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.

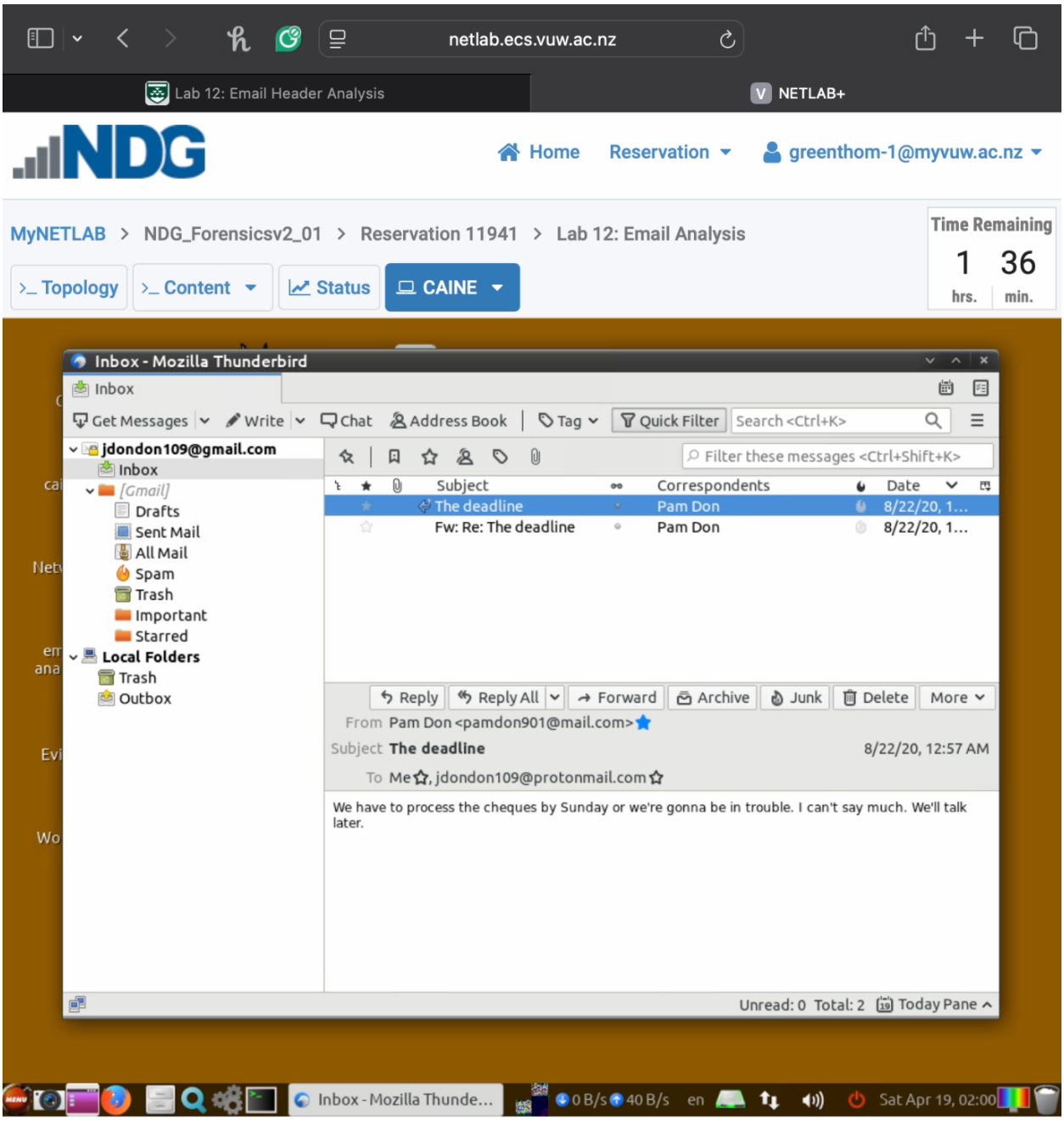
Submission Guidelines

- 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

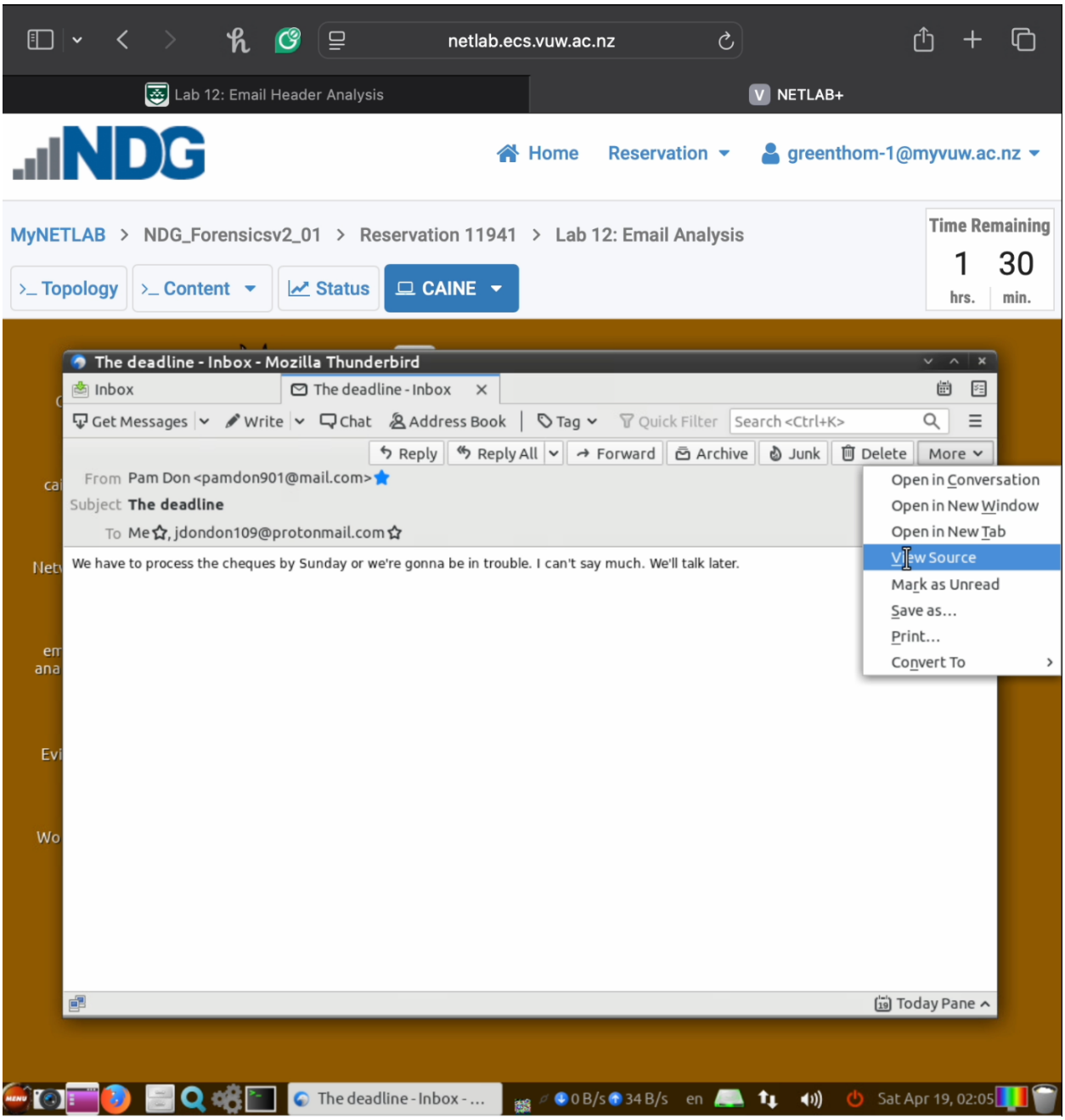
Part 1: Manual Email Header Extraction and Analysis (30 Marks)

