UMGC Lab

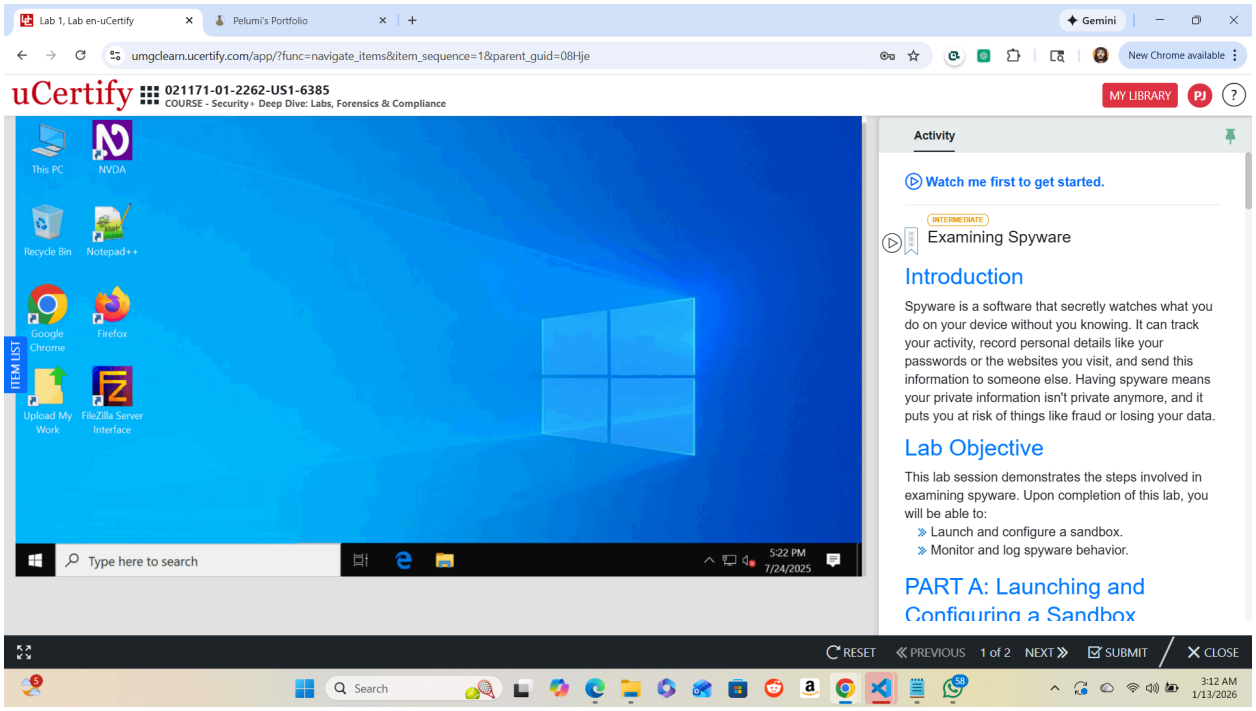
Name: Pelumi Johnson
Date: January 13, 2026
Course: CMIT 320 Network Security
Institution: University of Maryland Global Campus (UMGC)
Lab Title: Examining Spyware

Objective

The objective of this lab was to safely examine and analyze potential spyware behavior using a controlled sandbox environment. The lab focused on executing a file in isolation, monitoring system and network activity, and determining whether the file exhibited malicious characteristics.

