Packet Visualization

Packet Visualization System

End User Product Manual

Version 1.0.1

December 7, 2021

Document Control

Approval

The Guidance Team and the customers will approve this document.

Document Change Control

Initial Release	0.1
Current Release	1.0.1
Indicator of Last Page in Document	</3
Date of Last Review	12/7/2021
Date of Next Review	12/7/2021
Target Date for Next Update	12/7/2021

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

1.0	December 1, 2021	Team	User Manual for Sprint 3-6 version of the System
1.0.1	December 7, 2021	Team	Updated version format to match project, updated images to represent the new system

Table of Contents

1. Installation and Setup

1.1. Dependencies

Before the system can be run, the following external tools need to be installed in the system; mongodb service also needs to be running on your system:

Wireshark, tshark, mongodb

1.2. Installation

Listed below are the steps for running the Packet Visualization System

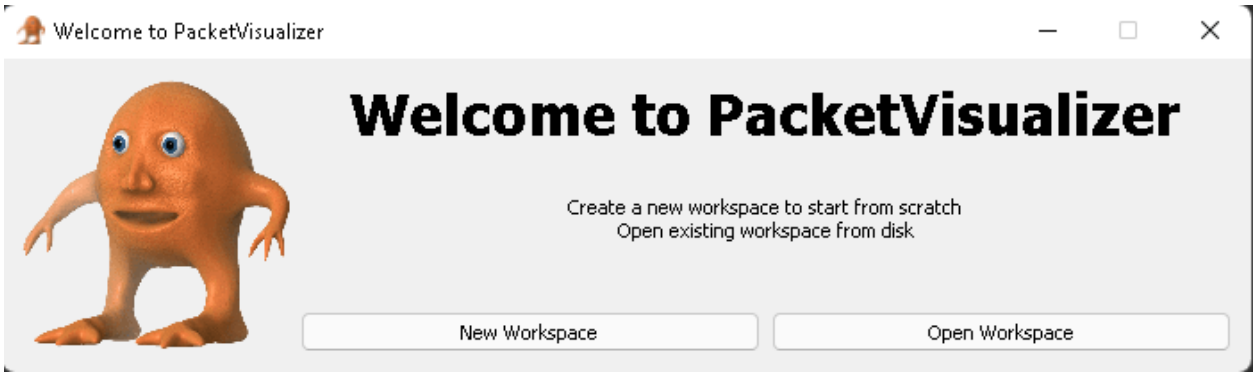
1. Run *pip install packetvisualization*
2. Run *python*
3. *Run the following Commands*
    a. from packetvisualiztion import run
    b. run()

See section 2 for the system's user manual.

2. Product/User Manual

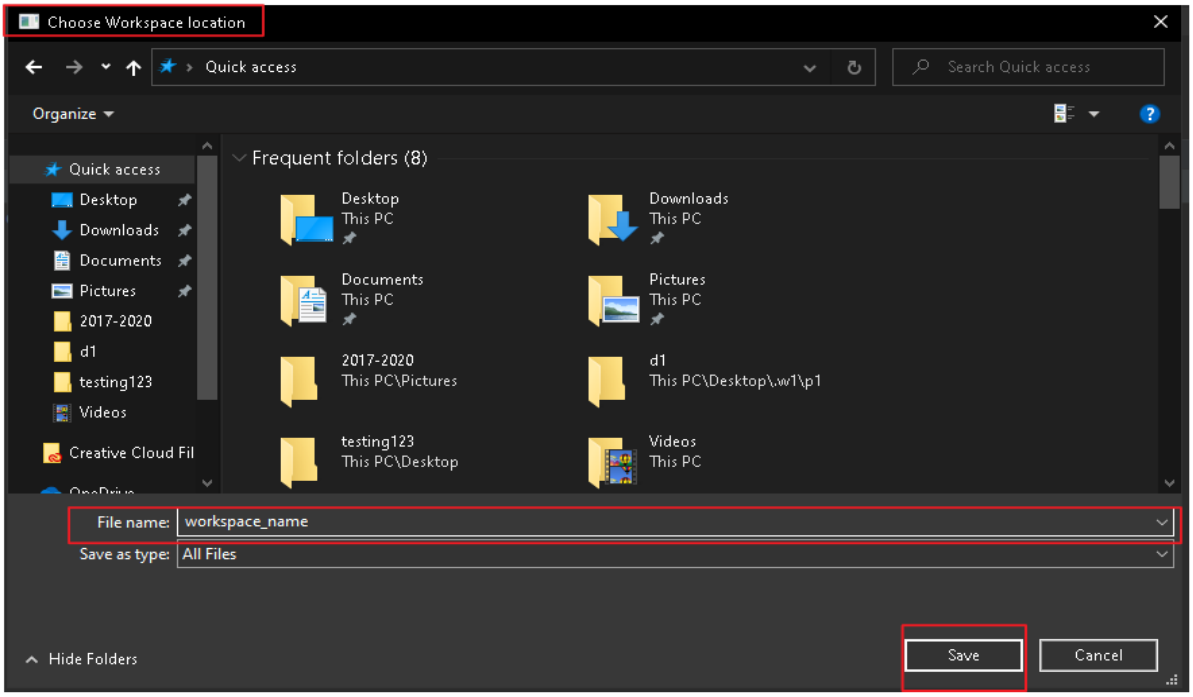
2.1. Startup

Upon starting the system, the user will be prompted to Start a new Workspace or Open an existing Workspace.



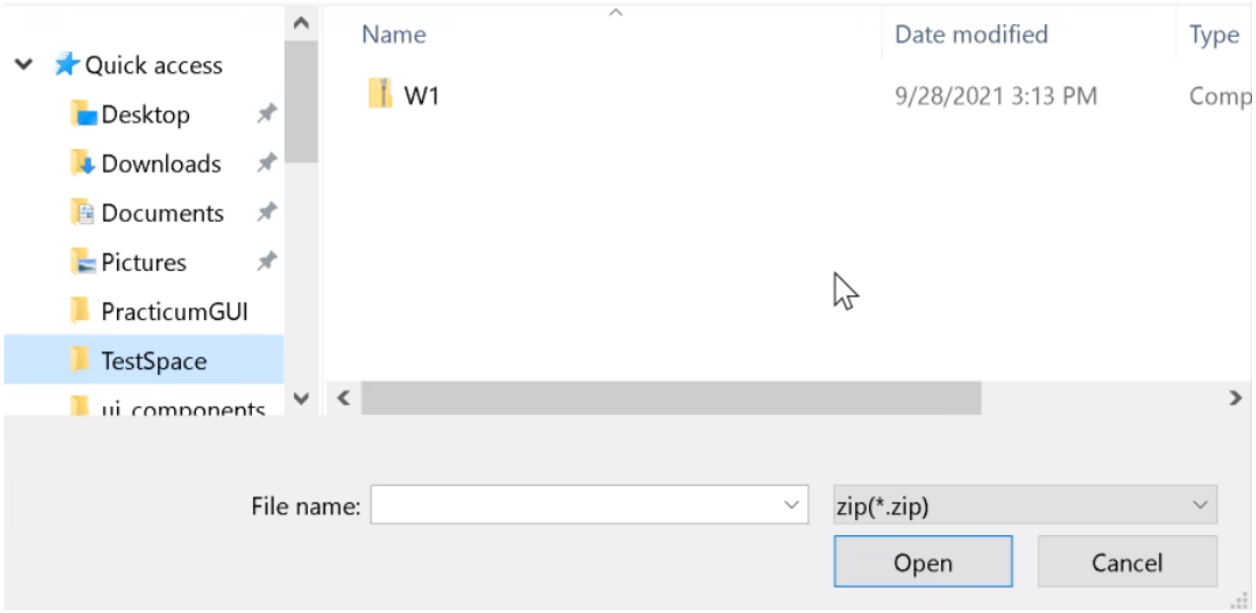
2.1.1. New Workspace

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.



2.1.2 Existing Workspace

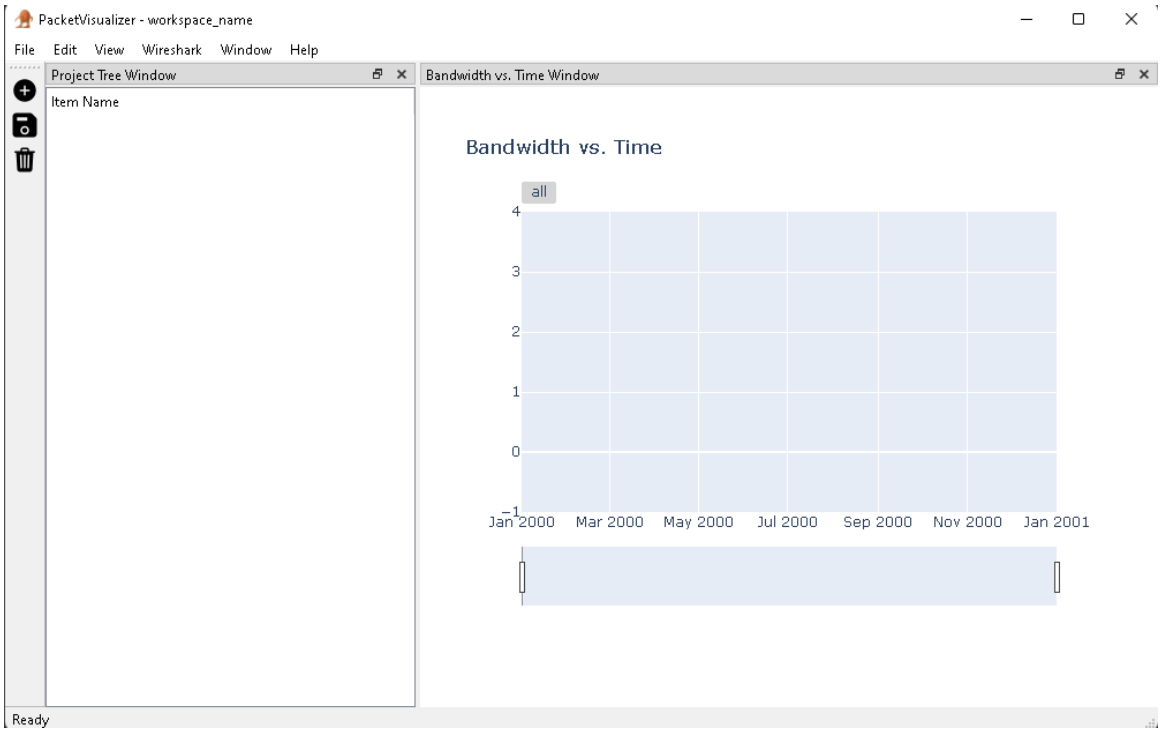
There is also an option for a user to load in an existing workspace. The expected input is a ZIP file that is the result of the save shown in Section 2.8. The following window appears:



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.

