

FIND THE PCAP VISUALIZATION & ANALYZE



DISUSUN OLEH:

NAMA : QONITA AL'AFWA

NIM : 09011281520103

KELAS : SK5C

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

FIND THE PCAP VISUALIZATION & ANALYZE

Hasil capture pada Wireshark (KapanLagi.com) yang menampilkan bentuk traffic yang warna-warni di mana terdapat keterangan seperti :

- Time (menampilkan waktu paket tersebut tertangkap);
- Source (menampilkan IP Source dari paket tersebut);
- Destination (menampilkan IP Destination dari paket tersebut);
- Protocol (menampilkan protokol yang difungsikan paket data tersebut);
- Info (menampilkan info detail paket tersebut).

The screenshot shows the Wireshark interface with a packet capture list and details pane. The packet list shows various protocols including TCP, TLSv1.2, and DNS. The details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
2...	85.399289	203.12.21.10	192.168.43.134	TCP	441	443 → 59279 [ACK] Seq=213956 Ack=3265 Win=263168 Len=387 [TCP segment of a reassembled PDU]
2...	85.439186	192.168.43.134	203.12.21.10	TCP	54	59279 → 443 [ACK] Seq=3265 Ack=214343 Win=66304 Len=0
2...	85.747330	192.168.43.134	203.12.21.5	TCP	55	[TCP Keep-Alive] 59273 → 443 [ACK] Seq=2143 Ack=11385 Win=65792 Len=1
2...	86.274942	38.72.130.155	192.168.43.134	TCP	54	443 → 59326 [RST, ACK] Seq=4555 Ack=8758 Win=0 Len=0
2...	86.275318	38.72.130.155	192.168.43.134	TCP	54	443 → 59326 [RST, ACK] Seq=4555 Ack=8293 Win=0 Len=0
2...	86.275430	203.12.21.10	192.168.43.134	TCP	1454	443 → 59279 [ACK] Seq=214343 Ack=3265 Win=263168 Len=1400 [TCP segment of a reassembled PDU]
2...	86.275552	203.12.21.10	192.168.43.134	TCP	197	443 → 59279 [PSH, ACK] Seq=215743 Ack=3265 Win=263168 Len=143 [TCP segment of a reassembled PDU]
2...	86.275681	203.12.21.5	192.168.43.134	TCP	54	[TCP Keep-Alive ACK] 443 → 59273 [ACK] Seq=11385 Ack=2144 Win=263168 Len=0
2...	86.275734	172.217.17.46	192.168.43.134	TCP	66	443 → 59371 [ACK] Seq=4824 Ack=2007 Win=51456 Len=0 SLE=747 SRE=1877
2...	86.275819	172.217.17.46	192.168.43.134	TLSv1.2	326	Application Data
2...	86.275895	172.217.17.46	192.168.43.134	TLSv1.2	870	Application Data, Application Data
2...	86.275958	172.217.17.46	192.168.43.134	TLSv1.2	100	Application Data
2...	86.276064	192.168.43.134	203.12.21.10	TCP	54	59279 → 443 [ACK] Seq=3265 Ack=215886 Win=66560 Len=0
2...	86.276324	192.168.43.134	172.217.17.46	TCP	54	59371 → 443 [ACK] Seq=2007 Ack=5912 Win=66048 Len=0
2...	86.278349	192.168.43.134	8.41.222.241	TCP	54	59349 → 443 [FIN, ACK] Seq=554 Ack=4468 Win=64061 Len=0
2...	86.278637	192.168.43.134	52.220.86.28	TCP	54	59369 → 443 [FIN, ACK] Seq=1 Ack=1 Win=65792 Len=0
2...	86.278762	192.168.43.134	52.74.109.40	TCP	54	59368 → 443 [FIN, ACK] Seq=1 Ack=1 Win=65792 Len=0
2...	86.278914	192.168.43.134	38.72.130.155	TCP	66	59373 → 443 [SYN] Seq=0 Win=65520 Len=0 MSS=1460 WS=256 SACK_PERM=1
2...	86.281134	192.168.43.134	172.217.17.46	TLSv1.2	100	Application Data
2...	86.311270	192.168.43.134	203.12.21.10	TLSv1.2	183	Application Data
2...	86.312173	192.168.43.134	192.168.43.1	DNS	71	Standard query 0x8579 A s.ytimg.com
2...	86.530475	192.168.43.134	38.72.130.155	TCP	66	59374 → 443 [SYN] Seq=0 Win=65520 Len=0 MSS=1460 WS=256 SACK_PERM=1

Hasil capture pada rumint 2.14

The screenshot shows the rumint application interface. It features a speedometer displaying '4400' in green, with 'Buffer 1' and 'Max Speed (pkts/sec) 4400' below it. The interface includes playback controls: '<<', 'Play', 'Pause', 'Stop', and '>>'. There are also buttons for 'loop', 'screenshots', and 'clear screen'.

