Packet Visualization

Packet Visualization System

End User Product Manual

Version 0.1

September 28, 2021

Document Control

Approval

The Guidance Team and the customers will approve this document.

Document Change Control

Initial Release	0.1
Current Release	0.1
Indicator of Last Page in Document	</3
Date of Last Review	9/27/2021
Date of Next Review	10/11/2021
Target Date for Next Update	10/11/2021

Distribution List

This following list of people will receive a copy of this document every time a new version of this document becomes available:

Guidance Team Members: Dr. Salamah

Customer: Dr. Acosta

Software Team Members: Alex Vasquez, Luis Ochoa, Adrian Belmontes, Eyan Meraz, Timmy Willams, Abraham Barraza Lomely

Change Summary

The following table details changes made between versions of this document

Version	Date	Modifier	Description
0.1	Sept 26, 2021	Team	Initial Draft, user manual for sprint 1

Table of Contents

1. Installation and Setup

1.1. Installation

Listed below are the steps for running the Packet Visualization System

1. Run *pip install packet visualization*
2. Run *python*
3. *Run the following Commands*
    a. from components.ui_components.startup_gui import Ui_startup_window
    b. ui = Ui_startup_window()
    c. ui.run_program()

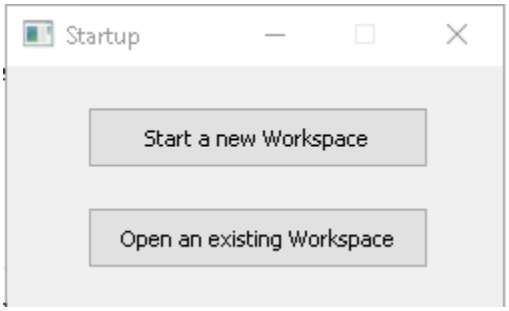
See section 2 for the system's user manual.

2. Product/User Manual

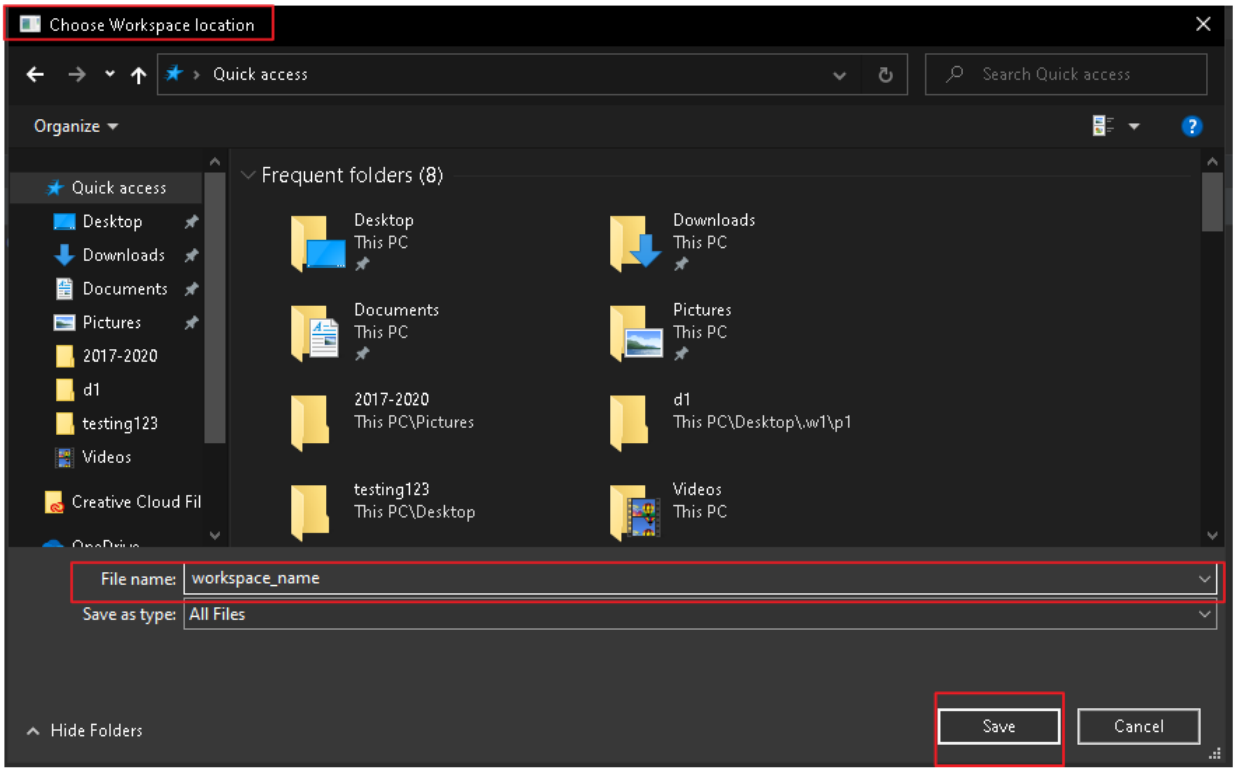
2.1. Startup

2.1.1 Description

Upon starting the system the user will be prompted to Start a new Workspace or Open an existing Workspace. For Opening an existing workspace please refer to section 2.9.

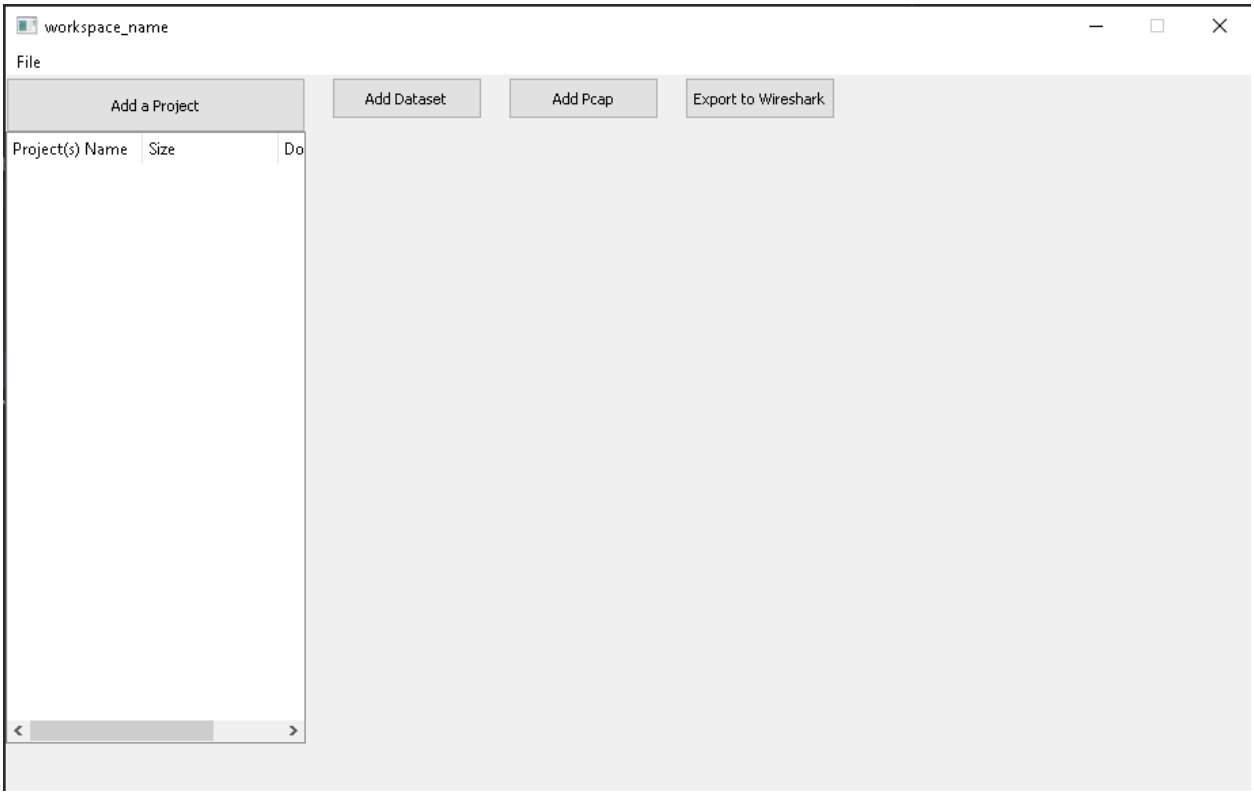


When the “Start a new Workspace” button is selected the user will be asked to assign a name for the workspace along with a save location. A directory with the workspace name will be created in the save location.



