VISUALISASI PCAP FILE WIRESHARK MENGGUNAKAN RUMINT

(TUGAS MATA KULIAH JARINGAN KOMPUTER)

DISUSUN OLEH :

NAMA : NANDA HASYIM MARFIANSHAR

NIM : 09011281520096

KELAS: SK5C

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

- Source Destination www.detik.com

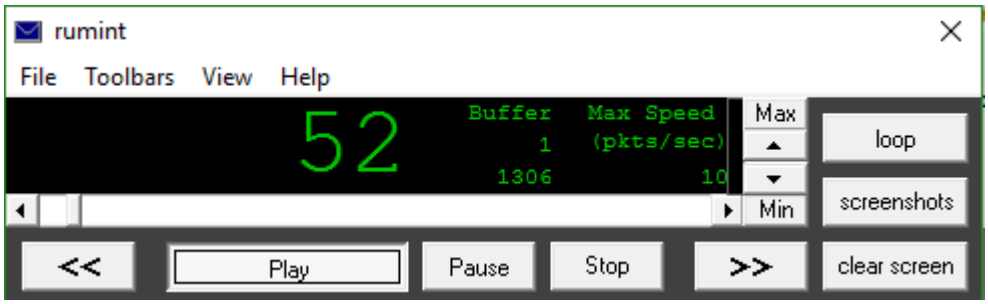
Pada data yang Analisa di wireshark dengan destinasion www.detik.com terlihat seperti gambar dibawah ini.

1	0.000000	fe80::2562:1776:7b01:dbb1	ff02::1:3	LLMNR	84 Standard query 0x78cb A wpad
2	0.000109	192.168.137.1	224.0.0.252	LLMNR	64 Standard query 0x78cb A wpad
3	0.340225	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
4	1.090845	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
5	9.538533	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
6	9.539041	fe80::2562:1776:7b01:dbb1	ff02::1:3	LLMNR	84 Standard query 0x0708 A wpad
7	9.539189	192.168.137.1	224.0.0.252	LLMNR	64 Standard query 0x0708 A wpad
8	9.949348	fe80::2562:1776:7b01:dbb1	ff02::1:3	LLMNR	84 Standard query 0x0708 A wpad
9	9.949457	192.168.137.1	224.0.0.252	LLMNR	64 Standard query 0x0708 A wpad
10	10.290579	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
11	11.040777	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
12	19.524495	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
13	19.524832	fe80::2562:1776:7b01:dbb1	ff02::1:3	LLMNR	84 Standard query 0xebe3 A wpad
14	19.524974	192.168.137.1	224.0.0.252	LLMNR	64 Standard query 0xebe3 A wpad
15	19.935519	fe80::2562:1776:7b01:dbb1	ff02::1:3	LLMNR	84 Standard query 0xebe3 A wpad
16	19.935580	192.168.137.1	224.0.0.252	LLMNR	64 Standard query 0xebe3 A wpad
17	20.275352	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
18	21.026230	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
19	29.592081	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
20	29.592302	fe80::2562:1776:7b01:dbb1	ff02::1:3	LLMNR	84 Standard query 0x5e11 A wpad
21	29.592397	192.168.137.1	224.0.0.252	LLMNR	64 Standard query 0x5e11 A wpad
22	30.002507	fe80::2562:1776:7b01:dbb1	ff02::1:3	LLMNR	84 Standard query 0x5e11 A wpad
23	30.002580	192.168.137.1	224.0.0.252	LLMNR	64 Standard query 0x5e11 A wpad
24	30.342270	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
25	31.095310	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>
26	39.513968	192.168.137.1	192.168.137.255	NBNS	92 Name query NB WPAD<00>

