# Using Wireshark in GNS3

In this part, you will become familiar with Wireshark and its filter expressions.[[1]](#footnote-1)

**IMPORTANT NOTE:** Whenever you STOP Wireshark Capture and start it again in the same GNS3 project, you HAVE to give the file a NEW NAME. If not, it can hang with the old file name and you won’t capture any traffic.

## Part (A). Starting Wireshark

1. Open GNS3 and set up the project as shown below:

A screenshot of a social media post

Description automatically generated

Figure 1.

1. Start GNS3 using the green play button. Use the command introduced in Lab 1 to set up the PC IP addresses in their console windows.

**PC1%** sudo ip addr add 10.0.1.11/24 dev eth0

**PC2%** sudo ip addr add 10.0.1.12/24 dev eth0

1. Before you start using Wireshark:
   1. For Windows: Make sure that the Packet Capture settings are set to Wireshark Live Traffic Capture from the "Packet Capture" tab under Edit -> Preferences as shown below in Figure 2

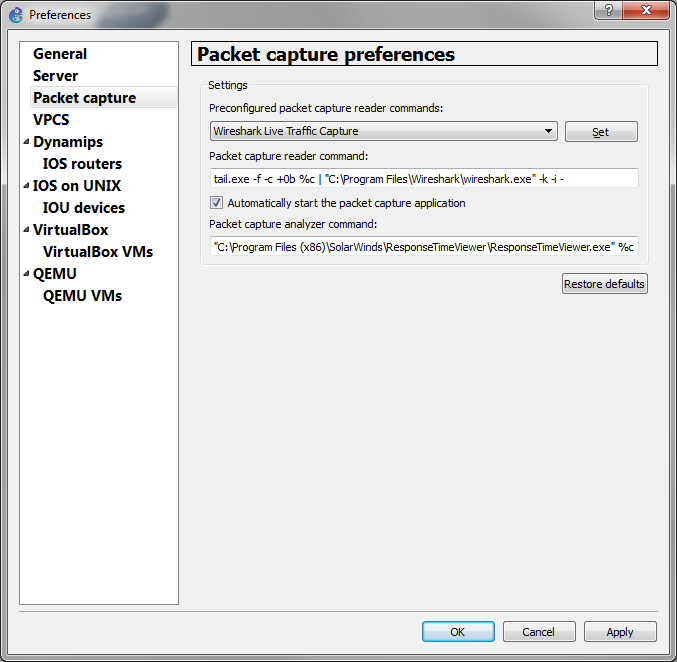


Figure 2. Packet capture Preferences

* 1. For Mac: The packet capture entries should be set under GNS3 -> Preferences as shown in Figure 3.

A screenshot of a cell phone

Description automatically generated

Figure 3 Mac OS Wireshark Settings

1. To start Wireshark Capture, right click[[2]](#footnote-2) on the link that connects PC1 and the Ethernet Hub and select “Start capture”. (If requested, choose option **ETHERNET** (only option available). Then right click on the icon and you will see "Start Wireshark”. The Wireshark Network Analyzer opens in a new window as shown below.

A screenshot of a social media post

Description automatically generated

Figure 4.

1. In the console window of PC1, issue a ping command to PC2:

**PC1%** ping 10.0.1.12 –c 5

1. Stop the capture process by clicking on the red stop button in the Wireshark window.
2. **Saving captured traffic**. You can save the capture as a ‘.pcap’ file by going to File -> Save. You can open this file for data analysis at any time by opening it in the Wireshark application.

## Part (B) Setting display filters

1. Restart the Wireshark capture under a different name, and once again ping PC2 from PC1 as we did before.
2. Now we can add some filters in. Click in the “Apply a display filter…” field.

A screenshot of a computer

Description automatically generated

Figure 5.

1. Type “ip” into the field. Notice how you have a list of options that begin with ip, all of which can be applied to the link between PC1 and the Ethernet Hub. For now select “ip.addr == 10.0.1.11” and press enter.

A screenshot of a computer

Description automatically generated

Figure 6.

A screenshot of a social media post

Description automatically generated

Figure 7.

1. Now notice how you only see the IP packets to and from PC1. This is because you are only viewing packets coming in and out of PC1 who has the IP address “10.0.1.11” as their source or destination.
2. Now let’s try something else. Go back the apply filters bar and change “ip.addr == 10.0.1.11” to “ip.src == 10.0.1.11”. You should now see the following:

A screenshot of a social media post

Description automatically generated

Figure 8.

1. Now only the packets that have PC1’s IP address as the source, meaning the ones sent from PC1, are displayed in Wireshark.
2. Another way you can do this is by right-clicking one the IP packets in the source field with 10.0.1.11 as the source and selecting “Apply as Filter > Selected”.

A screenshot of a computer

Description automatically generated

Figure 9.

1. Doing this in any of the fields will apply that as the filter. Selecting the source field will filter out any packets that weren’t sent from that IP, same applies for destination, time, and length.
2. Click the ‘X’ at the right end of the filters bar to get rid of any filters.
3. You can also apply multiple filters to a Wireshark capture. For example, select “Apply as Filter > Selected” in the Source field of the first line (MAC address op PC1), and then type in the bar the expression “&& arp”. This will show only ARP protocol packets from the MAC address of PC1 (you’ll notice before adding the second expression that it still shows ICMP protocol packets with the source IP “10.0.1.11”).

A screenshot of a social media post

Description automatically generated

Figure 10. Before adding the ARP filter

A screenshot of a social media post

Description automatically generated

Figure 11. After adding the ARP filter

1. If you have any programming or Boolean algebra background, you’ll notice this follows the Boolean logic format of AND (&&) and OR (||) functions to apply multiple filters. This means you can also filter out specific data types, using the NOT function, or the ‘!’ symbol, before typing a filter.
2. To get rid of any packets that the source IP is 10.0.1.11, clear out any current filters you have, and apply the “ip.src == 10.0.1.11” filter, but add an ‘!’ before it, so you have “!ip.src == 10.0.1.11” as a filter. You should see the following:

A screenshot of a social media post

Description automatically generated

Figure 12.

1. Note that this can also be done by right-clicking the source field and selecting “Apply as Filter > Not selected”, as well as the other Boolean operation options from that field.
2. So now that we’ve discussed what filters are and how to apply them, we will discuss how to save filters. Go to the plus sign (+) in the top right corner next to “Expression…” in the filter bar as shown below in Figure 13. A filter field will appear in the window as shown in Figure 14.

A screenshot of a social media post

Description automatically generated

Figure 13.

A screenshot of a social media post

Description automatically generated

Figure 14.

1. You can use this toolbar to save filters for future use in other projects. For example, in order to add the filter we applied in the beginning to see only PC1 traffic, ”ip.addr == 10.0.1.11”, type the expression in the “Filter” field, then type a name for it in the “Label” field, such as PC1.

A screenshot of a cell phone

Description automatically generated

Figure 15.

1. Press OK to save the filter.

A screenshot of a social media post

Description automatically generated

Figure 16.

1. Notice how now there is a PC1 filter you can apply as shown above. Click it to apply it to this Wireshark Capture.

A screenshot of a social media post

Description automatically generated

Figure 17.

1. You can save multiple filters , which can consist of a combination of expressions, using AND and OR functions.
2. All saved filters will remain in Wireshark and will appear every time you start a capture.
3. Take note that you can only apply one saved filter at a time; however, you can take a saved filter, and add onto it once it is displayed in the filter bar, using the Boolean notation.
4. You can remove the PC1 filter and close Wireshark. No need to save the output. Stop and quit GNS3.

1. The filtering capabilities and options of Wireshark are described under the help tab in Wireshark. [↑](#footnote-ref-1)
2. Reminder: Right Click on MAC is two fingers tap on track pad. [↑](#footnote-ref-2)