Alan Palayil

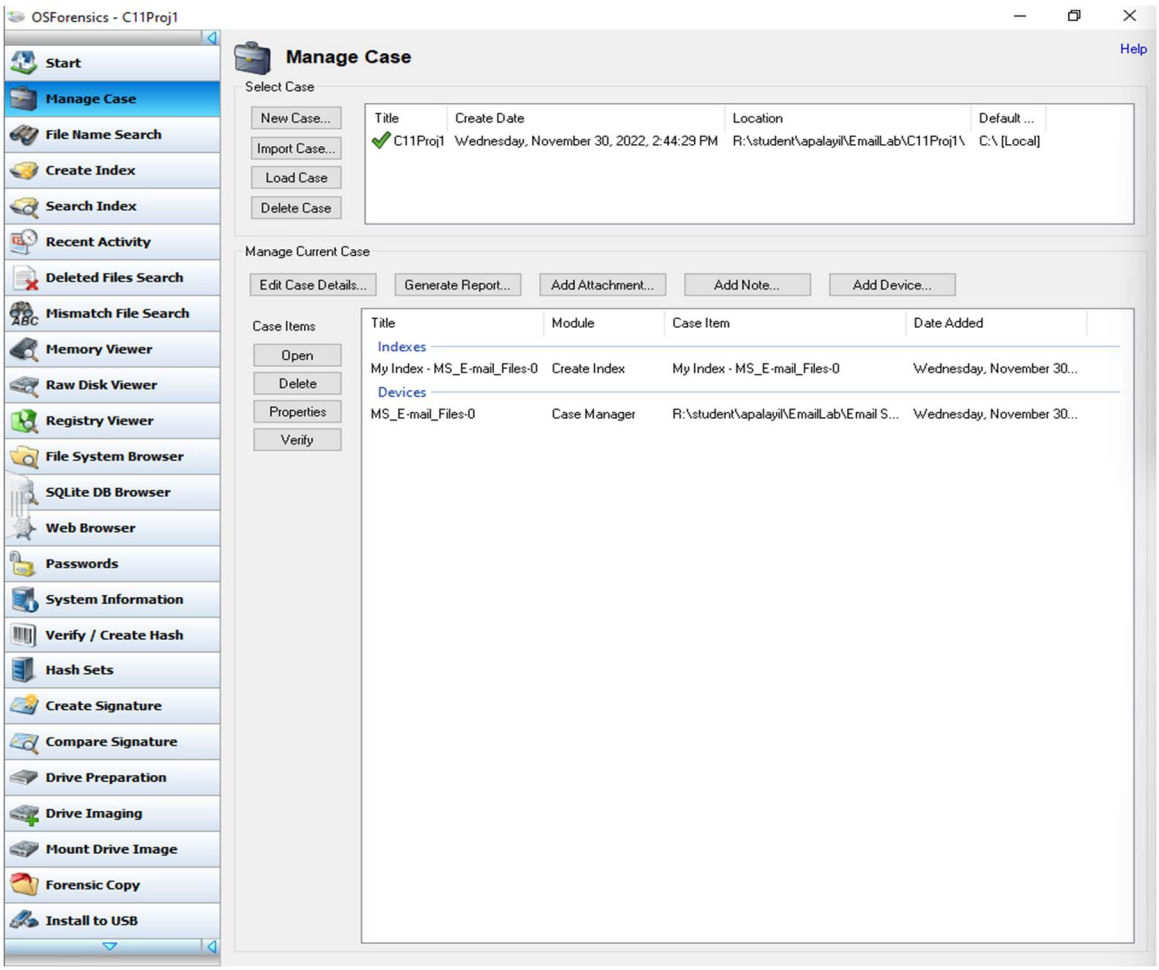
Due Date: 12/02/2022

Email Forensics Using OSForensics:

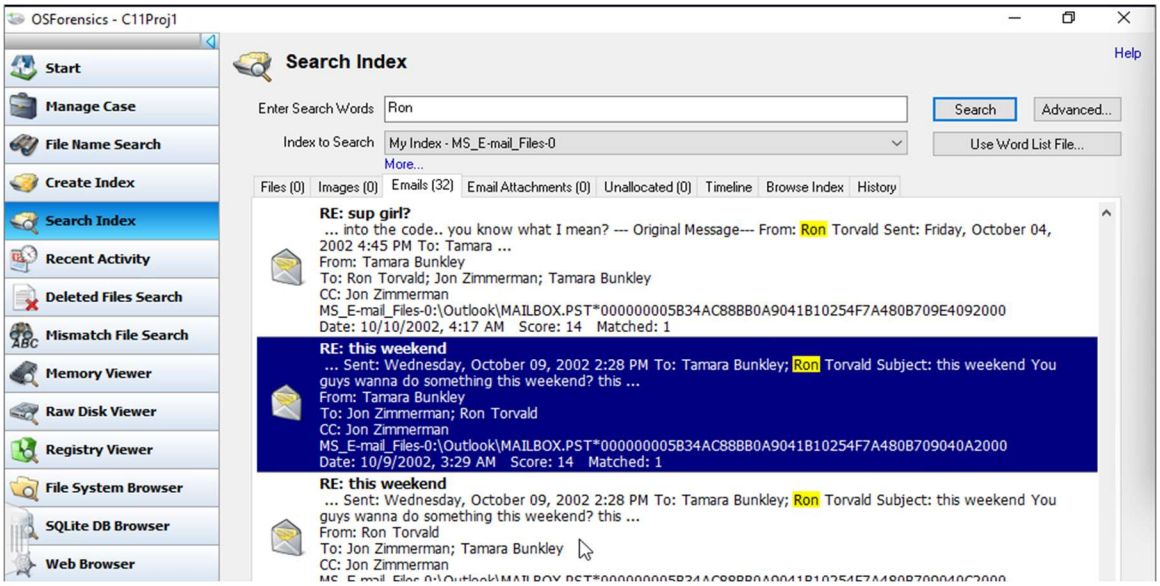
Introduction:

