CYBR472 Lab 06: Keyword Search and Analysis
greenthom – 300536064

Thomas Green – Lab06 – January 1st - 300536064

Assessment Overview

You will be using Autopsy in the case study. You will demonstrate your ability to create cases in Autopsy, perform different types of keyword searches and analyze the results. This lab is worth 6% of your total course grade.

Submission Requirements

- Heading for the report with lab number, birth month, your name and student ID
- Screenshots as indicated (with personalization requirements)
- Only write something when explicitly instructed to do so
- There are 6 questions in total
- Submit as a single PDF document

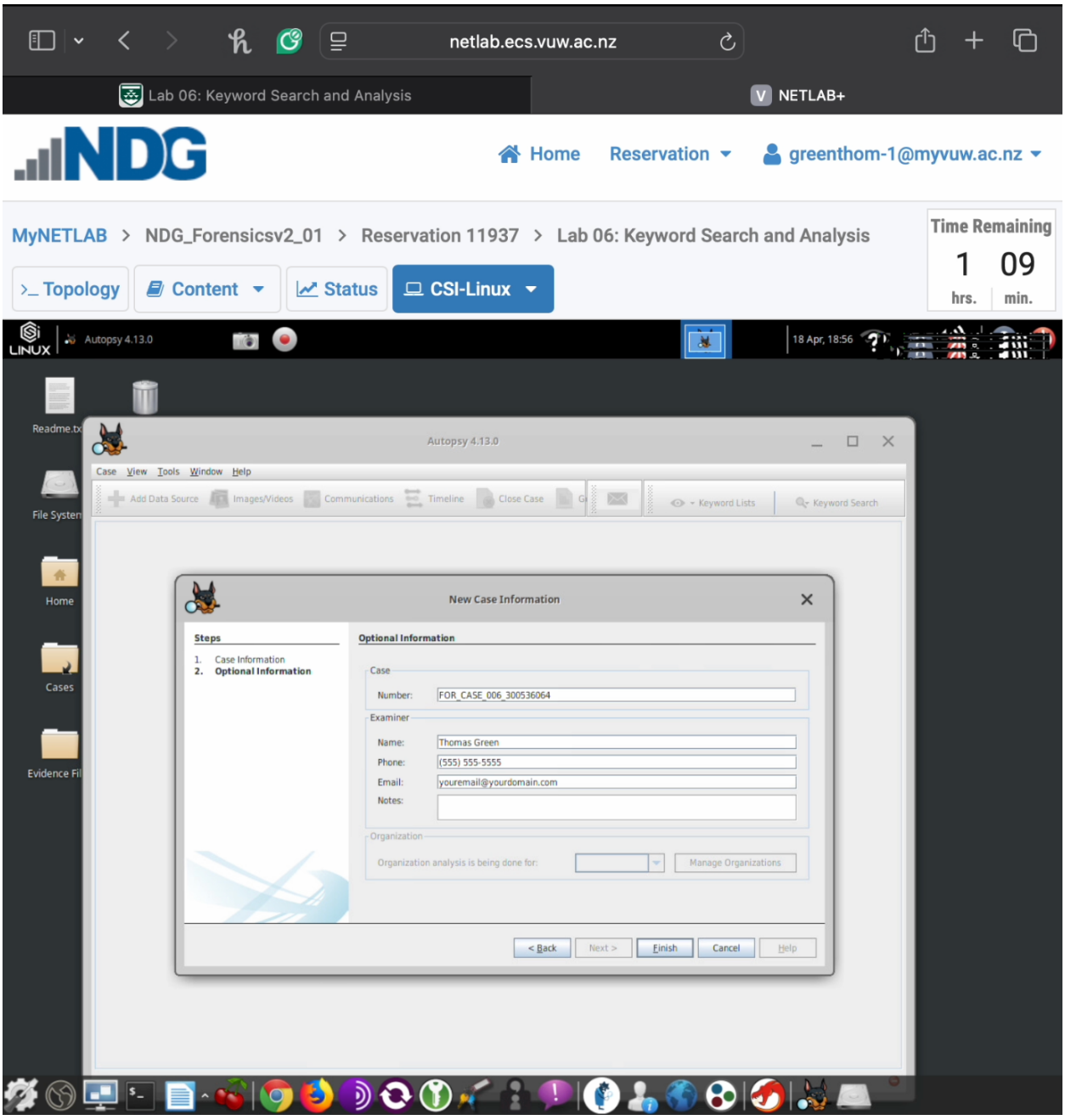
Part 1: Creating a Forensic Case in Autopsy (20 marks)

Complete the lab but when creating your case please:

- Use your full name as the examiner in the Optional Information window
- Include your student ID in the case number field (e.g., FOR_LAB_006_12345678)
- Use the keyword list name "For_LAB_006_[YourLastName]"

