



FORENSICS V2 LAB SERIES

Lab 12: Email Analysis

Document Version: 2021-01-14

Copyright © 2021 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and other countries. Google is a registered trademark of Google, LLC. Amazon is a registered trademark of Amazon in the United States and other countries.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Extracting and Understanding an Email Header	6
2 Parsing Email Headers with Email Header Analyzer	21

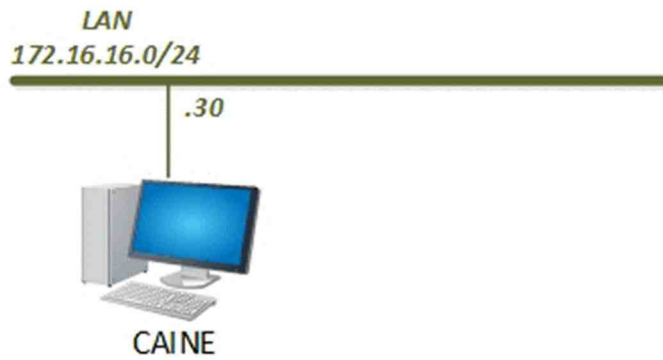
Introduction

Since email messages remain the most popular means of communication for businesses, it is essential to understand how they work and to learn how to investigate the tons of metadata they store.

Objectives

-) Learn what an email header is
-) Learn what type of data is stored in the email header and how it can help an investigation
-) Learn how to use Email Header Analyzer to parse email headers

Lab Topology



Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
Caine	172.16.16.30	caine	Train1ng\$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng\$
WinOS	172.16.16.10	Administrator	Train1ng\$

1 Extracting and Understanding an Email Header

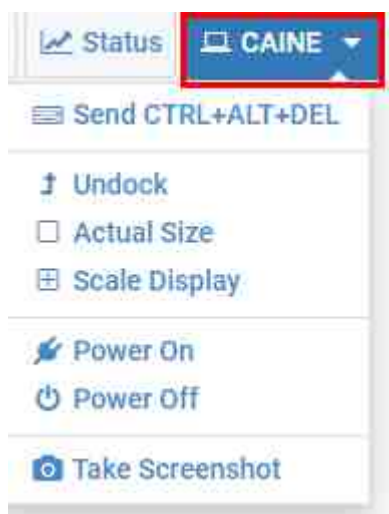
As a forensic examiner, the 2 main types of email files you encounter will be web-based email and email client database files. The webmail email is stored on the email company's mail server, and the user can access these emails using a web browser. This means that when the webpage is closed, the emails are no longer accessible to the user. The email client's database files allow the user to access their emails even when they are not connected to the internet. The emails are downloaded to a database file on the computer. Some of the most popular file extensions that email clients use are PST, OST, EDB, and MBOX. Individual emails can also be stored as files with extensions like PDF, HTML, MSG, and EML.

Regardless of how the email is stored, examiners should be able to identify and interpret the metadata within them. In this lab, we will delve into the email header, which is where the metadata for email files is stored. We will use an email client called Thunderbird Mail. It is a free and open-source email client that stores data in the MBOX format.

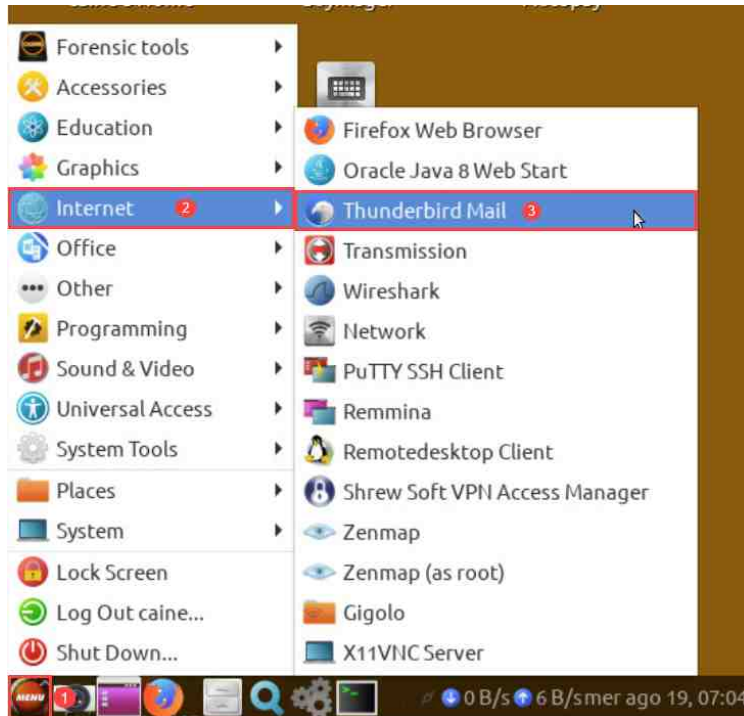
Please note that email investigations can be performed live, while systems are running. It is always recommended, however, to make a forensic copy of the drive or email file(s) before performing examinations. There are some situations where it is ok to access and review the headers for collection, such as time-sensitive situations or no access to email collection tools. In this lab, we will focus on the latter, live acquisition, and a review of email headers.

Let us get started by opening the Thunderbird Mail program.

1. To begin, launch the CAINE virtual machine to access the graphical login screen. Log in as `caine` using the password: `Trai n1ng$`

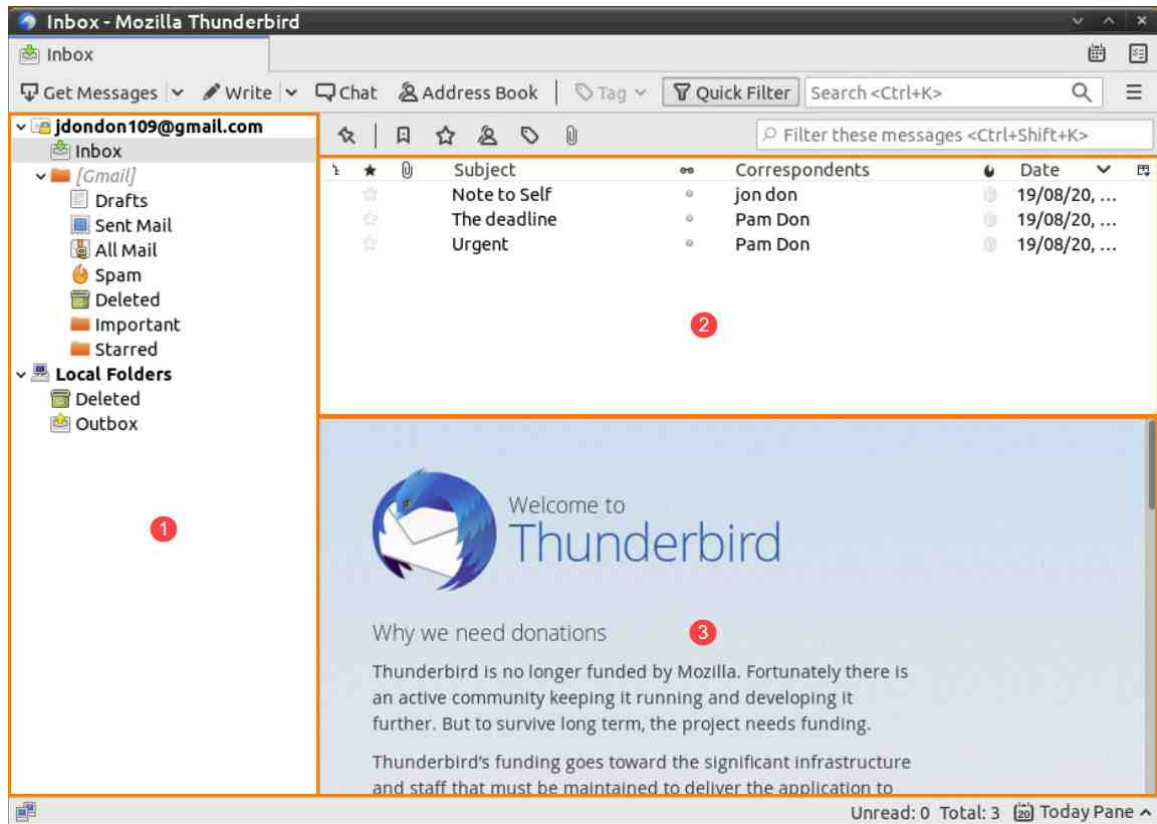


2. Once you are logged into the VM, launch the Thunderbird Mail program from the application menu by navigating to Application Menu > Internet > Thunderbird Mail, as seen in items 1, 2, and 3 below.

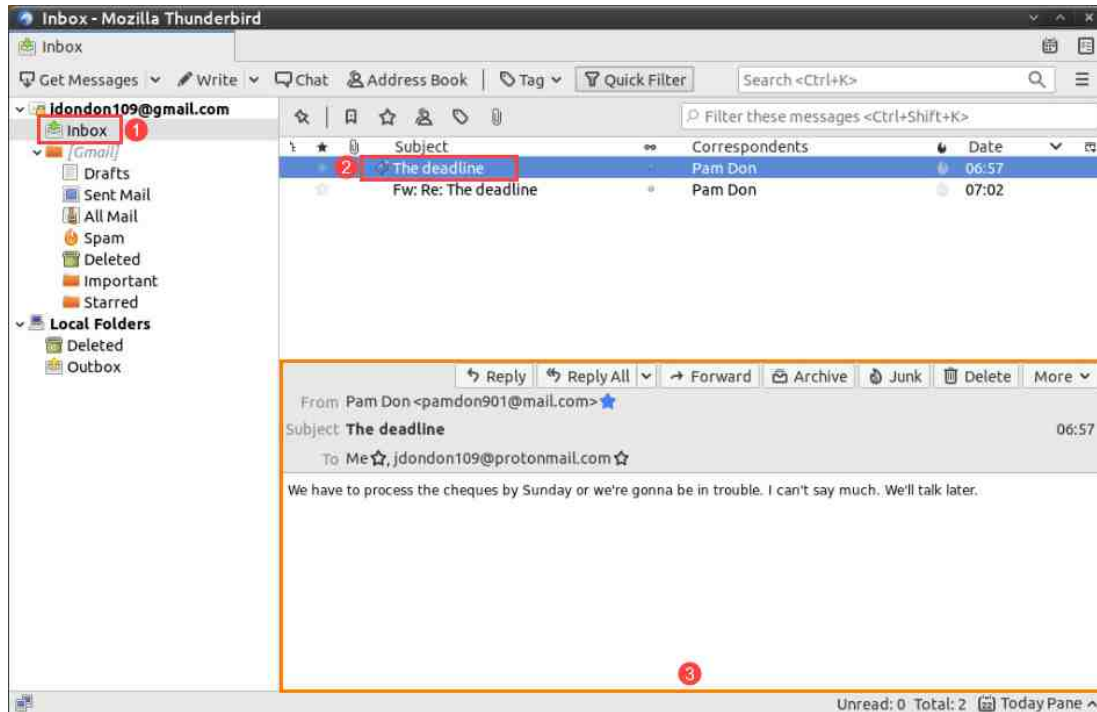


A browser window may appear in attempts to log in to the mail server associated with the email account in Thunderbird. There is no internet connectivity within the VM so feel free to close the browser window.

