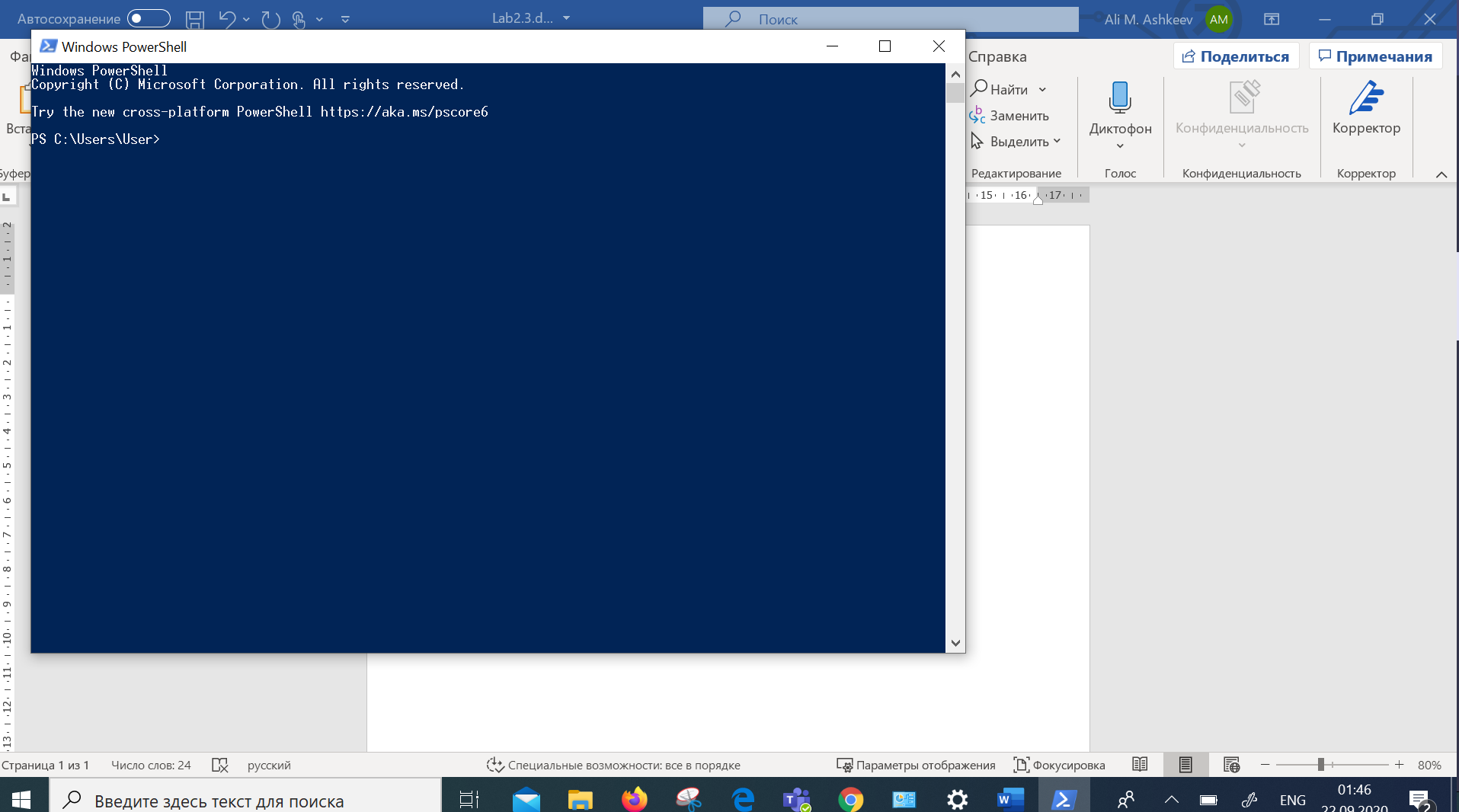
