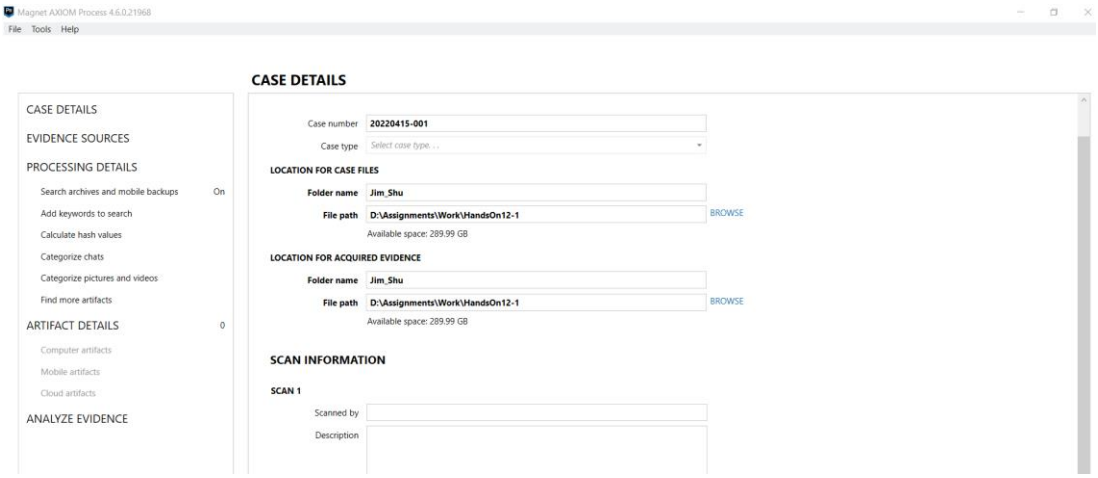
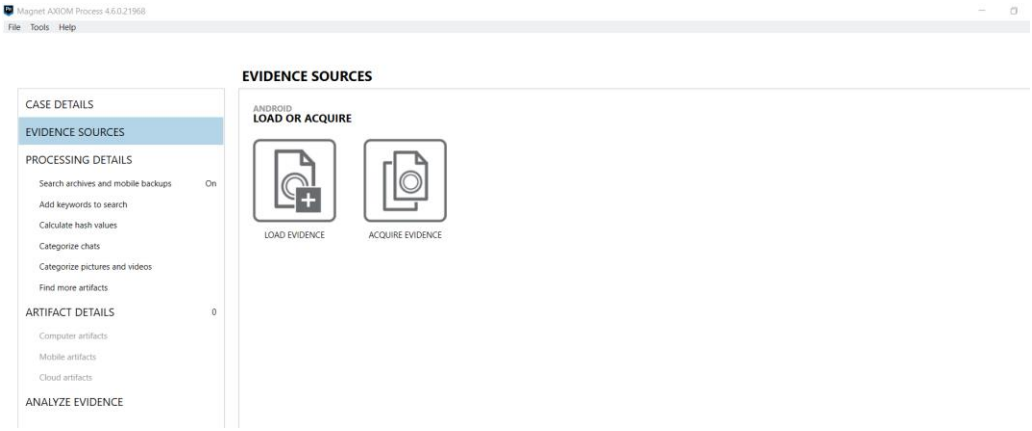
Hands-On Project 12-1

