

Membandingkan Traffic IP conversation dan Matrix

Tugas 2



Disusun oleh :

Nama : Nanda Defiani

Nim : 09031181520118

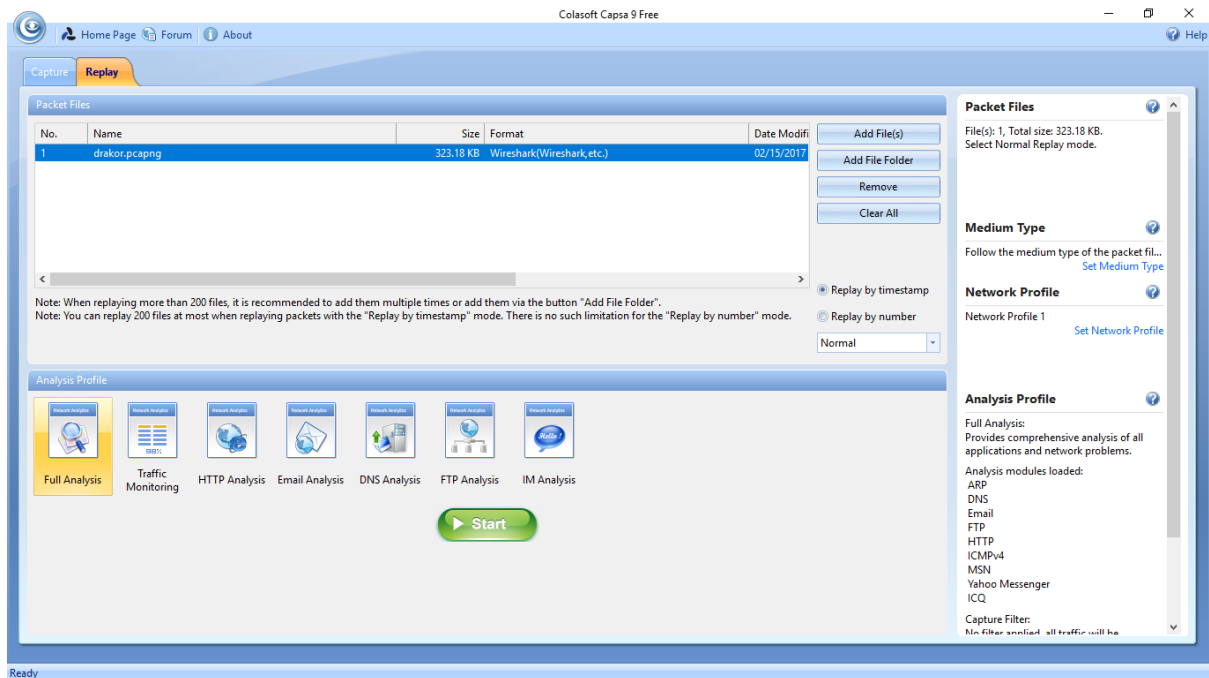
Mata Kuliah : Komunikasi Data Jaringan
komputer

Dosen : Deris Setiawan, M.T. Ph.d.

