

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

Lab 1, Lab en-uCertify

Pelumi's Portfolio

umgclearn.uCertify.com/app/?func=navigate_items&item_sequence=1&parent_guid=08Hj

G Gemini

MY LIBRARY

021171-01-2262-US1-6385

COURSE - Security + Deep Dive: Labs, Forensics & Compliance

This PC

NVIDIA

Recycle Bin

Notepad ++

Google Chrome

Firefox

Upload My Work

FileZilla Server Interface

Type here to search

5:22 PM 7/24/2025

Activity

Watch me first to get started.

Examining Spyware

Introduction

Spyware is a software that secretly watches what you do on your device without you knowing. It can track your activity, record personal details like your passwords or the websites you visit, and send this information to someone else. Having spyware means your private information isn't private anymore, and it puts you at risk of things like fraud or losing your data.

Lab Objective

This lab session demonstrates the steps involved in examining spyware. Upon completion of this lab, you will be able to:

- » Launch and configure a sandbox.
- » Monitor and log spyware behavior.

PART A: Launching and Configuring a Sandbox

RESET PREVIOUS 1 of 2 NEXT SUBMIT CLOSE

3:12 AM 1/13/2026

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.

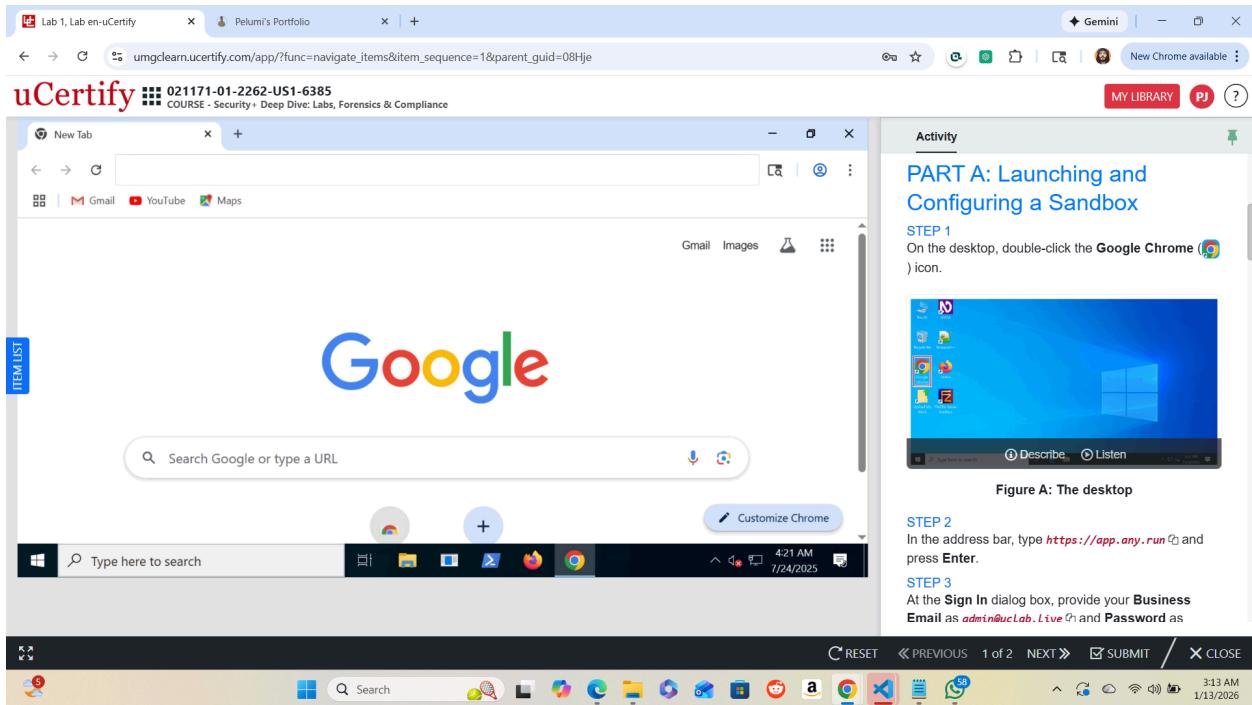


Figure A: The desktop

Lab 1, Lab en-uCertify Pelumi's Portfolio Gemini New Chrome available

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

Interactive Online Malware Analysis

and immediately see the feedback from your actions.

