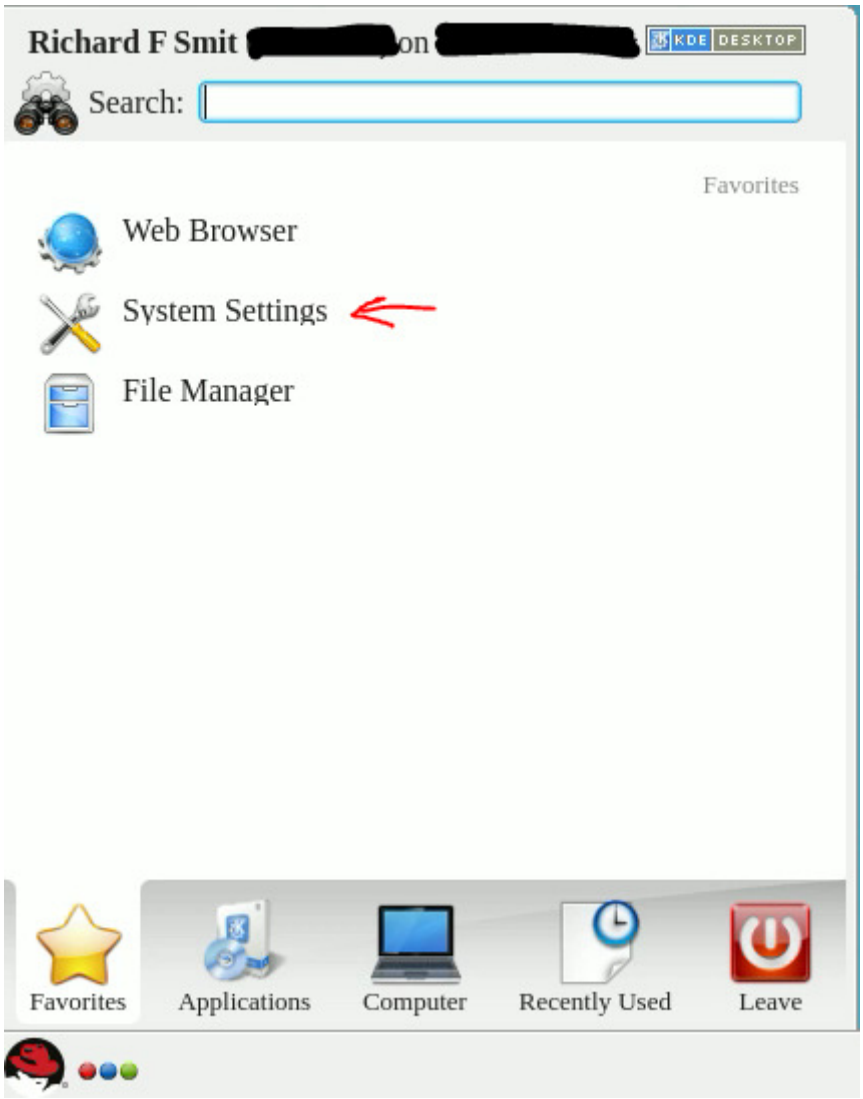
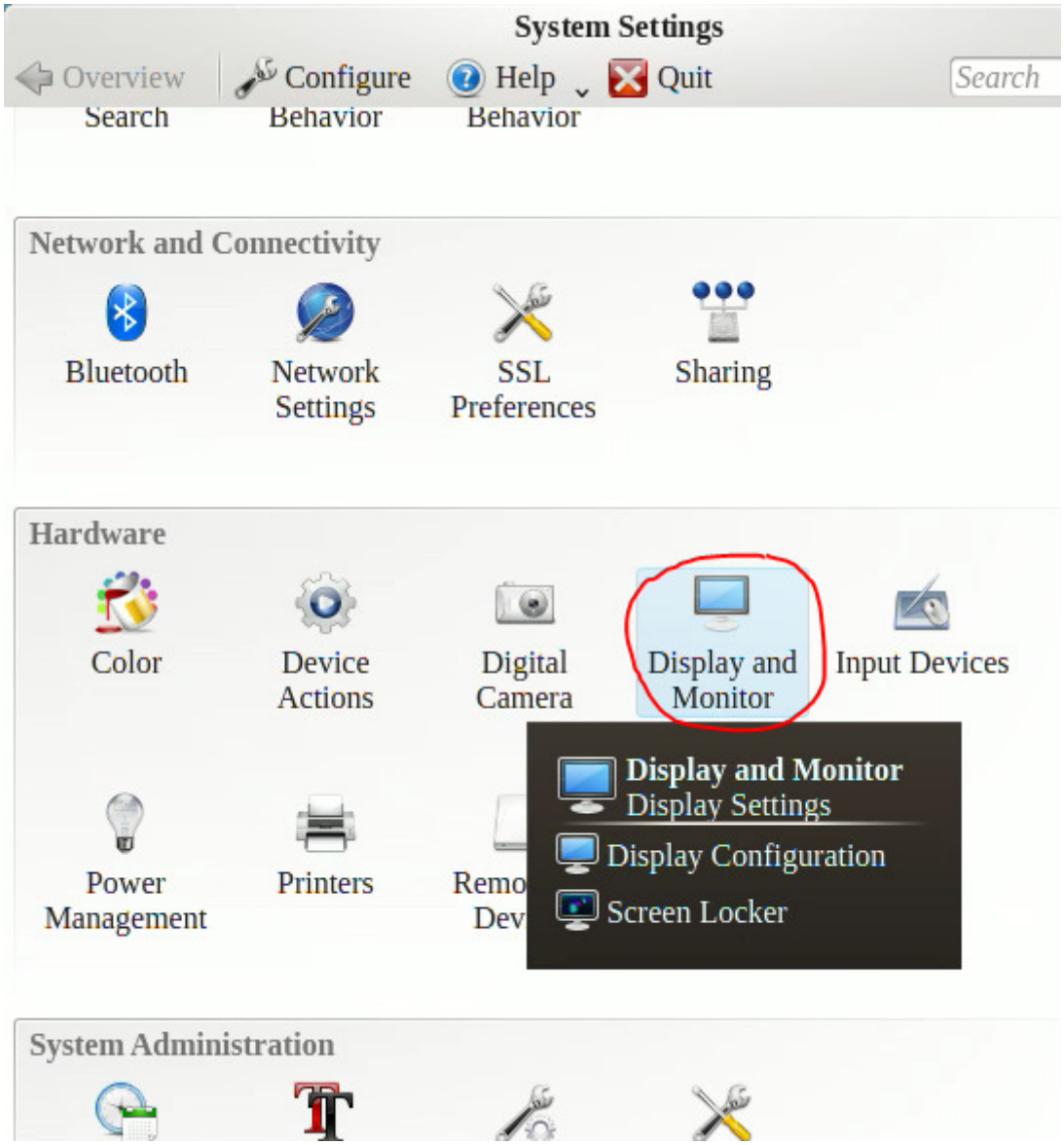
KDE Screenlock insecurity

