

Process Survey

1. What root-owned processes are running?

(a) Of course the processes are a lot and the below images show them all. However, in order to get the processes that are running as root I used the command: `ps -u root`

(b) The command used is: `Abduls-MacBook-Pro:/ AbdulZaid$ ps -u root`

(c)

UID	PID	TTY	TIME	CMD
0	1	??	9:47.10	/sbin/launchd
0	11	??	1:31.35	/usr/libexec/UserEventAgent (System)
0	12	??	0:05.77	/usr/libexec/kextd
0	13	??	0:24.11	/usr/libexec/taskgated -s
0	14	??	2:53.33	/usr/sbin/securityd -i
0	15	??	1:09.49	/usr/sbin/notifyd
0	16	??	0:56.64	/System/Library/CoreServices/powerd.bundle/power
0	17	??	2:06.44	/usr/libexec/configd
0	18	??	0:08.70	/usr/libexec/diskarbitrationd
0	19	??	2:26.52	/usr/sbin/distnoted daemon
0	20	??	2:19.54	/usr/sbin/syslogd
0	21	??	1:44.45	/usr/libexec/opaendirectoryd
0	25	??	0:02.82	/usr/libexec/warmd
0	29	??	0:01.45	/usr/libexec/stackshot -t
0	32	??	0:00.12	/System/Library/CoreServices/SleepServicesD
0	34	??	0:18.68	/System/Library/PrivateFrameworks/GenerationalSt
0	39	??	28:16.78	/System/Library/Frameworks/CoreServices.framework
501	43	??	2:13.39	/System/Library/CoreServices/loginwindow.app/Con
0	44	??	0:00.41	/System/Library/CoreServices/loginind
0	46	??	0:00.04	/usr/sbin/KernelEventAgent
0	116	??	0:02.31	/usr/libexec/networkd_privileged
0	125	??	0:01.61	/System/Library/Frameworks/OpenGL.framework/Vers
0	164	??	0:08.03	/usr/sbin/racoon -D
0	165	??	0:04.98	/usr/libexec/securityd_service
0	227	??	0:07.50	/usr/sbin/filecoordinationd
0	283	??	0:02.86	/usr/libexec/syspolicyd
0	417	??	3:05.83	/System/Library/Frameworks/CoreMediaIO.framework
0	484	??	0:40.12	/sbin/launchd
0	487	??	0:00.09	/System/Library/Frameworks/CoreServices.framework
0	31580	??	0:04.56	/usr/sbin/cfprefsd daemon
0	31583	??	0:07.19	/usr/libexec/systemstatsd
0	31615	??	0:00.18	com.apple.CodeSigningHelper
0	32693	??	0:02.55	/usr/sbin/ocspd
0	32877	??	0:00.28	sysmond
0	32951	??	0:00.06	/System/Library/PrivateFrameworks/SoftwareUpdate
0	32952	??	0:00.03	/usr/libexec/xpcd
0	33105	??	0:00.19	/usr/libexec/sandboxd -n PluginProcess -n
0	33110	??	0:00.02	/System/Library/PrivateFrameworks/CoreSymbolicat
0	33178	??	3:02.14	com.apple.coremedia.videodecoder
0	33217	??	0:00.03	/System/Library/PrivateFrameworks/TCC.framework/
501	43	??	2:13.39	/System/Library/CoreServices/loginwindow.app/Con
0	44	??	0:00.41	/System/Library/CoreServices/loginind
0	46	??	0:00.04	/usr/sbin/KernelEventAgent
0	48	??	38:15.21	/usr/libexec/hidd
0	49	??	5:02.54	/System/Library/Frameworks/CoreServices.framework
0	51	??	0:00.02	/sbin/dynamic_pager -F /private/var/vm/swapfile
0	54	??	1:11.48	/System/Library/CoreServices/launchservicesd
0	59	??	0:07.08	/usr/sbin/awacsd
0	60	??	0:01.46	autofs
0	61	??	0:31.08	/System/Library/PrivateFrameworks/ApplePushServi
0	63	??	1:47.64	/usr/libexec/airportd
0	65	??	1:44.90	/System/Library/CoreServices/coreservicesd
0	69	??	0:04.67	com.apple.authd
0	82	??	12:44.46	/System/Library/Frameworks/CoreServices.framework
88	85	??	293:42.85	/System/Library/Frameworks/ApplicationServices.f
0	96	??	0:12.36	/usr/libexec/usbd
0	97	??	0:03.51	/usr/sbin/ntpd -c /private/etc/ntp-restrict.conf
0	98	??	0:04.89	/usr/sbin/cupsd -l
0	100	??	1:10.54	/usr/libexec/pacemaker -b -e 0.0001 -a 10
0	116	??	0:02.31	/usr/libexec/networkd_privileged
0	125	??	0:01.61	/System/Library/Frameworks/OpenGL.framework/Vers
0	164	??	0:08.03	/usr/sbin/racoon -D
0	165	??	0:04.98	/usr/libexec/securityd_service
0	227	??	0:07.50	/usr/sbin/filecoordinationd