2.2 Workspace Layout

Once a workspace is successfully created, the following window will be displayed:

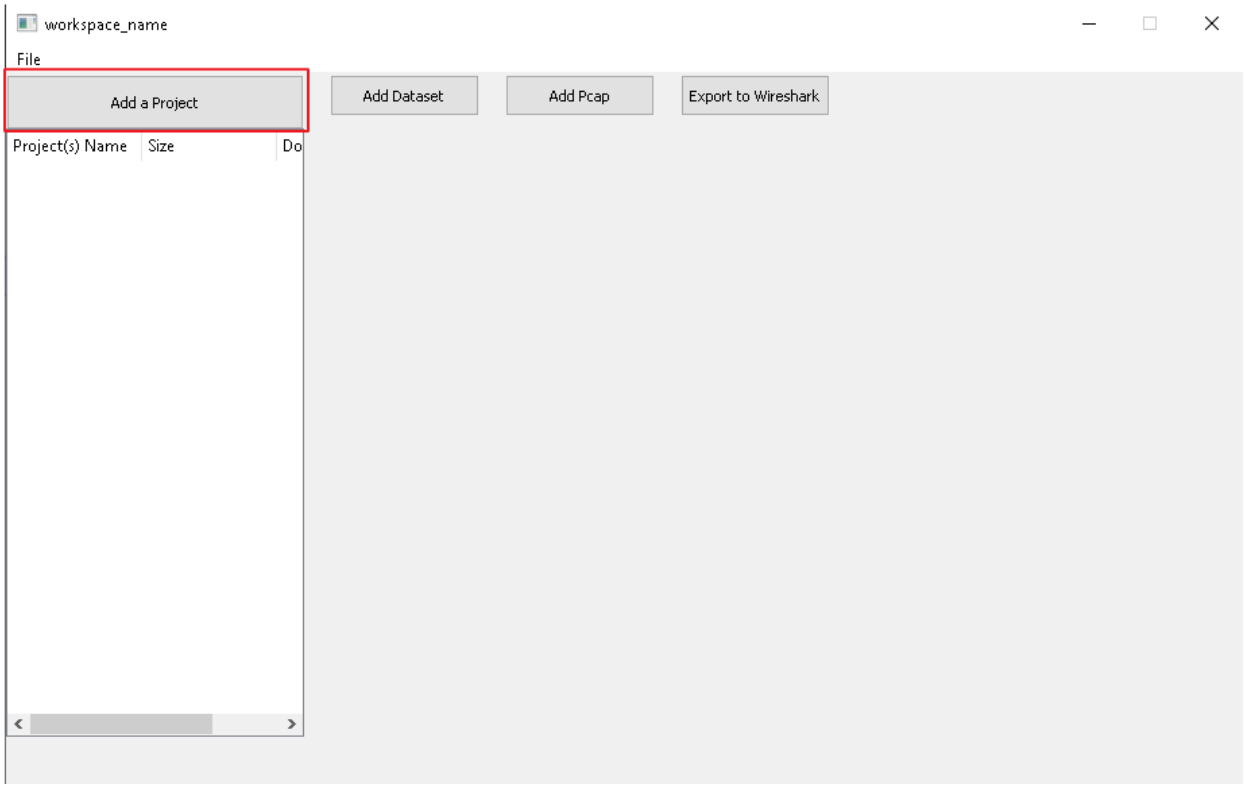


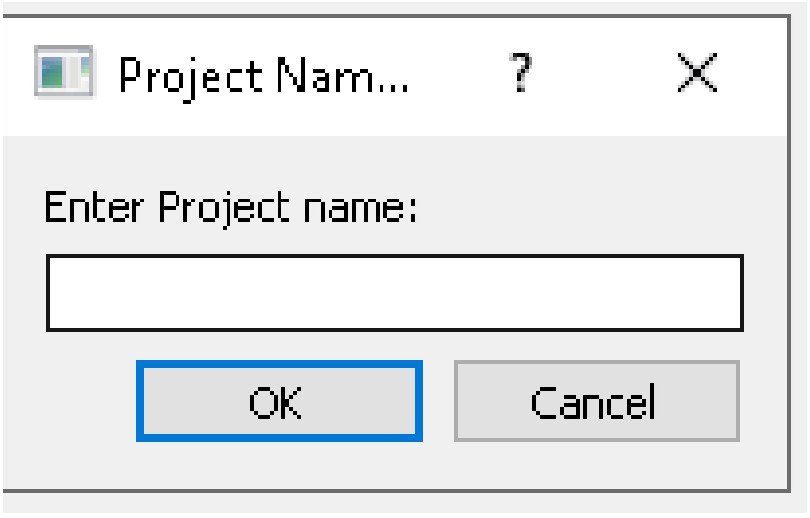
In this pane only the “Add a Project” button will have functionality. The functionality for the other 3 buttons displayed can be found in the following sections. As of version 0.1, there is no view of selected datasets however the intention will be to display this data in future versions.

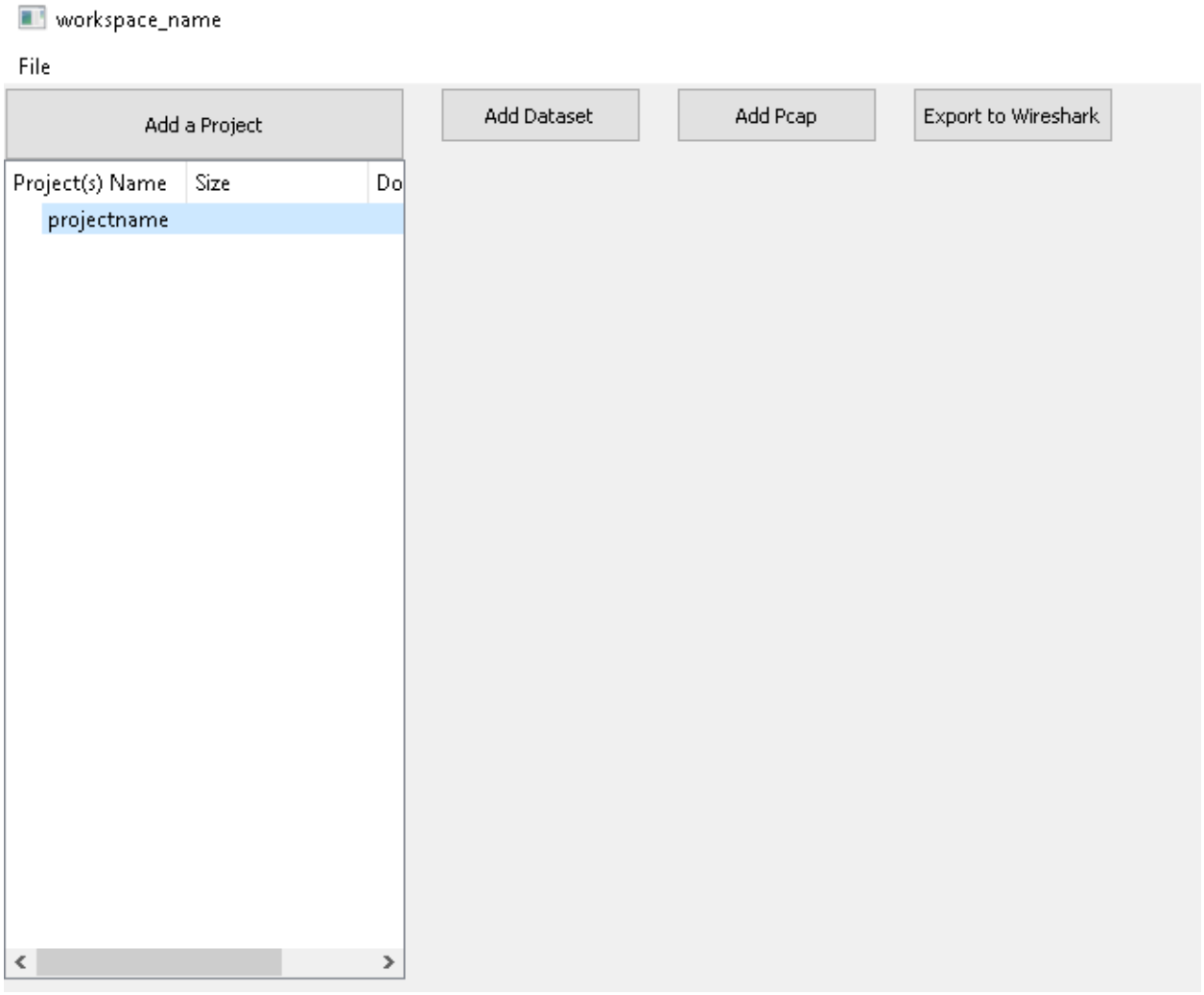
2.3 Add Project

When creating a project the user will follow a similar procedure and will be asked to name the project. Once the project is successfully created a directory will be created using the project's name with a location inside of the workspace. The project will then appear in the left pane as follows:

Note: A user can add multiple projects to a workspace. This “Add a Project” button will always prompt the user for a project name as long as the workspace is successfully created.