Pada saat klik file → load pcap dataset

Maka muncul angka/nilai pada rumint

Rumint adalah

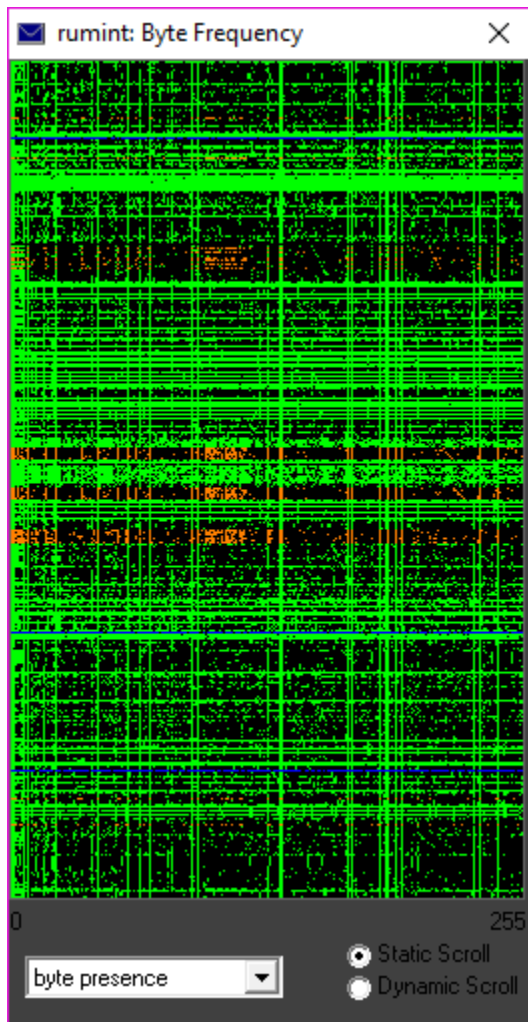
Tahap selanjutnya ialah

- Klik play pada rumint
- Klik view

Hasil capture pada rumint : Text Rainfall

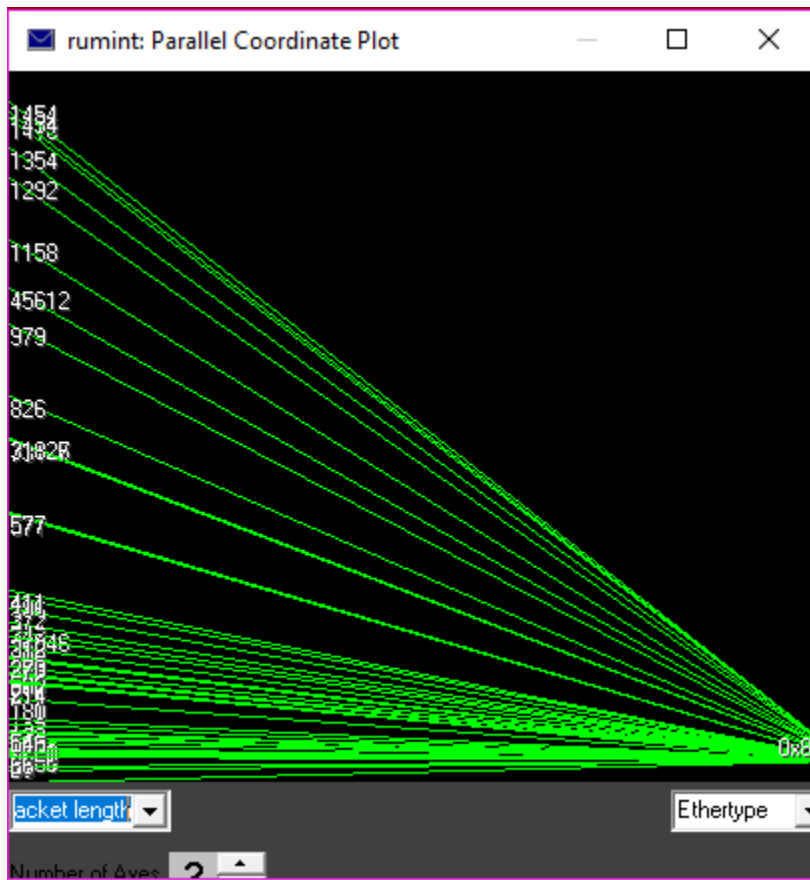
```
<308> .:.]...Z...E...4r.@...V...+...Dd..l.Y.....1.3.l.Y.
<309> .:.]...Z...E...8#.....?...+...+...5.$.#v.....a.props.id.....
<310> .:.]...Z...E...J#.....>...+...+...5.6j.....d5nxst8fru4z.cloudfront.n
<311> .:.]...Z...E...9#.....?...+...+...5.%_.....d.infeed.id.....
<312> ...Z...:.]...E...[.w.....+.....J...=P...m...4.n.2Y...o.....U..5.P.c.
<313> .:.]...Z...E...({.@.....+.....c...P...#...
<314> ...Z...:.]...E...\.w.....+.....=P...{...U..w6...RVb...}0d..$...
<315> .:.]...Z...E...({.@.....+.....c...:P.....
<316> ...Z...:.]...E...A.w.....+.....=P...iN...['h..S.x-G.A...z.....L
<317> .:.]...Z...E...({.@.....+.....c...P...3...
<318> ...Z...:.]...E...!@.....Hd...+.....=..bS.=P..h%).....U...Q..D...Q~?;,;#..P.
<319> ...Z...:.]...E..."@.....Hd...+.....=..bS.=P..h...H.....0..1.0...U...USl.
<320> .:.]...Z...E...(Q.@.....+...Hd...bS.=...P.....
<321> .:.]...Z...E...@...@...+.....|.....P...3R...../...z.)?....
<322> ...Z...:.]...E...#@.....Hd...+.....=..bS.=P..h.....Class 3 Public Primary C
<323> .:.]...Z...E...~Q.@...2...+...Hd...bS.=...|P...}W.....L.....7..1..6+'
<324> ...Z...:.]...E...q.w.....+.....cP...H.....]9...D.Ek?fb.@:...wLv.
<325> .:.]...Z...E...({.@.....+.....c...*P.....
<326> ...Z...:.]...E...28.@.@)...+...+...5.|.F.....scontent-sin6-2.xx.fbcdn.n
<327> ...Z...:.]...E...\.8.@.@)...+...+...5.w.HuG.....scontent.fp1ml-1.fna.fbcdn
<328> ...Z...:.]...E...k8.@.@)...+...+...5.5.W.0V%.....www.facebook.com.....
<329> ...Z...:.]...E...X9.@.@)...+...+...5...D...#v.....a.props.id.....
<330> ...Z...:.]...E...9.@.@)J...+...+...5...N.....d5nxst8fru4z.cloudfront.n
<331> ...Z...:.]...E...W9.@.@)...+...+...5.)C.k.....d.infeed.id.....m
<332> ...Z...:.]...E...w..J...+.....cP...C..D...l.....Vn9"Tk.o.E.
<333> ...Z...:.]...E...b.w.....+.....*...cP...J.,+...../C.....3\<.X
<334> ...Z...:.]...E...c.w.....+.....cP...#..f.a.>..K!.8.X.NB.bV..)\8..
<335> ...Z...:.]...E...w.....+.....cP...Z..'cV..M.....%K.]...R...W+
<336> .:.]...Z...E...4{.@.....+.....c...*.....
<337> .:.]...Z...E...4{.@.....+.....c.....t.....
<338> .:.]...Z...E...({.@.....+.....c...P...S...
<339> .:.]...Z...E...4x[@..."+...+...9...w..r.....#.....
<340> .:.]...Z...E...D#.....?...+...+...5.0Q..._.....d.kapanlaginetwork.com...
<341> .:.]...Z...E...45.@.....+h..\...[".....+.....
<342> .:.]...Z...E...@#.....?...+...+...5,..gW.....graph.facebook.com.....
<306> .:.]...Z...E...;c.@..._...+.....(X.P...)m.....r=Qh}+h.YW.ni.b
```

