**Project report**

1. Introduction

Malicious activity in the digital world has become a serious concern for individuals, businesses, and organizations of all sizes. Cybercriminals are constantly developing new and sophisticated techniques to compromise systems, steal data, and disrupt operations. In order to, protect against these threats, it's important to have a solid understanding of the signs of malicious activity and the tools and techniques used to investigate them. One such tool is Redline, which allows analysts to perform memory and file analysis to identify indicators of compromise and other signs of malicious activity. In this topic, we will explore how to use Redline to investigate signs of malicious activity through memory and file analysis and provide some best practices for using this tool to improve your overall cybersecurity posture.

* Objective of the project

The objective of this project is to demonstrate how to use the Redline tool to investigate signs of malicious activity through memory and file analysis. The project aims to provide a practical understanding of how to use this tool to identify indicators of compromise and other signs of malicious activity, and to showcase the capabilities of Redline in the context of a real-world cybersecurity investigation. By the end of the project, participants will have gained a solid understanding of the Redline tool, its features, and functions, and how it can be used to improve their overall cybersecurity posture.

* Description of the project

The project will involve a step-by-step guide on how to use the Redline tool to investigate signs of malicious activity through memory and file analysis. The project will begin with an introduction to the Redline tool and its capabilities, followed by an overview of the different types of malicious activity that can be detected through memory and file analysis.

The project will then walk through the process of installing and configuring the Redline tool, including setting up a new analysis and selecting the appropriate memory image and file analysis options. Participants will learn how to review the results of the memory and file analysis, and how to identify potential indicators of compromise and other signs of malicious activity. The project will also cover best practices for using the Redline tool, including how to interpret the results of the analysis and how to take appropriate action in response to identified threats.

Throughout the project, participants will be provided with real-world examples of how the Redline tool can be used to investigate signs of malicious activity in a variety of different scenarios. By the end of the project, participants will have gained practical experience in using the Redline tool to improve their cybersecurity posture and protect against cyber threats.

* Scope of the project

The scope of this project is focused on demonstrating how to use the Redline tool to investigate signs of malicious activity through memory and file analysis. The project will cover the basic functionalities of Redline, including how to install, configure, and use the tool to perform memory and file analysis.

The project will provide real-world examples of how Redline can be used to investigate signs of malicious activity in a variety of different scenarios, including detecting malware, analyzing system compromises, and identifying potential insider threats. The project will not cover the use of other memory and file analysis tools or techniques, as it is focused specifically on the Redline tool. Additionally, the project will assume a basic level of familiarity with cybersecurity concepts and terminology.

Overall, the project is intended to provide a practical guide for using the Redline tool to improve cybersecurity posture and protect against cyber threats.

1. System description

The system being described is the Redline tool, which is used to investigate signs of malicious activity through memory and file analysis. Redline is a free and open-source tool developed by FireEye, a cybersecurity company specializing in threat intelligence and incident response.

Redline allows analysts to perform memory and file analysis on Windows systems, detecting indicators of compromise and other signs of malicious activity. The tool provides a user-friendly interface for performing analysis, and offers a variety of features including process analysis, network analysis, and malware detection.

Redline is designed to be used by cybersecurity professionals with expertise in memory and file analysis, and requires a basic understanding of cybersecurity concepts and terminology. The tool is not intended for use by non-experts or for casual use and should be used in conjunction with other security tools and techniques to ensure a comprehensive security posture.

Overall, Redline is a powerful tool for investigating signs of malicious activity and improving cybersecurity posture and is widely used by cybersecurity professionals around the world.

1. Analysis Report

* Open Redline application and feed the file and memory image created with the help of Ftk imager.
* Run analysis on file image.

