CYBR472 Lab 13: Internet Browser Forensics
greenthom – 300536064

Assessment Overview

This lab assesses your browser forensics skills through the analysis of web browser artifacts from different browsers. You will reconstruct user activities, identify visited websites, and establish timelines using metadata. This lab is worth 6% of your course grade.

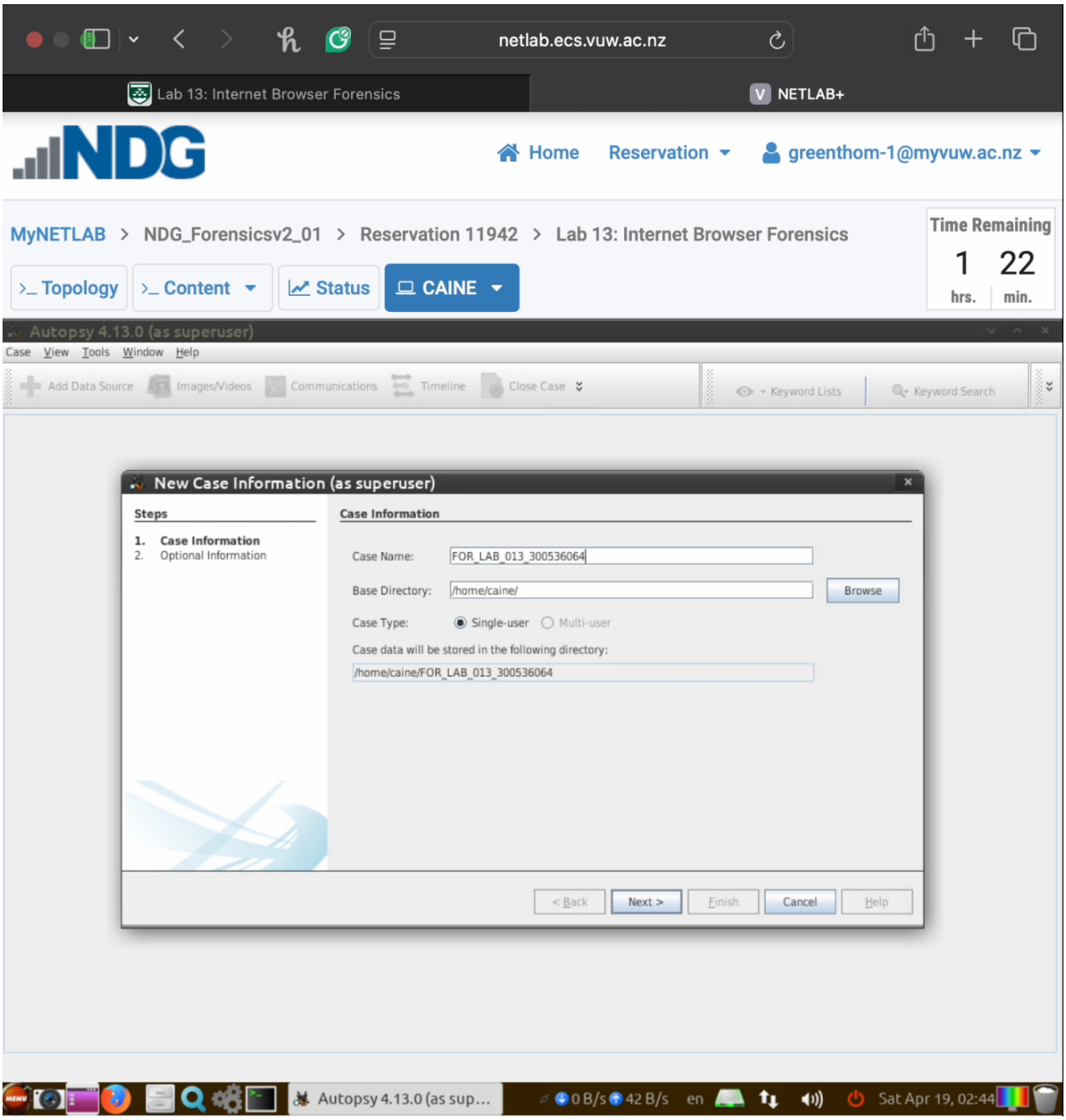
Submission Guidelines

- 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

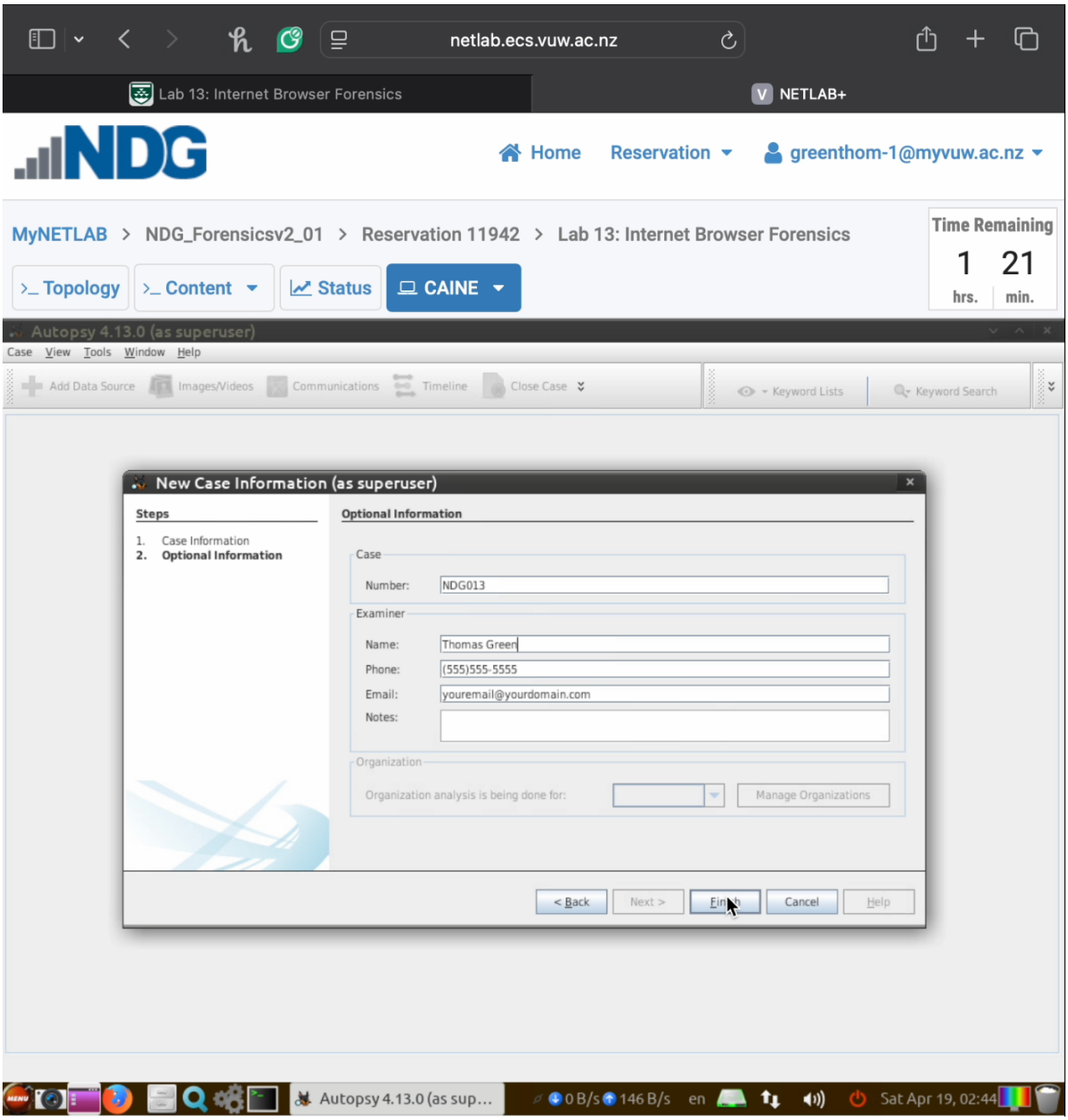
Part 1: Google Chrome Browser Forensics (30 marks)

