## Task V Jaringan Komputer



Disusun Oleh :

Nama: Sigit Wijaya PramonoNim: 09011181419012Kelas: SK.5A

Dosen Pengampuh : Dr. Deris Stiawan, M.T.

## JURUSAN SISTEM KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA 2016

## Capturing dan Analisa Protokol Jaringan Menggunakan Wireshark dan CMD

Pada tugas kali ini yaitu mengcapture traffic atau paket-paket data pada suatu jaringan yang menggunakan software wireshark, setelah mengcapture terdapat banyak sekali IP - IP dan protokol muncul dalam software wireshark. Setelah memulai mengcapture kita membuka browser dan browsing suatu website dengan tujuan agar tercapture oleh aplikasi wireshark dan untuk selanjutnya akan dianalisa lalu dibangingkan dengan hasil capture menggunakan cmd. Selain menggunakan wireshark, capturing juga menggunakan cmd dengan command netstat –a.

Dibawah berikut merupakan screenshoot dari hasil capturing menggunakan aplikasi wireshark dengan destisani web kompas.com :

<b>4</b> *1	A/i - Ei				<b>—</b> - 6	×			
File	Edit View Go	Canture Analyze Stati	stics Telenhony Wireless	Tools H		~			
	🔳 🖉 🛞 📙 🔚	🗙 🖾 🔍 ⇔ ⇔ 🕾	₩ 4 = = 0.0	Q, II					
h	tto			•	Expression.	+			
No	Time	Source	Destination	Protocol	Leadh Infa	-			
1	10806 85 055951	54 82 233 105	192 168 43 12	HTTP	518 HTTP/1 1 200 0K				
	10845 85 220070	192 168 43 12	139 162 146 37	HTTP	473 GFT /2 cmsrc_annosyuc&idt=100&did=607709701719623529 HTTP/1 1				
	10846 85,220887	192,168,43,12	118.98.95.56	HTTP	849 GET /pins t=14742779630538ps c=UTE-88ps ad brt=9398ps p=14742779620398c1=38c3= e0 6950258c4=391084278c5=_				
	10848 85,221455	192,168,43,12	118.98.95.41	HTTP	94 GET /p2ns t=14742779631408ns c=UTF-88uid=ebBannerIFrame 39108427 96999343058447448(1=38c3= e0 6950258c4=3_				
	10854 85.256505	4.26.67.16	192.168.43.12	HTTP	464 HTTP/1.1 200 OK (text/javascript)				
1	10871 85.346932	118.98.95.56	192.168.43.12	HTTP	363 HTTP/1.1 200 0K (GIF89a) (GIF89a) (image/gif)				
1	10908 85.441238	118.98.95.41	192.168.43.12	HTTP	363 HTTP/1.1 200 0K (GIF89a) (GIF89a) (image/gif)				
-> 1	10934 85.515457	192,168,43,12	180,250,127,114	HTTP	523 GET /data/2014/kompascom/images/favicon.ico HTTP/1.1				
1	11112 85.752681	139.162.146.37	192.168.43.12	HTTP	471 HTTP/1.1 200 0K (GIF89a) (GIF89a) (image/gif)				
+ 1	11116 85.830320	180.250.127.114	192.168.43.12	HTTP	1204 HTTP/1.1 200 OK (text/plain)				
1	11119 86.150531	192.168.43.12	74.125.200.155	HTTP	1135 GET /activeview?avi=BH-S20LLfV6qYLNjBogOXt5u4CwAAAAAQATgByAEJwAIC4AIA4AQBoAYw&cid=CAASFeRoIRKN4-1Nh DZXYPJH				
1	11132 86.345333	74.125.200.155	192.168.43.12	HTTP	524 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)				
