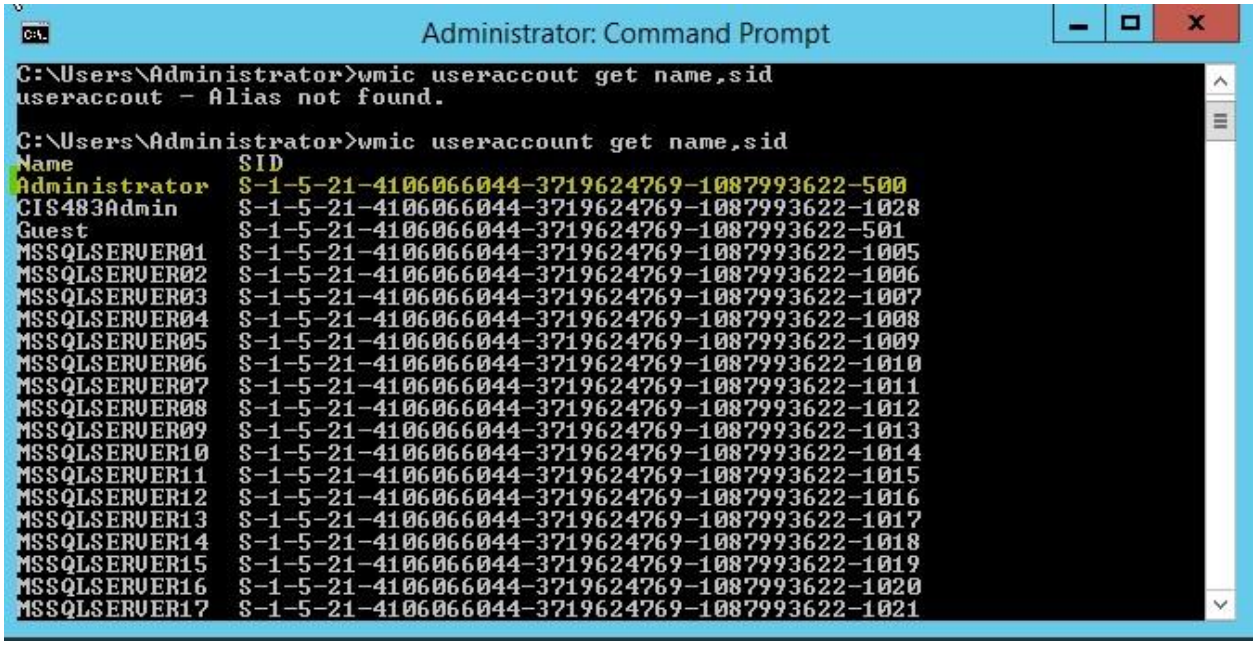
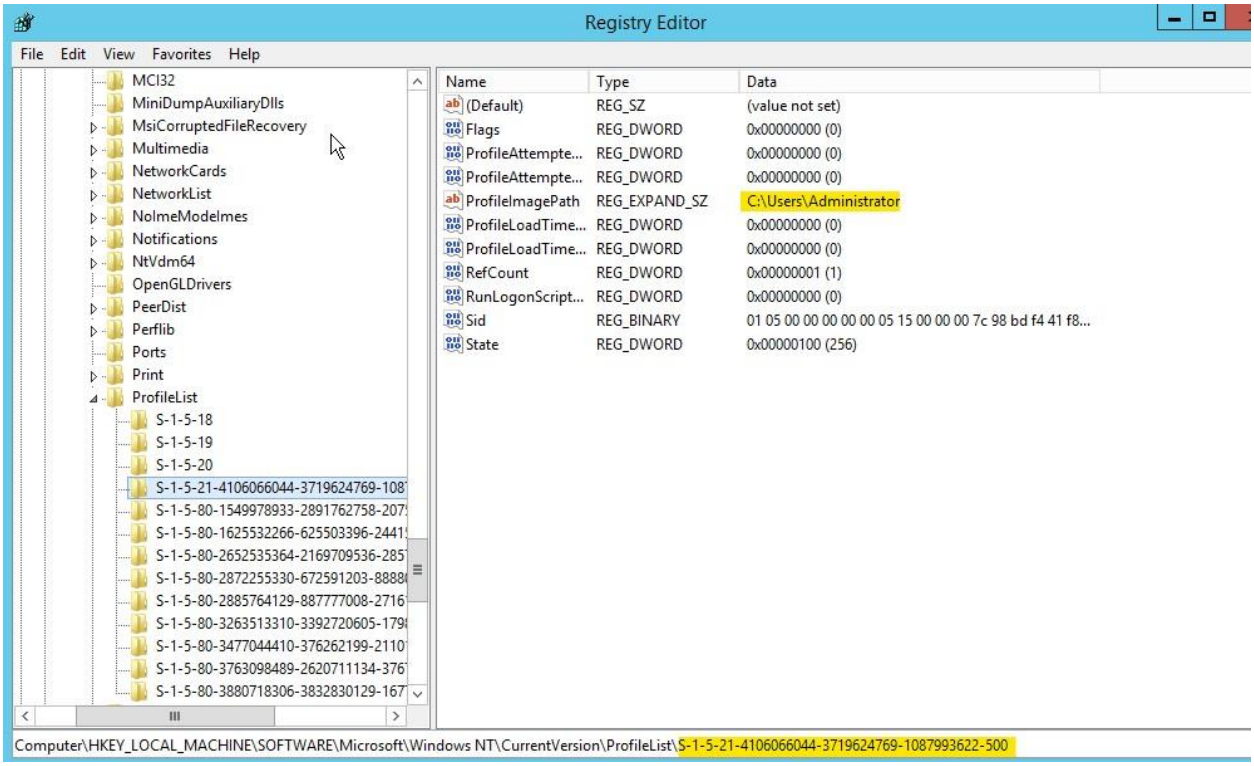
Lab 4 – SID, PowerShell

