Lab Assignment 4B – Mobile Device Analysis

Background

Students will have the opportunity to use open source tools to review several mobile device images, internal components, and cloud backups. This relatively short assignment will provide students with experience in performing basic searches while familiarizing themselves with the capabilities of open source tools.

Commercial tools and iOS devices will be covered in another assignment.

OneDrive Link:
https://northeastern-my.sharepoint.com/:f:/g/personal/e_booker_northeastern_edu/EtalfUuT7EhHj_nfhQPcGoMBVFnjyhWU94ipYz_OYLg_HA?e=VbSfXy

Objectives

- Review a Motorola collection including MicroSD storage for potential evidence
- Become familiar with using FTK Imager to review mobile extractions
- Parse cloud backups for potential evidence and understand various storage areas

Exercise Preparation

1. Using Autopsy to Examine a Motorola Cellphone

Examine a Motorola cell phone and its MicroSD storage device to look for forensic evidence [estimated completion 90-120 minutes].

a. Start Autopsy, and in the Welcome window, click the **New Case** button. In the New Case Information window, type **LabAssignment4b1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**.

b. In the Optional Information window, type **LabAssignment4b1** in the Case Number text box and your name in the Examiner text box, and then click **Finish** to create the database.

c. In the Select Host window, click **Next**. In the Select Data Source Type window, click **Disk Image or VM file**, if necessary .In the Select Data Source window, click the **Browse** button, navigate to your work folder, click the **Motorola.E01** file, and click **Open**. Click **Next**. In the Configure Ingest Modules window ensure the **Recent Activity**, **File Type Identification, Extension Mismatch Detector, Embedded File Extractor, Picture Analyzer** (4.17 change), **Keyword Search**, **Email Parser**, **Interesting File Identifier** and **PhotoRec Carver** check boxes are selected, click **Next**, and **Finish** to start analyzing the evidence.

FOR THOSE USING THE PRE-PROCESSES EVIDENCE – LOAD THE EVIDENCE FILE AND START HERE

d. In the left pane, expand **Data Sources**, and expand the **Motorola.E01** folder to view the phone's OS folders and its MicroSD storage device.

e. With the Motorola.E01 file highlighted on the left, Click the **motorola** folder in the Result Viewer pane, and click the **File Metadata** tab in the Content Viewer pane to see the MicroSD storage device. In the Result Viewer pane, a red × next to files means they were deleted. The Unallocated entry in the Flags(Dir) column means these files are in unallocated space on the storage device. Click the first two deleted files to see the recovered JPG files on this storage device. Click the third deleted file, and notice a blank photo in the Content Viewer pane, which indicates the file header was recovered, but the image content can't be recovered.

f. Scroll down the Result Viewer pane, and click the **$MBR** file. Its icon and metadata are grayed out, indicating it's a hidden system file. This file is the Master Boot Record and contains the file system information needed to mount the storage device. Click the **Indexed Text** tab in the Content Viewer pane, if necessary, to see that the file system is FAT16 and the storage device is named SANVOL. SANVOL, manufactured by SanDisk, is a MicroSD storage device, which can help forensics investigators identify it.

g. Click the **$CarvedFiles** folder in the left pane to see data on graphics files carved from unallocated space. Click the **Thumbnail** tab in the Result Viewer pane, and scroll down to see all the recovered files, including blank (unrecovered) photos in the cell phone's memory storage.

h. In the left pane, expand **Analysis Results**, if necessary, and click the **EXIF Metadata** folder. In the Result Viewer pane, click the first graphics file, and then click the **Analysis Results** tab in the Content Viewer pane to see detailed metadata about this file, including the camera resolution. Click the **Text > Indexed Text** tabs, and notice that the second and third lines list Motorola and 1.3 Megapixel. Autopsy interprets and displays this information in the Result Viewer pane as the phone's device make and model.

i. Leave Autopsy open as you answer the below review questions. When you're finished, exit Autopsy.

