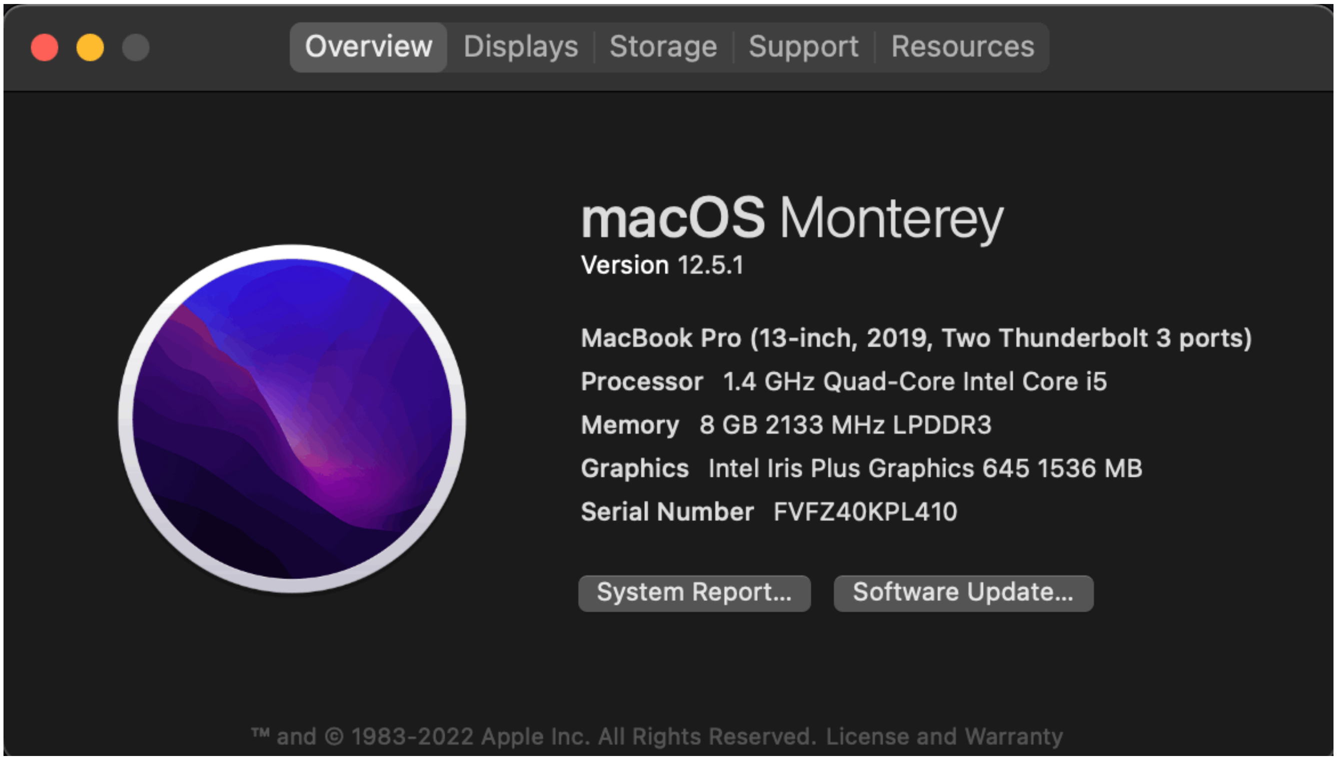
Devin Rankin

System Profiling Procedure

1. To profile my system, I first launced the `System Information` application.
2. From here, I was able to retrieve the Computer Name and Serial Number.



