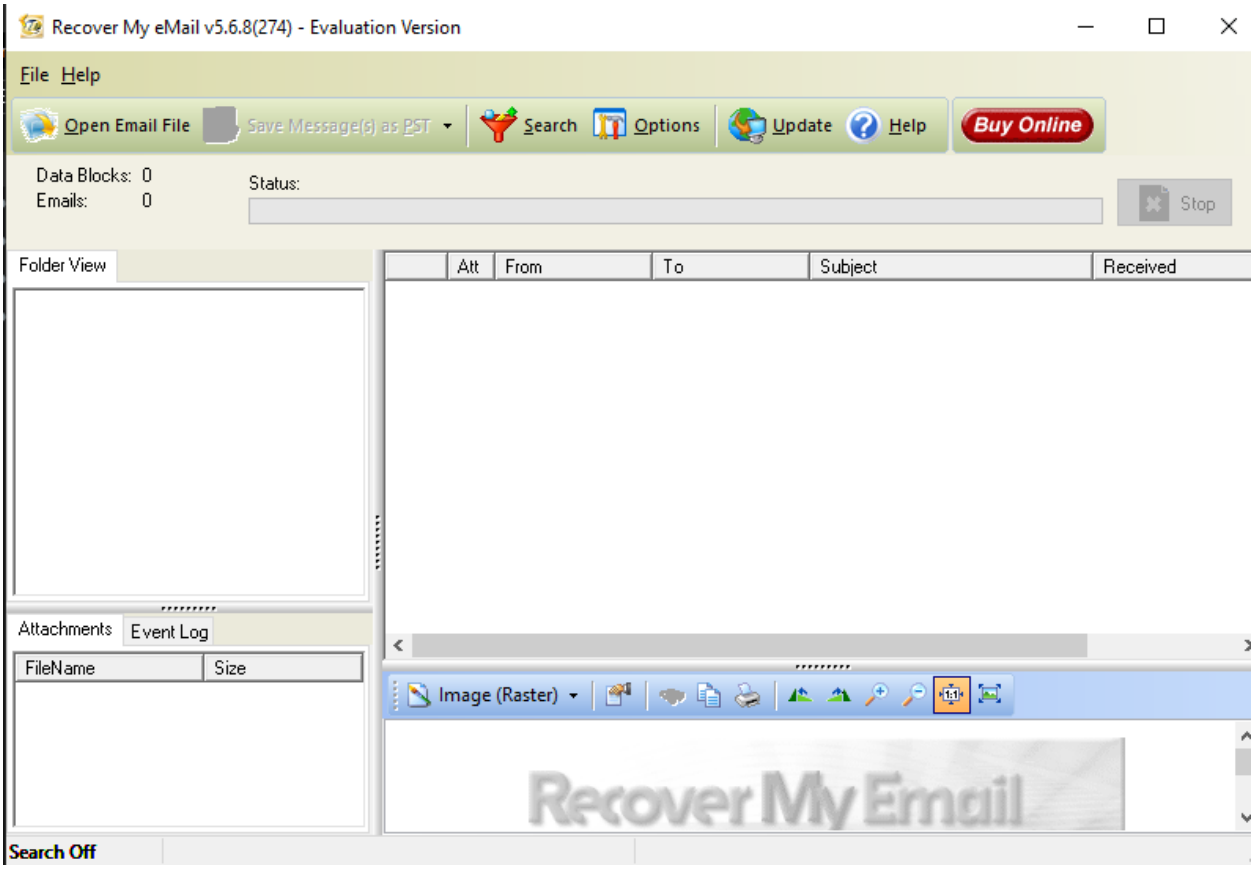
Karthikeyan G

CB.SC.P2CYS24008

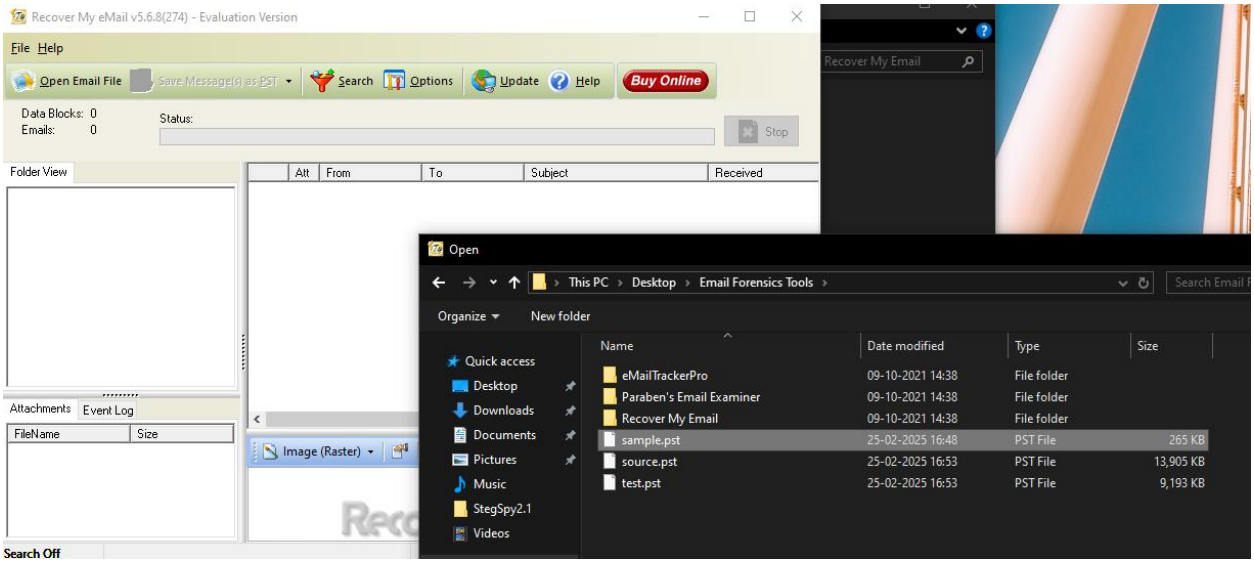
Digital Forensics
LAB 06 - Investigating Email Crimes

Recovering Deleted Emails Using *Recover My Email*