2. FTK Imager Analysis of Mobile Evidence

Use FTK Imager Lite to view text messages, phone numbers and photos [Estimated completion time: 30-60 minutes]. **There is no pre-processing required for this section.**

a. Start FTK Imager Lite, clicking **Yes** in the UAC message box, if necessary.

b. Click **File**, **Add Evidence Item** from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.

c. In the Select File dialog box, click **Browse**, navigate to your work folder, double-click the **LG_6000_4d76e052.ad1** file, and then click **Finish**.

d. In the Evidence Tree pane, expand **LG_6000_4d76e052.ad1**, **External-File-System [AD1]**, and **LG VX6000**. Expand the **LG VX6000** and **Phonebook** subfolders.

e. Click the **Last dialed numbers** folder. The most recent numbers stored in the phone's memory are shown in the File List pane on the right. Use the scrollbar, if needed, to view all the numbers.

f. Click the **Received calls** folder to see inbound calls. This image file doesn't show the times and dates of these calls, but you can get this information from the service provider or through AccessData MPE+. Next, click the **Missed calls** folder to see inbound calls that weren't answered.

g. In the Evidence Tree pane, expand **File System**, and then click the **sms** folder to view text messages sent to the phone. In the File List pane, click the **mediacan000.dat** file, and read its contents in the lower-right pane.

h. Click the **eyeglass** toolbar icon, and then click the **cam** folder in the Evidence Tree pane to look for photos taken by the phone's camera. Click each **.jpg** file in the File List pane to see it in the viewer.

i. Leave FTK Imager Lite open as you answer the following review questions. When you're finished, exit FTK Imager Lite.

3. Using Autopsy to Analyze Cloud Backups

Using Autopsy to search cloud backups of mobile devices for evidence involving money transfers between bank accounts [Estimated time to completion: 60-90 minutes].

a. Extract the **InCh12Randall.exe** and **InCh12Sarah.exe** files to your work folder. (This process might take a few minutes.)

b. Start Autopsy, and in the Welcome window, click the **New Case** button. In the New Case Information window, type **LabAssignment4b3** in the Case Name text box, verify that your work folder is displayed in the Base Directory text box, and then click **Next**.

c. In the Optional Information window, type **LabAssignment4b3** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

d. Next we add a data source. In the Select Host window, choose **Generate new host name based on data source name**, and then click **Next**.

e. In the Add Data Source window, click **Disk Image or VM file** in the "Select Data Source Type" list box, if necessary. Click Next.

f. In the Select Data Source window, under Path:, click the **Browse** button, navigate to and click your work folder, double-click the **InCh12Randall.001** file, and then click **Next**.

g. In the Configure Ingest Modules window, click **Select All**, and then click **Next** and **Finish** to start analyzing the evidence.

h. Click the **Add Data Source** button. In the Select Host window, choose **Generate new host name based on data source name**, and then click **Next**.

i. In the Add Data Source window, click **Disk Image or VM file** in the "Select Data Source Type" list box, if necessary. Click **Next**.

j. In the Select Data Source window, under Path:, click the **Browse** button, navigate to and click your work folder, double-click the **InCh12Sarah.001** file, and then click **Next**.

k. Click **Next** to accept the ingest modules configured for the previous evidence source, and then click **Finish** to start analyzing the evidence, which takes a few minutes. When it's finished, you should see the two image files in the Directory Listing pane on the right.

l. Click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click the **Search** button. Wait until the search is finished before going on to the next step.

FOR THOSE USING THE PRE-PROCESSES EVIDENCE – LOAD THE EVIDENCE FILE AND START HERE

m. Click **Keyword Search** at the upper right, type **Wells Fargo**, and click **Search**. Click **Keyword Search** again, type **Offshore Accounts**, and click **Search**.

n. Click the **Keyword search 2 - Wells Fargo** tab, and click the first e-mail listed. The Content Viewer pane shows the keyword highlighted in yellow. Click the **Inbox**, **Sent Mail**, and **Trash** e-mails in the Result Viewer pane, and read each one in the Content Viewer pane.

o. Click the **Keyword search 3 - Offshore Accounts** tab, and click the first e-mail listed. The Content Viewer pane shows the keyword highlighted in yellow. Click the **Inbox**, **Sent Mail**, and **Trash** e-mails in the Result Viewer pane, and read each one in the Content Viewer pane.

p. Leave Autopsy open as you answer the following review questions. Use additional functions in Autopsy, such as other keyword searches, to find the answers to these questions. When you're finished, exit Autopsy.

