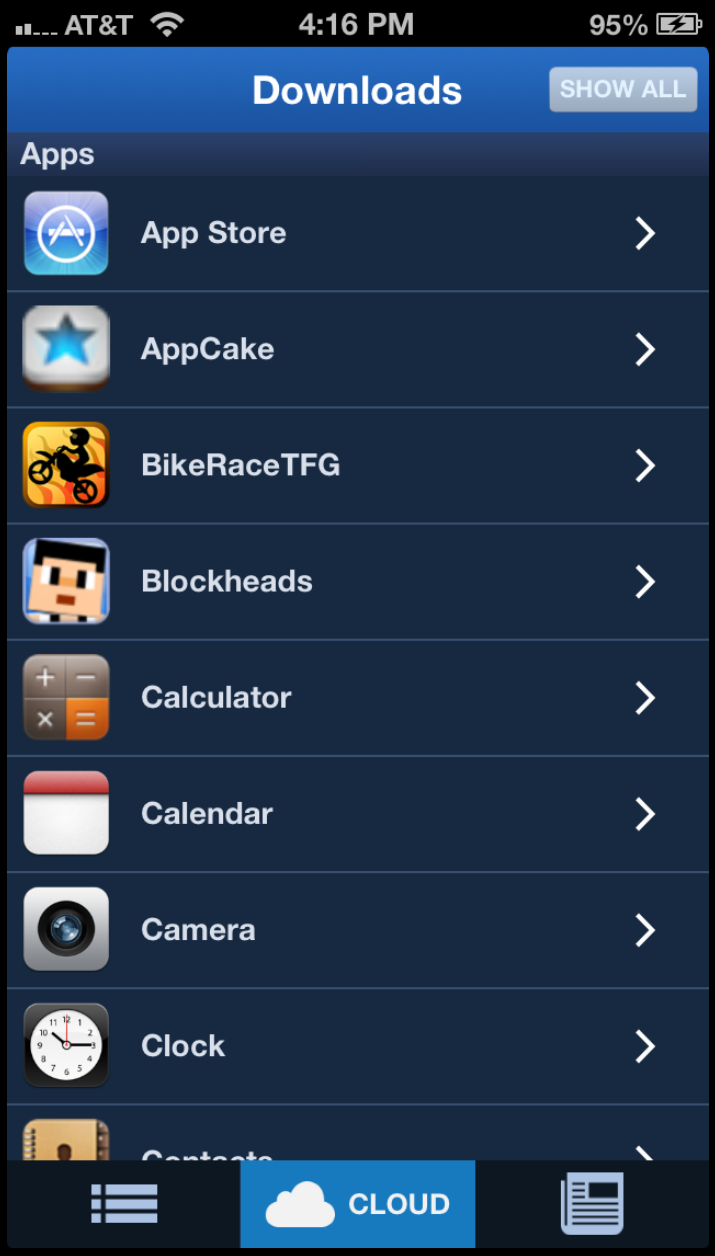
(ERT2 menu to buy in-game gold)



(ERT2 getting tricked by IAPfree)

Boom. After clicking, it simply gives me the gold.
You'll notice, however, that after leaving the app, deleting it from backgrounding, and reopening it, your gold is actually gone. Maybe it has something to detect a sudden surplus in gold, or a false value of gold, or its simple IAPFree failing on the job! I don't know, but once

again, ERT2 has partially succeeded the hack test.
IAPfree DOES work on MANY apps, including but not limited to: Lazors, Hill Climb Racer, and Bike Race.

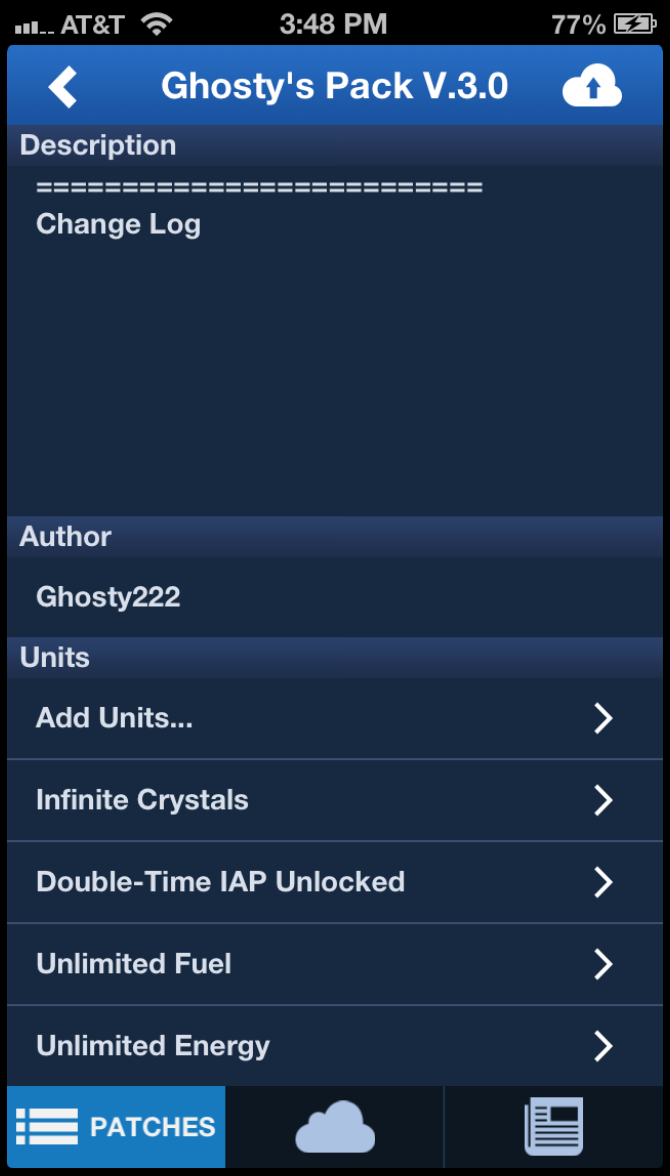


FLEX's homescreen

3.This is FLEX

FLEX is a very creative, new way you can tweak almost any software on your device (you can even modify FLEX itself in FLEX)
FLEX allows you to modify all the executable files inside an app, test out your tweaks, AND install other people's FLEX tweaks right on to

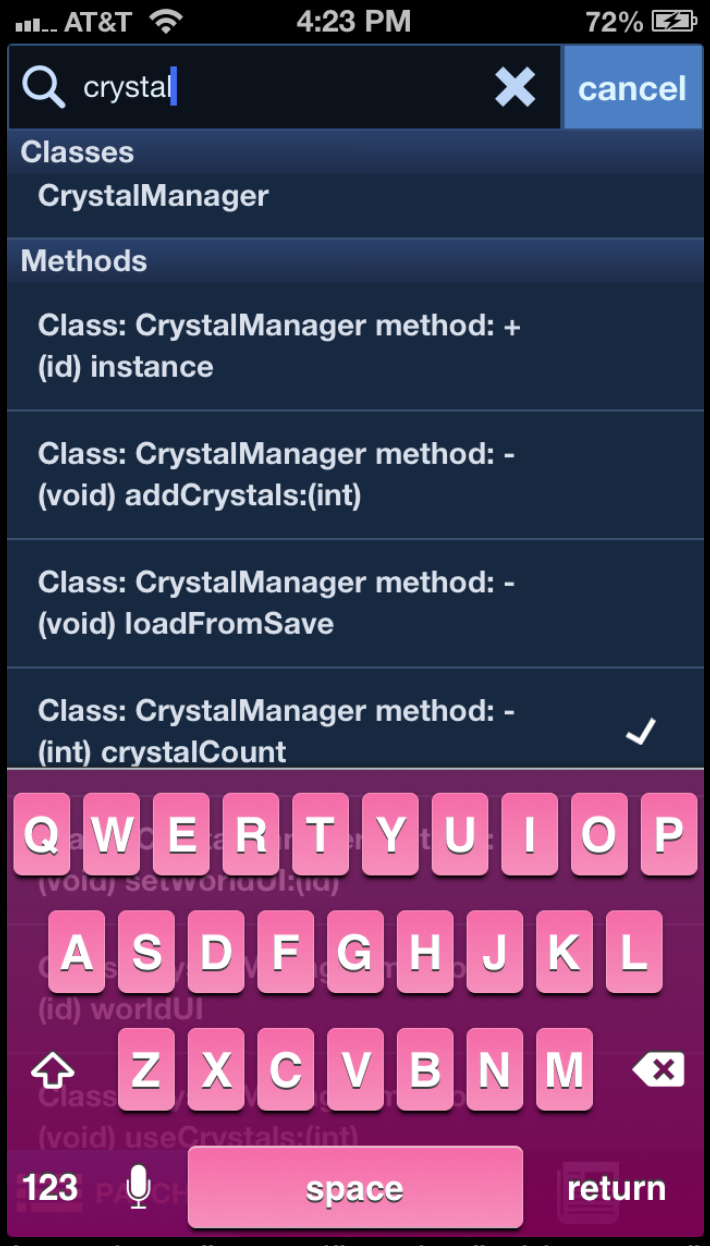
your device (by FAR the EASIEST way to get hacks for games and VERY easy to use)
Lets go over how to install "FLEX".
Go to Cydia, search for "FLEX" in the search bar, it should pop up. If you want the REAL FLEX, with the ability to download other people's tweaks, you MUST purchase FLEX for $3.99. There simply is no way around this. Please contribute to the development of FLEX by purchasing it, it is a very well-made app and it is worth a simple $4.
If your just looking to use FLEX to make your own hacks and for the purpose of this tutorial, you can download flex from "http://www.sinfuliphonerepo.com", however, be cautious that this technically is stealing FLEX, and could be considered illegal.
Now that we have FLEX, lets discuss how it works and how to work it.
If you would like to tweak a game with FLEX, you have to think creatively sometimes. You can't always just find a value of gold, or a value of coins and change it.
Go to Patches, click "+" at the top right, then choose the app you would like to edit. For the purpose of the tutorial, i will use the app "The Blockheads".
Once you have selected the app, click "Add Units..."