Log into a system with KDE.

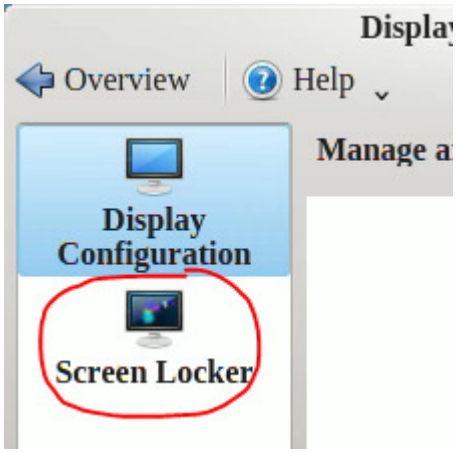
Open the System Settings



From the Hardware section, select the Display and Monitor item

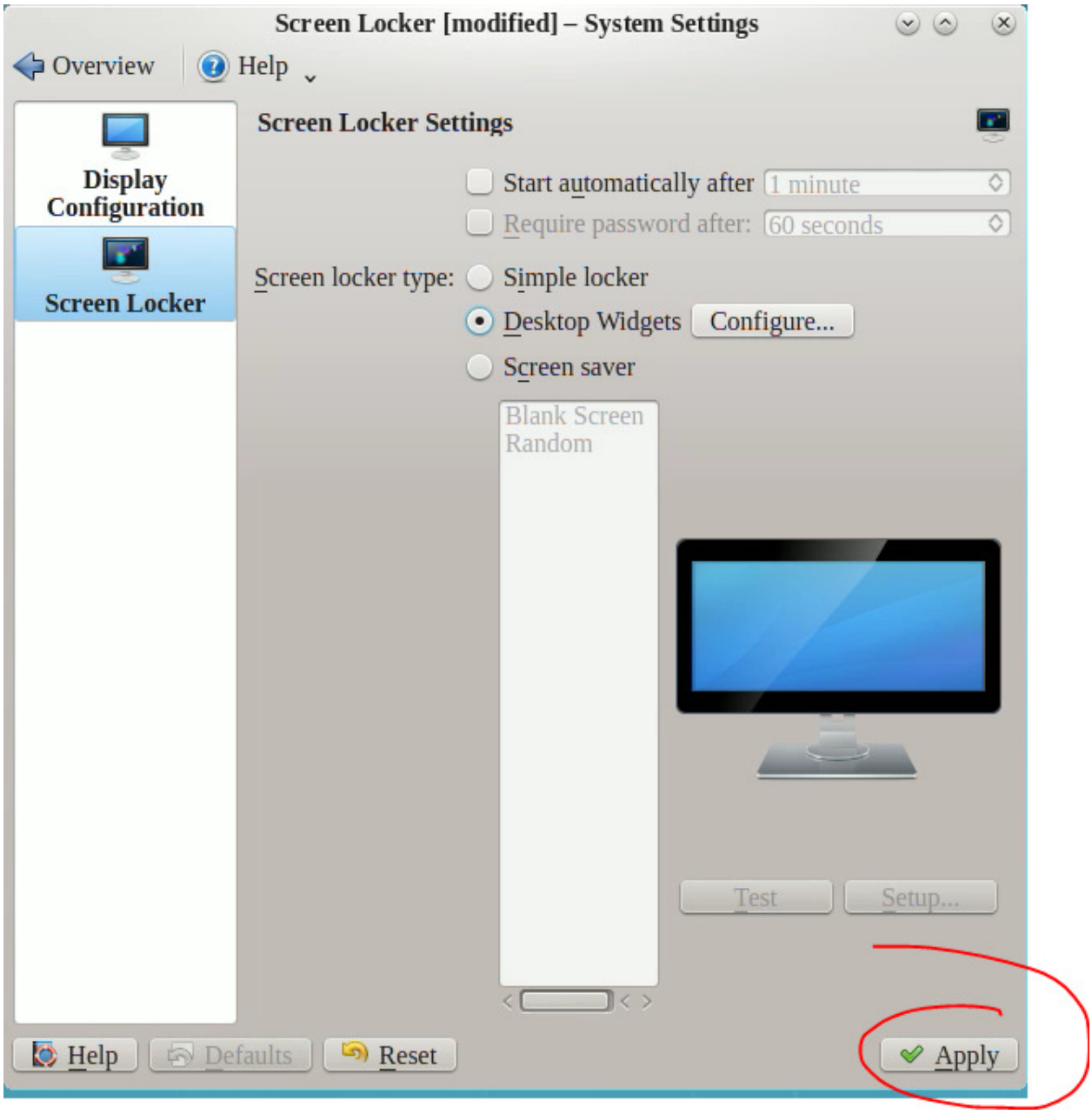


Select the Screen Locker



For the Screen locker type, select Desktop Widgets

And Apply



From the KDE Desktop “cashew” in the upper right of the screen, select Desktop

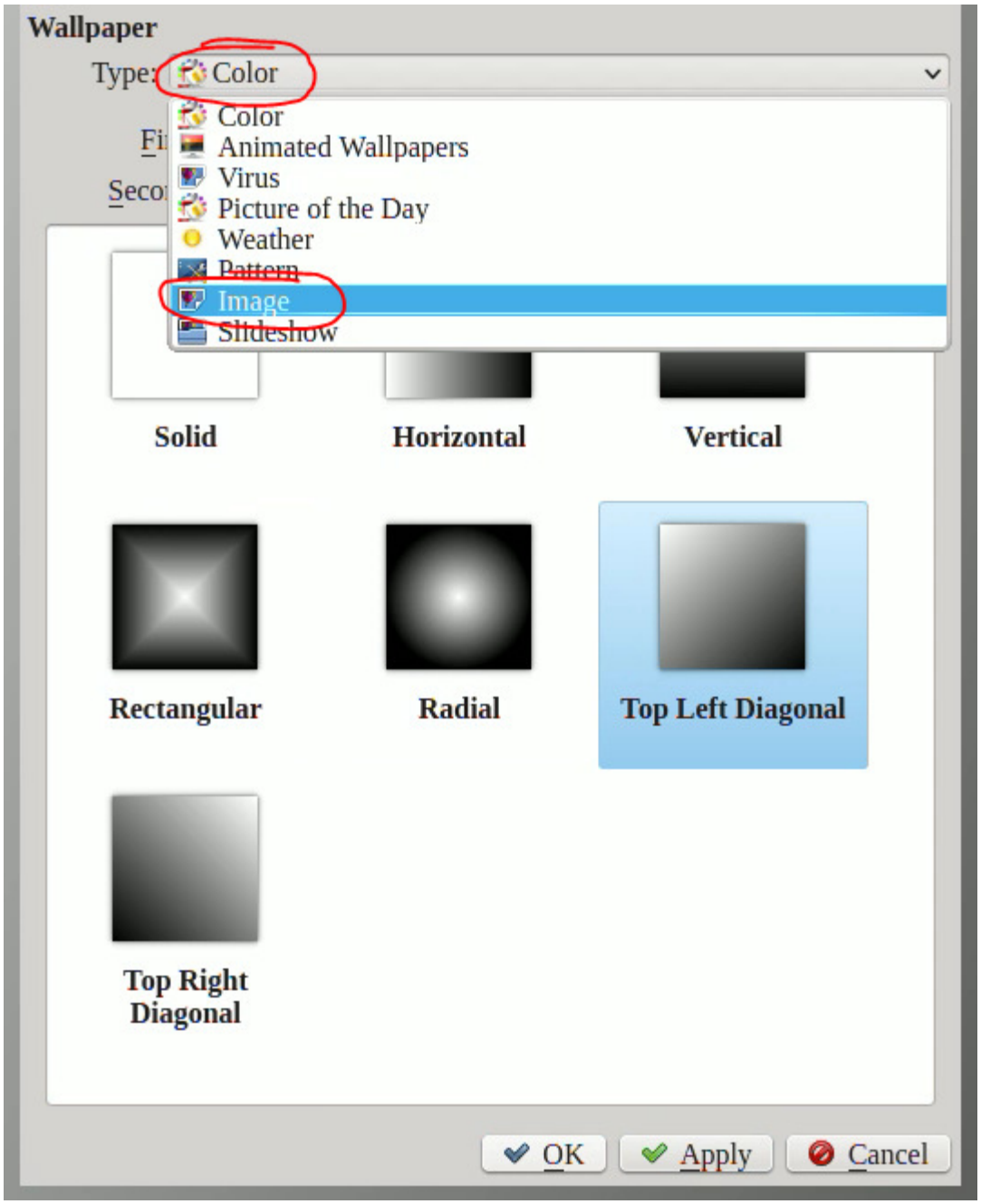
