TUGAS JARINGAN KOMPUTER VISUALISASI DAN ANALISA PCAP FILE DENGAN MENGGUNAKAN RUMINT



Nama	: Endi Kumara
NIM	: 09011281520098
Kelas	: SK5 C

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

I. Judul

Visualisasi dan Analisa PCAP File Menggunakan Rumint

II. Penjelasan

Rumint adalah aplikasi yang di gunakan untuk membaca trafik jaringan dan juga untuk memvisualisasikan paket data. PCAP file merupakan proses tracing dari wireshark yang di save dengan .pcap.

Kasus 1 (www.kompas.com)

📕 *Wi-F	i					_		×
File Edit	t View Go	Canture Analyze Statist	tics Telephony Wireles	s Tools H	teln			
				0 FF	юр			
	2 🙂 🚺 🖬		જ 👲 💶 🔍 લ	9				
📕 Apply a	a display filter <	:Ctrl-/>					Expression.	+
No.	Time	Source	Destination	Protocol	Length Info			^
4052	2 92.155872	74.125.68.136	192.168.1.101	TCP	66 [TCP Keep-Alive ACK] 443 → 52008 [ACK] Seq=5176 Ack=1176 Win=50432 Len=0 SLE=1175 SR	E=1176	
4053	3 92.577805	192.168.1.101	192.168.1.255	NBNS	92 Name query NB WORKGROUP<1c>			
4054	4 93.328234	192.168.1.101	192.168.1.255	NBNS	92 Name query NB WORKGROUP<1c>			
4055	5 93.487510	192.168.1.101	74.125.130.84	TCP	55 [TCP Keep-Alive] 52011 → 443 [ACK] Se	q=654 Ack=4268 Win=65536 Len=1		
4056		74.125.130.84				[] Seq=4268 Ack=655 Win=45056 Len=0 SLE=654 SRE=	655	
4057	7 93.862591	Shenzhen_28:a4:5a	Broadcast	ARP	42 Who has 192.168.1.102? Tell 192.168.1	1		
4058	8 93.972035		54.231.120.227		55 [TCP Keep-Alive] 52063 → 443 [ACK] Se	q=0 Ack=9 Win=66816 Len=1		
4059	9 94.277370	54.231.120.227	192.168.1.101	TCP	54 [TCP Keep-Alive ACK] 443 → 52063 [ACK	[] Seq=9 Ack=1 Win=14848 Len=0		
4066	94.886413	Shenzhen_28:a4:5a	Broadcast	ARP	42 Who has 192.168.1.102? Tell 192.168.1	1		
4061	1 95.144558	192.168.1.101	192.168.1.255	NBNS	92 Name query NB WORKGROUP<1c>			
4063	2 95.526575				55 [TCP Keep-Alive] 52016 → 443 [ACK] Se	q=649 Ack=4228 Win=65792 Len=1		
406	3 95.610384	172.217.27.36	192.168.1.101	TCP	66 [TCP Keep-Alive ACK] 443 → 52016 [ACK	[] Seq=4228 Ack=650 Win=47104 Len=0 SLE=649 SRE=	650	
4064	4 95.808320	Shenzhen_28:a4:5a	Broadcast	ARP	42 Who has 192.168.1.102? Tell 192.168.1	.1		
4065	5 95.894145	192.168.1.101	192.168.1.255	NBNS	92 Name query NB WORKGROUP<1c>			
4066	5 96.645076	192.168.1.101	192.168.1.255	NBNS	92 Name query NB WORKGROUP<1c>			~
> Frame	1: 78 bytes	on wire (624 bits), 7	8 bytes captured (62	4 bits) on	interface 0			^
> Ether	net II. Src:	Azureway c9:8e:cf (74	:c6:3b:c9:8e:cf), Ds	t: Shenzhe	n 28:a4:5a (fc:dd:55:28:a4:5a)			
> Inter	net Protocol	Version 4, Src: 192.1	.68.1.101, Dst: 192.1	68.1.1	,			
> User	Datagram Pro	tocol, Src Port: 49376	(49376), Dst Port:	53 (53)				~
0000 4		4 En 74 aC 3h a0 8a a	£ 08 00 45 00 U/	74 .	E			
0000 1	0 40 2b =4 0	9 99 89 11 8h 52 c9 a	8 01 65 c0 38 GL	.21. j				
0020 0	1 01 00 00 0	0 35 00 2c 06 d3 de f	3 01 00 00 01	.5				
0030 0	0 00 00 00 0	0 00 04 61 75 74 68 0	9 67 72 61 6d	a uth.g	ram			
0040 6	d 61 72 6c 7	9 03 63 6f 6d 00 00 0	1 00 01 marl	y.co m	-			
				04.0				
07	wireshark_pcapn	g_F3F1D7D7-0967-4168-9832-9	A631ADF8018_2017082923	1658_a04688		Packets: 4071 · Displayed: 4071 (100.0%)	Profile: Def	fault

Gambar 1. Hasil Tracing Kompas.com

Setelah di dapatkan hasil tracing dari wireshark kemudian masukkan/load di aplikasi Rumint lalu di visualisasikan.



Gambar 2. Tampilan rumint setelah di load

🔛 rumint					×
File Toolba	rs View Help				
	4106	Buffer 1	Max Speed (pkts/see	d Max	loop
•	+ + 0 0	4106		10 ← ▶ Min	screenshots
<<	Play	Pause	Stop	>>	clear screen

Gambar 3. Setelah di play

Setelah di play terlihat bahwa di dalam file pcap itu terdapat 4106 data, buffer 1 dan kecepatan transmisinya 10 pkts/sec.



