**Name : Shuvo Biswas**

**ID : IT-16014**

**Lab Report No : 07**

**Lab Report Name : Install Wireshark in Linux**

**Introduction:**

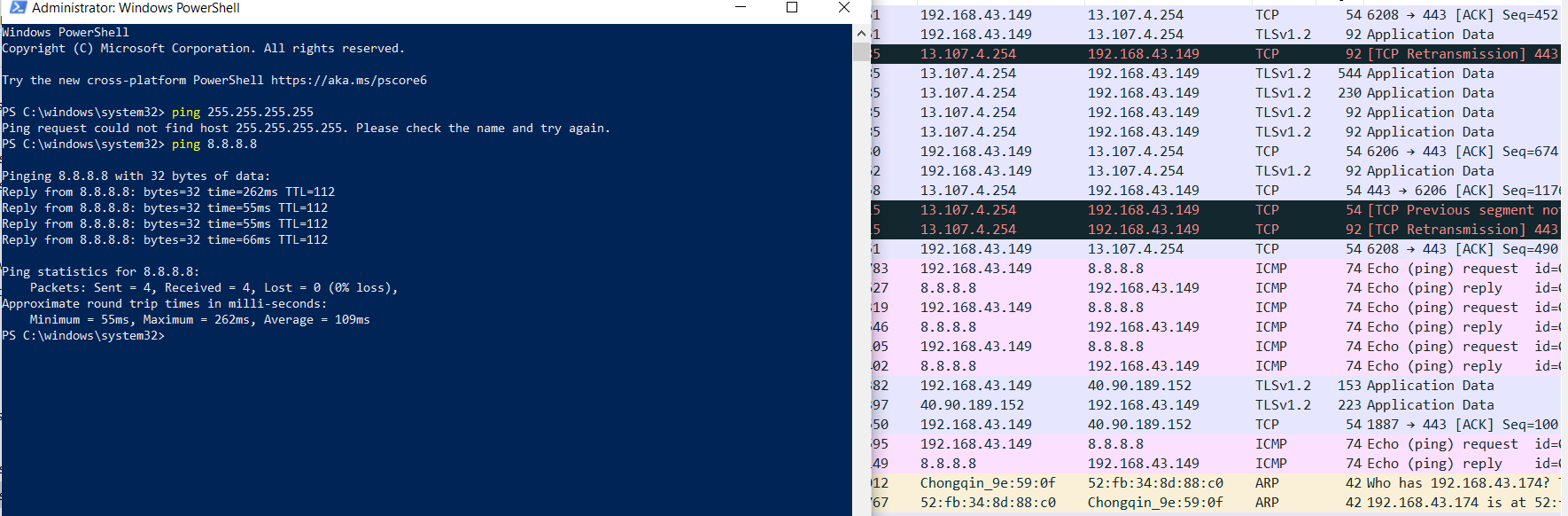
Wireshark is a network packet analyzer. It captures every packet getting in or out of a network interface and shows them in a nicely formatted text. It is used by Network Engineers all over the world.

