

Maria Valencia

CSC 153

Lab 11

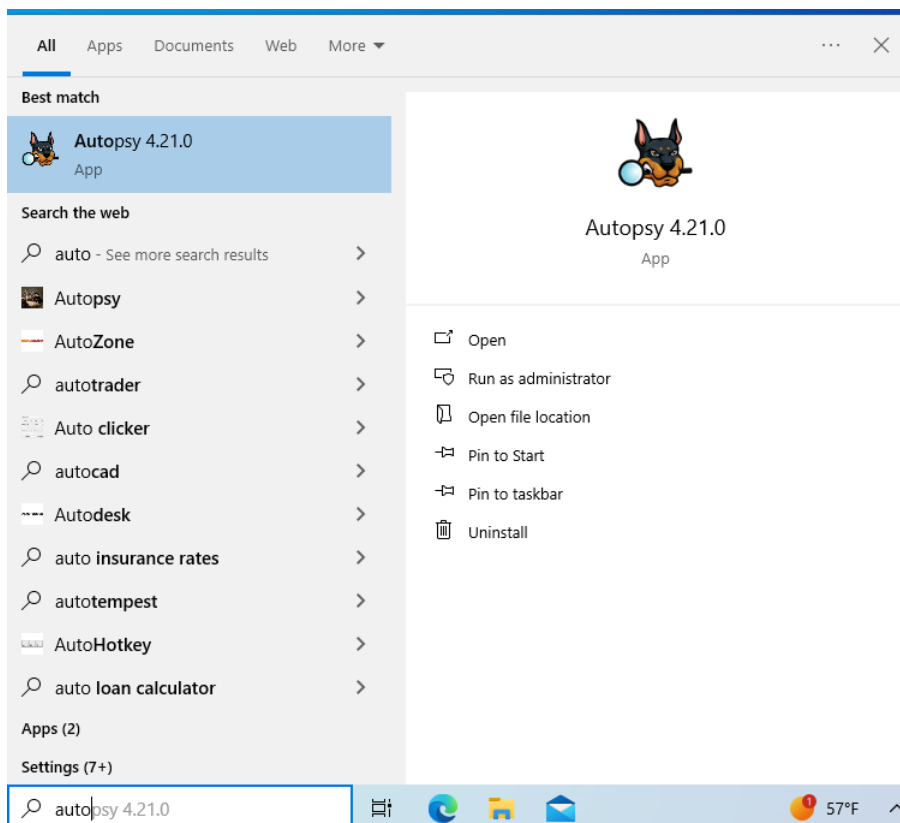
Lab 11: Email and Social Media

Task 1 – Recover PST Emails

In this task, I will collect email evidence from the Jim Shu. Pst image using Autopsy. After I have identified evidence email, i will analyze email headers using the online MXToolBox

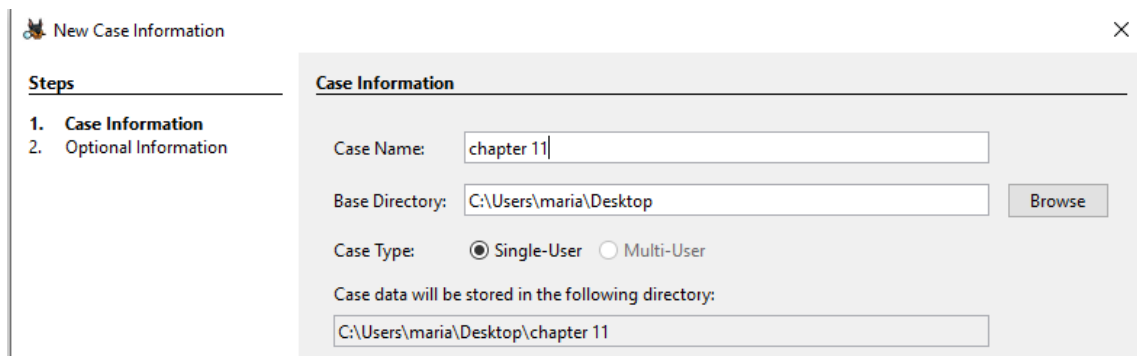
Step 1: Install Autopsy

From my windows VM I check if I have Autopsy installed, and I do!



Step 2: Create Case

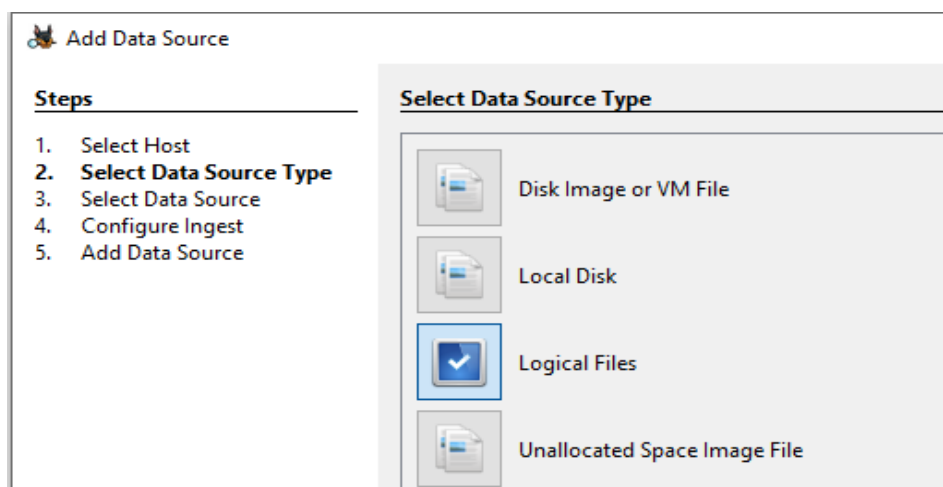
I copied the "Jim Shu.pst" file to my windows VM and launched Autopsy. I create a new case calling it Chapter 11.



