

# **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)

The screenshot shows a Windows desktop environment with several open windows. At the top, there's a browser window titled "netlab.ecs.vuw.ac.nz" showing "Lab 07: Data Carving & Analysis". Below it is a "NETLAB+" interface with "Home", "Reservation", and "greenthom-1@myvuw.ac.nz" buttons. The main workspace displays a "MyNETLAB" navigation tree under "NDG\_Forensicsv2\_01" with "Reservation 11938" selected, leading to "Lab 07: Data Carving". Below this are tabs for "Topology", "Content", "Status", and "WinOS" (which is currently active). A "Time Remaining" timer shows 0 hours and 20 minutes. The central area contains a hex editor for "HxD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab7\NDG Lab7.001]". The hex dump shows a file starting with a JPEG header (FF DB FF E0 00 1A 46 49 00 00 00 00 00 00 00 00) followed by a lot of zeros. To the right of the hex dump is a "Special editors" pane with a "Data inspector" tab showing various memory types and their addresses. The bottom of the screen has a taskbar with icons for File Explorer, Task View, Start, and the system tray.

Screenshot of a web-based forensic tool interface titled "MyNETLAB > NDG\_Forensicsv2\_01 > Reservation 11938 > Lab 07: Data Carving".

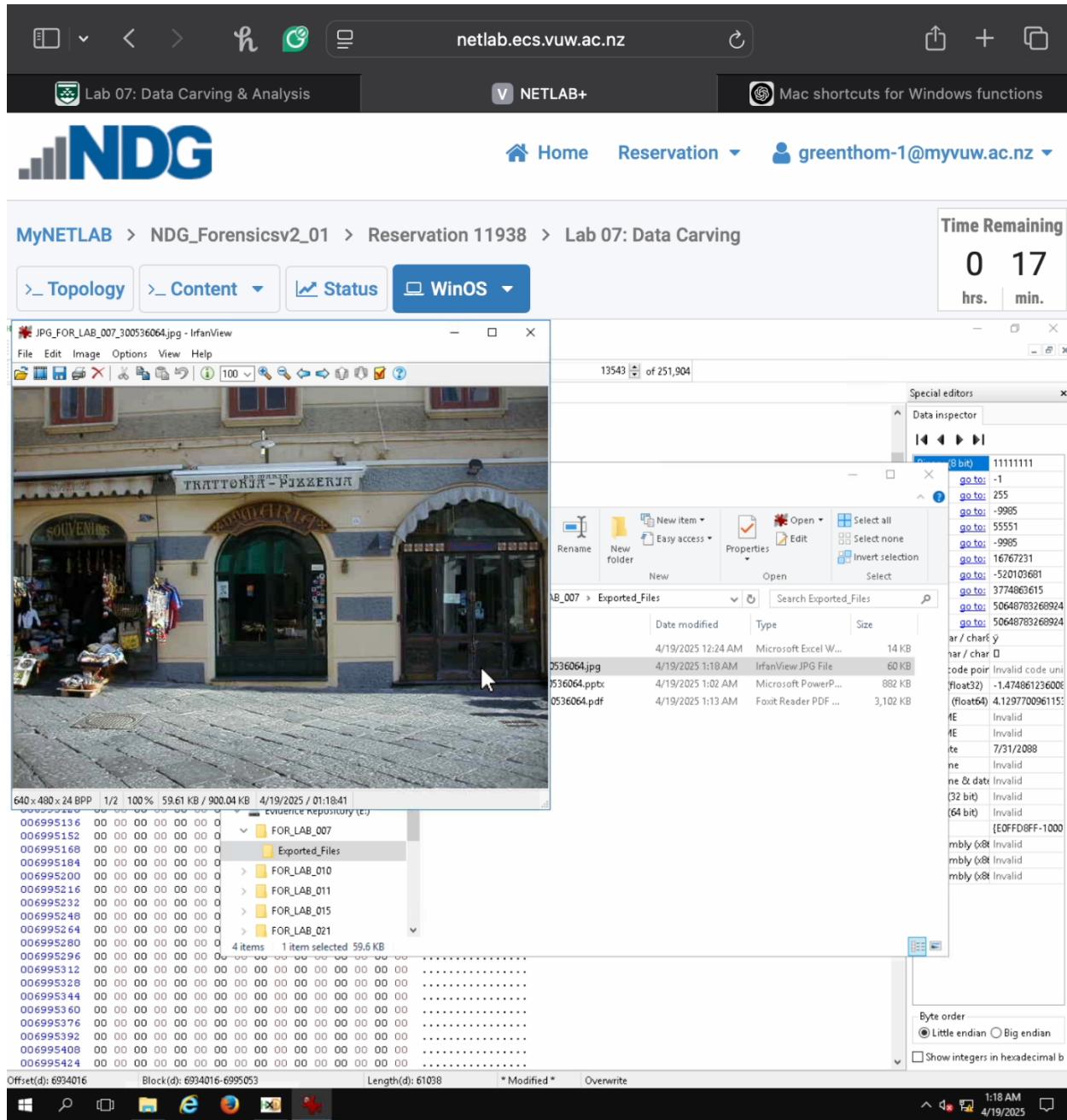
The interface includes a top navigation bar with tabs: Home, Reservation, and a user account section. A sidebar on the left shows a file tree under "HdD - [C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab\NDG Lab7.001]".

