Logical Forensics of an Android Device using AFLogical

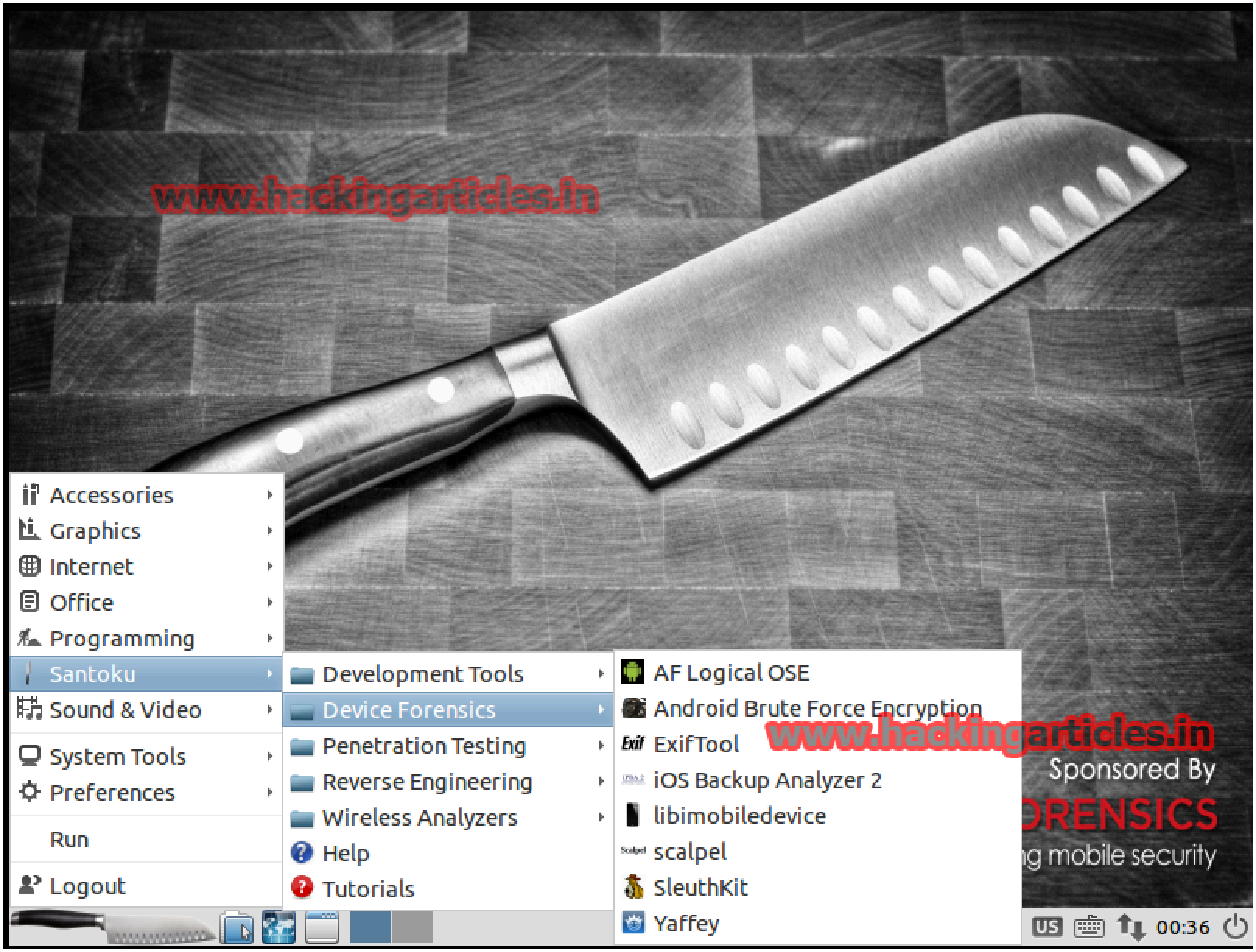
October 6, 2015 By Raj Chandel

First need to install SANTOKU tool kit. How to install it read this article given below

http://www.hackingarticles.in/santoku-linux-overview-of-mobile-forensics-operating-system/

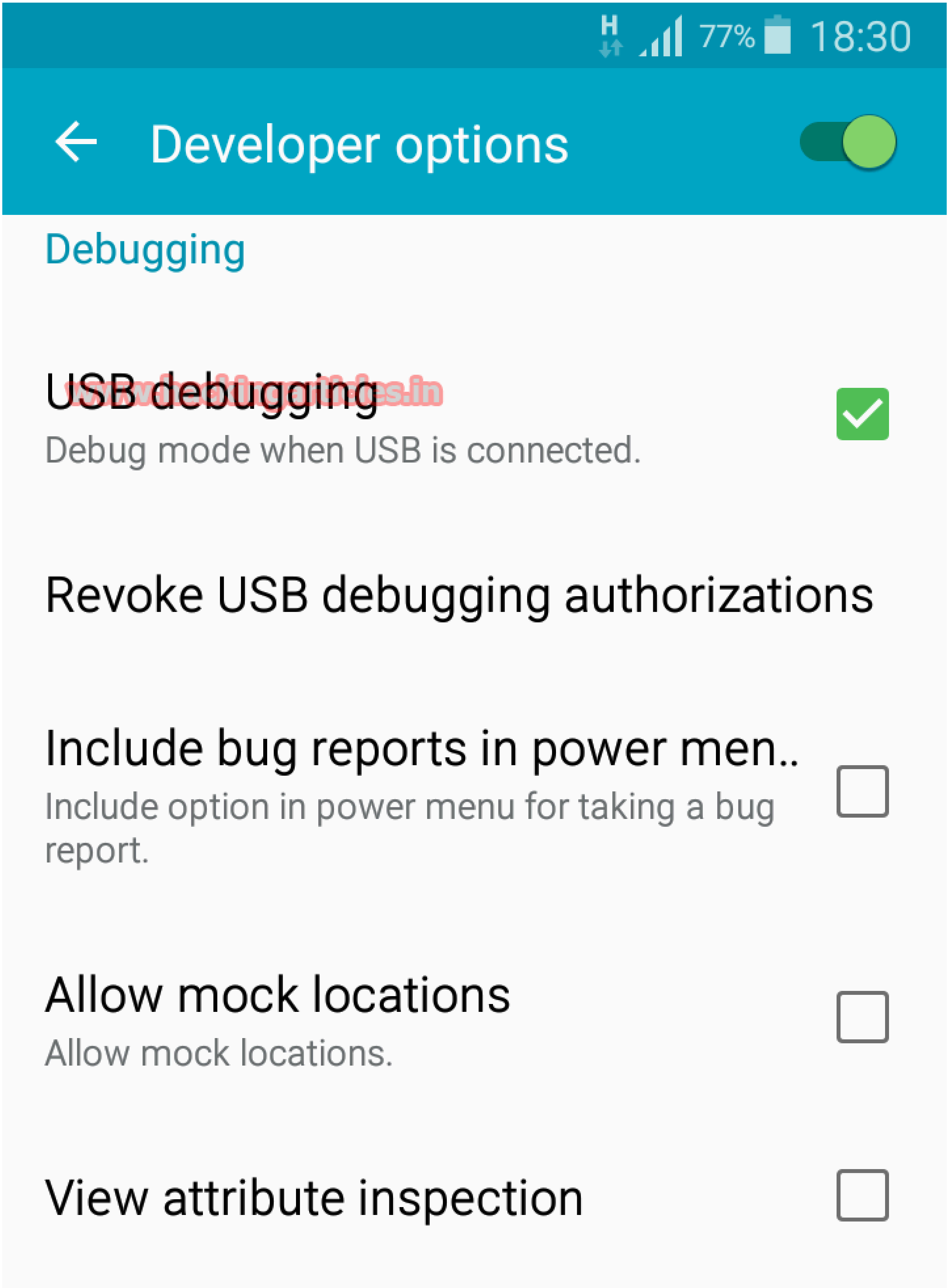
Note : You need an Android mobile device with USB debugging on