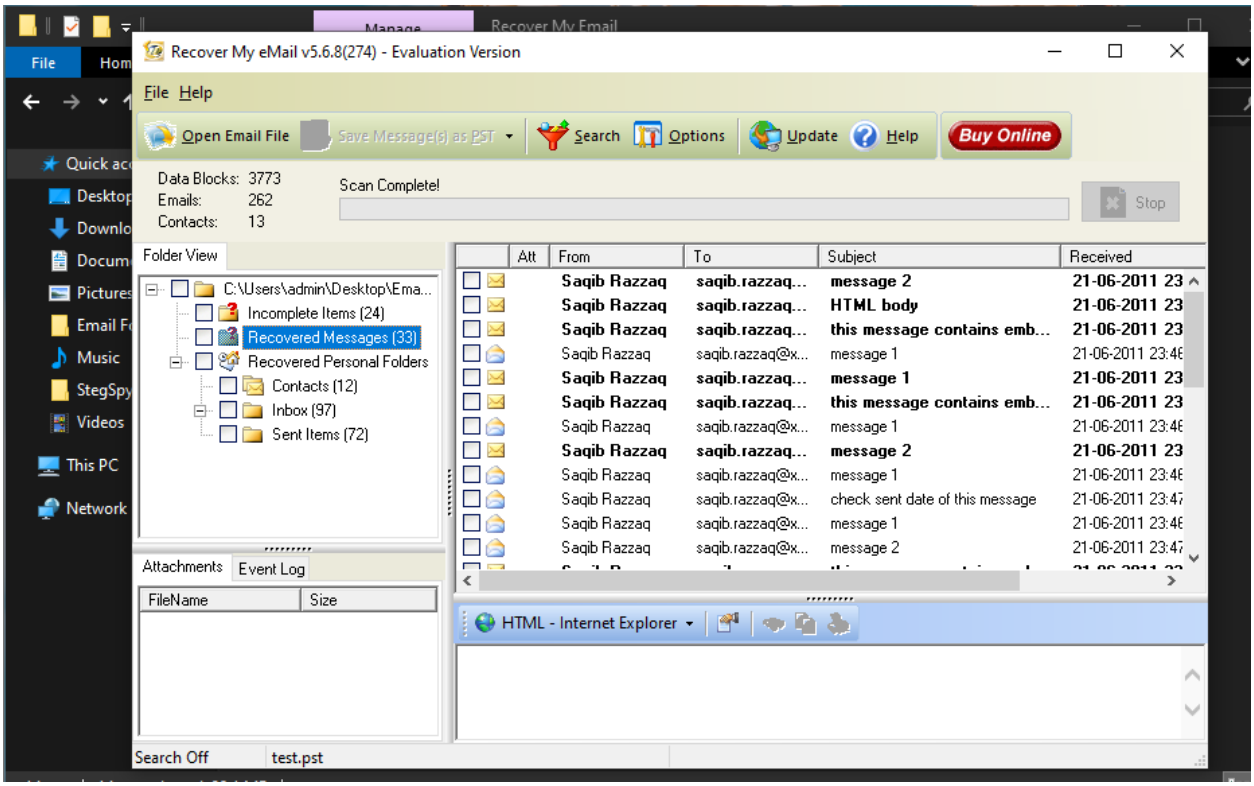
The first step in this process is to install *Recover My Email* software. This tool helps retrieve deleted emails, which can be crucial in digital forensic investigations.



