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:.

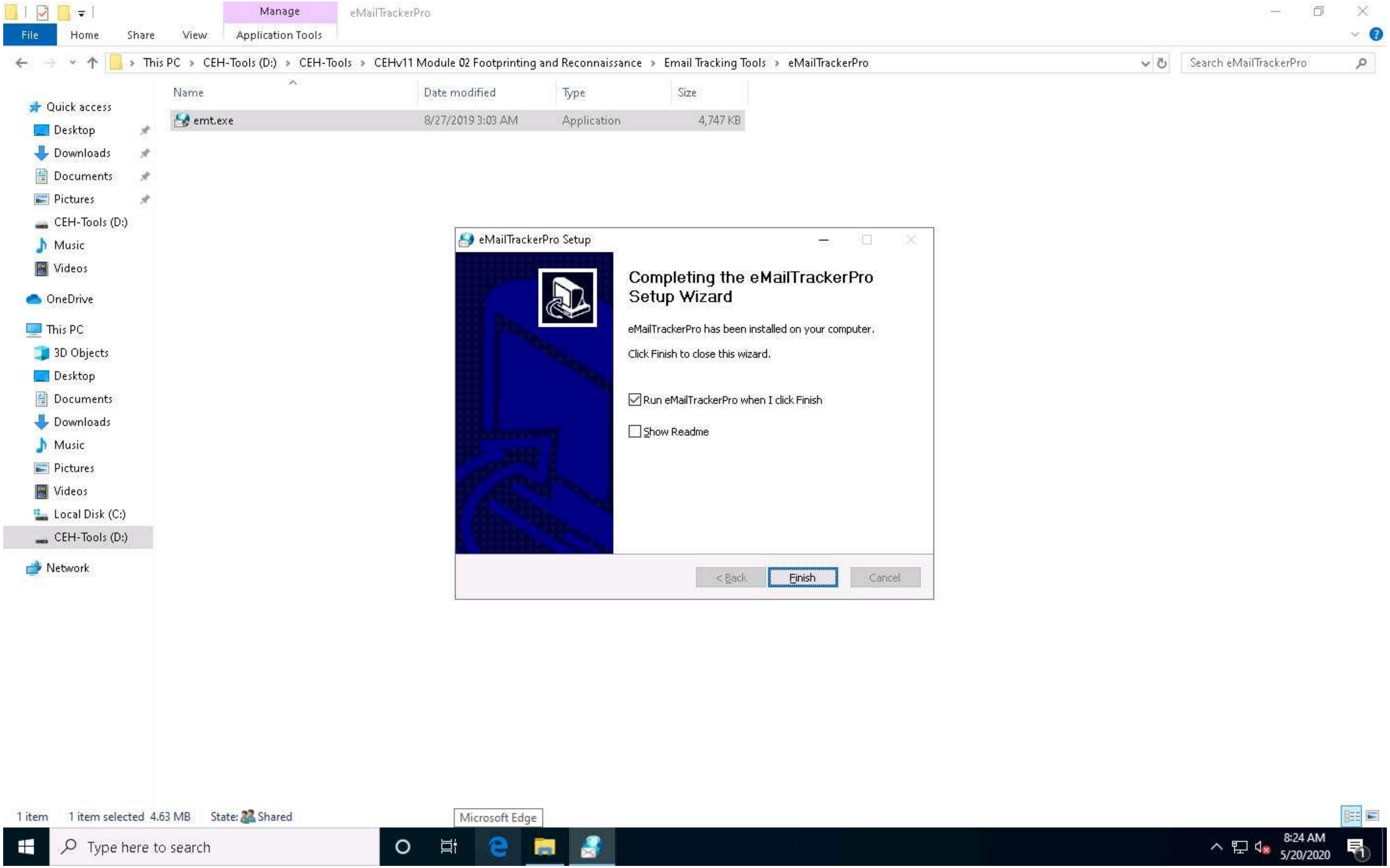
- Recipient's system IP address
- The GPS coordinates and map location of the recipient
- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- The time spent reading the email
- Whether or not 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 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.



Name	Date modified	Type	Size
emt.exe	8/27/2019 3:03 AM	Application	4,747 KB

Completing the eMailTrackerPro Setup Wizard

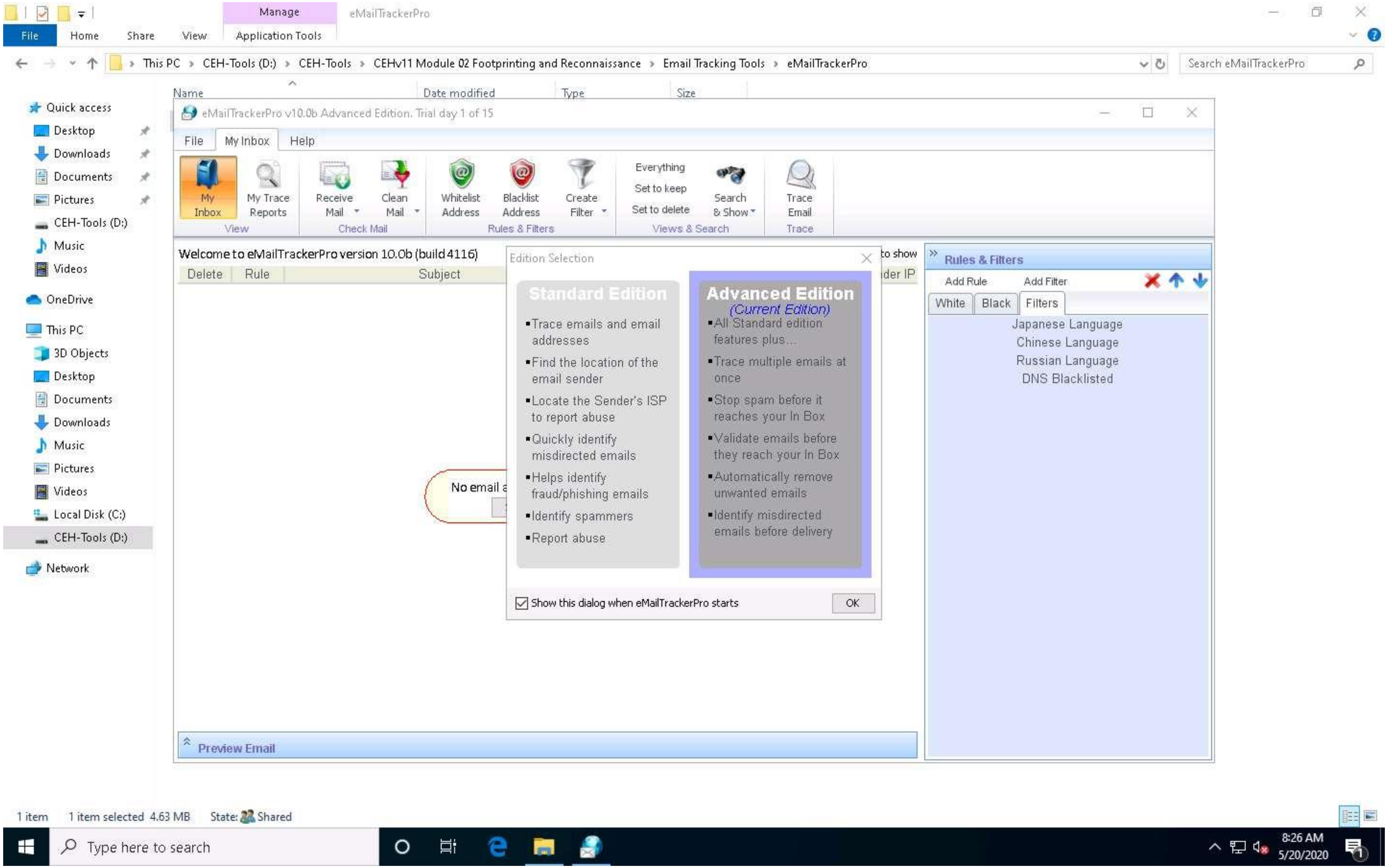
eMailTrackerPro has been installed on your computer.

