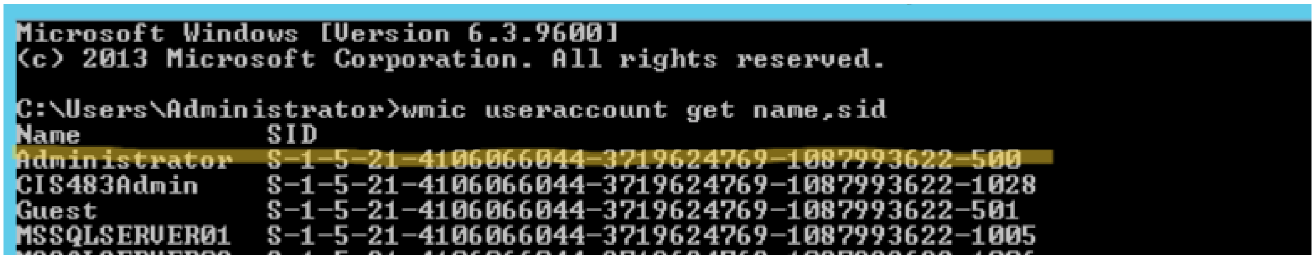
Lab 4 – SID, PowerShell

Jackson Hallahan

Task 1: Getting SID, SAT on Windows

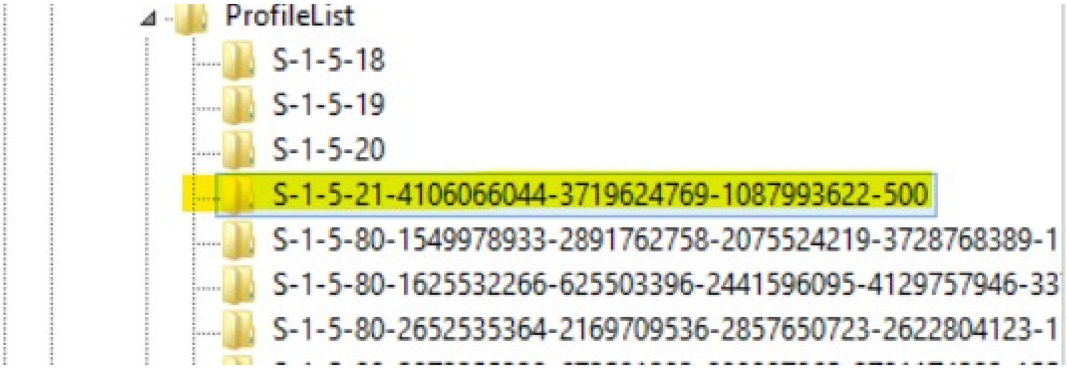
- Obtain the SID of the current login with **WMIC** command. Attach a screenshot for the SID and highlight it in red/yellow.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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
```

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



```
ProfileList
    S-1-5-18
    S-1-5-19
    S-1-5-20
    S-1-5-21-4106066044-3719624769-1087993622-500
    S-1-5-80-1549978933-2891762758-2075524219-3728768389-1
    S-1-5-80-1625532266-625503396-2441596095-4129757946-33
    S-1-5-80-2652535364-2169709536-2857650723-2622804123-1
```

Task 2: Getting SID on SQL Server

Get the SID of the account you used for SQL Server login.
A. SID: **_0x0105000000000005150000007C98BDF441F8B4DD1677D940F4010000**______

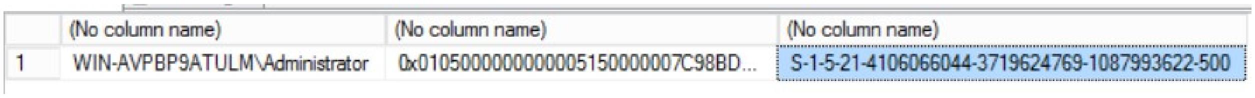
B. What is the role of the function "fn_SIDToString" in the above?

It converts the binary SID value to the readable string format used in SQL server for SIDs.

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?

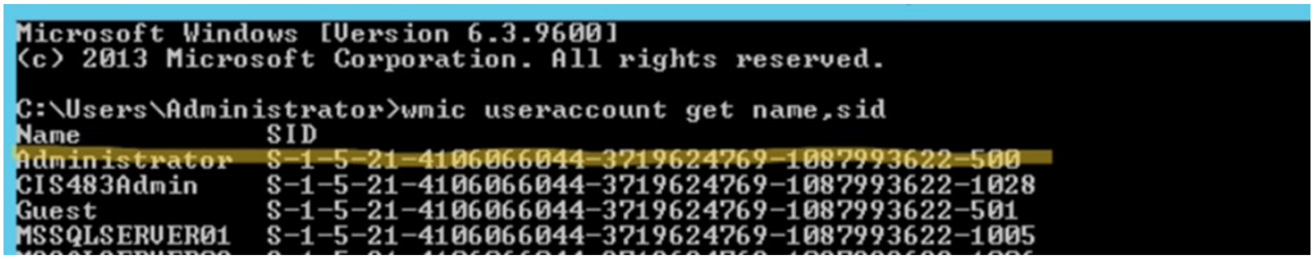
Yes, the SIDs are the same.

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



	(No column name)	(No column name)	(No column name)
1	WIN-AVPBP9ATULM\Administrator	0x010500000000000515000000 7C98BD...	S-1-5-21-4106066044-3719624769-1087993622-500

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



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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
```

