Sun City Computer Club

Cyber Security SIG

March 18, 2021

Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

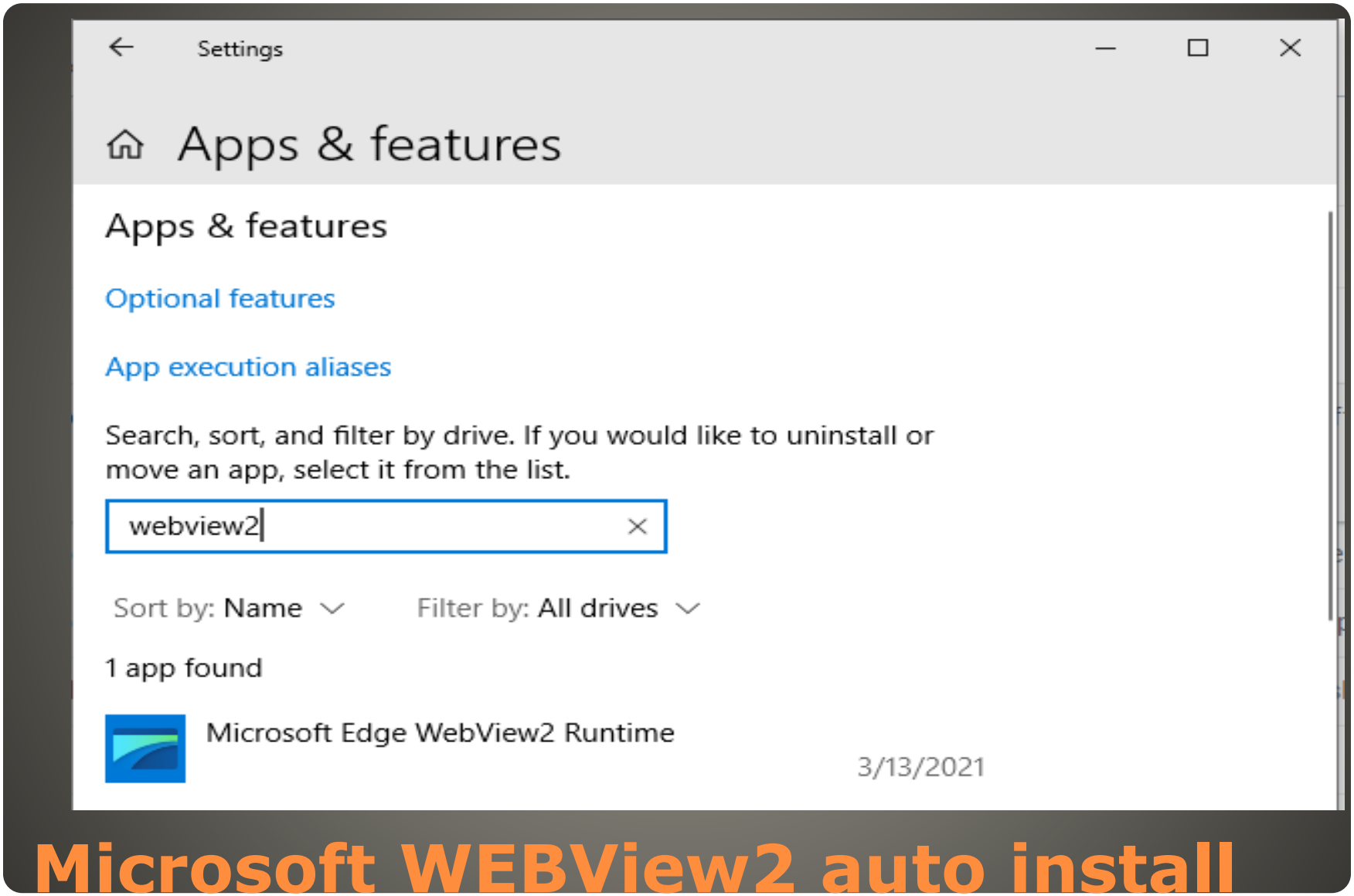
SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

Current Issues

- Microsoft Exchange vulnerability
  - Patch in March
  - Microsoft notified in January
  - Exchange server – free patch ??
  - Patch gives NO indication of patch failure

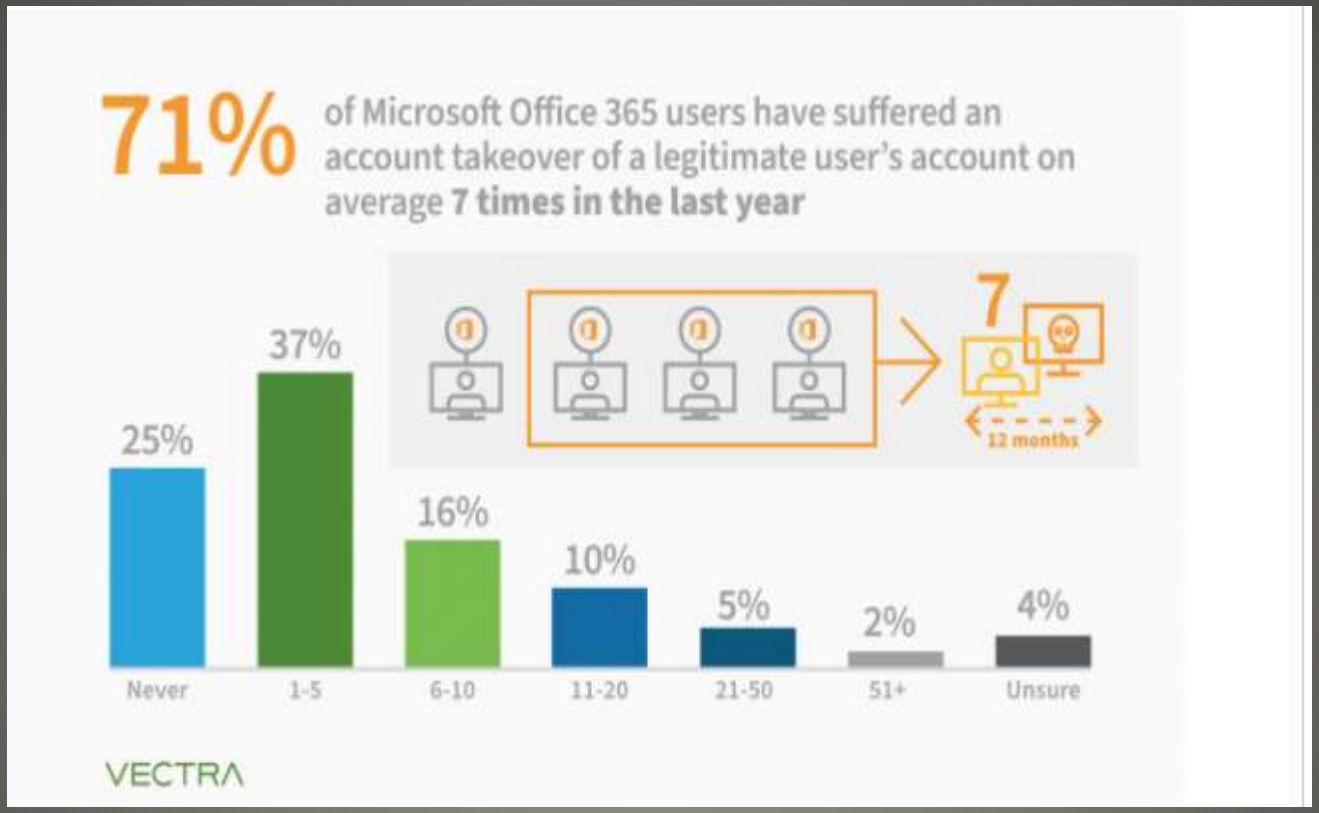
- Doubling every hour
- Ten fold increase March 11 – March 15
- Attack Tsunami
- Thousands of Web shells deployed
  on very protected servers
  and undetected
- Then ransomware DearCry
  Sophisticated & Strong
- Use of “leftover” web shells
- GitHub POC removed
- The doors are open, the map is updating

Microsoft Exchange vulnerabilities



Microsoft WEBView2 auto install

- SolarWinds media coverage
- “Who do you trust?”



Microsoft authentication outages

Blog Archive

- 2021 (9)
  - March (2)
    - iOS update for iPhone iPad, iWatch, and MacOS
    - Microsoft Exchange Servers – SERIOUS vulnerabiliti...
  - February (3)
    - MacOS & Silver Sparrow
    - REALLY SOARING UTILITY BILLS?
    - I have been hacked, now what?
  - January (4)
    - How Hackers hack/attack
    - Messaging Applications
    - Medical devices and iPhone12 and MagSafe
    - MAJOR Android system Update 9-Jan-2021

Cyber Security News Archive

Sun City Texas Community Association File Library Mac User's Group Meeting Notes (sctexas.org)

MAC USER'S GROUP MEETING NOTES

2019

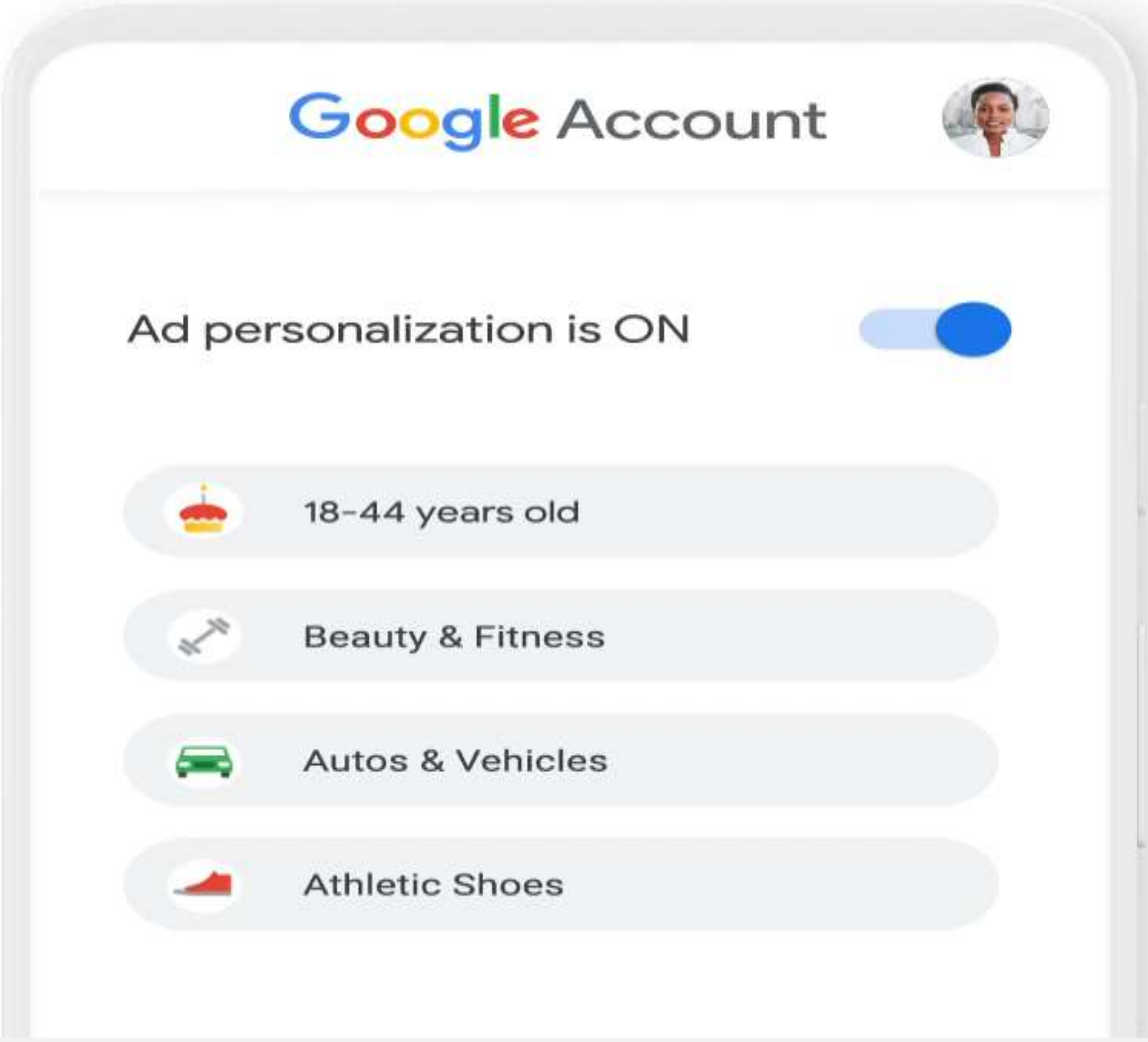
September 2019 – macOS Catalina	View	Download
May 2019 – iCloud Considerations	View	Download
April 2019 – Photo Project Extension Apps	View	Download
March 2019 – Markups	View	Download
February 2019 – Cyber Security	View	Download
January 2019 – Some New Things in Mojave	View	Download

2018

November 2018 – Some Little Extras	View	Download
October 2018 – Numbers, A Powerful Spreadsheet	View	Download

MAC Users Group (MUG)

- Microsoft Exchange
- SolarWinds
- DNS logs
- Browser extensions
  Terms of Service
- 50 years? Creeper Reaper
- Apple's Bluetooth tracking *Find My*
- WeLeakedInfo[.]com
- Bank sites overwhelmed due to stimulus
- Chrome 0-days fixed
  less resources used
  Spectre POC
  project 0
- Most major browsers, extensions, add-ons updated


Google Account
Ad personalization is ON
18-44 years old
Beauty & Fitness
Autos & Vehicles
Athletic Shoes

Malwarebytes Browser Guard

Size 22.8 MB **Version** 2.2.21

Description

The fastest and safest web browsing experience.

Permissions

- Read your browsing history
- Manage your downloads

Site access

Allow this extension to read and change all your data on websites you visit

On all sites

☐ Allow in InPrivate

If you select this option, your browser history may still be recorded. Edge can't prevent the extension from saving your browser history, even in InPrivate mode.

☐ Allow access to file URLs

Source Added by a third-party

Remove

- Tesla, Cloudflare, others Verkada camera hack

Current Issues

signing in to your MyPanera account.

