

# Lab 7: 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::

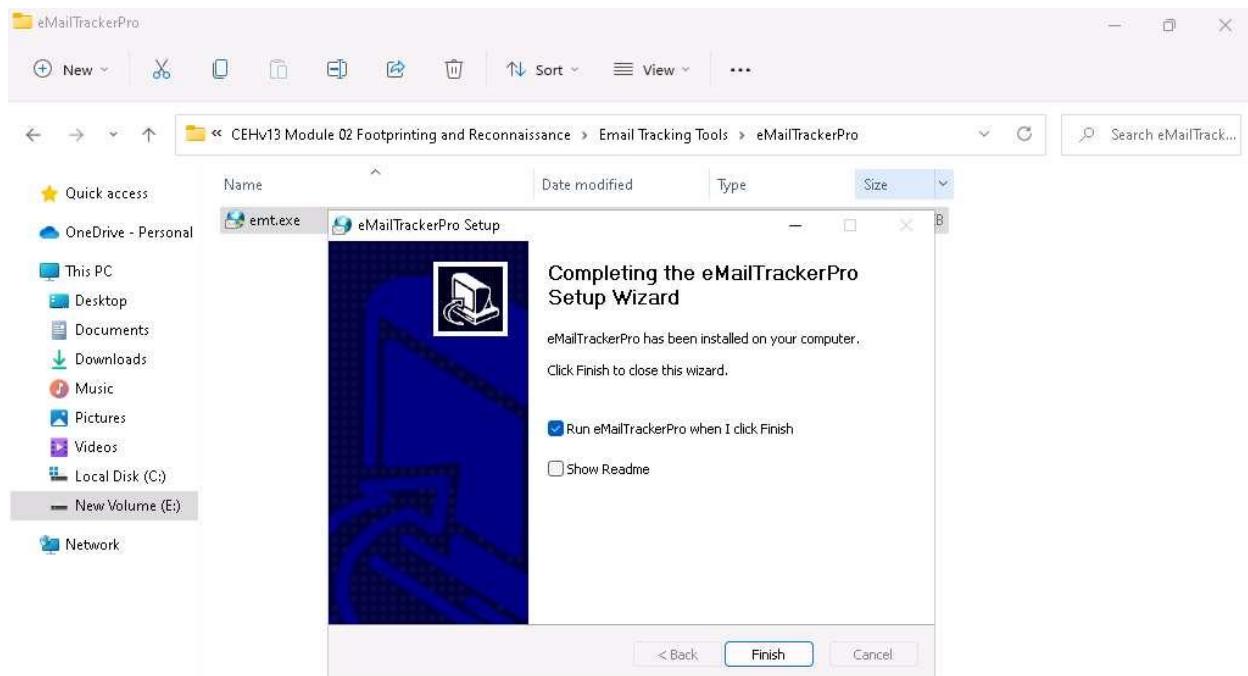
- Recipient's system IP address
- The GPS coordinates and map location of the recipient
- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- The time spent reading the email
- Whether or not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

