How to find the usage of files in Remote victim PC (Remote PC Forensics)

March 29, 2015 By Raj Chandel

Today we are going to learn about managing a bunch of files on a remote system using the forfiles command via meterpreter.

Table of Content:

Requirements

Attacker: Kali Linux

Target: Windows

Introduction to forfiles command

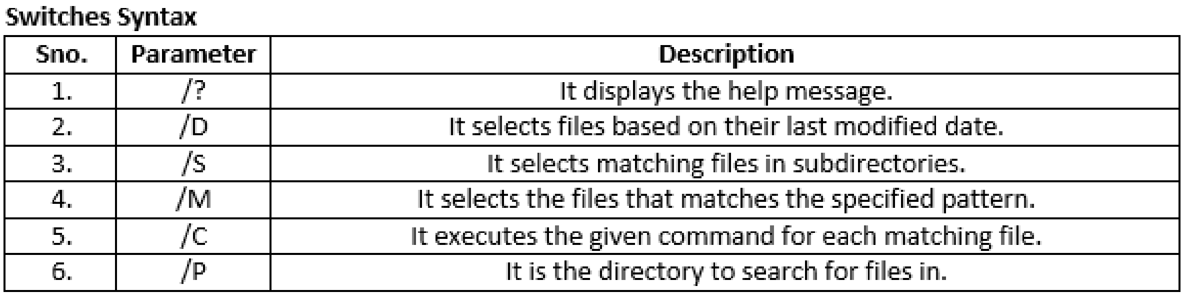
Forfiles is a command line utility software. It was shipped with Microsoft Windows Vista. During that time, management of multiples files through the command line was difficult as most of the commands at that time we made to work on single files. Seeing this as a major drawback, Microsoft introduced forfiles. This command runs a command on a bunch of files at the same time. Operations that can be done by for files are file selection based on the first or last modified date. Forfiles can be used directly on the command-line or it can be used in batch files or scripts.

The parameters of the forfiles command are divided into two parts:

- Switches

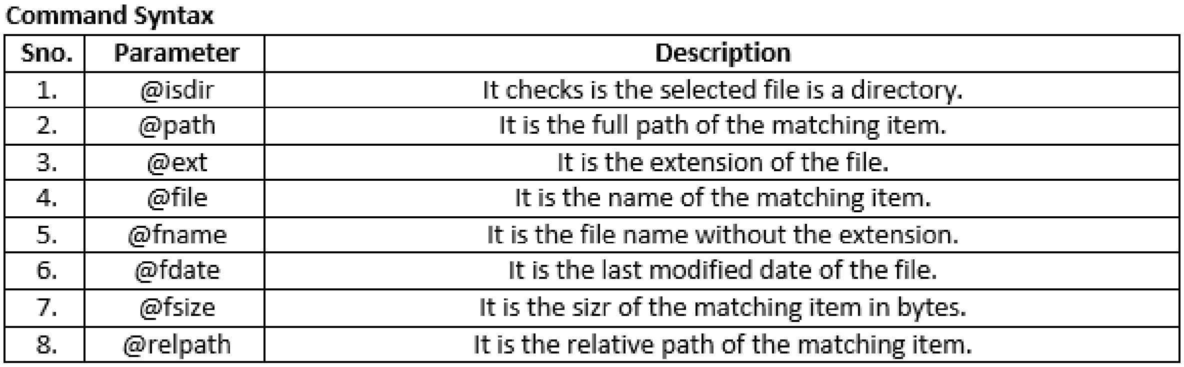
- Command

Switches Syntax



Switches Syntax

Sno.	Parameter	Description
1.	/?	It displays the help message.
2.	/D	It selects files based on their last modified date.
3.	/S	It selects matching files in subdirectories.
4.	/M	It selects the files that matches the specified pattern.
5.	/C	It executes the given command for each matching file.
6.	/P	It is the directory to search for files in.



Command Syntax

Sno.	Parameter	Description
1.	@isdir	It checks is the selected file is a directory.
2.	@path	It is the full path of the matching item.
3.	@ext	It is the extension of the file.
4.	@file	It is the name of the matching item.
5.	@fname	It is the file name without the extension.
6.	@fdate	It is the last modified date of the file.
7.	@fsize	It is the sizr of the matching item in bytes.
8.	@relpath	It is the relative path of the matching item.

Date Syntax

Based on the last modified date, the date switch(/D) selects the files.

The date is accepted in the **MM/DD/YYYY format**. But the date can be given in terms of the number of days. Like we can use the (-) minus operator to give the days earlier.

For example: If we write /D -40 then this means 40 days **before the last modified** date.

Similarly, we can use the (+) plus operator to give the days **after the last modified** date.