1	11331 96.456399	202.78.199.195	192.168.43.12	HTTP	54 HTTP/1.0 400 Bad request (text/html)				
1	11472 107.910200	192.168.43.12	202.78.199.195	HTTP	836 GET /247/adServer/act interaction/cid 1472718023/bid 1472773747/pid 1330508896/wid 1397192086/zid 139719218_				
1	11476 108.021290	202.78.199.195	192.168.43.12	HTTP	54 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)				
1	11488 110.799983	192.168.43.12	202.78.199.195	HTTP	838 GET /247/adServer/act interaction/cid 1472718023/bid 1472773747/pid 1330508896/wid 1397192086/zid 139719218_				
1	11491 110.896537	202.78.199.195	192.168.43.12	HTTP	54 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)				
1	11511 113.429630	192.168.43.12	118.98.95.41	HTTP	75 GET /p?ns_t=1474277991367&ns_c=UTF-8&c1=3&c3=_es_695025&c4=39108427&c5=18508020&c10=1&c11=Xaxis%205G&c13=_				
1	11522 113.636686	192.168.43.12	69.172.216.111	HTTP	1277 GET /dt?anId=8022&asId=79c2cd93-b367-4640-63d7-ee744de172a5&tv={c:oM1qhL,pingTime:0,time:32222,type:pf,fc:0				
1	11528 113.756947	118.98.95.41	192.168.43.12	HTTP	363 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)				
1	11541 114.031975	69.172.216.111	192.168.43.12	HTTP	277 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)				
1	11550 114.386014	192.168.43.12	74.125.200.155	HTTP	1151 GET /activeview?avi=BcKk2OLLfV6uYLNjBogOXt5u4CwAAAAQATgByAEJwAIC4AIA4AQBoAYW&cid=CAASFeRo3_vJvY-2RZ5fRZTyo…	~			
> F	rame 10934: 523 b	ytes on wire (4184 b	oits), 523 bytes captur	ed (4184	bits) on interface 0	^			
> E	thernet II, Src:	LiteonTe_88:dc:a9 (2	24:fd:52:88:dc:a9), Dst	: Asustek	C_34:d8:db (14:dd:a9:34:d8:db)				
> 1	nternet Protocol	Version 4, Src: 192.	168.43.12, Dst: 180.25	0.127.114					
> T	ransmission Contr	ol Protocol, Src Por	rt: 53645, Dst Port: 80	, Seq: 27	933, Ack: 119562, Len: 469	~			
000	0 14 dd a9 34 d8	db 24 fd 52 88 dc	a9 08 00 45 004.	.\$. R	.E.	^			
001	0 01 fd 6f d4 40	00 40 06 a9 05 c0	a8 2b 0c b4 fao.@	).@+					
002	0 7f 72 d1 8d 00	50 06 97 17 41 60	c0 4f 0b 50 18 .r	PA`.0	.P.				
003	0 00 fc 30 12 00	00 30 5a 6e 64 6a	41 58 5a 47 540	.0Z ndjOX	ZGT				
004	0 00 00 49 00 54 0 6c 56 6d 57 55	- +a uc bb /a +e /4 - 5a 78 57 58 6c 35	+e 33 40 40 52 VIIVI 65 6a 52 63 4c 1VmM	JIV ZNCNJ IZVU X15ei	rnn Rei				
006	0 31 6c 31 4f 45	31 4c 55 30 46 5a	4e 54 49 7a 4e 1110E	1LU ØFZNT					
007	0 7a 4e 32 4d 6d	38 72 57 54 68 36	58 43 39 4b 63 zN2Mm	8rW Th6XC	9Kc				
008	0 45 78 34 61 47	68 78 55 48 70 4c	54 57 31 6c 4e Ex4aG	ihxU HpLTW	11N	~			
Fran	Frame (523 bytes) Reassentibled TCP (1869 bytes)								
0	Wypertext Transfer Protocol: Protocol Profile: Default								