Hasil capture pada rumint : Byte Frequency

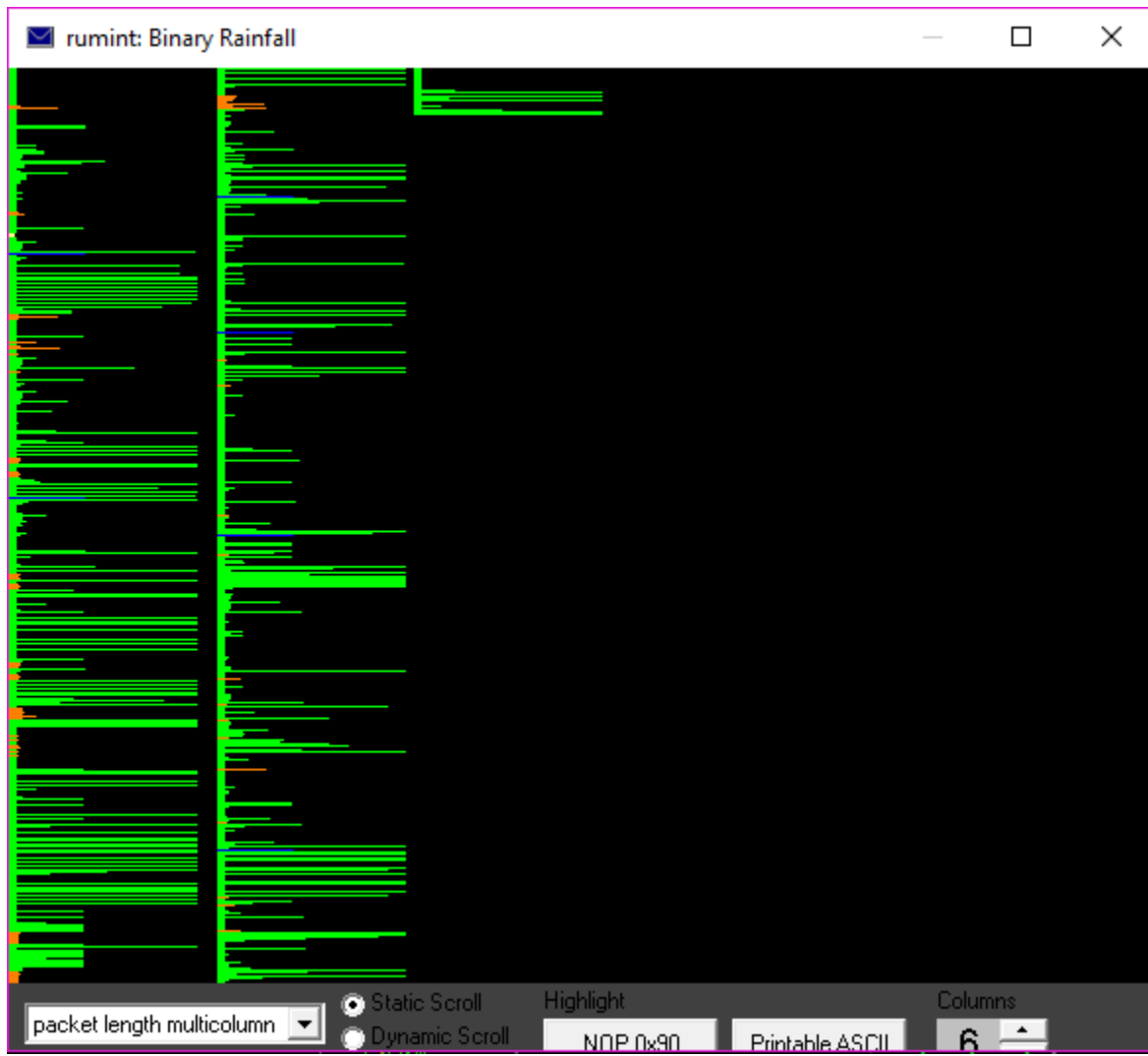


Byte Frequency maka akan muncul yaitu frekuensi byte pada suatu paket.

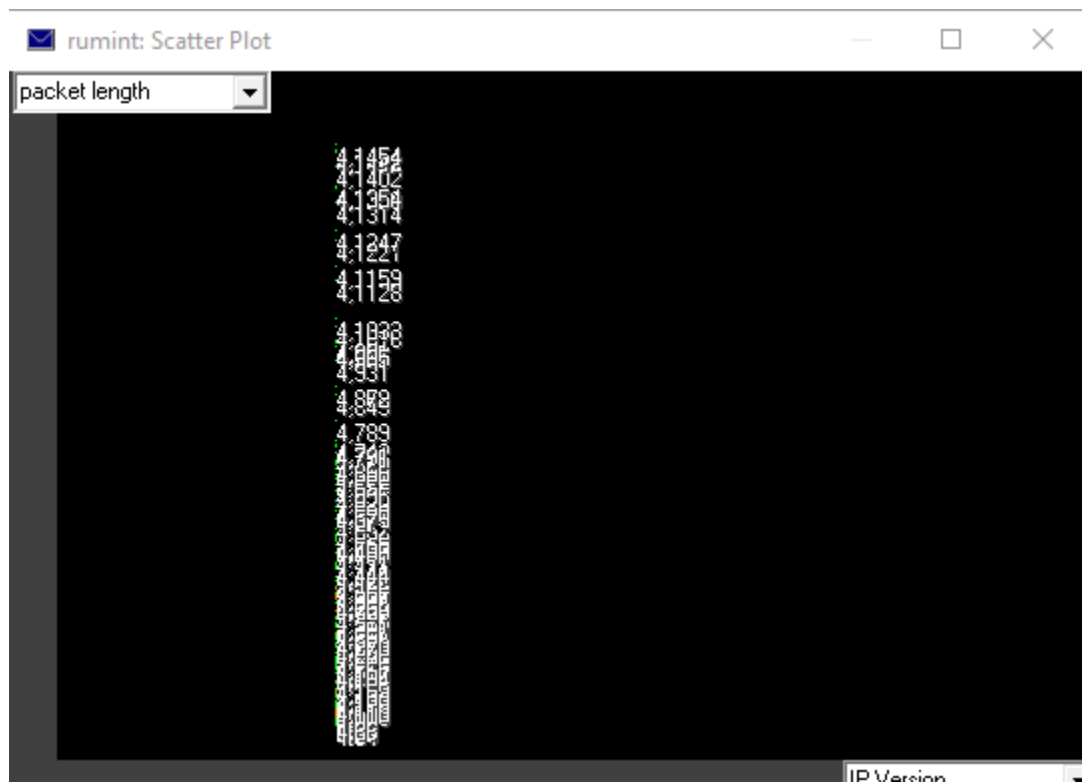
Hasil capture pada rumint : Parallel Coordinate Plot



