

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 to STIX

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

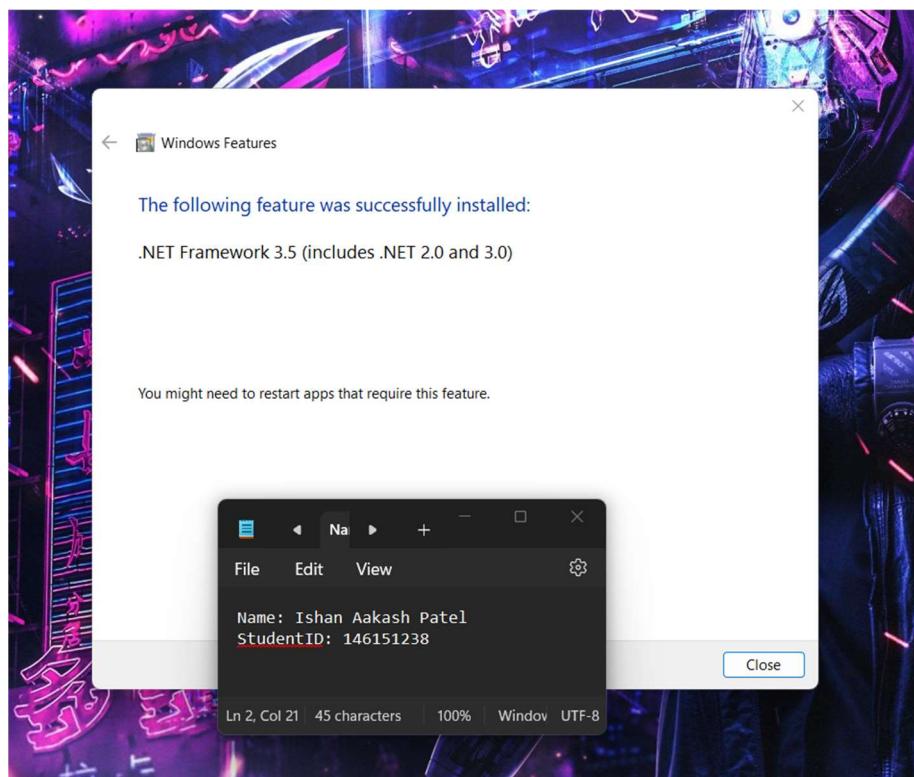
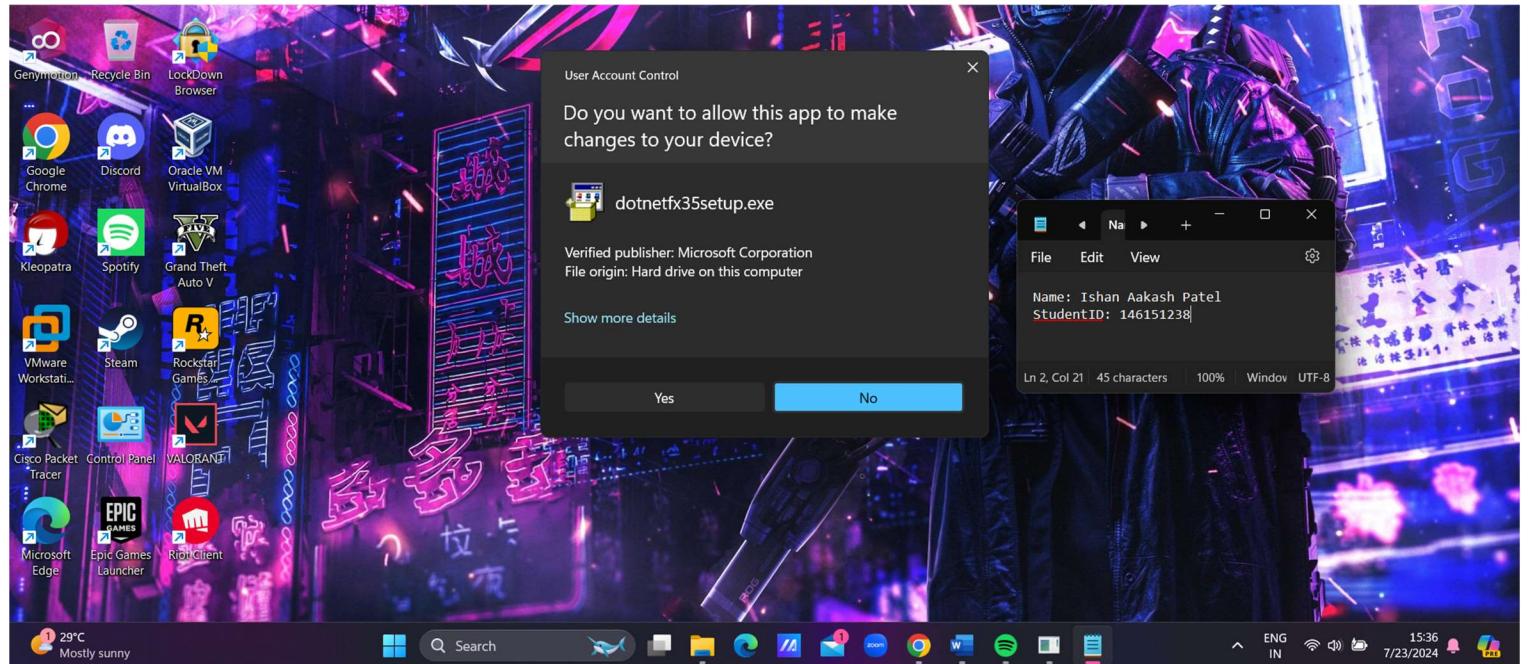
1. **Enhanced Detection Capabilities:** Using OpenIOC helps organizations improve their ability to detect and respond to threats more quickly and accurately.
2. **Improved Collaboration:** The standardized format of OpenIOC makes it easier for organizations to share threat information and collaborate 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