Reset My Password

Can't click the button? Copy the link below into your browser:
https://delivery.panerabread.com/forgotPassword?utm_medium=email&utm_

[redacted]

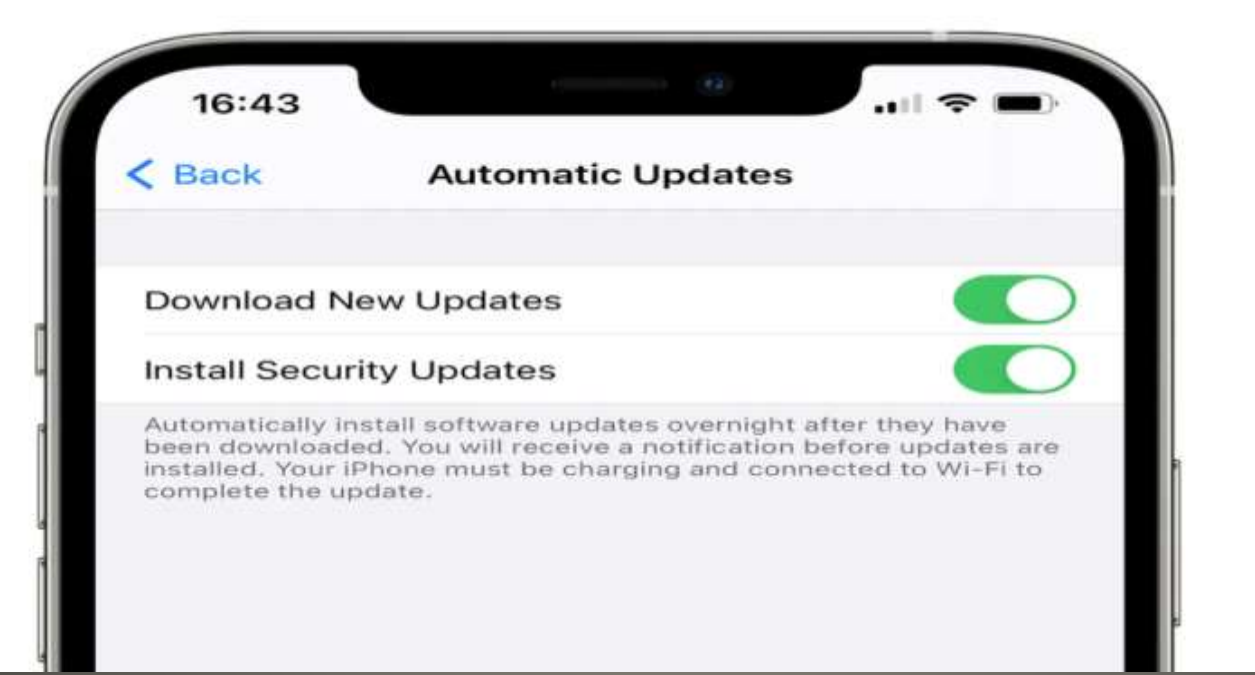
You'll receive an email with instructions on how to reset your password.

If you need help, please contact our Customer Care team.

Current Issues

- Apple Watch fall thru ice
- Top 3 Russian cybercrime forums hacked
- Got 1099-G ?
- Wells Fargo “strengthen your password”
  PassPhrase
  SMS warning
- Chicago coronavirus hotline – random resident
- McGirt vs. Oklahoma
- Emotet -> Trickbot, Qbot, Formbook, Glupteba, Ramnit,
- FBI & CISA Alert Trickbot
- Linux malware “RedXOR”
- Microsoft 365 authentication down yet again
- Facetime Group calls

- $69.3M jpg nonfungible token
- 15 year old Linux kernel lib iSCSI kernel
- Separation of iOS security patching?

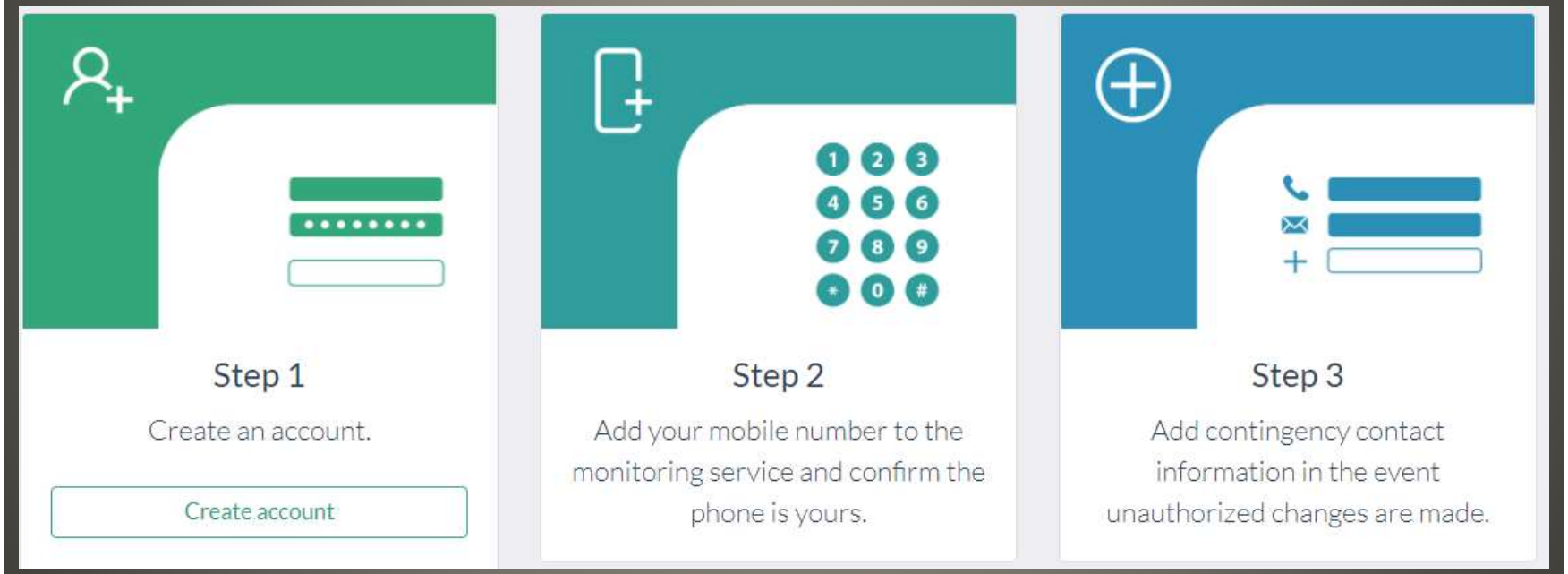


Current Issues

Current Issues

- Intelligence agencies PDF sanitization
  Your PDF sanitization
  Your document sanitization
  track changes metadata previous versions
- Molson Coors production
- UK Home Office & National Crime Agency
  UK resident's browsing History
  EU granted temp adequacy till July 1, 2021
- Spectre POC from Google M1 ?
- DoD supply chain study from congress
- Deep Fake AI "sing with the stars"
- Facetime group 31 random
- Windows 10 printer emergency patch

- SMS mass messaging & marketing
- Letter of Authorization
- SMS authorization for SMS



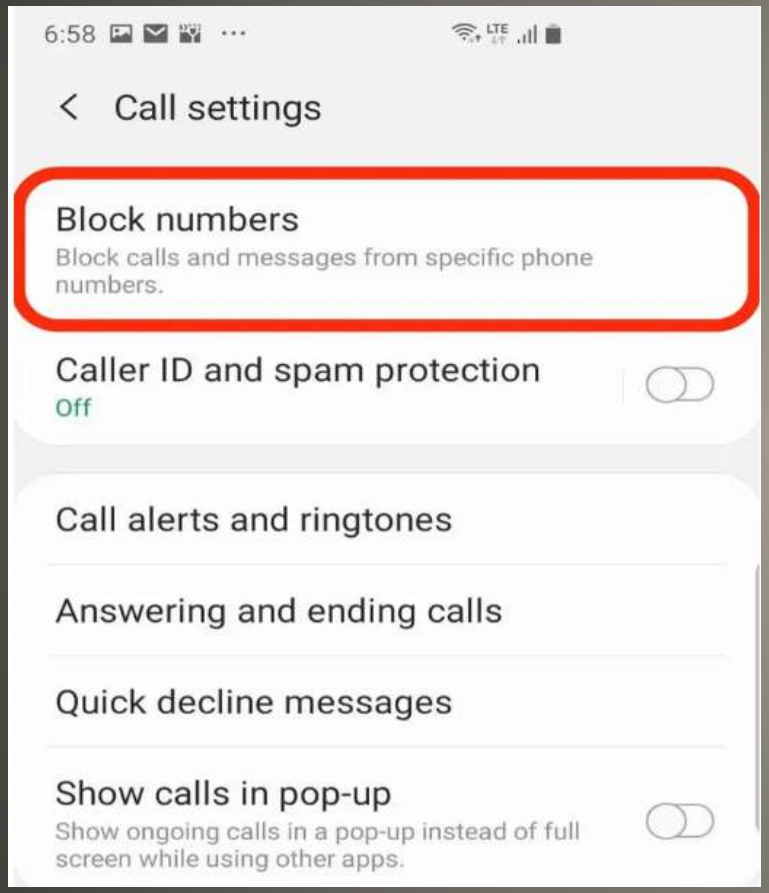
Sakari

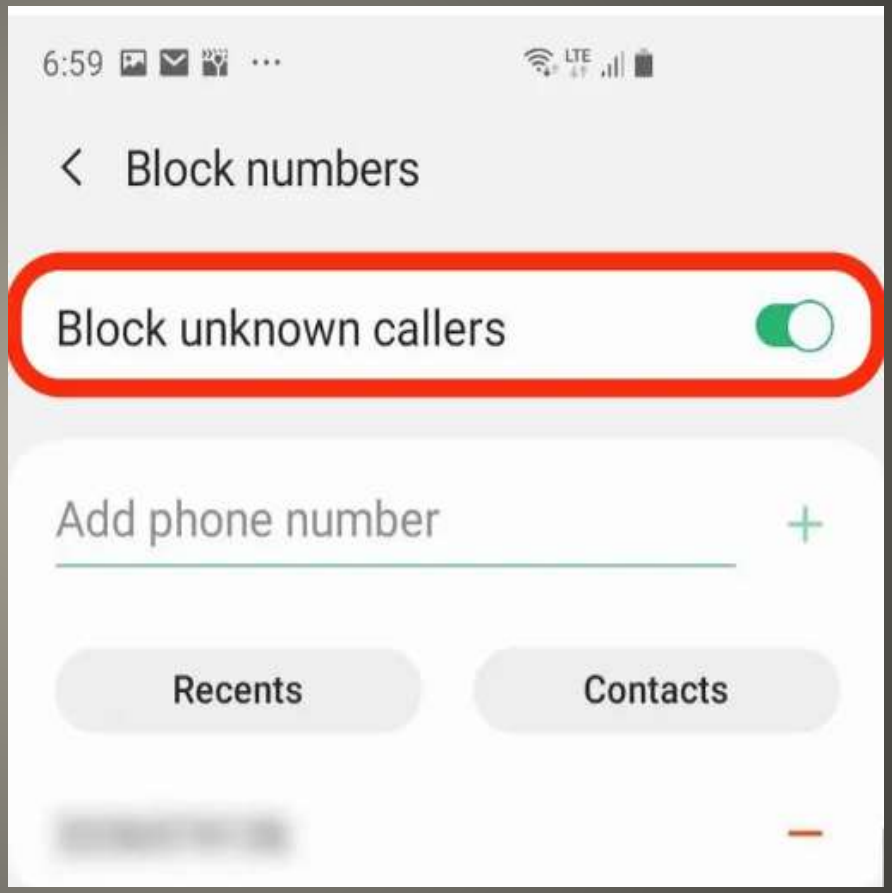
- iPhone

  Settings > Phone > Silence Unknown Callers

Robocalls

- Android





Robocalls

Google Pixel

Major Carriers

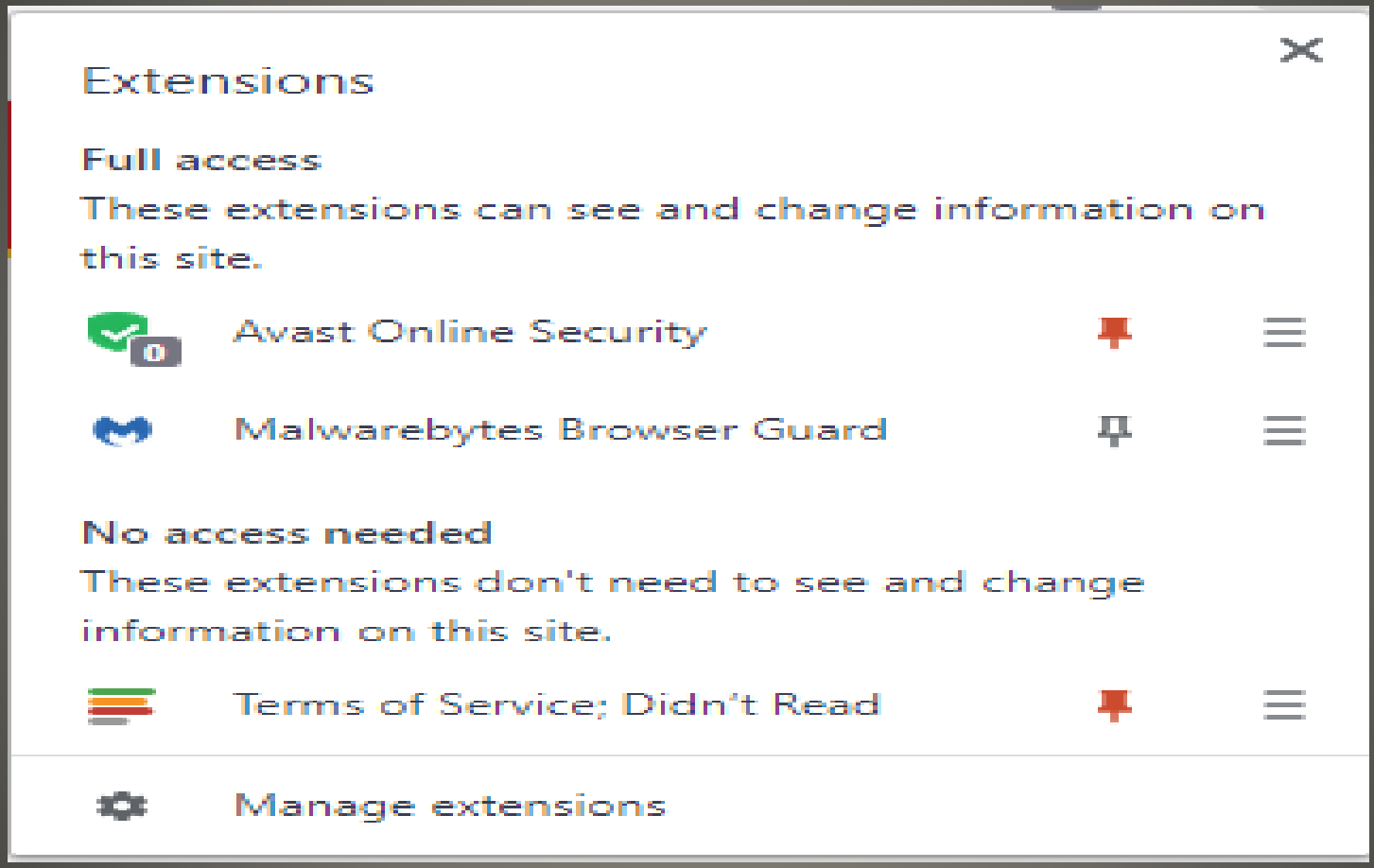
- STIR/SHAKEN TRACED Act
- AT&T
  Check or Manage Voicemail & Features
  Call Protect
- T-Mobile
  SCAM ID
    Dial #ONI# (#664#) + call button
  Scam Block
    Dial #ONB# (#662#) + call button