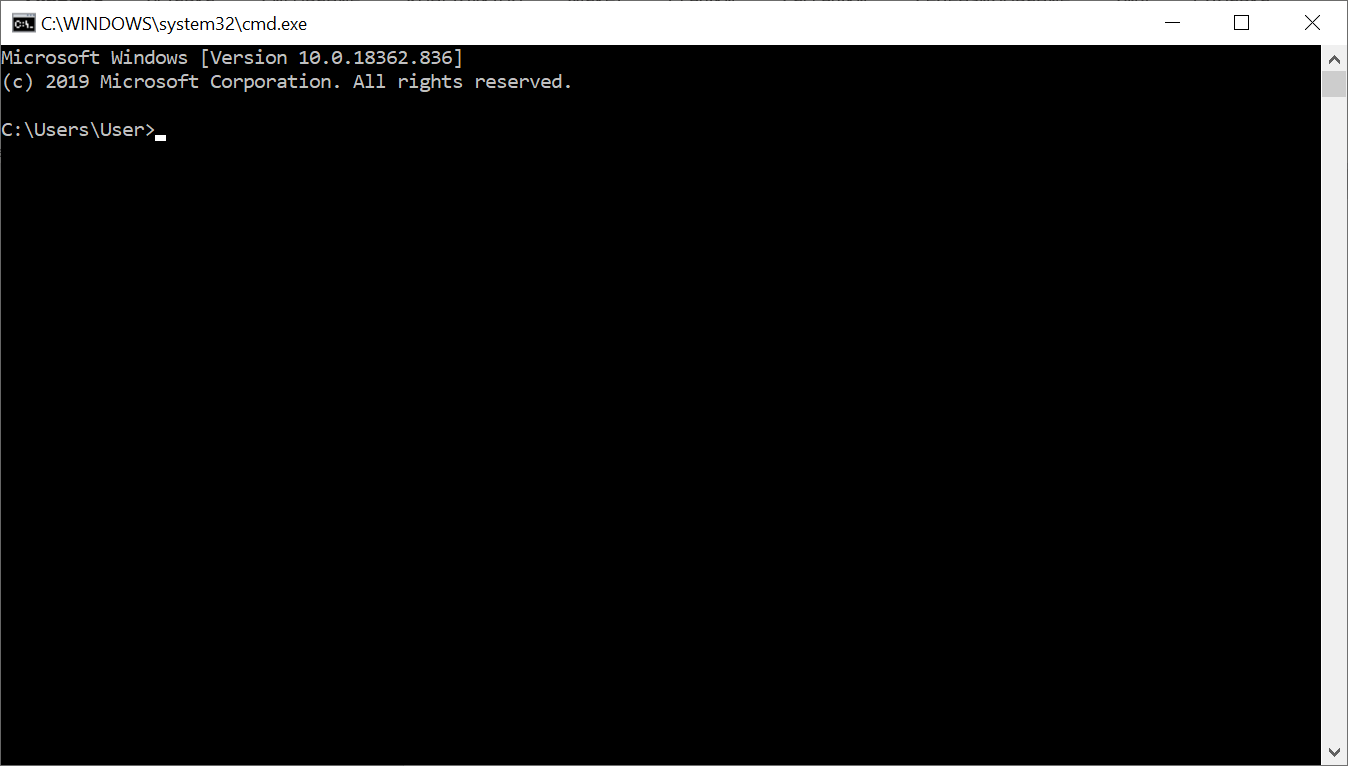
Ali Ashkeyev 18BD11079

