CYT-250-Threat Investigation

Lab 8- Open IOC format

Elaborate by:

Leandro Delgado

Student Number: 114416241

Professor: Tatiana Outkina

CYT250 Lab8_Winter2025 – OpenIOC format – 4%

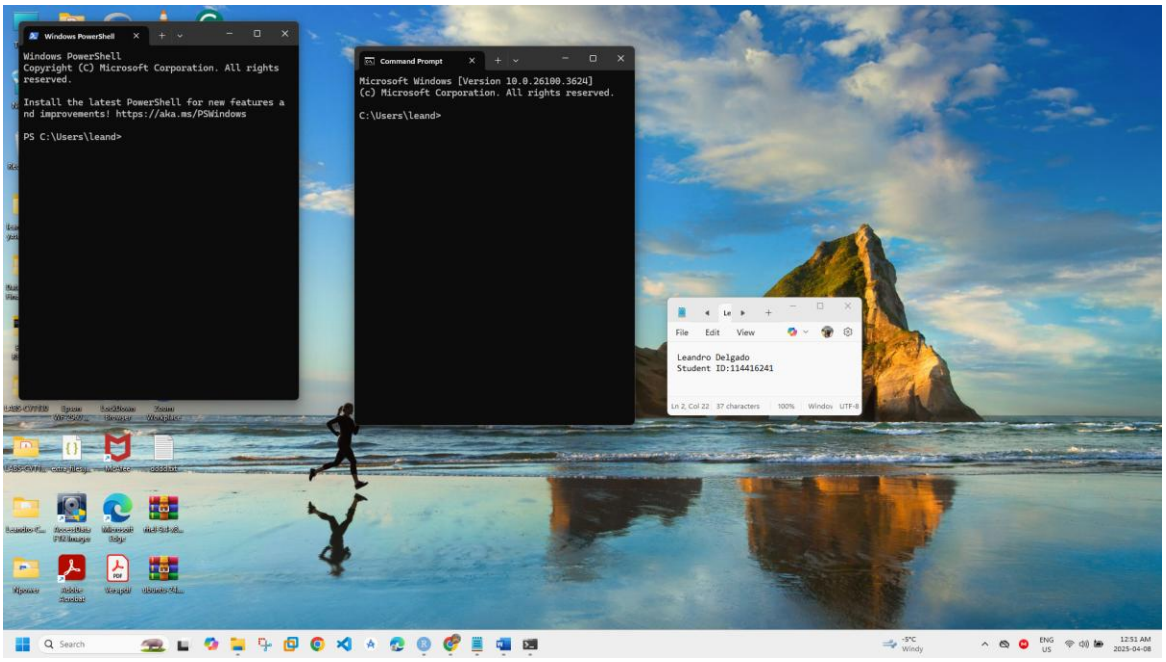

Figure 1. 0 Screen

Task 1.

This screenshot shows the Mandiant IOCe tool (IOC Editor) launched from the Windows Start Menu. It was installed using resources provided by the instructor and will be used to complete the lab tasks involving IOC creation and comparison. A notepad with my name and student number is included for identification.

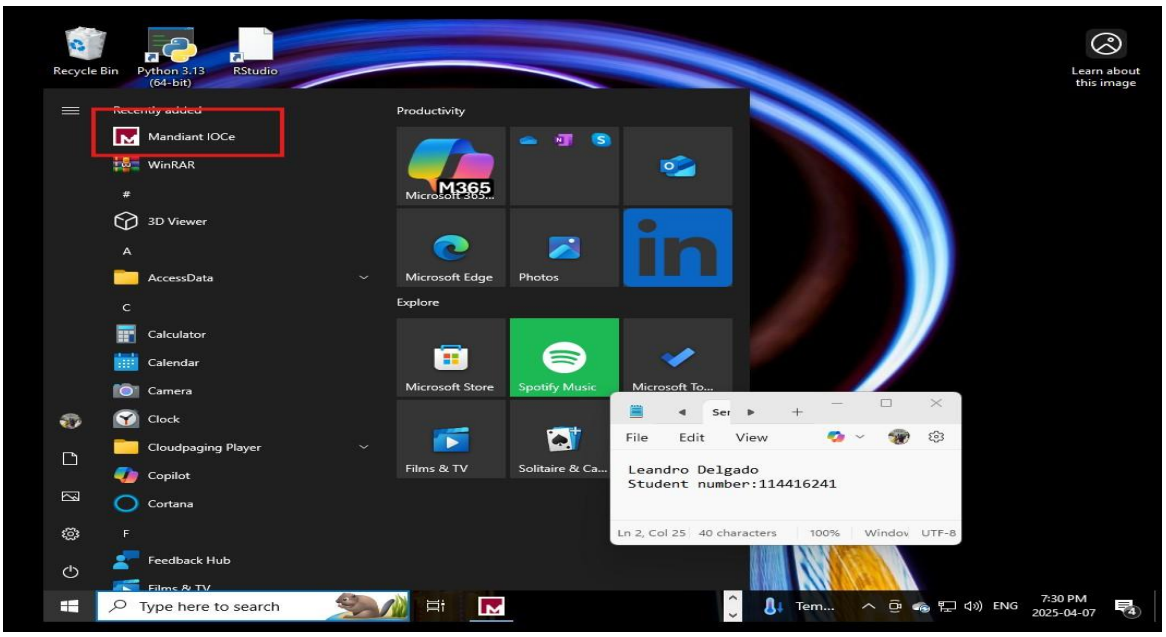

Figure 2. Installation of IOC tool.

Task 2.

