**ANALISA DAN VISUALISASI PCAP PROTOCOL SNMP DENGAN MENGGUNAKANWIRESHARK DAN ORANGE**

***Ria Siti Juairiah (09011281520128)***

***Sistem Komputer, Universitas Sriwijaya***

SNMP (Simple Network Management Protocol) adalah protokol yang dapat digunakan untuk melakukan manajemen jaringan. Dengan menggunakan protokol ini kita bisa mendapatkan informasi tentang status dan keadaan dari suatu jaringan. Protokol ini menggunakan transpor UDP pada port 161.

Terdapat 3 konsep dasar pada SNMP, yaitu: manager, agent, dan management information based (MIB).

**Manager**Sebuah managed device adalah sebuah node di jaringan yang berisi agen SNMP yang berada di jaringan yang dapat di manage. Managed device akan mengumpulkan dan menyimpan informasi manajemen dan membuat informasi ini tersedia bagi NMS menggunakan SNMP. Pada beberapa konfigurasi di titik manager menjalankan suatu software management, dimana perangkat yang dapat dimanage seperti bridges, routers, servers dan workstations yang dapat integrasikan dengan sebuah modul software agent.

**Agent**  
Agent pertanggung jawab untuk menyediakan akses ke lokal MIB dari object resources dan aktivitas node tersebut. Agen tersebut juga akan bereaksi terhadap perintah manager untuk mendapat kembali nilai-nilai dari MIB dan untuk menetapkan nilai nilai di dalam MIB. Satu contoh dari suatu obyek didapat kembali dari suatu perhitungan dari banyaknya paket-paket pengirim dan penerima pada sebuah node. Manager dapat memonitor nilai yang diload pada jaringan tersebut. Software Agent berada pada di devices tersebut, beberapa agent menerima pesan yang masuk dari manager, pesan permintaan tersebut di baca atau ditulis pada data device tersebut. Agent akan mengirimkan kembali respon yang diterima, dimana agent tidak harus menunggu untuk bertanya tentang sebuah informasi. Namun pada beberapa kasus tertentu agent akan mengirimkan sebuah pesan notifikasi untuk melakukan trap ke satu atau lebih manager. Software Management pada sebuah station management akan mengirimkan pesan request ke agent dan menerima respon dan trap dari agent. Protocol UDP yang biasa digunakan sebagai pembawa paket tersebut dengan karakteristiknya yang hemat dengan bandwidth, namun protocol pembawa lainnya juga dapat digunakan.

**MIB (Management Information Base)**

Management Information Base, merupakan struktur basis data variabel dari elemen jaringan yang dikelola. Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah. MIB di akses menggunakan protokol network-manajemen seperti SNMP. MIB terdiri dari managed objek dan di identifikasi oleh object identifier (pengidentifikasi objek). Sebuah managed object, kadang kala di sebut sebagai MIB object, objek, atau MIB, adalah satu dari banyak karakteristik spesifik dari peralatan yang di manage.

Untuk mendapatkan hasil pcap traffic jaringan berbasis SNMP dan untuk mengetahui lebih dalam lagi mengenai SNMP, maka telah dilakukan percobaan di Fakultas Ilmu Komputer Universitas Sriwijaya pada hari sabtu (20 Oktober 2018).

Tapping traffic SNMP ini menggunakan wi-fi public sebagai objek untuk dianalisa. Pada percobaan ini, Wi-Fi public yang dipakai memiliki IP 10.94.16.135. aplikasi yang digunakan adalah aplikai Ubuntu untuk Windows 10, Wireshark dan Orange.

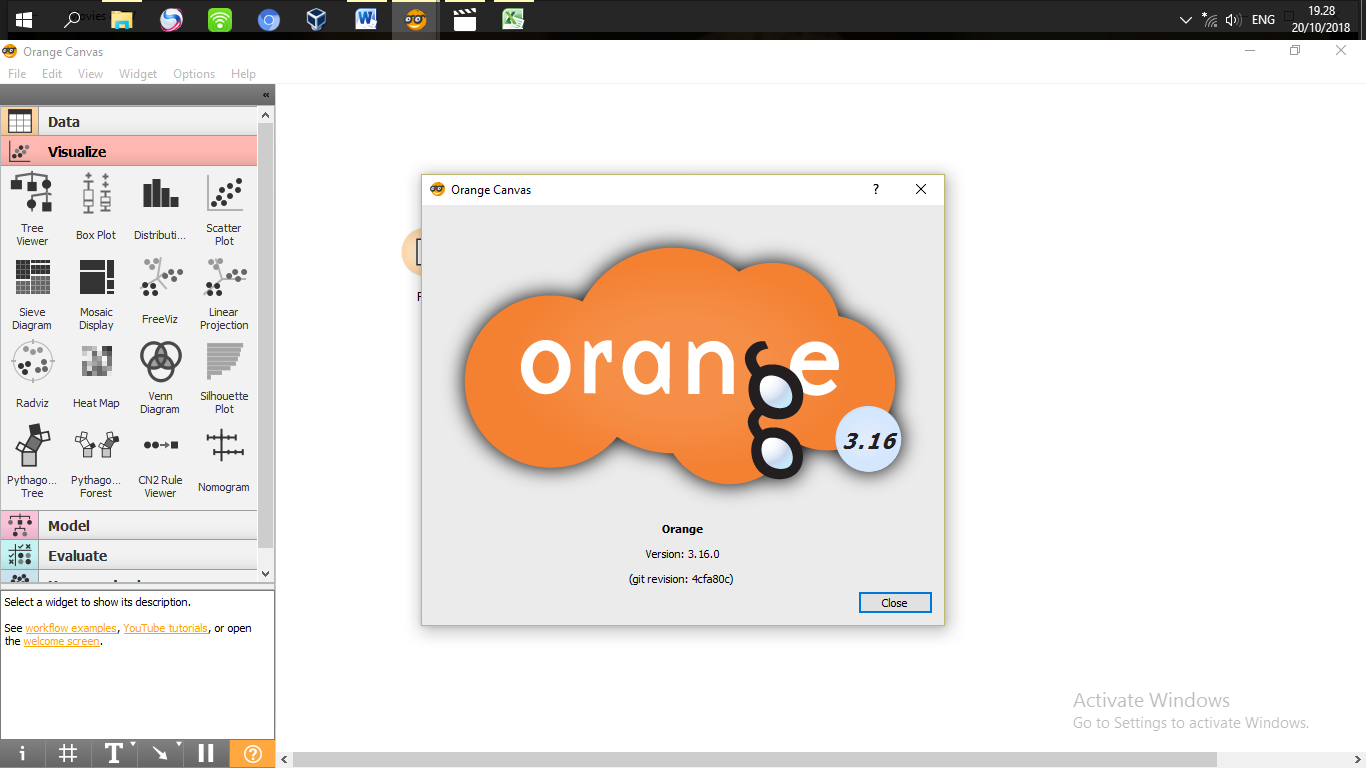
Pada Ubuntu, dimasukkan sebuah command line untuk menangkap SNMP.