2.2 Workspace Layout

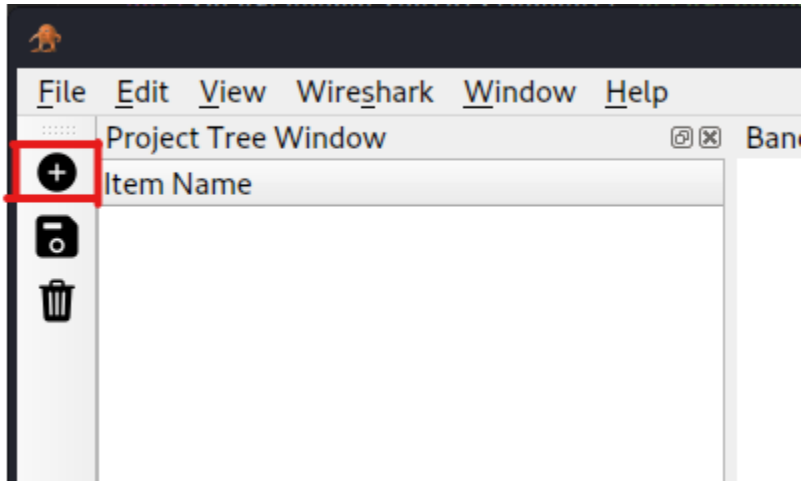
Once a workspace is successfully created, the following window will be displayed:

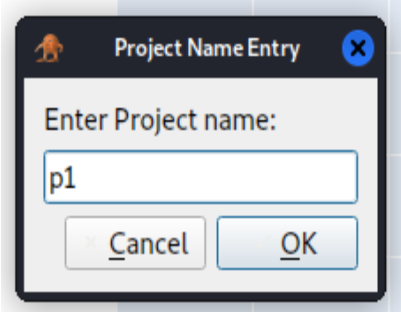


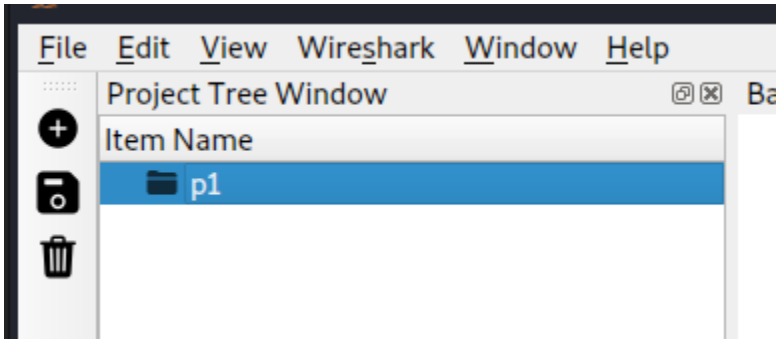
2.2.1 Add Project

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.

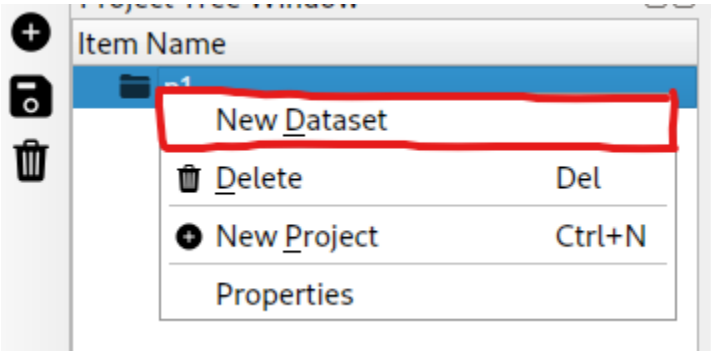


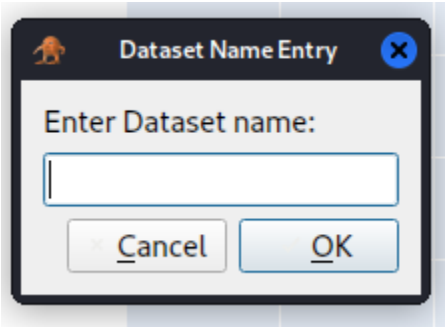




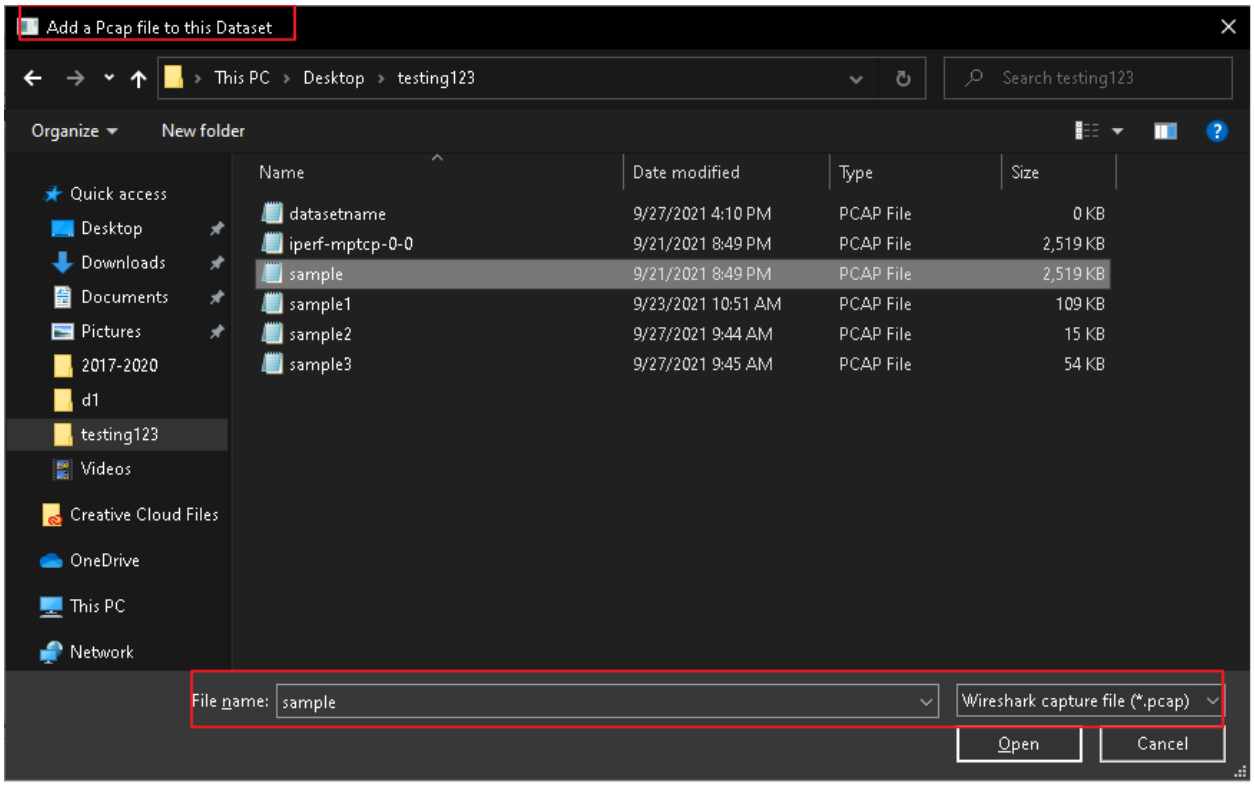
2.2.2 Add Dataset

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 by right-clicking on the project.

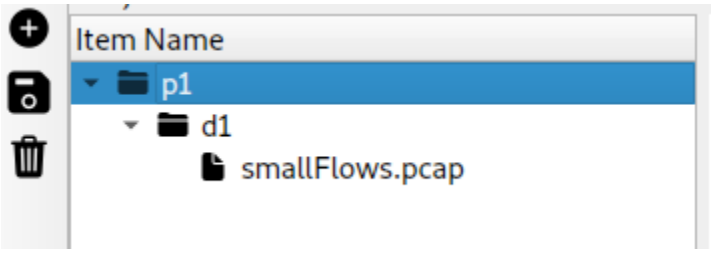




A key difference in this procedure is that upon naming the dataset the user will be prompted to select a PCAP file to add to the dataset. Note a user cannot create an empty dataset, every dataset must have at least one PCAP file.