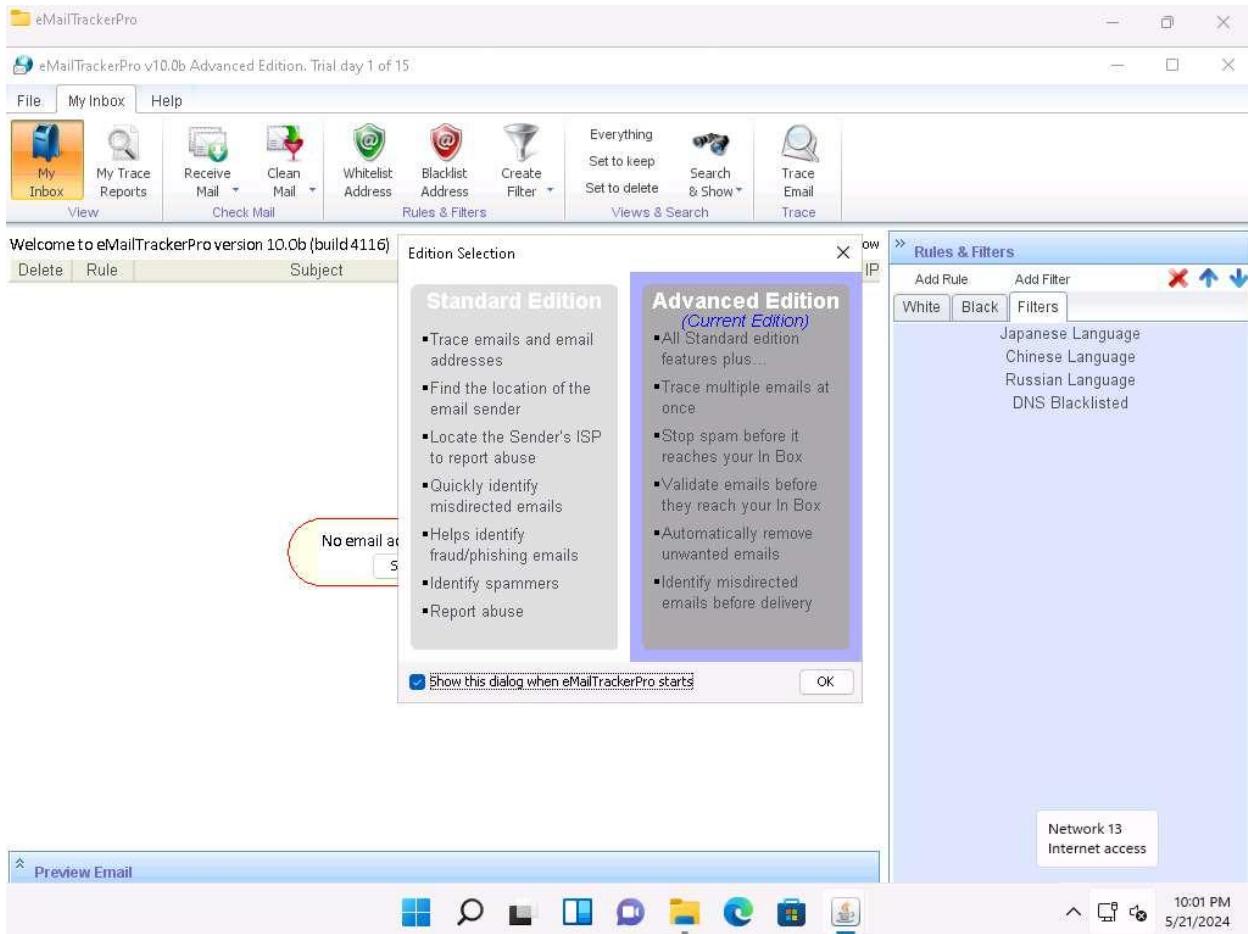
The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email 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.

