Email Labs

OSForensics

Autopsy

Initial Set Up

On your Windows 10 RADISHng desktop

Copy over the `MS E-mail Files.E01` *data file from:*

`R:\share\Labs\Email Social Media Lab\`

to your private directory. e.g.:

`R:\student\<username>\EmailLab\Email Social Media Lab\`

For the remainder of this lab description, your private directory will be referred to as your *Work Folder*

Email Forensics Using OSForensics

Goal & Background

In this lab, you will be using OSForensics to search for e-mail evidence involving **Ron Torvald**

You will be examining **Ron Torvald**'s Outlook mailbox

OSForensics can't process Outlook's mailbox (.pst) files individually, so you must search an entire image to find e-mail evidence.

Out with the New…

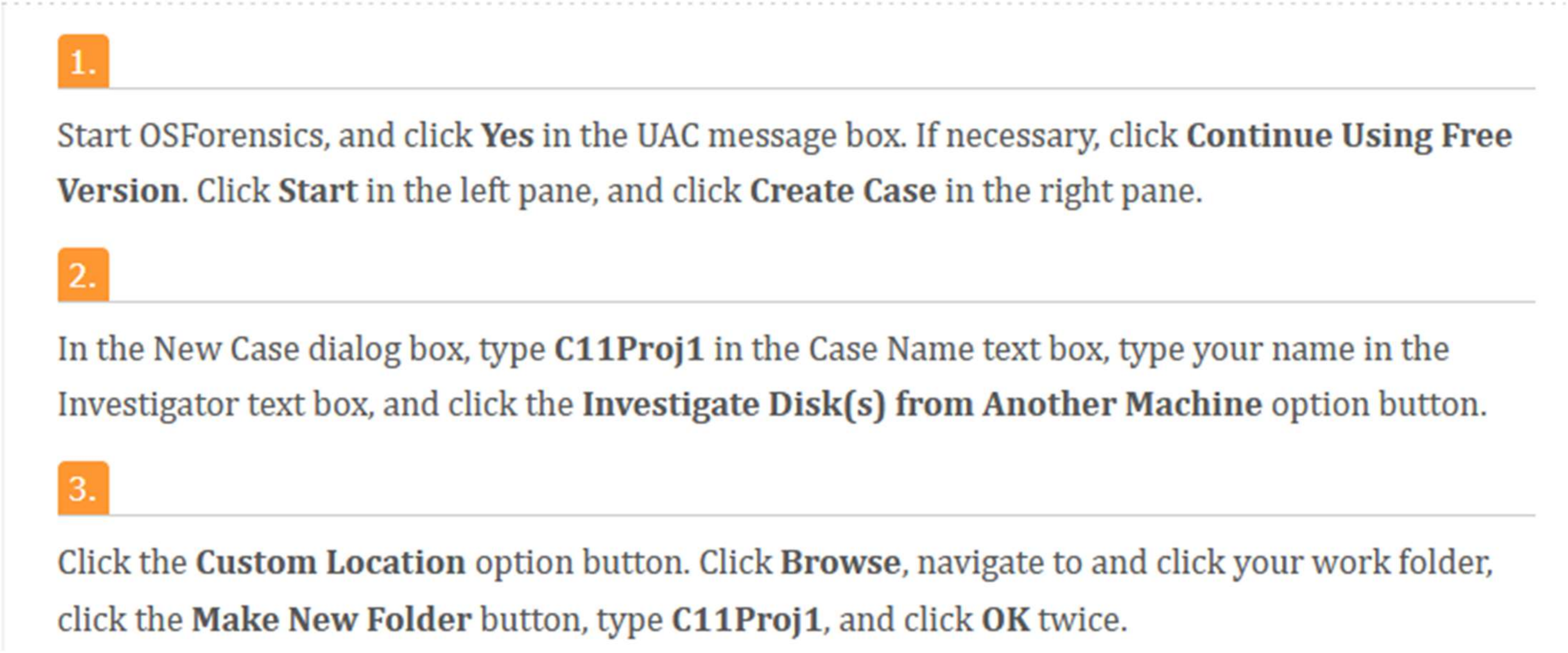
To complete this lab, you'll have to:

- *Install an older (free) version of OSForensics*

To install the older version:

- *Copy the* `R:\tools\OSForensics\osf_older.exe` *image to your* `Documents` *directory*
- *Double-click on it to install*
- *Follow the default prompts*

Create New Case

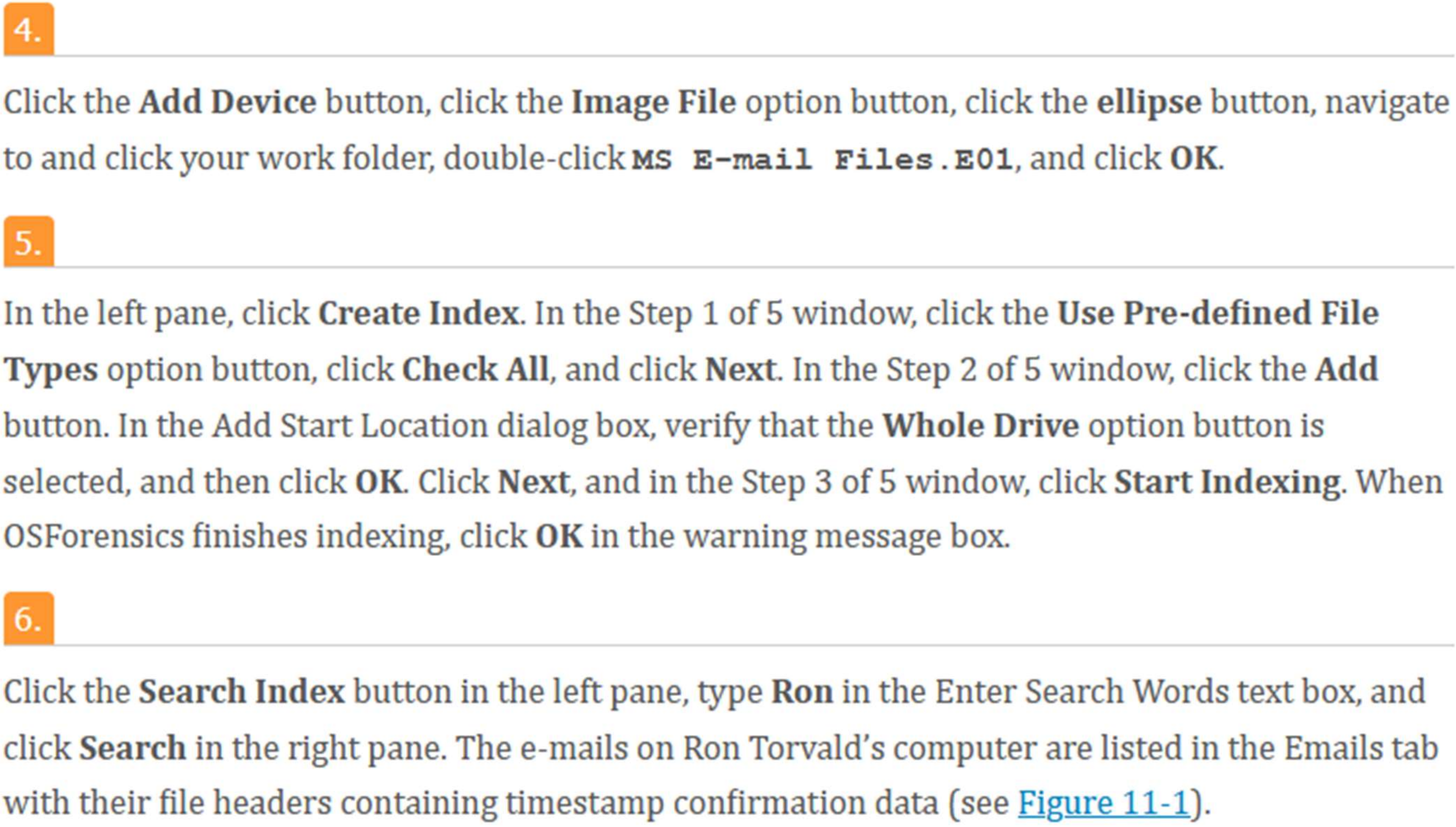


1. Start OSForensics, and click **Yes** in the UAC message box. If necessary, click **Continue Using Free Version**. Click **Start** in the left pane, and click **Create Case** in the right pane.

2. In the New Case dialog box, type **C11Proj1** in the Case Name text box, type your name in the Investigator text box, and click the **Investigate Disk(s) from Another Machine** option button.

3. Click the **Custom Location** option button. Click **Browse**, navigate to and click your work folder, click the **Make New Folder** button, type **C11Proj1**, and click **OK** twice.

Load and Scan Data



4.

Click the **Add Device** button, click the **Image File** option button, click the **ellipse** button, navigate to and click your work folder, double-click `MS E-mail Files.E01`, and click **OK**.

5.

