Lab-06

Recovering Deleted Emails Using the Recovery My Email

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

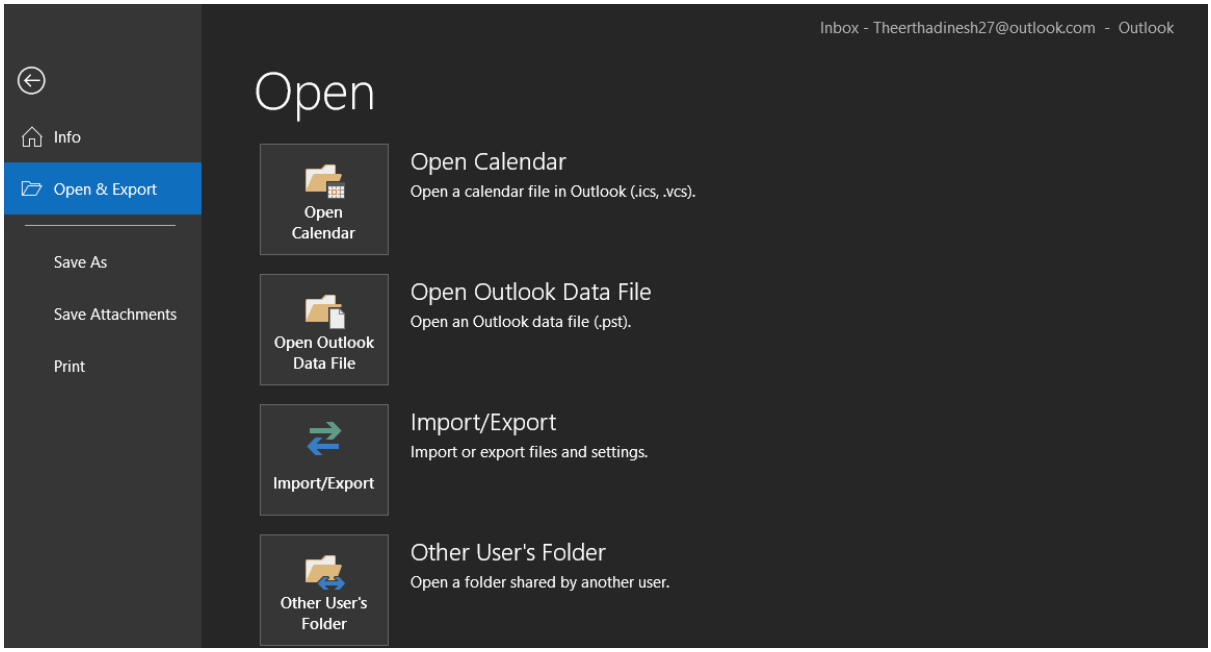
Lab objectives:

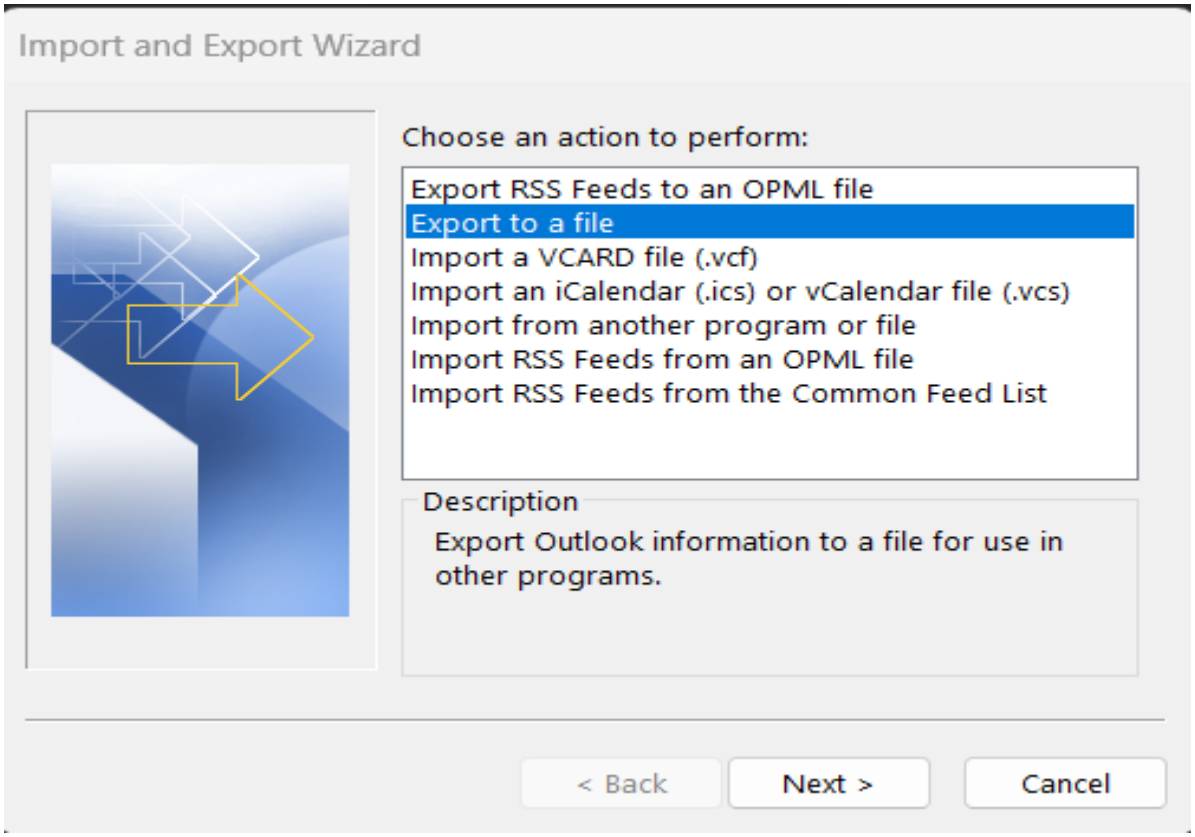
The objective of this lab is to help investigators understand how to track and investigate email crime using various tools to obtain :

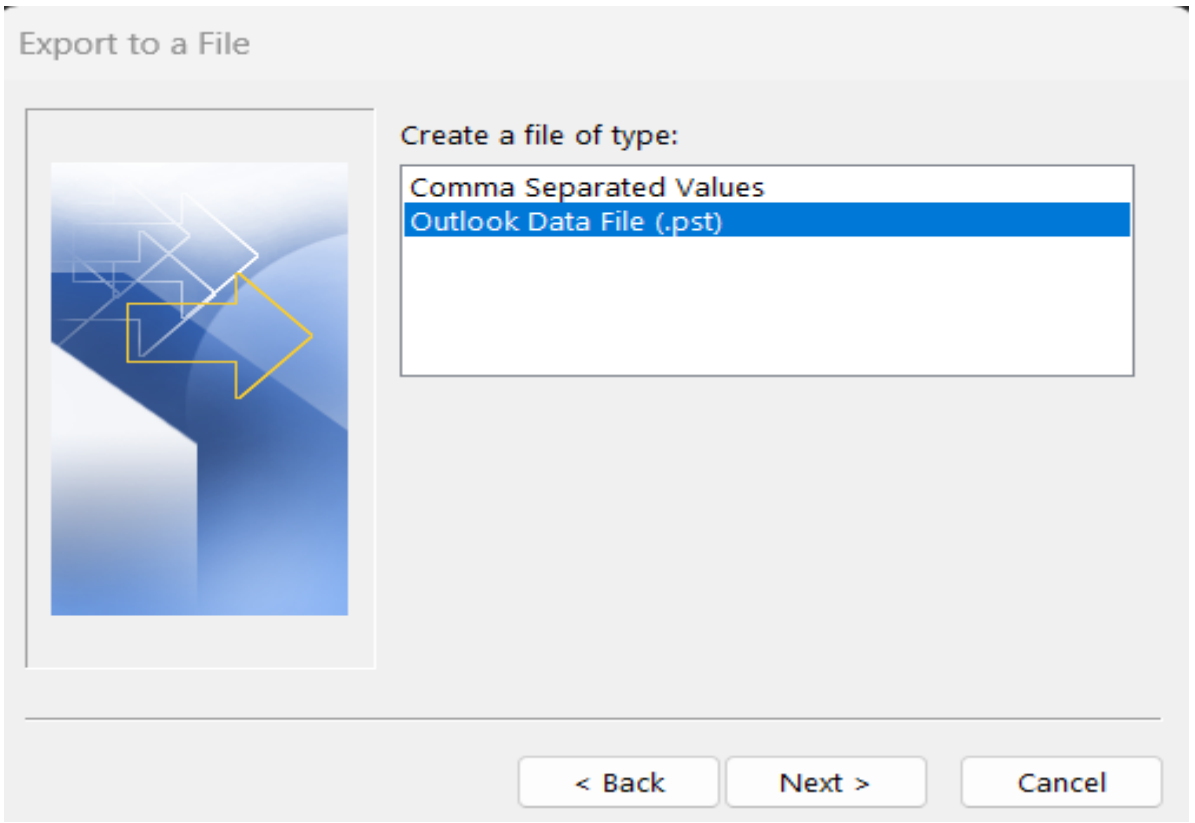
- Message contacts
- Deleted email messages and attachments.

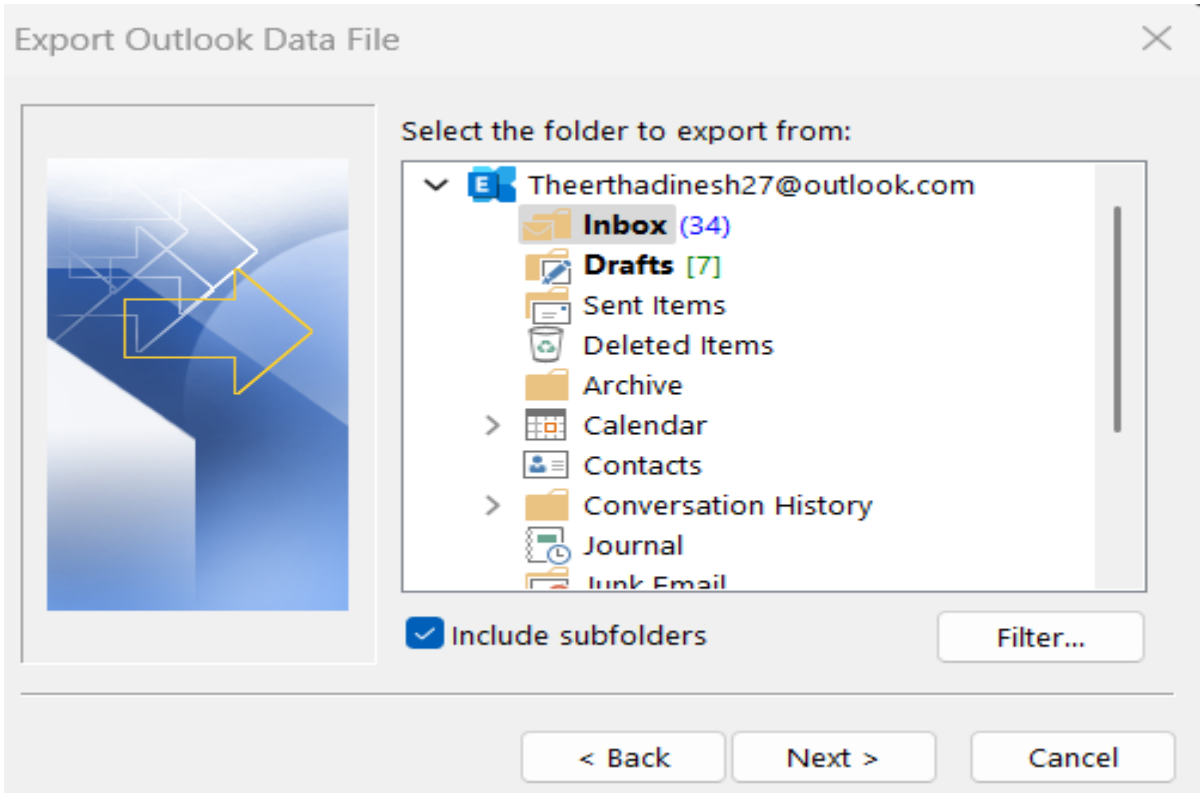
Create a target.pst file in outlook

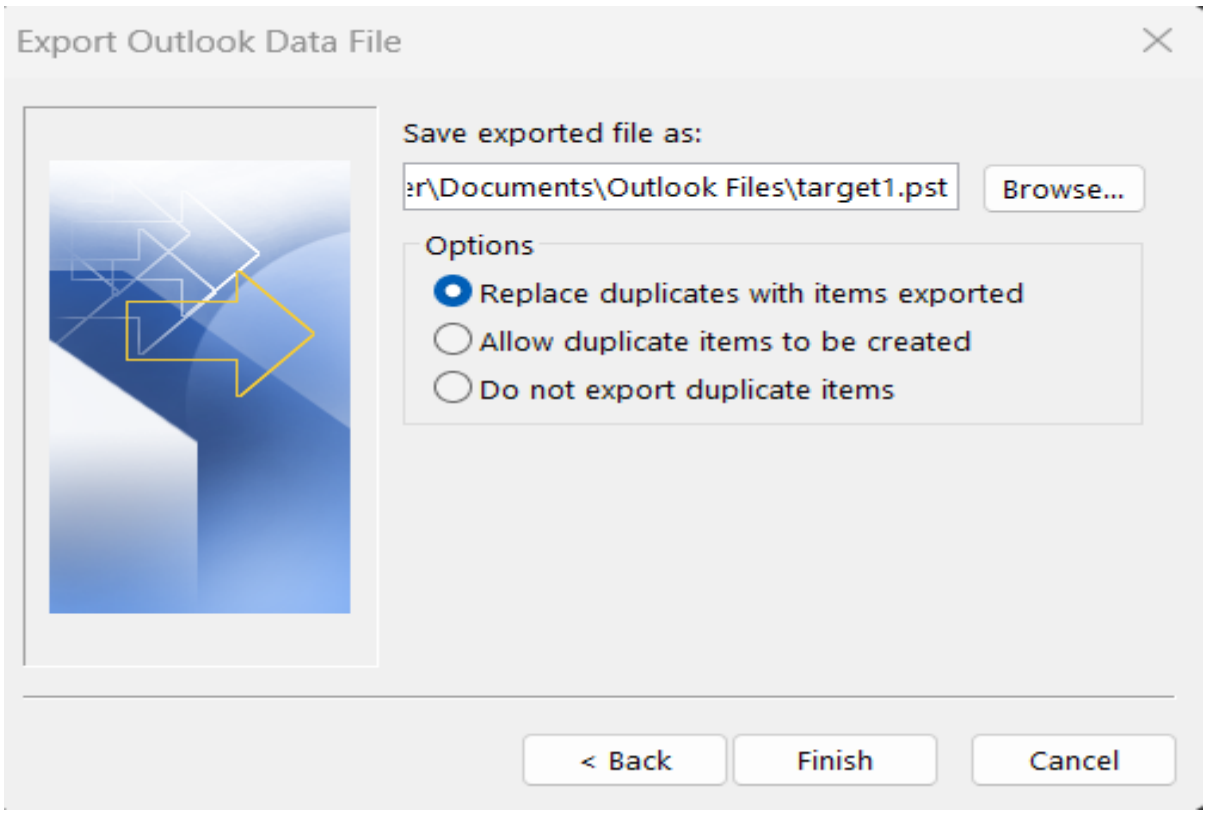
File->Open&Export->Import/Export->Export to a file->outlook datafile(.pst)->select the folder->save exported file as

