
User Interface Design Document

Team: Lighthouse Solutions

Version: 1.0

Date: 11/28/2022

Client: Ben Drozdenko of the Naval Undersea Warfare
Center Division Newport (NUWC DIVNPT)

Prepared by Johnny Driscoll, Sean Staton, Dylan
Haughton, Brody Looney and Andy Howe



Abnormal Network Traffic Flow Dashboard Tool User Interface Design Document

Table of Contents

1.	Introduction	1
1.1	Purpose of This Document	1
1.2	References	1
2.	User Interface Standards	2
3.	User Interface Walkthrough	5
4.	Data Validation	9
	Appendix A – Agreement Between Customer and Contractor	11
	Appendix B – Team Review Sign-off	12
	Appendix C – Document Contributions	
	13	

1. Introduction

This is a capstone project for Ben Drozdenko representing the Naval Undersea Warfare Center Division Newport (NUWCDIVNPT), in partial fulfillment of the Computer Science BS degree for the University of Maine. The purpose of this project is to give the client a viable means of analyzing traffic that moves around their network in order to protect the integrity of confidentiality of all data that flows through. The project serves to detect statistical anomalies and give minimalist, user-friendly reports.

1.1 Purpose of This Document

This document naturally serves to outline the user interface design of the coming project to be developed. Below, you will find the design standards that will be maintained, a walkthrough of our interface, and a data validation description. This document is meant to be viewed and approved by the client, and thereafter, referred back to by the developers.

1.2 References

There are four references to speak on currently. The first two of these are the original and revised SRS documents. These inform us on the necessary requirements of the project. The third reference document is a data set procured from the University of New South Wales, used as reference to the proposed file structure, type of information to be analyzed by the program, and the way in which data recording should be conducted. The fourth document is our SDD document.

2. User Interface Standards

This portion of the UIDD will provide the standards as well as the general design elements that are key to the application. Tkinter a GUI for python is the software that the UI is built upon in order to have a UI with basic functionality and minimal bloat elements. The layout and general designs consists of a graph that takes up the largest portion of the UI, along with six buttons on the left hand side “Train from file”, “Train from capture”, “Start capture”, “View Feed”, “Settings”, and “Exit”.

There is no page mapping, but the user will be prompted with alerts if abnormal activity is detected in which a “Yes” or “No” button is shown to either mark this connection as normal or abnormal. These designs are intended to present the user with a basic, but functional UI to view network connections and adjust the algorithm on a need basis. As can be seen with the UI photos, the blue portion will be the graph and visual representation of the data, on the left hand side aforementioned the buttons can be seen. Lastly the title can be seen at the top of the UI “Traffic Monitor Tool”.