The main content area displays a hex dump of a file, with columns for Address (Offset(d)), Hex, ASCII, and Decoded text. The "Decoded text" column shows various binary strings, some of which are partially readable or decoded by the tool.

On the right side, there is a "Time Remaining" timer showing 0:19, and a "Special editors" panel containing a "Data inspector" tab with a binary dump of the file content.

At the bottom, a Windows taskbar is visible with icons for File Explorer, Task View, Start, Internet Explorer, and others.

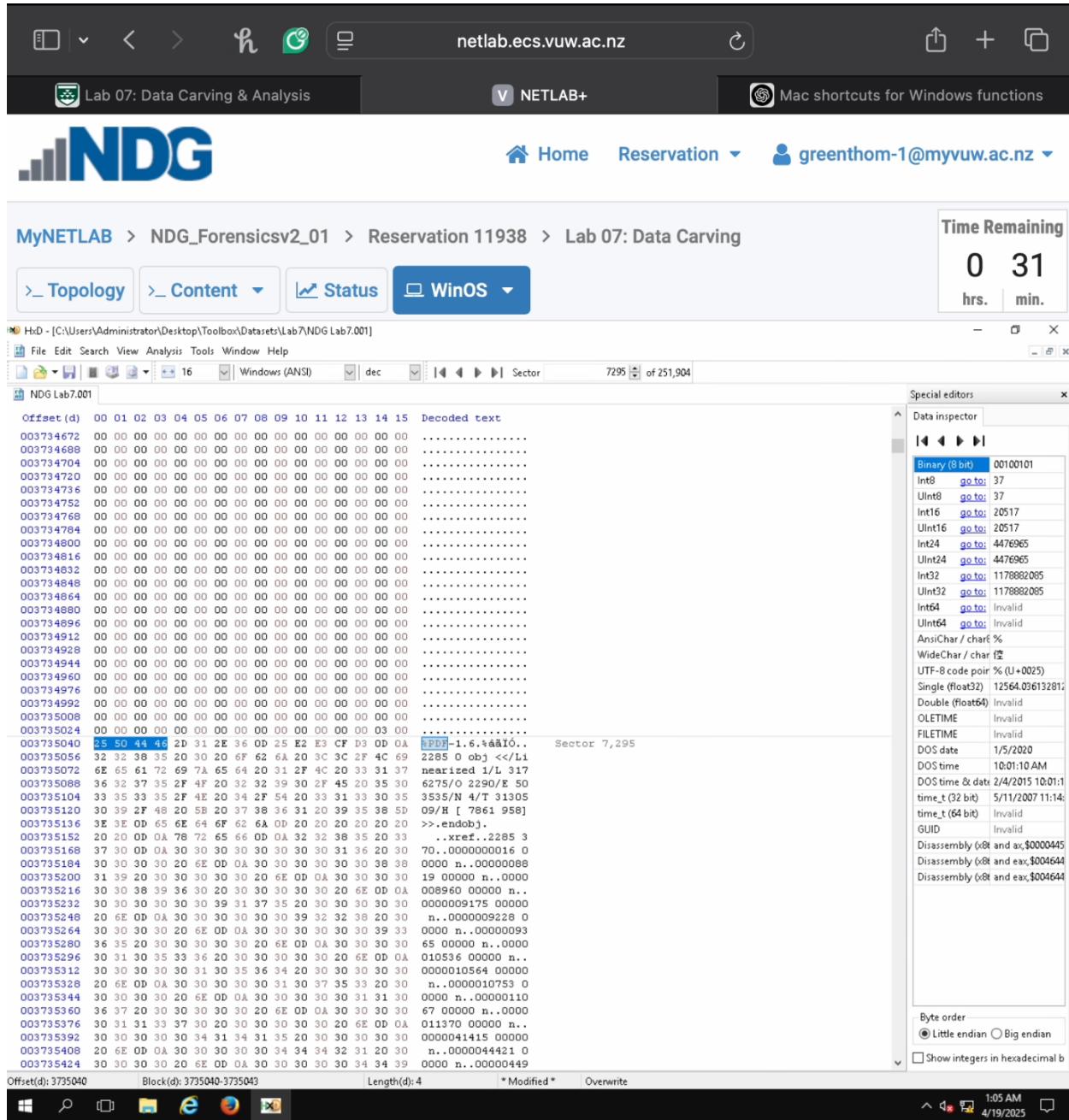
- The saved image opened in an image viewer (step 4.12)