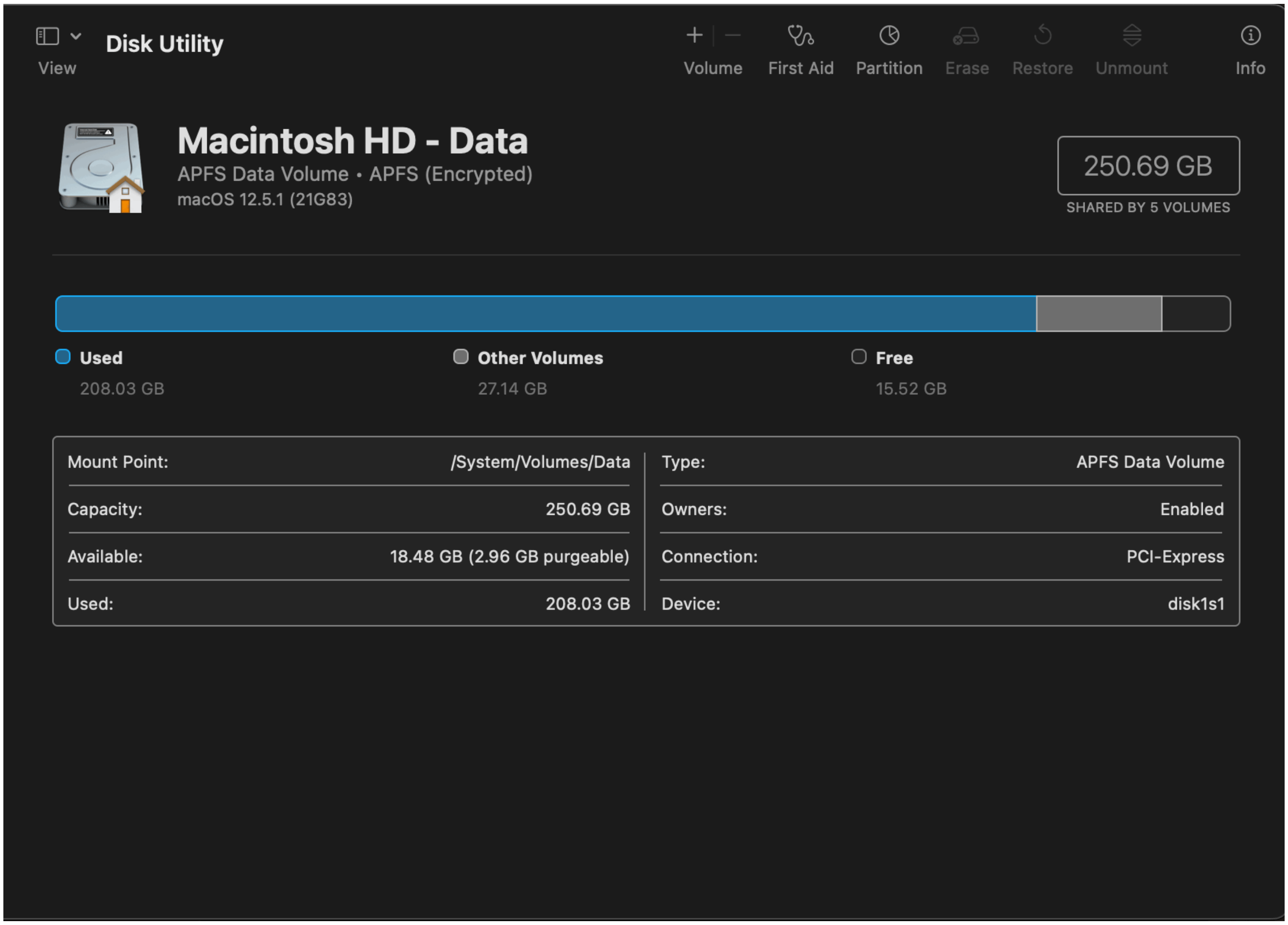
macOS Monterey
Version 12.5.1

MacBook Pro (13-inch, 2019, Two Thunderbolt 3 ports)
Processor 1.4 GHz Quad-Core Intel Core i5
Memory 8 GB 2133 MHz LPDDR3
Graphics Intel Iris Plus Graphics 645 1536 MB
Serial Number FVFZ40KPL410

™ and © 1983-2022 Apple Inc. All Rights Reserved. License and Warranty

3. I opened the `Disk Utility` application on MacOS, which shows information on the disks associated with the computer. I currently have `208GB` used and this data has a capacity of

`205.69GB` shared by 5 volumes.