Major Carriers

- Verizon
  - Call Filter select phone models
  - Call Filter Plus $2.99/mo.
    - Call Filter App > subscribe
    - Verizon account page
    - My Verizon App
- Suddenlink SPAM ROBO

Third Party Apps

- Nomorobo
- Niya
- Mr. Number
- RoboKiller
- YouMail
- ??
- *Consumer Beware*



Browser Extensions

Lay's Potato Chips: Lay's Crispy Subtitles

Embed Video

▸ Save for $5 ▸ Download FREE with PRO membership

Tweet

BEST **Top 6 this week**

In their newest campaign, Lays Potato Chips have released a plug in for Google Chrome that detects the sounds of crunching chips and automatically turns subtitles on for the YouTube video you are watching. Happiness Saigon, an FCB alliance, knew that people love to snack while they're watching their favourite Youtubers, but when you're crunching and munching it can be hard to hear the audio. And Lays is the crispiest chip of all. To solve this problem, and make the video watching experience better for everyone, Crispy Subtitles was the answer. The team trained an AI on 178 hours of crispy chip crunch sounds gathered from around the world, to create a one-of-a-kind plugin which is able to detect and activate subtitles from the second it hears a crunch, so viewers can snack without missing a single thing. This revolution in snacking is available for free on the Google Chrome store globally.

Category	Confectionery & snacks
URL	https://chrome.google.com/webstore/detail/crisp subtitles-from- lay/kokpckgbhcmeobdddflajfcpmmfhkekn
Client	Pepsico
Agency	Happiness Saigon
Production	Bliss Innovative Maker Studio
Country	Vietnam
Uploaded	5 March, 2021

Browser Extensions


NT SNACK & BEVERAGE VENDING
041 778 7756
89254
Doritos
SMITHS
WARNING
Do not use endoscopy equipment to steal chocolate from this vending machine.
Theft is a crime and next time the Police will be notified.
041 77877 56
www.ntsnackbevvending.com.au
Starlight Supporter
Accepts Bills:
$5, $10, $20.

Apple

- Find My
  Safety Alerts AirTags 3rd party devices
- Randomize MAC serial numbers
- Useful Mac Utilities
- Amphetamine

Welcome to Amphetamine

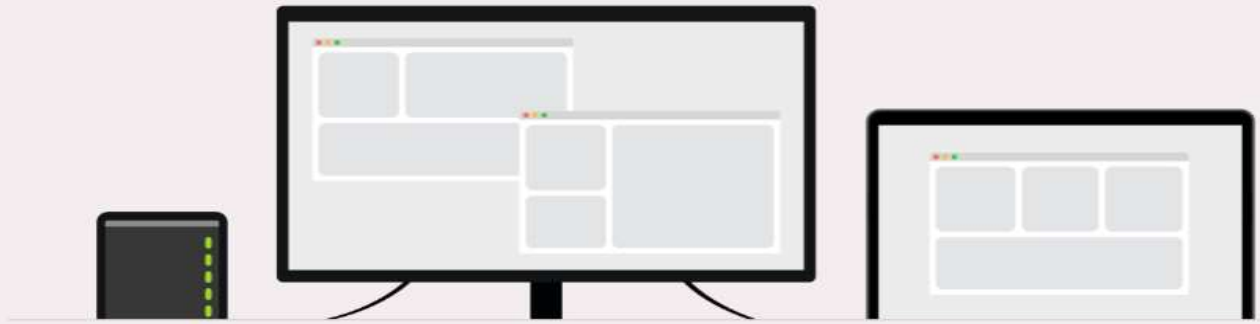
Created with ♥ by William Gustafson

Amphetamine is a super-awesome, powerful, and flexible keep-awake utility for macOS.
Even with all of its features and options, Amphetamine remains incredibly easy to use.

It only takes a few short steps to set up Amphetamine. Click Next to get started.

☐ Don't show this window again

Next



What does Amphetamine do?

Amphetamine keeps your Mac awake. And its displays. And its drives.

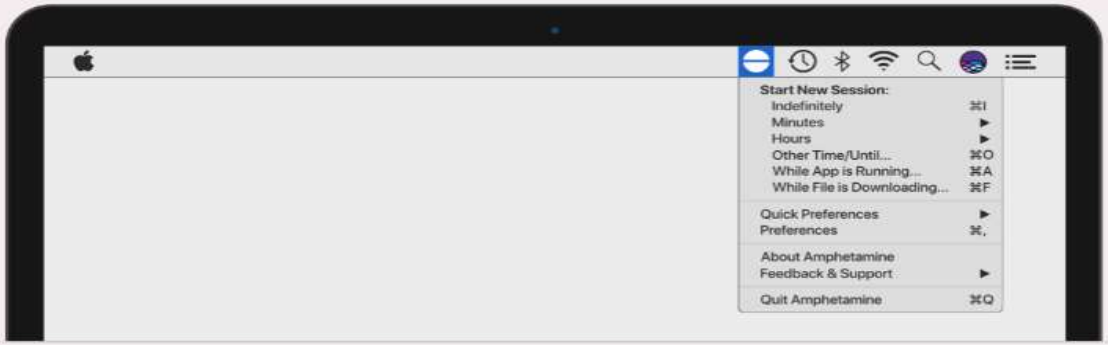
When Amphetamine is keeping your Mac awake it's called a "session." To start a session, click on Amphetamine in the menu bar and select a session duration. Alternatively, right/control click to start a session using the Default Duration. Change the Default Duration in Preferences → Sessions.

If you have a MacBook, and want to keep it awake while its display is closed this is now possible to achieve with Amphetamine. It is highly recommended you install Amphetamine Enhancer as a fail-safe, however.

Click Here to Learn More About Amphetamine Enhancer

Don't show this window again

Previous Next



Where is Amphetamine?

Amphetamine lives in the menu bar at the top right corner of your screen.

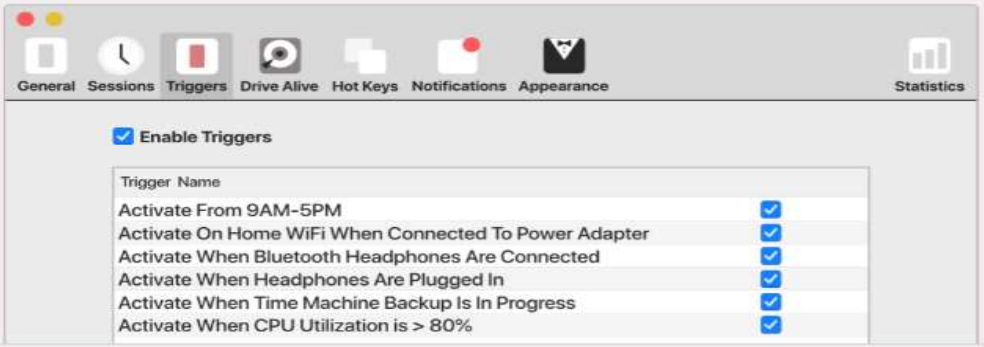
By default, clicking on Amphetamine in the menu bar will show Amphetamine's menu. Right clicking (or control clicking) will start or stop a keep-awake session. You can switch this behavior if you want.

Amphetamine is highly customizable. You can change all kinds of things like the menu bar image, when notifications should appear, and what sounds to play in Amphetamine's Preferences.

Click Here to Locate Amphetamine

Don't show this window again

Previous Next



What else does Amphetamine do?

Amphetamine can do a lot more than you think.

Triggers automate keeping your Mac awake based on things like its Wi-Fi connection, battery level, USB and Bluetooth device connections, time of the day, running applications, IP address, and much more. Visit Amphetamine's Preferences to set up your first Trigger, or click the button below to learn more.

Drive Alive keeps the drives connected to your Mac awake by periodically writing a tiny amount of data to each drive. Visit Amphetamine's Preferences to set up Drive Alive.

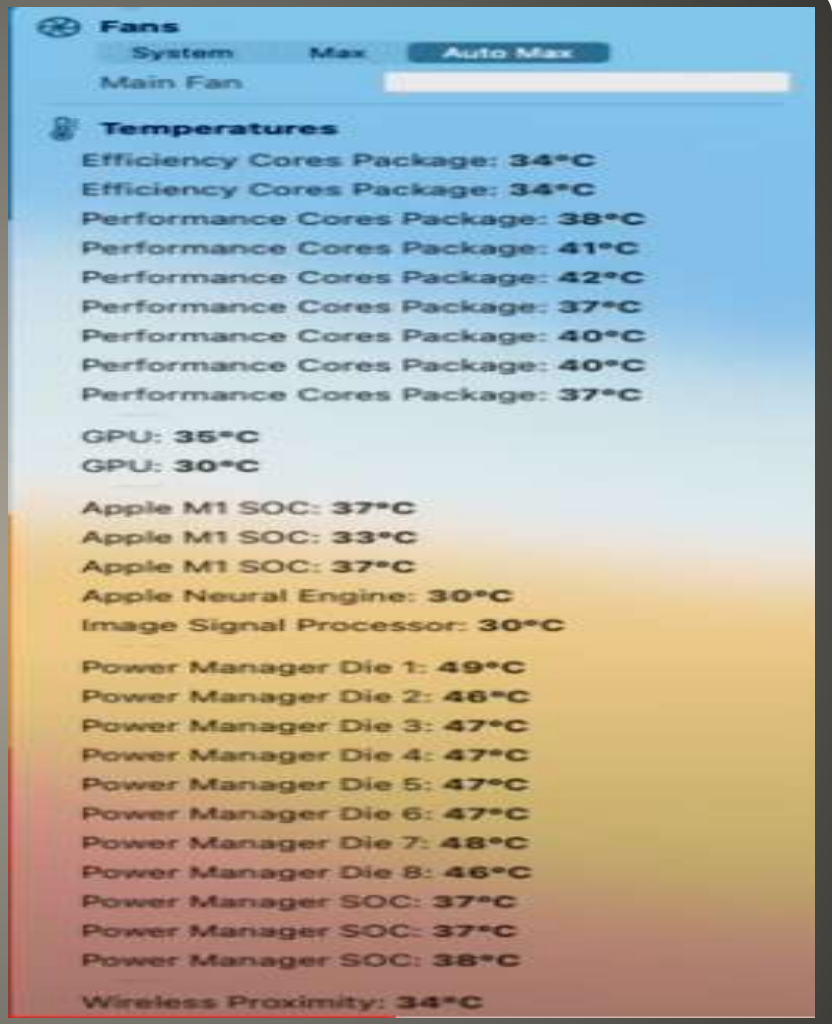
Click Here to Learn More About Triggers

Don't show this window again

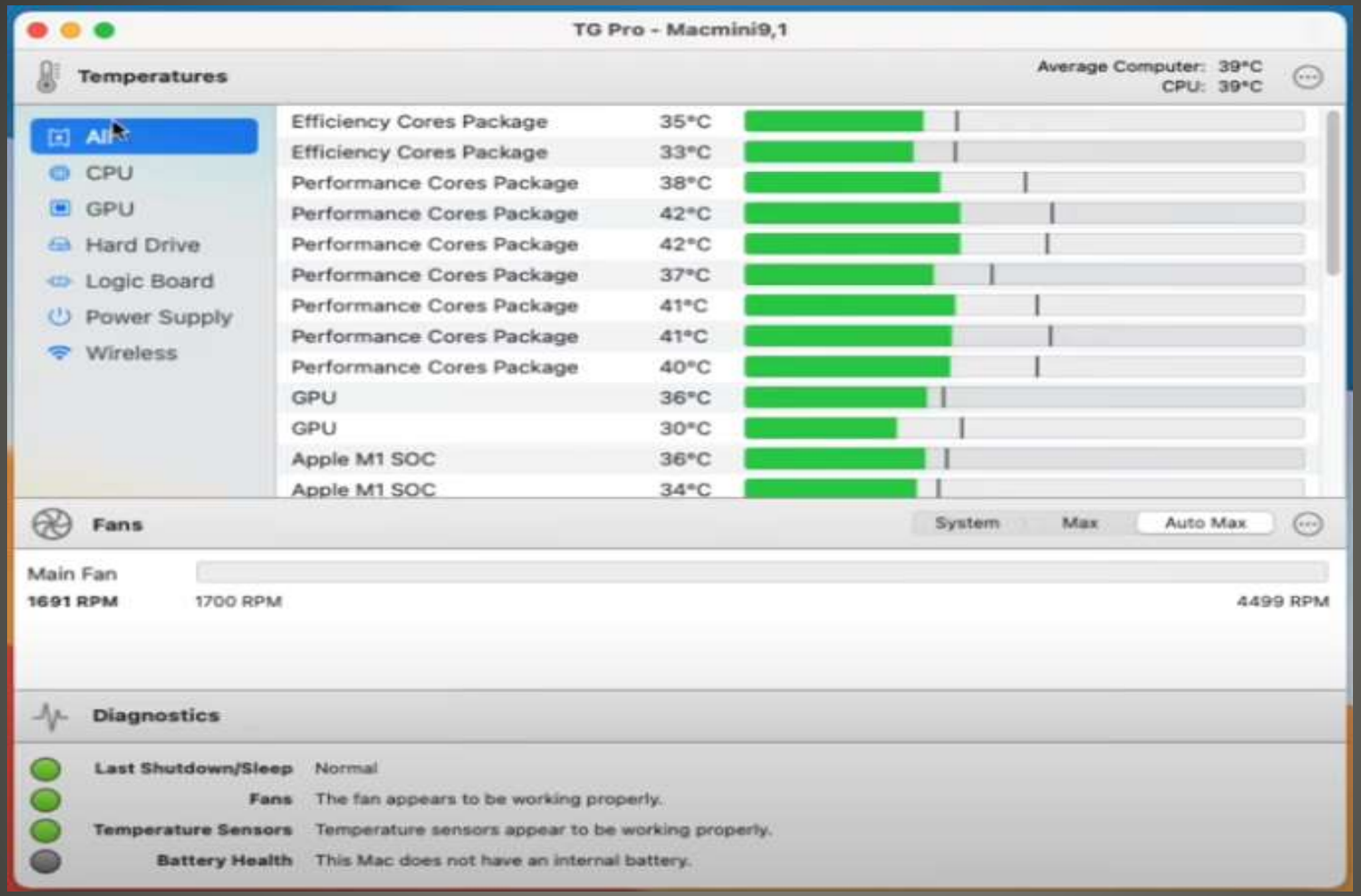
Previous Next

Your favorite MAC app?