## 2) PDF Document Carving (10 marks)

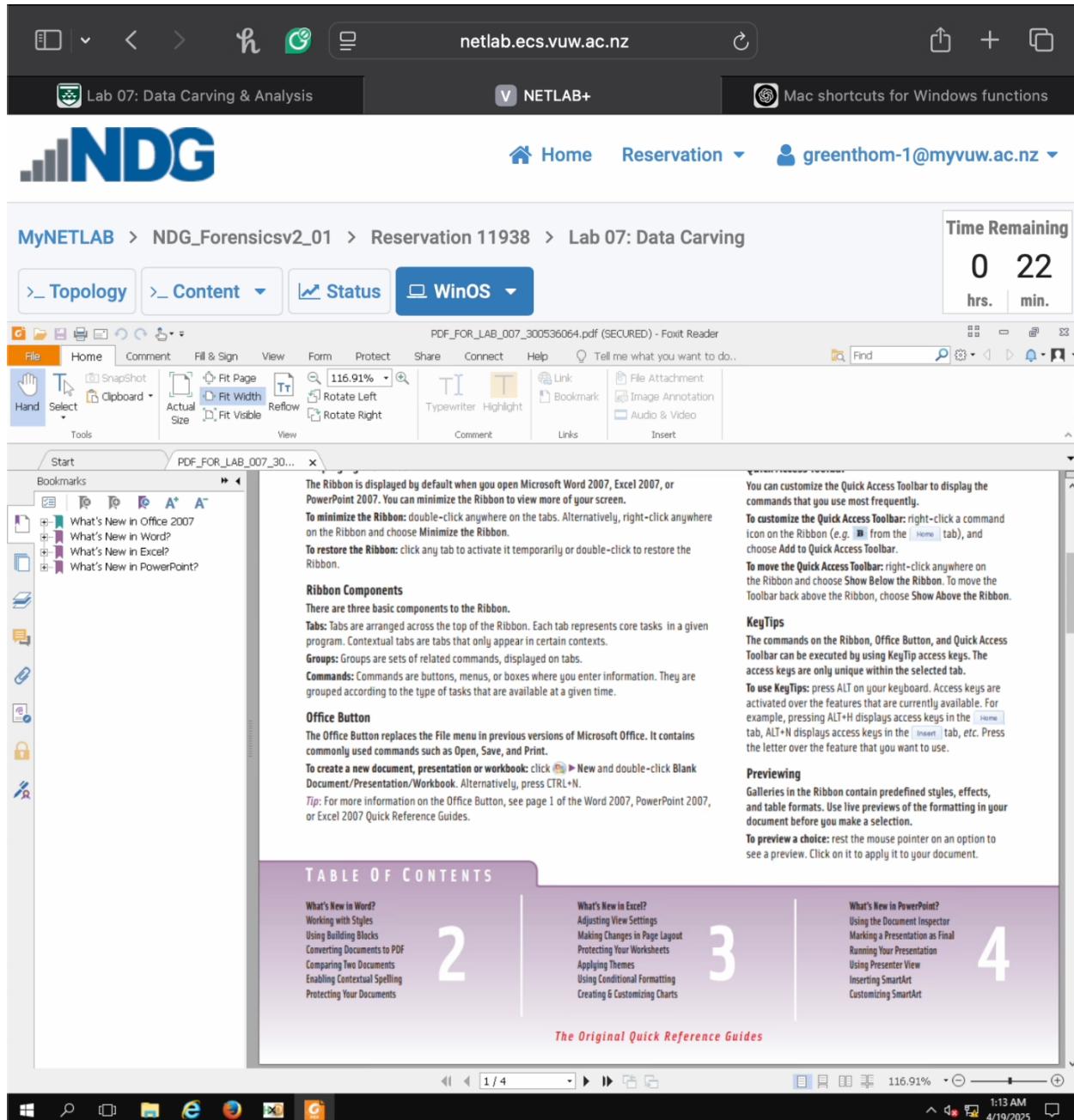
- Locate a PDF file using its header signature (25 50 44 46)
- Find the EOF marker (%EOF)
- Extract and save the file, include your student ID in the file name (e.g., FOR\_LAB\_007\_12345678.pdf)
- When viewing the file, make sure filename is visible in the title bar of the viewer
- Provide screenshots showing:

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



The screenshot shows the MyNETLAB interface for Lab 07: Data Carving. The main window displays a hex dump of a file from offset 00 to 3735040. The dump includes columns for Offset(d), Block(d), Length(d), \*Modified\*, and Overwrite. The 'Special editors' panel on the right shows a 'Data inspector' tab with memory dump types like Binary (8 bit), Int8, UInt8, Int16, UInt16, Int32, UInt32, Int64, UInt64, AnsiChar / char %, WideChar / char %, UTF-8 code pair % (U+0025), Single (float32), Double (float64), OLETIME, FILETIME, DOS date, DOS time, DOS time & date, time\_t (32 bit), time\_t (64 bit), GUID, Disassembly (x86 and x64), and Disassembly (x86 and x64). The interface also includes a navigation bar with tabs for Home, Reservation, and a user account, and a status bar at the bottom.

