CYBR472 Lab 07: Data Carving & Analysis
greenthom – 300536064

Assessment Overview

In this lab, you will demonstrate your understanding of file carving techniques and your ability to recover deleted files from digital evidence. Using both manual and automated methods, you will extract various file types and analyze their contents. This lab is worth 6% of your total course grade.

Submission Requirements

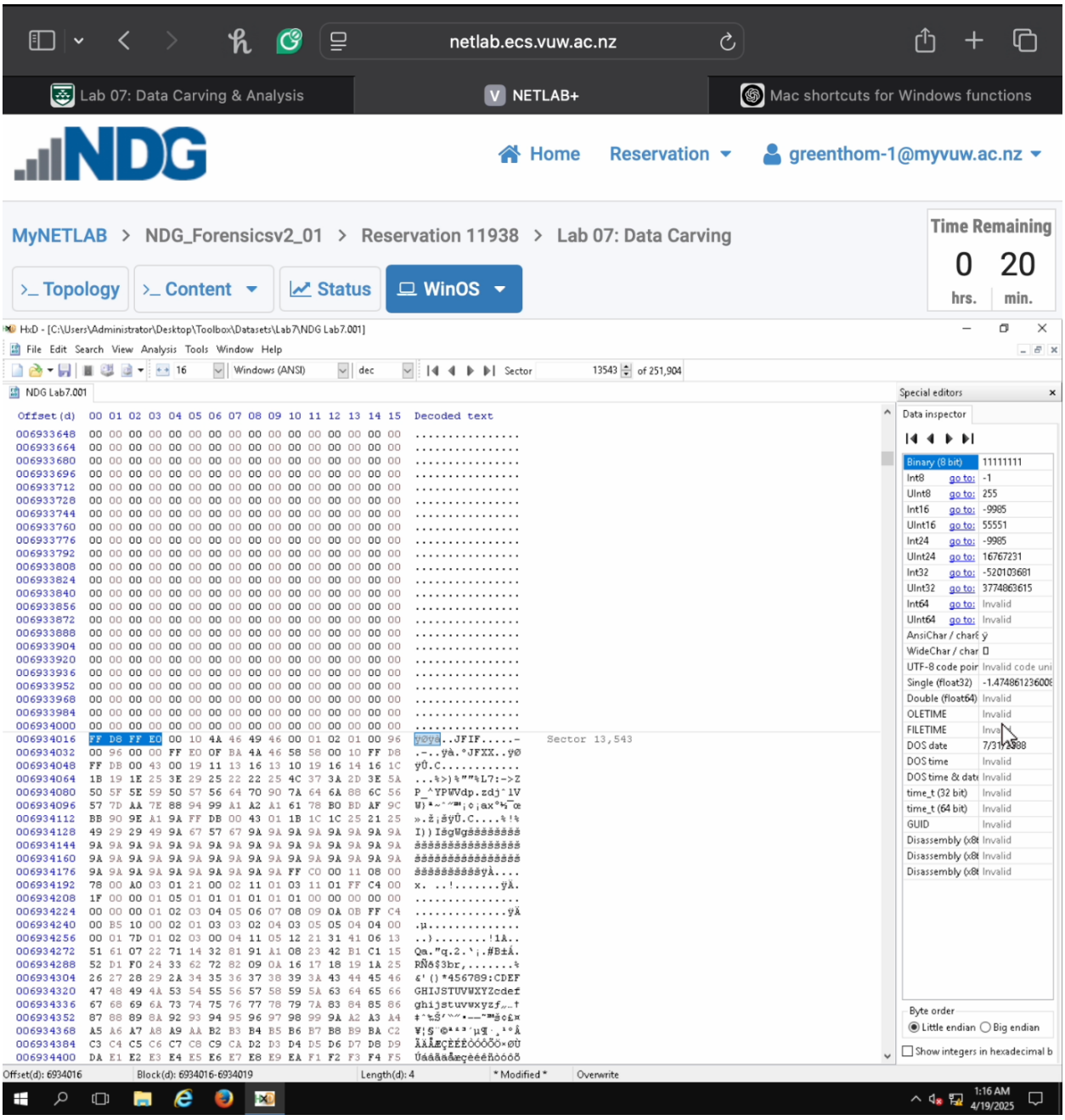
- Heading for the report with lab number, your name, and student ID
- Screenshots as indicated (with personalization requirements)
- Brief descriptions only when specifically requested
- There are 5 questions in total
- Submit as a single PDF document

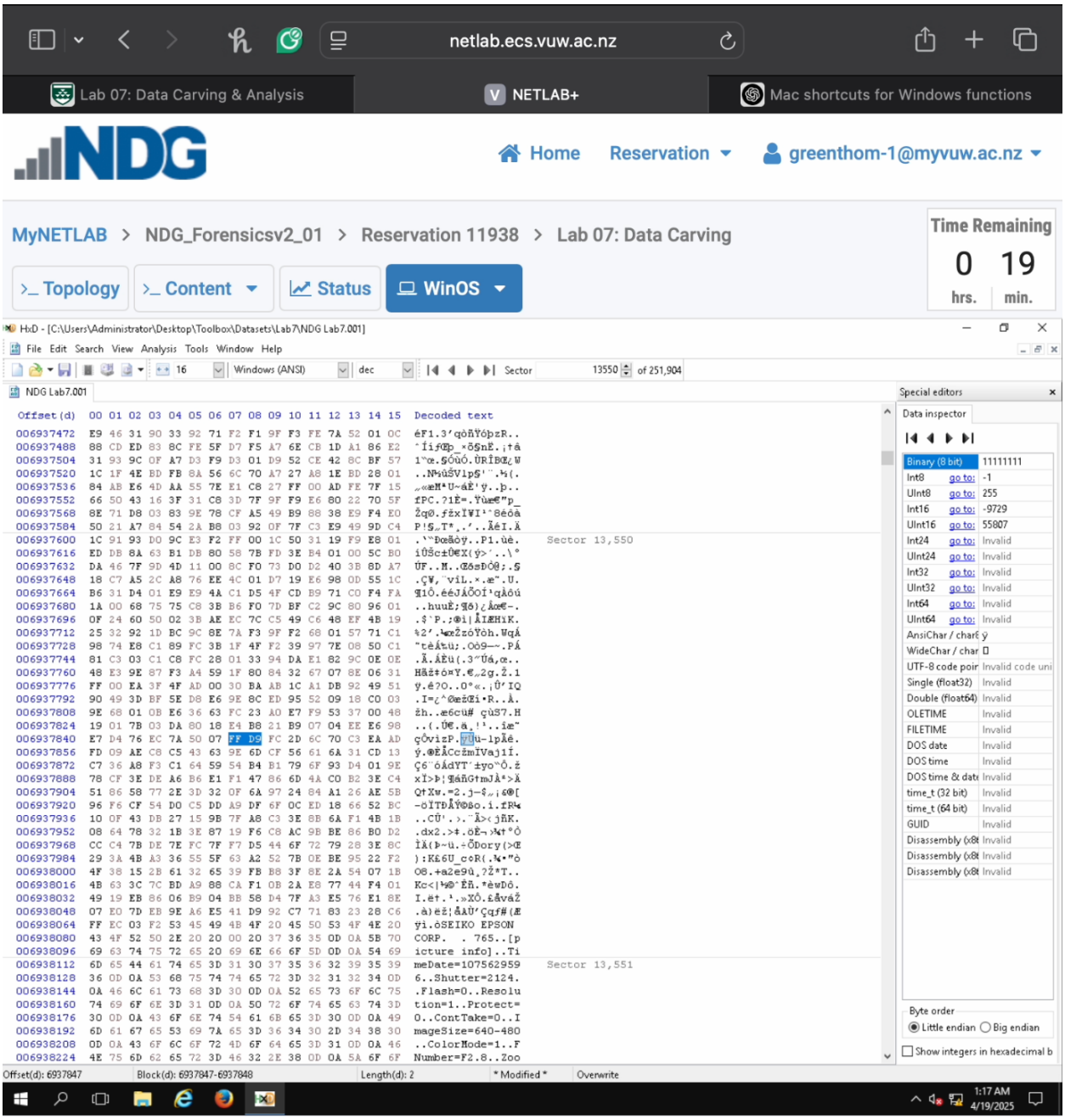
Part 1: Manual File Carving with a Hex Editor (30 marks)

Using HxD Hex Editor, you will manually locate and extract files based on their file signatures.

