


Investigating Email Crimes


Module 12


Investigating Email Crimes


Like any other form of communication, email is also misused by criminal elements. The ease, speed, and relative anonymity of email have made it a powerful tool for criminals. Investigating email crimes is the process of tracking, collecting, analyzing, and investigating the digital evidence and cyber trails.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

Emily had received an email stating that she has won a huge amount from a big company, but the amount can be collected only after paying certain taxes. The email also had instructions along with the account number to send the amount for receiving the cash prize. She did as stated in the email and later came to know that it was a spam email and someone has cheated her.

To investigate email crimes as a **forensic investigator**, you must know how to **track emails** and **extract** or **recover deleted email** messages from Microsoft Outlook PST files or Microsoft Outlook Express DBX files, etc., using various email tracking and investigation tools.

Lab Objectives

The objective of this lab is to provide expert knowledge on tracking emails, investigating email crimes, and other responsibilities that include:

- Recovering deleted email messages and attachments
- Recovering message contacts
- Tracking sender's IP address
- Recovering and saving deleted emails
- Tracing an email to its true geographical source
- Collecting Network (ISP) and Domain Whois information for any email traced


Lab Environment

To carry out the lab, you need:

- A computer running **Windows Server 2012** virtual machine.
- A web browser with an **Internet** connection.
- Administrative privileges to run the tools.

Lab Duration

Time: 50 Minutes

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes**

Overview of Investigating Email Crimes

Investigating email crimes is the process of **tracking, collecting, analyzing**, and **investigating the digital evidence and cyber trails**. Digital evidence and cyber trails can relate to email spamming, mail bombing/mail storms, email spoofing, identity fraud/chain letters, phishing attacks, and email hijacking.



TASK 1

Overview

Lab Tasks

Recommended labs to assist you in investigating email crimes:

- Recovering Deleted Emails Using the **Recover My Email** utility.
- Investigating Email Crimes Using **Paraben's Email Examiner** Tool.
- Tracing an Email Using the **eMailTrackerPro** Tool.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your expert opinion on email crime.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Recovering Deleted Emails Using the Recover My Email

Recover My Email is mail recovery software that can recover deleted email messages from either Microsoft Outlook PST files or Microsoft Outlook Express DBX files.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Daniel is a web expert and part of a group that hacks other's accounts for monetary benefits. Daniel was a suspect in a case; wherein the attacker has used email attachments to send malware to the victim that could copy the user's passwords and other private details and prompt them to the sender. However, when investigators checked Daniel's system, they did not find any such emails as he had deleted them already. How can the investigators proceed further in such cases?

The ease, speed, and relative anonymity of email have made it a powerful tool for criminals. To avoid being traced or tracked, criminals usually delete the message after performing the email crimes. Recovering those deleted messages is very crucial for investigating email crimes. To investigate email crimes as a **forensic investigator**, you must know how to recover deleted email messages from Microsoft Outlook PST files or Microsoft Outlook Express DBX files, etc., using various email recovery tools.

Lab Objectives

The objective of this lab is to help investigators understand how to track and investigate email crime using various tools to obtain:

- Message contacts.
- Deleted email messages and attachments.

Lab Environment

To carry out the lab, you need:


- Recover My Email, located at **C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes\Email Forensics Tools\Recover My Email**

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes

- You can also download the latest version of **Recover My Email** from the link <http://www.recovermyemail.com/inbox-repair-tool-download.php>
- If you decide to download the latest version, screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- Administrative privileges to run the tools

Lab Duration

Time: 15 Minutes

 Mail Recovery for Outlook.PST files with the 2 GB size limit problem

Overview of Recover My Email

Recover My Email is mail recovery software that can recover deleted email messages from either Microsoft Outlook PST files or Microsoft Outlook Express DBX files. It also allows saving mail recovery results and attachments.

Lab Tasks

The idea in this lab is to:

- Recover the deleted or corrupted email and collect various information related to that specific email
 - Analyze and examine the collected information for suspicious activity
1. Navigate to **C:\CHFI-Tools\Evidence Files\Outlook Files\Outlook .pst files** for evidence files. These two files are sample deleted email files which we have used for the demonstration purpose.

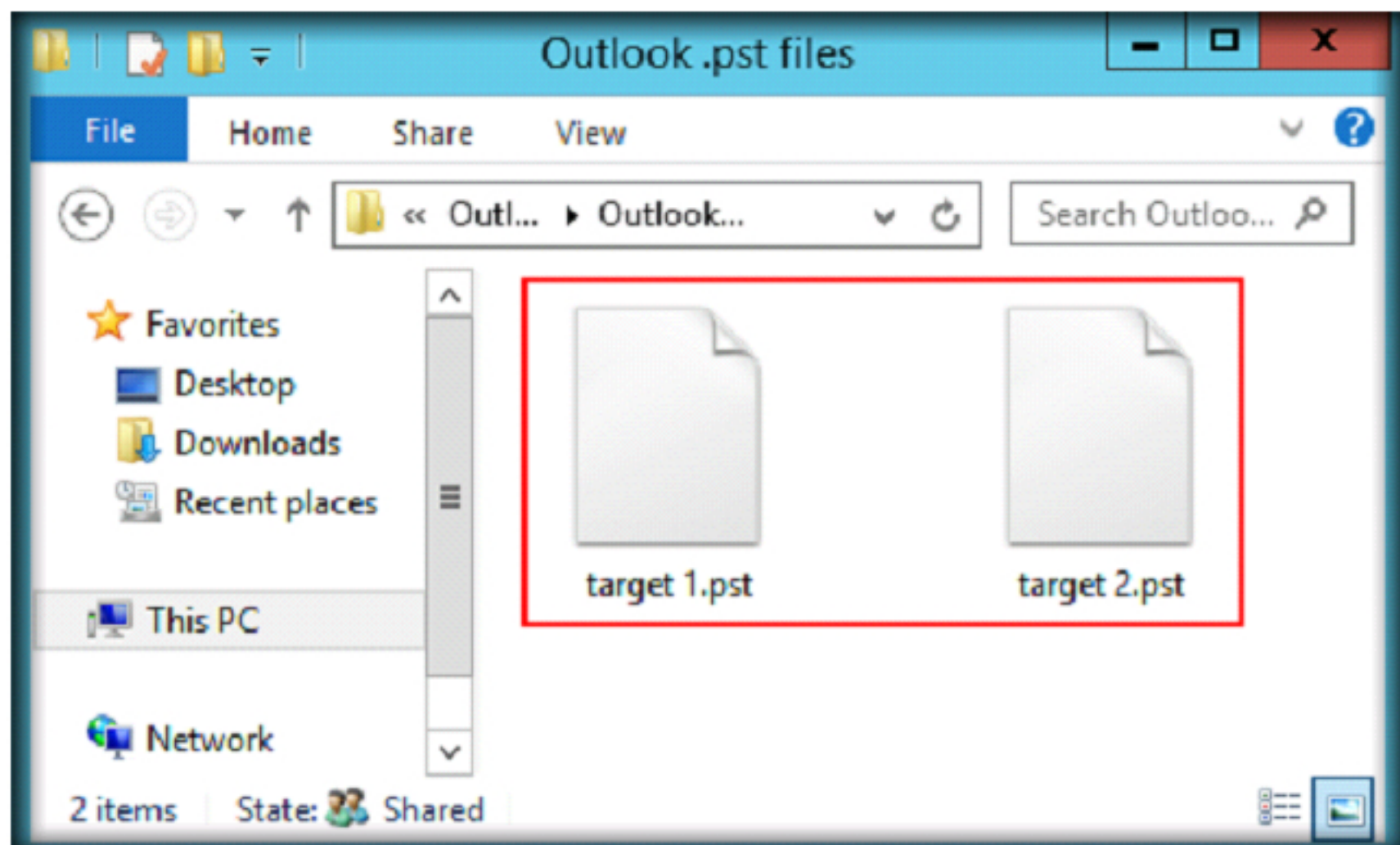


FIGURE 1.1: Sample evidence files

2. Navigate to **C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes\Email Forensics Tools\Recover My Email**.
3. Double-click **RecoverMyEmail-Setup.exe** to launch the setup.


Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. While installing the application, check **Create a desktop icon** option, click **Next**, and follow the wizard-driven installation steps to install the application.
5. Once the installation is finished make sure that **Launch Recover My Email** option is checked and click **Finish** button to automatically launch the Application.
6. Alternatively, you can double-click Short-cut icon on the desktop to launch, or you can also launch from Start menu apps.
7. The **Recover My Email** main window appears along with Tip of the Day pop-up as shown in the screenshot, click **Close** button to close the pop-up window.

Note: If you want to see the next tip, click the **Next Tip** button; otherwise, click **Close** button to close the window.

TASK 1

Launching Recover My Email

 Repair corrupt Microsoft Outlook PST and Outlook Express DBX files.

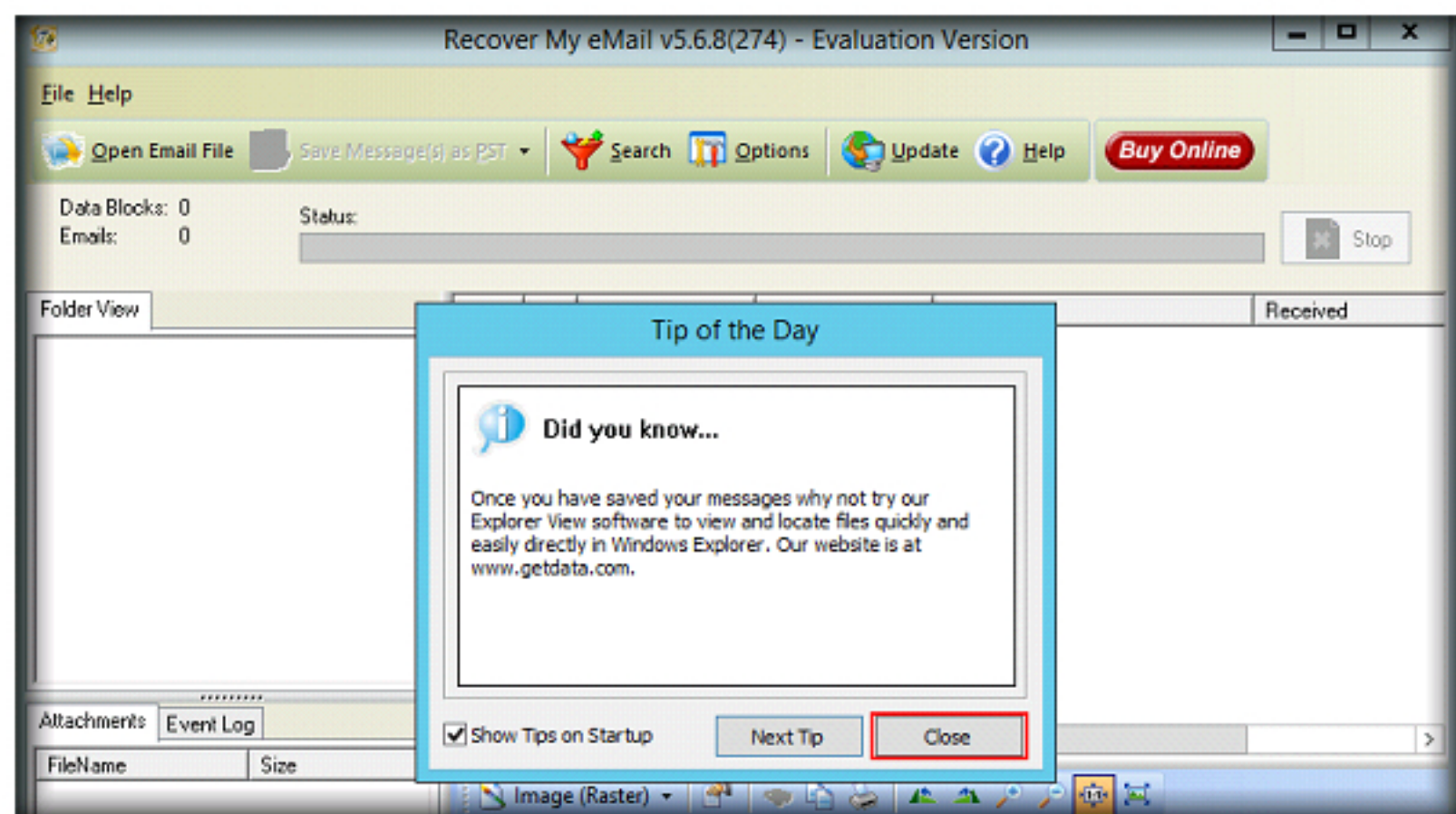


FIGURE 1.2: Recover My eMail main window

8. Click the **Open Email File** button to open the email files.

TASK 2

Selecting the Target PST File

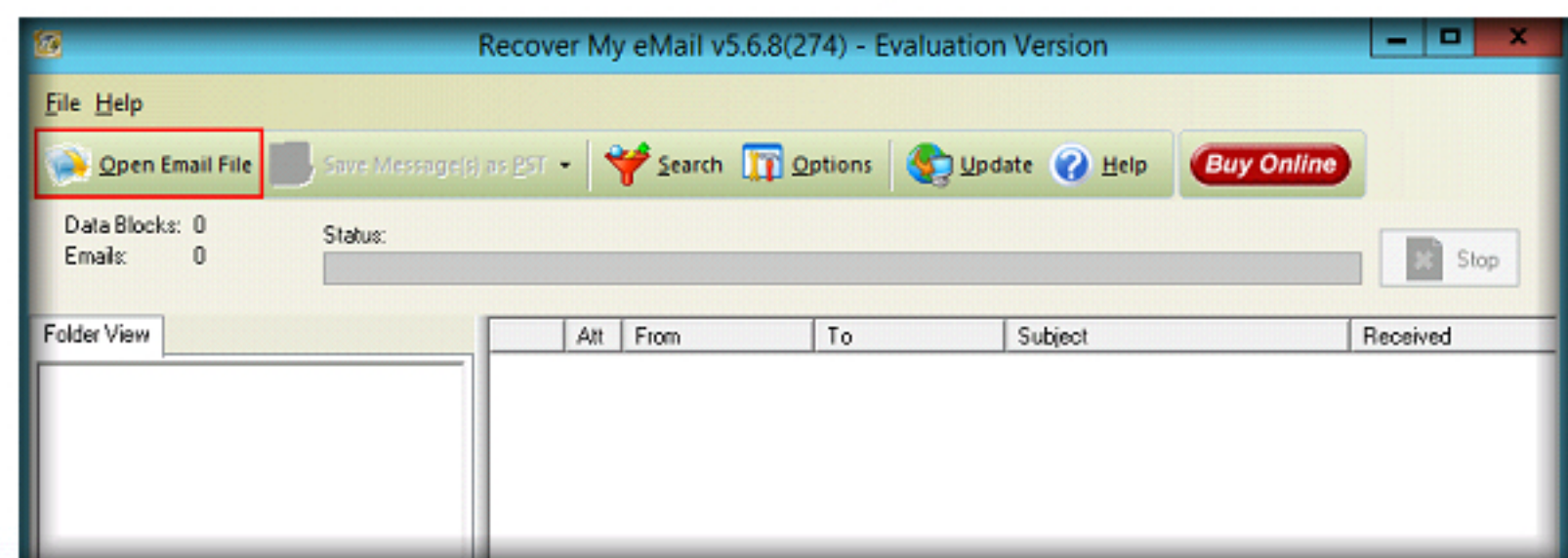


FIGURE 1.3: Browsing for target PST file

9. An **Open** window appears, select the target account's .pst file (**C:\CHFI-Tools\Evidence Files\Outlook Files\Outlook .pst files**) from which you want to recover the deleted files and click **Open**. Here we are considering "target 1.pst" as the target.

It allows saving mail recovery results, including message contacts and attachments in an error-free new PST file with full folder structure.

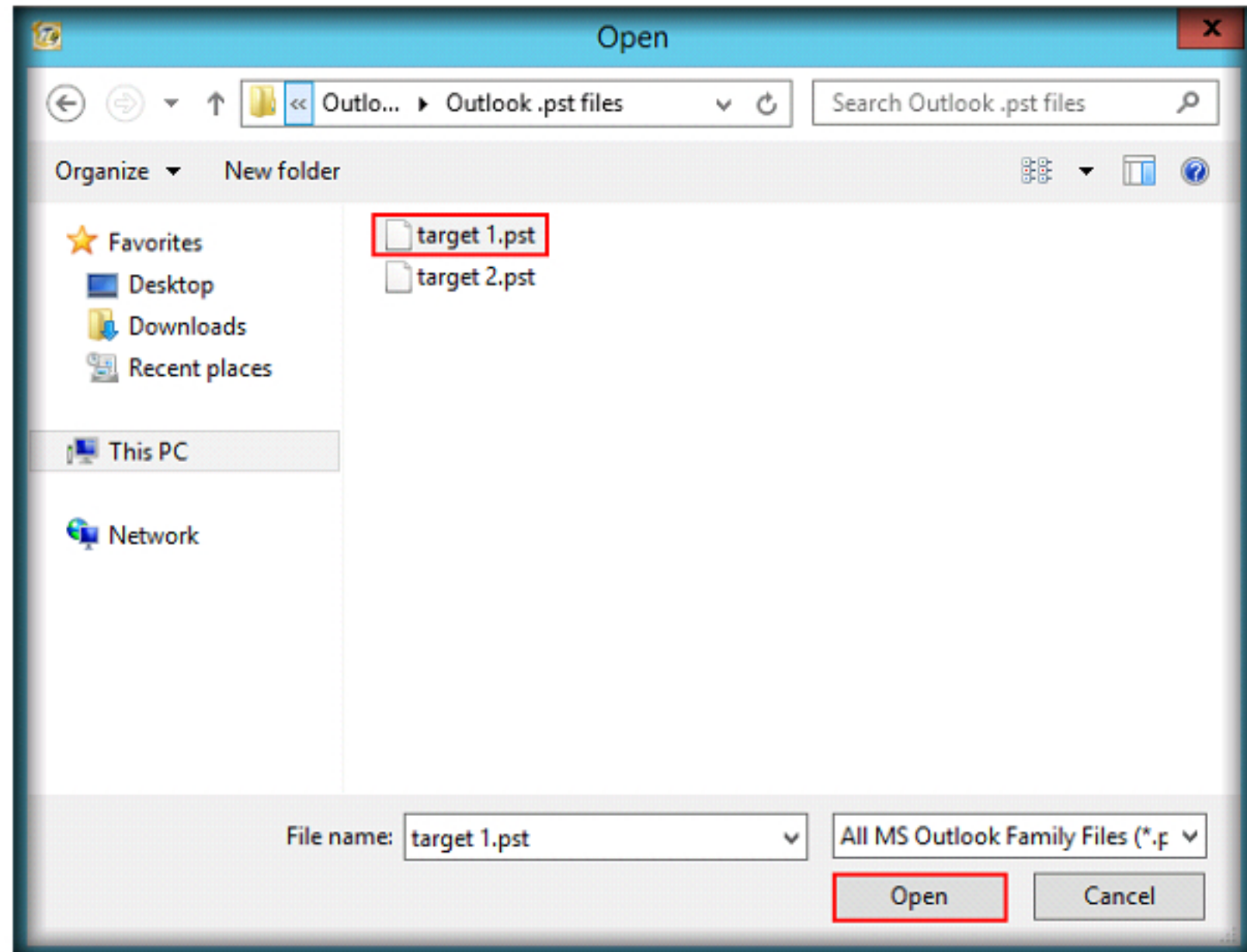


FIGURE 1.4: Selecting the target PST file

10. When you click the **Open** button, the Recover My Email tool will scan the selected .pst email file and display the folder view with the results obtained in the left pane of the window.

Supports Outlook (PST recovery): 2000, 2002, 2003, 2007, and 2010 (including Outlook 2010 32- and 64-bit versions).

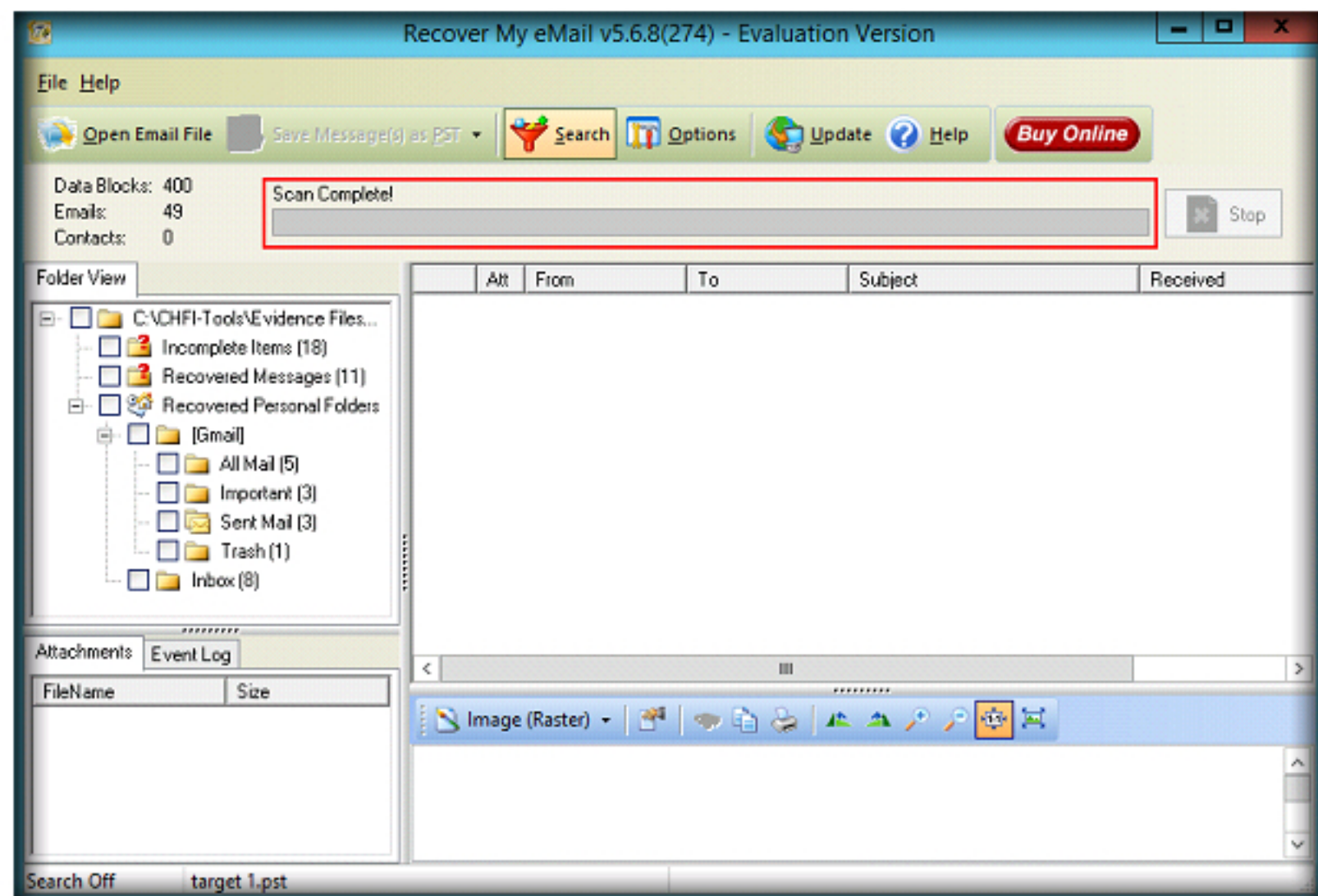


FIGURE 1.5: Figure showing Scan Complete notification

11. To see the recovered emails, click **Recovered Messages** in the **Folder View** tab (Left pane). It will display the list of recovered emails and messages. Here it will show the recipient's email address, subject, and received date and time.

