FORENSICS V2 LAB SERIES

Lab 12: Email Analysis

Document Version: 2022-11-04

Contents

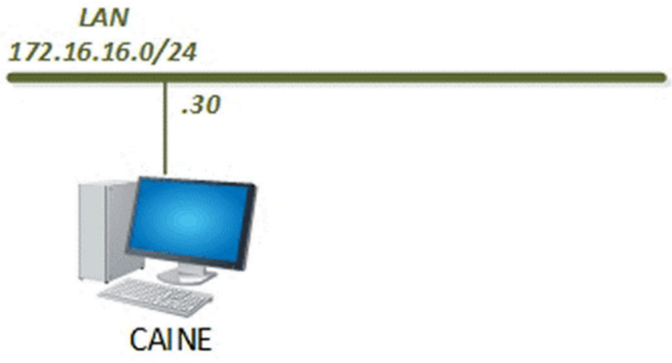
Introduction

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

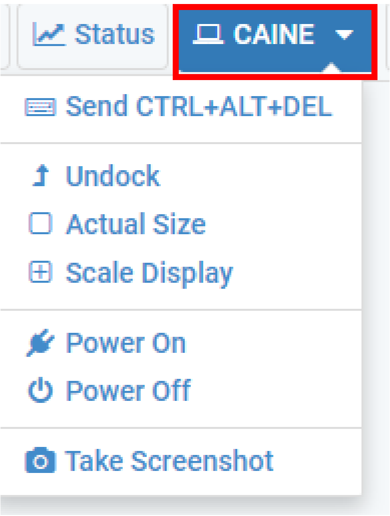
As a forensic examiner, the 2 main types of email files you encounter will be web-based email and email client database files. The webmail email is stored on the email company's mail server, and the user can access these emails using a web browser. This means that when the webpage is closed, the emails 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.

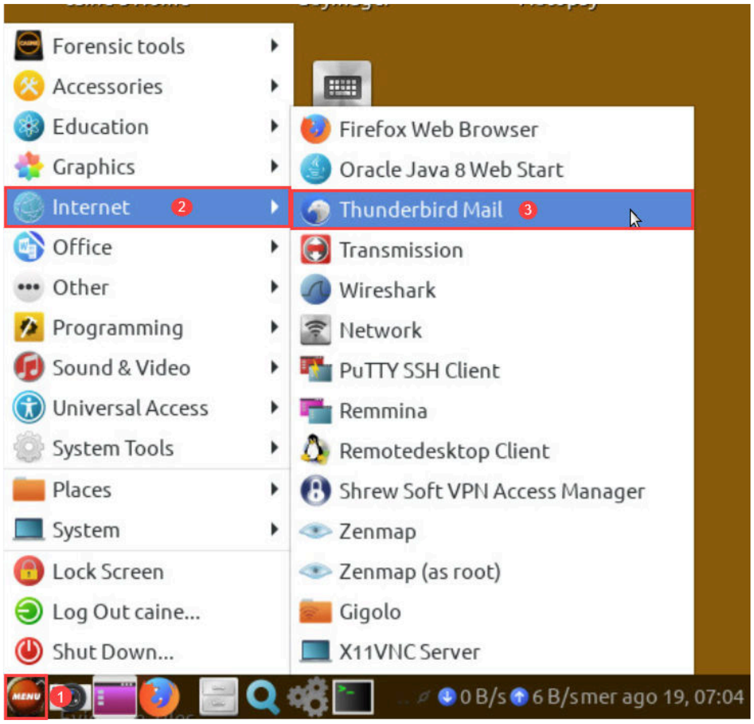
Please note that email investigations can be performed live, while systems are running. It is always recommended, however, to make a forensic copy of the drive or email file(s) before performing examinations. There are some situations where it is ok to access and review the headers for collection, such 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: `Train1ng$`

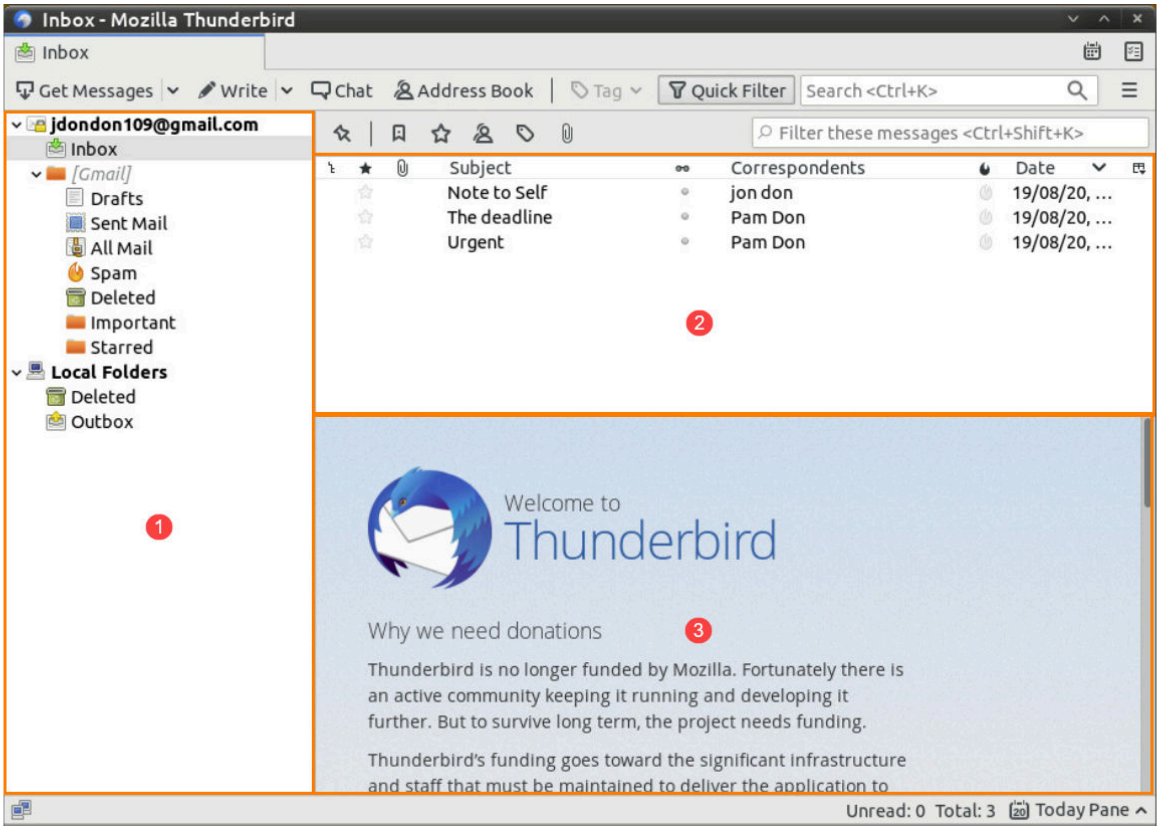


2. Once you are logged into the VM, launch the *Thunderbird Mail* program from the application menu by navigating to **Application Menu > Internet > Thunderbird Mail**, as seen in *items* **1, 2,** and **3** below**.**



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.**



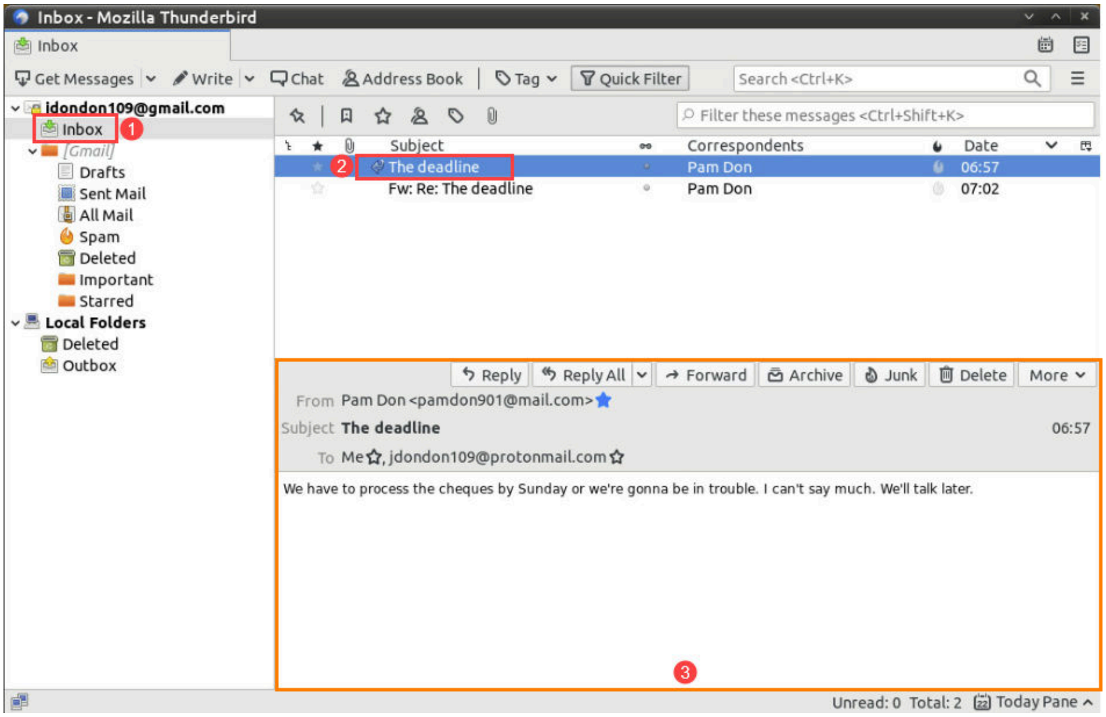
Subject	Correspondents	Date
Note to Self	jon don	19/08/20, ...
The deadline	Pam Don	19/08/20, ...
Urgent	Pam Don	19/08/20, ...

Why we need donations

Thunderbird is no longer funded by Mozilla. Fortunately there is an active community keeping it running and developing it further. But to survive long term, the project needs funding.

Thunderbird's funding goes toward the significant infrastructure and staff that must be maintained to deliver the application to

4. 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.

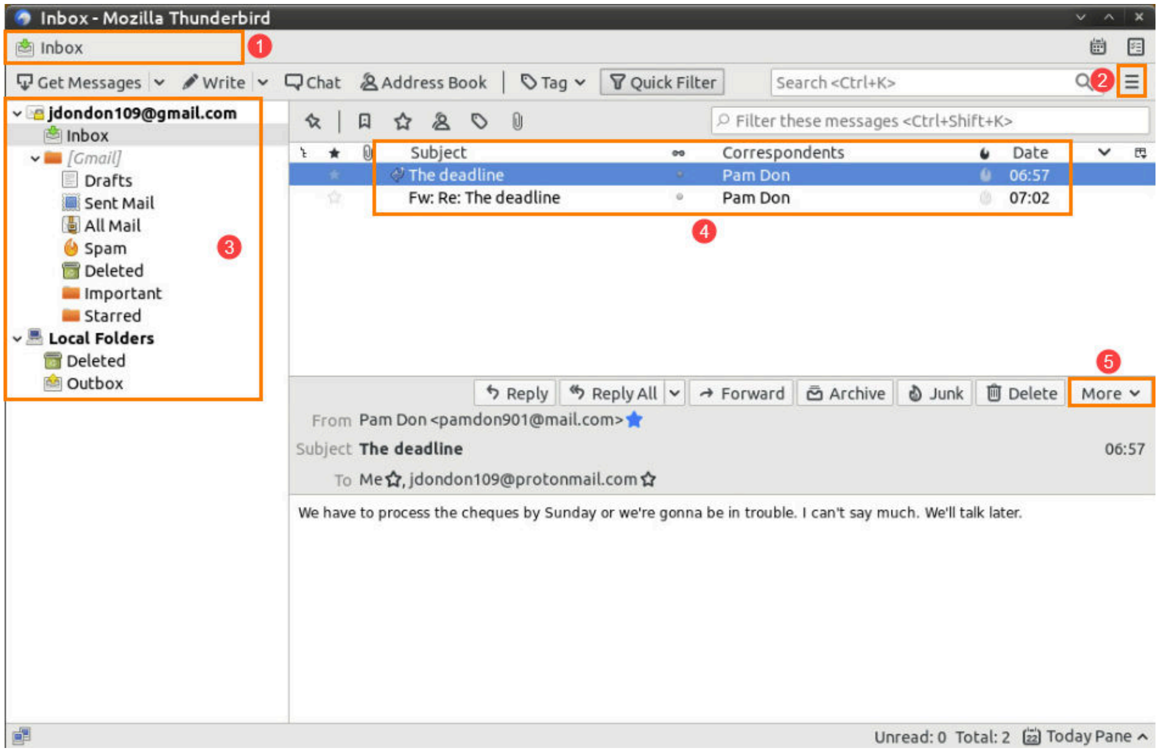


Subject	Correspondents	Date
The deadline	Pam Don	06:57
Fw: Re: The deadline	Pam Don	07:02

From Pam Don <pamdon901@mail.com>
Subject **The deadline** 06:57
To Me, jdondon109@protonmail.com

We have to process the cheques by Sunday or we're gonna be in trouble. I can't say much. We'll talk later.

