TUGAS MATA KULIAH JARINGAN KOMPUTER

“Visualisasi dan Analisis pcap File Menggunakan Aplikasi Rumint”

Nama : **ARFATTUSTARY NOORFIZIR**

NIM : **09011281520105**

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

BAB I

PENDAHULUAN

I.1. Latar Belakang

Forensik jaringan adalah ilmu yang berhubungan dengan pengambilan, perekaman, dan analisis lalu lintas jaringan untuk mendeteksi penyusupan dan menginvestigasinya. *Capturing Data* adalah kegiatan atau operasi yang berfungsi mencatat atau merekam semua data yang masuk dan keluar saat melakukan *browsing.*

Sebelum administrator jaringan beberapa tahun bekerja hanya dengan alat berbasis teks. Alat ini sering tidak memberikan ikhtisar yang akan membantu pengguna memahami gambar besarnya. Alat visualisasi lalu lintas jaringan telah berhasil mengaktifkan analis keamanan untuk memahami sifat lalu lintas yang ada dalam jaringan. Namun alat ini sangat bergantung pada keahlian manusia untuk menemukan anomali dalam pola lalu lintas dan serangan.

Sistem forensik jaringan melakukan analisis forensik dengan mengumpulkan data tingkat paket. Meskipun setiap paket harus diperiksa dengan menggunakan analisis terperinci, sangat penting untuk menemukan lalu lintas jaringan berbahaya dengan menganalisis keseluruhan aliran dan karakteristik. Data korelasi non-dimensional data tidak mudah dipahami namun membutuhkan keahlian dalam analisis data.

I.2. Rumusan Masalah

Sulitnya memahami dan menganalisis lalu lintas jaringan data.

I.3. Tujuan

Dapat memahami dan menganalisis lalu lintas jaringan data.