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

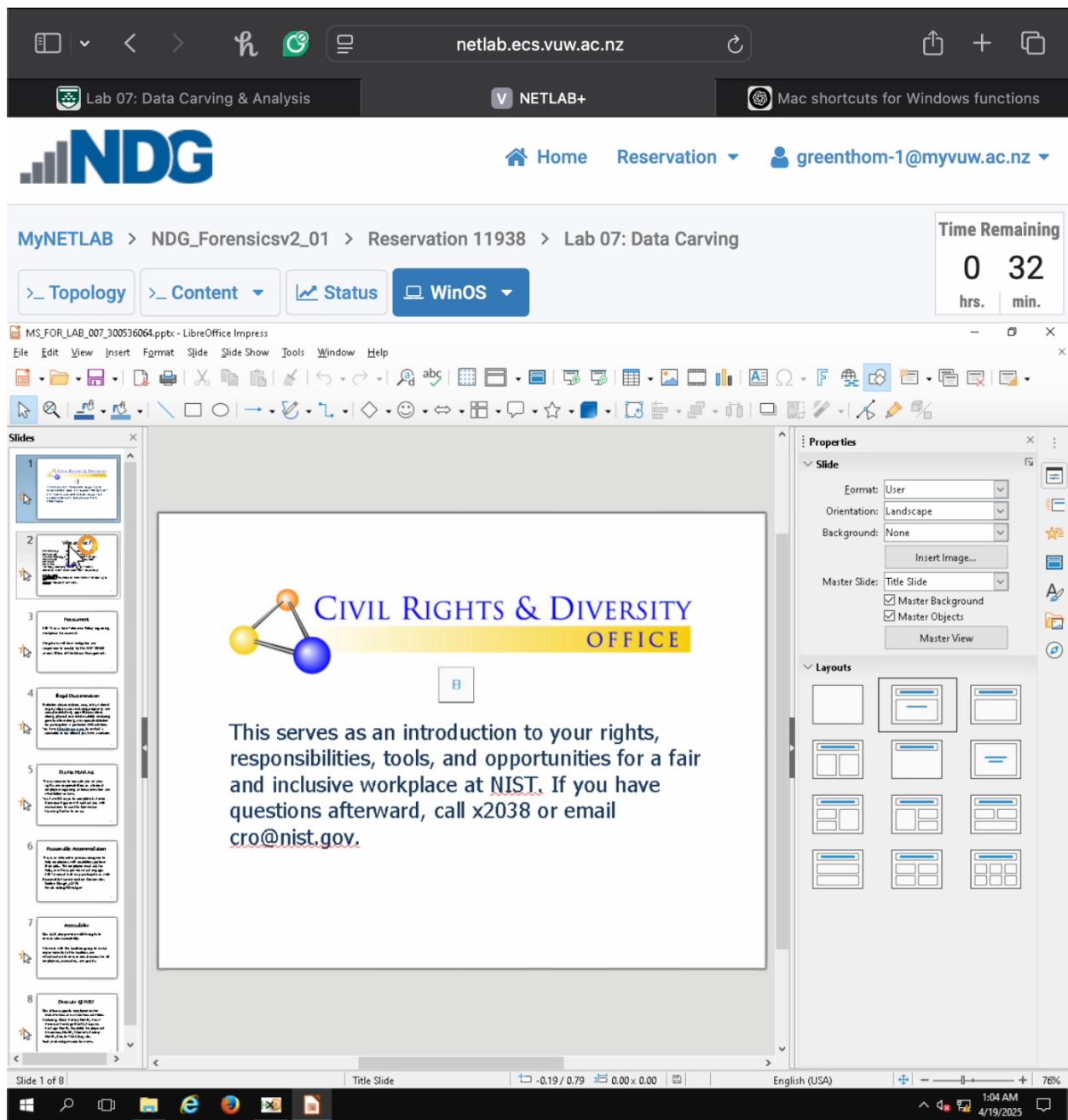


### 3) MS Office Document Carving (10 marks)

- 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 screenshot shows the MyNETLAB interface for Lab 07: Data Carving & Analysis. The main window displays the results of a data carving operation on reservation 11938. The status bar indicates the time remaining is 0 hours and 36 minutes. The main content area shows a hex dump of the data, with the first few bytes highlighted in red (50 4B 03 04). The 'Data inspector' panel on the right provides detailed information about the highlighted bytes, including binary values, offsets, and various data types like Int8, UInt16, and OLETIME.