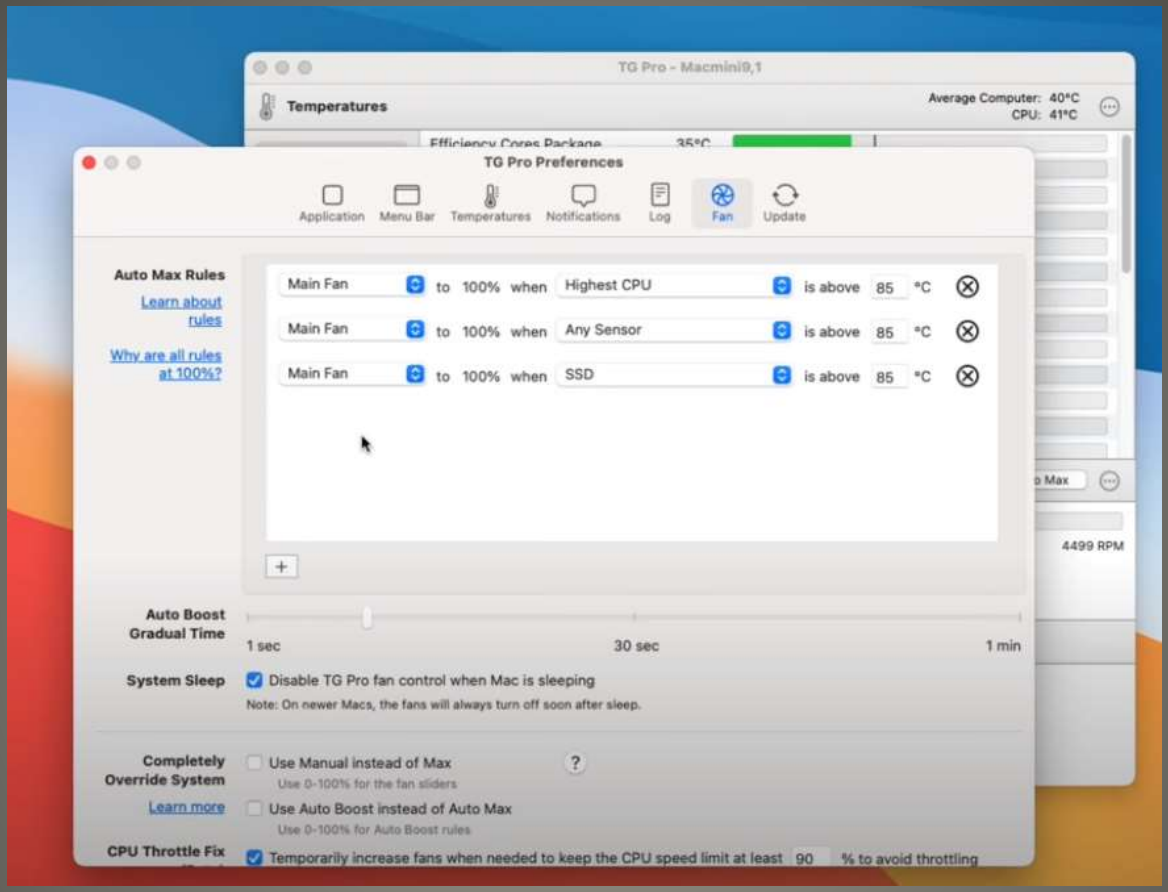
- Rendering on laptop
- Notarized by Apple



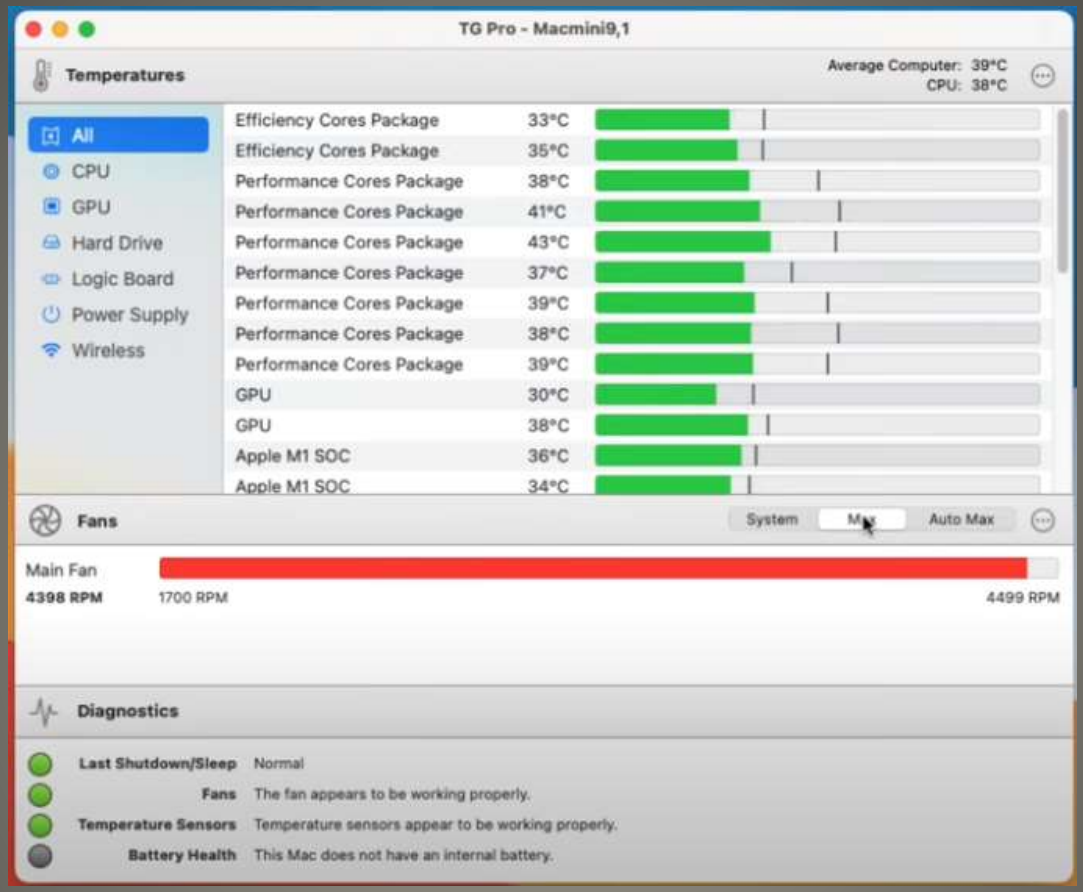
TG Pro Fan Speed & Temperature


TG Pro - Macmini9,1
Temperatures
Average Computer: 39°C
CPU: 39°C
All
CPU
GPU
Hard Drive
Logic Board
Power Supply
Wireless
Efficiency Cores Package 35°C
Efficiency Cores Package 33°C
Performance Cores Package 38°C
Performance Cores Package 42°C
Performance Cores Package 42°C
Performance Cores Package 37°C
Performance Cores Package 41°C
Performance Cores Package 41°C
Performance Cores Package 40°C
GPU 36°C
GPU 30°C
Apple M1 SOC 36°C
Apple M1 SOC 34°C
Fans
System
Max
Auto Max
Main Fan
1691 RPM
1700 RPM
4499 RPM
Diagnostics
Last Shutdown/Sleep Normal
Fans The fan appears to be working properly.
Temperature Sensors Temperature sensors appear to be working properly.
Battery Health This Mac does not have an internal battery.

TG Pro



TG Pro Fan control

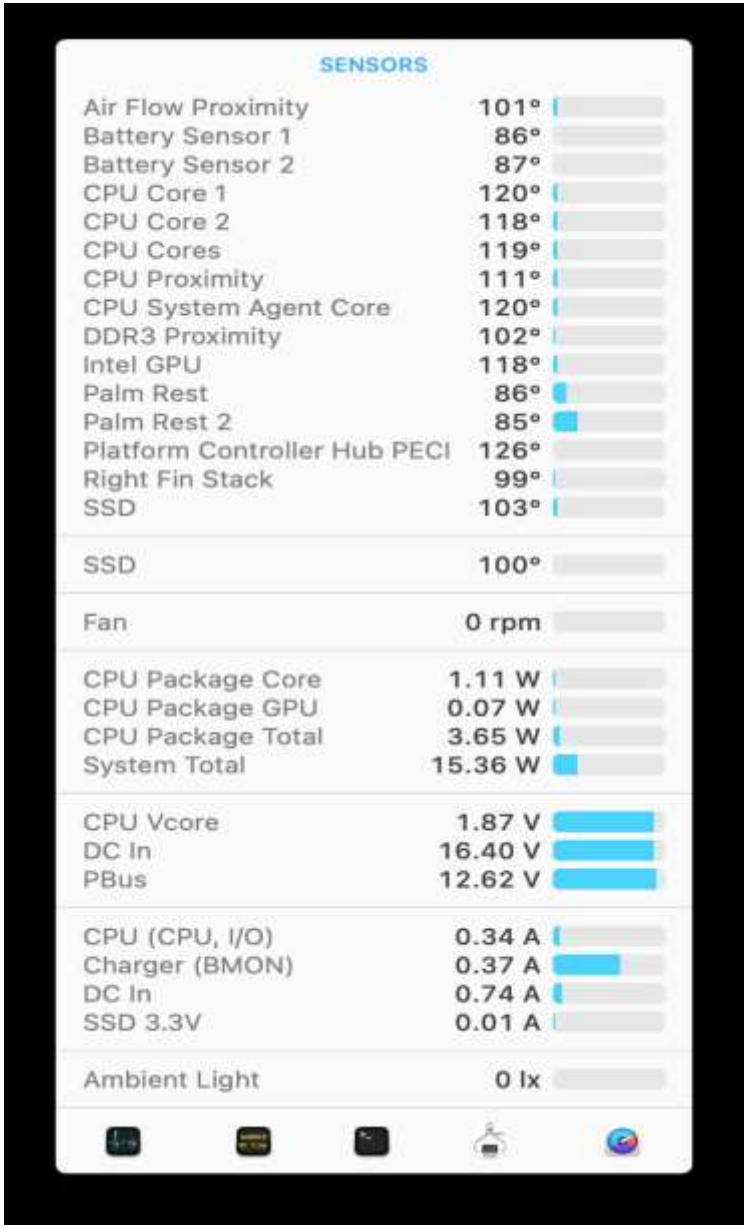

TG Pro - Macmini9,1
Temperatures
Average Computer: 39°C
CPU: 38°C
All
CPU
GPU
Hard Drive
Logic Board
Power Supply
Wireless
Efficiency Cores Package 33°C
Efficiency Cores Package 35°C
Performance Cores Package 38°C
Performance Cores Package 41°C
Performance Cores Package 43°C
Performance Cores Package 37°C
Performance Cores Package 39°C
Performance Cores Package 38°C
Performance Cores Package 39°C
GPU 30°C
GPU 38°C
Apple M1 SOC 36°C
Apple M1 SOC 34°C
Fans
System
Auto Max
Main Fan
4398 RPM
1700 RPM
4499 RPM
Diagnostics
Last Shutdown/Sleep Normal
Fans The fan appears to be working properly.
Temperature Sensors Temperature sensors appear to be working properly.
Battery Health This Mac does not have an internal battery.

