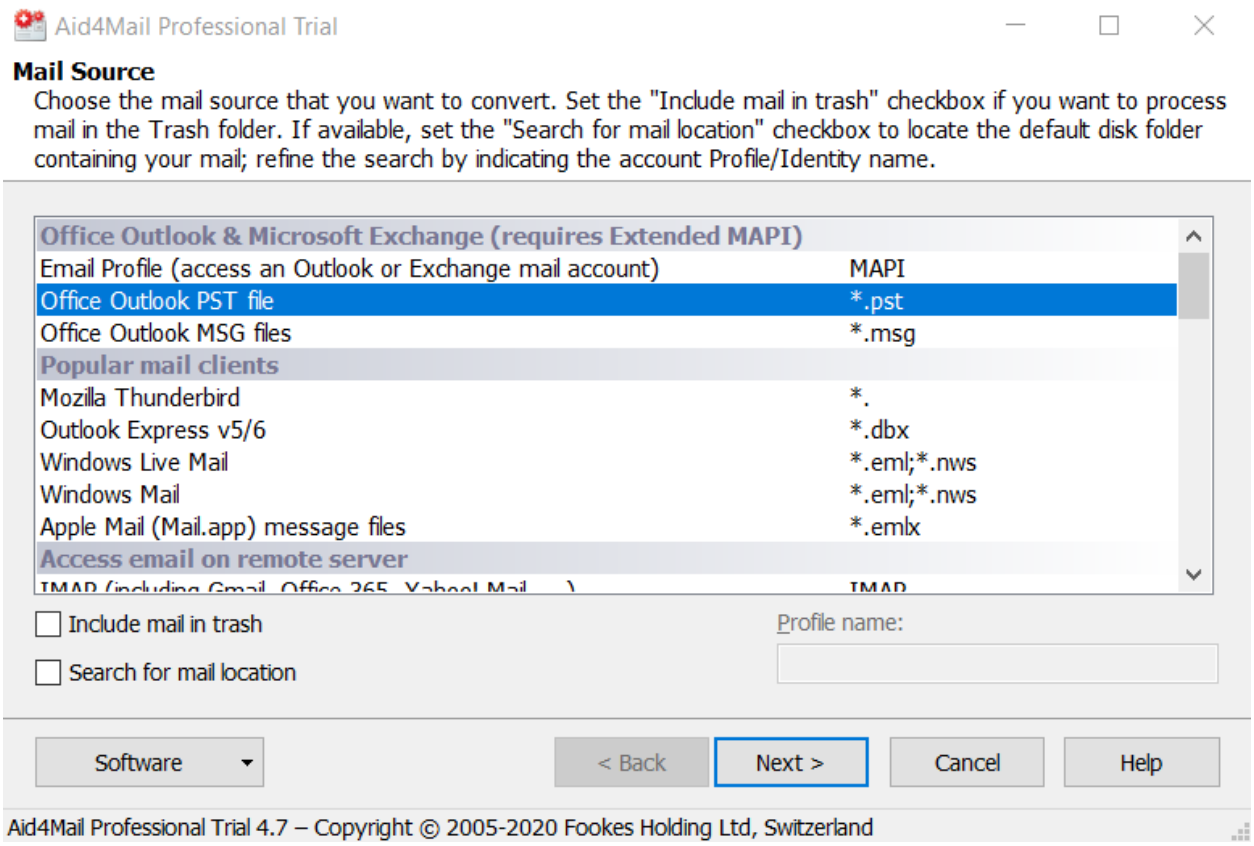
Hands-On Project 11-1

For this project, you use Aid4Mail to examine an Enron employee's e-mail.