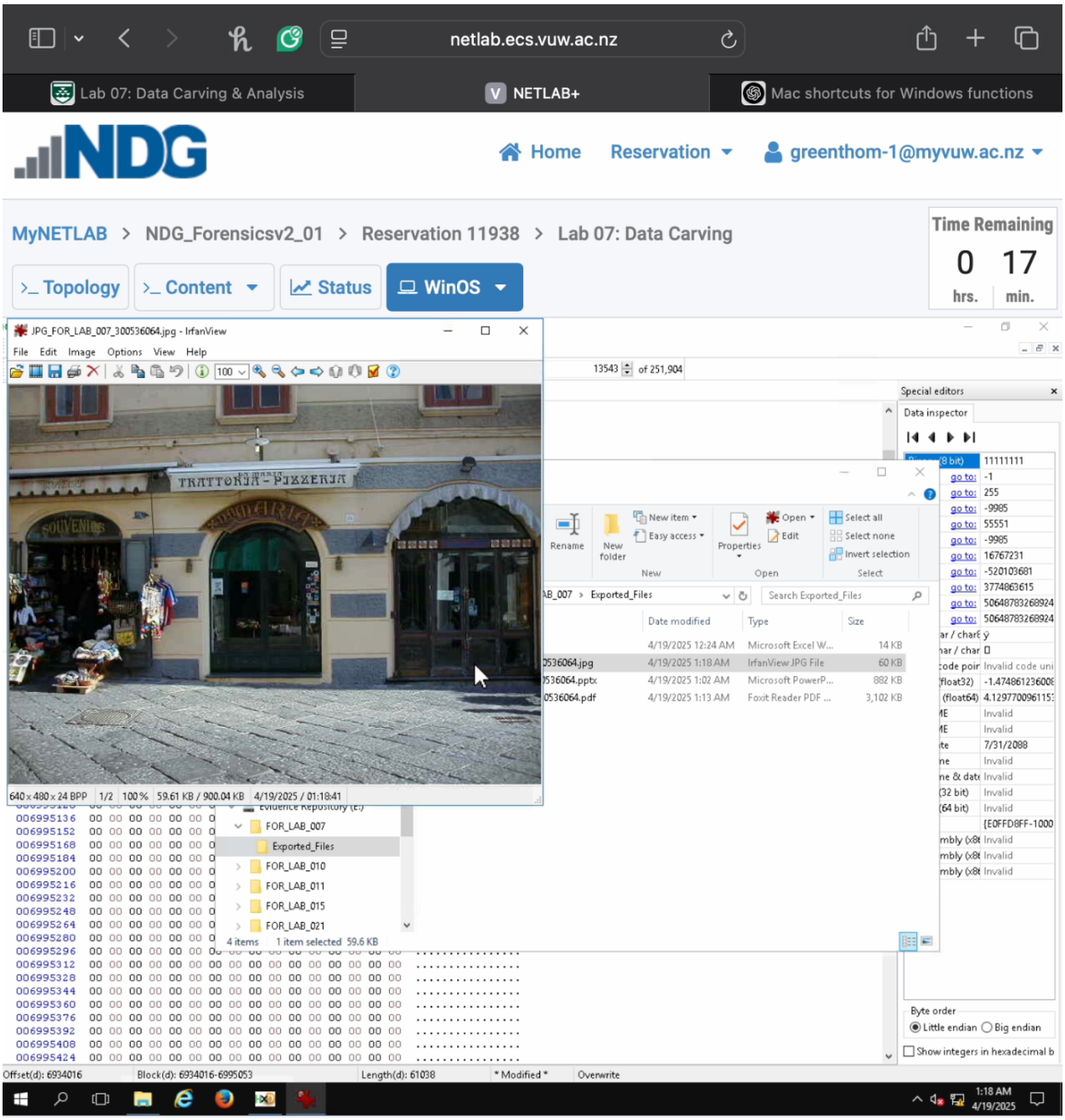
1) JPEG Image Carving (10 marks)

- **Load the provided evidence file in HxD Hex Editor**
- **Locate a JPEG file using its header signature (FF D8 FF E0)**
- **Find the footer signature (FF D9)**
- **Extract and save the file, include your student ID in the file name (e.g. FOR_LAB_007_12345678.jpg)**
- **When viewing the file, make sure filename is visible in the title bar of the viewer**
- **Provide screenshots showing:**
    - **The hex view with the JPEG header signature highlighted (step 4.3)**


netlab.ecs.vuw.ac.nz
Lab 07: Data Carving & Analysis
NETLAB+
Mac shortcuts for Windows functions
NDG
Home
Reservation
greenthom-1@myvuw.ac.nz
MyNETLAB > NDG_Forensicsv2_01 > Reservation 11938 > Lab 07: Data Carving
Time Remaining
0 hrs. 20 min.
Topology
Content
Status
WinOS
HxD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001]
File Edit Search View Analysis Tools Window Help
NDG Lab7.001
Offset (d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 Decoded text
006934016 FF D8 FF EO 00 10 4A 46 49 46 00 01 02 01 00 96 ÿØÿà..JFIF.....– Sector 13,543
Special editors
Data inspector
Offset(d): 6934016
Block(d): 6934016-6934019
Length(d): 4
* Modified *
Overwrite
1:16 AM
4/19/2025