Achieve Meterpreter on Remote System

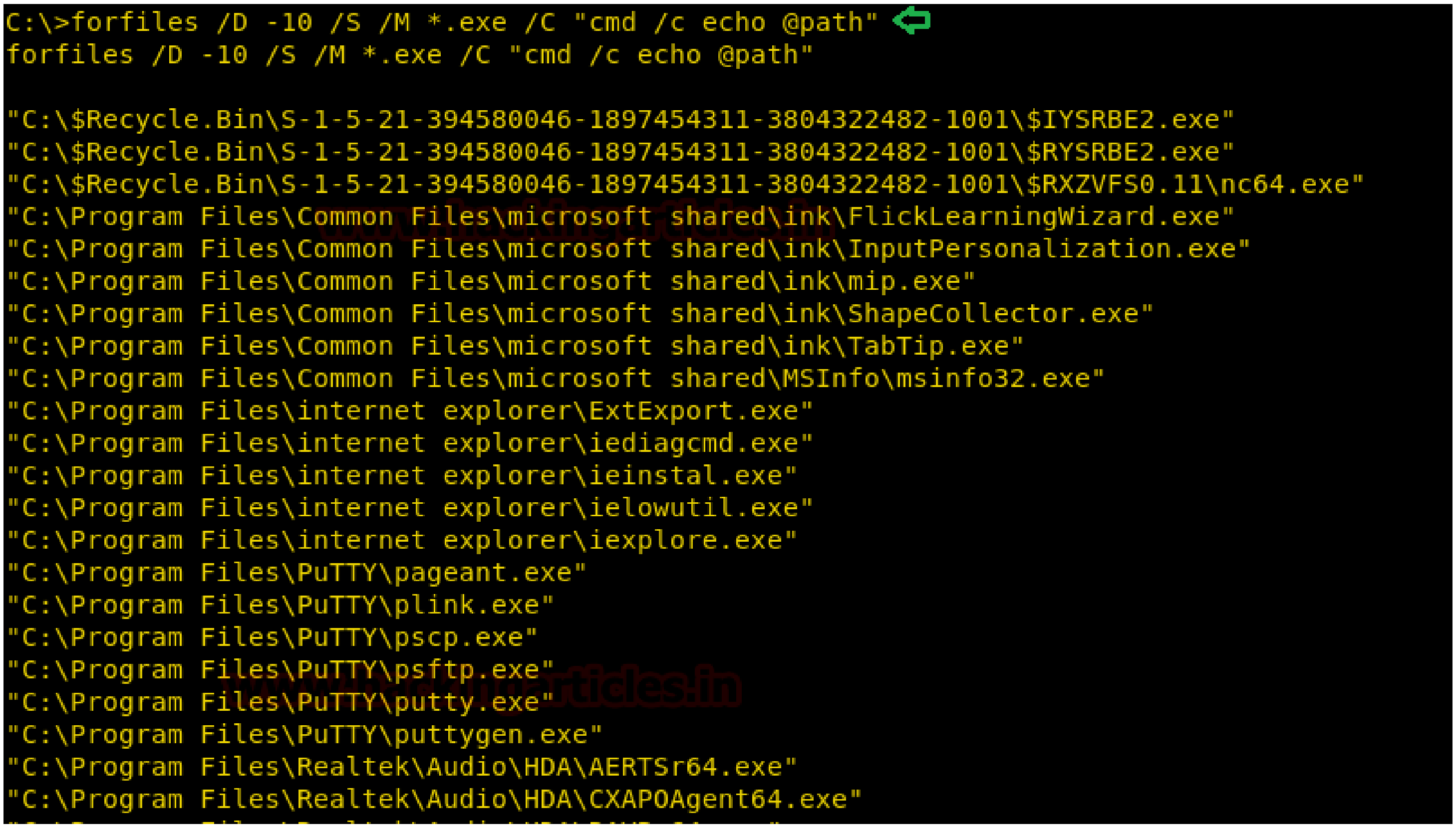
Open Kali Linux terminal and type msfconsole in order to load Metasploit framework. Now we need to compromise victim's machine one to achieve any type of session either meterpreter or shell and to do so we can read our previous article from **here**.

After getting meterpreter on the remote system, we need to get to the shell of the target system. This is necessary as the forfiles is a windows command-line command. So, get to the Windows command-line using **"shell"** command.

List all the files of a particular extension modified in last 10 days

In a scenario where we want to list the files with their path which were modified recently, we can use this command. Here we are using the date switch to define the number of days. We can change the number of days with /D to our requirement. Then we specified the extension .exe this can be any extension we want to search. And then finally we used the @path to make the complete path listed in the output.

```
forfiles /D -10 /S /M *.exe /C "cmd /c echo @path"
```