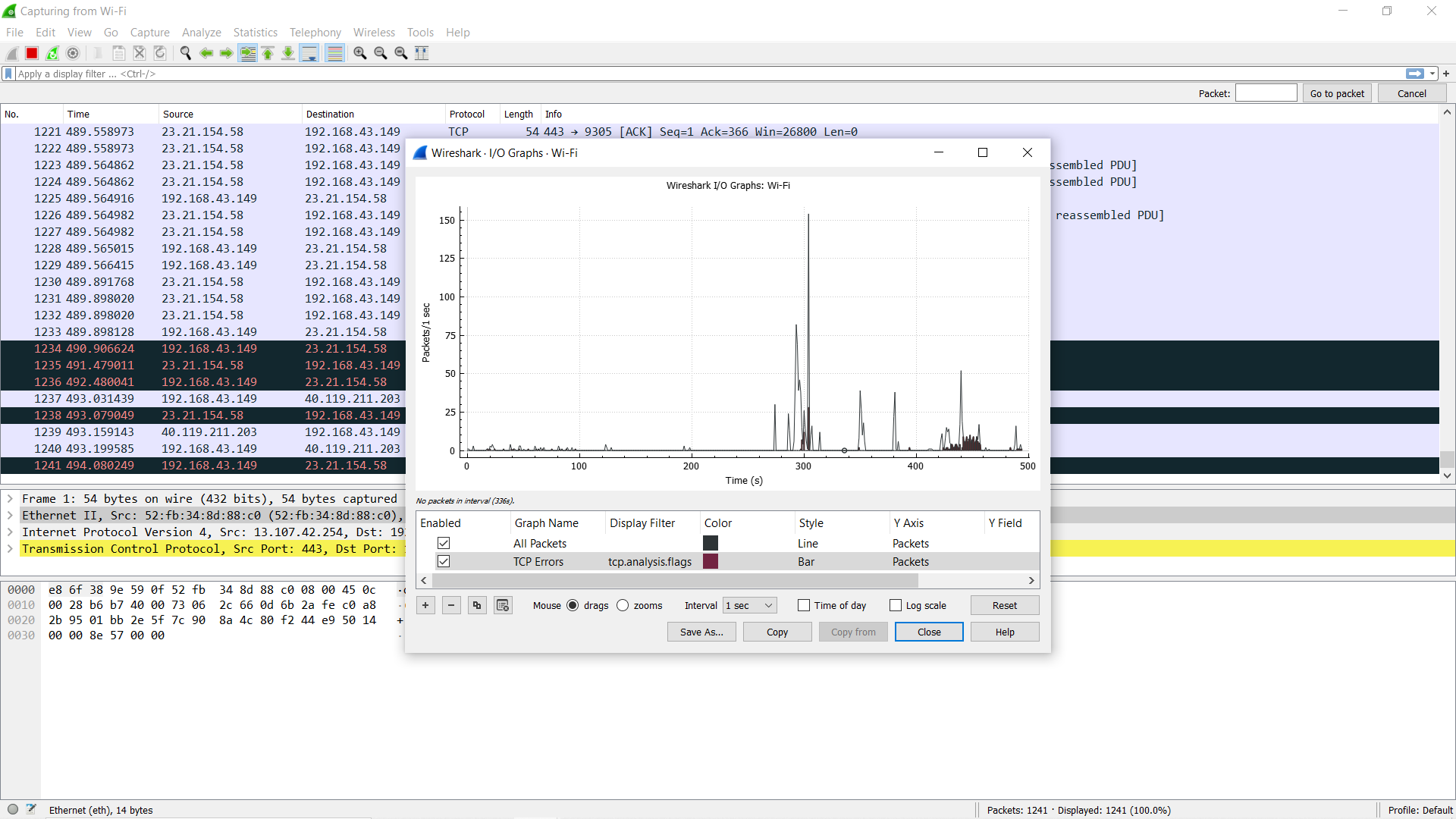
Wireshark is cross platform and it is available for Linux, Windows and Mac OS. You get the same user experience in any operating system you use.