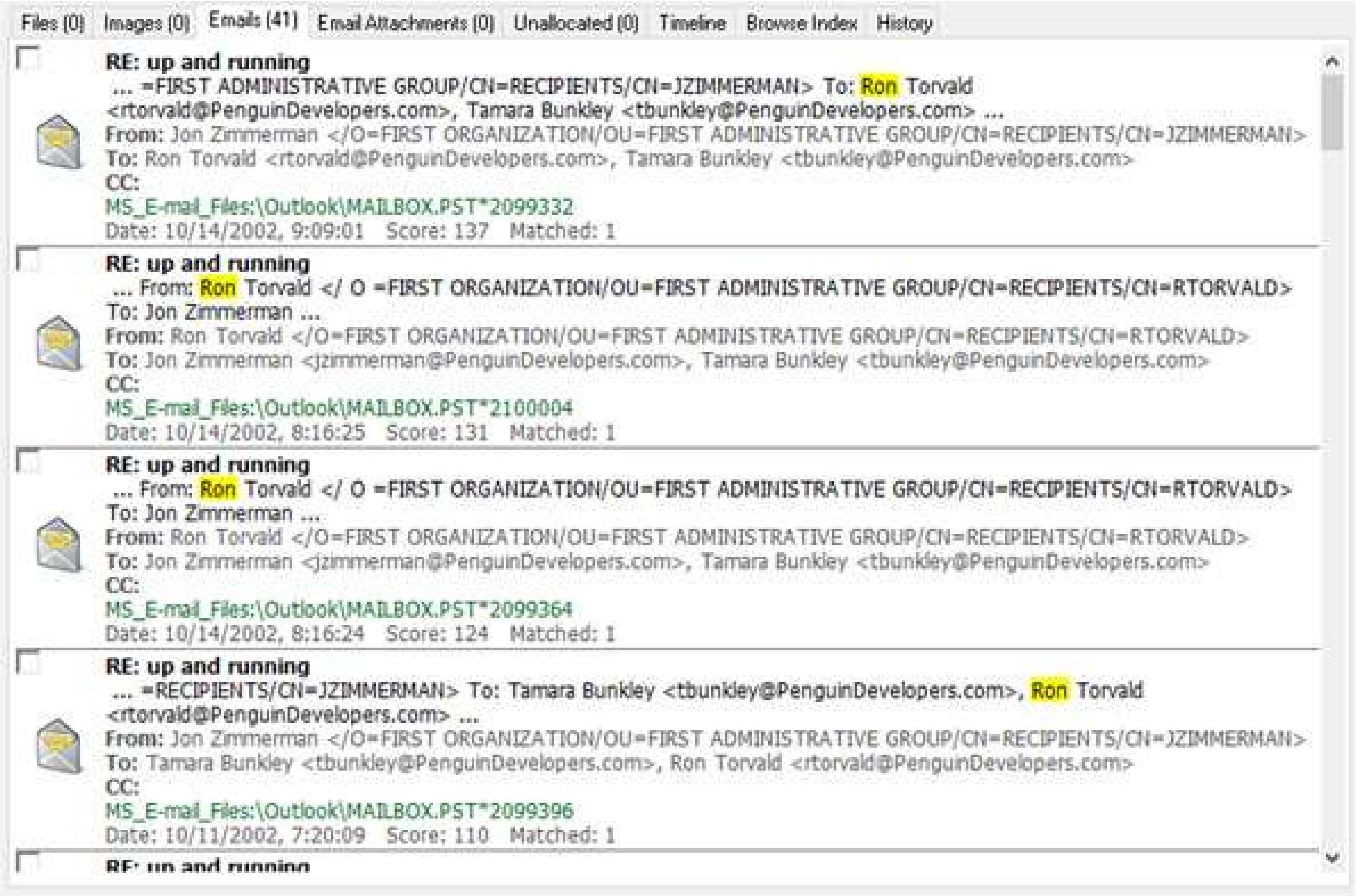
In the left pane, click **Create Index**. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click **Check All**, and click **Next**. In the Step 2 of 5 window, click the **Add** button. In the Add Start Location dialog box, verify that the **Whole Drive** option button is selected, and then click **OK**. Click **Next**, and in the Step 3 of 5 window, click **Start Indexing**. When OSForensics finishes indexing, click **OK** in the warning message box.

6.

Click the **Search Index** button in the left pane, type **Ron** in the Enter Search Words text box, and click **Search** in the right pane. The e-mails on Ron Torvald's computer are listed in the Emails tab with their file headers containing timestamp confirmation data (see Figure 11-1).

Emails Displayed with File Headers

Figure 11-1



RE: up and running
... =FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JZIMMERMAN> To: Ron Torvald <rtorvald@PenguinDevelopers.com>, Tamara Bunkley <tbunkley@PenguinDevelopers.com> ...
From: Jon Zimmerman </O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JZIMMERMAN>
To: Ron Torvald <rtorvald@PenguinDevelopers.com>, Tamara Bunkley <tbunkley@PenguinDevelopers.com>
CC:
MS_E-mail_Files:\Outlook\MAILBOX.PST*2099332
Date: 10/14/2002, 9:09:01 Score: 137 Matched: 1

RE: up and running
... From: Ron Torvald </ O =FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=RTORVALD>
To: Jon Zimmerman ...
From: Ron Torvald </O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=RTORVALD>
To: Jon Zimmerman <jzimmerman@PenguinDevelopers.com>, Tamara Bunkley <tbunkley@PenguinDevelopers.com>
CC:
MS_E-mail_Files:\Outlook\MAILBOX.PST*2100004
Date: 10/14/2002, 8:16:25 Score: 131 Matched: 1

RE: up and running
... From: Ron Torvald </ O =FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=RTORVALD>
To: Jon Zimmerman ...
From: Ron Torvald </O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=RTORVALD>
To: Jon Zimmerman <jzimmerman@PenguinDevelopers.com>, Tamara Bunkley <tbunkley@PenguinDevelopers.com>
CC:
MS_E-mail_Files:\Outlook\MAILBOX.PST*2099364
Date: 10/14/2002, 8:16:24 Score: 124 Matched: 1

RE: up and running
... =RECIPIENTS/CN=JZIMMERMAN> To: Tamara Bunkley <tbunkley@PenguinDevelopers.com>, Ron Torvald <rtorvald@PenguinDevelopers.com> ...
From: Jon Zimmerman </O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JZIMMERMAN>
To: Tamara Bunkley <tbunkley@PenguinDevelopers.com>, Ron Torvald <rtorvald@PenguinDevelopers.com>
CC:
MS_E-mail_Files:\Outlook\MAILBOX.PST*2099396
Date: 10/11/2002, 7:20:09 Score: 110 Matched: 1

RE: up and running

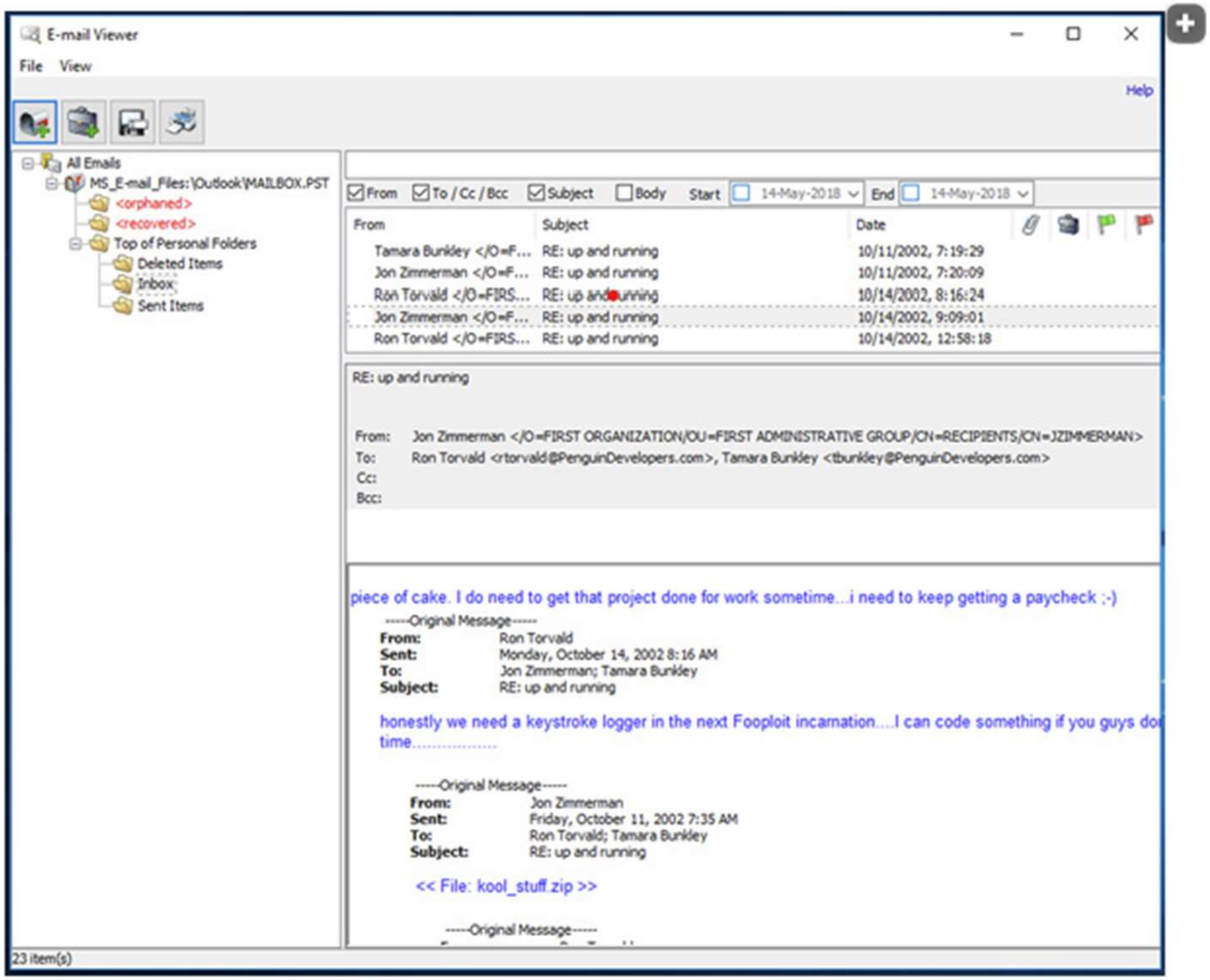
Open E-mail Viewer

7.