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.**



Subject	Correspondents	Date
The deadline	Pam Don	06:57
Fw: Re: The deadline	Pam Don	07:02

From Pam Don <pamdon901@mail.com>

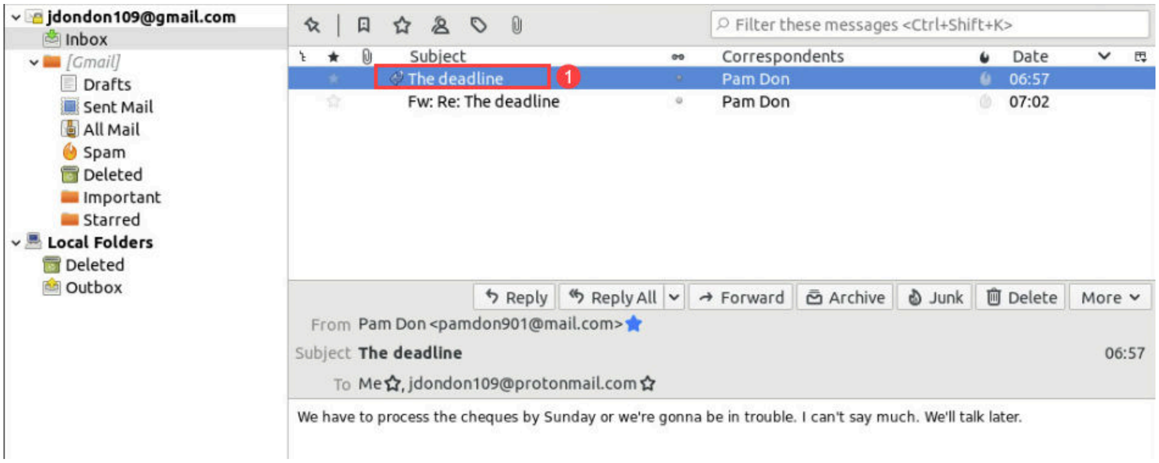
Subject **The deadline** 06:57

To Me, jdondon109@protonmail.com

We have to process the cheques by Sunday or we're gonna be in trouble. I can't say much. We'll talk later.

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.

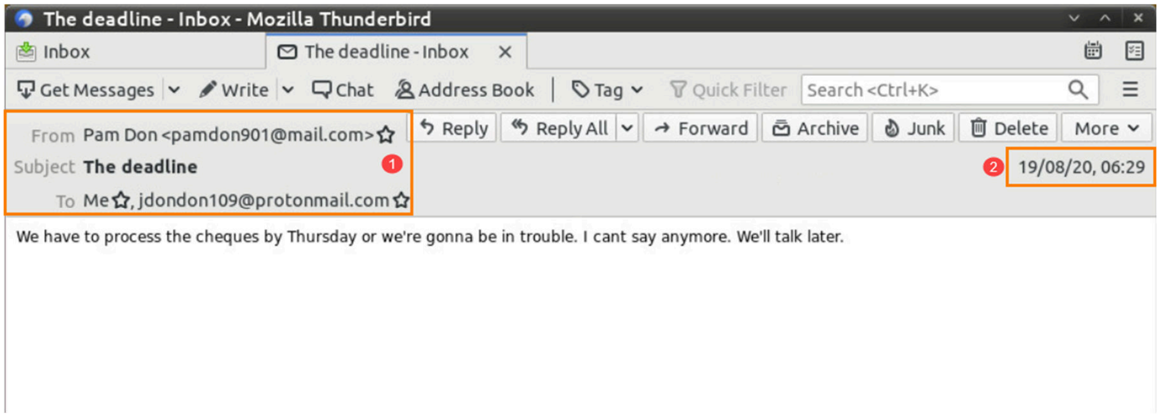


Subject	Correspondents	Date
The deadline	Pam Don	06:57
Fw: Re: The deadline	Pam Don	07:02

From Pam Don <pamdon901@mail.com>
Subject **The deadline** 06:57
To Me, jdondon109@protonmail.com

We have to process the cheques by Sunday or we're gonna be in trouble. I can't say much. We'll talk later.

7. 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.

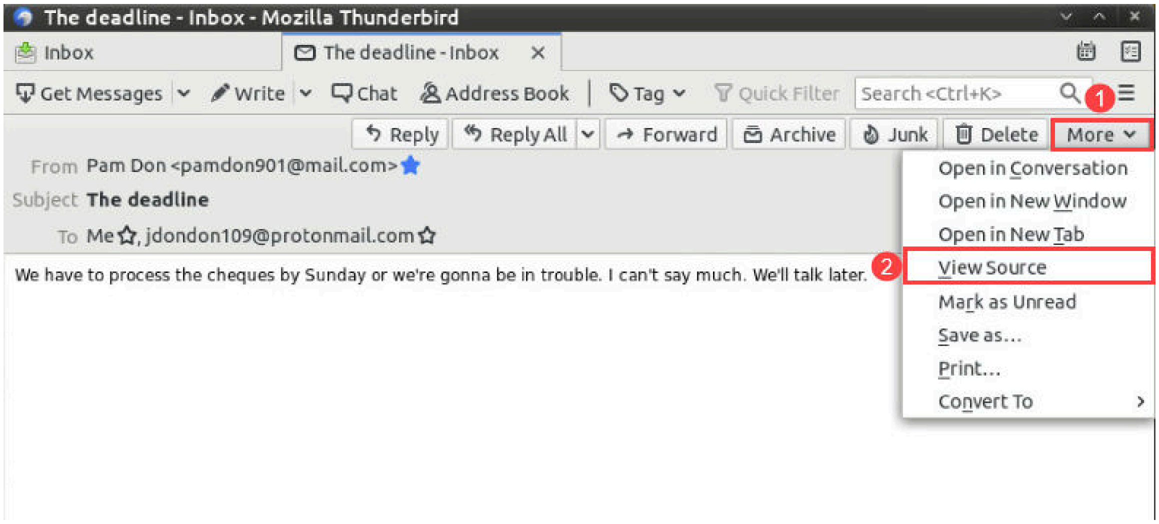


From Pam Don <pamdon901@mail.com>
Subject **The deadline**
To Me, jdondon109@protonmail.com

19/08/20, 06:29

We have to process the cheques by Thursday or we're gonna be in trouble. I cant say anymore. We'll talk later.

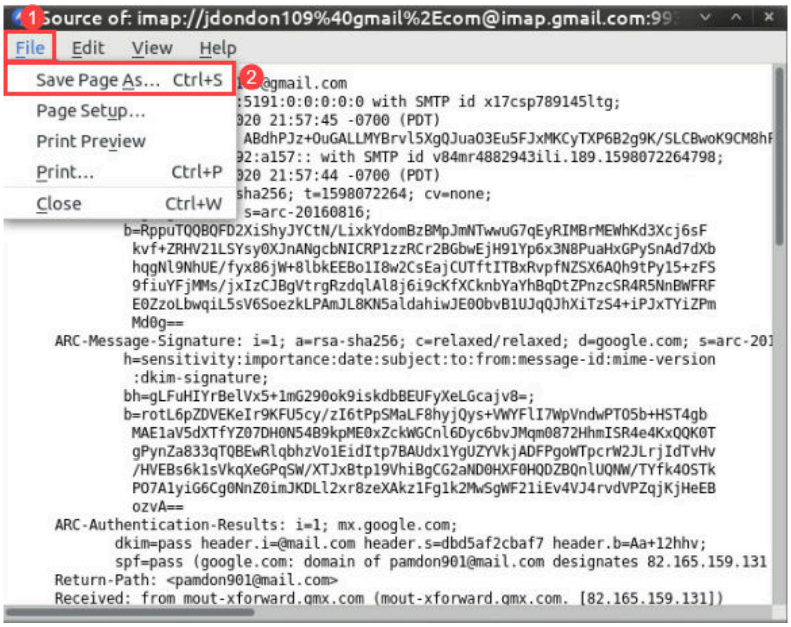
8. Let us capture the email header for this email and save it so that we can review it later. Begin by clicking **More > View Source** as seen in *items* **1** and **2** below.



From Pam Don <pamdon901@mail.com>
Subject **The deadline**
To Me, jdondon109@protonmail.com

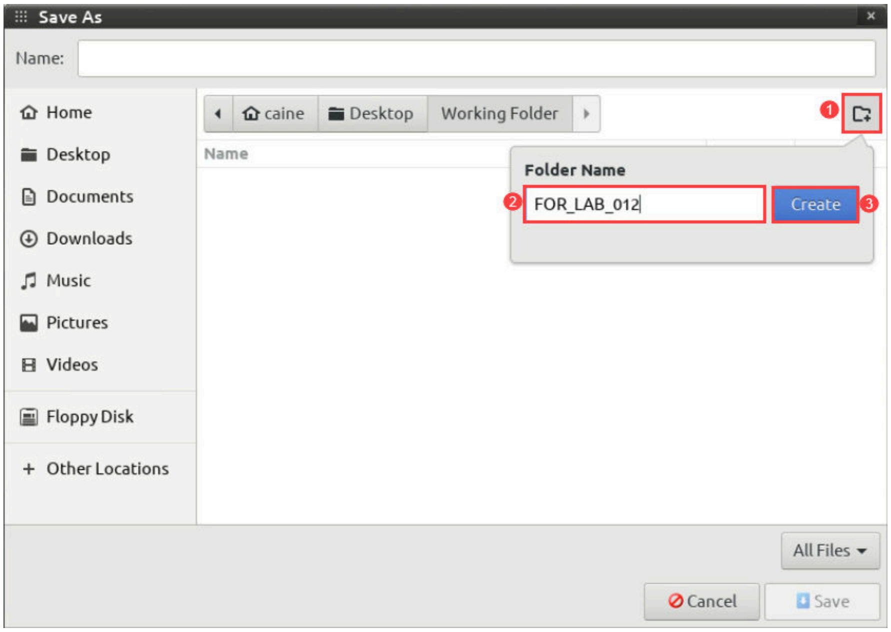
We have to process the cheques by Sunday or we're gonna be in trouble. I can't say much. We'll talk later.

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.



