

Using Wireshark for Packet Captures

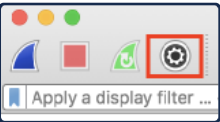
Wireshark is a utility that will display the [packets](#) seen by a device. Packets contain the data that is transmitted between computers. Viewing this information can often aid in the diagnosis of issues that may be occurring in a network. It is possible for a device to not see all packets transmitted on a network if a device is hardwired. In this instance, the device may only see broadcast packets and packets addressed to itself due to the functionality of modern networking equipment.

Installation

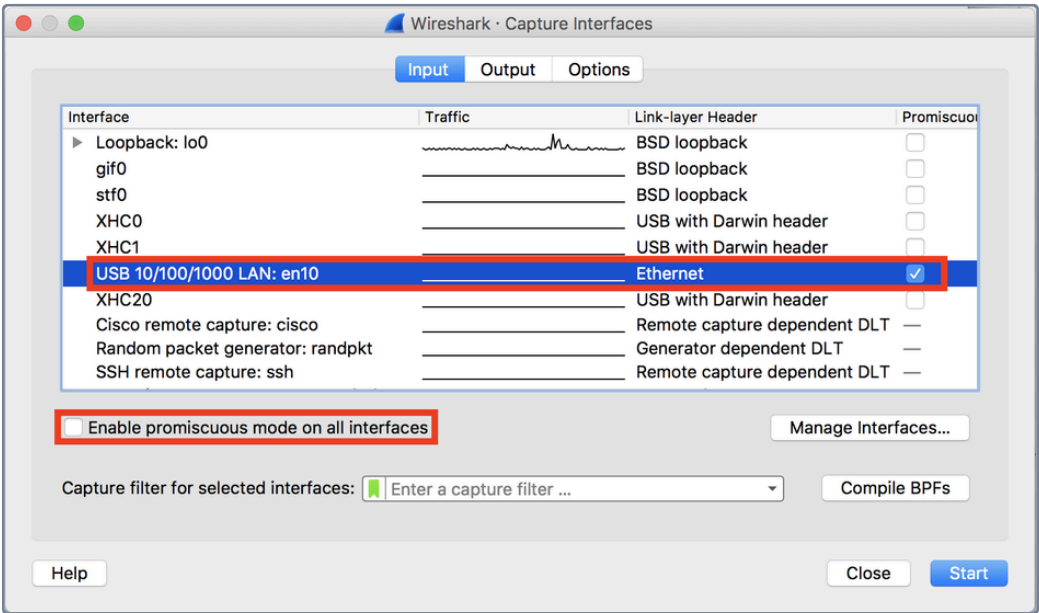
Please visit [Wireshark's download page](#) to download Wireshark. When downloading, simply follow the prompts.