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

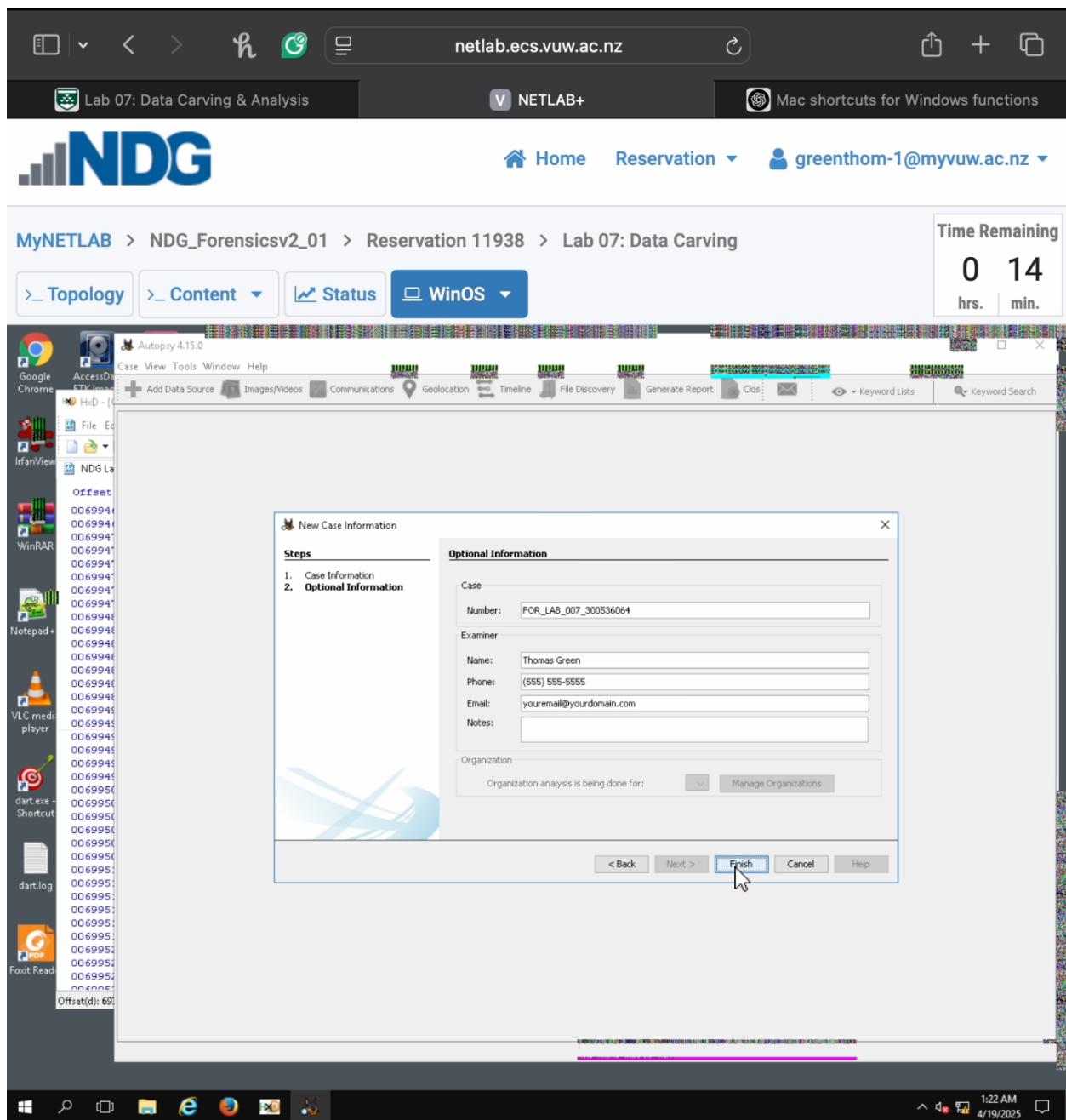


## Part 2: Automated File Carving with Forensic Tools (20 marks)

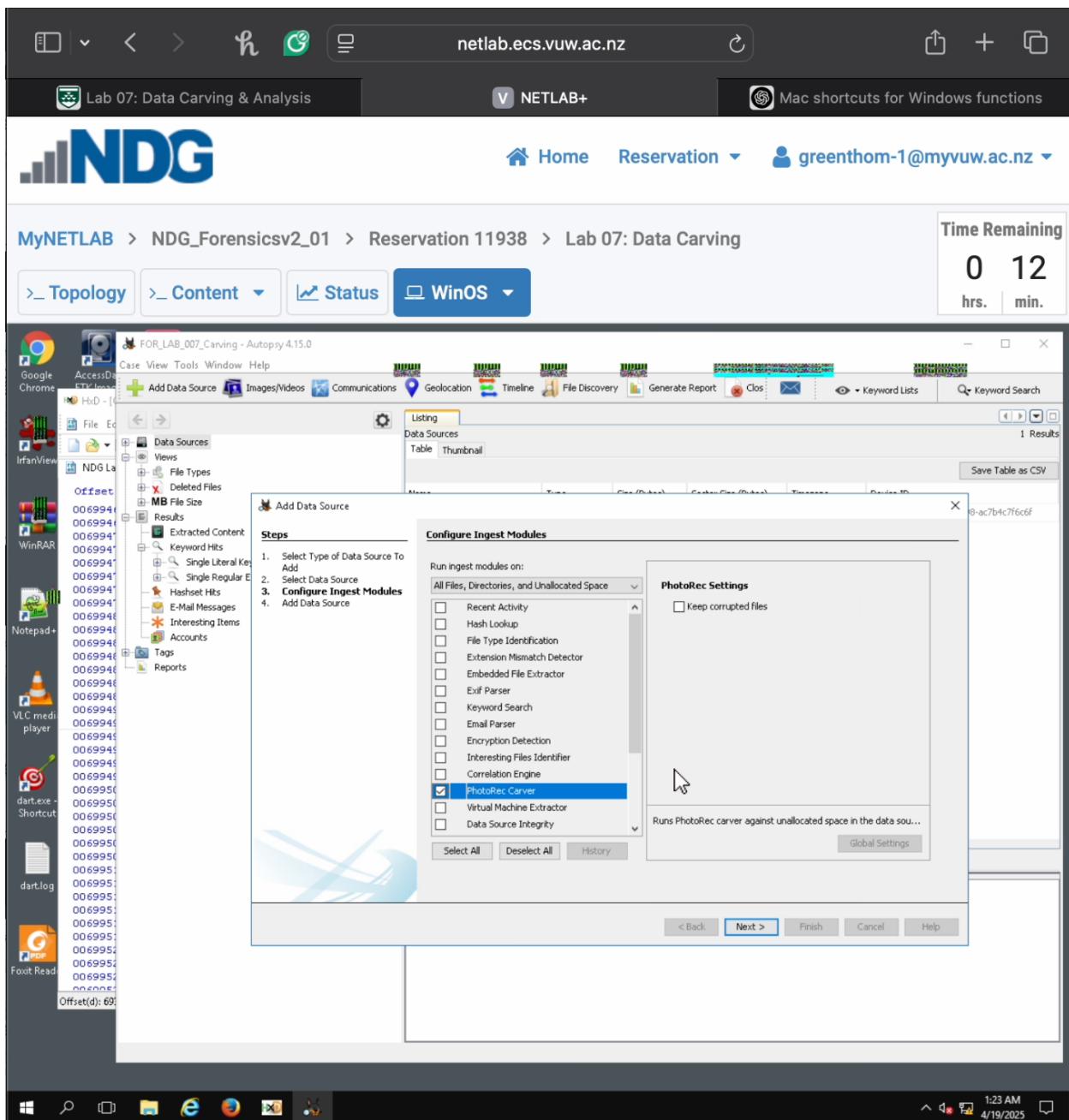
Using Autopsy, you will perform automated file carving and analyze the results.