Terlihat dari gambar diatas beberapa dari hasil capture traffic / paket-paket data yang termasuk dalam satu jaringan tersebut. Selanjutnya ini merupakan capture dari *GET* yang terdapat dalam salah satu IP pada hasil capture di wireshark yang mana IP tersebut sama seperti web yang saya cari dalam broser :

Wireshark · Packet 10934 · wireshark_85BD8EB0-0F2F-4DB0-95B6-FB03	EED56416_20160919163755_a04288				_	- [	1)	<
Host: assets kompas com\r\n							-	•
Connection: keep-alive\r\n								
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)	AppleWebKit/537.36 (KHTML, li	ke Gecko) Chr	ome/49.0.2623	.87 Safari/537.	36\r\n			
Accept: */*\r\n Referer: http://otomotif.kompas.com/produkmotor\r	·\n							
Accept-Encoding: gzip, deflate, sdch\r\n								
Accept-Language: en-US,en;q=0.8\r\n								
<pre>&gt; [truncated]Cookie:gads=ID=60cfdd4ea111f4a9:T= )aba</pre>	1460205071:S=ALNI_MaNy3qFNBVE	0EjY0-0425I	iUa6g; _em_vt:	=26fc094d3140b7	/ba7defa185182/	456e53o	:9d966	
[Full request URI: http://assets.kompas.com/data/	2014/kompascom/images/favicor	.icol						
[HTTP request 15/15]								
[Prev request in frame: 7818]								
[Response in frame: 11116]		_						*
	GET /dat a/2014/k							-
0010 6f 6d 70 61 73 63 6f 6d 2f 69 6d 61 67 65 73 2f	ompascom /images/							î.
0020 66 61 76 69 63 6f 6e 2e 69 63 6f 20 48 54 54 56	favicon. ico HTTP							а.
0040 74 73 2e 6b 6f 6d 70 61 73 2e 63 6f 6d 0d 0a 43	ts.kompa s.comC							
0050 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 20	onnectio n: keep-							
0000 61 6c 69 76 65 00 0a 55 73 65 72 20 41 67 65 66 0070 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28	aliveU ser-Agen t: Mozil la/5.0 (							
0080 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3t	Windows NT 10.0;							
0090 20 57 4t 57 36 34 29 20 41 70 70 6c 65 57 65 62 00a0 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 40	WOW64) AppleWeb Kit/537.36 (KHTM							
00b0 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 4	L, like Gecko) C							
00c0 68 72 6f 6d 65 2f 34 39 2e 30 2e 32 36 32 33 2e 00d0 38 37 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36	hrome/49 .0.2623.							
00e0 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 52	Accept : */*R							
00f0 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 6f 0100 74 6f 6d 6f 74 69 66 2e 6b 6f 6d 70 61 73 2e 63	eferer: http://o tomotif kompas c							J
Frame (523 bytes) Reassembled TCP (1869 bytes)	comperie kompaste						-	_
No.: 10934 · Time: 85.515457 · Source: 192.168.43.12 · Destination: 180.250.127.114 · Prote	ocol: HTTP · Length: 523 · Info: GET /data/2014/	kompascom/images/fav	ricon.ico HTTP/1.1					
					Close		Help	
								_
• · · · · · · · · · · · · · · · · · · ·								
Wireshark · Follow TCP Stream (tcp.stream eq 149) · Kom	pas				_	Ц	>	ζ
							-	
GET /thumb/data/photo/2016/09/19/1554490Jeep-	Barut.jpg?x=150&v=150 HT	TP/1.1						
Connection: keep-alive							- 1	
Accept: image/webp,image/*,*/*;q=0.8								
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW	164) AppleWebKit/537.36 (	KHTML, like	Gecko) Chro	ome/49.0.262	3.87 Safari,	/537.3	86	
Referer: http://www.kompas.com/								
Accept-Language: en-US.en:g=0.8								
