ANALISA HASIL CAPTURE, FOLLOW STREAM, DAN FOLLOW GRAPH JARINGAN MENGGUNAKAN APLIKASI WIRESHARK, DAN VISUAL ROUTE



Disusun oleh :

Yoggie al hanif 09011381621113 SK 4B

SISTEM KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

Cara menganalisa ip jaringan kita

Sebelum melakukan menganalisa paket jaringan,terlebih dahulu mengetahui berapa adress yang sedang kita pakai.dengan cara membuka cmd dan ketik perintah "arp –a" maka adress jaringan kita akan diketahui sepeerti gambar dibawah ini.

🔤 Command Prompt			—	×
Microsoft Windows [Vers (c) 2017 Microsoft Cor	sion 10.0.15063] coration. All rights re	eserved.		
C:\Users\ACER≻arp-a "arp-a' is not recognia operable program or bat	zed as an internal or (tch file.	external command,		
C:\Users\ACER≻arp –a				
Interface: 192.168.0.16	01 0xe			
Internet Address	Physical Address	Туре		
192.168.0.1	90-c7-d8-9d-12-60	dynamic		
192.168.0.255	₣ <u></u> - <u>+</u> <u>+</u> - <u>+</u> <u>+</u> - <u>+</u> <u>+</u> - <u>+</u> <u>+</u>	static		
224.0.0.22	01-00-5e-00-00-16	static		
224.0.0.251	01-00-5e-00-00-fb	static		
224.0.0.252	01-00-5e-00-00-fc	static		
239.255.255.250	01-00-5e-7f-ff-fa	static		
255.255.255.255	╋╃╌ ╋╪╌╋╋╌╋╋╌╋╋	static		
Interface: 192.168.56.1	l 0x2a			
Internet Address	Physical Address	Туре		
192.168.56.255	₣ ╒ ╶ ╒ _╏ ╴ <u></u> <u></u> _┠ ╴ <u></u>	static		
224.0.0.22	01-00-5e-00-00-16	static		
224.0.0.251	01-00-5e-00-00-fb	static		
224.0.0.252	01-00-5e-00-00-fc	static		
239.255.255.250	01-00-5e-7f-ff-fa	static		
C:\Users\ACER>				
				_

Selanjutnya kita dapatkan, langkah selanjutnya adalah kita membuka aplikasi WIRESHARK. Disini saya menggunakan wifi dari andromax saya Andromax-M3Z-1260.

Image: WirFi2 - File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help - Image: Imag					- 0	×		
	o.src==47,74,175,31			• -	Expression.	+		
No.	Time	Source	Destination	Protocol Length Info		<u> </u>		
	14818 706.192693	47.74.175.31	192.168.0.101	TLSv1.2 520 Certificate, Server Key Exchange, Server Hello Done				
	14815 706.191790	47.74.175.31	192.168.0.101	TCP 1448 443 → 63523 [ACK] Seq=1395 Ack=192 Win=30720 Len=1394 [TCP segment of a reassembled PDU]				
	14814 706.191784	47.74.175.31	192.168.0.101	TLSv1.2 1448 Server Hello		_		
	14813 706.191782	47.74.175.31	192.168.0.101	TCP 54 443 → 63523 [ACK] Seq=1 Ack=192 Win=30720 Len=0				
	14810 706.191778	47.74.175.31	192.168.0.101	TLSv1.2 620 Certificate, Server Key Exchange, Server Hello Done				
	14809 706.191776	47.74.175.31	192.168.0.101	TCP 1448 443 → 63521 [ACK] Seq=1395 Ack=192 Win=30720 Len=1394 [TCP segment of a reassembled PDU]				
	14808 706.191773	47.74.175.31	192.168.0.101	TLSv1.2 1448 Server Hello				
	14807 706.191770	47.74.175.31	192.168.0.101	TCP 54 443 → 63521 [ACK] Seq=1 Ack=192 Win=30720 Len=0		_		
	14800 705.877970	47.74.175.31	192.168.0.101	TCP 66 443 → 63523 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1394 SACK_PERM=1 WS=512		_		
	14782 705.829982	47.74.175.31	192.168.0.101	TCP 66 443 → 63521 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1394 SACK_PERM=1 WS=512		~		
> > >	<pre>> Frame 14800: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 > Ethernet II, Srci 172-9012:60 (9012:06) 9012:06 (9012:06). 9012:06:001200; 10012:06) (9012:</pre>							
000 003 003 004	Protocol: TCP (9 94 53 30 3b ce 0 00 34 00 00 40 0 00 65 01 bb f8 0 72 10 0b f6 00 0 3 09	6)	2 60 08 00 45 00 .50;. f 4a af 1f c0 a8 .4@ of 58 f 30 12 .e 1 01 04 02 01 03					
0	Wireshark_4F0ACS	85-4EC9-42A9-8718-5FA	58CD3F8D6_20180222095504_a04	568 Packets: 29759 · Displayed: 67 (0.2%) · Dropped: 0 (0.)%) Profile:	Default		
=		e 📒 🕯	Pi 🧿 🕨	🍳 🏹 🕿 📶 🔤 🚿 📶	(10.55 ND 22/02/2018			

