2.3 Registry Operations

* PowerShell has the ability to query and modify the registry
* Multiple methods available for access
* PowerShell Drive mappings
  + Get-PSDrive
  + HKCU (HKey Current User)
  + HKLM (HKey Local Machine)
* Using PSDrives
  + Set-Location HKLM:
  + CD HKLM:\
* Keys can be handled like files
  + copy (Copy-Item)
  + dir (Get-ChildItem)
  + delete (Remove-Item)
* Examples of listing a registry key:
  + Get-ChildItem "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
  + Get-ChildItem -Path "Microsoft.PowerShell.Core\Registry::HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
* Changing your "directory" can help eliminate the need to type in long paths - Set-Location "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"  
  Get-ChildItem
* Listing existing registry entries
  + Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name DefaultDomainName -PropertyType String -Value ITPROTVNET
  + Set-Location "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"  
    Get-ItemProperty -Path .\
  + Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name DefaultDomainName
  + You cannot truly filter by property name
  + Property names represent virtual directories, not actual properties
  + You have to be a little creative to return one individual value
  + (Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name DefaultDomainName).DefaultDomainName
* Deleting a registry entry
  + Remove-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name DefaultDomainName
* Creating a registry entry
  + New-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name DefaultDomainName -PropertyType String -Value VIKARLEARNINGPOWERSHELL
  + Set-Location "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"  
    New-ItemProperty -Name DefaultDomainName -PropertyType String -Value VIKARLEARNINGPOWERSHELL