C:\Users\10\Downloads\Screenshotria1.png

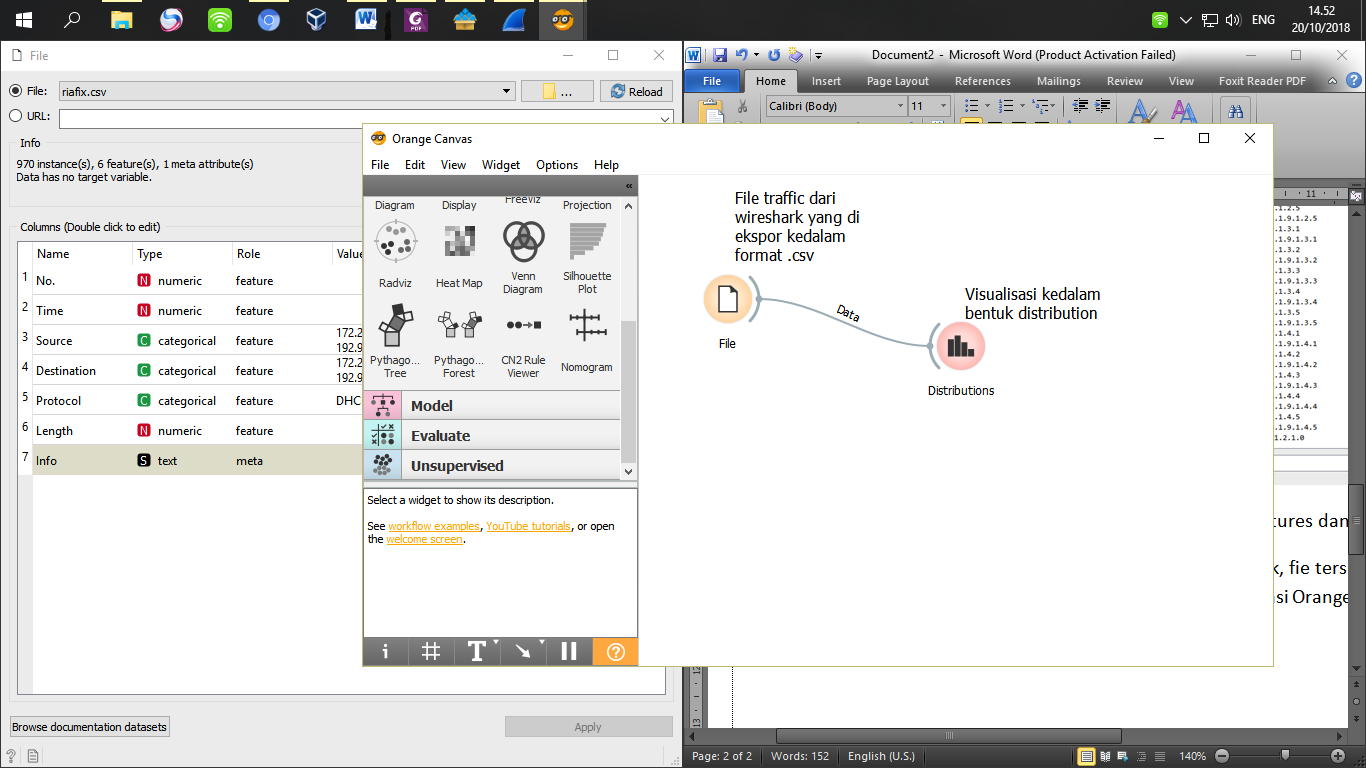
Kemudian dilakukan penangkapan traffic melalui Wireshark.

Terhitung terdapat 49 instance SNMP dari 280 instance. Artinya, hanya terdapat 0.175% dari keseluruhan traffic.

