

## Module 3: Acquisition with AFLogical

### Objectives

- Create a virtual Android phone in Santoku Linux.
- Perform mobile phone acquisition with AFLogical in Santoku Linux.

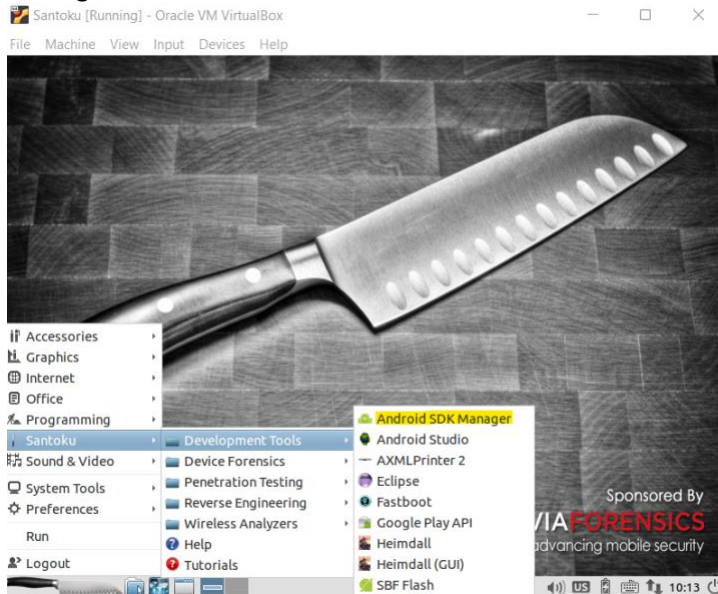
### Task

#### Task 1. Software Preparation

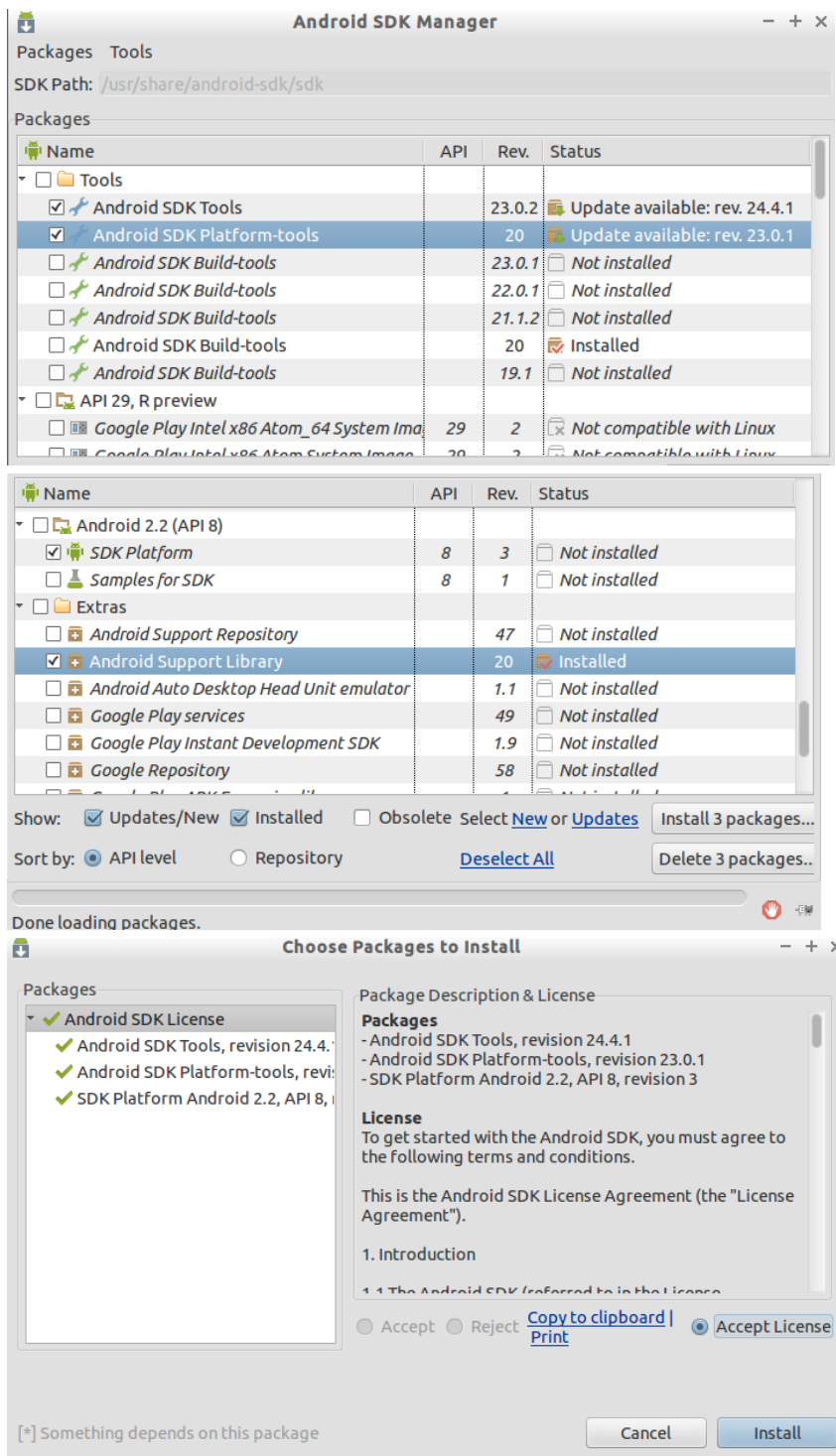
1. Download Santoku. Both the username and password are **santoku**. (Note: lowercase)

