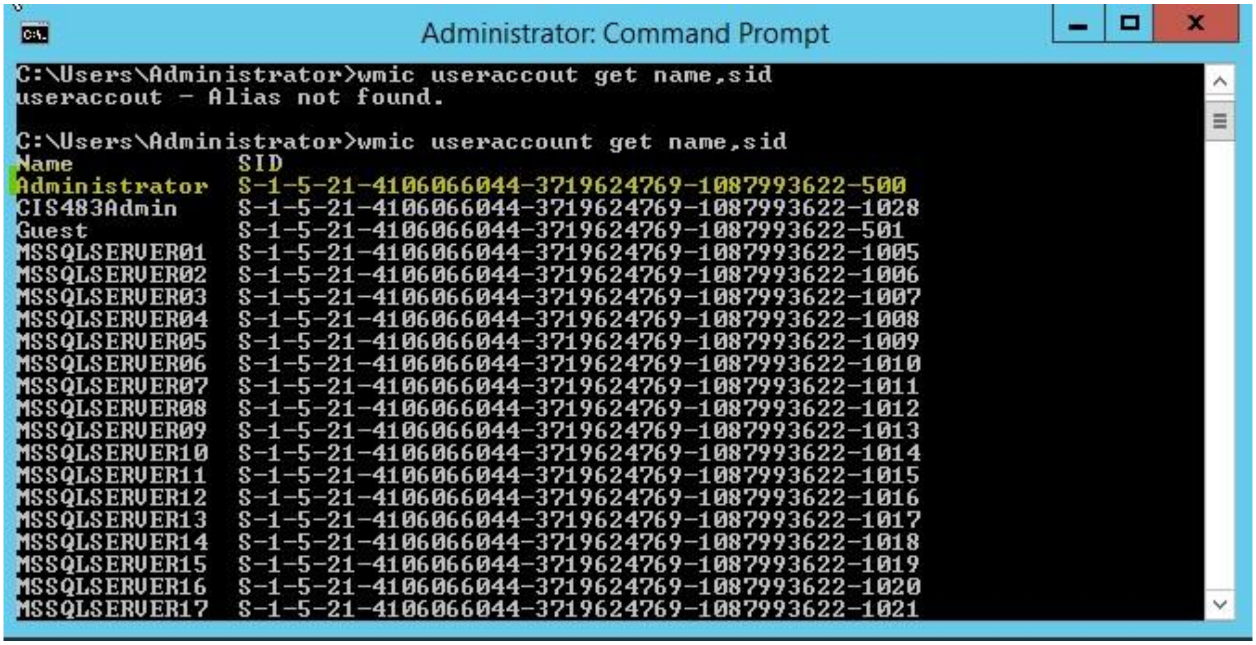
Lab 4 – SID, PowerShell

Task 1: Getting SID, SAT on Windows

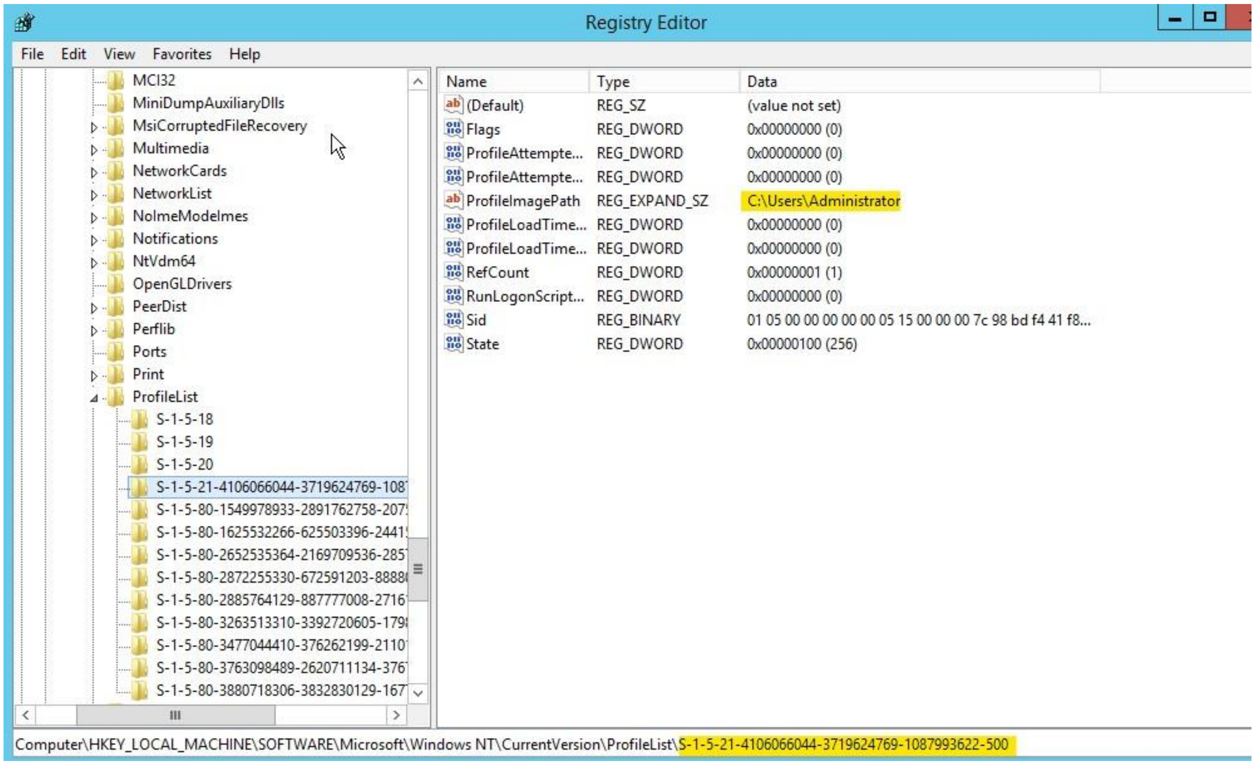
- Obtain the SID of the current login with **WMIC** command. Attach a screenshot for the SID and highlight it in red/yellow.



```
C:\Users\Administrator>wmic useraccout get name,sid
useraccout - Alias not found.

C:\Users\Administrator>wmic useraccount get name,sid
Name              SID
Administrator     S-1-5-21-4106066044-3719624769-1087993622-500
CIS483Admin       S-1-5-21-4106066044-3719624769-1087993622-1028
Guest             S-1-5-21-4106066044-3719624769-1087993622-501
MSSQLSERVER01     S-1-5-21-4106066044-3719624769-1087993622-1005
MSSQLSERVER02     S-1-5-21-4106066044-3719624769-1087993622-1006
MSSQLSERVER03     S-1-5-21-4106066044-3719624769-1087993622-1007
MSSQLSERVER04     S-1-5-21-4106066044-3719624769-1087993622-1008
MSSQLSERVER05     S-1-5-21-4106066044-3719624769-1087993622-1009
MSSQLSERVER06     S-1-5-21-4106066044-3719624769-1087993622-1010
MSSQLSERVER07     S-1-5-21-4106066044-3719624769-1087993622-1011
MSSQLSERVER08     S-1-5-21-4106066044-3719624769-1087993622-1012
MSSQLSERVER09     S-1-5-21-4106066044-3719624769-1087993622-1013
MSSQLSERVER10     S-1-5-21-4106066044-3719624769-1087993622-1014
MSSQLSERVER11     S-1-5-21-4106066044-3719624769-1087993622-1015
MSSQLSERVER12     S-1-5-21-4106066044-3719624769-1087993622-1016
MSSQLSERVER13     S-1-5-21-4106066044-3719624769-1087993622-1017
MSSQLSERVER14     S-1-5-21-4106066044-3719624769-1087993622-1018
MSSQLSERVER15     S-1-5-21-4106066044-3719624769-1087993622-1019
MSSQLSERVER16     S-1-5-21-4106066044-3719624769-1087993622-1020
MSSQLSERVER17     S-1-5-21-4106066044-3719624769-1087993622-1021
```