(Ghosty's Pack V.3.0 on FLEX)

I am using someone else's tweak, Ghosty's patch, for my example, thats why there are already-added units.
Now click "Blockheads", or whatever the file is that your editing; basically click on the first executable that is displayed.
Once in this file, your going to want to think up some good key-words for your game. If your game uses gold, search "gold", if it has a car that can go up to 30mph, search "speed", or maybe its a Mario-like game where you jump a lot, so search "jump". Basically anything that would be beneficial to change. Some good key-words to search are: Gold, coins, crystals, jump, speed, unlocked, locked, rotation, gravity.
After searching "crystal", you should have something that looks like

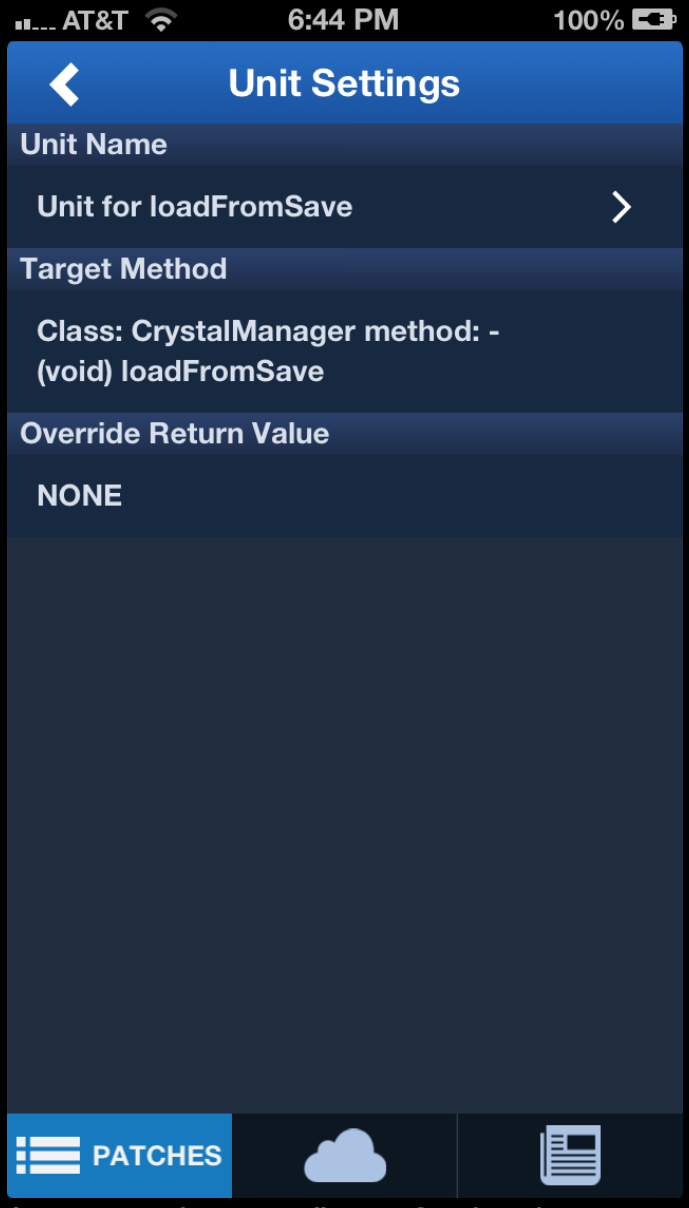
this: (without the pink key-board)



(searching "crystal" in the "add units..." search bar)

The units displayed are potentially valuable data. They are basically the commands of the game. When you tap on the unit, it will add that unit to your list of units back on the screen where you pressed "add Units...".
Figuring out which file to select comes with time and practice, however, there are simple rules you can stick to to help you pick. Typically, "(int)" and "(float)" units have number values, "(BOOL)"s are true/false statements, and units that have "set" in them, are

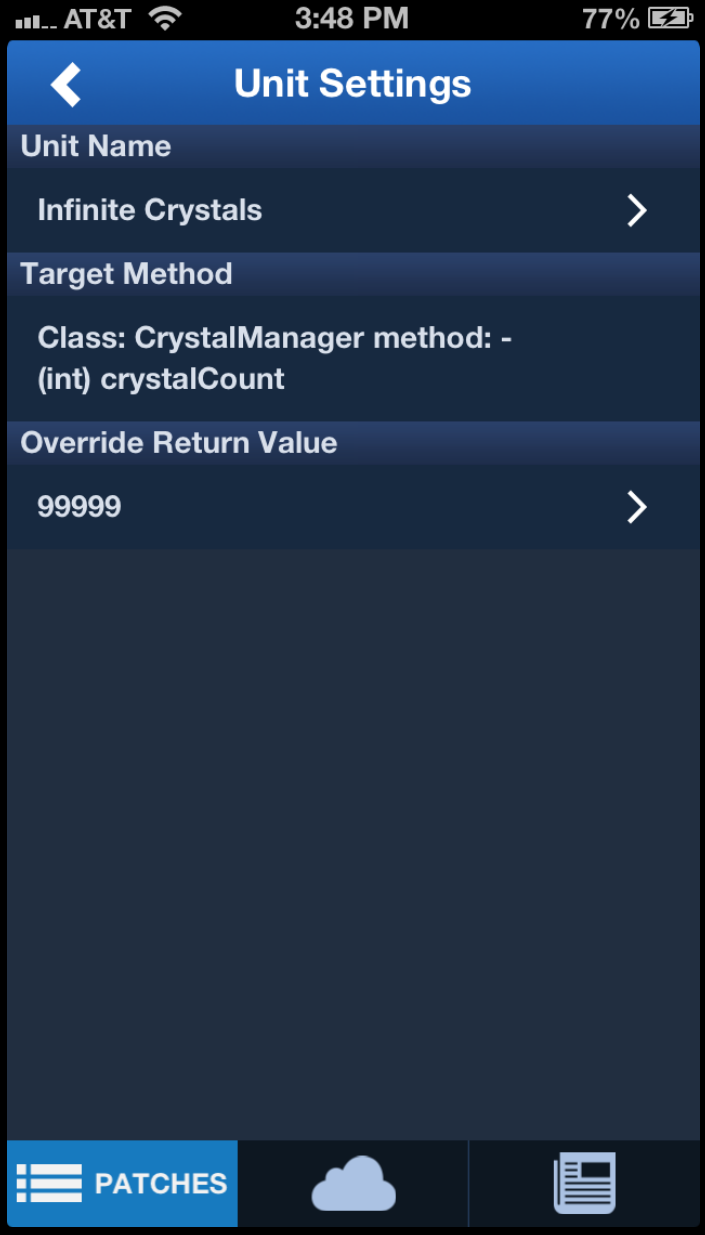
useless units (typically you will find two units where the only difference is the word "set", for example, "Class: Bumper method: -(float) speedX" and "Class: Bumper method: -(float) setSpeedX". The unit with "set" in it is useless, ignore it)
So, its hard to say exactly which units you want to edit, so just add a bunch. If you aren't sure of what it will do, add it and then try it out later. Once you are ready to try to tweak the added units, click the back arrow. Now scroll down and all your added units should be there. Click on them all individually to view their potential.



(viewing the unit "Unit for loadFromSave)

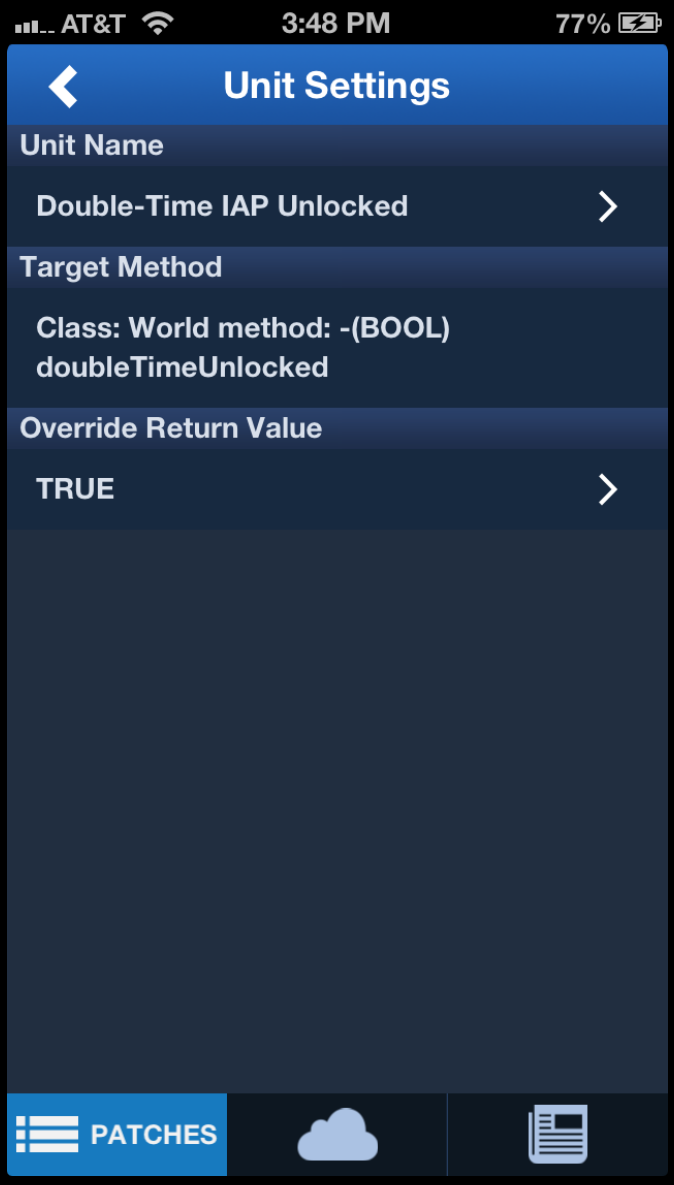
What you want to look at is the "Override Return Value" section. If it

says "NONE" or "NULL", simply exit out of the unit, then delete it. Its useless for FLEX.
However, if it displays a number value, you can change it.



(editing the crystalCount unit)

Sometimes, changing a file from "FALSE" to "TRUE" can be all it takes for a very helpful hack:



(editing the doubleTimeUnlocked unit)

