

Visualisasi data wireshark ini menggunakan aplikasi rumint versi 2.14.

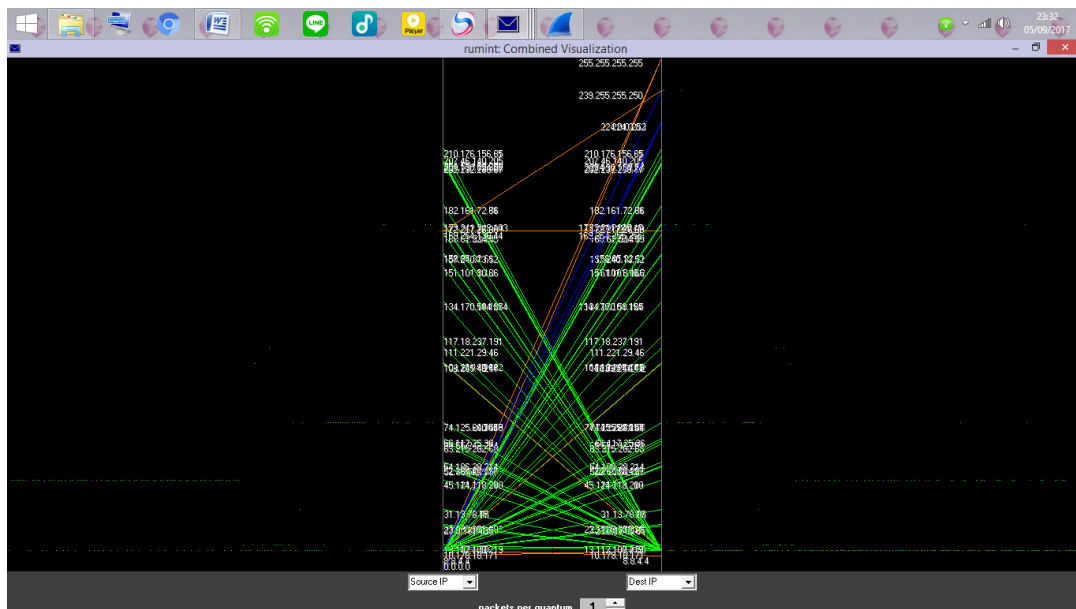
- A. Data pertama yang akan di visualisasikan adalah aliran data dari komputer saat mengakses dan melakukan penjelajahan di beritateknologi.com.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	173.241.248.143	10.178.18.171	TLSv1.2	85	Encrypted Alert
2	0.0000298	10.178.18.171	207.46.140.205	TCP	60	62001 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.122565	207.46.140.205	10.178.18.171	TCP	64	443 → 62001 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.122565	10.178.18.171	207.46.140.205	TCP	54	62001 → 443 [ACK] Seq=1 Ack=1 Win=60480 Len=0
5	0.160356	10.178.18.171	207.46.140.205	TLSv1.2	254	Client Hello
6	0.264017	207.46.140.205	10.178.18.171	TCP	1514	443 → 62001 [ACK] Seq=1 Ack=201 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
7	0.264023	207.46.140.205	10.178.18.171	TCP	1514	443 → 62001 [ACK] Seq=1461 Ack=201 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
8	0.264027	207.46.140.205	10.178.18.171	TCP	1514	443 → 62001 [ACK] Seq=2921 Ack=201 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
9	0.264030	207.46.140.205	10.178.18.171	TCP	1514	443 → 62001 [ACK] Seq=4381 Ack=201 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
10	0.275284	10.178.18.171	207.46.140.205	TCP	54	62001 → 443 [ACK] Seq=201 Ack=5941 Win=60480 Len=0
11	0.348880	10.178.18.171	74.125.24.94	TCP	55	7335 → 80 [ACK] Seq=1 Ack=1 Win=256 Len=1
12	0.539752	207.46.140.205	10.178.18.171	TLSv1.2	487	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
13	0.539466	74.125.24.94	10.178.18.171	TCP	68	80 → 7335 [ACK] Seq=1 Ack=2 Win=0 Len=0 SLE=1 SRE=2
14	0.538430	SansungL_Ah5f:19	Broadcast	ARP	42	Who has 10.178.18.1? Tell 10.178.18.17
15	0.566571	10.178.18.171	207.46.140.205	TCP	54	62001 → 443 [ACK] Seq=201 Ack=6274 Win=65792 Len=0
16	0.800377	10.178.18.171	207.46.140.205	TLSv1.2	268	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	0.861320	207.46.140.205	10.178.18.171	TLSv1.2	181	Change Cipher Spec, Encrypted Handshake Message
18	0.867255	10.178.18.171	207.46.140.205	TCP	1494	62001 → 443 [ACK] Seq=415 Ack=6381 Win=65536 Len=1440 [TCP segment of a reassembled PDU]
19	0.867744	10.178.18.171	207.46.140.205	TCP	843	Application Data
20	0.932054	207.46.140.205	10.178.18.171	TCP	60	443 → 62001 [ACK] Seq=6381 Ack=2044 Win=131328 Len=0
21	0.932059	207.46.140.205	10.178.18.171	TLSv1.2	139	Encrypted Handshake Message
22	0.936127	10.178.18.171	207.46.140.205	TLSv1.2	331	Encrypted Handshake Message
23	1.001382	207.46.140.205	10.178.18.171	TCP	1514	443 → 62001 [ACK] Seq=6466 Ack=2921 Win=131072 Len=1460 [TCP segment of a reassembled PDU]
24	1.001388	207.46.140.205	10.178.18.171	TCP	1514	443 → 62001 [ACK] Seq=7936 Ack=2921 Win=131072 Len=1460 [TCP segment of a reassembled PDU]
25	1.001392	207.46.140.205	10.178.18.171	TCP	1514	443 → 62001 [ACK] Seq=9386 Ack=2921 Win=131072 Len=1460 [TCP segment of a reassembled PDU]
26	1.001395	207.46.140.205	10.178.18.171	TCP	1514	443 → 62001 [ACK] Seq=10846 Ack=2921 Win=131072 Len=1460 [TCP segment of a reassembled PDU]
27	1.001400	207.46.140.205	10.178.18.171	TLSv1.2	603	Encrypted Handshake Message

