MICHIGAN STATE
UNIVERSITY

Beta Presentation
Defeating Malware Payload Obfuscation

The Capstone Experience

Team Proofpoint

Adam Johanknecht
Nick Lojewski
Vivian Qian
Derek Renusch
Dan Somary

Department of Computer Science and Engineering
Michigan State University

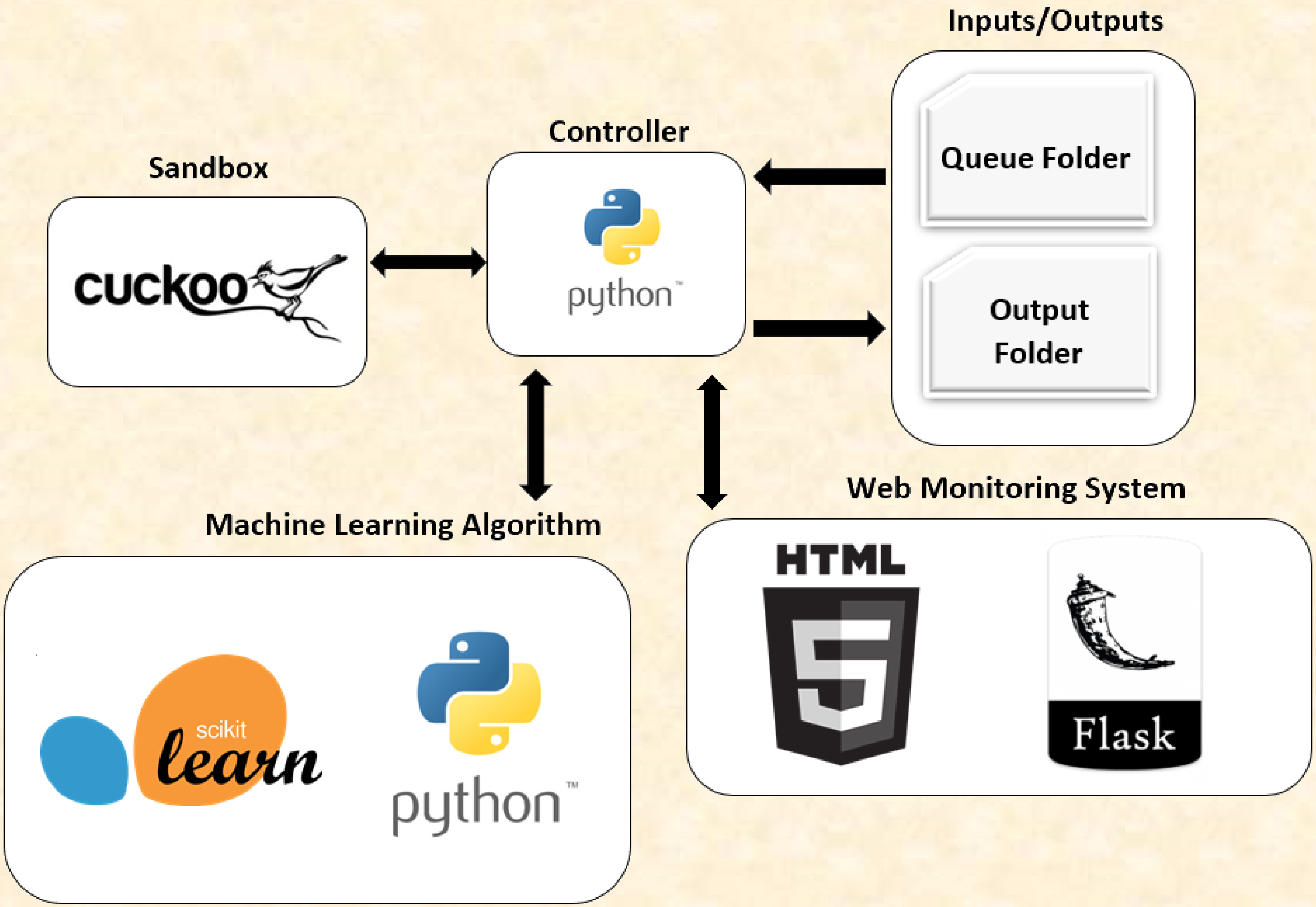
Spring 2019

From Students…
…to Professionals

Project Overview

- Create a machine learning system to classify files as malicious or benign
  - Accuracy goal: have at least the same accuracy as sandbox detonation
  - Performance goal: be at least 50% faster than detonation in Cuckoo
- Display information in web dashboard
  - High level system information
  - Ability to look at details for individual files

