# Lab 11

# Creating and Using IOCs

Mina Salehi

University of Maryland Baltimore County

CYBR 642 Introduction to Digital Forensics

Presented to: Gina Scaldaferri

05/07/2025

## Introduction

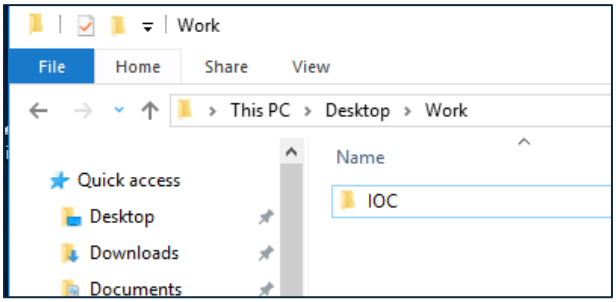
Identifying and responding to threats promptly is critical to minimizing damage and preventing further compromise. One of the most effective techniques for achieving this is using Indicators of Compromise (IOCs). An IOC is a piece of forensic data—such as a file hash, IP address, domain name, or registry key—that can serve as a signpost of malicious activity within a system or network (Scarfone & Mell, 2023). Lab 11 focuses on the creation and practical application of IOCs specific to a known malicious application.

The first component of this lab involves generating an IOC that uniquely identifies the behavior or signature of a malicious program. This IOC can then be shared with stakeholders or used internally to detect similar threats organizational threats. The second component utilizes the crafted IOC to search multiple computer systems for the presence of this threat, helping security teams identify affected machines and trace the extent of compromise. This process is foundational to incident response and threat intelligence sharing, aligning with modern practices in digital forensics and proactive defense strategies.

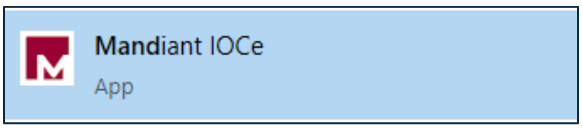
By the end of this lab, students will gain hands-on experience in both creating and leveraging IOCs, thereby enhancing their ability to detect, respond to, and mitigate cybersecurity threats efficiently.

# Instructions: Creating an Indicator of Compromise (IOC)

1. Set Up the Working Directory
    a. Create a new folder on your desktop for organizing IOC files.
    b. Example: Create a folder named IOC inside a parent folder called Work (i.e., Desktop > Work > IOC).




2. Open Mandiant IOC Editor
    a. Launch the Mandiant IOC Editor application on your system.




3. Create a New Indicator File
    a. In the IOC Editor, navigate to the menu and select: File > New > Indicator
    b. This will open a new blank IOC template.
4. Enter Basic IOC Metadata
    a. In the Header section of the IOC:
        i. Enter a Name for the indicator (e.g., *LairNetPutty IOC*).
        ii. Enter your Name or Identifier in the Author field.

5. Add Indicator Values

    a. Begin populating the IOC with specific artifacts observed during earlier analysis of the LairNetPutty.exe file (from Week 1).

    b. Suggested values to include:

        i. Filename: LairNetPutty.exe

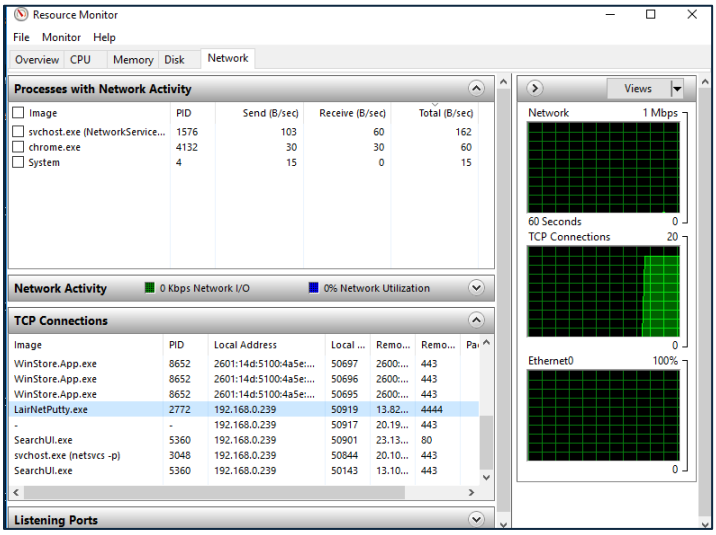
        ii. File hash: Add any available MD5, SHA-1, or SHA-256 hash values.