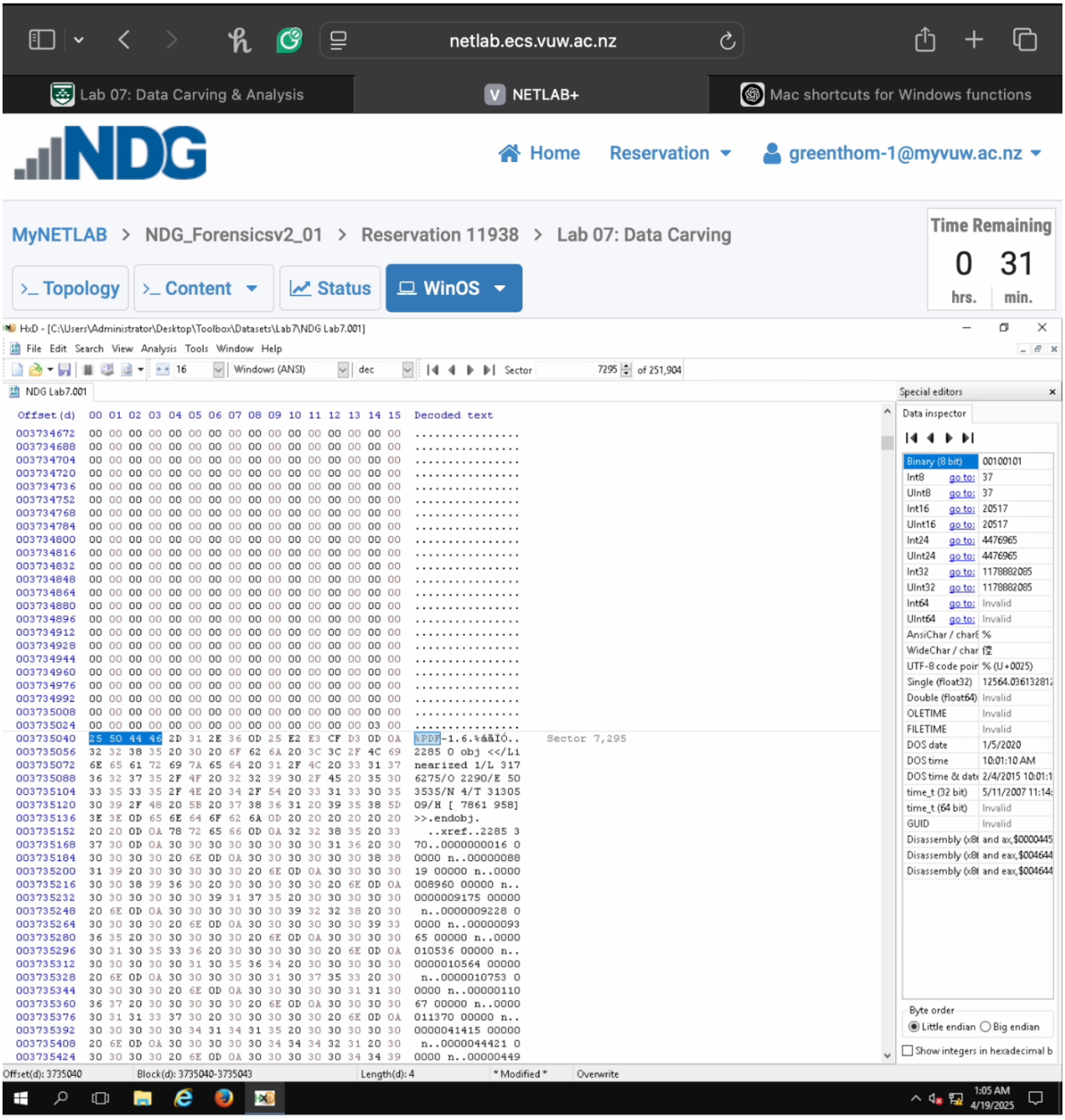
- **The saved image opened in an image viewer (step 4.12)**

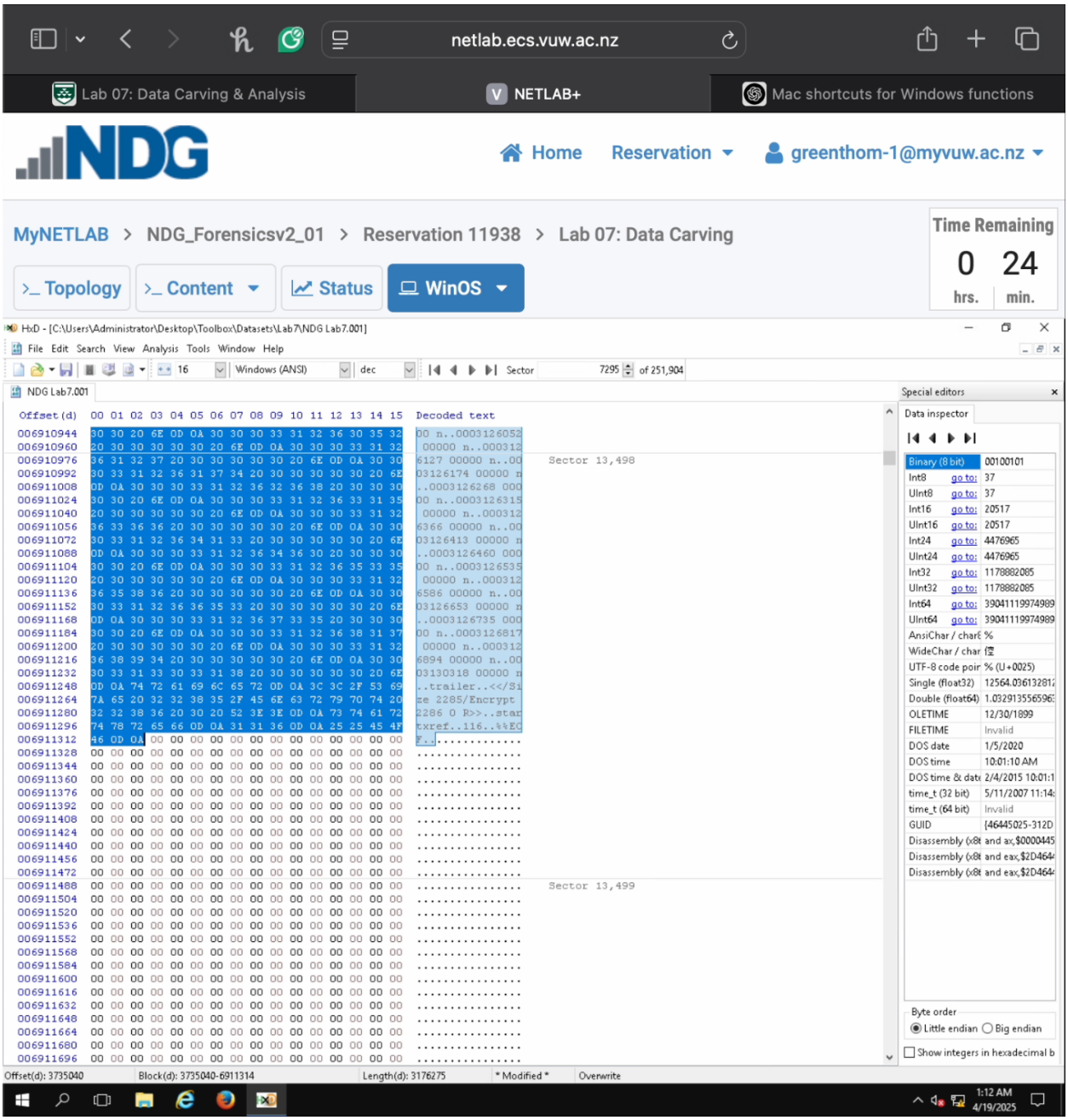


2) PDF Document Carving (10 marks)

