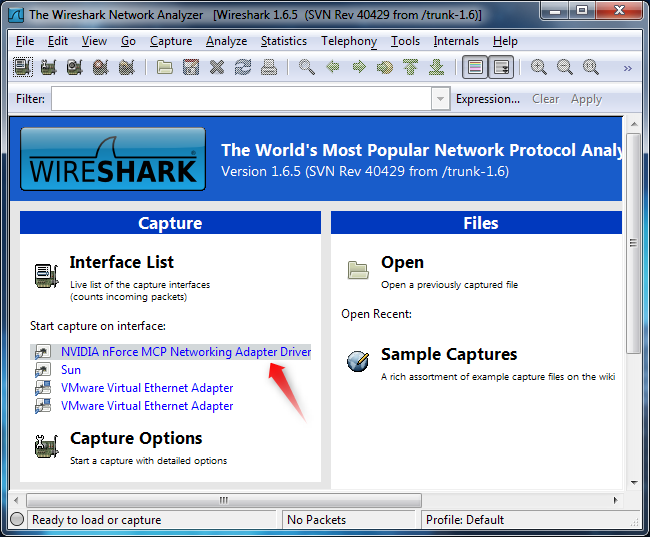
**1.Introduction**

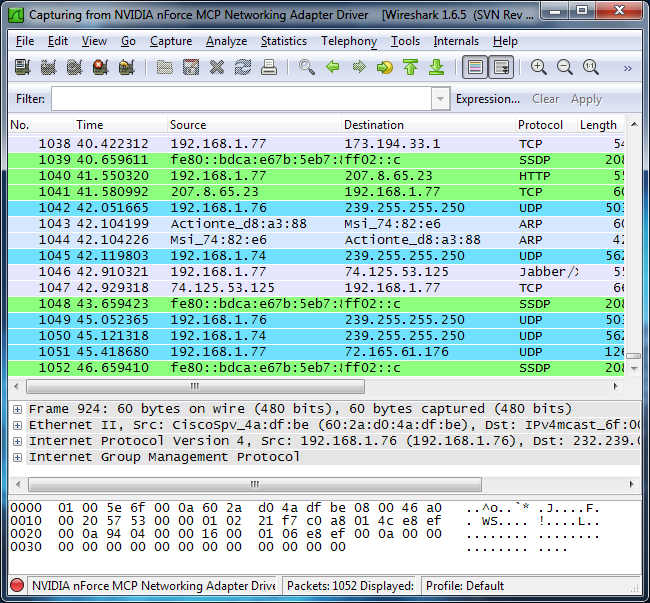
Wireshark, a network analysis tool to capture packets in real time and display them in readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

Wireshark installer can be downloaded for Windows or Mac OS X from <http://www.wireshark.org/download.html>

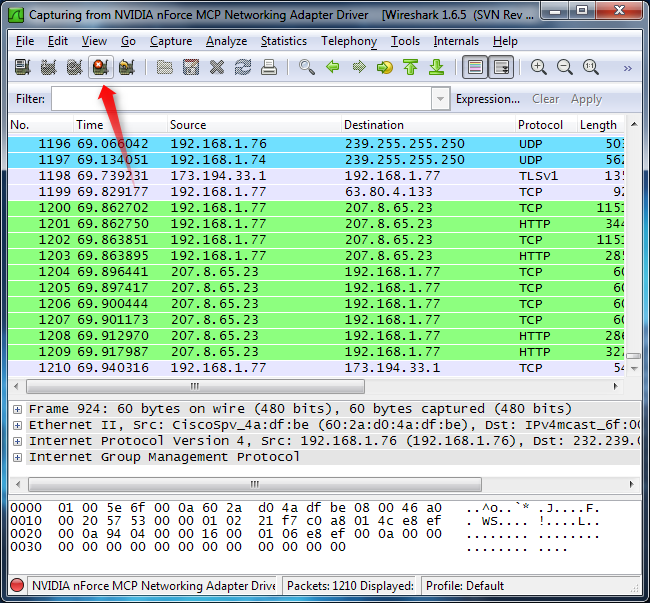
**Capturing Packets**

After downloading and installing Wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options, but this isn’t necessary for now.