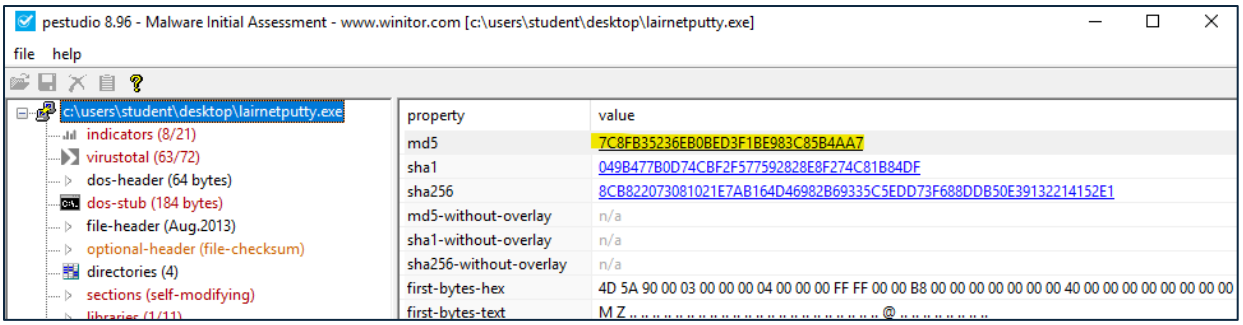
        iii. IP address or Domain name: Include any external connections made by the file.

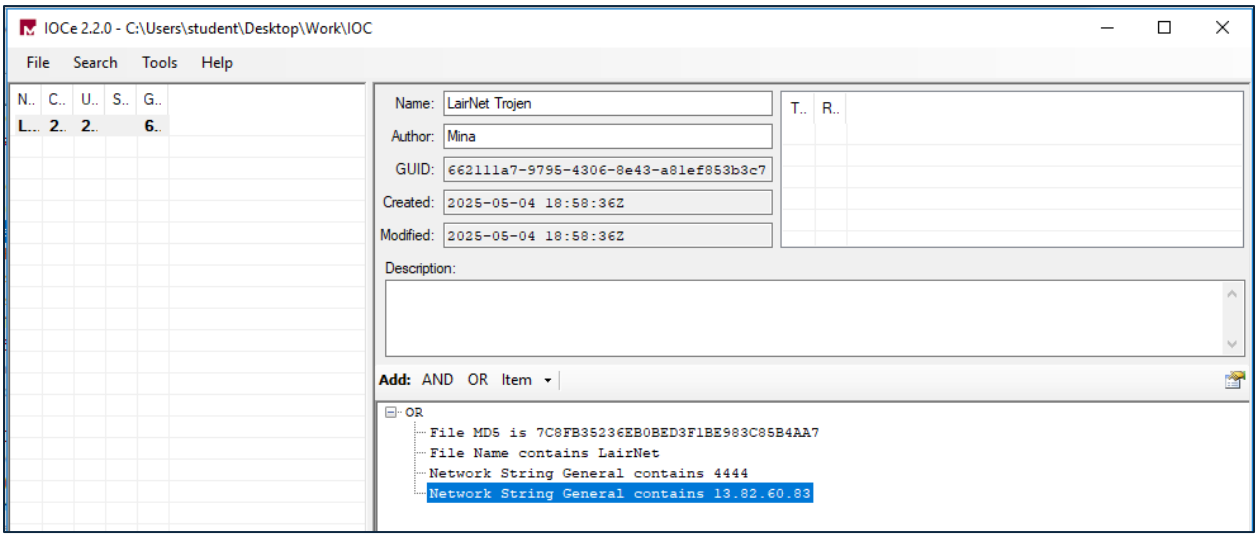
        iv. Registry keys, file paths (if previously discovered).

        v. Each value should be added as a separate indicator item.

