

KOMUNIKASI DATA DAN JARINGAN KOMPUTER
ANALISA TRAFFIC IP CONVERSATION DAN MATRIX



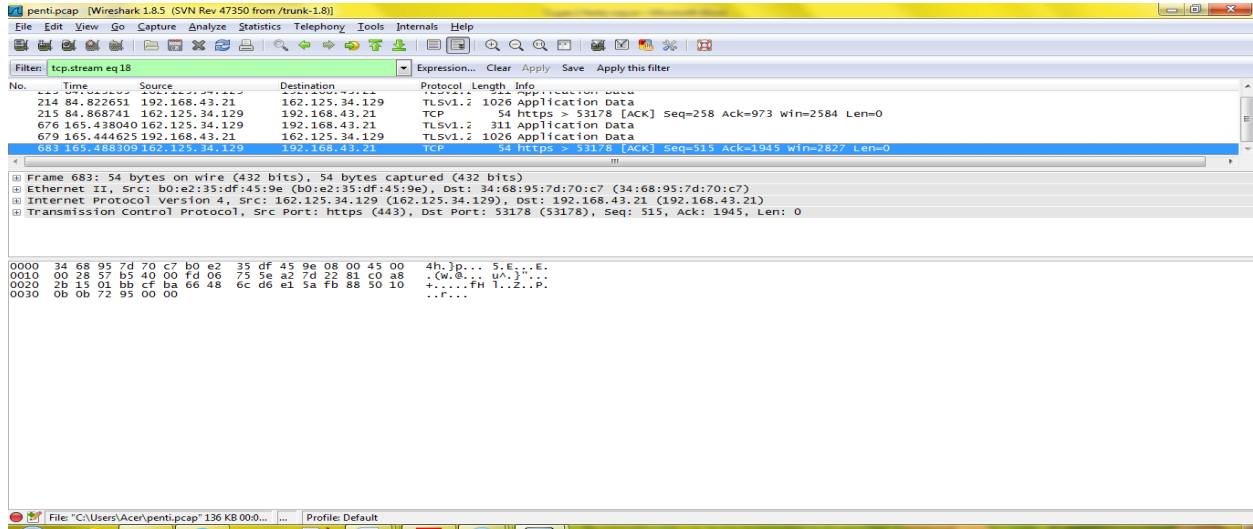
Disusun Oleh :

