Packet Visualization

Packet Visualization System

End User Product Manual

Version 0.3

December 1, 2021

Document Control

Approval

The Guidance Team and the customers will approve this document.

Document Change Control

Initial Release	0.1
Current Release	0.3
Indicator of Last Page in Document	</3
Date of Last Review	12/1/2021
Date of Next Review	12/8/2021
Target Date for Next Update	12/8/2021

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, 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
0.2	October 12, 2021	Team	User Manual for Sprint 2, Sprint 1 Updates, New Features

0.3	December 1, 2021	Team	User Manual for Sprint 3-6 version of the System

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()

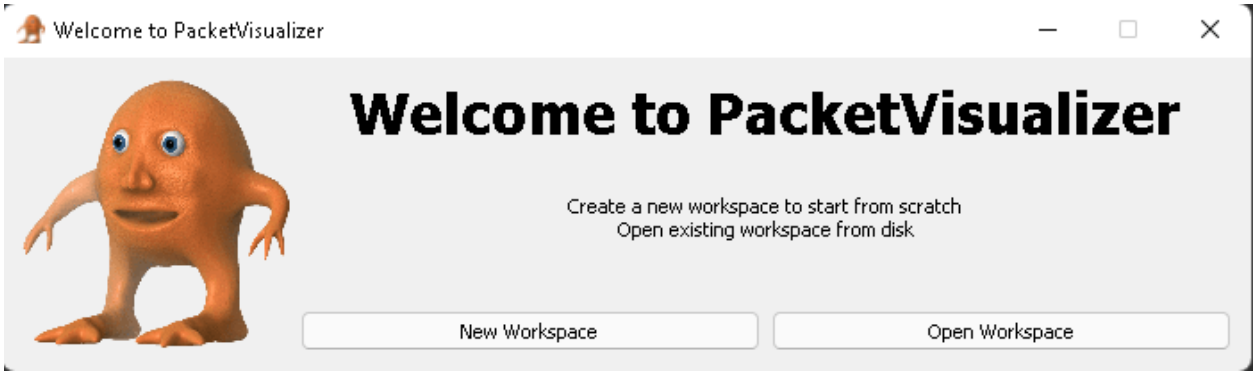
See section 2 for the system's user manual.

2. Product/User Manual

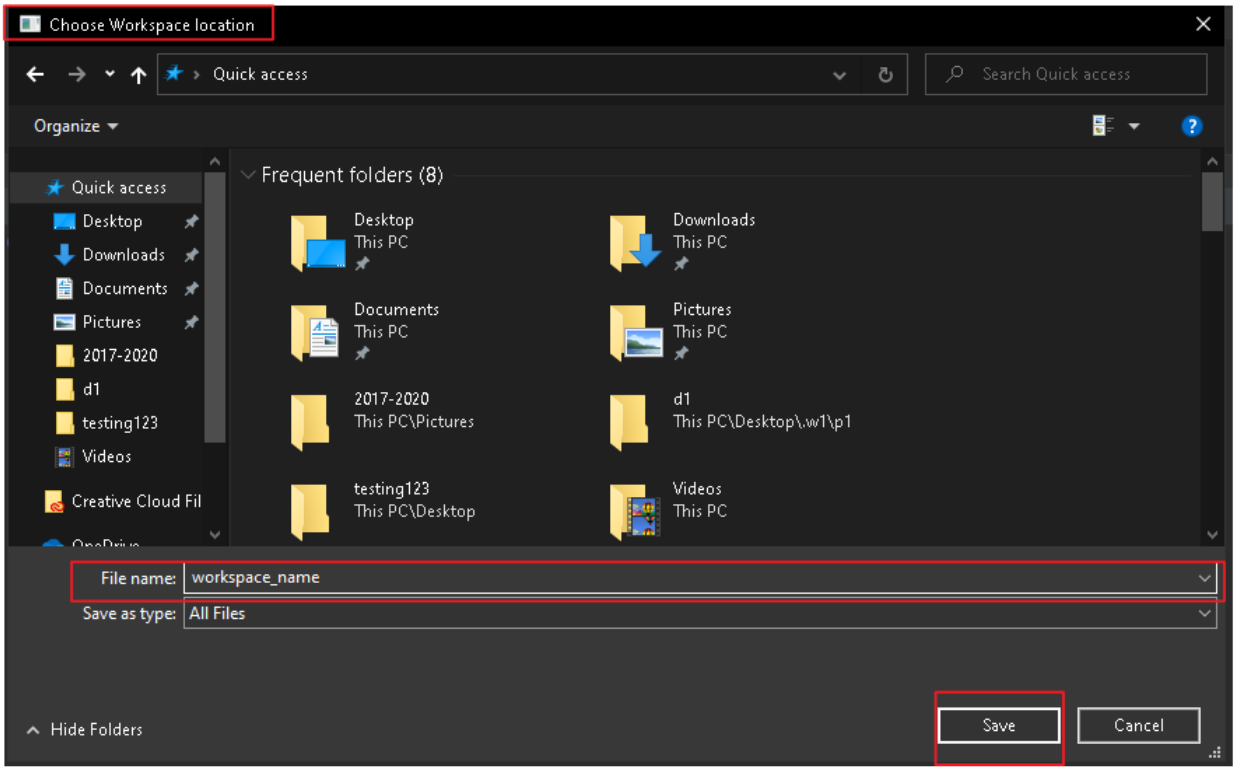
2.1. Startup

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.

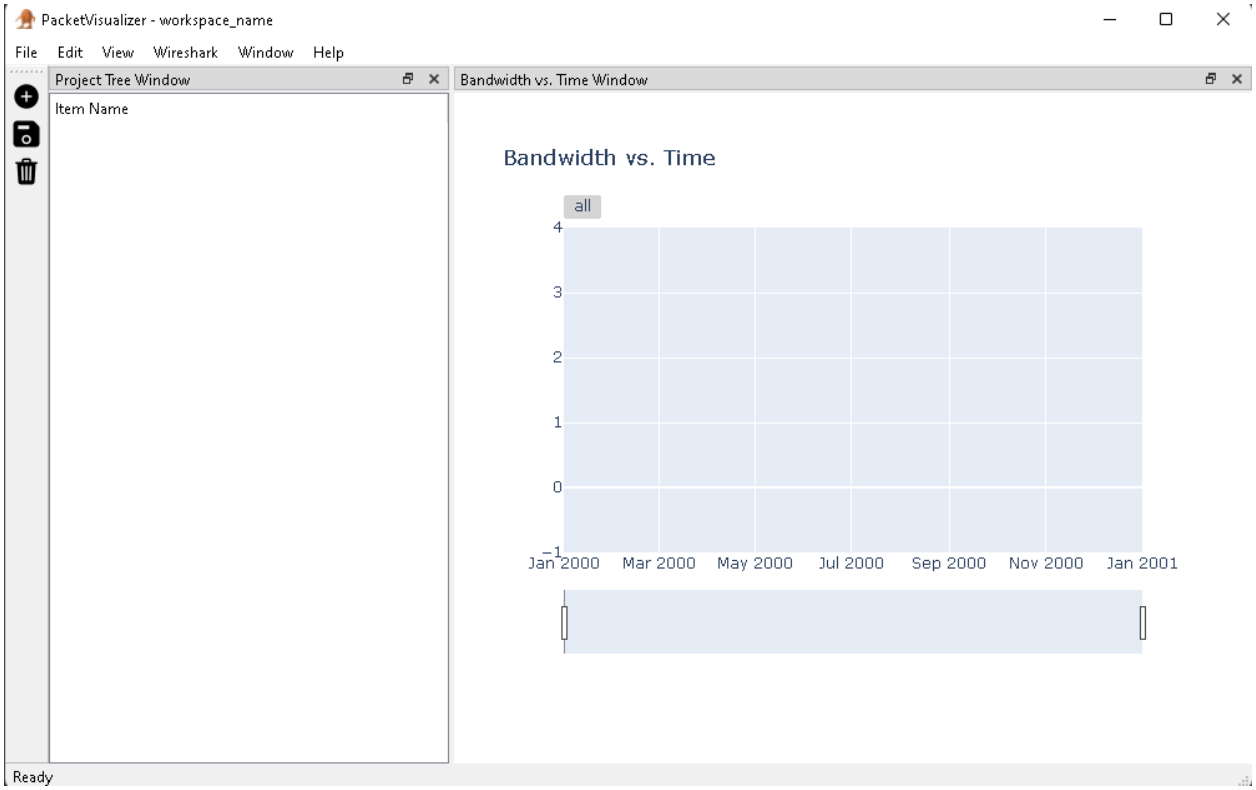


When the “Start a new Workspace” button is selected the user will be asked to assign a name for the workspace along with a save location. A directory with the workspace name will be created in the save location.



2.2 Workspace Layout

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

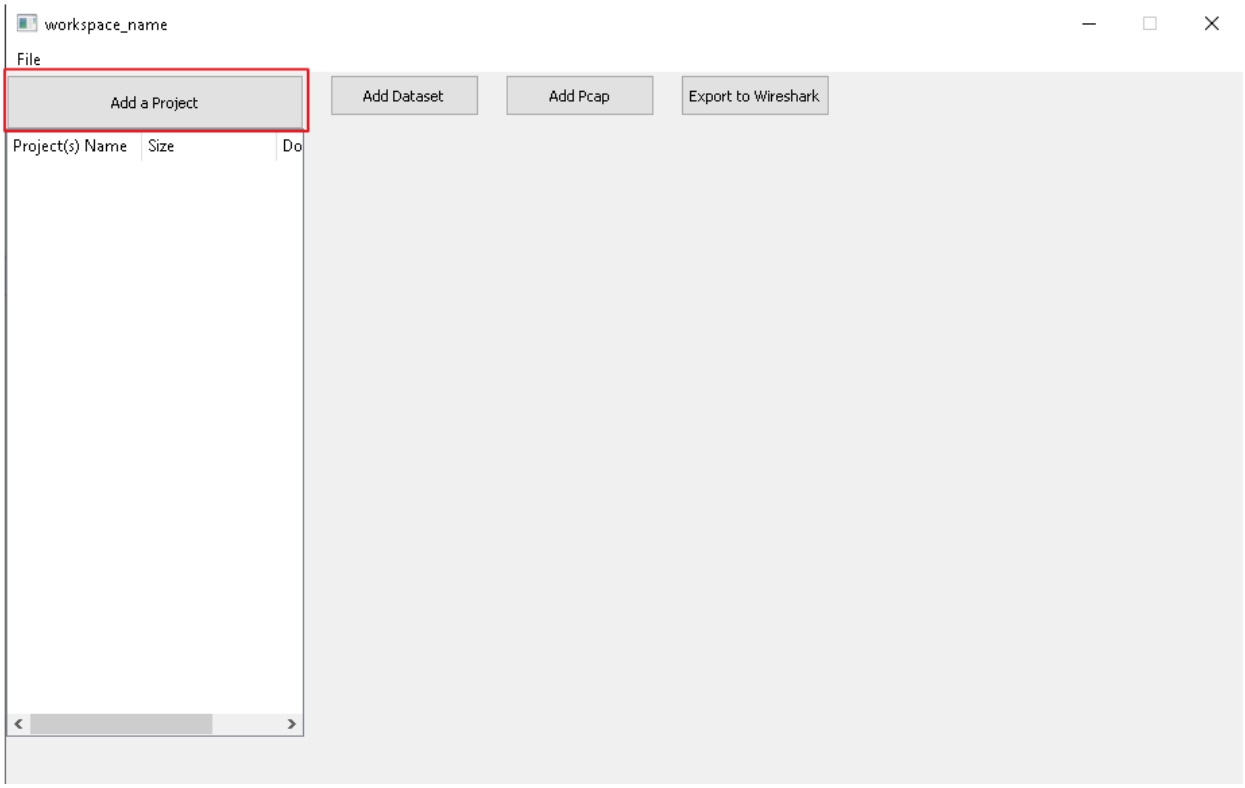


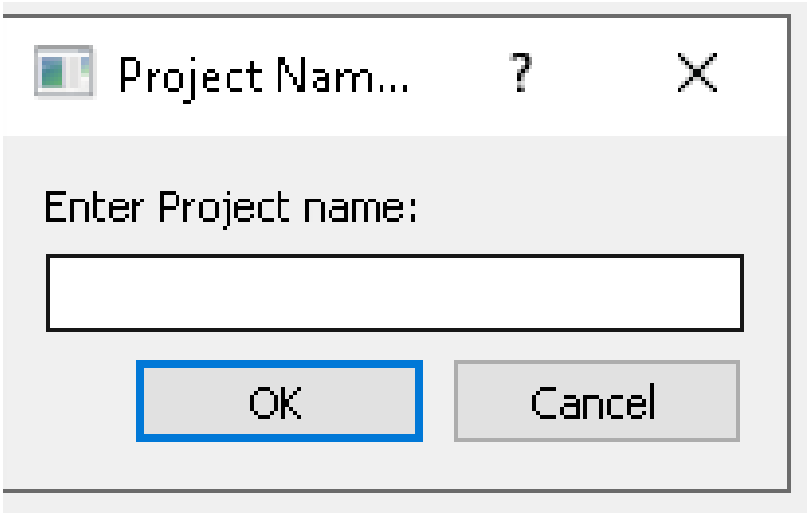
In this pane only the “Add a Project” button will have functionality. The functionality for the other 3 buttons displayed can be found in the following sections. As of version 0.1, there is no view of selected datasets however the intention will be to display this data in future versions.

