

## **CYBR472 Lab 12: Email Header Analysis**

### **Assessment Overview**

This lab assess your email forensics skills through the extraction and analysis of email headers. You will identify message origins, verify authenticity, and establish timelines using metadata. This lab is worth 6% of your course grade.

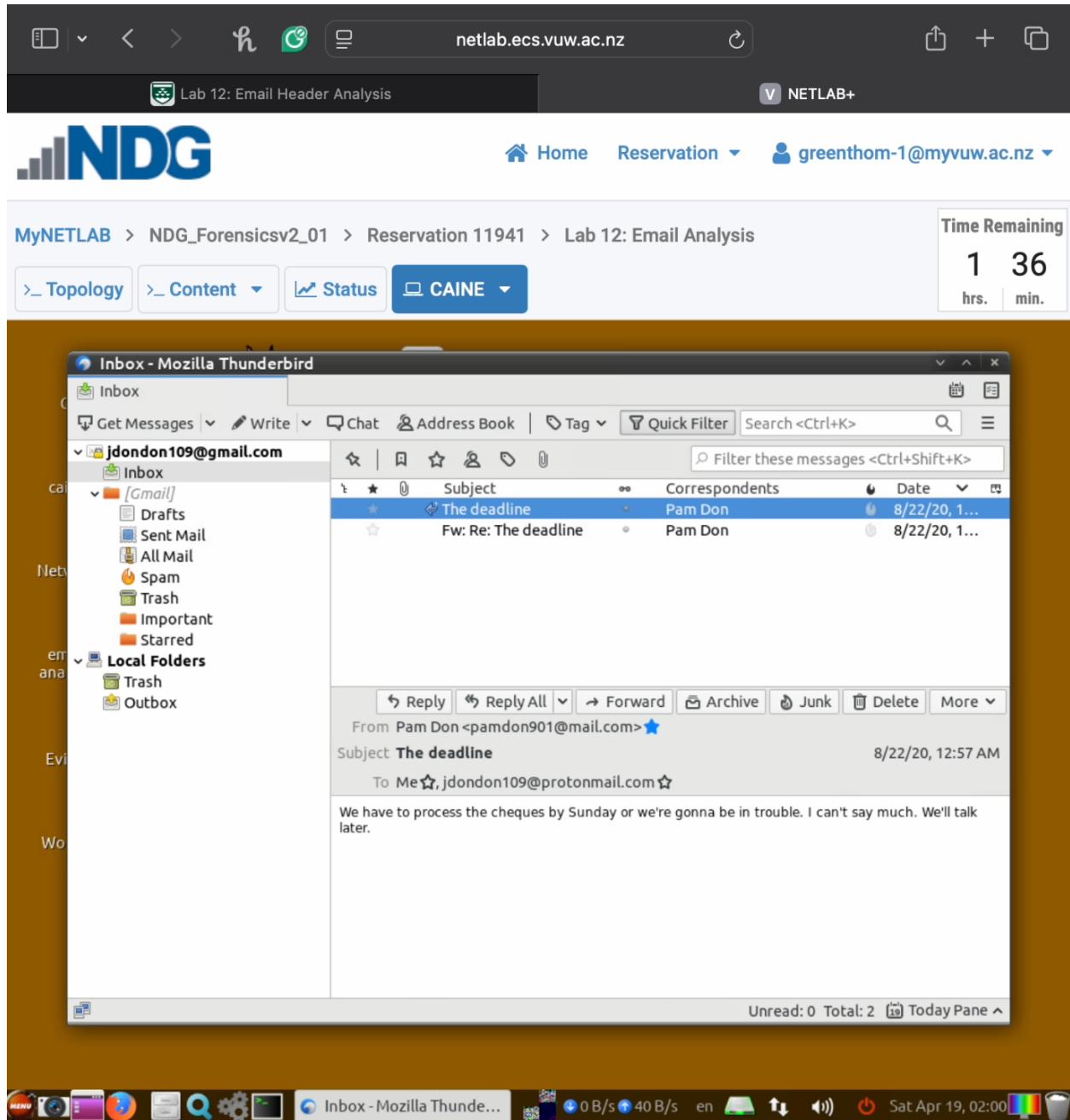
### **Submission Guidelines**

- Include a heading with lab number, your name, and student ID
- Provide numbered screenshots as specified
- Include brief descriptions only when requested
- Submit as a single PDF document

