CyberSentinel AI

Memory Forensics Analyzer

Comprehensive Project Report

Project Title:	AI-Based Memory Forensics Analyzer
Version:	2.0
Date:	December 2025
Document Type:	Technical Project Report

Generated: December 16, 2025

Table of Contents

1. Executive Summary

This report presents the development of CyberSentinel AI, an advanced AI-powered memory forensics analyzer designed to detect malware within memory dumps using Machine Learning and Deep Learning techniques.

Key Achievements:

- 99.99% Detection Accuracy using ensemble learning methods
- Multi-c

The system processes the CIC-MalMem-2022 dataset containing 58,596 memory samples with 55 Volatility-extracted features, providing forensic analysts with a powerful, automated tool for threat detection.

2. Introduction

2.1 Background

Memory forensics is a critical discipline in cybersecurity, focusing on the analysis of volatile memory (RAM) to detect malicious activity, recover artifacts, and investigate security incidents. Traditional memory analysis relies heavily on manual inspection and signature-based detection, which is time-consuming and ineffective against obfuscated malware.

2.2 Project Scope

This project develops an AI-based solution that automates memory forensics analysis using advanced machine learning techniques. The system provides automated ingestion of memory dump features, classification of samples as Benign or Malware, identification of specific malware families, anomaly detection for unknown threats, and interactive visualization.

2.3 Stakeholders

- Primary Users: Forensic Analysts, Cybersecurity Researchers
- Secon

3. Problem Statement

Traditional memory forensics faces several critical challenges:

- Volume of Data: Memory dumps can be 8GB-128GB in size
- Obfusc

Research Question: How can ML/DL be applied to automate memory forensics while maintaining high accuracy?

4. Objectives

4.1 Primary Objectives

- Develop ML system with >99% classification accuracy

- Implen

4.2 Success Criteria

Objective	Target	Achieved
Binary Accuracy	>99%	99.99%
Multi-class F1	>95%	99.9%
Inference Time	<1s	~0.1s
Load Time	<5s	~3s

5. Dataset Analysis

5.1 Dataset Overview

Source: CIC-MalMem-2022 (Obfuscated-MalMem2022 Dataset)
Origin: Canadian Institute for Cybersecurity
Purpose: Benchmark dataset for memory-based malware detection

5.2 Dataset Statistics

Metric	Value
Total Samples	58,596
Features	55
Missing Values	0
Class Balance	50/50

5.3 Feature Categories

Features extracted via Volatility plugins: pslist (processes), dlllist (DLLs), handles (handle counts), ldrmodules (hidden modules), malfind (code injection), and svcscan (services).

6. Results & Evaluation

6.1 Model Performance

Model	Accuracy	F1-Score
Logistic Regression	99.88%	99.8%
Decision Tree	99.98%	99.9%
Random Forest	99.99%	100%
Optimized MLP	99.99%	100%
Ensemble	99.99%	100%

6.2 Confusion Matrix

	Pred. Benign	Pred. Malware
Actual Benign	5,859	1
Actual Malware	0	5,860

6.3 Performance Rationale

Near-perfect accuracy is attributed to high-quality Volatility features, balanced dataset, effective feature engineering, and ensemble combination.

7. User Interface Design

7.1 Design Philosophy

The dashboard uses a Cyberpunk Glitch aesthetic designed to appeal to the cybersecurity community while maintaining visual hierarchy and usability.

7.2 Color Palette

Element	Color	Hex
Background	Void Black	#050505
Primary	Electric Cyan	#00F0FF
Secondary	Hot Pink	#FF007F
Success	Acid Green	#00FF9F

7.3 Key UI Features

- Animated hexagon grid background
- Glitch

8. Conclusion

CyberSentinel AI successfully demonstrates ML application to automated threat detection in memory forensics.

Key Accomplishments:

- Exceptional Accuracy: 99.99% detection rate
- Compr

The system provides forensic analysts with a powerful, automated tool that significantly reduces analysis time while maintaining high accuracy.

9. Future Work

Short-term

- Add SHAP/LIME explanations to dashboard
- Implen

Medium-term

- Live memory acquisition
- Volatili

Long-term

- Docker containerization
- Cloud-

10. References

1. Walters, A. (2007). The Volatility Framework. Digital Investigation.

2. Liu, F. T., et al. (2008). Isolation Forest. ICDM 2008.

3. CIC. (2022). CIC-MalMem-2022 Dataset.

4. Lundberg, S. M. (2017). SHAP. NeurIPS.

5. Pedregosa, F. (2011). Scikit-learn. JMLR.