CYT245 Final Project – Learn OpenIOC framework and tools – 15%

Individual work

You are asked to enter student names below:

Ishan Aakash Patel - 146151238	

Team leader is _____Ishan Patel_____

Project 1 - Learn OpenIOC framework and tools – 15%

Objectives:

- **Familiarize yourself with the OpenIOC framework**
- **Familiarize yourself with the OpenIOC format**
- **Download and install the tools**
- **Run the IOC Editor and complete practical exercise**
- **Familiarize yourself with the functions of IOC Finder**
- **OpenIOC toSTIX**

Task description

Part 1. Learn OpenIOC framework – 1%

Connect to

https://cyware.com/security-guides/cyber-threat-intelligence/what-is-open-indicators-of-compromise-openioc-framework-ed9d

https://www.mandiant.com/resources/blog/openioc-basics

Review posted materials and write your comments about OpenIOC services, use cases and benefits of usage.

Part 2. Download and work with the OpenIOC tools

Task 1. Download IOC editor – 1%

You can find different sources to download IOC editor. You see below some options but other sources also can be found

https://fireeye.market/apps/238651

IOC streaming

https://fireeye.market/apps/xhmhhgul

Download the editor and install it on your computer.

Make screenshot of the result.

Task 2. Familiarize yourself with the capabilities of IOC Editor. – 1%

Play with the Editor following the instructions from the Tutorial. Try major functions:

- **Creating IOC**
- **Searching**
- **Building IOC**
- **Adding/Editing**
- **Comparison IOCs**

To complete this part use any sample of IOC you wish.

Make screenshots of your actions, comment and include them into MS Word document.

Task 3. Create IOC indicators – 7%

Connect AlienVault sites (2 samples) and create OpenIOC versions for the set of indicators taken from the alerts (take first 10 indicators in each case).

Nokoyawa ransomware attacks with Windows zero-day - AlienVault - Open Threat Exchange

https://otx.alienvault.com/pulse/64304e379620a4a8159e2d2a?utm_userid=tato1234&utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_following

Make screenshots of the resulting OpenIOC documents and comments.

Task 4. OpenIOC to STIX – 5%

At the github site

Utilities & Developer Resources | STIX Project Documentation

Find the section OpenIOC to STIX. Here you see the link to the source code for this utility. Run the code for any sample of the IOC documents created in the task 3.

GitHub - STIXProject/openioc-to-stix: Generate STIX XML from OpenIOC XML

Alternatively, you can use STIX visualization tools after you download IOCs from the AlienVault Site in STIX format.

Submission includes MS Word document uploaded to the BB. The name of the document must follow Submission Upload Requirements (see below).

Include 0-screen as usual.

Submission Upload Requirements

Make online submission to BB, only one submission from your team.

If you have more than one document, wrap it up to ZIP, 7ZIP, or RAR folder

Name the file you will uploading as indicated below. The name must include:

- Course ID (CYT245)
- What is this (e.g. lab1, assignment 1, etc)
- Authors by name(s)

Sample: CYT245Lab1_PeterJohnMohammadSue

Note: submissions that do not follow the requirements will not be accepted

Part 1 - Learn OpenIOC framework

The OpenIOC framework is a system developed to create, share, and interpret indicators of compromise (IOCs) to help in identifying and responding to security threats.

Services

1. **IOC Creation and Sharing**: OpenIOC allows security teams to create IOCs, which are pieces of forensic data used to identify potential security breaches. These IOCs can then be shared within the organization or with other entities to help in identifying and mitigating threats.
2. **Threat Detection and Response**: By utilizing IOCs, organizations can enhance their ability to detect and respond to security incidents. OpenIOC integrates with various security tools to automate the detection process.
3. **Standardization**: OpenIOC provides a standardized format for IOCs, which facilitates easier sharing and interpretation of threat information across different security platforms and teams.

Use Cases

1. **Incident Response**: Security teams use OpenIOC to quickly identify indicators of an ongoing or past attack, allowing them to take immediate action to mitigate the threat.
2. **Threat Intelligence Sharing**: Organizations can share IOCs with peers or industry groups to collaboratively enhance their defense mechanisms against common threats.
3. **Automated Detection**: Integrating OpenIOC with security information and event management (SIEM) systems and other security tools enables automated threat detection, reducing the time required to identify and respond to incidents.

Benefits

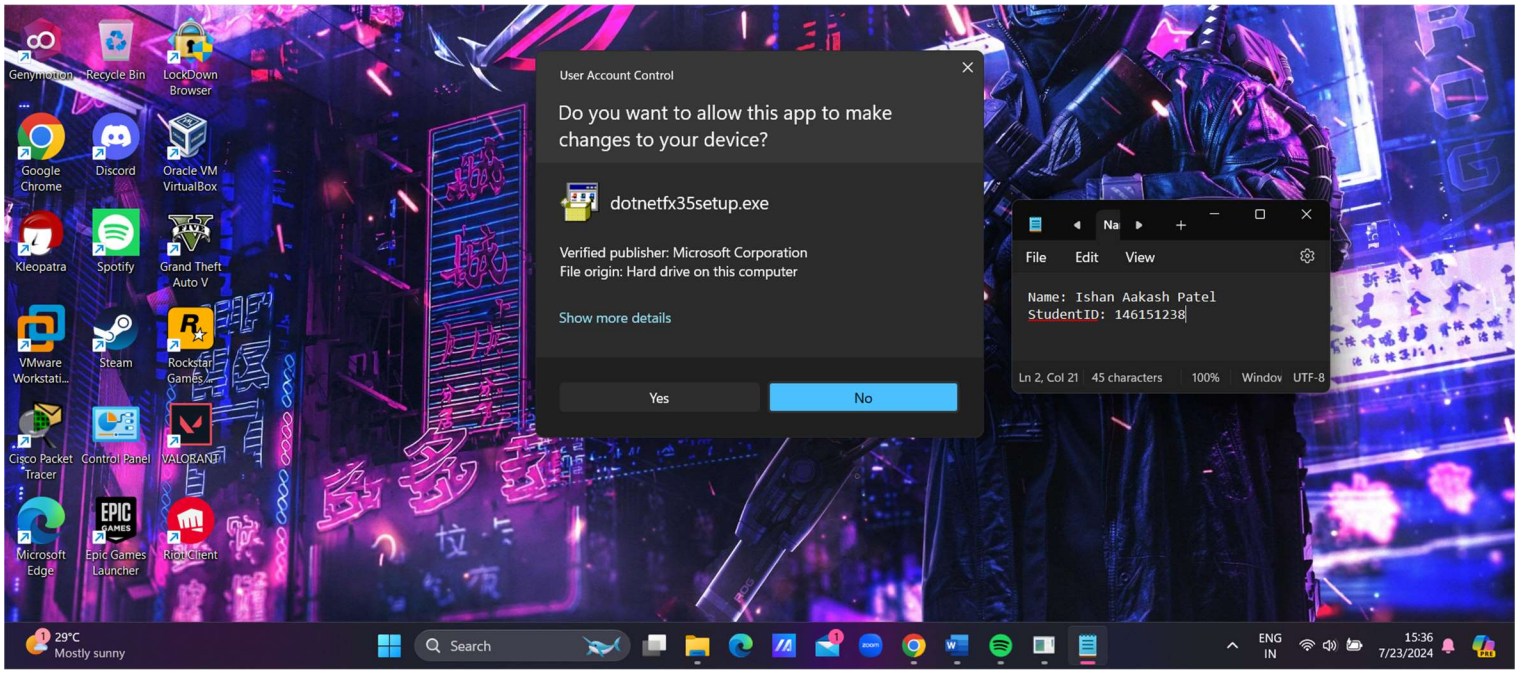
1. **Enhanced Detection Capabilities**: Using OpenIOC helps organizations improve their ability to detect and respond to threats more quickly and accurately.
2. **Improved Collaboration**: The standardized format of OpenIOC makes it easier for organizations to share threat information and collaborate on security efforts.
3. **Resource Efficiency**: Automating the detection and response processes through OpenIOC integration can save time and resources, allowing security teams to focus on more strategic tasks.

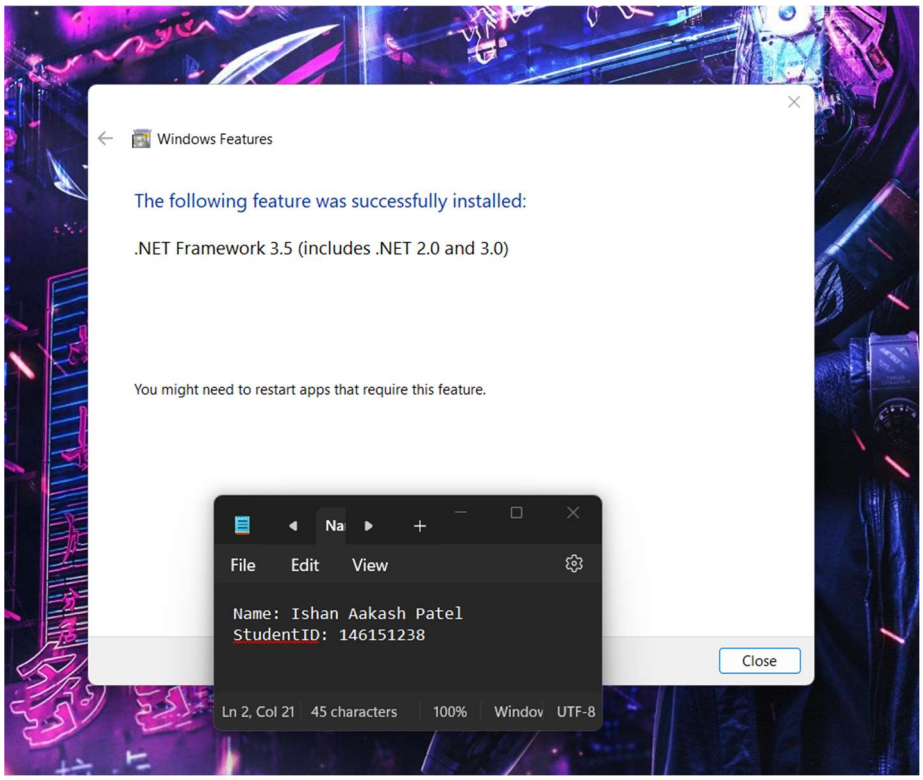
Overall, OpenIOC provides a robust framework for improving an organization's cybersecurity posture by enabling better detection, response, and collaboration capabilities.