D. SID: **_0x9E64D8303DB5F34C998271E870B331DB________**.

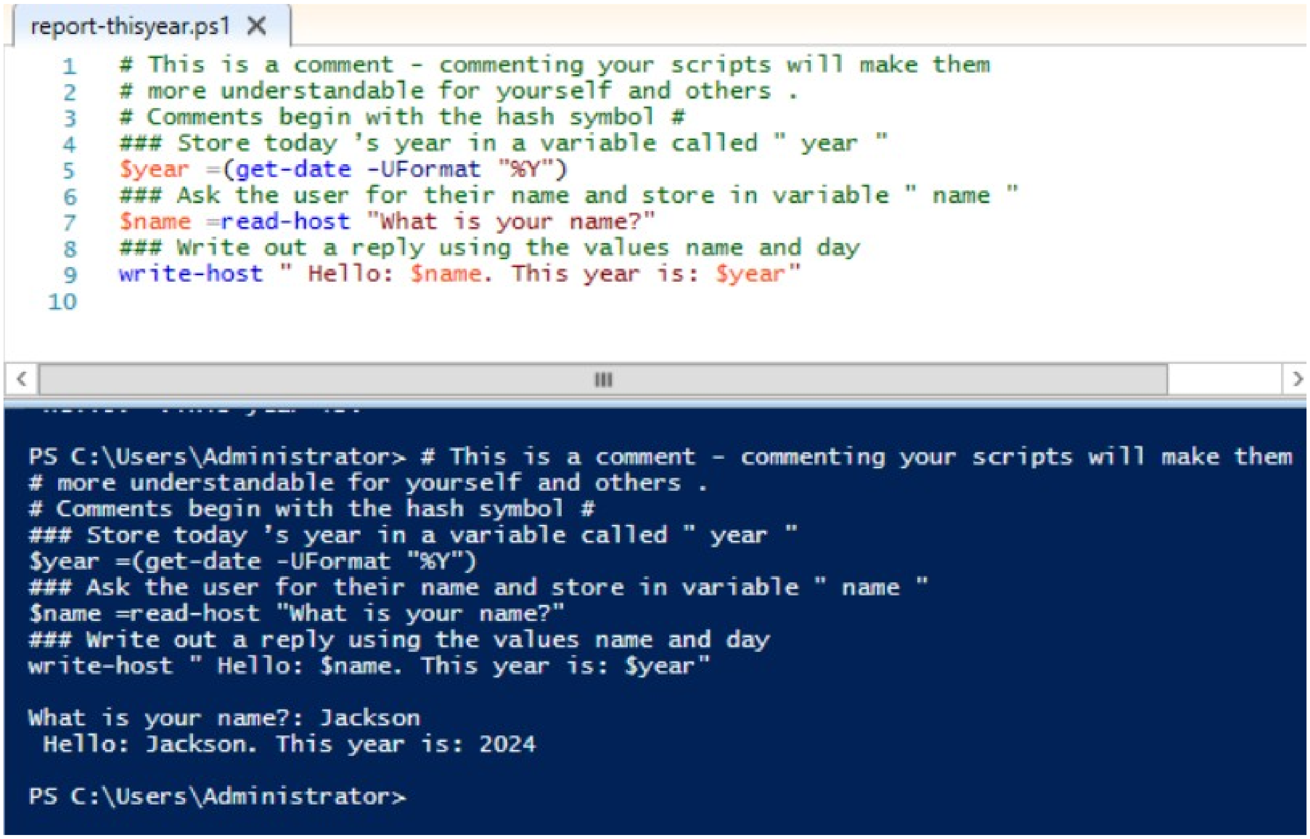
E. SID: **_0x10D3C34B47ADF849965C3F6DC3210E05_________**.

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

> **No. They are different because the server generates a unique SID for each login because they are unique to each user, not to the login name "SIDTest".**

Task 3: Learn PowerShell Scripting

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



```
# 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"
```

```
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"

What is your name?: Jackson
 Hello: Jackson. This year is: 2024

PS C:\Users\Administrator>
```