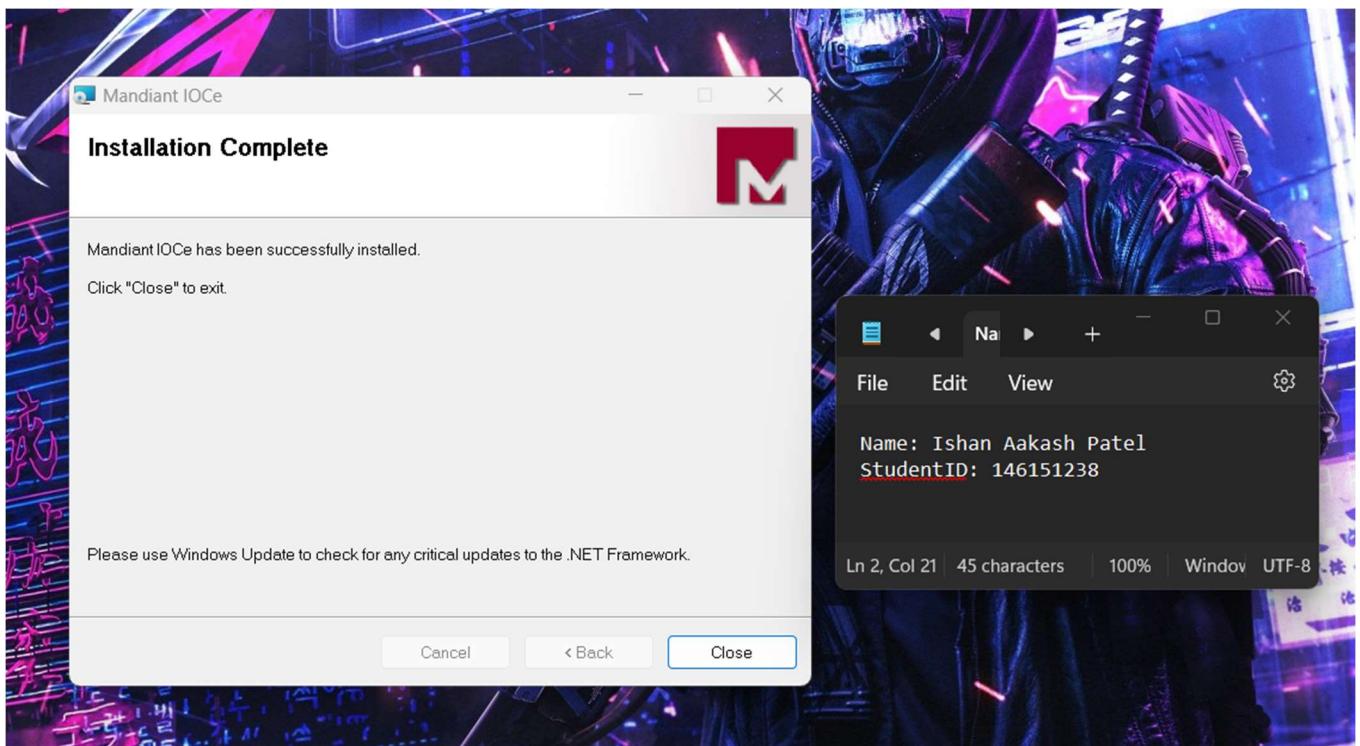
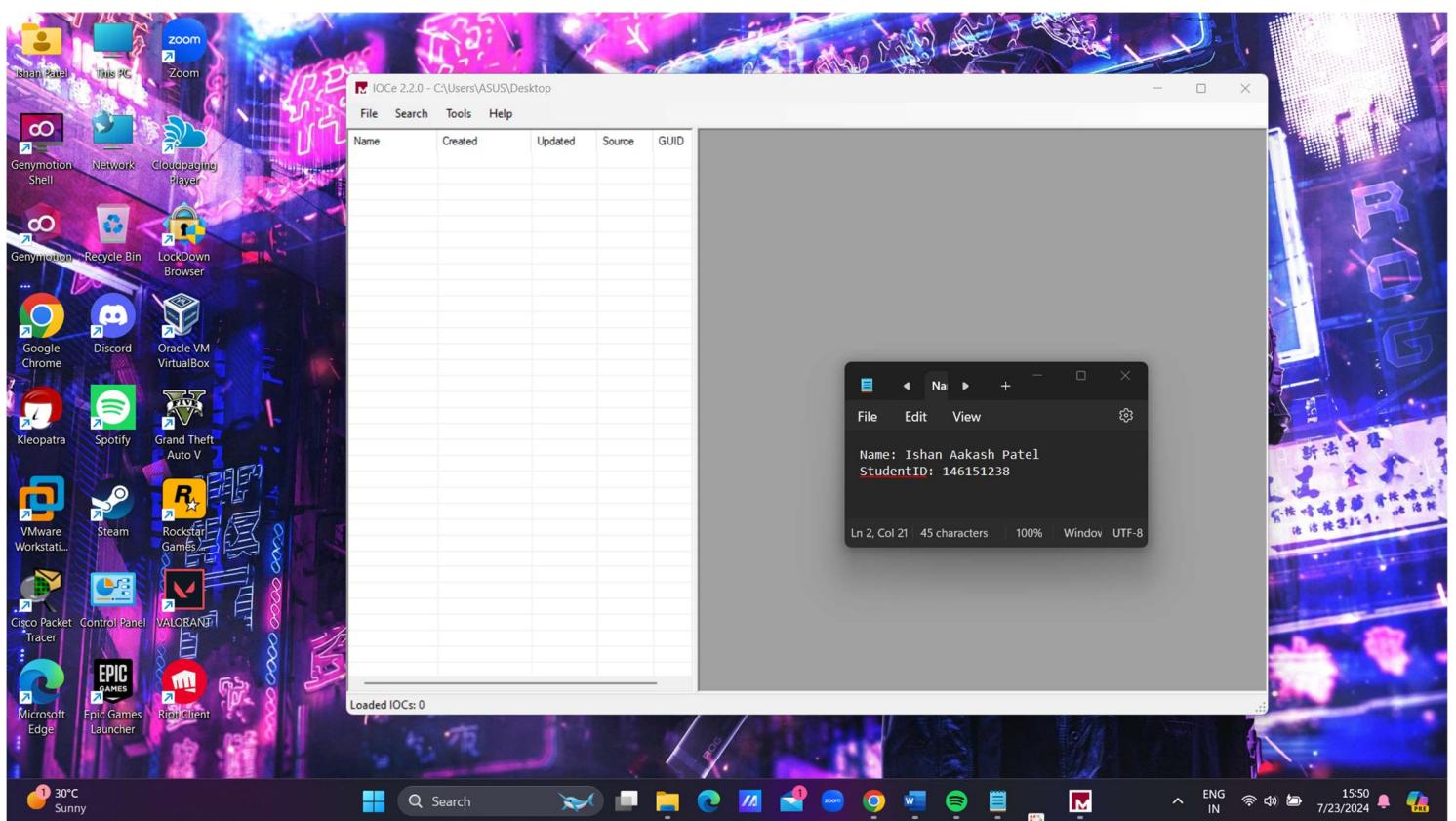