Dari gambar di atas kita telah mendapatkan bentuk pakeet jaringan karena semua paket tersaing dengan cepat, maka lebih baik di filter terlebih dahulu dengan menggunakan sintak "ip.src==192.168.0.101".

Dan setelah di filter maka akan terdapat lagi data yang berupa yakni:



Dapat dilihat sendiri bahwa dengan komputer yang ber alamatkan 192.168.0.101 sedang mengakses 47.74.175.31 atau website <u>www.tokopedia.com</u> dengan menggunakan protocol TCP,stelah itu klik dibagian kotak tengah di menu internet protocol version 4,

▲ "Wi-Fi2 File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					-	Ð	×		
1		0	🗙 🖨 🧣 👄 👄	🕾 👔 🌡 🥃 📕 Q, Q	0.1				
	ip.src=	=47.74.175.31					$X \rightarrow $	Expression	
	Iprore	Time	Courses	Destination	Destaval	Lanath Tafa)	
INC	14919	706 102603	47 74 175 31	102 168 0 101	TI Sv1 2	630 Certificate Server Key Exchange Server Hello Done			
	14010	706.192095	47.74.175.31	192.108.0.101	TCP	1448 443 + 6323 [ACV] Septials Action 10 bine 2020 [article and a constant of a consta			
	14814	706.191784	47 74 175 31	192.168.0.101	TLSv1 2	1448 Server Hello			
	14813	706.191782	47.74.175.31	192.168.0.101	TCP	54 443 + 63523 [ACK] Seg=1 Ack=192 Win=30720 Len=0			
	14810	706.191778	47.74.175.31	192.168.0.101	TLSv1.2	620 Certificate, Server Key Exchange, Server Hello Done			
	14809	706.191776	47.74.175.31	192.168.0.101	TCP	1448 443 → 63521 [ACK] Seq=1395 Ack=192 Win=30720 Len=1394 [TCP segment of a reassembled PDU]			
	14808	3 706.191773	47.74.175.31	192.168.0.101	TLSv1.2	1448 Server Hello			
	14807	706.191770	47.74.175.31	192.168.0.101	TCP	54 443 → 63521 [ACK] Seq=1 Ack=192 Win=30720 Len=0			
	14800	705.877970	47.74.175.31	192.168.0.101	TCP	66 443 → 63523 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1394 SACK_PERM=1 WS=512			
	14782	2 705.829982	47.74.175.31	192.168.0.101	TCP	66 443 → 63521 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1394 SACK_PERM=1 WS=512			
	C	14000, CC		hite) of huter continues	4 (500 Liter				
5	Ether	14000: 00 D	7te 9d-12-60 (90-	c7:d8:9d:12:60) Det: Ho	onHaiPr 3b:) on internate o			Â
Í.	Inter	net Protocol	Version 4. Src: 4	7.74.175.31. Dst: 192.16	68.0.101				
	01	00 = Ve	rsion: 4						
	> Di	fferentiated	Services Field: 0	x00 (DSCP: CS0, ECN: Not	t-ECT)				
	Total Length: 52								
	Id	entification	: 0x0000 (0)						
	> F1	ags: 0x02 (D	on't Fragment)						
	Fragment offset: 0								
	Ti	me to live:	49						
	Pro	ntocol· TCP	(6)						*
0	000 9	4 53 30 3b e	e b7 90 c7 d8 9d	12 60 08 00 45 00 .SO;		E.			
0	010 0	0 34 00 00 4 9 65 91 bb f	0003105 aa 40. 83365 bc 985f	2T 4a at 1T C0 a8 .4 80 d5 d8 f3 80 12	.@.1M/J. #≏				
0	030 7	2 10 0b f6 0	0 00 02 04 05 72	01 01 04 02 01 03 r					
0	040 0	3 09							
(Q 2 wireshark_4F0AC985-#EC9-42A9-8718-SFAS8CD3F806_20180222095504_a0-4668 Packets: 29759 · Displayed: 67 (0.2%) · Dropped: 0 (0.0%) Profile: Default								
			<u> </u>		· · ·		2	2/02/2018	~

Dari gambar di atas di jelaskan komputer tersebut mengakses web tersebut memiliki web adress,selain itu kita mendapatkan info mengenai mac adressnya kita desaian juga dapat mengetahui bahwa panjang yang terbaca dan mendapatkan info mengetahui tentang port.