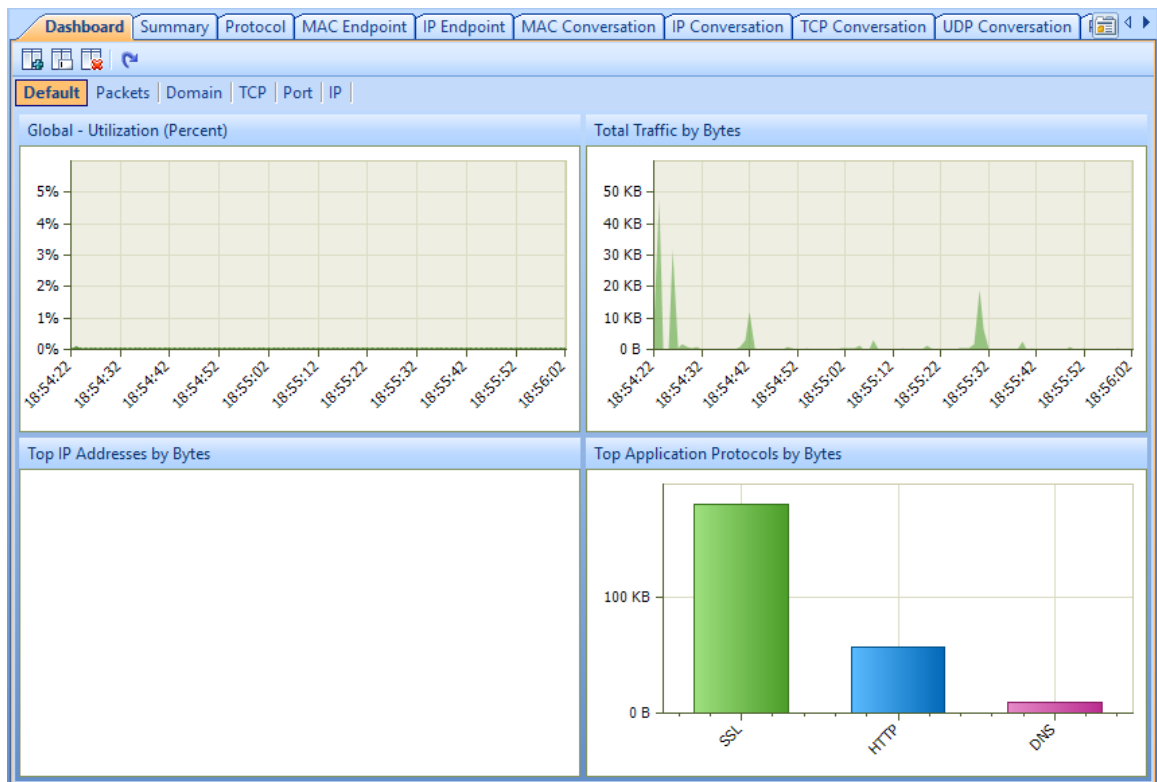
**SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

2017

Tampilan awal saat memasukkan file dari wireshark :



Setelah memasukan file yang telah disimpan melalui WireShark sebelumnya di dapat data seperti dashboard yang menunjukkan grafik dari server drakorindo.com seperti di bawah ini



IP Conversation

Tab IP conversation sangat berguna untuk banyak insinyur. Hal ini memungkinkan pelacakan percakapan antara endpoint pada jaringan Anda, dengan asumsi semua traffic melewati workstation dimana Capsa Jaringan Analyser diinstal.

The screenshot displays two panels from the Capsa Jaringan Analyser interface. The top panel is the 'IP Conversation' tab, showing a list of network conversations between nodes. The bottom panel is the 'TCP Conversation' tab, showing details for specific TCP connections.

Node 1 ->	<- Node 2	Duration	Bytes	Bytes ->	<- Bytes	Packets
192.168.43.99	e.dtscout.com	00:00:06.342779	4.64 KB	1.18 KB	3.47 KB	25
192.168.43.99	t.dtscdn.com	00:00:06.353301	2.27 KB	1.14 KB	1.13 KB	20
192.168.43.99	hypertracker.com	00:00:05.655867	535.00 B	228.00 B	307.00 B	6
192.168.43.99	drakorindo.com	00:00:26.096033	27.41 KB	2.69 KB	24.72 KB	58
192.168.43.99	tags.bluekai.com	00:00:21.079139	1.94 KB	1.10 KB	861.00 B	15
192.168.43.99	192.0.73.2	00:00:06.101065	696.00 B	456.00 B	240.00 B	12
192.168.43.99	192.0.77.32	00:00:30.252200	582.00 B	582.00 B	0.00 B	9
192.168.43.99	192.168.43.1	00:01:02.486851	9.64 KB	3.63 KB	6.01 KB	81
192.168.43.99	shield-normandy-el...	00:01:03.650638	28.55 KB	6.49 KB	22.06 KB	128
192.168.43.99	pipeline-tee-n-elb-1...	00:00:09.318732	582.00 B	582.00 B	0.00 B	9
192.168.43.99	sb.l.google.com	00:00:59.183272	19.89 KB	3.80 KB	16.09 KB	67
192.168.43.99	photos-ugc.l.google...	00:00:59.217630	22.04 KB	4.40 KB	17.64 KB	84

Node 1 ->	Port 1 ->	<- Node 2	<- Port 2	Packets	Bytes	Protocol
192.168.43.99	49964	drakorindo.com	80	6	348.00 B	TCP
192.168.43.99	49961	drakorindo.com	80	6	348.00 B	TCP
192.168.43.99	49963	drakorindo.com	80	7	402.00 B	TCP
192.168.43.99	49962	drakorindo.com	80	39	26.33 KB	HTTP

Setelah membuka tab IP conversation kemudian kita akan mencari dimana 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 .

