Packet Analysis (Wireshark)

Practical 3

UCD School of Computer Science

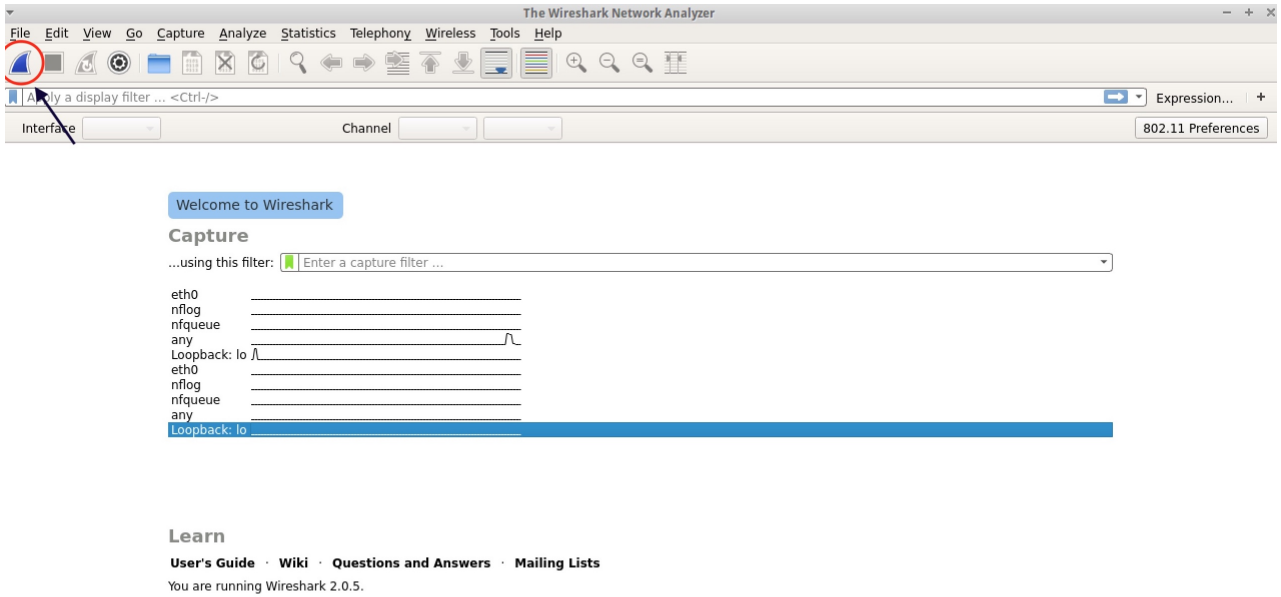
October 1, 2018

0. Introduction

- `Wireshark` is an extremely powerful tool to debug network protocol implementations, examine security problems and inspect network protocol internals.
- Download Wireshark https://www.wireshark.org/download.html
- Warning: Many organizations don't allow Wireshark and similar tool on their networks. Don't use this tool at work unless you have permission.

1. Capturing Packets

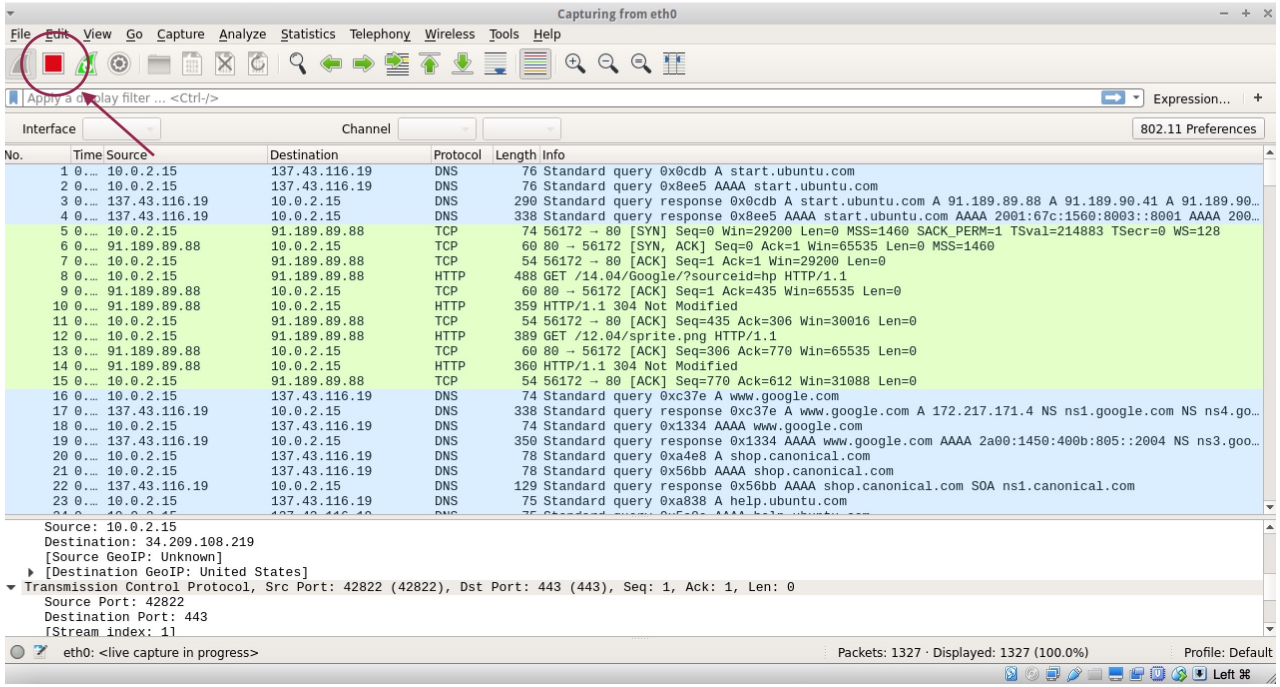
- Launching Wireshark → Choose network interface that you want to scan (For example: `eth0` in your VM)