Lab – Using Windows PowerShell

Objectives The objective of the lab is to explore some of the functions of PowerShell.

Step 1: Access PowerShell console.

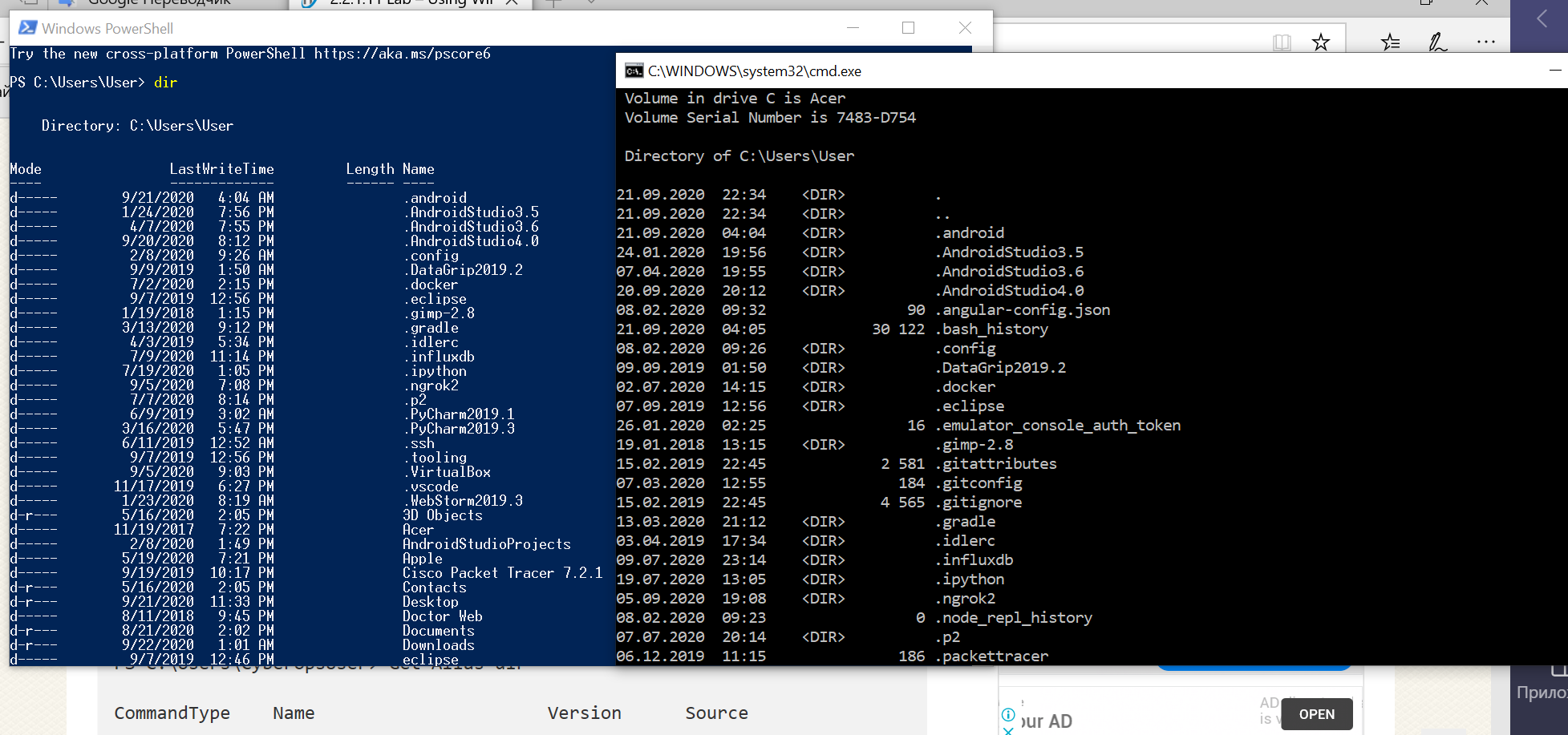




**Step 2: Explore Command Prompt and PowerShell commands.**

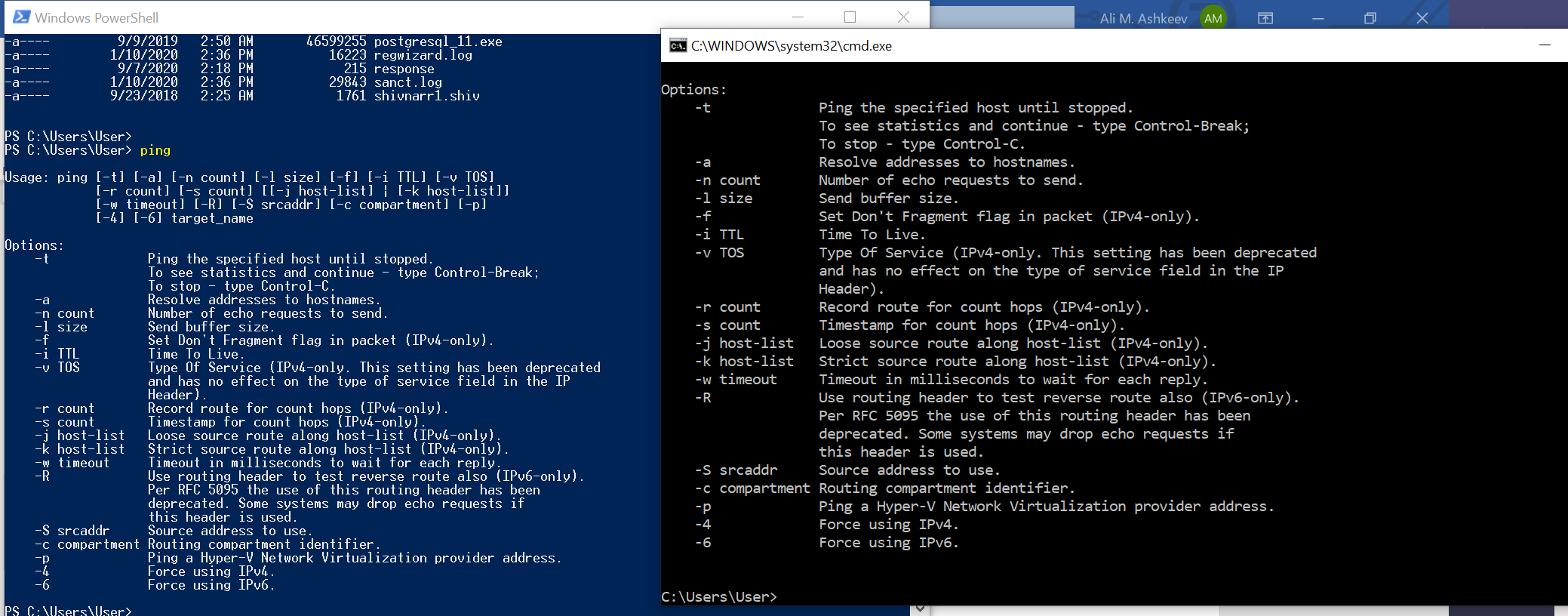
1. What are the outputs to the dir command?