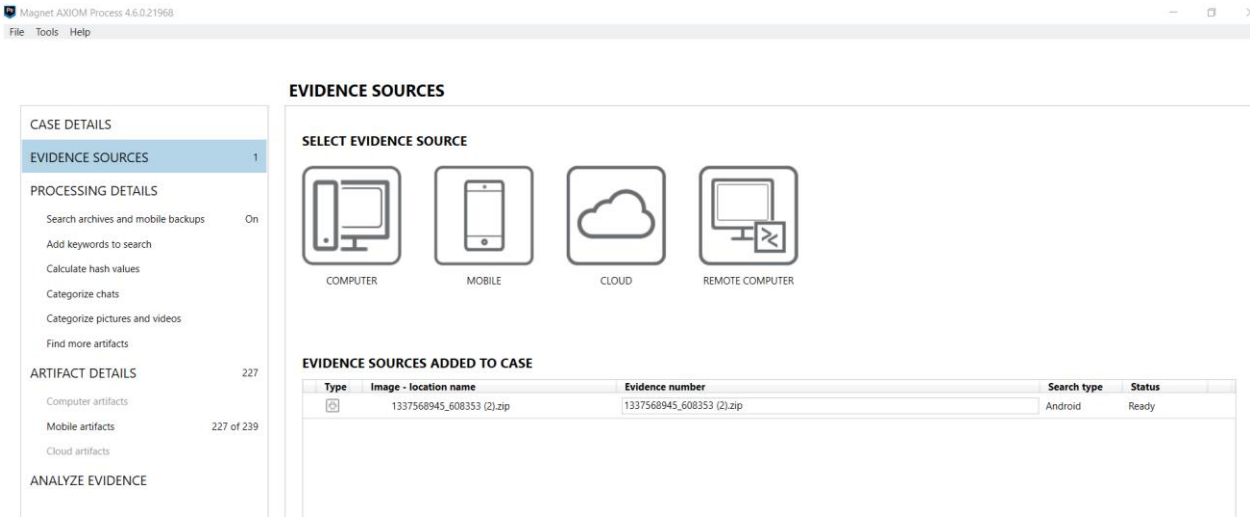
In this project, you're using Magnet AXIOM to examine the image of Jim Shu's cell phone. (Assume someone else did the acquisition.)

1. Start Magnet AXIOM Process and click the CREATE NEW CASE button. In the Case number text box, type today's date followed by a hyphen and the number of the case you're working on that day. In both the LOCATION FOR CASE FILES and LOCATION FOR ACQUIRED EVIDENCE sections, type Jim_Shu in the Folder name text box. In both sections, click the BROWSE button next to the File path text box, navigate to and click your work folder, and click Select Folder. Click the GO TO EVIDENCE SOURCES button.

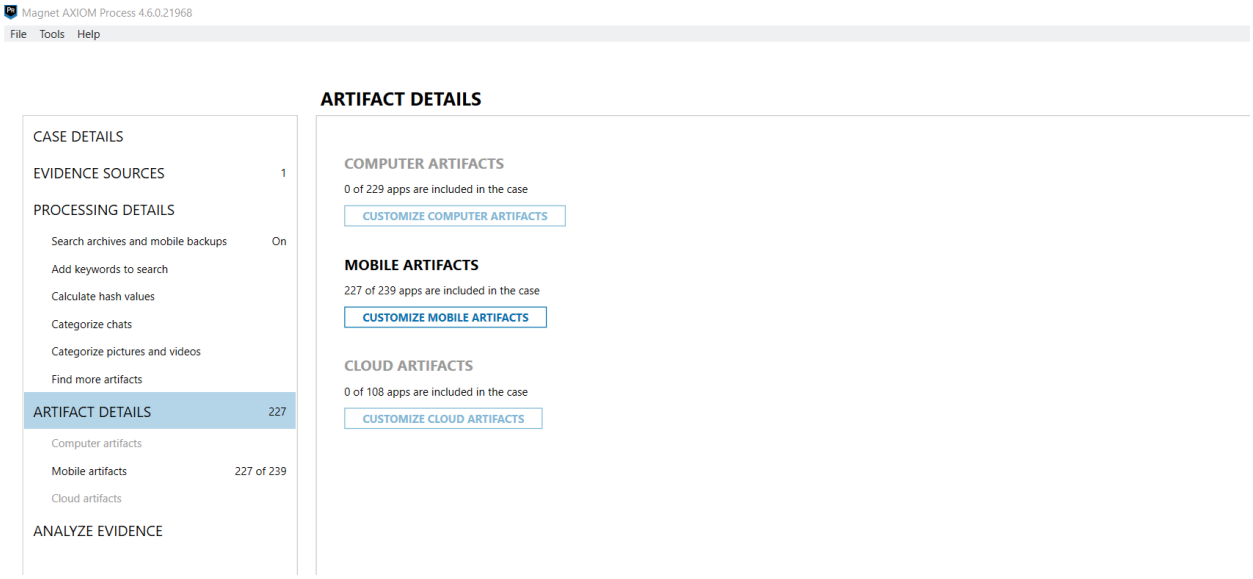


2. In the SELECT EVIDENCE SOURCE section, click the MOBILE icon. In the next window, click ANDROID to specify the type of device you're accessing, and then click NEXT. In the next window, click the LOAD EVIDENCE icon, and then click IMAGE. Browse to and click the TCL Alcatel_JShu.zip file, and then click Open. In the EVIDENCE SOURCES window, click NEXT.