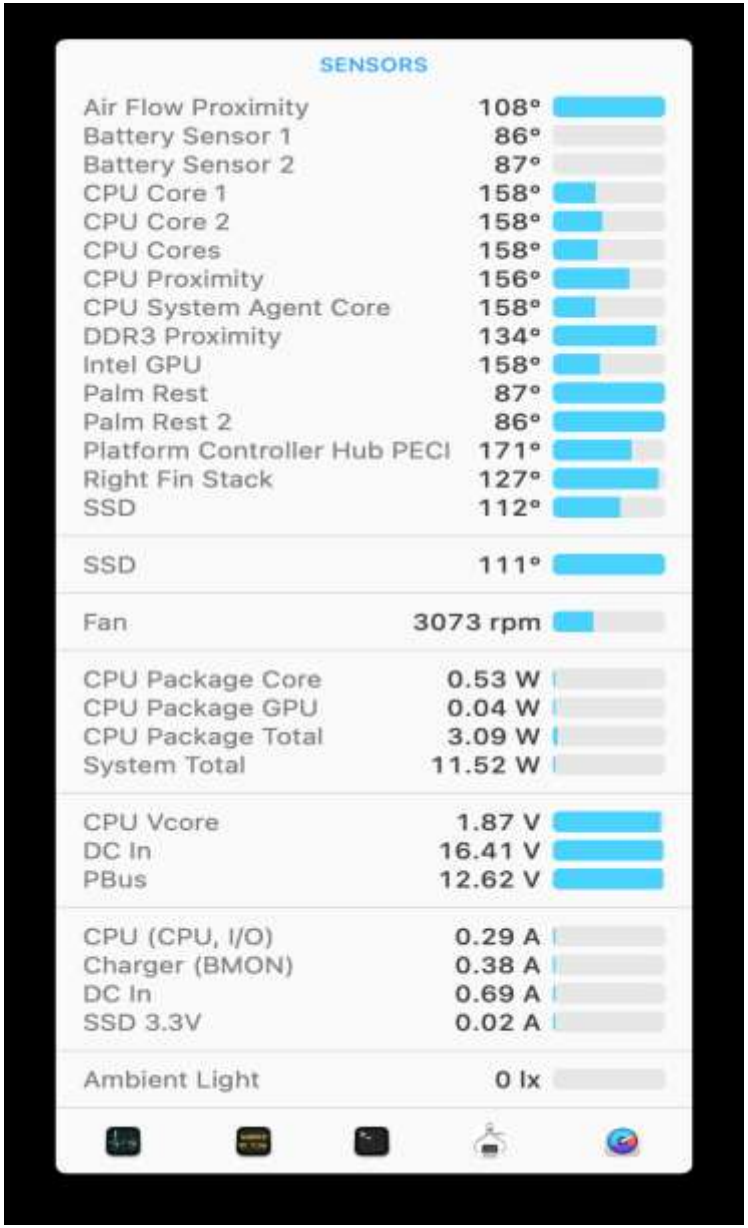
TG Pro

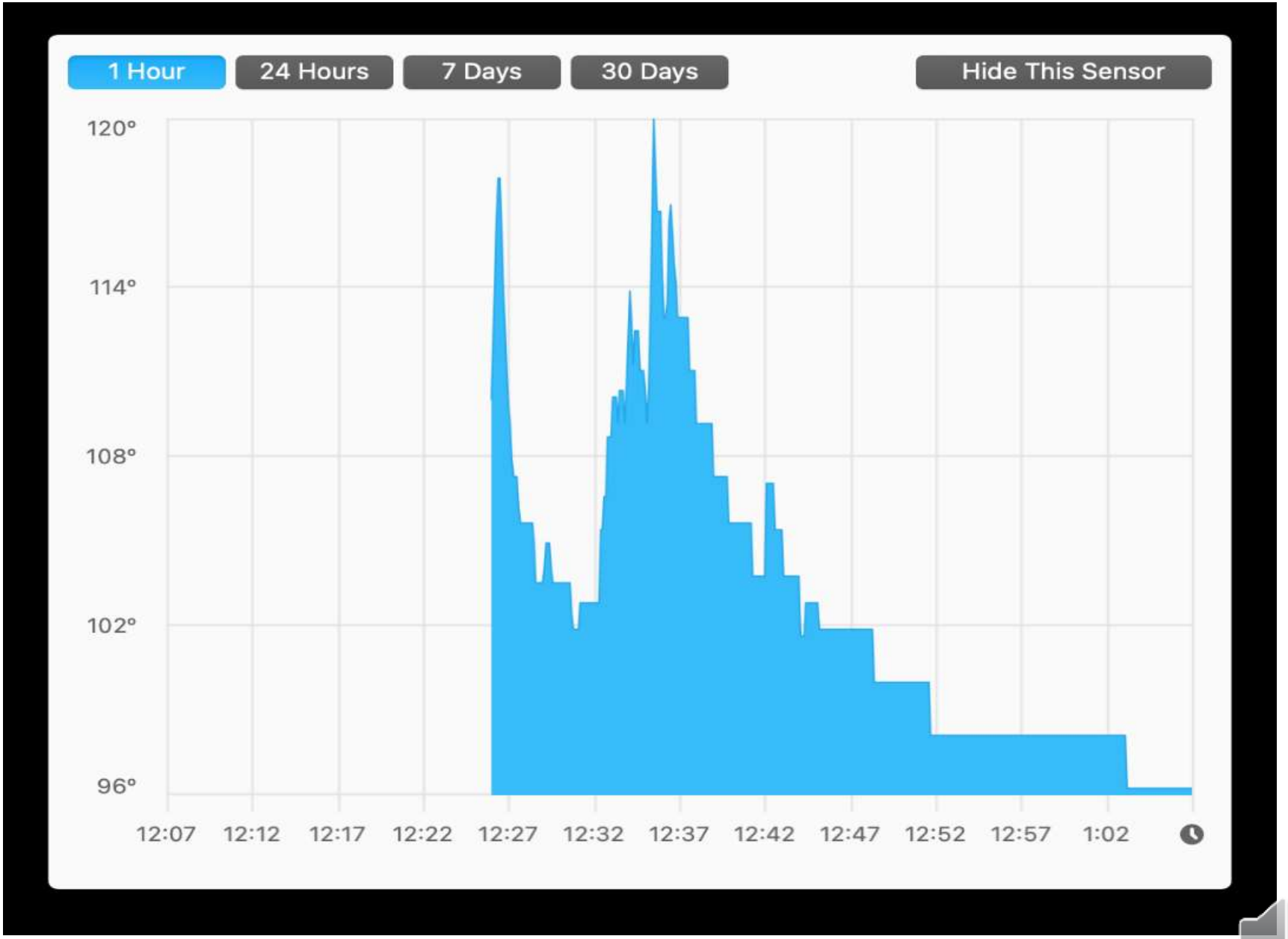

Hardware turned fan off
This model of Mac will safely turn the fan off when the CPU is running at low capacity.
Once the system turns it back on, fan control in the app will be available.
OK
Do not show this message again

- Fast + Small > Hot
- Roku
- MacBook Lap combustible table top
- First degree burn 118 Fahrenheit

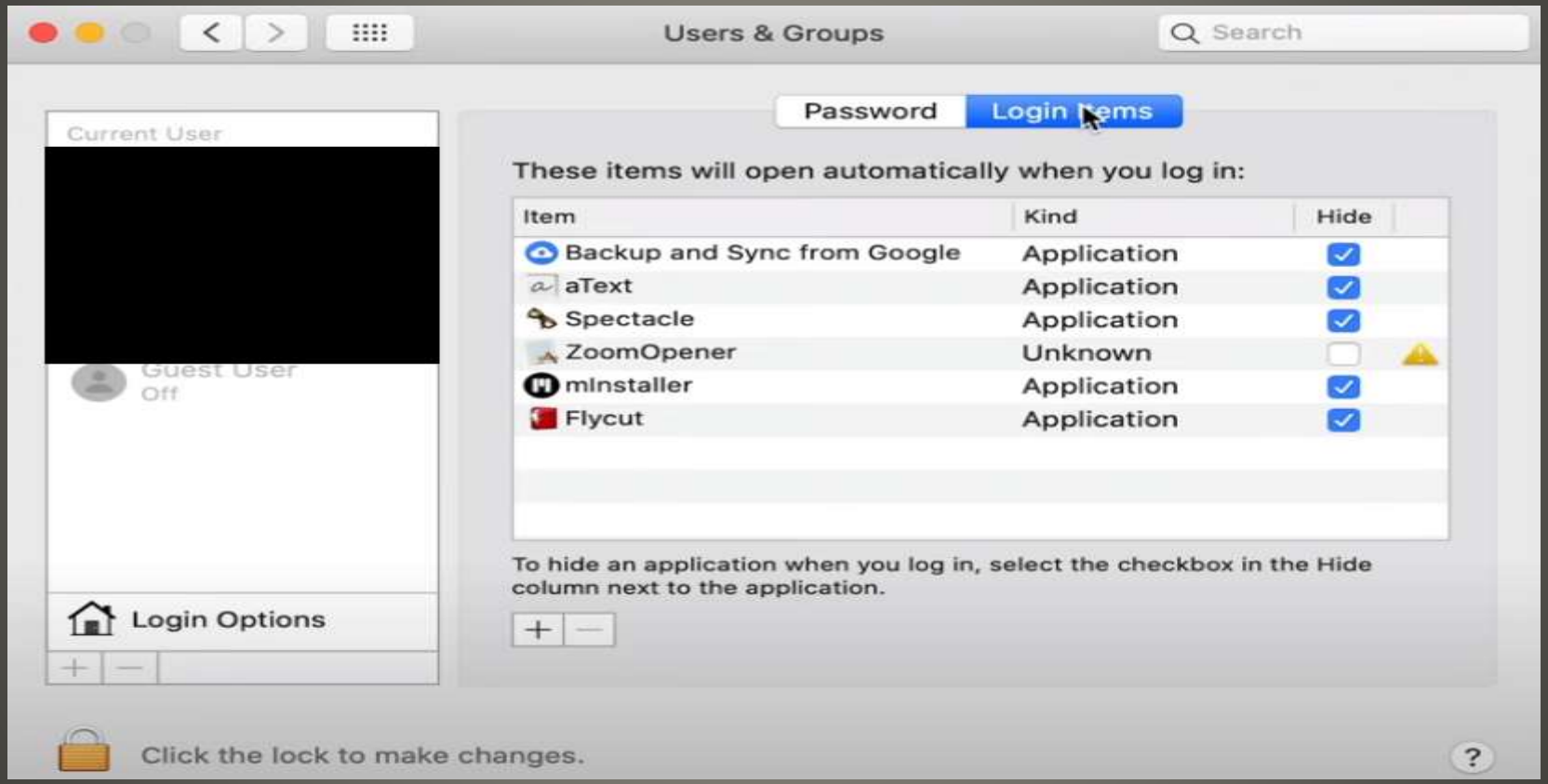
Global Warming


SENSORS
Air Flow Proximity 101°
Battery Sensor 1 86°
Battery Sensor 2 87°
CPU Core 1 120°
CPU Core 2 118°
CPU Cores 119°
CPU Proximity 111°
CPU System Agent Core 120°
DDR3 Proximity 102°
Intel GPU 118°
Palm Rest 86°
Palm Rest 2 85°
Platform Controller Hub PECI 126°
Right Fin Stack 99°
SSD 103°
SSD 100°
Fan 0 rpm
CPU Package Core 1.11 W
CPU Package GPU 0.07 W
CPU Package Total 3.65 W
System Total 15.36 W
CPU Vcore 1.87 V
DC In 16.40 V
PBus 12.62 V
CPU (CPU, I/O) 0.34 A
Charger (BMON) 0.37 A
DC In 0.74 A
SSD 3.3V 0.01 A
Ambient Light 0 lx


SENSORS
Air Flow Proximity 108°
Battery Sensor 1 86°
Battery Sensor 2 87°
CPU Core 1 158°
CPU Core 2 158°
CPU Cores 158°
CPU Proximity 156°
CPU System Agent Core 158°
DDR3 Proximity 134°
Intel GPU 158°
Palm Rest 87°
Palm Rest 2 86°
Platform Controller Hub PECI 171°
Right Fin Stack 127°
SSD 112°
SSD 111°
Fan 3073 rpm
CPU Package Core 0.53 W
CPU Package GPU 0.04 W
CPU Package Total 3.09 W
System Total 11.52 W
CPU Vcore 1.87 V
DC In 16.41 V
PBus 12.62 V
CPU (CPU, I/O) 0.29 A
Charger (BMON) 0.38 A
DC In 0.69 A
SSD 3.3V 0.02 A
Ambient Light 0 lx

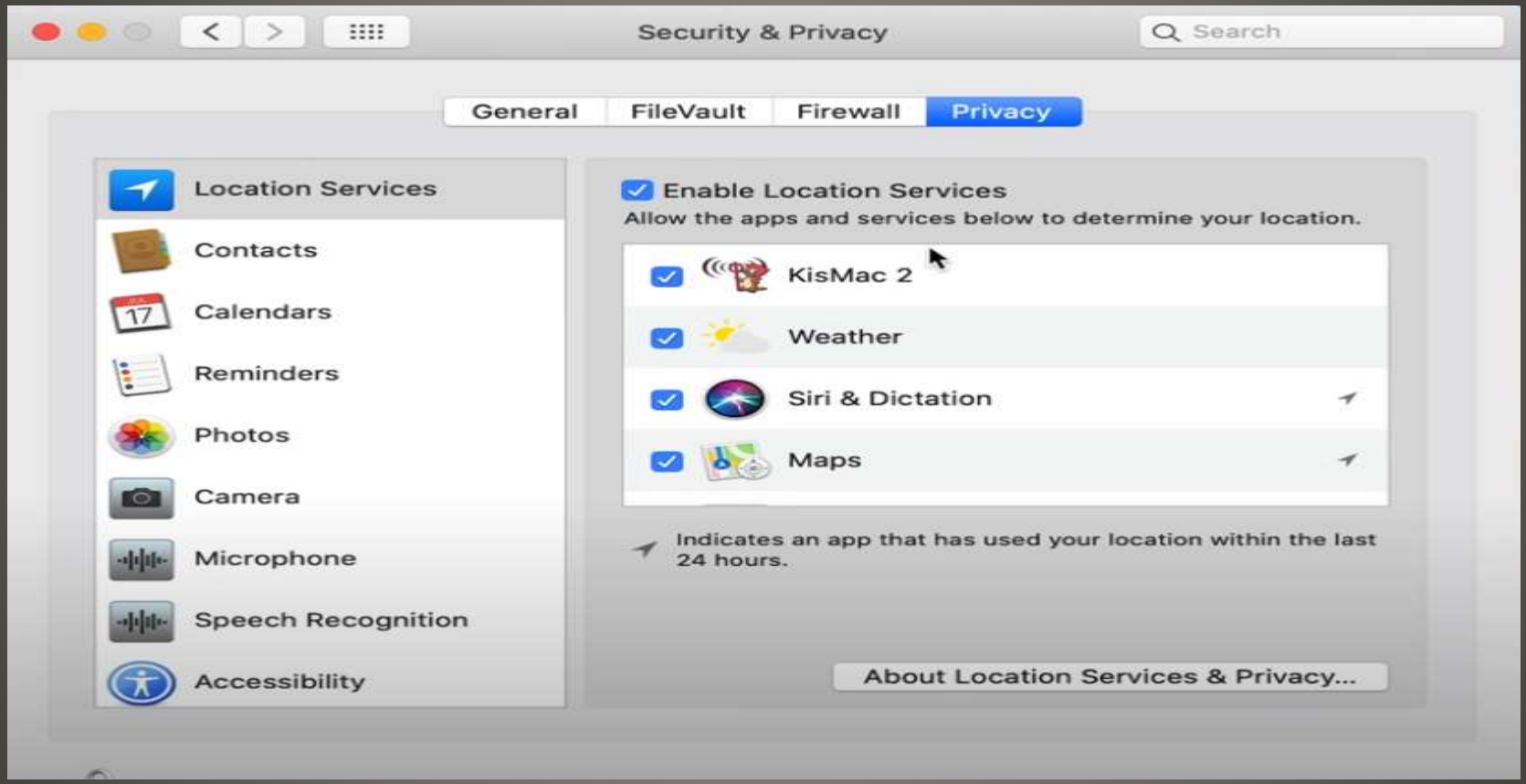

1 Hour
24 Hours
7 Days
30 Days
Hide This Sensor
120°
114°
108°
102°
96°
12:07
12:12
12:17
12:22
12:27
12:32
12:37
12:42
12:47
12:52
12:57
1:02

