CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 9: Email

Lauren Pixley, Cassidy Elwell, and James Poirier

May 2019 (Version 2)

9

Email Review

Introduction

Email can become a vital part of your investigation. In this case, you are looking for fraudulent coupons and now there are issues with CP. It is important to check email, because you need to know who your suspect was communicating with and if they were trading any data. You know that there were fraudulent coupons and CP associated with a USB device, but could the suspect have also received this type of data from other people?

Suspects can use webmail or software such as Thunderbird or Outlook to view their mail. It can be difficult to sometimes recover any email if the user was just using webmail, since most of it is not stored on the computer itself. However, if the suspect uses software to view their mail, then you can typically see what emails or attachments they sent and received.

Windows 8 Mail App

In Autopsy, click on E-Mail Messages under Results in the left pane. As you can see, Autopsy is reporting that there are zero email messages.

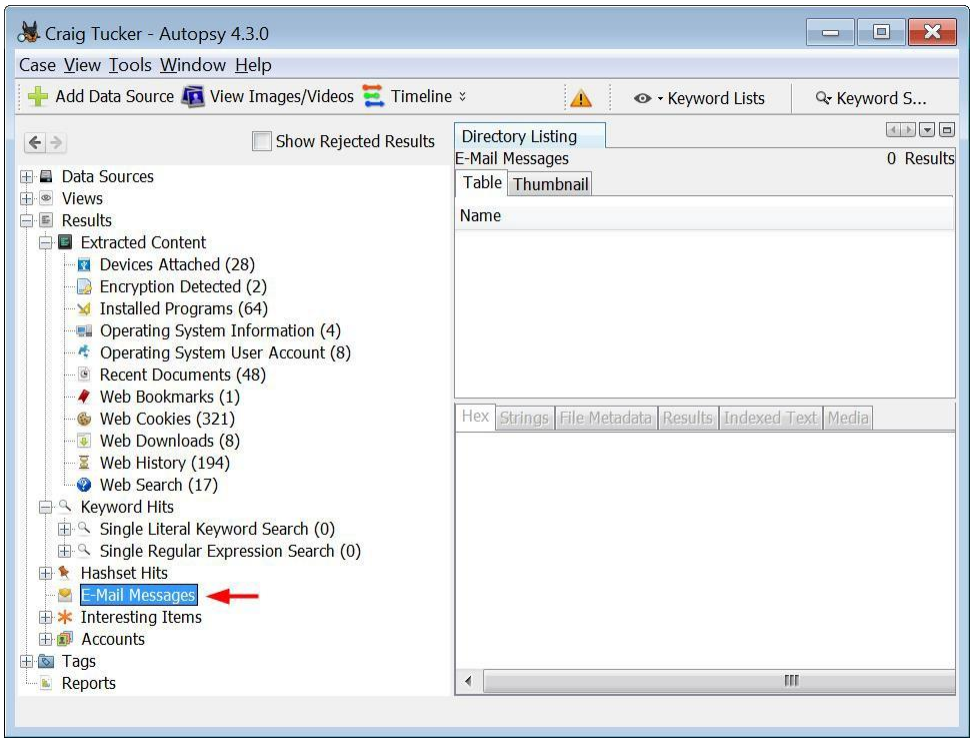

Figure 9-1 – Autopsy Shows Zero E-Mail Messages

Just because Autopsy shows zero email under this tab, that does not necessarily mean the suspect didn't have any email. They could have been using mail through their web browser or they could have been using a mail app that Autopsy does not recognize. You know that for this image, the suspect's operating system is Windows 8. That means the suspect could have been using the built-in Windows 8 Mail app, which is a program that Autopsy does not pull or recognize as email. To see if Craig used the Windows 8 Mail app, navigate to the following subfolder:

```
C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_
8wekyb3d8bbwe\LocalState\Indexed\LiveComm\ba871ed4e8a350e0\120712-
0049\Mail\1
```

In a Windows 10 image, the path is slightly different to get to all the emails and the way they are stored is not the same as it was in Windows 8 and earlier. Now, they are stored as .dat files which can be opened through a web browser. This adds a level of security in Windows 10 for consumers, but makes your job as a forensic examiner more difficult. To see if Craig had used the Windows 10 Mail app, you would navigate to the following subfolder:

```
C:\Users\Craig\AppData\Local\Comms\Unistore\data/1/a
```