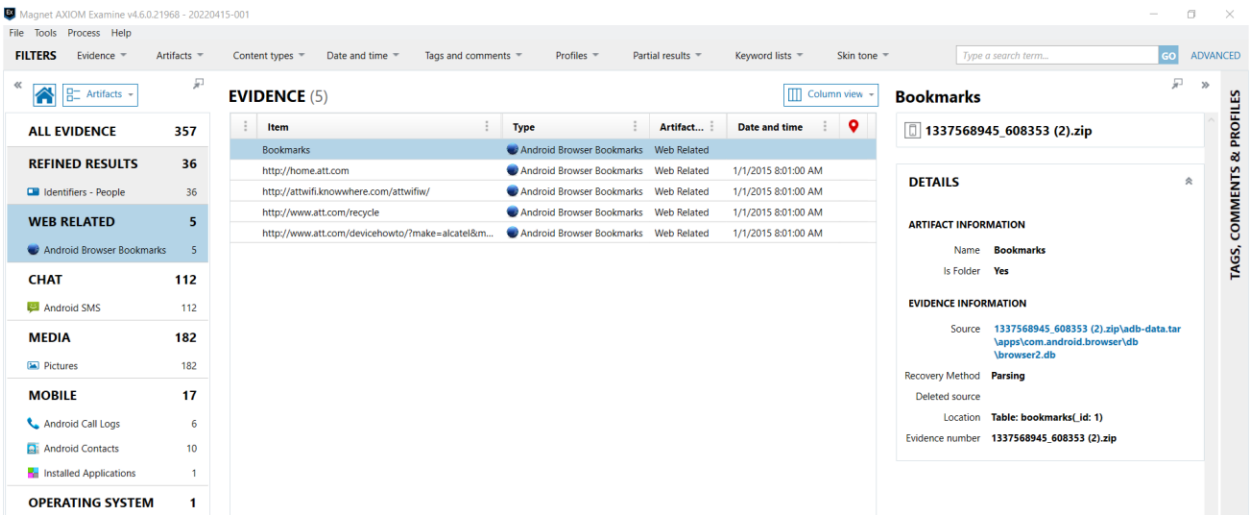




3. Click GO TO PROCESSING DETAILS. In the following windows, click GO TO ARTIFACT DETAILS, GO TO ANALYZE EVIDENCE, and then ANALYZE EVIDENCE to start Magnet AXIOM Examine.



4. Click REFINED RESULTS in the left pane to see the recovered items. Notice that you can also examine evidence in the categories CHAT, EMAIL, WEB RELATED, and MOBILE. Examine the evidence in these categories to see who Jim Shu was in contact with.



5. Write a one- to two-page report summarizing your findings, and exit Magnet AXIOM Examine.

Magnet AXIOM is a trustworthy, field-proven digital forensics solution that lets you recover lost data and analyze digital evidence from mobile, computer, cloud, and vehicle sources all in one case file, with sophisticated analytical tools to help you automatically uncover more case-relevant evidence.

Magnet AXIOM's analytical tools can help you cut through the digital clutter so you can focus on what matters. To identify the evidence you need, use Media Explorer, Cloud Insights Dashboard, Magnet.AI, Connections, Timeline, and other tools.

In one case, examine your evidence.Using an artifact-first approach, recover, analyze, and report data from mobile, computer, cloud, and vehicle sources in a single case file. With Magnet AXIOM, you can easily recover erased data, evaluate digital evidence, make reports, and distribute portable case files.