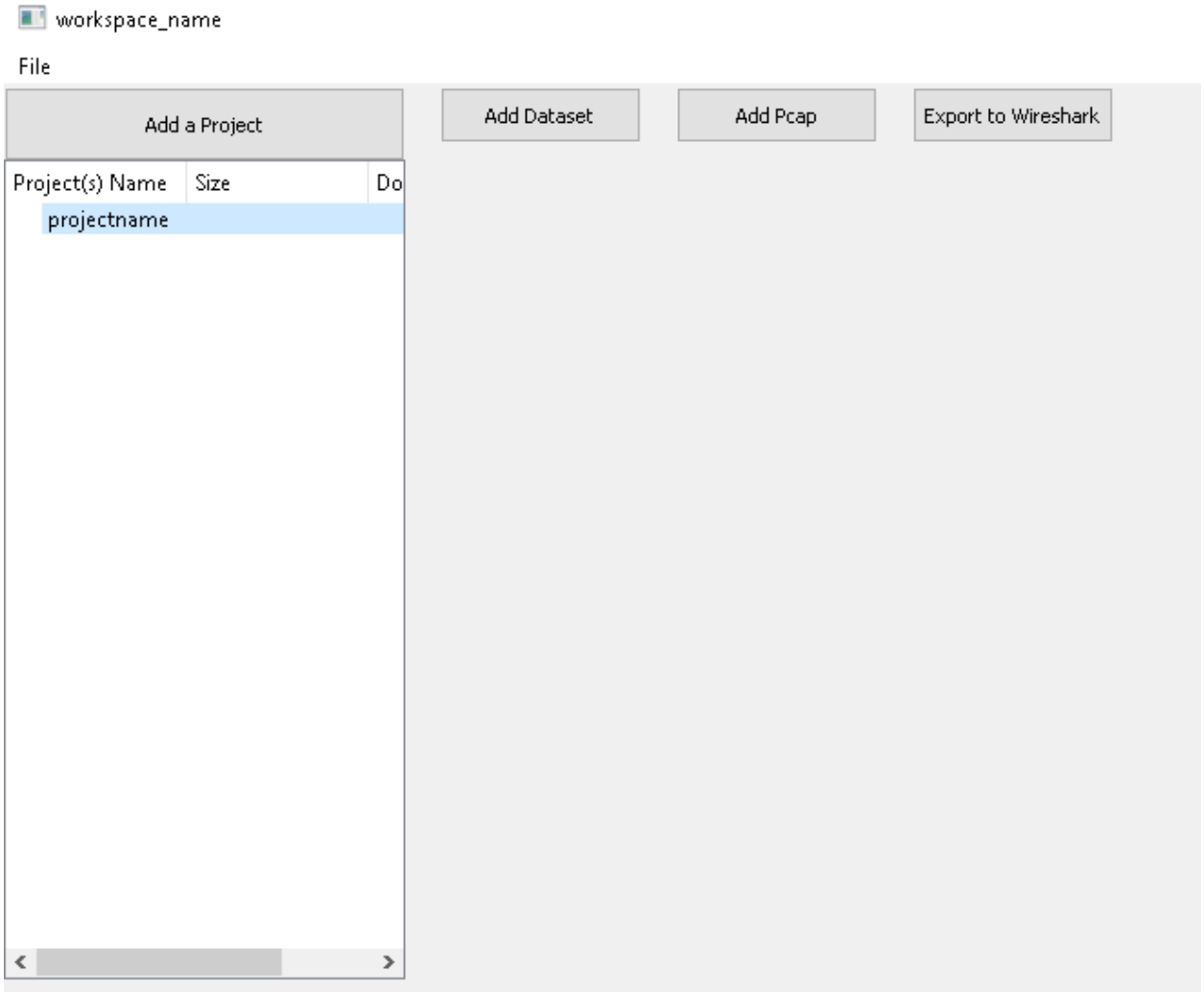
2.3 Add Project

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.

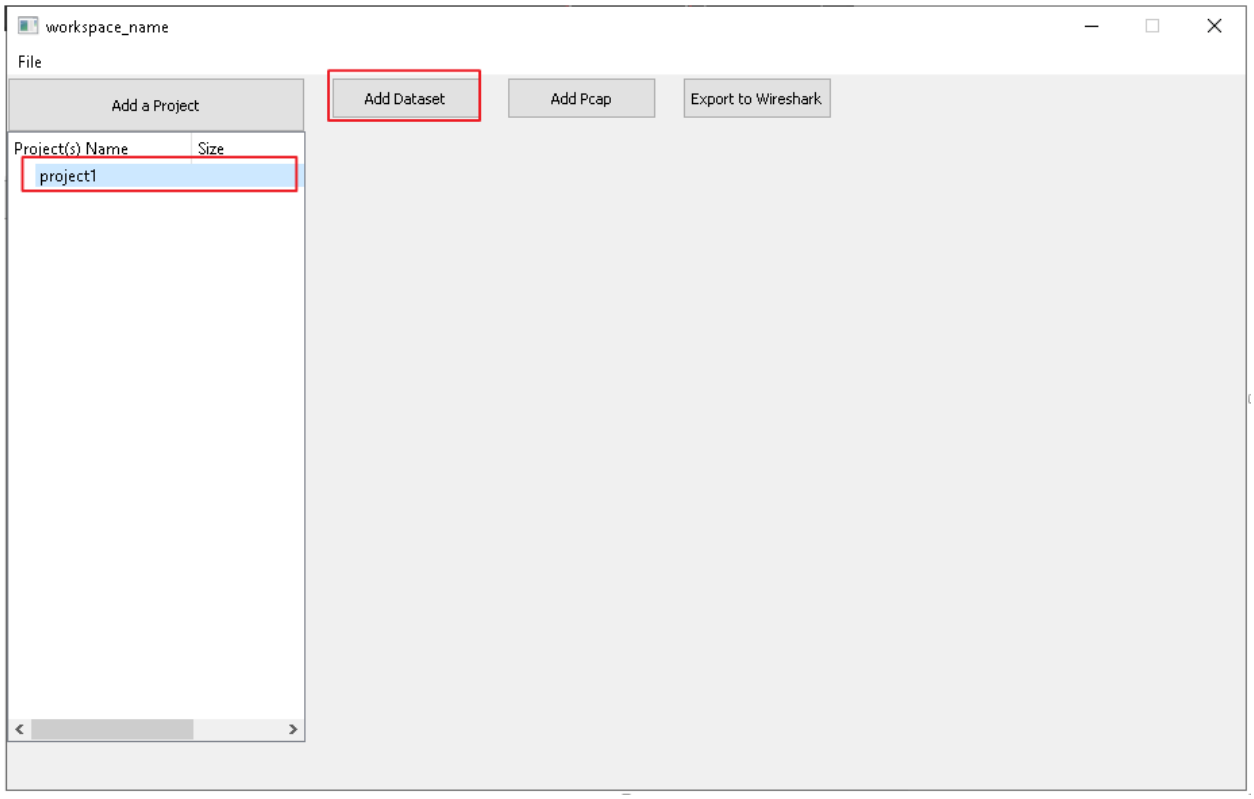

workspace_name
File
Add a Project
Add Dataset
Add Pcap
Export to Wireshark
Project(s) Name
Size
Do

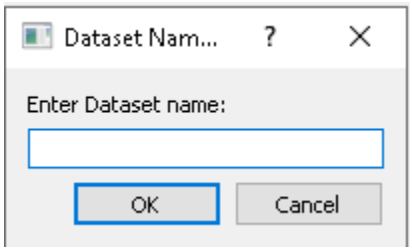

Project Nam...
Enter Project name:
OK
Cancel



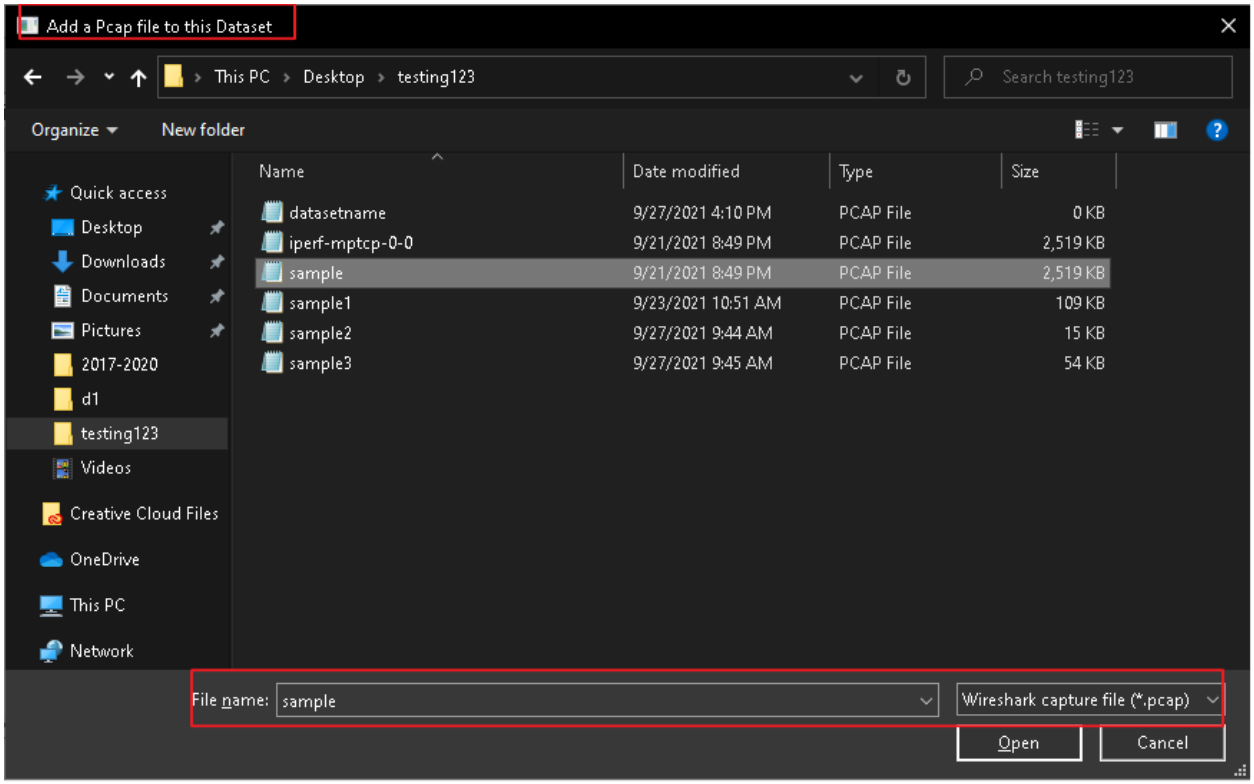
2.4 Add Dataset

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.