Figure 1 : Successfull Installed



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

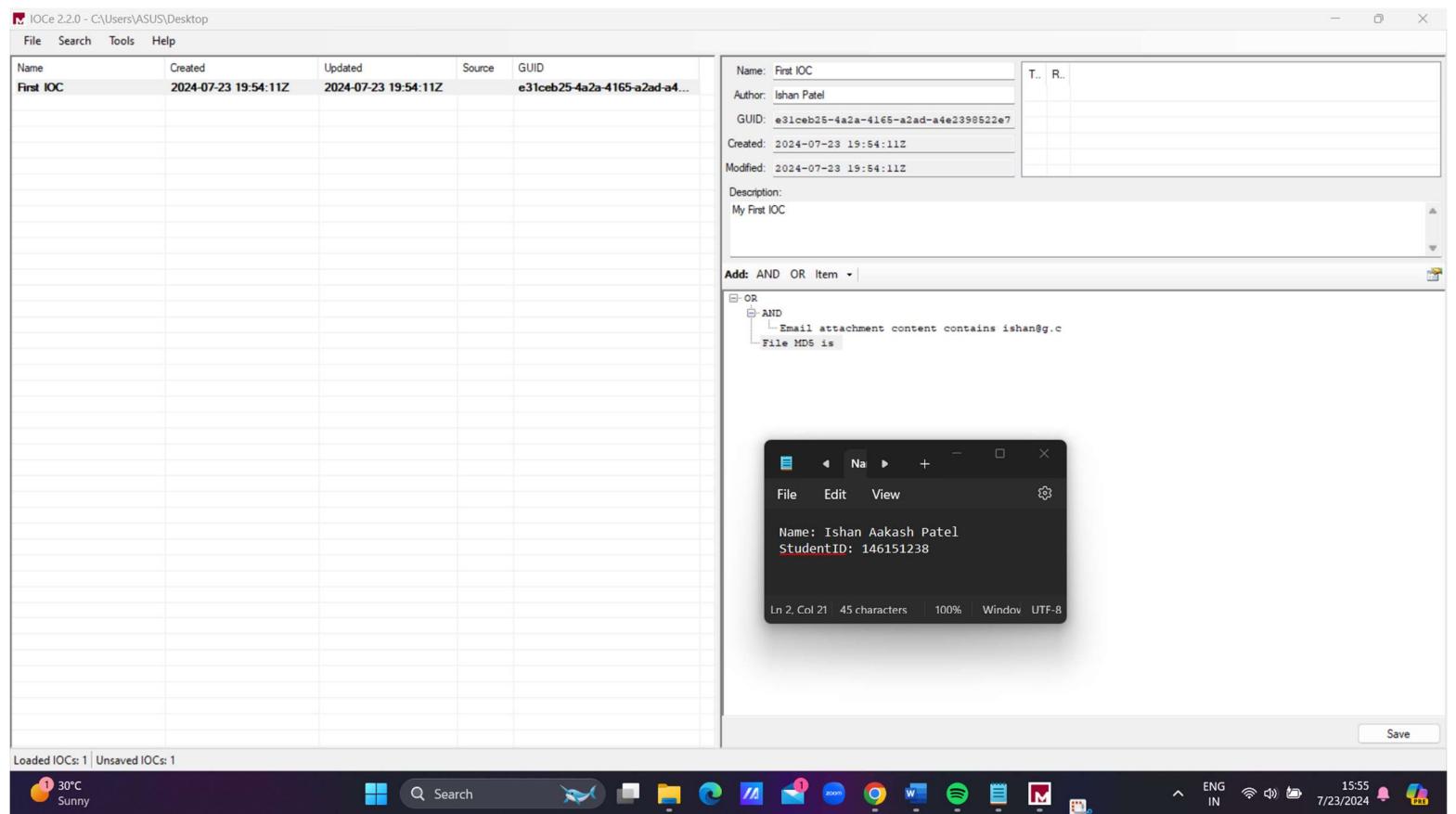


Figure 2 : Creating an IOC

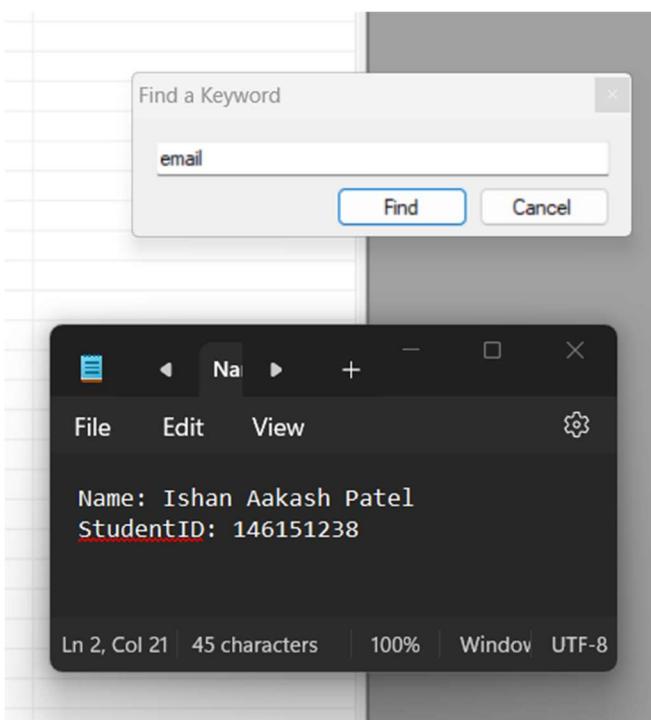


Figure 3 : Searching a Keyword

IOCe 2.2.0 - C:\Users\ASUS\Desktop

File Search Tools Help

Name	Created	Updated	Source	GUID
First IOC	2024-07-23 19:54:11Z	2024-07-23 19:56:19Z	Ishan Patel	e31ceb25-4a2a-4165-a2ad-a4e2398522e7