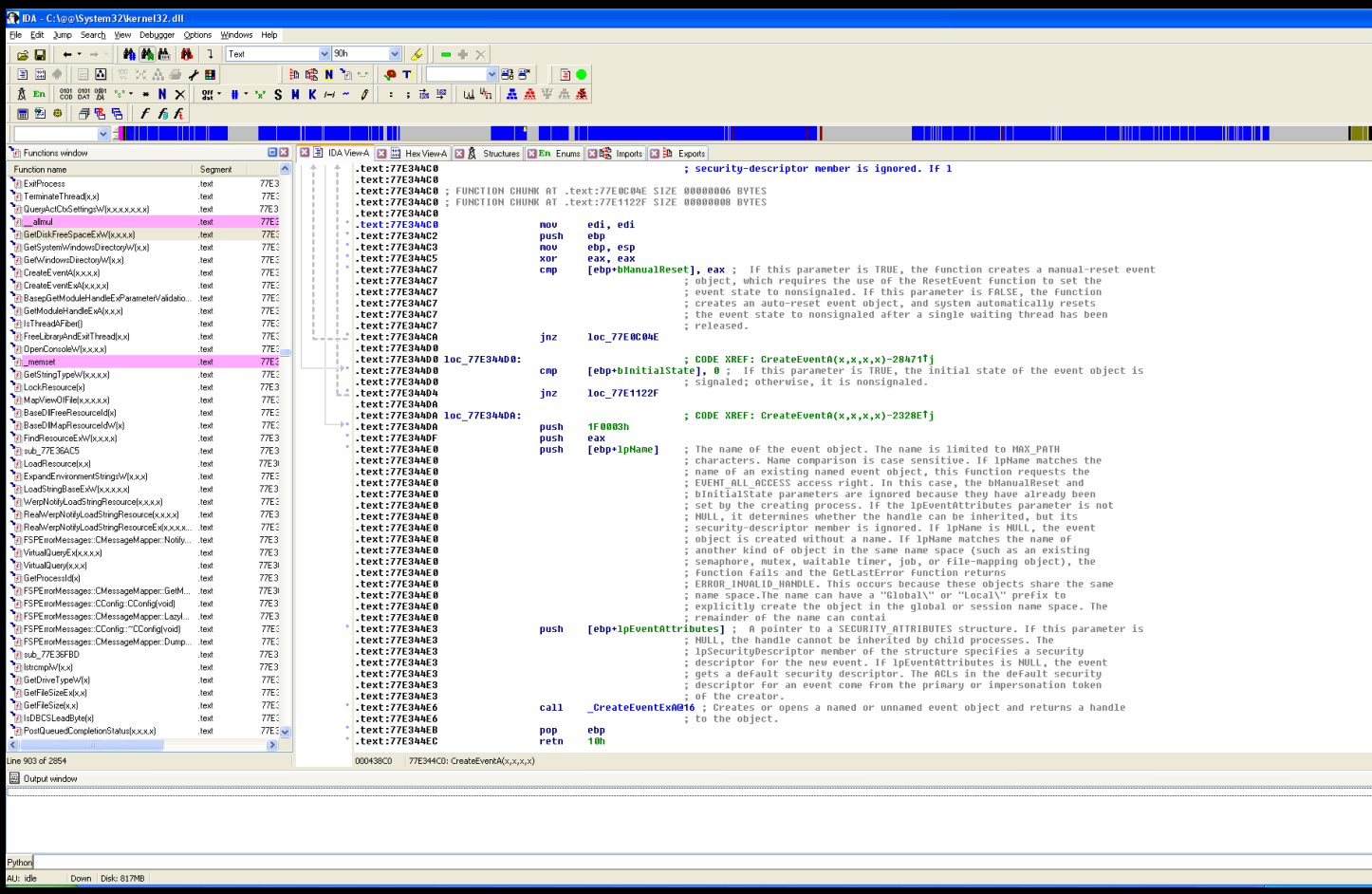
(the double-time feature in The Blockheads app is an in-app-purchase that speeds up the worker in-game) This is why its always super helpful to search for "unlocked" and "locked" as key-words in FLEX; they are always true and false statements and they are in many apps. Not all apps are as easy, however. Many times, you'll find strangely named units that dont entirely make sense. Typically, if i find any unit that i can edit and it has a good keyword in the name, i will change it whether or not i have any clue what it will do. I, then, run the patch, delete the game from backgrounding, and play the game. Now test the game and see if anything changed about it. If not, its back to square one. If something does change, then go back to FLEX and see if you

can't work the tweaks to your advantage.

There is lots left to be said about FLEX, however i feel like ive spent enough of this tutorial on it. If your looking for more help on FLEX, check out these two tutorials made by the developers of FLEX:
http://tweaktuesday.com/flex/docs/?page=patchMessages
http://tweaktuesday.com/flex/docs/?page=tutTinyTower

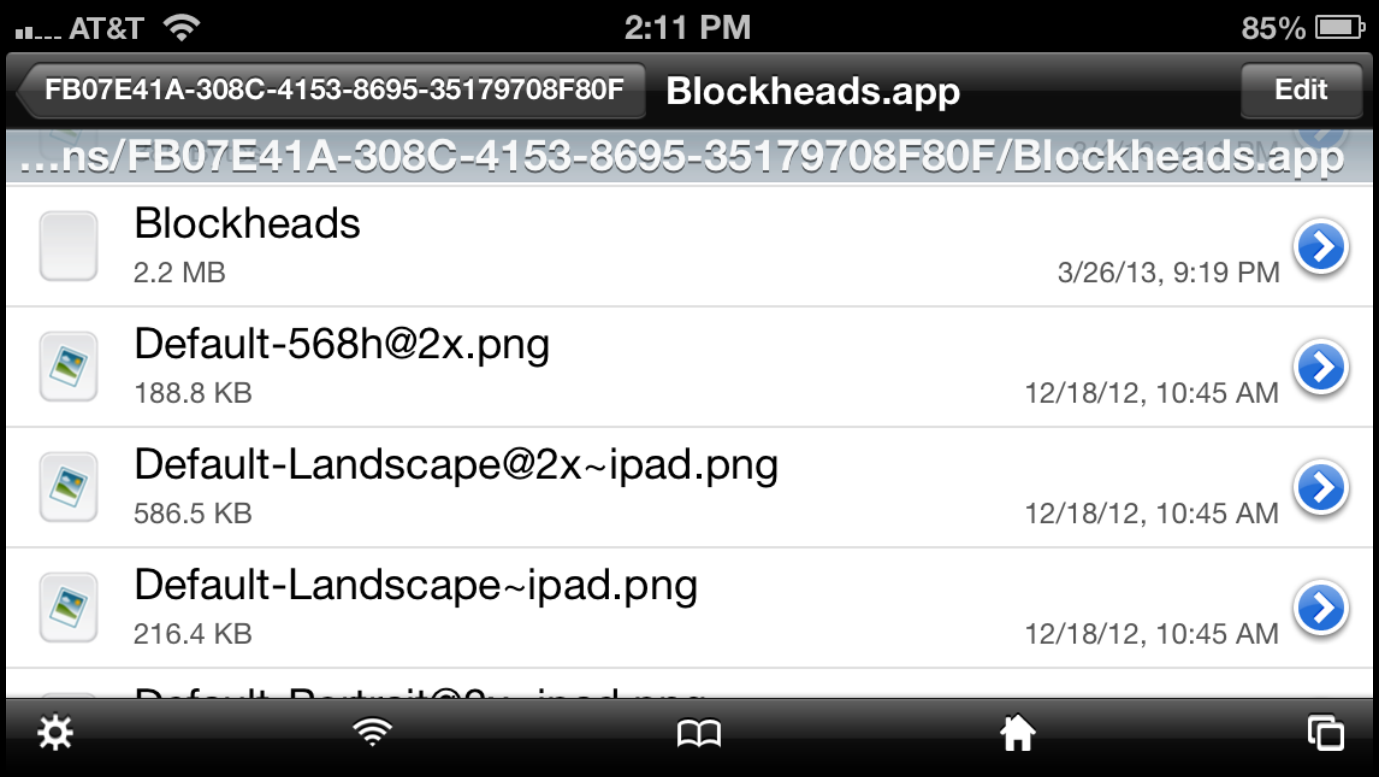
7. IDA editing- Difficult

Description: Editing IDA files with IDA editor pro (the file in the app without an extension)
What you Need: IDA Pro, ARM/ASM Converter, File manager, Clutch/Rasticrac, Mobile Terminal, SSH, GNU Debugger 1821-2, GNU Debugger 1708
IDA editing is not easy, and I am NOT an expert on it. IDA editing involves taking the IDA file from the app your looking to hack, transferring it onto your computer, debugging/decrypting/decompiling the file, editing it using IDA editor pro, then recompiling it. Typically, a HEX editor is also used to edit the IDA file.



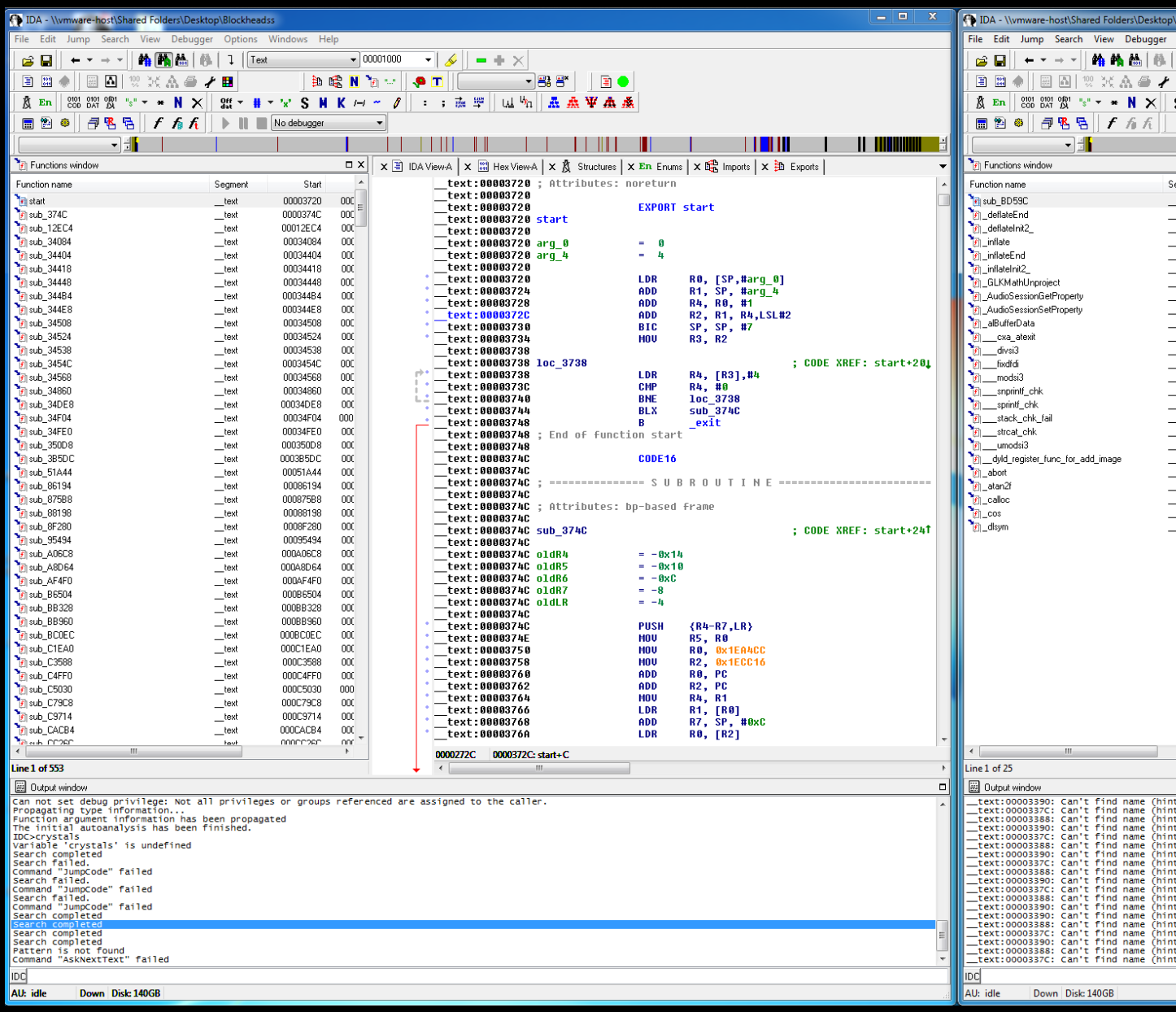
(IDA Pro editing a file)

Time to get IDA Pro.
IDA Pro is not free, nor cheap; however, you can download the demo version which has all the functions you will need right on your Mac, Lunix, or Windows computer at: https://www.hex-rays.com/products/ida/support/download_demo.shtml
There are other alternatives to getting the full IDA pro, however, these are highly illegal and are as serious of a crime as shoplifting in your local market; I would NOT suggest taking the torrent route to getting IDA Pro.
First lets start by showing you where to locate your IDA file.
Go to "Var>mobile>AppYouWantToHack>AppYouWantToHack.app>AppYouWantToHack (the app you want to hack's IDA should be named the exact same thing as the app and have NO extension. Typically it is also a very large file).



