TC 2.0
Terminal Commands module 2: Terminal commands and your computer
(commands are usually in **bold**)
Topics covered: fsck, pram reset, top, ps, kill, activity monitor, network utility

Repair stuff:
If you are on a mac that does not have super-secret-double-dog-dare-you security on it (like many macs folks will approach you to repair) you can do a simple repair process with no tools, and look like a hero/heroine every time.
Interested?
Read on...
First, turn off the mac completely.
Hold the power key until it all goes dark.
Then restart the computer, holding down the command and s keys together (command-s)
You should see a great deal of text.
When it all settles down, type this:
fsck -yf
and return

What does this do?
fsck stands for file system check (I know, it looks like something else).
the space means "and do something special"
-yf means "don't argue with me, say yes to every questions, and force it if it resists"

After a bit, you should see things settle down.
type "exit"
the computer should start, and if you look closely, you'll see what it repaired flash by the screen.
What?
Imagine you are driving your new Tesla to a party. You get out, the nice valet takes your keys, gives you a little ticket with a number on it, parks your car and puts your keys on a board that says "stall 35".

When you want your car back, you give them your little ticket, they run back, match the ticket with the stall number, and hopefully bring you your car back intact.
On your computer, the board where the keys were stored is your directory.
The keys on the board are your data.
When your computer freezes, or you turn it off suddenly, or it crashes, the car is parked, but there is no key on the board, or the reverse.
File system check counts the cars and the keys and if there are "orphans" it repairs them.
A more serious version of this is "Disk Warrior" a program that actually takes all of the keys, dumps them on the ground, then runs around to every stall, matching a key to a car.
Much more powerful.

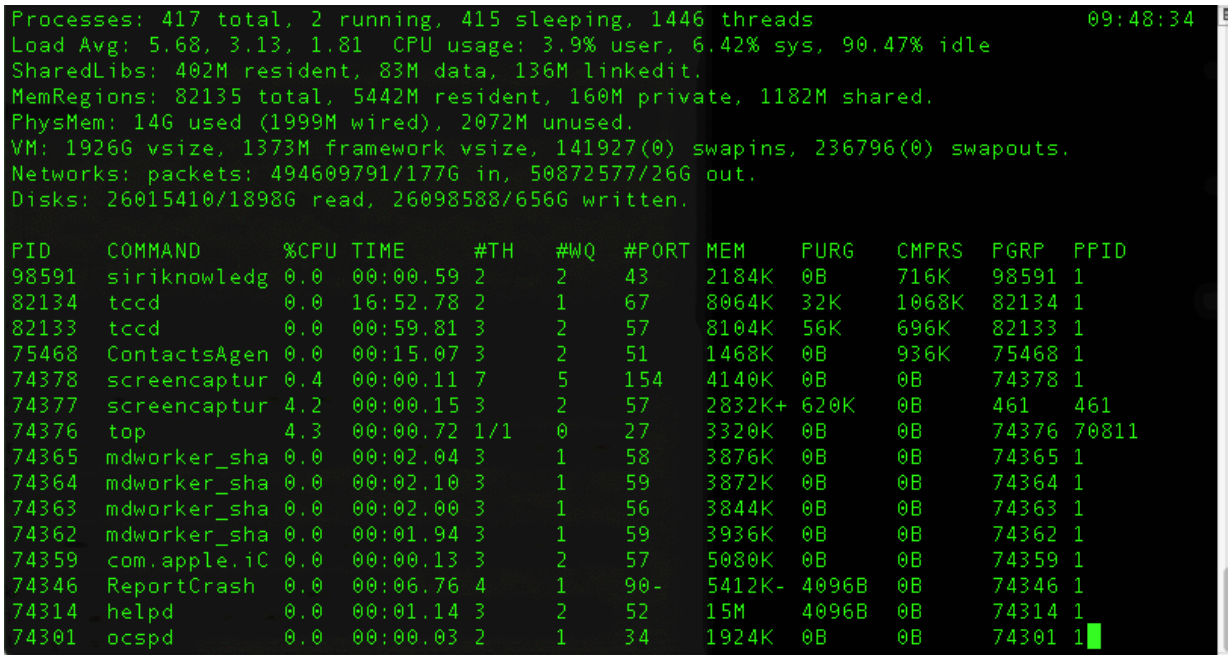
PRAM
Is not just a carriage for carrying babies…
If your mac is still having issues, or you just want to show off, try this:

1. turn off the mac
2. restart, holding the command-option-P-R keys together (you get good at this eventually)
3. hold these until you hear some chimes (not the church across the street)
4. listen until the chimes repeat 3 times
5. release, the computer will start normally

What did I do?
You reset the "permanent random access memory", or pram that holds preferences like time, date and location.
It sometimes solves sticky issues with macs.