**Installing Wireshark:**

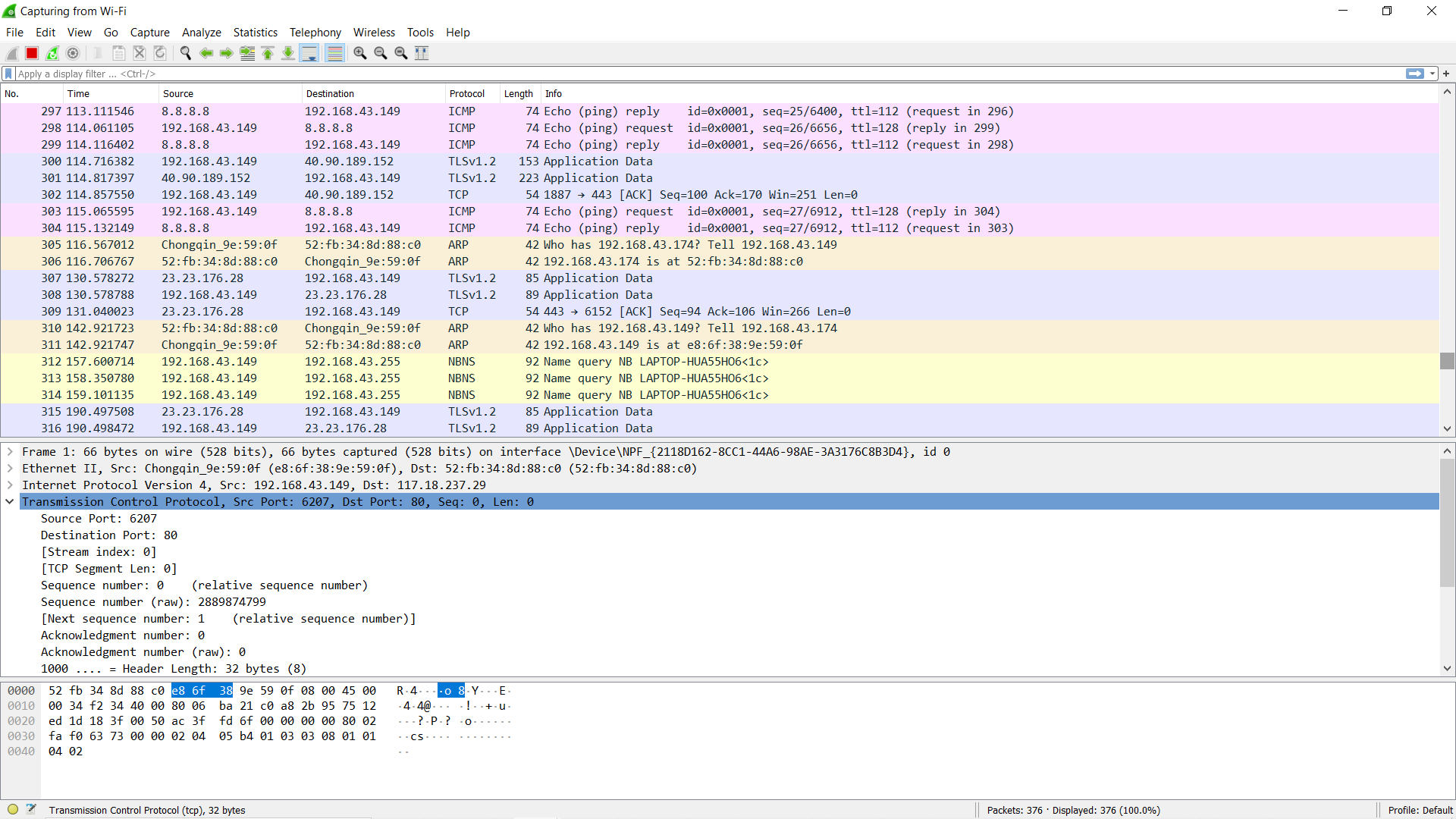
Wireshark is available in the official package repository of Ubuntu 14.04 LTS and later. So it is really easy to install.

