MICHIGAN STATE UNIVERSITY

Project Plan

Improved Detonation of Evasive Malware

The Capstone Experience

Team Proofpoint

Ian Murray

Ryan Gallant

Jack Mansueti

Sean Joseph

Tae Park

Department of Computer Science and Engineering
Michigan State University

Fall 2018

From Students…
…to Professionals

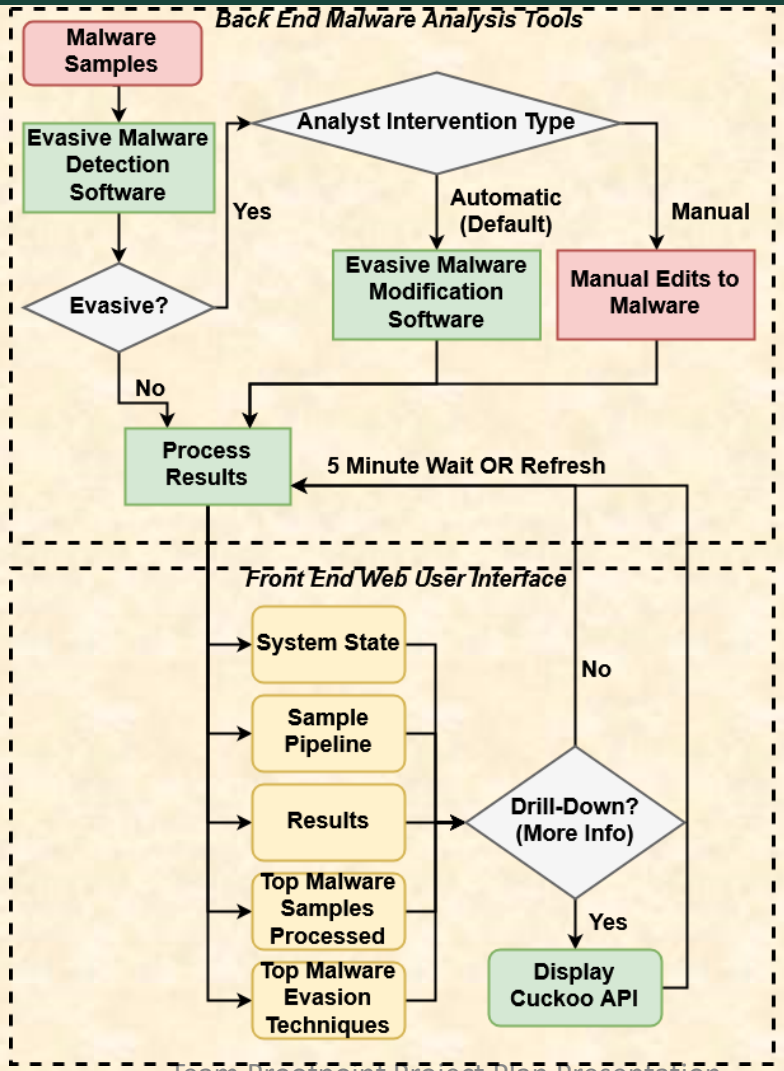
Functional Specifications

- Sandbox is essential for malware analysis
- New evasive techniques hinder quarantine
- **Fundamental Solution:** Flag malware whose execution deviates in sandboxes.
- **Auxiliary Solution:** Support autonomous code modification to remove the ability to avoid sandbox execution
- Display in intuitive web UI