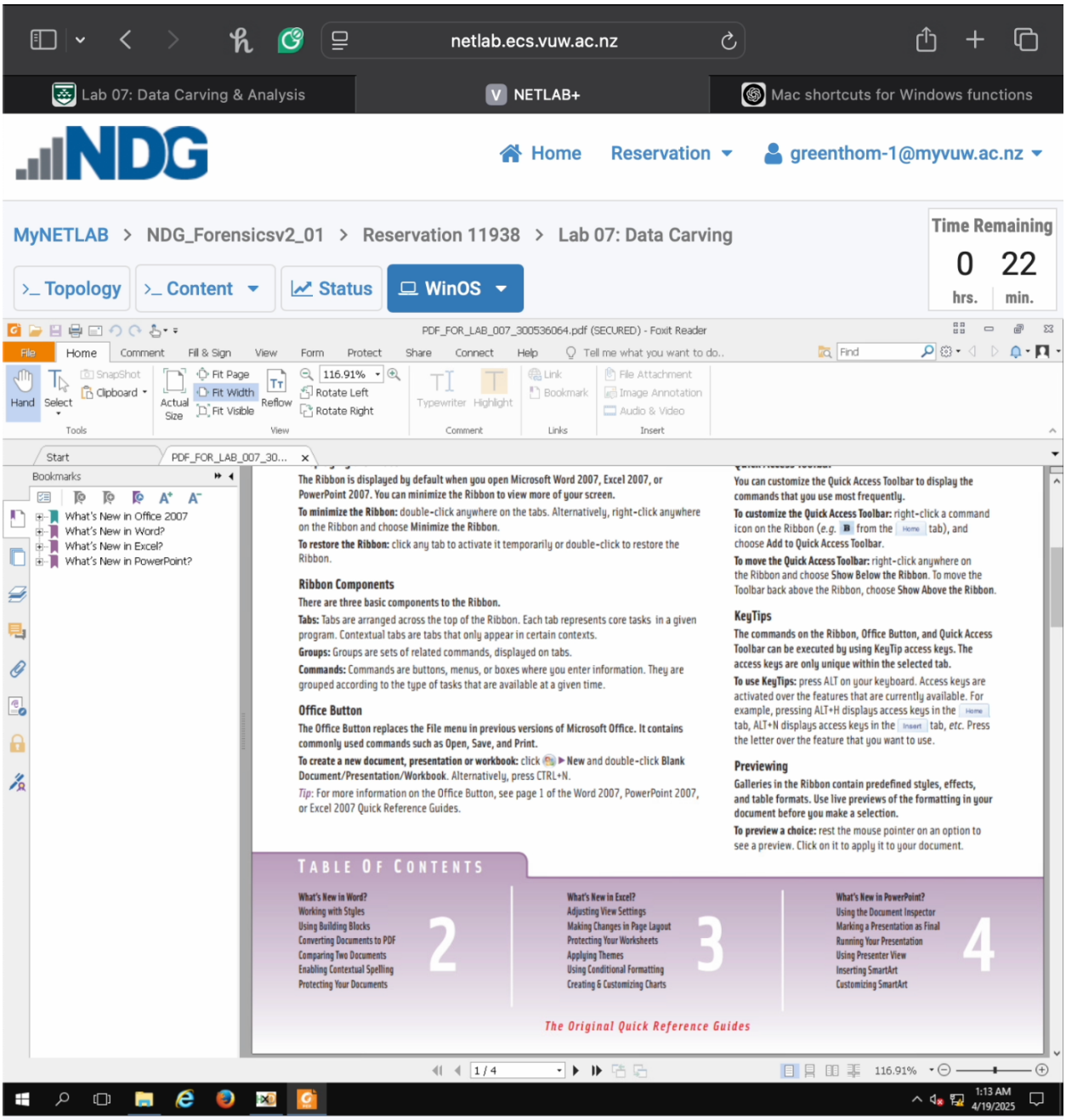
- **Locate a PDF file using its header signature (25 50 44 46)**
- **Find the EOF marker (%%EOF)**
- **Extract and save the file, include your student ID in the file name (e.g., FOR_LAB_007_12345678.pdf)**
- **When viewing the file, make sure filename is visible in the title bar of the viewer**
- **Provide screenshots showing:**