(viewing The Blockhead's IDA in Ifile)

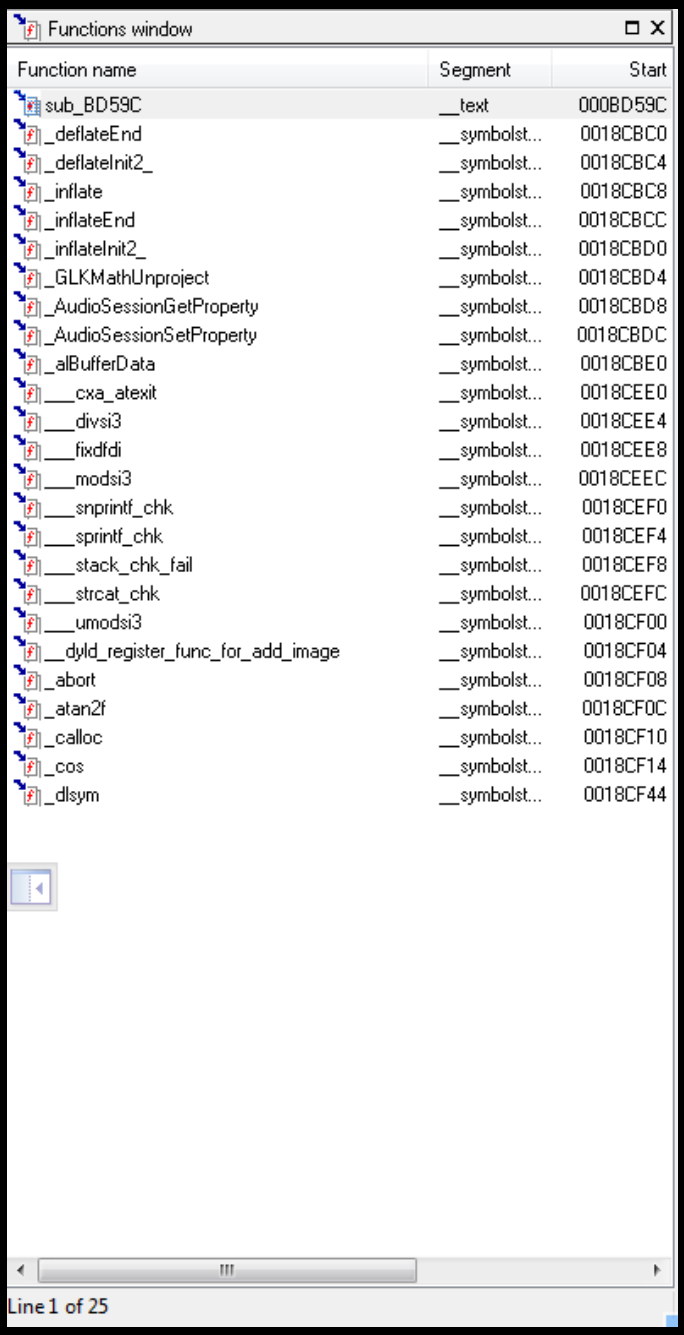
This is the file that holds all of the app's commands. All of the core code, basically. Heres the issue: When you put this file into IDA pro, as is, the code is going to be EXTREMELY confusing because, well, its encrypted/compiled.
Lets take a look at a file in IDA pro that is encrypted/compiled compared to one that is not:

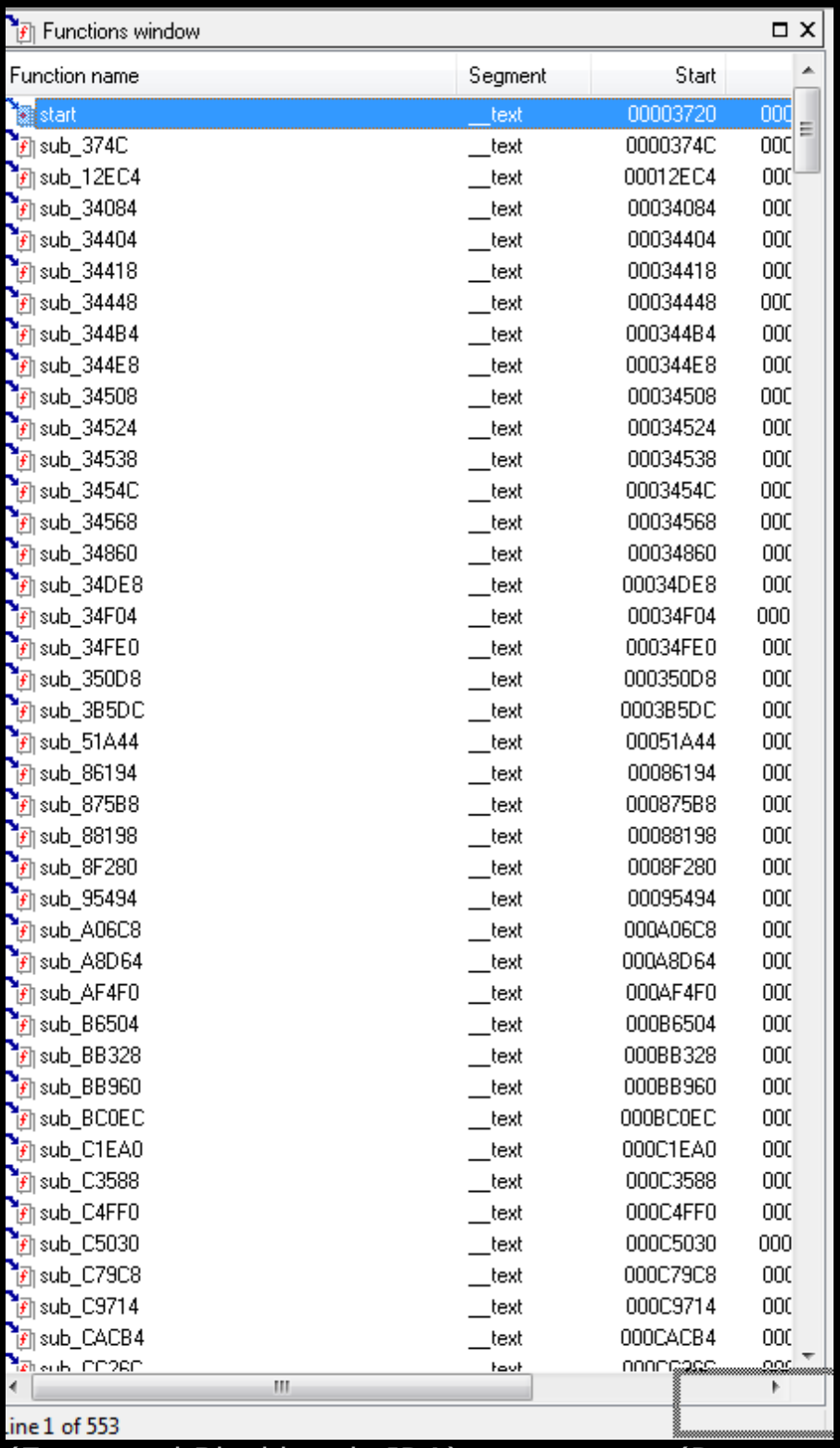


(The Bockheads' IDA file encrypted next to the same file decrypted)

***NOTE: To better read this photo, right click on it, then click open in new tab or window. Now you are able to zoom in/out with better quality**

To notice the MAJOR difference in these two files, look at the left side of IDA pro on both the programs; see the area that says "Function Window"? These are, well, the functions of the file. As you can see, in the Decrypted file, there is MANY more functions than the encrypted file. In fact, over 20 times more functions.


Functions window
Function name
Segment
Start
sub_BD59C __text 000BD59C
_deflateEnd __symbolst... 0018CBC0
deflateInit2 __symbolst... 0018CBC4
_inflate __symbolst... 0018CBC8
_inflateEnd __symbolst... 0018CBCC
inflateInit2 __symbolst... 0018CBD0
_GLKMathUnproject __symbolst... 0018CBD4
_AudioSessionGetProperty __symbolst... 0018CBD8
_AudioSessionSetProperty __symbolst... 0018CBDC
_alBufferData __symbolst... 0018CBE0
___cxa_atexit __symbolst... 0018CEE0
___divsi3 __symbolst... 0018CEE4
___fixdfdi __symbolst... 0018CEE8
___modsi3 __symbolst... 0018CEEC
___snprintf_chk __symbolst... 0018CEF0
___sprintf_chk __symbolst... 0018CEF4
___stack_chk_fail __symbolst... 0018CEF8
___strcat_chk __symbolst... 0018CEFC
___umodsi3 __symbolst... 0018CF00
__dyld_register_func_for_add_image __symbolst... 0018CF04
_abort __symbolst... 0018CF08
_atan2f __symbolst... 0018CF0C
_calloc __symbolst... 0018CF10
_cos __symbolst... 0018CF14
_dlsym __symbolst... 0018CF44
Line 1 of 25



(Encrypted Blockheads IDA) (Decrypted Blockheads IDA)

So, what is decrypting? "to decode (a message) with or without previous knowledge of its key"- thefreedictionary.com
What is decompiling? "to take machine or source code for a computer program and convert it to a higher-level programming language so that it can be read by a human"-Dictionary.com
(decompiling is done when we put the file into IDA pro. IDA pro is a decompiler)
Basically, when we go to edit the IDA file without having done anything to it, it is hidden away from crackers and hackers by converting it into a complex, computer language so that they cannot reverse engineer the file.
Well, as i just showed you, hackers CAN decrypt these files, and as far as I've heard, they can decrypt ALL of the apps and their IDA's out there.