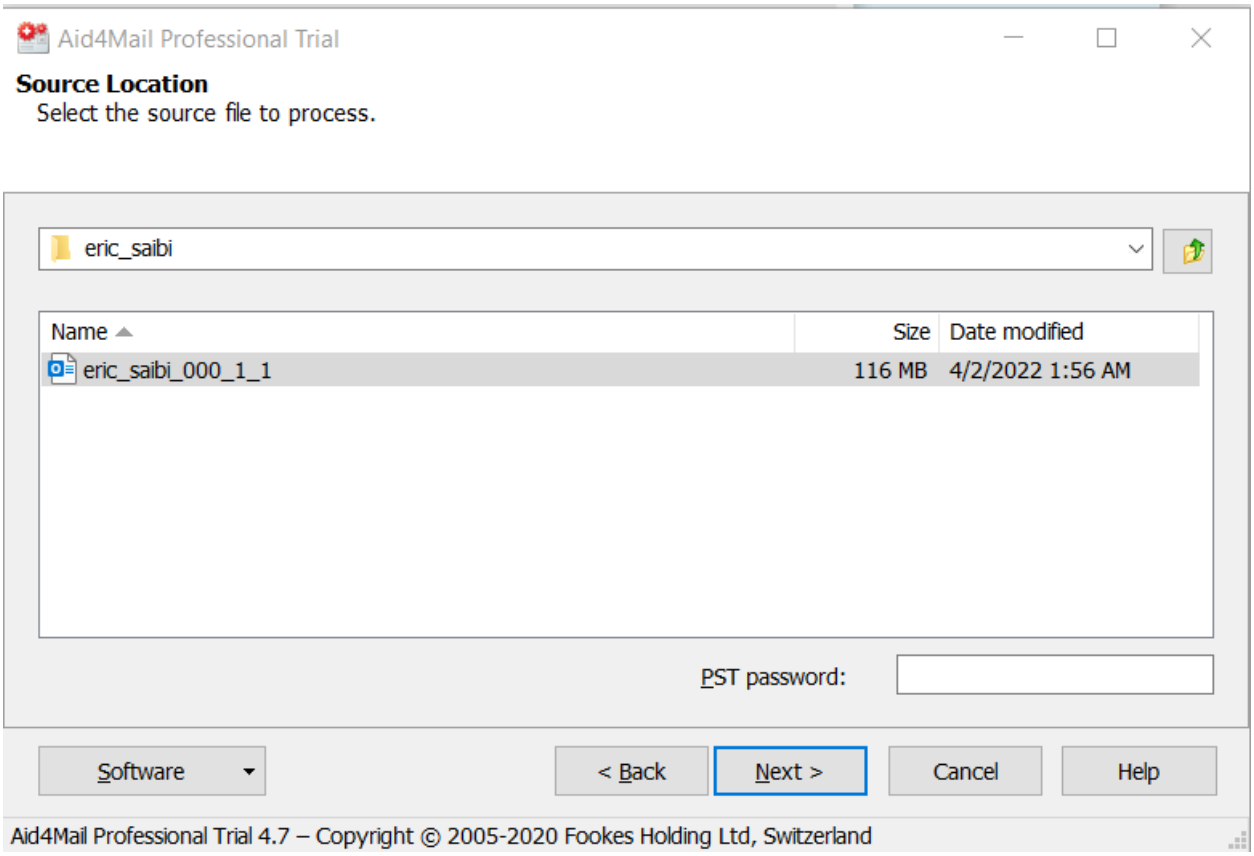
1. First, create a subfolder of your work folder called HandsOn11-1. Then start your Web browser and go to www.aid4mail.com/download-free-trial. Download and install Aid4Mail.

2. Go to the link you got for cleansed Enron e-mail. Download the complete Enron EDRM data set of 18 GB. Uncompress the file to your work folder, and copy the eric_saibi. pst file to your Work\Chap11\Projects folder.

