

**KOMUNIKASI DATA DAN JARINGAN KOMPUTER**  
**ANALISA TRAFFIC IP CONVERSATION DAN MATRIX**



Disusun Oleh :

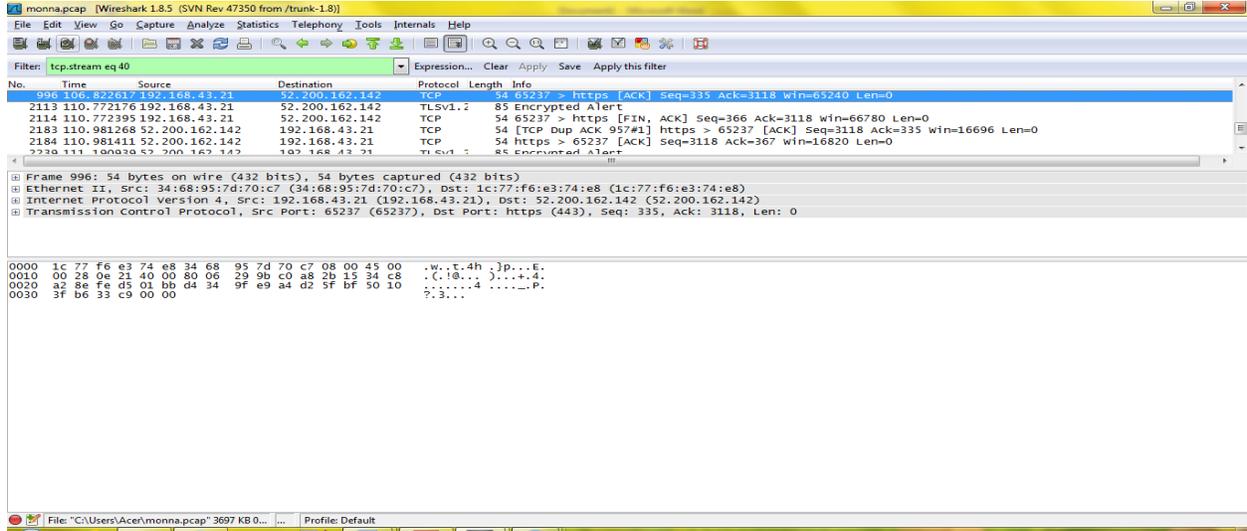
Nama : Ayu Monaputri

NIM : 09031181520031

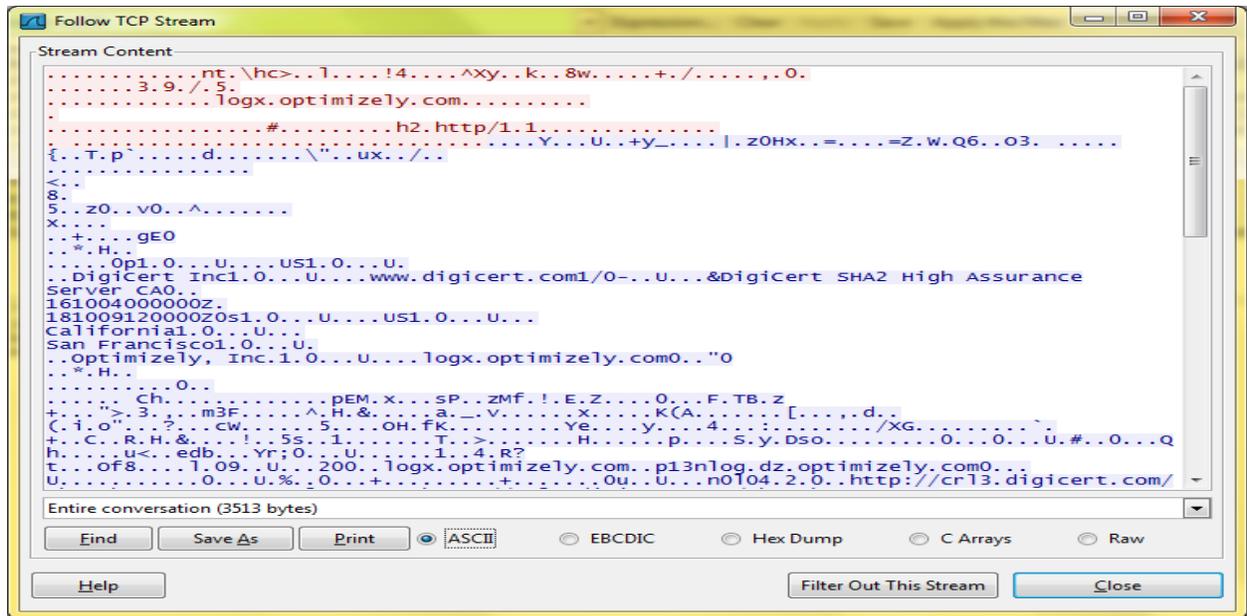
**SISTEM INFORMASI**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS SRIWIJAYA**