#### Task 2. Create a virtual Android device.

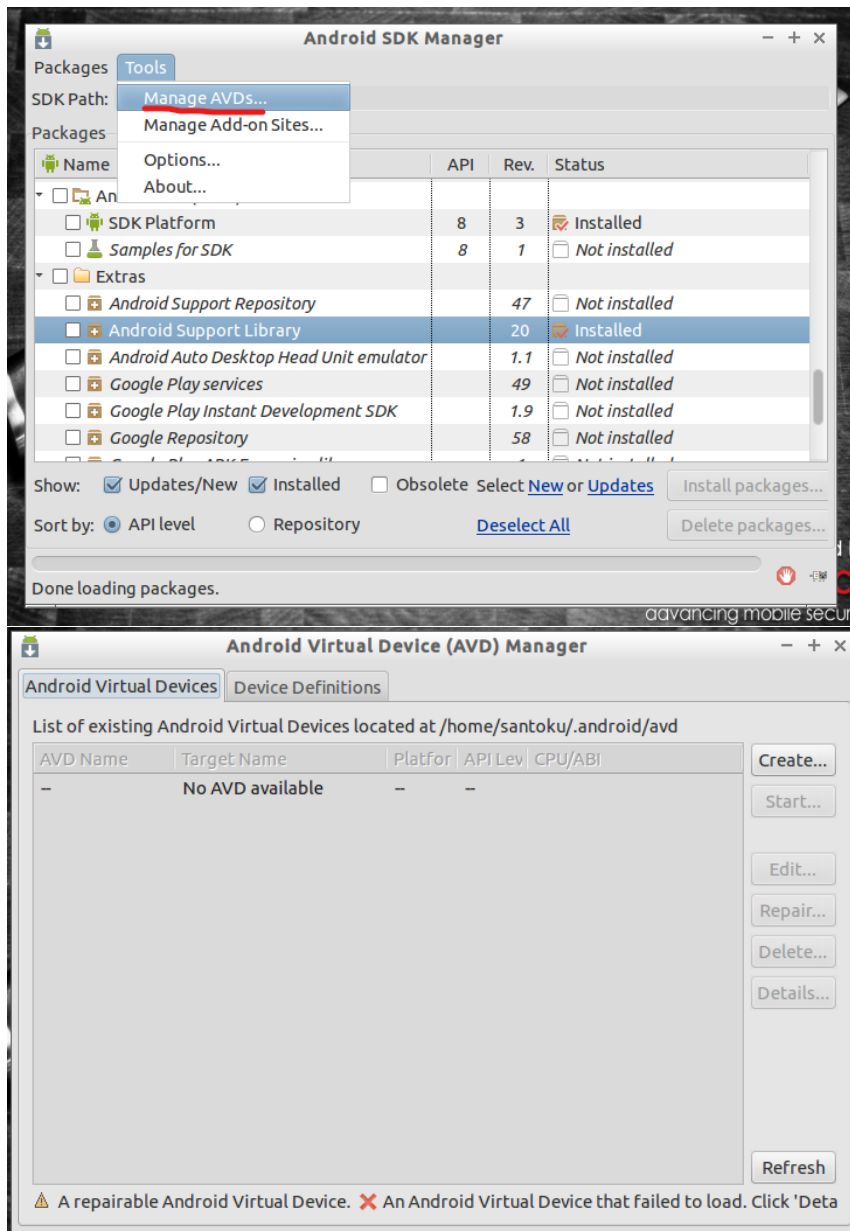
2. Click the 'knife' icon on the left corner, choose 'Santoku' -> 'Development Tools' -> 'Android SDK Manager'.



