Title: With the help of disk monitoring identify the read and write process having length>5.

Objective:

The objective of this project is to utilize disk monitoring software to identify read and write processes that have a length greater than 5. By analyzing the data collected through disk monitoring, we aim to identify processes with significant read and write operations on the disk.

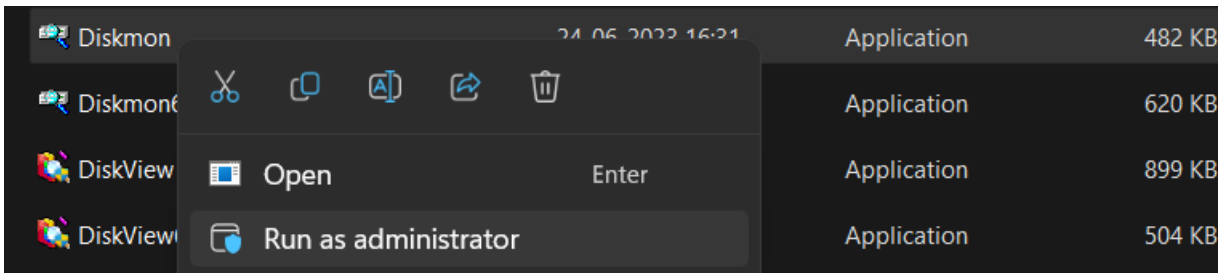
Requirements:

Sysinternal suite
Diskmon.exe

Procedure/Experiment Steps:

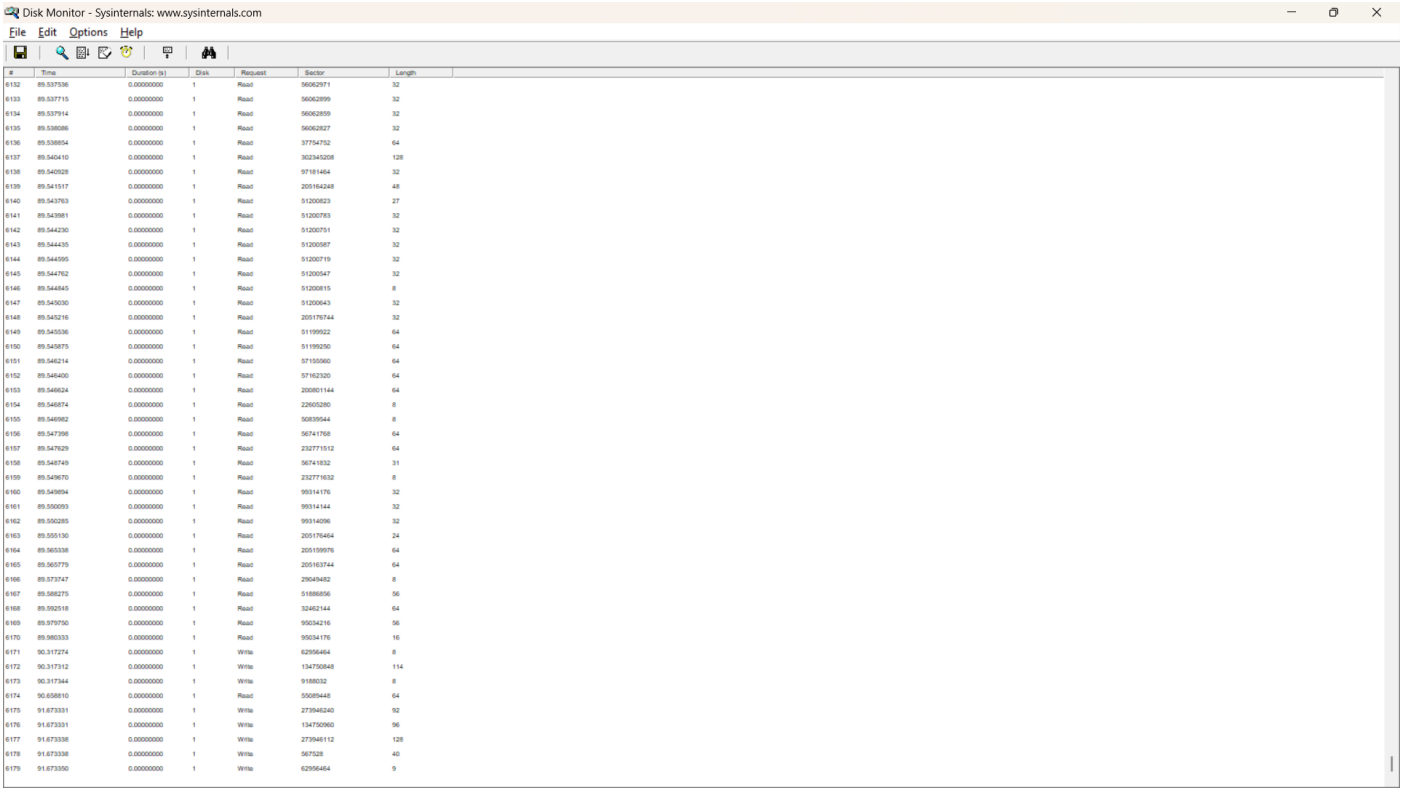
1. Download Disk Monitor:
    a. Open a web browser.
    b. Visit the official Microsoft website.
    c. Search for "Disk Monitor" or Sysinternal suite and navigate to the official download page.
    d. Download the appropriate version that compatible with your Windows operating system.
    e. Save the downloaded file.