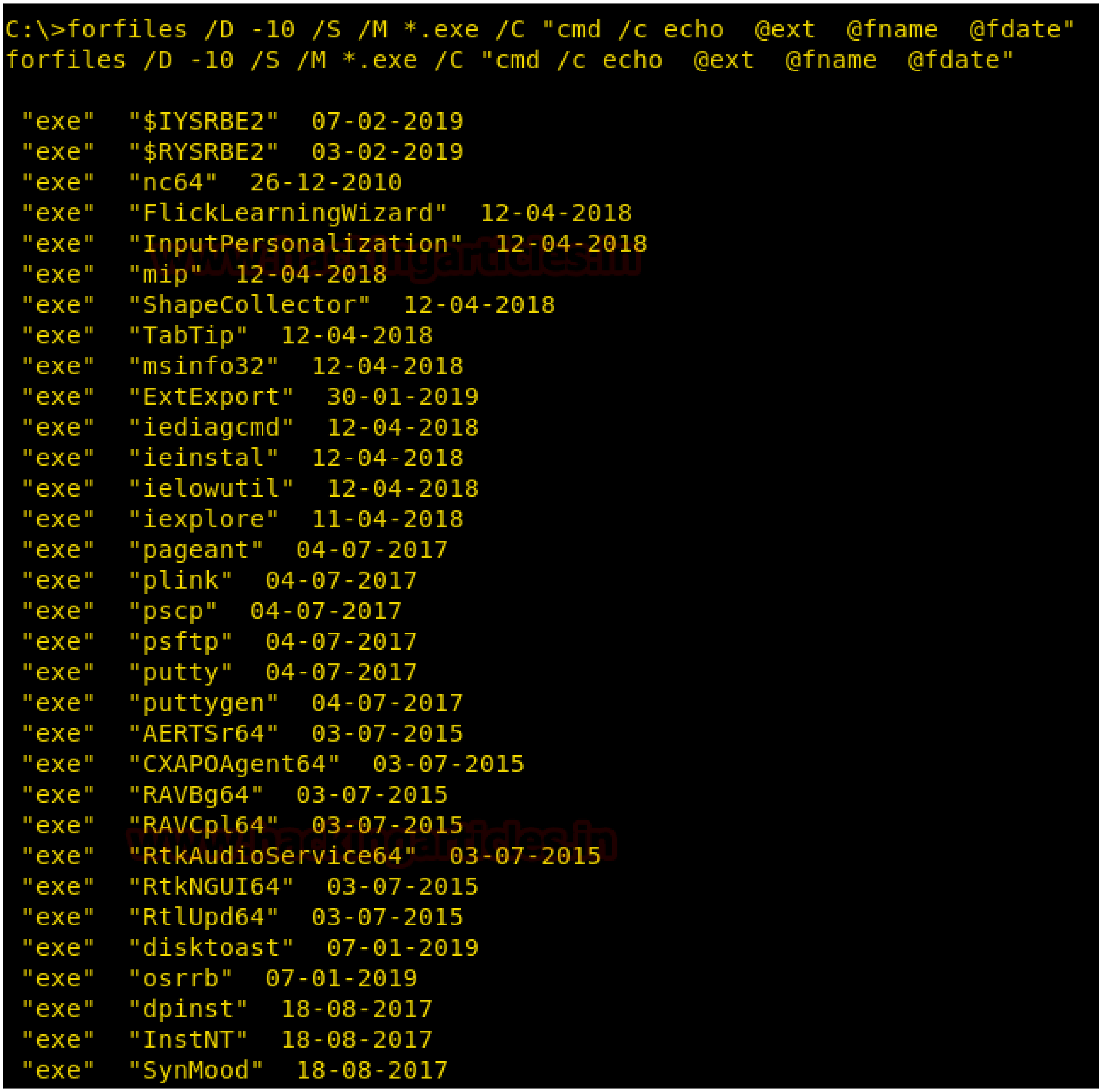


```
C:\>forfiles /D -10 /S /M *.exe /C "cmd /c echo @path"
forfiles /D -10 /S /M *.exe /C "cmd /c echo @path"

"C:\$Recycle.Bin\S-1-5-21-394580046-1897454311-3804322482-1001\$IYSRBE2.exe"
"C:\$Recycle.Bin\S-1-5-21-394580046-1897454311-3804322482-1001\$RYSRBE2.exe"
"C:\$Recycle.Bin\S-1-5-21-394580046-1897454311-3804322482-1001\$RXZVFS0.11\nc64.exe"
"C:\Program Files\Common Files\microsoft shared\ink\FlickLearningWizard.exe"
"C:\Program Files\Common Files\microsoft shared\ink\InputPersonalization.exe"
"C:\Program Files\Common Files\microsoft shared\ink\mip.exe"
"C:\Program Files\Common Files\microsoft shared\ink\ShapeCollector.exe"
"C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe"
"C:\Program Files\Common Files\microsoft shared\MSInfo\msinfo32.exe"
"C:\Program Files\internet explorer\ExtExport.exe"
"C:\Program Files\internet explorer\iediagcmd.exe"
"C:\Program Files\internet explorer\ieinstal.exe"
"C:\Program Files\internet explorer\ielowutil.exe"
"C:\Program Files\internet explorer\iexplore.exe"
"C:\Program Files\PuTTY\pageant.exe"
"C:\Program Files\PuTTY\plink.exe"
"C:\Program Files\PuTTY\pscp.exe"
"C:\Program Files\PuTTY\psftp.exe"
"C:\Program Files\PuTTY\putty.exe"
"C:\Program Files\PuTTY\puttygen.exe"
"C:\Program Files\Realtek\Audio\HDA\AERTSr64.exe"
"C:\Program Files\Realtek\Audio\HDA\CXAPOAgent64.exe"
```

List all the files of a particular extension, name and modification date

In a scenario where we want to list the files with their path and when they were modified recently, we can use this command. Here we are using the date switch to define the number of days. We can change the number of days with /D to our requirement. Then we specified the extension .exe this can be any extension we want to search. And then finally we used the @fdate to make the date it was modified listed in the output.

```
forfiles /D -10 /S /M *.exe /C "cmd /c echo @ext @fname @fdate"
```

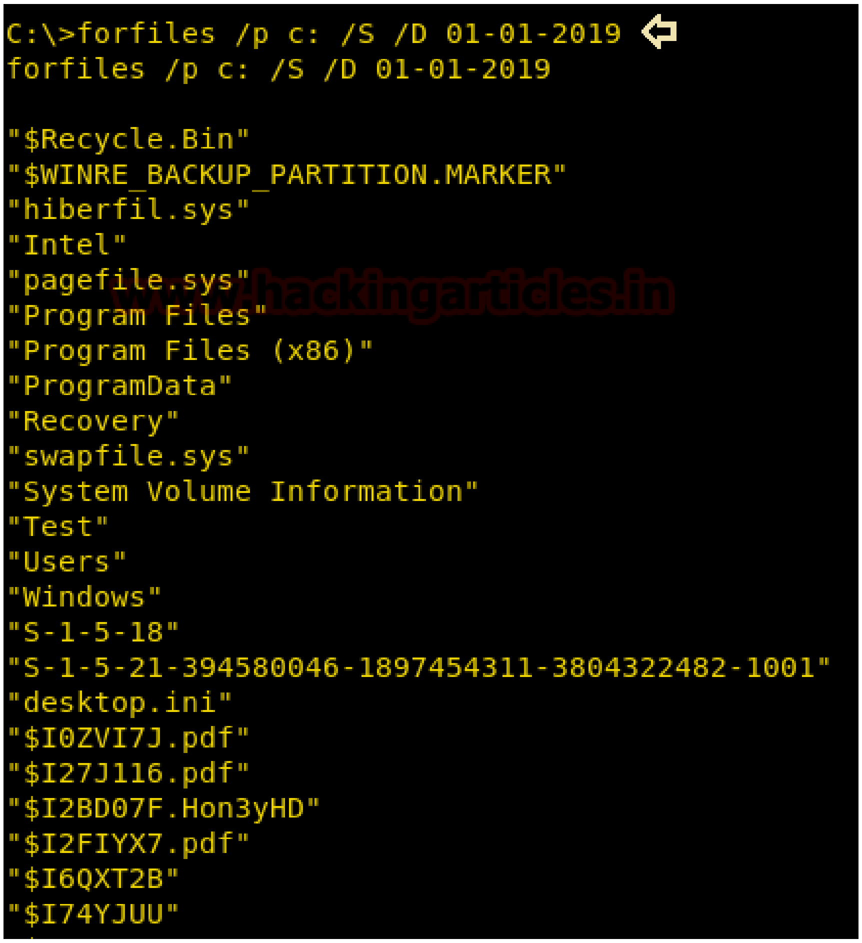


```
C:\>forfiles /D -10 /S /M *.exe /C "cmd /c echo  @ext  @fname  @fdate"
forfiles /D -10 /S /M *.exe /C "cmd /c echo  @ext  @fname  @fdate"

 "exe"  "$IYSRBE2"  07-02-2019
 "exe"  "$RYSRBE2"  03-02-2019
 "exe"  "nc64"  26-12-2010
 "exe"  "FlickLearningWizard"  12-04-2018
 "exe"  "InputPersonalization"  12-04-2018
 "exe"  "mip"  12-04-2018
 "exe"  "ShapeCollector"  12-04-2018
 "exe"  "TabTip"  12-04-2018
 "exe"  "msinfo32"  12-04-2018
 "exe"  "ExtExport"  30-01-2019
 "exe"  "iediagcmd"  12-04-2018
 "exe"  "ieinstal"  12-04-2018
 "exe"  "ielowutil"  12-04-2018
 "exe"  "iexplore"  11-04-2018
 "exe"  "pageant"  04-07-2017
 "exe"  "plink"  04-07-2017
 "exe"  "pscp"  04-07-2017
 "exe"  "psftp"  04-07-2017
 "exe"  "putty"  04-07-2017
 "exe"  "puttygen"  04-07-2017
 "exe"  "AERTSr64"  03-07-2015
 "exe"  "CXAPOAgent64"  03-07-2015
 "exe"  "RAVBg64"  03-07-2015
 "exe"  "RAVCpl64"  03-07-2015
 "exe"  "RtkAudioService64"  03-07-2015
 "exe"  "RtkNGUI64"  03-07-2015
 "exe"  "RtlUpd64"  03-07-2015
 "exe"  "disktoast"  07-01-2019
 "exe"  "osrrb"  07-01-2019
 "exe"  "dpinst"  18-08-2017
 "exe"  "InstNT"  18-08-2017
 "exe"  "SynMood"  18-08-2017
```