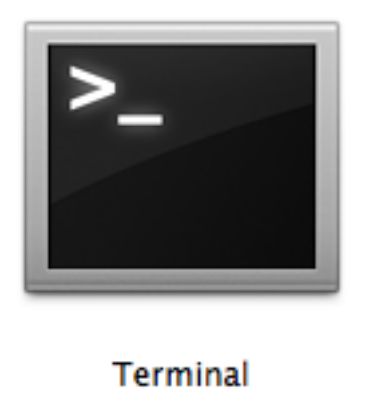
Decrypting- to decrypt an app's IDA, you need to do whats called "crack" the app. If you have ever had your game pirated (or hopefully not pirated other people's games), this is what hackers are doing to your app. They are cracking them; taking away apple's code so that they can be used and played on another person's jailbroken device. Every app is assigned a license, or a code from apple that basically says "yep, this game is legit", and when its custom, that code is basically destroyed or altered in a way that allows all jailbroken devices to run it.
Alright. Lets begin cracking.
There are TWO methods to cracking an app that i know of. I will run through them both.
1. Rasticrac
2. Clutch
Both require either mobile terminal, or terminal on your computer along with SSH.

Rasticrac- Rasticrac is the PREFERRED way to crack your apps. Its newer, its better, and its more efficient. For the purposes of hacking the IDAs, you will be fine with clutch, however i would suggest Rasticrac. The original Rasticrac, the one downloaded in Cydia, cracks the ENTIRE app, decrypting the whole app; however, if you use a modified version of Rasticrac that ToR made and very kindly gave me, you can crack and decrypt JUST the IDA file of the app. This saves

LOTS of time because you then don't have to search through the custom IPA/app to find the IDA, PLUS, if your cracking a large app, thats around 500MB, it takes probably three seconds to crack and decrypt just the IDA compared to a couple minutes cracking and decrypting the whole app.
This explanation may be slightly confusing, however, after reading through more of the IDA hacking tutorial, you will begin to understand more of what i am saying.

Lets get Rasticrac. Go to Cydia, make sure you have the repo "http://cydia.iphonecake.com/" added. now search "Rasticrac" and the package should come up. Download and install.
Now you have the Original Rasticrac. To get ToR's modified version, you'll need to go to:
http://www.mediafire.com/?naz85vck8n5652y
you need to paste this file over the old Rasticrac file in /usr/bin by using a file manager either on your iDevice (Ifile) or on your computer (Ifunbox, Iexplorer, or SSH)
Click "Yes" when it asks you to overwrite the old version of "r30c5.sh" (Rasticrac).
Now that we have the modified version of Rasticrac installed, we need to get set up with SSH or mobile terminal. In the Clutch tutorial below i describe how to get and use Mobile terminal, so for this tutorial, i will show how to get and use SSH. I would suggest just using SSH because your going to need it later on for Debugging the IDA.

SSH basically allows you to directly connect your idevice to your computer in terminal and using other software. Search "SSH" in the search bar, then click on "OpenSSH". Now that we have this, plug in your idevice to your computer, then, if your on a mac, i will provide a tutorial for how to run SSH for how to connect your idevice to ssh on your computer. If your on mac, then use this tutorial:
http://www.iclarified.com/entry/index.php?enid=3221
(You will also need to install "WinSCP" to connect to your idevice through SSH on windows)
For a mac, connect your idevice to your computer. Now open up the application, Terminal. by going to Macintosh SSD/Applications/Utilities/Terminal.

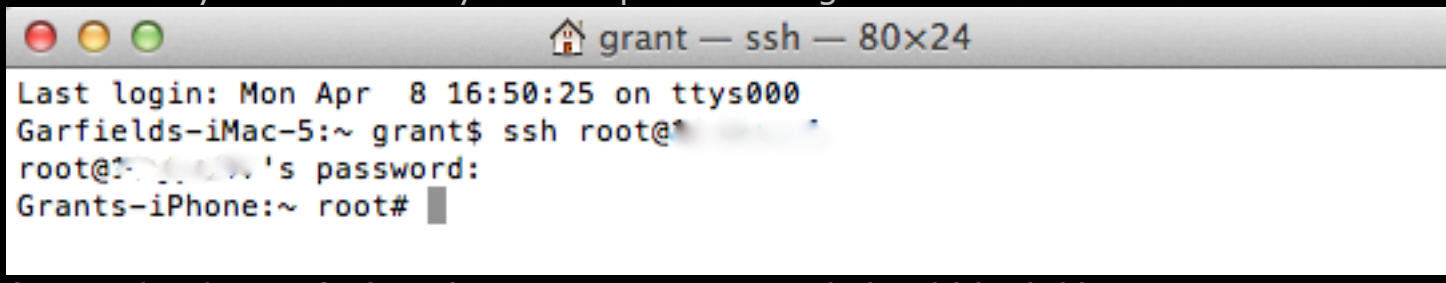


(Terminal Icon on Mac)

Now we need your Wifi IP address. Go to Settings/Wifi, then click on the wifi your connected to. It should display the Wifi's IP. Make note of this.

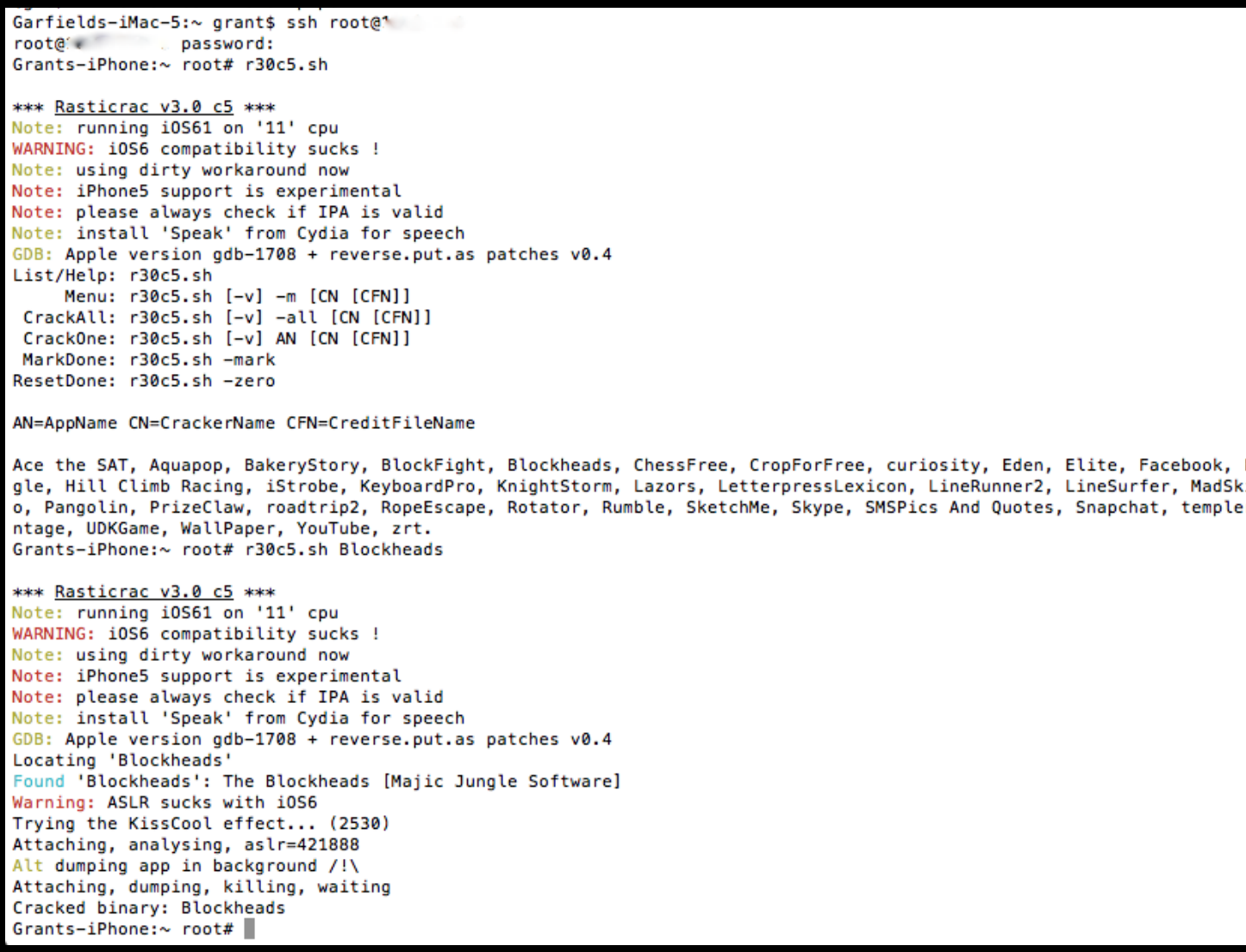
(Settings/Wifi/yourwifi. NOTE** I took out my IP and other info for safety and security reasons, however it will display your IP in the "IP Address" box.)

Now, In Terminal, type 'ssh root@"yourIPhere"' without the quotes. So it should look something like: ssh root@192.168.1.103
It should ask for a password after that. If you have never made a root password, it will be "alpine" (without quotes). Mobile terminal should return with "Grants-iPhone:~ root#" ("Grant's-Iphone" will be the name of your idevice).
Give yourself a pat on the back because you have successfully connected your device to your computer through ssh!



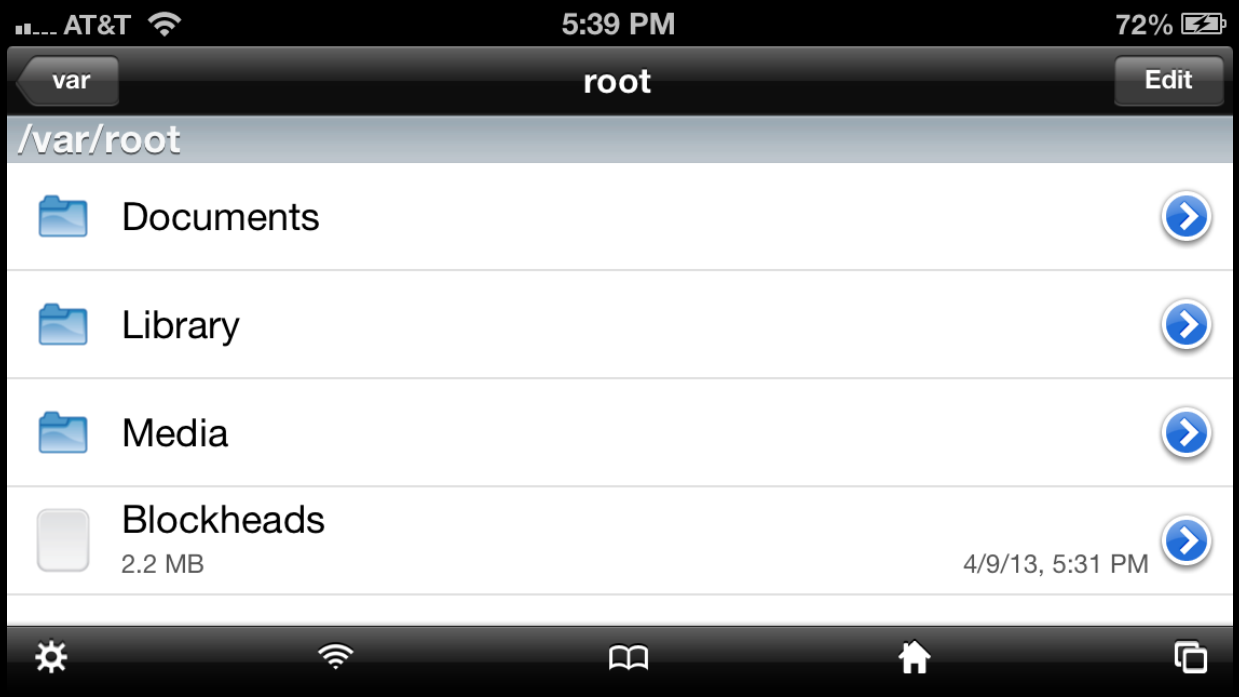
(example photo of what the process in terminal should look like. Keep in mind i blurred my IP, thats why its not there.