I utilized Windows Resource Monitor to observe system activity. LairNet PuTTY established a connection to IP address 13.82.60.83 via port 4444. This IP address is registered to Microsoft Corporation.



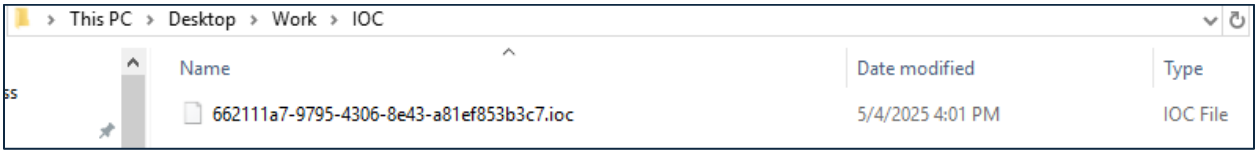



6. Save the IOC File

    a. After populating the indicator, go to File > Save As.

    b. Save the .ioc file in your previously created IOC directory on your desktop.

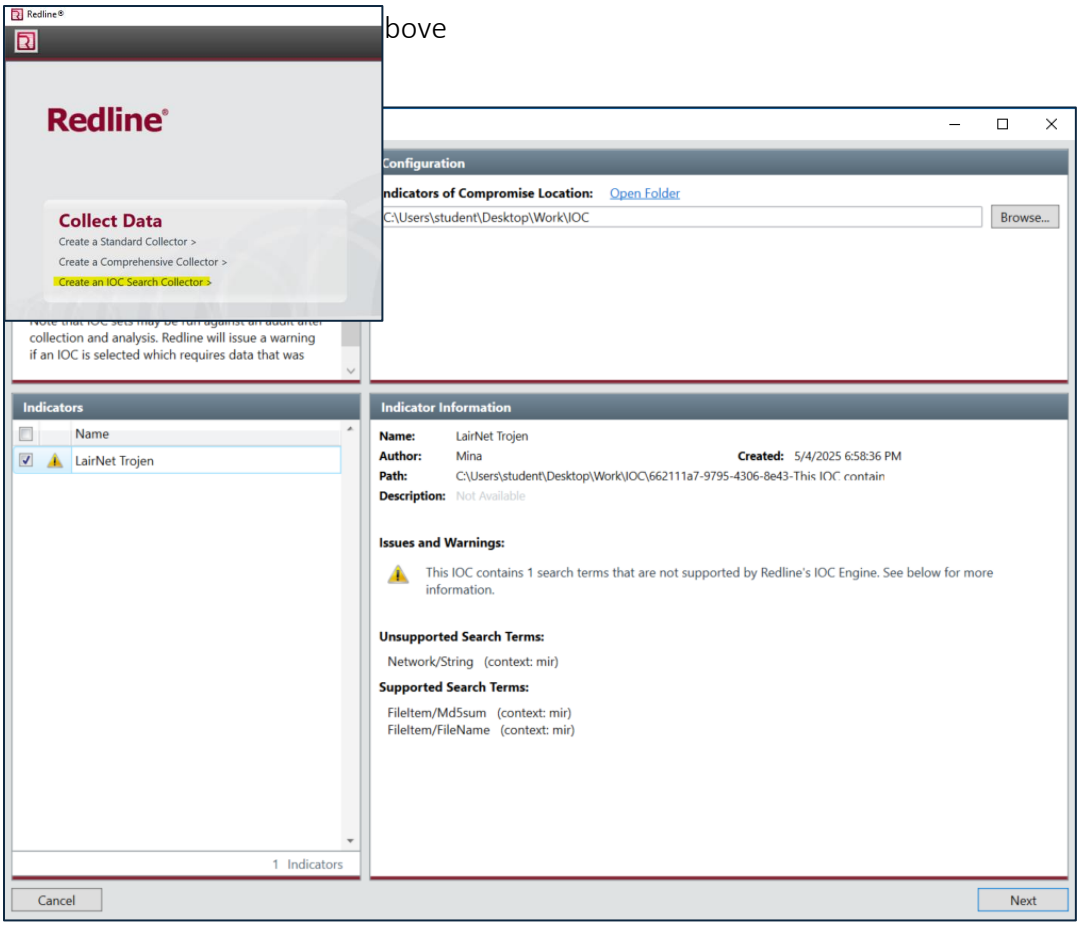



Using the Indicator of Compromise

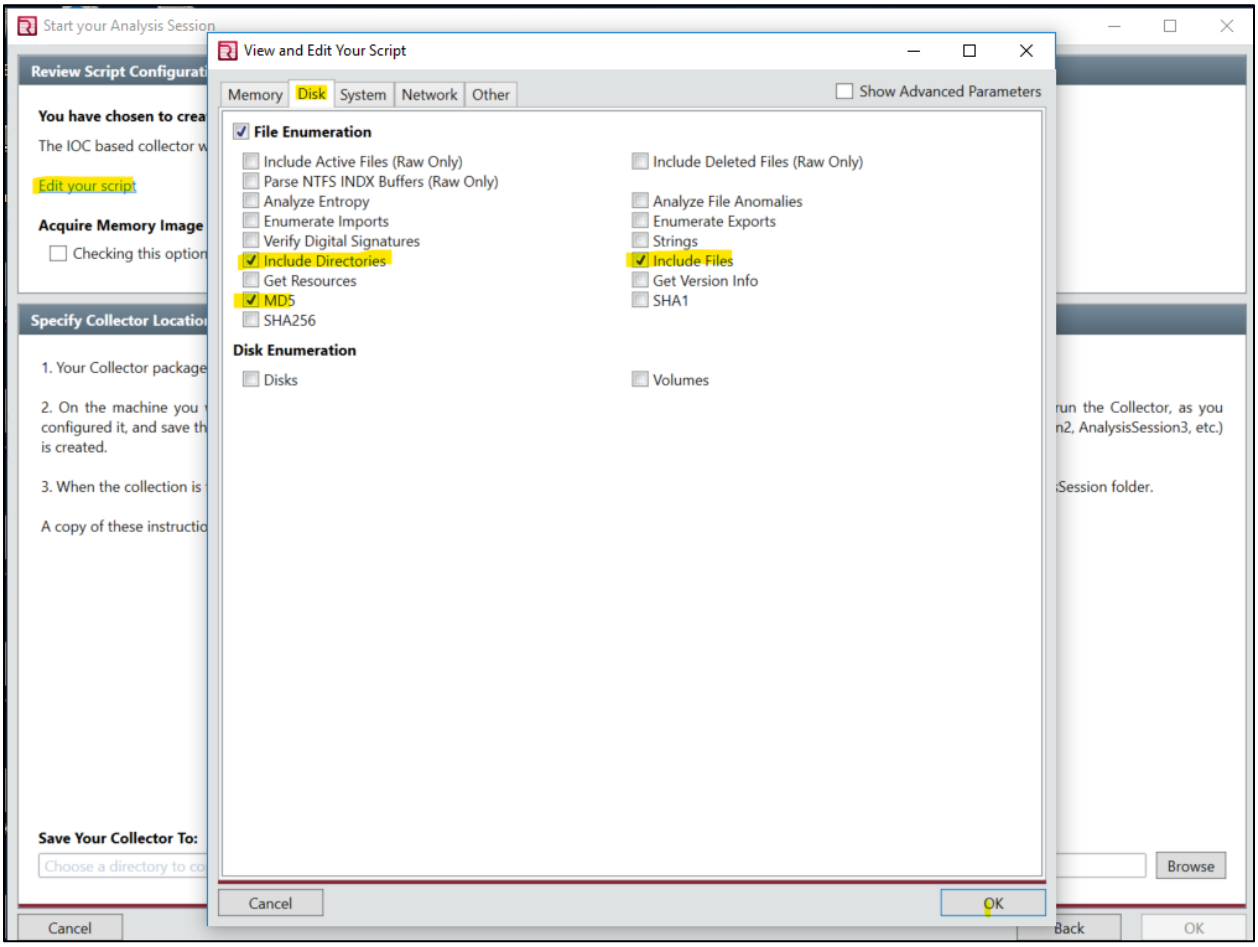
1- Using Mandiant's Redline application, create a new IOC