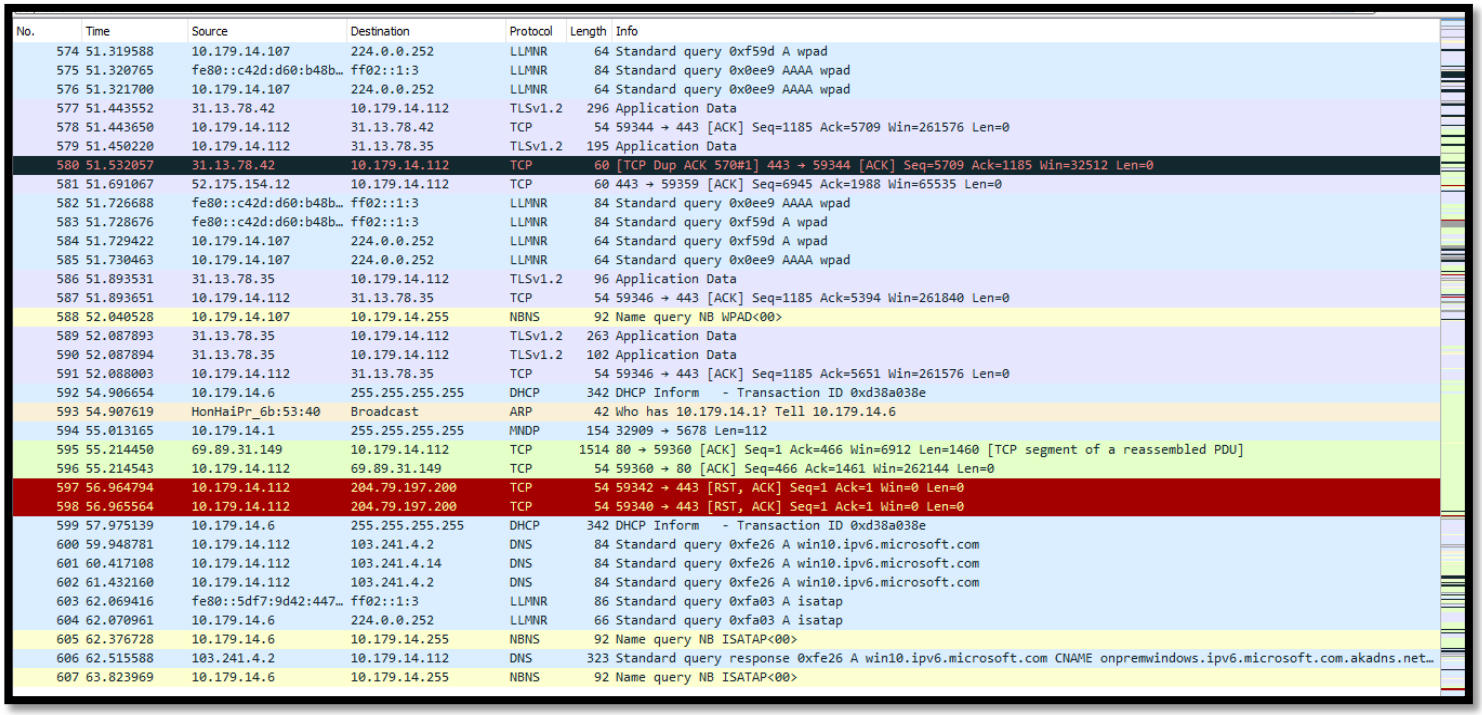
BAB II

HASIL DAN ANALISA

1. Cases Web Browsing (rahasiagadis.com)

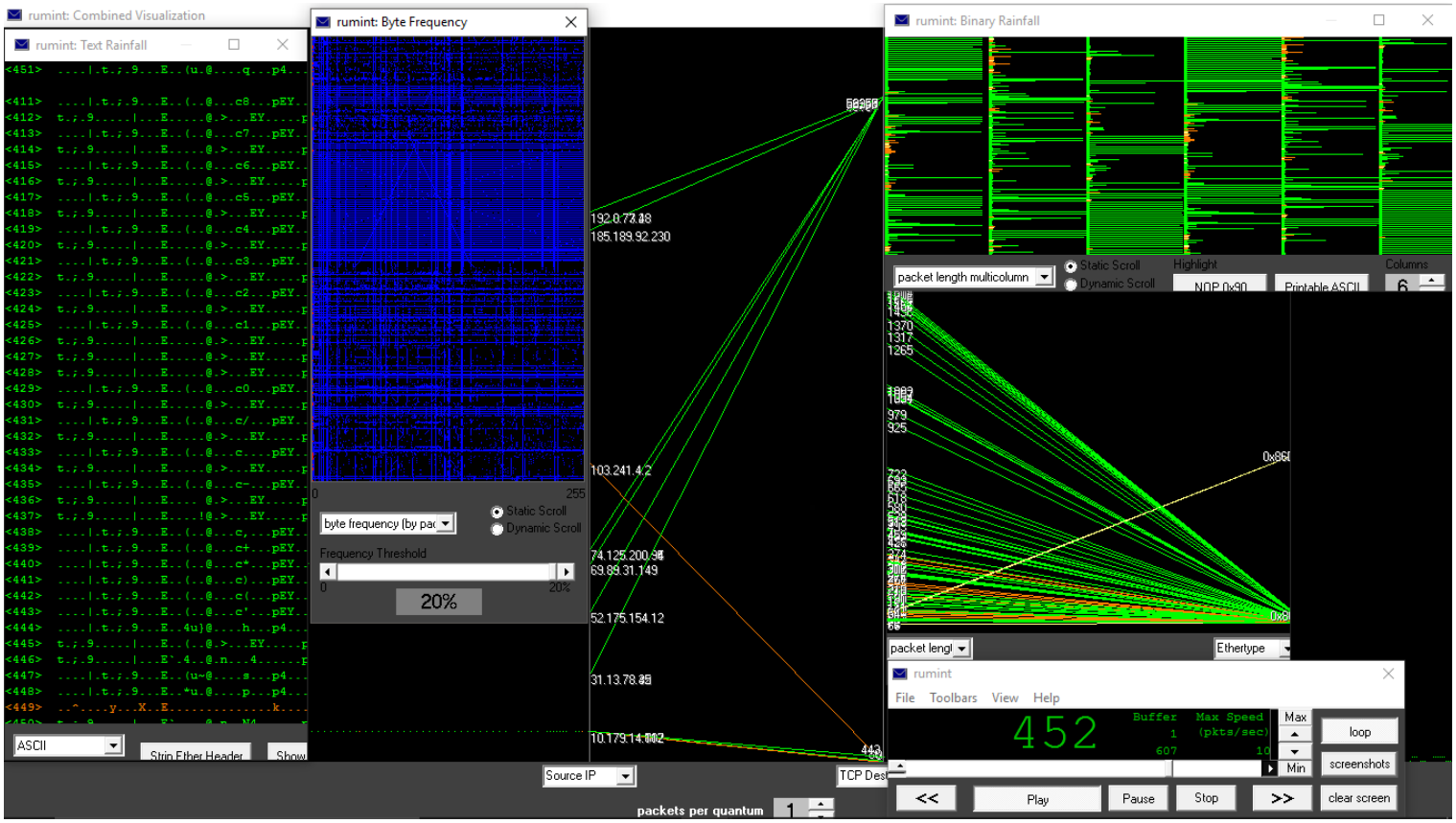
- IP Source : 10.179.14.112
- IP Destination : 69.89.31.149
- MAC Source : 74.C6.3B.81.39.0D
- MAC Destination : E4.8D.8C.17.7C.8C
- Lama Waktu : Dilakukan selama ±1 Menit