Right-click the first e-mail and click **Open** to open the OSForensics E-mail Viewer (see Figure 11-2).

Figure 11-2

Opening an e-mail in the built-in viewer



From	Subject	Date
Tamara Bunkley </O=F...	RE: up and running	10/11/2002, 7:19:29
Jon Zimmerman </O=F...	RE: up and running	10/11/2002, 7:20:09
Ron Torvald </O=FIRS...	RE: up and running	10/14/2002, 8:16:24
Jon Zimmerman </O=F...	RE: up and running	10/14/2002, 9:09:01
Ron Torvald </O=FIRS...	RE: up and running	10/14/2002, 12:58:18

RE: up and running

From: Jon Zimmerman </O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JZIMMERMAN>
To: Ron Torvald <rtorvald@PenguinDevelopers.com>, Tamara Bunkley <tbunkley@PenguinDevelopers.com>
Cc:
Bcc:

piece of cake. I do need to get that project done for work sometime...i need to keep getting a paycheck ;-)

-----Original Message-----
From: Ron Torvald
Sent: Monday, October 14, 2002 8:16 AM
To: Jon Zimmerman; Tamara Bunkley
Subject: RE: up and running

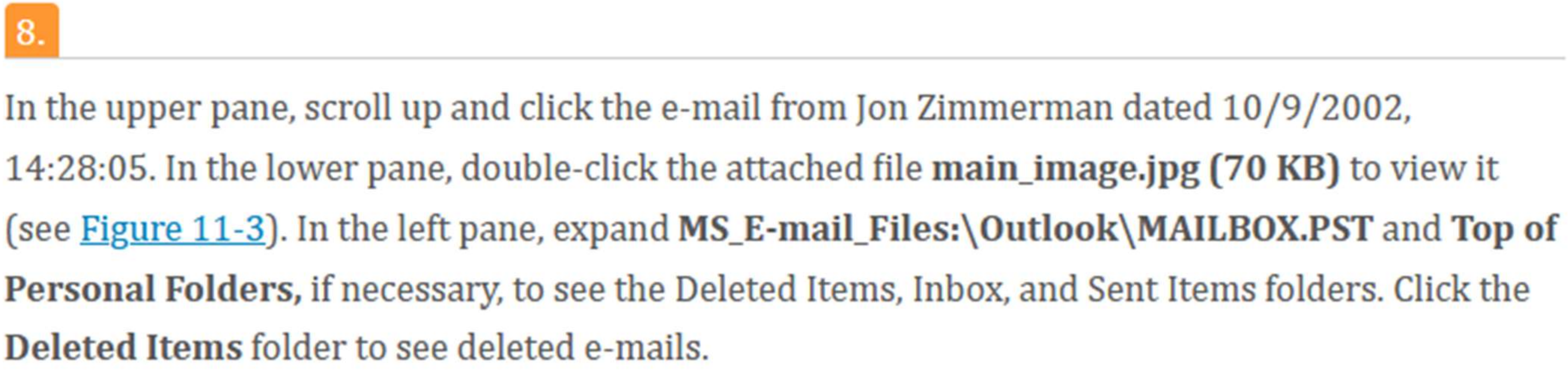
honestly we need a keystroke logger in the next Fooploit incarnation....I can code something if you guys do
time..................

-----Original Message-----
From: Jon Zimmerman
Sent: Friday, October 11, 2002 7:35 AM
To: Ron Torvald; Tamara Bunkley
Subject: RE: up and running

<< File: kool_stuff.zip >>

-----Original Message-----

Examine Email with Attachments & Deleted Emails

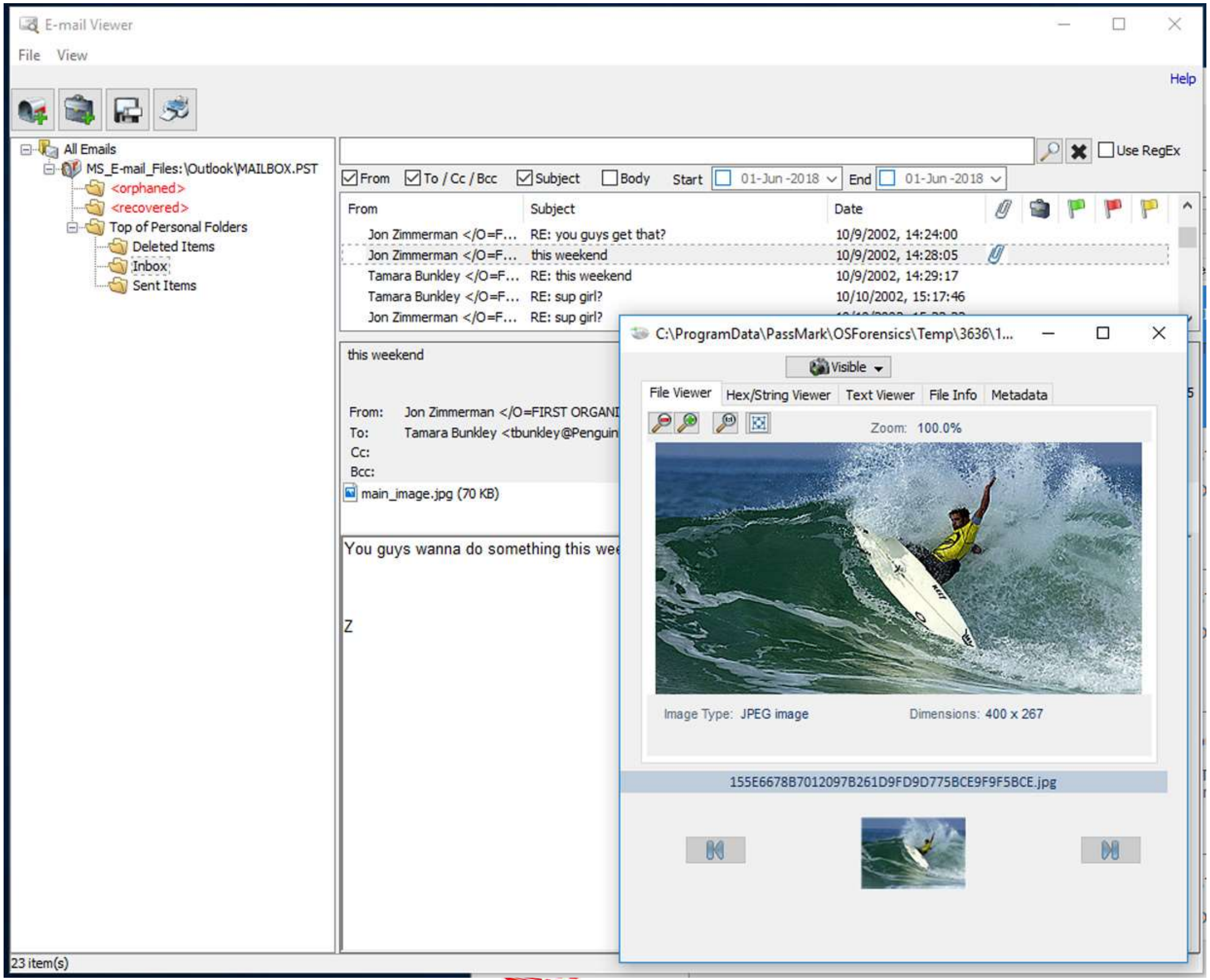


8.

In the upper pane, scroll up and click the e-mail from Jon Zimmerman dated 10/9/2002, 14:28:05. In the lower pane, double-click the attached file **main_image.jpg (70 KB)** to view it (see Figure 11-3). In the left pane, expand **MS_E-mail_Files:\Outlook\MAILBOX.PST** and **Top of Personal Folders,** if necessary, to see the Deleted Items, Inbox, and Sent Items folders. Click the **Deleted Items** folder to see deleted e-mails.

