CAPSTONE DESIGN EXPO | **Computer** Science | **CS** 25-345

Network Feature Extraction From High Cyber Fidelity Simulation Environment

Team members: Christopher Castro, Ryan Collette, William Lagos, Sam Soltanian | **Faculty adviser:** Irfan Ahmed, Ph.D. | **Sponsor:** DoD ASPIRE | **Mentor:** Joao Soares

Introduction

In today's world, wireless network traffic is ubiquitous. Our devices constantly communicate over networks, creating a rich stream of data.
What if we could tap into this passive flow to identify the operating systems of connected devices without any interaction?
OsirisML is an existing machine learning-based application created by the U.S. Department of Defense, designed to identify the operating systems of devices communicating over a wireless network through packet capture (PCAP) files.

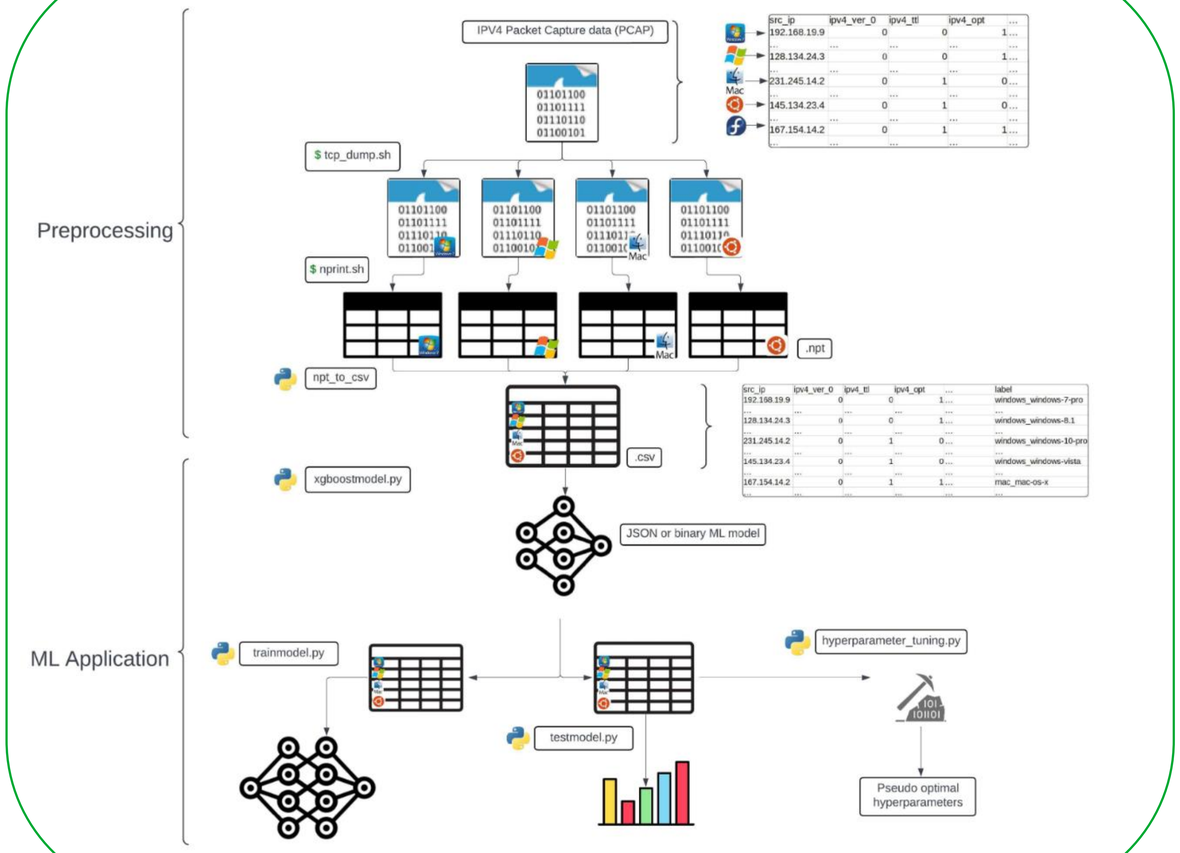
Goal

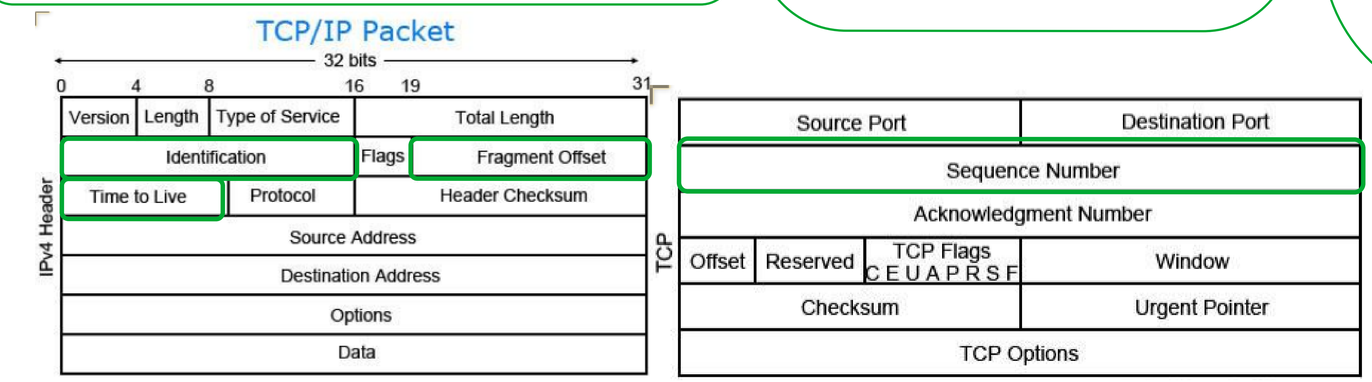
- Expand OsirisML's functionality to identify not only the operating system, but also its specific builds and versions, while also improving general usability.

Improvements

- Improve accuracy and add ability to detect OS builds & versions. Model benchmarks at 74.09% and struggles to identify specific versions of operating systems, e.g. Ubuntu 20.1 vs. 24.04
- Reduce required memory. Currently requires 405GB RAM to execute.
- Containerization to allow deployment across multiple operating systems. The application is currently confined to Debian based OS's.
- Implementing a Command Line Interface for ease of use. Currently each element of the application must be run independently without the assistance of an interactive CLI.

Workflow





Packet Identification

- OsirisML identifies operating systems by analyzing TCP/IP headers and leveraging machine learning algorithms to detect patterns unique to specific OS versions.
- Fragment Id/Offset
- Time To Live (TTL),
- Initial Sequence Number (ISN)
- Other identifiers such as Timestamps, Window Scaling, Maximum Segment Size, Explicit Congestion Notification, Internet Control Message Protocol

VCU College of Engineering