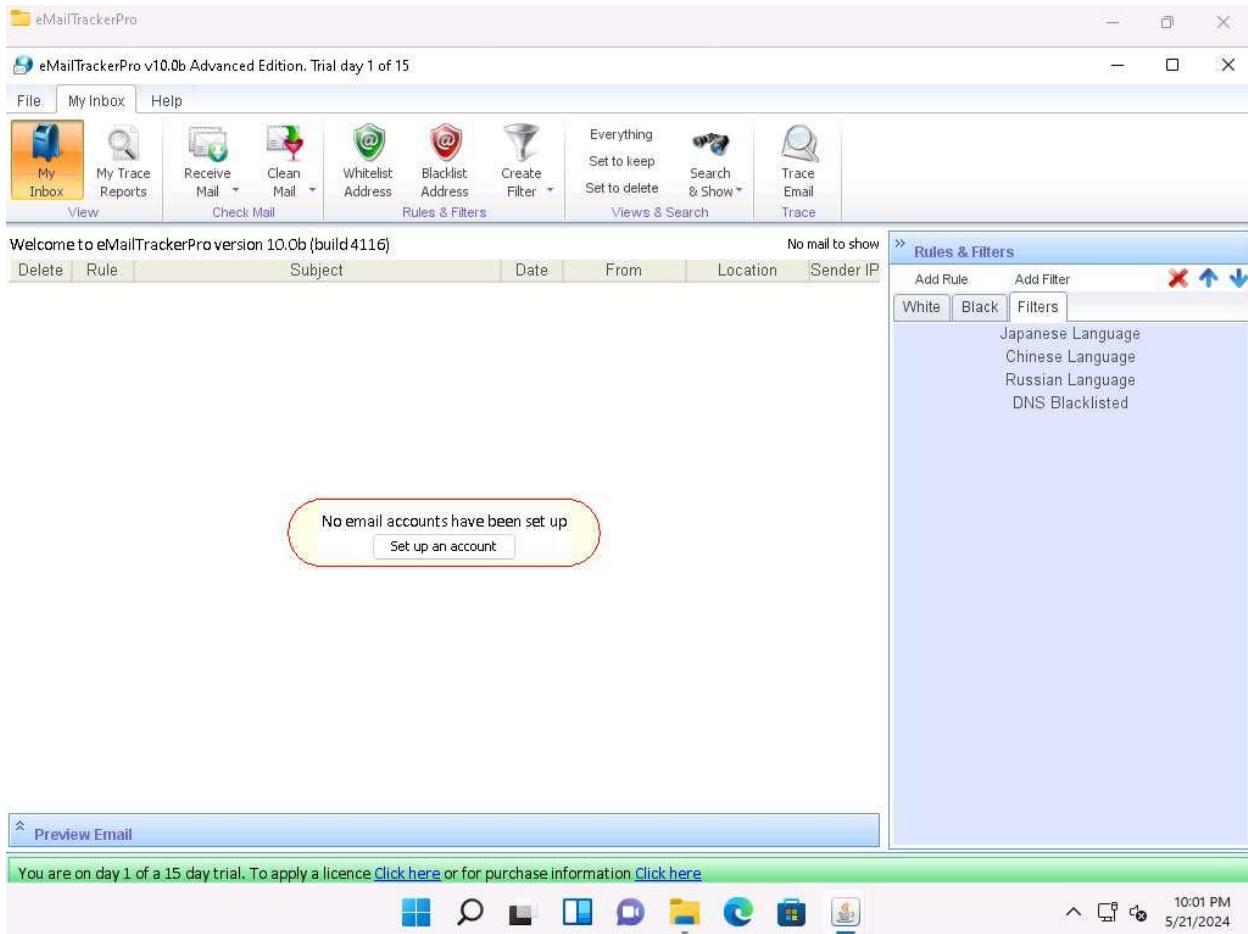
1. Click [Windows 11](#) to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 02 Footprinting and Reconnaissance>Email Tracking Tools\EmailTrackerPro** and double-click **emt.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. The **eMailTrackerPro 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.



