MICHIGAN STATE UNIVERSITY

Project Plan

Next Generation Malware Detection, Clustering and Heuristics

The Capstone Experience

Team Proofpoint

Crystal Lewis
Yash Patel
George Zhao
Graham Thomas
Brad Doherty

Department of Computer Science and Engineering
Michigan State University

Spring 2018

From Students…
…to Professionals

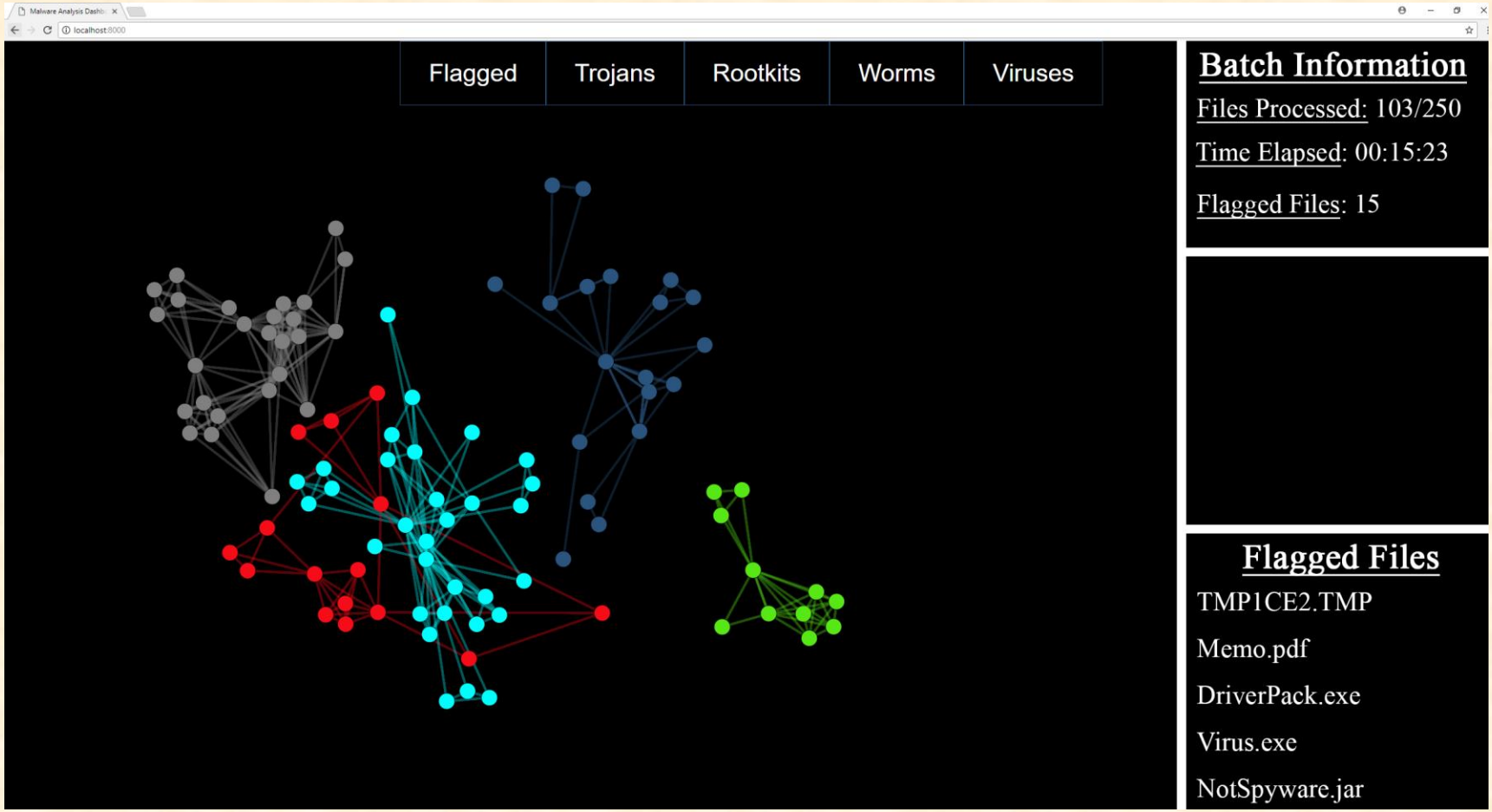
Functional Specifications

- Detect and cluster malware
- Provide a Web Dashboard for analysts
- Provide a framework for assigning signatures to new malware