Task 1: Autopsy Case Creation and Chrome History Database Analysis (10 marks)

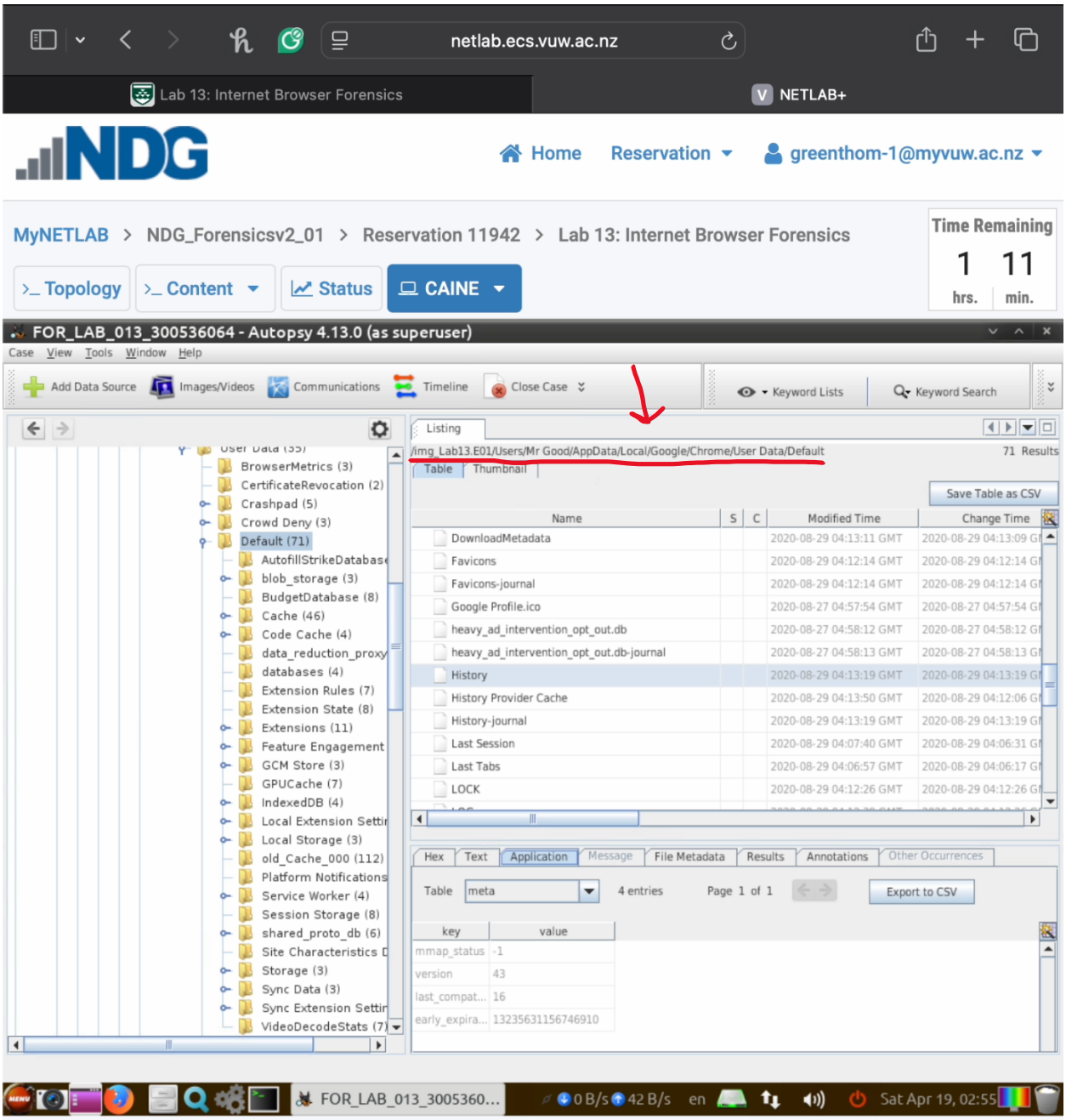
- **Launch Autopsy and create a new case named "FOR_LAB_013_[your student ID]"**
- **Enter your full name as the examiner in the Optional Information window**
- **Add the provided Lab13.E01 evidence file as your data source**
- **Enable only the Recent Activity ingest module**
- **Locate the Chrome History database file in the appropriate user profile folder**
- **Include the Autopsy title window showing case name in screenshots**
- **Required screenshots:**
    - **New Case information window with your student ID in the case name (step 1.4)**



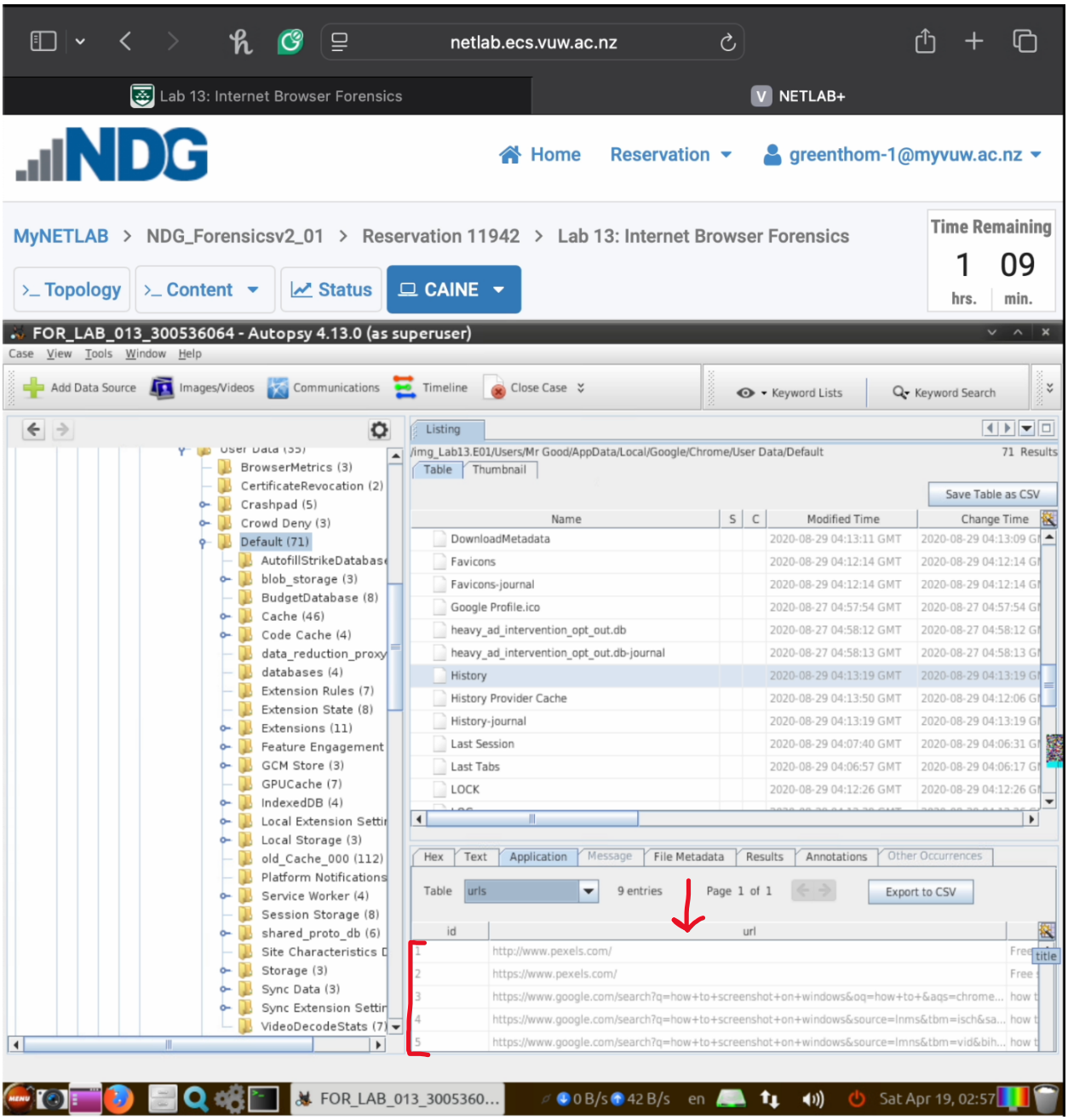
- **Optional Information window with your name as examiner (step 1.5)**