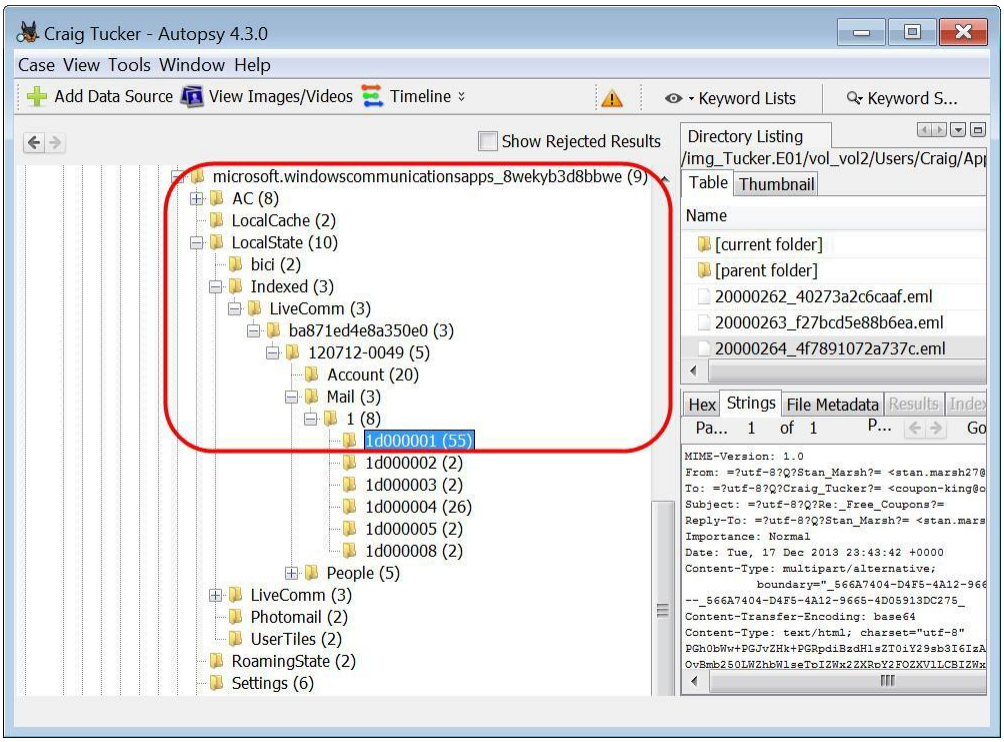

Figure 9-2 – Subfolders for Windows 8 Mail App

Below the Mail\1 subfolders, there are six subfolders. These subfolders that are named 1d00000# represent a mail folder, such as Inbox, Sent, Deleted. Take a look at the first eml file in the 1d000001 subfolder that has the subject “Free Coupons”.

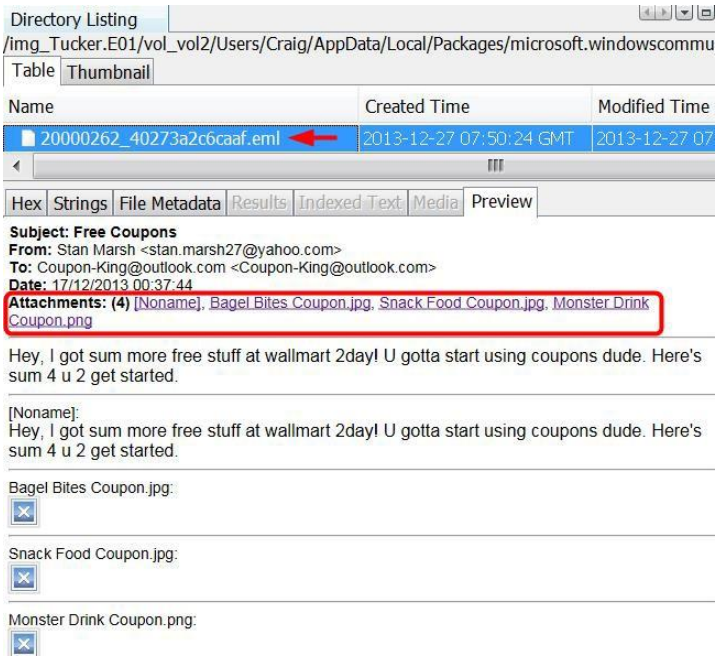

Figure 9-3 – Free Coupons Email in 1d000001 Subfolder

This email is from someone named Stan Marsh and they sent 3 attachments. Since this relates to your investigation, go ahead and tag the eml file with any tag name you prefer (see Figure 9-4).

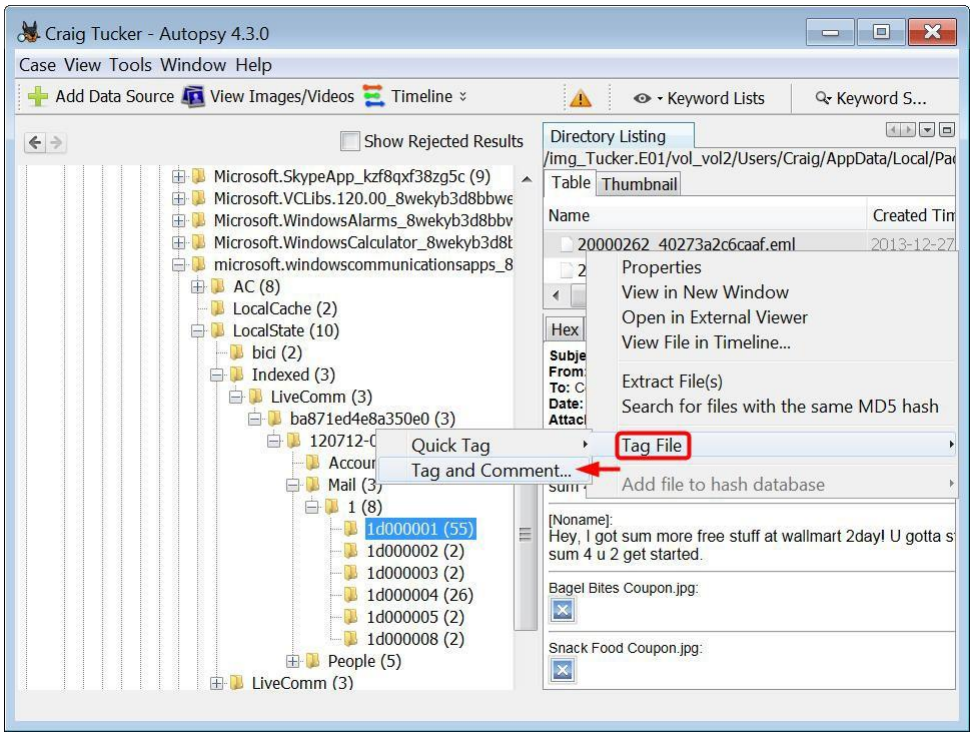

Figure 9-4 – Tag Free Coupons Email

Attachments

With Windows 8 mail, all of these emails are being stored in eml files. If you look at the line in the email called "Attachments", you will see the names of three jpgs attached to the email. With Windows 8 mail, the user has to download the attachments. Even when the attachments are downloaded, they are not encoded and stored in the same eml file as the email. If the user downloaded the attachment from mail, it is stored in an attachment folder called Att.