Name: First IOC
 Author: Ishan Patel
 GUID: e31ceb25-4a2a-4165-a2ad-a4e2398522e7
 Created: 2024-07-23 19:54:11Z
 Modified: 2024-07-23 19:56:19Z
 Description:
 My First IOC

Add: AND OR Item |

OR

- File MD5 is
- AND
 - Email attachment content contains ishan@g.c

File Edit View

Name: Ishan Aakash Patel
 StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window UTF-8

Figure 4 : Result after searching

IOCe 2.2.0 - C:\Users\ASUS\Desktop

File Search Tools Help

Name	Created	Updated	Source	GUID
IOC ...	2024-07-23 20:3...	2024-07-23 20:3...	93	
First ...	2024-07-23 19:5...	2024-07-23 19:5...	Ishan ...	e3

Name: IOC Messi
 Author: Ishan
 GUID: 93e97da0-19f1-4577-90de-06546361977f
 Created: 2024-07-23 20:36:32Z
 Modified: 2024-07-23 20:36:32Z
 Description:

Add: AND OR Item |

OR



Loaded IOCs: 2 | Unsaved IOCs: 2

Save

1 29°C Sunny

Search

Windows Taskbar icons: File Explorer, Edge, Mail, Spotify, etc.

System tray: ENG IN, WiFi, Battery, 16:38, 7/23/2024, etc.

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

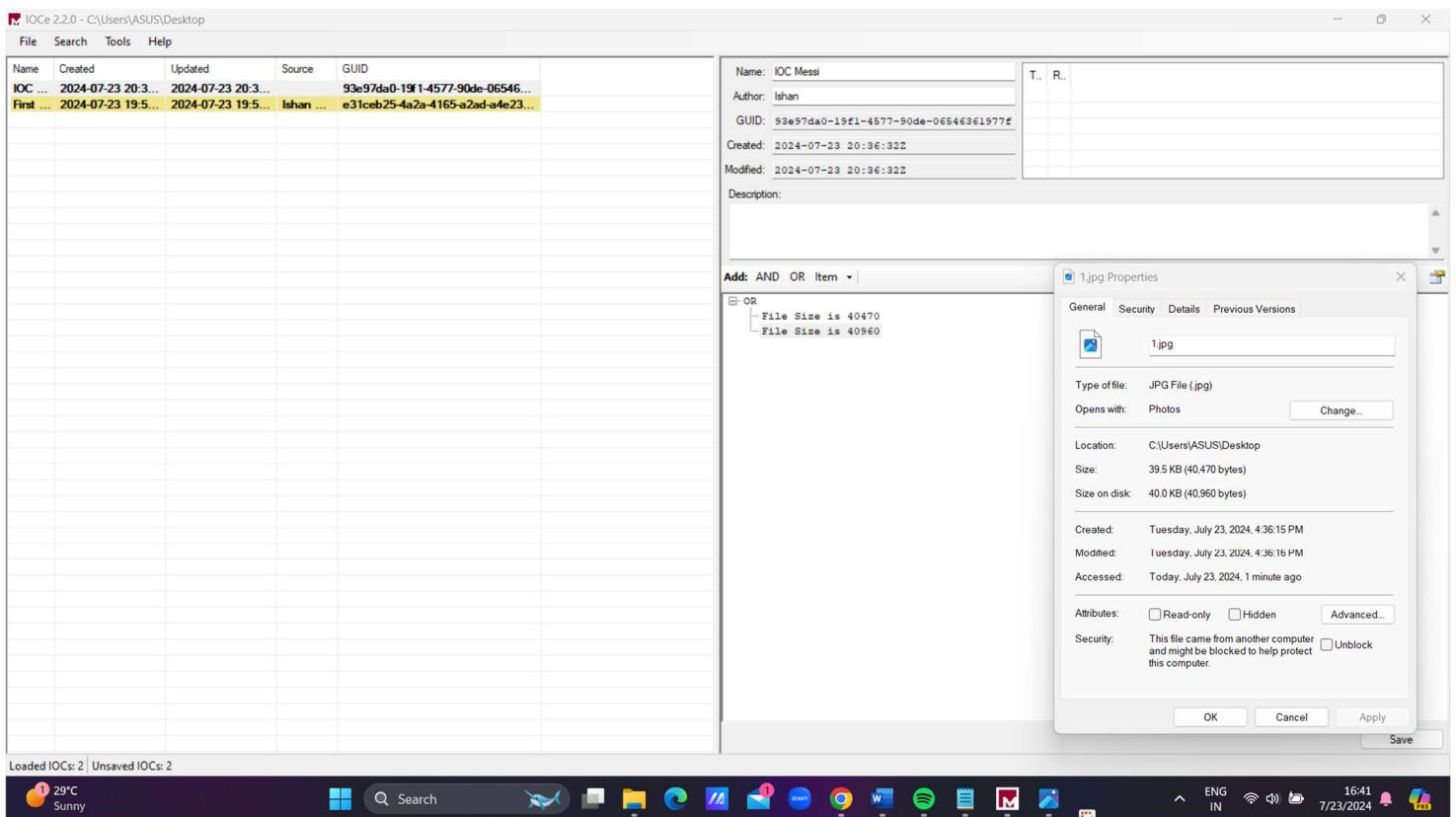


Figure 6: Adding file size

```

Windows PowerShell
PS C:\Users\ASUS\Desktop> Get-FileHash .\1.jpg
Algorithm      Hash
----- -----
SHA256        5557DC06D1FE988B02721A11D613F2A23B096190D3CC83F46255D5CC9081087D

PS C:\Users\ASUS\Desktop> Get-FileHash .\1.jpg -algorithm MD5
Algorithm      Hash
----- -----
MD5          60632D07B9EECB95BB278DFA2493BF95

PS C:\Users\ASUS\Desktop> Get-FileHash .\1.jpg -algorithm SHA1
Algorithm      Hash
----- -----
SHA1         2BE706FA1C914B711FB4EF9C61A41AF18AA663B3

```

Name: IOC Messi
Author: Ishan
GUID: 93e97da0-19f1-4577-90de-06546e31977f
Created: 2024-07-23 20:36:32Z
Modified: 2024-07-23 20:36:32Z
Description:

File Size is 40470
File Size is 40560

File Properties for 1.jpg:
General Security Details Previous Versions
Type of file: JPG File (.jpg)
Opens with: Photos Change...
Location: C:\Users\ASUS\Desktop
Size: 39.5 KB (40,470 bytes)
Size on disk: 40.0 KB (40,960 bytes)
Created: Tuesday, July 23, 2024, 4:36:15 PM
Modified: Tuesday, July 23, 2024, 4:36:16 PM
Accessed: Today, July 23, 2024, 1 minute ago
Attributes: Read-only Hidden Advanced...
Security: This file came from another computer and might be blocked to help protect this computer. Unblock
OK Cancel Apply Save

Loaded IOCs: 2 | Unsaved IOCs: 2

1 29°C Sunny Search Photos 16:45 7/23/2024 ENG IN WiFi Battery

Figure 7 : Now Adding different hashes

IOCe 2.2.0 - C:\Users\ASUS\Desktop

File Search Tools Help

Name	Created	Updated	Source	GUID
IOC ...	2024-07-23 20:3...	2024-07-23 20:3...		93e97da0-19f1-4577-90de-06546...
First ...	2024-07-23 19:5...	2024-07-23 19:5...	Ishan ...	e31ceb25-4a2a-4165-a2ad-a4e23...

1.jpg Properties

General Security Details Previous Versions

1.jpg

Type of file: JPG File (.jpg)

Opens with: Photos Change...

Location: C:\Users\ASUS\Desktop

Size: 39.5 KB (40,470 bytes)

Size on disk: 40.0 KB (40,960 bytes)

Created: Tuesday, July 23, 2024, 4:36:15 PM

Modified: Tuesday, July 23, 2024, 4:36:16 PM

Accessed: Today, July 23, 2024, 9 minutes ago

Attributes: Read-only Hidden Advanced...

Security: This file came from another computer and might be blocked to help protect this computer. Unblock

OK Cancel Apply

Loaded IOCs: 2 | Unsaved IOCs: 2

Windows PowerShell

```
PS C:\Users\ASUS\Desktop> Get-FileHash .\1.jpg
```

Algorithm	Hash	Path
SHA256	5557DC06D1FE988B02721A11D613F2A23B096190D3CC83F46255D5CC9081087D	C:\Users\ASUS\Desktop\1.jpg

```
PS C:\Users\ASUS\Desktop> Get-FileHash .\1.jpg -algorithm MD5
```

Algorithm	Hash	Path
MD5	60632D07B9EECB95BB278DFA2493BF95	C:\Users\ASUS\Desktop\1.jpg

```
PS C:\Users\ASUS\Desktop> Get-FileHash .\1.jpg -algorithm SHA1
```

Algorithm	Hash	Path
SHA1	2BE706FA1C914B711FB4EF9C61A41AF18AA663B3	C:\Users\ASUS\Desktop\1.jpg

29°C Sunny

Search

File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 45 characters 100% Window UTF-8

Add: AND OR Item |

OR

- File Size is 40470
- File Size is 40960
- File Stream Sha256sum is 5557DC06D1FE988B02721A11D613F2A23B096190D3CC83F46255D5CC9081087D
- File MD5 is 60632D07B9EECB95BB278DFA2493BF95
- File Shalsum is 2BE706FA1C914B711FB4EF9C61A41AF18AA663B3

Figure 8 : After adding everything

Name: IOC Messi

Author: Ishan

GUID: 93e97da0-19f1-4577-90de-06546361977f

Created: 2024-07-23 20:36:32Z

Modified: 2024-07-23 20:36:32Z

Description:

Add: AND OR Item ▾ |

- [-] OR
 - [-] File Size is 40470
 - [-] File Size is 40960
 - [-] File Name contains 1.jpg
- [-] AND
 - [-] OR
 - [-] File MD5 is 60632D07B9EECB95BB278DFA2493BF95
 - [-] File Shalsum is 2BE706FA1C914B711FB4EF9C61A41AF18AA663B3
 - [-] File Stream Sha256sum is 5557DC06D1FE988B02721A11D613F2A23B096190D3CC83F46255D5CC9081087D

The screenshot shows a search interface with a query builder. At the top, there are fields for Name, Author, GUID, Created, Modified, and Description. Below these is a dropdown menu labeled 'Add: AND OR Item ▾'. A red box highlights a section of the query tree under 'OR'. This section contains three items: 'File Size is 40470', 'File Size is 40960', and 'File Name contains 1.jpg'. Below this is another 'OR' node under 'AND', which contains three hash values: 'File MD5 is 60632D07B9EECB95BB278DFA2493BF95', 'File Shalsum is 2BE706FA1C914B711FB4EF9C61A41AF18AA663B3', and 'File Stream Sha256sum is 5557DC06D1FE988B02721A11D613F2A23B096190D3CC83F46255D5CC9081087D'. At the bottom of the interface is a terminal-like window showing the command-line input and output.

```
Name: IOC Messi
Author: Ishan
GUID: 93e97da0-19f1-4577-90de-06546361977f
Created: 2024-07-23 20:36:32Z
Modified: 2024-07-23 20:36:32Z
Description:

Add: AND OR Item ▾ |
```

- [-] OR
 - [-] File Size is 40470
 - [-] File Size is 40960
 - [-] File Name contains 1.jpg
- [-] AND
 - [-] OR
 - [-] File MD5 is 60632D07B9EECB95BB278DFA2493BF95
 - [-] File Shalsum is 2BE706FA1C914B711FB4EF9C61A41AF18AA663B3
 - [-] File Stream Sha256sum is 5557DC06D1FE988B02721A11D613F2A23B096190D3CC83F46255D5CC9081087D

```
Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window UTF-8
```

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

The screenshot shows the OTX AlienVault interface with three tabs open: "Greeting and Assistance - Cloud", "Nokoyawa ransomware attacks", and "ALPHV Ransomware-Affiliate T1". The "Nokoyawa ransomware attacks" tab is active, displaying a list of IOCs. A modal window titled "Create Pulse" is open, showing the details for a new IOC named "okoyawa ransomware attacks with Windows zero-day". The IOC has been created on 2024-07-27 03:39:10Z and modified on 2024-07-27 03:39:10Z by user ishan. The modal also shows a description field and a condition builder section. The condition builder shows an OR operator with two conditions: File MD5 is 1e4dd35b16ddc59c1ecf240c22b8a4c4 and File MD5 is 46168ed7dbe33ffc4179974f8bf401aa. Below the condition builder, there is a note about AND/OR operators and a save button.