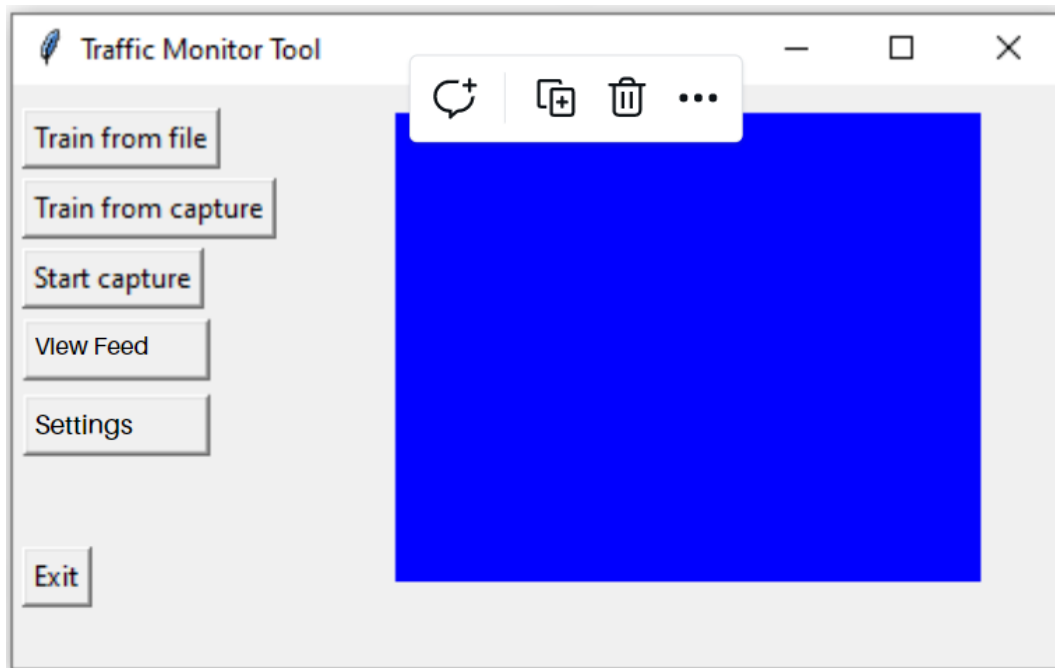


Figure 1. Home screen of the tool. This screen shows the main functionalities of the system and allows the user to access these functionalities through the use of the buttons shown.

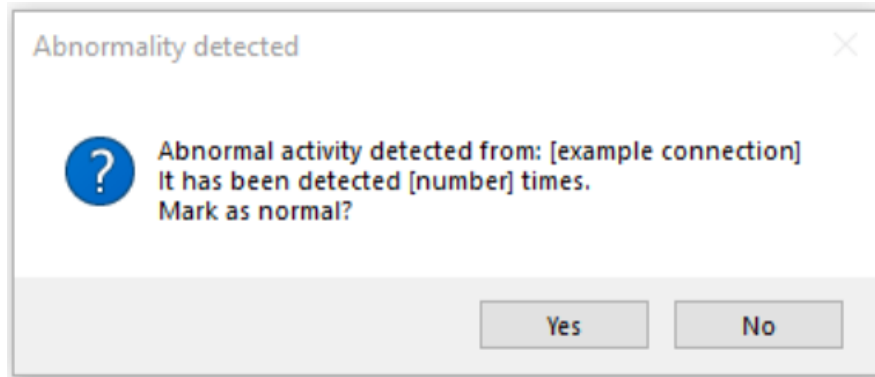


Figure 2. Individual Abnormality Screen. This screen shows more information about a specific abnormality and it allows the user to mark it as normal or abnormal through the use of the buttons shown.

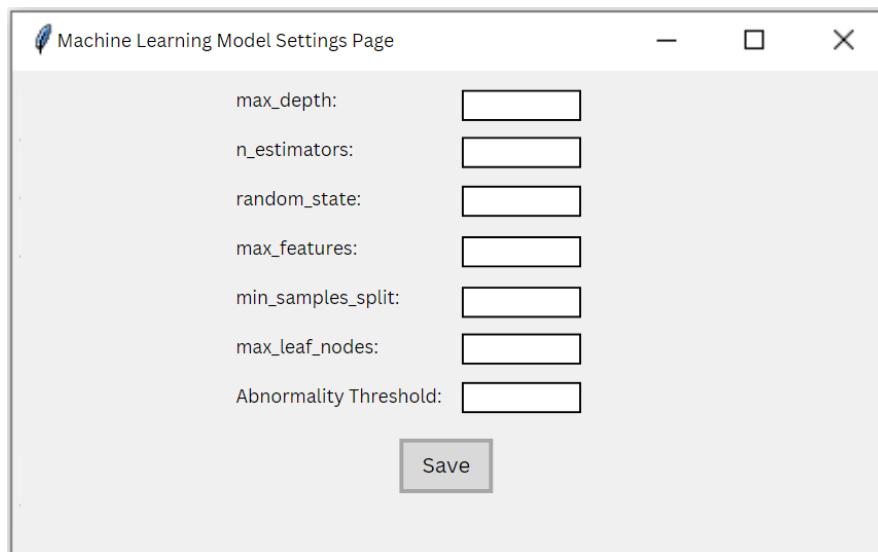


Figure 3. Machine Learning Model Settings Page. This page allows the user to enter in information for each hyperparameter of the model as well as the threshold for determining whether the connection is abnormal.