First, take a look at the eml file that this email is being stored in. One thing you should check before looking at the attachments folder is the first part of the eml name. This number is the Message ID and will match the email's attachment folder. Make note that the Free Coupons email attachment folder will be named 20000262. The attachment folder is located in:

```
C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_
8wekyb3d8bbwe\LocalState\LiveComm\ba871ed4e8a350e0\120712-0049\Att
```

There are several subfolders below the Att folder, and their name matches up to an eml file name. Look for the subfolder 20000262. This contains the Free Coupons email attachments (see Figure 9-5).

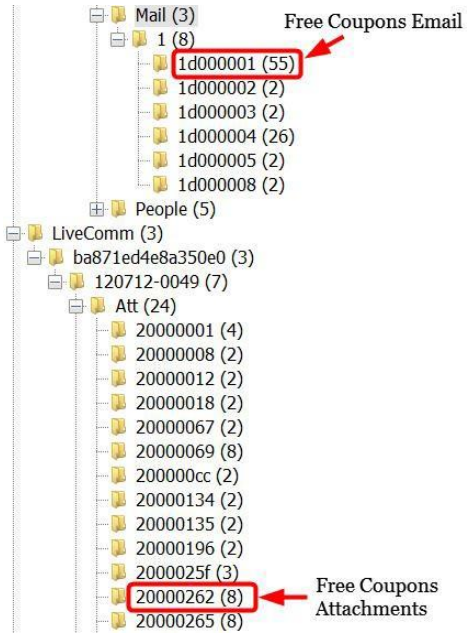

Figure 9-5 - Email Stored under Mail Subfolder and Attachments Stored in Corresponding Att Subfolder

The three jpg files in the Att subfolder match the names of the attachments you saw in the email.

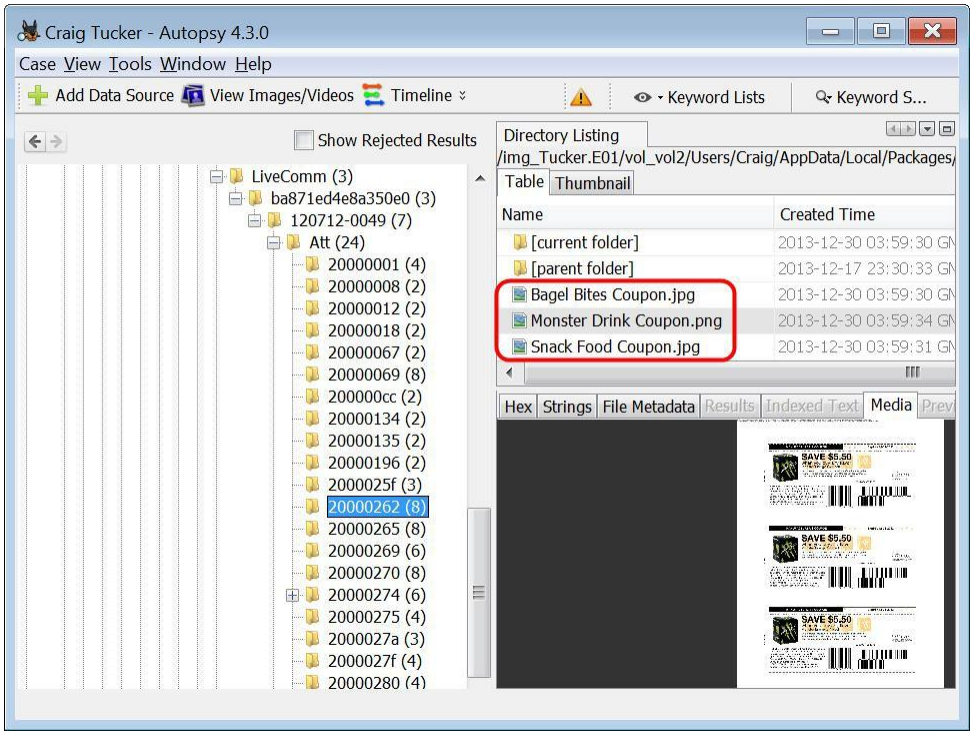

Figure 9-6 - Free Coupons Email Attachments

The Monster Drink coupon was one of the coupons Craig was caught with. Go ahead and tag these three picture attachments.

Windows 10 Mail App

In Autopsy, click on E-Mail Messages under Results in the left pane. As you can see, Autopsy is reporting that there are zero email messages again.