Ok, back to terminal stuff:

How do I know how busy my computer is? It seems slow…
Try this:
top



Not only does this look cool, it shows you lots of important stuff.
The top line is about the processes going on. Pay attention to the numbers. Sleeping is good.
There is also a category called “nice”.
No kidding.
Look next at the load averages, there will be one for each “core” of your processor.
Most of you will have at least two of these. At the elab we have servers with 16 cores.
Gamers go nuts over cores…
Skip down to this line:
PhysMem: 14G used (2006M wired), 2082M unused
This is how much of your physical memory is used.
Now look at the line after that:
VM: 1913G vsize, 1373M framework vsize, 141927(0) swapins, 236796(0) swapouts.

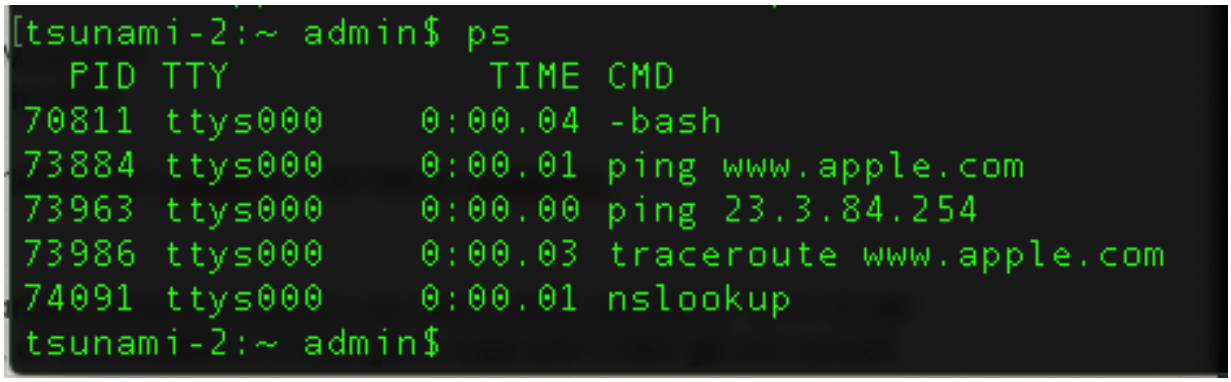
This is really important.
The first line is how much physical RAM (random access memory) you have, likely around 8, 16 or 32 gB.
In my case, it says I’m using 14 gB of RAM, of this 2006M or 2.006 gB is used and 2.082 gB are unused
Look next at the VM, which means “virtual memory”

This is memory created by the computer on the hard drive, using what is known as “swap space”.
This goes way back to when RAM cost an arm and a leg, so programmers devised cool ways to create space to run programs using the space in the hard drive.
Bad news: hard drives used to be spinning platters of metal. Very slow to read and write.
Good news: most hard drives now are SSD or solid state drives. Not quite as fast as RAM, but much bigger.
Something you need to know: if you have less space on your drive (SSD or other) than you have in RAM, your computer will not have enough space to operate, and it will slow to a crawl.
Mac, PC, linux, Unix, no matter what, this will make you crazy.
Solution? Get rid of all of those cat videos.