# IP Conversation

IP Conversation dapat memungkinkan pelacakan percakapan antara endpoint pada jaringan Anda, dengan asumsi semua traffic melewati workstation.



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 terdapat banyak kode yang sulit dimengerti namun ada beberapa kode yang masih dapat dipahami seperti terlihat di gambar user mengakses domain server www.digicert.com.

- Melihat endpoint baik physical atau IPnya.

Full Analysis/Physical Endpoint: 90

Name	Bytes	Packets	Bits Per Second	Bytes Received	Packets Rec
Local Segment	3,625 MB	7,794	716.712 Kbps	0 B	
Local Host	3,625 MB	7,790	716.712 Kbps	3,135 MB	4
34:68:95:7D:70:C7	3,610 MB	7,688	716.712 Kbps	3,135 MB	4
192.168.43.21	3,608 MB	7,648	716.712 Kbps	3,135 MB	4
0A:00:27:00:00:00	14,854 KB	102	0 bps	0 B	
192.168.56.1	14,443 KB	97	0 bps	0 B	
1C:77:F6:E3:74:E8	3,497 MB	6,904	716.712 Kbps	435,657 KB	2
104.93.122.35	1,194 MB	1,512	302.408 Kbps	57,885 KB	
104.93.87.225	1,180 MB	2,047	1.296 Kbps	72,879 KB	
216.58.221.70	164,521 KB	249	124.704 Kbps	12,427 KB	
210.176.156.41	111,657 KB	247	432 bps	38,516 KB	
128.199.158.79	99,407 KB	143	0 bps	4,105 KB	
151.101.100.73	88,878 KB	187	0 bps	17,680 KB	
151.101.8.68	77,665 KB	142	54.440 Kbps	17,683 KB	
52.200.162.142	57,219 KB	185	0 bps	24,879 KB	
118.97.159.24	50,381 KB	64	0 bps	1,511 KB	
54.153.109.234	46,052 KB	171	0 bps	20,405 KB	
216.58.221.66	42,288 KB	95	0 bps	8,335 KB	
210.176.156.31	39,487 KB	82	0 bps	11,472 KB	
104.93.230.128	25,654 KB	93	440 bps	6,044 KB	
74.125.68.157	25,181 KB	81	1.232 Kbps	6,607 KB	
23.21.225.249	16,540 KB	39	0 bps	14,958 KB	
23.41.75.27	14,561 KB	60	44.008 Kbps	4,284 KB	
52.72.203.93	13,569 KB	39	32.808 Kbps	3,424 KB	

Full Analysis/IP Endpoint: 89

Name	Bytes	Packets	Bits Per Second	Bytes Received	Packets Rec
Local Subnet	3,622 MB	7,745	716.712 Kbps	3,062 MB	4
192.168.43.0/24	3,608 MB	7,648	716.712 Kbps	3,062 MB	4
192.168.43.21	3,608 MB	7,648	716.712 Kbps	3,135 MB	4
192.168.43.1	95,108 KB	522	13.680 Kbps	20,759 KB	
192.168.43.255	3,853 KB	32	0 bps	3,853 KB	
192.168.56.0/24	14,443 KB	97	0 bps	0 B	
192.168.56.1	14,443 KB	97	0 bps	0 B	
192.168.56.255	3,853 KB	32	0 bps	3,853 KB	
Internet Addresses	3,510 MB	7,083	703.032 Kbps	458,502 KB	2
N/A	2,481 MB	4,171	353.856 Kbps	181,350 KB	1
104.93.122.35	1,194 MB	1,512	302.408 Kbps	57,885 KB	
104.93.87.225	1,180 MB	2,047	1.296 Kbps	72,879 KB	

Local Subnet/IP Conversation: 76

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	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
192.168.43.21	172.217.24.106	00:02:33	4,400 KB	2,478 KB	1,923 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.