List all the files that we modified on a particular date

In a scenario where we want to list the files that were modified on a particular date. In our example, we take 1st in January 2019. This can be modified as per the user's choice. But we need to take care of the format that we mentioned in the Introduction.

```
forfiles /p c: /S /D 01-01-2019
```

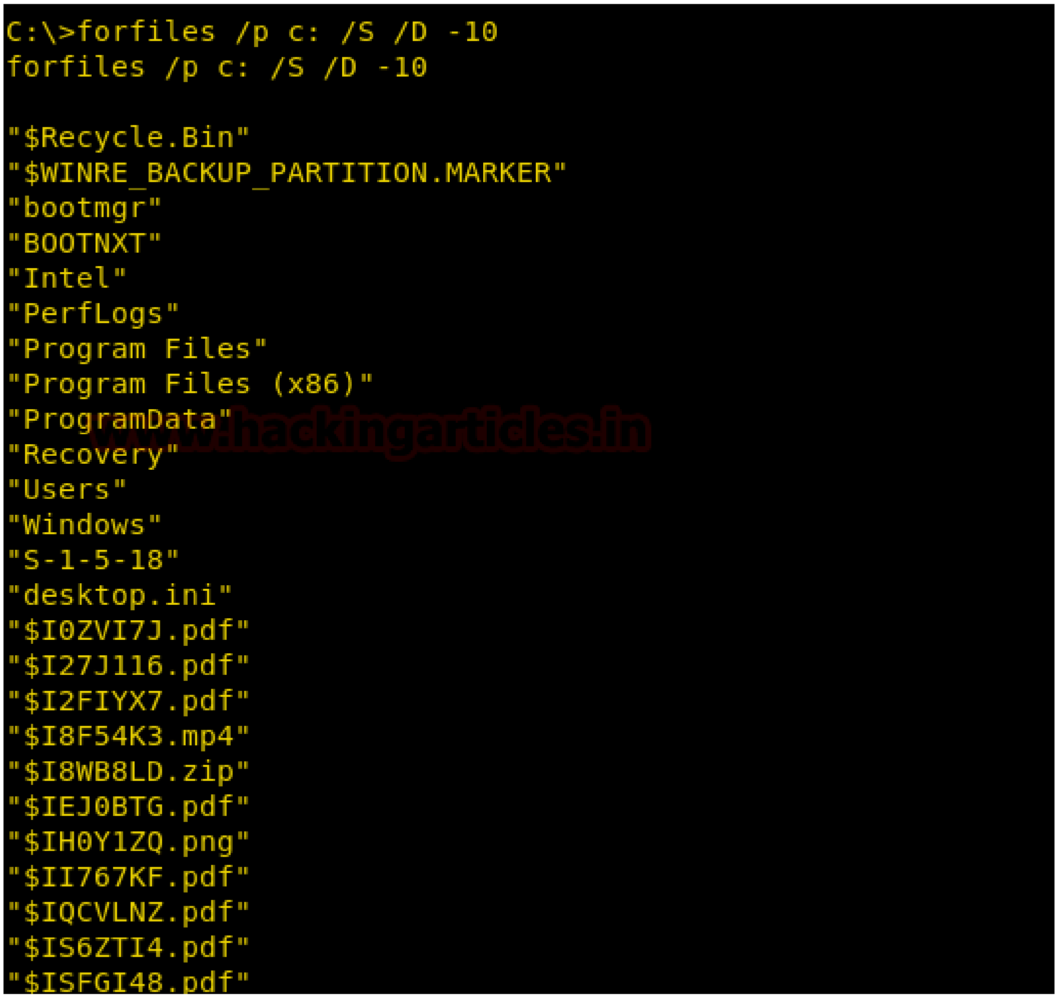


```
C:\>forfiles /p c: /S /D 01-01-2019
forfiles /p c: /S /D 01-01-2019

"$Recycle.Bin"
"$WINRE_BACKUP_PARTITION.MARKER"
"hiberfil.sys"
"Intel"
"pagefile.sys"
"Program Files"
"Program Files (x86)"
"ProgramData"
"Recovery"
"swapfile.sys"
"System Volume Information"
"Test"
"Users"
"Windows"
"S-1-5-18"
"S-1-5-21-394580046-1897454311-3804322482-1001"
"desktop.ini"
"$I0ZVI7J.pdf"
"$I27J116.pdf"
"$I2BD07F.Hon3yHD"
"$I2FIYX7.pdf"
"$I6QXT2B"
"$I74YJUU"
```