- Users & Groups -> Login Items



Unnecessary Login Items

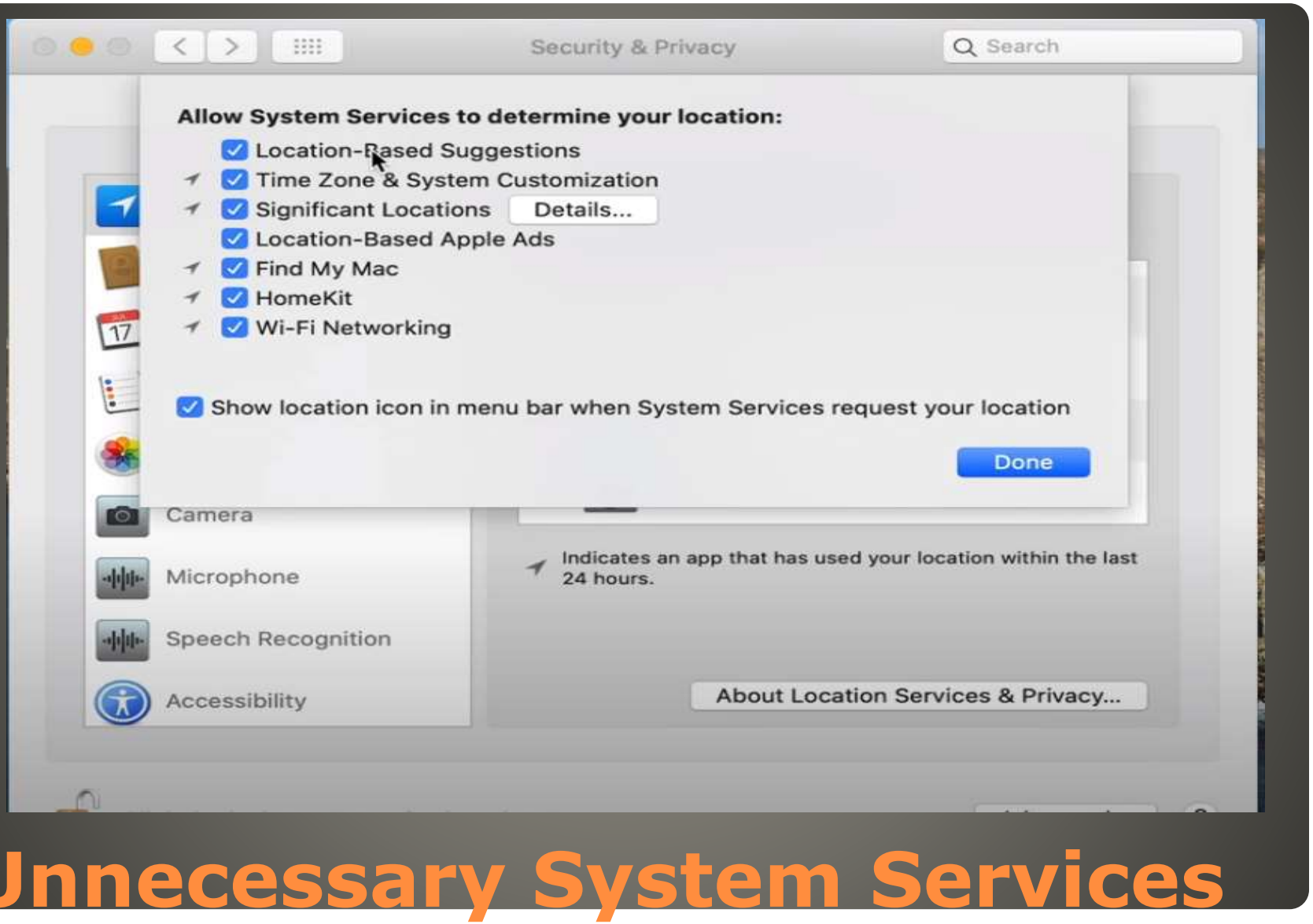
- Security & Privacy -> Location Services