System Architecture



Inputs/Outputs

Queue Folder

Output Folder

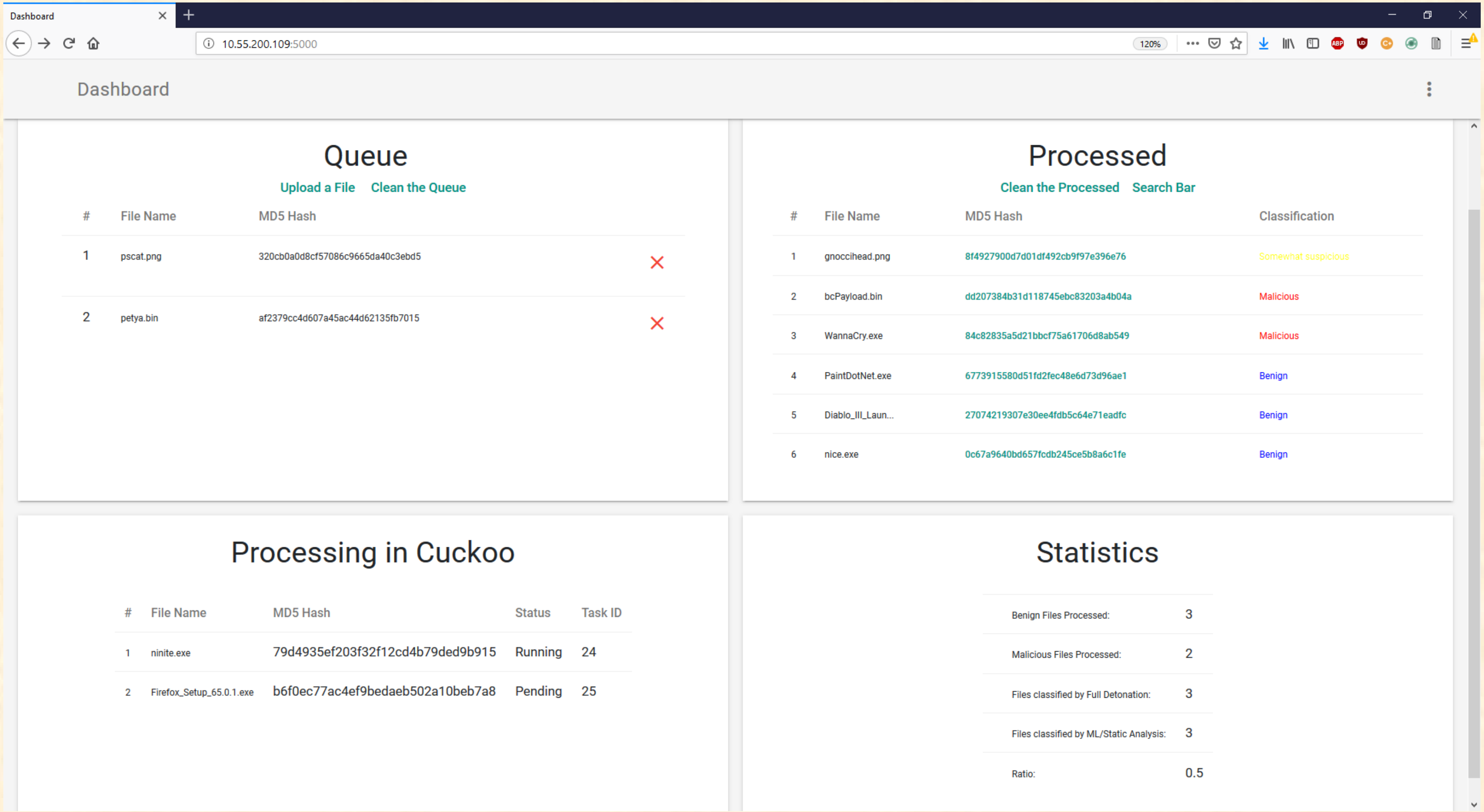
Controller

Sandbox

Machine Learning Algorithm

Web Monitoring System

Updated Main Dashboard



Dashboard

Queue

Upload a File   Clean the Queue

#	File Name	MD5 Hash	
1	pscat.png	320cb0a0d8cf57086c9665da40c3ebd5	✕
2	petya.bin	af2379cc4d607a45ac44d62135fb7015	✕

Processed

Clean the Processed   Search Bar

#	File Name	MD5 Hash	Classification
1	gnoccihead.png	8f4927900d7d01df492cb9f97e396e76	Somewhat suspicious
2	bcPayload.bin	dd207384b31d118745ebc83203a4b04a	Malicious
3	WannaCry.exe	84c82835a5d21bbcf75a61706d8ab549	Malicious
4	PaintDotNet.exe	6773915580d51fd2fec48e6d73d96ae1	Benign
5	Diablo_III_Laun...	27074219307e30ee4fdb5c64e71eadfc	Benign
6	nice.exe	0c67a9640bd657fcdb245ce5b8a6c1fe	Benign