Let's open a .pst file and run a scan to identify any deleted emails.

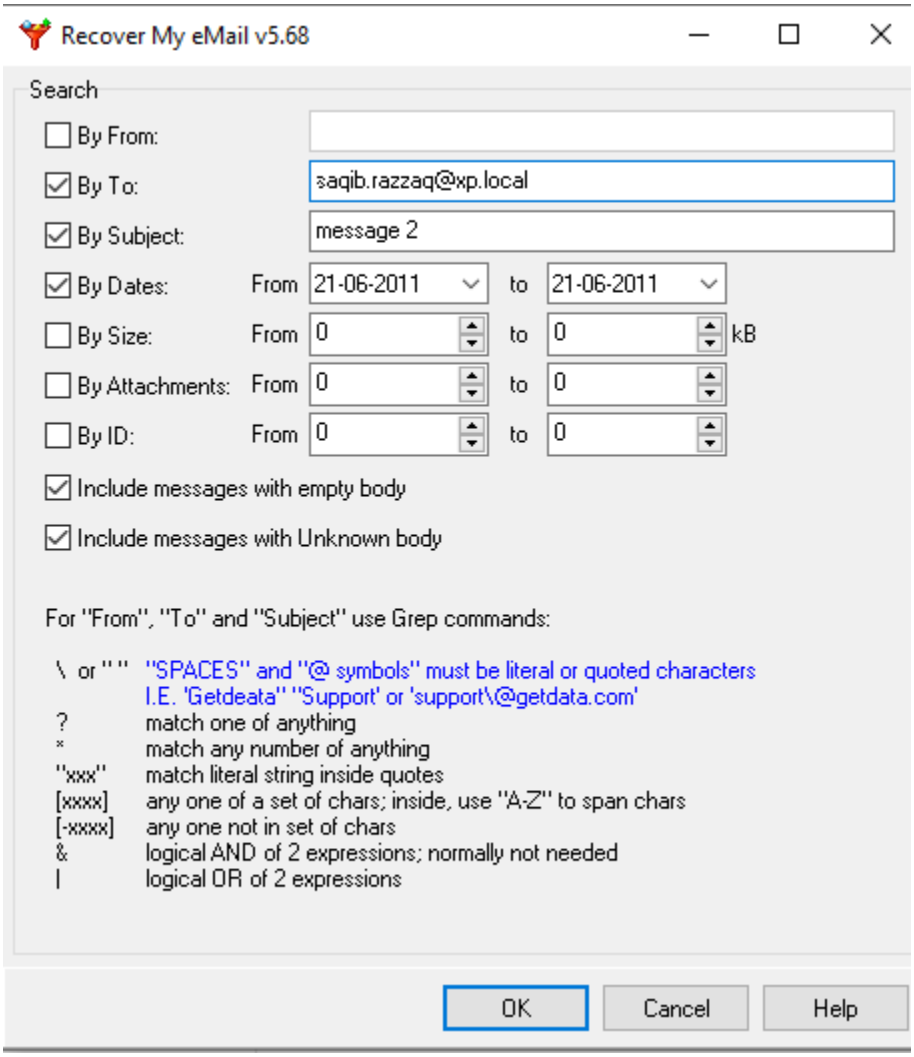


- Navigate to: **Desktop → Email Forensics Tools**
- Select **`test.pst`** (Size: 9,193 KB).