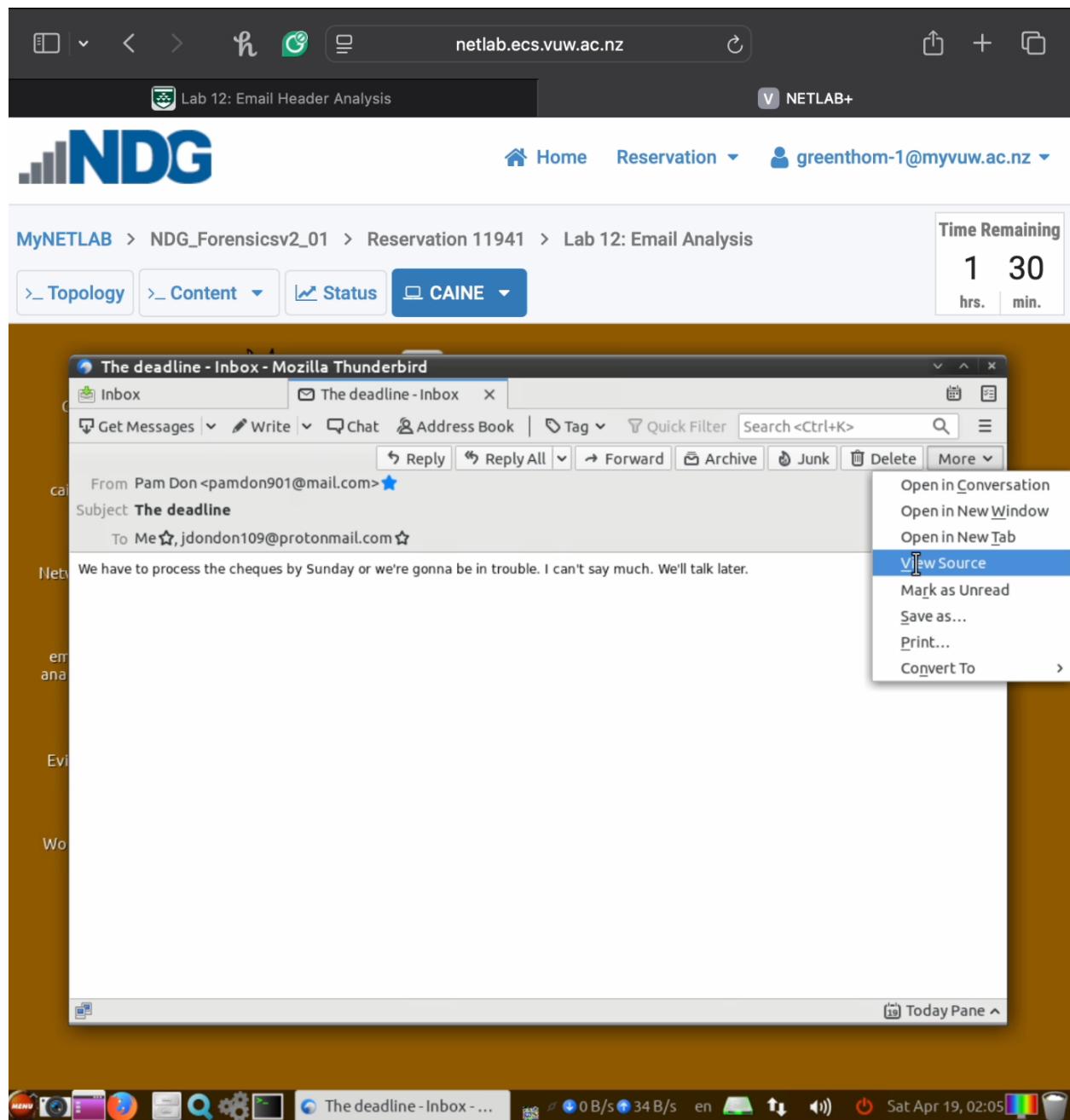
### **Part 1: Manual Email Header Extraction and Analysis (30 Marks)**

#### **Task 1: Email Header Extraction (10 marks)**

- Launch Thunderbird and select the email with subject “The deadline”
- Extract the header using View Source
- Save with filename format: FOR\_LAB\_012\_[YOUR-STUDENT-ID].txt
- Required screenshots:
  - Thunderbird interface with email selected (step 1.4)



- View Source option accessed through More menu (step 1.8)



The screenshot shows a Linux desktop environment with a terminal window, a mail client window, and a system tray.

**Terminal Window:**

```

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+0uGALLMYBrvl5xg0Jua03EuFJxTP6B2g9K/5LCBwo9Cm8hf
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=RppuTQQ8QFD2XiShyJYCTN/LixkYdomBzMpJmNTwuG7qEyRIMBrMEWhKd3Xcj6sF
kvfZRHV21LSYsy0JnANgcbNICRP1zzRCr2BGbwEjH91Yp6x3N8PuHxGPySnAd7dXb
hqgnl9NhUE/fyx86jW+8lbkEEBo1IBw2CsEajUTffITBxRvpfnZSX6A0h9tPy15+zFS
9fiuYFjMMMs/jxIzCJBgVtrgRzdqlAl8j6i9ckfxCknbYaYhBqDtZPnzcsR4R5NnBWFRF
E0Zzolbwqil5s6SoezklLAmJL8KN5aldaihwJE00bvB1UjqQjhKiTzS4+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=glFuHlYBelVx5+1mG290ok91skdbEUfyXeLGcajv8=;
b=rotL6pZDVEKeIr9KFU5cy/zI6tPpSMaLF8hyjQys+WVYFlI7WpVndwPT05b+HST4gb
MAElasV5dTfyZ07DH0N5489kpmEOxZckWGcnL6Oyc6bvJMqm0872hHmISRa4KxQQK0T
gPynZa833qTOBEwRlqbhzVo1eidItp7BAUdx1YgUZYVkjADFPgoNTpcrW2JLrj1dtVhv
/HVEBs6kisVkjXeqPgSw/XTJxBtp19VhiBgCg2aND0HXFB0HQDZBQnlUQNw/TYfk40STK
P07Aiy1g6CcG0NnZ0imJKDLl2xr8zeXAkz1Fg1k2Mw5gWF21iEv4VJ4rvdVPzqjKjHeEB
OVA==

ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@mail.com header.s=dbd5af2cbaf7 header.b=Aa+1hhv;
spf=pass (google.com: domain of pamdon901@mail.com designates 82.165.159.131
Return-Path: <pamdon901@mail.com>
Received: from mout-xforward.qmx.com (mout-xforward.qmx.com. [82.165.159.131])
```

**Mail Client Window:**

Subject: Lab 12: Email Header Analysis

Time Remaining: 1 30 hrs. min.