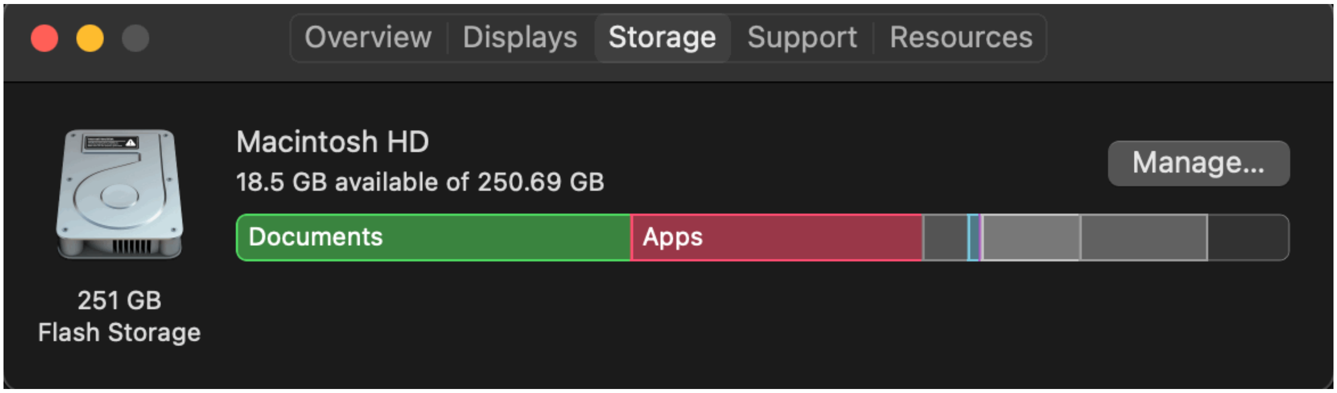
Macintosh HD - Data
APFS Data Volume • APFS (Encrypted)
macOS 12.5.1 (21G83)

250.69 GB
SHARED BY 5 VOLUMES

● **Used** 208.03 GB
○ **Other Volumes** 27.14 GB
○ **Free** 15.52 GB

Mount Point:	/System/Volumes/Data	Type:	APFS Data Volume
Capacity:	250.69 GB	Owners:	Enabled
Available:	18.48 GB (2.96 GB purgeable)	Connection:	PCI-Express
Used:	208.03 GB	Device:	disk1s1

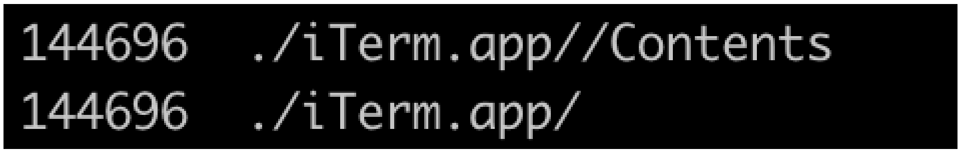
4. Then using `System Information`, I can see the space used by specific folders.



Macintosh HD
18.5 GB available of 250.69 GB

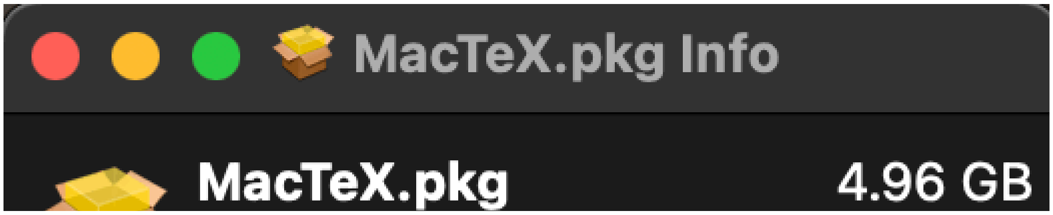
251 GB
Flash Storage

5. I can then use `du` to find what is taking up space in the Apps folder. It appears that iTerm is taking up a bit of space.