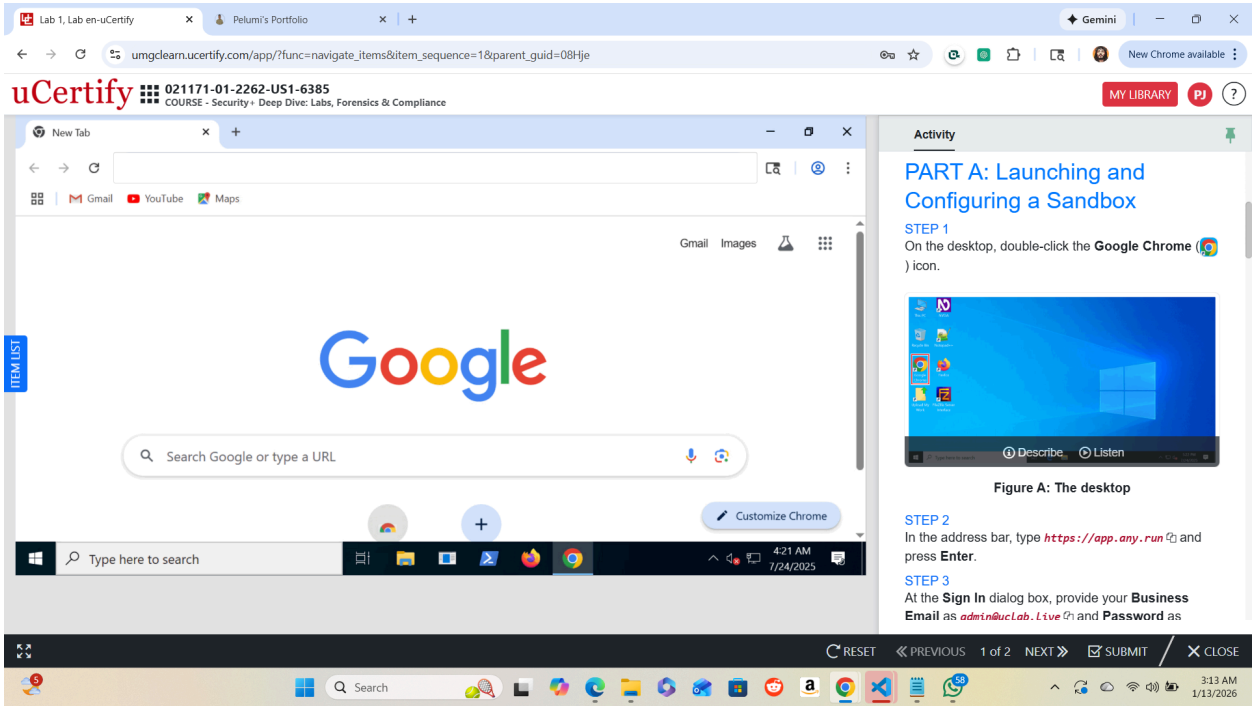
Tools & Environment Used

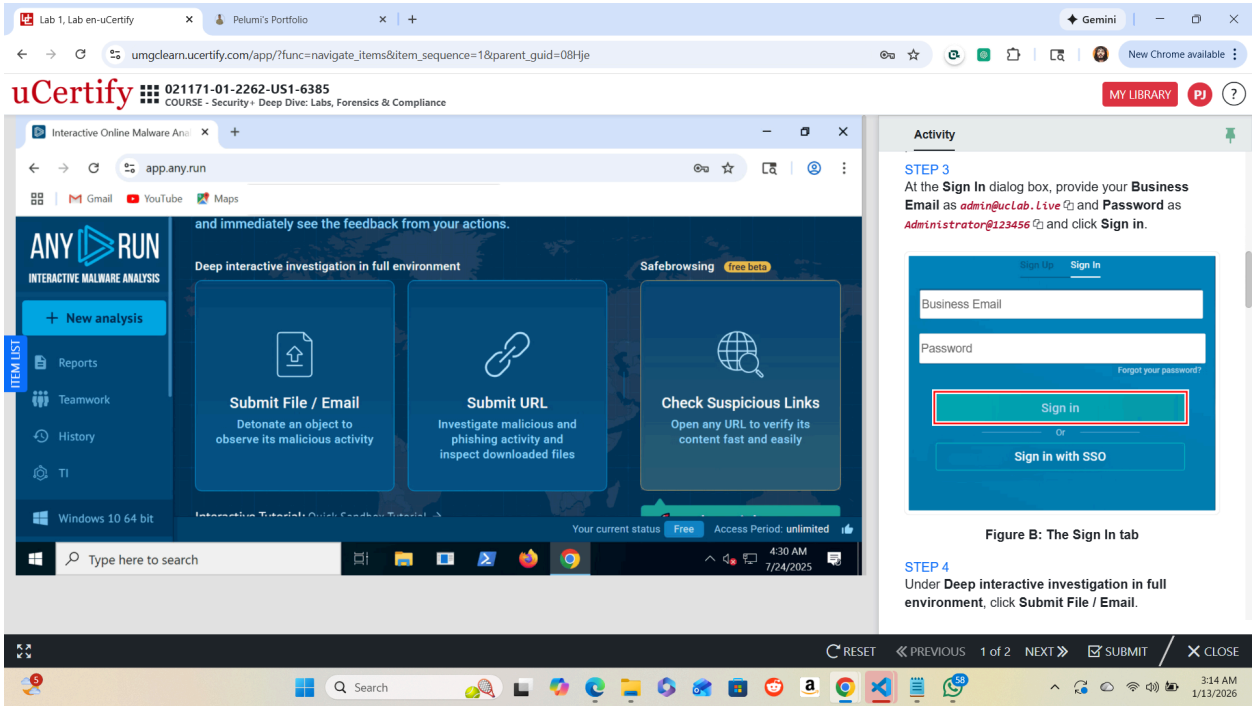
- uCertify Virtual Lab (Windows 10)
- Google Chrome
- ANY.RUN Interactive Malware Analysis Sandbox
- Executable file: write.exe
- Monitoring components:
    - Process tree
    - Child processes
    - HTTP requests
    - Network activity

