Nama	:	Dini Ayu Lestari
NIM	:	09031181520005
Kelas	:	SI Reguler 4A
Mata Kuliah	:	Komunikasi Data dan Jaringan Komputer
Dosen Pembimbing	:	Deris Stiawan, Ph.D

## Analisa Paket Data Menggunakan Wireshark

Wireshark merupakan salah satu tools atau aplikasi "Network Analyzer" atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk sniffing (memperoleh informasi penting seperti password email, dll). Wireshark sendiri merupakan free tools untuk Network Analyzer yang ada saat ini. Dan tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan user karena menggunakan tampilan grafis atau GUI (Graphical User Interface).

1. Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website <u>www.facebook.com</u>

<b>E</b>	facebook lagi.pcapno e Edit View Go	g Capture Analyze	Statistics Telephony Wirele	ess Tools He	lp	-	- 0	х
4		ै 🔀 🖸 🍳 👄 🤿	😫 👔 🎍 🧮 📃 Q, G	Q 🔍				
	Apply a display filter	<ctrl-></ctrl->					Expressio	n   +
No.	Time	Source	Destination	Protocol L	ength Info			^
Г	1 0.000000	157.240.7.26	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record			
	2 0.014585	157.240.7.26	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record			
	3 0.014588	157.240.7.26	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record			
4	4 0.014590	157.240.7.26	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record			-
	5 0.014768	192.168.43.83	157.240.7.26	TCP	54 58454 → 443 [ACK] Seq=1 Ack=5601 Win=388 Len=0			
	6 0.027069	192.168.43.83	157.240.7.41	TLSv1.2	407 Application Data			
	7 0.046171	157.240.7.26	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record			
	8 0.050153	157.240.7.26	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record			
	9 0.050155	157.240.7.26	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record			
	10 0.050276	192.168.43.83	157.240.7.26	TCP	54 58454 → 443 [ACK] Seq=1 Ack=9801 Win=382 Len=0			
	11 0.052064	157.240.7.26	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record			
	12 0.052182	192.168.43.83	157.240.7.26	TCP	54 58454 → 443 [ACK] Seq=1 Ack=11201 Win=382 Len=0			~
~	Internet Protoco	l Version 4 Src	192 168 43 83 Dst+ 157	240 7 26				^
	0100 = \	/ersion: 4	1921100149109, 0901 1971	24017120				
	0101 = H	leader Length: 20 b	/tes (5)					
	> Differentiate	d Services Field:	0x00 (DSCP: CS0, ECN: No	t-ECT)				
	Total Length:	40	,,	,				
	Identificatio	on: 0x4624 (17956)						
	> Flags: 0x02 (	Don't Fragment)						
	Fragment offs	set: 0						
	Time to live:	128						
	Protocol: TCF	P (6)						
	Header checks	um: 0x23a6 [valida	tion disabled]					
	[Header check	sum status: Unveri	fied]					
	Source: 192.1	168.43.83	-					
	Destination:	157.240.7.26						
	[Source GeoIF	: Unknown]						
	[Destination	GeoIP: Unknown]						~
00	00 08 3d 88 4e	7e 0c 70 8b cd 8d	dc 6d 08 00 45 00 .=.	N~.pm	E.			
00	10 00 28 46 24	40 00 80 06 23 a6	c0 a8 2b 53 9d f0 .(F	\$@ #+S				
00	20 07 1a e4 56	01 bb a3 16 13 58	d8 39 64 af 50 10	VX.9d.	P.			
00	30 01 84 43 e1	00 00	0					
	2 m//							
	<ul> <li>Differentiated</li> </ul>	Services Heid (ip.dsfield), 1	byte			Packets: 29168 ' Displayed: 29168 (100.0%) ' Load time: 0:4.749	Profi	.e: Default

Pada gambar diatas dapat diketahui bahwa **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari website yang dituju** (destination) yaitu Facebook adalah **157.240.7.26**, dikarenakan saya sudah terlebih dahulu membuka facebook dan sedang berinteraksi dihalaman tersebut, jadi pada nomor 1 sampai 4 adalah

proses ketika paket data dari facebook kembali ke PC saya, dan nomor 5 adalah request dari PC saya ke destination dengan menggunakan protocol TCP. TCP sendiri adalah suatu protokol pengiriman data yang berbasis Internet Protocol (IP) dan bersifat connection oriented.

```
✓ Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
     Interface id: 0 (\Device\NPF_{B2471995-9A2F-4AC4-BF2D-D7481A211ED9})
     Encapsulation type: Ethernet (1)
     Arrival Time: Apr 12, 2017 19:35:17.661986000 SE Asia Standard Time
     [Time shift for this packet: 0.00000000 seconds]
     Epoch Time: 1492000517.661986000 seconds
     [Time delta from previous captured frame: 0.000178000 seconds]
     [Time delta from previous displayed frame: 0.000178000 seconds]
     [Time since reference or first frame: 0.014768000 seconds]
     Frame Number: 5
     Frame Length: 54 bytes (432 bits)
     Capture Length: 54 bytes (432 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:tcp]
     [Coloring Rule Name: TCP]
     [Coloring Rule String: tcp]
```

Pada frame diatas dapat dilihat bahwa frame ke 5 ini diakses pada pukul 19:35:17 tanggal 12 April 2017 sesuai dengan standar waktu Asia karena website diakses dari negara yang merupakan bagian dari benua Asia.

```
Y Transmission Control Protocol, Src Port: 58454, Dst Port: 443, Seq: 1, Ack: 5601, Len: 0
     Source Port: 58454
     Destination Port: 443
     [Stream index: 0]
     [TCP Segment Len: 0]
     Sequence number: 1 (relative sequence number)
     Acknowledgment number: 5601 (relative ack number)
     Header Length: 20 bytes
  > Flags: 0x010 (ACK)
     Window size value: 388
     [Calculated window size: 388]
     [Window size scaling factor: -1 (unknown)]
     Checksum: 0x43e1 [unverified]
     [Checksum Status: Unverified]
     Urgent pointer: 0
   > [SEQ/ACK analysis]
```

Pada bagian trasmission control protocol ini, dapat diketahui bahwa **Source Port nya** adalah 58454 dan Destination Portnya adalah 443. Lalu dapat dilihat bahwa header length nya sebesar 20 bytes. Selain protocol TCP, terdapat juga beberapa protocol yang tercapture saat membuka website ini seperti :

	Apply a display filter	<ctrl-></ctrl->				📑 🔹 Express	ion	+
No.	Time	Source	Destination	Protocol	Length	Info	T	۸
Г	1 0.000000	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record		
	2 0.014585	157.240.7.26	192.168.43.83	TLSv1.2	1454	4 Ignored Unknown Record		
	3 0.014588	157.240.7.26	192.168.43.83	TLSv1.2	1454	4 Ignored Unknown Record		
1	4 0.014590	157.240.7.26	192.168.43.83	TLSv1.2	1454	4 Ignored Unknown Record		
	5 0.014768	192.168.43.83	157.240.7.26	TCP	54	4 58454 → 443 [ACK] Seq=1 Ack=5601 Win=388 Len=0		
	6 0.027069	192.168.43.83	157.240.7.41	TLSv1.2	407	7 Application Data		
	7 0.046171	157.240.7.26	192.168.43.83	TLSv1.2	1454	4 Ignored Unknown Record		
	8 0.050153	157.240.7.26	192.168.43.83	TLSv1.2	1454	4 Ignored Unknown Record		
	9 0.050155	157.240.7.26	192.168.43.83	TLSv1.2	1454	4 Ignored Unknown Record		
	10 0.050276	192.168.43.83	157.240.7.26	TCP	54	4 58454 → 443 [ACK] Seq=1 Ack=9801 Win=382 Len=0		
	11 0.052064	157.240.7.26	192.168.43.83	TLSv1.2	1454	4 Ignored Unknown Record		۷
۷	Ethernet II, Sro	: AsustekC_8d:dc:6d (	70:8b:cd:8d:dc:6d), Dst	: Samsung	E_4e:7	e:0c (08:3d:88:4e:7e:0c)		٨
	> Destination:	SamsungE_4e:7e:0c (08	:3d:88:4e:7e:0c)		_			
	Courses Acust	alic odidated /70.0hrs	d. 0d. da. cd\					

> Source: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d) Turner TDu4 (ouegee)

Type: IPv4 (0x0800)

Pada bagian ethernet terlihat bahwa source (**192.168.43.83**) memiliki mac address **70:8b:cd:8d:dc:6d** dan destinationnya (**157.240.7.26**) memiliki mac address **08:3d:88:4e:7e:0c**.

1	lo. Time	Source	Destination	Protocol	Length	Info	^			
	251 1.910014	157.240.7.41	192.168.43.83	TLSv1.2	628	Application Data				
	252 1.910164	192.168.43.83	157.240.7.41	TCP	54	58466 → 443 [ACK] Seq=4685 Ack=12606 Win=61 Len=0				
	253 1.917208	157.240.7.36	192.168.43.83	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message				
	254 1.917400	157.240.7.36	192.168.43.83	TLSv1.2	135	Application Data				
	255 1.917484	192.168.43.83	157.240.7.36	TCP	54	58471 → 443 [ACK] Seq=1371 Ack=3827 Win=16128 Len=0				
	256 1.917839	192.168.43.83	157.240.7.36	TLSv1.2	92	Application Data				
	257 1.928504	192.168.43.83	157.240.7.20	TCP	54	58470 → 443 [ACK] Seq=5001 Ack=4395 Win=15709 Len=0				
	258 1.949923	157.240.7.26	192.168.43.83	TLSv1.2	1454	Application Data[TCP segment of a reassembled PDU]				
	259 1.949927	157.240.7.26	192.168.43.83	TLSv1.2	1454	Application DataApplication Data, Application Data, Application Data, Application Data				
	260 1.949935	157.240.7.26	192.168.43.83	TLSv1.2	1454	Application Data[TCP segment of a reassembled PDU]	=			
	261 1.949938	157.240.7.26	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]	~			
Γ	[Next sequenc	e number: 3746	(relative sequence number)	1			^			
	Acknowledgmen	t number: 337	(relative ack number)							
	Header Length	: 20 bytes	. ,							
	Flag: Wolf (PSH, ACK)									
	Window size v	alue: 115								
	[Calculated w	indow size: 2944	.0]							
	[Window size	scaling factor:	256]							
	Checksum: 0x3	be8 [unverified]								
	[Checksum Sta	tus: Unverified]								
	Urgent pointe	r: 0								
	> [SEQ/ACK anal	ysis]								
	Secure Sockets L	ayer								
	> TLSv1.2 Recor	d Layer: Handsha	ke Protocol: New Session Tic	ket						
	> TLSv1.2 Recor	d Layer: Change	Cipher Spec Protocol: Change	Cipher Spec						
L	> TISU1 2 Decor	d Lavon Handeba	ka Doatacal, Encounted Hands	hako Moreano			¥			
Γ	0000 70 8b cd 8d	dc 6d 08 3d 88	4e 7e 0c 08 00 45 00 p	m.= .N∼E.			^			
	0010 <b>01 2a d0 80</b>	40 00 57 06 c1	3d 9d f0 07 24 c0 a8 .*@	).W=\$						
	0020 2b 53 01 bb	e4 67 c9 4e 58	65 47 f8 36 39 50 18 +S	g.N XeG.69P.						
	0030 00 73 3b e8	00 00 16 03 03	00 ca 04 00 00 c6 00 .s;							
	0040 02 33 00 00	C0 0D T5 C2 1/	ae o/ bt ic 4t 0c b9	κ0.0 ∧ ¢ #						
	0050 JC 19 20 41 0060 14 e5 2e 58	2a d9 a3 ca 28	24 00 03 23 02 10 10 2.4. 2h 10 9a 4e 5a f4 2a X*	· · · · · · · · · · · · · · · · · · ·						
	0070 53 2c 9d 55	d2 0e bd 5b 87	8e 46 81 33 a1 db 8e SU.	[F.3						
	0080 e9 03 eb e7	a3 8b 29 4c 2f	c0 b1 f2 e5 51 66 6c	.)L /Qfl			v			
	🥚 🕺 facebook lagi					Packets: 29168 · Displayed: 29168 (100.0%) · Load time: 0:2.151 Profile: D	Default			

Pada gambar diatas, yaitu pada **frame 253** terdapat **handshake** dari source 157.240.7.36 (IP address dari facebook) ke destination dengan IP address 192.168.43.83 (PC).

Selain menggunakan protokol TPC, ada juga protokol – protokol lainnya, seperti :

• HTTP

A	ply a dsplay filter <ctrl-></ctrl-> Expression +									
No.	Time	Source	Destination	Protocol	Length Info	^				
2	34 336.163581	192.168.43.83	13.107.4.50	TCP	54 58724 → 80 [ACK] Seq=5445 Ack=563134 Win=185856 Len=0					
• 2	34 336.178193	13.107.4.50	192.168.43.83	TCP	1454 [TCP segment of a reassembled PDU]					
• 2	34 336.178597	13.107.4.50	192.168.43.83	TCP	1454 [TCP segment of a reassembled PDU]					
2	34 336.178682	192.168.43.83	13.107.4.50	тср	54 58724 → 80 [ACK] Seq=5445 Ack=565934 Win=185856 Len=0					
• 2	34 336.182670	13.107.4.50	192.168.43.83	TCP	1454 [TCP segment of a reassembled PDU]					
<b>- 4</b> − 2	34 336.183131	13.107.4.50	192.168.43.83	HTTP	604 HTTP/1.1 206 Partial Content (application/octet-stream)					
2	34 336.183247	192.168.43.83	13.107.4.50	TCP	54 58724 → 80 [ACK] Seq=5445 Ack=567884 Win=185856 Len=0					
• 2	34 336.902466	192.168.43.83	13.107.4.50	HTTP	380 GET /d/msdownload/update/software/defu/2017/04/am_delta_39dbd238ca98aa89565908ebefb55ab6b6e979d4.exe HTTP/1…					
2	34 337.077245	13.107.4.50	192.168.43.83	TCP	54 80 → 58724 [ACK] Seq=567884 Ack=5771 Win=130816 Len=0					
2	34 337.079116	13.107.4.50	192.168.43.83	TCP	1454 [TCP segment of a reassembled PDU]					
2	34 337.089287	13.107.4.50	192.168.43.83	TCP	1454 [TCP segment of a reassembled PDU]					
2	34 337.089452	192.168.43.83	13.107.4.50	ТСР	54 58724 → 80 [ACK] Seq=5771 Ack=570684 Win=185856 Len=0	v				
	X-CCC: SG\r\n					٨				
	X-MSEdge-Ref:	Ref A: 048DA341C7034F	4388331099F7F0F1AE Ref	B: SG1ED	DGE0115 Ref C: Wed Apr 12 05:40:35 2017 PST\r\n					
	X-MSEdge-Ref-	OriginShield: Ref A: A	BAF440E18174B1EBD4C4A0	D18A55CC8	3 Ref B: SG2SCHEDGE0113 Ref C: Wed Apr 12 03:08:57 2017 PST\r\n					
	Date: Wed, 12	Apr 2017 12:40:35 GMT	\r\n							
	\r\n									
	[HTTP response	e 17/38]								
	[Time since r	equest: 0.296206000 se	conds]							
	[Prev request	in frame: 23255]	-							
	[Prev_respons	e in frame: 23344]								
	[Request in f	name: 23349]								
	[Next request	in frame: 23431]								
	File Data: 76	934 bytes				_				

HTTP (HyperText Transfer Protocol) adalah protocol pada layer aplikasi baik TCP/IP maupun OSI yang digunakan untuk mengakses web pages dari suatu website. Secara spesifik dalam penggunaannya banyak pada pengambilan sumber daya yang saling terhubung dengan tautan yang disebut hiperteks, yang kemudian membentuk WWW (Word Wide Web).

• DNS

[ <b>M</b> ]/H	лу а израу пісі	NUU17/2			🗾 ) uyrua	MI
No.	Time	Source	Destination	Protocol	Length Info	-
	165 1.607926	192.168.43.83	157.240.7.26	TLSv1.2	135 Application Data	
	1.636855	192.168.43.83	157.240.7.41	TCP	54 58466 → 443 [ACK] Seq=4685 Ack=11641 Win=59 Len=0	
	1.653242	203.104.174.12	192.168.43.83	TCP	54 443 → 58248 [ACK] Seq=236 Ack=28 Win=105 Len=0	
<u>ج</u> ل	168 1.653244	192.168.43.1	192.168.43.83	DNS	117 Standard query response 0x55ce A pixel.facebook.com CNAME z-m.cl0r.facebook.com A 157.240.7.36	
	1.653244	157.240.7.41	192.168.43.83	TCP	54 443 → 58466 [ACK] Seq=11641 Ack=4615 Win=263 Len=0	
	1.653367	192.168.43.83	203.104.174.12	SSL	114 Continuation Data	
	171 1.655046	157.240.7.26	192.168.43.83	TCP	54 443 → 58454 [ACK] Seq=25456 Ack=680 Win=119 Len=0	
	172 1.655048	157.240.7.26	192.168.43.83	TCP	54 443 → 58454 [ACK] Seq=25456 Ack=1219 Win=119 Len=0	
	173 1.656245	192.168.43.83	157.240.7.36	TCP	66 58471 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
	174 1.657607	157.240.7.26	192.168.43.83	TLSv1.2	96 Application Data	
	1.657906	157.240.7.26	192.168.43.83	TLSv1.2	849 Application Data	
	1.657979	192.168.43.83	157.240.7.26	TCP	54 58469 → 443 [ACK] Seq=443 Ack=12279 Win=61 Len=0	
	Canture Lengt	h: 117 bytes (936	hits)			^
	[Frame is mar	ked: Falsel	,			
	[Frame is ign	ored: False]				
	[Protocols in	frame: eth:ethert	<pre>ype:ip:udp:dns]</pre>			
	Coloring Rul	e Name: UDP]				
	[Coloring Rul	e String: udp]				
✓ Et	hernet II, Src	: SamsungE_4e:7e:0	c (08:3d:88:4e:7e:0c), Ds	t: Asustek	C_8d:dc:6d (70:8b:cd:8d:dc:6d)	
$\rightarrow$	Destination:	AsustekC_8d:dc:6d	(70:8b:cd:8d:dc:6d)			
>	Source: Samsu	ngE_4e:7e:0c (08:30	d:88:4e:7e:0c)			
	Type: IPv4 (0	x0800)				
⊻ Ir	ternet Protoco	l Version 4, Src:	192.168.43.1, Dst: 192.10	8.43.83		
	0100 = V	ersion: 4				
	0101 = H	eader Length: 20 b	ytes (5)			
>	Differentiate	d Services Field: (	0x00 (DSCP: CS0, ECN: Not	-ECT)		
	Total Length:	103				
	Identificatio	n: 0xf4d0 (62672)				V
0000	70 8b cd 8d	dc 6d 08 3d 88 4e	7e 0c 08 00 45 00 p	.m.= .N~	.E.	^

DNS (Domain Name System) adalah protocol yang digunakan untuk mentranslate hostname ke IP address dan sebaliknya. Karena di dunia manusia ini, lebih susah menghafalkan IP dibanding dengan deretan tulisan yang membentuk nama host.

Pada setiap paket data yang tercapture memiliki data – data yang berbeda mulai dari frame, ethernet, internet protocol dan lainnya.

## 2. Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website <u>www.twitter.com</u>

File Jief View Go Capute Analyz Jatitics Telephony Tools Internal: Help         Image: Source Analyz Jatitics Internal: Help         Image: Source Analyz Jati	<b>_</b> *W	i-Fi 2 [Wireshark 2	.2.4 (v2.2.4-0-gcc3dc1b)]			-	٥	×
Image: Source Action       Person:       P	<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u> <u>Statist</u>	tics Telephony <u>T</u> ools !	nternals <u>H</u> elp			
Filte         Source         Depresion Clear Apply Save           No.         Time         Source         Definition         Protocol         Length Info           10.0000000         192:168.43.83         TCP         54 6413 - 59878         LCR	0 (	ð 🛋 🔳 🔬	🖻 🗋 💥 🔁   🔍	🗇 🏟 🥥 ዥ 👱		Q. Q. 🖭   🐺 🔟 🥵 %   🛄		
No.         Time         Source         Destination         Protocl         Length Info           10.000000         192.168.43.83         TCP         54.443 ~ 59878 (AK) Seq-1.Ack-225 win-946 Len-0         10.000000         10.000000         10.000000         10.000000         10.000000         10.000000         10.000000         10.000000         10.0000000         10.0000000         10.0000000         10.0000000         10.0000000         10.0000000         10.000000000         10.000000000	Filter:				<ul> <li>Expression</li> </ul>	Clear Apply Save		
10.000000       192.166.43.83       104.115.106.104       115.V1.2       278 Client wello         30.24955       104.115.106.104       192.166.43.83       TCP       54 443 - 59878 [Ack] Seq-1 Ack-225 win-946 Len=0         40.249555       104.115.106.104       192.166.43.83       TCP       54 9878 - 443 [Ack] Seq-225 Ack-280 win-1024 Len=0         60.257079       104.115.106.104       172.168.43.83       TCP       54 9878 - 443 [Ack] Seq-225 Ack-280 win-1024 Len=0         70.251825       192.168.43.83       104.115.106.104       TCP       54 59878 - 443 [Ack] Seq-225 Ack-362 win-1024 Len=0         80.50227       192.168.43.83       104.115.106.104       TCV       54 59878 - 443 [Ack] Seq-225 Ack-362 win-1024 Len=0         90.504020       192.168.43.83       104.115.106.104       TCV.2       813 Application Data         100.677981       192.168.43.83       104.115.106.104       TCV.2       813 Application Data         100.677981       192.168.43.83       112.15.184.49       012       132 Client wello.PKK: Clange Clipher Spec, Encrypted Handshake Message         110.677981       192.168.43.83       102.168.43.83       112.215.184.49       012 Client wello.PKK: Client Well	No.	Time	Source	Destination	Protocol	Length Info		~
2 0.24938 104.115.106.104 192.165.43.83 TCP 54 443 - 59878 [Ack] Seq-1 Ack-225 wih-946 tem=0 3 0.24936 104.115.106.104 192.165.43.83 TCP 1454 [TCP segment of a reassembled PoU] 4 0.24956 104.115.106.104 192.165.43.83 TCP 1454 [TCP segment of a reassembled PoU] 5 0.24968 192.166.43.83 104.115.106.104 TCP 54 59876 - 443 [Ack] Seq-25 Ack-2601 wih-1024 Len=0 6 0.25170 104.115.106.104 192.165.43.83 TCP 1454 [TCP segment of a reassembled PoU] 7 0.25122 192.166.43.83 104.115.106.104 TCP 54 59876 - 443 [Ack] Seq-25 Ack-2602 wih-1020 Len=0 8 0.502577 192.166.43.83 104.115.106.104 TCP 54 59876 - 443 [Ack] Seq-25 Ack-2602 wih-1020 Len=0 8 0.502577 192.166.43.83 104.115.106.104 TCP 24 15378 - 443 [Ack] Seq-25 Ack-2602 wih-1020 Len=0 10 0.577981 192.166.43.83 104.115.106.104 TCP 25 35878 - 443 [Ack] Seq-110 Ack-3920 wih-1019 Len=0 11 0.577981 193.166.43.83 104.115.106.104 TCP 25 35878 - 443 [Ack] Seq-110 Ack-3920 wih-1019 Len=0 12 0.57187 192.166.43.83 104.115.106.104 TCP 25 35878 - 443 [Ack] Seq-110 Ack-3920 wih-1019 Len=0 13 0.75987 192.166.43.83 104.115.106.104 TCP 25 35878 - 443 [Ack] Seq-110 Ack-3920 wih-1019 Len=0 13 0.75987 192.166.43.83 104.115.106.104 TCP 25 35878 - 443 [Ack] Seq-110 Ack-3920 wih-1019 Len=0 14 0.757981 192.166.43.83 104.115.106.104 TCP 25 35878 - 443 [Ack] Seq-110 Ack-3920 wih-1019 Len=0 14 0.757981 192.166.43.83 104.115.106.104 TCP 25 35878 - 443 [Ack] Seq-110 Ack-3920 wih-1019 Len=0 14 0.757981 192.166.43.83 104.115.106.104 TCP 25 35878 - 443 [Ack] Seq-110 Ack-3920 wih-1019 Len=0 14 0.75781 192.166.43.83 104.115.106.104 TCP 25 3597 142.1578 15 PCan Time is 220 115.33 104.115.106.104 TCP 25 3597 142.100 1132 Clinet Hello, PKH.1, 1CH 55119205 PSH.2 16 PCan Time is 2402077.1959.2027 44.4820.2000000 seconds] 17 Time is 4202077.1959.2027 44.4820.2000000 seconds] 17 Time is apacket r.0182 PCTNH2 PSH.224 Dits) 17 Time is figure of the fise Implement is 100000000 seconds] 18 PCan Extended Tender PCH.2 19 PCAN PSH.2 10 PCAN 2 10 PCAN PSH.2 10 PCAN PSH.2 10 PCAN 2 10 PCAN PSH.2		1 0.000000	192.168.43.83	104.118.106.104	TLSV1.2	278 Client Hello		
3 0.249565 104.118.106.104 192.168.43.83 TLSV1.2 1454 Server Hello 4 0.249565 104.118.106.104 192.168.43.83 TLSV1.2 1454 Server Hello 5 0.249681 192.168.43.83 104.118.106.104 TCP 54 59878 - 443 [Ack] Seq=25 Ack-2801 win=1024 Len-0 6 0.55709 104.118.106.104 192.168.43.83 TLSV1.2 95 CertificateServer Key Exchange Server Hello Done 7 0.551825 192.168.43.83 104.118.106.104 TCV 54 59878 - 443 [Ack] Seq=25 Ack-3662 win=1020 Len-0 8 0.50257 192.168.43.83 104.118.106.104 TLSV1.2 180 Client Key Exchange, Change Clipher Spec, Encrypted Handshake Message 10 0.677861 104.118.106.104 112.105.143.83 TLSV1.2 112 New Session Ticket, Change Clipher Spec, Encrypted Handshake Message 11 0.677981 192.168.43.83 104.118.106.104 TLSV1.2 112 New Session Ticket, Change Clipher Spec, Encrypted Handshake Message 11 0.677981 192.168.43.83 104.118.106.104 TLSV1.2 112 New Session Ticket, Change Clipher Spec, Encrypted Handshake Message 11 0.677981 192.168.43.83 104.118.106.104 TLSV1.2 112 New Session Ticket, Change Clipher Spec, Encrypted Handshake Message 11 0.758987 192.168.43.83 104.118.106.104 TLSV1.2 112 New Session Ticket, Change Clipher Spec, Hello Request 9 Crashing 192.168.43.83 104.118.106.104 TLSV1.2 1132 Client Hello, PMK: 1, CID: 65119223511424190 11 0.75987 192.168.43.83 104.118.106.104 TCP 192.21391.10 Ack=3920 Win=1019 Len=0 12 0.751187 192.168.43.83 104.212.15.144.99 QUC 1392 Client Hello, PMK: 1, CID: 651192235114.0424190 13 0.75987 192.168.43.83 104.212.15.144.99 QUC 1392 Client Hello, PMK: 1, CID: 6511922353114.0421490 14 0.7512 PLSVES ON UNIC Q242 Hiss) ON Interface 0 11 Thereface 10 (New/Ice/WPF.[02471905-9A2F-4A24-BF2D-D7481A211ED9]) Propertient orge First Frame: 0.000000000 seconds] Frame Number: 1 Frame Number: 1 Frame Kumber: 7P] Coloring Rule Name: TCP] Coloring Rule Name:		2 0.249381	104.118.106.104	192.168.43.83	TCP	54 443 → 59878 [ACK] seq=1 Ack=225 Win=946 Len=0		
4 0.249568       104.118.106.104       192.168.43.83       TCP       1454       [TCP segment of a reassembled POU]         5 0.249568       194.118.106.104       192.168.43.83       TLSN1.2       915 Certificateserver Key Exchange, Server Hello Done         7 0.25128       192.168.43.83       104.118.106.104       TLSN1.2       915 Certificateserver Key Exchange, Server Hello Done         8 0.502327       192.168.43.83       104.118.106.104       TLSN1.2       813 Application Data         10 0.677801       104.118.106.104       TLSN1.2       813 Application Data         10 0.677801       104.118.106.104       TLSN1.2       813 Application Data         11 0.677801       104.118.106.104       TLSN1.2       813 Application Data         12 0.753187       192.168.43.83       112.215.184.49       QUIC       1392 Client Hello, PKN:1, CID: 6531392235311764190         13 0.759887       192.168.43.83       112.215.184.49       QUIC       1392 Client Hello, PKN:1, CID: 653139223531764190         13 0.759887       192.168.43.83       102.168.43.83       103.125.184.49       QUIC       1392 Client Hello, PKN:1, CID: 653139223531764190         13 0.759887       192.168.43.83       102.168.43.83       103.168.43.83       103.125.184.49       QUIC       1392 Client Hello, PKN:1, CID: 65313922531764190         13 0.759		3 0.249565	104.118.106.104	192.168.43.83	TLSV1.2	1454 Server Hello		
50.249681       192.168.43.83       104.118.106.104       TCP       54 59878 - 443 [ack] seq-225 ack-280 imin-1024 Lem-0         60.25270       192.168.43.83       104.118.106.104       TCP       54 59878 - 443 [ack] seq-225 ack-2662 win-1020 Lem-0         80.502527       192.168.43.83       104.118.106.104       TLSV.2       115 application pata         90.504020       192.168.43.83       104.118.106.104       TLSV.2       120 application pata         90.504020       192.168.43.83       104.118.106.104       TLSV.2       130 application pata         10.677981       192.168.43.83       104.118.106.104       TLSV.2       130 application pata         12.075187       192.168.43.83       104.118.106.104       TCP       54 59878 - 443 [ack] seq-110 ack-3920 win=1019 Lem-0         12.075181       192.168.43.83       104.118.106.104       TCP       54 59878 - 443 [ack] seq-110 ack-3920 win=1019 Lem-0         13.0.759867       192.168.43.83       112.215.184.49       QUIC       139 Client Hello, PRC121 Application pata       130 application pata         13.0.759867       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.83       192.168.43.		4 0.249568	104.118.106.104	192.168.43.83	TCP	1454 [TCP segment of a reassembled PDU]		
6 0.231709       104.118.106.104       192.168.43.83       TLSVL.2       915 CertificateServer Key Exchange, Server Hello Done         7 0.231825       192.168.43.83       104.118.106.104       TLSVL.2       180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request         9 0.50420       192.168.43.83       104.118.106.104       TLSVL.2       180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request         10 0.677801       104.118.106.104       125.12       312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message         11 0.677801       104.118.106.104       125.125.184.49       QUIC       1392 Client Hello, PKH: 1, CID: 6531192253511764190         13 0.75807       102.168.43.83       112.157.84.49       QUIC       1392 Client Hello, PKH: 1, CID: 6531192253511764190         13 0.75807       102.168.43.83       112.162.43.1       DNS       75 Standard query Outfold A muttifyer Spect.com         14 0.751040       102.158.42       92       103 158.25       DN THERES       DN THERES         13 0.75807       102.168.43.83       112.167.443.10       DN THERES       DN THERES       DN THERES         13 0.75807       102.168.43.83       112.158.144.9       QUIC       1392 Client Hello, PKH: 1, CID: 6531192253511764190       DN THERES         13 0.758078       102.168.43.83       102.168.43.83 </td <td></td> <td>5 0.249681</td> <td>192.168.43.83</td> <td>104.118.106.104</td> <td>TCP</td> <td>54 59878 - 443 [ACK] Seq=225 Ack=2801 Win=1024 Len=0</td> <td></td> <td></td>		5 0.249681	192.168.43.83	104.118.106.104	TCP	54 59878 - 443 [ACK] Seq=225 Ack=2801 Win=1024 Len=0		
7 0.251825       192.168.43.83       104.118.106.104       TCP       54 59878 - 443 [ACK] Seq=225 ACK=3602 Win=1020 Len=0         8 0.50227       192.168.43.83       104.118.106.104       TLSV.1.2       183 Application Data         9 0.504020       192.168.43.83       104.118.106.104       TLSV.1.2       183 Application Data         10 0.67780       104.118.106.104       TCV.2       183 Application Data       103 Application Data         11 0.67780       104.118.106.104       TCP       54 59878 - 443 [ACK] Seq=1110 AcK=3290 Win=1019 Len=0         12 0.75187       192.168.43.83       112.215.148.449       QUIC       1392 Client Hello, PKK:1, CID: 6531192253511764190         13 0.758987       192.168.43.83       192.168.43.1       DNS       77 Standard query Oxb0b0 A fonts.gstatic.com         14 0.75180       192.168.43.83       192.168.43.10       DNS       77 Standard query Oxb0b0 A fonts.gstatic.com         14 0.75180       192.168.43.83       192.168.43.11       DNS       77 Standard query Oxb0b0 A fonts.gstatic.com         14 0.75180       192.168.43.83       192.168.43.10       DNS       77 Standard query Oxb0b0 A fonts.gstatic.com         14 0.75180       192.168.43.81       192.168.43.10       DNS       77 Standard query Oxb0b0 A fonts.gstatic.com         12 0.751817       192.168.43.80       192.		6 0.251709	104.118.106.104	192.168.43.83	TLSV1.2	915 CertificateServer Key Exchange, Server Hello Done		
8 0.502327       192.168.43.83       104.118.106.104       TLSV.1.2       180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request         9 0.50420       192.168.43.83       104.118.106.104       192.168.43.83       TLSV.1.2       312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message         11 0.677801       102.168.43.83       112.15.184.49       QUIC       1392 Client Hello, PKN: 1, CD: 6531132253511764190         13 0.759807       192.168.43.83       112.15.184.49       QUIC       1392 Client Hello, PKN: 1, CD: 6531132253511764190         14 0.751040       102 158.42       92       103 168 792 Client Hello, PKN: 1, CD: 6531132253511764190         13 0.759807       192.168.43.83       112.168.43.1       DNS       77 Standard Query Oxt6321 a perifications acould com         14 0.751040       103 158 42 92       103 168 92 91       158 ytes captured (2224 bits) on interface 0       Interface 0         Interface id: 0 (Newice/WPF_[82471995-9A2F-4A2C-AF20P-O7481A211E09])       Interface 0       Interface 0       Interface 0         Interface id: 0 (Nowice Captured (224 bits)       728 bytes (000000 seconds]       If meessatis       If manual acould com       If manual acould com         If indelta from previous captured frame: 0.000000000 seconds]       If meessatis       If meessatis       If meessatis       If meessatis       If meessatis       If meess		7 0.251825	192.168.43.83	104.118.106.104	TCP	54 59878 → 443 [ACK] seq=225 ACk=3662 Win=1020 Len=0		
9 0.304020 192.168.43.83 104.118.106.104 TLSVL2 813 Application Data 10 0.67780 104.118.106.104 192.168.43.83 TLSVL2 312 New Session Ticket, change Cipher Spec, Encrypted Handshake Message 11 0.67780 1192.168.43.83 104.118.106.104 TCP 54 59878 - 443 [AcK] Seq=1110 AcK-3920 Win=1019 Len-0 12 0.75187 192.168.43.83 102.115.184.49 QUIC 1392 Cilent Hello, PKK: 1, CID: 6531192253511764190 13 0.75988 192.168.43.83 192.168.43.1 DNS 77 Standard query 0xbbb0 A forts.gstatic.com 14 0.7501 104.118 102.108.43.83 192.168.43.1 DNS 77 Standard query 0xbbb0 A forts.gstatic.com 14 0.75184 192.186.43.83 192.168.43.1 DNS 77 Standard query 0xbbb0 A forts.gstatic.com 14 0.75184 192.186.43.83 192.168.43.1 DNS 77 Standard query 0xbbb0 A forts.gstatic.com 14 0.75701 104.118 106.104 Hell A fort Distribution for the statistic of		8 0.502527	192.168.43.83	104.118.106.104	TLSV1.2	180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request		
10       0.677801       104.118.106.104       192.168.43.83       TLSVL.2       312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message         12       0.75781       192.168.43.83       112.215.184.49       QUIC       1392 Client Hello, PKN: 1, CD: 6531192235311764190         13       0.75887       192.168.43.83       112.215.184.49       QUIC       1392 Client Hello, PKN: 1, CD: 6531192235311764190         13       0.75887       192.168.43.83       112.215.184.49       QUIC       1392 Client Hello, PKN: 1, CD: 6531192235311764190         14       0.751487       102.168.43.83       112.215.184.49       QUIC       1392 Client Hello, PKN: 1, CD: 6531192235311764190         14       0.751487       102.168.43.83       112.64.21       DNS       77 Standard query Oxt621 4 partifications could com         14       0.751487       102.168.43.83       112.64.21       DNS       77 Standard query Oxt621 4 partifications could com         17       DS887       102.168.43.83       102.168.43.83       100.0000000 seconds]       Time charts packet: 0.000000000 seconds]         17       Ifme delta from previous captured (224 bits)       Capture Length: 278 bytes (224 bits)       Capture Length: 278 bytes (224 bits)         Capture Length: 278 bytes (224 bits)       Frame Length: 278 bytes (224 bits)       Frame Length: 278 bytes (224 bits)		9 0.504020	192.168.43.83	104.118.106.104	TLSV1.2	813 Application Data		
11 0.0/7981       192.108.43.83       104.118.106.104       TCP       54.598/8       104.118.106.114       TCP       53.11225511766119       TCP       53.11225511766119       TCP       53.11225511766119       TCP       53.11225511766119       TCP       TCP       54.598/8       TCP       TCP       54.598/8       TCP       53.11225511766119       TCP       TCP       TCP       TCP       54.598/8       TCP       TCP       54.598/8       TCP       TCP       TCP       54.598/8       TCP       TCP       TCP       TCP       54.598/8       TCP <t< td=""><td></td><td>10 0.677801</td><td>104.118.106.104</td><td>192.168.43.83</td><td>TLSV1.2</td><td>312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message</td><td></td><td></td></t<>		10 0.677801	104.118.106.104	192.168.43.83	TLSV1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message		
120.7518/192.108.43.83       112.715.184.43       QUIC       139.210.1192       139.2108.43.83       112.715.1184.43       QUIC       139.210.1192         130.7588/7       192.108.43.83       112.715.1184.11       DNS       77 Standard query Oxbb0A for Chris.static.com       140.757.010         140.7588/7       102.108.43.83       112.75.1184.11       DNS       77 Standard query Oxbb0A for Chris.static.com       140.757.010         140.758/010       100.152.42.02       bits, 7.75 Bytes captured (2224 bits) on interface 0       110.757.000       140.757.000         1110.778       27.850/10.000       0.00000000 seconds]       1110.110       1110.110       1110.110         11111.778       12.201.711.78800000 seconds]       11110.110       1111.711       1111.711       1111.711         11111.778       14.721.711.810.01.711.711       0.00000000 seconds]       11111.711       1111.7111       1111.711       1111111		11 0.6//981	192.168.43.83	104.118.106.104	TCP	54 598/8 → 443 [ACK] Seq=1110 ACK=3920 W1n=1019 Len=0		
130.75898/ 192.108.43.83       192.108.43.1       DNS       // Standard query 0x0000 A fonts.gstatc.com         140.75018/102.108.43.83       100.108.91.100       100.108.91.100       100.108.91.100       100.108.91.100         180.750898/ 192.108.43.83       100.108.91.100       100.108.91.100       100.108.91.100       100.108.91.100         180.750898/ 192.108.43.83       100.108.91.100       100.108.91.100       100.108.91.100       100.108.91.100         180.750898/ 192.108.43.83       100.108.91.100       100.108.91.100       100.108.91.100       100.108.91.100         180.750898/ 192.108.43.83       100.108.91.100       100.108.91.100       100.108.91.100       100.108.91.100         180.7508.91.100       100.108.91.100       100.108.91.100       100.108.91.100       100.108.91.100       100.108.91.100         180.7508.91.100.100.91.1		12 0.751187	192.168.43.83	112.215.184.49	QUIC	1392 Client Hello, PKN: 1, CID: 6531192253511/64190		
Prame 1: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface 0 Interface 1d: 0 (\Device\wFr_[62471995-9A2F-4Ac4-B2D-0781A211E09]) Encapsulation type: Ethernet (1) Arrival Time: Apr 12, 2017 21:36:01.478800000 Se Asia Standard Time [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1492007761.478800000 seconds] [Time delta from previous displayed frame: 0.000000000 seconds] [Time delta from previous displayed frame: 0.000000000 seconds] [Time delta from previous displayed frame: 0.000000000 seconds] [Time shift for this: 1 Frame Length: 278 bytes (2224 bits) Capture Length: 278 bytes (2224 bits) [Frame is marked: False] [Frame is ingrored: False] [Frame is ingrored: False] [Frame is ingrored: False] [Frame is displayed frame: the:thertype:ip:tcp:ssl] [Coloring Rule Name: TCP] [Coloring Rule Name: TCP] [Coloring Rule Name: TCP] [Coloring Rule Name: TCP] [Coloring Rule String: 1 48 20 00 00 00 00 00 00 00 00 00 00 00 00		13 0.758987	192.168.43.83	192.168.43.1	DNS	// Standard query Oxbbb0 A fonts.gstatic.com		~
P Hame 1. 278 bytes of wire (224 bits) (758 bytes (224 bits) (778 bytes) (244 bits) (778 bytes) (224 bits) (788 bytes) (788 bytes) (224 bits) (788 bytes) (78	0.50	amo 1 : 279 b	stor on wine (2224	hitc) 378 but of a	antuned (22	Va standard Jorry Jorry a potatacations doodla com		
0000       08 3d 88 4e 7e 0c 70 8b cd 8d dc 6d 08 00 45 00      NpmE.         0010       01 08 01 cc 40 00 80 06 39 4a c0 a8 2b 53 68 7c      epmE.         0020       6a 8e 9e 60 1b b8 c1 a8 37 01 2d 66 5c 50 18       911 7P.P.         0030       04 00 d1 8e 00 00 16 03 03 00 db 01 00 00 d7 03		Interface id Encapsulatio Arrival Time Time shift: poch Time: Time delta Time delta Time since Frame Number Frame Leng Frame is ng [Prane is ng [Protocols i [Coloring Ru	: 0 (\Device\VPF_[6] : yor 12, 2017 21:3 for this packet: 0. 1492007761.47880000 from previous captu from previous captu from previous captu from previous captu from the form of first : 278 bytes (2224 b th: 278 bytes (2224 b) th: 278 bytes (2224 b th: 278 bytes (2224 b) th: 278 bytes (2224 b th: 278 bytes (2224 b) th: 278 bytes (224 b) th: 278 b) th: 278 bytes (224 b) th: 278 bytes (224 b) th: 278 b) th: 27	2471995-9027-4Ac4- ) 6:01.478800000 se 000000000 seconds] 00 seconds 100 seconds read frame: 0.0000 ayed frame: 0.0000 frame: 0.000000000 htts) bits) ype:1p:tcp:ss1]	BF2D-D7481A Asia Standa 0000 second 00000 secon seconds]	211E09}) rd Time s] ds]		
0010         01         05         01         01         05         01         01         05         01         01         05         01         01         05         01         01         05         01         01         05         01         01         05         01         01         01         01         01         01         01         01         01         01         01         01         01         01         01         01         01         01         01         0	0000	08 24 88 4	o Zo Oc ZO Sh cd S	d dc 6d 08 00 45 0				
	0010 0020 0030 0040	01 08 01 c 6a 68 e9 e 04 00 d1 8 03 58 ee 3	c 40 00 80 06 39 4 c 40 00 80 06 39 4 6 01 bb 8c 31 89 3 e 00 00 16 03 03 0 b 51 d8 c2 0d 0c 2	a c0 a8 2b 53 68 7 7 01 2d 66 5c 50 1 0 db 01 00 00 d7 0 c 9c bf f5 84 a7 7 8 d0 10 bb c7 65 8	6@ 8 jh f .x.;Q	9) +Siv 1 . 7F\P.		^
	0050		7 02 00 ee DC ae D	Bashata 14465 Disalara	H 14455 (100 08/	Durfler Defeute		~

Pada gambar diatas dapat diketahui bahwa frame pertama memiliki **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari halaman yang dituju (destination)** yaitu Twitter adalah **104.118.106.104**. Pada frame 1 adalah request dari PC saya ke destination dan pada frame 2,3 dan 4 adalah respon dari website yang dituju tadi kembali ke PC yang saya gunakan.

```
□ Frame 1: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface 0
    Interface id: 0 (\Device\NPF_{B2471995-9A2F-4AC4-BF2D-D7481A211ED9})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 12, 2017 21:36:01.478800000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1492007761.478800000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 278 bytes (2224 bits)
    Capture Length: 278 bytes (2224 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ss]]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
```

Pada frame diatas dapat dilihat bahwa frame ke 1 ini diakses pada pukul 21:36:01 tanggal 12 April 2017 sesuai dengan standar waktu Asia karena website diakses dari negara yang merupakan bagian dari benua Asia.

No.	Time	Source	Destination	Protocol	Length Info	$\wedge$
	1 0.000000	192.168.43.83	104.118.106.104	TLSv1.2	278 Client Hello	
	2 0.249381	104.118.106.104	192.168.43.83	ТСР	54 443 → 59878 [ACK] Seq=1 Ack=225 win=946 Len=0	
	3 0.249565	104.118.106.104	192.168.43.83	TLSV1.2	1454 Server Hello	<u> </u>
	4 0.249568	104.118.106.104	192.168.43.83	TCP	1454 [TCP segment of a reassembled PDU]	
	5 0.249681	192.168.43.83	104.118.106.104	TCP	54 59878 → 443 [ACK] Seq=225 Ack=2801 Win=1024 Len=0	
	6 0.251709	104.118.106.104	192.168.43.83	TLSV1.2	915 CertificateServer Key Exchange, Server Hello Done	
	7 0.251825	192.168.43.83	104.118.106.104	ТСР	54 59878 → 443 [ACK] Seq=225 Ack=3662 Win=1020 Len=0	
	8 0.502527	192.168.43.83	104.118.106.104	TLSV1.2	180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request	
	9 0.504020	192.168.43.83	104.118.106.104	TLSv1.2	813 Application Data	
	10 0.677801	104.118.106.104	192.168.43.83	TLSV1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
	11 0.677981	192.168.43.83	104.118.106.104	ТСР	54 59878 → 443 [ACK] Seq=1110 Ack=3920 Win=1019 Len=0	
	12 0.751187	192.168.43.83	112.215.184.49	QUIC	1392 Client Hello, PKN: 1, CID: 6531192253511764190	
	13 0.758987	192.168.43.83	192.168.43.1	DNS	77 Standard query OxbbbO A fonts.gstatic.com	
	1/ 0 7610/0	100 160 /0 00	100 160 /0 1	DMC	RA Standard quory OxeO21 A notifications google com	×
Ξ.	ransmission C	ontrol Protocol, Sr	c Port: 443, Dst Por	rt: 59878,	Seq: 1, Ack: 225, Len: 0	^
	Source Port:	443				
	Destination I	Port: 59878				
	[Stream inde	x: 0]				
	[TCP Segment	Len: 0]				
	Sequence num	ber:1 (relative	sequence number)			
	Acknowledgme	nt number: 225 (I	relative ack number)	)		
	Header Lengt	h: 20 bytes				
1	-	-				

Untuk frame kedua ini, IP address dari source nya adalah 104.118.106.104 (twitter) dan IP address destination nya adalah 192.168.43.83 (PC) , frame kedua ini merupakan respon dari frame 1 yang mana frame 1 adalah request ketika PC mengirimkan paket ke destination. Frame kedua ini menggunakan protokol TCP yang mana Source Portnya dalah 443 dan Destination Port nya 59878.

No.	Time	Source	Destination	Protocol	Length Info	$\wedge$
	1 0.000000	192.168.43.83	104.118.106.104	TLSV1.2	278 Client Hello	
	2 0.249381	104.118.106.104	192.168.43.83	ТСР	54 443 → 59878 [ACK] Seq=1 Ack=225 Win=946 Len=0	
	3 0.249565	104.118.106.104	192.168.43.83	TLSV1.2	1454 Server Hello	
	4 0.249568	104.118.106.104	192.168.43.83	TCP	1454 [TCP segment of a reassembled PDU]	
	5 0.249681	192.168.43.83	104.118.106.104	TCP	54 59878 → 443 [ACK] Seq=225 Ack=2801 Win=1024 Len=0	
	6 0.251709	104.118.106.104	192.168.43.83	TLSV1.2	915 CertificateServer Key Exchange, Server Hello Done	
	7 0.251825	192.168.43.83	104.118.106.104	TCP	54 59878 → 443 [ACK] Seq=225 Ack=3662 Win=1020 Len=0	
	8 0.502527	192.168.43.83	104.118.106.104	TLSV1.2	180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request	
	9 0.504020	192.168.43.83	104.118.106.104	TLSV1.2	813 Application Data	
	10 0.677801	104.118.106.104	192.168.43.83	TLSV1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
	11 0.677981	192.168.43.83	104.118.106.104	тср	54 59878 → 443 [ACK] Seq=1110 Ack=3920 Win=1019 Len=0	
	12 0.751187	192.168.43.83	112.215.184.49	QUIC	1392 Client Hello, PKN: 1, CID: 6531192253511764190	
	13 0.758987	192.168.43.83	192.168.43.1	DNS	77 Standard query OxbbbO A fonts.gstatic.com	
	1/ 0 7610/0	107 160 /2 02	100 160 /0 1	DMC	PA Standard quary OveOD1 A notifications google com	Y
	[Coloring Ru	le String: tcp]				٨
	thernet II, S	c: SamsungE_4e:7e:	Oc (08:3d:88:4e:7e:0	)c), Dst:/	AsustekC_8d:dc:6d (70:8b:cd:8d:dc:6d)	
6	Destination:	AsustekC_8d:dc:6d	(70:8b:cd:8d:dc:6d)			
6	Source: Sams	ungE_4e:7e:0c (08:3	d:88:4e:7e:0c)			
	Type: IPv4 (	)x0800)				

B Source: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c) Type: IPv4 (0x0800)

Pada bagian ethernet terlihat bahwa source (104.118.106.104) memiliki mac address 08:3d:88:4e:7e:0c dan destinationnya (192.168.43.83) memiliki mac address 70:8b:cd:8d:dc:6d.

N	o. Time	Source	Destination	Protocol	Length	Info	~
ſ	1 0.000000	192.168.43.83	104.118.106.104	TLSv1.2	278	8 Client Hello	
	2 0.249381	104.118.106.104	192.168.43.83	TCP	54	4 443 → 59878 [ACK] Seq=1 Ack=225 Win=946 Len=0	
	3 0.249565	104.118.106.104	192.168.43.83	TLSv1.2	1454	4 Server Hello	
	4 0.249568	104.118.106.104	192.168.43.83	TCP	1454	4 [TCP segment of a reassembled PDU]	
	5 0.249681	192.168.43.83	104.118.106.104	TCP	54	4 59878 → 443 [ACK] Seq=225 Ack=2801 Win=1024 Len=0	
	6 0.251709	104.118.106.104	192.168.43.83	TLSv1.2	915	5 CertificateServer Key Exchange, Server Hello Done	
	7 0.251825	192.168.43.83	104.118.106.104	TCP	54	4 59878 → 443 [ACK] Seq=225 Ack=3662 Win=1020 Len=0	
~	8 0.502527	192.168.43.83	104.118.106.104	TLSv1.2	180	0 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request	
	9 0.504020	192.168.43.83	104.118.106.104	TLSv1.2	813	3 Application Data	
	10 0.677801	104.118.106.104	192.168.43.83	TLSv1.2	312	2 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
	11 0.677981	192.168.43.83	104.118.106.104	TCP	54	4 59878 → 443 [ACK] Seq=1110 Ack=3920 Win=1019 Len=0	<b>—</b> •
Γ	Frame Length:	312 bytes (2496 bits	.)				^
	Capture Lengt	h: 312 bytes (2496 bi	ts)				
	[Frame is mar	ked: False]					
	[Frame is ign	ored: False]					
	[Protocols in	frame: eth:ethertype	:ip:tcp:ssl]				
	[Coloring Rul	e Name: TCP]					
	[Coloring Rul	e String: tcp]					
)	Ethernet II, Src	: SamsungE_4e:7e:0c	08:3d:88:4e:7e:0c), D	st: AsustekC_	8d:dc:6	5d (70:8b:cd:8d:dc:6d)	
3	Internet Protoco	l Version 4, Src: 104	.118.106.104, Dst: 19	2.168.43.83			
)	Transmission Con	trol Protocol, Src Po	ort: 443, Dst Port: 59	878, Seq: 366	2, Ack:	: 351, Len: 258	
	Secure Sockets L	ayer					
	> TLSv1.2 Recon	d Layer: Handshake Pr	otocol: New Session T	icket			
	> TLSv1.2 Recon	d Layer: Change Ciphe	r Spec Protocol: Chan	ge Cipher Spe	c		
	> TLSv1.2 Recon	d Layer: Handshake Pr	otocol: Encrypted Han	dshake Message	e		
							*
0	000 70 8b cd 8d	dc 6d 08 3d 88 4e 7e	0c 08 00 45 00 p		•		^
0	010 01 2a 61 16	40 00 30 06 1e de 68	76 6a 68 C0 a8 .*a	@.;nvjn.	•		
6	1020 20 55 01 00 1	e9 e6 01 20 74 d9 60 00 00 16 03 03 00 ca	04 00 00 c6 00 F5.	····- (···I··P			
6	040 00 1c 20 00	c0 00 00 07 6a 44 cd	83 3e 1d 63 cf	iD			
6	050 5a f2 69 a7	84 23 41 d6 23 90 f4	09 bc 4a f7 b3 Z.i	#A. #J.			
(	060 9d 43 16 be	52 0e b1 be dd 1d co	ff 3b 0a 05 4e .C.	.R;	N		
(	070 3a 1b 40 4e	96 17 90 49 7e b2 3b	e5 dd eb 5e 5f :.@	NI ~.;^	_		
(	080 a3 e5 64 aa	7b 9e 1e 32 15 ed 5e	ee 45 fb 84 46d	.{2^.E	F		¥
1	🗎 🏋 🛛 Frame is ignored	d hv the dissectors (frame.ion	ored)			Parkets: 14465 • Displayed: 14465 (100.0%) • Load time: 0:2.240	Profile: Default

Pada gambar diatas, yaitu pada **frame 10** terdapat **handshake** dari source 104.118.106.104 (IP address dari twitter) ke destination dengan IP address 192.168.43.83 (PC). Pada frame ke 9, 192.168.43.83 melakukan request kedestinationnya yaitu 104.118.106.104 kemudian ada respon dari 104.118.106.104 kembali ke IP address dari PC yang digunakan. 3. Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website <u>www.detik.com</u>

No. 720	Time	Source	Destination	Protocol	Length	Info	^
730	5 00 702564	192.168.43.83	216 58 221 66	OUTC	77	(044 - 45 [ACK] SQ(44) ACCOUNT #12552 Color	
739	6 99,801351	203.190.242.59	192,168,43,83	ТСР	66	TOP Dun ACK 7350#1 443 → 60450 [ACK] Seg=153 Ark=518 win=15872 Len=0 SLE=1 SRE=518	i.
739	7 99,820428	192,168,43,83	203, 190, 242, 59	TLSV1.2	1114	Application Data	ť
739	8 99.826879	192.168.43.83	74.125.68.154	QUIC	1392	Client Hello, PKN: 1, CID: 4755907082276700669	1
739	9 99.828389	192.168.43.83	74.125.68.154	QUIC	422	2 Payload (Encrypted), PKN: 2, CID: 4755907082276700669	
740	0 99.839368	203.190.242.59	192.168.43.83	TLSV1.2	1454	Ignored Unknown Record	
740	1 99.839747	203.190.242.59	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record	
740	2 99.839830	192.168.43.83	203.190.242.59	TCP	54	↓ 60444 → 443 [ACK] Seq=4450 Ack=89571 Win=25088 Len=0	
740	3 99.843615	203.190.242.59	192.168.43.83	TLSv1.2	1454	I Ignored Unknown Record	
740	4 99.843893	203.190.242.59	192.168.43.83	TLSV1.2	1454	Ignored Unknown Record	
740	5 99.843896	203.190.242.59	192.168.43.83	TLSv1.2	1321	1 Ignored Unknown Record	
740	6 99.843972	192.168.43.83	203.190.242.59	тср	54	↓ 60444 → 443 [ACK] Seq=4450 Ack=93638 win=25088 Len=0	í.,
740	7 99 844259	203 190 241 95	192 168 43 83	тср	380	TCP Retransmission] 443 → 60447 [PSH _ACK] Sen=2801_Ack=208_Win=15872_Len=326	1 1
🖃 Fran	ne 7398: 139	2 bytes on wire (1	1136 bits), 1392 byt	es captur	ed (1113	136 bits) on interface 0	$\wedge$
Ir	terface id:	0 (\Device\NPF_{B	2471995-9A2F-4AC4-BF	2D-D7481A	211ED9})	رە 1	
Er	capsulation	i type: Ethernet (1	)				
Ar	rival Time:	Apr 12, 2017 22:5	4:40.613773000 SE AS	ia Standa	rd Time	2	
1	ime shift f	or this packet: 0.	000000000 seconds]				
Ep	och Time: 1	492012480.61377300	0 seconds				
1 17	ime delta f	rom previous captu	red frame: 0.0064510	00 second:	s		
1 1	ime delta f	rom previous displ	ayed frame: 0.006451	.000 secon	ids J		
0	ime since r	eterence or tirst	rrame: 99.8268/9000	seconasj			
Fr	ame Number:	/398	11. X				
F	ame Length:	1392 Dytes (11136	DITS)				
Ca	ipture Lengt	n: 1392 bytes (111	30 DILS)				
	rame is mar	Ked: Faisej					
LF LF	rame is igr	oreu: Faisej					
1	rococois ir	i irame: etn:etnert	ype: ip:udp:duic]				
	oloring Rul	e Name: UDPj					
10		e string: uup)					
0000	08 3d 88 4e	7e 0c 70 8b cd 8	d dc 6d 08 00 45 00	.=.N~.p.	m	.E.	$\wedge$
0020	44 9a c1 d2	01 bb 05 4e ed 0	c 0d fd 01 de 1f 4b	D I	N+2		
0030	60 00 42 51	30 33 35 01 a4 3	e 23 33 45 4f 3d 27	.BQ035	>#3E0	:0=*	
0040	9c 43 d1 c5	a0 01 00 04 43 4	8 4c 4f 1d 00 00 00	.c	. CHLO		
0050	50 41 44 00	eb 00 00 00 53 4	e 49 00 08 01 00 00	PAD	. SNI	,	٧
🔵 💅 F	ile: "C:\Users\AS	US-pc\Documents\detik.p	Packets: 24926 · Displayed:	24926 (100,0%)	) • Prof	ofile: Default	

Pada gambar diatas dapat diketahui bahwa pada frame 7398 **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari halaman yang dituju (destination)** yaitu detik.com adalah **74.125.68.154** . Selain itu dapat kita ketahui pada bagian frame bahwa frame 7398 ini diakses pada pukul 22:54:40 tanggal 12 april 2017.