Task 1: Getting SID, SAT on Windows

- Obtain the SID of the current login with **WMIC** command. Attach a screenshot for the SID and highlight it in red/yellow.



- Obtain the SID of the current login in the Registry. Attach a screenshot for the SID and highlight it in red/yellow.



Task 2: Getting SID on SQL Server

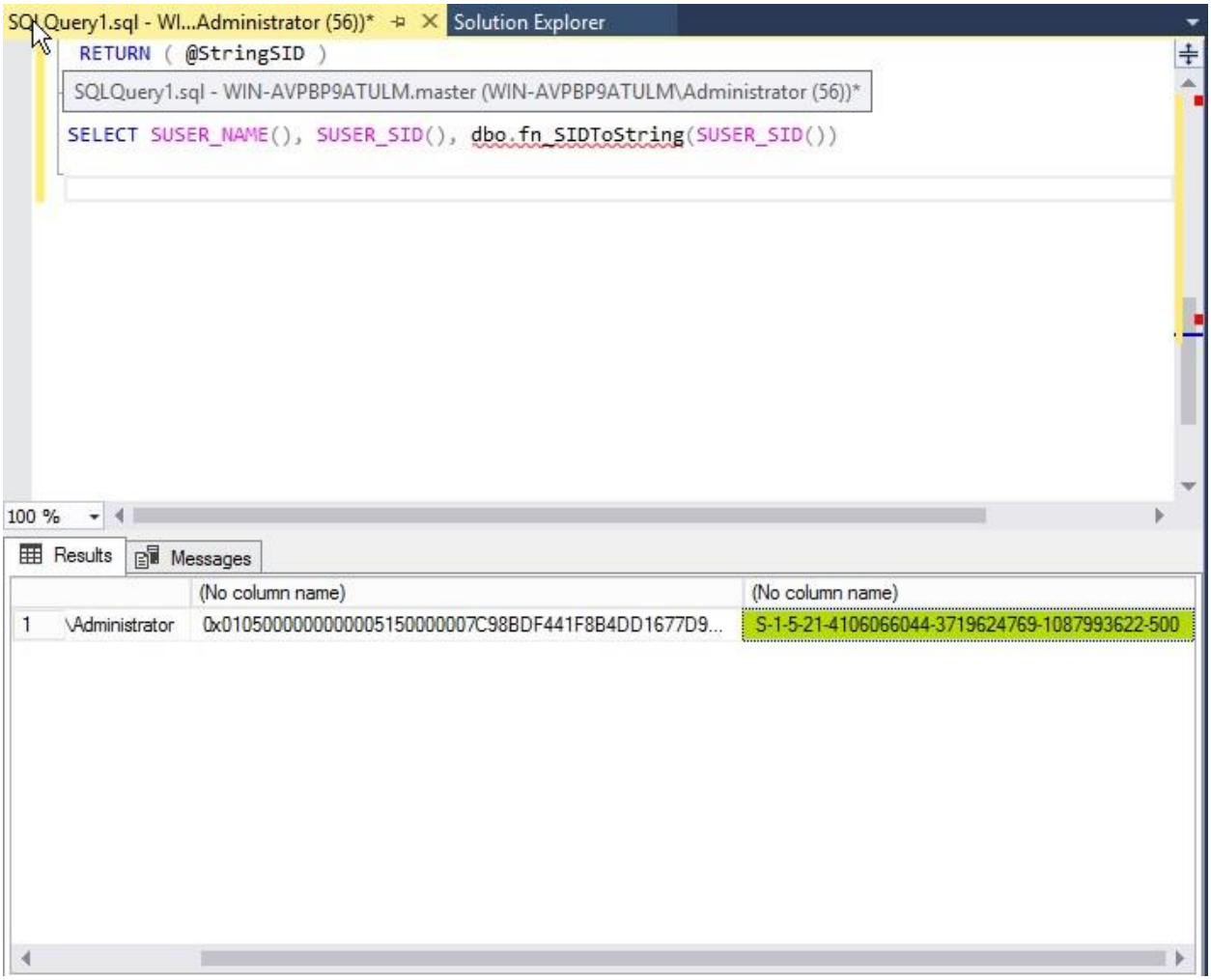
Get the SID of the account you used for SQL Server login.
A. **SID for WIN-AVPBP9ATULM\Administrator:**
0x0105000000000005150000007C98BDF441F8B4DD1677D940F4010000