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


Registry Editor
File
Edit
View
Favorites
Help
MCI32
MiniDumpAuxiliaryDlls
MsiCorruptedFileRecovery
Multimedia
NetworkCards
NetworkList
NoImeModelmes
Notifications
NtVdm64
OpenGLDrivers
PeerDist
Perflib
Ports
Print
ProfileList
S-1-5-18
S-1-5-19
S-1-5-20
S-1-5-21-4106066044-3719624769-108
S-1-5-80-1549978933-2891762758-207
S-1-5-80-1625532266-625503396-2441
S-1-5-80-2652535364-2169709536-285
S-1-5-80-2872255330-672591203-8888
S-1-5-80-2885764129-887777008-2716
S-1-5-80-3263513310-3392720605-179
S-1-5-80-3477044410-376262199-2110
S-1-5-80-3763098489-2620711134-376
S-1-5-80-3880718306-3832830129-167

Name	Type	Data
(Default)	REG_SZ	(value not set)
Flags	REG_DWORD	0x00000000 (0)
ProfileAttempte...	REG_DWORD	0x00000000 (0)
ProfileAttempte...	REG_DWORD	0x00000000 (0)
ProfileImagePath	REG_EXPAND_SZ	C:\Users\Administrator
ProfileLoadTime...	REG_DWORD	0x00000000 (0)
ProfileLoadTime...	REG_DWORD	0x00000000 (0)
RefCount	REG_DWORD	0x00000001 (1)
RunLogonScript...	REG_DWORD	0x00000000 (0)
Sid	REG_BINARY	01 05 00 00 00 00 00 05 15 00 00 00 7c 98 bd f4 41 f8...
State	REG_DWORD	0x00000100 (256)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4106066044-3719624769-1087993622-500

