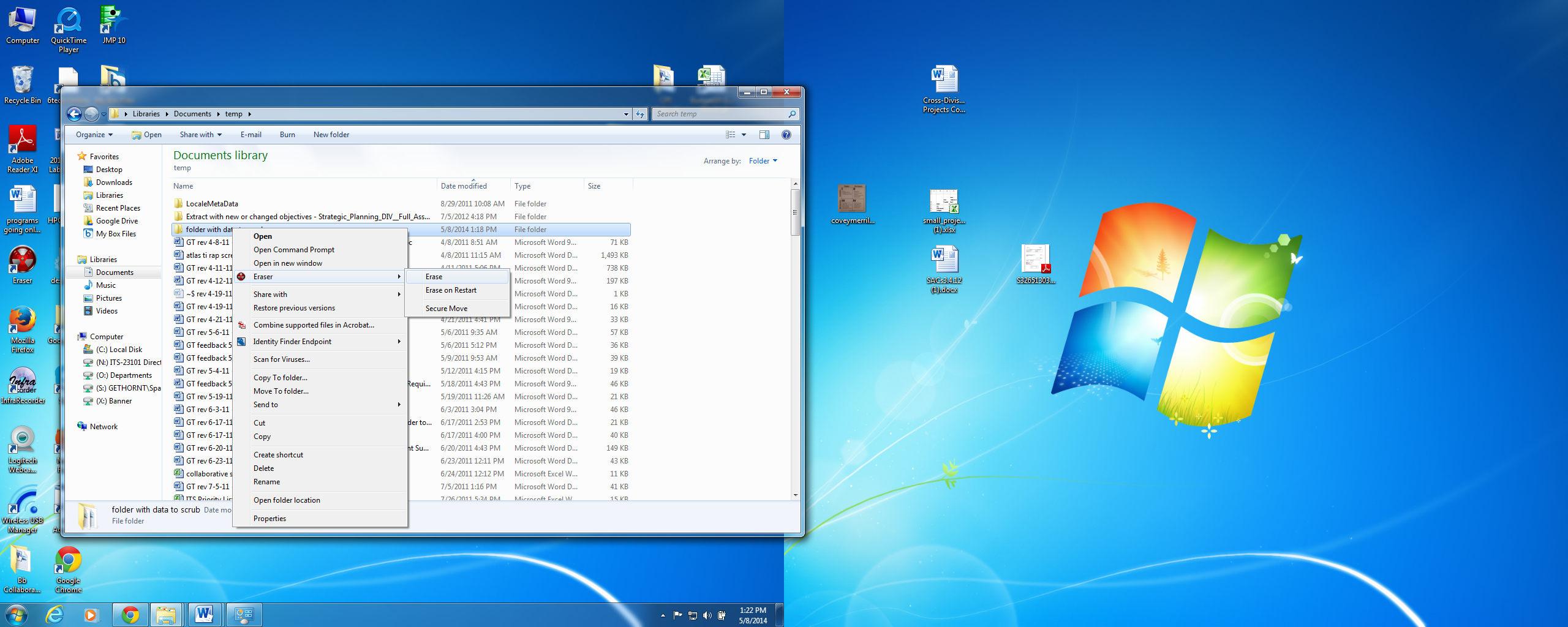
**Securely Erasing (“scrubbing”) Data Files or Folders with Eraser on a Windows Computer**

This document explains how to securely remove selected files or folders from a Windows computer using **Eraser** software.

Computers running the UNCG standard office computer software load (2013-2014) have Eraser pre-installed. If a computer does not have Eraser pre-installed, it may be downloaded from the Eraser website at <http://eraser.heidi.ie/> . This website also contains information regarding why it’s important to use a tool such as Eraser to securely delete files.\*

To securely delete files or folders with Eraser:

1. Select the file(s) or folder(s) to be securely deleted.
2. With the files or folder selected (highlighted), **right click** and select **Eraser** then **Erase** from the pop-up menu (see image below).
3. Click **Yes** when asked to confirm that you want to delete the selected items.
4. You will see a **Task Executed** pop-up message that confirms deletion was successful.



\* From <http://eraser.heidi.ie/> :  
  
**“Your first thought may be that when you ‘delete’ the file, the data is gone. Not quite**, when you delete a file, the operating system does not really remove the file from the disk; it only removes the reference of the file from the file system table. The file remains on the disk until another file is created over it, and even after that, it might be possible to recover data by studying the magnetic fields on the disk platter surface.

Before the file is overwritten, anyone can easily retrieve it with a disk maintenance or an undelete utility.”