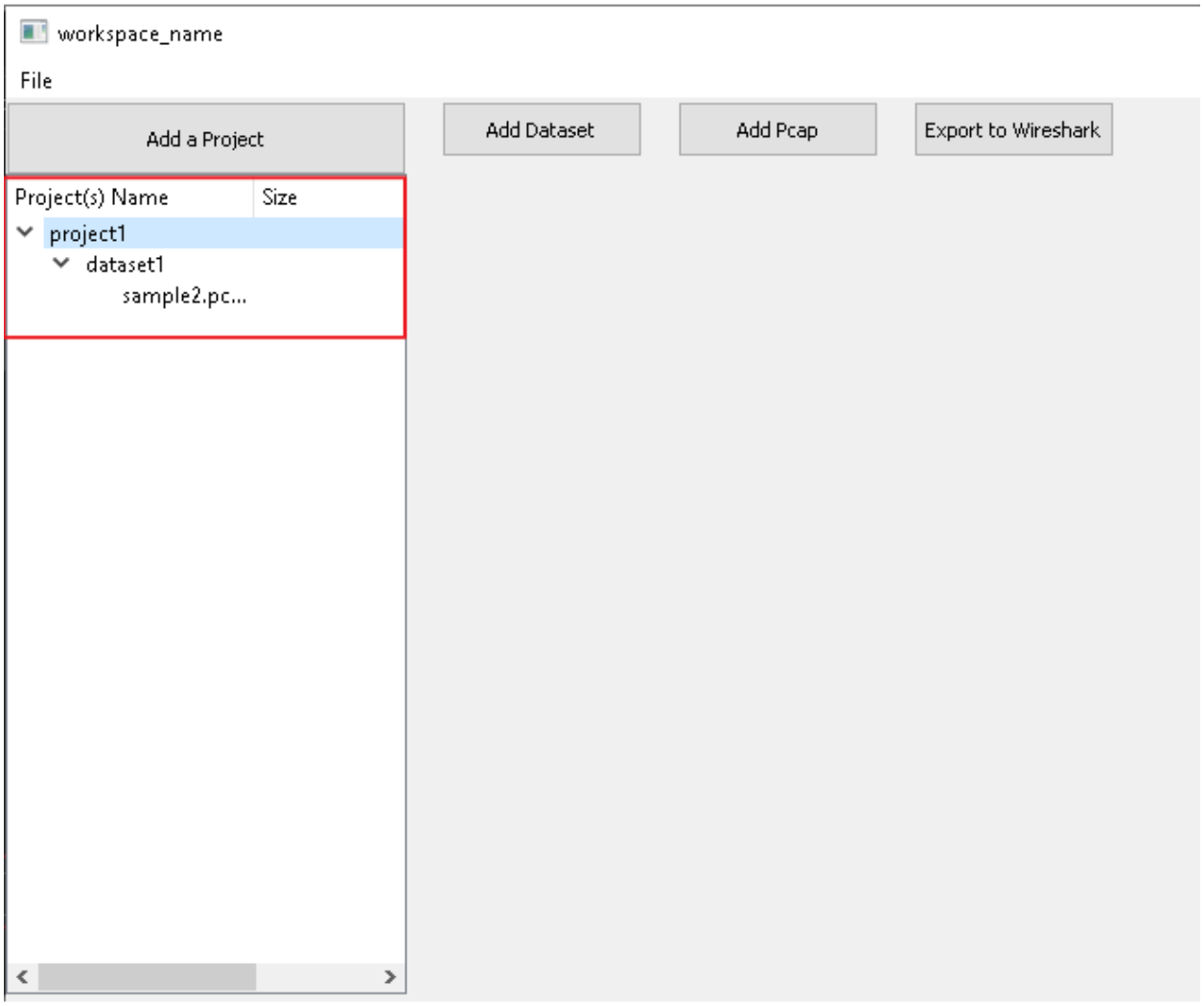




A key difference in this procedure is upon naming the dataset the user will be prompted to select a PCAP file to add to the dataset. Note a user cannot create an empty dataset, every dataset must have at least one PCAP file.



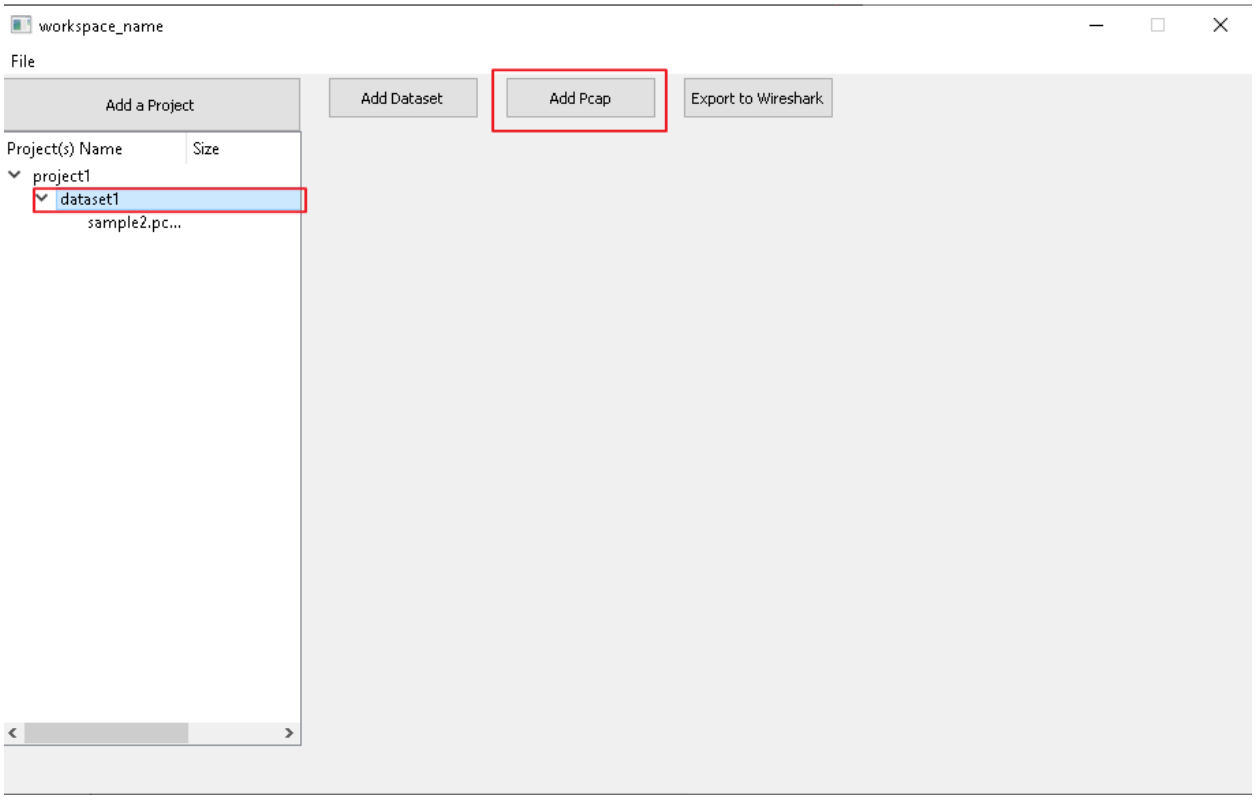
Upon successfully creating the Dataset, the user will see a dropdown under the project that contains the dataset and the pcap file added. As shown below:



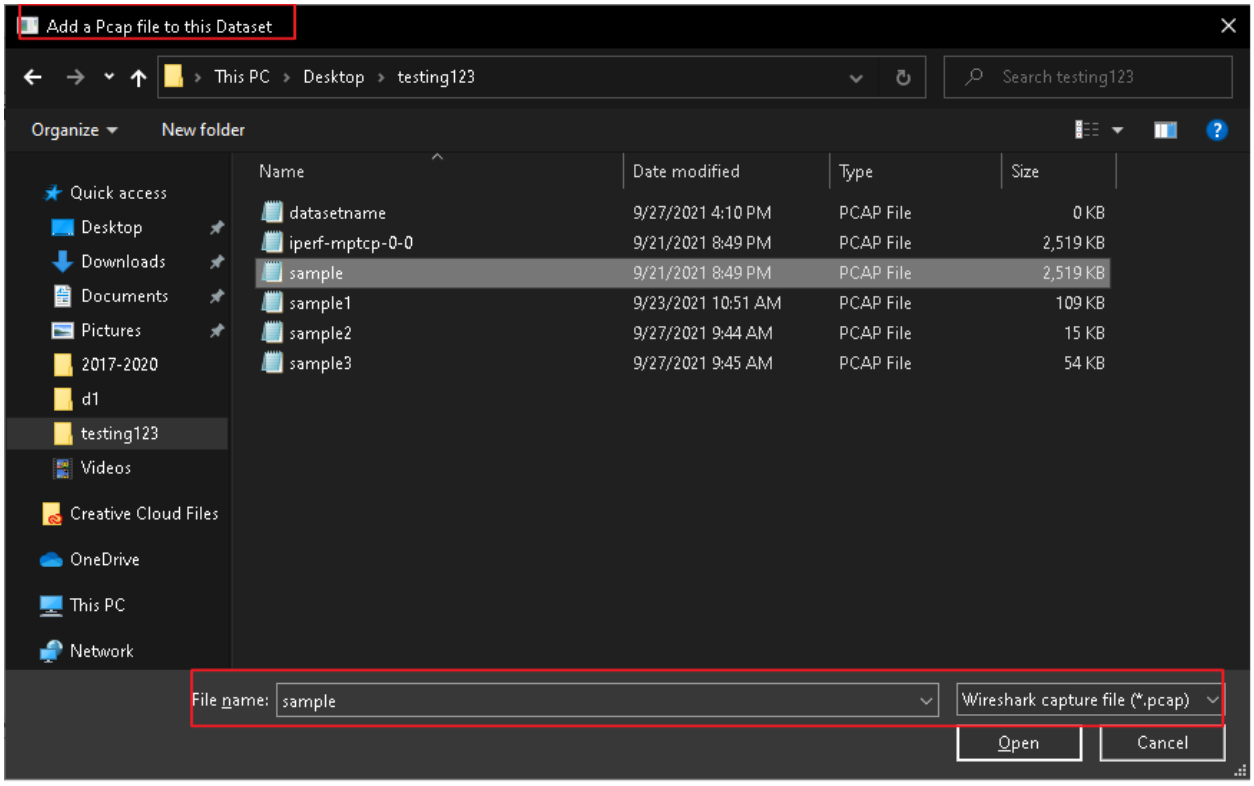
Note in the first iteration of the system, there is no way to view the data as requested, this is an expected feature for future release.