Taking Packet Captures

1. Open Wireshark.
2. Click Capture Options.

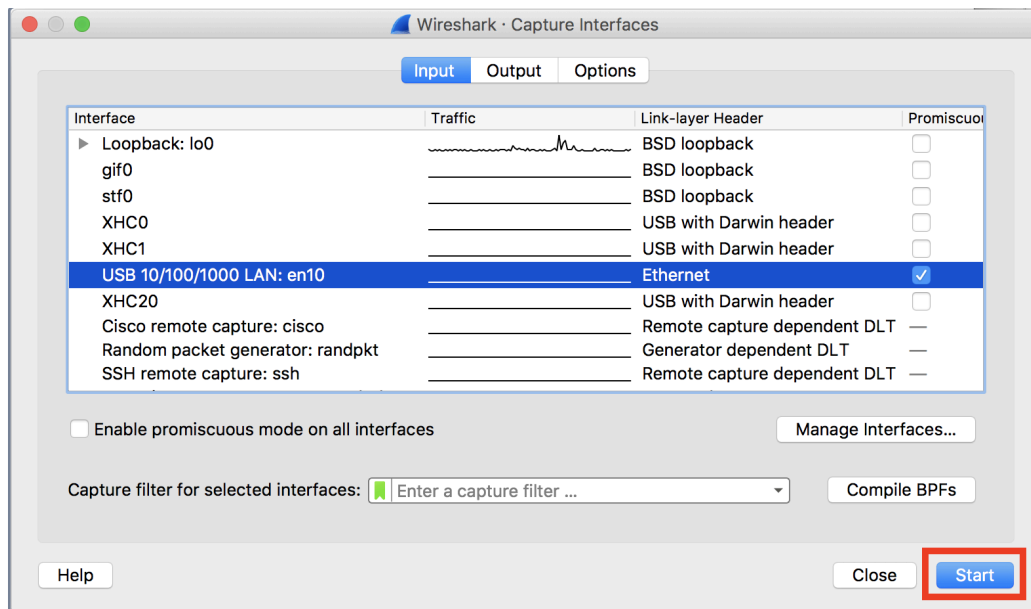


3. Uncheck "Enable promiscuous mode on all interfaces", check the "Promiscuous" option for your capture interface and select the interface.

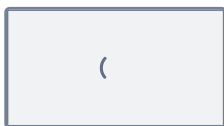


Note: [Rolling captures](#) can be configured if required. This option will allow packets to be captured continuously without filling up the storage on your device.

4. Click start. This will take you to a new window that will show the packets that the device is picking up.



5. When the desired packets have been obtained click stop.



6. Save the capture from the "File menu" with a distinct name.

=====

Rolling Captures

A "Rolling Capture" is a capture which automatically saves the output to files at set intervals and can break up a large capture into multiple smaller files. This can be extremely useful when trying to run a long-term capture for troubleshooting intermittent troubles such as choppy audio on VOIP.

Best Way to Run Rolling Captures

For some issues, it may be necessary to perform port mirrors or span port captures which run for long periods of time until the issue occurs. The goal is to run a capture and once the issue surfaces stop the packet capture. If a packet capture is run for a long duration of time, 6 hours, for example, the .pcap file will be too large for your computer to open as captures larger than 100mb become too difficult to open on some computers. To mitigate this trouble, the capture can be set with multiple different options which makes this easier.

What is the Ring Buffer

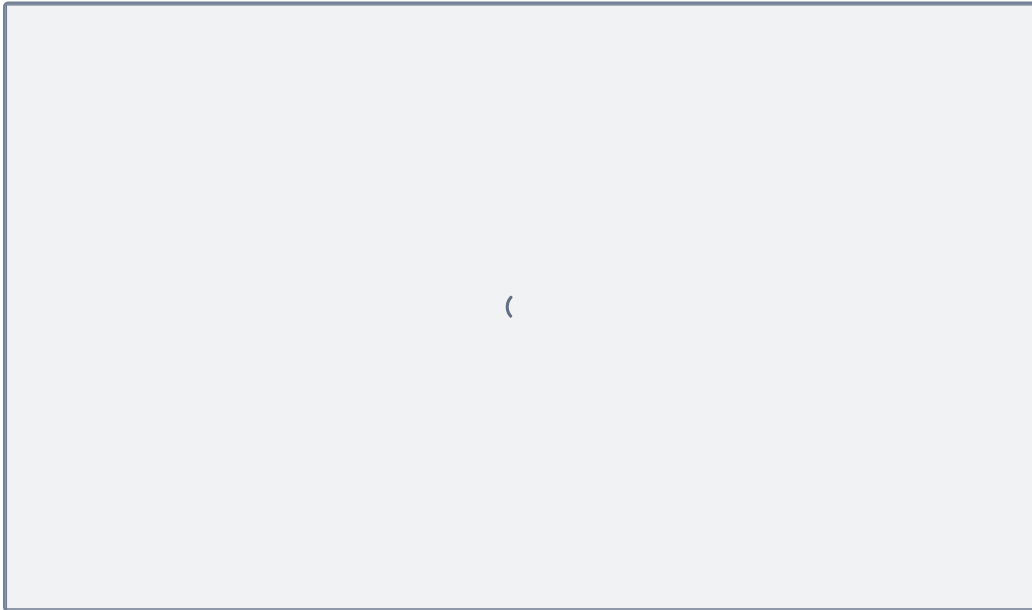
Ring Buffers can be set to ensure that you will not fill up all of the disk space on your device. It will start overwriting the oldest file based off how many files you specify. This does not have to be used, but it is useful to ensure you do not fill up your HDD.