Indicators of Compromise (7)

FileHash-MD5 (5)

Domain (2)

TYPES OF INDICATORS

Show [10] entries

TYPE	INDICATOR
FileHash-MD5	1e4dd35b16ddc59c1ecf240c22b8a4c4
FileHash-MD5	46168ed7dbe33ffc4179974f8bf401aa
FileHash-MD5	8800e6f1501f69a0a04ce709e9fa251c
FileHash-MD5	a2313d7fdb2f8f5e5c1962e22b504a17
FileHash-MD5	f23be19024fcc7c8f885dfa16634e6e7
domain	qqgle.top
domain	vsexec.com

Showing 1 TO 7 OF 7 ENTRIES

Name: okoyawa ransomware attacks with Windows zero-day
Created: 2024-07-27 03:39:10Z
Updated: 2024-07-27 03:39:10Z
Author: ishan
GUID: 33232e72-b349-4ecc-be84-6a0a3c114f11
Created: 2024-07-27 03:39:10Z
Modified: 2024-07-27 03:39:10Z
Description:

Add: AND OR Item

OR

- File MD5 is 1e4dd35b16ddc59c1ecf240c22b8a4c4
- File MD5 is 46168ed7dbe33ffc4179974f8bf401aa
- File MD5 is 8800e6f1501f69a0a04ce709e9fa251c
- File MD5 is a2313d7fdb2f8f5e5c1962e22b504a17
- File MD5 is f23be19024fcc7c8f885dfa16634e6e7

OR

- Network DNS contains vsexec.com
- Network DNS contains google.top

Ln 2, Col 21 45 characters 100% Window UTF-8

Loaded IOCs: 2 | Unsaved IOCs: 1

Save

66°F Clear

Search

File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

23:58 7/26/2024

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

LevelBlue/Labs Dashboard Browse Scan Endpoints Create Pulse Search OTX

IPv4 (4) FileHash-SHA256 (3)

TYPES OF INDICATORS

Show 10 entries

Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 45 characters 100% Window UTF-8

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	1f437347917f0a4ced71fb7df53bla05	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: Expiration: Related Pulses: 68

Role:

IOCe 2.2.0 - C:\Users\ASUS\Desktop

File Search Tools Help

Name	Created	Updated	So...	GUID
ALPH...	2024-07-27 04:0...	2024-07-27 04:0...		037c3a35-85aa-4!
IOC Mess...	2024-07-23 20:36:32Z	2024-07-23 20:54:36Z	Ishan	93e97da0-19f1-4577-
Nokoy...	2024-07-27 03:3...	2024-07-27 03:3...		33232e72-b348-4

Name: ALPHV Ransomware Affiliate Targets Vulnerable Back Author: Ishan GUID: 037c3a35-85aa-4864-b4f0-3e36f8256edc2 Created: 2024-07-27 04:07:242 Modified: 2024-07-27 04:07:242 Description:

Add: AND OR Item ▾

OR

- 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

- File MD5 is 17424a22f01b7b996810ba1274f7b8e9
- File MD5 is 5fe66b2835511f9d4d3703b6c639b866
- File MD5 is b41dc7bef82ef384bc884973f3d0e8ca
- File MD5 is da202cc4b3679fdb47003d603a93c90d
- File MD5 is e31270e4a6f215f45abad65916da9db4

OR

- File Name contains GoLandBuildPE
- File MD5 is 1f437347917f0a4ced71fb7df53bla05

OR

- File Name contains HackTool:Win32/LaZagne
- File MD5 is 68d3bf2c363144ec6874ab360fdda00a

File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 45 characters 100% Window UTF-8

Save

Loaded IOCs: 3 | Unsaved IOCs: 2

from Lawrence... Closed road

Search

7/27/2024 00:19 ENG IN

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

```

Windows PowerShell x Windows PowerShell x + -
PS C:\Users\ASUS> cd .\Downloads\
PS C:\Users\ASUS\Downloads> cd .\openioc-to-stix-master\
PS C:\Users\ASUS\Downloads\openioc-to-stix-master> cd .\openioc-to-stix-master\examples\
PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master\examples> ls

Directory: C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master\examples

Mode                LastWriteTime       Length Name
----                -----        ---- 
-a----    7/27/2024      00:47         3291 ccapp.ioc.xml
-a----    7/27/2024      00:47         7947 ccapp.stix.xml
-a----    7/27/2024      00:47         8794 duqu.ioc.xml
-a----    7/27/2024      00:47        25003 duqu.stix.xml
-a----    7/27/2024      00:47         4469 find_windows.ioc.xml
-a----    7/27/2024      00:47        10401 find_windows.stix.xml
-a----    7/27/2024      00:47         7371 msbgt.ioc.xml
-a----    7/27/2024      00:47        18913 msbgt.stix.xml
-a----    7/27/2024      00:47          427 README
-a----    7/27/2024      00:47        10063 shelldc_backdoor.ioc.xml
-a----    7/27/2024      00:47        25853 shelldc_backdoor.stix.xml
-a----    7/27/2024      00:47         6029 stuxnet.ioc.xml
-a----    7/27/2024      00:47        15556 stuxnet.stix.xml
-a----    7/27/2024      00:47         4407 zeus.ioc.xml
-a----    7/27/2024      00:47        14450 zeus.stix.xml

PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master\examples> pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
ERROR: Could not open requirements file: [Errno 2] No such file or directory: 'requirements.txt'
PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master\examples> cd ..
PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master> pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting cybox==2.1.0.13 (from -r requirements.txt (line 1))
  Using cached cybox-2.1.0.13-py3-none-any.whl
Collecting lxml==3.7.1 (from -r requirements.txt (line 2))
  Using cached lxml-3.7.1.tar.gz (3.8 MB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done

65°F Clear  Search File Edit View  ENG IN 00:59 7/27/2024  File Explorer  Requirements.txt
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

