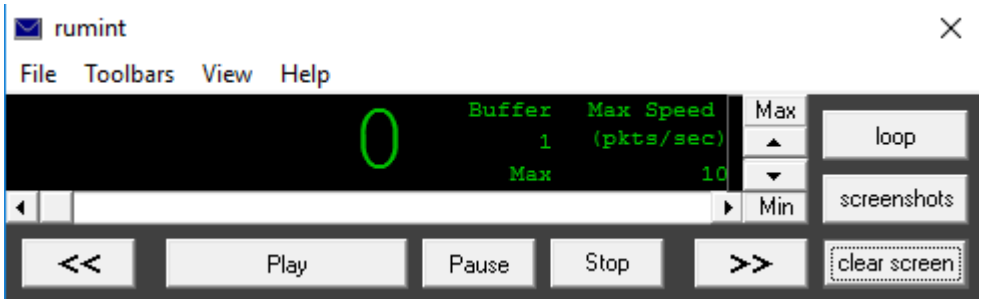
Virtualisasi dalisis Data .pcap Wireshark

Created by Henny Pratiwi_09011281520129

Virtualisasi dan Analisis Data .pcap Wireshark

Setelah menyimpan data capture wireshark kedalam format pcap kemudian download aplikasi rumint v.214 pada www.rumint.org

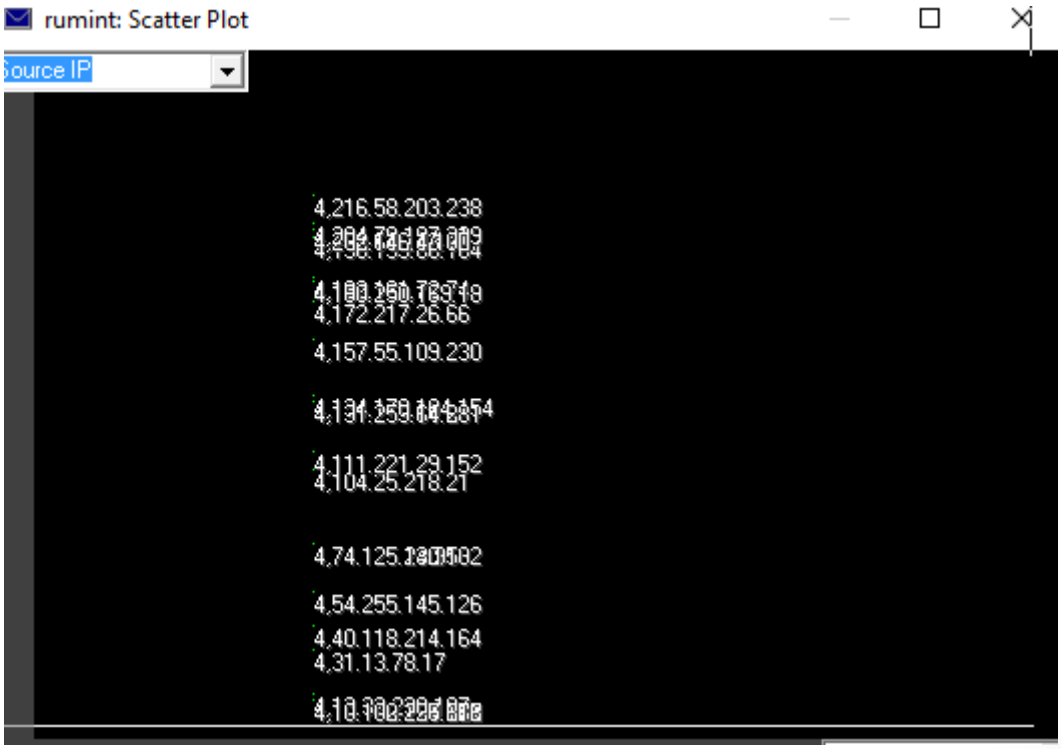
Setelah itu install dan running aplikasi, maka akan tampil kontak dialog seperti pada gambar dibawah ini:



Pilih dan klik file, kemudian pilih dan klik juga load pcap dataset dan klik play