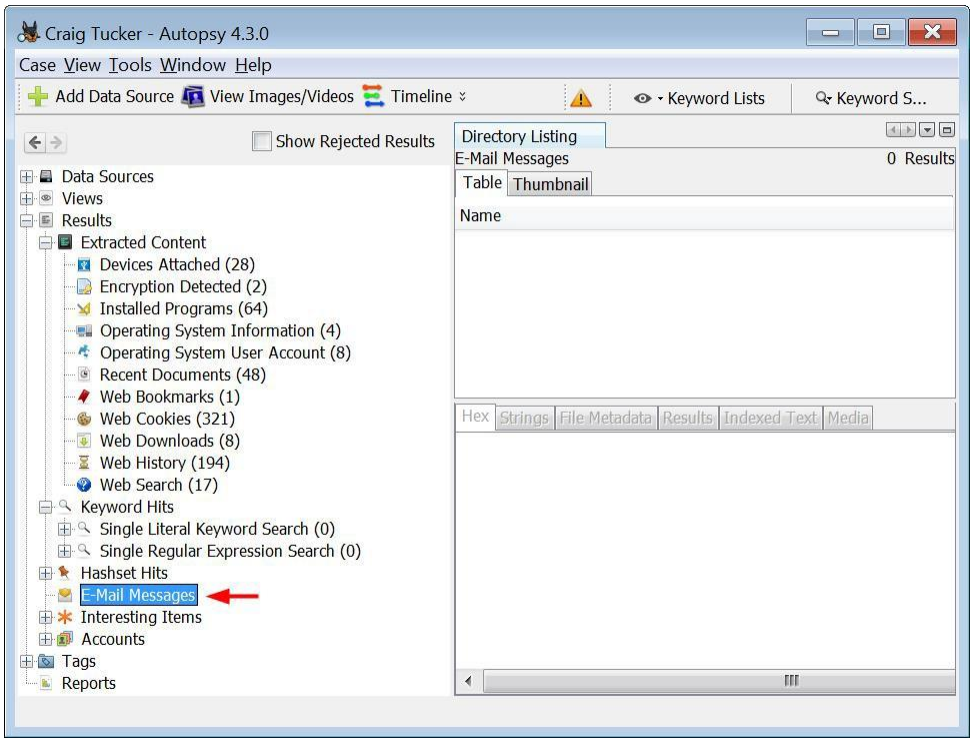

Figure 9-7 – Autopsy Shows Zero E-Mail Messages

Windows 10 Mail stores the emails in the following subfolder:

```
C:\Users\Craig\AppData\Local\Comms\Unistore\data\1\a
```

Once you have navigated to the data folder, there will be numbered folders with corresponding lettered folders containing the emails. The emails are web based in Windows 10 Mail, which means that you cannot simply export them as a .eml file. The files save by default as .dat files now, which for your purposes is a way to save HTML source code and view the email.

The easiest way to convert these to a readable format unless you are comfortable reading html source code is to simply change the file extension to a .html. This will allow you to open the .dat file in a web browser of your choice and see what the formatted message looks like. To do this, open the .dat file in notepad or some other text editor and click the "Save As" button. This will give you the option to change the extension and open it in a web browser. When it is saved, you should have an icon that looks like the web browser that you chose (In this example, Google Chrome was used)

Note: You MUST open the .dat file in notepad or another text editor before changing the file extension. If you don't it will put null characters between all of your letters and make it unreadable by the browser. We recommend that you use notepad (not notepad++) because it is a good basic text editor that comes pre-installed on all windows machines.

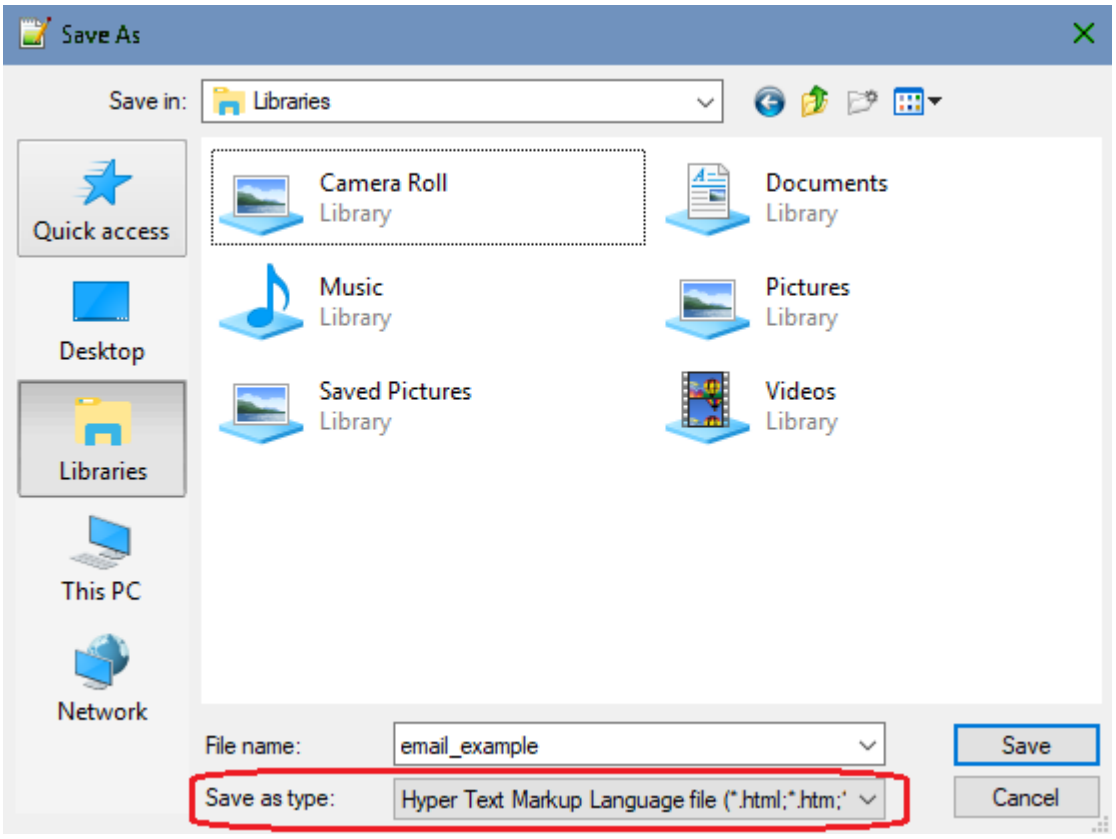

Figure 9-8 – Saving the email as a .html

The new email file will appear wherever you saved it last, so it is recommended to use either the export folder or create an emails folder to place all of the newly converted .html files for easy access. Note that you should include in your report that you had to export and change the extensions, since that is technically modifying evidence and without reason can cause your discovered data to be dismissed.

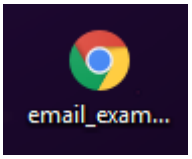

Figure 9-9 – New email_example file that can be opened in a web browser to view

MD5 Hash

There are several coupons in Craig's email attachment folder. If you want to know if Craig has these files saved anywhere else on his computer, you can conduct a search for the coupon based on its MD5 hash value.