Taking a Rolling Capture

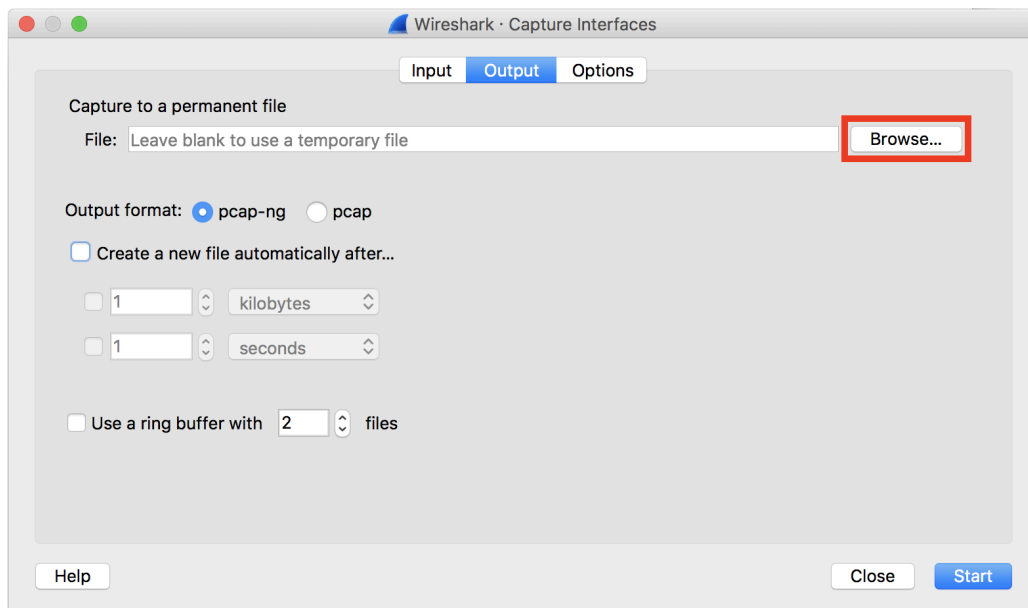
1. Open Wireshark.
2. Click Capture Options.



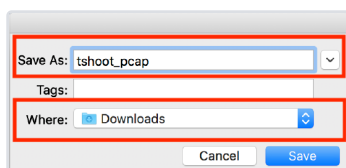
3. Uncheck "Enable promiscuous mode on all interfaces", check the "Promiscuous" option for your capture interface and select the interface.