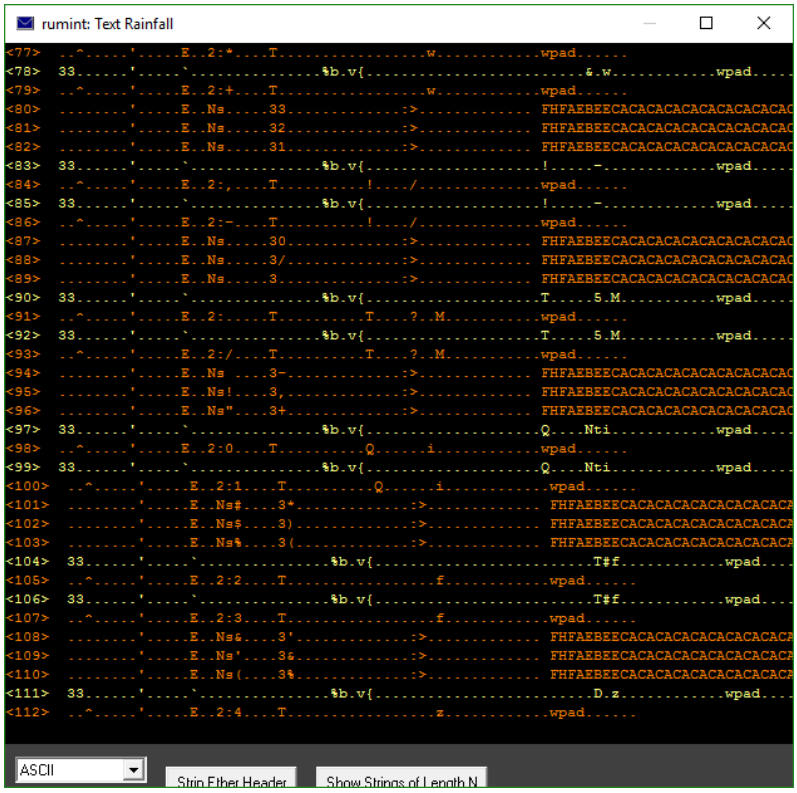
Gambar 1. Hasil tracing www.detik.com menggunakan wireshark

Wireshark menggunakan pcap untuk menangkap paket, sehingga hanya dapat menangkap paket-paket pada jenis jaringan yang pcap mendukung. .pcap adalah berkas data, yang dibuat oleh Ethereal, yang sekarang menjadi Wireshark. Ini adalah program gratis yang digunakan terutama untuk analisis jaringan.

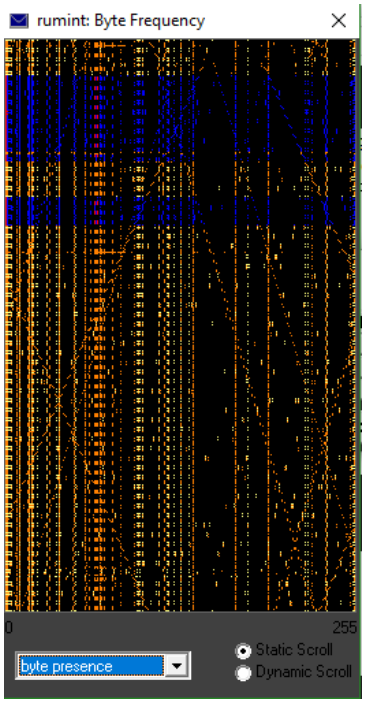
Data dari wireshark tadi disimpan dalam bentuk pcap kemudian di load file ke aplikasi rumint untuk divisualisasikan ke dalam banyak *view*.



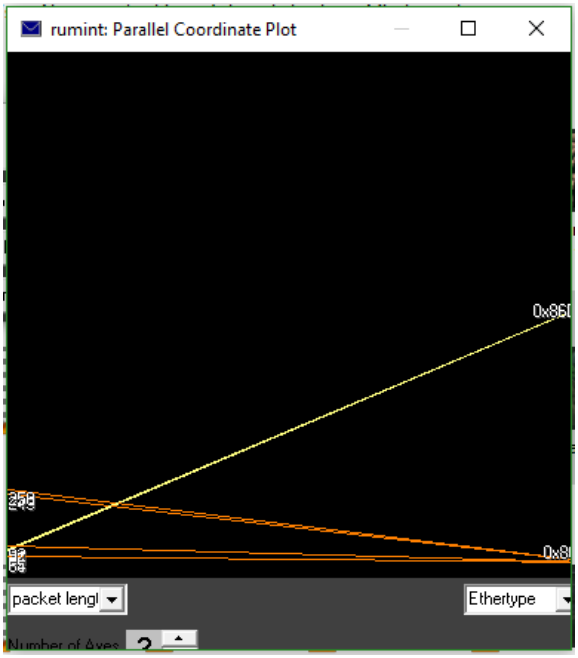
Gambar 1. Proses load play file www.detik.com ke rumint