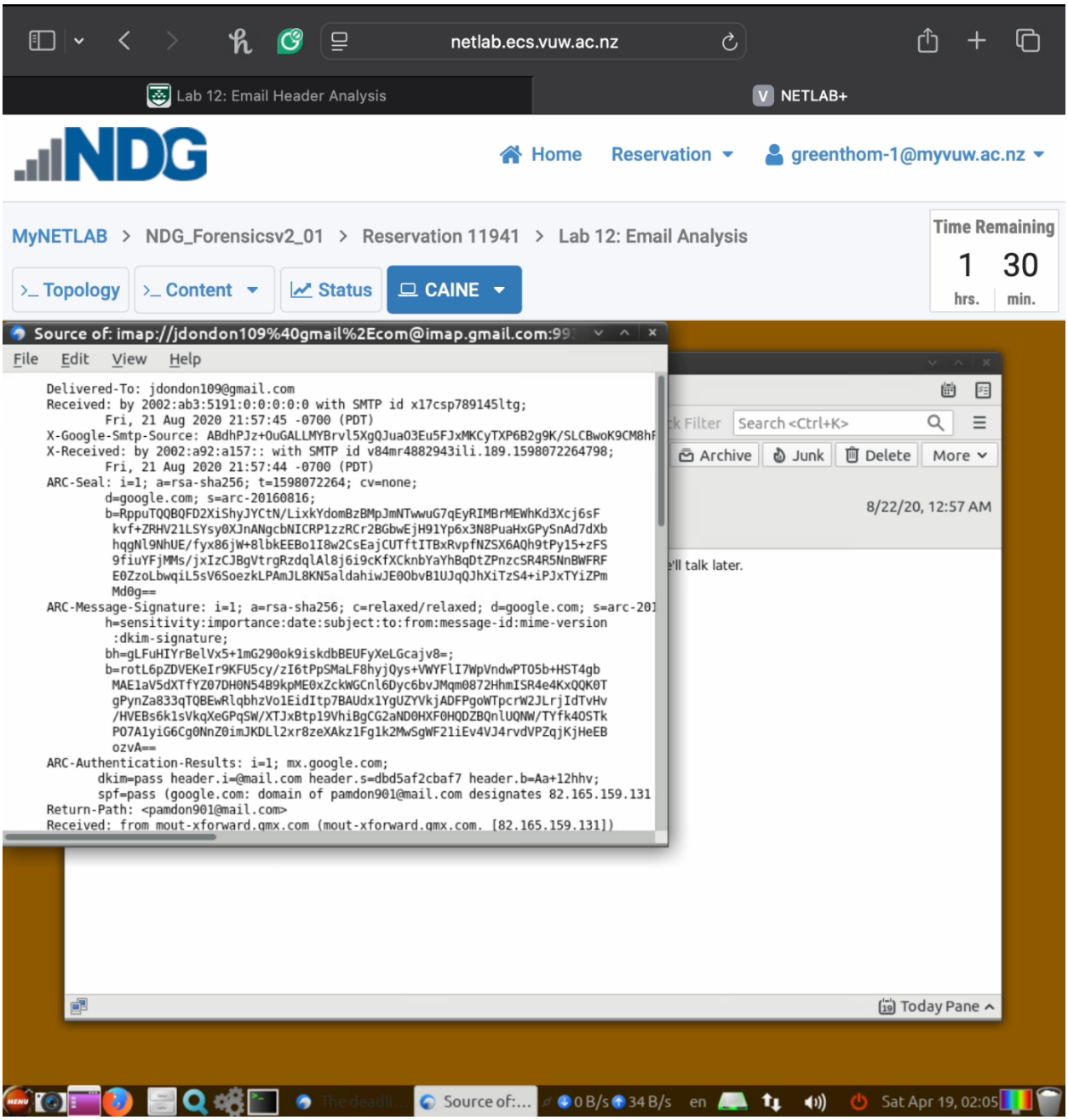
Task 1: Email Header Extraction (10 marks)