Once connected via SSh, use Rasticrac by typing "r30c5.sh". You should get a bunch of code along with a list of all the apps on your iDevice. To crack the app of your choice, scan through all the apps in the list and copy the name of the one you would like to crack. Now type 'r30c5.sh "appNameHere"', for example, in the photo below, i typed: r30c5.sh Blockheads
NOTE** the name of the file must be the EXACT SAME as displayed in the list of apps



(Using Rasticrac to crack the app "The Blockheads" IDA file through SSH)

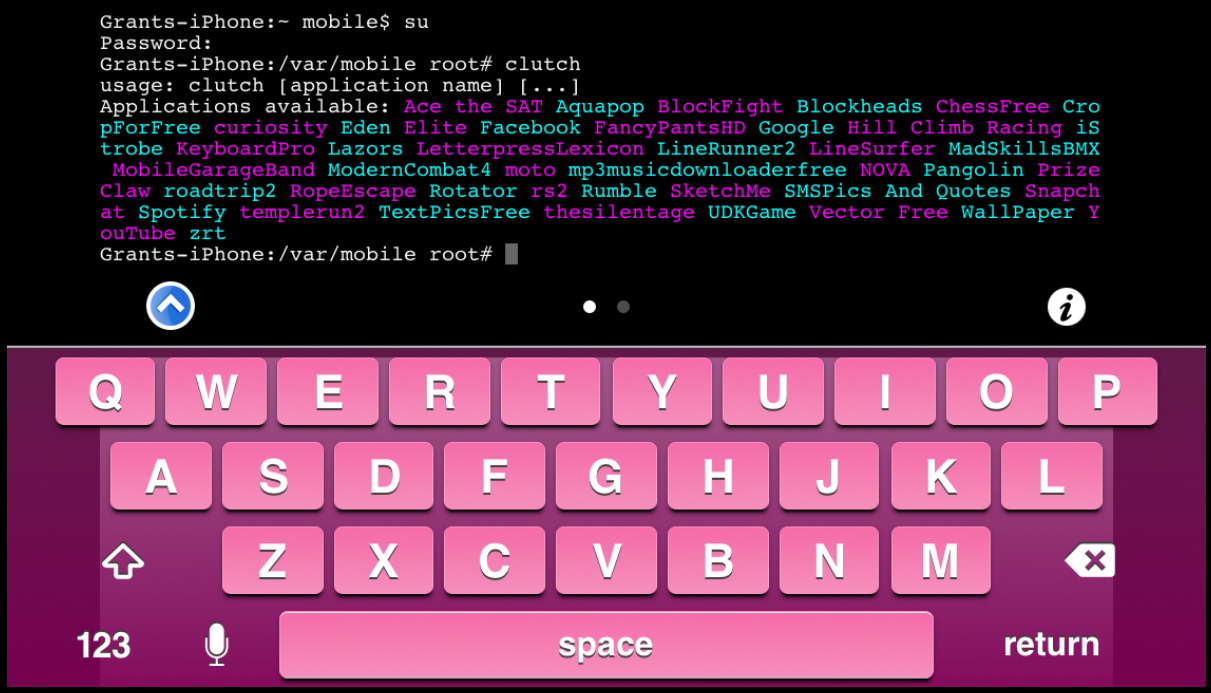
To get to the IDA file that you just custom and decrypted, go to var/root and you should find a file with the same name as the one you custom. This is the IDA file.



(var/root after cracking The Blockheds' IDA)
Now put this on your computer using your file manager/SSH/email.

Clutch

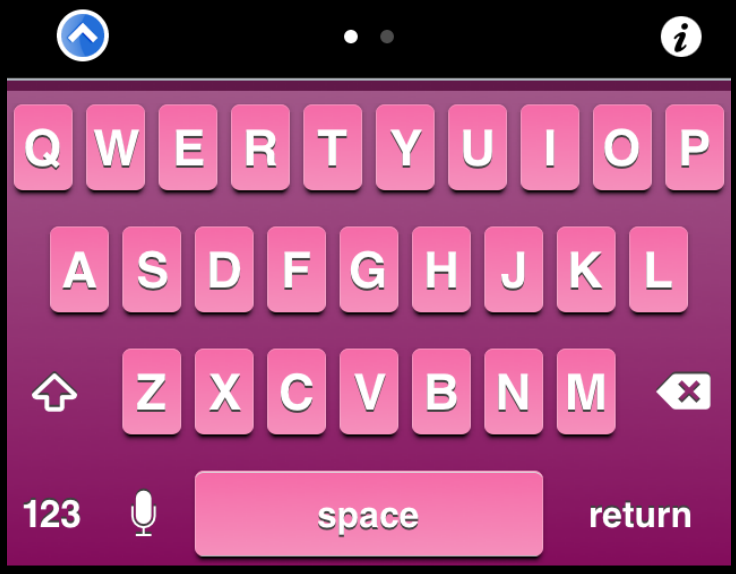
**NOTE: you can skip this step if you already used rasticrac to crack and decrypt your app! Both methods are in here for the tutorials sake.
Now lets learn how to use clutch.
On your jailbroken device, you will need two things. Go to Cydia and search "Clutch". It should come up, but if not, make sure you've added "http://ihacksrepo.com/". Once installed, respring/restart, then go back to cydia and search for "Mobile Terminal". Install that, exit Cydia, now your set to crack some apps!
Find the Mobile terminal app on your home-screen. Type in "su". It will prompt you for a password; if you have never set a root password, it will be "alpine". Once you gain access, to see a list of encrypted apps, type "clutch".



(viewing a list of apps to crack in mobile terminal)

To crack, just type clutch "app name". Its that simple! To crack all encrypted apps at one type 'clutch --'

```
Password:
Grants-iPhone:/var/mobile root# clutch
usage: clutch [application name] [...]
Applications available: Ace the SAT Aquapop BlockFigh
t Blockheads ChessFree CropForFree curiosity Eden Eli
te Facebook FancyPantsHD Google Hill Climb Racing iSt
robe KeyboardPro Lazors LetterpressLexicon LineRunner
2 LineSurfer MadSkillsBMX MobileGarageBand ModernComb
at4 moto mp3musicdownloaderfree NOVA Pangolin PrizeCl
aw roadtrip2 RopeEscape Rotator rs2 Rumble SketchMe S
MSPics And Quotes Snapchat Spotify templerun2 TextPic
sFree thesilentage UDKGame Vector Free WallPaper YouT
ube zrt
Grants-iPhone:/var/mobile root#
Grants-iPhone:/var/mobile root# clutch blockheads
Cracking Blockheads...
warning: iTunesMetadata.plist item named 'product-typ
e' is unrecognized
warning: iTunesMetadata.plist item named 'asset-info'
 is unrecognized
        /var/root/Documents/Cracked/Blockheads-v1.2.1
.ipa
Grants-iPhone:/var/mobile root#
```

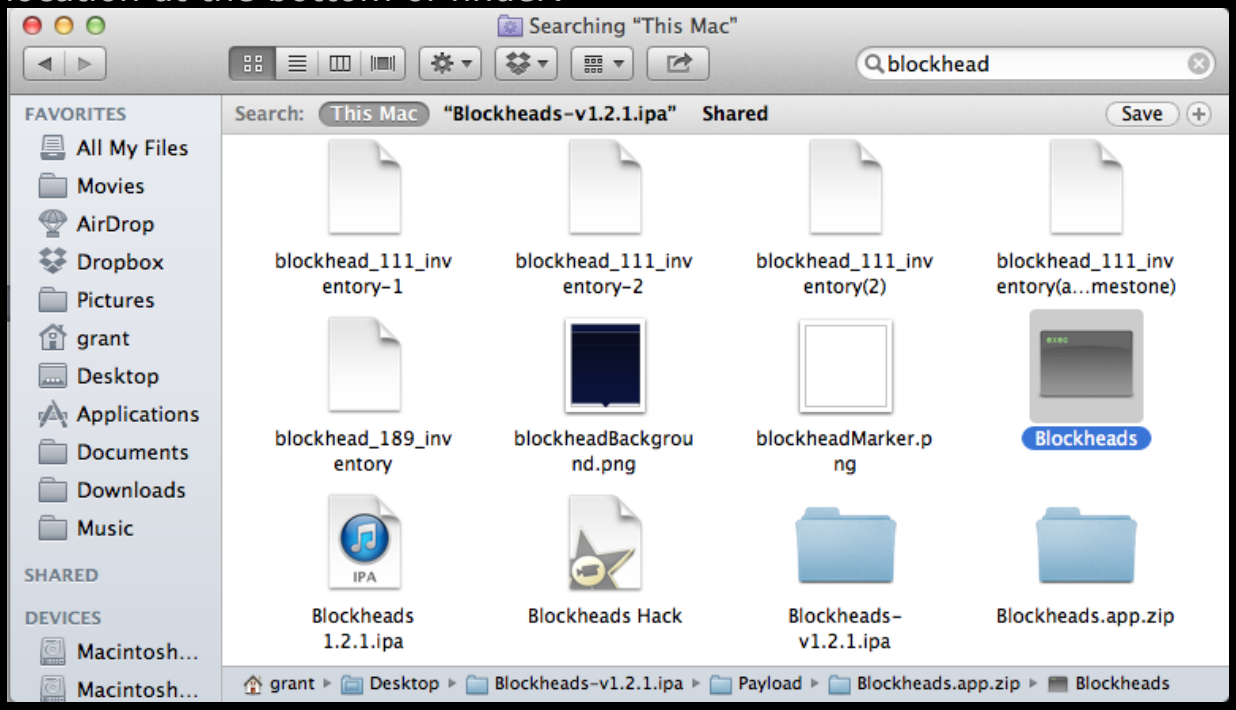


(cracking The Blockheads with Clutch in Mobile Terminal)

