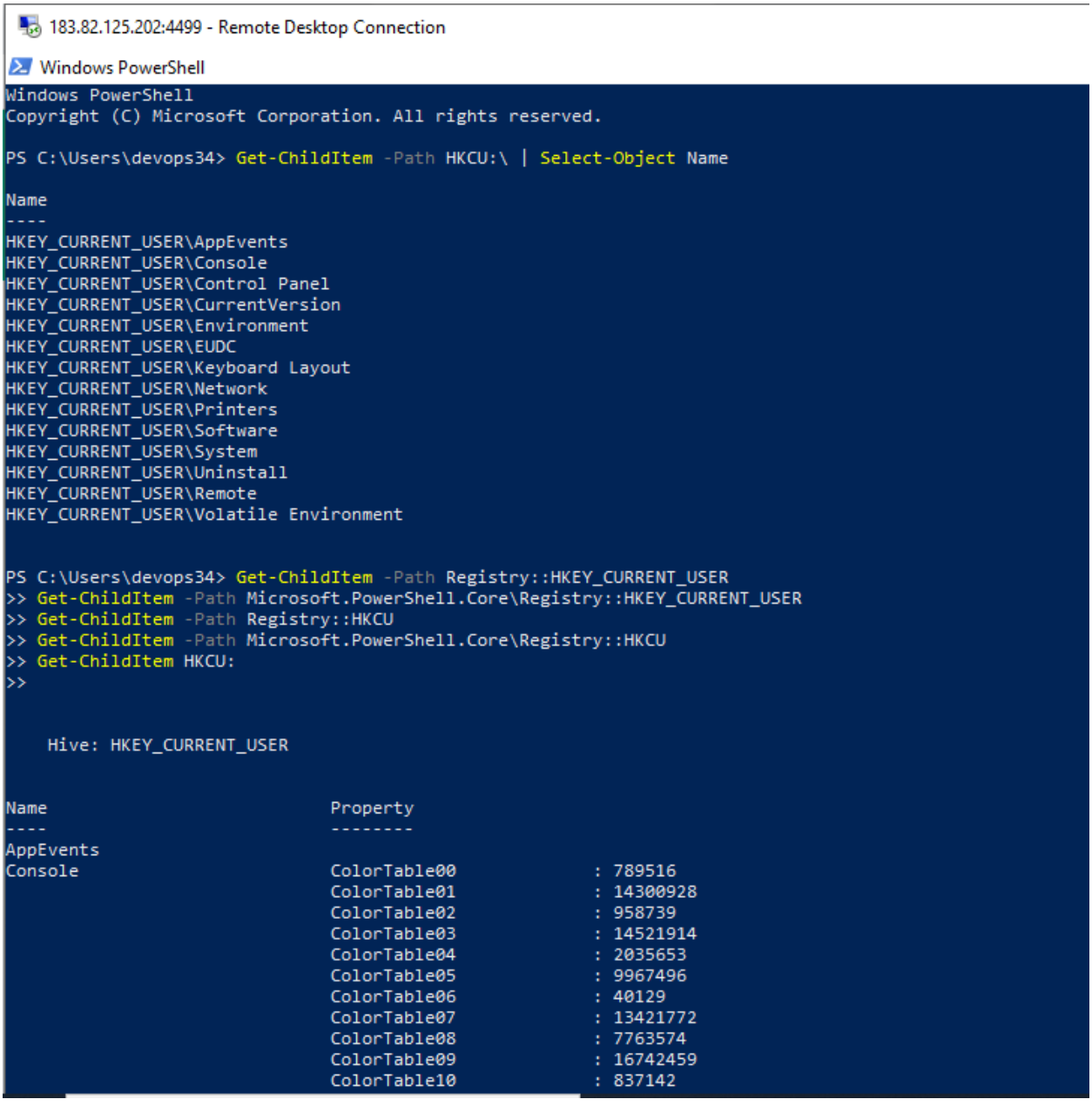
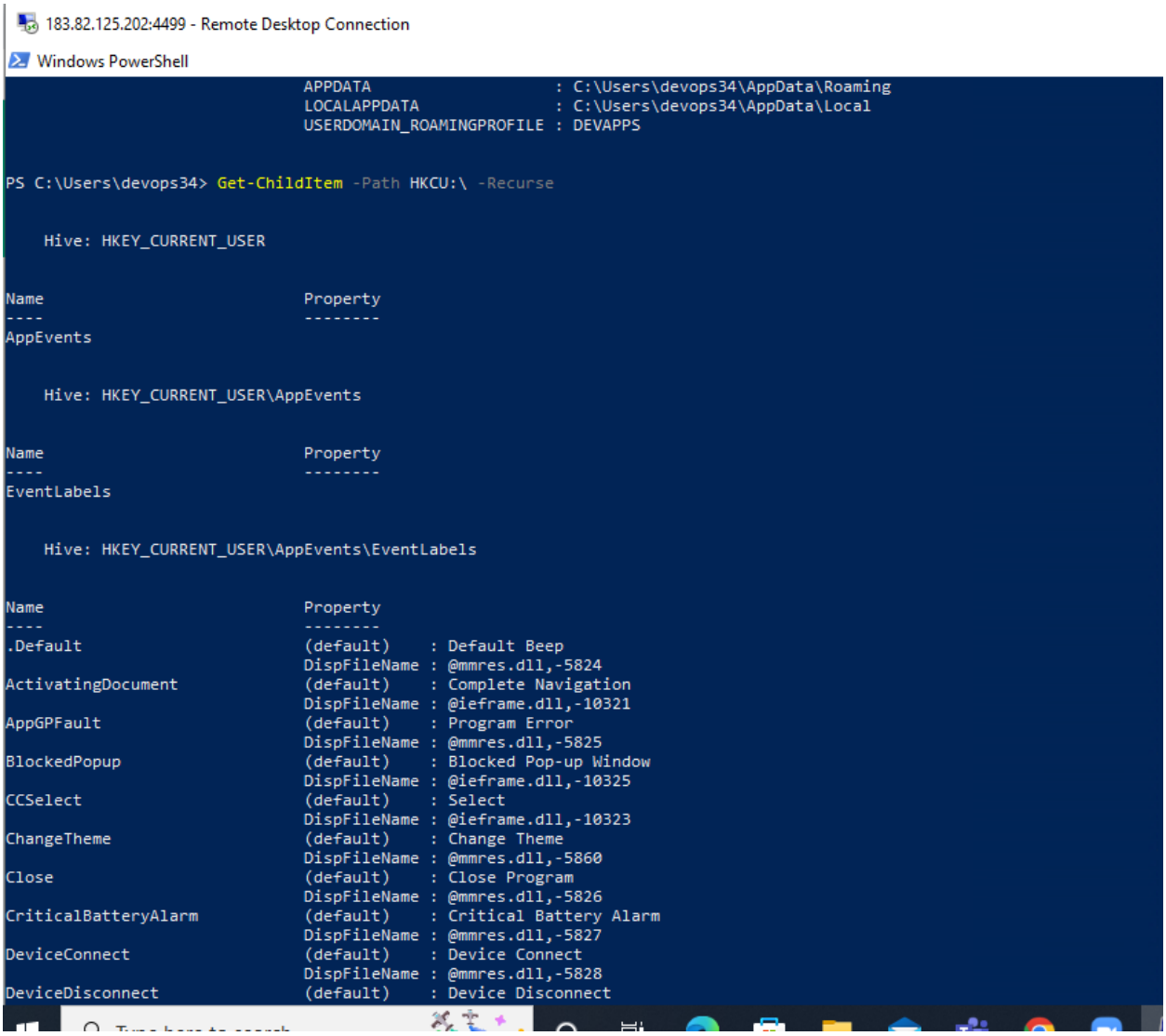
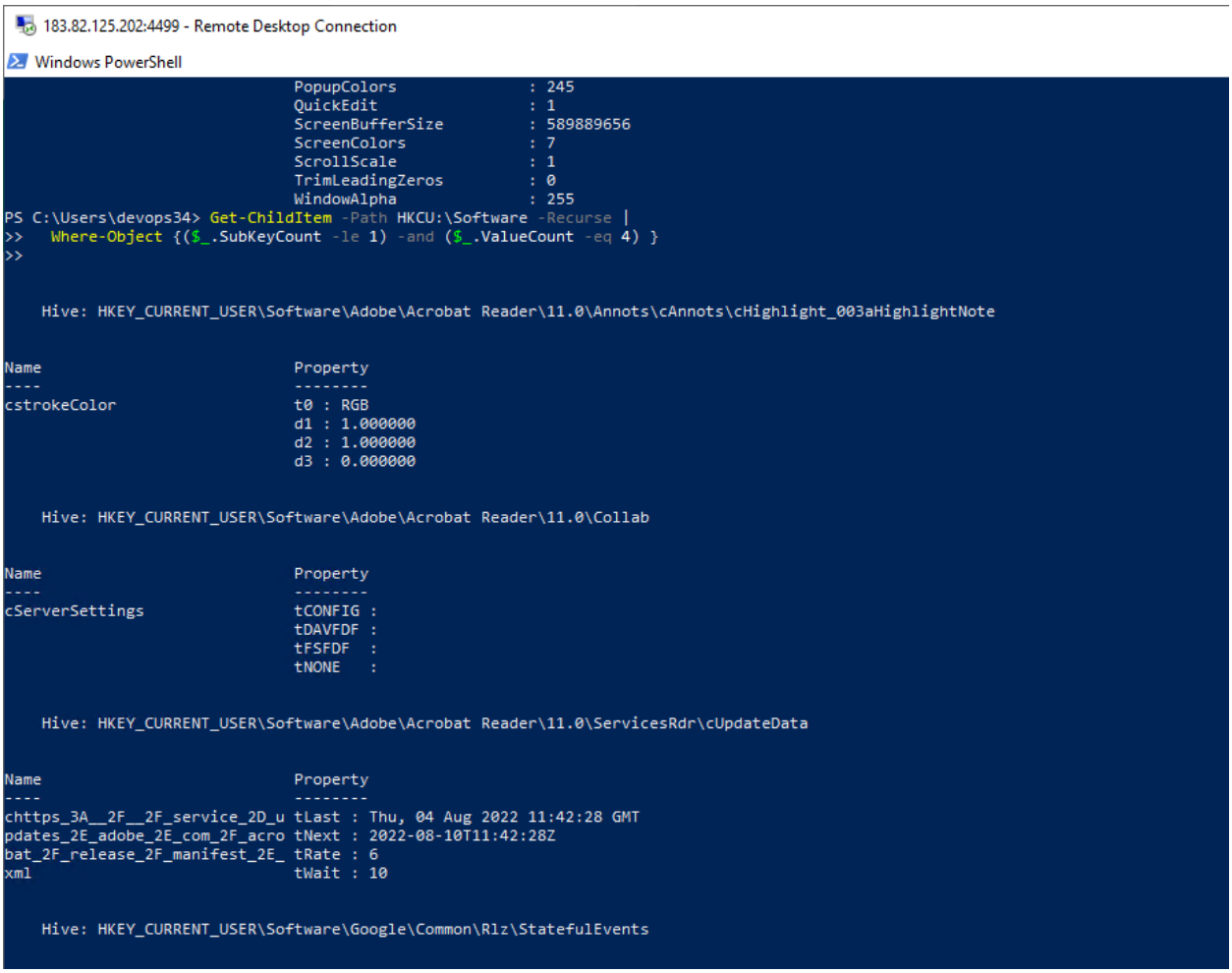
Working with Registry Keys

Output Screenshots:




183.82.125.202:4499 - Remote Desktop Connection
Windows PowerShell
APPDATA : C:\Users\devops34\AppData\Roaming
LOCALAPPDATA : C:\Users\devops34\AppData\Local
USERDOMAIN_ROAMINGPROFILE : DEVAPPS
PS C:\Users\devops34> Get-ChildItem -Path HKCU:\ -Recurse
Hive: HKEY_CURRENT_USER
Name Property
AppEvents
Hive: HKEY_CURRENT_USER\AppEvents
Name Property
EventLabels
Hive: HKEY_CURRENT_USER\AppEvents\EventLabels
Name Property
.Default (default) : Default Beep
DispFileName : @mmres.dll,-5824
ActivatingDocument (default) : Complete Navigation
DispFileName : @ieframe.dll,-10321
AppGPFault (default) : Program Error
DispFileName : @mmres.dll,-5825
BlockedPopup (default) : Blocked Pop-up Window