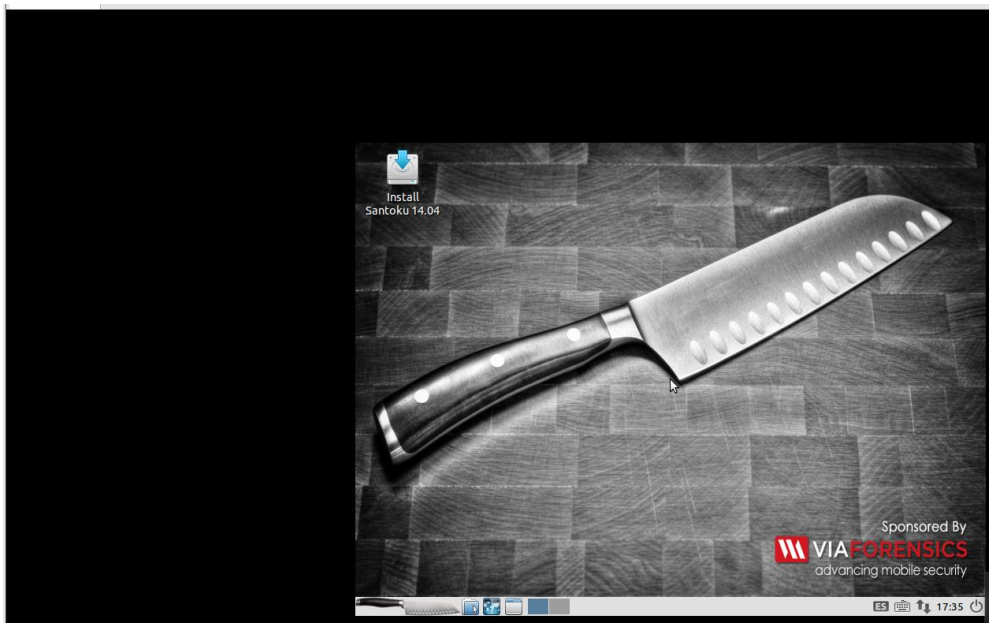
We can get the findings from once mobile devices and what are the thing that can be found which can be seen in the last screenshot.

