

Extracting and Parsing Apple Unified Logs

Step 1: Open iOS full file system extraction with 7-zip (right click – 7-zip – open archive)

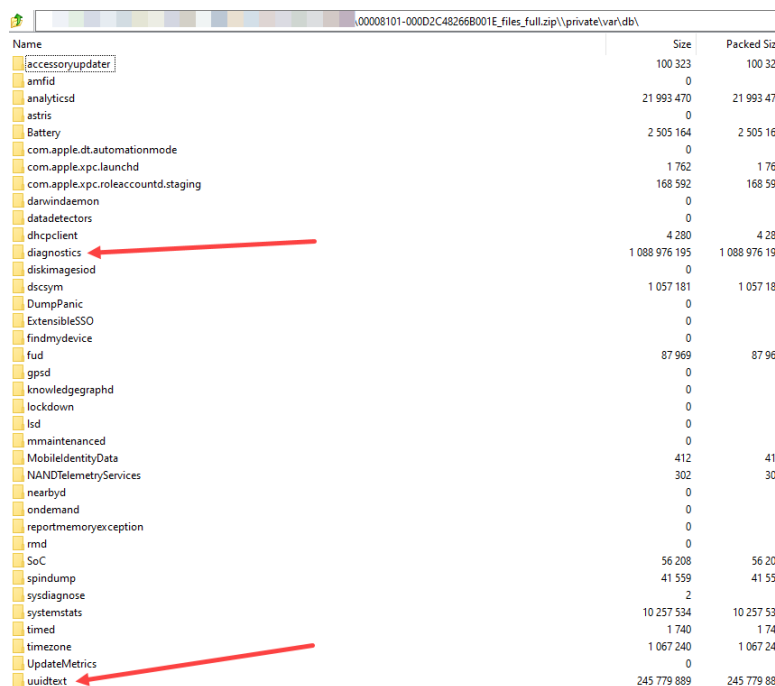
Step 2: Navigate to the following file path within the extraction

00008101-000D2C48266B001E_files_full.zip\private\var\db\

Step 3: Copy the following two folders onto a USB drive, formatted in exFAT. Simply drag and drop them from 7-zip onto the formatted USB.

-diagnostics

-uidtext



The screenshot shows a 7-Zip file explorer window with the following table of contents:

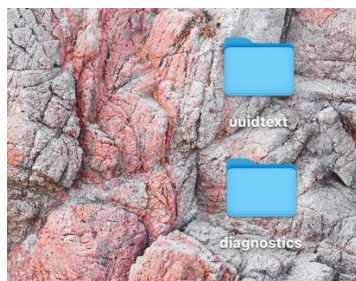
Name	Size	Packed Size
accessoryupdater	100 323	100 323
amfid	0	0
analyticsd	21 993 470	21 993 470
astris	0	0
Battery	2 505 164	2 505 164
com.apple.dt.automationmode	0	0
com.apple.xpc.launchd	1 762	1 762
com.apple.xpc.roleaccountd.staging	168 592	168 592
darwindaemon	0	0
datadetectors	0	0
dhcpcclient	4 280	4 280
diagnostics	1 088 976 195	1 088 976 195
diskimagesiod	0	0
dscsym	1 057 181	1 057 181
DumpPanic	0	0
ExtensibleSSO	0	0
findmydevice	0	0
fud	87 969	87 969
gpsd	0	0
knowledgegraphd	0	0
lockdown	0	0
isd	0	0
mmaintenanced	0	0
MobileIdentityData	412	412
NANDTelemetryServices	302	302
nearbyd	0	0
ondemand	0	0
reportmemoryexception	0	0
rmd	0	0
SoC	56 208	56 208
spindump	41 559	41 559
sysdiagnose	2	2
systemstats	10 257 534	10 257 534
timed	1 740	1 740
timezone	1 067 240	1 067 240
UpdateMetrics	0	0
uidtext	245 779 889	245 779 889

Red arrows point to the 'diagnostics' and 'uidtext' folders in the list.

Step 4: Property eject the USB from your Windows Computer. This ensures all contents have been written to the USB (Windows is a quick read/slow write operating system).