Task 2: Getting SID on SQL Server

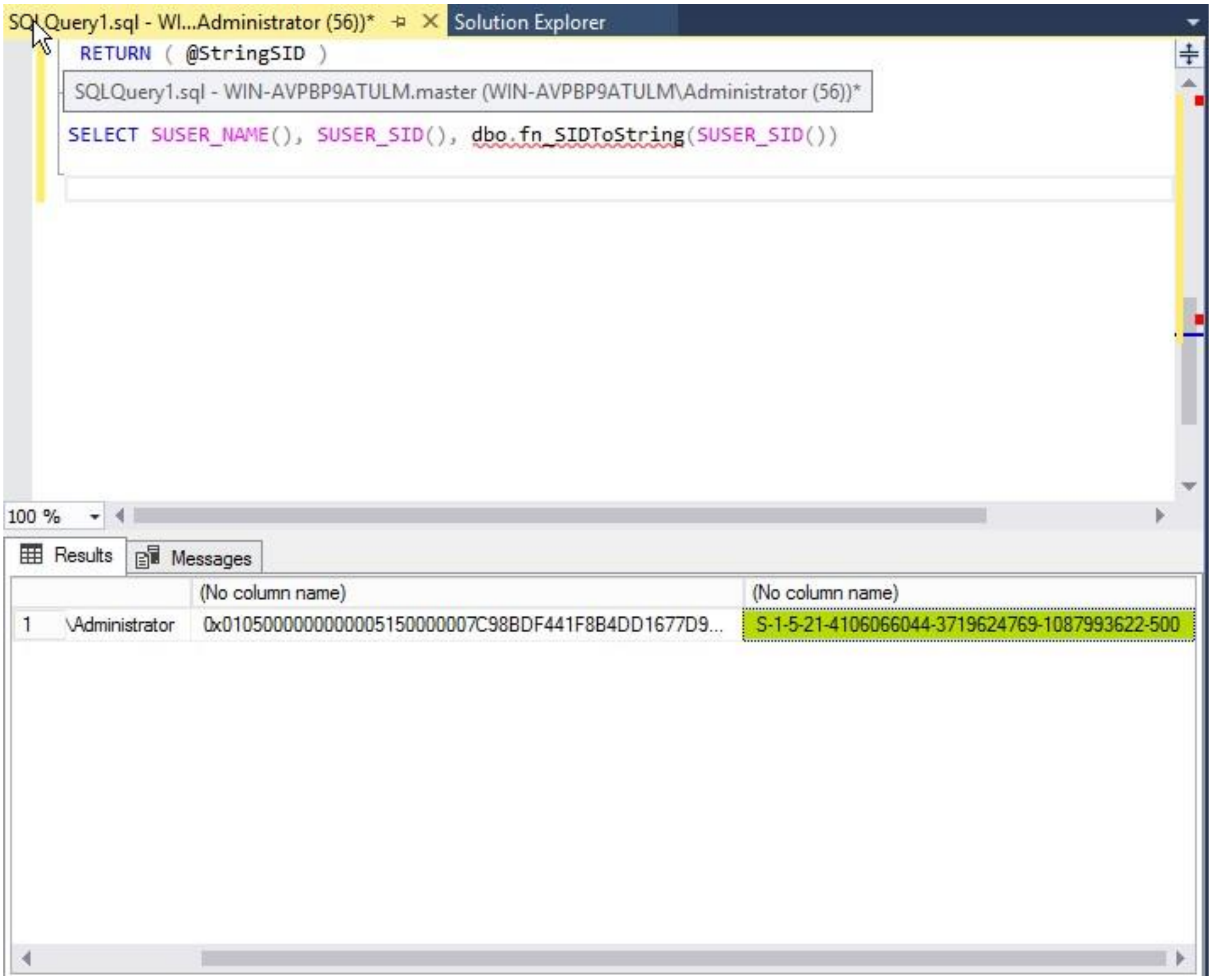
Get the SID of the account you used for SQL Server login.
A. **SID for WIN-AVPBP9ATULM\Administrator:**
0x0105000000000005150000007C98BDF441F8B4DD1677D940F4010000

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)



