**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.

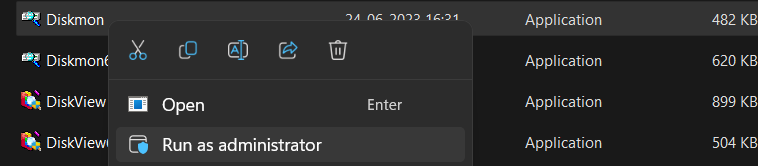
**Requirements:**

Sysinternal suite

Diskmon.exe

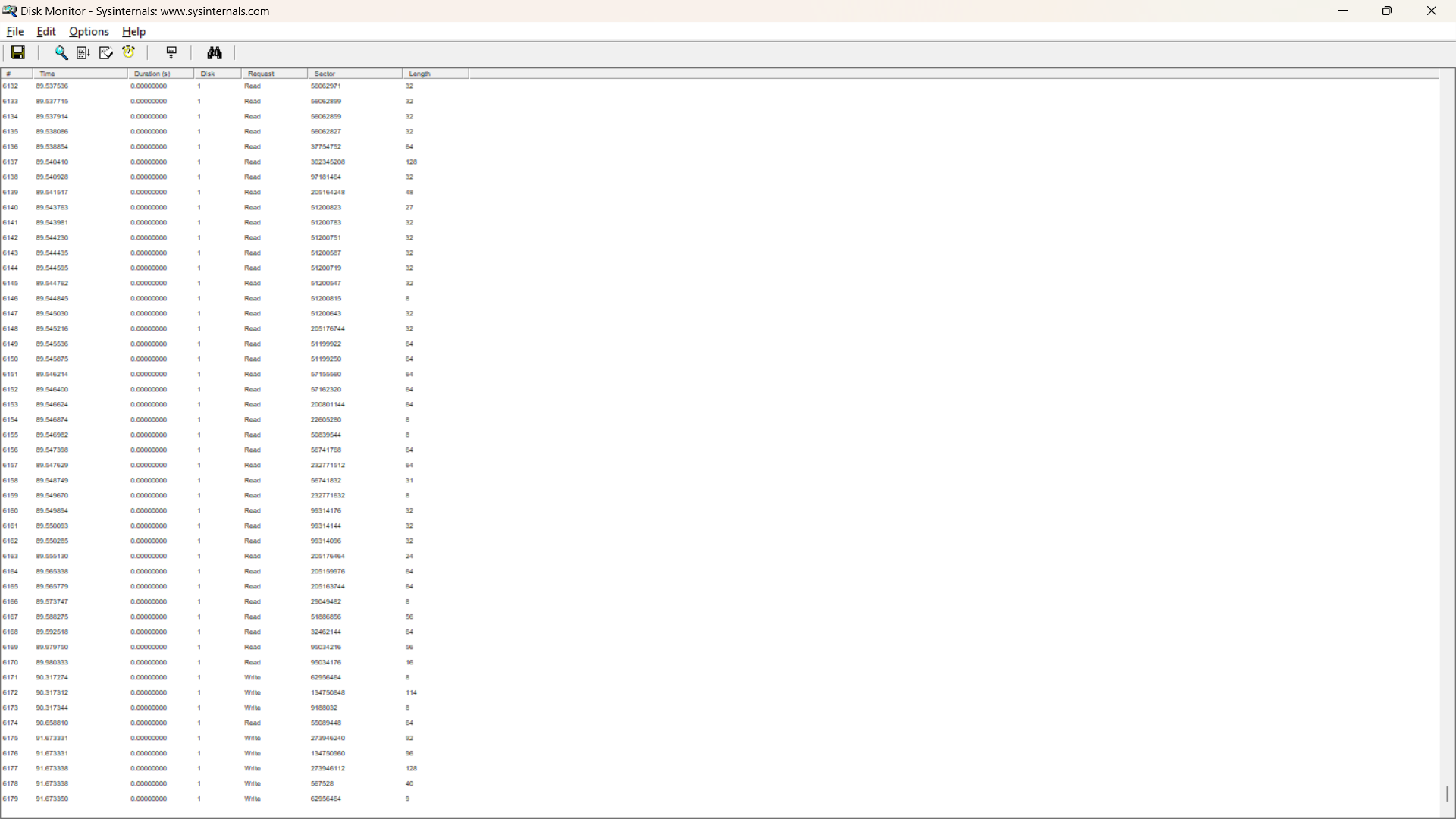
**Procedure/Experiment Steps:**

1. Download Disk Monitor:
   1. Open a web browser.
   2. Visit the official Microsoft website.
   3. Search for "Disk Monitor" or Sysinternal suite and navigate to the official download page.
   4. Download the appropriate version that compatible with your Windows operating system.
   5. Save the downloaded file.
2. Launch Disk Monitor:
   1. Navigate to the installation location of Disk Monitor.
   2. Double-click on the "Diskmon.exe" file to launch Disk Monitor.