Cookie:gads=ID=60cfdd4ea111f4a9:T=14602050	71:S=ALNI_MaNy3qFNBVE0	EjY0-0425Ii	Ua6g;					
_em_vt=26fc094d3140b7ba7defa185182456e53c9d96	6685-294794015708f625; _	_asc=4e2483	e815741ced7	9e8032c1d7;				
auc=d16915ec153fb01855d838b7420; crtg_rta=;	_dc_gtm_UA-39495442-1=1	; _dc_gtm_U	A-3374285-20	0=1;				
laravel session=evJpdiI6IiFvdHBw00J2XC9zT1Nke	FhDTGk2SDBRPT0iLCJ2YWx17	SIGT1ZSM1VN	OTRZMUVpMØd	hVk55SWFES2o	3dXFmRmZHaX	FmdmZk	WHM	
xbjlZTmxnTTJPdTYxV2xkNUdzN1hYbWVF0FE0Q2pha3Vs	aG1sVUxuMkQrZjVZYWJ3PT0i	LCJtYWMiOiI	2MTI3MDE2MD	c5NjExY2IØNG	NjMDA3NDg2Y	TN1Y2Y	ZMG	
Y4ODNiZmF1MTQ0MTJjMGMwOWJ1MDYwYTA10WE0ZWV1In0	%3D;			-	5 0			
f22340cf2cbb69ff9adf83a2177c57188341d247=eyJp	diI6IkVXWStSaUU4cnl2cDB3	aFliN2t2cVE	9PSIsInZhbH	VlIjoiSnhKcT	RMazlUbnR6W	EwrcUN	Ikek	
JxakFyMFh1T056d1J4ZjNZNCtLaXd3aFptdzhPU0R0U3N	11bGNFbDBMZDVoOEtvMW8wV1N	5dCtoaWFhMm	ZFVWwwSnpUd: C+ThulovEvo	2RJcUVrVFh6a	jduZ21jeHFq/	MVFyWw	ItYO	
RGET /thumb/data/photo/2016/09/19/1554490Jeer	-Barut.ipg?x=150&v=150 H	TTP/1.1	CCIDOIGVEVI.	20VIICC20IID2	abubkesbwiiw	IKI120	1213	
Host: assets.kompas.com	510							
Connection: keep-alive								
Accept: image/webp,image/*,*/*;q=0.8		KUTMI 141	Casha) Cha		2 87 5-6	/537 3		
Referer: http://www.kompas.com/	(04) Appiewebkit/357.56	KHIML, IIKe	decko) chro	ome/49.0.262	5.07 Satari,	/ 55/.3	00	
Accept-Encoding: gzip, deflate, sdch								
Accept-Language: en-US,en;q=0.8								
Cookie:gads=ID=60cfdd4ea111f4a9:T=14602050	71:S=ALNI_MaNy3qFNBVE0	EjY0-0425Ii	Ua6g;					
_em_Vt=26TC094d31400/Da/deTa185182456e53C9d96	dc atm 110-39495442-1=1	_asc=4e2483 · dc_atm_II	e815/41ced/ A=3374285=20	9e8032C10/; 0-1·				
ga=GA1.2.1761504923.1474277903; dc gtm UA-3	9495442-3=1;	, _uc_scii_o	A 3374203 2	0-1,				
<pre>laravel_session=eyJpdiI6IjFvdHBwQ0J2XC9zT1Nke</pre>	FhDTGk2SDBRPT0iLCJ2YWx1Z	SI6IlZSM1VN	OTRZMUVpMØd	hVk55SWFES2o	3dXFmRmZHaX	FmdmZk	<b>WHM</b>	
xbjlZTmxnTTJPdTYxV2xkNUdzN1hYbWVF0FE0Q2pha3Vs	aG1sVUxuMkQrZjVZYWJ3PT0i	LCJtYWMiOiI	2MTI3MDE2MD	c5NjExY2IØNG	NjMDA3NDg2Y	TN1Y2Y	/zMG	
Y4ODN12mF1M1Q0M1J3MGMwOWJ1MDYwY1A1OWE02WV11ne f22340cf2cbb60ff0adf83a2177c57188341d247=ev3r	183D; ditetk/VWS+SauudealaenBa	>=1:N2+2-VE	ODSTeTe7bbH	VITioiSphKcT	PMaz 1UboP6W	Ewochth	Ikak	
JxakFvMFhiT056d1J4ZiNZNCtLaXd3aFptdzhPU0R0U3N	ibGNFbDBMZDVoOEtvMW8wV1N	5dCtoaWFhMm	ZFVWwwSnpUd	2RJcUVrVFh6a	iduZ21ieHFa	MVFvW	ItY0	
FZPeE1zWX1WR1NmY11XU0E0Y2g4YjZxWGJMTGNLM115VT	UwcXN5dDBKWHpxdDd1M05leV	gzcFQxWnpuM	ctTbUlGVEVr:	ZØVYTCtZaHB2	aDdBREJDWnN	nK1Ýza	ElJ	
RGJXRUxwYjZjZzBNVnpXMndxc1ZubW9RdGs0TjhZYVdDQ	jc3XC9NZlh5RzdPYU1BQU4xM	FlGaDcxWVQ0	WWhHdVwvYkV	XbVhqcVwvc1h	zQ1hQTlltbl	RySkNU	JNjN	
15mo4WFp4R2JXb0NnMDQ1bn1zd09JVWxn0VRrMDc5RGpF 8x0YV4eT3cK0xMeTN1NiNLYT3cL6EUTU+6skv12=pp=ip	azaev21w1zBEczVxVmZFQmp3	QmtTMWNrWVZ	KaTZBREXVdU.	INDEJISHF1Tm	0XSXBQYUY0Y)	XRWalj		
oxuxverijskoznie ininjni rijecofu u tuakvizmkrejki bhrsemnyi aqmerszopsuzyizaski knisubrqvi gzvi dqScsz2e4znizAwumjvi E8xUUNLR3RzT UhTWnBYS1B6V310czkwPSIsIm1hYvI6IiUwZWNhmE3NmMzZDBhNDgzZGR1ZDU3MmI3MidiY23kNTF5VzMzYWI3NmF17W1i7GM2Mih1NzO4Mz4vV2O4NmVifO								
\$30\$3D								
31 client pkt(s), 134 server pkt(s), 29 turn(s).								
Entire conversation (280 kB)	Show and save data as ASCII	•			1	Stream	149	•
Find:						Find	d Next	٦
L					-1			5
	Filter Out This Stream	Print	Save as	Back	Close	H	Help	