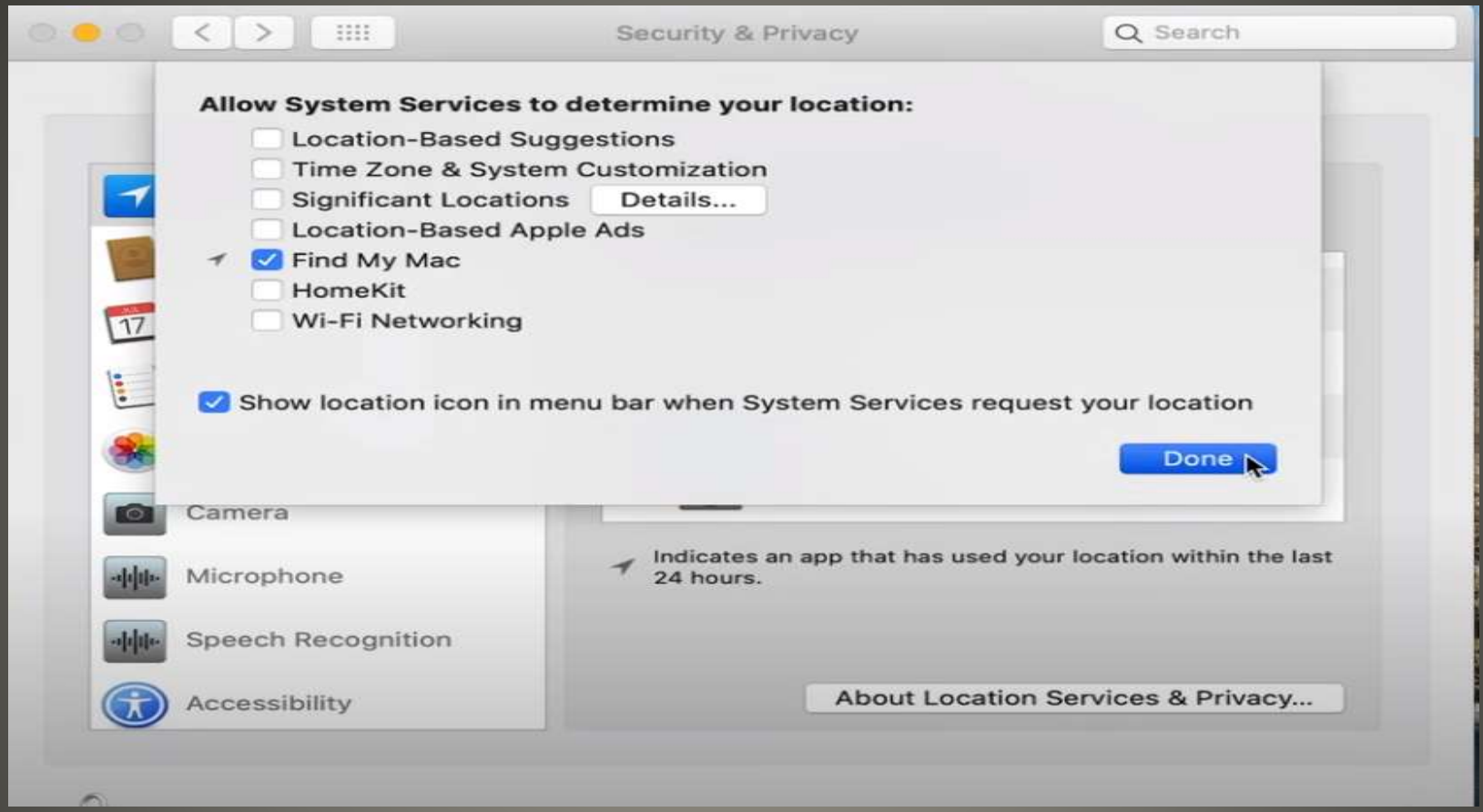
Unnecessary Location Services

- Security & Privacy

Unnecessary System Services



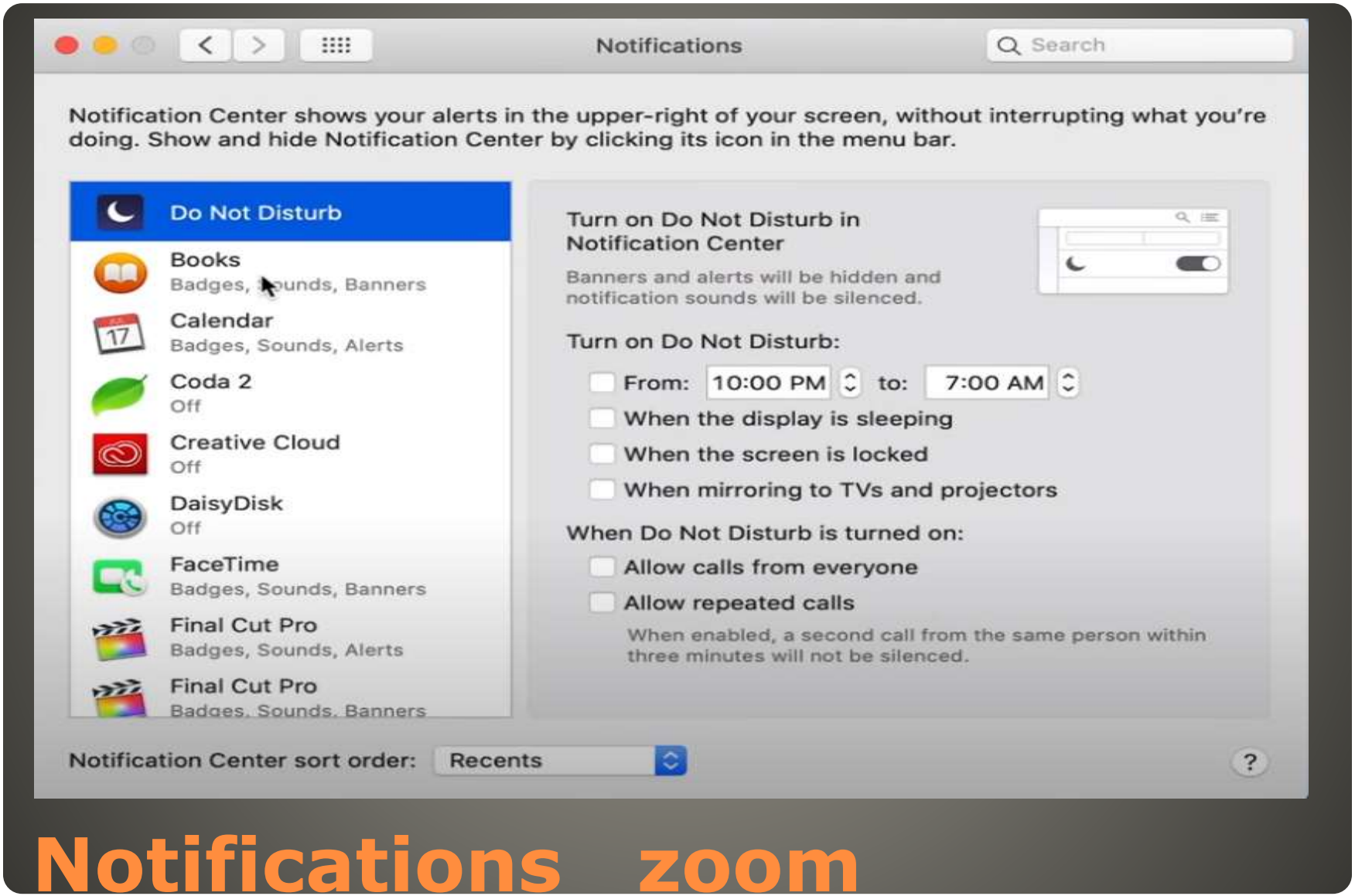
Unnecessary System Services



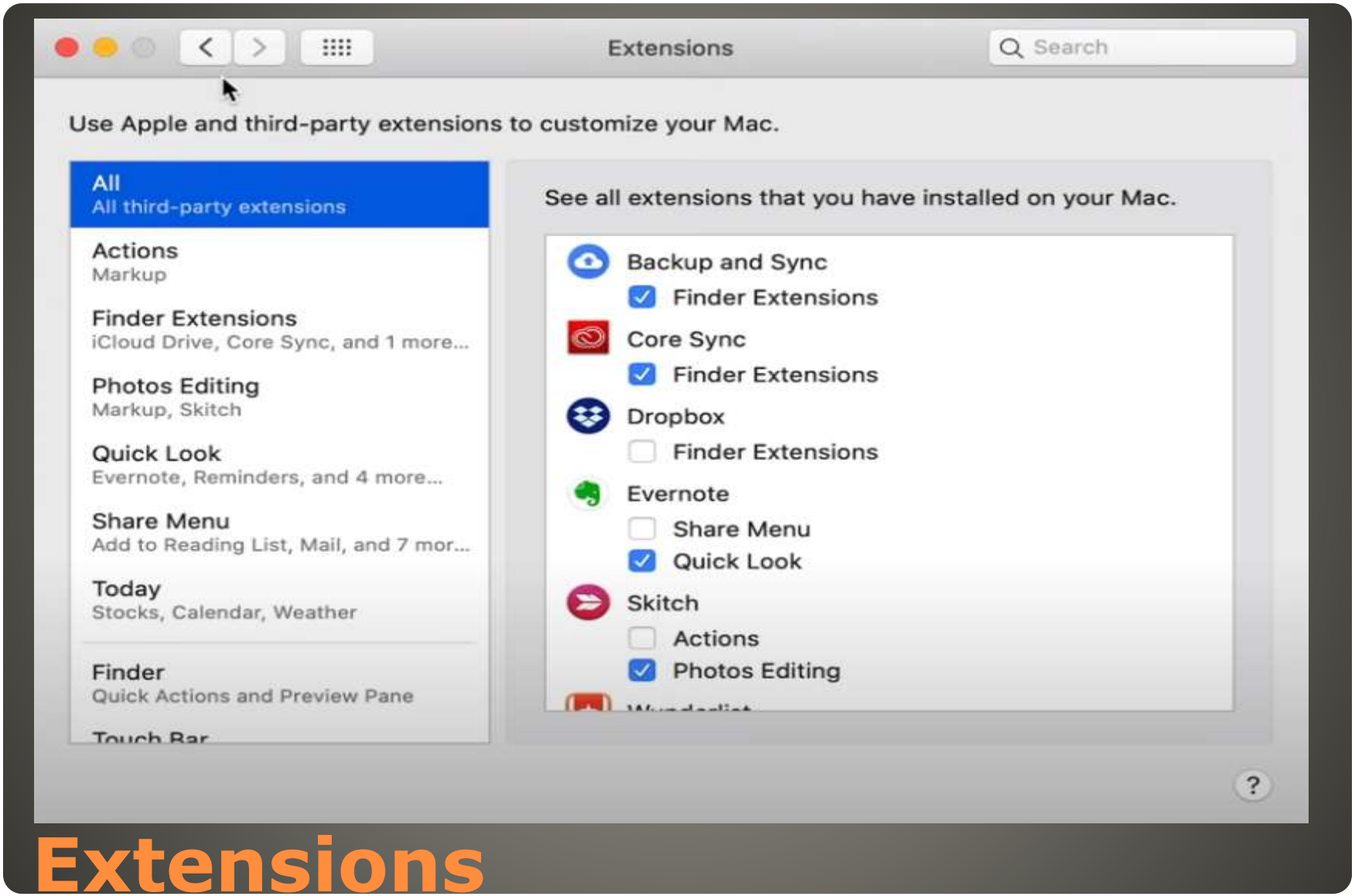
System Services - Location

MAC Analytics

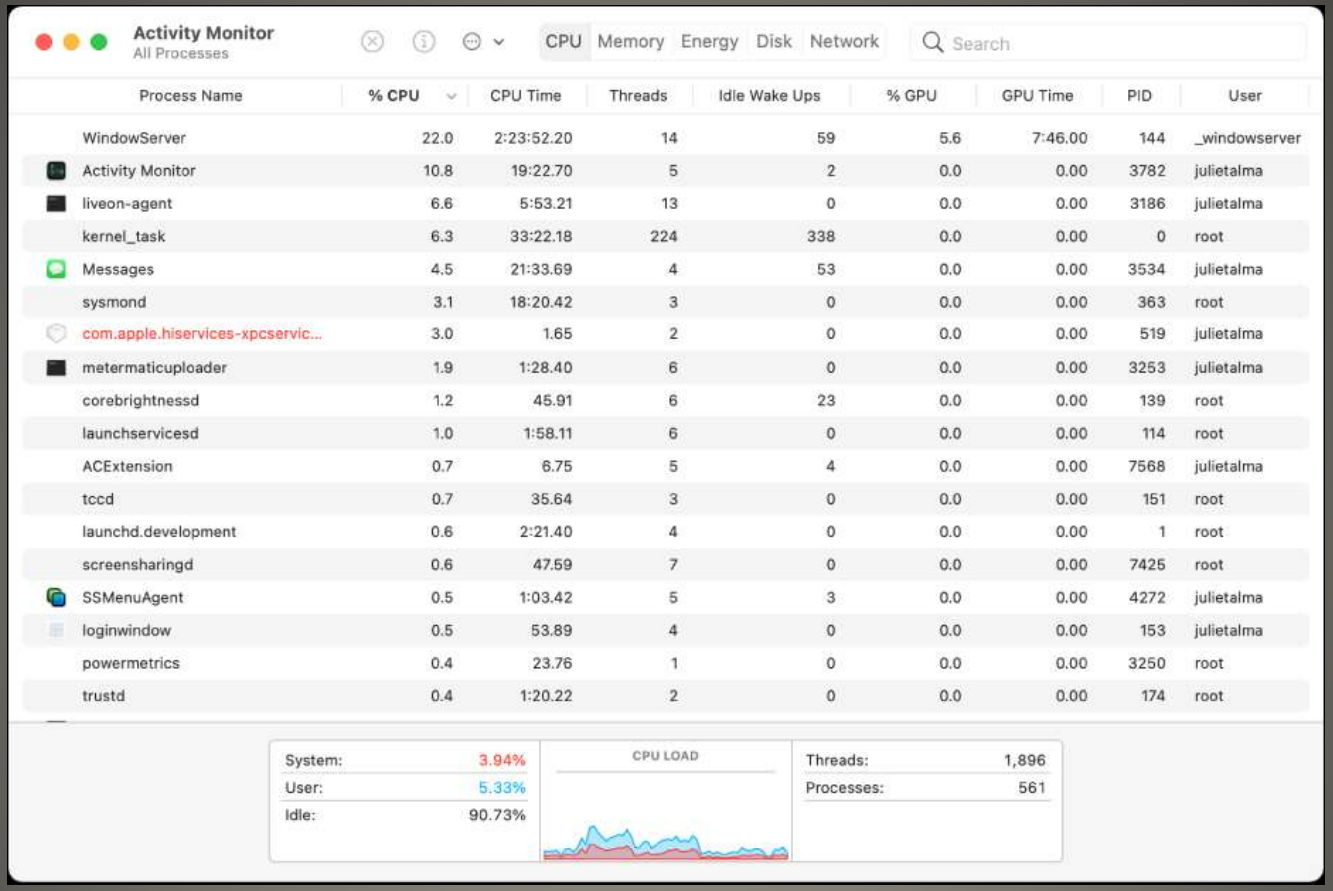
Limit Ad Tracking



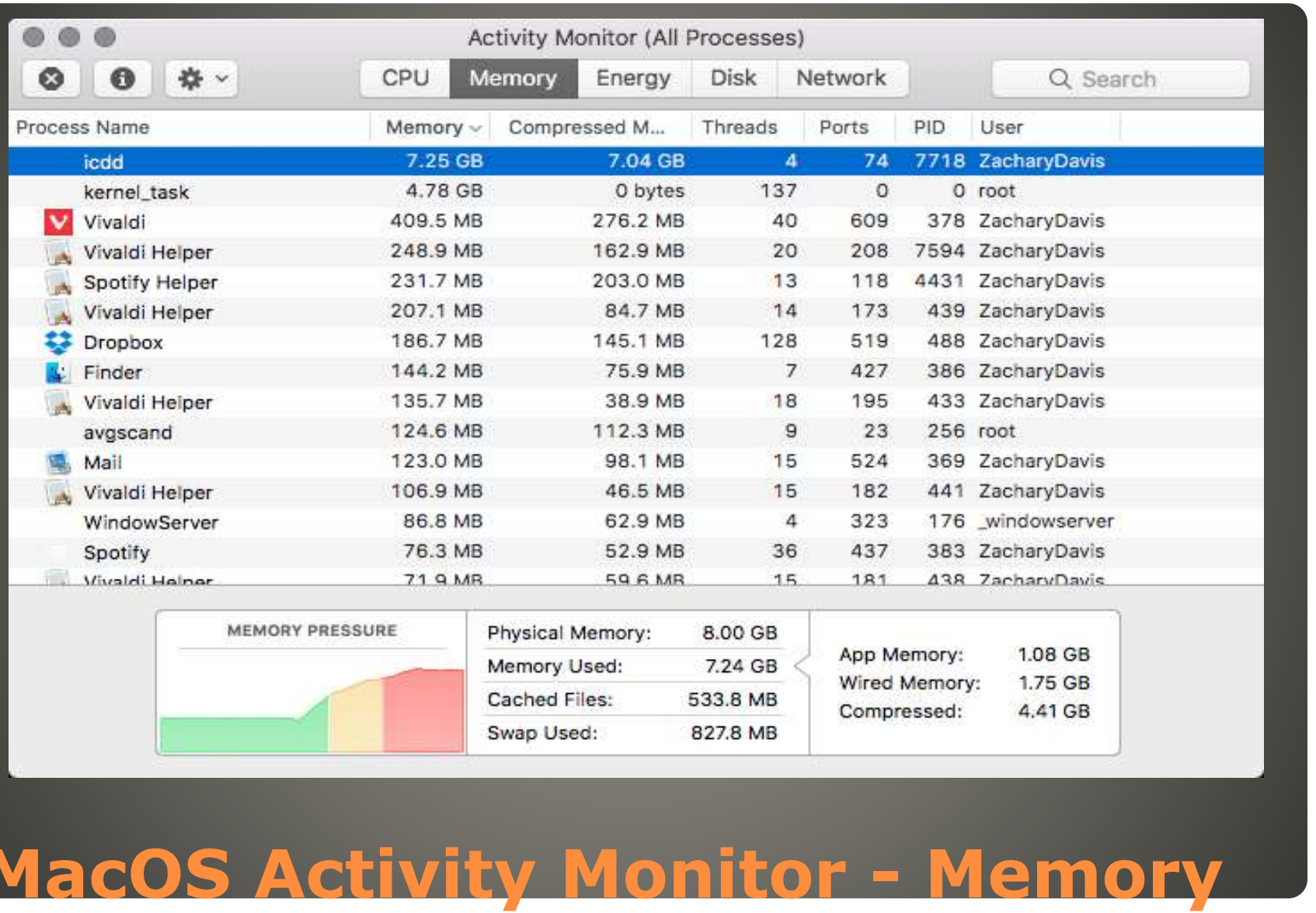
Notifications zoom


Extensions
Search
Use Apple and third-party extensions to customize your Mac.
All
All third-party extensions
Actions
Markup
Finder Extensions
iCloud Drive, Core Sync, and 1 more...
Photos Editing
Markup, Skitch
Quick Look
Evernote, Reminders, and 4 more...
Share Menu
Add to Reading List, Mail, and 7 mor...
Today
Stocks, Calendar, Weather
Finder
Quick Actions and Preview Pane
Touch Bar
See all extensions that you have installed on your Mac.
Backup and Sync
Finder Extensions
Core Sync
Finder Extensions
Dropbox
Finder Extensions
Evernote
Share Menu
Quick Look
Skitch
Actions
Photos Editing
?