Filter:			`	<ul> <li>Expression</li> </ul>	Clear Apply Save	
No.	Time	Source	Destination	Protocol	Length Info	^
73	94 99.789746	192.168.43.83	203.190.242.59	TCP	54 60444 → 443 [ACK] seq=4450 ACk=86771 Win=23552 Len=0	
73	95 99.792564	192.168.43.83	216.58.221.66	QUIC	77 Payload (Encrypted), PKN: 10, CID: 12369586900995331160	
73	96 99.801351	203.190.242.59	192.168.43.83	тср	66 [TCP Dup ACK 7350#1] 443 → 60450 [ACK] Seq=153 Ack=518 Win=15872 Len=0 SLE=1 SRE=518	
73	97 99.820428	192.168.43.83	203.190.242.59	TLSV1.2	1114 Application Data	
73	98 99.826879	192.168.43.83	74.125.68.154	QUIC	1392 Client Hello, PKN: 1, CID: 4755907082276700669	
73	99 99.828389	192.168.43.83	74.125.68.154	QUIC	422 Payload (Encrypted), PKN: 2, CID: 4755907082276700669	
74	00 99.839368	203.190.242.59	192.168.43.83	TLSV1.2	1454 Ignored Unknown Record	
74	01 99.839747	203.190.242.59	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record	
74	02 99.839830	192.168.43.83	203.190.242.59	TCP	54 60444 → 443 [ACK] seq=4450 Ack=89571 win=25088 Len=0	
74	03 99.843615	203.190.242.59	192.168.43.83	TLSV1.2	1454 Ignored Unknown Record	
74	04 99.843893	203.190.242.59	192.168.43.83	TLSv1.2	1454 Ignored Unknown Record	
74	05 99.843896	203.190.242.59	192.168.43.83	TLSV1.2	1321 Ignored Unknown Record	
74	06 99.843972	192.168.43.83	203.190.242.59	TCP	54 60444 → 443 [ACK] seq=4450 Ack=93638 Win=25088 Len=0	
74	07 99 844259	203 190 241 95	192 168 43 83	тср	380 [TCP_Retransmission] 443 → 60447 [PSH_ACK] Sen=2801 Ack=208 Win=15872 Len=326	ľ
	lime deita f	rom previous disp	layed trame: 0.0064:	SIUUU Secon	asj	^
	Time since r	ererence or first	Trame: 99.8268/9000	u secondsj		
	rame Number:	/ 398				
	rame Length:	1392 Dytes (1113	10 DILS)			
	apture Lengt	n: 1392 bytes (11	130 DITS)			
	Frame 15 mar	Ked: Faisej				
	Frame 15 1gr	iored: Faisej				
	Protocols in	i frame: etn:etner	type:ip:uap:quic]			
	Coloring Rul	e Name: UDPj				
	COTOPING RUI	e string: uapj		- 12 - 1		.8
Et	hernet II, Sr	c: AsustekC_8d:dc	::60 (/0:80:Cd:8d:dc:	:6a), DST:	SamsungE_4e:/e:uc (U8:30:88:4e:/e:UC)	
÷	Destination:	Samsungt_4e:/e:0c	: (U8:30:88:4e:/e:OC)	)		
_		1 - 0				
Ŧ	Source: Asust	ekC_8d:dc:6d (70:	8b:cd:8d:dc:6d)			I

Pada bagian ethernet terlihat bahwa source (**192.168.43.83**) memiliki mac address **70:8b:cd:8d:dc:6d** dan destinationnya (**74.125.68.154**) memiliki mac address **08:3d:88:4e:7e:0c**.

No.	Time	Source	Destination	Protocol	Length Info	۸
157	26 156.1483	16192.168.43.83	203.190.242.102	ТСР	54 60594 → 443 [FIN, ACK] Seq=337 Ack=3455 Win=15872 Len=0	i.
157	27 156.1489	47 192.168.43.83	203.190.242.102	тср	54 60594 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0	L
157	28 156.1495	15192.168.43.83	203.190.242.102	ТСР	54 60595 → 443 [FIN, ACK] Seq=337 Ack=3455 win=16128 Len=0	i.
157	29 156.1497	60 192.168.43.83	203.190.242.102	ТСР	54 60595 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0	
157	30 156.1505	16192.168.43.83	203.190.242.102	ТСР	54 60597 → 443 [FIN, ACK] Seq=337 Ack=3455 win=16128 Len=0	
157	31 156.1507	55192.168.43.83	203.190.242.102	ТСР	54 60597 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0	
157	32 156.1515	10192.168.43.83	203.190.242.102	ТСР	54 60596 → 443 [FIN, ACK] Seq=337 Ack=3455 win=16128 Len=0	
157	33 156.1519	20192.168.43.83	203.190.242.102	тср	54 60596 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0	
157	34 156.1525	62 192.168.43.83	203.190.242.102	ТСР	54 60598 → 443 [FIN, ACK] Seq=337 Ack=3455 win=16128 Len=0	
157	35 156.1527	73192.168.43.83	203.190.242.102	тср	54 60598 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0	
157	36 156.1534	55192.168.43.83	74.125.68.157	тср	54 60582 → 80 [FIN, ACK] Seq=1752 Ack=989 Win=15616 Len=0	
157	37 156.1537	60192.168.43.83	74.125.68.157	ТСР	54 60583 → 80 [FIN, ACK] Seq=1792 Ack=989 Win=15616 Len=0	
157	38 156.1542	39192.168.43.83	74.125.68.157	тср	54 60584 → 80 [FIN, ACK] Seq=919 Ack=495 Win=15872 Len=0	۷
	уре: тъла	(UXU8UU)				
∃ Int	ernet Prot	ocol Version 4, Src:	192.168.43.83, Dst	74.125.6	8.157	
🗄 Tra	Insmission	Control Protocol, Sro	: Port: 60583, Dst F	Port: 80,	Seq: 1792, Ack: 989, Len: 0	
5	Source Port	: 60583				
[	estination	Port: 80				
	Stream ind	ex: 358]				
	TCP Segmen	t Len: 0]				
5	Sequence nu	mber: 1792 (relati	ive sequence number)			
1	<pre>\cknowledgm</pre>	ent number: 989 (r	elative ack number)			
H	leader Leng	th: 20 bytes				1
E F	lags: 0x01	1 (FIN, ACK)				
V	/indow size	value: 61				
	Calculated	window size: 15616]				
	Window siz	e scaling factor: 256	5]			
(	hecksum: 0	xfea0 [unverified]				
	Checksum S	tatus: Unverified]				
l	rgent poin	ter: O				$\lor$

Untuk frame ke 15736 request dari source ke destination (detik.com) menggunakan protokol TPC dengan **Source Port nya 192** dan **Destination Port nya 80.** 

l.	_	-		1		
N	o. Time	Source	Destination	Protocol	Length Info	=^
	129 3.640086	192.168.43.83	112.215.88.59	QUIC	80 Payload (Encrypted), PKN: 8, CID: 18275625714750010923	_
l	130 3.700314	192.168.43.83	203.190.242.102	тср	264 [TCP Retransmission] 60262 → 443 [PSH, ACK] Seq=1 Ack=1 Win=16384 Len=210	
	131 3.706838	112.215.88.59	192.168.43.83	QUIC	80 Payload (Encrypted), PKN: 10, CID: 18275625714750010923	
	132 3.746363	203.190.242.172	192.168.43.83	тср	1454 [TCP Out-Of-Order] 443 → 60263 [ACK] Seq=1 Ack=209 Win=30464 Len=1400	-
	133 3.746561	192.168.43.83	203.190.242.172	тср	66 60263 → 443 [ACK] Seq=209 Ack=1401 Win=16384 Len=0 SLE=2801 SRE=3129	
	134 3.750470	203.190.242.172	192.168.43.83	тср	1454 [TCP Out-Of-Order] 443 → 60263 [ACK] Seq=1401 Ack=209 Win=30464 Len=1400	
	135 3.750634	192.168.43.83	203.190.242.172	TCP	54 60263 → 443 [ACK] Seq=209 Ack=3129 Win=16384 Len=0	
~	136 3.754527	192.168.43.83	203.190.242.172	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request	-
	137 3.819639	203.190.242.102	192.168.43.83	тср	66 [TCP Previous segment not captured] 443 → 60262 [ACK] Seq=3128 Ack=211 Win=30464 Len=0 SLE=1 SRE=211	
	138 3.880572	203.190.242.172	192.168.43.83	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
	139 3.880575	203.190.242.172	192.168.43.83	TLSv1.2	123 Application Data	- v
	Acknowledgmer	at number: 335 ()	relative ack number)			
	Header Length	n: 20 bytes	relacive ack number)			~
	> Elager Av018	(DCH ACK)				
	Window size )	(PDI), ACK)				
	[Calculated a	vindow cize: 20464]				
	[Window cize	scaling factors 250	41			
	Chocksum, Ave	101 [upportial]	0]			- 14
	Checksum Sta	ature Unvertited]				
	Unerst asists	acus: onvertiteuj				
	> [SEO/ACK anal	iri e				
	Cocupa Sockets	Lysisj				-
	TISUL 2 Becor	ad Lawani. Handshaka	Protocol, New Section Tick	kat		-
	TLSv1.2 Recor	d Layer. Hanushake	when Spec Protocol, Change	Cinhon Enor		_
	TLSVI.2 Recor	nd Lavon, Handshako	Destacal, Encounted Handel	haka Massaga		-
	/ ILSVI.2 Recor	ru Layer: Hanushake	Protocol: Encrypted Handsi	nake nessage		¥
(	000 70 8b cd 8d	dc 6d 08 3d 88 4e	7e 0c 08 00 45 00 p	m.= .N~E.	· · · · · · · · · · · · · · · · · · ·	^
(	010 01 2a d6 79	40 00 37 06 c1 ed	cb be f2 ac c0 a8 .*.y@	.7		
(	020 2b 53 01 bb	eb 67 a6 54 86 20	c6 21 ea 1f 50 18 +5	g.T!P.		
(	030 00 77 d1 91	00 00 16 03 03 00	ca 04 00 00 c6 00 .w			
(	040 00 01 2c 00	c0 f3 b1 5e 06 a7	a5 d5 90 a9 21 55,	··^ ·····!U	J	
6	1050 2c cd ca c4	91 0e 06 be c7 af	53 ba 90 74 96 a1 ,	St		
6	1000 93 50 85 e8	ap /3 bt 84 ac 8e	b5 4a 30 at e/ b5 .[	scJU		
6	070 aD T6 ef 36	03 9/ 08 09 0C 93 03 70 62 c2 0= 64	10 /2 00 00 ac 52b. 07 32 7h 51 h1 63 /V	⊥rnK		
	CD 20 39 CC	CJ / J UZ UZ 98 04	3/ 32 /0 31 01 03 .(T	yuu.zių.u	· · · · · · · · · · · · · · · · · · ·	×

Pada gambar diatas, yaitu pada **frame 138** terdapat **handshake** dari source 203.190.242.172 ke destination dengan IP address 192.168.43.83 (PC).

## 4. Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website <u>www.kompas.com</u>

Filte	in .		~	Expression	Clear Apply Save		
No.	Time	Source	Destination	Protocol	Length Info	^	
	162 6.024866	192.168.43.83	74.125.24.94	QUIC	80 Payload (Encrypted), PKN: 36, CID: 16810017306748636352		
	163 6.187581	192.168.43.83	74.125.24.94	QUIC	263 Payload (Encrypted), PKN: 37, CID: 16810017306748636352		
	164 6.273358	74.125.24.94	192.168.43.83	QUIC	141 Payload (Encrypted), PKN: 61		
	165 6.300887	192.168.43.83	74.125.24.94	QUIC	77 Payload (Encrypted), PKN: 38, CID: 16810017306748636352		
	166 6.595651	192.168.43.83	112.215.184.49	тср	66 62418 → 443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 wS=256 SACK_PERM=1		
	167 6.630999	192.168.43.83	112.215.184.49	QUIC	1392 Client Hello, PKN: 1, CID: 3979321133185802354		
	168 6.723794	112.215.184.49	192.168.43.83	TCP	66 443 - 62418 [SYN, ACK] seq=0 Ack=1 win=29200 Len=0 MSS=1400 WS=128 SACK_PERM=1		
	169 6.724045	192.168.43.83	112.215.184.49	TCP	54 62418 → 443 [ACK] Seq=1 Ack=1 Win=16384 Len=0		
	170 6.724628	192.168.43.83	112.215.184.49	TLSV1.2	265 Client Hello		
	171 6.748183	192.168.43.83	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1		
	172 6.816008	112.215.184.49	192.168.43.83	QUIC	1392 Payload (Encrypted), PKN: 1, CID: 3979321133185802354		
	173 6.817218	192.168.43.83	112.215.184.49	QUIC	81 Payload (Encrypted), PKN: 2, CID: 3979321133185802354		
	174 6.817478	112.215.184.49	192.168.43.83	QUIC	81 Payload (Encrypted), PKN: 2, CID: 3979321133185802354	Y	
- F	rame 166: 66	bytes on wire (528	bits), 66 bytes cap	tured (528	bits) on interface O	~	
	Interface id	: 0 (\Device\NPF_{B	2471995-9A2F-4AC4-B	F2D-D7481A	211ED9})		
	Encapsulation	n type: Ethernet (1	.)				
	Arrival Time	: Apr 12, 2017 23:3	8:38.986983000 SE A	sia Standa	rd Time		
	[Time shift i	for this packet: 0.	000000000 seconds]				
	Epoch Time: 3	1492015118.98698300	0 seconds				
	[Time delta i	from previous captu	red frame: 0.294764	000 second	5]		
	[Time delta i	from previous displ	ayed frame: 0.29476	4000 secon	ds]		
	[Time since I	reference or first	frame: 6.595651000	seconds]			
	Frame Number	: 166					
	Frame Length: 66 bytes (528 bits)						
	Capture Length: 66 bytes (528 bits)						
	[Frame is marked: False]						
	[Frame is ignored: False]						
	[Protocols i	n frame: eth:ethert	ype:ip:tcp]				
	ICOLOCING RULE NAME: TCP SYN/FTNI						

Pada gambar diatas dapat diketahui bahwa pada frame 166, **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari halaman yang dituju (destination)** yaitu kompas adalah **112.215.184.49**. Frame 166 terakses pada pukul 23:38:38.

No.	Time	Source	Destination	Protocol	Length Info	٨			
	162 6.024866	192.168.43.83	74.125.24.94	OUIC	80 Pavload (Encrypted), PKN: 36, CID: 16810017306748636352				
	163 6.187581	192.168.43.83	74.125.24.94	QUIC	263 Payload (Encrypted), PKN: 37, CID: 16810017306748636352				
	164 6.273358	74.125.24.94	192.168.43.83	QUIC	141 Payload (Encrypted), PKN: 61				
	165 6.300887	192.168.43.83	74.125.24.94	QUIC	77 Payload (Encrypted), PKN: 38, CID: 16810017306748636352				
	166 6.595651	192.168.43.83	112.215.184.49	ТСР	66 62418 → 443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 wS=256 SACK_PERM=1				
	167 6.630999	192.168.43.83	112.215.184.49	QUIC	1392 Client Hello, PKN: 1, CID: 3979321133185802354				
	168 6.723794	112.215.184.49	192.168.43.83	TCP	66 443 → 62418 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1400 WS=128 SACK_PERM=1				
	169 6.724045	192.168.43.83	112.215.184.49	тср	54 62418 → 443 [ACK] Seq=1 Ack=1 Win=16384 Len=0				
	170 6.724628	192.168.43.83	112.215.184.49	TLSV1.2	265 Client Hello				
	171 6.748183	192.168.43.83	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1				
	172 6.816008	112.215.184.49	192.168.43.83	QUIC	1392 Payload (Encrypted), PKN: 1, CID: 3979321133185802354				
	173 6.817218	192.168.43.83	112.215.184.49	QUIC	81 Payload (Encrypted), PKN: 2, CID: 3979321133185802354				
	174 6.817478	112.215.184.49	192.168.43.83	QUIC	81 Payload (Encrypted), PKN: 2, CID: 3979321133185802354	¥			
E	Ethernet II. S	nc: AsustekC 8d:dc:	6d (70:8b:cd:8d:dc:)	6d). Dst:	SamsungE 4e:7e:0c (08:3d:88:4e:7e:0c)	•			
	Destination:	SamsungE 4e:7e:0c	(08:3d:88:4e:7e:0c)	,	Sambarige_ren erec (orbarior ren erec)	Ŷ			
	■ Source: Asus	tekc 8d:dc:6d (70:8	Sb:cd:8d:dc:6d)						
	Type: IPv4 (	0x0800)	,						
Type: 1994 (0x0800) Internet Protocol Version 4. Src: 192.168.43.83. Dst: 112.215.184.49									
Ξ	E Transmission Control Protocol, Src Port: 62418, Dst Port: 443, Seq: 0, Len: 0								
	Source Port:	62418	,						
	Destination	Port: 443							
	[Stream inde	x: 0]							
	[TCP Segment	Len: 0]							
	Sequence num	ber: 0 (relative	e sequence number)						
	Acknowledgme	nt number: 0							
	Header Lengt	h: 32 bytes							
	∃ Flags: 0x002	(SYN)							
	Window size	value: 8192							
	[Calculated	window size: 8192]							
	Checksum: Ox	949f [unverified]				*			
00	00 08 3d 88 4	e 7e 0c 70 8b cd 8	d dc 6d 08 00 45 00	.=.N~.D	· m E.	_			
00	10 00 34 1c e	5 40 00 80 06 c8 d	9 c0 a8 2b 53 70 d7	.4@	+Sp.				
00	20 b8 31 f3 d	2 01 bb be 0c f1 d	1 00 00 00 00 80 02	.1					
00	30 20 00 94 9	r uu uu u2 04 05 b	4 01 03 03 08 01 01						
00	40 04 02								

Pada bagian ethernet terlihat bahwa source (**192.168.43.83**) memiliki mac address **70:8b:cd:8d:dc:6d** dan destinationnya (**112.215.184.49**) memiliki mac address **08:3d:88:4e:7e:0c** . Sedangkan untuk Frame 166a ini menggunakan protokol TCP yang mana **Source Portnya dalah 62418** dan **Destination Port nya 433.** 

A	pply a display filter	<ctrl-></ctrl->			🖬 •	Expression +			
No.	Time	Source	Destination	Protocol	Length Info	^			
	401 7.922996	103.243.221.3	75 192.168.43.83	TCP	1354 [TCP segment of a reassembled PDU]				
	402 7.923113	192.168.43.8	3 103.243.221.75	TCP	54 62437 → 443 [ACK] Seq=209 Ack=2601 Win=16616 Len=0				
	403 7.926476	192.168.43.83	3 103.243.221.75	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request				
	404 7.928955	103.243.221.3	75 192.168.43.83	TLSv1.2	1354 Certificate[TCP segment of a reassembled PDU]				
	405 7.929199	103.243.221.3	75 192.168.43.83	TLSv1.2	763 Certificate StatusServer Key Exchange, Server Hello Done				
	406 7.929201	54.192.151.15	5 192.168.43.83	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message				
	407 7.929396	192.168.43.8	3 103.243.221.75	TCP	54 62437 → 443 [ACK] Seq=209 Ack=4610 Win=16616 Len=0				
	408 7.932804	192.168.43.8	3 103.243.221.75	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request				
	409 7.934632	54.239.16.23	5 192.168.43.83	TCP	62 80 → 62431 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360 WS=64				
	410 7.934634	54.239.16.23	5 192.168.43.83	TCP	62 80 → 62432 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360 WS=64				
	411 7.934635	54.239.16.23	5 192.168.43.83	TCP	62 80 → 62430 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360 WS=64				
	412 7.934952	192.168.43.8	54.239.16.235	TCP	54 62431 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0				
	413 7.935270	192.168.43.83	54.239.16.235	TCP	54 62432 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0				
	414 7.935452	192.168.43.83	54.239.16.235	TCP	54 62430 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0				
i -	415 7.945952	54.192.151.19	5 192.168.43.83	TI Sv1.2	312 New Session Ticket. Change Cinher Snec. Encrynted Handshake Message	¥			
> E > I > T > S	> Ethernet II, Src: SamsungE_4e:7e:0c (08:3d:08:4e:7e:0c), Dst: AsusteKC_8d:dc:6d (70:8b:cd:8d:dc:6d) > Internet Protocol Version 4, Src: 54.192.151.15, Dst: 192.168.43.83 > Transmission Control Protocol, Src Port: 443, Dst Port: 62427, Seq: 4943, Ack: 347, Len: 258 > Secure Sockets Layer								
000	70 8b cd 8d 01 2a 91 98	dc 6d 08 3d 8 40 00 f5 06 3	8 4e 7e 0c 08 00 45 00 9 6a 36 c0 97 0f c0 a8	pm.= .N~E .*@ 9j6	· · · · · · · · · · · · · · · · · · ·	^			
002	2b 53 01 bb	f3 db 9d 52 b	8 bc 87 7d da 3c 50 18	+SR}. <p< td=""><td></td><td></td></p<>					
003	00 77 at 24	00 00 16 03 0	3 00 ca 04 00 00 c6 00	.w.\$	•				
004	00 2a 30 00	C0 00 00 e7 a	e bT a2 03 aD 2a 17 09	.~0					
005	ac 35 0h a0	16 eb f0 6c c	6 ec ac e3 e0 3d 80 74	.5]=.t					
007	20 80 f1 03	84 f9 57 ba c	3 28 2c 82 8f 8f b0 bf	W(,	•				
008	03 0e c0 0a	e6 16 78 77 b	6 0e 99 2b c4 79 ff de	xw+.y.		~			
	🛛 kompas				Packets: 13366 · Displayed: 13366 (100.0%) · Load time: 0:2.204	Profile: Default			

Pada gambar diatas, yaitu pada **frame 1406** terdapat **handshake** dari source 54.192.151.15 ke destination dengan IP address 192.168.43.83 (PC).