

Forum:[Hack Forums](#)

Thread: [\[Android\] \[TUT\] how to run backtrack 5 on an android phone \[TUT\] \[Android\]](#)

shonitxx - July 26, 2013, 9:11 pm

credit goes to the owner of www.mytricksclub.com

Download and Run Backtrack on Android Devices:

Requirements:

1. Rooted Android Device with Busybox Installed. Read this tutorial

<https://hackforums.net/showthread.php?tid=3647378>

2. Download some apps from Android Market like Android Terminal Emulator and androidVNC.

<https://play.google.com/store/apps/details?id=jackpal.androidterm>

<https://play.google.com/store/apps/details?id=android.androidVNC>

3. 7zip (for PC), for extracting the files around 3.3 GB free on internal sdcard (/sdcard/)

4. Download Backtrack from here.

<http://www.mediafire.com/?f9gk3p3t9wip5>

File Setup:

You need to do this only once,

1. Download the files from the links provided in this thread.
2. Extract the files using 7zip to a temporary folder (needs 3.3GB free on that drive)
3. Connect your SGS2 to PC and mount USB storage.
4. Create a folder named 'bt' (without quotes) in the root of your sdcard and copy the bt.img in that folder.
5. Also place the file bt5_sgs2_shell_scripts_v2.zip in root of sdcard, this file has to be flashed via recovery.
6. Once you verify that the above is correct then un-mount usb storage.
7. Reboot into recovery and flash the file bt5_sgs2_shell_scripts_v2.zip stored in root of sdcard (or if you are using 4 app then just select the file for flashing and the app will do the rest)
8. once ur phone reboots into OS just check the /sdcard/bt folder.
9. Final directory structure should look like this:
/sdcard/bt/bt /sdcard/bt/bt.img /sdcard/bt/installbt.sh /sdcard/bt/startbt /sdcard/bt/stopbt
10. Once you verify that the above is correct then you can proceed.

Launch BackTrack 5:

Spoiler [\(Click to View\)](#) [img] <http://imageshack.us/photo/my-images/90/ev61.jpg> [/img]

1. Start Terminal Emulator app on your SGS2 and enter the following commands step by step (accept/allow any SuperUser request/popup that you may receive)
su

```
cd/sdcard/bt
sh installbt.sh
startbt
bt
```

2. Now you are in BackTrack5 shell.

3. To launch GUI (vncserver) enter the command ui.

Spoiler ([Click to View](#)) [img] <http://imageshack.us/photo/my-images/801/9q5p.jpg> [/img]

now note the number N shown localhost:N

e.g. as u can see from the above image that "New 'X' desktop is localhost:1", so N=1
the vncserver is running at (5900 + N, N=1 ; so server port is 5901)

4. Now launch androidVNC app on phone and fill in the details as follows:

Nick : bt
Address : 127.0.0.1
Port : 5901
Password : 12345678
Username : <leave it blank>
Color Format : 24-bit color (4 bpp)

Spoiler ([Click to View](#)) [img] <http://imageshack.us/photo/my-images/14/4k5o.jpg> [/img]

Inside vnc window select input mode (i personally recommend the following)
TouchPad (here your screen works like a big touchpad use it to navigate mouse.)

5. Then press connect, now you are in BackTrack GUI!

6.if you want to exit/close BT5 then u need to follow these steps:

close the androidVNC app (Menu > Disconnect)
Go back into Terminal Emulator app and enter the following commands
you should be at this shell root@localhost:~#
killui
exit

now you will get back to this shell> #
now enter the following commands to stop bt and exit
stopbt
exit
exit

you can now exit the Terminal Emulator app
i would also recommend that u reboot your android phone.

researchchem - March 15, 2014, 6:04 am

A quick question does the wifi drivers work correctly ?