Deep interactive investigation in full environment

Safebrowsing free beta

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

ITEM LIST

Reports Teamwork History TI Windows 10 64 bit Type here to search

Your current status Free Access Period: unlimited 4:30 AM 7/24/2025

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

Sign in with SSO

Figure B: The Sign In tab

Under Deep interactive investigation in full environment, click Submit File / Email.

Lab 1, Lab en-uCertify Pelumi's Portfolio Gemini New Chrome available

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

Open

Administrator Search Administrator

Organize New folder

Quick access This PC 3D Objects Contacts Desktop Documents Downloads Favorites Links Music Oracle Pictures Saved Games Searches Videos Local Disk (C:) Network

File name: All Files (*.*) Open Cancel

Windows 10 64 bit Your current status Free Access Period: unlimited 4:32 AM 7/24/2025

Type here to search

Activity

STEP 4 Under Deep interactive investigation in full environment, click Submit File / Email.

Safebrowsing free beta

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

ITEM LIST

RESET PREVIOUS 1 of 2 NEXT SUBMIT CLOSE

3:14 AM 1/13/2026

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**.

Open

Search Results in Local... write.exe

Organize

RESET PREVIOUS 1 of 2 NEXT SUBMIT CLOSE

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.

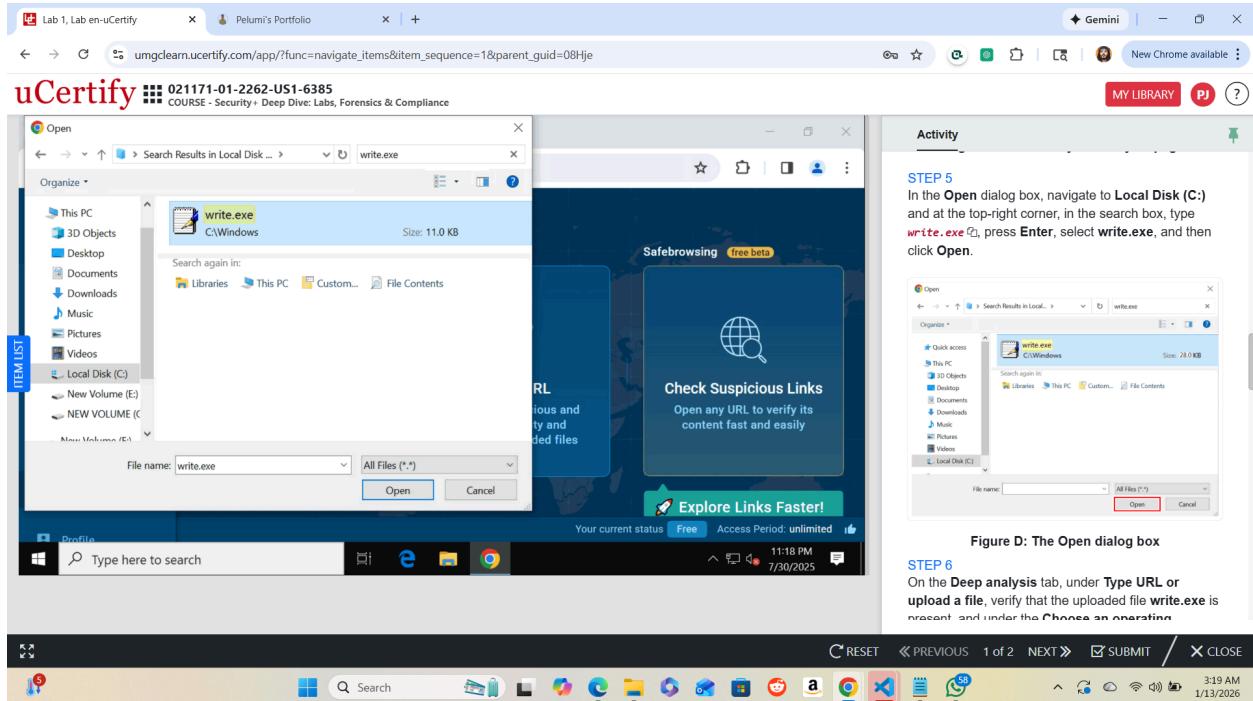


Figure D: The Open dialog box

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.