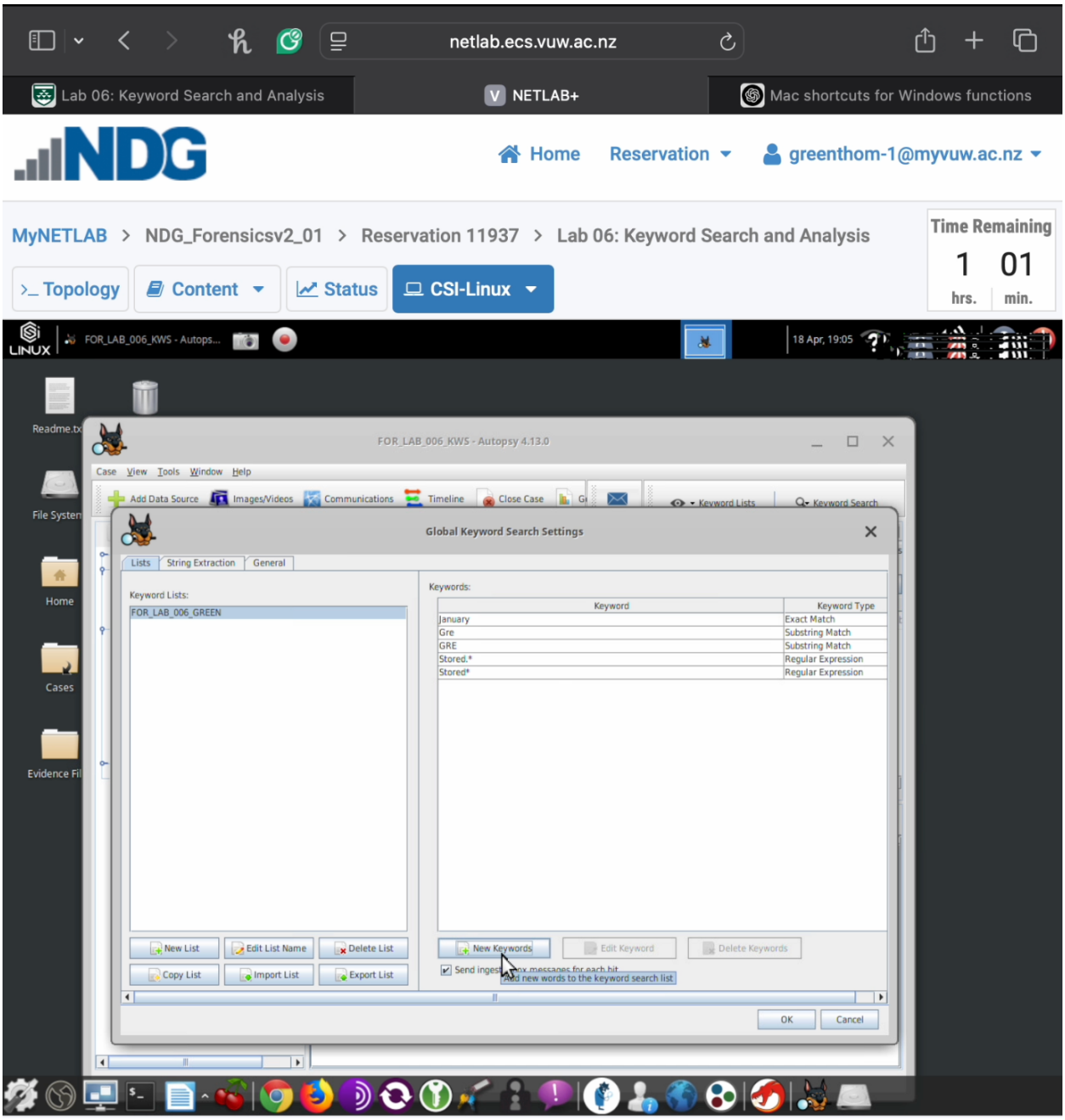
Document your process by providing the following screenshots:

1) Screenshot of step 3 showing your case creation with your name and student ID visible (5 marks)