2.1. Familiarize yourself with the capabilities of IOC Editor.

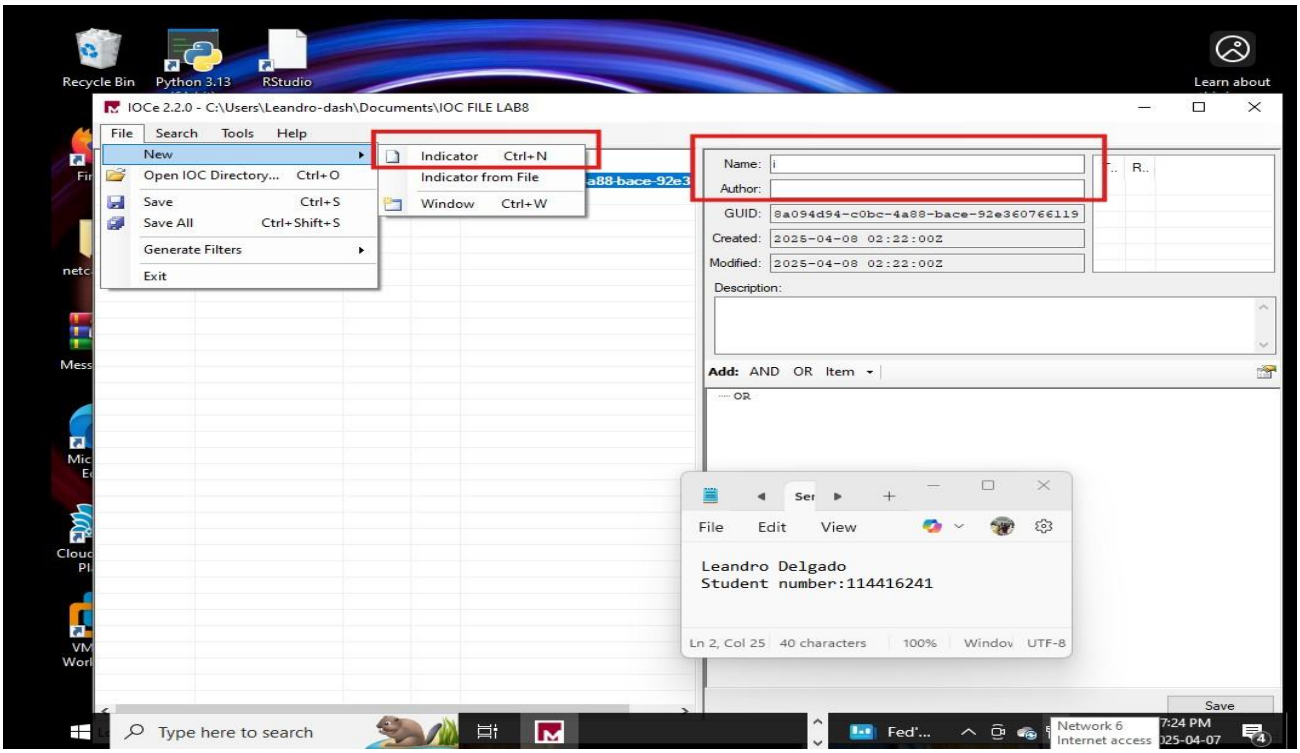

Figure 3. Exploring IOC Environment

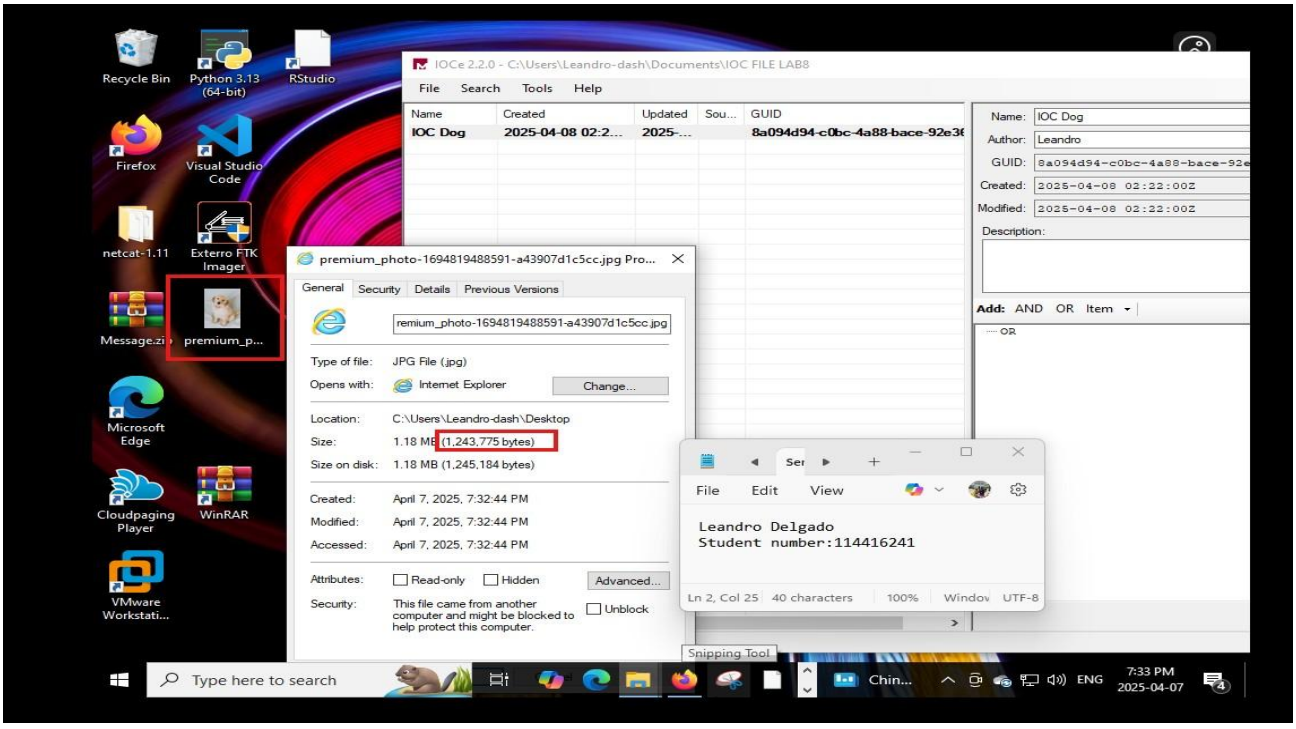

Figure 4. Exploring IOC Environment

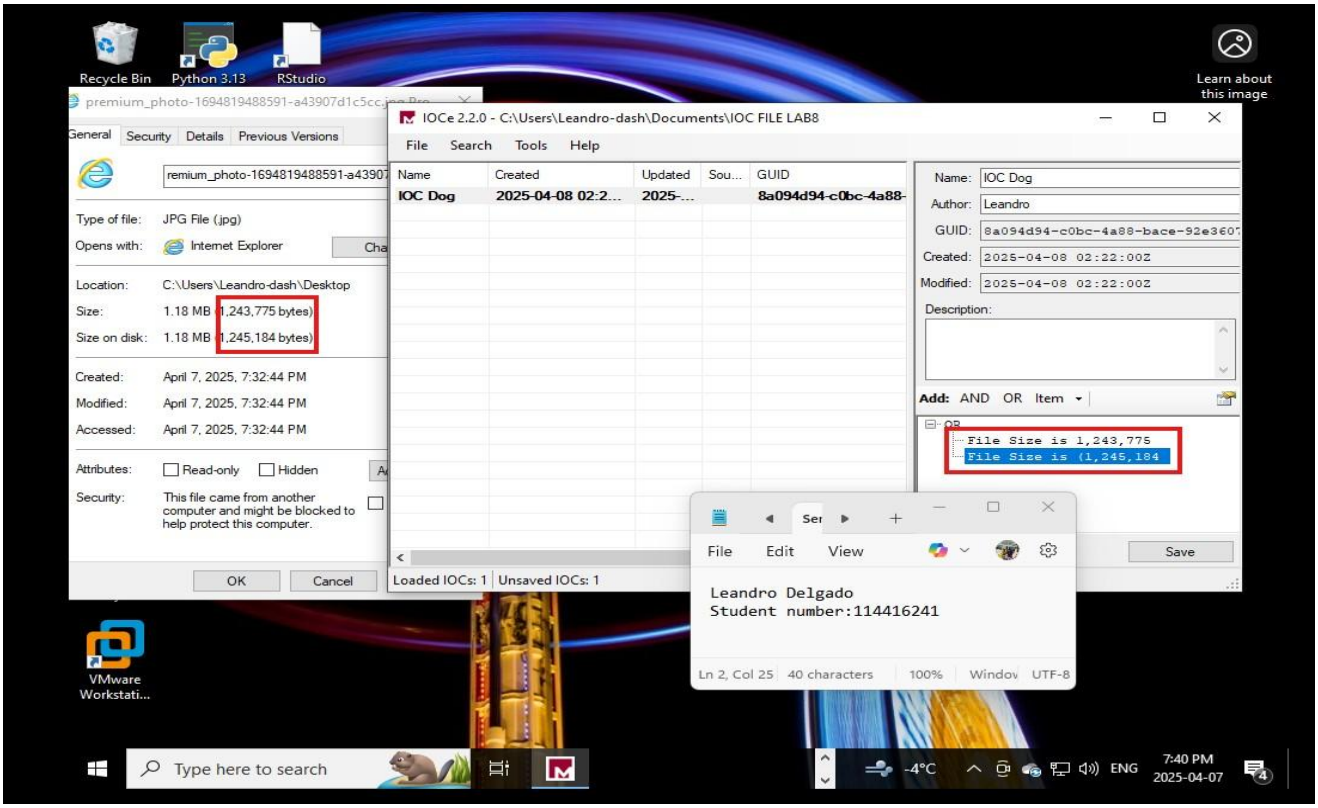

Figure 5. Exploring IOT Environment