Exercise – Questions

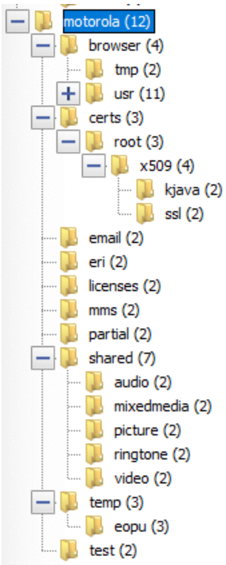
1. Using Autopsy to Examine a Motorola Cellphone

a. Under the **EXIF Metadata** folder in the left pane of Autopsy, how many pictures have been **recovered** from the cell phone image?

There are 90 .jpg files recovered on the cell phone image

b. How many subfolders are under the Motorola folder (the MicroSD storage device)? Do any readily stand out as worthy of investigation?

There are 12 subfolders within the Motorola folder. From that ‘email’ and ‘browser’ stand out as worthy of investigation. This helps investigators understand the browser history and email messages of a potential leak or criminal activities/downloads.



c. Which file system is in use on the MicroSD storage device?

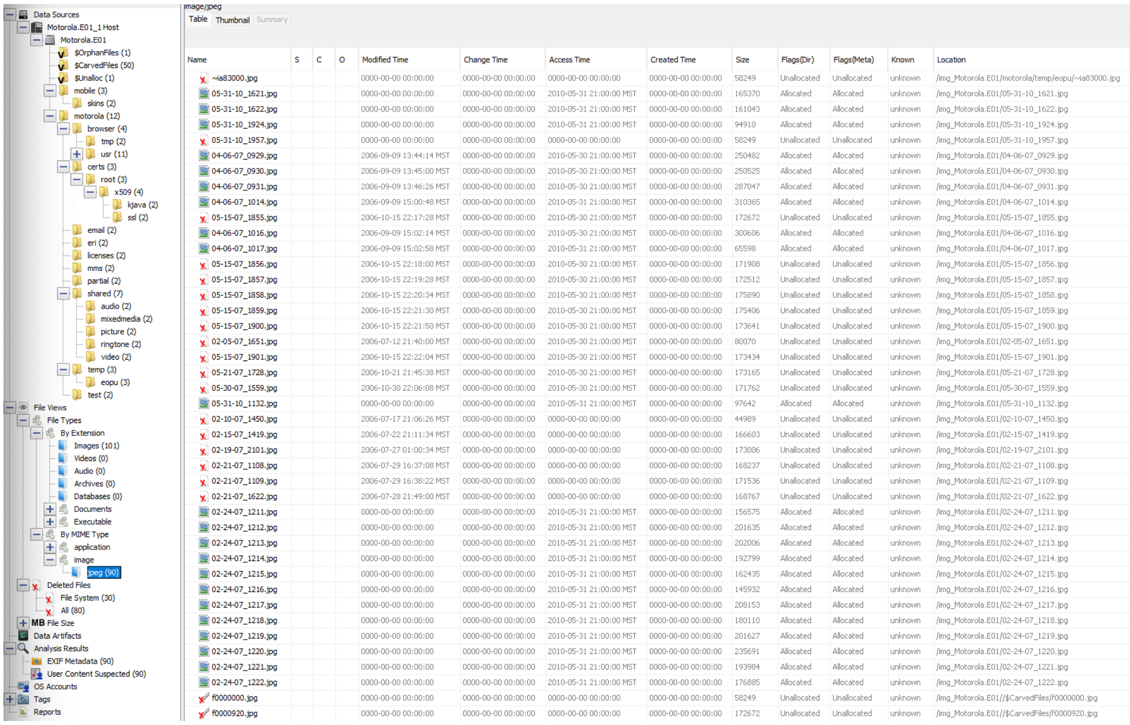
The file system of the MicroSD storage device is FAT16. This is found under Data Sources > Motorola.E01_1 Host > Text

d. What’s the resolution of the cell phone’s camera?

