Robert Hammen

Robert Hammen has been managing Macs for a long time - since before Apple shipped a Unix-based client OS. Robert was a long-time consultant to K-12 as well as small, medium, and enterprise organizations, but, for the past 3 1/2 years, has worked at the National Institutes of Health in suburban Washington DC, helping deploy, secure, and support Macs. Robert has numerous Apple and Jamf IT certifications, going back to OS X 10.4 and Jamf Pro 6.

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Why Test Beta OSes
Before Release?

- Provide feedback to Apple

- Find bugs/issues, potentially exclusive to your environment

- Be ready to support as close to release as possible

@roberthammen @hammen

Why Support Right Away?

- Previously: Benfer's Maxim: "Woe is me, if I deploy before .3"

- Security model has changed

- Gone from a slow, methodical change management approach…

- …to an Agile software development methodology, with development sprints and regularly-scheduled releases

@roberthammen @hammen

Regularly-Scheduled…

- Mac Office Team: monthly releases

- Adobe: Patch Tuesday (unless critical vulnerabilities)

- Apple: new major macOS in fall, .1 release after 30 days, then point releases every 45-60 days

- Apple Spring Release has new features/surprises (if you're not paying attention)

@roberthammen @hammen

Education, I Feel You

- Timing of Apple OS releases not great for most edu customers, at least in North America

- Adopt when you are ready

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Security!

- Unofficially (not documented anywhere, but SOP): Apple provides patches for current OS and previous 2, i.e. N-2

- Read the Apple Security Updates KB: https://support.apple.com/en-us/HT201222

- Not all fixes are back-ported to the previous OS (see: Spectre/ Meltdown initial response, ZombieLoad/FallOut only fully patched on 10.14.5): https://support.apple.com/en-us/HT210107

@roberthammen @hammen

Security!

- If you want to have the most secure Mac, you must be running the latest (N) macOS (with the latest app updates, of course)

@roberthammen @hammen

Rate of Change is Increasing

- macOS 10.13: APFS (end of imaging), User-Approved MDM, User-Approved Kernel Extension Loading

- macOS 10.14: PPPC (Privacy Preferences Policy Control), Notarization

- macOS 10.15: Read-Only Boot Volume, expansion of PPPC and Notarization, End of 32-bit processes, KEXTs deprecated, and much more…

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Apple is Playing Chess

- If you pay attention, you can see the pieces moving

- Read-only boot volume and separated user apps/data? Where might this be going?

CYLONS, WE HAVE A PLAN
AND SO DOES 🍎

@roberthammen @hammen

"Difficult to see.
Always in motion is the future."

@roberthammen @hammen

How Can You Obtain macOS Betas?

- Developer Seed - $99/yr - https://developer.apple.com/programs/

  Probably still a good idea if you create installer packages and

  need to sign/notarize them - available immediately

- Public Beta - https://beta.apple.com/sp/betaprogram/

  not available right away

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

How Can You Obtain
macOS Betas?

- AppleSeed for IT - https://appleseed.apple.com

- This is what most people should be using.

- Previously required you to ask/nag your Apple SE or AE

- Now allows access to Managed AppleID's (i.e. the ones you use to log into https://business.apple.com or https://school.apple.com)

@roberthammen @hammen

How Can You Obtain
macOS Betas?

- Latest version of installinstallmacos.py - https://github.com/munki/macadmin-scripts

  ```
  sudo python installinstallmacos.py --seedprogram=DeveloperSeed
  ```

- seedutil - https://derflounder.wordpress.com/2018/01/06/setting-your-mac-to-receive-macos-beta-updates-using-seedutil/

  ```
  sudo /System/Library/PrivateFrameworks/Seeding.framework/
  Versions/A/Resources/seedutil enroll DeveloperSeed
  ```

@roberthammen @hammen

How Should You Test?