2. What processes are running on your account?

(a) The processes that are running on my account are a lot, for example in my case, *bash*, *chrome*, *screen*, and a lot more. I used *ps -u AbdulZaid*

(b) The Command used is: *Abduls-MacBook-Pro:/ AbdulZaid\$ ps -u AbdulZaid*

(c)

Abduls-MacBook-Pro:/ AbdulZaid\$ ps -u AbdulZaid				
UID	PID	TTY	TIME	CMD
501	162	??	1:42.60	/sbin/launchd
501	167	??	1:03.69	/usr/libexec/UserEventAgent (Aqua)
501	168	??	8:53.38	/usr/sbin/distnoted agent
501	174	??	3:26.10	/System/Library/CoreServices/Dock.app/Contents/M
501	176	??	2:11.22	/System/Library/CoreServices/SystemUIServer.app/
501	177	??	19:19.72	/System/Library/CoreServices/Finder.app/Contents
501	184	??	0:00.08	/usr/sbin/pboard
501	189	??	0:08.54	/usr/libexec/sharingd
501	192	??	0:10.52	/usr/libexec/librariand
501	193	??	1:15.96	/System/Library/Frameworks/ApplicationServices.f
501	195	??	0:37.06	/System/Library/PrivateFrameworks/Ubiquity.frame
501	197	??	0:11.36	/usr/sbin/usernoted
501	198	??	0:37.48	/System/Library/CoreServices/NotificationCenter.
501	200	??	0:00.20	/System/Library/CoreServices/SocialPushAgent.app
501	201	??	0:18.67	/System/Library/PrivateFrameworks/MessageKit.fr
501	205	??	0:03.95	/usr/libexec/lsboxd
501	207	??	0:38.71	/System/Library/PrivateFrameworks/IMCore.framewo
501	208	??	1:01.51	/System/Library/PrivateFrameworks/IDSCore.framew
501	212	??	3:33.91	/System/Library/PrivateFrameworks/CalendarAgent.
501	230	??	2:52.58	/Applications/iPhoto.app/Contents/Library/LoginI
501	236	??	0:04.20	/Applications/iTunes.app/Contents/MacOS/iTunesHe
501	240	??	0:26.64	/Applications/Reader.app/Contents/Resources/read
501	241	??	52:53.72	/Applications/Google Drive.app/Contents/MacOS/Go
501	253	??	20:55.77	/Applications/Dropbox.app/Contents/MacOS/Dropbox
501	275	??	0:08.22	com.apple.dock.extra
501	332	??	416:32.50	/Applications/Google Chrome.app/Contents/MacOS/G
501	350	??	98:58.04	/Applications/Google Chrome.app/Contents/Version
501	353	??	0:19.57	/System/Library/Image Capture/Support/Image Capt
501	355	??	3:49.49	/Library/Image Capture/Support/LegacyDeviceDisco
501	367	??	0:04.27	/System/Library/PrivateFrameworks/UniversalAcces
501	398	??	0:36.18	/System/Library/Frameworks/CoreServices.framework
501	428	??	78:49.91	/Applications/Google Chrome.app/Contents/Version
501	429	??	0:22.17	/Applications/Google Chrome.app/Contents/Version
501	522	??	0:51.30	/System/Library/Services/AppleSpell.service/Cont
501	809	??	0:04.65	/System/Library/PrivateFrameworks/CloudServices.
501	1162	??	0:00.10	/System/Library/PrivateFrameworks/KerberosHelper
501	1363	??	0:04.90	/System/Library/PrivateFrameworks/CommerceKit.fr
501	1729	??	0:01.41	/System/Library/PrivateFrameworks/HelpData.frame
501	1746	??	348:14.16	/Applications/Google Chrome.app/Contents/Version
501	1790	??	0:02.86	/usr/bin/ssh-agent -l
501	4415	??	0:13.77	/usr/libexec/WiFiKeychainProxy
501	7234	??	447:13.88	/Applications/Google Chrome.app/Contents/Version
501	7934	??	0:00.20	/System/Library/Frameworks/CoreServices.framework