1.3 Megapixel. Found in File Views > File Types > By Extension > Images. Pick an image. And under Text provides information about the picture taken.

e. Which column do you check to determine whether a file is in unallocated space?

The columns that determine if a file is of Unallocated (Deleted Files) and Allocated (Non-Deleted Files) are found in the Flags columns (Dir and Meta).



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
~ia83000.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	58249	Unallocated	Unallocated	unknown	/img_Motorola.E01/motorola/temp/eopu/~ia83000.jpg
05-31-10_1621.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	165370	Allocated	Allocated	unknown	/img_Motorola.E01/05-31-10_1621.jpg
05-31-10_1622.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	161043	Allocated	Allocated	unknown	/img_Motorola.E01/05-31-10_1622.jpg
05-31-10_1924.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	94910	Allocated	Allocated	unknown	/img_Motorola.E01/05-31-10_1924.jpg
05-31-10_1957.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	58249	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-31-10_1957.jpg
04-06-07_0929.jpg				2006-09-09 13:44:14 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	250482	Allocated	Allocated	unknown	/img_Motorola.E01/04-06-07_0929.jpg
04-06-07_0930.jpg				2006-09-09 13:45:00 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	250525	Allocated	Allocated	unknown	/img_Motorola.E01/04-06-07_0930.jpg
04-06-07_0931.jpg				2006-09-09 13:46:26 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	287047	Allocated	Allocated	unknown	/img_Motorola.E01/04-06-07_0931.jpg
04-06-07_1014.jpg				2006-09-09 15:00:48 MST	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	310365	Allocated	Allocated	unknown	/img_Motorola.E01/04-06-07_1014.jpg
05-15-07_1855.jpg				2006-10-15 22:17:28 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	172672	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-15-07_1855.jpg
04-06-07_1016.jpg				2006-09-09 15:02:14 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	300606	Allocated	Allocated	unknown	/img_Motorola.E01/04-06-07_1016.jpg
04-06-07_1017.jpg				2006-09-09 15:02:58 MST	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	65598	Allocated	Allocated	unknown	/img_Motorola.E01/04-06-07_1017.jpg
05-15-07_1856.jpg				2006-10-15 22:18:00 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	171908	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-15-07_1856.jpg
05-15-07_1857.jpg				2006-10-15 22:19:28 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	172512	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-15-07_1857.jpg
05-15-07_1858.jpg				2006-10-15 22:20:34 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	175890	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-15-07_1858.jpg
05-15-07_1859.jpg				2006-10-15 22:21:30 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	175406	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-15-07_1859.jpg
05-15-07_1900.jpg				2006-10-15 22:21:50 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	173641	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-15-07_1900.jpg
02-05-07_1651.jpg				2006-07-12 21:40:00 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	80070	Unallocated	Unallocated	unknown	/img_Motorola.E01/02-05-07_1651.jpg
05-15-07_1901.jpg				2006-10-15 22:22:04 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	173434	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-15-07_1901.jpg
05-21-07_1728.jpg				2006-10-21 21:45:38 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	173165	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-21-07_1728.jpg
05-30-07_1559.jpg				2006-10-30 22:06:08 MST	0000-00-00 00:00:00	2010-05-30 21:00:00 MST	0000-00-00 00:00:00	171762	Unallocated	Unallocated	unknown	/img_Motorola.E01/05-30-07_1559.jpg
05-31-10_1132.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	97642	Allocated	Allocated	unknown	/img_Motorola.E01/05-31-10_1132.jpg
02-10-07_1450.jpg				2006-07-17 21:06:26 MST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	44989	Unallocated	Unallocated	unknown	/img_Motorola.E01/02-10-07_1450.jpg
02-15-07_1419.jpg				2006-07-22 21:11:34 MST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	166603	Unallocated	Unallocated	unknown	/img_Motorola.E01/02-15-07_1419.jpg
02-19-07_2101.jpg				2006-07-27 01:00:34 MST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	173006	Unallocated	Unallocated	unknown	/img_Motorola.E01/02-19-07_2101.jpg
02-21-07_1108.jpg				2006-07-29 16:37:08 MST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	168237	Unallocated	Unallocated	unknown	/img_Motorola.E01/02-21-07_1108.jpg
02-21-07_1109.jpg				2006-07-29 16:38:22 MST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	171536	Unallocated	Unallocated	unknown	/img_Motorola.E01/02-21-07_1109.jpg
02-21-07_1622.jpg				2006-07-28 21:49:00 MST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	168767	Unallocated	Unallocated	unknown	/img_Motorola.E01/02-21-07_1622.jpg
02-24-07_1211.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	156575	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1211.jpg
02-24-07_1212.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	201635	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1212.jpg
02-24-07_1213.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	202006	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1213.jpg
02-24-07_1214.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	192799	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1214.jpg
02-24-07_1215.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	162435	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1215.jpg
02-24-07_1216.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	145932	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1216.jpg
02-24-07_1217.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	208153	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1217.jpg
02-24-07_1218.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	180110	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1218.jpg
02-24-07_1219.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	201627	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1219.jpg
02-24-07_1220.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	235691	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1220.jpg
02-24-07_1221.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	193984	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1221.jpg
02-24-07_1222.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	2010-05-31 21:00:00 MST	0000-00-00 00:00:00	176885	Allocated	Allocated	unknown	/img_Motorola.E01/02-24-07_1222.jpg
f0000000.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	58249	Unallocated	Unallocated	unknown	/img_Motorola.E01//$CarvedFiles/f0000000.jpg
f0000920.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	172672	Unallocated	Unallocated	unknown	/img_Motorola.E01//$CarvedFiles/f0000920.jpg