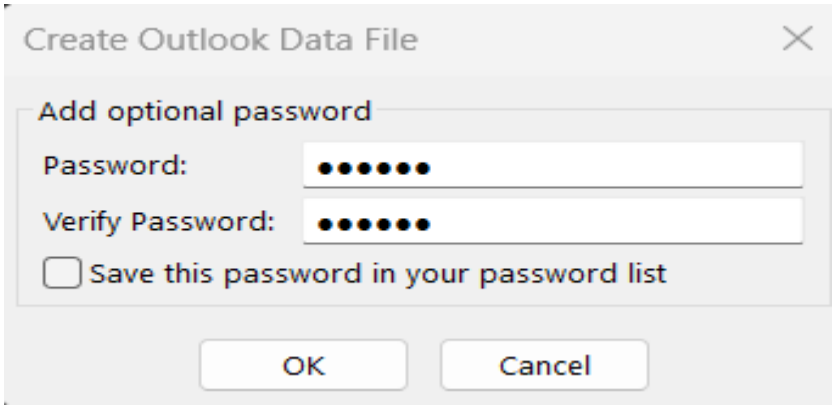


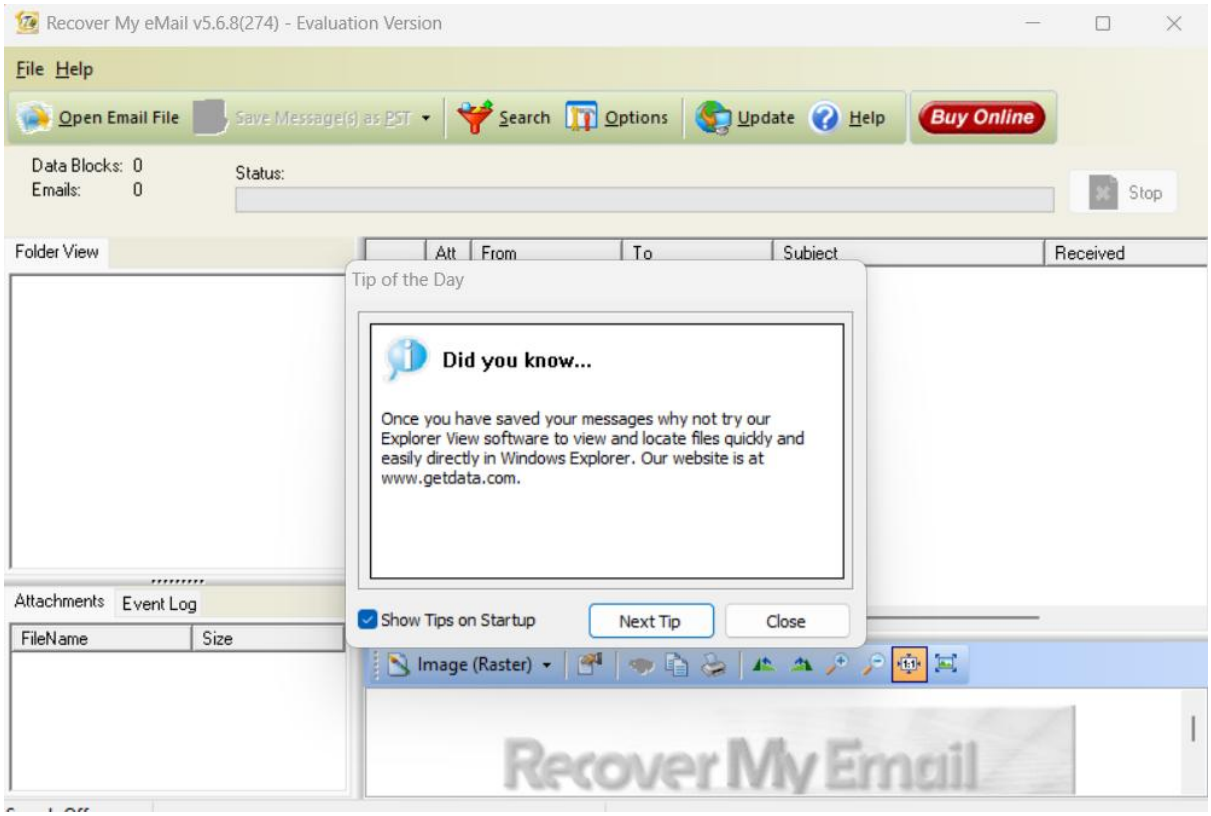

Import and Export Wizard
Choose an action to perform:
Export RSS Feeds to an OPML file
Export to a file
Import a VCARD file (.vcf)
Import an iCalendar (.ics) or vCalendar file (.vcs)
Import from another program or file
Import RSS Feeds from an OPML file
Import RSS Feeds from the Common Feed List
Description
Export Outlook information to a file for use in other programs.
< Back
Next >
Cancel


Export to a File
Create a file of type:
Comma Separated Values
Outlook Data File (.pst)
< Back
Next >
Cancel

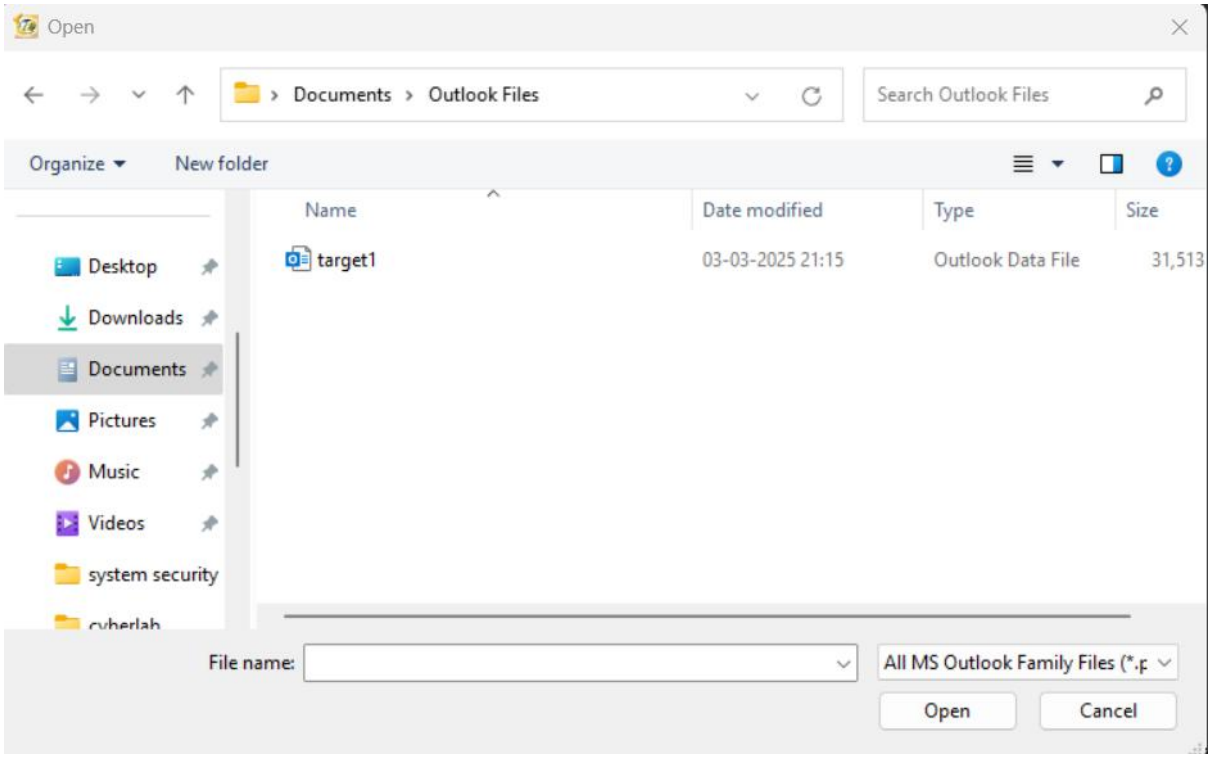

Export Outlook Data File
Select the folder to export from:
Theerthadinesh27@outlook.com
Inbox (34)
Drafts [7]
Sent Items
Deleted Items
Archive
Calendar
Contacts
Conversation History
Journal
Include subfolders
Filter...
< Back
Next >
Cancel

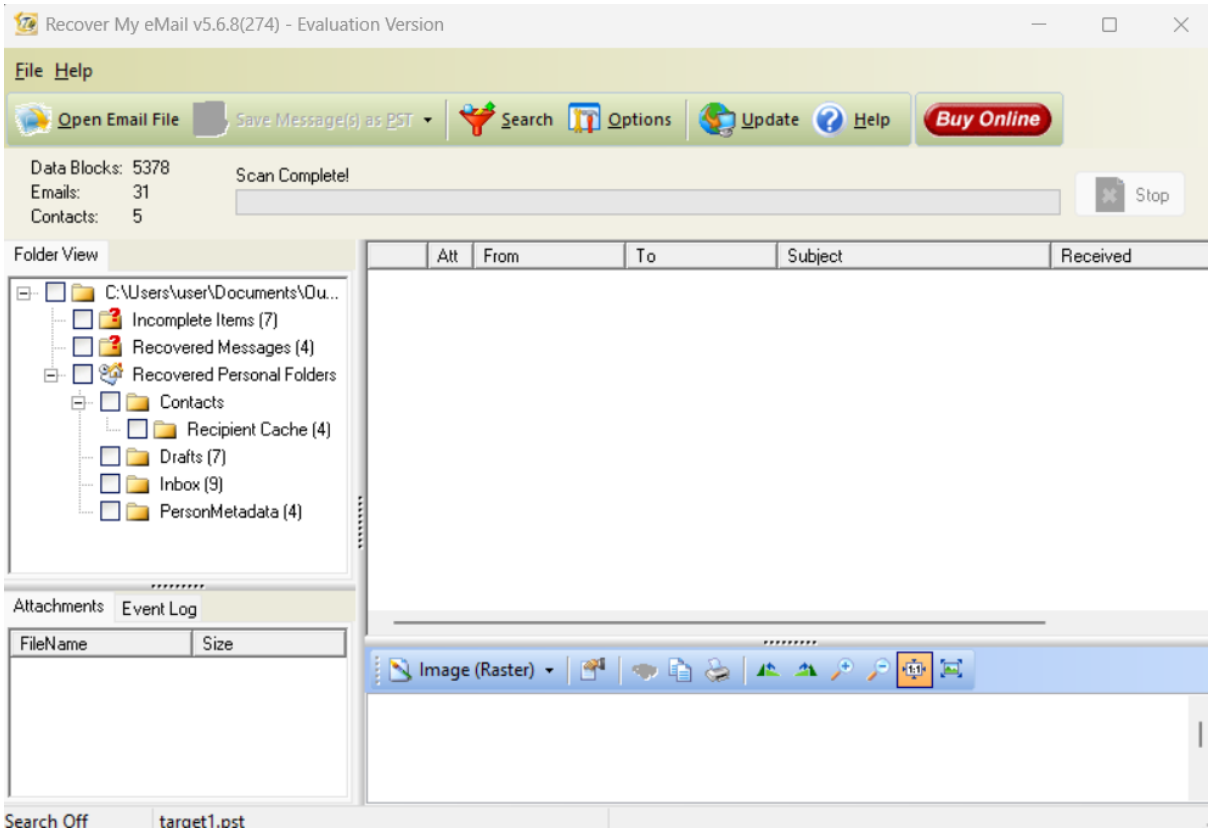

Export Outlook Data File
Save exported file as:
er\Documents\Outlook Files\target1.pst
Browse...
Options
Replace duplicates with items exported
Allow duplicate items to be created
Do not export duplicate items
< Back
Finish
Cancel