DispFileName : @ieframe.dll,-10325
CCSelect (default) : Select
DispFileName : @ieframe.dll,-10323
ChangeTheme (default) : Change Theme
DispFileName : @mmres.dll,-5860
Close (default) : Close Program
DispFileName : @mmres.dll,-5826
CriticalBatteryAlarm (default) : Critical Battery Alarm
DispFileName : @mmres.dll,-5827
DeviceConnect (default) : Device Connect
DispFileName : @mmres.dll,-5828
DeviceDisconnect (default) : Device Disconnect


183.82.125.202:4499 - Remote Desktop Connection
Windows PowerShell
PopupColors : 245
QuickEdit : 1
ScreenBufferSize : 589889656
ScreenColors : 7
ScrollScale : 1
TrimLeadingZeros : 0
WindowAlpha : 255
PS C:\Users\devops34> Get-ChildItem -Path HKCU:\Software -Recurse |
>> Where-Object {($_.SubKeyCount -le 1) -and ($_.ValueCount -eq 4) }
>>
Hive: HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\11.0\Annots\cAnnots\cHighlight_003aHighlightNote
Name Property
cstrokeColor t0 : RGB
d1 : 1.000000
d2 : 1.000000
d3 : 0.000000
Hive: HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\11.0\Collab
Name Property
cServerSettings tCONFIG :
tDAVFDF :
tFSFDF :
tNONE :
Hive: HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\11.0\ServicesRdr\cUpdateData
Name Property
chttps_3A__2F__2F_service_2D_u tLast : Thu, 04 Aug 2022 11:42:28 GMT
pdates_2E_adobe_2E_com_2F_acro tNext : 2022-08-10T11:42:28Z
bat_2F_release_2F_manifest_2E_ tRate : 6
xml tWait : 10
Hive: HKEY_CURRENT_USER\Software\Google\Common\Rlz\StatefulEvents

183.82.125.202:4499 - Remote Desktop Connection

Windows PowerShell

```
0EB058B}                        EditorGUID  : {25B02EE5-DB4E-48bd-A9BB-4FD280EB058B}
                                Package     : {1B437D20-F8FE-11D2-A6AE-00104BCC7269}
                                (default)   : WebUserControl Editor with Encoding
{29947C11-E110-4596-85B8-42A21 DisplayName : #20118
EF46F6B}                        EditorGUID  : {29947C11-E110-4596-85B8-42A21EF46F6B}
                                Package     : {1B437D20-F8FE-11D2-A6AE-00104BCC7269}
                                (default)   : Script Editor with Encoding
{31F89F6D-9A71-4484-B2A0-DCDE9 (default)   : DAX Query Editor with Encoding
FEC7AD5}                        DisplayName : #8
                                Package     : {4058755A-8FBE-41C7-BC99-3DBF5C74BA62}
                                EditorGUID  : {ADBD55DE-75C9-41CC-9032-8389A12D5856}
PS C:\Users\devops34> Copy-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion' -Destination HKCU:
PS C:\Users\devops34> Copy-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion' -Destination HKCU: -Recurse
Copy-Item : Requested registry access is not allowed.
At line:1 char:1
+ Copy-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion' -De ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (HKEY_LOCAL_MACH...\CurrentVersion:String) [Copy-Item], SecurityException
    + FullyQualifiedErrorId : System.Security.SecurityException,Microsoft.PowerShell.Commands.CopyItemCommand

PS C:\Users\devops34> New-Item -Path HKCU:\Software_DeleteMe


    Hive: HKEY_CURRENT_USER


Name                           Property
----                           --------
Software_DeleteMe


PS C:\Users\devops34> New-Item -Path Registry::HKCU\Software_DeleteMe
New-Item : A key in this path already exists.
At line:1 char:1
+ New-Item -Path Registry::HKCU\Software_DeleteMe
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceExists: (Microsoft.Power...RegistryWrapper:RegistryWrapper) [New-Item], IOException
    + FullyQualifiedErrorId : System.IO.IOException,Microsoft.PowerShell.Commands.NewItemCommand

PS C:\Users\devops34> Remove-Item -Path HKCU:\Software_DeleteMe
>> Remove-Item -Path 'HKCU:\key with spaces in the name'
>>
Remove-Item : Cannot find path 'HKCU:\key with spaces in the name' because it does not exist.
At line:2 char:1
+ Remove-Item -Path 'HKCU:\key with spaces in the name'
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (HKCU:\key with spaces in the name:String) [Remove-Item], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.RemoveItemCommand
```

183.82.125.202:4499 - Remote Desktop Connection

Windows PowerShell

```
    Hive: HKEY_CURRENT_USER


Name                           Property
----                           --------
Software_DeleteMe


PS C:\Users\devops34> New-Item -Path Registry::HKCU\Software_DeleteMe
New-Item : A key in this path already exists.
At line:1 char:1
+ New-Item -Path Registry::HKCU\Software_DeleteMe
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceExists: (Microsoft.Power...RegistryWrapper:RegistryWrapper) [New-Item], IOException
    + FullyQualifiedErrorId : System.IO.IOException,Microsoft.PowerShell.Commands.NewItemCommand

PS C:\Users\devops34> Remove-Item -Path HKCU:\Software_DeleteMe
>> Remove-Item -Path 'HKCU:\key with spaces in the name'
>>
Remove-Item : Cannot find path 'HKCU:\key with spaces in the name' because it does not exist.
At line:2 char:1
+ Remove-Item -Path 'HKCU:\key with spaces in the name'
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (HKCU:\key with spaces in the name:String) [Remove-Item], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.RemoveItemCommand

PS C:\Users\devops34> Remove-Item -Path HKCU:\CurrentVersion

Confirm
The item at HKCU:\CurrentVersion has children and the Recurse parameter was not specified. If you continue, all children will be removed with the item. Are you sure you want to continue?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
PS C:\Users\devops34> Remove-Item -Path HKCU:\CurrentVersion -Recurse
Remove-Item : Cannot find path 'HKCU:\CurrentVersion' because it does not exist.
At line:1 char:1
+ Remove-Item -Path HKCU:\CurrentVersion -Recurse
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (HKCU:\CurrentVersion:String) [Remove-Item], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.RemoveItemCommand

PS C:\Users\devops34> Remove-Item -Path HKCU:\CurrentVersion\* -Recurse
Remove-Item : Cannot find path 'HKCU:\CurrentVersion' because it does not exist.
At line:1 char:1
+ Remove-Item -Path HKCU:\CurrentVersion\* -Recurse
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (HKCU:\CurrentVersion:String) [Remove-Item], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.RemoveItemCommand
```