Sumber Gambar :

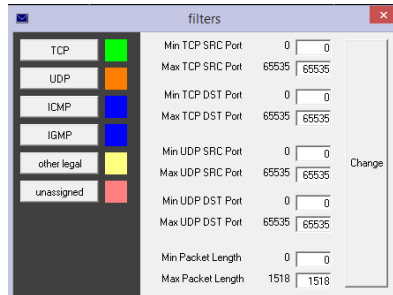
<http://edocs.ilkom.unsri.ac.id/id/eprint/1409>

Setelah data ini di upload di rumint, maka akan muncul view sebagai berikut:



Terdapat dua sisi yang dapat diatur di view tersebut, sisi kiri diatur sebagai Source IP atau IP Sumber sedangkan di sisi kanan diatur sebagai Destination IP atau IP Tujuan. View ini merupakan visualisasi dari data pcap di wireshark sehingga waktu dan IP yang ada sesuai dengan data-data tersebut. Waktu yang digunakan adalah 11351 detik atau 3.15 menit.

Pada tampilan view tersebut terdapat garis-garis yang enunjukkan aliran data dari kedua jenis IP (Source IP dan Destination IP) terdapat perbedaan warna pada garis-garis ini. Berdasarkan informasi dari aplikasi ini, perbedaan warna ini menunjukkan perbedaan protocol yang digunakan.

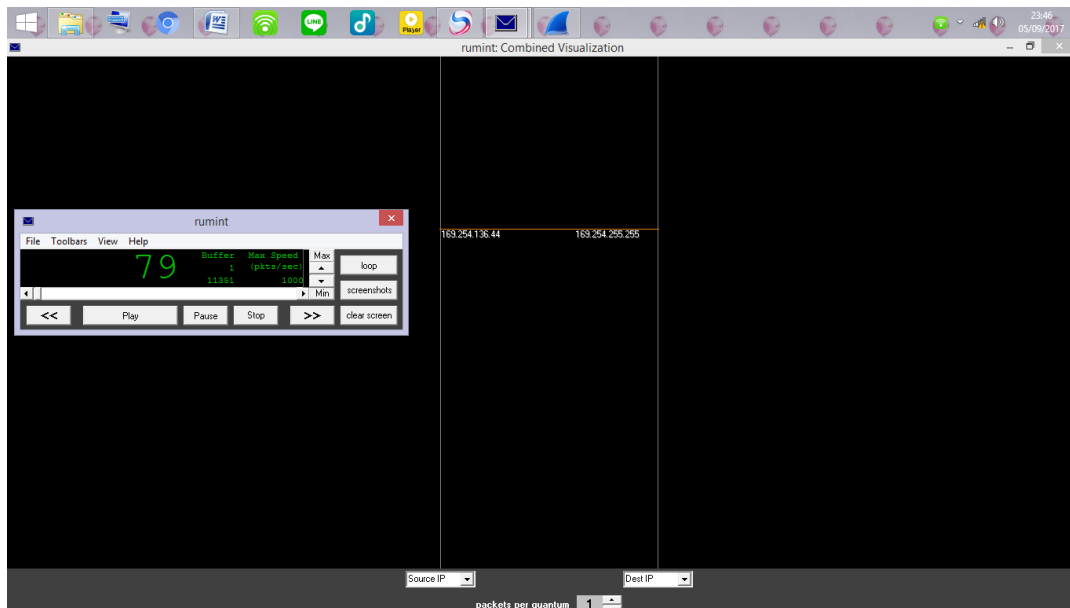


1. Garis Hijau

Garis hijau adalah garis yang paling mendominasi di proses ini. Ini artinya protokol yang paling banyak digunakan adalah TCP.