Emails with Attachment

Figure 11-3



All Emails
MS_E-mail_Files:\Outlook\MAILBOX.PST
<orphaned>
<recovered>
Top of Personal Folders
Deleted Items
Inbox
Sent Items

☐ Use RegEx

☑ From ☑ To / Cc / Bcc ☑ Subject ☐ Body Start ☐ 01-Jun-2018 End ☐ 01-Jun-2018

From	Subject	Date
Jon Zimmerman </O=F...	RE: you guys get that?	10/9/2002, 14:24:00
Jon Zimmerman </O=F...	this weekend	10/9/2002, 14:28:05
Tamara Bunkley </O=F...	RE: this weekend	10/9/2002, 14:29:17
Tamara Bunkley </O=F...	RE: sup girl?	10/10/2002, 15:17:46
Jon Zimmerman </O=F...	RE: sup girl?	

this weekend

From: Jon Zimmerman </O=FIRST ORGANI
To: Tamara Bunkley <tbunkley@Penguin
Cc:
Bcc:

main_image.jpg (70 KB)

You guys wanna do something this wee

Z

C:\ProgramData\PassMark\OSForensics\Temp\3636\1...

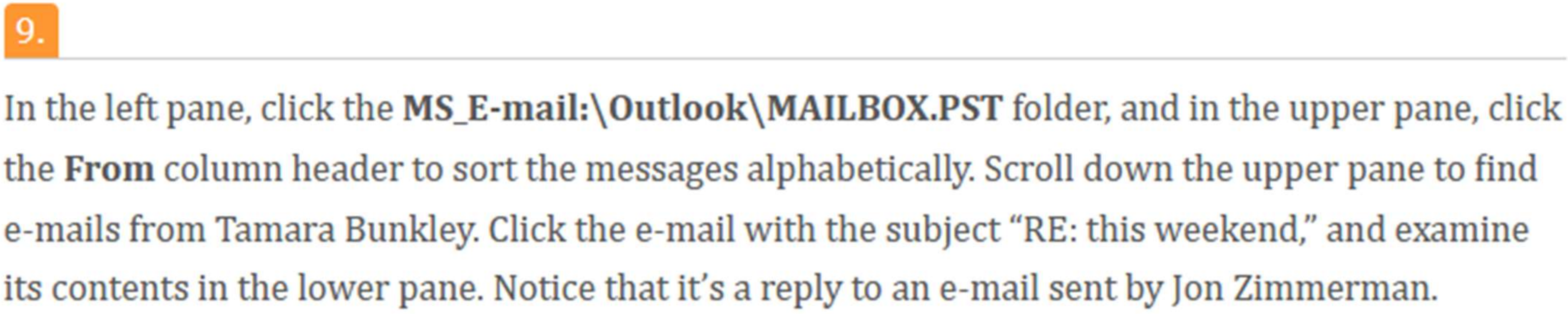
Zoom: 100.0%

Image Type: JPEG image
Dimensions: 400 x 267

155E6678B7012097B261D9FD9D775BCE9F9F5BCE.jpg

23 item(s)

Investigate



9.

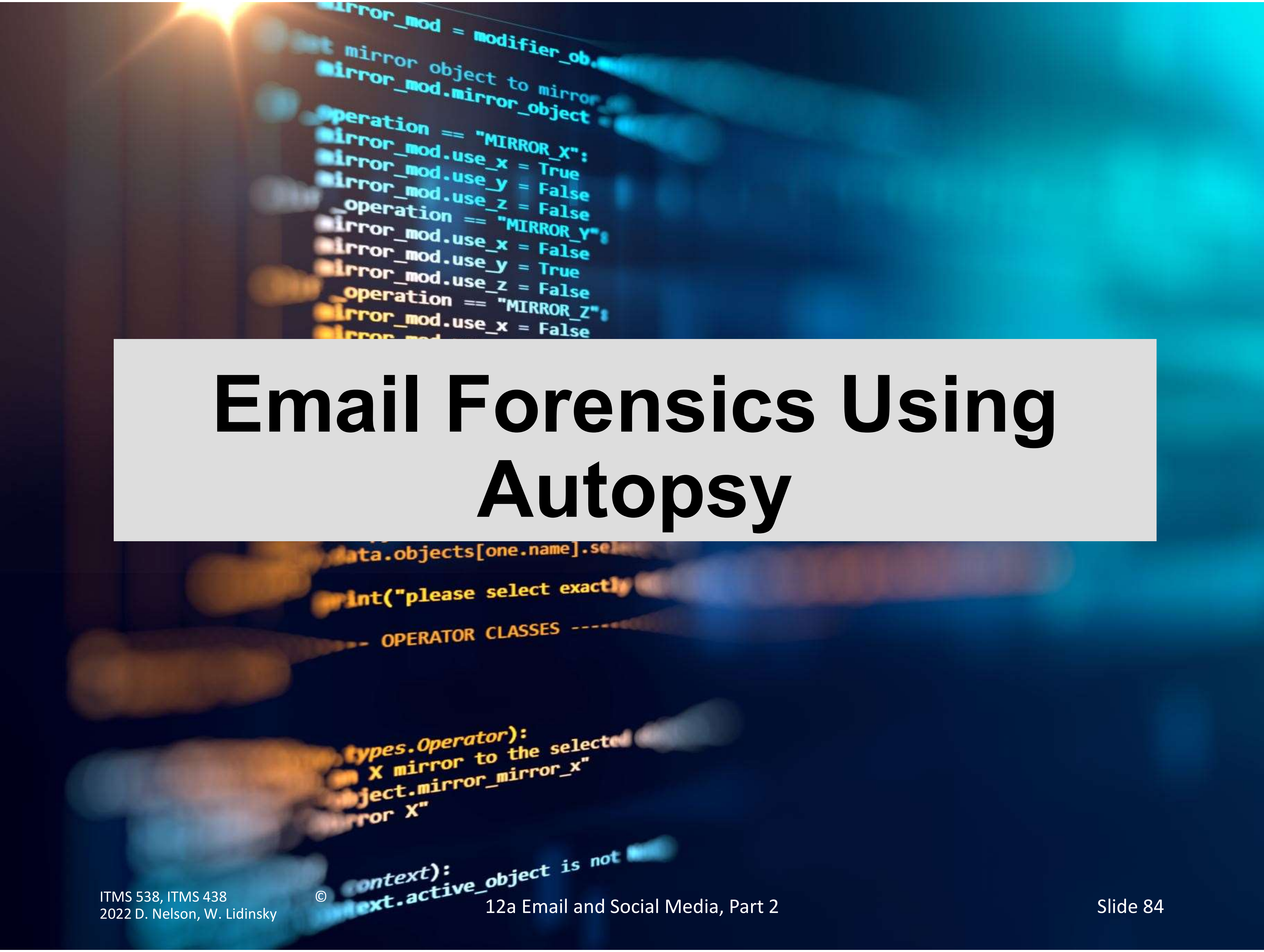
In the left pane, click the **MS_E-mail:\Outlook\MAILBOX.PST** folder, and in the upper pane, click the **From** column header to sort the messages alphabetically. Scroll down the upper pane to find e-mails from Tamara Bunkley. Click the e-mail with the subject "RE: this weekend," and examine its contents in the lower pane. Notice that it's a reply to an e-mail sent by Jon Zimmerman.

Follow-up Questions

Email Forensics using OSForensics Lab

Continue the ***Email Forensics using OSForensics Lab*** and answer the following questions

1. *How many e-mails were deleted from Ron Torvald's Outlook mailbox?*
2. *How many e-mails with attached files did Ron Torvald get from Tamara Bunkley?*
3. *Deleted e-mails with attachments can't be viewed.* ***True*** *or* ***False****?*
4. *How many e-mails did you find by using "Ron" as a search keyword?*
5. *How many zipped files are attached to e-mails?*



Email Forensics Using Autopsy

Goal & Background

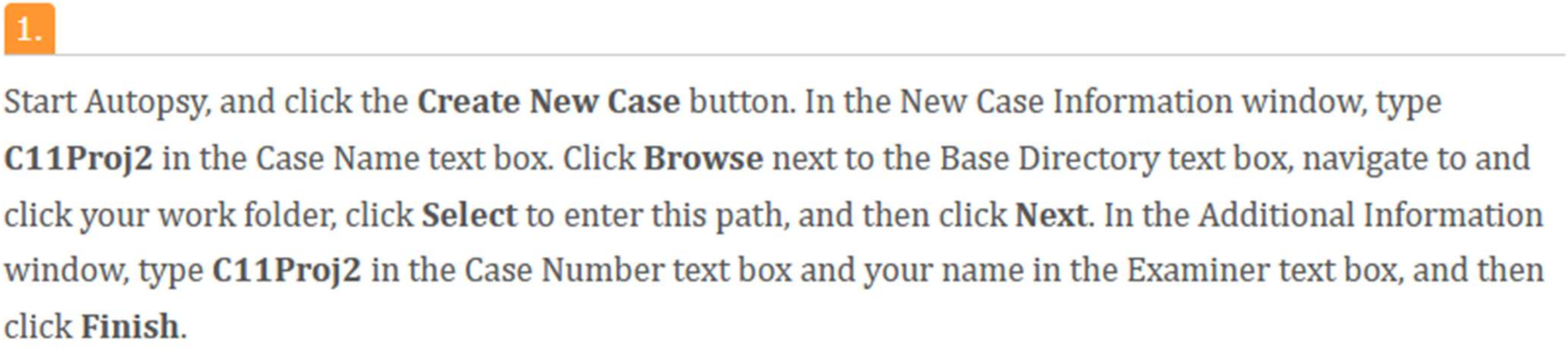
In this lab, you will be using Autopsy to search for e-mail evidence involving **Ron Torvald**

You will be examining **Ron Torvald**'s Outlook mailbox

Autopsy is like OSForensics in that it can't process Outlook mailbox (.pst) files individually, so you have to search an entire image to find e-mail evidence

We'll try to find additional e-mails that might not have been discovered with OSForensics.