2. Launch Disk Monitor:
    a. Navigate to the installation location of Disk Monitor.
    b. Double-click on the "Diskmon.exe" file to launch Disk Monitor.

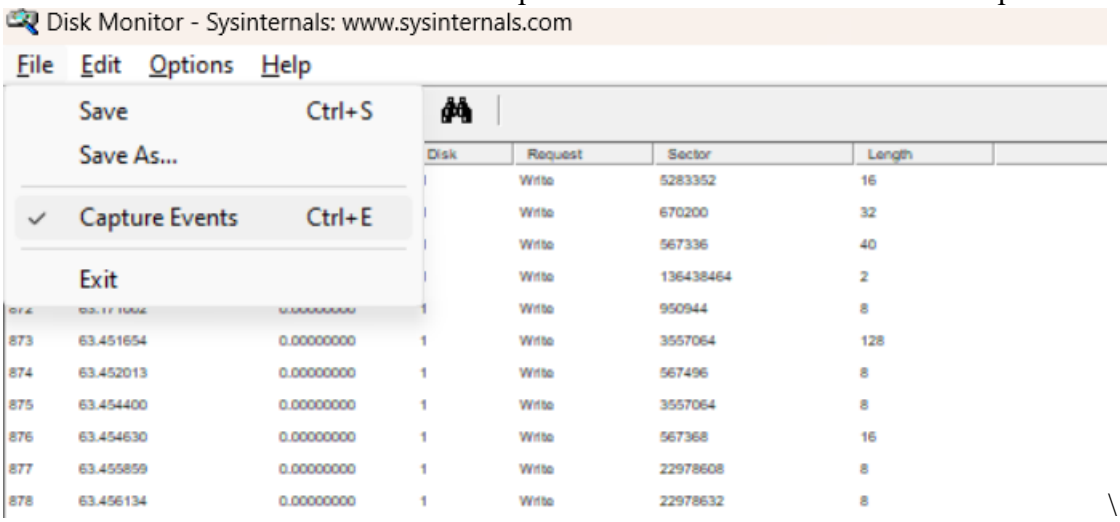


    c. It will ask for the installation for the first time only.