a. Capturing File Menggunakan Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
574	51.319588	10.179.14.107	224.0.0.252	LLMNR	64	Standard query 0xf59d A wpad
575	51.320765	fe80::c42d:d60:b48b…	ff02::1:3	LLMNR	84	Standard query 0x0ee9 AAAA wpad
576	51.321700	10.179.14.107	224.0.0.252	LLMNR	64	Standard query 0x0ee9 AAAA wpad
577	51.443552	31.13.78.42	10.179.14.112	TLSv1.2	296	Application Data
578	51.443650	10.179.14.112	31.13.78.42	TCP	54	59344 → 443 [ACK] Seq=1185 Ack=5709 Win=261576 Len=0
579	51.450220	10.179.14.112	31.13.78.35	TLSv1.2	195	Application Data
580	51.532057	31.13.78.42	10.179.14.112	TCP	60	[TCP Dup ACK 570#1] 443 → 59344 [ACK] Seq=5709 Ack=1185 Win=32512 Len=0
581	51.691067	52.175.154.12	10.179.14.112	TCP	60	443 → 59359 [ACK] Seq=6945 Ack=1988 Win=65535 Len=0
582	51.726688	fe80::c42d:d60:b48b…	ff02::1:3	LLMNR	84	Standard query 0x0ee9 AAAA wpad
583	51.728676	fe80::c42d:d60:b48b…	ff02::1:3	LLMNR	84	Standard query 0xf59d A wpad
584	51.729422	10.179.14.107	224.0.0.252	LLMNR	64	Standard query 0xf59d A wpad
585	51.730463	10.179.14.107	224.0.0.252	LLMNR	64	Standard query 0x0ee9 AAAA wpad
586	51.893531	31.13.78.35	10.179.14.112	TLSv1.2	96	Application Data
587	51.893651	10.179.14.112	31.13.78.35	TCP	54	59346 → 443 [ACK] Seq=1185 Ack=5394 Win=261840 Len=0
588	52.040528	10.179.14.107	10.179.14.255	NBNS	92	Name query NB WPAD<00>
589	52.087893	31.13.78.35	10.179.14.112	TLSv1.2	263	Application Data
590	52.087894	31.13.78.35	10.179.14.112	TLSv1.2	102	Application Data
591	52.088003	10.179.14.112	31.13.78.35	TCP	54	59346 → 443 [ACK] Seq=1185 Ack=5651 Win=261576 Len=0
592	54.906654	10.179.14.6	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xd38a038e
593	54.907619	HonHaiPr_6b:53:40	Broadcast	ARP	42	Who has 10.179.14.1? Tell 10.179.14.6
594	55.013165	10.179.14.1	255.255.255.255	MNDP	154	32909 → 5678 Len=112
595	55.214450	69.89.31.149	10.179.14.112	TCP	1514	80 → 59360 [ACK] Seq=1 Ack=466 Win=6912 Len=1460 [TCP segment of a reassembled PDU]
596	55.214543	10.179.14.112	69.89.31.149	TCP	54	59360 → 80 [ACK] Seq=466 Ack=1461 Win=262144 Len=0
597	56.964794	10.179.14.112	204.79.197.200	TCP	54	59342 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
598	56.965564	10.179.14.112	204.79.197.200	TCP	54	59340 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
599	57.975139	10.179.14.6	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xd38a038e
600	59.948781	10.179.14.112	103.241.4.2	DNS	84	Standard query 0xfe26 A win10.ipv6.microsoft.com
601	60.417108	10.179.14.112	103.241.4.14	DNS	84	Standard query 0xfe26 A win10.ipv6.microsoft.com
602	61.432160	10.179.14.112	103.241.4.2	DNS	84	Standard query 0xfe26 A win10.ipv6.microsoft.com
603	62.069416	fe80::5df7:9d42:447…	ff02::1:3	LLMNR	86	Standard query 0xfa03 A isatap
604	62.070961	10.179.14.6	224.0.0.252	LLMNR	66	Standard query 0xfa03 A isatap
605	62.376728	10.179.14.6	10.179.14.255	NBNS	92	Name query NB ISATAP<00>
606	62.515588	103.241.4.2	10.179.14.112	DNS	323	Standard query response 0xfe26 A win10.ipv6.microsoft.com CNAME onpremwindows.ipv6.microsoft.com.akadns.net…
607	63.823969	10.179.14.6	10.179.14.255	NBNS	92	Name query NB ISATAP<00>