From the dropdown menu, select Lock Screen

With the screen locked, and **without authenticating**, from the KDE Screenlock “cashew” menu in the upper right corner, select Settings

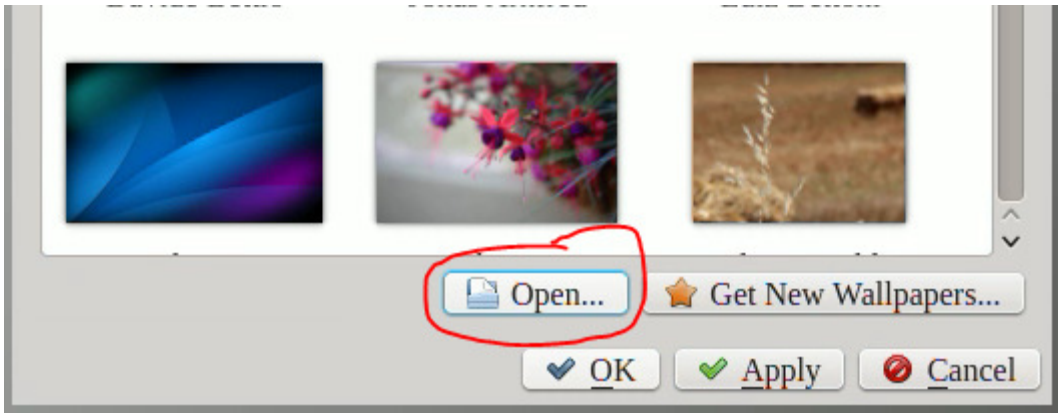
Observe the new dialog window which appears. This is running as the authenticated owner of the screenlock process. The operator was able to launch this dialog window without providing authentication credentials.