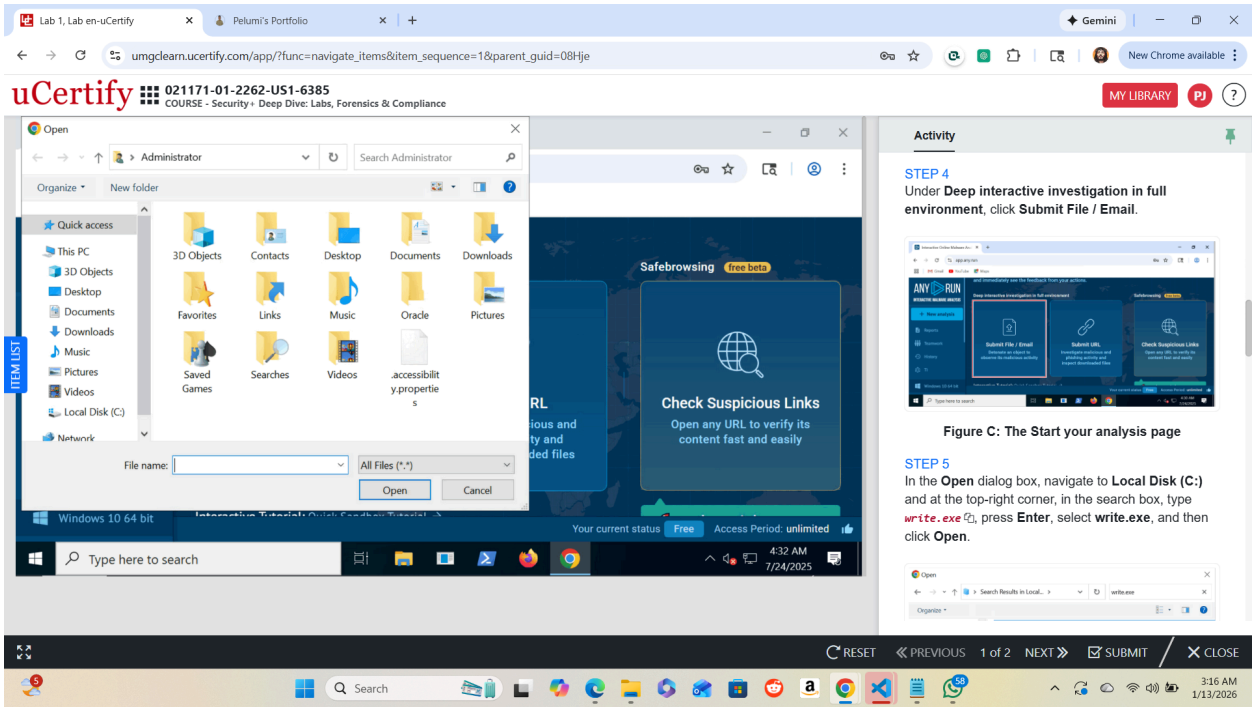


Step 1: Launching and Configuring the Sandbox

I launched Google Chrome from the virtual Windows desktop and navigated to **https://app.any.run**. Using the provided credentials, I signed into the ANY.RUN platform. From the Deep Interactive Investigation section, I selected **Submit File / Email** to begin a new analysis.