search collector, and point it to the directory you've

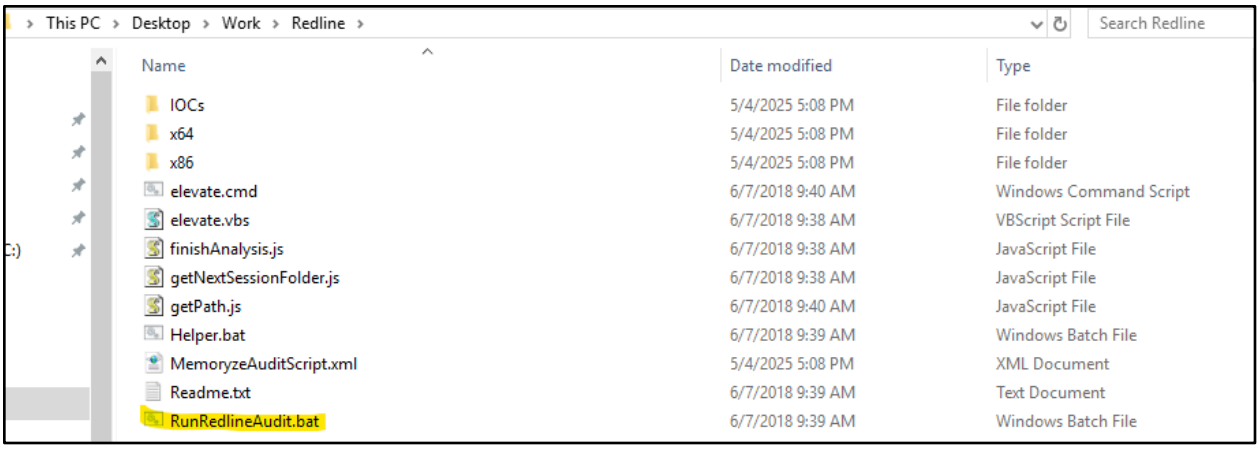
bove


Redline®
Redline
Collect Data
Create a Standard Collector >
Create a Comprehensive Collector >
Create an IOC Search Collector >
collection and analysis. Redline will issue a warning
if an IOC is selected which requires data that was
Configuration
ndicators of Compromise Location:
Open Folder
C:\Users\student\Desktop\Work\IOC
Browse...
Indicators
Name
LairNet Trojen
1 Indicators
Indicator Information
Name: LairNet Trojen
Author: Mina
Created: 5/4/2025 6:58:36 PM
Path: C:\Users\student\Desktop\Work\IOC\662111a7-9795-4306-8e43-This IOC contain
Description: Not Available
Issues and Warnings:
This IOC contains 1 search terms that are not supported by Redline's IOC Engine. See below for more information.
Unsupported Search Terms:
Network/String (context: mir)
Supported Search Terms:
FileItem/Md5sum (context: mir)
FileItem/FileName (context: mir)
Cancel
Next

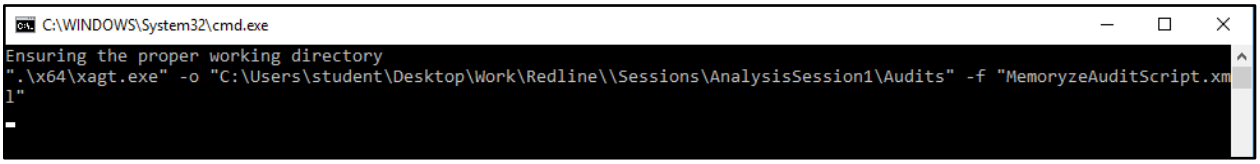
2- Select “Next” then “Edit Script” to make note of what the application has decided to capture based on the IOCs you created in your file. Make sure they align.