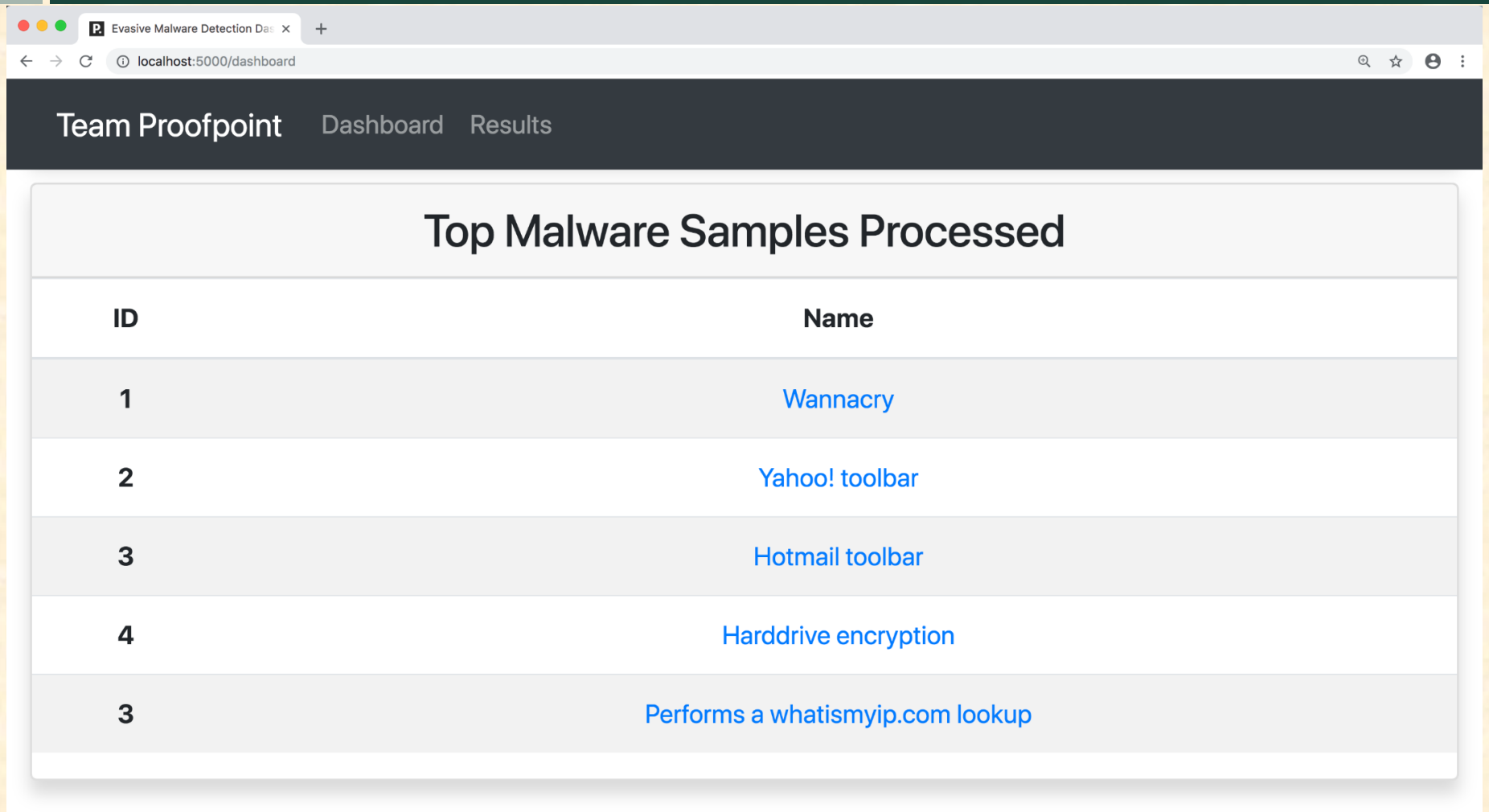
Design Specifications

- Evasive Malware Identification
  - Scan for known existing signatures
  - Develop own behavior detection methods
- Malware Modification & Detonation
  - Modify sandbox checks with reverse engineering
  - Forces malware to execute all relevant functions
- Web Interface
  - Top-Level: Displays broad real time data
  - Drill-Downs: Widgets, enters more detailed reports