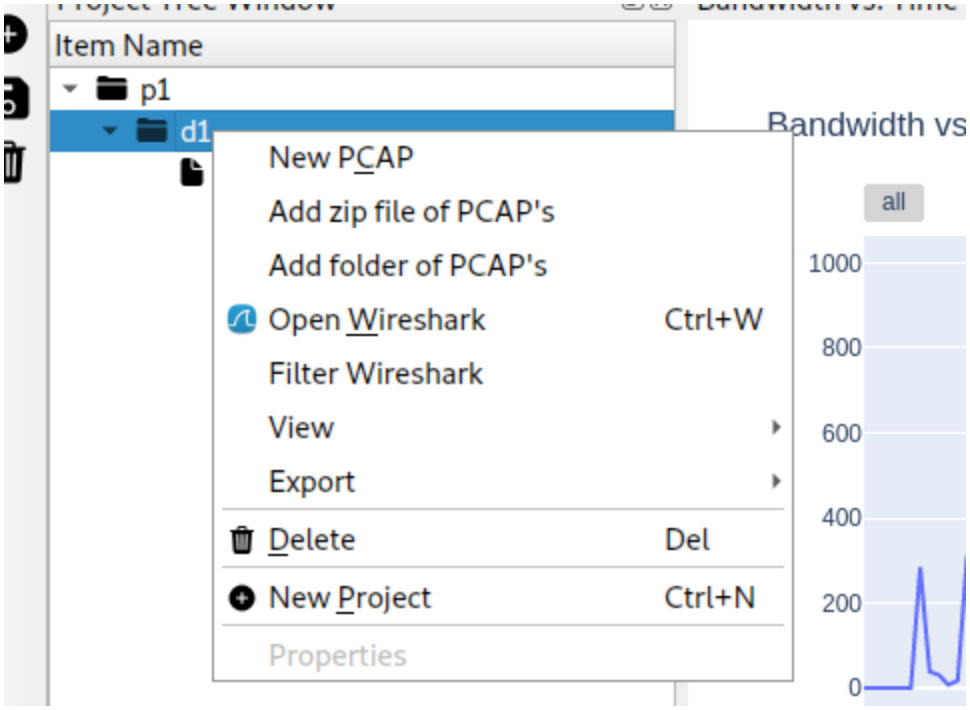


Upon successfully creating the Dataset, the user will see a dropdown under the project that contains the dataset and the pcap file added. As shown below:

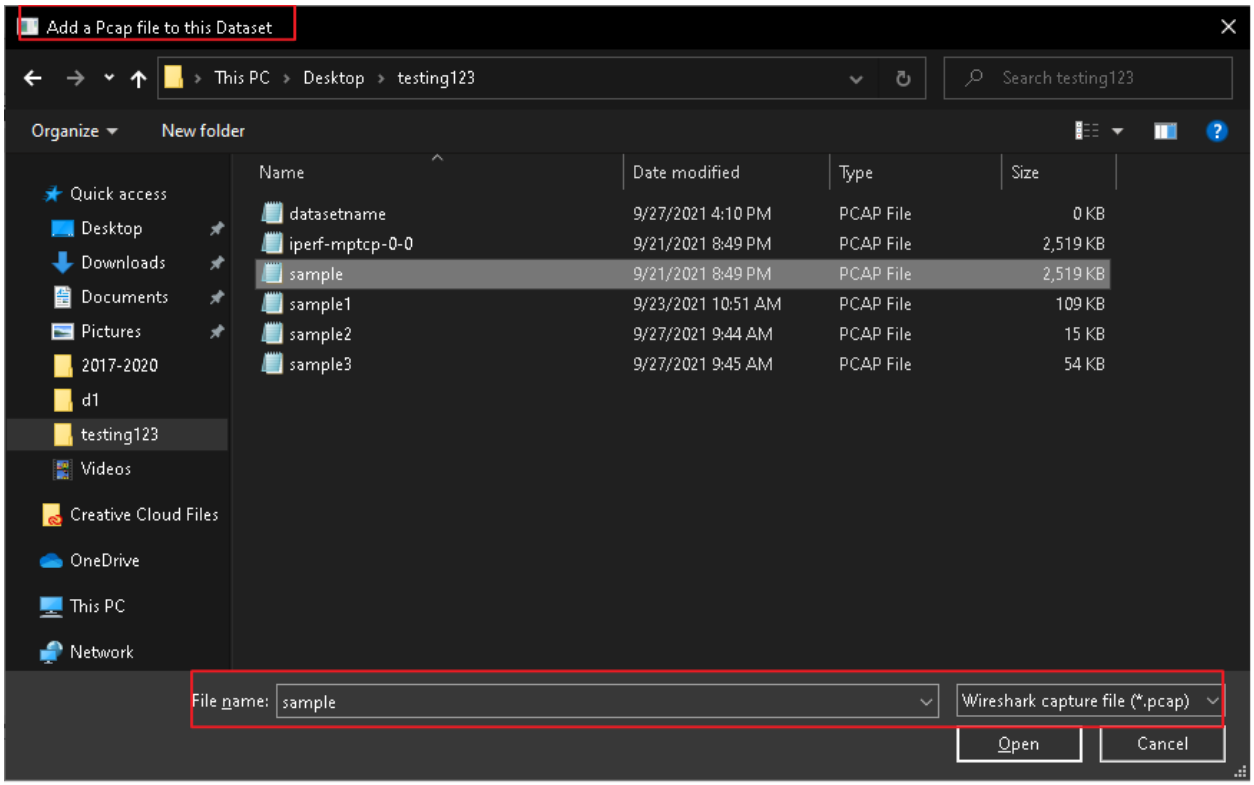


2.2.3 Add PCAP

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. By right clicking on the dataset, the user is provided the option to add a single pcap, a zip file of pcaps, or a folder of pcaps :



