Analisis hasil Capture, Follow Stream, dan Flow Graph Jaringan menggunakan aplikasi Wireshark dan VisualRoute



Disusun Oleh:

- Nama : Vanissa Wanika Siburian
- NIM : 09011381722094

Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya 2017/2018 BAGIAN PERTAMA "Analisis Paket Data"

 Step pertama sebelum melakukan analisis paket data jaringan, kita terlebih dahulu berapa IP Address yang sedang kita pakai.

Recycle Bin	PowerPoint 2016	Colasoft Capsa _				
	w		Administrator: Command Prompt		– 🗆 🗙	
Google	Word 2016	VisualRoute	Microsoft Windows [Version 10.0.15063] (c) 2017 Microsoft Corporation. All rights	reserved.	^ {/////	
Chrome		2010	C:\Users\User>arp -a			
Proteus 8 Professional	Excel 2016	Revo Uninstall	Interface: 10.9.44,120 0x12 Internet Address Physical Address 10.9.44,1 10.9.44,254	Types dynamic dynamic static static static static static		
Camera	Microsoft Visual Studi	PhotoScape				
CodeBlocks	Corel PHOTO-PAL					
Firefox	CorelDRAW X8 (64-Bit)					
GOM Player	Winamp					
Canon My Printer	R Wireshark					
م 🖿	0 0	🖿 🖻 O 🔮 🚏	🖻 🔕 💽 📶			へ 📾 🦟 🕸 9:07 AM 📮

Cara mengetahui IP Address kita buka cmd lalu ketikan perintah "<u>arp –a</u>", maka secara otomatis IP Address yang kita pakai akan muncul seperti gambar diatas.

✓ Setelah itu, langkah selanjutnya kita membuka aplikasi WireShark. Disini saya tersambung dengan Wi-Fi Unsri.Net.

e Edit View Go	o Capture Analyze Statistics					-
I 🖉 💿 📘		Telephony Wireless To	ols Help			
	🖹 🖹 🗳 🗣 🗣 🚺	👲 📃 📄 Q Q Q 👔	1			
oly a display filter	. < Ctrl-/>					Expressi
Time	Source	Destination	Protocol	Length Info		
6 0.03117	5 10.0.44.120	216.58.201.138	TCP	66 14430 → 80 [ACK] Seg=1 Ack=1 Win=258 Len=0 SLE=0 SRE=1		
7 0.15049	3 10.0.44.120	216.58.201.142	TCP	55 14383 → 80 [ACK] Seg=1 Ack=1 Win=255 Len=1		
8 0.44653	5 10.0.44.120	104.25.235.4	TCP	66 14431 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1		
9 0.45289	5 10.0.44.120	144.217.74.230	HTTP	450 GET /img/px.png?i=300&ts=1519264065245≥=ID&sa=59001&pid=75041&st=gr&do=www.kompas.com&bi=1&cha=993&di=7.28_0.98	pr=%2C%	20%20
10 0.45651	7 10.0.44.120	93.184.220.29	TCP	55 14388 → 80 [ACK] Seq=1 Ack=1 Win=256 Len=1		
11 0.46356	6 104.25.235.4	10.0.44.120	TCP	66 80 → 14431 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=1024		
12 0.46367	8 10.0.44.120	104.25.235.4	TCP	54 14431 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0		
13 0.46745	2 216.58.201.142	10.0.44.120	TCP	66 80 → 14383 [ACK] Seq=1 Ack=2 Win=172 Len=0 SLE=1 SRE=2		
14 0.72163	4 93.184.220.29	10.0.44.120	TCP	66 80 → 14388 [ACK] Seq=1 Ack=2 Win=288 Len=0 SLE=1 SRE=2		
15 0.73670	8 144.217.74.230	10.0.44.120	TCP	56 80 → 14171 [ACK] Seq=1 Ack=397 Win=104 Len=0		
16 0.73670	9 144.217.74.230	10.0.44.120	HTTP	274 HTTP/1.1 200 OK		
17 0.77626	9 10.0.44.120	144.217.74.230	TCP	54 14171 → 80 [ACK] Seq=397 Ack=221 Win=259 Len=0		
0 6c 3b 6b 1	fd 28 1d e4 42 a6 2f 9f	3b 08 00 45 00 1;k	(B./.;.	.ε.		
0 6c 3b 6b 1 0 1 b4 7e 0	Fd 28 1d e4 42 a6 2f 9f 33 40 90 80 95 66 a9 9a 5 40 9 46 7 - 2-	3b 08 00 45 00 1;k 00 2c 78 90 d9	:.(В./.;. с@ h,	.Е. Х.		
00 6c 3b 6b 1 00 01 b4 7e 0 01 a 63 67	fd 28 1d e4 42 a6 2f 9f fd 28 1d e4 42 a6 2f 9f 3 40 00 80 0f 68 a9 0a 3 6 00 50 09 df 8a fa 9c	3b 08 00 45 00 l;k 00 2c 78 90 d9 5c a5 28 50 18 J.7 6p 6d 67 57 70	(B/.;. c@h, '[.P\.	.б. ж. Ре		
0 6c 3b 6b 1 0 01 b4 7e 0 4a e6 37 9 0 01 03 67 9 78 2e 70 0	fd 28 1d e4 42 a6 2f 9f 63 40 00 80 06 68 a0 08 10 00 50 09 df 8a fa 9c 77 00 00 47 45 54 20 2f 10 7 16 00 47 45 34 33 30 30	3b 08 00 45 00 1;k 00 2c 78 90 d9 5c a6 28 50 18 3.7 69 6d 67 2f 70g 67 47 31 43 1 x n	:.(B ./.;. c@h, [.P\. ;GE T /im pr2i= 3088t	.Е. Х (Р. 2/9		
00 6c 3b 6b 1 10 01 b4 7e 0 10 4a e6 37 9 10 01 03 67 0 10 78 2e 70 35 31 39	fd 28 1d e4 42 a6 2f 9f 53 40 00 80 06 68 a9 0a 55 00 50 09 df 8a fa 9c 70 00 00 47 5 54 20 2f 16 67 3f 69 3d 33 30 30 12 36 34 30 63 53 23 24	3b 08 00 45 00 1;k 00 2c 78 90 d9 5c a6 28 50 18 3.7 69 6d 67 2f 70 26 74 73 3d 31 x.p 35 26 67 65 3d 519	:.(B ./.;. c@ h, '[.P\. :GE T /im ing?i= 300&t 26406 5245&	.б. я. я. а. а. а. ве		
00 6c 3b 6b 10 01 b4 7e 20 4a e6 37 0 01 03 67 10 78 2e 70 10 78 24 76 10 35 31 39 10 49 44 26	fd 28 1d e4 42 a6 2f 9f 53 40 00 80 66 68 a0 0a 50 06 50 06 47 45 54 20 2f 67 76 00 47 45 54 20 2f 67 3f 69 3d 33 30 30 12 36 34 30 36 35 32 34 3 61 3d 35 30 30 30 31	3b 08 00 45 00 1; 00 2c 78 90 d9 5c a6 28 50 18 66 d6 72 f70 25 74 73 3d 31 x,p 35 26 67 65 3d 519 26 70 69 64 4d 108	:.(B ./.;. c@h, [.P\ GE T /im ng?i= 300&t 126406 5245& sa=59 001&p	.Е. Х. (Р. ge ge= Ца		
6 3b 6b 4 0 1 b4 7e 6 4 a 6 37 5 0 1 0 37 3 3 0 78 2e 70 6 35 31 39 3 <	fd 28 ld e4 42 a6 2f 9f 53 40 00 80 66 68 a0 0a 55 00 50 09 df 8a fa 9c 70 00 00 47 5 54 20 2f 70 00 70 47 5 54 20 2f 13 64 30 35 39 30 30 31 43 61 30 35 39 30 30 31 43 12 67 37 4 36 67 72	3b 98 90 45 90 1;k 90 2c 78 90 d9 , 5c a6 28 50 18 J.7 e.g 26 74 73 31 x.p g 35 26 76 35 35 35 35 35 35 35 35 35 35 36 3	:.(B ./.;. c@h, '[.P\. :GE T /im ong i= 300&t 126406 5245& isa=59 001&p 41&st = gr&d	.Е. А. А. А. А. Ба Ба Ба Ба Сам		
00 6c 3b 6b 10 01 b4 7e 24 6e 37 36 10 01 03 67 42 62 35 31 9 50 49 44 26 37 37 35 36 77 77 26	Fd 28 1.d e4 42 a6 2.f 9.f 53 40 00 80 66 68 0 0a 50 60 90 90 66 8a fa 9.c 70 00 00 47 54 20 2.f 54 20 2.f 67 36 9.d 3.3 3.3 3.3 3.2 3.2 3.1 3.1 3.5 3.2 3.4 3.6 3.5 3.2 3.4 3.6 3.5 3.2 3.4 3.6 3.5 3.2 3.4 3.6 3.5 3.3 3.6 3.6 3.6 3.7 3.6 6.7 7.6 3.6 7.7 3.6 6.7 7.7 3.6 6.7 7.2 3.6 7.7 3.6 6.7 7.3 6.7 7.3 6.7 7.3 6.7 7.3 6.7 7.3 6.7 7.3 6.7 7.7 3.6<	3b 08 00 45 00 1;k 00 2c 78 90 30 5c a6 28 50 81 3.7 56 cd 72 73 46 7 7.73 57 26 76 53 45 108 26 46 67 47 73 41 26 64 67 45 34 118 26 64 67 47 73 64 64 64 34 77 759	:.(B ./.;. -c@ h, '[.P\. :GE T /im ing?i= 3066 5245& isa=59 001& M1&st =gr&d Kampa s.com	.Е. Х. (Р. 26 26 26 26 26 26 26 26 26 26 26 26 26		
00 6c 3b 6b+ 10 01 b4 7e 20 4a e6 37 30 01 03 67 36 35 31 39 56 35 31 39 670 37 35 36 36 77 77 2a 90 3d 31 26	fd 28 1.d e4 2 a6 27 b7 b4 00 80 66 68 a9 ba b5 09 50 06 68 a9 ba b7 00 04 74 36 34 35 10 b6 76 90 04 74 35 34 35 10 10 b6 76 76 34 33 30 35 32 34 36 33 32 34 35 32 34 36 33 32 34 35 32 34 36 37 36 33 32 34 36 34 37 36 36 36 36 36 37 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36	3b 08 00 45 00 1; 00 2: 78 90 60 50 64 74 73 61 3.7. 60 64 74 73 63 5.19 26 74 73 63 5.19 5.19 26 74 73 64 64 5.19 5.19 26 74 73 64 64 5.10 7.75 67 64 5.10 7.75 67 64 62 62 72 7 75 64 64 73 7.75 64 64 72 72 =.18 64 64 73 72 =.18 64 64 73 72 =.18 64 64 73 72 =.18 64 64 73 72 =.18 64 64 73 72 =.18 64 73 72 =.18	(B ./.;. .c@h, [.P\. 	-Е. Х., (Р, %/0 S=1 ge= ide очи db1 -7.		
00 6c 3b 6b + 10 01 b4 7e 20 4a e6 37 30 01 03 c7 4a e6 37 5 60 49 42 66 70 37 35 3e 80 77 72 e 90 3d 12 3e 610 32 38 5f	Id 28 1d e4 42 86 2f 9f 51 40 00 80 0f 68 a9 0a 55 00 56 00 9f 78 a fa 62 100 00 80 0f 53 30 55 21 56 34 30 56 23 16 34 30 56 35 32 45 23 16 34 30 56 35 32 45 36 13 43 57 37 43 36 77 32 68 36 66 47 05 17 32 68 36 66 47 05 17 32 48 36 66 47 05 17 28 45 36 68 63 34 39 38 33 33 36 86 63 34 39 77 34 34 37 28 45 36 28 63 34 39 37 28 45 38 28 28 28 27 77 28 45 38 28 28 28 28 28 28 28 38 28 28 28 28 28 28 28 28 28 28 28 28 28	3b 08 00 45 00 1; k 00 2c 78 90 90 5c a6 28 50 3 7. 56 c6 76 73 9. 6. 7. 57 67 67 65 3 7. 7. 5. 56 76 53 4.5 1.0. 1.0. 7. 7.6 52 66 67 65 3 7. 7.6 6. 6.5 4 1.0. 8 7. 7.6 6.6 7.6 7.0. 6.6 9 4 7.7 7.6 6.6 7.6 7.0. 6.6 9 6.6 9 3 7.8 3 7.8 3 7.8 3 3 7.8 3 7.8 3 7.8 3 3 7.8 3 7.8 3 3 3 3	:.(B ./.;. c@ h, [.P\. 	.Є. Х. (Р. g/p 543 543 546 Осан Аба Осан Аба Аба Аба Аба Аба Аба Аба Аба Аба Аба		
00 6c 3b 6b 10 01 b4 7c 6 20 4a e6 37 9 01 03 01 03 7 7 040 78 28 70 7 7 36 050 35 31 39 3 36 37 73 38 37 77 77 26 32 34 31 26 32 34 35 56 32 34 35 56 32 34 35 36 32 35 57 77 77 26 32 34 35 35 36 32 35 35 36 32 34 36	fd 28 1.d e4 42 a6 27 57 b0 08 00 66 68 a9 08 58 48 fa 90 90 67 88 fa 90<	3b 08 00 4.5 00 1.; 00 2.7 79 0.6 5c a6 25 90 18 5c a6 2.6 70 26 74 73 31 3. x.p. 25 26 67 63 51 51 26 74 76 64 63 37 7 26 64 64 34 7 758 64 64 34 11 32 43 28 7 759 64 63 32 7 759 64 64 32 32 83 28 32 32 33 24 32 33 32 33 34 32 33 34 34 32 33 34 32 33 34 34 34 34 34 34 34	:.(B ./.;. c@h, [GE T /im ng?i= 300&t (26406 5245& (26406 5245& (26406 5245& (26406 5245& (3630 4200 4000 4000 4000 4000 4000 4000 40	-Е. Х., (Р., %/D S=1 ge= ido очи Abi ~7. Я2С Я2С Но		
6c 3b 6b 4 0 10 bd 7 0 4 a 6 7 0 10 3 7 7 0 10 3 7 3 7 0 37 75 3 3 3 1 6 0 32 38 5 1 2 2 4 3 1 6 5 7 7 2 4 3 1 6 6 7 7 4 3 1 <t< td=""><td>Id 28 1d e4 42 a6 2f 5f 5d 40 60 66 a9 6a 5 35 56 56 66 66 a9 6a 56 56 56 96 67 84 56 55 36 57 36 36 51 31 36 56 36 57 37 36 57 37 36 57 32 36</td></t<> <td>3b 08 00 45 00 1; 00 2c 78 90 d3 5c a6 25 91 B3 26 a6 32 70 a6 26 a6 70 a6 a6 26 a6 70 66 63 100 26 a6 34 77 a6 63 26 a6 34 77 a6 46 34 .7. 26 a6 34 26 a6 34 .7. 26 a6 34 31 a5 34 .</td> <td></td> <td>.Е. Х (Р. «/Ф 5=1 5=4 0=34 8=4 0=34 841 8-7. Я2 С 4-7. А. 22 С 4-9 4-9 4-9 4-9 4-9 4-9 4-9 4-9 4-9 4-9</td> <td></td> <td></td>	Id 28 1d e4 42 a6 2f 5f 5d 40 60 66 a9 6a 5 35 56 56 66 66 a9 6a 56 56 56 96 67 84 56 55 36 57 36 36 51 31 36 56 36 57 37 36 57 37 36 57 32 36	3b 08 00 45 00 1; 00 2c 78 90 d3 5c a6 25 91 B3 26 a6 32 70 a6 26 a6 70 a6 a6 26 a6 70 66 63 100 26 a6 34 77 a6 63 26 a6 34 77 a6 46 34 .7. 26 a6 34 26 a6 34 .7. 26 a6 34 31 a5 34 .		.Е. Х (Р. «/Ф 5=1 5=4 0=34 8=4 0=34 841 8-7. Я2 С 4-7. А. 22 С 4-9 4-9 4-9 4-9 4-9 4-9 4-9 4-9 4-9 4-9		
6c 3b 6b 0 1b 47 6 0 4a 63 7 0 10 36 7 7 0 10 37 35 38 31 26 0 32 38 57 32 38 57 0 32 38 57 37 35 32 36 57 0 32 38 57 32 34 32 36 57 36 32 36 57 36 36 37 35 36 36 37 35 36 36 37 36 37 37 34 32 36 57 36 3	fd 28 1.d e4.42 a6.2 ff ff b 09.8 00.9 66 a.9 0a.5 b.9 05.6 b.9 04.6 b.9 04.6	3b 08 00 45 00 1, 5c a6 26 78 90 40 -, 5c a6 28 91 1, -, - - 5c a6 28 91 1, -, - </td <td>(B ./.;. c@h, cGE T /im mg71=3008k 25406 52458 53406 52458 53406 52458 53406 52458 53406 52458 53406 52458 53406 52458 53406 52458 53406 534 5340 5340 5340 5340 5340 5340 5340 5340 5340 5340 5340 53400 5340 5340 53400 5340 53400000000000000000000000000000000</td> <td>.Е. Х., (Р., ½/р S=1 S=2 S=3 S=4 S=4 S=4 S=4 S=4 S=4 S=4 S=4</td> <td></td> <td></td>	(B ./.;. c@h, cGE T /im mg71=3008k 25406 52458 53406 52458 53406 52458 53406 52458 53406 52458 53406 52458 53406 52458 53406 52458 53406 534 5340 5340 5340 5340 5340 5340 5340 5340 5340 5340 5340 53400 5340 5340 53400 5340 53400000000000000000000000000000000	.Е. Х., (Р., ½/р S=1 S=2 S=3 S=4 S=4 S=4 S=4 S=4 S=4 S=4 S=4		
00 6c 3b 6b 1 00 10 164 7c 1 01 04 10 3 7c 1 01 01 03 67 1 3 1 30 01 03 53 13 30 1 26 1 3 <td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td> <td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td> <td>(B./.;. c@h., [_P] </td> <td>.E. X (P g/p 5-35 5</td> <td></td> <td>Pro</td>	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	(B./.;. c@h., [_P] 	.E. X (P g/p 5-35 5		Pro

Pada gambar diatas telah didapatkan beberapa data dalam bentuk paketpaket data jaringan .Dikarenakan semua paket tersaring dengan cepat, maka kita akan filter terlebih dahulu dengan menggunakan sintaks "<u>ipc.rc==10.0.44.29</u>". Setelah di filter maka akan terdapat data sebagai berikut:

a maan waa					-	3 ×
File Edit View Go Ca	pture Analyze Statisti	cs Telephony Wireless Te	ools Help			
🖌 🔳 🧟 🔘 📘 🗋 🎽	रे 🙆 🔍 🗰 🗯 🗃 🕯	F 🛨 🛄 📄 Q Q Q	**			
ip.src==10.0.44.120					E - Ex	ression
io. Time	Source	Destination	Protocol	Length Info		
2.0.000055	10.0.44.120	216.58.201.138	TCP	66 14427 → 80 [ACK] Seg=1 Ack=1 Win=258 Len=0 SLE=0 SRE=1		
4 0,004685	10.0.44.120	216,58,201,138	TCP	66 14426 → 80 [ACK] Seg=1 Ack=1 Win=258 Len=0 SLE=0 SRE=1		_
6 0.031175	10.0.44.120	216,58,201,138	TCP	66 14430 → 80 [ACK] Seg=1 Ack=1 Win=258 Len=0 SLE=0 SRE=1		
7 0.150493	10.0.44.120	216.58.201.142	TCP	55 14383 → 80 [ACK] Seq=1 Ack=1 Win=255 Len=1		
8 0.446535	10.0.44.120	104.25.235.4	TCP	66 14431 → 80 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1		_
 9 0.452896 	10.0.44.120	144.217.74.230	HTTP	450 GET /img/px.png?i=300&ts=1519264065245≥=ID&sa=59001&pid=75041&st=gr&do=www.kompas.com&bi=1&cha=993&di=7.28_c	.9≺=%2C%2C%	2C _
10 0.456517	10.0.44.120	93.184.220.29	TCP	55 14388 → 80 [ACK] Seq=1 Ack=1 Win=256 Len=1		=
12 0.463678	10.0.44.120	104.25.235.4	TCP	54 14431 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0		
17 0.776269	10.0.44.120	144.217.74.230	TCP	54 14171 → 80 [ACK] Seq=397 Ack=221 Win=259 Len=0		
18 0.888037	10.0.44.120	216.58.211.238	TLSv1.2	353 Application Data		_
19 0.888197	10.0.44.120	216.58.211.238	TLSv1.2	804 Application Data		_
20 0.888413	10.0.44.120	216.58.211.238	TLSv1.2	795 Application Data		
000 6c 3b 6b fd 28	B 1d e4 42 a6 2f 9	f 3b 08 00 45 00 1;	k.(B./.;	I.		
020 4a e6 37 5b 00	0 50 09 df 8a fa 9	a oo xe ya 90 ug	······································			
		c 5c a6 28 50 18 J.	7[.P.,			
030 01 03 67 07 00	0 00 47 45 54 20 2	c 5c a6 28 50 18 J. f 69 6d 67 2f 70	7[.P\.() gGE T /img	2. /p		
030 01 03 67 07 0 040 78 2e 70 6e 6	0 00 47 45 54 20 2 7 3f 69 3d 33 30 3	c 5c a6 28 50 18 J. f 69 6d 67 2f 70 0 26 74 73 3d 31 x.	7[.P\.() gGE T /img, png?i= 300&ts-	ζ. /p -1		
030 01 03 67 07 0 040 78 2e 70 6e 6 050 35 31 39 32 30	0 00 47 45 54 20 2 7 3f 69 3d 33 30 3 6 34 30 36 35 32 3	c 5c a6 28 50 18 J. f 69 6d 67 2f 70 0 26 74 73 3d 31 x. 4 35 26 67 65 3d 51	7[.P\.(F gGE T /img, png?i= 300&ts- 926406 5245≥	ς, γρ -1 2*		
030 01 03 67 07 01 040 78 2e 70 6e 67 050 35 31 39 32 36 060 49 44 26 73 61	0 00 47 45 54 20 2 7 3f 69 3d 33 30 3 5 34 30 36 35 32 3 1 3d 35 39 30 30 3	c 5c a6 28 50 18 J. f 69 6d 67 2f 70 0 26 74 73 3d 31 x. 4 35 26 67 65 3d 51 1 26 70 69 64 3d ID	7[.P\.(I gGE T /img, png?i= 300&ts 926406 5245&g &sa=59 001&pic	2. 7p +1 4=		
030 01 03 67 07 00 040 78 2e 70 6e 61 050 35 31 39 32 36 060 49 44 26 73 61 070 37 35 30 34 31	0 00 47 45 54 20 2 7 3f 69 3d 33 30 3 5 34 30 36 35 32 3 1 3d 35 39 30 30 3 1 3d 35 39 30 30 3 1 2d 73 74 3d 67 6 47 74 3d 37 3	c 5c a6 28 50 18 J. f 69 6d 67 2f 70 0 26 74 73 3d 31 x. 4 35 26 67 65 3d 51 1 26 70 69 64 3d ID 2 26 64 6f 3d 77 75	7[.P\.(I gGE T /img, png?i= 300&ts 926406 5245&g &sa=59 001&pic 041&st =gr&do	5, fg -1, fa fa an		
030 01 03 67 07 01 040 78 2e 70 6e 6. 050 35 31 39 32 30 060 49 44 26 73 6. 070 37 35 30 34 31 080 77 72 2e 6b 61	0 0 47 45 54 20 2 7 3f 69 3d 33 30 3 5 34 30 36 35 32 3 1 3d 35 39 30 30 3 1 3d 35 39 30 30 3 1 2d 73 74 3d 67 7 f 6d 70 61 73 2e 6 6 81 24 29 29 23 23	c 5c 36 28 50 18 J. f 69 6d 67 2f 70 d 36 6d 67 2f 70 d 35 26 67 65 3d 31 x. d 35 26 67 65 3d 51 1 26 67 69 64 3d ID 2 26 64 67 67 75 3 6f 62 62 69 with 3 6f 62 62 62 69 with 41 76 75 3 6f 62 62 62 94 41 76	7[.P\.(I gGE T /img, png?i= 300&ts 926406 5245&g &sa=59 001&pic 041&st =gr&do: .kompa s.com&l &cha=0 92&di=			
030 01 03 67 07 01 044 78 2e 70 6e 6 050 35 31 39 32 36 050 35 31 39 32 36 060 49 44 26 73 65 070 37 35 30 34 31 080 77 77 2e 6b 61 090 3d 31 26 63 61 090 34 32 36 63 62	0 00 47 45 54 20 2 7 3f 69 3d 33 30 3 3 30 36 35 32 3 30 3 1 3d 35 39 30 36 35 32 30 3 1 3d 35 39 30 36 35 32 30 31 1 2d 73 74 3d 67 7 6 61 70 61 73 2e 6 8 61 3d 39 39 33 32 32 32 9 26 70 72 32 <th>c 5c a6 28 50 18 J. f 69 6d 67 2f 70 0 26 74 73 3d 31 x. 4 35 26 67 65 3d 51 1 26 70 69 64 3d ID 2 26 64 6f 3d 77 75 3 6f 6d 26 62 69 ww 6 64 69 3d 37 2e -1 3 24 32 53 24 43 28</th> <th>7[.P\.(I gGE T /img, png?i= 300&ts 926406 5245&g &sa=59 001&pic 041&st =gr&do .kompa s.com&l &cha=9 93&di= 0.9&p r=%2C%</th> <th>2. 19 19 19 19 19 10 7. 10</th> <th></th> <th></th>	c 5c a6 28 50 18 J. f 69 6d 67 2f 70 0 26 74 73 3d 31 x. 4 35 26 67 65 3d 51 1 26 70 69 64 3d ID 2 26 64 6f 3d 77 75 3 6f 6d 26 62 69 ww 6 64 69 3d 37 2e -1 3 24 32 53 24 43 28	7[.P\.(I gGE T /img, png?i= 300&ts 926406 5245&g &sa=59 001&pic 041&st =gr&do .kompa s.com&l &cha=9 93&di= 0.9&p r=%2C%	2. 19 19 19 19 19 10 7. 10		
030 01 03 67 07 04 0400 78 2e 70 6e 6 050 35 31 39 32 36 050 35 31 39 32 36 060 77 73 30 34 31 080 77 77 2e 6b 66 090 3d 31 26 36 080 77 77 2e 6b 66 090 3d 31 26 36 66 090 3d 31 26 36 66 090 3d 31 26 35 42 090 32 38 5f 30 24 090 32 38 5f 30 24 090 25 32 34 32 36	0 00 47 45 54 20 2 7 36 69 3d 33 30 3 5 34 30 35 35 32 3 1 3d 35 39 30 36 35 32 3 1 2d 73 74 3d 67 7 f 6d 70 61 73 2e 6 8 61 3d 39 39 33 2 6 8 61 3d 39 39 33 32 6 8 61 3d 39 39 33 2 6 8 52 54 54 56 72 3d 2 8 54 54 56 26 70 33 2 8 54 54 56 26 70 23 2	c 5c a6 28 50 18 J. f 69 6d 67 2f 70 0 26 74 73 3d 31 x. 4 35 26 67 65 3d 51 12 1 26 70 69 64 3d ID 2 26 66 62 69 2 36 66 62 62 69 w 6 64 69 3d 37 2e =1 5 32 43 25 32 43 28 28 31 04 0a 48 6f \$22	7[.P			
030 01 03 67 07 01 041 78 2e 70 6e 6 5 35 31 31 33 31 33 34 3 050 49 44 26 73 65 67 67 070 37 35 30 34 32 86 77 77 2e 6b 61 61 61 63 61 63 64 63 64 63 64 64 63 64 <th>00 047 45 54 202 7 3f 69 3d 33 36 35 3 36 35 32 33 36 35 32 31 36 35 32 31 31 36 35 32 31 31 36 35 32 31 31 36 35 32 31 31 36 35 32 31 31 32 31 31 32 31 31 36 35 32 31 31 36 37 74 34 31 70 74 34 77 74 34 77 74 34 77 74 34 77 74 34 70 73 74 34 73 74 34 73 74 34 32 32 32 32 32 32 32 32 32 32 32 32 32<th>$\begin{array}{c} c \ sc \ ab \ 28 \ 50 \ 18 \ J, \\ f \ 69 \ 6d \ 67 \ 27 \ 70 \ \\ ab \ 28 \ 26 \ 77 \ 75 \ 3d \ 31 \ x, \\ 4 \ 35 \ 26 \ 67 \ 65 \ 3d \ 51 \ 12 \ 75 \ 36 \ 6d \ 6d \ 3d \ 77 \ 75 \ 36 \ 6d \ 6d \ 26 \ 3d \ 77 \ 75 \ 36 \ 6d \ 6d \ 26 \ 3d \ 37 \ 7e \ 41 \ 53 \ 24 \ 32 \ 3d \ 3d \ 3d \ 3d \ 72 \ 4d \ 5d \ 3d \ 3d \ 7d \ 7d \ 3d \ 3d \ 3d \ 7d \ 7$</th><th>7[.P</th><th>2. 3. 4. 4. 4. 4. 4. 4. 4. 4. 4. 4</th><th></th><th></th></th>	00 047 45 54 202 7 3f 69 3d 33 36 35 3 36 35 32 33 36 35 32 31 36 35 32 31 31 36 35 32 31 31 36 35 32 31 31 36 35 32 31 31 36 35 32 31 31 32 31 31 32 31 31 36 35 32 31 31 36 37 74 34 31 70 74 34 77 74 34 77 74 34 77 74 34 77 74 34 70 73 74 34 73 74 34 73 74 34 32 32 32 32 32 32 32 32 32 32 32 32 32 <th>$\begin{array}{c} c \ sc \ ab \ 28 \ 50 \ 18 \ J, \\ f \ 69 \ 6d \ 67 \ 27 \ 70 \ \\ ab \ 28 \ 26 \ 77 \ 75 \ 3d \ 31 \ x, \\ 4 \ 35 \ 26 \ 67 \ 65 \ 3d \ 51 \ 12 \ 75 \ 36 \ 6d \ 6d \ 3d \ 77 \ 75 \ 36 \ 6d \ 6d \ 26 \ 3d \ 77 \ 75 \ 36 \ 6d \ 6d \ 26 \ 3d \ 37 \ 7e \ 41 \ 53 \ 24 \ 32 \ 3d \ 3d \ 3d \ 3d \ 72 \ 4d \ 5d \ 3d \ 3d \ 7d \ 7d \ 3d \ 3d \ 3d \ 7d \ 7$</th> <th>7[.P</th> <th>2. 3. 4. 4. 4. 4. 4. 4. 4. 4. 4. 4</th> <th></th> <th></th>	$ \begin{array}{c} c \ sc \ ab \ 28 \ 50 \ 18 \ J, \\ f \ 69 \ 6d \ 67 \ 27 \ 70 \ \\ ab \ 28 \ 26 \ 77 \ 75 \ 3d \ 31 \ x, \\ 4 \ 35 \ 26 \ 67 \ 65 \ 3d \ 51 \ 12 \ 75 \ 36 \ 6d \ 6d \ 3d \ 77 \ 75 \ 36 \ 6d \ 6d \ 26 \ 3d \ 77 \ 75 \ 36 \ 6d \ 6d \ 26 \ 3d \ 37 \ 7e \ 41 \ 53 \ 24 \ 32 \ 3d \ 3d \ 3d \ 3d \ 72 \ 4d \ 5d \ 3d \ 3d \ 7d \ 7d \ 3d \ 3d \ 3d \ 7d \ 7$	7[.P	2. 3. 4. 4. 4. 4. 4. 4. 4. 4. 4. 4		
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$ \begin{array}{c} c \ sc \ ab \ 28 \ 50 \ 18 \ J, \\ f \ 69 \ 6d \ 72 \ 77 \ 70 \ \\ 0 \ 26 \ 74 \ 73 \ 3d \ 31 \ x, \\ 43 \ 52 \ 6b \ 76 \ 53 \ ds \ 51 \ 126 \ 76 \ 53 \ ds \ 51 \ 126 \ 76 \ 53 \ ds \ 51 \ 126 \ 76 \ 69 \ 64 \ 3d \ 1D \ 22 \ 26 \ 64 \ 6f \ 3d \ 77 \ 75 \ 30 \ 6f \ 6d \ 6f \ 5d \ 72 \ 6d \ 6d \ 73 \ 2d \ 32 \ 73 \ 75 \ 3d \ 73 \ 75 \ 3d \ 73 \ 75 \ 75 \ 3d \ 74 \ 75 \ 75 \ 75 \ 75 \ 75 \ 75 \ 75$	7[.P gGE T /img, png?i= 300&ts. 926406 5245&gr &sa=59 001&bii 41&st =gr&do: .kompa s.com&& &cha=9 93&di=: _0.9&p r=%2C%. C HTTP /1.1.H : cdn3 .org.l -Agent : Mozi.			
01 03 67 07 00 0804 78 2 70 66 6 03040 78 2 70 66 6 13 13 23 3 0606 45 31 39 32 3	0 00 47 45 54 202 7 7 6 69 30 33 30 35 5 34 30 36 35 32 3 1 3d 35 39 30 36 35 32 3 1 3d 35 39 30 30 36 37 7 6 07 00 61 73 2e 6 8 61 3d 39 39 33 2 8 54 56 77 22 3d 2 8 54 56 27 72 3d 2 8 54 56 27 3a 20 47 7 65 6e 74 3a 20 4	$ \begin{array}{c} c \ >c \ ab \ 28 \ >b \ >b \ 28 \ >b \$	7[.P(() gGE T /img, ppg?i= 300&ts: 926406 5245&gr &sa=59 001π: 041&st = gr&do: .kompa s.com&& &cha=9 93&di= _0.9&p = n*2C%. C HTTP /1.1l : cdn3.org.t -Agent : Mozi:	-, 6 9 19 19 19 10 10 10 10 11 11 10 10 10 10 10 10 10		Frofile: De

dapat dilihat sendiri bahwa dengan komputer yang beralamatkan 10.0.44.29 sedang mencoba mengakses 144.217.74.20 atau website <u>www.kompas.com</u> dengan menggunakan protokol TCP. Setelah itu jika kita mengklik bagian kotak tengah di menu Internet Protocol.

BAGIAN KEDUA "Dengan Menggunakan Menu Follow Stream"

🚄 tug	as1.pcap									— r	5 ×
File	Edit View Go Ca	apture Analyze Statisti	ics Telephony Wireless Too	s Help							
	(đ 💿 📜 🗎 🕅	। २ 🖸 २ 🗰 🗰 🗃 व	F 👲 🚍 📄 Q Q Q 🕅								
ip.sr	c==10.0.44.120									B - • Ex	pression +
No	Time	Source	Destination	Protocol	Length Info						-
	2.0.000055	10.0.44.120	216 58 201 138	TCP	66 14427 + 8	ACKI Seg-1 Ack-1 Win-	258 Len-0 SLF	-0 SRE-1			
	4.0.004685	10.0.44.120	216.58.201.138	TCP	66 14426 → 8	ACK] Seg=1 Ack=1 Win=	258 Len=0 SLE	=0 SRF=1			
	6.0.031175	10.0.44.120	216.58.201.138	TCP	66 14430 → 8	ACK] Seg=1 Ack=1 Win=	258 Len=0 SLE	=0 SRE=1			
	7.0.150493	10.0.44.120	216.58.201.142	TCP	55 14383 → 8	ACK] Seg=1 Ack=1 Win=	255 Len=1				_
	8 0.446535	10.0.44.120	104.25.235.4	TCP	66 14431 → 8	[SYN] Seg=0 Win=64240	Len=0 MSS=146	0 WS=256 SACK P	ERM=1		
	9 0.452896	10.0.44.120	144,217,74,230	HTTP	450 GET /img/	nng24_2008+c_15103640	SCOASE -TOR	a=59001&pid=750	41&st=er&do=www.kompas.com&bi=1&cha=993&di=7.28 0	.98pr=%2C%2C%	2C
	10 0.456517	10.0.44.120	93,184,220,29	TCP	55 14388 → 8	Mark/Unmark Packet	Ctrl+M				-
	12 0.463678	10.0.44.120	104.25.235.4	TCP	54 14431 → 8	Ignore/Unignore Packet	Ctrl+D				
	17 0,776269	10.0.44.120	144,217,74,230	TCP	54 14171 → 8	Set/Unset Time Reference	Ctrl+T				
	18 0.888037	10.0.44.120	216.58.211.238	TLSv1.2	353 Applicati	Time Shift	Ctrl+Shift+T				
	19 0.888197	10.0.44.120	216,58,211,238	TLSv1.2	804 Applicati	Packet Comment	Ctrl+Alt+C				_
	20 0.888413	10.0.44.120	216.58.211.238	TLSv1.2	795 Applicati	Edit Becchurd Mamo					
2.5-		(3600 bit	 AEQ hotes continued. 	(3600 Lite)		Edit Resolved Name					
5 64	ame 9: 450 Dytes	TotalCan 26:06:2h	(ad: 42: ad: 26: 06: 2b) Dr	Solo Dits)	64.20.14 (64.2	Apply as Filter	,				
I DE	hernet II, Sectorel	Version A Case 10	(e4.42.80.21.91.30), DS	74 330	_10.20.10 (00.5	Prepare a Filter	,				
To	cernet Protocol	wei Sion 4, Sic. 10	Doct: 14171 Det Doct: 9	A Sec. 1	Aski 1 Lani 30	Conversation Filter	,				
	partext Transfer	Protocol, SPC P	ore. 14171, DSC PORC. 8	, seq. 1,	Ack: 1, Left: 39	Colorize Conversation	,				
	per cente in onorier	1100002				SCTP	,				
						Follow	•	TCP Stream			
						Comu		UDP Stream			
						сору		SSI Stream			
						Protocol Preferences	,	HTTP Stream			
						Decode As			1		
						Show Packet in New Windo	w				
	6c 2h 6h fd 2	9 1d a4 42 a6 26 0	of 2h 02 00 45 00 1.k	/ p / .	c						
0000	01 b4 7e 63 4	0 00 80 06 68 89 6	a a a z z 78 90 d9	a h y							
0020	4a e6 37 5b 0	0 50 09 df 8a fa 9	9c 5c a6 28 50 18 3.7[.P\.(Ρ.						
0030	01 03 67 07 0	0 00 47 45 54 20 2	2f 69 6d 67 2f 70g.	GE T /imp	/p						
0040	78 2e 70 6e 6	7 3f 69 3d 33 30 3	30 26 74 73 3d 31 x.pn	g?i= 300&ts	=1						
0050	35 31 39 32 3	6 34 30 36 35 32 3	34 35 26 67 65 3d 5192	6406 5245&g	e=						
0060	49 44 26 73 6	1 3d 35 39 30 30 3	31 26 70 69 64 3d ID&s	a=59 001π	d=						
0070	37 35 30 34 3	1 26 73 74 3d 67 7	72 26 64 6f 3d 77 7504	1&st =gr&dc	b=bd						
0000	7/ 7/ 2e 60 67	t 60 70 61 73 28 t	05 67 60 26 62 69 WW.K	ompa s.come	-7						
0050	32 38 5f 30 2	e 39 26 70 72 3d 3	25 32 43 25 32 43 28 6	98n r=\$209	20						
00b0	25 32 43 20 4	8 54 54 50 2f 31 2	2e 31 0d 0a 48 6f %2C	HTTP /1.1.	Ho						
00c0	73 74 3a 20 6	3 64 6e 33 2e 6f 3	72 67 0d 0a 55 73 st:	cdn3 .org	Us						
00d0	65 72 2d 41 6	7 65 6e 74 3a 20 4	4d 6f 7a 69 6c 6c er-A	gent : Mozi	11						
0.00											V
02	tugasl				-				Packets: 1282 · Displayed: 650 (50.7%) · Load time: 0:0.22		Profile: Default
-		📄 🖻 🕥 🍯	9 📲 📭 🧐 🖸	<u> </u>					^ I	(A. Q.) 9:57 A	AM 📮

Seperti yang terlihat di gambar atas,pilih paket yang memiliki bentuk protokol http,dan langsung klik **analyze** => pilih **follow** => pilih **TCP Stream** atau bias klik kanan pada mouse => pilih **follow** => pilih **TCP Stream**.



Bisa kita lihat pada gambar diatas info apa saja yang telah dapat kita baca yakni :

- 1. Sang pengguna yang sedang mengakses website <u>www.kompas.com</u> menggunakan aplikasi Mozila.
- 2. Waktu mengakses web tersebut pada tanggal 22 februari 2018 pada hari kamis.
- 3. Type data yang sedang diakses itu berupa image/png.

BAGIAN KETIGA "Flow Graph Jaringan Menggunakan Aplikasi WireShark dan Visual Route"

Untuk melihat FlowGraph, kita mengklik menu "Statistics" lalu pilih "Flowgraph" maka data yang akan muncul adalah seperti ini:



Lalu lintas berjalannya ekspedisi informasi dapat divisualisasikan menggunakan Flow Graph seperti gambar diatas. Berikut adalah penjelasan terhadap panah pada flow graph:

- 1. Panah 1 komputer user mengirim informasi address atau link ke router jaringan.
- Panah 2 ketika router menerima informasi, maka ia akan mengalamatkan data tersebut ke isp sumber terdekat (palembang).
- 3. Panah 3 isp akan menanggapi permintaan user tersebut, apakah address yang dituju itu tersedia atau tidak.
- 4. Panah 4 apabila address tesedia, maka isp akan mengarahkan informasi tersebut ke isp pusat (mis. Jakarta).
- 5. Panah 5 isp pusat pun akan menanggapi permintaan tersebut, dan informasi tanggapan akan dikirim kembali ke user.
- 6. Panah 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. Panah 7 jika informasi tersebut valid, isp akan kembali mengirimkan tanggapan dan mengarahkannya ke isp pusat.
- Panah 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. Panah 9 disini situs yang diakses adalah www.detik.com dengan mengambil berita International dan nasional
- 10. Panah 10 seperti pada isp tadi, server pun akan mengirimkan informasi kepada user apakah address yang dituju tersebut valid atau tidak.

Dan berikut adalah tampilan dari aplikasi visualroute :



Dapat kita lohat 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. Dapat dimengerti oleh pengguna pemula.
- c. Visualisasi tempat source dan destination terlihat jelas.
- d. Setiap hope ditampilkan semua.