Problem 1: unauthenticated operator is able to gain access to authenticated user's preferences.

If it is not already showing "Wallpaper // Type: Image", select "Image" from the dropdown list.



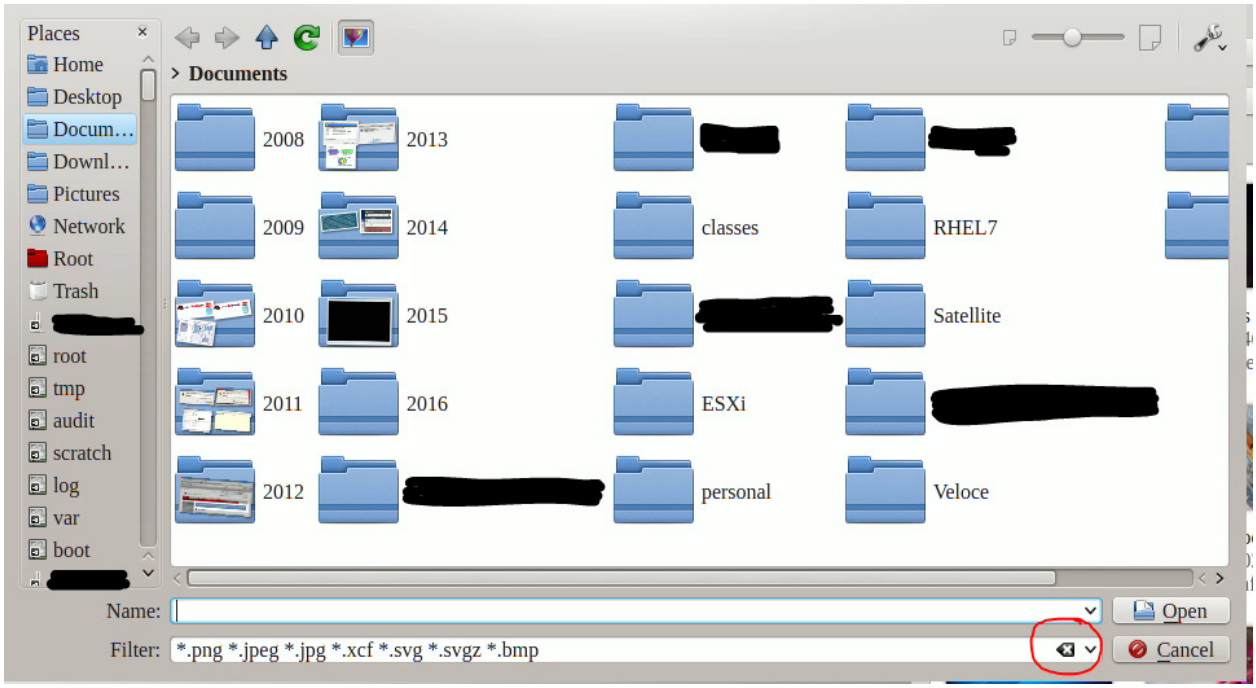
From the lower portion of the dialog, select the Open… button



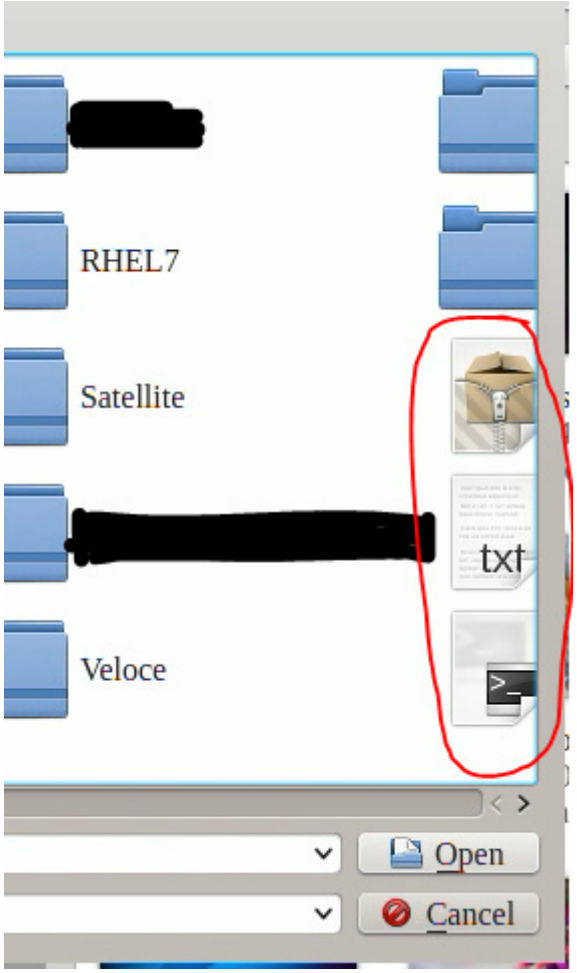
Notice the new file browser window which appears. This starts in the Documents directory of the authenticated owner of the KDE screenlock process.

Problem 2: unauthenticated user is able to browse image files belonging to an authenticated user.

Within the lower part of the file browser, remove the Filter by pressing the backspace icon. (Note: keyboard interaction is blocked by the screenlock.)