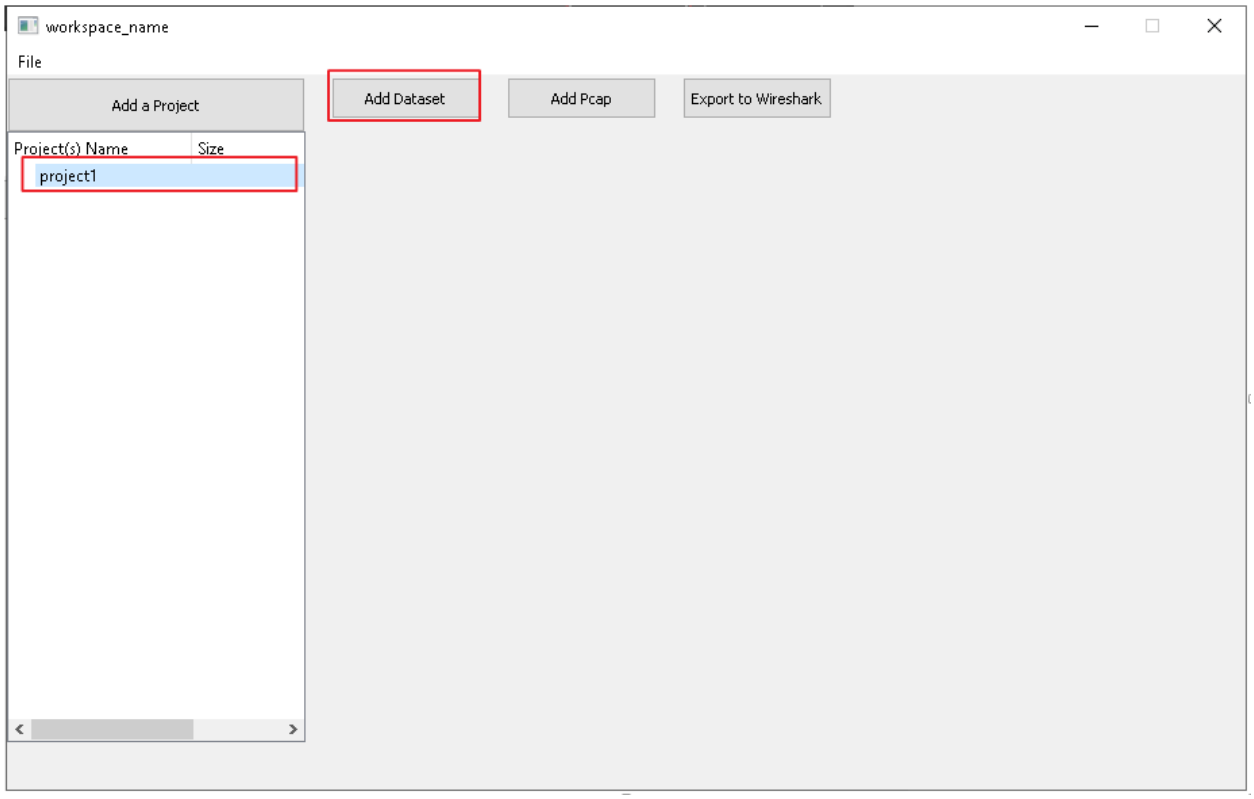

workspace_name
File
Add a Project
Add Dataset
Add Pcap
Export to Wireshark
Project(s) Name
Size
Do

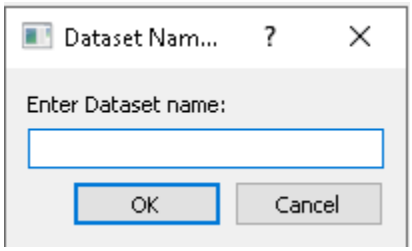

Project Nam...
Enter Project name:
OK
Cancel



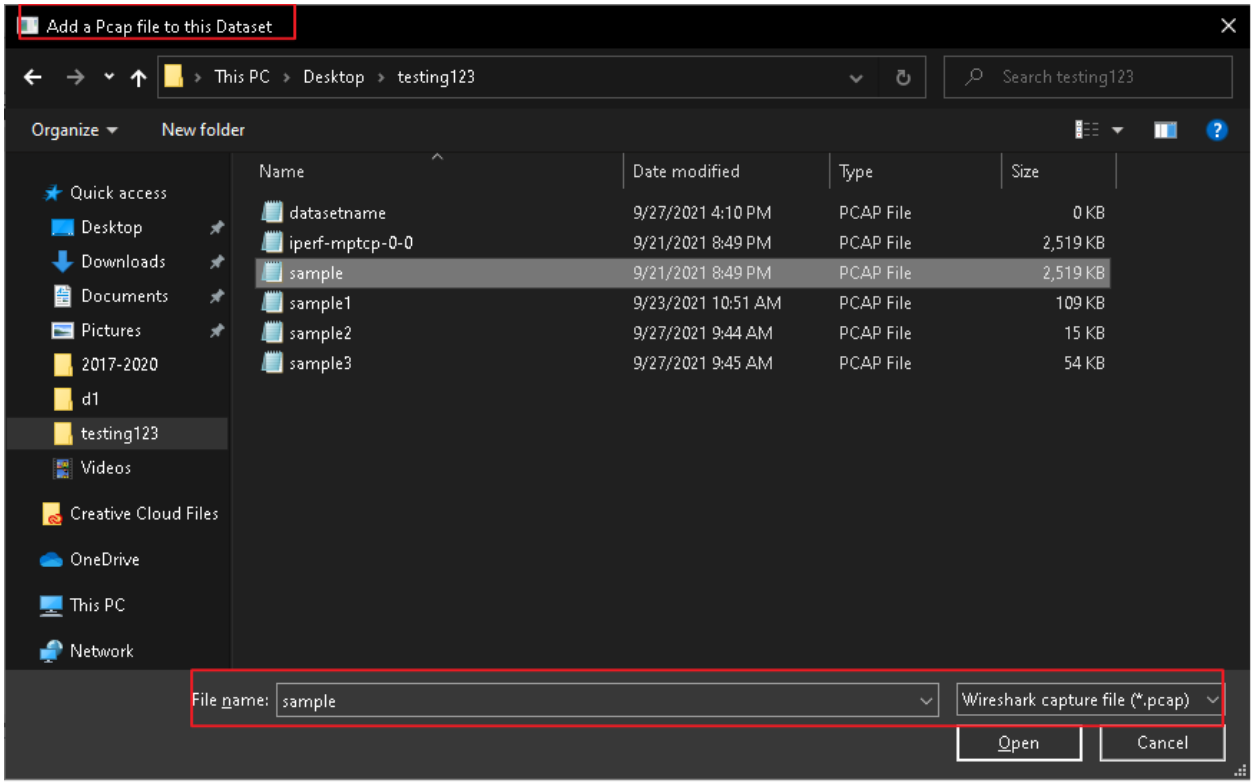
2.4 Add Dataset

Once a Workspace and Project have been successfully created, a user will now have the ability to add a dataset. The user must select a project for which the Dataset will be added and the user will follow the same procedure as adding a project.

