BAB IV

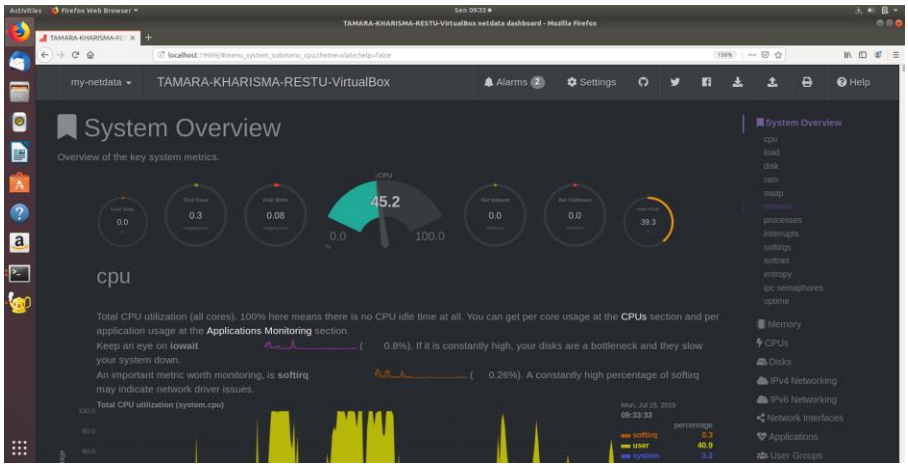
PENGUJIAN DAN ANALISIS

4.1 Pendahuluan

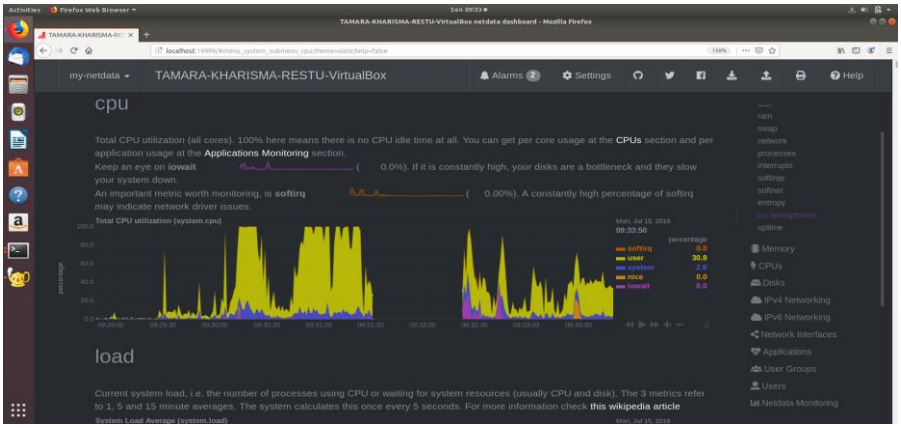
Pada bab ini dilakukan pengujian dan pengambilan data yang akan digunakan untuk analisis. Metode pengambilan data yang dilakukan mengacu pada bab III metodologi penelitian. Pada hasil pengujian akan dilakukan *feature extraction* dari masing-masing 3 skenario pada metodologi penelitian, yaitu pada skenario 1 ketika cloud diserang *brute force* menggunakan Kali Linux v.4.13 dengan wordlist 1000 dalam durasi 10 menit, skenario 2 ketika cloud diserang DoS dengan durasi 10 menit, dan terakhir pada skenario 3 ketika user mengupload file tinggi. Kemudian melakukan validasi data perbandingan hasil ektraksi fitur dengan data hasil *capture* pada *wireshark*.

4.2 Hasil Pengujian Monitoring Data

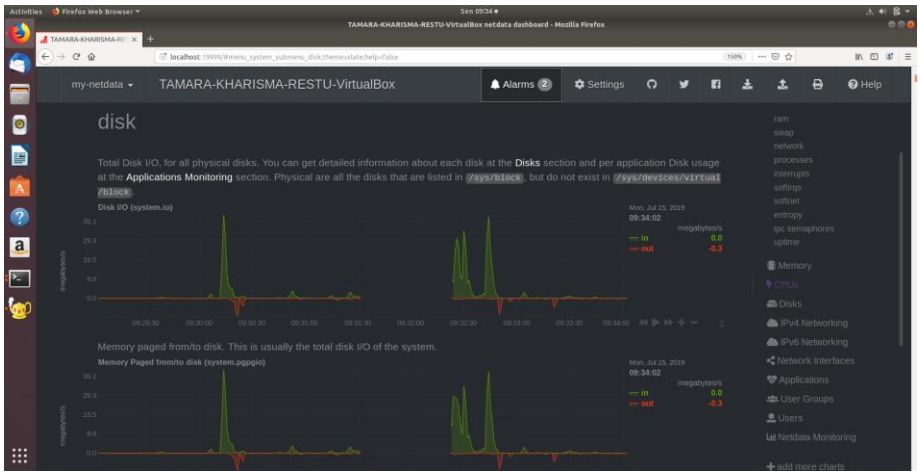
4.2.1 Pengujian pada Skenario 1



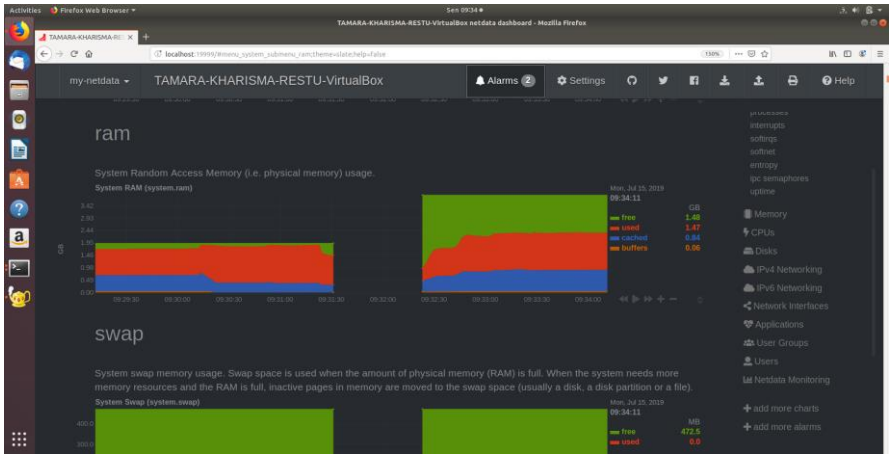
Gambar 4.1 Dashboard hasil pengujian skenario 1 menggunakan Netdata