Now, click bottom left of your conputer screeen select SANTOKU then Device Forensics and click on AF Logical OSE.



Note : make sure your android device is connected to computer via USB.

Enable USB debugging on your device. For Android 3.x and below, go to **Settings –> Applications –> Development**, then check '**USB debugging**'.



Developer options

Debugging

USB debugging ☑

Debug mode when USB is connected.

Revoke USB debugging authorizations

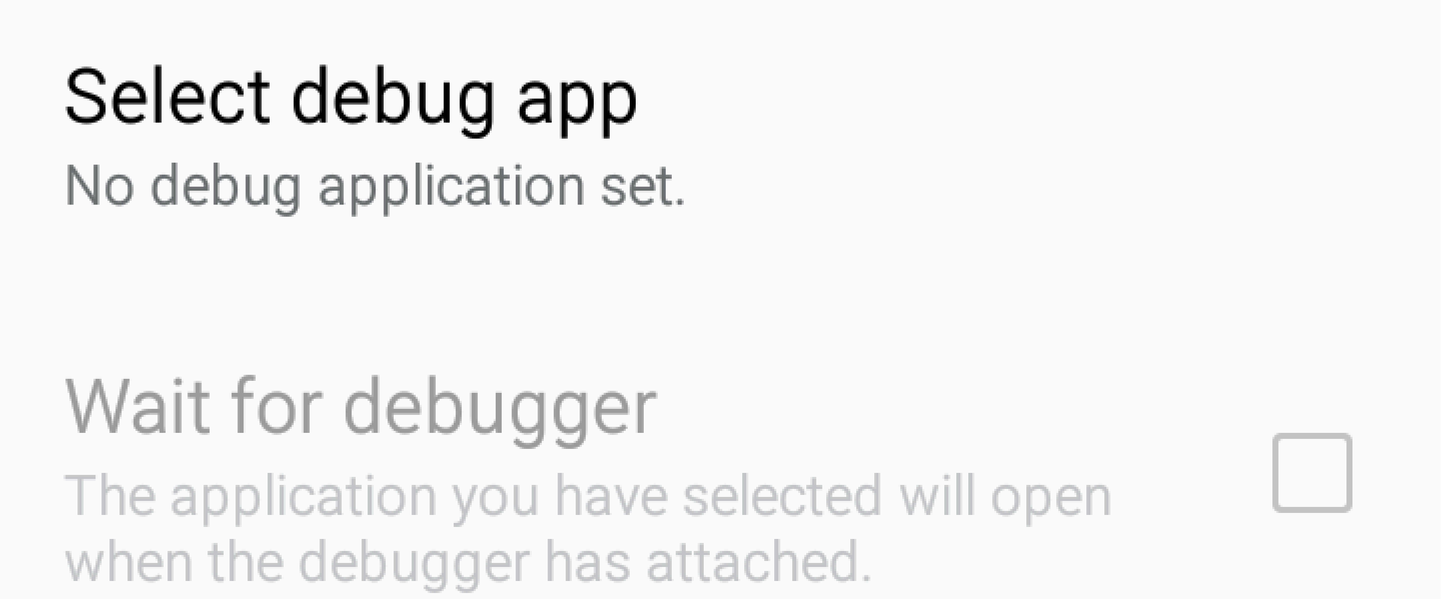
Include bug reports in power men.. □

Include option in power menu for taking a bug report.

Allow mock locations □

Allow mock locations.

View attribute inspection □



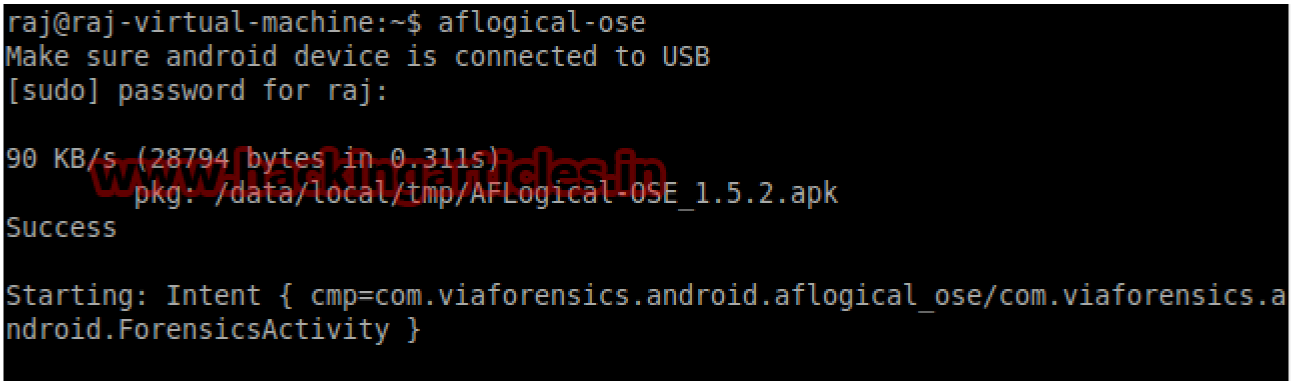
Select debug app

No debug application set.