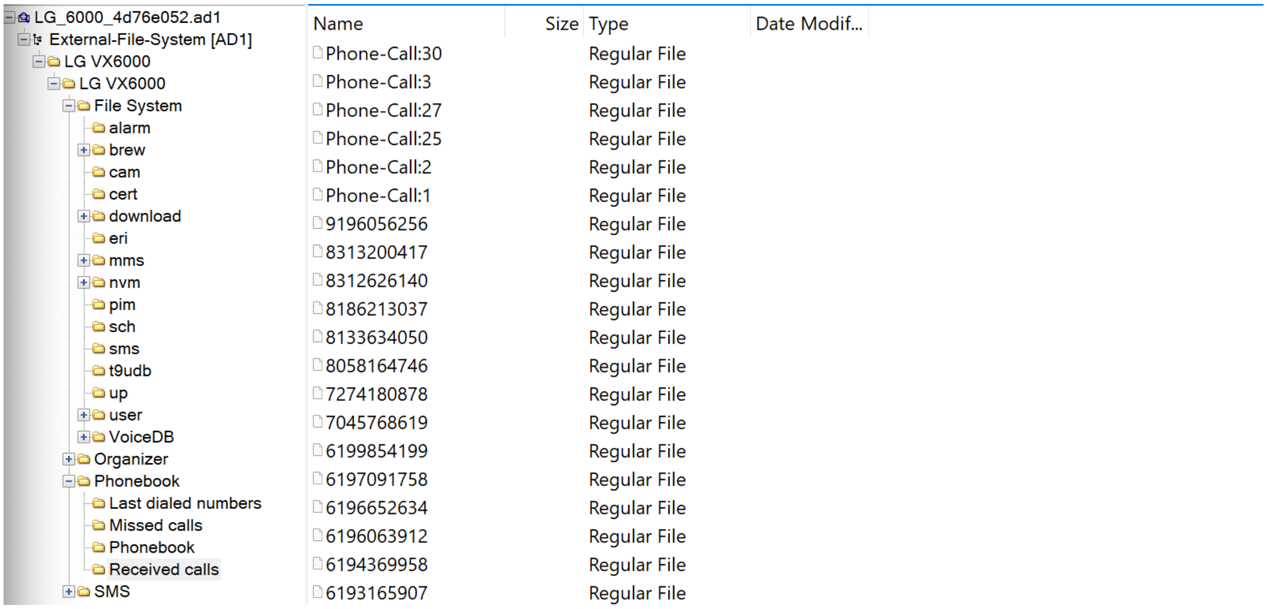
2. FTK Imager Analysis of Mobile Evidence

a. How many phone numbers were dialed on this phone (to include XXX-XXX-XXXX)?