```

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

```

Windows PowerShell x Windows PowerShell x + -
PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master\examples> cd ..
PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master> pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting cybox==2.1.0.13 (from -r requirements.txt (line 1))
  Using cached cybox-2.1.0.13-py3-none-any.whl
Collecting lxml==3.7.1 (from -r requirements.txt (line 2))
  Using cached lxml-3.7.1.tar.gz (3.8 MB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting mixbox==1.0.1 (from -r requirements.txt (line 3))
  Using cached mixbox-1.0.1-py2.py3-none-any.whl.metadata (2.3 kB)
Collecting python-dateutil==2.6.0 (from -r requirements.txt (line 4))
  Using cached python_dateutil-2.6.0-py2.py3-none-any.whl.metadata (1.1 kB)
Collecting six==1.10.0 (from -r requirements.txt (line 5))
  Using cached six-1.10.0-py2.py3-none-any.whl.metadata (1.3 kB)
Collecting stix==1.2.0.2 (from -r requirements.txt (line 6))
  Using cached stix-1.2.0.2-py2.py3-none-any.whl.metadata (4.7 kB)
Collecting nose==1.3.7 (from -r requirements.txt (line 8))
  Using cached nose-1.3.7-py3-none-any.whl.metadata (1.7 kB)
Collecting tox==2.5.0 (from -r requirements.txt (line 9))
  Using cached tox-2.5.0-py2.py3-none-any.whl.metadata (2.3 kB)
Collecting bumpversion==0.5.3 (from -r requirements.txt (line 10))
  Using cached bumpversion-0.5.3-py2.py3-none-any.whl.metadata (17 kB)
Requirement already satisfied: ordered-set in c:\users\asus\appdata\roaming\python\python312\site-packages (from mixbox==1.0.1->-r requirements.txt (line 3)) (4.1.0)
Requirement already satisfied: virtualenv>=1.11.2 in c:\users\asus\appdata\roaming\python\python312\site-packages (from tox==2.5.0->-r requirements.txt (line 9)) (20.26.2)
Collecting py>=1.4.17 (from tox==2.5.0->-r requirements.txt (line 9))
  Using cached py-1.11.0-py2.py3-none-any.whl.metadata (2.8 kB)
Collecting pluggy<1.0,>=0.3.0 (from tox==2.5.0->-r requirements.txt (line 9))
  Using cached pluggy-0.13.1-py2.py3-none-any.whl.metadata (15 kB)
Requirement already satisfied: distlib<1,>=0.3.7 in c:\users\appdata\roaming\python\python312\site-packages (from virtualenv>=1.11.2->tox==2.5.0->-r requirements.txt (line 9)) (0.3.8)
Requirement already satisfied: filelock<4,>=3.12.2 in c:\users\asus\appdata\roaming\python\python312\site-packages (from virtualenv>=1.11.2->tox==2.5.0->-r requirements.txt (line 9)) (3.14.0)
Requirement already satisfied: platformdirs>5,>=3.9.1 in c:\users\asus\appdata\roaming\python\python312\site-packages (from virtualenv>=1.11.2->tox==2.5.0->-r requirements.txt (line 9)) (3.11.0)
Using cached mixbox-1.0.1-py2.py3-none-any.whl (46 kB)
Using cached python_dateutil-2.6.0-py2.py3-none-any.whl (194 kB)

65°F Clear  Search File Edit View  ENG IN 00:59 7/27/2024  File Explorer  Requirements.txt
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