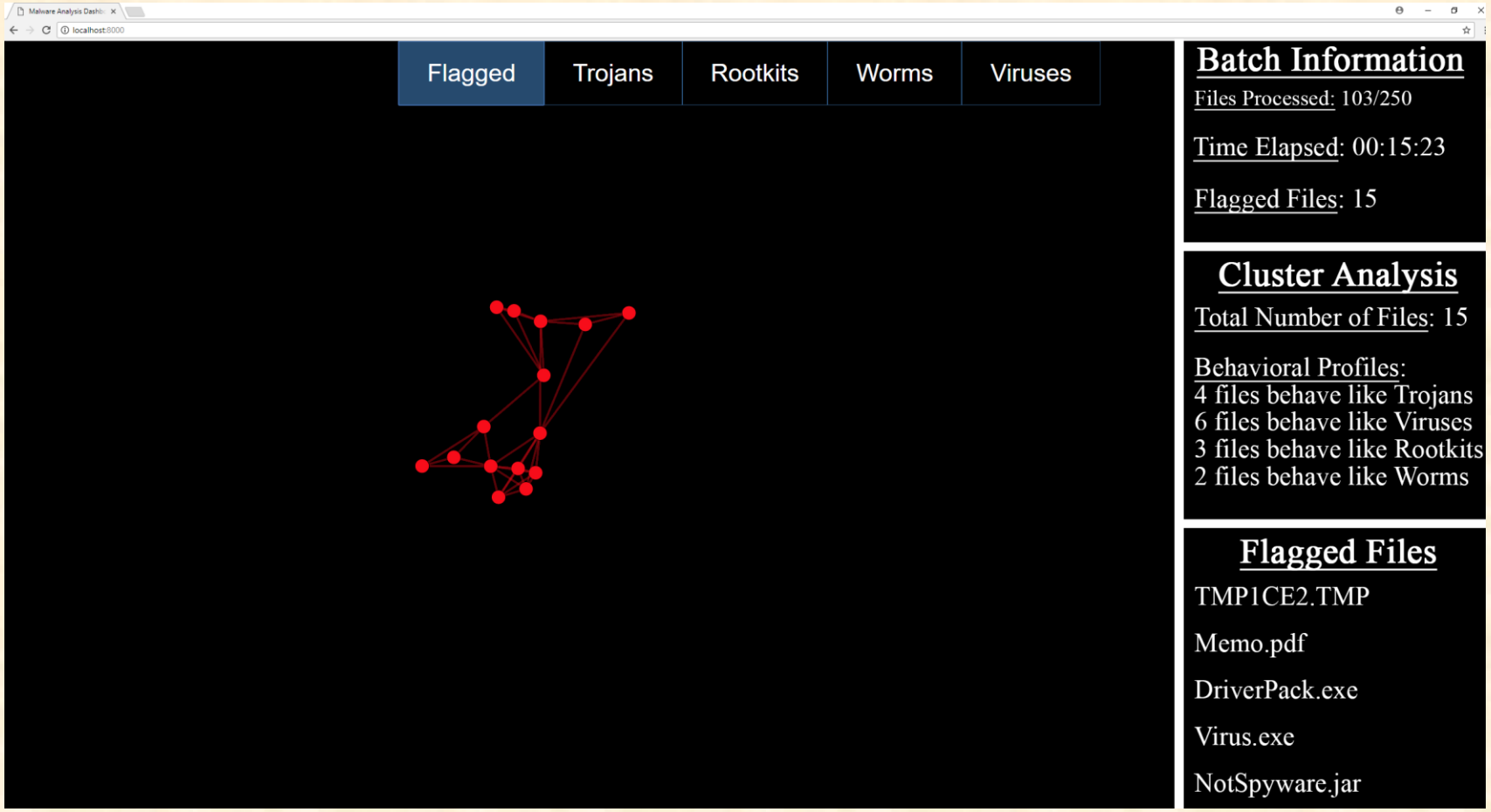
Design Specifications

- Malware analysis tool
- Malware aggregator
- Nodal graph display
- Malware statistics applets