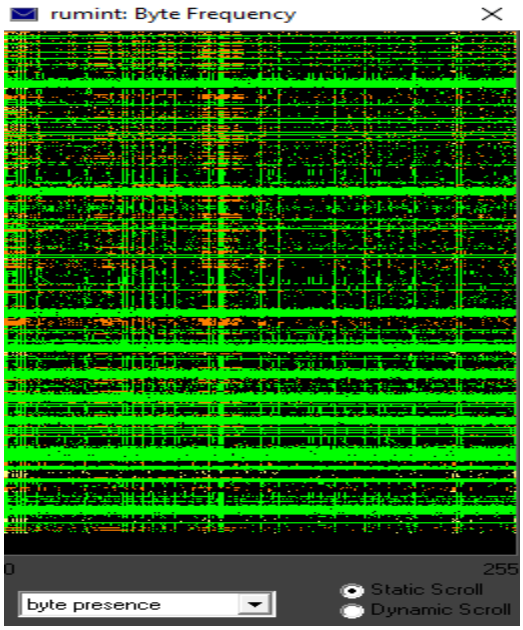
Setelah itu pada kolom view akan ada berbagai data yang bisa dilihat :

1. Scatter plot :



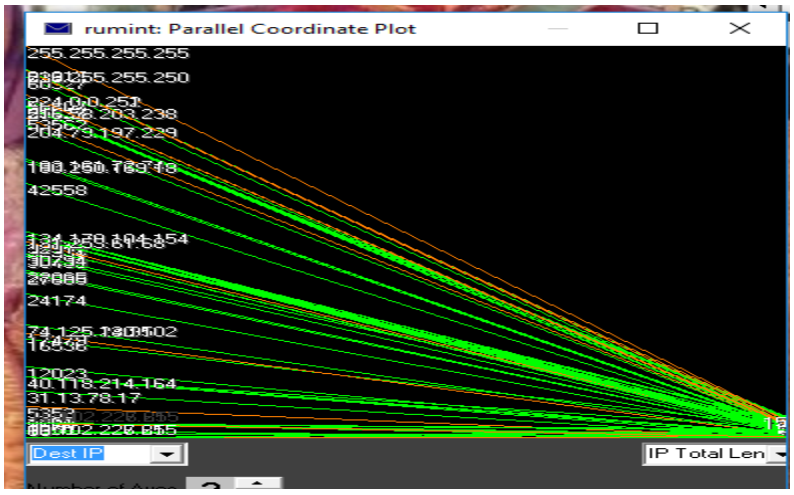
Pada data ini kita dapat melihat angka-angka yang berisi ip address pada source maupun destination.

2. Byte frequency



pada data ini dapat kita lihat garis hijau kuning saling memotong antara vertical dan horizontal.

3. Parallel coordinate plot

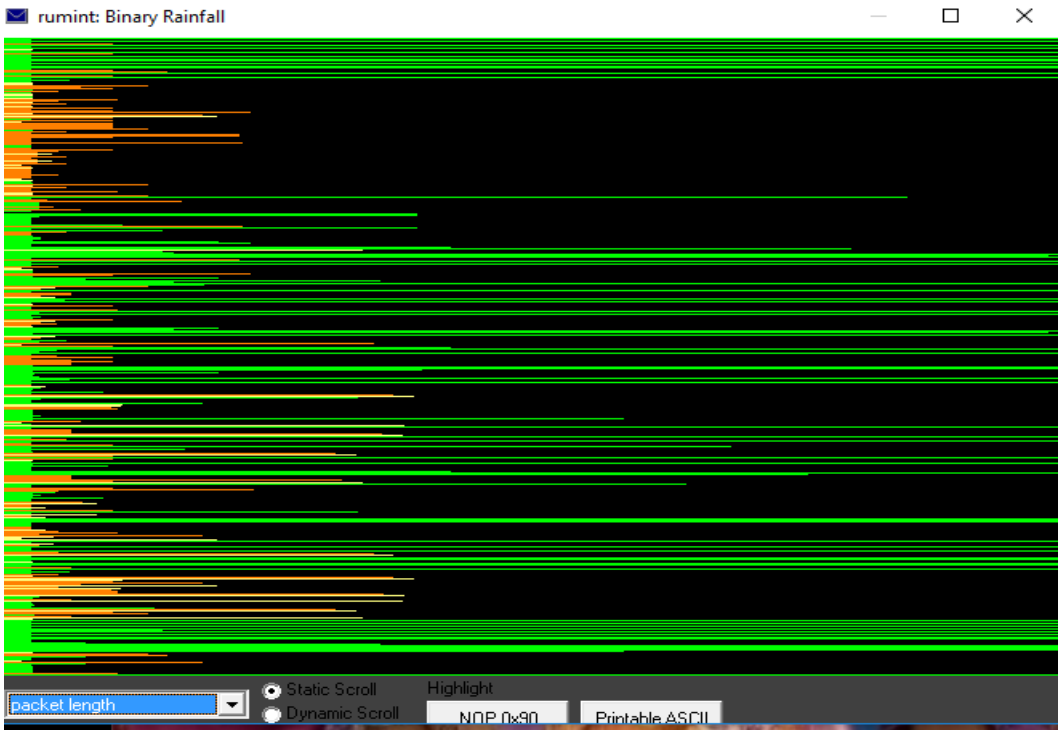


Pada gambar plot ini menunjukan dimana pada souce menuju ke berbagai destination yang dikunjungi .