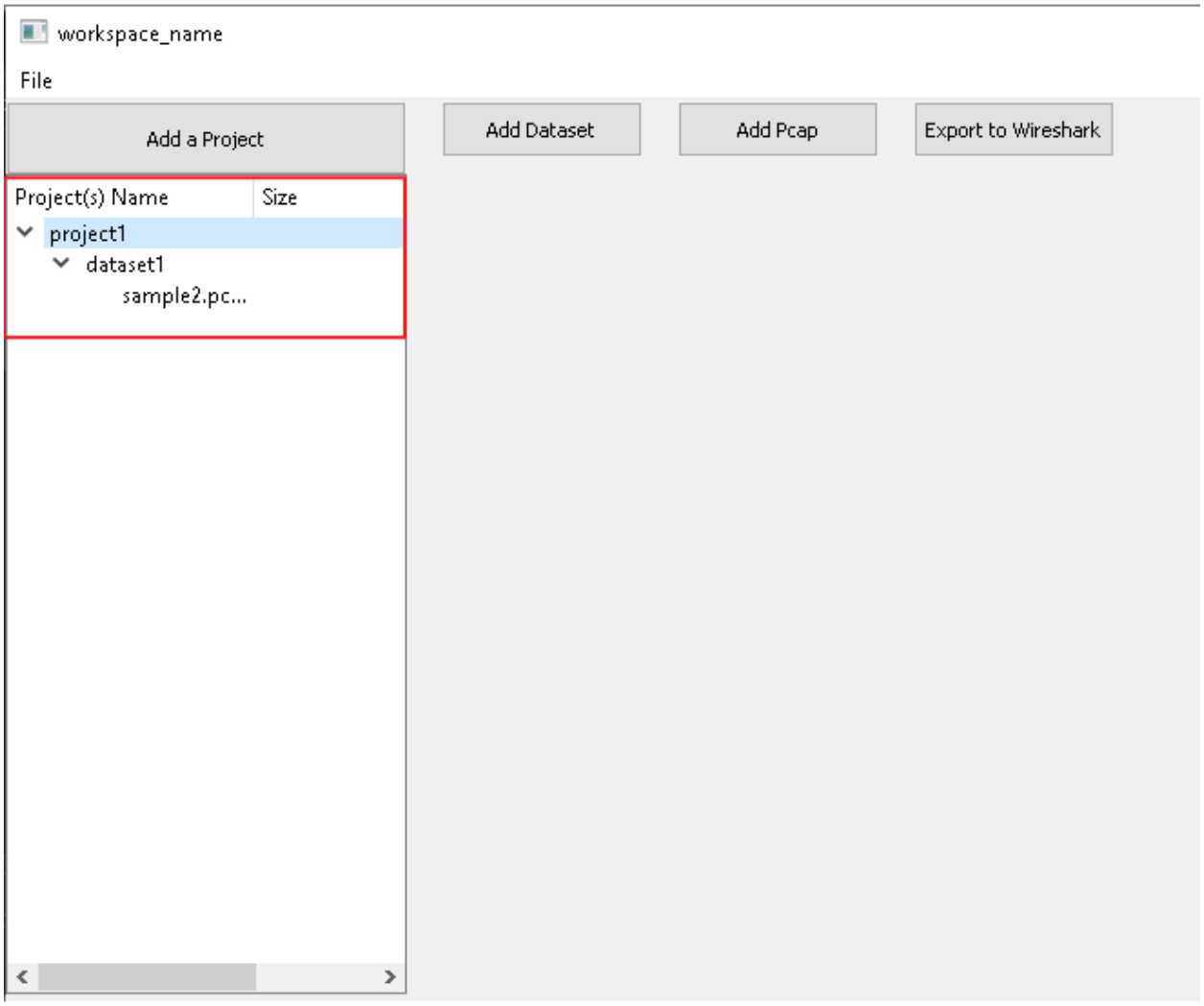




A key difference in this procedure is upon naming the dataset the user will be prompted to select a PCAP file to add to the dataset. Note a user cannot create an empty dataset, every dataset must have at least one PCAP file.



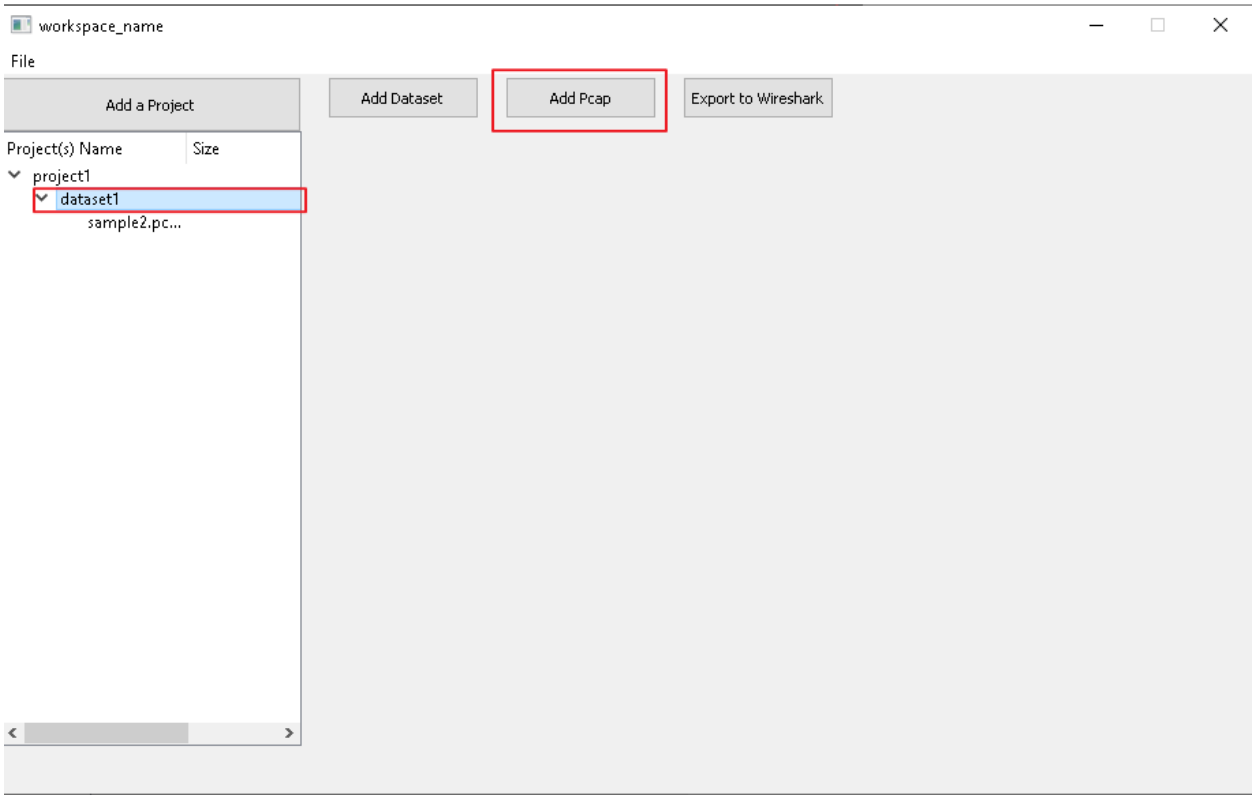
Upon successfully creating the Dataset, the user will see a dropdown under the project that contains the dataset and the pcap file added. As shown below:



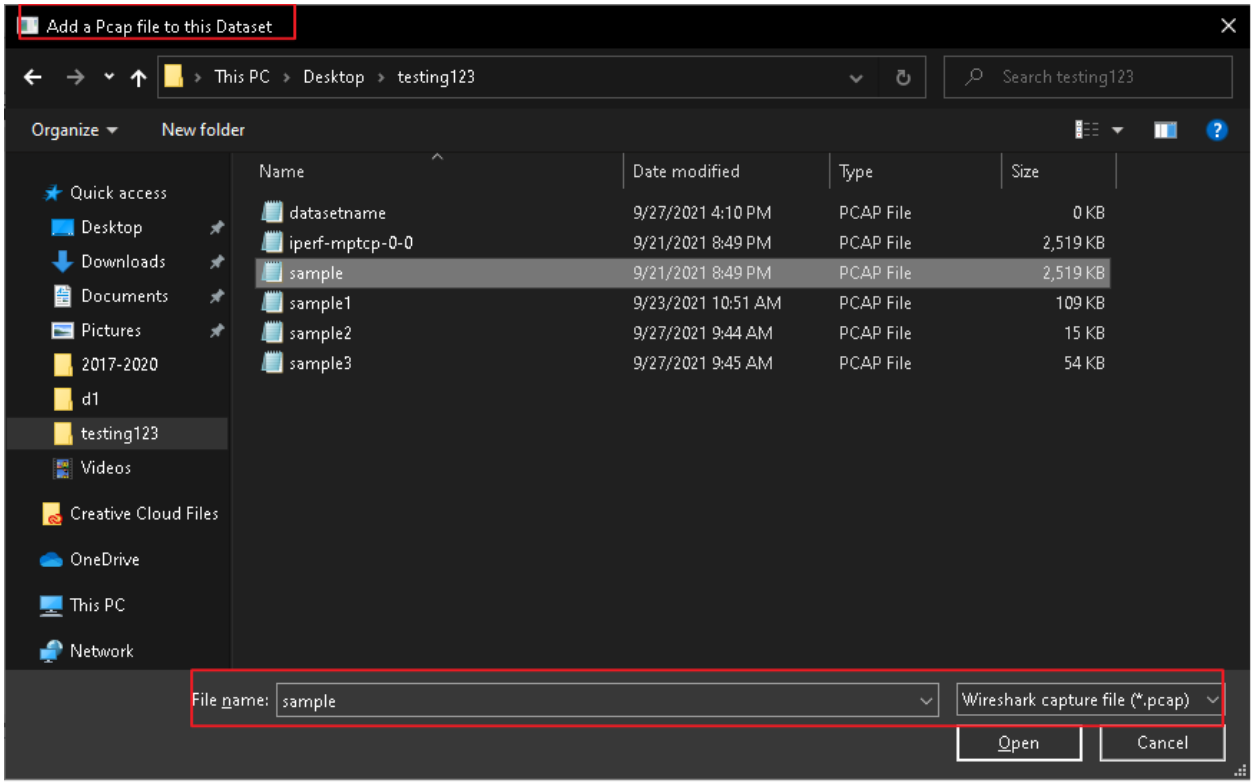
Note in the first iteration of the system, there is no way to view the data as requested, this is an expected feature for future release.

2.5 Add Individual PCAP

Once a Dataset has been successfully added to a project the user will have the ability to add PCAP files to the dataset at any time. The user must first select the dataset in the left pane, then select the “Add Pcap” button as shown below :



The user will then be prompted to select a PCAP file to add to the dataset:

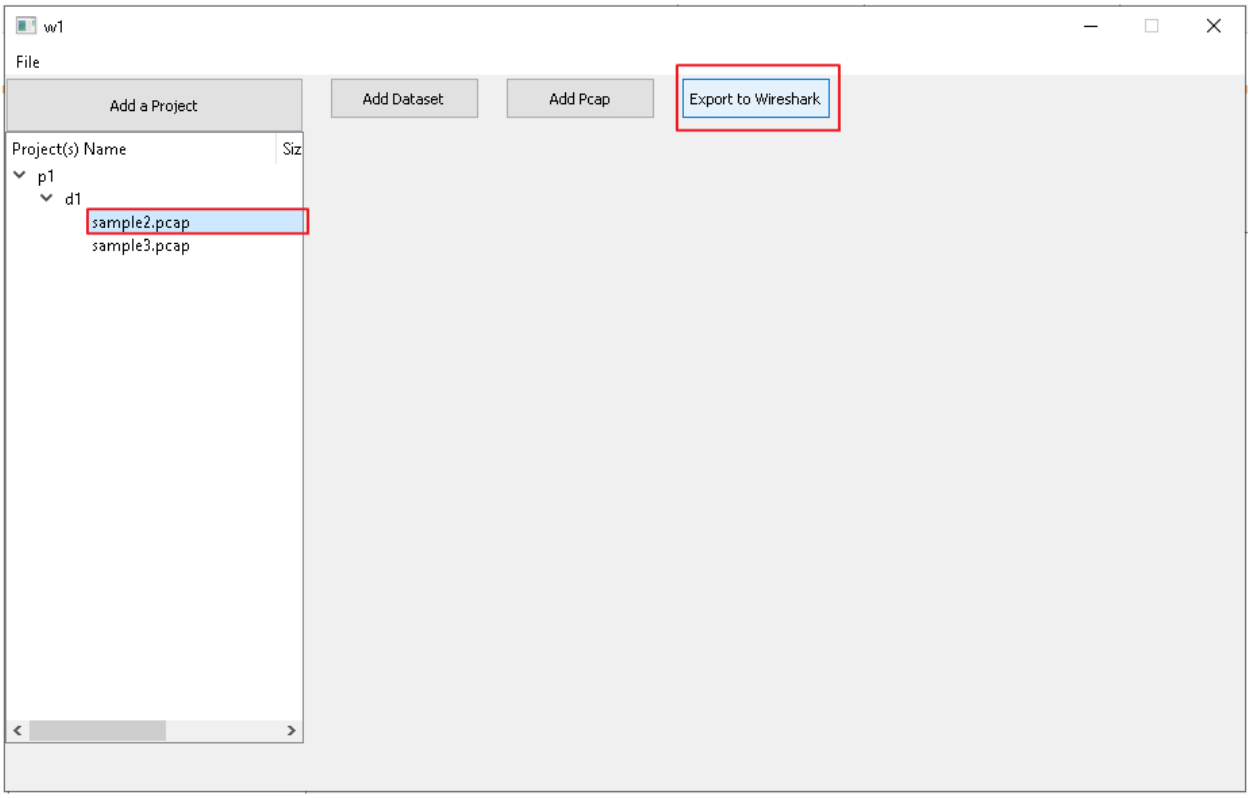


2.6 Export to Wireshark

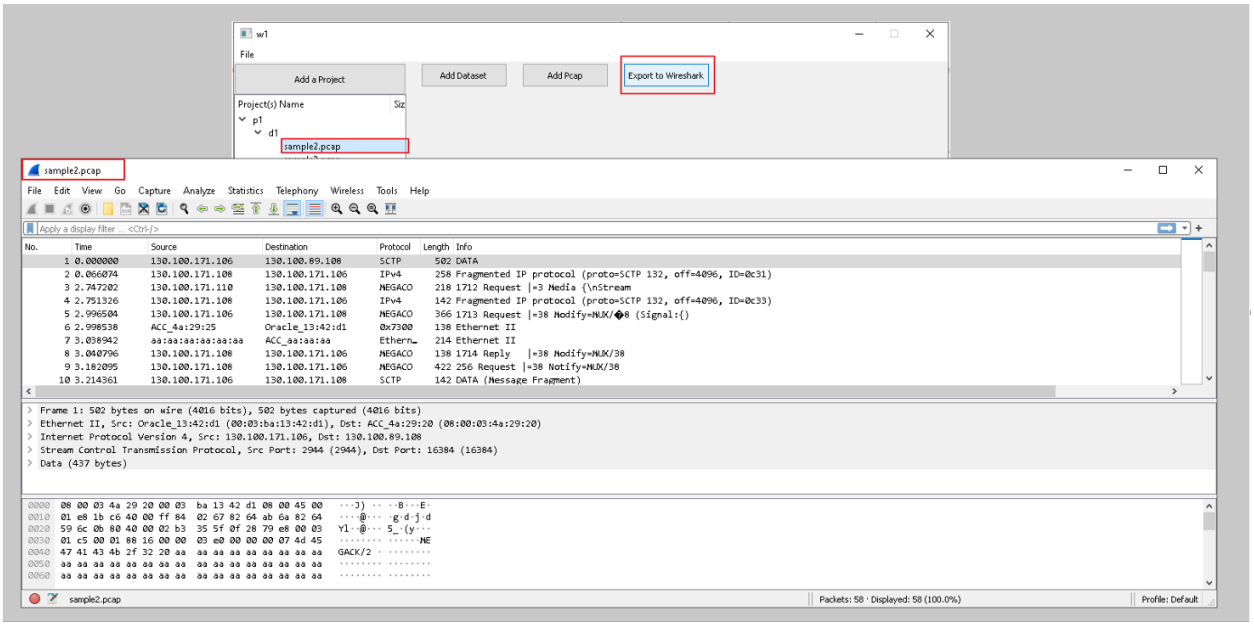
Once a Dataset is successfully added the user will have the ability to export the packet data to Wireshark. The user has the following two options:

Export an Individual Pcap file to wireshark:

The user can select a specific PCAP file in a dataset and press the “Export to Wireshark” button in order to view the pcap in wireshark.