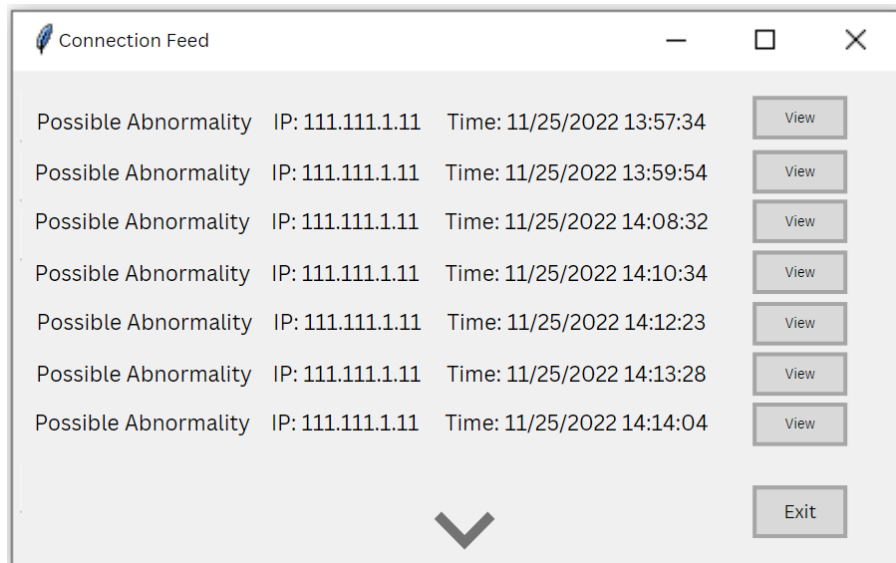


Figure 4. The connection feed page. This shows a list of the connections and some information about each connection. The user can select the 'view' button to learn more about the connection.

3. User Interface Walkthrough

This portion of the UIDD concerns a walkthrough for the UI. The figures below show each section of the user interface for this project.

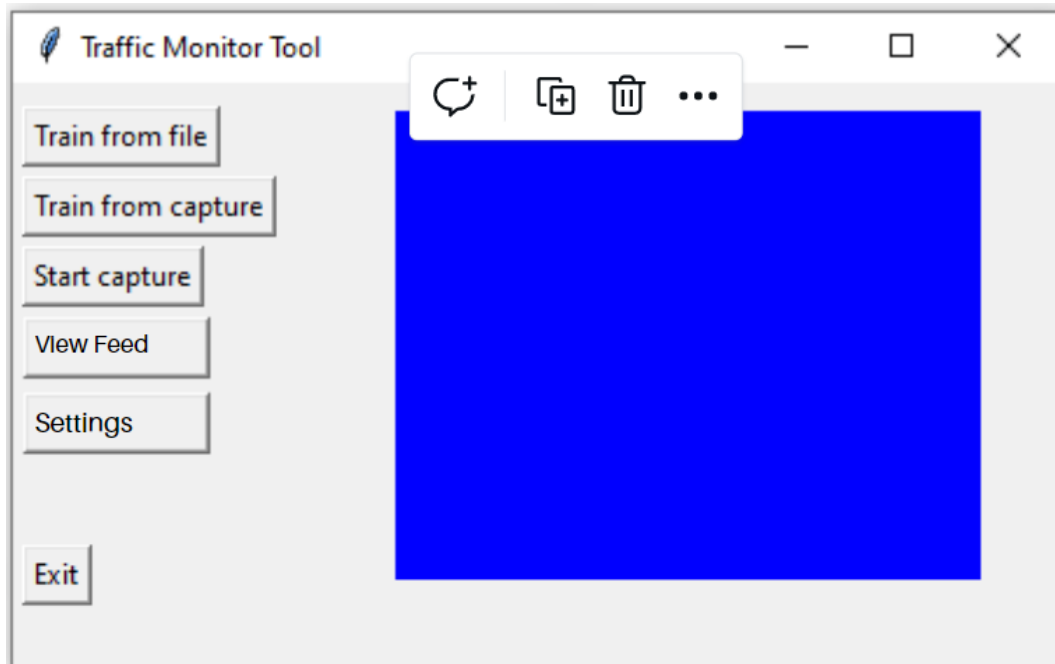
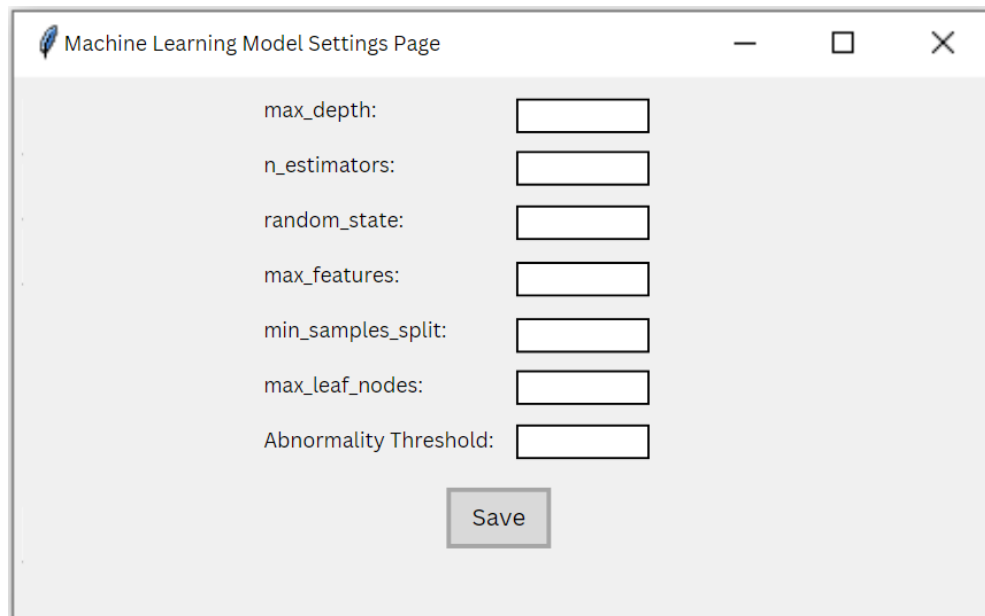