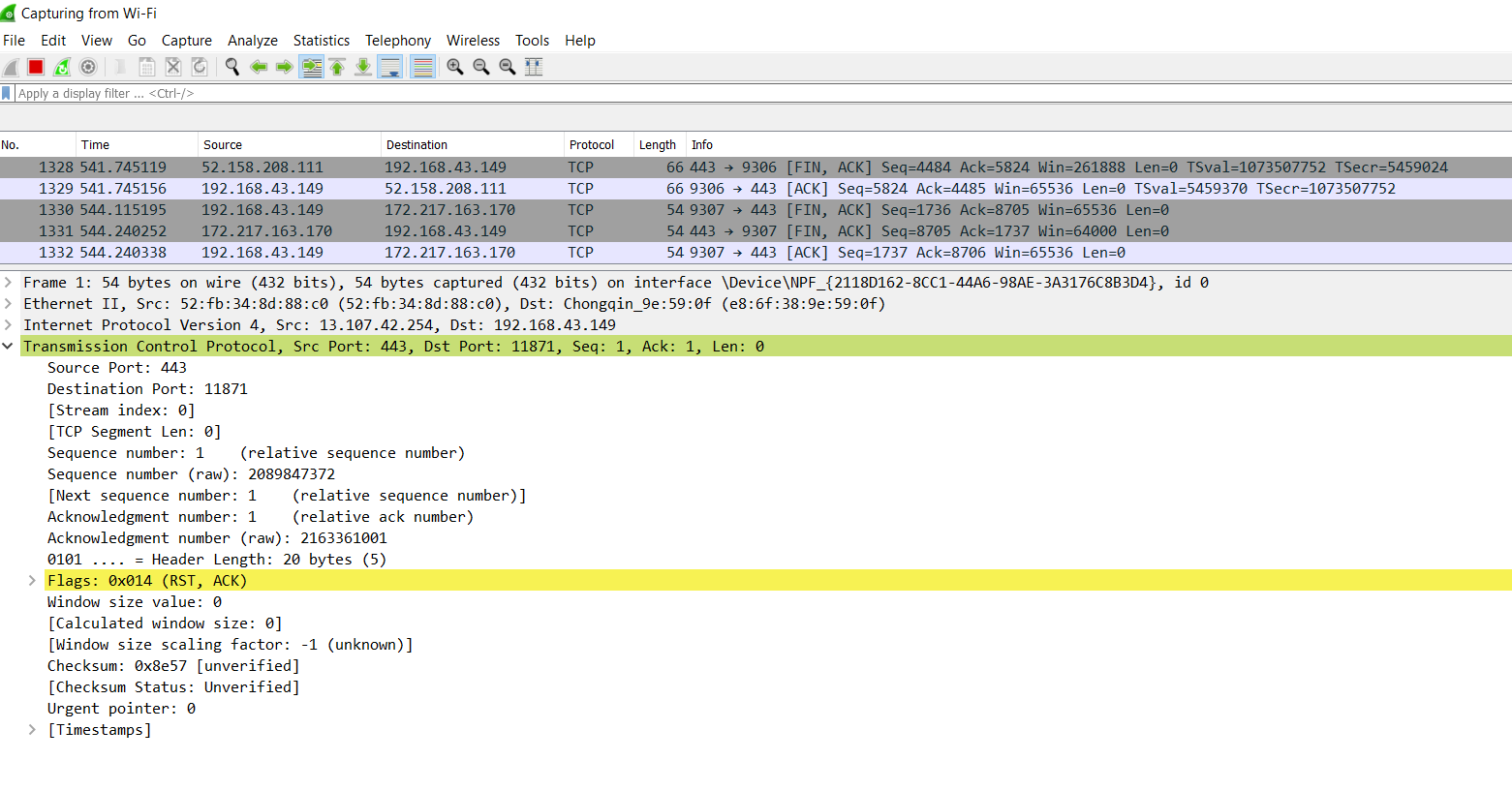
**Ping information & captured packet: ping 8.8.8.8 in powershell**