Dua gambar diatas memperlihatkan *GET* pada salah satu protokol dalam jaringan tersebut, disana tergambar ada beberapa diantaranya yang menuliskan *full request url* dengan

menyebutkan website yang saya buka. Sebuah permintaan *GET* mengambil data dari web server dengan menentukan parameter di bagian URL dari permintaan

Gambar selanjutnya merupakan capture dari *POST* pada salah satu IP yang tercapture pada wireshark yamg menunjukkan web yang saya tuju :

🖉 Wireshark - Follow HTTP Stream (tcp.stream eq 271) - Kompas 🤍 —	٥	×
POST /vevent?e=wqT_3QKyB_B-sgMAA4H1gAFAQ185P6- BRCsnvyc_5VJTFwVGc6F2b6_jKrUEAcQLQ1eVCLNttjUPAEXhtNetXPTPxKAAACgcD3yPyGFqnqk1LUPy1rrysiqhDNPzC2j94B0H5DQKg0SAJQw/NaGFjKrBgAG18BXiuqwSAAQGKAQUVU85SAQEGBEKYAawCOAH6AsgBAbABALgBAzs CdgBaAABAPACToKp12jgmVSISUDMSYLYyWymfUT301DIXHX00CFXARsscicISUDMH2L4H1/H3RhA4LGMLCAvbtk4Hz3MKYAChnJywgHz12V0KnEYdAABpARQMLE2H2EAHADwjTIChDTUNRBUXBaUEydFVHRUIHRRIOZIBQBAZ Z2RQUJJCUELUXRxXX2WbmdBkuJpRWFBQdBSG8Z6FRWIBRBFrUU9RQVFHWUFRZdBUXFvQVFP06FRQCVBVX2SJLUVX0M93UUZycn1zxKF8FdQOCHDIJa09sS124e19aQVFBQUEBA6BQQVBQUIHYKMIUFYCJVq1IgMdDSU Z2RQUJJCUELUXRxXX2WbmdBkuJpRWFBQdBSG8Z6FRWIBRBFrUU9RQVFHWUFRZdBUXFvQVFP06FRQCVBVX2SJLUVX0M93UUZycn1zxKF8FdQOCHDIJa09sS124e19aQVFBQUEBA6BQQVBQUIHYKMIUFYCJVq1IgMdDSU Z2VLQUEJUMWHZUMbgKENGADXSSSwnebd2BVKCVGQIAFE52xFJBEKUGGJAFKDEZEGCQGJAFKDEZEGCGQUEFZ2VJIGUUZIZZZSJDU.Z2XDUJZCUBUSKYXDWREFELiASHX5CHSWFBHD6JBES1tgC12F3/JACXHOCMH4AGLY9405DF3 VXWV72st13BJbZR1z2Jvd59XgrEferrerhttyX3X2FXFJtotmotff.kompas.com Z2FprodUmortXtype=QbAAGASSAv585ByF668bw=308bh=2508sf=1&sid=4034019105847158164185w=13668xh=7688pw=13498ph=25928wm=13668mh=7058ft=2&sv=51&tv=view5-1&au=chrome&p1=win&x=403401910584 Content-i=mainty Content-i=mainty	BBcgBANAE LckI4d0Fg yN3FFWWdC pZi5rb21w 4MjQ4MziA e14d2375d 471581641	^
<pre>Cachec-Control: max-sage=0 Origin: http://otomotif.kompas.com User-Agent: Mozilla/S.0 (Windows NT 10.0; KOW64) AppleWebKit/S37.36 (WHTML, like Gecko) Chrome/49.0.2623.87 Safari/S37.36 Content-Type: text/plain;charset=UTF-8 Accept: =/* Refere: http://otomotif.kompas.com/produkmotor Accept-tencoding: gip, deflate Accept-tencoding: gip, deflate Cockie: icu=ChIIID00EA0YASBKZ&amp;H-T-YgUKEgjjiS4CABIAEOATCKSP6-BRCHSP6-BRGB anj=dTM7kIM4/KSbyCo?