The 'New Case Information' dialog box is shown. It has a 'Steps' sidebar with '1. Case Information' and '2. Optional Information'. The 'Case Information' section contains the following fields:

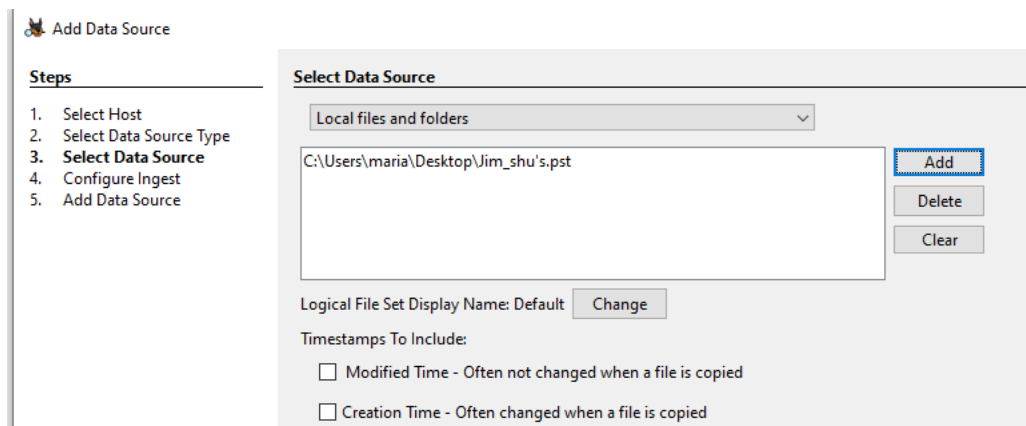
- Case Name: chapter 11
- Base Directory: C:\Users\maria\Desktop (with a 'Browse' button)
- Case Type: ☒ Single-User ☐ Multi-User
- Case data will be stored in the following directory: C:\Users\maria\Desktop\chapter 11

Add the "Jim Shu's.pst" file as the Data Source by selecting "Logical Files" during the "Select Data SourceType" step of the Add Data Source wizard. Press the Add button and navigate to the PST file during the "Select Data Source" step of the wizard.



The 'Add Data Source' wizard is shown at Step 2: 'Select Data Source Type'. The 'Steps' sidebar lists: 1. Select Host, 2. **Select Data Source Type**, 3. Select Data Source, 4. Configure Ingest, 5. Add Data Source. The main area shows four options with icons:

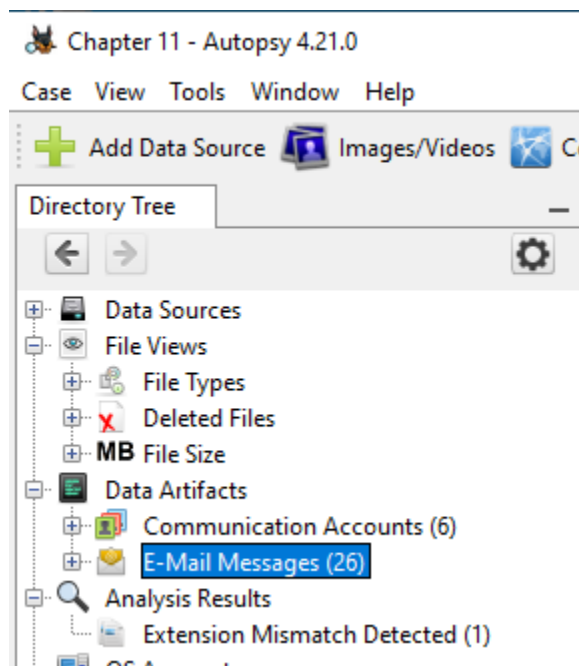
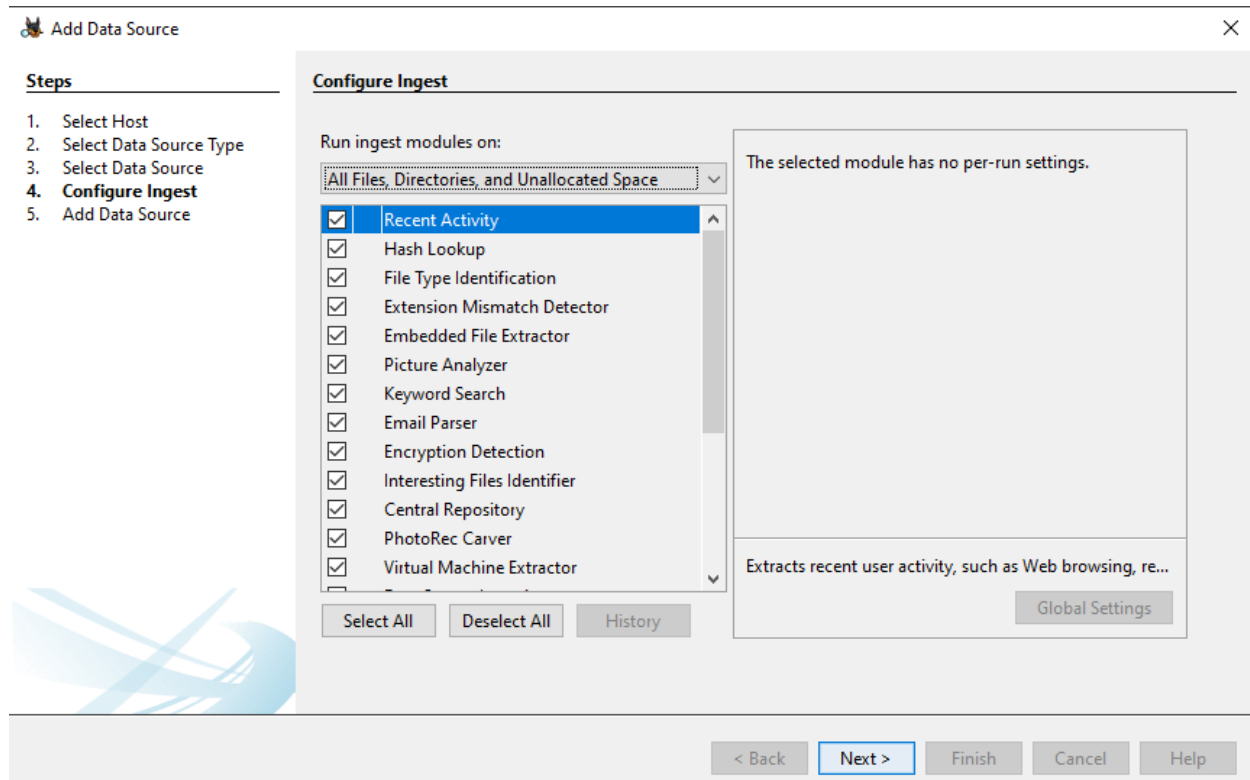
- Disk Image or VM File
- Local Disk
- Logical Files** (highlighted with a blue border and a checkmark icon)
- Unallocated Space Image File