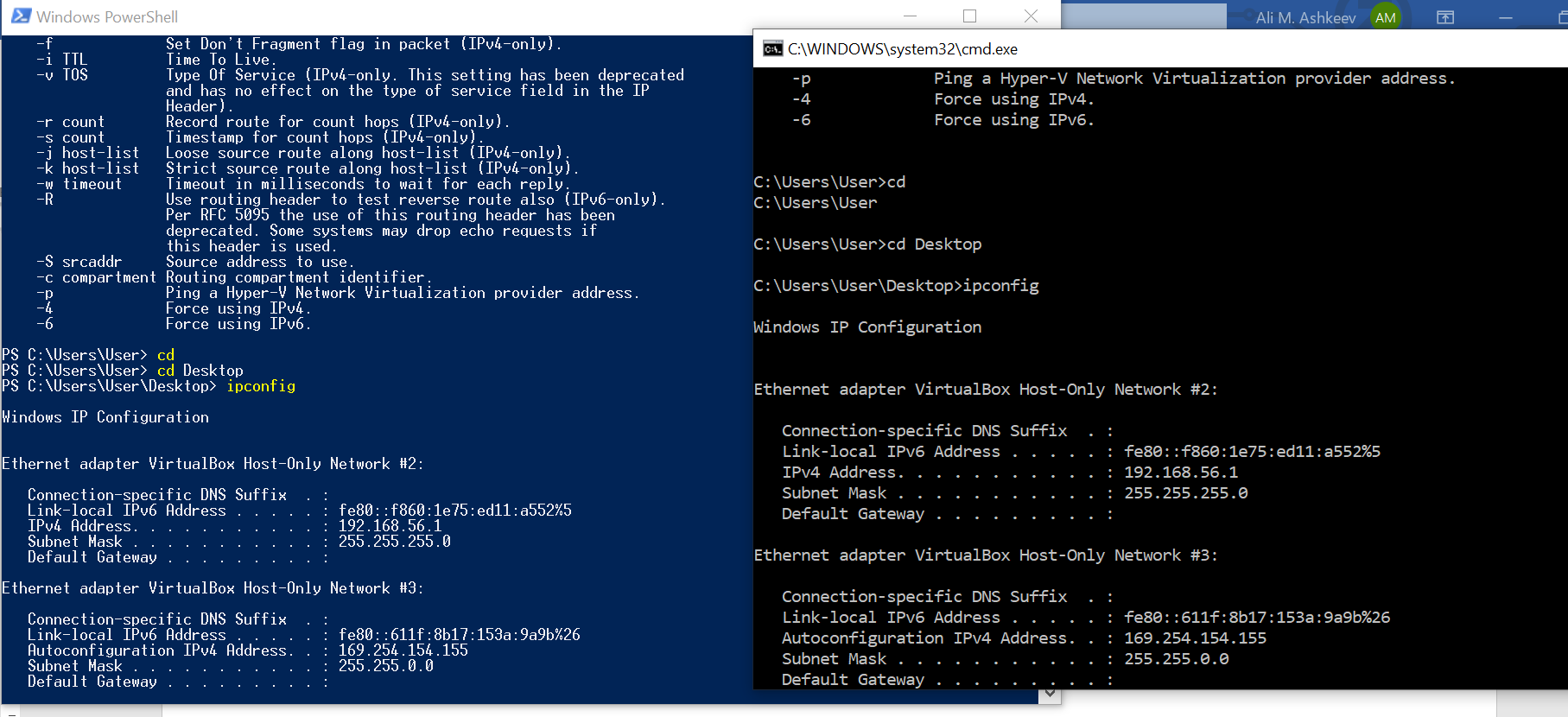
It shows subdirectories and files and information about them date,time,size and type. In power shell it shows mode



1. Try another command that you have used in the command prompt, such as ping, cd, and ipconfig. What are the results?

Same result ping shows instruction and if write ping vk.com it shows sending packets, cd moves to directory and ipconfig shows ip settings(configurations)