- **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)**

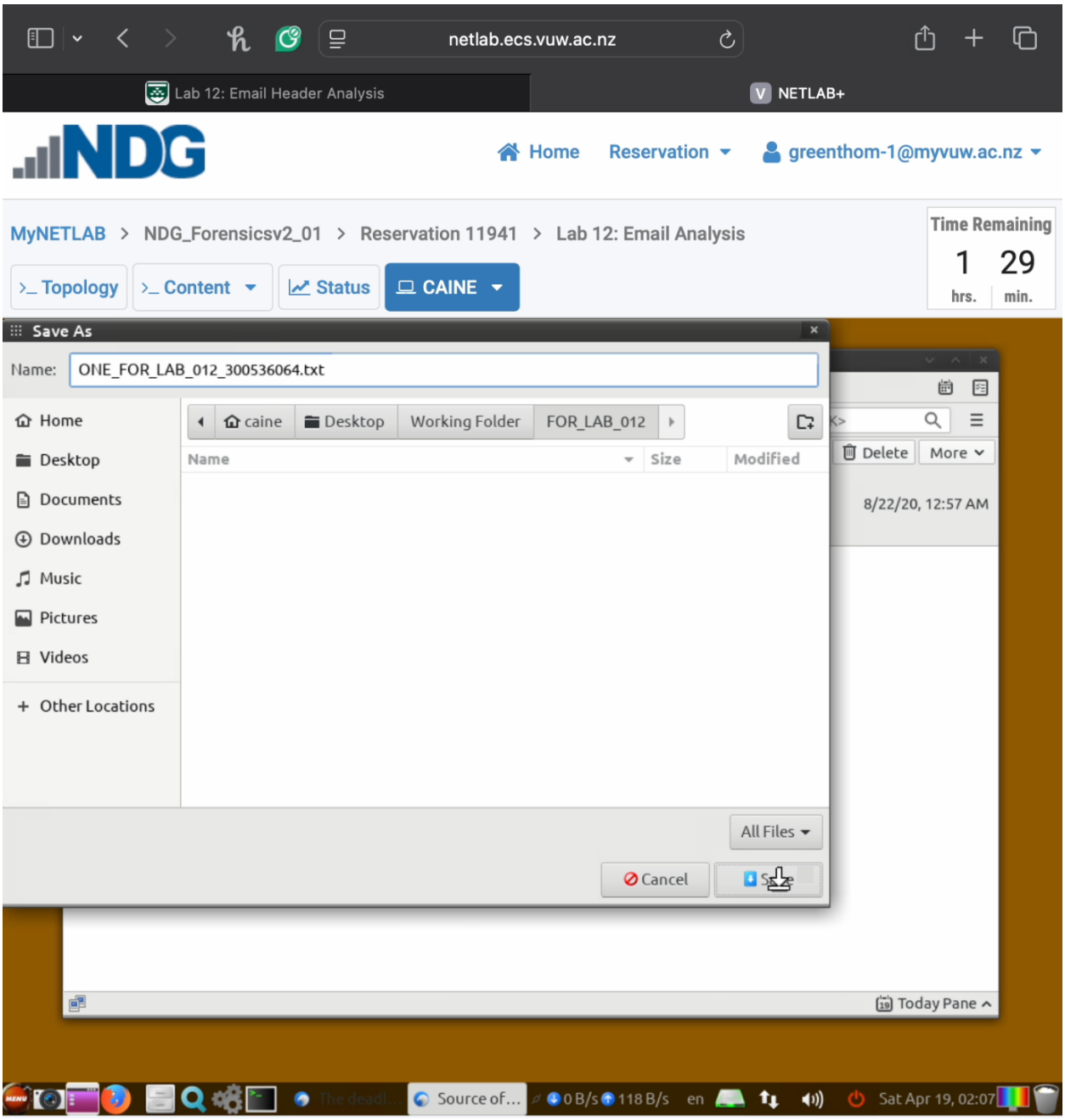


- **View Source option accessed through More menu (step 1.8)**


netlab.ecs.vuw.ac.nz
Lab 12: Email Header Analysis
NETLAB+
NDG
Home
Reservation
greenthom-1@myvuw.ac.nz
MyNETLAB > NDG_Forensicsv2_01 > Reservation 11941 > Lab 12: Email Analysis
Time Remaining
1 hrs.
30 min.
Topology
Content
Status
CAINE
The deadline - Inbox - Mozilla Thunderbird
Inbox
The deadline - Inbox
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Search <Ctrl+K>
Reply
Reply All
Forward
Archive
Junk
Delete
More
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.
Open in Conversation
Open in New Window
Open in New Tab
View Source
Mark as Unread
Save as...
Print...
Convert To
Today Pane
The deadline - Inbox - ...
0 B/s 34 B/s
en
Sat Apr 19, 02:05



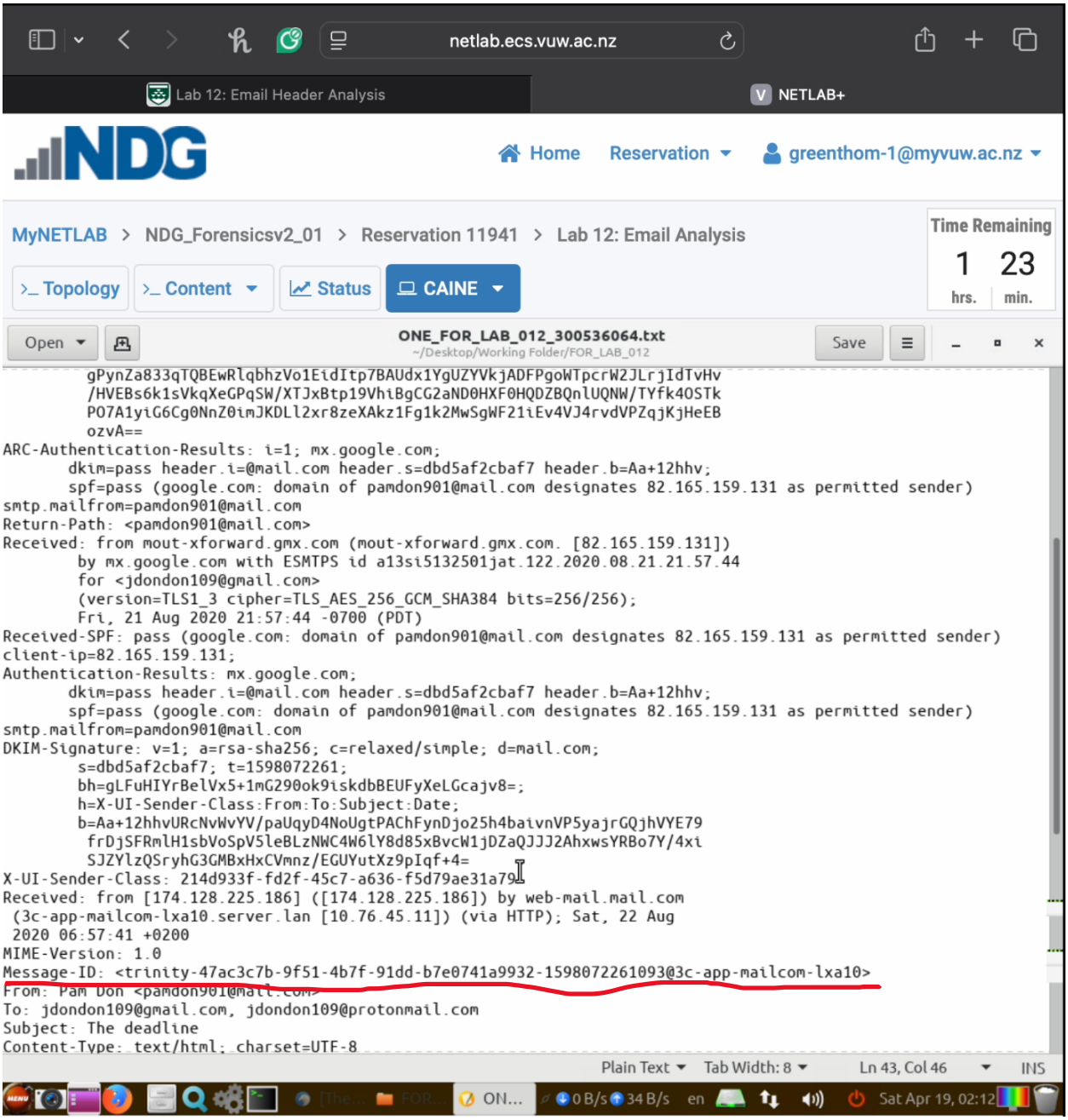
- **Saved header file in working directory (step 1.11)**



