Lab 11 – Examining Cell Phone Storage Devices

Cell Phones have removal memory storage devices. These devices can hold any type of data, personal, photos etc. which all can be useful in an investigation. It is recommended that a separate image is taken of a storage device to that one taken from the phone itself. Recovering data from a phone is very difficult as there is no one single standard to which all phones comply. For example, there are variations on where messages are stored and file systems used also differ.

In this lab we are going to create an image of a Motorola cell phone and MicroSD card.

Activity

1. Copy the Motorola.E01 file from the Data files folder on your VM to the Work\Labs\Evidence folder.
2. Start Autopsy. Click Create New Case.
3. Type C12Proj1 in the Case Name textbox. Click Browse, navigate to and click the Works\Labs\Cases folder, click OK to enter this path in the Base Directory text box and click Next. Type C12Proj1 in the Case Number and your name in Examiner text box. Click Finish.
4. In the Add Data Source dialog box, click Browse, navigate to your Evidence folder and click Motorola.E01 and click Open. Click Next twice and the click Finish to start analysing.
5. In the left pane, click Motorola.E01 to view the files OS folders and MicroSD storage. In the right pane, click the Motorola folder and click the Metadata tab at the bottom to see the MicroSD storage device. A red x next to file means they have been deleted. The unallocated entry in the Flag(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.
6. Scroll down the upper right pane and click $MBR file. Its icon is greyed out indicating a hidden system file. This file is the Master Boot Record and contains the file system information needed to mount the storage device. If necessary click the Text tab at bottom to see the file system for the storage device. The SANVOL name shown means the device was manufactured by San Disk, which can help an investigator identify the device.
7. Click the $CarvedFiles folder to see data on graphics files that has been carved from unallocated space. Click the thumbnail tab in the upper right pane and scroll to see all the recovered and blank images in the cells phone's memory storage.
8. In the left pane, expand Extracted Content and click EXIF Metadata. In the upper right pane, click the first graphics file and click the Test tab at the bottom to see the Exif information. If you scroll through this information you will see the photos taken by the camera phone. Click Table tab in upper pane. The camera information for these images is displayed in the Device Model and Data Source columns.
9. Exit Autopsy.

Lab 12 – Using FTK Imager to view Text Messages, Phone Numbers and Photos

As already said it can be difficulty to recover data off a mobile device due to differing platforms; Google, Apple OS, Android and Windows. Some tools capture data by using USB adapters or tablet device that creates a .E01 or raw image. Access data Mobile Phone Examiner (MPE) creates .adl images that can be processed in FTK to recover evidence. In this lab we will process an MPE image of a LG6000 phone.

Activity

1. Copy the file LG_6000_4d76e52.adl file from the data files stored (chapter 12) in the VM to your evidence folder.
2. Start FTK and click Yes on UAC box.
3. Click File, Add Evidence Item from menu. In the Select Source box click the Image file option button, and then click Next.
4. In the Select file dialog box, click Browse, navigate to the Evidence folder and click on the LG_6000_4d76e52.adl file, click Open and then click Finish.
5. In the evidence tree pane expand LG_6000_4d76e52.adl, External-Filesystem (AD1) and LGVX6000. Click the LGVX6000 sub folder and then click Phonebook folder.
6. Click the Last dialled numbers folder. The most recent numbers are stored in the phones memory. Scroll to see the numbers.
7. Click Received calls folder to see inbound calls. This image does not show date and time calls were received but can get you information from the service provider to through MPE. Next click on Missed calls to see all inbound class that were not answered.
8. In the Evidence tree pane expand File System and click sms folder to view text messages sent to this phone. In the file list pane click the mediacan000.dat file and read its contents in the lower right pane.
9. Click the eyeglass toolbar icon and click 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,
10. Exit FTK