

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Android / iPhone Memory hacking \(Game hacking / App Memory Hacking\)](#)

Ugleh - April 16, 2013, 8:11 pm

Tutorial Intro:

I will be showing you all how to use a memory editor app for jail broken iPhone and rooted Android. This can work for any game and hopefully any other app. For this tutorial I will be hacking Subway Surfers on my Android device. A game that makes you pay for gold coins if you don't want to waste your time collecting a lot.

I made the tutorial real simple to follow in this [imgur album](#), each image has a comment.

Intro:

I used to hack games all the time using [Memory Hacking Software](#) and [Cheat Engine](#) for PC. I would suggest Cheat Engine for beginners, it has a nice user friendly interface and tutorial. But then I thought, is it possible to hack Android or iPhone games? Googling and I found something called [Game Guardian](#). This program works nicely. It has answered my question.

Step 1:

Download [Game Guardian](#). They have 2 official downloads, [iGameGuardian](#) and [GameGuardian](#).

Step 2:

Once you run the app for the first time you may be confused, but once you exit out of the instruction screen you will see the Game Guardian logo, which looks like a dog. You can see it aligned on the right close to the center.

Step 3:

Here is the screen in Subway Surfers which shows me my coin amount. As you see I have 0, so I am going to play a round and collect some first. I would never search directly for the value of 0 because usually millions to billions of addresses have the value of 0, and we don't want to crash.

After playing a fast round I earned 17 coins. I will now search for 17 in Game Guardian program.

Step 4:

When you open up Game Guardian by clicking the dog icon, you will click Search. then search for "17" for example. Whatever your score is, is what you will search for.

This is the address results. Computers store memories in addresses. These addresses can be called from the programming code to get the value stored, and modify it. Our task is to find the correct address and modify it ourselves. There is almost 500000 values of 17. This can be anything from screen location to last finger location, ANYTHING. But 1 of them is the coin value, to find it we will play another round and increase the gold count.

Step 5:

Now we have 37 gold, so we are going to search for the value of 37 from the previous values of 17.

Like searching for a needle in a haystack, and receiving hay still, just less hay.

Here we are searching for the value 37, like I did with the 17 earlier.

This is the results. You can see we went from 500000 values to only 21. Not only that but some values already changed during the search. As you can see by the 252 and the 137, and the others.

Step 5:

I feel we need to play 1 more round to sift everything out. Now we have 91 gold.

Search for the value 91 from the previous 21 addresses.

Our result is only 4 values. We are getting real close. 1 more round!!!

Step 6:

Depending on the game just keep doing the previous steps over and over until you get results that wont change. At the end I was left last with 4 addresses. So I know all those addresses are involved with the money. Some games use multiple addresses to store the same value. It really depends on the game, but this game proved to use 4 addresses for the value, so I edit all 4 with the value of 999999. To edit the value press the value and hold till the editing window shows up.

Here is the final result, I am rich bitch!

T-rom - April 17, 2013, 7:36 am

great tutorial :)

too bad that im pretty sure this can get you 'banned' from certain apps

sonic208 - April 17, 2013, 8:15 am

it only looks like you have the amount of coins

But you dont have it am i right

its the same shit as with cheat engine

its only clientside only you on your smartphone see it

if you close the game and open it again the game compares the amount of coins with the stored number on the server,..

or am i not right?

Ugleh - April 17, 2013, 10:01 am

(Apr 17, 2013 08:15 AM)sonic208 Wrote: [\[CITE\]](#) it only looks like you have the amount of coins

But you dont have it am i right

its the same shit as with cheat engine

its only clientside only you on your smartphone see it

if you close the game and open it again the game compares the amount of coins with the stored number on the server,..

or am i not right?

I can use the coins if I wanted. Subway Surfers is not a multiplayer game which means the coins is

stored on my device and not on a server.

(Apr 17, 2013 07:36 AM)T-rom Wrote: [\[CITE\]](#) great tutorial :)

too bad that im pretty sure this can get you 'banned' from certain apps
You can't get banned from apps like this.

T-rom - April 17, 2013, 11:25 am

it makes sense, only local games can be edited... although a lot of games that have multiplayer options for highscores could be edited with this am I correct?

Xyzo - April 17, 2013, 11:27 am

Thanks for sharing, it will be fun to do this ;)

Ugleh - April 17, 2013, 2:51 pm

(Apr 17, 2013 11:25 AM)T-rom Wrote: [\[CITE\]](#) it makes sense, only local games can be edited... although a lot of games that have multiplayer options for highscores could be edited with this am I correct?

Yes. Most high score coding uses post data from client side. So the high score is stored on the client, but then at the end of the game it is stored in the server. At least that was the case for the flash game Pandemic 2.

P1rat3 - April 17, 2013, 2:58 pm

I know this does work for a lot of games I personally use it on my tablet but its not called game gaudian its called gameCIH

ALiEN_r00t - April 17, 2013, 3:17 pm

i did this long time to all my preferred games

so if anyone want i can send only data, and Done! you don't need to hack .apk

firewing - April 17, 2013, 8:23 pm

How do i download it in my ipod? I checked in cydia for lgameguardian or gameguardian .. No result. Can you help me?

Ugleh - April 18, 2013, 9:17 am

(Apr 17, 2013 02:58 PM)P1rat3 Wrote: [\[CITE\]](#) I know this does work for a lot of games I personally use it on my tablet but its not called game gaudian its called gameCIH

Game Guardian in my opinion superior to GameCIH. You just proved it by saying GameCIH doesn't work for many games. GameCIH tries to find the flash/java variables in a game, where as Game Guardian looks at the memory addresses.

(Apr 17, 2013 08:23 PM)firewing Wrote: [\[CITE\]](#) How do i download it in my ipod? I checked in cydia for lgameguardian or gameguardian .. No result. Can you help me?

Use the website links I posted. Your iDevice needs to be jailbroken I think, not positive but let me know. I know my Android device needs to be rooted.

Arbitrary - April 18, 2013, 2:27 pm

Looks like a nice solid tutorial! I really like how you made its nice and siple with the image album! sorry for spelling I'm om my phone :(

li-ning - *April 21, 2013, 9:21 am*

Nice really helped out with my low scores and poor skills xD

Funds - *February 5, 2014, 11:33 pm*

Great tutorial will try this out sometime
?

DEDSEC Crave - *June 14, 2014, 12:18 pm*

Works Great thanks! You got my vouche ?

You made my day
time to start!