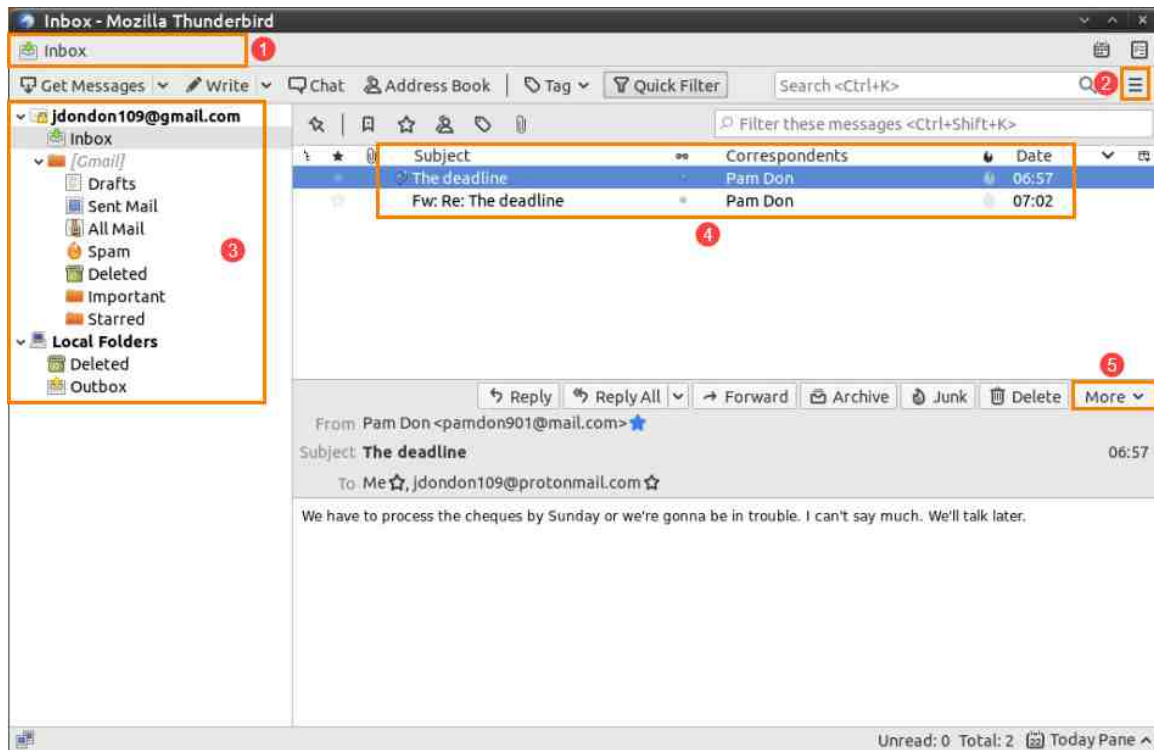
3. Thunderbird will open and you will see the familiar tree pane, list pane, and view pane layout as seen in items 1, 2, and 3 below. Using this interface is the same as the other tools we used in the past. You can navigate the folder tree in the tree pane in item 1. The emails within each folder will be displayed in item 2 in the list pane. Finally, the email body can be seen in the view pane in item 3.



- Let us open an email. To do this, click the Inbox folder and then click the first email, called The deadline, as seen in items 1 and 2 below. As you can see, the email's body appears in the view pane, as seen in item 3 below.

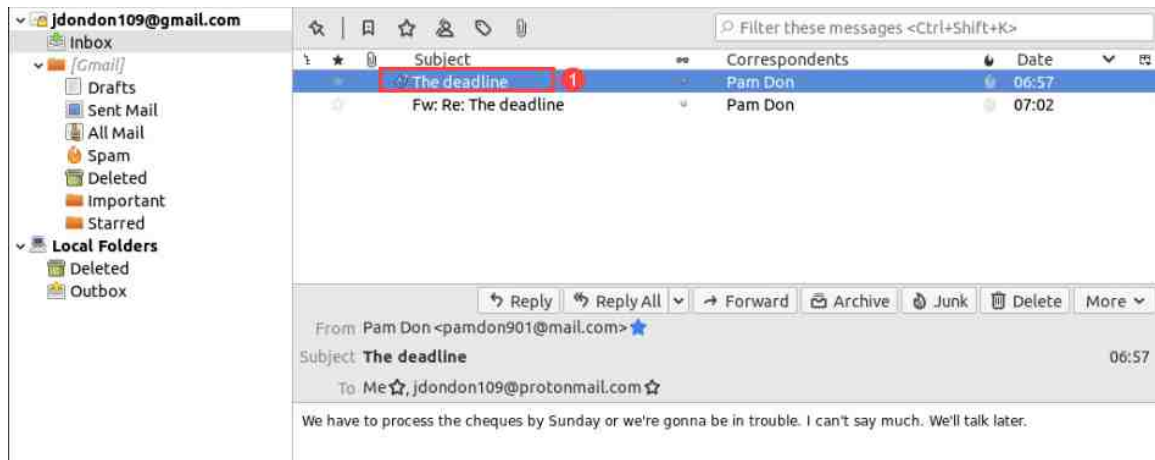


5. We will now look at the interface. The table below the following screenshot provides details about some of the features and settings we will use in this exercise. For more help and information about the program's features, you can access the help menu by clicking the menu button and navigating to Help, or by pressing F1.

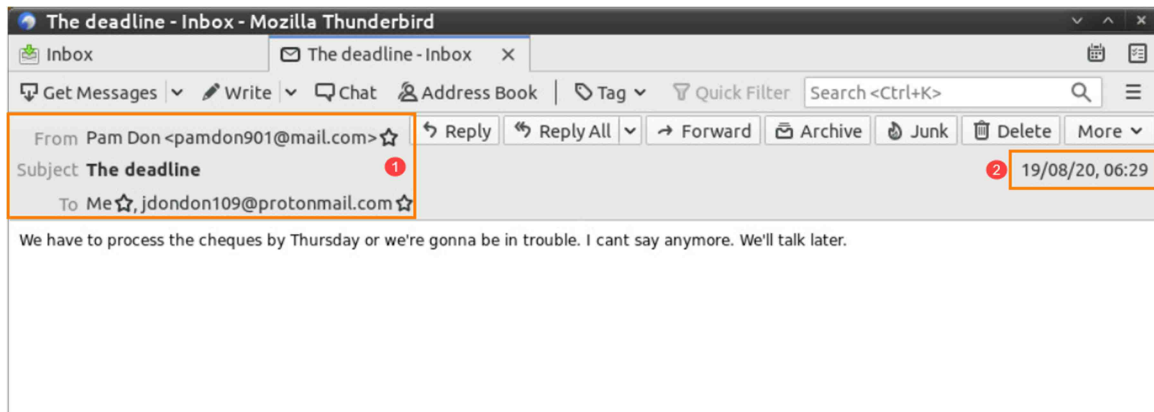


1	The area highlighted as item 1 is the tab selection area. The emails can be opened in different tabs to make it easier to navigate. Each tab will be shown in this area and can be moved or closed.
2	The area highlighted as item 2 is the Menu button and contains a dropdown menu that provides access to the File menu, Edit menu, Help menu, and many other important settings and options.
3	The area highlighted as item 3 lists each mailbox that is added to Thunderbird.
4	The area highlighted as item 4 is the file list area, and the columns provide details about the email's subject, the sender and other recipients, and the date and time that the email was received. It can also be configured to show more or less data.
5	The area highlighted as item 5 contains a dropdown list that provides additional options and settings for the specific mail item selected in the List pane above it.

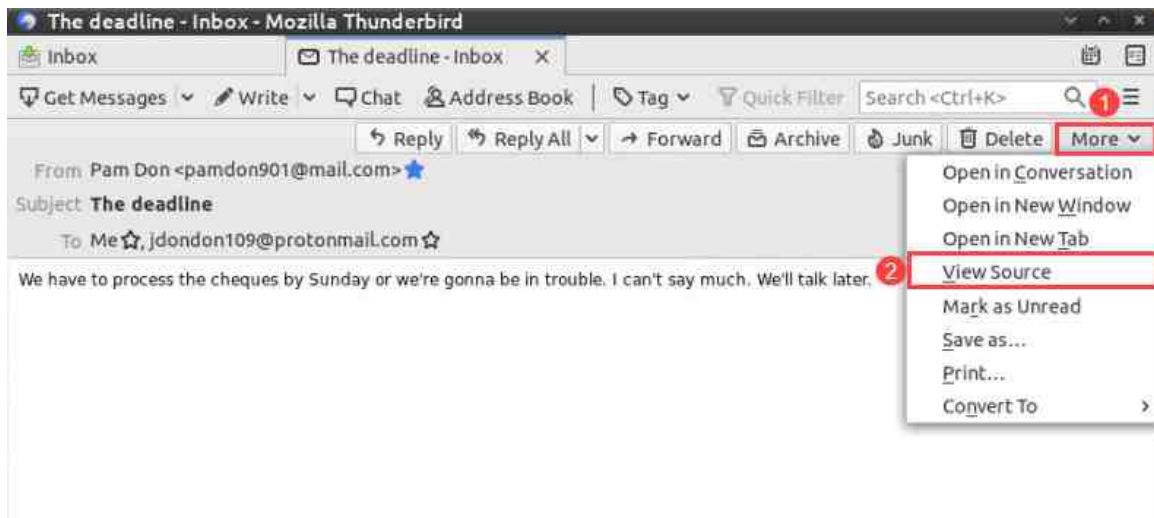
6. Now that you are a little more familiar with the software's features, let us take a closer look at the email we selected earlier. The email has some metadata that is already helpful. Let us take a closer look at the data in it. First, let us double-click the email, The deadline, from the file list pane in item 1 to open it in a new tab.