It supports all versions of Outlook Express (DBX recovery).

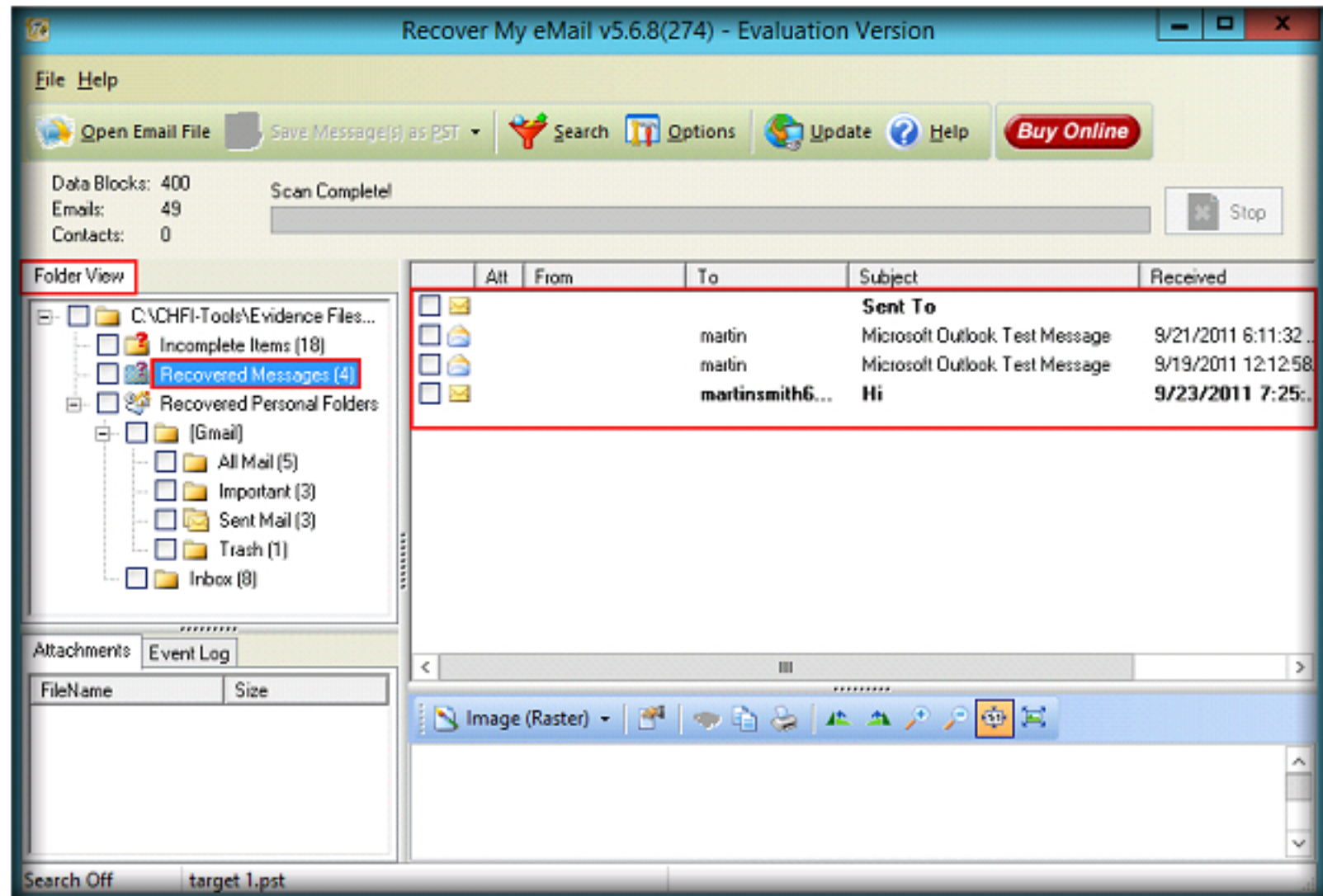


FIGURE 1.6: Viewing Recovered Messages folder in the Folder View tab

12. To see the recovered emails or messages, search the **All Mail** folder with the respective recipient address and the subject of the recovered email listed in the recovered messages folder. To search, first click the **Search** button.

It allows you to save the recovered emails in four formats: PST, EML, MSG, and List.

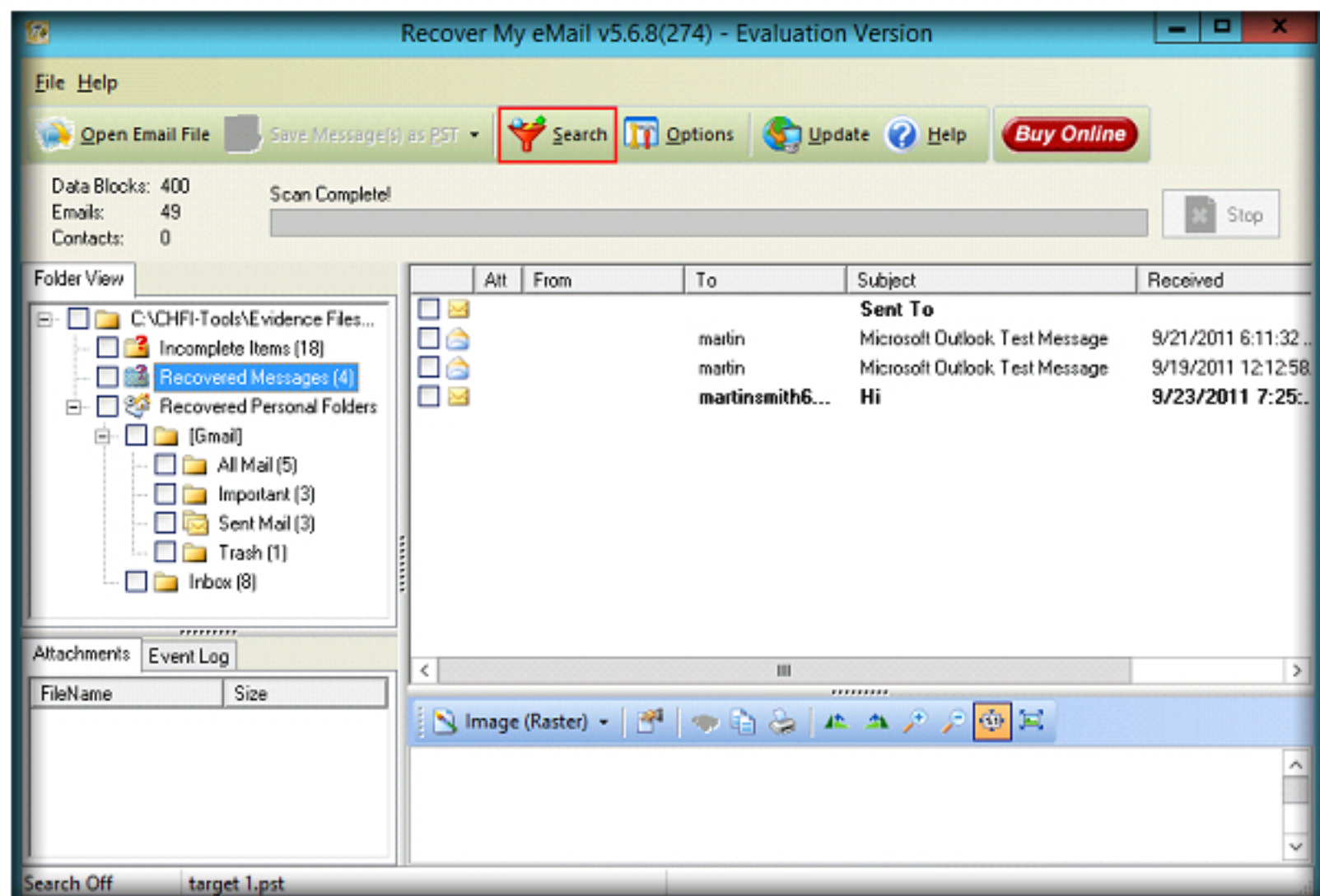


FIGURE 1.7: Figure showing Search button

13. A **Recover My eMail** window appears where you need to specify options to search the emails.

14. In this lab, we are selecting **By To:** (an email ID) and **By Subject:** (Hi) options.
15. Click **OK**.

It allows browsing all your mail messages and attachments.

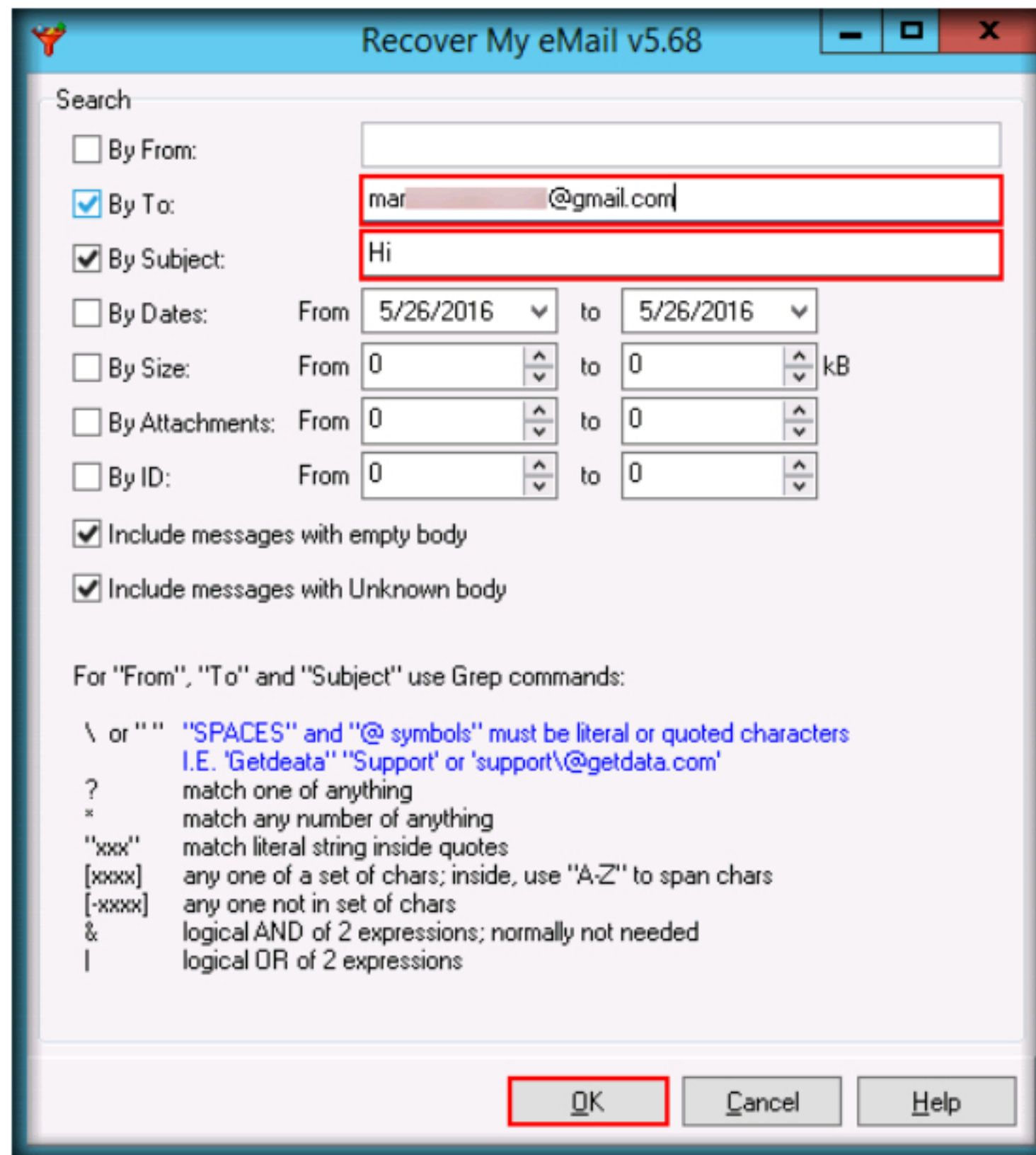


FIGURE 1.8: Searching recovered messages (pop-up window scaled down for resolution)

TASK 3

Viewing the Email Content and Attachments

16. Now click **All Mail** option in the left pane of the window, which displays the list of emails matching your search criteria.
17. If it is displaying more than one result, then make your search more specific by including other details, such as file size, etc. on the **Search** tab.

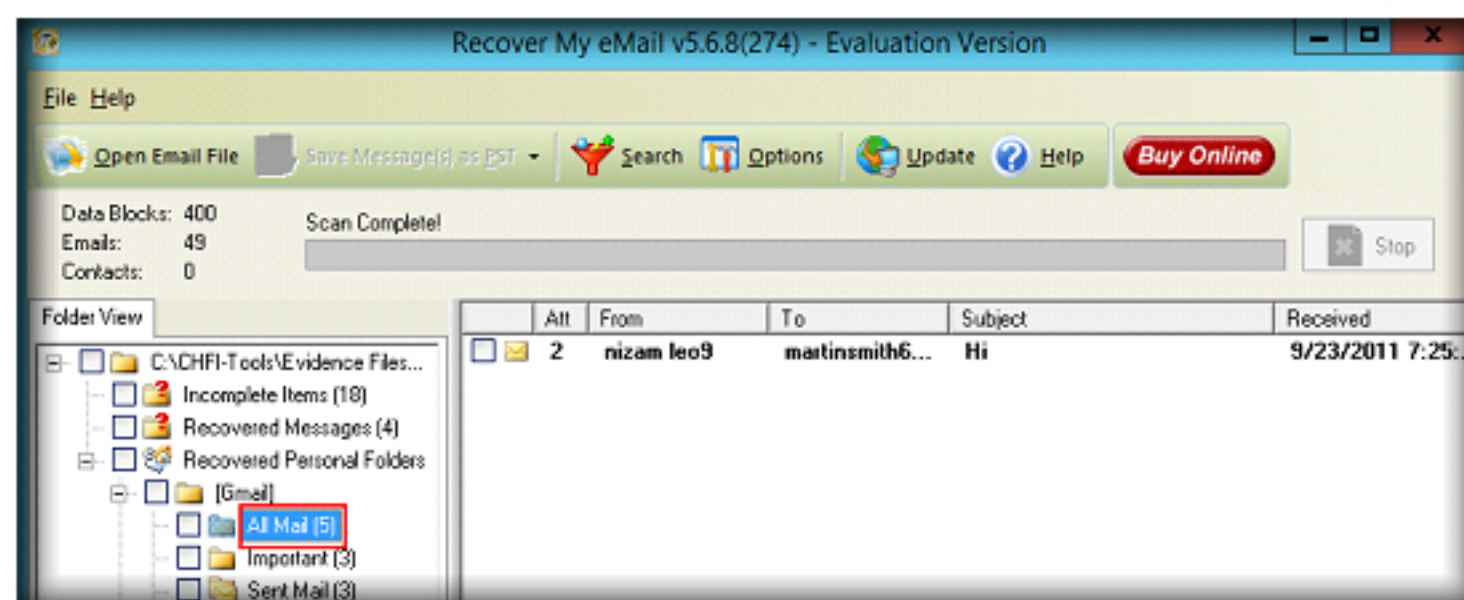


FIGURE 1.9: Search results in the All Mail folder

- To see the actual content of the email, click the email. The email content will display in the bottom pane of the window.

Preview the contents of all messages and attachments that can be recovered.

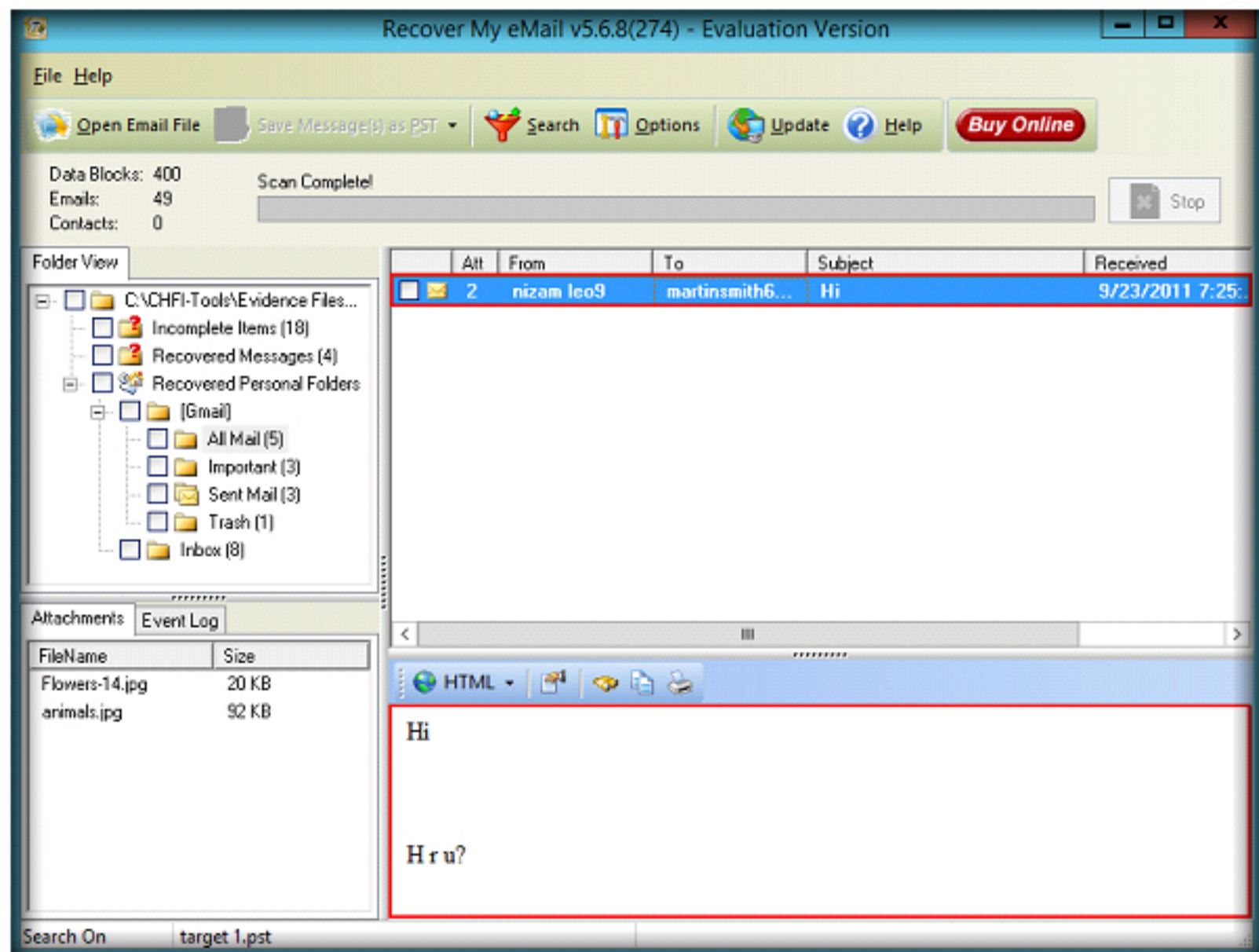


FIGURE 1.10: Viewing email contents

- To see the attachments, if any, click the file name of the attachment listed in the **Attachments** pane on the left of the window. It will display the attachment in the **Data Viewer** pane.

Save messages as a new email, or save individual messages as .eml files.

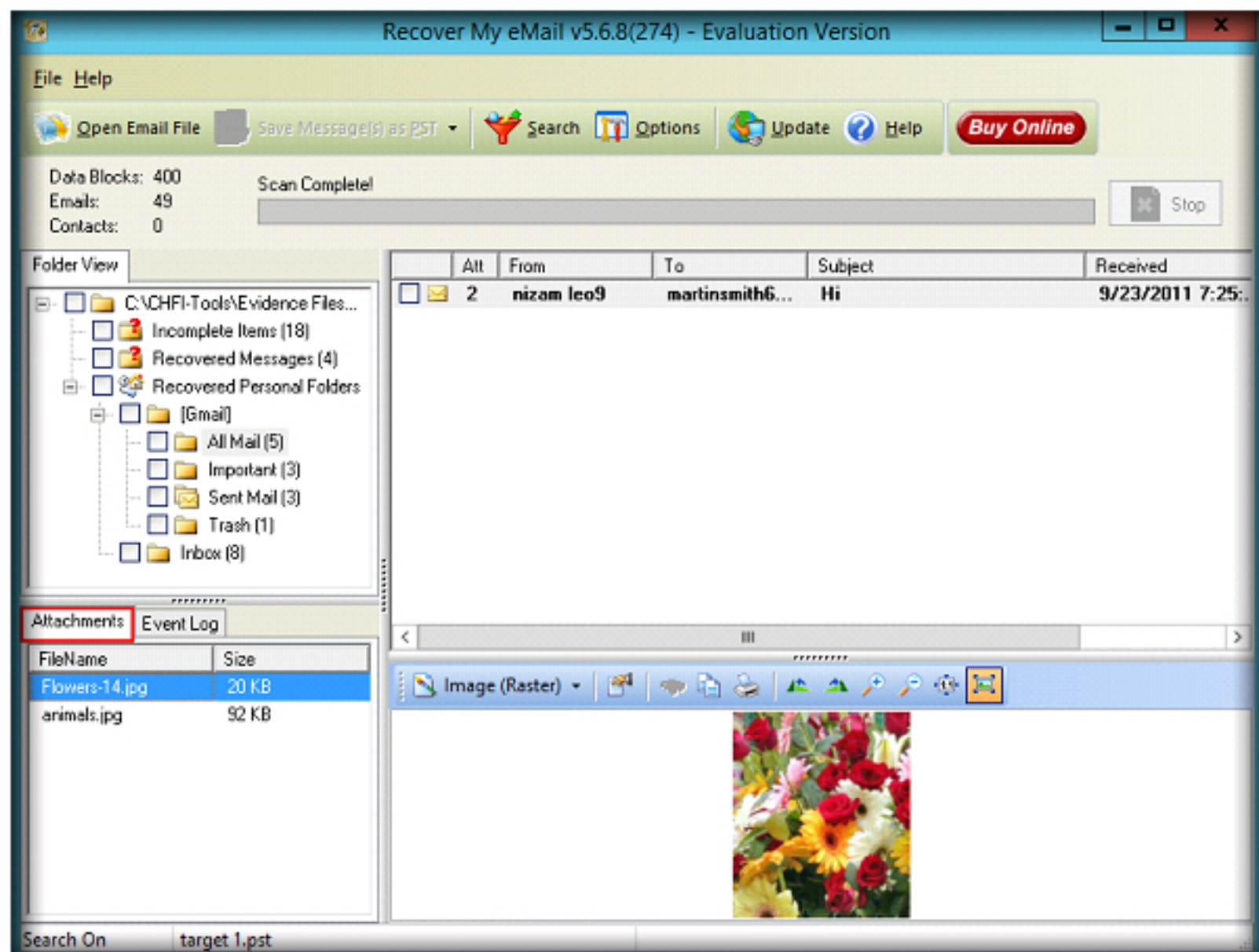


FIGURE 1.11: Viewing email attachments

20. To save the recovered emails, select the emails you want to save and click the **Save Messages** button. Select the format in which you want to save the email from the drop-down list.

