

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Факультет физики и информационных технологий

Кафедра общей физики

Обработка текста в ОС Windows

Отчет по лабораторной работе №4

Исполнитель
студент группы КИ-22:

Д.В.Скреженцевский

Проверил
ст. преподаватель:

В.В.Грищенко

Гомель 2025

Цель работы: Изучить основные принципы работы с текстом и текстовыми файлами в Windows.

1 Ознакомиться и изучить на практике программы и утилиты, предназначенные для работы с текстом в операционных системах Linux и Windows.

2. При помощи механизма перенаправления записать в файл output.txt содержимое домашнего каталога.

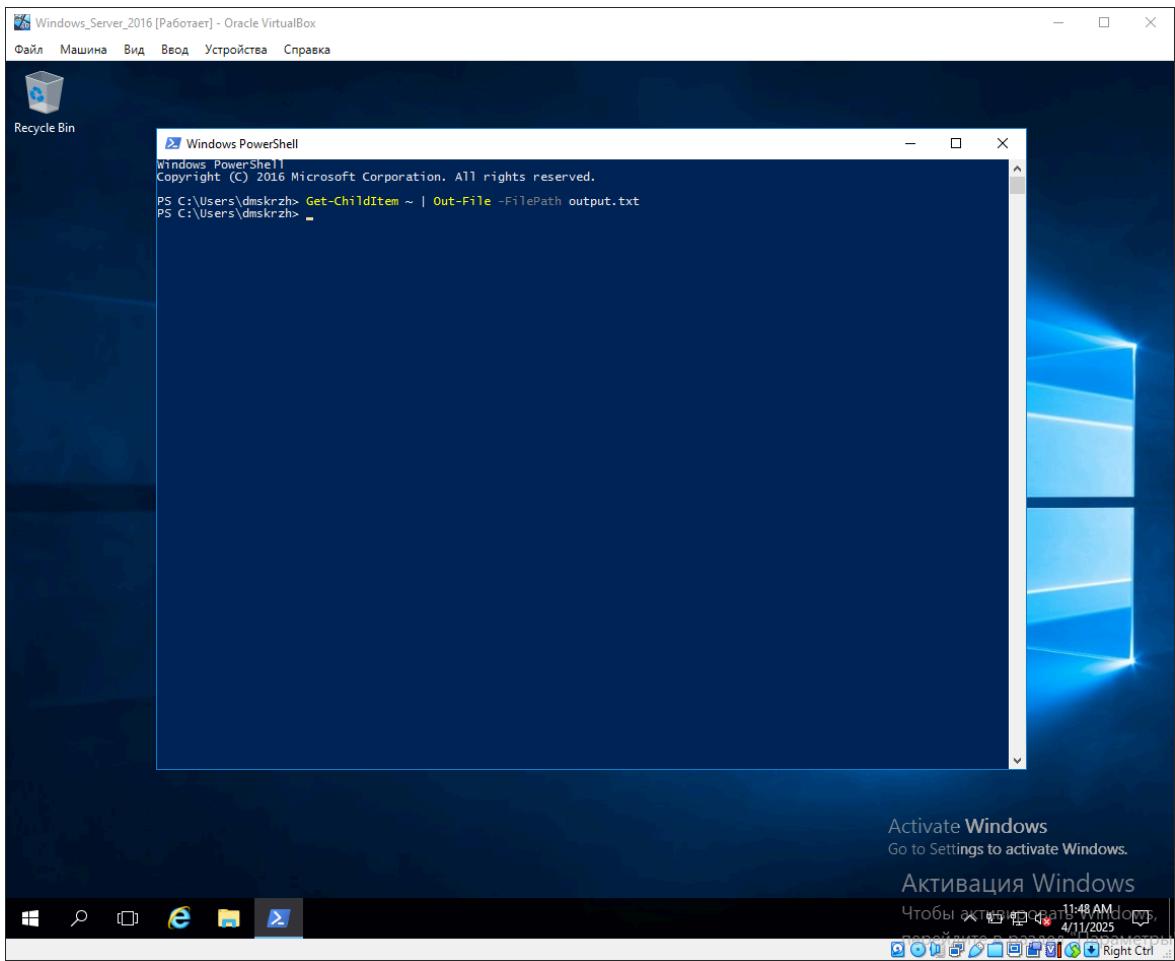
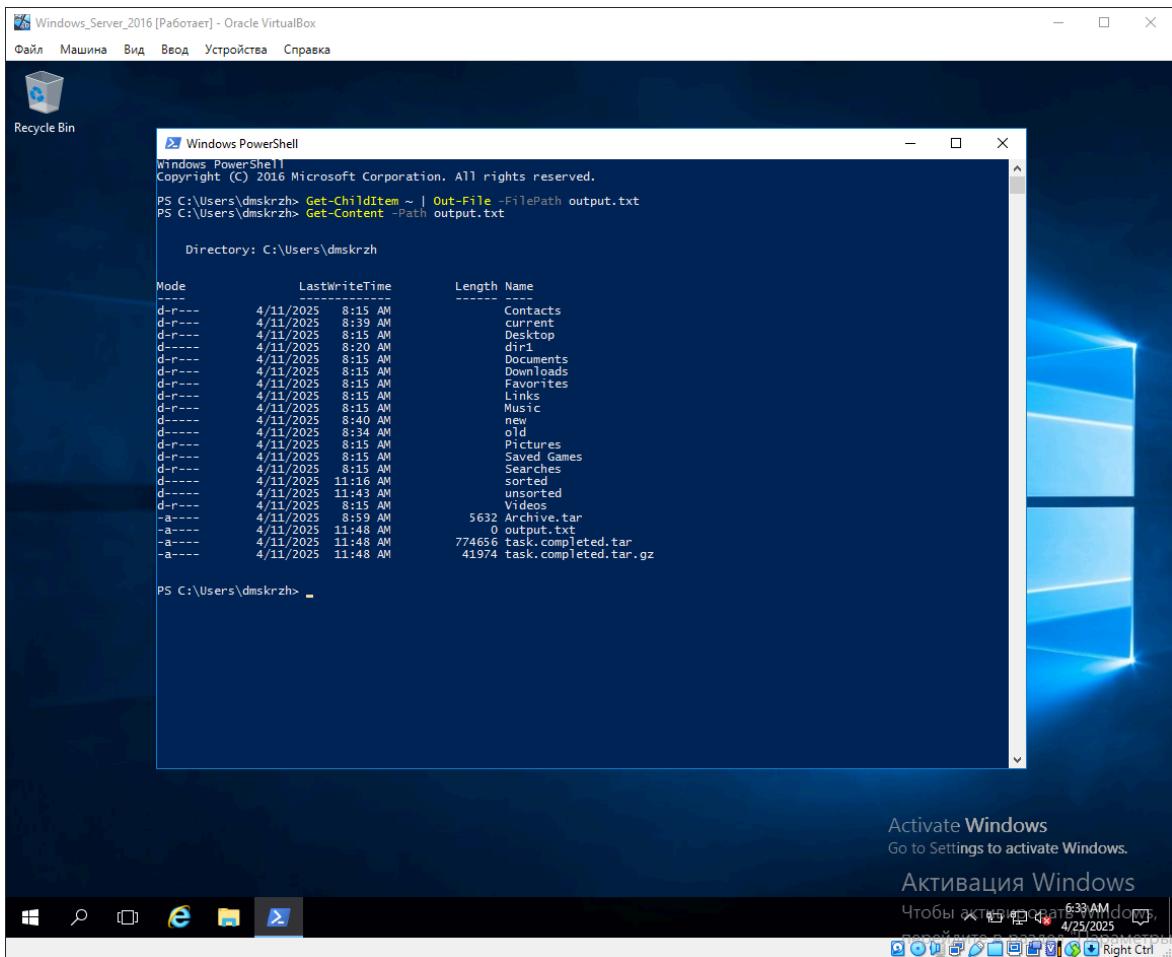


Рисунок 1 - Запись содержимого домашнего каталога в файл

3. Вывести на экран содержимое файла output.txt.



The screenshot shows a Windows Server 2016 desktop environment within Oracle VirtualBox. A Windows PowerShell window is open, displaying the command PS C:\Users\dmskrzh> Get-ChildItem ~ | Out-File -FilePath output.txt followed by the output of a directory listing. The output shows various folders and files in the user's home directory, including Contacts, current, Desktop, dir1, Documents, Downloads, Favorites, Links, Music, new, old, Pictures, Saved Games, Searches, sort, unsorted, Videos, Archive.tar, 0 output.txt, task.completed.tar, and task.completed.tar.gz. The desktop background is the standard Windows 10 blue gradient. A taskbar at the bottom shows icons for File Explorer, Task View, Edge browser, File Explorer again, and Task View again. A system tray icon for 'Активация Windows' (Windows Activation) is visible.

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\dmskrzh> Get-ChildItem ~ | Out-File -FilePath output.txt
PS C:\Users\dmskrzh> Get-Content -Path output.txt

Directory: C:\Users\dmskrzh

Mode LastWriteTime      Name
---- -----      ----
d-r--- 4/11/2025 8:15 AM Contacts
d-r--- 4/11/2025 8:39 AM current
d-r--- 4/11/2025 8:15 AM Desktop
d----- 4/11/2025 8:20 AM dir1
d-r--- 4/11/2025 8:15 AM Documents
d-r--- 4/11/2025 8:15 AM Downloads
d-r--- 4/11/2025 8:15 AM Favorites
d----- 4/11/2025 8:15 AM Links
d-r--- 4/11/2025 8:15 AM Music
d----- 4/11/2025 8:40 AM new
d----- 4/11/2025 8:34 AM old
d-r--- 4/11/2025 8:15 AM Pictures
d-r--- 4/11/2025 8:15 AM Saved Games
d-r--- 4/11/2025 8:15 AM Searches
d----- 4/11/2025 8:15 AM sort
d----- 4/11/2025 11:43 AM unsorted
d-r--- 4/11/2025 8:15 AM Videos
-a---- 4/11/2025 8:59 AM 5632 Archive.tar
-a---- 4/11/2025 11:48 AM 0 output.txt
-a---- 4/11/2025 11:48 AM 774656 task.completed.tar
-a---- 4/11/2025 11:48 AM 41974 task.completed.tar.gz