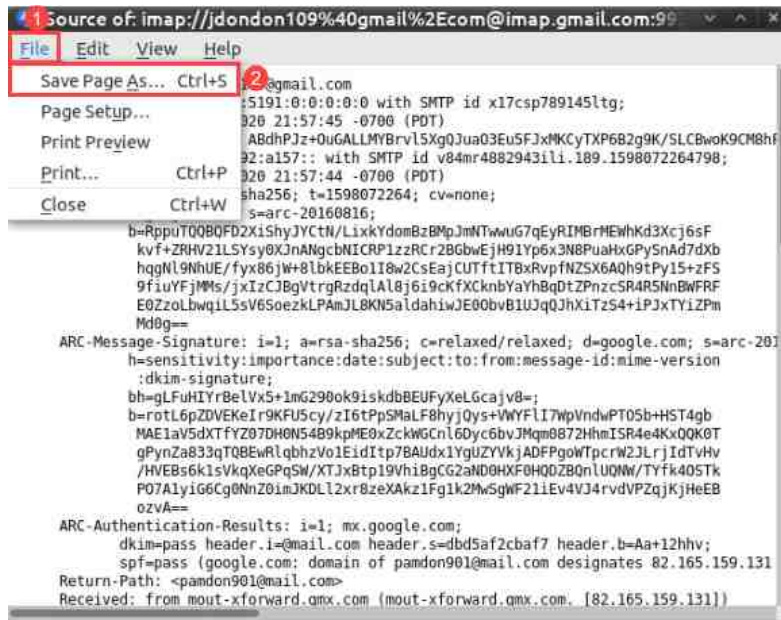
- Now that the email has its own tab, let us look at its contents. In item 1 below, we can see the sender, email subject, and recipients. In item 2, we can see the date the email was received. This information is helpful, but the header contains a lot more data and can be accessed very easily.



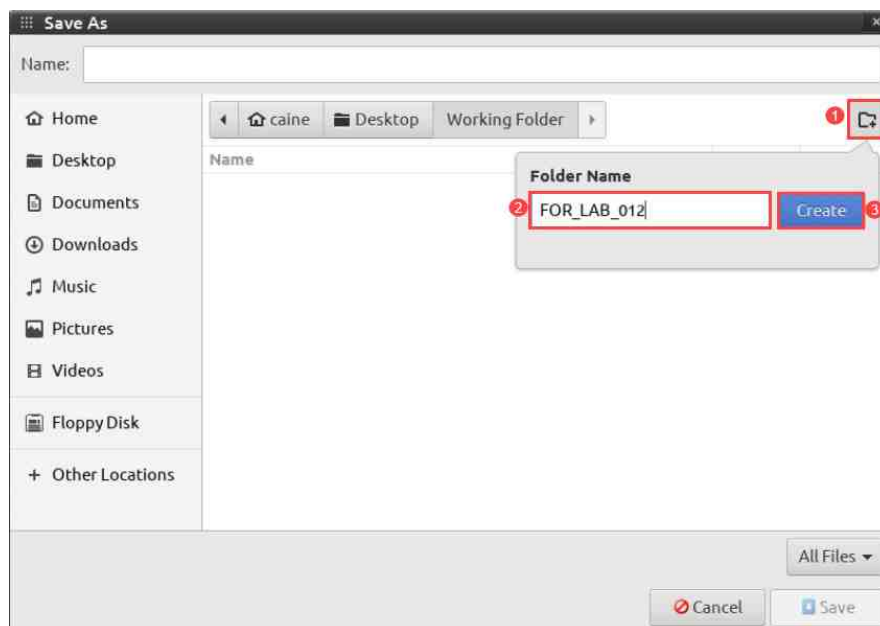
- Let us capture the email header for this email and save it so that we can review it later. Begin by clicking More > View Source as seen in items 1 and 2 below.



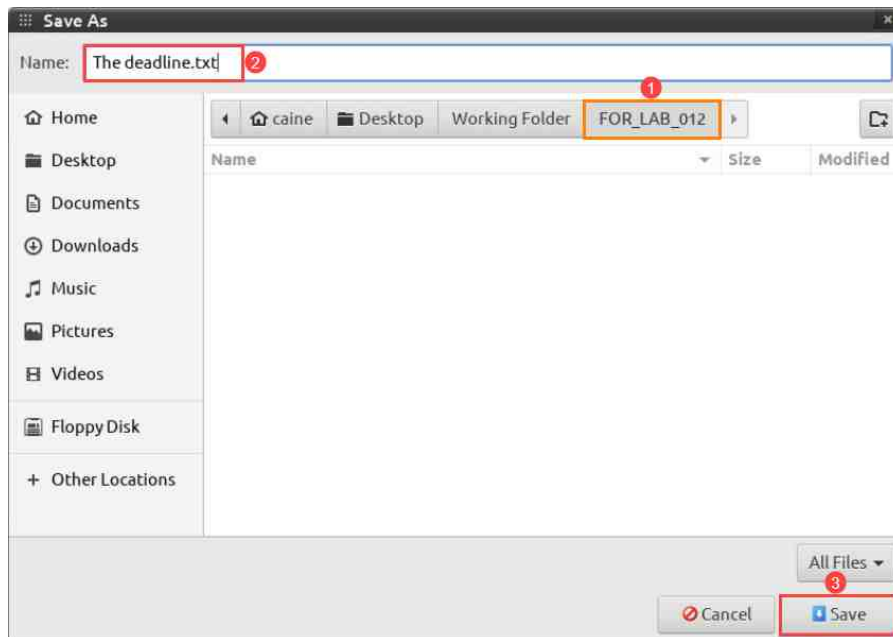
9. The window that appears will contain the header information for the selected email. There is a lot of data, and it can seem overwhelming, but there is a certain way to read the header information that makes it much easier to manage. We will go through that process after the header is saved. Let us do that by clicking File > Save Page As, as seen in items 1 and 2 below.



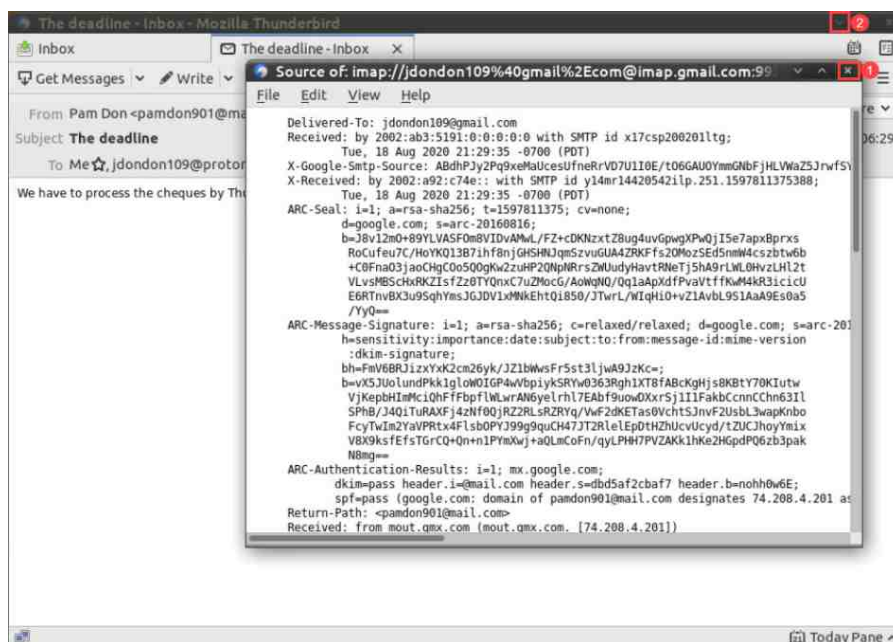
10. The Save as window will appear. Use this window to browse to Desktop > Working Folder and create a new folder by clicking the New Folder icon as seen in item 1 below. Name the new folder FOR_LAB_012 and then click Create as seen in items 2 and 3 below.