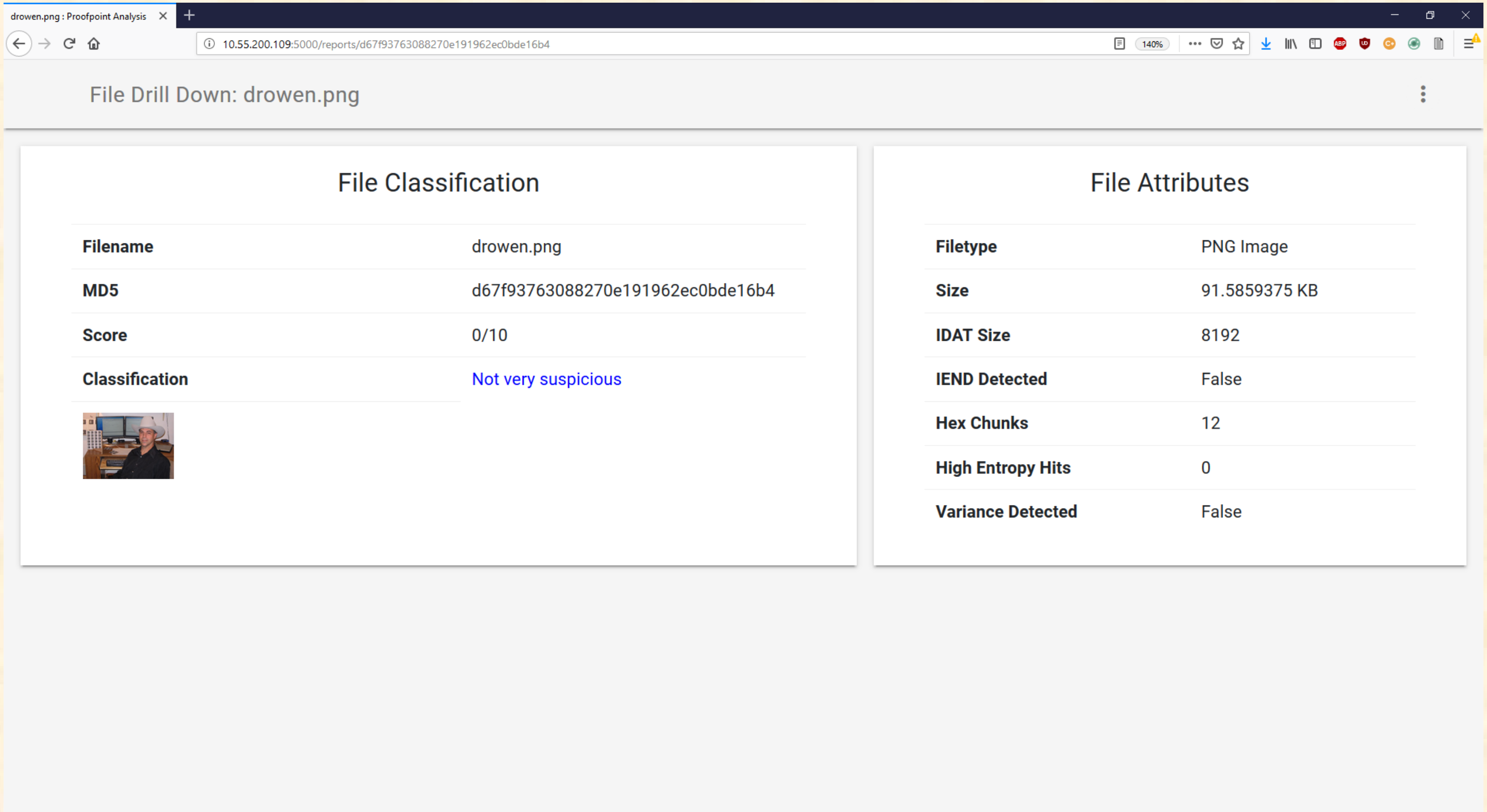
Processing in Cuckoo

#	File Name	MD5 Hash	Status	Task ID
1	ninite.exe	79d4935ef203f32f12cd4b79ded9b915	Running	24
2	Firefox_Setup_65.0.1.exe	b6f0ec77ac4ef9bedaeb502a10beb7a8	Pending	25

Statistics

Benign Files Processed:	3
Malicious Files Processed:	2
Files classified by Full Detonation:	3
Files classified by ML/Static Analysis:	3
Ratio:	0.5

Image Drill-Down Page


drowen.png : Proofpoint Analysis
10.55.200.109:5000/reports/d67f93763088270e191962ec0bde16b4
140%