### 4) Analyzing Carved Files (10 marks)

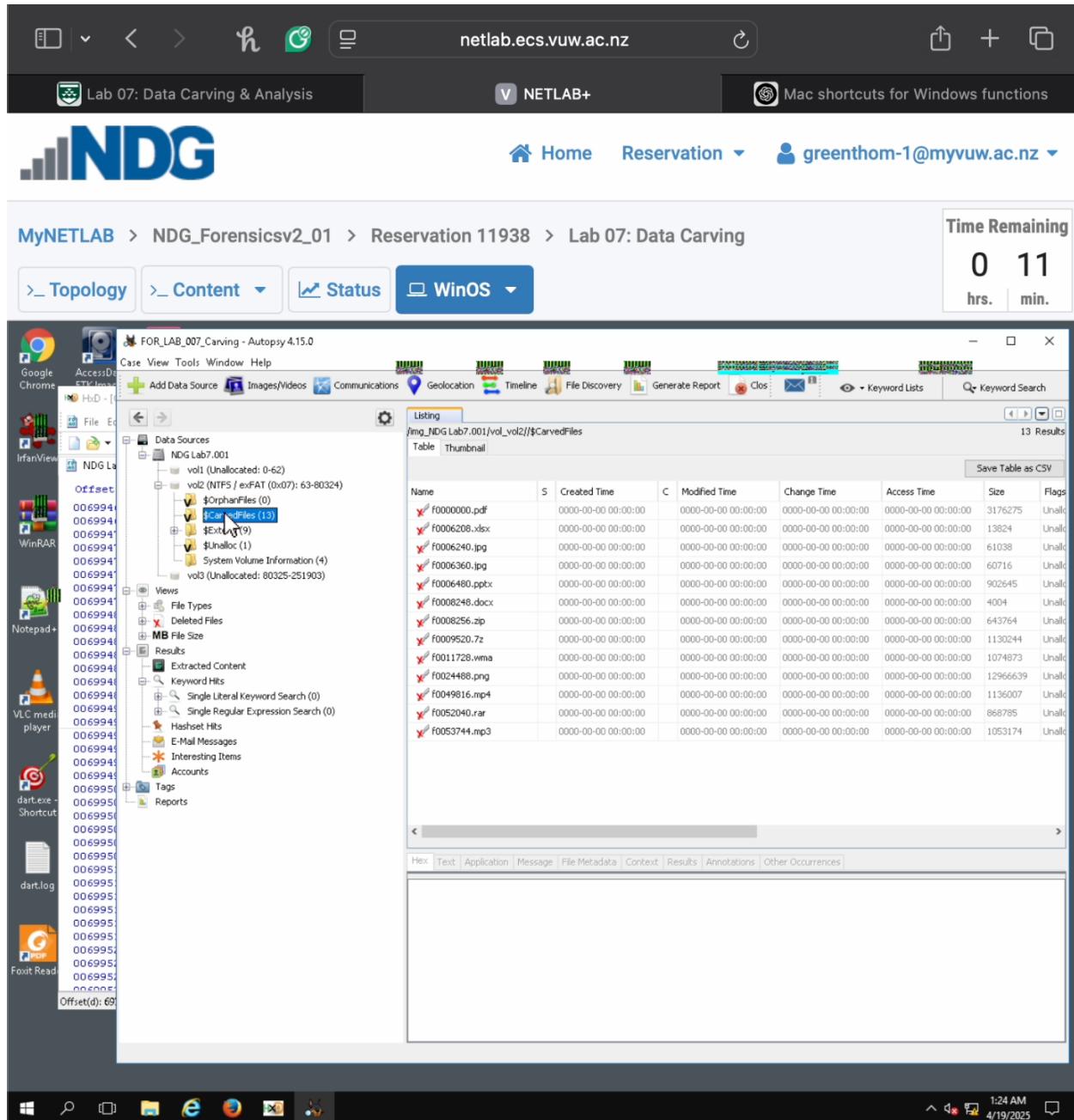
- Create a new case in Autopsy with your name as examiner
- Include your student ID in the case number field (e.g., FOR\_LAB\_007\_12345678)