Graphical user interface

Description automatically generated

Fig: Creating image of file to analyze

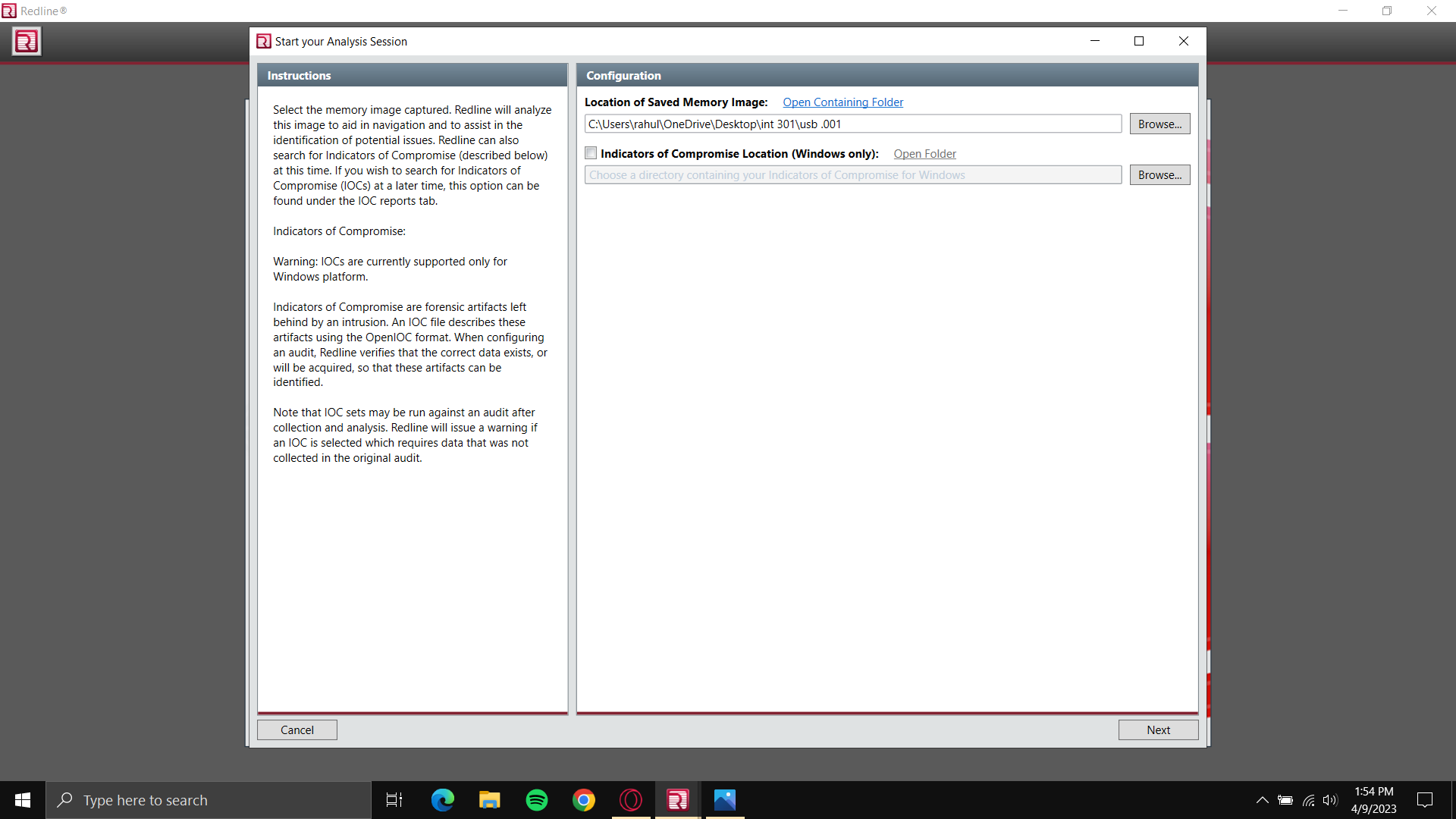


Fig: Selecting file for analyze

Graphical user interface, text, application

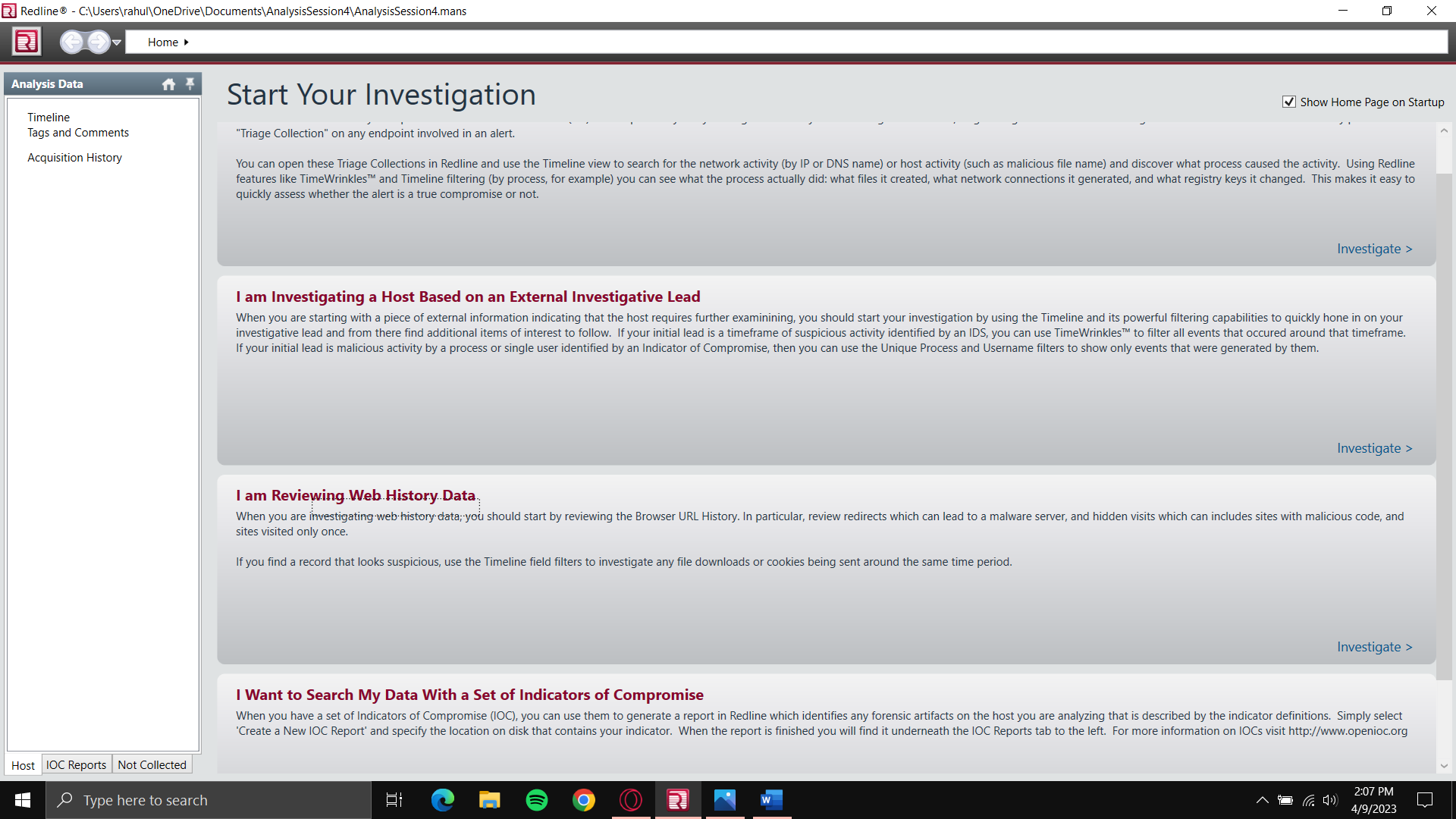