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:

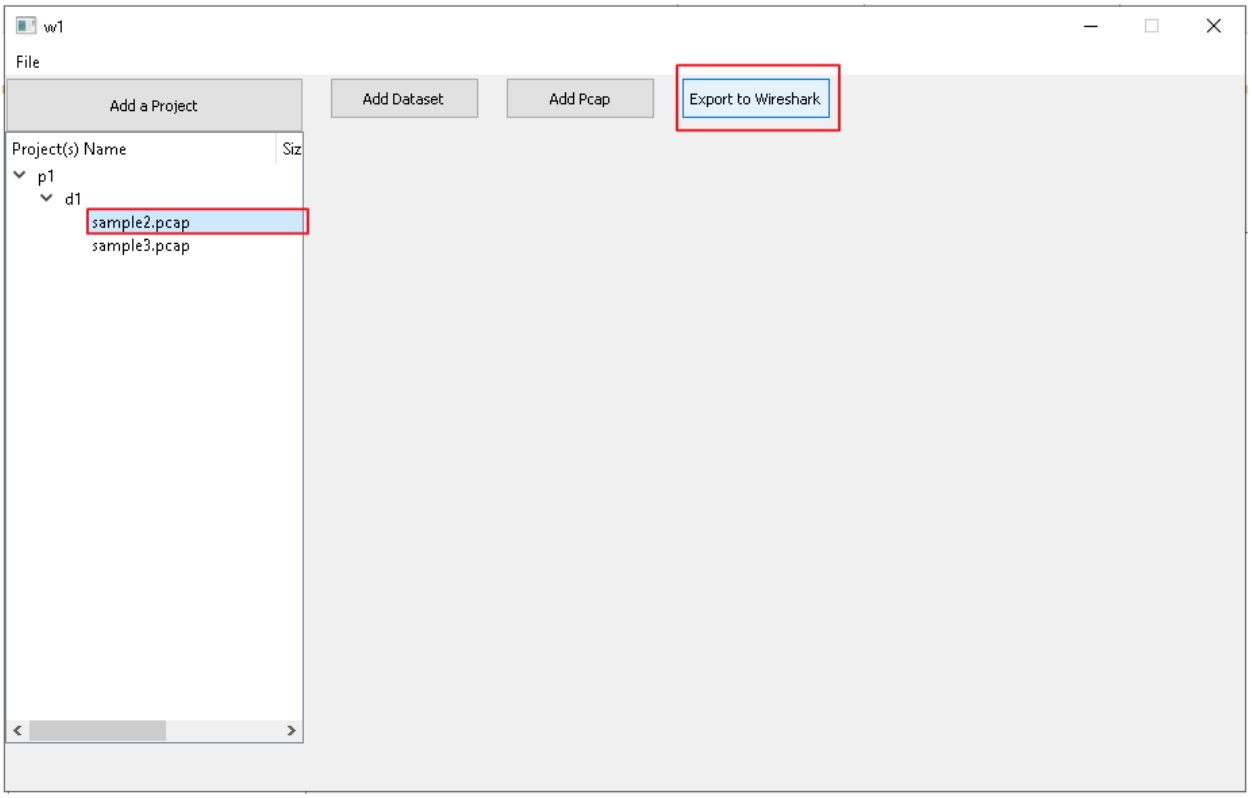


2.6 Export to Wireshark

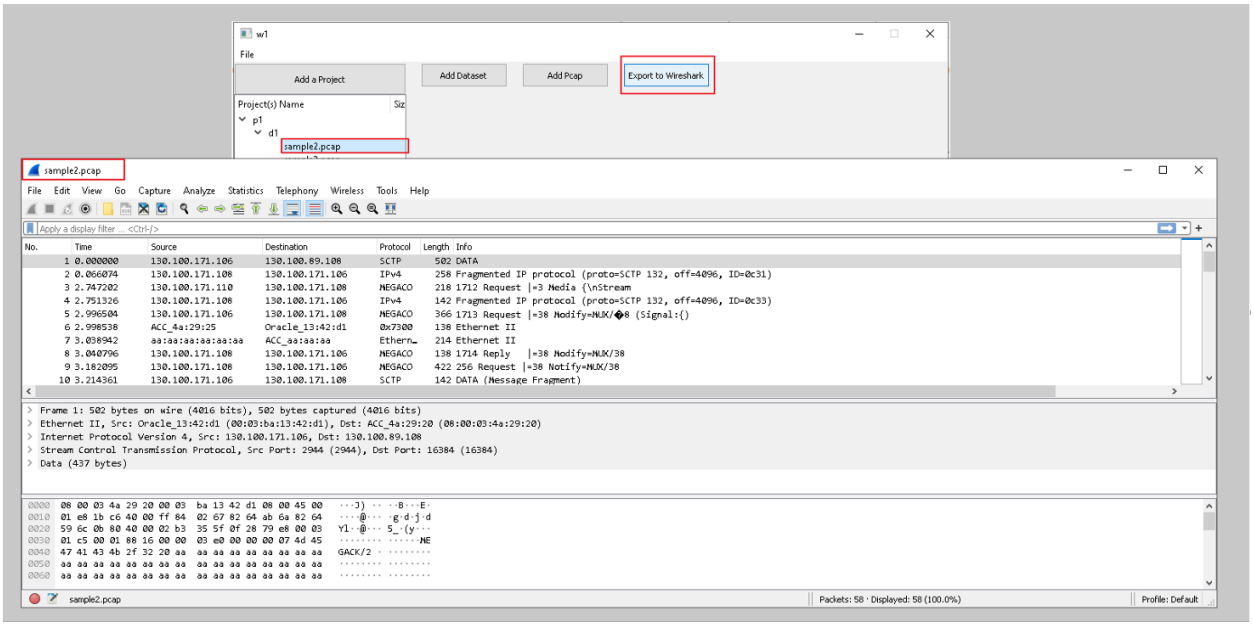
Once a Dataset is successfully added the user will have the ability to export the packet data to Wireshark. The user has the following two options:

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.

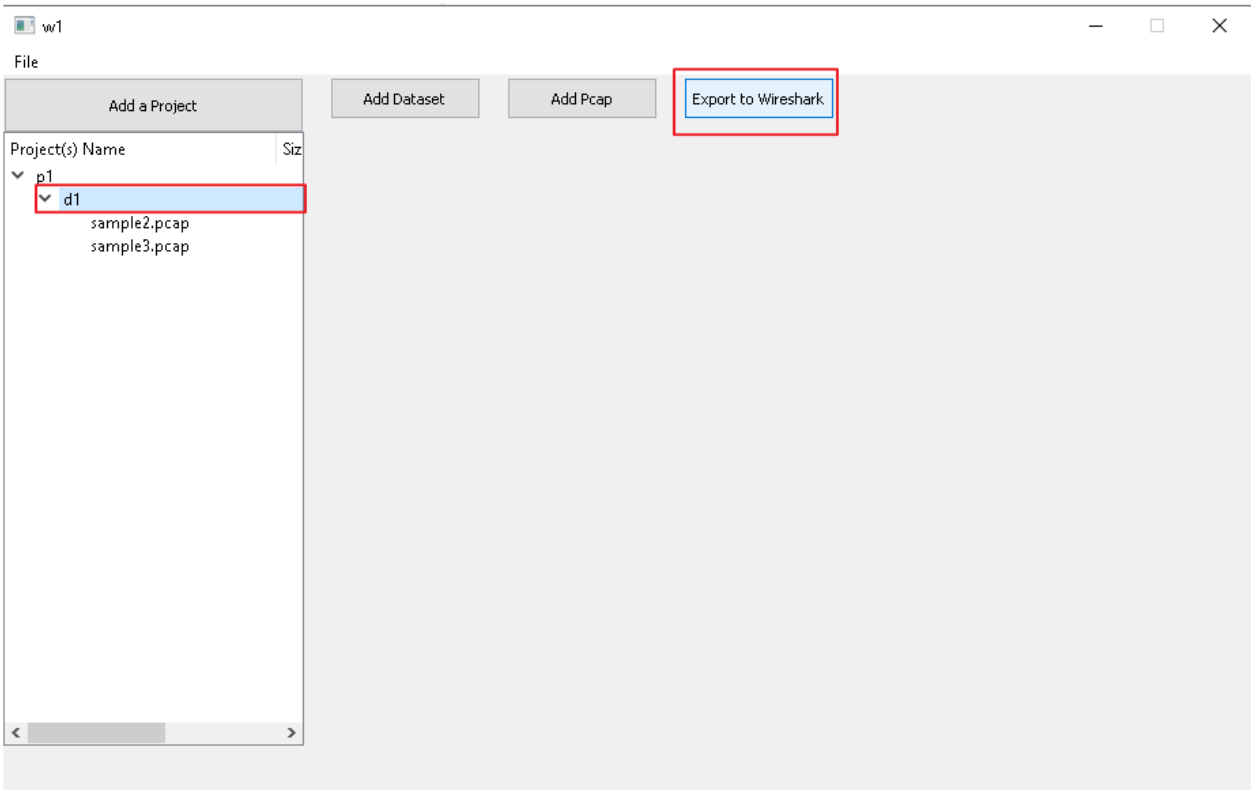


The system will then automatically open wireshark and display the packets of the selected pcap:



Export Dataset to Wireshark

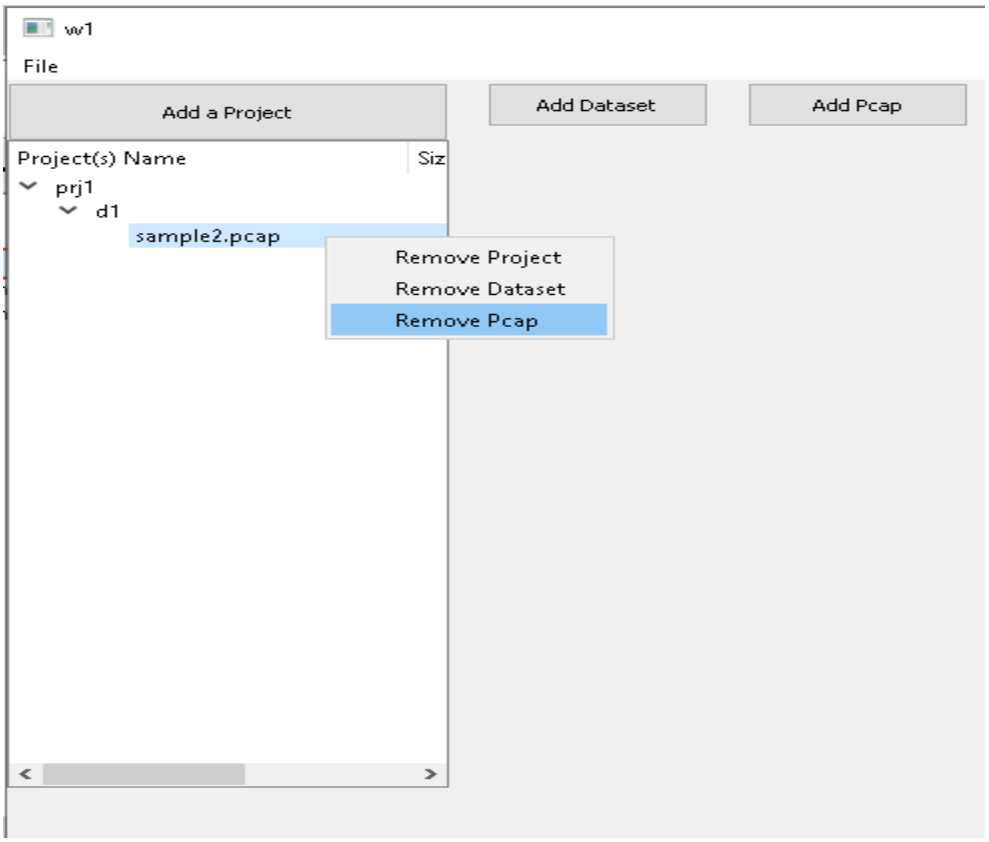
The user can also select the Dataset and select Export to Wireshark as shown below:



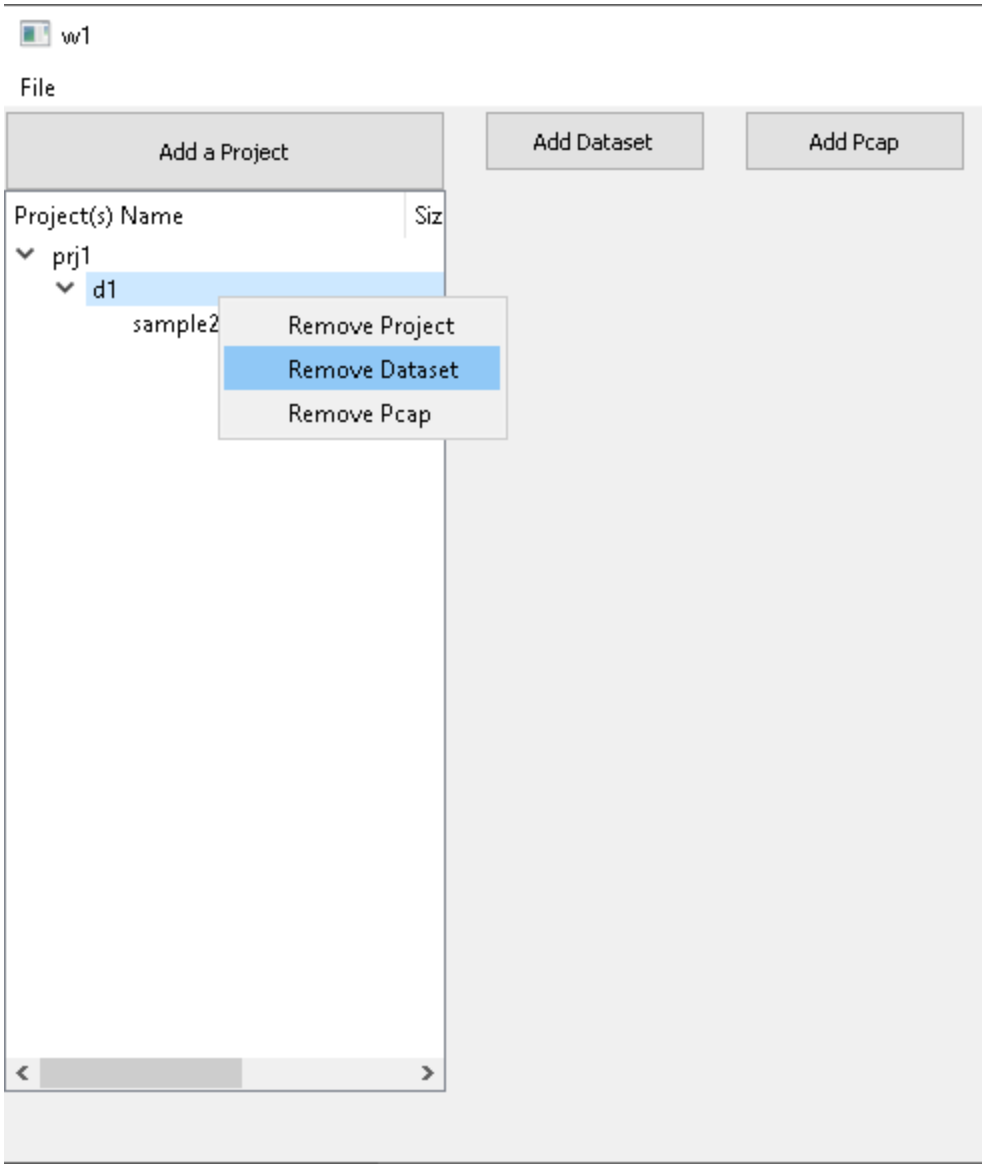
The will take ALL packets from the PCAP files present in the Dataset and export them to wireshark in the same manner as shown above.

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:

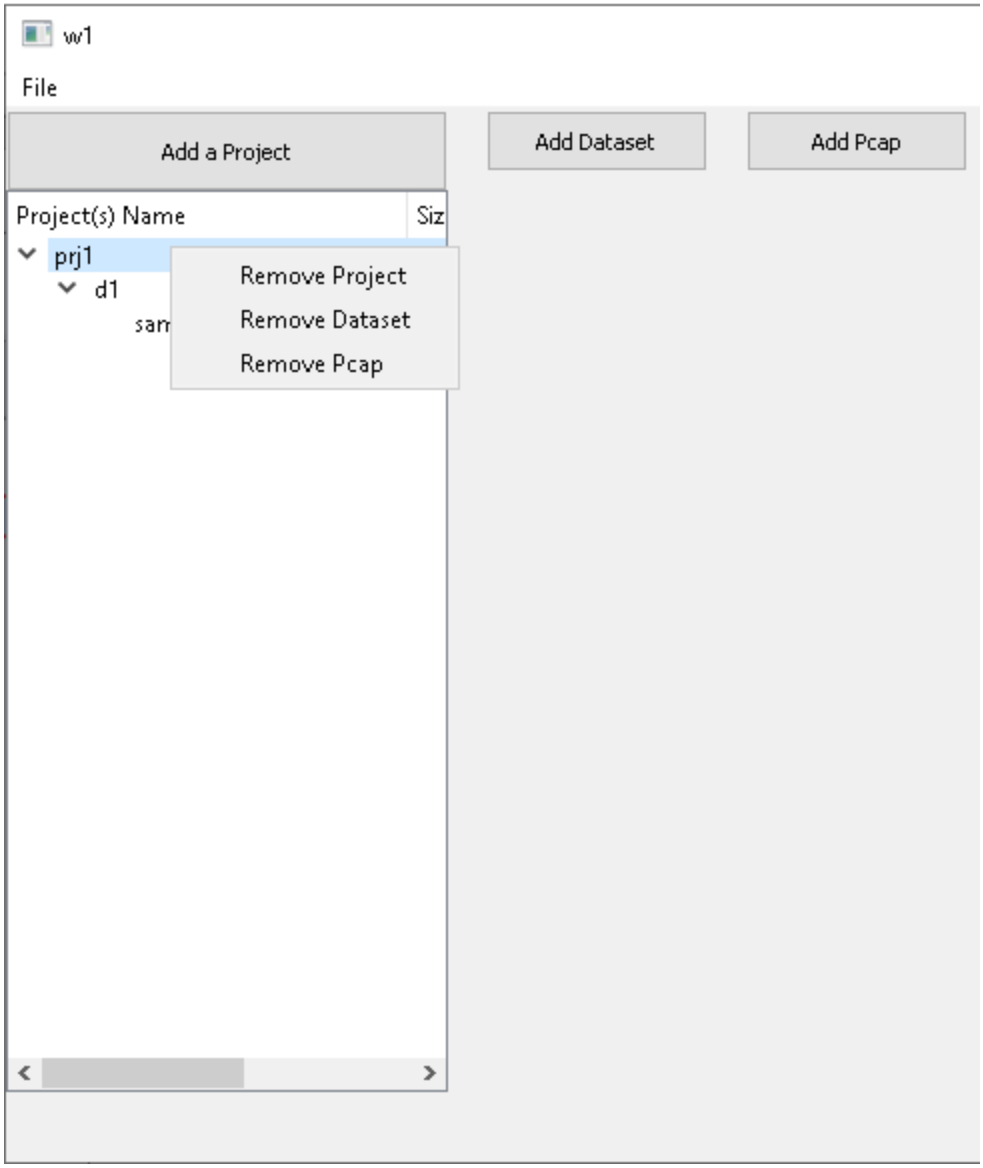


Remove PCAP



Delete Dataset

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

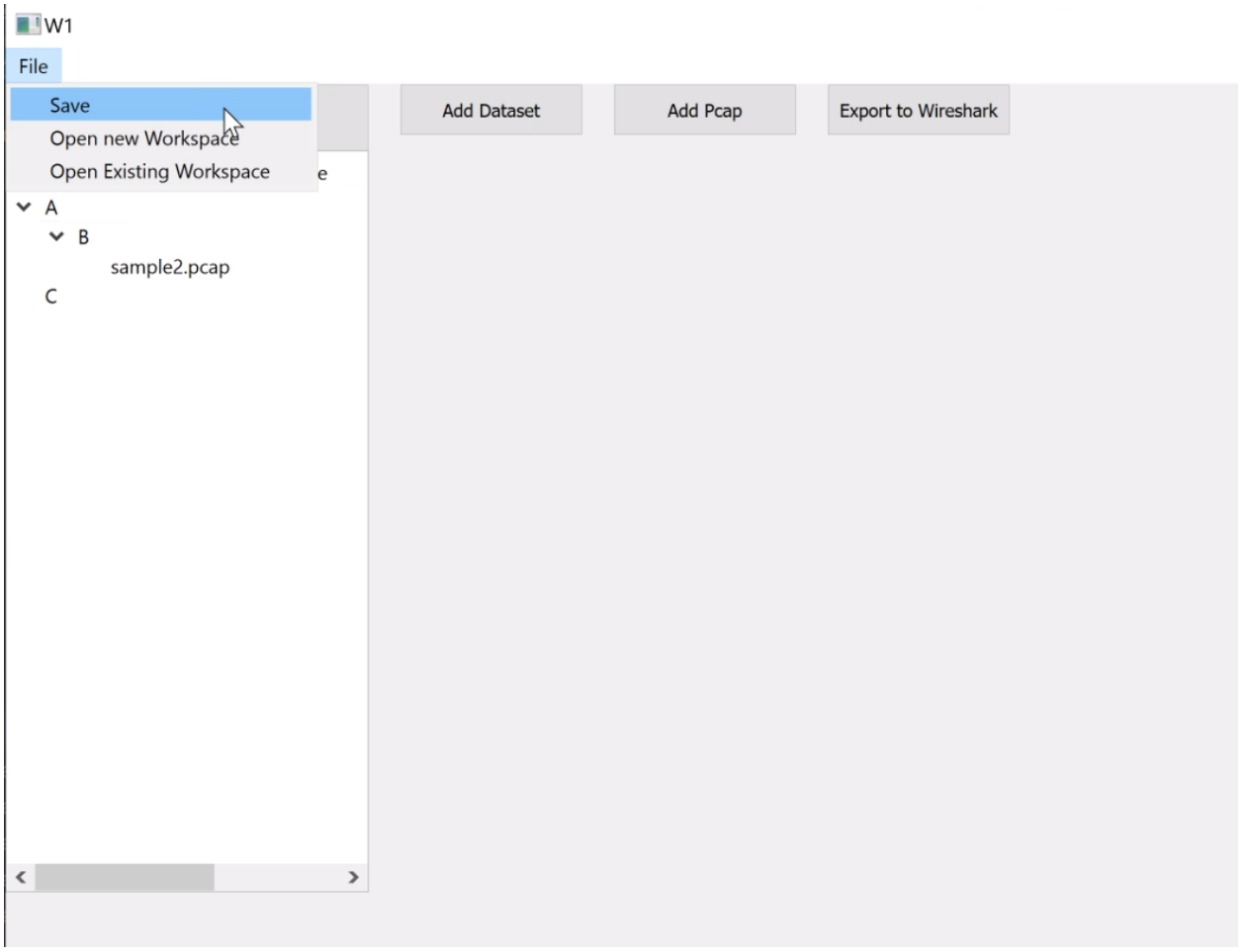


Delete Project

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

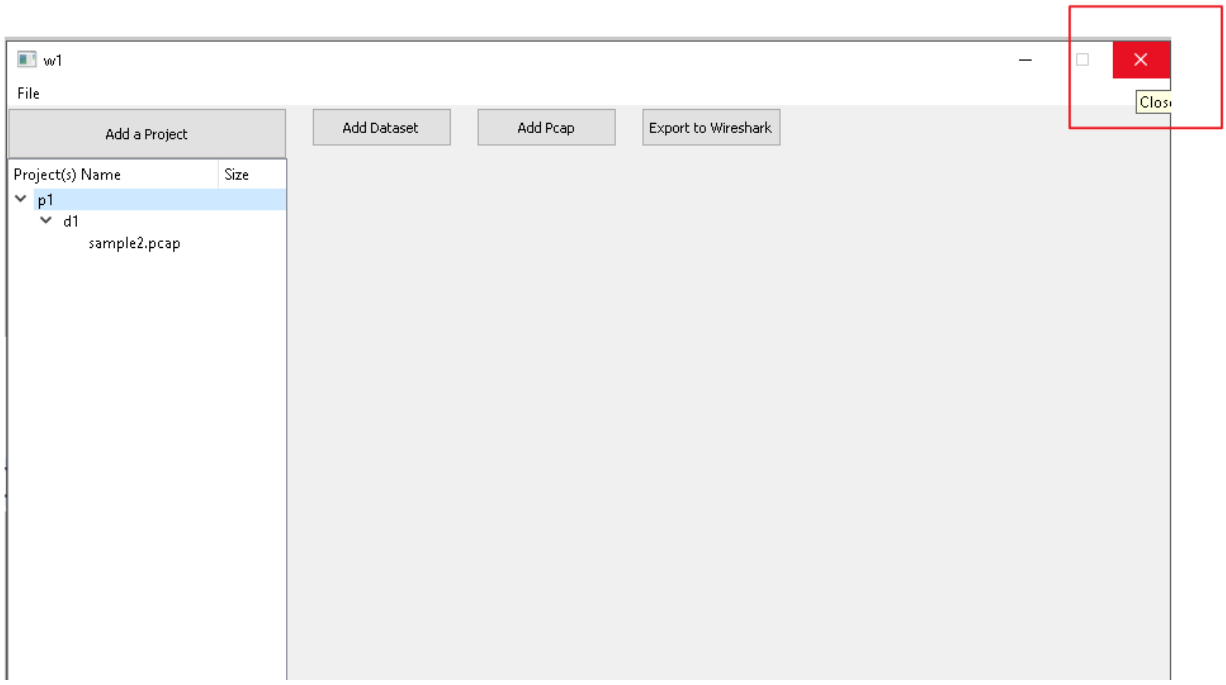
2.8 Save

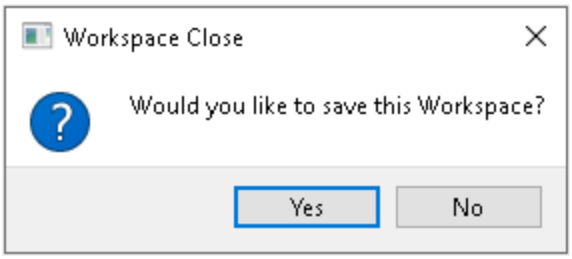
The user can choose to save any workspace that they have created. The system will automatically create a ZIP folder with the Workspace name and save it in the the directory that the user originally chose to create the workspace in as shown below:



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)

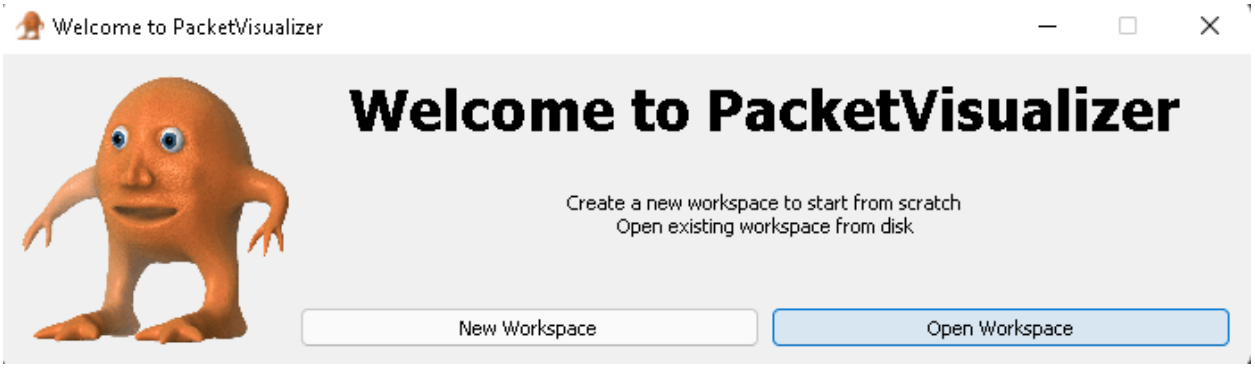
Should the user choose to close the workspace unexpectedly the system will prompt the user to save the workspace, as shown below:



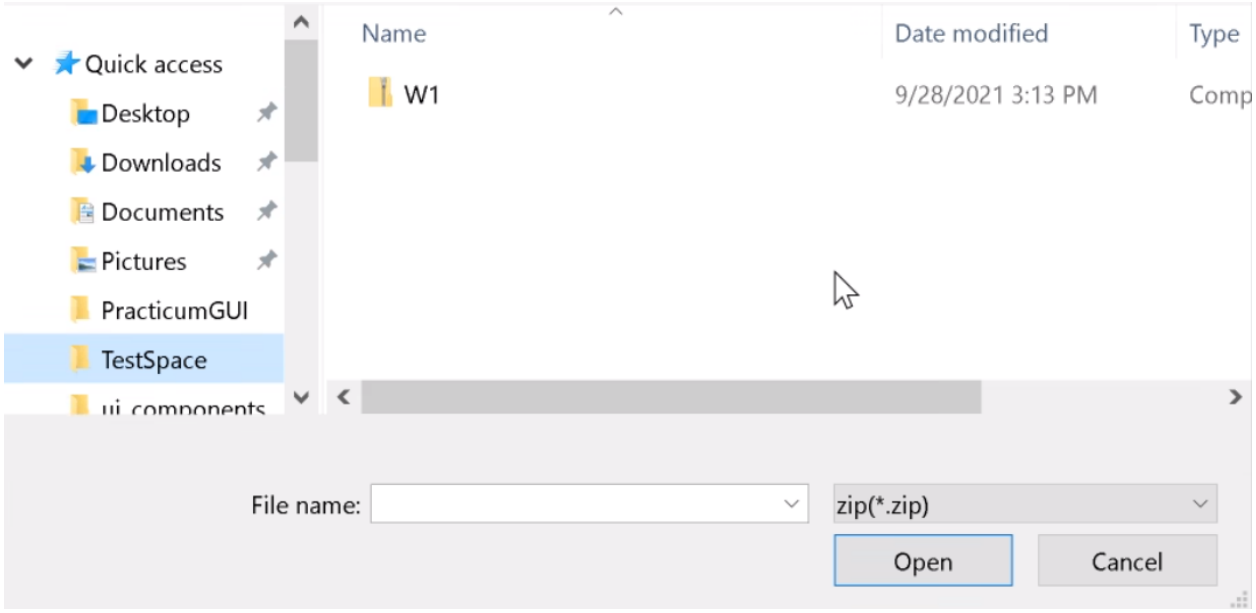


2.9 Reopening an Existing Workspace

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

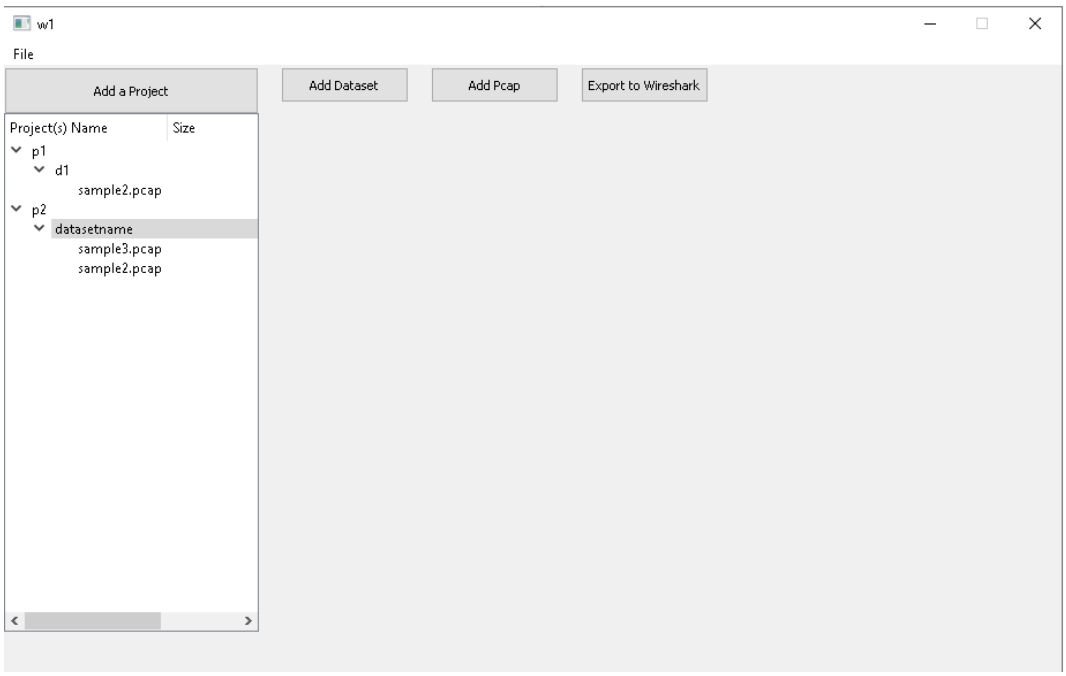


The expected input is a ZIP file that is the result of the save shown in Section 2.8. The following window appears:



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

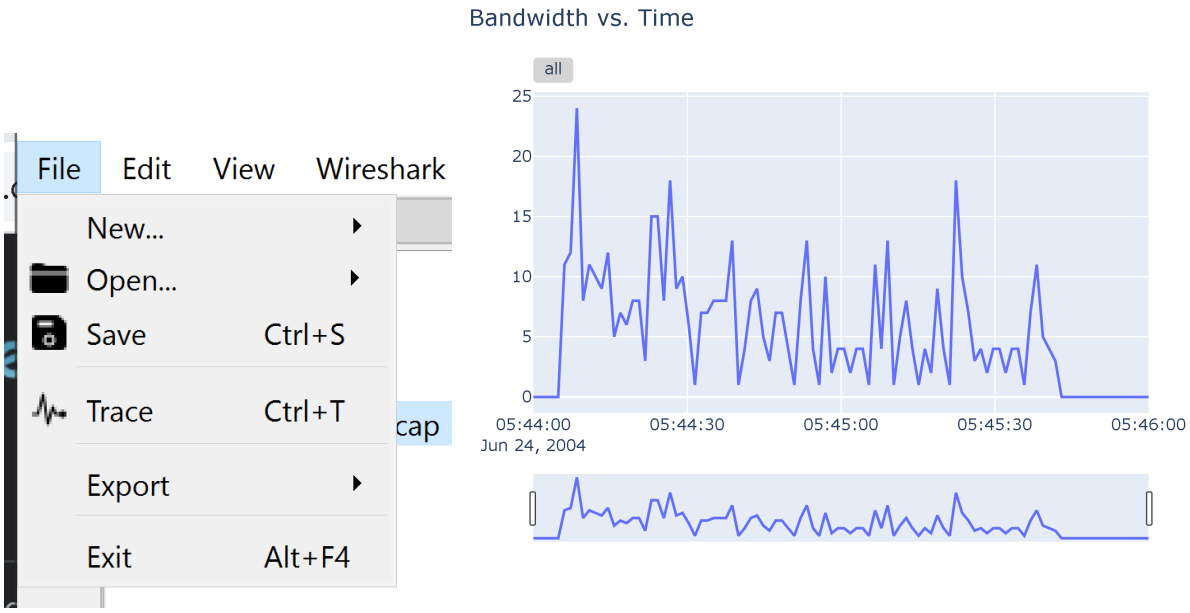
Example:



3.0 Bandwidth vs Time Graph

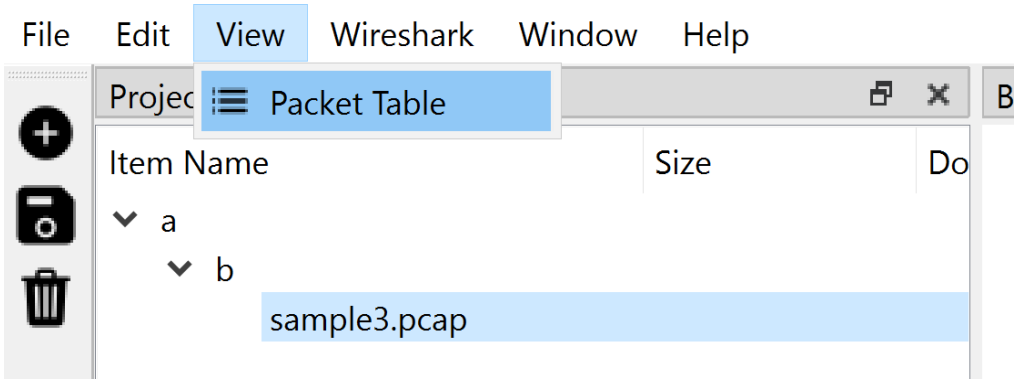
The Bandwidth vs Time Graph will start on the right dock area of the system in a “neutral” state. To display the graph information, simply select a Dataset from the Project Tree and select “Trace” from the File Menu.

