CSCE 5555 – Computer Forensics

Lab 08

Mobile Device Forensics

Student ID:11647576

Examining Cell Phone Storage Devices

Most modern cell phones support removable memory storage devices known as MicroSD and MiniSD flash devices, and these devices can store up to 32 GB of data. An experienced computer forensics investigator will find that personal information, pictures, and organizer data can be obtained from the flash memory device. When creating images of cell phone data, it is advisable to remove any secondary storage devices and image them separately because flash memory is usually formatted in a readable file system.

Recovering cell phone information can be challenging because no formal standards exist on operating systems, and the file systems vary greatly between manufacturers. In this lab, you will use OS Forensics and ProDiscover to process a forensically obtained image of a cell phone MicroSD storage device.

1. Start **OSForensics** on your workstation. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. Note that you may be prompted to enter your user ID and password. In the OSForensics message box, click **Continue Using Free Version**.

2. In the left pane, click **Manage Case**, if necessary. In the Manage Case pane on the right, click the **New Case** button. In the New Case dialog box, type **C12Proj1** in the Case Name text box and your name in the Investigator text box. For the Acquisition Type setting, click the **Investigate Disk(s) from Another Machine** option button. Click **Custom Location** for the Case Folder option. Click the **Browse** button on the lower right, navigate to and click your desired work folder, and then click **OK** twice.

3. To mount the disk image, scroll down the navigation bar on the left, and click **Mount Drive Image**. In the Mounted virtual disks window, click the **Mount new** button. In the OSFMount – Mount drive dialog box that opens, click the **...** button next to the Image file text box, navigate to the location of the **C12Proj01.E01** image, select the C12Proj01.E01 image, click **Open**, and then click **OK**, remembering the drive letter where the image was mounted. Click the **Exit** button to close the window.

4. In the left pane, click the **Create Index** button. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click to select all the file types listed, and click **Next**. In the Step 2 of 5 window, click the **Add** button. In the Add Start Location dialog box, select the **Whole Drive** option, select the drive letter for the virtual disk that you just mounted in the previous step, and then click **OK**, followed by **Next**. In the Step 3 of 5 window, click **Start Indexing**. Wait until OSForensics finishes indexing (which might take several minutes). When the OSForensics – Create Index dialog box appears, click **OK** (do not worry if it indicates that there were some errors in the indexing process).

5. Once completed, click the **Search Index** button in the left pane. Without typing anything in the Enter Search Words text box, click the **Search** button.

6. Select the **Images** tab. Search through these images for the answers to the following questions.

   a. How many files were found in the Images tab? 22

   b. What is the earliest date and time for a JPEG image found on this drive? Make note of this when we use another forensics tool. 02-24-07-1211

7. When done, close the window to exit the Internal Viewer.

8. Click the **File Name Search** button in the left pane. Select the **…** button to the right of the Start Folder text box to select the applicable drive for the virtual disk that you mounted in the Browse for Folder dialog box. Then, without typing anything in the Search String text box, click the **Search** button.

   c. How many total items were found? 56

   d. Right-click on the **05-31-10_1621.jpg** image, and select the **View with Internal Viewer…** menu option to view the image and its properties. Select the Metadata tab. Based on the Camera Model Name, what is the resolution of the camera built into the cell phone? 1.3 megapixel (X- Resolution -72, Y-Resolution-72)

9. Click the **Exit** button in the left pane to close the OSForensics program.

10. Start **ProDiscover Basic** on your workstation.

11. If the Launch Dialog box appears, type **C12Proj1** into the Project Number and Project File Name boxes in the New Project tab, and click **OK**. Otherwise, click the **File** tab and click **New Project** and type **C12Proj1** into the boxes as above for the New Project dialog box.

12. Click the **Action** tab and click **Add**; then in the submenu, click **Image File**.

13. In the Open dialog box, browse to the location of the **C12Proj1.E01** file, click the file, and select **Open**.

14. Expand the **Images** icon located under the **Content View** by clicking on the **+** symbol, and then clicking the **+** symbol next to the **C12Proj1.E01** image icon. Now, click on the **+** symbol to expand **C:** and then select **All Files** to show all the regular files in the right-window.

   e. How many total files are found? 51

   f. What is the Created Date (and time) for all of these files? 12/31/1969 18:00:00

   g. How many deleted files were found on this image? 29

15. Click the **View** tab and select Gallery View to see the gallery view of the files. This action should now show thumbnails of images in the right pane. You should now notice several images prominently featuring a vehicle.

h. What model vehicle is pictured? TOYOTA-SIENNA XLE

i. What is the license plate number of this vehicle? J56ZBX

j. Which file provides significant information about a possible suspect (i.e., the person who took one of the photos)? 02-24-07_1216.JPG

16. Click the **File** tab and select **Exit**. Click **No** in the ProDiscover dialog box to close ProDiscover.

Using FTK Imager to View Extracted Phone Evidence

Computer forensics investigators must be able to extract locally stored data in cell phones because service providers do not have access to the personal information. The imaging process requires both hardware and software tools to successfully connect a forensic recovery computer to the large variety of cell phone models in use. Special-purpose USB adaptors provide the electrical connections that allow AccessData's Mobile Phone Examiner (MPE) to read the stored data. AccessData's MPE creates .ad1-formatted images that can be processed by FTK or FTK Imager to recover potential forensic evidence. Because of the large variations among cell phone file systems, recovering data me be more efficient using FTK Imager because it provides a faster analysis of resident memory data. In this lab, you will process the MPE image of a LG 6000 cell phone to look for potential evidence.