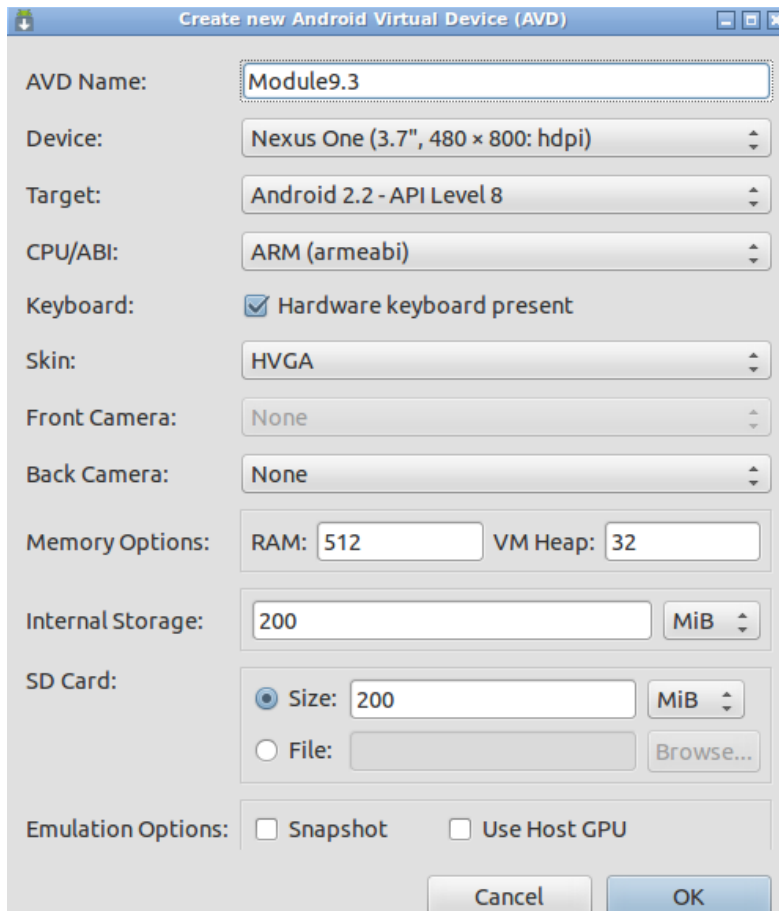
3. After opening the Android SDK Manager, install these four packages. (The virtual machine is installed with these packages, if yours do not have these packages, please install them as marked in the following images).



