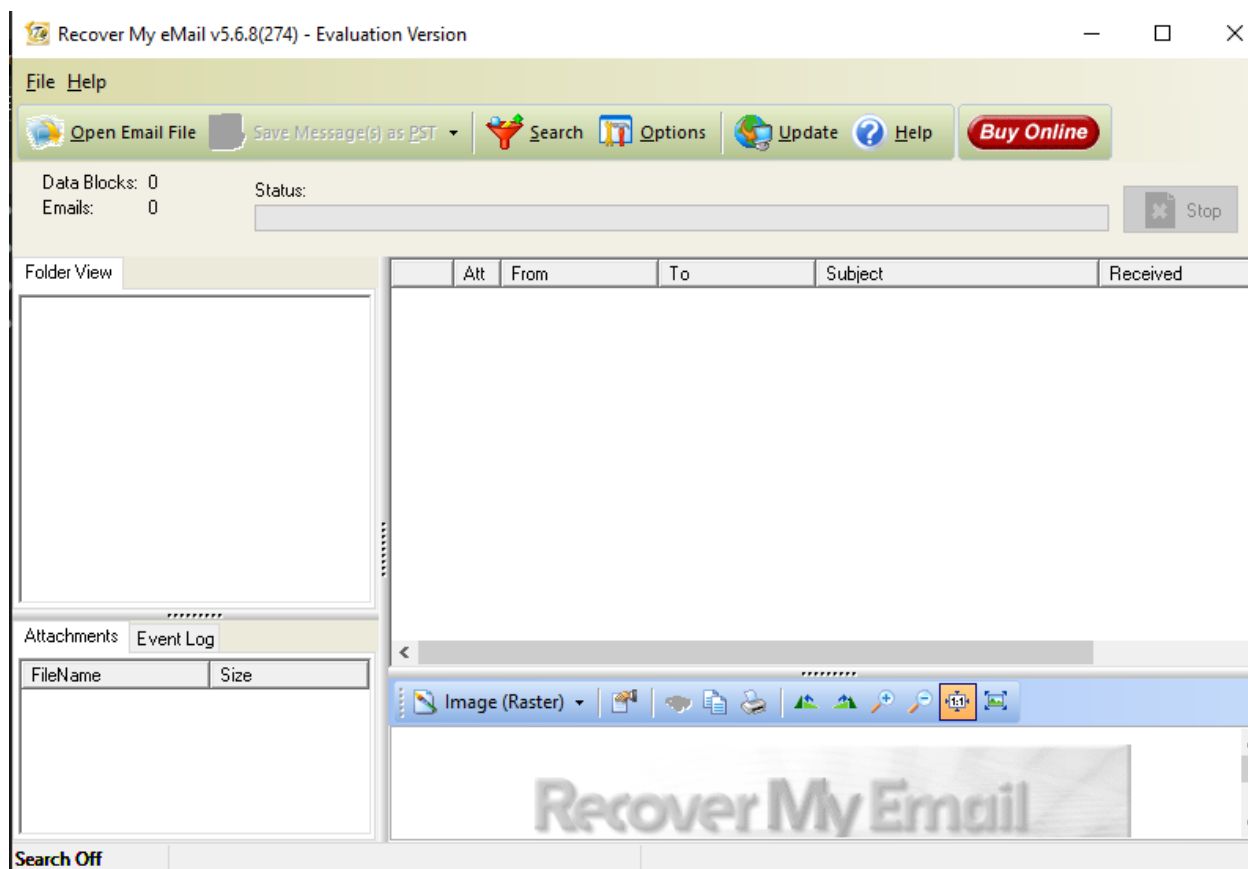


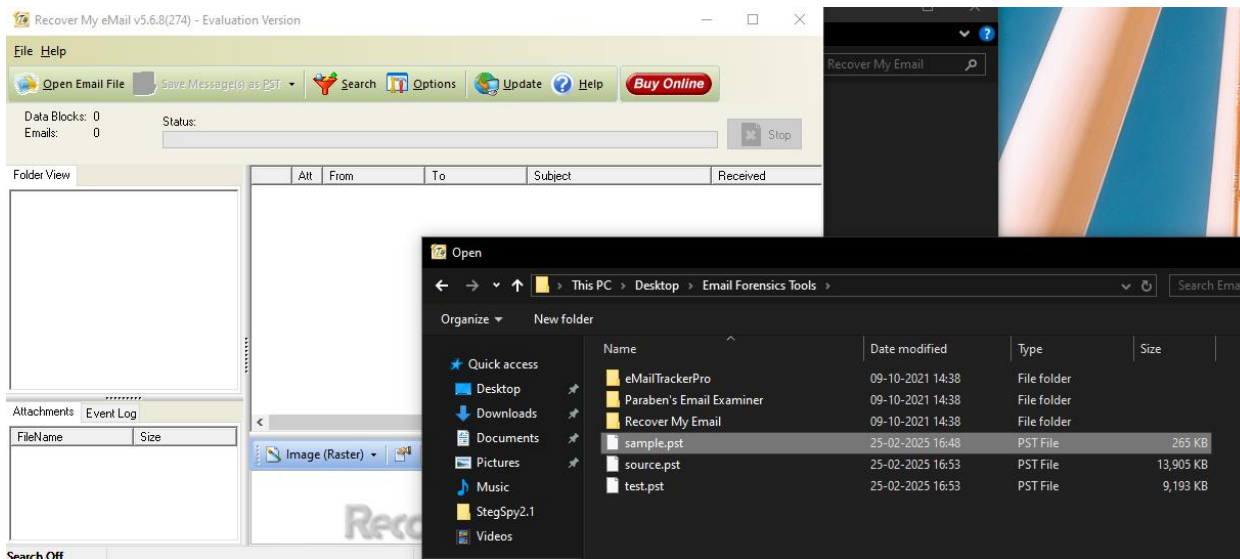
**Digital Forensics**  
**LAB 06 - Investigating Email Crimes**

**Recovering Deleted Emails Using *Recover My Email***

