

The text file “`ConsoleHost_history.txt`” located* at
%userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\
Holds a history of recent Windows PowerShell commands executed
<http://woshub.com/powershell-commands-history/>

**Unless changed by a user with the “Set-PSReadlineOption –HistorySavePath” option.
(If you do not add this parameter, the default path is
~\AppData\Roaming\PSReadline\$(\$host.Name)_history.txt.)*

The entries are appended at the bottom of the file after execution. The default size of
ConsoleHost_history.txt is 4096 commands
(note: Specifies the maximum number of commands to save in PSReadline history. PSReadline
history not the same thing as Windows PowerShell history.)
<https://docs.microsoft.com/en-us/powershell/module/psreadline/set-psreadlineoption?view=powershell-6>

```
PS C:\Users\  
> Get-PSReadlineOption  
  
EditMode : Windows  
ContinuationPrompt : >>  
ContinuationPromptForegroundColor : Green  
ContinuationPromptBackgroundColor : Black  
ExtraPromptLineCount : 0  
AddToHistoryHandler :  
CommandValidationHandler :  
CommandsToValidateScriptBlockArguments : {ForEach-Object, %, Invoke-Command, icm...  
HistoryNoDuplicates : False  
MaximumHistoryCount : 4096  
MaximumKillRingCount : 10  
HistorySearchCursorMovesToEnd : False  
ShowToolTips : False  
DingTone : 1221  
CompletionQueryItems : 100  
WordDelimiters : ;, ., [ ] { } ( ) \ ^ & * - + ' " ~ _  
DingDuration : 50  
BellStyle : Audible  
HistorySearchCaseSensitive : False  
ViModeIndicator : None  
HistorySavePath : C:\Users\  
                \AppData\Roam  
                eadline\ConsoleHost_history.txt  
HistorySaveStyle : SaveIncrementally  
DefaultTokenForegroundColor : Green  
CommentForegroundColor : DarkGreen  
KeywordForegroundColor : Green  
StringForegroundColor : DarkCyan  
OperatorForegroundColor : DarkGray  
VariableForegroundColor : Green  
CommandForegroundColor : Yellow  
ParameterForegroundColor : DarkGray  
TypeForegroundColor : Gray  
NumberForegroundColor : White  
MemberForegroundColor : White  
DefaultTokenBackgroundColor : Black  
CommentBackgroundColor : Black  
KeywordBackgroundColor : Black  
StringBackgroundColor : Black  
OperatorBackgroundColor : Black  
VariableBackgroundColor : Black  
CommandBackgroundColor : Black  
ParameterBackgroundColor : Black  
TypeBackgroundColor : Black  
NumberBackgroundColor : Black  
MemberBackgroundColor : Black  
EmphasisForegroundColor : Cyan  
EmphasisBackgroundColor : Black  
ErrorForegroundColor : Red  
ErrorBackgroundColor : Black  
  
PS C:\Users\  
> [datetime]::FromFileTime(1.316696446777243E+17)  
Wednesday, March 28, 2018 10:40:46 am  
  
PS C:\Users\  
>
```

Example of the entries found:

```
cd D:\User\Desktop\.temp
dir
esentutl /r
D:\User\Desktop\.temp\Windows.edb.copy0"
Get-PSReadlineOption
[datetime]::FromFileTime(1.3166696446777243E+17)
```

For a user, this can be helpful as previously executed commands can be accessed with the up/down key, even after a Console window is closed and a new opened. For DFIR it is proof that a command was executed in PowerShell console.