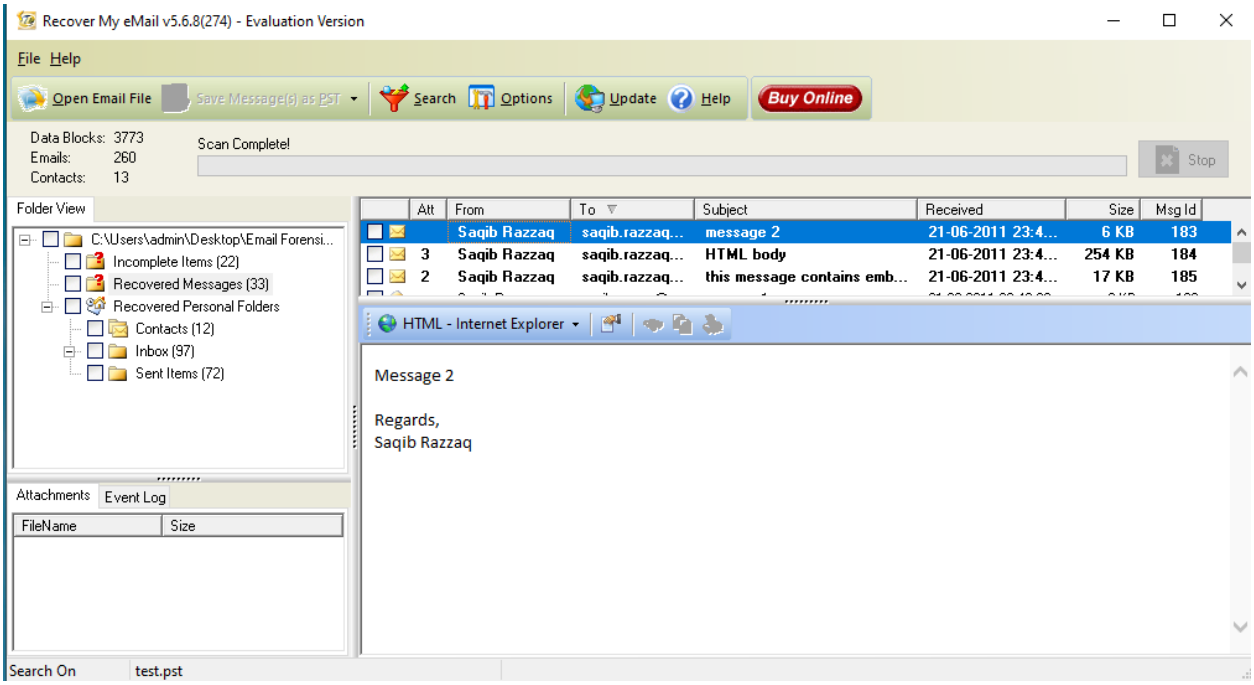


Let's review the emails we have successfully recovered.

Now, let's search for an email sent to a specific recipient with a particular subject and date.