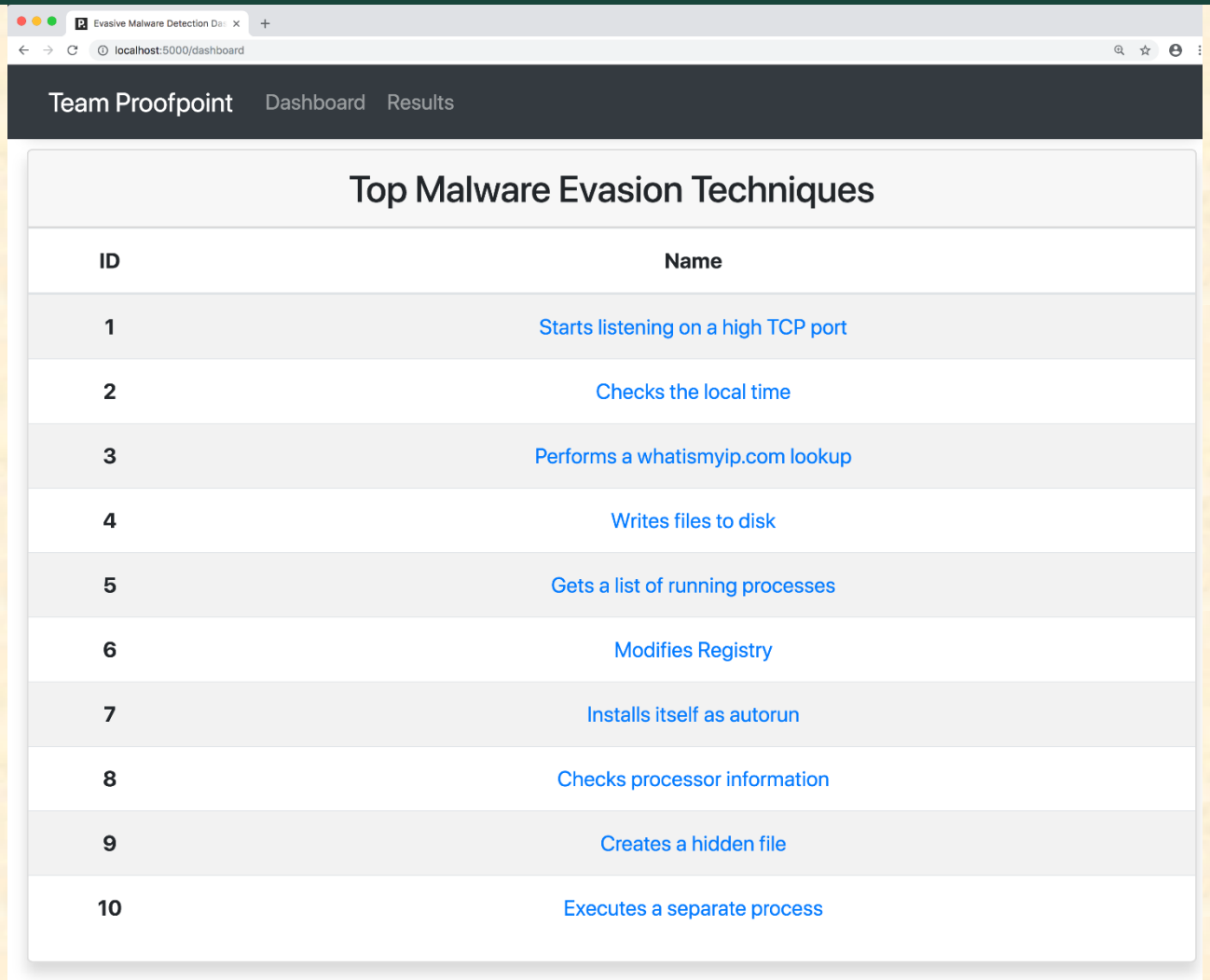
Design Specifications



Screen Mockup: Top Samples

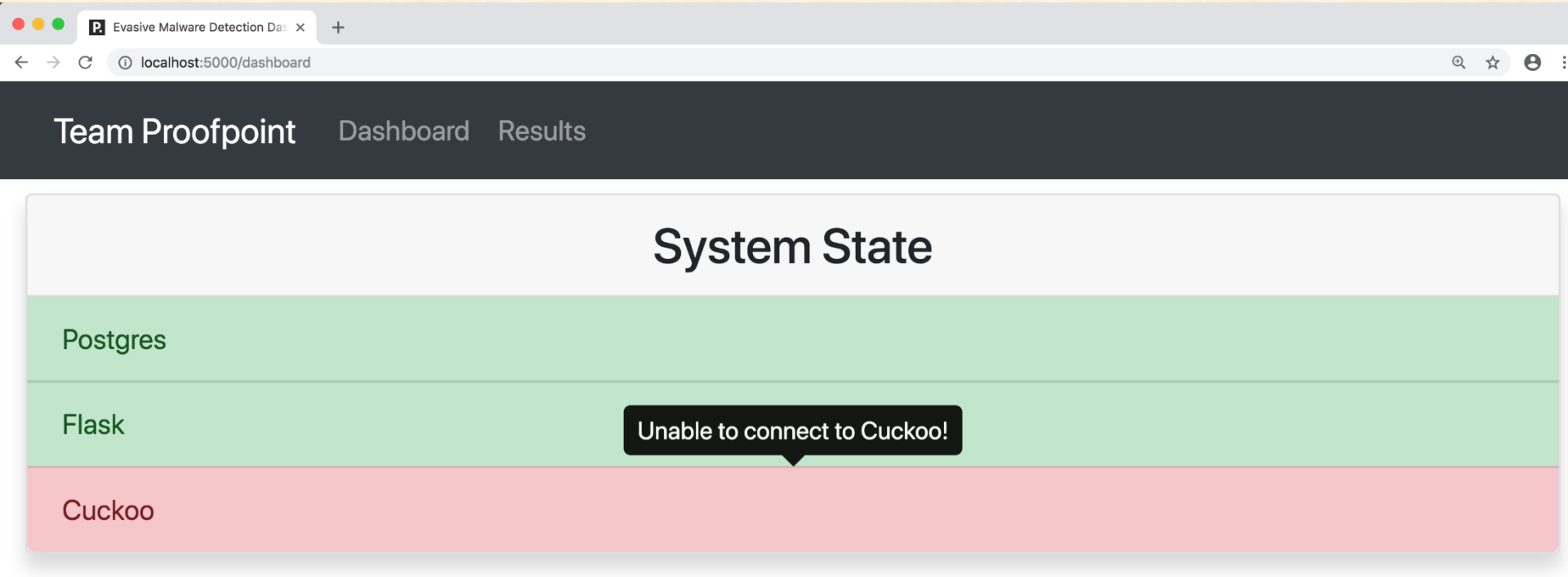


Screen Mockup: Top Techniques