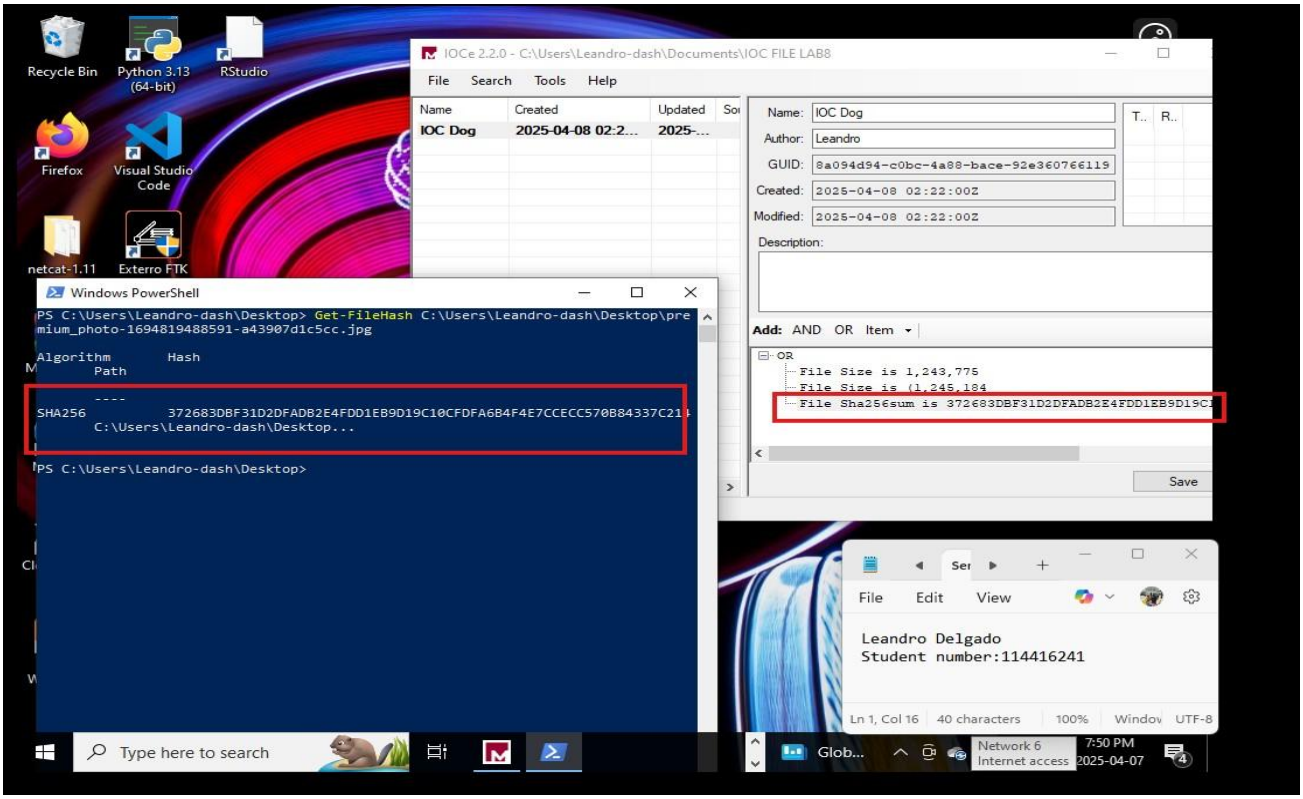

Figure 6.Exploring IOC Environment

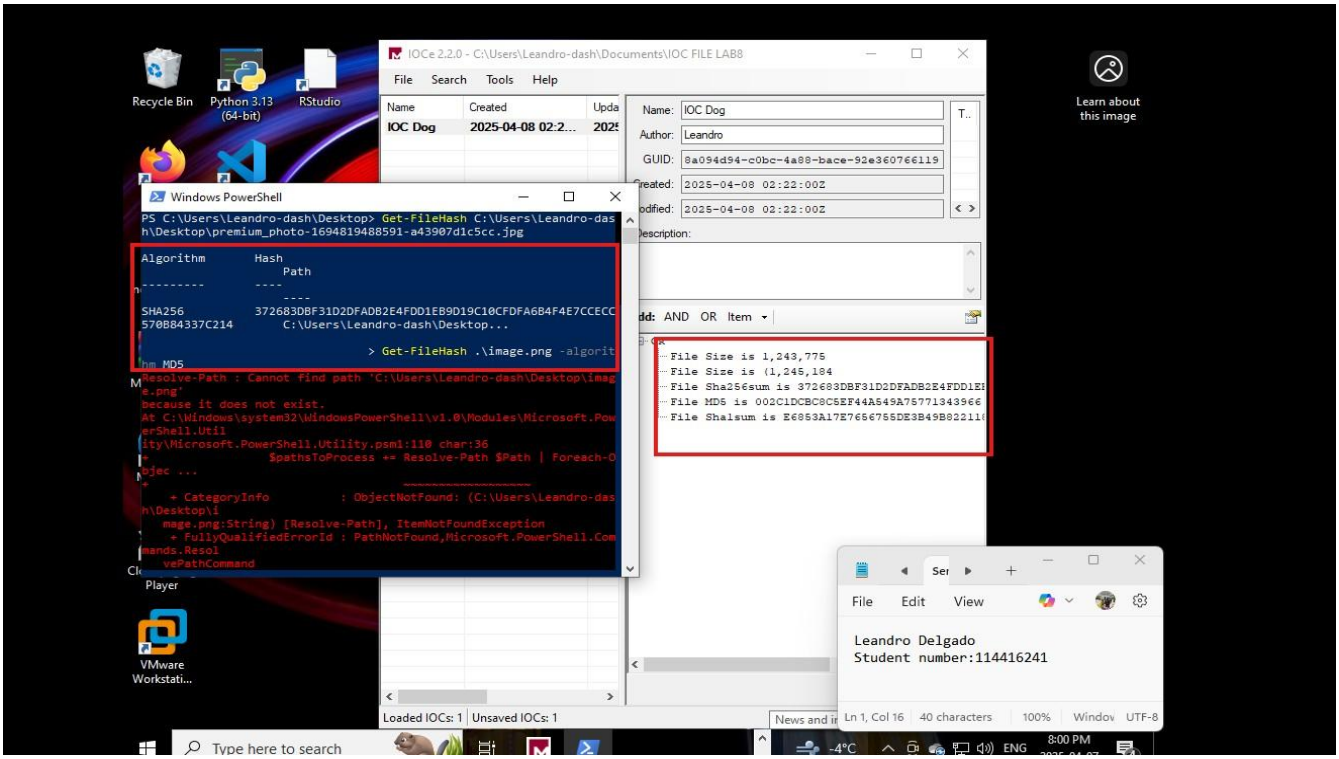

Figure 7. Exploring IOC Environment

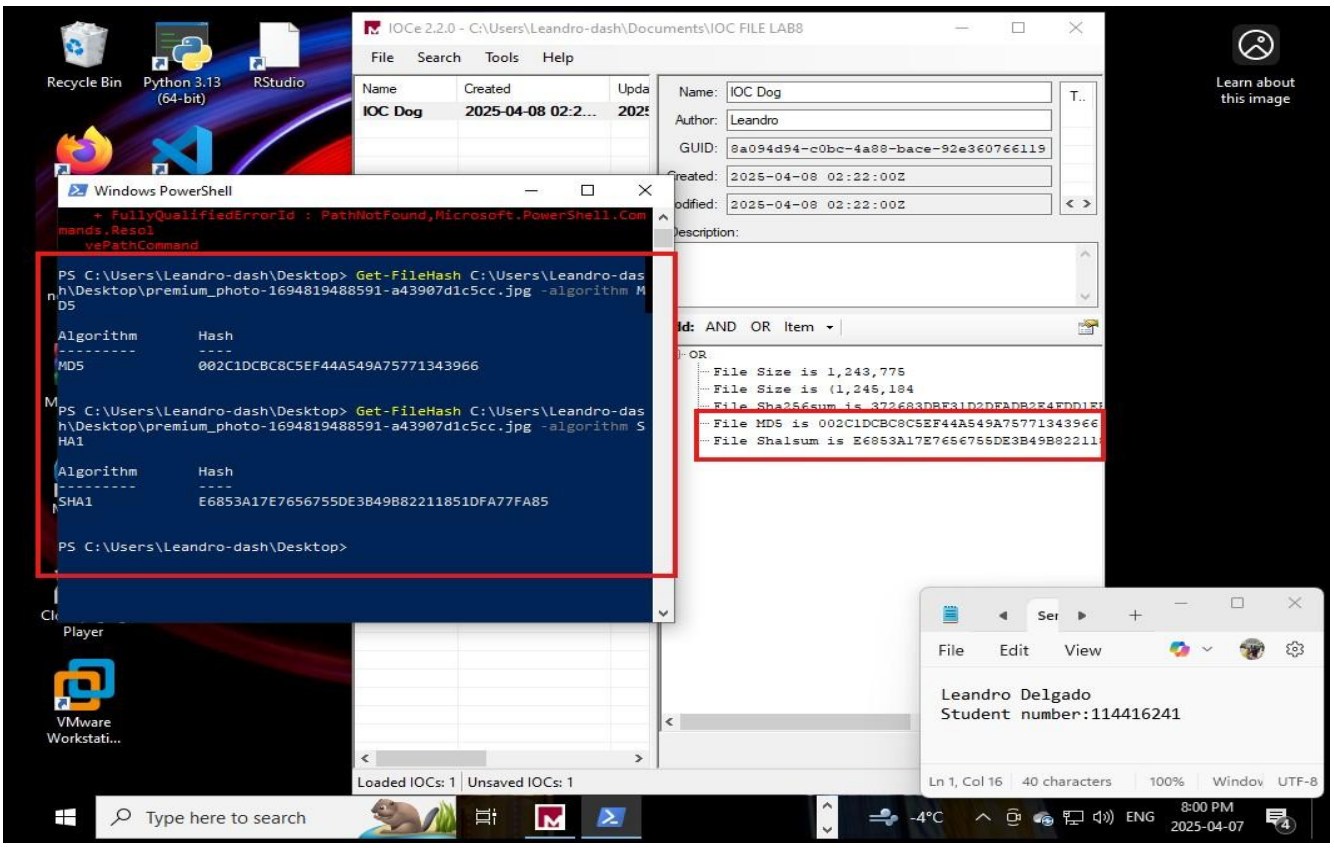

Figure 8. Exploring IOC Environment

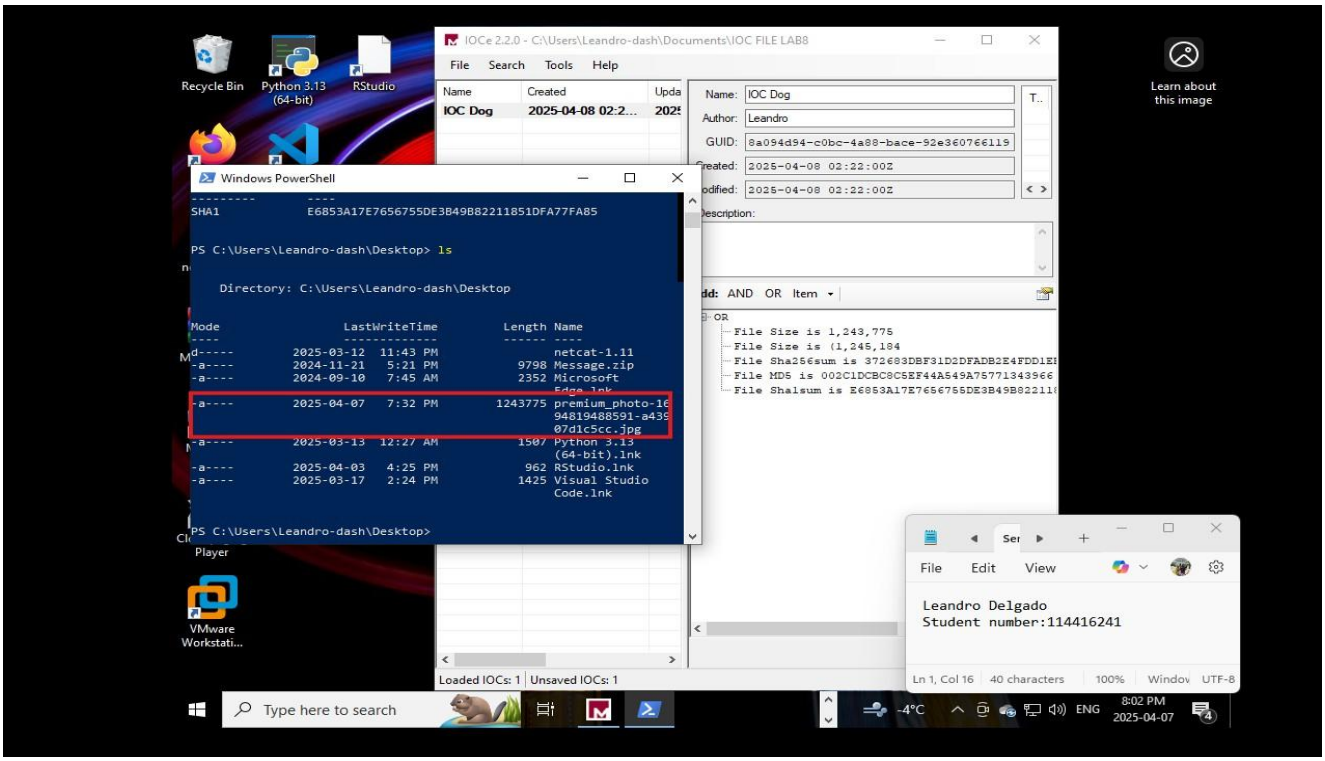

Figure 9. Exploring IOC Environment

Summary – Lesson Learned from Exploring the IOC Tools

Working with IOC Editor helped me understand how different types of indicators—like file hashes, file sizes, and names—can be structured to identify threats. I practiced extracting metadata and cryptographic hashes (SHA1, SHA256, MD5) using PowerShell and learned how to turn that information into IOC items using Mandiant IOCe. I also explored how to build both simple and complex IOC logic using OR and AND conditions to simulate real-world detection strategies. Overall, this gave me hands-on experience building digital forensic artifacts and thinking like a threat analyst.