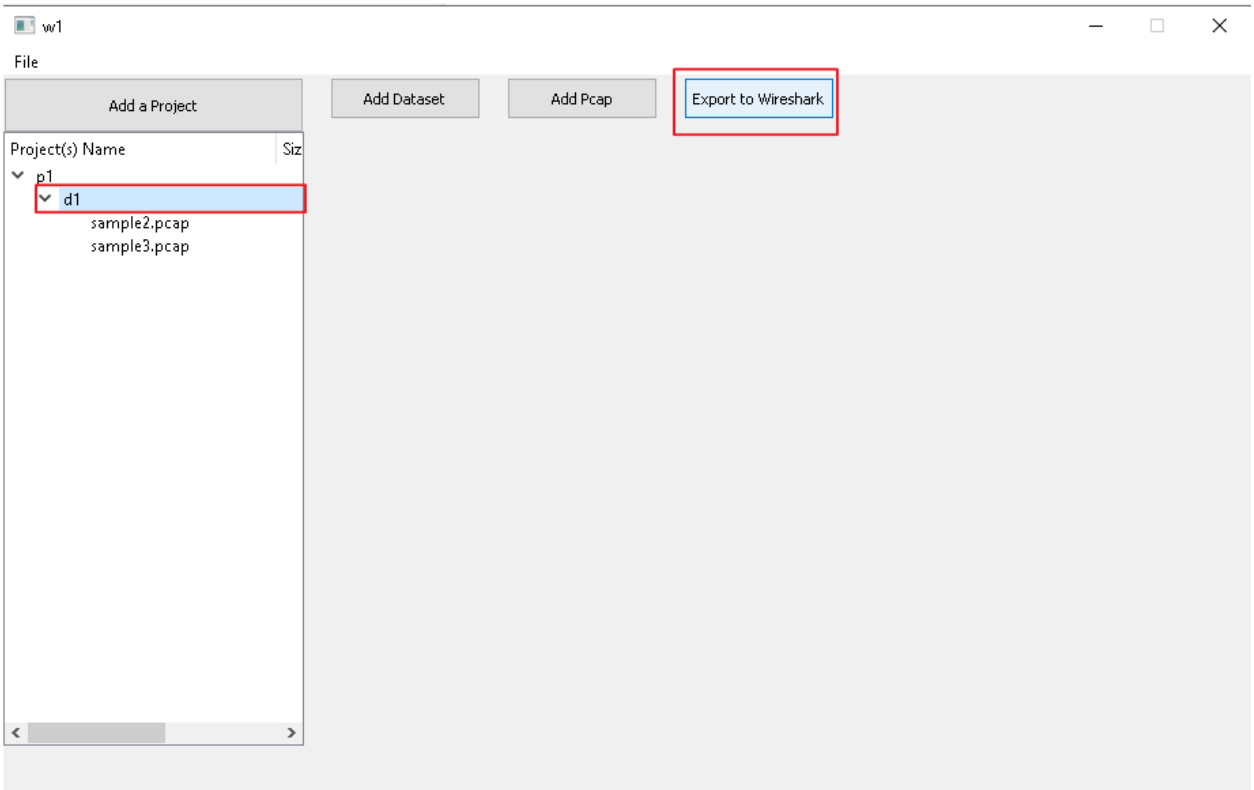


The system will then automatically open wireshark and display the packets of the selected pcap:



Export Dataset to Wireshark

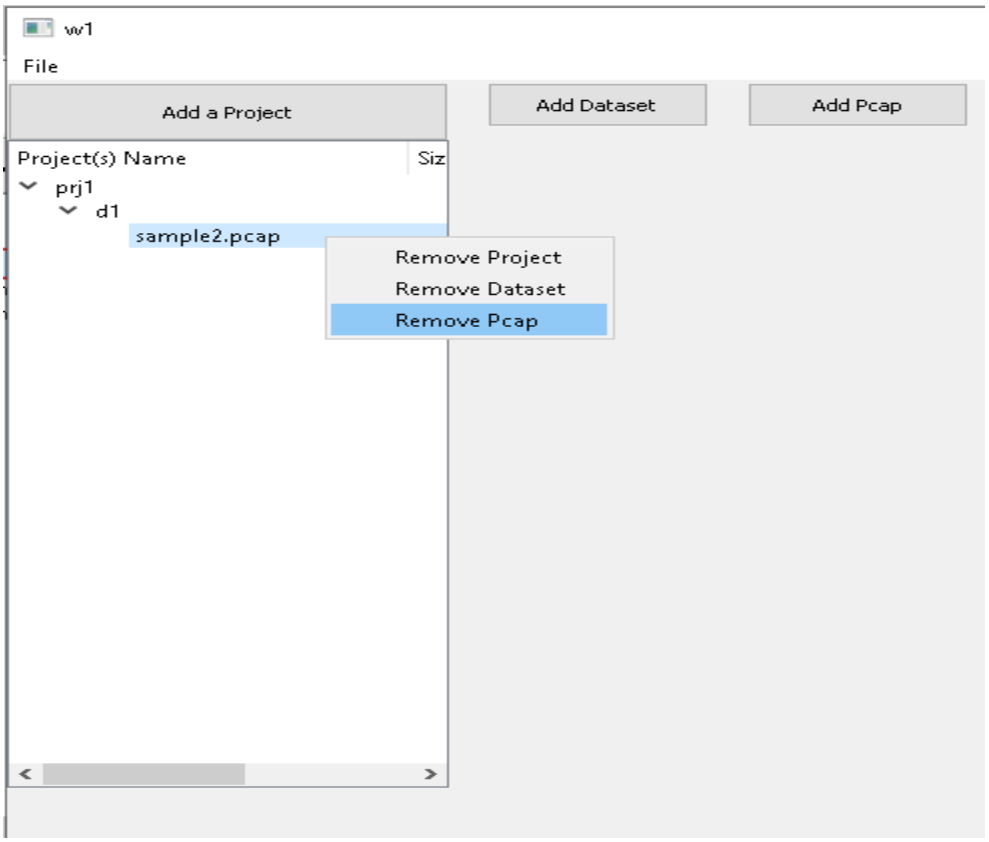
The user can also select the Dataset and select Export to Wireshark as shown below:



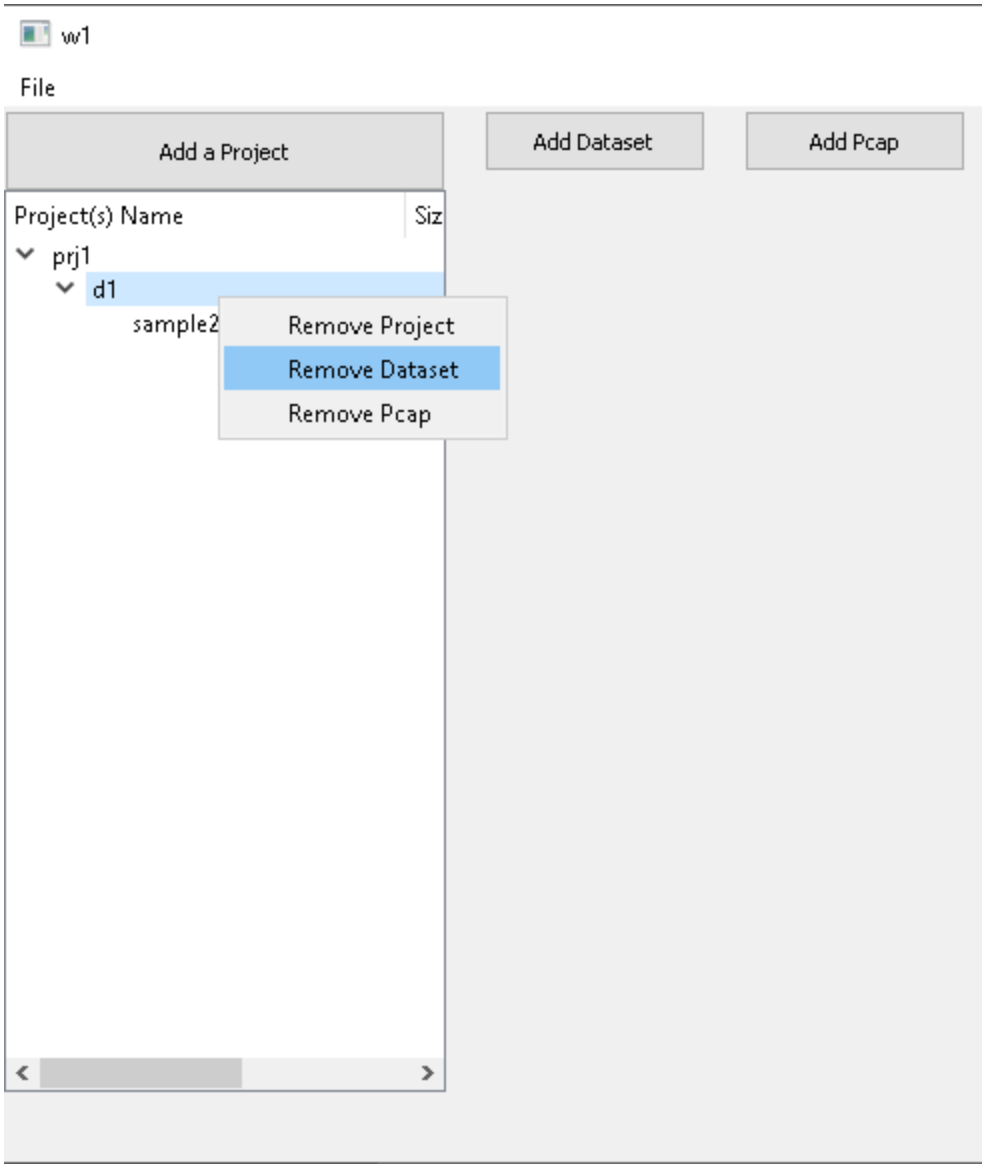
The will take ALL packets from the PCAP files present in the Dataset and export them to wireshark in the same manner as shown above.