4. Click on 'Tools' -> 'Manage AVDs...' to open Android Virtual Device (AVD) Manager.

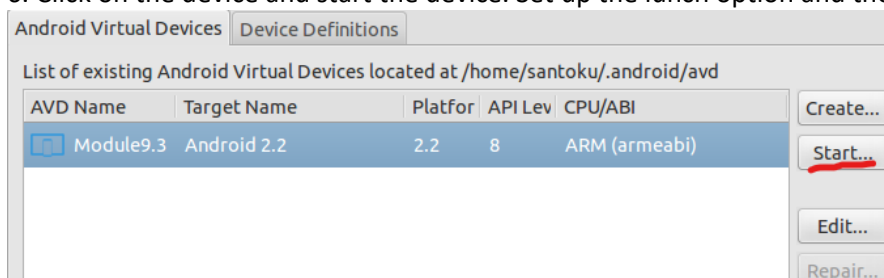


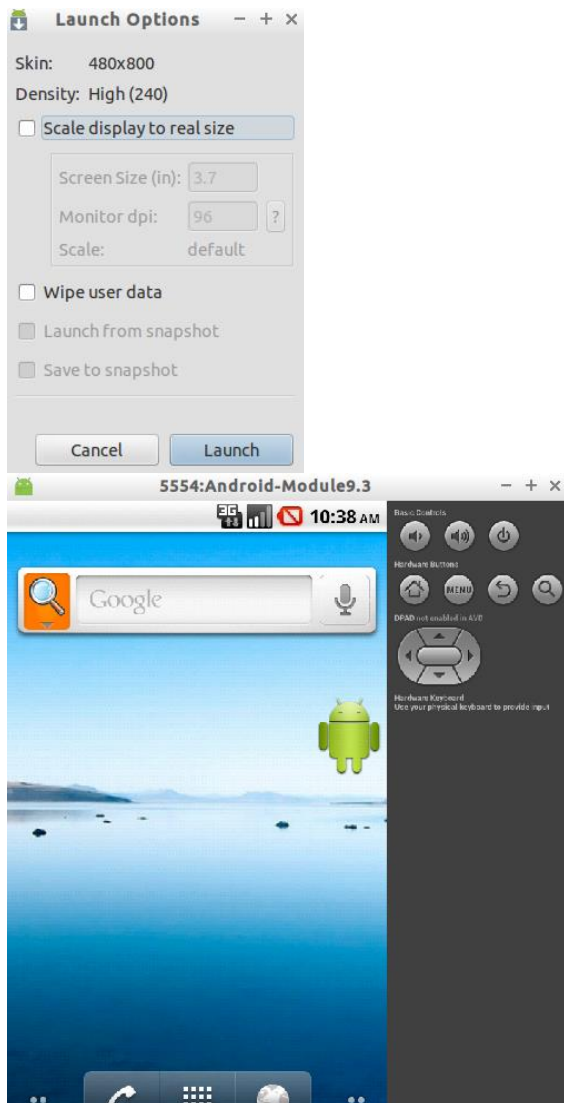
5. Then click on 'Create' on the right column to create a new Android Virtual Device. Follow the screenshot below to set up the device.



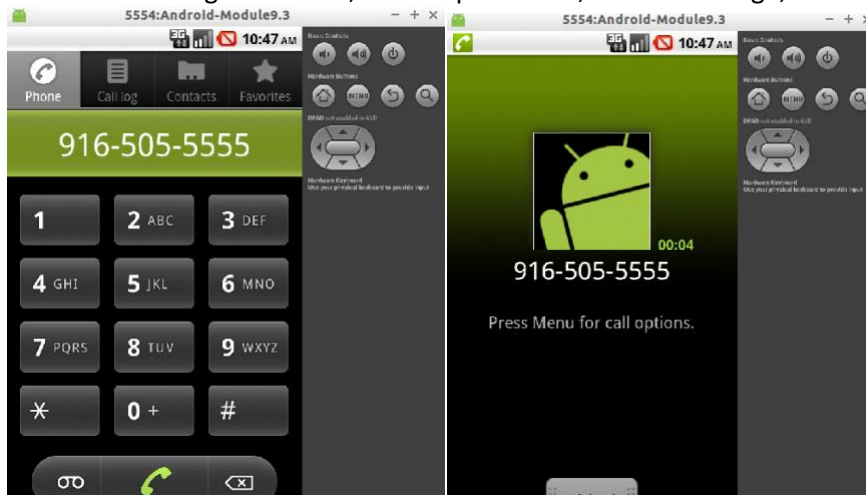
After setting up everything, click on 'OK'.