- **File path to the Chrome History database (step 1.15)**

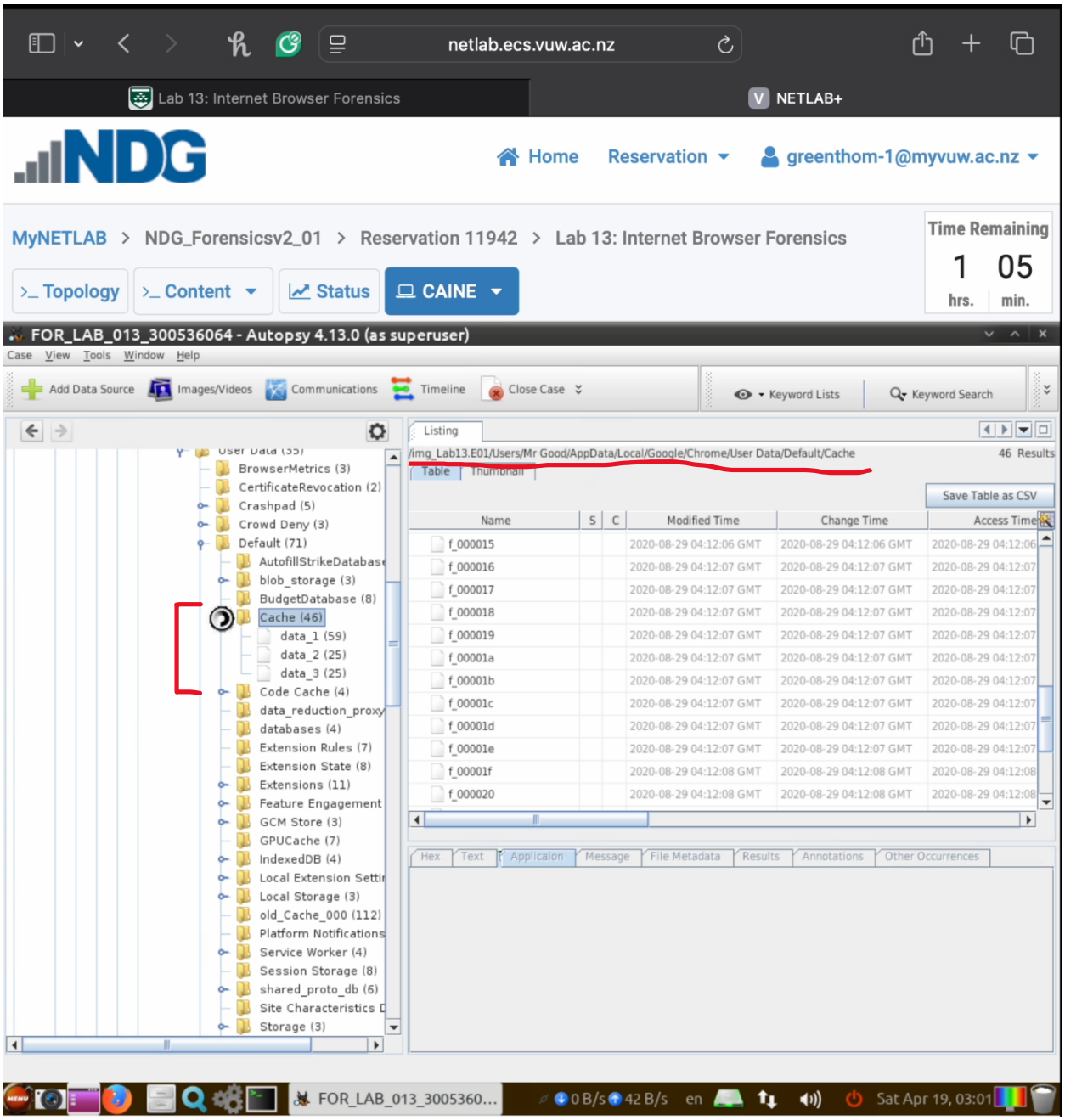


- **URLs table contents with visited websites highlighted (step 1.17)**

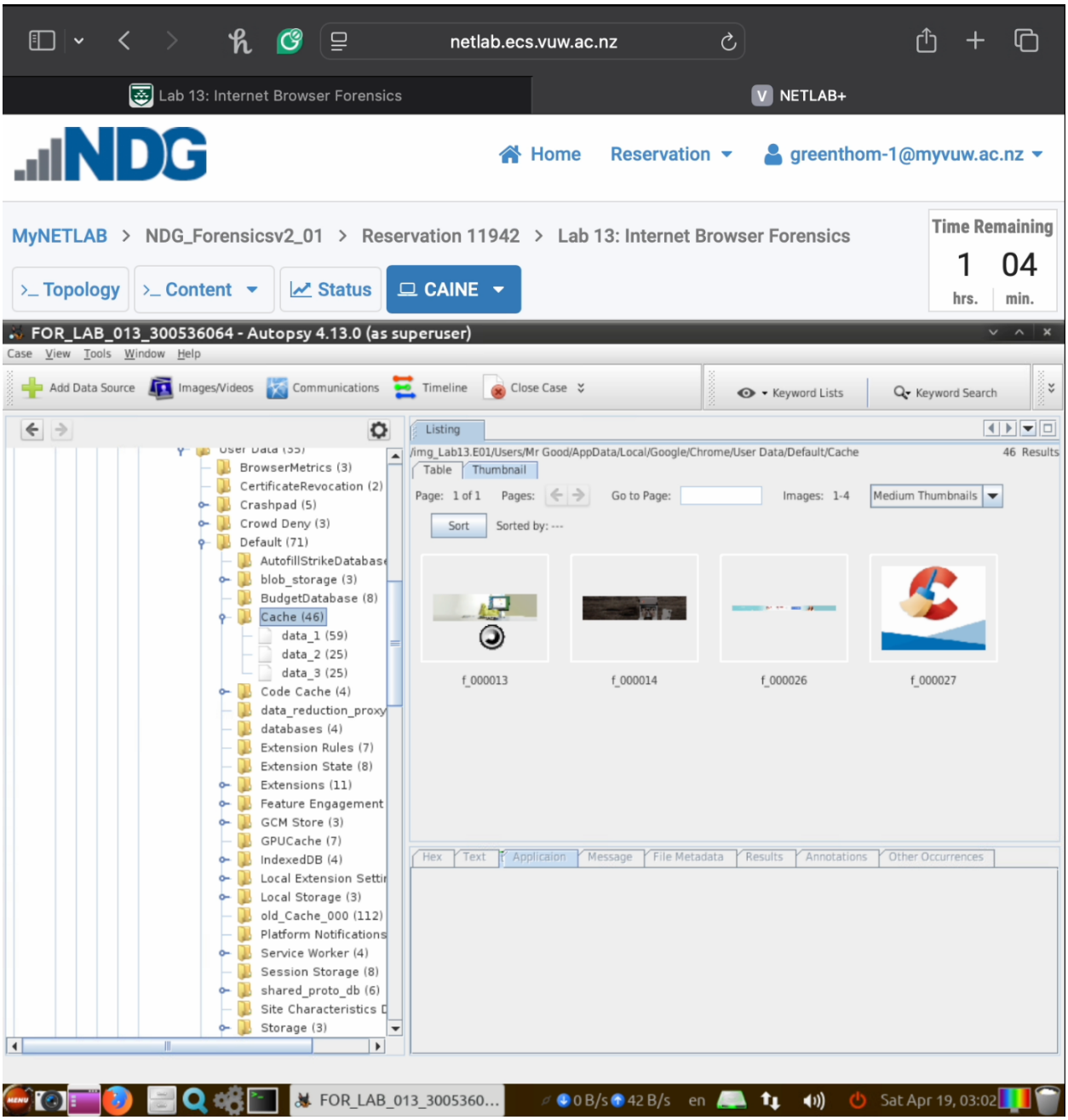


Task 2: Chrome Cache Analysis (10 marks)