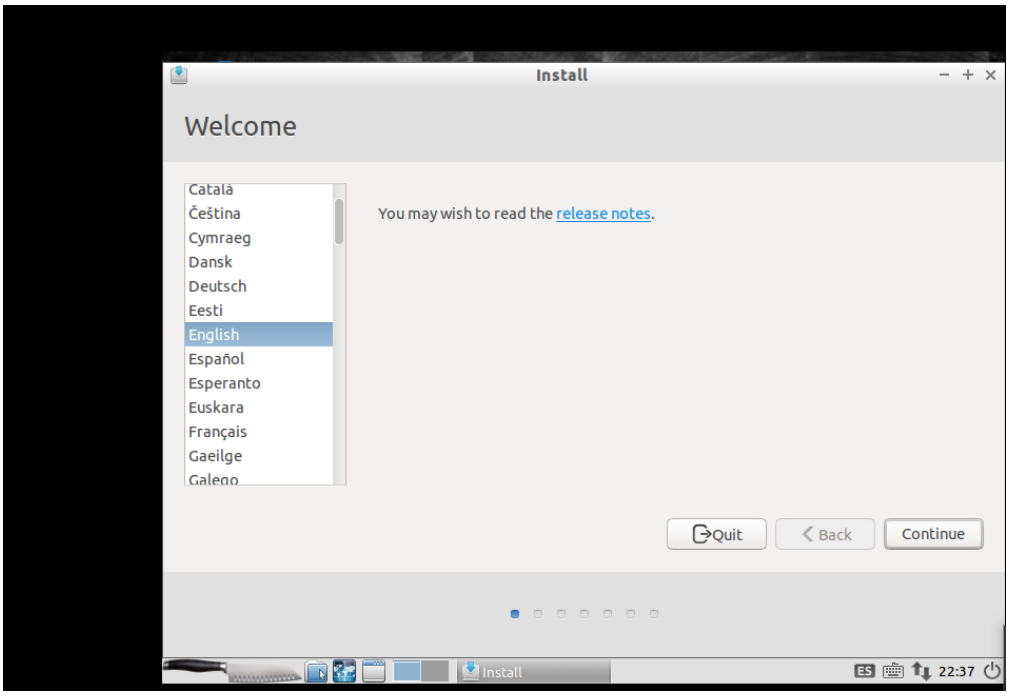
Hands-On Project 12-4

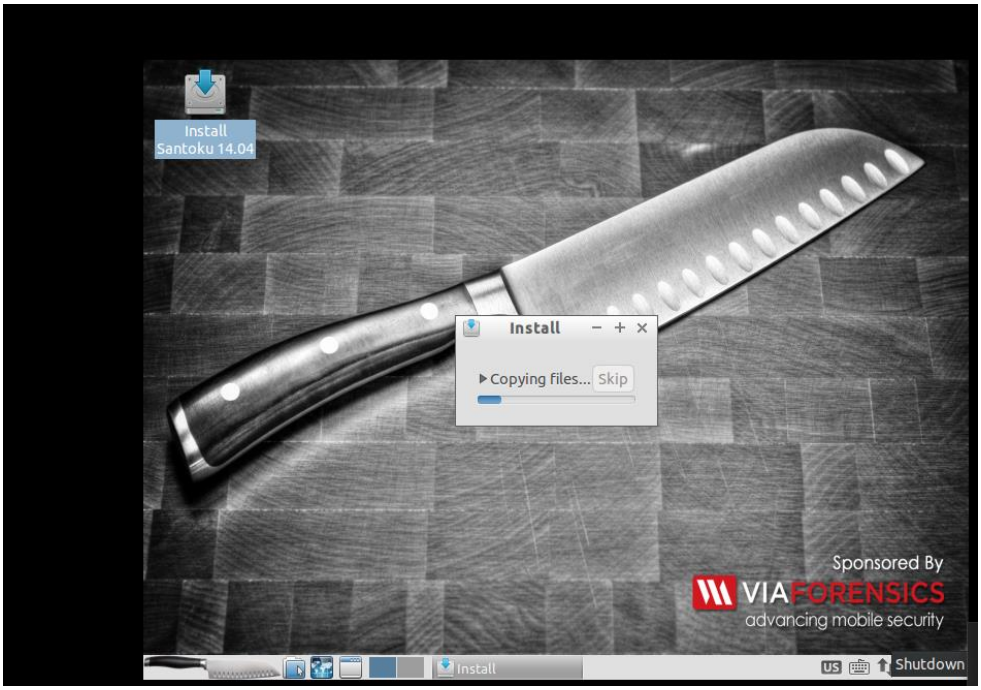
In this project, you download Santoku Linux to create an Android virtual device and then gather data from it. This useful tool gives you a way to experiment with a variety of practice mobile devices.

1. Start a Web browser, go to http://santoku-linux.com/download/, and download the ISO file for Santoku Linux.

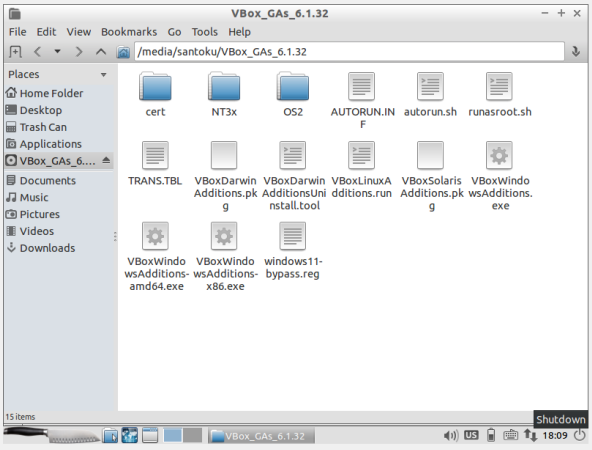
2. Start VirtualBox, and create a virtual machine with at least 4 GB RAM and 30 GB of hard drive storage. Start Santoku Linux, and click the Install Santoku 14.04 icon. When prompted, restart the VM.