Note: The trial version of the tool will not allow to save the recovered messages. If you want to save the files, you need to buy the product activation key from the vendor.

Lab Analysis

Analyze the deleted messages after recovery and document the results related to the lab exercise. Give your expert opinion on the suspicious email.


PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.


Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs


Investigating Email Crimes Using Paraben's Email Examiner Tool


Paraben's Email Examiner is a forensic email examination utility. It can examine various email formats such as America Online (AOL), Outlook Exchange (PST), Eudora, and many others.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario


A brokerage firm has filed a complaint with the district authorities stating that one of its employees has been sharing their trade secrets as well as contract information with their rivals. The court of law has ordered a probe, which includes scanning of individual devices for emails containing suspicious information. The company has adopted a BYOD policy, and users are allowed to use different email clients according to their requirement. The investigators use Paraben's Email Examiner to analyze various email clients and the formats they use.

To investigate email crimes as a **forensic investigator**, you must know how to trace out the person and the location of the person responsible for the specific email that you are investigating.

Lab Objectives

The objective of this lab is to help investigators learn and perform an investigation of email crimes. Using Paraben's Email Examiner you can:

- Add evidence image (.pst and .dbx) files
- Recover deleted emails
- Save recovered emails

 **Tools**
demonstrated in
this lab are
available in
**C:\CHFI-
Tools\CHFIv9
Module 12
Investigating
Email Crimes**

Lab Environment

To carry out the lab, you need:

- Paraben's Email Examiner, located at **C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes\Email Forensics Tools\Paraben's Email Examiner**.
- You can also download the latest version of **Paraben's Email Examiner** from this link <https://www.paraben.com/email-examiner.html>.
- To download the tool from Paraben's website, you need to fill out the registration form.
- If you decide to download the latest version, screenshots shown in the lab might differ.
- **Windows Server 2012** running on the virtual machine.
- Administrative privileges to install and run the tools.
- A web browser with an **Internet** connection.

Lab Duration

Time: 15 Minutes

Overview of Paraben's Email Examiner

Paraben's Email Examiner is a forensic email examination utility. It can examine various email formats such as America Online (AOL), Outlook Exchange (PST), Eudora, and many others. It can also recover deleted messages and folders. It doesn't just recover email in the deleted folders; it recovers email deleted from deleted items (deleted/deleted).

Lab Tasks

TASK 1

Install and Launch Email Examiner

1. Logon to **Windows Server 2012** virtual machine.
2. Navigate to **C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes\Email Forensics Tools\Paraben's Email Examiner**.
3. Double-click **emx-demo.exe** to launch the setup, and follow the wizard-driven installation instructions.
4. Once the installation is complete, **Paraben's Dongle Manager** wizard appears, follow the wizard driven steps to install the application. On completing the installation, **Paraben's Email Examiner** dialog box appears asking you to restart the computer. Click **Yes**.
5. **Restart** the computer after installation.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**

6. Double-click **E-mail Examiner** shortcut icon on the desktop to launch Email Examiner.

Note:

Paraben's Email Examiner has been integrated into the P2 Commander interface.

- An **Activation** pop-up appears, click **Later**.
- If **Warning** message about the license expiration appears, **download** the latest version of the Paraben Email Examiner from <http://www.paraben.com/programs/emx.html>, uninstall the previously installed **Paraben Email Examiner** tool, and install the newly downloaded **Paraben Email Examiner** tool.

7. Paraben's E-mail Examiner main window appears along with **Add Evidence** wizard, as shown in the screenshot.



FIGURE 2.1: Paraben's Email Examiner main window with Add Evidence wizard



TASK 2


Creating a New Case

8. Before starting an investigation, you should create a **case** by clicking the **Create New Case** button.



FIGURE 2.2: Creating a new case

9. A **New Case** window appears, displaying the **Welcome** section. Click **Next**.

 Features advanced Boolean searching.

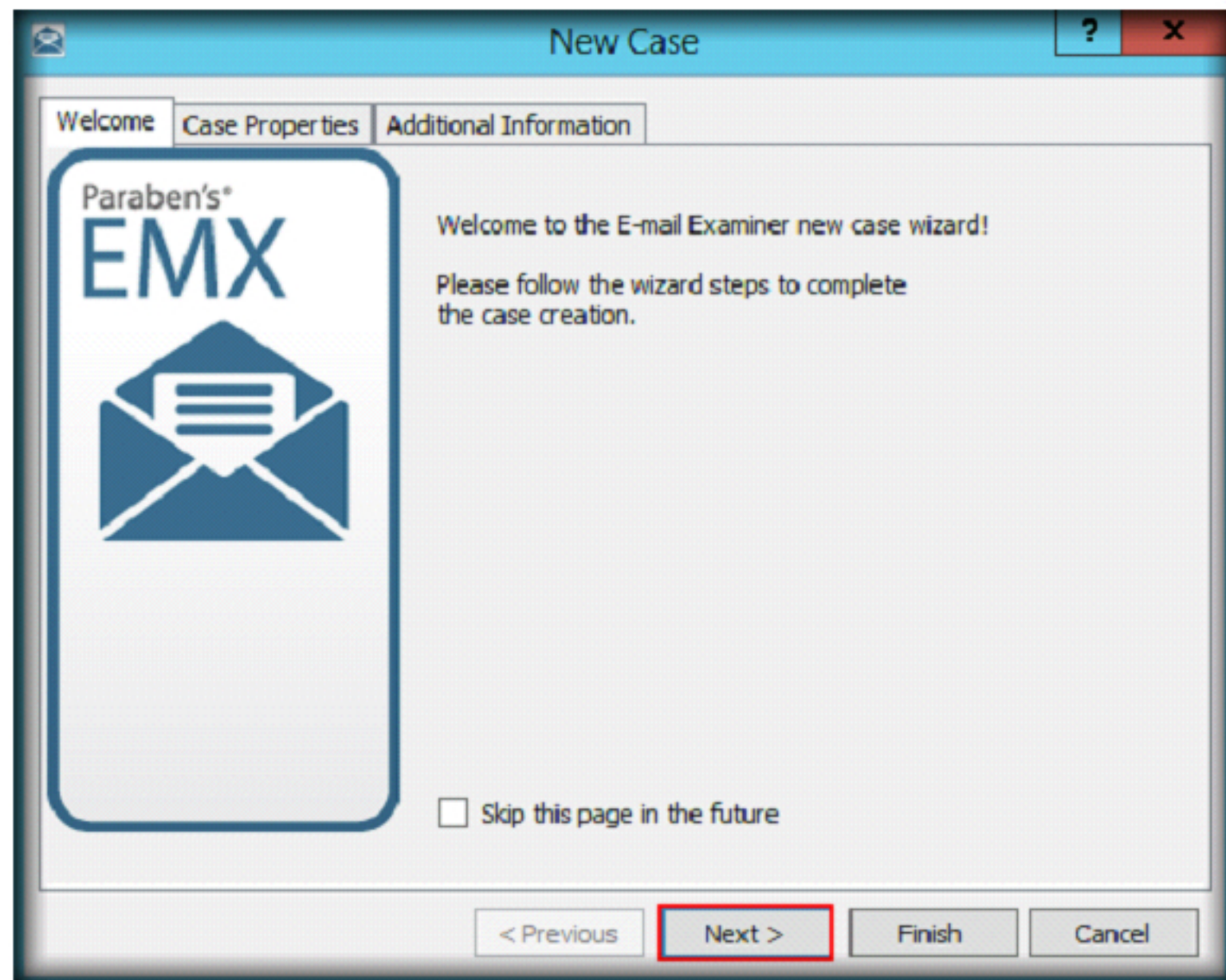



FIGURE 2.3: New Case wizard - Welcome tab

10. **Case Properties** section appears. Fill the **Case name** and **Description** fields with the appropriate information and click **Next**. This selection will take you to the **Additional Information** tab.

 Added support for Open Office document format with attachment preview.

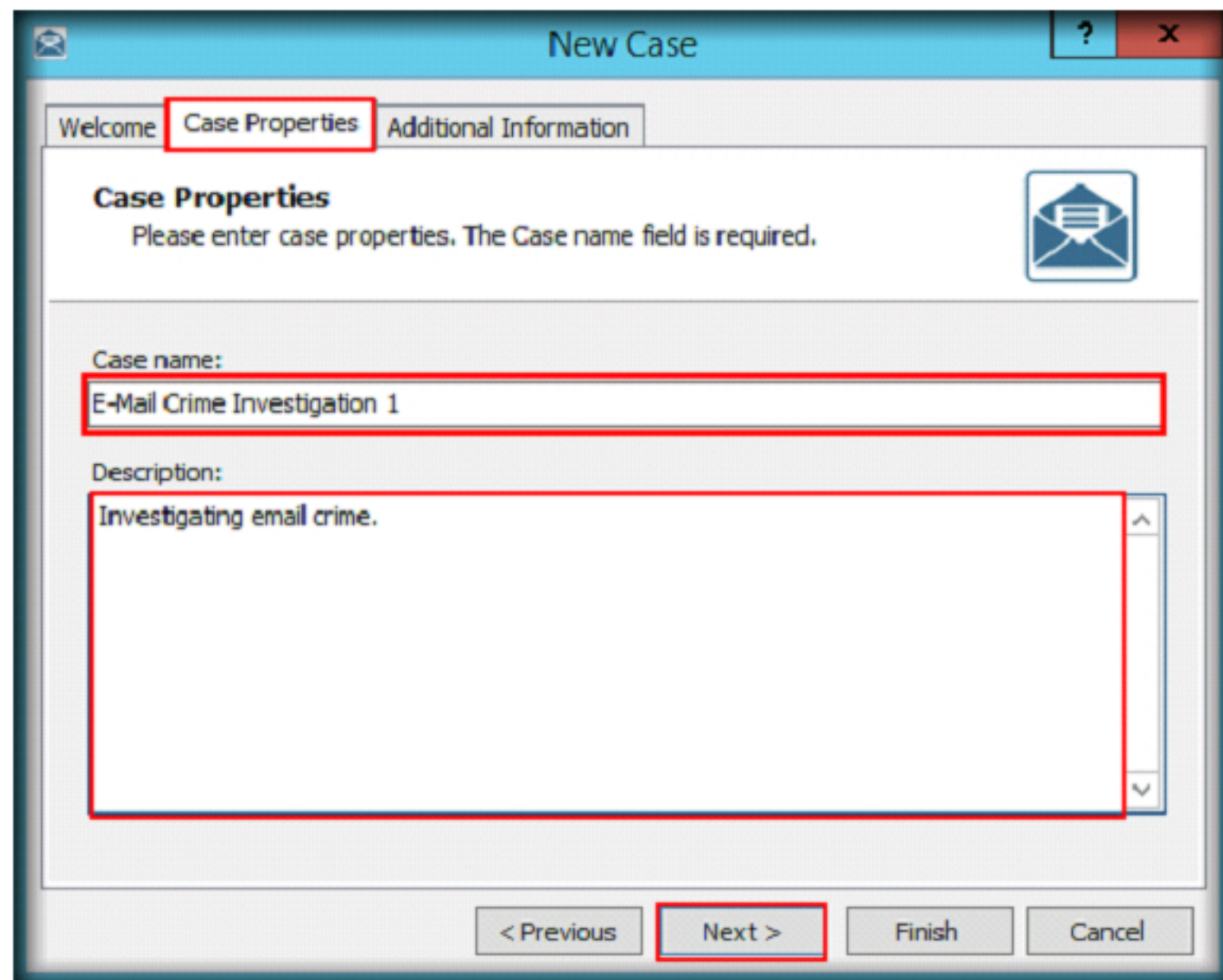


FIGURE 2.4: Case Properties tab

11. On the **Additional Information** tab, fill all the fields and click the **Finish** button.

Paraben's Email Examiner v6.8 works with Unicode encodings (UTF-8).

FIGURE 2.5: Additional Information tab

12. After clicking **Finish**, a **New case creation** window appears. Select the desired path where you want to save the new case and then, click **Save**. In this lab, we are choosing Desktop to save the file.

FIGURE 2.6: New case creation window

TASK 3

Adding New Evidence to a Case

13. It will save the case and launch the **Add New Evidence** window. In this window, select the desired **Source type** from the left pane and then click **OK**.
14. In this lab, we are choosing **MS Outlook database** as **Source type**.

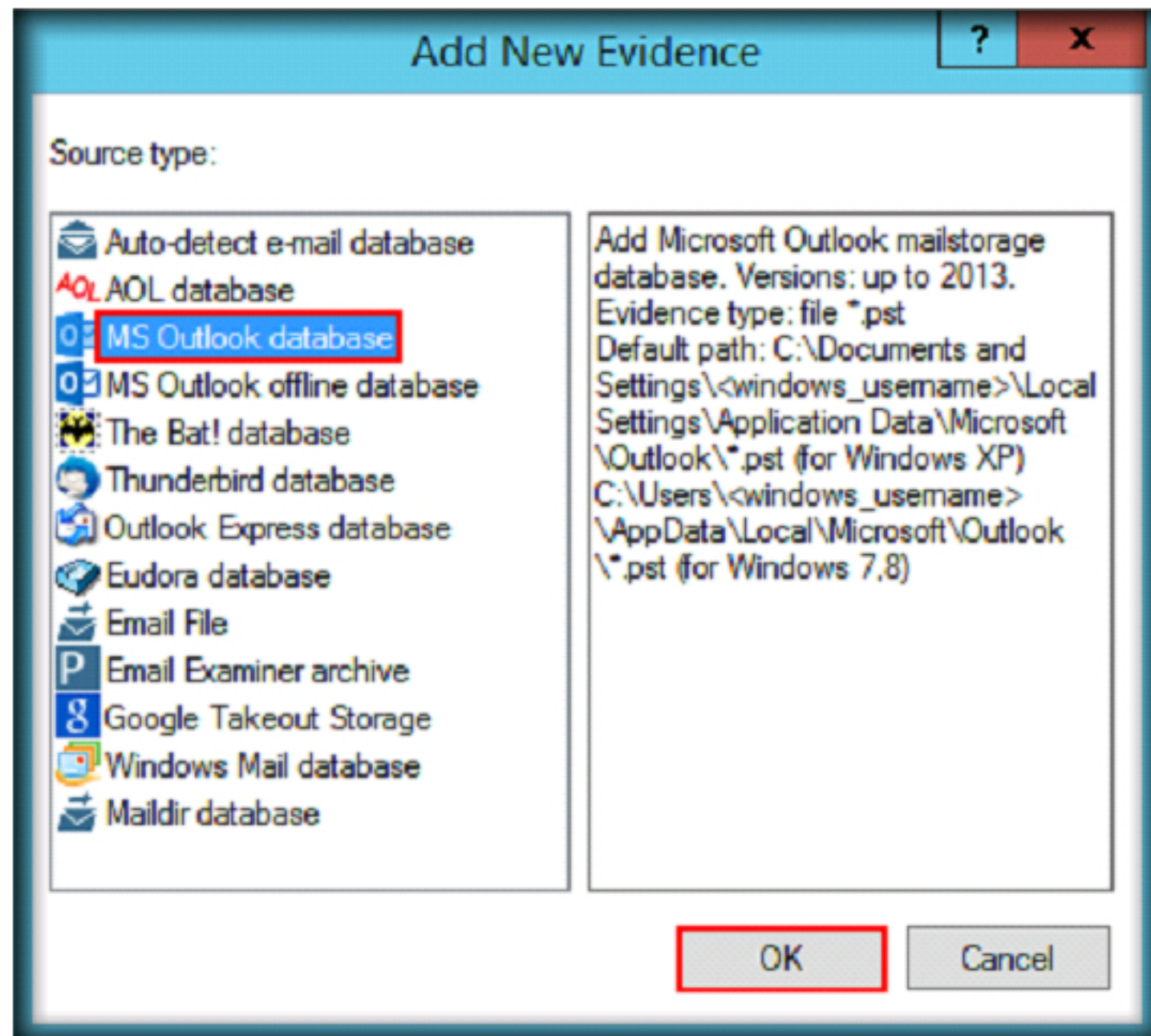


FIGURE 2.7: Add New Evidence window

15. **Open** window appears, navigate to **C:\CHFI-Tools\Evidence Files\Outlook Files\Outlook .pst files**, select the target source file **target 1.pst** and click **Open**.

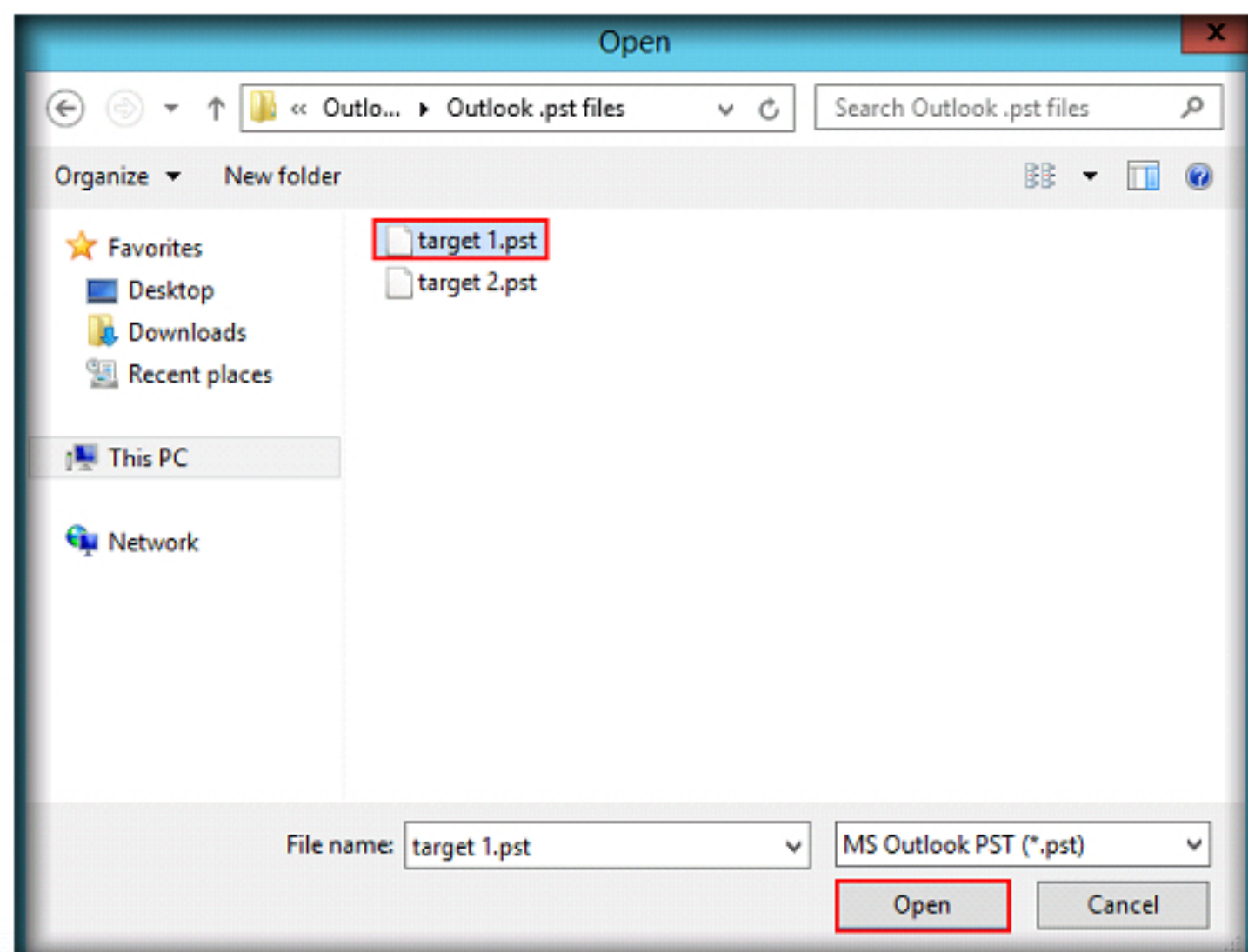


FIGURE 2.8: Browsing evidence file

16. A pop-up window appears, type the evidence name or leave default and click **OK**.

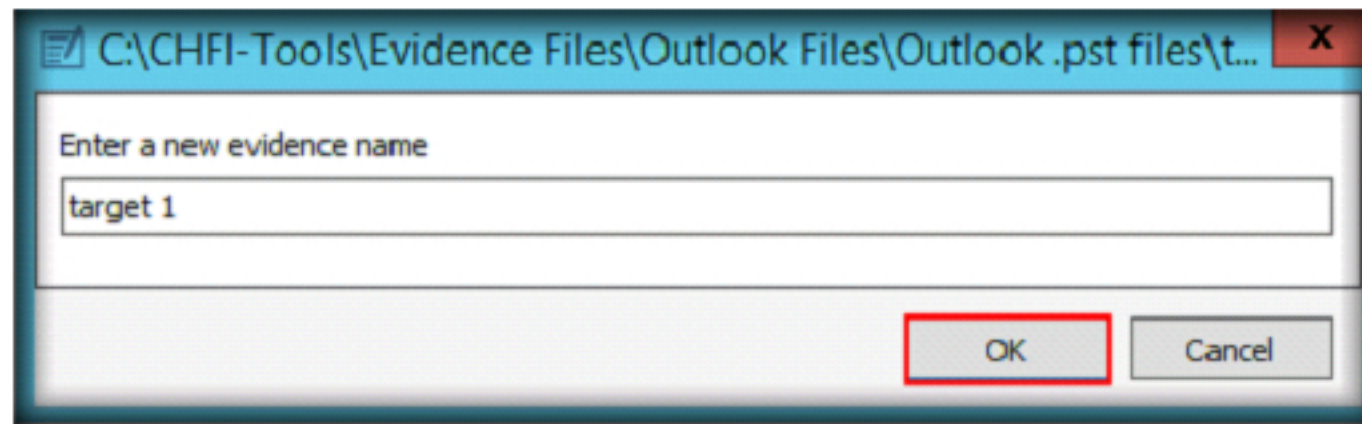


FIGURE 2.9: Naming evidence

17. Set the **MS Outlook Database Settings**. There are two options:
 - **Raw Mode:** Select this option to display all database content including system, orphaned, and deleted items.
 - **Scan database for deleted messages (slows down opening):** Select this option to find and recover deleted messages in the database. This can take longer time.