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

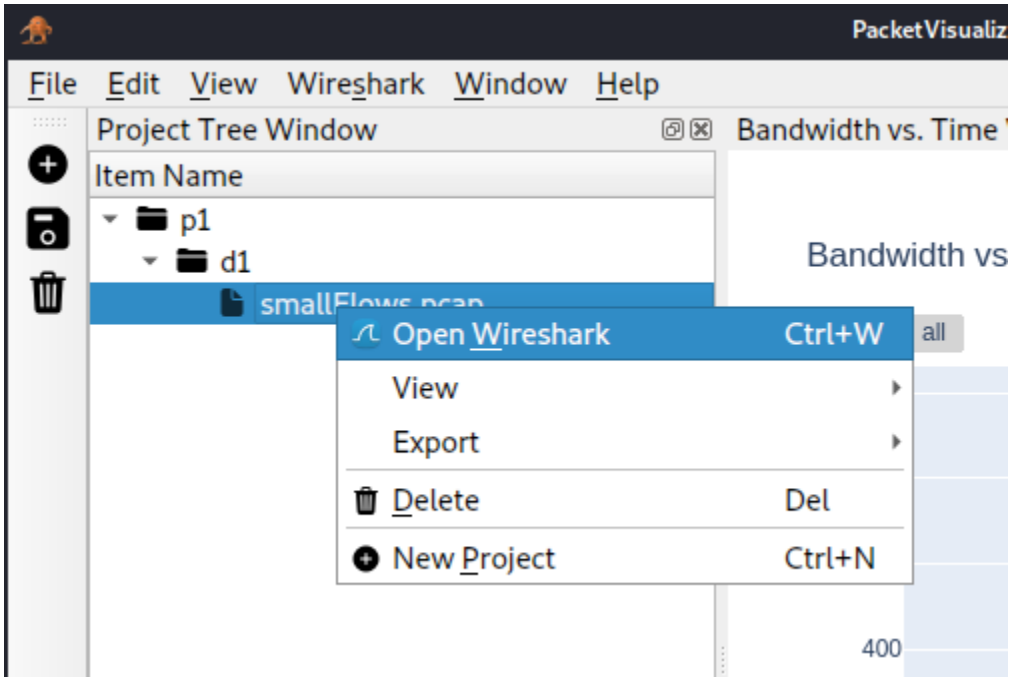


2.2.4 Open in Wireshark

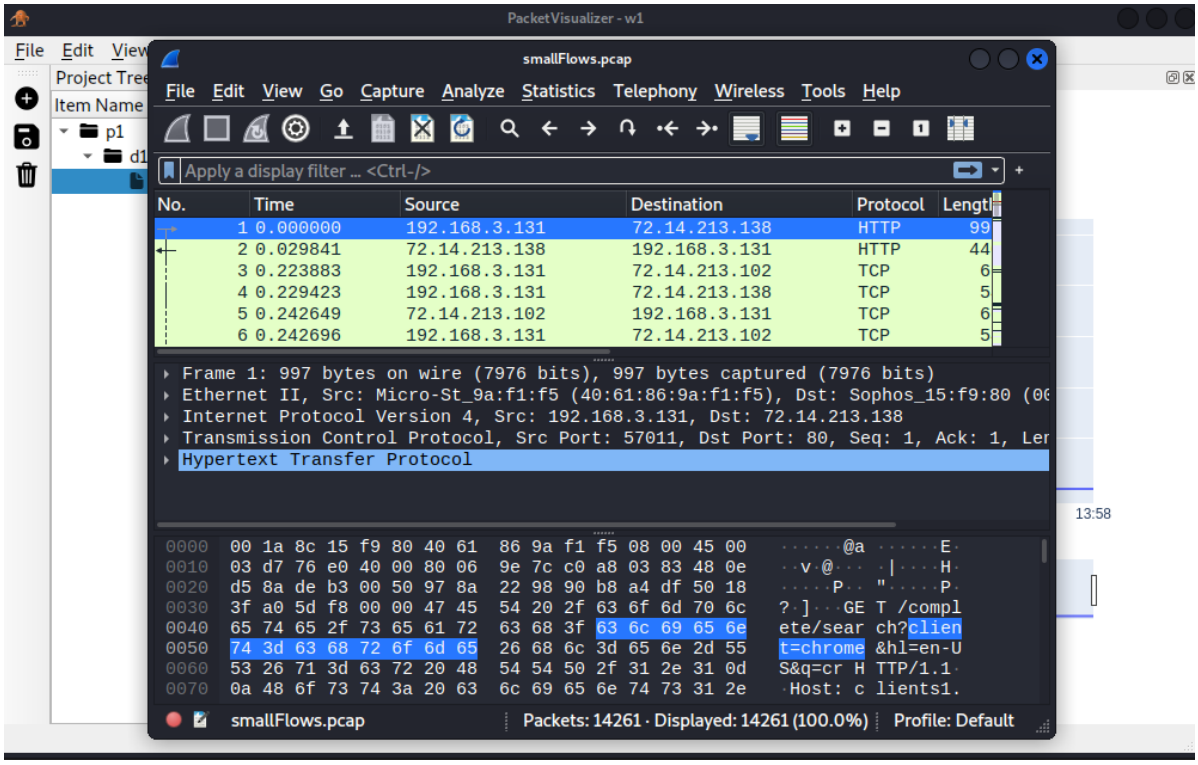
Once a Dataset is successfully added, the user will have the ability to open the packet data in Wireshark. The user has the following two options:

Open an Individual Pcap file in wireshark:

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

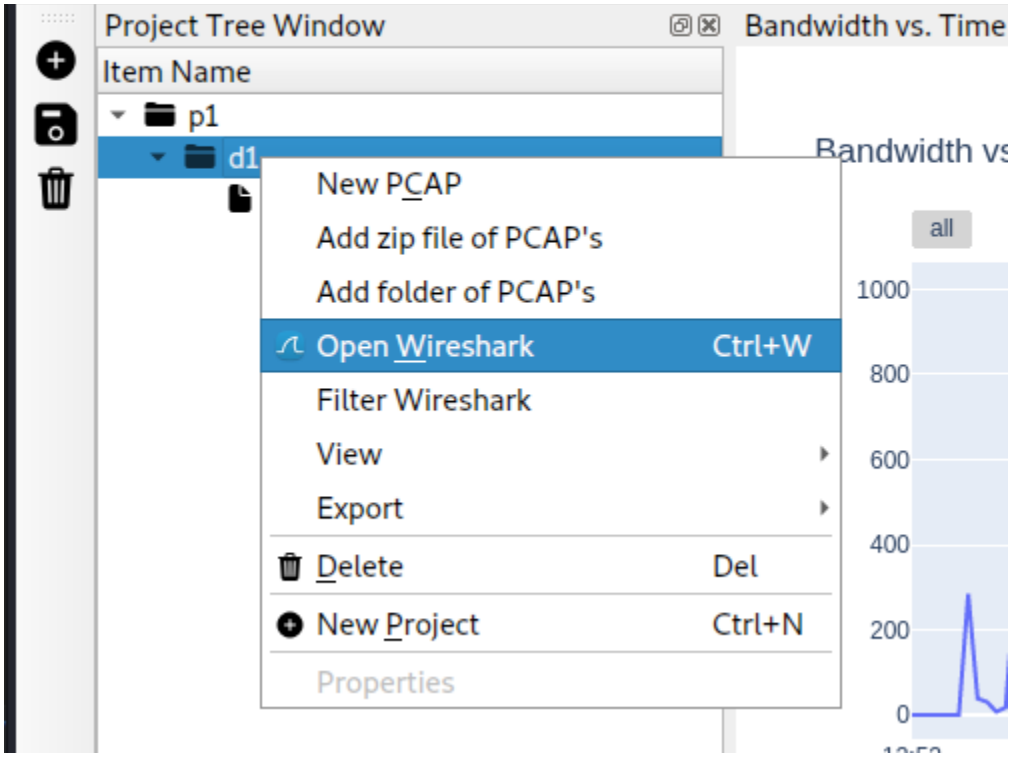


The system will then automatically open wireshark and display the packets of the selected pcap:



Open a Dataset in Wireshark:

The user can also select the Dataset and select open in Wireshark as shown below:

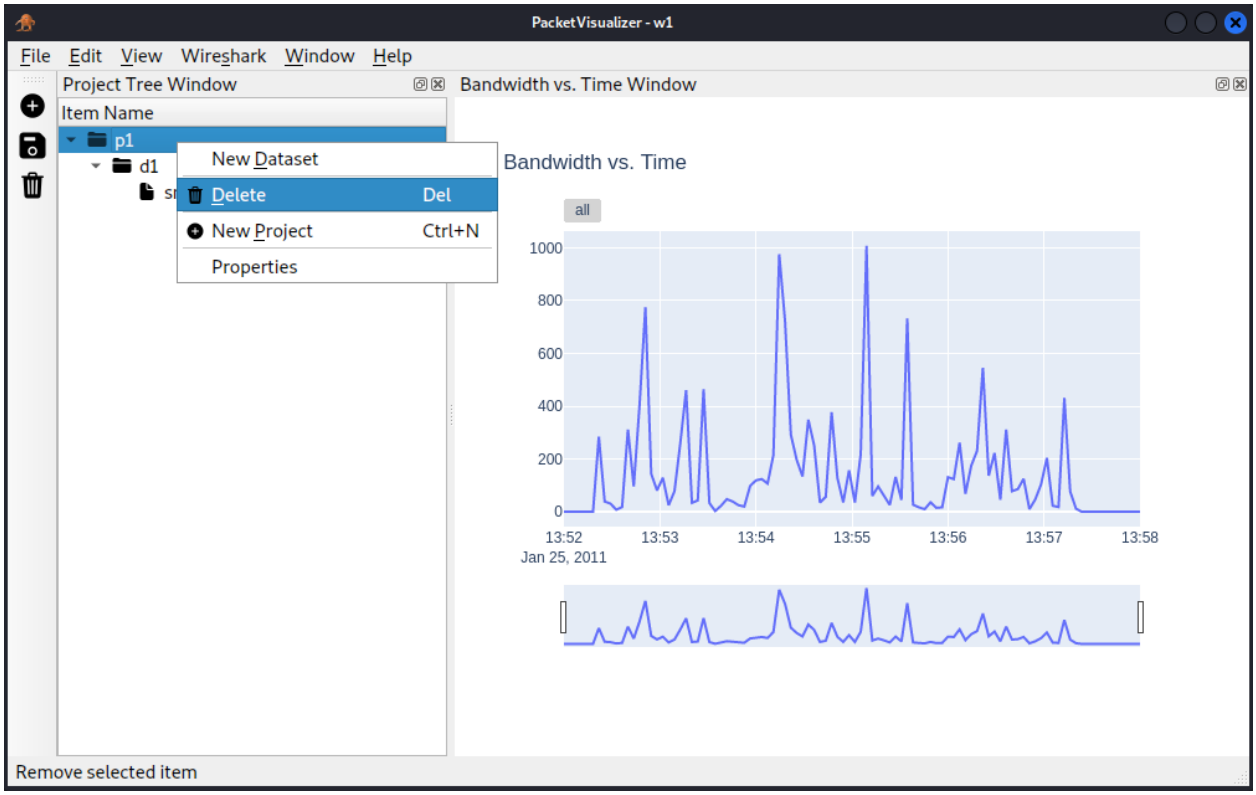


This will take ALL packets from the PCAP files present in the Dataset and export them to wireshark in the same manner as shown above.

2.2.5 Remove Pcap, Dataset, and Projects

At any point, a user can remove a Project, Dataset, and PCAP from the workspace. The user can do this in four ways:

1. Select the object and click the trash can button on the toolbar
2. Select the object and press the delete key on your keyboard
3. Right click the object and click on “Delete”
4. Through the file menu at the top, Edit>Delete

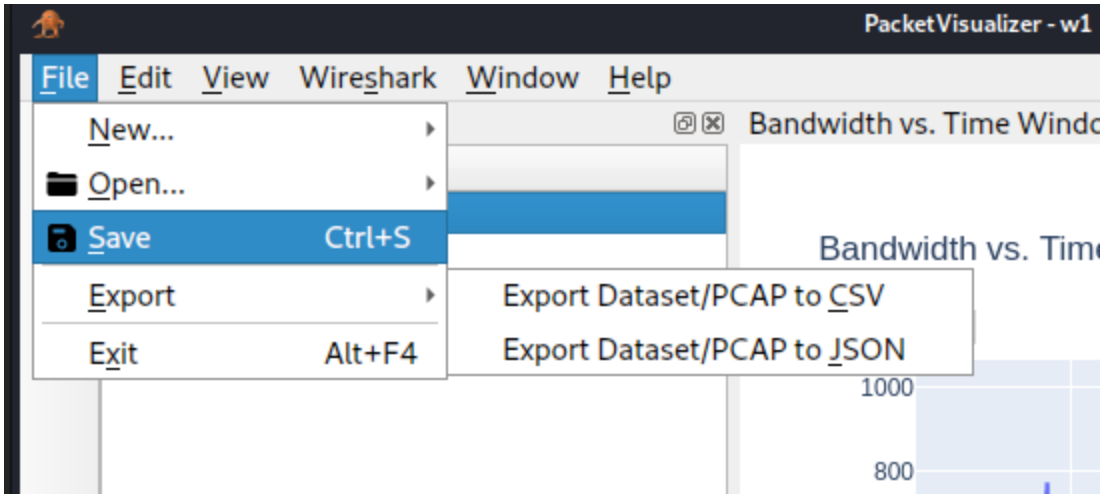


Deleting a Dataset will also delete all of the PCAPs that are contained in the Dataset. Deleting a project will also delete any of the Datasets present in the Project