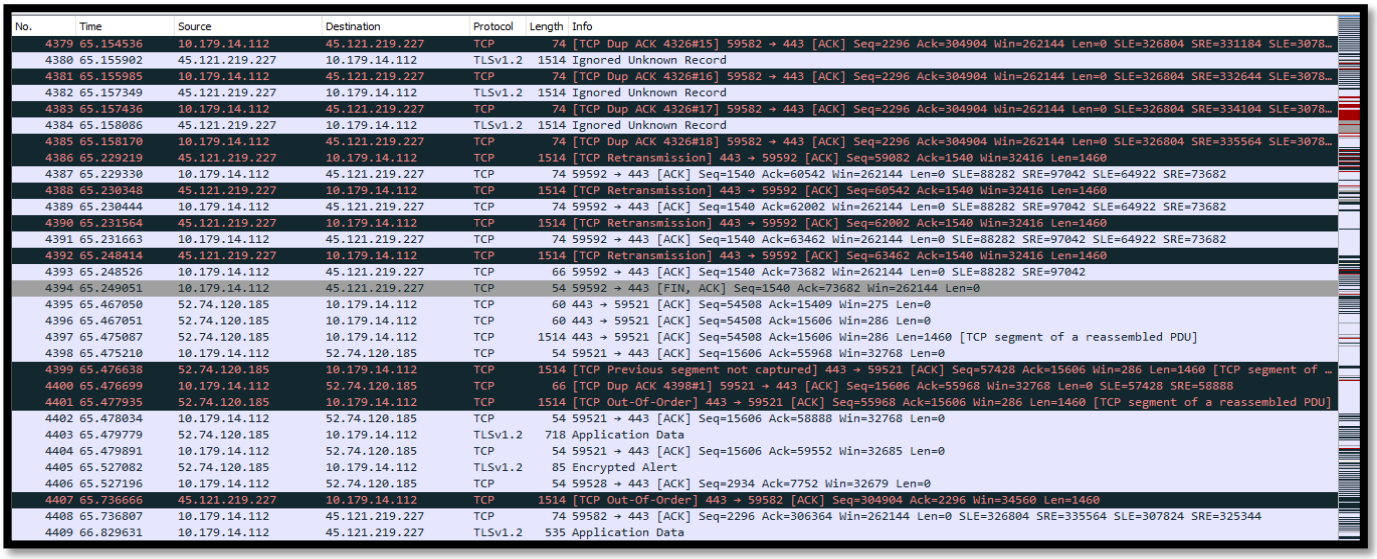
b. Visualization Menggunakan Rumint 2.14