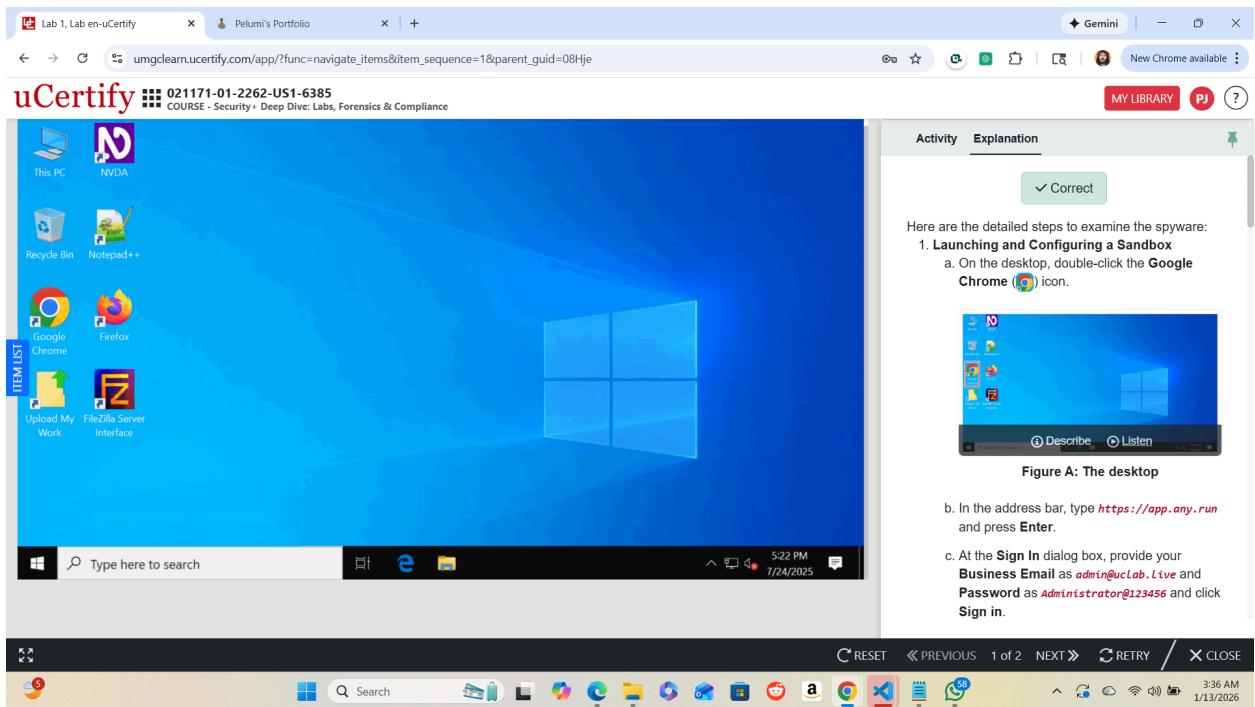
The screenshot shows the uCertify analysis interface for a file named 'write.exe'. The main window displays 'No threats detected' and lists several HTTP requests made by the file. The 'Processes' tab shows three processes: 'write.exe', 'svchost.exe', and 'wordpad.exe'. A warning message for 'wordpad.exe' states: 'Warning [t056] wordpad.exe Sets XML DOM element text (SCRIPT)'. On the right side, there is a sidebar titled 'Activity' with a section for 'STEP 2' which says: 'Check if slui.exe is also launched during execution, and in the middle pane, at the bottom, click the upward arrow (↑) icon to verify that the HTTP Requests tab shows GET requests indicating no suspicious malware.' Below this is a screenshot of the Windows taskbar.

Figure H: The HTTP Requests tab

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.