2.2.5 Save

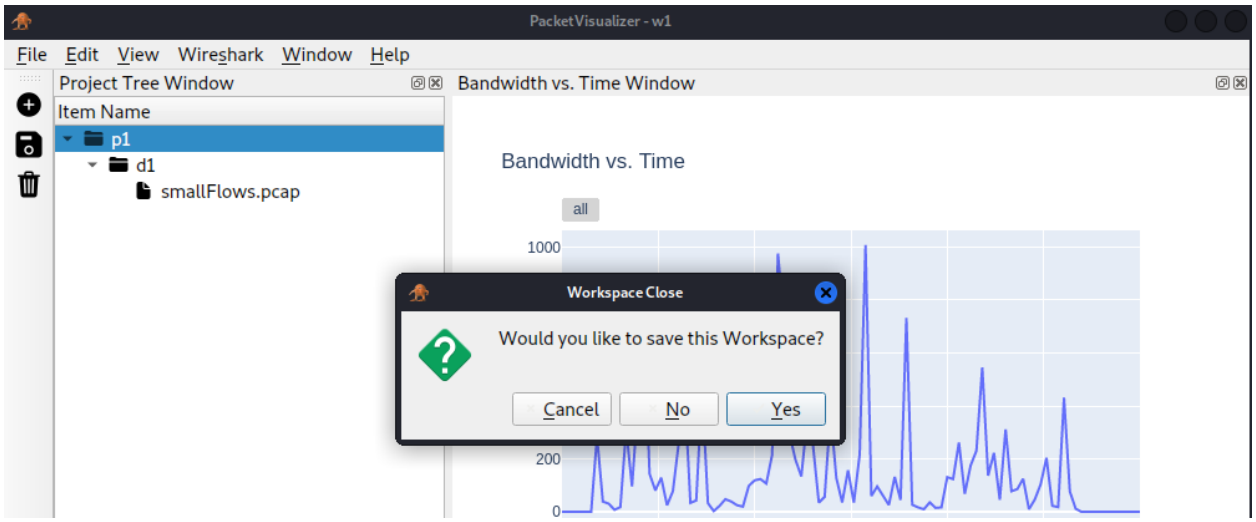
The user can choose to save any workspace that they have created. The system will automatically create a ZIP folder with the Workspace name and save it in the directory that the user originally chose to create the workspace. The user has the 3 options to save the workspace:

1. Through the file menu at the top, File>Save
2. Clicking on the save icon on the toolbar
3. Exiting and selecting “Yes” to save the workspace

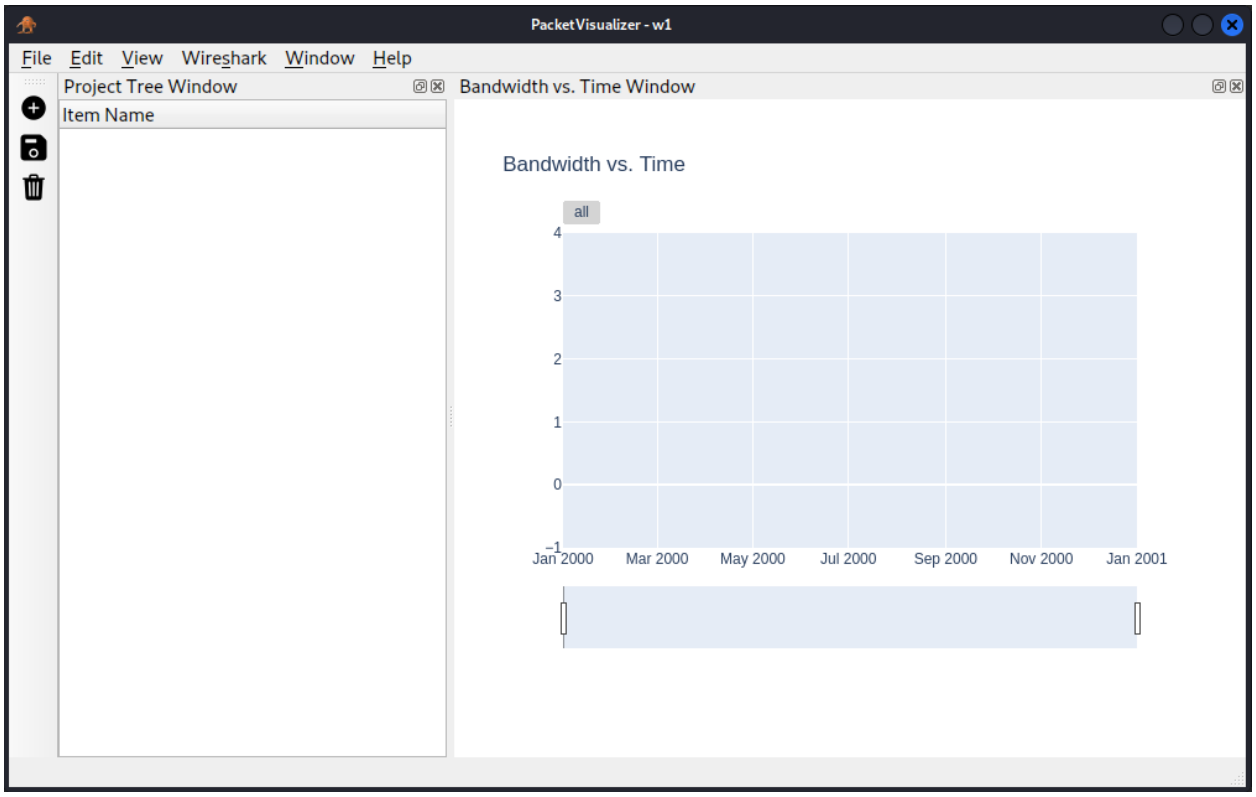


Note: All information: including Projects, Datasets, PCAP files as well as the database dump will be exported and available for relaunch should the user choose to import the ZIP (See Section 2.1.2).

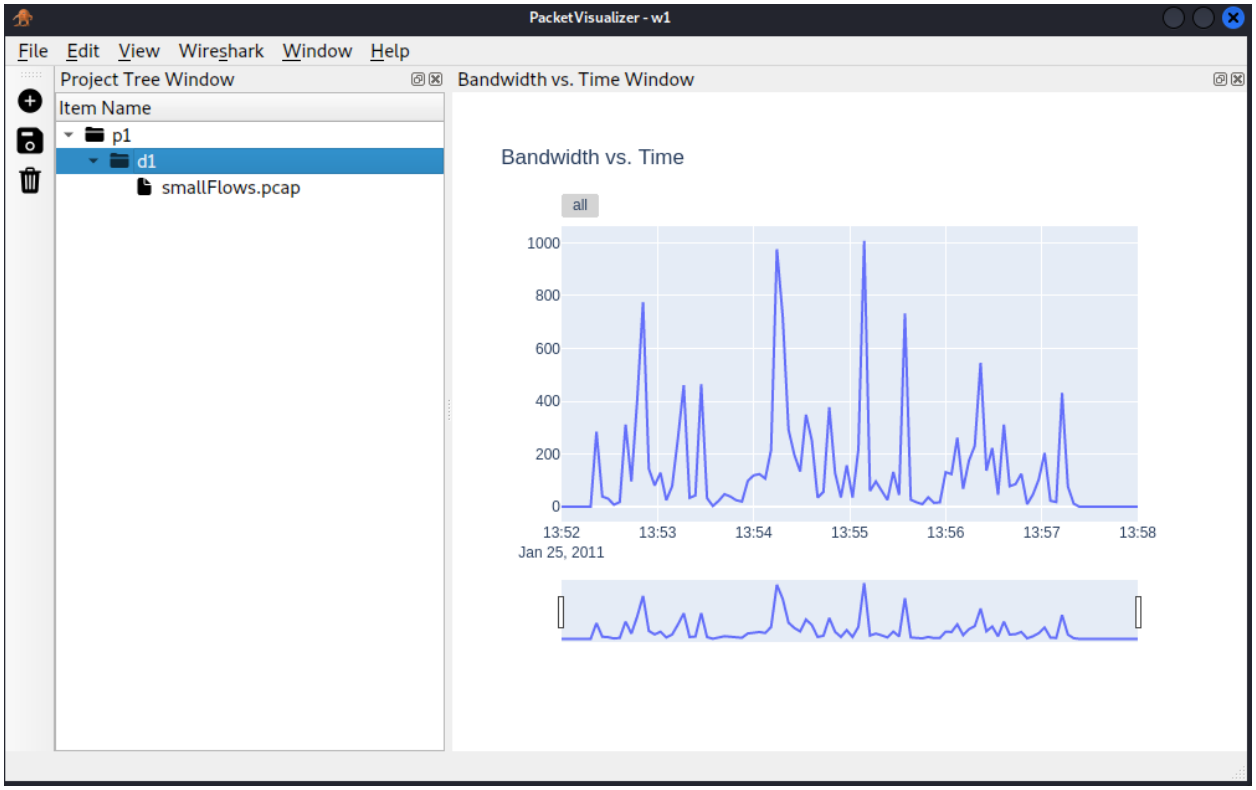
Should the user choose to close the workspace unexpectedly the system will prompt the user to save the workspace, as shown below:



2.2.6 Bandwidth vs Time Graph



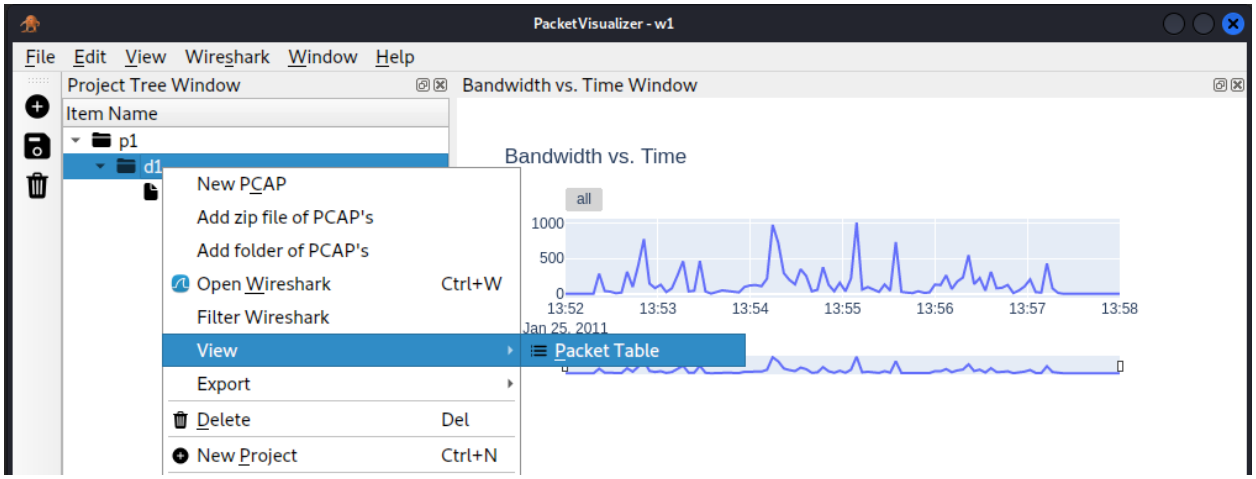
The Bandwidth vs Time Graph will start on the right dock area of the system in a “neutral” state. To display the graph information, simply select a Dataset from the Project Tree and the graph will automatically populate. If information in the dataset changes such as new information is added or removed, the graph is dynamically updated to accommodate the changes.



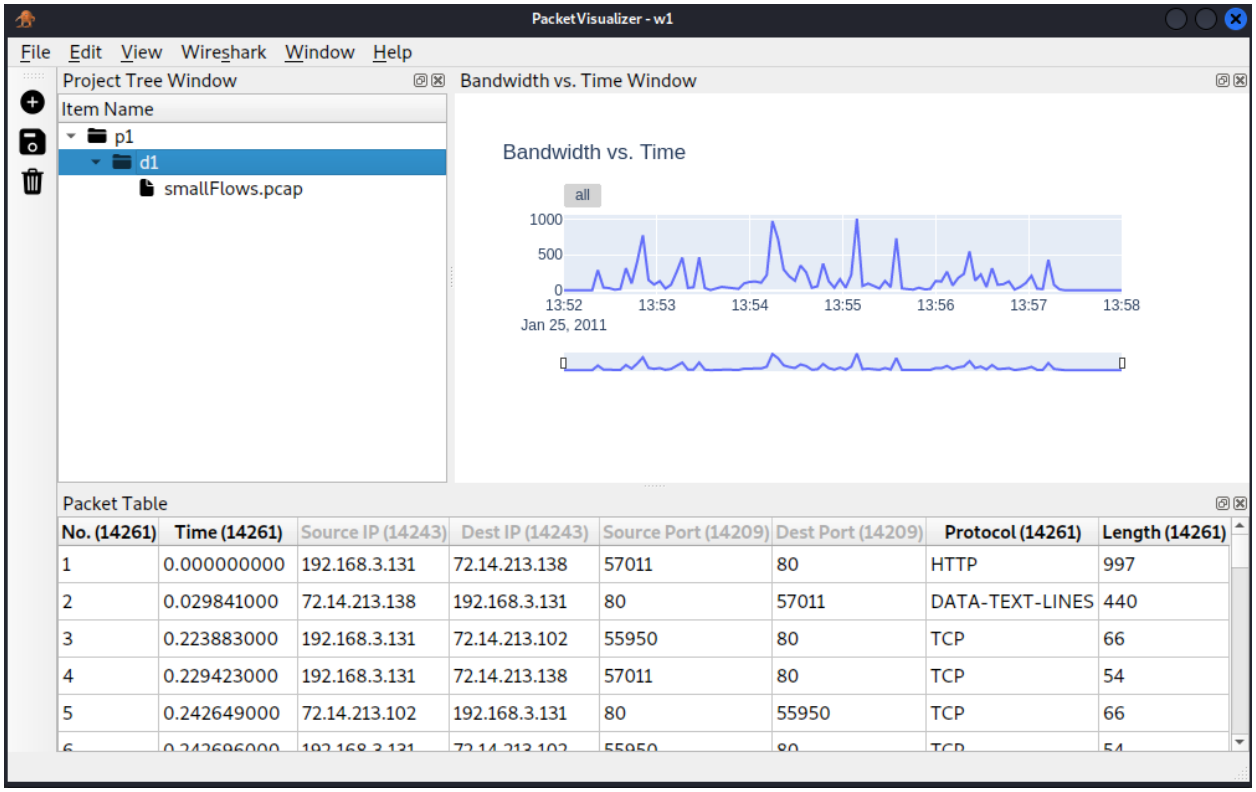
2.2.7 View Packet Table

The system also allows the user to view a table of packet information generated from a PCAP or Dataset. To do this, select a PCAP file or Dataset from the Project Tree and then select “Packet Table”; this can be done two ways:

1. Though the menu bar at the top, View>Packet Table
2. Right clicking on the object and clickon on View>Packet Table



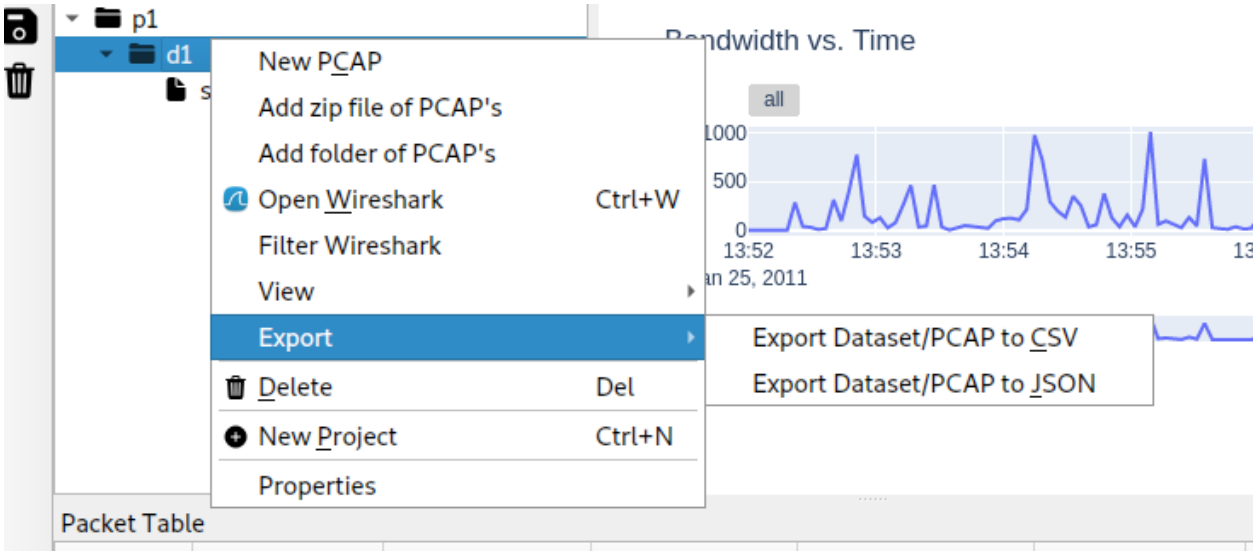
From that selection, a packet table with select field information will be docked in the lower window area.