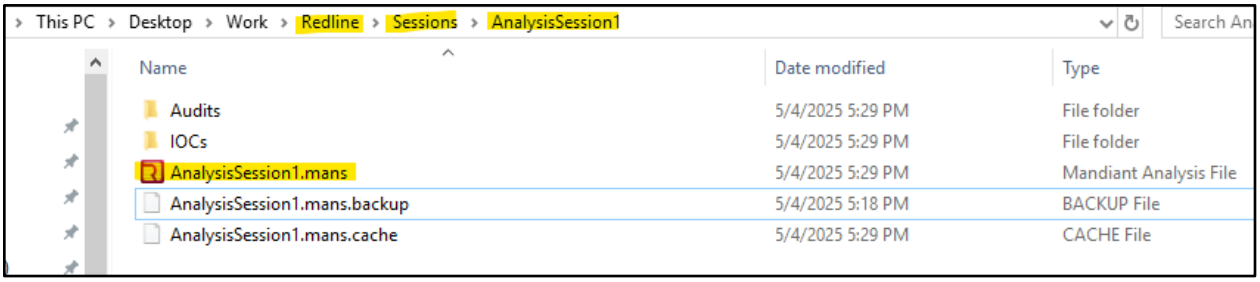

3- Save your collector script to a new directory, such as “Redline” under your work folder on your desktop.



