

MICHIGAN STATE

UNIVERSITY

Alpha Presentation

AMAP

The Capstone Experience

Accenture

Andrew Mitchell

Teng Xu

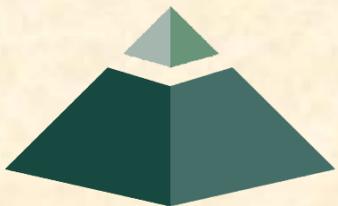
Griffin Metevia

Julian Ellis

Sam Kling

Department of Computer Science and Engineering
Michigan State University

Spring 2018



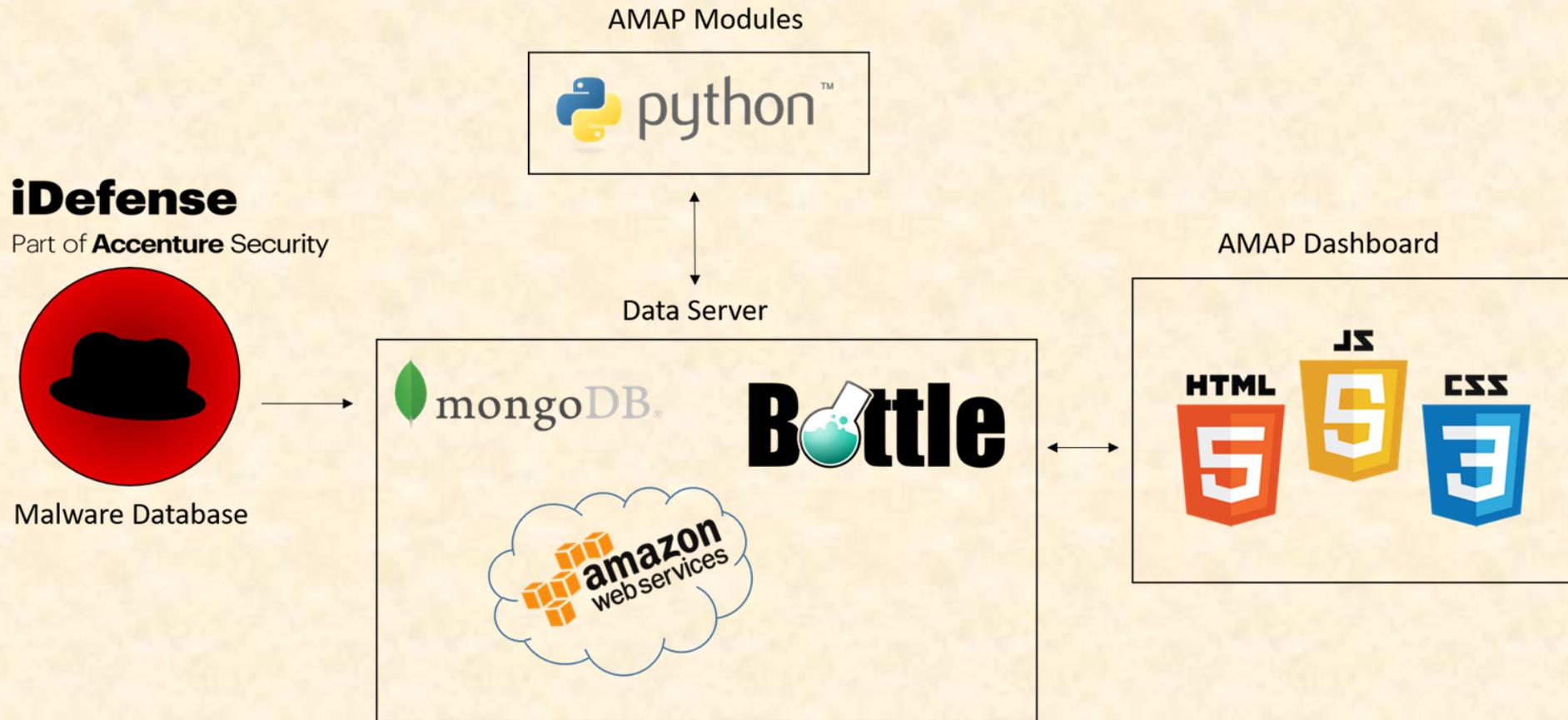
*From Students...
...to Professionals*

Project Overview

- Automated Malware Analysis
- Wizard Style UI
- High Volume Testing in Multithreaded Environment



System Architecture



Current Process Status Page

The screenshot shows a web browser window with the URL 'AMAP'. The page header includes the Accenture logo, a search bar, and the user name 'Andrew Mitchell'. The left sidebar contains navigation links for 'Dashboard (2 new updates)', 'File Upload', and 'Processes'. The main content area is titled 'Processes' and features a section for 'Analysis Status'.

#	SHA256	MD5	Overall Progress	Start Date	
1	b3d9cabf3ecb22dbccb0f13f95313e5ab95be94aec879e6edfaaf534d7f3799	eb684b584704e2fb599d6eaf883c1ae5	<div style="width: 20%;"></div>	18-1-27 1:54:24	View
2	dff02aca142d4fcfe7721b9c7cb5d7d4ef4965d11e77328d290aaf2eac8d4dd	4871e4752bd67662ac9435d84014391d	<div style="width: 10%;"></div>	18-2-2 1:59:32	View
3	dcf789f34aabe7ba4c34bbce09bfdd6ac6a2efde9f664ec0eab16fd0e37bef0d	3501fa1f022cb8ad97276d55c97377b5	<div style="width: 30%;"></div>	18-2-3 5:52:45	View
4	2e112bbf5fa0faf225eb2441b245539cd73f52fb473a6b749490d4749f7d105	9490fe6870d1273dda8c957cf1b81907	<div style="width: 5%;"></div>	18-2-3 6:00:23	View
5	9ac3accd466a70884091364b5d2e13534cfa78153b25f51fe477d6bfcc6f9abe	68b329da9893e34099c7d8ad5cb9c940	<div style="width: 40%;"></div>	18-2-5 12:32:02	View



File Upload

The screenshot displays a web browser window with the URL 'AMAP'. The page features a blue sidebar with the 'accenture' logo and navigation links for 'Dashboard (2 new updates)', 'File Upload', and 'Processes'. The main content area is titled 'File Input Page' and contains a 'File Input' section. This section includes a 'Select a file:' label, a 'Choose Files' button, the text 'No file chosen', and a 'Start upload' button. The browser's address bar shows 'AMAP', and the top right corner of the page displays the user's name 'Andrew Mitchell' and a power icon.