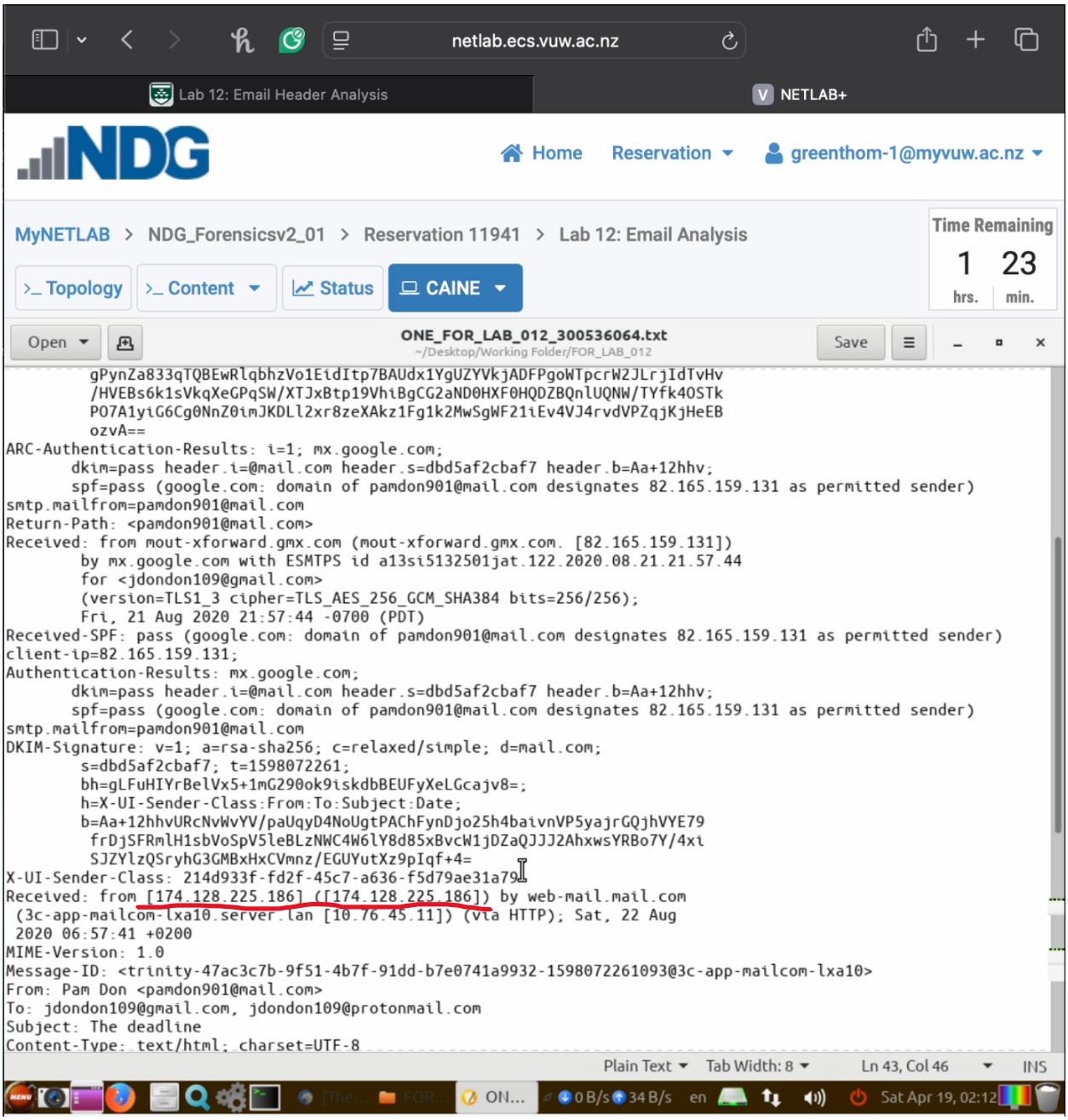
Task 2: Manual Header Analysis (10 marks)