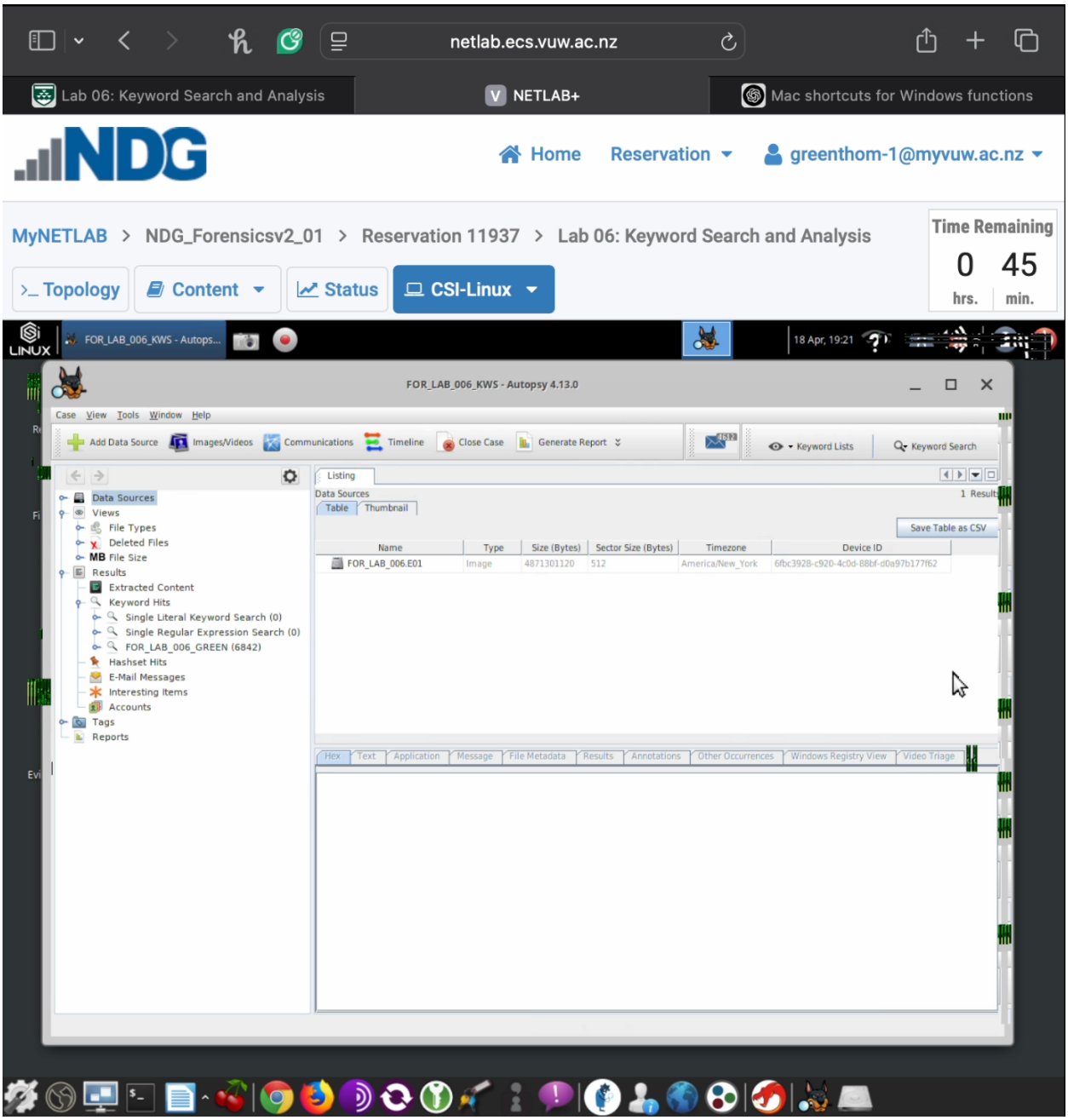


2) Screenshot of step 18 showing your keyboard list creation with the following visibly added keywords (10 marks):

- **Your birth month as an Exact Match term (e.g., “January”)**
- **The first three letters of your last name as a Substring Match term**
- **A Regular Expression search term with the pattern “Stored*”**



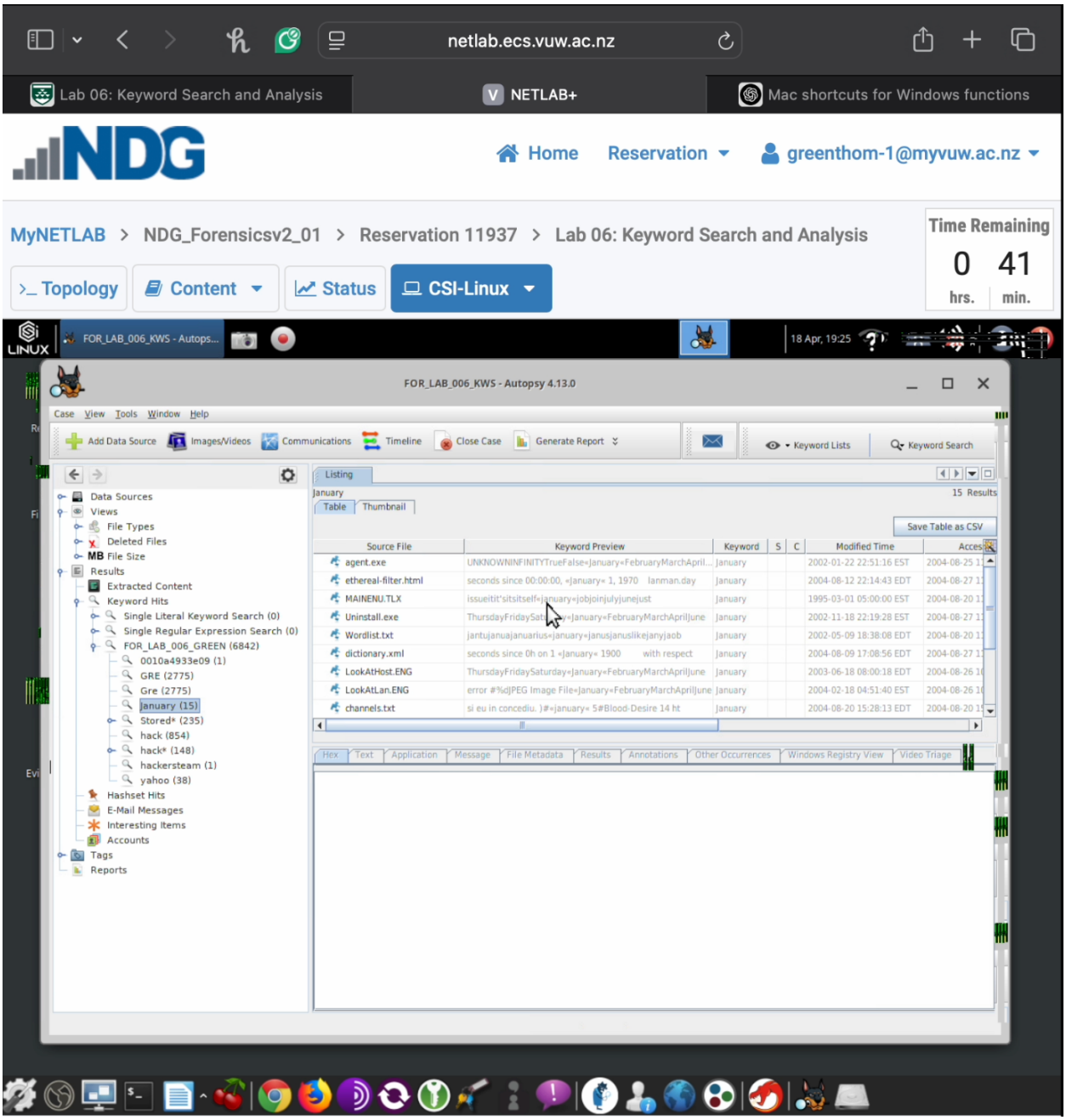
3) Screenshot of step 24 showing Autopsy's successful importing of the evidence file (5 marks)



