INTRUSION DETECTION SYSTEM USING A NEURAL NETWORK

PHASE THREE PRESENTATION

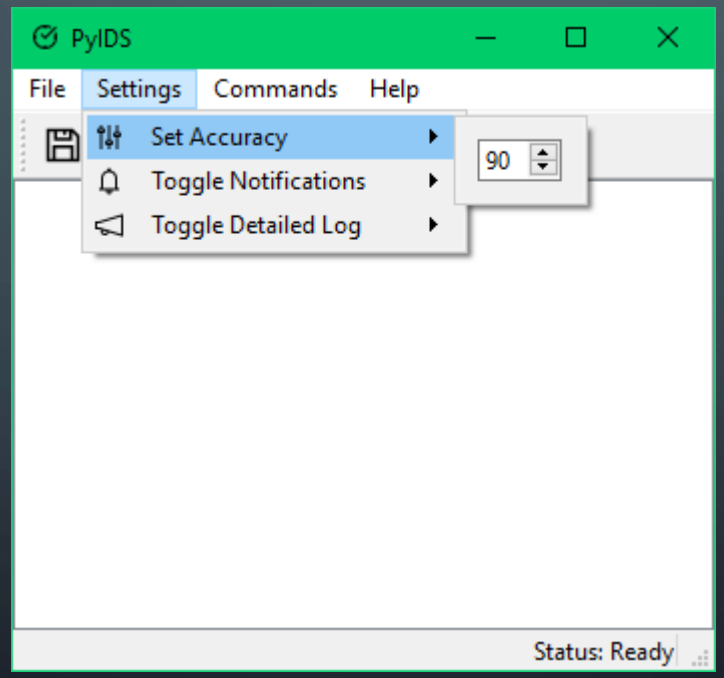
BLAKE KNEDLER

AGENDA

- Action Items
- Component Design
- User Manual
- Formal Technical Inspection
- Test Plan Update
- System Test Procedure
- Assessment Evaluation
- Project Evaluation
- Demonstration
- Questions and Comments

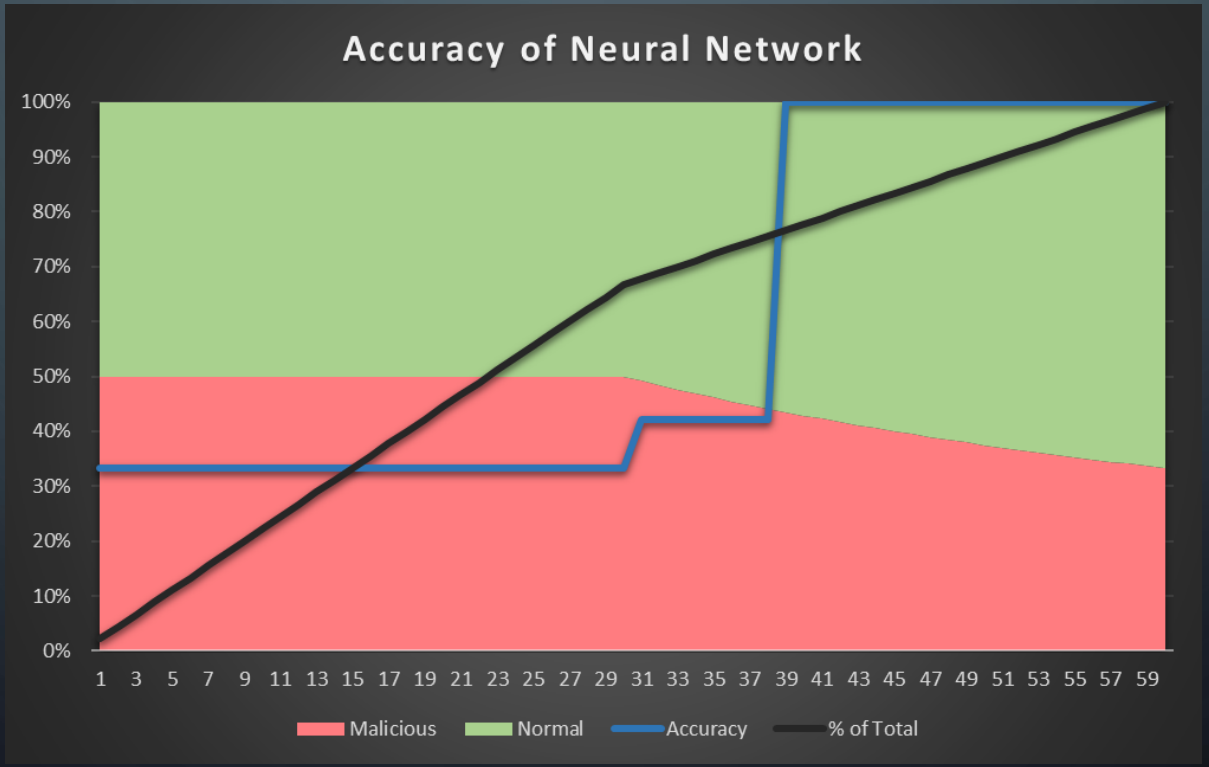
ACTION ITEMS

- Add minimum accuracy setting in the GUI
  - Shown in the User Manual portion and demonstration



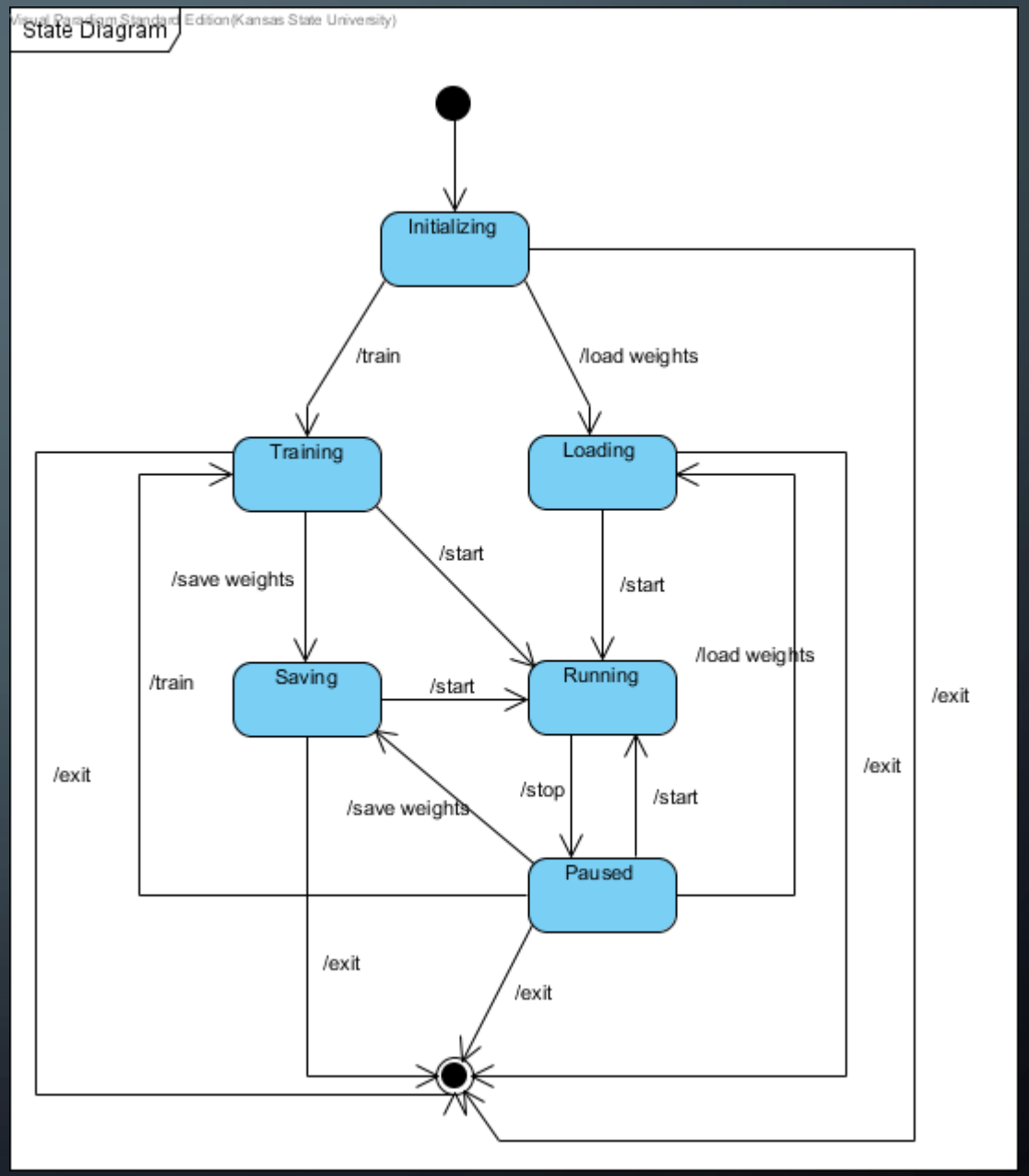
ACTION ITEMS

- Analyze the training of the Neural Network
  - Shown in the Project Evaluation section