(rulk/_pJ8#=1.:^9VM4JH:+h6'mrK4KX09MxI'wqAw=vkD SC/A015Y*Fer(Ma:'VALD2.VG()BHK.'hv7:1cg/h*BidEj0LA3X7doh04sxEE_UF]8S(IndACM2M7A20*CovmFFRV370xeOKFK7]'V680ng'M*8kgUdsy_e(DqgdgbGbGMdS5o*TR-U//IMTKtV4JL'zh7=xpsr]2U/6)A%=70 SiJu*u(K632er4f8UM=112)cpHk.sed01250xHH718_GAGHCH9F4_G.CSWAFEBR04EBR042DH71.VH4H/LE]DEEV1347XcdD04sxEE_UF]39JWH12+D64CH94F4TS9BJPLUHkp-minr't3thF7A5Bf(3UVU'PqL12C+MUG-G SiJu*u(K632er4f8UM=112)cpHk.sed01250xH4718_GAGHCH94F4_G.CSWAFEBR04EBR042DH71.VH4H/LE]DEEV1347XcdD04sxEE_UF]39JWH12+D64CH94F4TS9BJPLUHkp-minr't3thF7A5Bf(3UVU'PqL12C+MUG-G SiJu*u(K632er4f8UM=112)cpHk.sed01250xH4718_GAGHCH94F4_G.CSWAFEBR04EBR042DH71.VH4H/LE]DEEV1347XcdD04sxEE_UF]39JWH12+D64CH94F4W3UD45D+UK4KCH2H4+LH41_LB37YKH8A5Bf3UWU'PqL12C+MUG-G SiJu*u(K632er4f8UM=112)cpHk.sed01250xH4718_GAGHCH94F4_G.CSWAFEBR04EBR042DH71.VH4H4/LE]DEEV1347XcdD04sxEEUF]39JWH12+D64CH45BJB1UHKhp-minr't3thF7A5Bf3UWU'PqL12C+MUG-G SiJu*u(K632er4f8UM=112)cpHks.sed0125H71/G45134*632ESUF]79JWH12+D64CH45BJB1UHKH74D1455DVC3H714B4(M32UH47)A455BVAB4BF45B73VAB4F455DVA5AF455DVA5AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF455DV45AF4555DV45AF4555DV45AF4555DV45AF45555DV45AF4555DV45AF4555DV45AF45555DV45AF45555DV45AF45555DV45AF455555555555565658F45555555555556565555555555</pre>	lg <br u.NT#%d0 !	
<pre>eholde/:19*XLM28*)kQ4=e MBvdicse*3K/KKUp0(kd5tHovQqubXVh; sess=1; uuld2=00//099/01/19623529 HTTP/1.1 200 0K Server: nginx/1.9.13 Date: Mon, 19 Sep 2016 09:39:45 GMT Content-tength: 0 Content-tength: 0 Content-tength: 0 Content-tength: 0 Content-tength: 0 Content-control: no-store, no-cache, private Pragma: no-cache Expires: Sat, 15 Nov 2008 16:00:00 GMT P3P: policyref="http://ch.admxs.com/waC/policy/p3p.xml", CP="NOI DSP COR ADM PSAo PSDo OURo SAMo UNRO OTRO BUS COM NAV DEM STA PRE" X-XS5-Frotection: 0 Access-Control-Allow-Credentials: true</pre>		~
1 client ph(t), 1 server ph(t), 1 turn(t).		_
Entire conversation (3779 bytes) • Show and save data a	s ASCII	•
Find:	Find Ne	xt
Filter Out This Stream Print Save as Back Close	Help	