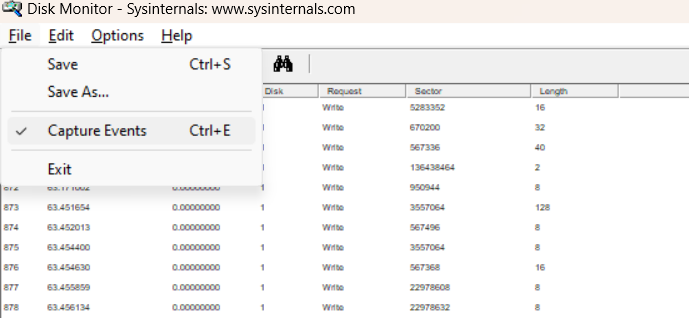


* 1. It will ask for the installation for the first time only.

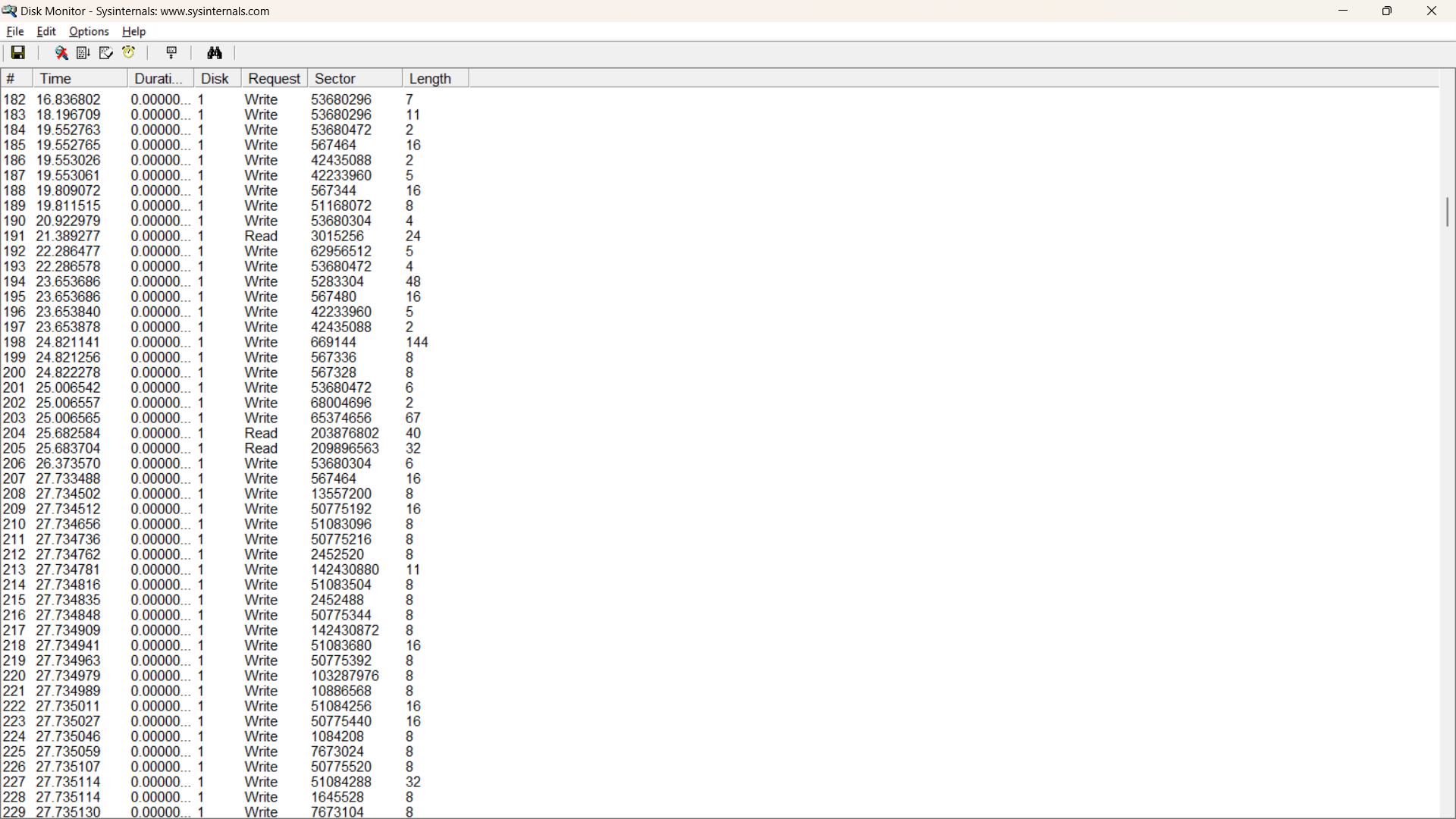
1. Explore Disk Monitor Interface:
   1. The Disk Monitor interface