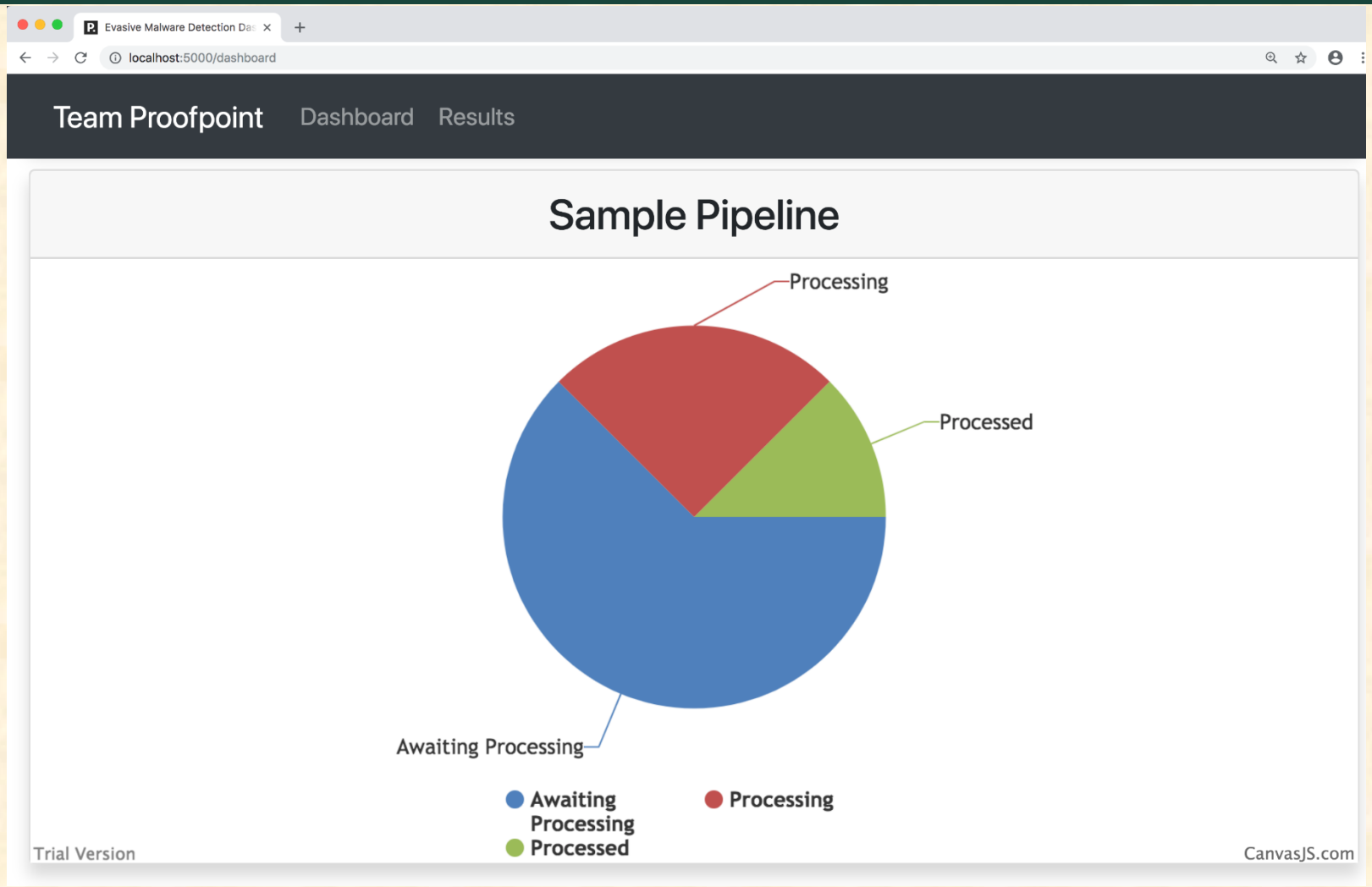


ID	Name
1	Starts listening on a high TCP port
2	Checks the local time
3	Performs a whatismyip.com lookup
4	Writes files to disk
5	Gets a list of running processes
6	Modifies Registry
7	Installs itself as autorun
8	Checks processor information
9	Creates a hidden file
10	Executes a separate process