Seperti yang telihat dalam gambar diatas yang menggambarkan isi *POST* dari IP yang masih berhubungan dengan web dengan protokol *http*. Sebuah permintaan *HTTP POST* memanfaatkan badan pesan untuk mengirim data ke server web.

Setelah beberapa gambar diatas yang menjelaskan sedikit proses dari capturing pada wireshark dan beberapa juga penjelasan tentang *post* dan *get* yang terdapat dalam capturing, selanjutnya ada proses capturing jaringan menggunakan cmd dan menggunakan command *netstat* -a yang bersamaan dengan capturing menggunakan wireshark. Berikut merupajan capture gambar hasil menggunakan cmd :

Select	t Command Prompt			_	$\times$
Microsof (c) 2015	ft Windows [Version 10.0 5 Microsoft Corporation.	.10586] All rights reserved.			^
C:\Users	s\toshiba≻netstat -a				
Active (	Connections				
Proto	Local Address	- Foreign Address	State		
TCP	0.0.0.0:135	TOSHIBA-PC:0	LISTENING		
TCP TCP	0.0.0.0:445 0.0.0.0:1688	TOSHIBA-PC:0 TOSHIBA-PC:0	LISTENING LISTENING		
TCP	0.0.0.0:5357	TOSHIBA-PC:0			
TCP	0.0.0.0:49665	TOSHIBA-PC:0	LISTENING		
TCP	0.0.0.0:49666 0 0 0 0:49667	TOSHIBA-PC:0	LISTENING		
TCP	0.0.0.0:49668	TOSHIBA-PC:0	LISTENING		
TCP	0.0.0.0:49669 0.0.0.0:49670	TOSHIBA-PC:0 TOSHIBA-PC:0	LISTENING		
TCP	192.168.43.12:139	TOSHIBA-PC:0	LISTENING		
TCP	192.168.43.12:53155 192.168.43.12:53255	111.221.29.1/1:https 138.201.31.14:3333	ESTABLISHED		
TCP	192.168.43.12:53256	138.201.31.14:3333	ESTABLISHED		
TCP	192.168.43.12:53257	138.201.31.14:3333	ESTABLISHED		
TCP	192.168.43.12:53368 192.168.43.12:53370	192.168.1.255:1688	ESTABLISHED		
TCP	192.168.43.12:53372	192.168.1.255:1688	ESTABLISHED		
TCP TCP	192.168.43.12:53405 192.168.43.12:53411	111.221.29.254:https 184.51.97.92:http	TIME_WAIT		~
TCP	192.168.43.12:53413	74.125.68.94:https	TIME_WAIT		^
TCP TCP	192.168.43.12:53416 192.168.43.12:53418	114.125.1.155:https 114.125.33.16:https	TIME_WAIT		
TCP	192.168.43.12:53423	202.146.4.100:http	TIME_WAIT		
TCP	192.168.43.12:53424 192.168.43.12:53425	202.146.4.100:http 202.146.4.100:http	TIME_WAIT		
TCP	192.168.43.12:53426	74.125.68.95:http			
TCP	192.168.43.12:53427	180.250.127.114:http	TIME_WAIT		
TCP	192.168.43.12:53429	180.250.127.114:http			
TCP	192.168.43.12:53431	180.250.127.114:http	TIME_WAIT		
TCP TCP	192.168.43.12:53432 192.168.43.12:53433	180.250.127.114:http 180.250.127.114:http	TIME_WAIT		
TCP	192.168.43.12:53434	180.250.127.114:http	TIME_WAIT		
TCP TCP	192.168.43.12:53435 192.168.43.12:53436	114.125.33.16:http 114.125.33.16:http	TIME_WAIT TIME_WAIT		
TCP	192.168.43.12:53437	202.146.4.64:http			
TCP	192.168.43.12:53438	118.98.95.130:http	TIME_WAIT		
TCP	192.168.43.12:53441	118.98.95.129:http			
TCP	192.168.43.12:53443	68.232.45.253:http	TIME_WAIT		
TCP TCP	192.168.43.12:53445 192.168.43.12:53446	202.146.4.163:http 202.146.4.64:http	TIME_WAIT		
TCP	192.168.43.12:53447	202.146.4.163:http	TIME_WAIT		
ТСР	192.168.43.12:53448 192.168.43.12:53449	202.146.4.210:http 202.146.4.210:http	TIME_WAIT		
TCP	192.168.43.12:53450	202.146.4.210:http			
ТСР	192.168.43.12:53552	54.239.16.235:http	TIME_WAIT		×
TCP	192.168.43.12:53553	54.239.16.235:http			
TCP	192.168.43.12:53555	180.250.127.114:http	ESTABLISHED		
TCP TCP	192.168.43.12:53556 192.168.43.12:53558	180.250.127.114:http 202.146.4.170:http	ESTABLISHED TTME WATT		
TCP	192.168.43.12:53559	202.146.4.170:http	TIME_WAIT		
TCP TCP	192.168.43.12:53563 192.168.43.12:53564	54.192.159.112:https 114.125.1.145:https	ESTABLISHED ESTABLISHED		
TCP	192.168.43.12:53571	114.125.33.31:http			
TCP	192.168.43.12:53572	202.146.4.64:http	ESTABLISHED		
TCP	192.168.43.12:53574	202.146.4.64:http	ESTABLISHED		
TCP	192.168.43.12:53576	202.146.4.64:http	ESTABLISHED		
TCP TCP	192.168.43.12:53578 192.168.43.12:53579	202.146.4.210:http 180.250.127.114:http	TIME_WAIT ESTABLISHED		
TCP	192.168.43.12:53580	180.250.127.114:http	ESTABLISHED		
TCP	192.168.43.12:53582 192.168.43.12:53583	54.230.159.100:http 54.230.159.100:http	TIME_WAIT		
TCP	192.168.43.12:53584	54.230.159.100:http			
TCP	192.168.43.12:53586	117.121.249.253.http	TIME_WAIT		
TCP	192.168.43.12:53588 192.168.43 12:53589	117.121.249.253:http 104.93.117_144.http	TIME_WAIT		
TCP	192.168.43.12:53590	104.93.117.144.http	TIME_WAIT		
TCP TCP	192.168.43.12:53591 192.168.43.12:53592	54.230.159.230:http 54.230.159.230:http	ESTABLISHED ESTABLISHED		
TCP	192.168.43.12:53593	54.230.159.230:http			
TCP	192.100.43.12.53595	74.125.130.155.NCCpS			V.