- **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):**

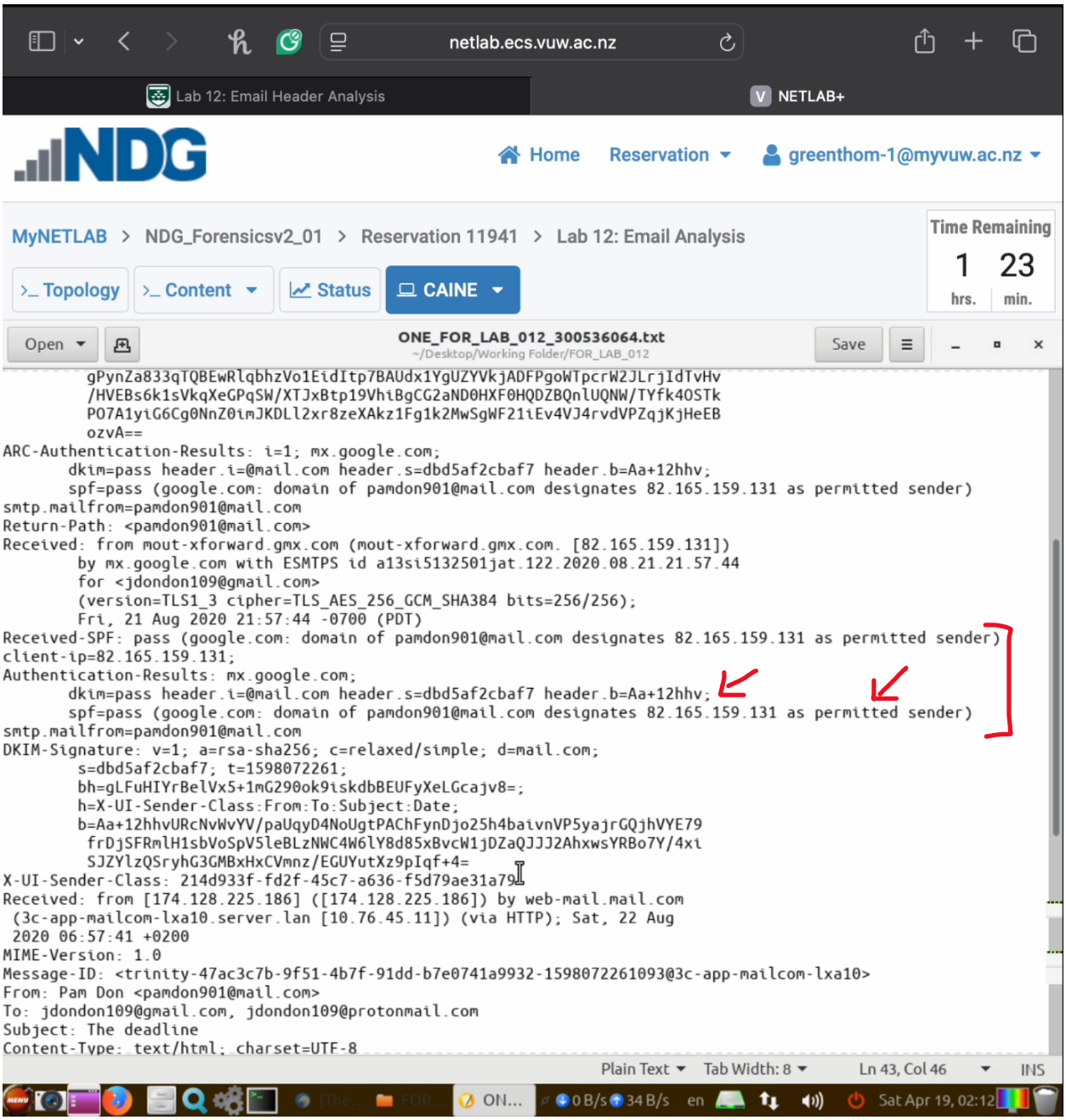
- **Header file in text editor with Message-ID highlighted (step 1.16)**



