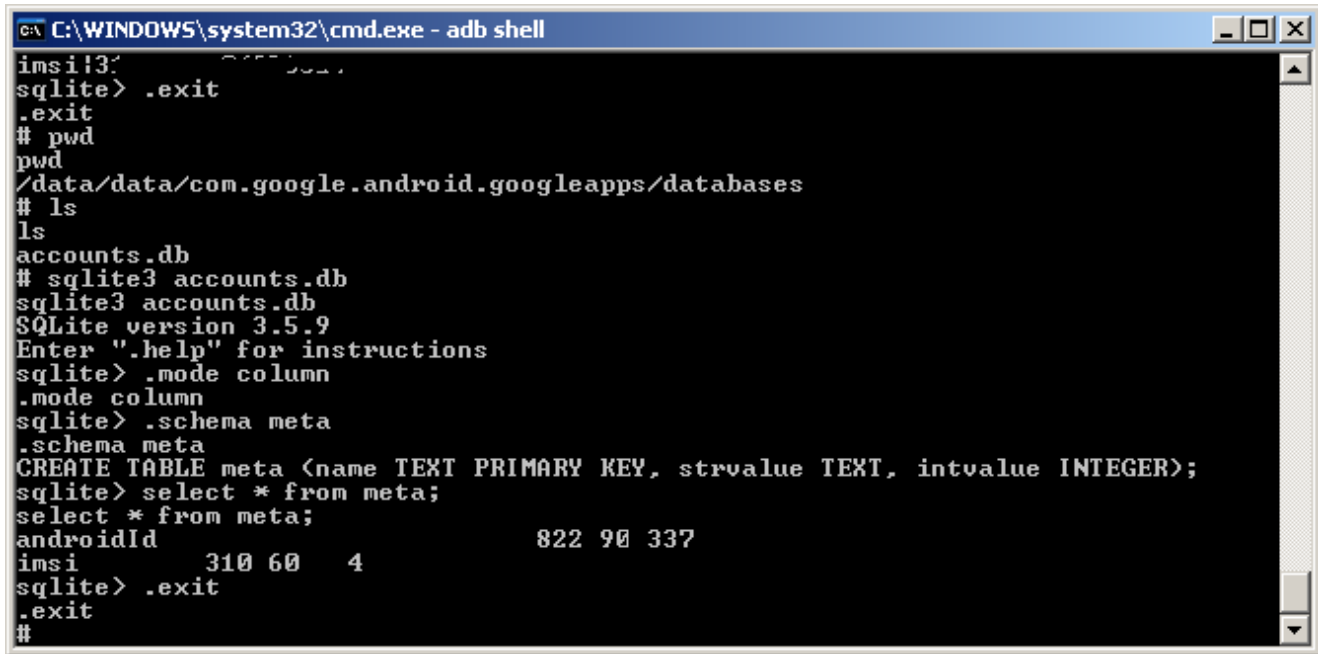


14

[More spoofing of the android id...](#)

April 9, 2009, Tim



```

C:\WINDOWS\system32\cmd.exe - adb shell
imsi{3:
sqlite> .exit
.exit
# pwd
pwd
/data/data/com.google.android.googleapps/databases
# ls
ls
accounts.db
# sqlite3 accounts.db
sqlite3 accounts.db
SQLite version 3.5.9
Enter ".help" for instructions
sqlite> .mode column
.mode column
sqlite> .schema meta
.schema meta
CREATE TABLE meta (name TEXT PRIMARY KEY, strvalue TEXT, intvalue INTEGER);
sqlite> select * from meta;
select * from meta;
androidId      imsi      value
822 90 337     310 60 4   4
sqlite> .exit
.exit
#

```

Finding the Android ID (img blacked out)

[In a previous article](#) I had posted some information about how it is possible to spoof the Android ID that is returned when calling the Settings.System.Android_ID function. Though I had noted at the end of my post the following;

Note that this will NOT change the android id used by google products since they use one that is linked to your gmail account that the phone is associated with...

This bugged me a little bit because I wanted to know how the google applications where using and getting the android information – did they pull it directly from the hardware? Where they just using private API that was more secure? So after a little research, I found exactly what was going on, and again how it would be possible to spoof the id.

Essentially the google applications use googleapps to store the android id, this is the program on the phone named “com.google.android.googleapps”. This is a very interesting program that sadly developers do not have access to as of yet, though hopefully this will change shortly.

Anyway, this program is also susceptible to being force-fed spoofed values. The method is essentially the same as the previous one, though just performed on a different database. From within adb or the shell, do the following;

```

$sqlite3 /data/data/com.google.android.googleapps/databases/accounts.db
update system set value=' deadbeef0000badf00d' where
name=' androidId' ;

```

This program also store in that table the imsi number linked to the phone, for simcard tracking purposes.



Tim

11 Comments

[Reply](#)

1.

Why .bmp screenshot?

[tamerlan311](#) [April 9, 2009 at 1:32 pm](#)

[Reply](#)

2.

@tamerlan311 — I wasn't on my normal developer machine, so I just quickly used mspaint 😊

[Tim](#) [April 9, 2009 at 4:54 pm](#)

[Reply](#)

3.