2.7 Remove Pcap, Dataset, and Projects

At any point, a user can remove a Project, Dataset, and PCAP from the workspace. The user must select the item from the left pane and right click. A new popup window will the appear and provide options as follows:

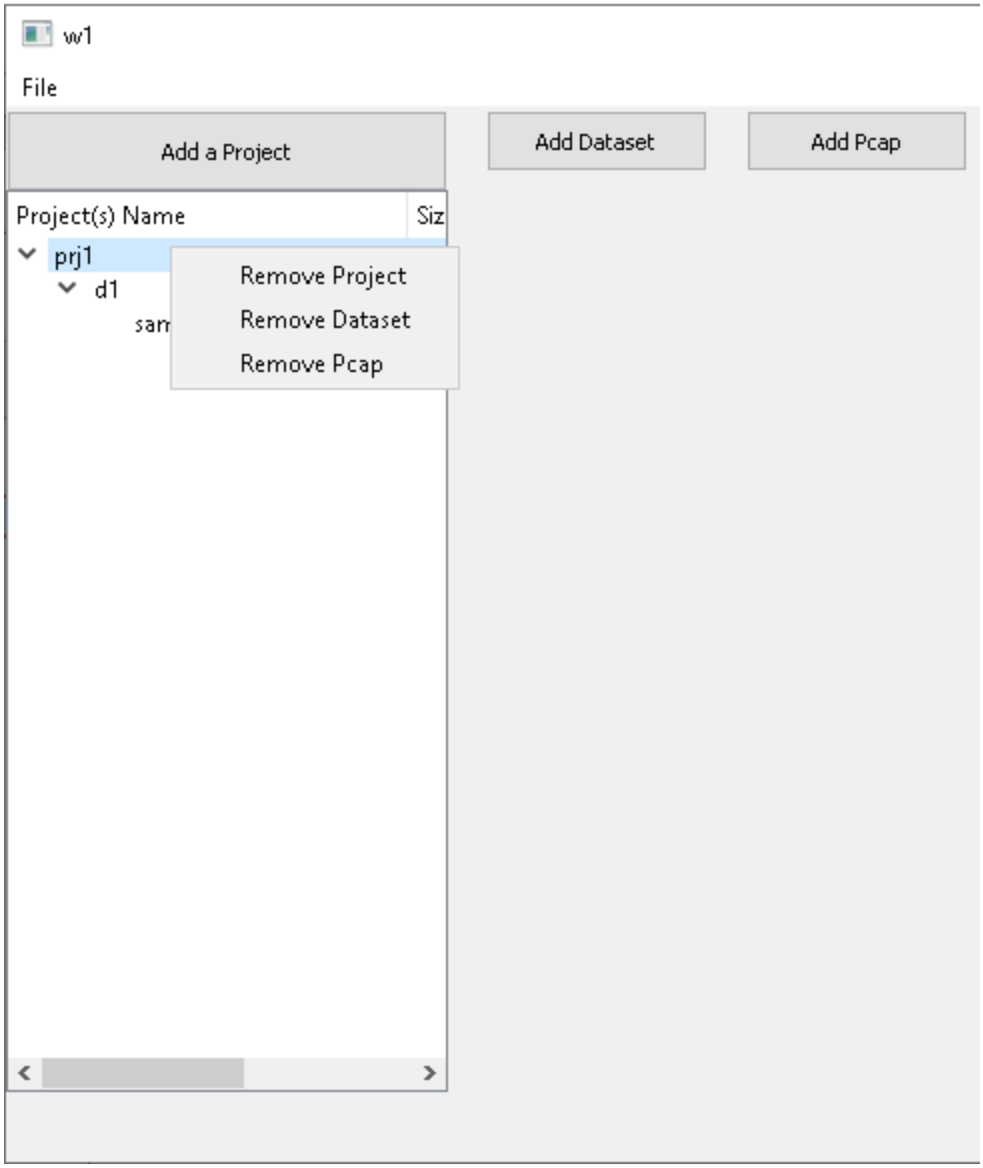


Remove PCAP



Delete Dataset

Deleting a Dataset will also delete all of the PCAPs that are contained in the Dataset.