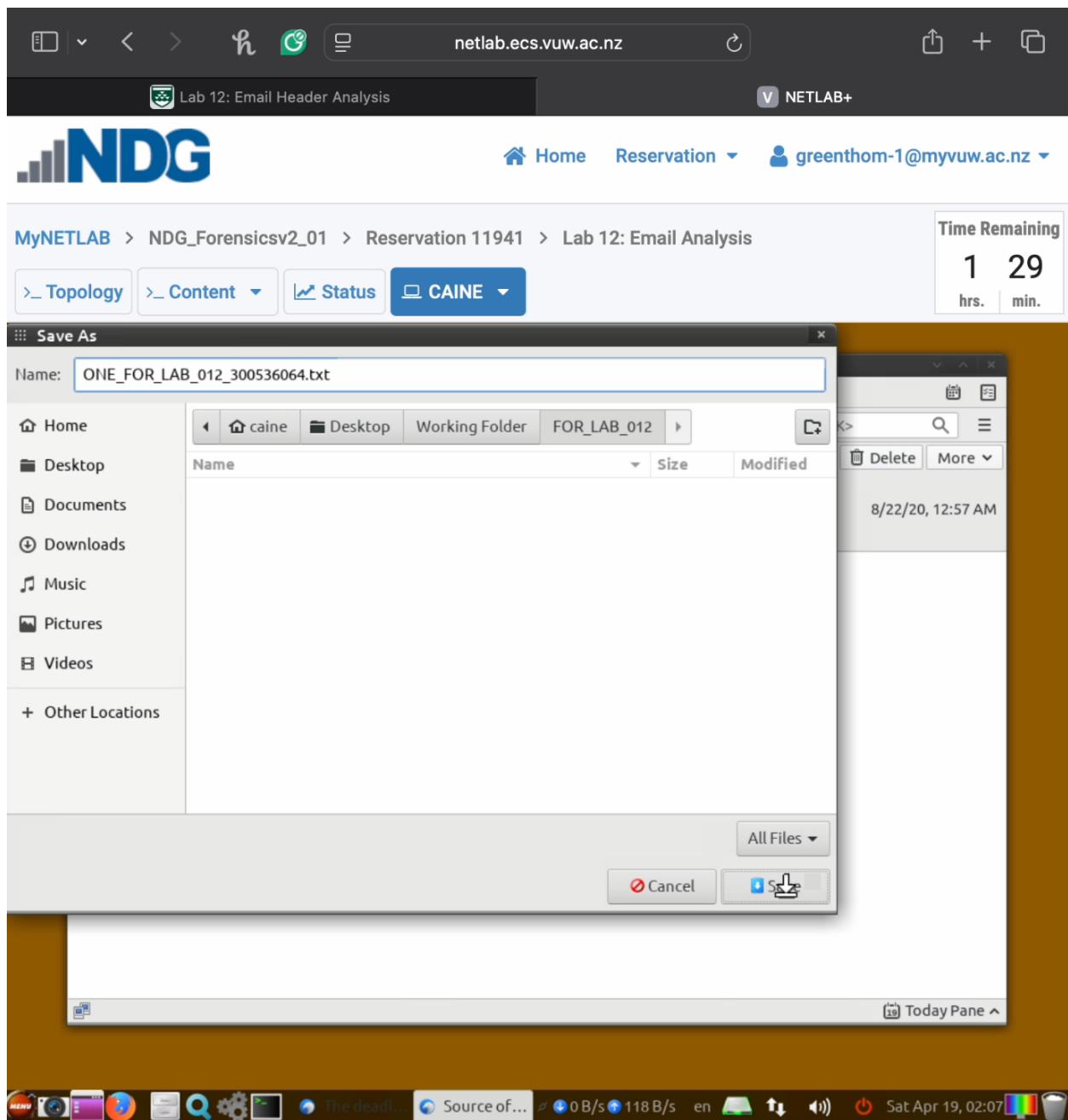
Message Preview:

I'll talk later.

**System Tray:**

- File, Edit, View, Help
- Source of: imap://jdondon109@gmail%2Ecom@imap.gmail.com:993
- File Filter Search <Ctrl+K>
- Archive, Junk, Delete, More
- Today Pane