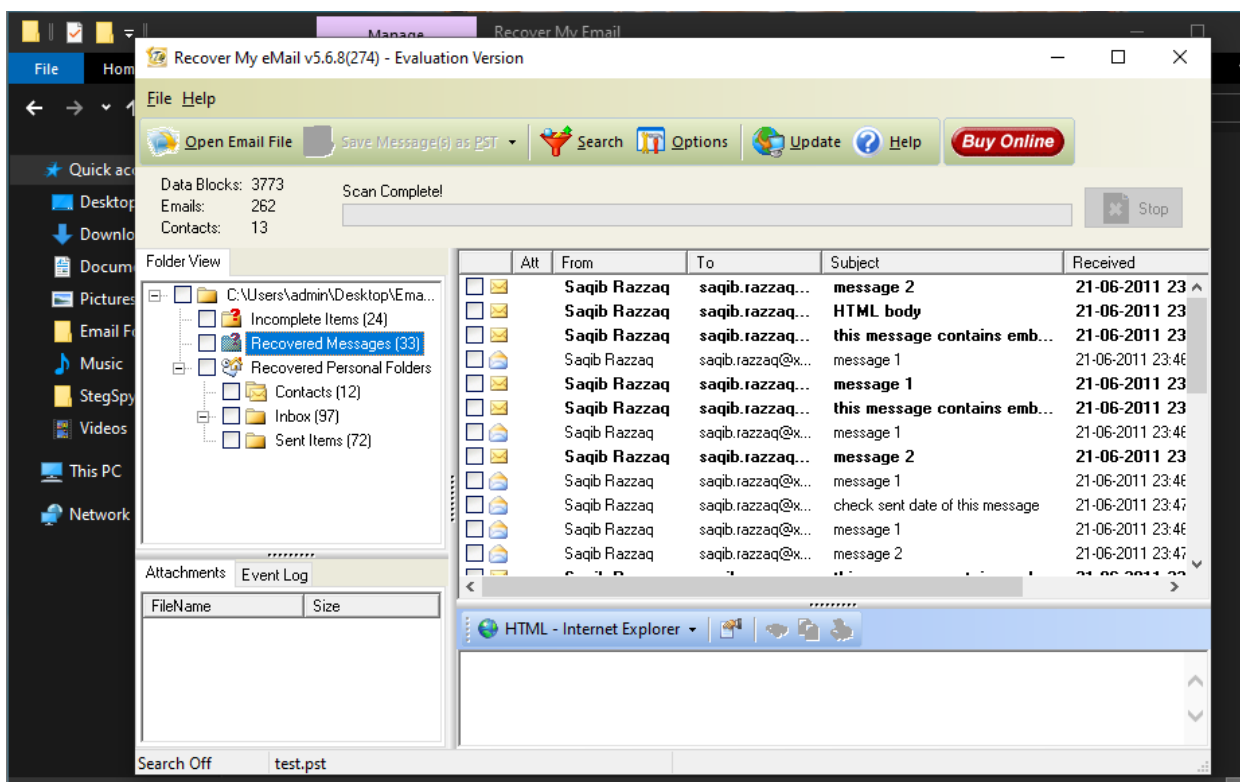
The first step in this process is to install *Recover My Email* software. This tool helps retrieve deleted emails, which can be crucial in digital forensic investigations.