I have a question and this topic seems to be the closest to what I'm looking to do. I want to spoof the (from what I understand) device_id on my entire phone so T-mobile will not know that it is an android. Because it does tell t-mobile it's an android, right now, t-mobile redirects my browser to a page saying I need to upgrade my internet account with them. In reality all I need is edge speeds and can't justify \$25/month just for phone internet. Of course my problem is that no internet apps work on the phone when t-mobile is blocking my "Android"

I also use an iPhone and edge is fine for everything I do but t-mobile doesn't track it like the android...so if I could spoof my android to look like an iphone...quack like an iphone...

Is this topic what I need to do to achieve what I need or do you have a different topic I should see? Or would this be a new project to try your hand at? 😊

Thanks!!
Bryan

[Bryan](#) [January 3, 2010 at 7:33 pm](#)

[Reply](#)

4.

@Bryan,

It's possible — though I think what your going to need to do is spoof the IMEI, not the android ID. From what I can tell, thats often what people with iPhones do.

Though that isn't exactly a legal subject to discuss openly – atleast in the US.

[Tim](#) [January 3, 2010 at 8:21 pm](#)

[Reply](#)

5.

@Tim

First off I'm very impressed with your response time! Most places I visit can take days to get a response!

Now I know IMEI spoofing is illegal but I feel this is not what T-mobile is blocking (could be wrong) nor do I want to mess with that. I am curious what you know of iPhone users spoofing their IMEI as I haven't heard of, or know of, a reason why iPhone users would need to do this. (I guess maybe if they stole it lol)

For the android though do you have a thought on what may be broadcasting that it's an android phone when it comes to the internet? I've seen some apps such as Steel that offer to spoof the "User Agent" to appear as other devices but since it's in the

app itself this really only effects how the page is rendered for the user (Like the differences between IE and Netscape Navigator). So this method is superficial on just the website/browser level and does not get around t-mobiles blocking either.

I wish I knew more about the android file system and design lol! Any thoughts? (And I did want to clarify that spoofing the phones h/w to t-mobiles servers isn't illegal as of yet...Apple's working hard to change this so people can't modify the s/w on their phones or they get a big fine but this is not in place yet, which means we still have time to tamper lol!

Bryan

Bryan [January 3, 2010 at 8:38 pm](#)



[Reply](#)

6.

Ok new question! I'm following your instructions from one of your other posts about spoofing the android_id and I'm stuck on the part that I'm supposed to type in "sqlite3 settings.db" (Already navigated to the folder for it) and it returns "sqlite3: not found"

I am using the Android SDK and ran adb and mounted my phone through the correct channels and sqlite3.exe is in the folder. Any thoughts?

Bryan [January 3, 2010 at 8:58 pm](#)



[Reply](#)

7.

Ok I got everything working like you've explained but this did not stop t-mobile's blocking.

I'm going to keep searching the interweb and see what else I can muster up! 😊

Thanks again!

Bryan [January 3, 2010 at 11:26 pm](#)



[Reply](#)

8.

@Bryan

Like I said, I'm pretty sure it is filtered by IMEI. I believe people have done this with the iPhone, as they take a blackberry IMEI and spoof their iPhone to broadcast this. So when your phone connects to the network of your choice – it sends the known IMEI opposed to the iPhone one.

I've never done this with an iPhone, just read/heard about it. It would theoretically possible to do this with an android device, though not with the method I stated above in this post.

Tim [January 4, 2010 at 1:36 pm](#)



[Reply](#)

9.

I've been using the open source Android Market API <http://bit.ly/dxcwIH> to play around accessing the market via Java. One thing I notice is that if I spoof my Android_id with a nonsensical hex string that I only get back application data for applications that do not have "Copy Protection" on. Is that what you found too?

Maybe there's a pattern that can be used to generate a valid spoof id but I haven't found it yet. You?

Jon [March 19, 2010 at 6:51 pm](#)

10.

[Reply](#)

Illegal???? I think, if changing/spoofing for criminal activities then it is illegal. Carriers clearly abuse that id to rip more money from people. Where is the government to protect us? I wouldn't mind, if there was an alternative, but there is none. How come I pay full price for the smartphone, and can't deny data plan? I want to use local hot spots offered for free by my cable provider to sync phone instead of X fuc...ing G!!!!

user [October 28, 2010 at 10:05 am](#)

[Reply](#)

11.

@user

I'm not one to disagree with you, but as it stands – it's illegal to spoof your IMEI number in the US.

Tim [October 28, 2010 at 4:52 pm](#)

Your Name Email Website

[Strazzere](#)

...it all can be reversed

[Twitter: timstrazz](#)

- Ops, twitter doesn't seem to be responding...

Categories

- [android](#) (98)
- [archos](#) (3)
- [coding](#) (14)
- [dex bytecode](#) (10)
- [life](#) (9)
- [max os x](#) (1)
- [other](#) (15)
- [random](#) (11)
- [reverse engineering](#) (37)
- [reversing](#) (2)
- [secure code](#) (10)
- [Uncategorized](#) (1)
- [updating](#) (8)
- [windows](#) (1)