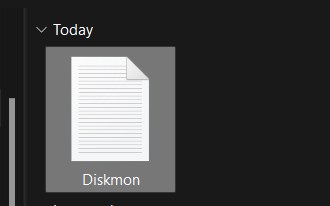
* 1. It automatic start capture the logs and data
  2. Go to file and click on capture Event or Press CTRL + E to stop

\

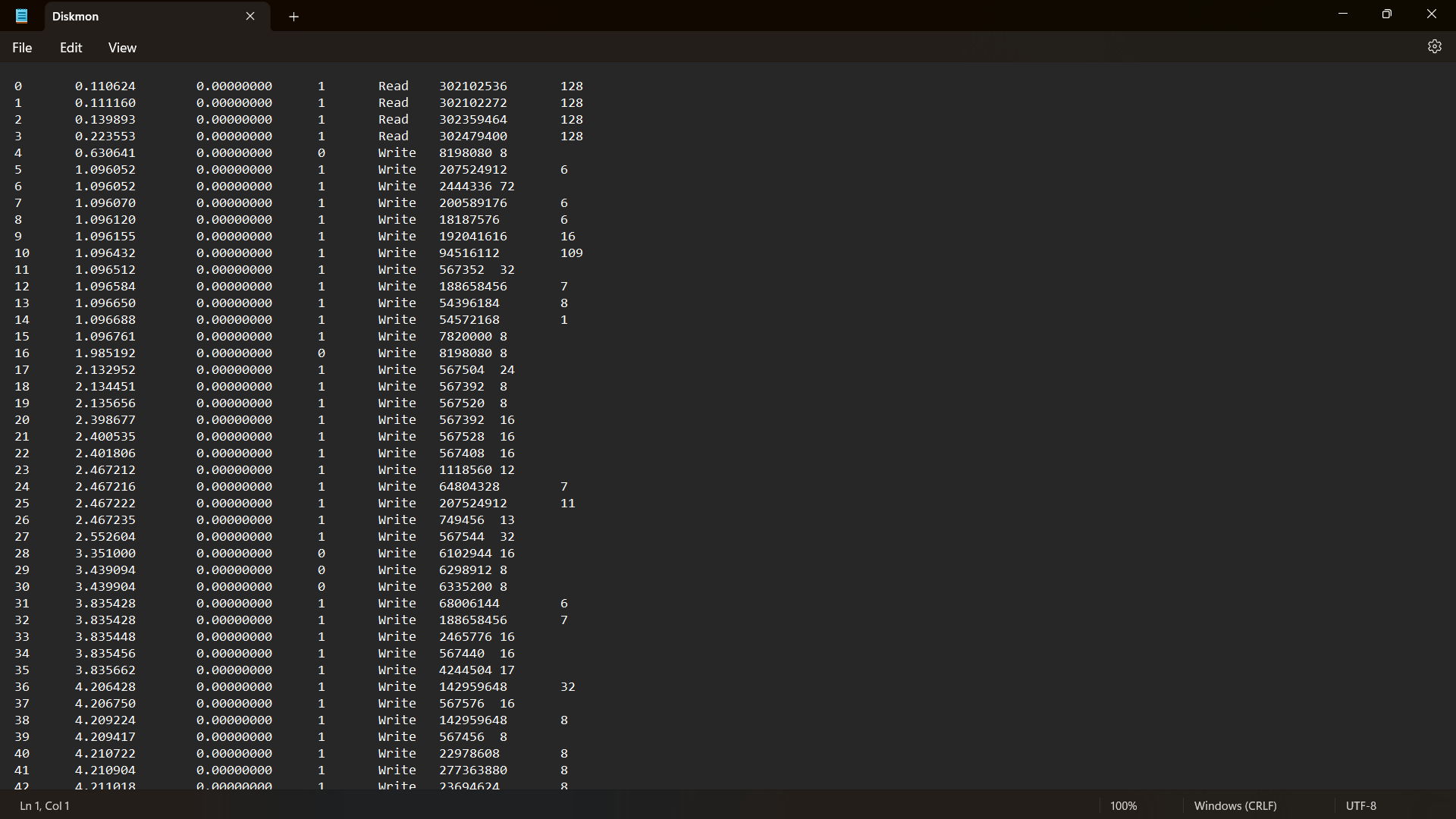
* 1. As we can see here all event in Read and write mode