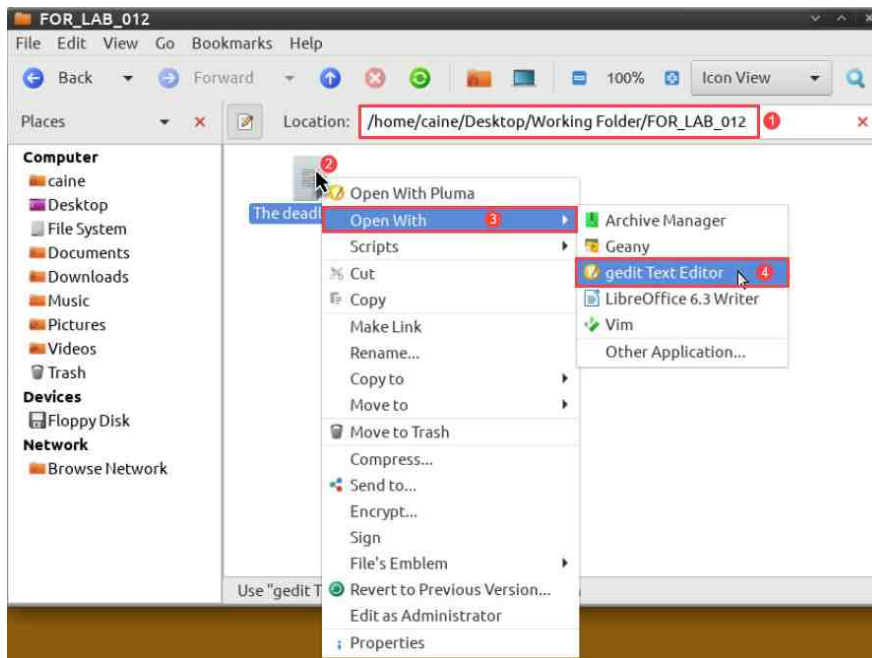
11. Double-click the folder you just created called FOR_LAB_012 to open it. We will save the email header here. To do this, type the filename you want to use; we will use the subject of the email, The deadline.txt, as seen in item 2 below. Once you are done, click Save as seen in item 3 below.



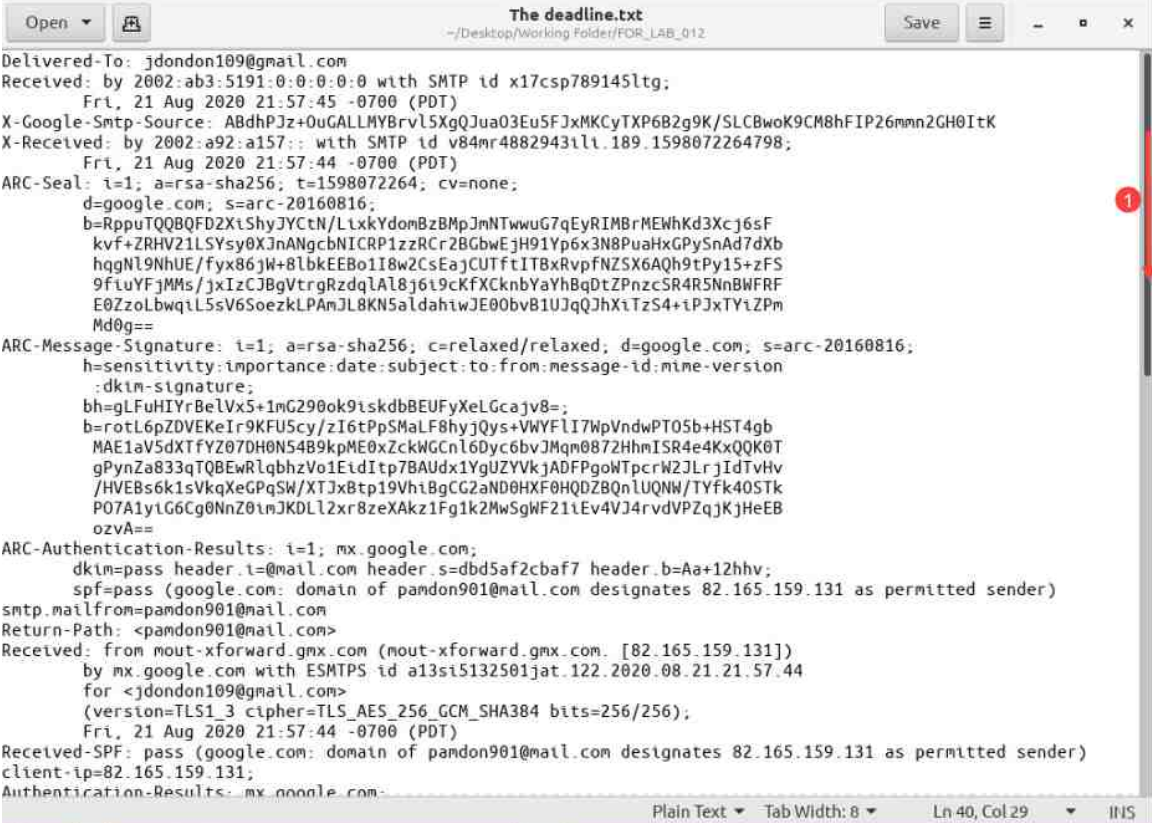
12. Now that the file is saved, let us close the Source window, minimize Thunderbird, and browse to the folder that we just created. Close the Source window by clicking the X, as seen in item 1 below. Next, minimize Thunderbird by clicking the Minimize button, as seen in item 2 below.



13. Now browse to the file you created at Desktop > Working Folder > FOR_LAB_012 as seen in item 1 below. Once there, right-click the file called, The deadline.txt, then select Open With > gedit Text Editor as seen in items 2, 3, and 4 below. The file you created will now be opened in the gedit Text Editor.



14. Once the file is open, we can begin reading through the data. When reading email headers, it is always advised to start from the bottom. This is mainly because the email passes through different servers during transmission, and each one adds data to the top of the header. This means the sequence of events are stacked on top of each other and the oldest data is found at the bottom. Let us scroll to the bottom of this email header by dragging the scroll bar as seen in item 1 below or by scrolling the mouse wheel.



```

Open [icon] The deadline.txt
~/Desktop/Working Folder/FOR_LAB_012 Save [icon] [icon] [icon] [icon]

Delivered-To: jdondon109@gmail.com
Received: by 2002:ab3:5191:0:0:0:0:0 with SMTP id x17csp789145ltg;
  Fri, 21 Aug 2020 21:57:45 -0700 (PDT)
X-GoogLe-Smtp-Source: ABdhPJz+OuGALLMYBrvL5XgQJua03Eu5FJxMKCyTXP6B2g9K/SLCBwoK9CM8hFIP26mmn2GH0ItK
X-Received: by 2002:a92:a157:: with SMTP id v84mr48829431l1.189.1598072264798;
  Fri, 21 Aug 2020 21:57:44 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1598072264; cv=none;
  d=google.com; s=arc-20160816;
  b=RppuTQ8QFD2XiShyJYCtN/LtxkYdomBzBMPjMNTwwuG7qEyRIMBrMEWhKd3Xcj6sF
  kvf+ZRHV21LSYsy0XJnANGcbNICRP1zzRCr2BGbWjH91Yp6x3N8PuaHxGPySnAd7dXb
  hggNl9NhUE/fyx86jW+8lBkEEBo1I8w2CsEajCUTftITBxRvpfNZSX6AQh9tPy15+zFS
  9ftuYfjMMs/jxIzCJBgVtrgRzdqLA18j6i9cKfXCknBYaYhBqDtZPnzcSR4R5NnBwFRF
  E0ZzoLbwqIL5sV6SoezkLPAmJL8KN5aldahiwJE00bvB1UJQJhXiTzS4+iPJxTYiZPm
  Md0g==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
  h=sensitivity:importance:date:subject:to:from:message-id:mime-version
  :dkim-signature;
  bh=gLfUHIYrBelVx5+1mG290ok9iskdbBEUFyXeLGcajv8=;
  b=rotL6pZDVEKeIr9KFU5cy/zI6tPpSMaLF8hyjQys+VWYfLI7WpVndwPT05b+HST4gb
  MAE1aV5dXTFY707DH0N54B9kpME0xZckWGCnl6Dyc6bvJMqm0872HhmISR4e4KxQQK0T
  gPynZa833qTQBEwRlqbhzVo1EidItp7BAUdx1YgUZYVkjADFpgoWTpcrW2JLrjIdTvHv
  /HVEBS6k1sVqKXeGPqSW/XTJxBtp19VhiBgCG2aND0HXF0HQDZBQnLUQNW/TYfk40STk
  P0Z1yiG6Cg0NnZ0imJKDL12xr8zeXAkz1Fg1k2MwSgWF21iEv4VJ4rvdVPZqjKjHeEB
  ozvA==
ARC-Authentication-Results: i=1; mx.google.com;
  dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=Aa+12hhv;
  spf=pass (google.com: domain of pandon901@mail.com designates 82.165.159.131 as permitted sender)
  smtp.mailfrom=pandon901@mail.com
Return-Path: <pandon901@mail.com>
Received: from mout-xforward.gmx.com (mout-xforward.gmx.com. [82.165.159.131])
  by mx.google.com with ESMTPS id a13si5132501jat.122.2020.08.21.21.57.44
  for <jdondon109@gmail.com>
  (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
  Fri, 21 Aug 2020 21:57:44 -0700 (PDT)
Received-SPF: pass (google.com: domain of pandon901@mail.com designates 82.165.159.131 as permitted sender)
client-ip=82.165.159.131;
Authentication-Results: mx.google.com;

Plain Text Tab Width: 8 Ln 40, Col 29 INS

```


15. Now that we are at the bottom of the email, let us dissect the data we see and look at some metadata that is of great value to investigations.