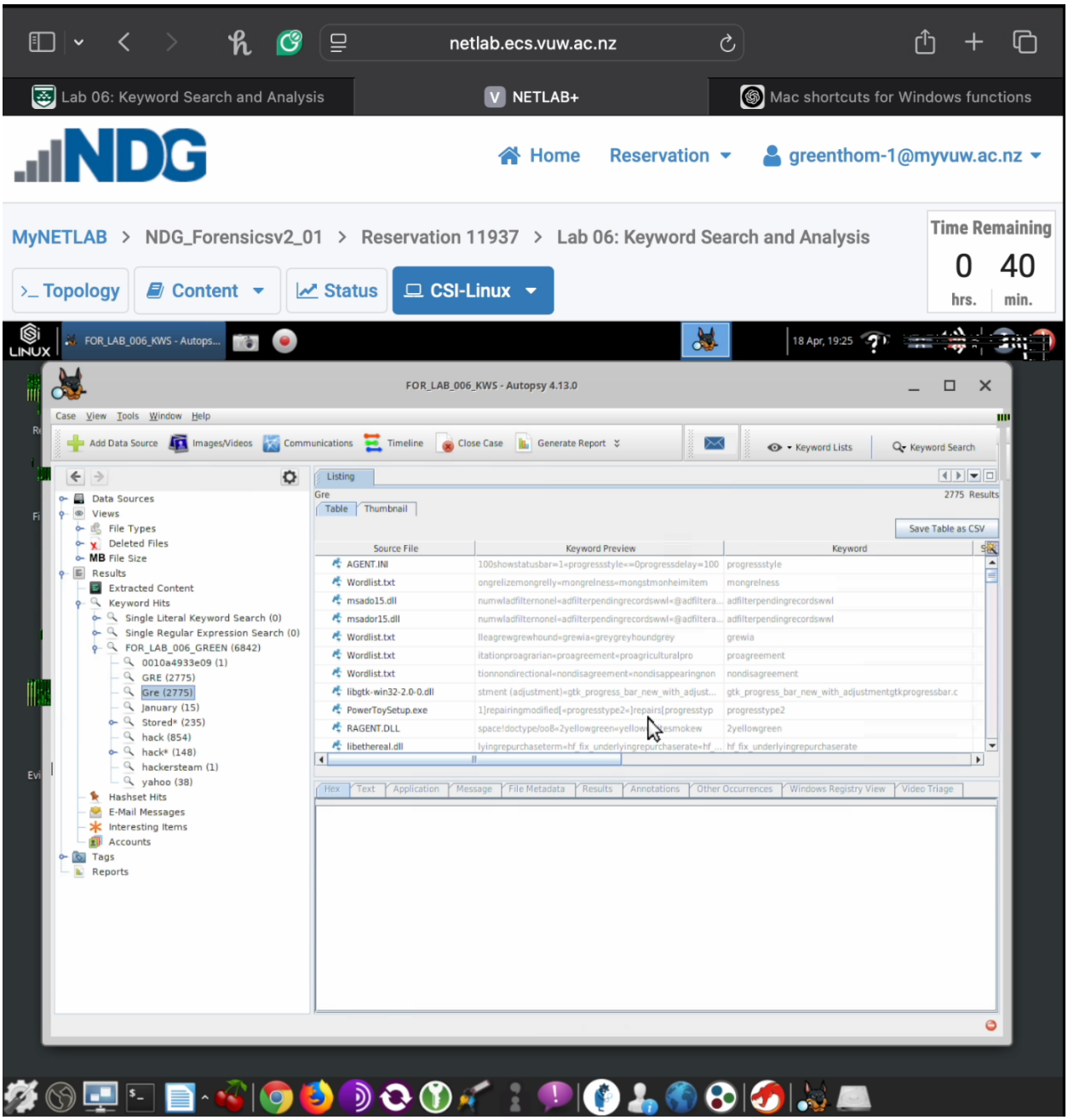
Part 2: Keyword Search Results Analysis (30 marks)

Perform keyword searches with your personalized terms and document your findings:

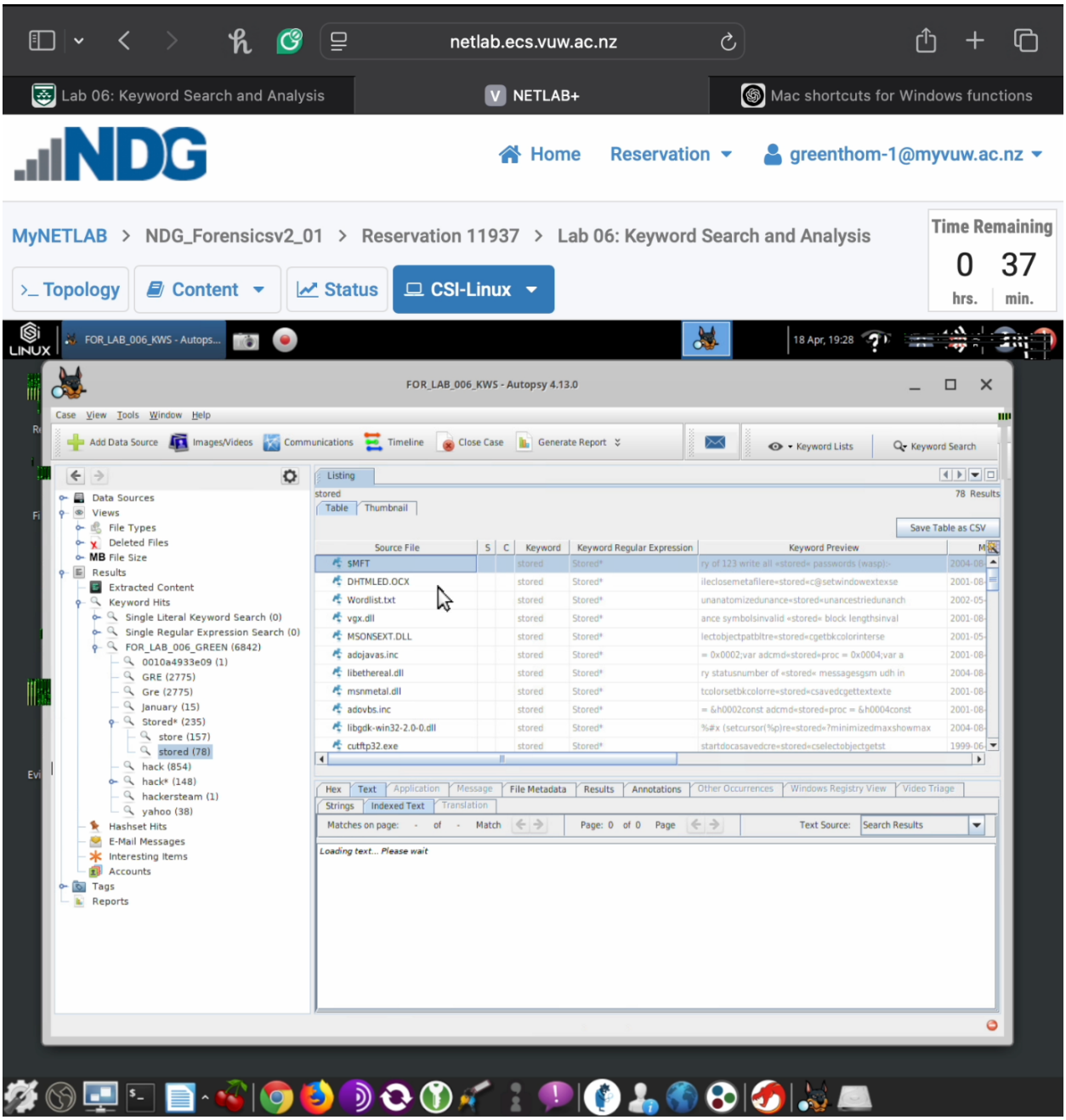
1) Screenshot of step 27 showing search results for your birth month keyword (if no results appear, use “January” instead) (5 marks)



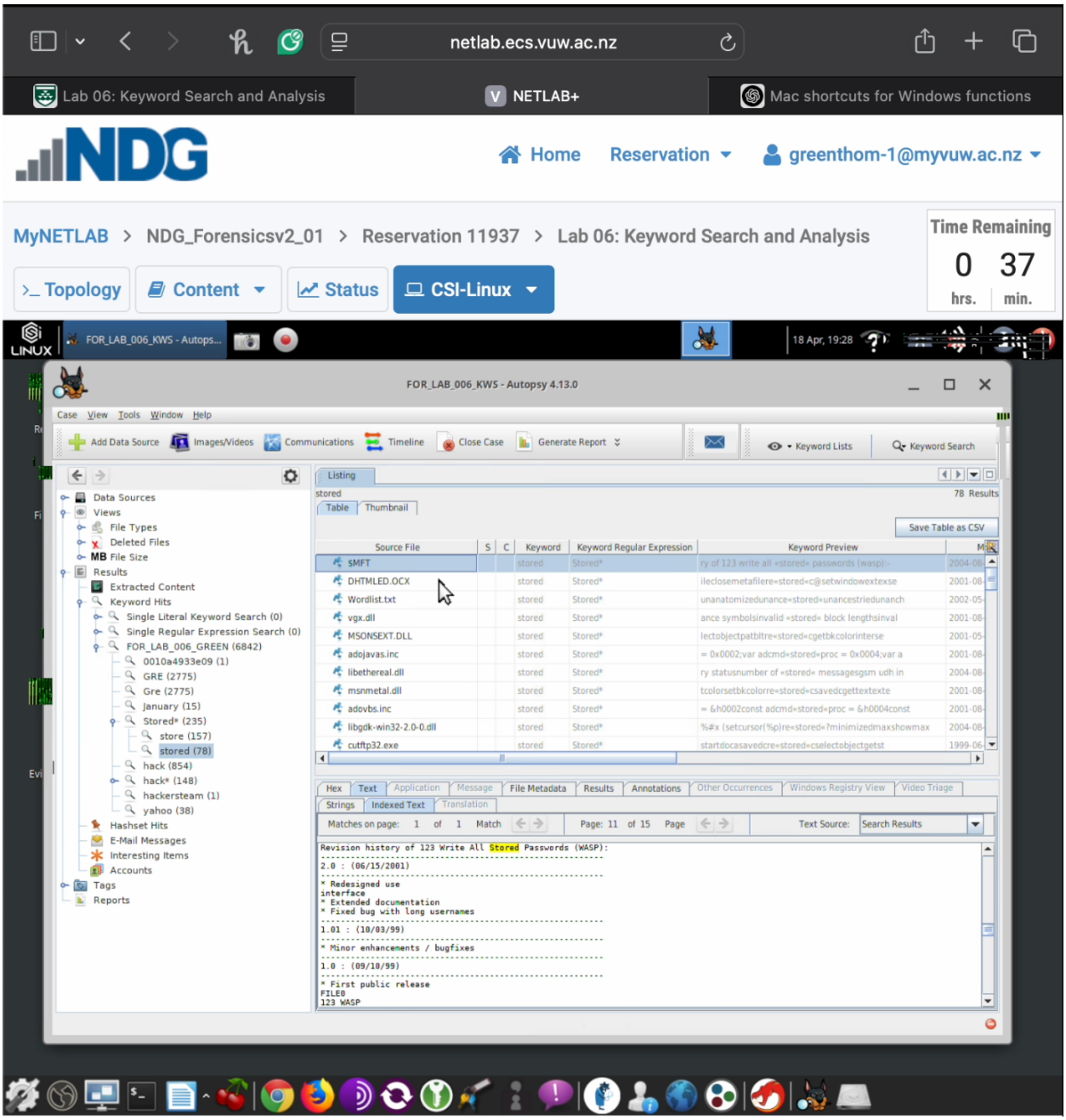
2) Screenshot of step 29 showing search results for your substring match term (if no results appear, use “hack” instead) (5 marks)