Click Finish to close this wizard.

☑ Run eMailTrackerPro when I click Finish

□ Show Readme

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



Welcome to eMailTrackerPro version 10.0b (build 4116)

Edition Selection

Standard Edition

- Trace emails and email addresses
- Find the location of the email sender
- Locate the Sender's ISP to report abuse
- Quickly identify misdirected emails
- Helps identify fraud/phishing emails
- Identify spammers
- Report abuse

Advanced Edition

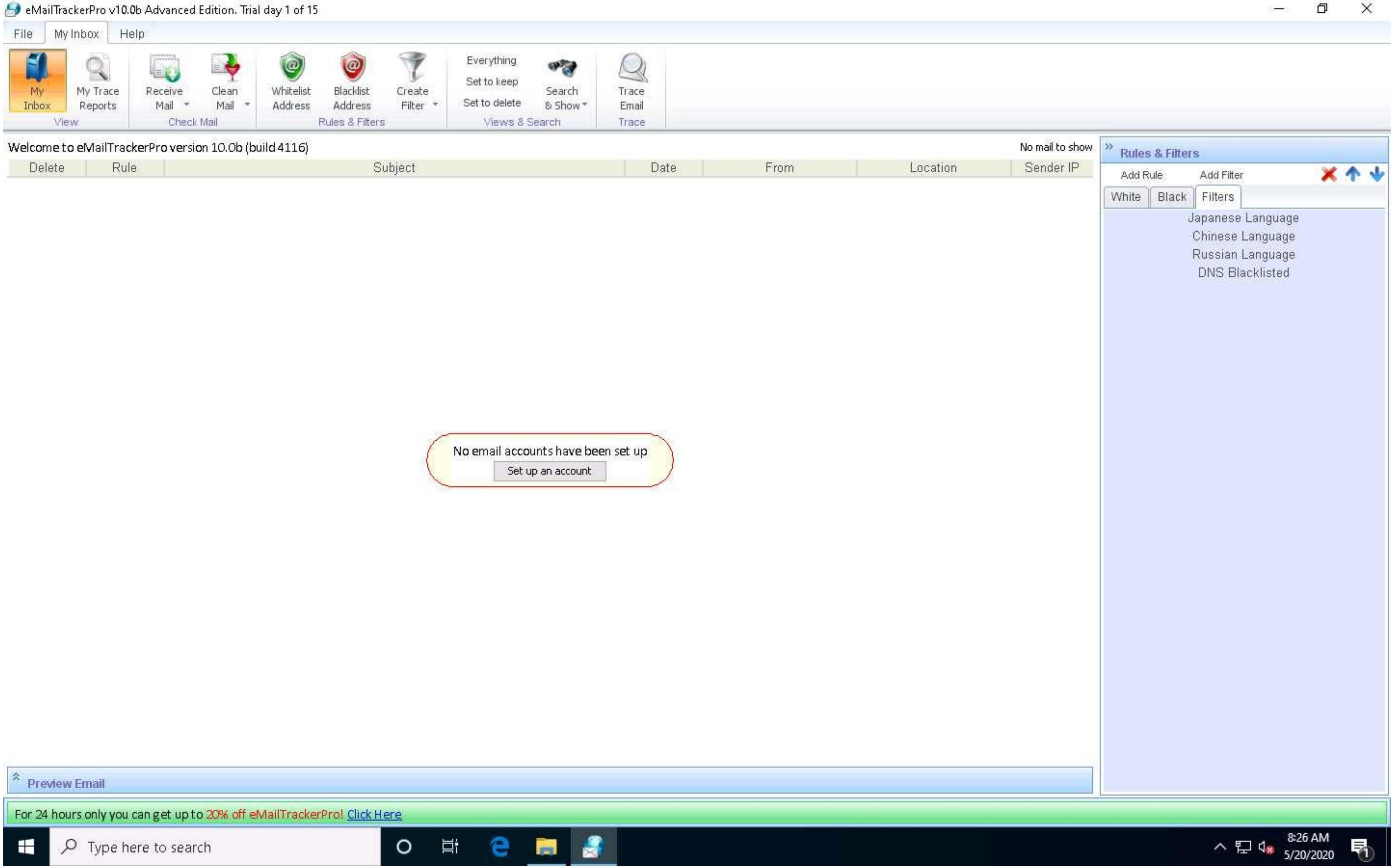
(Current Edition)

- All Standard edition features plus...
- Trace multiple emails at once
- Stop spam before it reaches your In Box
- Validate emails before they reach your In Box
- Automatically remove unwanted emails
- Identify misdirected emails before delivery

☑ Show this dialog when eMailTrackerPro starts

OK

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



eMailTrackerPro v10.0b Advanced Edition. Trial day 1 of 15

Welcome to eMailTrackerPro version 10.0b (build 4116)