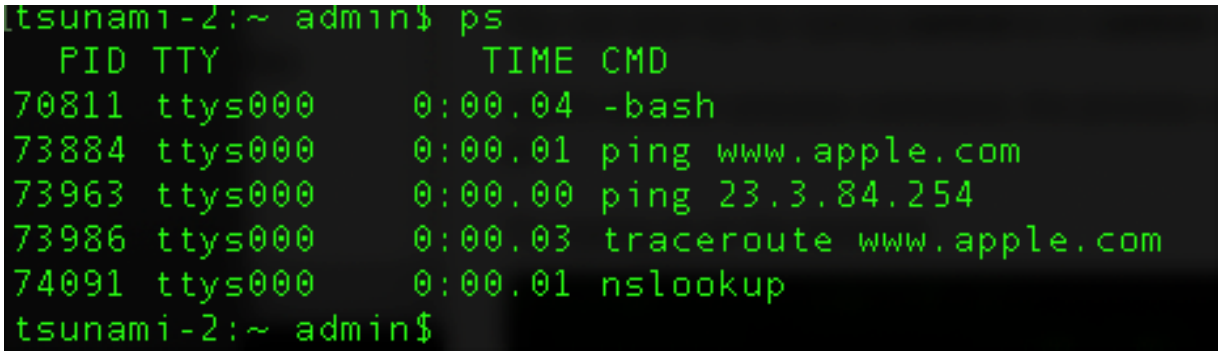
Further down the page you see lines that have numbers (PID) command, %CPU and a bunch of other stuff.
Let’s focus on the first two.
If your computer is slow, look at the %CPU column.
This actually may say something over 100%.
No, your computer is not a magical unicorn powered rainbow machine, it simply means you have more than one core to run processes on, so 200% on a 4 core machine might mean 2 of the 4 cores are being totally used.
You can end top by typing **control-x** or **control-z**

Here’s another process command, the process command:
ps

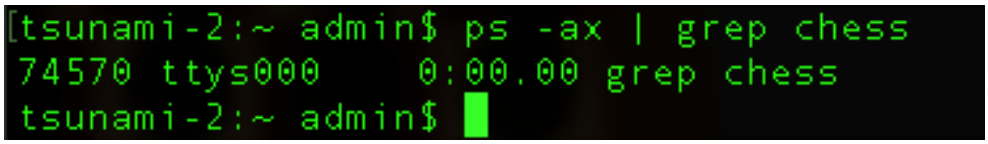
Try typing **ps** at the terminal:



Ok, so what?
It tells me which programs I, admin have running, namely the **ping**, **traceroute** and **nslookup** from last module
Ok, now open the program chess (look in applications, or hit **command-space**)
Repeat:



Same page.
Hmmmm...
Now enter this:
ps -ax
Yikes! lots of stuff showed up!
We only want chess, so we do this:
ps -ax | grep chess



Ok, lots going on here.

1. I asked the computer to show me all of the processes (ps -a) that were executable (ps -ax)
2. I entered a space then this little upright thingy (|) which is right below the delete key on most computers.
3. I used a command called “grep” which means “get regular expression”. I mean, who, who in the world talks like that?
4. then I asked it to search all of that wonderfulness for the process that had the word chess in it