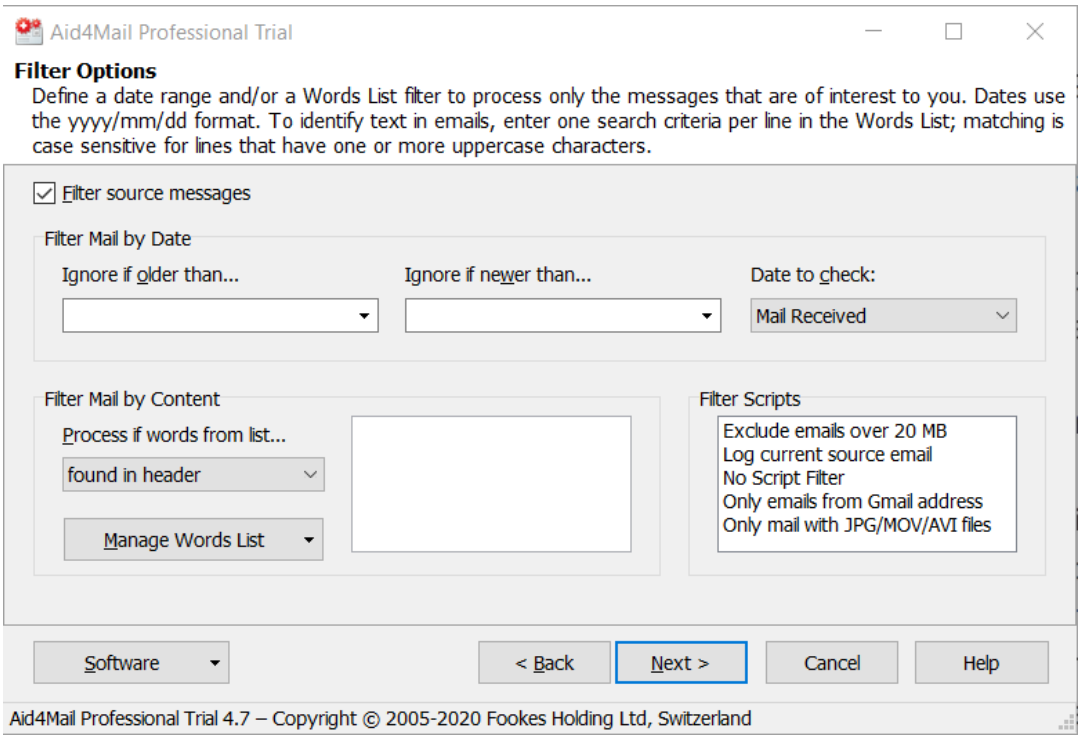
3. Start Aid4Mail. Click Next in the Welcome window. Click Office Outlook PST file, and then click Next.



4. Navigate to and click the eric_saibi.pst file, and then click Next. In the Source MAPI Folders window, click Next.



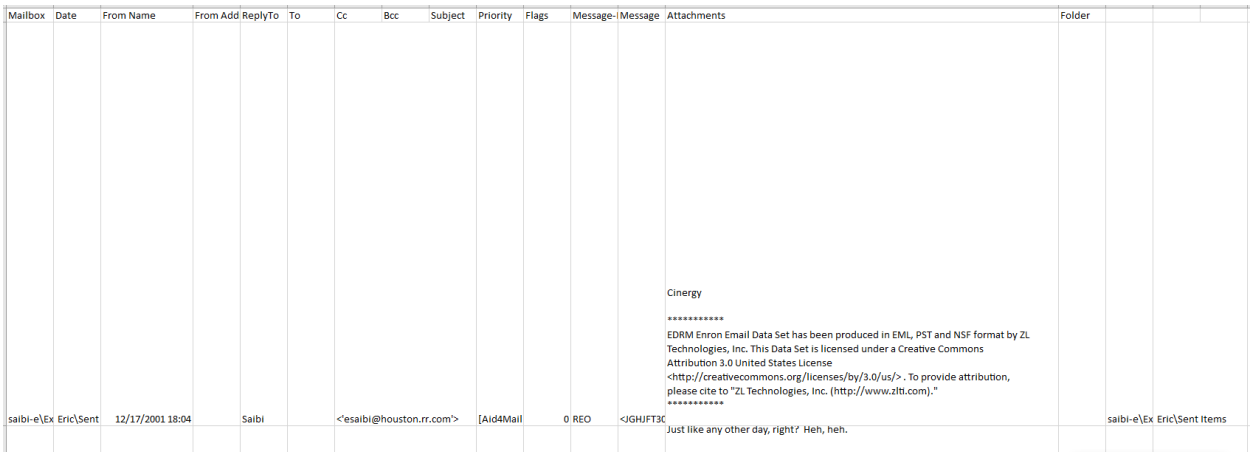
5. In the Filter Options window, you can select a range of dates and words to search for. For now, leave the default settings, and click Next.



