Alan Palayil

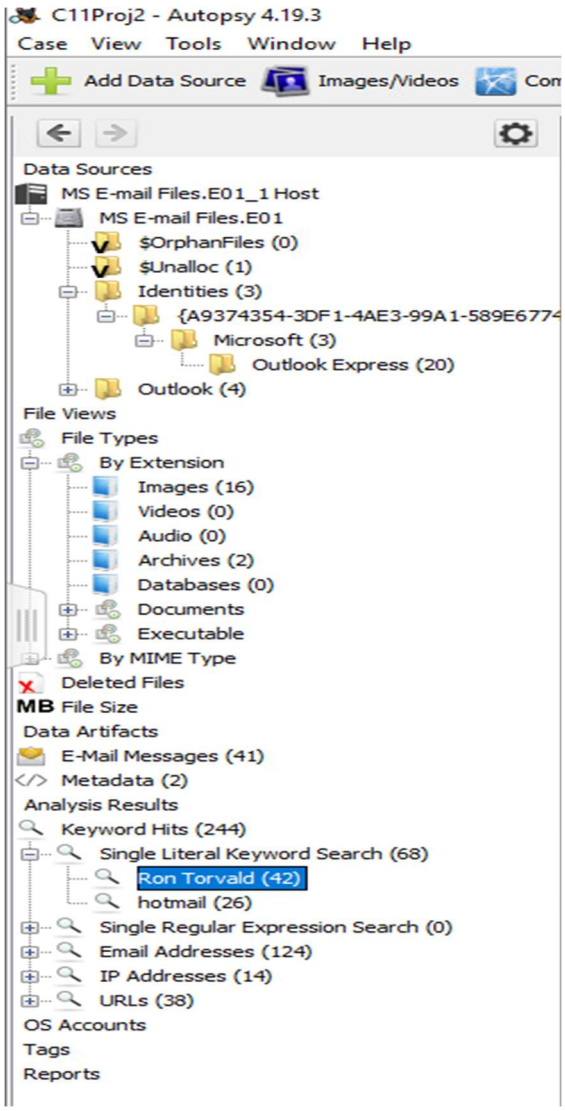
Due Date: 12/02/2022

Email Forensics Using Autopsy:

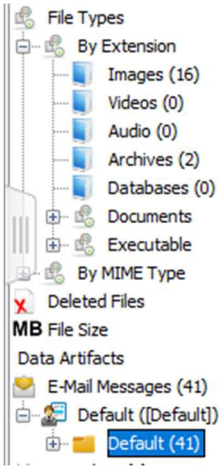
## Introduction:

In this lab we execute the three Email Forensics Labs which are conducted on RADISH Windows 10 desktop. Below are the key steps and answers to questions that are asked in each of the labs.

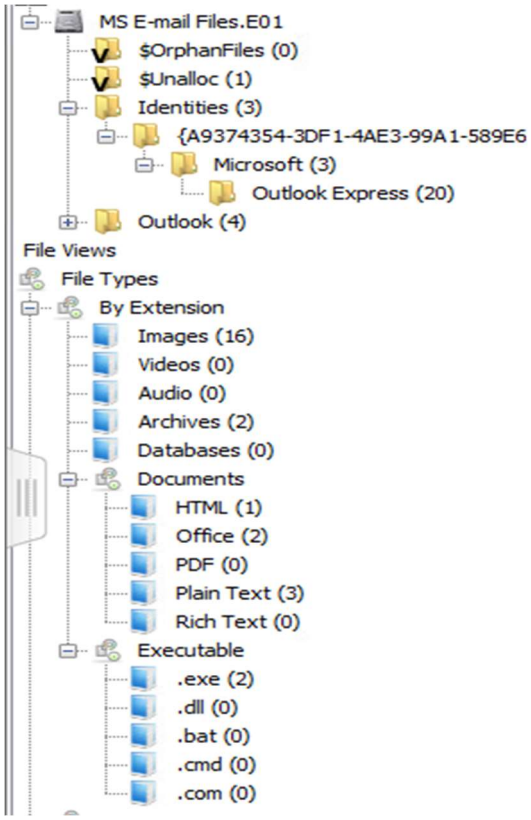
While following the steps, we open Autopsy and create a new case like previous assignments. We go over the steps 1~4 and the results are similar. After which, in step 5, instead of Result Viewer pane, we have Analysis Results.



Step 6~7 was to navigate within the Analysis Results pane. In step 8, we can view the type of attachments which were sent within various email chains.




Step 9, we can view the various emails, URLs, and IP addresses in the Analysis Results pane. While there are numerous more features that are not discussed within the lab such as viewing deleted directories, keyword searches, executable files, etc.



Questions asked in the Lab:

1. How many graphics files did Autopsy recover?
    - There are 16 graphic files that were recovered from Autopsy.
2. How many Hotmail e-mail addresses did you find?
    - There are 36 number of Hotmail email addresses that were found through Autopsy parsing Email Addresses in Analysis Results.
3. How many video files are attached to e-mails in the MS E-mail Files.E01 image?

    a. 16

    b. 0

    c. 2

    d. 3

    - 0, video files are attached to e-mails in the MS E-mail Files.E01 image.
4. In the archive folder (under the File Type, by Extension path), how many archive files did Autopsy recover?

    a. 0

    b. 1

    c. 2

    d. 5

    - In the archive folder (under the File Type, by Extension path), there are 2 archive files did Autopsy recover.
5. Autopsy recovered the same number of e-mails as OSForensics did. True or False?
    - False, Autopsy recovered 42 number of emails compared to OSForensics which only recovered 32.

## Conclusion:

Using Autopsy, we are able to view more of the deleted Outlook mailbox of Ron Torvald and due to software limitations, the search was done through the entire image to find email evidence. The layout of Autopsy makes duplicates of each file depending on the category which can be confusing at times.