Part 2 - Download and work with the OpenIOC tools

Task 1 – Download IOC editor

First we need to install .NET Framework, if we want to run IOC Editor





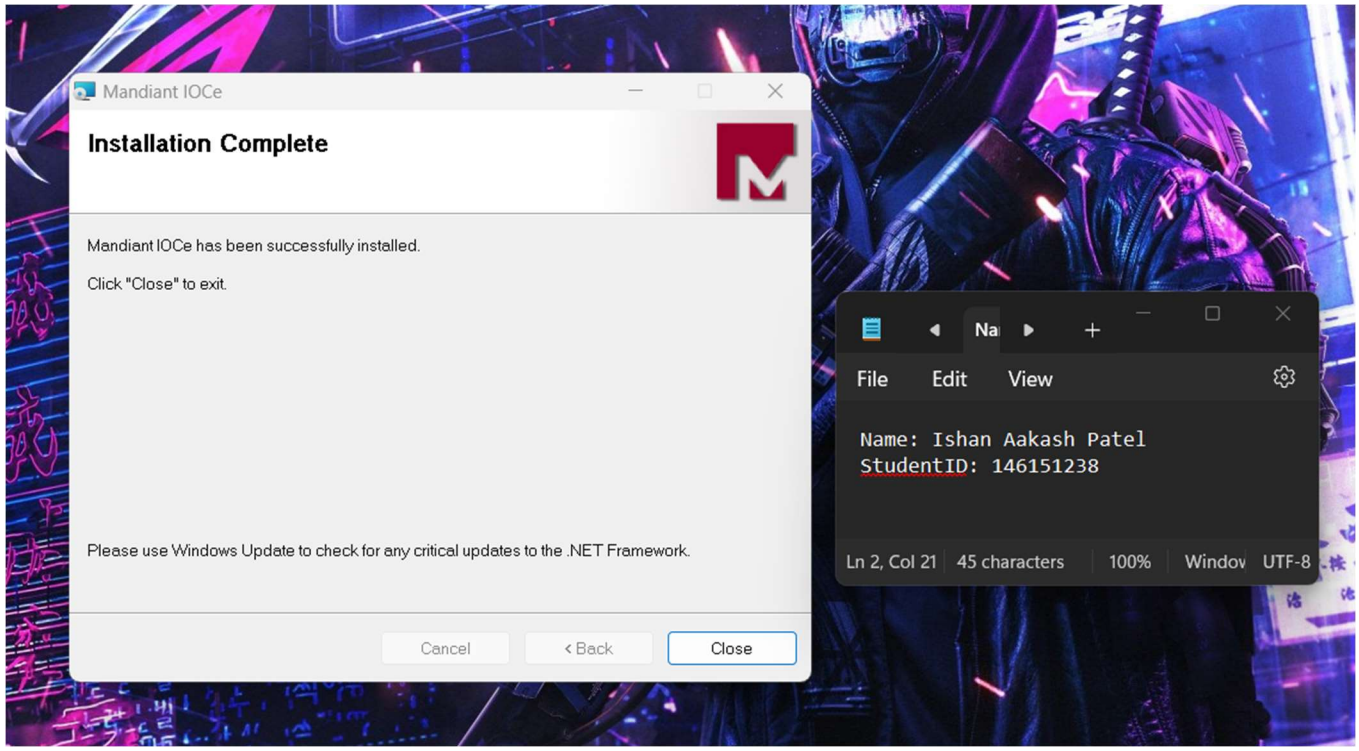
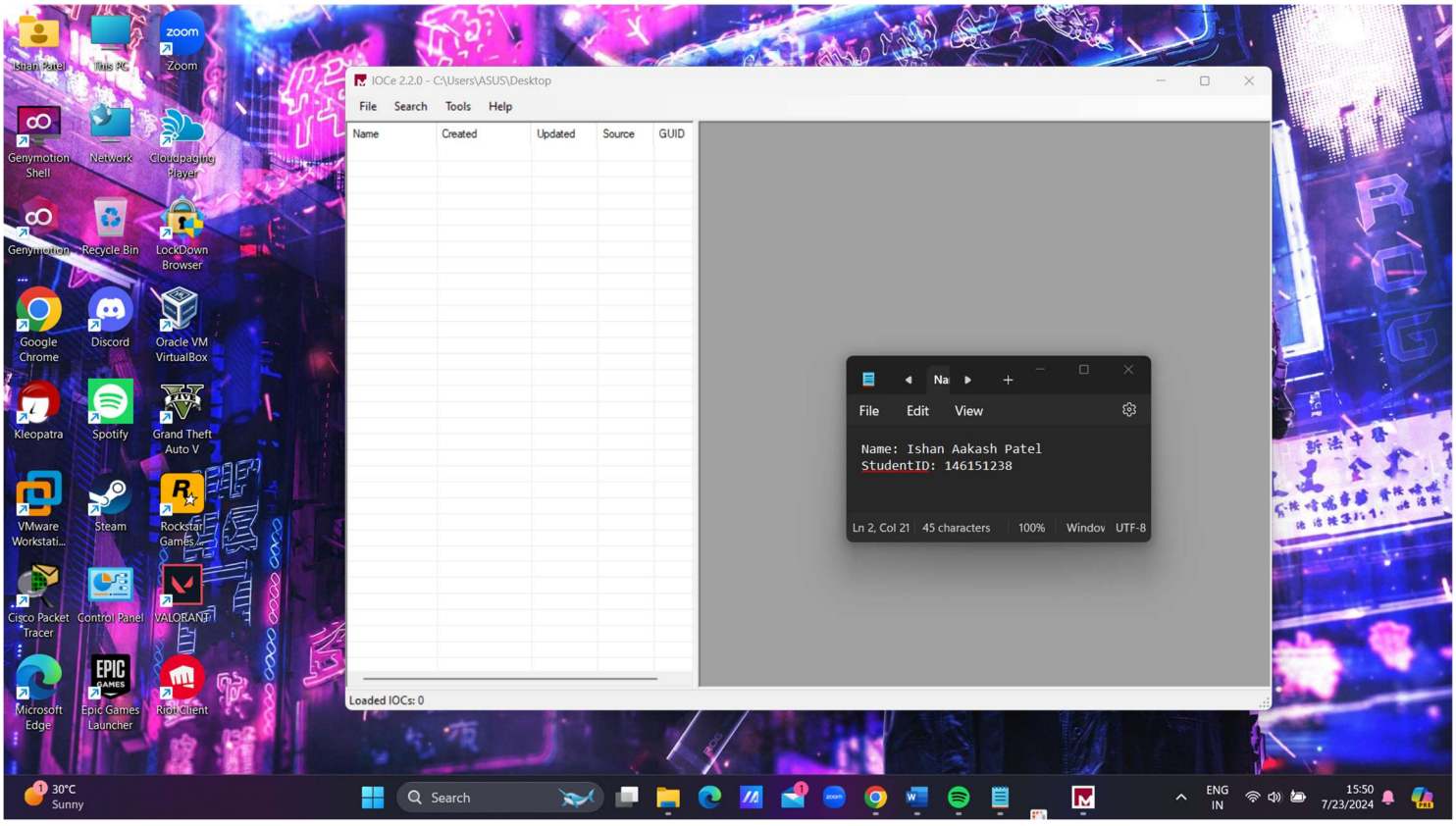


Figure 1 : Successfull Installed



Task 2. Familiarize yourself with the capabilities of IOC Editor.