ТСР	192.168.43.12:53597	202.146.4.163:http	TIME_WAIT	^
TCP	192.168.43.12:53598	202.146.4.2:http		
TCP	192.168.43.12:53600	202.146.4.2:http	TIME_WAIT	
тср	192.168.43.12:53603	54.182.210.122:http	ESTABLISHED	
TCP	192.168.43.12:53604	74.125.200.155:http		
TCP	192.168.43.12:53607	31.13.78.35:https	ESTABLISHED	
тср	192.168.43.12:53608	180.250.127.114:http	ESTABLISHED	
TCP	192.168.43.12:53612	202.61.113.71:http	ESTABLISHED	
ТСР	192.168.43.12:53622	104.244.42.8:https 118.98.95.74:https	ESTABLISHED	
TCP	192.168.43.12:53624	118.98.95.74:https	ESTABLISHED	
ТСР	192.168.43.12:53625	151.101.9.108:https	ESTABLISHED	
ТСР	192.168.43.12:53627	118.98.95.74:https		
TCP	192.168.43.12:53629	103.243.220.231:https	CLOSE WAIT	
TCP	192.168.43.12:53630	180.250.127.114:http	ESTABLISHED	
TCP	192.168.43.12:53631	104.93.114.237:https	ESTABLISHED	
ТСР	192.168.43.12:53632	54.77.147.27:https 52.17.24.234:https	ESTABLISHED	
TCP	192.168.43.12:53635	52.68.201.148:https	ESTABLISHED	
TCP	192.168.43.12:53636	54.248.98.228:https	ESTABLISHED	
ТСР	192.168.43.12:53638 192.168.43.12:53639	52./6.99.143:nttps 104 93 210 177.https	ESTABLISHED	
TCP	192.168.43.12:53641	104.93.210.177:https	TIME WAIT	
ТСР	192.168.43.12:53642	103.15.158.193:https	FIN_WAIT_2	
TCP	192.168.43.12:53644	103.243.221.87:https	TIME_WAIT	
ТСР	192.168.43.12:53646	180.250.127.114:http	ESTABLISHED	~
TCP	192.168.43.12:53647	180.250.127.114:http	ESTABLISHED	$\mathbf{A}$
TCP	192.168.43.12:53648	180.250.127.114:http	ESTABLISHED	
TCP	192.168.43.12:53649	180.250.127.114:http	ESTABLISHED	
TCP	192.168.43.12:53651	118.98.95.129.http	ESTABLISHED	
TCP	[::]:135	TOSHIBA-PC:0	LISTENING	
TCP	[::]:445	TOSHIBA-PC:0	LISTENING	
ТСР	[::]:1688 [··]·5357	TOSHIBA-PC:0	LISTENING	
TCP	[::]:49664	TOSHIBA-PC:0	LISTENING	
TCP	[::]:49665	TOSHIBA-PC:0	LISTENING	
TCP	[::]:49666	TOSHIBA-PC:0	LISTENING	
TCP	[::]:49668	TOSHIBA-PC:0	LISTENING	
TCP	[::]:49669	TOSHIBA-PC:0	LISTENING	
TCP	[::]:49670	TOSHIBA-PC:0	LISTENING	
	0.0.0.0:500	*:*		
UDP	0.0.0.0:3702	* *		
UDP	0.0.0.0:3702	* *		
UDP	0.0.0.0:3702	*:*		
UDP	0.0.0.0:3702	* *		
UDP	0.0.0.0:4500	* *		
UDP	0.0.0.0:5353	* *		
	0.0.0.0:5355	* • *		
UDP	0.0.0.0:58869	* *		
UDP	0.0.0.0:61674	*:*		
UDP	0.0.0.0:61895	*:*		× .
UDP	127.0.0.1:51505	* *		
UDP	192.168.43.12:137	* :*		
UDP	192.168.43.12:138	*:*		
UDP	192.168.43.12:1900	* *		
UDP	[::]:500	* *		
UDP	[::]:3702	* *		
	[::]:3/02	* *		
UDP	[::]:3702	* *		
UDP	[::]:3702	*:*		
UDP	[::]:3702	* *		
	[::]:4500	* *		
UDP	[::]:5355	* *		
UDP	[::]:56721	* *		
UDP	[::]:58870 [::]:61675	*:*		
UDP	[::]:61896	* *		
UDP	[::1]:1900	*:*		
UDP	[::1]:51503	*:*		
	[+e80::182d:b152:887f: [fe80::182d:b152:887f:	C6D6%10]:1900 *:*		
001	[1000.11020.0152.88/1.			
C:\Users	\toshiba>			
				$\sim$

Gambar diatas merupakan hasil dari capturing jaringan melalui cmd dengan command

*netstat* –*a* yang prosesnya bersamaan dengan capturing menggunakan wireshark. Pada gambar diatas terdapat beberapa protokol yang berbeda, ada TCP dan ada juga UDP. Transmission Control Protocol (TCP) adalah salah satu jenis protokol yang memungkinkan kumpulan komputer untuk berkomunikasi dan bertukar data didalam suatu network (jaringan). TCP merupakan suatu protokol yang berada di lapisan transpor (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (connection-oriented) dan dapat diandalkan (reliable). Lalu ada UDP, UDP singkatan dari User Datagram Protocol, adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP.

## **Port IP :**

Dari beberapa IP yang saya cek disitu menjelaskan bahwa Destination Port terdapat pada port 80, seperti yang di gambarkan oleh capture dibawah ini :

```
> Ethernet II, Src: LiteonTe_88:dc:a9 (24:fd:52:88:dc:a9), Dst: AsustekC_34:d8:db (14:dd:a9:34:d8:db)
> Internet Protocol Version 4, Src: 192.168.43.12, Dst: 180.250.127.114
  Transmission Control Protocol, Src Port: 53645, Dst Port: 80, Seq: 27933, Ack: 119562, Len: 469
  Source Port: 53645
  Destination Port: 80
  [Stream index: 149]
  [TCP Segment Len: 469]
  Sequence number: 27933 (relative sequence number)
  [Next sequence number: 28402 (relative sequence number)]
  Acknowledgment number: 119562 (relative ack number)
  Header Length: 20 bytes
```

Dari gambar diatas saya menggunakan IP yang saya ambil untuk melihat *get* sebelumnya, disana di tuliskan Source Port : 53645 dan Destination Port : 80. Setelah saya melihat beberapa IP dengan protokol http Get lain juga menerangkan bahwa destination port juga dituliskan 80.