3. Explore Disk Monitor Interface:
    a. The Disk Monitor interface



b. It automatic start capture the logs and data
c. Go to file and click on capture Event or Press CTRL + E to stop



d. As we can see here all event in Read and write mode

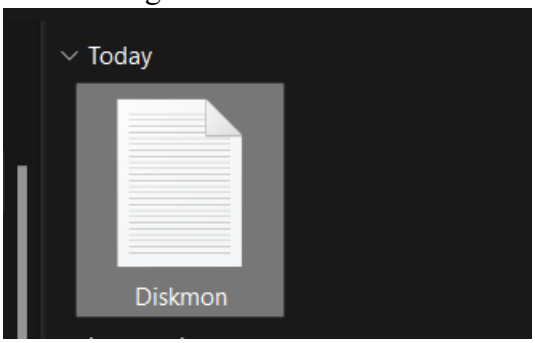
Disk Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

#	Time	Durati...	Disk	Request	Sector	Length
182	16.836802	0.00000...	1	Write	53680296	7
183	18.196709	0.00000...	1	Write	53680296	11
184	19.552763	0.00000...	1	Write	53680472	2
185	19.552765	0.00000...	1	Write	567464	16
186	19.553026	0.00000...	1	Write	42435088	2
187	19.553061	0.00000...	1	Write	42233960	5
188	19.809072	0.00000...	1	Write	567344	16
189	19.811515	0.00000...	1	Write	51168072	8
190	20.922979	0.00000...	1	Write	53680304	4
191	21.389277	0.00000...	1	Read	3015256	24
192	22.286477	0.00000...	1	Write	62956512	5
193	22.286578	0.00000...	1	Write	53680472	4
194	23.653686	0.00000...	1	Write	5283304	48
195	23.653686	0.00000...	1	Write	567480	16
196	23.653840	0.00000...	1	Write	42233960	5
197	23.653878	0.00000...	1	Write	42435088	2
198	24.821141	0.00000...	1	Write	669144	144
199	24.821256	0.00000...	1	Write	567336	8
200	24.822278	0.00000...	1	Write	567328	8
201	25.006542	0.00000...	1	Write	53680472	6
202	25.006557	0.00000...	1	Write	68004696	2
203	25.006565	0.00000...	1	Write	65374656	67
204	25.682584	0.00000...	1	Read	203876802	40
205	25.683704	0.00000...	1	Read	209896563	32
206	26.373570	0.00000...	1	Write	53680304	6
207	27.733488	0.00000...	1	Write	567464	16
208	27.734502	0.00000...	1	Write	13557200	8
209	27.734512	0.00000...	1	Write	50775192	16
210	27.734656	0.00000...	1	Write	51083096	8
211	27.734736	0.00000...	1	Write	50775216	8
212	27.734762	0.00000...	1	Write	2452520	8
213	27.734781	0.00000...	1	Write	142430880	11
214	27.734816	0.00000...	1	Write	51083504	8
215	27.734835	0.00000...	1	Write	2452488	8
216	27.734848	0.00000...	1	Write	50775344	8
217	27.734909	0.00000...	1	Write	142430872	8
218	27.734941	0.00000...	1	Write	51083680	16
219	27.734963	0.00000...	1	Write	50775392	8
220	27.734979	0.00000...	1	Write	103287976	8
221	27.734989	0.00000...	1	Write	10886568	8
222	27.735011	0.00000...	1	Write	51084256	16
223	27.735027	0.00000...	1	Write	50775440	16
224	27.735046	0.00000...	1	Write	1084208	8
225	27.735059	0.00000...	1	Write	7673024	8
226	27.735107	0.00000...	1	Write	50775520	8
227	27.735114	0.00000...	1	Write	51084288	32
228	27.735114	0.00000...	1	Write	1645528	8
229	27.735130	0.00000...	1	Write	7673104	8

