MIS5170 Forensic Assignment 1 – Project2400

* Windows 8 or higher
* Autopsy 3.1.2 for Windows (32bit or 64bit)

**1st Time Setup for Autopsy**

1. Create Folder for Work
2. Create Subfolder for Labs in Work Folder
3. Create Subfolder for Evidence in Labs Folder
4. Create Subfolder for Cases in Labs Folder
5. Start a Web Browser, and go to <http://soureforge.net/projects/autopsy/files/autopsy/3.1.2/>. Double-click on the .msi file to download and install Autopsy 3.1.2 for Windows.

**Data and Ingest**

1. Go to <http://digitalcorpora.org/corp/nps/scenarios/2009-m57-patents/drives-redacted/>, scroll down, and download the Charlie-2009-12-03.E01 file to the C:\Work\Labs\Evidence folder on your computer.
2. Double-click on Autopsy desktop icon.
3. In the Welcome window, click to Create New Case.
4. Type C6Proj1 inn the Case Name text box.
5. Click Browse, navigate to and click the C:\Work\Labs\Cases folder, click OK to enter this path in the base Directory text box and then click Next.
6. Type C6Proj1 in the Case Number text box and your initials in the Examiner text box, and then click Finish.
7. In the Add Data Source dialog box, click Browse, navigate to and click the Charlie-2009-12-03.E01 file your downloaded from the M57 site, click OK to enter this path, and then click Next. In the Configure Ingest Modules dialog box, click Next, and then click Finish to start analyzing the evidence. Watch the progress bar in the lower-right corner to determine when the process is finished.

**Exercise**

1. Click the Keyword Lists button at the upper right, click all four check boxes, and then click search.
2. Click all four check boxes, and the click Search.
3. Click the Keyword Search button at the upper right, type Project2400, and click the Search button. The Search will return 9 results
4. Click the Inbox entry in the right pane, and notice that the Project2400 results are highlighted in Yellow. Scroll through the results to find any evidence of Charlie receiving emails about Project2400. Click the Sent entry in the right pane, and look for emails sent about Project2400.
5. Click Tools, Timeline from the menu. This process takes a few minutes. By default, the timeline is displayed with a large date range. In this case, you’re interested in the period between Nov 16, 2009 and Dec 9, 2009. In the Timeline Window – Editor dialog box, use the slider to set the dates to November 16, 2009 at 12:00AM and December 9, 2009 at 11:59PM.
6. Click the Filters tab at the lower left, type Project2400, click the Text Filter check box, and then click on Apply button. Click the Counts button to see the dates with activity involving Project2400.
7. Click the Details button to see the emails for this filename. Move your mouse pointer over each event to see details.
8. When finished close the dialog box.
9. Click Tools, Generate Report from the menu. In the Generate Report dialog box, click Results – HTML, and then click, Next. Click All Results, and then click Finish.
10. When the green check mark is displayed, click the Results – HTML link, and leave the report open as you answer the below questions.
11. When you’re finished, exit the Web Browser and Autopsy. Save the case, if prompted.

Questions:

1. How many emails did Charlie get?
2. How many emails did Charlie Send?
3. What tools did Charlie search for on the Web?
4. Did Charlie install any tools on this computer?
5. How many cameras can be identified by checking the Exif information?