- The first set of data is the email body at the very bottom, as seen in item 1 below.
- Next, let us look at the data highlighted as item 2. This is the metadata we typically see when we view the email normally; it contains the sender's and recipients' email addresses, the subject of the email, and the date that it was sent.
- Next, we have the Message-ID seen in item 3. Message-IDs are unique to each email and are usually a combination of a domain name and an alphanumeric value. A Message-ID can be used to help determine the original sender. A communication service provider can use this information to uniquely identify the email and learn the IP address of the sender. The Message-ID is created by the server that sends the email message, so it can help to prove whether an email was actually sent, or whether it was just a draft moved to another folder. Finally, Message-IDs can be used to determine whether an email was a reply, a forward or if it was created from scratch. Most email replies and forwards will have a field called In-Reply-To: and/or References that provide the Message-ID of the email that it is responding to or forwarded from. Since the email below does not have these fields, we know that it was made from scratch.

```

Message-ID: <trinity-47ac3c7b-9f51-4b7f-91dd-b7e0741a9932-1598072261093@3c-app-mailcom-lxa10> 3
From: Pam Don <pamdon901@mail.com>
To: jdondon109@gmail.com, jdondon109@protonmail.com
Subject: The deadline
Content-Type: text/html; charset=UTF-8
Date: Sat, 22 Aug 2020 06:57:41 +0200
Importance: normal
Sensitivity: Normal
X-Priority: 3
X-Provags-ID: V03:K1:PBYGf0I4t9CKnTzk+p1E1xejk7kw6j57Xb0ez5q0RBEw3NUN0ClstZe5vmAEcQV41eNdh
1lubBbIfNuQdYqhUgJBkexd+uhfNNoFaR9SFdhMIzLmb+Uq1ea/7Ulutptm4+3ho0ktvYMG7Grm
rFeo5h4T4C5iKdTLxzG5G1j3W1KMKqGZM8/W+Inniy9DyAmzOf4QSK0UQaYVTsRGF07indIz6j9I
hfSSxcDxfz4bvn5A8G8hVX/VLswN0Z9ye4tYqglqWhVz3LVaaNGS+JGgkSy0yL0jC5ncq0B1GMBt
Ag=
X-Spam-Flag: YES
X-UI-Out-Filterresults: junk:10;V03:K0:Pabl6RZMjmo::qxdxnoLdtLRZSZE8TDe9wrKg
+5ZueEvYEF6wP5hQo59kXC8QhRxxX9GJSvcqQ3/takbemZP4CT8+5drrNPt+Z3CG8+SkMMJZx2
Jhebf/V3+2SEyoyRfNm1K0qx0wdp9xa4GB56Vn6tYjLhN6JjGH/0aYBko2GYLRkoCRn1Qwu4
5JdGeQZRWCKBWPiVwP8TY+WakBUSPJj2wffKa57s1TEoz/facFMrmRKYhk90+a1M4jADdtS9/
AxEpJOT2R2hxbRYHs5iY/26JH8FuLvxjMGy/zmNTBYCR2+S0qsUj1IrJcRQmWjkiV0ri489
dfbVrLpSwW8zLMDz+7Se6MasNLY9vUCVQfDEhPo9T8vKm4j5/5Pr9vqblphM2beltd0Y87UE
ULSMAstldABJ2XVefQ0x4fgMSVoh6xha/LzI3cCqsZnThQb7JvEMEMueldo1+tr1nq0FJnnDa
uYNpuBCzLizyXIk7k5+hmV+kH0fJS2b8YCUiZ5mdr0mSSb6sCiE5jyAmNnt5vzZ7x2ThycPNC
t+qtvFA3g6Z0GlnX0sY4h022w5z22PuW0Fj59CQb/p8HKXuzMkrrFo+ZMyA2Dd9tcm2+QMjW
r0hRL2GJFeUW1IFcSSMuI1jkeFnGKQTz1Odbub4LRW7ncuFL6Q4BDgIRcm9kdQ4rY6mrtcngC
S7ZZMdmrCLzFXztpc242t/nXromtv25DTLNVqep/LsMakXDKB3um6pALbn9iakSkvF0pTZt
yQZze8IGCttGMe
<html><head></head><body><div style="font-family: Verdana;font-size: 12.0px;"><div>We have to process the
cheques by Sunday or we&#39;re gonna be in trouble. I can&#39;t say much. We&#39;ll talk later.</div></div></
body></html>

```

16. Let us scroll up until Message-ID is at the bottom of the page, as seen below. The data highlighted as item 1 provides data about the first server that received the email. This entry is very important as it can also contain the IP address of the individual who sent the message. Some service providers prevent this data from being divulged, however. As you can see, it states that the message was sent from 174.128.225.186 and was received by web-mail.mail.com. The IP address refers to the one assigned to the sender, and it indicates that it was received by the mail.com webserver called web-mail.mail.com or 3c-app-mailcom-lxa10.server.lan. Next, look at the data highlighted in items 2 and 3. These are the Domain Keys Identified Mail (DKIM) and the Sender Policy Framework (SPF). They are security features used by email servers to assist in detecting spoofed and tampered emails.

```
-----
ARC-Authentication-Results: i=1; mx.google.com;
    dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=Aa+12hhv;
    spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender)
    smtp.mailfrom=pamdon901@mail.com
Return-Path: <pamdon901@mail.com>
Received: from mout-xforward.gmx.com (mout-xforward.gmx.com. [82.165.159.131])
    by mx.google.com with ESMTPS id a13si5132501jat.122.2020.08.21.21.57.44
    for <jdondon109@gmail.com>
    (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
    Fri, 21 Aug 2020 21:57:44 -0700 (PDT)
Received-SPF: pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender)
client-ip=82.165.159.131;
Authentication-Results: mx.google.com;
    dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=Aa+12hhv;
    spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender)
    smtp.mailfrom=pamdon901@mail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=mail.com;
    s=dbd5af2cbaf7; t=1598072261;
    bh=gLFuHIYrBelVx5+1mG290ok9iskdbBEUFyXeLGcajv8=;
    h=X-UI-Sender-Class:From:To:Subject:Date;
    b=Aa+12hhvURcNvWvYV/paUqyD4NoUgtPAChFynDjo25h4baivnVP5yajrGQjhVYE79
    frDjSFRmLH1sbVoSpV5leBLzNWC4W6lY8d85xBvcW1jDZaJJJ2AhxwsYRBo7Y/4xi
    SJZYlz0SrvhG3GMBxHxCVmnz/EGUYutXz9pIqf+4=
X-UI-Sender-Class: 214d933f-fd2f-45c7-a636-f5d79ae31a79
Received: from [174.128.225.186] ([174.128.225.186]) by web-mail.mail.com
    (3c-app-mailcom-lxa10.server.lan [10.76.45.11]) (via HTTP); Sat, 22 Aug
    2020 06:57:41 +0200
MIME-Version: 1.0
Message-ID: <trinity-47ac3c7b-9f51-4b7f-91dd-b7e0741a9932-1598072261093@3c-app-mailcom-lxa10>
```

17. The data highlighted in item 1 below provides details about the server that received the email after it was sent from the mail.com server and underwent the SPF and DKIM tests. As seen below, the email is received from mout-xforward.gmx.com by mx.google.com and provides the time.

```
ARC-Authentication-Results: i=1; mx.google.com;
    dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=Aa+12hhv;
    spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender)
smtp.mailfrom=pamdon901@mail.com
Return-Path: <pamdon901@mail.com>
Received: from mout-xforward.gmx.com (mout-xforward.gmx.com. [82.165.159.131])
    by mx.google.com with ESMTPS id a13si5132501jat.122.2020.08.21.21.57.44
    for <jdondon109@gmail.com>
    (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
    Fri, 21 Aug 2020 21:57:44 -0700 (PDT)
Received-SPF: pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender)
client-ip=82.165.159.131;
Authentication-Results: mx.google.com;
    dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=Aa+12hhv;
    spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender)
smtp.mailfrom=pamdon901@mail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=mail.com;
    s=dbd5af2cbaf7; t=1598072261;
    bh=gLFuHIYrBelVx5+1mG290ok9tskdbBEUFyXeLGcajv8=;
    h=X-UI-Sender-Class:From:To:Subject:Date;
    b=Aa+12hhvURcNvWvYV/paUqyD4NoUgtPACHFynDjo25h4baivnVP5yajrGQjhVYE79
    frDjSFRmlH1sbVoSpV5leBLzNWC4W6LY8d85xBvcW1jDZaQJJ2AhxwsYRBo7Y/4xi
    SJZYlzQSryhG3GMBxHxCVmnz/EGUYutXz9pIqf+4=
X-UI-Sender-Class: 214d933f-fd2f-45c7-a636-f5d79ae31a79
Received: from [174.128.225.186] ([174.128.225.186]) by web-mail.mail.com
    (3c-app-mailcom-lxa10.server.lan [10.76.45.11]) (via HTTP); Sat, 22 Aug
    2020 06:57:41 +0200
MIME-Version: 1.0
Message-ID: <trinity-47ac3c7b-9f51-4b7f-91dd-b7e0741a9932-1598072261093@3c-app-mailcom-lxa10>
```

18. Let us scroll right to the top now to look at the last set of metadata in the email header. The data highlighted in item 1 below is known as the Authenticated Received Chain (ARC) and is similar to DKIM and SPF. As before, it can tell whether the email passed the authenticity tests. The data in item 2 is the next server that received the email, and item 3 provides data about the final server that delivered the message to the recipient's inbox and the time of delivery.