e. We can see Time, Duration, Disk, Request, Sector, Length

f. Save the log file



g. Locket the file copy the data

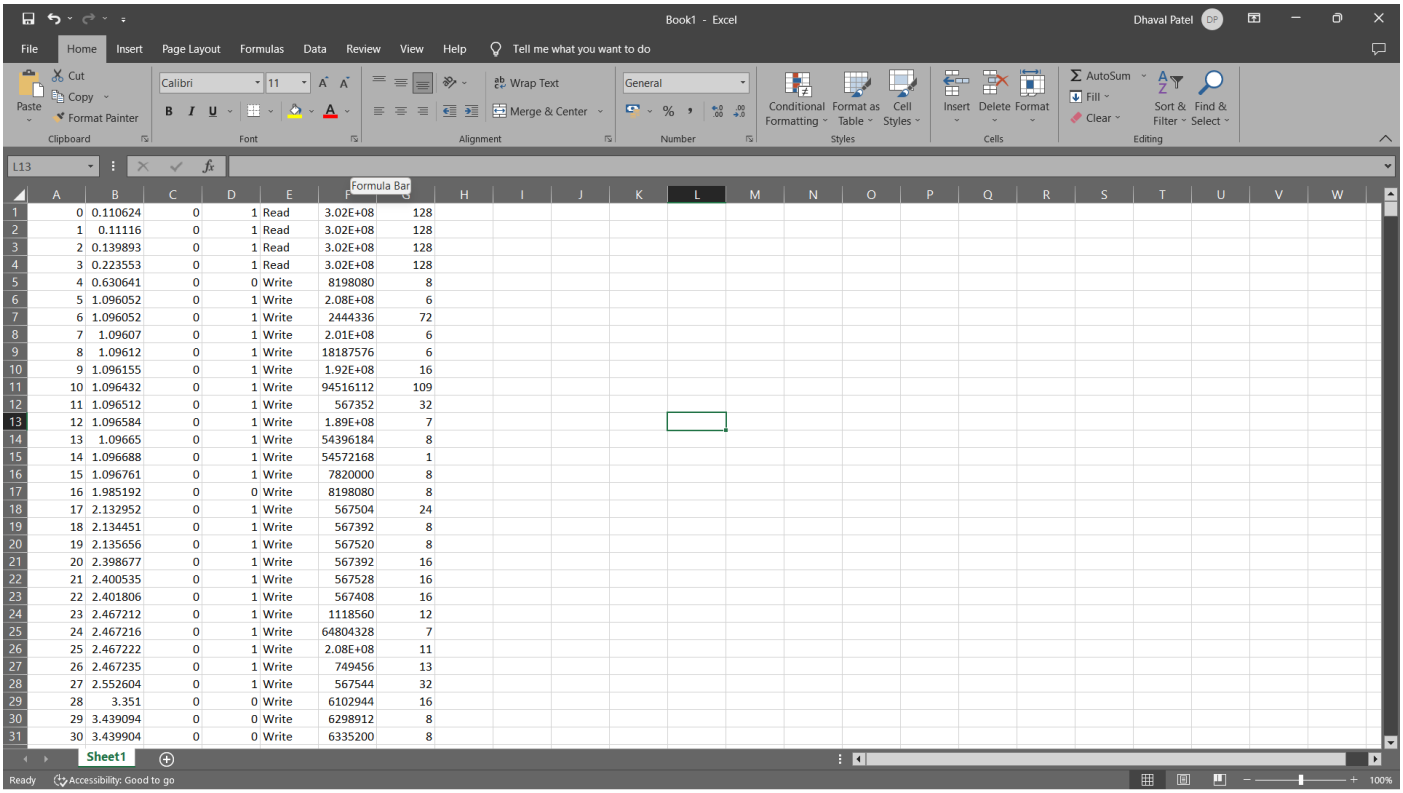
Diskmon

File Edit View

0	0.110624	0.00000000	1	Read	302102536	128
1	0.111160	0.00000000	1	Read	302102272	128
2	0.139893	0.00000000	1	Read	302359464	128
3	0.223553	0.00000000	1	Read	302479400	128
4	0.630641	0.00000000	0	Write	8198080 8	
5	1.096052	0.00000000	1	Write	207524912	6
6	1.096052	0.00000000	1	Write	2444336 72	
7	1.096070	0.00000000	1	Write	200589176	6
8	1.096120	0.00000000	1	Write	18187576	6
9	1.096155	0.00000000	1	Write	192041616	16
10	1.096432	0.00000000	1	Write	94516112	109
11	1.096512	0.00000000	1	Write	567352 32	
12	1.096584	0.00000000	1	Write	188658456	7
13	1.096650	0.00000000	1	Write	54396184	8
14	1.096688	0.00000000	1	Write	54572168	1
15	1.096761	0.00000000	1	Write	7820000 8	
16	1.985192	0.00000000	0	Write	8198080 8	
17	2.132952	0.00000000	1	Write	567504 24	
18	2.134451	0.00000000	1	Write	567392 8	
19	2.135656	0.00000000	1	Write	567520 8	
20	2.398677	0.00000000	1	Write	567392 16	
21	2.400535	0.00000000	1	Write	567528 16	
22	2.401806	0.00000000	1	Write	567408 16	
23	2.467212	0.00000000	1	Write	1118560 12	
24	2.467216	0.00000000	1	Write	64804328	7
25	2.467222	0.00000000	1	Write	207524912	11
26	2.467235	0.00000000	1	Write	749456 13	
27	2.552604	0.00000000	1	Write	567544 32	
28	3.351000	0.00000000	0	Write	6102944 16	
29	3.439094	0.00000000	0	Write	6298912 8	
30	3.439904	0.00000000	0	Write	6335200 8	
31	3.835428	0.00000000	1	Write	68006144	6
32	3.835428	0.00000000	1	Write	188658456	7