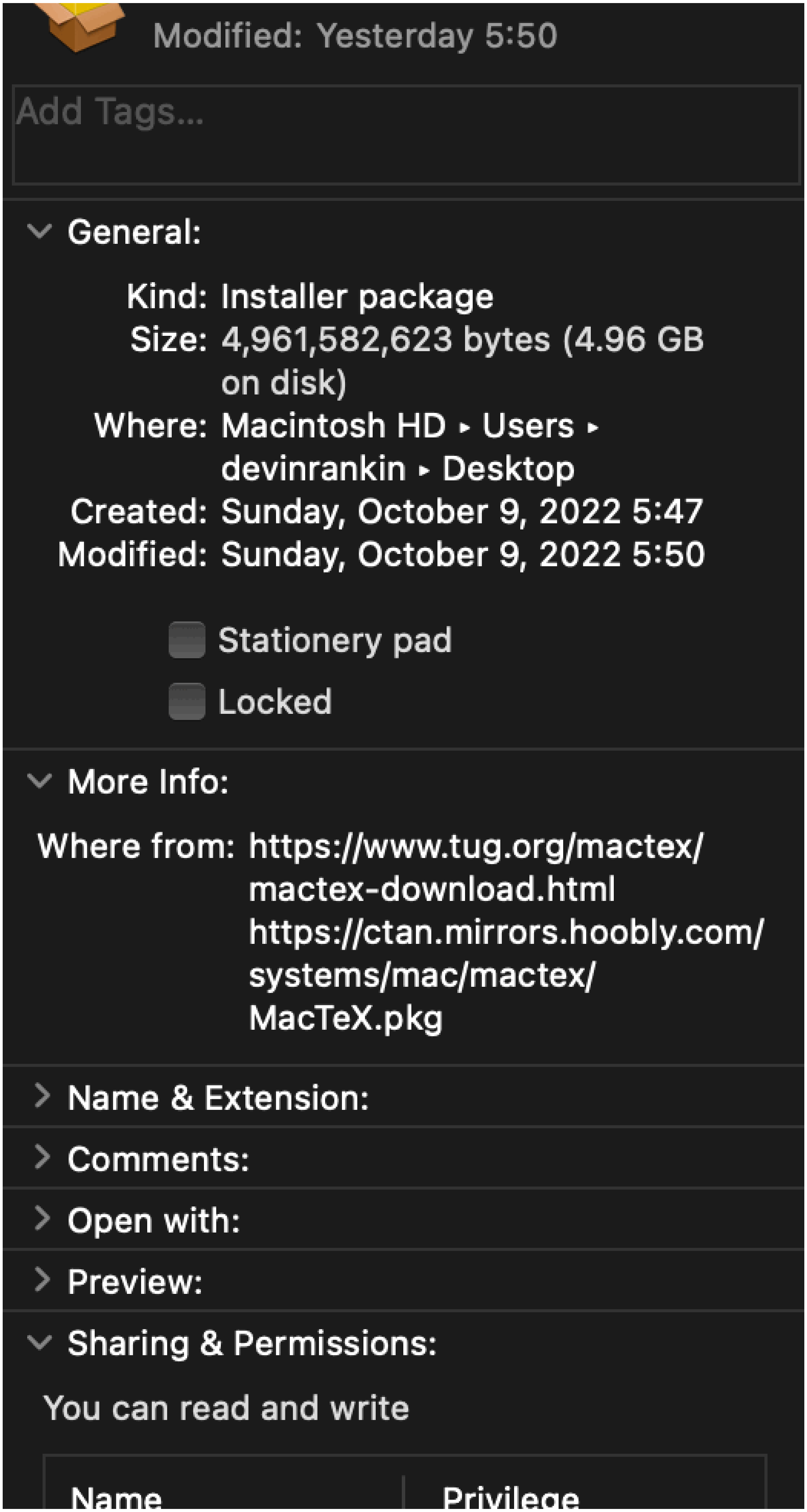
```
144696  ./iTerm.app//Contents
144696  ./iTerm.app/
```

6. Then I checked the metadata of a package that was downloaded off the internet.



MacTeX.pkg Info

MacTeX.pkg 4.96 GB



Modified: Yesterday 5:50

Add Tags...

General:

Kind: Installer package
Size: 4,961,582,623 bytes (4.96 GB on disk)
Where: Macintosh HD ▸ Users ▸ devinrankin ▸ Desktop
Created: Sunday, October 9, 2022 5:47
Modified: Sunday, October 9, 2022 5:50

☐ Stationery pad

☐ Locked

More Info:

Where from: https://www.tug.org/mactex/mactex-download.html
https://ctan.mirrors.hoobly.com/systems/mac/mactex/MacTeX.pkg

Name & Extension:

Comments:

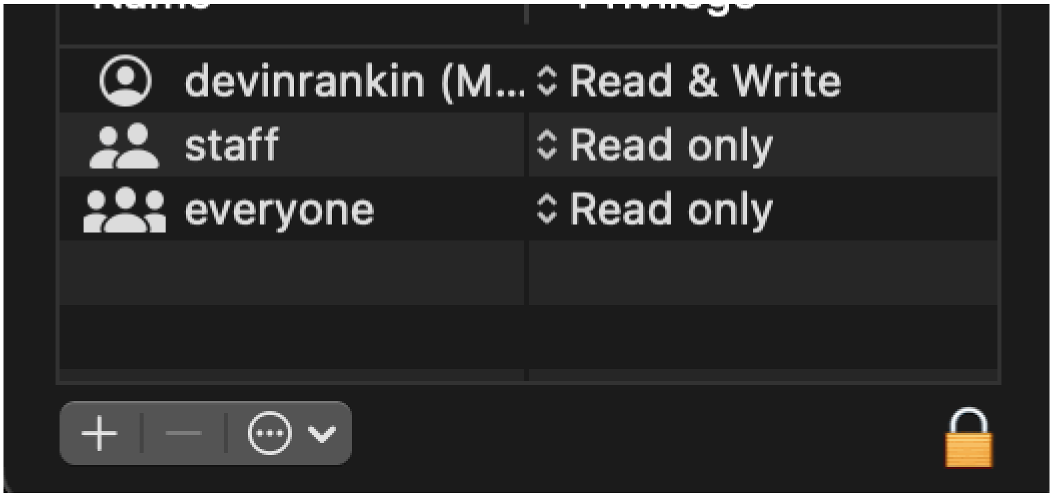
Open with:

Preview:

Sharing & Permissions:

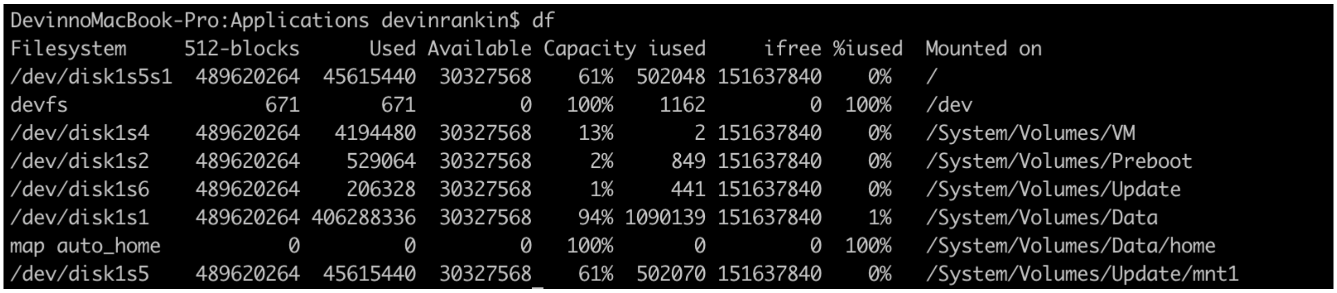
You can read and write

Name	Privilege



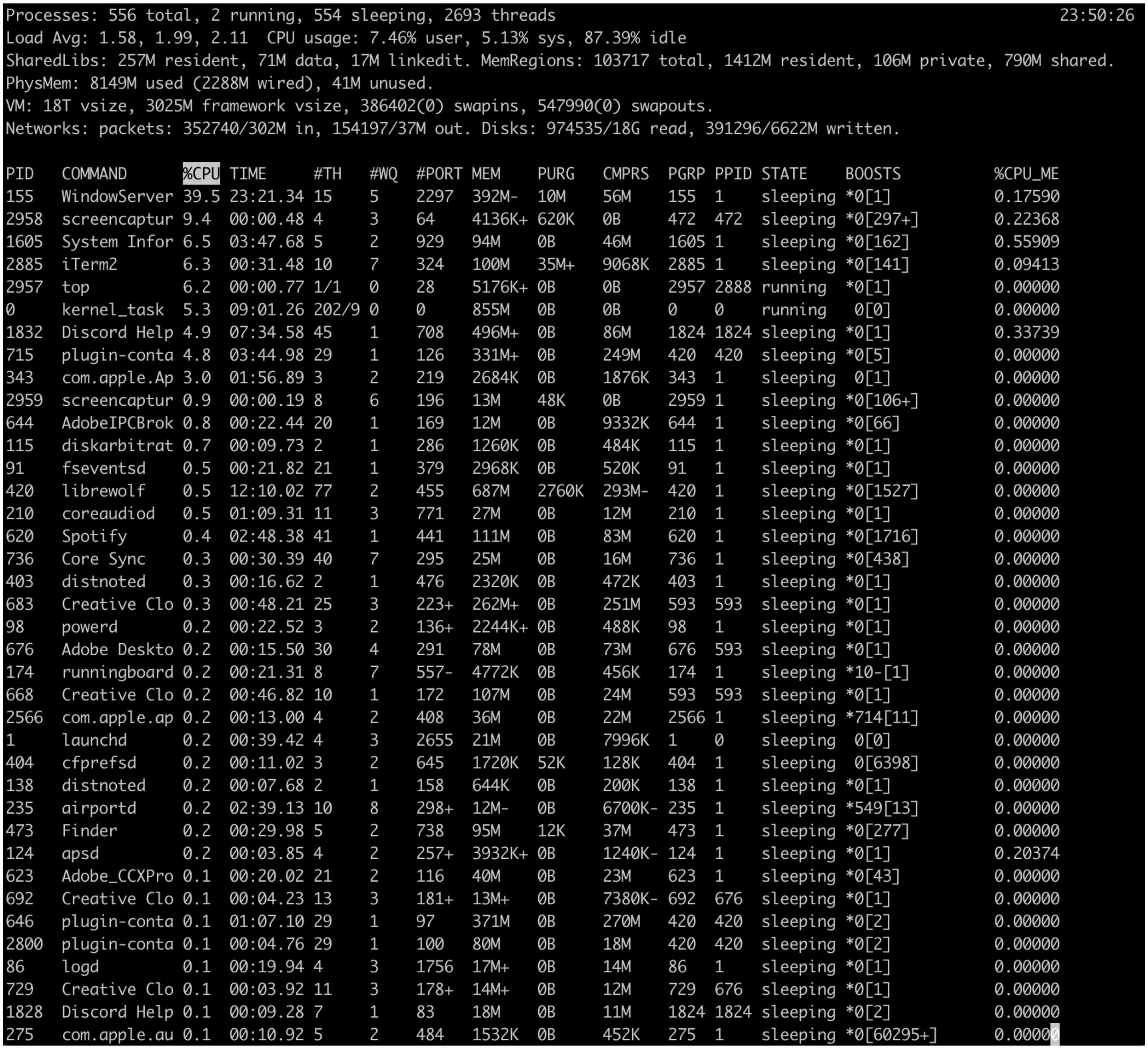
Name	Privilege
devinrankin (M…	Read & Write
staff	Read only
everyone	Read only