501	33207	??	0:07.97	/Applications/Google Chrome.app/Contents/Version
501	33228	??	0:00.06	/System/Library/Frameworks/Accounts.framework/Ve
501	33243	??	0:07.81	/Applications/iTunes.app/Contents/MacOS/iTunes
501	33246	??	0:00.05	com.apple.BKAgentService
501	33251	??	0:00.24	/System/Library/PrivateFrameworks/AirTrafficHost
501	33252	??	0:05.48	com.apple.MediaLibraryService
501	33254	??	0:00.05	/System/Library/PrivateFrameworks/MobileDevice.f
501	33275	??	0:00.66	/System/Library/Frameworks/CoreServices.framework
501	33280	??	0:00.35	/System/Library/Frameworks/CoreServices.framework
501	33282	??	0:02.77	/Applications/Google Chrome.app/Contents/Version
501	33288	??	0:00.74	/System/Library/Frameworks/CoreServices.framework
501	33289	??	0:00.01	/usr/sbin/traceroute -q 1 antitheft.zeobit.com
501	33299	??	0:00.07	/System/Library/Frameworks/CoreServices.framework
501	33300	??	0:00.07	/System/Library/Frameworks/CoreServices.framework
0	33203	ttys000	0:00.10	login -pf AbdulZaid
501	33204	ttys000	0:00.06	-bash
0	33301	ttys000	0:00.01	ps -u AbdulZaid
0	29959	ttys001	0:00.04	login -pflq AbdulZaid /bin/bash
501	29960	ttys001	0:00.02	bash
501	29961	ttys001	0:16.88	ping localhost
0	29967	ttys002	0:00.03	login -pflq AbdulZaid /bin/bash
501	29968	ttys002	0:00.01	bash

3. Run a typical working set of applications (e.g web browser, chat program, text editor, etc.). Which application is using the most real memory? The most virtual memory?

(a) The application that is using the most real memory (MEM) is **Google Chrome**, and the program that is using the most Virtual memory (VSIZE) is **Apple Pages**.

(b) The command used: *Abduls-MacBook-Pro:/ AbdulZaid\$ top*

(c)

Abduls-MacBook-Pro:/ AbdulZaid\$ top

Processes: 189 total, 2 running, 1 stuck, 186 sleeping, 1095 threads20:31:29

Load Avg: 10.80, 9.12, 9.30 CPU usage: 4.43% user, 7.31% sys, 88.24% idle

SharedLibs: 39M resident, 0B data, 3120K linkedit. MemRegions: 51626 total, 801M resident, 37M private, 283M shared.

PhysMem: 2301M used (1141M wired), 26M unused.

VM: 425G vsize, 1311M framework vsize, 219104(0) swapins, 550740(0) swapouts.

Networks: packets: 18190836/16G in, 12763045/4209M out. Disks: 7299243/143G read, 3574790/90G written.