****

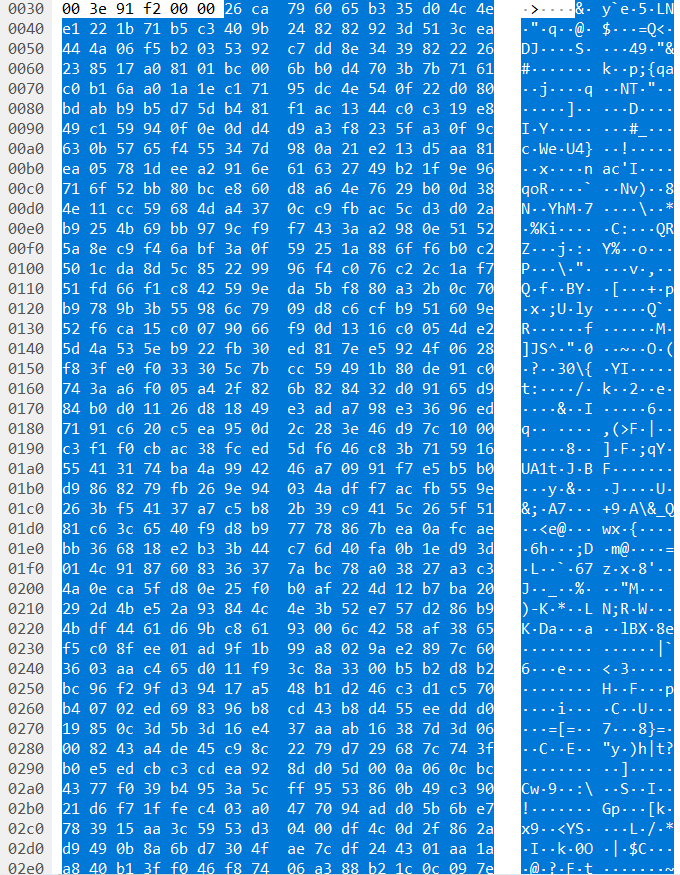
****

**The protocol information :**

****

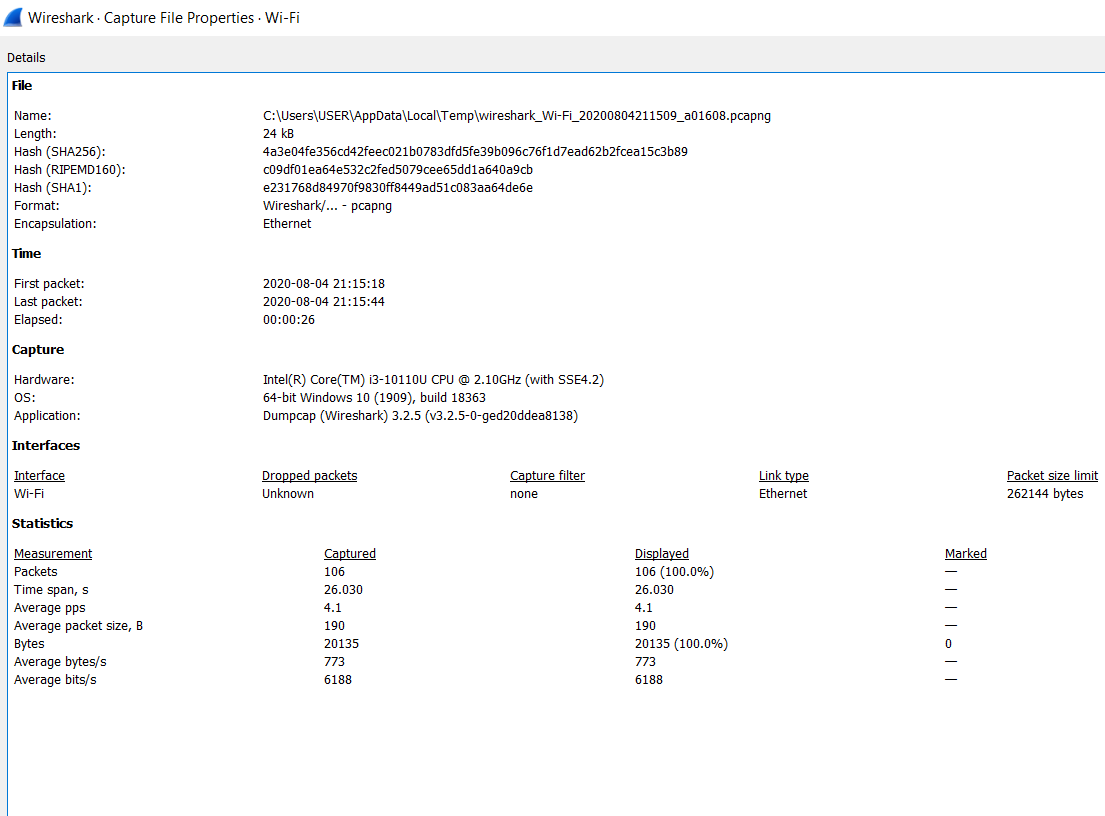
****

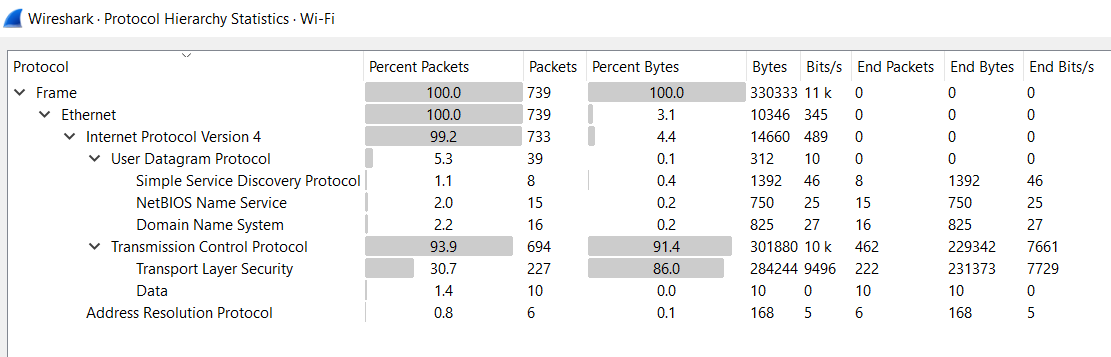
**Port Security Hashing Algorithm:**

****

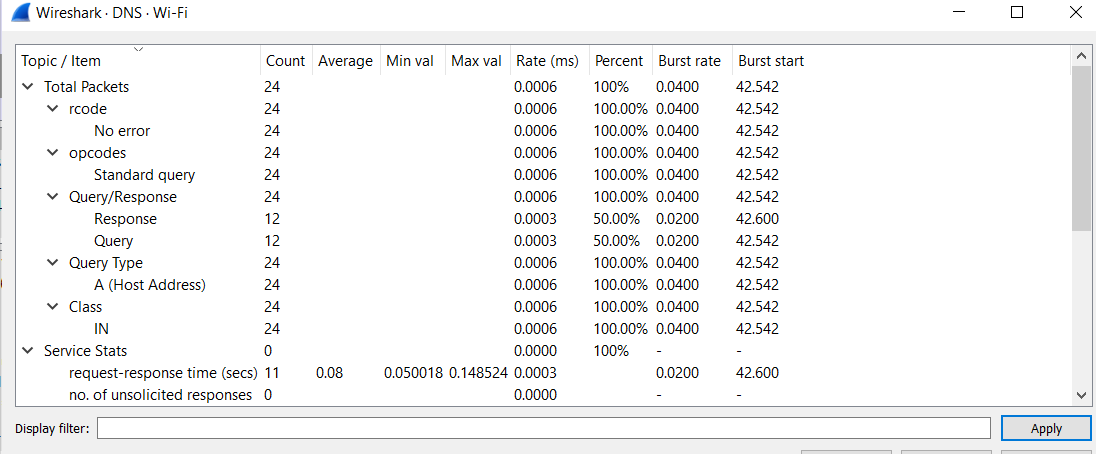
**Different Statistics:**

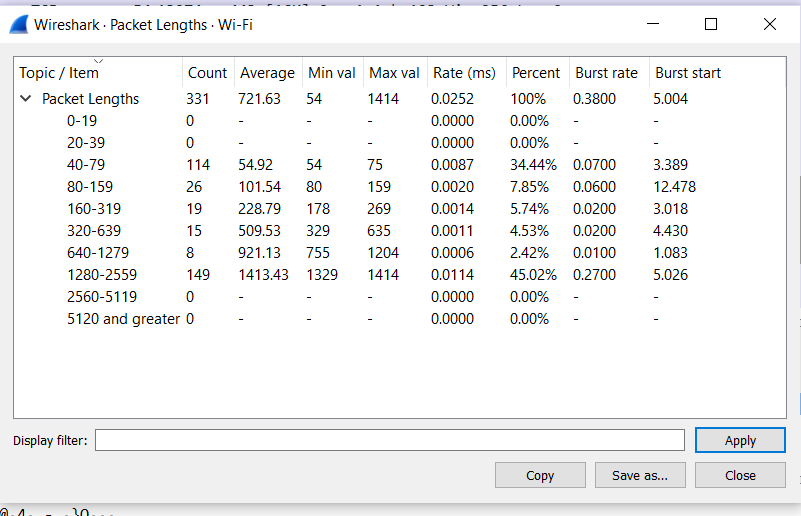