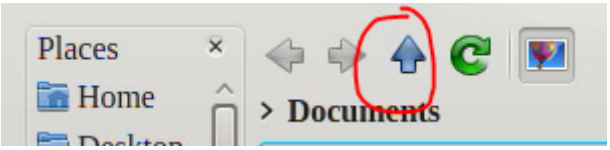


Observe that new non-image file icons appear to the right of the directory icons

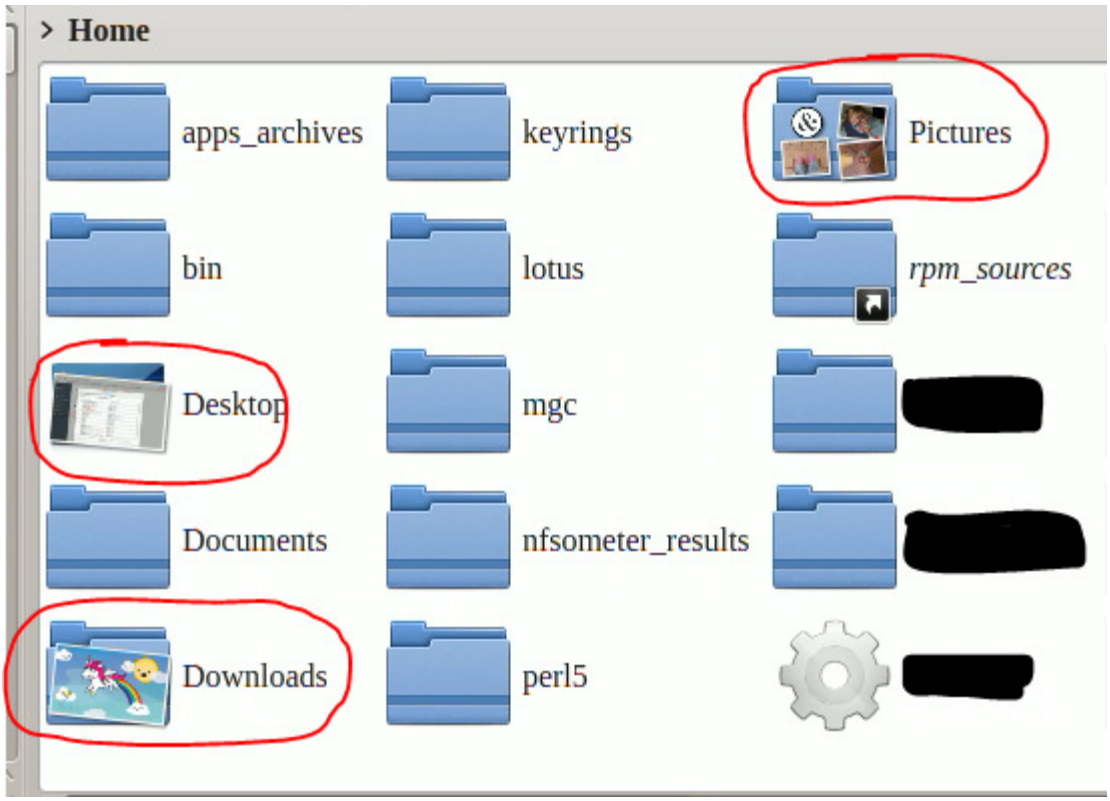


Problem 3: unauthenticated user is provided limited access to authenticated user's non-image files.

Navigate UP to the authenticated owner's homedirectory



Observe that directory icons show thumbnails of image contents.

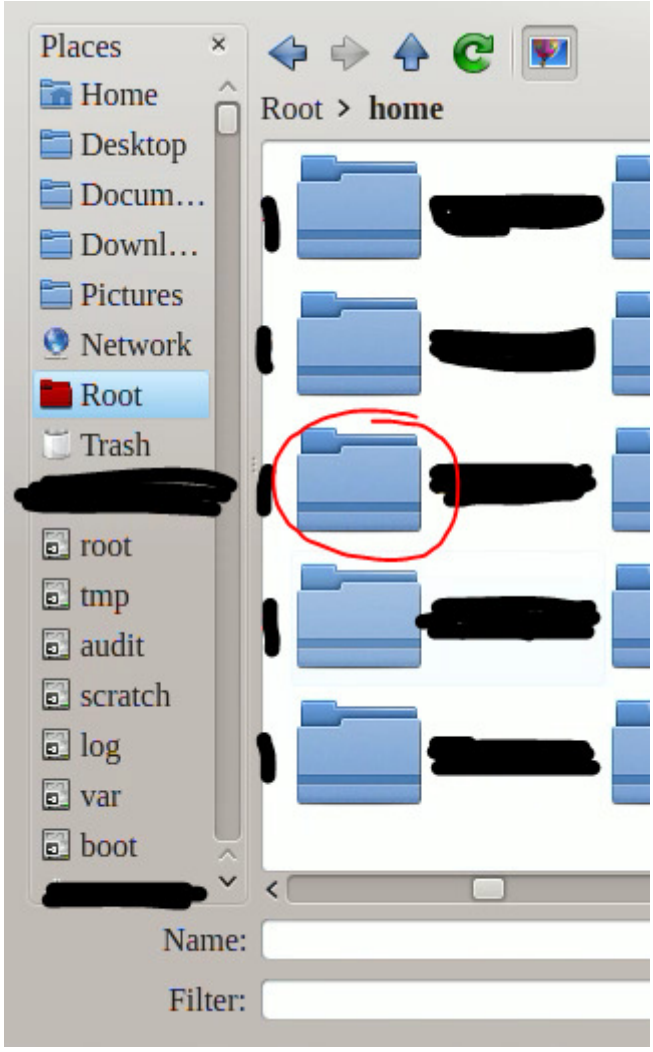


Problem 4: folder thumbnail generation simplifies navigation by unauthenticated user of image files in authenticated user's homedirectory.