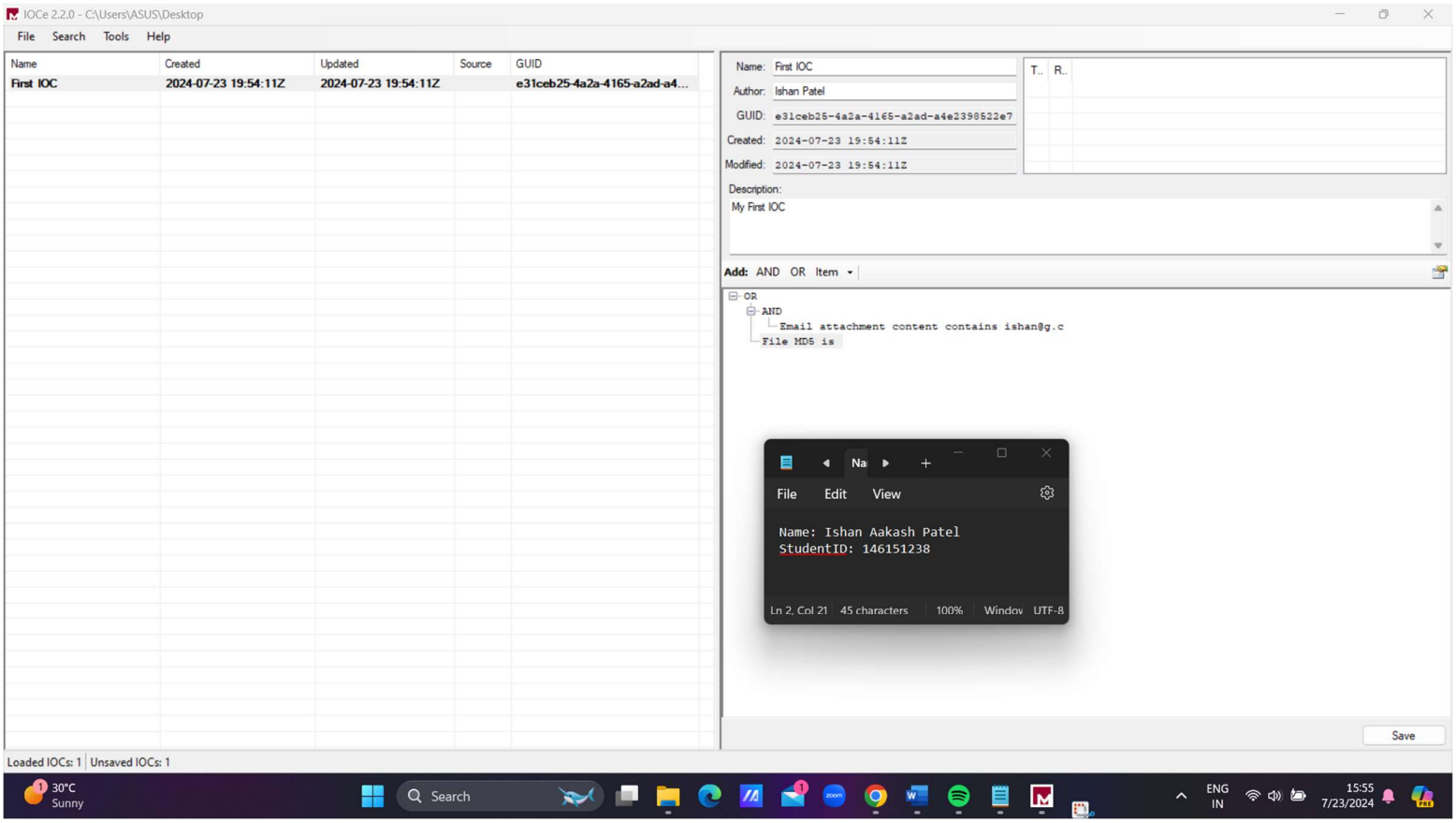


Figure 2 : Creating an IOC

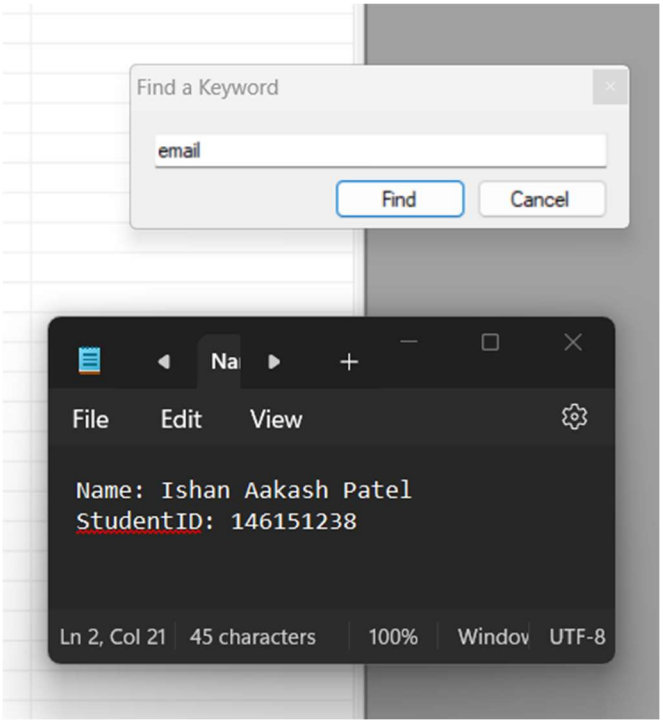


Figure 3 : Searching a Keyword

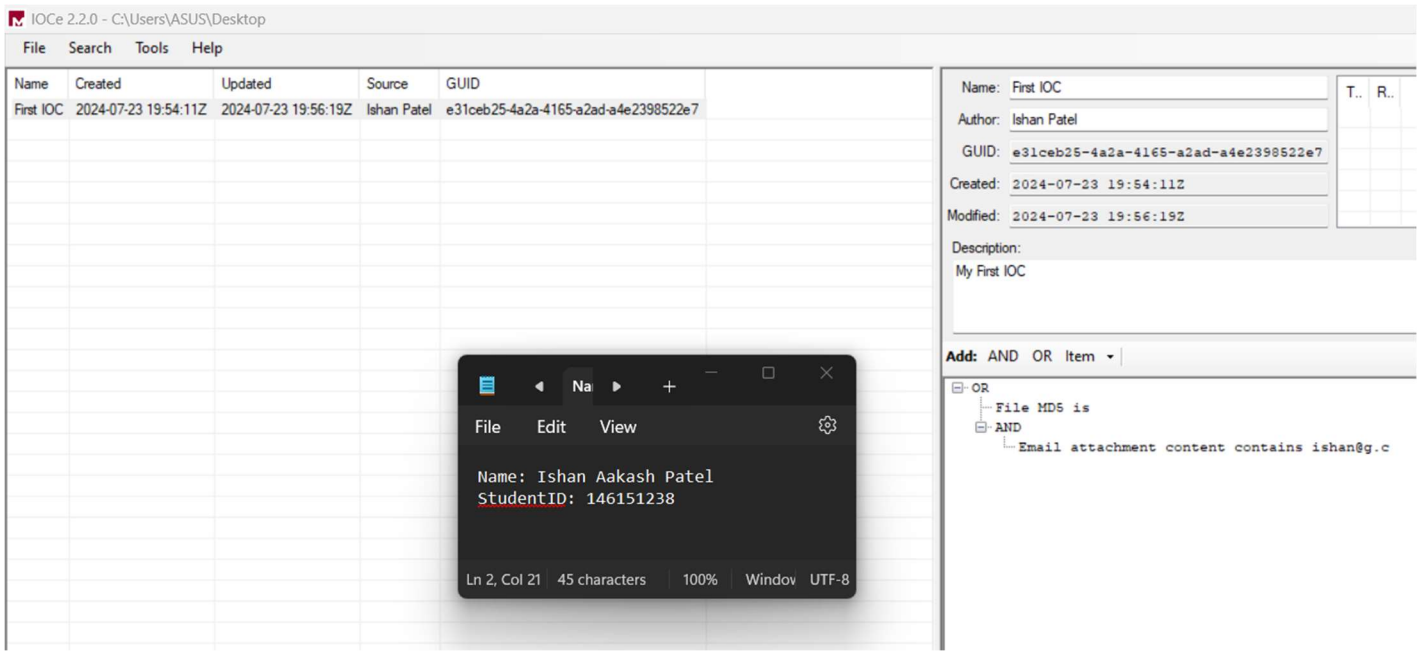


Figure 4 : Result after searching

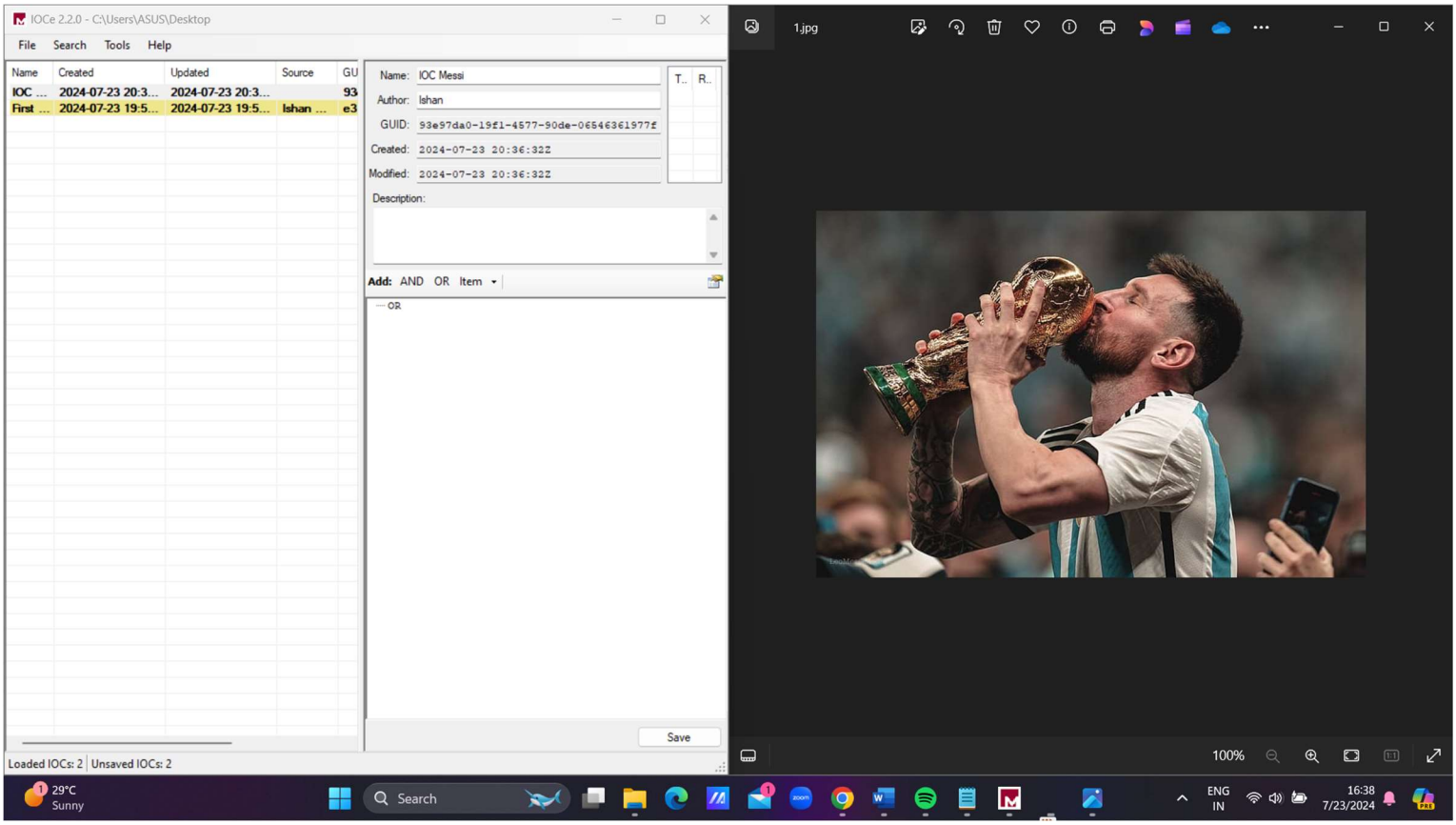


Figure 5 : Building an IOC of a simple image (sample)