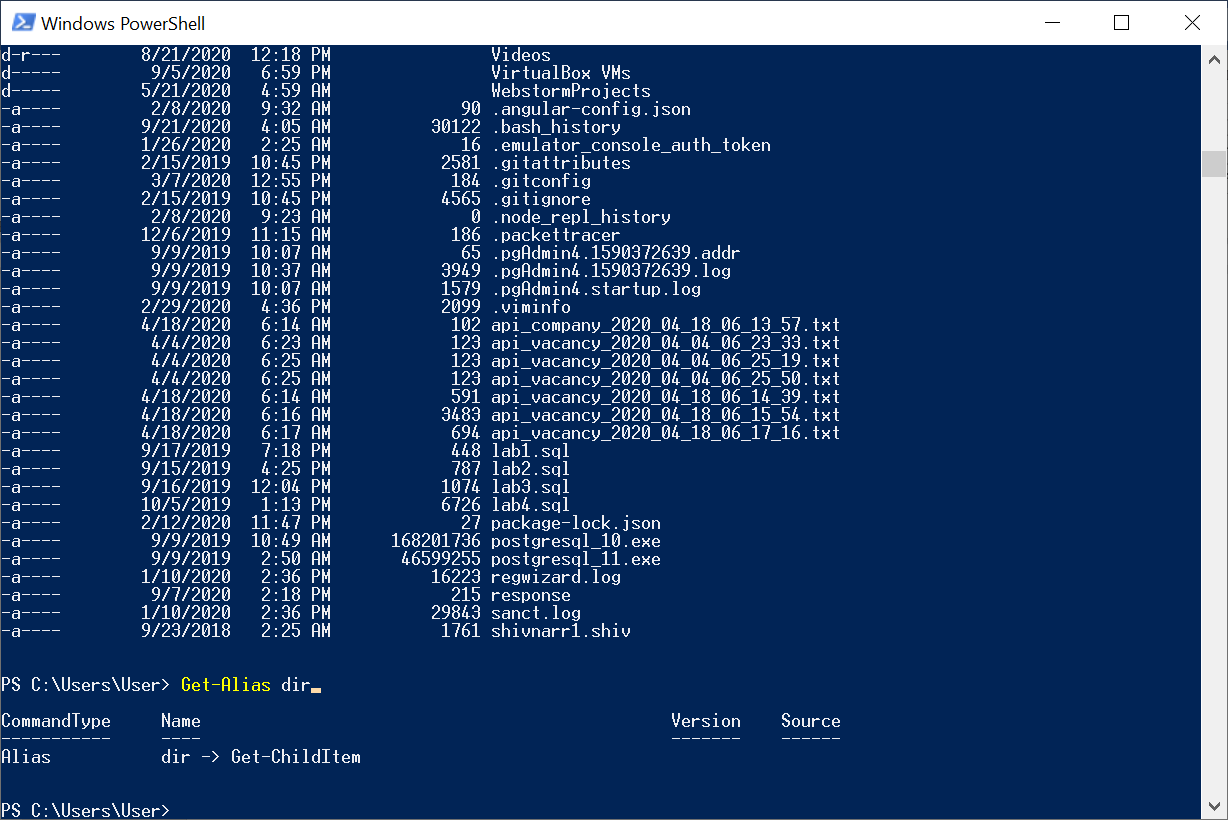




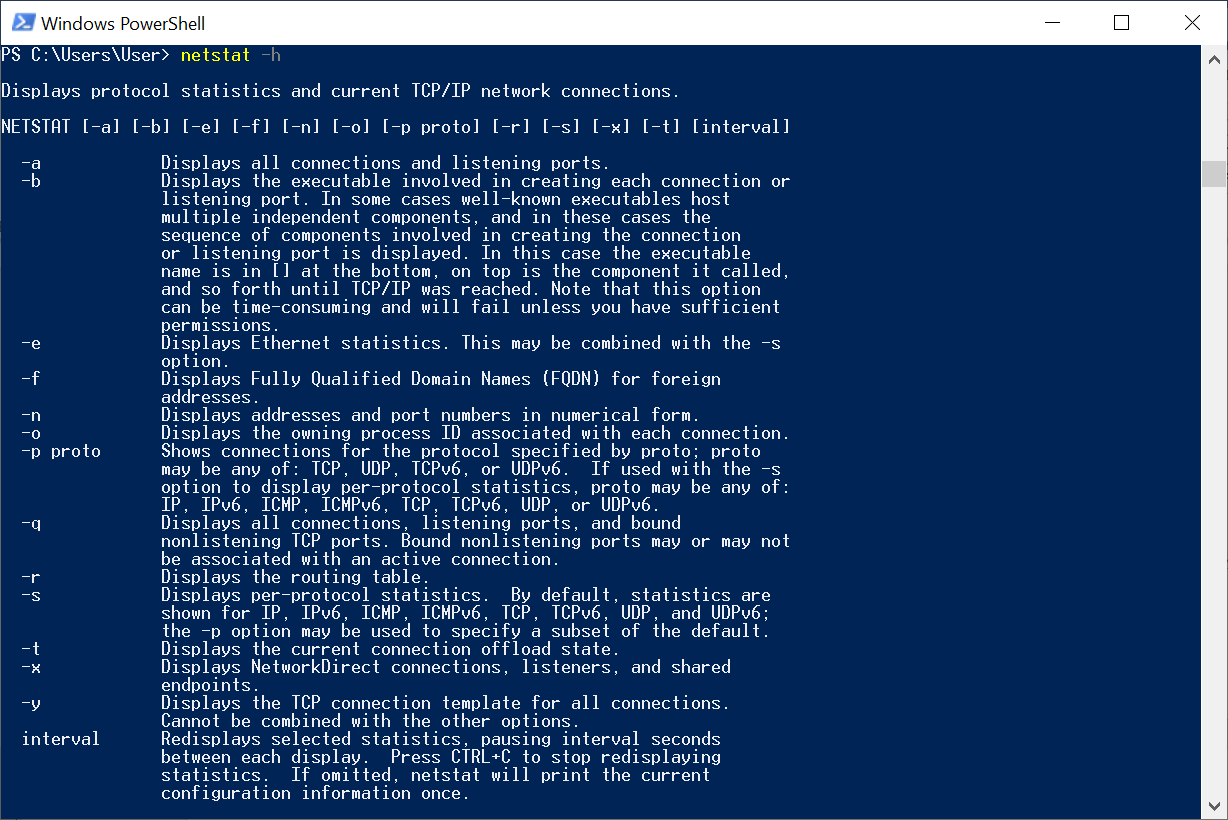
Step 3: Explore cmdlets.