A hash value is basically a fingerprint for a file. The chance of two MD5 hash values being the same is 2^{128}. You can use hash values to exclude known files, such as Windows operating system files. There are also "hash libraries", which are large files that contain hash values of alert files, such as CP or hacking software. You can then run these alert hash libraries against the hash values in the image to quickly see if the user has any of these "bad" files.

To find the hash value for files, you will need to run the Hash Lookup plugin. Click Tools►Run Ingest Modules►Tucker.E01. When the Run Ingest Modules window opens, check Hash Lookup and then click Start.

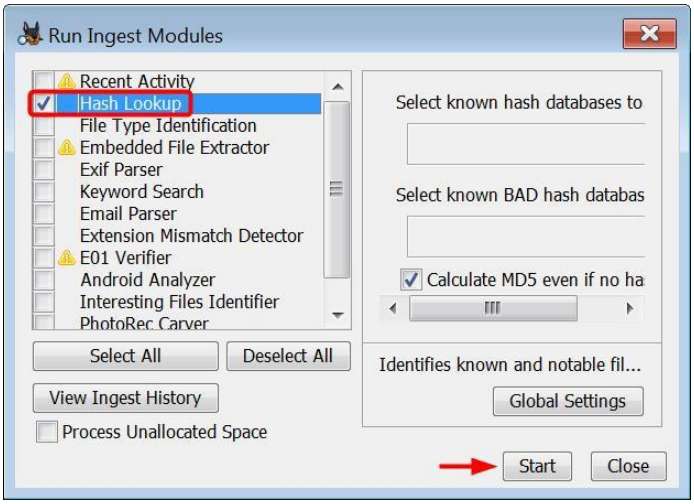

Figure 9-10 – Check Hash Lookup and Click Start

Once Autopsy finishes processing the hash values, take a look at the file 1353033721971.png in the 20000270 attachment subfolder (see Figure 9-8).

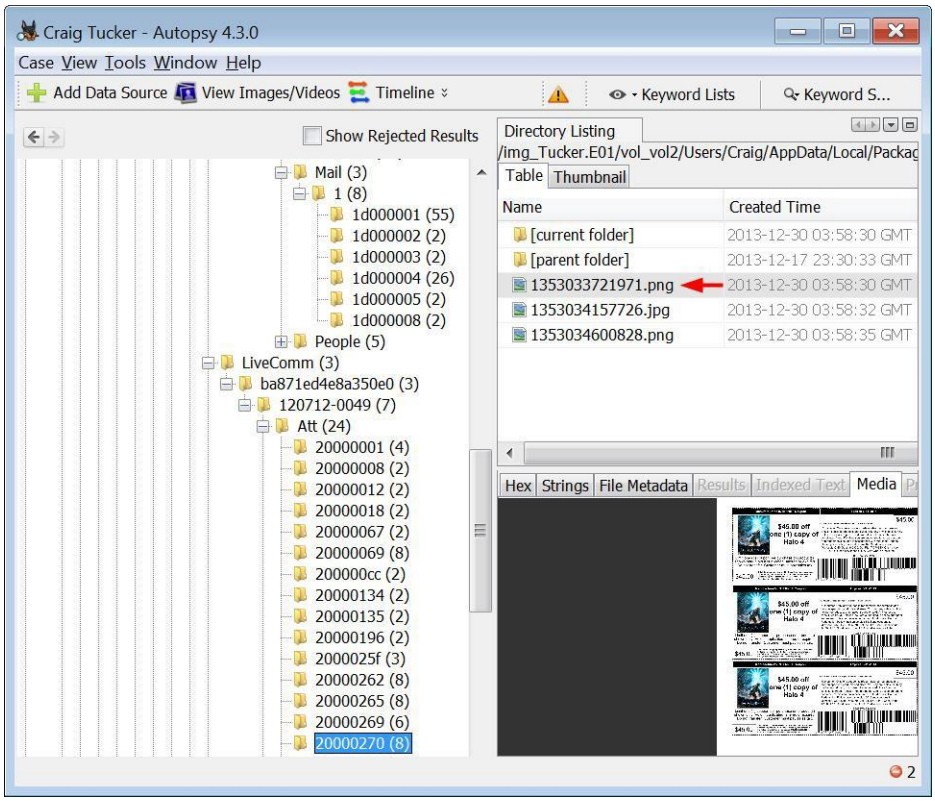

Figure 9-11– Coupon in 20000270 Attachment Subfolder

These attachments come from the 20000270 eml file in the 1d000001 mail subfolder.