33	3.835448	0.00000000	1	Write	2465776 16	
34	3.835456	0.00000000	1	Write	567440 16	
35	3.835662	0.00000000	1	Write	4244504 17	
36	4.206428	0.00000000	1	Write	142959648	32
37	4.206750	0.00000000	1	Write	567576 16	
38	4.209224	0.00000000	1	Write	142959648	8
39	4.209417	0.00000000	1	Write	567456 8	
40	4.210722	0.00000000	1	Write	22978608	8
41	4.210904	0.00000000	1	Write	277363880	8
42	4.211018	0.00000000	1	Write	23694624	8

Ln 1, Col 1 100% Windows (CRLF) UTF-8

h. open in excel



	A	B	C	D	E	F	G
1	0	0.110624	0	1	Read	3.02E+08	128
2	1	0.11116	0	1	Read	3.02E+08	128
3	2	0.139893	0	1	Read	3.02E+08	128
4	3	0.223553	0	1	Read	3.02E+08	128
5	4	0.630641	0	0	Write	8198080	8
6	5	1.096052	0	1	Write	2.08E+08	6
7	6	1.096052	0	1	Write	2444336	72
8	7	1.09607	0	1	Write	2.01E+08	6
9	8	1.09612	0	1	Write	18187576	6
10	9	1.096155	0	1	Write	1.92E+08	16
11	10	1.096432	0	1	Write	94516112	109
12	11	1.096512	0	1	Write	567352	32
13	12	1.096584	0	1	Write	1.89E+08	7
14	13	1.09665	0	1	Write	54396184	8
15	14	1.096688	0	1	Write	54572168	1
16	15	1.096761	0	1	Write	7820000	8
17	16	1.985192	0	0	Write	8198080	8
18	17	2.132952	0	1	Write	567504	24
19	18	2.134451	0	1	Write	567392	8
20	19	2.135656	0	1	Write	567520	8
21	20	2.398677	0	1	Write	567392	16
22	21	2.400535	0	1	Write	567528	16
23	22	2.401806	0	1	Write	567408	16
24	23	2.467212	0	1	Write	1118560	12
25	24	2.467216	0	1	Write	64804328	7
26	25	2.467222	0	1	Write	2.08E+08	11
27	26	2.467235	0	1	Write	749456	13
28	27	2.552604	0	1	Write	567544	32
29	28	3.351	0	0	Write	6102944	16
30	29	3.439094	0	0	Write	6298912	8
31	30	3.439904	0	0	Write	6335200	8

i. Analyze the result

Result:

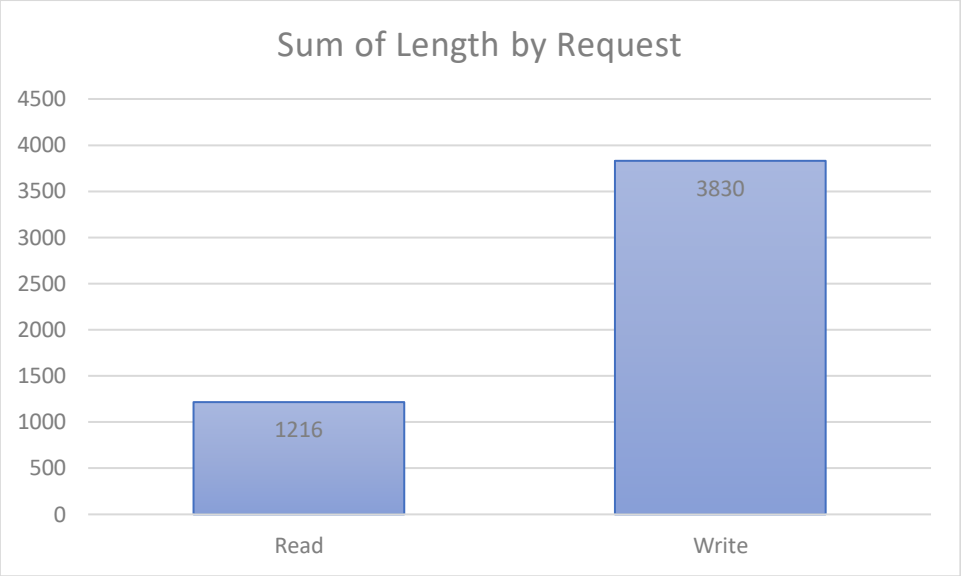
- Read and Write Process with length >5.

#	Time	Duration	Disk	Request	Sector	Length
85	24.997138	0	1	Write	64804568	7
1	8.642404	0	1	Write	101392440	8
17	10.544672	0	1	Write	567392	8
20	10.545294	0	1	Write	47474184	8
21	10.545326	0	1	Write	47474192	8
24	10.546761	0	1	Write	47474184	8
25	10.546978	0	1	Write	47474192	8
32	10.5489	0	1	Write	567520	8
33	10.549217	0	1	Write	567400	8
35	10.551006	0	1	Write	567528	8
37	10.551166	0	1	Write	567400	8
39	10.551573	0	1	Write	567528	8
40	10.551721	0	1	Write	80871376	8
41	10.551818	0	1	Write	80871384	8
42	10.552262	0	1	Write	567400	8
43	10.552373	0	1	Write	24583232	8
44	10.552491	0	1	Write	24583240	8
45	10.552678	0	1	Write	567528	8
47	10.55316	0	1	Write	24583232	8
48	10.553281	0	1	Write	24583240	8
49	10.553434	0	1	Write	567536	8
50	10.553618	0	1	Write	47474192	8
51	10.55377	0	1	Write	47474200	8
52	10.553827	0	1	Write	47474208	8
53	10.554253	0	1	Write	567408	8