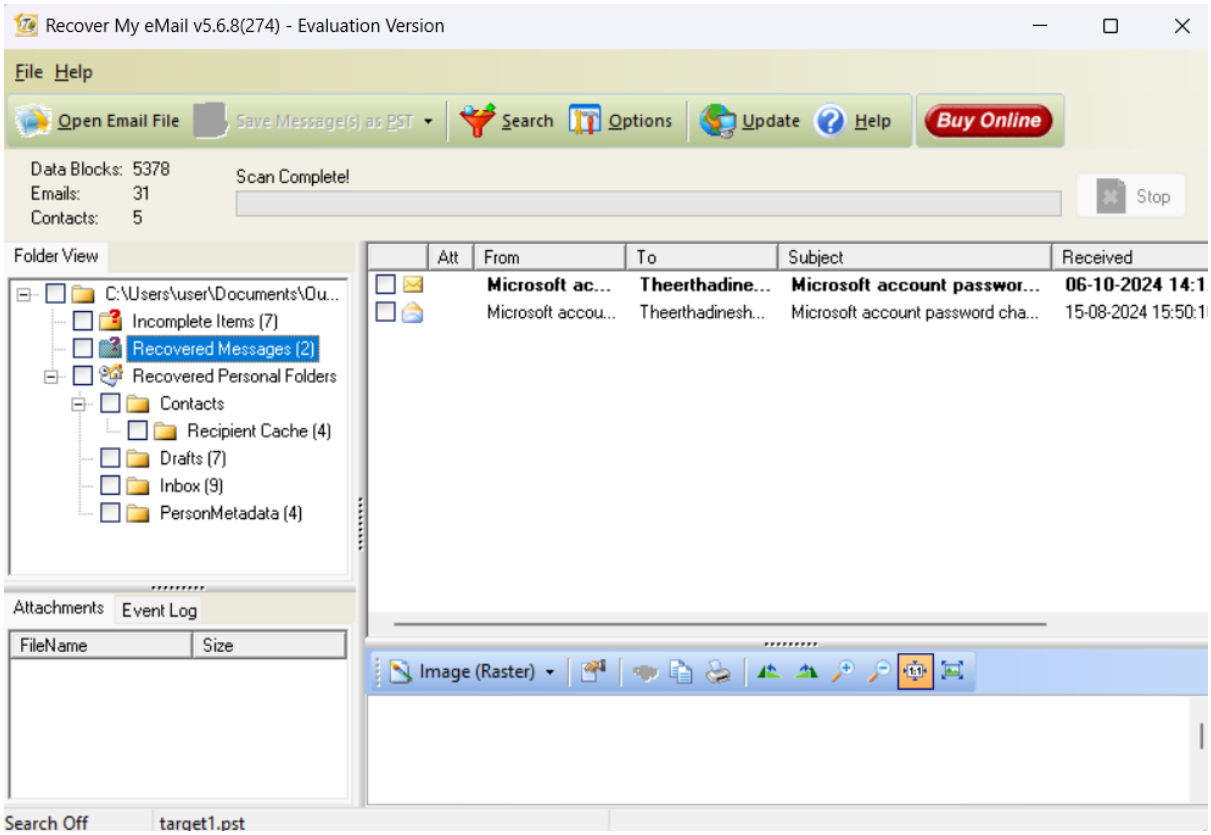


Click the open Email File button to open the email files. Select the target account's .pst file then click open. The Recovery My Email tool will scan the selected .pst email file and display the folder view with the result obtained in the left pane of the window.

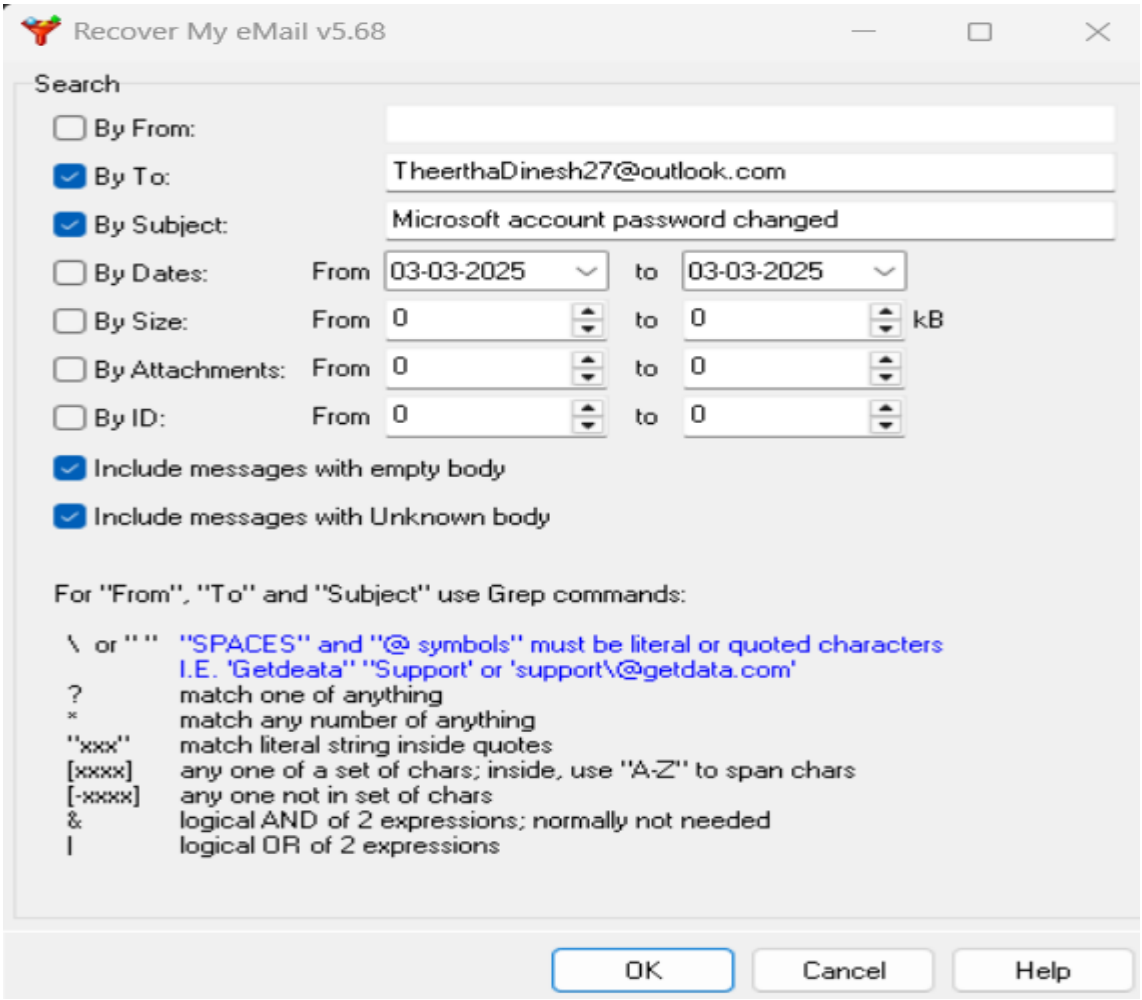


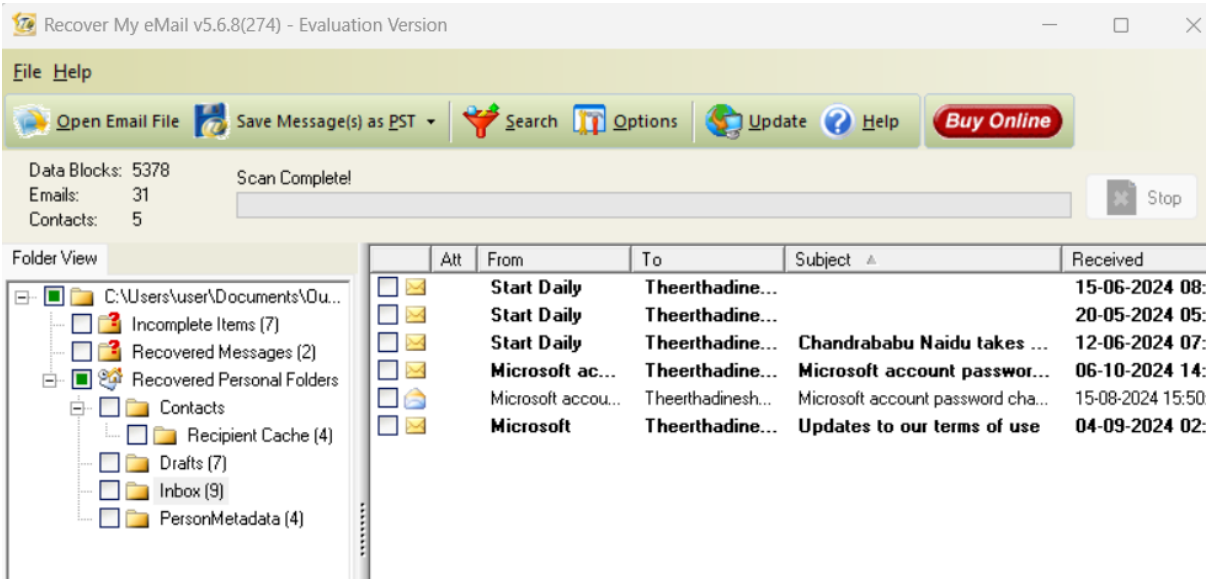


To see the Recovered emails, click Recovered Messages in the Folder view tab. It will display the list of recovered emails and messages. Here it will show the recipient's email address, subject, and received date and time .

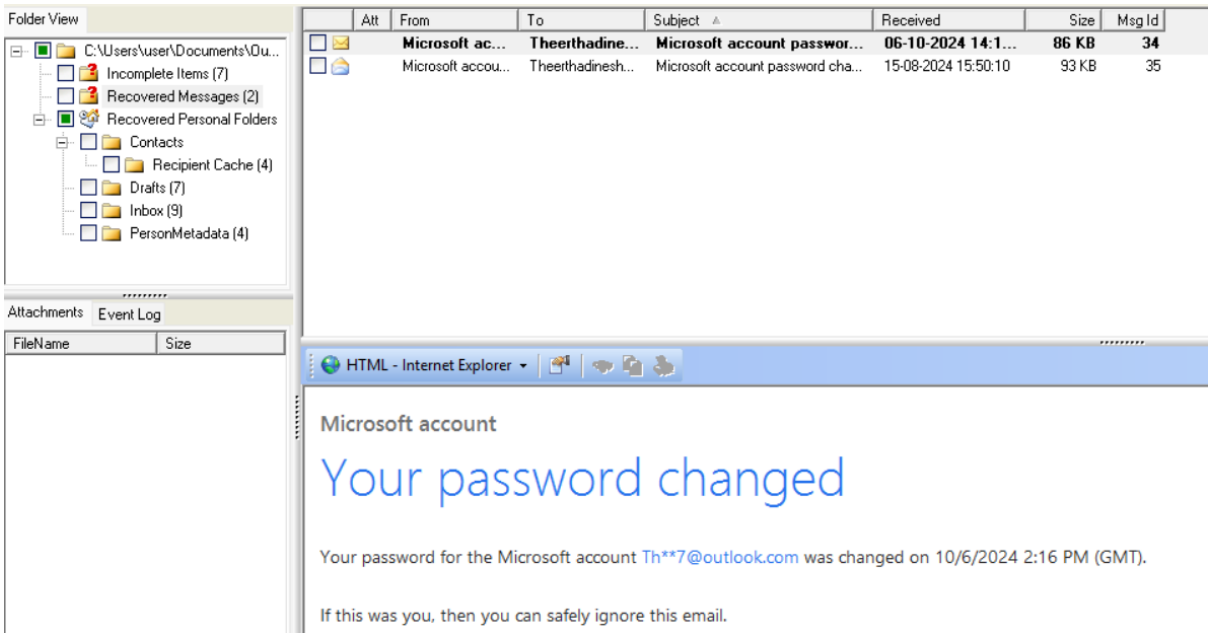


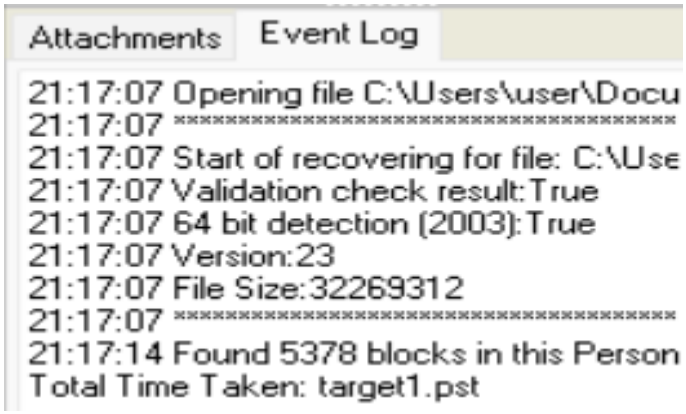
To search click the search button, A recovery email window appears where we need to specify options to search the mails.

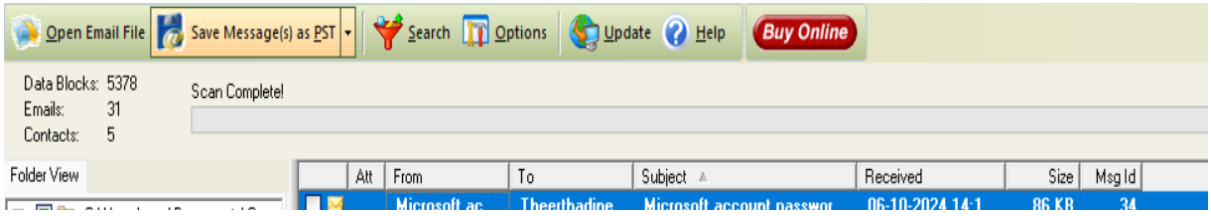




To see the actual content of the email , click the email. The email content will display in the bottom pane of window.