There are a total of 30 numbers listed in the Phonebook > Last Dialed Numbers directory. Out of the 30, 24 numbers are of the format (X)-XXX-XXX-XXXX, the others are 611, 411, #646, *86, and 2879050 (no optional country and/or area code)

b. How many received calls couldn't be identified (doesn't have a listed number)?

Similar to the above, 24 numbers are listed with 6 being unlisted with "Phone-Call:##". This can be linked to the others numbers above.



Name	Size	Type	Date Modif...
Phone-Call:30		Regular File	
Phone-Call:3		Regular File	
Phone-Call:27		Regular File	
Phone-Call:25		Regular File	
Phone-Call:2		Regular File	
Phone-Call:1		Regular File	
9196056256		Regular File	
8313200417		Regular File	
8312626140		Regular File	
8186213037		Regular File	
8133634050		Regular File	
8058164746		Regular File	
7274180878		Regular File	
7045768619		Regular File	
6199854199		Regular File	
6197091758		Regular File	
6196652634		Regular File	
6196063912		Regular File	
6194369958		Regular File	
6193165907		Regular File	

c. What text was recovered from the file **mediacan000.dat?**

The text recovered from the .dat file in File System > sms was "Is there anymore room in those jeansBecca i respect you a lot and i would never want to hurt your feelings"

d. How many photos were taken by this phone's camera?

Photos found in File System > cam were 6 .jpg files. There were also 4 .dat files which were not photos but seems like configuration files.

e. Are there any missed calls from the same number that could be indicative of a frequent contact or evidence of harassment/stalking?

There was one missed call "Phone-Call:6" that cannot be identified. There were a couple of frequent contact numbers that should be investigated for harassment/stalking:

- **8313200417 (3)**
- **8133634050 (3)**
- **8133634010 (2)**
- **6192044588 (2)**
- **3108505307 (5)**

3. Using Autopsy to Analyze Cloud Backups

a. How much money did Randall Simpson tell Sarah to ask her boss to fund initially? What was this amount changed to?

The amount was initially at 500K, but was changed to 300K.

b. What phone numbers were recovered from the evidence?

I was unable to find any phone numbers recovered from evidence. I was only able to find the email chains between Randall and Sarah, plus others.

c. How many recovered e-mails were in the Default folder?

There are 225 recovered emails in the Default folder found in Data Artifacts > Email Messages > Default (Default) > Default

d. Were any photos recovered from either device? If so, how many, and might there be related to any suspicious activity?

162 .jpg 163 .png images recovered from either device. From a total of 13629 files found in File Views > File Types > Deleted Files > All. From there no photos seemed to be related to suspicious activity. However photos in the location "/img_InCh12Randall.001/Program

Files/WindowsApps/Microsoft.BingFinance_1.2.0.135_x86__8wekyb3d8bbwe/platform/images/" seem of interest with text "Finance"

e. Was there any evidence to suggest that both Randall and Sarah were involved in transferring money? If so, what was that evidence?

There is evidence from an email sent between Sarah and Randall with Subject RE:Hi on 2014-08-06 11:44:17 EDT with the text "So where should we be depositing this money? I'm thinking a foreign account would be best?" This is in relation to the 300K transfer from their boss. From other messages there seems to be a relationship between the two and trying to steal money for themselves in foreign accounts. This is worthy of an investigation.

Exercise—Key Takeaways

- Examiners must understand the various locations where mobile evidence might be stored
- Some evidence is stored on additional storage areas or cloud backups by default

***Please submit the final assignment as a single .PDF and any applicable reports as a .ZIP file.**
**Screenshots may also be added to this document when appropriate.