List all the files modified in the last 10 days

In a scenario where we want to list the files modified in the last 10 days, we can use this command. This command is different from the earlier command as here we are using the date switch to define the number of days instead of a particular date.

```
forfiles /p c: /S /D -10
```

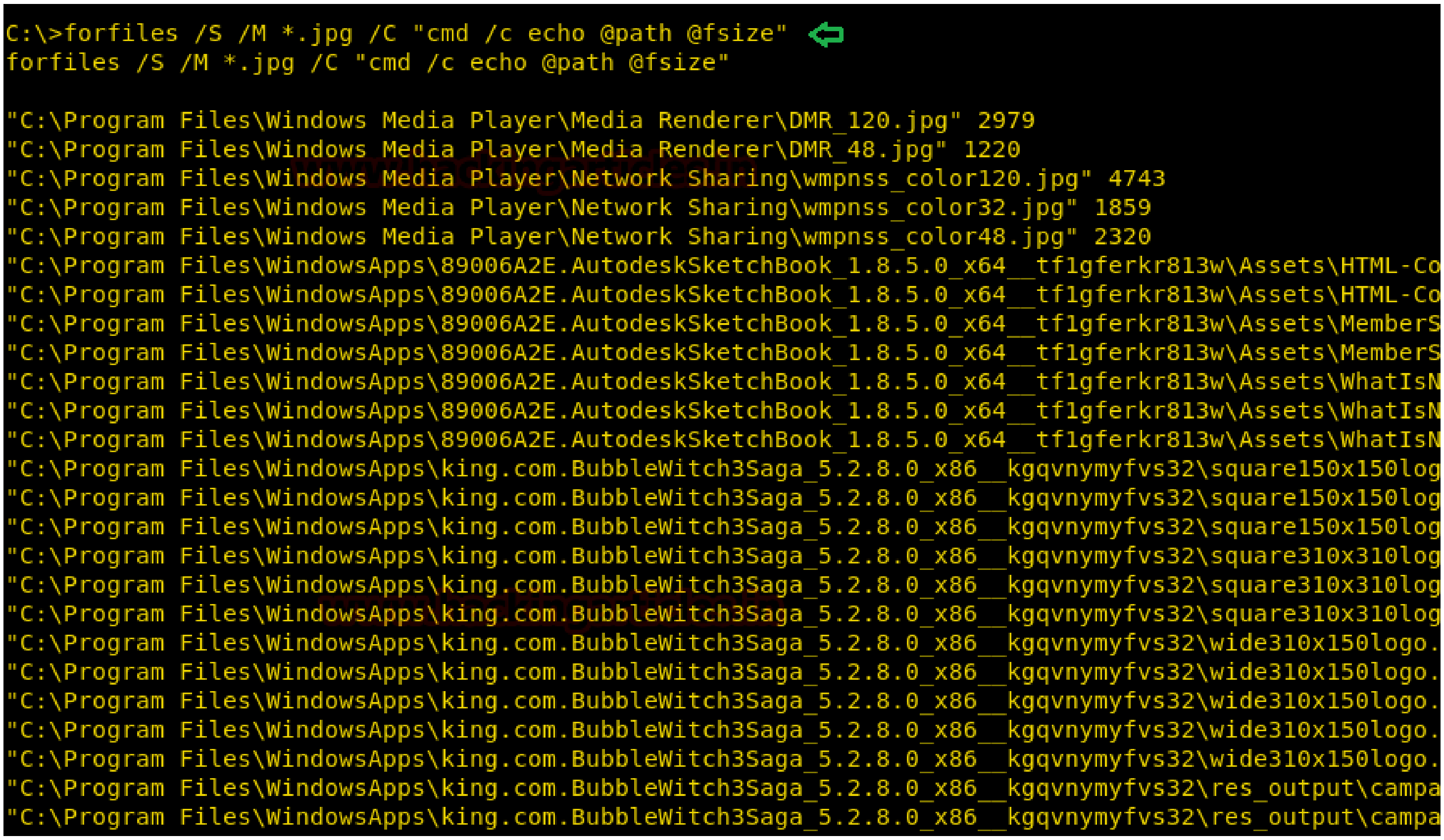


```
C:\>forfiles /p c: /S /D -10
forfiles /p c: /S /D -10

"$Recycle.Bin"
"$WINRE_BACKUP_PARTITION.MARKER"
"bootmgr"
"BOOTNXT"
"Intel"
"PerfLogs"
"Program Files"
"Program Files (x86)"
"ProgramData"
"Recovery"
"Users"
"Windows"
"S-1-5-18"
"desktop.ini"
"$I0ZVI7J.pdf"
"$I27J116.pdf"
"$I2FIYX7.pdf"
"$I8F54K3.mp4"
"$I8WB8LD.zip"
"$IEJ0BTG.pdf"
"$IH0Y1ZQ.png"
"$II767KF.pdf"
"$IQCVLNZ.pdf"
"$IS6ZTI4.pdf"
"$ISFGI48.pdf"
```

List path of all the image files with their size

In a scenario where we want to list image files with their path and size which were modified recently, we can use this command. Here we are using the @fsize extension to display the size of the files in bytes. We specified the extension .jpg this can be any extension we want to search. And then finally we used the @path to make the complete path listed in the output.

```
forfiles /S /M *.jpg /C "cmd /c echo @path @fsize"
```