Wait for debugger

The application you have selected will open when the debugger has attached. □

Now you will get a Terminal, In terminal type : **aflogical-ose** It will show you the success message on the terminal.

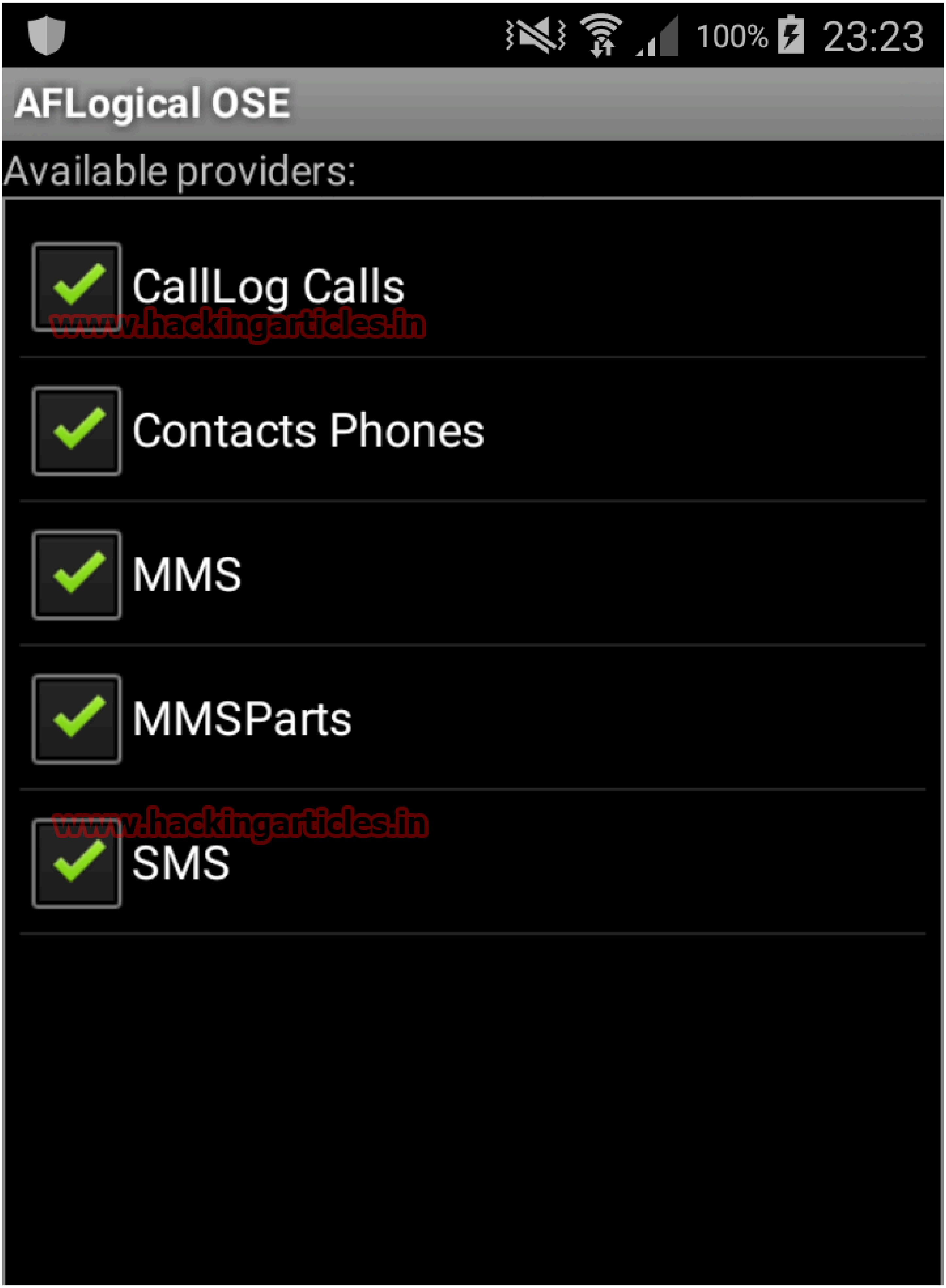


```
raj@raj-virtual-machine:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for raj:

90 KB/s (28794 bytes in 0.311s)
        pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success

Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.a
ndroid.ForensicsActivity }
```

ON your mobile screen you will see couple of options like **Call log, MMS** etc, select the option which you want to extract and then click on **Capture.** (I have selected all the options as you can see below).



AFLogical OSE

Available providers:

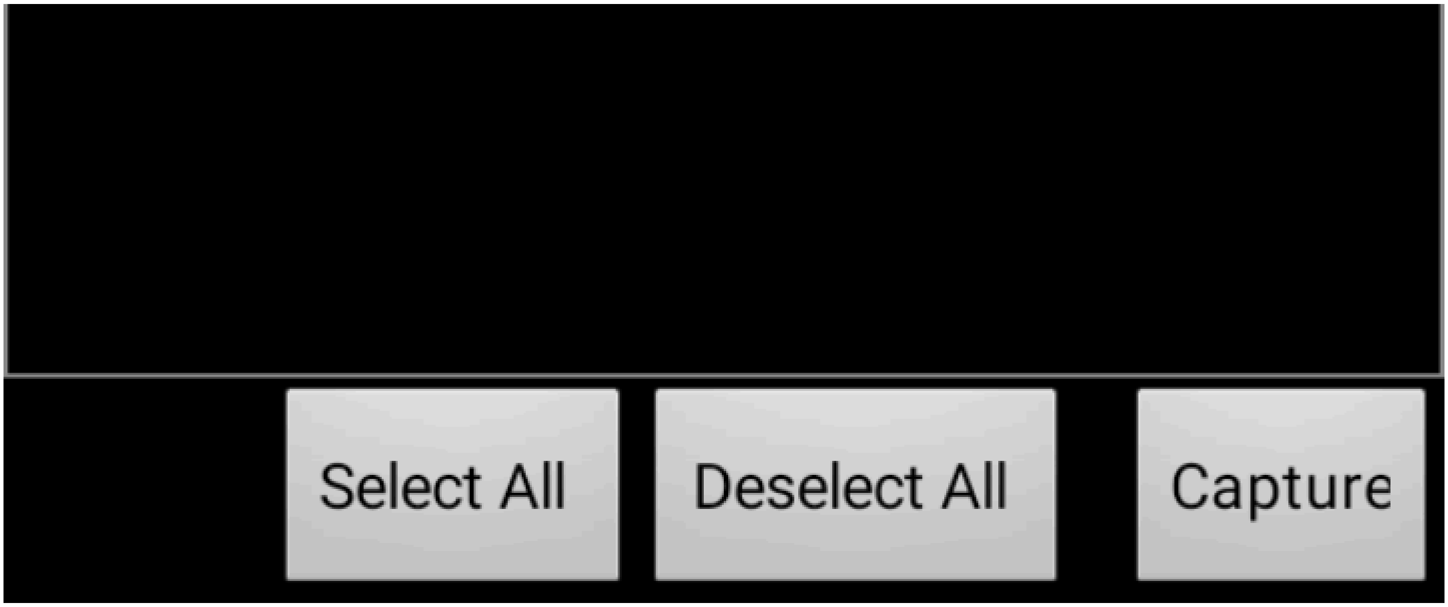
☑ CallLog Calls

☑ Contacts Phones

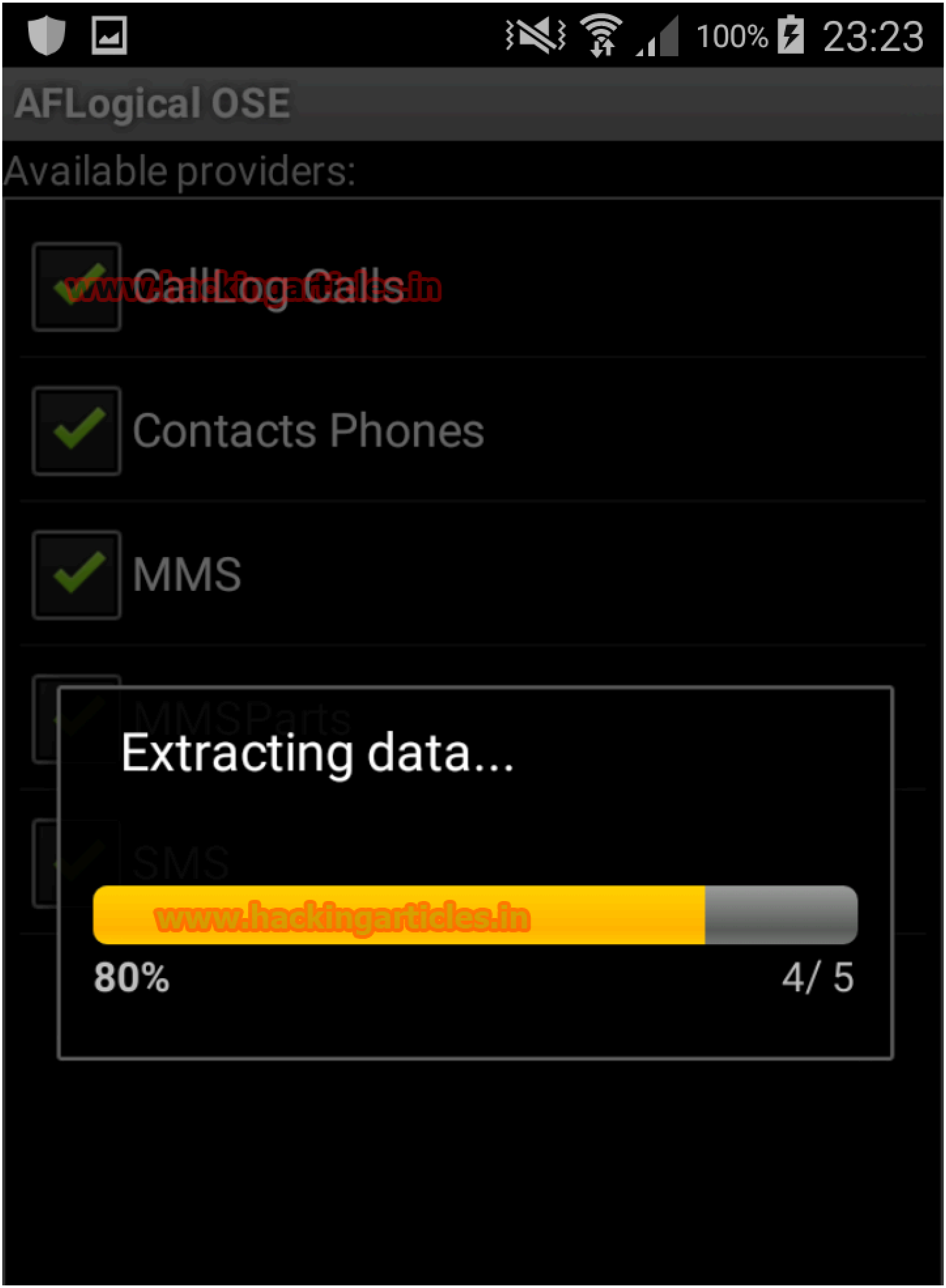
☑ MMS

☑ MMSParts

☑ SMS



Now on your mobile screen you will see the **Extracting Data** as shown in Image.