- 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/FROM your system.

1. Capturing Packets - Cont

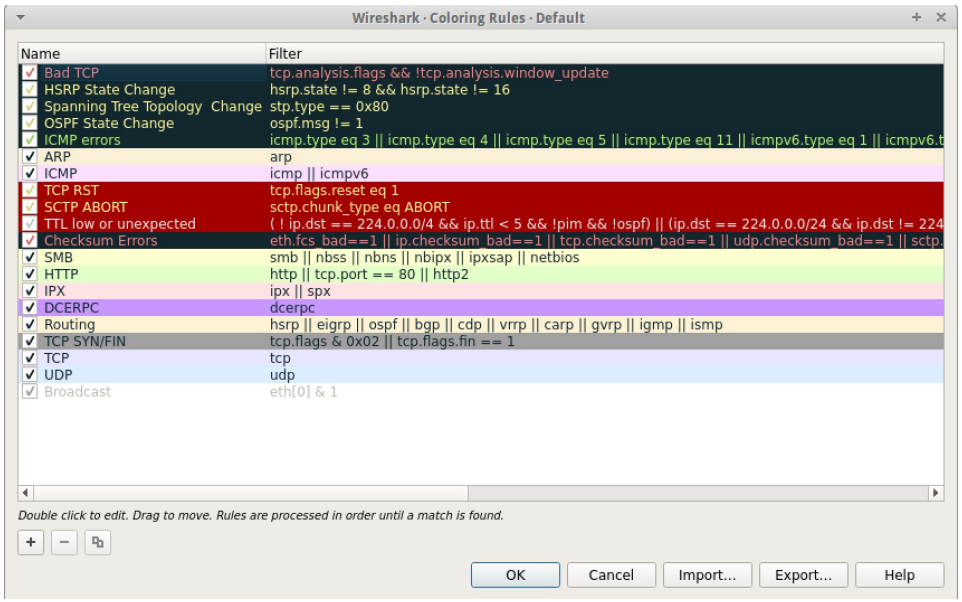
- To stop scanning → Click on `Stop` symbol or using shortcut `Ctrl+E`



- 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/FROM your system.

2. Color Coding

- Wireshark uses colors to highlight traffic type at a glance. For example (Click on **View** → **Coloring rules ...**



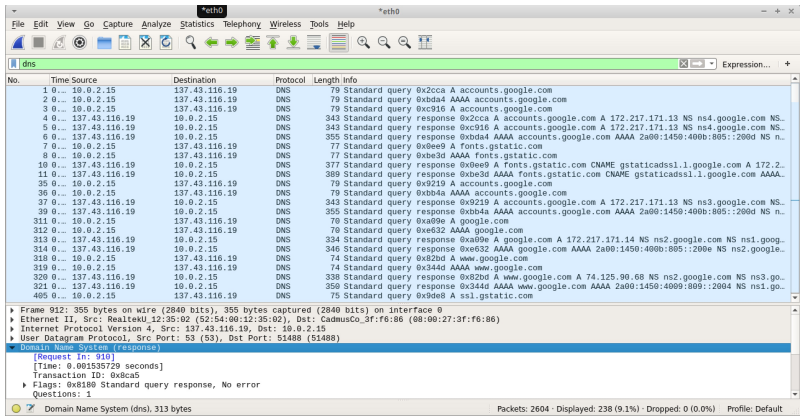
- Read more about Packet Colorization https://www.wireshark.org/docs/wsug_html_chunked/ChCustColorizatio