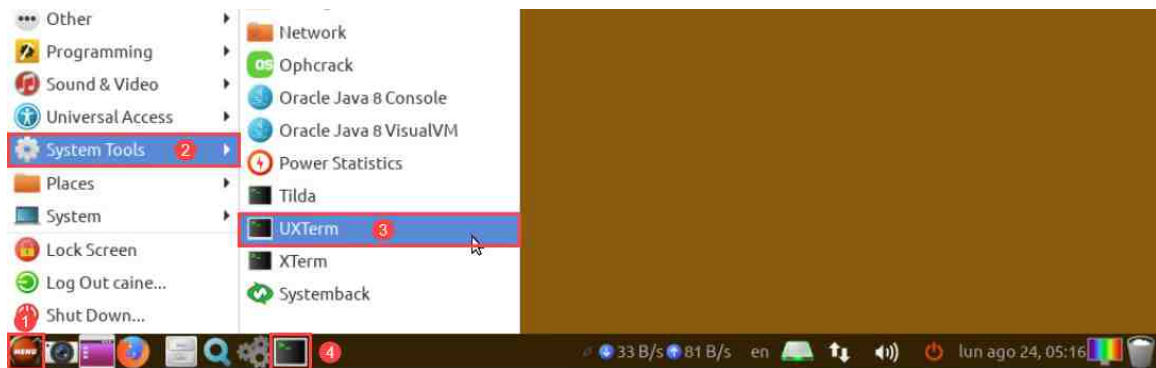
```
Delivered-To: jdondon109@gmail.com
Received: by 2002:ab3:5191:0:0:0:0:0 with SMTP id x17csp789145ltg; ③
    Fri, 21 Aug 2020 21:57:45 -0700 (PDT)
X-Goog-Smtp-Source: ABdhPJz+OuGALLMYBrv15XqQJua03Eu5FJxMKCyTXP6B2q9K/SLCBwoK9CM8hFIP26mmn2GH0ItK
X-Received: by 2002:a92:a157:: with SMTP id v84mr4882943ili.189.1598072264798; ②
    Fri, 21 Aug 2020 21:57:44 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1598072264; cv=none;
    d=google.com; s=arc-20160816;|
    b=RppuTQQBQFD2XtShyJYCtN/LixkYdomBzBMPJmNTwwG7qEyRIMBrMEWhKd3Xcj6sF
    kvf+ZRHV21LSysy0XJnAngcbNICRP1zzRCr2BGbwEjH91Yp6x3N8PuaHxGPySnAd7dXb
    hqgNl9NhUE/fyx86jW+8lBkEEBo1I8w2CsEajCUTftITBxRvpfNZSX6AQh9tPy15+zFS
    9fiuYFjMMs/jxIzCJBgVtrgRzdqlA18j6i9cKfXCknbyYhBqDtZPnzcSR4R5NnBWFRF
    E0ZzoLbwqiL5sV6SuezkLPAmJL8KN5aldahiwJE00bv81UJqQJhXitZs4+ipJxTYiZPm
    Md0g==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
    h=sensitivity:importance:date:subject:to:from:message-id:mime-version
    :dkim-signature;
    bh=gLFuHIYrBelVx5+1mG290ok9iskdbBEUFyXeLGcajv8=;
    b=rotL6pZDVEKeIr9KFU5cy/zI6tPpSMaLF8hyjQys+VWYF1I7WpVndwPT05b+HST4gb
    MAE1aV5dXTfYz07DH0N54B9kpME0xZckWGCnl6Dyc6bvJMqm0872HhmISR4e4KxQQK0T
    gPynZa833qTQBewRlqbhzVo1EidItp7BAUdx1YgUZYVkjADFPgoWTPcrW2JLrjIdTvHv
    /HVEBs6k1sVkqXeGpQSW/XTJxBtp19VhiBgCG2aND0HXF0HQDZBQnLUQNW/TYfk40STk
    P07A1yiG6Cg0NnZ0imJKDL12xr8zeXAKz1Fg1k2MwSgWF21iEv4VJ4rVdVPZqjKjHeEB
    ozvA==
ARC-Authentication-Results: i=1; mx.google.com;
    dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=Aa+12hhv;
    spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender)
smtp.mailfrom=pamdon901@mail.com
Return-Path: <pamdon901@mail.com>
Received: from mout-xforward.qmx.com (mout-xforward.qmx.com. [82.165.159.131])
```

19. As you saw in this exercise, the email header can contain a wealth of information and can assist in different kinds of ways. Headers can be used to determine the authenticity of an email and to trace an email back to its source. This is an exercise that is practiced by forensic examiners on a regular basis, and so you should become familiar with it if you plan to grow in the field.
20. Reading the header was not that hard, but it can be made much easier. In the next exercise, we will export the next email header and review it in a tool called Email Header Analyzer.

2 Parsing Email Headers with Email Header Analyzer

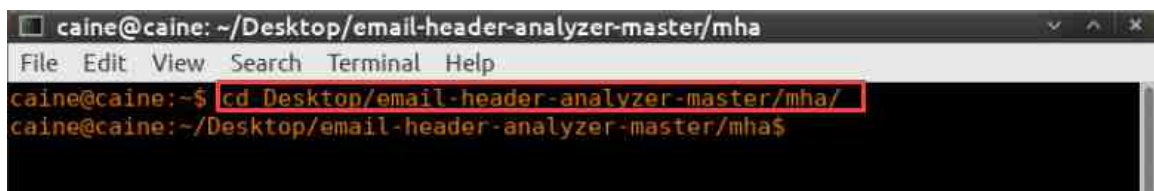
In the previous exercise, we manually went through the email header to learn about the different metadata stored within it. Because it can sometimes be overwhelming, specific tools were designed to help specialists review the data and go directly to the information they need. One such tool is Email Header Analyzer; it is an open-source offline email header parser. In this exercise, we will show you how to review email data with Email Header Analyzer.

1. Let us begin by starting the tool. The tool is run in the web browser, and so, a server needs to be run to allow the browser to access its options. To do this, open the command prompt by navigating to Application Menu > System Tools > UXTerm as seen in items 1, 2, and 3 below. Alternatively, you can open it by clicking the icon from the taskbar, as seen in item 4 below.



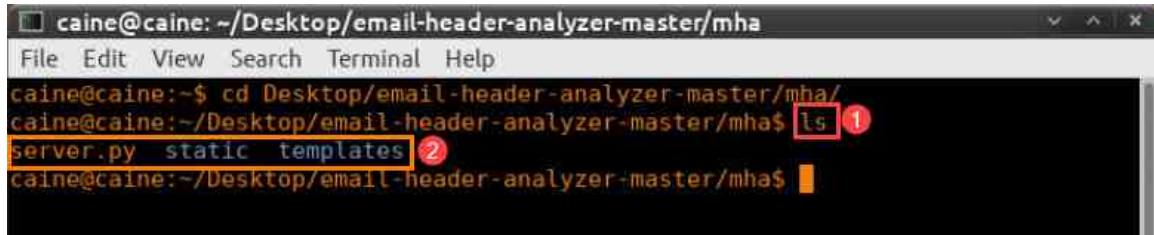
2. Once the terminal window opens, type the following command and press Enter to navigate to the folder that contains the application.

```
cd Desktop/email-header-analyzer-master/mha/
```



- Now let us do a quick file list to check what files are in this folder. Do this by typing the following command and pressing Enter, as seen in item 1. The files will appear as seen in item 2. The one that will start the server is the file called server.py.

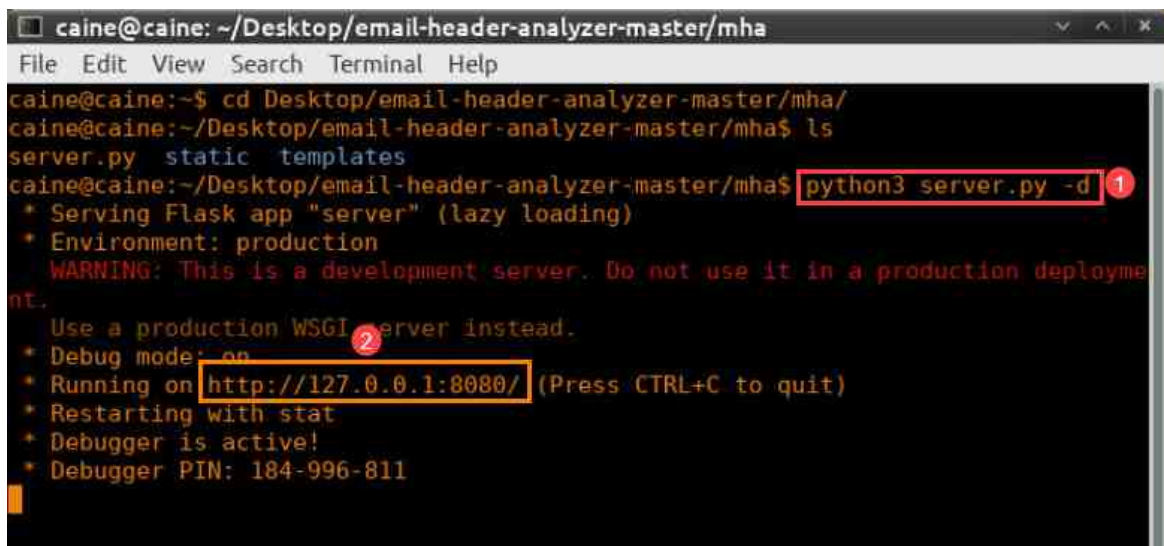
```
ls
```



A terminal window titled 'caine@caine: ~/Desktop/email-header-analyzer-master/mha'. The prompt is 'caine@caine:~\$'. The user enters 'cd Desktop/email-header-analyzer-master/mha/' and then 'ls'. The output shows 'server.py static templates'. Red annotations include a circled '1' next to the 'ls' command and a circled '2' next to the output files.

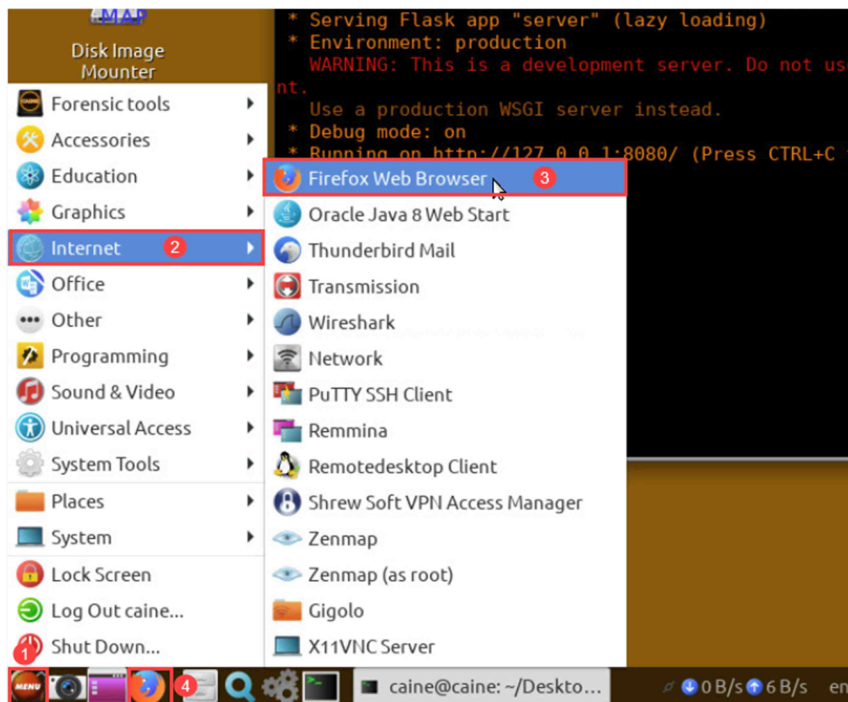
- Let us start the server by typing the following command and pressing Enter, as seen in item 1. This will begin the server and allow us to access the application using the web browser. The URL seen in item 2 below will provide access to the Email Header Analyzer program in the web browser.

```
python3 server.py -d
```