Gambar 4.2 CPU Usage pengujian 1 menggunakan Netdata

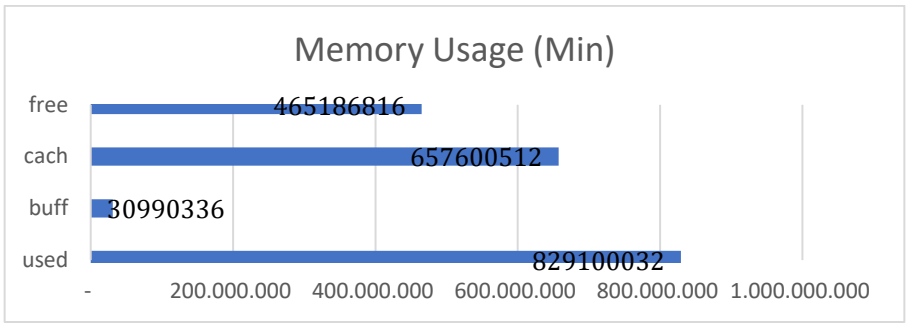


Gambar 4.3 Disk Usage pengujian 1 menggunakan Netdata

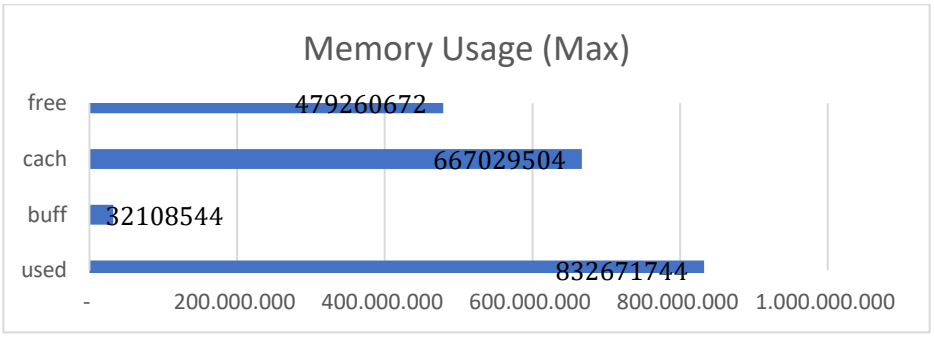


Gambar 4.4 RAM Usage pengujian 1 menggunakan Netdata

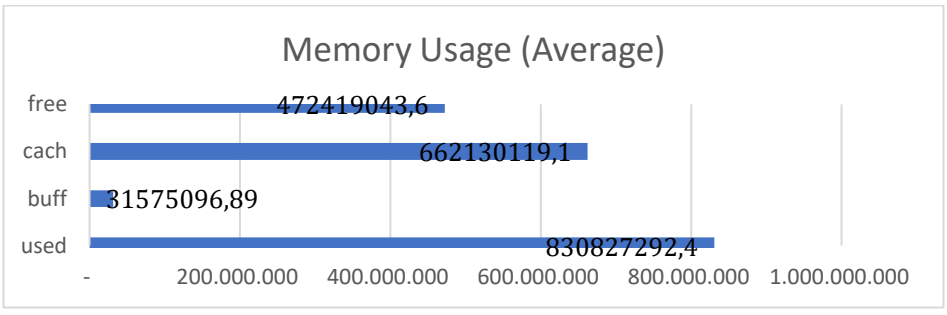
Hasil pengujian pertama pada skenario 1 yaitu ketika *Cloud* diserang dengan *brute force* menggunakan Kali Linux v.4.13. Dengan wordlist 1000 dalam durasi 10 menit, didapatkan hasil sebagai berikut:



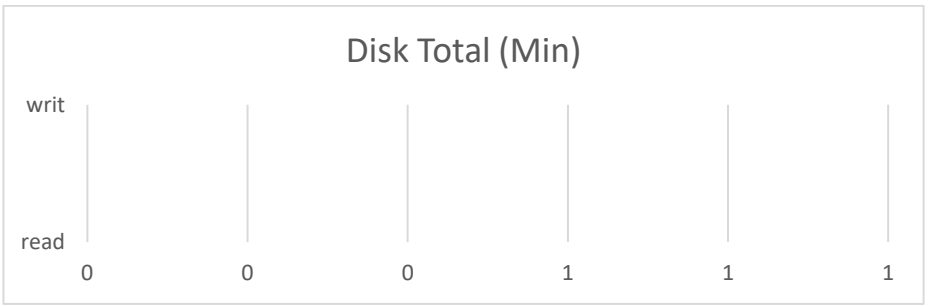
Gambar 4.5 Data Minimal RAM (Memory Usage) pada Scenario Pertama



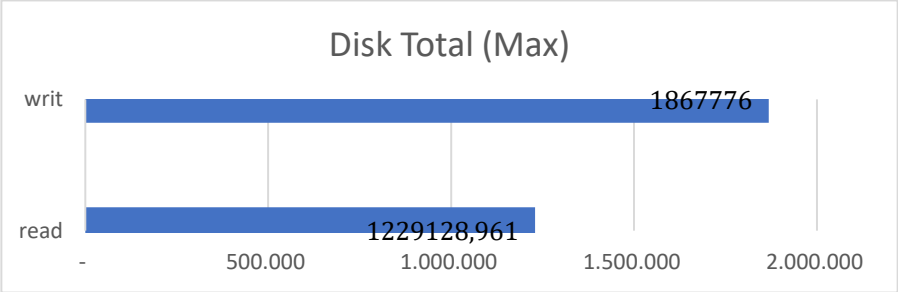
Gambar 4.6 Data Maksimum RAM (Memory Usage) pada Scenario Pertama



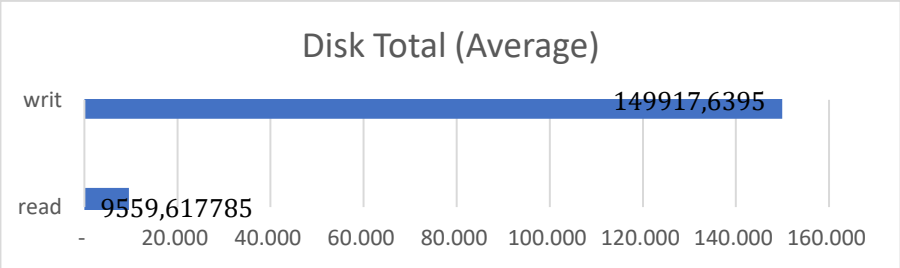
Gambar 4.7 Data Rata-Rata RAM (Memory Usage) pada Scenario Pertama



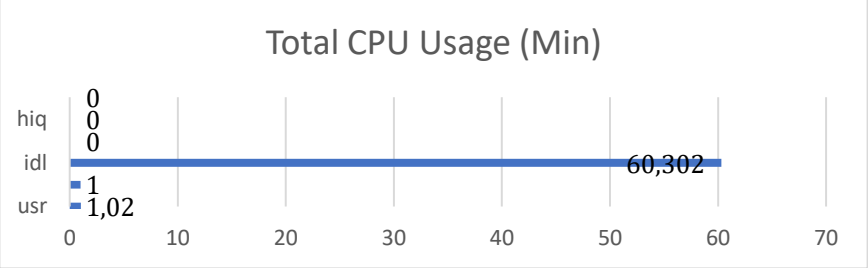
Gambar 4.8 Data Minimum Hardisk pada Scenario Pertama



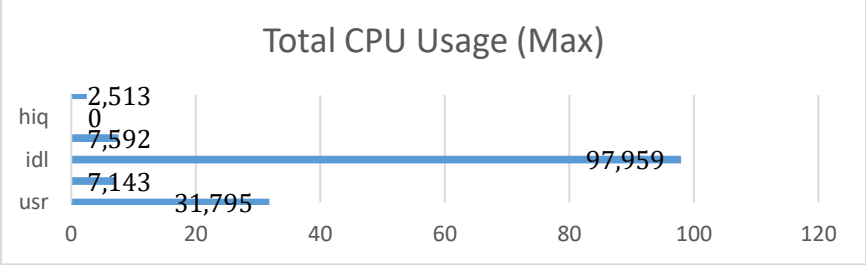
Gambar 4.9 Data Maksimum Hardisk pada Scenario Pertama



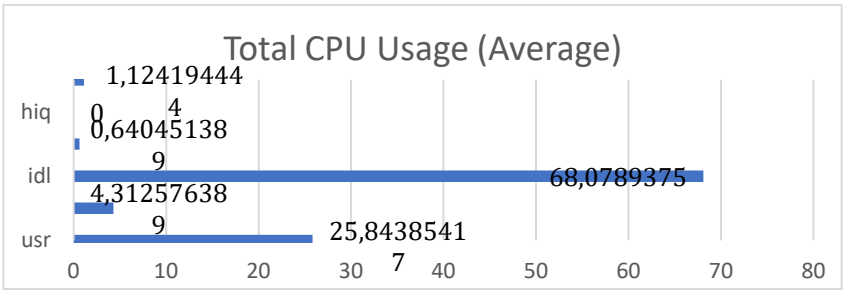
Gambar 4.10 Data Total Rata-Rata Hardisk pada Scenario Pertama