- Early Betas - Virtual Machines (VMware Fusion, Parallels)

- Official VMware support in 11.5, shipped on 09/19

- Parallels 15 offered full support in August

@roberthammen @hammen

General VMware Testing Tips

- Tools like the previously-mentioned installinstallmacos.py, AutoDMG https://github.com/MagerValp/AutoDMG and vFuse https://github.com/chilcote/vfuse would allow for automated VM creation

- Process documented here: https://www.modtitan.com/2019/10/back-in-business-catalina-vms-with.html

- Timing of VMware release was poor for the Catalina testing cycle

@roberthammen @hammen

General VMware Testing Tips

- Testing Device Enrollment with VMware Fusion
  https://www.rderewianko.com/how-to-create-a-vm-thatll-work-with-dep-on-vmware-fusion/

- If enrolling VMs in Jamf Pro, be sure to allocate 2 CPU cores to ensure MDM is functional
  https://www.jamf.com/jamf-nation/discussions/23549/reality-check-mdm-capability-with-virtual-machine#responseChild142635

General VMware Testing Tips

- Disable TouchID/authentication spins on TouchID Macs:

  `board-id.reflectHost = "FALSE"`

- Useful shortcuts in Setup Assistant

  https://chris-collins.io/2018/03/15/Using-Terminal-At-macOS-Setup-Assistant/

- Force DEP nag:

  `sudo profiles renew -type enrollment`

@roberthammen @hammen

Install on Real Hardware

- Secondary Mac, i.e. not your daily driver

- Any data on it **must be** backed up

- If upgrading an already-provisioned Mac, you should probably uninstall all security software

- Sign out of iCloud:
  https://ulysses.app/blog/2019/07/a-word-about-apples-os-betas/

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Notes About Testing Subsequent Betas

- Don't expect the App Store to be fully functional/reliable

- Don't expect Software Update (i.e. beta 2->beta 3) to work

- Be prepared to nuke and pave, or at least reinstall, especially for release version

- If you find a suspected bug, reproduce on a VM, other hardware, or nuke-and-pave and reproduce before reporting

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Resources Available
On AppleSeed

- Test Plans

- Discussion Forums

- The awesomely-well done "What's New for Enterprise and Education" PDF

@roberthammen @hammen

Betas Keep Coming…

- Approximately every 2 weeks or so

- Avoid the temptation of updating your primary Mac
  - At least wait until mid-August 😀

@roberthammen @hammen

Betas Keep Coming…

- You will most likely be waiting for your MDM vendor to release Day Zero support (not Zero Day support, that's something entirely undesirable)

- If you need to *test* new MDM functionality ahead of time, Profile Manager in macOS Server Beta is available…

- SimpleMDM, Jamf Pro 10.15 betas offered some Catalina support

@roberthammen @hammen

Organizational Considerations

- How is your organization structured?

- IT generalization vs silos of responsibility?

- Need to get everyone on board with testing, and adoption schedules

@roberthammen @hammen

Documenting your Provisioning Process

- Do you have a runbook that documents what applications/settings/profiles/configuration changes are made as part of your provisioning process?

- If the answer is **No**, time to create one

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Testing Your Provisioning Process

- Device Enrollment (via Apple Business Manager/Apple School Manager) on a non-T2 Mac

- Same, but on a T2 Mac

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

What Makes a T2 Mac Special?

- One computer, two OSes - macOS and bridgeOS

- bridgeOS gets updated when macOS does

- External boot disabled by default (Boot Security)

@roberthammen @hammen

Testing on a T2

- With external boot disabled by default, if the beta OS goes south, you may have a problem (might consider enabling)

- Suggest creating a new APFS container, and either installing Catalina on it, or installing Mojave on it as a backup, and upgrading your current OS to Catalina

- That way, you should still be able to Option-boot into a known-good OS.

@roberthammen @hammen

Test Your Apps

- Do they launch? Do they function correctly?

- RoaringApps - https://roaringapps.com/apps?platform=osx

- Template for Technical Readiness - https://www.modtitan.com/2019/06/template-for-macos-core-application.html

Application Name	Application Owner	Min. Version Required	Catalina Ready?	Notes
Google Chrome	Mac Eng	TBD	☐	20190619 - Version 75.0.3770.100 functions as expected, unsure about notarization requirements (@EKW)
"AV Software"	@Security Person		☐	20190618 - Version 1.2.3 appears to be functioning normally, waiting on confirmation of support from $vendor
"Random Internal App"	@Developer Person	RIP ☠	☐	It's dead, Jim
etc. ...			☐	

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Test Your VPN

- Does your VPN do posture detection? If so, may need updates for new OS support

- No security tools in betas = may fail - ability to whitelist?

@roberthammen @hammen

Test Your Productivity Apps

- Office

- WebEx, Zoom, etc.

@roberthammen @hammen

Test Your Backup Software

• Can it successfully back up user data from the beta OS?

