



FALSE MOUNTS: FINDING AND FIXING MAC'S "SILENT KILLER"

If your customers rely on external drives or network volumes during their day-to-day computing, they may have experienced a situation known as a *False Mount*. They will likely not even know that something has happened until they notice that important data has gone mysteriously missing.

Here's the good news: Watchman Monitoring can notify you as False Mounts occur, so you can step in and save the day.

WHAT ARE FALSE MOUNTS?

A False Mount is a folder left on the boot volume, which interferes with the normal mounting of external disks and network volumes.¹

False Mounts are typically created when an application or running process writes data to an external volume *after* an unexpected unmount. For external drives or network drives, unmounts

could be caused by any abrupt disconnection of a disk's connection: a power failure, a computer crash, or a user unexpectedly disconnecting an external drive could all result in a False Mount's creation. False Mounts of network volumes might be caused by poor network connections which silently disconnect a Mac from a file server. Corrupted sparse bundles, like the ones used for Time Machine backups to a network volume, could also result in a False Mount's creation.

¹Duplicate mount point in **/Volumes** after unexpected restart, *Apple Support*
<https://support.apple.com/HT203258>

When a computer attempts to mount an external volume which matches the name of a False Mount, it will not be mounted to the expected path. As writes are sent to that volume, data may accidentally be stored directly in the False Mount, and fill the boot volume. When they are not detected and managed, False Mounts can silently result in lost data or a too-full boot volume.

False Mounts wreak havoc and confusion when data isn't saved where expected. Repercussions may extend beyond the realm of a purely technical, resulting in intra-office finger pointing over why a user didn't save their work to a server, or why an admin didn't configure backup systems as expected.

EXAMPLE 1: WHAT HAPPENED TO THE FINAL DESIGN FILES?

A graphic designer's iMac accumulated 13 False Mounts due to a poor ethernet cable. These folders held the most current versions of several different files which the designer thought were properly saved to a shared network volume. Unfortunately, due to the False Mounts, these files were saved to the local computer instead. The problem was discovered only after the older version of a file was

sent to press, leaving the designer's colleagues frustrated, and the designer confused.

EXAMPLE 2: WHY WASN'T THE MAIL SERVER BACKED UP?

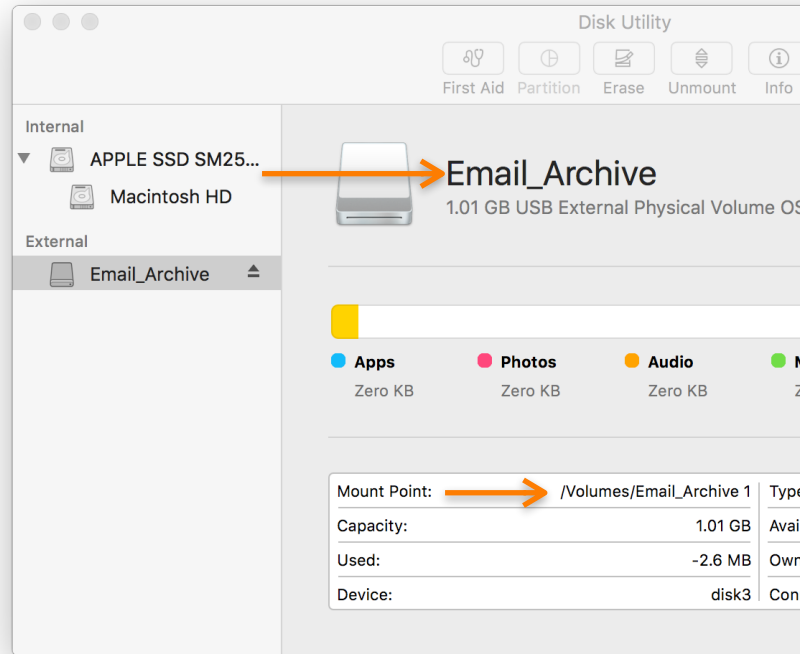
A business's mail server was configured to archive to an external drive. When the server developed a False Mount after a reboot, the server software started writing data to the boot volume instead. Before the False Mount was discovered, over 10GB of archives was written to the boot volume, resulting in a crash. After troubleshooting the issue, the server's administrator realized that had the boot volume failed, the archives would have been lost, as the daily clone would not have saved the data accidentally saved to /Volumes/Archive.

IDENTIFYING AND ADDRESSING FALSE MOUNTS

Now that you know about False Mounts — how do you find them, and how can they be addressed?