B. What is the role of the function "fn_SIDToString" in the above?

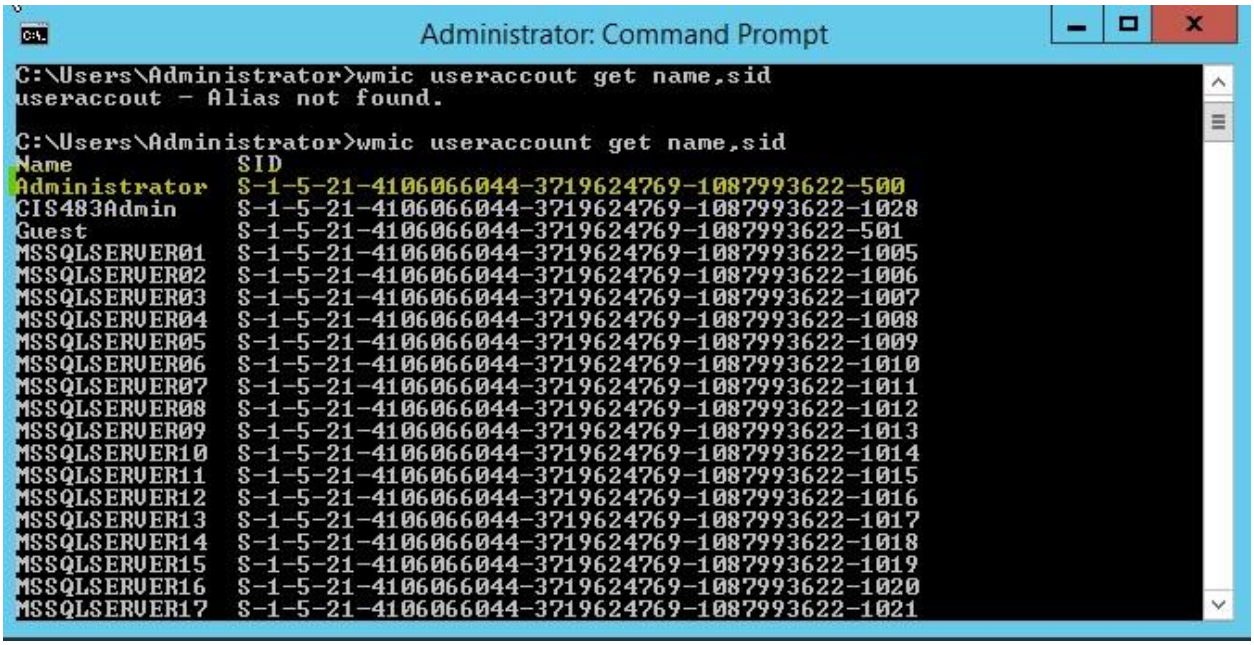
It takes a binary SID ('@BinSID') and converts the input into a string

C. Compare the SID from SQL Server for the administrator login with that from Windows Server for the administrator. Show the two screenshots. Use the SIDs in a string format (that is, in the S- format, not in Hex). Are they the same?