File Drill Down: drowen.png

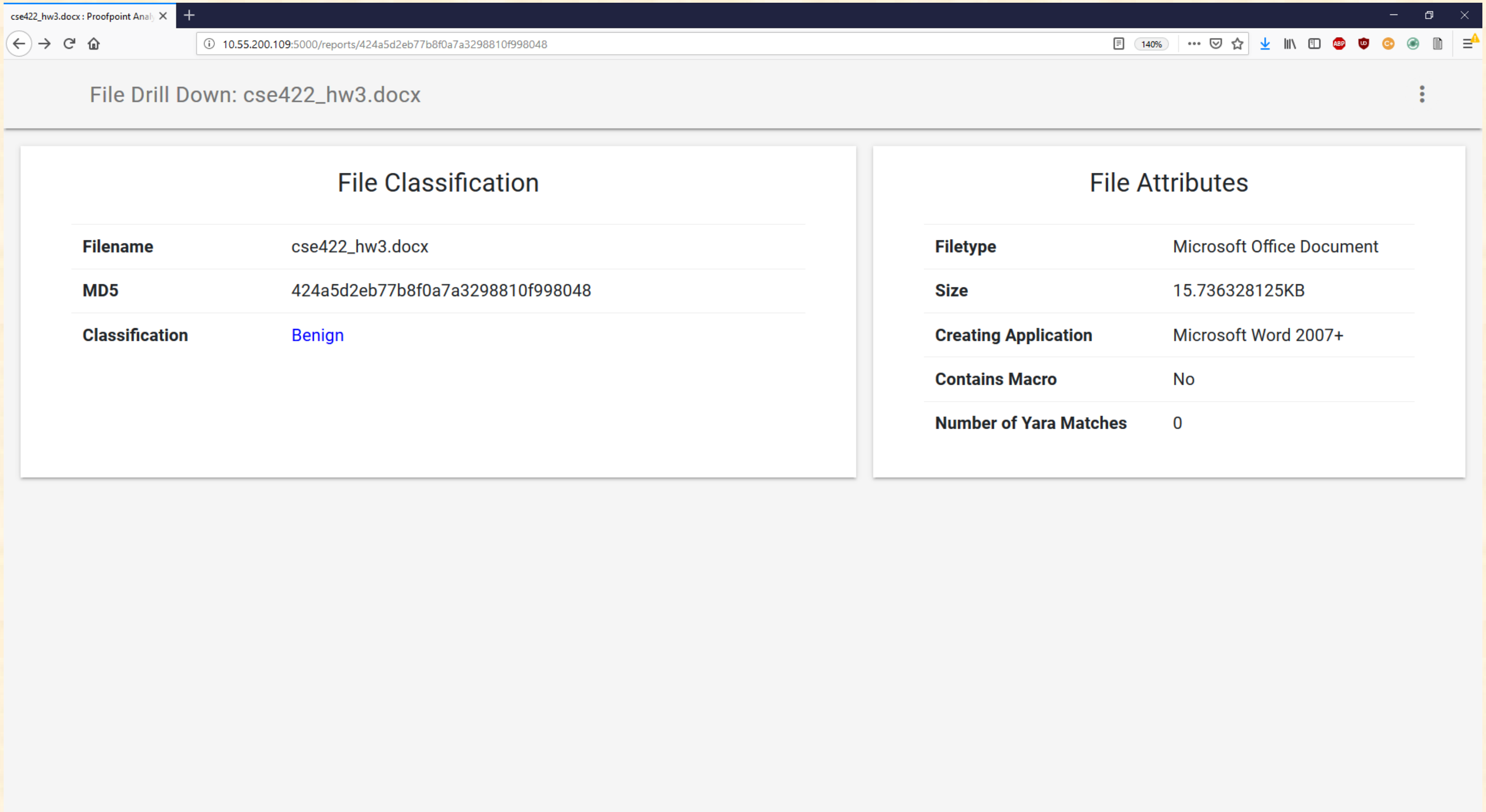
File Classification

Filename	drowen.png
MD5	d67f93763088270e191962ec0bde16b4
Score	0/10
Classification	Not very suspicious

File Attributes

Filetype	PNG Image
Size	91.5859375 KB
IDAT Size	8192
IEND Detected	False
Hex Chunks	12
High Entropy Hits	0
Variance Detected	False

Office Document Drill-Down Page



cse422_hw3.docx : Proofpoint Analy
10.55.200.109:5000/reports/424a5d2eb77b8f0a7a3298810f998048
140%