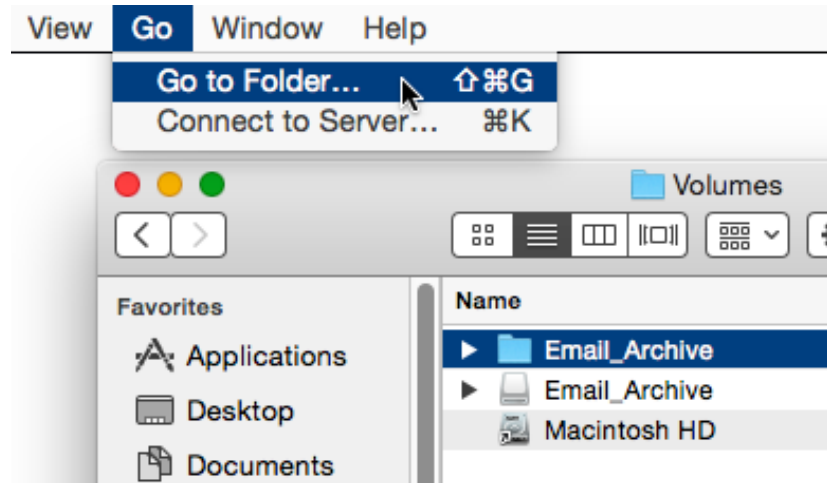
IDENTIFYING A FALSE MOUNT WITH DISK UTILITY

When viewed in Disk Utility, an external volume's mount point should match its name. In this image, Disk Utility reveals a volume's mount point is **Email_Archive 1**, despite the name of the volume appearing **Email_Archive** in the Finder. Because the volume was silently mounted to an incorrect path, writes in to the False Mount will go unnoticed until the boot volume fills up, or someone notices no data is being saved to the external volume as expected.



VERIFYING THE FALSE MOUNT IN THE FINDER

When Watchman Monitoring reports a False Mount you can verify the False Mount by going to the Finder, pressing Shift+Cmd+G (⇧⌘G), typing **/Volumes** into the field, and pressing Return (↵). You should see a folder with the same name as the external drive, in the Email Archive case it would be **Email_Archive**. You'll also notice that it contains the data that should have been stored on the external drive.