6. In the Target Format window, scroll to the bottom and examine the export options shown in Figure 11-13. You can export metadata in CSV or XML format, for example. Click Convert e-mails to CSV, and then click Next.

7. In the Target Settings window, click the HandsOn11-1 subfolder of your work folder, and enter the filename Eric_Saibi.CSV. Click Next, and then click Start.

8. After Aid4Mail has finished converting the e-mail to CSV format, open the file in Microsoft Excel (or any spreadsheet program), and exit Aid4Mail. Scroll through Eric Saibi's e-mail data and look for messages that might contain personal information or be related to the Enron scandal. Go to the Aid4Mail Web site and read the user manual. What can be done to make viewing data easier? Write a short paper describing the options



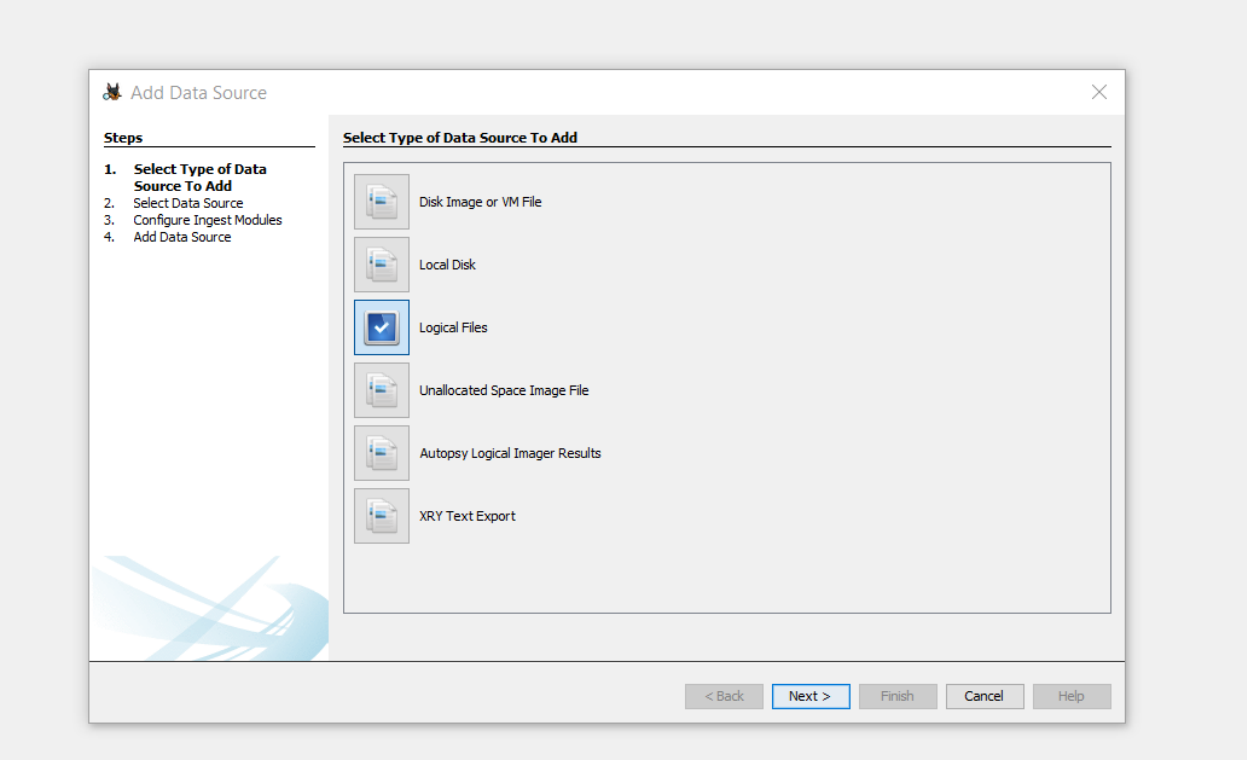
Mailbox	Date	From Name	From Add	ReplyTo	To	Cc	Bcc	Subject	Priority	Flags	Message-I	Message	Attachments	Folder			
													Cinergy ********** EDRM Enron Email Data Set has been produced in EML, PST and NSF format by ZL Technologies, Inc. This Data Set is licensed under a Creative Commons Attribution 3.0 United States License <http://creativecommons.org/licenses/by/3.0/us/> . To provide attribution, please cite to "ZL Technologies, Inc. (http://www.zlti.com)." **********			
saibi-e\Ex	Eric\Sent	12/17/2001 18:04		Saibi		<'esaibi@houston.rr.com'>		[AId4Mail	0	REO	<JGHJFT3(	Just like any other day, right? Heh, heh.		saibi-e\Ex	Eric\Sent Items		