File Drill Down: cse422_hw3.docx

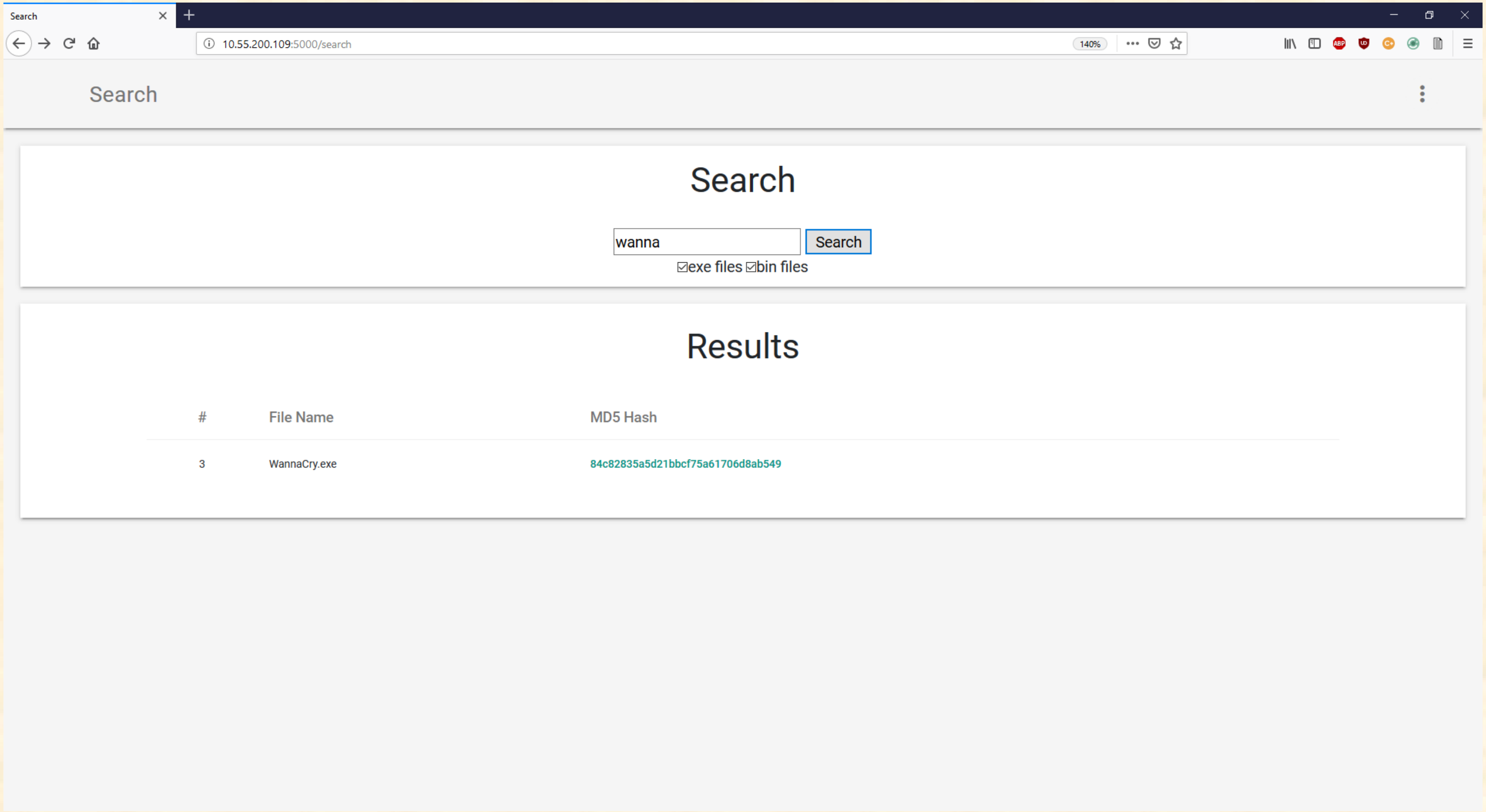
File Classification

Filename	cse422_hw3.docx
MD5	424a5d2eb77b8f0a7a3298810f998048
Classification	Benign

File Attributes

Filetype	Microsoft Office Document
Size	15.736328125KB
Creating Application	Microsoft Word 2007+
Contains Macro	No
Number of Yara Matches	0

File Search Page



Search

Search

wanna Search

☑exe files ☑bin files

Results

#	File Name	MD5 Hash
3	WannaCry.exe	84c82835a5d21bbcf75a61706d8ab549

What’s left to do?

- Improve accuracy of image and office document classification
- Enhance reporting on system health
- Create documentation and refactor the code base

Questions?

? ? ? ?

? ?

? ? ?