- **The hex view with the PDF header signature highlighted (step 3.3)**



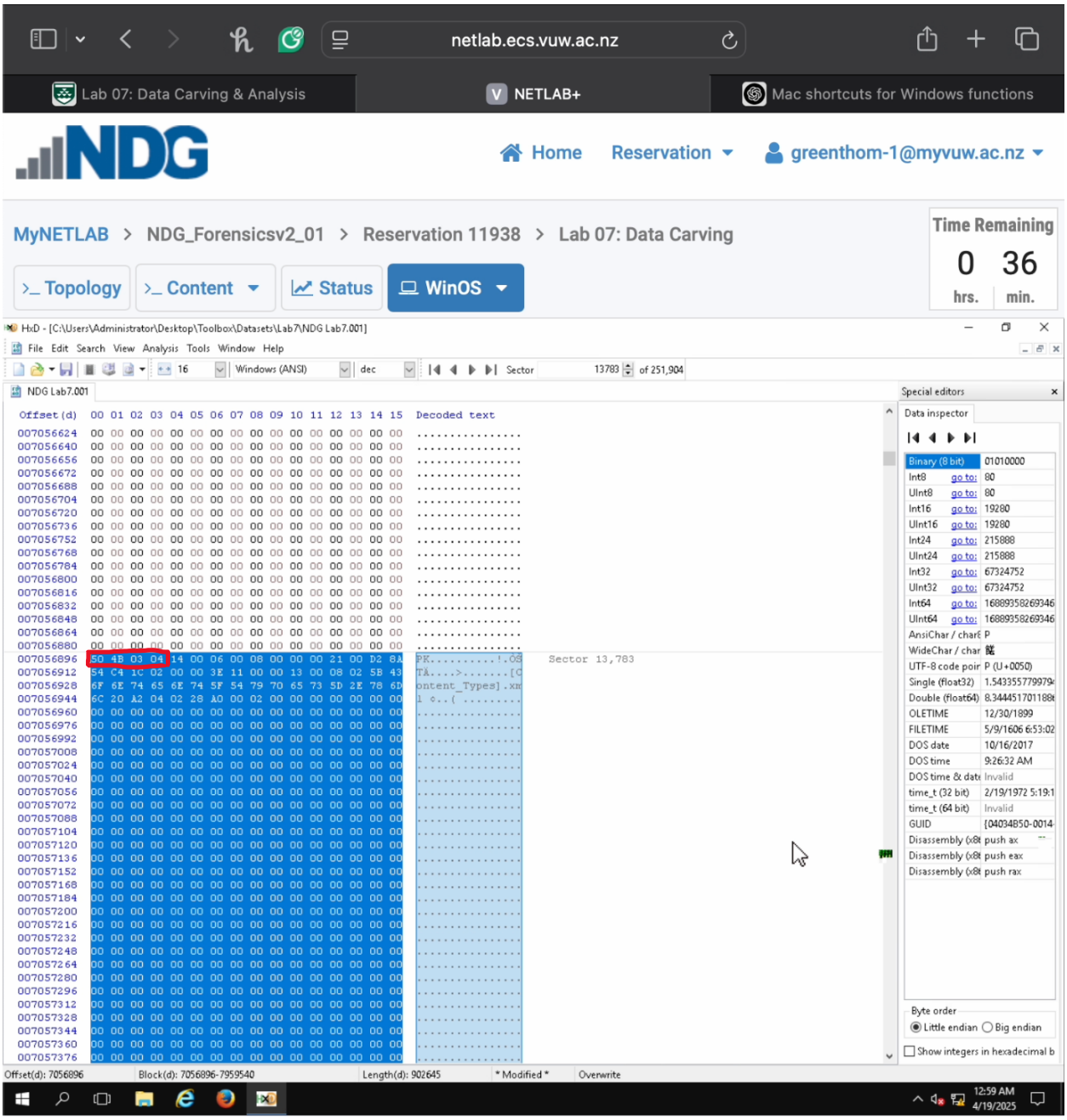


- **The saved PDF document opened in a PDF viewer (step 3.12)**

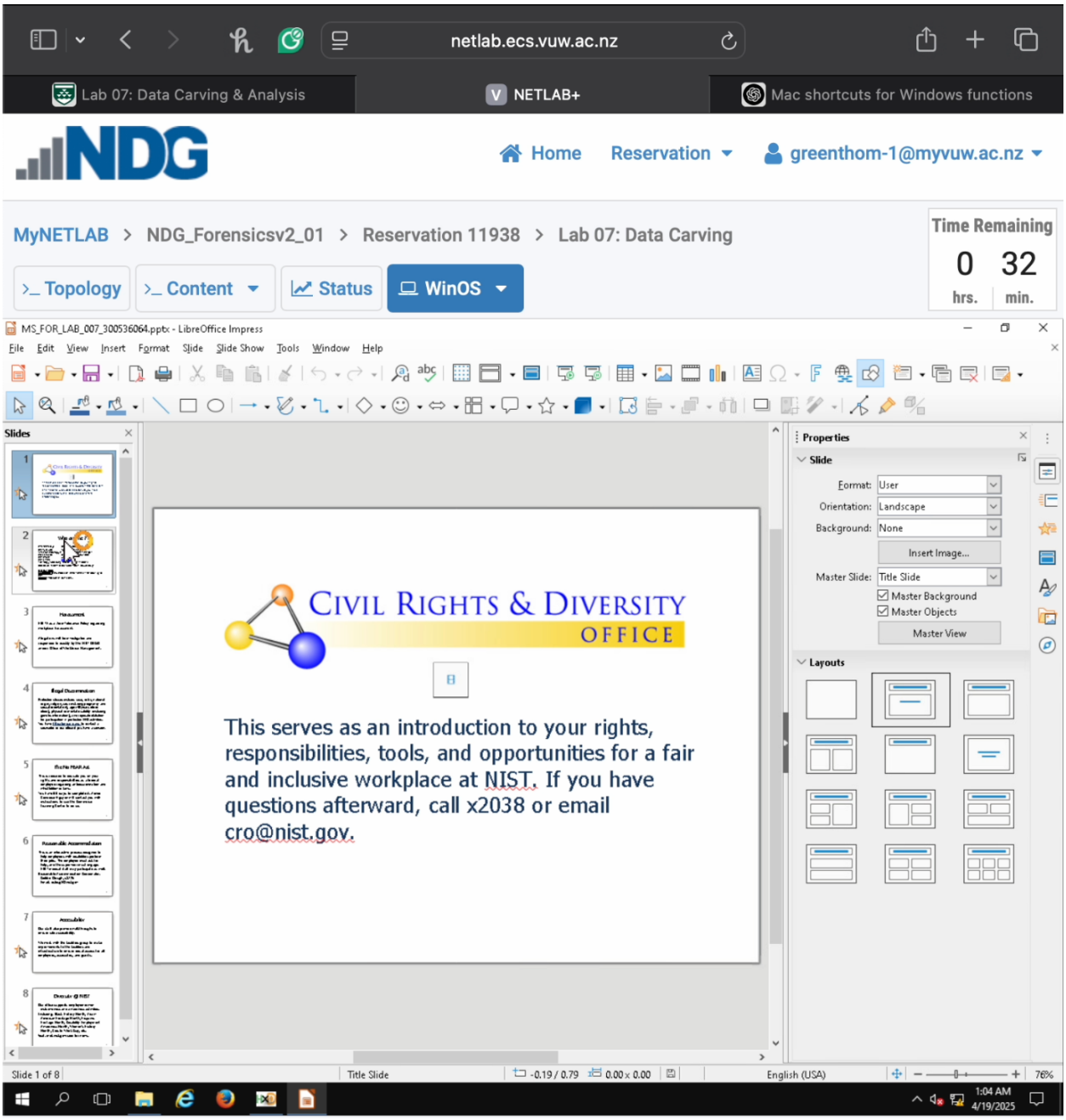


3) MS Office Document Carving (10 marks)

- **Locate a Microsoft Office document NOT THE EXAMPLE ONE FROM THE LABE INSTRUCTIONS (DOCX/XLSX/PPTX) using its signature (50 4B 03 04)**
- **Extract and save the file, include your student ID in the file name (e.g., FOR_LAB_007_12345678.docx)**
- **When viewing the file, make sure filename is visible in the title bar of the viewer**
- **Provide screenshots showing:**
    - **The hex view with the document's header signature highlighted (step 2.3)**



- **The saved document opened in the appropriate viewer (step 2.12)**

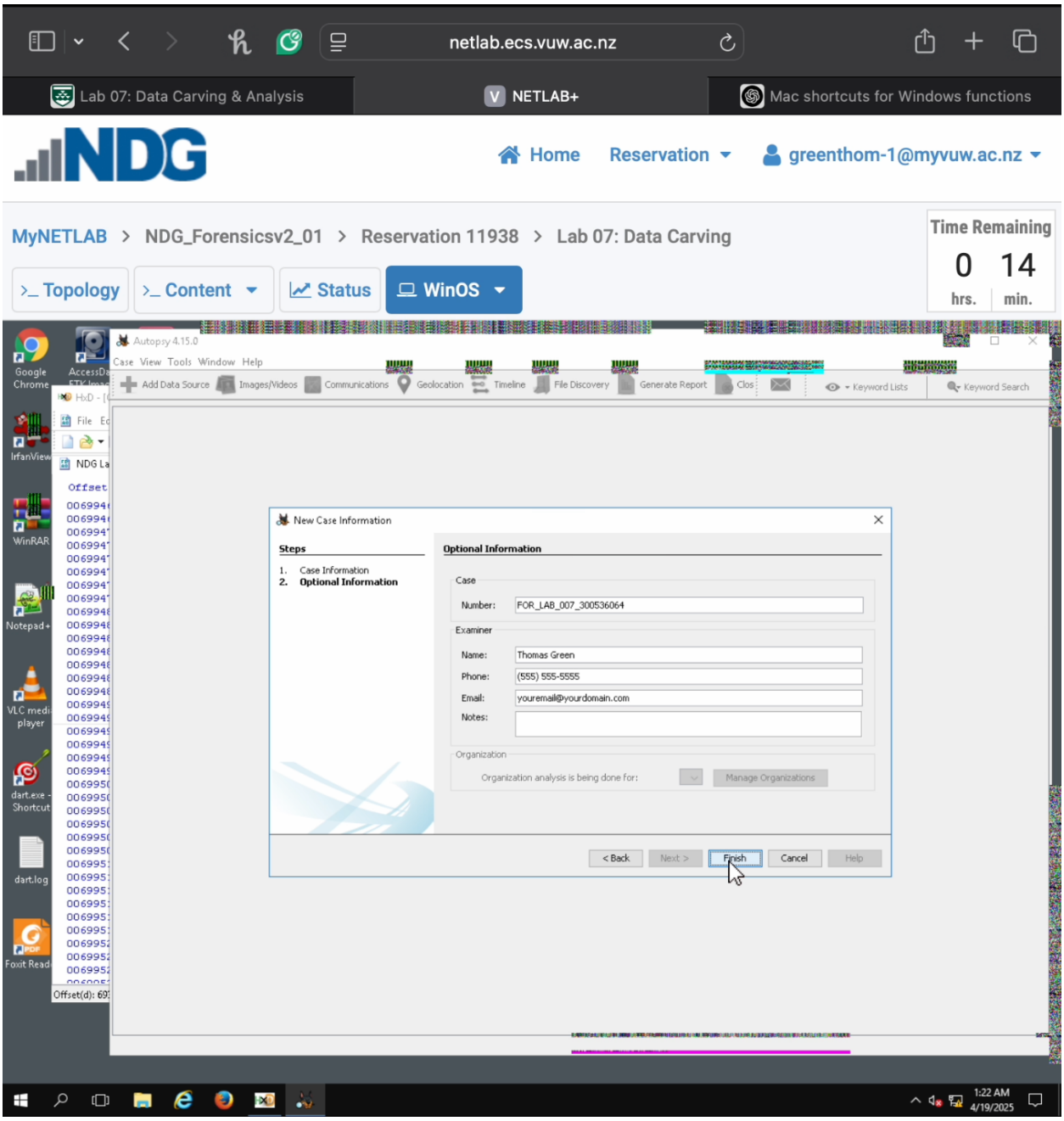


Part 2: Automated File Carving with Forensic Tools (20 marks)