The screenshot shows the 'Packet Decoding' window in Capsa Jaringan Analyser. It displays the raw packet data in hexadecimal and ASCII, along with the decoded content of the HTTP request. The decoded content shows a GET request for a specific resource on the drakorindo.com website.

```

0000003E 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 64 72 61 6B 6F 72 69 6E 64 6F 2E 63 6F 6D 0D 0A 55
0000003D 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73
0000007C 20 4E 54 20 31 30 2E 30 3B 20 57 4F 57 36 34 3B 20 72 76 3A 35 31 2E 30 29 20 47 65 63 6B 6F
0000009B 2F 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6F 78 2F 35 31 2E 30 0D 0A 41 63 63 65 70 74 3A
000000BA 20 74 65 78 74 2F 68 74 6D 6C 2C 61 70 70 6D 69 63 61 74 39 6F 6E 2F 78 68 74 6D 6C 2B 78 6D
000000D9 6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 6D 6C 3B 71 3D 30 2E 39 2C 2A 2F 2A 3B 71 3D 30
000000F8 2E 38 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 69 64 2C 65 6E 2D 55 53 3D 71
00000117 3D 30 2E 37 2C 65 6E 3B 71 3D 30 2E 33 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A
00000136 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D 0A 43 6F 6F 6B 69 65 3A 20 5F 5F 63 66 64 75 69
00000155 64 3D 64 39 38 65 36 61 62 32 64 36 62 63 65 31 62 32 36 37 35 32 36 37 35 39 64 34 64 33
00000174 32 32 35 65 31 34 39 30 32 33 33 33 34 34 3B 20 48 73 74 43 66 61 32 38 32 37 37 39 36 3D 31
00000193 34 38 30 32 33 33 33 35 32 30 35 37 3B 20 48 73 74 43 6C 61 32 38 32 37 37 39 36 3D 31 34 38
    
```

Decoded Content:

```

HTTP/1.1..Host: drakorindo.com..User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0..Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Accept-Language: id,en-US;q=0.7,en;q=0.3..Accept-Encoding: gzip, deflate..Cookie: _cfduid=d90e6ab2d6bce1b2675266759d4d3225e1480239344; HstCfa2827796=1480239352057; HstCfa2827796=1480239352057; HstCfa2827796=1480239352057
    
```