	■ Ø X					×		
	The Louis view ou capute Analyze statistics receipting whether to be the							
F							1.4	
<u> </u>	Ip.src==47.74.175.31					xpression.		
No	. Time	Source	Destination	Protocol Length Info			 ^	
	14818 706.192693	47.74.175.31	192.168.0.101	TLSv1.2 620 Certificate, Server Key Exchange, Server Hello Done			_	
	14815 706.191790	47.74.175.31	192.168.0.101	TCP 1448 443 → 63523 [ACK] Seq=1395 Ack=192 Win=30720 Len=1394 [TCP segment of a reassembled PDU]		1		
	14814 /06.191/84	47.74.175.31	192.168.0.101	ILSVI.2 1448 Server Hello		- I		
	14813 /06.191/82	47.74.175.31	192.168.0.101	ICP 54 443 + 63523 [ACK] Seq=1 Ack=192 Win=30/20 Len=0				
	14810 /06.191//8	47.74.175.31	192.168.0.101	ILSVI.2 620 Certificate, Server Key Exchange, Server Hello Done				
	14809 /06.191//6	47.74.175.31	192.168.0.101	ICP 1448 443 → 65521 [ACK] Seq=1395 Ack=192 Win=30/20 Len=1394 [ICP segment of a reassembled PDU]				
	14808 /06.191//3	47.74.175.31	192.168.0.101	ILSVI.2 1448 Server Hello				
i.	14807 706.191770	47.74.175.31	192.168.0.101	ICP 54 443 + 65521 [Ack] 560=1 Ack=192 win=30720 Len=0				
	14800 705.877970	47.74.175.31	192.168.0.101	ICP 66 443 + 65523 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1394 SACK_PERM=1 WS=512	_			
	14/82 /05.829982	47.74.175.51	192.168.0.101	ICP DE 443 + 63521 [SYN, ACK] SEQ=0 ACK=1 WIN=23200 LEN=0 MSS=1394 SACK_PERN=1 WS=512		-		
> > ~	<pre>> Frame 14800: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 > Ethernet II, Src: Zte_9di21:66 (90:C7:d8:9di12:60), Dst: HonHaiPr_3biseib7 (94:53:30:3biseib7) Unternet Protocol Version: 4 0101 - Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 52 Identification: 0x0000 (0) > Flags: 6x02 (Don't Fragment) Fragment Offset: 0 Time to live: 49 Perotocol: VEP.(6)</pre>							
00	0010 000							
	🔰 🍸 🛛 Total Length (ip.lei	i), 2 bytes		Packets: 29759 · Displayed: 67 (0.2%) · Dropped: 0 (0.0	%)	Profile:	: Default	
1		e 🛢 📫	🔁 🧕 👯	\$ The second sec) IND 10 22/0	0.55 2/2018	\Box	

Lalu klik analyze=> pilih follow dan => untuk pertama pilih bagian TCP stream seperti dibawah ini :