```

```
PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master> python openioc-to-stix.py -i C:\Users\ASUS\Desktop\33232e72-b348-4ecc-be84-6a0a3c114f11.ioc -o C:\Users\ASUS\Desktop\new.xml
Traceback (most recent call last):
  File "C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master\openioc-to-stix.py", line 14, in <module>
    from stix import utils
  File "C:\Users\ASUS\AppData\Roaming\Python\Python32\site-packages\stix\__init__.py", line 5, in <module>
    from .base import (Entity, EntityList, TypedCollection, TypedList, # noqa
  File "C:\Users\ASUS\AppData\Roaming\Python\Python32\site-packages\stix\base.py", line 20, in <module>
    from . import utils
  File "C:\Users\ASUS\AppData\Roaming\Python\Python32\site-packages\stix\utils\__init__.py", line 382, in <module>
    from .parser import * # noqa
  ^^^^^^^^^^^^^^^^^^
  File "C:\Users\ASUS\AppData\Roaming\Python\Python32\site-packages\stix\utils\parser.py", line 7, in <module>
    import mixbox.parser
  File "C:\Users\ASUS\AppData\Roaming\Python\Python32\site-packages\mixbox\parser.py", line 5, in <module>
    from distutils.version import StrictVersion
ModuleNotFoundError: No module named 'distutils'
PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master> sudo apt-get install python3-distutils
sudo: The term 'sudo' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the command, or if it exists, try 'sudo -l'.
was included, verify that the path is correct and try again.
At line:1 char:1
+ sudo apt-get install python3-distutils
+ ~~~~
  + CategoryInfo          : ObjectNotFound: (sudo:String) [], CommandNotFoundException
  + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master> python openioc-to-stix.py -i C:\Users\ASUS\Desktop\33232e72-b348-4ecc-be84-6a0a3c114f11.ioc -o C:\Users\ASUS\Desktop\new.xml
PS C:\Users\ASUS\Downloads\openioc-to-stix-master\openioc-to-stix-master> |
```

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 was okay.

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

Below will be the output...

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<stix:STIX_Package xmlns:FileObj="http://cybox.mitre.org/objects#fileObject-2" xmlns:NetworkConnectionObj="http://cybox.mitre.org/objects#NetworkConnectionObject-2" xmlns:cyboxVocab="http://cybox.mitre.org/default_vocabularies-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2" xmlns:stix="http://stix.mitre.org/stix-1" xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:openioc="http://openioc.org/openioc" id="openioc-Package-e6c06b9e-c853-4d42-ae8d-4741a1185b" version="1.2">
  <!-- stix:STIX_Header -->
  <stix:Description>CyBOX-represented Indicators Translated from OpenIOC File</stix:Description>
  </stix:STIX_Header>
  <stix:Indicators>
    <stix:Indicator id="openioc:indicator-64db544-e5cf-48a2-a41c-5fdd6a4851a" timestamp="2024-07-27T04:57:57.108320+00:00" xsi:type="IndicatorType">
      <Indicator>CyBOX-represented Indicator Created from OpenIOC File</Indicator>
      <Observable id="openioc:object-item-35dc445b-01c3-42c9-b228-03684dbb535">
        <cybox:ObservationComposition operator="OR">
          <cybox:Observation id="openioc:Observation-f8761a85-e0f6-4333-98e6-dc085dfaec38">
            <cybox:Object id="openioc:File-3681a762-aa55-4cad-89a9-a596f3239347">
              <cybox:Properties xsi:type="FileObj:FileObjectType">
                <FileObj:Hashes>
                  <cyboxCommon:Hash>
                    <cyboxCommon:Type xsi:type="cyboxVocab:HashNameVocab-1.0">MD5</cyboxCommon:Type>
                    <cyboxCommon:Simple_Hash_Value condition="Equals">1e4dd3b16ddc59c1ecf240c22b8a4c4</cyboxCommon:Simple_Hash_Value>
                  </cyboxCommon:Hash>
                </FileObj:Hashes>
              </cybox:Properties>
            </cybox:Observation>
          </cybox:ObservationComposition>
        </cybox:Observation>
      </cybox:ObservationComposition>
    </stix:Indicator>
    <stix:Indicator id="openioc:Observable-c92d3ef0-4bba-4b3f-bbd6-23cf5ce89f6">
      <Observable id="openioc:File-642bc760-507c-4f61-bc2d-1ad1e0dd3f1b">
        <cybox:Properties xsi:type="FileObj:FileObjectType">
          <FileObj:Hashes>
            <cyboxCommon:Hash>
              <cyboxCommon:Type xsi:type="cyboxVocab:HashNameVocab-1.0">MD5</cyboxCommon:Type>
              <cyboxCommon:Simple_Hash_Value condition="Equals">46168ed7edbe33ff4179974f8bf401aa</cyboxCommon:Simple_Hash_Value>
            </cyboxCommon:Hash>
          </FileObj:Hashes>
        </cybox:Properties>
      </Observable>
    </stix:Indicator>
    <stix:Indicator id="openioc:Observable-53870f46-5b69-4f6d-ad38-293e75d9e0cc">
      <Observable id="openioc:File-4d0c5de7-b5ca-4644-9cc4-f483f0569b1d">
        <cybox:Properties xsi:type="FileObj:FileObjectType">
          <FileObj:Hashes>
            <cyboxCommon:Hash>
              <cyboxCommon:Type xsi:type="cyboxVocab:HashNameVocab-1.0">MD5</cyboxCommon:Type>
              <cyboxCommon:Simple_Hash_Value condition="Equals">8800e6f101f69a0a04ce709e9fa251c</cyboxCommon:Simple_Hash_Value>
            </cyboxCommon:Hash>
          </FileObj:Hashes>
        </cybox:Properties>
      </Observable>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<stix:STIX_Package xmlns:WinExecutableFileObj="http://cybox.mitre.org/objects#WinExecutableFileObject-2" xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
  xmlns:cyboxVocab="http://cybox.mitre.org/default_vocabularies-2" xmlns:WinFileObj="http://cybox.mitre.org/objects#WinFileObject-2" xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:cyboxCommon="http://cybox.mitre.org/common-2" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:openioc="http://openioc.org/openioc" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="openioc:Package-9a4a7405-5681-4539-b53a-05890515e9e0" version="1.2">
  <stix:STIX_Header>
    <stix:Description>CyBOX-represented Indicators Translated from OpenIOC File</stix:Description>
  </stix:STIX_Header>
  <stix:Indicators>
    <stix:Indicator id="openioc:indicator-c4b24331-de6f-4798-af15-2734e4ecf20a" timestamp="2024-07-27T05:02:46.312390+00:00" xsi:type="indicator:IndicatorType">
      <indicator:Title>CyBOX-represented Indicator Created from OpenIOC File</indicator:Title>
      <indicator:Observable id="openioc:item-71d6673f-d219-41cf-bc3b-b3762ffebc1">
        <cybox:Observation_Composition operator="OR">
          <cybox:Observable id="openioc:Observable-2d061db3-66a3-4ad9-9bf-f607fd723725">
            <cybox:Object id="openioc:WinExecutableFile-ce3d1e06-0395-41ce-a369-ad6fd57be2c9">
              <cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutablefileObjectType">
                <WinExecutablefileObj:Resources>
                  <WinExecutablefileObj:VersionInfoResource xsi:type="WinExecutablefileObj:PEVersionInfoResourceType">
                    <WinExecutablefileObj:FileDescription condition="Contains">CVE-2021-27876</WinExecutablefileObj:FileDescription>
                  </WinExecutablefileObj:VersionInfoResource>
                </WinExecutablefileObj:Resources>
              </cybox:Properties>
            </cybox:Object>
          </cybox:Observable>
        </cybox:Observation_Composition>
        <cybox:Observable id="openioc:Observable-1f16f9c6-4634-47bd-a1c4-f9d4f53068a5">
          <cybox:Object id="openioc:WinExecutableFile-18b8287-2770-4c0d-bf19-3e4145ef2829">
            <cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutablefileObjectType">
              <WinExecutablefileObj:Resources>
                <WinExecutablefileObj:VersionInfoResource xsi:type="WinExecutablefileObj:PEVersionInfoResourceType">
                  <WinExecutablefileObj:FileDescription condition="Contains">CVE-2021-27877</WinExecutablefileObj:FileDescription>
                </WinExecutablefileObj:VersionInfoResource>
              </WinExecutablefileObj:Resources>
            </cybox:Properties>
          </cybox:Object>
        </cybox:Observable>
      </cybox:Observation_Composition>
      <cybox:Observable id="openioc:Observable-98c4ce34-c096-45e4-a0f2-be4da768cac3">
        <cybox:Object id="openioc:WinExecutableFile-7bcfb004-001a-49d2-9346-b167c108da43">
          <cybox:Properties xsi:type="WinExecutableFileObj:WindowsExecutablefileObjectType">
            <WinExecutablefileObj:Resources>
              <WinExecutablefileObj:VersionInfoResource xsi:type="WinExecutablefileObj:PEVersionInfoResourceType">
                <WinExecutablefileObj:FileDescription condition="Contains">CVE-2021-27878</WinExecutablefileObj:FileDescription>
              </WinExecutablefileObj:VersionInfoResource>
            </WinExecutablefileObj:Resources>
          </cybox:Properties>
        </cybox:Object>
      </cybox:Observation_Composition>
    </stix:Indicator>
  </stix:Indicators>

```

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