Gambar 4.11 Data Minimum CPU pada Scenario Pertama

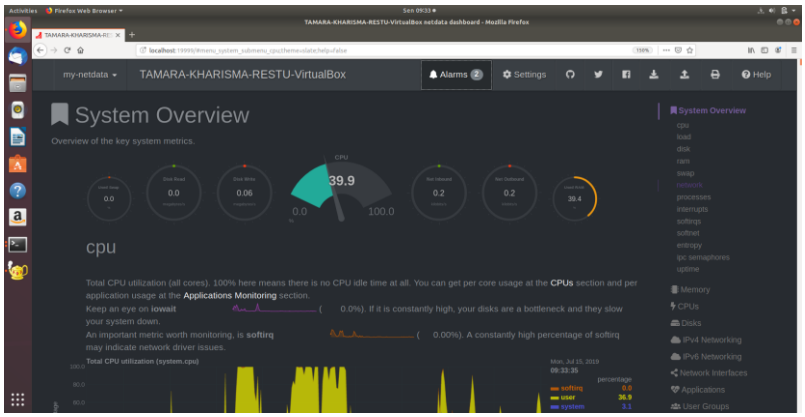


Gambar 4.12 Data Maksimum CPU pada Scenario Pertama

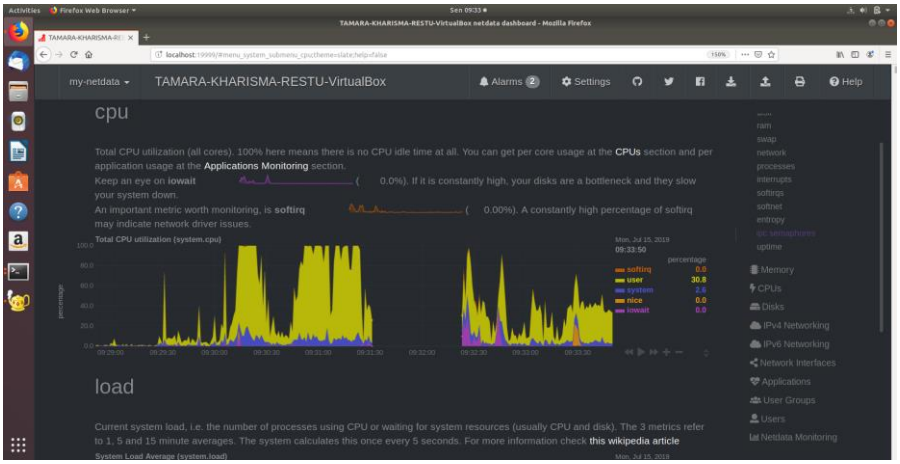


Gambar 4.13 Data Rata-Rata CPU pada Scenario Pertama

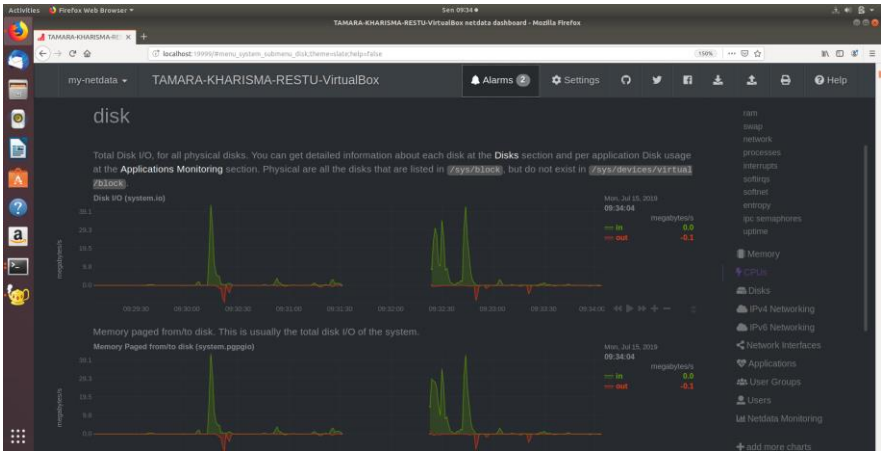
4.2.2 Pengujian pada Skenario 2



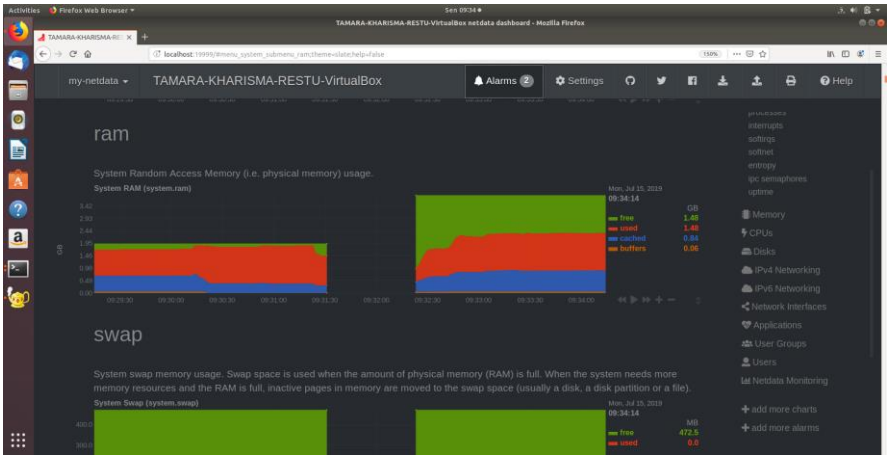
Gambar 4.14 Dashboard hasil pengujian skenario 2 menggunakan Netdata



Gambar 4.15 CPU Usage skenario 2 menggunakan Netdata

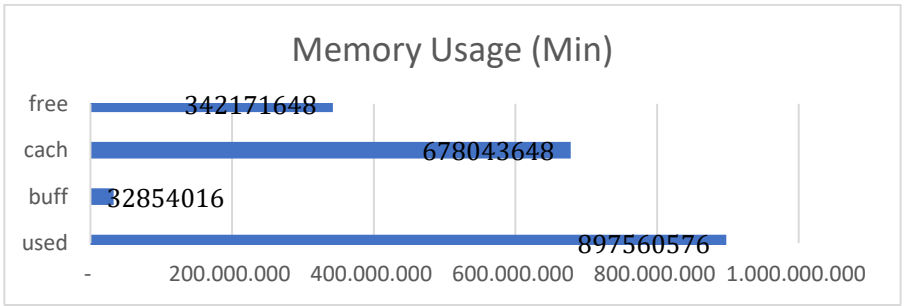


Gambar 4.16 Disk Usage pengujian 2 menggunakan Netdata

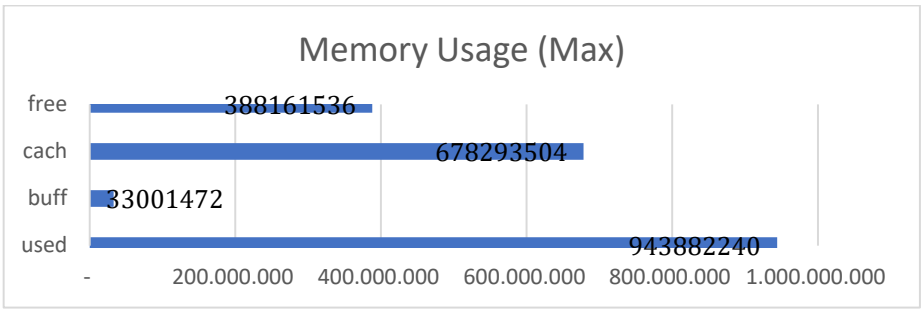


Gambar 4.17 RAM Usage pengujian 2 menggunakan Netdata

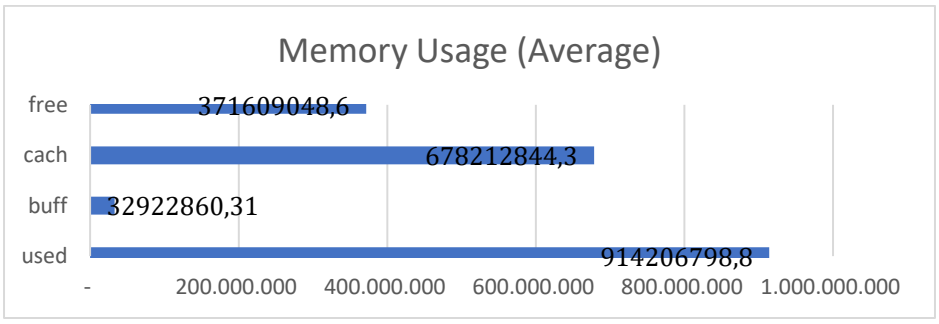
Pengujian skenario kedua ketika Cloud diserang oleh DoS (Denial of Service attacks) dengan durasi 10 menit, DoS merupakan jenis serangan yang menghabiskan resource pada sistem operasi komputer.