Create New Case



1. Start Autopsy, and click the **Create New Case** button. In the New Case Information window, type **C11Proj2** in the Case Name text box. Click **Browse** next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Additional Information window, type **C11Proj2** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

2.

In the Add Data Source Window, click Disk Image or VM File, if necessary, then click Next. In the Select Data Source window, click Browse, navigate to your work folder, select the `MS E-mail Files.E01` file, click Open, then click Next. In the Configure Ingest Modules window, click Select All, and then click Next and Finish to start analyzing the evidence.

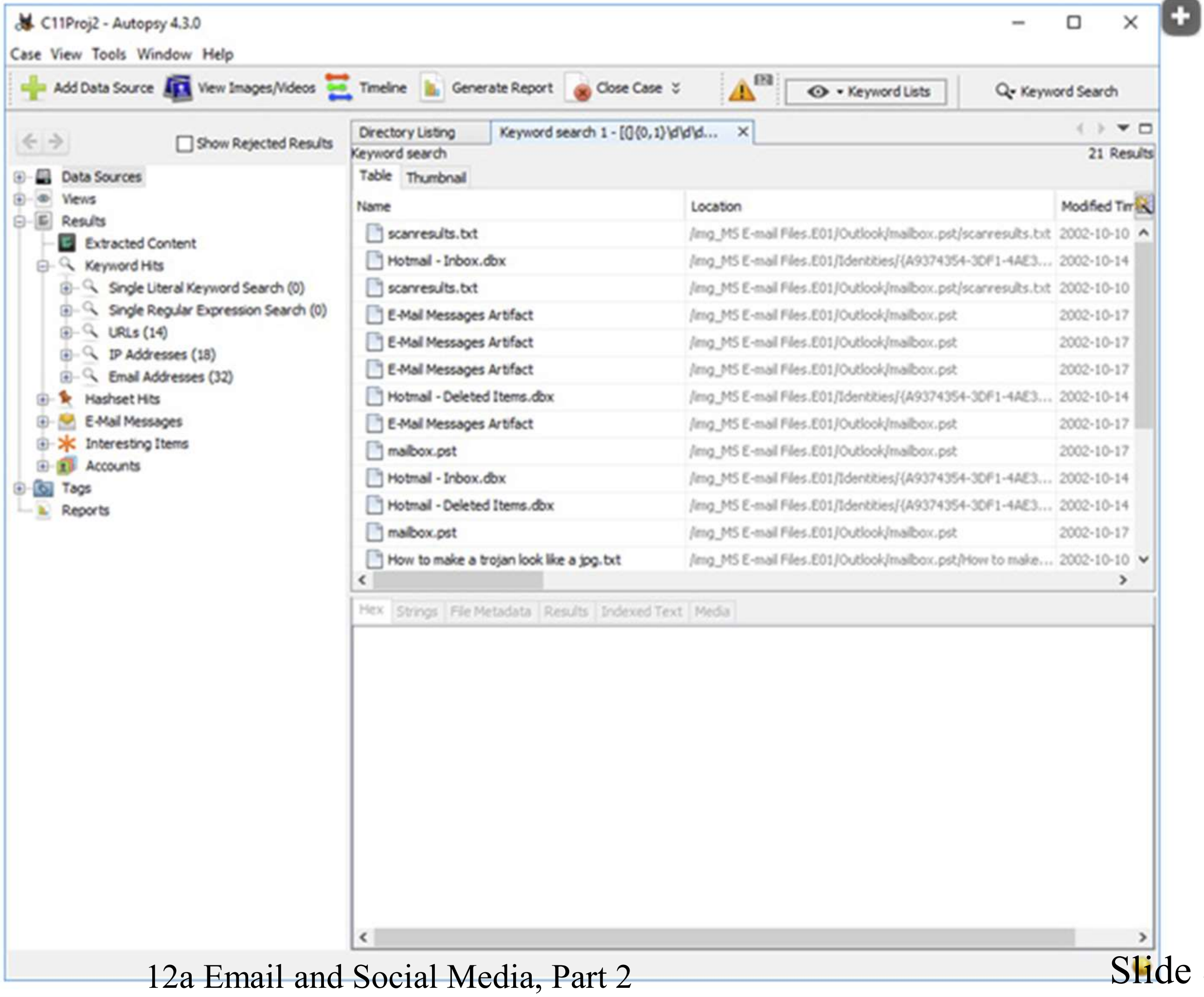
Start Analysis

3.

Click the **Keyword Lists** down arrow, click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click the **Search** button to begin searching for mailboxes and files that match the phone number, IP address, e-mail address, or URL patterns. Figure 11-4 shows the results.

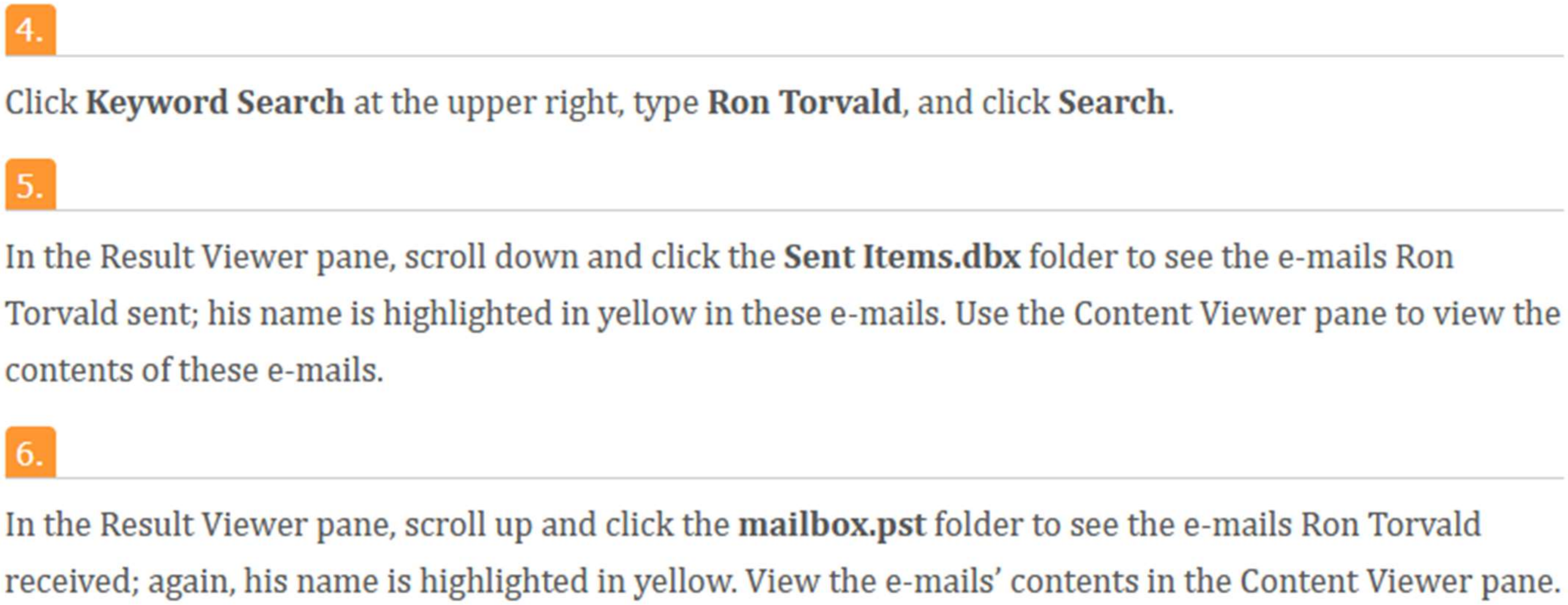
Figure 11-4

Viewing mailboxes found in an image



Name	Location	Modified Tim
scanresults.txt	/img_MS E-mail Files.E01/Outlook/mailbox.pst/scanresults.txt	2002-10-10
Hotmail - Inbox.dbx	/img_MS E-mail Files.E01/Identities/{A9374354-3DF1-4AE3...	2002-10-14
scanresults.txt	/img_MS E-mail Files.E01/Outlook/mailbox.pst/scanresults.txt	2002-10-10
E-Mail Messages Artifact	/img_MS E-mail Files.E01/Outlook/mailbox.pst	2002-10-17
E-Mail Messages Artifact	/img_MS E-mail Files.E01/Outlook/mailbox.pst	2002-10-17
E-Mail Messages Artifact	/img_MS E-mail Files.E01/Outlook/mailbox.pst	2002-10-17
Hotmail - Deleted Items.dbx	/img_MS E-mail Files.E01/Identities/{A9374354-3DF1-4AE3...	2002-10-14
E-Mail Messages Artifact	/img_MS E-mail Files.E01/Outlook/mailbox.pst	2002-10-17
mailbox.pst	/img_MS E-mail Files.E01/Outlook/mailbox.pst	2002-10-17
Hotmail - Inbox.dbx	/img_MS E-mail Files.E01/Identities/{A9374354-3DF1-4AE3...	2002-10-14
Hotmail - Deleted Items.dbx	/img_MS E-mail Files.E01/Identities/{A9374354-3DF1-4AE3...	2002-10-14
mailbox.pst	/img_MS E-mail Files.E01/Outlook/mailbox.pst	2002-10-17
How to make a trojan look like a jpg.txt	/img_MS E-mail Files.E01/Outlook/mailbox.pst/How to make...	2002-10-10

Sent and Received Emails



4.