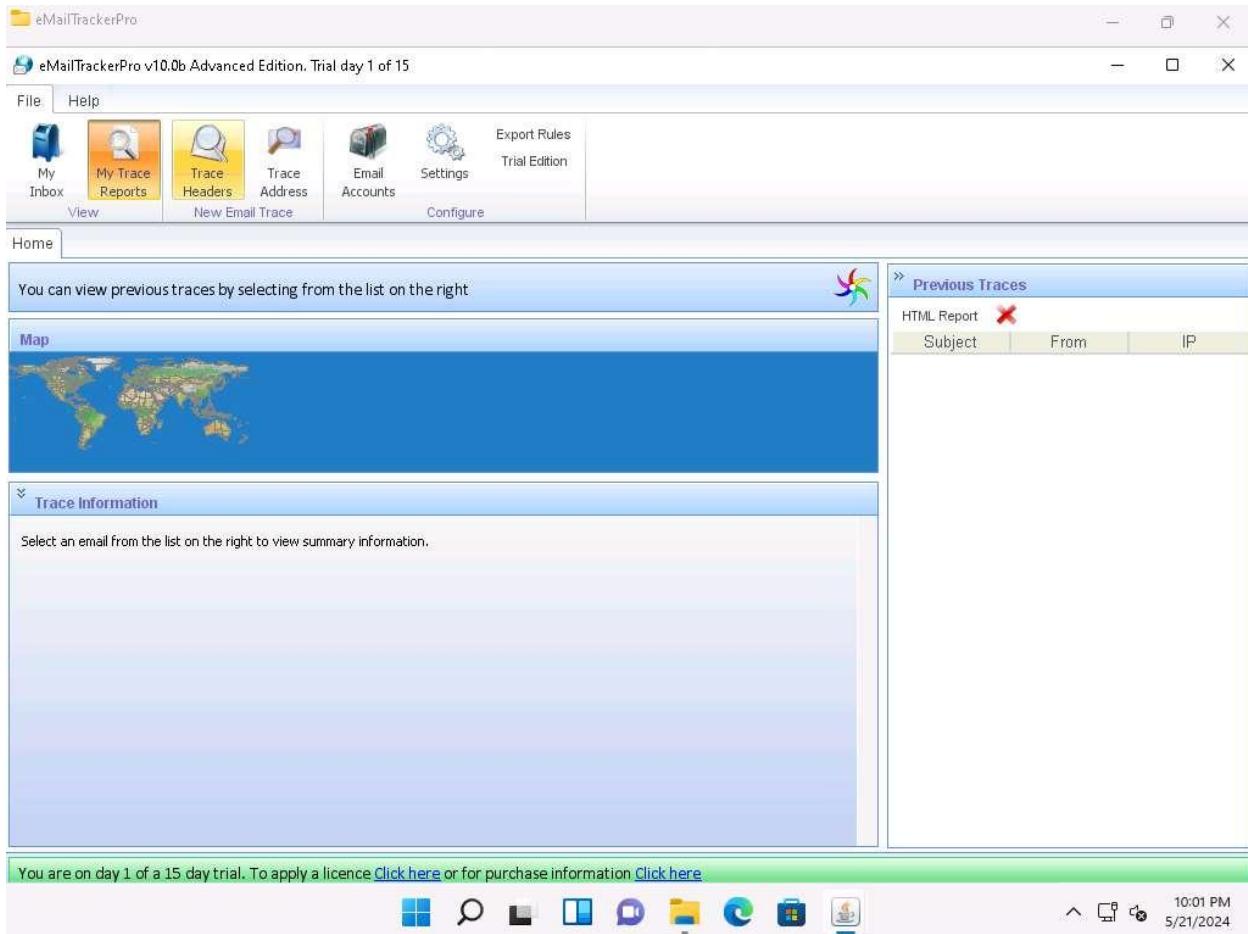
5. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.