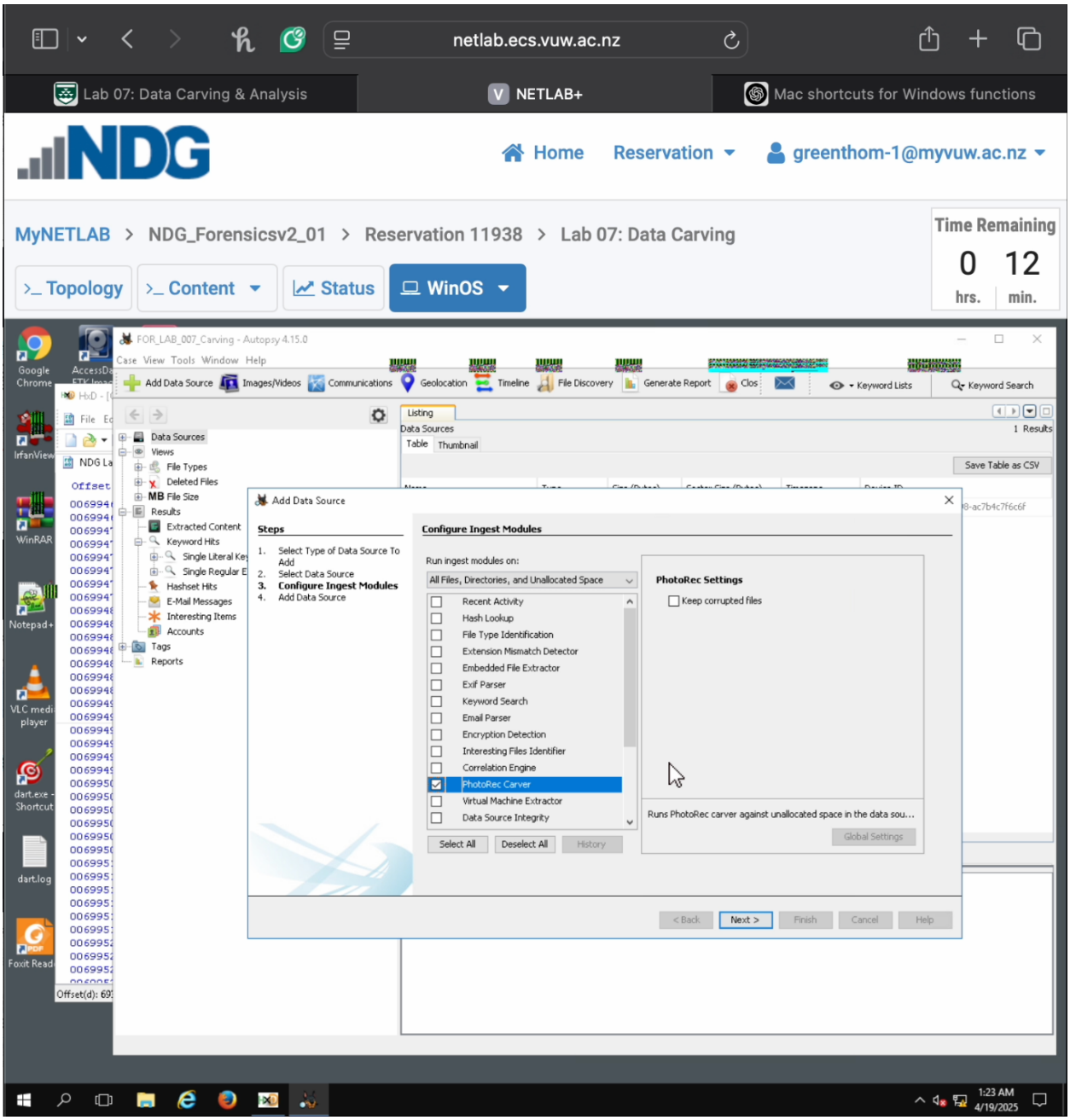
Using Autopsy, you will perform automated file carving and analyze the results.

4) Analyzing Carved Files (10 marks)

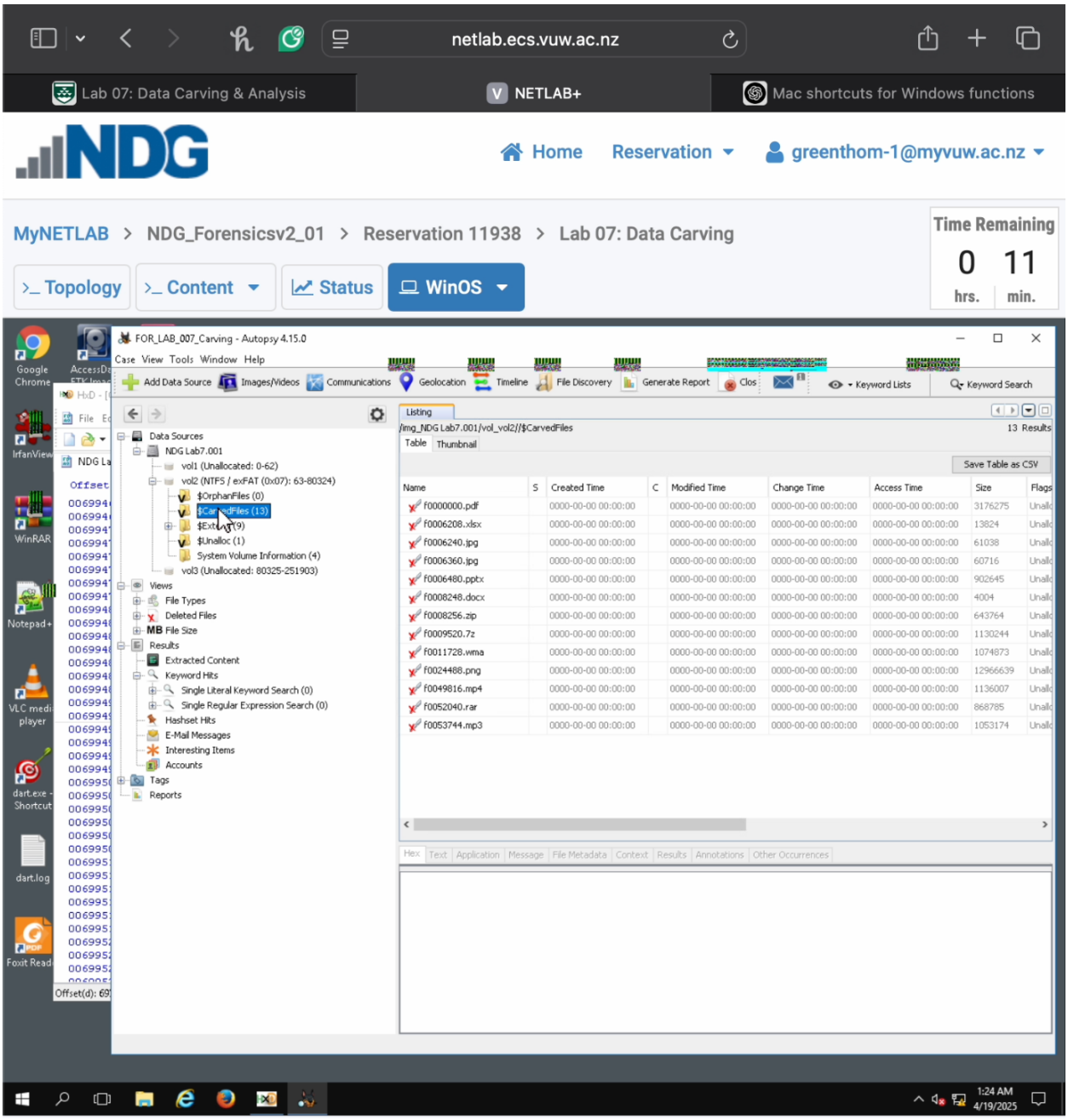
- **Create a new case in Autopsy with your name as examiner**
- **Include your student ID in the case number field (e.g., FOR_LAB_007_12345678)**