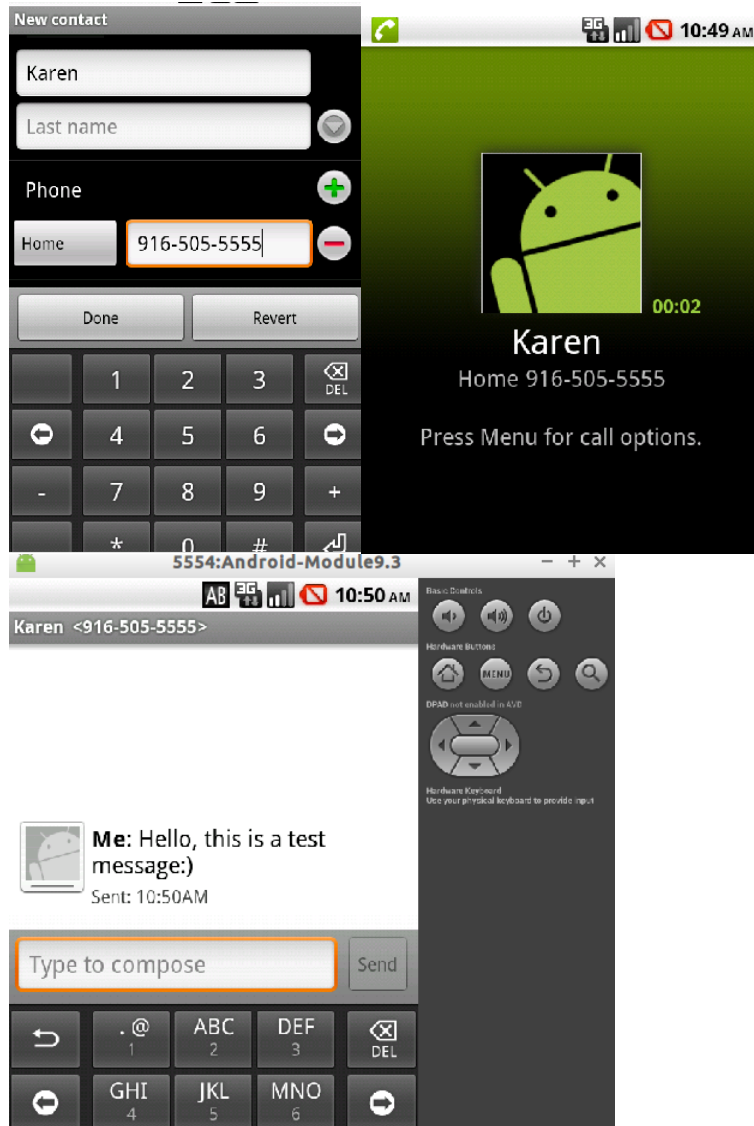
6. Click on the device and start the device. Set up the lunch option and then launch the device.