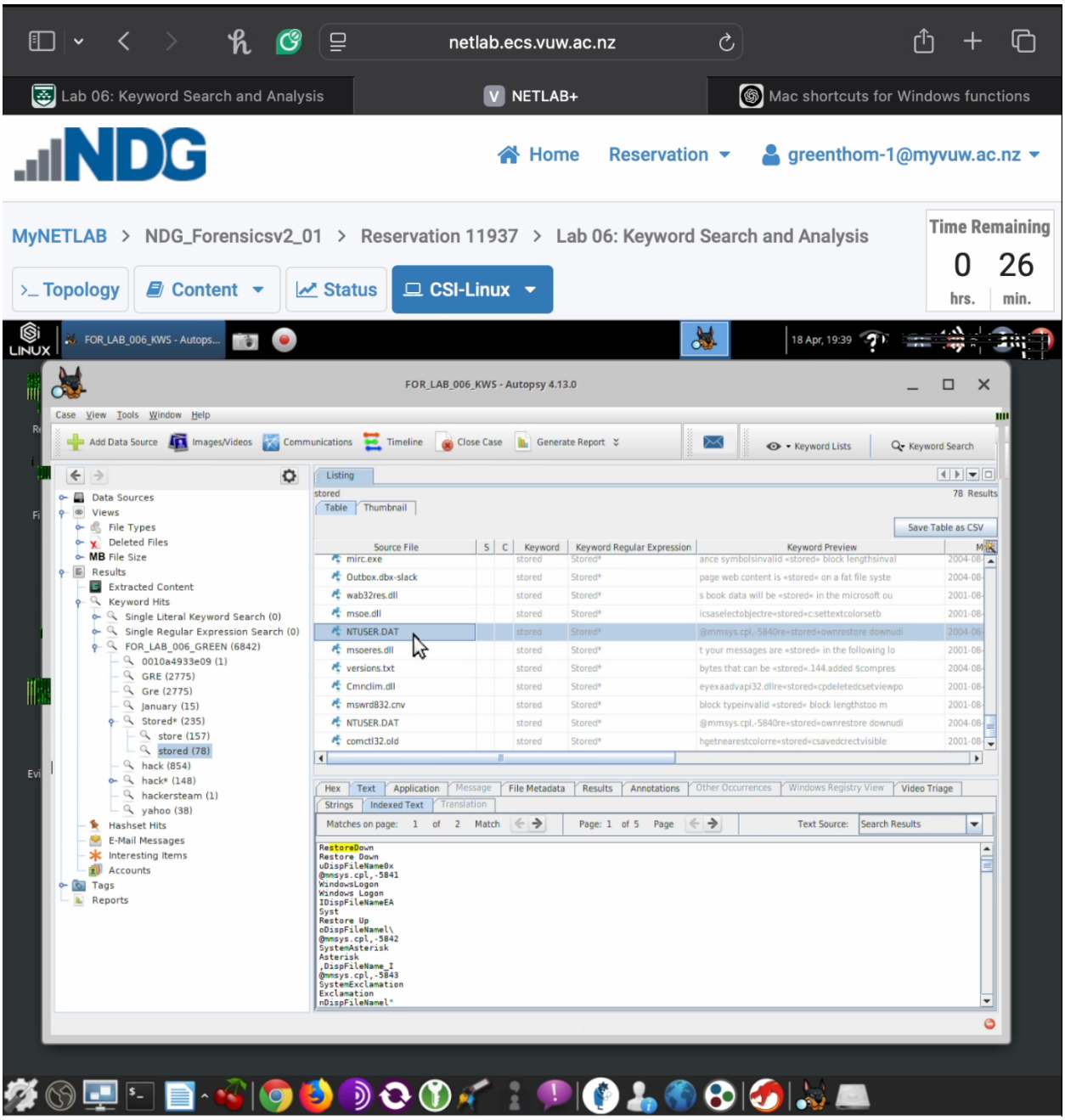
3) Screenshot of step 30 showing search results for your regular expression term (5 marks)



