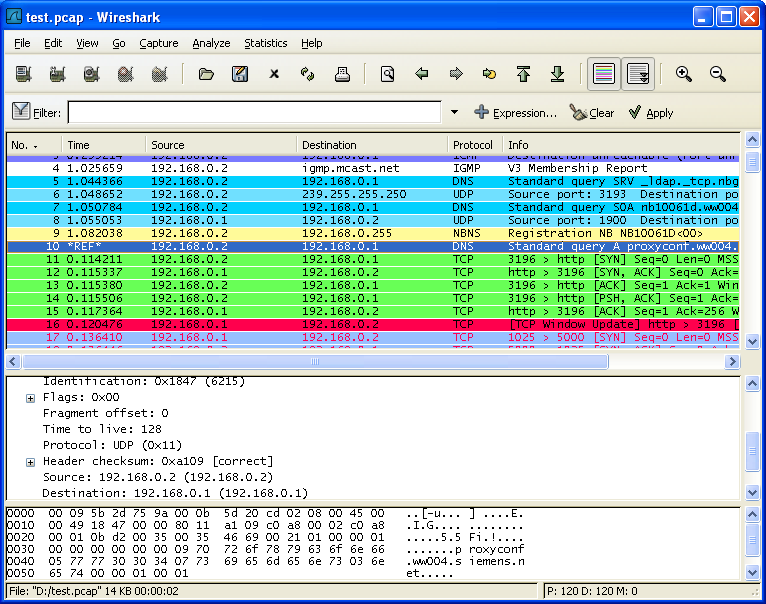
**Wireshark**

**Capture output**



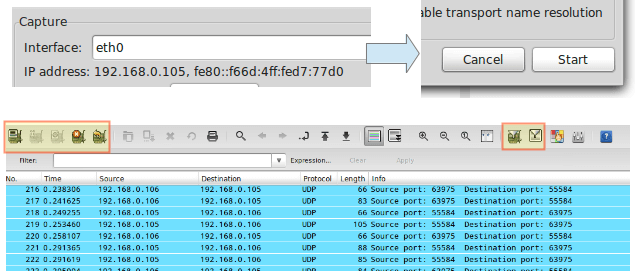
**Setting Capture Options**

The most useful capture options we will consider are:

1. **Network interface** – As we explained before, we will only analyze packets coming through **eth0**, either incoming or outcoming.
2. **Capture filter** – This option allows us to indicate what kind of traffic we want to monitor by port, protocol, or type.

Before we proceed with the tips, it is important to note that some organizations forbid the use of **Wireshark** in their networks. That said, if you are not utilizing Wireshark for personal purposes make sure your organization allows its use.

For the time being, just select eth0 from the dropdown list and click **Start** at the button. You will start seeing all traffic passing through that interface. Not really useful for monitoring purposes due to the high amount of packets inspected, but it’s a start.

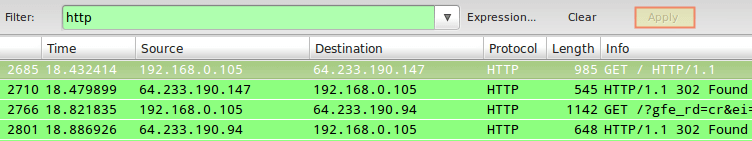
[](https://www.tecmint.com/wp-content/uploads/2012/08/Monitor-Network-Interface-Traffic.png)Monitor Network Interface Traffic

In the above image, we can also see the **icons** to list the available interfaces, to **stop** the current capture, and to **restart** it (red box on the **left**) and to configure and edit a filter (red box on the **right**). When you hover over one of these icons, a tooltip will be displayed to indicate what it does.

We will begin by illustrating capture options, whereas tips **#7** through **#10** will discuss how to do actually do something useful with a capture.

**#1 – Inspect HTTP Traffic**

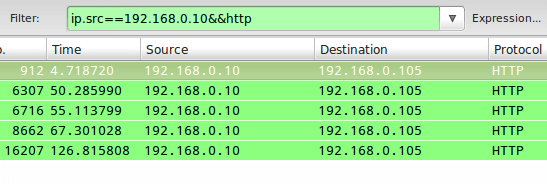
Type http in the filter box and click **Apply**. Launch your browser and go to any site you wish:

[](https://www.tecmint.com/wp-content/uploads/2012/08/Inspect-HTTP-Network-Traffic-.png)Inspect HTTP Network Traffic

To begin every subsequent tip, stop the live capture and edit the capture filter.

**#2 – Inspect HTTP Traffic from a Given IP Address**

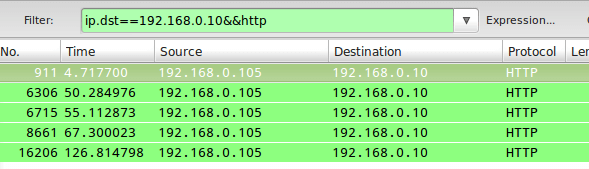
In this particular tip, we will prepend ip==192.168.0.10&& to the filter stanza to monitor HTTP traffic between the local computer and **192.168.0.10**:

[](https://www.tecmint.com/wp-content/uploads/2012/08/Inspect-HTTP-Traffic-on-IP-Address.png)Inspect HTTP Traffic on IP Address

**#3 – Inspect HTTP Traffic to a Given IP Address**

Closely related with **#2**, in this case, we will use ip.dst as part of the capture filter as follows:

ip.dst==192.168.0.10&&http

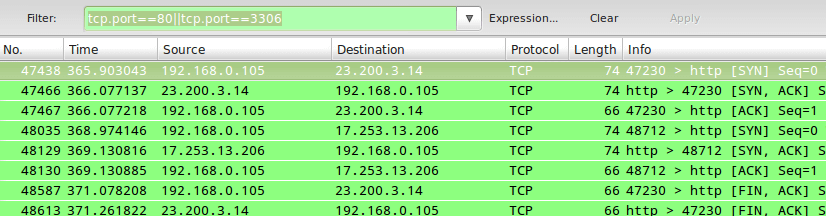
[](https://www.tecmint.com/wp-content/uploads/2012/08/Monitor-HTTP-Network-Traffic-to-IP.png)Monitor HTTP Network Traffic to IP Address

To combine tips **#2** and **#3**, you can use ip.addr in the filter rule instead of ip.src or ip.dst.

**#4 – Monitor Apache and MySQL Network Traffic**

Sometimes you will be interested in inspecting traffic that matches either (or both) conditions whatsoever. For example, to monitor traffic on TCP ports **80** (webserver) and **3306** (MySQL / MariaDB database server), you can use an OR condition in the capture filter:

tcp.port==80||tcp.port==3306

[](https://www.tecmint.com/wp-content/uploads/2012/08/Monitor-Apache-and-MySQL-Traffic.png)Monitor Apache and MySQL Traffic

In tips **#2** and **#3**, || and the word **or** produce the same results. Same with && and the word **and**.

**TIP #5 – Reject Packets to Given IP Address**

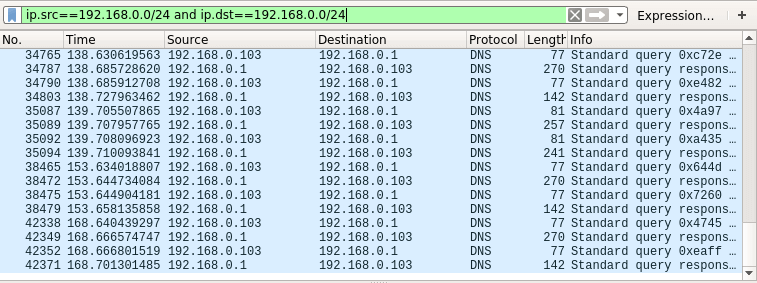
To exclude packets not matching the filter rule, use ! and enclose the rule within parentheses. For example, to exclude packages originating from or being directed to a given IP address, you can use:

!(ip.addr == 192.168.0.10)

**TIP #6 – Monitor Local Network Traffic (192.168.0.0/24)**

The following filter rule will display only local traffic and exclude packets going to and coming from the Internet:

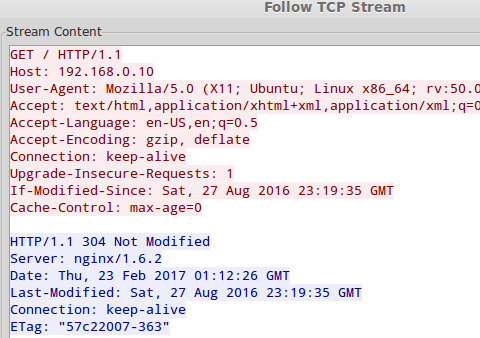
ip.src==192.168.0.0/24 and ip.dst==192.168.0.0/24

[](https://www.tecmint.com/wp-content/uploads/2012/08/Monitor-Local-Network-Traffic.png)Monitor Local Network Traffic

**TIP #7 – Monitor the Contents of a TCP Conversation**

To inspect the contents of a **TCP** conversation (data exchange), right-click on a given packet and choose Follow **TCP** stream. A window will pop-up with the content of the conversation.

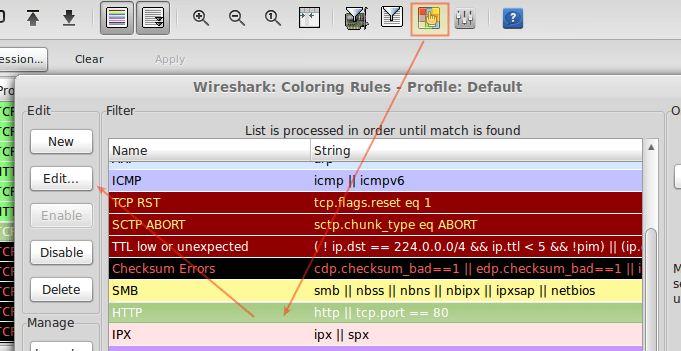
This will include **HTTP** headers if we are inspecting web traffic, and also any plain text credentials transmitted during the process if any.

[](https://www.tecmint.com/wp-content/uploads/2012/08/Monitor-TCP-Conversation.png)Monitor TCP Conversation

**TIP #8 – Edit Coloring Rules**

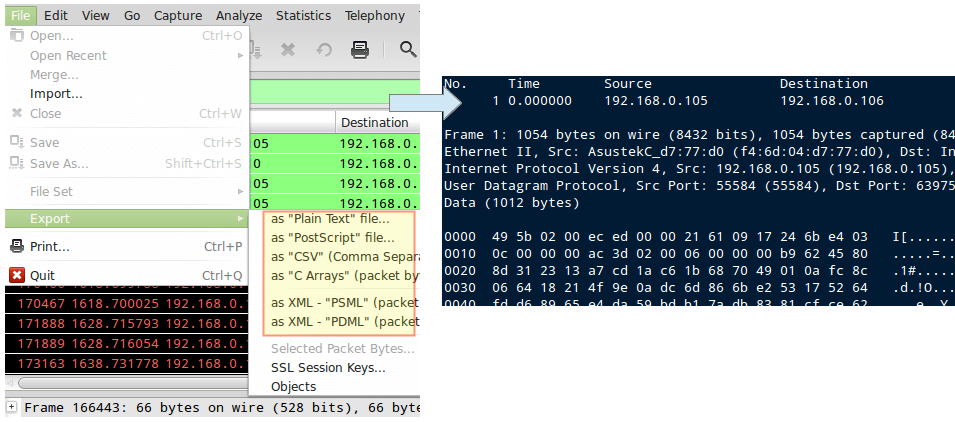
By now I am sure you already noticed that each row in the capture window is colored. By default, **HTTP** traffic appears in the **green** background with black text, whereas **checksum** errors are shown in **red** text with a black background.

If you wish to change these settings, click the **Edit** coloring rules icon, choose a given filter, and click **Edit**.

[](https://www.tecmint.com/wp-content/uploads/2012/08/Customize-Wireshark-Output-in-Colors.png)Customize Wireshark Output in Colors

**TIP #9 – Save the Capture to a File**

Saving the contents of capture will allow us to be able to inspect it with greater detail. To do this, go to **File → Export** and choose an export format from the list:

**[](https://www.tecmint.com/wp-content/uploads/2012/08/Save-Wireshark-Capture-to-File.png)**