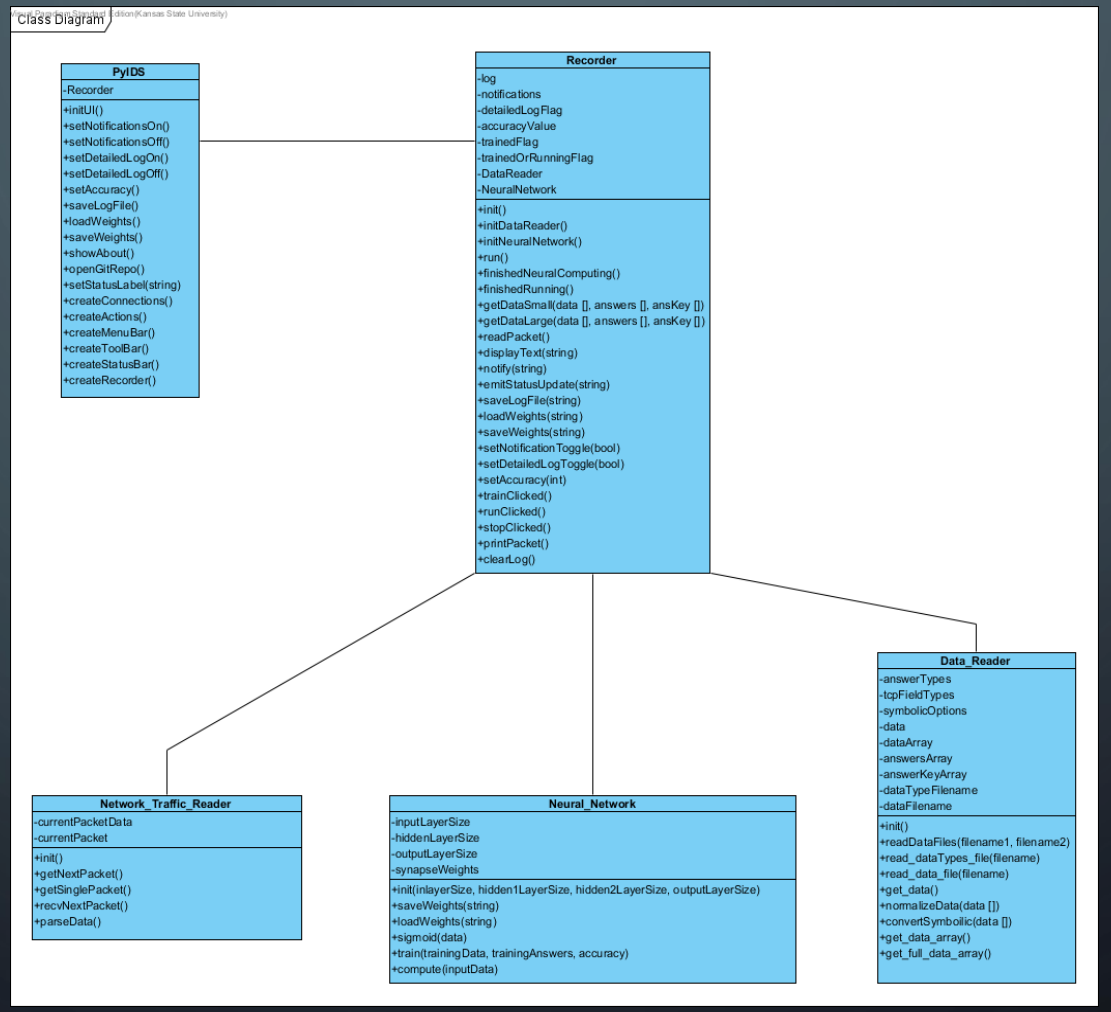
COMPONENT DESIGN

- State Diagram



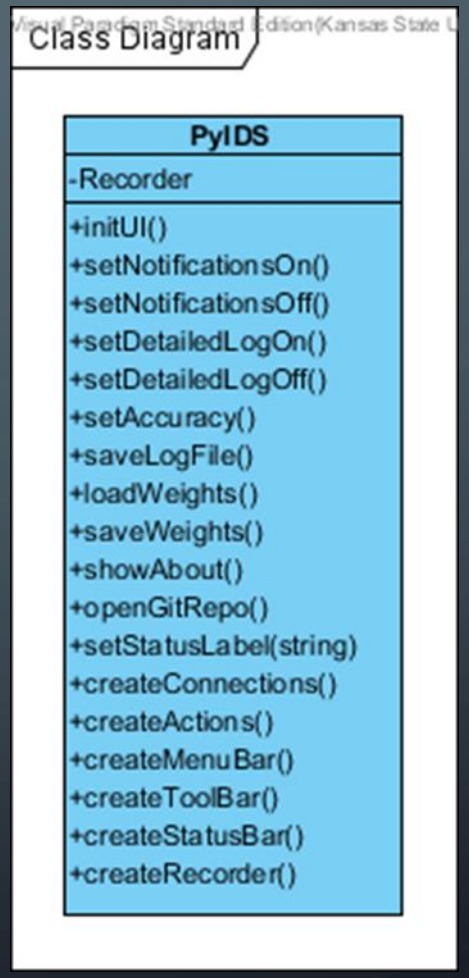
COMPONENT DESIGN

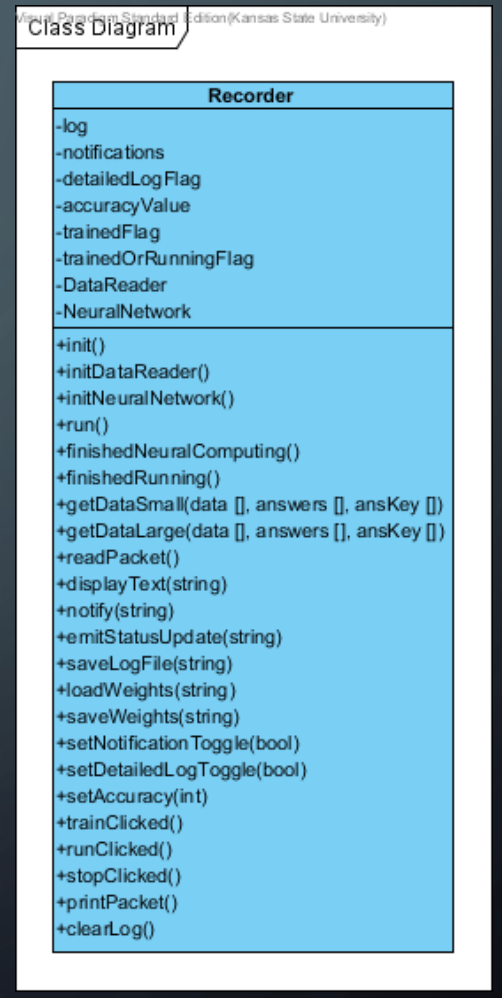
- Class Diagram



COMPONENT DESIGN

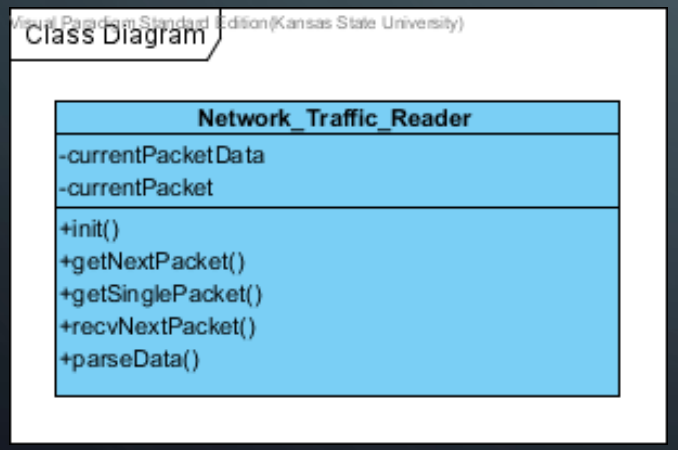
- Class Diagram
  - PyIDS (UI)
  - Recorder