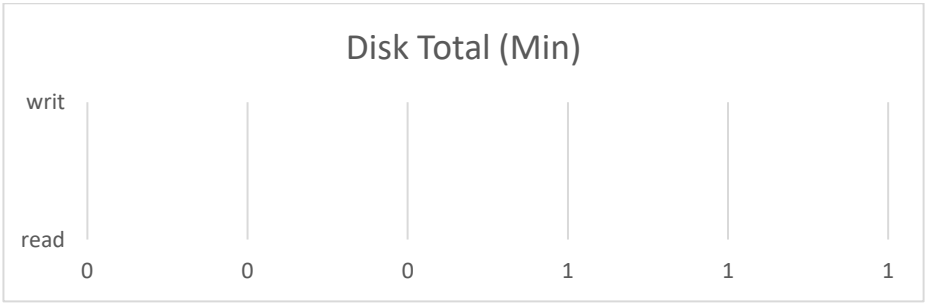
Gambar 4.18 Data Minimal RAM (Memory Usage) pada Scenario Kedua



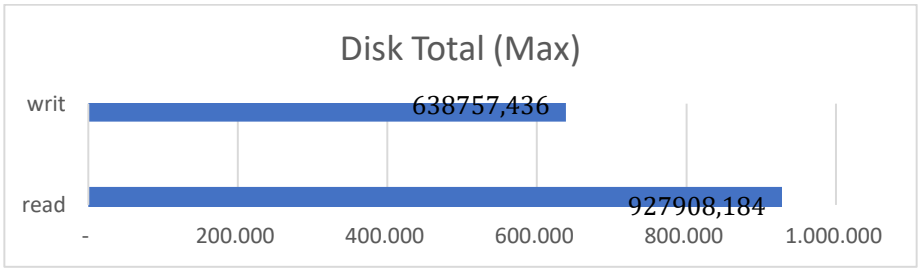
Gambar 4.19 Data Maksimum RAM (Memory Usage) pada Scenario Kedua



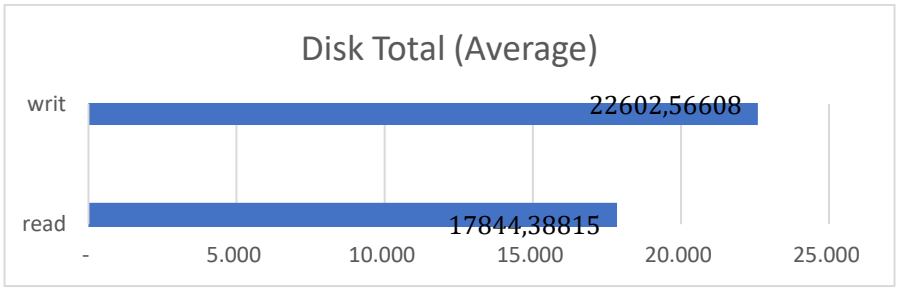
Gambar 4.20 Data Rata-Rata RAM (Memory Usage) pada Scenario Kedua



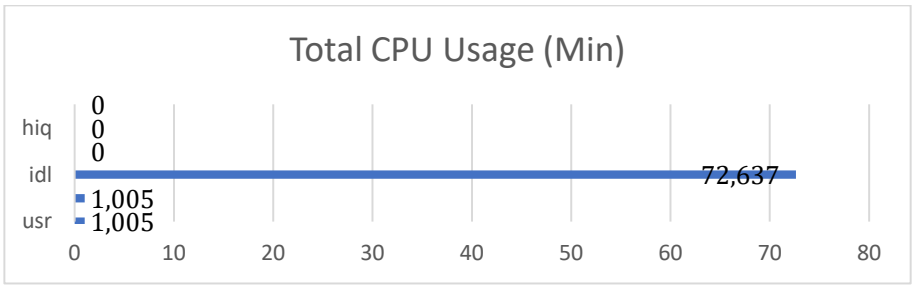
Gambar 4.21 Data Minimum Hardisk pada Scenario Kedua



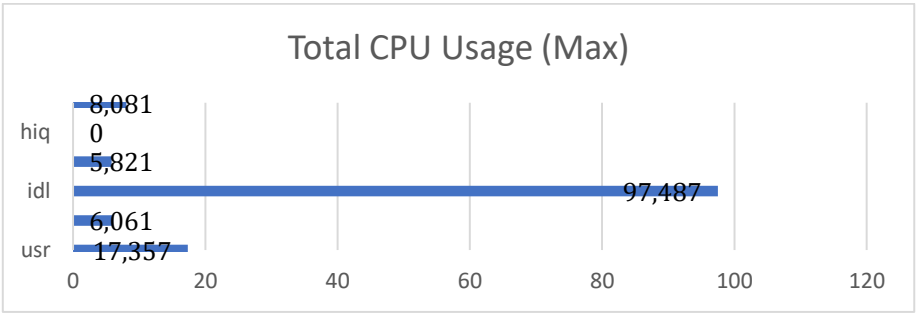
Gambar 4.22 Data Maksimum Hardisk pada Scenario Kedua



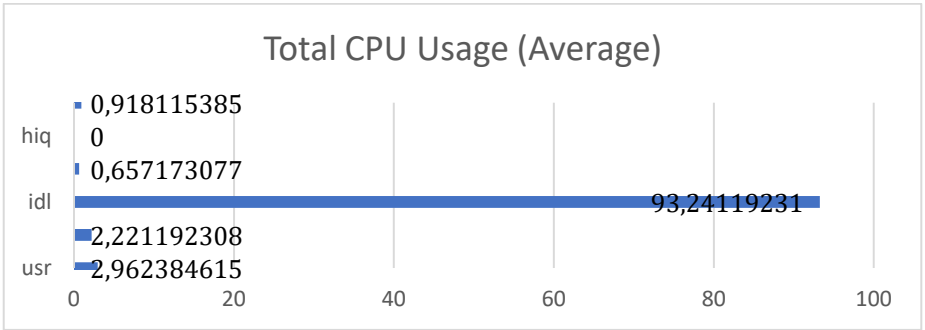
Gambar 4.23 Data Rata-Rata Hardisk pada Scenario Kedua