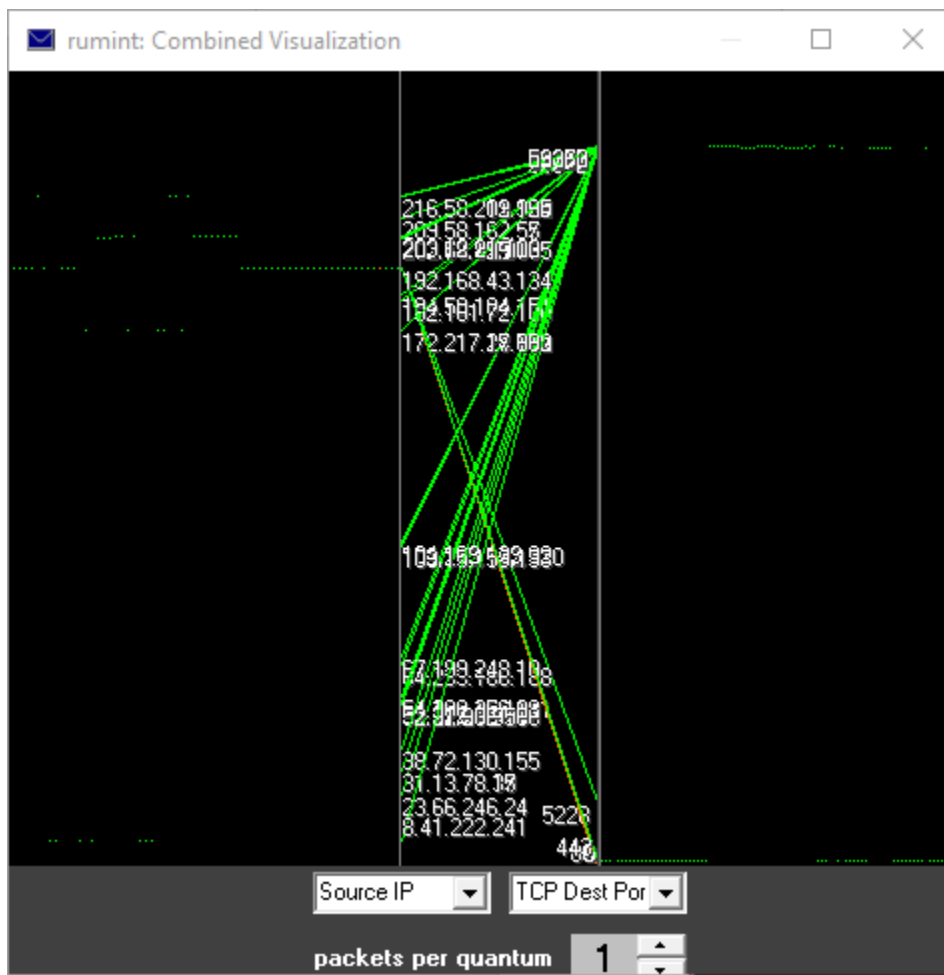
Hasil capture pada rumint : Binary Rainfall



Hasil capture pada rumint : Scatter Plot

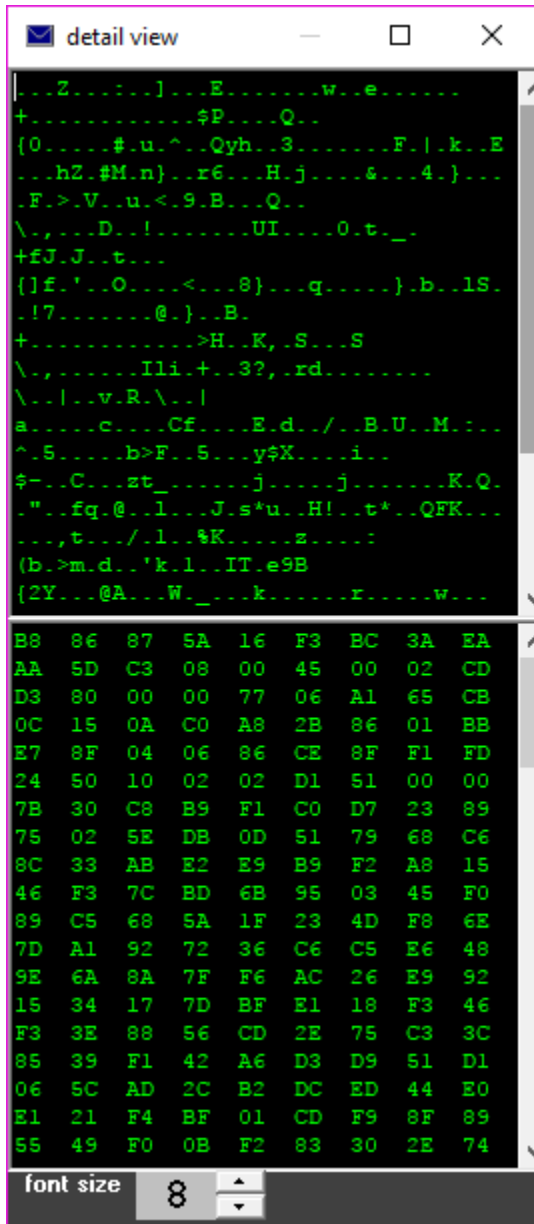


Hasil capture pada rumint : Combined Visualization



Combined Visualization maka akan terlihat masing-masing IP Source.

Hasil capture pada rumint : Detail View



Detail view maka keluar angka/huruf pada hexadecimal.