2.2. Create IOC indicator similar to the following sample description (page 6 from the Guide)

Create your own sample from IOCs which you find in the attached MS Excel file IOC_Lab2. There are 4 groups of IOCs in this sample:

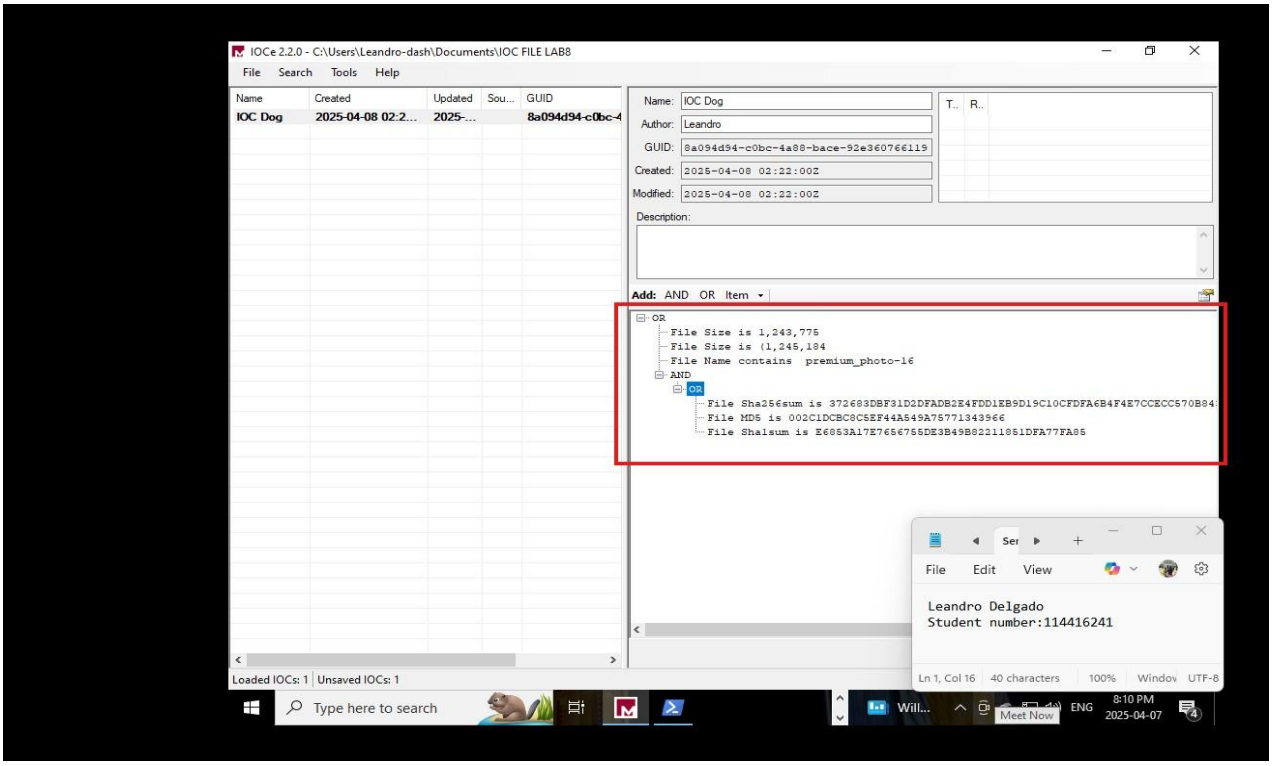

Figure 10. Creating own Sample

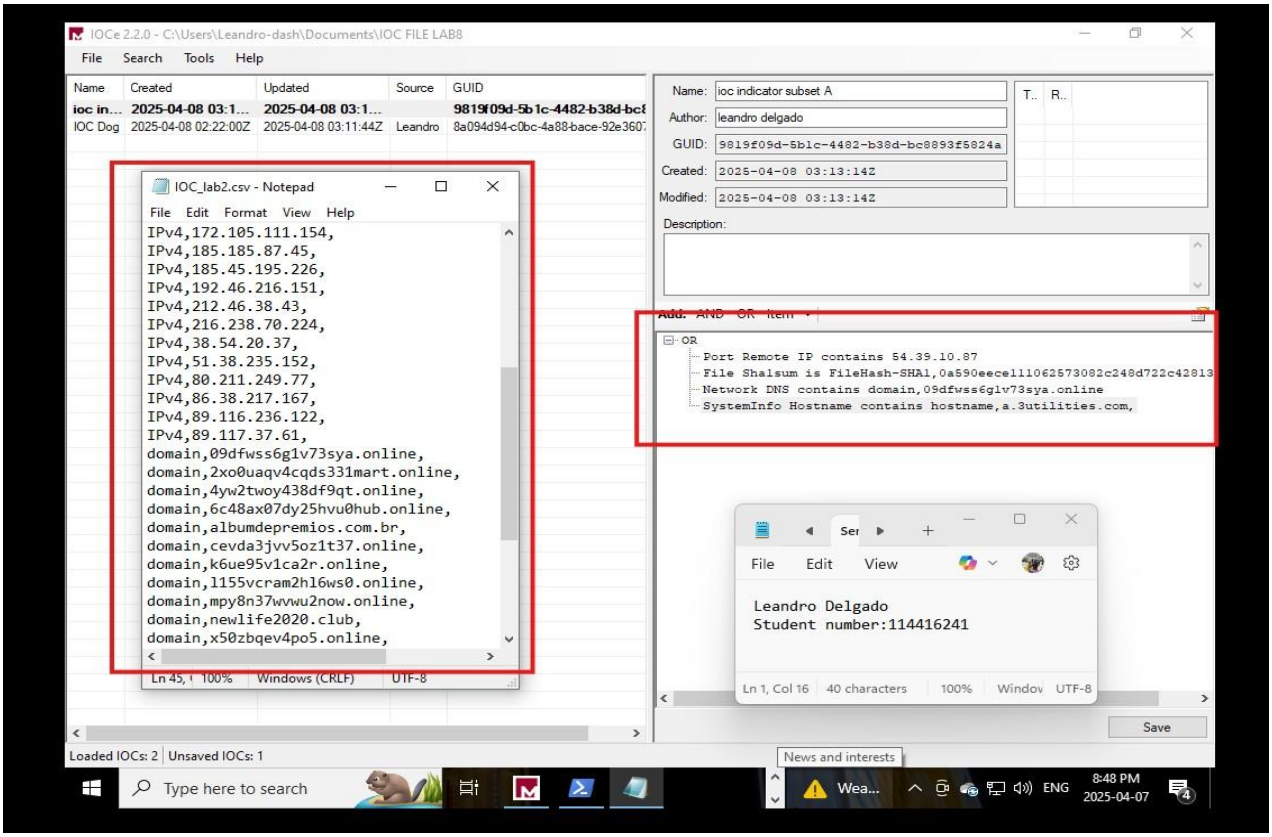

Figure 11. Creating Sample A