Step 5: Insert the USB into your Macintosh computer

Step 6: Drag the diagnostics and uidtext folders to your Macintosh desktop

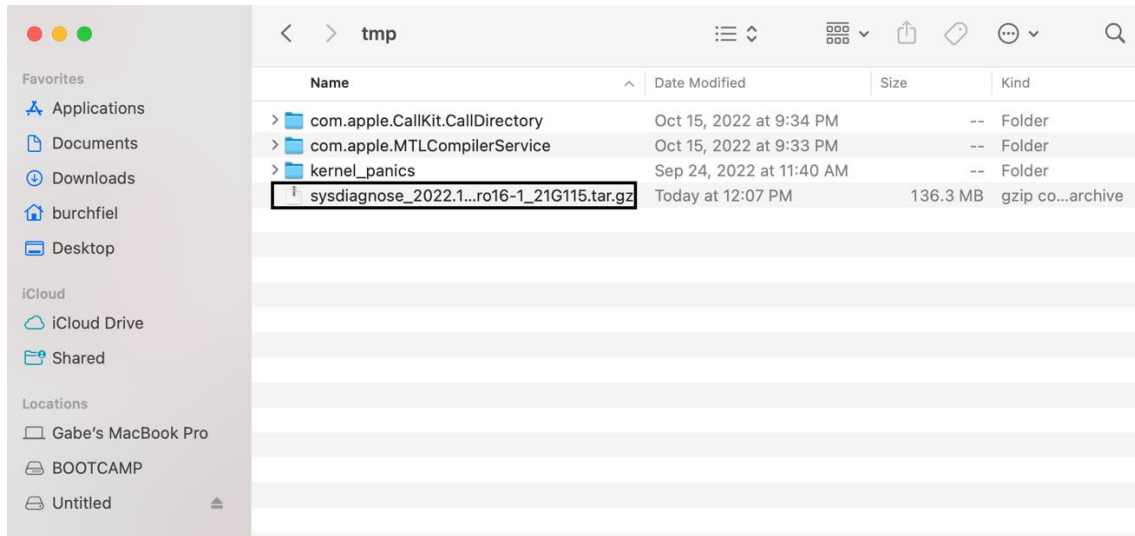


Step 7: Create a system diagnose log archive for your current Macintosh computer

To do this press the following keys simultaneously:

command+option+control+shift+period. Your screen should flash on success.

Step 8: Once completed, the log will pop up on the desktop (usually takes a few minutes)



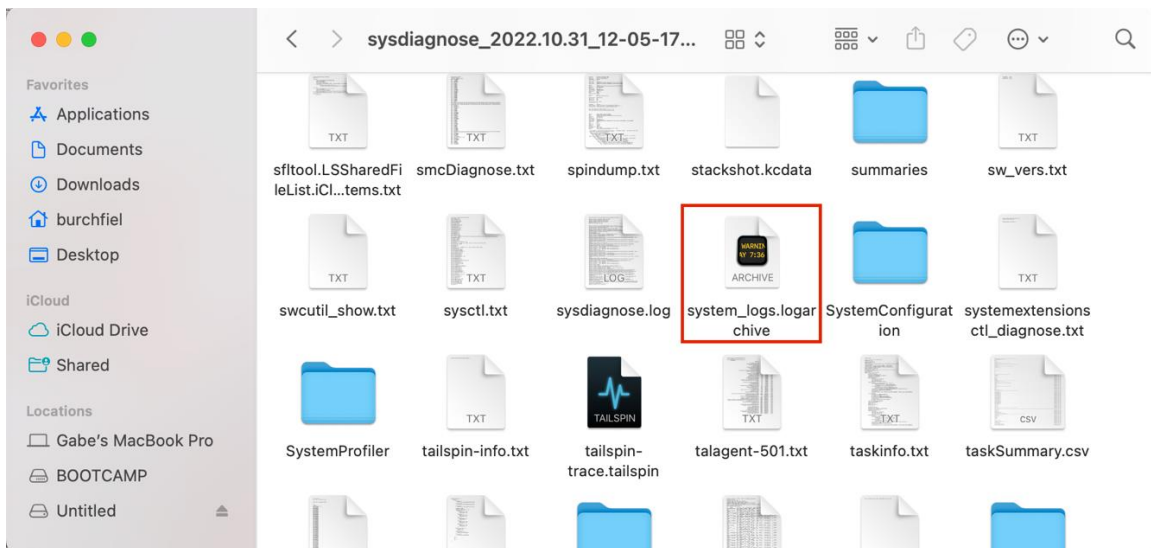
If it doesn't pop up, it can be located at the following path:

Macintosh HD - Data/Private/Var/Tmp (If the private folder isn't visible, simultaneously press command+shift+period to show hidden folders)

Step 9: Double click the sysdiagnose.tar.gz file to execute the extraction

Step 10: Once extracted, open the newly created folder of the same name as the tar.gz file

Step 11: Within this folder, locate the file system_logs.logarchive



Step 12: Right click the system_logs.logarchive file, and click “show package contents”

Step 13: Locate the info.plist file (usually toward the bottom), copy it, and paste it to the desktop

Step 14: Navigate back to the desktop, and open the uuidtext folder

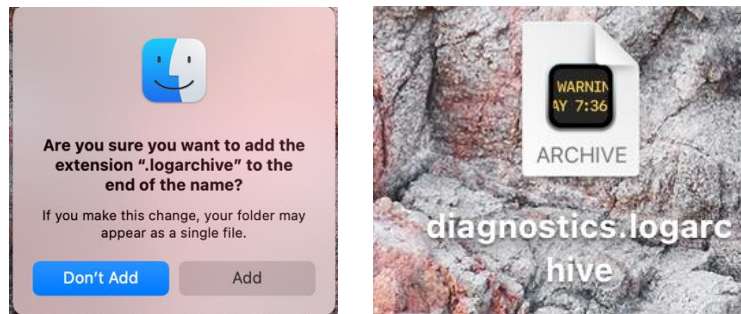
Step 15: Press command+A to highlight all files within this folder. Once highlighted, right click on one of the highlighted files, and click copy.

Step 16: Close the uuidtext folder, right click on the diagnostics folder, and paste all items

Step 17: Right click on the info.plist which you previously saved to the desktop, and copy

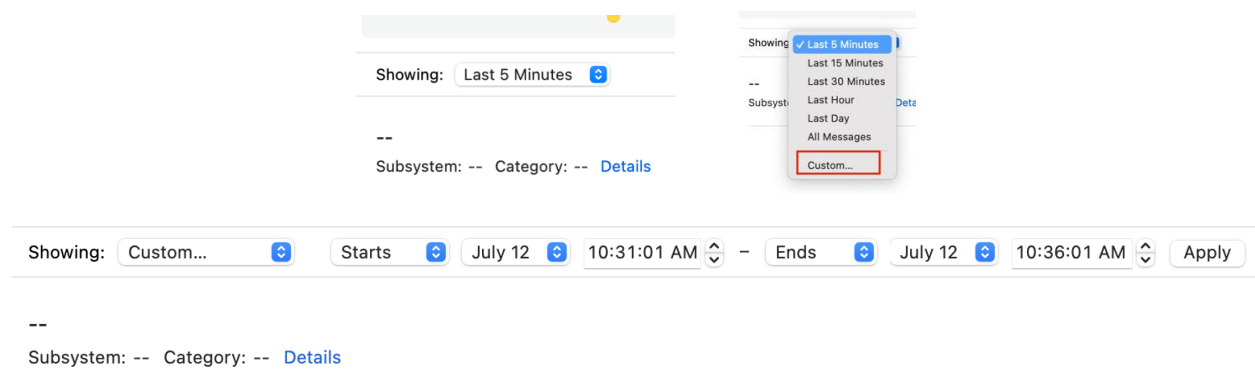
Step 18: Right click on the diagnostics folder, and paste in the info.plist file

Step 19: Append the diagnostics folder with the extension .logarchive, a popup window will open. Click Add, and the folder icon will change



Step 20: Once the icon changes, simply double click to open the file with the native Console application on the Macintosh computer.

Step 21: Filter by date, to do so the filter drop down is at the bottom (default is set to last 5 minutes). Change it to custom, then you can set the dates and times



NOTE: THERE ARE MILLIONS OF LOGS IN THESE FILES, IT MAY TAKE A LOT OF TIME TO OPEN THEM UP IF YOU DO NOT FILTER BY DATE