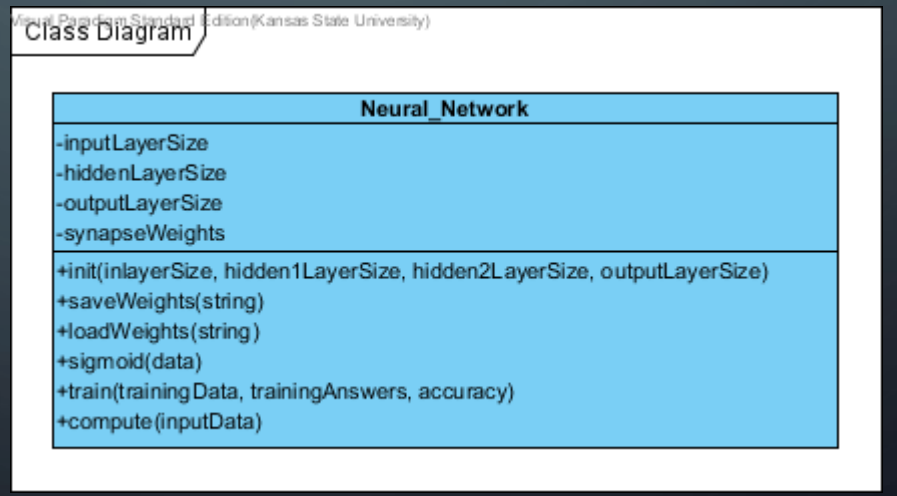


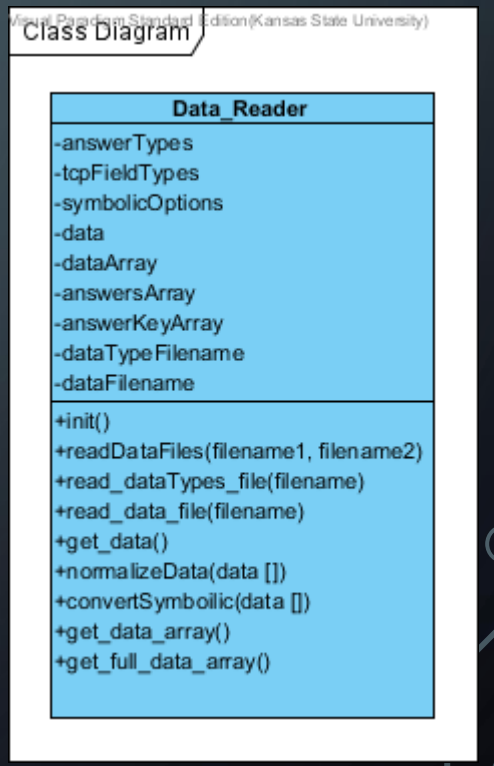


COMPONENT DESIGN

- Class Diagram
  - Network Traffic Reader
  - Neural Network
  - Data Reader

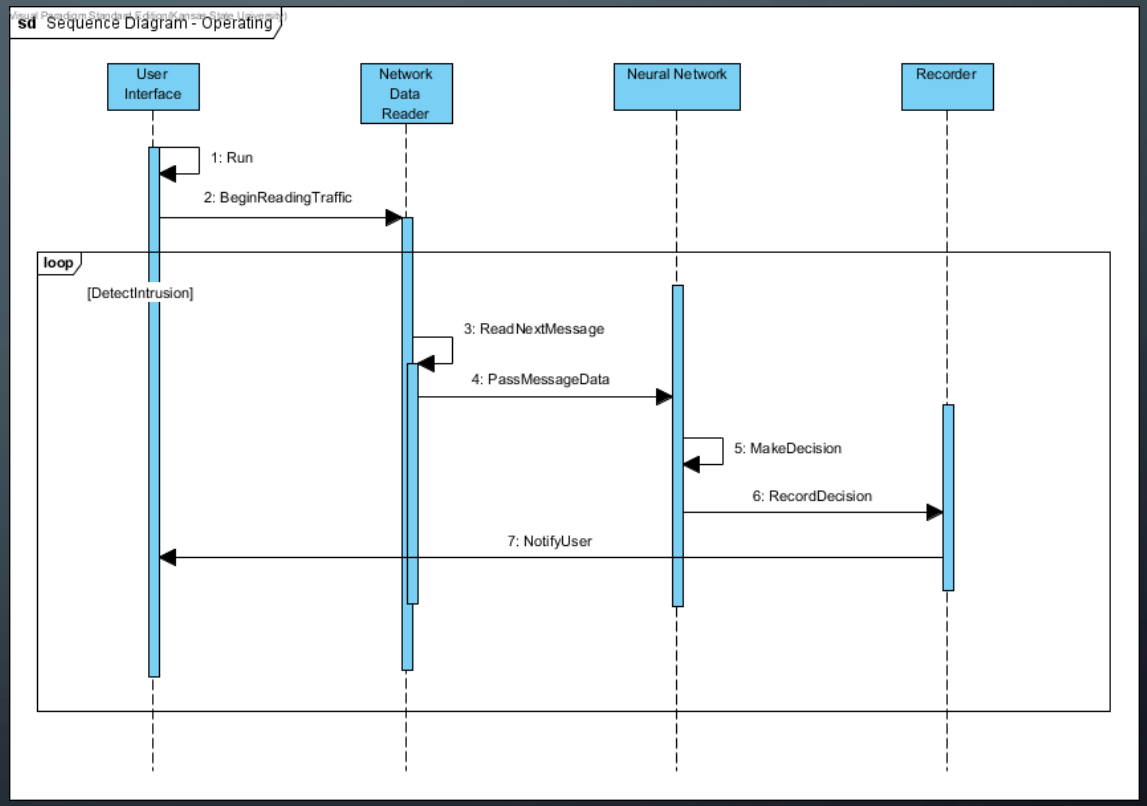






COMPONENT DESIGN

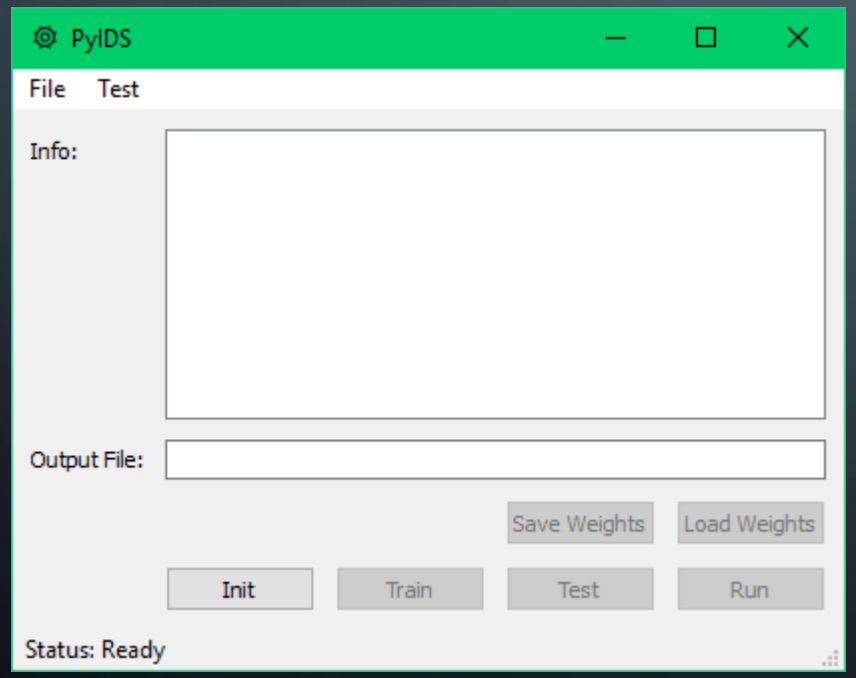
- Sequence Diagrams



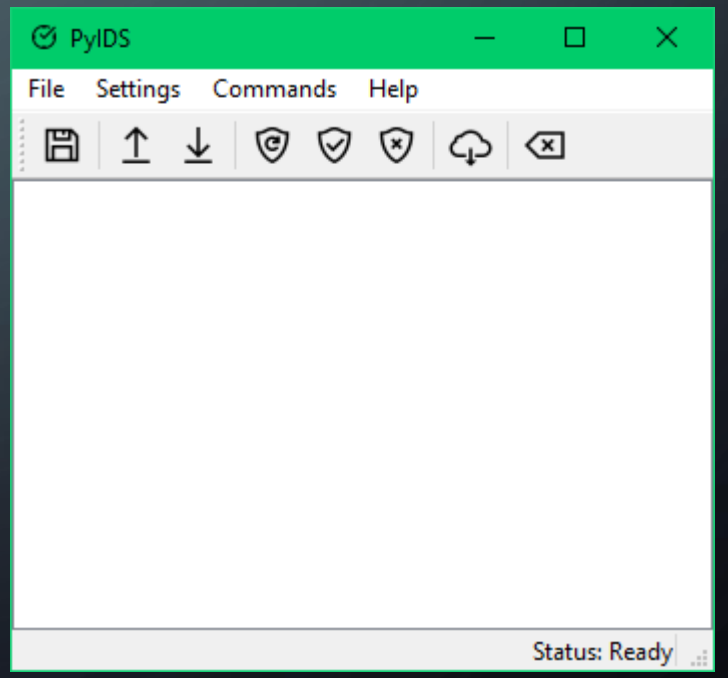
USER MANUAL

- Added descriptions to all major function interfaces
- Changed design of GUI for final product