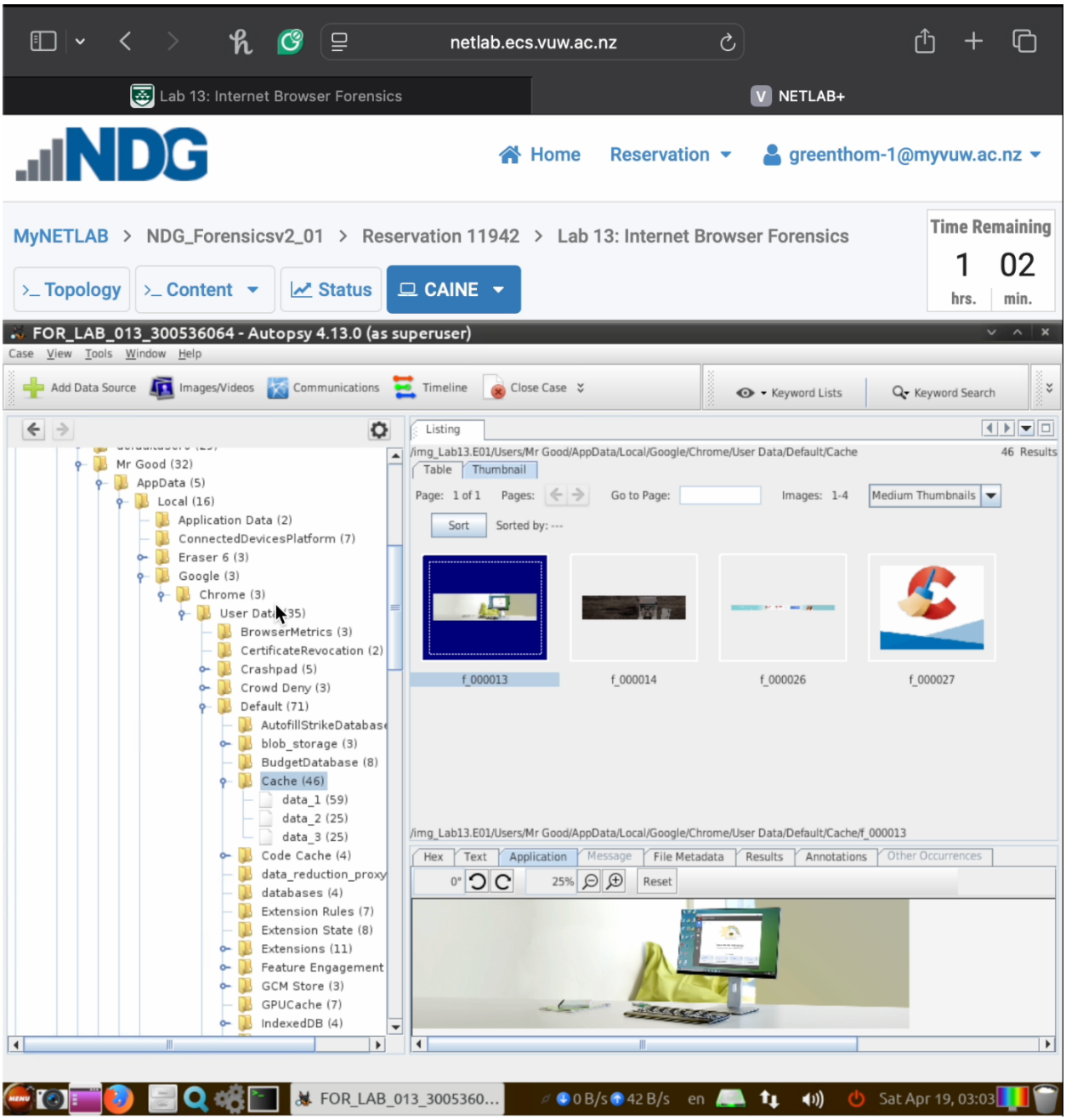
- **Navigate to the Chrome Cache folder in the user's profile**
- **Examine cached content using thumbnail view**
- **Identify a cached image**
- **Include the Autopsy title window showing case name in screenshots**
- **Required screenshots:**
    - **Chrome Cache folder location (step 1.27)**