No mail to show

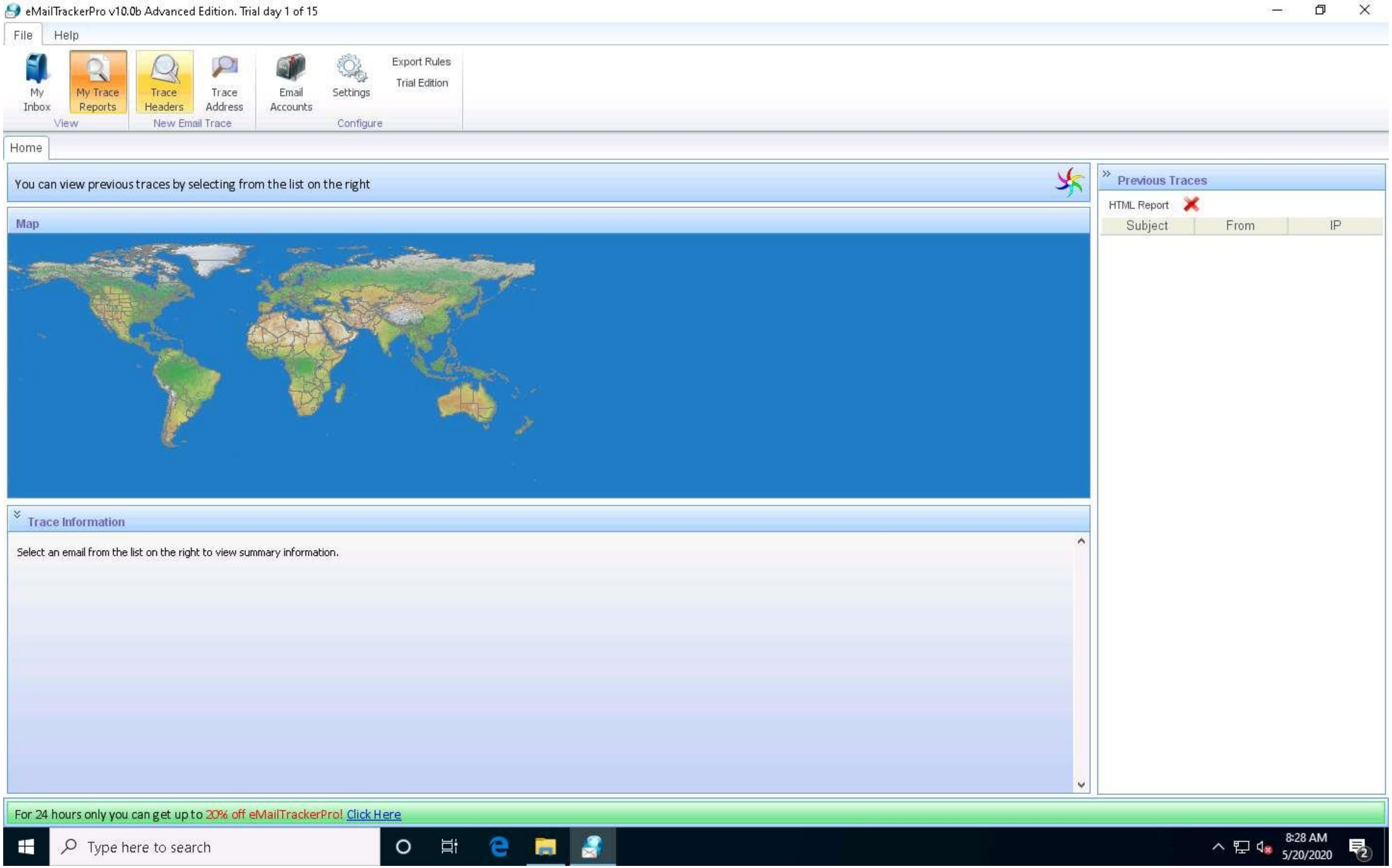
Delete	Rule	Subject	Date	From	Location	Sender IP

No email accounts have been set up

For 24 hours only you can get up to 20% off eMailTrackerPro! Click Here

7. □ 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).

8. □ Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.

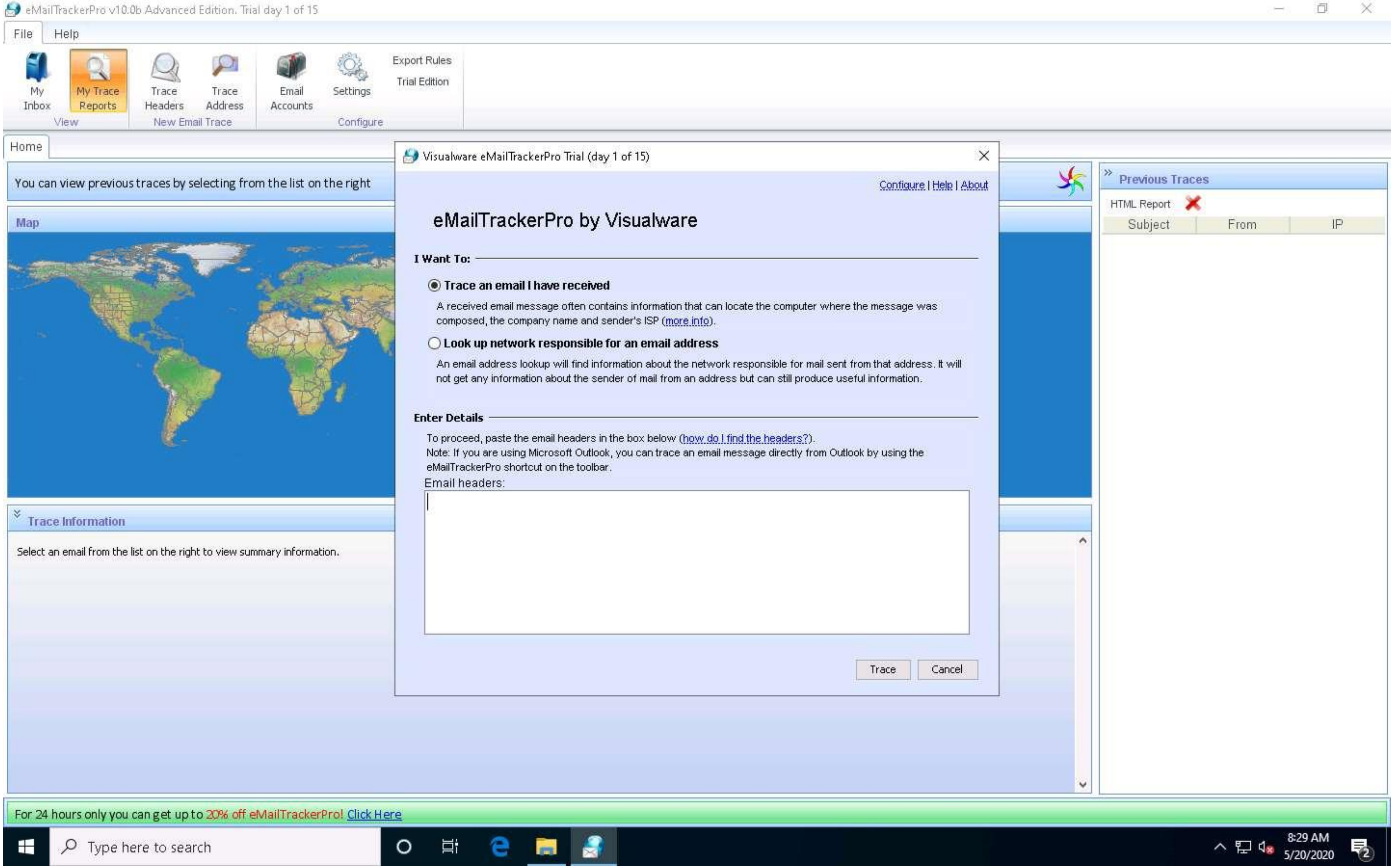


You can view previous traces by selecting from the list on the right

Select an email from the list on the right to view summary information.