OLD

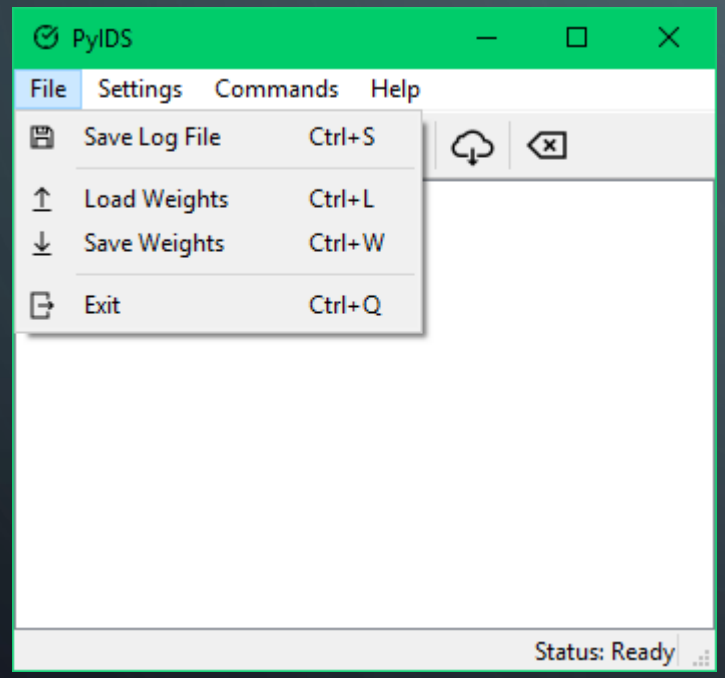


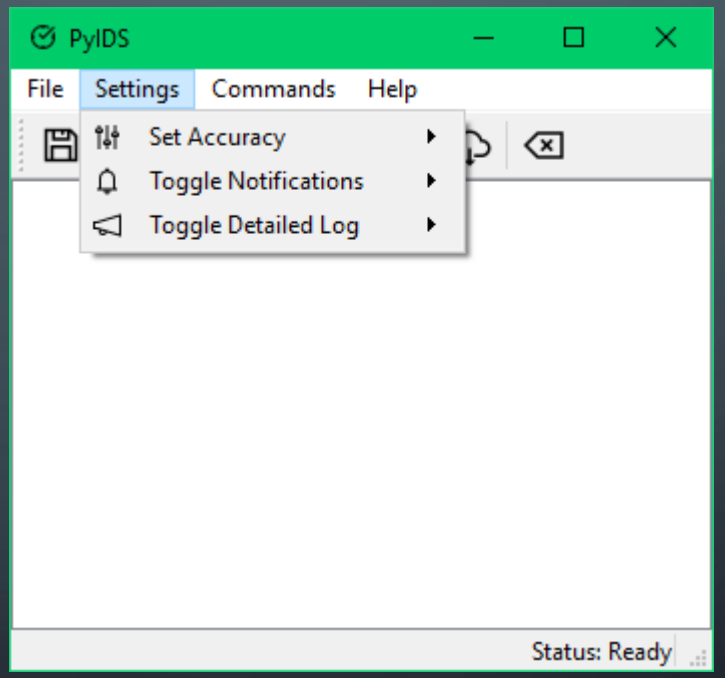
NEW

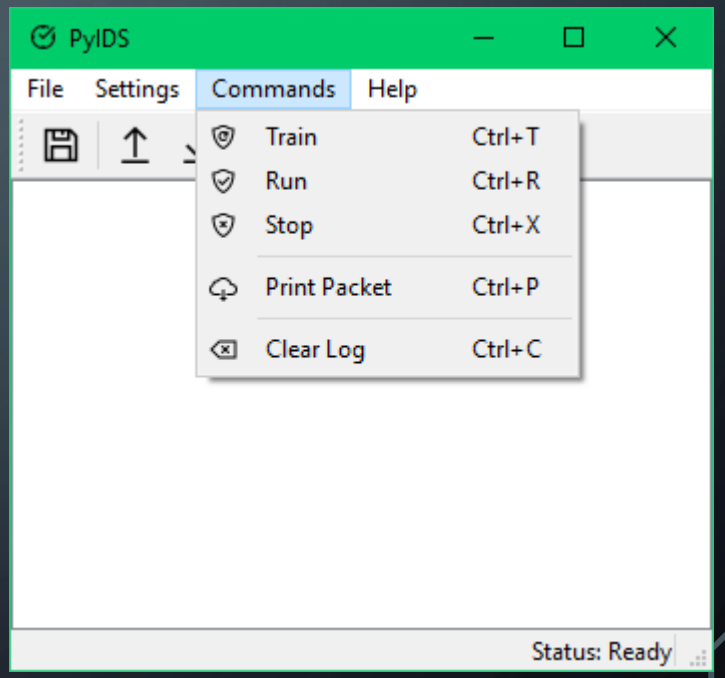


USER MANUAL

- New Menu Options

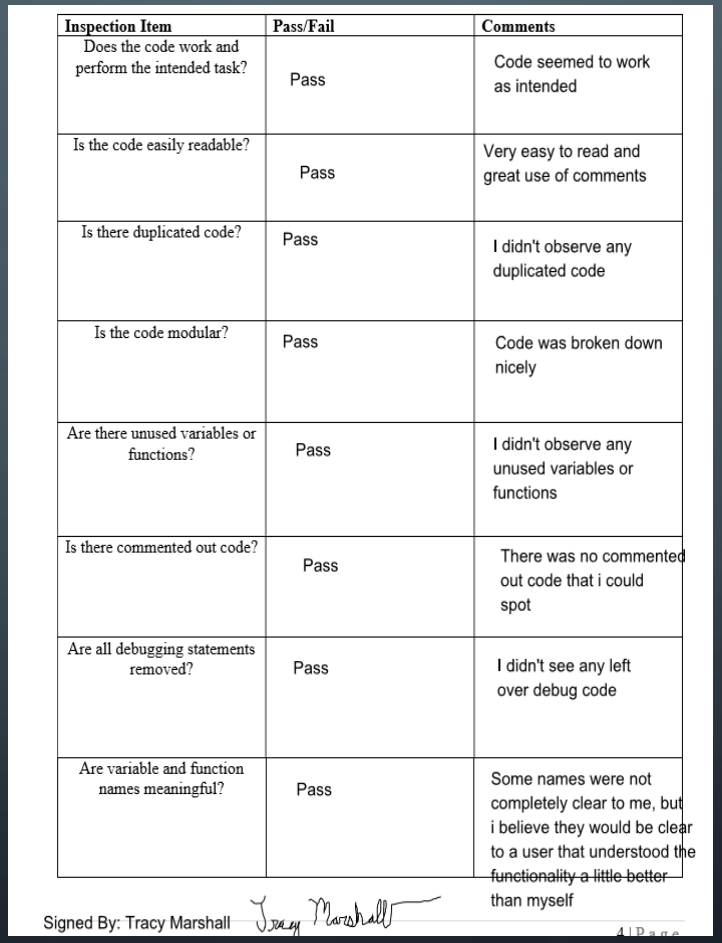






FORMAL TECHNICAL INSPECTION

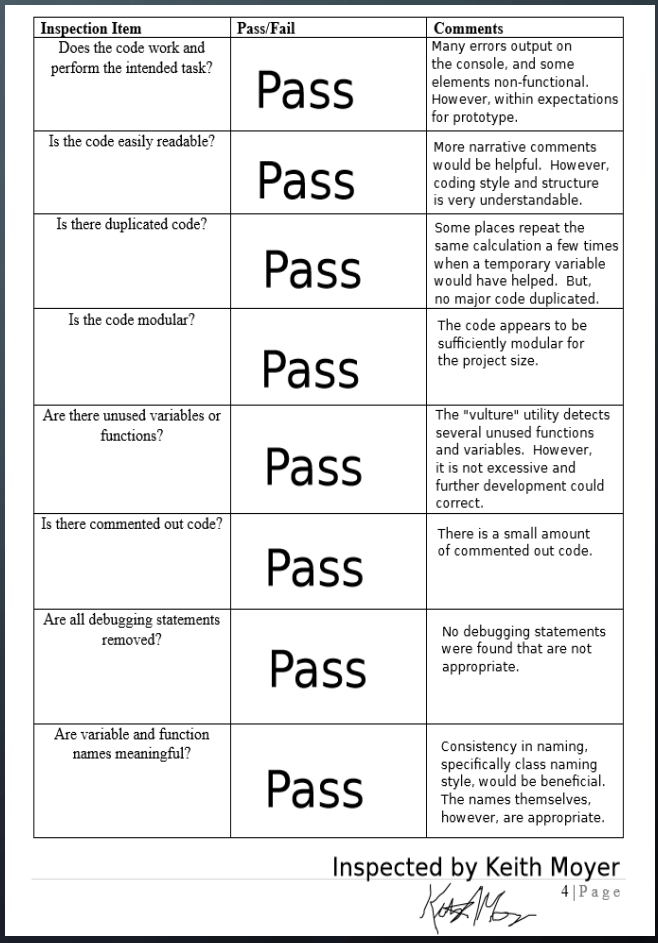
- All items were passed



Inspection Item	Pass/Fail	Comments
Does the code work and perform the intended task?	Pass	Code seemed to work as intended
Is the code easily readable?	Pass	Very easy to read and great use of comments
Is there duplicated code?	Pass	I didn't observe any duplicated code
Is the code modular?	Pass	Code was broken down nicely
Are there unused variables or functions?	Pass	I didn't observe any unused variables or functions
Is there commented out code?	Pass	There was no commented out code that i could spot
Are all debugging statements removed?	Pass	I didn't see any left over debug code
Are variable and function names meaningful?	Pass	Some names were not completely clear to me, but i believe they would be clear to a user that understood the functionality a little better than myself

