Project Plan: Automated Dynamic Analysis Signature Generation (Project 3)

Ikram Benfellah, Fadel Fatima Zahra

January 25, 2026

1 Project Information

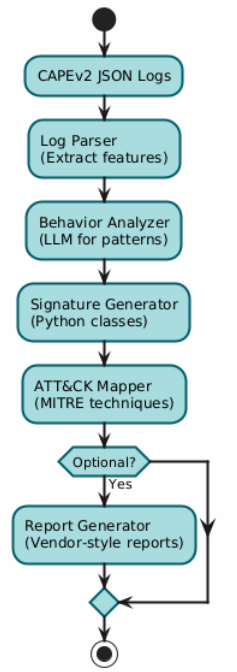
- **Project Title:** Automated Dynamic Analysis Signature Generation
- **Project Number:** 3
- **Team Members:** Ikram Benfellah (Lead Developer), Fadel Fatima Zahra (Research Lead)
- **GitHub Repository:** `https://github.com/yourusername/your-repo`

2 Methodology

High-level Approach:

1. Parse CAPEv2 JSON logs to extract behavioral patterns (API calls, network, file ops).
2. Use LLMs to identify and summarize key behaviors.
3. Automatically generate Python-based CAPEv2 signatures.
4. Map behaviors to MITRE ATT&CK techniques.
5. (Optional) Generate comprehensive, human-readable malware analysis reports.

System Architecture:



Key Components:

- **Log Parser:** Extracts features from CAPEv2 JSON logs.
- **Behavior Analyzer:** Uses LLMs to detect behavioral patterns.
- **Signature Generator:** Produces Python signature classes.
- **ATT&CK Mapper:** Maps behaviors to MITRE ATT&CK techniques.
- **Report Generator:** (Optional) Creates vendor-style analysis reports.

Technology Stack:

- Python 3.10+, PyTorch/Transformers (for LLMs), CAPEv2, MITRE ATT&CK framework, LaTeX (reporting)

3 Implementation Plan

Timeline and Milestones:

- **Jan 25:** Project plan submission
- **Feb 1-10:** Dataset acquisition and preprocessing
- **Feb 11-20:** Log parser and feature extraction
- **Feb 21-Mar 1:** LLM-based behavior analysis
- **Mar 2-10:** Signature generation and validation
- **Mar 11-15:** MITRE ATT&CK mapping

- **Mar 16-20:** Report generation, evaluation, and final write-up
- **Mar 22:** Final submission

Task Breakdown:

- **Dataset download and organization:** Ikram
- **Dataset cleaning and statistics:** Fatima Zahra
- **Log parsing module (lead):** Fatima Zahra
- **Log parsing module (support/testing):** Ikram
- **Feature extraction script (lead):** Ikram
- **Feature extraction script (support):** Fatima Zahra
- **LLM prompt design and integration (lead):** Fatima Zahra
- **LLM output post-processing (support):** Ikram
- **Signature class code generation (lead):** Ikram
- **Signature validation (unit tests, lead):** Fatima Zahra
- **MITRE ATT&CK mapping research (lead):** Ikram
- **MITRE ATT&CK mapping implementation (lead):** Fatima Zahra
- **Report generator (draft, lead):** Fatima Zahra
- **Report generator (review and polish, support):** Ikram
- **Evaluation metrics calculation (lead):** Ikram
- **Baseline comparison experiments (lead):** Fatima Zahra
- **Final report writing:** Both

Dependencies and Risks:

- LLM access (API limits, cost)
- Dataset size/quality
- CAPEv2 compatibility
- Mitigation: Early testing, fallback to manual feature extraction if needed

4 Research Component

4.1 Research Questions

1. How accurate are LLM-generated behavioral signatures compared to manually crafted ones?
2. Can automated signature generation reduce malware analysis time?
3. How well do generated signatures generalize to new malware variants?

Paper/Tool	Approach	Key Contribution	Our Difference
DeepSign (2017)	Deep learning (DBN) for automatic malware signature generation from sandbox logs	Demonstrates that deep learning can generate robust, invariant behavioral signatures for malware classification	We focus on generating actionable CAPEv2 Python signatures and mapping to MITRE ATT&CK, with LLM-based automation
Automatic-Malware-Signature-Generation (GitHub)	Open-source tool for automated malware signature generation	Provides practical implementation and code for signature automation	Our work targets CAPEv2 format, integrates MITRE ATT&CK mapping, and explores LLM-driven signature synthesis
LLM-Virus (Emergent-Mind)	Explores LLMs for malware analysis and signature creation	Highlights the potential of LLMs for automating malware signature generation and analysis	We apply LLMs specifically to automate CAPEv2 signature creation from sandbox logs and behavioral patterns

Table 1: Related work comparison

4.2 Related Work

Recent research has explored the use of deep learning and large language models (LLMs) for automating malware signature generation and behavioral analysis. DeepSign (David et al., 2017) introduced a deep belief network approach for generating robust malware signatures from sandbox logs, demonstrating high accuracy in classifying new variants. Open-source projects such as Automatic-Malware-Signature-Generation provide practical tools for automating signature creation, though they may not target the CAPEv2 format or integrate MITRE ATT&CK mapping. The LLM-Virus topic and related discussions highlight the growing interest in leveraging LLMs for malware analysis and signature automation. Our work builds on these foundations by focusing on the automated generation of actionable CAPEv2 Python signatures from sandbox execution logs, mapping behaviors to MITRE ATT&CK techniques, and synthesizing comprehensive analysis reports using LLMs.

4.3 Dataset Selection

- **Dataset:** AVAST-CTU CAPEv2 Dataset (`https://github.com/avast/avast-ctu-cape-dataset`)
- **Justification:** Large, diverse, public, includes CAPEv2 logs

- **Statistics:** >100,000 samples, multiple malware families
- **Preprocessing:** Filter for relevant behaviors, split into train/val/test
- **Split Strategy:** Chronological partitioning to avoid data leakage

5 Evaluation Plan

- **Metrics:** Precision, recall, F1-score (signature quality), coverage, ATT&CK mapping accuracy, report quality (expert review), efficiency (time savings)
- **Baselines:** Existing CAPEv2 signatures, manual analyst signatures, rule-based detection
- **Experimental Setup:** Evaluate on held-out test set, compare to baselines, statistical significance via paired t-test
- **Expected Outcomes:** LLM-generated signatures are competitive with manual, improve efficiency, and provide robust ATT&CK mapping