• Can it successfully *restore* user data from a beta OS?

@roberthammen @hammen

Test Printing

OFFICE SPACE ©2016FOX

- Do all of your printer drivers work, or do you need updates?

- Test with print servers, additional software like PaperCut, et. al.

@roberthammen @hammen

User Experience

- What new prompts will the users see?

- What can you whitelist? What *should* you whitelist?

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Surprises

- There will always be at least one

- macOS Catalina advertised in macOS Mojave Software Update prefs was... unexpected:

@roberthammen @hammen
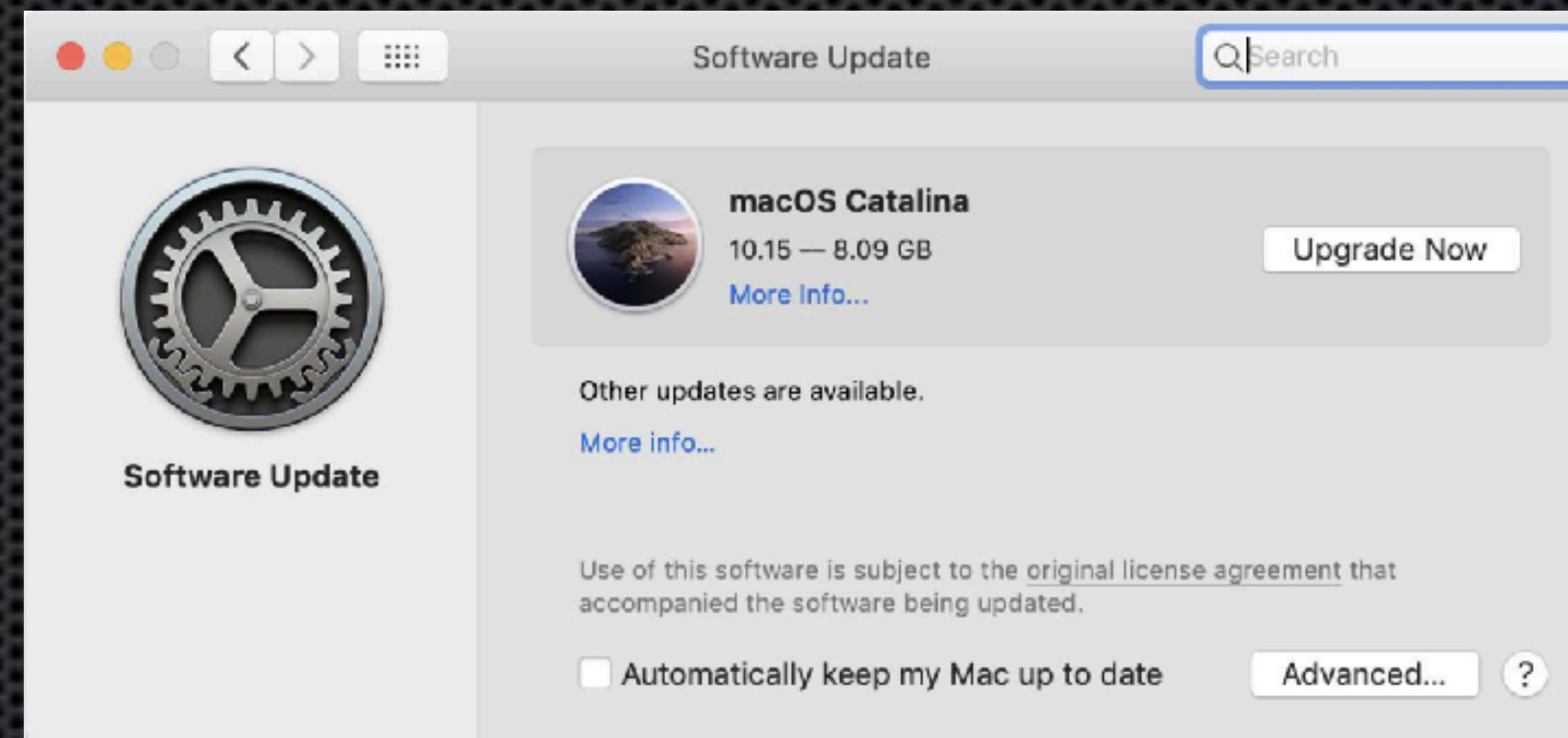
Test Your Re-Provisioning Process

- macOS Catalina changed volume formats, causing some issues with wipe-and-reload

- Also affects ability to easily downgrade

- More changes coming in future OSes

@roberthammen @hammen

Test Your Scripts

- Scripting languages may not be included in the OS

- On macOS Catalina, default Unix shell has changed to zsh

@roberthammen @hammen

Removal of Scripting Languages

- Reduces attack surface - does your dad really need a Python interpreter on his Mac?