3. Sample Captures

- If there is nothing interesting on your own network to inspect, $\rightarrow$ Go to **Sample Capture**, Wishark's wiki contains a page of sample capture files that you can load and inspect.
- To open a captured file: Click on **File** $\rightarrow$ **Open** (Be sure that you stop capturing before opening file)

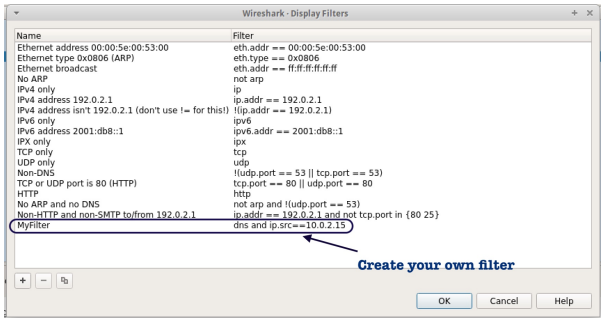
4. Filtering Packets

- If you are 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. BUT, you likely have a large amount of packets to sift through → Wireshark's filter can help
- The most basic way to apply filter is by typing it into the filter box at the top of window and clicking **Apply** (or pressing **Enter**). For example, I want to filter `dns` traffic

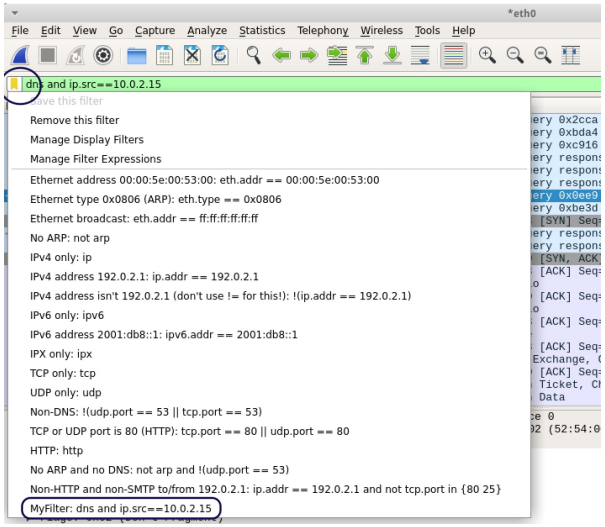


4. Filtering Packets - Cont

- Another way to apply filter: Click **Analyze** → Choose **Display Filters** to create a new filter