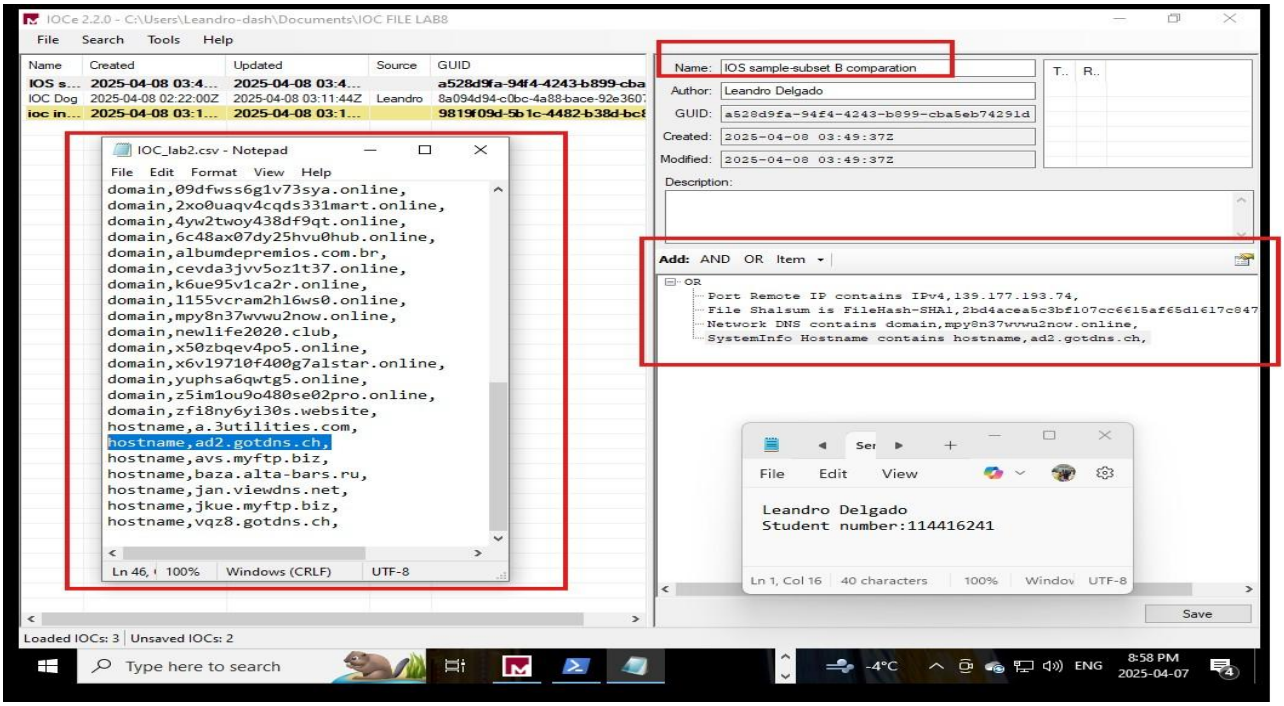

Figure 12. Creating Sample B for comparison

2.3. Proceed with comparison between 2 IOCs (pages 11-12 from the Guide). Create another subset of IOCs from the same collection. This is your subset B. Make sure that A and B include some portion of the same IOC and some different IOCs. Run the function “Compare” on these two subsets.