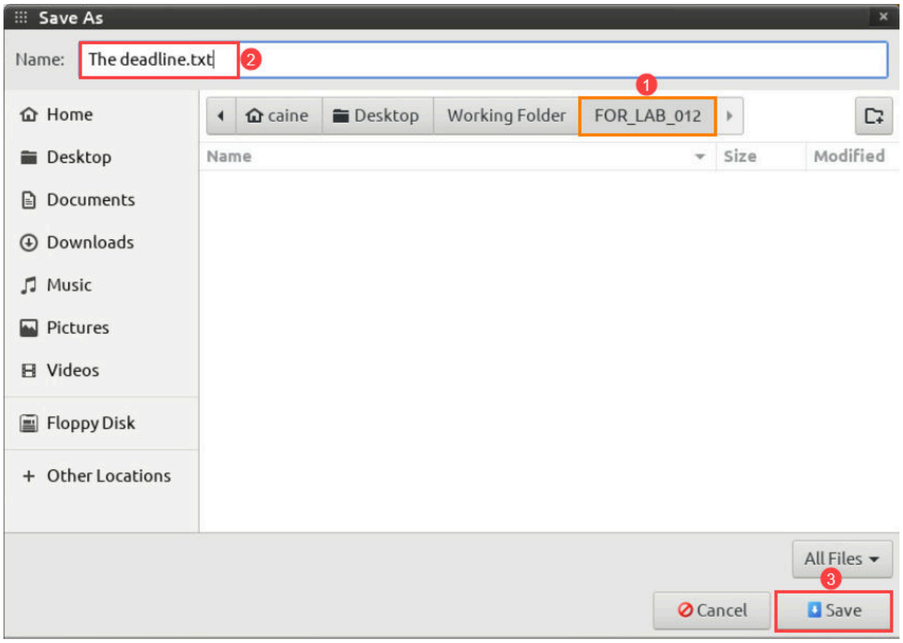
```
@gmail.com
:5191:0:0:0:0:0 with SMTP id x17csp789145ltg;
020 21:57:45 -0700 (PDT)
 ABdhPJz+OuGALLMYBrvl5XgQJua03Eu5FJxMKCyTXP6B2g9K/SLCBwoK9CM8hF
92:a157:: with SMTP id v84mr4882943ili.189.1598072264798;
020 21:57:44 -0700 (PDT)
sha256; t=1598072264; cv=none;
 s=arc-20160816;
        b=RppuTQQBQFD2XiShyJYCtN/LixkYdomBzBMpJmNTwwuG7qEyRIMBrMEWhKd3Xcj6sF
         kvf+ZRHV21LSYsy0XJnANgcbNICRP1zzRCr2BGbwEjH91Yp6x3N8PuaHxGPySnAd7dXb
         hqgNl9NhUE/fyx86jW+8lbkEEBo1I8w2CsEajCUTftITBxRvpfNZSX6AQh9tPy15+zFS
         9fiuYFjMMs/jxIzCJBgVtrgRzdqlAl8j6i9cKfXCknbYaYhBqDtZPnzcSR4R5NnBWFRF
         E0ZzoLbwqiL5sV6SoezkLPAmJL8KN5aldahiwJE0ObvB1UJqQJhXiTzS4+iPJxTYiZPm
         Md0g==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-201
        h=sensitivity:importance:date:subject:to:from:message-id:mime-version
         :dkim-signature;
        bh=gLFuHIYrBelVx5+1mG290ok9iskdbBEUFyXeLGcajv8=;
        b=rotL6pZDVEKeIr9KFU5cy/zI6tPpSMaLF8hyjQys+VWYFlI7WpVndwPTO5b+HST4gb
         MAE1aV5dXTfYZ07DH0N54B9kpME0xZckWGCnl6Dyc6bvJMqm0872HhmISR4e4KxQQK0T
         gPynZa833qTQBEwRlqbhzVo1EidItp7BAUdx1YgUZYVkjADFPgoWTpcrW2JLrjIdTvHv
         /HVEBs6k1sVkqXeGPqSW/XTJxBtp19VhiBgCG2aND0HXF0HQDZBQnlUQNW/TYfk4OSTk
         PO7A1yiG6Cg0NnZ0imJKDLl2xr8zeXAkz1Fg1k2MwSgWF21iEv4VJ4rvdVPZqjKjHeEB
         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
Return-Path: <pamdon901@mail.com>
Received: from mout-xforward.gmx.com (mout-xforward.gmx.com. [82.165.159.131])
```

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.



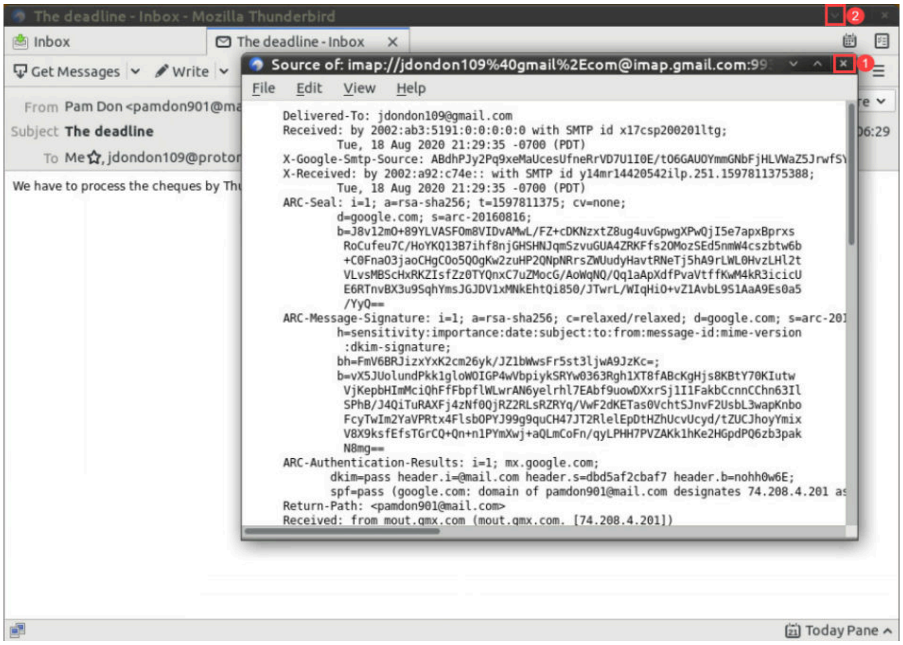
Folder Name: FOR_LAB_012

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.



Name: The deadline.txt

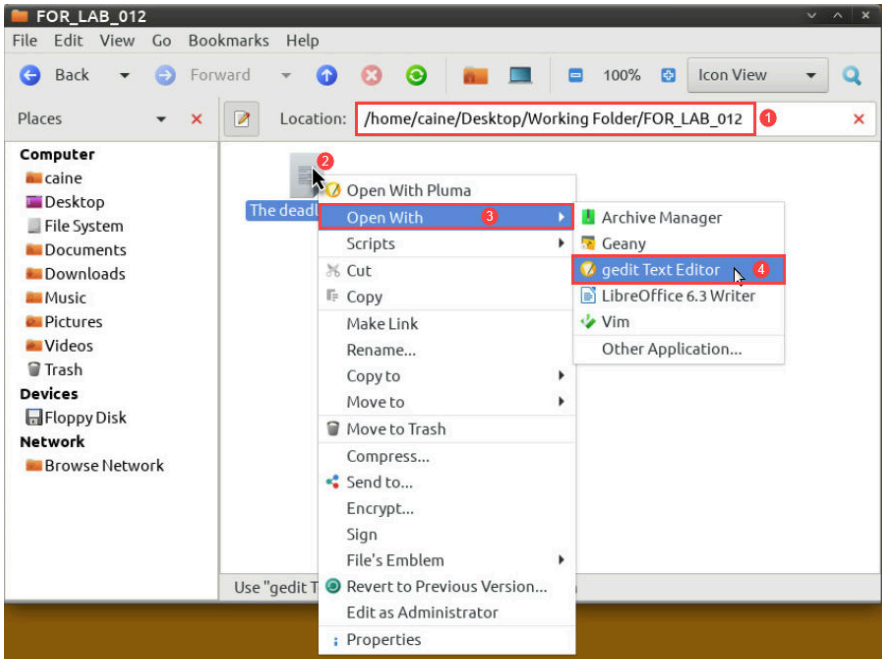
12. Now that the file is saved, let us close the *Source* window, minimize *Thunderbird,* and browse to the folder that we just created. Close the *Source* window by clicking the **X**, as seen in *item* **1** below. Next, minimize *Thunderbird* by clicking the **Minimize** button, as seen in *item*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


The deadline - Inbox - Mozilla Thunderbird
Inbox
The deadline - Inbox
Get Messages
Write
Source of: imap://jdondon109%40gmail%2Ecom@imap.gmail.com:99
File
Edit
View
Help
Today Pane
1
2

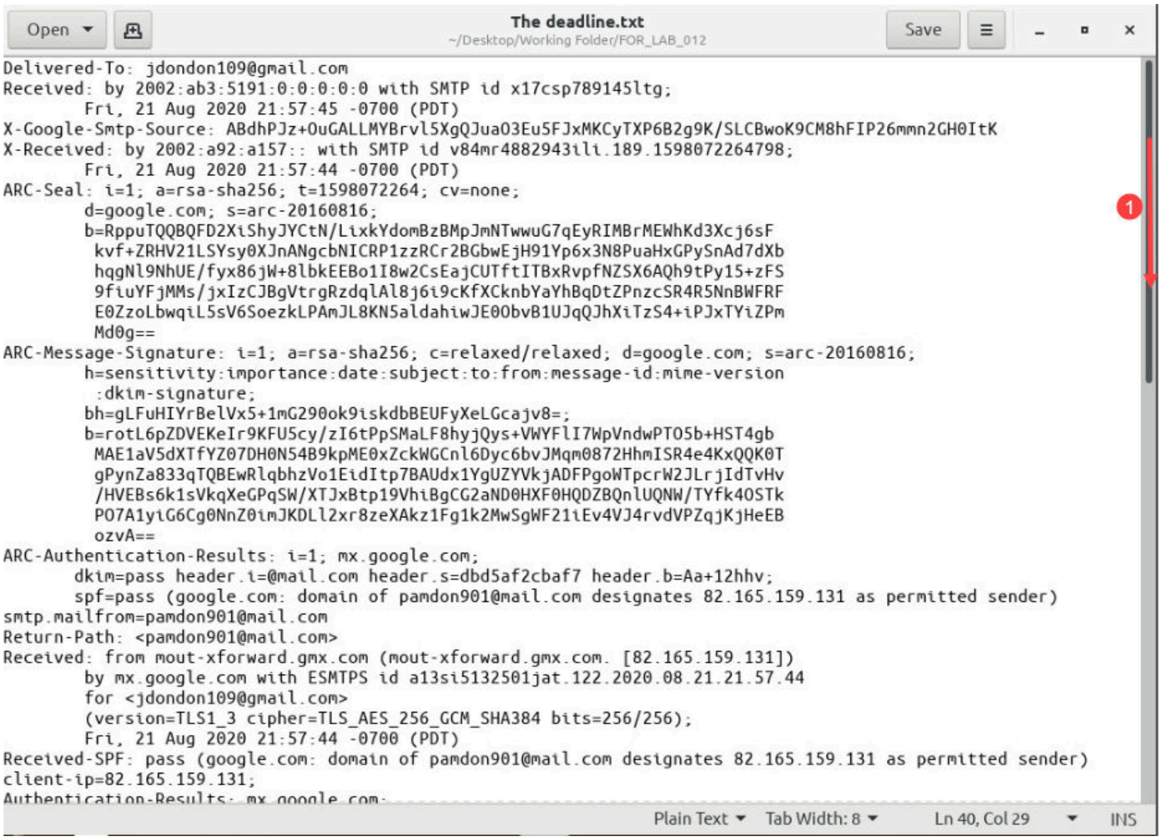
From Pam Don <pamdon901@ma
Subject The deadline
To Me, jdondon109@proton
We have to process the cheques by Th

```
Delivered-To: jdondon109@gmail.com
Received: by 2002:ab3:5191:0:0:0:0:0 with SMTP id x17csp200201ltg;
        Tue, 18 Aug 2020 21:29:35 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJy2Pq9xeMaUcesUfneRrVD7U1I0E/tO6GAUOYmmGNbFjHLVWaZ5JrwfSY
X-Received: by 2002:a92:c74e:: with SMTP id y14mr14420542ilp.251.1597811375388;
        Tue, 18 Aug 2020 21:29:35 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1597811375; cv=none;
        d=google.com; s=arc-20160816;
        b=J8v12mO+89YLVASFOm8VIDvAMwL/FZ+cDKNzxtZ8ug4uvGpwgXPwQjI5e7apxBprxs
         RoCufeu7C/HoYKQ13B7ihf8njGHSHNJqmSzvuGUA4ZRKFfs2OMozSEd5nmW4cszbtw6b
         +C0FnaO3jaoCHgCOo5QOgKw2zuHP2QNpNRrsZWUudyHavtRNeTj5hA9rLWL0HvzLHl2t
         VLvsMBScHxRKZIsfZz0TYQnxC7uZMocG/AoWqNQ/QqlaApXdfPvaVtffKwM4kR3icicU
         E6RTnvBX3u9SqhYmsJGJDV1xMNkEhtQi850/JTwrL/WIqHiO+vZ1AvbL9S1AaA9Es0a5
         /YyQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-201
        h=sensitivity:importance:date:subject:to:from:message-id:mime-version
         :dkim-signature;
        bh=FmV6BRJizxYxK2cm26yk/JZ1bWwsFr5st3ljwA9JzKc=;
        b=vX5JUolundPkk1gloWOIGP4wVbpiykSRYw0363Rgh1XT8fABcKgHjs8KBtY70KIutw
         VjKepbHImMciQhFfFbpflWLwrAN6yelrhl7EAbf9uowDXxrSj1I1FakbCcnnCChn63Il
         SPhB/J4QiTuRAXFj4zNf0QjRZ2RLsRZRYq/VwF2dKETas0VchtSJnvF2UsbL3wapKnbo
         FcyTwIm2YaVPRtx4FlsbOPYJ99g9quCH47JT2RlelEpDtHZhUcvUcyd/tZUCJhoyYmix
         V8X9ksfEfsTGrCQ+Qn+n1PYmXwj+aQLmCoFn/qyLPHH7PVZAKk1hKe2HGpdPQ6zb3pak
         N8mg==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=nohh0w6E;
       spf=pass (google.com: domain of pamdon901@mail.com designates 74.208.4.201 as
Return-Path: <pamdon901@mail.com>
Received: from mout.gmx.com (mout.gmx.com. [74.208.4.201])
```

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*.