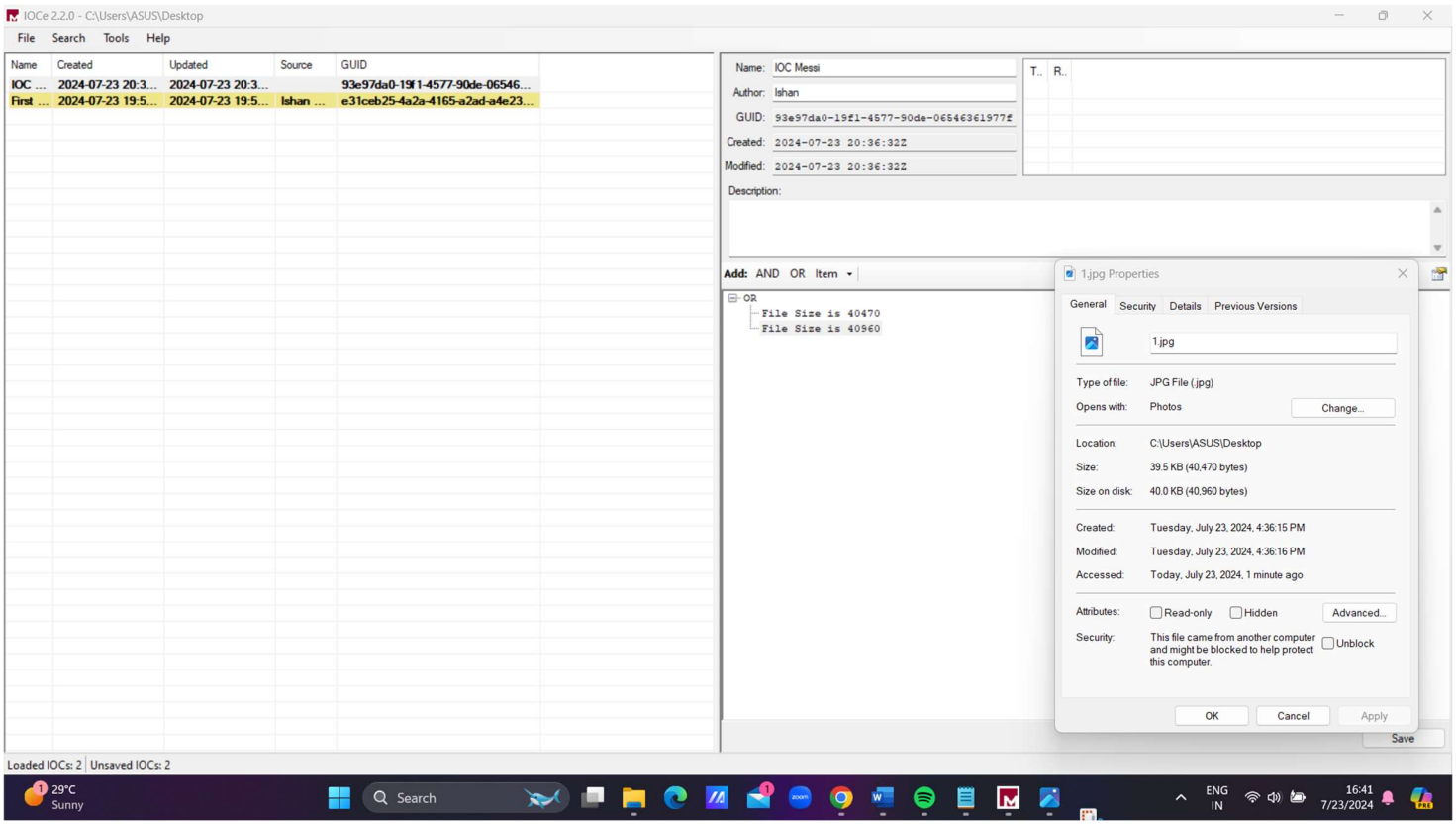


Figure 6: Adding file size

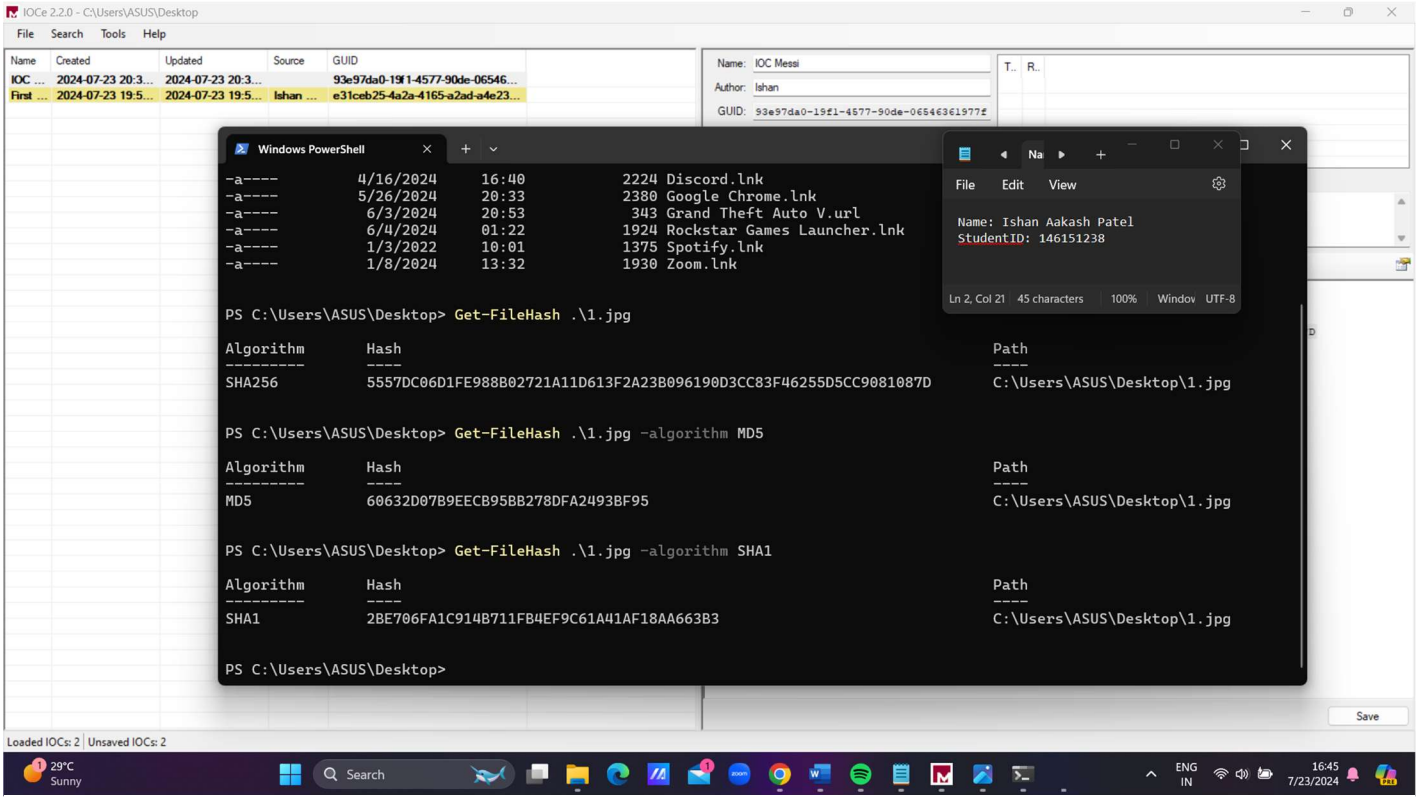


Figure 7 : Now Adding different hashes

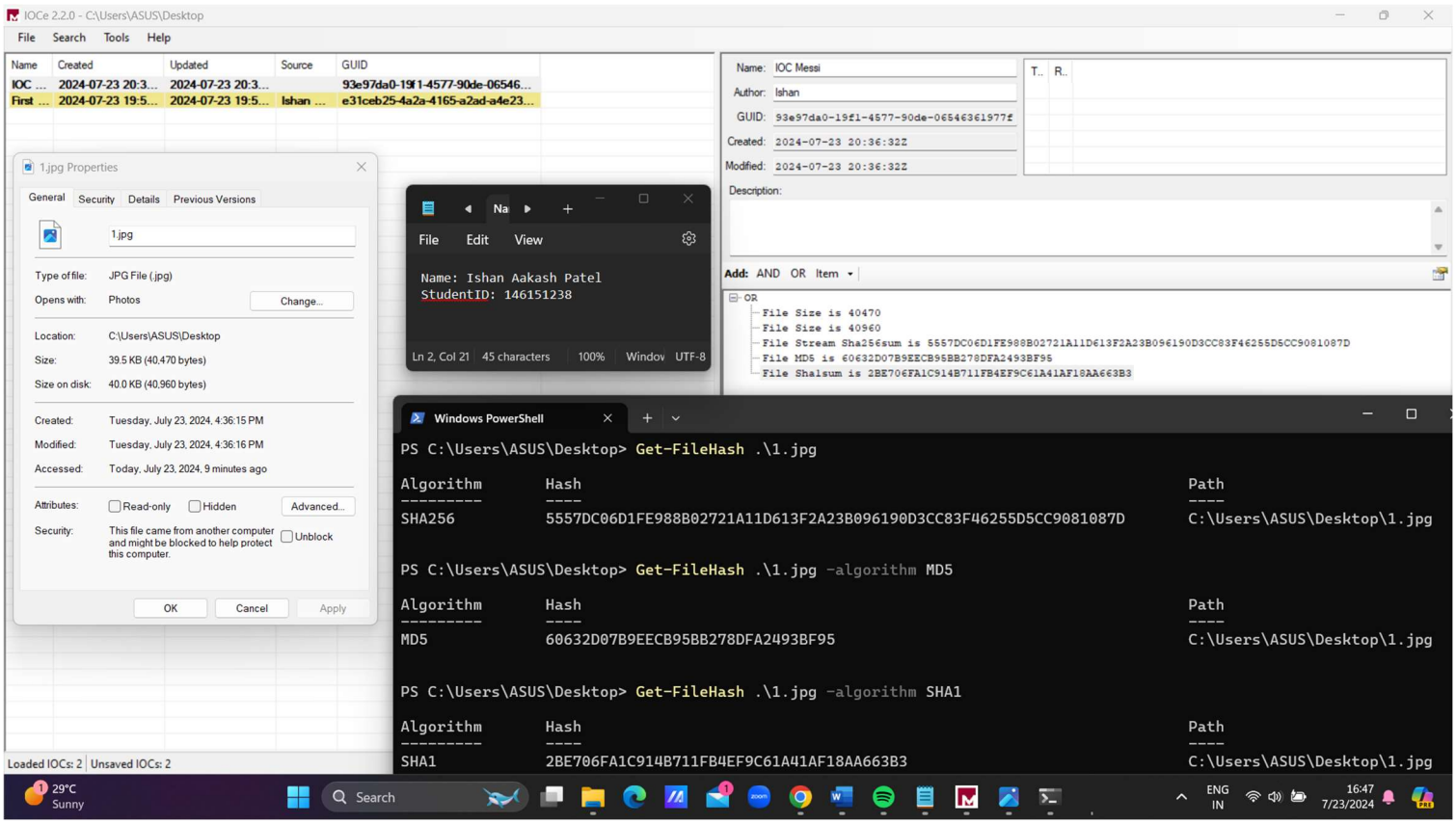


Figure 8 : After adding everything

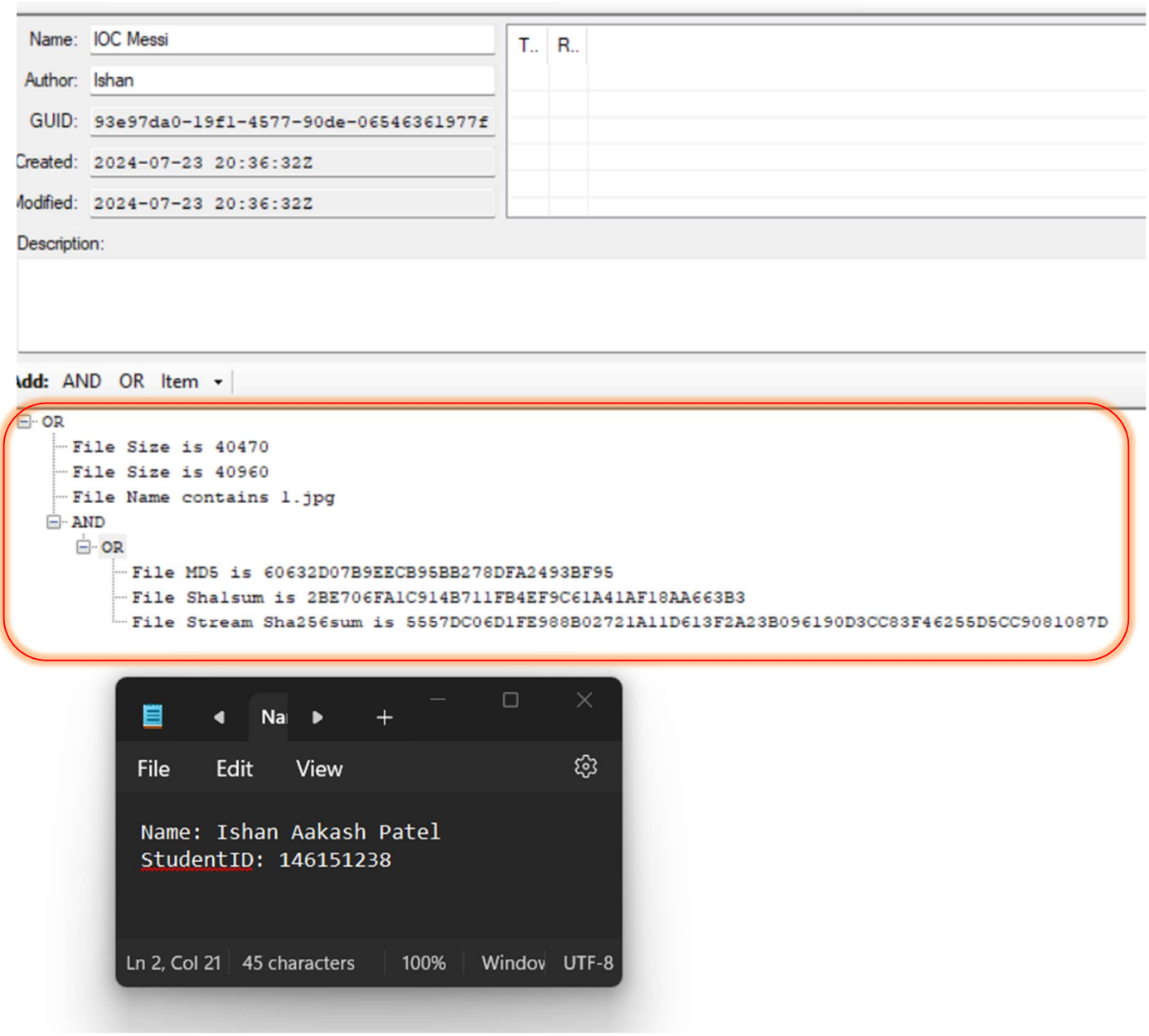


Figure 9 : Adding AND OR operator

1. IOC Details:

- Name: IOC Messi

- Author: Ishan

- Created/Modified: 2024-07-23 20:36:322

2. IOC Conditions:

The IOC uses AND/OR operators to define conditions for detecting a potential threat:

- OR Condition:

  - File Size is 40470

  - File Size is 40560

  - File Name contains "1.jpg"

- AND Condition:

  - OR:

    - File MD5 is E0632D07B92ECB95BB270DFA2493BF95

    - File Sha1sum is 2BE706FAC914B711FB4EF9C61A41AF10AA663B3

    - File Stream Sha256sum is 555DC06D1FF298B0272A1A1D413F2A23B0961902DCC39F4655D6CC90810997D

3. AND/OR Operators:

- AND: All conditions under AND must be true for the IOC to trigger.

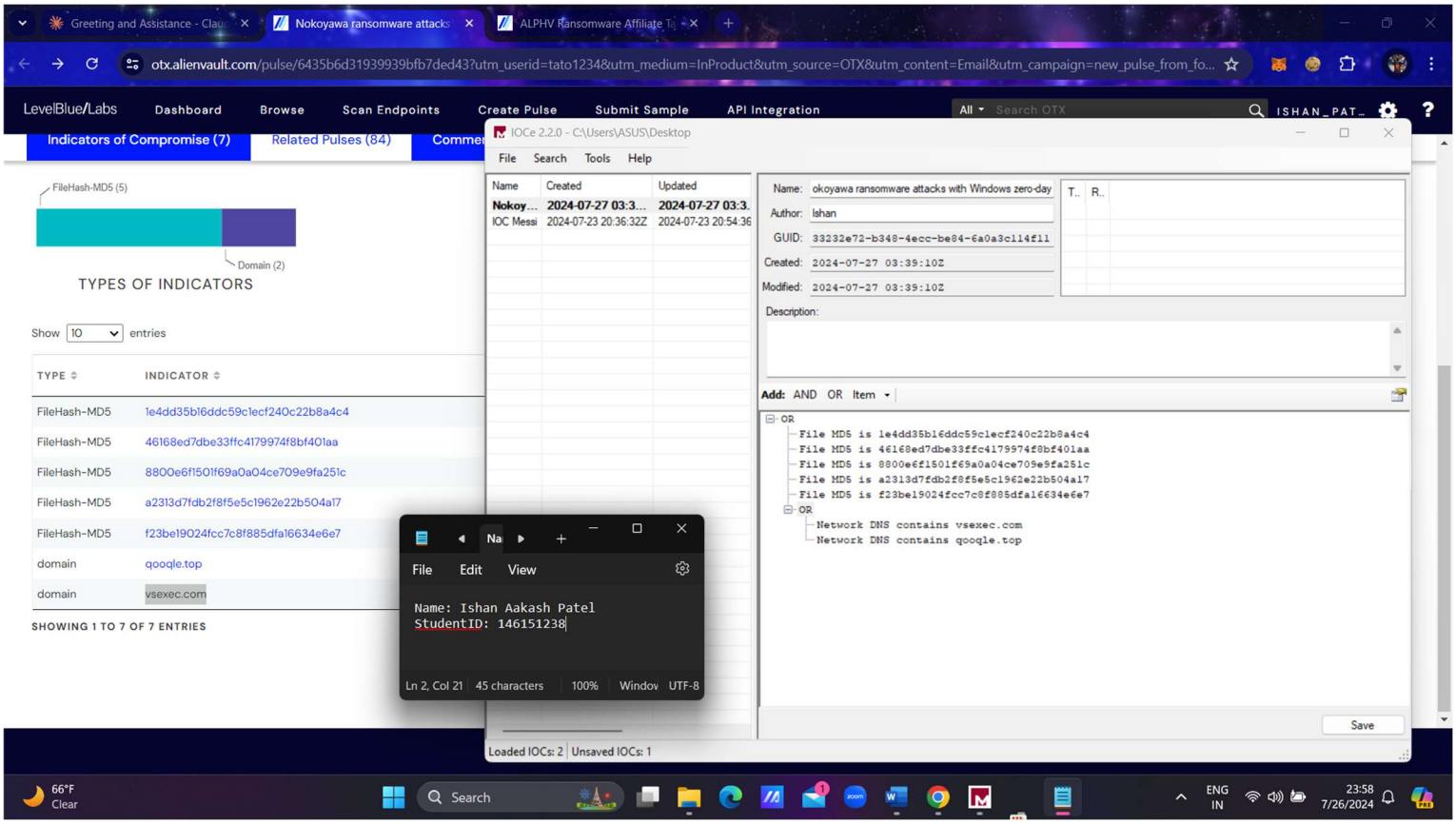
- OR: Any one of the conditions under OR being true is sufficient to satisfy that part of the IOC.

