Alan Palayil

Due Date: 12/02/2022

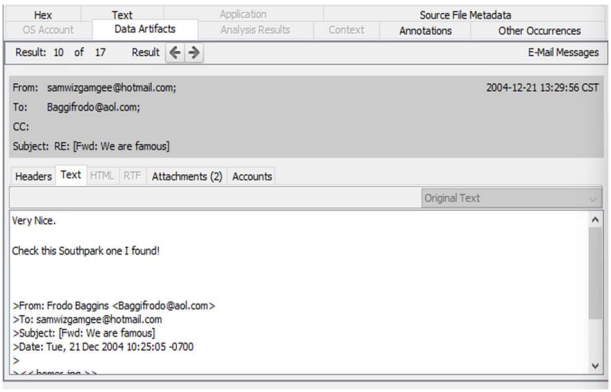
Finding Google Searches and Multiple Email Accounts:

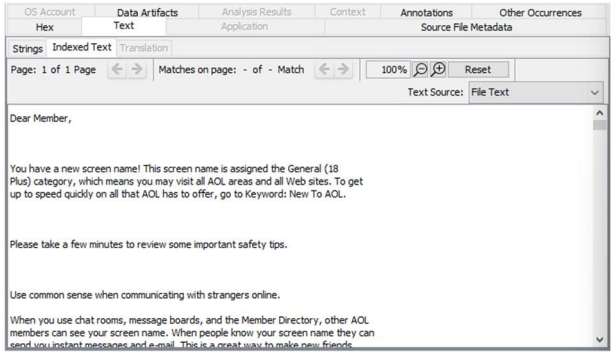
Introduction:

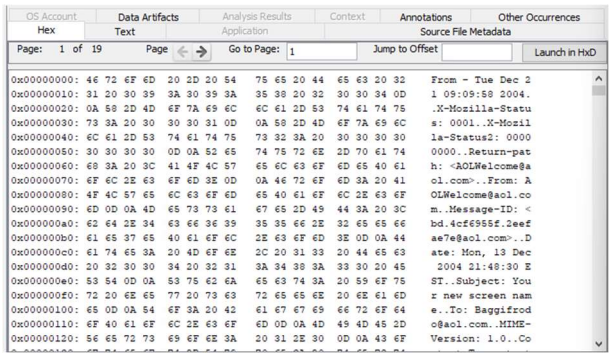
In this lab we execute the three Email Forensics Labs which are conducted on RADISH Windows 10 desktop. Below are the key steps and answers to questions that are asked in each of the labs.

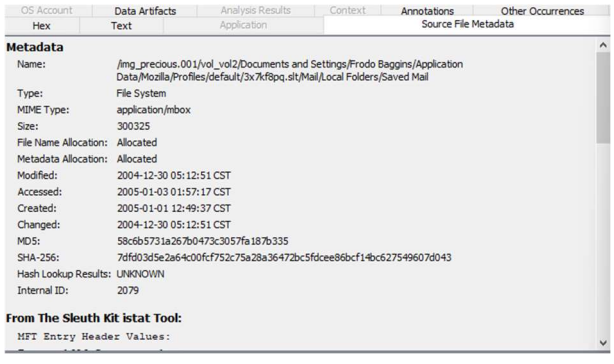
Like how we worked on the previous lab using Autopsy for Email forensics, the steps were similarly overwritten till step 5. With the big exception of excluding the Plaso ingest module in the Configure Ingest Modules window.

At step 6, we are introduced within a new pane to view over the email header to look over various content viewers.