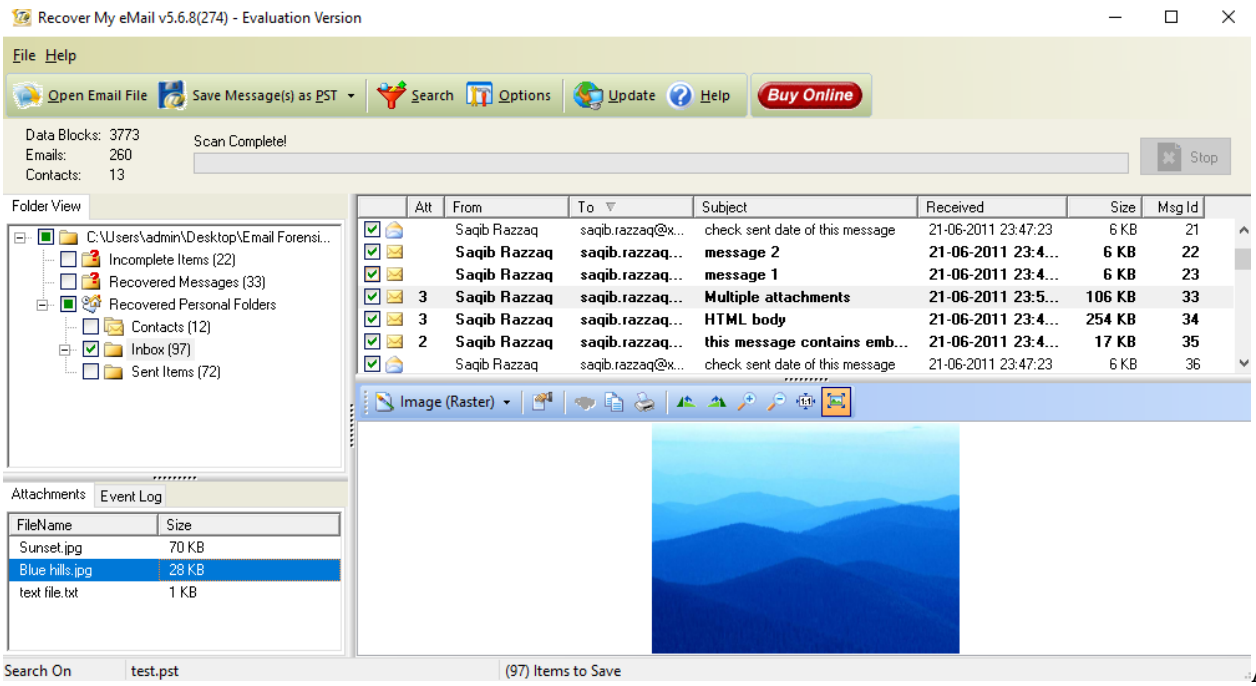


We can now view the filtered results.



If needed, you can save the selected messages as a .pst file.

Now, let's review the attachments in the email.