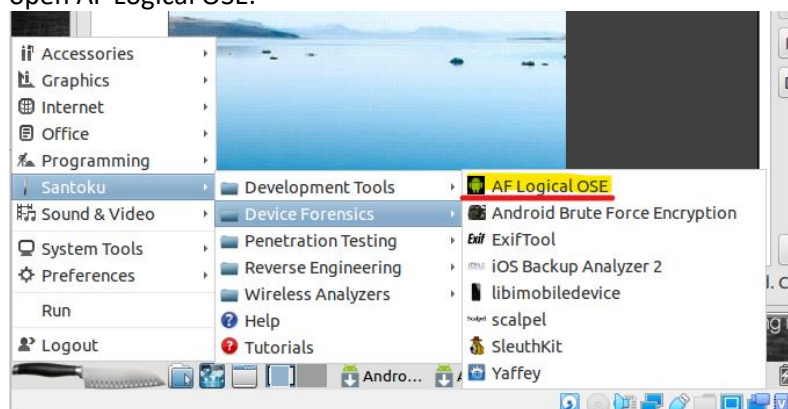
7. After launching the device, make a phone call, send a message, and save a new contact, etc.

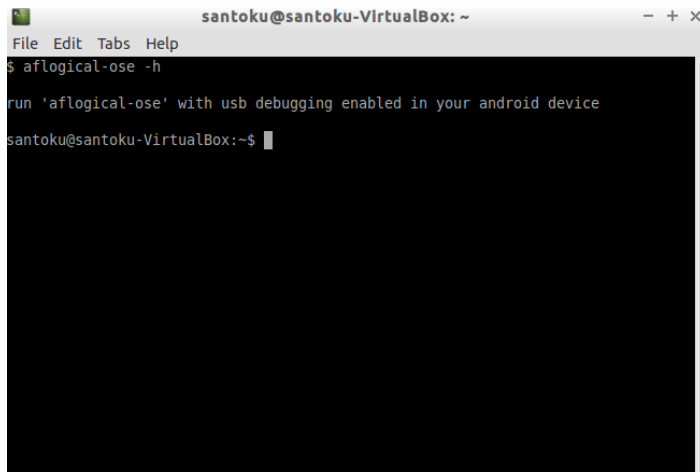




### Task 3. Perform the mobile phone acquisition using AFLogical.

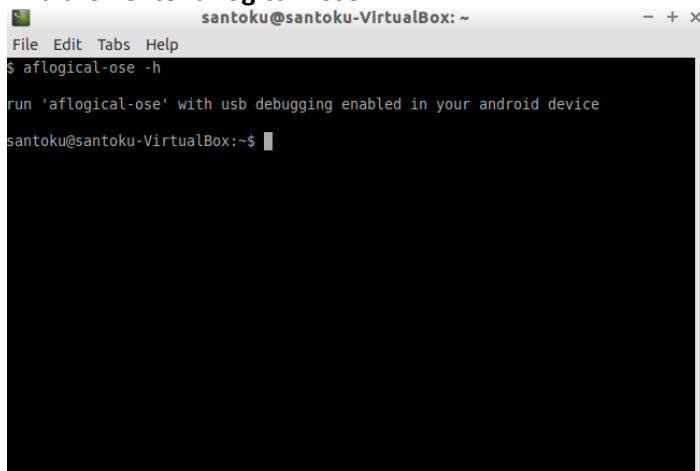
8. Click the knife icon on the left corner, choose 'Santoku' -> 'Device Forensics' -> 'AF Logical OSE' to open AF Logical OSE.



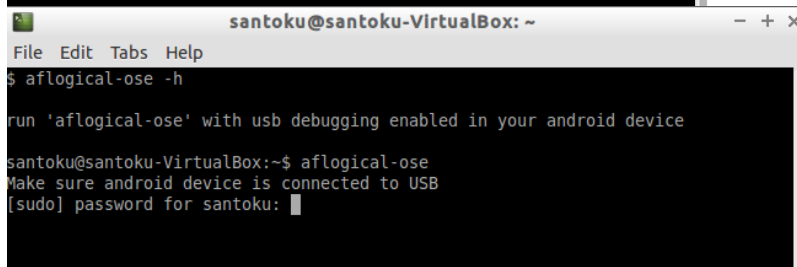


```
santoku@santoku-VirtualBox: ~  
File Edit Tabs Help  
$ aflogical-ose -h  
  
run 'aflogical-ose' with usb debugging enabled in your android device  
santoku@santoku-VirtualBox:~$
```