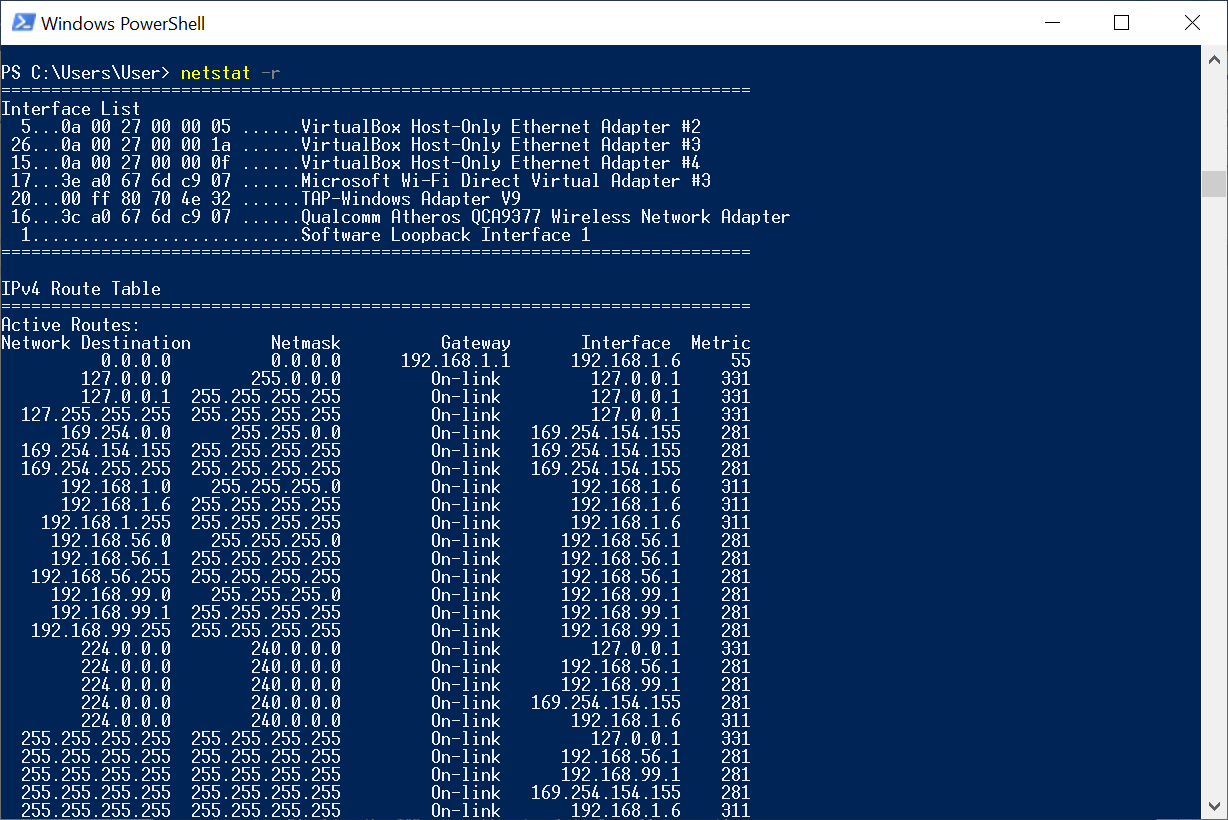
1. What is the PowerShell command for dir?

Get-ChildItem



Step 4: Explore the netstat command using PowerShell.