Gambar 4.24 Data Minimum CPU pada Scenario Kedua

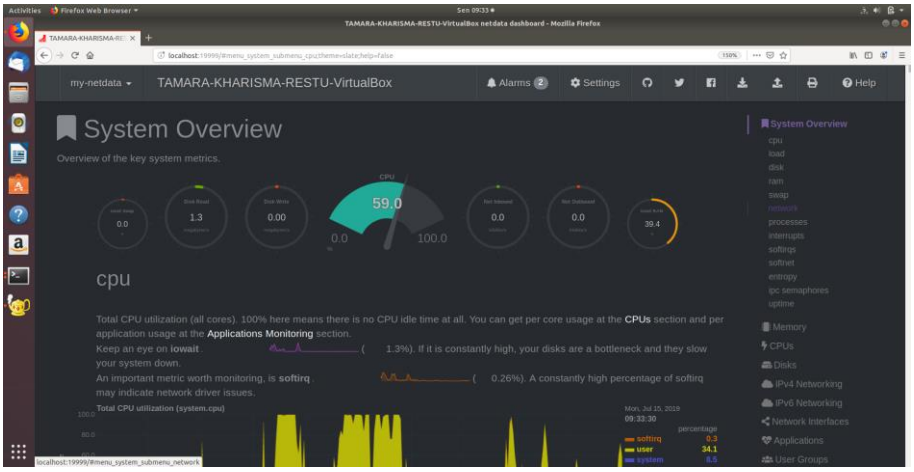


Gambar 4.25 Data Maksimum CPU pada Scenario Kedua

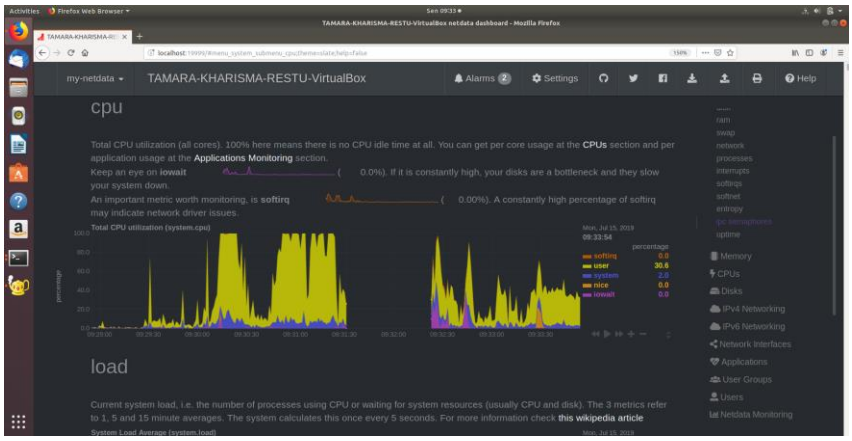


Gambar 4.26 Data Rata-Rata CPU pada Scenario Kedua

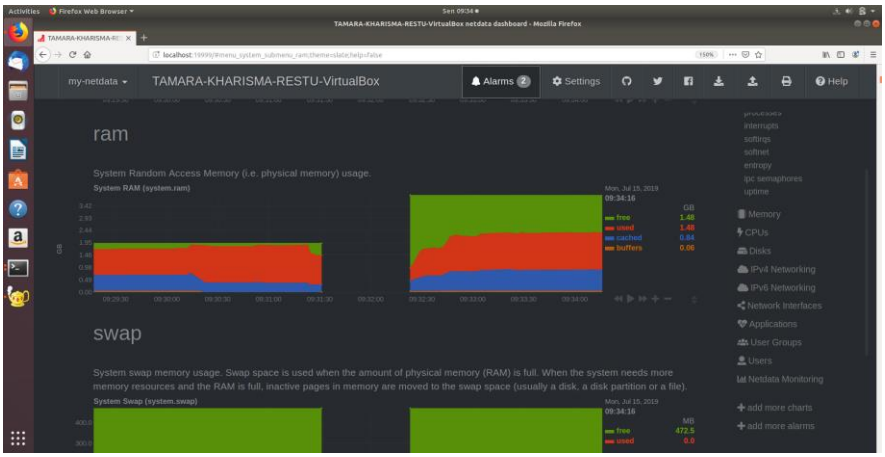
4.2.3 Hasil Pengujian Skenario 3



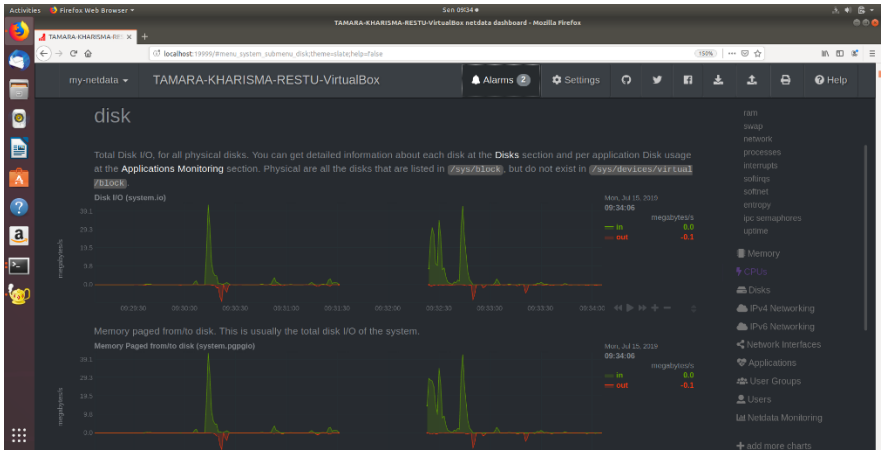
Gambar 4.27 Dashboard hasil pengujian 3 menggunakan netdata



Gambar 4.28 CPU usage hasil pengujian 3 menggunakan netdata

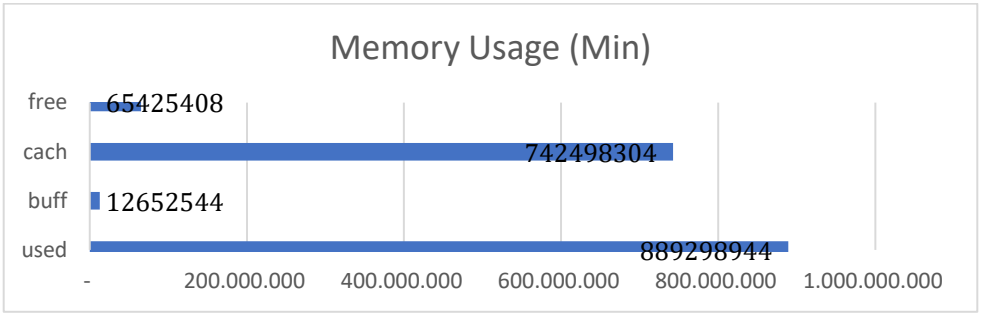


Gambar 4.29 RAM usage hasil pengujian 3 menggunakan netdata

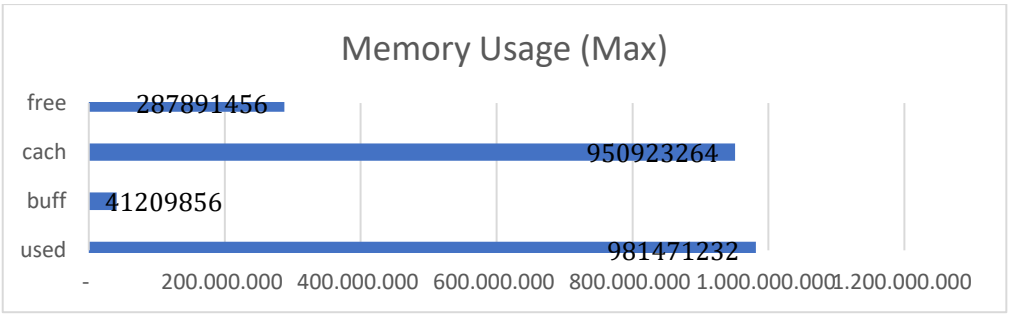


Gambar 4.30 Disk usage hasil pengujian 3 menggunakan netdata

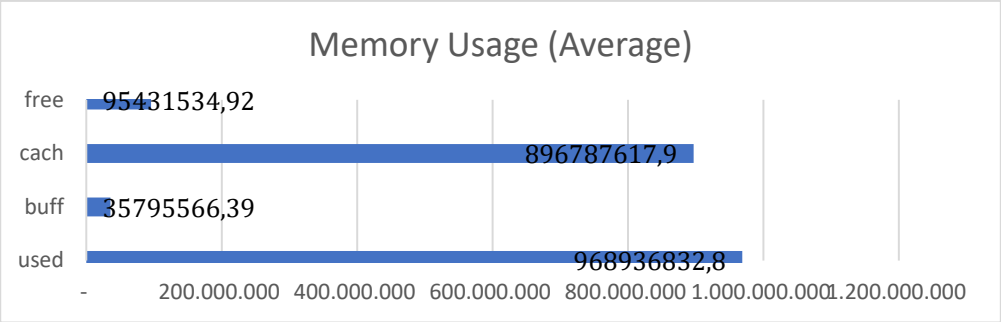
Pada pengujian ketiga dilakukan ketika user mengupload file 1 GB – 10 GB pada OwnCloud.



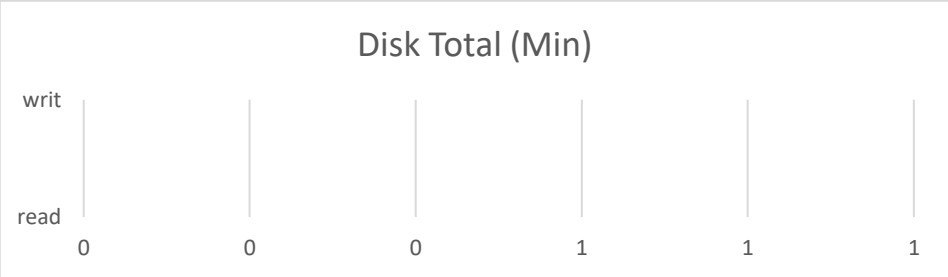
Gambar 4.31 Data Minimal RAM (Memory Usage) pada Scenario Ketiga



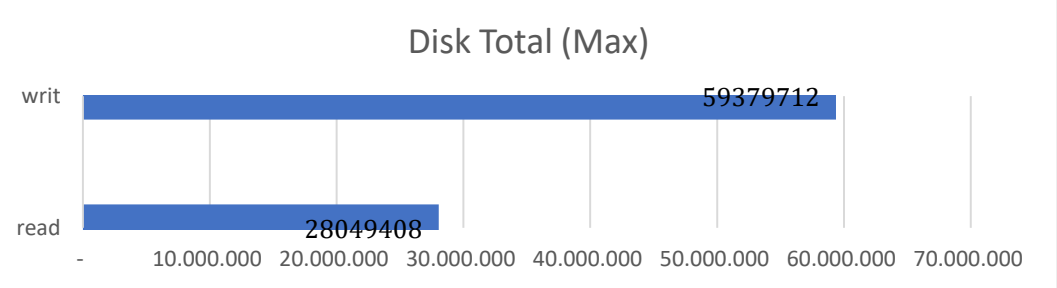
Gambar 4.32 Data Maksimum RAM (Memory Usage) pada Scenario Ketiga