Setelah mendapatkan file berisi traffic melalui wireshark, fie tersebut di export kedalam format .csv. kemudian divisualisasi menggunakan aplikasi Orange.

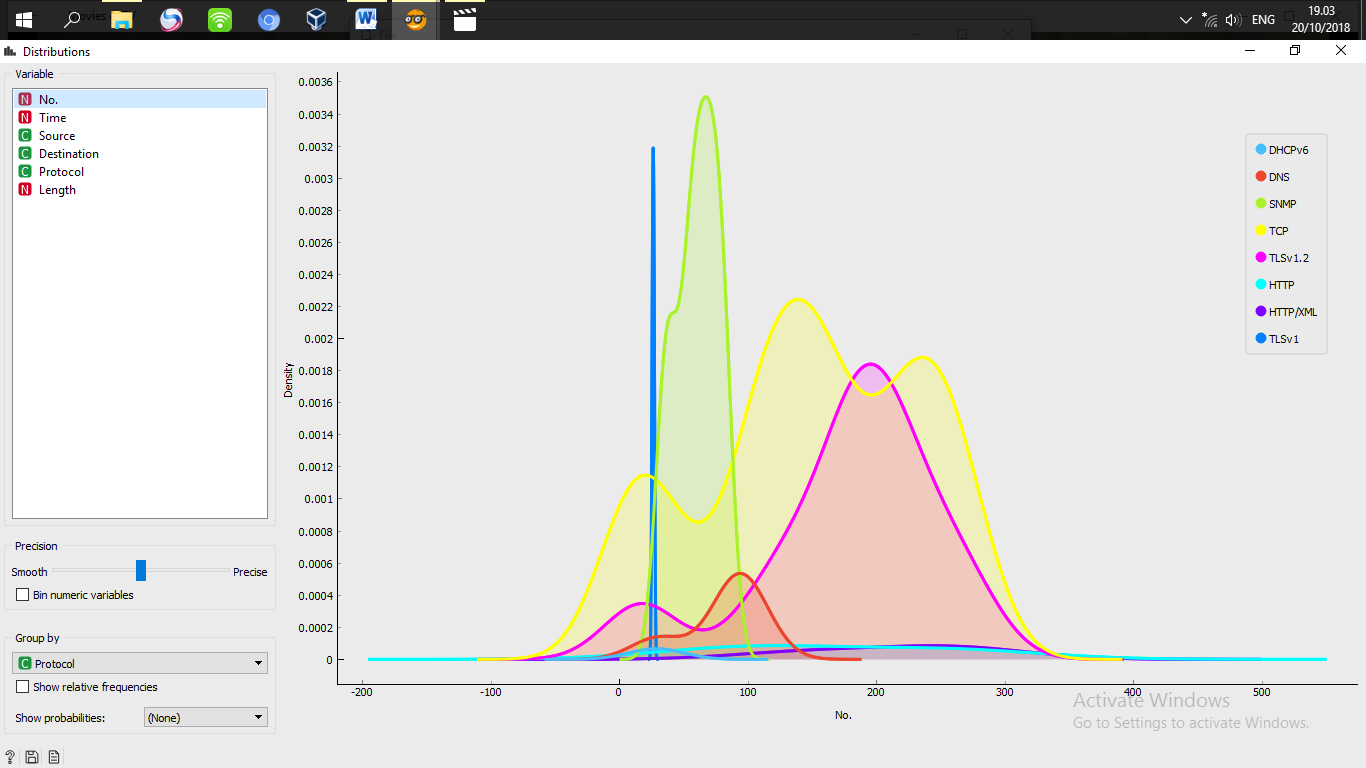


Berikut adalah proses visualisasi yang dilakukan:

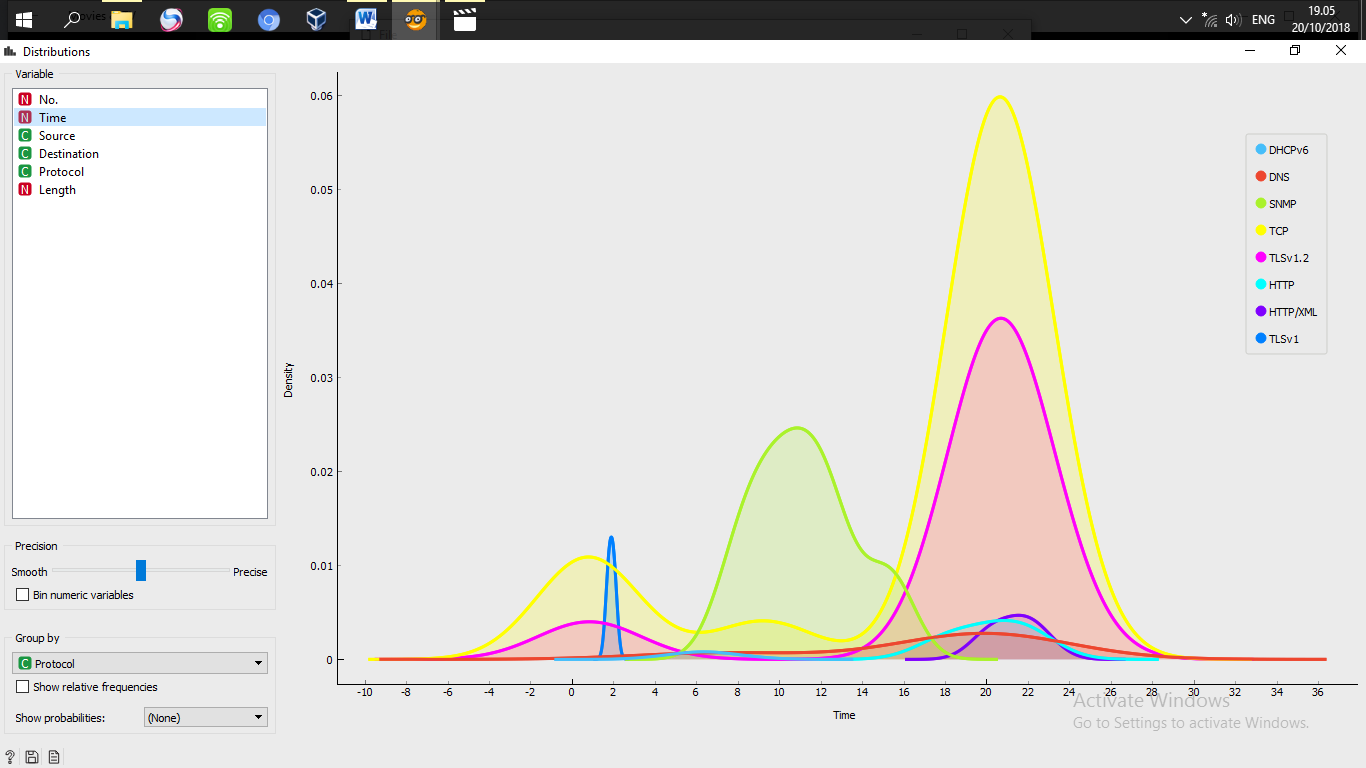


Terdapat 6 variabel pada grafik ini yaitu nomor, waktu, sumber, tujuan, protokol dan length. Sedangkan pengelompokan dapat terbagi menjadi Source, Destination, dan Protokol.

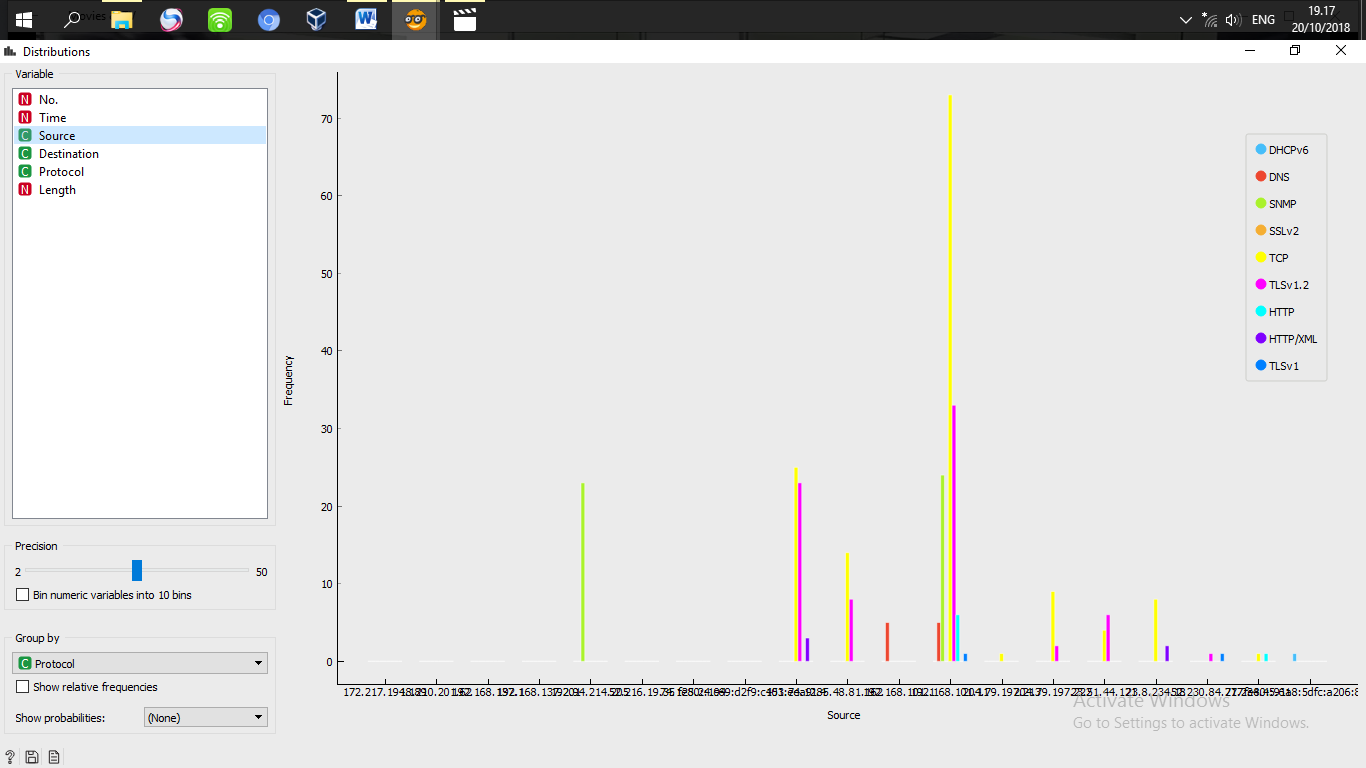
1. Berdasarkan Variabel
2. No (Nomor)