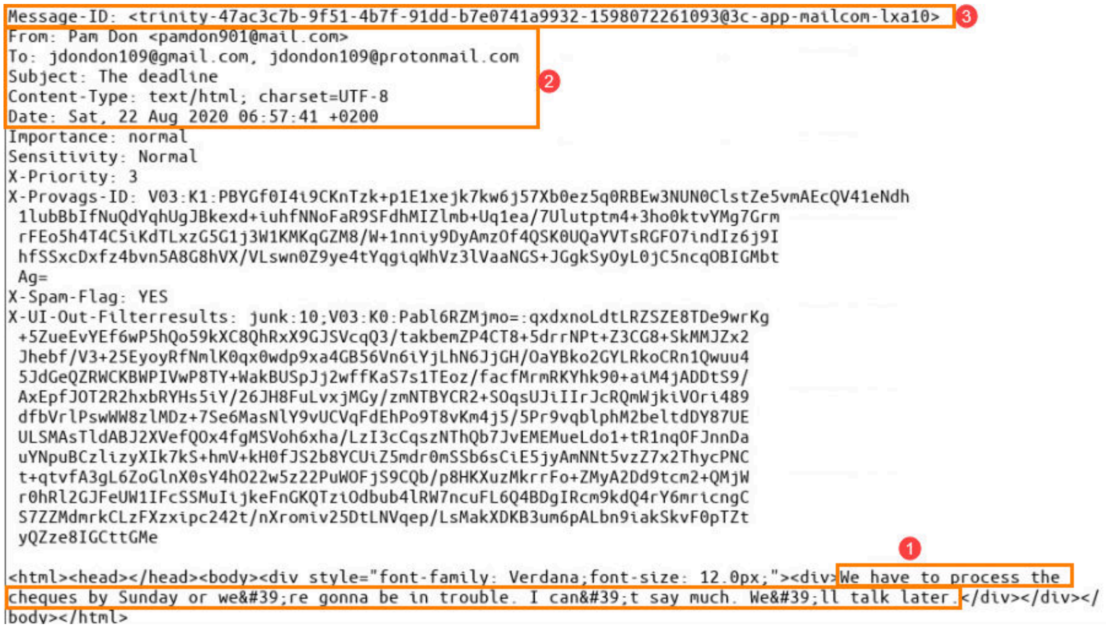
14. Once the file is open, we can begin reading through the data. When reading email headers, it is always advised to start from the bottom. This is mainly because the email passes through different servers during transmission, and each one adds data to the top of the header. This means the sequence 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.



```
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+OuGALLMYBrvl5XgQJuaO3Eu5FJxMKCyTXP6B2g9K/SLCBwoK9CM8hFIP26mmn2GH0ItK
X-Received: by 2002:a92:a157:: with SMTP id v84mr4882943ili.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=RppuTQQBQFD2XiShyJYCtN/LixkYdomBzBMpJmNTwwuG7qEyRIMBrMEWhKd3Xcj6sF
         kvf+ZRHV21LSYsy0XJnANgcbNICRP1zzRCr2BGbwEjH91Yp6x3N8PuaHxGPySnAd7dXb
         hqgNl9NhUE/fyx86jW+8lbkEEBo1I8w2CsEajCUTftITBxRvpfNZSX6AQh9tPy15+zFS
         9fiuYFjMMs/jxIzCJBgVtrgRzdqlAl8j6i9cKfXCknbYaYhBqDtZPnzcSR4R5NnBWFRF
         E0ZzoLbwqiL5sV6SoezkLPAmJL8KN5aldahiwJE0ObvB1UJqQJhXiTzS4+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+VWYFlI7WpVndwPTO5b+HST4gb
         MAE1aV5dXTfYZ07DH0N54B9kpME0xZckWGCnl6Dyc6bvJMqm0872HhmISR4e4KxQQK0T
         gPynZa833qTQBEwRlqbhzVo1EidItp7BAUdx1YgUZYVkjADFPgoWTpcrW2JLrjIdTvHv
         /HVEBs6k1sVkqXeGPqSW/XTJxBtp19VhiBgCG2aND0HXF0HQDZBQnlUQNW/TYfk4OSTk
         PO7A1yiG6Cg0NnZ0imJKDLl2xr8zeXAkz1Fg1k2MwSgWF21iEv4VJ4rvdVPZqjKjHeEB
         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.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;
```

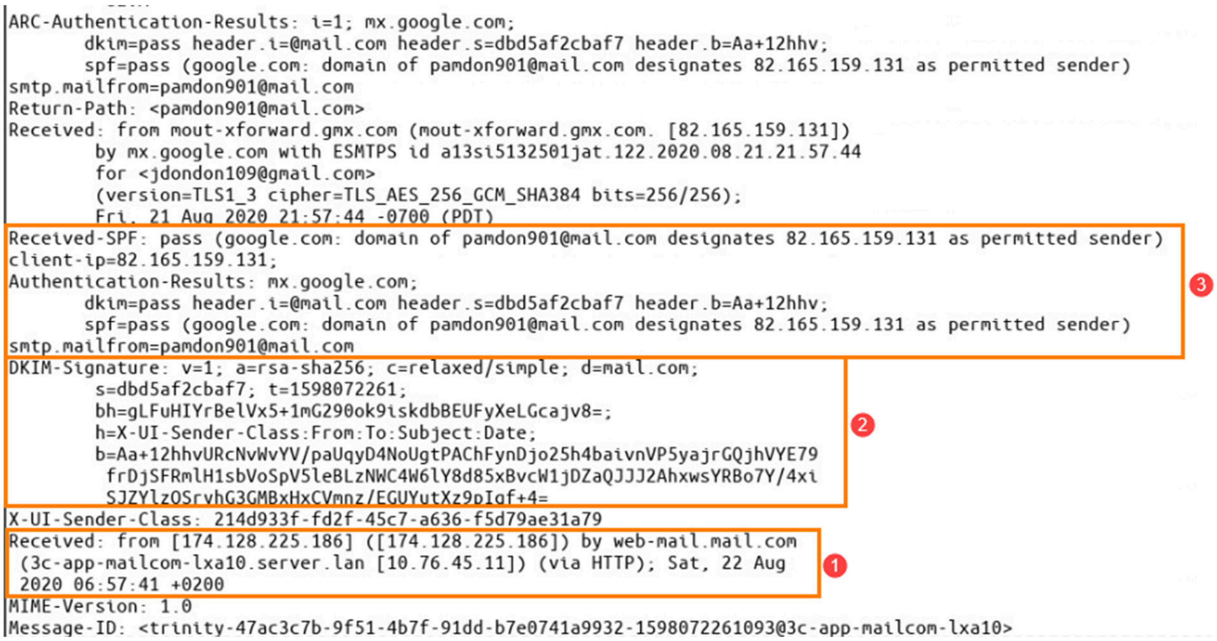
15. Now that we are at the bottom of the email, let us dissect the data we see and look at some metadata that is of great value to investigations.

    a. The first set of data is the email body at the very bottom, as seen in *item* **1** below.
    b. 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.
    c. 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.