Note: In an updated version of the system the “trace” will happen automatically upon clicking on an entity

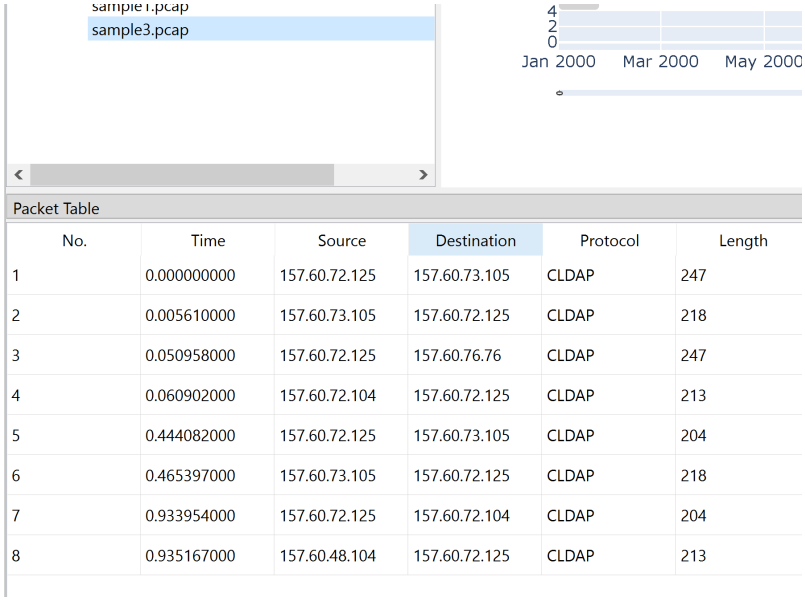


3.1 View Packet Table

The system also allows the user to view a table of packet information generated from a PCAP. To do this, select a PCAP File from the Project Tree and then select “Packet Table” from the View tab in the Menu bar



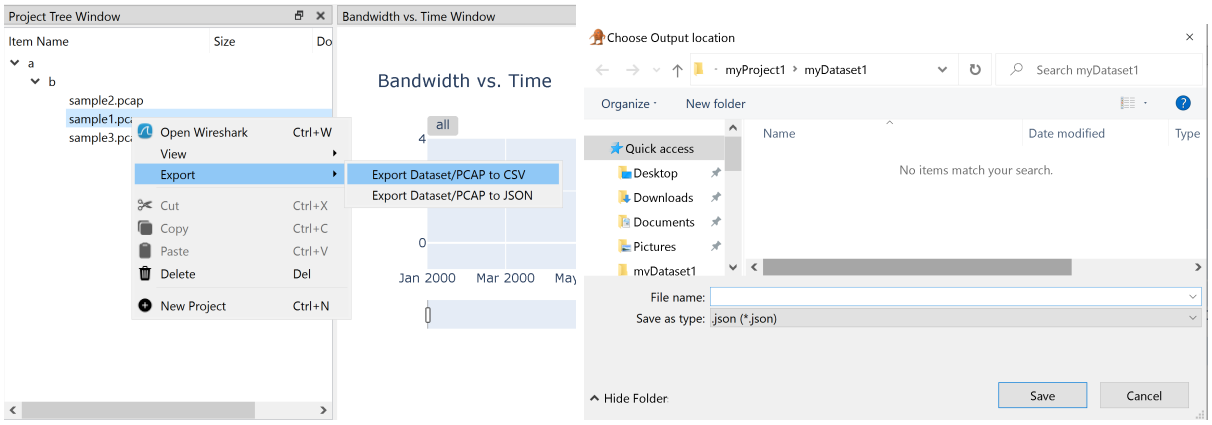
From that selection, a packet table with select field information will be docked in the lower window area.



No.	Time	Source	Destination	Protocol	Length
1	0.000000000	157.60.72.125	157.60.73.105	CLDAP	247
2	0.005610000	157.60.73.105	157.60.72.125	CLDAP	218
3	0.050958000	157.60.72.125	157.60.76.76	CLDAP	247
4	0.060902000	157.60.72.104	157.60.72.125	CLDAP	213
5	0.444082000	157.60.72.125	157.60.73.105	CLDAP	204
6	0.465397000	157.60.73.105	157.60.72.125	CLDAP	218
7	0.933954000	157.60.72.125	157.60.72.104	CLDAP	204
8	0.935167000	157.60.48.104	157.60.72.125	CLDAP	213

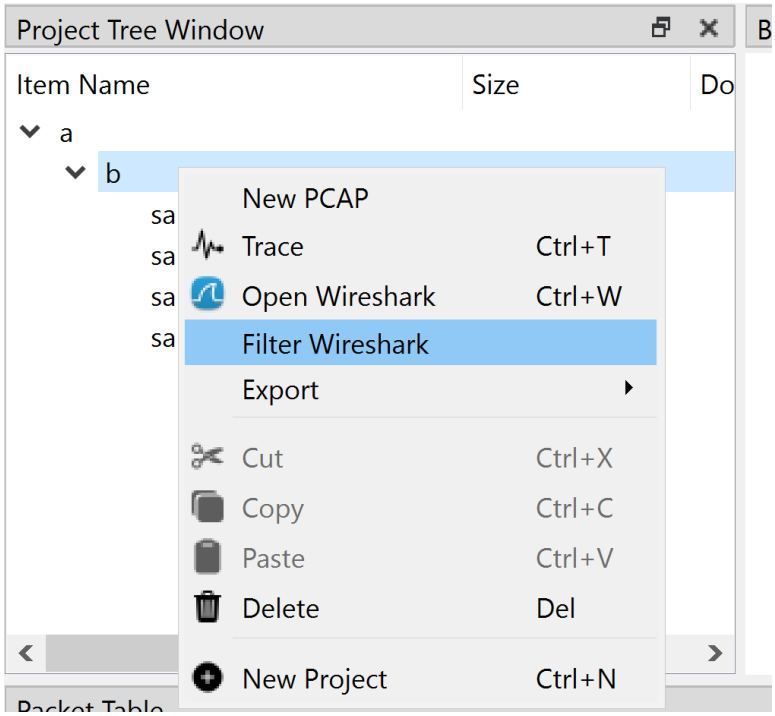
3.2 Export to CSV and JSON

From the project tree, select a PCAP or Dataset with a right-click. From the context menu, select export and then choose your output of either JSON or CSV. After that, you will be prompted to select a save location and name for the file.

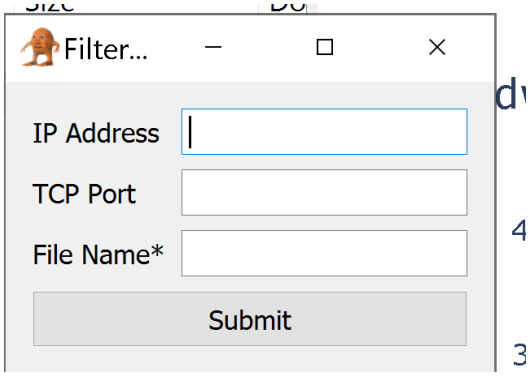


3.2 Filter to Wireshark

To apply filters to a Dataset simply select the Dataset from the Project Tree and then right click. From the context menu you can choose “Filter Wireshark”.

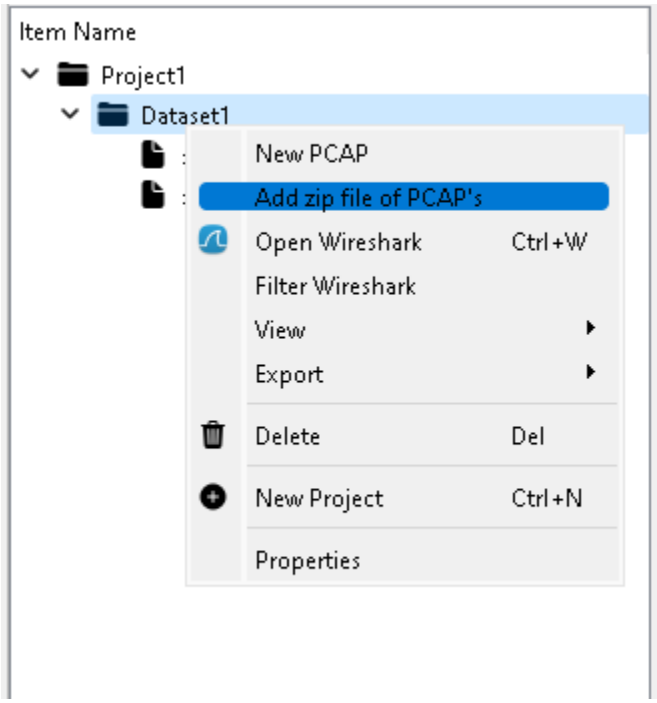


From there a prompt will be displayed on which filters you would like to apply before viewing in Wireshark



3.3 Add ZIP of PCAPS

Similar to section 2.5, the user now has the ability to add a zip file containing PCAPS. The system will process the zip and assign them to the correct project. In order to add a zip file, the user must right click on a dataset and select the, “Add Zip File of PCAPs” option.