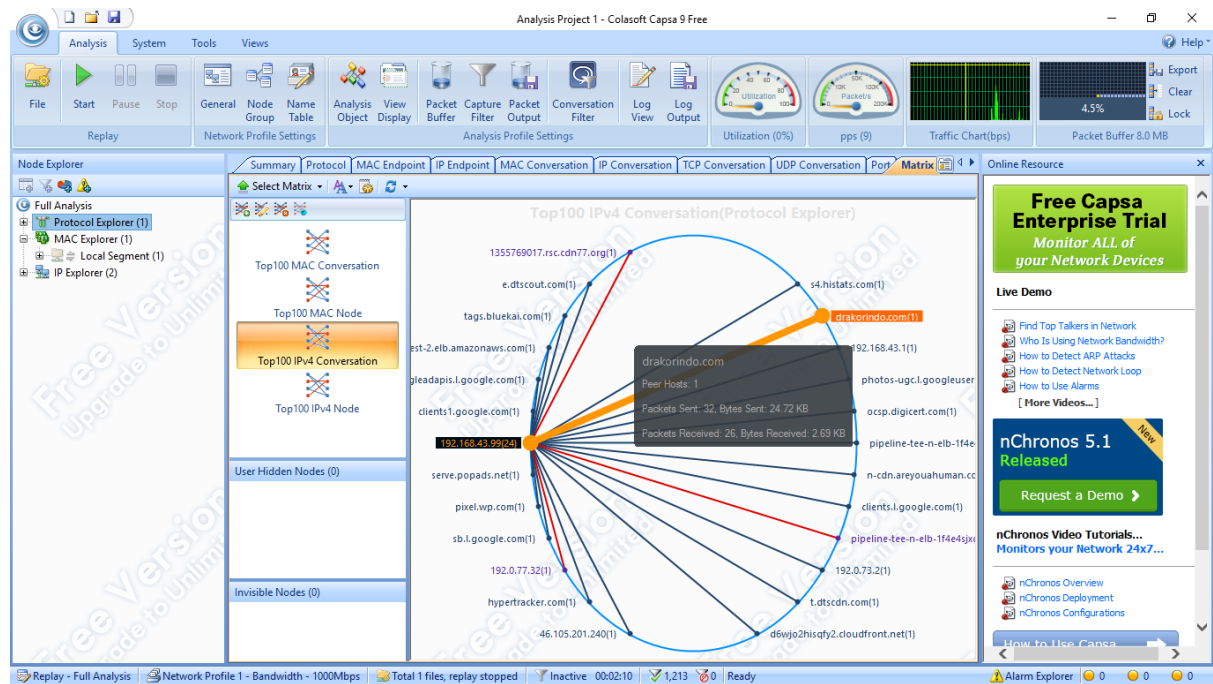
Terdapat perintah GET yang menunjukkan bahwa jaringan mulai terkoneksi atau memanggil server endpoint pada Drakorindo.com

```

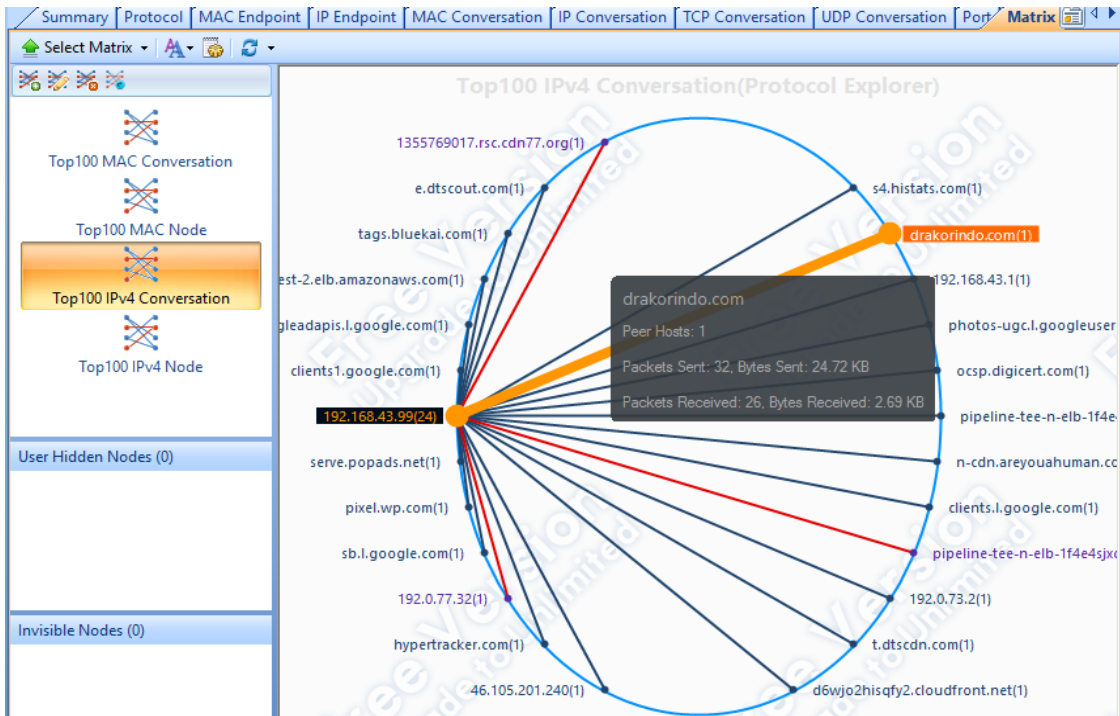
--0 End of data:          .... ...0 [47/1] 0x01
Window:                 64 [48/2]
Checksum:               0x6672 (Correct) [50/2]
Urgent point:          0 [52/2]
No TCP Option          [54/0]
HTTP - Hypertext Transfer Protocol
[54/631]
HTTP Request:          GET / HTTP/1.1
Host:                  drakorindo.com
User-Agent:            Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept:                text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:       id,en-US;q=0.7,en;q=0.3
Accept-Encoding:       gzip, deflate
Cookie:                __cfduid=d98e6ab2d6bce1b2675266759d4d3225e1480239344; HstCfa2827796=1480239352057; HstCla2827796=1487159486226; HstCmu2827796=148715948622
Connection:            keep-alive
Upgrade-Insecure-Requests: 1

000 7C 0B C6 19 B6 58 C0 38 96 01 A9 08 00 45 00 02 9F 2B E2 40 00 80 06 CA 37 C0 A8 2B 63 68 1B AE 78 C3 2A 00 50 51 56 AF CF DF A6 |.....X8.....E...+.8....7...+ch..x.*.PQV....
021 FF 50 18 00 40 66 72 00 00 47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 64 72 61 6B 6F 72 69 6E 64 6F 2E 63 6F 6D |.P..&fr..GET / HTTP/1.1..Host: drakorindo.com
05A 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 31 30 2E 30 3B 20 57 |..User-Agent: Mozilla/5.0 (Windows NT 10.0; W
087 4F 57 36 34 3B 20 72 76 3A 35 31 2E 30 29 20 47 65 63 6B 6F 2F 32 30 31 30 31 30 31 20 46 69 72 65 66 6F 78 2F 35 31 2E 30 0D 0A 41 |OW64; rv:51.0) Gecko/20100101 Firefox/51.0..A
0B4 63 65 70 74 3A 20 74 65 78 74 2F 68 74 6D 6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C 2C 61 70 70 6C 69 63 |ccept: text/html,application/xhtml+xml,applic