The 'Add Data Source' wizard is shown at Step 3: 'Select Data Source'. The 'Steps' sidebar lists: 1. Select Host, 2. Select Data Source Type, 3. **Select Data Source**, 4. Configure Ingest, 5. Add Data Source. The main area shows:

- A dropdown menu set to 'Local files and folders'.
- A text box containing the path: C:\Users\maria\Desktop\Jim_shu's.pst
- Buttons: 'Add' (highlighted with a blue border), 'Delete', and 'Clear'.
- A field for 'Logical File Set Display Name: Default' with a 'Change' button.
- A section 'Timestamps To Include:' with two unchecked checkboxes:
 - ☐ Modified Time - Often not changed when a file is copied
 - ☐ Creation Time - Often changed when a file is copied

Make sure that at least the module "Email Parser" is selected, if not all modules, during the "Configure Ingest" step. Press finish and allow a minute for the analysis to complete. Observe that "E-Mail Messages" were discovered in the Data Artifacts section of the tree pane.



Step 3: Analyze Email Attachment

With the PST file loaded as a Data Source in your Chapter 11 case in Autopsy, I am now ready to investigate the emails discovered. Find the from Jim Shu and to 5amspade@myway.com that has an attachment. Select the email and choose the Attachments subtab.

The screenshot shows the Autopsy interface with the 'Data Sources' pane on the left. The 'E-Mail Messages (26)' folder is selected under 'Data Artifacts'. The 'Default' subfolder is expanded, showing a list of 26 results. The 'Listing' pane displays a table with columns: Source Name, S, C, O, E-Mail From, and E-Mail To. The first row is highlighted, showing 'Jim_shu's.pst' as the source, 'Jim Shu <Jim_shu@comcast.net>' as the sender, and '5amspade@myway.com' as the recipient. The 'Data Content' pane shows the email headers: From: Jim Shu <Jim_shu@comcast.net>, To: '5amspade@myway.com', CC: , Subject: RE: Bike spec's, and Date: 2006-12-03 19:07:00 PST. The 'Attachments (1)' subtab is selected, showing a table with columns: Location, Size, Mime type, and Known. The first row is highlighted, showing the attachment path '/LogicalFileSet1/Jim_shu's.pst/AC19.gpj', size 6720, mime type 'image/jpeg', and known status 'unknown'.

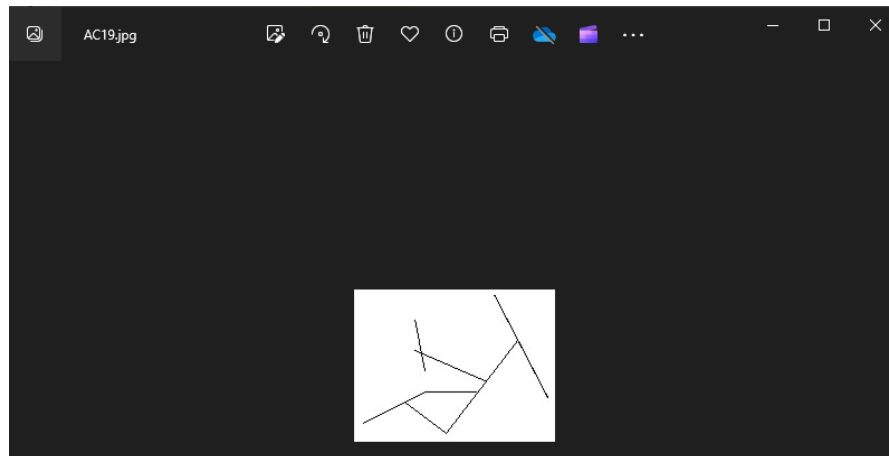
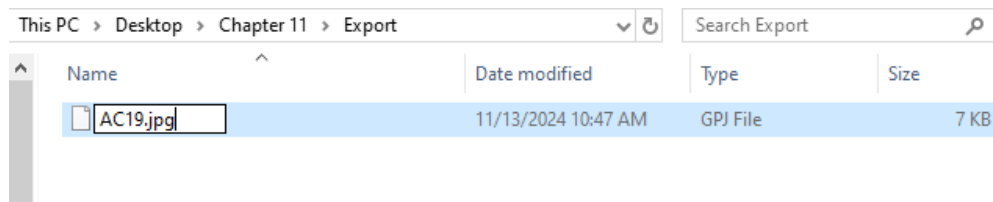
Source Name	S	C	O	E-Mail From	E-Mail To
Jim_shu's.pst				Jim Shu <Jim_shu@comcast.net>	'5amspade@myway.com'
lim_shu's.net				lim Shu <lim_shu@comcast.net>	'lim_shu1@yahoo.com'

Location	Size	Mime type	Known
/LogicalFileSet1/Jim_shu's.pst/AC19.gpj	6720	image/jpeg	unknown

Observe the attachment Mime type is "image/jpeg" which corresponds to its magic bytes. Right-click the "AC19.gpj" attachment and Extract File and save. Navigate to your case's folder page and observe the extension of the file is GPJ. Change the file extension to ".jpg" and open the file.