Screen Mockup: Nodal Graph



Screen Mockup: Flagged Filtering

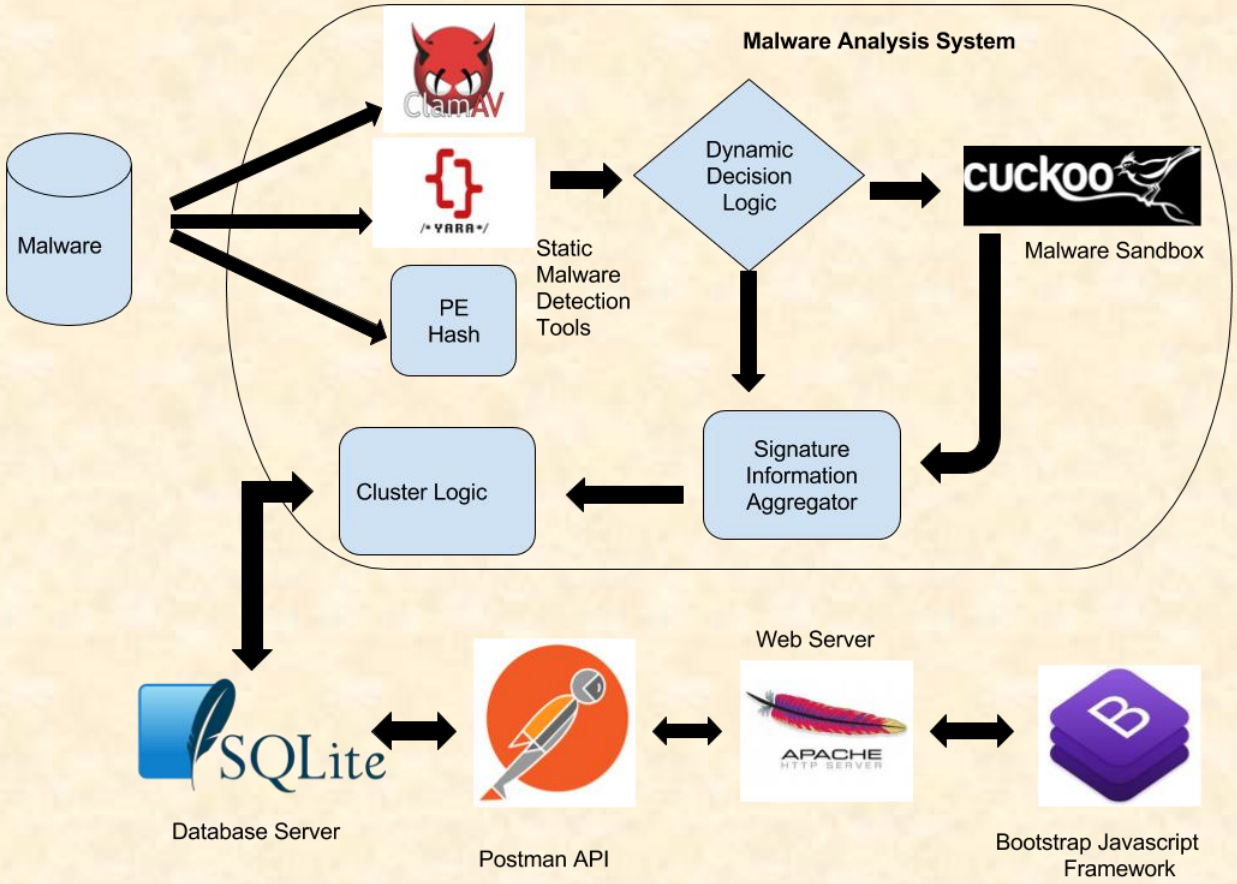


Screen Mockup: File analysis

Technical Specifications

- Static analysis module
- Dynamic analysis decision logic
- Malware sandboxing
- Signature information framework
- Malware aggregator
- Database
- Web Front End

System Architecture



System Components

- Hardware Platforms
  - Proofpoint hardware cluster
  - ESXi HyperVisor
  - Linux Ubuntu VMs
- Software Platforms / Technologies
  - Python, Yara, Cuckoo, ClamAV
  - SQLite, Apache
  - Postman API and Bootstrap Library

Risks

- Malware Clustering and Categorization
  - Clustering malware based on file characteristics
  - Research the best way to cluster malware (PE Hash or Fuzzy hashing)
- Understanding Dynamic and Static Analysis Tools
  - The tools behave differently and output different formats
  - Running different malware samples and analyzing outputs
- Scalability and Speed
  - Analyzing variable amounts of malware in an efficient way
  - Properly allocate resources for
- Signature Generation Framework
  - Provide a way for analysts to easily create the signature of a malware
  - Determine what analysis information is relevant for a signature

Questions?