Nama : Fenty Mareta

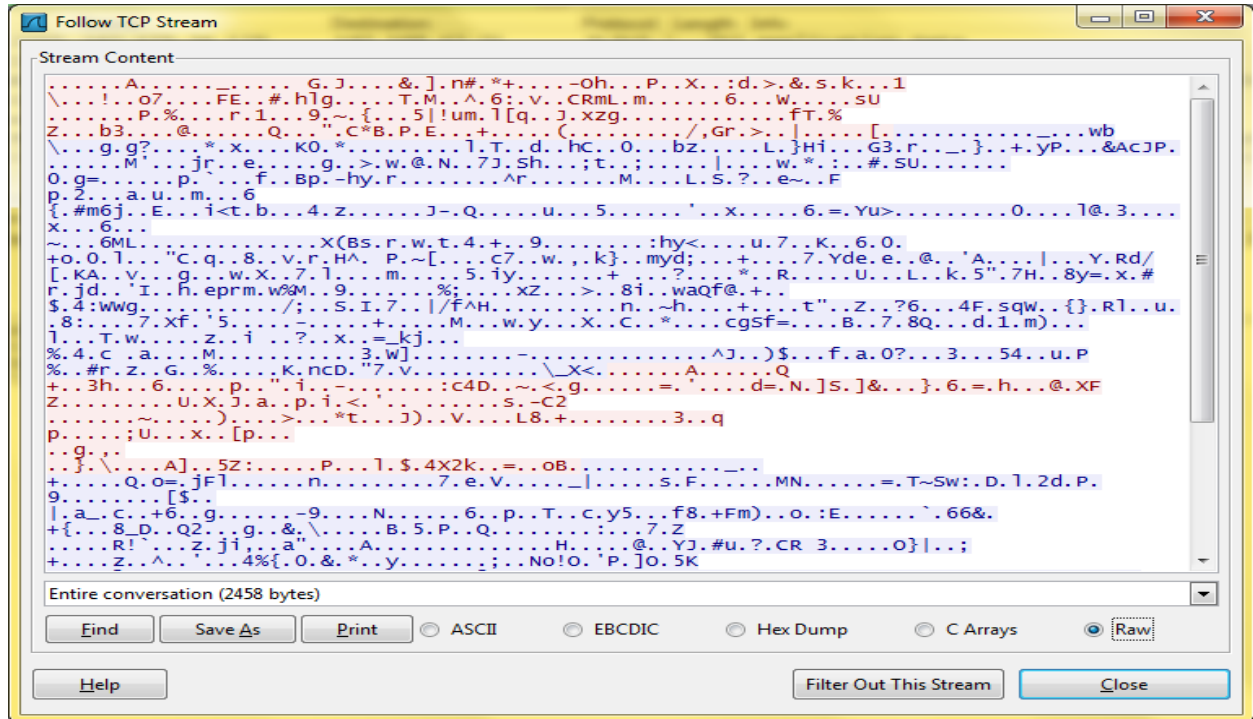
NIM : 09031181520010

SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

IP Conversation



Tampilan pada wireshark dibawah ini kita pilih source ke destination dengan protocol TCP untuk mengetahui kegiatan atau server yang dituju saat itu. Dengan cara klik kanan lalu pilih Follow TCP Stream, tampilannya seperti dibawah ini :



Terlihat pada gambar diatas bahwa jaringan tidak mengakses kemanapun.

❖ Melihat endpoint baik physical atau IPnya.

Full Analysis\Physical Endpoint: 35

Name	Bytes	Packets	Bits Per Second	Bytes Received	Packets Rec
Local Segment	123.890 KB	834	2.944 Kbps	0 B	
Local Host	123.421 KB	830	2.944 Kbps	65.765 KB	
34:68:95:7D:70:C7	114.407 KB	766	1.472 Kbps	65.765 KB	
192.168.43.21	112.322 KB	741	1.472 Kbps	65.560 KB	
0A:00:27:00:00:00	9.014 KB	64	1.472 Kbps	0 B	
192.168.56.1	8.686 KB	60	1.472 Kbps	0 B	
B0:E2:35:DF:45:9E	109.778 KB	722	0 bps	44.014 KB	
207.250.191.52	28.250 KB	62	0 bps	2.243 KB	
118.98.42.81	17.944 KB	140	0 bps	10.880 KB	
172.217.27.110	15.229 KB	125	0 bps	6.022 KB	
23.0.181.9	10.747 KB	66	0 bps	3.821 KB	
192.168.43.1	7.593 KB	56	0 bps	2.105 KB	

Local Segment\Physical Conversation: 10

Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Packets
28:C2:DD:4B:85:29	FF:FF:FF:FF:FF:FF	00:00:00	42 B	42 B	0 B	1
E0:B9:A5:FD:57:FB	33:33:00:01:00:02	00:01:03	438 B	438 B	0 B	3
34:68:95:7D:70:C7	33:33:00:01:00:02	00:01:03	1.019 KB	1.019 KB	0 B	7
0A:00:27:00:00:00	33:33:00:01:00:03	00:00:55	336 B	336 B	0 B	4
0A:00:27:00:00:00	01:00:5E:00:00:FC	00:00:55	256 B	256 B	0 B	4
34:68:95:7D:70:C7	33:33:00:01:00:03	00:00:55	672 B	672 B	0 B	8
34:68:95:7D:70:C7	01:00:5E:00:00:FC	00:00:55	512 B	512 B	0 B	8

Full Analysis\IP Endpoint: 33

Name	Bytes	Packets	Bits Per Second	Bytes Received	Packets Rec
Local Subnet	121.008 KB	801	2.944 Kbps	60.072 KB	
192.168.43.0/24	112.322 KB	741	1.472 Kbps	60.072 KB	
192.168.43.21	112.322 KB	741	1.472 Kbps	65.560 KB	
192.168.43.1	7.593 KB	56	0 bps	2.105 KB	
192.168.43.255	2.454 KB	21	1.472 Kbps	2.454 KB	
192.168.56.0/24	8.686 KB	60	1.472 Kbps	0 B	
192.168.56.1	8.686 KB	60	1.472 Kbps	0 B	
192.168.56.255	2.454 KB	21	1.472 Kbps	2.454 KB	
Internet Addresses	101.775 KB	656	0 bps	41.703 KB	
United States	45.981 KB	214	0 bps	14.101 KB	
207.250.191.52	28.250 KB	62	0 bps	2.243 KB	
199.119.33.178	7.231 KB	81	0 bps	5.228 KB	

