**Lab Experiment #09 B. Tech CSF-CSE Semester III**

**By: Dr. Gopal Singh Rawat**

**Lab Objective: Network Scanning**

**Tools:**

* **Wireshark**

Wireshark is a network packet analyzer or protocol analyzer which examines what is going inside a network cable. This tool tries to capture network packets and display that packet data as detailed as possible. Wireshark is designed to decode not only packet bits and bytes but also the relations between packets and protocols.

|  |  |  |
| --- | --- | --- |
| **Used by** |  | **Features** |
| * Students 🡪   Learn network protocol internals   * Network security engineers 🡪 Examine security problems * Network administrators 🡪 Troubleshoot network problems * QA engineers 🡪   Verify network applications   * Developers 🡪   Debug protocol implementations |  | * Available for UNIX and Windows. * Capture live packet data from a network interface. * Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs. * Import packets from text files containing hex dumps of packet data. * Display packets with very detailed protocol information. * Save packet data captured. * Export some or all packets in a number of capture file formats. * Filter packets on many criteria. * Search for packets on many criteria. * Colorize packet display based on filters. * Create various statistics |

* **What Wireshark is not…**
  + Wireshark is not an Intrusion Detection system.

It will not warn you when someone does strange things on your network that he/she is not allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

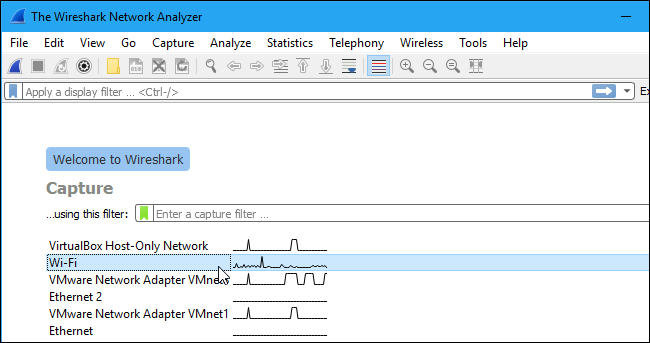
* + Wireshark will not manipulate things on the network

It will only “measure” things from it.

Wireshark does not send packets on the network or do other active things

**Practice Activities:**

1. **Add network interface to start capturing traffic**

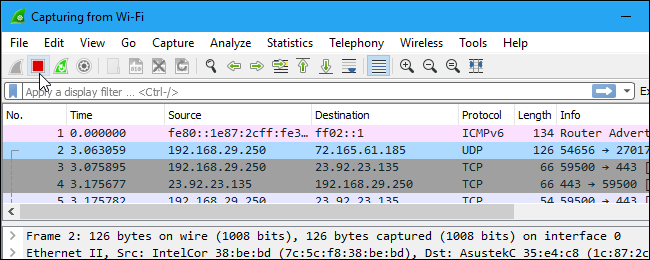


1. **Ensure Promiscuous Mode is enabled**

* View all the other packets on the network and not just packets addressed to your network adapter.
* To confirm Promiscuous mode is enabled 🡪 click Capture 🡪 Options 🡪 verify “Enable promiscuous mode on all interfaces” checkbox is activated

1. **Start & Stop capturing traffic**

* Click on “Start” or “Stop” under File option

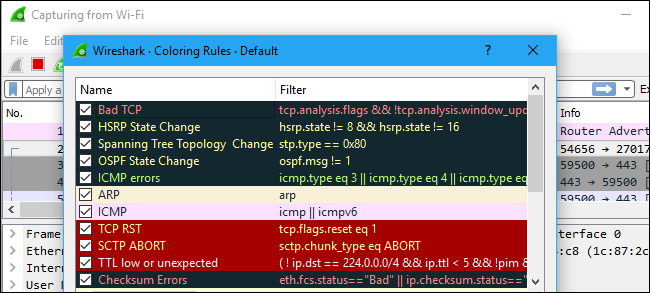


1. **Defined Color Coding**

* Wireshark uses colors to help you identify the types of traffic at a glance.
* By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors

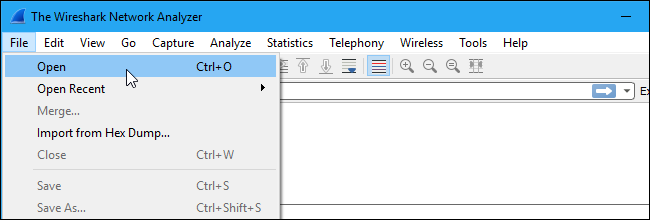
1. **Add Custom Colors**

* Click on View 🡪 Coloring Rules 🡪 Background --- to change the color you like



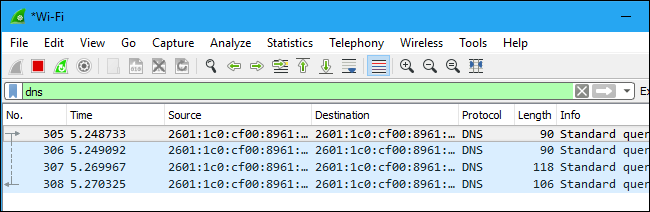
1. **Start Capture OR use Sample captures**