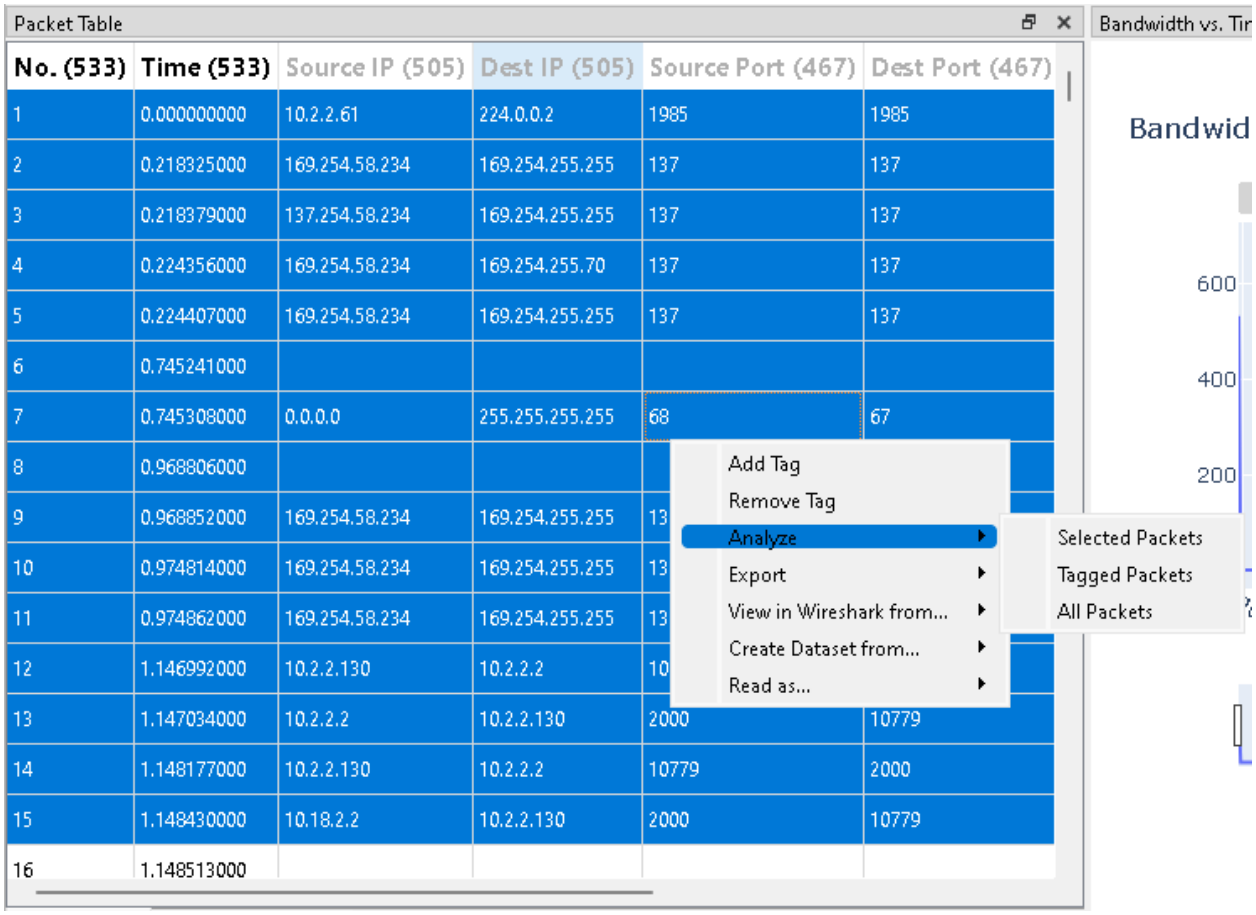


3.4 Analysis

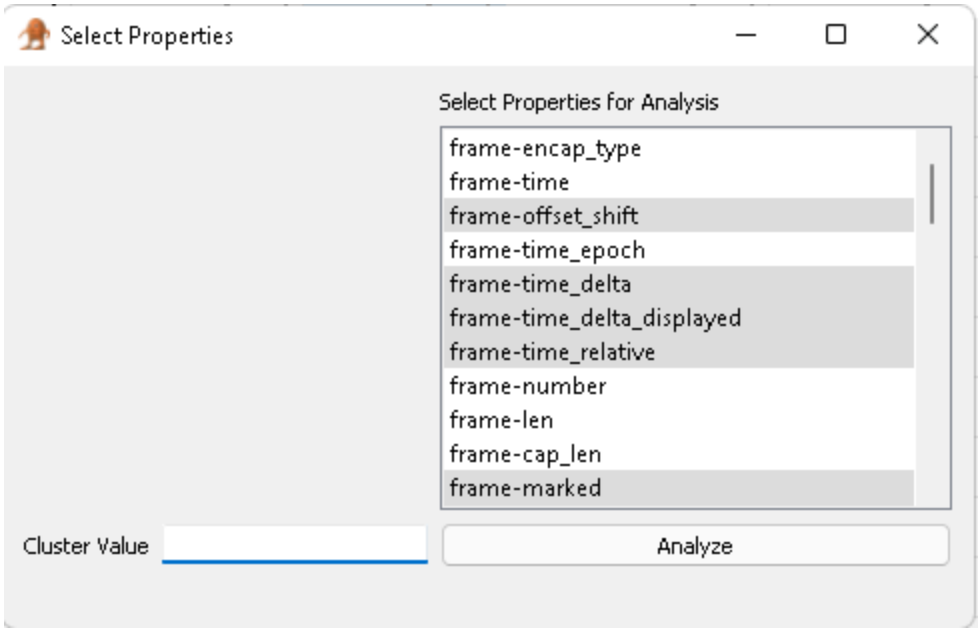
From the Packet table view the user now has the option to analyze packets. The following options are currently supported by the Packet Visualization system:

- Analyze Selected Packets
    - User must drag select packets in a given table for this functionality
- Analyze Tagged Packets
    - User must assign a “tag(s)” to the current packet table for this functionality
- Analyze All Packets

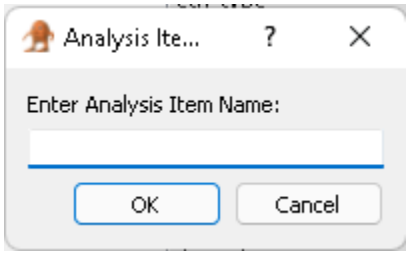
The user must right click over the packet to reach the “Analyze” option. Shown below:



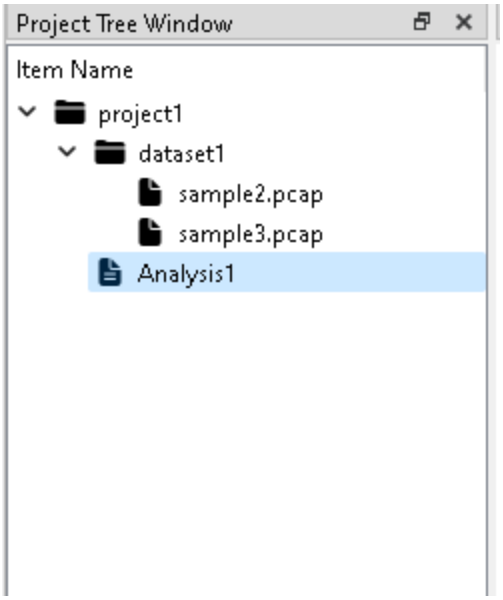
Upon selection of one of the options shown above, the user will be prompted with the following window:



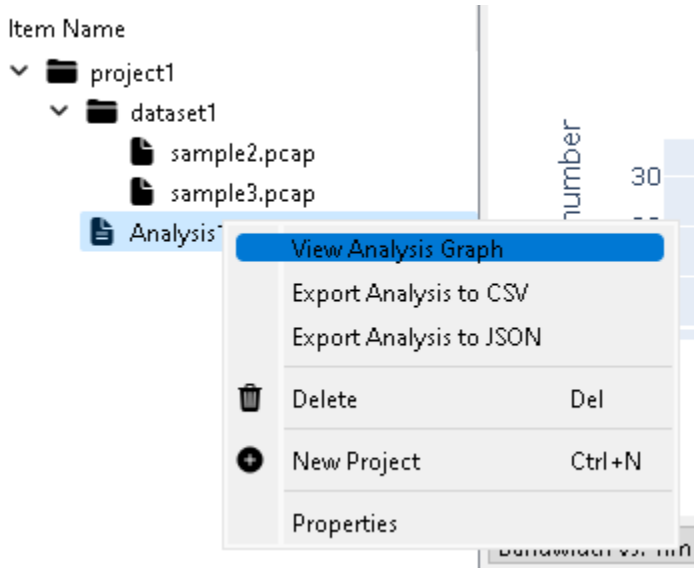
Note: The system currently only supports the K-Means clustering algorithm in which a cluster value is required. The architecture is a plugin architecture and provides an easy way to add algorithms to this window at a later date.



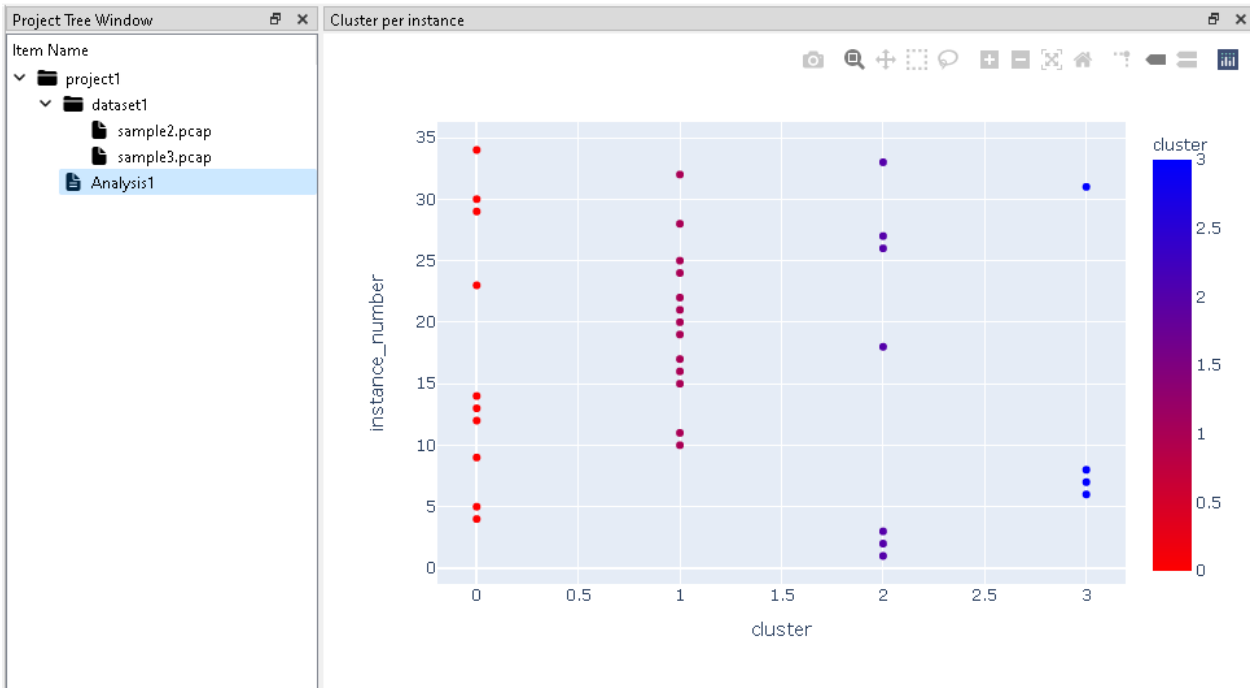
The user will then be prompted to name the analysis item. Upon successful creation of an Analysis, the user will see the Analysis item appear in the project tree, shown below:



To view the analysis graph, the user must right click on the analysis item and select, “View analysis in Graph”.

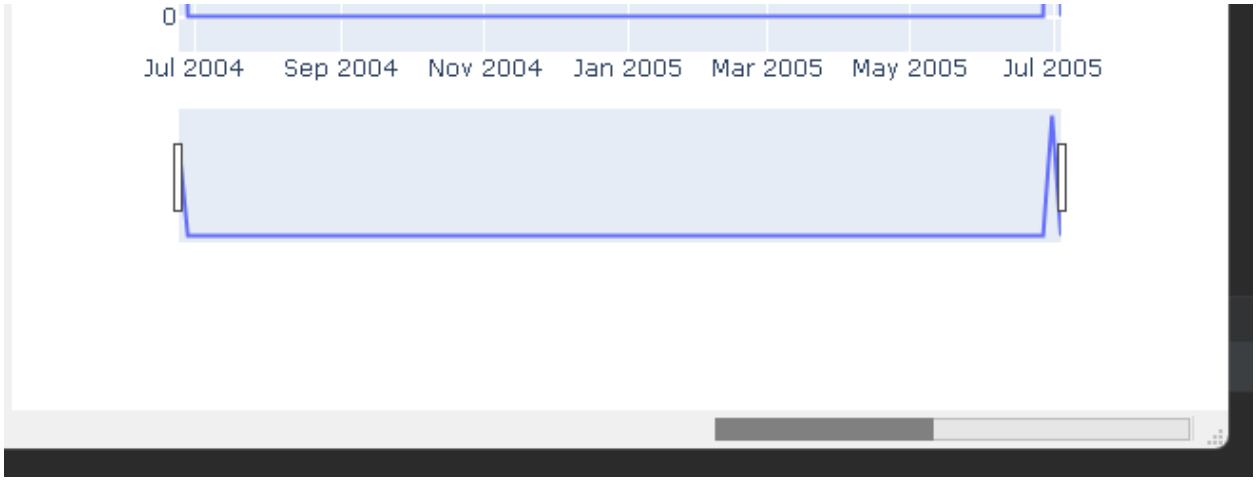


The following window will appear:



3.5 Ingesting Large PCAPs

Note the system has capability to ingest large PCAP files, however there is an associated wait time to process the data and insert it to the database. Please give the system adequate time to complete this. There is an associated progress bar for this process (bottom right of the interface) and the pcap will not be seen in the item project tree until the data is fully processed.



</3