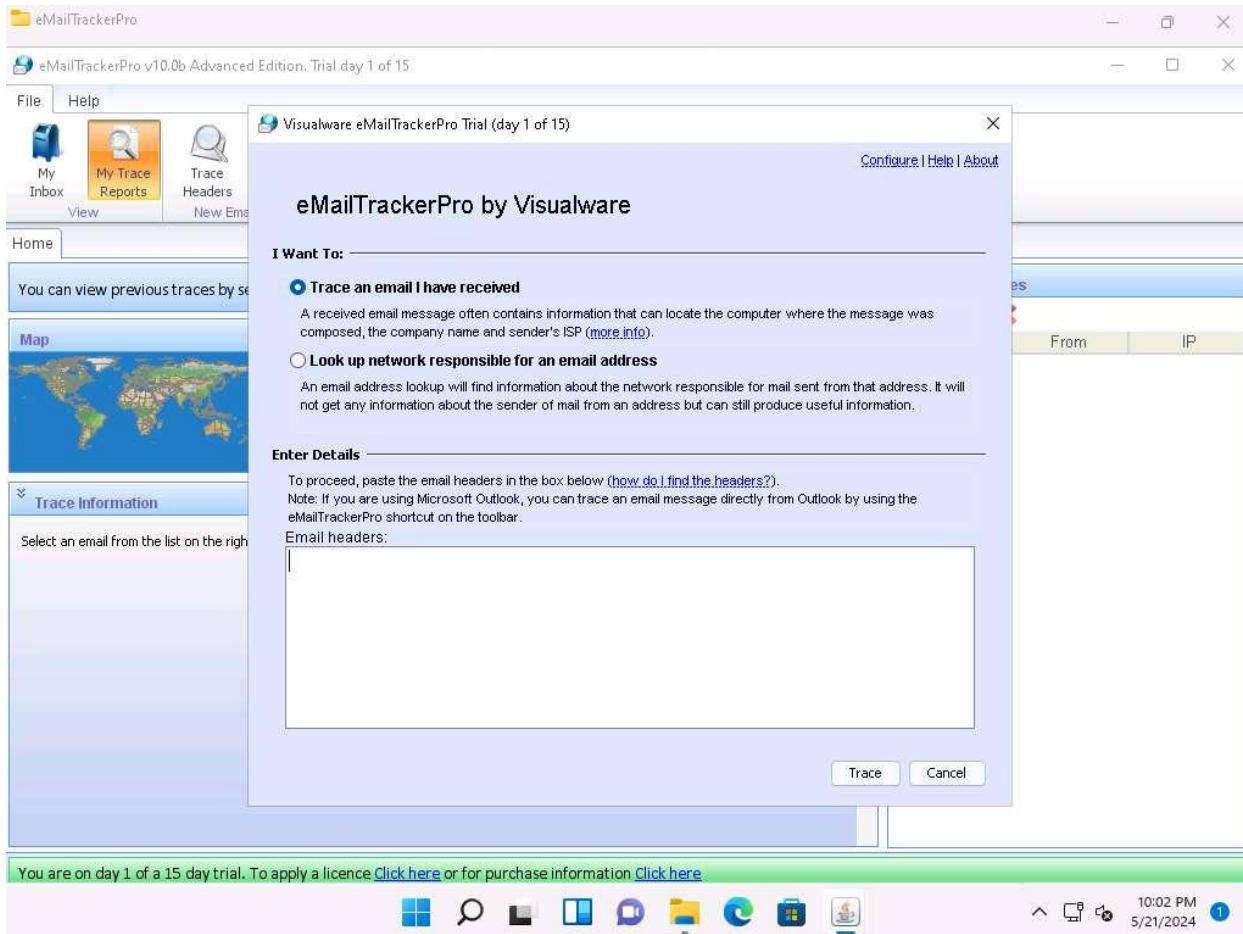
6. The eMailTrackerPro main window appears, as shown in the screenshot.



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.



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.



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

Original message

Message ID	<[REDACTED]@accounts.google.com>
Created on:	6 May 2024 at 21:54 (Delivered after 2 seconds)
From:	[REDACTED]@accounts.google.com
To:	[REDACTED]@gmail.com
Subject:	Security alert
SPF:	PASS with IP 209.85.220.73 <a href="#">Learn more</a>
DKIM:	'PASS' with domain accounts.google.com <a href="#">Learn more</a>
DMARC:	'PASS' <a href="#">Learn more</a>