The SID of the administrator login from SQL Server (show the S-format)



The SID of the administrator login from Windows Server (show the S-format)



They are the same

D. SID: **0xCBD189CBF1CE5E4BAE1310033D61F163**

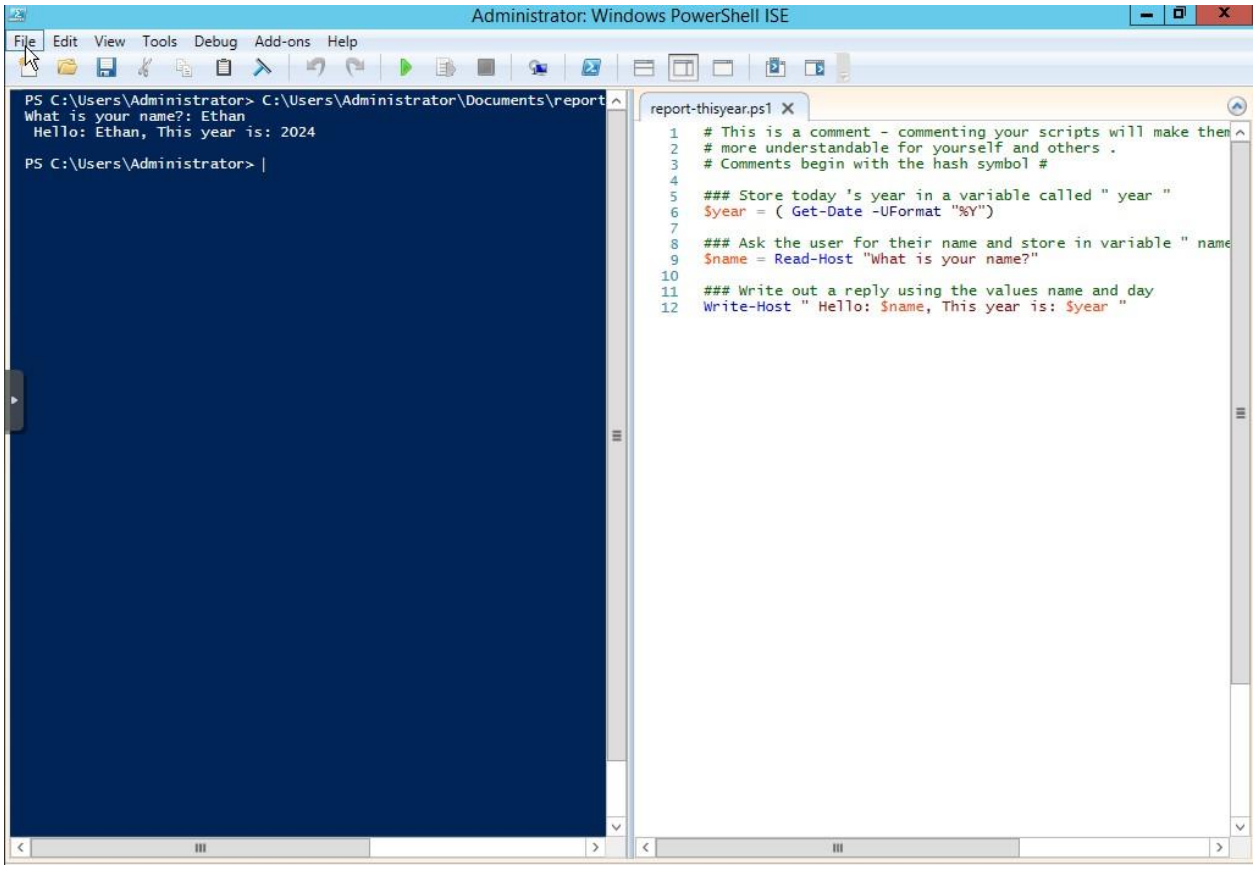
E. SID: **0XEE7C4ECFC463DE49BBD62A1C5E434372**

F. Are the SIDs of login `SIDTest` the same? Describe the reason why they are (not) the same?

They are not the same. SQL server generates a random new SID for security purposes whenever you create, drop, and recreate an account even if it's the same account.

Task 3: Learn PowerShell Scripting

- Run your script and report the output in a screenshot.


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\Users\Administrator> C:\Users\Administrator\Documents\report
What is your name?: Ethan
Hello: Ethan, This year is: 2024
PS C:\Users\Administrator>
report-thisyear.ps1
1 # This is a comment - commenting your scripts will make them
2 # more understandable for yourself and others .
3 # Comments begin with the hash symbol #
4
5 ### Store today 's year in a variable called " year "
6 $year = (Get-Date -UFormat "%Y")
7
8 ### Ask the user for their name and store in variable " name
9 $name = Read-Host "What is your name?"
10
11 ### Write out a reply using the values name and day
12 Write-Host " Hello: $name, This year is: $year "