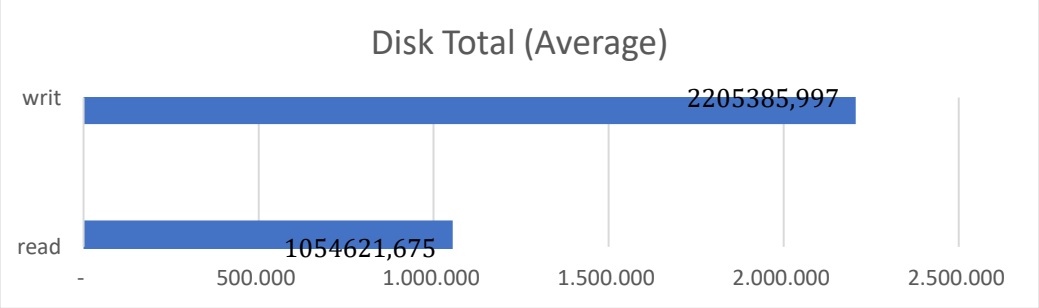
Gambar 4.33 Data Rata-Rata RAM (Memory Usage) pada Scenario Ketiga



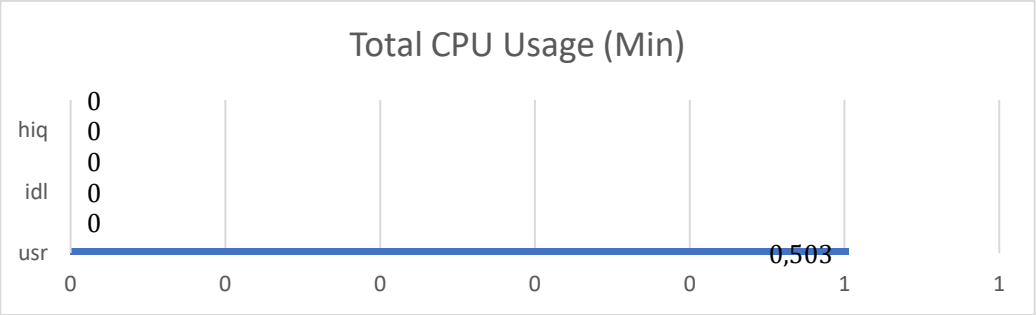
Gambar 4.34 Data Minimum Hardisk pada Scenario Ketiga



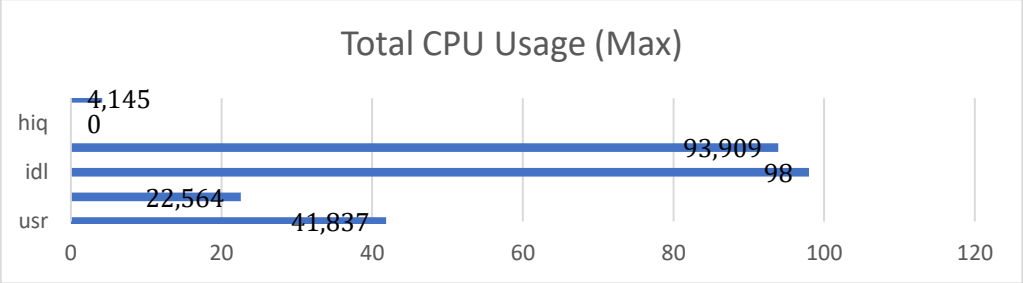
Gambar 4.35 Data Maksimum Hardisk pada Scenario Ketiga



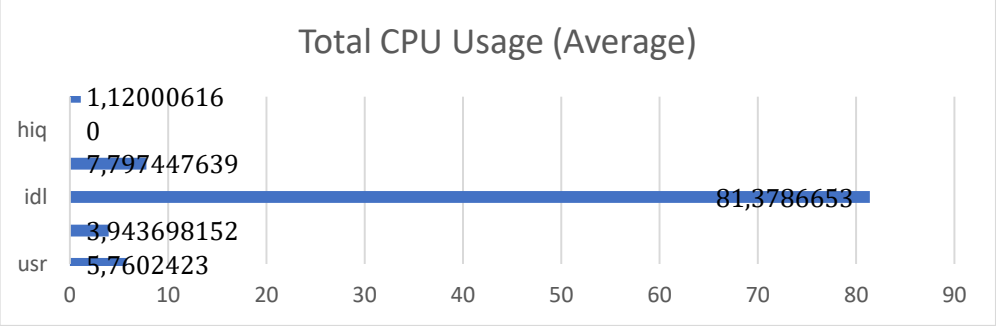
Gambar 4.36 Data Rata-Rata Hardisk pada Scenario Ketiga



Gambar 4.37 Data Minimum CPU pada Scenario Ketiga



Gambar 4.38 Data Maksimum CPU pada Scenario Ketiga



Gambar 4.39 Data Rata-Rata CPU pada Scenario Ketiga

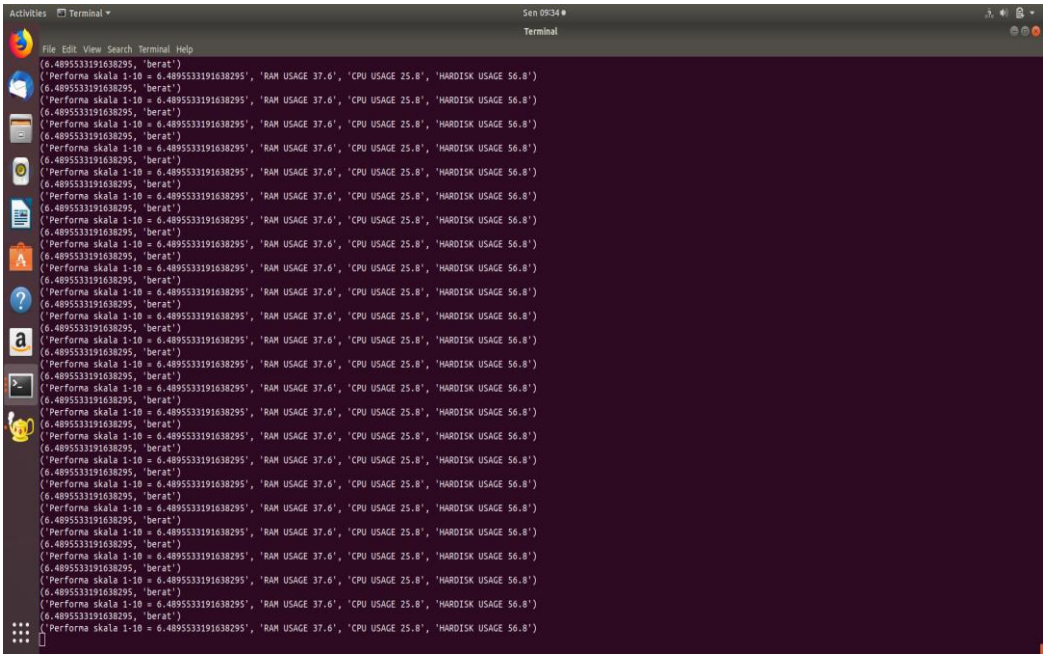
4.3 Perbandingan Pengujian Skenario Pertama, Skenario Kedua dan Skenario Ketiga

RAM	CPU	HARDISK
832 MB	32 %	233 MB/s
943 MB	17 %	80 MB/s
981 MB	42 %	7422 MB/s

Berdasarkan tabel diatas menunjukan hasil performa processor yang menujukan nilai maksimum dari 3 skenario tersebut. Dari hasil performa ini dapat digunakan sebagai pentunjuk untuk dapat menguji nilai scenario masing-masing dan sebagai pembuktian untuk dimasukkan ke logika fuzzy. Berikut adalah perhitungan manual dari perbandingan ketiga scenario diatas:

Skenario 1	Skenario 2	Skenario 3
µv RAM Ringan I =(600– 832 /600 – 0) = 0	µv RAM Ringan II = 0	µv RAM Ringan III = (1200 – 981) / (1200 – 600) = 0,36
µv RAM Normal I = (1200 – 832 / (1200 –600) = 0,63	µv RAM Normal II = (1200 – 943) / (1200 – 600) = 0,42	µv RAM Normal III = (981 – 600) / (1200 -600) = 0.63
µv RAM Berat I = (832 – 600) / (1200 – 600) =0,36	µv RAM Berat II = (943 – 600) / (1200 -600) = 0,57	µv CPU Ringan III = 0
µv CPU Ringan I = 0	µv CPU Ringan II = (0 – 17) / (0 – 30) = 0,56	µv CPU Normal III = (60 – 42) / (60 – 30) = 0,6
µv CPU Normal I = (60 – 32 / 60 – 30) = 0,93	µv CPU Normal II = (30-17) / (60-30) = 0,43	µv CPU Berat III = (42 -30) / (60 – 30) = 0,4

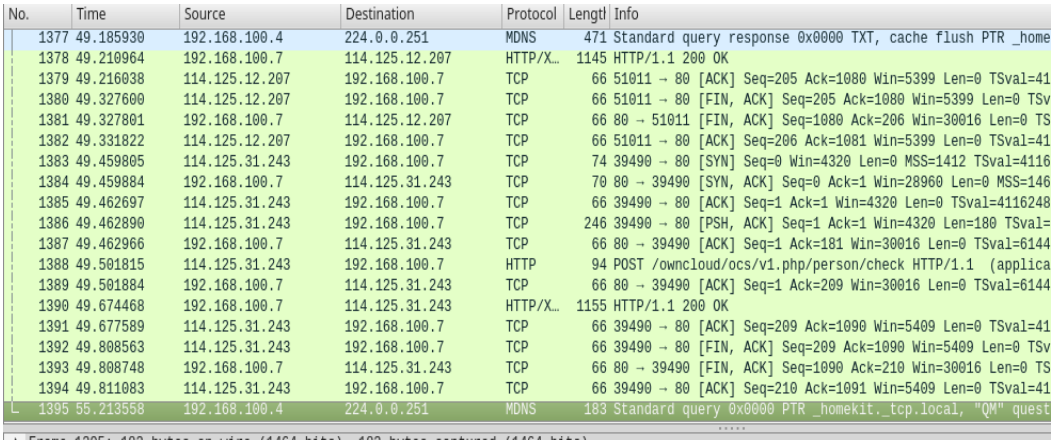
μv CPU Berat I = (32 – 30 / 60 – 30) = 0,06	μv CPU Berat II = 0	μv HD Ringan III = 0
μv HD Ringan I = (2500 – 233)/ (2500 – 0) = 0,90	μv HD Ringan II = (2500 – 80) / (2500 – 0) = 0,96	μv HD Normal III = 0
μv HD Normal I = (233 – 0) / (2500 – 0) = 0,09	μv HD Normal II = 0	μv HD CPU Normal III = 0
μv HD Berat I = 0	μv HD Berat II = 0	μv HD Berat III = 1



Gambar 4.40 Hasil program penentuan kategori performa cloud menggunakan logika fuzzy

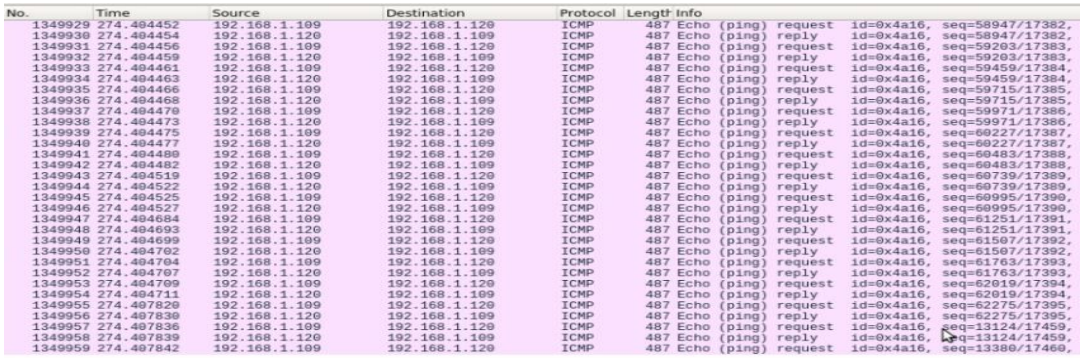
4.4 Hasil Data *Network Quality Of Service*

Setelah semua data pada skenario pertama kedua dan ketiga didapat, kemudian dilakukan ulang pada wireshark dengan cara peng-capturean, menggunakan protokol TCP. Dengan hasil sebagai berikut



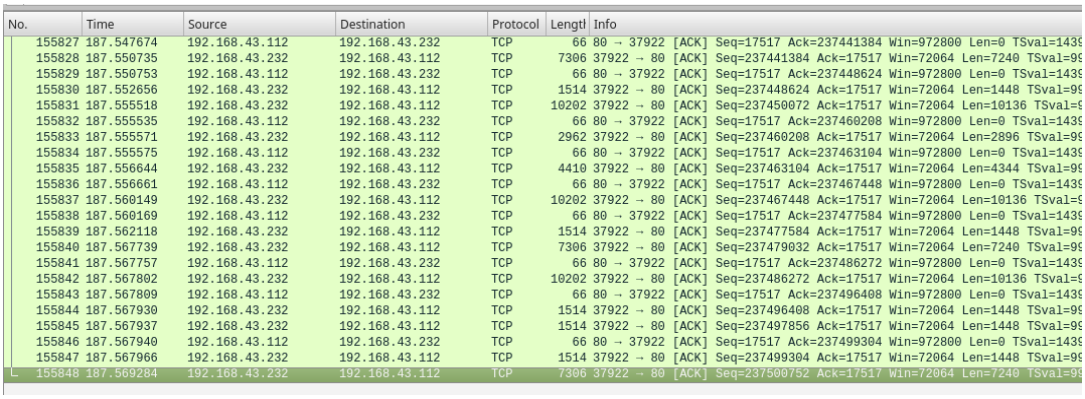
No.	Time	Source	Destination	Protocol	Lengtl	Info
1377	49.185930	192.168.100.4	224.0.0.251	MDNS	471	Standard query response 0x0000 TXT, cache flush PTR _home
1378	49.210964	192.168.100.7	114.125.12.207	HTTP/X…	1145	HTTP/1.1 200 OK
1379	49.216038	114.125.12.207	192.168.100.7	TCP	66	51011 → 80 [ACK] Seq=205 Ack=1080 Win=5399 Len=0 TSval=41
1380	49.327600	114.125.12.207	192.168.100.7	TCP	66	51011 → 80 [FIN, ACK] Seq=205 Ack=1080 Win=5399 Len=0 TSv
1381	49.327801	192.168.100.7	114.125.12.207	TCP	66	80 → 51011 [FIN, ACK] Seq=1080 Ack=206 Win=30016 Len=0 TS
1382	49.331822	114.125.12.207	192.168.100.7	TCP	66	51011 → 80 [ACK] Seq=206 Ack=1081 Win=5399 Len=0 TSval=41
1383	49.459805	114.125.31.243	192.168.100.7	TCP	74	39490 → 80 [SYN] Seq=0 Win=4320 Len=0 MSS=1412 TSval=4116
1384	49.459884	192.168.100.7	114.125.31.243	TCP	70	80 → 39490 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146
1385	49.462697	114.125.31.243	192.168.100.7	TCP	66	39490 → 80 [ACK] Seq=1 Ack=1 Win=4320 Len=0 TSval=4116248
1386	49.462890	114.125.31.243	192.168.100.7	TCP	246	39490 → 80 [PSH, ACK] Seq=1 Ack=1 Win=4320 Len=180 TSval=
1387	49.462966	192.168.100.7	114.125.31.243	TCP	66	80 → 39490 [ACK] Seq=1 Ack=181 Win=30016 Len=0 TSval=6144
1388	49.501815	114.125.31.243	192.168.100.7	HTTP	94	POST /owncloud/ocs/v1.php/person/check HTTP/1.1 (applica
1389	49.501884	192.168.100.7	114.125.31.243	TCP	66	80 → 39490 [ACK] Seq=1 Ack=209 Win=30016 Len=0 TSval=6144
1390	49.674468	192.168.100.7	114.125.31.243	HTTP/X…	1155	HTTP/1.1 200 OK
1391	49.677589	114.125.31.243	192.168.100.7	TCP	66	39490 → 80 [ACK] Seq=209 Ack=1090 Win=5409 Len=0 TSval=41
1392	49.808563	114.125.31.243	192.168.100.7	TCP	66	39490 → 80 [FIN, ACK] Seq=209 Ack=1090 Win=5409 Len=0 TSv
1393	49.808748	192.168.100.7	114.125.31.243	TCP	66	80 → 39490 [FIN, ACK] Seq=1090 Ack=210 Win=30016 Len=0 TS
1394	49.811083	114.125.31.243	192.168.100.7	TCP	66	39490 → 80 [ACK] Seq=210 Ack=1091 Win=5409 Len=0 TSval=41
1395	55.213558	192.168.100.4	224.0.0.251	MDNS	183	Standard query 0x0000 PTR _homekit._tcp.local, "QM" quest