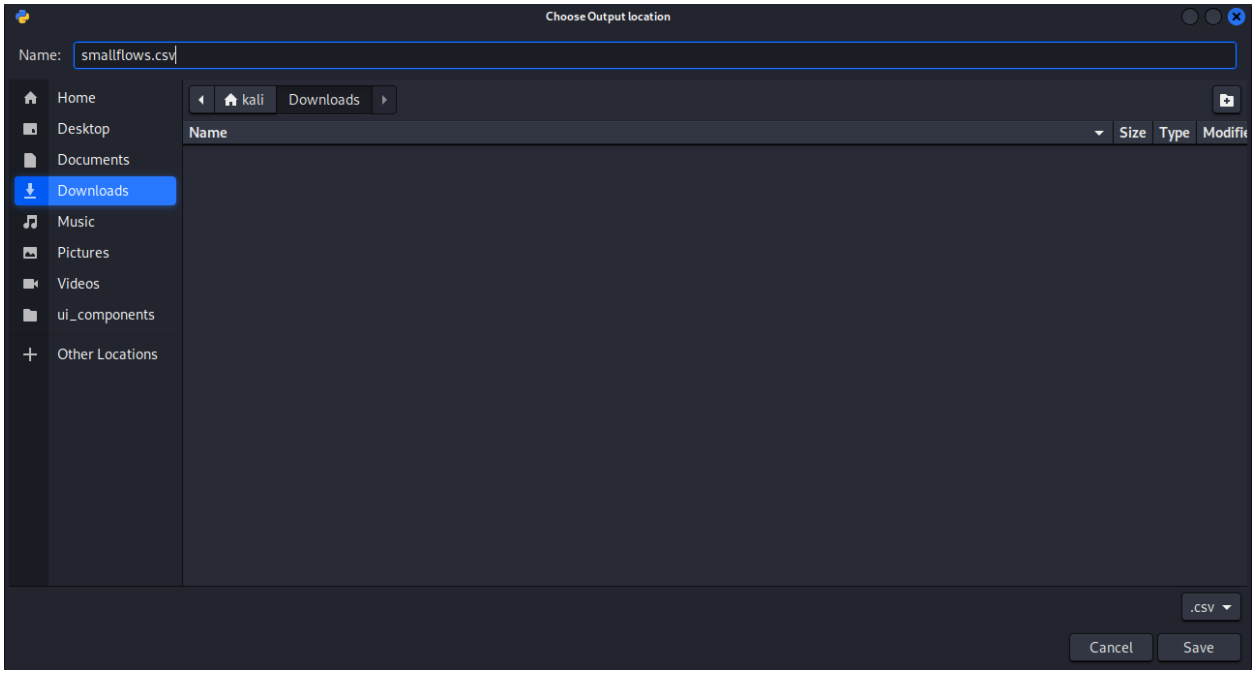
2.2.8 Export to CSV and JSON

The user can export to a CSV and JSON through two ways:

1. Right click on the object and select Export>Export Dataset/Pcap to {CSV or JSON}
2. Through the menu bar at the top, Export>Export Dataset/Pcap to {CSV or JSON}



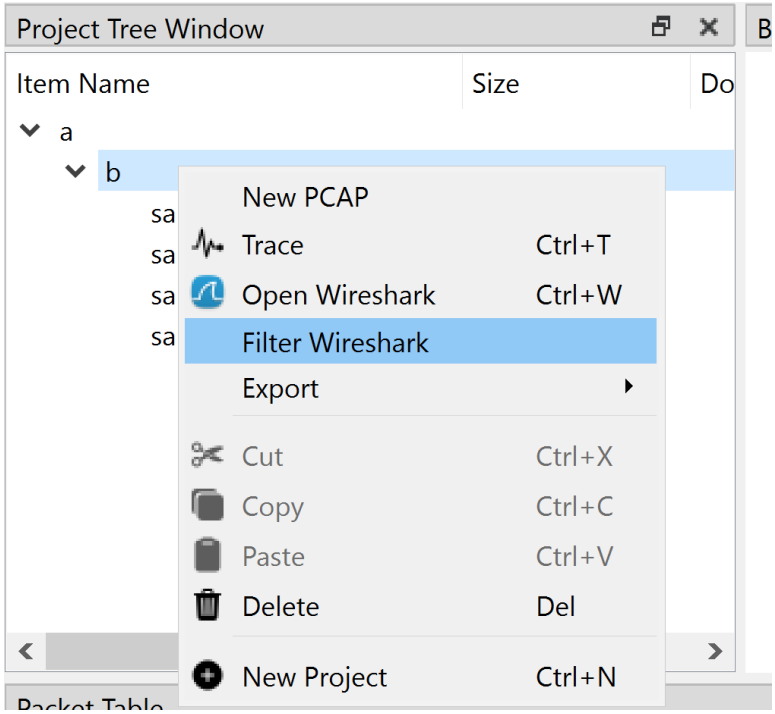
This will prompt the user for the name of the file.



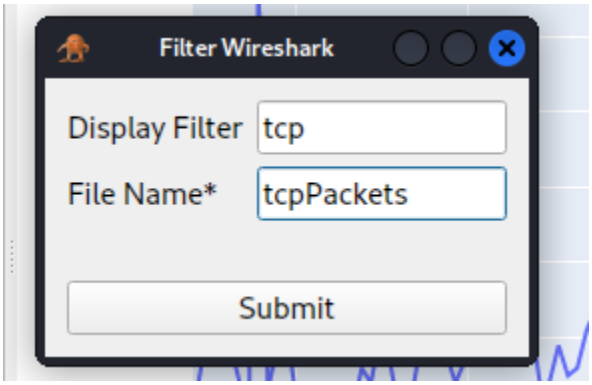
2.2.9 Filter

2.2.9.1 Wireshark

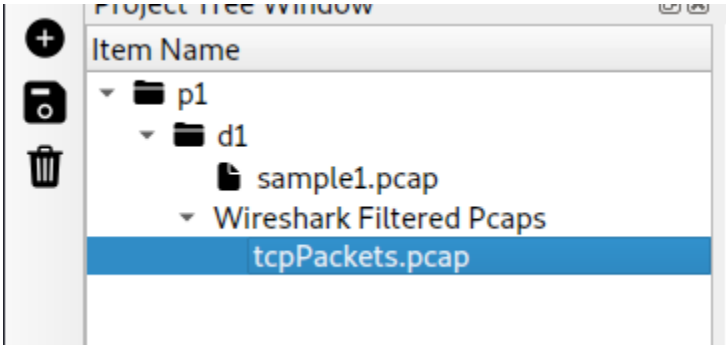
To apply filters to a Dataset simply select the Dataset from the Project Tree and then right click. From the context menu you can choose “Filter Wireshark”.



From there a prompt will be displayed on which the wireshark filter can be entered followed by the name of the pcap you want to create.



The result will be added to the project tree on the left as shown in the image below:

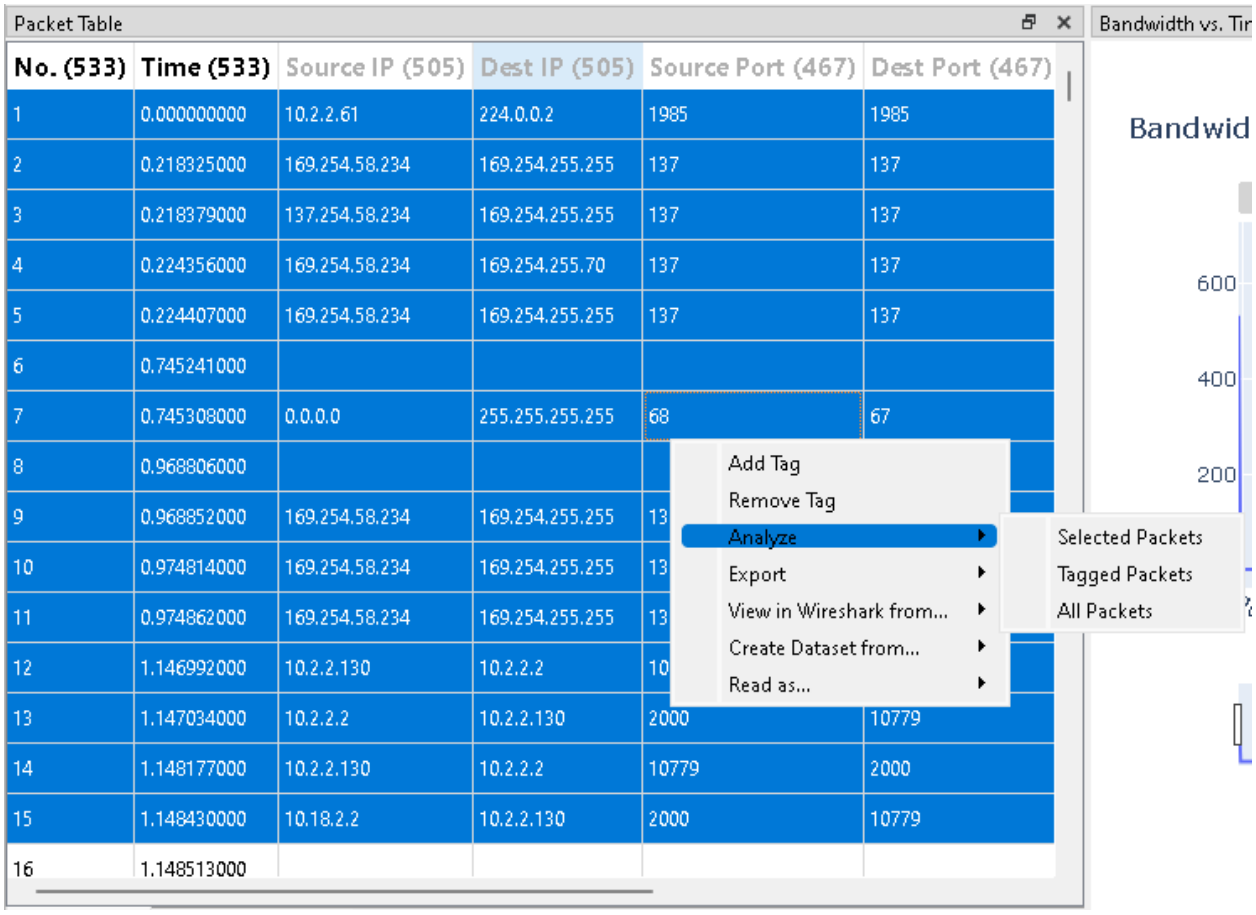


2.2.10 Analysis

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:

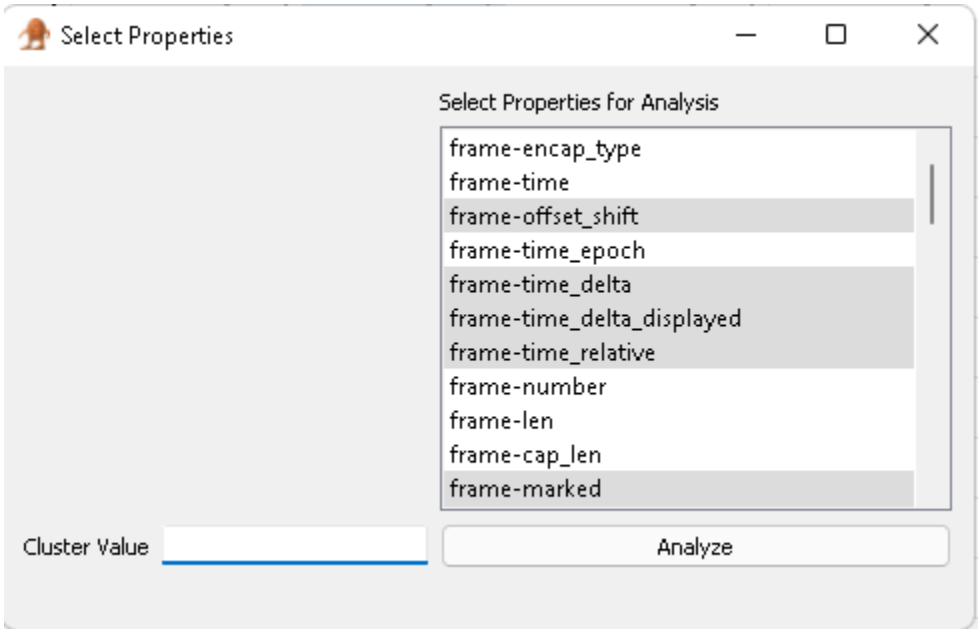
- Analyze Selected Packets
  - User must drag select packets in a given table for this functionality
- Analyze Tagged Packets
  - User must assign a “tag(s)” to the current packet table for this functionality
- Analyze All Packets

The user must right-click on the packet view table to reach the “Analyze” option. Shown below:

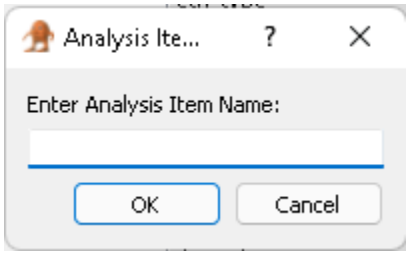


No. (533)	Time (533)	Source IP (505)	Dest IP (505)	Source Port (467)	Dest Port (467)
1	0.000000000	10.2.2.61	224.0.0.2	1985	1985
2	0.218325000	169.254.58.234	169.254.255.255	137	137
3	0.218379000	137.254.58.234	169.254.255.255	137	137
4	0.224356000	169.254.58.234	169.254.255.70	137	137
5	0.224407000	169.254.58.234	169.254.255.255	137	137
6	0.745241000				
7	0.745308000	0.0.0.0	255.255.255.255	68	67
8	0.968806000				
9	0.968852000	169.254.58.234	169.254.255.255	13	
10	0.974814000	169.254.58.234	169.254.255.255	13	
11	0.974862000	169.254.58.234	169.254.255.255	13	
12	1.146992000	10.2.2.130	10.2.2.2	10	
13	1.147034000	10.2.2.2	10.2.2.130	2000	10779
14	1.148177000	10.2.2.130	10.2.2.2	10779	2000
15	1.148430000	10.18.2.2	10.2.2.130	2000	10779
16	1.148513000				

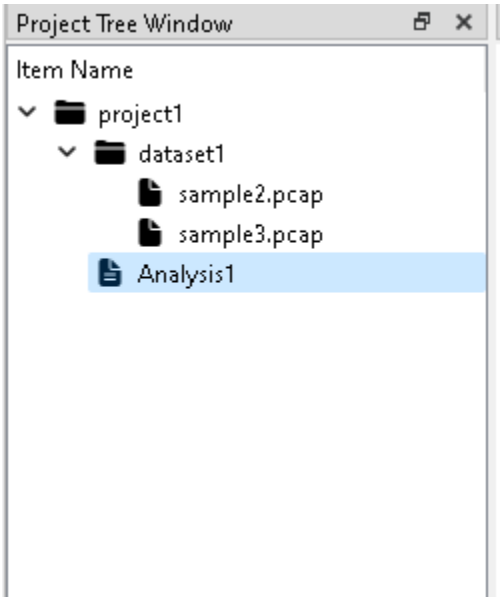
Upon selection of one of the options shown above, the user will be prompted with the following window:



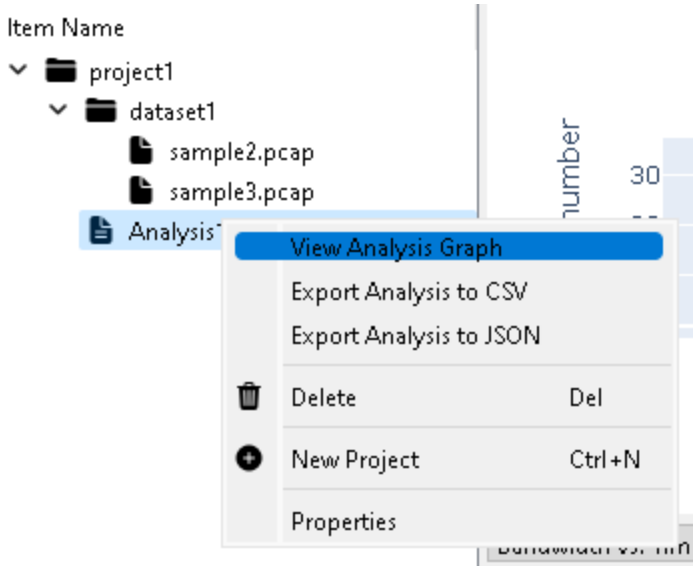
Note: The system currently only supports the K-Means clustering algorithm in which a cluster value is required. The architecture is a plugin architecture and provides an easy way to add algorithms to this window at a later date.



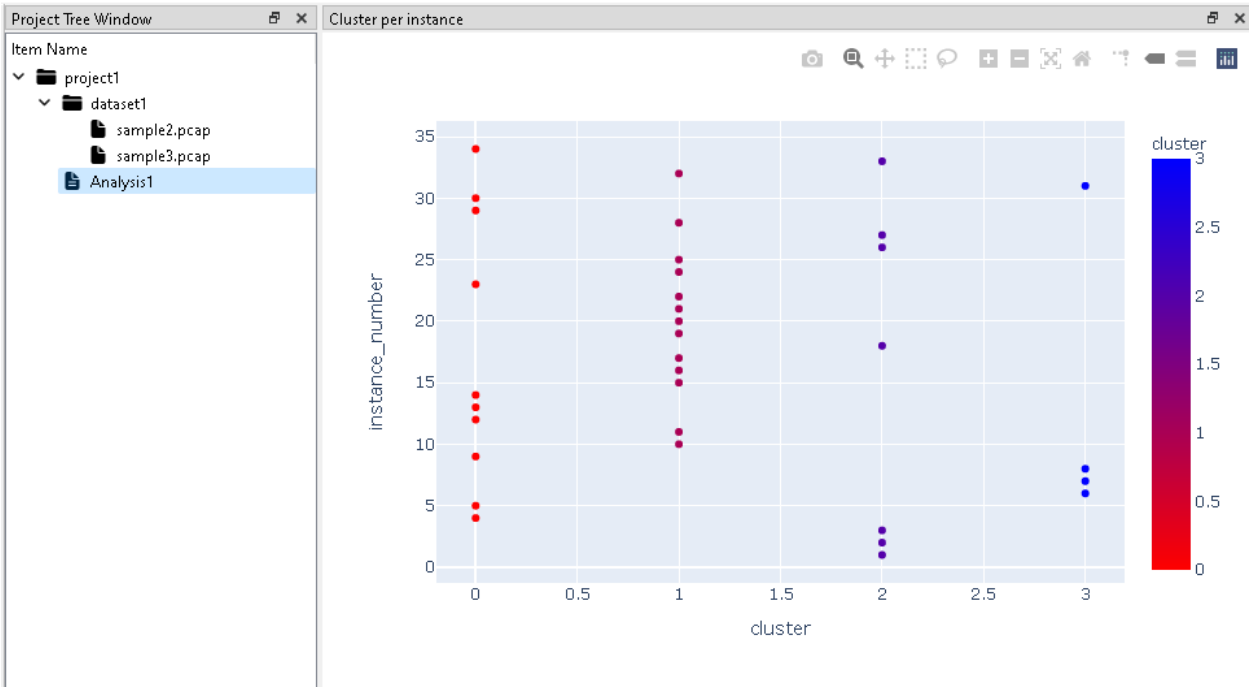
The user will then be prompted to name the analysis item. Upon successful creation of an Analysis, the user will see the Analysis item appear in the project tree, shown below:



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:



2.2.11 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