Hands-On Project 11-2

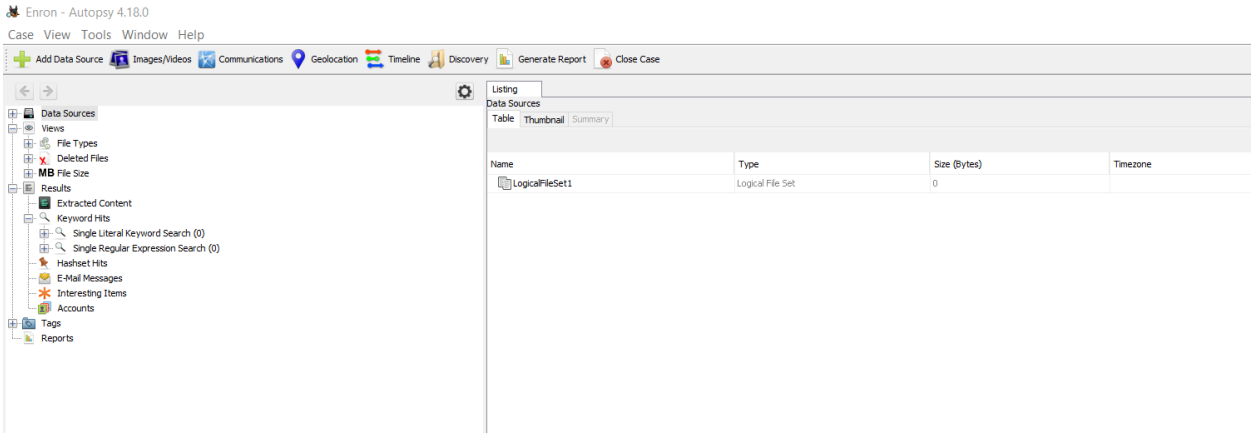
In this project, you use Autopsy for Windows to examine e-mail from the Enron case.

1. Start Autopsy for Windows and click the Create New Case button. In the New Case Information window, enter Enron in the Case Name text box, and click Browse next to the Base Directory text box. Navigate to and click your work folder, and then click Next. In the Additional Information window, type today's date in the Case Number text box and your name in the Examiner text box, and then click Finish.

2. In the Select Data Source window, click the Select data source type list arrow, and click Logical Files. Click the Browse button next to the "Browse for an image file" text box, navigate to your work folder, click the Kenneth Lay .pst files, and then click Open. Click Next.