The screenshot shows the context menu for the attachment 'AC19.gpj'. The menu options are: View File in Directory, View File in Timeline..., View in New Window, Open in External Viewer Ctrl+E, Extract File(s), Export Selected Rows to CSV, Add File Tag, and Remove File Tag. The 'Extract File(s)' option is highlighted.

Location
/LogicalFileSet1/Jim_shu's.pst/A



Step 4: Analyze Email Headers

Find the one email from baspen99@aol.com to Jim and select it. Navigate to the Headers subtab and copy the contents (excluding the first/last line with HEADERS/END HEADERS).

Listing
Default 26 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	E-Mail From	E-Mail To
Jim_shu's.pst				Sam <5amspace@myway.com>	Jim_shu@comcast.net
Jim_shu's.pst				baspen99@aol.com <baspen99@aol.com>	jim_shu@comcast.net
Jim_shu's.pst				Sam <5amspace@mvwav.com>	Jim_shu@comcast.net

Data Content

Hex	Text	Application	Source File Metadata	OS Account
Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences

Result: 9 of 32 Result

E-Mail Messages

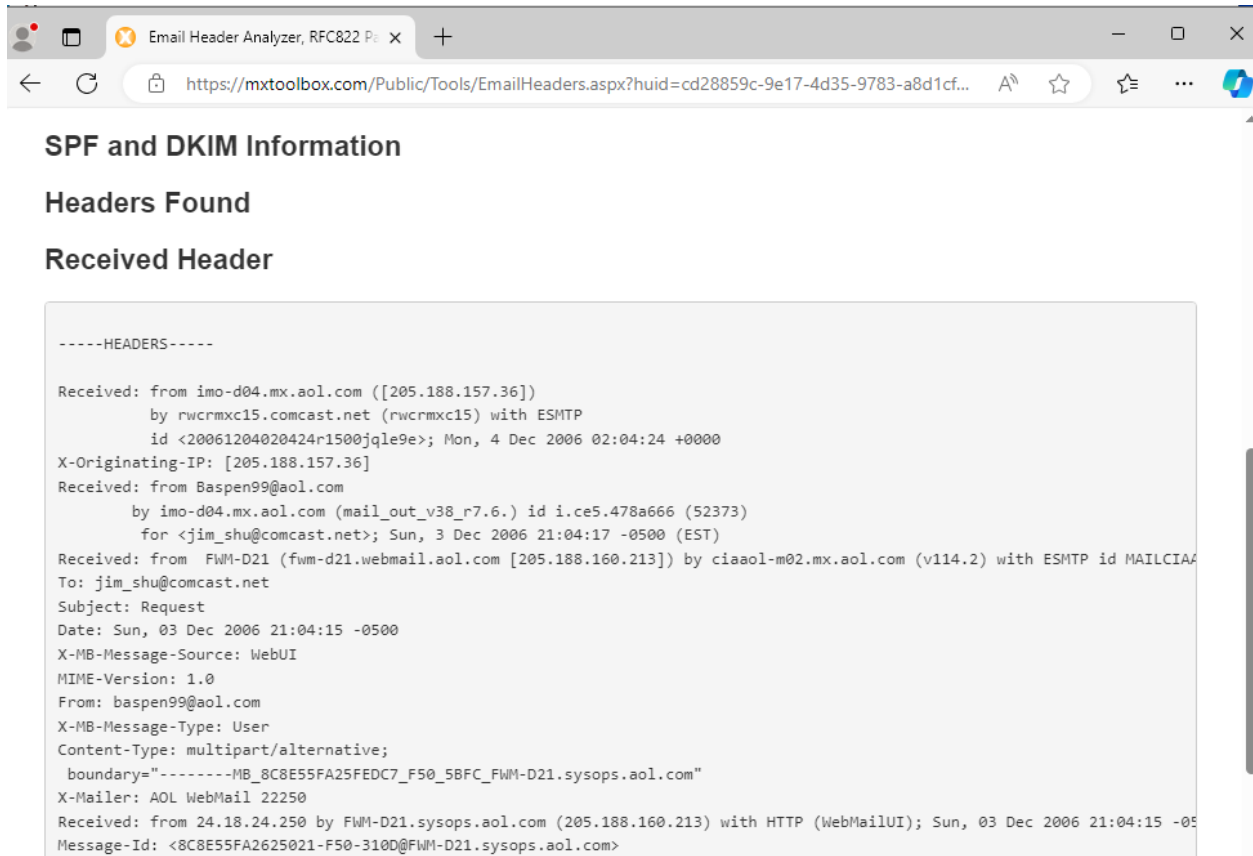
From: baspen99@aol.com <baspen99@aol.com> 2006-12-03 18:04:24 PST
 To: jim_shu@comcast.net
 CC:
 Subject: Request

Headers Text HTML RTF Attachments (0) Accounts

-----HEADERS-----

Received: from imo-d04.mx.aol.com ([205.188.157.36])
 by rwcrmxc15.comcast.net (rwcrmxc15) with ESMTP
 id <20061204020424r1500jql9e>; Mon, 4 Dec 2006 02:04:24 +0000
 X-Originating-IP: [205.188.157.36]
 Received: from Baspen99@aol.com
 by imo-d04.mx.aol.com (mail_out_v38_r7.6.) id i.ce5.478a666 (52373)
 for <jim_shu@comcast.net>; Sun, 3 Dec 2006 21:04:17 -0500 (EST)
 Received: from FWM-D21 (fwm-d21.webmail.aol.com [205.188.160.213]) by ciaaol-m02.mx.aol.com (v114.2) with

With the headers copied, navigate to <https://mxtoolbox.com/EmailHeaders.aspx> and paste in the headers and press “Analyze Header”.