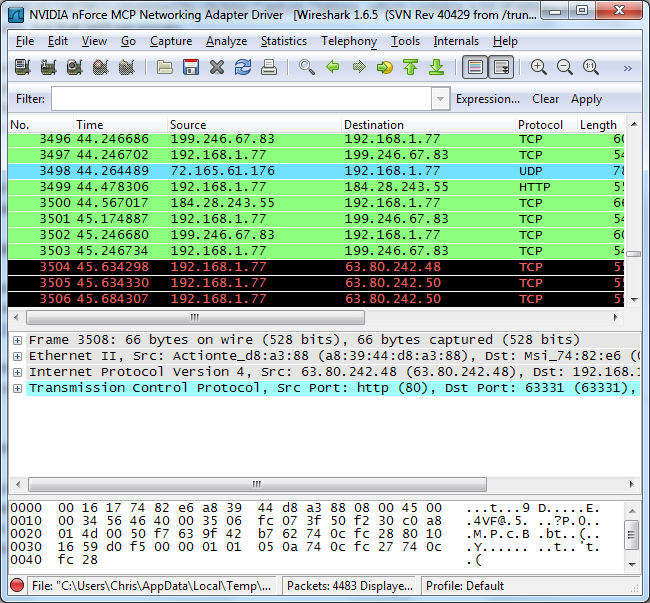
As soon as you click the interface’s name, you’ll see the packets start to appear in real time. Wireshark captures each packet sent to or from the system it is installed

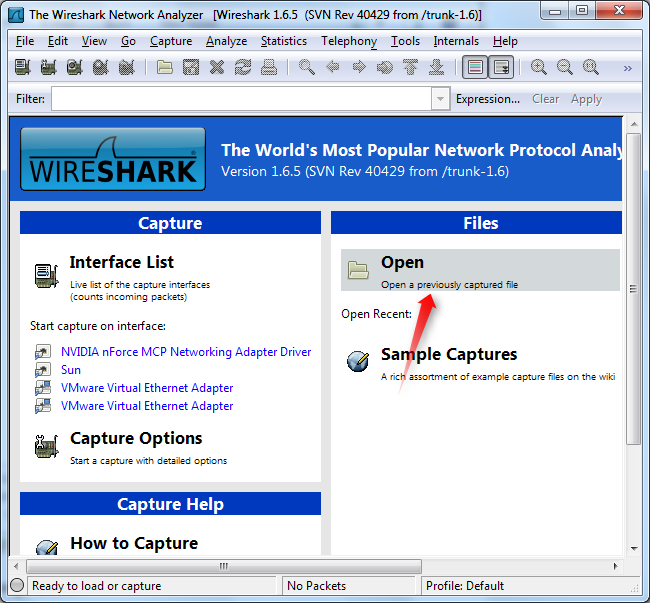
Click the stop capture button near the top left corner of the window when you want to stop capturing traffic.