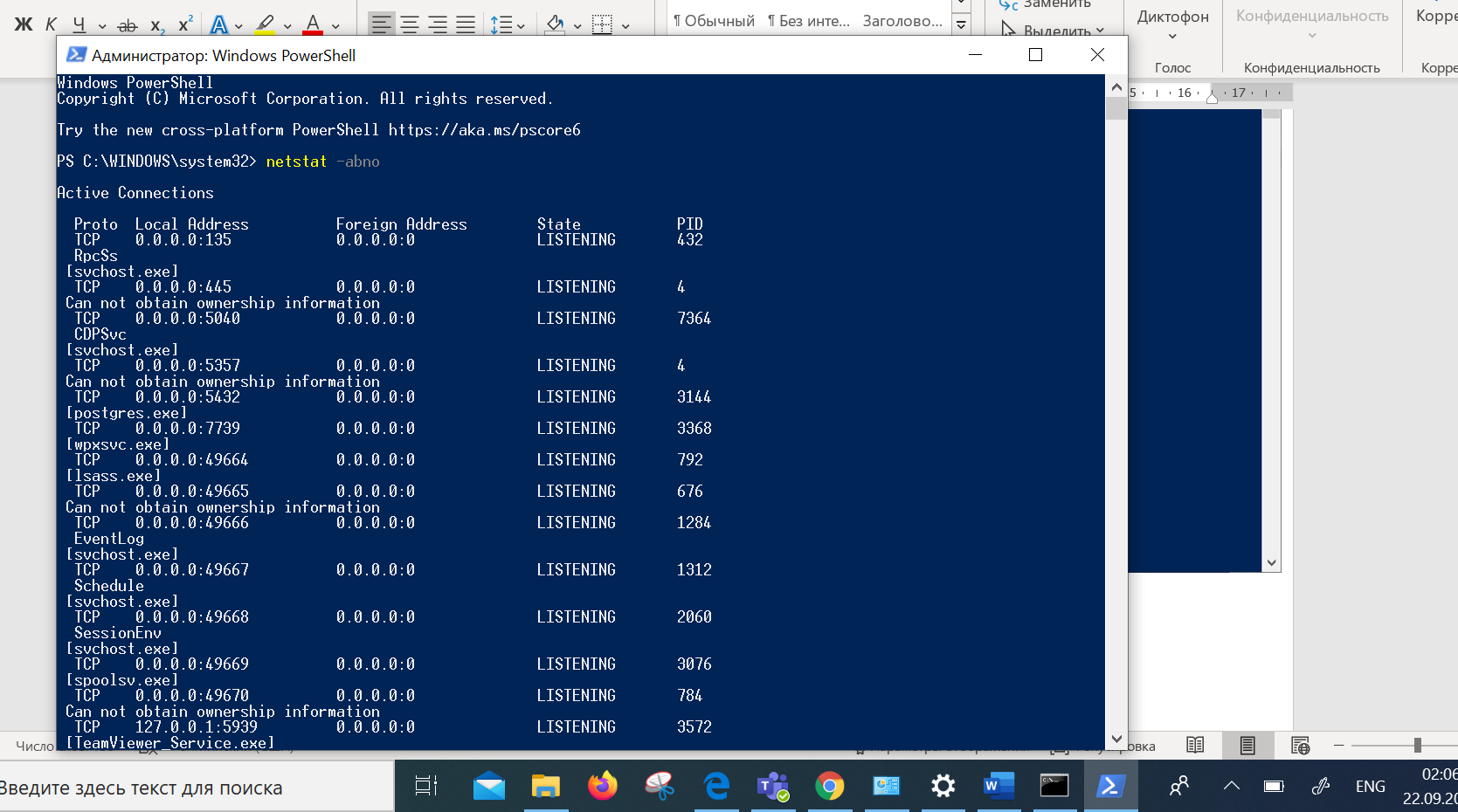
1. 
2. Netstat -r



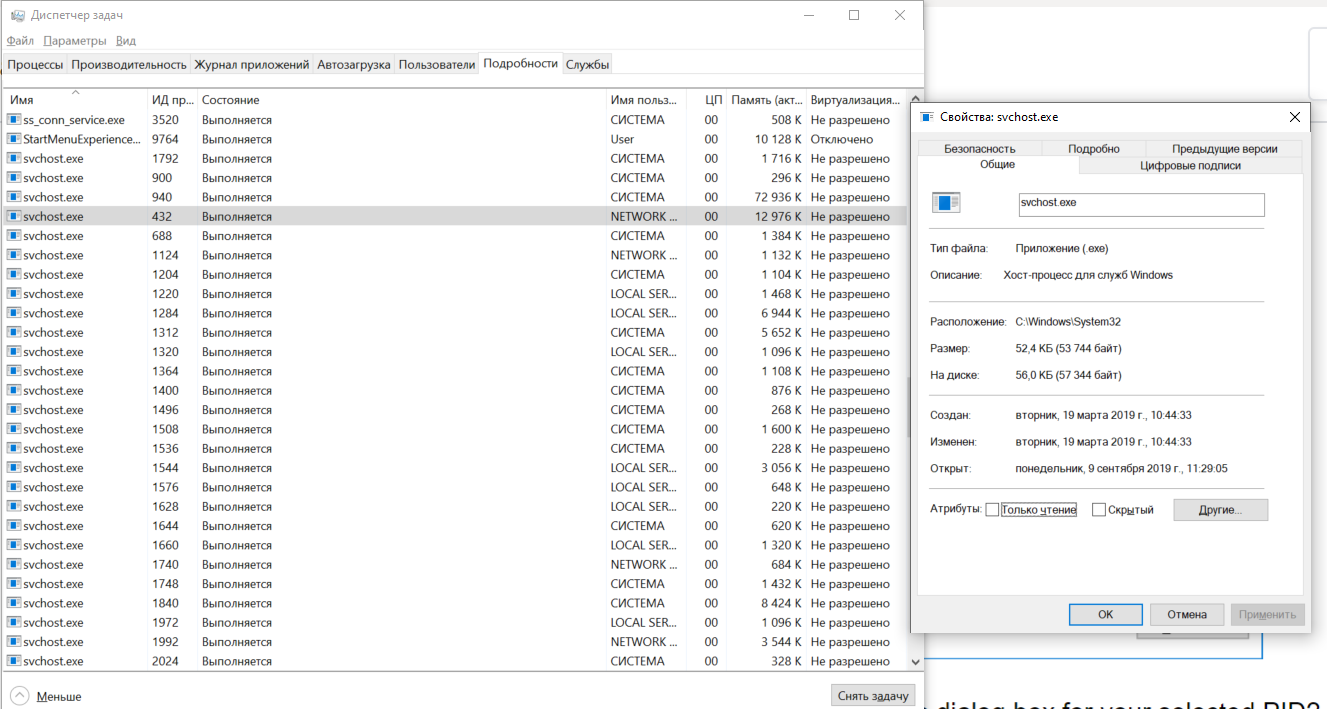
What is the IPv4 gateway?