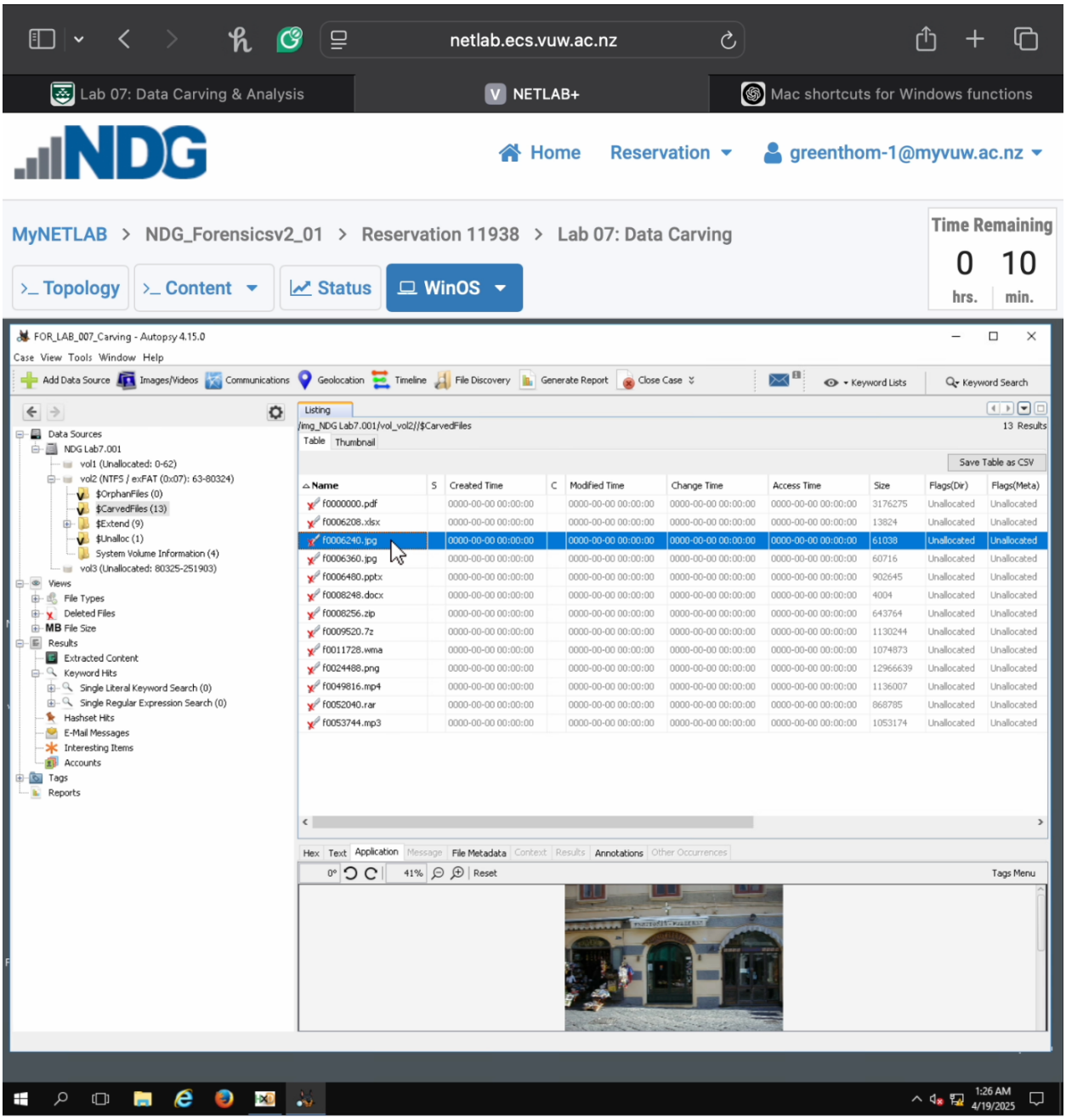
- **Add the provided evidence file as a data source**
- **Configure the PhotoRec Carver Ingest Module**



- **Examine the files recovered by Autopsy**
- **Compare the results with your manual carving**
- **Provide screenshots showing:**
    - **The list of carved files in Autopsy (step 15.15)**