- **Thumbnail view of cached content (step 1.28)**

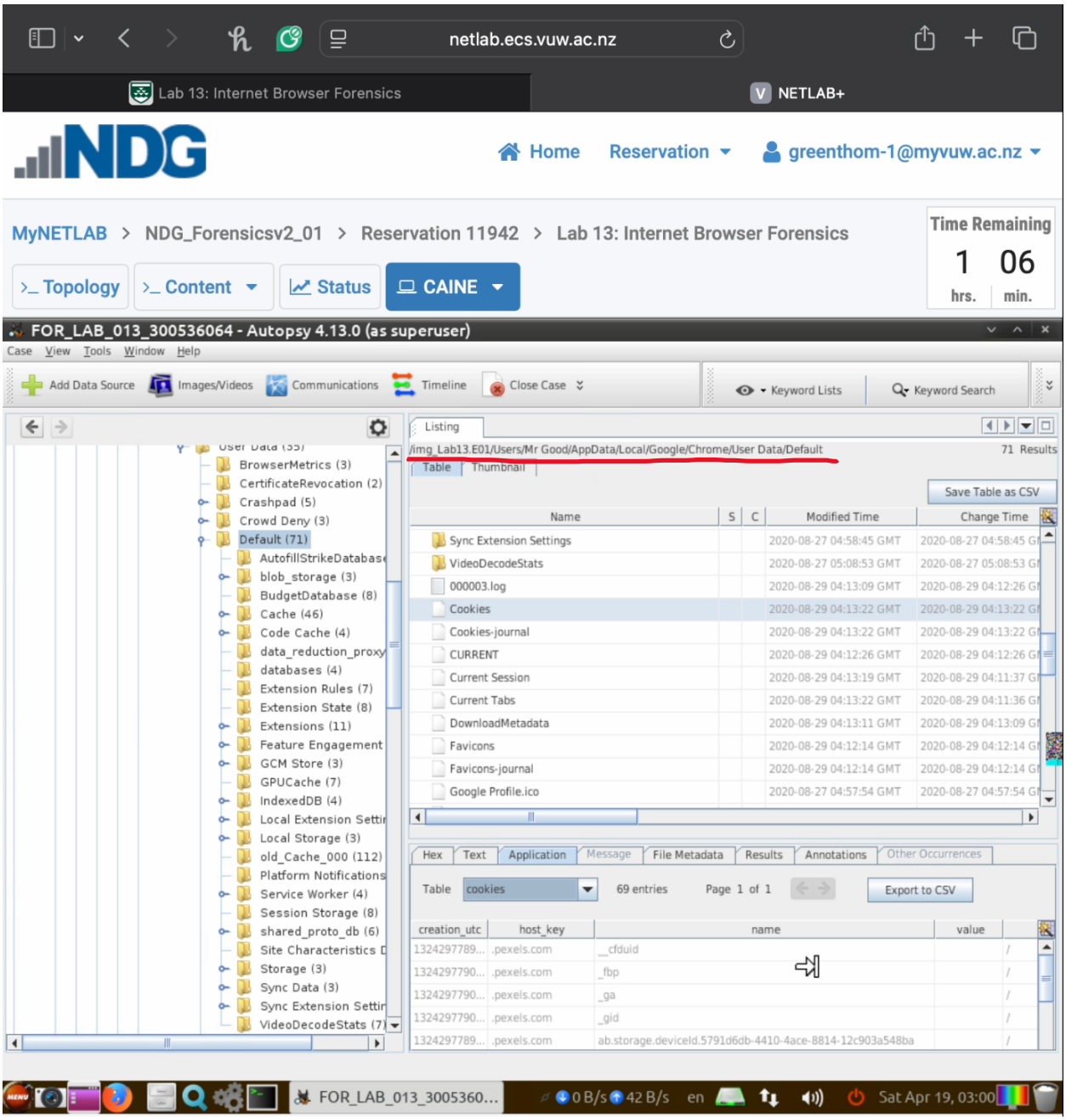


- **A selected cached image in full view (step 1.28)**

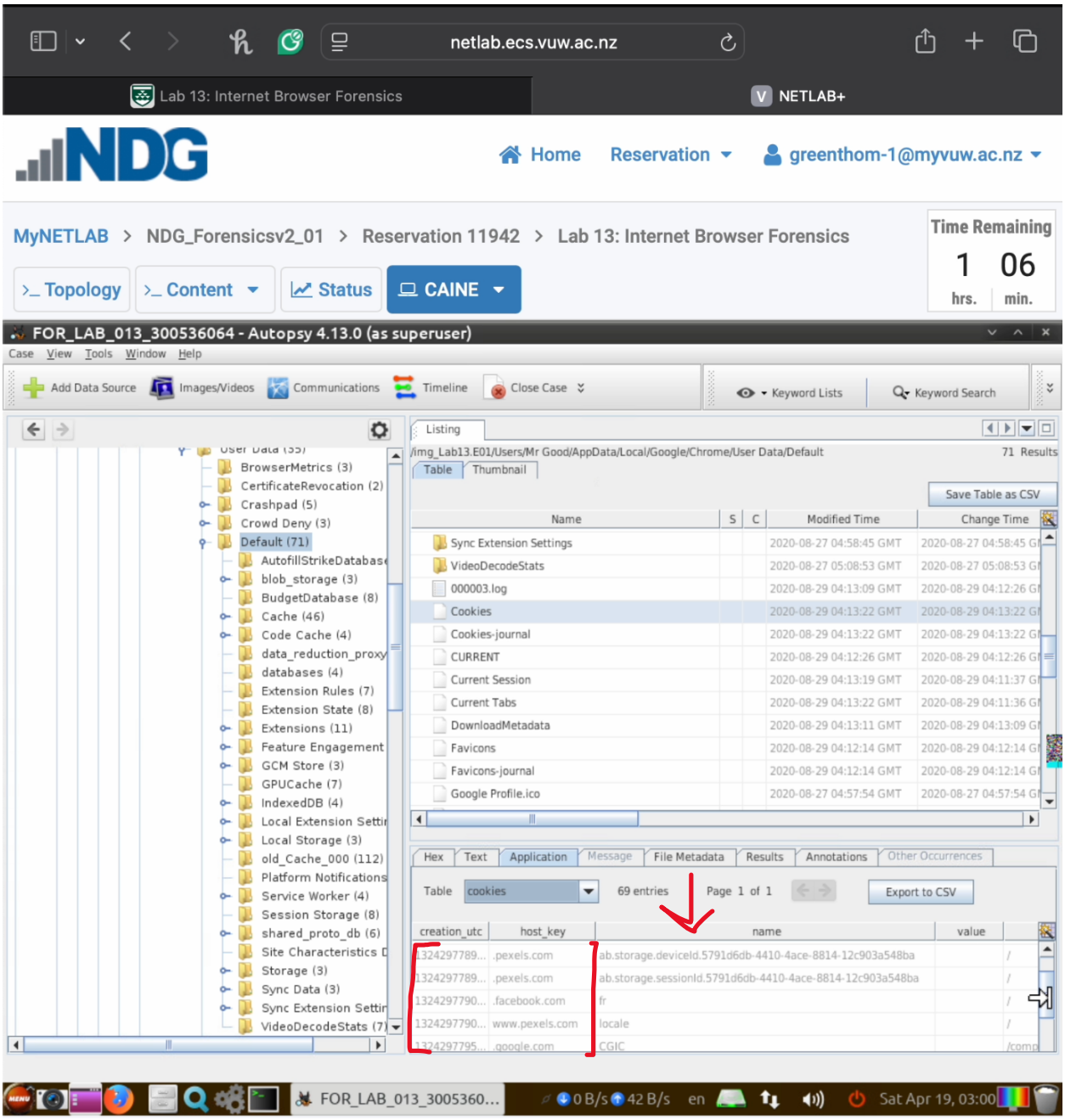


Task 3: Chrome Cookies Analysis (10 marks)

- **Locate the Chrome Cookies database in the user's profile**
- **Identify website-specific cookies and their properties**
- **Document cookie creation and expiration timestamps**
- **Include the Autopsy title window showing case name in screenshots**
- **Required:**
    - **Screenshot of Cookies database location (step 1.24)**



- **Screenshot of cookies table with domain information highlighted (step 1.25)**



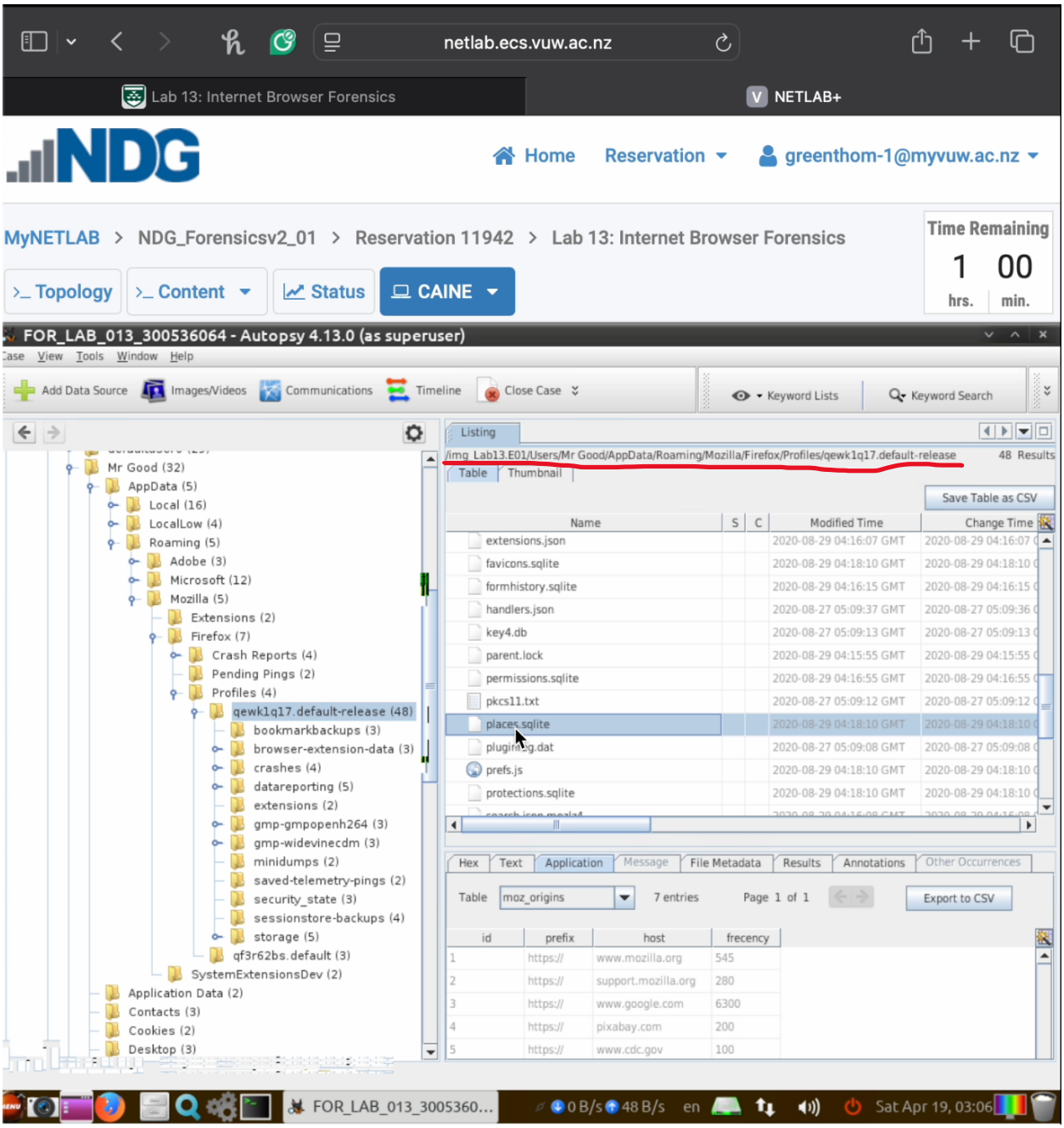
- **Brief explanation (50 words max) of what the cookies reveal about browsing activity**