[Download original](#) [Copy to clipboard](#)

```

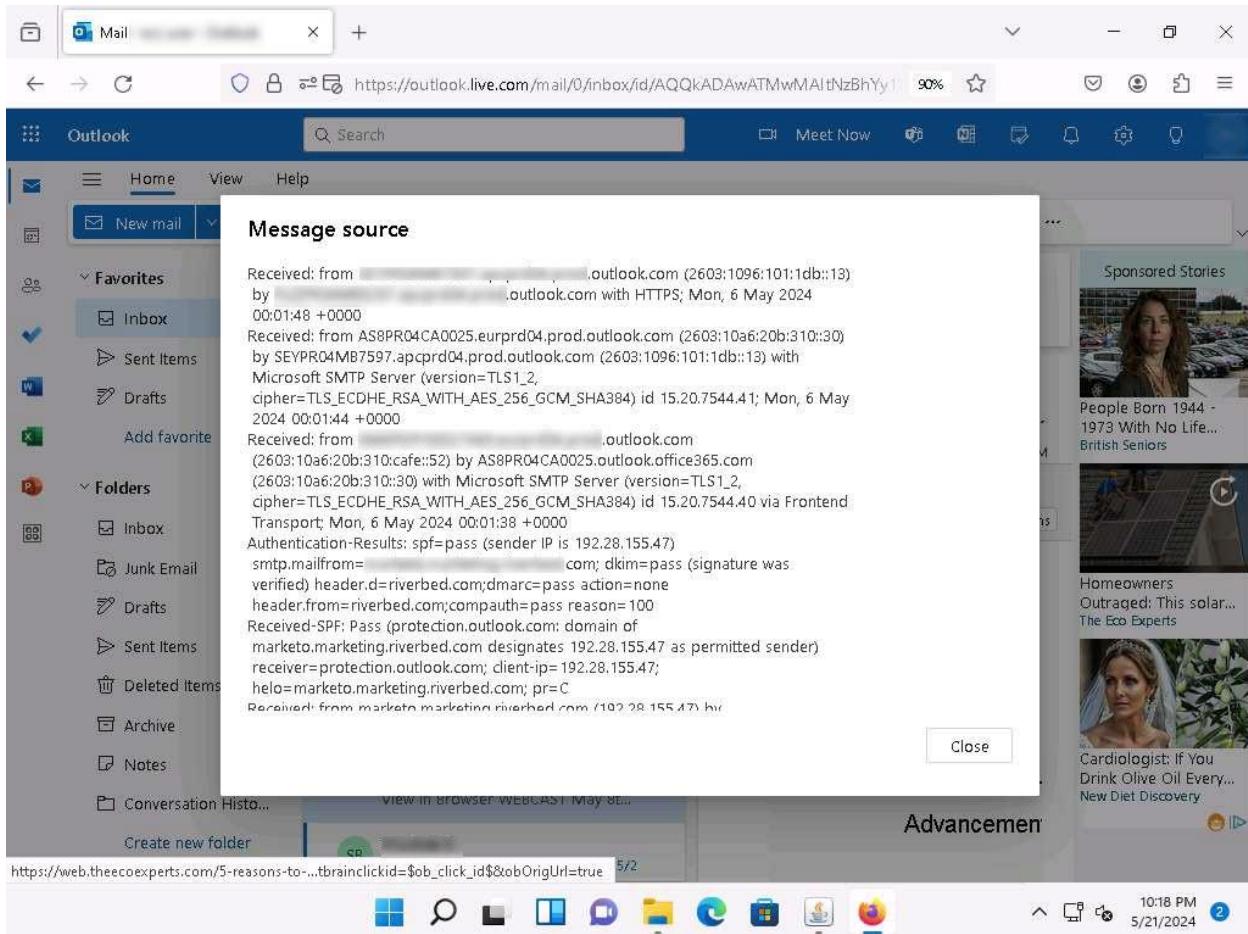
Delivered-To: [REDACTED]@accounts.google.com
Received: by 2002:a17:522:8809:b0:57f::019:7b93 with SMTP id cg9csp1708318pbv;
Mon, 6 May 2024 21:54:07 -0700 (PDT)
X-Received: by 2002:a05:6102:818:b0:47b:d3a9:e6ee with SMTP id g24-2002a056102081800b0047bd3a9e6eemr12195506vzb.
21.1715057647027;
Mon, 06 May 2024 21:54:07 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1715057647; cv=none;
d=google.com; s=arc-20160316;
b=HNzc59xx8Um2B+i408qjh491Zrt/Vmtm8kR/6jZ0yGTUv+x445b+p4RFmgcSLqhKT1w
H1UHszyp77zwXNx019k39WjNTGF1990Eb3A3VYDxk/JiR3XPMGhb5ghlrQpPKmsuS1RYu