Here we are selecting **Scan database for deleted messages (slows down opening)**. After selecting the desired mode, click **OK**.

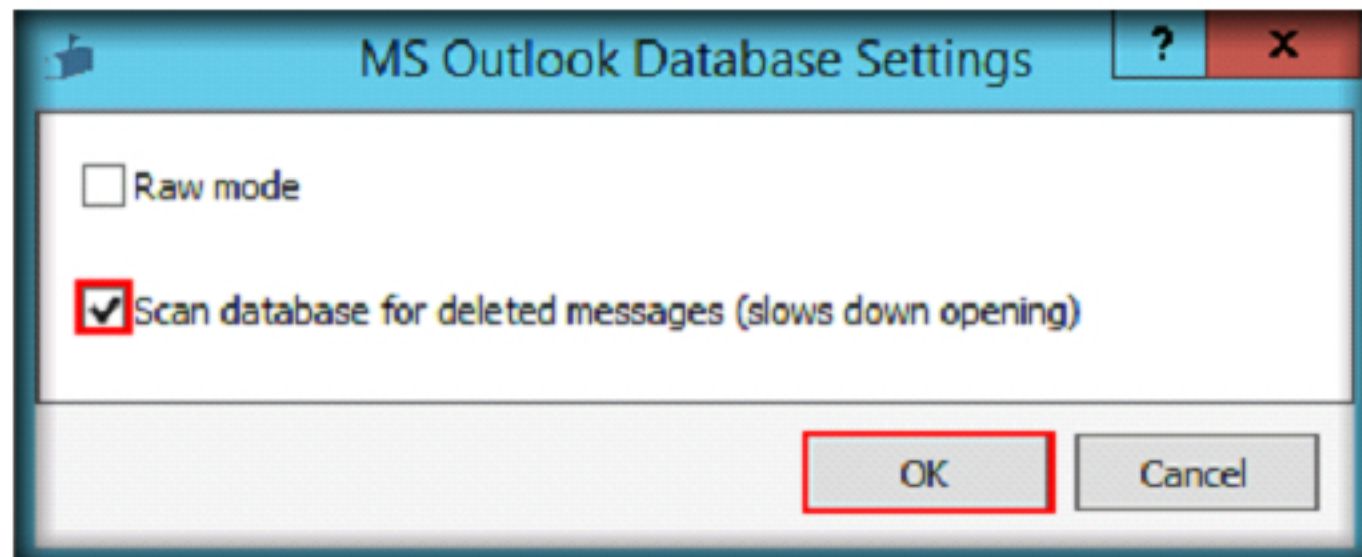


FIGURE 2.10: Database Settings options

Sort attachments by file type.

18. **Paraben's EMX Content Analysis Wizard** appears, displaying **General Options** section.
19. In this section, check all the options, and click **Next**.

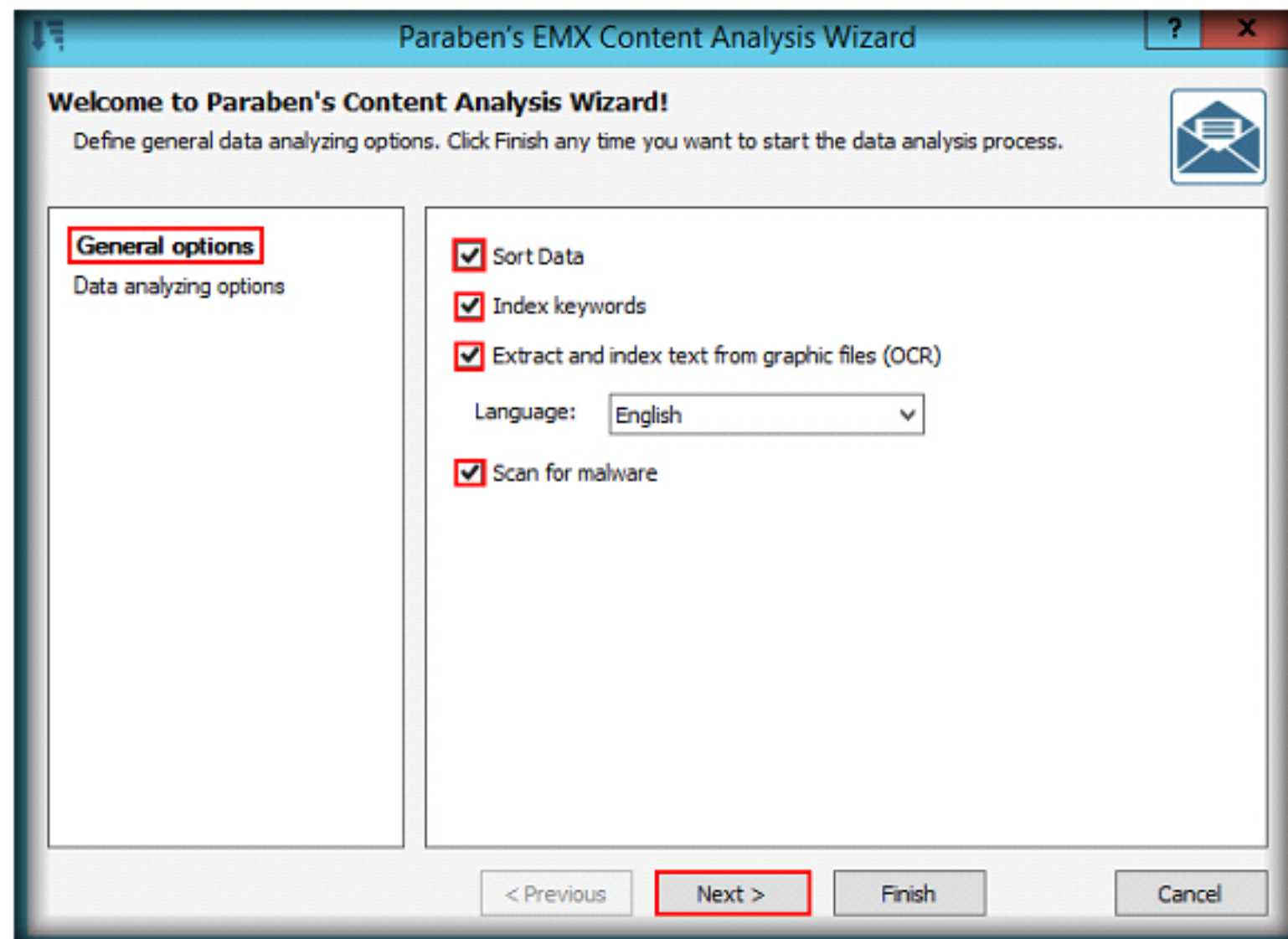


FIGURE 2.11: General options section

20. In **Data analyzing options** section, leave the settings to default and click **Finish**.

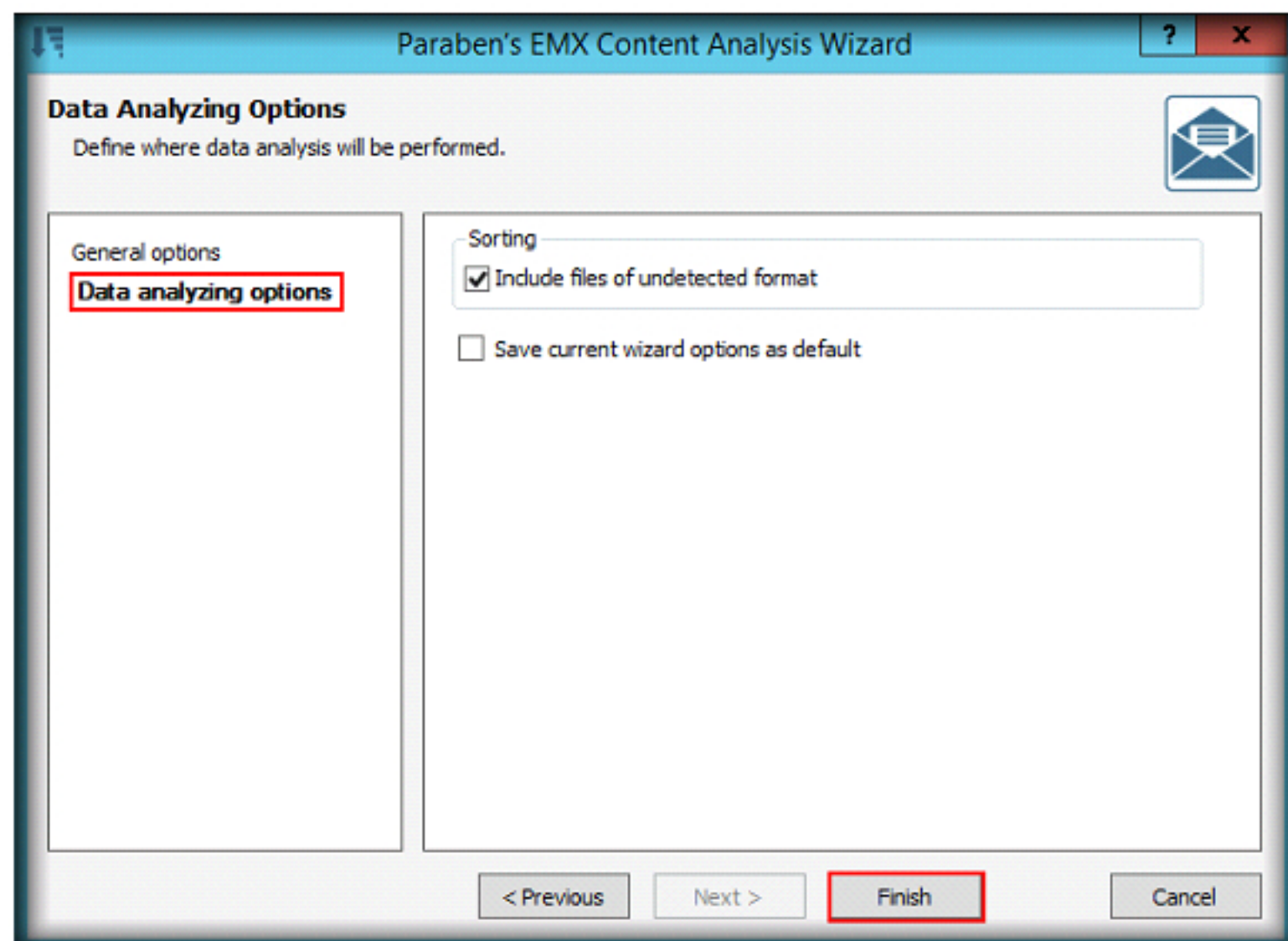


FIGURE 2.12: Data analyzing options section

21. After analyzing the added evidence file, Paraben's Email Examiner Case Content is displayed as shown in the screenshot:

Export mail storage contents to EML, EMX, PST, MHTML, and MSG formats.

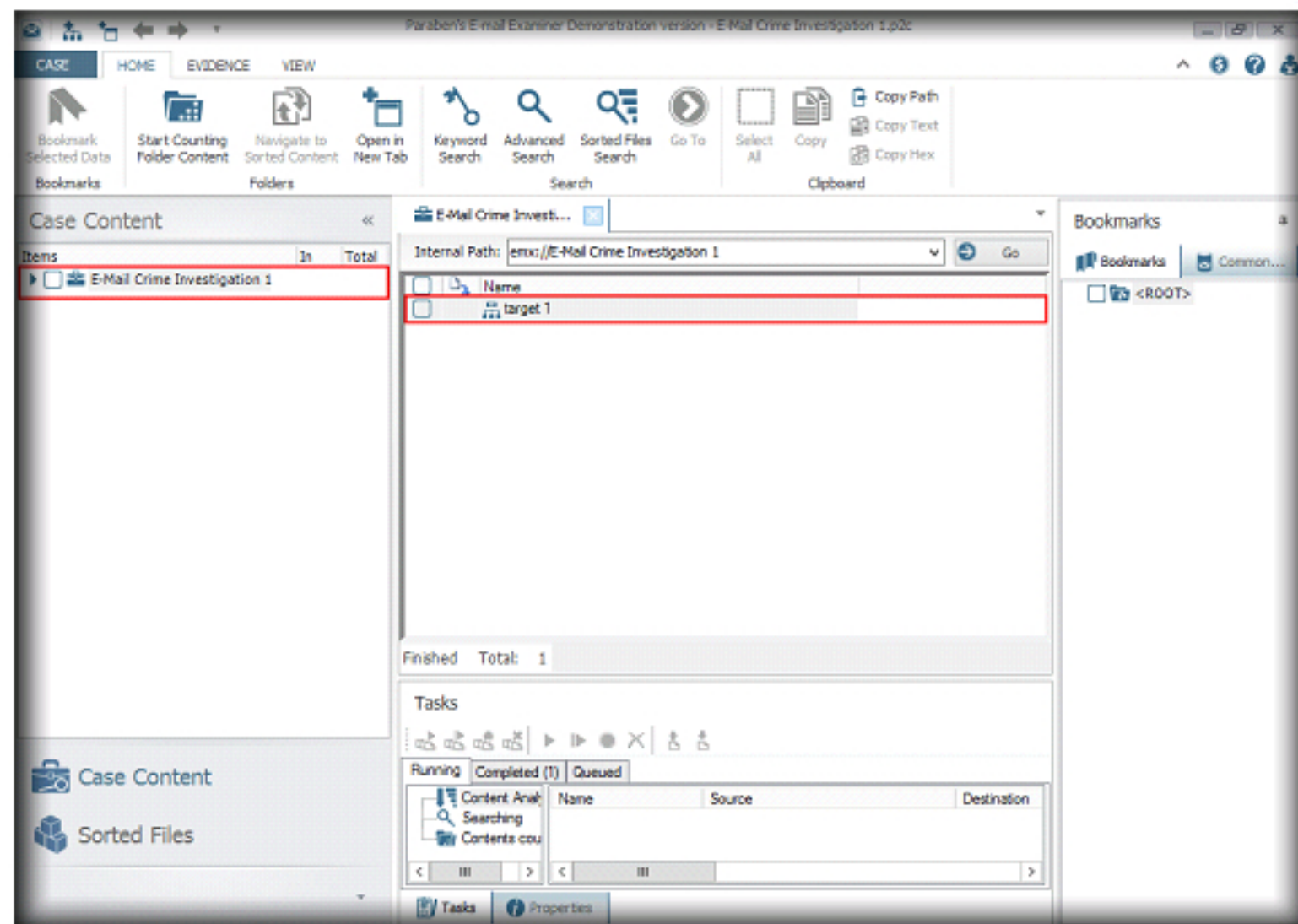


FIGURE 2.13: Email Examiner with evidence added

TASK 4

Investigating Outlook Mail storage

22. The email storage structure is displayed in the **Case Content** pane (to the left); messages stored in the mailbox are displayed in the **Data Viewer** pane (to the middle). To view the recovered files that have been deleted, expand **E-Mail Crime Investigation** → **target 1** → **Outlook Personal Storage** and select **Top of Outlook data file**.

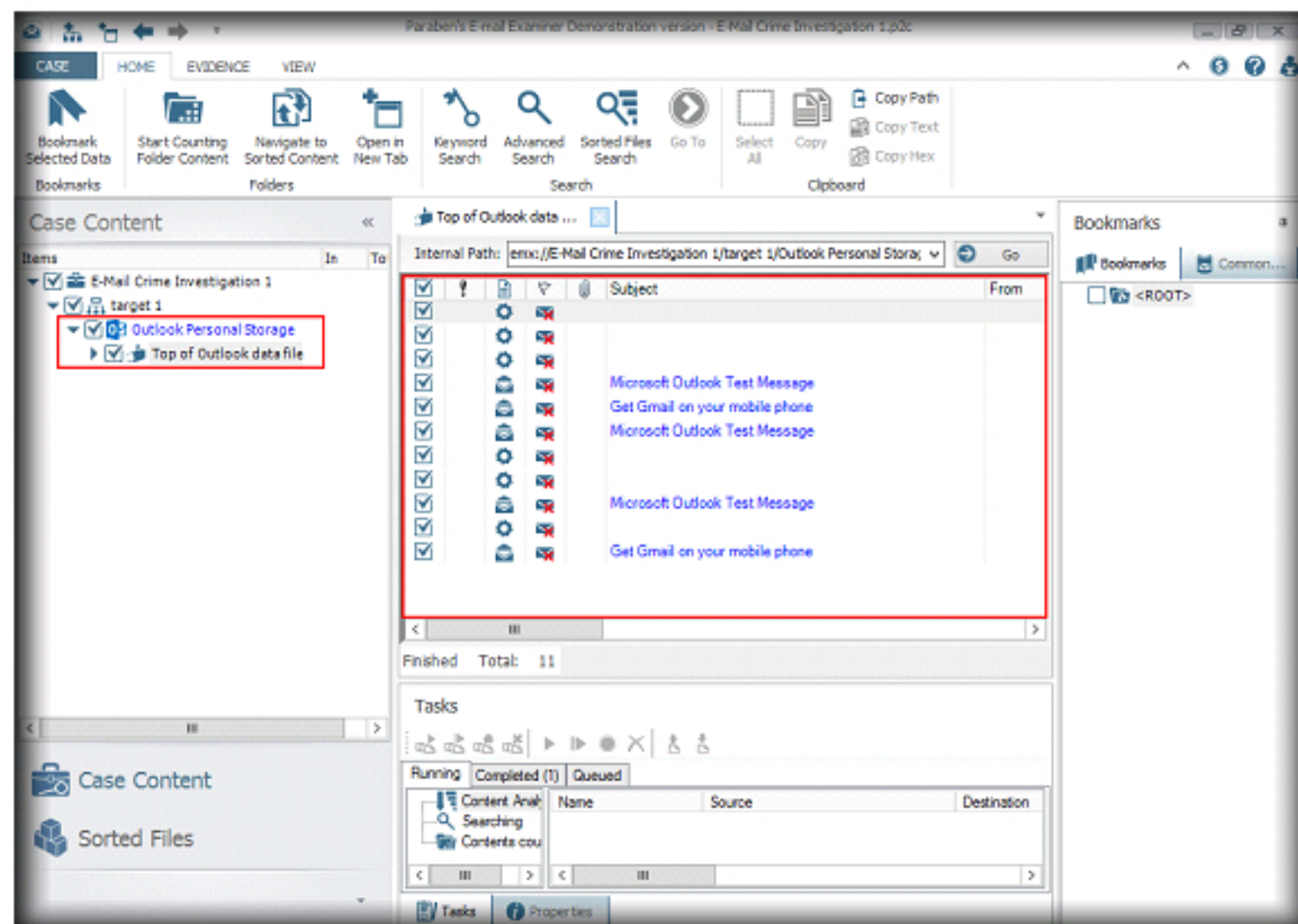


FIGURE 2.14: Email Examiner showing recovered emails

23. Select any message, and click **Properties** tab in E-mail Data section, to view properties of the email in the **General** tab as shown in the screenshot:

It supports advanced reporting (HTML, CSV, and Text).

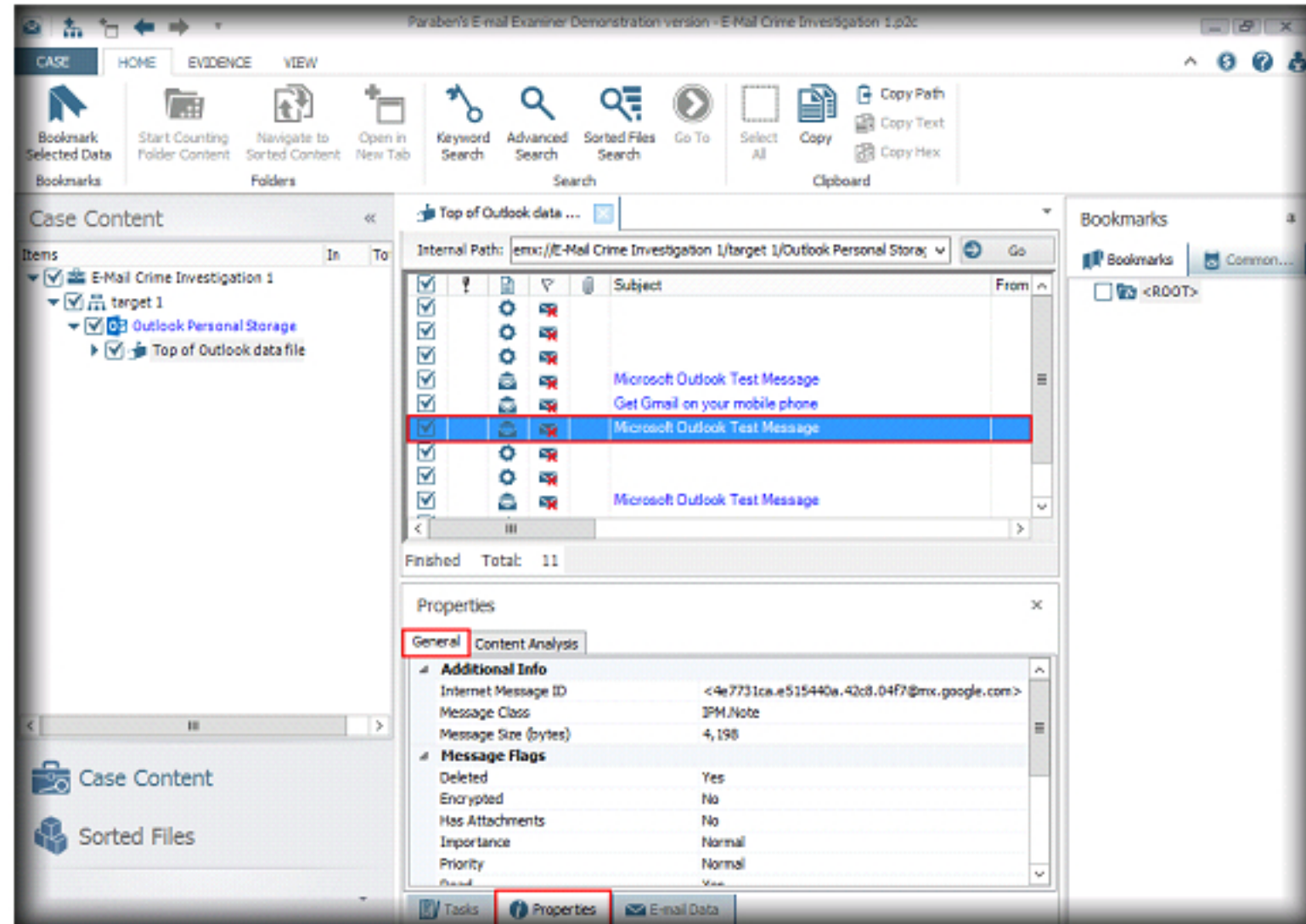


FIGURE 2.15: Figure showing Properties section

24. Now, click **Content Analysis** tab in Properties section to view the analyzed content of the deleted email:

Email Examiner allows batch search and export without adding mail storages as evidence to EMX.