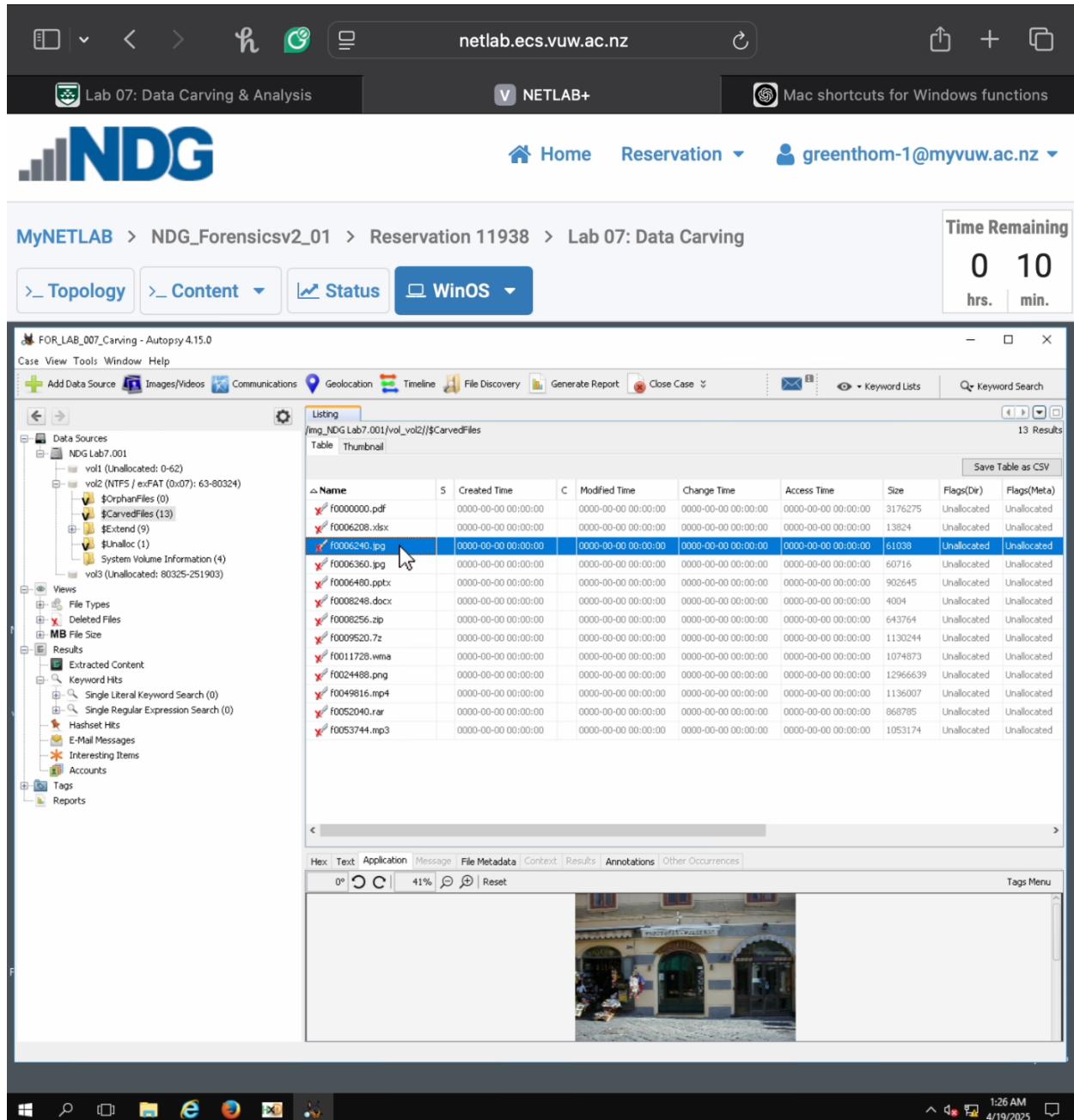
- Add the provided evidence file as a data source
- Configure the PhotoRec Carver Ingest Module