Hasil capture pada Wireshark (Vidio.com)

The screenshot displays the Wireshark interface with a network capture of an HTTP transaction. The packet list pane shows several packets, with packet 4 highlighted in red. The packet details pane shows the structure of the HTTP request, including the status line 'HTTP/1.1 304 Not Modified' and various headers. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	23.66.237.138	192.168.43.133	HTTP	469	HTTP/1.1 304 Not Modified
2	0.000192	172.217.19.206	192.168.43.133	TCP	66	443 → 49832 [ACK] Seq=1 Ack=1 Win=205 Len=0 SLE=176 SRE=1436
3	0.000606	192.168.43.133	172.217.19.206	TLSv1.2	1314	Ignored Unknown Record
4	0.021438	192.168.43.133	23.66.237.138	TCP	54	49953 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.022645	192.168.43.133	23.212.120.152	TCP	54	49951 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	0.022808	192.168.43.133	23.66.237.138	TCP	54	49954 → 80 [RST, ACK] Seq=1 Ack=416 Win=0 Len=0
7	0.061367	23.66.237.138	192.168.43.133	HTTP	469	[TCP Spurious Retransmission] HTTP/1.1 304 Not Modified
8	1.219280	192.168.43.133	172.217.19.206	TCP	1314	[TCP Retransmission] 49832 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1260
9	1.220961	172.217.19.206	192.168.43.133	TCP	66	[TCP ACKed unseen segment] 443 → 49832 [ACK] Seq=1 Ack=1436 Win=216 Len=0 SLE=176 SRE=1261
10	1.221101	172.217.19.206	192.168.43.133	TLSv1.2	100	[TCP ACKed unseen segment] [TCP Previous segment not captured], Application Data
11	1.221179	172.217.19.206	192.168.43.133	TCP	1185	[TCP ACKed unseen segment] [TCP Out-Of-Order] 443 → 49832 [PSH, ACK] Seq=106 Ack=1436 Win=216 Len=1051
12	1.221223	172.217.19.206	192.168.43.133	TCP	159	[TCP ACKed unseen segment] [TCP Out-Of-Order] 443 → 49832 [PSH, ACK] Seq=1 Ack=1436 Win=216 Len=1051
13	1.221304	172.217.19.206	192.168.43.133	TCP	92	[TCP ACKed unseen segment] [TCP Out-Of-Order] 443 → 49832 [PSH, ACK] Seq=1157 Ack=1436 Win=216 Len=38
14	1.221348	192.0.77.2	192.168.43.133	TLSv1.2	100	Application Data
15	1.221402	192.0.77.2	192.168.43.133	TLSv1.2	85	Encrypted Alert
16	1.221439	192.0.77.2	192.168.43.133	TCP	54	443 → 49796 [FIN, ACK] Seq=78 Ack=1 Win=62 Len=0
17	1.221518	192.168.43.133	172.217.19.206	TCP	66	[TCP Previous segment not captured] 49832 → 443 [ACK] Seq=1436 Ack=1 Win=254 Len=0 SLE=1195 SRE=1241
18	1.221783	192.168.43.133	172.217.19.206	TCP	74	[TCP Dup ACK 3#1] 49832 → 443 [ACK] Seq=1436 Ack=1 Win=254 Len=0 SLE=106 SRE=1157 SLE=1195 SRE=1241
19	1.221850	192.168.43.133	172.217.19.206	TCP	66	49832 → 443 [ACK] Seq=1436 Ack=1157 Win=258 Len=0 SLE=1195 SRE=1241
20	1.221917	192.168.43.133	172.217.19.206	TCP	54	49832 → 443 [ACK] Seq=1436 Ack=1241 Win=258 Len=0
21	1.221984	192.168.43.133	192.0.77.2	TCP	54	49796 → 443 [ACK] Seq=1 Ack=78 Win=256 Len=0
22	1.222042	192.168.43.133	192.0.77.2	TCP	54	49796 → 443 [ACK] Seq=1 Ack=79 Win=256 Len=0

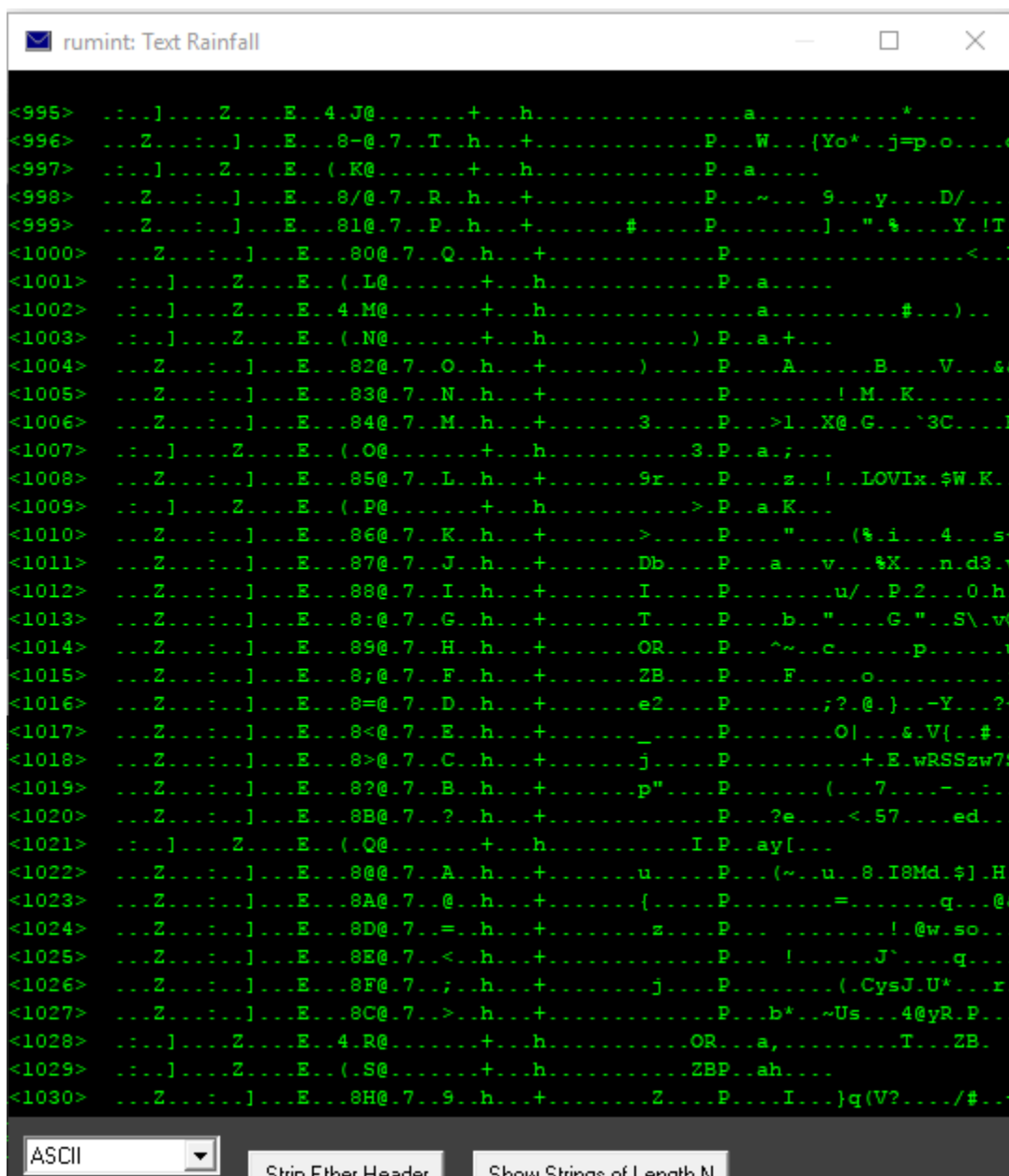
Hasil capture pada rumint 2.14

The screenshot displays the rumint application interface. The main display shows a large green number '3238' representing the current buffer size. Below it, there are controls for 'Max Speed' (1 pkt/s) and 'Max' (10). The interface also includes buttons for 'loop', 'screenshots', 'clear screen', 'Play', 'Pause', 'Stop', and navigation arrows.