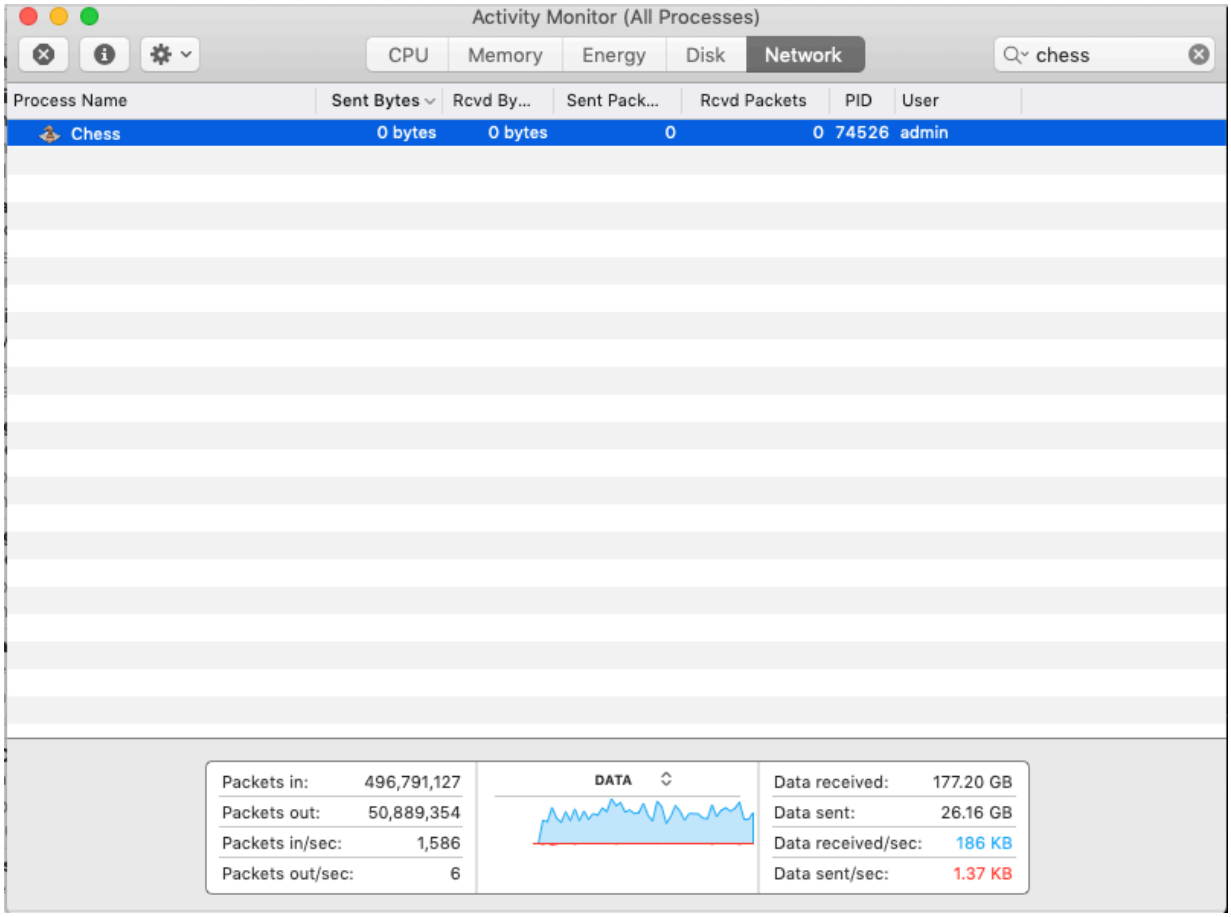
Ok, now what if I have a program I want to kill. Make it go away. Gone forever without a trace.

You want the kill command…
Here's an example:

Find Chess on your mac, either with command-space or some other clever means.
Open it.
Use this command:
ps -ax | grep chess
and find the PID (process id) for chess, in my case it was 74570
watch carefully to the chess window as you enter this command:
kill -9 74570
This should kill chess.
Dead.
Gone.
n.b. (nota bene, "note well" in Latin): you may find that it does not work. Repeat the ps command, if the process number changes, pick another program to kill.

There is another way you can do this:

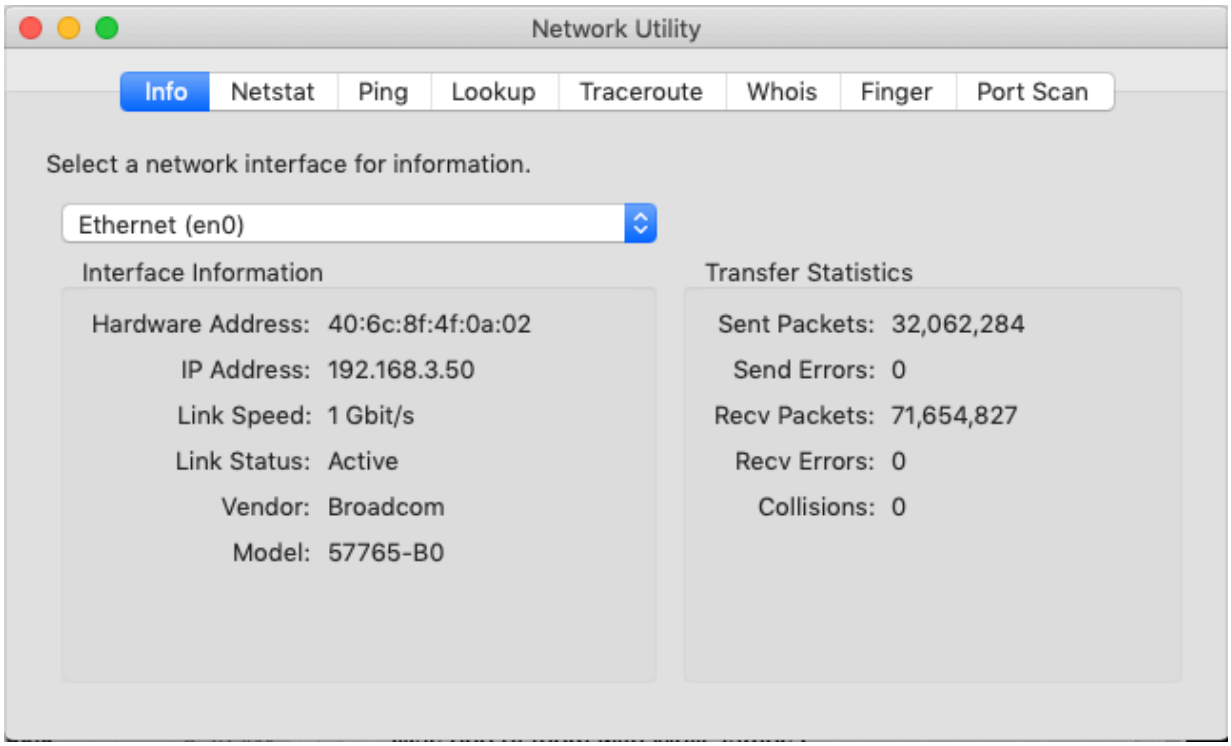
1. Under applications/utilities, find the program called "activity monitor"
2. Type chess in the search window
3. Click on it
4. look for the little X (upper left corner)
5. click on that
6. chess is dead (though it lives in certain nerdy dorms)



While we are here...
Look around at this program.
It shows you:

1. CPU use, just like top did,
2. memory again like top, but also
3. energy (power used if you are on a laptop, this might be useful)
4. Disk (about more than space, it also show activity, useful in detecting malware)
5. Network (useful in detecting if you have spyware or malware, or just how fast your internet connection is)

While you are in utilities, look for a program called “Network Utility”:



Some old favorites like **ping**, **lookup** and **traceroute**, but also several new ones: **info**, **netstat** and **port scan**.

INFO

INFO tells your MAC address (this means Media Access Control address, nothing about macs or pcs) which is an identifier for that specific network hardware (wired or wireless). These are wired into the wireless card on your computer, smart phone or any device on the internet, but can be “spoofed” to look like something else, which is a hacker trick. More on this soon.

Your IP address will likely be in the form of 192.168.x.y if you are on a home network with less than 254 devices attached, or 10.x.y.z if you are on a larger network. You may also see 172.x.y.x sometimes associated with VPN networks, but hardly ever.

These are agreed upon “fake” inside networks, not reachable on the internet. They are like extensions on a large company phone network. You call the switchboard (your router) and the switchboard passes your call to the correct extension. This also works in reverse: when you want to make a call out of the company, your extension tells the switchboard where you want to go, you go there, and the call goes from there. This is called network address translation, or NAT.

Link speed is good to know, but it is only the physical link speed, not the

actual speed.
Vendor is cool, and if you want to get a head start on hacking, look up wireshark and the term OUI.
Enter the first three pairs of numbers/letters in your MAC address and see what comes up in their utility.
Transfer statistics are useful, especially the errors. If you have errors, you have problems: a broken wire, bad connection or weasels living in your computer.

NETSTAT
Netstat means “network statistics”, try it out, using “comprehensive network statistics”, then open a web page and see what happens.

PORTSCAN
Is much more fun.
Try xserve.hpa.edu
You might see this data:
Port Scan has started...

Port Scan has started...