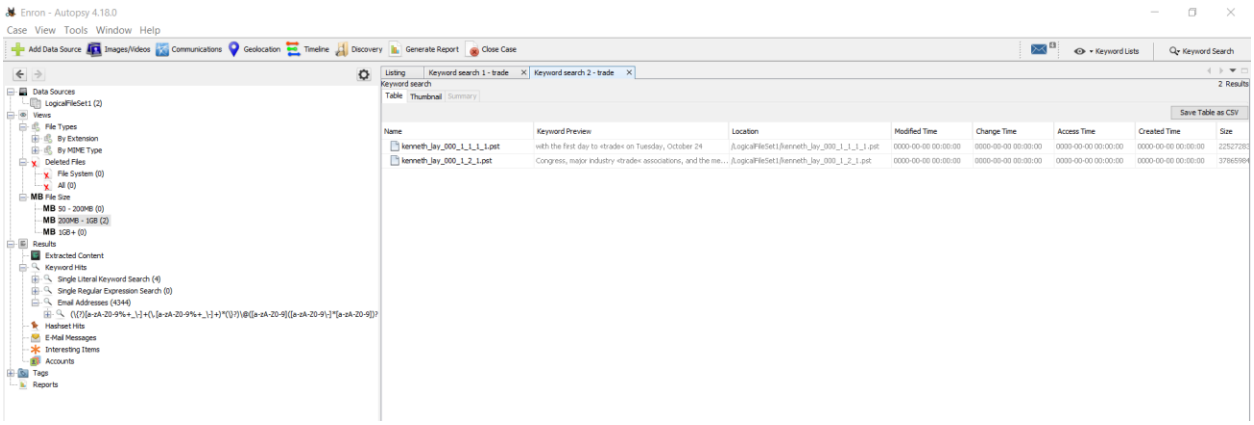


3. In the Configure Ingest Modules window, click Next, and then click Finish. When Autopsy has finished processing the ingest modules (about 20 minutes), click Keyword Search at the upper-right corner and enter the following search keywords: trade, trading, stocks, and money.

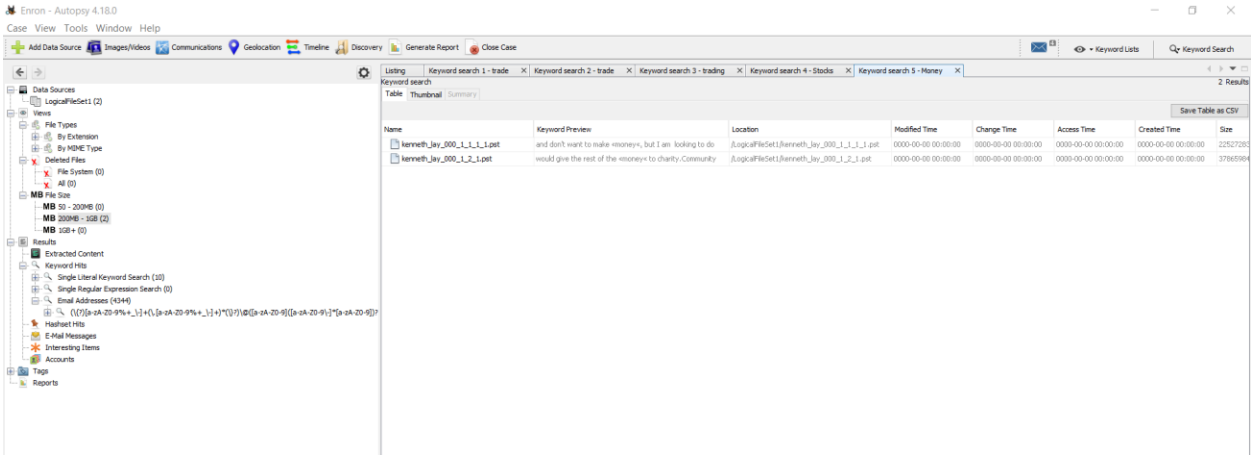


Keyword: trade

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)



Keyword: Money



4. Research Kenneth Lay's role in the Enron scandal, and then examine his e-mails. What additional words would you add to the search terms? When you're finished, exit Autopsy for Windows.

Additional keywords: dividends, Exchanges, Market

He received email from the media. The email demands him to donate which he had made from selling the stock. This was before the bankruptcy was declared to the employee's transition fund.

We know that autopsy helps to read the actual emails. It is very much helpful in completing investigation. The evidence that is being presented would be that Kenneth sold his stock before filing for bankruptcy. He knew he did this would make millions of dollars

We can implement these ways to make data viewing easier:

- Stop using applications like Antivirus that keeps track on emails so that its running smooth
- Enable “Donot add duplicate messages” options in export options
- Stop using MAPI conversion by using MapiConvOff switch. It is available in version 1.98 or higher which is slower and can be used faster method
- Enable generated emails processing faster by using CLI with no further reliable checks.