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.

Recover My eMail v5.68

Search

☐ By From:

☒ By To: saqib.razzaq@xp.local

☒ By Subject: message 2

☒ By Dates: From 21-06-2011 to 21-06-2011

☐ By Size: From 0 to 0 kB

☐ By Attachments: From 0 to 0

☐ By ID: From 0 to 0

☒ Include messages with empty body

☒ Include messages with Unknown body

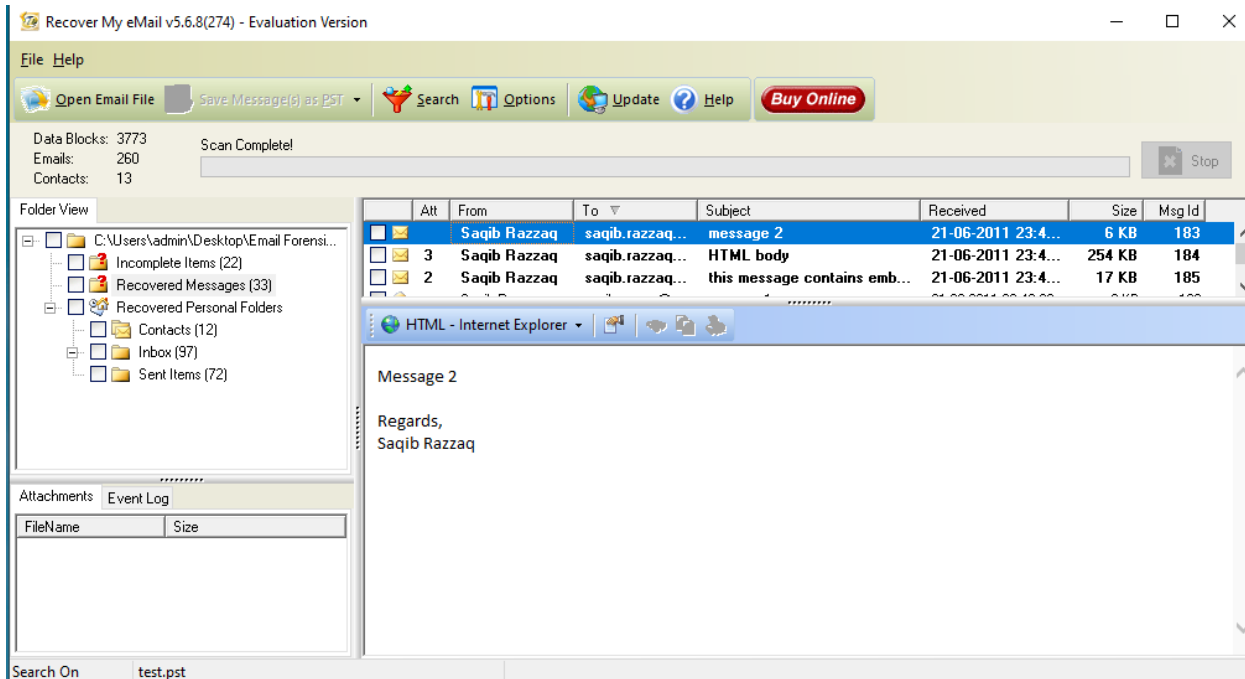
For "From", "To" and "Subject" use Grep commands:

\ or "" "SPACES" and "@ symbols" must be literal or quoted characters  
 I.E. 'Getdata' 'Support' or 'support\@getdata.com'

? match one of anything  
 \* match any number of anything  
 "xxx" match literal string inside quotes  
 [xxxx] any one of a set of chars; inside, use "A-Z" to span chars  
 [-xxxx] any one not in set of chars  
 & logical AND of 2 expressions; normally not needed  
 | logical OR of 2 expressions

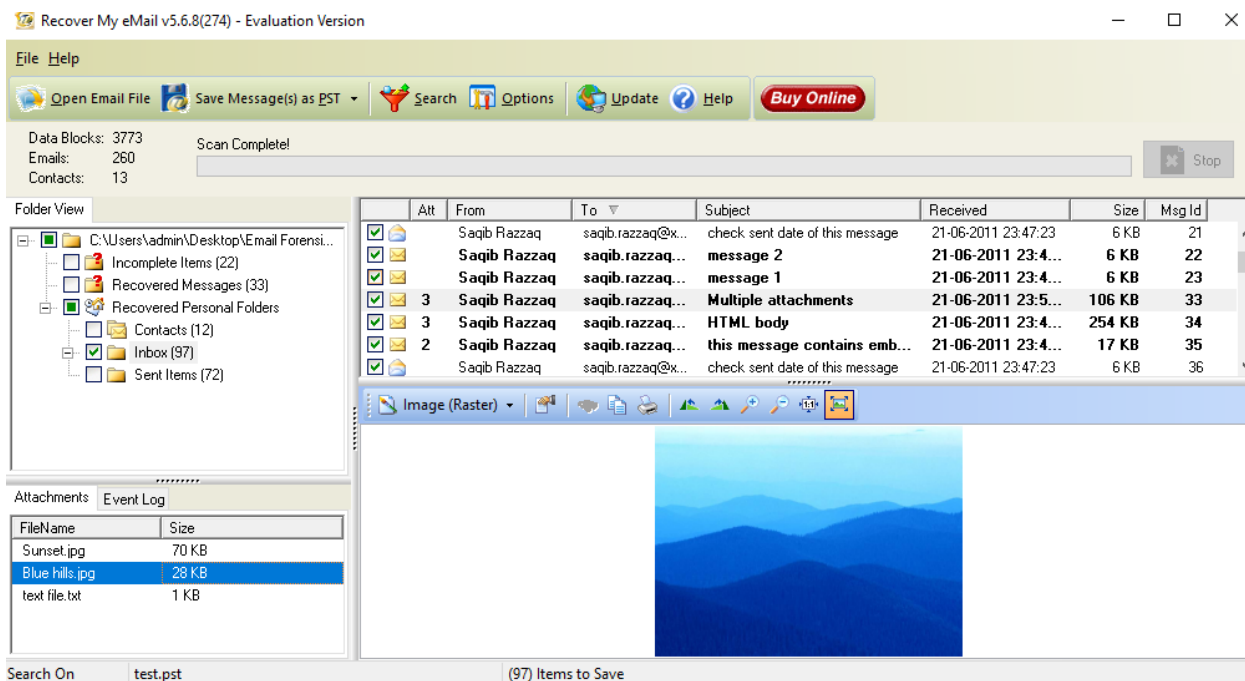
OK Cancel Help

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.

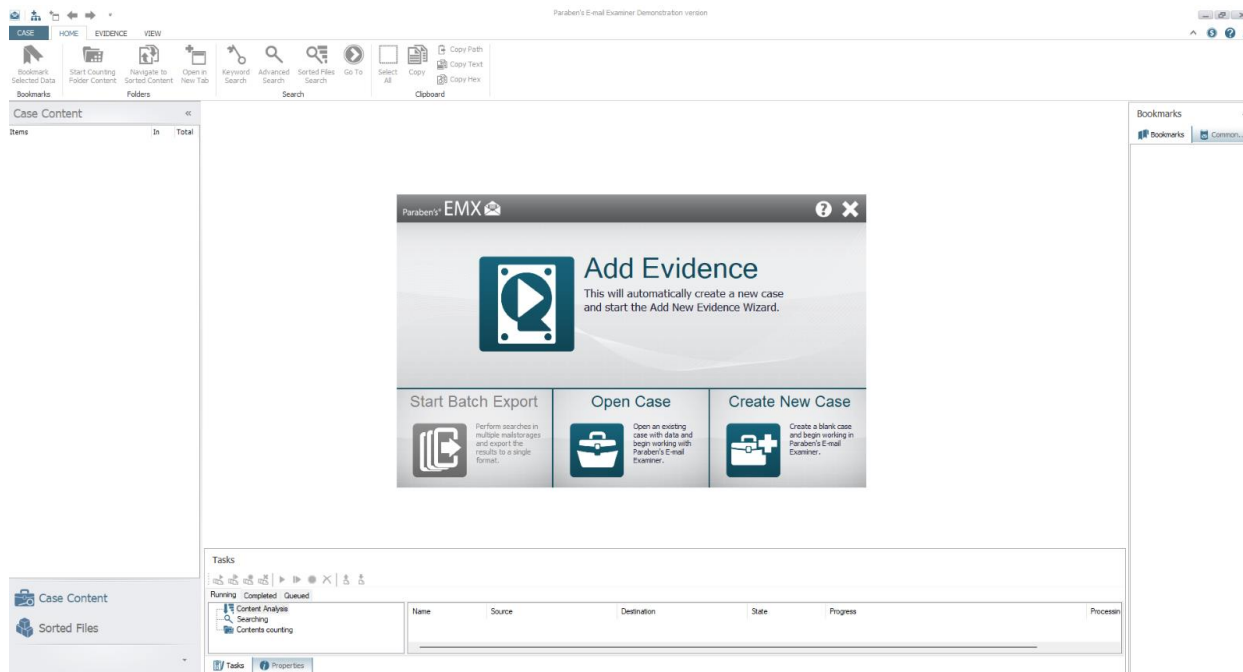


**Attachments:**

- 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.



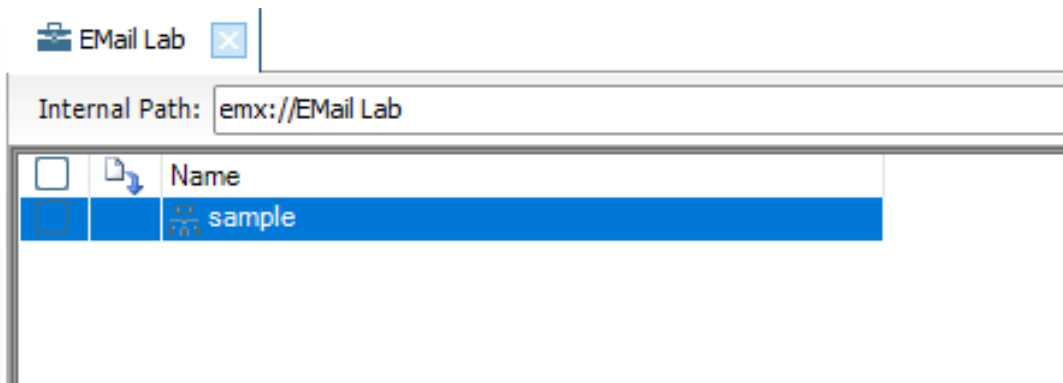
Now, let's create a new case.

The screenshot shows the "Case Properties" dialog box within the Paraben's Email Examiner application. The dialog has three tabs: "Welcome", "Case Properties", and "Additional Information". The "Case Properties" tab is active, displaying the text: "Please enter case properties. The Case name field is required." Below this, there is a "Case name:" label followed by a text input field containing "EMail Lab". Underneath, there is a "Description:" label followed by a large, empty text area. At the bottom of the dialog, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

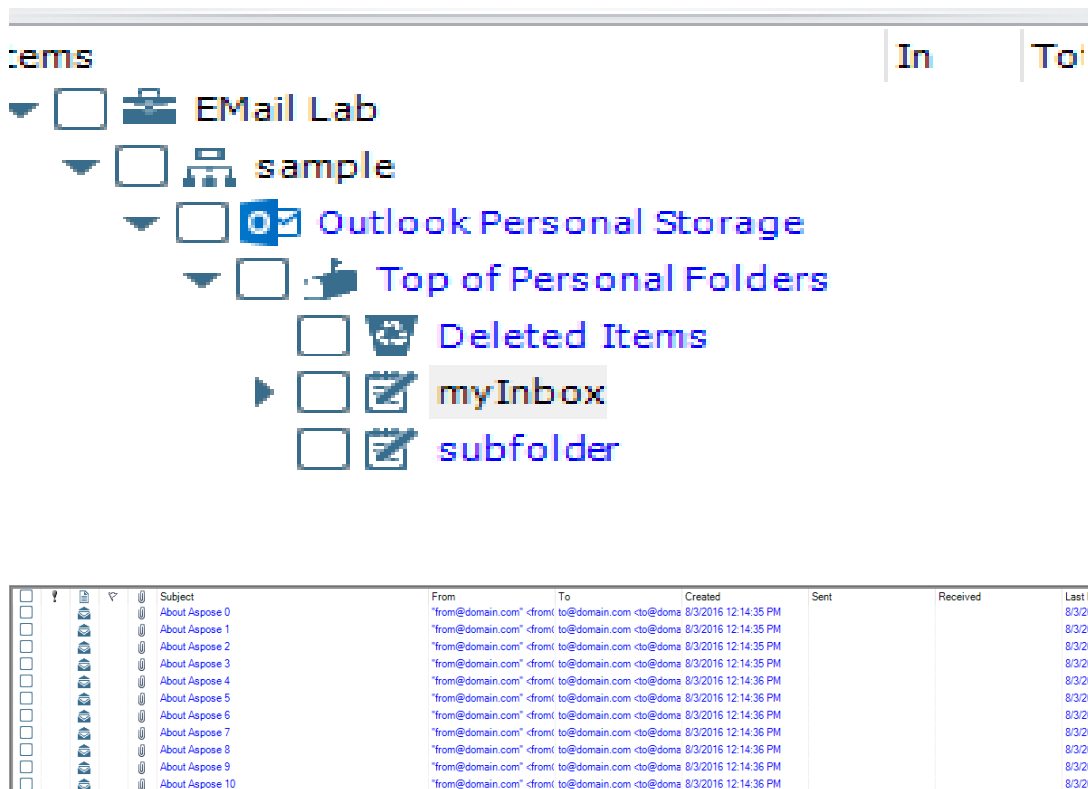
### Filled Fields:

- **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](mailto: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:

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

#### E-mail Data

##### About Aspose 29

"from@domain.com" <from@domain.com> on behalf of "from@domain.com" <from@domain.com>

To: to@domain.com <to@domain.com>

### 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)