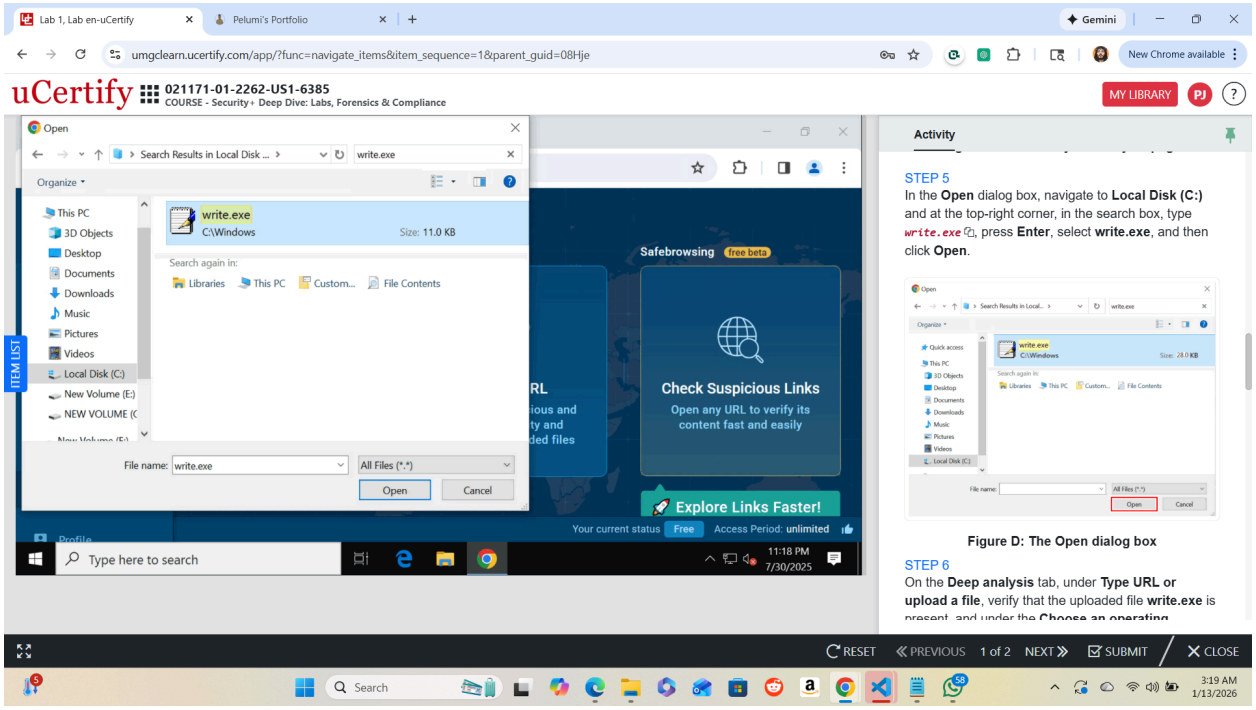

Lab 1, Lab en-uCertify
Pelumi's Portfolio
umgclearn.ucertify.com/app/?func=navigate_items&item_sequence=1&parent_guid=08Hje
uCertify
021171-01-2262-US1-6385
COURSE - Security+ Deep Dive: Labs, Forensics & Compliance
MY LIBRARY
Interactive Online Malware Ana
app.any.run
ANY RUN
INTERACTIVE MALWARE ANALYSIS
and immediately see the feedback from your actions.
Deep interactive investigation in full environment
Safebrowsing free beta
New analysis
Reports
Teamwork
History
TI
Windows 10 64 bit
Submit File / Email
Detonate an object to observe its malicious activity
Submit URL
Investigate malicious and phishing activity and inspect downloaded files
Check Suspicious Links
Open any URL to verify its content fast and easily
Your current status Free Access Period: unlimited
Type here to search
4:30 AM
7/24/2025
ITEM LIST
Activity
STEP 3
At the Sign In dialog box, provide your Business Email as admin@uclab.live and Password as Administrator@123456 and click Sign in.
Sign Up
Sign In
Business Email
Password
Forgot your password?
Sign in
Or
Sign in with SSO
Figure B: The Sign In tab
STEP 4
Under Deep interactive investigation in full environment, click Submit File / Email.
RESET
PREVIOUS
1 of 2
NEXT
SUBMIT
CLOSE
Search
3:14 AM
1/13/2026