The screenshot shows a web browser window with the title "Email Header Analyzer, RFC822 Po X". The address bar shows the URL <https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=cd28859c-9e17-4d35-9783-a8d1cf...>. The page content includes the following sections:

SPF and DKIM Information

Headers Found

Received Header

```
-----HEADERS-----

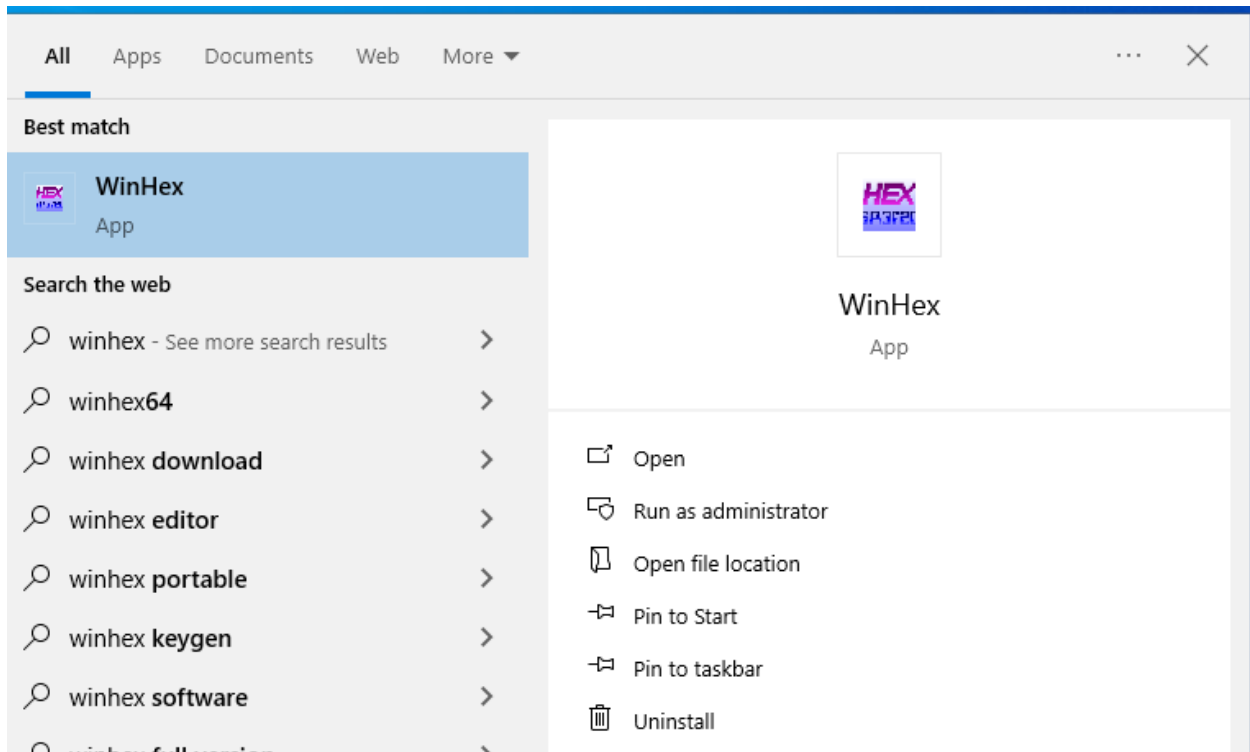
Received: from imo-d04.mx.aol.com ([205.188.157.36])
    by rwcrmxc15.comcast.net (rwcrmxc15) with ESMTP
    id <20061204020424r1500jqle9e>; Mon, 4 Dec 2006 02:04:24 +0000
X-Originating-IP: [205.188.157.36]
Received: from Baspen99@aol.com
    by imo-d04.mx.aol.com (mail_out_v38_r7.6.) id i.ce5.478a666 (52373)
    for <jim_shu@comcast.net>; Sun, 3 Dec 2006 21:04:17 -0500 (EST)
Received: from FWM-D21 (fwm-d21.webmail.aol.com [205.188.160.213]) by c1aaol-m02.mx.aol.com (v114.2) with ESMTP id MAILCIAA
To: jim_shu@comcast.net
Subject: Request
Date: Sun, 03 Dec 2006 21:04:15 -0500
X-MB-Message-Source: WebUI
MIME-Version: 1.0
From: baspen99@aol.com
X-MB-Message-Type: User
Content-Type: multipart/alternative;
    boundary="-----MB_8C8E55FA25FEDC7_F50_5BFC_FWM-D21.sysops.aol.com"
X-Mailer: AOL WebMail 22250
Received: from 24.18.24.250 by FWM-D21.sysops.aol.com (205.188.160.213) with HTTP (WebMailUI); Sun, 03 Dec 2006 21:04:15 -05
Message-Id: <8C8E55FA2625021-F50-310D@FWM-D21.sysops.aol.com>
```

Task 2 – Recover Other Emails

Sometimes you may come across an email format that is not easily parsed by forensic software. Learning how to carve and export emails from an email database can be a useful skill. In this task, I will carve emails from an Evolution tarball file using WinHex