- Python 2.7 deprecated, EOL in January 2020

- Python3 installation-on-demand (similar to Xcode command-line tool installation/prompts)

- Ruby and Perl may be removed from a future version of macOS

Removal of Scripting Languages

• Similar to when Apple stopped including Java and XQuartz

• Scripting and automation on macOS is not going away

@roberthammen @hammen

Default Unix Shell Changed

- zsh in lieu of bash (for new users, existing can change)

- bash still shipping as part of the OS, existing scripts will run

- https://github.com/rothgar/mastering-zsh

- Scripting OS X has an 8-part series on moving to zsh:

  https://scriptingosx.com/2019/06/moving-to-zsh/

@roberthammen @hammen

Test Your Security Tools

- Like your MDM vendor, you'll probably need to wait until the beta OS goes Golden Master, or close to it, for compatible security tools

- If the new OS is shipping, but your security vendors aren't ready, and won't be ready any time soon, time to change vendors

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

KEXTs are dead! Sort of...

Not dead, just... resting

- Kernel Extensions = run at kernel level

- Can have significant performance and stability effects on the OS (current environment: 7 mandatory agents and a poor user experience)

- macOS 10.15 Catalina is the last version where KEXTs will run without compromise

@roberthammen @hammen

What Replaces KEXTs?

• System Extensions, aka sysx's

• Part of new DriverKit

• Runs in User Space, not Kernel

• Typically part of an app bundle, not dispersed across the filesystem

@roberthammen @hammen

DriverKit

- Endpoint Security Framework - like previous Hypervisor and VPN Frameworks included in the OS

- Designed to provide functionality to security tool vendors

@roberthammen @hammen

Changes to the FileSystem

- New boot/system volume is created during installation, and is made read-only afterwards

- Existing "Macintosh HD" is renamed to "Macintosh HD-Data"

- New APFS feature called "firmlinks" allows Finder and Unix shell to show unified Applications folder, even though apps are dispersed between R/O system (Apple) and data volume (third-party)

@roberthammen @hammen

Changes to the FileSystem

- Explicit paths/locations of files have changed

- Have seen some scripts and commands show inconsistent or inaccurate results

- Fun troubleshooting boot issues with not knowing where exactly the problematic LaunchDaemons, KEXTs etc. are, or if the volumes are mounted read/write

@roberthammen @hammen

Changes to the FileSystem

- Erase and Install today will wipe both OS and data volume

- Will that behavior continue in a future OS?