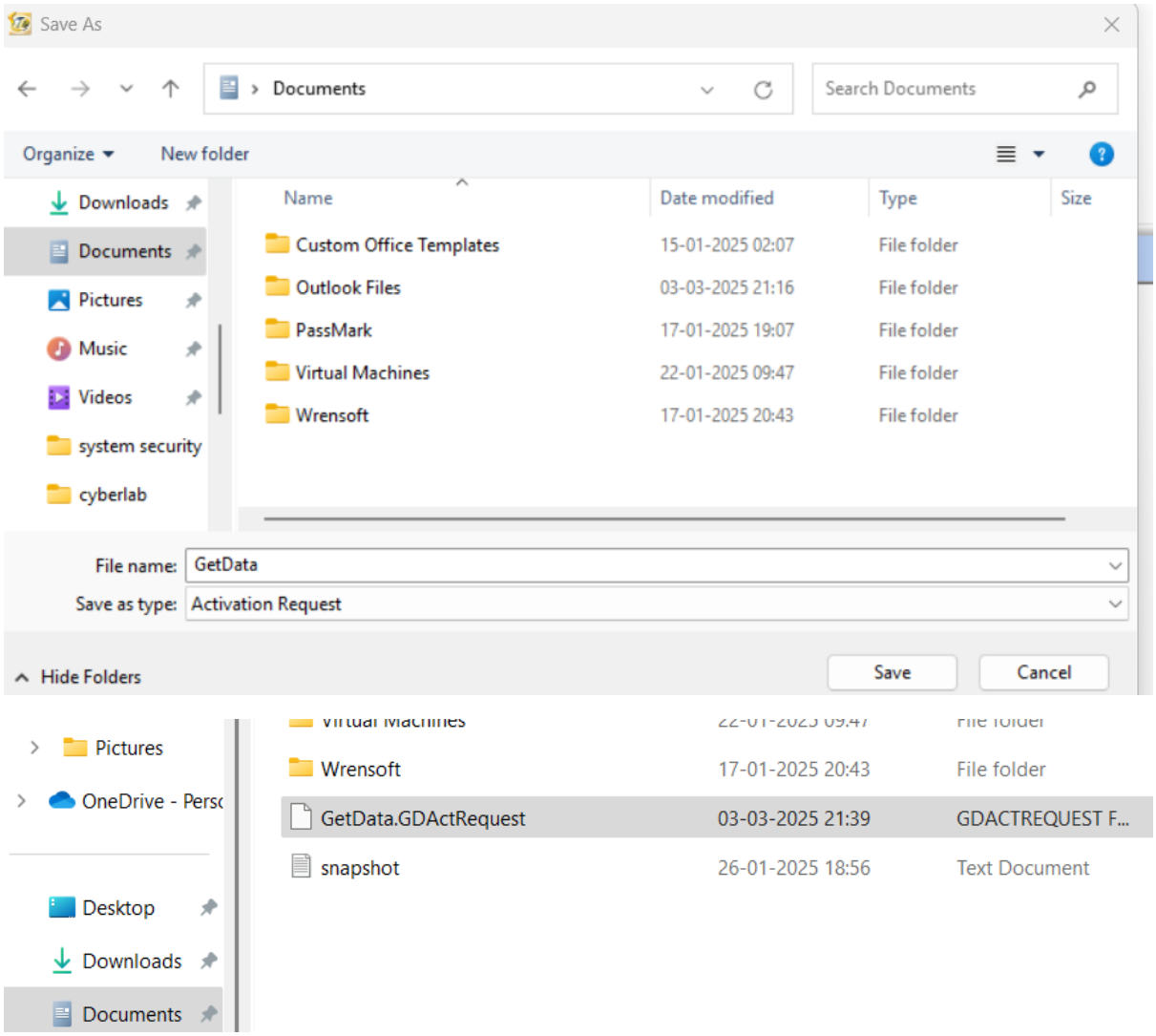

Folder View
C:\Users\user\Documents\Ou...
Incomplete Items (7)
Recovered Messages (2)
Recovered Personal Folders
Contacts
Recipient Cache (4)
Drafts (7)
Inbox (9)
PersonMetadata (4)
Att
From
To
Subject
Received
Size
Msg Id
Microsoft ac...
Theerthadine...
Microsoft account passwor...
06-10-2024 14:1...
86 KB
34
Microsoft accou...
Theerthadinesh...
Microsoft account password cha...
15-08-2024 15:50:10
93 KB
35
Attachments
Event Log
FileName
Size
HTML - Internet Explorer
Microsoft account
Your password changed
Your password for the Microsoft account Th**7@outlook.com was changed on 10/6/2024 2:16 PM (GMT).
If this was you, then you can safely ignore this email.


Attachments
Event Log
21:17:07 Opening file C:\Users\user\Docu
21:17:07 **********
21:17:07 Start of recovering for file: C:\Use
21:17:07 Validation check result:True
21:17:07 64 bit detection (2003):True
21:17:07 Version:23
21:17:07 File Size:32269312
21:17:07 **********
21:17:14 Found 5378 blocks in this Person
Total Time Taken: target1.pst


Open Email File
Save Message(s) as PST
Search
Options
Update
Help
Buy Online
Data Blocks: 5378
Emails: 31
Contacts: 5
Scan Complete!
Folder View
Att
From
To
Subject
Received
Size
Msg Id


Recover My eMail v5.6.8(274) - Evaluation Version
Activation
Online Activation
Online activation is an automated process that requires an internet connection. No personal information is sent.
Offline Activation
Offline activation is a manual process which can be used if internet access is limited.
GetData
< Back
Next >
Cancel


Recover My eMail v5.6.8(274) - Evaluation Version
Activation - Offline
Web Browser Activation
Step 1:
Export your activation request file
Export
Step 2:
Upload your activation request file, license key and email address at the following website:
getdata.com/offline
Step 3:
Import your new activation response file
Import
GetData
< Back
Next >
Cancel



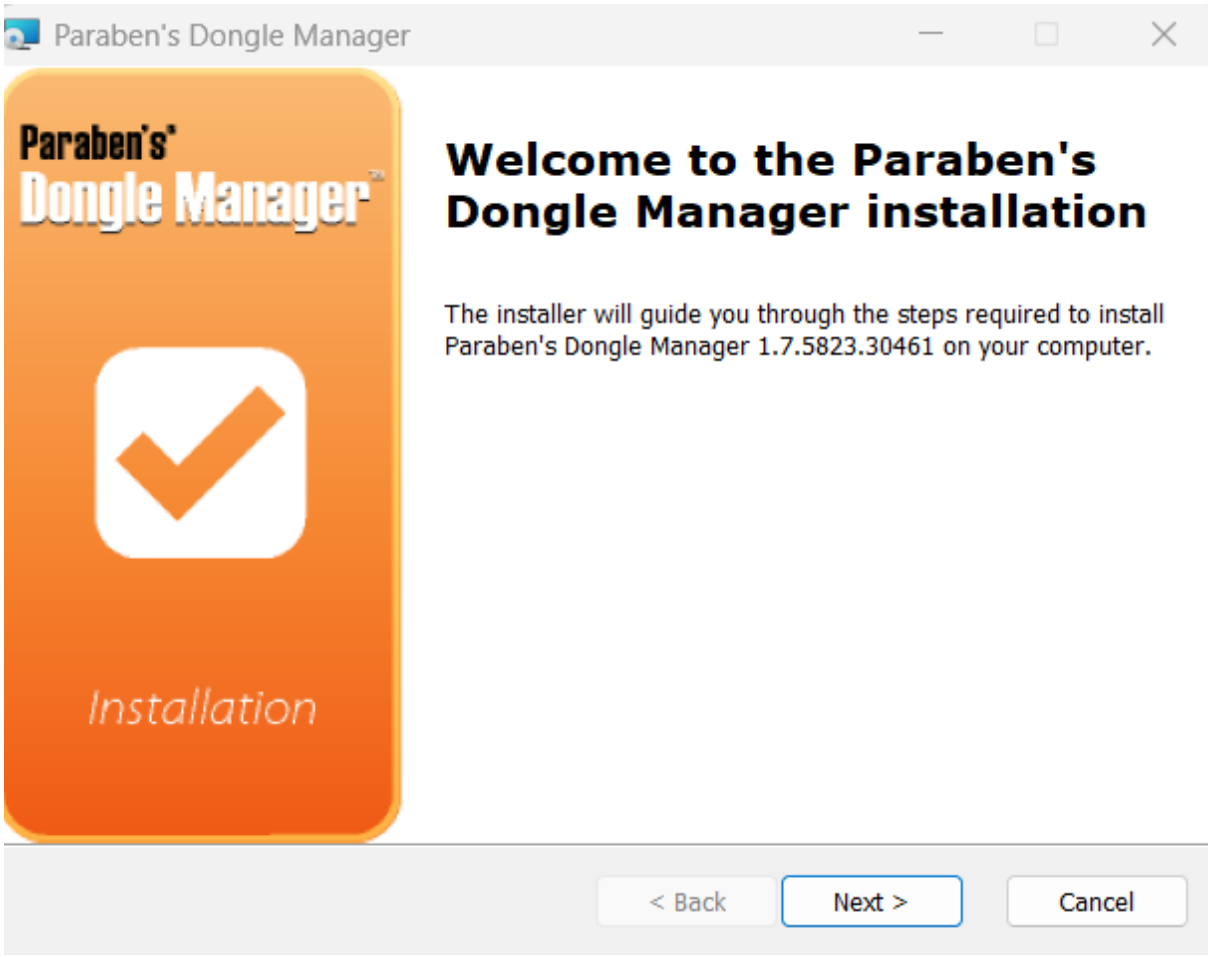
Here message is saved.

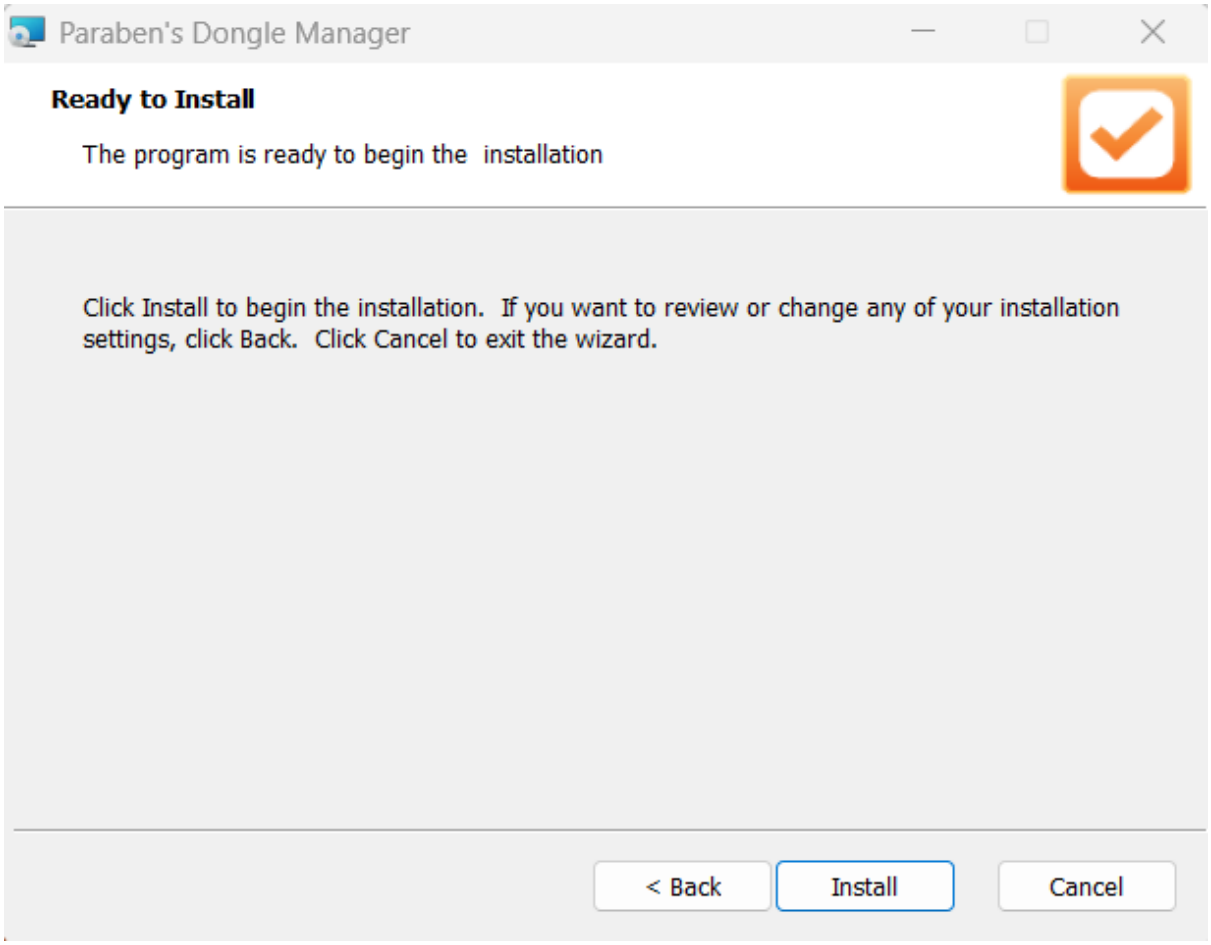
Investigating Email Crimes Using Paraben's Email Examiner Tool

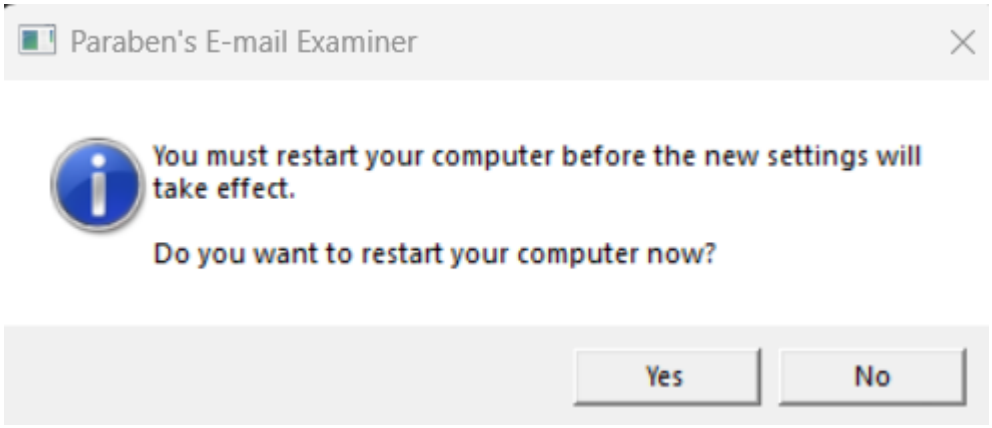
Lab objective:

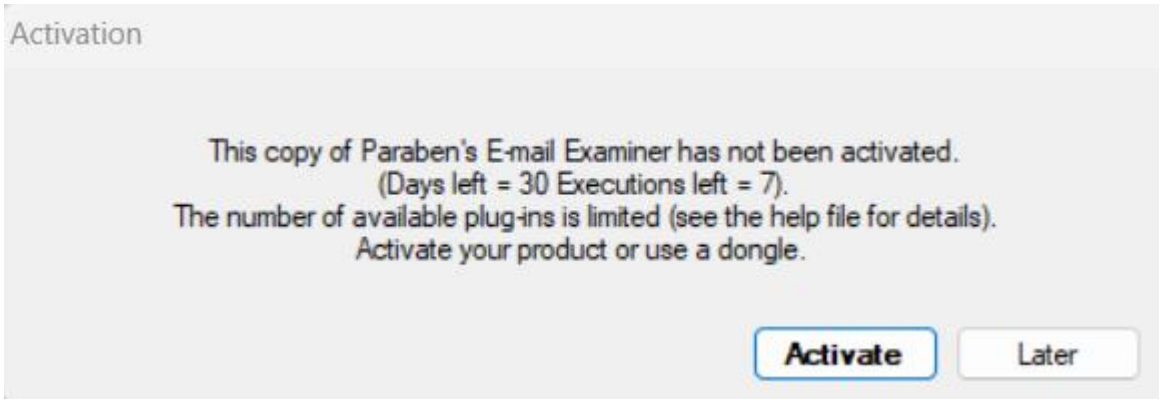
The objective of this lab is to help investigators and perform an investigation of email crimes. Using paraben's Email Examiner we can:

- Add evidence image
- Recover deleted emails
- Save recovered emails

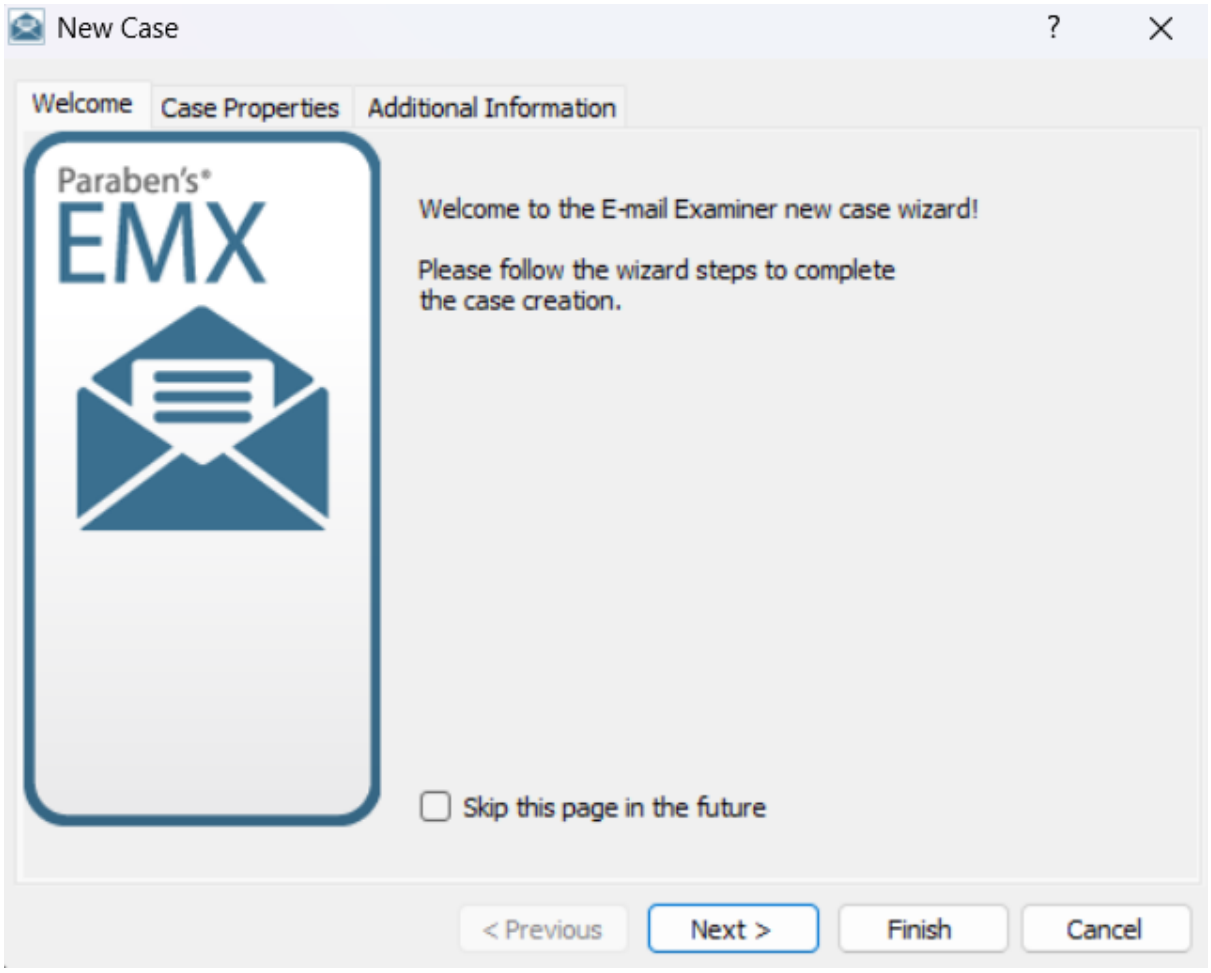

Paraben's Dongle Manager
Paraben's
Dongle Manager
Installation
Welcome to the Paraben's Dongle Manager installation
The installer will guide you through the steps required to install Paraben's Dongle Manager 1.7.5823.30461 on your computer.
< Back
Next >
Cancel


Paraben's Dongle Manager
Ready to Install
The program is ready to begin the installation
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
< Back
Install
Cancel

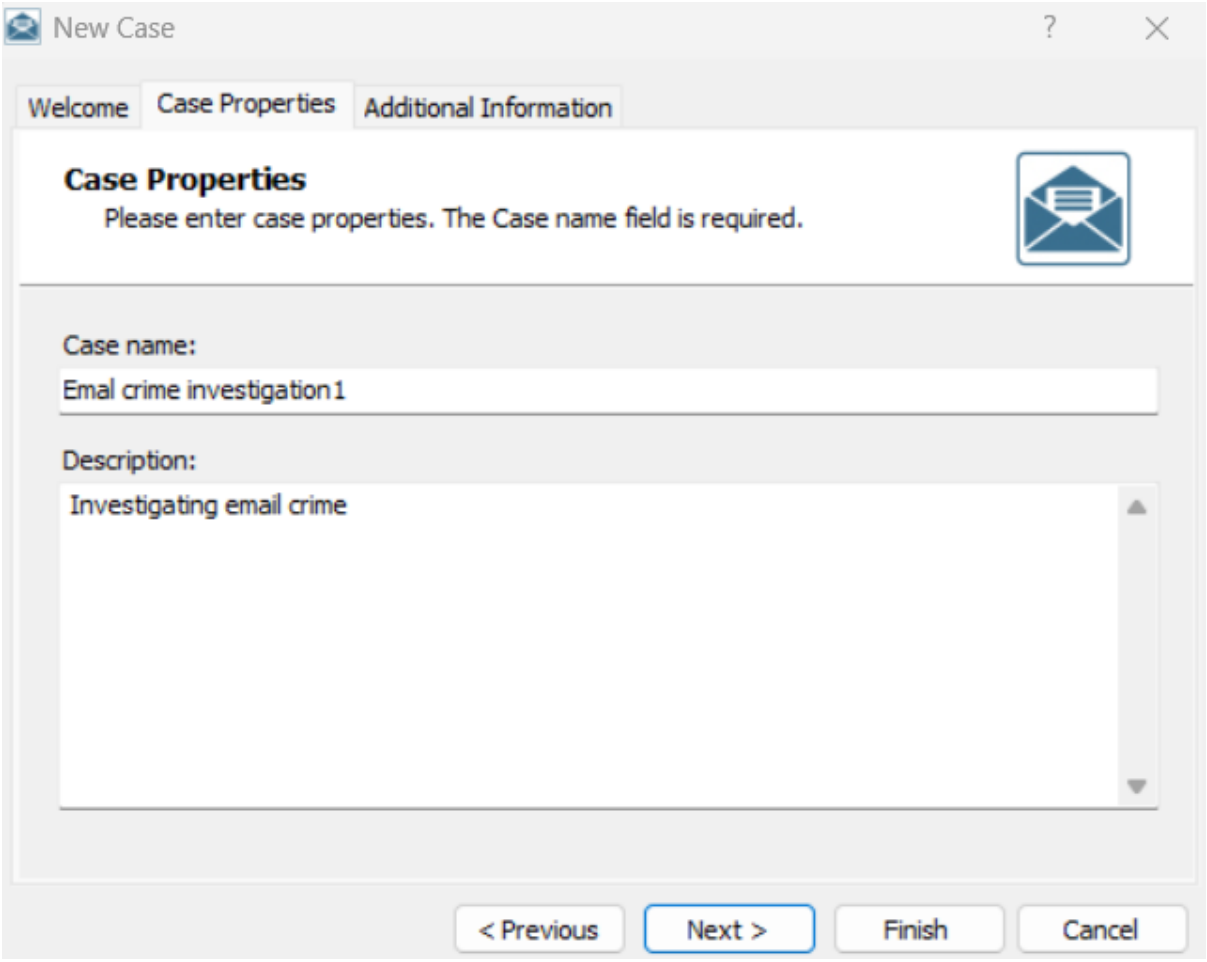

Paraben's E-mail Examiner
You must restart your computer before the new settings will take effect.
Do you want to restart your computer now?
Yes
No


Activation
This copy of Paraben's E-mail Examiner has not been activated.
(Days left = 30 Executions left = 7).
The number of available plug-ins is limited (see the help file for details).
Activate your product or use a dongle.
Activate
Later

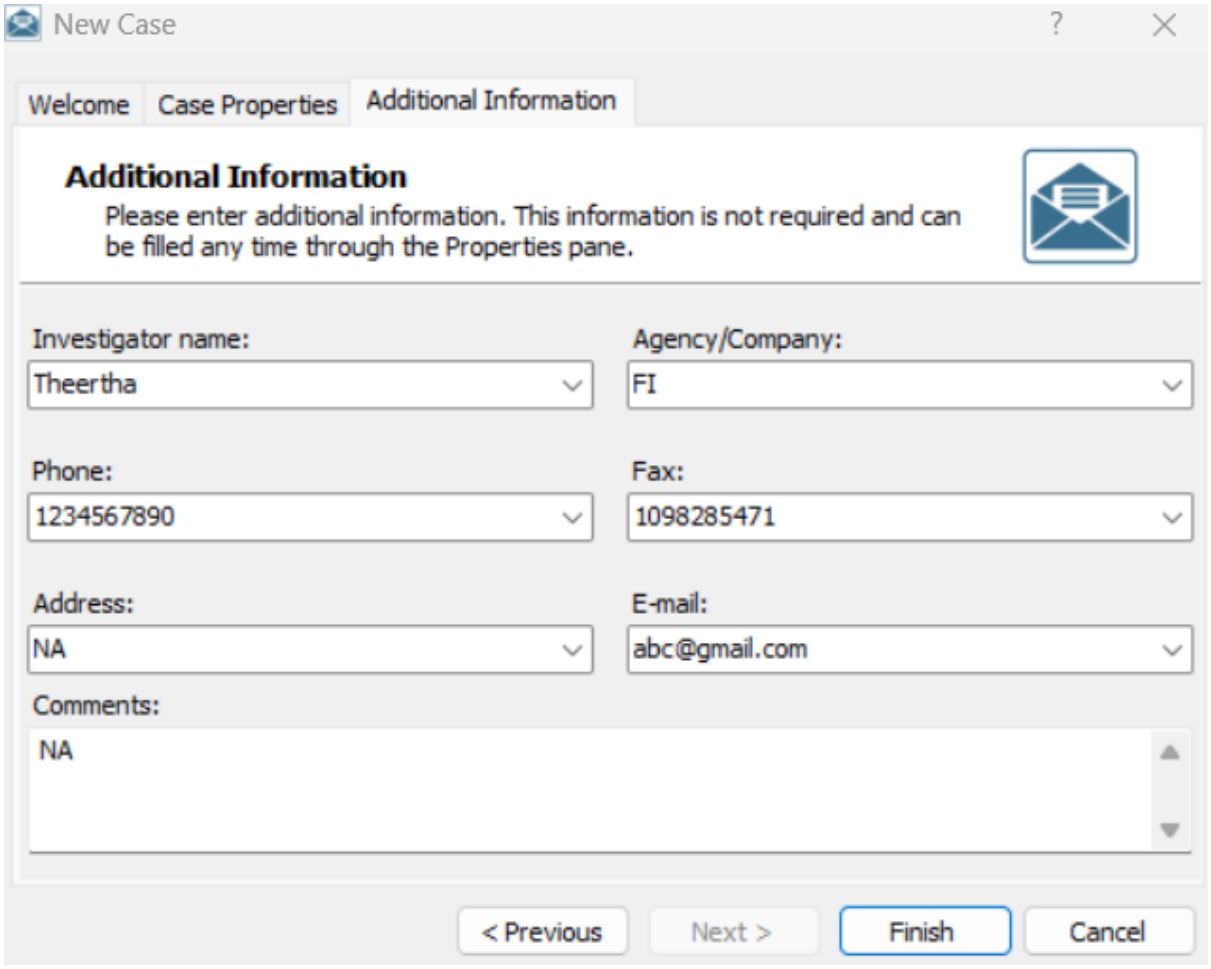
Before starting an investigation, we should create a case by clicking the create new case button.