2. Cases Online Streaming (vidio.com)

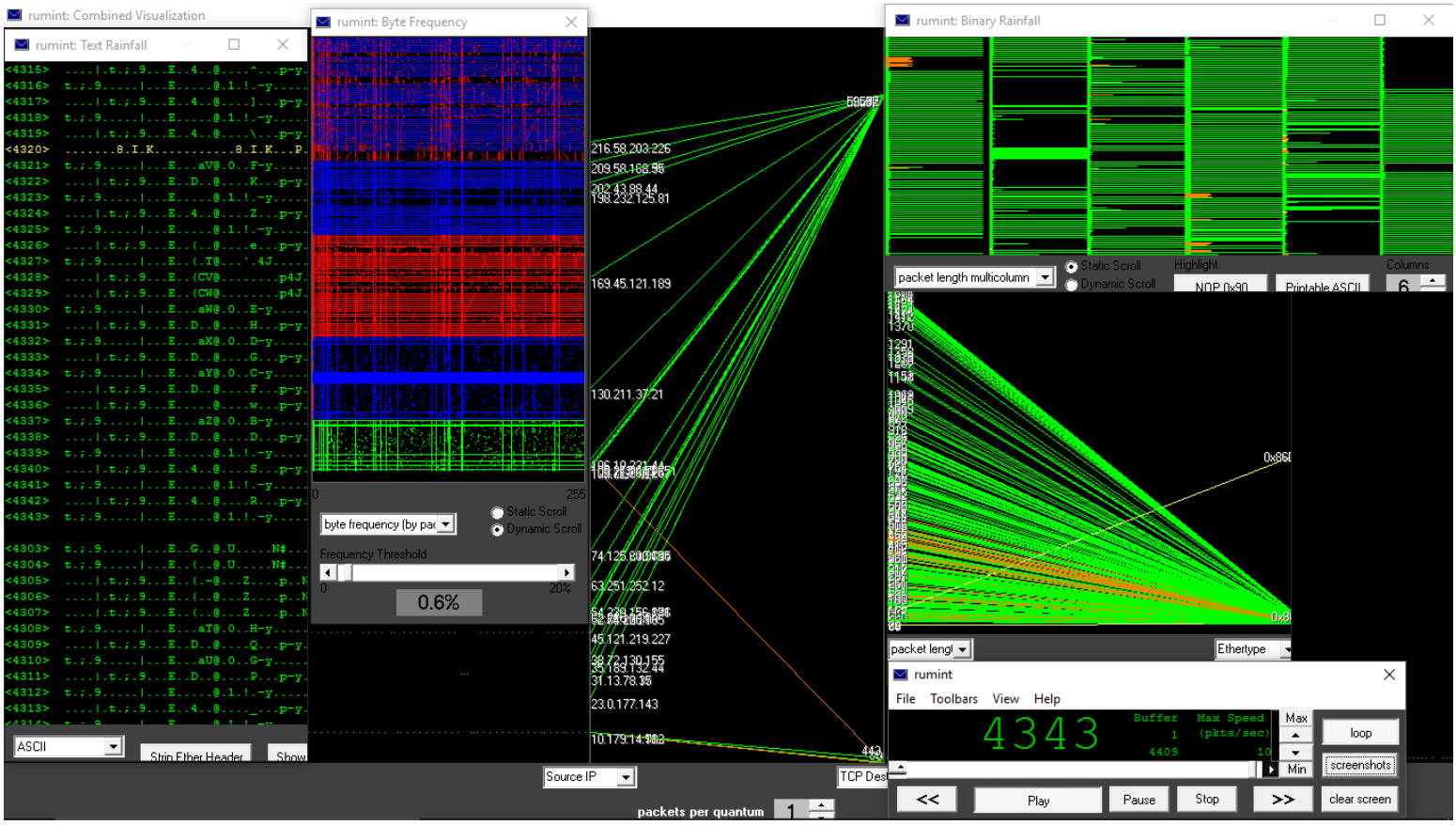
- IP Source : 10.179.14.112
- IP Destination : 209.58.162.57
- MAC Source : 74.C6.3B.81.39.0D
- MAC Destination : E4.8D.8C.17.7C.8C
- Lama Waktu : Dilakukan selama ±1 Menit