TCP digunakan untuk layanan-layanan yang membutuhkan keandalan data seerti WWW.

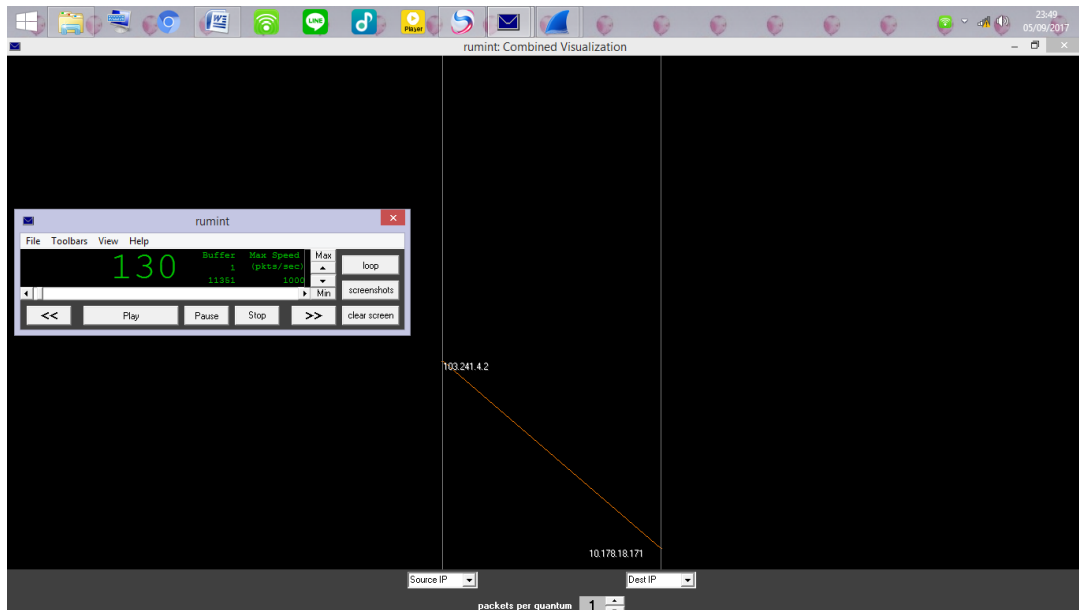
2. Garis kuning



Garis kuning ini pertama kali muncul pada proses ke 79 dengan Source IP 169.254.136.44 ke Destination IP 10.165.255.255. Berdasarkan data pada wireshark, pada proses ini protokol yang digunakan adalah NBNS.

79	5.735401	169.254.136.44	169.254.255.255	NBNS
----	----------	----------------	-----------------	------

Kemudian yang kedua adalah pada proses ke 130



Protokol yang digunakan adalah DNS.

130	6.675264	103.241.4.2	10.178.18.171	DNS
-----	----------	-------------	---------------	-----

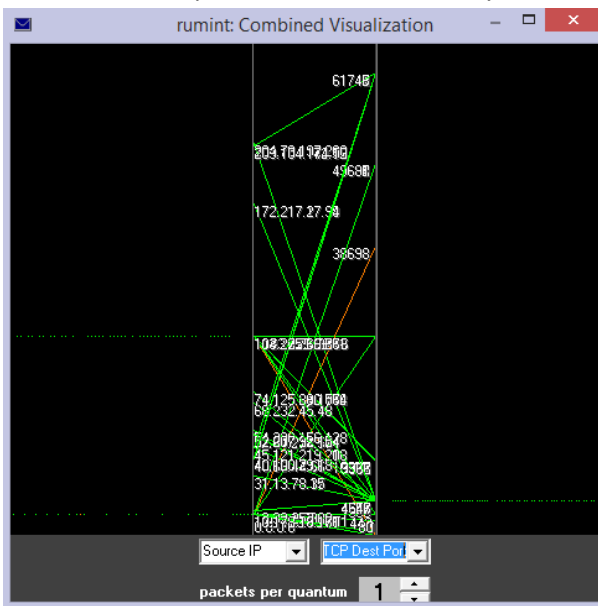
B. Data dari capture live streaming video.metrotv.com