- In the future, will OS updates be installed, or copied? We have .ipsw files for iOS, could there someday be a similar approach for macOS? Stay tuned.
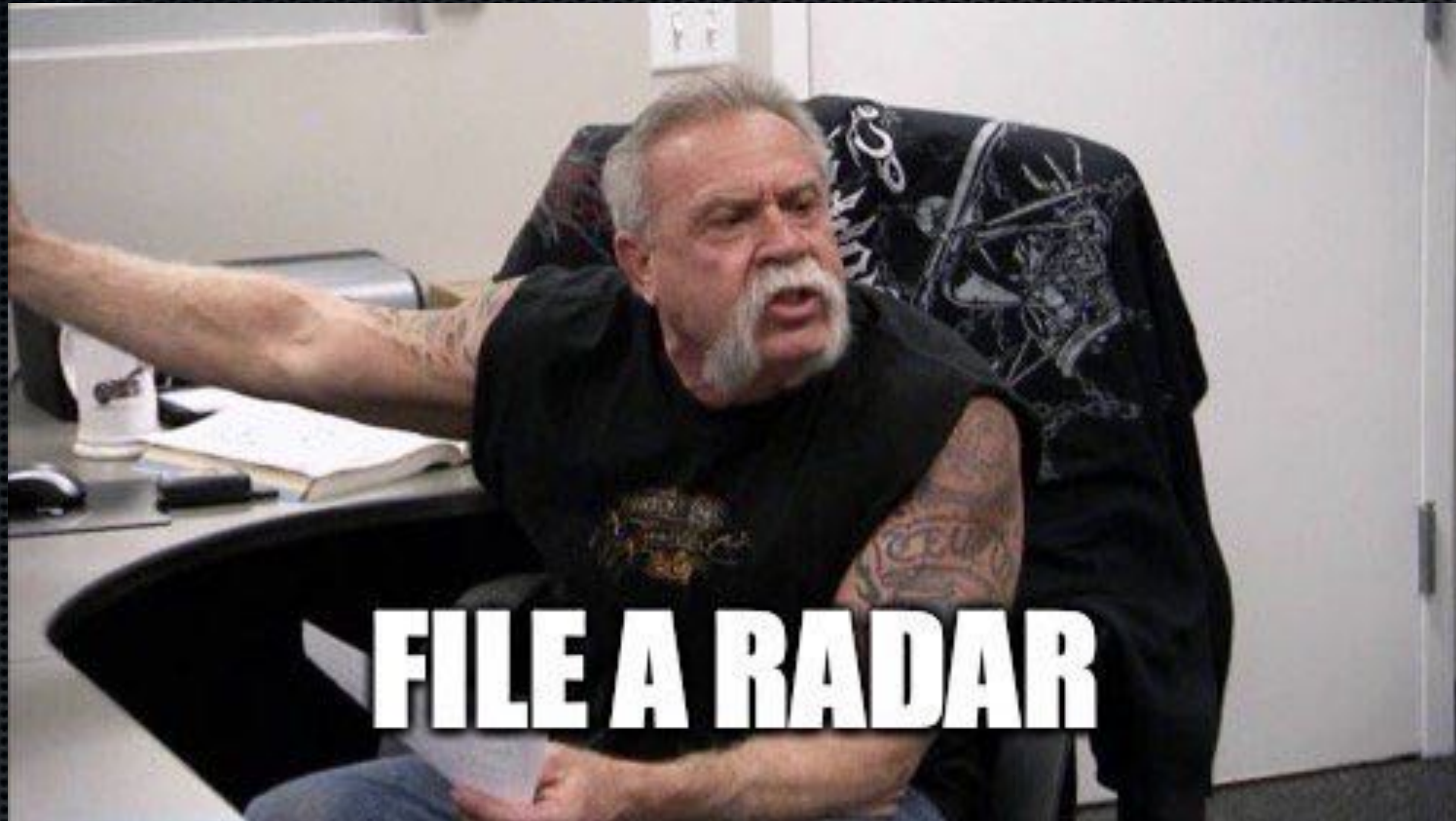
@roberthammen @hammen