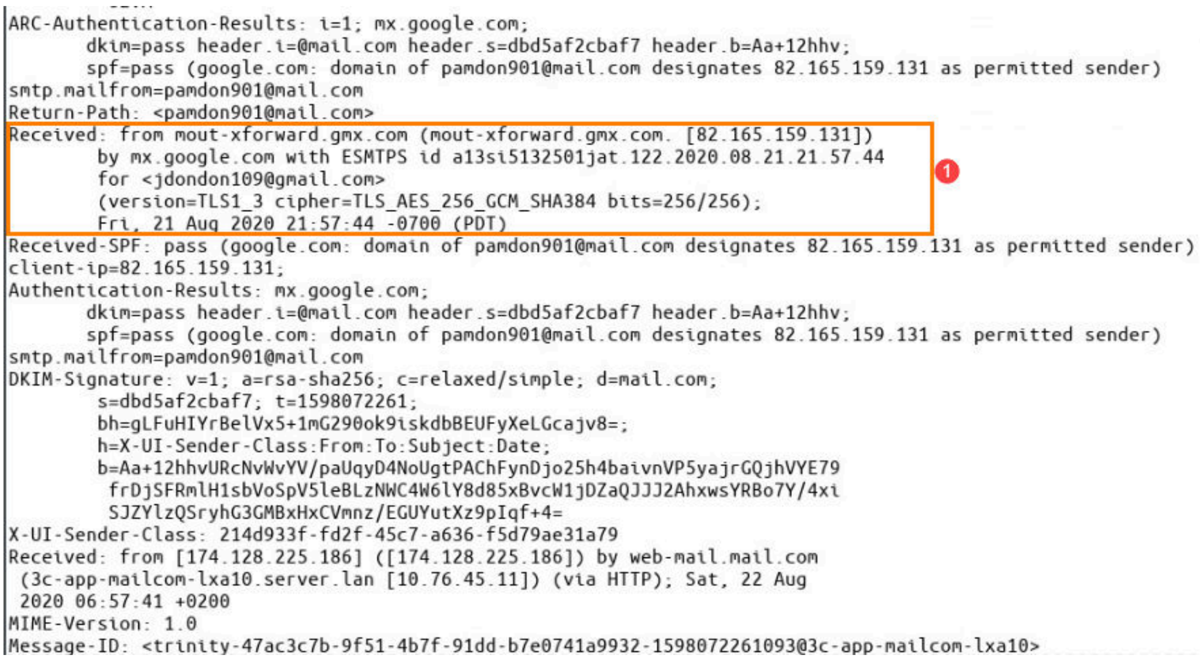
```
Message-ID: <trinity-47ac3c7b-9f51-4b7f-91dd-b7e0741a9932-1598072261093@3c-app-mailcom-lxa10>
From: Pam Don <pamdon901@mail.com>
To: jdondon109@gmail.com, jdondon109@protonmail.com
Subject: The deadline
Content-Type: text/html; charset=UTF-8
Date: Sat, 22 Aug 2020 06:57:41 +0200
Importance: normal
Sensitivity: Normal
X-Priority: 3
X-Provags-ID: V03:K1:PBYGf0I4i9CKnTzk+p1E1xejk7kw6j57Xb0ez5q0RBEw3NUN0ClstZe5vmAEcQV41eNdh
 1lubBbIfNuQdYqhUgJBkexd+iuhfNNoFaR9SFdhMIZlmb+Uq1ea/7Ulutptm4+3ho0ktvYMg7Grm
 rFEo5h4T4C5iKdTLxzG5G1j3W1KMKqGZM8/W+1nniy9DyAmzOf4QSK0UQaYVTsRGFO7indIz6j9I
 hfSSxcDxfz4bvn5A8G8hVX/VLswn0Z9ye4tYqgiqWhVz3lVaaNGS+JGgkSyOyL0jC5ncqOBIGMbt
 Ag=
X-Spam-Flag: YES
X-UI-Out-Filterresults: junk:10;V03:K0:Pabl6RZMjmo=:qxdxnoLdtLRZSZE8TDe9wrKg
 +5ZueEvYEf6wP5hQo59kXC8QhRxX9GJSVcqQ3/takbemZP4CT8+5drrNPt+Z3CG8+SkMMJZx2
 Jhebf/V3+25EyoyRfNmlK0qx0wdp9xa4GB56Vn6iYjLhN6JjGH/OaYBko2GYLRkoCRn1Qwuu4
 5JdGeQZRWCKBWPIVwP8TY+WakBUSpJj2wffKaS7s1TEoz/facfMrmRKYhk90+aiM4jADDtS9/
 AxEpfJOT2R2hxbRYHs5iY/26JH8FuLvxjMGy/zmNTBYCR2+SOqsUJiIIrJcRQmWjkiVOri489
 dfbVrlPswWW8zlMDz+7Se6MasNlY9vUCVqFdEhPo9T8vKm4j5/5Pr9vqblphM2beltdDY87UE
 ULSMAsTldABJ2XVefQOx4fgMSVoh6xha/LzI3cCqszNThQb7JvEMEMueLdo1+tR1nqOFJnnDa
 uYNpuBCzlizyXIk7kS+hmV+kH0fJS2b8YCUiZ5mdr0mSSb6sCiE5jyAmNNt5vzZ7x2ThycPNC
 t+qtvfA3gL6ZoGlnX0sY4hO22w5z22PuWOFjS9CQb/p8HKXuzMkrrFo+ZMyA2Dd9tcm2+QMjW
 r0hRl2GJFeUW1IFcSSMuIijkeFnGKQTziOdbub4lRW7ncuFL6Q4BDgIRcm9kdQ4rY6mricngC
 S7ZZMdmrkCLzFXzxipc242t/nXromiv25DtLNVqep/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.



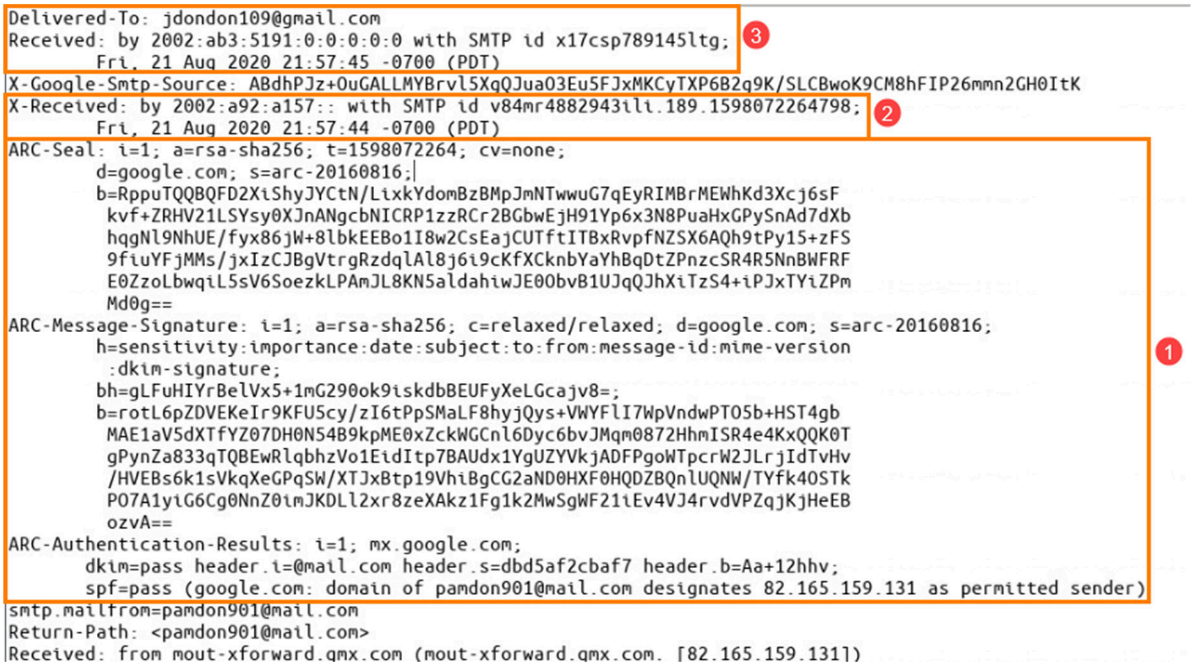
```
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=Aa+12hhv;
       spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender)
smtp.mailfrom=pamdon901@mail.com
Return-Path: <pamdon901@mail.com>
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+1mG29Ook9iskdbBEUFyXeLGcajv8=;
        h=X-UI-Sender-Class:From:To:Subject:Date;
        b=Aa+12hhvURcNvWvYV/paUqyD4NoUgtPAChFynDjo25h4baivnVP5yajrGQjhVYE79
         frDjSFRmlH1sbVoSpV5leBLzNWC4W6lY8d85xBvcW1jDZaQJJJ2AhxwsYRBo7Y/4xi
         SJZYlzOSrvhG3GMBxHxCVmnz/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+1mG290ok9iskdbBEUFyXeLGcajv8=;
        h=X-UI-Sender-Class:From:To:Subject:Date;
        b=Aa+12hhvURcNvWvYV/paUqyD4NoUgtPAChFynDjo25h4baivnVP5yajrGQjhVYE79
         frDjSFRmlH1sbVoSpV5leBLzNWC4W6lY8d85xBvcW1jDZaQJJJ2AhxwsYRBo7Y/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;
        Fri, 21 Aug 2020 21:57:45 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJz+OuGALLMYBrvl5XqQJua03Eu5FJxMKCyTXP6B2q9K/SLCBwoK9CM8hFIP26mmn2GH0ItK
X-Received: by 2002:a92:a157:: with SMTP id v84mr4882943ili.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=RppuTQQBQFD2XiShyJYCtN/LixkYdomBzBMpJmNTwwuG7qEyRIMBrMEWhKd3Xcj6sF
         kvf+ZRHV21LSYsy0XJnANgcbNICRP1zzRCr2BGbwEjH91Yp6x3N8PuaHxGPySnAd7dXb
         hqgNl9NhUE/fyx86jW+8lbkEEBo1I8w2CsEajCUTftITBxRvpfNZSX6AQh9tPy15+zFS
         9fiuYFjMMs/jxIzCJBgVtrgRzdqlAl8j6i9cKfXCknbYaYhBqDtZPnzcSR4R5NnBWFRF
         E0ZzoLbwqiL5sV6SoezkLPAmJL8KN5aldahiwJE0ObvB1UJqQJhXiTzS4+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+VWYFlI7WpVndwPTO5b+HST4gb
         MAE1aV5dXTfYZ07DH0N54B9kpME0xZckWGCnl6Dyc6bvJMqm0872HhmISR4e4KxQQK0T
         gPynZa833qTQBEwRlqbhzVo1EidItp7BAUdx1YgUZYVkjADFPgoWTpcrW2JLrjIdTvHv
         /HVEBs6k1sVkqXeGPqSW/XTJxBtp19VhiBgCG2aND0HXF0HQDZBQnlUQNW/TYfk40STk
         PO7A1yiG6Cg0NnZ0imJKDLl2xr8zeXAkz1Fg1k2MwSgWF21iEv4VJ4rvdVPZqjKjHeEB
         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.gmx.com (mout-xforward.gmx.com. [82.165.159.131])
```

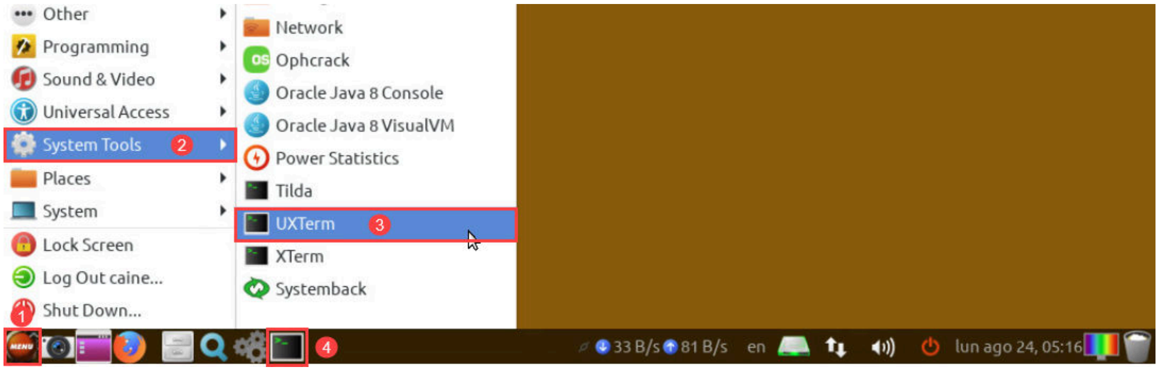
19. As you saw in this exercise, the email header can contain a wealth of information and can assist in different kinds of ways. Headers can be used to determine the authenticity of an email and to trace an email back to its source. This is an exercise that is practiced by forensic examiners on a regular 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

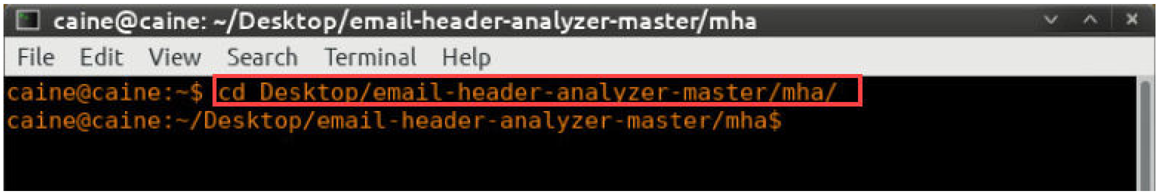
In the previous exercise, we manually went through the email header to learn about the different metadata stored within it. Because it can sometimes be overwhelming, specific tools were designed to help specialists review the data and go directly to the information they need. One such tool is *Email 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.

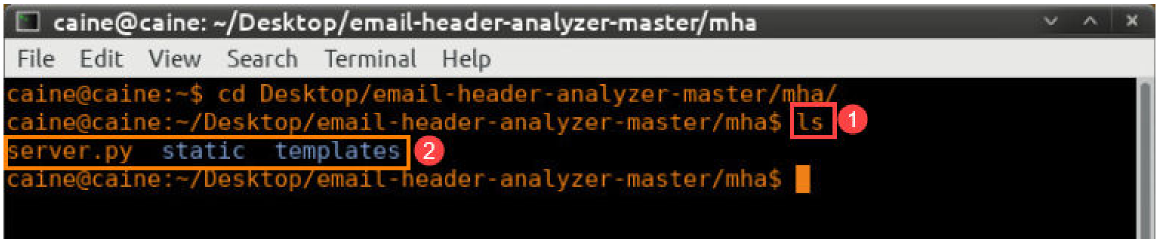
```
cd Desktop/email-header-analyzer-master/mha/
```


caine@caine: ~/Desktop/email-header-analyzer-master/mha
File Edit View Search Terminal Help

```
caine@caine:~$ cd Desktop/email-header-analyzer-master/mha/
caine@caine:~/Desktop/email-header-analyzer-master/mha$
```

3. 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
```

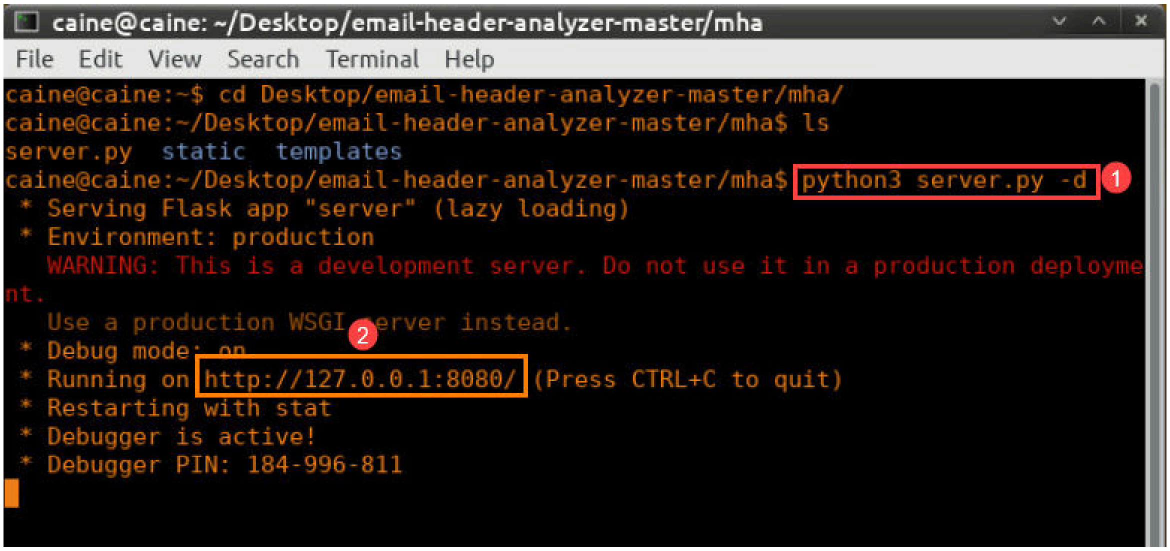


caine@caine: ~/Desktop/email-header-analyzer-master/mha
File Edit View Search Terminal Help
1
2

```
caine@caine:~$ cd Desktop/email-header-analyzer-master/mha/
caine@caine:~/Desktop/email-header-analyzer-master/mha$ ls
server.py  static  templates
caine@caine:~/Desktop/email-header-analyzer-master/mha$ 
```

4. 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.