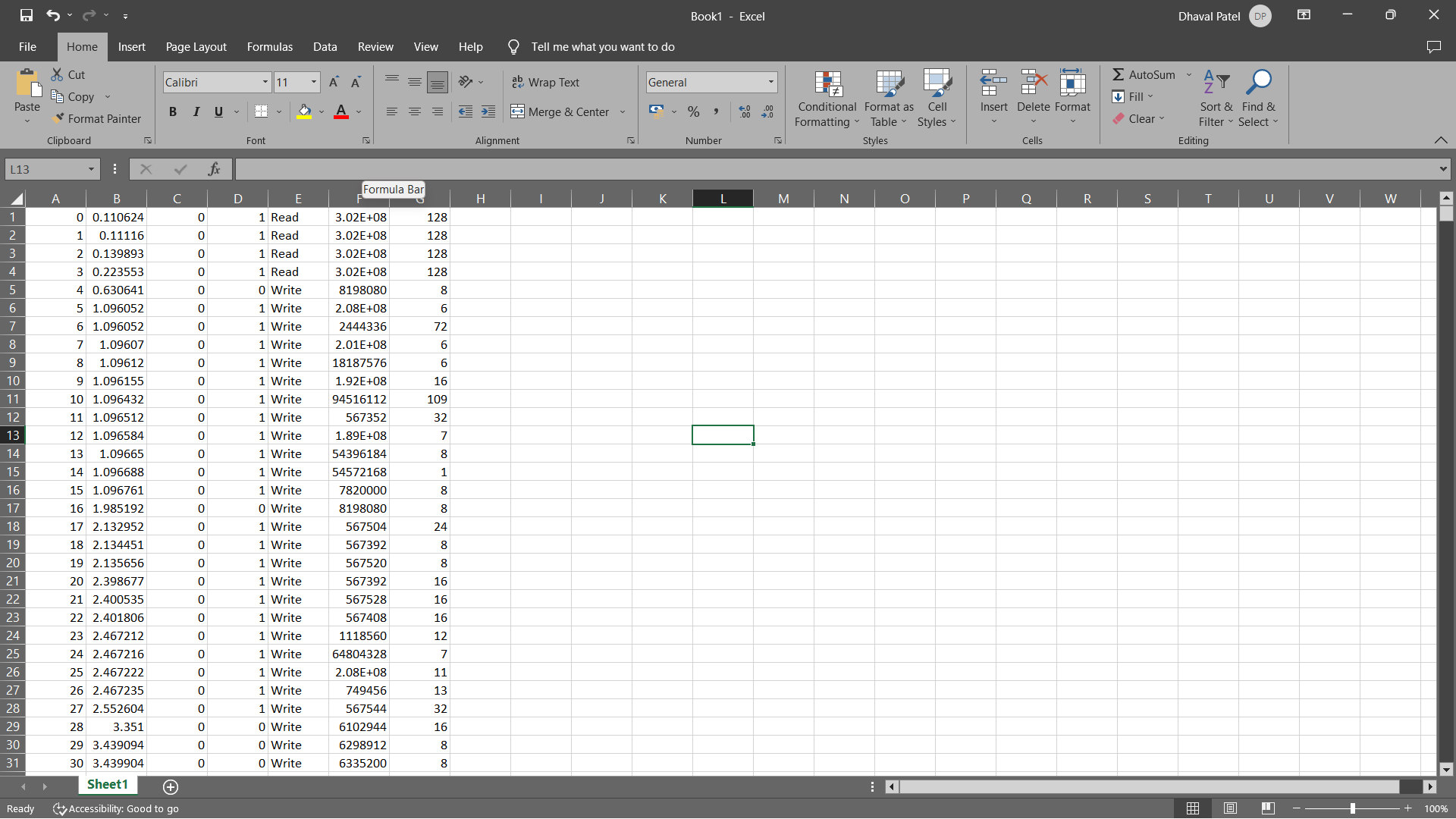
* 1. We can see Time, Duration, Disk, Request, Sector, Length
  2. Save the log file



* 1. Locket the file copy the data



* 1. open in excel



* 1. 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.