4) Screenshot of step 30 showing the contents of a specific file containing one of your keyword hits (5 marks)

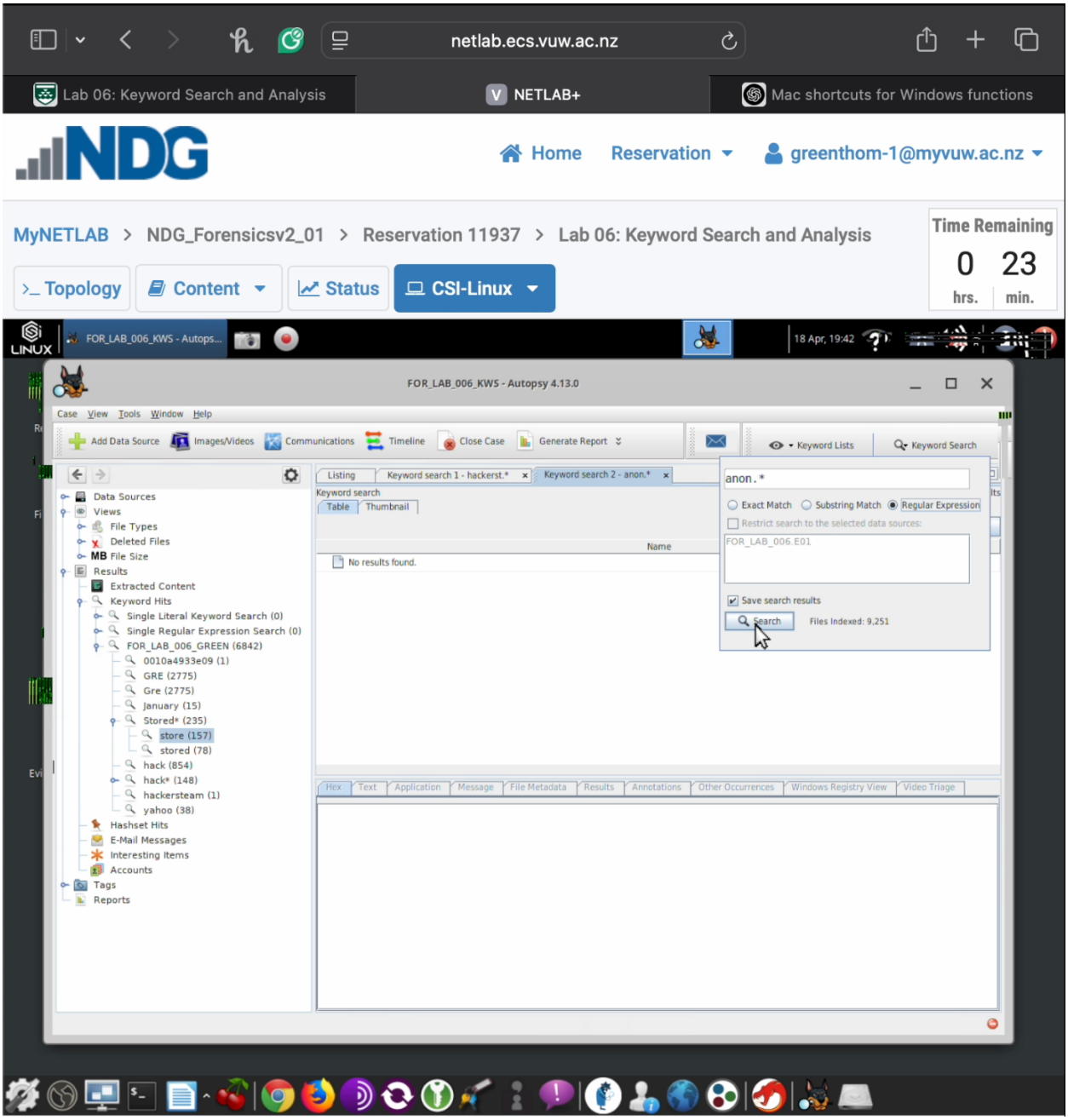


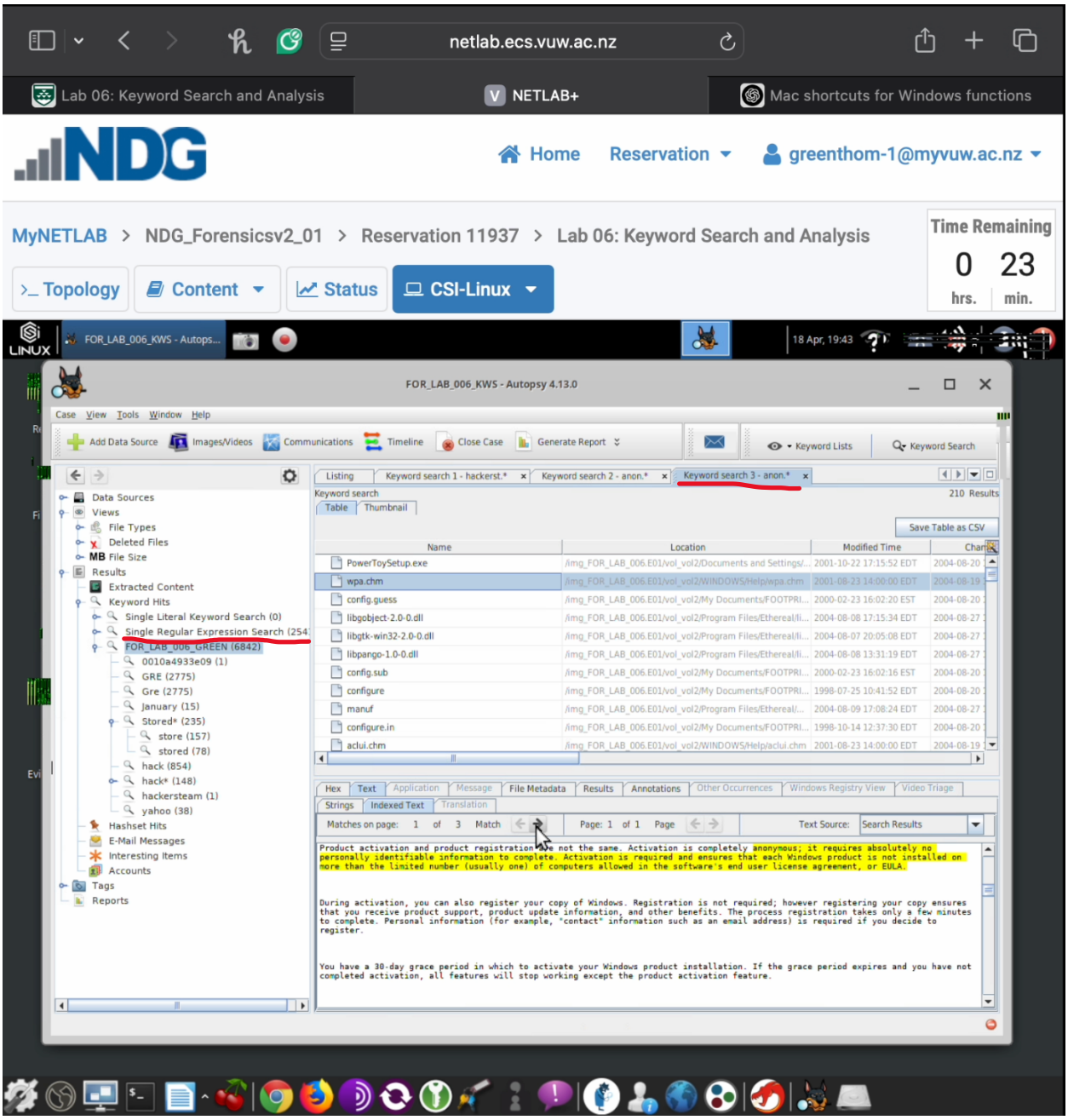
5) Screenshot of step 32 any file content your discovered during your keyword searches and explanation of why the content might be of forensic interest (5 marks)



Discovered a NTUSER.dat file. This file contains critical data such as user preferences, recently accessed files, typed URLs, and program execution history. This helps establish what the user was doing the system. The keyword “stored” is seen in registry-related context which may indicate saved credentials, login sessions, or cached settings, which would be potentially useful in uncovering unauthorized access or tracing user behavior. The .dat file is tied to a specific user profile, its contents can help attribute actions or files to a specific individual, which is crucial in forensic investigations.

6) Provide a screenshot of step 35 of you performing an index search for the term "anon.*" and the results it returns (5 marks)




netlab.ecs.vuw.ac.nz
Lab 06: Keyword Search and Analysis
NETLAB+
Mac shortcuts for Windows functions
NDG
Home
Reservation
greenthom-1@myvuw.ac.nz
MyNETLAB > NDG_Forensicsv2_01 > Reservation 11937 > Lab 06: Keyword Search and Analysis
Time Remaining
0 hrs. 23 min.
Topology
Content
Status
CSI-Linux
FOR_LAB_006_KWS - Autopsy 4.13.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Search
Data Sources
Views
File Types
Deleted Files
File Size
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (254
FOR_LAB_006_GREEN (6842)
0010a4933e09 (1)
GRE (2775)
Gre (2775)
January (15)