Click **Keyword Search** at the upper right, type **Ron Torvald**, and click **Search**.

5.

In the Result Viewer pane, scroll down and click the **Sent Items.dbx** folder to see the e-mails Ron Torvald sent; his name is highlighted in yellow in these e-mails. Use the Content Viewer pane to view the contents of these e-mails.

6.

In the Result Viewer pane, scroll up and click the **mailbox.pst** folder to see the e-mails Ron Torvald received; again, his name is highlighted in yellow. View the e-mails' contents in the Content Viewer pane.

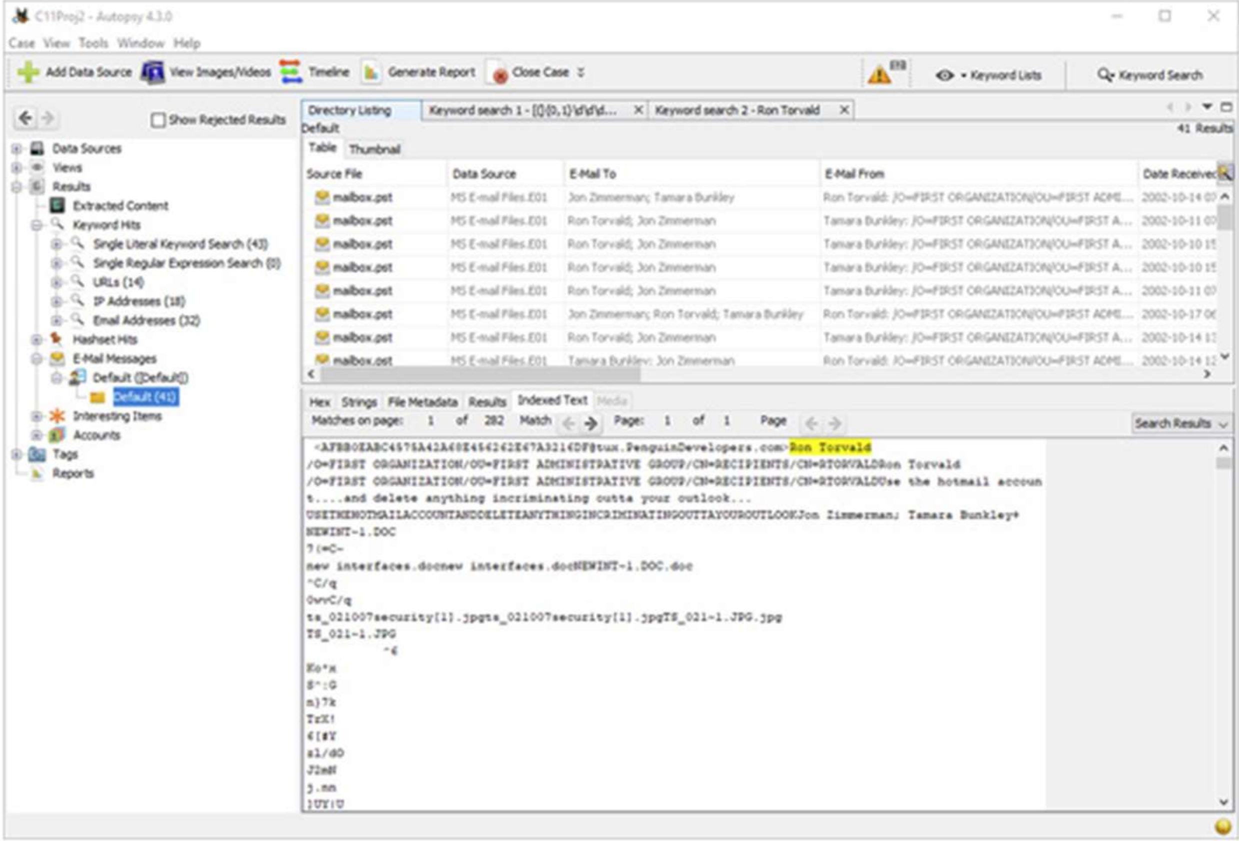
Other Email Views

7.

In the left pane, expand **E-Mail Messages** and **Default ([Default])**, and click the **Default** folder to see e-mails listed in the E-Mail To and E-Mail From columns, as shown in Figure 11-5.