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	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
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
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	172.217.27.110	00:03:21	15.229 KB	6.022 KB	9.207 KB	125
192.168.43.21	23.0.181.9	00:03:21	10.747 KB	3.821 KB	6.926 KB	66
192.168.43.21	118.98.42.81	00:00:54	17.944 KB	10.880 KB	7.064 KB	140
192.168.43.21	255.255.255.255	00:00:00	342 B	342 B	0 B	1
192.168.56.1	224.0.0.252	05:09:33	320 B	320 B	0 B	5
192.168.43.21	224.0.0.252	05:09:33	640 B	640 B	0 B	10
192.168.43.21	104.93.119.50	00:00:05	804 B	456 B	348 B	14
192.168.43.21	128.199.158.79	00:01:00	99.407 KB	4.105 KB	95.302 KB	143
192.168.43.21	31.13.78.17	00:00:00	3.197 KB	1.449 KB	1.748 KB	19
192.168.43.21	138.108.140.100	00:00:06	1.792 KB	985 B	850 B	18
192.168.43.21	31.13.78.35	00:00:01	3.486 KB	1.620 KB	1.866 KB	17
162.125.34.129	192.168.43.21	05:13:55	21.482 KB	8.519 KB	12.964 KB	53
192.168.43.21	54.230.150.201	00:00:10	1.397 KB	667 B	764 B	9
192.168.43.21	118.97.159.32	00:00:20	1.300 KB	794 B	537 B	11

Terdapat perintah GET yang menunjukkan bahwa jaringan mulai terkoneksi atau memanggil server endpoint pada beacon.krxd.net

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
3491	21:34:34.744663	54.244.124.93:80	192.168.43.21:65317	HTTP	54		Seq=0244363006,
3513	21:34:35.056924	54.244.124.93:80	192.168.43.21:65317	HTTP	658		S: HTTP/1.1 204 N
3528	21:34:35.257129	192.168.43.21:65317	54.244.124.93:80	HTTP	54		Seq=1352892827,,
3689	21:34:35.728724	192.168.43.21:65317	54.244.124.93:80	HTTP	479	GET /data.gif?_kuid=Kb...	C: GET /data.gif?
3699	21:34:35.932450	54.244.124.93:80	192.168.43.21:65318	HTTP	54		Seq=1321083748,,
3700	21:34:35.932591	192.168.43.21:65318	54.244.124.93:80	HTTP	54		Seq=1380778189,,
3701	21:34:35.933881	192.168.43.21:65318	54.244.124.93:80	HTTP	54		Seq=1380778189,,
3722	21:34:35.978502	54.244.124.93:80	192.168.43.21:65317	HTTP	54		Seq=0244363010