**Colour Coding**

You’ll see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

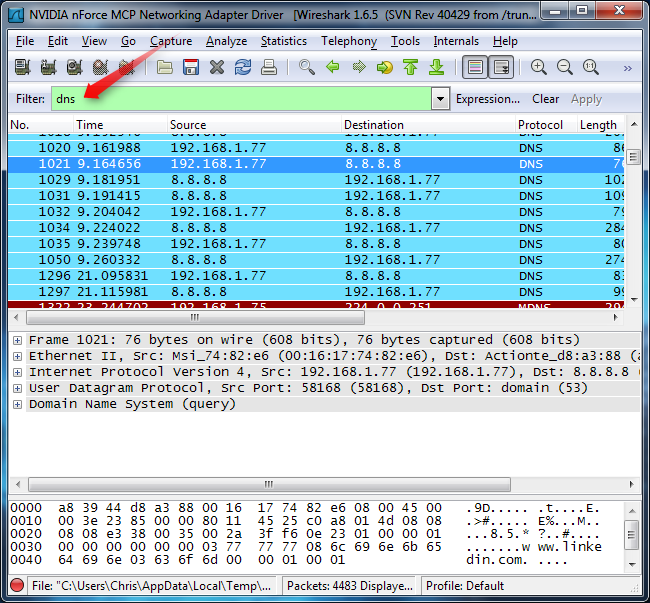




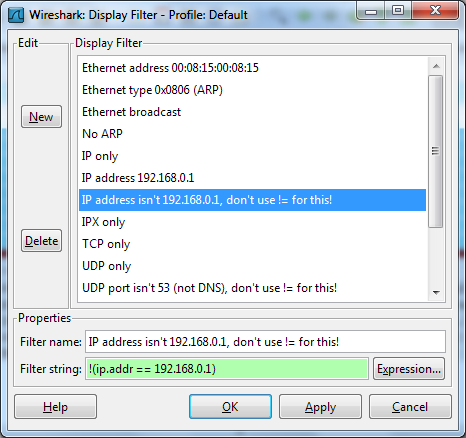
**Filtering Packets**

If you’re trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you’ll likely have a large amount of packets to sift through. That’s where Wireshark’s filters come in.

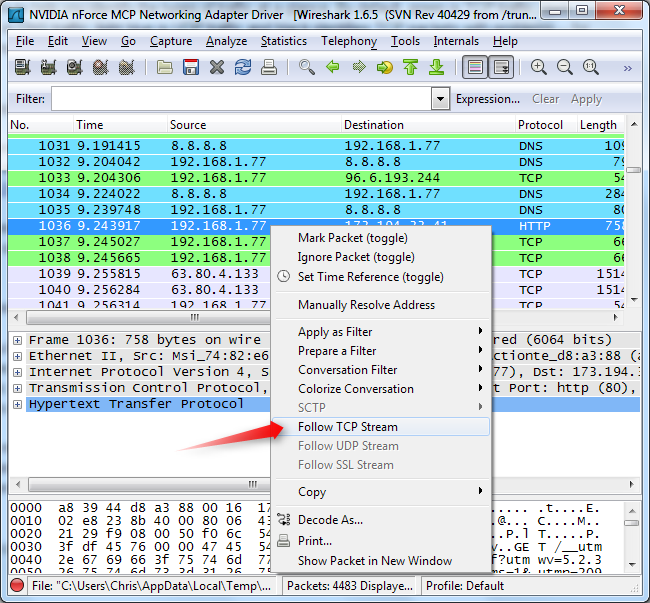
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type “dns” and you’ll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



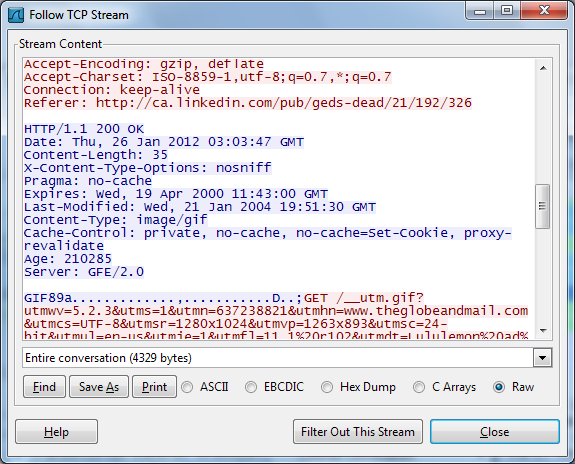
You can also click the Analyze menu and select Display Filters to create a new filter.