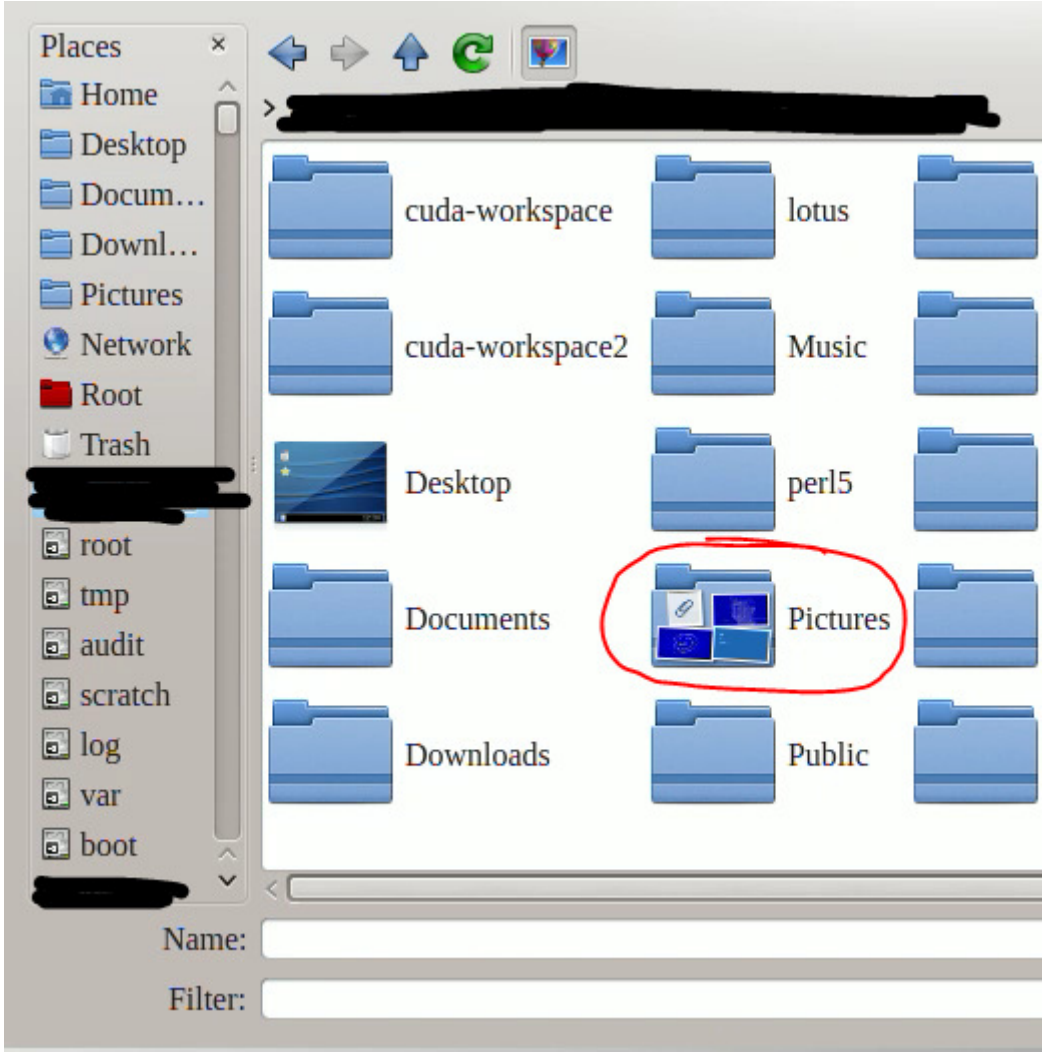
Navigate UP to the automount mountpoint /home

Observe that other users' homedirectories are visible.

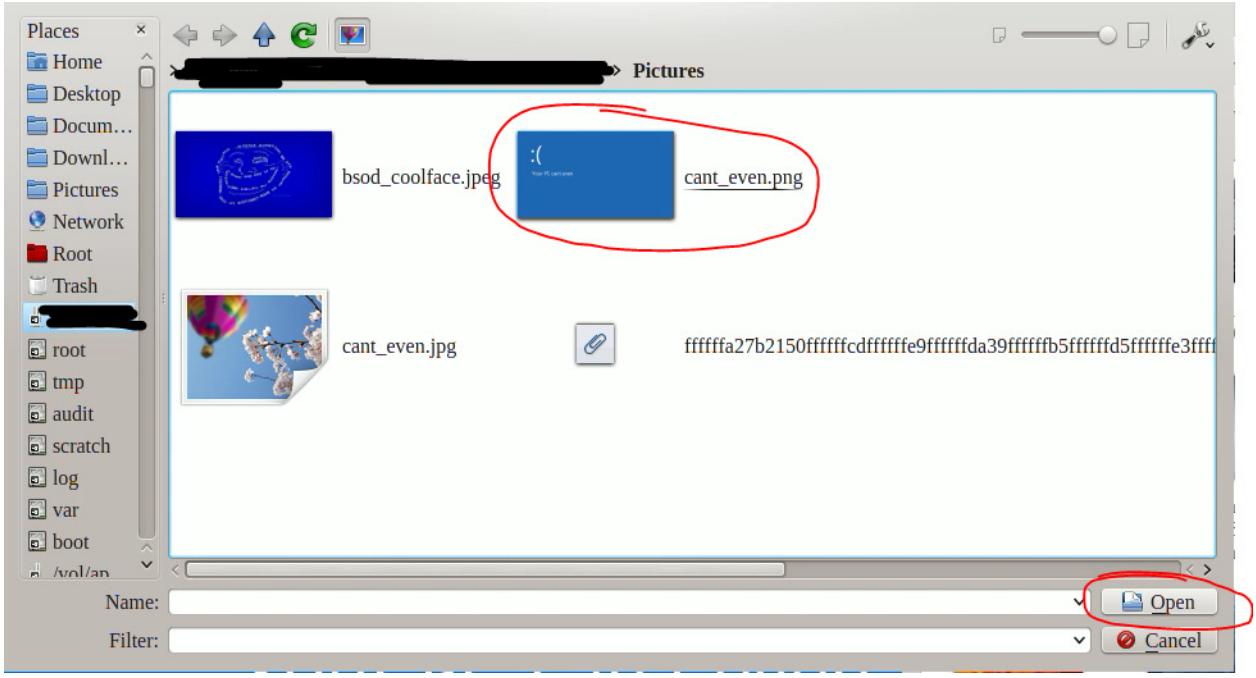
Navigate into another user's homedirectory