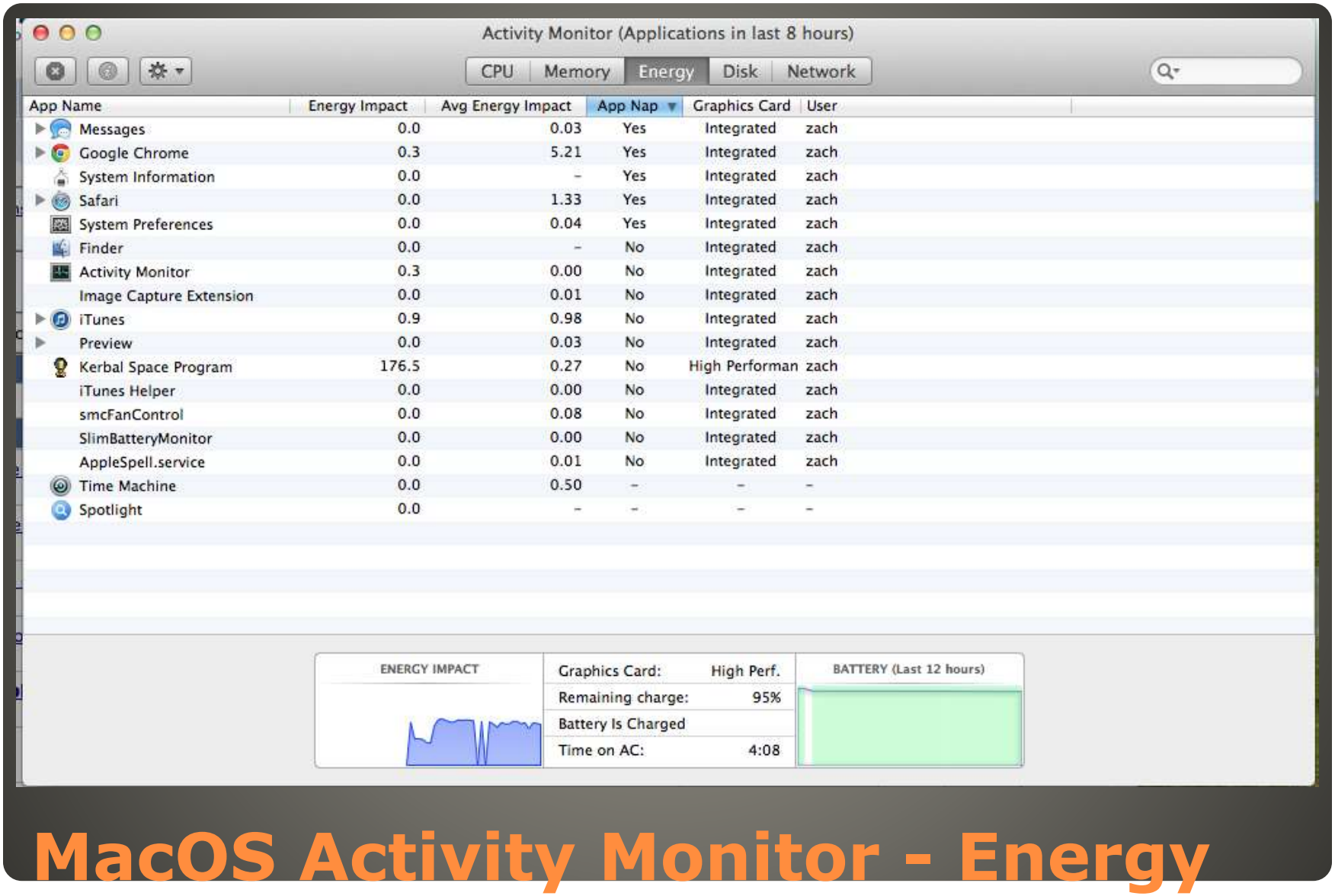
Extensions



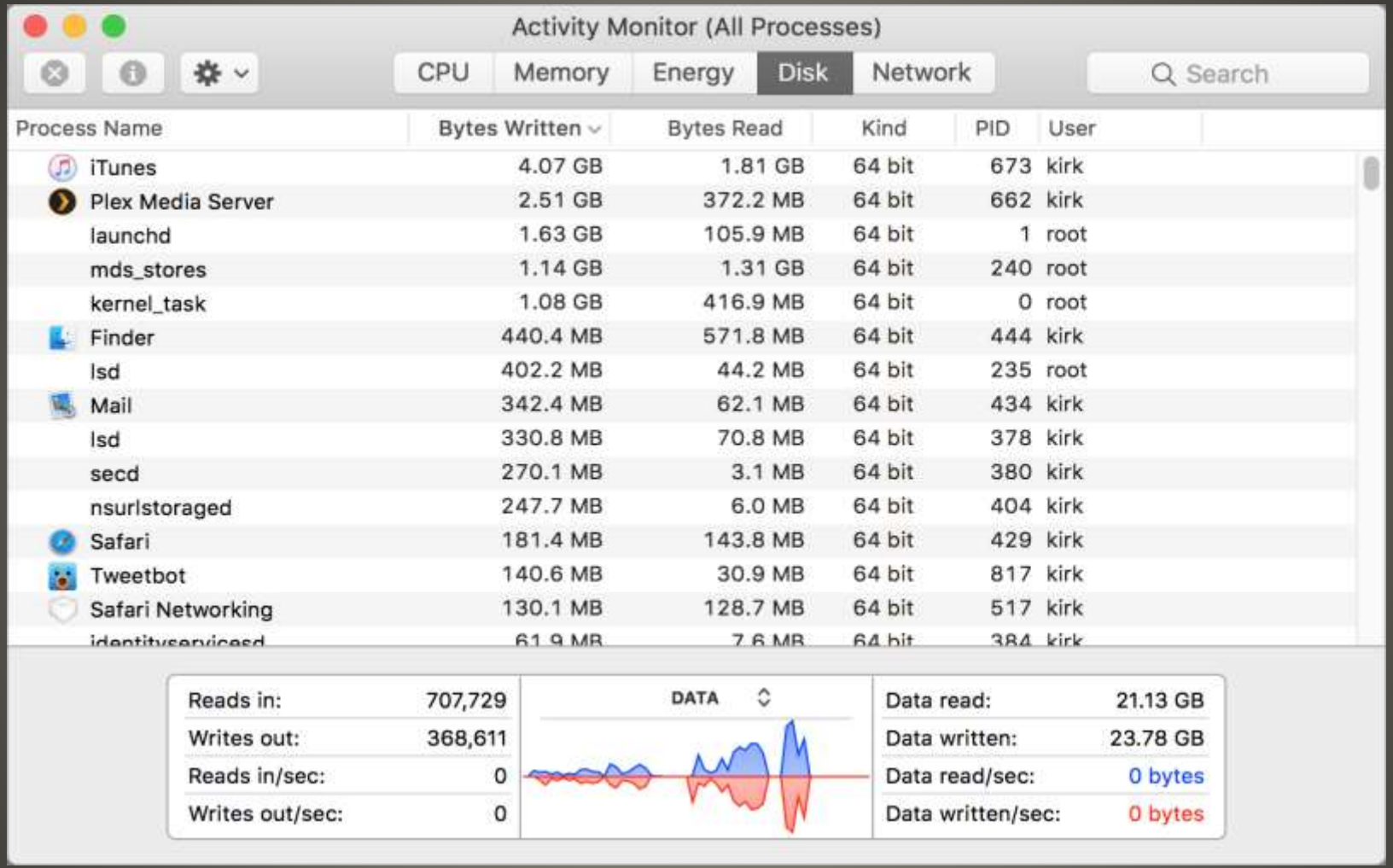
MacOS Activity Monitor - CPU



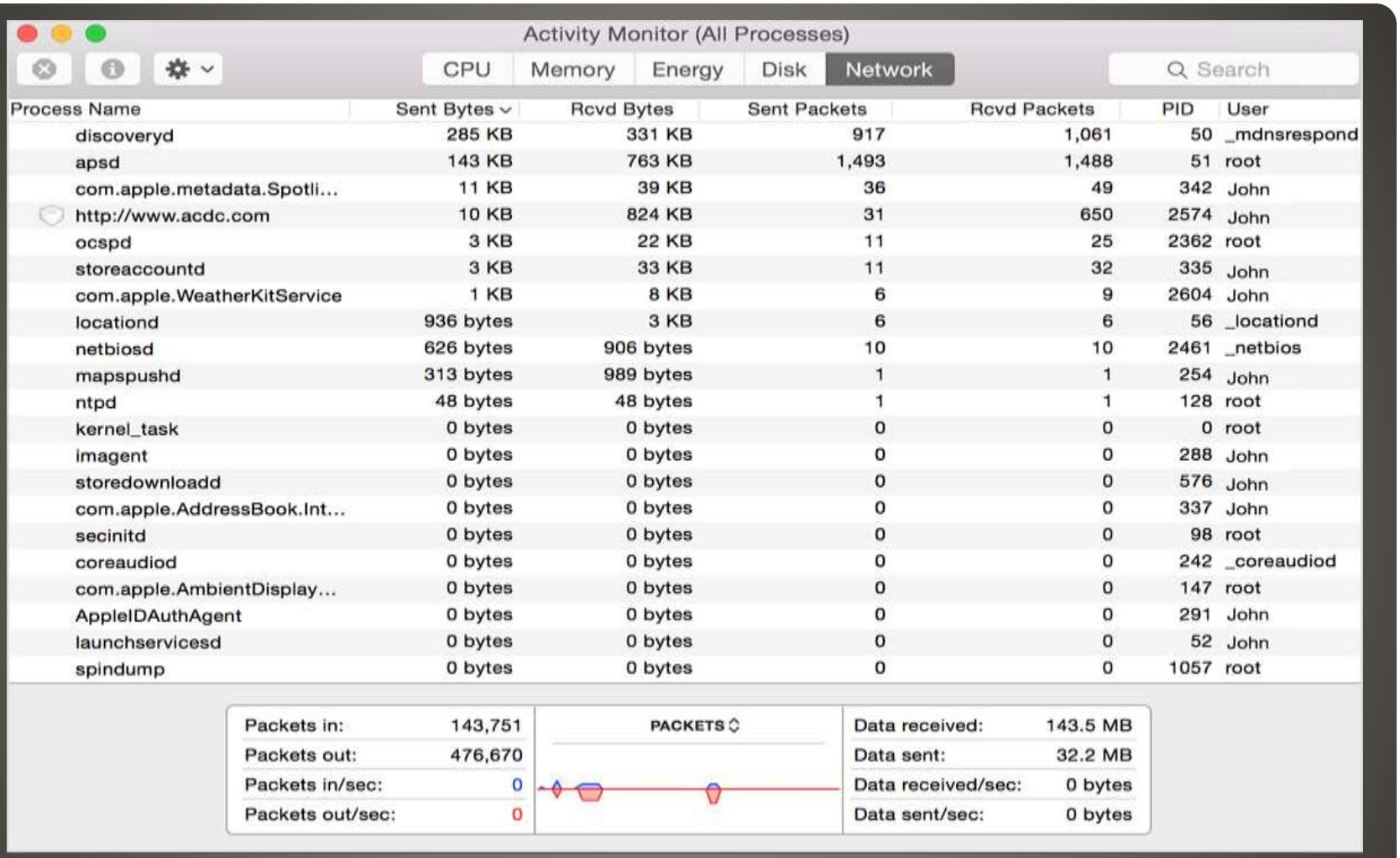
MacOS Activity Monitor - Memory



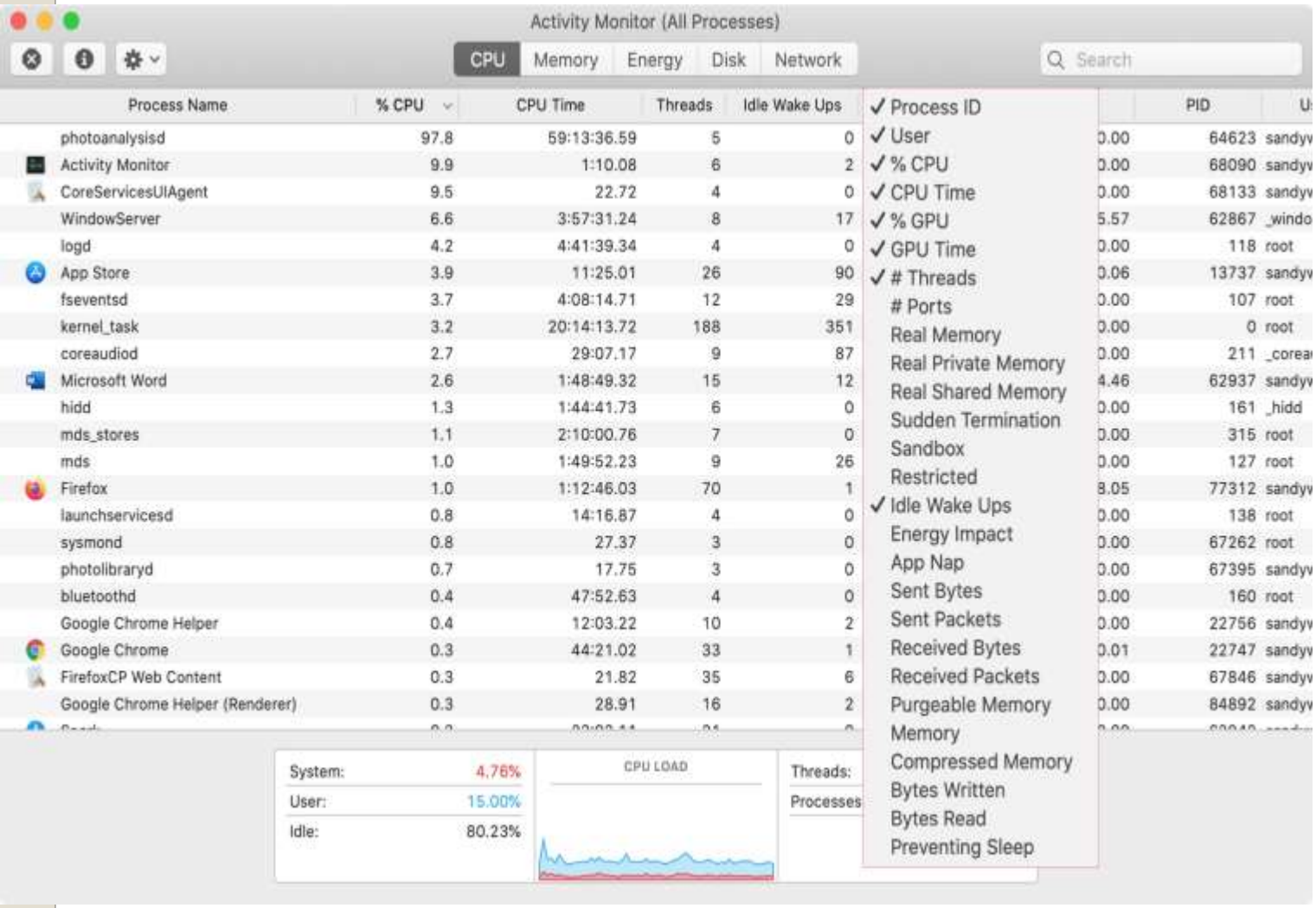
MacOS Activity Monitor - Energy



MacOS Activity Monitor - Disk

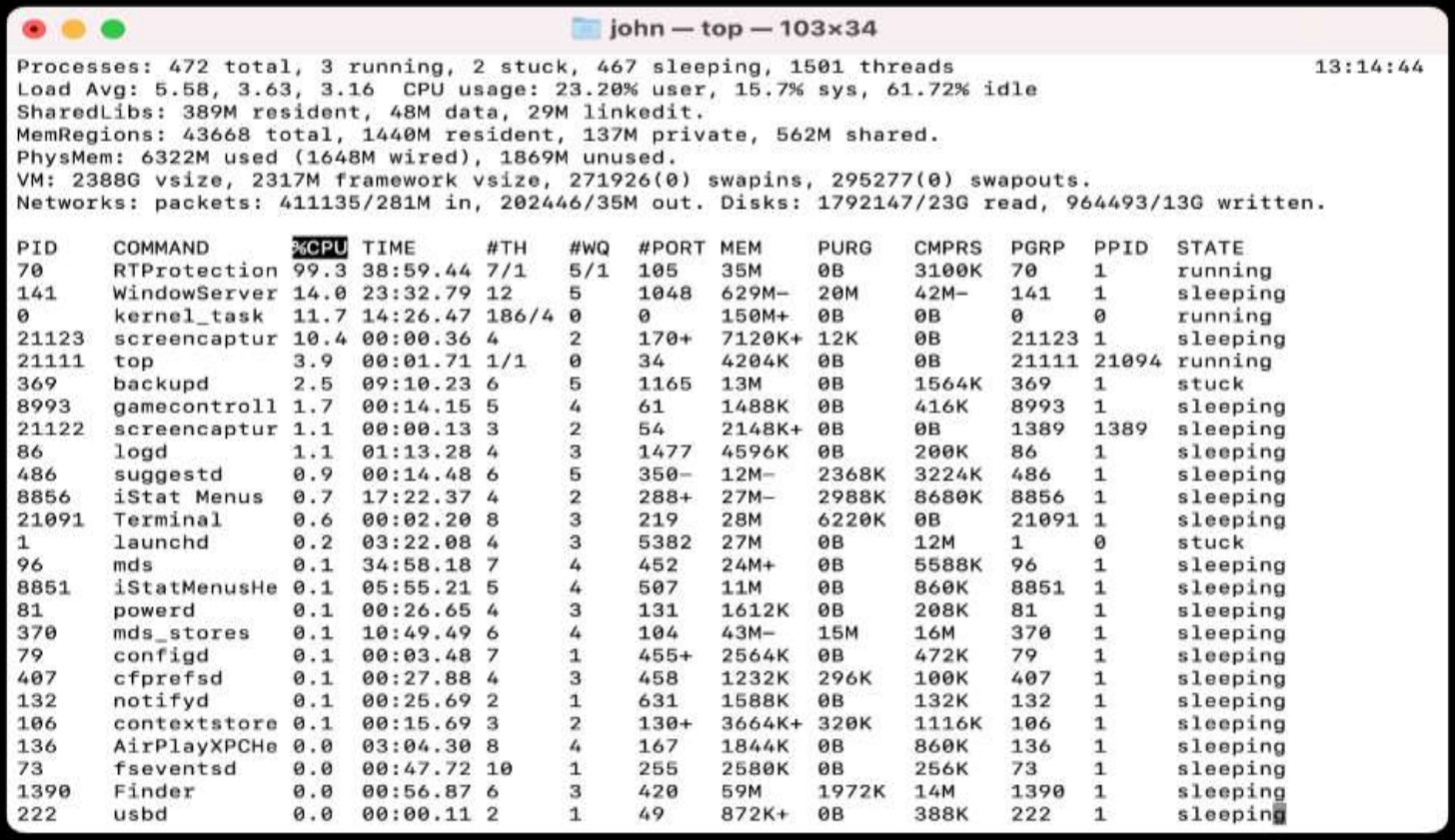


MacOS Activity Monitor - Network



MacOS Activity Monitor – add columns


Finder File Edit View Go Window Help
Wed Mar 17 11:23 AM



Linux commands in terminal app

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Chicken Little
Tortoise & Hare

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com


QUESTIONS?