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

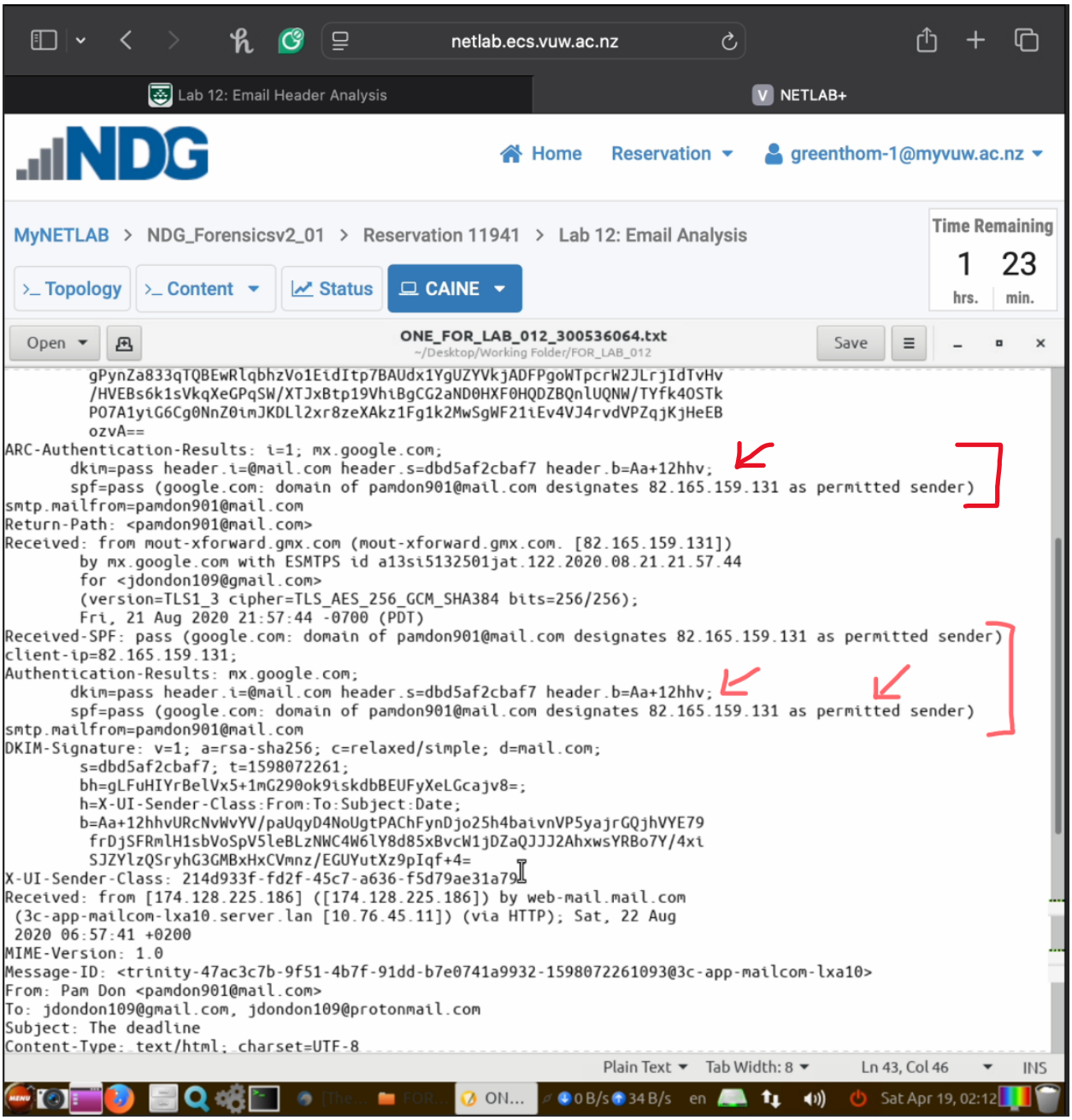


- **SPF and DKIM authentication results, if present (step 1.16)**



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)**



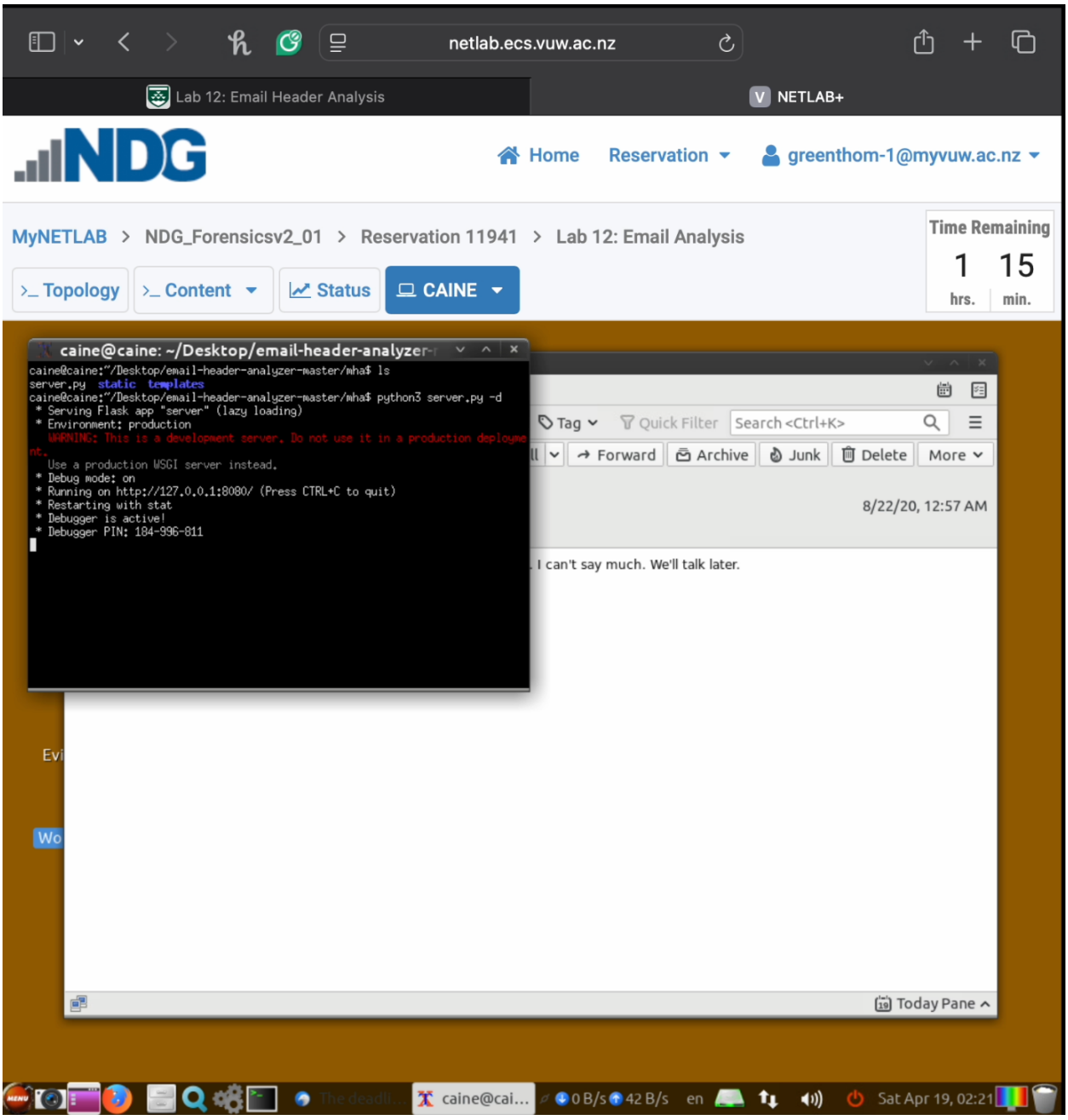
- **Brief explanation (50 words max) of email authenticity based on indicators**

Email appears authentic based on multiple SPF and DKIM pass results. The domain pandom901@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.

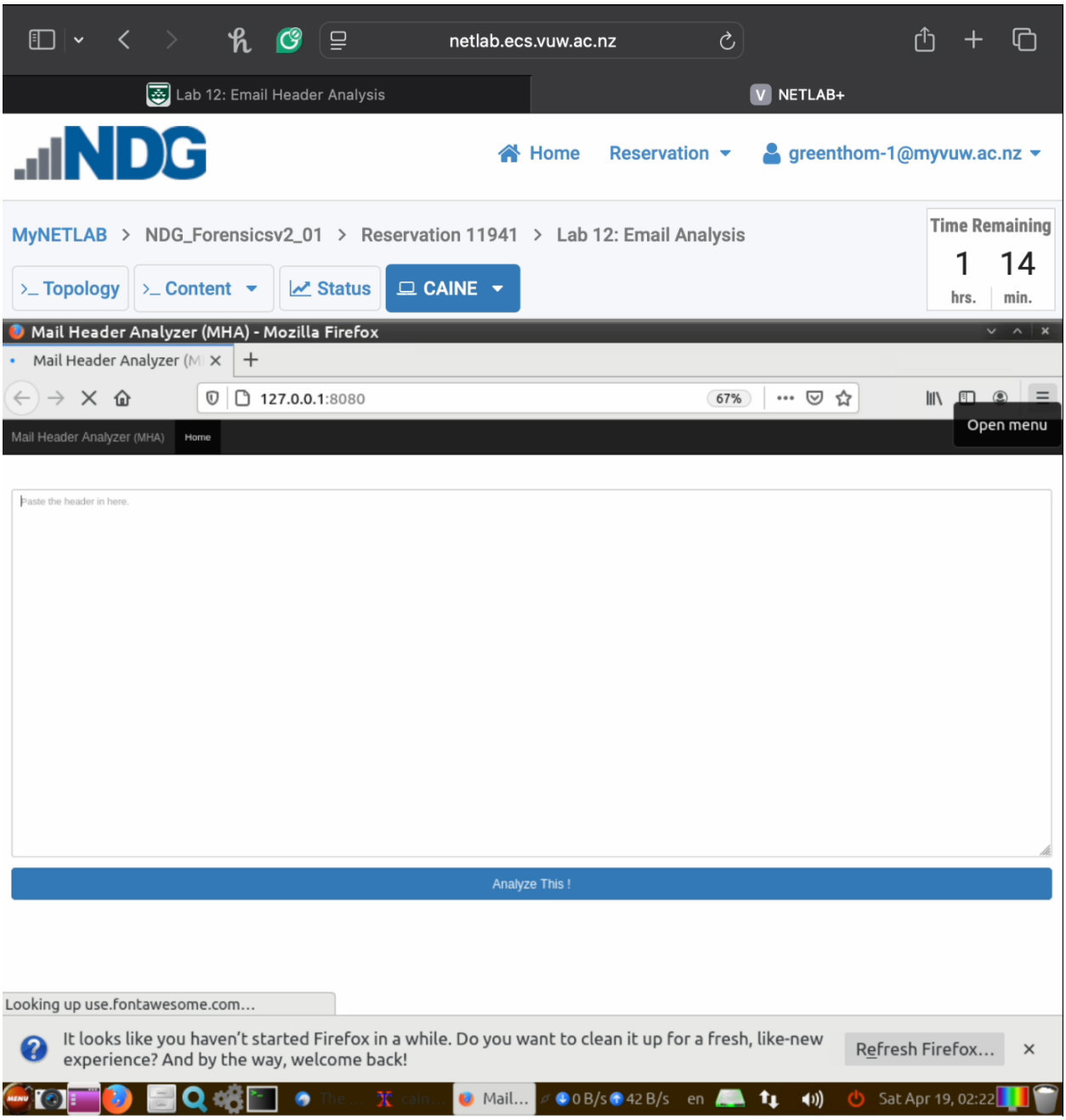
Part 2: Automated Email Header Analysis (20 marks)