In this case, the file must either have a specific size (40470 or 40560) OR contain "1.jpg" in its name, AND it must match one of the specified hash values (MD5, SHA1, or SHA256).

This structure allows for flexible and precise definition of indicators, combining multiple attributes to identify potential threats or compromised files.

Task 3. Create IOC indicators – 7%

1) Sample - Nokoyawa ransomware attacks with Windows zero-day



1. IOC Details:
    - Name: okoyawa ransomware attacks with Windows zero-day
    - Author: ishan
    - Created: 2024-07-27 03:39:10Z
    - Modified: 2024-07-27 03:39:10Z
    - GUID: 33232e72-b349-4ecc-be84-6a0a3c114f11
2. IOC Conditions: The IOC uses AND/OR operators to define conditions for detecting the Nokoyawa ransomware:
    - AND Condition:
        - OR:
            - File MD5 is 1e4dd35b16ddc59c1ecf240c22b8a4c4
            - File MD5 is 46168ed7dbe33ffc4179974f8bf401aa

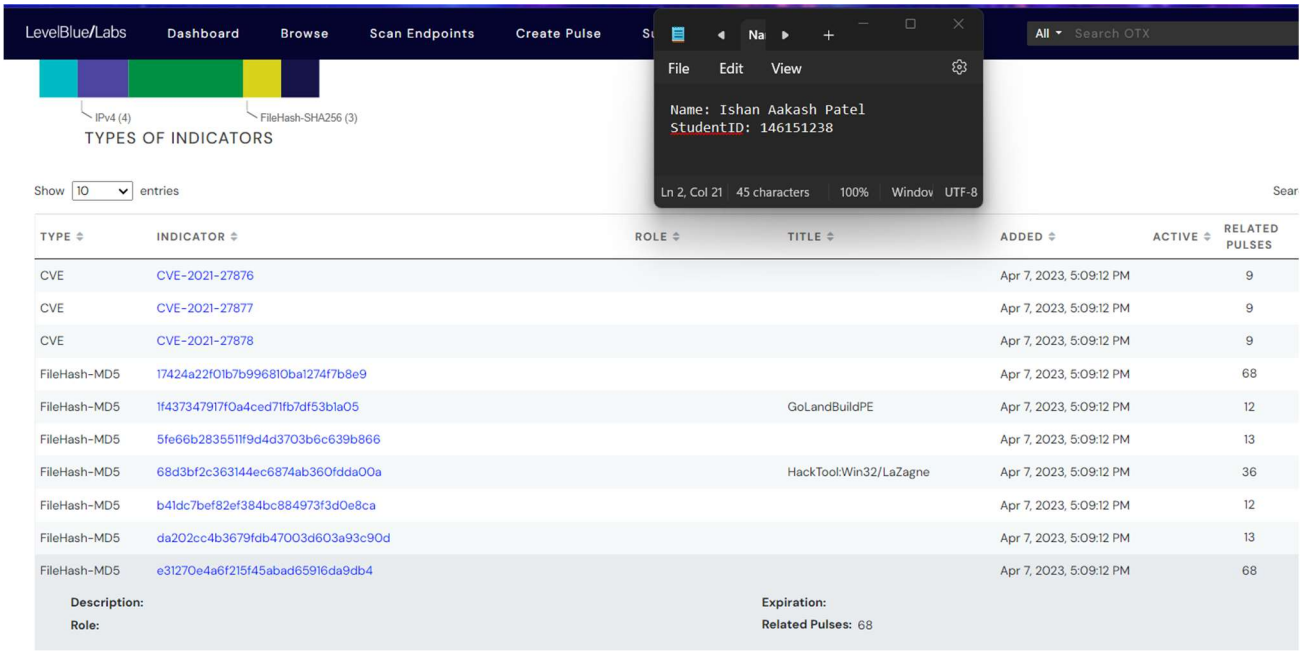
        - File MD5 is 8800e6f150f69a0a04ce709e9fa251c
        - File MD5 is a2313d7fdb2f8f5e5c1962e22b504a17
        - File MD5 is f23be19024fcc7c8f886dfa1ef34e6e7
    - OR:
        - Network DNS contains vsexec.com
        - Network DNS contains google.top

3. AND/OR Operators:
    - AND: All conditions under AND must be true for the IOC to trigger.
    - OR: Any one of the conditions under OR being true is sufficient to satisfy that part of the IOC.

In this case, for the IOC to trigger, there must be a match on one of the specified File MD5 hashes AND a match on one of the specified Network DNS entries. This structure allows for detection of the Nokoyawa ransomware based on both its file characteristics and its network communication patterns.

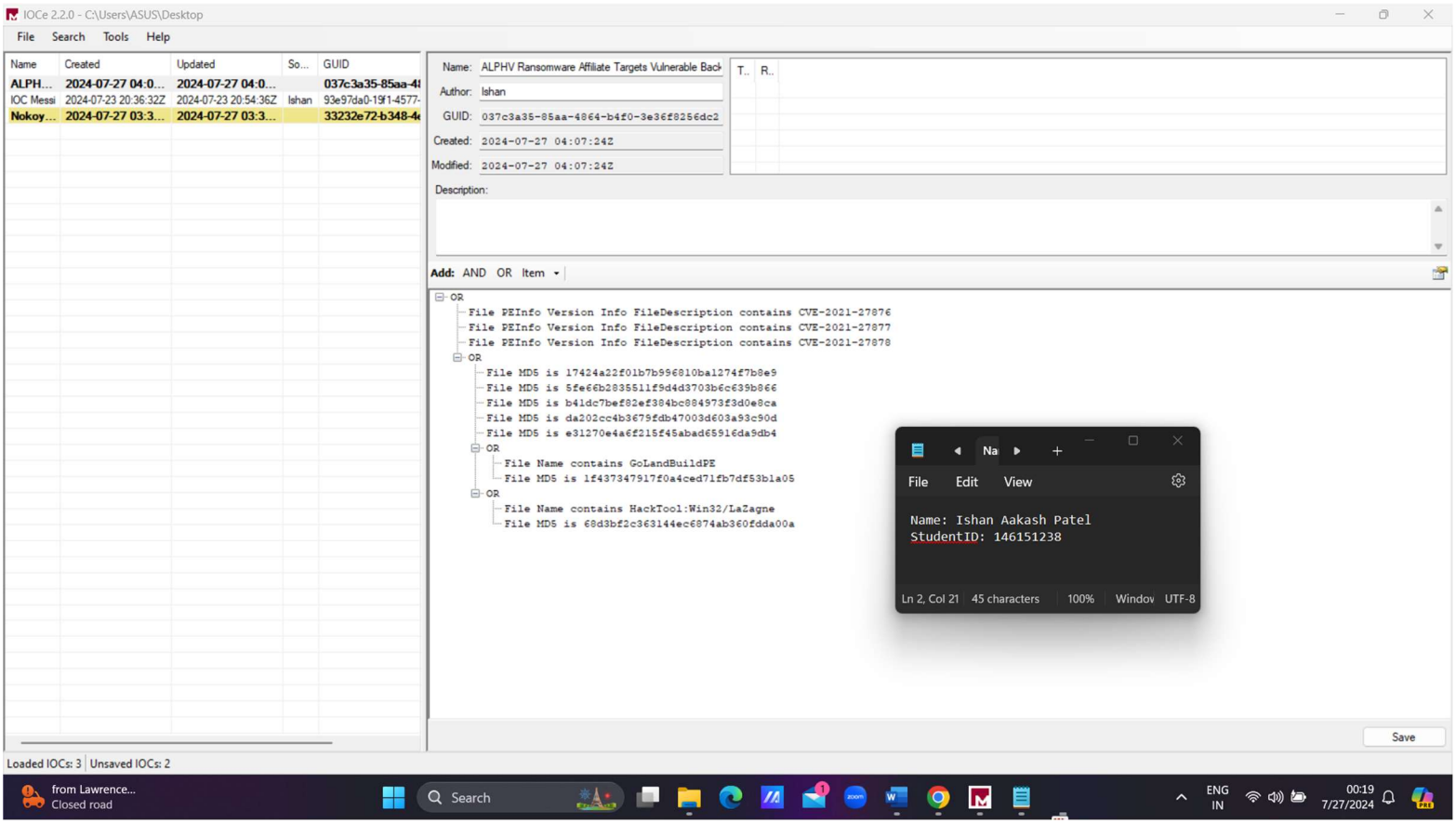
This combination of file hashes and domain indicators provides a flexible yet precise method for identifying potential Nokoyawa ransomware infections, as it can detect the threat based on either its file signatures or its network activities.

