Analisis hasil capture, Follow stream, dan Flow Graph Jaringan menggunakan aplikasi Wireshark dan VisualRoute



Disusun Oleh:

NAMA	: Robby Tri Putra
NIM	: 09011381621099
KELAS	: SK4B

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER PRODI SISTEM KOMPUTER 2018

BAGIAN ANALISIS PERTAMA "ANALISIS PAKET DATA".

Dalam melakukan pengecekkan analisis data jaringan, Langkah pertama ialah harus mengetahui beberapa ip address yang sedang kita pakai.

	C:\Windows\system	32\cmd.exe	-	×	
Microsoft Windows [Vers (c) 2013 Microsoft Corp	ion 6.3.9600] oration. All rights re	eserved.			^
C:\Users\ACER>arp -a					
Interface: 10.0.44.208 Internet Address 10.0.44.1 10.0.44.255 224.0.0.22 224.0.0.252 239.255.255.250 255.255.255.255	0x4 Physical Address 00-0b-86-b7-ab-0f ff-ff-ff-ff-ff-ff 01-00-5e-00-00-16 01-00-5e-00-00-fc 01-00-5e-7f-ff-fa ff-ff-ff-ff-ff-ff-ff	Type dynamic static static static static static static			
Interface: 192.168.56.1 Internet Address 192.168.56.255 224.0.0.22 224.0.0.252 239.255.255.250 255.255.255.255 C:\Users\ACER>_	0x1d Physical Address ff-ff-ff-ff-ff-ff 01-00-5e-00-00-16 01-00-5e-00-00-fc 01-00-5e-7f-ff-fa ff-ff-ff-ff-ff-ff	Type static static static static static static			~

Buka cmd lalu ketikan perntah "arp –a", maka secara otomatis ip address kita akan muncul seperti pada gambar diatas.

Setelah itu, langkah selanjutnya adalah membuka aplikas **WIRESHARK**. Disini tersambung dengan jaringan Unsri.net