Local Subnet\IP Conversation: 21

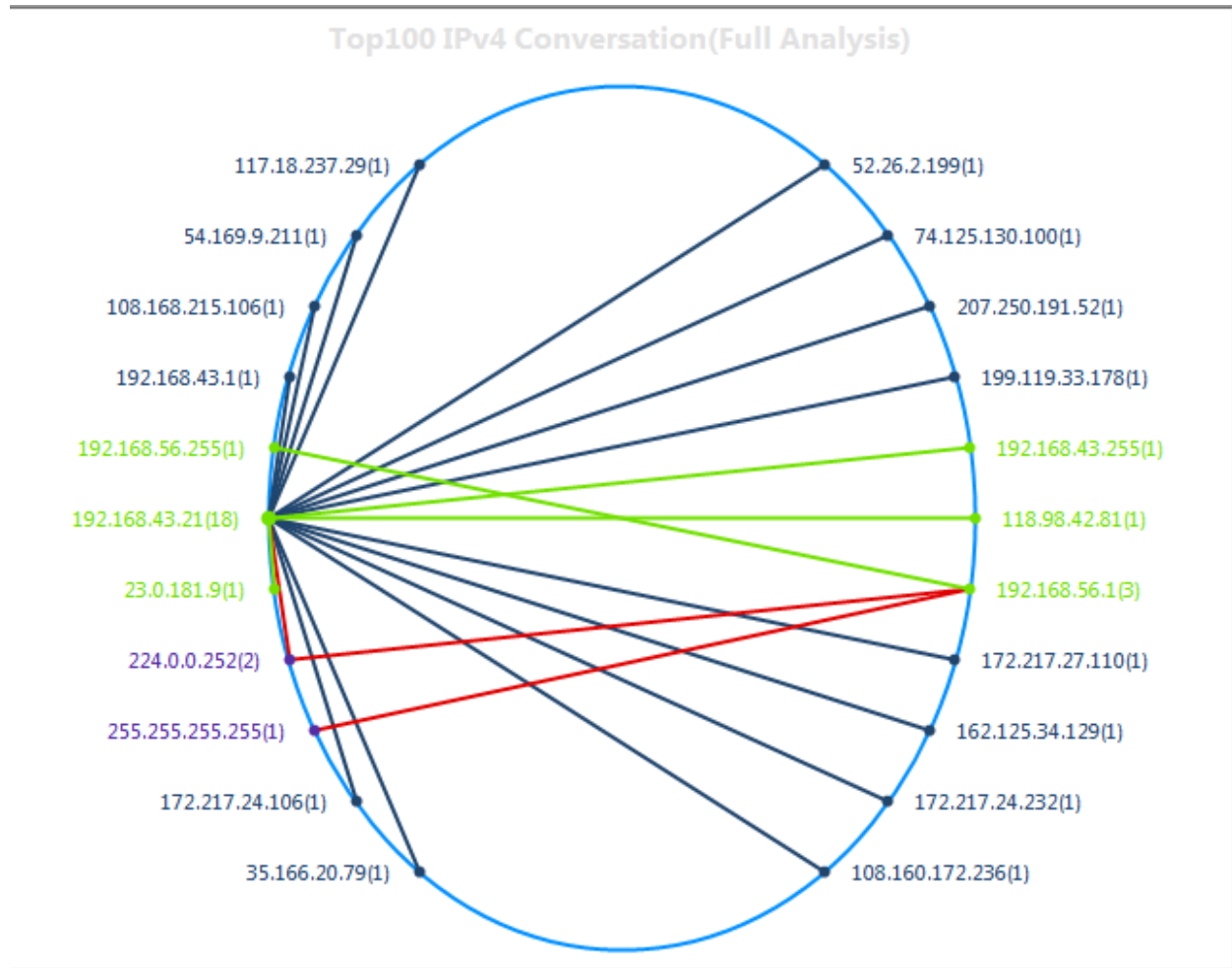
Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Packets
192.168.43.21	52.26.2.199	00:00:03	820 B	326 B	494 B	14
192.168.43.21	117.18.237.29	00:00:06	325 B	163 B	162 B	6
192.168.43.21	108.160.172.236	00:00:45	247 B	108 B	139 B	4
192.168.43.21	35.166.20.79	00:00:51	901 B	438 B	463 B	16
192.168.43.21	74.125.130.100	00:01:57	1.360 KB	701 B	692 B	19
192.168.43.21	54.169.9.211	00:00:00	248 B	124 B	124 B	4
192.168.43.21	172.217.24.232	00:02:32	4.354 KB	2.436 KB	1.919 KB	43

Akan terlihat statistic lalu lintas data yang terjadi pada masing-masing alamat mac address ataupun ip address pada jaringan yang terkoneksi dengan kita.