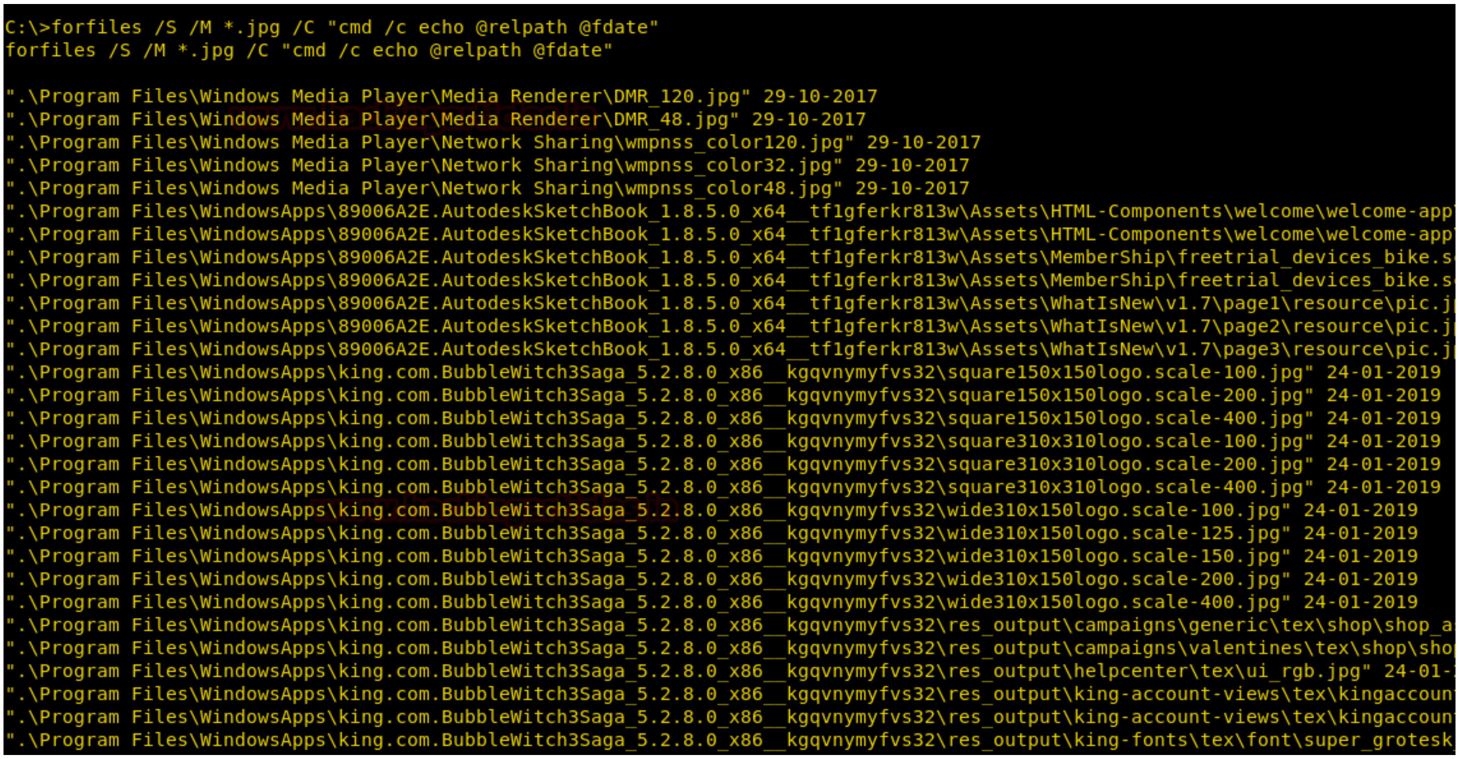


```
C:\>forfiles /S /M *.jpg /C "cmd /c echo @path @fsize"
forfiles /S /M *.jpg /C "cmd /c echo @path @fsize"

"C:\Program Files\Windows Media Player\Media Renderer\DMR_120.jpg" 2979
"C:\Program Files\Windows Media Player\Media Renderer\DMR_48.jpg" 1220
"C:\Program Files\Windows Media Player\Network Sharing\wmpnss_color120.jpg" 4743
"C:\Program Files\Windows Media Player\Network Sharing\wmpnss_color32.jpg" 1859
"C:\Program Files\Windows Media Player\Network Sharing\wmpnss_color48.jpg" 2320
"C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\HTML-Co
"C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\HTML-Co
"C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\MemberS
"C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\MemberS
"C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\WhatIsN
"C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\WhatIsN
"C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\WhatIsN
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square150x150log
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square150x150log
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square150x150log
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square310x310log
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square310x310log
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square310x310log
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\res_output\campa
"C:\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\res_output\campa
```

List all the image files with their Relative path and Date

In a scenario where we want to list the files with their relative path with the date on which modification was done, we can use this command. We specified the extension .jpg this can be any extension we want to search. Here we use a @fdate extension to display the date on which files were modified.

```
forfiles /S /M *.jpg /C "cmd /c echo @relpath @fdate"
```