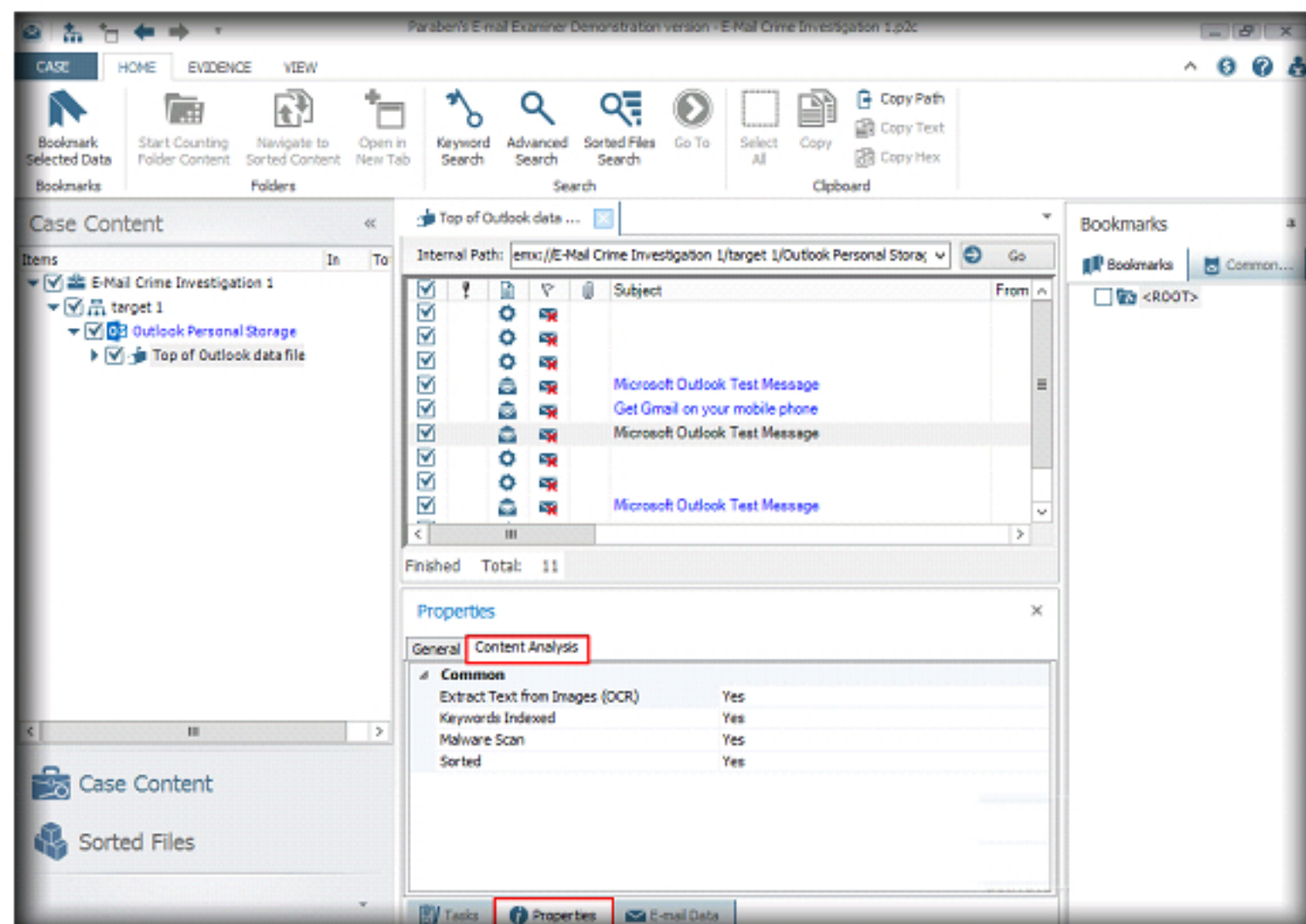


FIGURE 2.16: Figure showing Content Analysis tab in Properties section

25. Select the message in the **Data Viewer** pane and click **E-mail Data** pane (in the bottom of the window).

Note: As Paraben's E-mail Examiner is evaluation version, few options are disabled. Thus it is unable to show the email content.

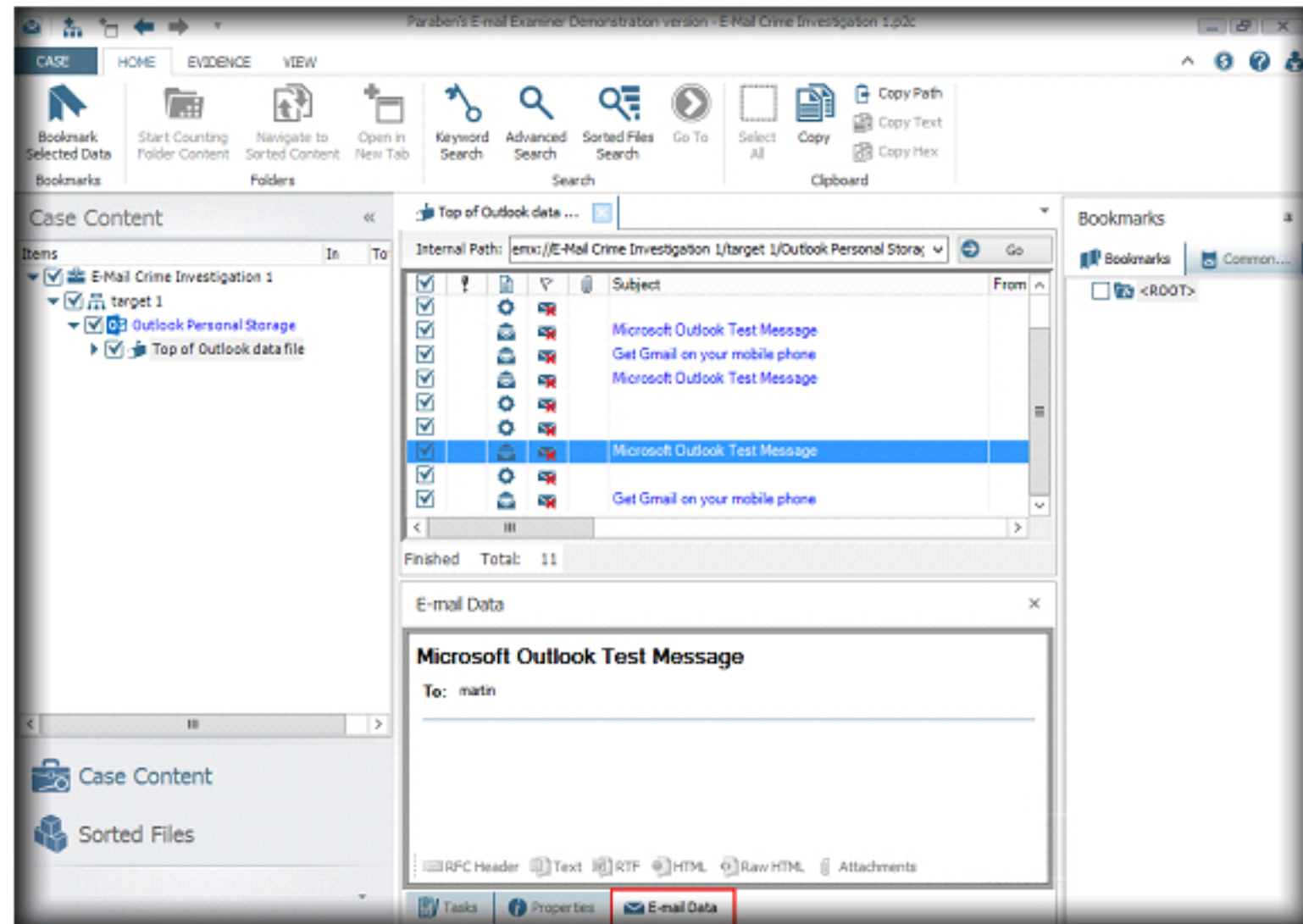


FIGURE 2.17: E-mail Data section showing selected message contents

26. You can view the contents of the selected message in five formats: RFC header, Text, RTF, HTML, Raw HTML, and Attachments. To view the message in the required format, click the corresponding tab on the bottom of the **E-mail Data** pane.
27. Messages with attachments (files attached to them) have a special symbol in the corresponding column. For such messages, the **Attachments** tab in the **E-mail Data Viewer** pane is enabled. Click the **Attachments** tab on the bottom of the **E-mail Data** pane to view attached files. Attachments are displayed in Hex, Text, and File viewers if they are enabled.

Note: The trial version of the tool will not allow you save the recovered messages and Generate Reports. You need to buy the product activation key from the vendor to save the files.

Lab Analysis

Analyze the generated report and document the results related to the lab exercise. Give your expert opinion on the target's email crime investigation.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Tracing an Email Using the eMailTrackerPro Tool

The eMailTrackerPro tool analyzes email headers to disclose the primary sender's location.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Naomi has registered a case with FBI about a person threatening her through emails. The investigators have taken up the case and gather her account details to trace the emails back. They are planning to use the eMailTrackerPro tool to trace the culprit.

To be an expert **forensic investigator**, you should be familiar with email headers and their related details. You must be able to track any email.

Lab Objectives

The objective of this lab is to demonstrate email tracing using eMailTrackerPro. Forensic investigators will learn how to:

- Trace an email to its true geographical source
- Collect Network (ISP) and Domain Whois information for any email traced

Lab Environment

To carry out the lab, you need:

- eMailTrackerPro, located at **C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes\Email Forensics Tools\eMailTrackerPro**.
- You can also download the latest version of **eMailTrackerPro** from **<http://www.emailtrackerpro.com/download.html>**.
- If you decide to download the latest version, screenshots shown in the lab might differ.
- A computer running **Windows Server 2012**.



Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes

- Administrative privileges to run this tool.
- A valid email account (Hotmail, Gmail, Yahoo, etc.). We suggest you sign up with any of these services to obtain a new email account for this lab.

Note: Do not use your legitimate email accounts and passwords in these exercises.

Lab Duration

Time: 20 Minutes

Overview of eMailTrackerPro

Email tracking is a method to monitor or spy on email delivered to the intended recipient:

- When an email message was received and read
- If destructive email is sent
- The GPS location and map of the recipient
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages are set to expire after a specified time

Lab Tasks



TASK 1

Install and Launch eMailTrackerPro

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 12 Investigating Email Crimes\Email Forensics Tools\eMailTrackerPro**
2. Double-click **emt.exe** to launch the setup and follow the wizard-driven installation instructions

Note: If an **Open File - Security Warning** pop-up appears, click **Run**

3. This tool installs Java runtime as a part of the installation

Note:

- If **Warning** message about the license expiration appears, **download** the latest version of eMailTrackerPro from **<http://www.emailtrackerpro.com/download.html>** and install it.
4. Once the installation is complete, make sure that **Run eMailTrackerPro when I click Finish** is checked and click **Finish**.

- The **eMailTrackerPro** main window displays, with **Edition Selection** pop-up. By default Advanced Edition is selected, you can choose the edition as per your requirement and click **OK** as shown in the screenshot:

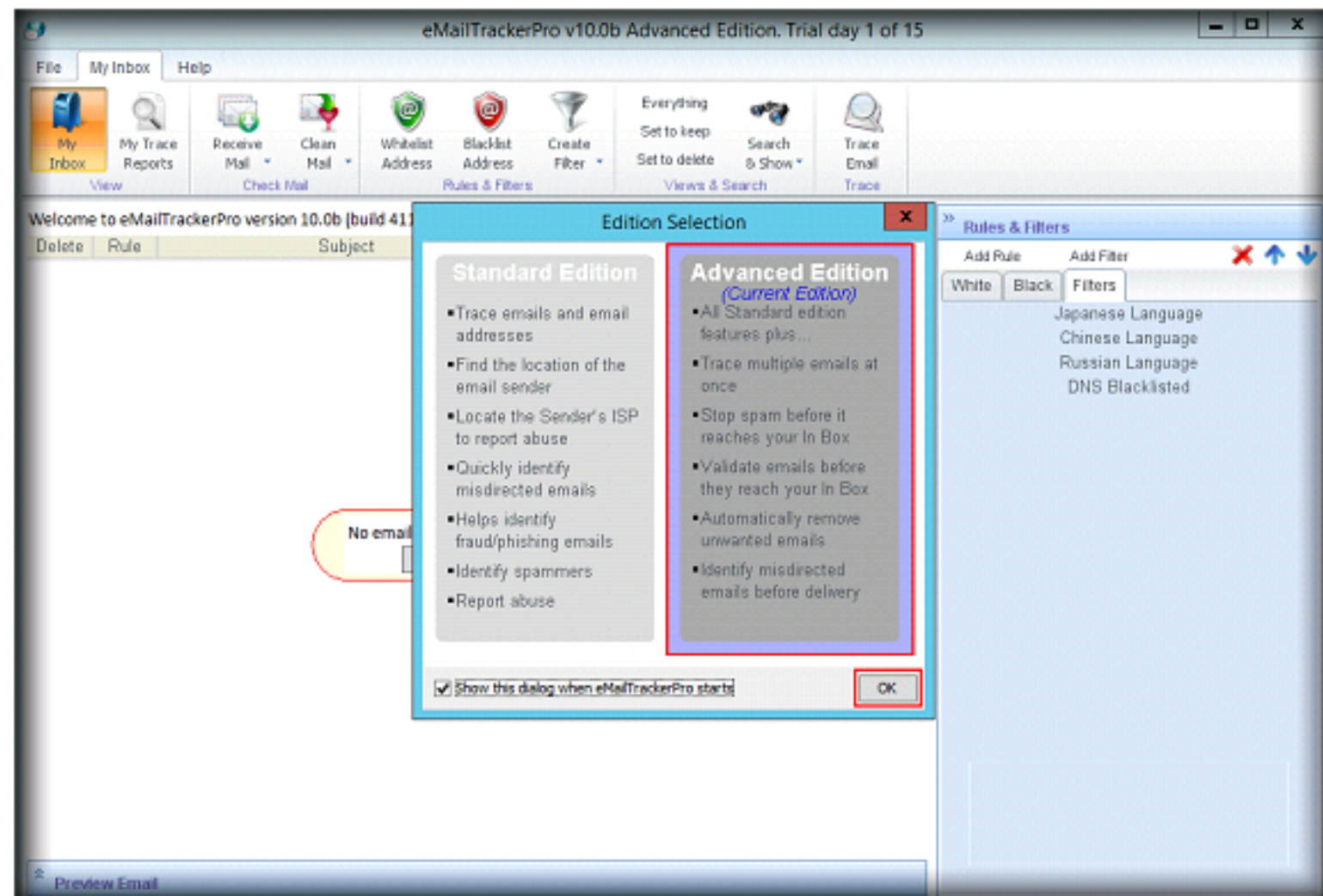


FIGURE 3.1: eMailTrackerPro main window

TASK 2

Tracing an Email

It can detect abnormalities in the email header and warn you that the email may be spam.

- Now, click **File** and then click **Trace Headers** button from the menu bar to trace the email.

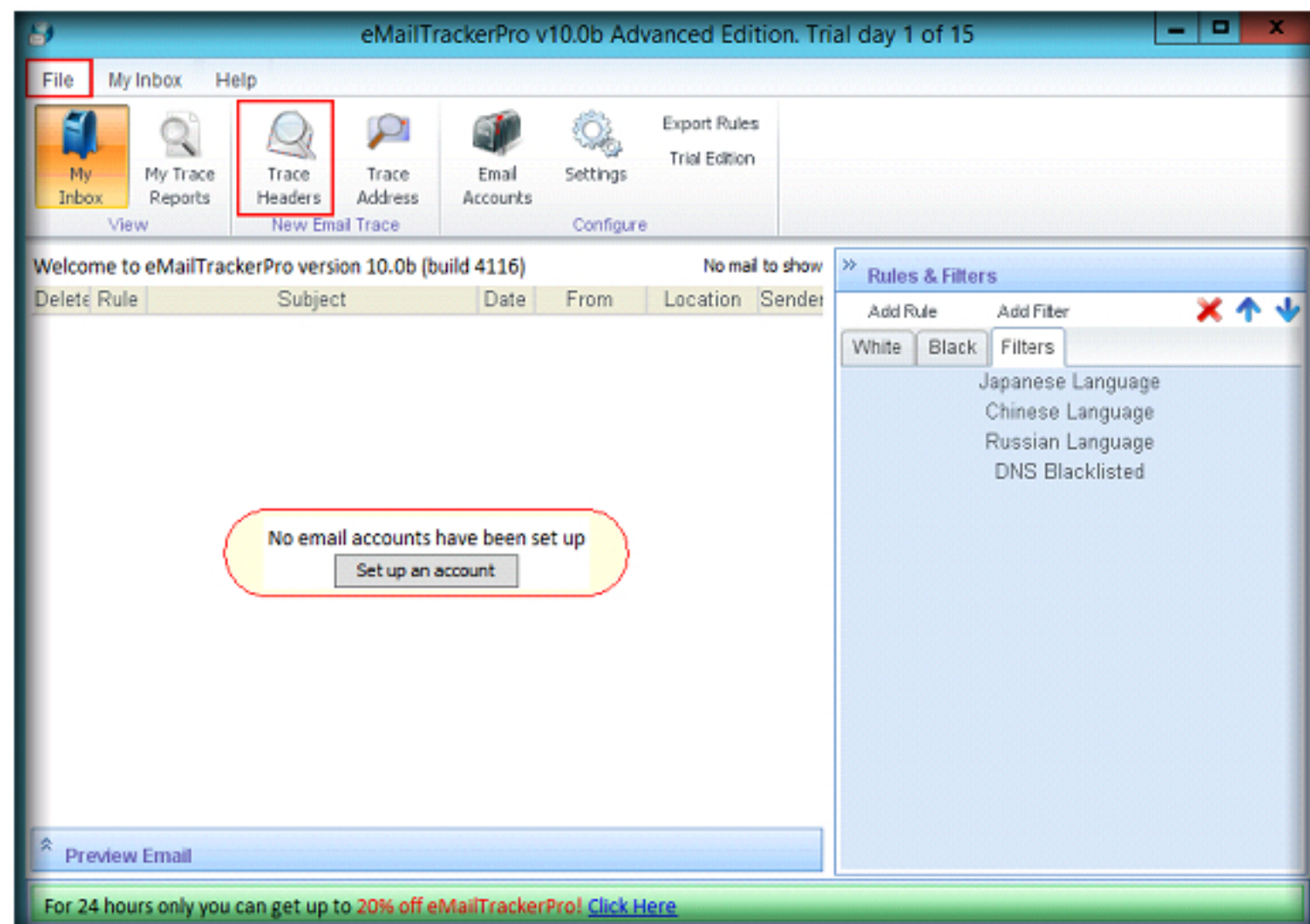


FIGURE 3.2: eMailTrackerPro options window

7. Select **Trace an Email I have received** in the **Visualware eMailTrackerPro** pop-up, and copy and paste the email header you want to trace.

It generates and sends abuse reports to the network responsible for spam and phishing email.

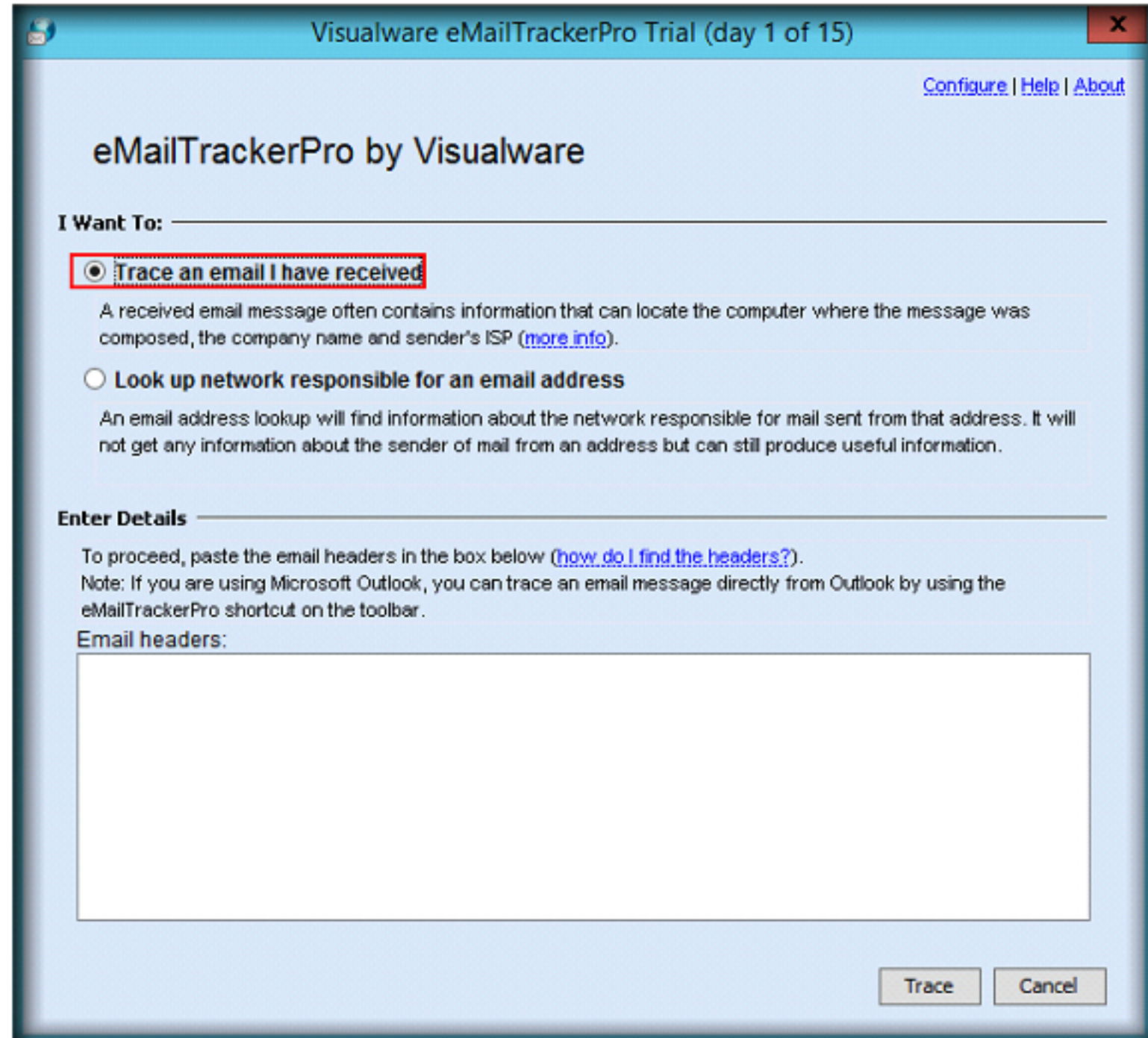


FIGURE 3.3: Tracing an email using email header

TASK 3

Finding Email Header

It gathers key information when trying to locate the sender.

8. Navigate to **C:\CHFI-Tools\Evidence Files\Outlook Files** folder and open the **Email Headers.docx** file. This file contains sample email headers.