6					*Wi-Fi 2	- 0	×
File Edi	it View Go	Capture Analyze Statist	tics Telephony Wireles	Tools H	Help		
	(() () () () () () () () () () () () ()	X C Q 👄 👄 🖼 🤇	🗿 🌡 🗮 📕 🔍 Q	Q. 11			
in erc-	-13 229 161 234		<u> </u>	•		Evoression	+
	-13.225.101.254						
No.	Time	Source	Destination	Protocol	Length Info		^
13	8 8.505288	13.229.161.234	10.0.44.208	TCP	66 443 → 56027 [ACK] Seq=1 Ack=2 Win=114 Len=0 SLE=1 SRE=2		
40	9 10.002372	13.229.161.234	10.0.44.208	TCP	56 443 → 56027 [ACK] Seq=1 Ack=33 Win=114 Len=0		
410	0 10.002373	13.229.161.234	10.0.44.208	TCP	56 443 → 56027 [FIN, ACK] Seq=1 Ack=33 Win=114 Len=0		
- 52	5 10.008718	13.229.161.234	10.0.44.208	TCP	56 443 → 56027 [ACK] Seq=2 Ack=34 Win=114 Len=0		
132	5 23.698242	13.229.161.234	10.0.44.208	TCP	66 80 → 56109 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1386 SACK_PERM=1 WS=256		
132	6 23.698243	13.229.161.234	10.0.44.208	TCP	66 80 → 56110 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1386 SACK_PERM=1 WS=256		
132	8 23.698246	13.229.161.234	10.0.44.208	TCP	66 80 → 56111 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1386 SACK_PERM=1 WS=256		
1374	4 23.967876	13.229.161.234	10.0.44.208	TCP	56 80 → 56109 [ACK] Seq=1 Ack=381 Win=28160 Len=0		
137	5 23.967877	13.229.161.234	10.0.44.208	TCP	1440 80 → 56109 [ACK] Seq=1 Ack=381 Win=28160 Len=1386 [TCP segment of a reassembled PDU]		
137	6 23.967879	13.229.161.234	10.0.44.208	TCP	1440 80 → 56109 [ACK] Seq=1387 Ack=381 Win=28160 Len=1386 [TCP segment of a reassembled PDU]		
137	7 23.967880	13.229.161.234	10.0.44.208	TCP	1440 80 → 56109 [ACK] Seq=2773 Ack=381 Win=28160 Len=1386 [TCP segment of a reassembled PDU]		
137	8 23.967883	13.229.161.234	10.0.44.208	TCP	1440 80 → 56109 [ACK] Seq=4159 Ack=381 Win=28160 Len=1386 [TCP segment of a reassembled PDU]		
1379	9 23.967884	13.229.161.234	10.0.44.208	TCP	1440 80 → 56109 [ACK] Seq=5545 Ack=381 Win=28160 Len=1386 [TCP segment of a reassembled PDU]		
138	0 23.967885	13.229.161.234	10.0.44.208	TCP	1440 80 → 56109 [ACK] Seq=6931 Ack=381 Win=28160 Len=1386 [TCP segment of a reassembled PDU]		
138	1 23.967887	13.229.161.234	10.0.44.208	TCP	1440 80 → 56109 [ACK] Seq=8317 Ack=381 Win=28160 Len=1386 [TCP segment of a reassembled PDU]		
138	2 23.967888	13.229.161.234	10.0.44.208	тср	1440 80 → 56109 [ACK] Seq=9703 Ack=381 Win=28160 Len=1386 [TCP segment of a reassembled PDU]		Ŷ
Frame	: 525: 56 byte	s on wire (448 bits),	, 56 bytes captured (448 bits)	on interface 0		
Ether	met II, Src:	Routerbo_fd:28:1d (6c	::3b:6b:fd:28:1d), Ds	t: Azurewa	v_67:f0:3f (28:c2:dd:67:f0:3f)		
Inter	net Protocol	Version 4, Src: 13.22	29.161.234, Dst: 10.0	.44.208			
Trans	mission Contr	ol Protocol, Src Port	:: 443, Dst Port: 560	27, Seq: 2	, Ack: 34, Len: 0		
VSS-M	Nonitoring eth	ernet trailer, Source	Port: 0				
0000 2	8 c2 dd 67 f0	3f 6c 3b 6b fd 28 1	d 08 00 45 00 (g	.?1: k.(.E.		
0010 0	0 28 40 0b 40	00 f2 06 62 25 0d e	5 al ea 0a 00 .(@.	д b%			
0020 2	c d0 01 bb da	db ff 50 19 69 5d 9	1 91 48 50 10 ,	P .i]	HP.		
0030 0	0 72 e4 98 00	00 00 00	.r				
0 7	wireshark_D05580	096-ECD2-4D72-A7DD-ACB087	68AB87_20180222101717_a0	5712	Packets: 12420 · Displayed: 123 (1.0%)	Profile:	Default
	7. =	- 📣 🦱				10:35	AM
						🖬 🕪 👩 📶 2/22/	2018

Dari gambar sebelumnya kita telah mendapaktan beberapa data dalam bentuk paket data jaringan. Karena semua paket data tersaring dengan cepat maka kita menggunakan filter terlebih dahulu menggunakan **"ip.src==10.0.44.208"**.