Step 1: Install WinHex

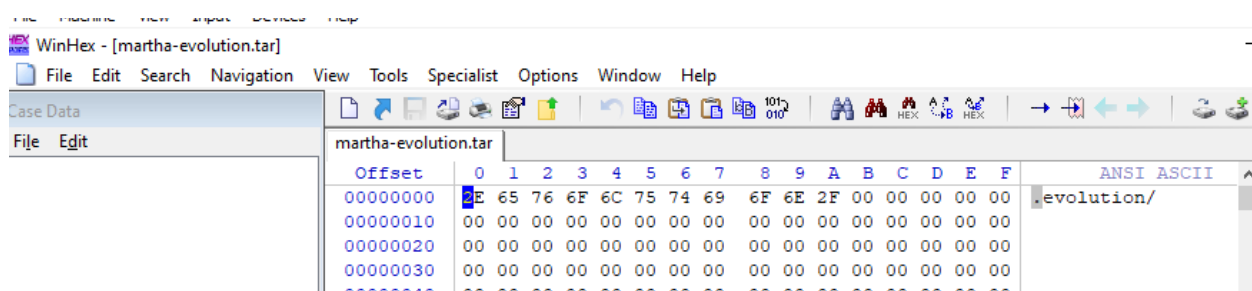
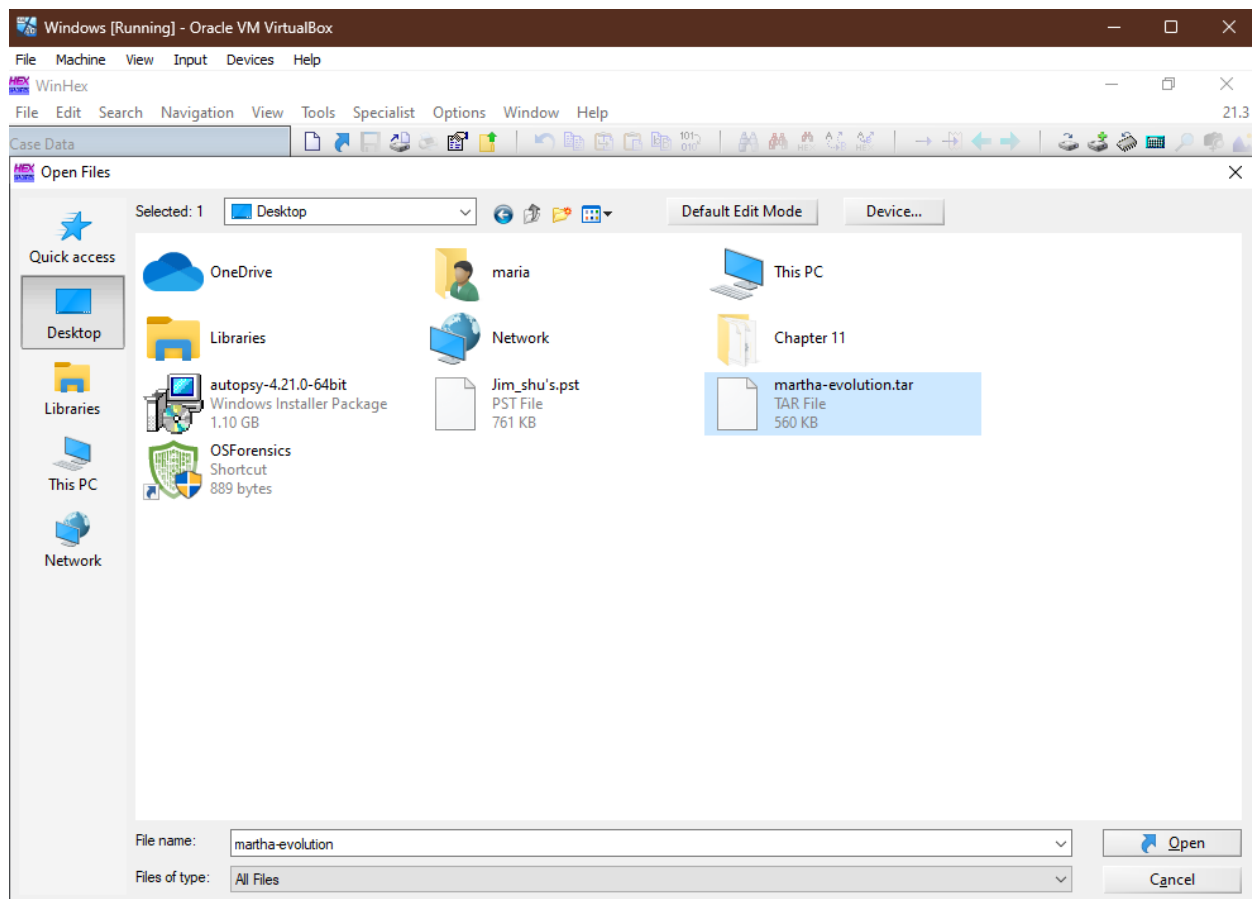
I already have WinHex installed in my Windows VM.



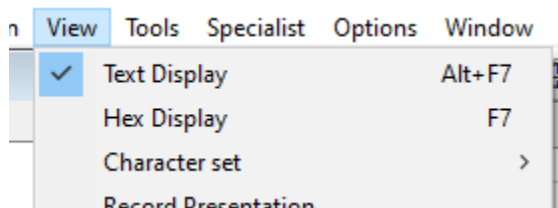
Step 2: Prepare Case

Copy the "martha-evolution.tar" file onto your Windows VM. A tar file is a "tape archive" file used on Unix systems for putting multiple files/folders into a single file. It is similar to a Zip file but without compression.

Launch the WinHex app and open the TAR file by selecting File, Open, and choosing "marth-evolution.tar".

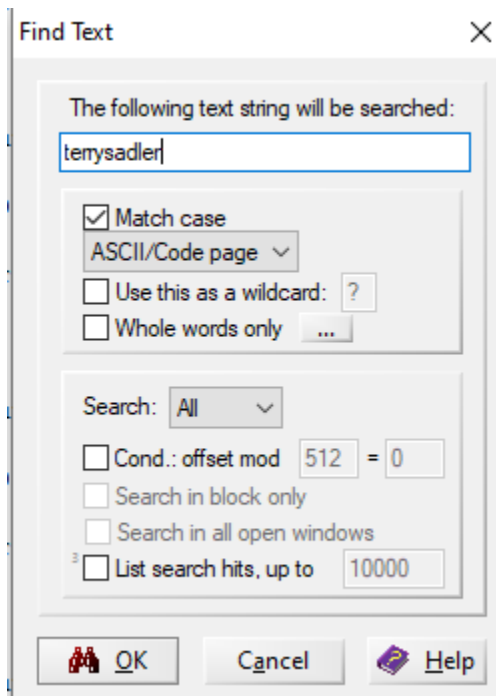


Remove the Hex view by selecting View and unchecking Hex Display.