PID	COMMAND	%CPU	TIME	#TH	#WQ	#PORT	#MREG	MEM	RPRVT	PURG	CMPRS	VPRVT	VSIZE	PGRP	PPID
40768	screencaptur	1.4	00:00.09	4	2	50	87	1704K	676K	4096B	0B	22M	2440M	176	176
40765	QuickLookSat	0.0	00:00.19	2	0	50	75	8544K	7544K	0B	0B	58M	2461M	40765	1
40764	top	11.1	00:03.93	1/1	0	24	37	2560K+	2332K+	0B	0B	44M	2403M	40764	40440
40762	quicklookd	0.0	00:00.53	5	1	89	88	9208K	8064K	0B	0B	69M	2972M	40762	162
40761	mdworker	0.0	00:00.43	3	0	56	66	6416K	5420K	0B	0B	55M	2424M	40761	162
40744	mdworker	0.0	00:00.36	4	0	54	96	3940K	2720K	0B	4136K	53M	2424M	40744	162
40736-	Google Chrom	0.2	00:46.74	12	0	144	529	49M	47M	0B	22M	144M	976M	332	332
40716-	Google Chrom	0.1	00:16.27	12	0	144	438	36M+	34M+	0B	18M-	130M	892M	332	332
40686	netbiosd	0.0	00:00.04	2	1	43	40	292K	192K	0B	656K	53M	2412M	40686	1
40552	sandboxd	0.0	00:00.14	3	1	60	45	260K	156K	0B	1420K	62M	2443M	40552	1
40551	GitHub Condu	0.0	00:00.29	3	0	130	82	1420K	844K	0B	2736K	45M	2455M	40551	162
40534	GitHub	0.0	00:04.10	5	0	210	523	10M	8296K	0B	34M	94M	2584M	40534	162
40440	bash	0.0	00:00.07	1	0	19	33	280K	308K	0B	380K	44M	2403M	40440	40438
40438	login	0.0	00:00.10	2	0	30	47	8192B	0B	0B	1000K	45M	2411M	40438	40436
40436	Terminal	0.5	00:25.76	8	2	189	169	15M	4312K	0B	4856K	55M	2510M	40436	162
40402-	Google Chrom	0.0	00:36.26	12	0	144	509	7832K	6976K	0B	50M	130M	938M	332	332
40397	com.apple.Co	0.0	00:00.02	2	1	30	45	12K	0B	0B	1016K	45M	2412M	40397	1
40381	Preview	0.0	00:13.50	3	0	256	405	14M	7400K	0B	28M	99M	2604M	40381	162
40342-	Google Chrom	0.1	00:30.71	12	0	144	493	24M+	23M+	0B	42M-	144M	916M	332	332
40336-	Google Chrom	0.0	00:18.29	12	0	76	510	2696K	1872K	0B	11M	67M	853M	332	332
40334-	Google Chrom	0.0	00:16.32	12	0	144	455	14M	13M	0B	45M	138M	899M	332	332
40331-	Google Chrom	0.0	00:12.30	12	0	144	530	33M	32M	0B	53M	167M	922M	332	332
40328	com.apple.ap	0.0	00:07.90	3	0	229	262	7376K	6188K	0B	17M	79M	2529M	40328	1
40326	com.apple.hi	0.0	00:00.04	2	0	30	42	8192B	0B	0B	1092K	45M	2411M	40326	1
40303	Pages	0.0	02:03.85	6	0	280	2330	41M	21M	0B	68M	142M	4045M	40303	162
40280	com.apple.la	0.0	00:00.21	5	1	95	71	332K	212K	0B	3488K	47M	2437M	40280	1

4. Login to my.cs.lmu.edu. Who else, other than root and you, has processes running at that time?

(a) The processes running at that time includes: *kthreadd*, *ksoftirqd*, *migration*, *udev*, *nfsd*, *apache2*, *sshd*, and *ps*, and many others.