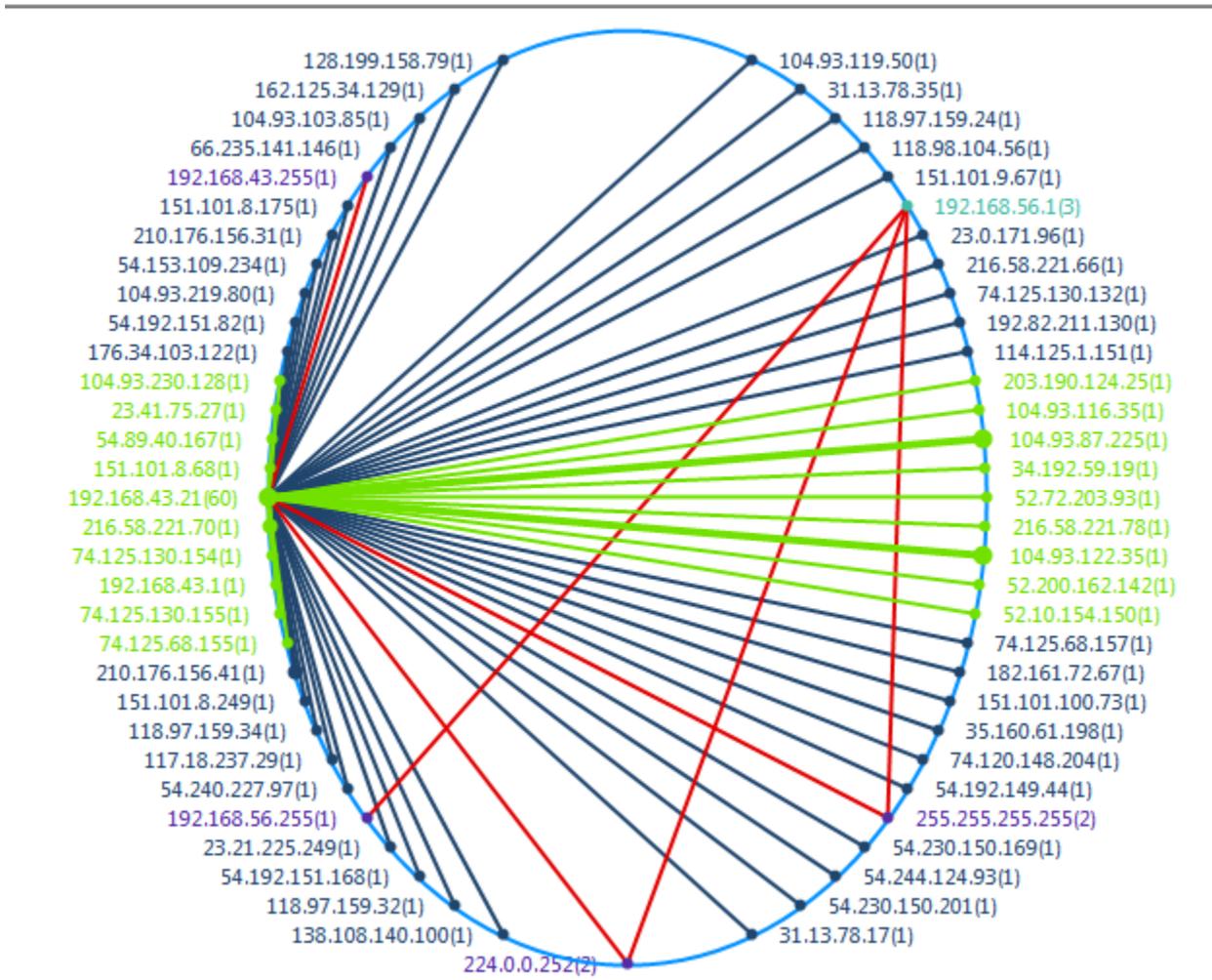
  

Checksum:	0x82C0	(Correct)	[50/2]
Urgent point:	0		[52/2]
No TCP Option			[54/0]
<b>HTTP - Hypertext Transfer Protocol</b>			[54/425]
HTTP Request:	GET /data.gif?_kuid=KbgPcZ9U6_kdpid=a8138b01-9fff-43bb-b649-99241ab62170&dldata=201604240826216890692761747		
Host:	beacon.krxd.net		
User-Agent:	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0		