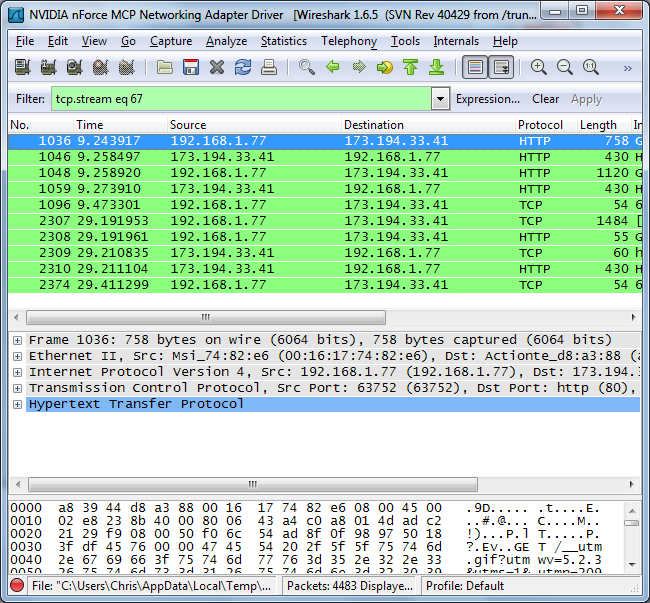
One way to get into details of a particular request is to select the packet and select Follow TCP Stream.



You’ll see the full conversation between the client and the server.

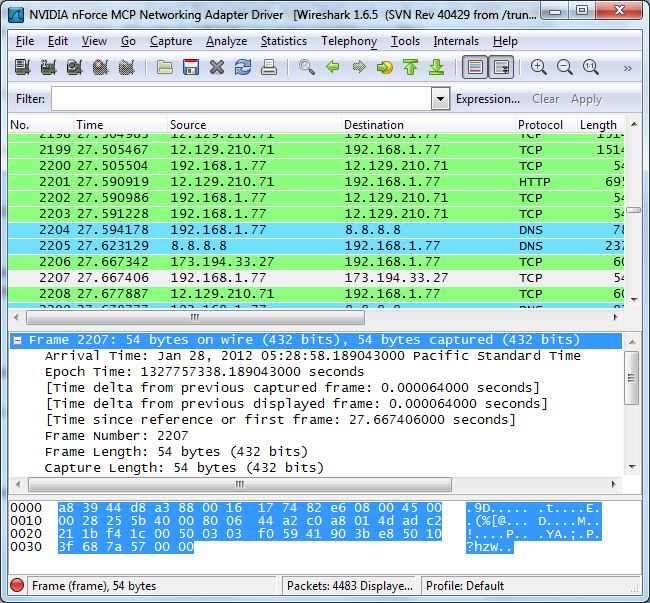


Close the window and you’ll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

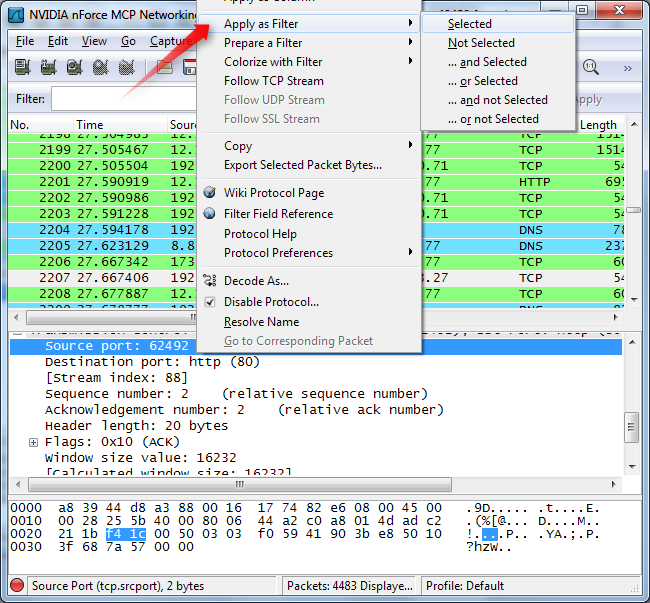


**Inspecting Packets**

Click a packet to select it and you can dig down to view its details.