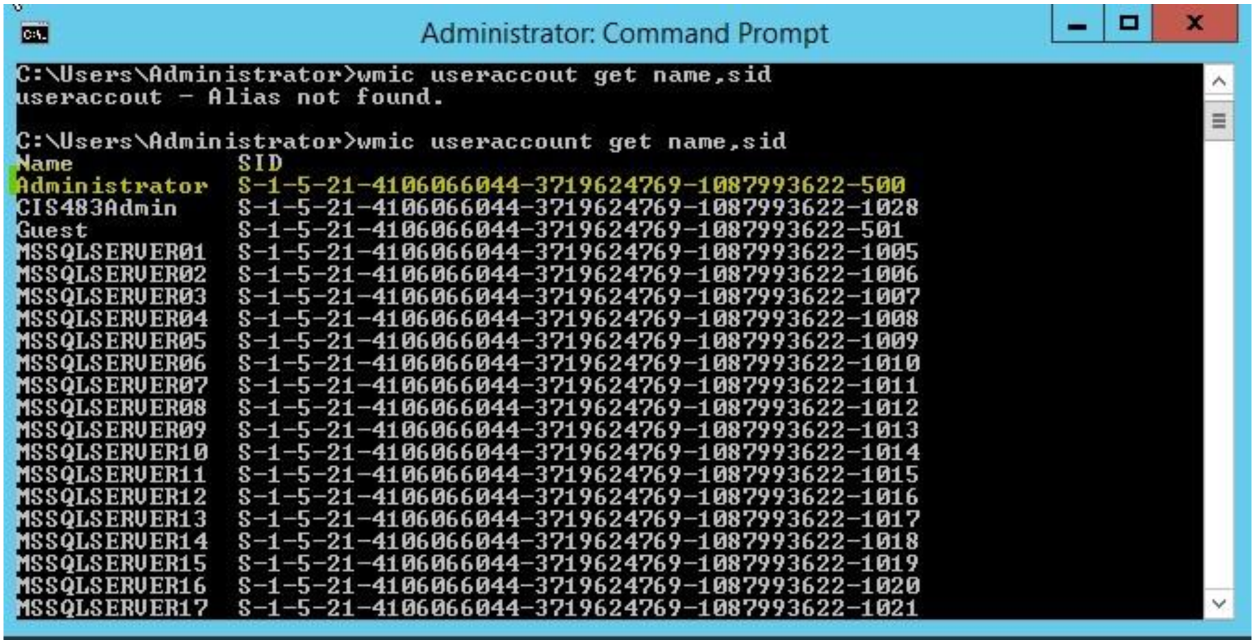
```
RETURN ( @StringSID )
```

SQLQuery1.sql - WIN-AVPBP9ATULM.master (WIN-AVPBP9ATULM\Administrator (56))*

```
SELECT SUSER_NAME(), SUSER_SID(), dbo.fn_SIDToString(SUSER_SID())
```

		(No column name)	(No column name)
1	\Administrator	0x0105000000000005150000007C98BDF441F8B4DD1677D9...	S-1-5-21-4106066044-3719624769-1087993622-500

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



```
C:\Users\Administrator>wmic useraccout get name,sid
useraccout - Alias not found.

C:\Users\Administrator>wmic useraccount get name,sid
Name           SID
Administrator  S-1-5-21-4106066044-3719624769-1087993622-500
CIS483Admin    S-1-5-21-4106066044-3719624769-1087993622-1028
Guest          S-1-5-21-4106066044-3719624769-1087993622-501
MSSQLSERVER01  S-1-5-21-4106066044-3719624769-1087993622-1005
MSSQLSERVER02  S-1-5-21-4106066044-3719624769-1087993622-1006
MSSQLSERVER03  S-1-5-21-4106066044-3719624769-1087993622-1007
MSSQLSERVER04  S-1-5-21-4106066044-3719624769-1087993622-1008
MSSQLSERVER05  S-1-5-21-4106066044-3719624769-1087993622-1009
MSSQLSERVER06  S-1-5-21-4106066044-3719624769-1087993622-1010
MSSQLSERVER07  S-1-5-21-4106066044-3719624769-1087993622-1011
MSSQLSERVER08  S-1-5-21-4106066044-3719624769-1087993622-1012
MSSQLSERVER09  S-1-5-21-4106066044-3719624769-1087993622-1013
MSSQLSERVER10  S-1-5-21-4106066044-3719624769-1087993622-1014
MSSQLSERVER11  S-1-5-21-4106066044-3719624769-1087993622-1015
MSSQLSERVER12  S-1-5-21-4106066044-3719624769-1087993622-1016
MSSQLSERVER13  S-1-5-21-4106066044-3719624769-1087993622-1017
MSSQLSERVER14  S-1-5-21-4106066044-3719624769-1087993622-1018
MSSQLSERVER15  S-1-5-21-4106066044-3719624769-1087993622-1019
MSSQLSERVER16  S-1-5-21-4106066044-3719624769-1087993622-1020
MSSQLSERVER17  S-1-5-21-4106066044-3719624769-1087993622-1021
```