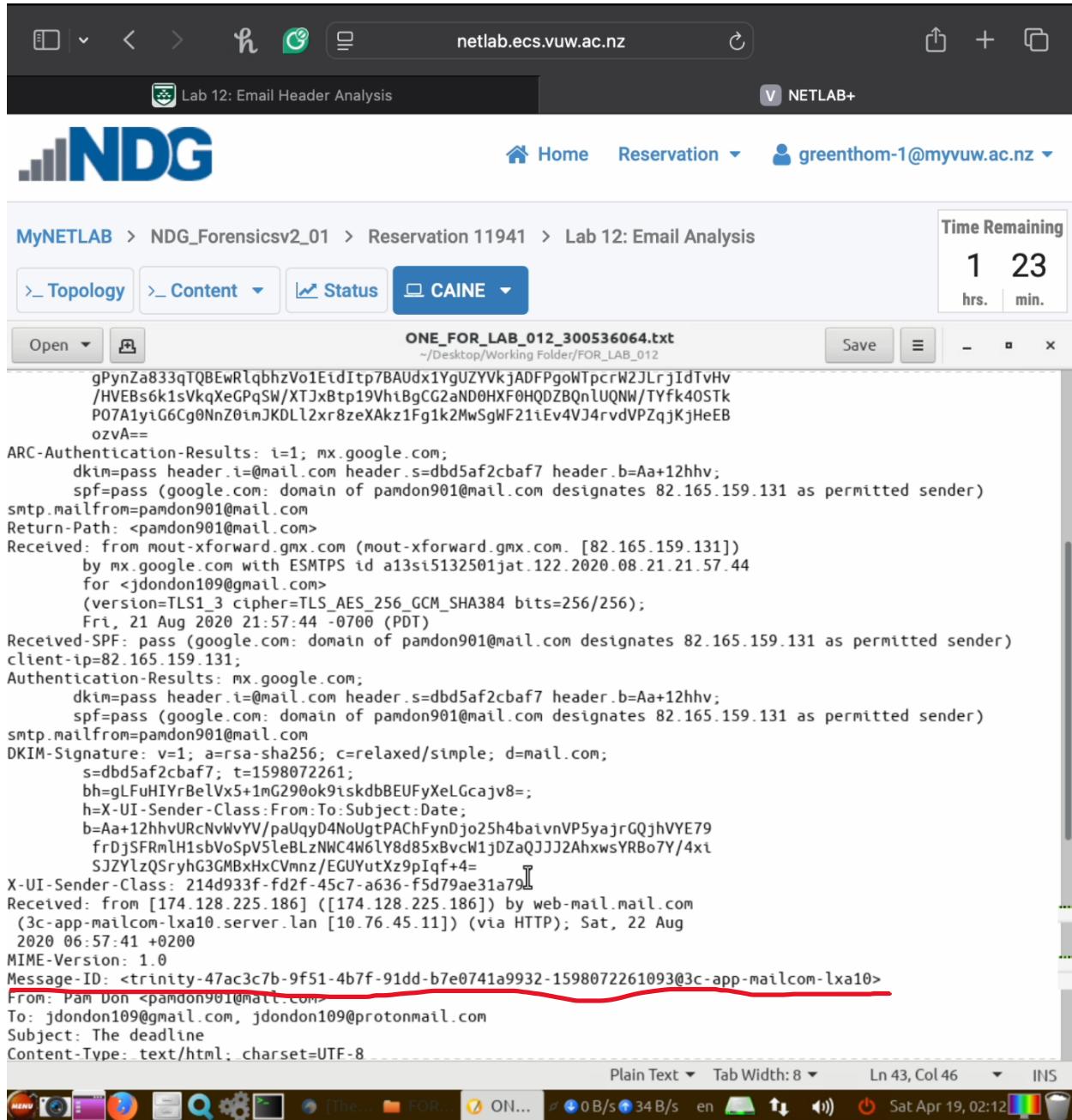
- Saved header file in working directory (step 1.11)



### Task 2: Manual Header Analysis (10 marks)

- **Identify in the extracted header:**
  - **Message-ID**
  - **Sender's email and IP address**
  - **Date and time spent**
  - **Email routing path**
- **Required screenshots (multiple screenshots of step 1.16 with different highlighted elements):**

- Header file in text editor with Message-ID highlighted (step 1.16)



The screenshot shows a web interface for 'Lab 12: Email Header Analysis'. At the top, there's a navigation bar with icons for file operations, a search bar containing 'netlab.ecs.vuw.ac.nz', and a tab labeled 'Lab 12: Email Header Analysis'. Below the navigation is a header bar with the 'NDG' logo, a 'Home' link, a 'Reservation' dropdown, and a user account 'greenthom-1@myvuw.ac.nz'. A 'Time Remaining' box shows '1 23 hrs. min.'.

The main content area displays a file named 'ONE\_FOR\_LAB\_012\_300536064.txt' located at '~/Desktop/Working Folder/FOR\_LAB\_012'. The file contains an email header with various fields like 'ARC-Authentication-Results', 'Received', 'Received-SPF', 'Authentication-Results', 'DKIM-Signature', 'X-UI-Sender-Class', 'Received', 'MIME-Version', 'Message-ID', 'From', 'To', 'Subject', and 'Content-Type'. The 'Message-ID' field is highlighted with a red underline.

At the bottom of the screen, there's a toolbar with icons for various functions and a status bar showing 'Plain Text', 'Tab Width: 8', 'Ln 43, Col 46', 'INS', and system information including network speed (0 B/s), battery level, and the date/time 'Sat Apr 19, 02:12'.

```

gPynZa833qTQBEwRlqbhzVo1EidItp7BAUdx1YgUZYVkjADFPgoWTpcrW2JLrjIdTvHv
/HVEBs6k1sVkkXeGPqSW/XTJxBtp19h1BgcG2aND0HXFOHQDZBQnluQNW/TYfk4OSTk
P07A1yiG6Cg0NnZ0imJKDLl2xr8zeXAkz1Fg1k2MwSgWF21iEv4VJ4rvdVPZqjKjHeEB
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;
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+1mG290ok9tSkdbBEUFyXeLGcavv8=;
h=X-UI-Sender-Class:From:To:Subject:Date;
b=Aa+12hhvURcNvkYY/paUqyD4NoUgtPACHFynDjo25h4baivnP5yajrGQjhVYE79
frDjSFRmlH1sbVoSpV5leBLzNC4W6lY8d85xBvcW1jDZaQJJ2AhxwsYRB07Y/4xi
SJZYlzQSryhG3GMByHxCVmnz/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>
From: Pam Don <pamdon901@mail.com>
To: jdondon109@gmail.com, jdondon109@protonmail.com
Subject: The deadline
Content-Type: text/html; charset=UTF-8

```

- Section showing sender's IP address highlighted (step 1.16)

The screenshot shows a web-based interface for network and security analysis. At the top, there are browser-like navigation buttons (back, forward, search, refresh) and a URL bar showing "netlab.ecs.vuw.ac.nz". To the right of the URL bar are icons for file operations (upload, download, etc.) and a "NETLAB+" button.

The main header includes the "NDG" logo, a "Home" link, a "Reservation" dropdown, and a user account "greenthom-1@myvuw.ac.nz".