(b) The command used: *aalzaid1@ab201:~\$ ps -d*

(c)

```
aalzaid1@ab201:~$ ps -d
```

PID	TTY	TIME	CMD
2	?	00:00:00	kthreadd
3	?	00:06:00	ksoftirqd/0
6	?	00:00:00	migration/0
7	?	00:00:00	migration/1
8	?	00:00:00	kworker/1:0
9	?	00:02:01	ksoftirqd/1
11	?	00:00:00	migration/2
12	?	00:02:28	kworker/2:0
13	?	00:02:56	ksoftirqd/2
14	?	00:00:00	migration/3
15	?	00:00:00	kworker/3:0
16	?	00:01:51	ksoftirqd/3
17	?	00:00:00	cpuset
18	?	00:00:00	khelper
19	?	00:00:00	netns
20	?	00:00:00	kworker/u:1
21	?	00:00:16	sync_supers
22	?	00:00:00	bdi-default
23	?	00:00:00	kintegrityd
24	?	00:00:00	kblockd
25	?	00:00:00	ata_sff
26	?	00:00:00	khubd
27	?	00:00:00	md
28	?	00:07:19	kworker/1:1
29	?	00:05:03	kworker/2:1
30	?	00:05:03	kworker/3:1
31	?	00:00:02	khungtaskd
32	?	01:00:02	kswapd0
33	?	00:00:00	ksmd
34	?	00:00:00	khugepaged
35	?	00:00:00	fsnotify_mark
36	?	00:00:00	ecryptfs-kthrea
37	?	00:00:00	crypto
45	?	00:00:00	kthrotld
46	?	00:00:00	scsi_eh_0
47	?	00:00:00	scsi_eh_1
48	?	00:00:01	kworker/u:2
257	?	00:00:22	jbd2/sda1-8
258	?	00:00:00	ext4-dio-unwrit
315	?	00:00:00	upstart-udev-br
466	?	00:00:00	udev
467	?	00:00:00	udev
532	?	00:00:00	kpsmouse
564	?	00:00:00	upstart-socket-
587	?	00:44:57	flush-8:0
613	?	00:00:00	jbd2/sda6-8
614	?	00:00:00	ext4-dio-unwrit
622	?	00:11:50	jbd2/sda10-8
623	?	00:00:00	ext4-dio-unwrit
628	?	00:00:00	jbd2/sda8-8
629	?	00:00:00	ext4-dio-unwrit
632	?	00:02:54	jbd2/sda7-8
633	?	00:00:00	ext4-dio-unwrit
640	?	00:15:17	jbd2/sda9-8
641	?	00:00:00	ext4-dio-unwrit
692	?	00:00:00	rpciod
694	?	00:13:32	rsyslogd
711	?	00:00:00	nfsiod
1049	?	00:00:00	lockd
1050	?	00:00:00	nfsd4
1051	?	00:00:00	nfsd4_callbacks
1052	?	00:13:59	nfsd
1053	?	00:13:55	nfsd
1054	?	00:14:07	nfsd
1055	?	00:14:16	nfsd
1056	?	00:13:59	nfsd
1057	?	00:14:09	nfsd
1058	?	00:13:54	nfsd
1059	?	00:14:01	nfsd
1094	?	00:00:37	ypbind
1301	?	00:00:07	qmgr
2926	?	00:00:00	kauditd
11923	?	00:00:03	tlsmgr
13016	?	00:00:00	apache2
13277	?	00:00:00	sshd
13380	pts/2	00:00:00	ssh
13410	?	00:00:00	apache2
14901	?	00:00:00	apache2
15188	?	00:00:00	apache2
16784	?	00:00:00	apache2
16785	?	00:00:00	apache2

```
17098 ?      00:00:13 kworker/0:2
19688 ?      00:00:06 kworker/0:0
20678 ?      00:00:00 apache2
20789 ?      00:00:00 apache2
24200 pts/1      00:00:25 ping
27610 ?      00:00:00 pickup
28620 ?      00:00:00 apache2
29027 ?      00:00:00 sshd
29188 pts/0      00:00:00 ssh
29264 ?      00:00:00 sshd
29636 ?      00:00:00 sshd
29887 pts/5      00:00:00 ps
```