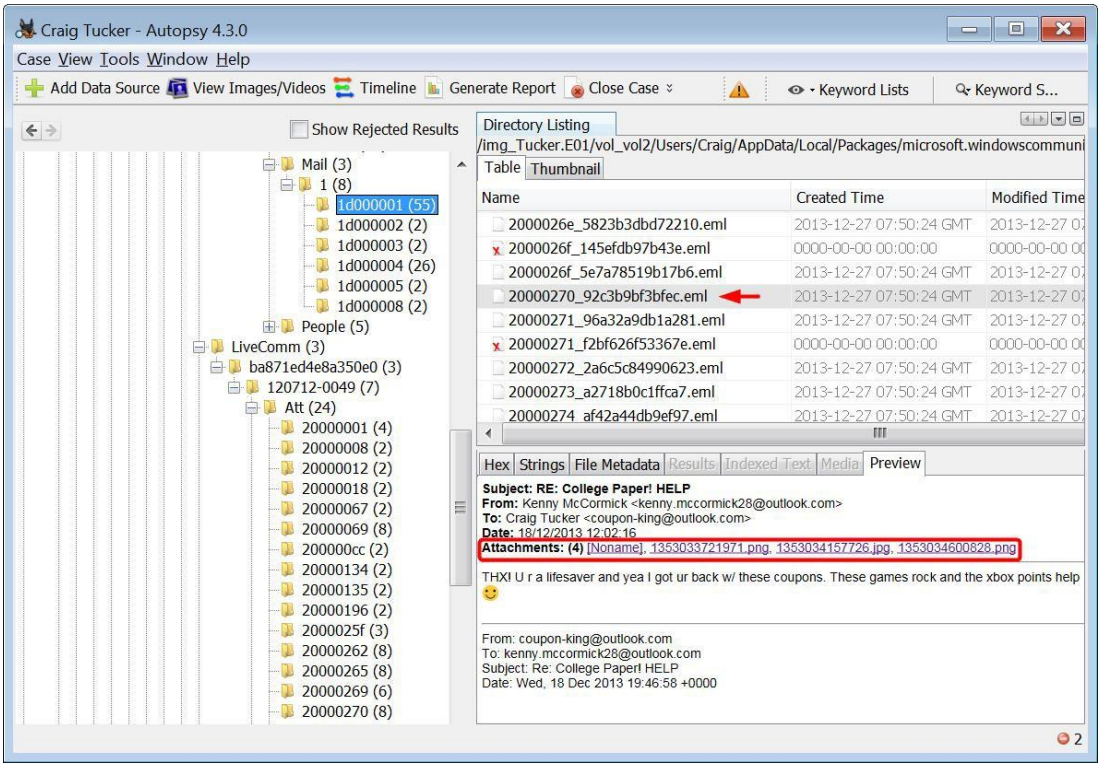

Figure 9-12 – Email with Coupon Attachments

If you want to see if these coupons are saved anywhere else on the computer, right-click the first coupon in the 20000270 attachment subfolder and click Search for Files with the Same MD5 Hash.

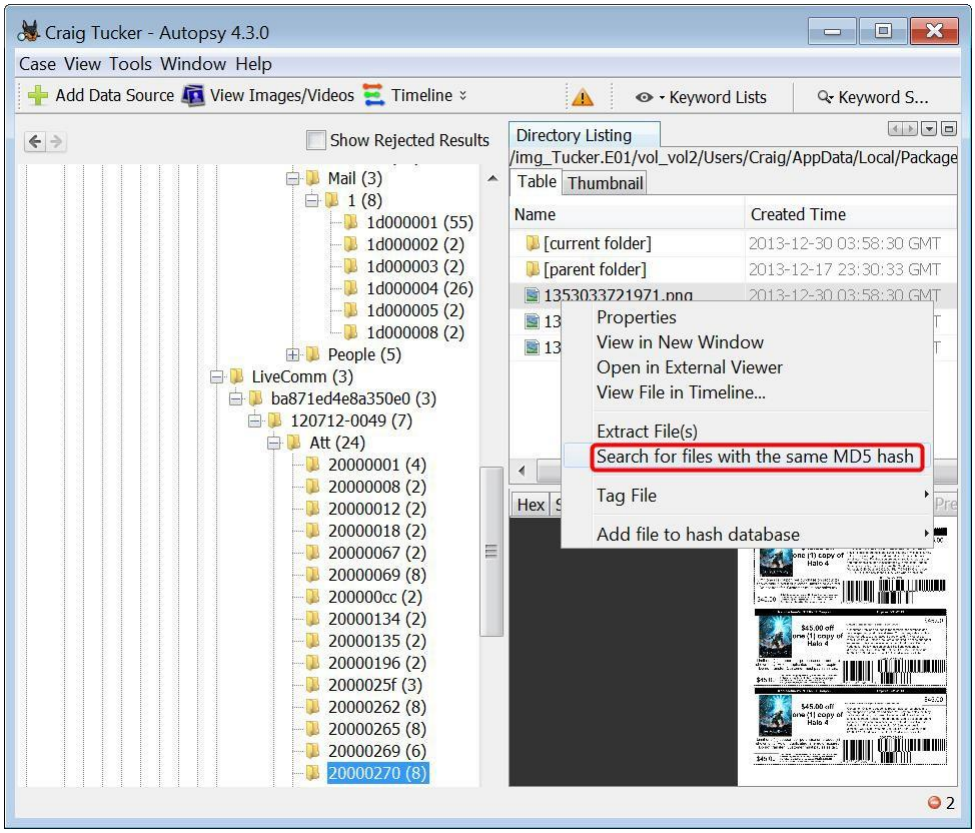

Figure 9-13 – Right-Click Coupon in 20000270 Attachment Subfolder and Search for Hash

There are three matches based on the MD5 hash value. One of the matches is in Craig's My Stuff folder and the other two matches are located in downloaded ZIP files. In the next chapter, you will look into where these downloaded ZIP files came from.

Name	Location
1353033721971.png	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunications...
1353033721971.png	/img_Tucker.E01/vol_vol2/Users/Craig/Documents/My Stuff/1353033721971.png
1353033721971.png	/img_Tucker.E01/vol_vol2/Users/Craig/Downloads/Coupons.zip/Coupons/1353033721971.png
1353033721971.png	/img_Tucker.E01/vol_vol2/Users/Craig/Downloads/Coupons.zip/Coupons/1353033721971.png

Figure 9-14 - MD5 Hash Match Locations

Email (Continued)

You should continue to look over and tag any emails or attachments of interest to your investigation. One email in particular you should check is the "Re: More Hot Pics", which is under the 20000286 eml in the 1d000004 mail subfolder.

If you remember from earlier, you found link files that pointed to CP. You then found two pictures and a video in the recycle bin. This email mentions "underage pictures", but there aren't any attachments since the original email, "More Hot Pics" is gone. You will go over this later, but tag the email for now.