The cookies show the user accessed sites like pexels.com, facebook.com, and google.com. Stored data like session IDs and user preferences indicate repeated visits, searches, or logins, revealing patterns of browsing activity. Cookies store session data, authentication tokens, or user preferences, indicating activity and login states across browsing sessions.

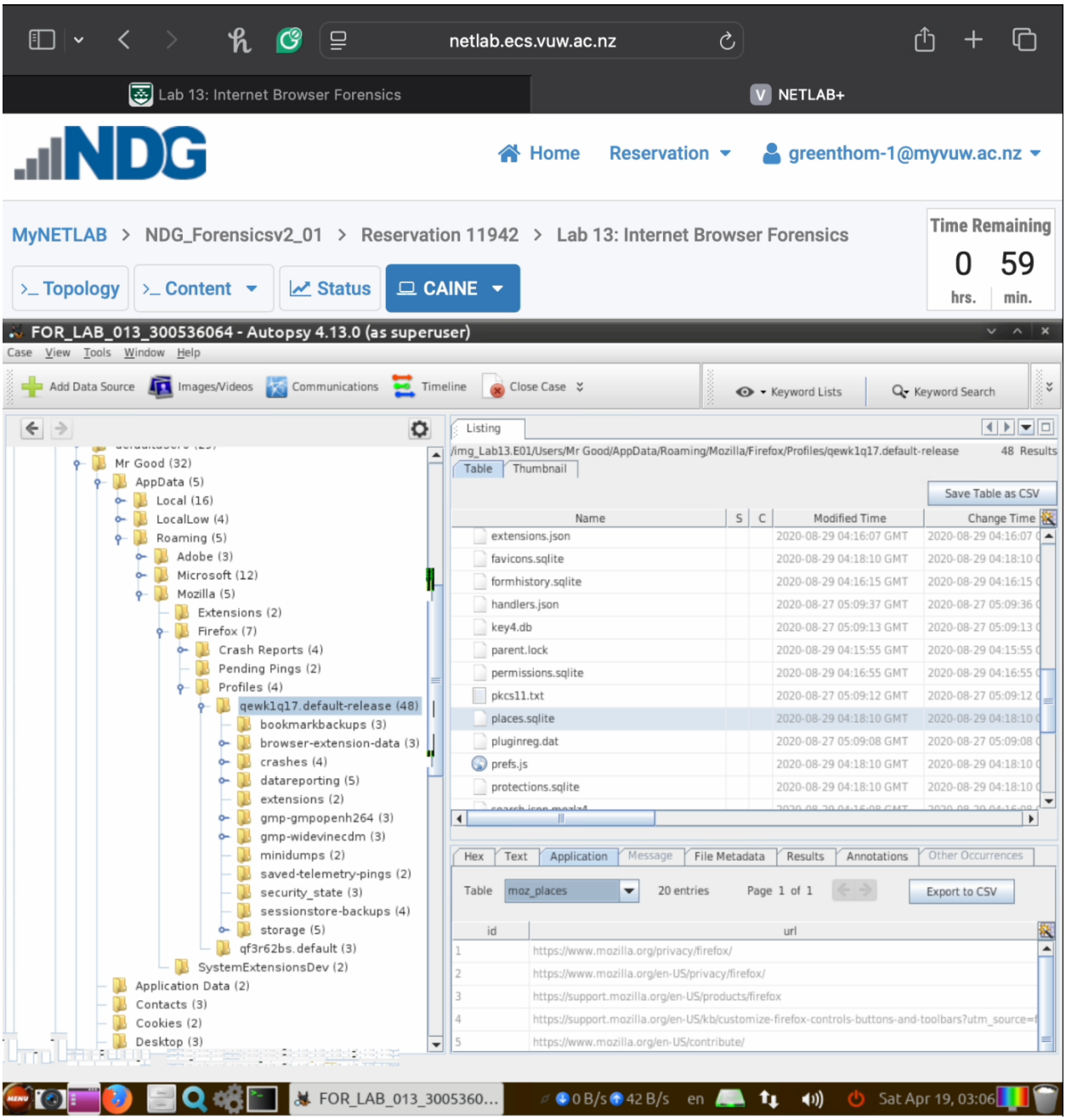
Part 2: Firefox and Internet Explorer Browser Forensics (20 marks)

Task 4: Firefox History Analysis (10 marks)