Gambar 4.41 *Traffic Data QoS Brute Force* pada Wireshark



No.	Time	Source	Destination	Protocol	Lengtl	Info
1349929	274.404452	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=58947/17382,
1349930	274.404454	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=58947/17382,
1349931	274.404456	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=59203/17383,
1349932	274.404459	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=59203/17383,
1349933	274.404461	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=59459/17384,
1349934	274.404463	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=59459/17384,
1349935	274.404466	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=59715/17385,
1349936	274.404468	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=59715/17385,
1349937	274.404470	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=59971/17386,
1349938	274.404473	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=59971/17386,
1349939	274.404475	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=60227/17387,
1349940	274.404477	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=60227/17387,
1349941	274.404480	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=60483/17388,
1349942	274.404482	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=60483/17388,
1349943	274.404519	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=60739/17389,
1349944	274.404522	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=60739/17389,
1349945	274.404525	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=60995/17390,
1349946	274.404527	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=60995/17390,
1349947	274.404684	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=61251/17391,
1349948	274.404693	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=61251/17391,
1349949	274.404699	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=61507/17392,
1349950	274.404702	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=61507/17392,
1349951	274.404704	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=61763/17393,
1349952	274.404707	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=61763/17393,
1349953	274.404709	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=62019/17394,
1349954	274.404711	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=62019/17394,
1349955	274.407820	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=62275/17395,
1349956	274.407830	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=62275/17395,
1349957	274.407836	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=13124/17459,
1349958	274.407839	192.168.1.120	192.168.1.109	ICMP	487	Echo (ping) reply id=0x4a16, seq=13124/17459,
1349959	274.407842	192.168.1.109	192.168.1.120	ICMP	487	Echo (ping) request id=0x4a16, seq=13380/17460,

Gambar 4.42 *Traffic Data QoS Denial of Service* pada Wireshark



No.	Time	Source	Destination	Protocol	Lengtl	Info
155827	187.547674	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237441384 Win=972800 Len=0 TSval=1439
155828	187.550735	192.168.43.232	192.168.43.112	TCP	7306	37922 → 80 [ACK] Seq=237441384 Ack=17517 Win=72064 Len=7240 TSval=99
155829	187.550753	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237448624 Win=972800 Len=0 TSval=1439
155830	187.552656	192.168.43.232	192.168.43.112	TCP	1514	37922 → 80 [ACK] Seq=237448624 Ack=17517 Win=72064 Len=1448 TSval=99
155831	187.555518	192.168.43.232	192.168.43.112	TCP	10202	37922 → 80 [ACK] Seq=237450072 Ack=17517 Win=72064 Len=10136 TSval=9
155832	187.555535	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237460208 Win=972800 Len=0 TSval=1439
155833	187.555571	192.168.43.232	192.168.43.112	TCP	2962	37922 → 80 [ACK] Seq=237460208 Ack=17517 Win=72064 Len=2896 TSval=99
155834	187.555575	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237463104 Win=972800 Len=0 TSval=1439
155835	187.556644	192.168.43.232	192.168.43.112	TCP	4410	37922 → 80 [ACK] Seq=237463104 Ack=17517 Win=72064 Len=4344 TSval=99
155836	187.556661	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237467448 Win=972800 Len=0 TSval=1439
155837	187.560149	192.168.43.232	192.168.43.112	TCP	10202	37922 → 80 [ACK] Seq=237467448 Ack=17517 Win=72064 Len=10136 TSval=9
155838	187.560169	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237477584 Win=972800 Len=0 TSval=1439
155839	187.562118	192.168.43.232	192.168.43.112	TCP	1514	37922 → 80 [ACK] Seq=237477584 Ack=17517 Win=72064 Len=1448 TSval=99
155840	187.567739	192.168.43.232	192.168.43.112	TCP	7306	37922 → 80 [ACK] Seq=237479032 Ack=17517 Win=72064 Len=7240 TSval=99
155841	187.567757	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237486272 Win=972800 Len=0 TSval=1439
155842	187.567802	192.168.43.232	192.168.43.112	TCP	10202	37922 → 80 [ACK] Seq=237486272 Ack=17517 Win=72064 Len=10136 TSval=9
155843	187.567809	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237496408 Win=972800 Len=0 TSval=1439
155844	187.567930	192.168.43.232	192.168.43.112	TCP	1514	37922 → 80 [ACK] Seq=237496408 Ack=17517 Win=72064 Len=1448 TSval=99
155845	187.567937	192.168.43.232	192.168.43.112	TCP	1514	37922 → 80 [ACK] Seq=237497856 Ack=17517 Win=72064 Len=1448 TSval=99
155846	187.567940	192.168.43.112	192.168.43.232	TCP	66	80 → 37922 [ACK] Seq=17517 Ack=237499304 Win=972800 Len=0 TSval=1439
155847	187.567966	192.168.43.232	192.168.43.112	TCP	1514	37922 → 80 [ACK] Seq=237499304 Ack=17517 Win=72064 Len=1448 TSval=99
155848	187.569284	192.168.43.232	192.168.43.112	TCP	7306	37922 → 80 [ACK] Seq=237500752 Ack=17517 Win=72064 Len=7240 TSval=99

Gambar 4.43 *Traffic Data QoS* pada saat *User Upload* file pada Wireshark

4.4 Perhitungan Manual *Quality of Service* pada Hasil Capture Wireshark

Tabel 10 Tabel hasil perhitungan *Quality of Service*

No.	Quality Of Service		
	Throughput	**Delay**	**Packet Loss**
Skenario 1	0,0047272727	0,0394265233	0%
Skenario 2	2,4781021898	0,0002060214	0%
Skenario 3	2,5668449198	0,0011998871	0%

- *Quality of Service* pada Skenario 1

$$Throughput = \frac{\text{ukuran data yang diterima}}{\text{waktu pengiriman data}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\frac{260}{55} = 4{,}72727273 : 1000$$

$$= 0{,}0047272727$$

$$\text{Rata-rata } Delay = \frac{\text{total waktu pengiriman paket}}{\text{total paket}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$\frac{55}{1395} = 0{,}03942652$$

$$Packet\ Lost = \frac{\sum packet\ delivered - packet\ received}{\sum Packet\ delivered} \text{ x } 100\% \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$\frac{1395-1395}{1395} x100 = 0\ \%$$

- *Quality of Service* pada Skenario 2

$$Throughput = \frac{\text{ukuran data yang diterima}}{\text{waktu pengiriman data}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\frac{679}{274} = 2{,}4781021898$$

$$\text{Rata-rata } Delay = \frac{\text{total waktu pengiriman paket}}{\text{total paket}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$\frac{274}{1329959} = 0{,}0002060214$$

$$Packet\ Lost = \frac{\sum packet\ delivered - packet\ received}{\sum Packet\ delivered} \text{ x } 100\% \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$\frac{1349959-1349959}{1349959} x100 = 0\ \%$$

- *Quality of Service* pada Skenario 3

$$Throughput = \frac{\text{ukuran data yang diterima}}{\text{waktu pengiriman data}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\frac{480}{187} = 2{,}5668449198$$

$$\text{Rata-rata } Delay = \frac{\text{total waktu pengiriman paket}}{\text{total paket}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$\frac{187}{155848} = 0{,}0011998871$$

$$Packet\ Lost\ = \frac{\sum packet\ delivered - packet\ received}{\sum Packet\ delivered} \text{ x } 100\% \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$\frac{155048-155048}{155048} x100 = 0\ \%$$

4.5 Grafik Hasil dari Pengujian Skenario

Gambar 4.44 Grafik QoS pada pengujian scenario pertama

Gambar 4.45 Grafik QoS pada pengujian scenario kedua

Gambar 4.46 Grafik QoS pada pengujian scenario ketiga


3
2,5
2
1,5
1
0,5
0
Throughput (Mbps)
Delay (s)
Packet Loss (%)