٨						*Wi-Fi 2	- 🗇 🗙
File	e Edit	t View Go	Capture Analyze	Statistics Telephony Wire	less Tools H	ielp	
			R C 9 0	ې 🖻 👳 🕁 🚍 🔍 (a, e, 🎹		
	ip.src=+	=10.0.44.208					Expression +
No.	^	Time	Source	Destination	Protocol	Length Info	^
	1222	21.167123	10.0.44.208	10.0.44.255	NBNS	92 Name query NB RBYKSXO<00>	
	1223	21.354627	10.0.44.208	74.125.24.94	QUIC	188 Payload (Encrypted), PKN: 76, CID: 14486123532944794968	
	1227	21.921248	10.0.44.208	10.0.44.255	NBNS	92 Name query NB RBYKSXO<00>	
	1228	21.921464	10.0.44.208	10.0.44.255	NBNS	92 Name query NB VKYJUVSR<00>	
	1229	21.921583	10.0.44.208	10.0.44.255	NBNS	92 Name query NB SVRPRXADFQELWQA<00>	
	1230	22.047500	10.0.44.208	74.125.24.94	QUIC	81 Payload (Encrypted), PKN: 77, CID: 14486123532944794968	
	1231	22.061816	10.0.44.208	8.8.8.8	DNS	72 Standard query 0x04cc A www.bola.com	
	1240	22.087836	10.0.44.208	74.125.24.94	QUIC	86 Payload (Encrypted), PKN: 78, CID: 14486123532944794968	
	1241	22.088028	10.0.44.208	74.125.24.94	QUIC	83 Payload (Encrypted), PKN: 79, CID: 14486123532944794968	
	1242	22.088096	10.0.44.208	74.125.24.94	QUIC	80 Payload (Encrypted), PKN: 80, CID: 14486123532944794968	
	1243	22.251459	10.0.44.208	103.241.4.2	DNS	72 Standard query 0X04cc A WWW.bola.com	
	1244	22.40005	10.0.44.208	10.0.44.255	NBNS	92 Name query NB WPAD/00>	
	1240	22.4000009	10.0.44.200	224.0.0.252	LLMND	64 Standard query 6x1504 A wood	
	1240	22.010/10	10.0.44.208	224.0.0.232	DNC	77 Standard guery Oxide A fasts estatis can	
	1249	22.90/050	10.0.44.200	0.0.0.0	DNS	75 Standard query 6x8366 A Tonts.gstatt.com	×.
	-	4024 . 22 1	10.0.441200				
P	rrame	1231: /2 D	ytes on wire (5/	b bits), /2 bytes capture	a (5/6 Dits)	on interface 0	
	Tetor	net II, Src	: Azurewav_07:10	. 10 0 44 200 Det. 9 9	o st: Koutero	0_10:20:10 (0C:50:00:10:20:10)	
	Linceri Ucon I	Datagram Dr	otocol Snc Port	57622 Drt Port: 53	.0		
	Domain	o Nomo Svet	ococor, she pont	: 57622, DSC POPC: 55			
	DOIIIGTI	n Name Syst	em (query)				
00	00 6 0	c 3b 6b fd	28 1d 28 c2 dd (57 f0 3f 08 00 45 00 1;	k.(.(g.?.	.E.	
00	10 00	0 3a 6d 1d	00 00 80 11 86 1	o6 0a 00 2c d0 08 08 .:	m,		
00	20 08	8 08 e1 16	00 35 00 26 b1	77 04 cc 01 00 00 01	5.& .w		
00	10 63	0 00 00 00 3 6f 6d 00	00 00 03 77 77	// 04 62 6T 6C 61 03	W WW.DO	13.	
00	+0 01	5 61 60 66	00 01 00 01	20			
0	7	wireshark_D05	58D96-ECD2-4D72-A7D0	-ACB08768AB87_20180222101717	_a05712	Packets: 12382 * Displayed: 4469 (36.1%)	Profile: Default
		7	- 1				10-35 AM
			= 🙂	V 🖳 🛏			▲ 🛛 🕪 😽 📶 2/22/2018

Dapat dilihat bahwa dengan computer yang beralamatkan ip 10.0.44.208 yang sedang mencoba mengakses website <u>www.bola.com</u> atau beralamtkan ip 13.229.161.234 dengan menggunakan TCP protocol. Setelah itu jika kita mengklik bagian kotak tengah di menu Internet Protocol Version 4, maka akan menampilkan jika computer sedang mengakses web tersebut.