9. Enter '**aflogical-ose -h**' to start the acquisition and enter the password. **Screenshot**  
And then enter **aflogical -ose**



```
santoku@santoku-VirtualBox: ~  
File Edit Tabs Help  
$ aflogical-ose -h  
  
run 'aflogical-ose' with usb debugging enabled in your android device  
santoku@santoku-VirtualBox:~$
```

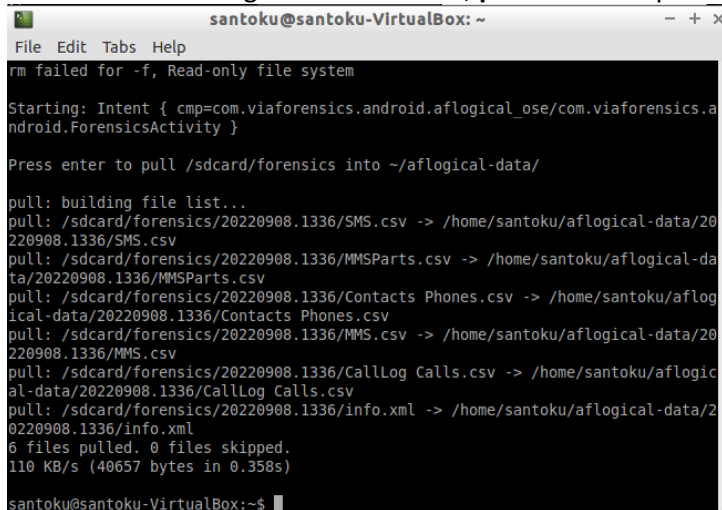


```
santoku@santoku-VirtualBox: ~  
File Edit Tabs Help  
$ aflogical-ose -h  
  
run 'aflogical-ose' with usb debugging enabled in your android device  
santoku@santoku-VirtualBox:~$ aflogical-ose  
Make sure android device is connected to USB  
[sudo] password for santoku:
```

10. After entering the password, go back to the virtual device interface and click 'capture'.

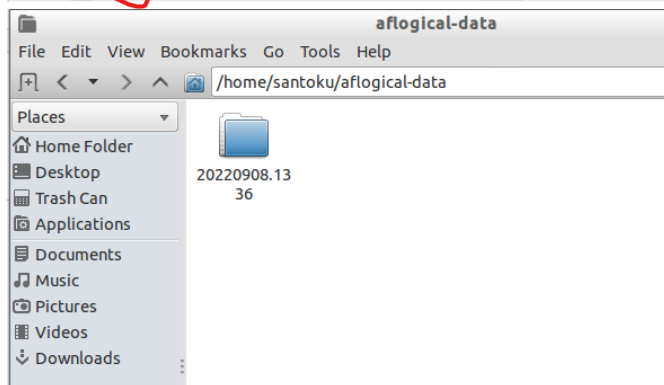
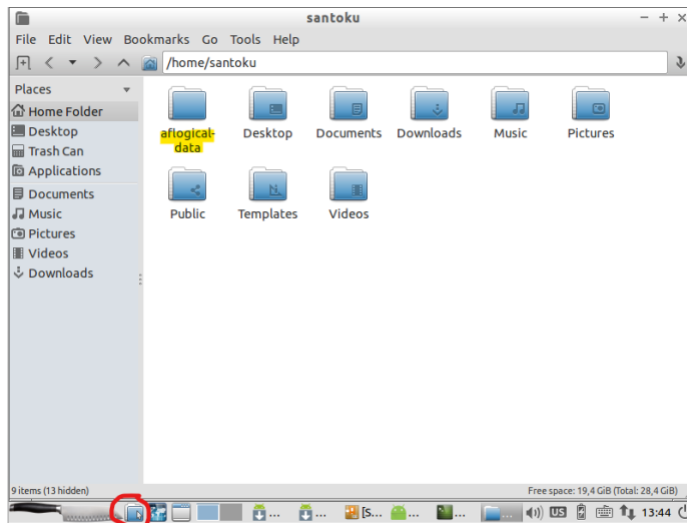