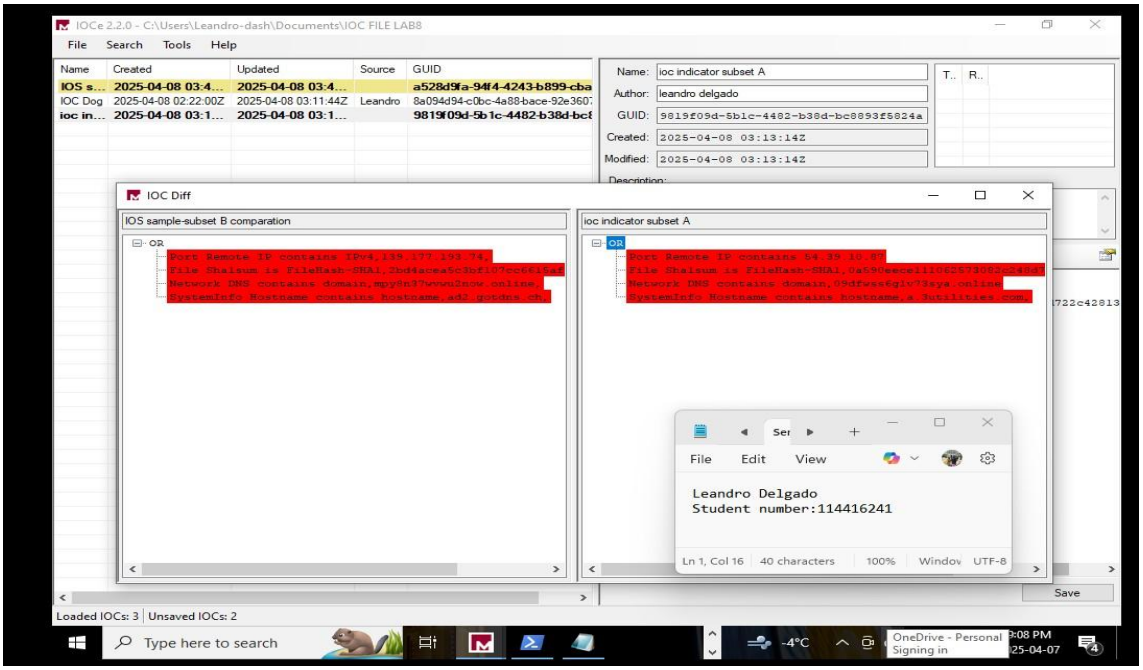

Figure 13. Comparation of IOC Aand B

2.4. Generate another IOC that would contain hashed value (similar to what is demonstrated in the video). Make screenshot and comments.

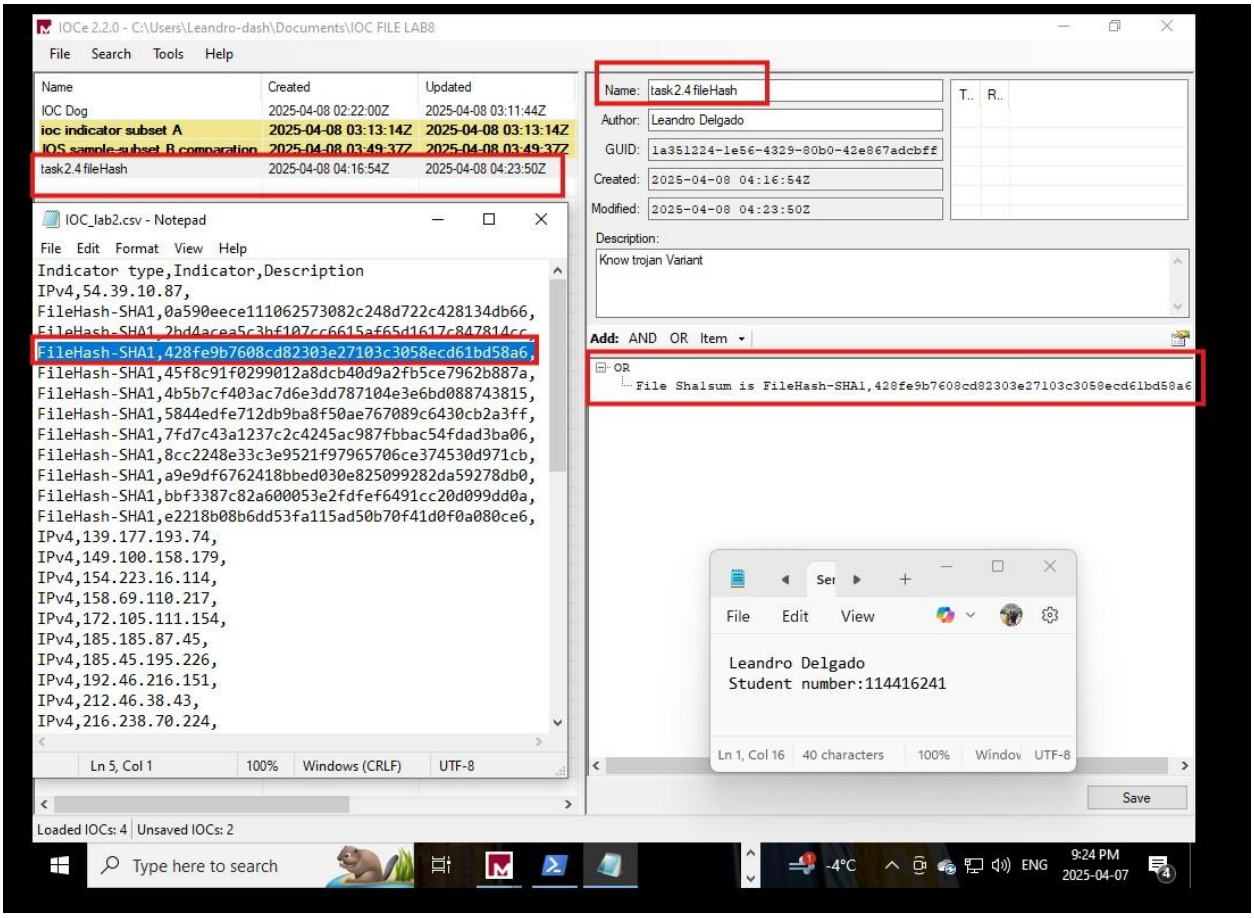

Figure 14. Hashed Value Trojan Variant

Summary of the lab

This lab provided hands-on experience using the IOC Editor tool (Mandiant IOCe) to create, edit, and compare Indicators of Compromise. I learned how to extract file hashes, file size, names, and other metadata using tools like PowerShell, and how to translate that information into meaningful IOC expressions. I practiced working with both simple and complex logic (OR/AND conditions), built multiple IOCs from real indicators, and validated their uniqueness through IOC comparison. Overall, this lab strengthened my understanding of how threat intelligence is structured and how IOCs can help detect malicious activity in a digital forensic investigation.