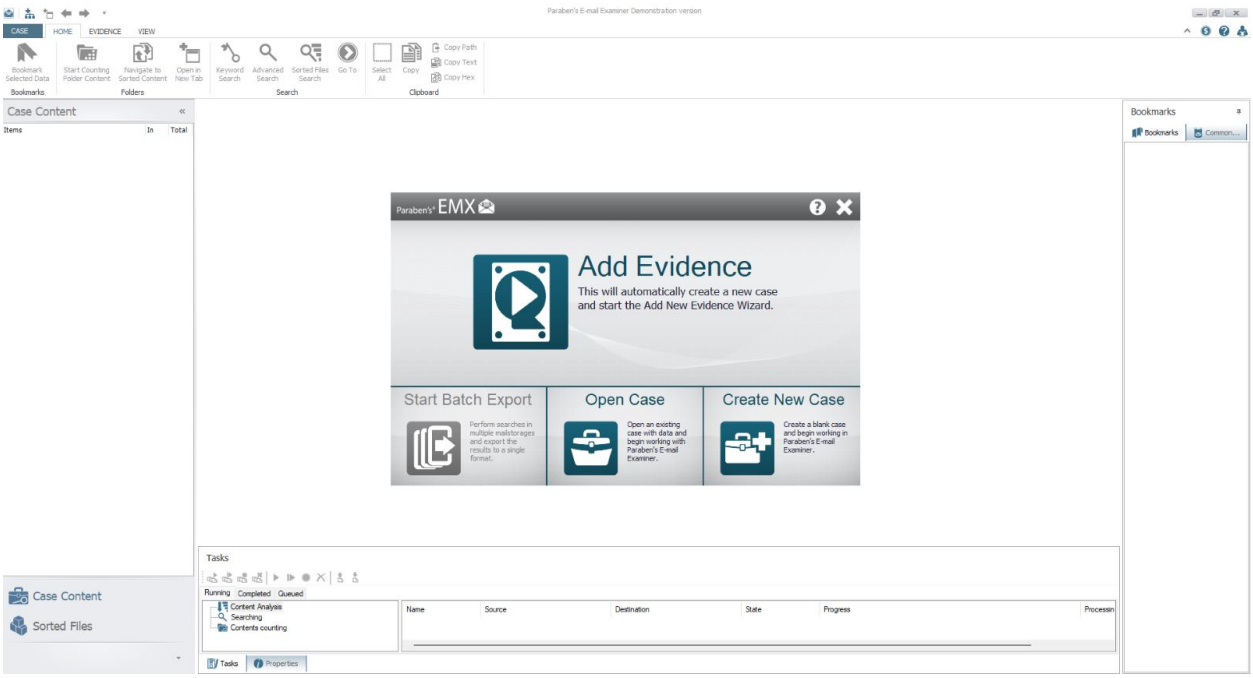


Attachments:

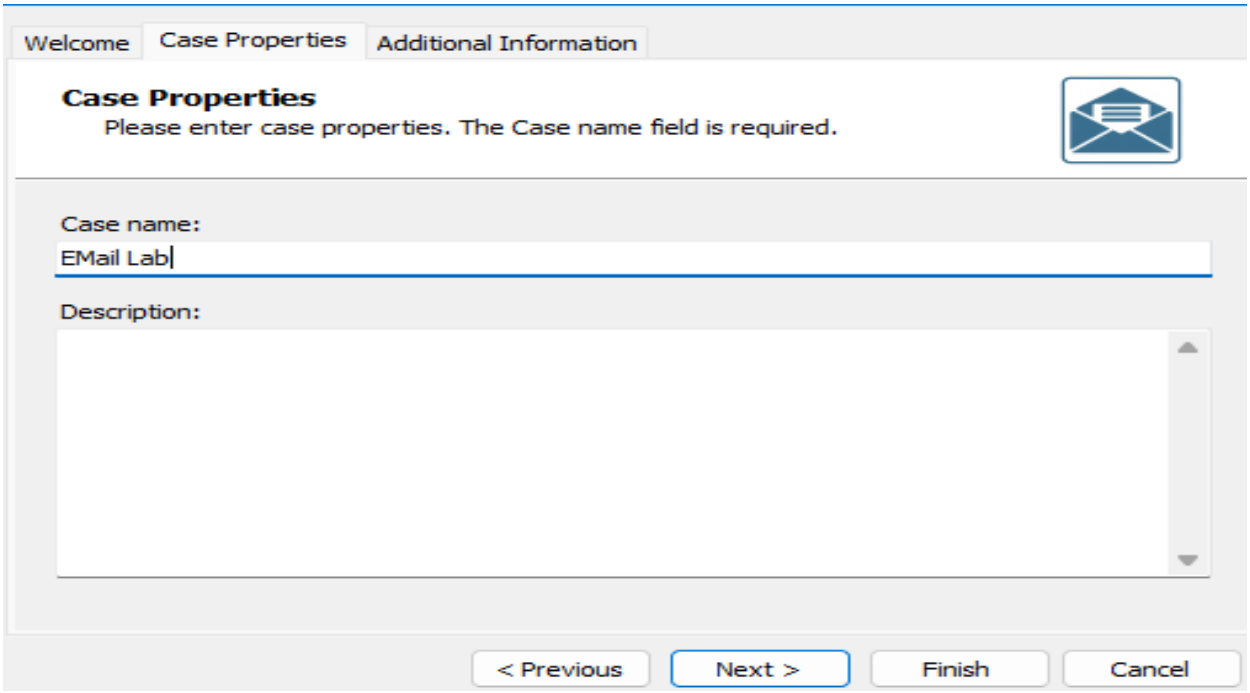
- Three attachments are listed:
  - *Sunset.jpg* (70 KB)
  - *Blue hills.jpg* (28 KB) – currently previewed in the software.
  - *text file.txt* (1 KB)
- The preview window displays the **"Blue hills.jpg"** image.