Figure 11-5

Viewing all e-mails

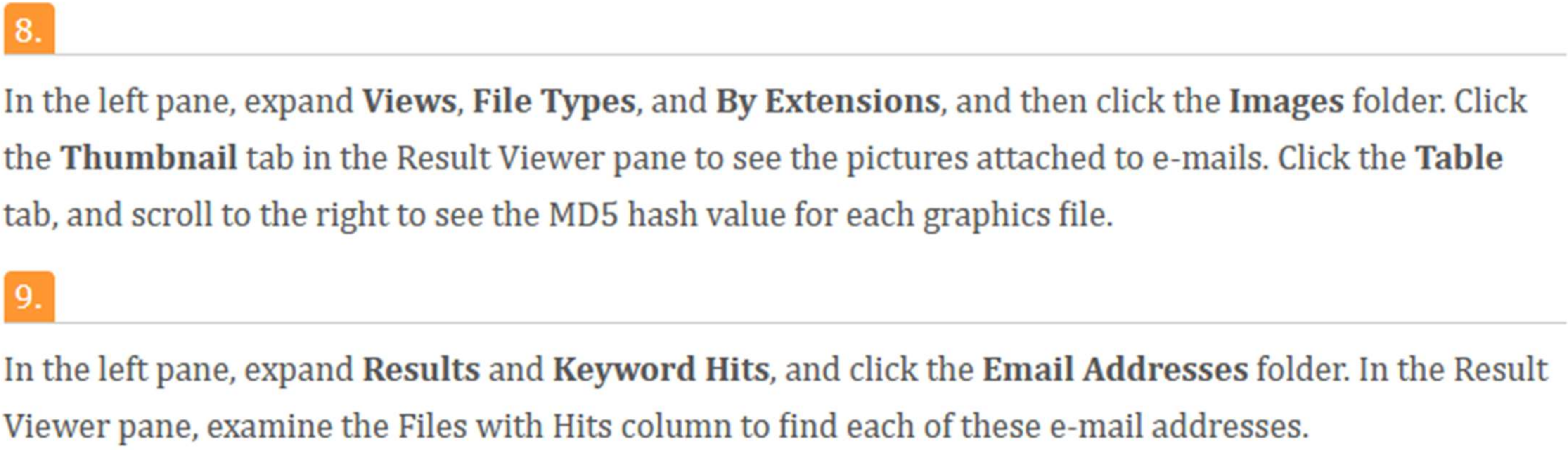


Source File	Data Source	E-Mail To	E-Mail From	Date Received
mailbox.pst	MS E-mail Files.E01	Jon Zimmerman; Tamara Bunkley	Ron Torvald: /O=FIRST ORGANIZATION/OU=FIRST ADMI...	2002-10-14 07
mailbox.pst	MS E-mail Files.E01	Ron Torvald; Jon Zimmerman	Tamara Bunkley: /O=FIRST ORGANIZATION/OU=FIRST A...	2002-10-11 07
mailbox.pst	MS E-mail Files.E01	Ron Torvald; Jon Zimmerman	Tamara Bunkley: /O=FIRST ORGANIZATION/OU=FIRST A...	2002-10-10 15
mailbox.pst	MS E-mail Files.E01	Ron Torvald; Jon Zimmerman	Tamara Bunkley: /O=FIRST ORGANIZATION/OU=FIRST A...	2002-10-10 15
mailbox.pst	MS E-mail Files.E01	Ron Torvald; Jon Zimmerman	Tamara Bunkley: /O=FIRST ORGANIZATION/OU=FIRST A...	2002-10-11 07
mailbox.pst	MS E-mail Files.E01	Jon Zimmerman; Ron Torvald; Tamara Bunkley	Ron Torvald: /O=FIRST ORGANIZATION/OU=FIRST ADMI...	2002-10-17 06
mailbox.pst	MS E-mail Files.E01	Ron Torvald; Jon Zimmerman	Tamara Bunkley: /O=FIRST ORGANIZATION/OU=FIRST A...	2002-10-14 13
mailbox.pst	MS E-mail Files.E01	Tamara Bunkley; Jon Zimmerman	Ron Torvald: /O=FIRST ORGANIZATION/OU=FIRST ADMI...	2002-10-14 12

```
 <AFBB0EABC4575A42A60E456262E67A3214DF@tux.PenguinDevelopers.com>Ron Torvald
/O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=RTORVALDRon Torvald
/O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=RTORVALDUse the hotmail accoun
t.....and delete anything incriminating outta your outlook...
USETHEHOTMAILACCOUNTANDDELETEANYTHINGINCRIMINATINGOUTTAYOUROUTLOOKJon Zimmerman; Tamara Bunkley+
NEWINT-1.DOC
7(=C-
new interfaces.docnew interfaces.docNEWINT-1.DOC.doc
^C/q
OwvC/q
ts_021007security[1].jpgts_021007security[1].jpgTS_021-1.JPG.jpg
TS_021-1.JPG
           ^6
Ko*m
$^:G
n)7k
TrX!
€[#Y
sl/dO
J2m¥
3.nn
}UY!U
```

Source: www.sleuthkit.org

Sent and Received Emails



8.

In the left pane, expand **Views**, **File Types**, and **By Extensions**, and then click the **Images** folder. Click the **Thumbnail** tab in the Result Viewer pane to see the pictures attached to e-mails. Click the **Table** tab, and scroll to the right to see the MD5 hash value for each graphics file.

9.

In the left pane, expand **Results** and **Keyword Hits**, and click the **Email Addresses** folder. In the Result Viewer pane, examine the Files with Hits column to find each of these e-mail addresses.

Follow-up Questions
Email Forensics using Autopsy Lab

Continue the ***Email Forensics using Autopsy Lab*** and answer the following questions

1. *How many graphics files did Autopsy recover?*
2. *How many Hotmail e-mail addresses did you find?*
3. *How many video files are attached to e-mails in the* `MS E-mail Files.E01` *image?*
   a. 16
   b. 0
   c. 2
   d. 3
4. *In the archive folder (under the File Type, by Extension path), how many archive files did Autopsy recover?*
   a. 0
   b. 1
   c. 2
   d. 5
5. *Autopsy recovered the same number of e-mails as OSForensics did.* ***True*** *or* ***False****?*

Finding Google Searches and Multiple Email Accounts

Initial Set Up

On your Windows 10 RADISHng desktop

Copy over the **`precious.001`** *data file from:*

`R:\share\Labs\Email OSN Lab\`

to your private directory. e.g.:

`R:\student\<username>\EmailLab\Email OSN Lab\`

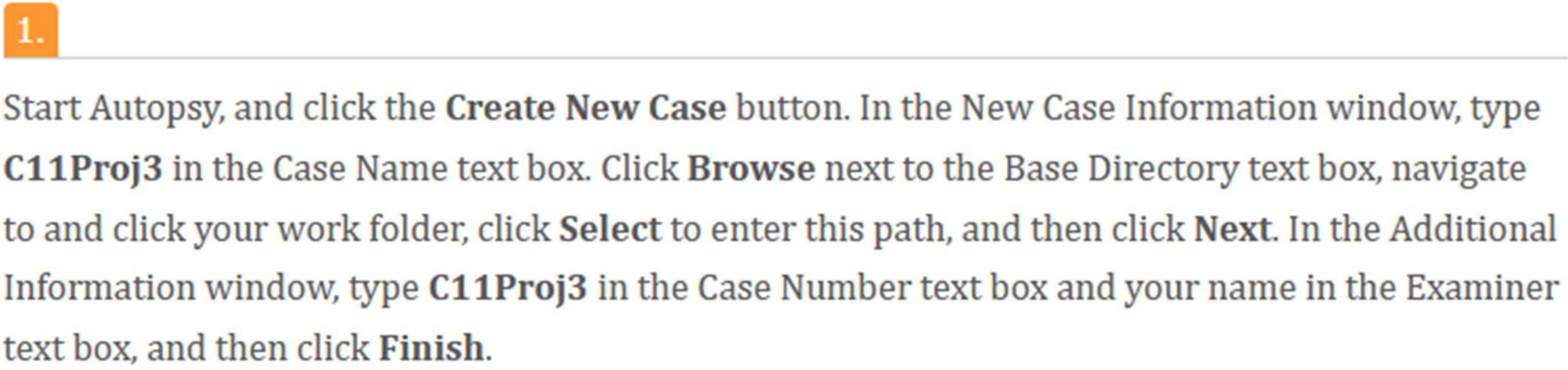
For the remainder of this lab description, your private directory will be referred to as your *Work Folder*

Goal & Background

Frodo Baggins, a suspect in a digital crime, used his forensics skills to discover account passwords by using information he found in the Windows Registry.

In this lab, you will be using Autopsy to find e-mail and Google search evidence showing that **Frodo Baggins** hacked a Windows computer's Registry to discover user account passwords.

Create New Case



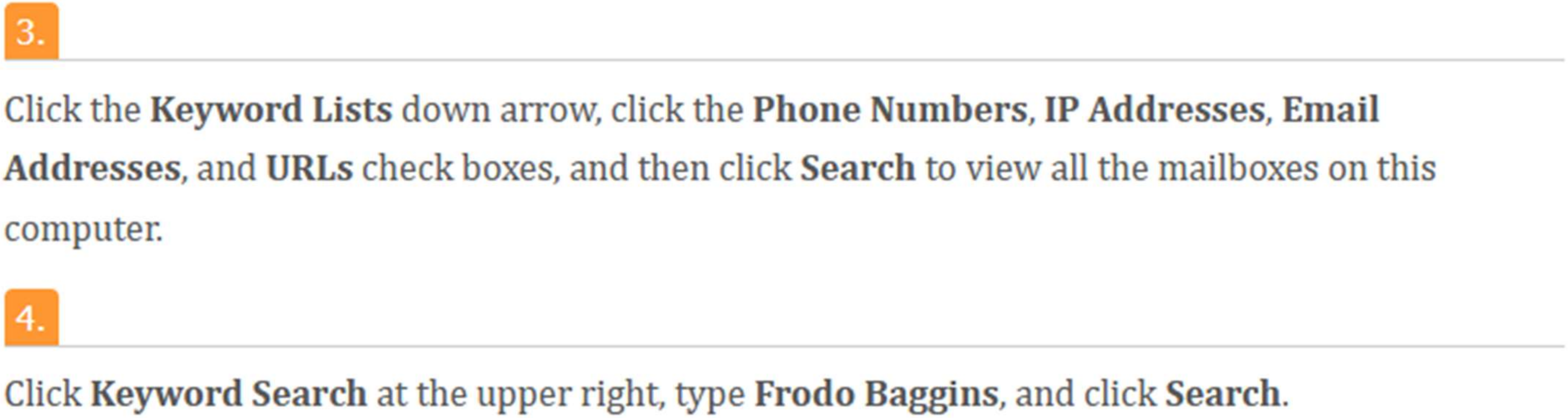
1.

Start Autopsy, and click the **Create New Case** button. In the New Case Information window, type **C11Proj3** in the Case Name text box. Click **Browse** next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Additional Information window, type **C11Proj3** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

2.

In the Add Data Source Window, click Disk Image or VM File, if necessary, then click Next. In the Select Data Source window, click Browse, navigate to your work folder, select the `precious.001` file, click Open, then click Next. In the Configure Ingest Modules window, select all but the Plaso ingest module, click Next and Finish to start analyzing the evidence.

Start Analysis



3.

Click the **Keyword Lists** down arrow, click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click **Search** to view all the mailboxes on this computer.

4.

Click **Keyword Search** at the upper right, type **Frodo Baggins**, and click **Search**.