4				*Wi-Fi 2		- 🗇 🗙		
File Edit View Go	Capture Analyze Statist	tics Telephony Wireless	Tools Hel	0				
1 🗖 🧖 🕥 🗋 🖻	ਲ਼ © ९ ↔ ↔	👔 il 📃 📃 🔍 Q 🖉	Q III					
ip.src==10.0.44.208						Expression +		
No. Time	Source	Destination	Protocol L	enoth Info		^		
721 13,542890	10.0.44.208	8.8.8.8	DNS	75 Standard query 0x2691 A www.gstatic.com				
746 14.401011	10.0.44.208	8.8.8.8	DNS	76 Standard query 0x254b A mtalk.google.com				
749 14.586055	10.0.44.208	103.241.4.2	DNS	76 Standard query 0x254b A mtalk.google.com				
						•		
Frame 1243: 72 by A Ethernet TT See	tes on wire (5/6 bits)), 72 bytes captured (5	/6 DITS) O	1 INTERTACE 0				
Destination: R	Azurewav_67:10:51 (20 outerbo_fd:28:1d (6c:3	b:6b:fd:28:1d)	Koucerbo_	u:28:10 (6C:50:60:10:28:10)				
Source: Azurew	av 67:f0:3f (28:c2:dd:	67:f0:3f)						
Type: IPv4 (0x	0800)							
4 Internet Protocol	Version 4, Src: 10.0.	44.208, Dst: 103.241.4	.2					
0100 = Ve	rsion: 4							
0101 = He	ader Length: 20 bytes	(5)						
Differentiated	Services Field: 0x00	(DSCP: CS0, ECN: Not-E	CT)					
Total Length:	58							
Identification	: 0x357b (13691)							
Flags: 0x00								
Fragment offse	t: 0							
Time to live:	128							
Protocol: UDP	(17)							
Header checksu	m: 0x6275 [validation	disabled]						
[Header checks	um status: Unverified]							
Source: 10.0.4	4.208							
Destination: 1	03.241.4.2							
[Source GeoIP:	Unknown							
User Determine Determine	eoir: Unknownj	Dat Daats 52						
Domain Name Syste	m (query)	, DSC POPC: 55						
> Domain Name Syste	in (query)							
0000 6c 3b 6b fd 2	8 1d 28 c2 dd 67 f0 3	f 08 00 45 00 1:k.(.	(g.?F					
0010 00 3a 35 7b 0	0 00 80 11 62 75 0a 0	0 2c d0 67 f1 .:5{	bug					
0020 04 02 e1 16 0	0020 04 02 e1 16 00 35 00 26 55 94 04 cc 01 00 00 015.& U							
0030 00 00 00 00 0	0030 00 00 00 00 00 00 03 77 77 77 04 62 6f 6c 61 03w ww.bola.							
0040 63 6† 6d 00 0	0 01 00 01	com	••					
🔵 🍸 Frame (frame), :	2 bytes				Packets: 13004 · Displayed: 4617 (35.5%)	Profile: Default		
7 1	= 🚯 👩		1			 Image: Image: Ima		
💒 🐚						2/22/2018		

BAGIAN KEDUA "DENGAN MENGGUNAKAN MENU FOLLOW STREAM"

6					*Wi-Fi 2	- 🗗 🗙		
F	ile Edit View G	o Capture Analyze Sta	atistics Telephony Wireless	Tools	Help			
4	(🔳 🖉 🛞 📗	🛅 🔀 🖸 I 🍳 👄 🖻	i T 🛓 🗐 Q Q	Q. 👖				
I.	tcp.stream eq 238					Expression +		
No	. Time	Source	Destination	Protocol	Length Info			
-++	11099 943.18453	3 10.0.44.208	52.77.231.227	HTTP	1162 GET /soccer-standings-sidebar/bola HTTP/1.1			
*	11139 943.30214	6 52.77.231.227	10.0.44.208	HTTP	1074 HTTP/1.1 200 OK (text/html)			
L C	11059 943.15037	0 10.0.44.208	52.77.231.227	TCP	66 56264 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1			
	11088 943.18096	0 52.77.231.227	10.0.44.208	TCP	66 80 → 56264 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1386 SACK_PERM=1 WS=1024			
	11096 943.18170	5 10.0.44.208	52.77.231.227	TCP	54 56264 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0			
	11125 943.23966	0 52.77.231.227	10.0.44.208	TCP	56 80 → 56264 [ACK] Seq=1 Ack=1109 Win=29696 Len=0			
	11136 943.29460	5 52.77.231.227	10.0.44.208	TCP	1440 80 \rightarrow 56264 [ACK] Seq=1 Ack=1109 Win=29696 Len=1386 [TCP segment of a reassembled PDU]			
	11137 943.29476	0 10.0.44.208	52.77.231.227	TCP	54 56264 → 80 [ACK] Seq=1109 Ack=1387 Win=66304 Len=0			
	11138 943.30214	5 52.77.231.227	10.0.44.208	TCP	1440 80 → 56264 [ACK] Seq=1387 Ack=1109 Win=29696 Len=1386 [TCP segment of a reassembled PDU]			
	11142 943.30239	8 10.0.44.208	52.77.231.227	TCP	54 56264 → 80 [ACK] Seq=1109 Ack=3793 Win=66304 Len=0			
	12030 988.31431	2 10.0.44.208						
	12039 988.70141	3 52.77.231.227	10.0.44.208	TCP	66 [TCP Keep-Alive ACK] 80 → 56264 [ACK] Seq=3793 Ack=1109 Win=29696 Len=0 SLE=1108 SRE=110	9		
	12204 1033.3739	53 52.77.231.227	10.0.44.208	TCP	56 80 → 56264 [FIN, ACK] Seq=3793 Ack=1109 Win=29696 Len=0			
	12205 1033.3740	61 10.0.44.208	52.77.231.227	TCP	54 [TCP Dup ACK 11142#1] 56264 → 80 [ACK] Seq=1109 Ack=3793 Win=66304 Len=0			
	12206 1033.3742	77 10.0.44.208	52.77.231.227	TCP	54 56264 → 80 [ACK] Seq=1109 Ack=3794 Win=66304 Len=0			
	12334 1078.3846	50 10.0.44.208	52.77.231.227		55 [TCP Keep-Alive] 56264 → 80 [ACK] Seq=1108 Ack=3794 Win=66304 Len=1			
-	12335 1078.4131	82 52.77.231.227	10.0.44.208	TCP	56 80 → 56264 [RST] Seq=3794 Win=0 Len=0			
	Erame 11000: 1162 hutes on wire (0206 hits) 1162 hutes cantured (0206 hits) on interface 0							
4	Ethernet II. Sr	: Azureway 67:f0:3f	(28:c2:dd:67:f0:3f). Dst	: Router	b fd:28:1d (6c:3b:6b:fd:28:1d)			
	Destination:	Routerbo fd:28:1d (6	:3b:6b:fd:28:1d)					
	Source: Azur	way 67:f0:3f (28:c2:0	d:67:f0:3f)					
	Type: TPv4 (3×0800)	,					
4	Internet Protoc	ol Version 4. Src: 10	.0.44.208. Dst: 52.77.23	1.227				
	0100 =	/ersion: 4	,,					
	0101 =	Header Length: 20 byte	es (5)					
	Differentiat	ed Services Field: 0x0	00 (DSCP: CS0, ECN: Not-	ECT)				
	Total Length	1148		· ·				
	Identificati	on: 0x6641 (26177)						
	Flags: 0x02	(Don't Fragment)				*		
0	000 6c 3b 6b fd	28 1d 28 c2 dd 67 f6	a 3f 08 00 45 00 1:k.(.(- F	^		
0	010 04 7c 66 41	40 00 80 06 3d 3a 0a	a 00 2c d0 34 4d . fA@		. 4M			
0	020 e7 e3 db c8	00 50 88 3d 3e 2a a	d d6 55 0f 50 18		J.P.			
0	030 01 03 e6 0b	00 00 47 45 54 20 21	f 73 6f 63 63 65		bcce			
0	040 72 2d 73 74	61 6e 64 69 6e 67 7	3 2d 73 69 64 65 r-sta	ndi ngs-	side	~		
(🔰 🍸 🛛 Frame (frame)	, 1162 bytes			Packets: 18359 · Displayed: 17 (0.1%)	Profile: Default		
F	- 7 ₆	📺 🚯 💽		<u>wi</u>		🔺 📋 🕪 📑 🏦 12:12 PM		
	2					2/22/2018		

Seperti gambar di atas, pilih paket ang memiliki bentuk protocol http, dan klik **analyze**=> pilih **follow** dan => untuk pertama pilih bagian **TCP Stream :**

4		- 1 ×
	A Wireshark - Follow TCP Stream (tcp.stream eq 82) - wireshark_D055BD96-ECD2-4D72-A7DD-ACB08/68AB87_2018022 – 😐 🗖	
File Edit View Go Capture Ar		
🔟 💻 🙋 🛞 🕼 🖾 🕱 🖾 🤇	GET / HTTP/1.1	
ten atraam as 92	Host: www.bola.com	Expraction 4
(m tcp.su ean eq oz	Connection: keep-allve	
No. Time Source	upgrade-insecure-Requests: 1 Hear-Agant: Morilla/5 & (Window: NT 6 3: Win64: v64) ApplaWakVit/537 36 (VHTML like Garko) Chrome/64 0 3282 167 Safari/	· · · · · · · · · · · · · · · · · · ·
3127 29.235759 13.229.1	Sar Agenet Holling S. 6 (windows windows	d PDU]
2013 28.278102 10.0.44.	Accept: text/html.application/xhtml+xml.application/xml:g=0.9.image/webp.image/appg.*/*:g=0.8	
2003 28.276340 13.229.1	Accept-Encoding: gzip, deflate	PDU]
1551 25.509011 10.0.44.	Accept-Language: en-US,en;q=0.9	
1520 25.268117 10.0.44.		
1519 25.267863 13.229.1	HTTP/1.1 200 0K	PDU]
1518 25.267862 13.229.1	Date: Thu, 22 Feb 2018 03:18:00 GMT	PDU]
1517 25.267860 13.229.1	Content-Type: text/html; charset=UTF-8	PDU]
1516 25.267857 13.229.1		PDU]
1515 25.267855 13.229.1	Server: nginy	PDU]
1514 25.267853 13.229.1	Vary: Accept-Encoding	PDU
1510 25.259916 10.0.44.	Cache-Control: no-cache, private	
1505 25.259648 13.229.1	Server-node: ip-10-0-207-206	PDU1
1504 25.259647 13.229.1	X-Hail-Hydra: Join the Darkside, we have cookies. Visit us at http://www.kmklabs.com/careers	PDUI
1503 25.259644 13.229.1	Content-Encoding: gzip	PDUI
1502 25.259642 13.229.1	X-Ttl: 300.000	PDU1
1501 25 259639 13 229 1	Age: 90	PDU1
	Vid: 1.1 varnish-v4	100]
Frame 1501: 1440 bytes on wi	X-Cache-Hits: 18	1
# Ethernet II, Src: Routerbo_f	Accept-Ranges: bytes	
Destination: Azurewav 67:		
Source: Routerbo_fd:28:1d	······	
Type: IPv4 (0x0800)	\$.aPTm/.@.D\$({&{k	
Internet Protocol Version 4,	3.F"vi.#.Zf/f".MC.jp!PPP%.kfG.1	
0100 = Version: 4		
0101 = Header Length		
Differentiated Services F	······································	
Total Length: 1426	<	
Identification: 0x675f (2	e.u/6`8fS0UK1.szzF065LG>m=<	
Flags: 0x02 (Don't Fragme	2QSpoGG.:wj.toCZxt.;P[3.].c.v.e.N*>0.FM,xaO.Q	
0000 28 c2 dd 67 f0 3f 6c 3h		
0010 05 92 67 5f 40 00 f2 06		
0020 2c d0 00 50 db 2d 15 0a	Entire conversation (111kB) Show and save data as ASCII Stream 82	
0030 00 6e fd d2 00 00 19 05	End	
0040 47 9f f5 a2 7a a1 7c 84		
🥚 🍸 Frame (frame), 1440 bytes	Filter Out This Stream Print Save as Back Close Help	Profile: Defaul
🔳 🥻 📜	🜔 🖉 🔤 🔟 🖉 👘 🖉	▲ 🗋 🕪 😼 📶 10:41 AM 2/22/2018

Bisa dilihat gambar di atas info apa saja yang dapat kit abaca yaitu :

- 1. Sang pengguna yang sedang mengakses website <u>www.bola.com</u> menggunakan aplikasi browser.
- 2. Waktu user mengakses web tersebut
- 3. Tipe data yang sedang diakses itu berupa text/html.

Untuk bagian keduanya kita gunakan kembali suatu pilihan yakni TCP Http :



BAGIAN KETIGA "dan Flow Graph jaringan menggunakan aplikas Wireshark dan visual route"

Kita mengklik menu statistics dan kita pilih flow graph maka data yang akan muncul akan seperti dibawah ini :



Lalu lintas berjalannya ekspedisi informasi dapat divisualisasikan menggunakan FlowGraph seperti gambar diatas. Berikut adalah penjelasan terhadap panah pada FlowGraph:

1. \rightarrow 1 – computer user mengirim informasi addres atau link ke router jaringan.

2. \rightarrow 2 – ketika router menerima informasi, maka ia akan mengkasihkan alamat data tersebut.

3. \rightarrow 3 – isp akan menanggapi permintaan user tersebut, apakah alamat yang dituju.

4. \rightarrow 4 – apabila alamat tersedia, maka isp akan mengarahkan informasi tersebut ke isp pusat

5. \rightarrow 5 – isp pusat pun akan menanggapi permintaan tersebut, dan informasi tanggapan akan dikirim kembali ke user.

6. \rightarrow 6 – ketika informasi tersebut tidak valid atau address tersebut tidak ditemukan, maka user diharuskan mengirim ulang informasi yang valid. Dimana data tersebut akan kembali diperiksa oleh isp terdekat.

7. \rightarrow 7 – jika informasi tersebut valid, isp akan kembali mengirimkan tanggapan dan mengarahkannya ke isp pusat.

8. \rightarrow 8 – apabila isp pusat menanggapi informasi tersebut valid, maka kita akan diarahkan ke server perusahaan yang memberi isp bandwidth. Yang mana disini kita akan di arahkan ke link server cloud berikutnya.

9. \rightarrow 9 – disini situs yang diakses adalah www.detik.com dengan mengambil berita International dan nasional

10. \rightarrow 10 – seperti pada isp tadi, server pun akan mengirimkan informasikepada user apakah address yang dituju tersebut valid atau tidak.

Di Bawah ini adalah tampilan dari aplikasi Visual Route :



Disini kita bias lihat sendiri perbedaan data yang diperoleh dari aplikasi wireshark dan aplikasi visualroute ini:

1. Pada aplikasi wireshark setiap lalu lintas perjalanan data dapat dilihat serta dianalis kemana dan apakah data tersebut memberi timbal balik kepada user, tentu saja dapat diambil satu point untuk

aplikasi ini yaitu sangat berguna bagi operator server atau server manager yang memiliki kemampuan expert dan para peneliti jaringan untuk mendapatkan data yang sangat mendetail, karena setiap hop terstruktur dengan rapi.Selain itu, aplikasi wireshark dapat memberikan fasilitas filter protocol sehingga dalam menganalis data lebih effective dan akurat.

2. Sedangkan pada aplikasi visualroute akan dibagi menjadi:

Kelemahan :

a. Kurang mendetailnya aliran data dari awal sesi hingga sampai ke destination atau tidak tersedianya fasilitas flow graph seperti wireshark.

b. Tidak adanya filter protocol.

c. Kurang mumpuni dalam mencapture data pada sebuah ip.

Kelebihan :

- a. Penggunaan yang mudah.
- b. Visualisasi tempat source dan destination terlihat jelas.
- c. Setiap hope ditampilkan semua dan panjang hopenya sudah ada di layar tampilan.