2) Sample - ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access



TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
CVE	CVE-2021-27876			Apr 7, 2023, 5:09:12 PM		9
CVE	CVE-2021-27877			Apr 7, 2023, 5:09:12 PM		9
CVE	CVE-2021-27878			Apr 7, 2023, 5:09:12 PM		9
FileHash-MD5	17424a22f01b7b996810ba1274f7b8e9			Apr 7, 2023, 5:09:12 PM		68
FileHash-MD5	1f437347917f0a4ced71fb7df53b1a05		GoLandBuildPE	Apr 7, 2023, 5:09:12 PM		12
FileHash-MD5	5fe66b2835511f9d4d3703b6c639b866			Apr 7, 2023, 5:09:12 PM		13
FileHash-MD5	68d3bf2c363144ec6874ab360fdda00a		HackTool:Win32/LaZagne	Apr 7, 2023, 5:09:12 PM		36
FileHash-MD5	b41dc7bef82ef384bc884973f3d0e8ca			Apr 7, 2023, 5:09:12 PM		12
FileHash-MD5	da202cc4b3679fdb47003d603a93c90d			Apr 7, 2023, 5:09:12 PM		13
FileHash-MD5	e31270e4a6f215f45abad65916da9db4			Apr 7, 2023, 5:09:12 PM		68

Description:
Role:
Expiration:
Related Pulses: 68



1. IOC Details:
    - Name: ALPHV Ransomware Affiliate Targets Vulnerable Back
    - Author: Ishan
    - Created: 2024-07-27 04:07:24Z
    - Modified: 2024-07-27 04:07:24Z
    - GUID: 037c3a35-85aa-4964-b4f0-3e3f6028fdc2
2. IOC Conditions: The IOC uses AND/OR operators to define conditions for detecting the ALPHV Ransomware:
    - OR Condition:
        - File PEInfo Version Info FileDescription contains CVE-2021-27876
        - File PEInfo Version Info FileDescription contains CVE-2021-27877
        - File PEInfo Version Info FileDescription contains CVE-2021-27878
    - OR Condition:
        - File MD5 is 17424a22f01b7b9968f10ba12747fb8e9
        - File MD5 is 5fe66b283551f9d4d3703b6c639b866
        - File MD5 is b41dc7bef82ef384bc884973f3d0e8ca
        - File MD5 is da202cc4b3679fdb47003d603a93c90d
        - File MD5 is e31270e4a6f215f45abad65916da9db4
    - OR Condition:
        - File Name contains GoLandBuildPE
        - File MD5 is 1f43734791710a4ced71fb7df53b1a05
    - OR Condition:
        - File Name contains HackTool:Win32/LaZagne
        - File MD5 is 68d3bf2c363144ec6874ab360fdda00a
3. AND/OR Operators:
    - The top-level operator is OR, meaning any of the main conditions being true is sufficient to trigger the IOC.
    - Within each OR block, individual conditions are also joined by OR.

This structure allows for flexible detection of the ALPHV Ransomware based on multiple criteria:

- Presence of specific CVE identifiers in file descriptions
- Matching any of several file MD5 hashes
- Presence of specific file names along with their corresponding MD5 hashes

This multi-faceted approach enables detection of the ransomware through various indicators, including vulnerability exploitation, specific file signatures, and known malicious tool names.

Task 4. OpenIOC to STIX

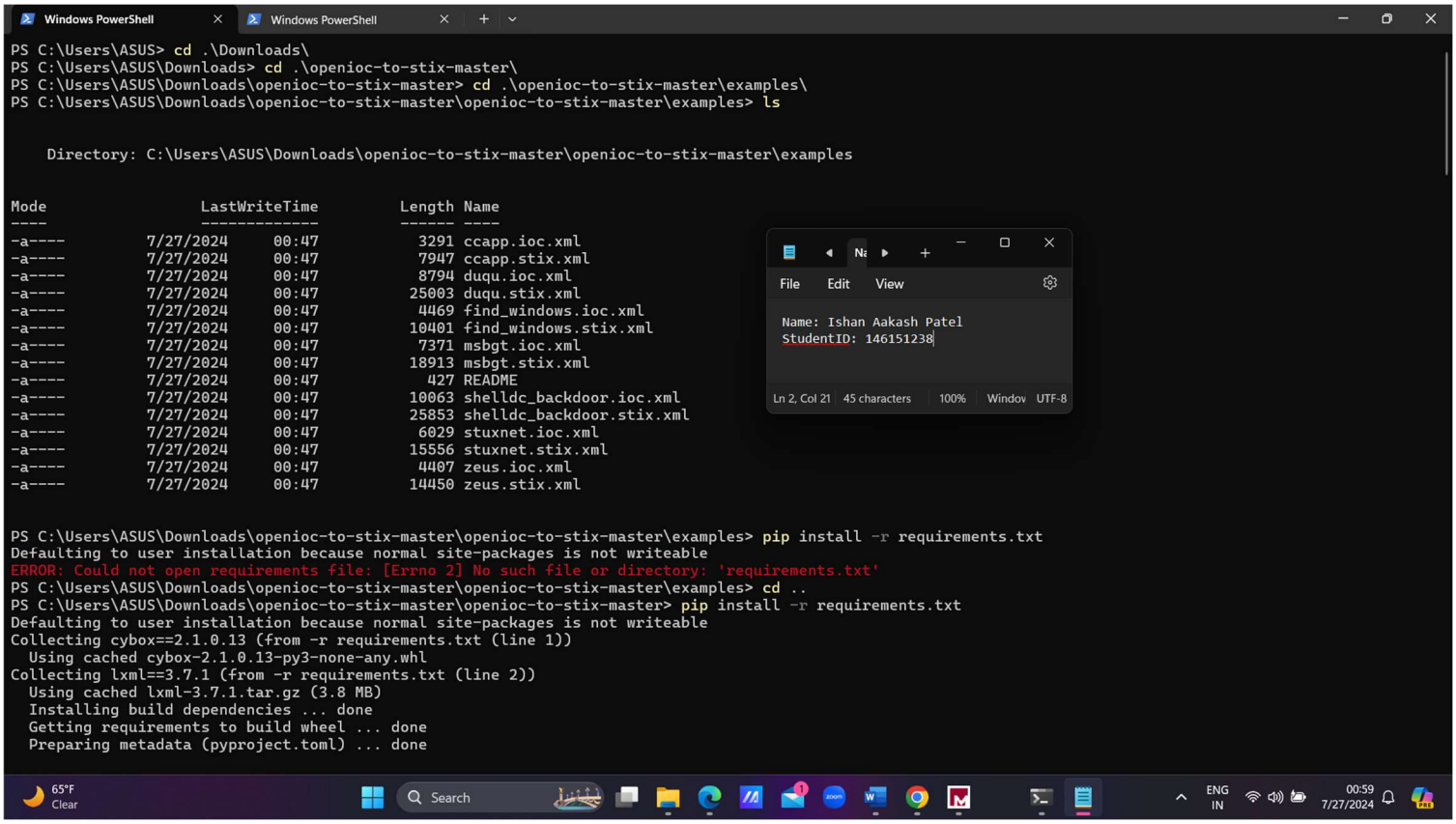
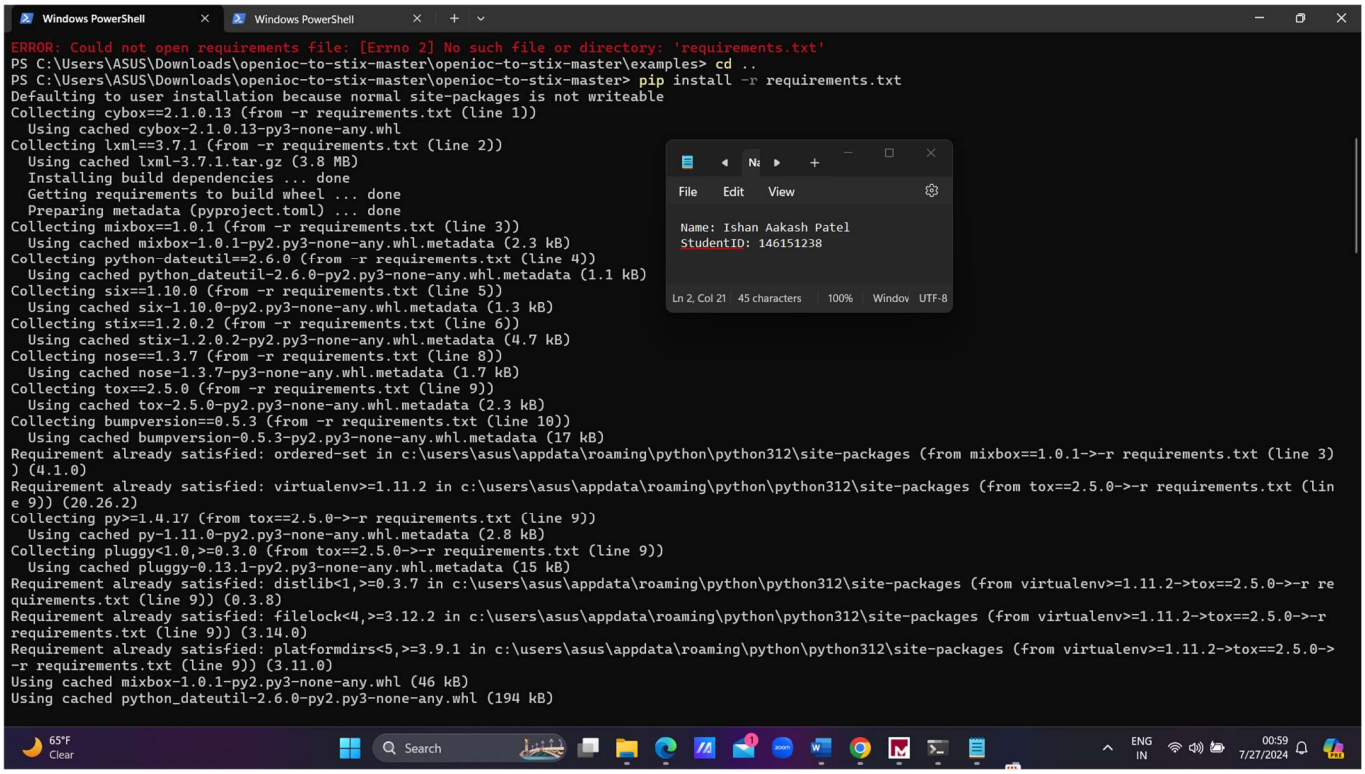
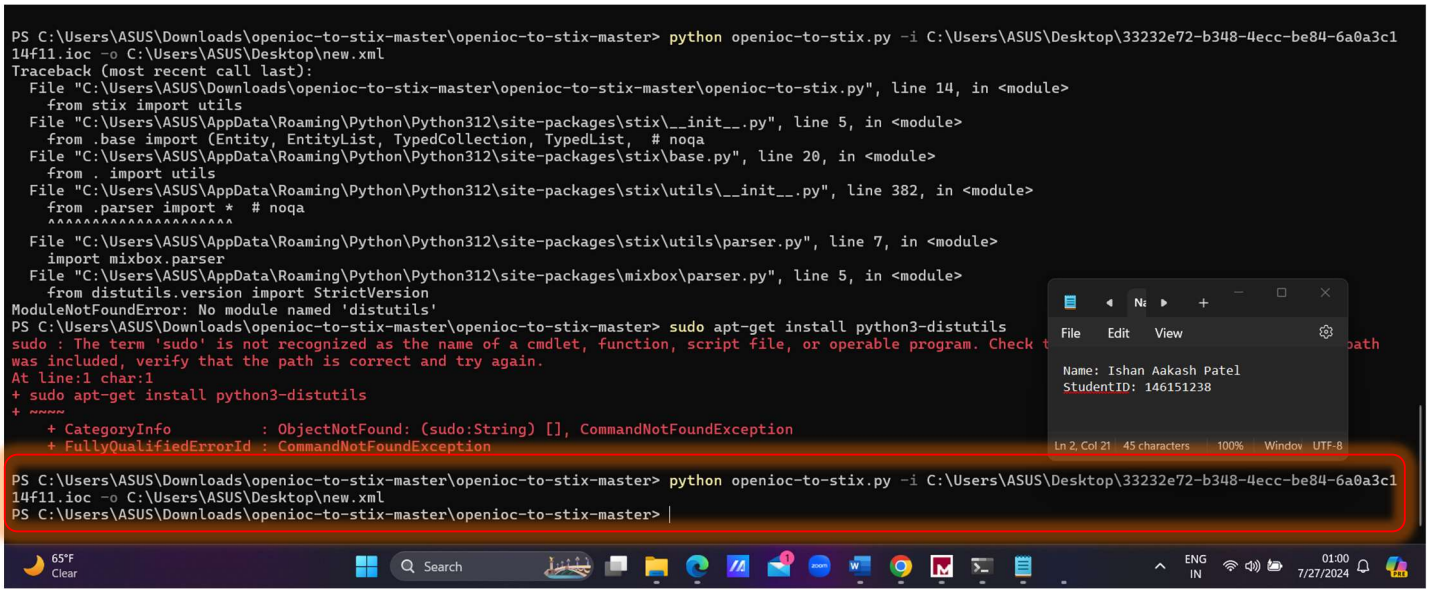


