

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.

The top screenshot displays the email header and body in the RADISH interface. The header includes the 'From' field (samwizgangee@hotmail.com), 'To' field (Baggifrodo@aol.com), 'Subject' (RE: [Fwd: We are famous]), and 'Date' (Tue, 21 Dec 2004 10:25:05 -0700). The body text reads: 'Very Nice. Check this Southpark one I found! >From: Frodo Baggins <Baggifrodo@aol.com> >To: samwizgangee@hotmail.com >Subject: [Fwd: We are famous] >Date: Tue, 21 Dec 2004 10:25:05 -0700 >'. The bottom screenshot shows the hex view of the email data and the metadata section. The hex view displays the raw data of the email, including the header and body. The metadata section shows details such as 'Name' (/img_preious.001/vol_vol2/Documents and Settings/Frodo Baggins/Application Data/Mozilla/Profiles/default/3x7f8pq.st/Mail/Local Folders/Saved Mail), 'Type' (File System), 'MIME Type' (application/mbox), 'Size' (300325), 'File Name Allocation' (Allocated), 'Metadata Allocation' (Allocated), 'Modified' (2004-12-30 05:12:51 CST), 'Accessed' (2005-01-03 01:57:17 CST), 'Created' (2005-01-01 12:49:37 CST), 'Changed' (2004-12-30 05:12:51 CST), 'MDS' (58c5b5731a267b0473c3057fa187b335), 'SHA-256' (7df03d5e2a64c00fcf752c75a28a36472bc5fdcee86bcf14bc527549607d043), 'Hash Lookup Results' (UNKNOWN), 'Internal ID' (2079), and 'From The Sleuth Kit istat Tool: MFT Entry Header Values:'. The bottom screenshot also shows the 'Launch in HxD' button.

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

The screenshot shows a digital forensics tool interface. The left pane displays a tree view of various data categories, including 'Web Search (17)'. The right pane shows a detailed view of the 'Web Search' results, listing 17 results. The results are displayed in a table with columns: Source Name, S, C, O, Domain, Text, Program Name, Date Accessed, and Document Name. The selected result is 'index.dat' from 'google.com' with the text 'WWW.HOBBYTES.COM' and 'Internet Explorer'.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Document Name
index.dat				google.com	Computer Forensics	Internet Explorer	2004-12-17 20:50:06 CST	pre
index.dat				google.com	Computer Forensics	Internet Explorer	2004-12-17 20:50:00 CST	pre
index.dat				google.com	Computer Forensics	Internet Explorer	2004-12-20 15:46:52 CST	pre
index.dat				google.com	Singles in the Shire	Internet Explorer	2004-12-17 20:34:16 CST	pre
index.dat				google.com	Singles in the Shire	Internet Explorer	2004-12-20 15:46:52 CST	pre
index.dat				google.com	WWW.HOBBYTES.COM	Internet Explorer	2004-12-17 20:50:48 CST	pre
index.dat				google.com	WWW.HOBBYTES.COM	Internet Explorer	2004-12-20 15:46:52 CST	pre
index.dat				google.com	digital hobbits	Internet Explorer	2004-12-17 20:52:21 CST	pre
index.dat				google.com	elven	Internet Explorer	2005-01-04 16:42:35 CST	pre
index.dat				google.com	irc	Internet Explorer	2004-12-17 21:40:40 CST	pre
index.dat				google.com	irc	Internet Explorer	2004-12-20 15:46:52 CST	pre

Below the table, there is a section for 'Web Search' details:

Web Search
Term: WWW.HOBBYTES.COM
Time: 2004-12-20 15:46:52 CST
Domain: google.com
Program Name: Internet Explorer

Source
Data Source: precious.001
File: /img_precious.001/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/MSHist01200411

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

The screenshot shows a digital forensics tool interface. The left pane displays a tree view of various data categories, including 'Email Addresses (1214)'. The right pane shows a detailed view of the 'Email Addresses' results, listing 205 results. The results are displayed in a table with columns: List Name, Files with Hits, and Document Name. The selected result is 'frodbaggi@yahoo.com (2)'.

List Name	Files with Hits	Document Name
frodbaggi@yahoo.com (2)	2	
feste@feste.org (4)	4	
ellenorzes@netlock.net (4)	4	
ebay@reply.ebay.com (12)	12	
ebay.300925089.268769.0@reply.ebay.com (2)	2	
ebay.300925089.265738.0@reply.ebay.com (2)	2	
ebay.300925089.264462.0@reply.ebay.com (2)	2	
eay@cryptsoft.com (2)	2	
dmca@comcast.net (12)	12	
dicavender.cart@fbi.gov (2)	2	
directmail@yahoo-inc.com (2)	2	
debi@accessdata.com (10)	10	
daleynatasha@accessdata.com (6)	6	
dairymen88@yahoo.com (2)	2	
dadams@accessdata.com (4)	4	
csagan1934@hotmail.com (2)	2	
cps@netlock.net (4)	4	
cps-requests@verisign.com (4)	4	
correo_cert@correo.com.uy (4)	4	
communicationsonline.communications@comcast.net (2)	2	
certificate@trustcenter.de (4)	4	
cbsphotoarchive@cbs.com (2)	2	
ca@ptt-post.nl (4)	4	
ca@digsigtrust.com (4)	4	
bilbobaggins@hotmail.com (2)	2	
bd.4cf6955f.2eefae7e@aol.com (6)	6	
bagginsfrodbaggi@comcast.net (6)	6	
baggins@zedo.com (2)	2	

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.