Signed By: Tracy Marshall

4 | Page



Inspection Item	Pass/Fail	Comments
Does the code work and perform the intended task?	Pass	Many errors output on the console, and some elements non-functional. However, within expectations for prototype.
Is the code easily readable?	Pass	More narrative comments would be helpful. However, coding style and structure is very understandable.
Is there duplicated code?	Pass	Some places repeat the same calculation a few times when a temporary variable would have helped. But, no major code duplicated.
Is the code modular?	Pass	The code appears to be sufficiently modular for the project size.
Are there unused variables or functions?	Pass	The "vulture" utility detects several unused functions and variables. However, it is not excessive and further development could correct.
Is there commented out code?	Pass	There is a small amount of commented out code.
Are all debugging statements removed?	Pass	No debugging statements were found that are not appropriate.
Are variable and function names meaningful?	Pass	Consistency in naming, specifically class naming style, would be beneficial. The names themselves, however, are appropriate.

Inspected by Keith Moyer

4 | Page

TEST PLAN UPDATE

- Decided to go with Unit Test type test plan along with a system test of the important pieces of the GUI
- Added additional tests
- Used Python's common unit testing framework unittest
- Wrote a System Test Procedure for the GUI critical requirements of notifications and log output
- Updated Test Plan to reflect changes

SYSTEM TEST PROCEDURE

- Testing Notification and Log output

Step	Action	Expected Outcome
1	Start the PyIDS Application	PyIDS is shown and operating
2	Toggle Notifications "On"	
3	Press "Print Packet" button	Notification appears
		Packet information displayed in log
4	Press "Save Log File" button	Save File browser appears
5	Enter name for log file and press save	
6	Open up system file browser	
7	Go to location designated for log file	
8	Open log file saved	Log file contains packet information

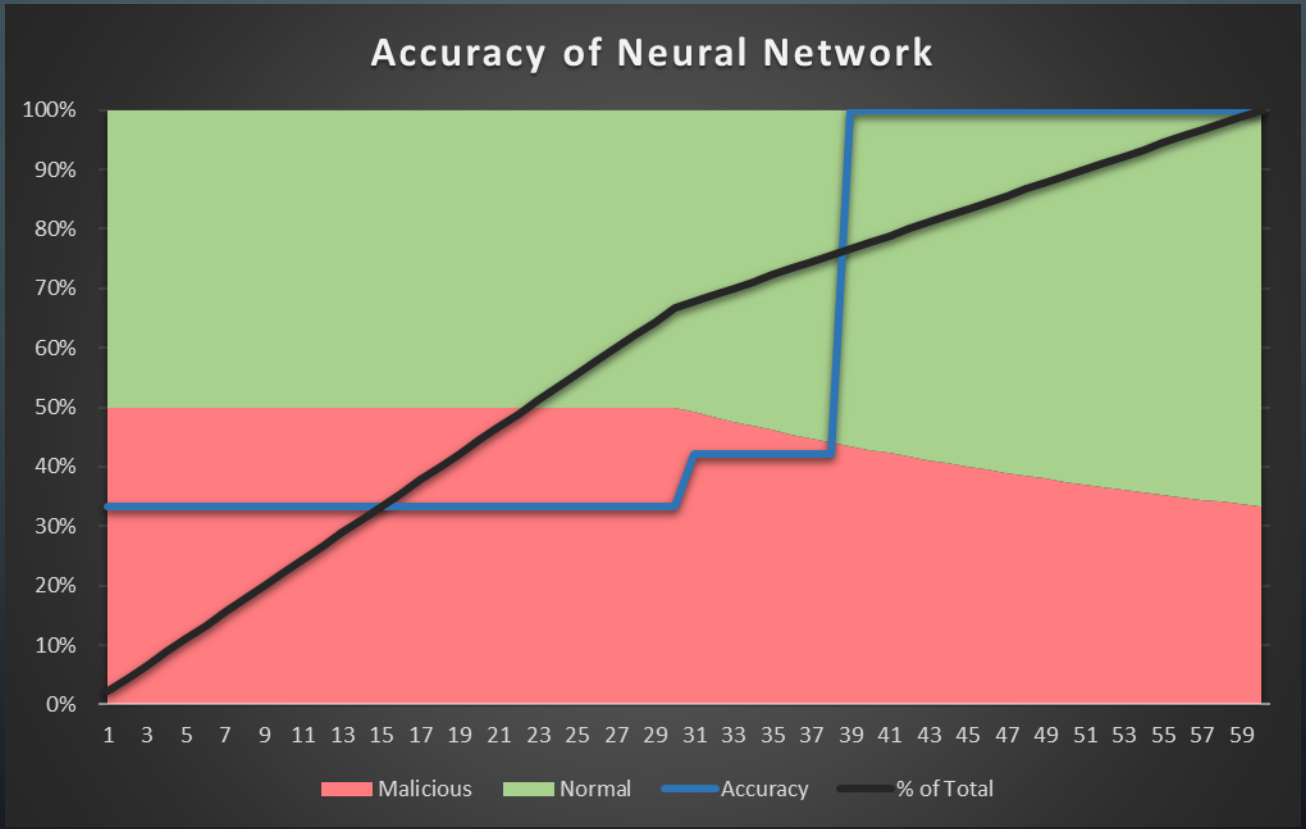
ASSESSMENT EVALUATION

- All tests passed
- Tested all critical requirements

#	Requirement(s)	Test Name	Time (sec)	Result
1	SR4.1	test_DR_getDataArray	11	PASS
2	SR4.1	test_DR_getFullDataArray	15	PASS
3	SR4.1	test_DR_readData	11	PASS
4	SR3.1, SR4.1	test_NN_determineMalicious	11	PASS
5	SR3.1, SR4.1	test_NN_trainAndCompute	12	PASS
6	SR1.1	test_NTR_getNextPacket	6	PASS
7	SR2.1	test_NTR_getSinglePacket	5	PASS
8	SR5.1, SR6.1	System Test	N/A	PASS