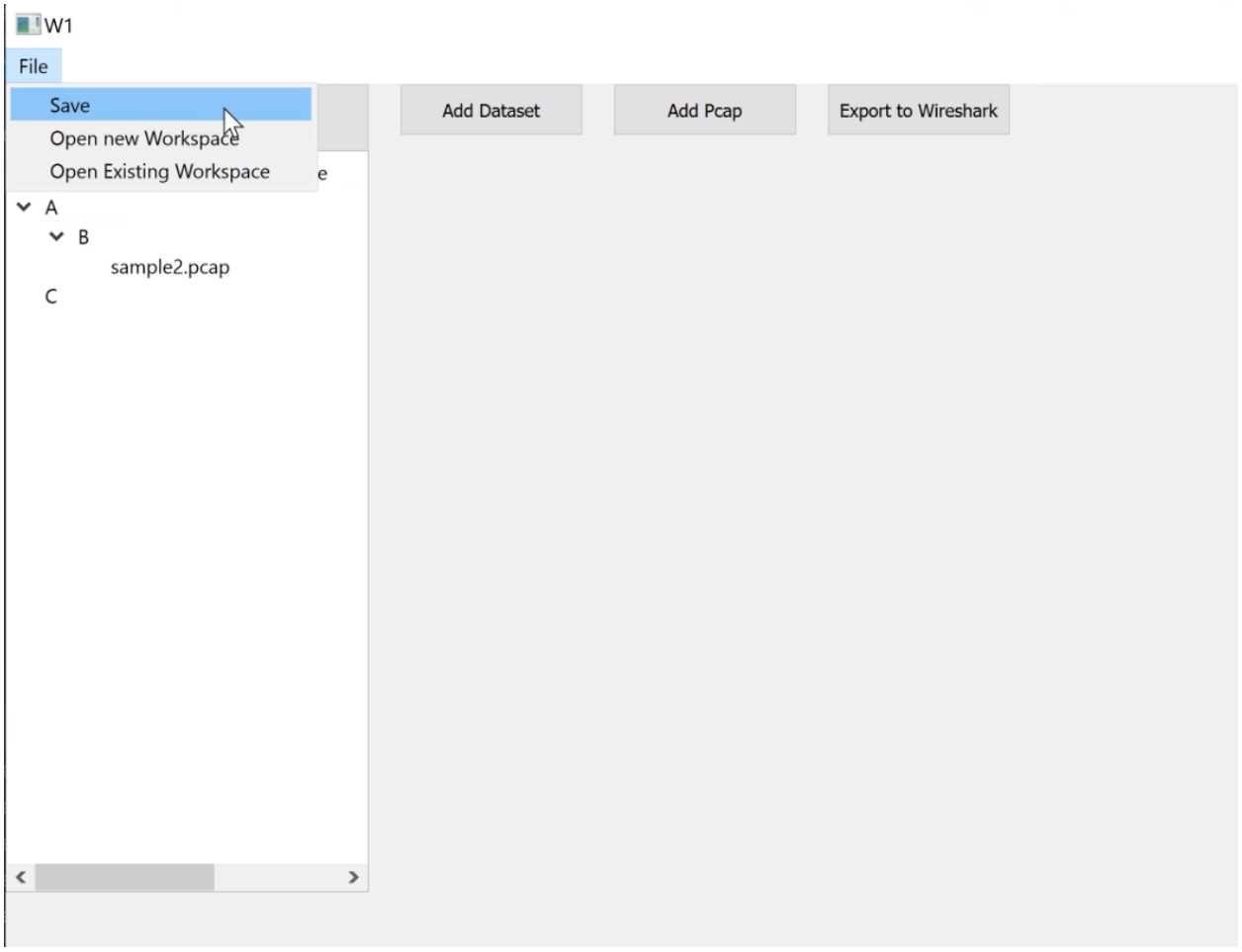


Delete Project

Deleting a project will also delete any of the Datasets present in the Project

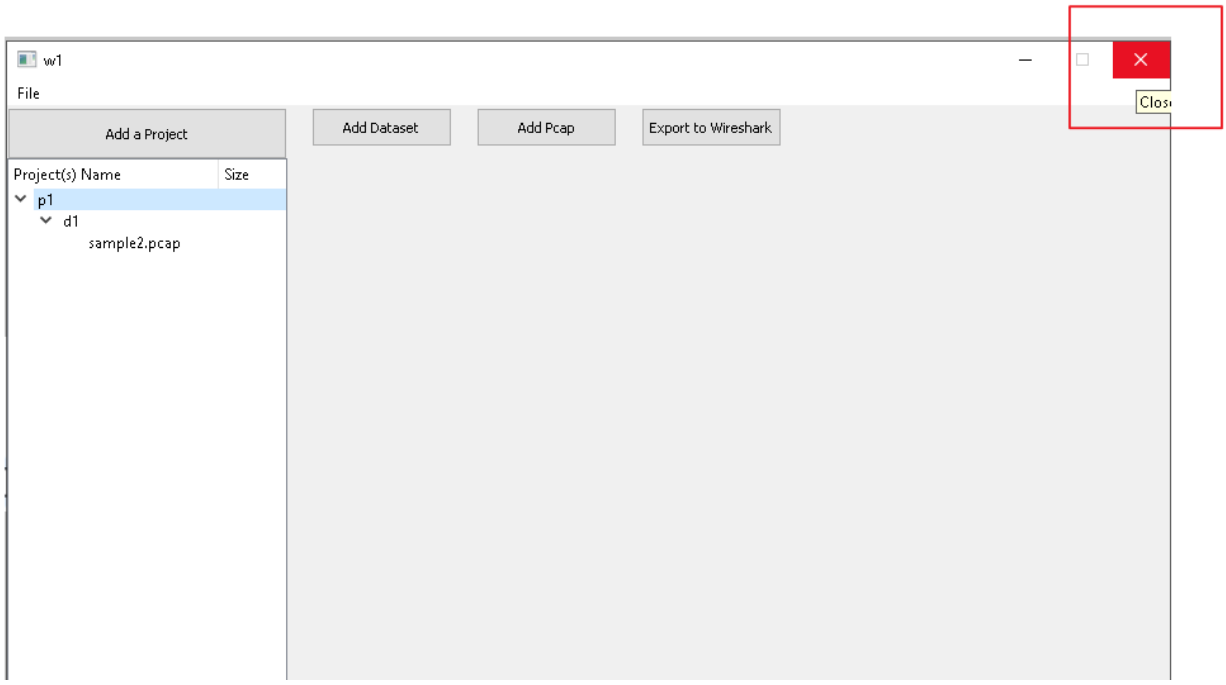
2.8 Save

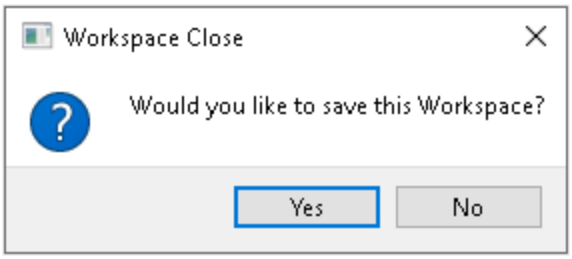
The user can choose to save any workspace that they have created. The system will automatically create a ZIP folder with the Workspace name and save it in the the directory that the user originally chose to create the workspace in as shown below:



Note: All information: including Projects, Datasets, and PCAP files will be exported and available for relaunch should the user choose to import the ZIP (See 2.9)

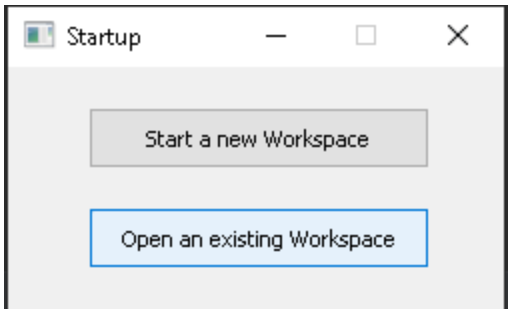
Should the user choose to close the workspace unexpectedly the system will prompt the user to save the workspace, as shown below:



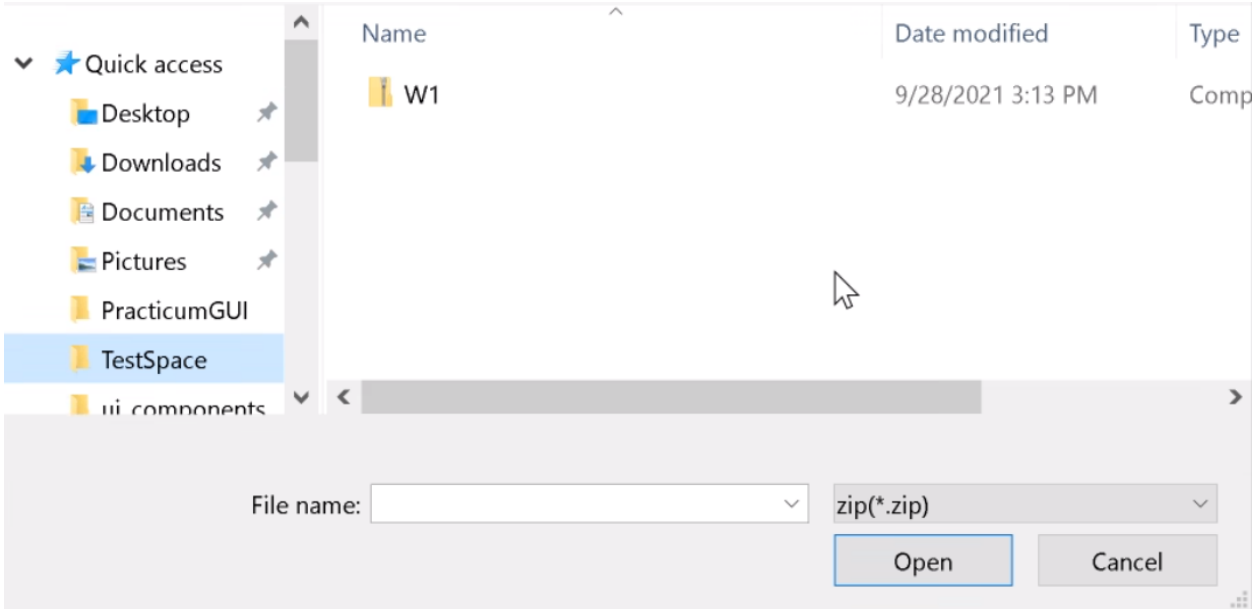


2.9 Reopening an Existing Workspace

There is also an option for a user to load in an existing workspace.



The expected input is a ZIP file that is the result of the save shown in Section 2.8. The following window appears:



Upon successfully loading the data provided from the ZIP, the user can expect the workspace interface to appear with all of the data that was previously saved

Example: