TUGAS II JARINGAN KOMPUTER



Nama	: Rofby Hidayadi
NIM	: 09011281520132
Dosen Pengampuh	: Deris Stiawan, M.T., Ph.D

JURUSAN SISTEM KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA 2017

I. JUDUL TUGAS

Capturing Data Browsing dan Online Streaming menggunakan Wireshark dan Command Prompt.

II. PROSEDUR

Adapun prosedur dalam melakukan capturing data kali ini adalah sebagai berikut:

- 1. Install aplikasi Wireshark.
- 2. Capturing data :
 - a. Web browsing.
 - b. Online streaming (selain youtube).
- 3. Capturing data menggunakan aplikasi Wireshark.
- 4. Capturing data menggunakan Command Prompt (*netsat -a*) lalu gunakan Ctrl + C untuk perintah break.
- 5. Analisa IP dan MAC address source dan destination.
- 6. Filter berdasarkan IP address kita.
- 7. Buatlah tabel yang berisikan IP dan Info dari paket data yang di capture setelah di filter.

III. DASAR TEORI

Wireshark merupakan salah satu program untuk menganalisis suatu jaringan, baik jaringan kabel ataupun nirkabel. Wireshark sering digunakan untuk troubleshooting, memeriksa keamanan jaringan dan lain-lain. Wireshark akan menangkap paket data pada jaringan yang kemudian, data yang ditangkap tersebut ditampilkan sedetail mungkin. Sedangkan Command Prompt atau CMD merupakan command line interpreter pada sebuah Operating System yang digunakan untuk mengeksekusi suatu hal tertentu dengan cara menuliskan perintahnya pada Command Prompt.

IV. ANALISA PAKET DATA : WEB BROWSING MENGGUNAKAN WIRESHARK DAN CMD

Adapun website yang akan dibrowsing yang kemudian paket datanya di analisa adalah <u>www.viva.co.id</u> yang merupakan salah satu situs berita online Indonesia.

Berikut adalah hasil capturing data ke <u>www.viva.co.id</u> menggunakan Wireshark:

1000	100 C				- 112 - Partie
104	biores	Serveter.	- Personal P	inst life	
1 14.000703	202, 10, 49, 222	891.108.1.280		to be a similar (AD) best high spectrum inner	
# Lx, #00299#	100.39.49.033	102.168.1.165	TER	34 DW + 10146 [708, APP] Sepril Activit Monosetta Larvett	
5.34.00066	101,008.5.385	(MR.78, 49.355	140Y	54 30148 + 98 (ADC) Sept Articl Interesting Lines.	
N SALDERNEY	3,9,2,-2491-3,-3,853	382.78.46.333	110	94 SELET + BETADE SHEET ALL HER HER HER HER F	
1.11.000100	101.110.310.10	100,188-1.00	10.0	to be - table (1996, ADI) teach fully constant revel marked (0-122	
E.T.W. MOMPHE	101.108.1.181	- HRA 3,229,2236,385	167	the little + 00 (with) tampes within this weight law-0	
0.14.820028	181.348.5.181	292,135.256,28	OLD.	and dry treating to the source of the standard for any second standard and	
# 14.41113P	384,34,333,398	210:108.4.385	100	34 58 + 51108 (150, 901) Sept acted speciality (pros-	
CALLER .	100.0011011200	100.000.4.000	1.768	29 48 4 10111 Link 411 Mark while benefitie three	
3 14.41334	282-348-1-381	384.14,128.156	129	Se SENSE + BE [ACC] Segni autor sizerdille Lend	
1.14-11110	00.10.1.00	101110.101.100	1.164	AN YEAR - MA THAT PART PART PROVIDE THE PART	
1.14.11.0111	200.00.101.018	101.108.1.00)	100	48 48 + ULLEL [A[9]] Suppl Side 1 32-3000 (see 8)	
T 14. MINTI	388.00.121.018		100	WW UN + STILL [TTH, ADV] IMD-1 AUXIVIAL-COMPRESSION	
6 14.613560	181,348,1.181	384,18-325,155	158	34 SEISE + RELACES Seded HOR-2 SCHWEISE Land	
7.14.417100	121.215.217.11	391,168.1.391	TOF-	28 08 * 30324 [k107 w(y] 260+1 wind situation itsees	
0.04140304	341-318-1-381	108-101-10-1	100	24 20124 - 00 1902 2404 minut appropriate thread -	
+ 14,430033	184, M. 194, 218	290 Lot 1 1981	100	An on a Tallin DADA, Add Server Ashad Manufacture (serve)	
H LA. KINESA	181-108-1-101	28811912381266	100	\$5 SZUSE + BE [ADV] Sept Alary Minorely (and	
H-TW-WINLING	121.311.10.1	- 301-148-1186	107	to the + still [fill, all] deprind the differences	
rest IL, Solo rest Protocol effortion Contro tool Transfer	Arian ani Print an in Wordlay A, Jroj JML of Pretocal, Sec Her Pressed	and a the Program of a and a the data and a ministration of the terms of	iti Biyinta 129.21X.34 90.5191 Te	General Peralmonicals AN-1- Jan 201	

Gambar 1. Hasil capturing data ke <u>www.viva.co.id</u> menggunakan Wireshark

Dan berikut adalah hasil capturing data ke <u>www.viva.co.id</u> menggunakan CMD (netstat -a):

Active C	onnections		
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:445	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1536	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1537	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1538	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1539	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1540	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1541	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:5357	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:7680	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:1001	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:6543	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:30409	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:30409	www:31880	ESTABLISHED
TCP	127.0.0.1:31880	www:30409	ESTABLISHED
TCP	192.168.1.101:139	LENOVO-PC:0	LISTENING
TCP	192.168.1.101:14277	LENOVO-PC:0	LISTENING
TCP	192.168.1.101:31802	hk2sch130021958:https	ESTABLISHED
TCP	192.168.1.101:32017	sc-in-f188:5228	ESTABLISHED
TCP	192.168.1.101:32019	104.20.159.22:http	ESTABLISHED
TCP	192.168.1.101:32130	www:http	ESTABLISHED
TCP	192,168.1.101:32131	www:http	ESTABLISHED
TCP	192.168.1.101:32132	174.138.36.153:http	ESTABLISHED
TCP	192.168.1.101:32133	174.138.36.153:http	ESTABLISHED
TCP	192.168.1.101:32134	174.138.36.153:http	ESTABLISHED
TCP	192.168.1.101:32135	174.138.36.153:http	ESTABLISHED
TCP	192.168.1.101:32136	174.138.36.153:http	ESTABLISHED
TCP	192.168.1.101:32137	174.138.36.153:http	ESTABLISHED
TCP	192.168.1.101:32138	104.16.135.156:http	ESTABLISHED
TCP	192.168.1.101:32139	104.16.135.156:http	ESTABLISHED
		ADA AC ADD ADD LARD	PETADI TELIPO

Gambar 2. Hasil capturing data ke <u>www.viva.co.id</u> menggunakan CMD

Setelah dilakukan capturing data proses ke <u>www.viva.co.id</u> kita dapat mengetahui IP dan MAC Address milik perangkat kita dan IP dan MAC address milik perangkat website yang menjadi tujuan kita.

Tabel 1. IP dan MAC Address

S	ource	Des	stination
IP	MAC	IP	MAC
192.168.1.101	FC:DE:56:FF:01:06	202.129.216.26	FC:DD:55:4B:9C:2E

Kemudian, hasil capturing data yang telah diperoleh, kita filter berdasarkan IP dan MAC address pada tabel 1. Didapatlah hasilnya sebagai berikut:



Gambar 3.1. Hasil capturing data setelah di filter



Gambar 3.2. Hasil capturing data setelah di filter

	10003030000	10110011-001	TRUES LOOP	11.5	11.114 A. a. A. S. MARTEL, 14204 - 34, 1521 (Aug. 10) (AL-1423) (Br. 1883) (AL-1423)	
	NUMBER OF T	100000-000			(1) The disc sector states + minimal resolution and managements are as	
	los territori	Distance of the	ARC LANSING MAL		(1) AP and (0) and (1) areas in the line of our off and the state on the	
	artists who	Transaction of	Market Market		 OF My AN ADMIT ADDA + INC (A) AN ADVANCE IN ADMIT ADDA ADDA ADDA 	
	#18-38-3074EF	100.000.0000	101-107-120-38	151	11 (27) And 65 (6001) 1000 - 80 (20) 100 (21) Ad 1000 Ma 1000 by 1	
	795 18-83899	410.310.2.510	282-180-254-28		THE PART AND AND A DESCRIPTION OF A DESC	
	222,18:39:02:03	110.100.1100	T\$1.126.216.28	11.2	44 (218) + 25 (70) Start R. AMINA (A HE MONTAL STARK STARK STAR	
	771.16.307261	100.000.0.000	101.101.914.28	11-0	TT TATUE - AT LOCK - An est As est Muller and the estimate	
	712 36.827818	10:10.1:00	101.120.214.28	10120	1011 2017 A support and a STY/LT committee (spectrum) is a stell	
	215032-0010	140.310.31540	100103-00103-001	111	This of Managements and Aller + A Date (with the History History +	
- 5	0212.00M	340.018.0.540	30.126.214.38	11.4	(1) (204) + 32 (CE) in product Activity Reviewice Letter.	
	244537-221846	340.010.000	IN. 1.5 218.38	IL.	11 1210 - 12 1/cl.) we use the Ad-State Mar-which Lands	
	101117-010000	310.000.0.000	101.129.210.38	TC*	11 IIIII - II [/II] Ber B' Av IIIII He dato te 4	
	203 12-1993 0	102.101.1.101.	101-100-258-28	TES	11 YOM THE REPORT OF A DESCRIPTION OF A	
	2011/10.1A0821	142.142.1.40	197, 126, 214, 78	TLe.	11 12101 - 25 LOTE SHEME SHEME HERE AND A HERE AND A HERE	
	282 23.021423	102.139.4.1W	TEL 104 (114-218	12.0	11 12101 - 25 (PPL) OF C SHORE & SHOTEP ALMOSTIC LINES	
	404 21,2100,00	10.140.1.191	121.120.210.28	111	41 (2180 - 21 (CT) & -21276 J.A128 M4064 (- 4064	
	\$5.5 45.019181	10.130.1.100	281.120.014.28	.111	11 (200 x 40 (40), (94) 5-5009 (2002) 21+9900 (2004)	
					The Aller And Aller Al	

Gambar 3.3. Hasil capturing data setelah di filter

Dari ketiga gambar tersebut dapat kita ketahui bahwa paket data berdasarkan IP dan MAC address source dan destination adalah sebanyak 66 paket data dari 932 paket data secara keseluruhan.

IP Source	IP Destination	Info
		32129 80 [SYN] Seq=0 Win=64240
192.168.1.101	202.129.216.26	Len=0 MSS=1460 WS=256
		SACK_PERM=1
		32130 80 [SYN] Seq=0 Win=64240
192.168.1.101	202.129.216.26	Len=0 MSS=1460 WS=256
		SACK_PERM=1
		32131 80 [SYN] Seq=0 Win=64240
192.168.1.101	202.129.216.26	Len=0 MSS=1460 WS=256
		SACK_PERM=1
192 168 1 101	202 129 216 26	32129 80 [ACK] Seq=1 Ack=1
172.100.1.101	202.129.210.20	Win=66816 Len=0
192 168 1 101	202 129 216 26	32130 80 [ACK] Seq=1 Ack=1
172.100.1.101	202.129.210.20	Win=66816 Len=0
192 168 1 101	202 129 216 26	32131 80 [ACK] Seq=1 Ack=1
172.100.1.101	202.129.210.20	Win=66816 Len=0
192.168.1.101	202.129.216.26	GET / HTTP/1.1
192 168 1 101	202 129 216 26	32129 80 [FIN, ACK] Seq=738
		Ack=1120 Win=65792 Len=0
192.168.1.101	202.129.216.26	GET / HTTP/1.1
192.168.1.101	202.129.216.26	[TCP Retransmission] 32130 80 [PSH,
		ACK] Seq=1 Ack=1 Win=66816 Len=770
192.168.1.101	202.129.216.26	32130 80 [ACK] Seq=771 Ack=1395
		Win=66816 Len=0
		[TCP Dup ACK 253#1] 32130 80
192.168.1.101	202.129.216.26	[ACK] Seq=771 Ack=1395 Win=66816
		Len=0
		[TCP Dup ACK 253#2] 32130 80
192.168.1.101	202.129.216.26	[ACK] Seq=771 Ack=1395 Win=66816
		Len=0
		[TCP Dup ACK 253#3] 32130 80
192.168.1.101	202.129.216.26	[ACK] Seq=771 Ack=1395 Win=66816
		Len=0
100 1 00 1 101		[TCP Dup ACK 253#4] 32130 80
192.168.1.101	202.129.216.26	[ACK] Seq=//1 Ack=1395 Win=66816
		Len=0

Tabel 2. Info paket data setelah di filter

		[TCP Dup ACK 253#5] 32130 80
192.168.1.101	202.129.216.26	[ACK] Seq=771 Ack=1395 Win=66816
		Len=0
102 168 1 101	202 120 216 26	32130 80 [ACK] Seq=771 Ack=2789
192.108.1.101	202.129.216.26	Win=66816 Len=0
102 168 1 101	202 120 216 26	32130 80 [ACK] Seq=771 Ack=4183
192.108.1.101	202.129.210.20	Win=66816 Len=0
102 168 1 101	202 120 216 26	32130 80 [ACK] Seq=771 Ack=6971
192.108.1.101	202.129.210.20	Win=66816 Len=0
		[TCP Dup ACK 311#1] 32130 80
192.168.1.101	202.129.216.26	[ACK] Seq=771 Ack=6971 Win=66816
		Len=0
		[TCP Dup ACK 311#2] 32130 80
192.168.1.101	202.129.216.26	[ACK] Seq=771 Ack=6971 Win=66816
		Len=0
192.168.1.101	202.129.216.26	32130 80 [ACK] Seq=771 Ack=9759
1,2,100,1101		Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 80 [ACK] Seq=771 Ack=11153
1,2,100,1101		Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 80 [ACK] Seq=771 Ack=12547
		Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 80 [ACK] Seq=771 Ack=16729
		Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 80 [ACK] Seq=771 Ack=18123
		Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 80 [ACK] Seq=771 Ack=18326
		Win=66816 Len=0
192.168.1.101	202.129.216.26	32131 80 [ACK] Seq=1 Ack=2
		Win=66816 Len=0
192.168.1.101	202.129.216.26	32131 80 [FIN, ACK] Seq=1 Ack=2
		Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Dup ACK 462#1] 32131 80
		[ACK] Seq=2 Ack=2 Win=66816 Len=0
192.168.1.101	202.129.216.26	[TCP Retransmission] 32131 80 [FIN,
		ACK Seq=1 Ack=2 Win=66816 Len=0
192.168.1.101	202.129.216.26	32130 80 [ACK] Seq=771 Ack=18327
		W1n=66560 Len=0

192.168.1.101 202.129.216.26		32130 80 [FIN, ACK] Seq=771
172.100.1.101	202.129.210.20	Ack=18327 Win=66560 Len=0
		32163 80 [SYN] Seq=0 Win=64240
192.168.1.101	202.129.216.26	Len=0 MSS=1460 WS=256
		SACK_PERM=1
192 168 1 101	202 129 216 26	32163 80 [ACK] Seq=1 Ack=1
1/2.100.1.101	202.127.210.20	Win=66816 Len=0
		GET /indepth/fokus/951050-konflik-
192.168.1.101	202.129.216.26	rohingya-di-myanmar-membara-lagi
		HTTP/1.1
192 168 1 101	202 129 216 26	32163 80 [ACK] Seq=854 Ack=1395
192.100.1.101	202.129.210.20	Win=66816 Len=0
		[TCP Dup ACK 635#1] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=1395 Win=66816
		Len=0
		[TCP Dup ACK 635#2] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=1395 Win=66816
		Len=0
		[TCP Dup ACK 635#3] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=1395 Win=66816
		Len=0
		[TCP Dup ACK 635#4] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=1395 Win=66816
		Len=0
		[TCP Dup ACK 635#5] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=1395 Win=66816
		Len=0
		[TCP Dup ACK 635#6] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=1395 Win=66816
		Len=0
		[TCP Dup ACK 635#7] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=1395 Win=66816
		Len=0
102 168 1 101	202 120 216 26	32163 80 [ACK] Seq=854 Ack=12547
192.100.1.101	202.129.210.20	Win=66816 Len=0
102 168 1 101	202 120 216 26	32163 80 [ACK] Seq=854 Ack=13941
192.100.1.101	202.129.210.20	Win=66816 Len=0

102 168 1 101	202 129 216 26	32163 80 [ACK] Seq=854 Ack=16729
192.100.1.101	202.129.210.20	Win=66816 Len=0
102 169 1 101	202 120 216 26	32163 80 [ACK] Seq=854 Ack=18123
192.168.1.101	202.129.216.26	Win=66816 Len=0
		[TCP Dup ACK 663#1] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=18123 Win=66816
		Len=0
		[TCP Dup ACK 663#2] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=18123 Win=66816
		Len=0
		[TCP Dup ACK 663#3] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=18123 Win=66816
		Len=0
		[TCP Dup ACK 663#4] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=18123 Win=66816
		Len=0
		[TCP Dup ACK 663#5] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=18123 Win=66816
		Len=0
		[TCP Dup ACK 663#6] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=18123 Win=66816
		Len=0
		Len=0 32168 80 [SYN] Seq=0 Win=64240
192.168.1.101	202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
192.168.1.101	202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.101	202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1
192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Win=0 HTTP/1.1
192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Win=66816 HTTP/1.1 POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded) HTTP/1.1
192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Win=66816 Len=0 POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded) 80 [PSH,
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 32168 80 [ACK] Seq=1 Ack=1 Ack=1 Win=66816 Len=0 HTTP/1.1 (application/x-www-form-urlencoded) 80 [PSH, ACK] Seq=1 Ack=1 ACK] Seq=1 Ack=1 Win=66816
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Win=66816 Len=0 POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded) ITCP Retransmission] 32168 80 [PSH, ACK] Seq=1 Ack=1 Win=66816
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Win=66816 HTTP/1.1 POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded) 80 [PSH, ACK] Seq=1 Ack=1 Win=66816 Len=1069 32163 80 [ACK] Seq=854 Ack=19517
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 VS VS POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded) 80 [PSH, ACK] Seq=1 Ack=1 Vin=66816 Len=1069 Vin=66816 S2163 80 [ACK] Seq=854 Ack=19517 Win=66816 Len=0 Vin=66816
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Win=66816 Len=0 POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded) [TCP Retransmission] 32168 80 [PSH, ACK] Seq=1 Ack=1 Win=66816 Len=1069 32163 80 [ACK] Seq=854 Ack=19517 Win=66816 Len=0 32168 80 [ACK] Seq=1070 Ack=1267
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Win=66816 Len=0 POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded) ITCP Retransmission] 32168 80 [PSH, ACK] Seq=1 Ack=1 Win=66816 Len=1069 32163 80 [ACK] Seq=854 Ack=19517 Win=66816 Len=0 32168 80 [ACK] Seq=1070 Ack=1267 Win=65536 Len=0 Win=65536 Len=0
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26 202.129.216.26	Len=0 32168 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 32168 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Vost Vost POST /request/comment HTTP/1.1 (application/x-www-form-urlencoded) 80 [PSH, ACK] Seq=1 Ack=1 Win=66816 Len=1069 32163 80 [ACK] Seq=854 Ack=19517 Win=66816 Len=0 32168 80 [ACK] Seq=1070 Ack=1267 Win=65536 Len=0 32163 80 [ACK] Seq=854 Ack=21858

		[TCP Dup ACK 764#1] 32163 80
192.168.1.101	202.129.216.26	[ACK] Seq=854 Ack=21858 Win=66816
		Len=0
102 168 1 101	202 120 216 26	32163 80 [ACK] Seq=854 Ack=21859
192.100.1.101	202.129.210.20	Win=66816 Len=0
192 168 1 101	202 129 216 26	32163 80 [FIN, ACK] Seq=854
1)2.100.1.101	202.129.210.20	Ack=21859 Win=66816 Len=0
102 168 1 101	202 120 216 26	32168 80 [ACK] Seq=1070 Ack=1268
192.100.1.101	202.129.210.20	Win=65536 Len=0
102 168 1 101	202 129 216 26	32168 80 [FIN, ACK] Seq=1070
172.100.1.101	202.129.210.20	Ack=1268 Win=65536 Len=0
		1

Dari tabel tersebut dapat kita ketahui bahwa, tabel yang berwarna hitam merupakan paket data yang bermasalah. Sedangkaan tabel yang berwarna hijau merupakan paket data dengan protokol HTTP, dan tabel yang putih merupakan paket data dengan protokol TCP.

V. ANALISA PAKET DATA : ONLINE STREAMING MENGGUNAKAN WIRESHARK DAN CMD

Adapun website online streaming yang akan dibrowsing yang kemudian paket datanya di analisa adalah <u>www.indomovie.tv</u> yang merupakan salah satu situs online streaming Indonesia.

Berikut adalah hasil capturing data ke <u>www.indomovie.tv</u> menggunakan Wireshark:

Time			Contraction of the last	and of the second se	and the second se
	Barra .	19494-0001	Freed	tangin laris	
230.12.576446	101104-0.1	00.104.1.141	1001	of bisking any reprise heats larger fillers fit best drained area.	
221, 75, 216941	242,348,4,384	102.568 A.A	DNC	AT Sharehard supery \$100000 STE 200 AT 201 Unit for and args	
258 13 755647	242.188.4.1	PRG 068.1.184	Des	al transferd sport response Autobic Server Autors PTA 200-42 (Ad. 104 St. Adv. organ	
296 13:75MILL	100.000.0.00	294-168-1-1	DAC	BT Mandard sparty Bolling PTE per al 254 100 10 and a per	
100 11.000001	101.101.1.1.	001.000.1.001	1995	all transmitting upper response housing housing failures fill and 42 244 185 or only artist	
341 13.815441	202.102.1.341	184.244.43.298	1810	TO DATE SHOULD BE AND A TO A DECIDENT AND A DECIDEN	
ALL D. HULL	294.388.42,286	292.545.1.185	2179	W DetElation shree ball on grant second and	
201 13,311,09	CONTRACTORS	CONTRACTOR OF	10.44	The set office to be a set of the	12
109.11.111101	199.25.79.218	1. 101.2(0.1.10)	TIP	14 18 - 34428 [ALK] BOH-CITER AD-1ANY INV-12188 (AV-6	
	1000 NO. 10. ALC	THE PART OF		- LANE INT PROVIDENT HER CONTINUES INTO ANY	
100111-32500	104.01 10.00			THE TWO DOT TO THE REAL PROPERTY AND A DAMAGE THE PARTY AND A DEPARTMENT OF A DAMAGE.	- C
101 (1, 41000)	101.004.0.101	C BREAT AND A CHIEF.	110	IN 157 24 AN UNCERTAINT AND ACCOUNTS AND ADDRESS AND ADDRES	
388 11.1703#4	- BUINT BUILDER	1994,71.19.208	100	THE DAMAGE A BE TRUE TO A STRETCH AND A DAMAGED TO A DAMA	
Her LI Stende	104 11-34-110	THE DESIGNATION	THE	Land Child State On Section 2 (in the Section 2) State	
The Tartinger	104(10:20-110	100.009.1-101	66.28	AND AND INCOME INCOME.	
370.13.200190	102.088CE.109	044-11-16-200	TLP	an and a fact and the second second second second	
111 11 10000F	100.11.12.114	883.108.1.181	10.28	LALE Fortunation	1.00
274 13-294141	242.348.1.361	361,51,78,154	TOP	14 Julie + Br [mil] Selection schedular consults cause	
- International	CONTRACTOR OF STREET	- Internet and the		THE UP ANY LOD DESCRIPTION OF THE CONTRACTOR	
The state of the s	100000		17.14	10 10 Percent and the second stations	
and YE'rear	104, 24, 28, 110	UNUMUM	10.04	PH Table publication	
THUR HAR	A REAL PROPERTY AND A REAL	「「「「「」」		A AN AN ANALY THE AN ANALY CARD AND AND AND AND AND AND AND AND AND AN	100 C
THE EXCLUSION OF		INC. INCOME.		The second	THE STREET
	And in the local data in the local	the local sector of the sector of the	111		IT I HILL I
Company 2011 Test Byte	farmini state (1996) and	Forder, bar, Progenser, 20	to these as	No. an anterface B. e. Marke Dr. (Recold Will Barke da)	
Internet Sectoral	variables A. Birds 1982	348.1.281. 048. 184.1	11.75.205		
Transmission Courts	al Protocol, Dra Per	PL PHON, DAP PARTY I	N. 145-18	6, addr 18712, lawr 198	
bisites Parts 18					

Gambar 4. Hasil capturing data ke <u>www.indomovie.tv</u> menggunakan Wireshark

Dan berikut adalah hasil capturing data ke <u>www.indomovie.tv</u> menggunakan CMD (netstat -a):

C:\Users	<pre>\rofby>netstat -a</pre>		
Active C	Connections		
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:445	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1536	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1537	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1538	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1539	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1540	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:1541	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:5357	LENOVO-PC:0	LISTENING
TCP	0.0.0.0:27036	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:1001	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:6543	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:27060	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:30409	LENOVO-PC:0	LISTENING
TCP	127.0.0.1:30409	www:34316	ESTABLISHED
TCP	127.0.0.1:34316	www:36469	ESTABLISHED
TCP	192.168.1.101:139	LENOVO-PC:0	LISTENING
TCP	192.168.1.101:14277	LENOVO-PC:0	LISTENING
TCP	192.168.1.101:33477	hk2sch130021929:https	ESTABLISHED
TCP	192.168.1.101:33583	103.28.54.12:27021	ESTABLISHED
TCP	192.168.1.101:34314	sc-in-f188:5228	ESTABLISHED
TCP	192.168.1.101:34315	104.20.158.22:http	ESTABLISHED
TCP	192.168.1.101:34341	104.244.42.200:https	ESTABLISHED
TCP	192.168.1.101:34357	sc-in-f103:https	ESTABLISHED
TCP	192.168.1.101:34371	104.16.61.155:https	ESTABLISHED
TCP	192.168.1.101:34378	sb-in-f94:https	ESTABLISHED
TCP	192.168.1.101:34382	104.28.8.5:https	ESTABLISHED
TCP	192.168.1.101:34383	104.20.70.47:https	ESTABLISHED
TCP	192.168.1.101:34389	104.18.59.68:https	ESTABLISHED
TCP	192.168.1.101:34395	151.101.24.193:http	ESTABLISHED
TCP	192.168.1.101:34397	104.20.69.47:https	ESTABLISHED
TCP	192.168.1.101:34399	68.232.45.48:https	ESTABLISHED
TCP	192.168.1.101:34402	arn02s05-in-f131:https	ESTABLISHED
TCP	192.168.1.101:34404	ec2-52-207-92-154:http	s CLOSE_WAIT
TCP	192.168.1.101:34406	sa-in-f94:https	ESTABLISHED
TCP	192.168.1.101:34408	sin11s03-in-f46:http	ESTABLISHED

Gambar 5.1. Hasil capturing data ke <u>www.indomovie.tv</u>

menggunakan CMD

TCP	[::]:445	LENOVO-PC:0	LISTENING
TCP	[::]:1536	LENOVO-PC:0	LISTENING
TCP	[::]:1537	LENOVO-PC:0	LISTENING
TCP	[::]:1538	LENOVO-PC:0	LISTENING
TCP	[::]:1539	LENOVO-PC:0	LISTENING
TCP	[::]:1540	LENOVO-PC:0	LISTENING
TCP	[::]:1541	LENOVO-PC:0	LISTENING
TCP	[::]:5357	LENOVO-PC:0	LISTENING
UDP	0.0.0.0:123	*:*	
UDP	0.0.0:3702	*:*	
UDP	0.0.0.0:3702	*:*	
UDP	0.0.0.0:5050	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5355	· · · ·	
UDP	0.0.0.0:27036	* *	
UDP	0.0.0:49830	*:*	
UDP	0.0.0.0:51168	* *	
UDP	0.0.0:52370	* : *	
UDP	0.0.0.0:55566	* : *	
UDP	0.0.0.0:55619	* : *	
UDP	0.0.0.0:55622	*:*	
UDP	0.0.0.0:57965	* *	
UDP	0.0.0.0:62176	* *	
UDP	0.0.0.0:63470	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	127.0.0.1:53382	* : *	
UDP	127.0.0.1:57762	* *	
UDP	192.168.1.101:137	* *	
UDP	192.168.1.101:138	* *	
UDP	192.168.1.101:1900	* *	
UDP	192.168.1.101:14277	* *	
UDP	192.168.1.101:57761	*:*	
UDP	[::]:123	* : *	
UDP	[::]:3702	*:*	

Gambar 5.2. Hasil capturing data ke <u>www.indomovie.tv</u>

menggunakan CMD

UDP	[::]:3702	* *	
UDP	[::]:5353	*:*	
UDP	[::]:5353	* • *	
UDP	[::]:5355	*:*	
UDP	[::]:55567	* : *	
UDP	[::]:57966	* : *	
UDP	[::]:62177	* : *	
UDP	[::]:63470	*:*	
UDP	[::1]:1900	* : *	
UDP	[::1]:57760	* • *	
UDP	[fe80::a429:32c5	:b626:c7ce%21]:1900	* *
UDP	[fe80::a429:32c5	:b626:c7ce%21]:57759	*:*

Gambar 5.3. Hasil capturing data ke <u>www.indomovie.tv</u> menggunakan CMD

Setelah dilakukan capturing data proses ke <u>www.indomovie.tv</u> kita dapat mengetahui IP dan MAC Address milik perangkat kita dan IP dan MAC address milik perangkat website online streaaming yang menjadi tujuan kita.

S	ource	Des	stination
IP MAC		IP	MAC
192.168.1.101	FC:DE:56:FF:01:06	104.31.78.216	FC:DD:55:4B:9C:2E

Tabel 3. IP dan MAC Address

Kemudian, hasil capturing data yang telah diperoleh, kita filter berdasarkan IP dan MAC address pada tabel 3. Didapatlah hasilnya sebagai berikut:



Gambar 6.1. Hasil capturing data setelah di filter

_					
	LIVE STORE	the most state	101 2021-020	- 16.6	CONTRACTOR CONTRA
14	381.11.331.04	181.182.3.341	101 . A. A. A. A.	11.14	Ave Auto 700 em control de aveca de la terraria
	396.03.900.000	10011071-001	100012-00000	10.4	(1) The Disconstruction of the product of the second se
	20. 40.20.M.	120.10/0.001	ALC: March and	14.65	to their way (way) second deviations, they are set from over the
	ALLANG ALL DIS	101-102-1-121	Wet Sectionals	15.6	12-12-42 + 62 (403) SEC-102 MOVE MOVE AND ADDRESS COMPANY
	375 LL 390145	137 150 1.424	104.01.70.810	16.2	SA DHUS A BY (ACC) SIGNACE ASSACD? HERADOLUMAN
	REAL PROPERTY.	124 1142 11 101	104.35.30.300	TC2	THE REPORT OF A DESCRIPTION OF A DESCRIP
	in the second	1002-007 AC444			The same of where a first sign and where she was set of the second and and and and the second s
	in least	101 102 103	an and the		an and prove out which have not were same allowed by any problem. An early a second second second second second
1	A.U. 46	151 110.3.341	160 Sectional	11.4	AN UNIT A BE (ALC) SECTION REPORT AND AND A DRIVE STATISTICS AND A DRIVE AND A
	Paraterial As	194-160.0.941	100 Sections	160	se prece e av texel septembring researcher rendered carrie
	AMMA: LT.	U.S. 100 1, 101	204 Automatic	1104	3. D. C. M. AND MAD 2448 - COMMONDARY AND ADDRESS INCOMES INTO ADDRESS AND ADDRE ADDRESS AND ADDRESS AND ADDRE ADDRESS AND ADDRESS AND ADDR ADDRESS AND ADDRESS
	ALL LAND	UNITARY AND			the INTERVAL AND MARK & CASE OF SHE AS A REPORT OF AND AN AN AN AN AN AN
-	12/24.46.004	DOC: 180. 3. 341	340. A. M. St.	31.19	Average and the restrict of the propagation of a statement is a section of a sector of the statement of the sector
-	400 W.L.L.M.M.	and seed to set	13.4. S 1	11.4	th press wire (rece) see and not draw rate care in
	14.4	CR4.16V.0.101	609-32.71 AL	1.63	Dr. Weith + eV (111, VDV) seg-L reck Links-could her-to
	242.42.40144	171.107.3.107	105 2. 71 125	15.4	24 2962 + 60 111, 620 2691 Asset the e2000 cm-6
	11.01.00.00	157 167 1 161	101.01.21.328	11.4	by 1961 + 86 (41, 720) mart Acort Martinita Level
	178 million	187, 186, 1, 197	184	11.8	the state was (see, state) and a solution state and a
	25.00.00.00	LTL 160.3 161	10. 2. 11.10	10.0	in the state of th
	10.00.00.00.00.0	171.107.3.501	10. S. A. &.	11.4	th under why physical card a state budge base of
	375 23. 28242	101 107 1 101	101.10.01.00.008	12.4	8" STALL + 68 (NC) Say's Yak'd La-68038 Low-0
	170 18 240 012	DU., the 1, 197	101.01.01.00.008	12.4	WY STOLD + BU [AND] Negot Yik-D bis-Bullt Los-T
	100-10-12-014	101 1101 3 141	107. N O 116	11.4	WT 2768 + BK TCC SeyS CLASS AN HURLE Lee 8
	- and the should be	100 TALL & 107	100 0 00000	12.0	The state a particular state with a state party tax of

Gambar 6.2. Hasil capturing data setelah di filter

Dari ketiga gambar tersebut dapat kita ketahui bahwa paket data berdasarkan IP dan MAC address source dan destination adalah sebanyak 49 paket data dari 4.888 paket data secara keseluruhan.

IP Source	IP Destination	Info
		34409 80 [SYN] Seq=0 Win=64240
192.168.1.101	104.31.78.216	Len=0 MSS=1460 WS=256
		SACK_PERM=1
		34410 80 [SYN] Seq=0 Win=64240
192.168.1.101	104.31.78.216	Len=0 MSS=1460 WS=256
		SACK_PERM=1
		34411 80 [SYN] Seq=0 Win=64240
192.168.1.101	104.31.78.216	Len=0 MSS=1460 WS=256
		SACK_PERM=1
		34412 80 [SYN] Seq=0 Win=64240
192.168.1.101	104.31.78.216	Len=0 MSS=1460 WS=256
		SACK_PERM=1
		34413 80 [SYN] Seq=0 Win=64240
192.168.1.101	104.31.78.216	Len=0 MSS=1460 WS=256
		SACK_PERM=1
		34414 80 [SYN] Seq=0 Win=64240
192.168.1.101	104.31.78.216	Len=0 MSS=1460 WS=256
		SACK_PERM=1
192 168 1 101	104 31 78 216	34410 80 [ACK] Seq=1 Ack=1
192.100.1.101	104.51.70.210	Win=66816 Len=0
192 168 1 101	104 31 78 216	34409 80 [ACK] Seq=1 Ack=1
192.108.1.101	104.51.70.210	Win=66816 Len=0

Tabel 4. Info paket data setelah di filter

192.168.1.101	104.31.78.216	34411 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Image: Constraint of the second
192.168.1.101	104.31.78.216	34413 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0 Image: Constraint of the second
192.168.1.101	104.31.78.216	34414 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	34412 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
192.168.1.101	104.31.78.216	GET / HTTP/1.1
192.168.1.101	104.31.78.216	[TCP Dup ACK 68#1] 34410 80 [ACK] Seq=685 Ack=1 Win=66816 Len=0 SLE=1395 SRE=2789
192.168.1.101	104.31.78.216	34410 80 [ACK] Seq=685 Ack=2789 Win=66816 Len=0
192.168.1.101	104.31.78.216	34410 80 [ACK] Seq=685 Ack=5334 Win=66816 Len=0
192.168.1.101	104.31.78.216	[TCP Dup ACK 159#1] 34410 80 [ACK] Seq=685 Ack=5334 Win=66816 Len=0 SLE=6728 SRE=8122
192.168.1.101	104.31.78.216	[TCP Dup ACK 159#2] 34410 80 [ACK] Seq=685 Ack=5334 Win=66816 Len=0 SLE=9516 SRE=10910 SLE=6728 SRE=8122
192.168.1.101	104.31.78.216	[TCP Dup ACK 159#3] 34410 80 [ACK] Seq=685 Ack=5334 Win=66816 Len=0 SLE=12304 SRE=13698 SLE=9516 SRE=10910 SLE=6728 SRE=8122
192.168.1.101	104.31.78.216	34410 80 [ACK] Seq=685 Ack=8122 Win=66816 Len=0 SLE=12304 SRE=13698 SLE=9516 SRE=10910
192.168.1.101	104.31.78.216	[TCP Dup ACK 167#1] 34410 80 [ACK] Seq=685 Ack=8122 Win=66816 Len=0 SLE=9516 SRE=13698
192.168.1.101	104.31.78.216	34410 80 [ACK] Seq=685 Ack=13698 Win=66816 Len=0
192.168.1.101	104.31.78.216	34410 80 [ACK] Seq=685 Ack=13718 Win=66816 Len=0 SLE=5334 SRE=6728

		[TCP Dup ACK 174#1] 34410 80
192.168.1.101	104.31.78.216	[ACK] Seq=685 Ack=13718 Win=66816
		Len=0 SLE=8122 SRE=9516
		[TCP Dup ACK 174#2] 34410 80
192.168.1.101	104.31.78.216	[ACK] Seq=685 Ack=13718 Win=66816
		Len=0 SLE=10910 SRE=12304
192.168.1.101	104.31.78.216	GET /the-hitmans-bodyguard/ HTTP/1.1
	104.31.78.216	[TCP Dup ACK 174#3] 34410 80
192.168.1.101		[ACK] Seq=1430 Ack=13718 Win=66816
		Len=0 SLE=16506 SRE=17900
		34410 80 [ACK] Seq=1430 Ack=15112
192.168.1.101	104.31.78.216	Win=66816 Len=0 SLE=16506
		SRE=17900
102 168 1 101	104 21 78 216	34410 80 [ACK] Seq=1430 Ack=17900
192.108.1.101	104.31.78.210	Win=66816 Len=0
102 168 1 101	10/ 31 78 216	34410 80 [ACK] Seq=1430 Ack=20327
192.108.1.101	104.31.78.210	Win=66816 Len=0
		[TCP Dup ACK 273#1] 34410 80
192.168.1.101	104.31.78.216	
192.168.1.101	104.31.78.210	[ACK] Seq=1430 Ack=2032 / Win=66816
192.168.1.101	104.51.78.210	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115
192.168.1.101	104.51.78.210	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80
192.168.1.101	104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816
192.168.1.101 192.168.1.101	104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328
192.168.1.101 192.168.1.101	104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115
192.168.1.101	104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80
192.168.1.101 192.168.1.101	104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816
192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348
192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 [SLE=24509 SRE=25348 SLE=21721 SRE=23115 SRE=25348
192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216 104.31.78.216 104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 34410 80 [ACK] Seq=1430 Ack=23115
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216 104.31.78.216 104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 34410 80 [ACK] Seq=1430 Ack=23115 Win=66816 Len=0 SLE=24509
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216 104.31.78.216 104.31.78.216 104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 34410 80 [ACK] Seq=1430 Ack=23115 Win=66816 Len=0 SLE=24509 SRE=25348
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216 104.31.78.216 104.31.78.216 104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 34410 80 [ACK] Seq=1430 Ack=23115 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=24509 SRE=25348 34410 80 [ACK] Seq=1430 Ack=25348
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216 104.31.78.216 104.31.78.216 104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 RCK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 34410 80 [ACK] Seq=1430 Ack=23115 Win=66816 Len=0 SRE=25348 34410 80 [ACK] Seq=1430 Ack=25348 Win=66816 Len=0 SRE=25348
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216 104.31.78.216 104.31.78.216 104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 RCK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=23115 [TCP Dup ACK 273#3] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 34410 80 [ACK] Seq=1430 Ack=23115 Win=66816 Len=0 SRE=25348 34410 80 [ACK] Seq=1430 Ack=25348 Win=66816 Len=0 SLE=24509 SRE=25348 34410 80 [ACK] Seq=1430 Ack=25348
192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	104.31.78.216 104.31.78.216 104.31.78.216 104.31.78.216 104.31.78.216	[ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=21721 SRE=23115 [TCP Dup ACK 273#2] 34410 80 [ACK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25328 SLE=21721 SRE=23115 [TCP Dup ACK 273#3] 34410 RCK] Seq=1430 Ack=20327 Win=66816 Len=0 SLE=24509 SRE=25348 SLE=21721 SRE=23115 34410 80 [ACK] Seq=1430 Ack=23115 Win=66816 Len=0 SRE=25348 34410 80 [ACK] Seq=1430 Ack=25348 Win=66816 Len=0 SRE=25348 34410 80 [ACK] Seq=1430 Ack=25348 Win=66816 Len=0 [TCP Dup ACK 283#1] 34410 80 [ACK] Seq=1430 Ack=25348 Win=66816

		[TCP Dup ACK 283#2] 34410 80
192.168.1.101	104.31.78.216	[ACK] Seq=1430 Ack=25348 Win=66816
		Len=0 SLE=20327 SRE=21721
192.168.1.101	104.31.78.216	GET /wp-admin/admin-
		ajax.php?postviews_id=16814&action=po
		stviews&_=1504035932782 HTTP/1.1
102 169 1 101	104.31.78.216	34410 80 [ACK] Seq=2172 Ack=25818
192.108.1.101		Win=66304 Len=0
102 168 1 101	104.31.78.216	34409 80 [FIN, ACK] Seq=1 Ack=1
192.108.1.101		Win=66816 Len=0
102 168 1 101	104 21 79 216	34413 80 [FIN, ACK] Seq=1 Ack=1
192.108.1.101	104.31.78.210	Win=66816 Len=0
102 168 1 101	104.31.78.216	34411 80 [FIN, ACK] Seq=1 Ack=1
192.108.1.101		Win=66816 Len=0
102 168 1 101	104.31.78.216	34414 80 [FIN, ACK] Seq=1 Ack=1
192.108.1.101		Win=66816 Len=0
100 100 1 101	104 21 79 216	34412 80 [FIN, ACK] Seq=1 Ack=1
192.108.1.101	104.51.78.210	Win=66816 Len=0
192.168.1.101	104.31.78.216	34411 80 [ACK] Seq=2 Ack=2
		Win=66816 Len=0
102 168 1 101	104.31.78.216	34413 80 [ACK] Seq=2 Ack=2
192.108.1.101		Win=66816 Len=0
102 168 1 101	104.31.78.216	34414 80 [ACK] Seq=2 Ack=2
192.108.1.101		Win=66816 Len=0
102 168 1 101	104.31.78.216	34409 80 [ACK] Seq=2 Ack=2
192.100.1.101		Win=66816 Len=0
102 168 1 101	104.31.78.216	34412 80 [ACK] Seq=2 Ack=2
192.108.1.101		Win=66816 Len=0

Dari tabel tersebut dapat kita ketahui bahwa, tabel yang berwarna hitam merupakan paket data yang bermasalah. Sedangkaan tabel yang berwarna hijau merupakan paket data dengan protokol HTTP, dan tabel yang putih merupakan paket data dengan protokol TCP.