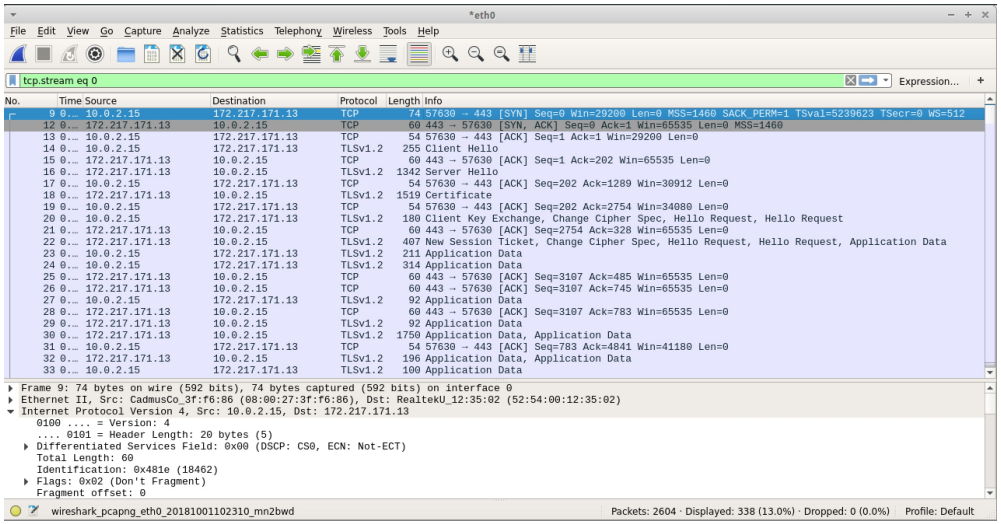


- To apply filter



4. Filtering Packets - Cont

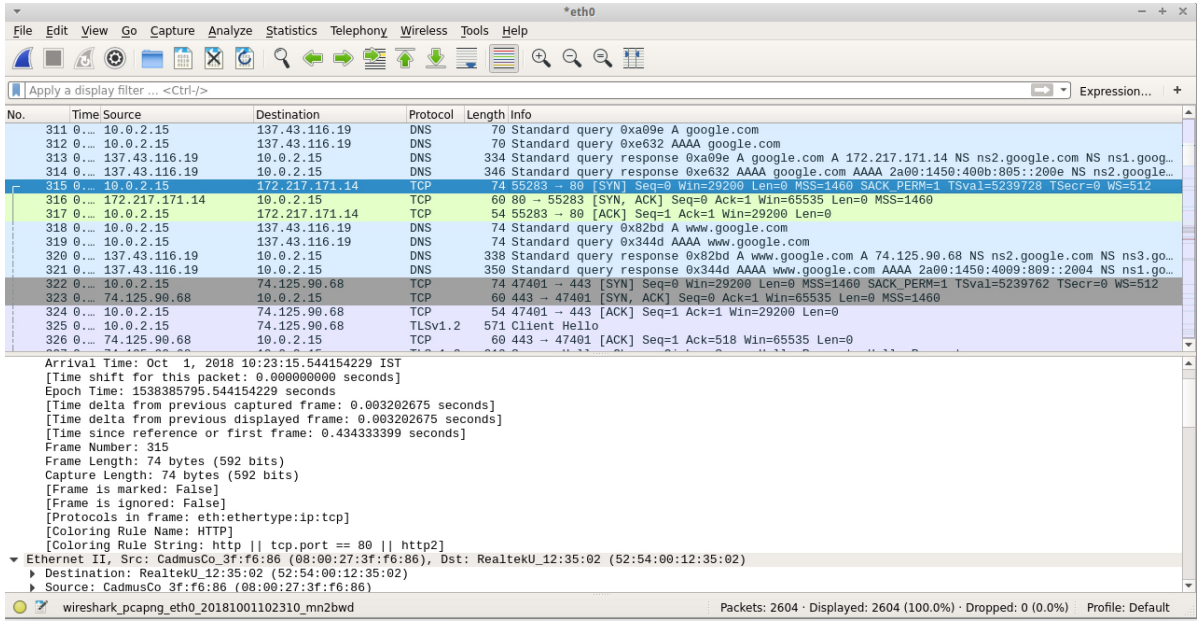
- Another interesting thing you can do is right-click a packet and select **Follow TCP Stream**



- You'll then see the full conversation between 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.

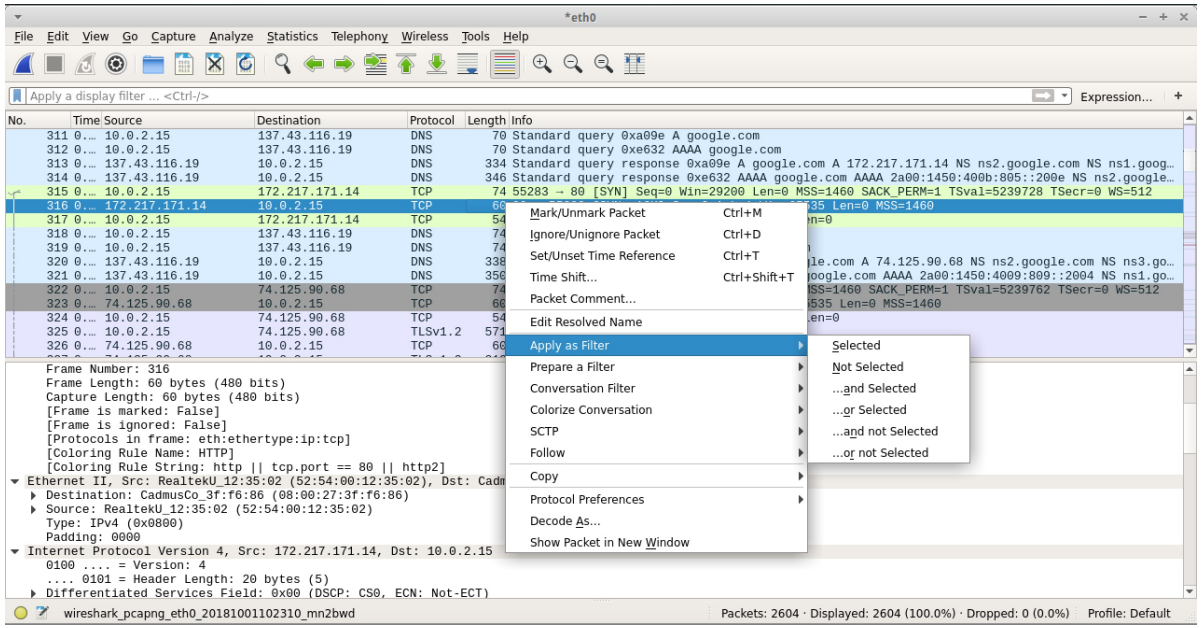
5. Inspecting Packets

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



5. Inspecting Packets - Cont

- 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.



ENJOY !!!