Early Adopters

• You need them

• Identifying good ones is an art, not a science

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Reporting Bugs to Apple

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

Circle of a Bug Report's Life

FILE A RADAR

@roberthammen @hammen

Circle of a Bug Report's Life

@roberthammen @hammen
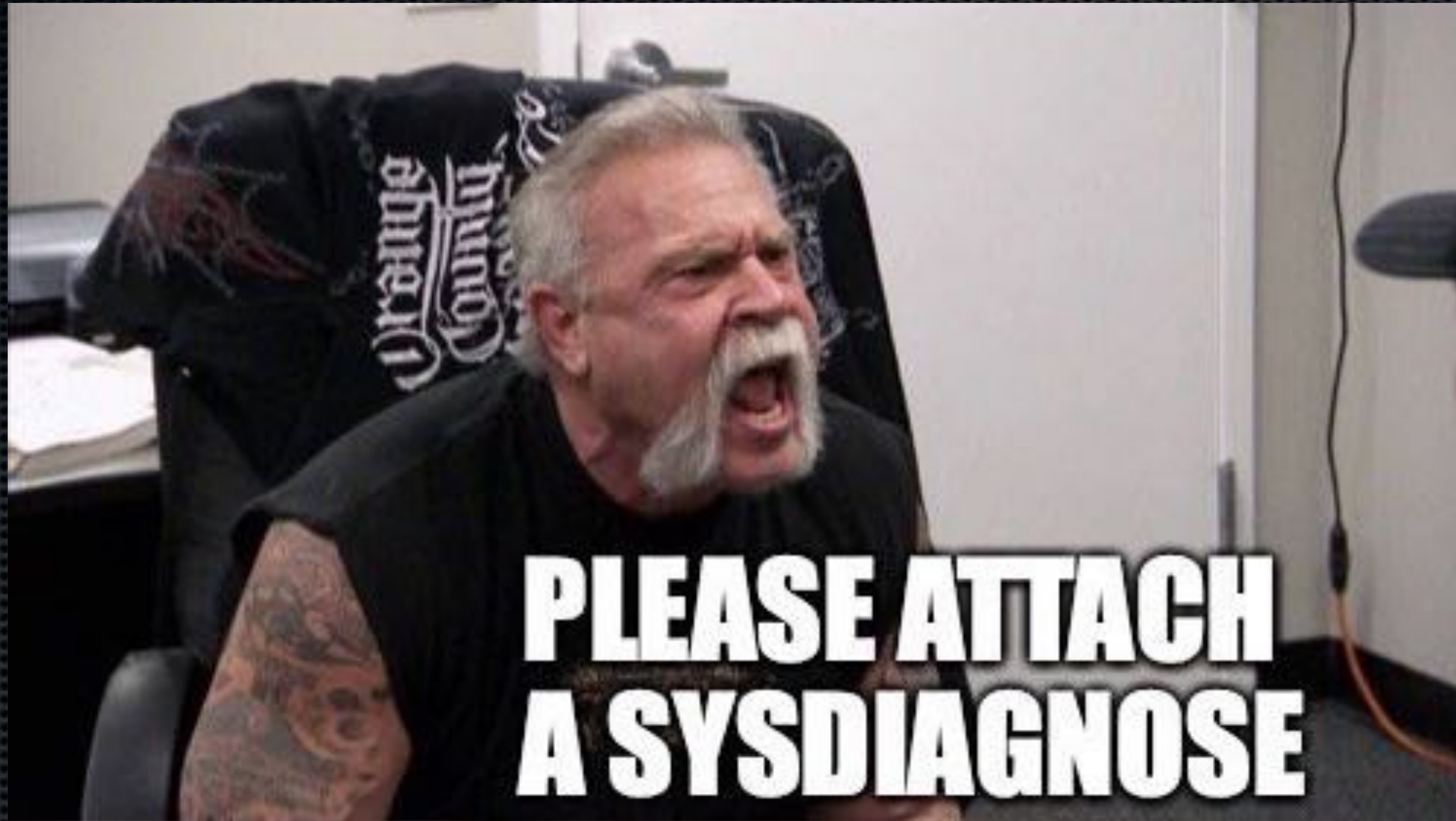
Circle of a Bug Report's Life

R.I.P. BugReporter

- New method of reporting bugs to Apple is Feedback Assistant (on both macOS and iOS)

- Located in /System/Library/CoreServices/Applications

- History of previous bugs maintained in app or at https://feedbackassistant.apple.com

@roberthammen @hammen

Feedback Assistant

@roberthammen @hammen

55

How To Write a Good Bug Report

• Provide an accurate title/subject

• What are you trying to accomplish?

• Please write an explicit description of the issue.

• Is it a new problem, or something that used to work?

• Can you reproduce it? What are the steps to do so?

@roberthammen @hammen

How To Write a Good Bug Report

- Include any screen shots or videos of the issue

- Sample scripts, sample code, test cases

- Any error messages, in full

- What the expected results were, versus the actual results

- Any workarounds you were able to identify

- Explain the impact/how many potential systems this affects

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

sysdiagnose

- command-line tool to gather system diagnostic information, logs, etc.