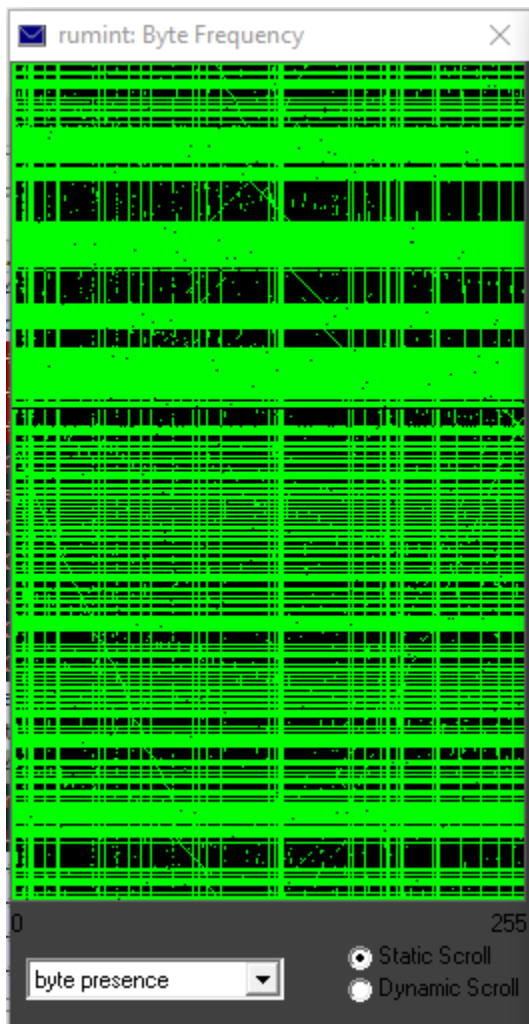
Pada saat klik file → load pcap dataset

Maka muncul angka/nilai pada rumint

Hasil capture pada rumint : Text Rainfall

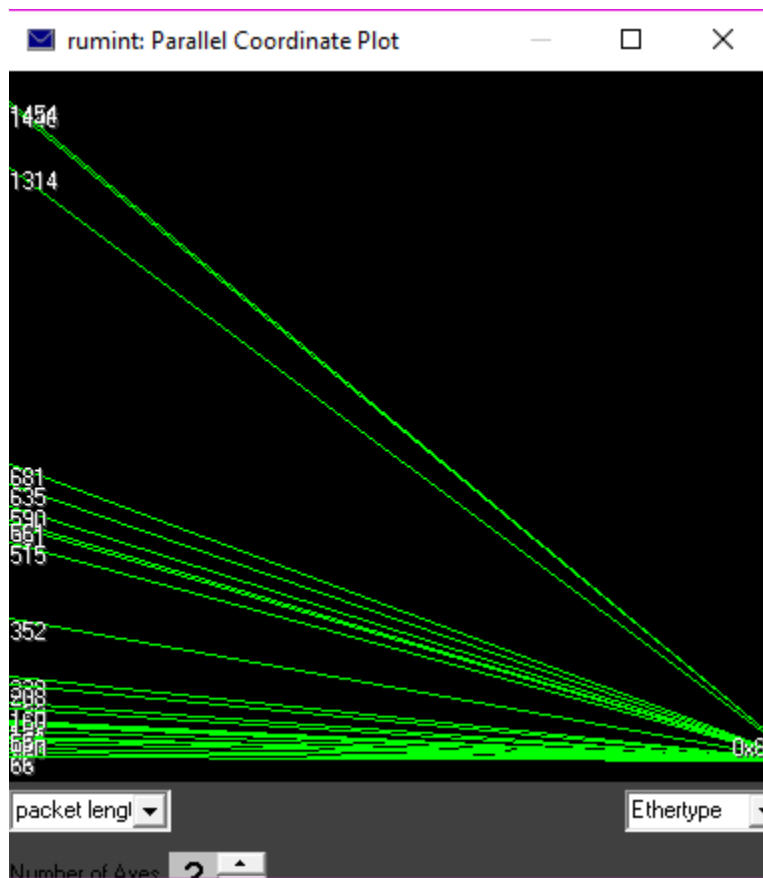


Hasil capture pada rumint : Byte Frequency