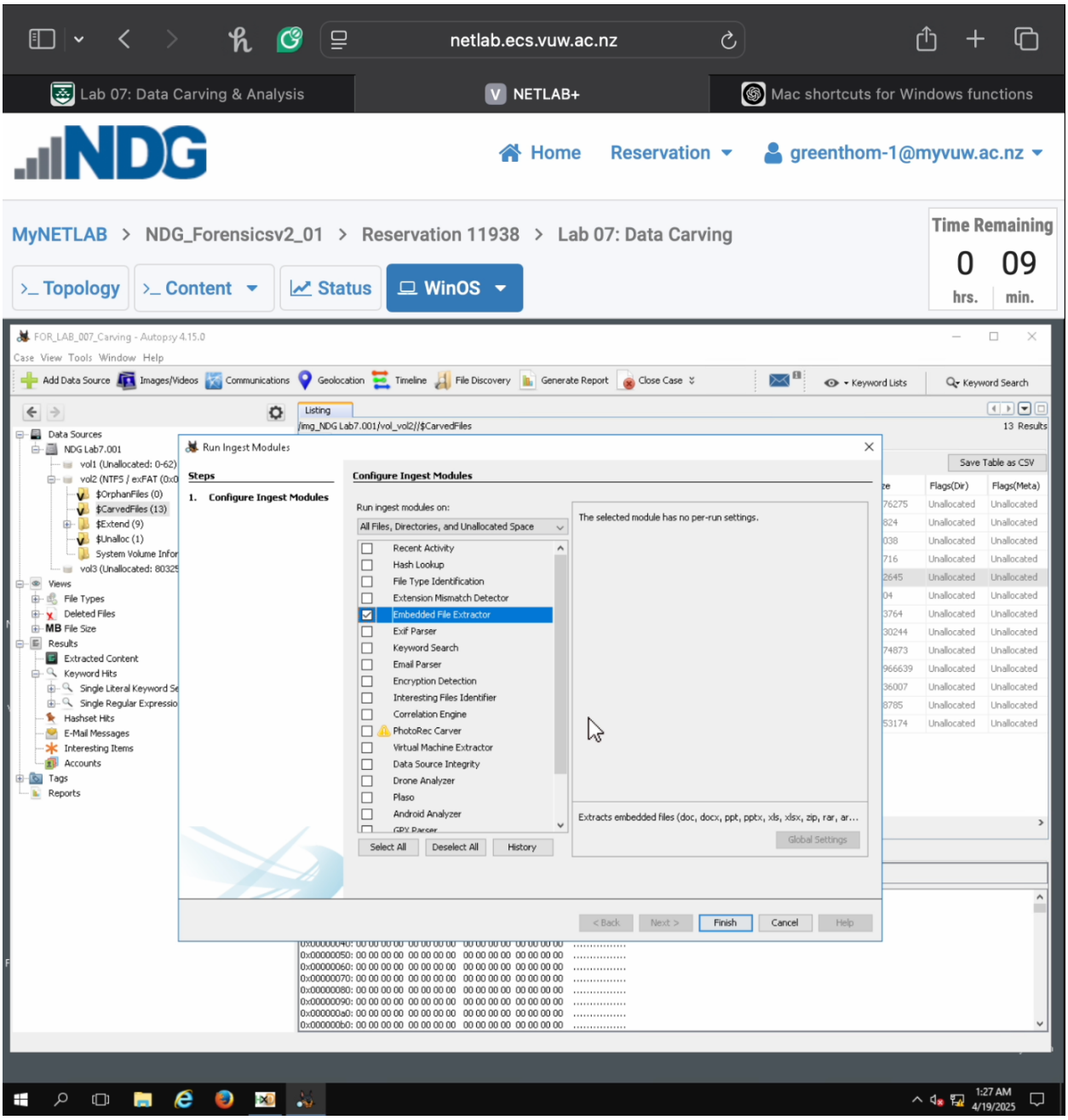


- **Highlight a file that was successfully carved both manually and automatically (step 15.16)**

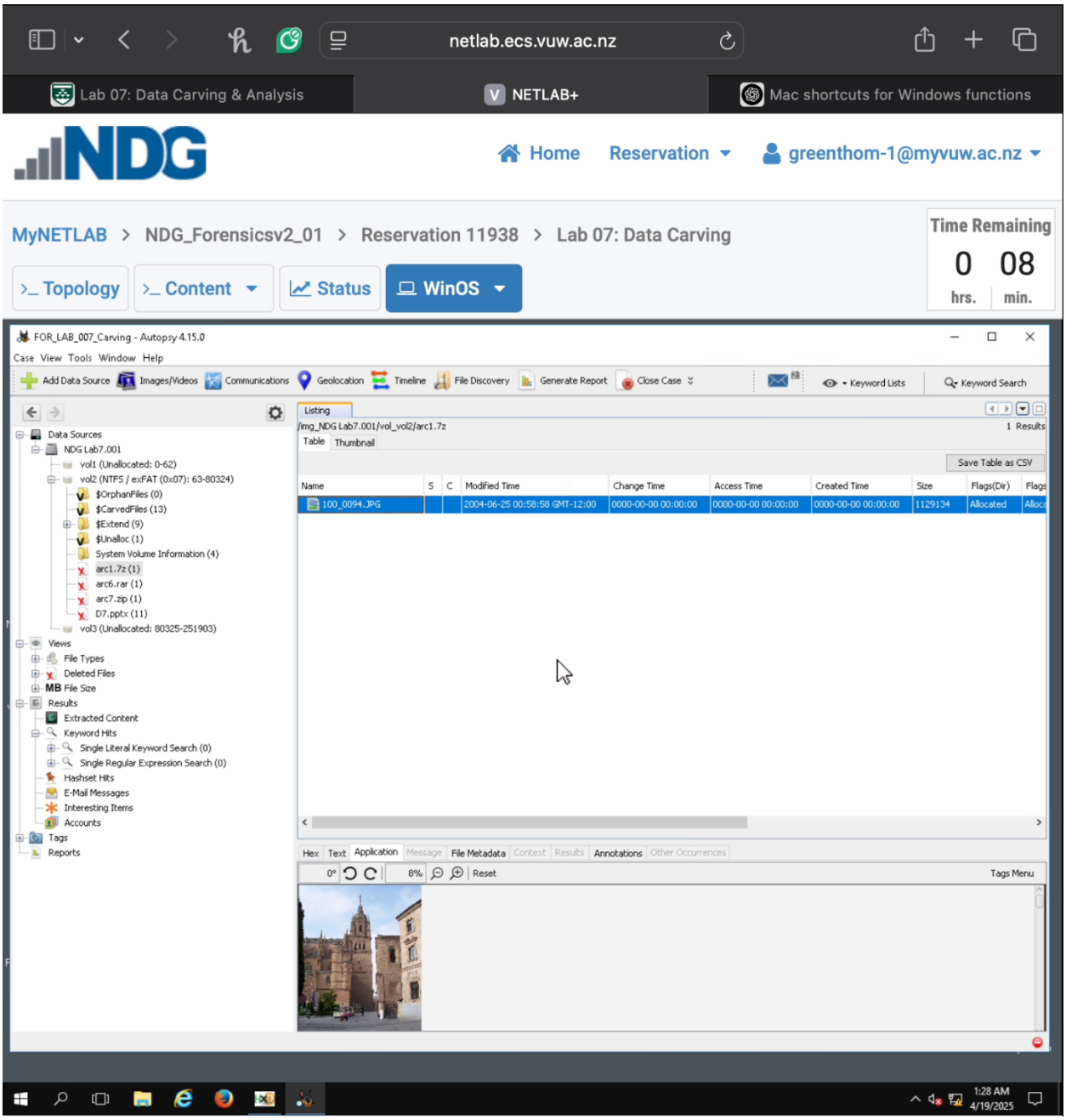


5) Extracting Embedded Files (10 marks)

- **Configure the Embedded File Extractor Ingest Module**
- **Run it on the carved files**
- **Provide screenshots showing:**
    - **The Embedded File Extractor configuration (step 15.18)**



- **The extracted content from an archive file (step 15.20)**


netlab.ecs.vuw.ac.nz
Lab 07: Data Carving & Analysis
NETLAB+
Mac shortcuts for Windows functions
NDG
Home
Reservation
greenthom-1@myvuw.ac.nz
MyNETLAB > NDG_Forensicsv2_01 > Reservation 11938 > Lab 07: Data Carving
Time Remaining
0 hrs. 08 min.
Topology
Content
Status
WinOS
FOR_LAB_007_Carving - Autopsy 4.15.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
File Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
NDG Lab7.001
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-80324)
$OrphanFiles (0)
$CarvedFiles (13)
$Extend (9)
$Unalloc (1)
System Volume Information (4)
arc1.7z (1)
arc6.rar (1)
arc7.zip (1)
D7.pptx (11)
vol3 (Unallocated: 80325-251903)
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
/img_NDG Lab7.001/vol_vol2/arc1.7z
1 Results
Table
Thumbnail
Save Table as CSV
Name
S
C
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags
100_0094.JPG
2004-06-25 00:58:58 GMT-12:00
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
1129134
Allocated
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
0°
8%
Reset
Tags Menu
1:28 AM
4/19/2025