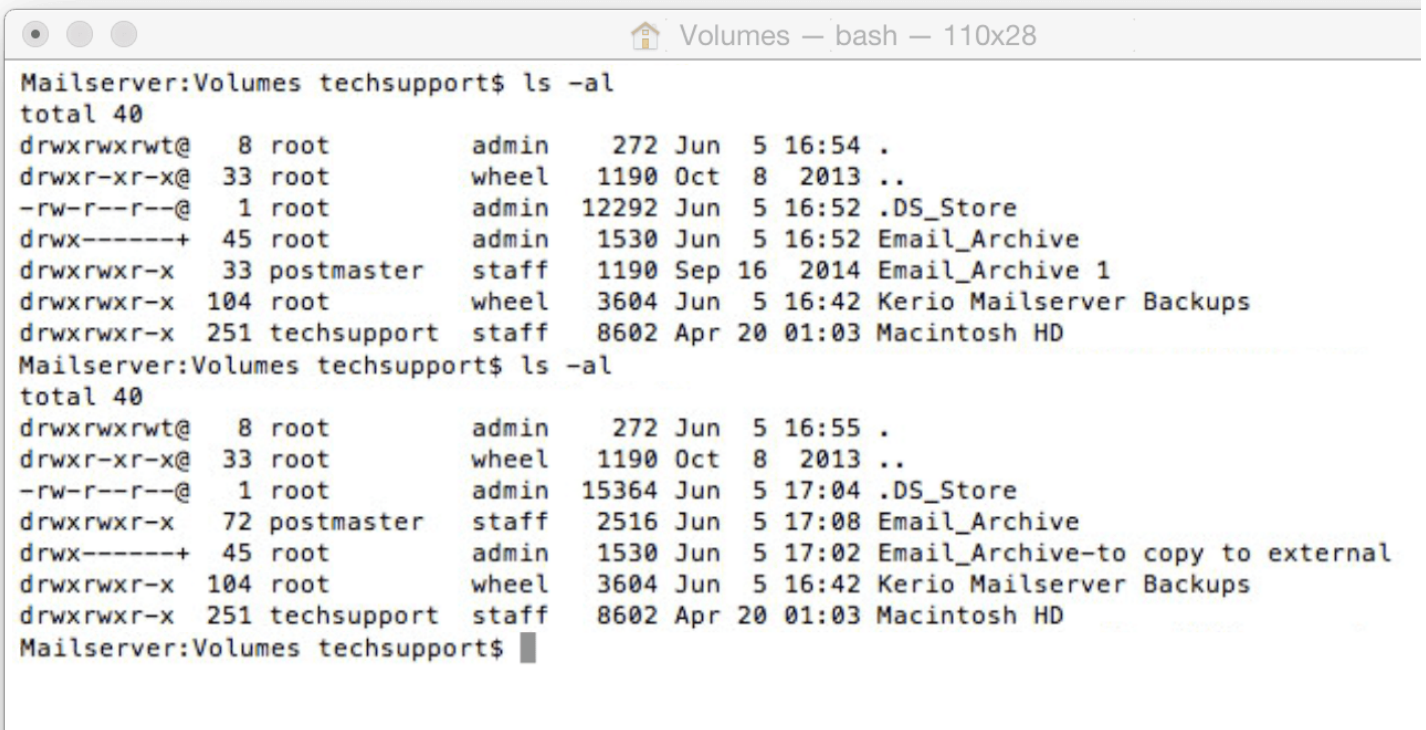


IDENTIFYING FALSE MOUNTS ON THE COMMAND LINE

To hunt False Mounts on the command line, start by opening Terminal.app and listing the the /Volumes directory. From the prompt, enter:

```
ls -al /Volumes
```

In this example, two paths for the volume exist: **Email_Archive** and **Email_Archive 1**. Because a folder named **Email_Archive** was present when the storage volume was being mounted, a 1 was appended to its name. This would prevent it from being used when data is written to /**Volumes/Email_Archive**.



```
Mailserver:Volumes techsupport$ ls -al
total 40
drwxrwxrwt@  8 root      admin   272 Jun  5 16:54 .
drwxr-xr-x@ 33 root      wheel  1190 Oct  8 2013 ..
-rw-r--r--@  1 root      admin 12292 Jun  5 16:52 .DS_Store
drwx-----+ 45 root      admin  1530 Jun  5 16:52 Email_Archive
drwxrwxr-x  33 postmaster staff  1190 Sep 16 2014 Email_Archive 1
drwxrwxr-x 104 root      wheel  3604 Jun  5 16:42 Kerio Mailserver Backups
drwxrwxr-x 251 techsupport staff  8602 Apr 20 01:03 Macintosh HD
Mailserver:Volumes techsupport$ ls -al
total 40
drwxrwxrwt@  8 root      admin   272 Jun  5 16:55 .
drwxr-xr-x@ 33 root      wheel  1190 Oct  8 2013 ..
-rw-r--r--@  1 root      admin 15364 Jun  5 17:04 .DS_Store
drwxrwxr-x  72 postmaster staff  2516 Jun  5 17:08 Email_Archive
drwx-----+ 45 root      admin  1530 Jun  5 17:02 Email_Archive-to copy to external
drwxrwxr-x 104 root      wheel  3604 Jun  5 16:42 Kerio Mailserver Backups
drwxrwxr-x 251 techsupport staff  8602 Apr 20 01:03 Macintosh HD
Mailserver:Volumes techsupport$
```

FIXING THE FALSE MOUNT

False Mounts which are related to network shares are owned by the logged in user, and are typically cleared during the log out restart process. False Mounts created by processes such as email or cacheing servers typically have more restrictive permissions and will remain in **/Volumes** until resolved manually.

The data written in to a False Mount is typically important, and should be inspected before removal. The creation date and permission settings can help determine the cause of the False Mount, and lend clues to the importance of the data. In the previous example, **Email_Archive** is owned by root. It was created by a privileged service, a mail server in this case, and was intended to be stored on an external volume. Simply removing the False Mount would mean the permanent loss of the archives.

In the case of the poor network connection, the data was intended to be saved to the file server, and may well be the most recent version of the work in progress. Again, reviewing the content of the False Mount before removal can prevent important data loss. The creation date of the False Mounts are an indicator of when connectivity to the server was lost, and may be useful in troubleshooting the root of the issue..

In the end, unmounting the related volume, moving all related folders out of **/Volumes**, and re-mounting the volume will allow the computer to function as intended. Preventing False Mounts is not always possible, discovering them as they occur is the best protection against downtime and data loss.

REDUCE THE PAIN OF FALSE MOUNTS WITH WATCHMAN MONITORING

Catching False Mounts quickly is critical to keeping your end users' data safe. The longer False Mounts go undiscovered, the more difficult and complex they are to unravel. Watchman Monitoring checks for False Mounts as a part of its hourly run, and we have included a step by step for your reference. Watchman Monitoring will tell you the path of False Mount as they are detected. Find it fast. Fix it faster.

FIXING FALSE MOUNTS

1. In Finder, press Shift+Cmd+G (⇧⌘G)
2. Type **/Volumes** into the Go to pane.
3. Press Return (↵) to view the **/Volumes** folder
4. Look for multiple folders with names which match an external drive or network volume.
5. Unmount the actual volume, and move the remaining folders to the Desktop. Those are the False Mounts.
The use of `sudo mv` may be required.
6. Re-mount the external volume and compare its contents to that of the False Mount.
7. Copy the most recent files to the external volume, and dispose of the False Mounts.