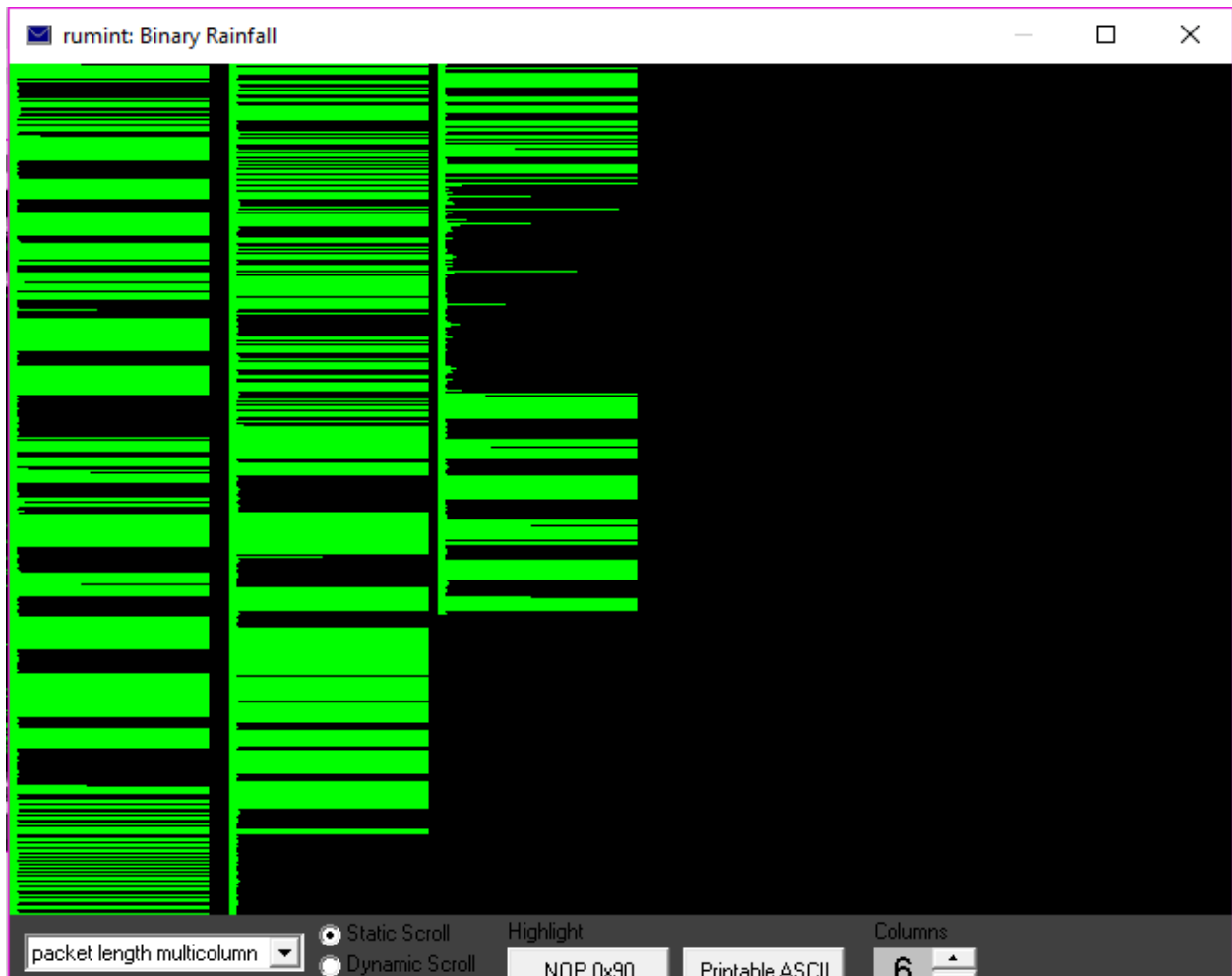


Byte Frequency maka akan muncul yaitu frekuensi byte pada suatu paket.

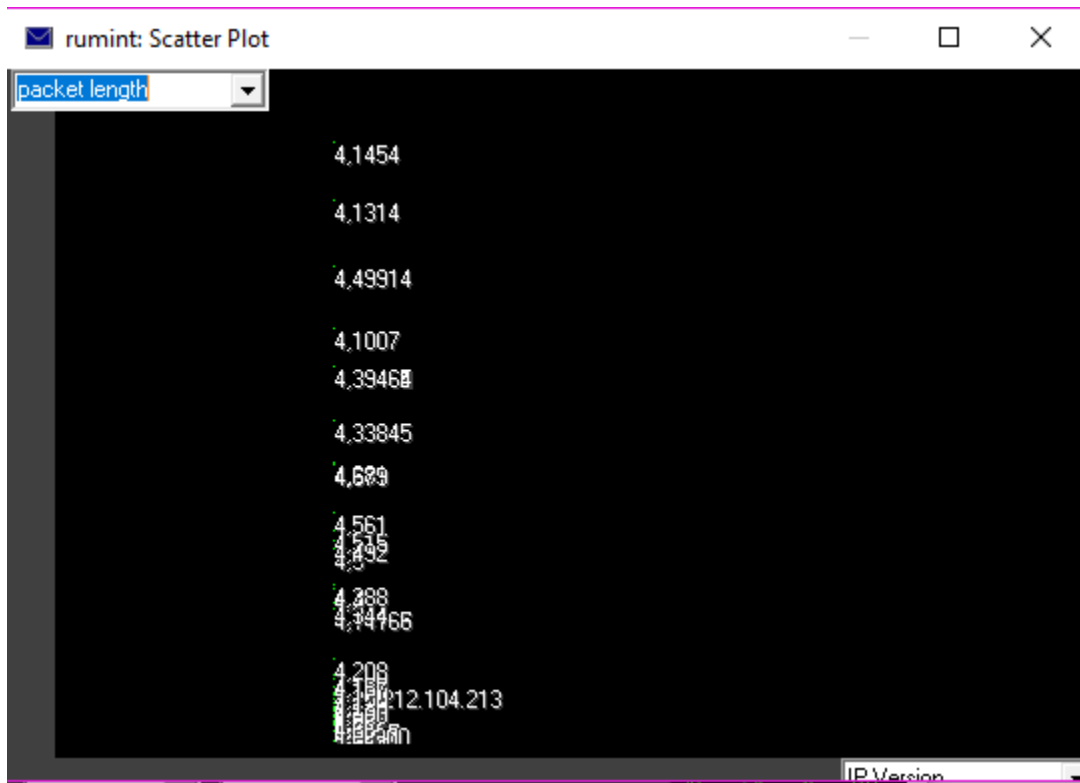
Hasil capture pada rumint : Parallel Coordinate Plot