```

10:11 PM  
5/21/2024

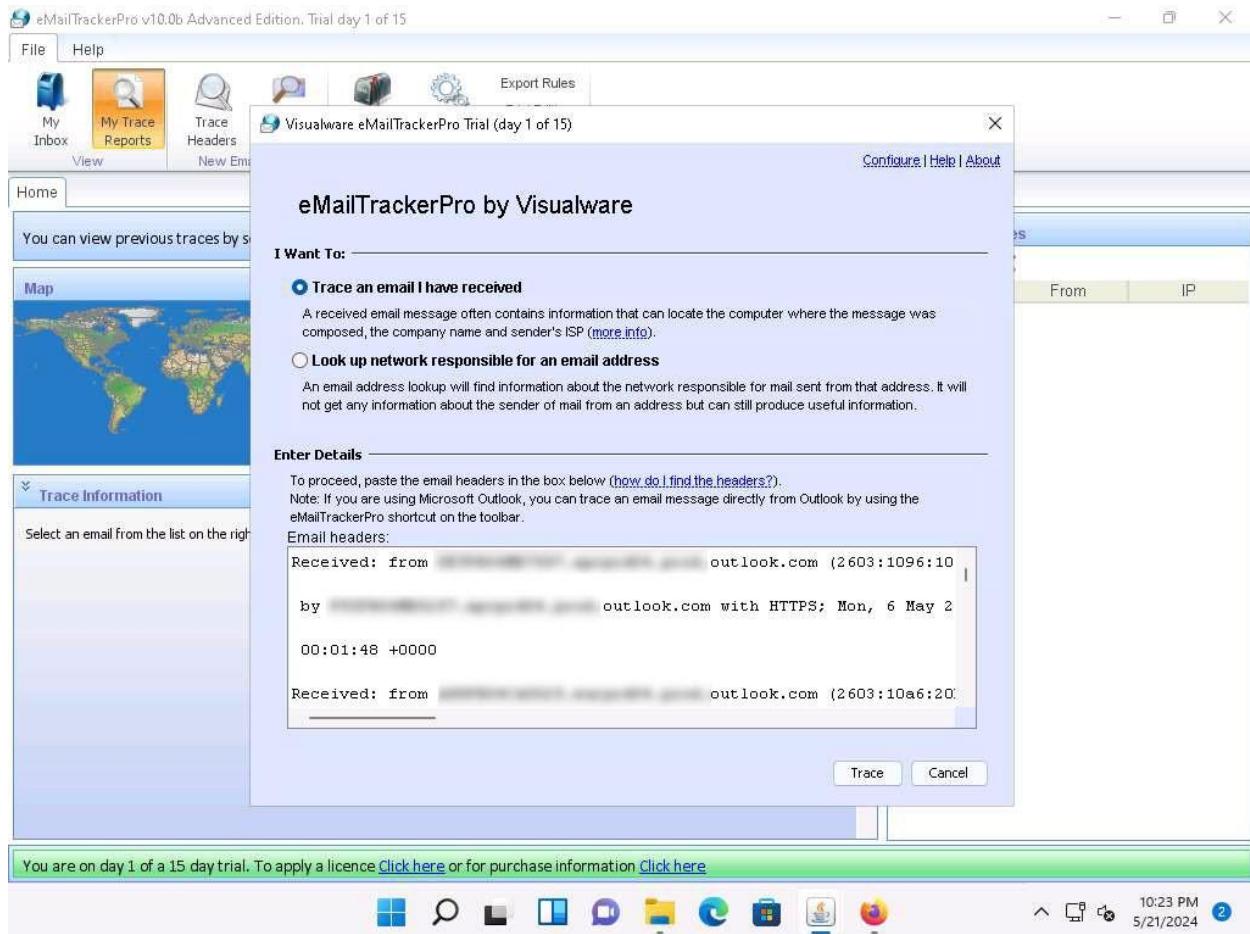
In **Outlook**, find the email header by following the steps:

- 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**
- The **view message source** window appears with all the details about the email, including the email header



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.