54	10.554363	0	1	Write	24583232	8
55	10.554487	0	1	Write	24583240	8
56	10.554652	0	1	Write	567536	8
59	10.566633	0	1	Write	567544	8
70	18.891933	0	1	Write	567344	8
75	19.5396	0	1	Write	50971336	8
76	19.539738	0	1	Write	50971576	8
78	19.53999	0	1	Write	50971656	8
79	19.540114	0	1	Write	50974832	8
87	27.718742	0	1	Write	64804568	8
96	34.193014	0	1	Write	567424	8
104	35.889885	0	1	Write	567464	8
105	35.8928	0	1	Write	50984512	8
106	35.892826	0	1	Write	18045224	8
108	35.892883	0	1	Write	65642656	8
109	35.892938	0	1	Write	8168040	8
110	35.893005	0	1	Write	148436648	8
111	35.893094	0	1	Write	51008976	8
112	35.893142	0	1	Write	8167600	8
113	35.893181	0	1	Write	65655000	8
114	35.893187	0	1	Write	50775480	8
115	35.893206	0	1	Write	51009288	8
116	35.893242	0	1	Write	27761576	8
117	35.893254	0	1	Write	17904984	8
118	35.893274	0	1	Write	50775568	8
120	35.893322	0	1	Write	29124384	8
121	35.893325	0	1	Write	27761712	8
122	35.893357	0	1	Write	51009440	8
124	35.893379	0	1	Write	27761792	8
126	35.893414	0	1	Write	51009488	8
127	35.893462	0	1	Write	50775808	8
128	35.893488	0	1	Write	27761344	8
129	35.893507	0	1	Write	51009896	8
131	35.893536	0	1	Write	50776736	8
132	35.893568	0	1	Write	27761488	8
133	35.893658	0	1	Write	50776784	8
136	35.893722	0	1	Write	3683248	8
137	35.893734	0	1	Write	50776960	8
138	35.89377	0	1	Write	29124032	8
139	35.893789	0	1	Write	51010448	8
140	35.893805	0	1	Write	3683272	8
141	35.893821	0	1	Write	50777424	8
143	35.893853	0	1	Write	51074312	8
144	35.893872	0	1	Write	1814872	8
145	35.893885	0	1	Write	83221488	8
146	35.893904	0	1	Write	29124088	8
147	35.89392	0	1	Write	51078792	8
148	35.893939	0	1	Write	1645528	8
149	35.893958	0	1	Write	83226456	8
151	35.893994	0	1	Write	51085920	8
152	35.894019	0	1	Write	872208	8

153	35.894029	0	1	Write	50773824	8
156	35.894096	0	1	Write	5058712	8
157	35.894112	0	1	Write	50773840	8
159	35.894154	0	1	Write	51168072	8
160	35.894176	0	1	Write	16548600	8
163	35.894384	0	1	Write	103287976	8
164	35.894406	0	1	Write	200485976	8
167	35.894547	0	1	Write	1084208	8
168	35.894582	0	1	Write	200489400	8
169	35.894621	0	1	Write	50773984	8
171	35.894832	0	1	Write	280650632	8
173	35.89489	0	1	Write	50774064	8
175	35.895002	0	1	Write	279925152	8
176	35.895027	0	1	Write	43554632	8
177	35.89505	0	1	Write	50774168	8
178	35.895098	0	1	Write	80469344	8
179	35.895114	0	1	Write	24786184	8
180	35.89513	0	1	Write	50774232	8
181	35.895142	0	1	Write	21172040	8
182	35.895168	0	1	Write	80628872	8
183	35.895197	0	1	Write	50774272	8
184	35.895274	0	1	Write	7673024	8
185	35.895341	0	1	Write	50774304	8
186	35.895392	0	1	Write	10886568	8
64	16.813885	0	1	Write	64804560	9
90	31.815923	0	1	Write	64804568	10
5	9.998371	0	1	Write	72869200	12
26	10.54725	0	1	Write	24612512	16
27	10.54754	0	1	Write	24612528	16
28	10.547809	0	1	Write	24612512	16
29	10.547995	0	1	Write	24612512	16
36	10.551123	0	1	Write	24491056	16
38	10.551286	0	1	Write	2562160	16
46	10.553044	0	1	Write	567400	16
57	10.554891	0	1	Write	567408	16
63	16.8138	0	1	Write	14520456	16
68	18.891208	0	1	Write	567464	16
74	19.539421	0	1	Write	50971296	16
77	19.539867	0	1	Write	50971616	16
80	20.909389	0	1	Write	73912776	16
81	22.25939	0	1	Write	567384	16
86	27.718742	0	1	Write	567520	16
94	34.192336	0	1	Write	567544	16
119	35.893283	0	1	Write	51009400	16
123	35.893363	0	1	Write	50775784	16
142	35.893837	0	1	Write	29124064	16
155	35.894077	0	1	Write	51088632	16
158	35.89415	0	1	Write	29124248	16
161	35.894243	0	1	Write	29124272	16
165	35.894515	0	1	Write	29124304	16
174	35.89495	0	1	Write	80416888	16