Figure 5. Home screen of the tool. This screen shows the main functionalities of the system and allows the user to access these functionalities through the use of the buttons shown.

This image shows the home screen of the tool and the user will be shown this screen upon launching the application. Each interface is as follows;

- Train from file
 - This button will prompt the user with a filesystem explorer, to which they may select a file for import. The file will begin training the ML algorithm.
- Train from capture
 - This button will start a network capture that will train the ML algorithm.
- Start capture
 - This button will begin live network capture to detect malicious network activity. If a 'train from capture' procedure was processing, this cancels it.
- View Feed
 - This button will bring the user to the 'Connection Feed' page when selected.
- Settings
 - This button will bring the user to the 'Machine Learning Model Settings Page' when selected.
- Exit

- This button merely exits the program.
- The blue subwindow
 - This subwindow is a placeholder for the graph that will eventually be programmed. The graph will naturally display the amount of malicious connections detected in the y axis, over time in the x axis.



The image shows a window titled "Machine Learning Model Settings Page". Inside the window, there are seven text input fields arranged vertically, each preceded by a label: "max_depth:", "n_estimators:", "random_state:", "max_features:", "min_samples_split:", "max_leaf_nodes:", and "Abnormality Threshold:". Below these fields is a "Save" button. The window has a standard title bar with a minimize button, a maximize button, and a close button.

Figure 6. Machine Learning Model Settings Page. This page allows the user to enter in information for each hyperparameter of the model as well as the threshold for determining whether the connection is abnormal.

This image shows the settings screen for the machine learning model. There are text boxes for each feature of the machine that allows for the user to manually enter in values.

- This page will allow the user to manually enter in the values for each hyperparameter of the machine learning model. The user may also enter in a value from 0 to 1 that will be used as the threshold for determining what is classified as abnormal behavior. After clicking the 'Save' button on this page the user will be returned to the home screen

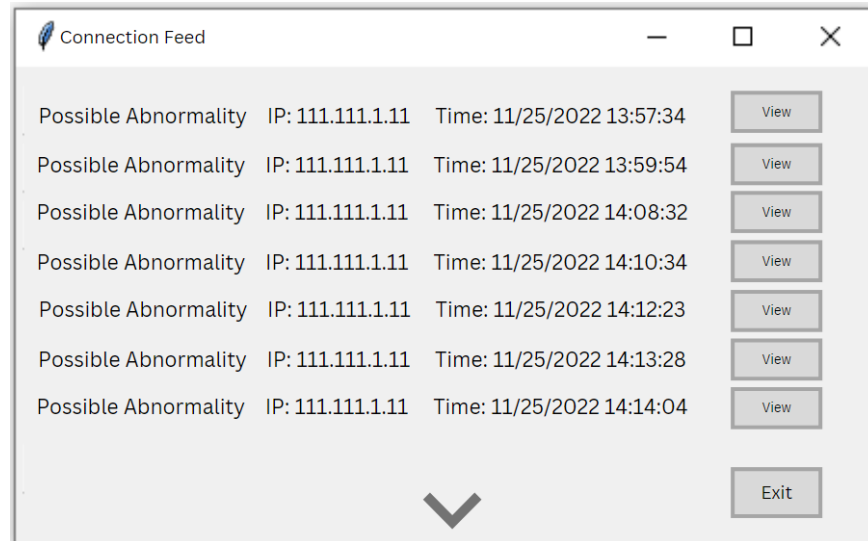


Figure 7. The connection feed page. This shows a list of the connections and some information about each connection. The user can select the 'view' button to learn more about the connection.