PROJECT EVALUATION

- Neural Network Analysis

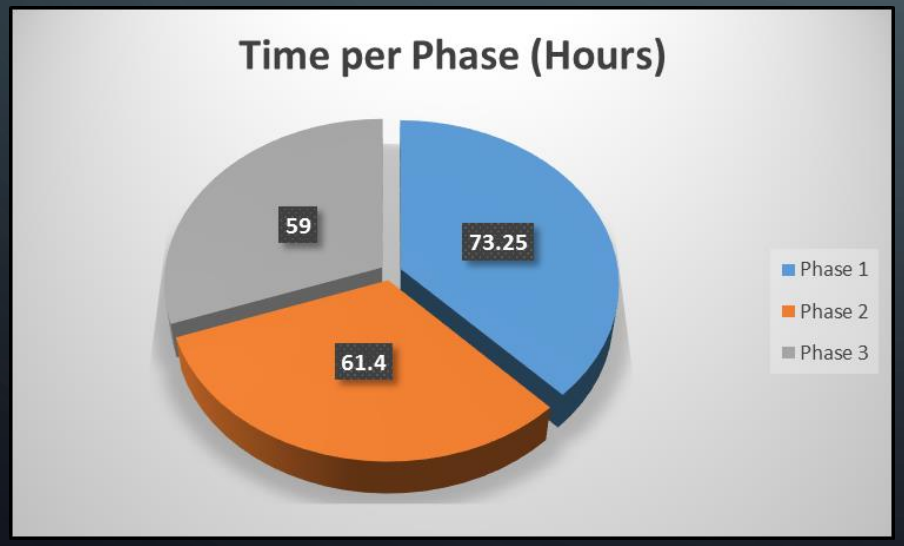


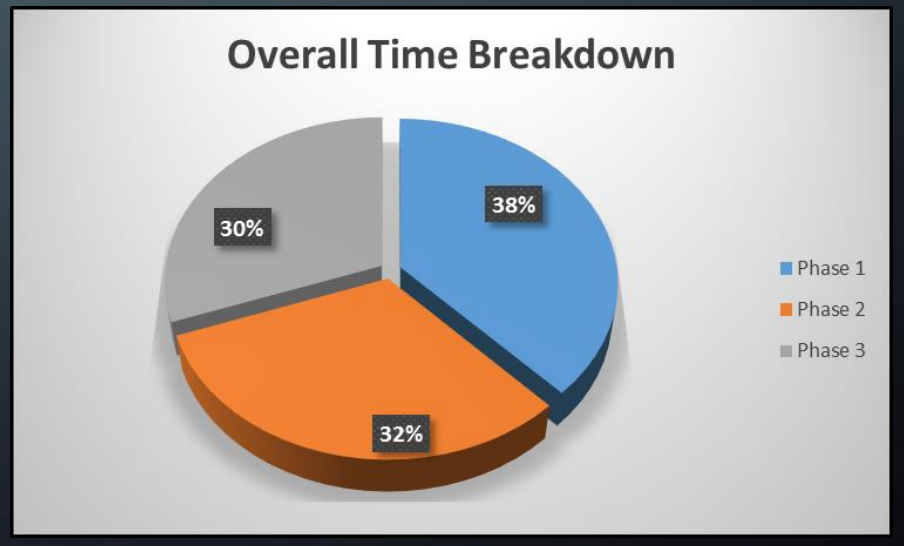
PROJECT EVALUATION

- SLOC and Time Estimates to Actuals

	SLOC	Time (months)
Estimate	4000	6.59
Final	1172	6.33
Accuracy	29.30%	96.11%

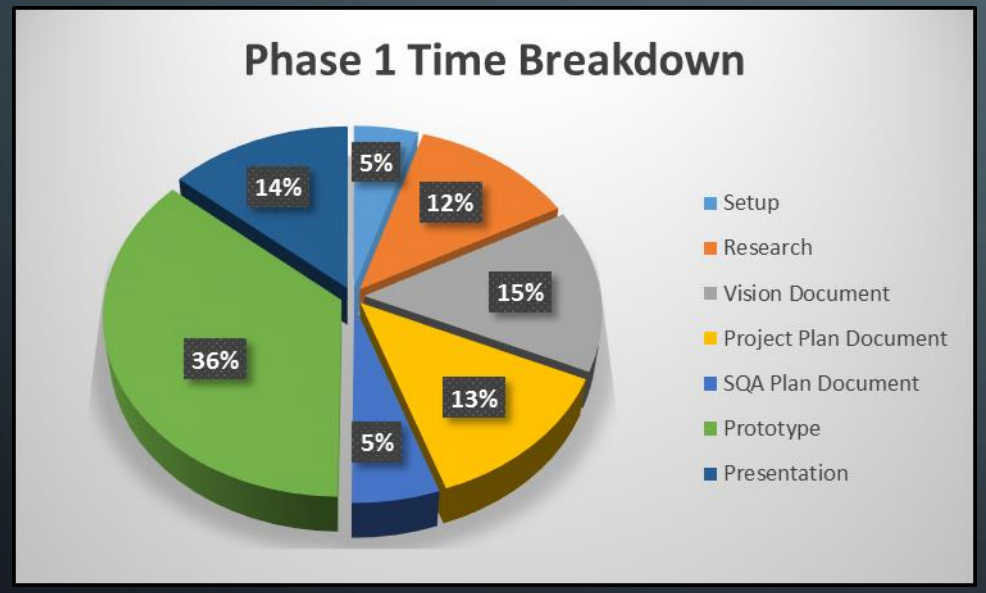
- Time per Phase

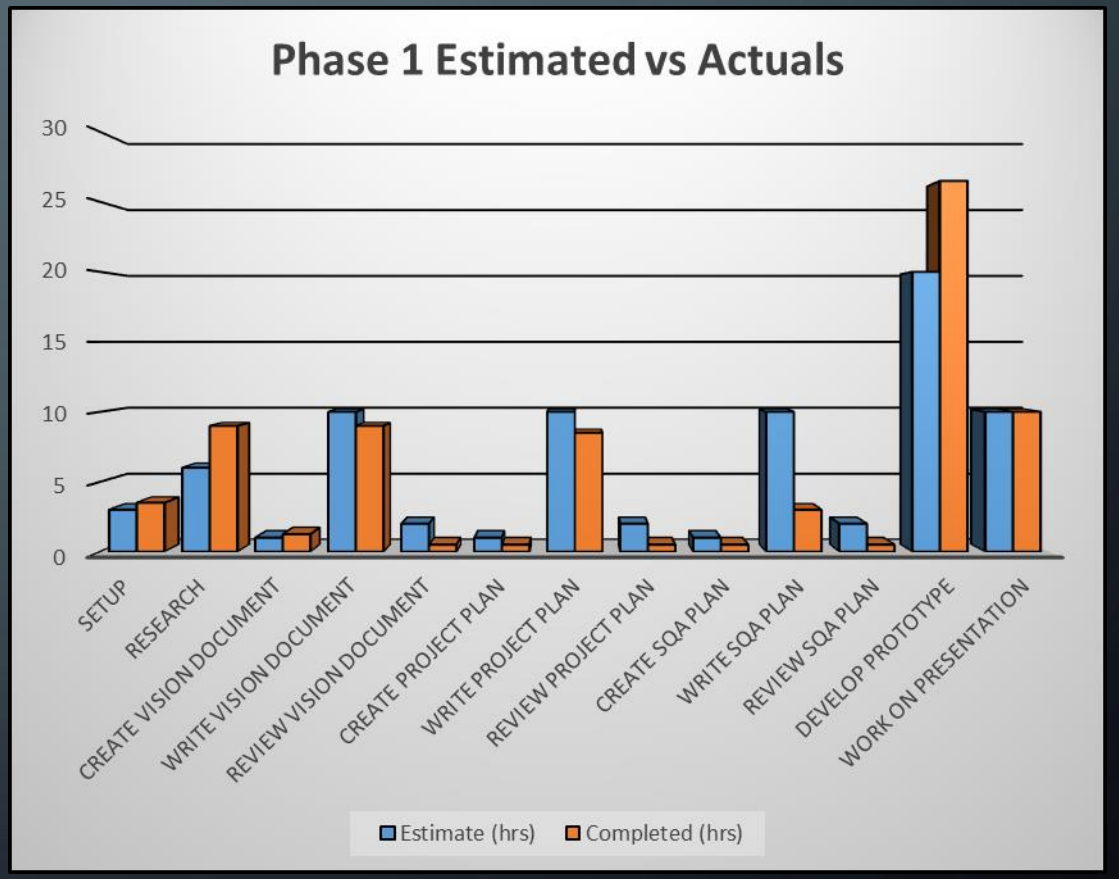




PROJECT EVALUATION

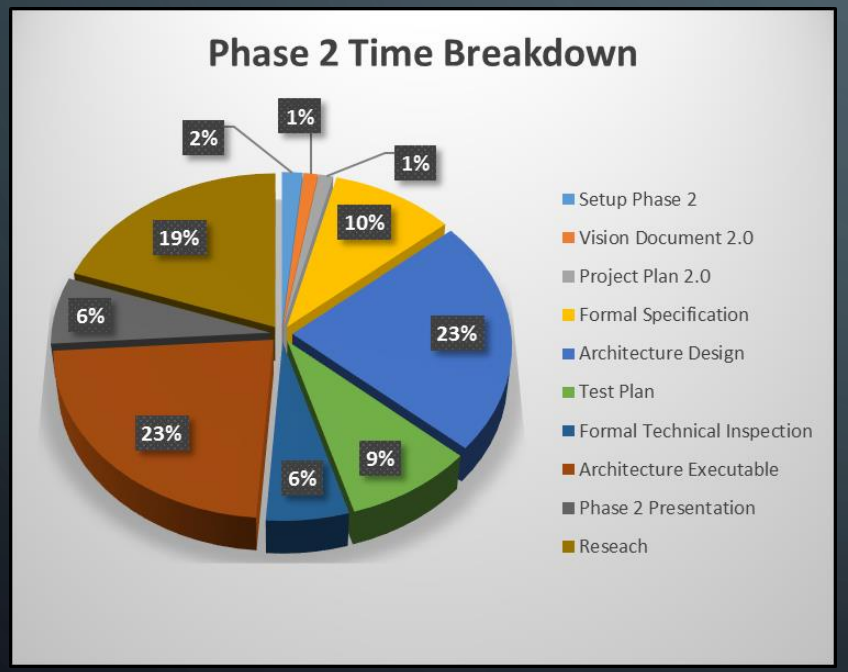