91	33.165651	0	1	Write	567400	24
150	35.893978	0	1	Write	29124104	24
172	35.894867	0	1	Write	80416840	24
2	8.642429	0	1	Write	567496	32
10	10.539772	0	1	Read	27134568	32
11	10.540274	0	1	Read	27134536	32
12	10.540792	0	1	Read	27134224	32
13	10.541379	0	1	Read	54988880	32
14	10.54212	0	1	Read	54988752	32
15	10.542783	0	1	Read	54988720	32
130	35.893526	0	1	Write	29124472	32
162	35.894288	0	1	Write	50773872	32
166	35.894531	0	1	Write	50773912	32
107	35.892842	0	1	Write	148436656	40
154	35.894067	0	1	Write	29124144	40
8	10.53831	0	1	Read	54988040	48
16	10.5438	0	1	Read	27129584	48
72	19.538261	0	1	Write	567472	48
125	35.893402	0	1	Write	29124416	48
135	35.893699	0	1	Write	51010392	48
62	16.747099	0	1	Read	24129256	56
170	35.894784	0	1	Write	29124328	56
0	8.393994	0	1	Read	208032818	64
6	10.53689	0	1	Read	54987976	64
7	10.537573	0	1	Read	54988088	64
9	10.539061	0	1	Read	27130936	64
18	10.545037	0	1	Write	75053728	64
19	10.545158	0	1	Write	75053792	64
22	10.54593	0	1	Write	75060256	64
23	10.545934	0	1	Write	75060512	64
30	10.54828	0	1	Write	75051680	64
31	10.548511	0	1	Write	75051744	64
34	10.549894	0	1	Read	54987816	64
58	10.555232	0	1	Read	27129728	64
60	10.566827	0	1	Write	53299328	64
61	10.58215	0	1	Write	53298368	64
99	35.862893	0	1	Read	301720040	64
134	35.893686	0	1	Write	29124512	72
103	35.889744	0	1	Write	581920	128
65	18.170083	0	1	Write	581784	136
101	35.865245	0	1	Write	304010488	136
98	35.86288	0	1	Read	301720104	168
69	18.891597	0	1	Write	96081248	232
95	34.192707	0	1	Write	39353696	232
102	35.868669	0	1	Read	303151640	256
100	35.864877	0	1	Write	301779744	688



Result Analise:

After monitoring the disk activity and identifying the read and write processes with a length greater than 5, the following observations were made:

- The read processes listed above indicate the processes that performed data read operations with a length greater than 5.
- The write processes listed above indicate the processes that performed data write operations with a length greater than 5.
- By analysing these processes, further insights can be gained into potentially resource-intensive or suspicious activities on the system.

Conclusion:

- Disk monitoring can be a valuable technique to identify read and write processes with a length greater than 5. This information can be helpful in identifying potential performance bottlenecks, resource-intensive processes, or suspicious activities on the system.

Future scope:

- provide real-time alerts for processes with length > 5.
- Conducting a deeper analysis of the identified processes to understand their impact on system performance and security.
- Integrating the disk monitoring functionality with other security tools for comprehensive threat detection and prevention.