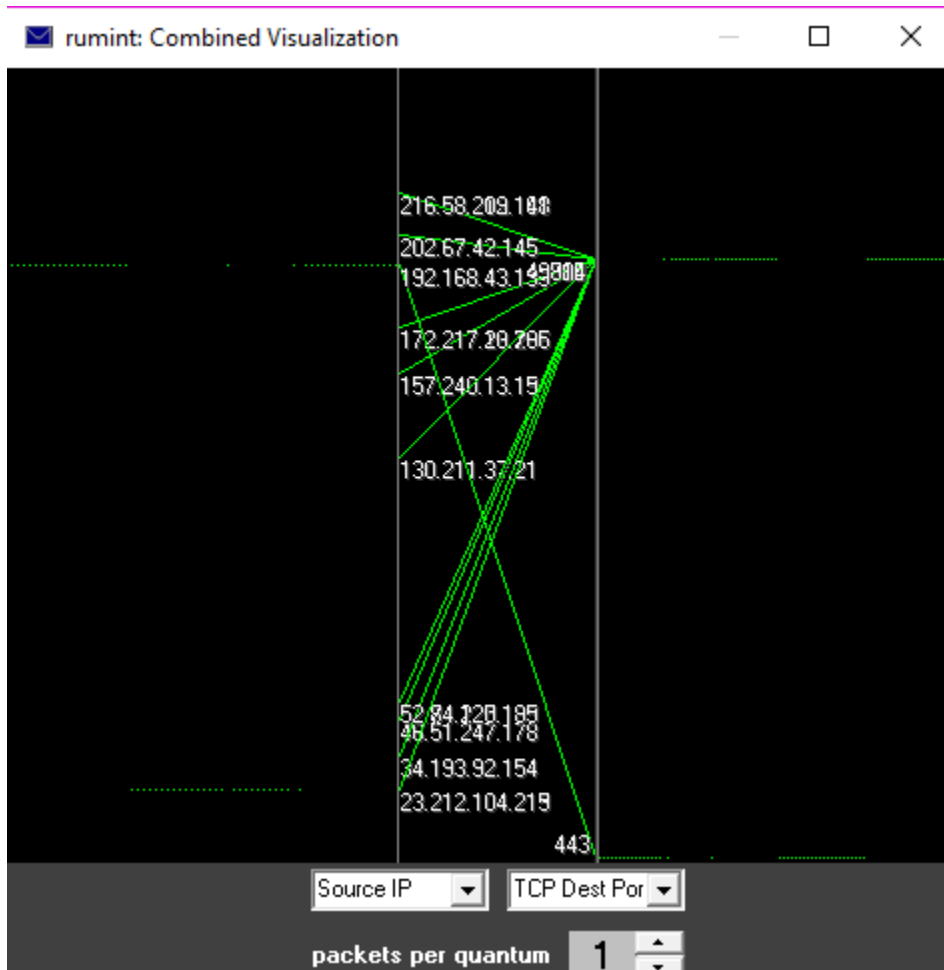
Hasil capture pada rumint : Binary Rainfall



Hasil capture pada rumint : Scatter Plot

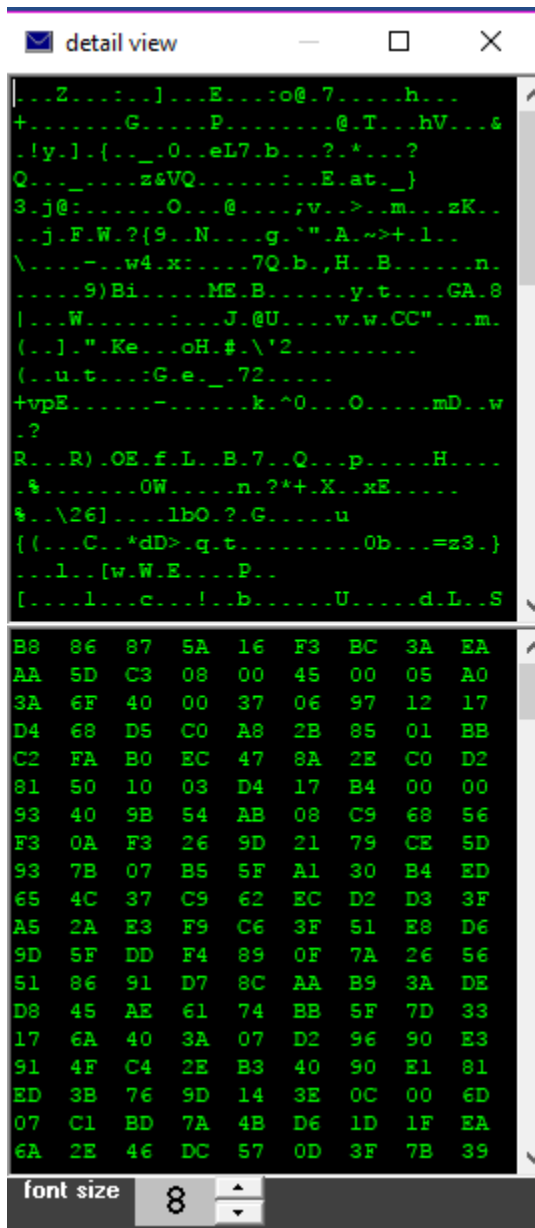


Hasil capture pada rumint : Combined Visualization



Combined Visualization maka akan terlihat masing-masing IP Source.

Hasil capture pada rumint : Detail View



```
detail view
[...Z...].E...o@.7...h...
+.....G.....P.....@.T...hV...&
.!y.l.{..._0...eL7.b...?.*...?
Q...z&VQ.....E.at_)
3.j@:.....O...@...;v...>...m...zK...
.j.F.W.?(9..N...g.`".A.~>.l...
\...-...w4.x:...7Q.b.,H..B.....n.
.....9)Bi.....ME.B.....y.t...GA.8
|...W.....J.@U...v.w.CC"...m.
(..)."Ke...oH.#.\'2.....
(..u.t...:G.e._72.....
+vpE.....-.....k.^0...O.....mD..w
.?
R...R).OE.f.L..B.7..Q...p....H....
.%.....0W.....n.?*+X..xE.....
%.\26]....lbO?.G.....u
{(...C...*dD>.q.t.....0b...=z3.)
...l..[w.W.E...P..
[...l...c...!.b.....U.....d.L..S
B8 86 87 5A 16 F3 BC 3A EA
AA 5D C3 08 00 45 00 05 A0
3A 6F 40 00 37 06 97 12 17
D4 68 D5 C0 A8 2B 85 01 BB
C2 FA B0 EC 47 8A 2E C0 D2
81 50 10 03 D4 17 B4 00 00
93 40 9B 54 AB 08 C9 68 56
F3 0A F3 26 9D 21 79 CE 5D
93 7B 07 B5 5F A1 30 B4 ED
65 4C 37 C9 62 EC D2 D3 3F
A5 2A E3 F9 C6 3F 51 E8 D6
9D 5F DD F4 89 0F 7A 26 56
51 86 91 D7 8C AA B9 3A DE
D8 45 AE 61 74 BB 5F 7D 33
17 6A 40 3A 07 D2 96 90 E3
91 4F C4 2E B3 40 90 E1 81
ED 3B 76 9D 14 3E 0C 00 6D
07 C1 BD 7A 4B D6 1D 1F EA
6A 2E 46 DC 57 0D 3F 7B 39
font size 8
```

Detail view maka keluar angka/huruf pada hexadecimal.

Referensi

<https://edocs.ilkom.unsri.ac.id/cgi/users/home?screen=EPrint::View&eprintid=1464>