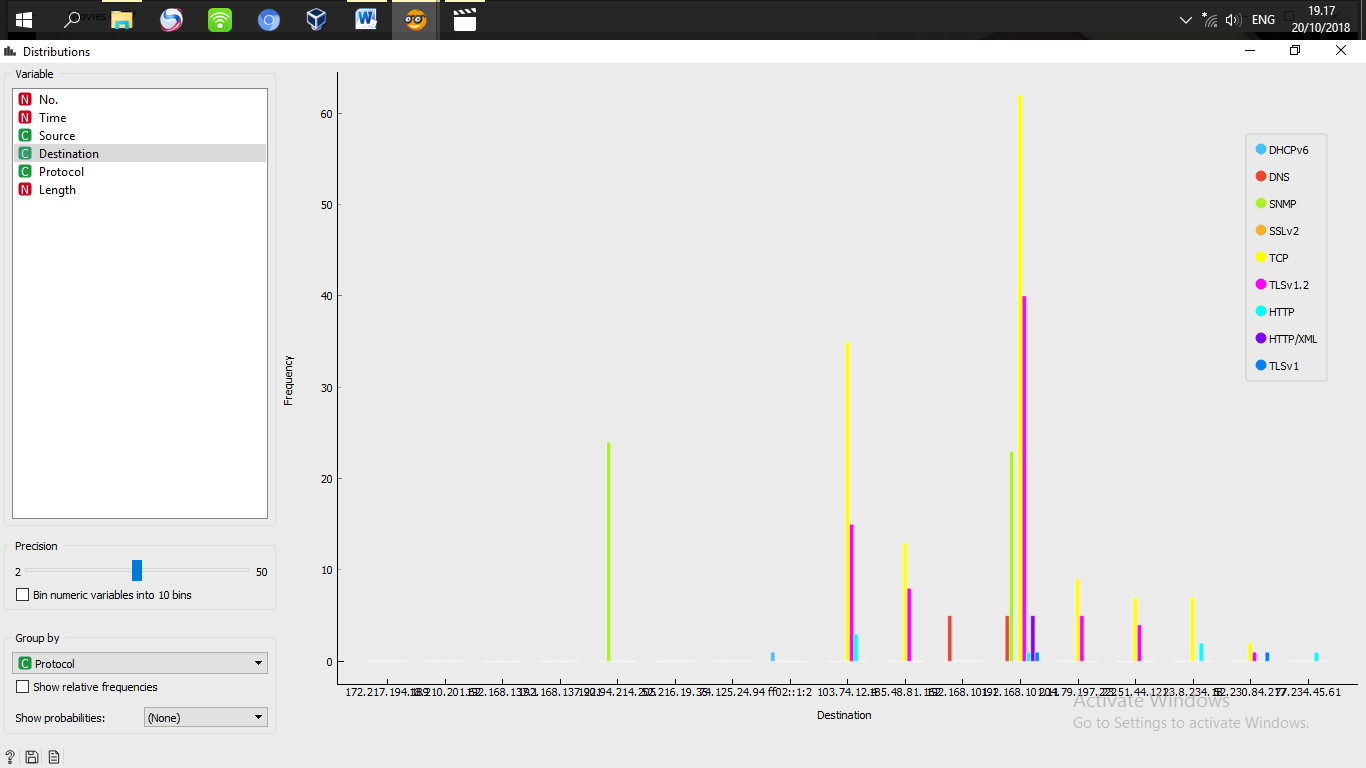
1. Time (Waktu)