For 24 hours only you can get up to 20% off eMailTrackerPro! Click Here

9. □ 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.



You can view previous traces by selecting from the list on the right

Select an email from the list on the right to view summary information.

Visualware eMailTrackerPro Trial (day 1 of 15)

Configure | Help | About

eMailTrackerPro by Visualware

I Want To:

● **Trace an email I have received**

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP (more info).

○ **Look up network responsible for an email address**

An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details

To proceed, paste the email headers in the box below (how do I find the headers?).
Note: If you are using Microsoft Outlook, you can trace an email message directly from Outlook by using the eMailTrackerPro shortcut on the toolbar.

Email headers:

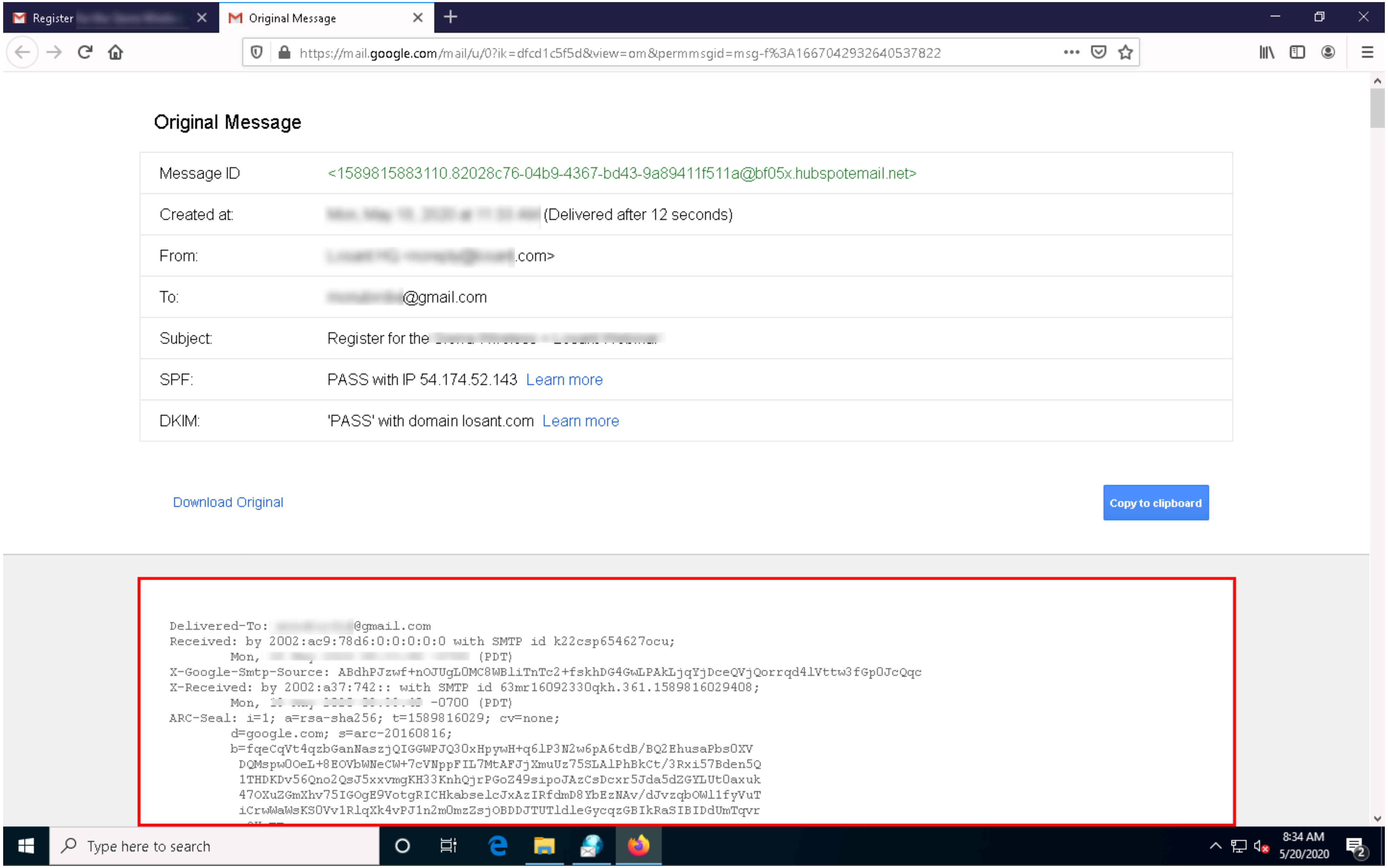
Trace | Cancel

For 24 hours only you can get up to 20% off eMailTrackerPro! Click Here

10. □ 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



Register [redacted]
Original Message
https://mail.google.com/mail/u/0?ik=dfcd1c5f5d&view=om&permmsgid=msg-f%3A1667042932640537822
Type here to search
8:34 AM
5/20/2020

Original Message

Message ID	<1589815883110.82028c76-04b9-4367-bd43-9a89411f511a@bf05x.hubspotemail.net>
Created at:	[redacted] (Delivered after 12 seconds)
From:	[redacted].com>
To:	[redacted]@gmail.com
Subject:	Register for the [redacted]
SPF:	PASS with IP 54.174.52.143 Learn more
DKIM:	'PASS' with domain losant.com Learn more

Download Original

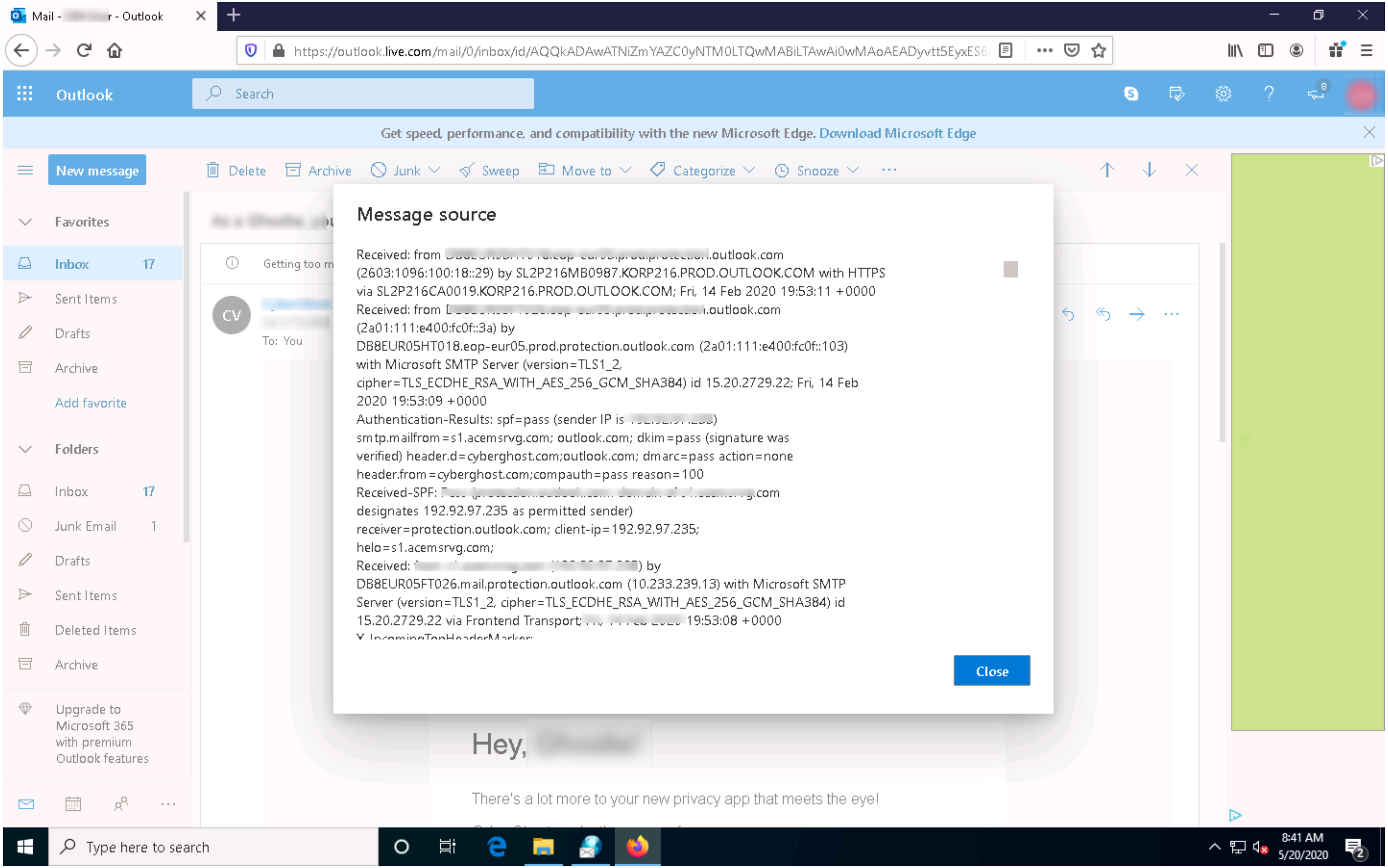
Copy to clipboard

```
Delivered-To: [redacted]@gmail.com
Received: by 2002:ac9:78d6:0:0:0:0:0 with SMTP id k22csp654627ocu;
        Mon, [redacted] (PDT)
X-Google-Smtp-Source: ABdhPJzwf+nOJUgLOMC8WBliTnTc2+fskhDG4GwLPAkLjqYjDceQVjQorrqd4lVttw3fGp0JcQqc
X-Received: by 2002:a37:742:: with SMTP id 63mr16092330qkh.361.1589816029408;
        Mon, [redacted] -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1589816029; cv=none;
        d=google.com; s=arc-20160816;
        b=fqeCqVt4qzbGanNaszjQIGGWPJQ30xHpywH+q6lP3N2w6pA6tdB/BQ2EhusaPbs0XV
         DQMspw0OeL+8EOVbWNeCW+7cVNppFIL7MtAFJjXmuUz75SLAlPhBkCt/3Rxi57Bden5Q
         1THDKDv56Qno2QsJ5xxvmgKH33KnhQjrPGoZ49sipoJAzCsDcxr5Jda5dZGYLUt0axuk
         47OXuZGmXhv75IGOgE9VotgRICHkabselcJxAzIRfdmD8YbEzNAv/dJvzqbOWl1fyVuT
         iCrwWaWsKS0Vv1RlqXk4vPJ1n2m0mzZsjOBDDJTUTldleGycqzGBIkRaSIBIDdUmTqvr
```

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

- Double-click the email to open it in a new window

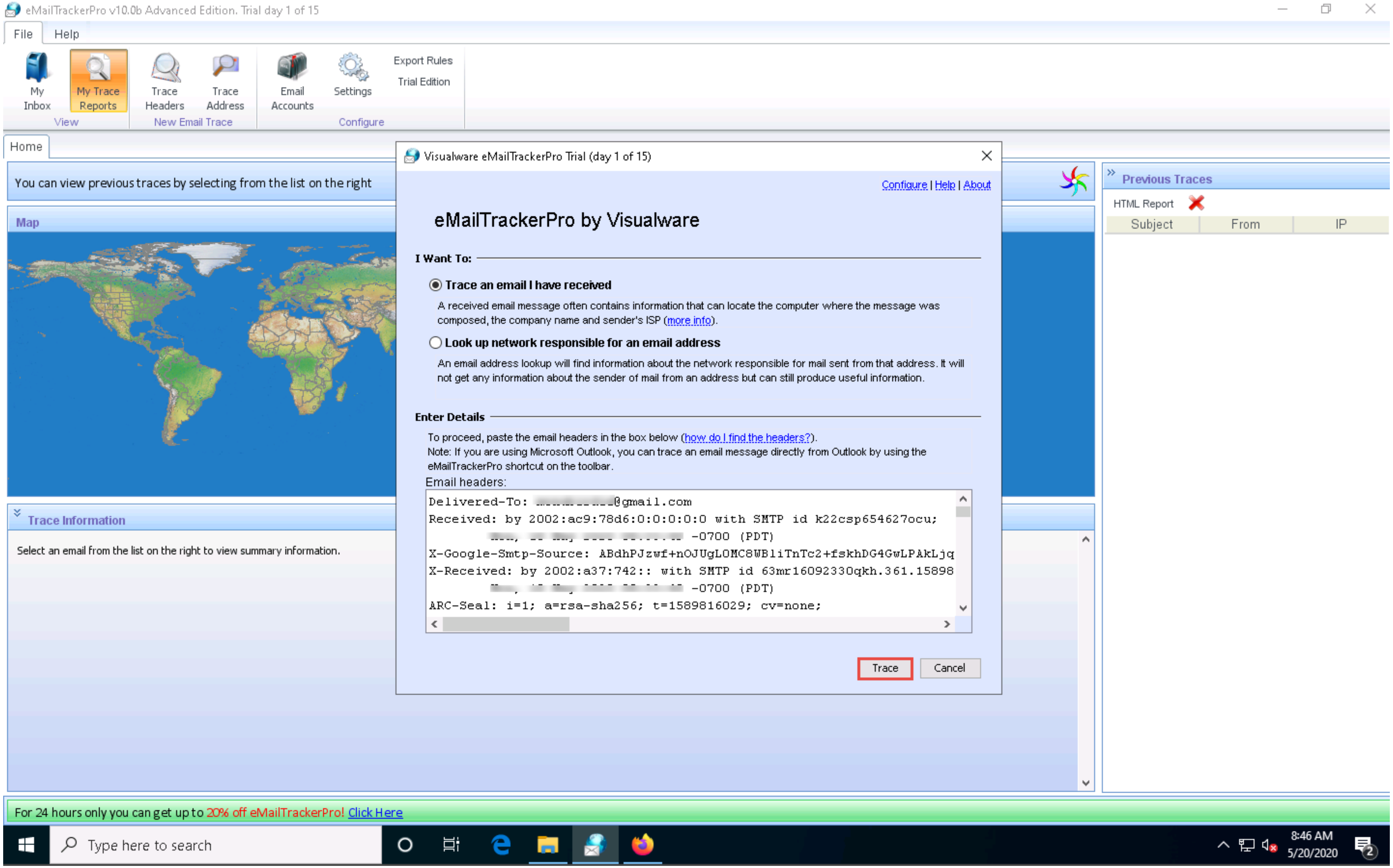
- Click the **… (More actions)** icon present at the right of the message-pane to open message options
- From the options, click **View message details**
- The **message details** window appears with all the details about the email, including the email header


Mail - [redacted] - Outlook
https://outlook.live.com/mail/0/inbox/id/AQQkADAwATNiZmYAZC0yNTM0LTQwMABiLTAwAi0wMAoAEADyvtt5EyxES6
Outlook
Search
Get speed, performance, and compatibility with the new Microsoft Edge. Download Microsoft Edge
New message
Delete
Archive
Junk
Sweep
Move to
Categorize
Snooze
Favorites
Inbox 17
Sent Items
Drafts
Archive
Add favorite
Folders
Inbox 17
Junk Email 1
Drafts
Sent Items
Deleted Items
Archive
Upgrade to Microsoft 365 with premium Outlook features
Getting too m
CV
To: You
Hey, [redacted]
There's a lot more to your new privacy app that meets the eye!
Message source
Close
Type here to search
8:41 AM
5/20/2020

```
Received: from [redacted].outlook.com
(2603:1096:100:18::29) by SL2P216MB0987.KORP216.PROD.OUTLOOK.COM with HTTPS
via SL2P216CA0019.KORP216.PROD.OUTLOOK.COM; Fri, 14 Feb 2020 19:53:11 +0000
Received: from [redacted].outlook.com
(2a01:111:e400:fc0f::3a) by
DB8EUR05HT018.eop-eur05.prod.protection.outlook.com (2a01:111:e400:fc0f::103)
with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.2729.22; Fri, 14 Feb
2020 19:53:09 +0000
Authentication-Results: spf=pass (sender IP is [redacted])
smtp.mailfrom=s1.acemsrvg.com; outlook.com; dkim=pass (signature was
verified) header.d=cyberghost.com;outlook.com; dmarc=pass action=none
header.from=cyberghost.com;compauth=pass reason=100
Received-SPF: [redacted].com
designates 192.92.97.235 as permitted sender)
receiver=protection.outlook.com; client-ip=192.92.97.235;
helo=s1.acemsrvg.com;
Received: [redacted]) by
DB8EUR05FT026.mail.protection.outlook.com (10.233.239.13) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.2729.22 via Frontend Transport; [redacted] 19:53:08 +0000
X-IncomingTopHeaderMarker:
```

11. □ 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.



You can view previous traces by selecting from the list on the right

Select an email from the list on the right to view summary information.

Visualware eMailTrackerPro Trial (day 1 of 15)

Configure | Help | About

eMailTrackerPro by Visualware

I Want To:

● **Trace an email I have received**

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP (more info).

○ **Look up network responsible for an email address**

An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details

To proceed, paste the email headers in the box below (how do I find the headers?).
Note: If you are using Microsoft Outlook, you can trace an email message directly from Outlook by using the eMailTrackerPro shortcut on the toolbar.

Email headers:

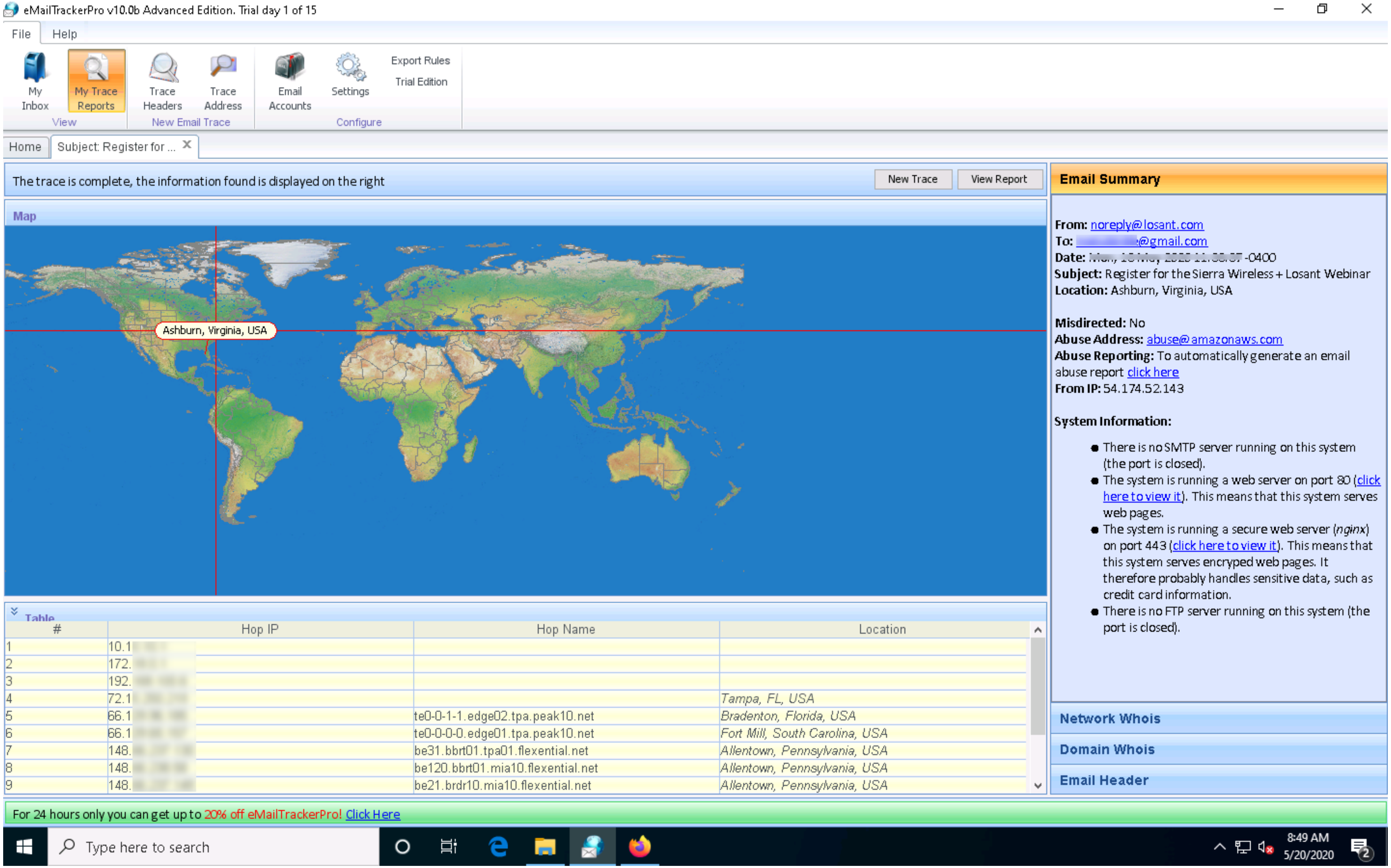
```
Delivered-To: [redacted]@gmail.com
Received: by 2002:ac9:78d6:0:0:0:0:0 with SMTP id k22csp654627ocu;
        [redacted] -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzwf+nOJUgLOMC8WBliTnTc2+fskhDG4GwLPAkLjq
X-Received: by 2002:a37:742:: with SMTP id 63mr16092330qkh.361.15898
        [redacted] -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1589816029; cv=none;
```