- **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)**

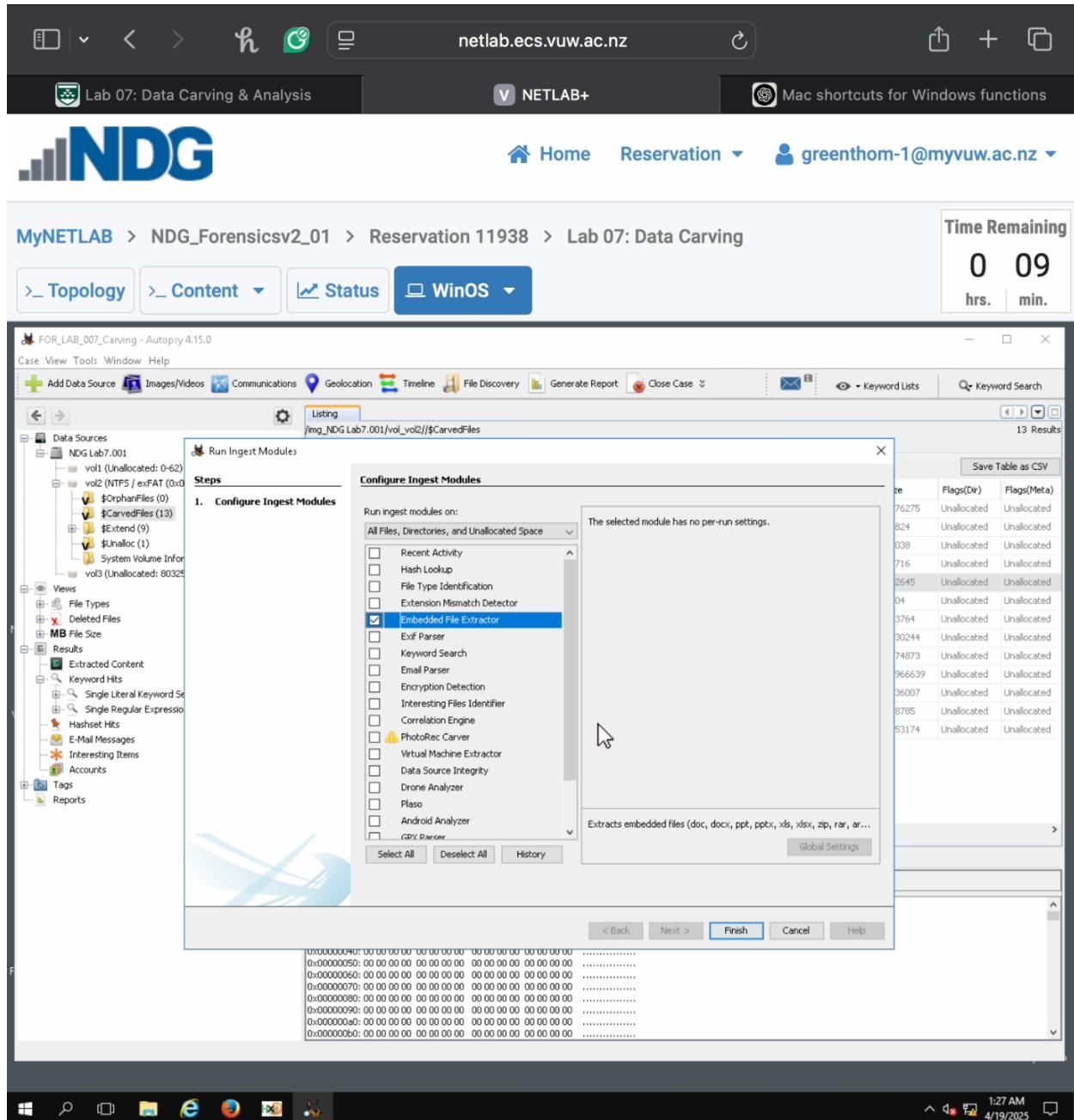


- **Highlight a file that was successfully carved both manually and automatically (step 15.16)**



## 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 08 hrs. 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

Listing /img\_NDG Lab7.001/vol\_vvol2/arc1.7z

Table Thumbnail

Name S C Modified Time Change Time Access Time Created Time Size Flags(Or) Flags

100\_0094.JPG 2004-06-25 00:56:58 GMT-12:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1129134 Allocated Allocated

Data Sources

- NDG Lab7.001
  - vol1 (Unallocated: 0-62)
    - \$OrphanFiles (0)
    - \$CarvedFiles (13)
    - \$Extend (9)
    - \$Unalloc (1)
    - System Volume Information (4)
    - arc1.7z (1)
    - arc6.rar (1)
    - arc7.zip (1)
    - D7.pptx (11)
  - 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

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

1:28 AM 4/19/2025