PS C:\Users\dmskrzh>
```

Рисунок 2 - Вывод содержимого домашнего каталога из файла

4. Произвести замену знаков препинания (.,-) на знак + в файле output.txt. Результат сохранить в файле result.txt.

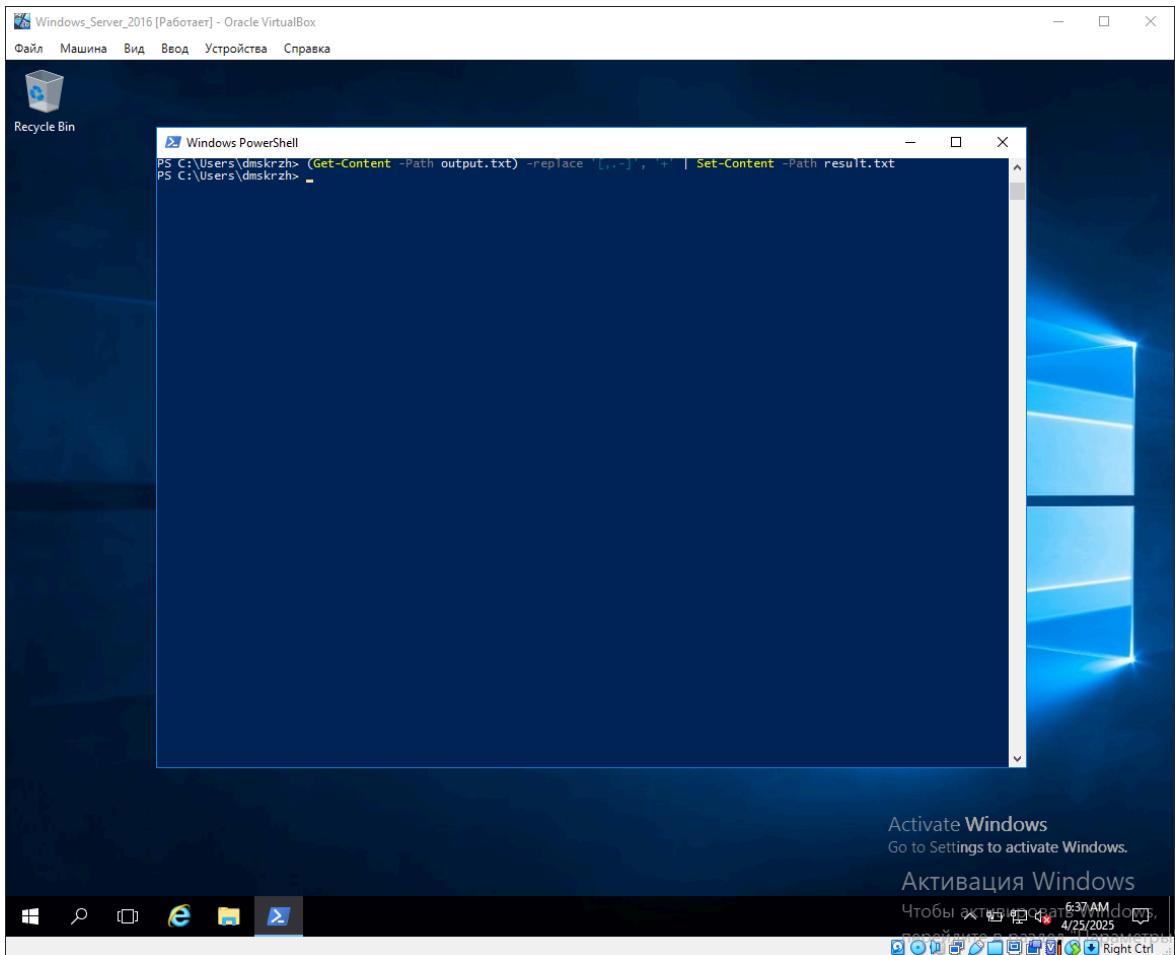


Рисунок 3 - Выполнение замены знаков

5. Результат замены вывести на экран.

The screenshot shows a Windows Server 2016 desktop environment. A PowerShell window is open, displaying the output of the command `Get-Content -Path result.txt`. The output lists various files and folders in the current directory (C:\Users\dmkskrzh) with their last write times and lengths. Below the PowerShell window, the taskbar is visible with several pinned icons. A watermark for 'Activate Windows' and 'Go to Settings to activate Windows.' is present in the center of the screen.

```
PS C:\Users\dmkskrzh> Get-Content -Path result.txt

Directory: C:\Users\dmkskrzh

Mode                LastWriteTime         Length Name
----                -----        +---+ +---+
d+r++ 4/11/2025 8:15 AM          0 Contacts
d+r++ 4/11/2025 8:39 AM          0 current
d+r++ 4/11/2025 8:15 AM          0 Desktop
d+r++ 4/11/2025 8:15 AM          0 dir
d+r++ 4/11/2025 8:15 AM          0 Documents
d+r++ 4/11/2025 8:15 AM          0 Downloads
d+r++ 4/11/2025 8:15 AM          0 Favorites
d+r++ 4/11/2025 8:15 AM          0 Links
d+r++ 4/11/2025 8:15 AM          0 Music
d+r++ 4/11/2025 8:40 AM          0 new
d+r++ 4/11/2025 8:39 AM          0 old
d+r++ 4/11/2025 8:15 AM          0 Pictures
d+r++ 4/11/2025 8:15 AM          0 Saved Games
d+r++ 4/11/2025 8:15 AM          0 Searches
d+r++ 4/11/2025 11:16 AM          0 sorted
d+r++ 4/11/2025 11:43 AM          0 unsorted
d+r++ 4/11/2025 8:15 AM          5632 Videos
+a+r++ 4/11/2025 8:15 AM          0 Archivertar
+a+r++ 4/11/2025 11:48 AM          0 output.txt
+a+r++ 4/11/2025 11:48 AM          774656 task+completed+tar
+a+r++ 4/11/2025 11:48 AM          41974 task+completed+tar+gz

PS C:\Users\dmkskrzh>
```

Рисунок 4 - Вывод результата замены

6. Сбор системной информации:

6.1 Сохранить текущую загрузку дисков (размеры) в файл hdd.txt:

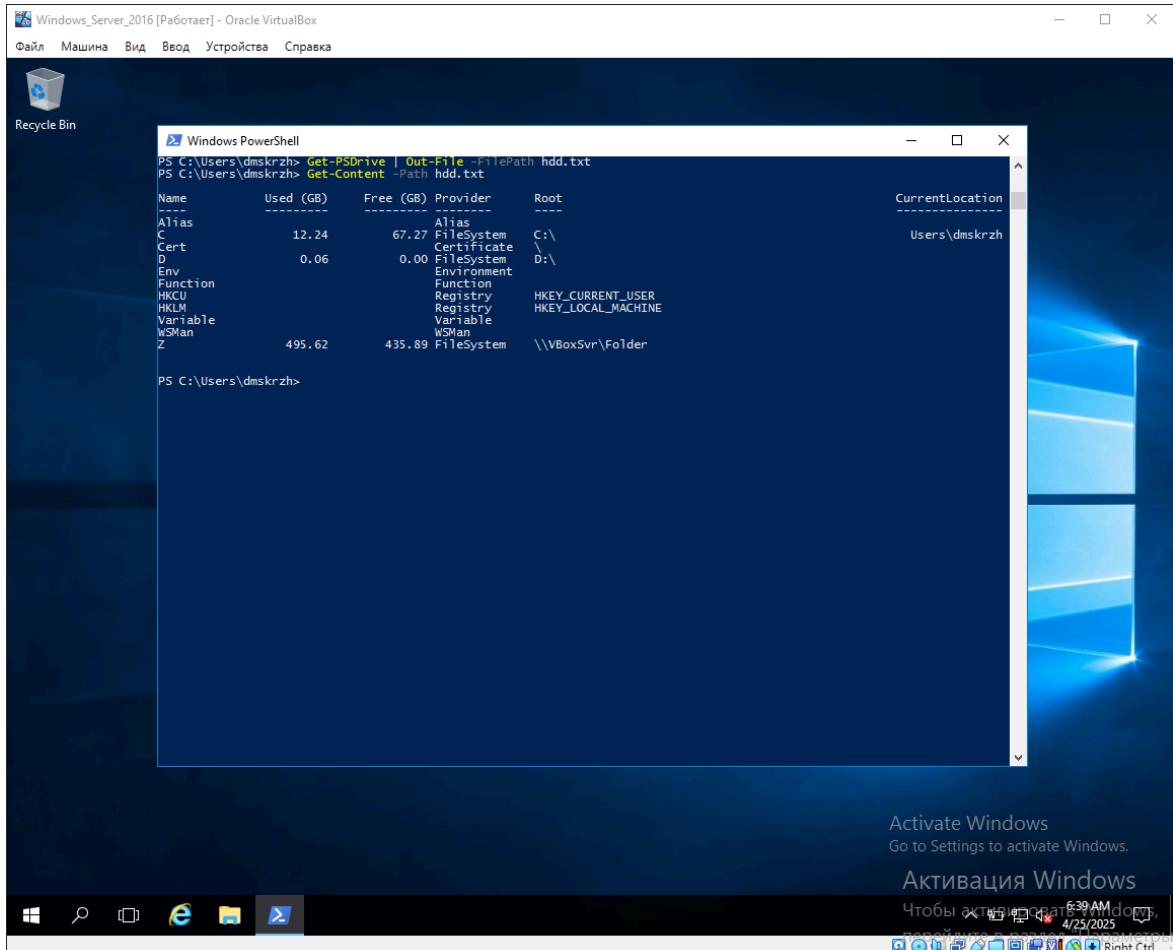


Рисунок 5 - Запись загрузки дисков

6.2 Сохранить текущий список процессов пользователей в файл pl.txt:

The screenshot shows a Windows Server 2016 desktop environment within Oracle VirtualBox. A PowerShell window titled 'Windows PowerShell' is open, displaying a command-line session. The command run is:

```
PS C:\Users\dmskrzh> Get-Process | Out-File -FilePath pl.txt  
PS C:\Users\dmskrzh> Get-Content -Path pl.txt
```

The output is a table of processes, listing Handles, NPM(K), PM(K), WS(K), CPU(s), Id, SI, and ProcessName. The table includes numerous system processes like ApplicationFrameHost, csrss, explorer, and svchost, along with user-specific processes.

Handles	NPM (K)	PM (K)	WS (K)	CPU (s)	Id	SI	ProcessName
203	14	4100	17472	35.92	1	ApplicationFrameHost	
485	27	15440	29328	0.27	4560	2	comnTaskHost
131	11	3108	13984	0.19	3788	2	conhost
241	10	1880	4704		384	0	csrss
183	11	1940	13200		460	1	csrss
234	15	1904	6396		1112	2	csrss
141	10	3104	13856		2812	1	DataExchangeHost
142	10	2596	13572	0.00	5600	2	DataExchangeHost
326	26	1280	32484		304	0	dum
343	26	29284	52204		1472	2	dum
1308	57	19344	72252		2924	1	explorer
1569	63	25296	90104	8.53	3296	2	explorer
0	0	0	4		0	0	Idle
985	23	6808	16488		596	0	lsass
241	12	2920	10492		5012	0	MpCmdRun
168	12	2764	9700		3864	0	msdtc
497	202	279568	233752		11844	0	PowerEng
689	31	64272	75264	0.70	3888	2	powershell
207	13	4424	17428		2472	1	RuntimeBroker
565	27	14360	31756	1.63	4452	2	RuntimeBroker
556	28	11728	44188		2400	1	SearchUI
642	33	14660	53048	0.81	4948	2	SearchUI
232	9	3124	7124		588	0	services
649	29	2024	57250		226	0	ShellExperienceHost
855	35	20548	63856	1.25	4848	2	ShellExperienceHost
368	15	3892	19540		2508	1	sihost
373	15	3960	19556	0.36	2776	2	sihost
54	2	392	1196		288	0	smss
426	22	5696	15612		1592	0	spoolsv
311	19	4588	20612	0.05	140	2	svchost
52	18	13726	23154		340	0	svchost
453	54	12164	17948		348	0	svchost
731	21	6376	20028		672	0	svchost
670	17	5232	11204		740	0	svchost
2142	103	38596	69284		864	0	svchost
535	28	11656	21556		900	0	svchost
815	37	10972	27468		1032	0	svchost
163	12	2020	6904		1080	0	svchost
775	193	14720	29344		1160	0	svchost
198	13	2164	7716		1668	0	svchost
266	23	6564	18264		1700	0	svchost
447	23	8516	23876		1744	0	svchost
288	18	4360	19248		2536	1	svchost
187	15	1856	6860		6124	0	svchost
1003	0	128	140		4	0	System

Activate Windows
Go to Settings to activate Windows.
Активация Windows
Чтобы активировать Windows, нажмите **Next**.
6:40 AM 4/25/2025
Right Ctrl

Рисунок 6 - Запись списка процессов

6.3 Сохранить информацию о процессоре в файл cpu.txt:

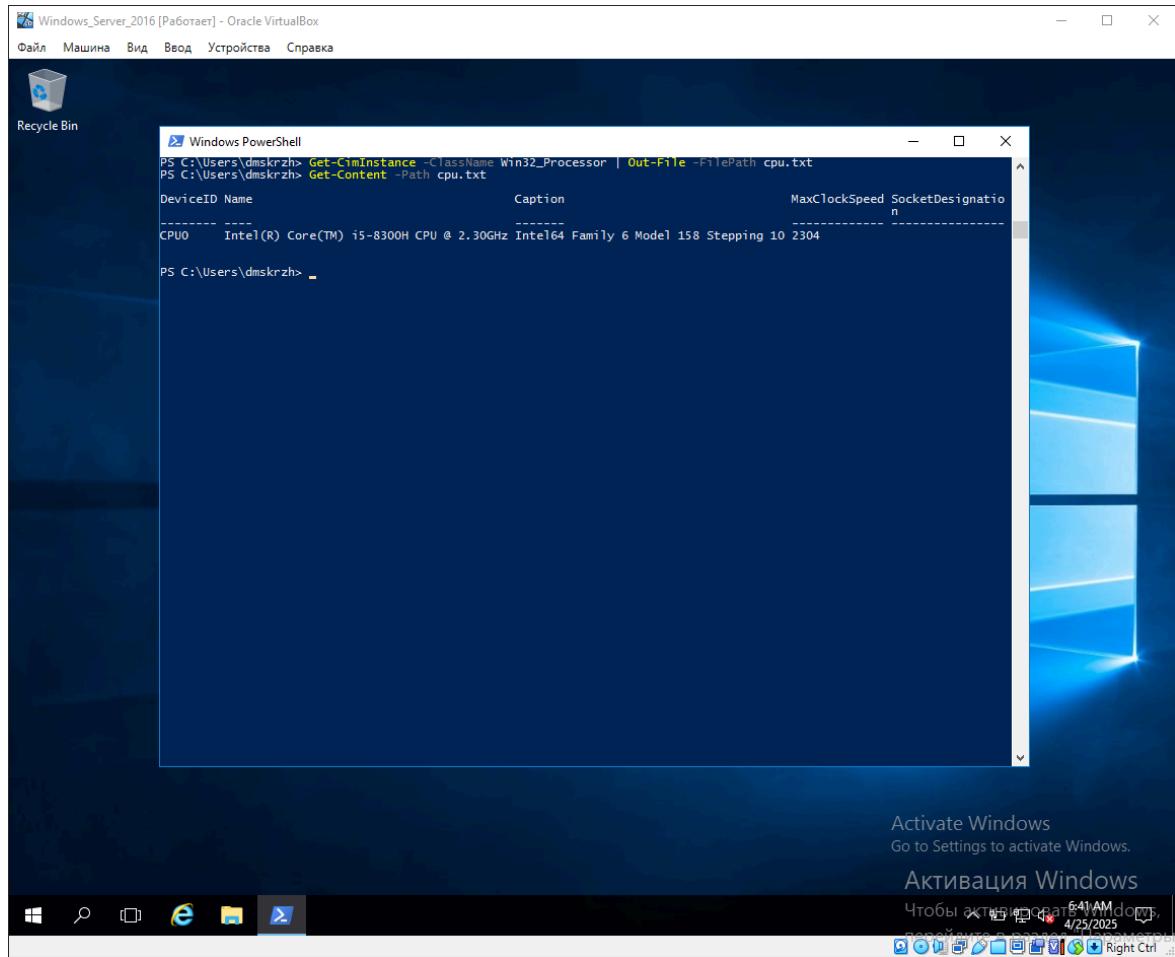


Рисунок 7 - Запись данных о процессоре

6.4 Сохранить информацию о любом процессе в файл <id_процесса>.txt:

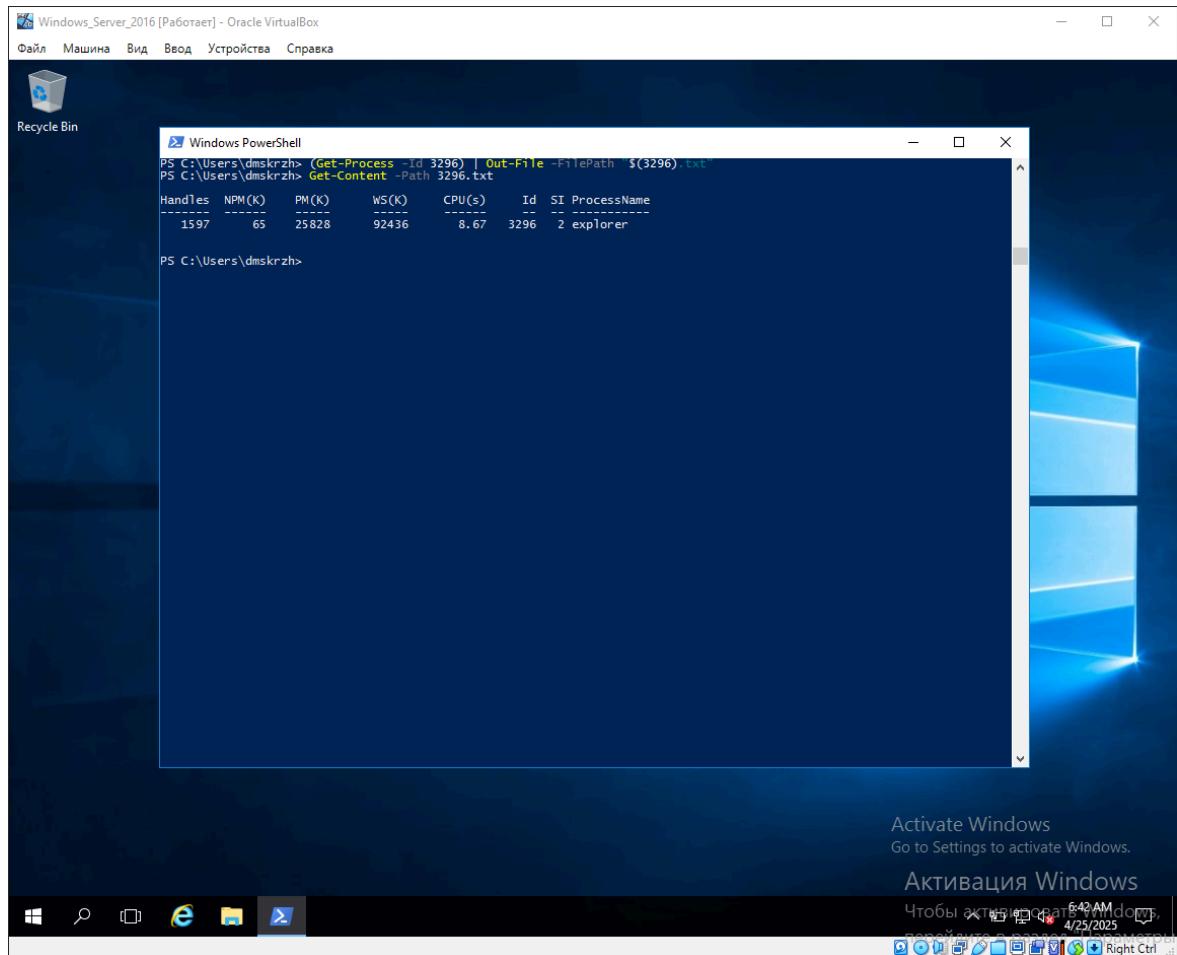
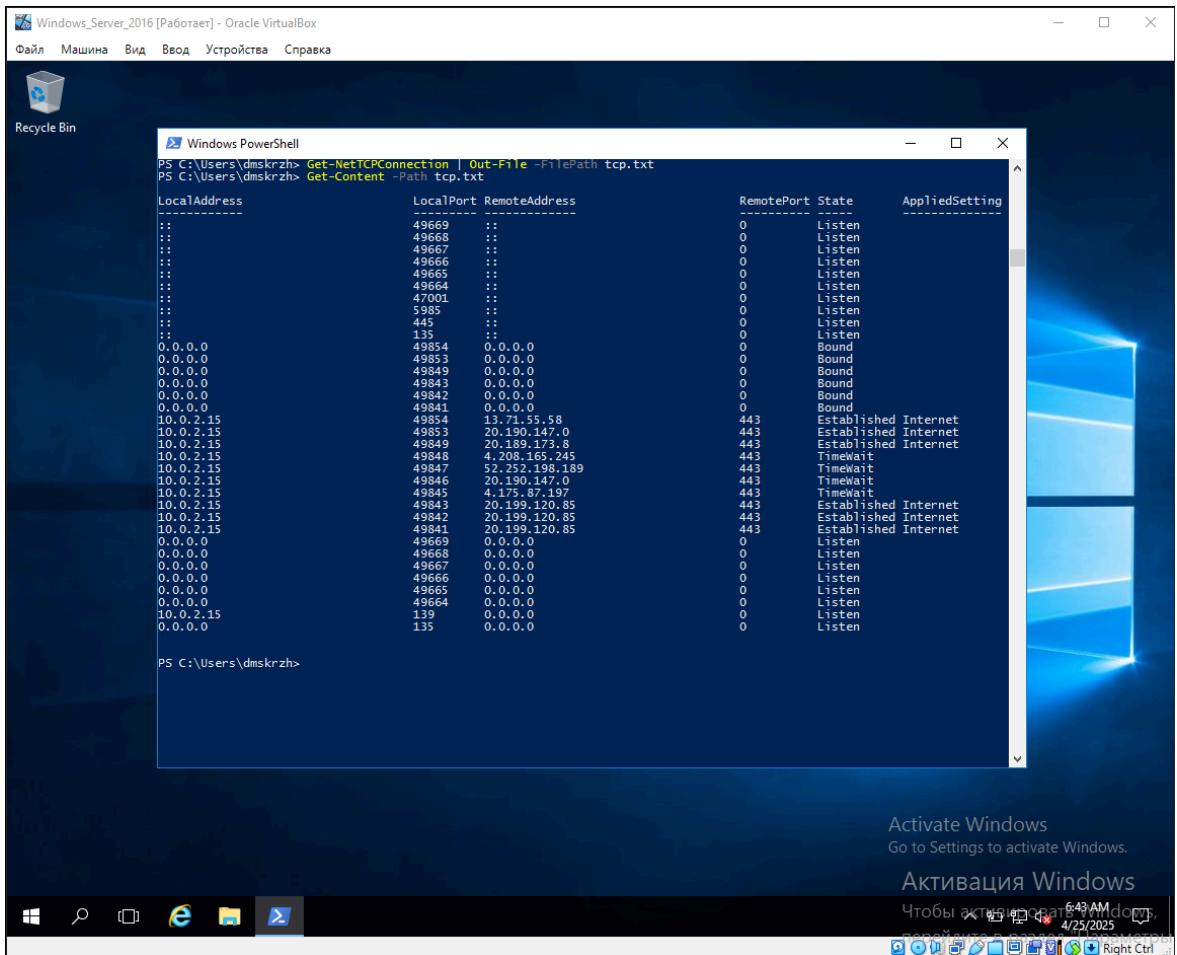


Рисунок 8 - Запись информации о процессе

6.5 Получить список всех TCP портов на машине и сохранить в файл tcp.txt:



```
Windows Server_2016 [Работает] - Oracle VirtualBox
Файл Машина Вид Ввод Устройства Справка
Recycle Bin
Windows PowerShell
PS C:\Users\dmskrzh> Get-NetTCPConnection | Out-File -FilePath tcp.txt
PS C:\Users\dmskrzh> Get-Content -Path tcp.txt
LocalAddress LocalPort RemoteAddress RemotePort State AppliedSetting
----:-----:-----:-----:-----:-----:
::: 49660 :: 0 Listen
::: 49663 :: 0 Listen
::: 49667 :: 0 Listen
::: 49666 :: 0 Listen
::: 49665 :: 0 Listen
::: 49664 :: 0 Listen
::: 47001 :: 0 Listen
::: 5985 :: 0 Listen
::: 443 :: 0 Listen
::: 135 :: 0 Listen
0.0.0.0 49854 0.0.0.0 0 Bound
0.0.0.0 49853 0.0.0.0 0 Bound
0.0.0.0 49849 0.0.0.0 0 Bound
0.0.0.0 49843 0.0.0.0 0 Bound
0.0.0.0 49842 0.0.0.0 0 Bound
0.0.0.0 49840 0.0.0.0 0 Bound
10.0.2.15 49854 13.71.55.58 443 Established Internet
49853 20.190.147.0 443 Established Internet
49849 20.189.173.8 443 Established Internet
10.0.2.15 49848 4.208.165.245 443 TimeWait
10.0.2.15 49847 52.252.198.189 443 TimeWait
10.0.2.15 49846 20.190.147.0 443 TimeWait
10.0.2.15 49845 4.175.87.97 443 TimeWait
10.0.2.15 49843 20.189.120.85 443 Established Internet
49842 20.199.120.85 443 Established Internet
10.0.2.15 49841 20.199.120.85 443 Established Internet
0.0.0.0 49669 0.0.0.0 0 Listen
0.0.0.0 49668 0.0.0.0 0 Listen
0.0.0.0 49667 0.0.0.0 0 Listen
0.0.0.0 49666 0.0.0.0 0 Listen
0.0.0.0 49665 0.0.0.0 0 Listen
0.0.0.0 49664 0.0.0.0 0 Listen
10.0.2.15 135 0.0.0.0 0 Listen
0.0.0.0 135 0.0.0.0 0 Listen
Activate Windows
Go to Settings to activate Windows.
Активация Windows
Чтобы активировать Windows, нажмите Enter или Esc, чтобы отменить. 6:43 AM
4/25/2023 Right Ctrl
```

Рисунок 9 - Запись списка TCP портов

6.6 Получить список всех UDP портов на машине и сохранить в файл udp.txt:

The screenshot shows a Windows Server 2016 desktop environment. A PowerShell window titled "Windows PowerShell" is open, displaying the command output:

```
PS C:\Users\dmskrzh> netstat -a -p udp | Out-File -FilePath udp.txt
PS C:\Users\dmskrzh> Get-Content -Path udp.txt
```

Active Connections

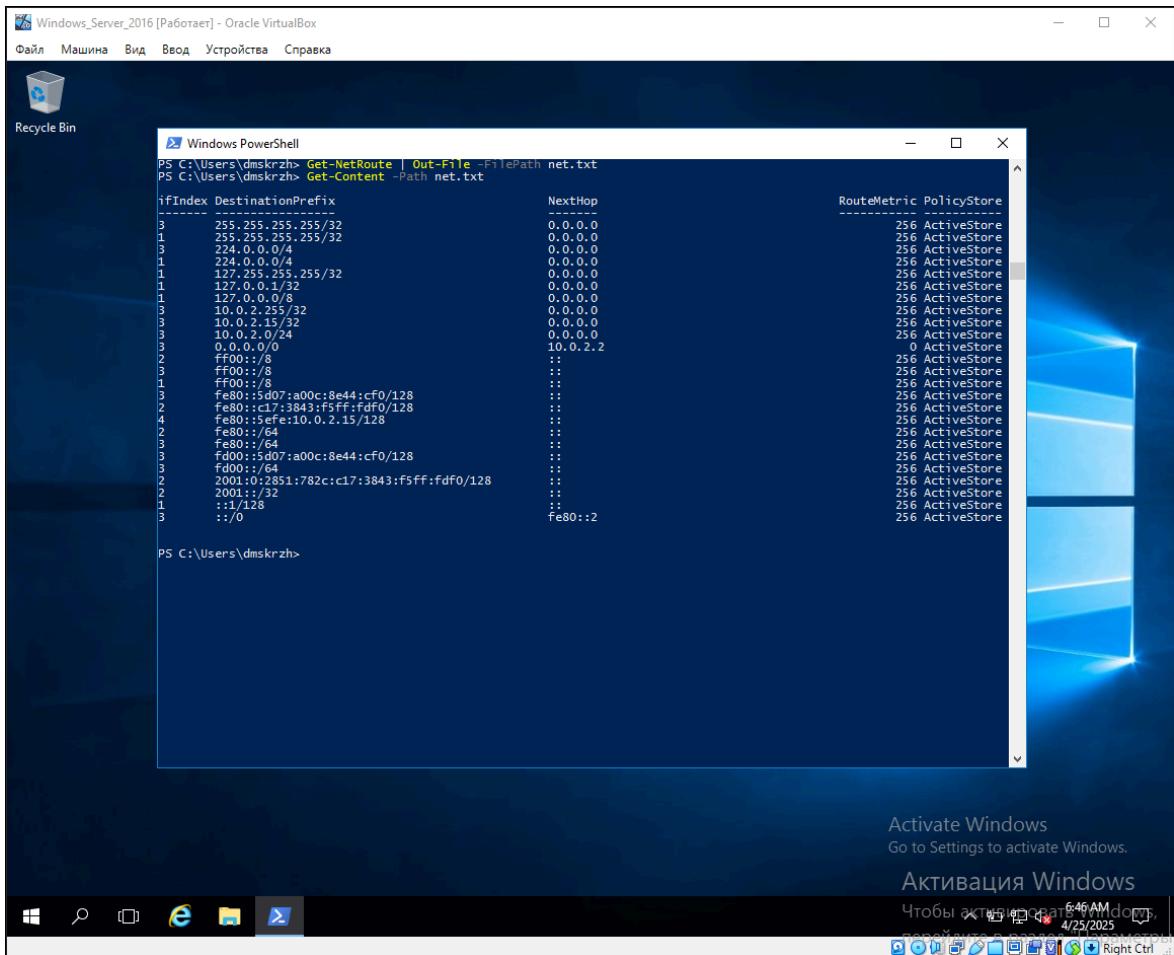
Proto	Local Address	Foreign Address	State
UDP	0.0.0.0:132	*	*
UDP	0.0.0.0:5050	*	*
UDP	0.0.0.0:5353	*	*
UDP	0.0.0.0:5355	*	*
UDP	10.0.2.15:137	*	*
UDP	10.0.2.15:138	*	*
UDP	10.0.2.15:4000	*	*
UDP	10.0.2.15:54725	*	*
UDP	127.0.0.1:1900	*	*
UDP	127.0.0.1:54726	*	*

PS C:\Users\dmskrzh>

The taskbar at the bottom shows several pinned icons, including File Explorer, Task View, and others. A notification for "Activate Windows" is visible, along with a "Активация Windows" (Activation) message and a timestamp of "6:44 AM 4/25/2023".

Рисунок 10 - Запись списка UDP портов

6.7 Получить таблицу маршрутизации на машине и сохранить в файл net.txt:



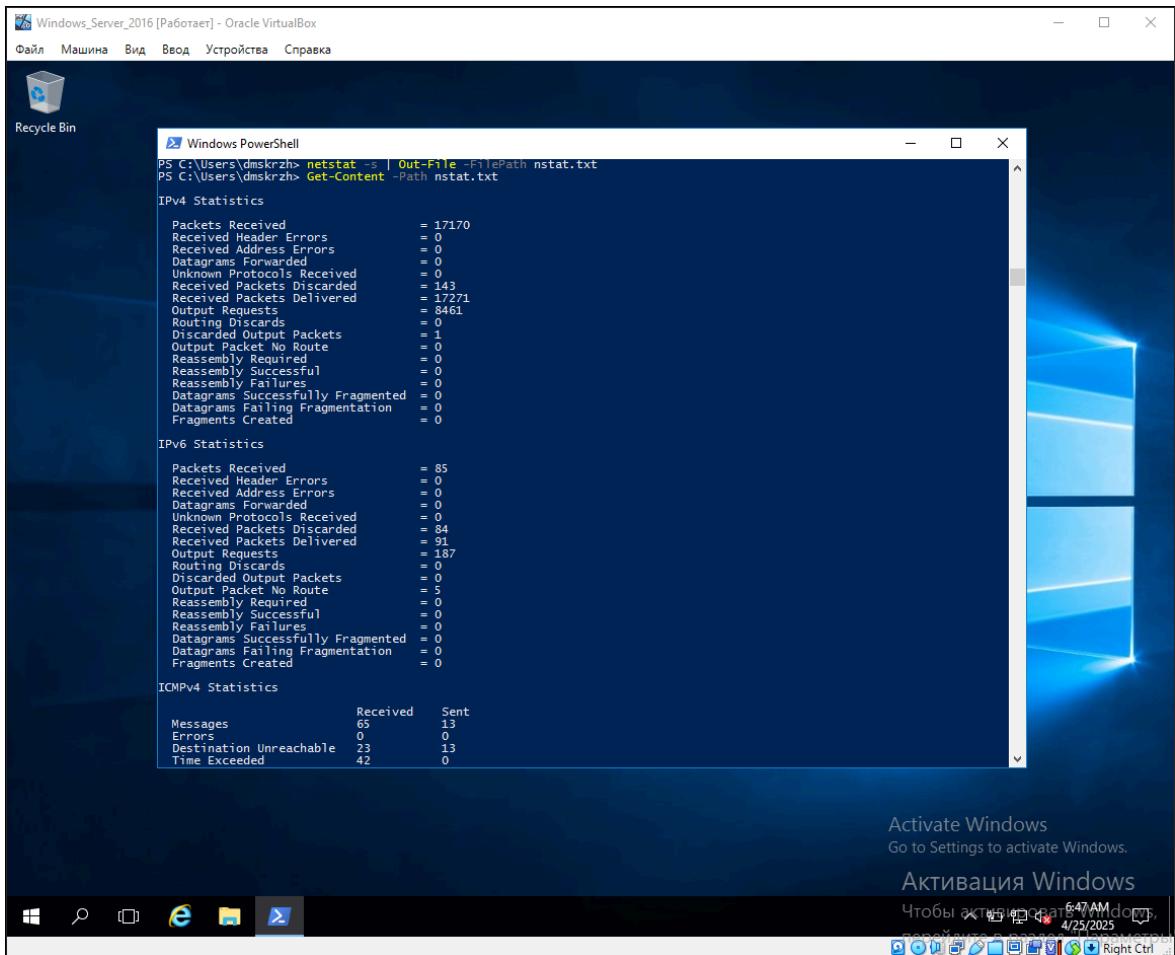
The screenshot shows a Windows Server 2016 desktop environment. A PowerShell window titled "Windows PowerShell" is open, displaying the output of the command "Get-NetRoute | Out-File -FilePath net.txt" followed by "Get-Content -Path net.txt". The output lists a routing table with columns: ifIndex, DestinationPrefix, NextHop, RouteMetric, and PolicyStore. The table includes entries for various network interfaces (e.g., 255.255.255.255/32, 127.0.0.1/32) and IPv6 link-local addresses. The PowerShell window is located in the center of the screen, with the taskbar visible at the bottom.

ifIndex	DestinationPrefix	NextHop	RouteMetric	PolicyStore
3	255.255.255.255/32	0.0.0.0	256	ActiveStore
1	255.255.255.255/32	0.0.0.0	256	ActiveStore
3	224.0.0.0/4	0.0.0.0	256	ActiveStore
1	224.0.0.0/4	0.0.0.0	256	ActiveStore
1	127.255.255.255/32	0.0.0.0	256	ActiveStore
1	127.0.0.1/32	0.0.0.0	256	ActiveStore
1	127.0.0.0/8	0.0.0.0	256	ActiveStore
3	10.0.2.255/32	0.0.0.0	256	ActiveStore
3	10.0.2.0/32	0.0.0.0	256	ActiveStore
3	10.0.2.0/24	0.0.0.0	256	ActiveStore
3	0.0.0.0/0	10.0.2.2	0	ActiveStore
2	ff00::/8	:	256	ActiveStore
3	ff00::/8	:	256	ActiveStore
1	fe80::5d07:a00c:8e44:cff0/128	:	256	ActiveStore
2	fe80::c1f3:843:f5ff:fdff/128	:	256	ActiveStore
4	fe80::10.0.2.15/128	:	256	ActiveStore
2	fe80::/64	:	256	ActiveStore
3	fe80::/64	:	256	ActiveStore
3	fd00::5d07:a00c:8e44:cff0/128	:	256	ActiveStore
3	fd00::/64	:	256	ActiveStore
2	2001:0:2851:782c:c17:3843:f5ff:fdff/128	:	256	ActiveStore
2	2001::/32	:	256	ActiveStore
1	::1/128	:	256	ActiveStore
3	::/0	fe80::2	256	ActiveStore

PS C:\Users\dmskrzh>

Рисунок 11 - Запись таблицы маршрутизации

6.8 Получить статистику для каждого протокола на машине и сохранить в файл nstat.txt:



The screenshot shows a Windows Server 2016 desktop environment within Oracle VirtualBox. A PowerShell window titled 'Windows PowerShell' is open, displaying network statistics. The command run was `netstat -s | Out-File -FilePath nstat.txt`. The output includes detailed statistics for IPv4, IPv6, and ICMPv4 protocols.

