## JARINGAN KOMPUTER Capture Data Web Browser Dan Online Streaming Menggunakan Wireshark Dan Netstat –a



Nama : Alfiansyah Nim : 09011281520131 Dosen Pengampuh : Deris Setiawan

Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya 2017

### 1. <u>Capture data WEB Browser (http://wiki.teamliquid.net/)</u>

Sebelum mulai melakukan capture data, terlebih dahulu kita harus mengetahui IP address komputer kita (source) dan juga IP address dari web browser yang kita tuju (destination), hal ini nantinya akan dapat kita gunakan untuk mempermudah memfilter hasil capture data.

- IP Address Source : 10.178.10.18

(Dapat kita ketahui dengan mengetikan perintah ipconfig/all melalui cmd)

ireless LAN adapter Wireless Network Connection:							
Connection-specific DNS Suffix . : Description Atheros AR9485WB-EG Wireless Network Adap							
Physical Address							
Autoconfiguration Enabled : Yes Link-local IPv6 Address : fe80::9da9:a4e7:48dc:d5a4%14(Preferred)							
IPv4 Address							
Lease Expires							
DHCP Server							
DHCPvb Client DULD							
8.8.4.4 NetBIOS over Tcpip : Enabled							

- IP Adress Destination : 144.217.237.5

(Dapat kita ketahui dengan melakukan ping ke web yang kita tuju melalui cmd)



- Hasil capture data dengan menggunakan wireshark yang sudah di filter berdasarkan IP

📕 ip.	dst == 144.217.237.5	&& tcp				🛛 🔁 🔹 B	xpression +
No.	Time	Source	Destination	Protocol	Length Info		-
E	155 13.632759	10.178.10.18	144.217.237.5	TCP	66 57996 → 80 [SYN] Seg=0 Win=63443 Len=0 MSS=1460 W	IS=64 SACK PERM=1	
	156 13.642000	10.178.10.18	144.217.237.5	TCP	66 57997 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 W	IS=64 SACK_PERM=1	
	157 13.906745	10.178.10.18	144.217.237.5	TCP	66 57998 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 W	IS=64 SACK_PERM=1	
	160 14.011754	10.178.10.18	144.217.237.5	TCP	54 57998 → 80 [ACK] Seq=1 Ack=1 Win=365 Len=0		
	162 14.014786	10.178.10.18	144.217.237.5	HTTP	706 GET / HTTP/1.1		
	163 14.275157	10.178.10.18	144.217.237.5	HTTP	55 [TCP Spurious Retransmission] Continuation		
	165 14.337705	10.178.10.18	144.217.237.5	HTTP	706 [TCP Spurious Retransmission] GET / HTTP/1.1		
1	166 14.555983	10.178.10.18	144.217.237.5	TCP	55 [TCP Spurious Retransmission] [TCP segment of a r	eassembled PDUj	
	167 14.649838	10.1/8.10.18	144.217.237.5	TCO	706 [TCP Spurious Retransmission] Get / HTTP/1.1		
	1/0 15.362/96	10.178.10.18	144.217.237.5	TCP	54 57996 + 60 [ACK] Seq=055 ACK=1461 W1R=365 Len=0		
	172 15.505545	10.170.10.10	144.217.237.5	TCP	54 57555 4 66 [ACK] Seq=653 Ack=2321 Win=568 Len=6		
	176 15 412706	10.178.10.18	144 217 237 5	TCP	54 57998 + 80 [ACK] Seq=653 Ack=5841 Win=434 Len=0		
	178 15 415419	10.178.10.18	144,217,237,5	TCP	54 57998 + 80 [ACK] Sequ653 Acku5927 Winu457 Lenu0		
	179 15,421926	10.178.10.18	144,217,237,5	TCP	66 57999 → 80 [SYN] Seg=0 Win=63443 Len=0 MSS=1460 W	IS=64 SACK PERM=1	
	181 15,429139	10,178,10,18	144,217,237,5	TCP	66 58000 → 80 [SYN] Seg=0 Win=63443 Len=0 MSS=1460 W	S=64 SACK PERM=1	
	184 15.646913	10.178.10.18	144.217.237.5	TCP	66 58001 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 W	IS=64 SACK PERM=1	=.
	chernet 11, Srci ) Destination: Ro ) Source: Samsung — Type: IPv4 (0x0 ternet Protocol ransmission Contr	Samsungt_/a:83:00 ( uterbo_21:90:19 (e4 E_7a:83:0b (18:67:bi 800) Version 4, Src: 10.: ol Protocol, Src Po	18:6/100:74:85:80), D 88:76:21:90:19) 8:7a:83:0b) 178:10:18, Dst: 144.2 rt: 57996, Dst Port: i	st: Kouterb 17.237.5 80, Seq: 0,	o_21190119 (e4180180:21190:29)		
0000 0010 0020 0030 0040	e4 8d 8c 21 90 00 34 38 d3 40 ed 05 e2 8c 00 f7 d3 6a 95 00 04 02	19 18 67 b0 7a 83 00 80 06 2f 4e 0a 50 ca 45 cc e3 00 00 02 04 05 b4 01	0b       08       00       45       00          b2       0a       12       90       d9       .48         00       00       08       02        03       03       06       01       01      j	!g .z .@ ∕N P.E	.£.		
	<ul> <li>Frame (frame), 66</li> </ul>	bytes				Packets: 10645 * Displayed: 187 (1.8%) * Dropped: 0 (0.0%)	Profile: Defau

destination dan protokol FTP

- Tabel hasil capture data

IP Source	IP Destination	Info
10.178.10.18	144.217.237.5	57996 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	57997 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	57998 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=1 Ack=1 Win=365 Len=0
10.178.10.18	144.217.237.5	GET / HTTP/1.1
10.178.10.18	144.217.237.5	[TCP Spurious Retransmission] Continuation
10.178.10.18	144.217.237.5	[TCP Spurious Retransmission] GET / HTTP/1.1
10.178.10.18	144.217.237.5	[TCP Spurious Retransmission] [TCP segment of a reassembled PDU]
10.178.10.18	144.217.237.5	[TCP Spurious Retransmission] GET / HTTP/1.1
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=1461 Win=365 Len=0
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=2921 Win=388 Len=0
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=4381 Win=411 Len=0
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=5841 Win=434 Len=0
10.178.10.18	144.217.237.5	57998 > 80 [ACK] Seq=653 Ack=5927 Win=457 Len=0
10.178.10.18	144.217.237.5	57999 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	58000 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	58001 > 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
10.178.10.18	144.217.237.5	[TCP Window Update] 57998 > 80 [ACK] Seq=653 Ack=5927 Win=480 Len=0
10.178.10.18	144.217.237.5	58000 > 80 [ACK] Seq=1 Ack=1 Win=365 Len=0

- Setelah melakukan capture data menggunakan wireshark kita dapat melihat detail dari tiap data yang telah kita capture, yang mana diantaranya kita dapat mengetahui MAC address source dan juga destination.

MAC address source : 18-67-B0-7A-83-0B

MAC address destination : E4-8D-8C-21-90-19

p.dst == 144.217.237.5 8.8 top									
No. Time Source Destination Protocol Length Info									
[ 155 13.632759 10.178.10.18 144.217.237.5 TCP 66 57996 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1     [ 155 13.632759 10.178.10.18 144.217.237.5 TCP 66 57996 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1     [ 155 13.632759 10.178.10.18 144.217.237.5 TCP 66 57996 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1     [ 155 13.632759 10.178.10.18 144.217.237.5 TCP 66 57996 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1     [ 155 13.632759 10.178.10.18 144.217.237.5 TCP 66 57996 → 80 [SYN] Seq=0 Win=63443     [ 155 13.632759 10.178.10.18 144.217.237.5 TCP 66 57996 → 80 [SYN] Seq=0     [ 155 13.632759 10.178.10.18 144.217.237.5 TCP 66 57996 → 80 [SYN] Seq=0     [ 155 13.632759     [ 155 13.632759     [ 155 13.632759     [ 155 13.632759     [ 155 13.63275     [ 155 13.63275     [ 155 13.63275     [ 155 13.63275     [ 155 13.63275     [ 155 13.63275     [ 155 13.6327     [ 155 13.6327     [ 155 13.6327     [ 155 13.6327     [ 155 13.632									
156 13.642000 10.178.10.18 144.217.237.5 TCP 66 57997 + 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1									
157 13.906745 10.178.10.18 144.217.237.5 TCP 66 57998 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1									
160 14.011754 10.178.10.18 144.217.237.5 TCP 54 57998 + 80 [ACK] Seq=1 Ack=1 Win=365 Len=0									
162 14.014786 10.178.10.18 144.217.237.5 HTTP 706 GET / HTTP/1.1									
163 14.275157 10.178.10.18 144.217.237.5 HTTP 55 [TCP Spurious Retransmission] Continuation									
165 14.337705 10.178.10.18 144.217.237.5 HTTP 706 [TCP Spurious Retransmission] GET / HTTP/1.1									
166 14.555983 10.178.10.18 144.217.237.5 TCP 55 [TCP Spurious Retransmission] [TCP segment of a reassembled PDU]									
167 14.649838 10.178.10.18 144.217.237.5 HTTP 706 [TCP Spurious Retransmission] GET / HTTP/1.1									
170 15.362798 10.178.10.18 144.217.237.5 TCP 54 57998 → 80 [ACK] Seq=653 Ack=1461 Win=365 Len=0									
172 15.363549 10.178.10.18 144.217.237.5 TCP 54 57998 → 80 [ACK] Seq=653 Ack=2921 Win=388 Len=0									
174 15.411486 10.178.10.18 144.217.237.5 TCP 54 57998 → 80 [ACK] Seq=653 Ack=4381 Win=411 Len=0									
176 15.412706 10.178.10.18 144.217.237.5 TCP 54 57998 → 80 [ACK] Seq=653 Ack=5841 Win=434 Len=0									
178 15.415419 10.178.10.18 144.217.237.5 TCP 54 57998 → 80 [ACK] Seq=653 Ack=5927 Win=457 Len=0									
179 15.421926 10.178.10.18 144.217.237.5 TCP 66 57999 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1									
181 15.429139 10.178.10.18 144.217.237.5 TCP 66 58000 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1									
184 15.646913 10.178.10.18 144.217.237.5 TCP 66 58001 → 80 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1									
∂) Frame 155: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 ⊕) Ethernet II, Src: SansungE 7a:83:0b (18:67:b0:7a:83:0b), Dst: Routerbo_21:90:19 (e4:8d:8c:21:90:19)									
UP DESTINATION: NOUTEPO _21:90:19 (04:00:00:21:90:19) (04:00:00:21:90:19) N.N.(									
Tradurce: Samsunge_ratiosidu (16:07:00:74:05:00)									
- " ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' '									
G Internet Flotter Velskoll velskoll og bette 1900 bet 144-127-13									

- Hasil capture data menggunakan netstat –a

C:\Users\Samsung>netstat -a							
Active Co	onnections						
Proto	Local Address	Foreign Address	State				
TCP	0.0.0.0:135	0:0	LISTENING				
TCP	0.0.0.0:445	0:0	LISTENING				
TCP	0.0.0.0:2508	0 : 0	LISTENING				
TCP	0.0.0.0:49152	0 : 0	LISTENING				
TCP	0.0.0.0:49153	0:0	LISTENING				
TCP	0.0.0.0:49154	0:0	LISTENING				
TCP	0.0.0.0:49155	0 = 0	LISTENING				
TCP	0.0.0.0:49156	0 = 0	LISTENING				
TCP	10.178.10.18:139	0:0	LISTENING				
TCP	10.178.10.18:56985	203.104.174.13:https	ESTABLISHED				
TCP	10.178.10.18:58308	sa-in-f136:https	TIME_WAIT				
TCP	10.178.10.18:58309	sa-in-f102:https	TIME_WAIT				
TCP	10.178.10.18:58310	sc-in-f154:https	ESTABLISHED				
TCP	10.178.10.18:58311	wiki:http	TIME_WAIT				
TCP	10.178.10.18:58312	wiki:http	TIME_WAIT				
TCP	10.178.10.18:58313	wiki:http	TIME_WAIT				
TCP	10.178.10.18:58314	wiki:http	ESTABLISHED				
TCP	10.178.10.18:58316	sa-in-f138:https	ESTABLISHED				
TCP	10.178.10.18:58317	sa-in-f155:https	ESTABLISHED				
TCP		sin11s03-in-f34:http	ESTABLISHED				
TCP	10.178.10.18:58319	sa-in-f132:https	ESTABLISHED				
TCP		sin11s03-in-f34:http	ESTABLISHED				
TCP	10.178.10.18:58322	sa-in-f95:https	ESTABLISHED				
TCP		sin11s03-in-f34:https	ESTABLISHED				
ŤČP TCP	10.178.10.18:58324	wiki:http wiki:httn	ESTABLISHED				
TCP	10.178.10.18:58327	a45-121-219-200:http 74 125 24 94:https	TIME_WAIT				
TCP	10.178.10.18:58329	23.111.9.30:http					
TCP		pixel:http	ESTABLISHED				
TCP		ec2-52-205-185-135:http sa-in-f95:https	ESTABLISHED				
TCP	10.178.10.18:58335	sc-in-f157:https 74.125.24.99:https	ESTABLISHED				
TCP	10.178.10.18:58339	103.231.198.13:http sin11s03-in-f34:https	ESTABLISHED				
TCP	10.178.10.18:58343	sa-in-f132:http	TIME_WAIT				
TCP	10.178.10.18:58344	sa-in-f132:http	TIME_WAIT				
TCP	10.178.10.18:58345	sa-in-f94:https	ESTABLISHED				
TCP	10.178.10.18:58346	74.125.24.190:https	ESTABLISHED				

Setelah kita menggunakan netstat –a untuk melakukan capture data terdapat beberapa informasi yang kita dapatkan dari koneksi yang terjadi seperti protocol yang digunakan kemudian local dan foreign address dan juga state.

#### 2. <u>Capture data online streaming (http://indoxxi.net/)</u>

- IP Source : 192.168.43.36

Wir	eless	LAN a	dapt	er	Wi	rel	ess	s h	let	two	)r}	< (	Connection:
	Connec Descri	tion- ption	spec	ifi	.c	DNS	Su •	ıff	i) ·	< _		:	Atheros AR9485WB-EG Wireless Network Adap
cer	Physic	al Ad	dres	s.								=	18-67-B0-7A-83-0B
	DHČP E	nable	d		-		-					Ξ	Yes
	Autoco	nfigu	rati	on	En	abl	ed					-	Yes
	Link-l	ocal	I Pv6	Ád	ldr	ess							fe80::9da9:a4e7:48dc:d5a4%14(Preferred)
	IPv4 A	ddres	s									-	192.168.43.36(Preferred)
	Subnet	Mask										-	255.255.255.0
	Lease	Obtai	ned.									-	Wednesday, August 30, 2017 1:12:07 AM
	Lease	Expir	es.									-	Wednesday, August 30, 2017 2:12:07 AM
	Defaul	t Gat	eway									-	192.168.43.1
	DHCP S	erver											192.168.43.1
	DHCPv6				-							-	286812080
	DHCPvb	Clie	nt D	ULD	' - I								00-01-00-01-20-A0-A2-FH-18-67-B0-7H-83-0B
	DNS Se	rvers										:	8.8.8
	NetBI0	IS ove	r Tc	pip	).							=	Enabled

- IP Destination : 104.25.235.118

C:\Users\Samsung>ping indoxxi.net Pinging indoxxi.net [104.25.235.118] with 32 bytes of data: Reply from 104.25.235.118: bytes=32 time=408ms TTL=54 Reply from 104.25.235.118: bytes=32 time=79ms TTL=54 Reply from 104.25.235.118: bytes=32 time=71ms TTL=54 Reply from 104.25.235.118: bytes=32 time=77ms TTL=54 Ping statistics for 104.25.235.118: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 71ms, Maximum = 408ms, Average = 158ms

- Hasil capture data dengan menggunakan wireshark yang sudah di filter berdasarkan IP

destination dan protokol FTP

, ip	.dst == 104.25.235.118	&& tcp				E Contraction of the second seco	Expression +
No.	Time	Source	Destination	Protocol L	ength Info		<u> </u>
E	29 4.251086	192.168.43.36	104.25.235.118	тср	66 61053 → 443 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 S	ACK_PERM=1	
	45 4.325921	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=1 Ack=1 Win=365 Len=0		
	47 4.326063	192.168.43.36	104.25.235.118	TLSv1.2	571 Client Hello		
	75 4.451218	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=518 Ack=157 Win=365 Len=0		
	79 4.451459	192.168.43.36	104.25.235.118	TLSv1.2	105 Change Cipher Spec, Hello Request, Hello Request		
	81 4.451507	192.168.43.36	104.25.235.118	TLSv1.2	231 Application Data		
	97 4.682872	192.168.43.36	104.25.235.118	TCP	54 [TCP Window Update] 61053 → 443 [ACK] Seq=746 Ack=157 Wi	a=409 Len=0	
	100 4.682980	192.168.43.36	104.25.235.118	TCP	55 [TCP Spurious Retransmission] [TCP segment of a reassemb	led PDU]	
	111 4.725425	192.168.43.36	104.25.235.118	тср	54 61053 → 443 [ACK] Seq=746 Ack=226 Win=411 Len=0		
	127 4.771014	192.168.43.36	104.25.235.118	TLSv1.2	92 Application Data		
	135 4.793926	192.168.43.36	104.25.235.118	тср	54 61053 → 443 [ACK] Seq=784 Ack=264 Win=434 Len=0		
	145 4.882464	192.168.43.36	104.25.235.118	TLSv1.2	509 Application Data		
	1/1 4.955534	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=1239 Ack=1662 Win=457 Len=0		
	1/3 4.95/961	192.168.43.36	104.25.235.118	TCP	54 61053 + 443 [ACK] Seq=1239 ACK=3062 Win=480 Len=0		
	175 4.959788	192.168.43.36	104.25.235.118	TCP	54 61053 + 443 [ACK] Seq=1239 ACK=4458 W1n=502 Len=0		
	177 4.902704	192.100.45.50	104.25.255.110	TCP	54 61053 + 445 [ACK] Seg=1239 ACK=3656 Win=525 Len=0		
	1/9 4.9000/4	192.108.43.30	104.23.233.118	TCP	54 01055 4 445 [ACK] Seq-1259 ACK-7250 W10-548 Len-0		
	thernet II, Src: S Destination: 36: Source: Samsungt Type: IPv4 (0x08 nternet Protocol ) ransmission Contro	Samsungt_/a:83:00 (18: :97:f6:4b:16:cf (36:97 _7a:83:00 (18:67:b0:7 300) Version 4, Src: 192.16 ol Protocol, Src Port:	6/:b0:/a:83:06), Dst: :f6:4b:16:cf) a:83:06) 88.43.36, Dst: 104.25. 61053, Dst Port: 443	36:97:16: 235.118 , Seq: 0,	bollo:cf (∂6:9/;T6:40:16:c7) Len: 0		
0000 0010 0020 0030 0040	36         97         f6         4b         16           00         34         61         bf         40           eb         76         ee         7d         01           f7         d3         5a         cc         00           04         02         02         04         02	cf 18 67 b0 7a 83 0b 00 80 06 59 a8 c0 a8 bb 14 d5 d8 07 00 00 00 02 04 05 b4 01 03	08         00         45         00         6K           2b         24         68         19         .4a.@.           00         00         80         02         .v.}           03         06         01         01        Z	.g .zE Y+\$h			
	Frame (frame) 66	hyter			Packet	c: 8822 · Displayed: 189 (2, 1%) · Dropped: 0 (0, 0%)	Profile: Defaul

- Tabel hasil capture data

Source	Destination	Info
192.168.43.36	104.25.235.118	61053 > 443 [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1 Ack=1 Win=365 Len=0
192.168.43.36	104.25.235.118	Client Hello
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=518 Ack=157 Win=365 Len=0
192.168.43.36	104.25.235.118	Change Cipher Spec, Hello Request, Hello Request
192.168.43.36	104.25.235.118	Application Data
192.168.43.36	104.25.235.118	[TCP Window Update] 61053 > 443 [ACK] Seq=746 Ack=157 Win=409 Len=0
192.168.43.36	104.25.235.118	[TCP Spurious Retransmission] [TCP segment of a reassembled PDU]
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=746 Ack=226 Win=411 Len=0
192.168.43.36	104.25.235.118	Application Data
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=784 Ack=264 Win=434 Len=0
192.168.43.36	104.25.235.118	Application Data
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=1662 Win=457 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=3062 Win=480 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=4458 Win=502 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=5858 Win=525 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=7258 Win=548 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=8658 Win=571 Len=0
192.168.43.36	104.25.235.118	61053 > 443 [ACK] Seq=1239 Ack=10058 Win=594 Len=0

- MAC address source

#### : 18-67-B0-7A-83-0B

MAC address destination

: 36-97-F6-4B-16-CF

	↓ [p.dst == 104.25.235.118 && tcp Expression									
No.	Time	Source	Destination	Protocol	Length Info					
E.	29 4.251086	192.168.43.36	104.25.235.118	TCP	66 61053 → 443 [SYN] Seg=0 Win=63443 Len=0 MSS=1460 WS=64 SACK PERM=1					
	45 4.325921	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seg=1 Ack=1 Win=365 Len=0					
	47 4.326063	192.168.43.36	104.25.235.118	TLSv1.2	571 Client Hello					
	75 4.451218	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=518 Ack=157 Win=365 Len=0					
	79 4.451459	192.168.43.36	104.25.235.118	TLSv1.2	105 Change Cipher Spec, Hello Request, Hello Request					
	81 4.451507	192.168.43.36	104.25.235.118	TLSv1.2	231 Application Data					
	97 4.682872	192.168.43.36	104.25.235.118	TCP	54 [TCP Window Update] 61053 → 443 [ACK] Seq=746 Ack=157 Win=409 Len=0					
	100 4.682980	192.168.43.36	104.25.235.118		55 [TCP Spurious Retransmission] [TCP segment of a reassembled PDU]					
	111 4.725425	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=746 Ack=226 Win=411 Len=0					
	127 4.771014	192.168.43.36	104.25.235.118	TLSv1.2	92 Application Data					
	135 4.793926	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=784 Ack=264 Win=434 Len=0					
	145 4.882464	192.168.43.36	104.25.235.118	TLSv1.2	509 Application Data					
	171 4.955534	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=1239 Ack=1662 Win=457 Len=0					
	173 4.957961	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=1239 Ack=3062 Win=480 Len=0					
	175 4.959788	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=1239 Ack=4458 Win=502 Len=0					
	177 4.962704	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=1239 Ack=5858 Win=525 Len=0					
	179 4.966074	192.168.43.36	104.25.235.118	TCP	54 61053 → 443 [ACK] Seq=1239 Ack=7258 Win=548 Len=0	<b>_</b> _				
÷	Frame 29: 66 byte	s on wire (528 bits)	, 66 bytes captured (5	28 bits) or	n interface 0					
- P	Ethernet II, Src:	SamsungE_7a:83:0b (:	18:67:b0:7a:83:0b), Ds <sup>.</sup>	t: 36:97:f0	6:4b:16:cf (36:97:f6:4b:16:cf)					
	Destination: 3	6:97:f6:4b:16:cf (36	:97:f6:4b:16:cf)	λr						
	E Source: Samsun	gE_7a:83:0b (18:67:be	0:7a:83:0b)	m						
	Type: IPv4 (0x	0800)								
1 B	Internet Protocol	Version 4, Src: 192.	.168.43.36, Dst: 104.2	5.235.118						
⊞	Transmission Cont	rol Protocol, Src Por	rt: 61053, Dst Port: 4	43, Seq: 0	, Len: 0					

- Hasil capture data menggunakan netstat –a

C:\Users	C:\Users\Samsung>netstat -a							
Active C	Active Connections							
Active C Proto TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	onnections Local Address 0.0.0.0:135 0.0.0.0:2508 0.0.0.0:49152 0.0.0.0:49153 0.0.0.0:49155 0.0.0.0:49155 0.0.0.0:49156 127.0.0.1:10400 127.0.0.1:10401 127.0.0.1:54930 127.0.0.1:54931	Foreign Address 0:0 0:0 0:0 0:0 0:0 0:0 0:0 0:0 0:0 Samsung-PC:54942 0:0 Samsung-PC:54931 Samsung-PC:54930	State LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING ESTABLISHED ESTABLISHED ESTABLISHED					
TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	127.0.0.1:54931 127.0.0.1:54932 127.0.0.1:54933 127.0.0.1:54942 127.0.0.1:60615 127.0.0.1:60616 127.0.0.1:60618 192.168.43.36:61174 192.168.43.36:61174 192.168.43.36:61181 192.168.43.36:61184 192.168.43.36:61185 192.168.43.36:61185 192.168.43.36:61185 192.168.43.36:61185 192.168.43.36:61185 192.168.43.36:61185 192.168.43.36:61185	Samsung-PC:54930 Samsung-PC:54933 Samsung-PC:54932 Samsung-PC:10401 Samsung-PC:60616 Samsung-PC:60615 Samsung-PC:60617 0:0 203.104.174.20:https 172.217.27.14:https 172.217.27.35:https 104.25.236.118:https 74.125.200.132:https 172.217.27.34:https 172.217.27.34:https	ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED LISTENING ESTABLISHED TIME_WAIT TIME_WAIT TIME_WAIT TIME_WAIT TIME_WAIT TIME_WAIT					
TCP TCP TCP TCP TCP TCP TCP	$\begin{array}{r} 192.168.43.36:61195\\ 192.168.43.36:61197\\ 192.168.43.36:61198\\ 192.168.43.36:61198\\ 192.168.43.36:61203\\ 192.168.43.36:61203\\ 192.168.43.36:61204\\ 192.168.43.36:61205\end{array}$	172.217.24.102:https 216.58.203.226:https 172.217.24.97:https 172.217.24.102:https 74.125.200.154:https 74.125.68.148:https 216.58.221.74:https	TIME_WHIT ESTABLISHED TIME_WAIT TIME_WAIT TIME_WAIT TIME_WAIT TIME_WAIT					

# 3. <u>Perbandingan capture data menggunakan Wireshark dan Netstat –a</u>

Perbandingan	Wireshark	Netstat -a
Protokol	1482 lebih protokol	TCP & UDP
Filtering paket data jaringan	Ya	Tidak
Menampilkan detail dari hasil capture data	Ya	Tidak
Hasil capture dapat disimpan untuk dianalisa kembali	Ya	Tidak