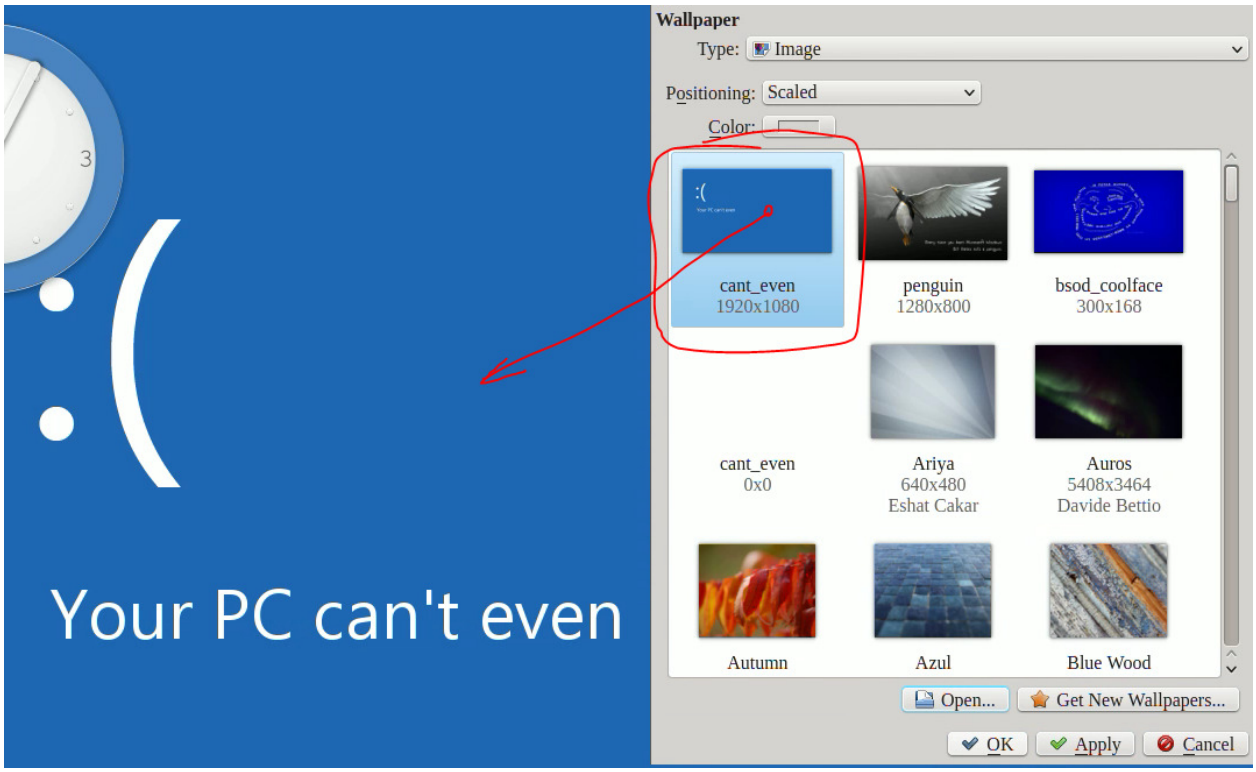
Observe that the other user's publicly readable images show through in the icon of the Pictures directory



Navigate into the other user's Pictures directory, choose a suitable image, and select the Open button



Observe that the image belonging to another user, from that other user's homedirectory, is added to the currently authenticated user's KDE Screenlock Wallpaper choices and set as the current wallpaper.

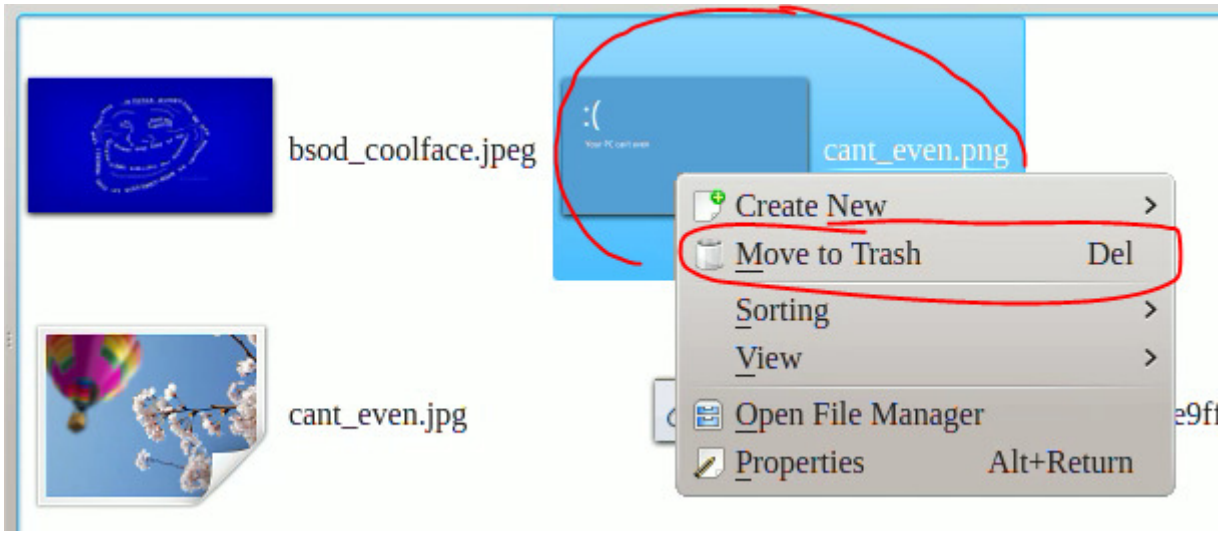


Problem 5: the potential for mischief is enabled by exposing every user's images readable, and every user's files browsable by an appropriately authenticated user, to an unauthenticated user.