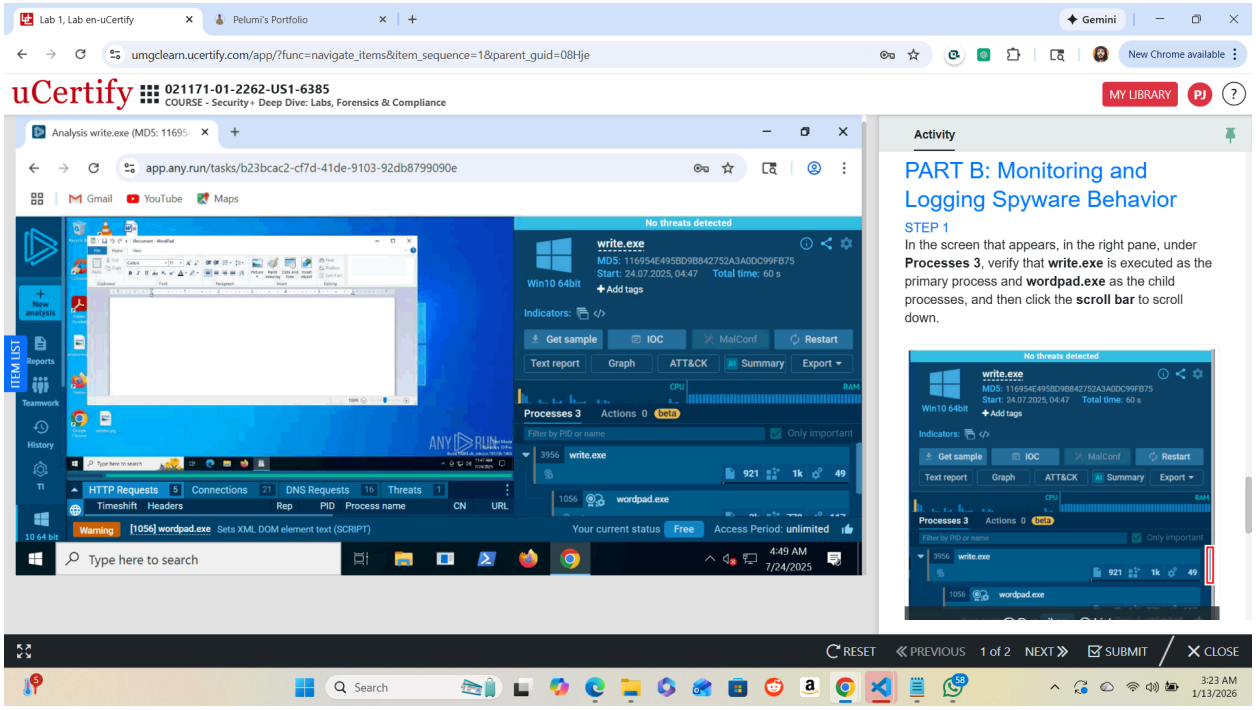

Lab 1, Lab en-uCertify
Pelumi's Portfolio
umgclearn.ucertify.com/app/?func=navigate_items&item_sequence=1&parent_guid=08Hje
uCertify
021171-01-2262-US1-6385
COURSE - Security+ Deep Dive: Labs, Forensics & Compliance
MY LIBRARY
Open
Administrator
Search Administrator
Organize
New folder
Quick access
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
3D Objects
Contacts
Desktop
Documents
Downloads
Favorites
Links
Music
Oracle
Pictures
Saved Games
Searches
Videos
.accessibility.properties
File name:
All Files (*.*)
Open
Cancel
Safebrowsing free beta
Check Suspicious Links
Open any URL to verify its content fast and easily
Windows 10 64 bit
Your current status Free Access Period: unlimited
Type here to search
4:32 AM
7/24/2025
ITEM LIST