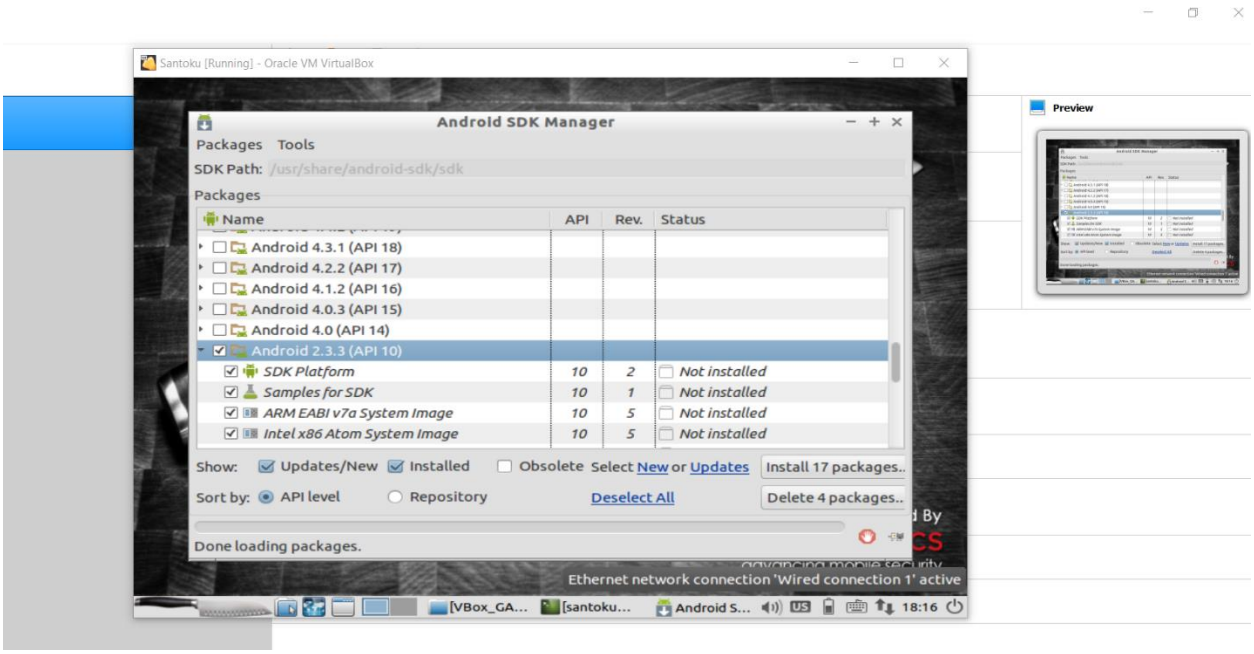


3. When the installation is finished, click Device, Insert Guest Additions CD Image from the menu. When prompted to open the image in File Manager, click OK. Click Start, Accessories, LXTerminal to open a command prompt window. Type cd/media/ username/VBOXADDITIONS_5.1.22_115126 and press Enter, and then type sudo sh ./VBoxLinuxAdditions.run and press Enter. You can then use scaled mode for window sizing to make viewing easier. Click View, Scaled Mode from the menu.

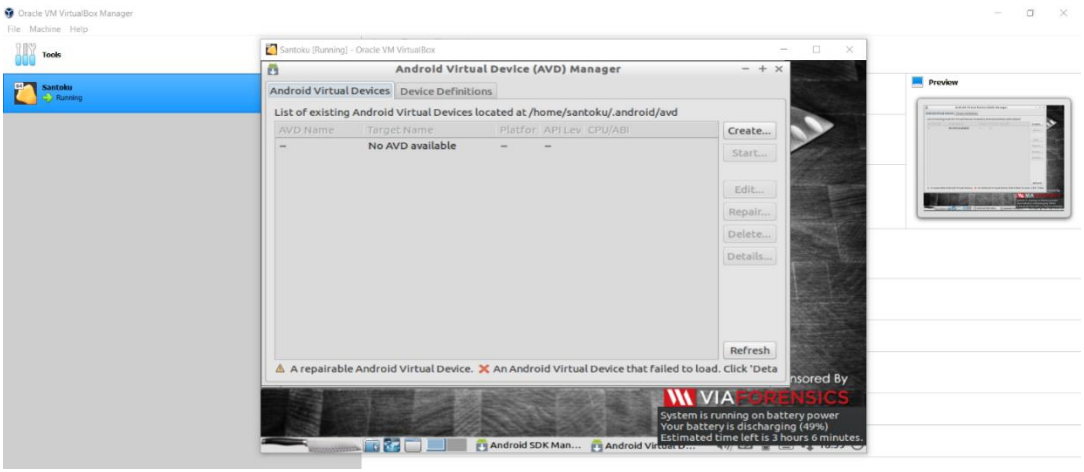


4. Next, you need to create an Android 2.3.3 virtual device (AVD) for making a forensic extraction. Click Start, Santoku, Development Tools, SDK Manager. Santoku downloads the development tools, which might take a few minutes.