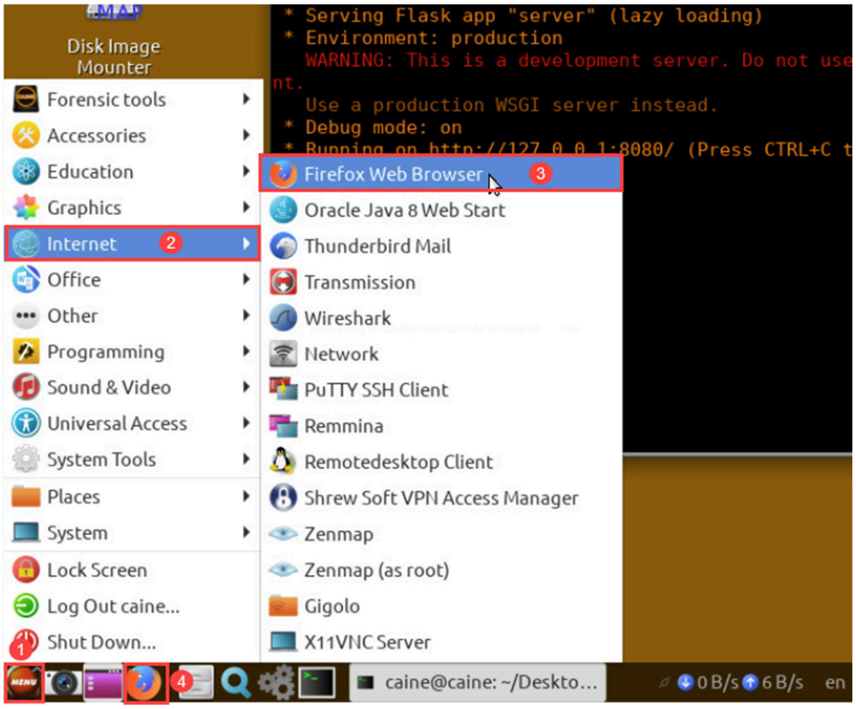
```
python3 server.py -d
```



caine@caine: ~/Desktop/email-header-analyzer-master/mha
File Edit View Search Terminal Help
1
2

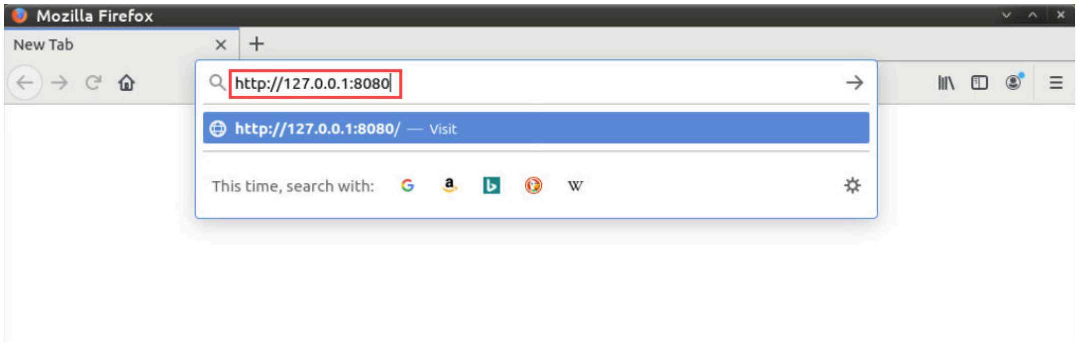
```
caine@caine:~$ cd Desktop/email-header-analyzer-master/mha/
caine@caine:~/Desktop/email-header-analyzer-master/mha$ ls
server.py  static  templates
caine@caine:~/Desktop/email-header-analyzer-master/mha$ python3 server.py -d
 * Serving Flask app "server" (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployme
nt.
   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
```

5. 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.

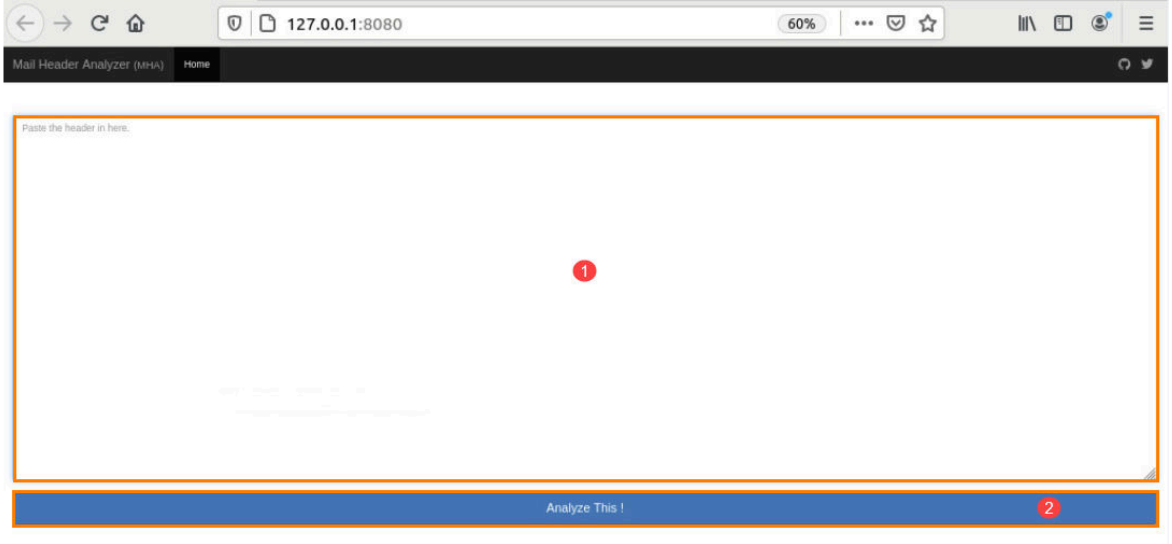


```
 * Serving Flask app "server" (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use
nt.
   Use a production WSGI server instead.
 * Debug mode: on
 * Running on http://127.0.0.1:8080/ (Press CTRL+C t
```

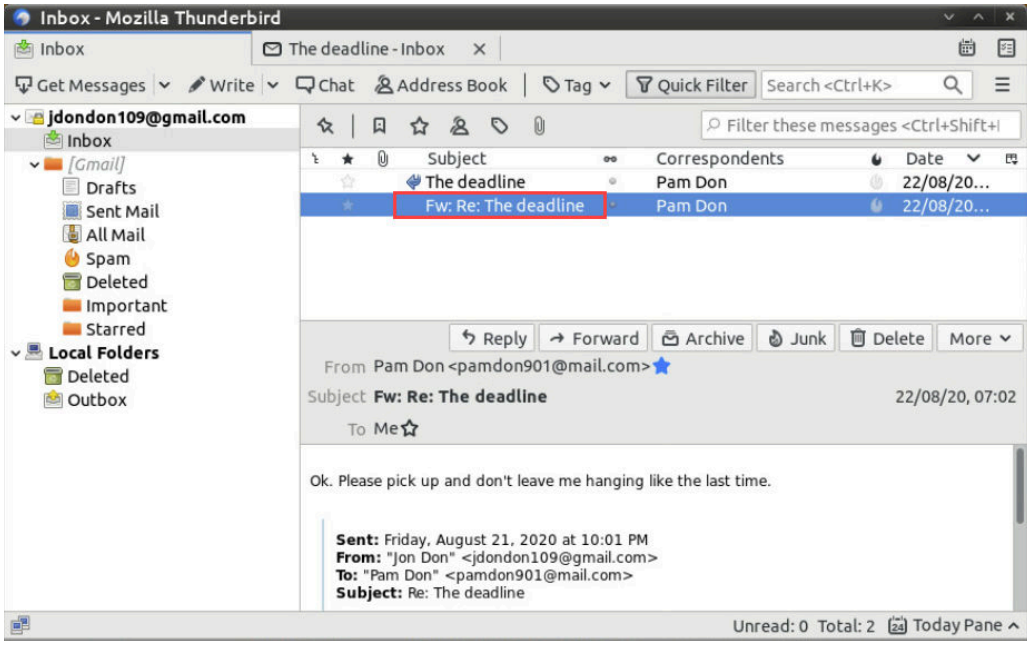
6. Now that the web browser is open, type the URL `http://127.0.0.1:8080` in the address bar of the web browser, as highlighted below, and press **Enter**. This will take us to the *Email Header Analyzer* interface.



7. 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**.



8. 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.



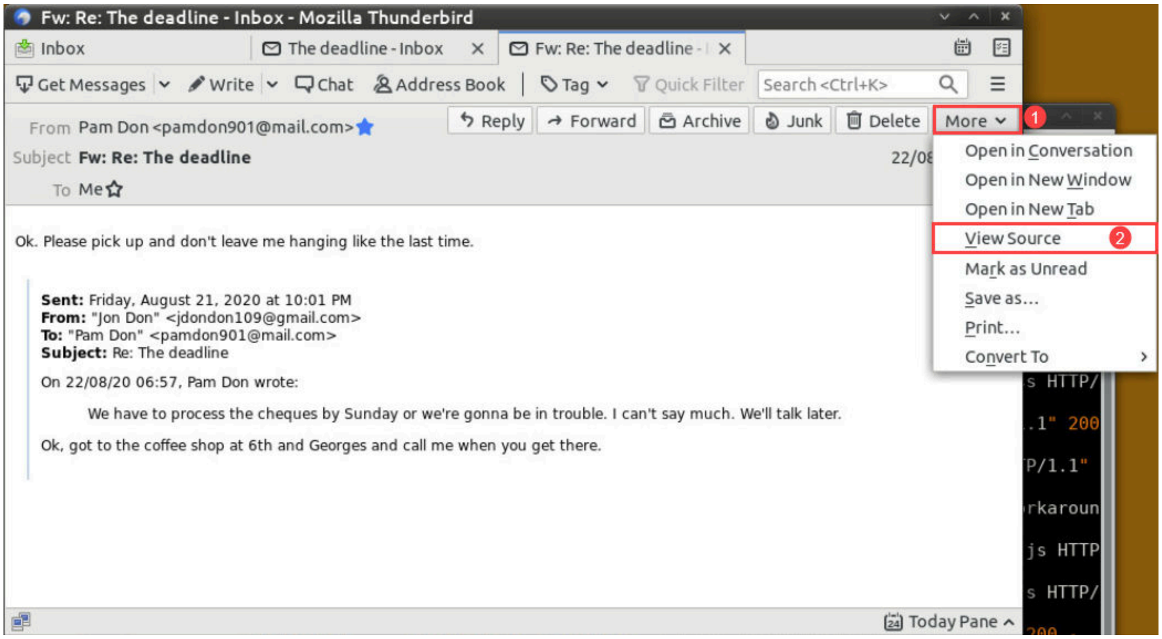
Subject	Correspondents	Date
The deadline	Pam Don	22/08/20…
Fw: Re: The deadline	Pam Don	22/08/20…

From Pam Don <pamdon901@mail.com>
Subject **Fw: Re: The deadline** 22/08/20, 07:02
To Me

Ok. Please pick up and don't leave me hanging like the last time.