This image shows the connection feed page. Possible abnormalities are listed and display some information about the possible abnormality.

- View
 - This button will open up a page that displays more information about the possible abnormality. The user can click on the arrow in the bottom of the page to view more listings.
- Exit
 - This button can be clicked to exit this screen and return to the home page

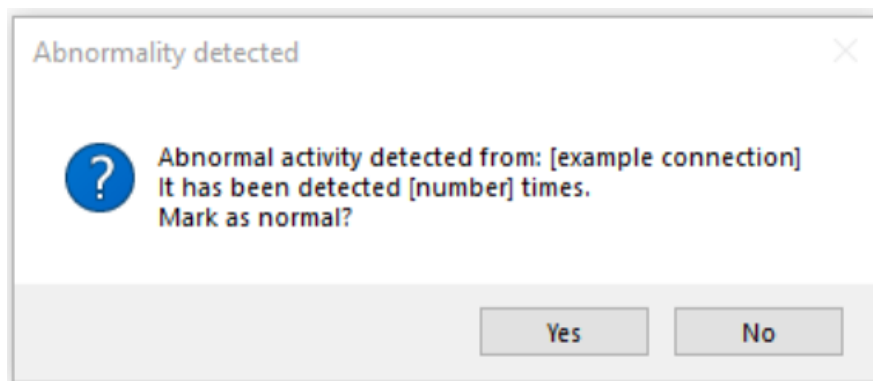


Figure 8. Individual Abnormality Screen. This screen shows more information about a specific abnormality and it allows the user to mark it as normal or abnormal through the use of the buttons shown.

In this screen the user will be able to obtain some more information about the connection and they will also be able to manually classify the connection as abnormal or normal.

- Yes
 - This will mark the connection as normal and return the user to the 'connection feed' page.
- No
 - This will mark the connection as abnormal and return the user to the 'connection feed' page.

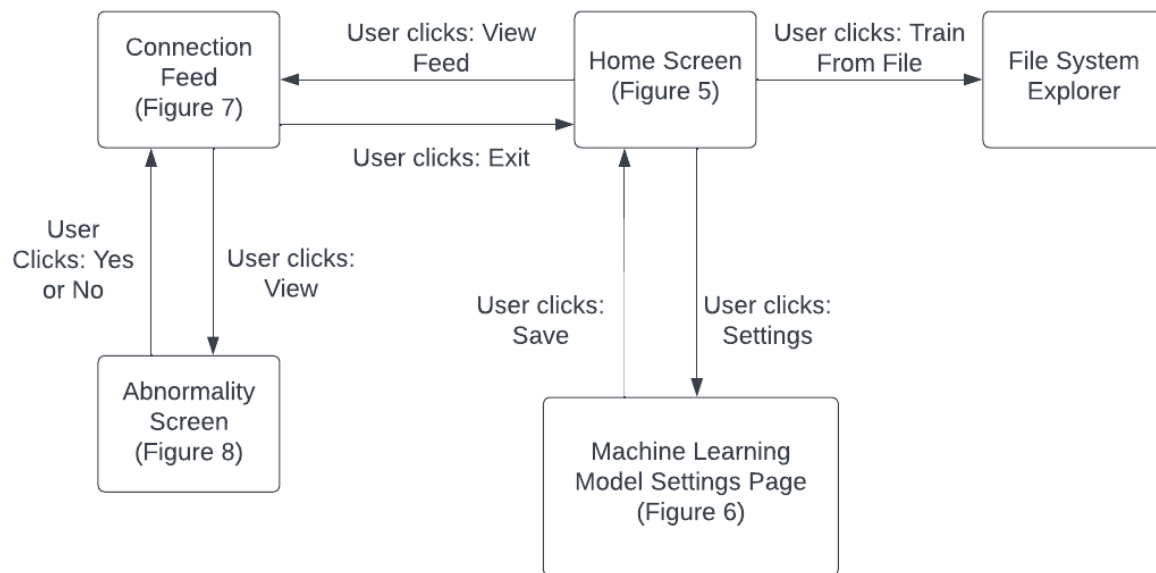


Figure 9. Navigation Diagram. This diagram shows the flow of our application. The boxes represent each individual page and the arrows show the actions of the user that will bring the user to each individual page.