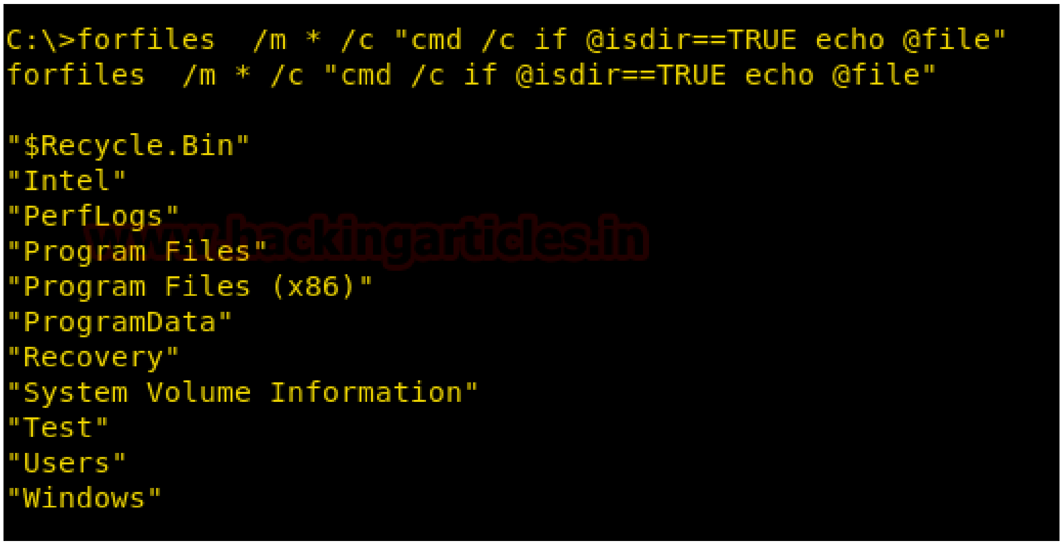


```
C:\>forfiles /S /M *.jpg /C "cmd /c echo @relpath @fdate"
forfiles /S /M *.jpg /C "cmd /c echo @relpath @fdate"

".\Program Files\Windows Media Player\Media Renderer\DMR_120.jpg" 29-10-2017
".\Program Files\Windows Media Player\Media Renderer\DMR_48.jpg" 29-10-2017
".\Program Files\Windows Media Player\Network Sharing\wmpnss_color120.jpg" 29-10-2017
".\Program Files\Windows Media Player\Network Sharing\wmpnss_color32.jpg" 29-10-2017
".\Program Files\Windows Media Player\Network Sharing\wmpnss_color48.jpg" 29-10-2017
".\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\HTML-Components\welcome\welcome-app
".\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\HTML-Components\welcome\welcome-app
".\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\MemberShip\freetrial_devices_bike.s
".\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\MemberShip\freetrial_devices_bike.s
".\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\WhatIsNew\v1.7\page1\resource\pic.j
".\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\WhatIsNew\v1.7\page2\resource\pic.j
".\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_1.8.5.0_x64__tf1gferkr813w\Assets\WhatIsNew\v1.7\page3\resource\pic.j
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square150x150logo.scale-100.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square150x150logo.scale-200.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square150x150logo.scale-400.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square310x310logo.scale-100.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square310x310logo.scale-200.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\square310x310logo.scale-400.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.scale-100.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.scale-125.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.scale-150.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.scale-200.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\wide310x150logo.scale-400.jpg" 24-01-2019
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\res_output\campaigns\generic\tex\shop\shop_a
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\res_output\campaigns\valentines\tex\shop\sho
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\res_output\helpcenter\tex\ui_rgb.jpg" 24-01-
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\res_output\king-account-views\tex\kingaccoun
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\res_output\king-account-views\tex\kingaccoun
".\Program Files\WindowsApps\king.com.BubbleWitch3Saga_5.2.8.0_x86__kgqvnymyfvs32\res_output\king-fonts\tex\font\super_grotesk
```

List all the sub-directories inside any directory

In a scenario where we want to list all the subdirectories inside a directory, we can use this command. Here we are using a logical statement to check the condition that the selected file is a directory or not. This is being checked using the @isdir extension.

```
forfiles /m * /c "cmd /c if @isdir==TRUE echo @file"
```



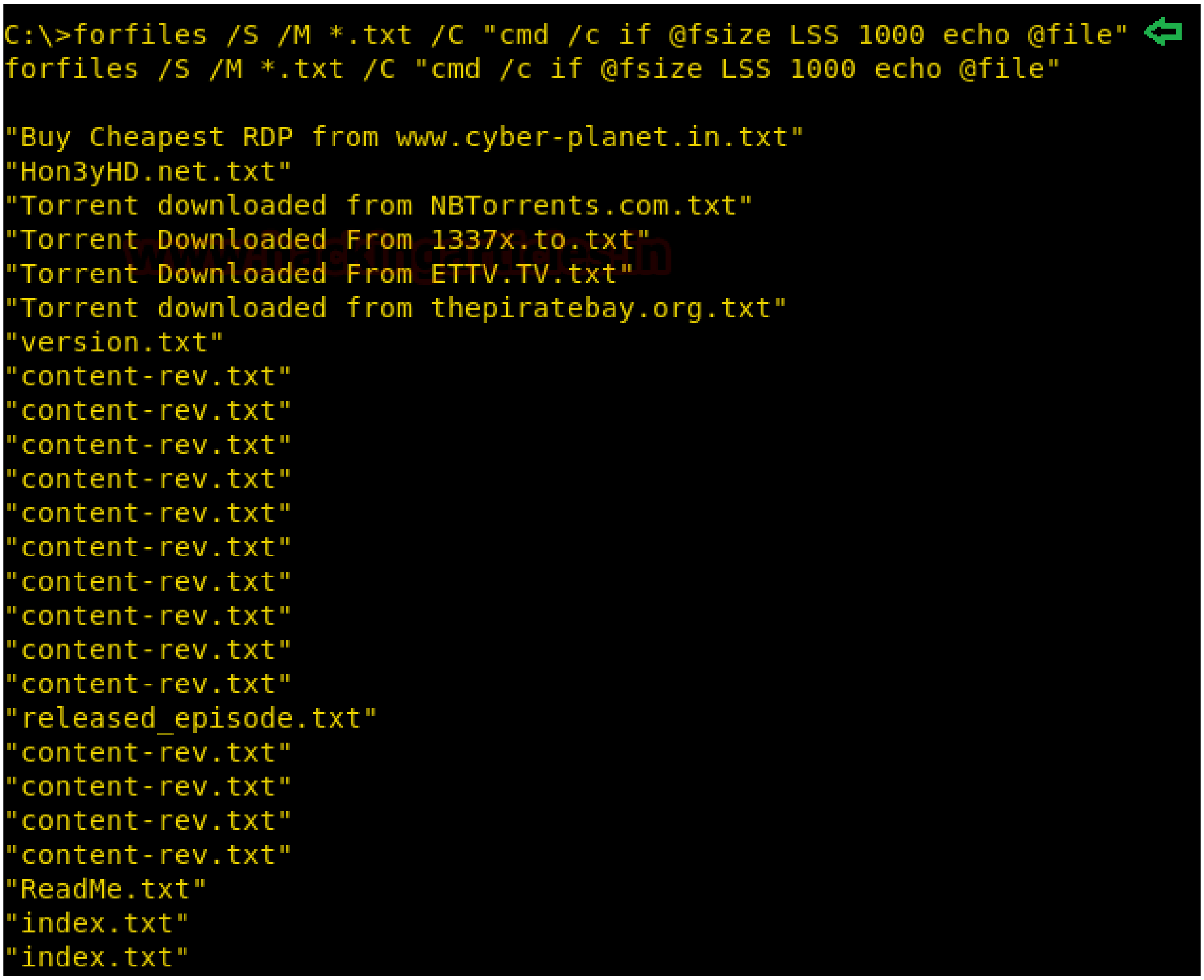
```
C:\>forfiles  /m * /c "cmd /c if @isdir==TRUE echo @file"
forfiles  /m * /c "cmd /c if @isdir==TRUE echo @file"

"$Recycle.Bin"
"Intel"
"PerfLogs"
"Program Files"
"Program Files (x86)"
"ProgramData"
"Recovery"
"System Volume Information"
"Test"
"Users"
"Windows"
```