The page title is "Lab 12: Email Header Analysis". Below the title, the path is "MyNETLAB > NDG\_Forensicsv2\_01 > Reservation 11941 > Lab 12: Email Analysis".

A "Time Remaining" box shows "1 23 hrs. min.". Below it, a toolbar has buttons for "Topology", "Content", "Status", and "CAINE" (selected).

The main content area displays the raw text of an email header from "ONE\_FOR\_LAB\_012\_300536064.txt". The file is located at "/Desktop/Working Folder/FOR\_LAB\_012".

```

gPynZa833qTQBewRlqbhzVo1EidItp7BAUdx1YgUZYVkjADFPgoWTpcrW2JLrjIdTvHv
/HVEBs6k1sVkkXeGPqSW/XTJxBtp19VhiBgCG2aND0HXF0HQDZBQnlUQNw/TYfk40STk
P07A1yiG6Cg0NnZ0imJKDLL2xr8zeXAkz1Fg1k2MwSgWF211Ev4VJ4rvdVPZqjKjHeEB
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;
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+1mg290ok9iskdbBEUFyXeLGajv8=;
h=X-UI-Sender-Class:From:To:Subject:Date;
b=Aa+12hhvURcNvWvV/paUqyD4NoUgtPACfynDjo25h4baivnVP5yajrGQjhVYE79
frDjSFRmlH1sbVoSpV5leBLzNWC4W6lY8d85xBvcW1jDzaQJJ2AhxwsYRBo7Y/4xt
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>
From: Pam Don <pamdon901@mail.com>
To: jdondon109@gmail.com, jdondon109@protonmail.com
Subject: The deadline
Content-Type: text/html; charset=UTF-8

```

The bottom of the interface features a toolbar with various icons (menu, search, file operations, etc.) and a status bar showing "Plain Text", "Tab Width: 8", "Ln 43, Col 46", "INS", and the date/time "Sat Apr 19, 02:12".

- SPF and DKIM authentication results, if present (step 1.16)

MyNETLAB > NDG\_Forensicsv2\_01 > Reservation 11941 > Lab 12: Email Analysis

Time Remaining  
1 23 hrs. min.

**Content Tab (highlighted)**

```

ONE_FOR_LAB_012_300536064.txt
~/Desktop/Working Folder/FOR_LAB_012

gPynZa833zTQBewRlqbhzVo1EidItp7BAUDx1YgUZYVkjADFPgoWTpcrW2JLrjIdTvHv
/HVEBs6k1sVqkXeGPqSW/XTJxBtp19VhiBgCG2aND0HXF0HQDZBQnLUQNw/TYfk40STk
P07A1yG6Cg0NnZ0imJKDLl2xr8zeXAkz1Fg1k2MwSgWF21tEv4VJ4rvdVPZqjKjHeEB
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 ESMTP 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+1mG290ok91skdbBEUFyXeLGcavj8=;
h=X-UI-Sender-Class:From:To:Subject:Date;
b=Aa+12hhvURcNvWVY/paUqyD4NoUgtPACfYnDjo25h4baivnVP5yajrGQjhVYE79
frDjsFRmlH1sbVoSpV5leBLzNWc4W6lY8d85xBvcW1jDzaQJJ2AhxwsYRB07Y/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>
From: Pam Don <pamdon901@mail.com>
To: jdondon109@gmail.com, jdondon109@protonmail.com
Subject: The deadline
Content-Type: text/html; charset=UTF-8

```

Plain Text ▾ Tab Width: 8 ▾ Ln 43, Col 46 ▾ INS

Toolbar icons: MENU, Camera, PDF, Firefox, File, Search, Gear, etc.

### Task 3: Email Authentication Analysis (10 marks)

- Examine SPF, DKIM, and ARC authentication indicators
- Determine if email passed authentication checks
- Identify potential spoofing or tampering signs
- Required:
  - Screenshot of authentication results section (step 1.16, with authentication section highlighted) with your student ID visible (can be added as a note or overlay)

```

PynZa833qTQBewRlqbhzVo1EidItp7BAUdx1YgUZYVkjADFPgoWTpcrW2JLrjIdTvHv
/HVEBs6k1sVkjXeGPqSW/XTJxBtp19Vh1BgCG2aND0HXF0HQDZBQnLUQNW/TYfk40STk
P07A1yiG6Cg0NnZ0imJKDLL2xr8zeXAkz1Fg1k2MwSgWF21iEv4VJ4rvdVPZqjKjHeEB
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;
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+1mG290ok9isKdbBEUFyXeLGcav8=;
h=X-UI-Sender-Class:From:To:Subject:Date;
b=Aa+12hhvURcNvWVV/paUqyD4NoUgtPACHFynDjo25h4baivnVP5yajrGQjhVYE79
frAaSFrmLH1sbVoSpV5leBLz4W6ly8d85xBvcW1jDzaQJJ2AhxwsYRB07Y/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>
From: Pam Don <pamdon901@mail.com>
To: jdondon109@gmail.com, jdondon109@protonmail.com
Subject: The deadline
Content-Type: text/html; charset=UTF-8