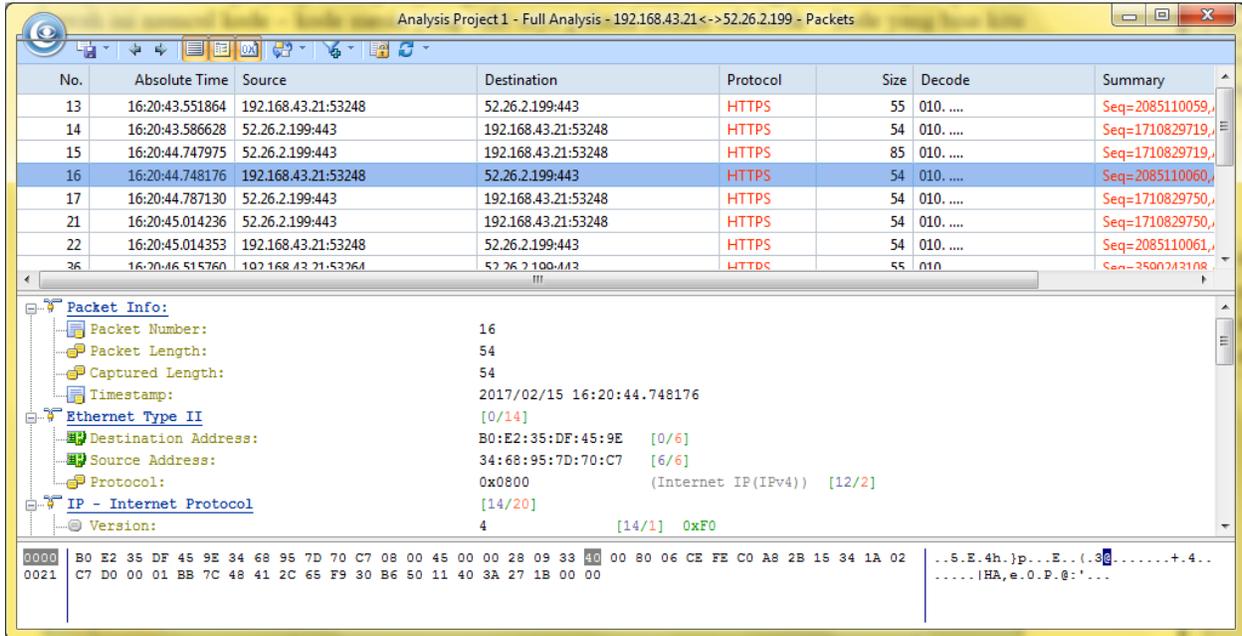
0000	1C 77 F6 E3 74 E8 34 68 95 7D 70 C7 08 00 45 00 01 D1 10 D2 40 00 80 06 49 46 C0 A8 2B 15 36 F4	.w.t.4h.jp...E.....@...IF...+6.
0020	7C 5D FF 25 00 50 50 A3 81 9B 0E 90 B1 5A 50 18 40 A0 82 C0 00 00 47 45 54 20 2F 64 61 74 61 2E	]%.PP.....ZP.....GET /data
0040	67 69 66 3F 5F 6B 75 69 64 3D 4B 62 67 50 63 5A 39 55 26 5F 6B 64 70 69 64 3D 61 38 31 33 38 62	gif?_kuid=KbgPcZ9U6_kdpid=a8138b
0060	30 31 2D 39 66 66 66 66 2D 34 33 62 62 2D 62 36 34 39 2D 39 39 32 34 31 61 62 36 32 31 37 30 26 64	01-9fff-43bb-b649-99241ab62170&d
0080	6C 78 69 64 3D 32 30 31 36 30 34 32 34 30 38 32 36 32 31 36 38 39 30 36 39 32 37 36 31 37 34 37	ldata=201604240826216890692761747
00A0	31 26 64 6C 78 64 61 74 61 3D 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 62 65 61 63 6F	Host: beaco
00C0	6E 2E 6B 72 78 64 2E 6E 65 74 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F	n.krxd.net...User-Agent: Mozilla/
00E0	35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 72 76 3A 35	5.0 (Windows NT 6.1; WOW64; rv:5

# MATRIX



IP	Peer Hosts	Packets Sent	Bytes Sent	Packets Received	Bytes Received
104.93.119.50	1	6	348 B	8	456 B
31.13.78.35	1	8	1.866 KB	9	1.620 KB
118.97.159.24	1	42	48.870 KB	22	1.511 KB
118.98.104.56	1	8	1.001 KB	14	1.897 KB
151.101.9.67	1	4	1.007 KB	5	803 B
23.0.171.96	1	15	3.020 KB	19	1.686 KB
216.58.221.66	1	58	33.953 KB	37	8.335 KB
203.190.124.25	1	24	8.393 KB	21	2.750 KB
104.93.116.35	1	1	66 B	3	593 B
104.93.87.225	1	1.494	1.109 MB	553	72.879 KB

Hasil dari Matrix (TOP100 IPv4 Conversatio) sama seperti IP conversation menunjukkan saat endpoint tersambung ke jaringan atau apa saat sedang terjadi traffic data dilihat dari bagian Summary seperti di bawah ini muncul kode – kode mesin yang sulit dipahami namun ada pula kode – kode yang masih bisa dibaca dan menunjukkan suatu kegiatan yang sedang terjadi saat itu.



### 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.