Trace | Cancel

For 24 hours only you can get up to 20% off eMailTrackerPro! Click Here

12. □ The **My Trace Reports** window opens.

13. □ 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.



The trace is complete, the information found is displayed on the right

Email Summary

From: noreply@losant.com
To: [redacted]@gmail.com
Date: [redacted] -0400
Subject: Register for the Sierra Wireless + Losant Webinar
Location: Ashburn, Virginia, USA

Misdirected: No
Abuse Address: abuse@amazonaws.com
Abuse Reporting: To automatically generate an email abuse report click here
From IP: 54.174.52.143

System Information:

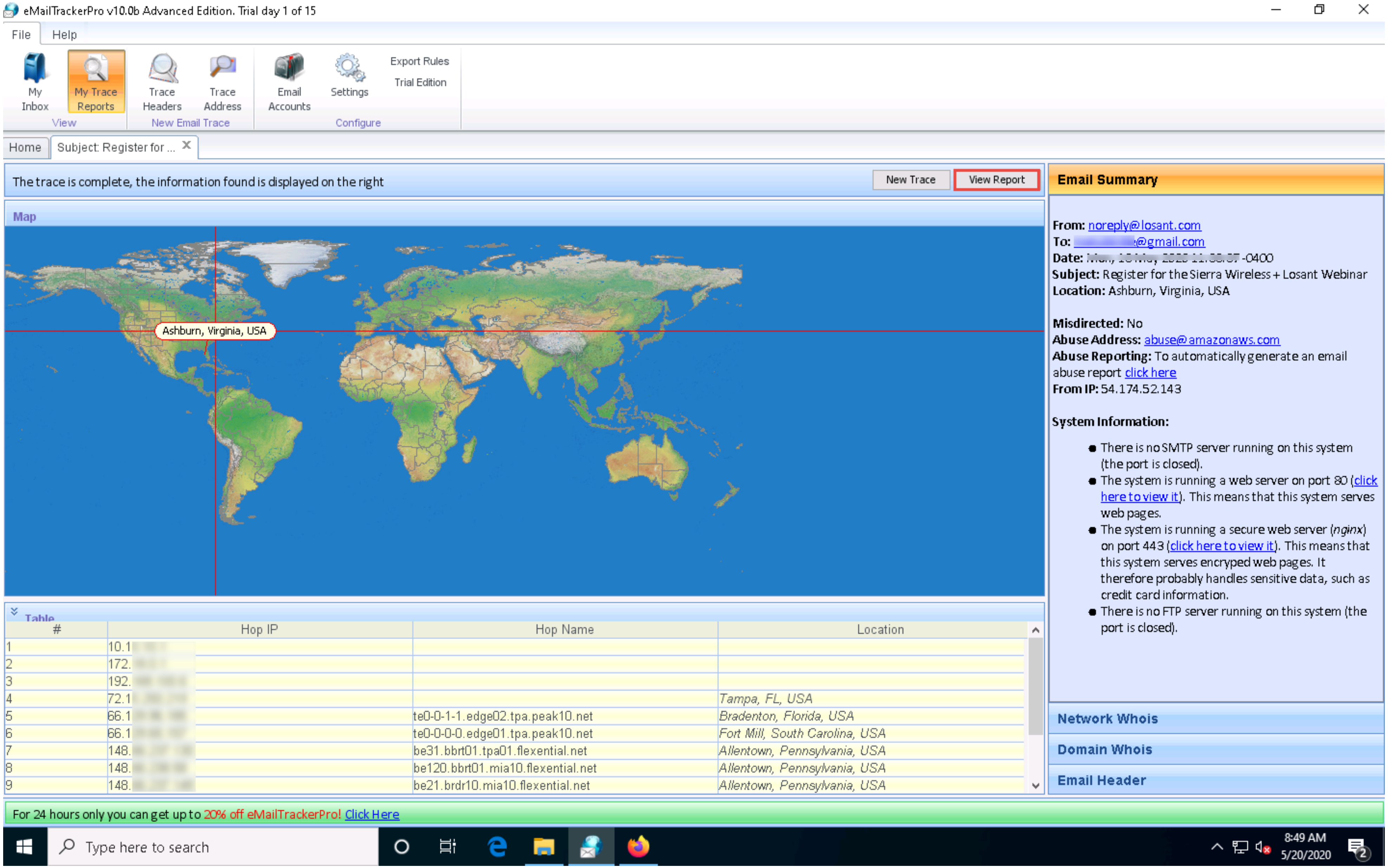
- There is no SMTP server running on this system (the port is closed).
- The system is running a web server on port 80 (click here to view it). This means that this system serves web pages.
- The system is running a secure web server (*nginx*) on port 443 (click here to view it). This means that this system serves encrypted web pages. It therefore probably handles sensitive data, such as credit card information.
- There is no FTP server running on this system (the port is closed).