NOTE: distributing this custom app is highly illegal, I DO NOT SUPPORT PIRACY OF APPS Now, to get your decrypted IDA file, you need to go into your file manager and navigate your way to /var/root/Documents/custom. Paste the ".IPA" file on to your computer.
Getting to the actual IDA file is a little tedious. Put the IPA file onto your desktop. Right click on the file, click get info, rename, then add on ".zip" to the end of the file. Double click on your renamed file. This

should create a folder kind of like this one:

Open this up. Open the file called "Payload". Now you'll see your app without an extension. add ".zip" to the end of it again. Now it should become a folder with a LOT of contents. Locate the IDA file in this folder. It may appear that it doesn't exist, for example, when i scan through the folder's contents which are in alphabetics order, "Blockheads" is not in alphabetical order with the other files. Best thing to do is just do a quick search in finder for the IDA. When i search "Blockheads" in finder, its obvious this is the file because of the location at the bottom of finder:

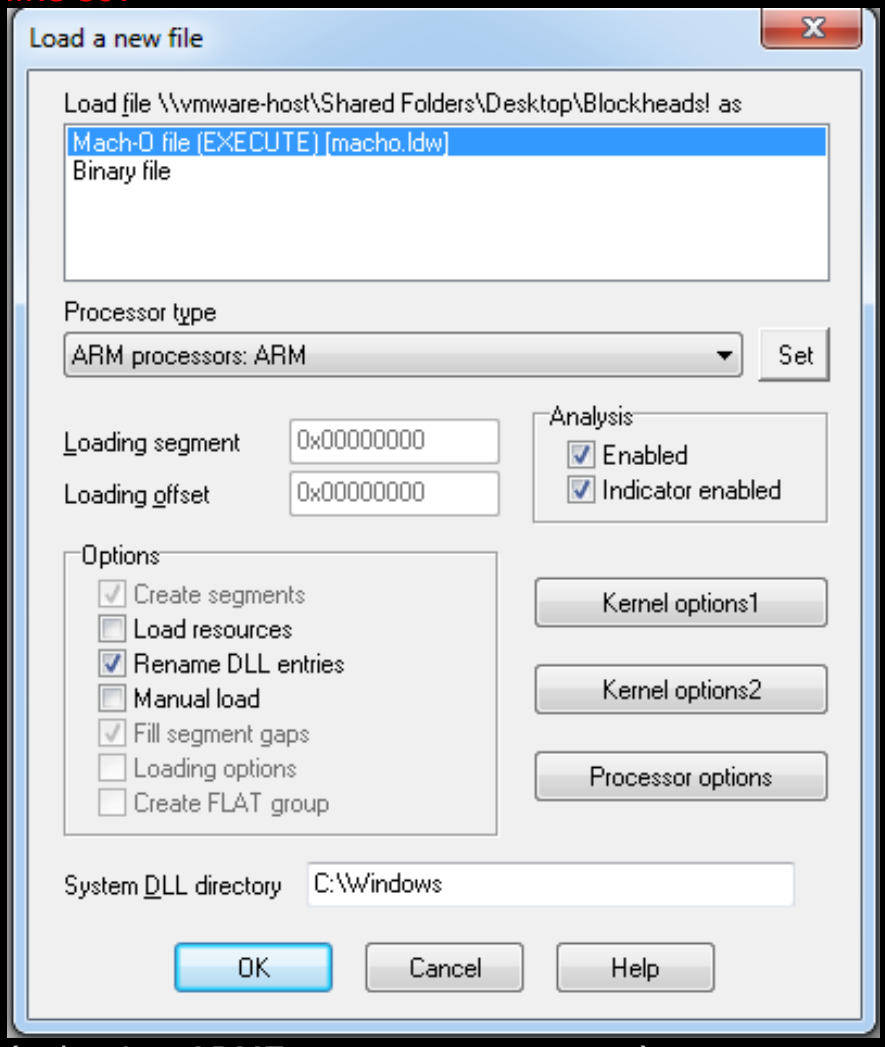


(finding "Blockheads" ida in Finder)

Once you located this, well, you can simply load it up in IDA Pro by dragging-and-dropping the ida into it; congrats! you did it. This is where IDA hacking begins.

MAKE SURE where it says "Processor Type" that you select "ARM 7"

like so:



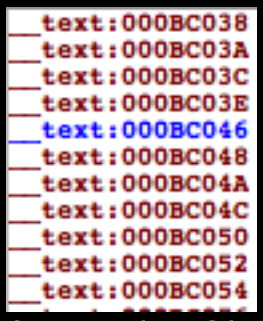
(selecting ARM7 as a processor type)

Heres where i cant really teach you directly what to do for your app to hack it. You need to be able to interpret ARM language. In order to learn basic ARM, i would suggest reading other tutorials on app hacking with ARM. Here are some links i would suggest:
http://www.iapphacks.com/tutorials-f8/hacking-tutorials-t14002.html (many tutorials on many things including 4 for IDA hacking)
http://www.iapphacks.com/tutorials-f8/ida-pro-basics-t8246.html (GREAT guide sheet for hacking ARM, Thanks, HackJack!)
http://www.iapphacks.com/tutorials-f8/ida-pro-1-t13386.html (simple tutorial to hack a game)
http://www.youtube.com/watch?v=ZogTQsVu92M
http://www.youtube.com/watch?v=o8CR_sDrKGE(3:13-5:30 is a VERY helpful example of how to interpret ARM code)

http://www.iapphacks.com/viewtopic.php?f=8&t=9372 (definitions of many of ARM abbreviations)
http://www.mediafire.com/?i8cd23ueck2pb03 (plants vs. zombies TUT)
http://ininjas.com/forum/index.php?PHPSESSID=cpmchq7nnaijjk0d597tspqqt1&topic=2455.0(read the second quote- good translation of ARM)
http://www.se7ensins.com/forums/threads/tut-how-to-hack-ios-games-and-apps.701845/

I was planning on covering how to IDA hack with my own tutorial on the Blockheads, however i spent so much time into this tutorial that i lost interest a while back and never posted it. So i decided i would summarize what i missed, then post the tutorial. My suggestion would be to learn from the above links how to IDA hack. There is more than enough information above to learn!

To summarize the process, You want to use IDA Pro to search the Objective-C code translated into arm. Search for keywords by clicking on the "search" function at the top, then click "text". Search all kinds of keywords that would work for your game (gold, crystals, bucks, coins, health, speed, ammo, etc.). You then need to understand how ARM works to know what to edit. To edit the arm, you open up the IDA file in a Hex editor, then use the side header to determine where in the Hex to find the exact code you were looking for.



(example of headers in the Blockheads)

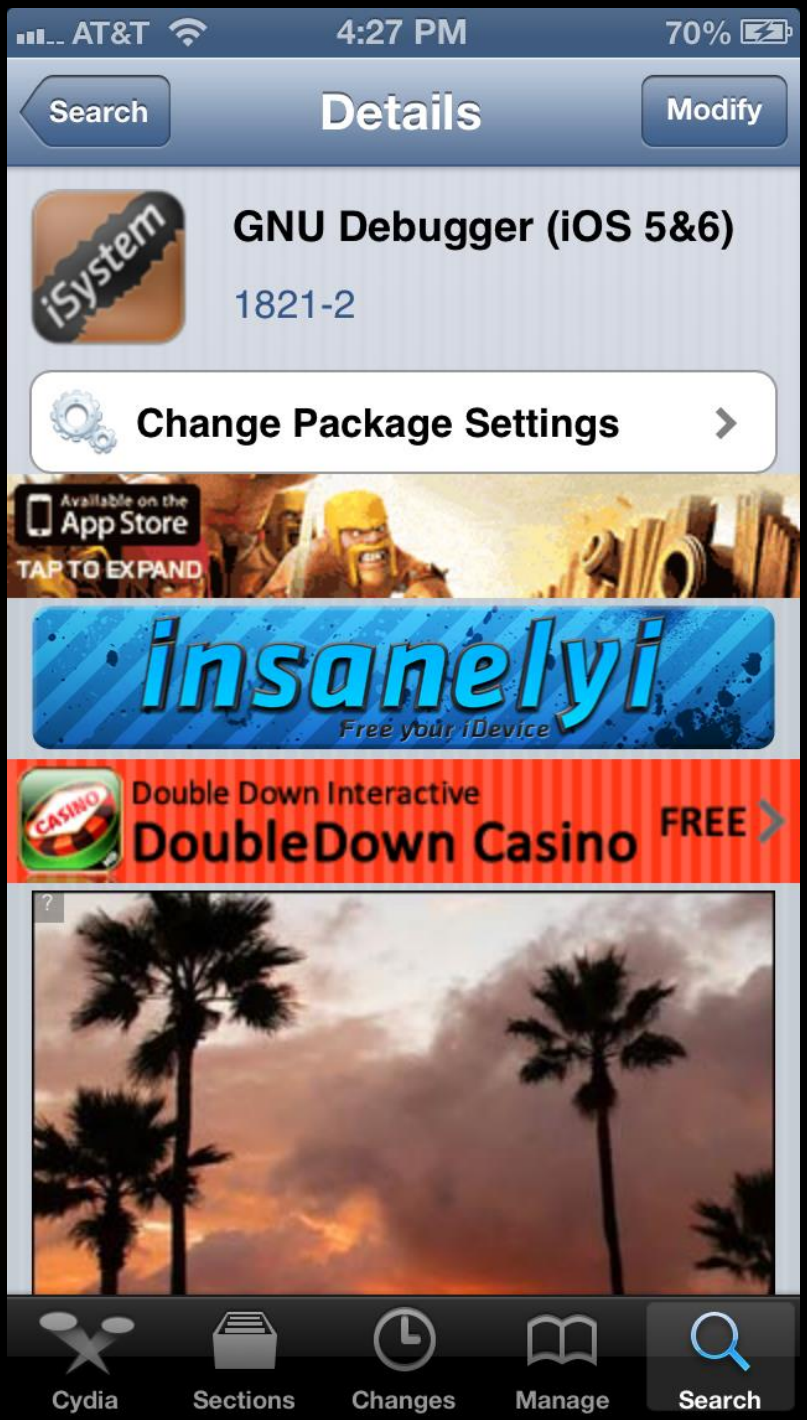
You then use an ARM-HEX converter http://puu.sh/1mC2f (or go to http://www.iapphacks.com/tutorials-f8/ida-pro-basics-t8246.html for many pre- done conversions) to figure out what code it is you want to change. Figure out what and where you need to implement the code you want to put in, then in the ARM/ASM converter, enter the code

you want to put in. For example, you can put in "ADD R1, R2" to the converter and it will translate it into binary for you. Paste that binary into the hex editor, save the file, then paste it into your app on your phone and overwrite the old one, test the hack, then evaluate.
This is a basic summary of how IDA hacking is done! Please read the above tutorials, HackJack, here on Iapphacks, has made most of them and he does a wonderful job of explaining how things should be done.

