# Virtualisasi dalisis Data .pcap Wireshark

Created by Henny Pratiwi\_09011281520129

# Virtualisasi dan Analisis Data .pcap Wireshark

Setelah menyimpan data capture wireshark kedalam format pcap kemudian download aplikasi rumint v.214 pada <u>www.rumint.org</u>

Setelah itu install dan running aplikasi, maka akan tampil kontak dialog seperti pada gambar dibawah ini:

🔤 rumint								×	
File	Toolbars	View	Help						
				0	Buffe	r Max 1 (pkt	Speed s/sec)	Max	loop
•					Ma.	x	•		screenshots
<	<		Play		Pause	Stop		•>	clear screen

Pilih dan klik file, kemudian pilih dan klik juga load pcap dataset dan klik play

Setelah itu pada kolom view akan ada berbagai data yang bisa dilihat :

1. Scatter plot :



1

Pada data ini kita dapat melihat angka-angka yang berisi ip address pada source maupun destination.

2. Byte frequency



pada data ini dapat kita lihat garis hijau kuning saling memotong antara vertical dan horizontal.

3. Parallel coordinate plot



Pada gambar plot ini menunjukan dimana pada souce menuju ke berbagai destination yang dikunjungi .

## 4. Text rainfall

🖂 rumi	int: Text Rainfall			$\times$
1407>	~E.Y.6@f.%	_D2CA5178sub	googl	ecast.
1408>	Pti.E.NE.f.I.f	FHFAEBEECACAC	ACACACAC	ACACAC
1409>	33Pti`HX.u.;d	<b>u</b> "	W	pad
1410>	33Pti`HX.u.;d	<b>u</b>	W	pad
1411>	Fti.E.2Jtf.IFz"	wpad		
1412>		wpad		
1413>	^s.E. (ys.f.			
1414>				
1415>		TTP/1.1.HOST:	239.255	.255.2
1416>	UJEl;k.mE`@.6.Bf.=.PLP.u@.n'	"**"!==d  !g.se	elector)	(m.s
1417>		TTP/1.1.HOST:	239.255	.255.2
1418>	l;k.mUJEE(,0@f.=PPP			
1419>	33Pti	u"	w	pad
1420>		wpad		
1421>		_805741C9sul	googl	ecast.
1422>	l;k.mJJE.E.]&G@Z;.f.=0]T.0.[.P.?.4	0i.uVGc		*!-p^-
1423>				
1424>	l;k.mUJEE)=.@r<.f.=Pp]P			
1425>	UJEl;k.mEa@.6.Bf.=.PP.u@.*	n.isWindow(e)	{m=e[h]	, m&& (e
1426>	l;k.mUJE.E.(,q@f.=PPZg			
1427>	UJEl;k.mEb@.6.Bf.=.PP.u@e	=h.props?this	props.c	oncat (
1428>	l;k.mUJE.E.(,r@f.=PhPT			
1429>	Pti.E.NE.f.I.f	FHFAEBEECACAC	ACACACAC	ACACAC
1430>				
1431>	^s.E. (yas.f			
1432>	l;k.mUJE.E.V.@f.=J}\$\$			<b>u</b>
1433>	UJEl;k.mE`@.m.yIof.=0.[]U,PW	×	2R7.9.w.	.~.R1.
1434>	l;k.mUJEE(&H@Zo.f.=o]U,0.\.P.?{.n			
1435>	Z.PZ.P.d.Id			-
1436>	UJEl;k.mE(@.6jf.=.P]pP&.[			
1400>	l;k.mUJEE(,m@f.=PPPk			
1401>	x=£			
1402>	**dd.			
1403>		TTP/1.1.HOST:	239.255	.255.2
1404>	UJEl;k.mE@.6.Bf.=.PP.u@.uk	o,e,d,c)})}n.ev	/ent={gl	obal:(
1405>	l;k.mUJE.E.(,n@f.=PLPe.			
ASCIL				
AJCII	Strip Ether Header Show Strips of Length N			

Pada gambar diatas menunjukan port dan text url yang dikunjungi.

5. Binary rainfall

rumint: Binary Rainfall		$\times$
o Static Scroll Highlight		
Printable ASCI		

Pada gambar diatas menunjukan aliran binary dalam berupa garis horizontal bewarna hijau kuning,orange.

#### 6. Combined visualization



pada gambar ini adalah kombinasi dari data view gambar kelima diatas sebelumnya.

### 7. Filter

☑ filters			×
TCP	Min TCP SRC Port	0 0	
UDP	Max TCP SRC Port	65535 65535	
ICMP	Min TCP DST Port	0 0	
IGMP	Max TCP DST Port	65535   65535	
other legal	Min UDP SRC Port	0 0	Change
ounernegar	Max UDP SRC Port	65535 65535	change
unassigned	Min UDP DST Port	0 0	
	Max UDP DST Port	65535 65535	
	Min Packet Length	0 0	
	Max Packet Length	1518 1518	

Pada setiap garis bewarna diatas merupakan perwakilan dari nama-nama protocol maupun yang lainnya seperti pada tertera gambar ini.