They are the same

D. SID: **0xCBD189CBF1CE5E4BAE1310033D61F163**

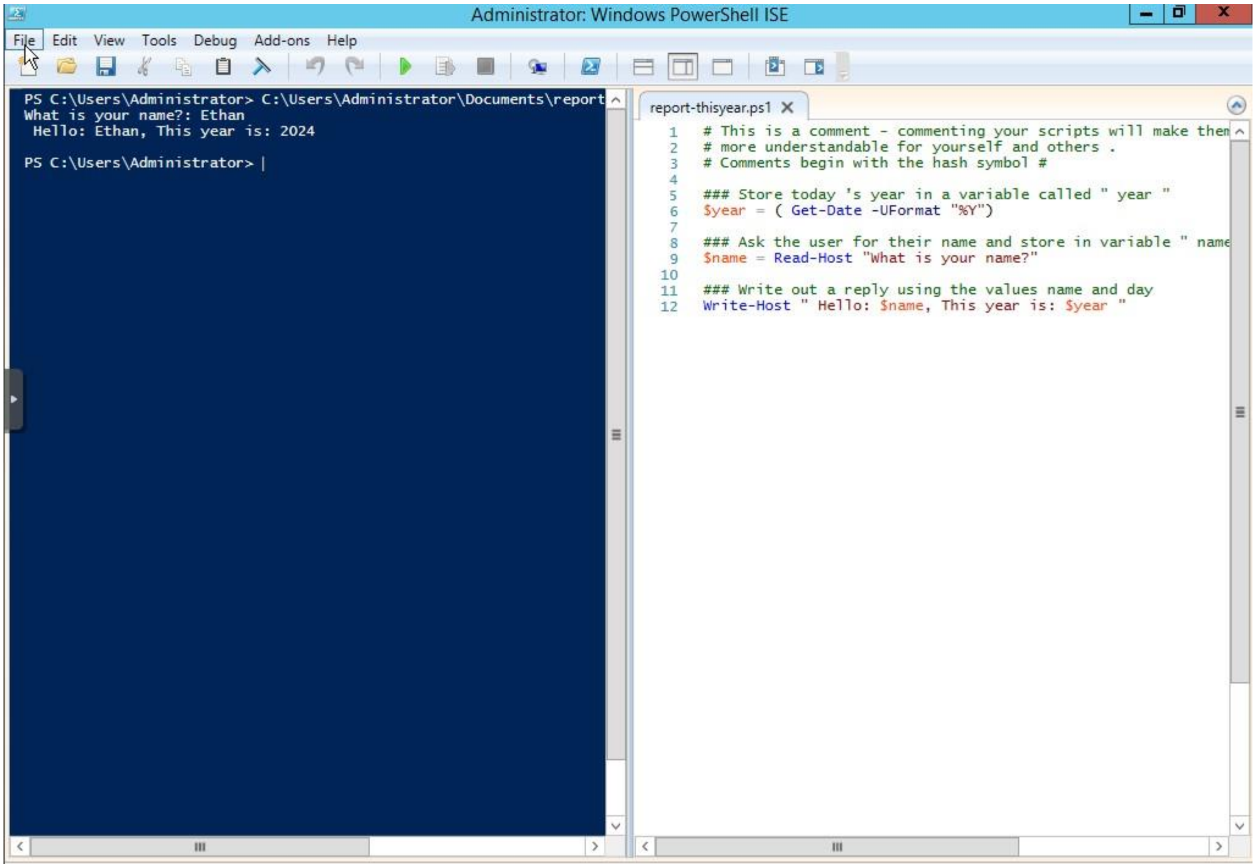
E. SID: **0XEE7C4ECFC463DE49BBD62A1C5E434372**

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.



```
PS C:\Users\Administrator> C:\Users\Administrator\Documents\report
What is your name?: Ethan
 Hello: Ethan, This year is: 2024

PS C:\Users\Administrator> |
```

```
# This is a comment - commenting your scripts will make them
# more understandable for yourself and others .
# Comments begin with the hash symbol #

### Store today 's year in a variable called " year "
$year = ( Get-Date -UFormat "%Y")

### Ask the user for their name and store in variable " name
$name = Read-Host "What is your name?"

### Write out a reply using the values name and day
Write-Host " Hello: $name, This year is: $year "
```