You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.

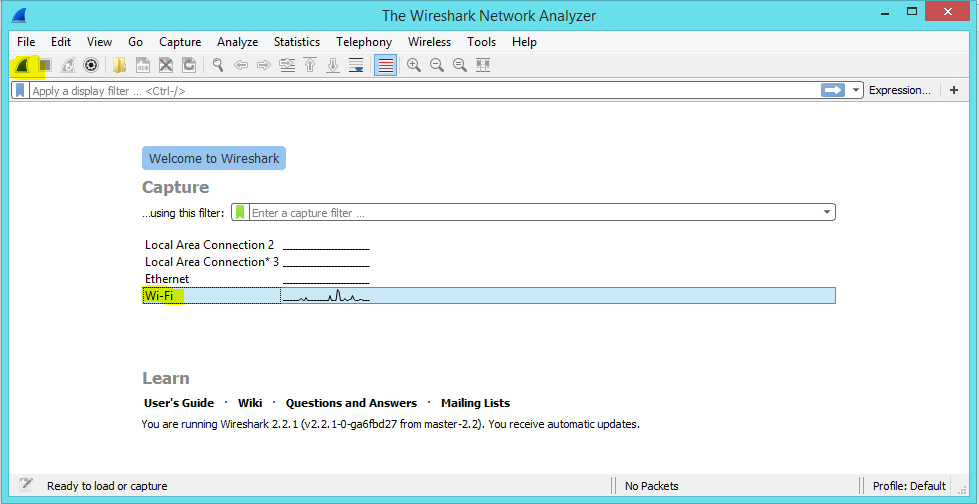


1. **Using Wireshark latest version**

You may download it from: <https://www.wireshark.org/download.html>

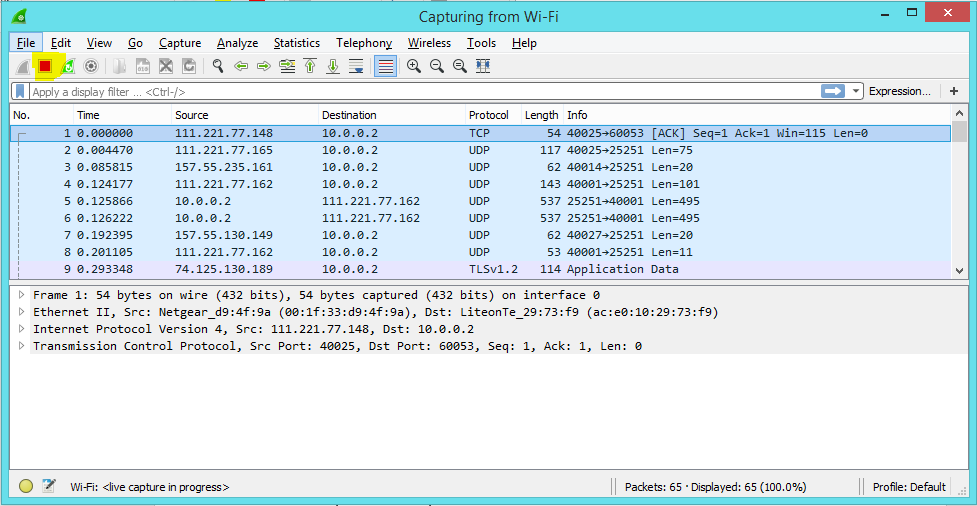
Stable Release 2.2.1

1. Open Wireshark

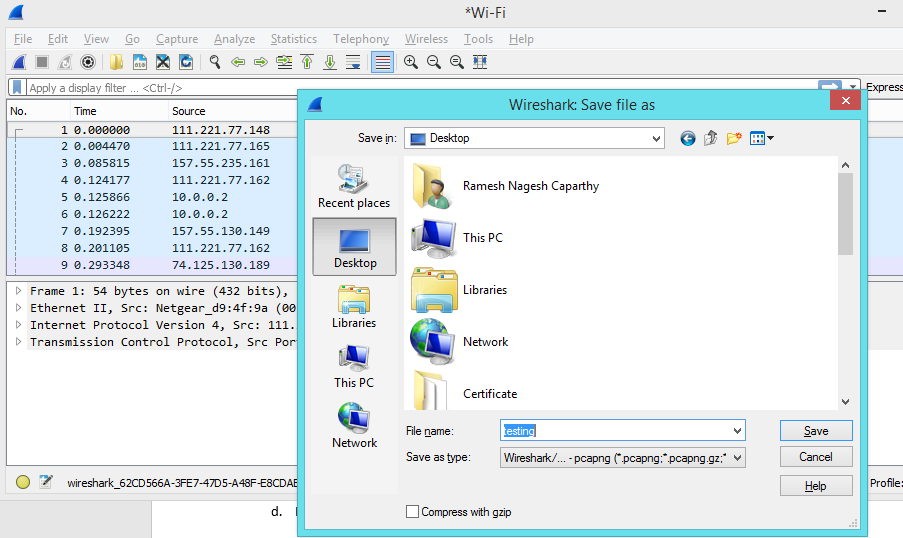


Note: To start the Wireshark packet capture, select the respective connection to your laptop. In our case it is Wi-Fi, after you select it, click on start “Start capturing packets” as marked above.

1. You will now be able to see the packets capturing in Wireshark. Open Windows application and try to connect to your SMP Server.