Gambar 4. Visualisasi dalam bentuk byte frequency



Gambar 5. Visualisasi dalam bentuk binary rainfall



Gambar 6. Tampilan visualisasi bentuk combined visualization

Kasus 2 (www.lk21.net)

Pada kasus kedua ini yaitu melakukan tracing data melalui streaming. Langkah-langkah nya sama seperti pada kasus yang pertama tadi.

📕 *Wi-	Fi				щ — <u>п</u>	×
File Ec	it View G	o Capture Analyze Statis	tics Telephony Wireless	Tools H	Help	
	6 💿 📘	🖹 🖹 🖸 । ९ 👄 🔿 🔮	₹ ₺ 🚆 🗏 🤤 🤤	Q. 🎹		
Apply	a display filter .	<ctrl-></ctrl->			Expression	+
No.	Time	Source	Destination	Protocol	Length Info	^
995	3 96.266561	119.110.77.232	192.168.1.101	TCP	1448 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]	
995					1448 [TCP Out-Of-Order] [TCP segment of a reassembled PDU]	
995	5 96.266600				66 [TCP Dup ACK 9952#1] 52350 → 80 [ACK] Seq=409 Ack=342925 Win=66816 Len=0 SLE=344319 SRE=345713	
995	6 96.266683	192.168.1.101	119.110.77.232	TCP	54 52350 → 80 [ACK] Seq=409 Ack=345713 Win=66816 Len=0	
995	7 96.282024	119.110.77.232			1448 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]	
995	8 96.282069				66 [TCP Dup ACK 9956#1] 52350 → 80 [ACK] Seq=409 Ack=345713 Win=66816 Len=0 SLE=347107 SRE=348501	
995	9 96.284567		192.168.1.101		1448 [TCP Out-Of-Order] [TCP segment of a reassembled PDU]	
996	0 96.284603	192.168.1.101	119.110.77.232	TCP	54 52350 → 80 [ACK] Seq=409 Ack=348501 Win=66816 Len=0	
996	1 96.288377	119.110.77.232	192.168.1.101	TCP	1448 [TCP segment of a reassembled PDU]	
996	2 96.293307	119.110.77.232	192.168.1.101	TCP	1448 [TCP segment of a reassembled PDU]	
996	3 96.293308	119.110.77.232	192.168.1.101	TCP	1448 [TCP segment of a reassembled PDU]	
996	4 96.293377	192.168.1.101	119.110.77.232	TCP	54 52350 → 80 [ACK] Seq=409 Ack=352683 Win=66816 Len=0	
996	5 96.293876	119.110.77.232	192.168.1.101	TCP	1448 [TCP segment of a reassembled PDU]	
996	6 96.293879	119.110.77.232	192.168.1.101	TCP	1448 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]	
996	7 96.293946	192.168.1.101	119.110.77.232	TCP	66 52350 → 80 [ACK] Seq=409 Ack=354077 Win=66816 Len=0 SLE=355471 SRE=356865	~
> Fram	e 1: 62 byt	es on wire (496 bits),	62 bytes captured (49	5 bits) on	n interface 0	
> Ethe	rnet II, Sr	c: Shenzhen_28:a4:5a (f	c:dd:55:28:a4:5a), Ds	t: Azurewa	av_c9:8e:cf (74:c6:3b:c9:8e:cf)	
<pre>> Inte</pre>	rnet Protoc	ol Version 4, Src: 208.	93.230.133, Dst: 192.	168.1.101		
> Tran	smission Co	ntrol Protocol, Src Por	t: 8080 (8080), Dst P	ort: 52286	6 (52286), Seq: 1, Ack: 1, Len: 8	
0000	74 c6 3b c9	8e cf fc dd 55 28 a4 !	5a 08 00 45 28 t.;.	U(.Z.	E(
0010	30 30 f3 ab	40 00 2e 06 e0 03 d0	5d e6 85 c0 a8 .0(@].		
0020	01 65 1f 90	cc 3e 92 0a 3a 34 4c	57 a8 1a 50 18 .e	.> :4LW.		
0030	30 ee 06 8c	00 00 81 06 6e 3a 32	63 61 36	n:2ca	a6	
0 7	wireshark_pca	png_F3F1D7D7-0967-4168-9832-	9A631ADF801B_20170829233	128_a08152	Packets: 10149 · Displayed: 10149 (100.0%) Profile: Defau	ilt

Gambar 7. Tracing data streaming (www.lk21.net)

🔟 rumint				×
File Toolbars View Help				
11105	Buffer 1 11105	Max Speed (pkts/sec)	Max	loop
•	11100	•	Min	screenshots
<< Play	Pause	Stop 🗦	·>	clear screen

Gambar 8. Tampilan rumint

Setelah di load terdapat 11105 data pada file pcap streaming (<u>www.lk21.net</u>), buffer 1 dan kecepatan transmisinya 1000 pkts/sec karena data yang banyak jadi kecepatan saat visualisa si di percepat.



Gambar 9. Tampilan visualisasi bentuk byte frequency



Gambar 10. Tampilan visualisasi bentuk parallel coordinate plot



Gambar 11. Tampilan Visusalisasi bentuk combined visualization

III. Analisa

Setelah melakukan tracing data dan melakukan visualisasi terlihat bahwa data pada streaming lebih banyak karena pada streaming pengiriman data dari source ke destination nya lebih besar di bandingkan dengan browsing biasa. Pada visualisasi terlihat bahwa pada pengiriman paket data melewati rute terbaik dengan melihat ip address.

IV. Referensi

Anonim.(online) <u>http://www.rumint.org/</u>. Diakses pada tanggal 5 September 2017.

Kumara, Endi.2017. Analisis Paket Data dengan Mengunakan Wireshark dan Command

Prompt. (online) <u>http://edocs.ilkom.unsri.ac.id/cgi/users/home</u>. Diakses pada tanggal 5 September 2017.