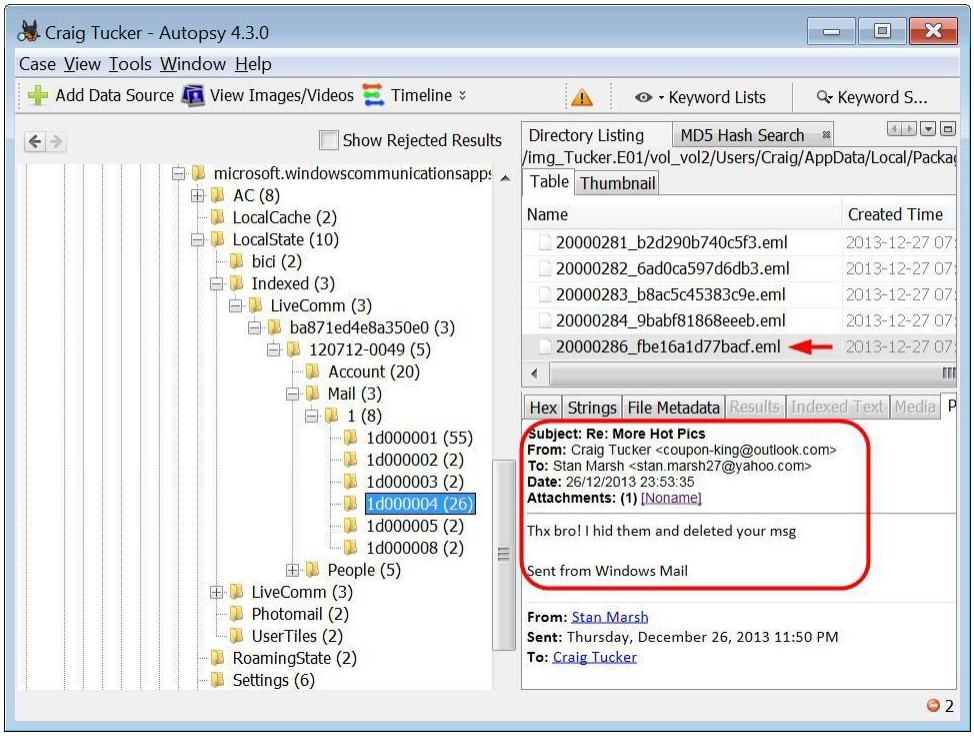

Figure 9-15 – Potential CP Email

Note: The way these emails and attachments are being stored is specific to Windows 8 mail. See Appendix E for information on Windows Live Mail and Mozilla Thunderbird.

Contacts and Keyword Search

With Windows 8 mail, you can see the user's contacts under the People folder, which is located at:

```
C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_
8wekyb3d8bbwe\LocalState\Indexed\LiveComm\ba871ed4e8a350e0\120712-0049
\People\AddressBook
```

Each file in the AddressBook folder will show a contact name and email address. Craig only has one actual contact: Kenny McCormick.

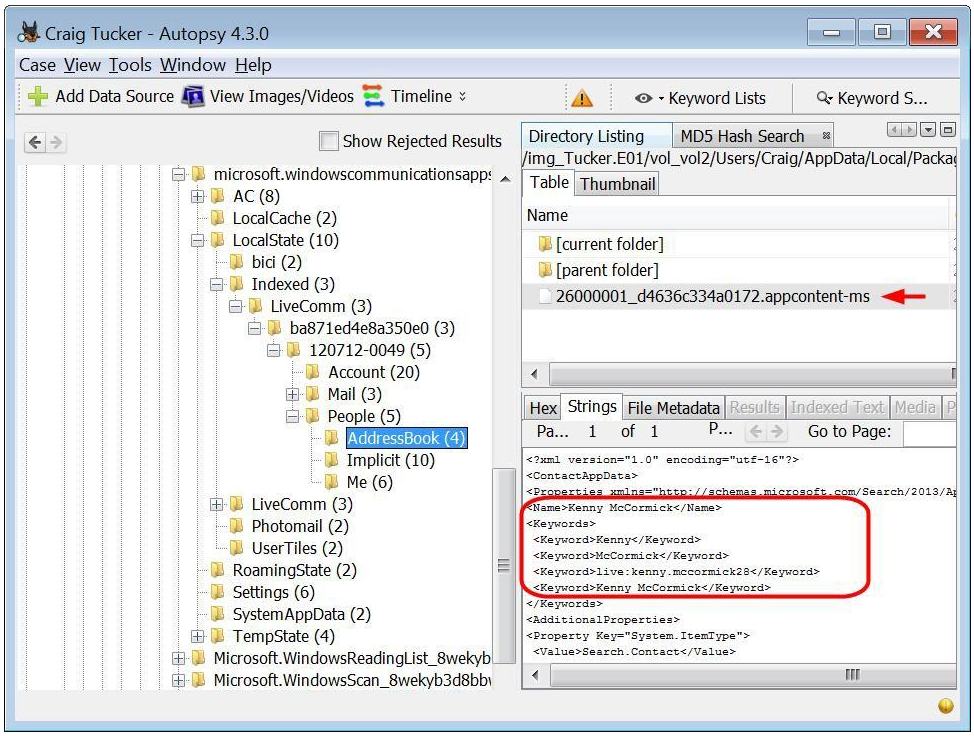

Figure 9-16 - Craig's Email Contact

Look at the subfolder called Implicit under the People folder (see Figure 9-14). Each file in this list shows a name and email address that Craig either sent emails to or received emails from. This information is stored here so when a user begins typing in who the email is "To:", a drop down menu will appear and allow you to auto complete a name or email address.