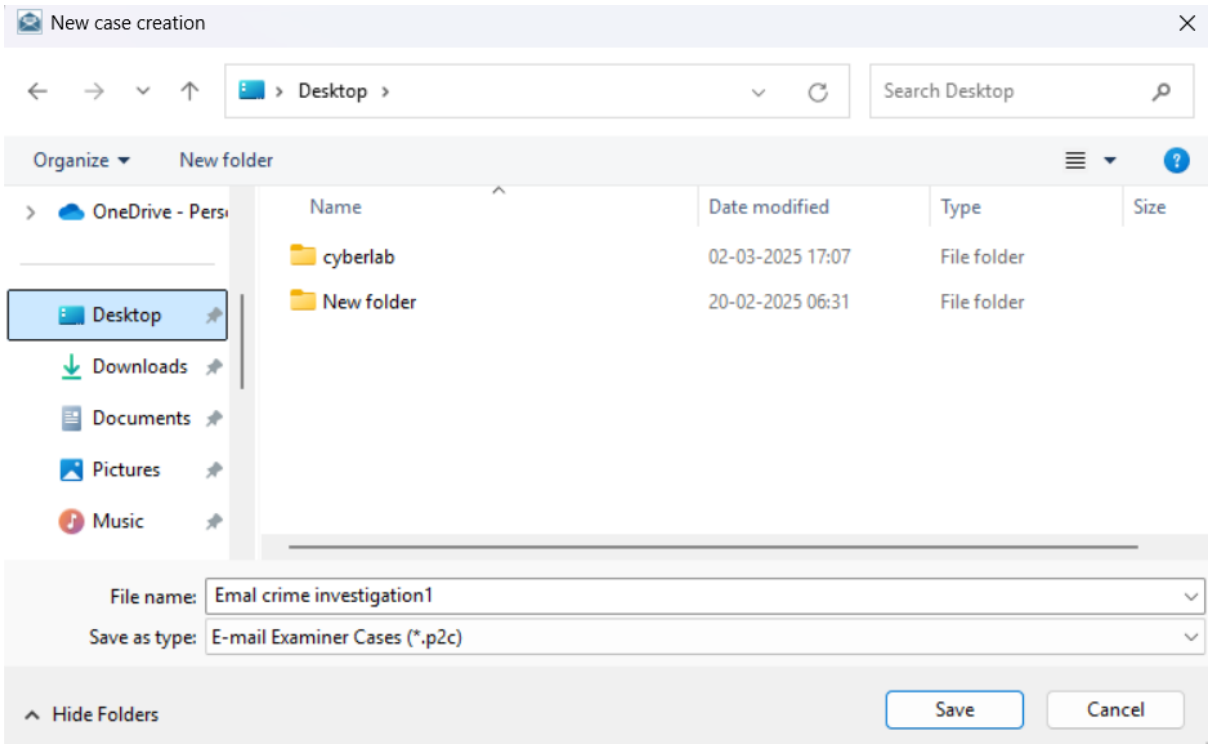
Case properties section appears. Fill the case name and Description fields with appropriate information and click next. This selection will take us to the Additional information tab.

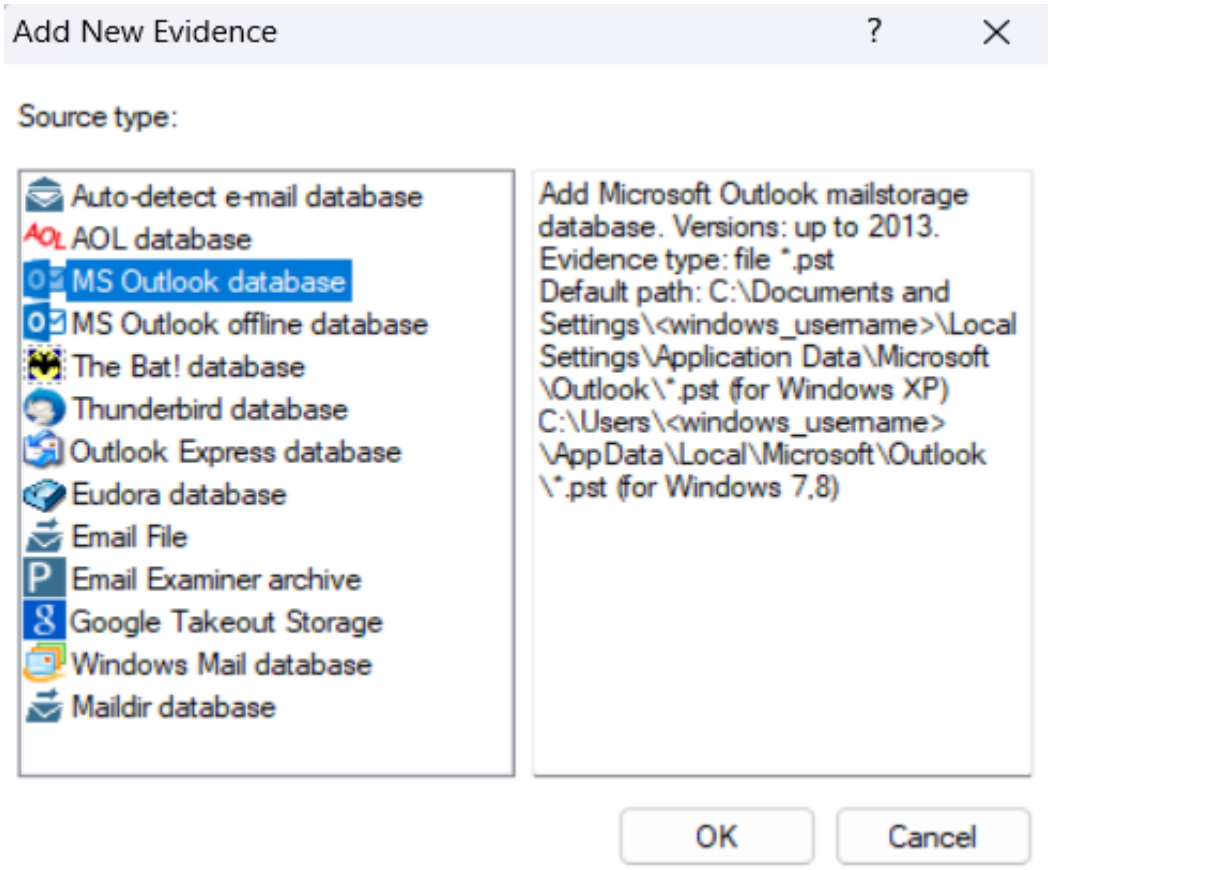


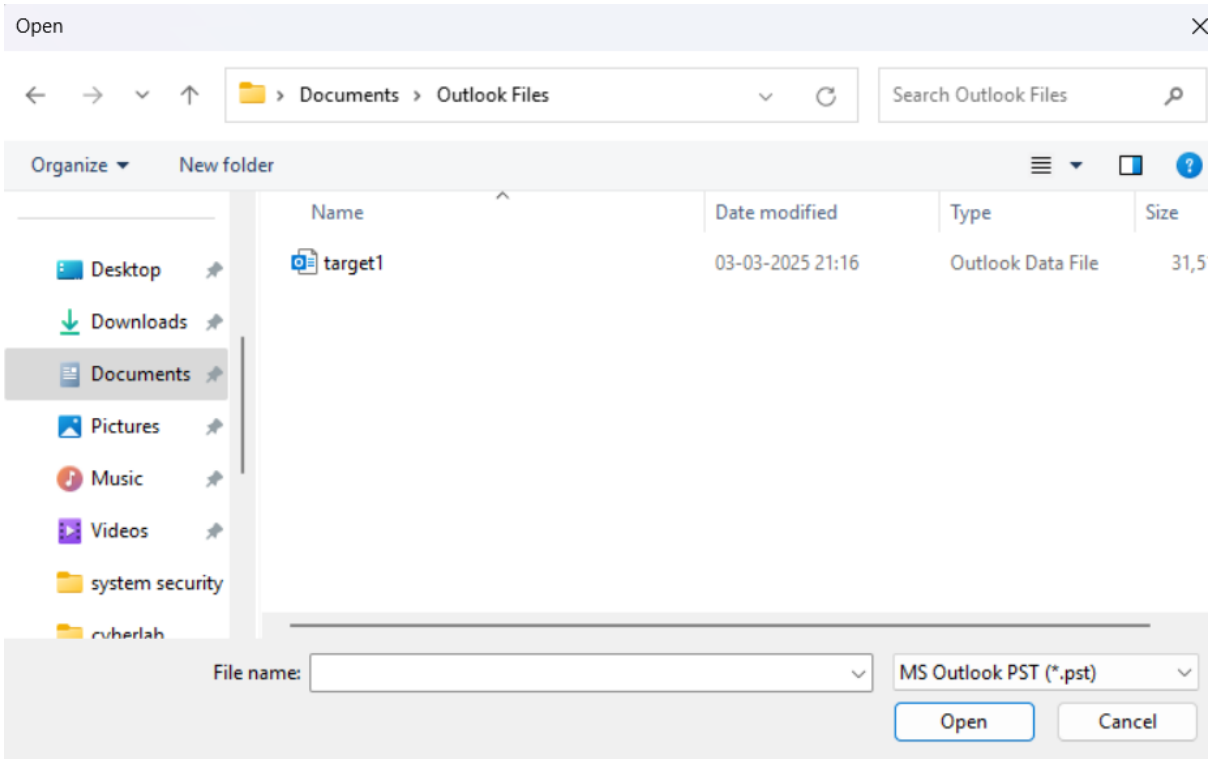
On the Additional information tab, fill all the fields and click the finish button.

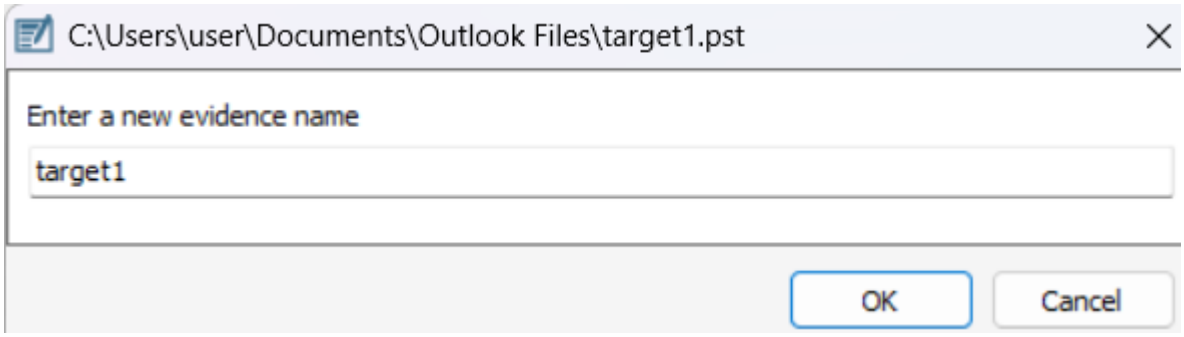


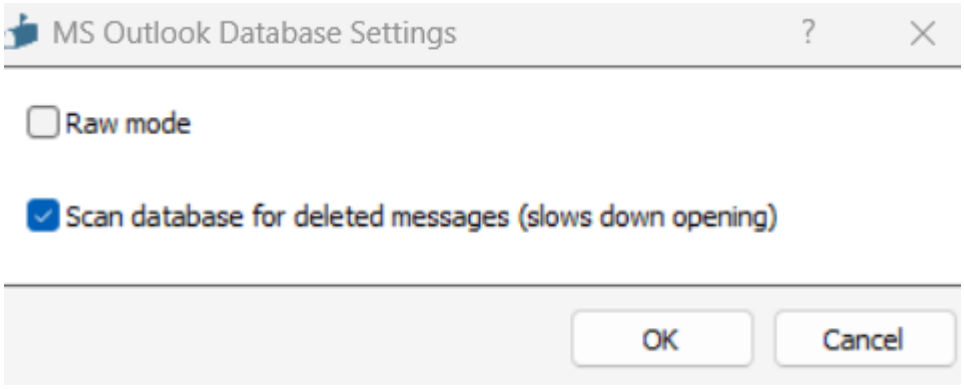
After clicking finish, a new case creation window appears.select the desired path.