```

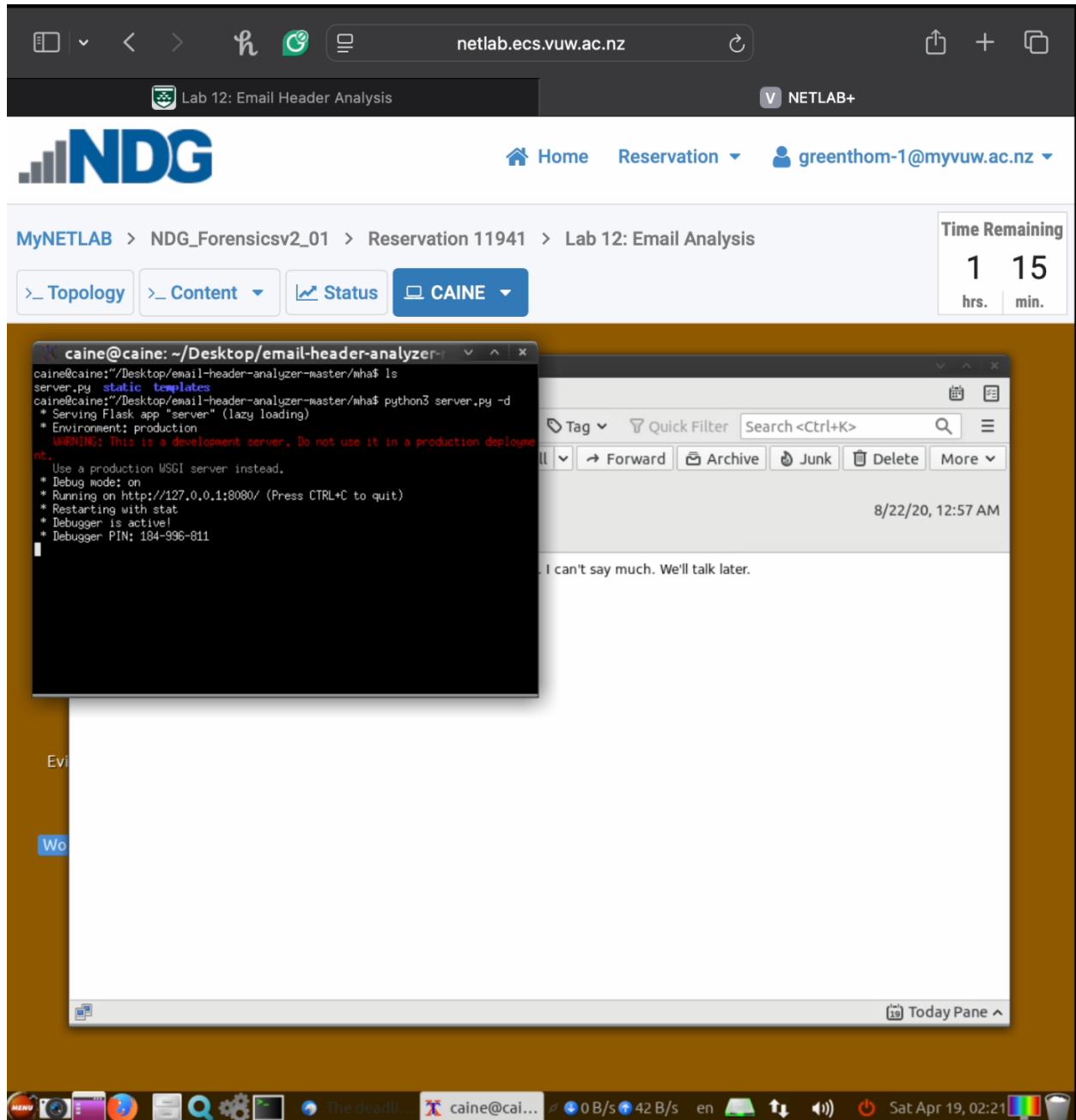
- Brief explanation (50 words max) of email authenticity based on indicators

Email appears authentic based on multiple SPF and DKIM pass results. The domain [pamdon901@mail.com](mailto:pamdon901@mail.com) is verified as a permitted sender from IP 82.165.159.131, indicating the message likely originated from an authorized server without spoofing or tampering.

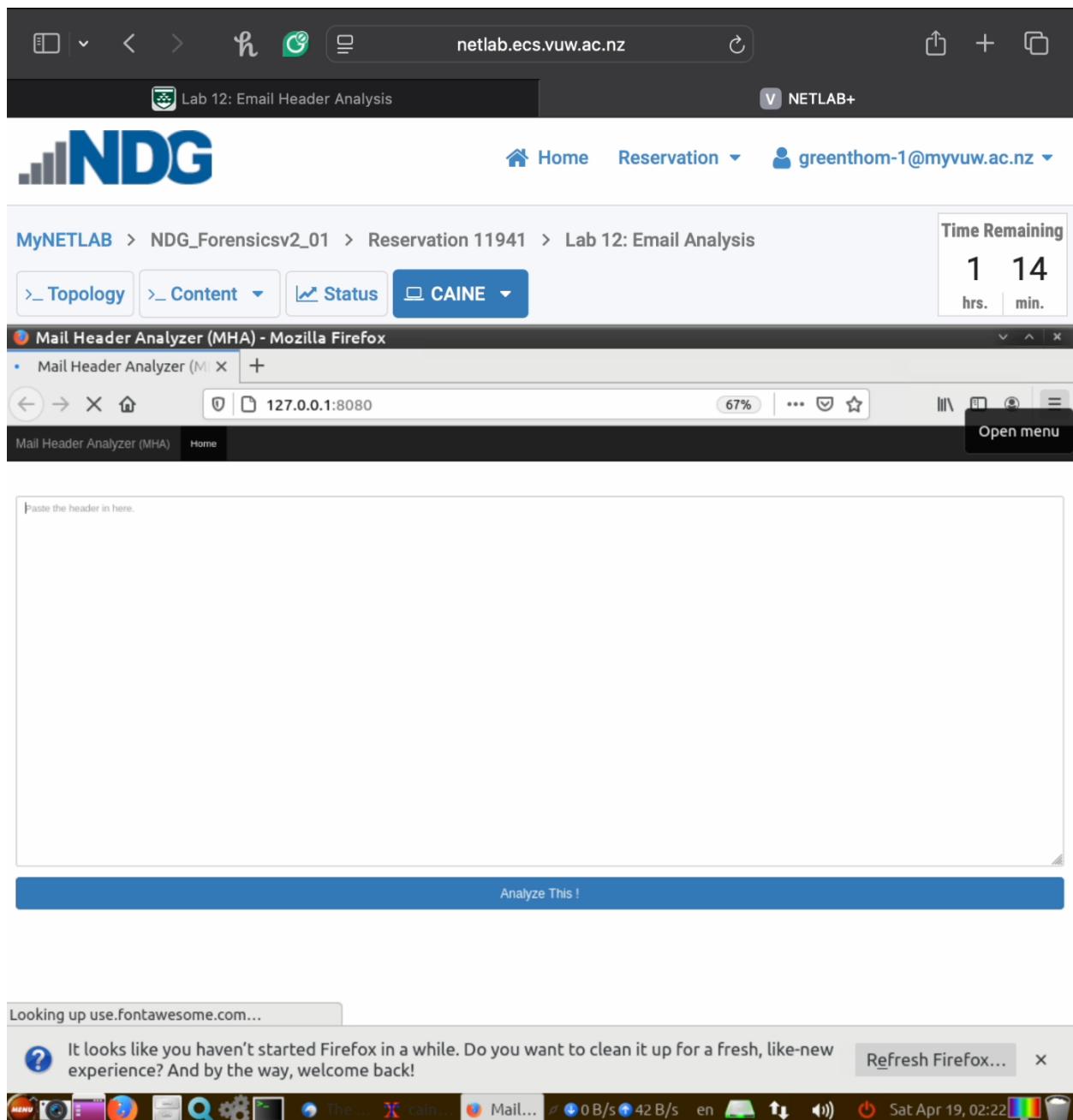
## **Part 2: Automated Email Header Analysis (20 marks)**