**Wi\_Fi file capture**

****

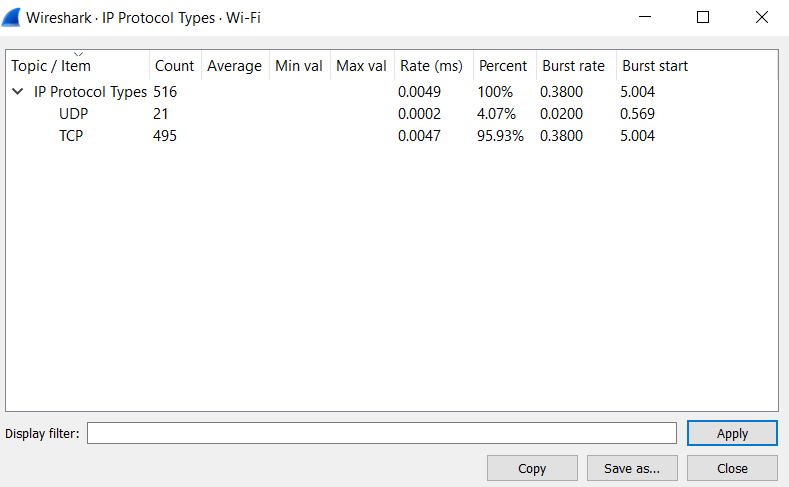
****

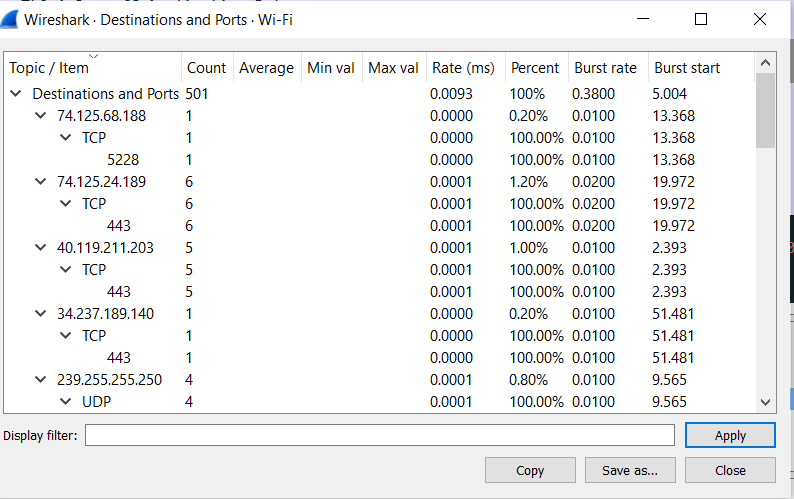
**DNS**

****

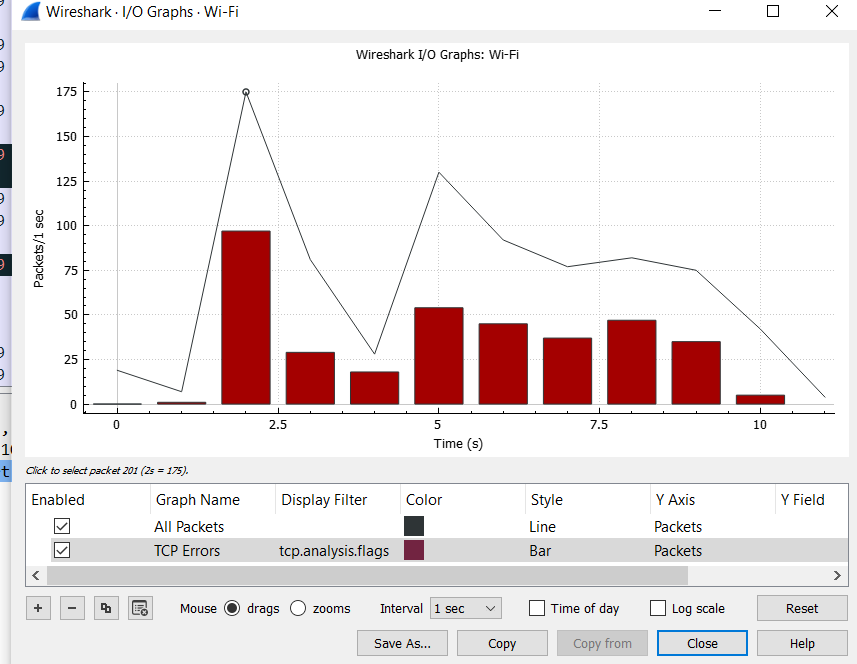
****

**Protocl have been used:**

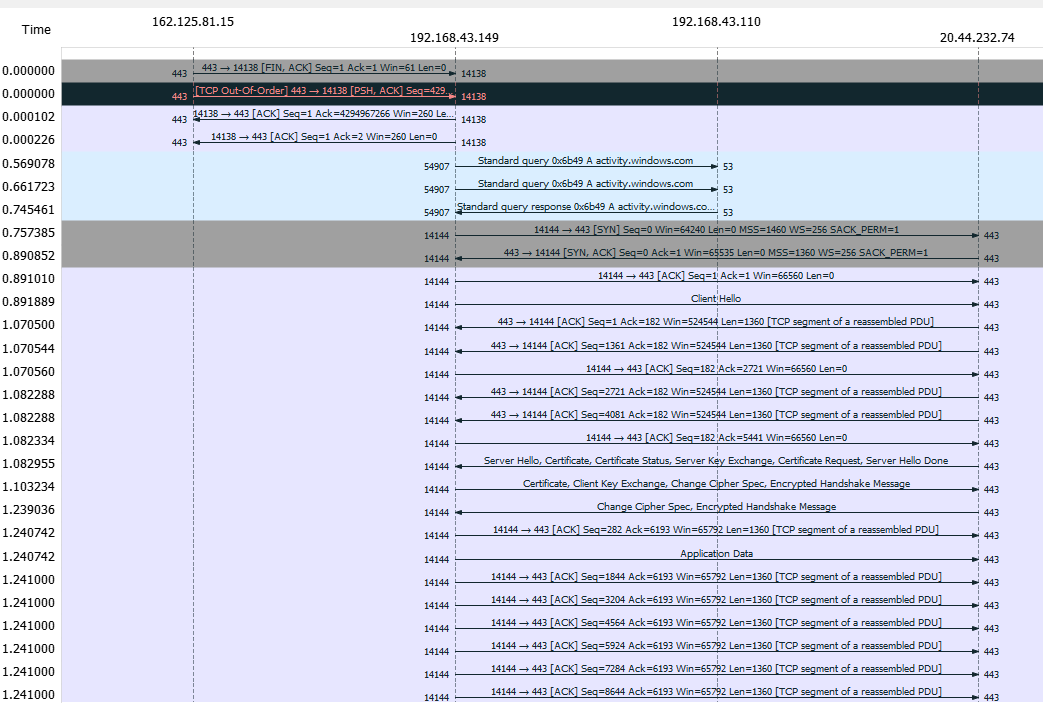
****

****

**Error & Success Rates:**

****

**Real time Response:**

****

**Conclution:**

The Wireshark package contains a network protocol analyzer. Wireshark is a open source and free software. It is a Graphical alternative to TCP dump and display packet in details. Open files contains packet data captures. Filtering is essential when dealing with a lot of packets. This is useful for analyzing data captured “off the wire” from a live network connection, or data read from a capture file.

Wireshark provides both a graphical and a TTY-mode front-end for examining captured network packets from over 500 protocols, as well as the capability to read capture files from many other popular network analyzers.