Step 3: Carve Email from Terry

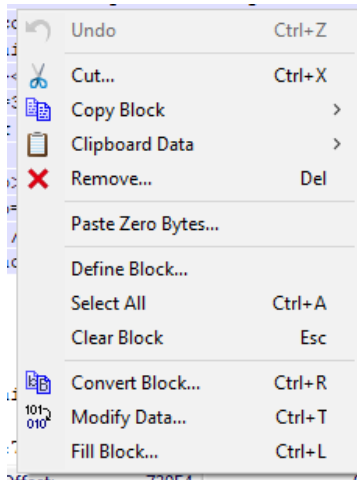
Search for the string "terrysadler" by selecting Search and Find text.



Observe the hit and the preceding word "From" starting at offset 000710EF. Click and hold the F in from (offset 000710EF) then drag down to the bottom of the email highlighting all the text in the email from terrysadler.

```
00071C80 | y><SPAN style=3D= 'color: #000000;font-size: 12px;font-family: V
00071CC0 | erdana;'><p><font face=3D"= Verdana" size=3D"2"></font></p><p><f
00071D00 | ont face=3D"Verdana" size=3D"2">Hell= o, </font></p><p><font fac
00071D40 | e=3D"Verdana" size=3D"2"></font></p><p><font= face=3D"Verdana"
00071D80 | size=3D"2">Are you looking for investors for your comp= any? We
00071DC0 | specialize in small to medium size companies that have a proven=
00071E00 | track record for making quality products and services. Our inv
00071E40 | estor pro= gram will provide to you the necessary consultation t
00071E80 | o achieve success= in the market place along with the needed fi
00071EC0 | nancing to maintain a compe= tive edge against your competitors
00071F00 | . </font></p><p><font face=3D"Verdana= " size=3D"2"></font></p><
00071F40 | p><font face=3D"Verdana" size=3D"2">If you hare= interest check
00071F80 | out our link here to find out more about this unique and= succ
00071FC0 | essful offer. </font></p><p><font face=3D"Verdana" size=3D"2"></
00072000 | fon= t></p><p><font face=3D"Verdana" size=3D"2"><a href=3D"http:
00072040 | //www.superio= rbicycles.biz">www.superiorbicycles.biz</a> </fon
00072080 | t></p><p><br /></p></SP= AN></body></html></body></html> -----
000720C0 | _EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019b--
```

Right-click the highlighted text space, select Edit, Copy Block, and "Into New File".



Save the file as "martha-evolution.txt". Open the saved/carved file in Notepad to view its contents.

```

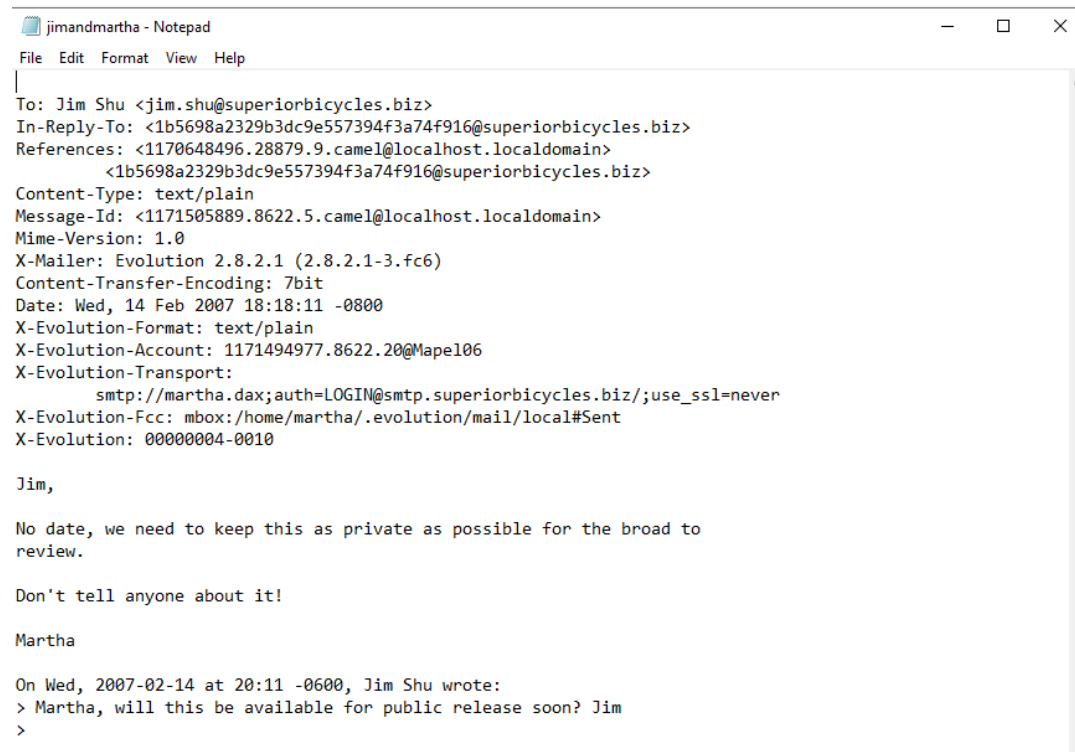
martha-evolution - Notepad
File Edit Format View Help
From terrysadler@goowy.com Sat Feb 17 15:15:45 2007
Received: from smtp-sjt-01.vividround.com ([199.249.224.252]) by
mail.vividround.com with Microsoft SMTPSVC(6.0.3790.1830); Sat, 17 Feb 2007
15:15:45 -0600
Received: from smtp1.goowy.com (smtp1.goowy.com [209.126.247.205]) by
smtp-sjt-01.vividround.com (8.12.11/8.12.11) with ESMTP id 11HLAcgD060105
for <martha.dax@superiorbicycles.biz>; Sat, 17 Feb 2007 15:10:38 -0600 (CST)
Received: (qmail 2864 invoked from network); 17 Feb 2007 21:01:53 -0000
Received: by simscan 1.1.0 ppid: 2857, pid: 2859, t: 0.1710s scanners:
attach: 1.1.0 clamav: 0.88.4/m:38/d:1506 spam: 3.1.2
X-Spam-Checker-Version: SpamAssassin 3.1.2 (2006-05-25) on smtp1.goowy.com
X-Spam-Level:
X-Spam-Status: No, score=0.5 required=4.5 tests=ALL_TRUSTED,BIZ_TLD,
HTML_50_60,HTML_MESSAGE autolearn=disabled version=3.1.2
Received: from unknown (HELO webserver002) ([192.168.25.102])
(envelope-sender <terrysadler@goowy.com>) by smtp1.goowy.com
(qmail-ldap-1.03) with SMTP for <martha.dax@superiorbicycles.biz>; 17 Feb
2007 21:01:53 -0000
goowy: id: : 520051
From: terrysadler <terrysadler@goowy.com>
Reply-To: terrysadler <terrysadler@goowy.com>
To: martha.dax@superiorbicycles.biz
Date: Sat, 17 Feb 2007 21:15:44 GMT
Message-ID: <2af031584b5c460e95b36ddd6719529f@webserver002>
Subject: Investors
MIME-Version: 1.0
X-Mailer: goowy mail - http://www.goowy.com
Priority: Normal
X-Priority: 3
Content-Type: multipart/alternative; boundary="-----_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019b"
X-ePrism-Trap: Default Trap
X-eGuard-Score: () 0.6 BIZ TLD,HTML 50 60,HTML MESSAGE