Sent: Friday, August 21, 2020 at 10:01 PM
From: "Jon Don" <jdondon109@gmail.com>
To: "Pam Don" <pamdon901@mail.com>
Subject: Re: The deadline

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



From Pam Don <pamdon901@mail.com>
Subject **Fw: Re: The deadline**
To Me
22/08

Ok. Please pick up and don't leave me hanging like the last time.

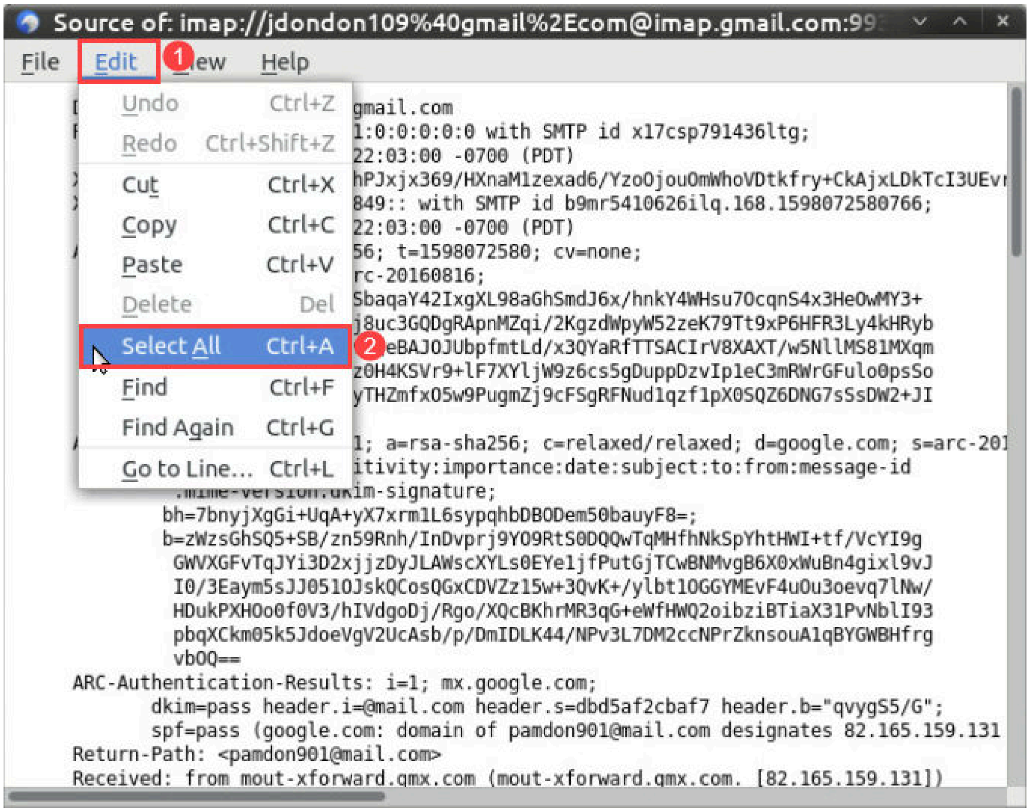
Sent: Friday, August 21, 2020 at 10:01 PM
From: "Jon Don" <jdondon109@gmail.com>
To: "Pam Don" <pamdon901@mail.com>
Subject: Re: The deadline

On 22/08/20 06:57, Pam Don wrote:

> We have to process the cheques by Sunday or we're gonna be in trouble. I can't say much. We'll talk later.

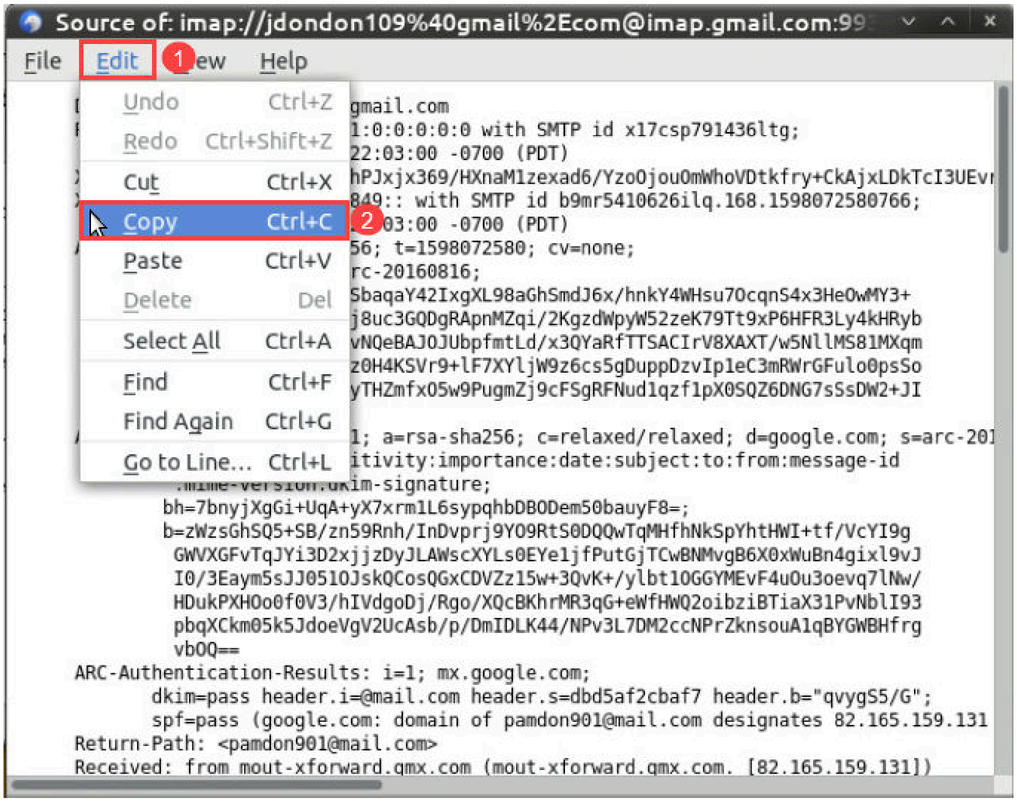
Ok, got to the coffee shop at 6th and Georges and call me when you get there.

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.**



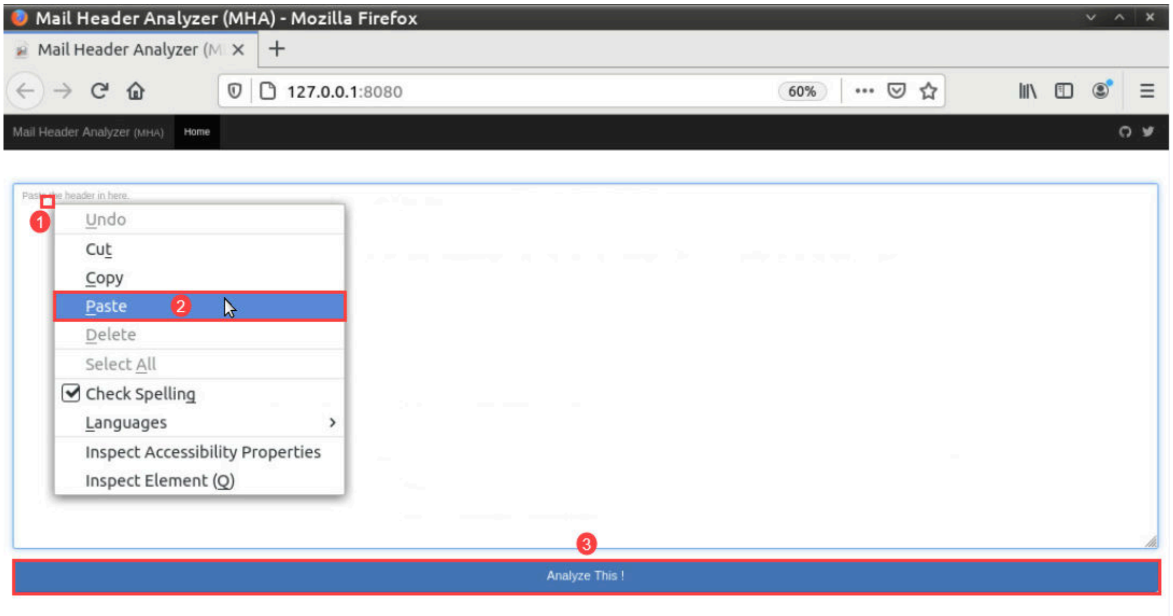
```
gmail.com
1:0:0:0:0:0 with SMTP id x17csp791436ltg;
22:03:00 -0700 (PDT)
hPJxjx369/HXnaM1zexad6/YzoOjouOmWhoVDtkfry+CkAjxLDkTcI3UEv
849:: with SMTP id b9mr5410626ilq.168.1598072580766;
22:03:00 -0700 (PDT)
56; t=1598072580; cv=none;
rc-20160816;
SbaqaY42IxgXL98aGhSmdJ6x/hnkY4WHsu7OcqnS4x3HeOwMY3+
j8uc3GQDgRApnMZqi/2KgzdWpyW52zeK79Tt9xP6HFR3Ly4kHRyb
eBAJOJUbpfmtLd/x3QYaRfTTSACIrV8XAXT/w5NllMS81MXqm
z0H4KSVr9+lF7XYljW9z6cs5gDuppDzvIp1eC3mRWrGFulo0psSo
yTHZmfx05w9PugmZj9cFSgRFNud1qzf1pX0SQZ6DNG7sSsDW2+JI

1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-201
itivity:importance:date:subject:to:from:message-id
    :mime-version:dkim-signature;
        bh=7bnyjXgGi+UqA+yX7xrm1L6sypqhbDBODem50bauyF8=;
        b=zWzsGhSQ5+SB/zn59Rnh/InDvprj9YO9RtS0DQQwTqMHfhNkSpYhtHWI+tf/VcYI9g
         GWVXGFvTqJYi3D2xjjzDyJLAWscXYLs0EYe1jfPutGjTCwBNMvgB6X0xWuBn4gixl9vJ
         I0/3Eaym5sJJ051OJskQCosQGxCDVZz15w+3QvK+/ylbt1OGGYMEvF4uOu3oevq7lNw/
         HDukPXHOo0f0V3/hIVdgoDj/Rgo/XQcBKhrMR3qG+eWfHWQ2oibziBTiaX31PvNblI93
         pbqXCkm05k5JdoeVgV2UcAsb/p/DmIDLK44/NPv3L7DM2ccNPrZknsouA1qBYGWBHfrg
         vbOQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b="qvygS5/G";
       spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131
Return-Path: <pamdon901@mail.com>
Received: from mout-xforward.gmx.com (mout-xforward.gmx.com. [82.165.159.131])
```