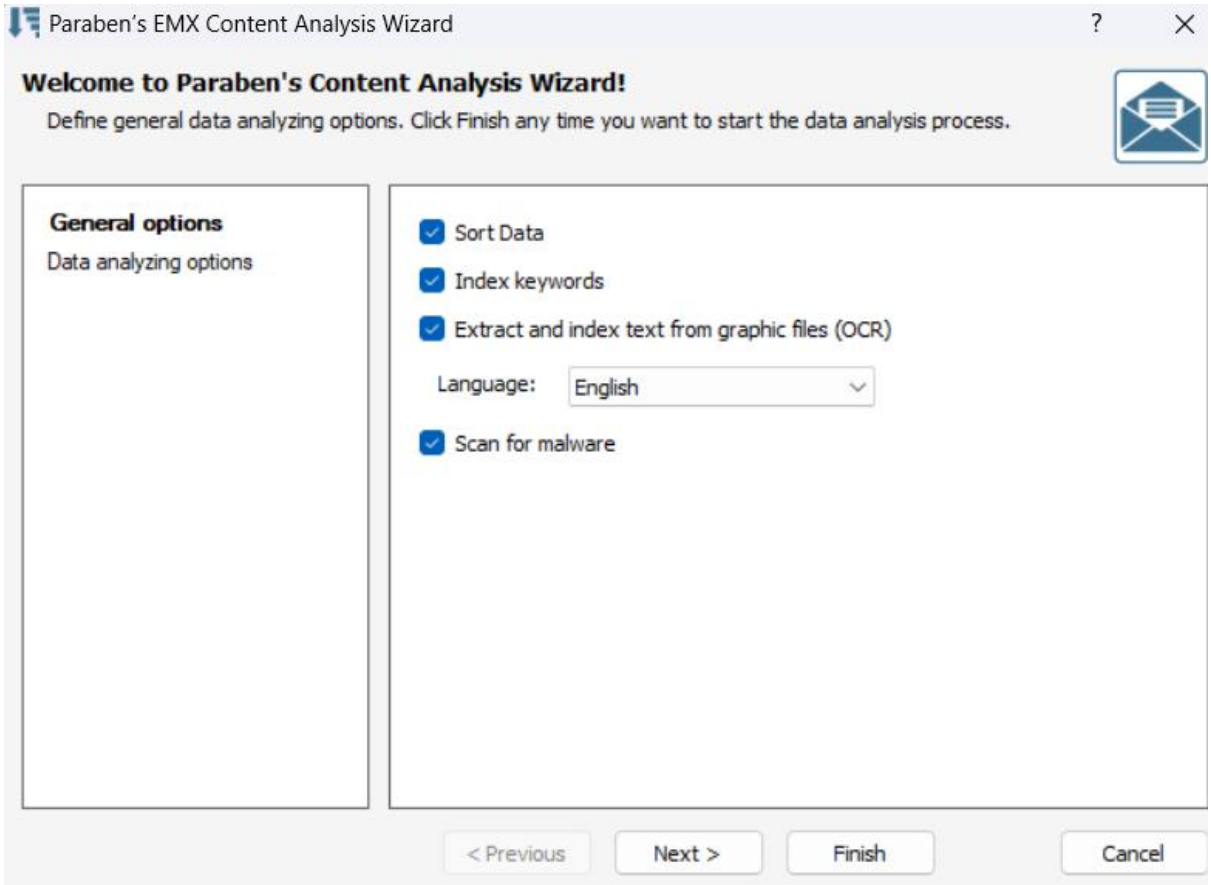


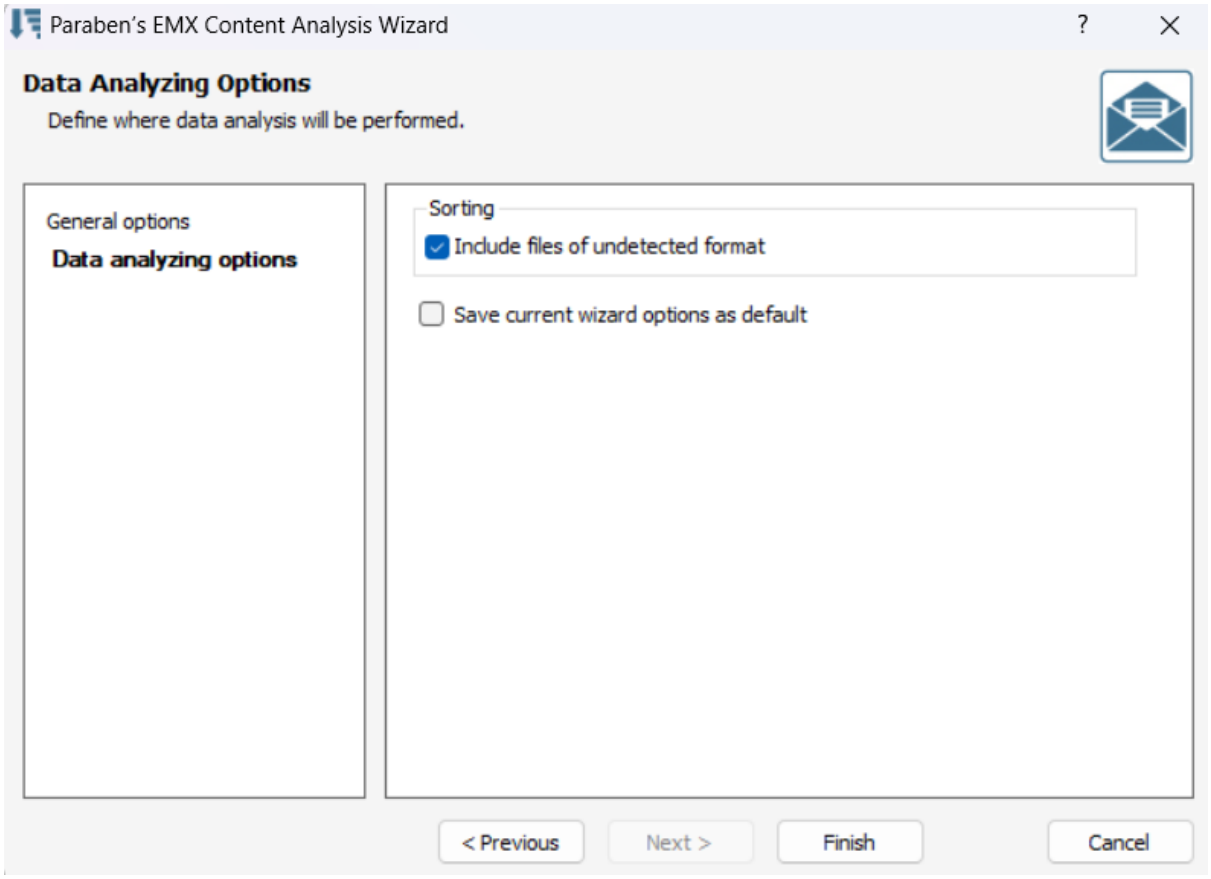

Add New Evidence
Source type:
Auto-detect e-mail database
AOL database
MS Outlook database
MS Outlook offline database
The Bat! database
Thunderbird database
Outlook Express database
Eudora database
Email File
Email Examiner archive
Google Takeout Storage
Windows Mail database
Maildir database
Add Microsoft Outlook mailstorage database. Versions: up to 2013.
Evidence type: file *.pst
Default path: C:\Documents and Settings\<windows_username>\Local Settings\Application Data\Microsoft\Outlook*.pst (for Windows XP)
C:\Users\<windows_username>\AppData\Local\Microsoft\Outlook*.pst (for Windows 7,8)
OK
Cancel

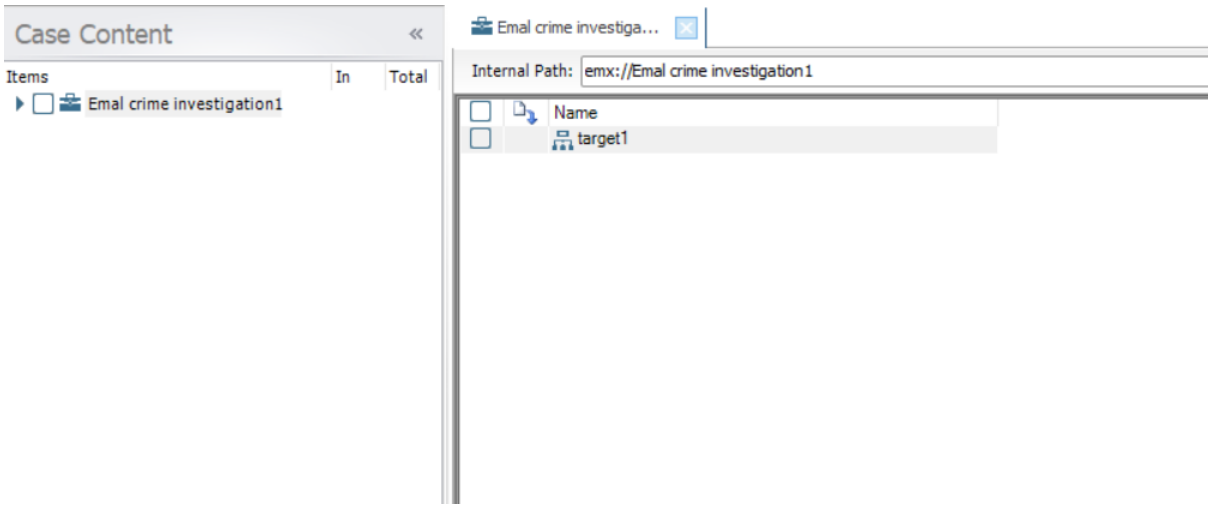

Open
Documents
Outlook Files
Search Outlook Files
Organize
New folder
Name
Date modified
Type
Size
target1
03-03-2025 21:16
Outlook Data File
31,5
Desktop
Downloads
Documents
Pictures
Music
Videos
system security
File name:
MS Outlook PST (*.pst)
Open
Cancel

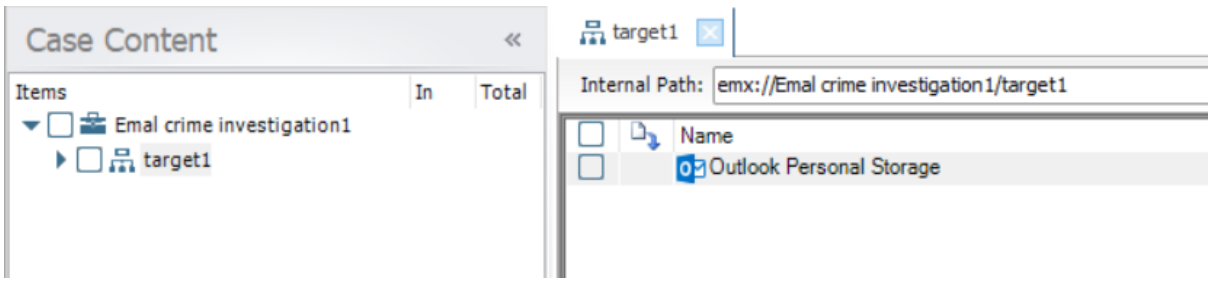

C:\Users\user\Documents\Outlook Files\target1.pst
Enter a new evidence name
target1
OK
Cancel

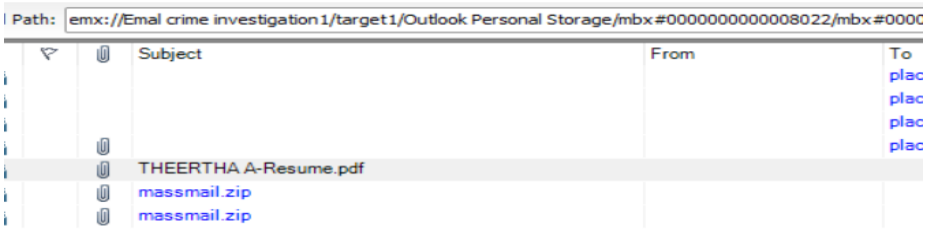

MS Outlook Database Settings
Raw mode
Scan database for deleted messages (slows down opening)
OK
Cancel

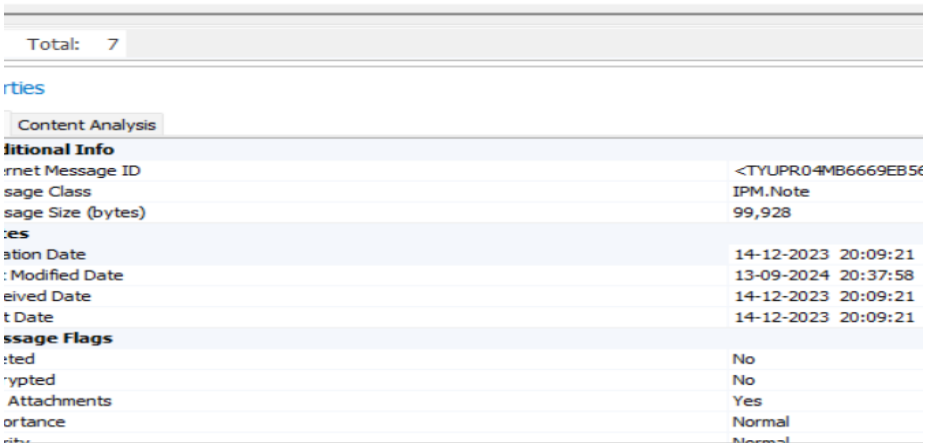

Paraben's EMX Content Analysis Wizard
Welcome to Paraben's Content Analysis Wizard!
Define general data analyzing options. Click Finish any time you want to start the data analysis process.
General options
Data analyzing options
Sort Data
Index keywords
Extract and index text from graphic files (OCR)
Language:
English
Scan for malware
< Previous
Next >
Finish
Cancel

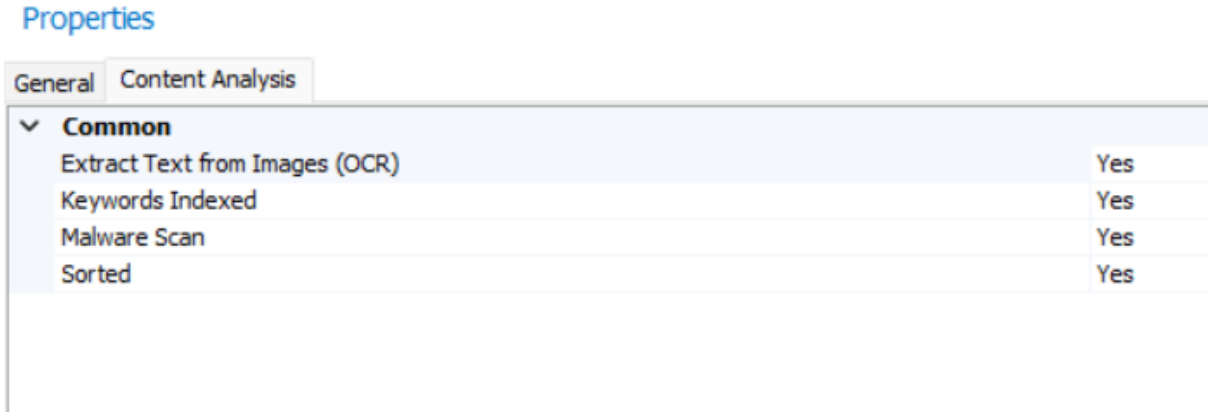

Paraben's EMX Content Analysis Wizard
Data Analyzing Options
Define where data analysis will be performed.
General options
Data analyzing options
Sorting
Include files of undetected format
Save current wizard options as default
< Previous
Next >
Finish
Cancel


Case Content
Items
In
Total
Emal crime investigation1
Emal crime investiga...
Internal Path: emx://Emal crime investigation1
Name
target1


Case Content
Items
In
Total
Emal crime investigation1
target1
target1
Internal Path: emx://Emal crime investigation1/target1
Name
Outlook Personal Storage