Port Scanning host: 67.53.209.187

Open TCP Port: 21	ftp
Open TCP Port: 22	ssh
Open TCP Port: 25	smtp
Open TCP Port: 53	domain
Open TCP Port: 80	http
Open TCP Port: 88	kerberos
Open TCP Port: 106	3com-tsmux
Open TCP Port: 110	pop3
Open TCP Port: 143	imap
Open TCP Port: 311	asip-webadmin
Open TCP Port: 366	odmr
Open TCP Port: 407	timbuktu
Open TCP Port: 465	urd
Open TCP Port: 548	afpovertcp
Open TCP Port: 587	submission

Open TCP Port: 625 dec_dlm

Imagine for a moment you are a burglar. The first thing you do is “case the joint” or look for open windows or doors.
The “ports” on the physics server are doors that are open for traffic.

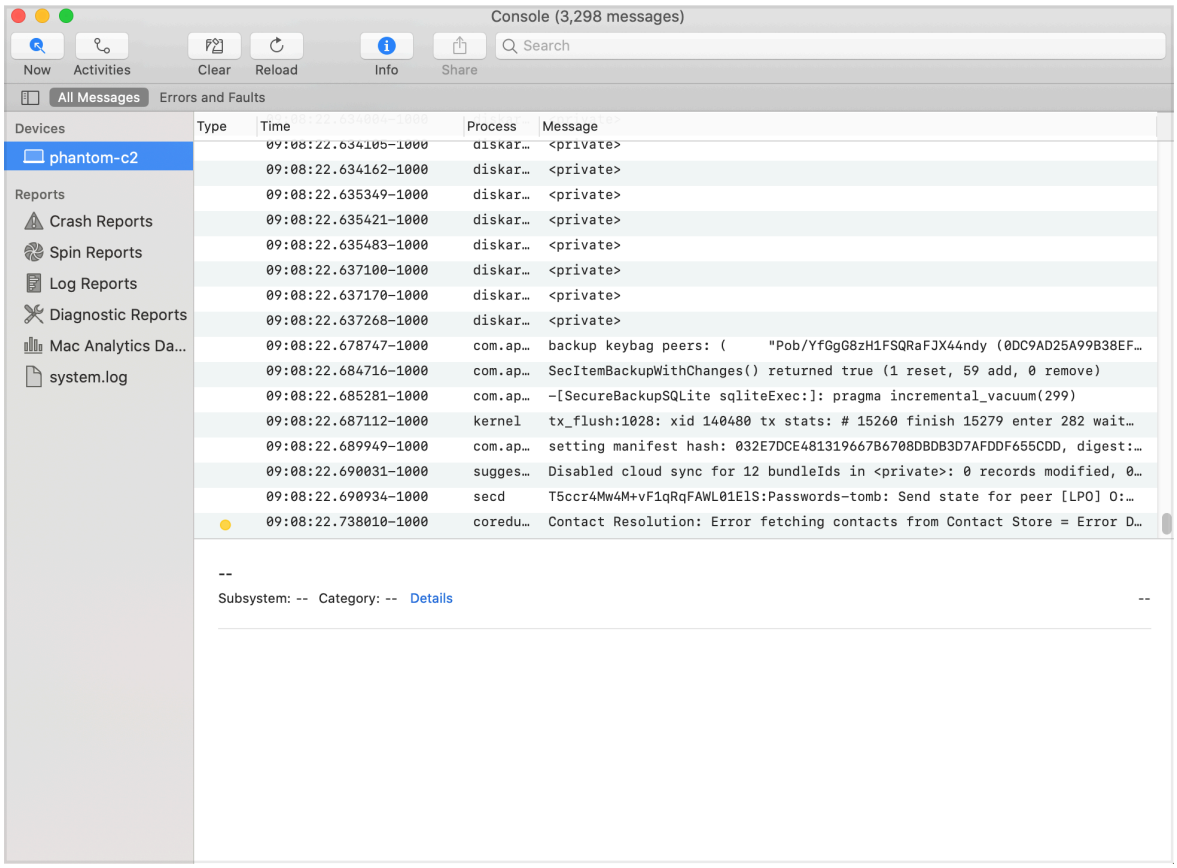
FTP means file transfer protocol, a means of sending or receiving files
ssh is secure shell, a means of communicating in terminal
domain is DNS, the directory translating names into numbers
http is web server, just web pages
kerberos is the name of the three headed dog that guarded the river styx to the underworld with the ferryman Cheron. No kidding. It is a security protocol.
Speaking of protocol, you’ll find that many things end in P, which stands for protocol or “agreed on manners”
POP3 is post office protocol-a way of picking up mail, often taking it from the server
IMAP is the internet mail access protocol, a web based way of picking up mail, leaving stuff on a server
ASIP is web admin for the server
timbuktu is a program that enables remote control, like nomachine or apple remote desktop
afpovertcp is apple file sharing over tcp, the internet protocol