```

Step 4: Carve Email Involving Jim Shu

Remember Jim Shu from the previous task? We suspect he has had communication with Martha. Search Martha's Evolution file for signs of communication with Jim. Extract an email that includes Jim (To, From, CCed, BCCed, etc) and describe its contents.

```
000271C0 To: Jim Shu <jim.shu@superiorbicycles.biz> In-Reply-To: <1b5698
00027200 a2329b3dc9e557394f3a74f916@superiorbicycles.biz> References: <11
00027240 70648496.28879.9.camel@localhost.localdomain> <1b5698a2329b3dc
00027280 9e557394f3a74f916@superiorbicycles.biz> Content-Type: text/plain
000272C0 Message-Id: <1171505889.8622.5.camel@localhost.localdomain> Mim
00027300 e-Version: 1.0 X-Mailer: Evolution 2.8.2.1 (2.8.2.1-3.fc6) Cont
00027340 ent-Transfer-Encoding: 7bit Date: Wed, 14 Feb 2007 18:18:11 -080
00027380 0 X-Evolution-Format: text/plain X-Evolution-Account: 1171494977
000273C0 .8622.20@Mapel06 X-Evolution-Transport: smtp://martha.dax;auth=
00027400 LOGIN@smtp.superiorbicycles.biz;/use_ssl=never X-Evolution-Fcc:
00027440 mbox:/home/martha/.evolution/mail/local#Sent X-Evolution: 000000
00027480 04-0010 Jim, No date, we need to keep this as private as poss
000274C0 ible for the broad to review. Don't tell anyone about it! Mar
00027500 tha On Wed, 2007-02-14 at 20:11 -0600, Jim Shu wrote: > Martha,
00027540 will this be available for public release soon? Jim > > On Feb
```



```
jimandmartha - Notepad
File Edit Format View Help

To: Jim Shu <jim.shu@superiorbicycles.biz>
In-Reply-To: <1b5698a2329b3dc9e557394f3a74f916@superiorbicycles.biz>
References: <1170648496.28879.9.camel@localhost.localdomain>
<1b5698a2329b3dc9e557394f3a74f916@superiorbicycles.biz>
Content-Type: text/plain
Message-Id: <1171505889.8622.5.camel@localhost.localdomain>
Mime-Version: 1.0
X-Mailer: Evolution 2.8.2.1 (2.8.2.1-3.fc6)
Content-Transfer-Encoding: 7bit
Date: Wed, 14 Feb 2007 18:18:11 -0800
X-Evolution-Format: text/plain
X-Evolution-Account: 1171494977.8622.20@Mapel06
X-Evolution-Transport:
smtp://martha.dax;auth=LOGIN@smtp.superiorbicycles.biz;/use_ssl=never
X-Evolution-Fcc: mbox:/home/martha/.evolution/mail/local#Sent
X-Evolution: 00000004-0010

Jim,

No date, we need to keep this as private as possible for the broad to
review.

Don't tell anyone about it!

Martha

On Wed, 2007-02-14 at 20:11 -0600, Jim Shu wrote:
> Martha, will this be available for public release soon? Jim
>
```

The context of this email is a conversation between Jim and Martha talking about a private release for the bike company and Jim asking if it will be released soon.

I am incorporating this screenshot because it organizes the header for easier understanding.

SPF and DKIM Information

Headers Found

Header Name	Header Value
TO	JIM SHU <JIM.SHU@SUPERIORBICYCLES.BIZ>
IN-REPLY-TO	<1B5698A2329B3DC9E557394F3A74F916@SUPERIORBICYCLES.BIZ>
REFERENCES	<1170648496.28879.9.CAMEL@LOCALHOST.LOCALDOMAIN> <1B5698A2329B3DC9E557394F3A74F916@SUPERIORBICYCLES.BIZ>
CONTENT-TYPE	TEXT/PLAIN
MESSAGE-ID	<1171505889.8622.5.CAMEL@LOCALHOST.LOCALDOMAIN>
MIME-VERSION	1.0
X-MAILER	EVOLUTION 2.8.2.1 (2.8.2.1-3.FC6)
CONTENT-TRANSFER-ENCODING	7BIT
DATE	WED, 14 FEB 2007 18:18:11 -0800
X-EVOLUTION-FORMAT	TEXT/PLAIN
X-EVOLUTION-ACCOUNT	1171494977.8622.20@MAPEL06
X-EVOLUTION-	SMTP://MARTHA.DAX;AUTH=LOGIN@SMTP.SUPERIORBICYCLES.BIZ/;USE_SSL=NEVER