Module Selection Page

The screenshot shows a web browser window with the URL 'AMAP'. The page header includes the 'accenture' logo, a search bar, and a user profile for 'Andrew Mitchell'. The left sidebar contains navigation links for 'Dashboard (2 new updates)', 'File Upload', and 'Processes'. The main content area is titled 'Modules' and features a checkbox for 'Match Modules For all Files'. Below this, two file entries are listed, each with a set of selected analysis modules and a 'Submit' button.

13413701_10209874704294851_7569077515899457902_n.Jpg

- File Type
- MD5
- SHA1
- SHA256
- Entropy
- Decoder
- NETDATA

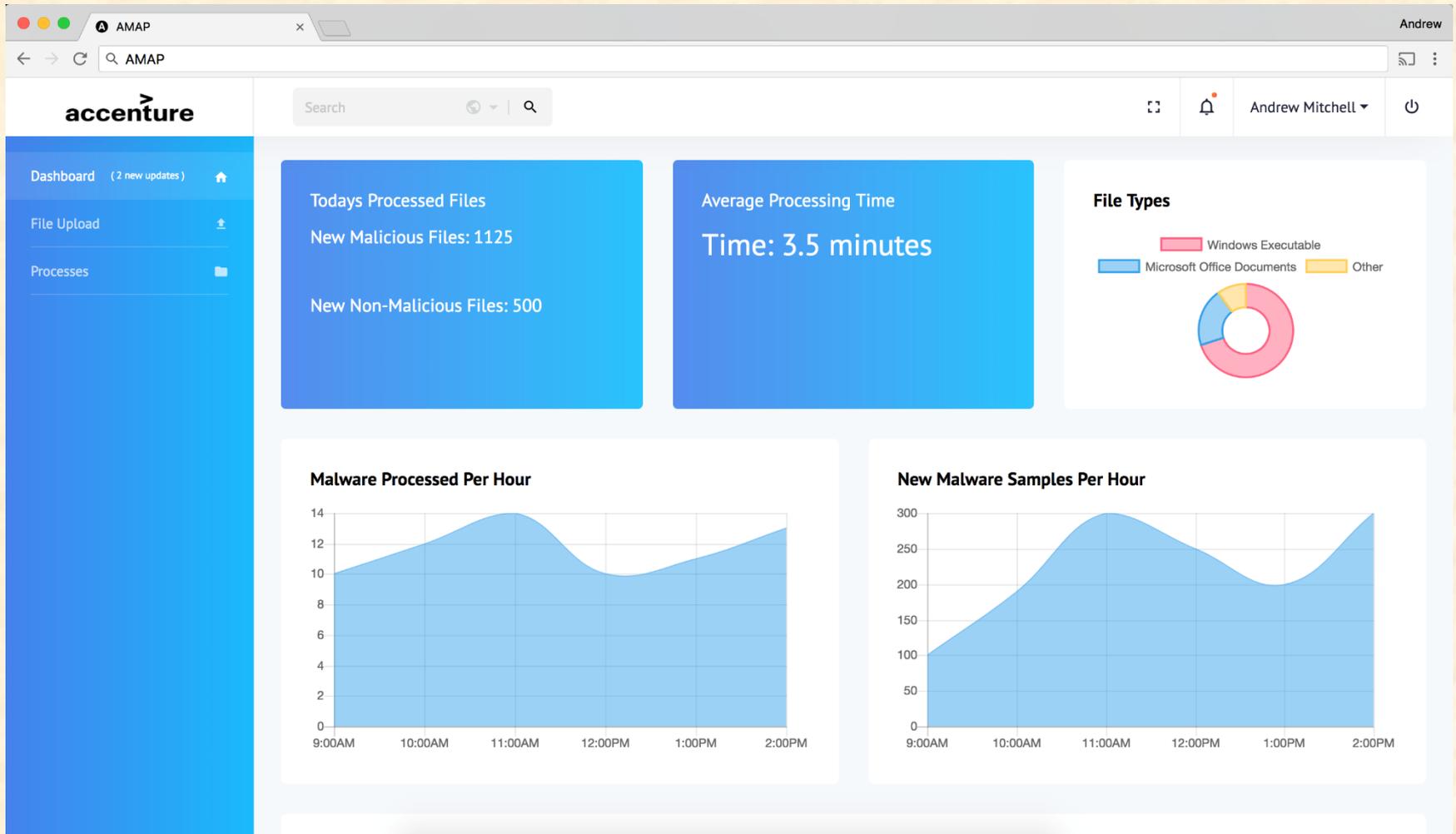
Submit

19989639_10213842700812284_7767808038276667761_n.Jpg

- File Type
- MD5
- SHA1



Dashboard



What's left to do?

- Add More Dynamic Analysis Modules
- Add More Information to Dashboard Page
- Create Login Page
- Write and Pull Malware Information to/from iDefense Database



Questions?

?

?

?

?

?

?

?

?

?