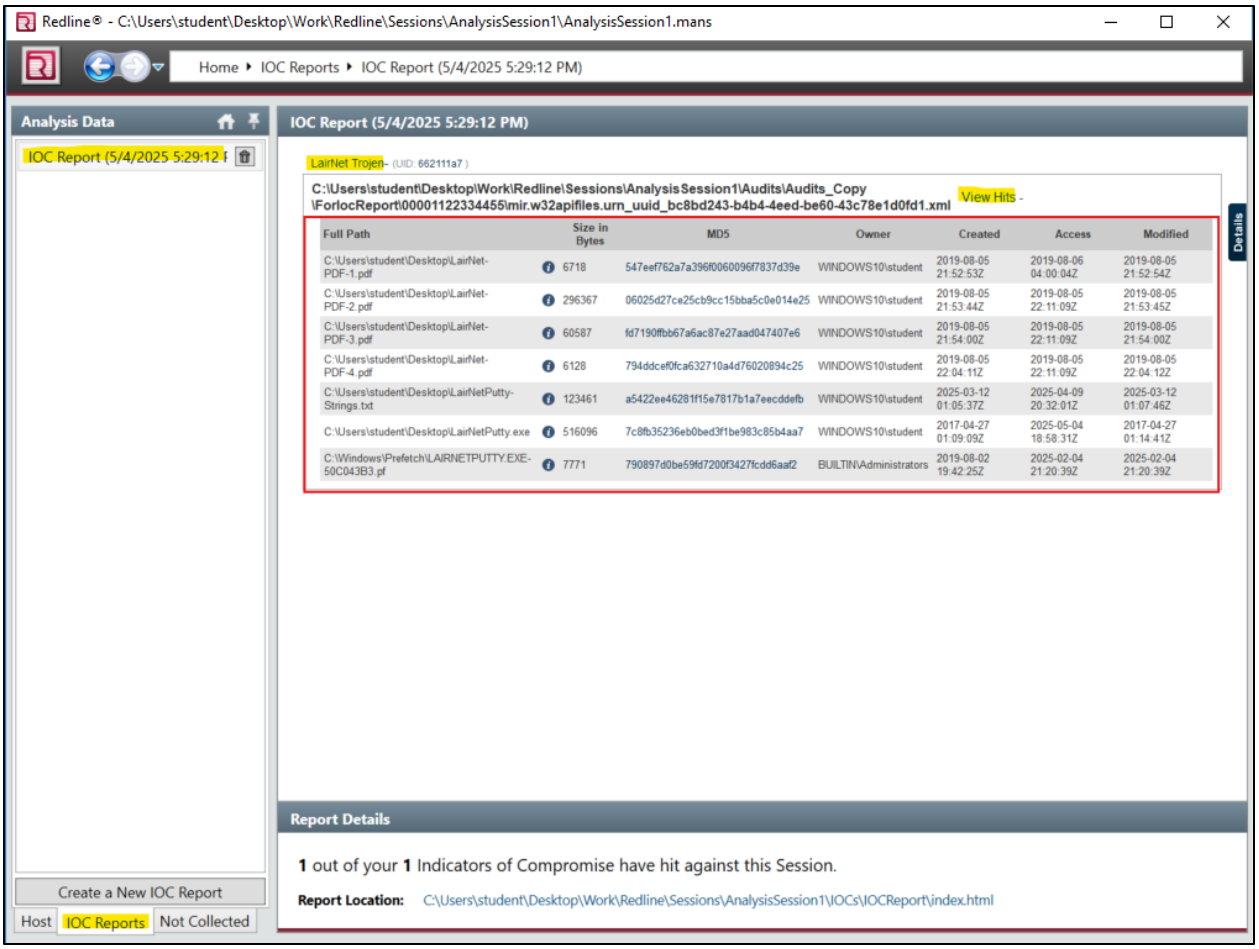

4- Navigate to Redline directory and select “RunRedlineAudit.bat”.




5- Then open the Sessions folder and select AnalysisSession#.mans




6- The file will open in Redline application. On the left side select IOC Report tab




## Conclusion

In this lab, we utilized FireEye's *Redline* tool to validate the effectiveness of an Indicator of Compromise (IOC) created for the malicious LairNetPutty.exe application. By importing our IOC into Redline and executing a session analysis, we successfully detected artifacts related to the malware on the system (TheSecMaster, n.d.). Specifically, Redline flagged a total of six items: the LairNetPutty.exe binary itself (matched via MD5 hash and filename), a prefetch file generated when the executable was first executed, and four PDF documents that shared a naming convention containing the string "LairNet."

Detecting the executable and its associated artifacts demonstrates the practical value of IOCs in digital forensics and incident response. Redline's ability to correlate file metadata, such as hash values and filenames, with pre-defined indicators enabled a targeted and efficient threat-hunting process. This lab not only reinforces the importance of crafting precise IOCs but also highlights the need for tools like Redline in real-world scenarios where rapid detection and attribution are critical (Scarfone & Mell, 2023).

Furthermore, detecting supporting files (e.g., PDFs and Prefetch data) shows how malware often interacts with or is accompanied by other artifacts that can serve as secondary indicators. Identifying these reinforces the importance of a multi-layered detection strategy that combines signature-based IOCs with contextual awareness of user environments.

Overall, this lab demonstrated end-to-end IOC lifecycle usage—from creation to operational detection—using professional forensic tools. This hands-on experience strengthens our preparedness to respond to cybersecurity threats in enterprise settings and aligns with modern practices in threat intelligence and incident containment.

## Glossary

Indicator of Compromise (IOC): Artifacts observed on a network or system that indicate a potential intrusion or malicious activity.

Malicious Application: Software designed to disrupt, damage, or gain unauthorized access to systems.

Digital Forensics: The field involving the recovery and investigation of material found in digital devices, often in relation to cybercrime.

Threat Intelligence: Information used to understand, prevent, and respond to cybersecurity threats.

Incident Response: A structured approach to handle and manage the aftermath of a security breach or cyberattack.

## References

TheSecMaster. (n.d.). *Redline*. https://thesecmaster.com/tools/redline

Scarfone, K., & Mell, P. (2023). *Guide to Malware Incident Prevention and Handling for Desktops and Laptops (NIST Special Publication 800-83 Revision 1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-83r1