0E1 61 74 69 6F 6E 2F 78 6D 6C 3B 71 3D 30 2E 39 2C 2A 2F 2A 3B 71 3D 30 2E 38 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 69 |action/xml;q=0.9,*/*;q=0.8..Accept-Language: i
10E 64 2C 65 6E 2D 55 53 3B 71 3D 30 2E 37 2C 65 6E 3B 71 3D 30 2E 33 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 |d,en-US;q=0.7,en;q=0.3..Accept-Encoding: gzip
13B 2C 20 64 65 66 6C 61 74 65 0D 0A 43 6F 6F 6B 69 65 3A 20 5F 5F 63 66 64 75 69 64 3D 64 39 38 65 36 61 62 32 64 36 62 63 65 31 62 32 36 |,deflate..Cookie: __cfduid=d98e6ab2d6bce1b26
168 37 35 32 36 36 37 35 39 64 34 64 33 32 35 65 31 34 38 30 32 33 39 33 34 3A 3B 20 48 73 74 43 66 61 32 38 32 37 37 39 36 3D 31 34 38 |75266759d4d3225e1480239344; HstCfa2827796=148
195 30 32 33 39 33 35 32 30 35 37 3B 20 48 73 74 43 6C 61 32 38 32 37 37 39 36 3D 31 34 38 37 31 35 39 34 38 36 32 32 36 3B 20 48 73 74 43 |0239352057; HstCla2827796=1487159486226; HstC
1C2 6D 75 32 38 32 37 37 39 36 3D 31 34 38 37 31 35 39 34 38 36 32 32 36 3B 20 48 73 74 50 6E 32 38 32 37 37 39 36 3D 31 3B 20 48 73 74 50 |mu2827796=1487159486226; HstPz2827796=1; HstP
1EF 74 32 38 32 37 37 39 36 3D 31 3B 20 48 73 74 43 6E 76 32 38 32 37 37 39 36 3D 31 3B 20 48 73 74 43 6E 73 32 38 32 37 37 39 36 3D 31 3B |c2827796=1; HstCm2827796=1; HstCm2827796=1;
21C 20 63 5F 72 65 66 5F 32 38 32 37 37 39 36 3D 6E 74 74 70 73 25 33 41 25 32 46 25 32 46 77 77 77 2E 67 6E 6F 67 6C 65 2E 63 6F 6D 25 32 |c_ref_2827796=https://www.google.com/
249 46 3B 20 5F 67 61 3D 47 41 31 2E 32 2E 32 30 33 30 32 38 38 35 37 30 2E 31 34 38 30 32 33 39 33 35 34 3B 20 5F 67 61 74 3D 31 0D 0A 43 |F_ga=GAL.2.203028570.1480239354; gat=1..C
276 6F 6E 6E 63 74 69 6E 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65 0D 0A 55 70 67 72 61 64 65 6E 2D 49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 |onnection: keep-alive..Upgrade-Insecure-Req
2A3 73 74 73 3A 20 31 0D 0A 0A 0A |sts: 1....
  