Investigating Email Crimes Using Paraben's Email Examiner Tool

The first step is to install the *Paraben's Email Examiner* tool.



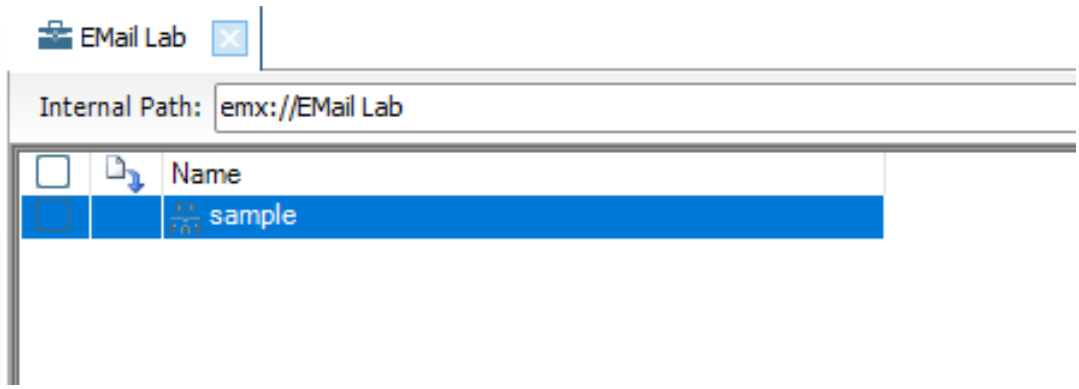
Now, let's create a new case.



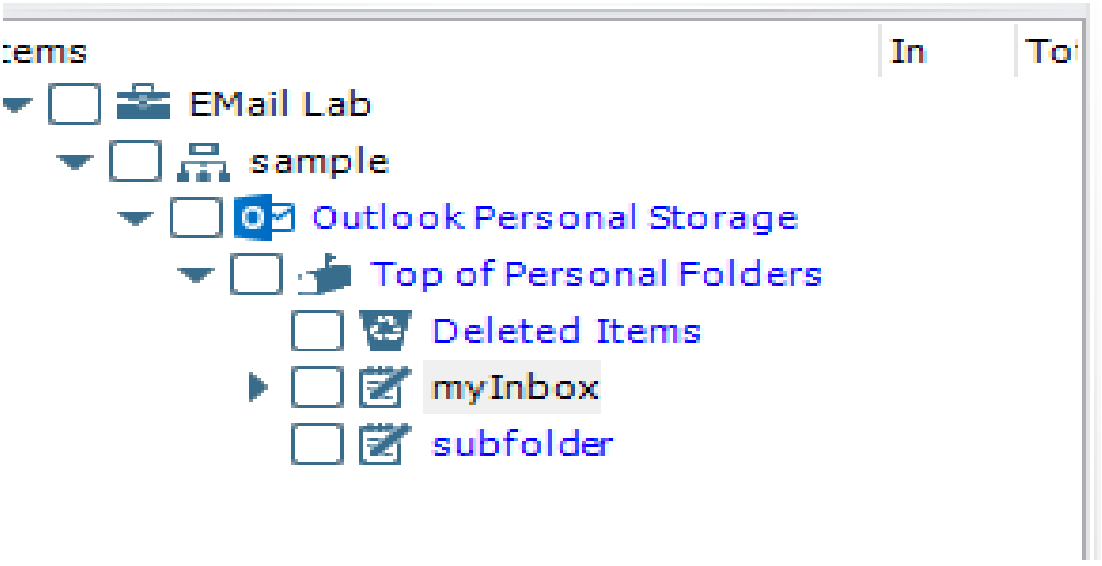
Filled Fields:

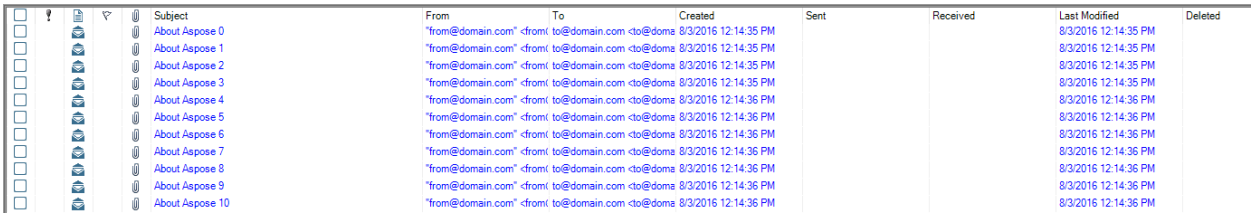
- **Investigator Name:** *Karthikeyan*
- **Agency/Company:** *Cyber Forensics Lab*
- **Phone:** *+91 98765 43210*
- **Fax:** *+91 4422334455*
- **Address:** *123, Digital Forensics Street, Chennai, India*
- **E-mail:** *karthikeyan@cyberforensicslab.com*
- **Comments:** *Investigating email fraud case related to phishing attacks.*

Now, let's add our email file to the case for analysis.



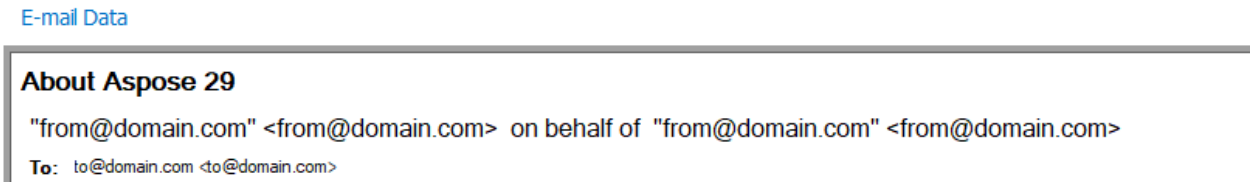
Now, let's proceed with analyzing the email.





Observation: Email Analysis Using Paraben's Email Examiner

1. **Email List Overview:**
    a. The displayed emails have the subject **"About Aspose X"**, where X represents different numbers.
    b. All emails are from **"from@domain.com"** and have the same sender domain.
    c. The emails were **created, last modified, and possibly deleted** on the same date and time (8/22/16 at 12:34 PM).
    d. The "Received" and "Sent" columns are empty, which may indicate missing metadata or incomplete recovery.



Email Details (Second Image):

- The selected email has the subject **"About Aspose 29."**
- The sender is listed as **"from@domain.com"**, with the same address appearing in the "on behalf of" section.
- The recipient is **"to@domain.com"**, suggesting a generic or placeholder email structure.

otential Issues & Analysis:

- The identical timestamps and structured email names indicate **automated or scripted email generation**.
- The "on behalf of" field suggests **email spoofing** or possible **phishing activity**.
- The missing "Received" and "Sent" timestamps could indicate **manipulated email headers** or **recovered but incomplete emails**.

Tracing an Email Using the eMailTrackerPro Tool

Step 1: Installing the Tool

Before we begin email tracing, we need to install *eMailTrackerPro*.

Issue Encountered:

- The tool appears to be outdated and does not recognize the installed **Java Runtime Environment (JRE)**.
- Despite meeting all dependencies, the installation is unsuccessful.
- This is likely due to the service being **discontinued after 2022**, making it non-functional for current use.

Alternative Approach:

Since *eMailTrackerPro* is no longer supported, we can explore modern alternatives for email tracing, such as:

- **MX Toolbox** (Online email header analysis)
- **IP Tracker** (For IP lookup and geolocation)
- **Wireshark** (Packet analysis for email traffic)
- **Traceroute & WHOIS Tools** (For tracking email origin)