7. Using `df` I was able to get a list of all of my drives, their used and available space, and their capacity, as well as where they are mounted.



```
DevinnoMacBook-Pro:Applications devinrankin$ df
Filesystem     512-blocks      Used Available Capacity iused     ifree %iused  Mounted on
/dev/disk1s5s1  489620264  45615440  30327568    61%  502048 151637840    0%   /
devfs                 671       671         0   100%    1162         0  100%   /dev
/dev/disk1s4    489620264   4194480  30327568    13%       2 151637840    0%   /System/Volumes/VM
/dev/disk1s2    489620264    529064  30327568     2%     849 151637840    0%   /System/Volumes/Preboot
/dev/disk1s6    489620264    206328  30327568     1%     441 151637840    0%   /System/Volumes/Update
/dev/disk1s1    489620264 406288336  30327568    94% 1090139 151637840    1%   /System/Volumes/Data
map auto_home           0         0         0   100%       0         0  100%   /System/Volumes/Data/home
/dev/disk1s5    489620264  45615440  30327568    61%  502070 151637840    0%   /System/Volumes/Update/mnt1
```

8. Using `top`, I was able to get a list of processes and their memory and CPU usage.

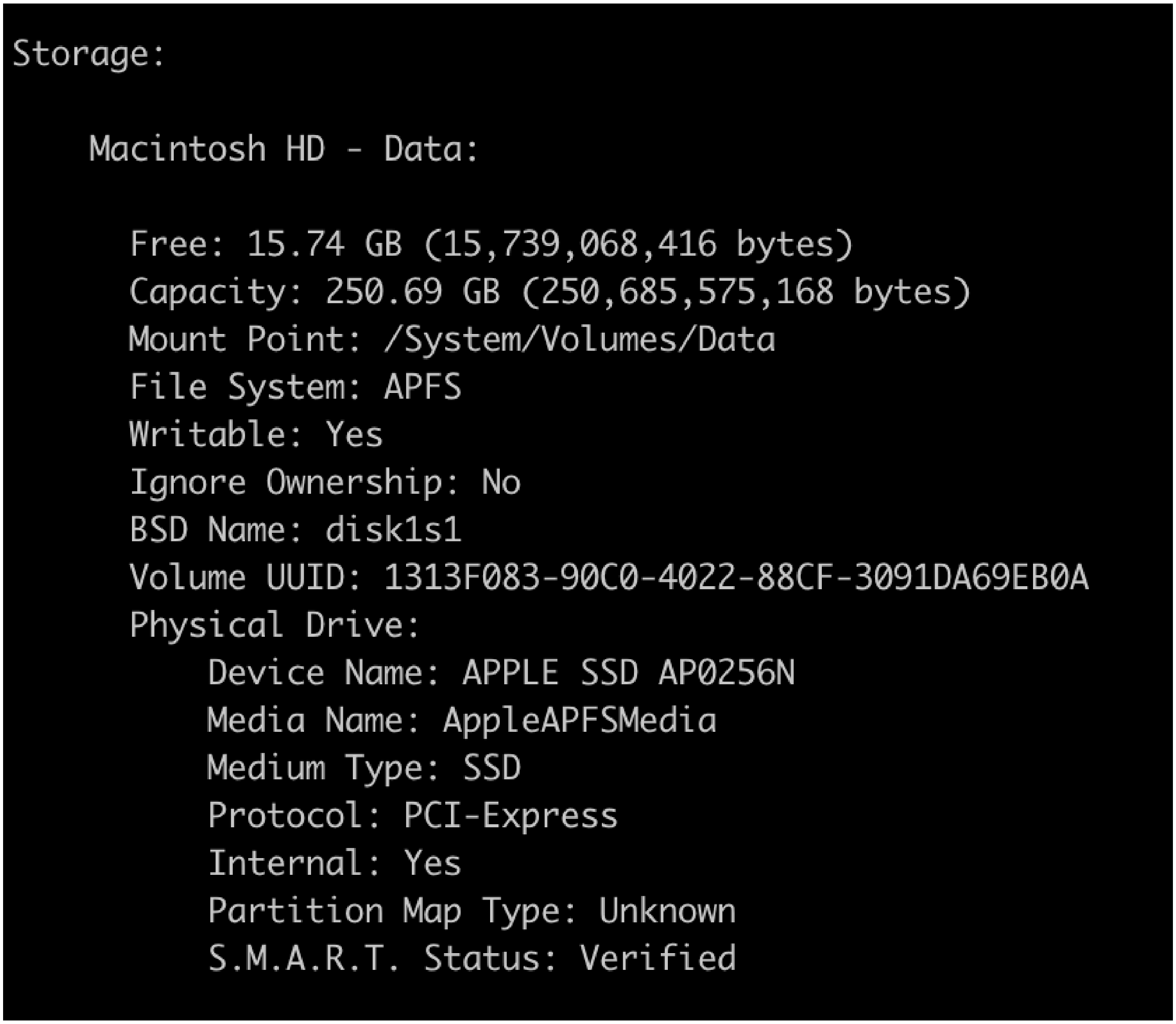


```
Processes: 556 total, 2 running, 554 sleeping, 2693 threads                                                            23:50:26
Load Avg: 1.58, 1.99, 2.11  CPU usage: 7.46% user, 5.13% sys, 87.39% idle
SharedLibs: 257M resident, 71M data, 17M linkedit. MemRegions: 103717 total, 1412M resident, 106M private, 790M shared.
PhysMem: 8149M used (2288M wired), 41M unused.
VM: 18T vsize, 3025M framework vsize, 386402(0) swapins, 547990(0) swapouts.
Networks: packets: 352740/302M in, 154197/37M out. Disks: 974535/18G read, 391296/6622M written.

PID   COMMAND      %CPU TIME     #TH   #WQ  #PORT MEM    PURG   CMPRS  PGRP PPID STATE    BOOSTS          %CPU_ME
155   WindowServer 39.5 23:21.34 15    5    2297  392M-  10M    56M    155  1    sleeping *0[1]           0.17590
2958  screencaptur 9.4  00:00.48 4     3    64    4136K+ 620K   0B     472  472  sleeping *0[297+]        0.22368
1605  System Infor 6.5  03:47.68 5     2    929   94M    0B     46M    1605 1    sleeping *0[162]         0.55909
2885  iTerm2       6.3  00:31.48 10    7    324   100M   35M+   9068K  2885 1    sleeping *0[141]         0.09413
2957  top          6.2  00:00.77 1/1   0    28    5176K+ 0B     0B     2957 2888 running  *0[1]           0.00000