* Click on File 🡪 Capture OR File 🡪 Open (sample log captures)

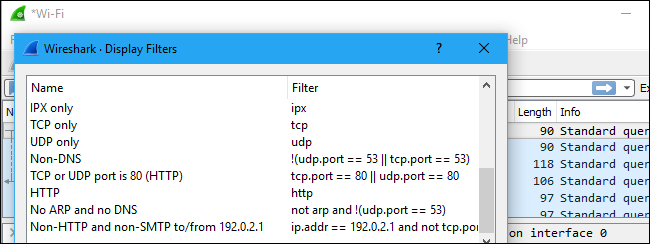


Download from <https://wiki.wireshark.org/SampleCaptures>

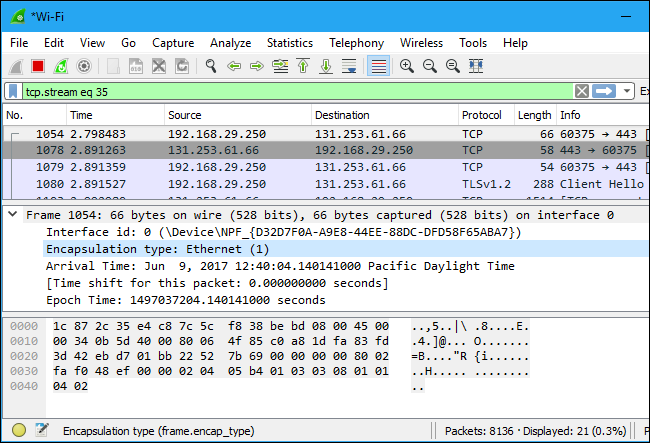
1. **Filtering Packets**



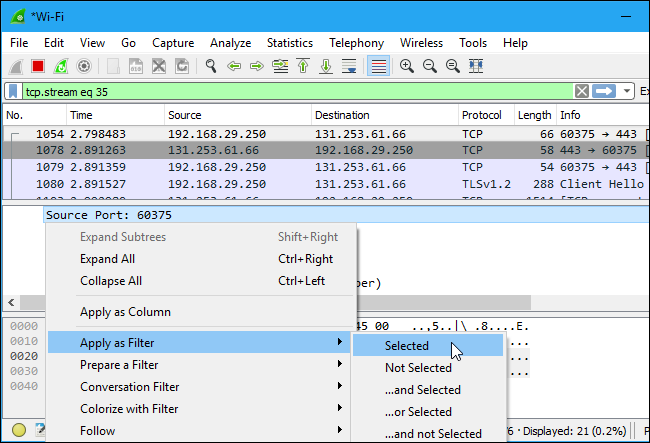
1. **Analyze Display**



1. **Inspect Packet**



1. **Apply Filters**



**Lab #09 File Work:**

1. Perform this experiment to capture Network Traffic for at least 15 minutes from your desktop/laptop.
2. PING other systems on the Lab Network (say your system is 10.1.2.49 & neighbor system is 10.1.2.50)
3. Run Wireshark to capture network traffic
4. Save the Network Packets
5. Open Browser to access [www.upes.ac.in](http://www.upes.ac.in) (OR your favorite web portal)
6. Perform this experiment to capture ONLY UDP and TCP packets
   1. Capture only udp packets 🡪 Capture filter = “udp”
   2. Capture only tcp packets 🡪 Capture filter = “tcp”
   3. Capture only DNS Requests 🡪 “udpdst port 53”
   4. Capture only UDP packets with source port 53 (DNS replies) 🡪 “udpsrc port 53”
   5. Capture only packets destined to [www.upes.ac.in](http://www.upes.ac.in) 🡪 “dst host [www.upes.ac.in](http://www.upes.ac.in)”
7. Filter to find out
   1. Find out PING traffic 🡪 “icmp”
   2. Packets coming to your system 🡪 “dst host <Your\_system\_name/IP>”
   3. Packets from other system 🡪 “src host <Neighbour\_System\_name/IP>”

Weblink to try for bonus activity: <http://demo.testfire.net/>

<https://www.acunetix.com/>