

Windows Anti-Forensics Cheat Sheet
http://www.system7.org
v1.2 - April 2010

Don't Hibernate running Windows – from anti-forensics.com... "did you know that by putting your computer into "hibernation" mode you are essentially creating a snapshot of the contents of your computers RAM which is then saved to the root of the hard drive as "hiberfil.sys"?

This means that current running applications and other data in RAM will be written to the hard disk. This is a pretty serious privacy risk and by not using this feature you are in effect implementing an anti-forensics technique."

Disable Hibernation mode on Windows XP:

1. Right-click empty area on desktop
2. Choose "Properties"
3. Select the "Screen Saver" tab
4. Click "Power..."
5. Select the "Hibernate" tab
6. Uncheck "Enable hibernation"

Disable Hibernation mode on Windows 7:

1. Open "Control Panel"
2. Click "Power Options"
3. Click "Change plan settings" for you current power plan
4. Click "Change advanced power settings"
5. Expand "Sleep"
6. Expand "Hibernate after"
7. Enter "0" for "Setting:" to set hibernate to "Never"

Automatically permanently delete (Nuke on Delete)- Normally Delete sends files to the Recycle Bin and a Shift+Delete will permanently delete them. With the registry tweak below the normal Delete will also behave as a permanent delete. ***Note: Delete does not mean a file is deleted. It only frees up the file record and clusters so they could be overwritten.

1. Go to Start -> Run and type Regedit
2. On the left hand side select the "+" to navigate to the following.
3. HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ BitBucket
4. On the right look for NukeOnDelete
5. Right click it and set the key value for NukeOnDelete to 1

Scheduled Task to Zero out unused disk space – As I mentioned above a deleted file only insures that there is a chance the file will be overwritten. If you run the below command it will zero out all unused disk space which should be good enough to prevent file content

recovery. ***Note: The deleted file name will still be lying around until a new file happens to overwrite it.

1. >cipher /W:[directory_to_wipe]
2. i.e. C:\WINDOWS\system32\cmd.exe /c cipher /W:C:\

Scheduled Task to Delete Recent Items – Even if you permanently delete a file and or use Eraser there's a copy of the filename in your Recent directory. I have the following scheduled task command which clears my Recent items once a day....

Task for Recent Items:

1. >C:\WINDOWS\system32\cmd.exe /c del "c:\documents and settings\[username]\recent*.lnk"
2. Task for Recent Office Items:
3. >C:\WINDOWS\system32\cmd.exe /c del /Q "C:\Documents and Settings\[username]\Application Data\Microsoft\Office\Recent*.*)"
4. [Eraser](#)

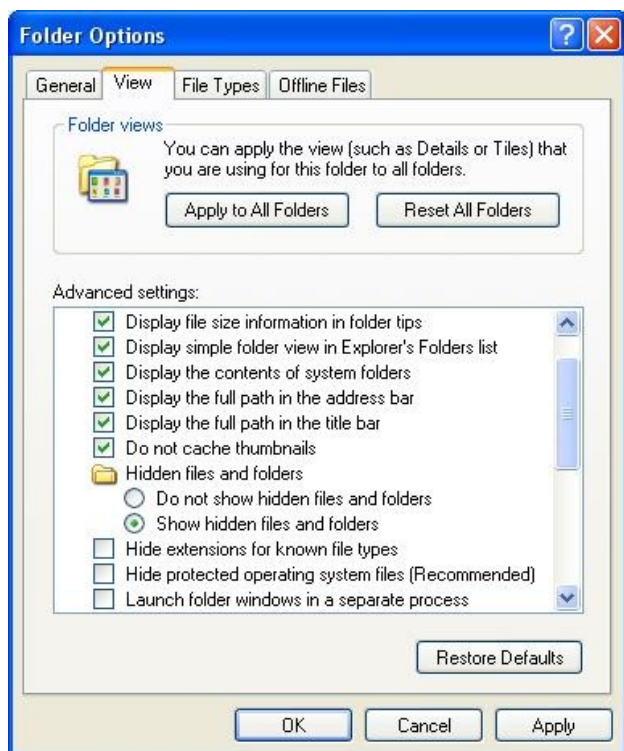
Do not cache thumbnails (thumbs.dat) - (<http://www.anti-forensics.com>)

The thumbs.db file on a Windows system can be a treasure chest of 96 x 96 pixel artifacts. By default, a thumbs.db file is created in folders viewed in the thumbnail view which contain jpegs, bitmaps, GIFs, PNGs and other files.

These thumbs.db files are very useful to forensic examiners because they can contain thumbnails of pictures and other media which currently exist and previously existed in the same directory as the thumbs.db file."

It's very easy to disable thumbnail caching on a Windows system so that existing thumbs.db files are not updated with new thumbnails and new thumbs.db files are prevented from being created. Just follow the instructions below.

1. Open explorer
2. Click the "Tools" menu
3. Choose "Folder Options..."
4. Select the "View" tab
5. Under "Files and Folders" checkmark "Do not cache thumbnails"



Do not cache thumbnails

The actual registry key value that is modified which you can change manually is located here:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Modify the value: DisableThumbnailCache

Remember that you have only disabled thumbnail caching and any previous thumbs.db files still exist on the system. To find these files you can run a simple search from explorer for the file name "Thumbs.db".

Links:

- <http://www.anti-forensics.com>
- <http://www.irongeek.com/i.php?page=videos/anti-forensics-occult-computing>
-