```

Matrix



Tab Matrix visualisasi menunjukkan semua koneksi jaringan dan rincian Traffic dalam satu grafik tunggal. Berat dari garis antara node menunjukkan volume lalu lintas dan warna menunjukkan status. Ketika kursor dipindahkan pada node tertentu, rincian Traffic jaringan dari node akan disediakan seperti gambar di bawah ini .



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 .

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
117	18:54:16.444560	192.168.43.99:49961	drakorindo.com:80	TCP	66		[SYN] Se
118	18:54:16.444814	192.168.43.99:49962	drakorindo.com:80	TCP	66		[SYN] Se
120	18:54:16.445026	192.168.43.99:49963	drakorindo.com:80	TCP	66		[SYN] Se
121	18:54:16.445321	192.168.43.99:49964	drakorindo.com:80	TCP	66		[SYN] Se
133	18:54:19.073950	drakorindo.com:80	192.168.43.99:49962	TCP	66		[SYN, AC
134	18:54:19.074163	192.168.43.99:49962	drakorindo.com:80	TCP	54		[ACK] Se
135	18:54:19.074360	drakorindo.com:80	192.168.43.99:49961	TCP	66		[SYN, AC
136	18:54:19.074516	192.168.43.99:49961	drakorindo.com:80	TCP	54		[ACK] Se
137	18:54:19.074825	192.168.43.99:49962	drakorindo.com:80	HTTP_GET	685		C: GET /
138	18:54:19.078868	drakorindo.com:80	192.168.43.99:49963	TCP	66		[SYN, AC
139	18:54:19.079122	192.168.43.99:49963	drakorindo.com:80	TCP	54		[ACK] Se

Packet Info:		Hex	ASCII
Number:	137	00000027	56 AF CF CF DF A6 FF 50 18 00 40 66 72
Packet Length:	685	00000034	00 00 47 45 54 20 2F 20 48 54 50 2F
Capture Length:	685	00000041	31 2E 31 0D 0A 48 6F 73 74 3A 20 64 72
Timestamp:	2017/02/15 18:5	0000004E	61 6B 6F 72 69 6E 64 6F 2E 63 6F 6D 0D
Ethernet Type II	[0/14]	0000005B	0A 55 73 65 72 2D 41 67 65 6E 74 3A 20
Destination Address:	7C:0B:C6:19:B6:	00000068	4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28
Source Address:	C0:38:96:99:01:	00000075	57 69 6E 64 6F 77 73 20 4E 54 20 31 30
Protocol:	0x0800	00000082	2E 30 3B 20 57 4F 57 36 34 3B 20 72 76
IP - Internet Protocol	[14/20]	0000008F	3A 35 31 2E 30 29 20 47 65 63 6B 6F 2F
Version:	4	0000009C	32 30 31 30 30 31 30 31 20 46 69 72 65
		000000A9	66 6F 78 2F 35 31 2E 30 0D 0A 41 63 63
		000000B6	65 70 74 3A 20 74 65 78 74 2F 68 74 6D
		000000C3	6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E
			V.....P..@r ..GET / HTTP/ 1.1..Host: dr akorindo.com. .User-Agent: Mozilla/5.0 (Windows NT 10 .0; WOW64; rv :51.0) Gecko/ 20100101 Fire fox/51.0..Acc ept: text/htm l,application

Kesimpulan :

Pada dasarnya 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 dan lebih menyukai tampilan matrix namun tampilan IP conversation juga sangat familiar dan menampilkan detail – detail traffic data dengan rinci hal tersebut sangat membantu bagi para Insinyur untuk pekerjaannya.