a. Menggunakan Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
4379	65.154536	10.179.14.112	45.121.219.227	TCP	74	[TCP Dup ACK 4326#15] 59582 → 443 [ACK] Seq=2296 Ack=304904 Win=262144 Len=0 SLE=326804 SRE=331184 SLE=3078…
4380	65.155902	45.121.219.227	10.179.14.112	TLSv1.2	1514	Ignored Unknown Record
4381	65.155985	10.179.14.112	45.121.219.227	TCP	74	[TCP Dup ACK 4326#16] 59582 → 443 [ACK] Seq=2296 Ack=304904 Win=262144 Len=0 SLE=326804 SRE=332644 SLE=3078…
4382	65.157349	45.121.219.227	10.179.14.112	TLSv1.2	1514	Ignored Unknown Record
4383	65.157436	10.179.14.112	45.121.219.227	TCP	74	[TCP Dup ACK 4326#17] 59582 → 443 [ACK] Seq=2296 Ack=304904 Win=262144 Len=0 SLE=326804 SRE=334104 SLE=3078…
4384	65.158086	45.121.219.227	10.179.14.112	TLSv1.2	1514	Ignored Unknown Record
4385	65.158170	10.179.14.112	45.121.219.227	TCP	74	[TCP Dup ACK 4326#18] 59582 → 443 [ACK] Seq=2296 Ack=304904 Win=262144 Len=0 SLE=326804 SRE=335564 SLE=3078…
4386	65.229219	45.121.219.227	10.179.14.112	TCP	1514	[TCP Retransmission] 443 → 59592 [ACK] Seq=59082 Ack=1540 Win=32416 Len=1460
4387	65.229330	10.179.14.112	45.121.219.227	TCP	74	59592 → 443 [ACK] Seq=1540 Ack=60542 Win=262144 Len=0 SLE=88282 SRE=97042 SLE=64922 SRE=73682
4388	65.230348	45.121.219.227	10.179.14.112	TCP	1514	[TCP Retransmission] 443 → 59592 [ACK] Seq=60542 Ack=1540 Win=32416 Len=1460
4389	65.230444	10.179.14.112	45.121.219.227	TCP	74	59592 → 443 [ACK] Seq=1540 Ack=62002 Win=262144 Len=0 SLE=88282 SRE=97042 SLE=64922 SRE=73682
4390	65.231564	45.121.219.227	10.179.14.112	TCP	1514	[TCP Retransmission] 443 → 59592 [ACK] Seq=62002 Ack=1540 Win=32416 Len=1460
4391	65.231663	10.179.14.112	45.121.219.227	TCP	74	59592 → 443 [ACK] Seq=1540 Ack=63462 Win=262144 Len=0 SLE=88282 SRE=97042 SLE=64922 SRE=73682
4392	65.248414	45.121.219.227	10.179.14.112	TCP	1514	[TCP Retransmission] 443 → 59592 [ACK] Seq=63462 Ack=1540 Win=32416 Len=1460
4393	65.248526	10.179.14.112	45.121.219.227	TCP	66	59592 → 443 [ACK] Seq=1540 Ack=73682 Win=262144 Len=0 SLE=88282 SRE=97042
4394	65.249051	10.179.14.112	45.121.219.227	TCP	54	59592 → 443 [FIN, ACK] Seq=1540 Ack=73682 Win=262144 Len=0
4395	65.467050	52.74.120.185	10.179.14.112	TCP	60	443 → 59521 [ACK] Seq=54508 Ack=15409 Win=275 Len=0
4396	65.467051	52.74.120.185	10.179.14.112	TCP	60	443 → 59521 [ACK] Seq=54508 Ack=15606 Win=286 Len=0
4397	65.475087	52.74.120.185	10.179.14.112	TCP	1514	443 → 59521 [ACK] Seq=54508 Ack=15606 Win=286 Len=1460 [TCP segment of a reassembled PDU]
4398	65.475210	10.179.14.112	52.74.120.185	TCP	54	59521 → 443 [ACK] Seq=15606 Ack=55968 Win=32768 Len=0
4399	65.476638	52.74.120.185	10.179.14.112	TCP	1514	[TCP Previous segment not captured] 443 → 59521 [ACK] Seq=57428 Ack=15606 Win=286 Len=1460 [TCP segment of …
4400	65.476699	10.179.14.112	52.74.120.185	TCP	66	[TCP Dup ACK 4398#1] 59521 → 443 [ACK] Seq=15606 Ack=55968 Win=32768 Len=0 SLE=57428 SRE=58888
4401	65.477935	52.74.120.185	10.179.14.112	TCP	1514	[TCP Out-Of-Order] 443 → 59521 [ACK] Seq=55968 Ack=15606 Win=286 Len=1460 [TCP segment of a reassembled PDU]
4402	65.478034	10.179.14.112	52.74.120.185	TCP	54	59521 → 443 [ACK] Seq=15606 Ack=58888 Win=32768 Len=0
4403	65.479779	52.74.120.185	10.179.14.112	TLSv1.2	718	Application Data
4404	65.479891	10.179.14.112	52.74.120.185	TCP	54	59521 → 443 [ACK] Seq=15606 Ack=59552 Win=32685 Len=0
4405	65.527082	52.74.120.185	10.179.14.112	TLSv1.2	85	Encrypted Alert
4406	65.527196	10.179.14.112	52.74.120.185	TCP	54	59528 → 443 [ACK] Seq=2934 Ack=7752 Win=32679 Len=0
4407	65.736666	45.121.219.227	10.179.14.112	TCP	1514	[TCP Out-Of-Order] 443 → 59582 [ACK] Seq=304904 Ack=2296 Win=34560 Len=1460
4408	65.736807	10.179.14.112	45.121.219.227	TCP	74	59582 → 443 [ACK] Seq=2296 Ack=306364 Win=262144 Len=0 SLE=326804 SRE=335564 SLE=307824 SRE=325344
4409	66.829631	10.179.14.112	45.121.219.227	TLSv1.2	535	Application Data

b. Visualization Menggunakan Rumint 2.14



Percobaan ini menggunakan teknik visualisasi dari software Rumint 2.14 yang digunakan untuk memantau pola lalu lintas jaringan. Software ini memberikan gambaran lalu lintas dalam bentuk Text Rainfall, Bye Frequency, Parallel Plot, Binary Plot, dan Combined.

BAB III

PENUTUP

III.1. Kesimpulan

Lalu lintas jaringan dapat divisualisasikan dalam bentuk Text Rainfall, Byet Frequency, Parallel Plot, Binary Plot, dan Combined dengan menggunakan Software.

REFERENSI

Marode and K.Chavan. Survey of Network Traffic Visualization Techniques, 2014. https://pdfs.semanticscholar.org/3b29/11b99879c1c5f3178d5a562fb8cd1b248b46.pdf

Noorfizir, Arfattustary. Capturing Data, 2017. http://edocs.ilkom.unsri.ac.id/1454/1/09011281520105_Arfattustary_Noorfizir2.pdf