Windows System File Locations

Prefetch Folder

- %SystemRoot%\Windows\Prefetch\
- Prefetch files have a .pf file extension.

User Profile Locations

- Windows XP: %SystemRoot%\Documents and Settings\
- Windows Vista, 7, 8, 10: %SystemRoot%\Users\

System Restore Points

- %SystemRoot%\System Volume Information\
- System Restore Points do not include user data files.

Volume Shadow Copies

- %SystemRoot%\System Volume Information\
- Volume Shadow Copies backup system and user data files.
- Command to access shadow copies: vssadmin list shadows /for=[VolumeLetter]
- Command to acquire data from copies: mklink /D [TARGET DIR] [COPY VOLUME]\

Temporary Files

- %SystemRoot%\Windows\Temp
- Temp filenames often start with ~ with a file extension of .tmp

Hosts File

- %SystemRoot%\Windows\System32\drivers\etc
- Filename: hosts

Page File

- %SystemRoot%\
- Used as if it was physical memory when the system is low on RAM
- Filename: Pagefile.sys

Hibernation File

- %SystemRoot%\
- Filename: hiberfil.sys

Shimcache

- HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache

Recycle Bin

- Windows XP: %SystemRoot%\Recycler\%SID%\
- Windows Vista & Above: %SystemRoot%\$Recycle.Bin\%SID%\

Windows Event Logs

- Windows XP: %SystemRoot%\System32\Config*.evt
- Windows Vista & Above: %SystemRoot%\Windows\System32\winevt\Logs*.evtx

NT Directory Services (Active Directory)

- Windows Server 2000: %SystemRoot%\ntds\
- Windows Server 2003 and %SystemRoot%\Windows\ntds\