- Phase 1

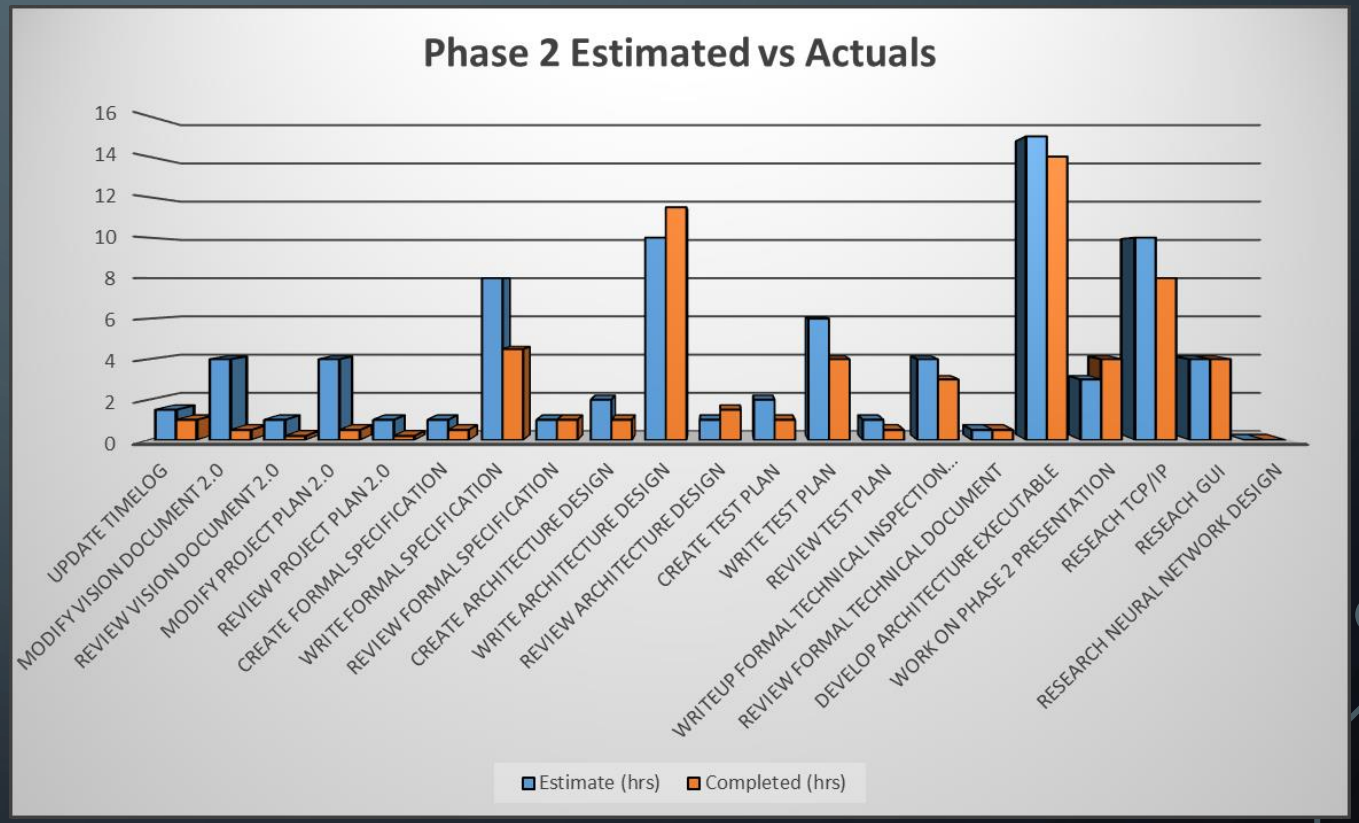




PROJECT EVALUATION

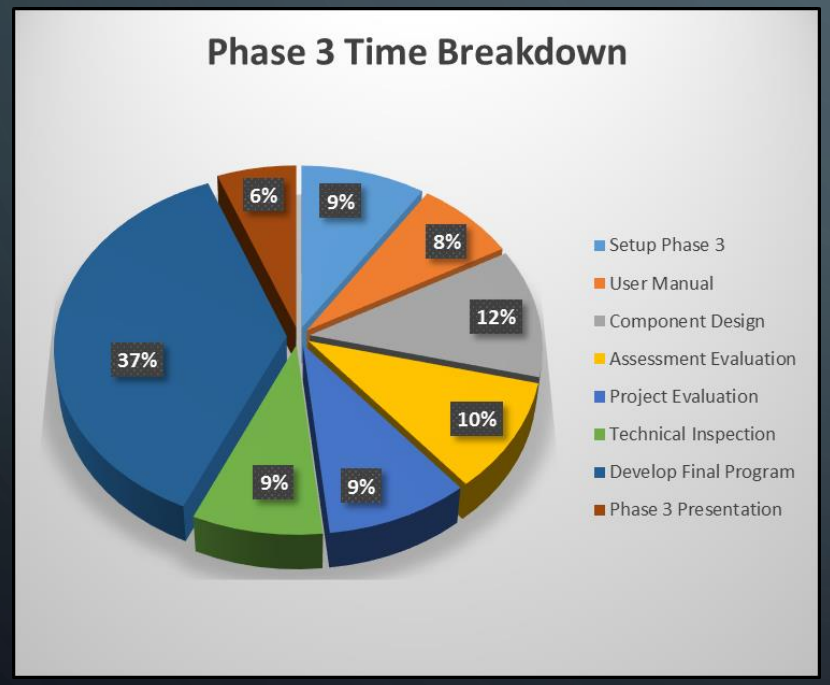
- Phase 2

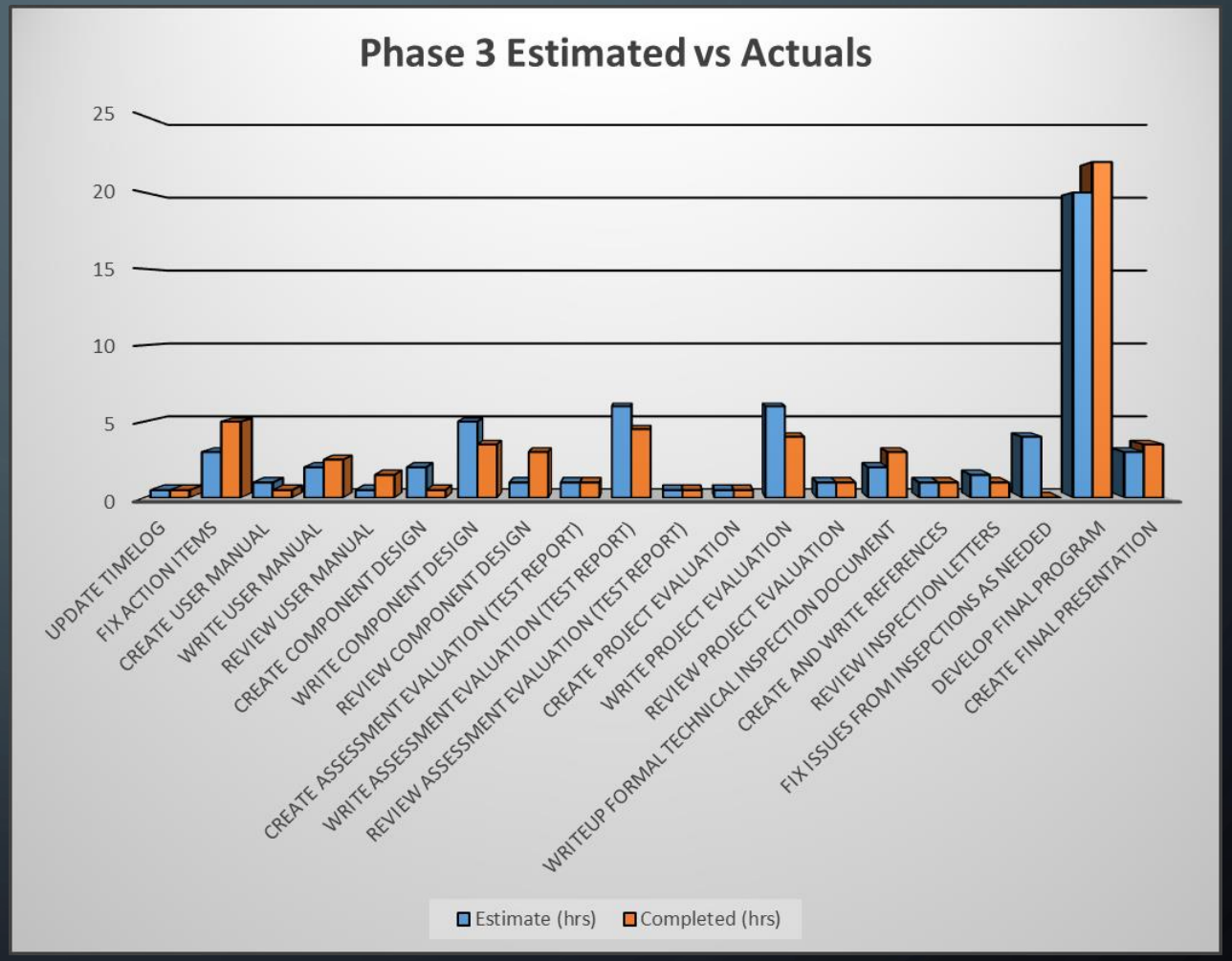




PROJECT EVALUATION

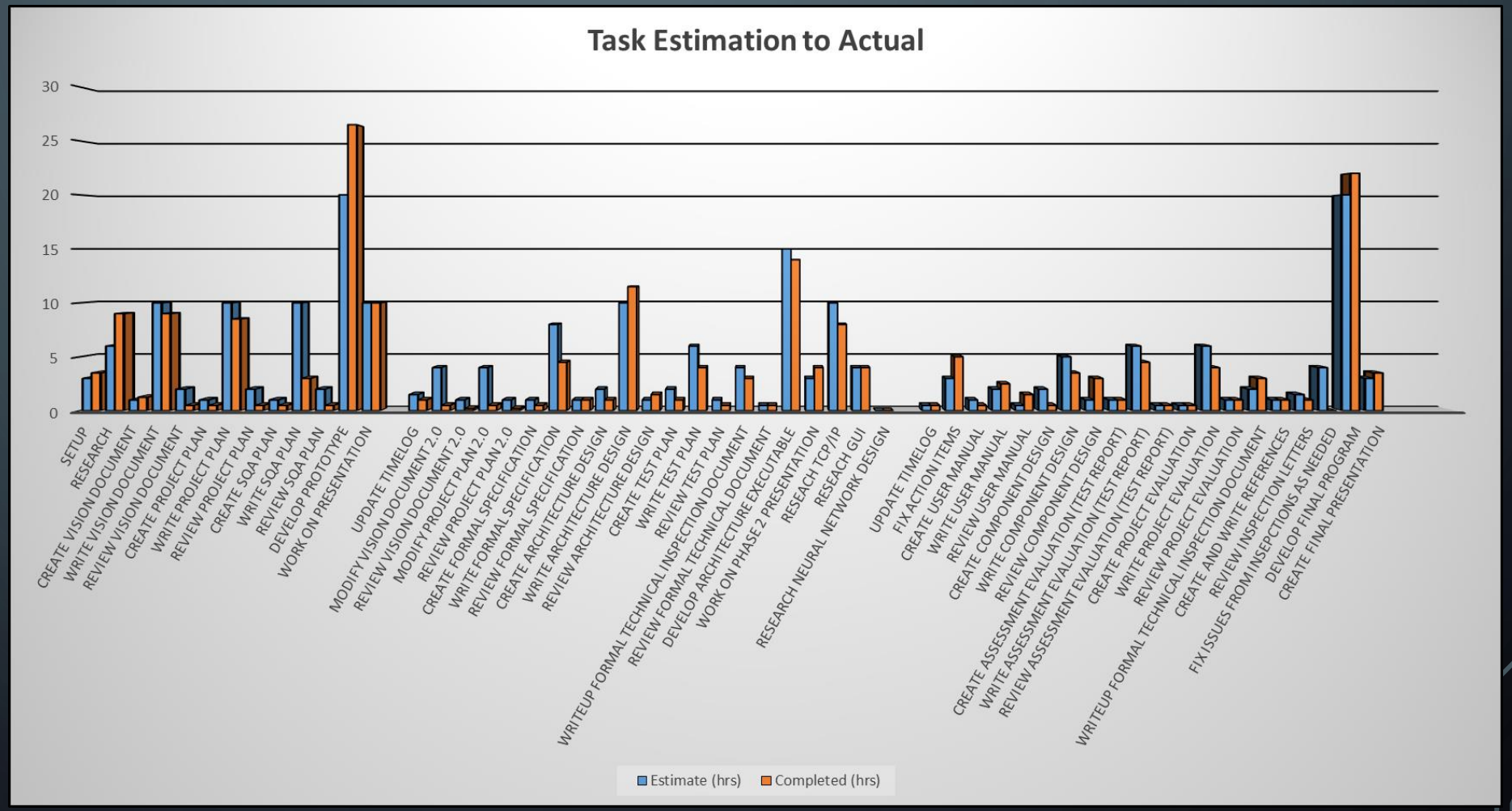
- Phase 3





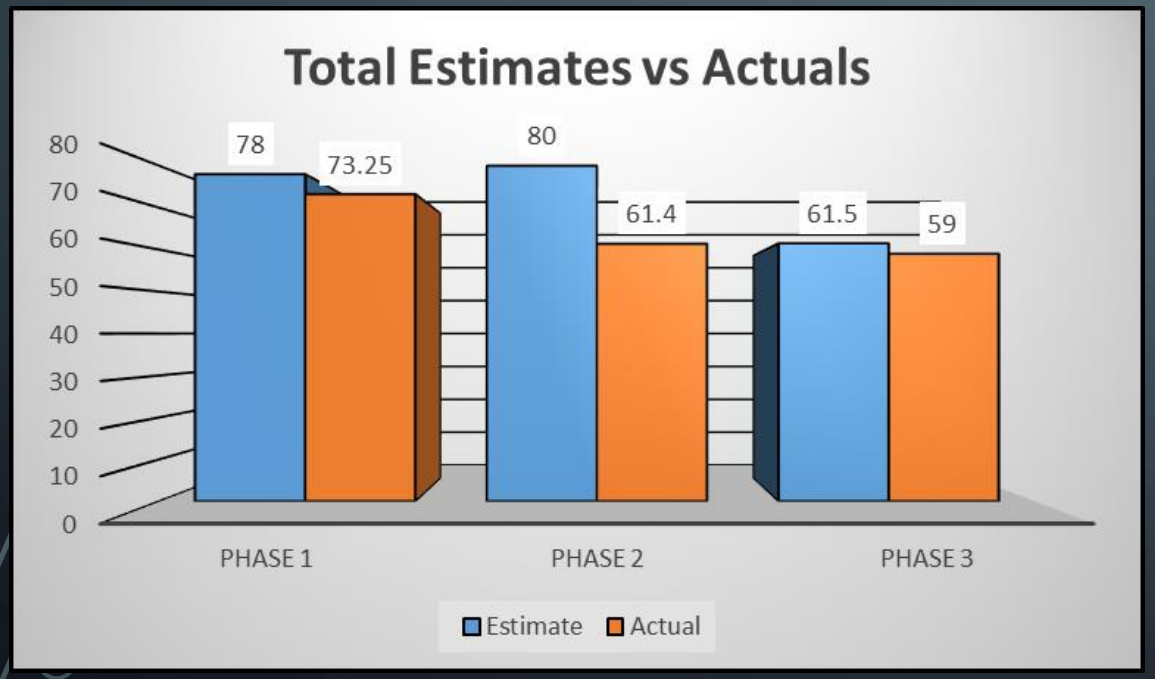
PROJECT EVALUATION

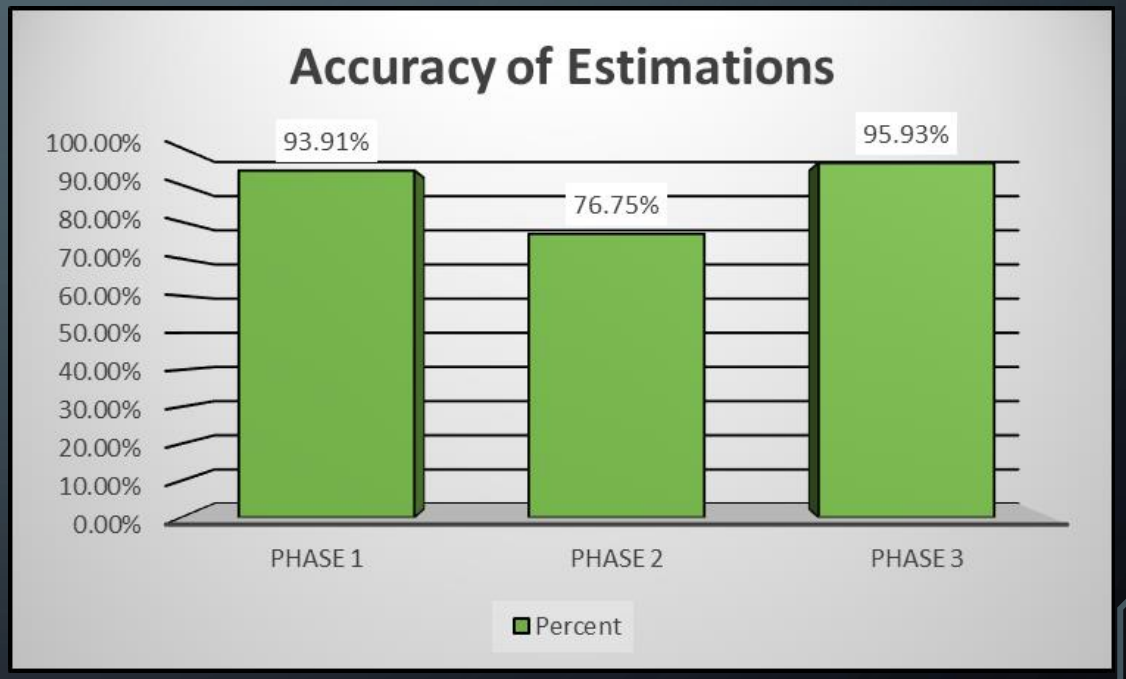
- All Tasks



PROJECT EVALUATION

- Estimation Accuracy





PROJECT EVALUATION

- Lessons Learned
  - Neural Networks
  - Networking
  - DOS Attacks
- Future Work
  - Gather better training data
  - Expert System Tracking
  - Prevent along with detection
  - Feedback false positives/negatives
  - Efficiency Improvements

DEMONSTRATION

- GitHub Repository Location:
  - https://github.com/bneedy/PyIDS
- All components of the system are working

QUESTIONS AND COMMENTS