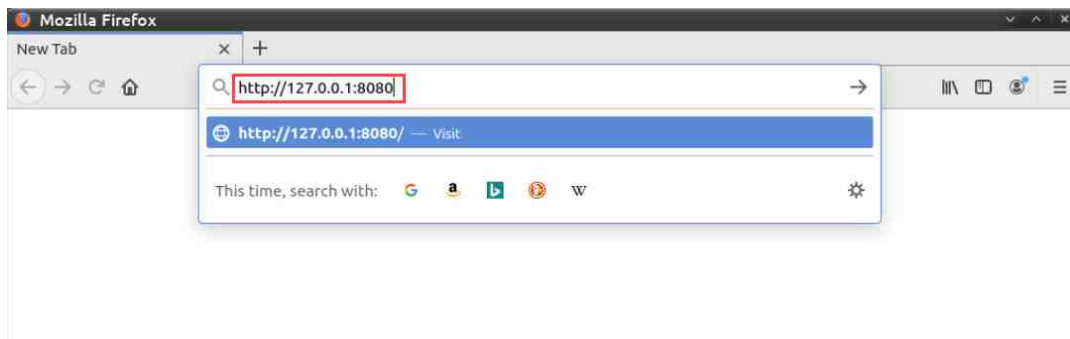


A terminal window titled 'caine@caine: ~/Desktop/email-header-analyzer-master/mha'. The prompt is 'caine@caine:~\$'. The user enters 'cd Desktop/email-header-analyzer-master/mha/' and then 'ls', which outputs 'server.py static templates'. Then the user enters 'python3 server.py -d'. The output shows: '* Serving Flask app "server" (lazy loading)', '* Environment: production', 'WARNING: This is a development server. Do not use it in a production deployment.', 'Use a production WSGI server instead.', '* Debug mode: on', '* Running on http://127.0.0.1:8080/ (Press CTRL+C to quit)', '* Restarting with stat', '* Debugger is active!', '* Debugger PIN: 184-996-811'. Red annotations include a circled '1' next to the command and a circled '2' next to the 'Running on' line.

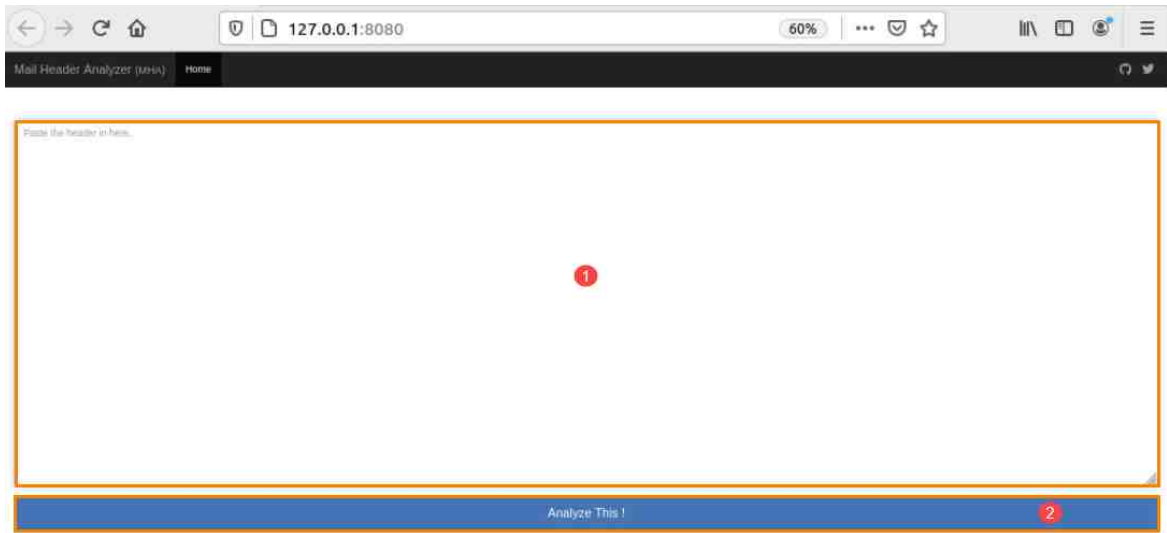
- Now that we have the server running, let us open a web browser. To do this, click the Application Menu > Internet > Firefox Web Browser as seen in items 1, 2, and 3 below. Alternatively, you can click the Firefox icon from the taskbar, as seen in item 4 below.



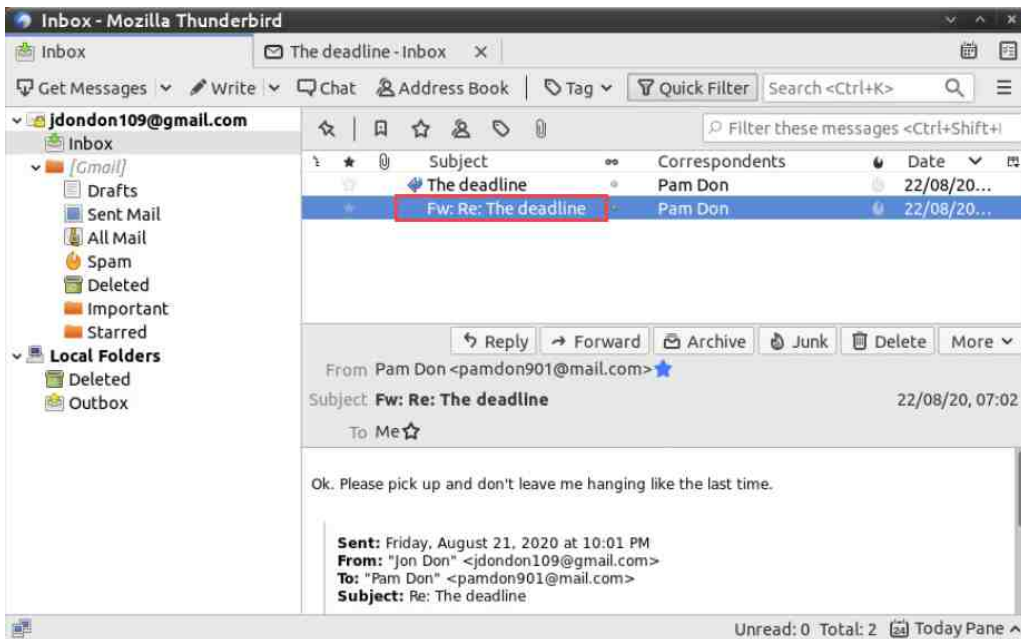
- Now that the web browser is open, type the URL `http://127.0.0.1:8080` in the address bar of the web browser, as highlighted below, and press Enter. This will take us to the Email Header Analyzer interface.



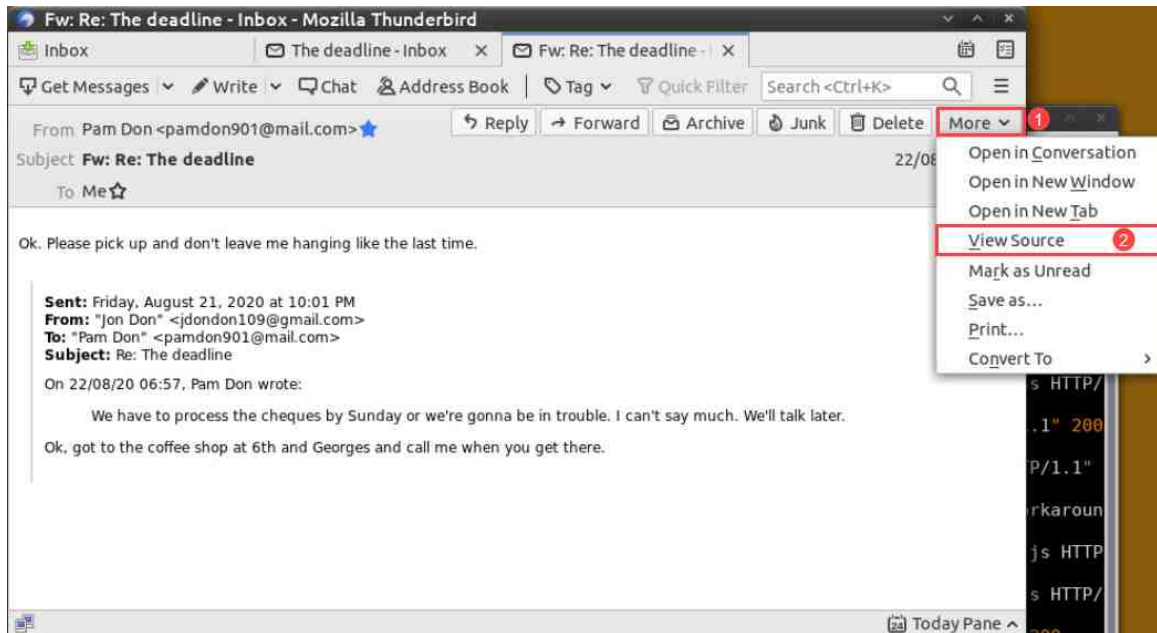
- You will now see the main GUI for Email Header Analyzer. It is very simple: paste the entire email header into the area highlighted as item 1 and then click the Analyze This! Button, as seen in item 2.



- Now that we have got the tool up and running, let us test it out by analyzing the header of the other email that was in the Thunderbird inbox. Let us minimize the Firefox web browser for now. If Thunderbird was closed, reopen it, and double-click the email called Fw: Re: The deadline to open it in a new tab, as seen below.