Table

#	Hop IP	Hop Name	Location
1	10.1[redacted]		
2	172.[redacted]		
3	192.[redacted]		
4	72.1[redacted]		*Tampa, FL, USA*
5	66.1[redacted]	te0-0-1-1.edge02.tpa.peak10.net	*Bradenton, Florida, USA*
6	66.1[redacted]	te0-0-0-0.edge01.tpa.peak10.net	*Fort Mill, South Carolina, USA*
7	148.[redacted]	be31.bbrt01.tpa01.flexential.net	*Allentown, Pennsylvania, USA*
8	148.[redacted]	be120.bbrt01.mia10.flexential.net	*Allentown, Pennsylvania, USA*
9	148.[redacted]	be21.brdr10.mia10.flexential.net	*Allentown, Pennsylvania, USA*

For 24 hours only you can get up to 20% off eMailTrackerPro! Click Here

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



The trace is complete, the information found is displayed on the right

#	Hop IP	Hop Name	Location
1	10.1[redacted]		
2	172.[redacted]		
3	192.[redacted]		
4	72.1[redacted]		Tampa, FL, USA
5	66.1[redacted]	te0-0-1-1.edge02.tpa.peak10.net	Bradenton, Florida, USA
6	66.1[redacted]	te0-0-0-0.edge01.tpa.peak10.net	Fort Mill, South Carolina, USA
7	148.[redacted]	be31.bbrt01.tpa01.flexential.net	Allentown, Pennsylvania, USA
8	148.[redacted]	be120.bbrt01.mia10.flexential.net	Allentown, Pennsylvania, USA
9	148.[redacted]	be21.brdr10.mia10.flexential.net	Allentown, Pennsylvania, USA

Email Summary

From: noreply@losant.com
To: [redacted]@gmail.com
Date: [redacted] -0400
Subject: Register for the Sierra Wireless + Losant Webinar
Location: Ashburn, Virginia, USA

Misdirected: No
Abuse Address: abuse@amazonaws.com
Abuse Reporting: To automatically generate an email abuse report click here
From IP: 54.174.52.143

System Information:

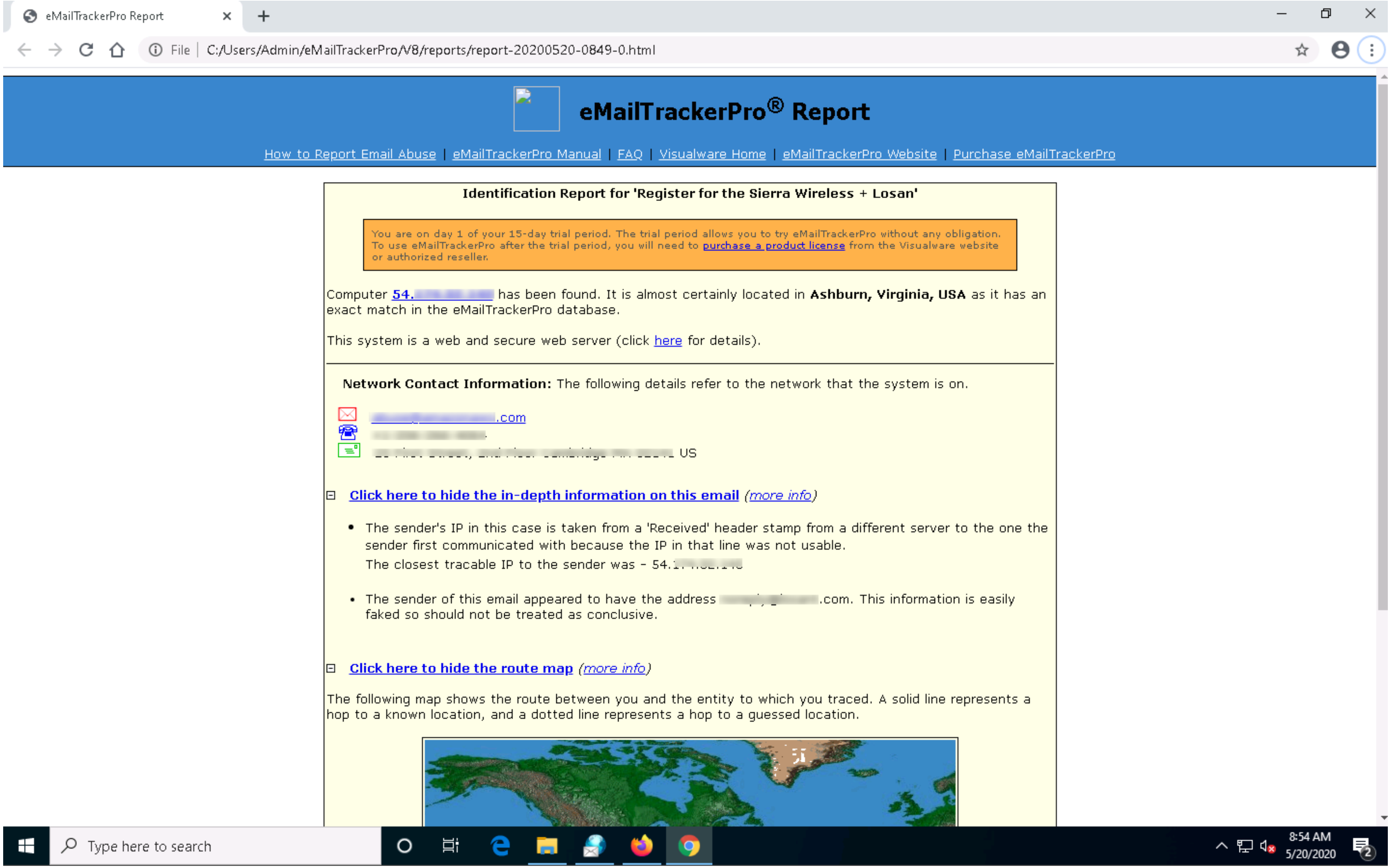
- There is no SMTP server running on this system (the port is closed).
- The system is running a web server on port 80 (click here to view it). This means that this system serves web pages.
- The system is running a secure web server (*nginx*) on port 443 (click here to view it). This means that this system serves encryped web pages. It therefore probably handles sensitive data, such as credit card information.
- There is no FTP server running on this system (the port is closed).

For 24 hours only you can get up to 20% off eMailTrackerPro! Click Here

15. □ 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**.

16. □ Expand each section to view detailed information.



eMailTrackerPro Report
File | C:/Users/Admin/eMailTrackerPro/V8/reports/report-20200520-0849-0.html
Type here to search
8:54 AM
5/20/2020

eMailTrackerPro® Report

How to Report Email Abuse | eMailTrackerPro Manual | FAQ | Visualware Home | eMailTrackerPro Website | Purchase eMailTrackerPro

Identification Report for 'Register for the Sierra Wireless + Losan'

You are on day 1 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to purchase a product license from the Visualware website or authorized reseller.

Computer **54.**[redacted] has been found. It is almost certainly located in **Ashburn, Virginia, USA** as it has an exact match in the eMailTrackerPro database.

This system is a web and secure web server (click here for details).

Network Contact Information: The following details refer to the network that the system is on.

✉ [redacted].com
☎ [redacted]
[redacted] US

⊟ **Click here to hide the in-depth information on this email** (*more info*)

- The sender's IP in this case is taken from a 'Received' header stamp from a different server to the one the sender first communicated with because the IP in that line was not usable.
  The closest tracable IP to the sender was - 54.[redacted]
- The sender of this email appeared to have the address [redacted].com. This information is easily faked so should not be treated as conclusive.

⊟ **Click here to hide the route map** (*more info*)

The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.

17. □ This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.

18. □ 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.

19. □ Close all open windows and document all the acquired information.