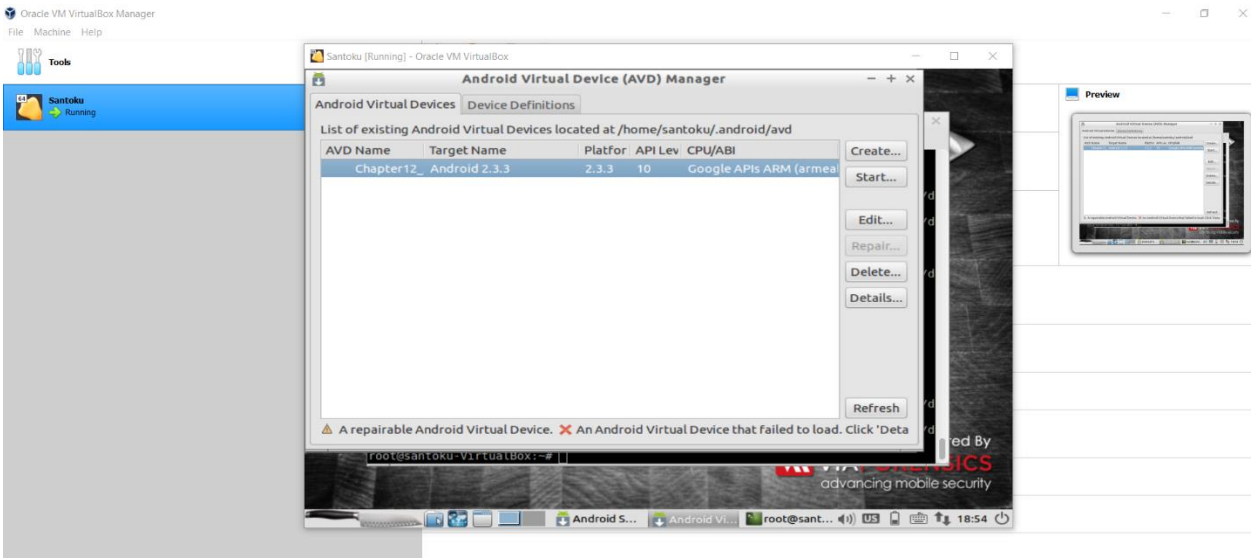
5. In the window that opens, select all the bulleted items under Tools, and then scroll to Android 2.3.3 and select all the bulleted items for Android 2.3.3. At the lower right, click the Install 17 packages button. In the next window, click the Accept License option button and then the Install button. Click OK. Close SDK Manager and reopen it.



6. Click Tools, Manage AVDs from the menu, and then click the Create button at the upper right. For the name, type Chapter12_AVD, and for the device type, click Nexus One. Click the CPU/ABI list arrow, and click Google APIs ARM. For the skin type, click WVGA 800. Enter 100 GB for the siz of the SD card, and then click OK.



7. The next window shows the details of the new AVD. Click OK to open the window shown in Figure 12-7.



8. Click to select the Chapter12_AVD virtual device, and then click the Start button. In the window that opens, click Launch. (Note: This window might take a few minutes to open.)

9. APK files contain source data for Android applications, to install one for collecting data from your AVD, go to https://github.com/nowsecure/android-forensics/downloads and download the APLogical-OSE software to the VM.

10. In the VM's command prompt window, type adb install ~/Desktop/AFlogicalOSE_1.5.2.apk and press Enter. When you see the "Success" message, you know the APK was able to retrieve data from the Android virtual device.

11. Close the AVD and any other open windows, and exit Santoku.

Hands-On Project 12-5

In this project, you download UFED Reader from Cellebrite and compare a logical acquisition with a physical acquisition. The Web site you go to in Step 1 contains logical and physical acquisitions performed by NIST to help you learn how to read these files.

1. Start a Web browser, go to www.cfreds.nist.gov, and scroll to the table at the bottom of the page. Click Mobile Device Images, and on the next page, click the Cellebrite UFED link.

2. Download the UFED Reader 3.2.exe file. In the table on the first page, find the entry with Nokia in the first column and Logical Acquisition in the second column. In the third column, click the ufdr link, and download Nokia-logical.ufdr. Go back to the table, find the entry with Nokia in the first column and Physical Acquisition in the second column. In the third column, click the ufdr link, and download Nokia-physical.ufdr.

3. Start UFED Reader. Click File, Open from the menu, and click Nokia-logical.ufdr (a logical acquisition). It should open to the Extraction Summary tab shown in Figure 12-8. On the left you can see the file structure, and on the right, you can see the type of phone, SMS messages, contacts, the call log, and so forth. Examine the information acquired from the phone, and take screenshots of this information. When you're finished, click File, Close from the menu.

4. Next, open the Nokia-physical.ufdr file (a physical acquisition). Examine the information acquired from the phone, and take screenshots of this information. 5. Exit your Web browser and UFED Reader. Write a one- to two-page paper describing the differences between the logical and physical acquisitions you examined.

Findings: We cannot examine the logical and physical acquisition without application. UFED reader application is not available in the internet.