2. Now click on Stop after you receive error message from windows application



1. Now click on File and Save As, give a name to save the packet capture results.



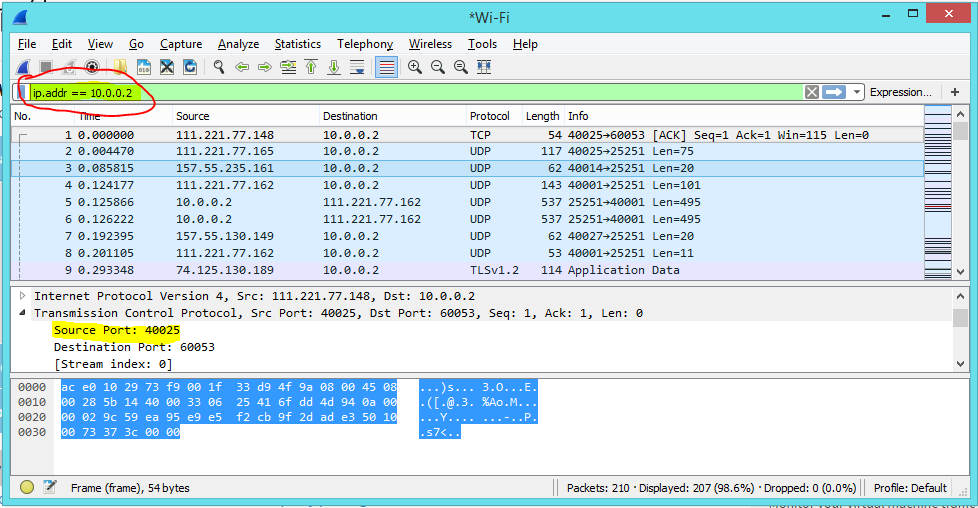
Now this file can be used for understanding the issue.

1. Within the same file you may filter the IP address to understand the traffic from HCP to Hana Cloud Connector and Hana Cloud Connector to SAP Gateway system.

Pre-requisite:

* HCP IP Address
* Hana Cloud Connector IP Address
* SAP Gateway IP Address

Follow the syntax below to filter:



Detailed packets will help us to understand the Traffic issues from laptop to server.