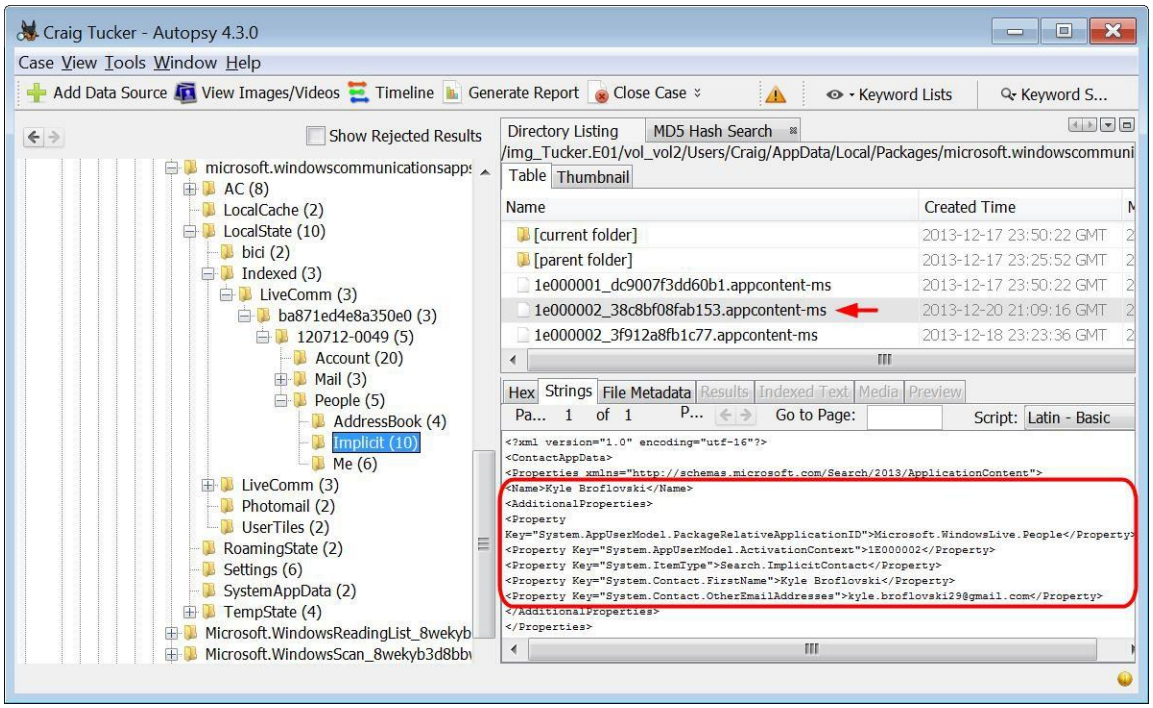

Figure 9-17 - People Craig Sent Email To or Received Email From

Between the AddressBook and Implicit subfolders, you can tell that Craig sent emails to and received email from:

Kyle Broflovski

Stan Marsh

Kenny McCormick

Since Craig was discussing coupons with these three people, go ahead and conduct a Keyword Search for them to see if their names show up anywhere else. To run a Keyword search, you need to first run the Keyword Search plugin. Click Tools►Run Ingest Modules►Tucker.E01. When the Run Ingest Modules window opens, check Keyword Search and click Start.

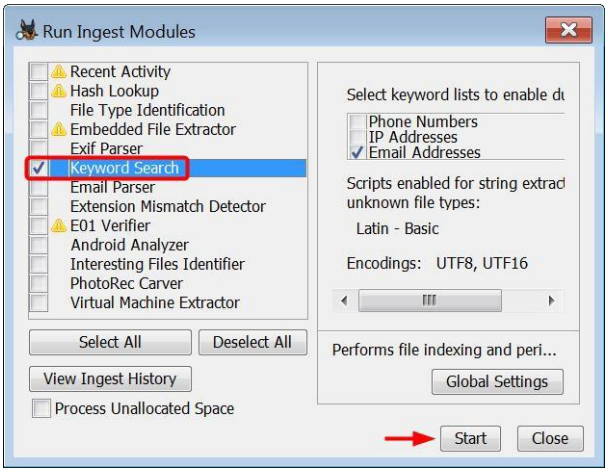

Figure 9-18 – Check Keyword Search Plugin and Click Start

Once Autopsy finishes processing, click the Keyword Search button in the top right corner. Type in Craig's first contact, "Kenny McCormick", and then click the Search button.

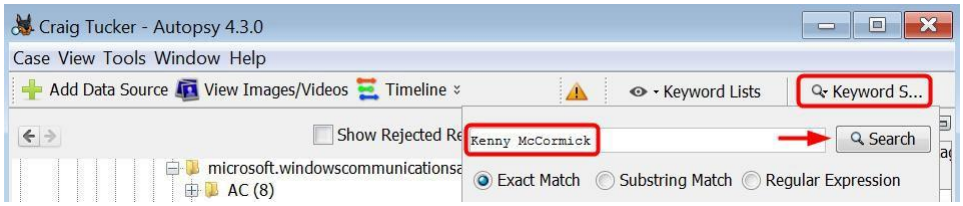

Figure 9-19 – Conduct Keyword Search for Kenny McCormick

You should see several results in the table pane. One keyword search result of particular interest is the main.db file. This file is a database for Skype.

Table | Thumbnail

Name	Location
20000275_d3734e1d1aa77.eml	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps...
20000280_4003b9ba1d2c9a.eml	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps...
1e000066_aee915a8efc74b.appcontent-ms	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps...
main.db	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/Microsoft.SkypeApp_kzf8qxf38zg5c/Loc...
pagefile.sys	/img_Tucker.E01/vol_vol2/pagefile.sys
main.db-journal	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/Microsoft.SkypeApp_kzf8qxf38zg5c/Loc...
$LogFile	/img_Tucker.E01/vol_vol2/$LogFile
livecomm.edb	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps...
Microsoft-Windows-PushNotification-Platform%	/img_Tucker.E01/vol_vol2/Windows/System32/winevt/Logs/Microsoft-Windows-PushNotification-Platfor...
2000026f_5e7a78519b17b6.eml	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps...
edb00009.log	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps...
edbtmp.log	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps...
26000001_d4636c334a0172.appcontent-ms	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps...

Figure 9-20 – Keyword Search Results for Kenny McCormick

Since there are search hits in the Skype database for Kenny McCormick, this indicates that Craig may have been using Skype to communicate with him. Make note of this, because later you will look into chat programs that Craig may have used.