```
PS C:\Users\dmskrzh> netstat -s | Out-File -FilePath nstat.txt
PS C:\Users\dmskrzh> Get-Content -Path nstat.txt

IPv4 Statistics
    Packets Received          = 17170
    Received Header Errors    = 0
    Received Address Errors   = 0
    Datagram Forwarded       = 0
    Unknown Protocols Received = 0
    Received Packets Discarded = 143
    Received Packets Delivered = 17271
    Output Requests           = 8461
    Routing Discards          = 0
    Discarded Output Packets  = 1
    Output Packet No Route    = 0
    Reassembly Required       = 0
    Reassembly Successful     = 0
    Reassembly Failures      = 0
    Datagrams Successfully Fragmented = 0
    Datagrams Failing Fragmentation = 0
    Fragments Created         = 0

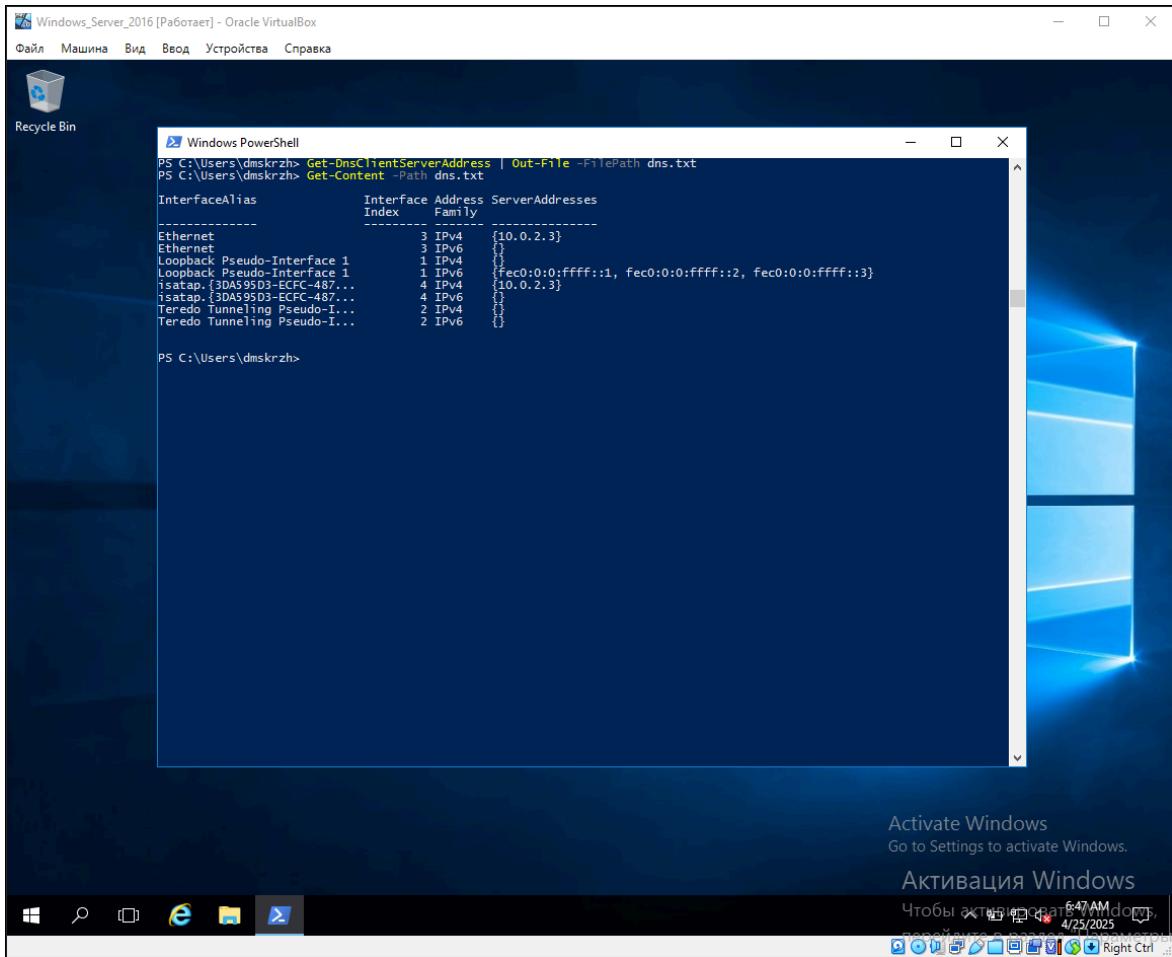
IPv6 Statistics
    Packets Received          = 85
    Received Header Errors    = 0
    Received Address Errors   = 0
    Datagram Forwarded       = 0
    Unknown Protocols Received = 0
    Received Packets Discarded = 84
    Received Packets Delivered = 91
    Output Requests           = 187
    Routing Discards          = 0
    Discarded Output Packets  = 0
    Output Packet No Route    = 0
    Reassembly Required       = 0
    Reassembly Successful     = 0
    Reassembly Failures      = 0
    Datagrams Successfully Fragmented = 0
    Datagrams Failing Fragmentation = 0
    Fragments Created         = 0

ICMPv4 Statistics
    Received      Sent
    Messages      65      13
    Errors        0       0
    Destination Unreachable 23      13
    Time Exceeded 42      0
```

The desktop background is blue, and the taskbar at the bottom shows standard icons like Start, Search, Task View, Edge browser, File Explorer, and Task Manager. A watermark for 'Activate Windows' is visible in the center of the screen.

Рисунок 12 - Запись статистики каждого протокола на машине

6.9 Получить список DNS и сохранить в файл dns.txt:



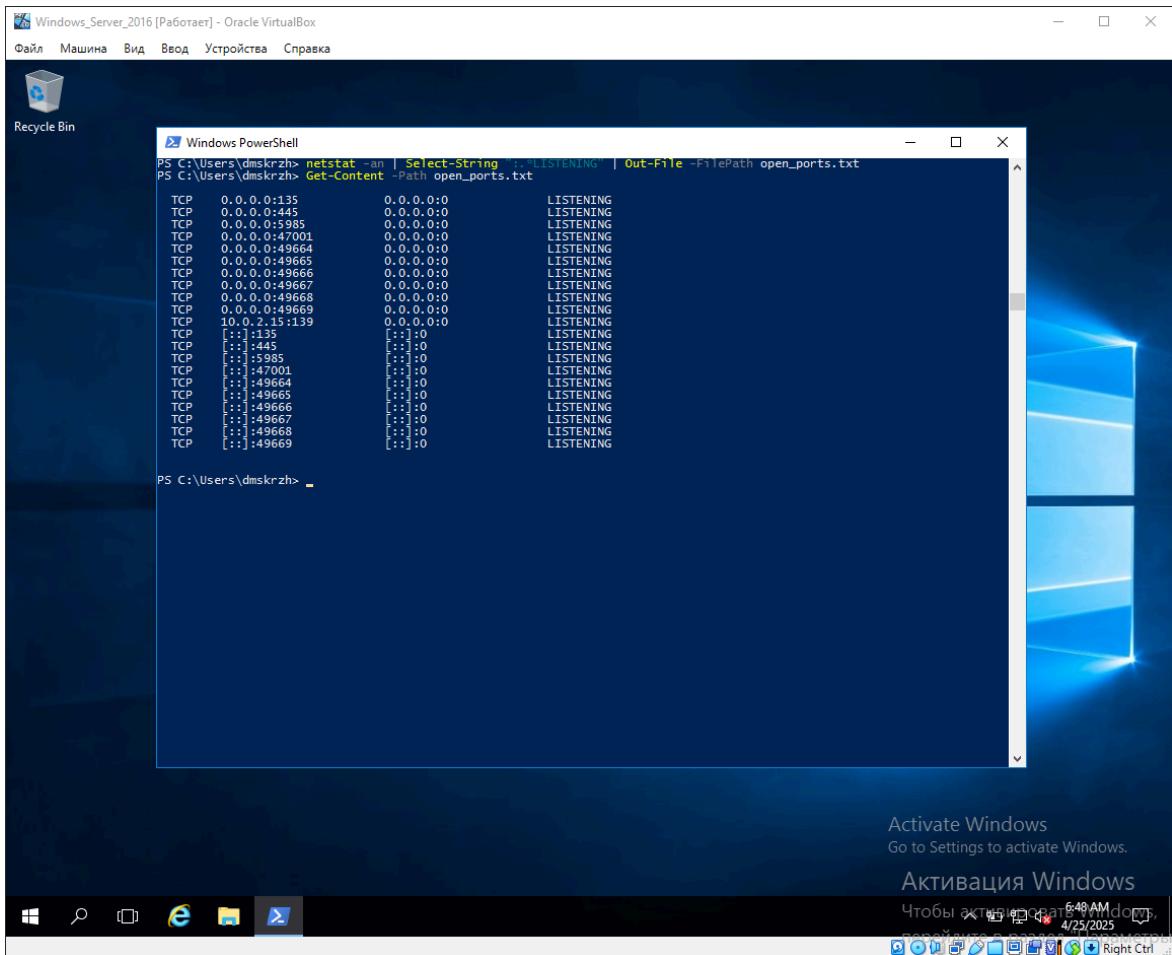
```
Windows PowerShell
PS C:\Users\dmskrzh> Get-DnsClientServerAddress | Out-File -FilePath dns.txt
PS C:\Users\dmskrzh> Get-Content -Path dns.txt
InterfaceAlias      Interface Index Address Family ServerAddresses
-----            -----   -----
Ethernet           IPv4       3 {10.0.2.3}
Ethernet           IPv6       3 {}
Loopback Pseudo-Interface 1 IPv4       1 {}
Loopback Pseudo-Interface 1 IPv6       1 {fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3}
isatap.{3DA595D3-ECFC-487... IPv4       4 {10.0.2.3}
isatap.{3DA595D3-ECFC-487... IPv6       4 {}
Teredo Tunneling Pseudo-Interface 1 IPv4       2 {}
Teredo Tunneling Pseudo-Interface 1 IPv6       2 {}