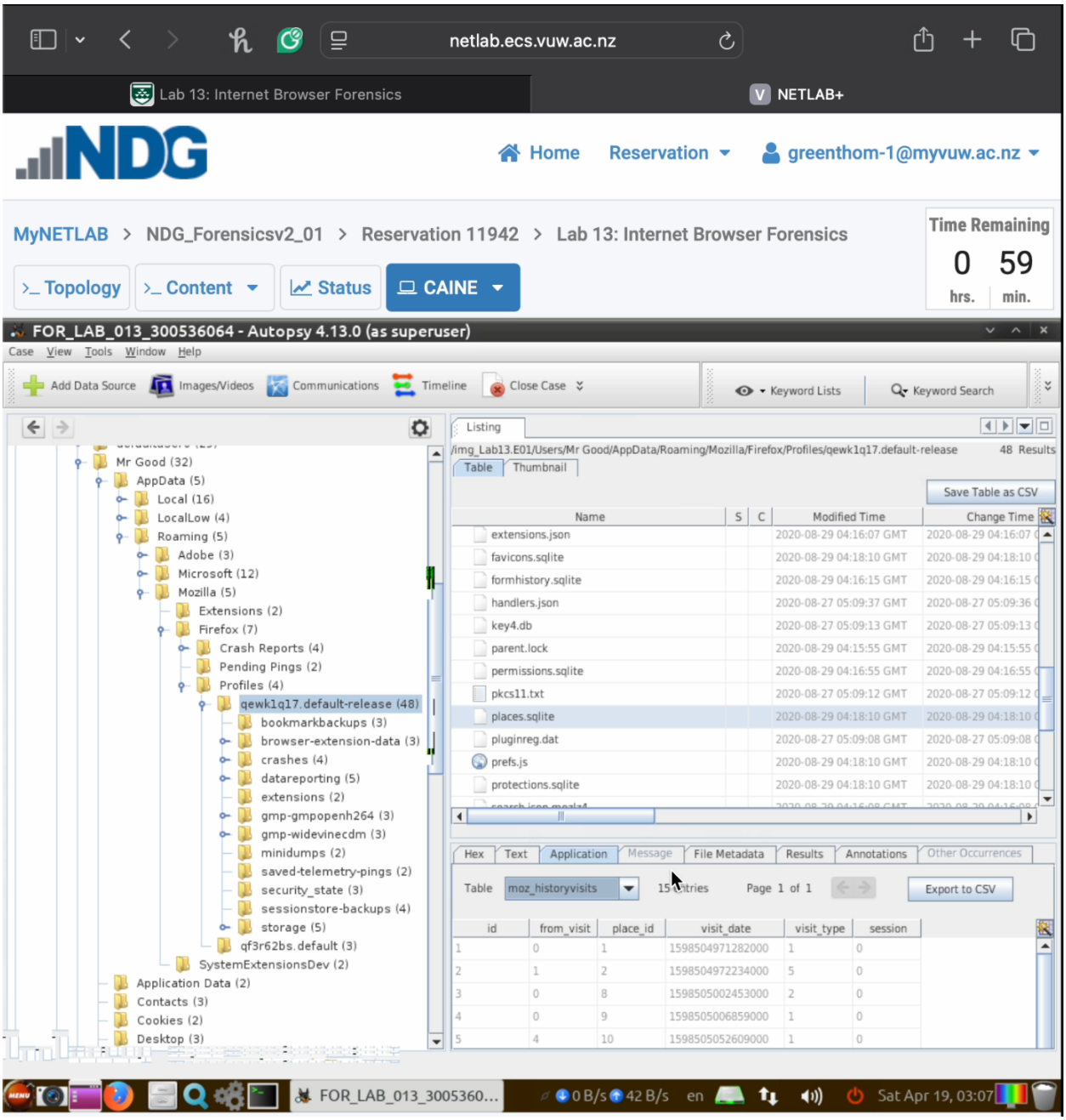
- **Locate the Firefox places.sqlite database in the user's profile**
- **Extract and document browsing history from the moz_places table**
- **Analyze URL visit timestamps from the moz_historyvisits table**
- **Include the Autopsy title window showing case name in screenshots**
- **Required screenshots:**
    - **File path to the Firefox places.sqlite database (step 2.3)**