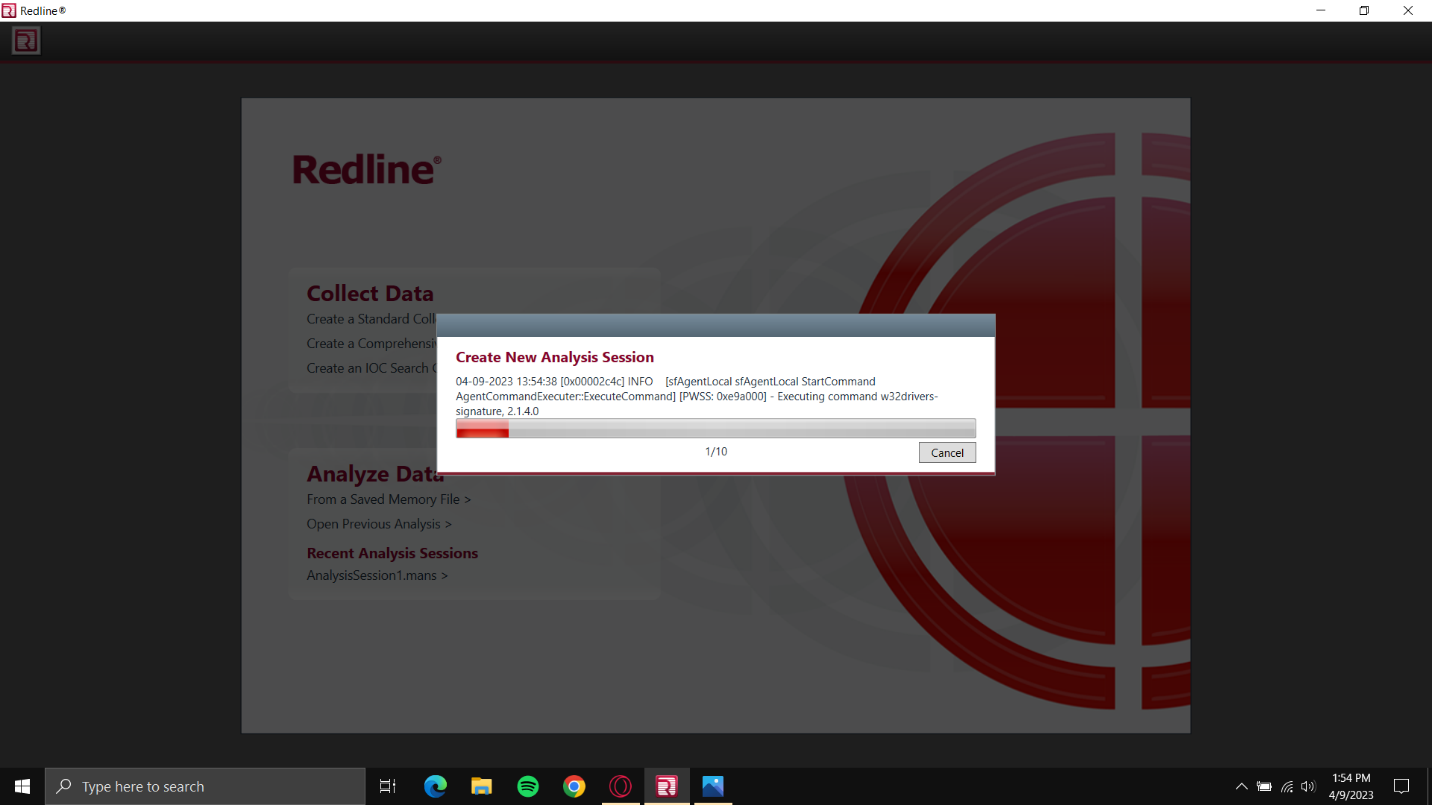
Description automatically generated

Fig: Final report of investigation

* Same can be done for memory analysis.

Graphical user interface, text, application

Description automatically generated

Fig: Creating memory image to analyze

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

Fig: Final report of memory analysis

1. Reference/Bibliography

<https://youtu.be/h-OAUPZiIwU> from YouTube

<https://youtu.be/HXv45dsL8xI> from YouTube