**NOTE: I was not able to finish the up-coming tutorial on Debugging.

Sorry guys! Tor is a busy guy and he was helping to teach me how to debug, but he must have gotten more busy and he stopped replying to my Skype messages. Either way, he was a HUGE help to me and i thank him for that!

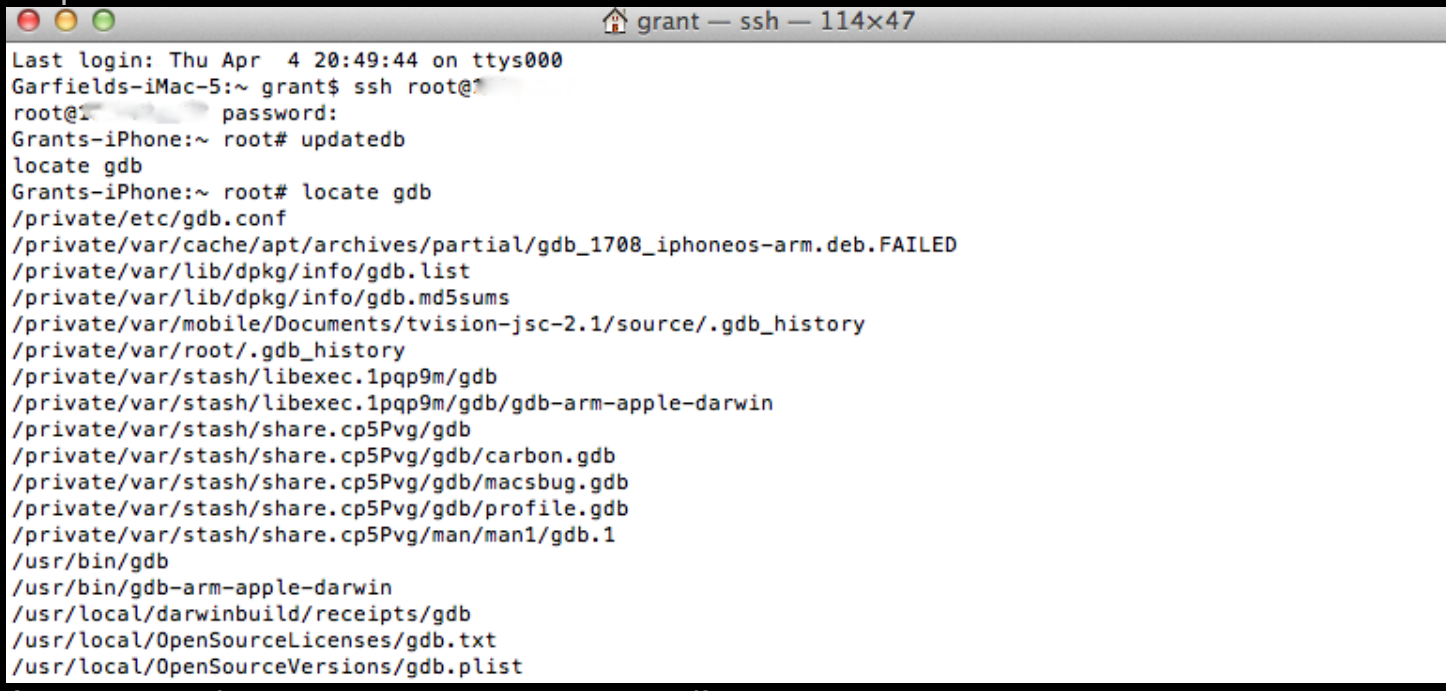
Debugging-Debugging is basically a way to make the commands of the executable file more clear and understandable. Its another method to IDA hacking. In order to debug, were going to need a tool made for developers of apps, GNU debugger (GDB). Get ready, because GDB is confusing to install for people who don't have experience with terminal, like me.
For this tutorial, i had ToR's help (Global Administrator of Iapphacks), THANKS, ToR, for the hours of help on Skype!
Anyways. Lets begin. Go to cydia and add the repo: "http://cydia.radare.org/". Now go to back to "Manage", then click "Settings" at the top left. Congrats, you require a developers status on Cyida to download something! So change it to developer (if it isn't already).
Go back to your search bar now search "GNU Debugger". Alright, according to ToR, we need two of these GNU Debuggers. First, download "GNU Debugger (IOS 5&6)" (assuming your on IOS 5or6). To be SURE this is the right one, make sure after clicking on the package, it says "1821-2" under the package name, like so:



("GNU Debugger (IOS 5&6)" on InsanelyI's repo in Cydia)

Cool. You've got that successfully installed. Now go back to cydia. The other GNU debugger we need is the one on the repo i gave you, called "GNU Debugger". Make sure once you click on it, it has the number "1708" under the name. This is the correct file. Download and install that.

Now that your connected to SSH, you need to set up your GDB that you installed. Type in "updatedb" to terminal. You shouldn't get a response from terminal. Now type "locate gdb". At first it will appear nothing has happened, but wait a moment and terminal should respond with some code. This is how terminal should look so far:



(SSHing and setting up GDB in terminal)

The Debugging tutorial ends here. If you were looking to learn how to use GDB to debug and are still interested, please PM or email me at grantman100@gmail.com and just let me know so. If i get enough requests, ill add it to this post.

Q. Is a jailbroken device needed?
A. No, not always. Sometimes, yes, but it depends on the hack. Why not jailbreak? If your into hacking, i see no reason not to jailbreak.

Q. Do i need to know any programming languages to hack/secure apps?
A. Nope! It would help to know some, live java, for basic knowlege, however it is not needed. The knowlege of ARM would also be very helpful for the more difficult IDA hacking.

Q.Is app hacking illegal?

A. Depends. No, its not illegal if your simply hacking a game and not stealing anything or effecting online play. Lets say, for example, you hack angry birds and give yourself 3 stars on every map. This is not illegal since you have not stolen or affected other players. However, if you steal something that is sold in an in-app-purchase, or hack to give yourself unlimited ammo, or something of that sort for an online game, then YES, this is technically illegal.

Q. How long has it taken you to master these methods?
A. I have not, in any way, mastered these methods. Ive been hacking apps for about two years now on and off, however I continue to learn where to find vulnerabilities and how hackers are able to reverse-engineer apps. I even got help from the moderator, Tor, of this site to help me complete this tutorial.

Q. Where can I get someone to hack/secure an app for me?
A. If your looking for help with SECURING an app, I can help you. If you send me your app, I would be glad to attempt to hack it for you, however I will not hack apps for others for malicious purposes. If you would like that done, please ask someone else.

What to do if your able to modify files in your game.
Well, shoot. Your app turned up positive for hacks via one of these methods. What should you do?
Well, first, let me point out that MOST games out there are easily hackable by using the first five methods listed. MOST apps don't require an IDA hack. If your hack is only hackable via an IDA hack well, you've done much better than many other developers. Obviously, patching up the vulnerabilities you've found depends on HOW the hack is done.
First, lets note what your goal is. Do you want a hack-free app? Or do you want to limit hackers so that there aren't numerous people running around with hacks for your app?
If your simply looking to limit hackers, there is a couple things to note that will help.

No one on IOS 6.0+ can hack your game as long as they aren't jailbroken if you simply keep your valuable info in the .app folder of the game. I would guesstimate that about only 1 in 10 people are not on IOS 6+ and/or are jailbroken. If you leave your app with vulnerabilities in it in any folder other than the .app folder, you are

opening up your app to every single person who has access to a computer.

Do you realize that? Because developers seem to ignore this. All that must be done to secure your apps and prevent about 90% of people from hacking your apps is to simply DONT take the easy way and store data that is valuable in ANY folder other than the .app folder.
Fortunately for all of you developers whose apps aren't multiplayer or online, this is all the correction that is essential to protect what most developers are in the app developing business for- money. You see, when hacks are easily available for users that aren't jailbroken, developers **lose money**. People are able to steal the in-app purchases quite easily and many do this over pay for them.
If your a developer who is looking for a fast solution to not losing money on hackers stealing in-app purchases, just be sure to store your valuable data in the .app folder, this will prevent 90% of users from stealing over purchasing the IAP.

However, if your goal is prevent ALL hackers and keep your leader boards completely clean of fake scores, you have some extra work to do to secure your data. I am not a good source of ideas of how exactly to go about this, but i can say that most of the apps that i have not been able to hack are due to encryption of data within the game and games that store almost all of the data in the IDA of the game.
Heres another tip: if a file in the game does not have an obvious name and/or file format that us hackers know are easy targets (.txt, .plist, .xml), then we will skip over it and ignore it. If i go to modify a file, and lets say its called "nyx_JCT" and it opens up completely encrypted, chances are i'm going to completely ignore it. Maybe if I was extremely determined, i would come back and hex edit it, but for the most part, i would assume its nothing valuable and pass on by.
If your looking to prevent ALL hackers, heres a really good link that suggests the idea of adding jailbreak/crack checks in your app.
http://iphonedevwiki.net/index.php/Crack_prevention#AppStore
This is definitely a good idea to help secure your app, however, simple jailbreak check are easily over-ridden. Just check FLEX, i can guarantee you that one of the apps on your device has had their jailbreak check over-ridden by FLEX.
Heres a link with a tutorial of how to make hack-detectors:
http://iphonedevsdk.com/forum/iphone-sdk-tutorials/29509-iphone-piracy-protection-code-a-tutorial.html

Another useful tip:
"The golden rule is: If you put something you want to protect on the device then it is going to get hacked."- Peter Molyneux, developer of Curiosity and his developers (http://www.polygon.com/2012/12/28/3811032/curiosity-besieged-by-hackers-but-the-secret-remains-safe)
What does this mean? Well, in the game Curiosity, an online, single-server game, the objective was to destroy this cube and whoever succeeded received a "Life-changing" gift. Well the lead developer was smart enough not to put this gift in every person's device. He knew no matter how much he tried to hide it, it would have been uncovered, so he made it server-sided. Unfortunately, Molyneux didnt also make the currency OR in app purchases in the game server-sided, so all the hackers were able to blow up their in-game bank account.

(Curiosity App- Bottom of screen shows hacked gold value)

So the lesson to be learned here is IF your looking to make a completely hack-free iPhone app, you'll need servers. Period.

These, quite honestly are the only tips i can give to preventing hacks; I have never made an app, so I have limited knowledge on how one would go about securing an application. A book I read, however, that did help teach me quite a bit about hacking and securing ios

applications is, well, Hacking and Securing IOS Applications: [url]http://www.amazon.com/Hacking-Securing-iOS-Applications-Hijacking/dp/1449318

Once again! You can download this tutorial in a Microsoft Word file at http://www.mediafire.com/download/jqreibbq1kn5d86/Hacking_tutorial_for_apps.docx
Thanks for reading my tutorial! If it helped you, hit the THANKS button for me! I spent probably over a day making this tutorial for you guys, so if it helped you in any way, let me know because it would mean a lot!

Questions? Comments? Requests? E-mail me at Grantman100@gmail.com