0     kernel_task  5.3  09:01.26 202/9 0    0     855M   0B     0B     0    0    running   0[0]           0.00000
1832  Discord Help 4.9  07:34.58 45    1    708   496M+  0B     86M    1824 1824 sleeping *0[1]           0.33739
715   plugin-conta 4.8  03:44.98 29    1    126   331M+  0B     249M   420  420  sleeping *0[5]           0.00000
343   com.apple.Ap 3.0  01:56.89 3     2    219   2684K  0B     1876K  343  1    sleeping  0[1]           0.00000
2959  screencaptur 0.9  00:00.19 8     6    196   13M    48K    0B     2959 1    sleeping *0[106+]        0.00000
644   AdobeIPCBrok 0.8  00:22.44 20    1    169   12M    0B     9332K  644  1    sleeping *0[66]          0.00000
115   diskarbitrat 0.7  00:09.73 2     1    286   1260K  0B     484K   115  1    sleeping *0[1]           0.00000
91    fseventsd    0.5  00:21.82 21    1    379   2968K  0B     520K   91   1    sleeping *0[1]           0.00000
420   librewolf    0.5  12:10.02 77    2    455   687M   2760K  293M-  420  1    sleeping *0[1527]        0.00000
210   coreaudiod   0.5  01:09.31 11    3    771   27M    0B     12M    210  1    sleeping *0[1]           0.00000
620   Spotify      0.4  02:48.38 41    1    441   111M   0B     83M    620  1    sleeping *0[1716]        0.00000
736   Core Sync    0.3  00:30.39 40    7    295   25M    0B     16M    736  1    sleeping *0[438]         0.00000
403   distnoted    0.3  00:16.62 2     1    476   2320K  0B     472K   403  1    sleeping *0[1]           0.00000
683   Creative Clo 0.3  00:48.21 25    3    223+  262M+  0B     251M   593  593  sleeping *0[1]           0.00000
98    powerd       0.2  00:22.52 3     2    136+  2244K+ 0B     488K   98   1    sleeping *0[1]           0.00000
676   Adobe Deskto 0.2  00:15.50 30    4    291   78M    0B     73M    676  593  sleeping *0[1]           0.00000
174   runningboard 0.2  00:21.31 8     7    557-  4772K  0B     456K   174  1    sleeping *10-[1]         0.00000
668   Creative Clo 0.2  00:46.82 10    1    172   107M   0B     24M    593  593  sleeping *0[1]           0.00000
2566  com.apple.ap 0.2  00:13.00 4     2    408   36M    0B     22M    2566 1    sleeping *714[11]        0.00000
1     launchd      0.2  00:39.42 4     3    2655  21M    0B     7996K  1    0    sleeping  0[0]           0.00000
404   cfprefsd     0.2  00:11.02 3     2    645   1720K  52K    128K   404  1    sleeping  0[6398]        0.00000