AFLogical OSE

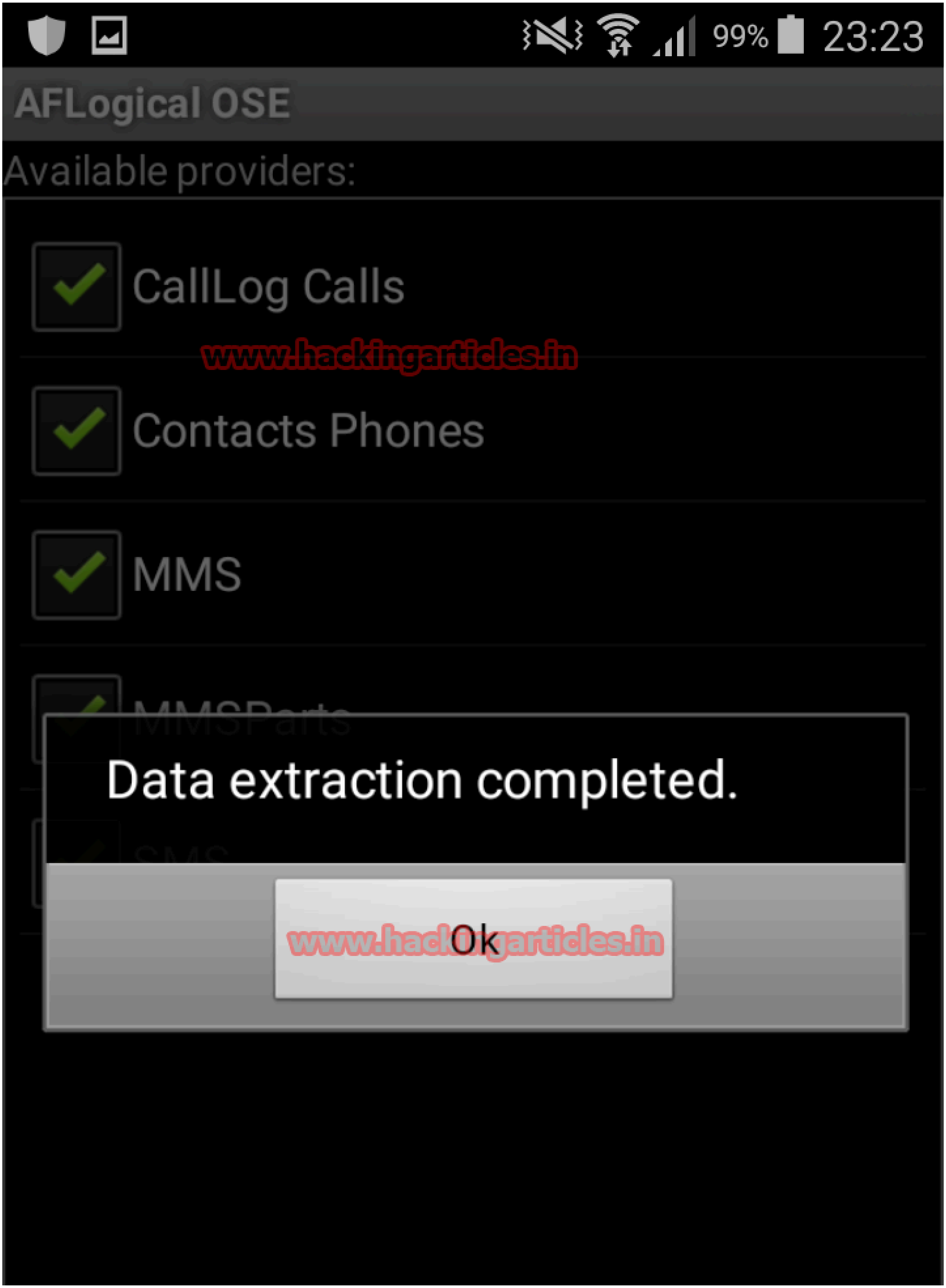
Available providers:

- ☑ CallLog Calls
- ☑ Contacts Phones
- ☑ MMS
- ☑ MMSParts
- ☑ SMS

Extracting data...

80% 4/ 5

Select All
Deselect All
Capture



AFLogical OSE

Available providers:

☑ CallLog Calls

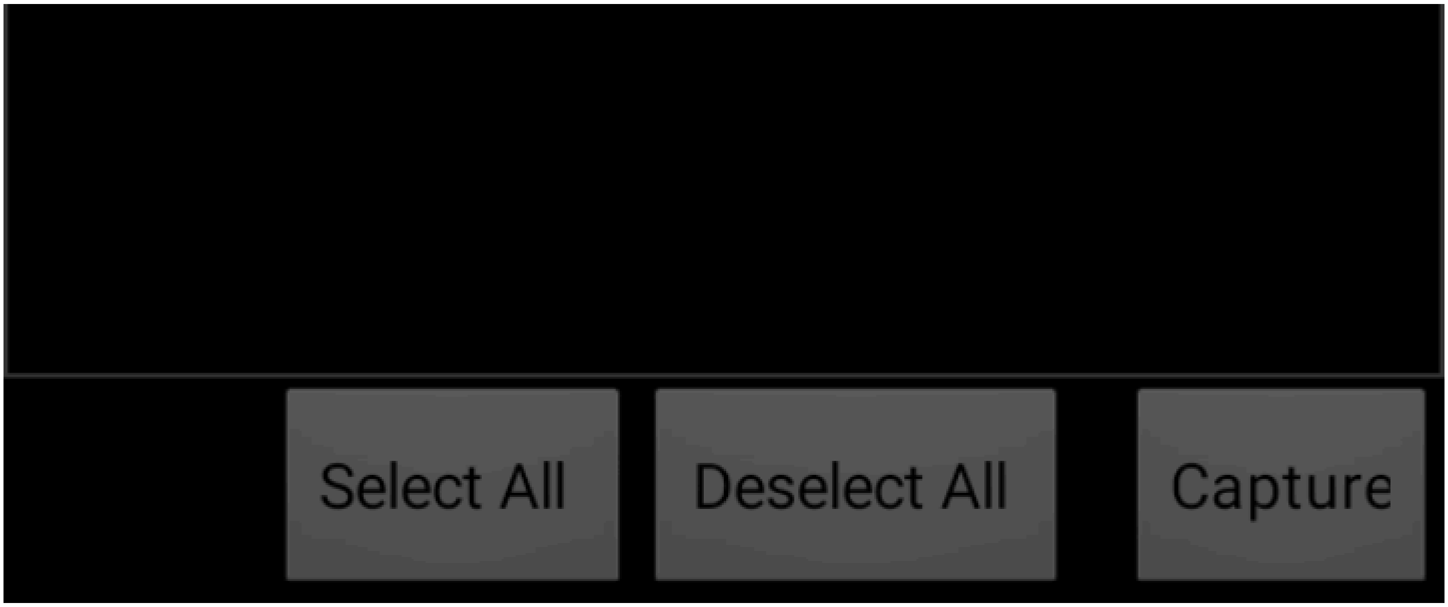
☑ Contacts Phones

☑ MMS

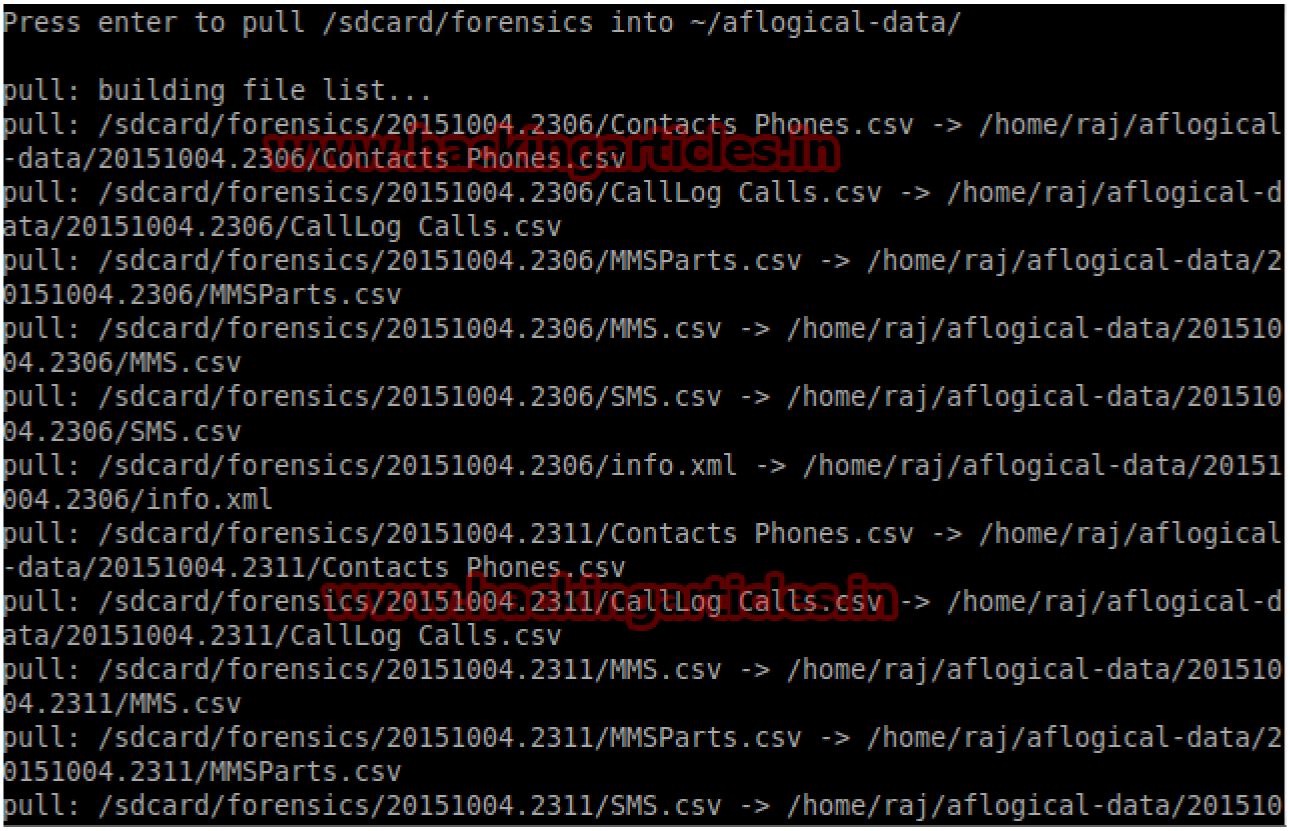
☑ MMSParts

☑ SMS

Data extraction completed.

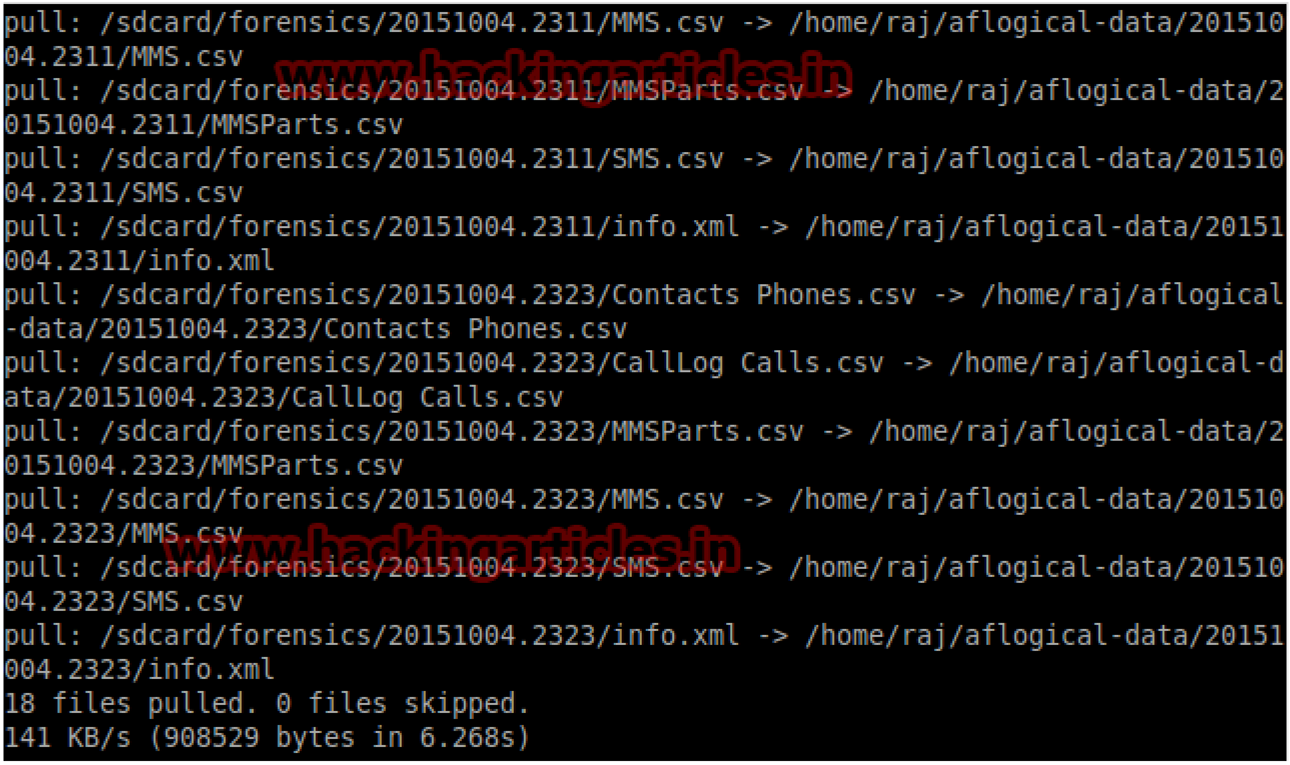


In terminal press **Enter** and now it will save the data and make a new folder in SD card by the name of **Forensics .**