192.168.1.1

d.netstat -abno



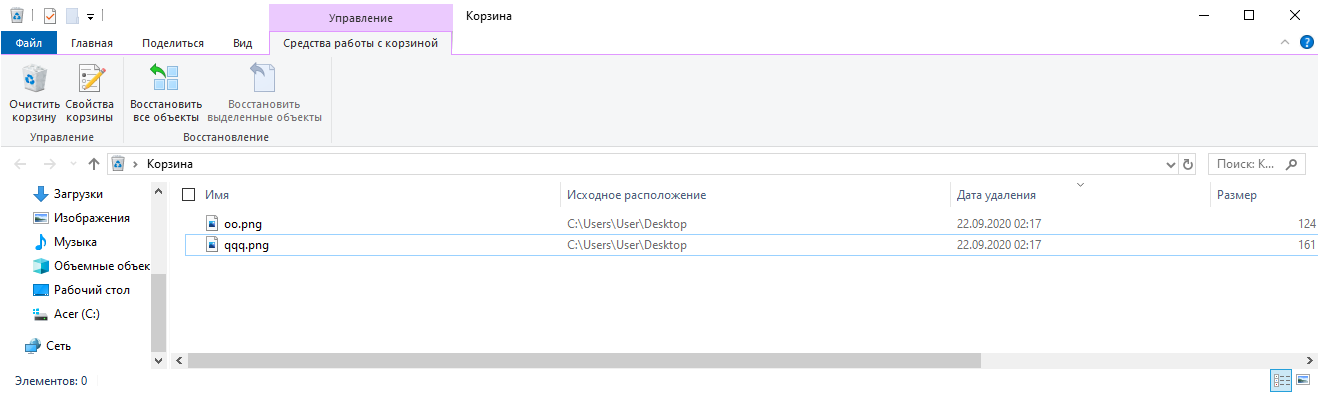
g.PID=432 svchost details



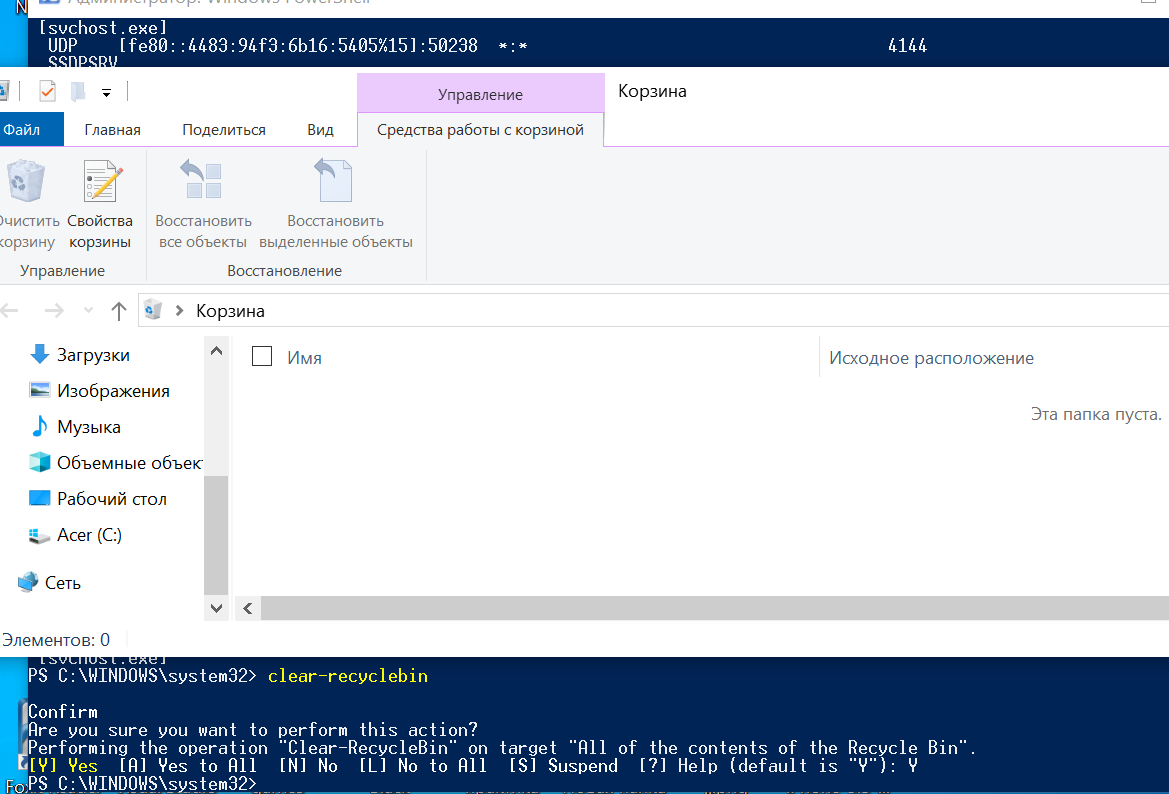
PID=432 attached to svhost.exe with user Network Service and using 12976K of memory.

Step 5: Empty recycle bin using PowerShell.

Bin before clearing



Clearing recyclebin



What happened to the files in the Recycle Bin?

Recycle Bin was cleared and files in it deleted.

Reflection

PowerShell was developed for task automation and configuration management. Using the Internet, research commands that you could use to simplify your tasks as a security analyst. Record your findings.

The “Get-UserLockCommand” command lists all the commands provided by the UserLock module.

To administer a remote UserLock server, change the variable $UserLockServerName by running: $UserLockServerName = <remote UserLock server>

Set-ExecutionPolicy command to control the level of security surrounding PowerShell scripts: Set-ExecutionPolicy Unrestricted

Sometimes, it's helpful to create a report you can send to someone. One way of accomplishing this is by using the ConvertTo-HTML commandЖGet-Service | ConvertTo-HTML -Property Name, Status > C:\services.htm