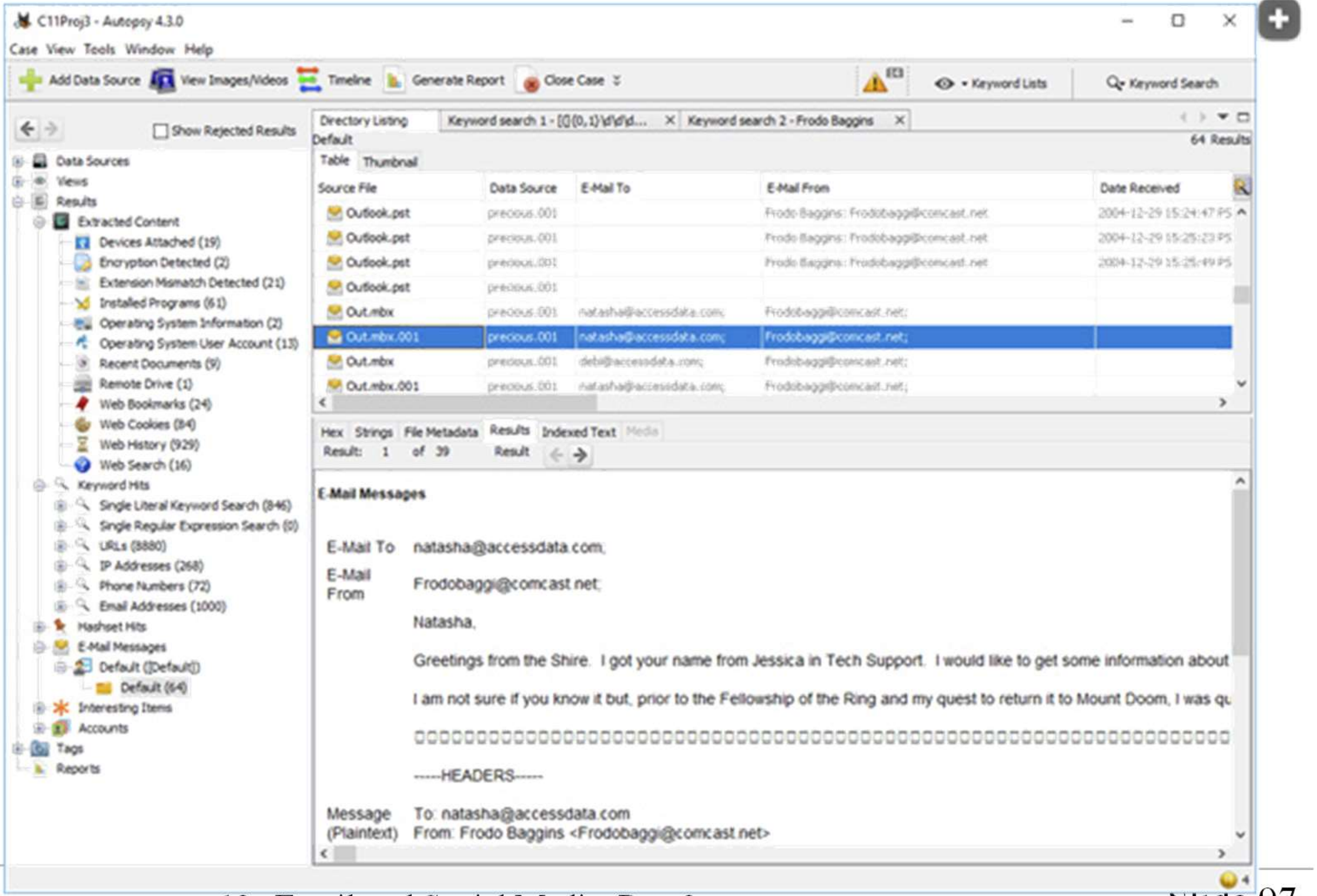
Examine Emails

5.

In the left pane, expand **E-Mail Messages** and **Default ([Default])** and click the **Default** folder. Scroll down the Result Viewer pane, and click the first `Out.mbx.001` mailbox to see its contents in the Content Viewer pane (see Figure 11-6).

Figure 11-6

Viewing the text of an e-mail



Default — 64 Results

Source File	Data Source	E-Mail To	E-Mail From	Date Received
Outlook.pst	precious.001		Frodo Baggins: Frodobaggi@comcast.net	2004-12-29 15:24:47 PS
Outlook.pst	precious.001		Frodo Baggins: Frodobaggi@comcast.net	2004-12-29 15:25:23 PS
Outlook.pst	precious.001		Frodo Baggins: Frodobaggi@comcast.net	2004-12-29 15:25:49 PS
Outlook.pst	precious.001			
Out.mbx	precious.001	natasha@accessdata.com;	Frodobaggi@comcast.net;	
Out.mbx.001	precious.001	natasha@accessdata.com;	Frodobaggi@comcast.net;	
Out.mbx	precious.001	debi@accessdata.com;	Frodobaggi@comcast.net;	
Out.mbx.001	precious.001	natasha@accessdata.com;	Frodobaggi@comcast.net;	

Result: 1 of 39 Result

E-Mail Messages

E-Mail To natasha@accessdata.com;

E-Mail From Frodobaggi@comcast.net;

Natasha,

Greetings from the Shire. I got your name from Jessica in Tech Support. I would like to get some information about

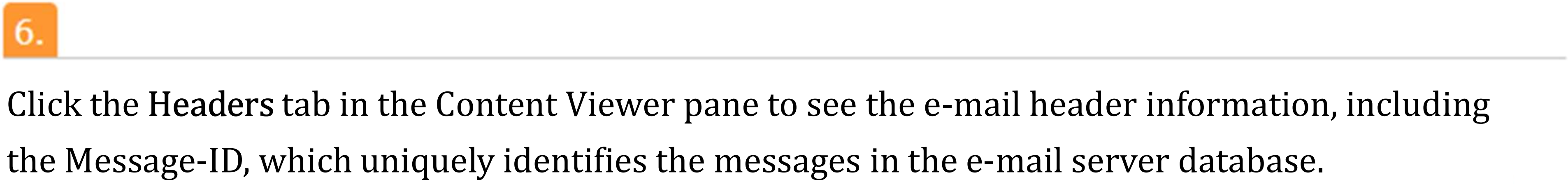
I am not sure if you know it but, prior to the Fellowship of the Ring and my quest to return it to Mount Doom, I was qu

□□

-----HEADERS-----

Message (Plaintext) To: natasha@accessdata.com
From: Frodo Baggins <Frodobaggi@comcast.net>

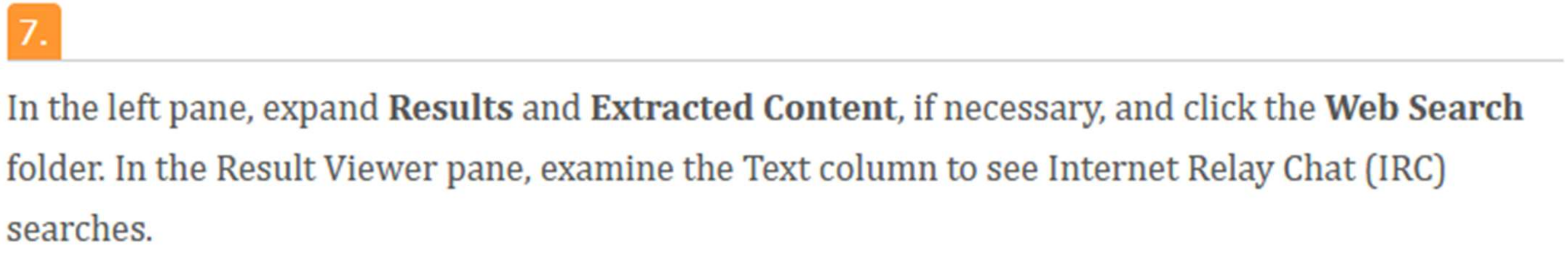
Examine Email Headers



6.

Click the **Headers** tab in the Content Viewer pane to see the e-mail header information, including the Message-ID, which uniquely identifies the messages in the e-mail server database.

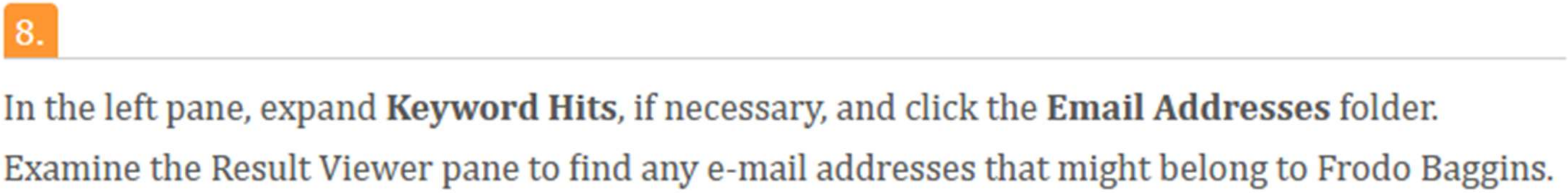
Analyze Web Searches



7.

In the left pane, expand **Results** and **Extracted Content**, if necessary, and click the **Web Search** folder. In the Result Viewer pane, examine the Text column to see Internet Relay Chat (IRC) searches.

Find Email Accounts



8.

In the left pane, expand **Keyword Hits**, if necessary, and click the **Email Addresses** folder. Examine the Result Viewer pane to find any e-mail addresses that might belong to Frodo Baggins.

Follow-up Questions

Finding Google Searches and Multiple Email Accounts

Continue the ***Finding Google Searches and Multiple Email Accounts Lab*** and answer the following questions.

1. *How many e-mails, including duplicates, did you find?*
2. *How many different Frodo Baggins e-mail addresses did Autopsy recover?*
3. *Frodo Baggins didn't have an AOL e-mail account.* ***True*** *or* ***False****?*
4. *How many Google searches for the term "computer forensics" were made?*
5. *MD5 hash values are displayed automatically in the default mailbox view.* ***True*** *or* ***False****?*