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.

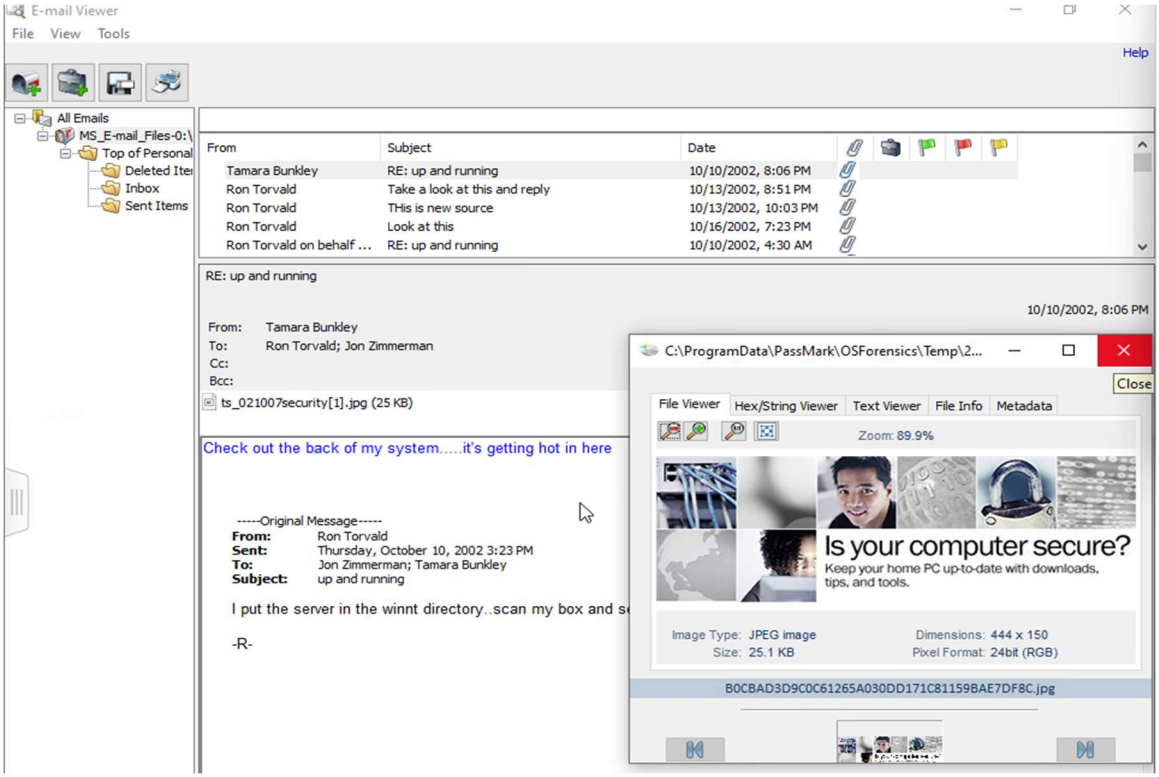
After following through the steps starting from Slide 76 of Email Labs, completing between steps 1~5:



In step 6, we look up the emails from the suspect:



Following through steps 7~9, we can go over the Outlook's Top Personal Folders which includes Deleted Items, Inbox, and Sent Items. The attachments of the emails along with the reply-chains which can viewed in the image below.



Questions asked in the Lab:

1. How many e-mails were deleted from Ron Torvald's Outlook mailbox?
    - There are 3 emails in Ron Torvald's Outlook mailbox that were deleted.
2. How many e-mails with attached files did Ron Torvald get from Tamara Bunkley?
    - Tamara Bunkley sent a total of 3 emails with attached files to Ron Torvald with 1 email written by Ron on behalf of Tamara.
3. Deleted e-mails with attachments can't be viewed. True or False?
    - False, we can view the attachments within deleted e-mails in OSForensics.
4. How many e-mails did you find by using "Ron" as a search keyword?
    - Using "Ron" as a search keyword in OSForensics, there are 32 email chains in the Mailbox.pst folder.
5. How many zipped files are attached to e-mails?
    - There are two zipped files attached to the emails which are named Ackcmd.zip and Source Code 1.zip both the attachments were sent from Ron to Jon Zimmerman and Tamara Bunkley.

Conclusion:

Using OSForensics we are able to view the deleted Outlook mailbox of Ron Torvald and due to software limitations the search was done through the entire image to find email evidence.