List all the files of a particular extension and Size

In a scenario where we want to list the files with a particular extension and size, we can use this command. We specified the extension .txt this can be any extension we want to search. We use @fsize to specify the file size.

Also, we use LSS to limit the size of the files to a specified size.

```
forfiles /S /M *.txt /C "cmd /c if @fsize LSS 1000 echo @file"
```

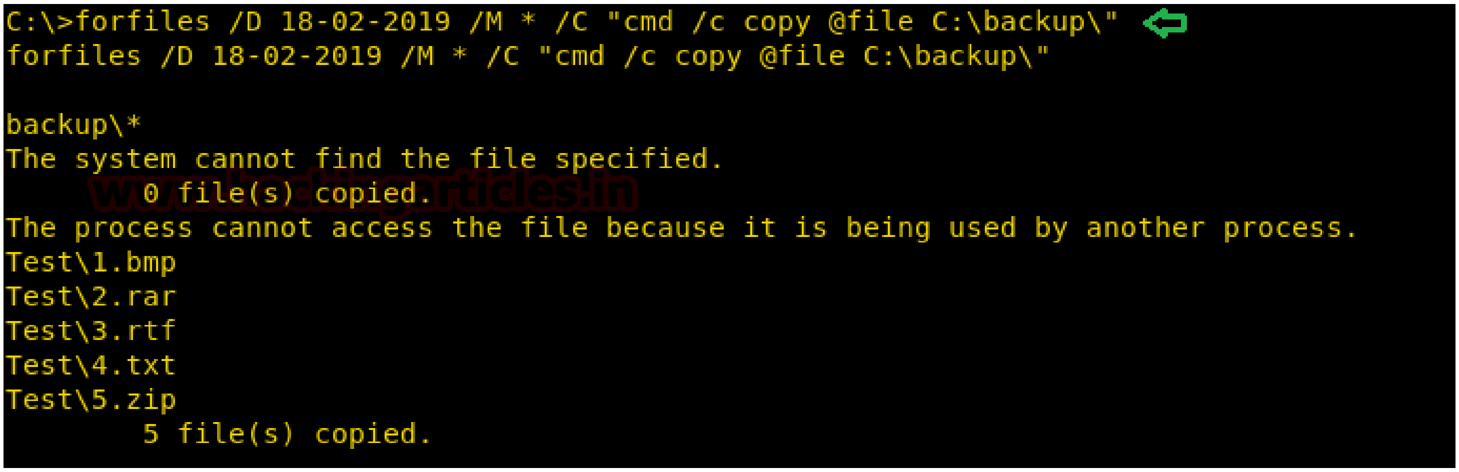


```
C:\>forfiles /S /M *.txt /C "cmd /c if @fsize LSS 1000 echo @file"
forfiles /S /M *.txt /C "cmd /c if @fsize LSS 1000 echo @file"

"Buy Cheapest RDP from www.cyber-planet.in.txt"
"Hon3yHD.net.txt"
"Torrent downloaded from NBTorrents.com.txt"
"Torrent Downloaded From 1337x.to.txt"
"Torrent Downloaded From ETTV.TV.txt"
"Torrent downloaded from thepiratebay.org.txt"
"version.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"released_episode.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"content-rev.txt"
"ReadMe.txt"
"index.txt"
"index.txt"
```

Backup files modified on a particular date

In a scenario where we want to take a backup or copy all the files that were modified on a particular date, we can use this command. Here we are using the date switch to define the number of days. We can change the number of days with /D to our requirement. Here we need to keep in mind that we need to first create the folder where we want to take backup otherwise, this command won’t get executed properly.

```
forfiles /D 18-02-2019 /M * /C "cmd /c copy @file C:\backup\"
```

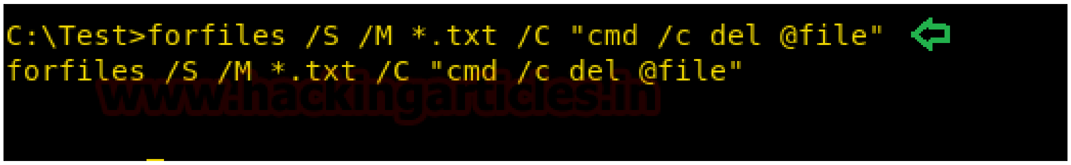


```
C:\>forfiles /D 18-02-2019 /M * /C "cmd /c copy @file C:\backup\"
forfiles /D 18-02-2019 /M * /C "cmd /c copy @file C:\backup\"

backup\*
The system cannot find the file specified.
        0 file(s) copied.
The process cannot access the file because it is being used by another process.
Test\1.bmp
Test\2.rar
Test\3.rtf
Test\4.txt
Test\5.zip
        5 file(s) copied.
```

Delete files of a particular extension

In a scenario where we want to delete some files, we can use this command. Here we are using the /c parameter to specify the del command that will delete files. Also, we are specifying an extension to sort the files to delete. We can use any condition instead of the extension and the command will work fine. Here we need to keep in mind that we need to run this command in the directory where we want to delete files. Like in our case we used it a directory named Test

```
forfiles /S /M *.txt /C "cmd /c del @file"
```



```
C:\Test>forfiles /S /M *.txt /C "cmd /c del @file"
forfiles /S /M *.txt /C "cmd /c del @file"
```