11. Go back to AF logical OSE interface, **press enter** to pull the data.

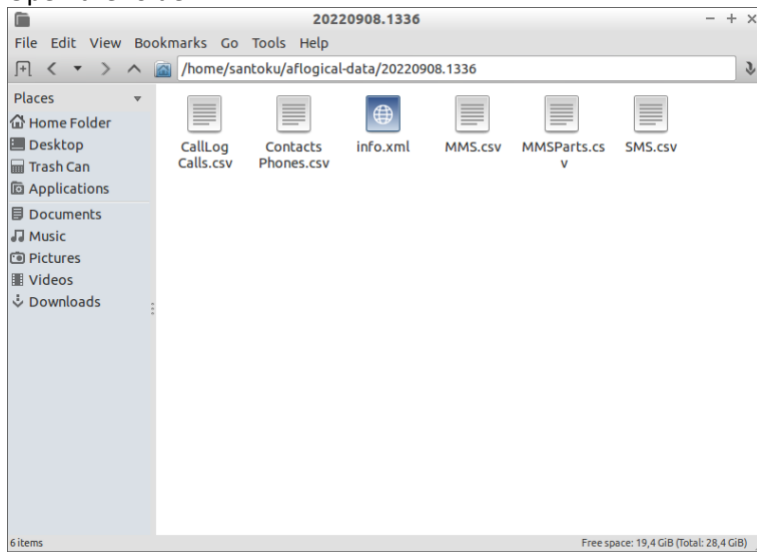


12. Click the folder icon on the bottom column, and double click 'aflogical-data' folder to check all the files pulled from the virtual phone. **Screenshot**





Open the folder.



13. View all the files. **Screenshots**  
Phone calls:

CallLog Calls.csv - Gnumeric

File Edit View Insert Format Tools Statistics Data Help

Sans 10 a a a

A1 ↓ X ✓ ▾ = \_id

	A	B	C	D	E	F	G
1	id	number	date	duration	type	new	name
2	1	9165055555	1662659268316	19	2	1	Karen
3	2	9165055555	1662659367387	18	2	1	Karen
4							
5							
6							
7							
8							
9							
10							
11							
12							

CallLog Calls.csv Sum = 0

### Contacts:

Contacts Phones.csv - Gnumeric

File Edit View Insert Format Tools Statistics Data Help

Sans 10 a a a

A1 ↓ X ✓ ▾ = times\_contacted

	E	F	G	H	I	J	K	L	M	N
1	phonetic	isprimary	label	number	type	last_time_contact	display_i_id		number_key	starred
2			0	916-505	1	1662659388309	Karen		1 5555505619	0
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										

### Message:

SMS.csv - Gnumeric

File Edit View Insert Format Tools Statistics Data Help

Sans 10 a a a

L2 ↓ X ✓ ▾ = Hello, this is a test message:)

	G	H	I	J	K	L	M	N	O	P	Q	R
1	read	status	type	reply_pa	subject	body	service_c	locked	error_co	seen		
2	1	-1	2			Hello, this is a test			0	0	1	
3												
4												
5												
6												
7												

### Deliverable:

You need to submit a lab report to Canvas. (You can submit a report with all the screenshots and questions for activity 8 in one file or you can submit several files for each module). Note: Your lab report should contain two parts.

1) Screenshots (3-4 screenshots in total for this module): Please take screenshot after you open the AFLogical interface and enter the **aflogical -ose** command, step 9. Please submit a screenshot of the aflogical-data folder and the files or folders inside this folder. Please also take some screenshots of the .csv files, as shown in step 13.

2) Please answer the following questions:

1. Which command is used in the module to start the AFLogical forensics?
2. Which folder contains all the files that we pulled from the virtual machine? And what files are in this folder?
3. Please find the phone call logs. (Please provide a screenshot).
4. Please find the message logs. (Please provide a screenshot).
5. Please find the contact list. (Please provide a screenshot).