

## Re: Moved & Deleted Files

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-02/1237.html>

---

**From:** mugs (mugs\_at\_discussions.microsoft.com)

**Date:** 02/28/05

Date: Mon, 28 Feb 2005 07:47:01 -0800

Thanks for your advice and help. Will try what you have advised.

"Steven L Umbach" wrote:

- > *Since you are experiencing strange behavior be sure to run full virus scan*
- > *on your server. Then check your group memberships including all the*
- > *administrators groups to make sure membership is proper. Verify that the*
- > *share has correct share/ntfs permissions and that the permissions are not*
- > *excessive meaning that only the users that need full control/modify*
- > *permissions have that permission. If you do not have backups the file may be*
- > *recoverable with a third party program. Note that files deleted on a network*
- > *share will not go to the recycle bin on the server.*
- >
- > *For Windows 2000 you can enable auditing of object access in the Local*
- > *Security Policy or Domain Controller Security Policy for domain controllers*
- > *and then audit folders for user access. If your case I would audit just the*
- > *two delete permissions for the users group. Be sure to increase the size of*
- > *your security log in Event Viewer to at least 10MB. Then look for object*
- > *access 560 and 564 events paired by timestamp. You should then be able to*
- > *see who is deleting the files. This is not a user friendly task as you will*
- > *see a lot of seemingly unrelated object access events but if you dig deep*
- > *enough you should find what you need. I pasted an example for what to look*
- > *for. In the example the file deleted was firewalls.doc by user Steve from*
- > *the folder d:\extra. Look for the file name that was deleted in object*
- > *name – not image file name for event 560. Note that both events have the*
- > *same timestamp. Interestingly the event 564 shows that a file was deleted*
- > *but does not actually list the file object, just the same image file name*
- > *as event 560. But taking the information of these two events together shows*
- > *the actual file that was*