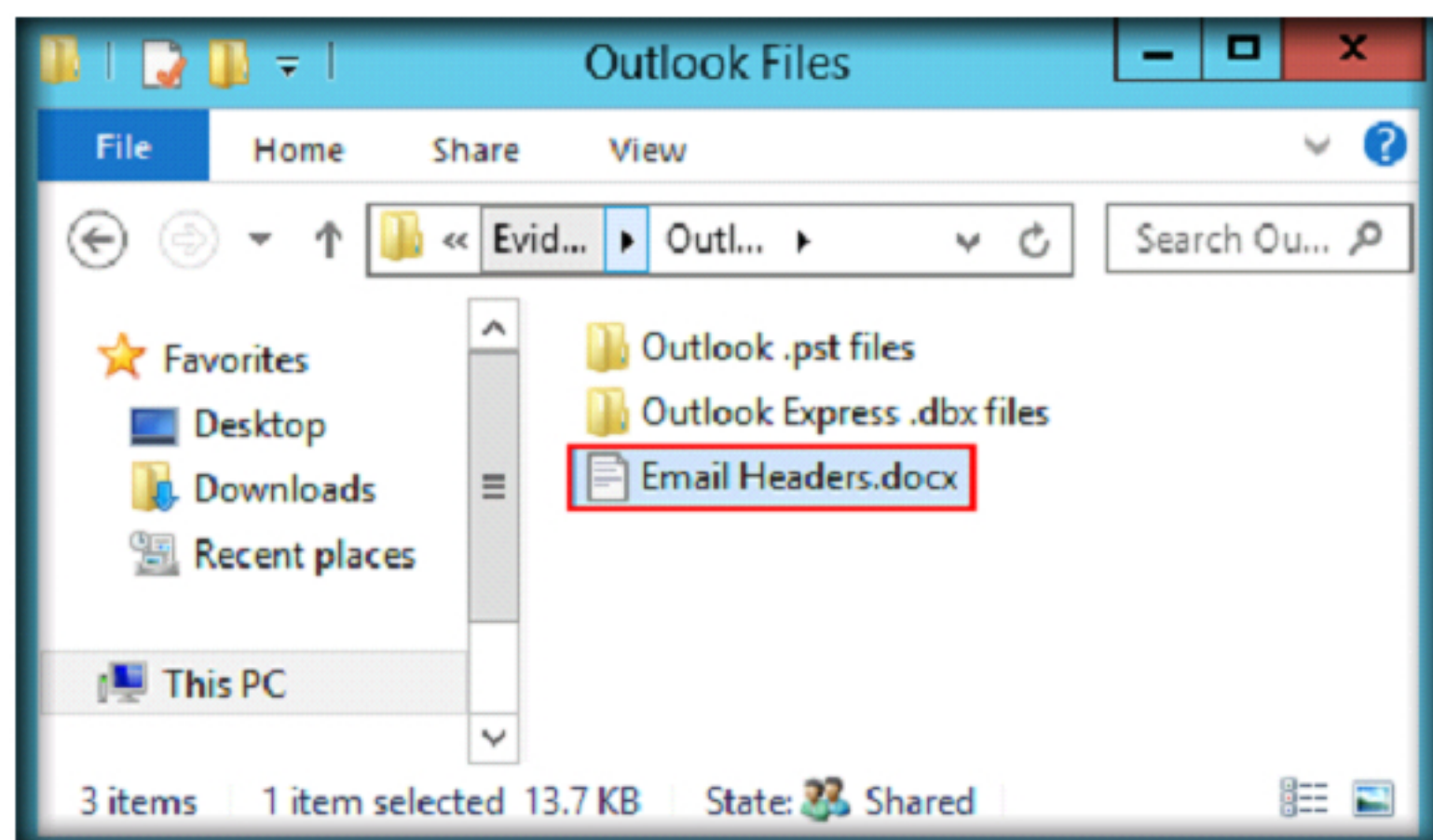


FIGURE 3.4: Evidence Files

9. Copy the content of **header 1** from **Email Headers.docx** file.

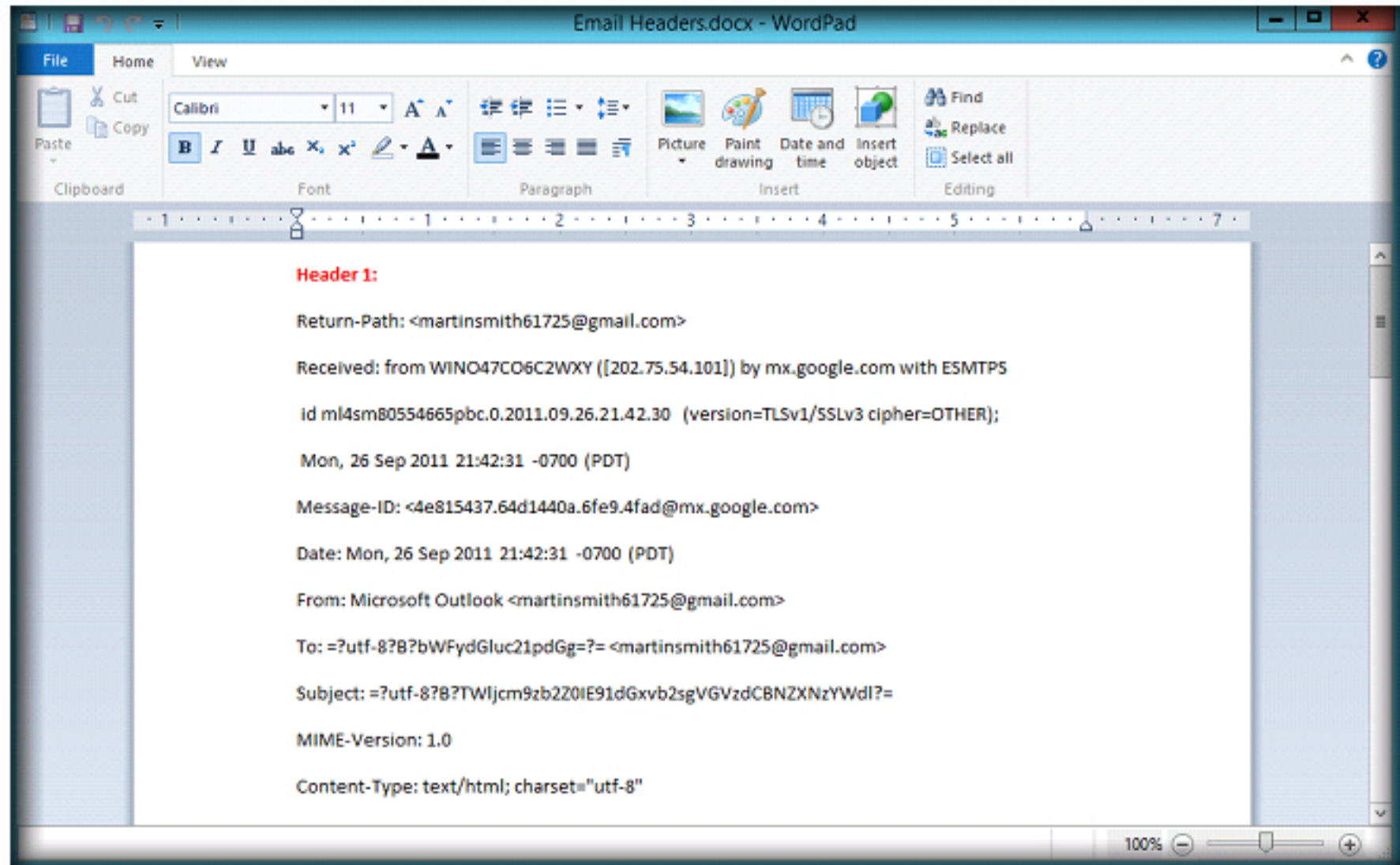


FIGURE 3.5: Figure showing contents of Email Headers.docx file

Note: The header should paste itself into the text box. If not, click inside the text box and paste the header.

TASK 4

Investigating Traced Information

Features:

- Email tracing
- Previous email trace reports
- World map/Email location
- Network Whois
- Domain Whois
- Abuse reporting
- Sender IP address
- Misdirection detection
- Spam filtering
- White and black lists
- Support for POP access
- In-depth filter system
- Language filters

10. Paste the header into the **eMailTrackerPro's** text box, and click the **Trace** button.

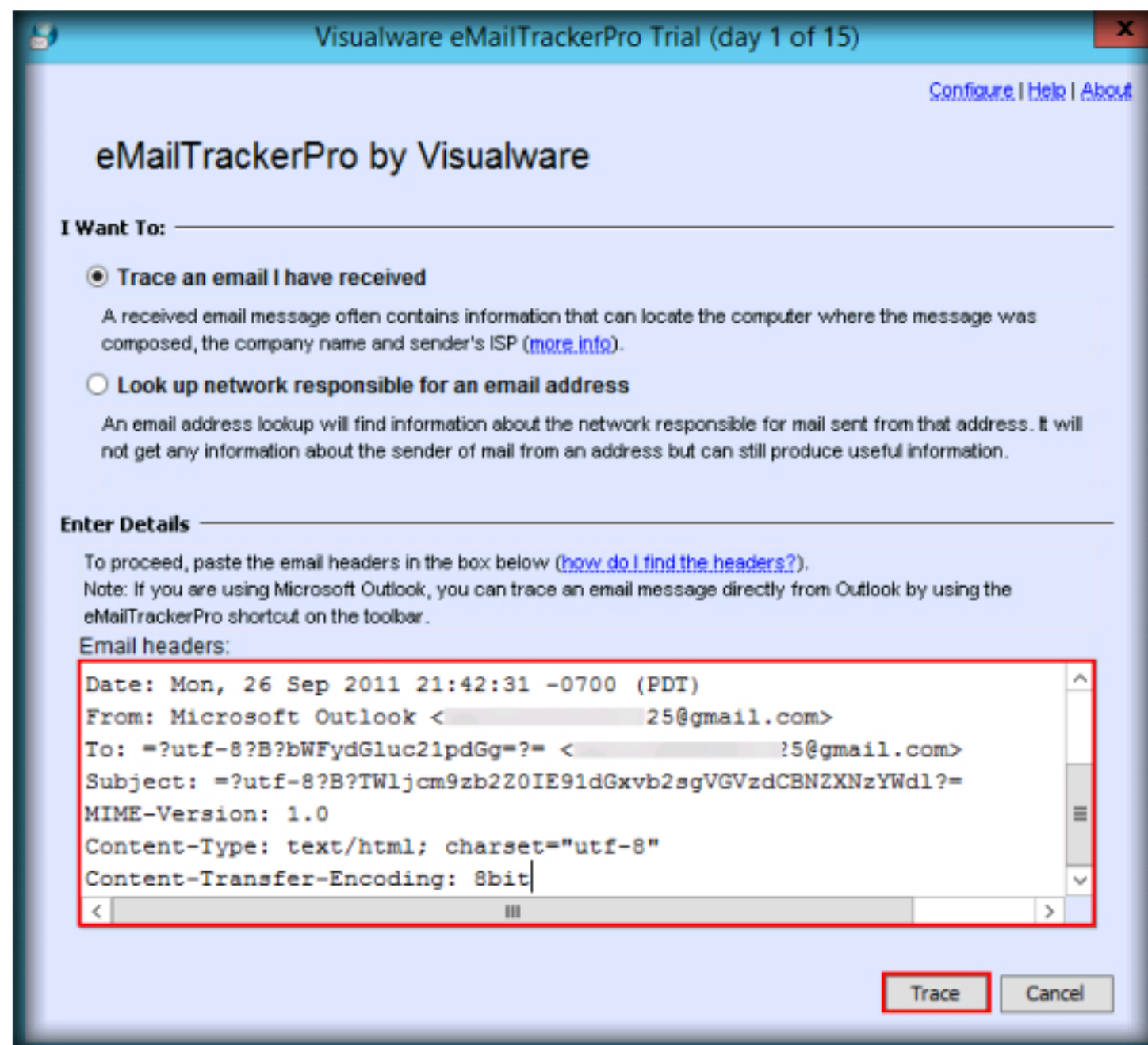



FIGURE 3.6: eMailTrackerPro with email header pasted

11. To view the trace details of an email, click **My Trace Reports** button.
12. When you click the **My Trace Reports** button, it will show the following window with **Email Summary**:

 In the future, new DNS databases can be added manually to provide even more protection.

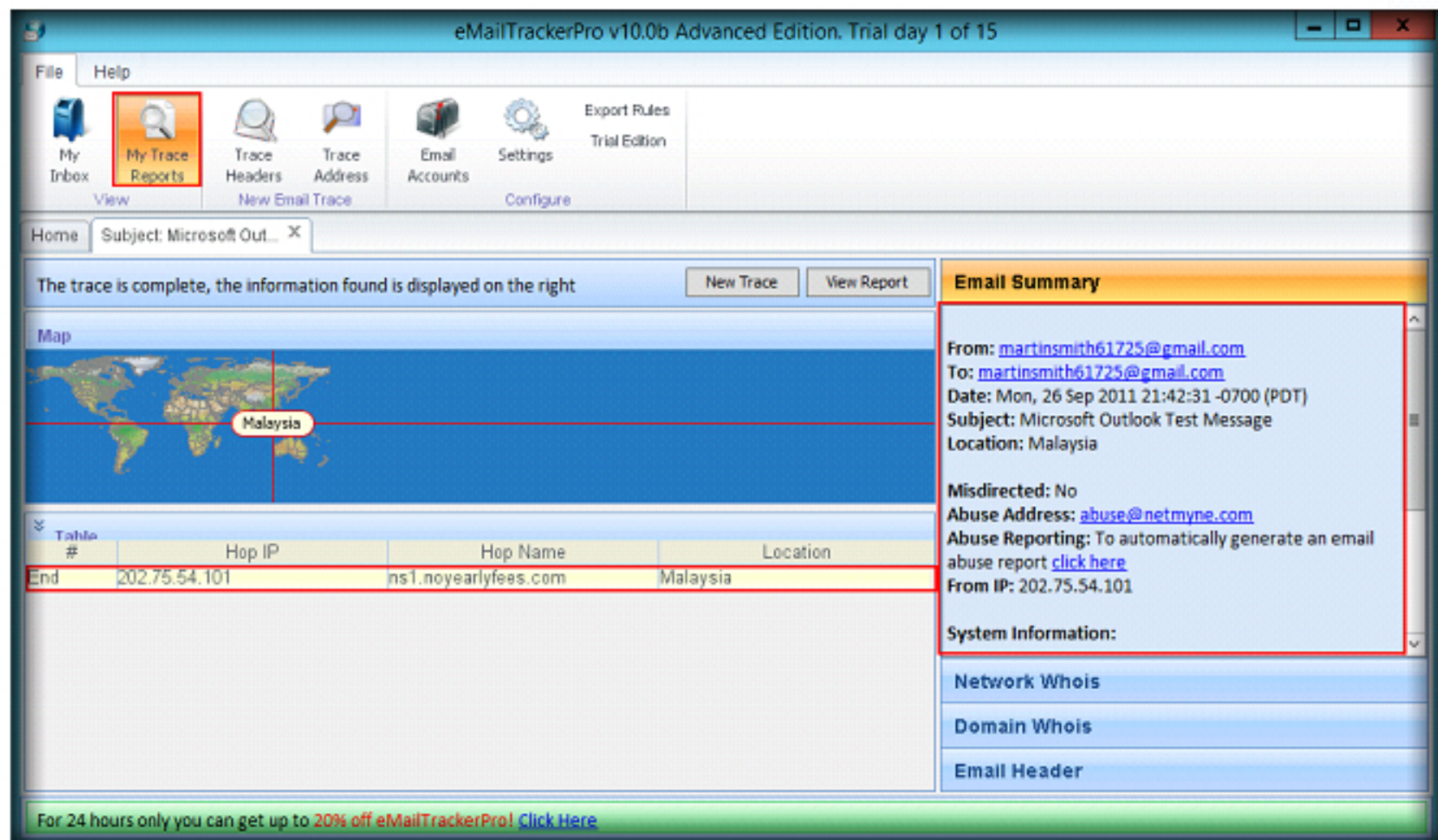



FIGURE 3.7: Trace report

13. To trace the information about the Network Whois, click the **Network Whois** button on the right side of the window. The following figure shows the Network Whois information of the target email header:

 The major feature in eMailTrackerPro is abuse reporting. Once an email is traced, eMailTrackerPro can create a report to send to the ISP behind the email.

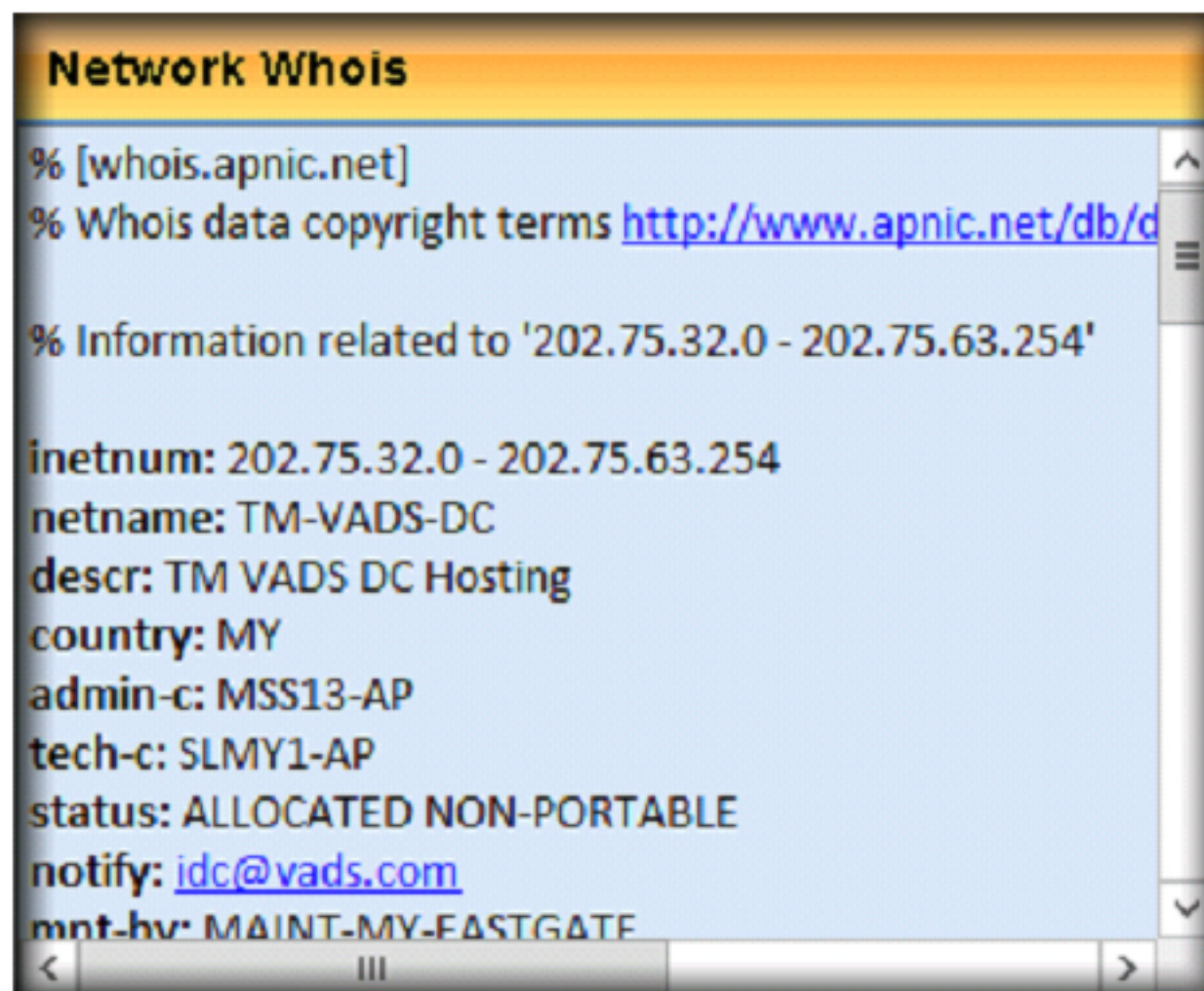


FIGURE 3.8 Network Whois pane

14. To trace the information about the Domain Whois, click the **Domain Whois** button on the right side of the window. The following figure shows the Domain Whois information of the target email header:

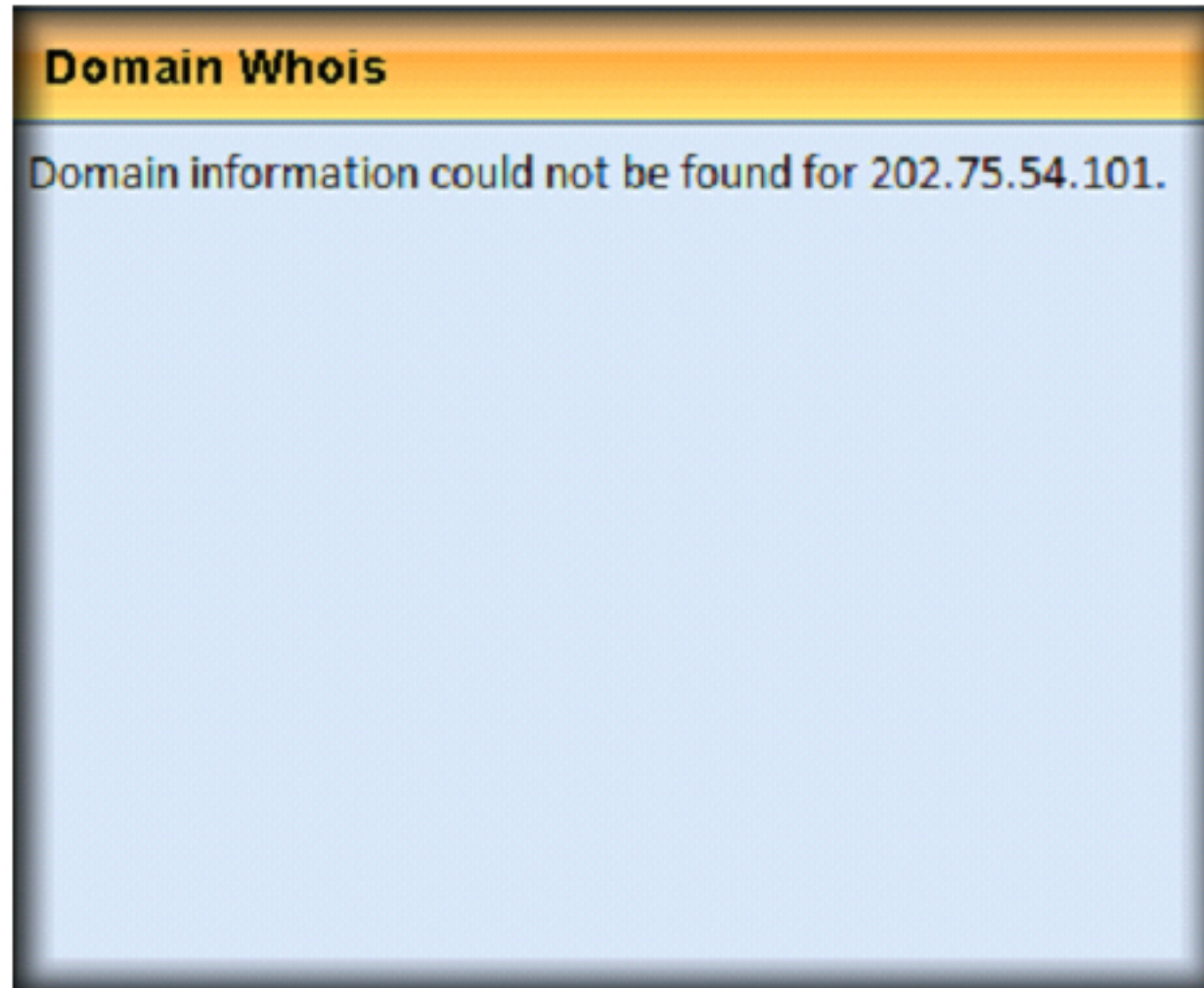


FIGURE 3.9: Domain Whois pane

15. Click the **Home** tab to view Trace Information of an email as shown in the screenshot:

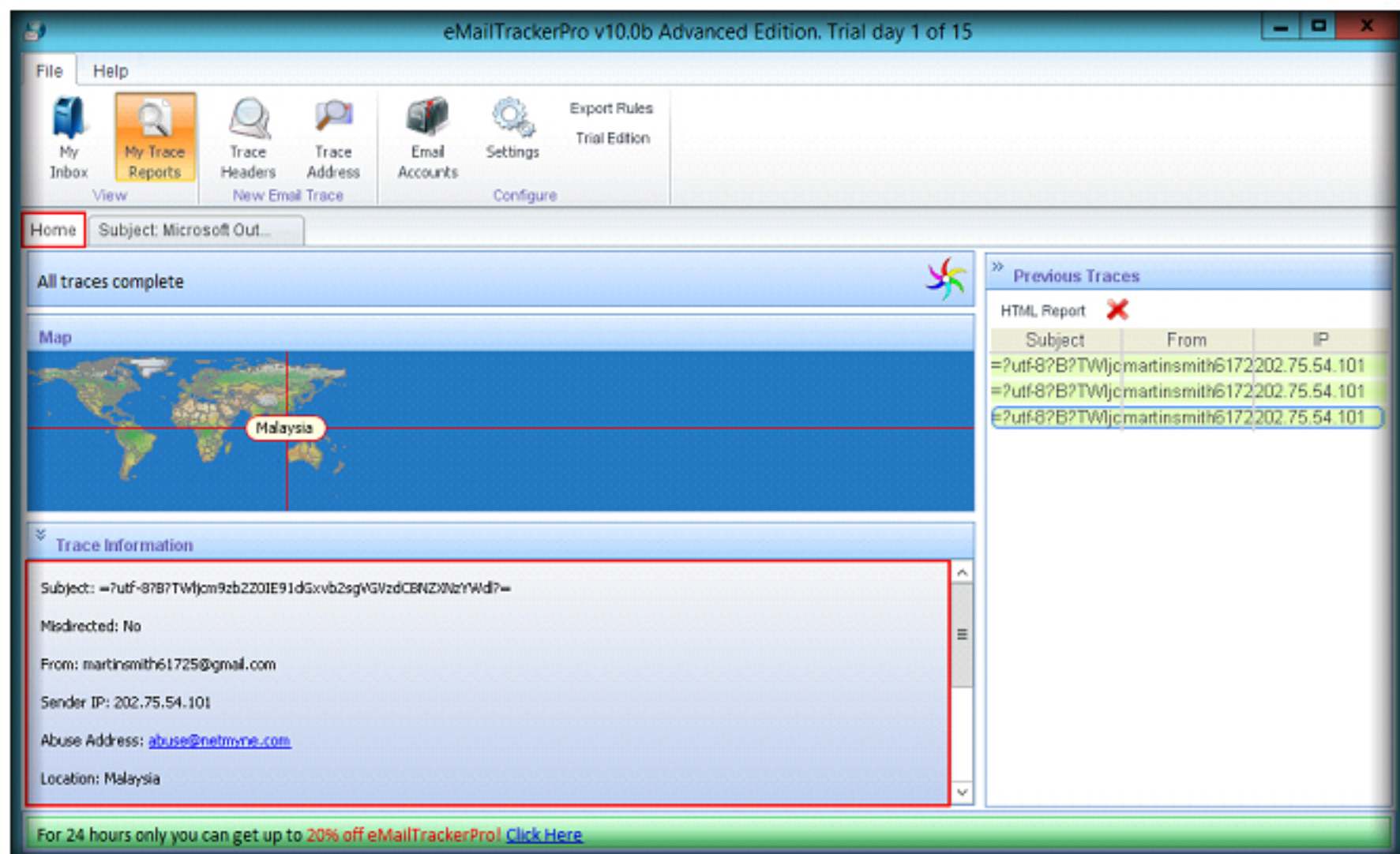


FIGURE 3.10: Figure showing Trace Information

Tracking an email is useful for identifying the company and network providing service for the address.

Each email message includes an Internet header with valuable information. eMailTrackerPro analyzes the message header and reports the IP address of the computer where the message originated, its estimated location, the individual or organization the IP address is registered to, the network provider, and additional information as available.

16. Click the **Trace Address** button in the **File** menu section from the menu bar to track an email address.

The abuse report option from the My Trace Reports window automatically launches a browser window with the abuse report included.

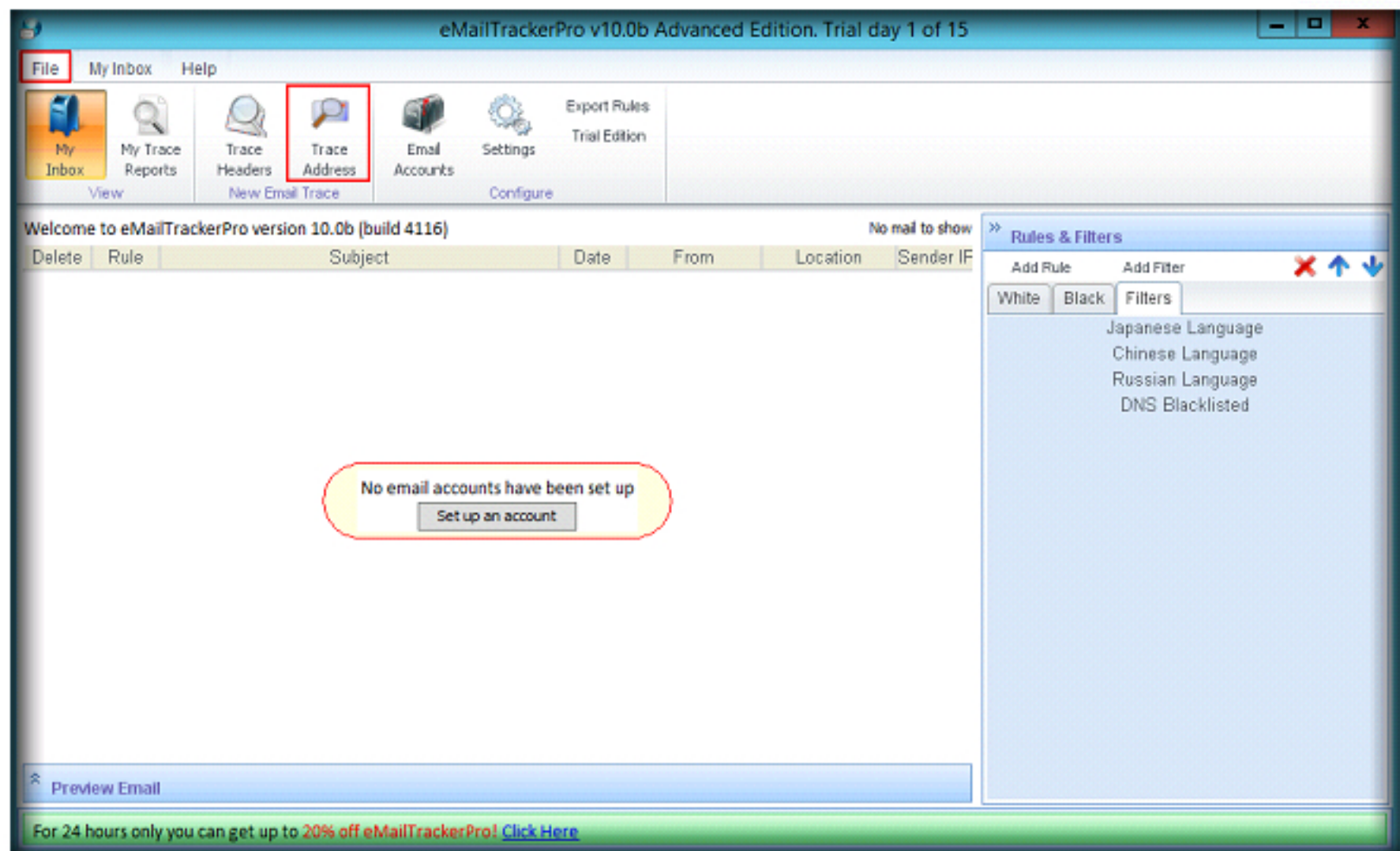


FIGURE 3.11: Figure showing Trace Address option

17. Select **Look up network responsible for an email address** radio button, type an email address in the **Enter address** field, and click **Trace**.

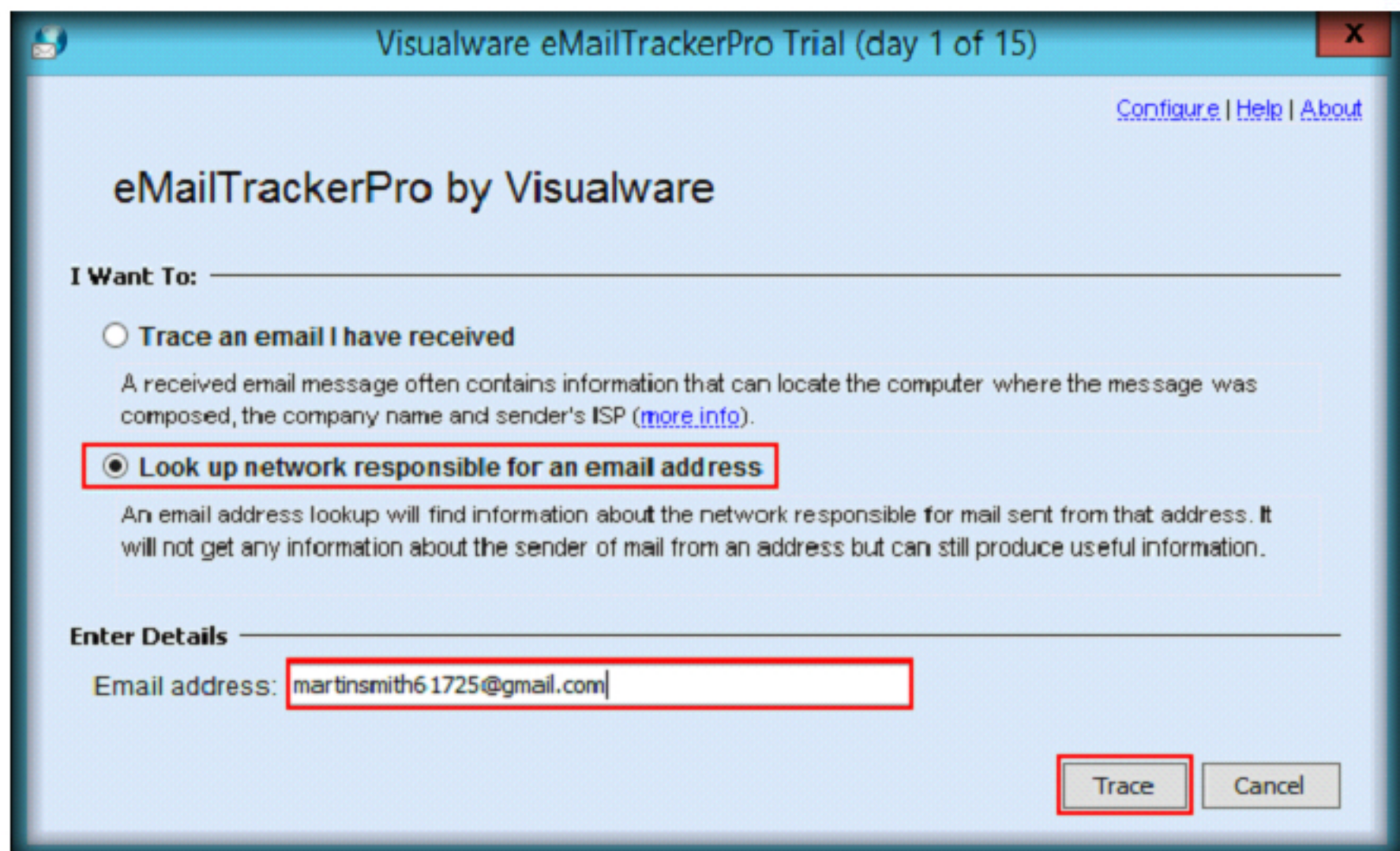



FIGURE 3.12: Tracing an email using an email address

TASK 5

Looking up Network Responsible for an Email Address

18. Now, click **My Trace Reports** button to view email address trace. Each new trace opens in a new tab in the main window of **eMailTrackerPro**.

 This tool also uncovers common SPAM tactics.

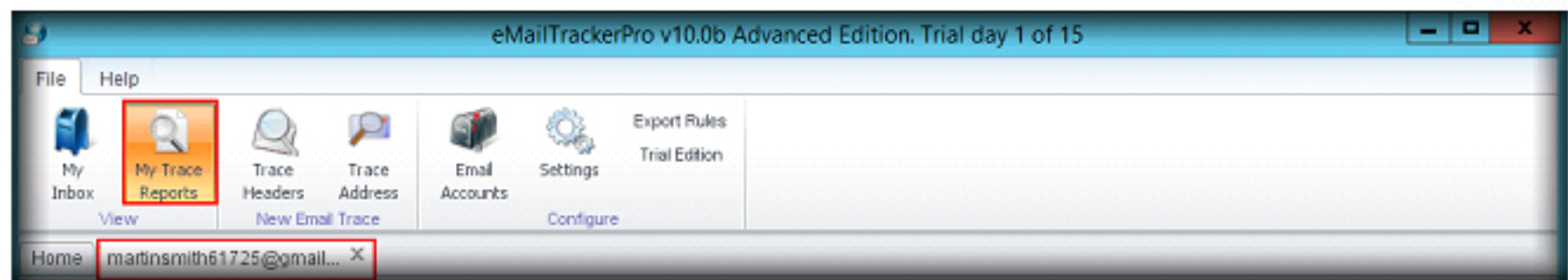



FIGURE 3.13: eMailTrackerPro showing the entered mail address

19. The **eMailTrackerPro** tool will display the trace results.

 The filter system in eMailTrackerPro allows you to create custom filters to match your incoming mail.

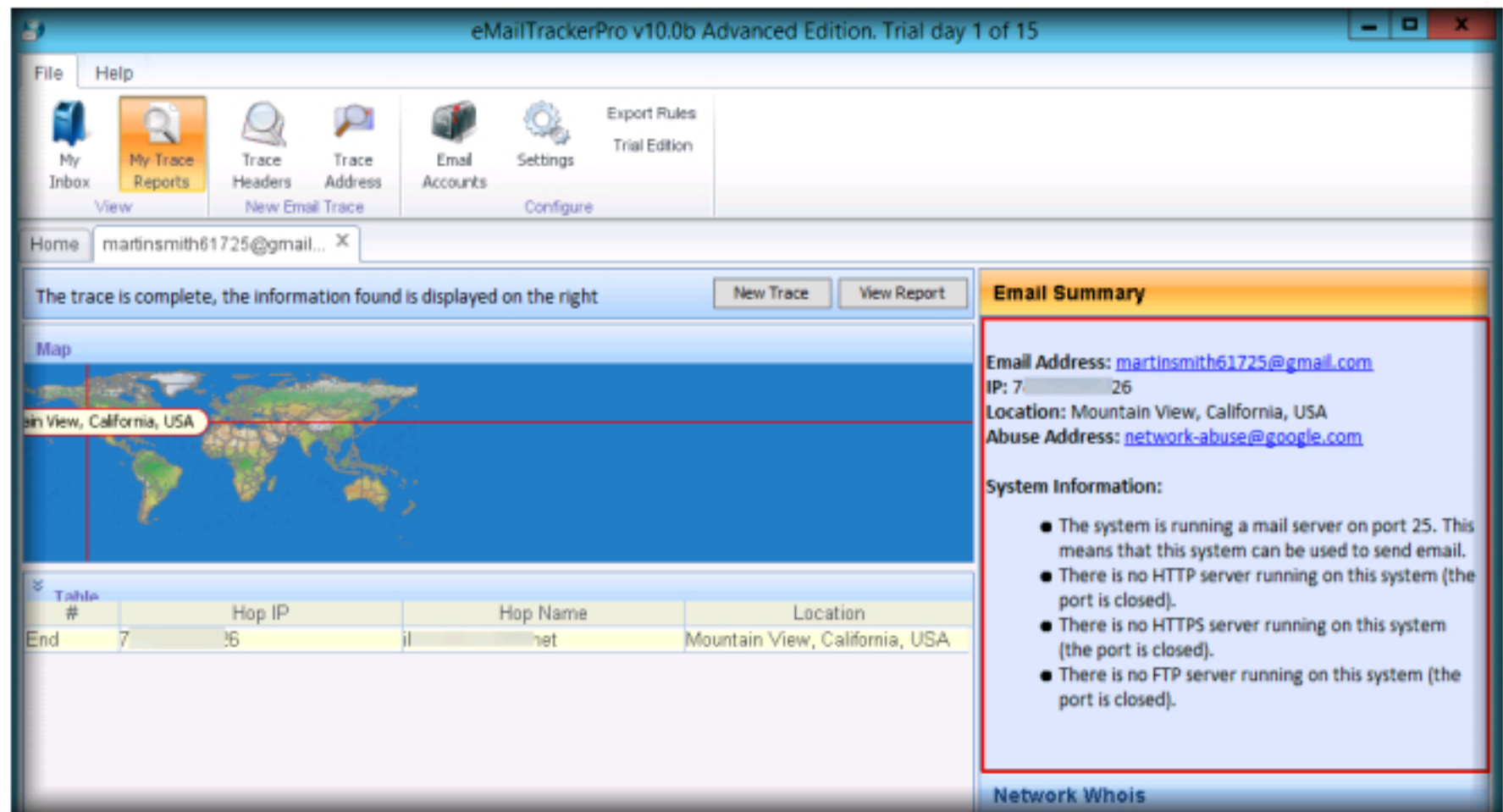


FIGURE 3.14: eMailTrackerPro displaying trace results

20. The email can be traced even if the email headers are unknown. To trace an email, click **My Inbox** and click **Setup an account** to add an account in eMailTrackerPro.

Note: If no email account has been set up, then you need to set up one. Click the **Setup an account** button.

TASK 6

Tracing Emails without Finding Email Header

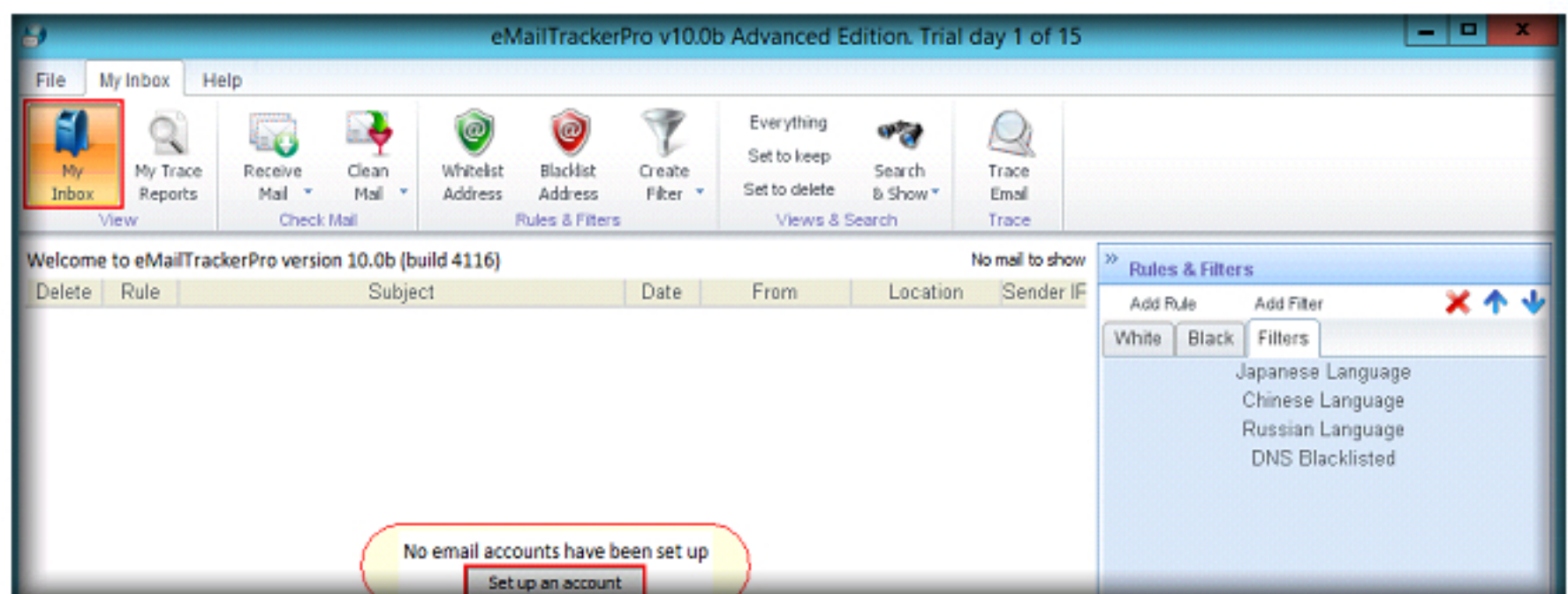


FIGURE 3.15: eMailTrackerPro options window

TASK 7**Creating a New Mail Account**

21. In the **New Mail Account** pop-up window, create a new mail account with port number 995 as the default, fill the proper information in all fields in the window, and click **OK**.

Note: In this lab, we are adding a Gmail account for demonstration.