Task 4: Email Header Analyzer Setup (10 marks)

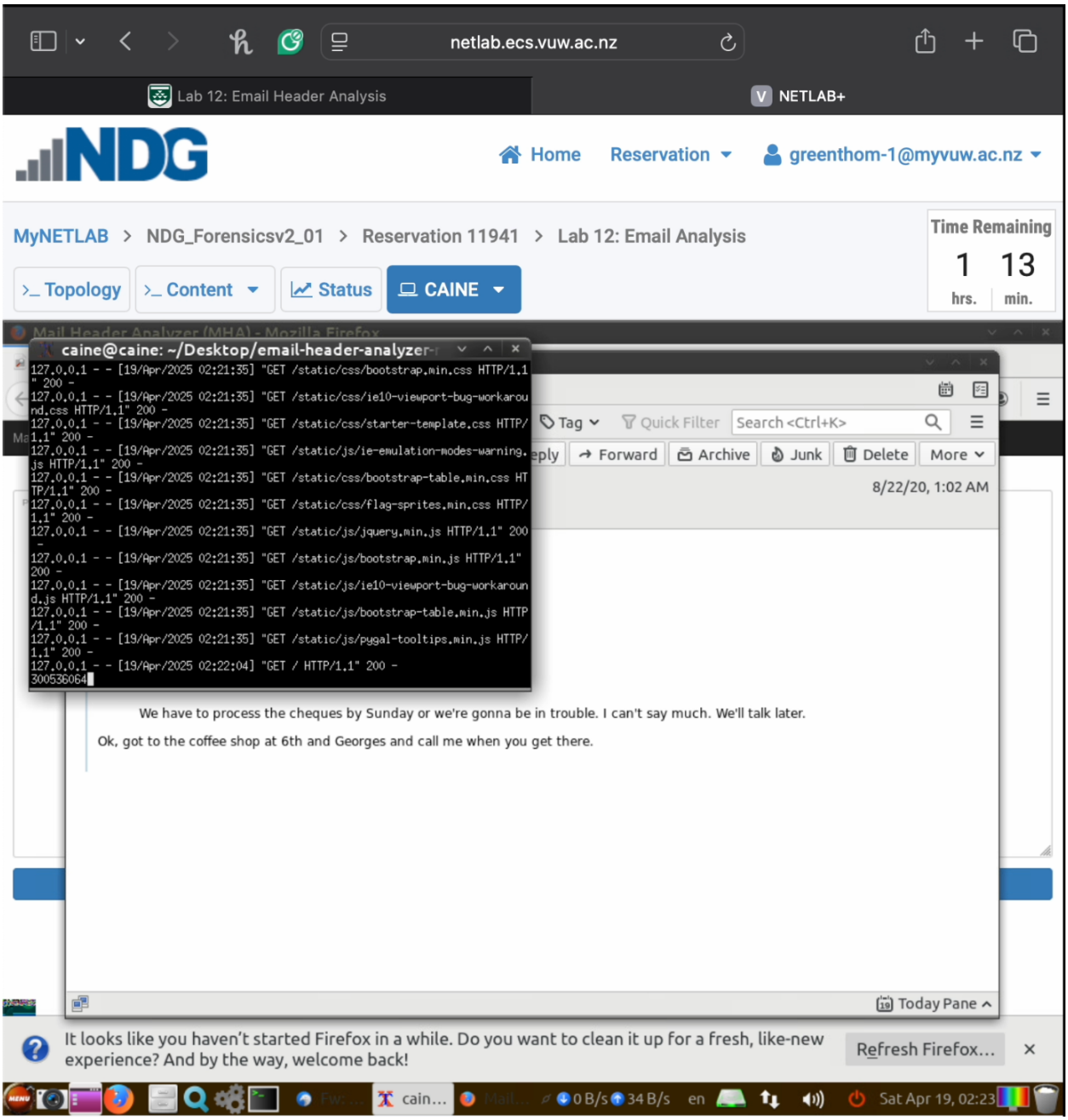
- **Set up Email Header Analyzer via terminal**
- **Configure and run the server locally**
- **Launch in web browser**
- **Required screenshot:**
    - **Terminal window with server start command (step 2.2)**