### **Task 4: Email Header Analyzer Setup (10 marks)**

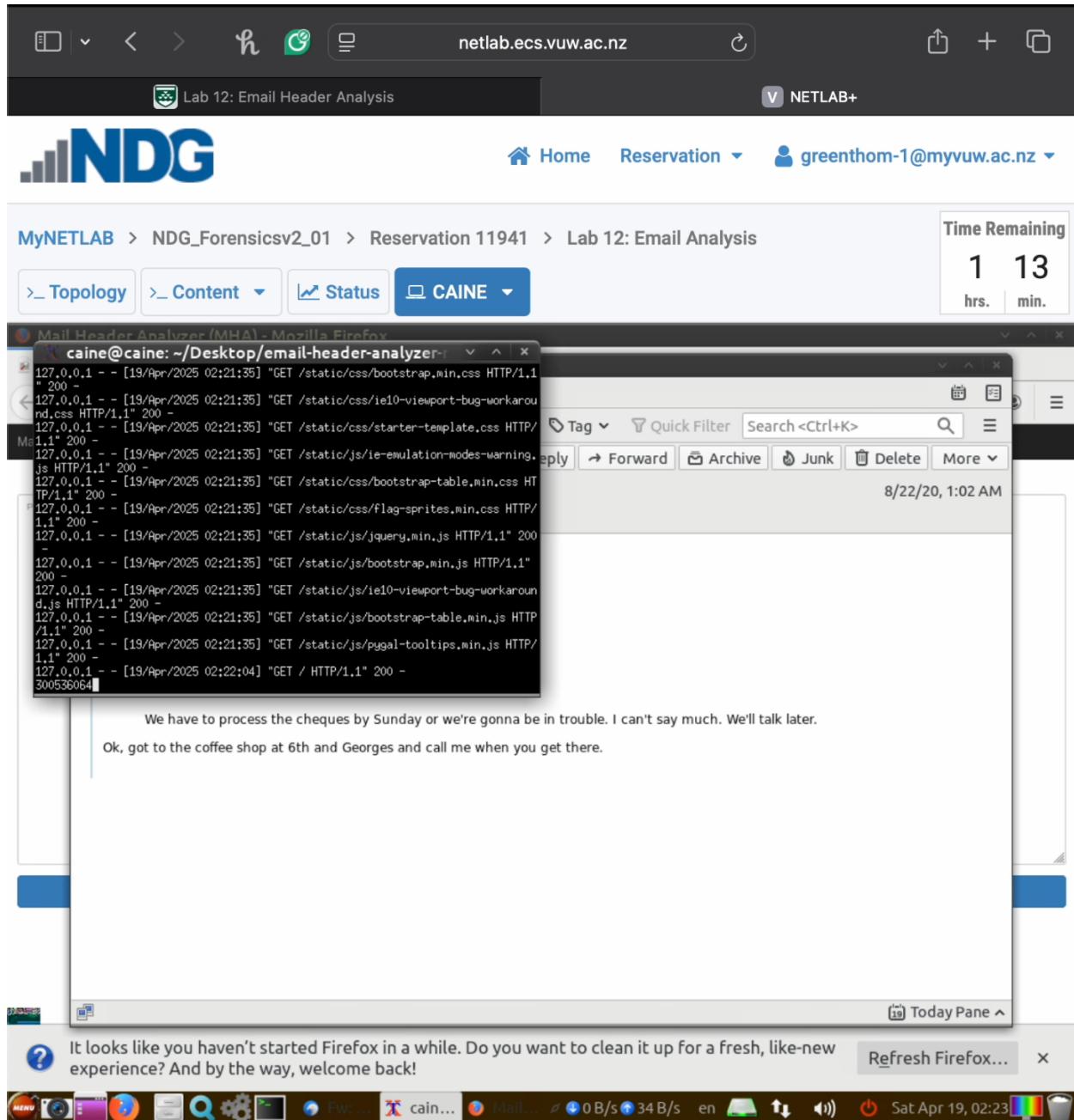
- Set up Email Header Analyzer via terminal
- Configure and run the server locally
- Launch in web browser
- Required screenshot:
  - Terminal window with server start command (step 2.2)