- Invoked by **sudo sysdiagnose** or Control-Option-Command-Shift-period

- Automatically performed when submitting a report via Feedback Assistant

- High-security environments may not be able to use this tool

@roberthammen @hammen

Sysdiagnose

@roberthammen @hammen
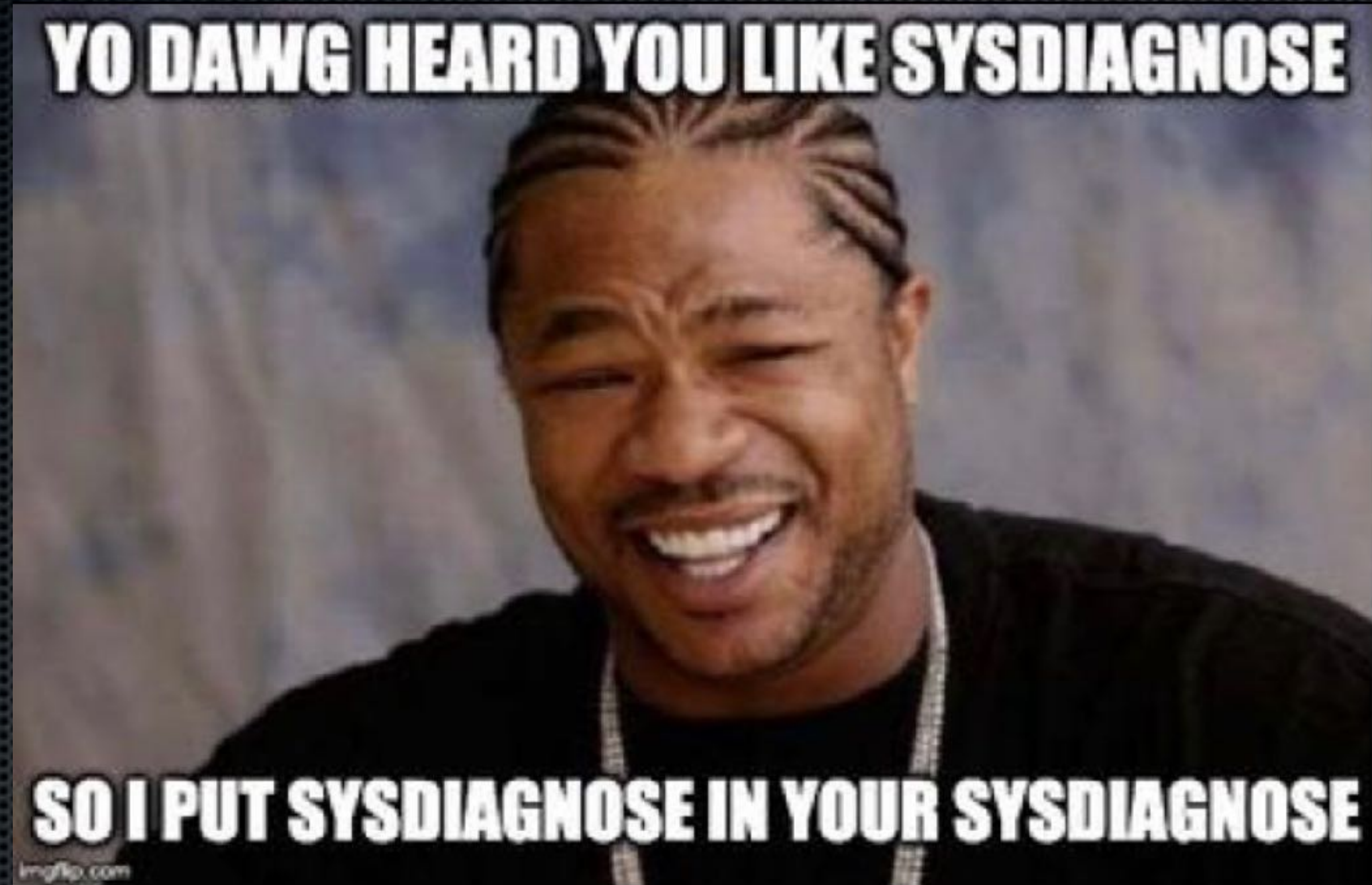
If It's A Critical Bug

- Be sure to file it using a Managed AppleID from Apple Business Manager/Apple School Manager (goes to a different queue)

- Open an AppleCare Enterprise Case

- Email both the Feedback ID and the AppleCare Enterprise Case numbers to your SE

- SE's have an escalation path for serious issues

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Bug Report Links

- Profiles and Logging instructions for Apple technologies:

  https://developer.apple.com/bug-reporting/profiles-and-logs/

- SysDiagnose Logging Instructions:

  https://download.developer.apple.com/OS_X/OS_X_Logs/

  sysdiagnose_Logging_Instructions.pdf

@roberthammen @hammen

Please Dupe Feedback Requests

- <u>Dropbox Paper for Catalina Issues</u>

- Fleetsmith blog - <u>https://blog.fleetsmith.com/macos-enterprise-security-roadmap/</u>

- Discussion in #catalina, #appleseed-private on MacAdmins Slack

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

@roberthammen @hammen

Questions?