Now try this on a firewalled computer: 67.53.209.186:

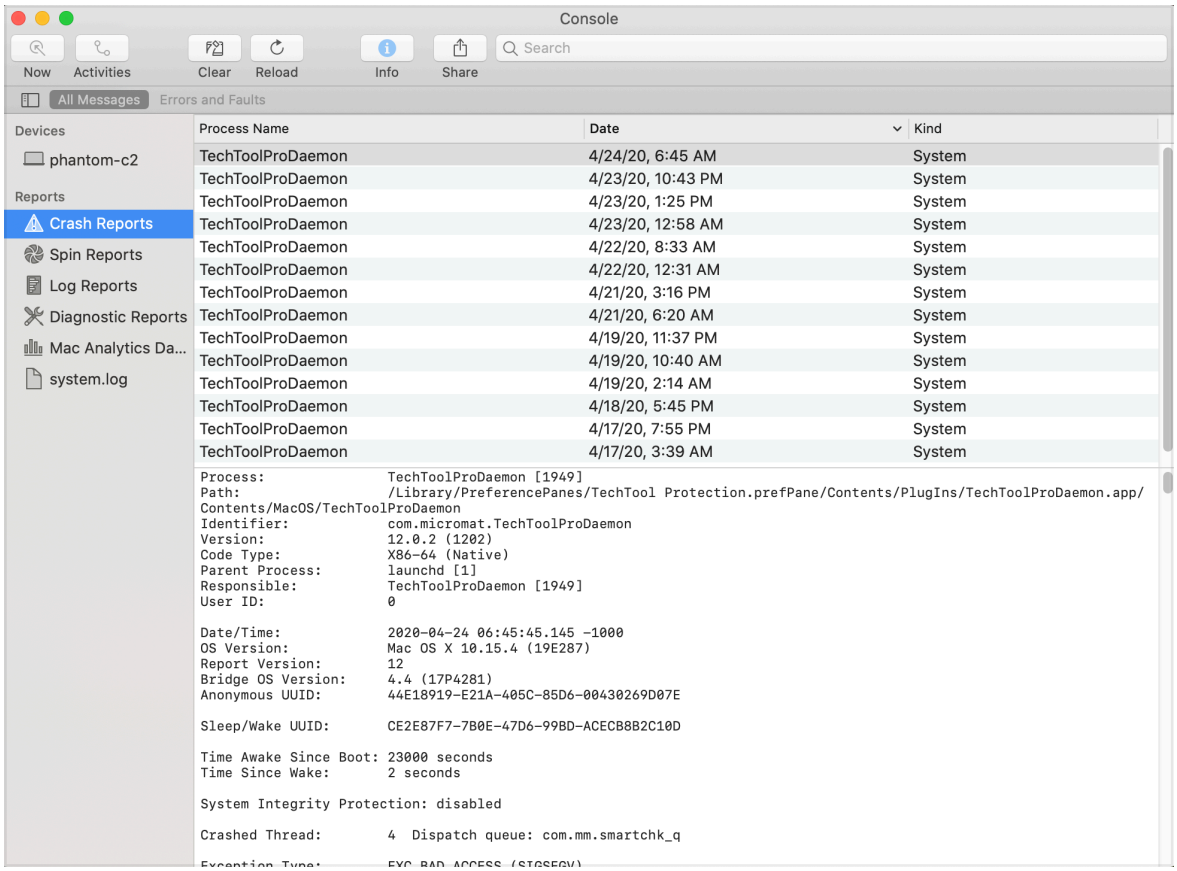
Pretty boring, right?

Your firewall:
Using the site whatsmyip.com find your IP address
Share with a friend, ask them to port scan your router
If nothing is open, this is good

Console:
Also in the utilities folder is a program called console
This page shows how busy your computer is:



this page is more useful, showing why your computer crashed:



————————end of module 2: terminal commands and your computer ————————————————