Screen Mockup: System State



Screen Mockup: Sample Queue



Screen Mockup: Results

Evasive Malware Detection Das

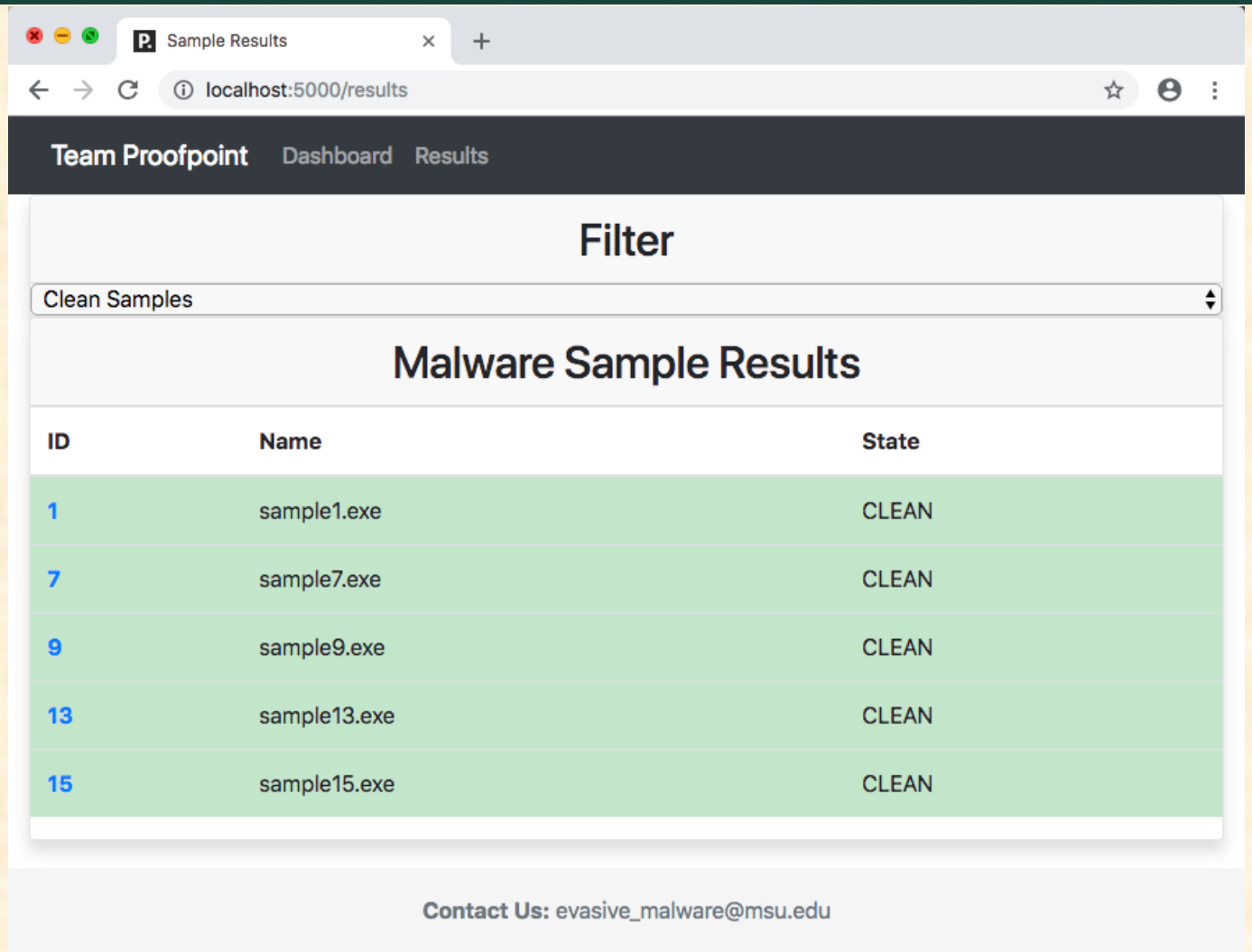
localhost:5000/dashboard

Team Proofpoint Dashboard Results

Results

ID	Name	State
1	sample1.exe	CLEAN
2	sample2.exe	SUCCESSFUL EXECUTION
3	sample3.exe	INTERESTING
4	sample4.exe	MODIFIED