- **moz_places table content showing URLs (step 2.5)**

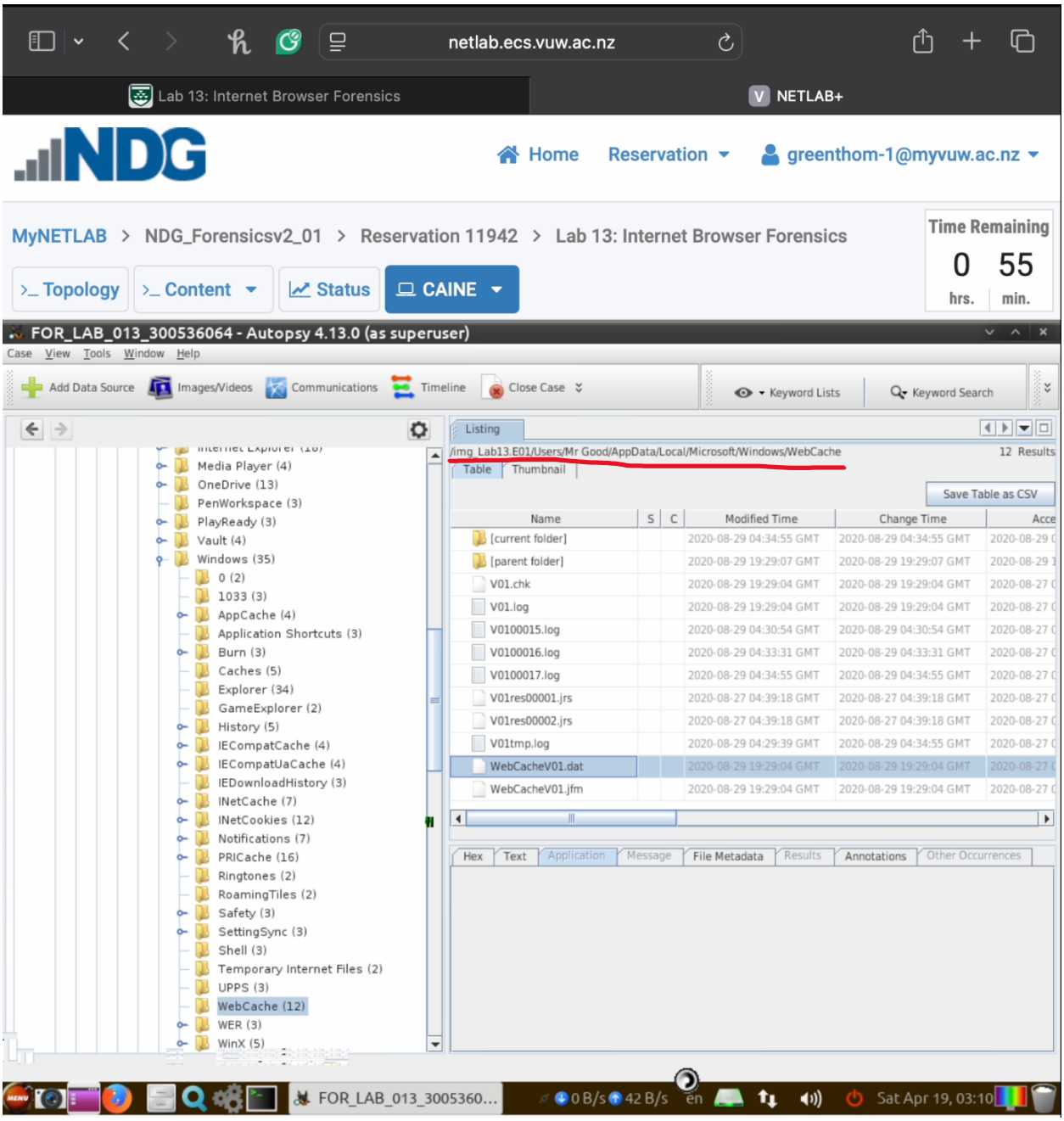


- **moz_historyvisits table with timestamps (step 2.7)**

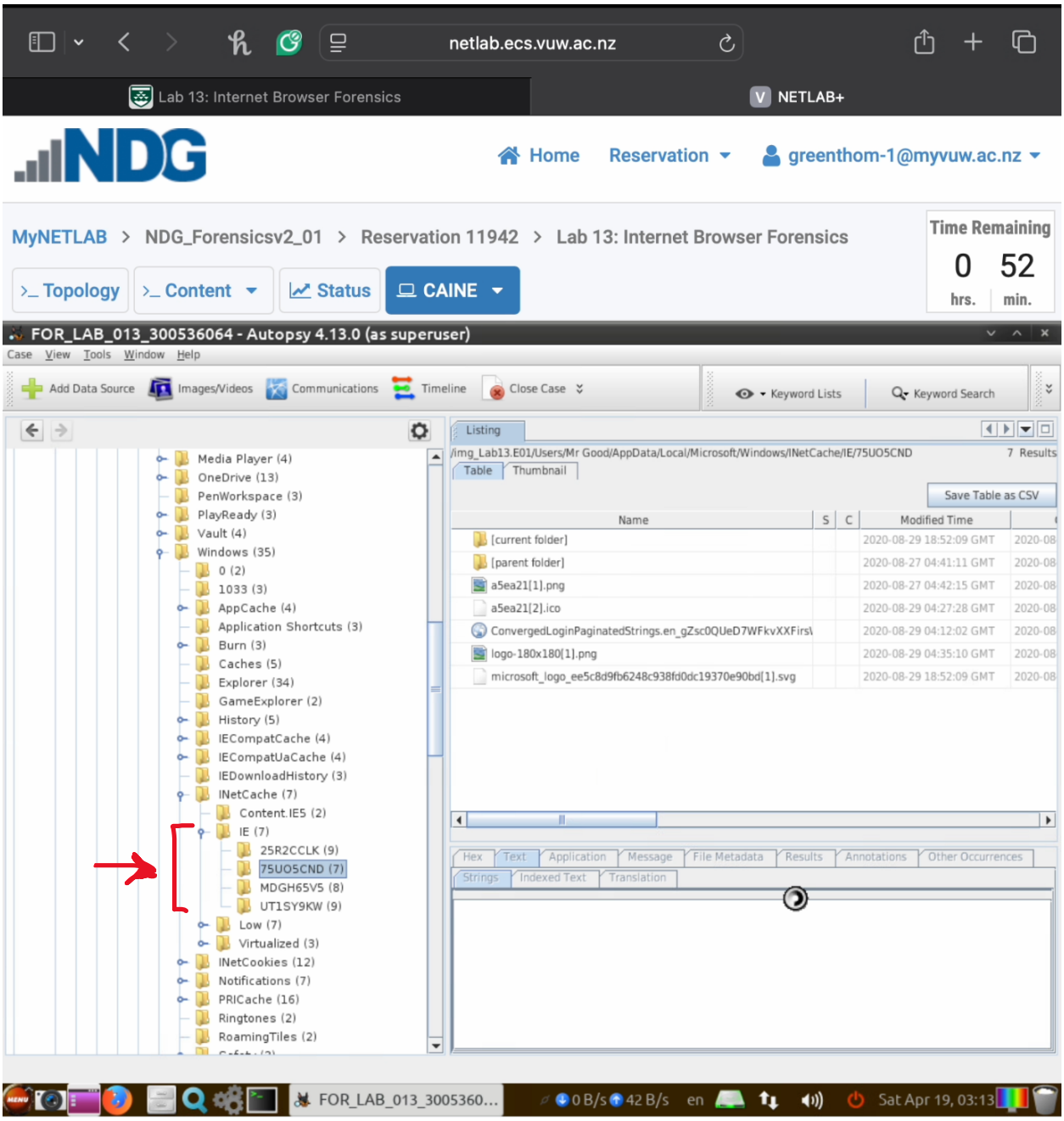


Task 5: Internet Explorer Cache and History Analysis (10 marks)

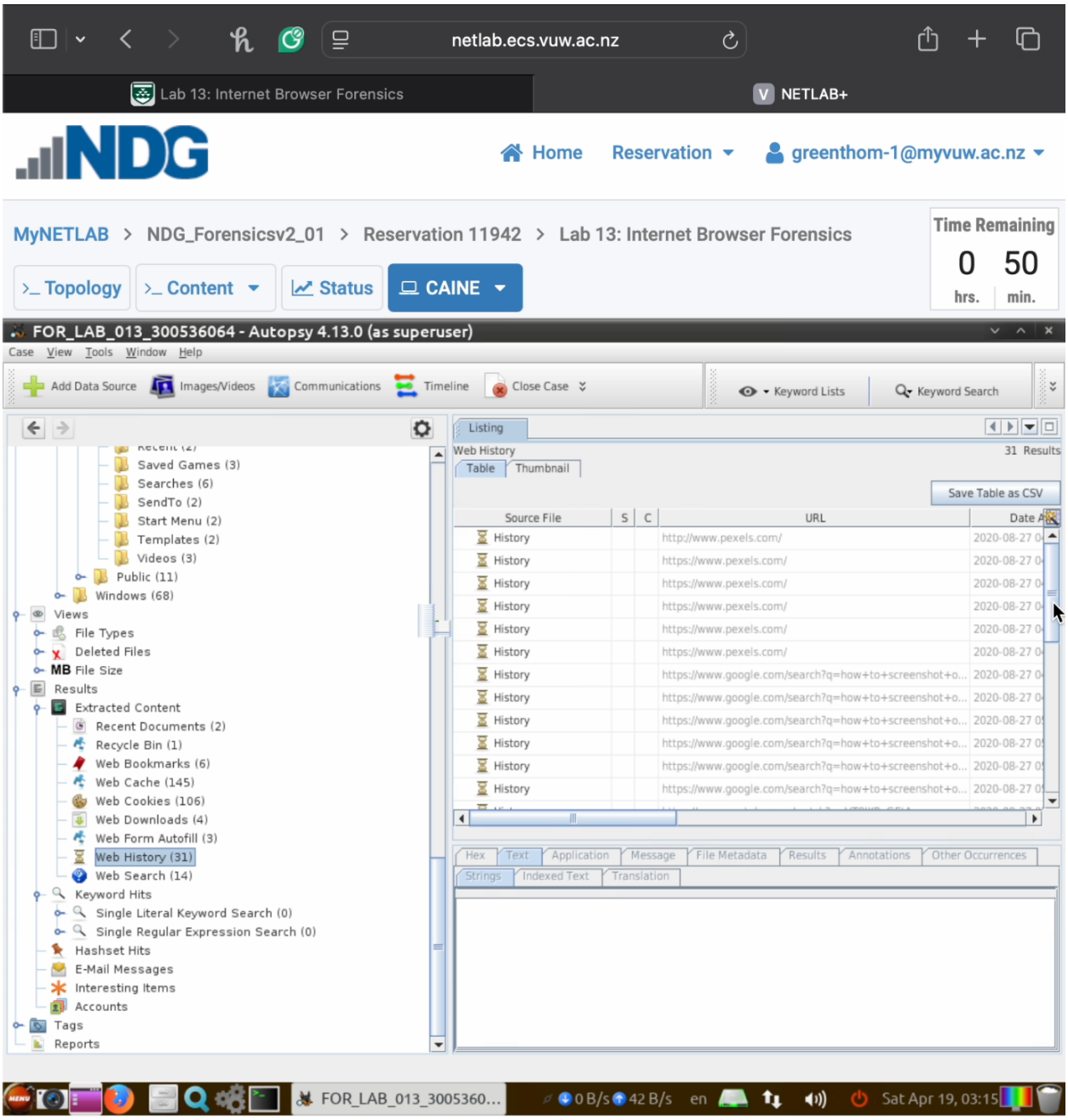
- **Locate Internet Explorer's WebCache database and cache folders**
- **Examine the structure of IE's browsing artifacts**
- **View Autopsy's extracted web history results from all three browsers**
- **Include the Autopsy title window showing case name in screenshots**
- **Required screenshots:**
    - **WebCacheV01.dat file location (step 3.3)**



- **IE cache folder structure (step 3.6)**



- **Autopsy extracted web history results pane (step 4.3 from Part 4)**


netlab.ecs.vuw.ac.nz
Lab 13: Internet Browser Forensics
NETLAB+
NDG
Home
Reservation
greenthom-1@myvuw.ac.nz
MyNETLAB > NDG_Forensicsv2_01 > Reservation 11942 > Lab 13: Internet Browser Forensics
Time Remaining
0 hrs. 50 min.
Topology
Content
Status
CAINE
FOR_LAB_013_300536064 - Autopsy 4.13.0 (as superuser)
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Keyword Lists
Keyword Search
Saved Games (3)
Searches (6)
SendTo (2)
Start Menu (2)
Templates (2)
Videos (3)
Public (11)
Windows (68)
Views
File Types
Deleted Files
File Size
Results
Extracted Content
Recent Documents (2)
Recycle Bin (1)
Web Bookmarks (6)
Web Cache (145)
Web Cookies (106)
Web Downloads (4)
Web Form Autofill (3)
Web History (31)
Web Search (14)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Web History
31 Results
Table
Thumbnail
Save Table as CSV
Source File
S
C
URL
Date A
History
http://www.pexels.com/
https://www.pexels.com/
https://www.google.com/search?q=how+to+screenshot+o...
Hex
Text
Application
Message
File Metadata
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
FOR_LAB_013_3005360...
0 B/s 42 B/s
en
Sat Apr 19, 03:15