Timeline Analysis

This week we are working on how to analyze the timeline by reviewing a data set that is based on temporal metadata. We will be organizing the data by dates and times to help see how we can locate necessary data and information through metadata.

To start we open Autopsy either through start or the desktop icon. We choose new case and enter the name as FOR\_LAB\_014\_Timeline, then we hit browse. We go to the pc, evidence repository or E drive, and then make a new folder called FOR\_LAB\_014 making sure it is selected then hitting select and next. We fill in the optional information then click finish. On add data source, we click next, then browse following the path, Desktop > Toolbox > Datasets > Lab 14 and clicking on the file called Lab14.E01, hitting open. We set the time zone to GMT+0 UTC and hit next. On the configure ingest modules we hit deselect all, check recent activity box and hit next then finish. Then we wait for the ingest module to finish running in the right-hand bottom corner. Now we hit timeline on the toolbar to look over then timeline then hit x to close it after review. Next we look at the folder tree and hit the plus next to data sources, Lab12.E01, vol2, documents and settings, Fred, and my documents, then we open my pictures folder. We control and click the m001.gif, m002.gif, m003.gif, m004x.gif, and m006.gif, we hit right click, add file tags, and bookmark. We then sort by created time and see that the gif files we selected were each created within a half hour of one another. We reopen the timeline with the button in the toolbar, switch the display times in to the GMT/UTC zone, we can then highlight the bar on the graph marked 2006 then enter filters choosing must be tagged and hitting apply. We then look at the table and then unclick the must be tagged in the filters and hit apply. We double click the bar called 2006 to see then month then double click again to see the dates of interest. We click the bottom segment of the bar called 08 and scroll down in the table to find the first file created at 7:56:04. Now we see the first of the gif from earlier and scroll up to see what occurred prior to its creation starting with the time 07:55:53. Then we go to 07:55:39 and see a folder created called temporary internet files. We then click the middle section of the bar and change the time back to local time zone. We now scroll until we reach the time of the first file, 7:56:04 and click the entry, Documents and Settings/Fred/My Documents/My Pictures/m001.gif and look at the details in the view pane right of the table. Now we have finished the lab.

Looking through the timeline is interesting as it stores so many of our actions. I can see how this can be useful when trying to find data and how we can look at the activity next to our searched for data to determine what happened. This lab was not a long one but I still found it enjoyable as I love seeing how things can connect with one another.

Section 1 Step 15

A screenshot of a computer

Description automatically generated

Section 2 Step 21

A screenshot of a computer

Description automatically generated