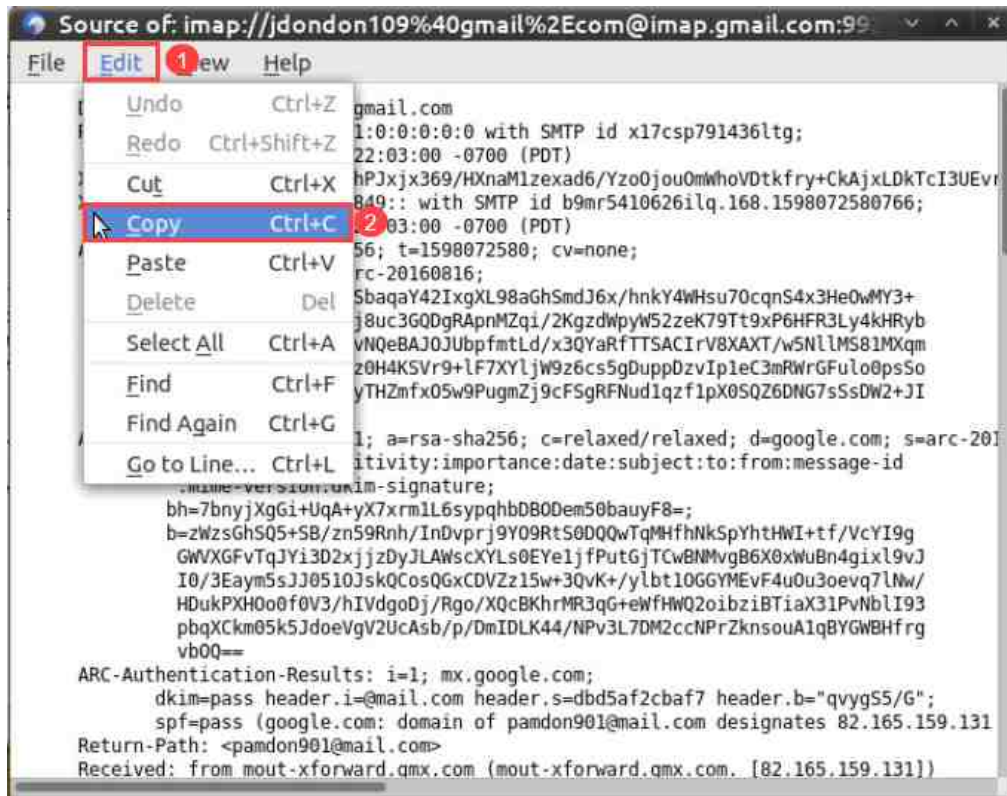
9. As we did before, view the email header by navigating to More > View Source, as seen in items 1 and 2 below.



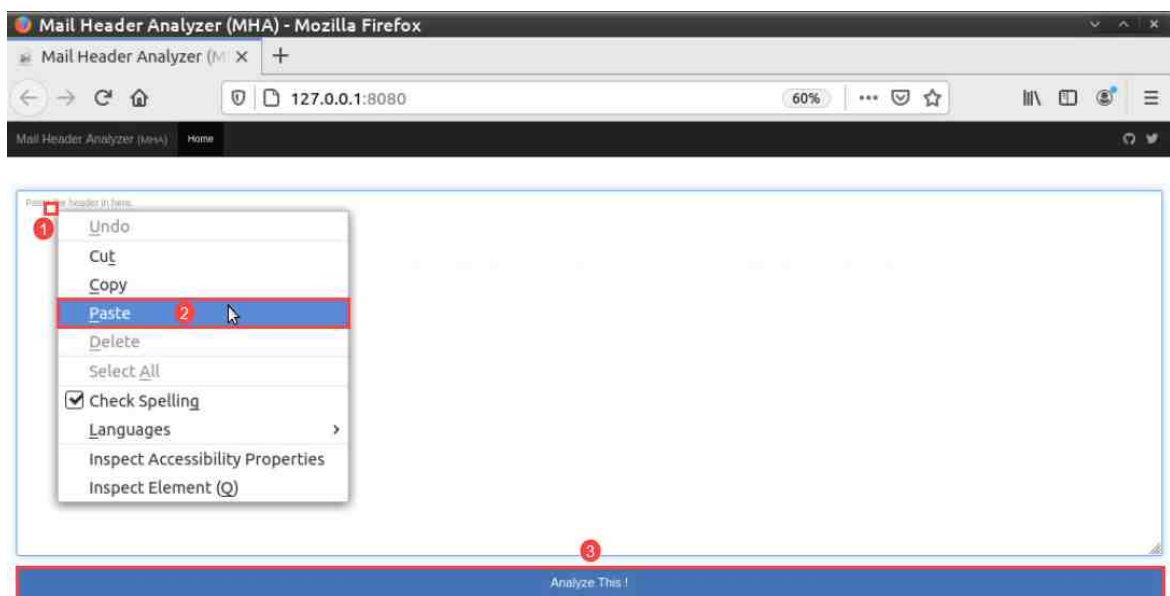
10. In the View Source window, highlight the email header by navigating to Edit > Select All, as seen in items 1 and 2 below. Alternatively, you can use Ctrl+A.



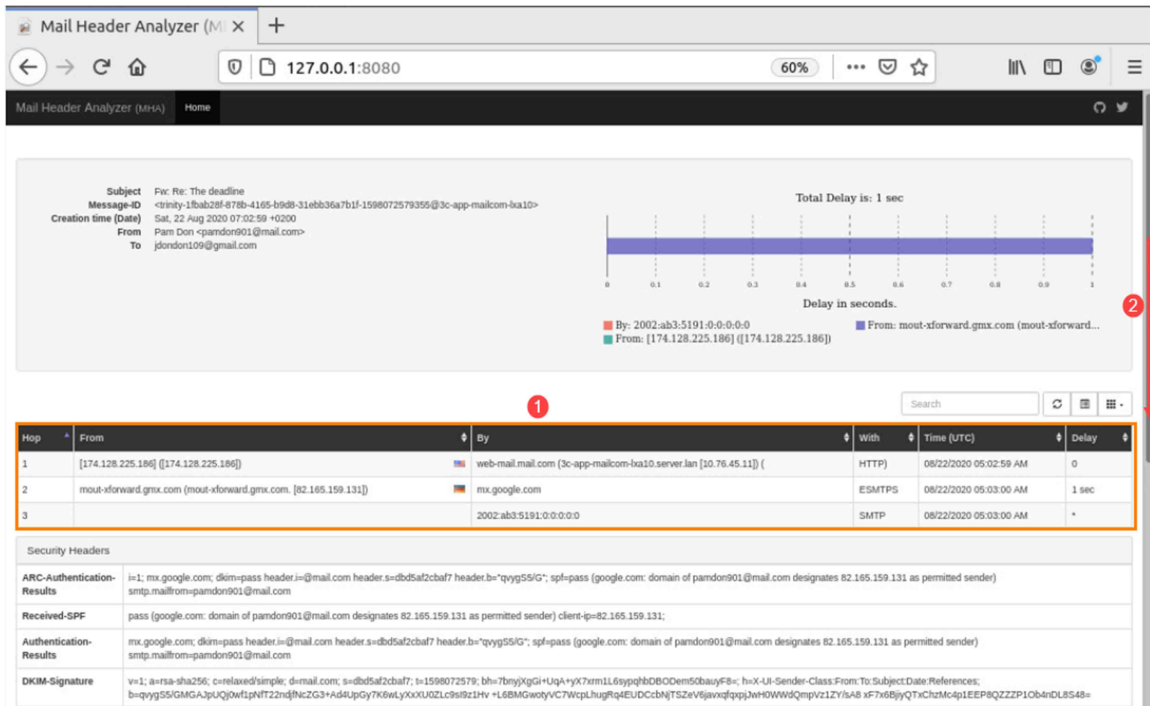
11. Now, copy the data by navigating to Edit > Copy as seen in items 1 and 2 below. Alternatively, you can use Ctrl+C.



12. Now that the data is copied, let us paste it in Email Header Analyzer. Do this by maximizing the Firefox web browser. In the text box, right-click and click Paste, as seen in items 1 and 2 below. Once the content is pasted, click the Analyze This! button, shown in item 3 below.

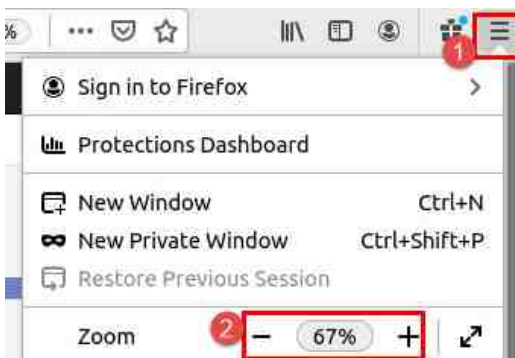


13. As seen in the screenshot below, the header is parsed, and a lot of useful information will be displayed. The email servers and IP addresses are provided at the top of the table, seen in item 1 below. You can drag the scroll bar down, as shown in item 2, or use the mouse wheel, to scroll through the other fields. The fields will be the same, except for the In-reply-To or References fields, which only appear when the email is a reply or forward.



This tool is ideal because it is completely offline. Many email parsers exist but most of them are found online. Due to privacy issues, examiners may not want to use these services. This option makes it

14. If you are unable to see the full view of Mail Header Analyzer, feel free to zoom in or out as need. You can achieve this by clicking the Open Menu icon to the right of Mozilla Firefox and select the + or - button from the option Zoom, as seen in items 1 and 2 below.



15. As you saw in this exercise, the email header can be parsed quickly and easily using Email Header Analyzer.
16. In this lab, we learned how to extract and interpret the header information that can be found in electronic mail. Equipped with this information, an examiner can thoroughly investigate email communication and provide valuable findings.
17. You are at the end of the lab. Close all the programs by clicking the X at the top-right corner of the windows, as seen below.