Dashboard Summary Diagnosis Protocol Physical Endpoint IP Endpoint Physical Conversation IP Conversation x TCP Conversation UDI							
Full Analysis\IP Conversation:							21
Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Packets	
192.168.43.21	52.26.2.199	00:00:03	820 B	326 B	494 B	14	
192.168.43.21	117.18.237.29	00:00:06	325 B	163 B	162 B	6	
192.168.43.21	108.160.172.236	00:00:45	247 B	108 B	139 B	4	
192.168.43.21	35.166.20.79	00:00:51	901 B	438 B	463 B	16	
192.168.43.21	74.125.130.100	00:01:57	1.360 KB	701 B	692 B	19	
192.168.43.21	54.169.9.211	00:00:00	248 B	124 B	124 B	4	
192.168.43.21	172.167.24.232	00:02:32	4.354 KB	2.436 KB	1.919 KB	43	
192.168.43.21	172.217.24.106	00:02:33	4.400 KB	2.478 KB	1.923 KB	43	
192.168.43.21	207.250.191.52	00:00:12	28.250 KB	2.243 KB	26.007 KB	62	
192.168.43.21	108.168.215.106	00:00:09	2.560 KB	1.701 KB	879 B	15	
162.125.34.129	192.168.43.21	00:02:50	7.217 KB	2.139 KB	5.078 KB	18	
192.168.56.1	255.255.255.255	00:03:01	5.981 KB	5.981 KB	0 B	35	
192.168.43.21	199.119.33.178	00:03:11	7.231 KB	5.228 KB	2.004 KB	81	
192.168.43.21	192.168.43.21	00:02:12	7.502 KB	3.105 KB	5.407 KB	56	

TCP Conversation UDP Conversation							
192.168.43.21 <-> 52.26.2.199\TCP Conversation:							2
Endpoint 1 ->	<- Endpoint 2	Packets	Bytes	Protocol	Duration	Bytes ->	
192.168.43.21:53248	52.26.2.199:443	7	410 B	HTTPS	00:00:01	163 B	
192.168.43.21:53264	52.26.2.199:443	7	410 B	HTTPS	00:00:00	163 B	

Matrix



Hasil dari Matrix sama saja seperti IP conversation menunjukkan saat endpoint tersambung ke jaringan kita atau apa yang sedang terjadi pada traffic data dilihat dari bagian Summary seperti di bawah ini muncul kode – kode mesin yang sulit saya pahami namun ada kode – kode yang bisa kita baca dan menunjukkan suatu kegiatan yang sedang terjadi pada data disaat itu .

IP	Peer Hosts	Packets Sent	Bytes Sent	Packets Received	Bytes Received
172.217.24.232	1	23	1.919 KB	20	2436 KB
162.125.34.129	1	12	2.139 KB	6	5.078 B
172.217.27.110	1	65	9.207 KB	60	6.022 KB
192.168.56.1	1	60	8.686 KB	0	0 B
118.98.42.81	1	70	7.064 KB	70	10.880 KB
192.168.43.255	1	0	0 B	21	2.454 KB
199.119.33.178	1	36	2.004 KB	45	5.228 KB
207.250.191.52	1	44	26.007 KB	18	2.243 KB
74.125.130.100	1	10	692 B	9	701 B
52.26.2.199	1	8	494 B	6	326 B

Kesimpulan :

Traffic pada Ip conversation dan Matrix adalah sama memiliki satu fungsi yang pada akhirnya tujuannya sama namun tampilan pada tab-nya yang berbeda secara kasat mata kita lebih mudah memahami dan tampilan matrix lebih menarik namun tampilan IP conversation juga sangat familiar dan menampilkan detail – detail traffic data dengan rinci hal tersebut sangat membantu dalam memahami traffic tersebut.