4. Data Validation

A requirement of this system is that it has a lightweight interface with no bloat elements. User interaction with the system is very minimal due to this requirement. There is only one area of this project where the user is able to enter in data. That is on the machine learning model settings page, on this page the user is able to set values for the hyper parameters of the model.

Data Item Label	Description	Data Type	Limits	Screen Name
max_depth	This represents the maximum depth of the tree	integer	No limit	Machine Learning Model Settings Page
n_estimators	This represents the number of trees in the random forest.	integer	No limit	Machine Learning Model Settings Page
random_state	This controls the randomness involved in the random forest.	integer	No limit	Machine Learning Model Settings Page
max_features	This controls the number of features to use when splitting the data.	integer, float, or string.	If it is a string then it can only be 'auto', 'sqrt', or 'log2'. For integer and float there is no limit	Machine Learning Model Settings Page
min_samples_split	This controls the minimum number of samples that are required to split an internal node.	integer or float.	No limit	Machine Learning Model Settings Page
max_leaf_nodes	This controls the maximum number of leaf	integer	No limit	Machine Learning

	nodes that can be in a tree.			Model Settings Page
Abnormality Threshold	This controls the value that is used to determine what is classified as abnormal behavior	float	0 to 1	Machine Learning Model Settings Page

Figure 10. Data Validation Table. This table shows the different data items present in our UI.

The table above shows the different data items that are present on the 'Machine Learning Model Settings Page'. This table shows the effect of each item, the data type, and the limit. Currently there are 6 hyperparameters in use but this is subject to change depending on if more hyperparameters are added to the model to enhance performance.

Appendix A – Agreement Between Customer and Contractor

This document states the user interface design for the *Abnormal Network Traffic Flow Dashboard Tool* contracted by Ben Drozdenko and the Naval Undersea Warfare Center Division Newport (NUWCDIVNPT). Both the customer and the development team agree that this document clearly states the design of the user interface for this project.

In the event that there are future changes made to this document the development team and customer will discuss the changes during our bi-weekly check-in meetings. If everyone agrees on the changes, we will document the change below and sign-off showing that the amendment has been approved.

Brody Looney	<i>Brody Looney</i>	11/29/2022
Typed Name	Signature	Date
Dylan Haughton	<i>Dylan Haughton</i>	11/29/2022
Typed Name	Signature	Date
Sean Staton	<i>Sean Staton</i>	11/29/2022
Typed Name	Signature	Date
Johnathan Driscoll	<i>Johnathan Driscoll</i>	11/29/2022
Typed Name	Signature	Date
Andrew Howe	<i>Andrew Howe</i>	11/29/2022
Typed Name	Signature	Date
Typed Name	Signature	Date

Customer Comments:

Appendix B – Team Review Sign-off

Andy Howe, Dylan Haughton, Johnny Driscoll, Sean Staton, and Brody Looney have all reviewed this document. We all have agreed on the content that listed in this document is accurate and complete. We all agree that the format follows the correct structure. The signatures below prove the information stated previously is correct.

Brody Looney	<i>Brody Looney</i>	11/29/2022
Typed Name	Signature	Date
Dylan Haughton	<i>Dylan Haughton</i>	11/29/2022
Typed Name	Signature	Date
Sean Staton	<i>Sean Staton</i>	11/29/2022
Typed Name	Signature	Date
Johnathan Driscoll	<i>Johnathan Driscoll</i>	11/29/2022
Typed Name	Signature	Date
Andrew Howe	<i>Andrew Howe</i>	11/29/2022
Typed Name	Signature	Date

Comments:

Appendix C – Document Contributions

Group Member	Sections Worked On	Contribution Percentage
Sean Staton	User Interface Walkthrough	15%
Dylan Haughton	Formatting	5%
Andy Howe	SDD Review	20%
Johnny Driscoll	User Interface Standards	15%
Brody Looney	Introduction, User Interface Standards, User Interface Walkthrough, Data Validation, Appendix A, Appendix B, and Appendix C	45%