Gambar 2. Visualisasi dari rumint : Text Rainfall

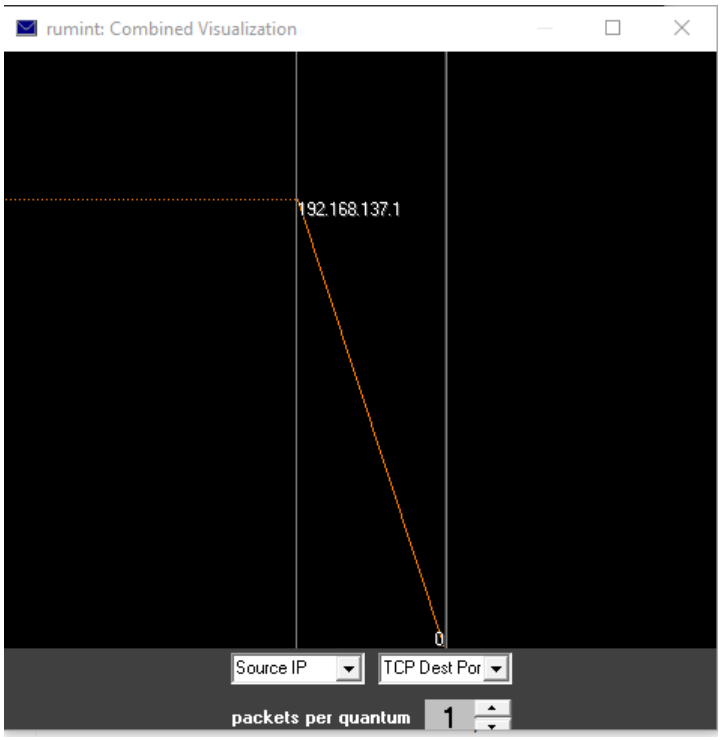


Gambar 3. Visualisasi dari rumint : Byte Frequency

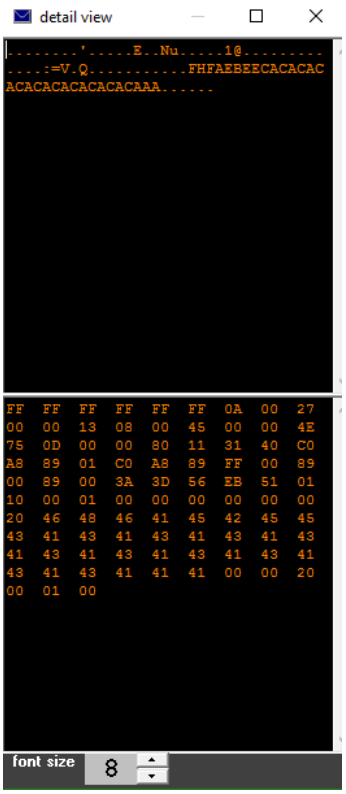


Gambar 4. Visualisasi dari rumint : Parallel Coordinate Plot

Gambar 5. Visualisasi dari Binari Rainfall



Gambar 6. Visualisasi dari rumint : Combined Visualization



Gambar 7. Visualisasi dari detail view

Analisa

Pada Analisa dari gambar diatas tampak visualisasi dilihat dari beberapa penglihatan yang ada di aplikasi rumint. Packet yang sudah ditracert dari wireshark tadi kemudia di load file ke dalam aplikasi rumint kemudian dihasilkanlah visualization.

Hasyim, nanda.2017. *Perbandingan Wireshark dan CMD*.
https://edocs.ilkom.unsri.ac.id/cgi/users
/home?screen=EPrint%3A%3AMove&eprintid=1452&_action_move_archive.x=10&_action_move_archive.y=20. Diakses pada tanggal 6 september 2017