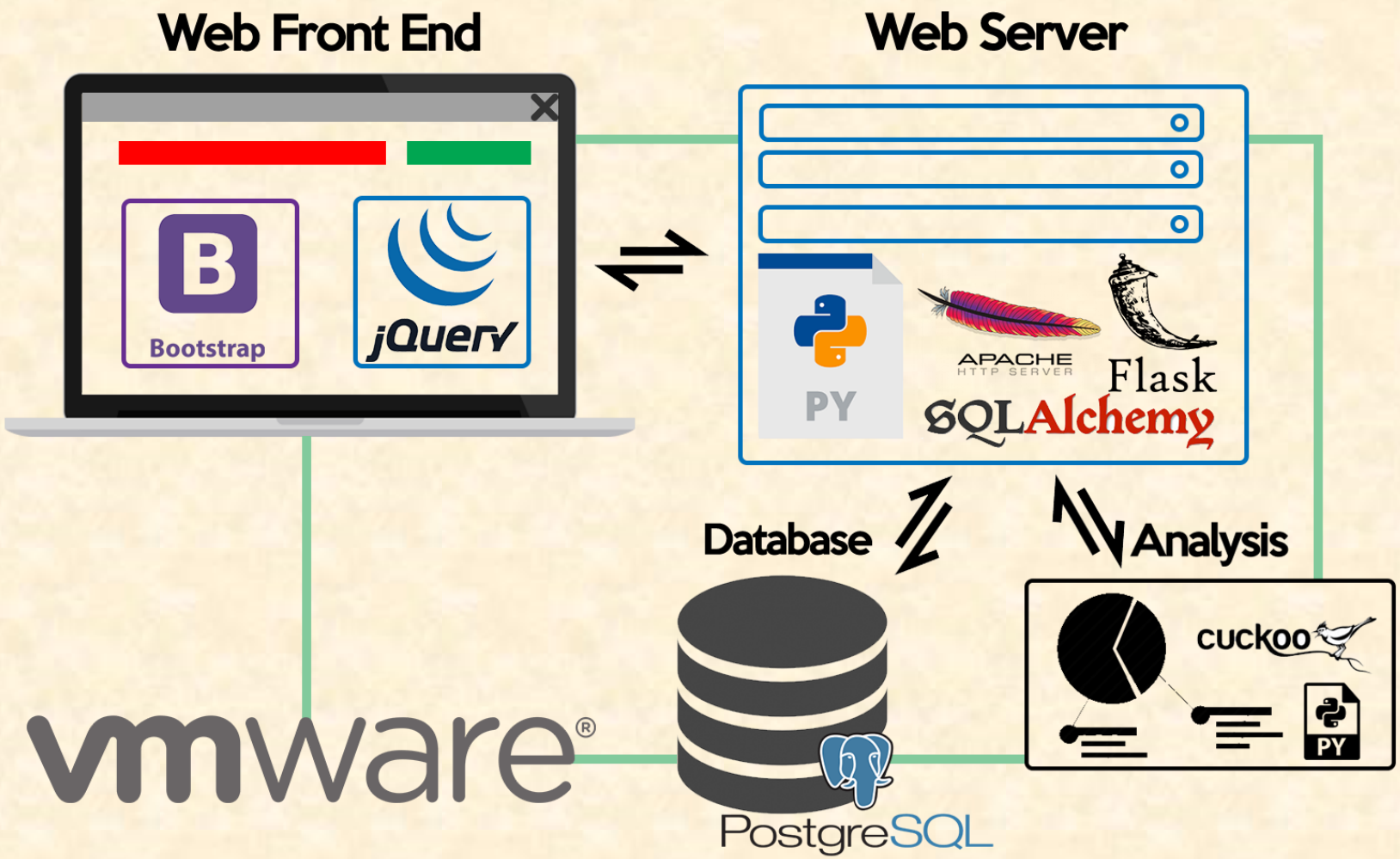
Screen Mockup: Results w/ Filter



Technical Specifications

- Front End UI
  - Bootstrap, jQuery, HTML5, and CSS3 are used to effectively present users with appropriate data from the malware detonation system.
- Web Application
  - Apache, Flask, and Python are used to serve our web application.
  - PostgreSQL is used for data storage outside the data Cuckoo's API provides.
  - SQLAlchemy is used for mapping Python Objects to PostgreSQL statements and schema.
- Backend Malware Analysis
  - Cuckoo and Suricata are used for detonation and classification, Python is used to disassemble and modify malware samples classified as evasive.

System Architecture



System Components

- Software Platforms / Technologies
  - Front End
    - Python 3.6
    - HTML & CSS3
    - Bootstrap CSS
    - Cuckoo API
    - Flask
    - jQuery
  - Back End
    - Python 2.7
    - Cuckoo
    - Suricata
    - PostgresSQL
    - SQLAlchemy
    - Apache
    - VMWare

Risks

- Reverse Engineering Difficulty
  - Malware samples are rarely available as readable code.
  - Variety of tools for disassembly.
- Multiple Language Proficiency
  - Malware comes in variety of languages.
  - Limit analysis to a subset of the greater universe of languages.
- Navigating Proofpoint's Lab
  - Unknown how customizable Proofpoint's lab environment is.
  - Client runs samples the team uploads via Secureshare.
- Malware Samples Evade through Unknown Means
  - Unknown how a sample determines the difference between a live machine and a sandbox.
  - Proofpoint has identified several evasive malware for the team to examine.

Questions?