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

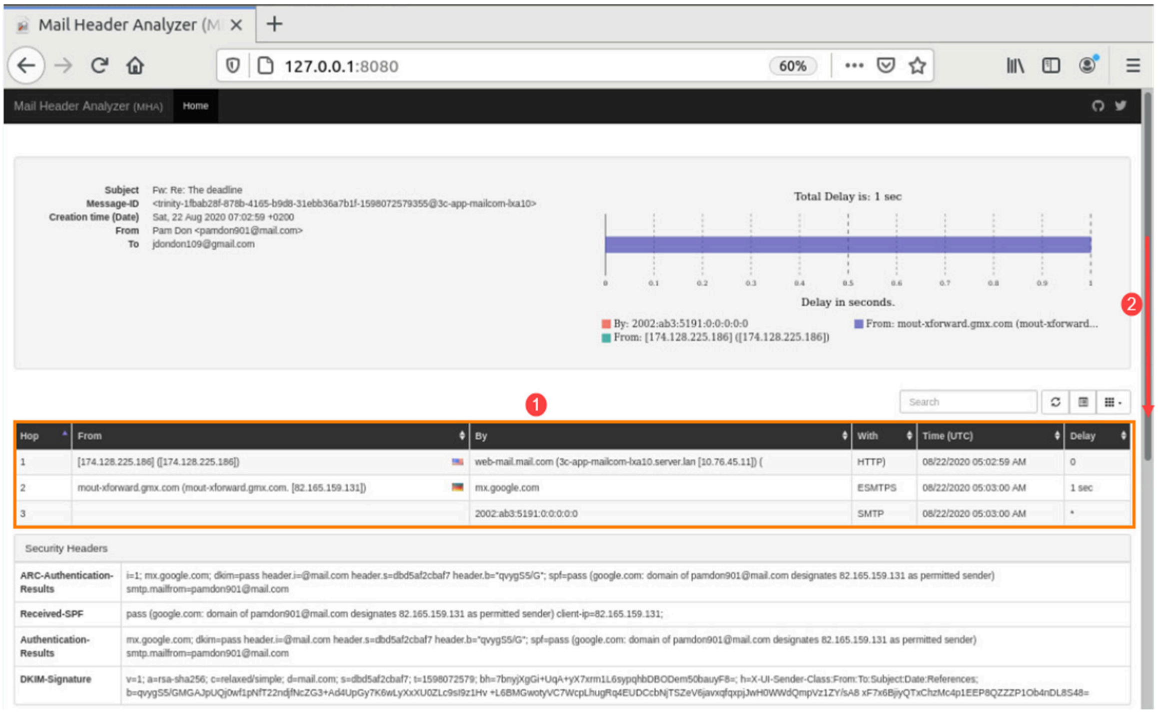


```
gmail.com
1:0:0:0:0:0 with SMTP id x17csp791436ltg;
22:03:00 -0700 (PDT)
hPJxjx369/HXnaM1zexad6/YzoOjouOmWhoVDtkfry+CkAjxLDkTcI3UEvr
849:: with SMTP id b9mr5410626ilq.168.1598072580766;
03:00 -0700 (PDT)
56; t=1598072580; cv=none;
rc-20160816;
SbaqaY42IxgXL98aGhSmdJ6x/hnkY4WHsu7OcqnS4x3HeOwMY3+
j8uc3GQDgRApnMZqi/2KgzdWpyW52zeK79Tt9xP6HFR3Ly4kHRyb
vNQeBAJOJUbpfmtLd/x3QYaRfTTSACIrV8XAXT/w5NllMS81MXqm
z0H4KSVr9+lF7XYljW9z6cs5gDuppDzvIpleC3mRWrGFulo0psSo
yTHZmfx05w9PugmZj9cFSgRFNud1qzf1pX0SQZ6DNG7sSsDW2+JI

1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-201
itivity:importance:date:subject:to:from:message-id
    :mime-version:dkim-signature;
   bh=7bnyjXgGi+UqA+yX7xrm1L6sypqhbDBODem50bauyF8=;
   b=zWzsGhSQ5+SB/zn59Rnh/InDvprj9YO9RtS0DQQwTqMHfhNkSpYhtHWI+tf/VcYI9g
    GWVXGFvTqJYi3D2xjjzDyJLAWscXYLs0EYe1jfPutGjTCwBNMvgB6X0xWuBn4gixl9vJ
    I0/3Eaym5sJJ051OJskQCosQGxCDVZz15w+3QvK+/ylbt1OGGYMEvF4uOu3oevq7lNw/
    HDukPXHOo0f0V3/hIVdgoDj/Rgo/XQcBKhrMR3qG+eWfHWQ2oibziBTiaX31PvNblI93
    pbqXCkm05k5JdoeVgV2UcAsb/p/DmIDLK44/NPv3L7DM2ccNPrZknsouA1qBYGWBHfrg
    vbOQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b="qvygS5/G";
       spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131
Return-Path: <pamdon901@mail.com>
Received: from mout-xforward.gmx.com (mout-xforward.gmx.com. [82.165.159.131])
```

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.


Mail Header Analyzer (M ×
127.0.0.1:8080
60%
Mail Header Analyzer (MHA)
Home
1
2

Subject	Fw: Re: The deadline
Message-ID	<trinity-1fbab28f-878b-4165-b9d8-31ebb36a7b1f-1598072579355@3c-app-mailcom-lxa10>
Creation time (Date)	Sat, 22 Aug 2020 07:02:59 +0200
From	Pam Don <pamdon901@mail.com>
To	jdondon109@gmail.com

Total Delay is: 1 sec
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
Delay in seconds.
By: 2002:ab3:5191:0:0:0:0:0
From: [174.128.225.186] ([174.128.225.186])
From: mout-xforward.gmx.com (mout-xforward...
Search

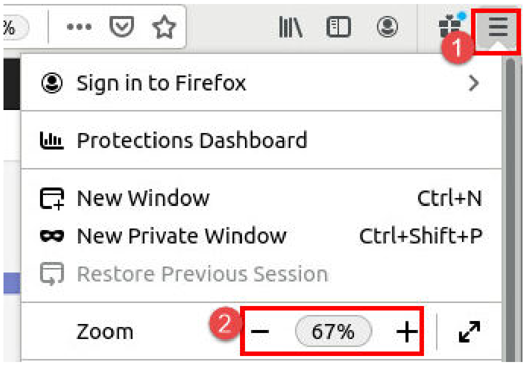
Hop	From	By	With	Time (UTC)	Delay
1	[174.128.225.186] ([174.128.225.186])	web-mail.mail.com (3c-app-mailcom-lxa10.server.lan [10.76.45.11]) (	HTTP)	08/22/2020 05:02:59 AM	0
2	mout-xforward.gmx.com (mout-xforward.gmx.com. [82.165.159.131])	mx.google.com	ESMTPS	08/22/2020 05:03:00 AM	1 sec
3		2002:ab3:5191:0:0:0:0:0	SMTP	08/22/2020 05:03:00 AM	*

Security Headers

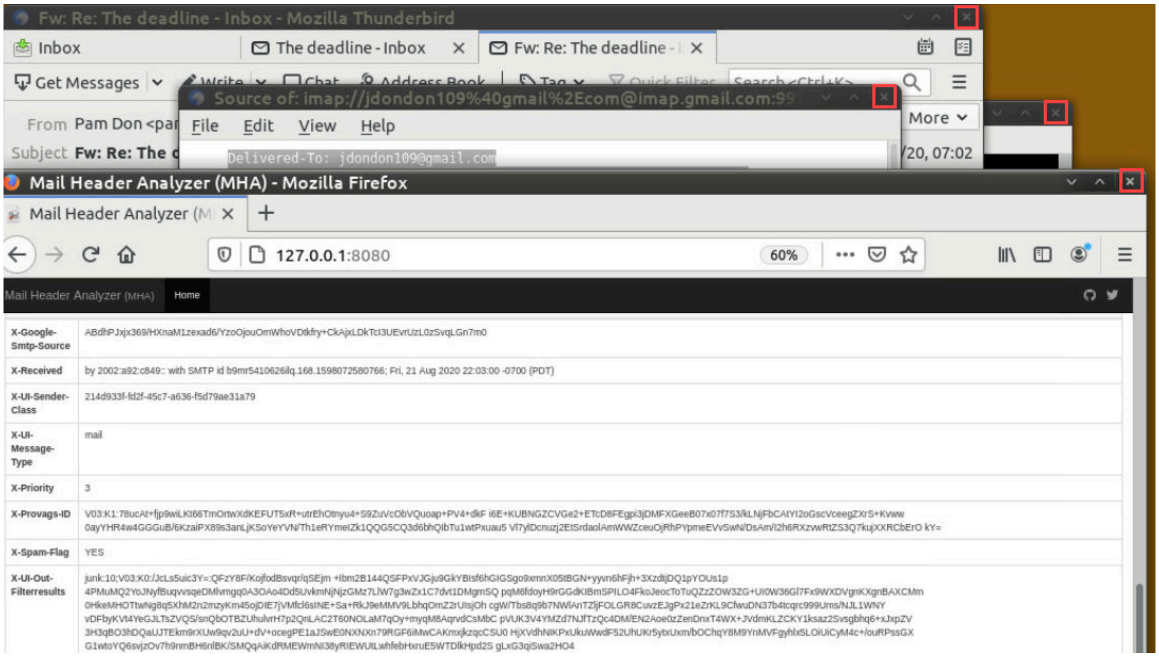
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b="qvygS5/G"; spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131 as permitted sender) smtp.mailfrom=pamdon901@mail.com
Received-SPF	pass (google.com: domain of pamdon901@mail.com 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="qvygS5/G"; 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=1598072579; bh=7bnyjXgGi+UqA+yX7xrm1L6sypqhbDBODem50bauyF8=; h=X-UI-Sender-Class:From:To:Subject:Date:References; b=qvygS5/GMGAJpUQj0wf1pNfT22ndjfNcZG3+Ad4UpGy7K6wLyXxXU0ZLc9sI9z1Hv +L6BMGwotyVC7WcpLhugRq4EUDCcbNjTSZeV6javxqfqxpjJwH0WWdQmpVz1ZY/sA8 xF7x6BjiyQTxChzMc4p1EEP8QZZZP1Ob4nDL8S48=

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.



```
Delivered-To: jdondon109@gmail.com
```

X-Google-Smtp-Source	ABdhPJxjx369/HXnaM1zexad6/YzoOjouOmWhoVDtkfry+CkAjxLDkTcI3UEvrUzL0zSvqLGn7m0
X-Received	by 2002:a92:c849:: with SMTP id b9mr5410626ilq.168.1598072580766; Fri, 21 Aug 2020 22:03:00 -0700 (PDT)
X-UI-Sender-Class	214d933f-fd2f-45c7-a636-f5d79ae31a79
X-UI-Message-Type	mail
X-Priority	3
X-Provags-ID	V03:K1:78ucAt+fjp9wiLKt66TmOrtwXdKEFUT5xR+utrEhOtnyu4+S9ZuVcObVQuoap+PV4+dkF i6E+KUBNGZCVGe2+ETcD8FEgpi3jDMFXGeeB07x07f7S3/kLNjFbCAtYI2oGscVceegZXrS+Kvww 0ayYHR4w4GGGuB/6KzaiPX89s3anLjKSoYeYVN/Th1eRYmeIZk1QQG5CQ3d6bhQIbTu1wtPxuau5 Vl7ylDcnuzj2EtSrdaolAmWWZceuOjRhPYpmeEVvSwN/DsAm/I2h6RXzvwRtZS3Q7kujXXRCbErO kY=
X-Spam-Flag	YES
X-UI-Out-Filterresults	junk:10;V03:K0:/JcLs5uic3Y=:QFzY8F/KojfodBsvqr/qSEjm +Ibm2B144QSFPxVJGju9GkYBIsf6hGIGSgo9xmnX05tBGN+yyvn6hFjh+3XzdtjDQ1pYOUs1p 4PMuMQ2YoJNyfBuqvvsqeDMlvmgq0A3OAo4Dd5UvkmNjNjzGMz7LlW7g3wZx1C7dvt1DMgmSQ pqM6fdoyH9rGGdKIBmSPILO4FkoJeocToTuQZzZOW3ZG+UI0W36Gl7Fx9WXDVgnKXgnBAXCMm 0HkeMHOTtwNg8q5XhM2n2mzyKm45ojDIE7jVMfcl6sINE+Sa+RkJ9eMMV9LbhqOmZ2rUIsjOh cgW/Tbs8q9b7NWlAnTZljFOLGR8CuvzEJgPx21eZrKL9CfwuDN37b4tcqrc999Ums/NJL1WNY vDFbyKVt4YeGJLTsZVQS/snQbOTBZUhulvrH7p2QnLAC2T60NOLaM7qOy+myqM8AqrvdCsMbC pVUK3V4YMZd7NJfTzQc4DM/EN2Aoe0zZenDnxT4WX+JVdmKLZCKY1ksaz2Svsgbhq6+xJxpZV 3H3qBO3hDQaUJTEkm9rXUw9qv2uU+dV+ocegPE1aJSwE0NXNXn79RGF6iMwCAKmxjkzqoCSU0 HjXVdhNIKPxUkuWwdF52UhUKr5ytxUxm/bOChqY8M9YnMVFgyhlxSLOiUiCyM4c+/ouRPssGX G1wtoYQ6svjzOv7h9nmBH6nlBK/SMQqAiKdRMEWmNI38yRIEWUtLwhfebHxruE5WTDlkHpd2S gLxG3qiSwa2HO4