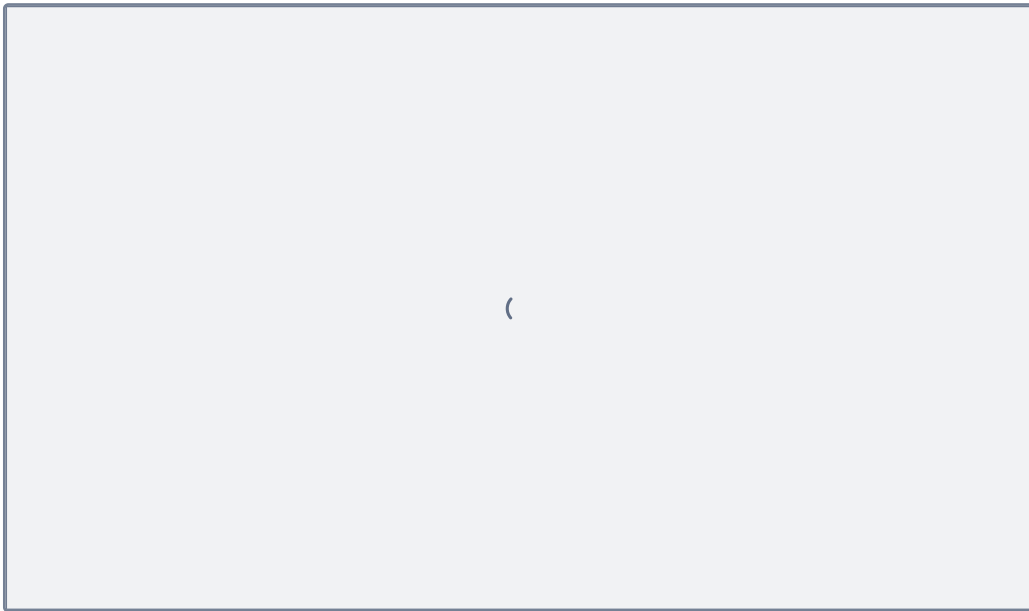
4. In the "Output" tab, click "Browse..."



5. Enter a filename in the "Save As:" field and select a folder to save captures to. Click Save.



6. Select "Create a new file automatically after..." and "Use a ring buffer with x files". This creates a maximum of x number of files, with each file set to the size or timeframe configured. For example, creating a new file automatically after **32 megabytes**, with a ring buffer of **128 files**, will provide **4 gigabytes** of rolling captures.



7. Click start. This will take you to a new window that will show the packets that the device is picking up.

Filtering Packet Captures

In certain instances, it can be beneficial to filter a capture for a specific client's IP address or for a specific type of traffic. This filtering can be done prior to the capture as well as after the capture, however, the filters used in these instances differ.

What is a Capture Filter

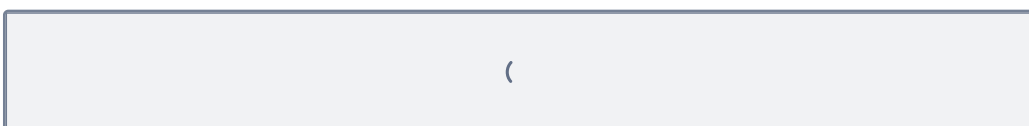
A capture filter is a type of filter which is used to limit the type of data which is captured and saved to the file and is not used as frequently because of this. The syntax for these differs from the Display Filters. Additional information regarding the different filters and syntax which can be used as a Capture Filter can be found in the [Wireshark database](#).

What is a Display Filter

Display filters are the more common type of filter as they do not reduce the type of traffic which is being captured. This eliminates the possibility of having an incorrect filter applied and missing the traffic required in order to troubleshoot. This type of filter is applied inside of Wireshark when viewing the completed capture and outlined below. Additional information regarding the different filters and syntax which can be used as a Display Filter can be found in the [Wireshark database](#).

Using a Display Filter

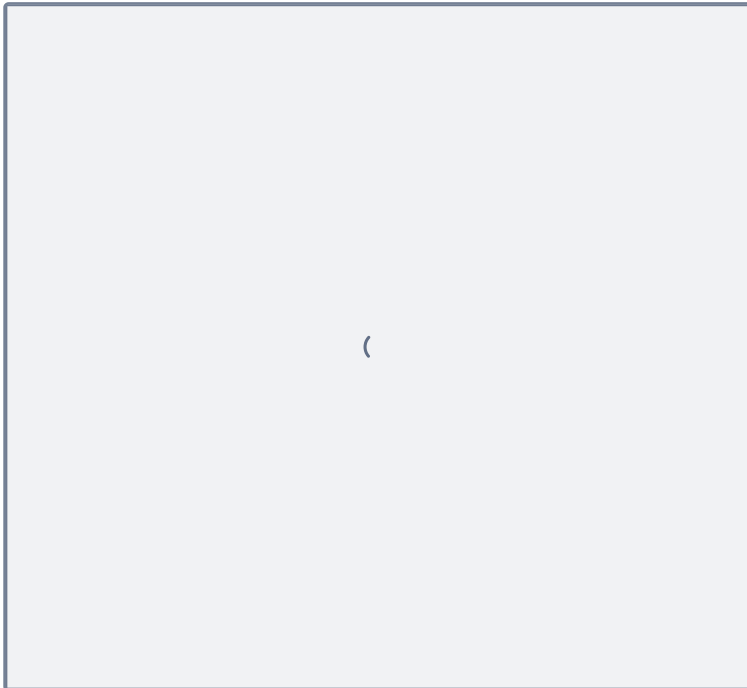
1. Open your packet capture
2. Select the filter box.



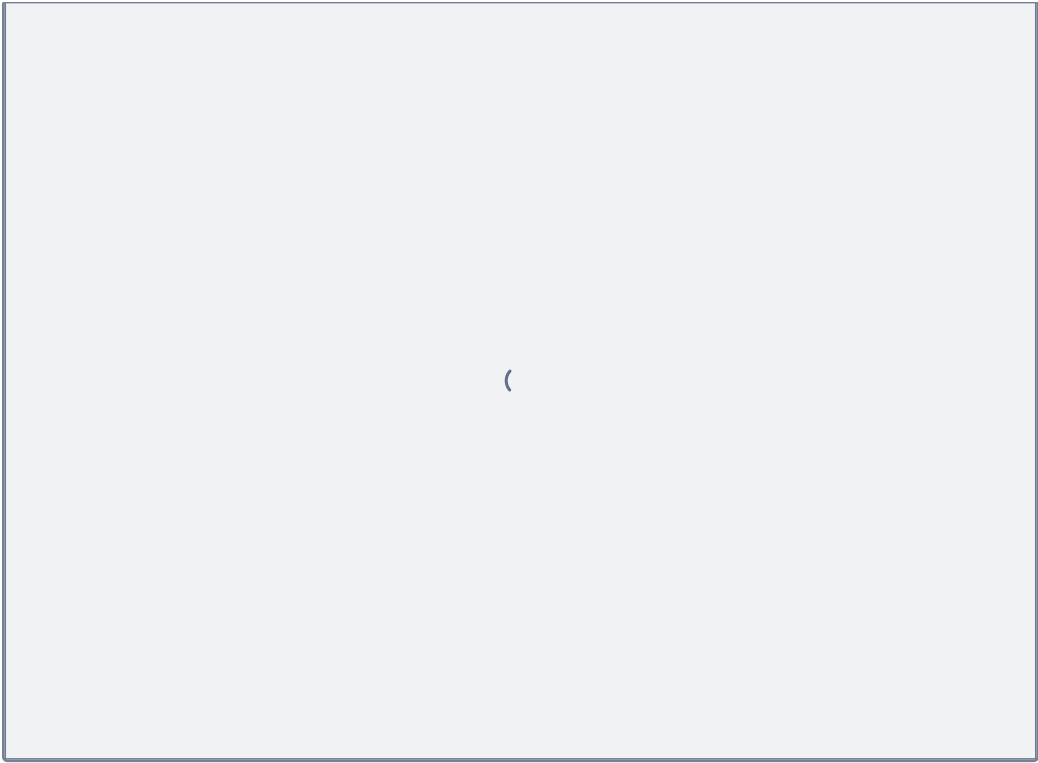
3. Input filter string as provided by support engineer. Click the "Apply" button.



4. To save the filtered data, go to **File -> Export Specified Packets...**



5. Make sure that the "Displayed" radio button is checked and that the file has a unique filename. Once this is complete, select "Save".



Reference: [Using Wireshark for Packet Captures - Cisco Meraki Documentation](#)