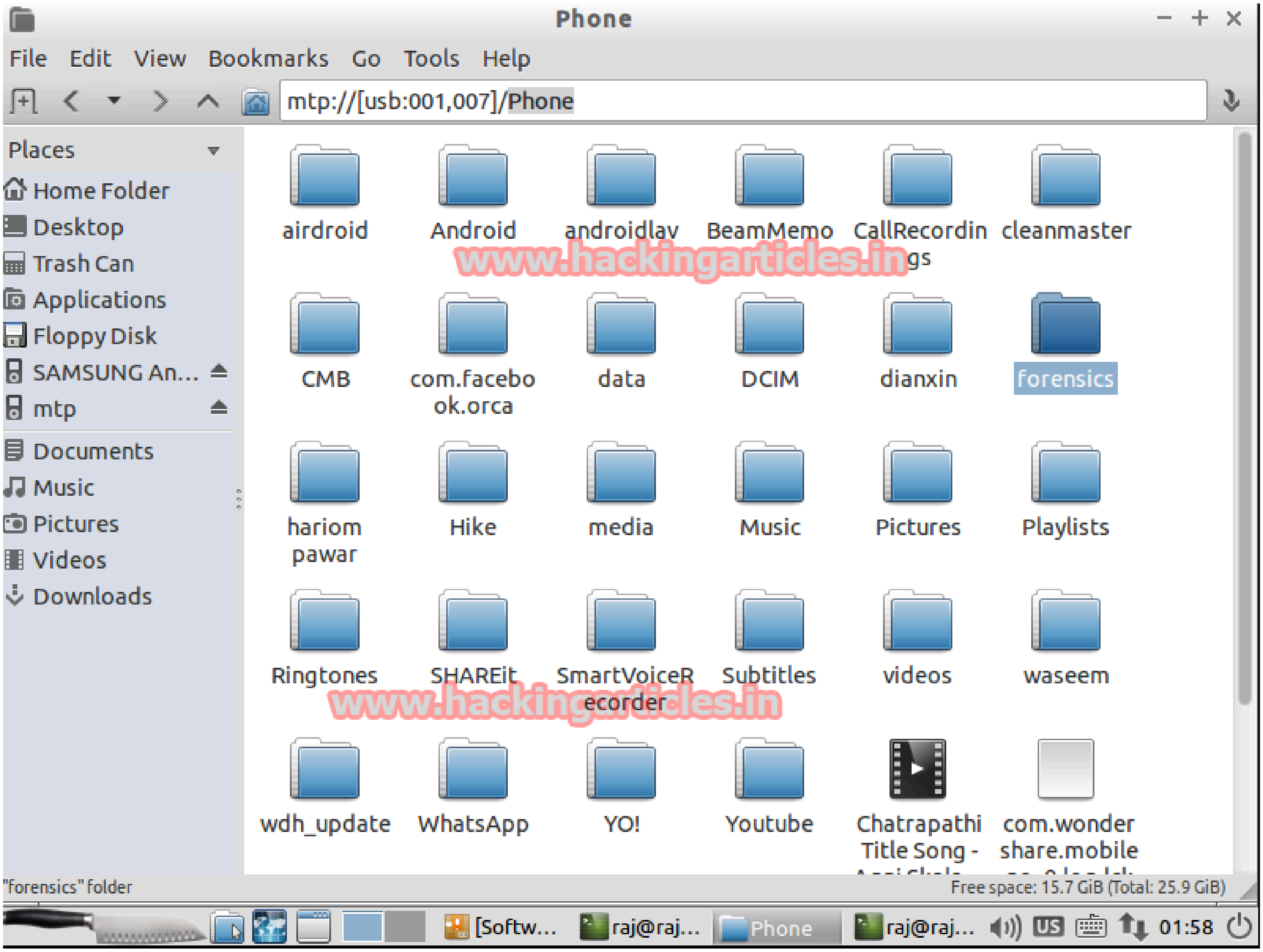
```
Press enter to pull /sdcard/forensics into ~/aflogical-data/

pull: building file list...
pull: /sdcard/forensics/20151004.2306/Contacts Phones.csv -> /home/raj/aflogical
-data/20151004.2306/Contacts Phones.csv
pull: /sdcard/forensics/20151004.2306/CallLog Calls.csv -> /home/raj/aflogical-d
ata/20151004.2306/CallLog Calls.csv
pull: /sdcard/forensics/20151004.2306/MMSParts.csv -> /home/raj/aflogical-data/2
0151004.2306/MMSParts.csv
pull: /sdcard/forensics/20151004.2306/MMS.csv -> /home/raj/aflogical-data/201510
04.2306/MMS.csv
pull: /sdcard/forensics/20151004.2306/SMS.csv -> /home/raj/aflogical-data/201510
04.2306/SMS.csv
pull: /sdcard/forensics/20151004.2306/info.xml -> /home/raj/aflogical-data/20151
004.2306/info.xml
pull: /sdcard/forensics/20151004.2311/Contacts Phones.csv -> /home/raj/aflogical
-data/20151004.2311/Contacts Phones.csv
pull: /sdcard/forensics/20151004.2311/CallLog Calls.csv -> /home/raj/aflogical-d
ata/20151004.2311/CallLog Calls.csv
pull: /sdcard/forensics/20151004.2311/MMS.csv -> /home/raj/aflogical-data/201510
04.2311/MMS.csv
pull: /sdcard/forensics/20151004.2311/MMSParts.csv -> /home/raj/aflogical-data/2
0151004.2311/MMSParts.csv
pull: /sdcard/forensics/20151004.2311/SMS.csv -> /home/raj/aflogical-data/201510
```