Activity
STEP 4
Under Deep interactive investigation in full environment, click Submit File / Email.
Figure C: The Start your analysis page
STEP 5
In the Open dialog box, navigate to Local Disk (C:) and at the top-right corner, in the search box, type write.exe, press Enter, select write.exe, and then click Open.
RESET
PREVIOUS
1 of 2
NEXT
SUBMIT
CLOSE
Search
3:16 AM
1/13/2026

Step 4: Monitoring Processes

During execution, I monitored the **Processes** pane:

- write.exe executed as the primary process.
- wordpad.exe appeared as a child process.
  No additional or suspicious processes were observed during execution.

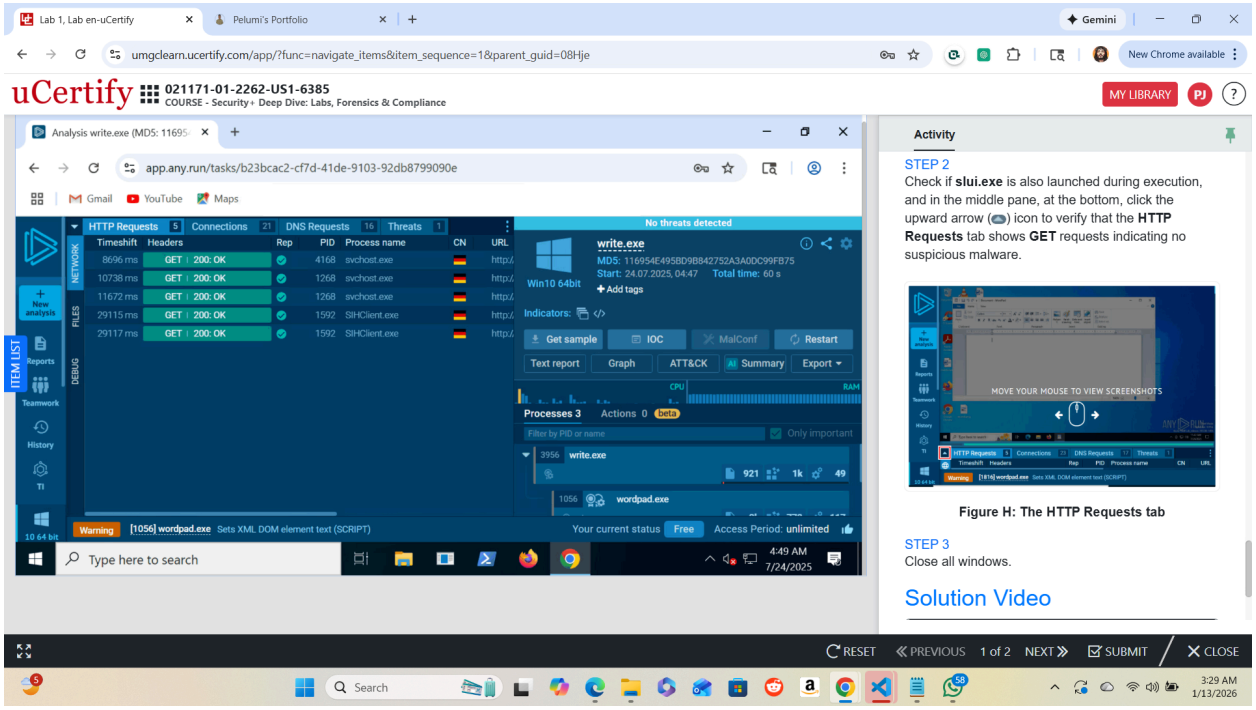




Step 5: Reviewing Network and HTTP Activity

I navigated to the **HTTP Requests** tab to examine network behavior:

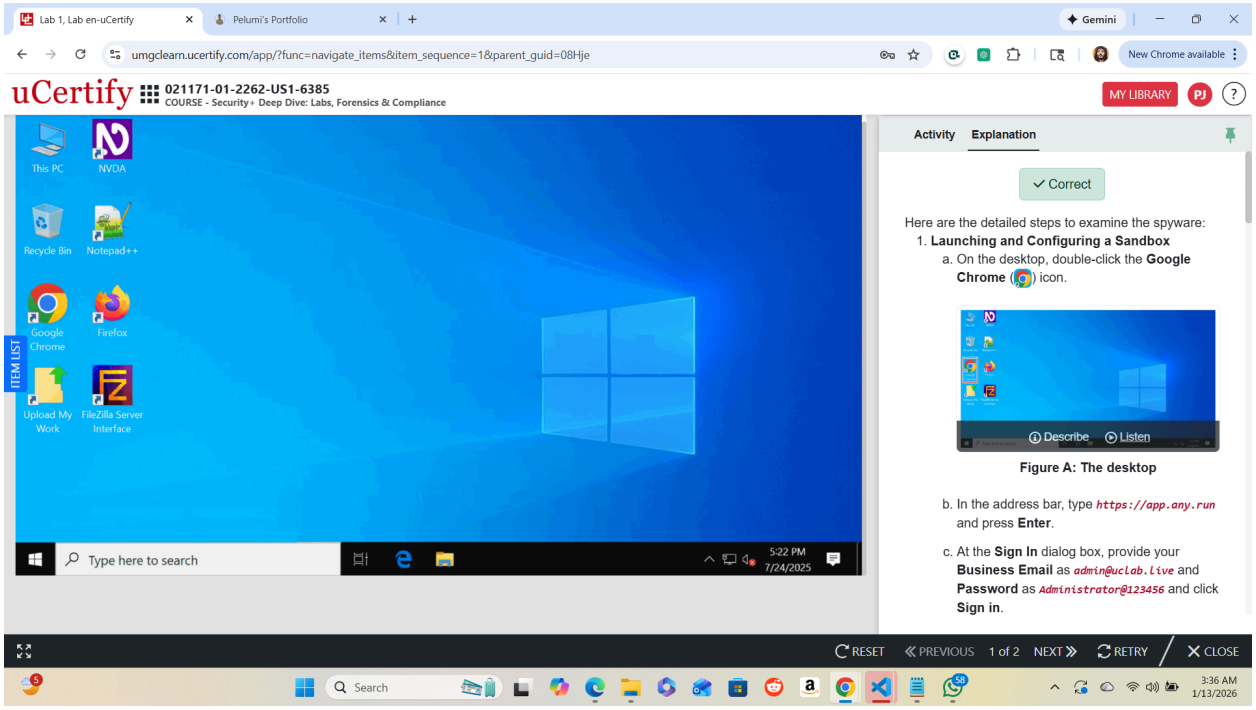
- Multiple GET requests were observed.
- All requests returned **200 OK** responses.
- No suspicious domains, abnormal traffic, or malicious indicators were detected.



Step 6: Analysis Results

Upon completion of the execution, the analysis summary reported:

- **Status:** No threats detected
- **Execution behavior:** Normal
- **Network activity:** Benign
  The file did not demonstrate spyware or malicious behavior.



Conclusion

This lab demonstrated the importance of sandbox environments in malware and spyware analysis. By executing write.exe in an isolated environment, I was able to safely monitor process behavior and network activity without risking a production system. The analysis confirmed that the file did not exhibit spyware characteristics, reinforcing the value of controlled execution and detailed monitoring in cybersecurity investigations.

Key Takeaways

- Sandbox environments are essential for safely analyzing unknown files.
- Process trees help identify legitimate versus suspicious execution behavior.
- Network and HTTP monitoring play a critical role in detecting spyware activity.
- A “no threat detected” result is a valid and meaningful analytical outcome.