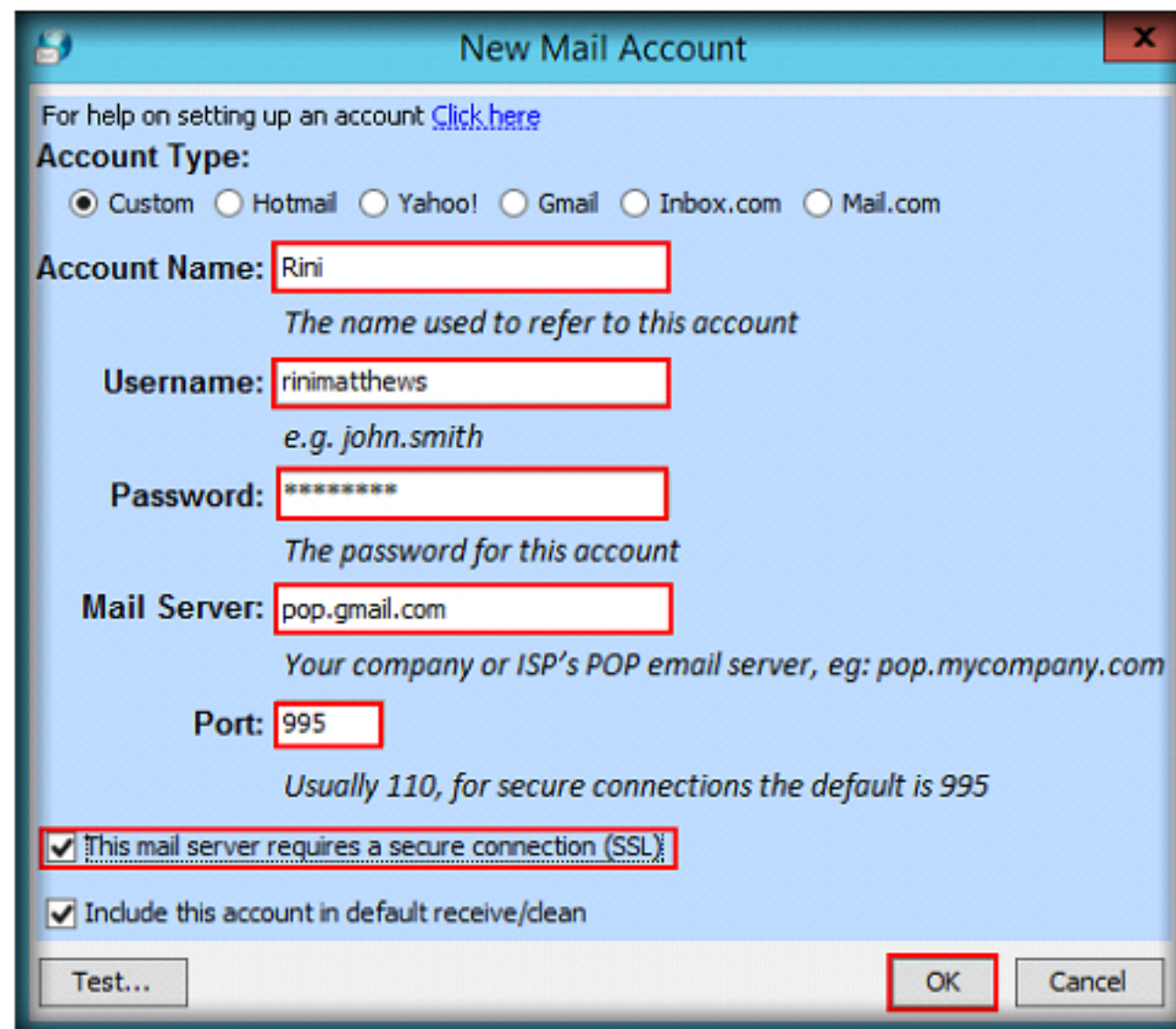


FIGURE 3.16: New Mail Account window

TASK 8**Tracing Email**

22. On the **Preferences** tab, select your mail account and click **OK**.

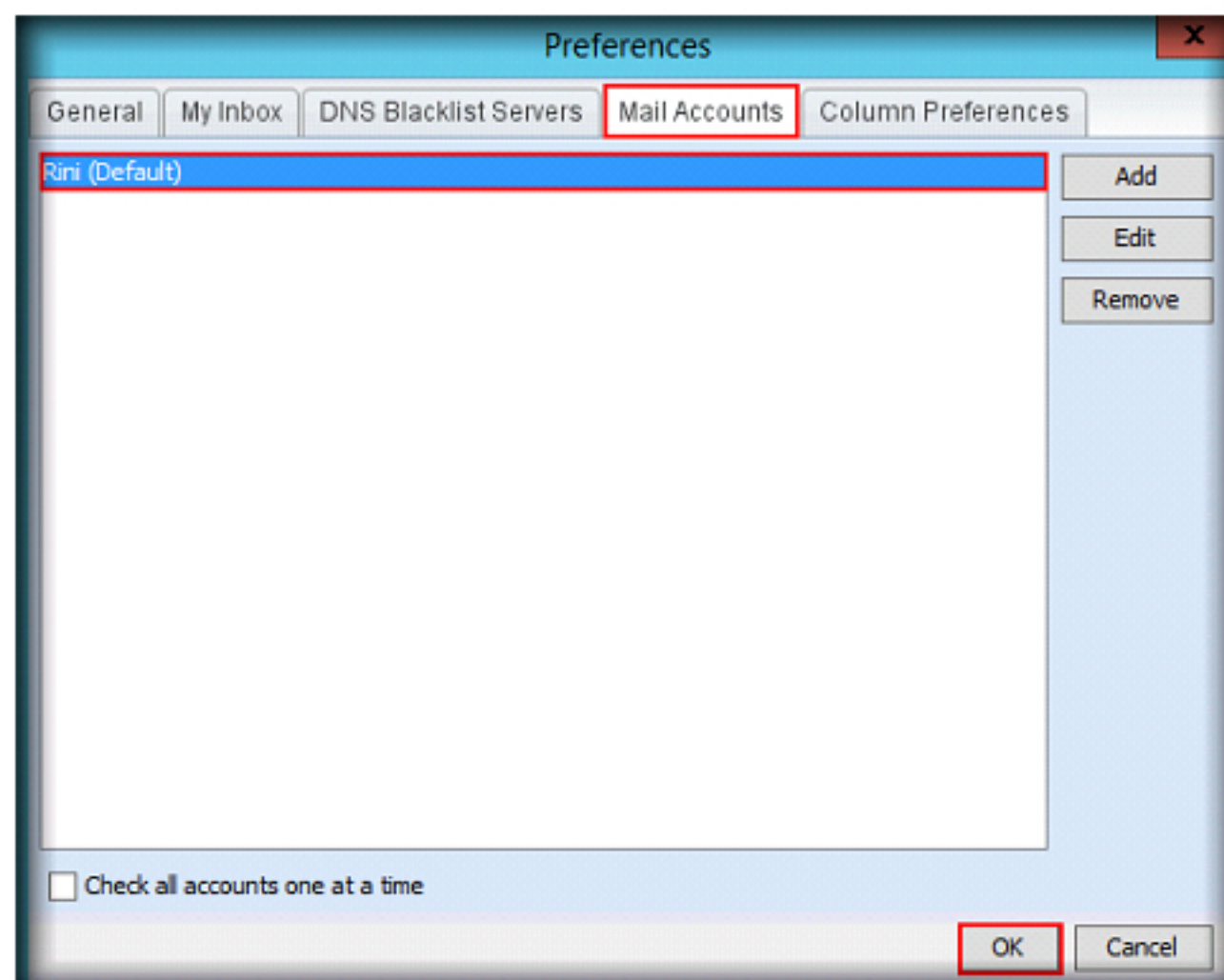


FIGURE 3.17: Preferences tab

Module 12 - Investigating Email Crimes

23. Click the **Receive Mail** tab on the left corner of the window and select the email account that is entered. It will display the email list with location, subject, sender, and other fields.

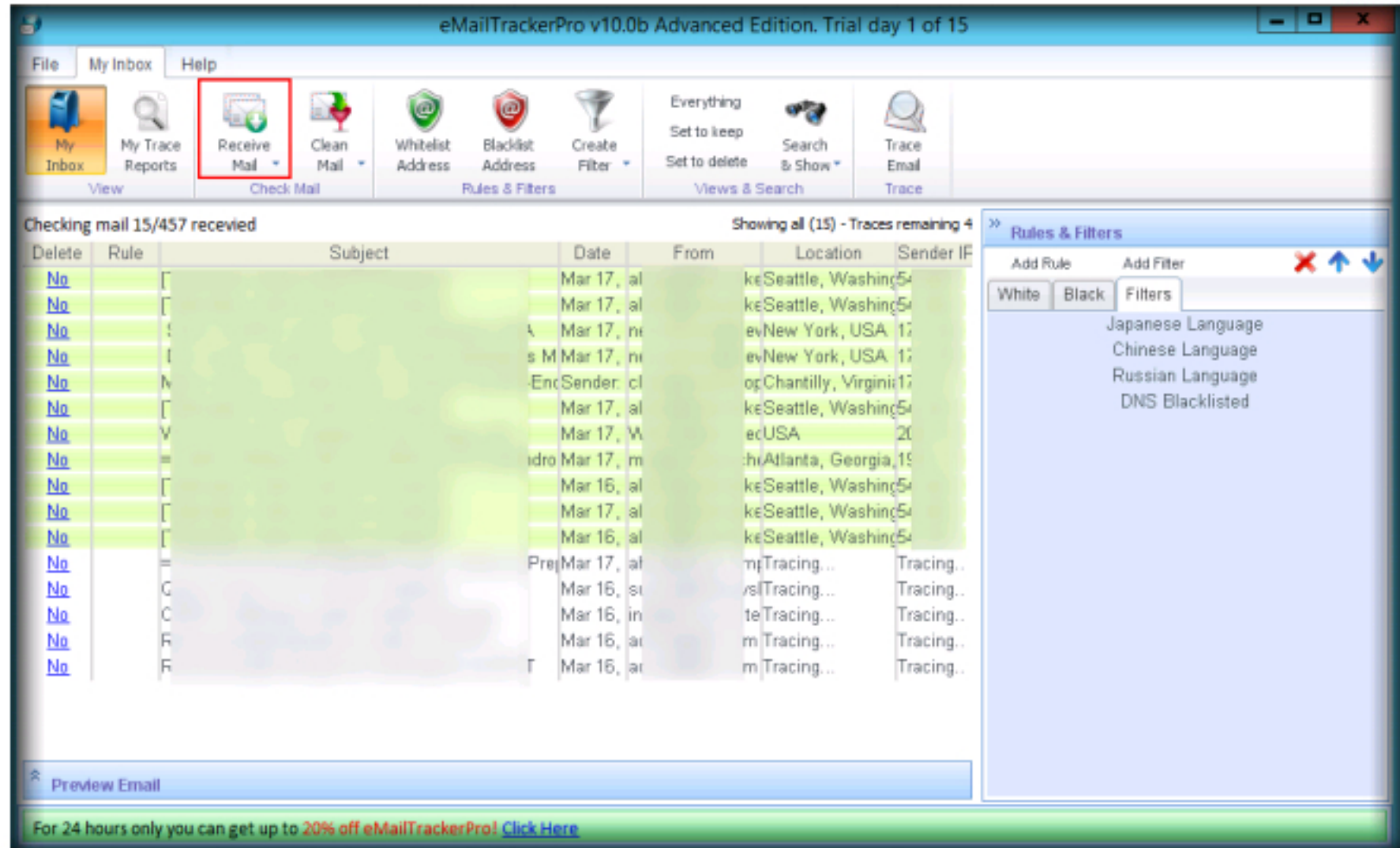


FIGURE 3.18: eMailTrackerPro showing contents of Receive Mail option

24. Select the email from the list that you want to trace and click the **Trace email** option in the toolbar.

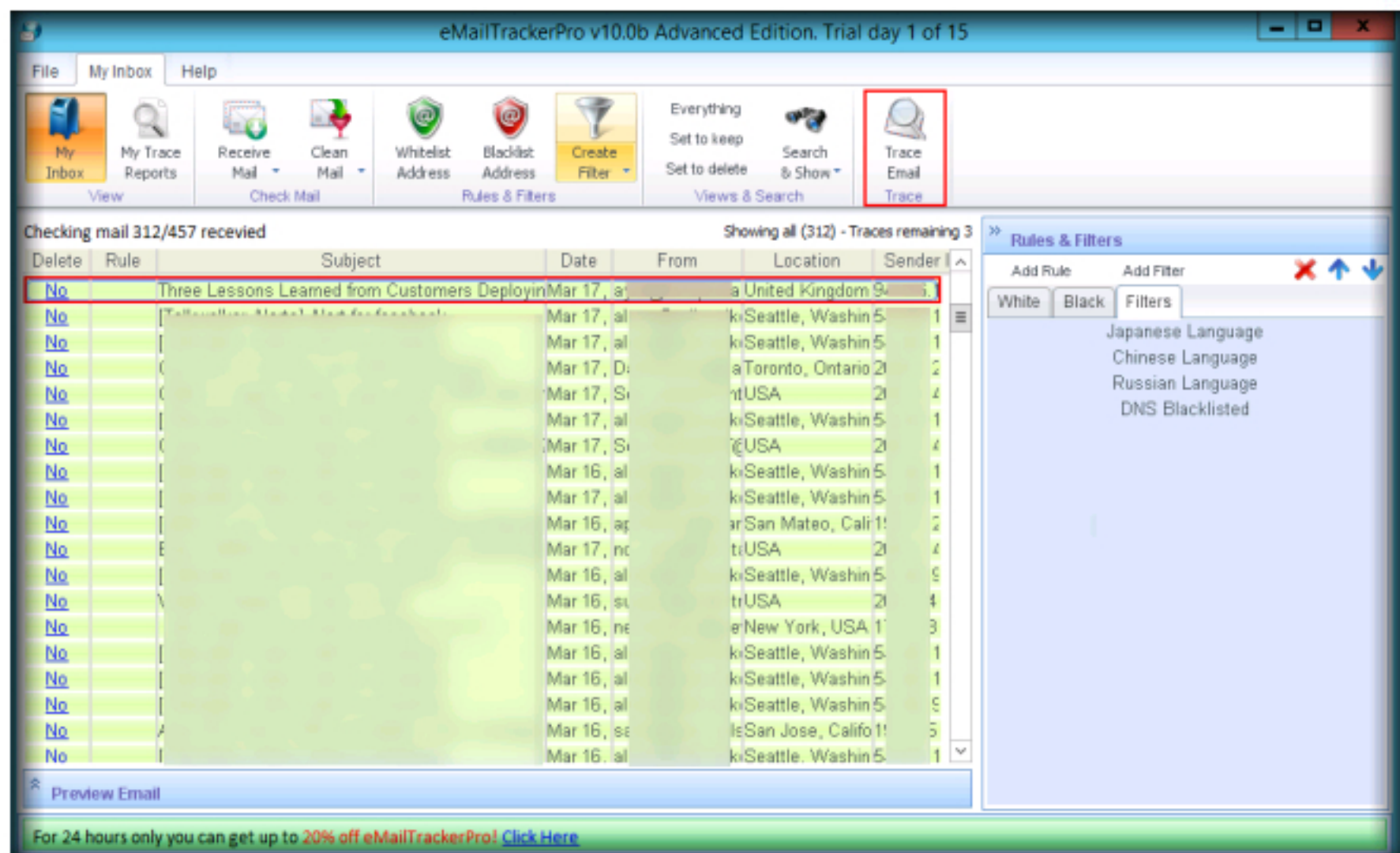


FIGURE 3.19: Tracing an email

TASK 9

Viewing Report

25. Another window will open showing all the tracing information of that particular mail. Click **View Report**.

Note: Once you click on **View Report** button a pop-up appears to choose the browser options.

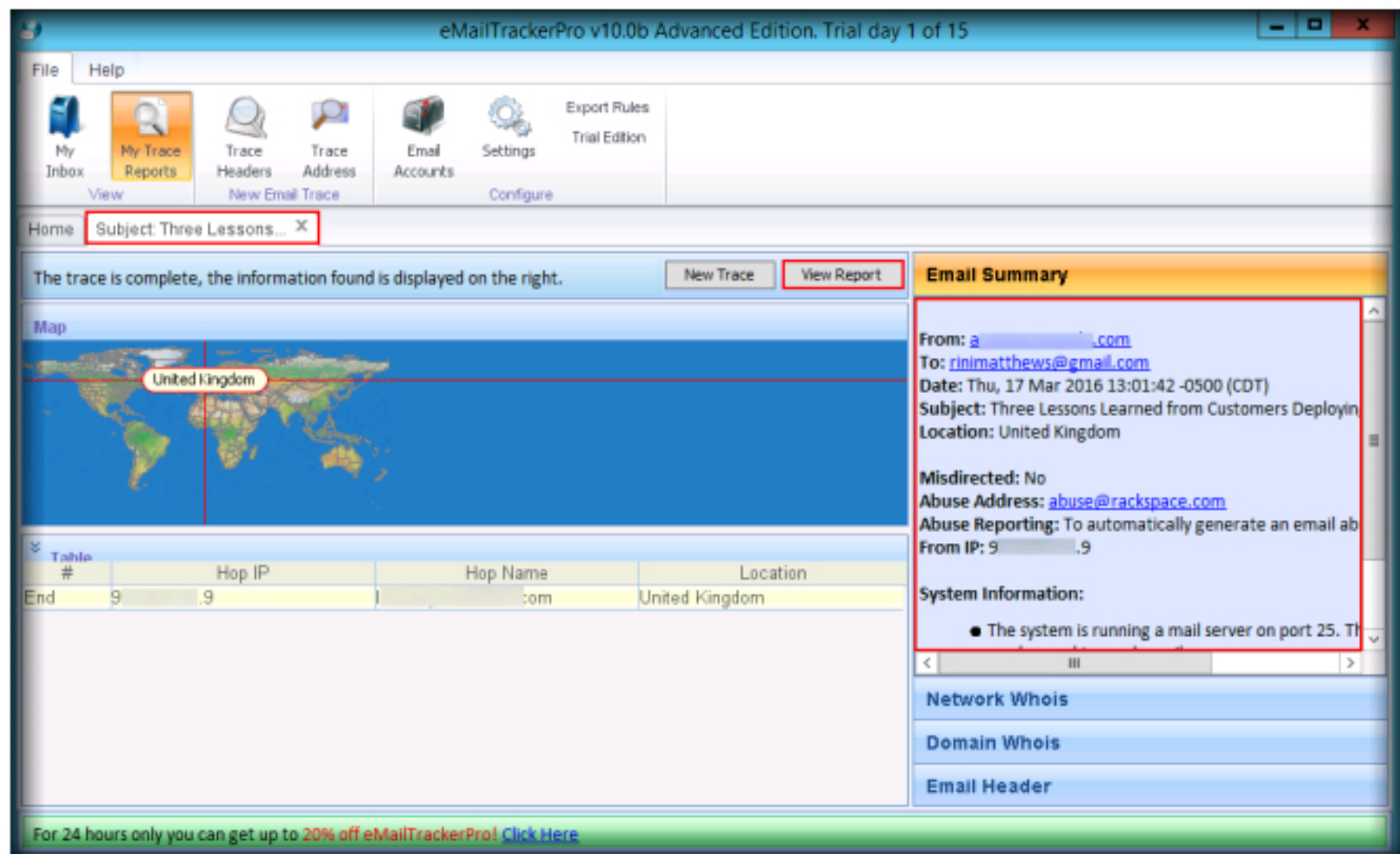


FIGURE 3.20: eMailTrackerPro displaying trace information

26. A browser with tracking information of the selected mail will open. Tracking information will vary, depending on the location.

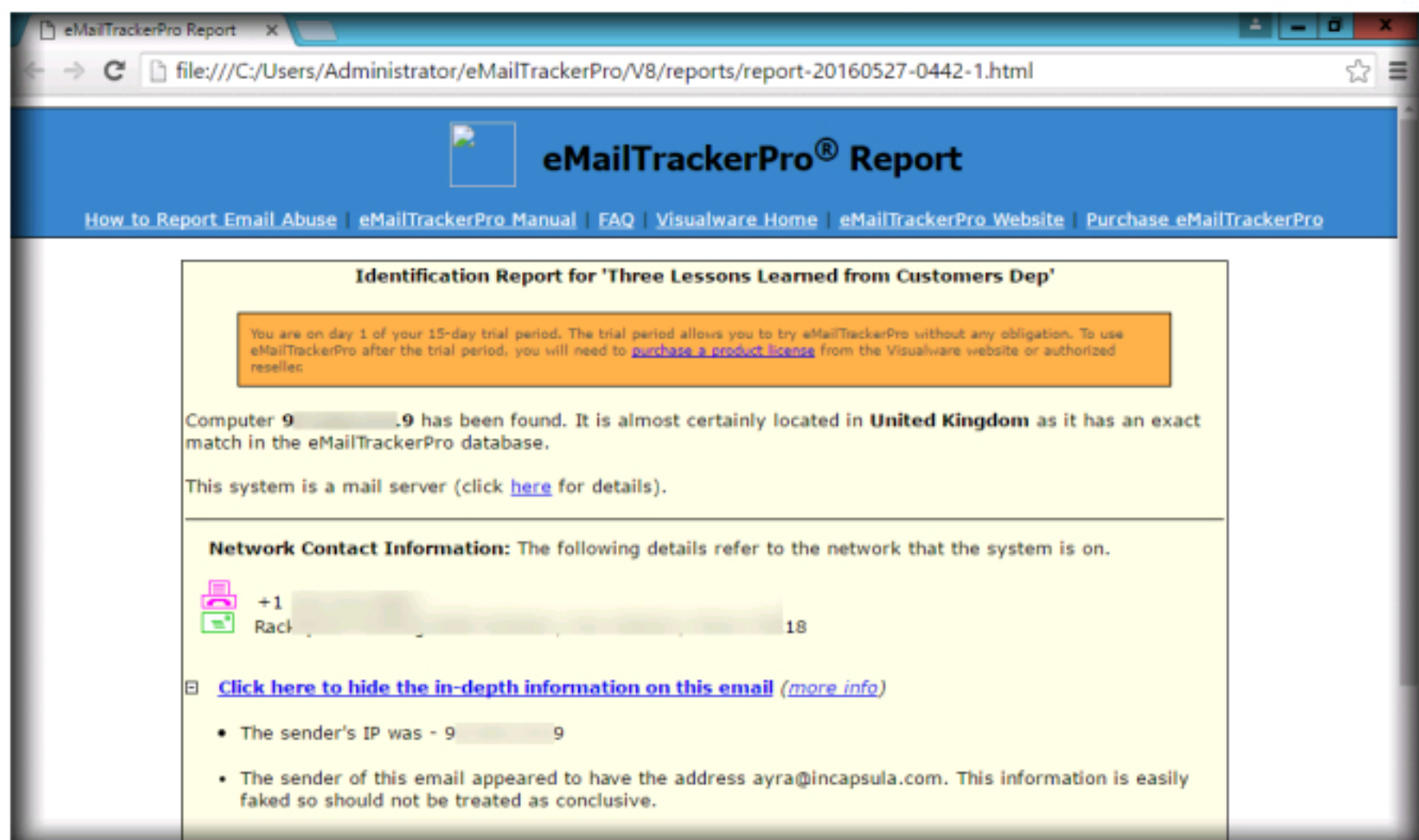


FIGURE 3.21: An eMailTrackerPro report

Note: A browser with tracing information of the selected mail will open. Tracking information will vary, depending on the location.

Lab Analysis

Analyze all the information that has been retrieved by using the eMailTrackerPro tool, and document the results related to the lab exercise. Give your expert opinion on the target email address.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs