Lab 5: Perform Email Footprinting

**Lab Scenario**

As a professional ethical hacker, you need to be able to track emails of individuals (employees) from a target organization for gathering critical information that can help in building an effective hacking strategy. Email tracking allows you to collect information such as IP addresses, mail servers, OS details, geolocation, information about service providers involved in sending the mail etc. By using this information, you can perform social engineering and other advanced attacks.

**Lab Objectives**

* Gather information about a target by tracing emails using eMailTrackerPro

**Overview of Email Footprinting**

E-mail footprinting, or tracking, is a method to monitor or spy on email delivered to the intended recipient. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email.

Email footprinting reveals information such as:.

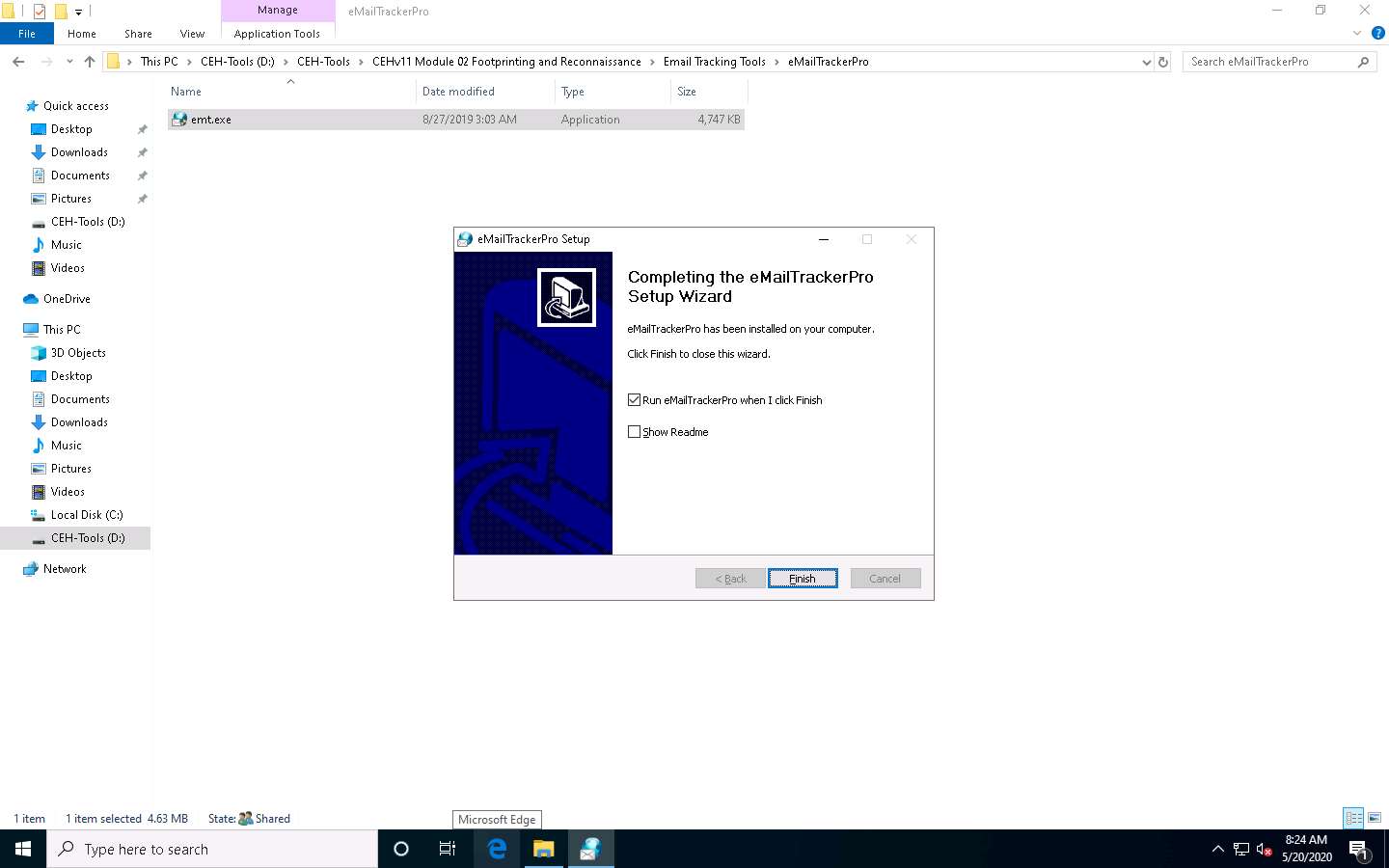
* Recipient's system IP address
* The GPS coordinates and map location of the recipient
* When an email message was received and read
* Type of server used by the recipient
* Operating system and browser information
* If a destructive email was sent
* The time spent reading the email
* Whether or not the recipient visited any links sent in the email
* PDFs and other types of attachments
* If messages were set to expire after a specified time

Task 1: Gather Information about a Target by Tracing Emails using eMailTrackerPro

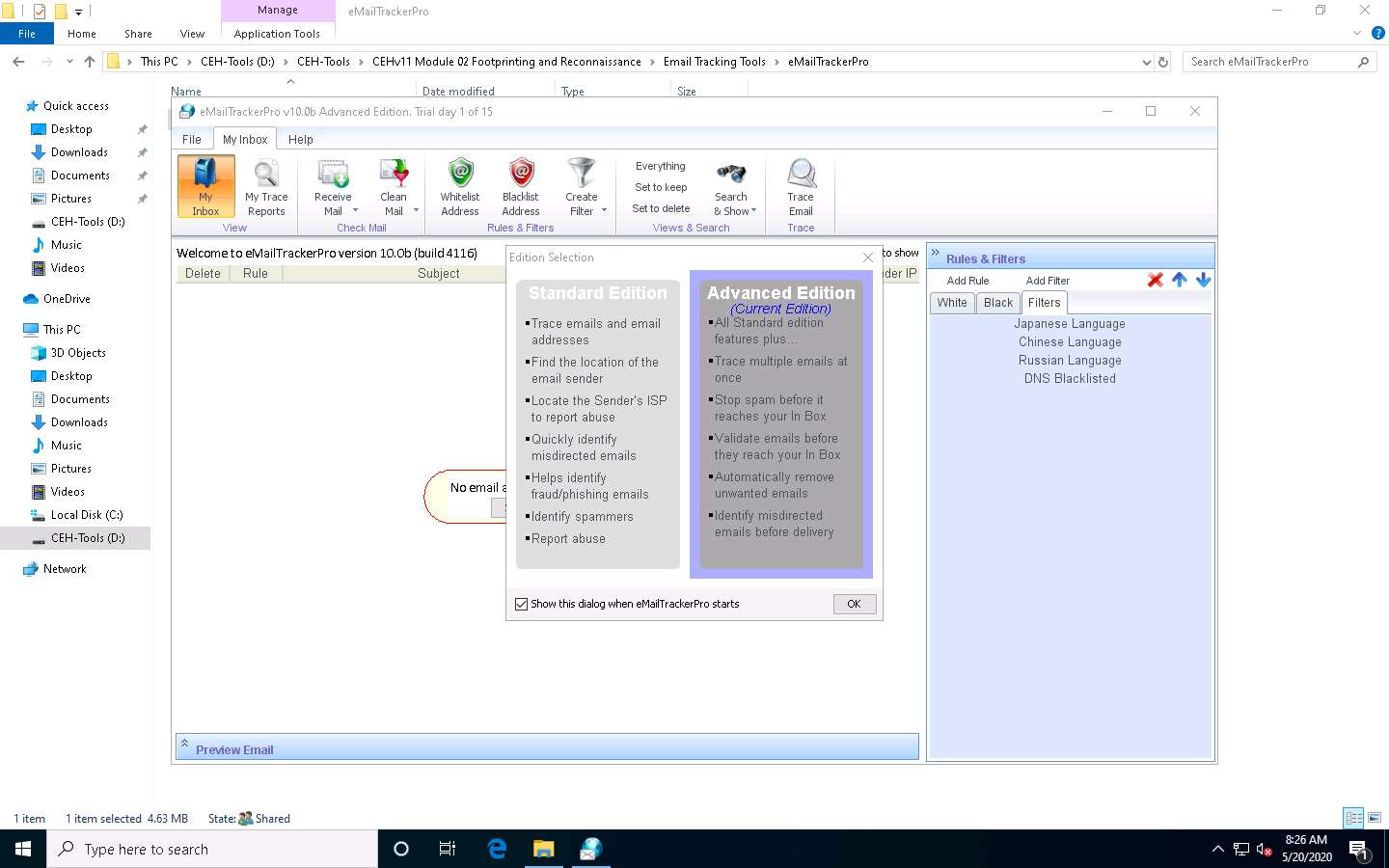
The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email header helps ethical hackers to trace the routing path taken by an email before delivering it to the recipient.

Here, we will gather information by analyzing the email header using eMailTrackerPro.

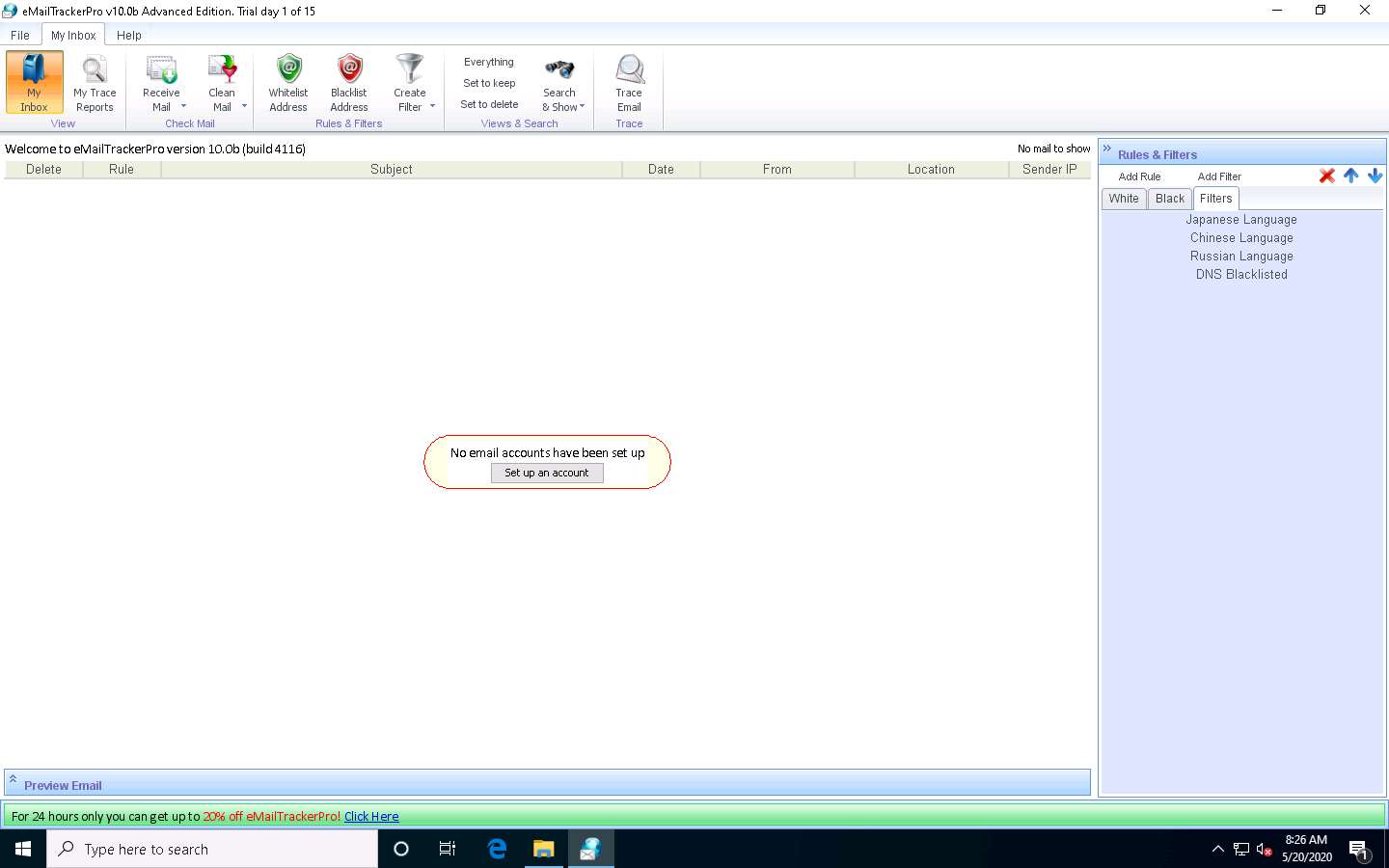
1. Click [Windows 10](https://labclient.labondemand.com/Instructions/b16bedc2-7151-47a3-9211-5daccdd8c426?rc=10) to switch to the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.
4. After the installation is complete, in the **Completing the eMailTrackerPro Setup Wizard**, uncheck the **Show Readme** check-box and click the **Finish** button to launch the eMailTrackerPro.



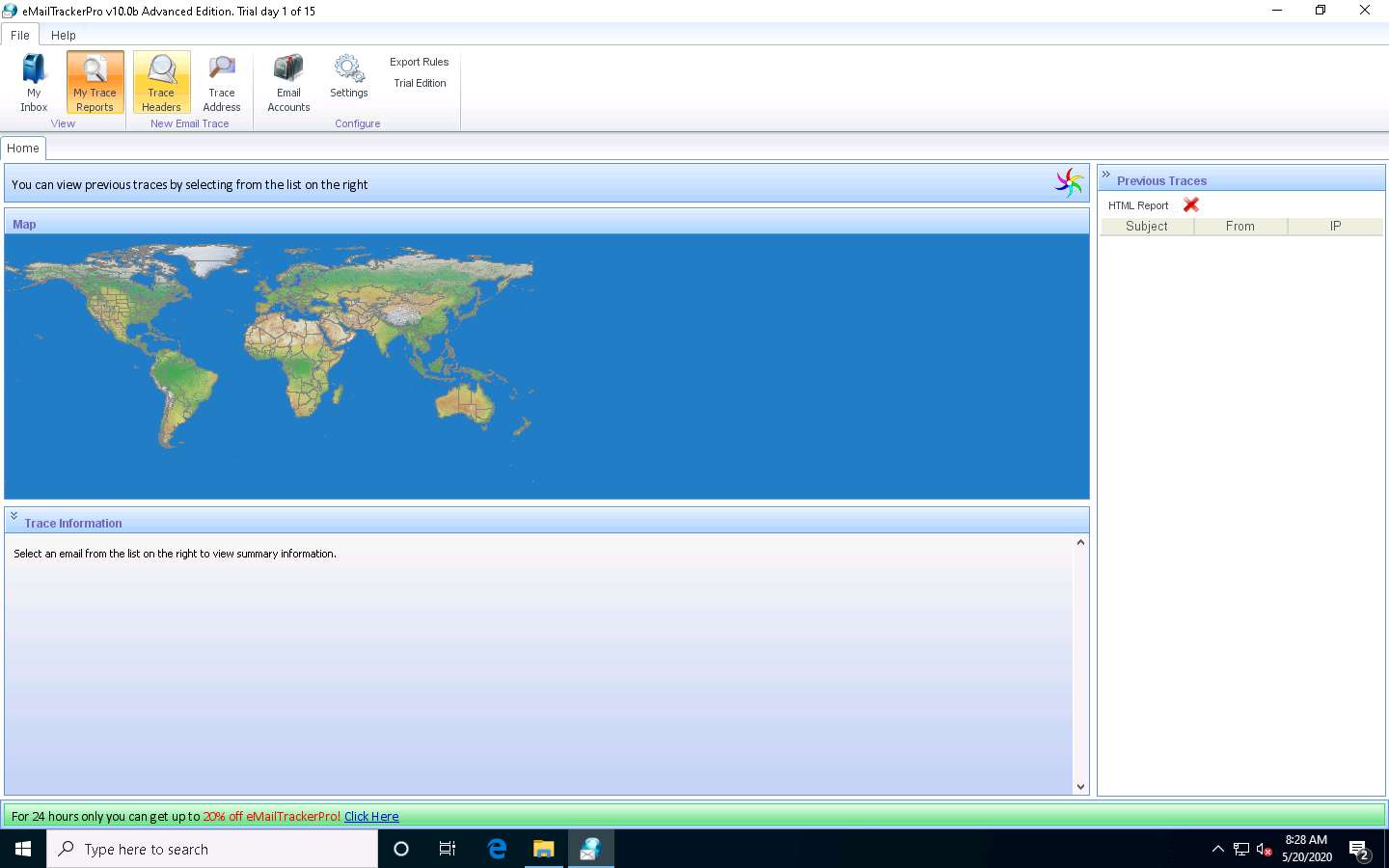
1. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.



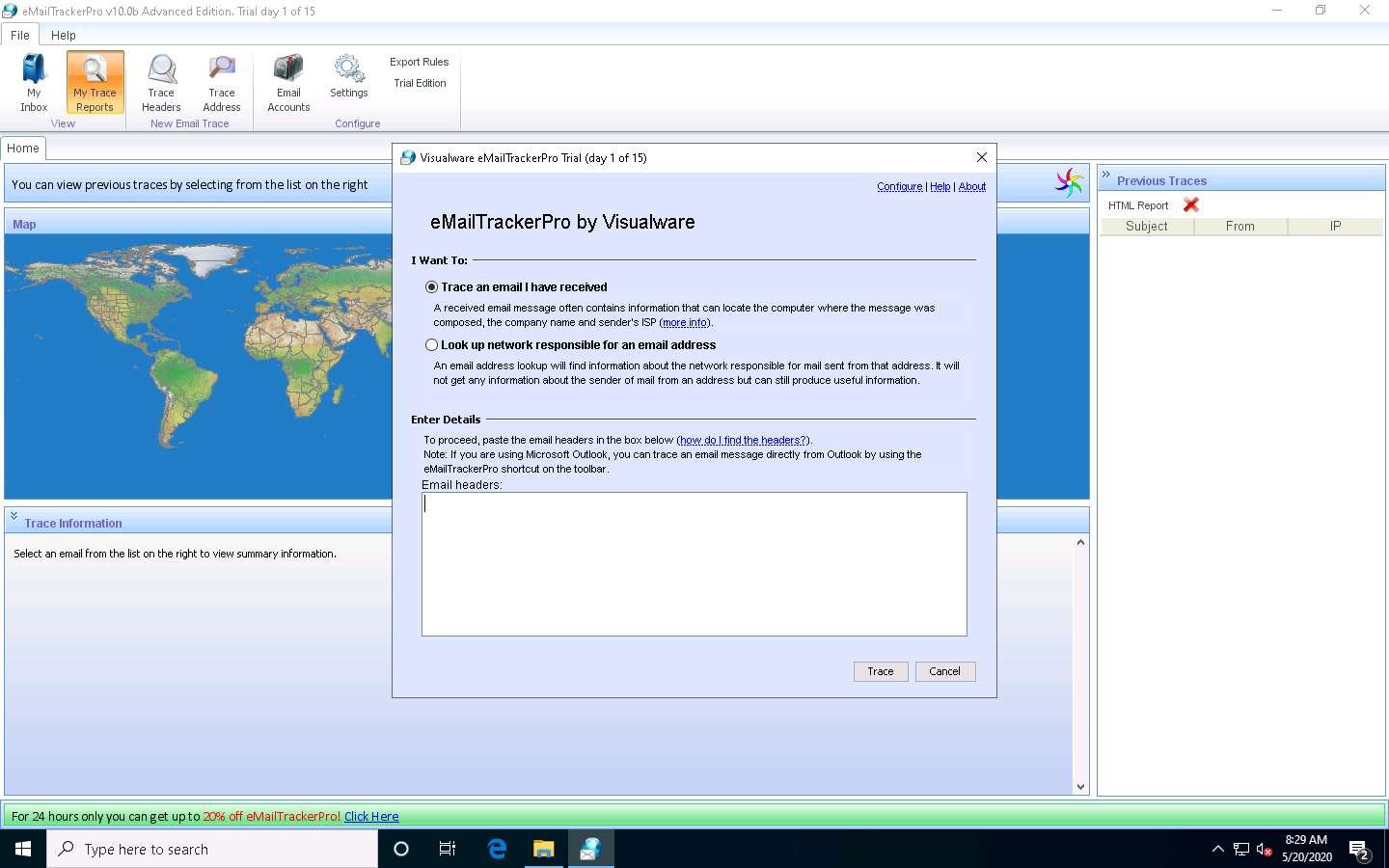
1. The **eMailTrackerPro** main window appears, as shown in the screenshot.



1. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header).
2. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.



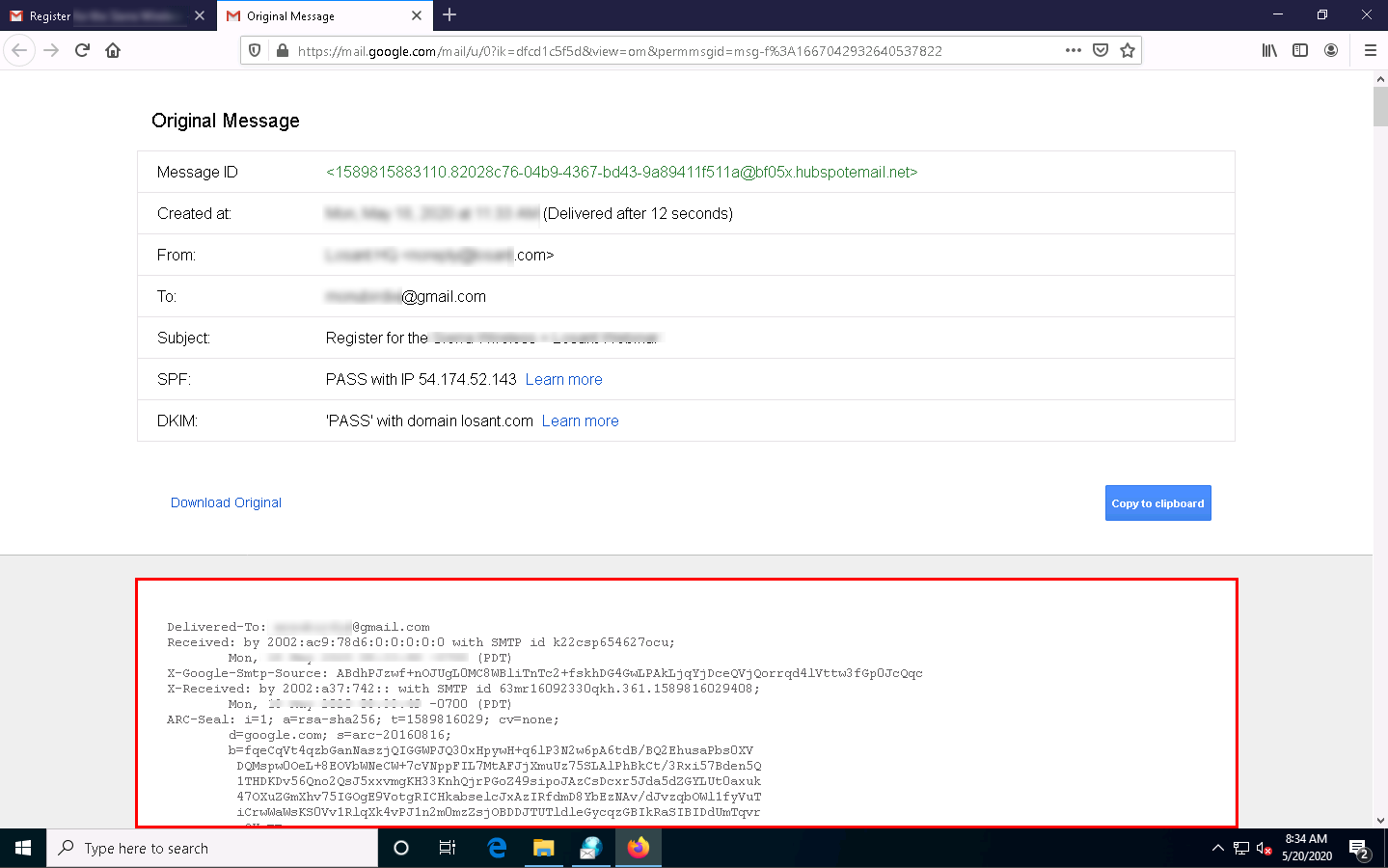
1. A pop-up window will appear; select **Trace an email I have received**. Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers**: field under **Enter Details** section.



1. For finding email headers, open any web browser and log in to any email account of your choice; from the email inbox, open the message you would like to view headers for.

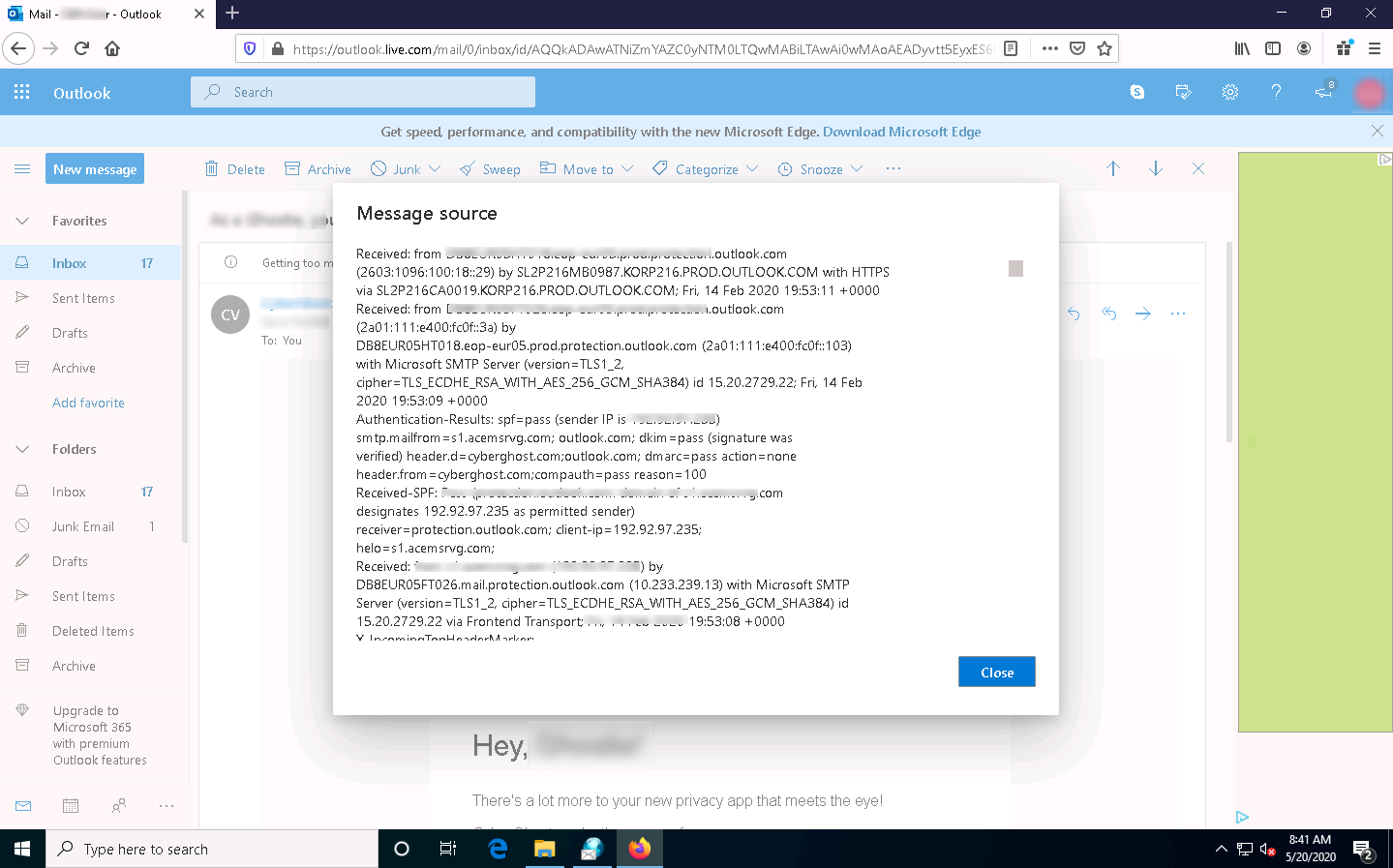
In **Gmail**, find the email header by following the steps:

* + Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.
  + Select **Show original** from the list.
  + The **Original Message** window appears in a new browser tab with all the details about the email, including the email header



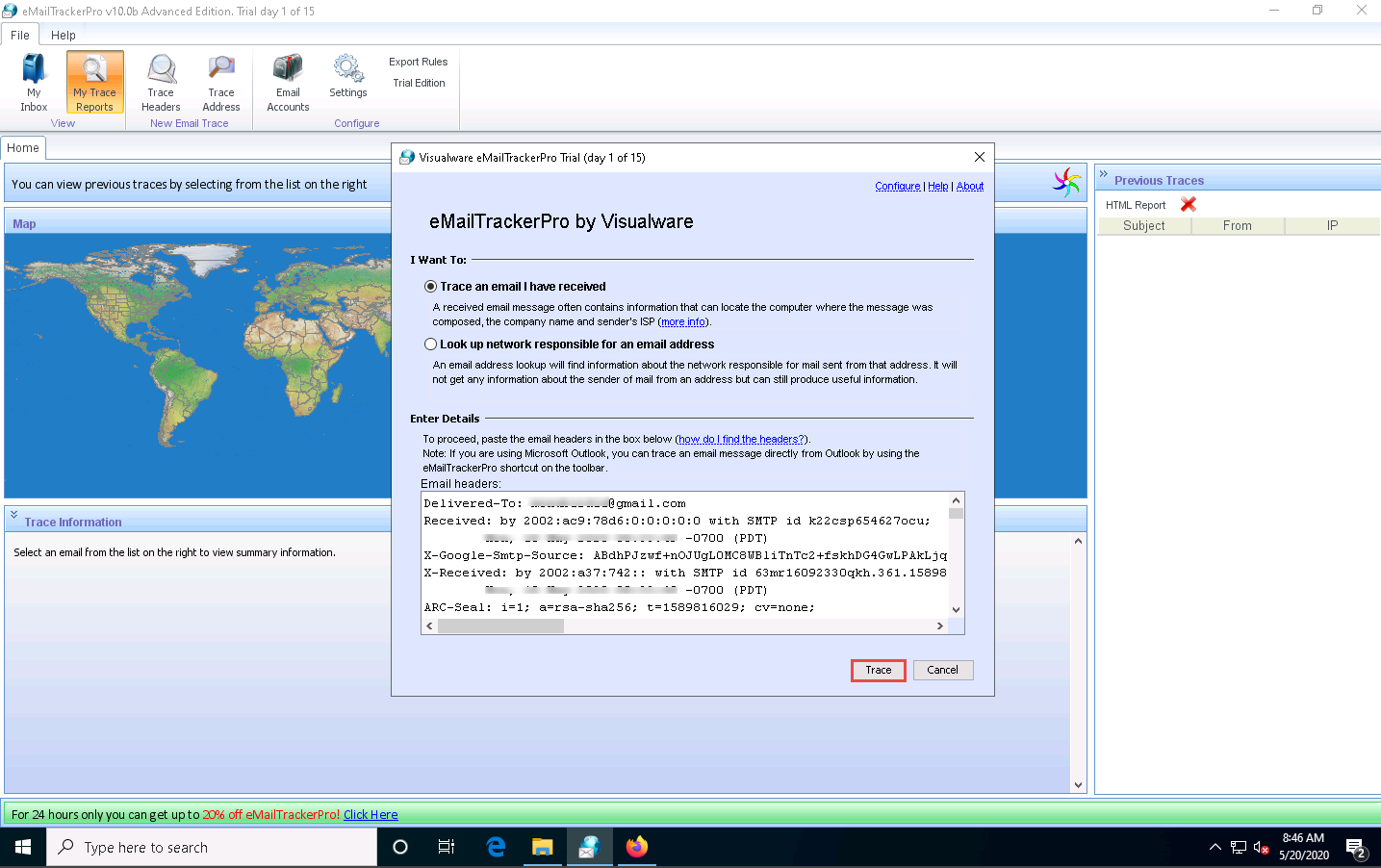
In **Outlook**, find the email header by following the steps:

* + Double-click the email to open it in a new window
  + Click the **… (More actions)** icon present at the right of the message-pane to open message options
  + From the options, click **View message details**
  + The **message details** window appears with all the details about the email, including the email header

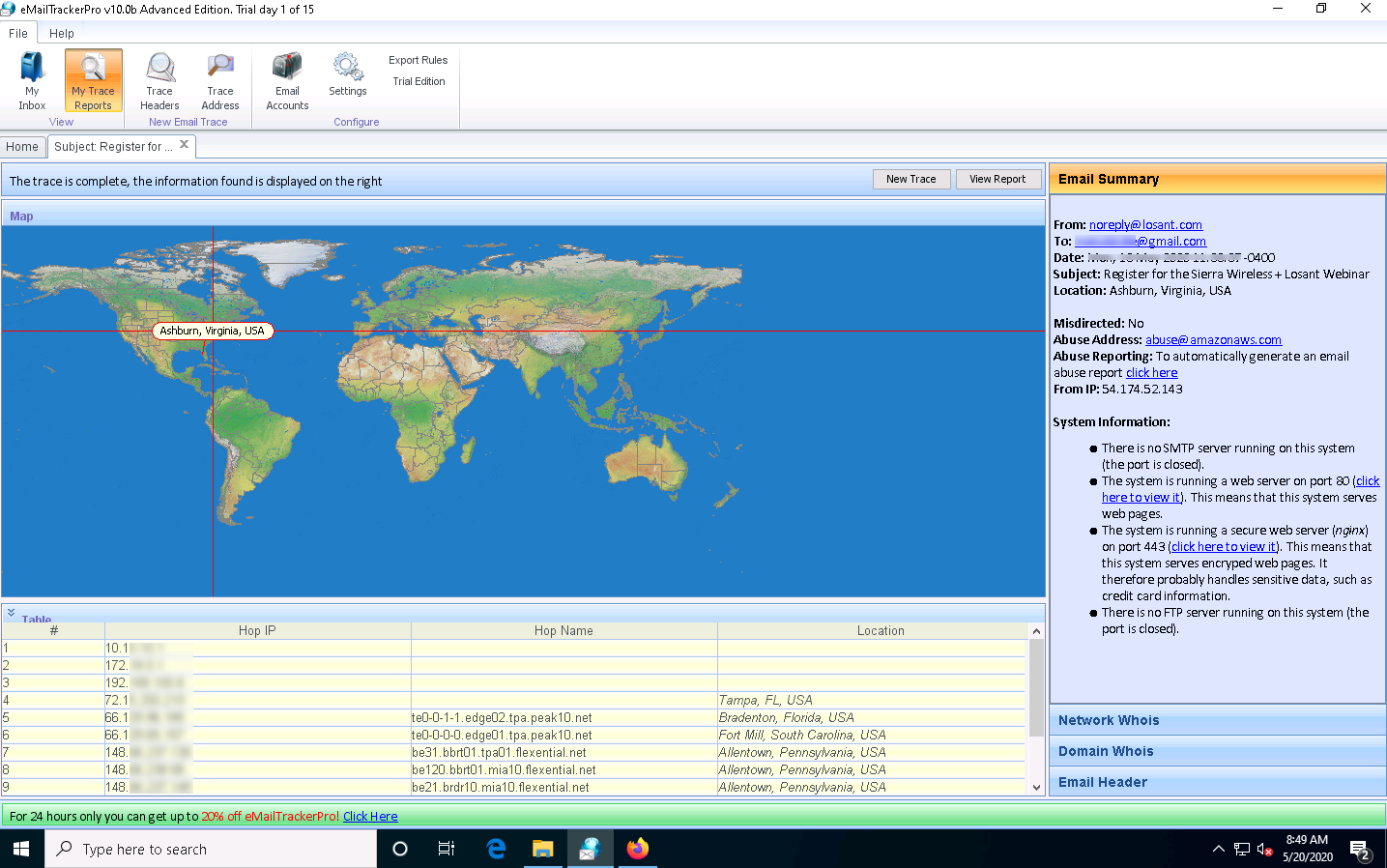


1. Copy the entire email header text and paste it into the **Email headers**: field of eMailTrackerPro, and click **Trace**.

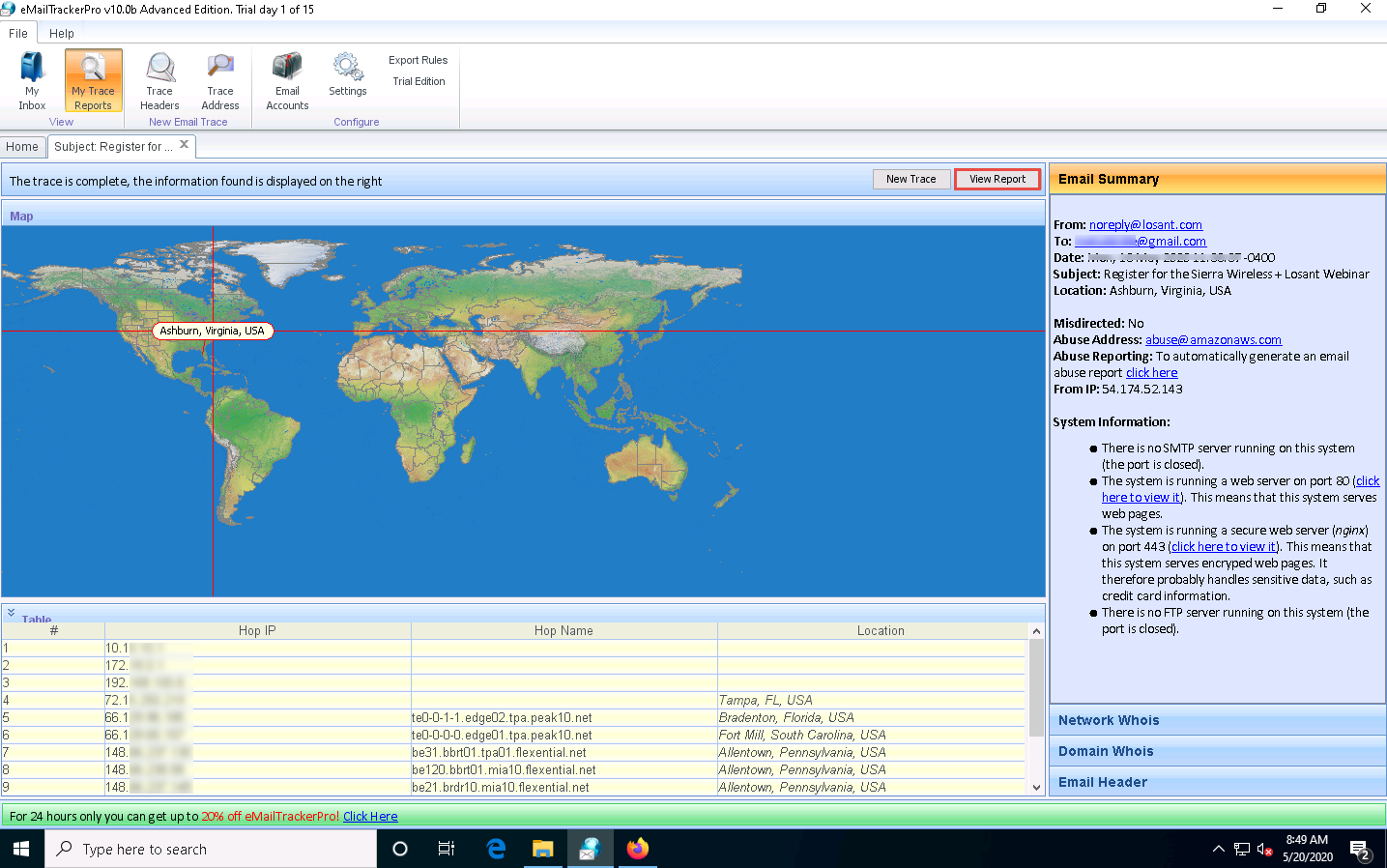
Here, we are analyzing the email header from gmail account. However, you can also analyze the email header from outlook account.



1. The **My Trace Reports** window opens.
2. The email location will be traced in a **Map** (world map GUI). You can also view the summary by selecting **Email Summary** on the right-hand side of the window. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.



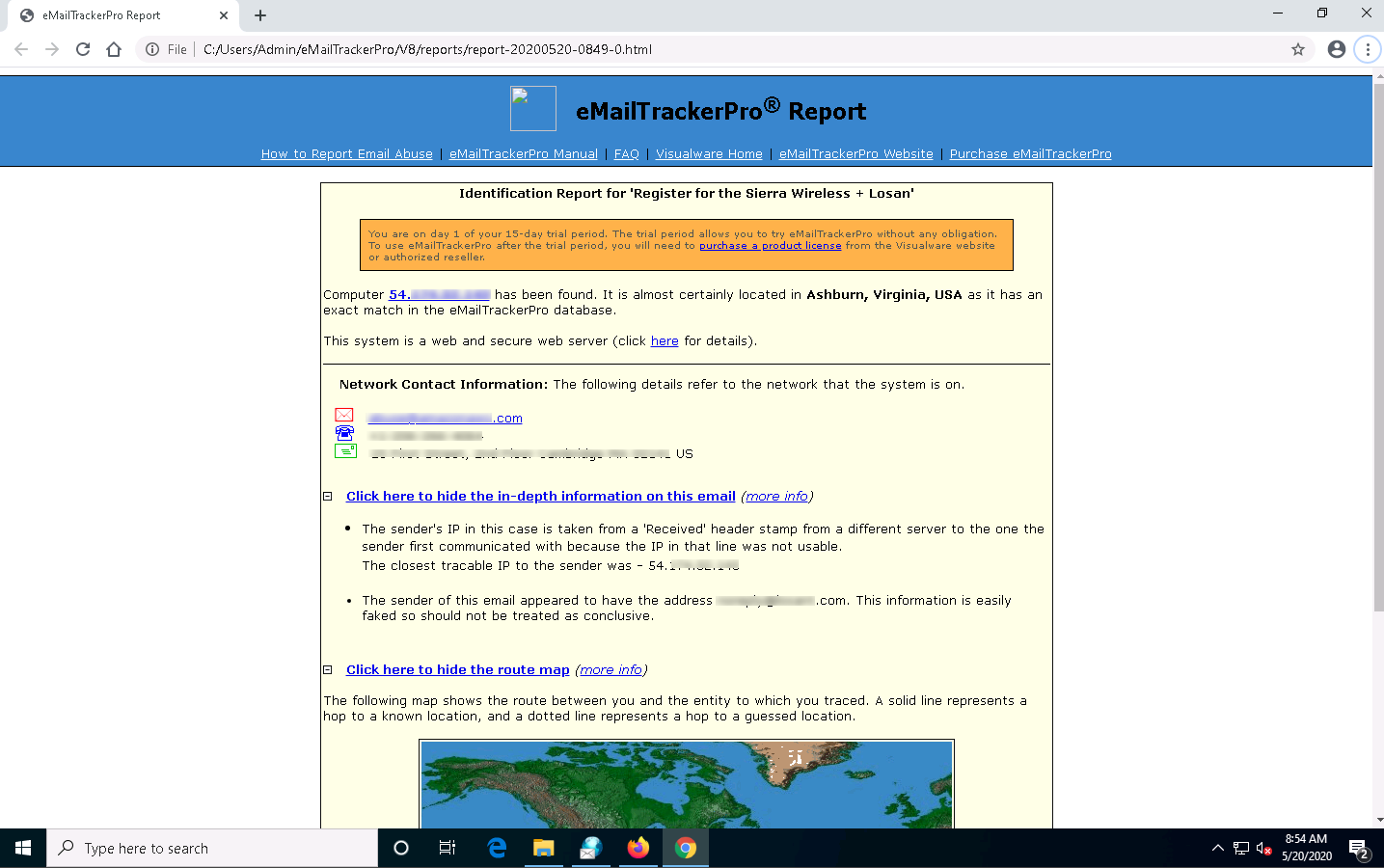
1. To examine the report, click the **View Report** button above **Map** to view the complete trace report.



1. The complete report appears in the default browser.

If a pop-up window appears asking for a browser to be selected, select **Firefox** and click **OK**.

1. Expand each section to view detailed information.



1. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
2. You can also use email tracking tools such as **Infoga** (https://github.com), **Mailtrack** (https://mailtrack.io), etc. to track an email and extract target information such as sender identity, mail server, sender’s IP address, location, etc.
3. Close all open windows and document all the acquired information.