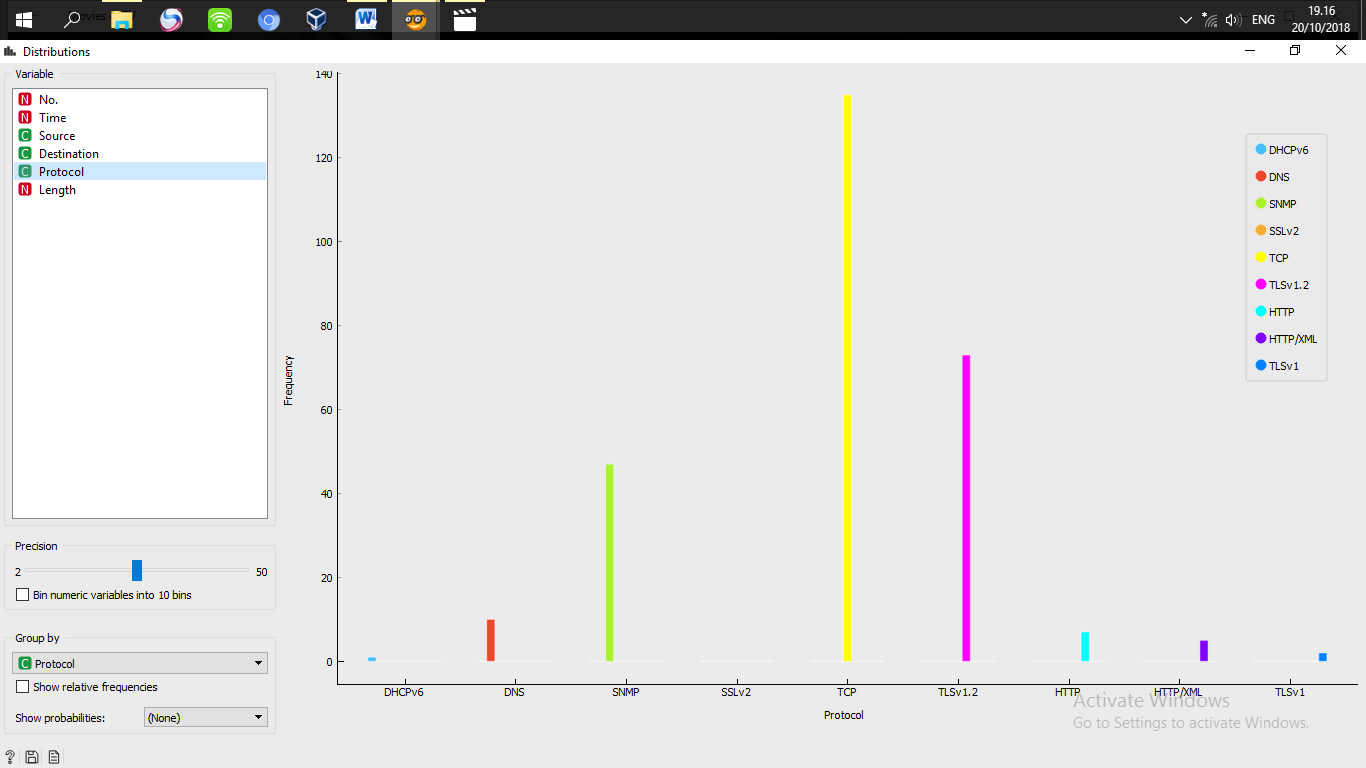
1. Source



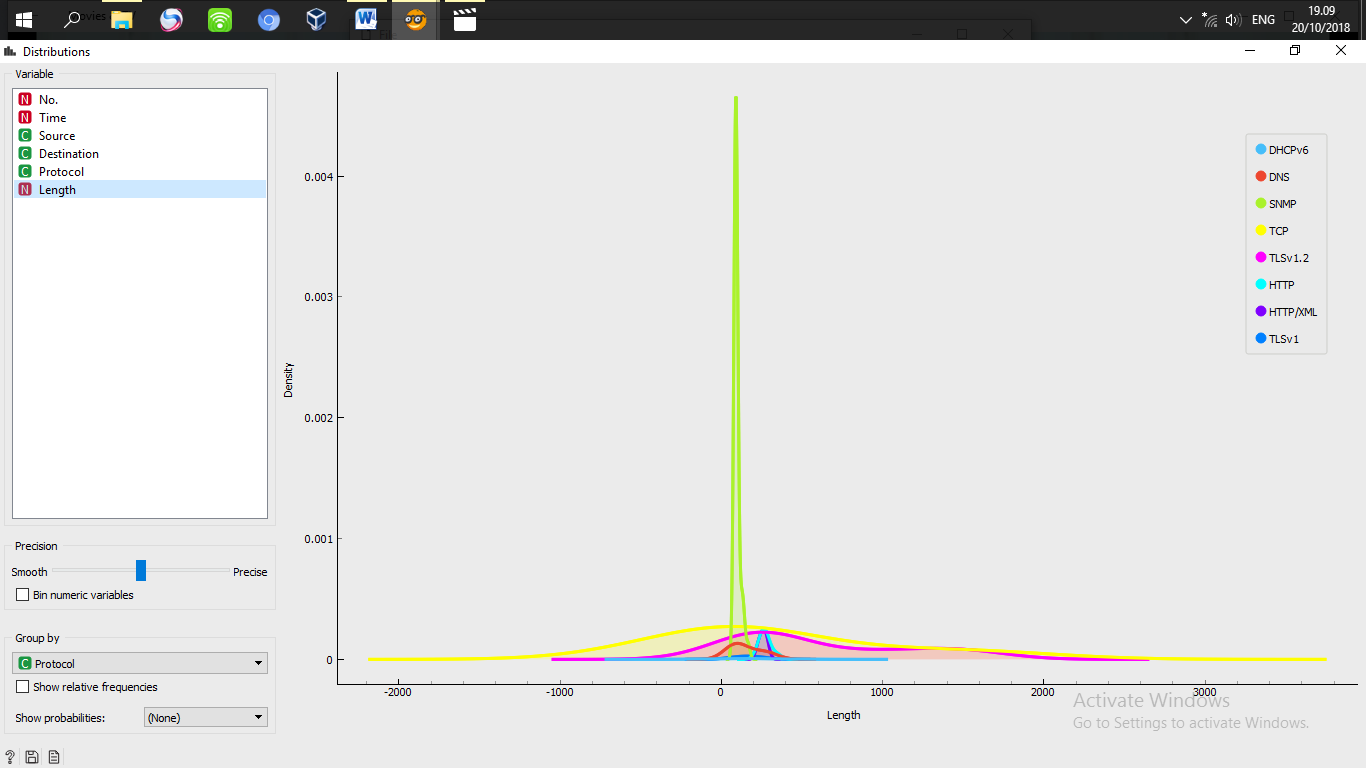
1. Destination



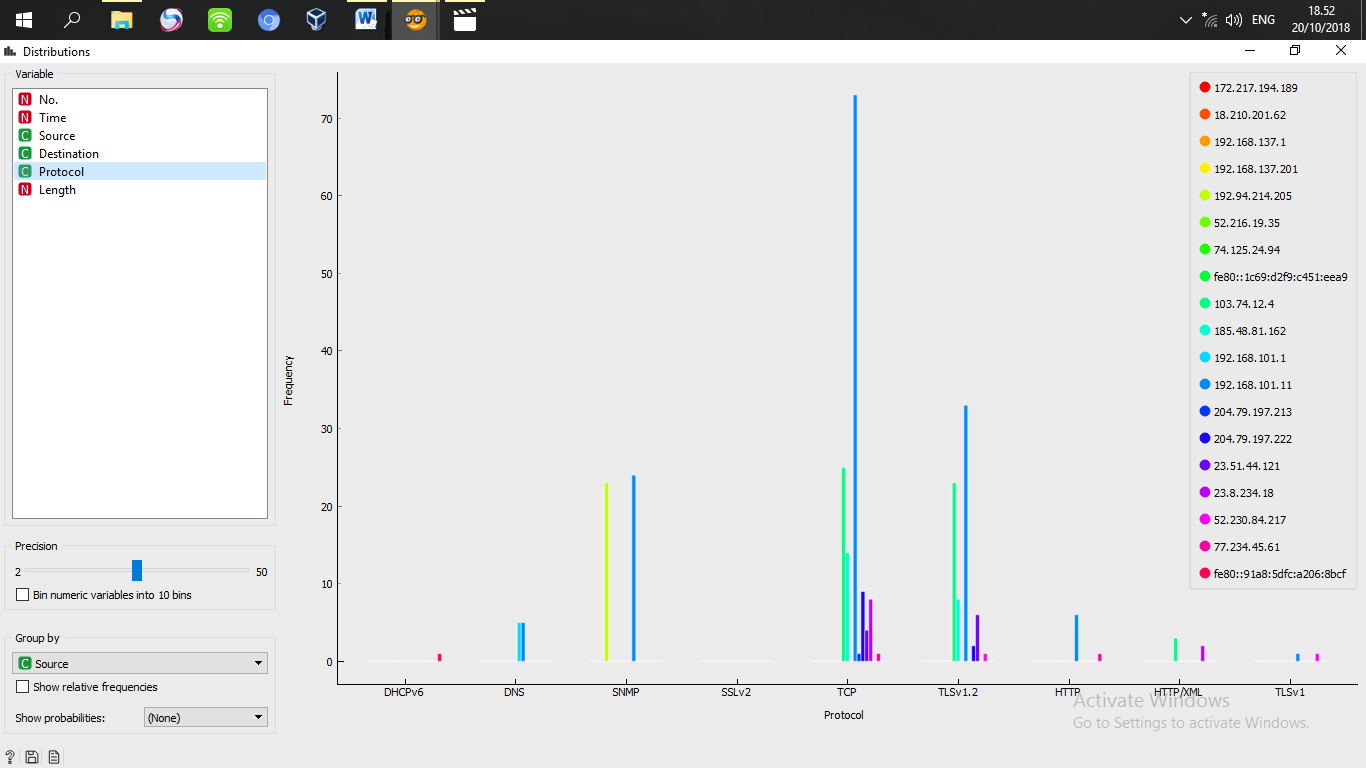
1. Protocol



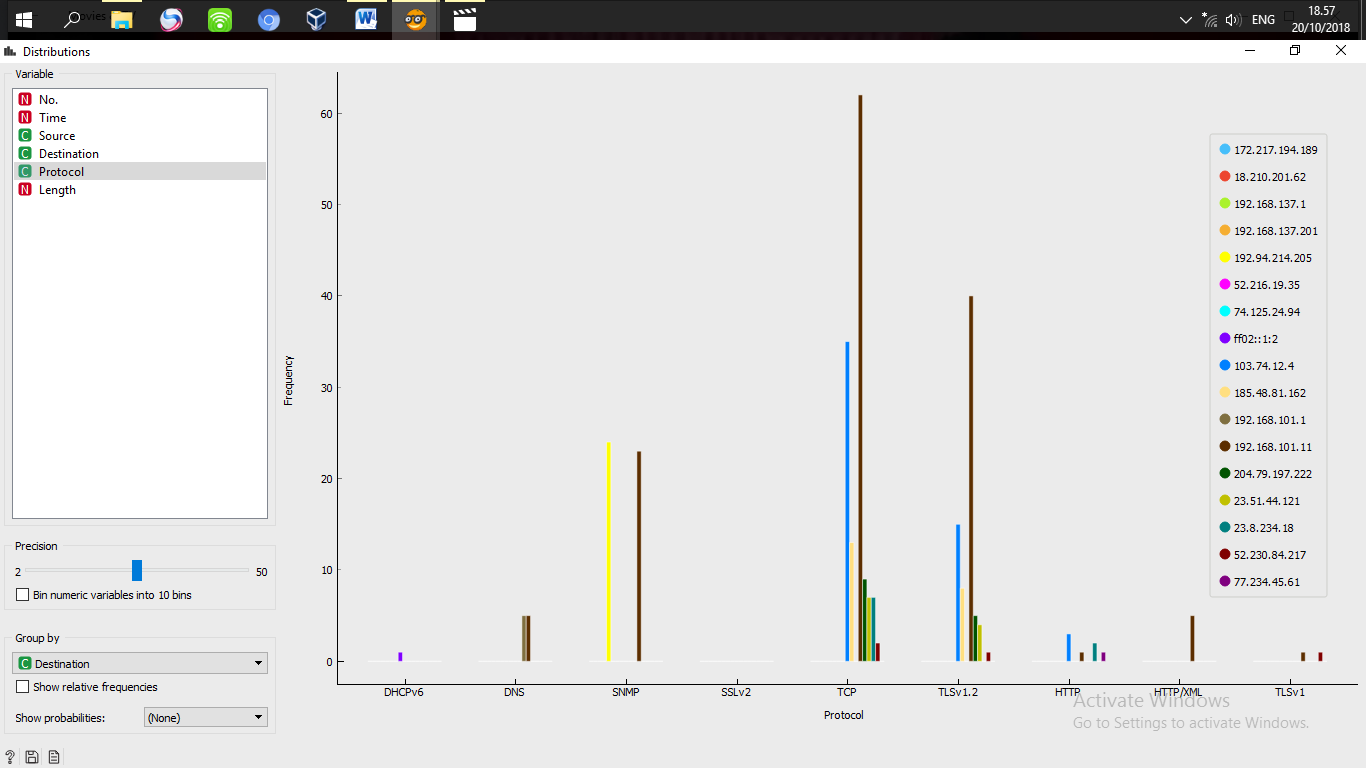
1. Length



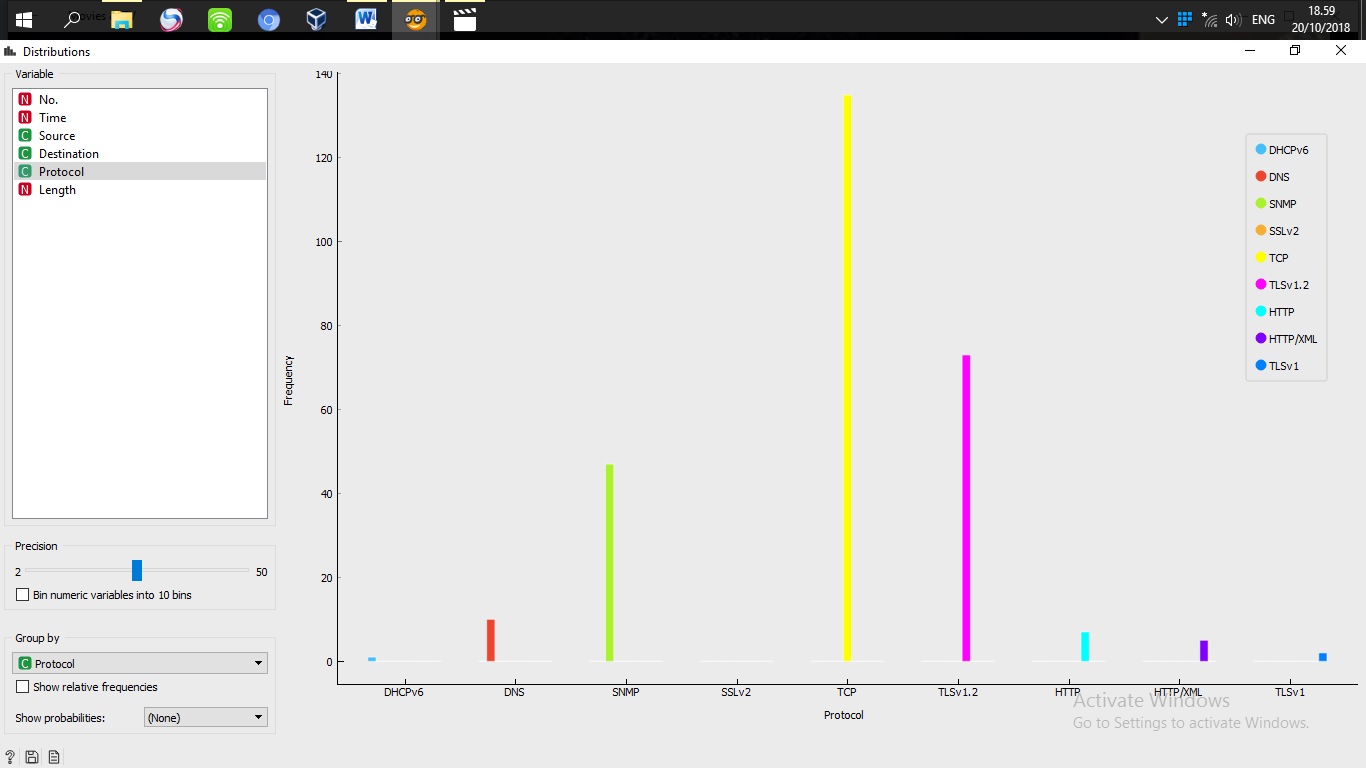
1. Berdasarkan Group
2. Data dikelompokkan ke Source



1. Data dikelompokkan ke Destination



1. Data dikelompokkan ke Protokol



Analisa:

NO adalah nomor urutan traffic yang ditangkap oleh Wireshark. SNMP memiliki Nomor antara 0-100 dengan Density atau massa jenis paling tinggi yaitu 0.034. SNMP memiliki Length paling besar yaitu diatas 0.004. Frekuensi Source untuk SNMP berada diantara 20-30. Dengan dua buah IP Source yaitu 192.94.214.205 dan 204.79.197.213. IP Destinationnya adalah 192.94.214.205 dan 192.168.101.11. Frekuensi protokol SNMP berada diantara 40-60.