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.

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

File Help

My Inbox My Trace Reports Trace Headers Trace Address Email Accounts Settings Export Rules Trial Edition

View New Email Trace Configure

Home Subject: Last Chance! ... X

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

New Trace View Report

**Email Summary**

From: [REDACTED]  
 To: [REDACTED]  
 Date: Sun, 5 May 2024 19:01:35 -0500 (CDT)  
 Subject: Last Chance! Register for Riverbed Launch Webcast  
 Location: [America]

Misdirected: No  
 Abuse Address: mktabuse@adobe.com  
 Abuse Reporting: To automatically generate an email abuse  
 From IP: 192.28.155.47

System Information:

- The system is running a mail server (\*\*\*\*\* port 25. This means that this system can be used to send emails)
- There is no HTTP server running on this system (the port 80 is free)
- There is no HTTPS server running on this system (the port 443 is free)
- There is no FTP server running on this system (the port 21 is free)

**Network Whois**

**Domain Whois**

**Email Header**

You are on day 1 of a 15 day trial. To apply a licence [Click here](#) or for purchase information [Click here](#)

10:27 PM 5/21/2024 ②

#	Hop IP	Hop Name	Location
1	10.		
2	17.		
3	19.		
4	18.		(Australia)
6	5.5	lonap-gw-no-dns-yet.zayo.com	(Australia)
10	64.	ae15.er4.iad10.us.zip.zayo.com	(America)
11	120.	128.177.77.186.IPYX-260031-910	(America)
12	200.	rt-bt-1-be-1.va5.ne.adobe.net	(America)
13	200.	sr-cobs-1-po-6.va5.omniture.com	(America)

14. To examine the Network Whois data, click the **Network Whois** button below **Email Summary** to view the Network Whois data.

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

File Help

My Inbox My Trace Reports Trace Headers Trace Address Email Accounts Settings Export Rules Trial Edition

View Configure

Home Subject: Last Chance! ... X

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

New Trace View Report

Map

America

#	Hop IP	Hop Name	Location
1	10.1		
2	172.		
3	192.		
4	185.		(Australia)
6	5.57	lonap-gw-no-dns-yet.zayo.com	(Australia)
10	64.1	ae15.er4.iad10.us.zip.zayo.com	(America)
11	128.	128.177.77.186.IPYX-260031-91	(America)
12	208.	rt-bt-1-be-1.va5.ne.adobe.net	(America)
13	208.	sr-cdbs-l1-po-6.va5.omnitrite.com	(America)

You are on day 1 of a 15 day trial. To apply a licence [Click here](#) or for purchase information [Click here](#)

Network Whois

```

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy
#
# Copyright 1997-2024, American Registry for Internet Numbers
#
NetRange: 192.28.144.0 - 192.28.191.255
CIDR: 192.28.144.0/20, 192.28.160.0/19
NetName: MARKETO-CORE2
NetHandle: NET-192-28-144-0-1
Parent: NET192 (NET-192-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: MARKETO, Inc. (MARKE-120)
RegDate: 2014-02-27
Updated: 2024-02-06

```

Domain Whois

Email Header

10:37 PM 5/21/2024 ②

15. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
16. You can also use email tracking tools such as **MxToolbox** (<https://mxtoolbox.com/>), **Social Catfish** (<https://socialcatfish.com/>), **IP2Location Email Header Tracer** (<https://www.ip2location.com/>) etc. to track an email and extract target information such as sender identity, mail server, sender's IP address, location, etc.
17. Close all open windows and document all the acquired information.