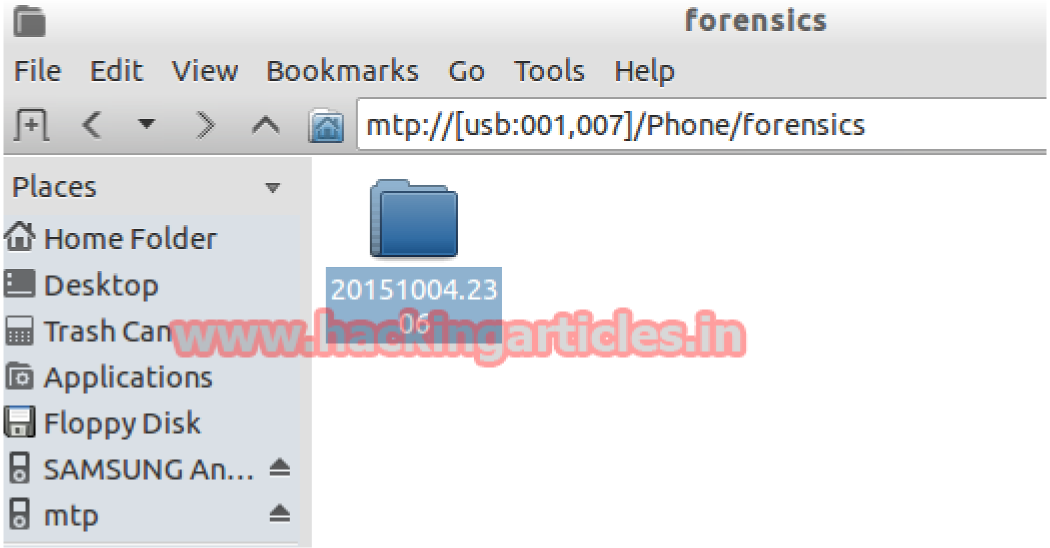


```
pull: /sdcard/forensics/20151004.2311/MMS.csv -> /home/raj/aflogical-data/201510
04.2311/MMS.csv
pull: /sdcard/forensics/20151004.2311/MMSParts.csv -> /home/raj/aflogical-data/2
0151004.2311/MMSParts.csv
pull: /sdcard/forensics/20151004.2311/SMS.csv -> /home/raj/aflogical-data/201510
04.2311/SMS.csv
pull: /sdcard/forensics/20151004.2311/info.xml -> /home/raj/aflogical-data/20151
004.2311/info.xml
pull: /sdcard/forensics/20151004.2323/Contacts Phones.csv -> /home/raj/aflogical
-data/20151004.2323/Contacts Phones.csv
pull: /sdcard/forensics/20151004.2323/CallLog Calls.csv -> /home/raj/aflogical-d
ata/20151004.2323/CallLog Calls.csv
pull: /sdcard/forensics/20151004.2323/MMSParts.csv -> /home/raj/aflogical-data/2
0151004.2323/MMSParts.csv
pull: /sdcard/forensics/20151004.2323/MMS.csv -> /home/raj/aflogical-data/201510
04.2323/MMS.csv
pull: /sdcard/forensics/20151004.2323/SMS.csv -> /home/raj/aflogical-data/201510
04.2323/SMS.csv
pull: /sdcard/forensics/20151004.2323/info.xml -> /home/raj/aflogical-data/20151
004.2323/info.xml
18 files pulled. 0 files skipped.
141 KB/s (908529 bytes in 6.268s)
```

Here is it will look like(I have selected the forensics folder see below)

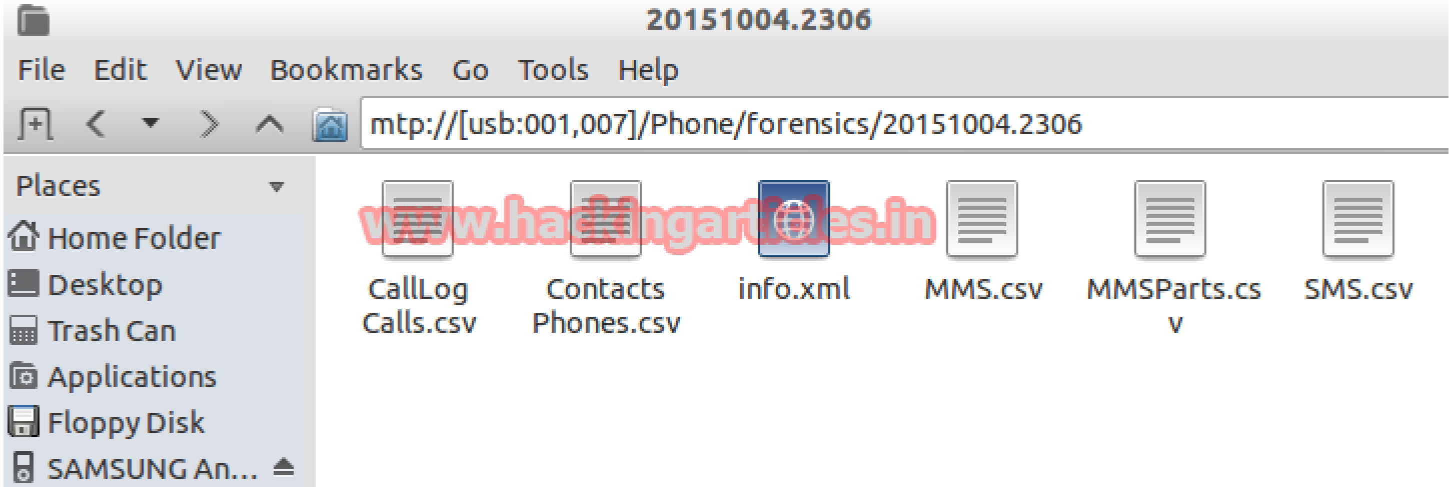


mtp://[usb:001,007]/Phone



mtp://[usb:001,007]/Phone/forensics

Click on **Forensics** folder here you will see the data you have selected.



mtp://[usb:001,007]/Phone/forensics/20151004.2306