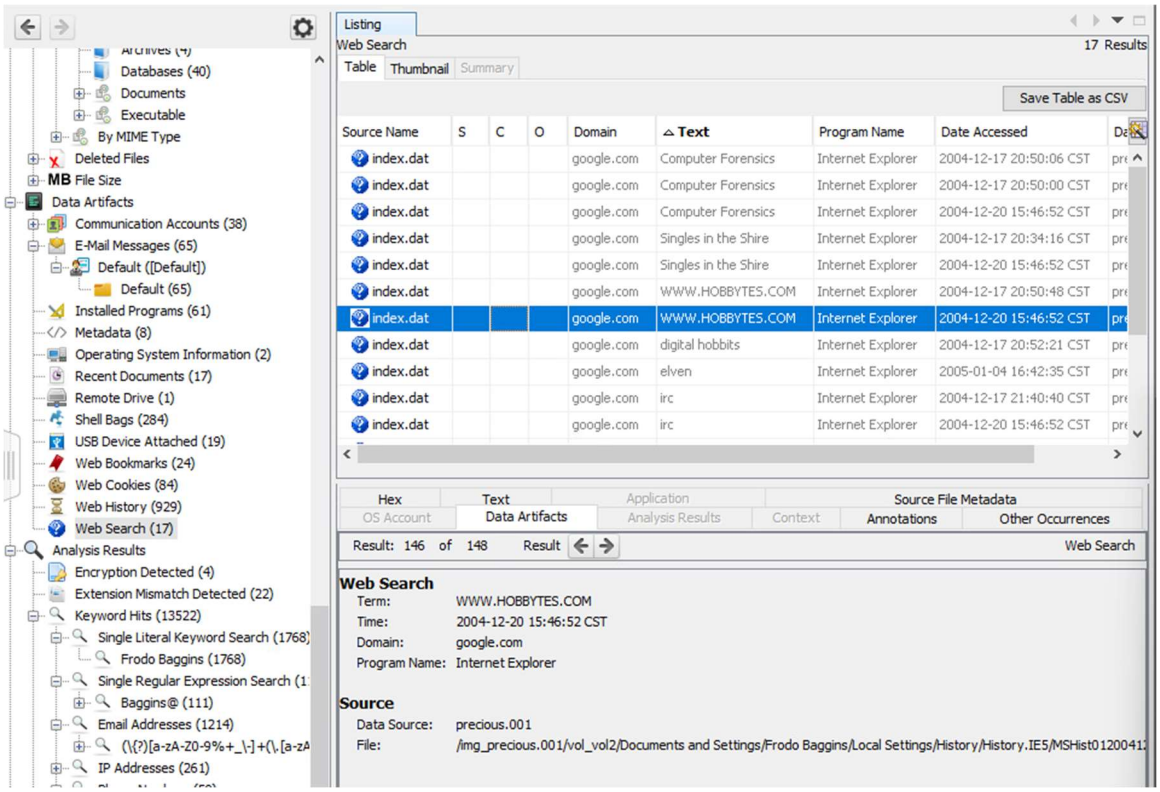




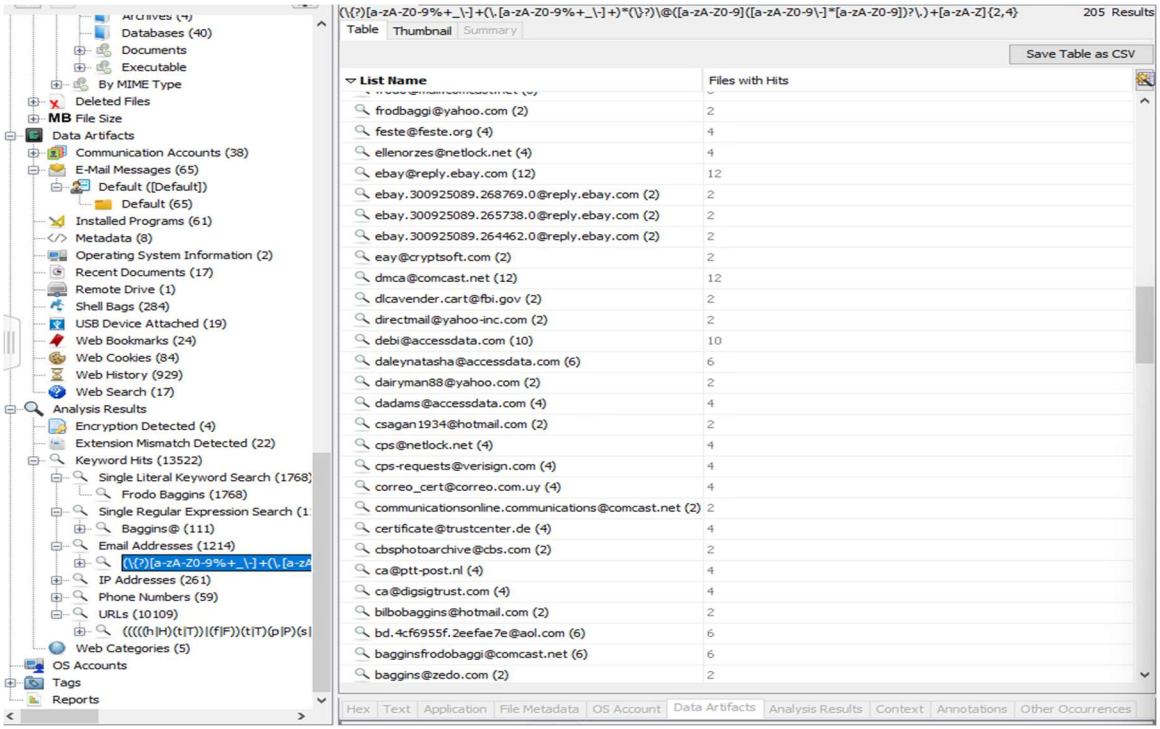




Step 7 we are shown how to navigate to Web Search folder how its viewed in the content view.



Step 8 was like the previous with looking over the email addresses for our suspect Frodo Baggins.



Questions asked in the Lab:

1. How many e-mails, including duplicates, did you find?
    - I found a total of 65 emails which includes duplicates.
2. How many different Frodo Baggins e-mail addresses did Autopsy recover?
    - There were 81 (9) different Frodo Baggins e-mail addresses which were recovered from Autopsy.
3. Frodo Baggins didn't have an AOL e-mail account. True or False?
    - False, Frodo Baggins did have an AOL e-mail account.
4. How many Google searches for the term "computer forensics" were made??
    - There were 3 number of Google searches for the term "computer forensics" were made.
5. MD5 hash values are displayed automatically in the default mailbox view. True or False?
    - False, MD5 hash values aren't displayed automatically in the default mailbox view. We need to click on the Source File Metadata tab to view the MD5 and SHA-256 hash values.

Conclusion:

Using Autopsy, we are able to find e-mail and Google search evidence showing that Frodo Baggins hacked a Windows computer's Registry to discover user account passwords.