Email Analysis

This lab was created so we can learn how to find metadata within email messages. As email is one of the biggest means of communication, we need to be able to use these messages as evidence by making sure that the metadata lines up.

We start with launching the CAINE machine using the login we are given. We open the application menu and go to the internet then thunderbird mail. Click the inbox folder then double click on the first email named the deadline to open it. We click more, view source then file, and save page as. On the desktop we make a folder called FOR\_LAB\_012 and save the file inside as The deadline.txt and hit save. Opening our new folder through the desktop, we right click The deadline.txt and open with gedit text editor and we can now read through the metadata within the header. Now we move on and go to the application menu, system tools, and open UXTerm. We type in the line, cd Desktop/email-analyzer-master/mha/ then we type in ls, then python3 server.py -d and move to the application bar to now open Firefox web browser. In the URL we type, <http://127.0.0.1:8080> and then we paste the entire email header and click analyze this! Then we repeat with the other email Fw: Re: The deadline and we do the more, view source, edit select all, copy, and then paste in the Firefox window.

Email is something that we all use even if we have not all used the same email type. There are a lot of different cases we can work with revolving around email so it is important to know how to handle it and get the needed metadata. This lab was quite interesting to work through.

Section 1 Step 18

Graphical user interface, text, application

Description automatically generated

Section 2 Step 12

Graphical user interface, text, application

Description automatically generated