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



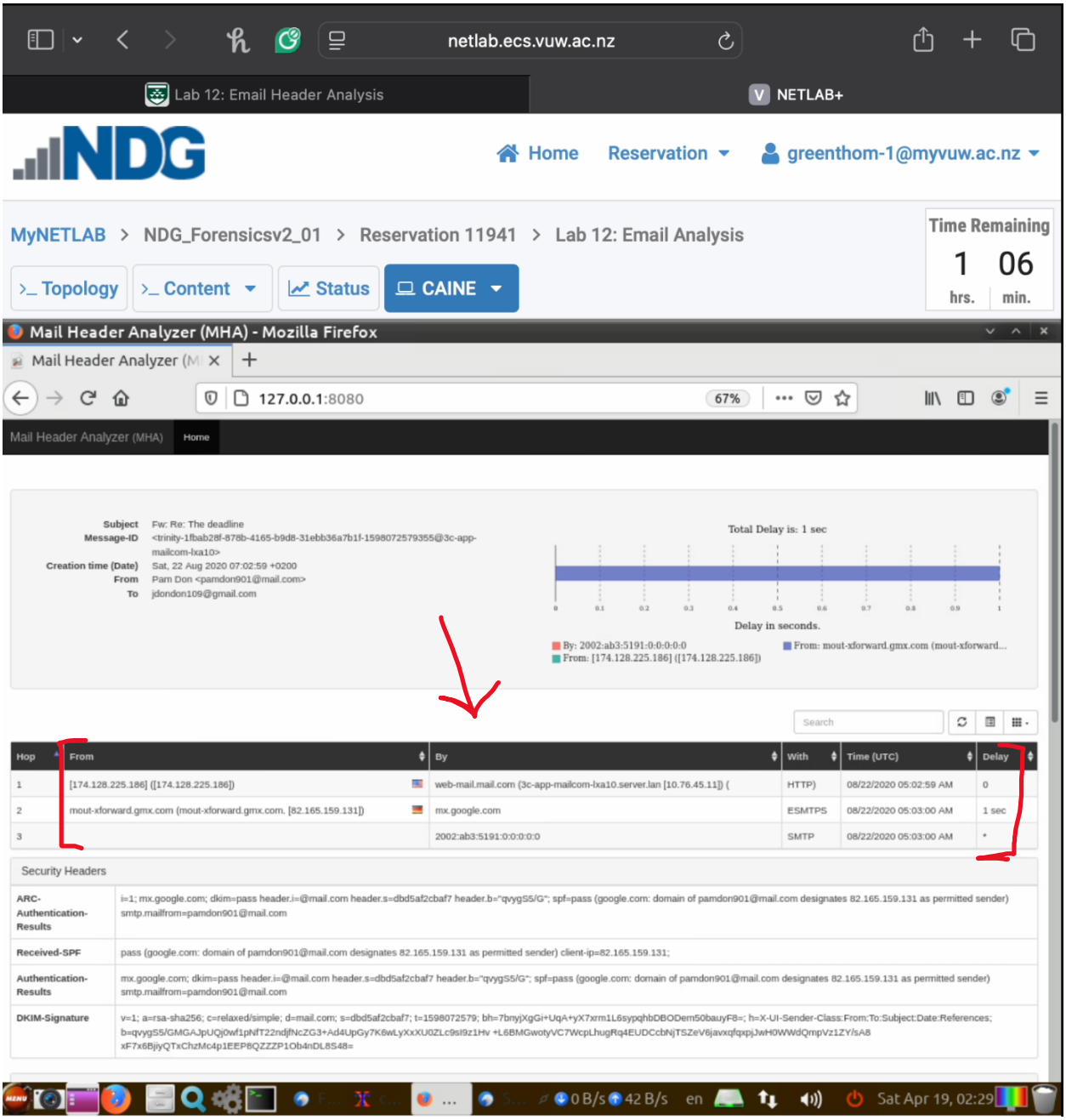
- **Your student ID visible in terminal prompt or as added note**



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)**

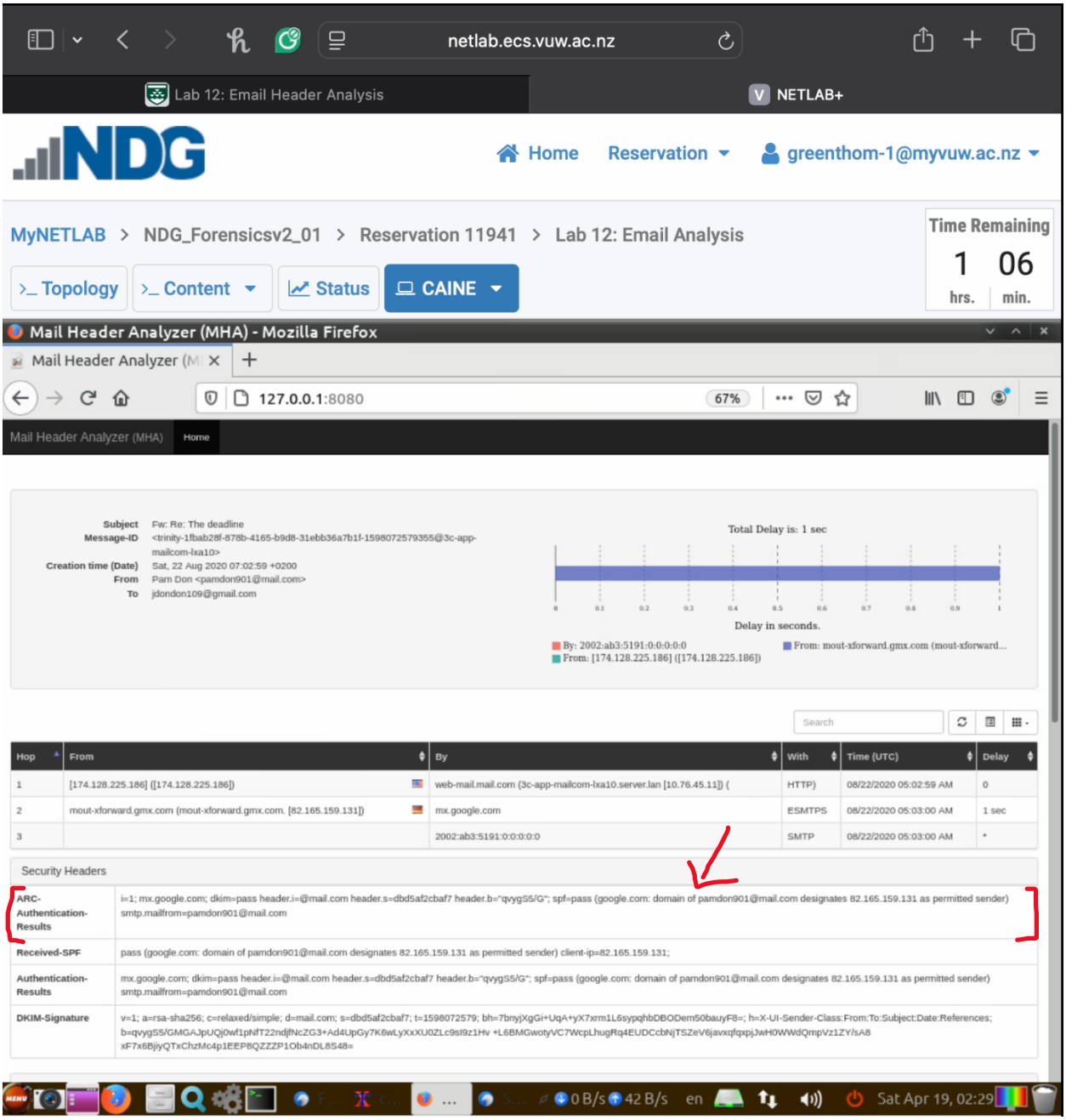


Email passed through 3 main hops:

1. [174,128,225,186] originating from web-mail.mail.com (3c-app-mailcom-lxa10.server.lan)
2. [82.165.199.131] -> passed through mout-xforward.gmx.com
3. [2002:ab3:5191:0:0:0:0:0 -> received by mx.google.com

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

- **Parsed authentication results section (step 1.13)**



1. Received-SPF: pass, IP 82.165.159.131 is authorized to send on behalf of parndon901@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)**