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::169e3:a1ad:76bc::ff02::1:12	ff02::1:12	DHCPv6	138	Solicit XID: 0x949553 CID: 0001000128d684954a058a0003
2	0.057532	fe80::169e3:a1ad:76bc::ff02::1:12	ff02::1:12	LLNR	84	Standard query 0x204f A spad
3	0.057542	10.178.18.157	224.0.0.252	LLNR	64	Standard query 0x204f A spad
4	0.664714	10.178.18.157	10.178.18.255	NMSG	92	Name query 80 UPAD:000
5	1.002508	fe80::169e3:a1ad:76bc::ff02::1:12	ff02::1:12	LLNR	84	Standard query 0x204f A spad
6	1.002559	10.178.18.157	224.0.0.252	LLNR	64	Standard query 0x204f A spad
7	1.382954	10.178.18.157	10.178.18.255	NMSG	92	Name query 80 UPAD:000
8	2.208749	10.178.18.157	10.178.18.255	NMSG	92	Name query 80 UPAD:000
9	4.004378	fe80::169e3:a1ad:76bc::ff02::1:12	ff02::1:12	DHCPv6	138	Solicit XID: 0x949553 CID: 0001000128d684954a058a0003
10	4.658174	Microsoft 48163:82	Broadcast	ARP	60	who has 10.178.18.17 Tell 10.178.18.182
11	4.849637	10.178.18.171	103.241.4.2	DNS	81	Standard query 0x0225 A video.metrotv.com
12	4.851906	10.178.18.171	103.241.4.2	DNS	80	Standard query 0x0f57 A edge.metrotv.com
13	4.851795	10.178.18.171	103.241.4.2	DNS	78	Standard query 0x1777 A jupltx.com
14	4.851693	10.178.18.171	103.241.4.2	DNS	89	Standard query 0x4e15 A pageid2.googleplaynotification.com
15	4.861441	10.178.18.171	103.241.4.2	DNS	76	Standard query 0x0f28 A s1.l-p-jpdc.com
16	4.861336	10.178.18.171	103.241.4.2	DNS	78	Standard query 0x2cab A va.metrotv.com
17	4.918549	103.241.4.2	10.178.18.171	DNS	105	Standard query response 0x0225 A video.metrotv.com CNAME metrotv.com A 103.225.66.90 NS ns2.metrotv...
18	4.918412	10.178.18.171	103.225.66.90	TCP	66	4615 - 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 US=256 SACK_PERM=1
19	4.920893	10.178.18.171	74.125.200.192	TCP	66	4616 - 843 [SYN] Seq=0 Win=0 Len=0 MSS=1460 US=256 SACK_PERM=1
20	4.920799	10.178.18.171	103.241.4.2	DNS	79	Standard query 0x0081 A www.metrotv.com
21	4.920792	10.178.18.171	74.125.200.192	TCP	66	4617 - 441 [SYN] Seq=0 Win=0 Len=0 MSS=1460 US=256 SACK_PERM=1
22	4.920906	10.178.18.171	74.125.200.192	TCP	66	4618 - 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 US=256 SACK_PERM=1
23	4.940808	103.241.4.2	10.178.18.171	DNS	446	Standard query response 0x4e15 A pageid2.googleplaynotification.com CNAME pageid41.1.dmblclck.net A 172.217.2...
24	4.940832	103.241.4.2	10.178.18.171	DNS	399	Standard query response 0x1777 A jupltx.com A 52.207.92.154 A 54.164.231.176 A 52.21.52.114 A 54.174.16.175...
25	4.940833	103.241.4.2	10.178.18.171	DNS	150	Standard query response 0x2cab A va.metrotv.com A 103.225.66.100 NS ns3.metrotv.com NS ns1.metrotv...
26	4.947281	10.178.18.171	172.217.27.34	TCP	66	4619 - 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 US=256 SACK_PERM=1
27	4.947773	10.178.18.171	172.217.27.34	TCP	66	4620 - 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 US=256 SACK_PERM=1

Sumber Gambar :

<http://edocs.ilkom.unsri.ac.id/id/eprint/1409>

Jumlah proses yang ada adalah 1924 proses. Hasil visualisasinya adalah sebagai berikut:



Pada visualisasi diatas, sisi kiri sebagai Source IP dan sisi kanan sebagai TCP Dest Port.

Referensi

- [1] Siti Juairiah, Ria (2017) *Layanan TCP dan UDP*. Diakses dari <http://edocs.ilkom.unsri.ac.id/id/eprint/1409>