4. Text rainfall

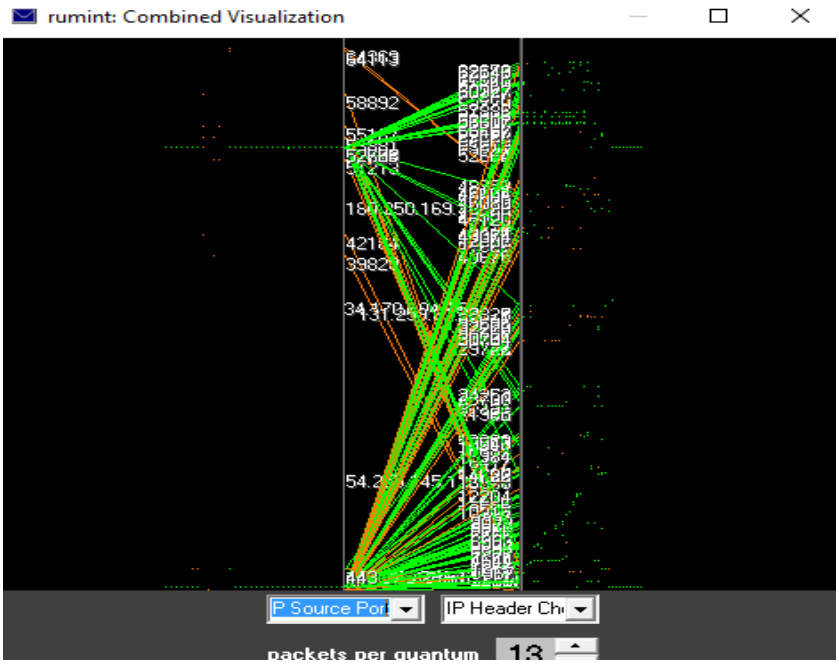
Pada gambar diatas menunjukan port dan text url yang dikunjungi.

5. Binary rainfall



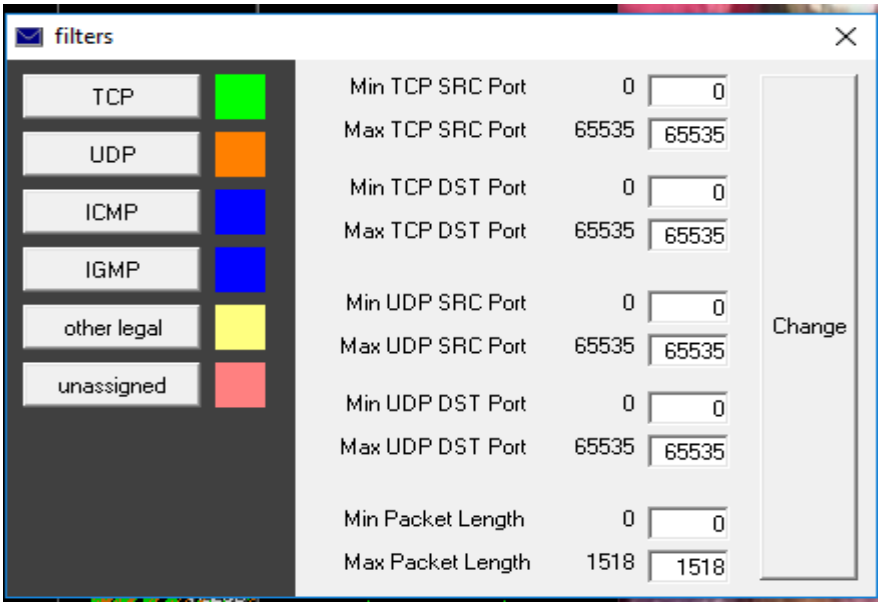
Pada gambar diatas menunjukan aliran binary dalam berupa garis horizontal bewarna hijau kuning,orange.

6. Combined visualization



pada gambar ini adalah kombinasi dari data view gambar kelima diatas sebelumnya.

7. Filter



Pada setiap garis bewarna diatas merupakan perwakilan dari nama-nama protocol maupun yang lainnya seperti pada tertera gambar ini.