17. Start **FTK Imager** on your workstation. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. When FTK Imager has finished loading, click the **File** tab and select the **Add Evidence Image** item.

18. Select the **Image File** radio button in the Select Source dialog box, and click **Next**.

19. Click the **Browse** button, navigate to and select the **LG_6000_4d76e052.ad1** image file, and click **Open**. Click **Finish** in the Select File dialog box.

20. In the upper-left Evidence Tree window, click the + symbols to expand the **LG_6000_4d76e052.ad1**, the **External-File-System [AD1]** connector object, and the following folders: **LG VX6000**, **LG VX6000**, and **Phonebook** folders to display the list of directories located in the Phonebook folder.

21. Click the **Last dialed numbers** folder to view the last numbers stored in the phone's internal memory. The numbers are displayed in the upper-right window. Use the scroll bar on the right side to view all the numbers, if necessary.

    k. Abbreviated dialing is the use of a very short telephone number to reach public services. What abbreviated dialing telephone number was used to report a problem with telephone service? 611

22. Click the **Received calls** folder to see all the inbound calls to the phone. The time and date are not available in this capture, but they can be obtained from the service provider.

l. How many calls were from long distance numbers (i.e., how many numbers received had a "1" plus the 10-digit number)? 1

23. Click the **Missed calls** folder to see all the inbound calls to the phone that were not answered.

m. What area code were *most* of the missed calls from? 619

24. Click the + symbol next to the **File System** folder to expand it and view the subfolders. Click the **sms** folder below the File System folder to view any text messages sent to the phone. Make sure the **Properties** tab is selected in the bottom-left window.

n. Even though you cannot "hear" any voice messages, how can you tell that there some voice mails stored for this cell phone number? As a hint, you can take a look at the next item (and associated questions). **Voice.dat**

25. Click the **mediacan000.dat** file, and click the **TEXT Eyeglass** icon on the tool bar to view the text message sent to the phone in the lower-right window.

o. Who is this text addressed to? Becca

p. What is the file size (i.e., how many characters is this text message)? 108

26. Click the **pim** folder, and click the **outgoing_log.dat** file to see the outgoing call log and the caller ID name. Use the scroll bar on the right side of the lower window to see all the numbers and their associated names. Disregard the ASCII characters to the left of the numbers because they are used by the phone database.

q. What number code is used to access the cell phone owner's voice mail? *86

r. Based on this file, what is one type of food that the cell phone owner enjoys?

D Pizza

27. Click the **missed_log.dat** file to see the numbers and names of calls that were not answered on the phone.

s. How many calls from Fancy Nancy were missed? 3

28. Click the **incoming_log.dat** file to see the inbound call list.

t. What are the two key words shown in this file that indicate there is no caller information (or that the caller did not provide his/her information)? This question is not asking about calls with no caller ID. Unavailable

Restricted

29. Click the **Eyeglass** icon on the tool bar, and click the **cam** folder to look for graphics images taken by the cell phone camera. Click each picture to see it in the viewer.

u. How many camera pictures were found on this cell phone? 6

v. How many "selfies" did the owner of the cell phone take? 4

30. Click the File tab, and select Exit to close FTK Imager.

Analyzing Cell Phone Evidence Using the FTK Imager

Modern cell phones can contain multimedia and text files such as pictures, movies, and documents that may be valuable to an investigation. Because there are no worldwide cell phone standards used to store electronic data, forensics tools must be able to read the various file formats to locate information. In this lab, you will process a Nokia 5300 MPE image with FTK Imager to look for forensic evidence.

31. Start **FTK Imager** on your workstation. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. When FTK Imager has finished loading, click the **File** tab and select the **Add Evidence Image** item.

32. Select the **Image File** radio button in the Select Source dialog box, and click **Next**.

33. Click the **Browse** button, navigate to and select the **Nokia_5300.ad1** image file, and click **Open**. Click **Finish** in the Select File dialog box.

34. In the upper-left Evidence Tree window, click the + symbols to expand the **Nokia_5300.ad1**, the **External-File-System [AD1]** connector object, and the following folders: **Nokia 5300**, **Nokia 5300:356964012353048**, and **SMS** folders to display a directory located in the SMS folder. Select the Inbox folder to view the SMS messages on the phone.

    w. Scroll down until you find the message that starts with "I FOUND THE …" in all capital letters. What did this cell phone user find? DINOSAUR

35. Select the **File System** folder and then click on the **+** symbol to expand the **NO NAME** and **Playlists** folders. Now, in the select the Images folder under the Playlists folder. Then, select the Image001.jpg file.

    x. What is the name prominently displayed in this image? Jay Morrison

36. Now select the **Video clips** folder under the File System folder to reveal the **Test000.3gp** file. Right-click the file and select **Export Files…** to save it to your computer, where you can use an application such as Real Player or QuickTime to view the video.

    y. When was this video downloaded to the cell phone? 3/25/2008 5:34:38AM

    z. Although the video may be blurry, what is the video of? It shows the data and SO the person in video getting to find out the data or modify the data in one tool.

37. Close the Real Player or QuickTime application (or whatever applicable application that you used), but keep FTK Imager open.

38. Now select the **%INTERNALFS2%** folder under the File System folder followed by the HTTP folder to reveal three directories. Select the cache directory to reveal a number of cache files.

aa. Search through these files (by selecting them individually) to reveal a picture of a female. What is the name of the cache file? CCUigCRR2vncwa4Dp.dat COVcz4rc80gzb6S5I.dat

39. Click the **File** tab and select **Exit**. Click **No** in the ProDiscover dialog box to close ProDiscover.

You are to submit this document, with your solutions, to the **Lab 08** dropbox on Canvas by the due date and time.