- **Email Header Analyzer interface in browser (step 1.7)**



- Your student ID visible in terminal prompt or as added note



### Task 5: Automated Analysis (10 marks)

- Extract the header from the email with subject “Fw: Re: The deadline” in Thunderbird
- Analyze using Email Header Analyzer focusing on:
  - Email servers and IP addresses in communication chain
  - Time delays between servers
  - Authentication results
- Required screenshots (multiple views from step 1.13):

- Email Header Analyzer results path visualization (step 1.13)

MyNETLAB > NDG\_Forensicsv2\_01 > Reservation 11941 > Lab 12: Email Analysis

Time Remaining  
1 06 hrs. min.

Topology Content Status CAINE

Mail Header Analyzer (MHA) - Mozilla Firefox

Mail Header Analyzer (M) 127.0.0.1:8080

Subject: Fw: Re: The deadline  
Message-ID: <trinity-1bab2f8-878b-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

Delay in seconds.

By: 2002:ab3:5191:0:0:0:0 From: mout-xforward.gmx.com (mout-xforward...  
From: [174.128.225.186] ([174.128.225.186])

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	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="qvyyg55/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="qvyyg55/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=7bnyXgGi+UqA+yX7xrml6syppghDBO0em50bauyFB=; h=X-UI-Sender-Class:From:To:Subject:Date:References; b=qvyyg55/GMGAJ3pUQj0wf1pNT22ndjhNcZG3+d4UpGy7K6wLyXxU02Lc9s9z1Hv +L6BMGwotyVC7WcpLhugRt4EUDCcbNjTSZeV6javxfqpjJwhOWWdQmpVz1ZY/sA8 xf7x6BjyjQTxChzMc4p1EEP8QZZZP1Ob4nDLBS48=

Email passed through 3 main hops:

- [174,128,225,186] originating from web-mail.mail.com (3c-app-mailcom-lxa10.server.lan)
- [82.165.199.131] -> passed through mout-xforward.gmx.com
- [2002:ab3:5191:0:0:0:0] -> received by mx.google.com

Total delay is 1 second, which occurs being hop 1 and 2 during the ESMTP stage from sender's mail server to the forwarding relay.

- Parsed authentication results section (step 1.13)

Subject: Fw: Re: The deadline  
 Message-ID: <trinity-1bab28f-878b-4165-b9d8-31ebb36a7bf-1598072579355@3c-app-mailcom-ixat10>  
 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

Delay in seconds.

By: 2002:ab3:5191:0:0:0:0  
 From: mout-xforward.gmx.com (mout-xforward...  
 From: [174.128.225.186] ([174.128.225.186])

Hop	From	By	With	Time (UTC)	Delay
1	[174.128.225.186] ([174.128.225.186])	web-mail.mail.com (3c-app-mailcom-ixat10.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		08/22/2020 05:03:00 AM	1 sec
3		2002:ab3:5191:0:0:0:0		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=qvyg55/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=qvyg55/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+yX7xrm1L6syphbDBODem50bawyF8=; h=X-UI-Sender-Class:From:To:Subject:Date:References; b=qvyg55/GMGAJpUQjow1pnFT2zndjfncZG3+adLUpGy7K6wLyXXU0ZLc9sI9z1Hv+L6BMGwotyVC7WcpLhugRq4EUDCbnjTSZeV6javxfqxpjJwh0WWdQmpVz1ZYlsA8=xf7x6BjyieQTxChzMu4p1EPBQZZZP1ObdnDLBS48=

1. Received-SPF: pass, IP 82.165.159.131 is authorized to send on behalf of [pardon901@gmail.com](mailto:pardon901@gmail.com).
2. DKIM-Signature (DomainKeys Identified Mail): Email was cryptographically signed using the sending domain -> SHA256.
3. Authentication-Results: 'dkim=pass....spf=pass'. Alignment and policies are validated correctly.

4. ARC-Authentication-Results: 'i=1; mx.google.com; dkim=pass', shows all key authentication checks passed at the first hop.

- Your student ID visible in screenshot (can be added as a note or overlay)

MyNETLAB > NDG\_Forensicsv2\_01 > Reservation 11941 > Lab 12: Email Analysis

Time Remaining  
1 06 hrs. min.

**Mail Header Analyzer (MHA) - Mozilla Firefox**

Mail Header Analyzer (MHA) x +

300536064

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	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=qvygSS/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=qvygSS/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=7bnjXgGi+UqA+yX7xm1L6syqghbDBODem50bauyF8=; h=X-UI-Sender-Class:From:To:Subject:Date:References; b=qvygSS/GMGAJpUQjw1pNt22ndjNcZG3+Ad4UpGy7K6wLyXxU0ZLc9sI9z1Hv +L6BMGwotyVC7WcpLhugRq4EUDCcbNjTSZeV6javqlppjJwH0WWdQmpVz1ZY/sAxF7x6BjyQTxChzM4p1EEP8QZZZP1Ob4nDL8S48=

**X- headers**

X-Google-Smtp-Source	ABdhPjxk369/HxnaM1zexad6/YzoOjouOmWhoVDtkfry+CkAjxLdkTcl3UEvrUzL0zSvqLGr7m0
X-Received	by 2002:a92:c849: with SMTP id b9mr5410626liq.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