*Wi-Fi 2 File Edit View Go Capture Ana	📕 Wireshark - Follow TCP Stream (tcp.stream eq 183) - wireshark_4F0AC985-4EC9-42A9-8718-5FA58CD3F8D6_20180222095504_804668 – 🗆 X	- 0 ×
Image: Constraint of the state of	<pre>GET /anx.gif?anxuu=9FF0A739-9D5E-43E8-9A08-CF1ACF040CE2&anxa=WebTooltab&anxv=webtooltab-2.1.1&anxd=-&anxsn=&anxu=http%3A%2F %2Fhp.myway.com%2Fmyeasylotto%2Ftab02%2Findex.html&anxl==m&anxlv=15102068796190&anxrd=-d=none&anxrp=-&anxrk=-&anxrb=- %anxrc=-&anxmrs=-&anxa=3&anxt=9b6FEAA-1080=43A3-A35-56660ACS0758Anapr&SecT0 %5Exdm228%5ETTAB02%2Fid&anxsi=1477276&buid=12220efe-58d4-4a23-b09c-dd27efd4Seb4&pageType=tab&productData=%7E%22pageLoad %22%3A6%7D&mxe=HeartbeatBanxr=861E3078 HTTP/1.1 Host: anx.tb.ask.com User-Agent: Nozilla/5.0 (Windows NT 10.0; W0W64; rv:43.0) Gecko/20100101 Firefox/43.0</pre>	Expression + 1tab-2.1.1&anxd=-&anxsn=&anxu=_
11941 690.363028 192.168.4 12085 690.655611 74.113.22 12087 690.655761 92.168.4 1216 691.658069 74.113.22 12198 691.658029 74.113.22 12198 691.658731 92.168.6 12223 691.779387 192.168.6 12237 692.246854 74.113.22	Accept-image/png,image/ig=0.8,*/*iq=0.5 Accept-lenguage: en-US;enig=0.5 Accept-lenguage: en-US;enig=0.5 Accept-lenguage: en-US;enig=0.5 MSExHIZ28X5ETTAB02X5Eid&n-783acf65&ptb=996FEFAA-1689-43A3-AA35-5F0660AC5057&si=1477276&st=tab Connection: keep-alive Pragma: no-cache Cache-Control: no-cache HTTP/1.1 204 No Content Server: nginx/1.0.10 Date: Thu, 22 Feb 2018 03:06:40 GMT	
	Connection: Close Expires: Thu, 01 Jan 1970 00:00:01 GHT Cache-Control: no-cache Cache-Control: max-age=0	
 > Frame 12197: 250 bytes on win > Ethernet II, Sec: Zte 94:12:6 ✓ Internet Protocol Version 4, 0:00 = Version: 4 0:101 = Header Length: > Differentiated Services Fi Total Length: 236 Identification: 0xb075 (45 > Flags: 0x02 (Don't Fragmen Fragmen offset: 0 Time to live: 235 		
0010 00 ec b0 75 40 00 eb 06 0020 00 65 00 50 f7 f7 51 0030 14 04 69 98 00 04 854 0040 30 34 20 4e 6f 20 43 6f 0050 65 72 76 65 72 3a 20 6e	Jeter pit(s), J zerver	
🔵 🍸 Total Length (ip.len), 2 bytes	Filter Out This Stream Print Save as Back Close Help	ped: 0 (0.0%) Profile: Default
🗄 A 🗆 🤤 🚞	- 🔒 📴 💹 🌀 🥻 🕿 🌌 📶 📼 🐗 🥼	口 (d)) IND 11.03 口 (d)) IND 22/02/2018

1. Pengguna yang sedang mengakses website <u>www.tokopedia.com</u> menggunakan apliksi mozilla.

- 2. Waktu user mengakses web tersebut pada tanggal 22 februari 2018 pada hari kamis
- 3. Tipe data yang sedang diakses itu berupa text/html.

FLOWGRAPH Jaringan menggunakan aplikasi Wireshark dan Visual route

Caranya kita klik menu statistic dan kita pilih flow grap maka data yang akan muncul seperti berikut.



Lalu lintas berjalannya ekspedisi informasi dapat divisualisasikan menggunakan flow graph seperti gambar diatas. Berikut ini adalah penjelasan terhadap panah-panah pada flowgraph:

- Panah 1, komputer user mengirim informasi adress atau linkke router jaringan.
- Panah 2, ketika router menerima informasi, maka ia mengalamatkan data tersebut
- Panah 3, isp akan menaggapi permintaan user tersebut, apakah adress yagn dituju itu tersedia atau tidak
- Panah 4, apabila adress tersedia, maka isp akan mengarahkan informasi ke isp pusat
- Panah 5, isp pusat pun akan menaggapi permintaan tersebut dan informasi tanggapan akan dikirim kembali ke user
- Panah 6, jika tidak valid atau tidak ditemukan, maka akan diperiksa oleh isp tersebut
- Panah 7, jika informasi tersebut valid,isp akan kembali mengirim tanggapan dan mengarahkanke isp pusat
- Panah 8, apabila isp pusat menanggapi atau valid,maka akan diarahkan ke server perusahaan yg memberi isp bandwith.

- Panah 9, yang diakses adalah <u>www.tokopedia.com</u> dengan mengambil berita internasional dan nasional.
- Panah 10, seperti pada isp tadi, server pun akan mengirim informasi ke user apakah yang dituju valid atau tidak

BERIKUT INI TAMPILAN DARI APLIKASI VISUALROUTE :

Perbedaan antara wireshark dan visualroute:

- Aplikasi wireshark, dapat di analisa dan ada timbal balik kepada user,sangat berguna bagi operator server atau server manager yang memiliki kemampuan expert dan dapat meneliti data dengan detail. lebih akurat dan efektif.
- 2. Visual route, penggunaan aplikasi ini mudah dan mudah di mngerti oleh pengguna, dan destinasion terlihat jelas dan setiap hope ditampilkan semua tetapi kurang mumpuni dan mencapture data pada sebuah ip.dan tidak adanya filter protocol.