# **KOMUNIKASI DATA**

Analisis jaringan menggunakan Wireshark & Visual Route



### Disusun Oleh

NAMA	: Ahmad Yusuf Aditama
NIM	: 09011381621098
KELAS	: SK4B

# UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER PRODI SISTEM KOMPUTER 2017/2018

#### 1) Paket data

(c) 2017 Microsoft Corp	oration. All rights re	eserved.
C:\Users\Excalibur>arp	-a	
Interface: 192.168.100.	4 0x8	
Internet Address	Physical Address	Туре
192.168.100.1	2c-55-d3-2e-1f-4a	dynamic
192.168.100.255	ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
224.0.0.253	01-00-5e-00-00-fd	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff	static
Interface: 192.168.56.1	0xd	
Internet Address	Physical Address	Туре
192.168.56.255	<del>ff-ff-ff-ff-ff</del>	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
C:\Users\Excalibur>		

Dengan menggunakan Command Prompt, ketikkan perintah "arp –a", dengan begitu IP Address milik kita akan terlihat seperti gambar diatas.

Setelah itu, buka aplikasi Wireshark dan membuka web <u>www.kompas.com</u>. Lalu, akan muncul hasil seperti gambar berikut:

1101	oodree	besenation	1100000	
- 1 0.000000	192.168.100.4	104.244.42.67	SSL	55 Continuation Data
2 0.024751	104.244.42.67	192.168.100.4	TCP	66 443 → 50123 [ACK] Seq=1 Ack=2 Win=127 Len=0 SLE=1 SRE=2
3 0.432051	LiteonTe_89:c7:27	HuaweiTe_2e:1f:4a	ARP	42 Who has 192.168.100.1? Tell 192.168.100.4
4 0.432935	HuaweiTe_2e:1f:4a	LiteonTe_89:c7:27	ARP	42 192.168.100.1 is at 2c:55:d3:2e:1f:4a
5 1.915534	192.168.100.4	82.137.57.41	UDP	145 10044 → 30084 Len=103
6 2.438635	LiteonTe_89:c7:27	HuaweiTe_2e:1f:4a	ARP	42 Who has 192.168.100.1? Tell 192.168.100.4
7 2.439549	HuaweiTe_2e:1f:4a	LiteonTe_89:c7:27	ARP	42 192.168.100.1 is at 2c:55:d3:2e:1f:4a
8 2.833457	192.168.100.4	111.221.29.254	TCP	66 50378 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9 2.889645	111.221.29.254	192.168.100.4	TCP	66 443 → 50378 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1412 WS=256 SACK_PERM=1
10 2.889796	192.168.100.4	111.221.29.254	TCP	54 50378 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
11 2.890471	192.168.100.4	111.221.29.254	TLSv1.2	270 Client Hello
12 2.949140	111.221.29.254	192.168.100.4	TCP	1466 443 → 50378 [ACK] Seq=1 Ack=217 Win=131072 Len=1412 [TCP segment of a reassembled PDU]
13 2.949870	111.221.29.254	192.168.100.4	TCP	1466 443 → 50378 [ACK] Seq=1413 Ack=217 Win=131072 Len=1412 [TCP segment of a reassembled PDU]
14 2.949873	111.221.29.254	192.168.100.4	TLSv1.2	997 Server Hello, Certificate, Server Key Exchange, Server Hello Done
15 2.949928	192.168.100.4	111.221.29.254	TCP	54 50378 → 443 [ACK] Seq=217 Ack=3768 Win=66304 Len=0
16 2.952506	192.168.100.4	111.221.29.254	TLSv1.2	236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17 3.010194	111.221.29.254	192.168.100.4	TLSv1.2	161 Change Cipher Spec, Encrypted Handshake Message
18 3.011398	192.168.100.4	111.221.29.254	TLSv1.2	1323 Application Data
19 3.011662	192.168.100.4	111.221.29.254	TLSv1.2	635 Application Data
20 3.067613	111.221.29.254	192.168.100.4	TCP	56 443 → 50378 [ACK] Seq=3875 Ack=2249 Win=131072 Len=0
21 3.105400	111.221.29.254	192.168.100.4	TLSv1.2	395 Application Data
22 3.148647	192.168.100.4	111.221.29.254	TCP	54 50378 → 443 [ACK] Seq=2249 Ack=4216 Win=65792 Len=0
23 4.447271	LiteonTe_89:c7:27	HuaweiTe_2e:1f:4a	ARP	42 Who has 192.168.100.1? Tell 192.168.100.4
24 4.448123	HuaweiTe_2e:1f:4a	LiteonTe_89:c7:27	ARP	42 192.168.100.1 is at 2c:55:d3:2e:1f:4a
<ul> <li>Frame 1: 55 bytes of</li> <li>Ethernet II, Src: L</li> <li>Internet Protocol V</li> <li>Transmission Contro Secure Sockets Layer</li> </ul>	on wire (440 bits), 55 iteonTe_89:c7:27 (a4: /ersion 4, Src: 192.16 ol Protocol, Src Port: rr	5 bytes captured (440 db:30:89:c7:27), Dst: 58.100.4, Dst: 104.244 50123, Dst Port: 443	bits) on HuaweiTe 4.42.67 4, Seq: 1,	interface 0 _2e:1f:4a (2c:55:d3:2e:1f:4a) Ack: 1, Len: 1
0000 2c 55 d3 2e 1f 0010 00 29 56 aa 40 0020 2a 43 c3 cb 01 0030 00 ff 50 28 00	4a a4 db 30 89 c7 27 00 80 06 ec 40 c0 a8 bb 1b 9a b6 d3 2f f8 00 00	V 08 00 45 00 ,UJ 64 04 68 f4 .)V.@. 8 de db 50 10 *C P(	0' @d. /	E. h. P.

Setelah data-data paket terlihat, ketikkan "ip.src== 192.168.100.4" pada kolom filter. Lalu, hasilnya seperti gambar berikut:

🚺 *Wi	-Fi						- 0	×
File	Edit	View Go	Capture Analyze Statistic	cs Telephony Wireless	Tools He	lp		
<i>(</i>	۵	•	X ©   X ↔ ↔ ∰ 1	ि 🕭 🚍 🔲 🔍 🔍 🖉	2, 11			
ip.sr	c==1	92.168.100.4					Expres	sion   +
No.	1	īme	Source	Destination	Protocol	Length Info		*
31	187 5	30,320767	192,168,100,4	202.146.5.149	TCP	- 54 50551 → 443 [ACK] Seg=537 Ack=3589 Win=64715 Len=0		
3:	188 5	30.641493	192.168.100.4	23.66.253.191	TCP	1466 50540 → 443 ACK Seq=320 Ack=3768 Win=66048 Len=1412 ACP segment of a reassembled PDU		
3:	189 5	30.641508	192.168.100.4	23.66.253.191	TLSv1.2	1135 Application Data		
3:	197 9	30.693163	192.168.100.4	23.66.253.191	тср	66 [TCP Dup ACK 2636#1] 50540 → 443 [ACK] Seq=2813 Ack=3768 Win=66048 Len=0 SLE=9416 SRE=10828		
31	198 5	30.693276	192.168.100.4	23.66.253.191	TCP	54 50540 → 443 [ACK] Seq=2813 Ack=10828 Win=66304 Len=0		
32	203 5	30.723244	192.168.100.4	23.66.253.191	TCP	66 50540 → 443 [ACK] Seq=2813 Ack=12159 Win=65024 Len=0 SLE=3768 SRE=6592		
32	204 5	30.844507	192.168.100.4	24.94.56.187	UDP	145 10044 → 49607 Len=103		
32	205 5	30.885527	192.168.100.4	202.61.113.151	TCP	54 50536 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0		
32	208 5	30.915270	192.168.100.4	202.61.113.151	TCP	54 50536 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0		
► 32	211 9	31.024082	192.168.100.4	192.168.100.1	DNS	74 Standard query 0x0cf8 A www.kompas.com		
32	215 9	31.048173	192.168.100.4	192.168.100.1	DNS	74 Standard query 0x2d9a A www.kompas.com		
32	217 5	31.115473	192.168.100.4	23.66.253.191	TCP	1466 50540 → 443 [ACK] Seq=2813 Ack=12159 Win=65024 Len=1412 [TCP segment of a reassembled PDU]		
32	218 5	31.115489	192.168.100.4	23.66.253.191	TLSv1.2	1126 Application Data		
32	225 5	31.170507	192.168.100.4	23.66.253.191	TCP	54 50540 → 443 [ACK] Seq=5297 Ack=16259 Win=66304 Len=0		
33	226 5	31.176130	192.168.100.4	23.66.253.191	TCP	1466 50540 → 443 [ACK] Seq=5297 Ack=16259 Win=66304 Len=1412 [TCP segment of a reassembled PDU]		
32	227 5	31.176143	192.168.100.4	23.66.253.191	TLSv1.2	1126 Application Data		
33	228	31.178119	192.168.100.4	23.66.253.191	тср	1466 50542 → 443 [ACK] Seq=320 Ack=3768 Win=66048 Len=1412 [TCP segment of a reassembled PDU]		*
▷ Fra	me 3	211: 74 byt	es on wire (592 bits),	74 bytes captured (	692 bits)	on interface 0		
▷ Eth	erne	t II, Src:	LiteonTe_89:c7:27 (a4:	db:30:89:c7:27), Dst	HuaweiTe	_2e:1f:4a (2c:55:d3:2e:1f:4a)		
▷ Int	erne	t Protocol	Version 4, Src: 192.16	8.100.4, Dst: 192.16	3.100.1			
⊳ Use	r Da	tagram Prot	ocol, Src Port: 50505,	Dst Port: 53				
Dom	ain	Name System	(query)					
0000	2c	55 d3 2e 1f	4a a4 db 30 89 c7 27	08 00 45 00 ,U	0'	E		
0010	00	3c 7a 29 00	00 80 11 77 31 c0 a8	64 04 c0 a8 . <z).< td=""><td> w1d.</td><td>••</td><td></td><td></td></z).<>	w1d.	••		
0020	64	01 c5 49 00	35 00 28 3e 32 0c f8	01 00 00 01 dI.	5.( >2	••		
0030	00	00 00 00 00	00 03 77 77 77 06 6b	6† 6d 70 61	.w ww.kom	pa		
0040	/5	05 05 07 00	00 00 01 00 01	s.com				
0 7				FD 4D 2010022122222 -002	20			fler Defer it
	W	resnark_830C88	00-01E3-4AA4-A1/9-/8C09846	3040_20180221233232_a007	20	Packets: 19650 • Displayed: 7322 (37.3%)	Pro	one: Default
	0	) (T)	iii (i) 👔	📕 💥 🚺	0	s 🔽 🔤 📶 🚺 🖉 🖉	↓ 11:56 PM	<b>R</b>
							2/21/2018	

Dari gambar diaatas, terlihat Source-nya adalah 192.168.100.4 dan Destination-nya adalah 202.61.113.151 dengan menggunakan protocol TCP. Setelah itu, Klik Internet Protocol Version 4, dan hasilnya sebagai berikut:

ip.src:	==192.168.100.4					Expression
No.	Time	Source	Destination	Protocol	Length Info	
318	37 530.320767	192.168.100.4	202.146.5.149	TCP	54 50551 → 443 [ACK] Seq=537 Ack=3589 Win=64715 Len=0	
318	38 530.641493	192.168.100.4	23.66.253.191	TCP	1466 50540 → 443 [ACK] Seq=320 Ack=3768 Win=66048 Len=1412 [TCP segment of a reassembled PDU]	
318	39 530.641508	192.168.100.4	23.66.253.191	TLSv1.2	1135 Application Data	
319	97 530.693163	192.168.100.4	23.66.253.191		66 [TCP Dup ACK 2636#1] 50540 → 443 [ACK] Seq=2813 Ack=3768 Win=66048 Len=0 SLE=9416 SRE=10828	3
319	98 530.693276	192.168.100.4	23.66.253.191	TCP	54 50540 → 443 [ACK] Seq=2813 Ack=10828 Win=66304 Len=0	
320	03 530.723244	192.168.100.4	23.66.253.191	TCP	66 50540 → 443 [ACK] Seq=2813 Ack=12159 Win=65024 Len=0 SLE=3768 SRE=6592	
320	04 530.844507	192.168.100.4	24.94.56.187	UDP	145 10044 → 49607 Len=103	
320	05 530.885527	192.168.100.4	202.61.113.151	TCP	54 50536 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0	
320	08 530.915270	192.168.100.4	202.61.113.151	TCP	54 50536 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0	
Fram	e 3211: 74 byt	es on wire (592 bits),	74 bytes captured (	592 bits)	on interface 0	
▷ Ethe	rnet II, Src:	LiteonTe 89:c7:27 (a4:	db:30:89:c7:27), Dst	: HuaweiTe	: 2e:1f:4a (2c:55:d3:2e:1f:4a)	
⊿ Inte	rnet Protocol	Version 4, Src: 192.16	8.100.4, Dst: 192.16	8.100.1		
0:	100 = Ver:	sion: 4				
	0101 = Head	der Length: 20 bytes (	5)			
⊳ D:	ifferentiated :	Services Field: 0x00 (	DSCP: CS0, ECN: Not-	ECT)		
Te	otal Length: 6	9				
I	dentification:	0x7a29 (31273)				
⊳ F	lags: 0x00					
F	ragment offset	: 0				
T	ime to live: 1	28				
P	rotocol: UDP (	17)				
H	eader checksum	: 0x7731 [validation d	isabled]			
0	Header checksu	n status: Unverified]				
S	ource: 192.168	.100.4				
D	estination: 19	2.168.100.1				
[	Source GeoIP:	Jnknown]				
[]	Destination Ge	oIP: Unknown]				
D llser	Datagram Prot	ocol Sec Port: 50505	Det Port+ 53			
0000	2c 55 d3 2e 1f	4a a4 db 30 89 c7 27	08 00 45 00 ,U	J 0'		
0010	00 3c 7a 29 00	00 80 11 77 31 c0 a8	64 04 c0 a8 . <z).< td=""><td> w1d.</td><td></td><td></td></z).<>	w1d.		
0020	64 01 c5 49 00	35 00 28 3e 32 0c f8	01 00 00 01 d.I.	5.( >2		
0030	00 00 00 00 00 00 72 02 62 6f 6d	00 00 01 00 01	1 01 00 /0 01	w ww.kom	ipa	
0040	/5 05 05 01 0u	00 00 01 00 01	5.00			

Di kolom Internet Protocol Version 4, terlihat MAC Addres yang dimiliki adalah a4:db:30:89:c7:27, dan MAC Address router-nya adalah 2c:55:d3:2e:1f:4a. Terlihat juga kalau Panjang datanya adalah 60.

#### 2) TCP Stream & HTTP Stream

Untuk membuka TCP Stream, klik Analyze -> Follow -> TCP Stream. Web yang sedang diakses saat ini adalah <u>www.kompas.com</u> disini Browser yang digunakan adalah Mozilla Firefox. Diakses pada Rabu, 21 Februari 2018.



Pada menu tersebut data TCP Stream yang tak bisa terbaca, akan terbaca di menu TCP http seperti gambar berikut ini:



#### 3) Flow Graph dengan menggunakan Wireshark

Time	74.125.24.9	91 192.16	8.100.4	5.60.37 54.230	LiteonTe	_89:c7:27	Comment
000000	443 -	→ 50497 [ACK] Seq=1 Ack=1 Win=238 L.	1 1 1 50497				TCD: 443
020745	113	499(7)	Application Data	40			TI Sv1 2: Application Data
063679		49967	443 → 49862 [ACK] Seq=1 Ack=54 Win=34 L.	442			TCP: 443 49852 [ACK] Sen=1 Ark=54 Win=34
316436		49867	Application Data	443			TISv1.2: Application Data
366877		49002	49862 → 443 [ACK] Seq=54 Ack=33 Win=254	443			TCP: 49867
37547		5002	TCP segment of a	reassembled PDU]	- 442		TCP: [TCP segment of a reassembled PD11]
64709		50492	443 → 50492 [ACK] Seq=1 Ack=	2 Win=127 Len=0 SLE=1 SRE=2	443		TCP: 443 $\rightarrow$ 50492 [ACK] Sec=1 Ark=2 Win=12
24892		50152			10	Who has 192.168.100.1? T	ARP: Who has 192 168 100 12 Tell 192 168 100 4
48477						192.168.100.1 is at 2ct	ARP: 192.168.100.1 is at 2c:55:d3:2e:1f:4a
85971	443	Application Data	50497				TLSv1.2: Application Data
86125	443	Application Data	50497				TLSv1.2: Application Data
86377	443	Application Data	50497				TLSv1.2: Application Data
90875	443	Application Data	50497				TLSv1.2: Application Data
91009	443	Application Data	50497				TLSv1.2: Application Data
49451		50490			[TCP segment of a reassembled PDU]		TCP: [TCP segment of a reassembled PDU]
49551		50493			[TCP segment of a reassembled PDU]		TCP: [TCP segment of a reassembled PDU]
49581		50491			[TCP segment of a reassembled PDU]		TCP: [TCP segment of a reassembled PDU]
80555		50510			Continu	ation Data	SSL: Continuation Data
35650		50509				50509 → 80 [ACK] Seq=1 Ac	TCP: 50509 → 80 [ACK] Seq=1 Ack=1 Win=259
51197	443 TCP	Retransmission] 50497 → 443 [PSH, AC	50497				TCP: [TCP Retransmission] 50497 → 443 [PSH,
79456	443 -	+ 50497 [ACK] Seq=1 Ack=996 Win=250.	50497				TCP: 443 → 50497 [ACK] Seq=1 Ack=996 Win=
79463	443 -	+ 50497 [ACK] Seq=1 Ack=1742 Win=25.	50497				TCP: 443 → 50497 [ACK] Seq=1 Ack=1742 Win
79464	443 443 -	<ul> <li>50497 [ACK] Seq=1 Ack=1947 Win=26.</li> </ul>	50497				TCP: 443 → 50497 [ACK] Seq=1 Ack=1947 Win
79464	443 443 -	+ 50497 [ACK] Seq=1 Ack=2620 Win=26.	50497				TCP: 443 → 50497 [ACK] Seq=1 Ack=2620 Win:
79465	443	Application Data	50497				TLSv1.2: Application Data
79466	443	Application Data, Application Data	50497				TLSv1.2: Application Data, Application Data
79467		Application Data	59497	1	1		TLSv1.2: Application Data
dan 170 725 in							
							Add
All packets	•			How type: All Hows			Addresses: Any
							Res
							Save As Close He

1. Komputer mengirim informasi address ke router.

2. Router menerima informasi, dan akan menyampaikan data ke ISP terdekat.

3. ISP akan menanggapi permintaan user tersebut, apakah address yang dituju itu tersedia atau tidak.

4. Apabila address tesedia, maka ISP akan mengarahkan informasi tersebut ke ISP pusat.

5. ISP pusat akan menanggapi permintaan tersebut, dan informasi tanggapan akan dikirim kembali ke user.

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. Jika informasi tersebut valid, isp akan kembali mengirimkan tanggapan dan mengarahkannya ke isp pusat.

8. Jika ISP pusat menganggap informasi tersebut benar, maka akan diarahkan ke server perusahaan yang memberi ISP bandwidth. Yang mana akan di arahkan ke link server cloud berikutnya.

9. Disini situs yang diakses adalah <u>www.kompas.com</u>.

10. Seperti pada isp tadi, server pun akan mengirimkan informasi kepada user apakah address yang dituju tersebut benar atau tidak.

## 4) Perbandingan Visual Route dengan Wireshark



Gambar diatas merupakan hasil dengan menggunakan Visual Route. Aplikasi ini memiliki tampilan yang lebih sederhana disbanding Wireshark, sehingga sangat mudah untuk digunakan. Dari tes menggunakan <u>www.kompas.com</u>, terlihat jika memiliki 9 hops dan juga ditampilkan dengan grafik agar mudah dipahami.

Visualisai penggunaan Source to Destination disini sangat jelas, yaitu dari IP 192.168.56.1 sampai 202.61.113.35 . Rata-rata kecepatan akses-nya dalah 13 ms. Dan juga, web <u>www.kompas.com</u> berlokasi di Indonesia.