Stored* (235)
store (157)
stored (78)
hack (854)
hack* (148)
hackersteam (1)
yahoo (38)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Keyword search 1 - hackerst.*
Keyword search 2 - anon.*
Keyword search 3 - anon.*
Keyword search
210 Results
Table
Thumbnail
Save Table as CSV
Name
Location
Modified Time
PowerToySetup.exe
wpa.chm
config.guess
libgobject-2.0-0.dll
libgtk-win32-2.0-0.dll
libpango-1.0-0.dll
config.sub
configure
manuf
configure.in
aclui.chm
Hex
Text
Application
Message
File Metadata
Results
Annotations
Other Occurrences
Windows Registry View
Video Triage
Strings
Indexed Text
Translation
Matches on page: 1 of 3 Match
Page: 1 of 1 Page
Text Source: Search Results
Product activation and product registration are not the same. Activation is completely anonymous; it requires absolutely no personally identifiable information to complete. Activation is required and ensures that each Windows product is not installed on more than the limited number (usually one) of computers allowed in the software's end user license agreement, or EULA.
During activation, you can also register your copy of Windows. Registration is not required; however registering your copy ensures that you receive product support, product update information, and other benefits. The process registration takes only a few minutes to complete. Personal information (for example, "contact" information such as an email address) is required if you decide to register.
You have a 30-day grace period in which to activate your Windows product installation. If the grace period expires and you have not completed activation, all features will stop working except the product activation feature.