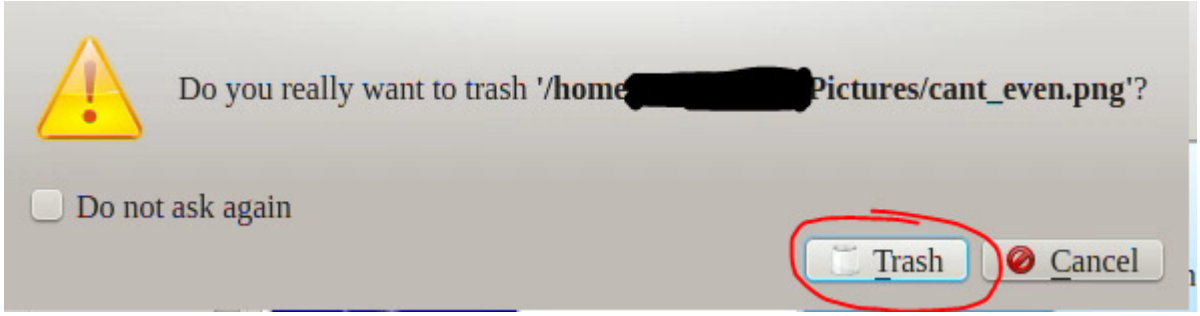
From the Wallpaper choice dialog, press the Open… button again.

Observe that file browsing is resumed at the other user's Pictures directory.

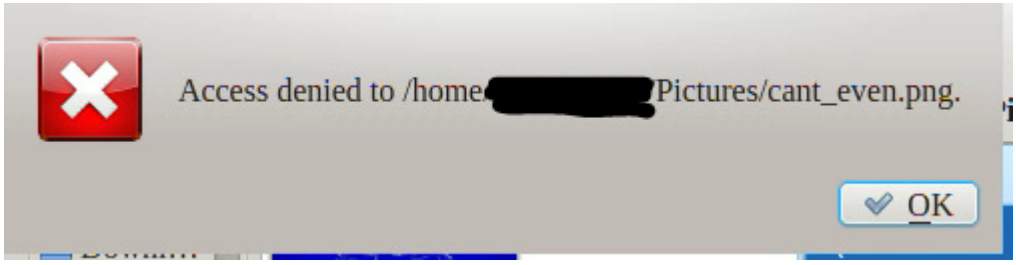
Right-select a file and attempt to Move to Trash



Select Trash



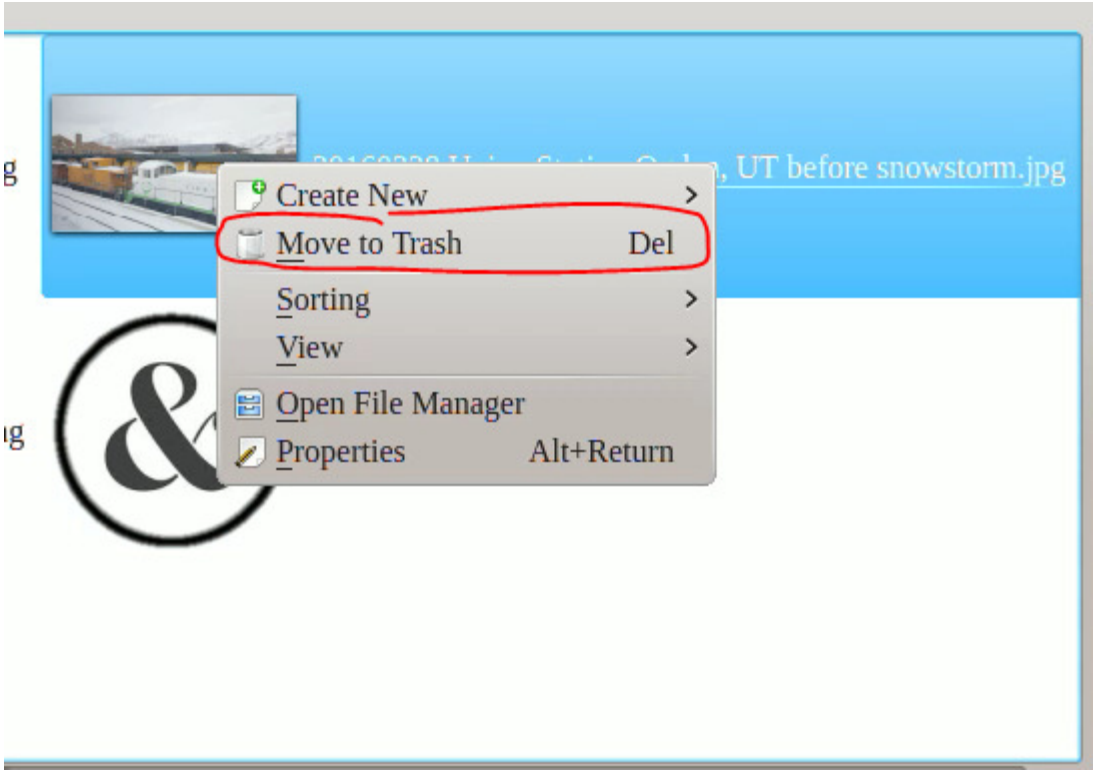
Observe that the system *attempted* but failed to move the image file to the authenticated user's Trash.



Problem 6: the system attempted to move a file to Trash.

In the file browser, return to the authenticated owner of the KDE screenlock process's Pictures directory.

Attempt to delete a picture from there.



Observe that the unauthenticated operator of the KDE screenlock dialog was able to move a file to trash.

Problem 7: unauthenticated operator of KDE Screenlock dialogs was able to trash a file belonging to the authenticated owner of the KDE Screenlock process, which entirely circumvents the purpose of a screen lock program.