138   distnoted    0.2  00:07.68 2     1    158   644K   0B     200K   138  1    sleeping *0[1]           0.00000
235   airportd     0.2  02:39.13 10    8    298+  12M-   0B     6700K- 235  1    sleeping *549[13]        0.00000
473   Finder       0.2  00:29.98 5     2    738   95M    12K    37M    473  1    sleeping *0[277]         0.00000
124   apsd         0.2  00:03.85 4     2    257+  3932K+ 0B     1240K- 124  1    sleeping *0[1]           0.20374
623   Adobe_CCXPro 0.1  00:20.02 21    2    116   40M    0B     23M    623  1    sleeping *0[43]          0.00000
692   Creative Clo 0.1  00:04.23 13    3    181+  13M+   0B     7380K- 692  676  sleeping *0[1]           0.00000
646   plugin-conta 0.1  01:07.10 29    1    97    371M   0B     270M   420  420  sleeping *0[2]           0.00000
2800  plugin-conta 0.1  00:04.76 29    1    100   80M    0B     18M    420  420  sleeping *0[2]           0.00000
86    logd         0.1  00:19.94 4     3    1756  17M+   0B     14M    86   1    sleeping *0[1]           0.00000
729   Creative Clo 0.1  00:03.92 11    3    178+  14M+   0B     12M    729  676  sleeping *0[1]           0.00000
1828  Discord Help 0.1  00:09.28 7     1    83    18M    0B     11M    1824 1824 sleeping *0[2]           0.00000
275   com.apple.au 0.1  00:10.92 5     2    484   1532K  0B     452K   275  1    sleeping *0[60295+]      0.00000
```

9. A command that may be worth noting but is way too large to possibly screenshot is `system_profiler`. In this instance, I just grabbed some storage information, but it displays

almost all system information.



```
Storage:

    Macintosh HD - Data:

      Free: 15.74 GB (15,739,068,416 bytes)
      Capacity: 250.69 GB (250,685,575,168 bytes)
      Mount Point: /System/Volumes/Data
      File System: APFS
      Writable: Yes
      Ignore Ownership: No
      BSD Name: disk1s1
      Volume UUID: 1313F083-90C0-4022-88CF-3091DA69EB0A
      Physical Drive:
          Device Name: APPLE SSD AP0256N
          Media Name: AppleAPFSMedia
          Medium Type: SSD
          Protocol: PCI-Express
          Internal: Yes
          Partition Map Type: Unknown
          S.M.A.R.T. Status: Verified
```

Metadata

- Important metadata to include in a chain of custody includes:
  - Creation date
  - Modification dates
  - File or directory permissions
  - Logs
  - Download location (if downloaded)
  - Disk partitions
  - Size and file type