Figure 4 : Installing the requirements.txt for the openioc to stix



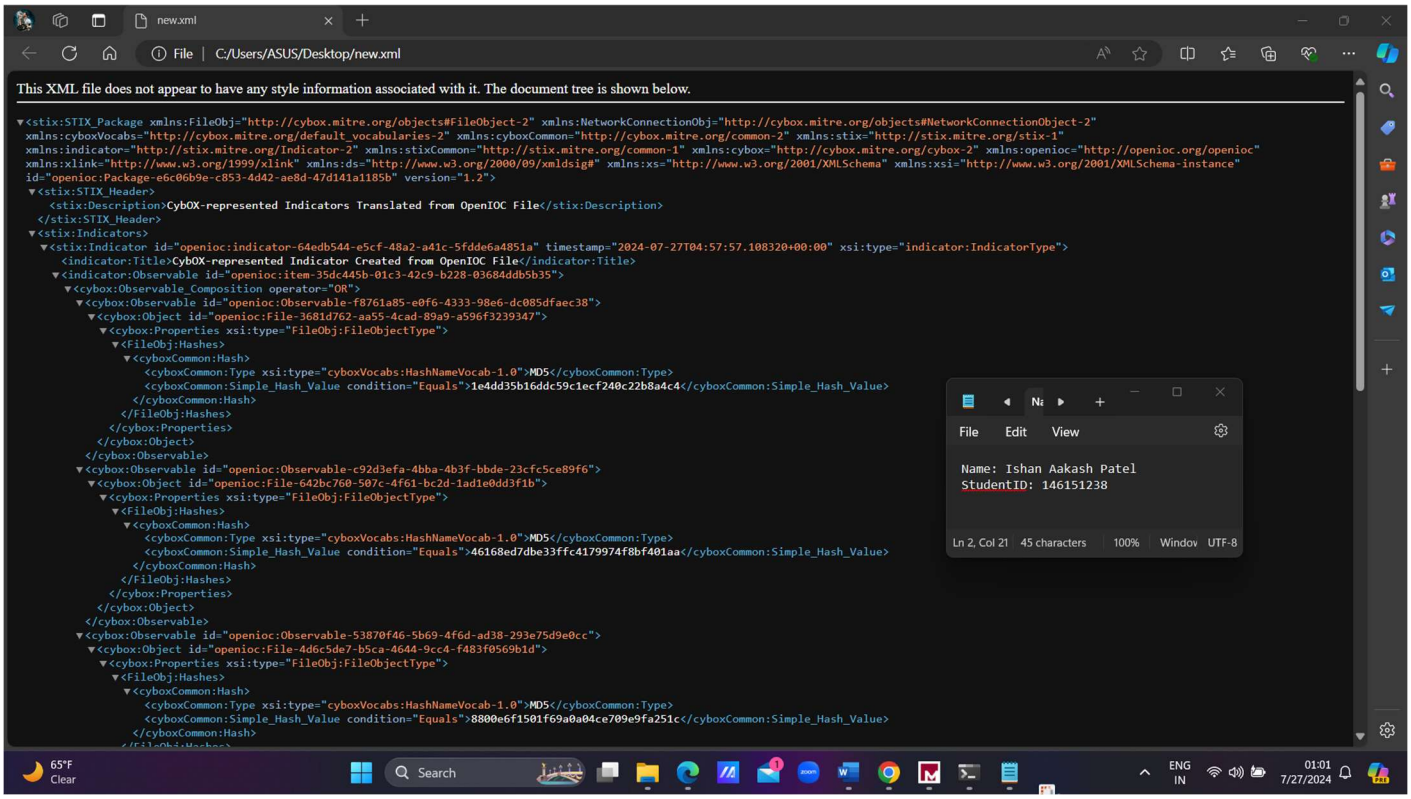


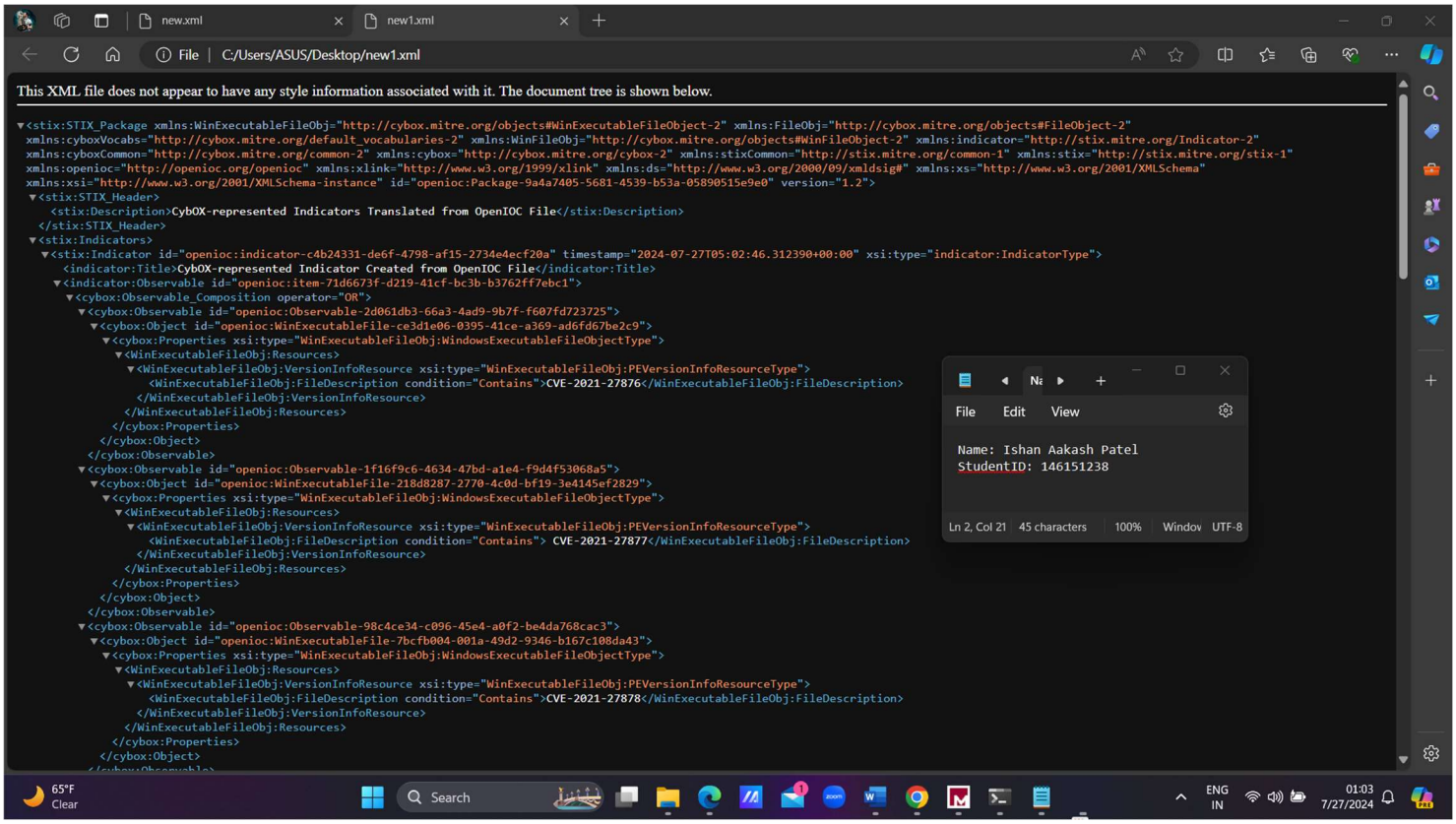
Command - python openioc-to-stix.py -i C:\Users\ASUS\Desktop\33232e72-b348-4ecc-be84-6a0a3c114f11.ioc -o C:\Users\ASUS\Desktop\new.xml

First I got error but then I installed some libs, and then everything way okay.

I ran both the iocs which I created in task 3.

Below will be the output…





I will also attach both the files - The IOCs that I have created and also the output xml files with the submission file.