Path: emx://Emal crime investigation1/target1/Outlook Personal Storage/mbx#0000000000008022/mbx#0000
Subject
From
To
plac
plac
plac
plac
THEERTHA A-Resume.pdf
massmail.zip
massmail.zip


Total: 7
rties
Content Analysis
ditional Info
rnet Message ID
<TYUPR04MB6669EB56
sage Class
IPM.Note
sage Size (bytes)
99,928
ces
ation Date
14-12-2023 20:09:21
Modified Date
13-09-2024 20:37:58
eived Date
14-12-2023 20:09:21
t Date
14-12-2023 20:09:21
ssage Flags
ted
No
ypted
No
Attachments
Yes
ortance
Normal


Properties
General
Content Analysis
Common
Extract Text from Images (OCR)
Yes
Keywords Indexed
Yes
Malware Scan
Yes
Sorted
Yes


Finished Total: 7
E-mail Data
<No Subject>
To: placement@cethalassery.ac.in <placement@cethalassery.ac.in>

Tracing an Email Using the eMailTrackerPro Tool

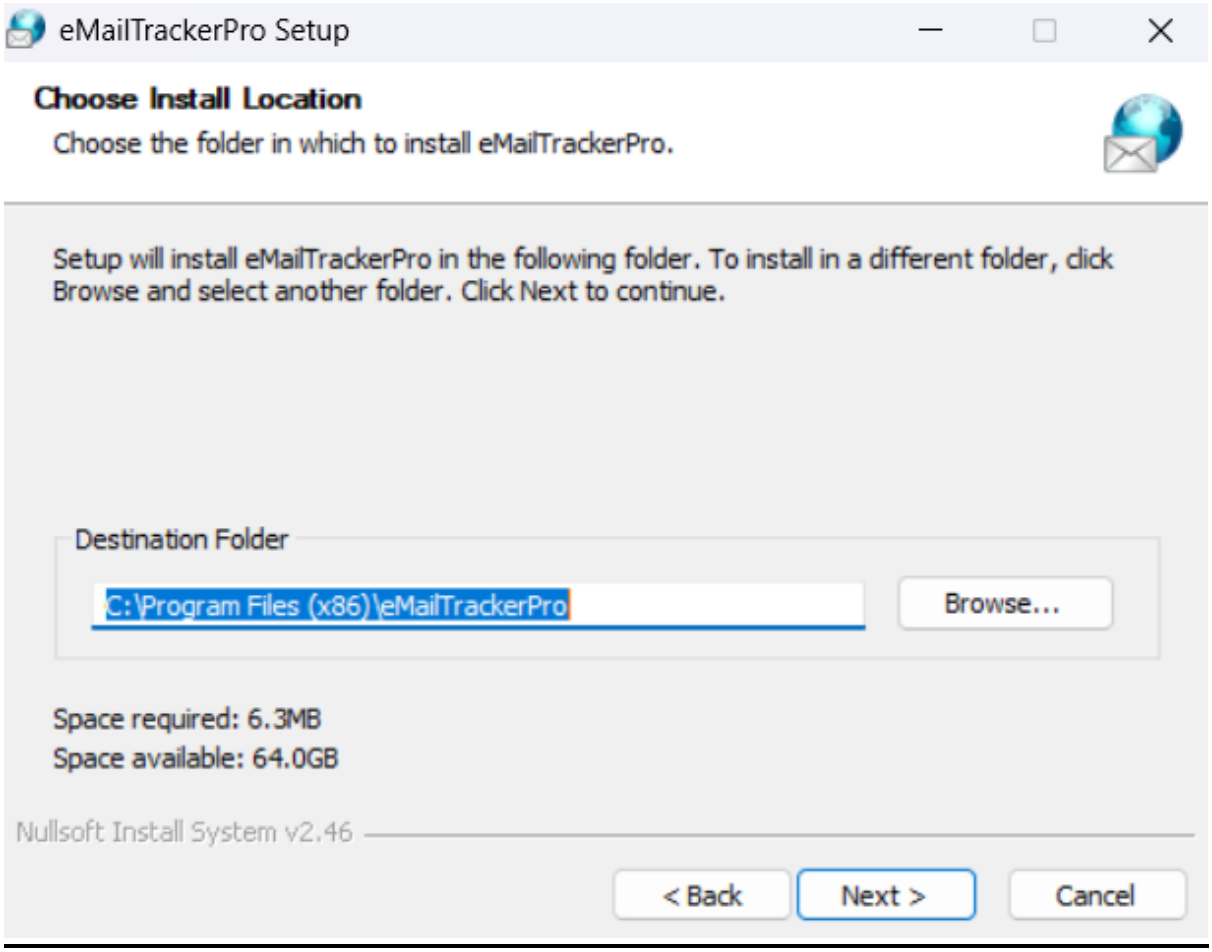
Lab objective:

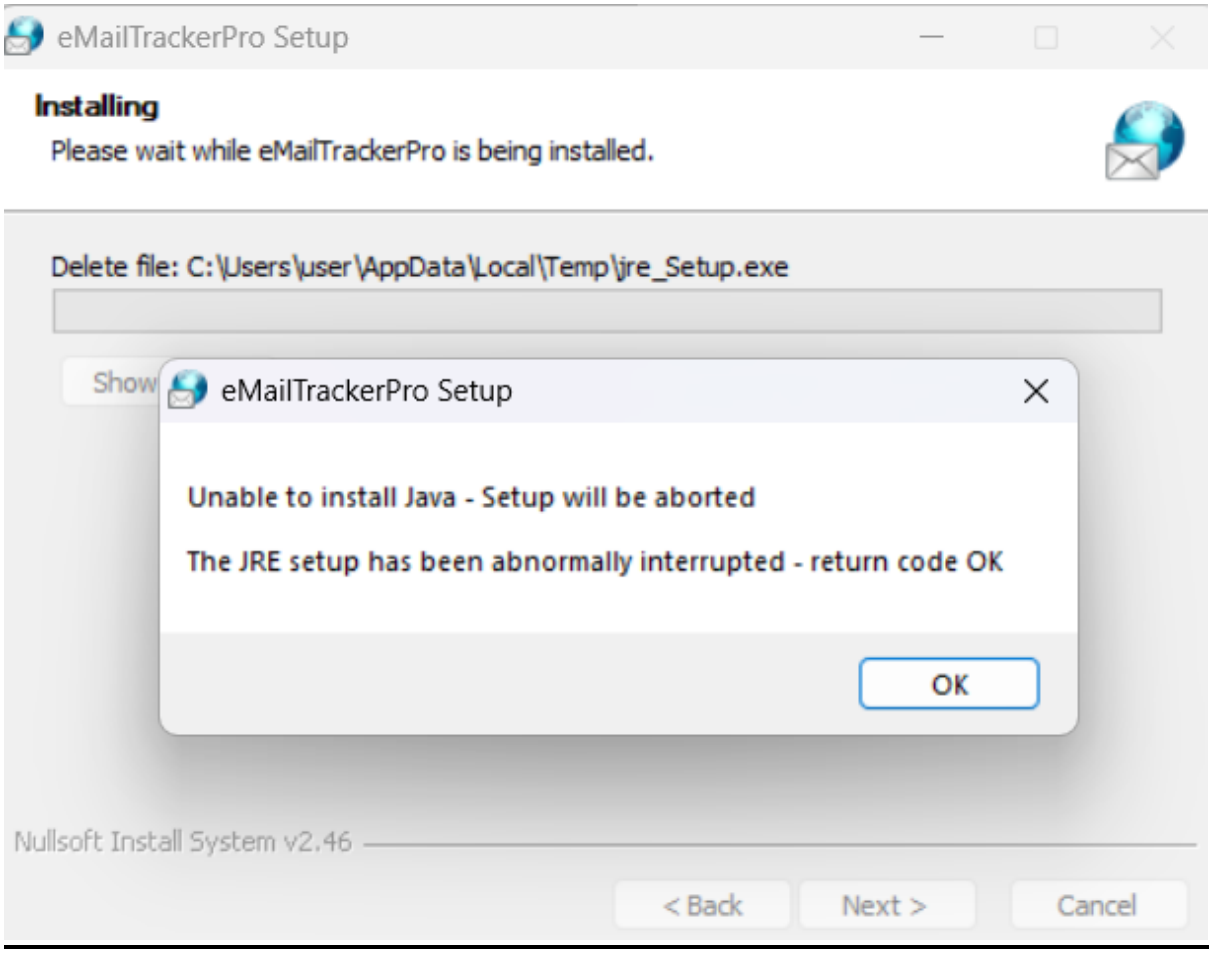
The objective of this lab is to demonstarate email tracing using eMailTrackerpro

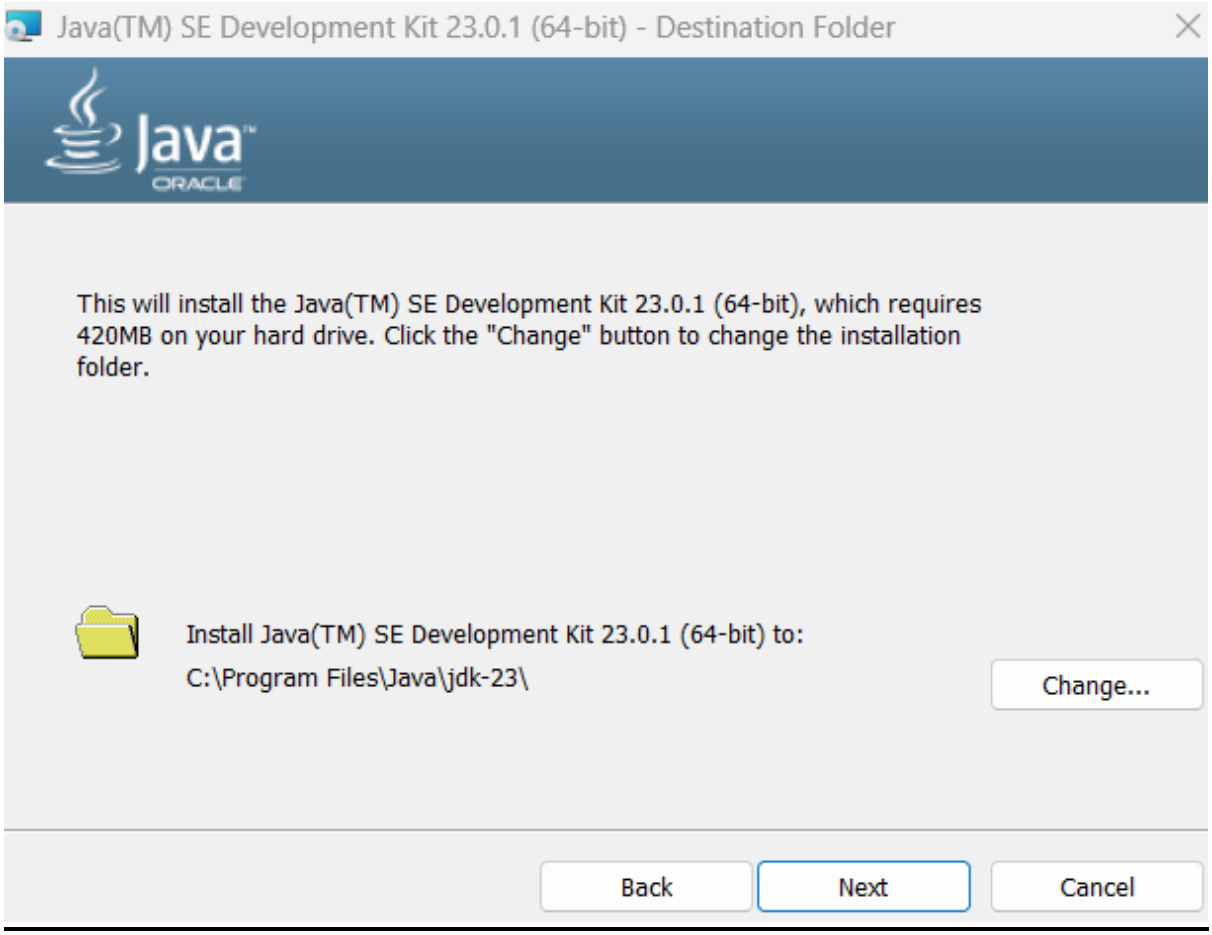
Forensic investigators will learn how to:

How to trace an email to its geographical source.

Collect Network(ISP) and Domain Whos information for any email traced.




eMailTrackerPro Setup
Installing
Please wait while eMailTrackerPro is being installed.
Delete file: C:\Users\user\AppData\Local\Temp\jre_Setup.exe
Show
eMailTrackerPro Setup
Unable to install Java - Setup will be aborted
The JRE setup has been abnormally interrupted - return code OK
OK
Nullsoft Install System v2.46
< Back
Next >
Cancel



I m not able to install this tool.

eMailTrackerPro is an email forensics tool used to analyze email headers and determine the sender's location and network information. It helps cybersecurity professionals and forensic investigators detect phishing, email spoofing, and spam attacks.

Key Features of eMailTrackerPro

- Email Header Analysis
  - Extracts information from the email header to trace the originating IP address.
  - Detects hidden relays, proxies, and spoofed addresses.
- Geolocation and IP Tracking
  - Identifies the approximate geographical location of the sender.
  - Determines the Internet Service Provider (ISP) of the email sender.
- Domain WHOIS Lookup

- Fetches WHOIS records of domains linked to the email.
- Provides details like domain owner, registration date, and contact information.

◆ Spam and Phishing Detection

- Helps detect fraudulent emails by analyzing mail servers and relay paths.
- Identifies if an email has passed through blacklisted or suspicious servers.

Working of emailTrackerPro

1. The investigator copies the email header from an email.
2. The header is pasted into eMailTrackerPro for analysis.
3. The tool extracts the originating IP address and maps it to a geographical location.
4. The ISP and domain information are retrieved for further investigation.
5. The results help determine if the email is legitimate or fraudulent.