PS C:\Users\dmskrzh>
```

The screenshot shows a Windows Server 2016 desktop environment with a blue theme. A Windows PowerShell window is open in the foreground, displaying a command to export DNS client server addresses to a file named 'dns.txt'. The command is: `Get-DnsClientServerAddress | Out-File -FilePath dns.txt`. Below this, the contents of the 'dns.txt' file are shown, listing various network interfaces and their corresponding IP addresses and families. The desktop background features the classic Windows 10 Start screen. A watermark for 'Activate Windows' is visible in the center of the screen.

Рисунок 13 - Запись списка DNS

6.10 Получить список всех открытых портов и сохранить в файл open_ports.txt



The screenshot shows a Windows Server 2016 desktop environment. A PowerShell window titled "Windows PowerShell" is open, displaying the command and its output:

```
PS C:\Users\dmskrzh> netstat -an | Select-String ":LISTENING" | Out-File -FilePath open_ports.txt
PS C:\Users\dmskrzh> Get-Content -Path open_ports.txt
```

Сокет	Локальный порт	Состояние
TCP	0.0.0.0:135	LISTENING
TCP	0.0.0.0:445	LISTENING
TCP	0.0.0.0:5985	LISTENING
TCP	0.0.0.0:47001	LISTENING
TCP	0.0.0.0:49664	LISTENING
TCP	0.0.0.0:49665	LISTENING
TCP	0.0.0.0:49666	LISTENING
TCP	0.0.0.0:49667	LISTENING
TCP	0.0.0.0:49668	LISTENING
TCP	0.0.0.0:49669	LISTENING
TCP	[::]:135	LISTENING
TCP	[::]:445	LISTENING
TCP	[::]:5985	LISTENING
TCP	[::]:47001	LISTENING
TCP	[::]:49664	LISTENING
TCP	[::]:49665	LISTENING
TCP	[::]:49666	LISTENING
TCP	[::]:49667	LISTENING
TCP	[::]:49668	LISTENING
TCP	[::]:49669	LISTENING

Below the PowerShell window, a message from the operating system says "Activate Windows Go to Settings to activate Windows." and "Активация Windows". The taskbar at the bottom shows various icons including File Explorer, Task View, and Start.

Рисунок 14 - Запись списка всех открытых портов

7. Управление процессами и службами:

7.1 Используя команды для получения информации о процессе в ОС получите список процессов, использующие более 2% CPU.

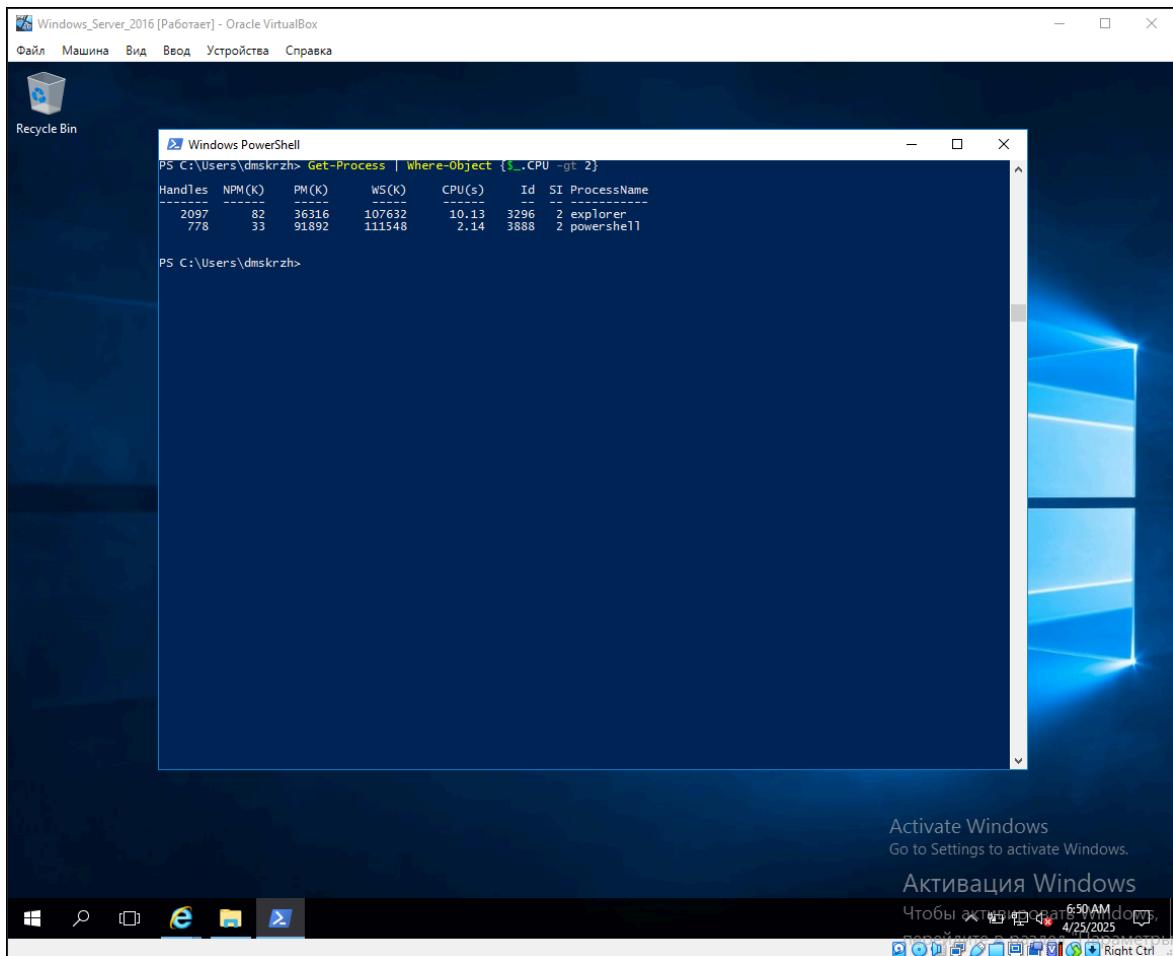
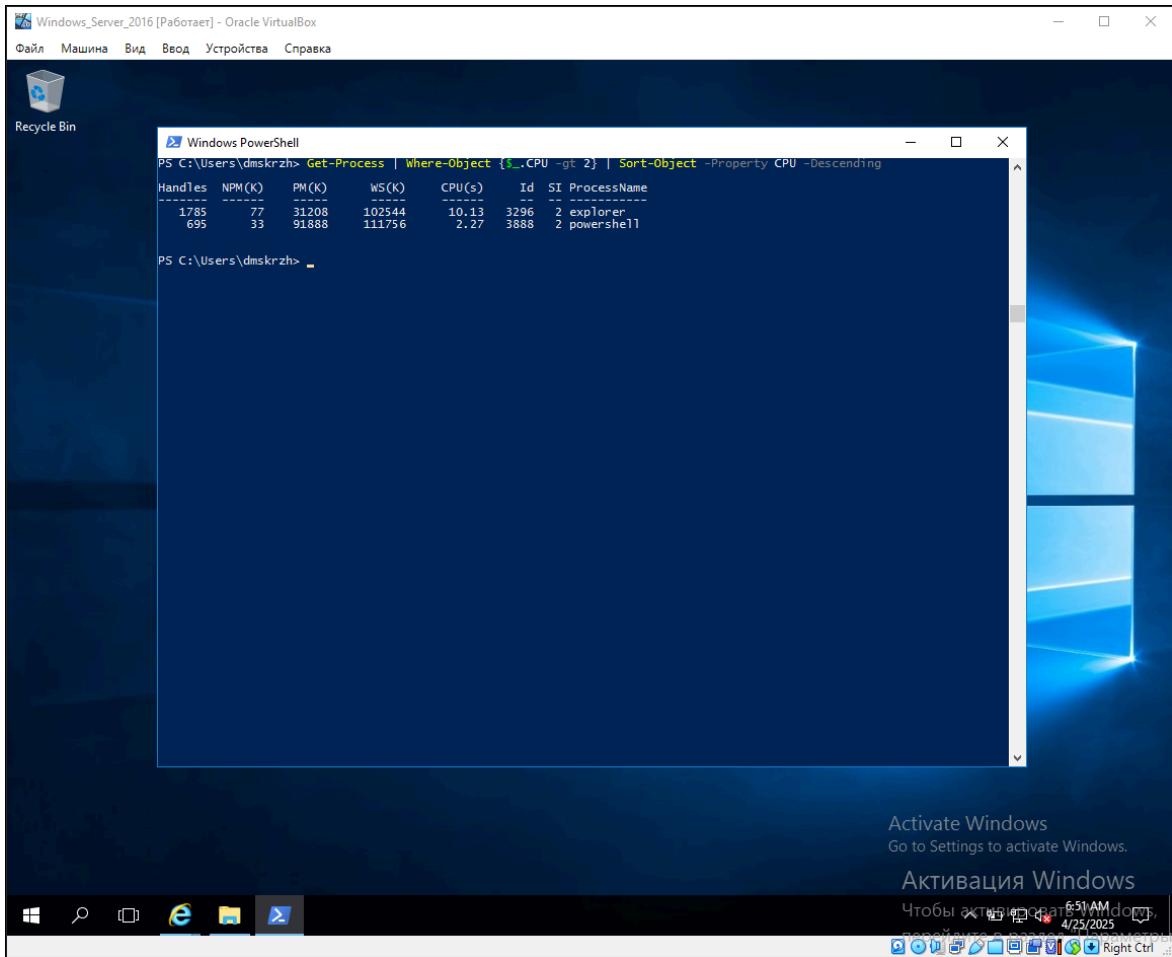


Рисунок 15 - Вывод процессов с загрузкой более 2%

7.2 Отсортируйте список в порядке убывания



The screenshot shows a Windows Server 2016 desktop environment within Oracle VirtualBox. A PowerShell window is open, displaying a command to sort processes by CPU usage in descending order. The command is:

```
PS C:\Users\dmskrzh> Get-Process | Where-Object {$_.CPU -gt 2} | Sort-Object -Property CPU -Descending
```

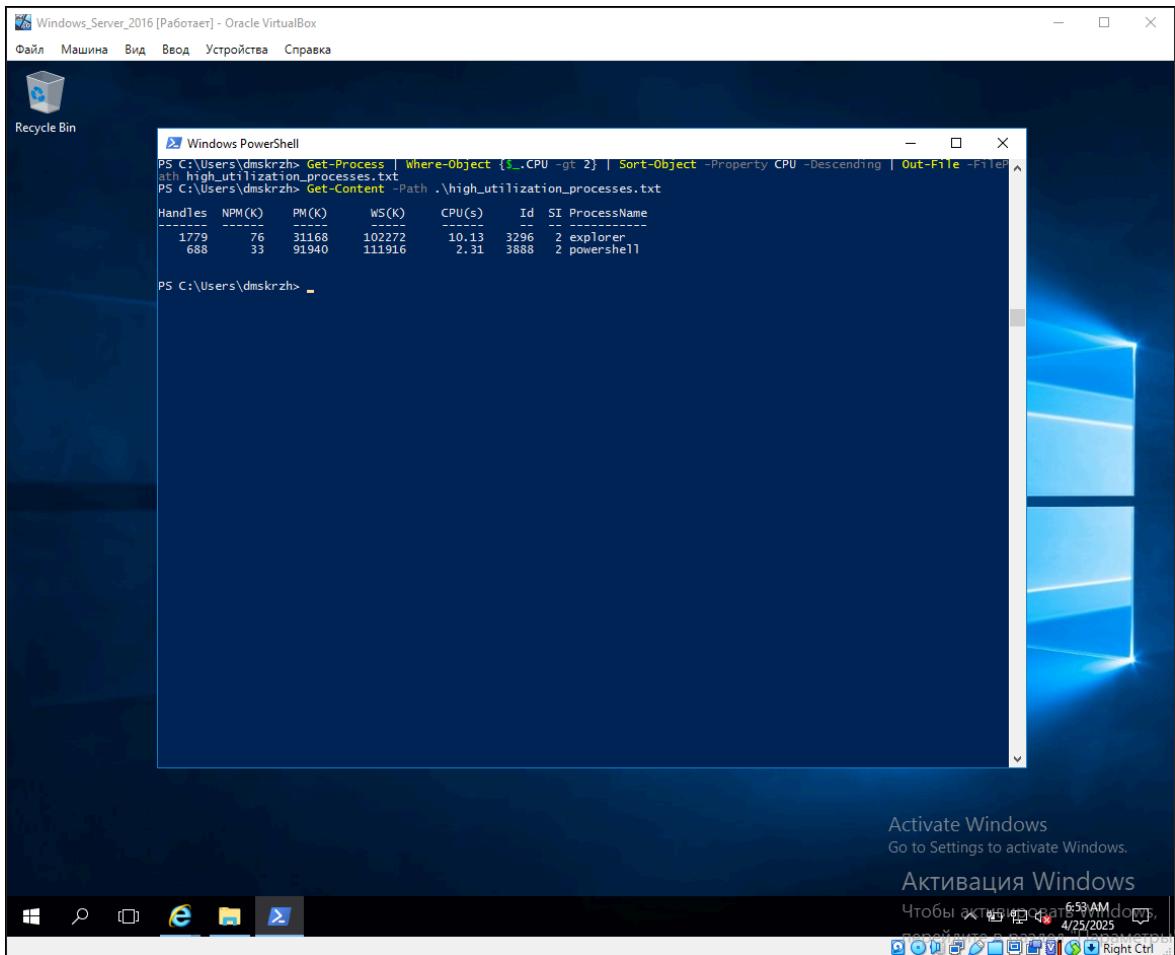
The resulting table shows the following data:

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
1785	77	31208	102544	10.13	3296	2	explorer
695	33	91888	111756	2.27	3888	2	powershell1

The taskbar at the bottom includes icons for Start, Search, Task View, Edge browser, File Explorer, and File Explorer (with a red notification badge).

Рисунок 16 - Сортировка по убыванию

7.3 Запишите информацию о процессах в файл **high_utilization_processes.txt**.



The screenshot shows a Windows Server 2016 desktop environment within Oracle VirtualBox. A PowerShell window titled "Windows PowerShell" is open, displaying the following command and its output:

```
PS C:\Users\dmskrzh> Get-Process | Where-Object {$_CPU -gt 2} | Sort-Object -Property CPU -Descending | Out-File -FilePath .\high_utilization_processes.txt
PS C:\Users\dmskrzh> Get-Content -Path .\high_utilization_processes.txt
```

The output table shows the following data:

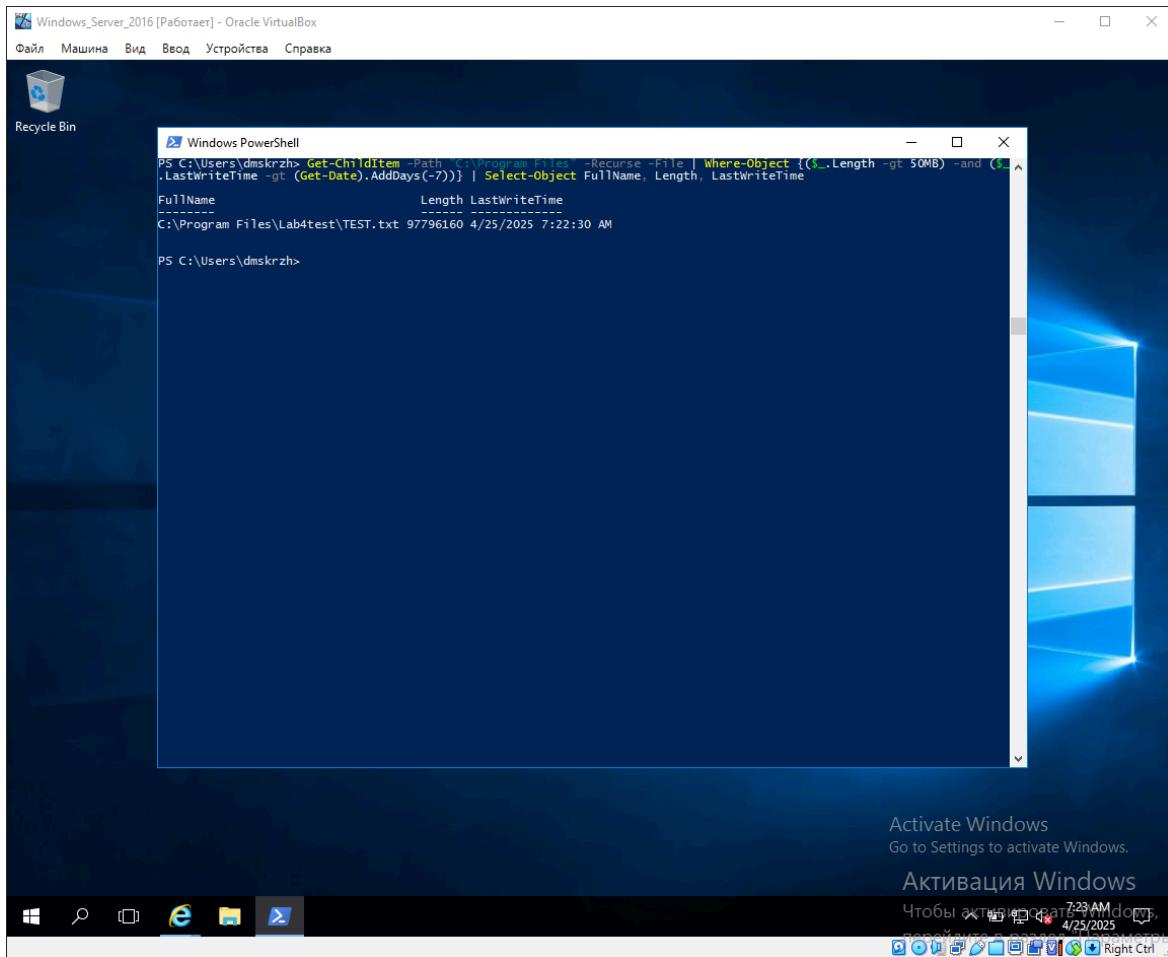
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
1779	76	31168	102272	10.13	3296	2	explorer
688	33	91940	111916	2.31	3688	2	powershell

The desktop background is dark blue, and the taskbar at the bottom includes icons for Start, Search, Task View, Edge browser, File Explorer, and Task Manager. A watermark for "Activate Windows" and "Активация Windows" is visible in the center of the screen.

Рисунок 17 - Запись в файл

8. Поиск файлов по размеру и дате изменения:

8.1 Используйте необходимые командлеты, чтобы найти все файлы в каталоге C:\Program Files, размер которых превышает 50МВ (значение может быть скорректировано, если поиск не даст результата) и которые были изменены за последние 7 дней.



The screenshot shows a Windows Server 2016 desktop environment. A PowerShell window is open, displaying the following command and its output:

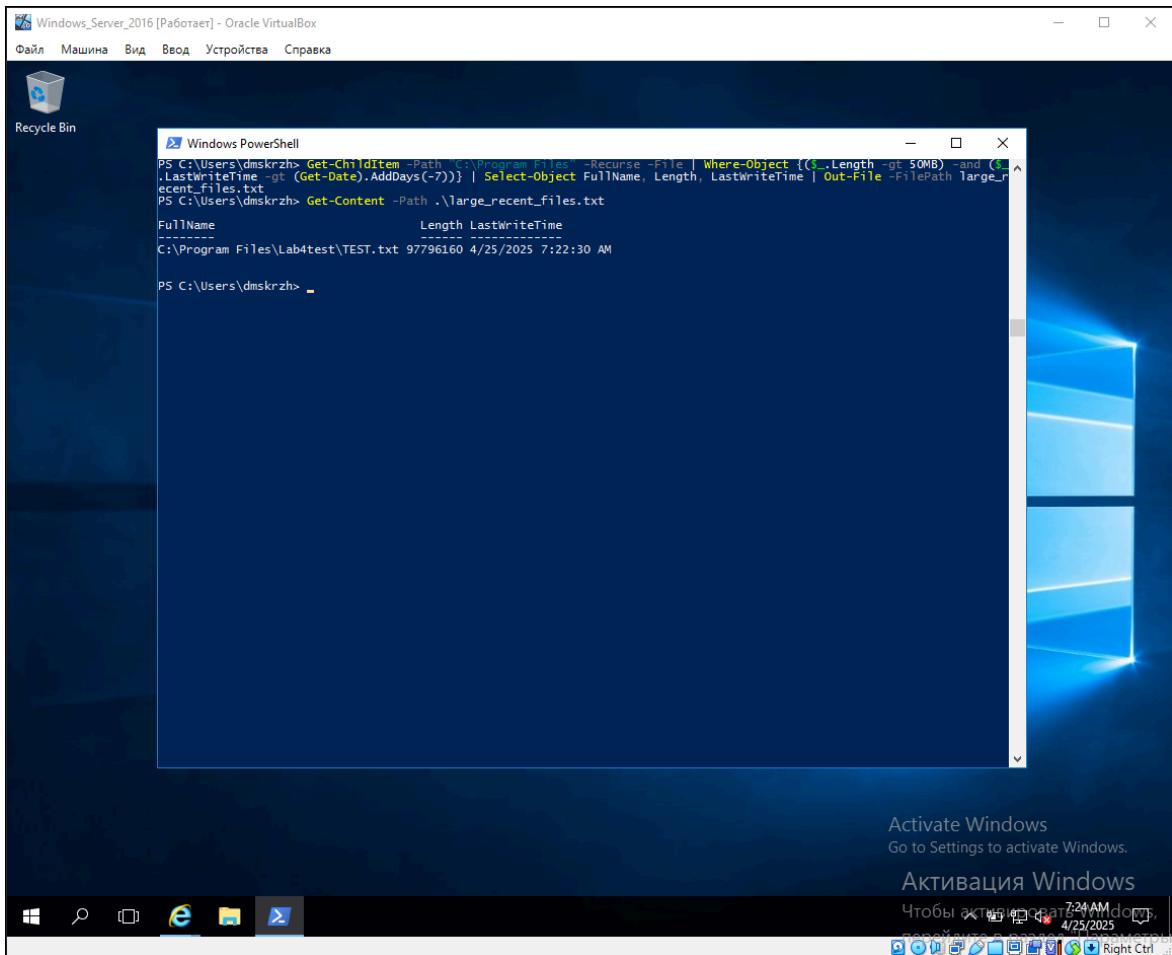
```
PS C:\Users\dmskrzh> Get-ChildItem -Path "C:\Program Files" -Recurse -File | Where-Object {($_.Length -gt 50MB) -and ($_.LastWriteTime -gt (Get-Date).AddDays(-7))} | Select-Object FullName, Length, LastWriteTime
```

FullName	Length	LastWriteTime
C:\Program Files\Lab4test\TEST.txt	97796160	4/25/2025 7:22:30 AM

The desktop background is dark blue, and the taskbar at the bottom shows standard icons like Start, Search, Task View, Internet Explorer, File Explorer, and PowerShell.

Рисунок 18 - Список файлов

8.2 Запишите список найденных файлов в файл **large_recent_files.txt**.



The screenshot shows a Windows Server 2016 desktop environment. A PowerShell window titled "Windows PowerShell" is open, displaying the following command and its output:

```
PS C:\Users\dmskrzh> Get-ChildItem -Path 'C:\Program Files' -Recurse -File | Where-Object {($_.Length -gt 50MB) -and ($_.LastWriteTime -gt (Get-Date).AddDays(-7))} | Select-Object FullName, Length, LastWriteTime | Out-File -FilePath large_recent_files.txt
PS C:\Users\dmskrzh> Get-Content -Path .\large_recent_files.txt
FullName                           Length LastWriteTime
Labeled...
C:\Program Files\Lab4test\TEST.txt 97796160 4/25/2025 7:22:30 AM
PS C:\Users\dmskrzh>
```

The output shows a single file entry: "C:\Program Files\Lab4test\TEST.txt" with a length of 97796160 bytes and a last write time of 4/25/2025 7:22:30 AM.

The desktop background is blue, and the taskbar at the bottom includes icons for File Explorer, Task View, Edge browser, and File Explorer again. A system tray icon for "Windows Update" is visible, along with the date and time (4/25/2025 7:24 AM).

Рисунок 19 - Запись списка

9. Поиск файлов с определенным содержимым:

9.1 Используйте командлет Get-ChildItem, чтобы найти все файлы в указанном вами каталоге, содержащие слово "error".

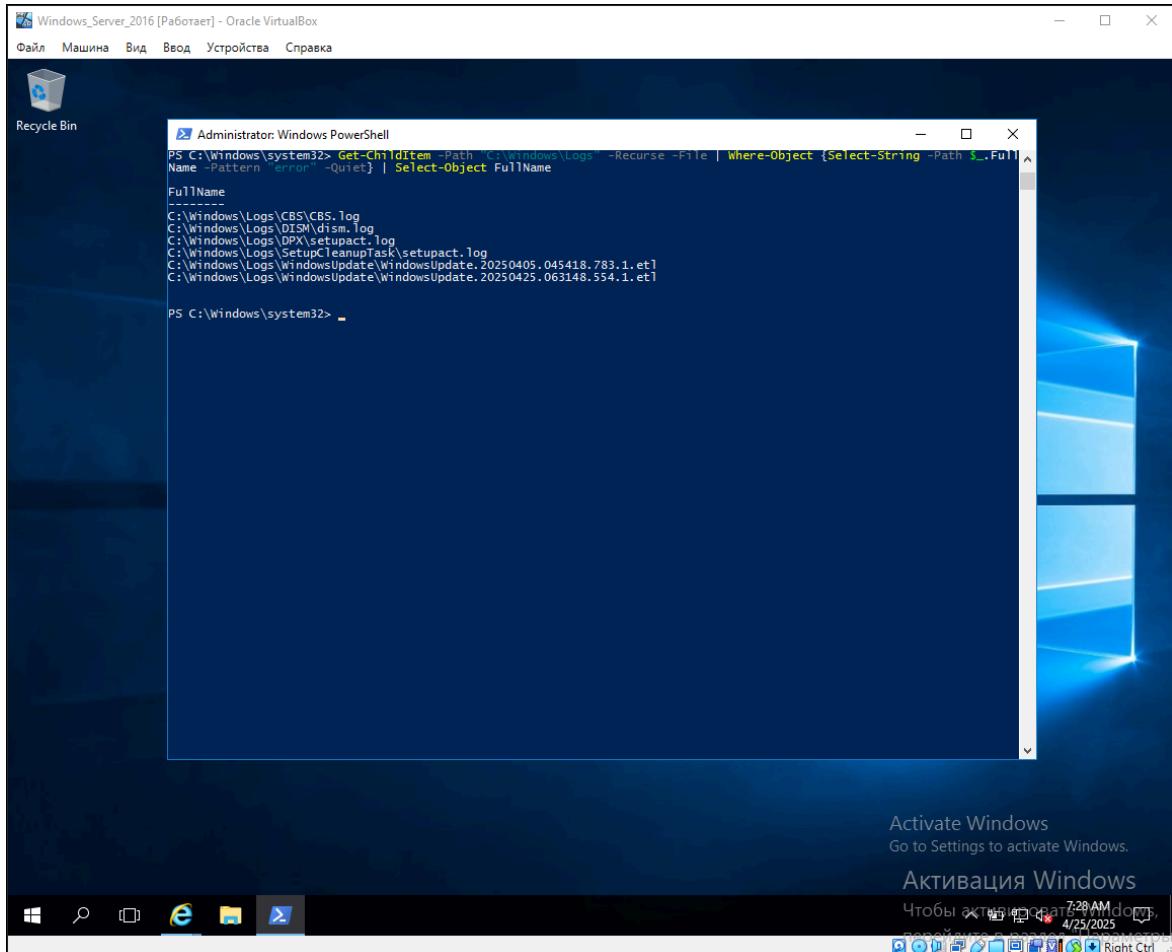
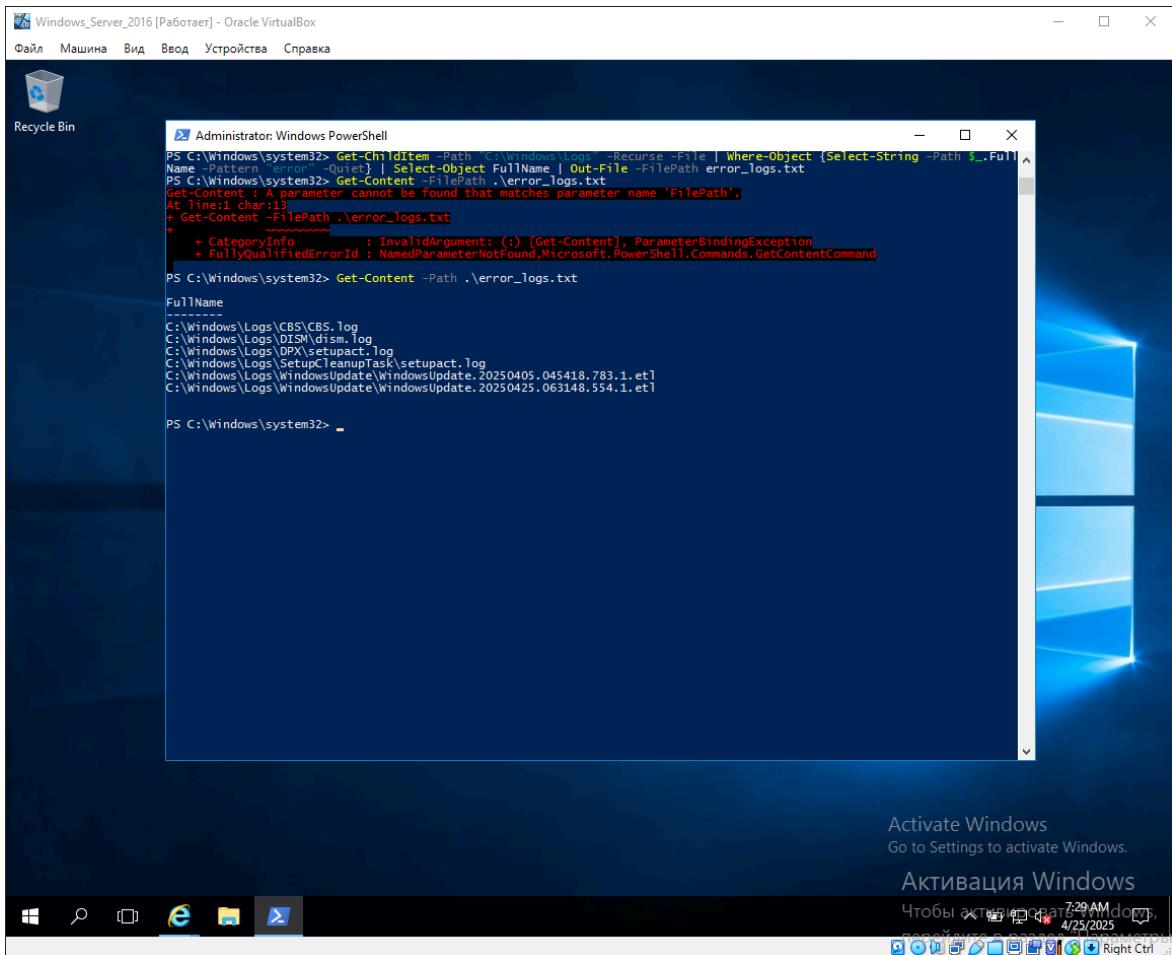


Рисунок 20 - Список файлов

9.2 Запишите список найденных файлов и строки, содержащие "error", в файл error_logs.txt.



The screenshot shows a Windows Server 2016 desktop environment. A PowerShell window titled 'Administrator: Windows PowerShell' is open, displaying the following command and its output:

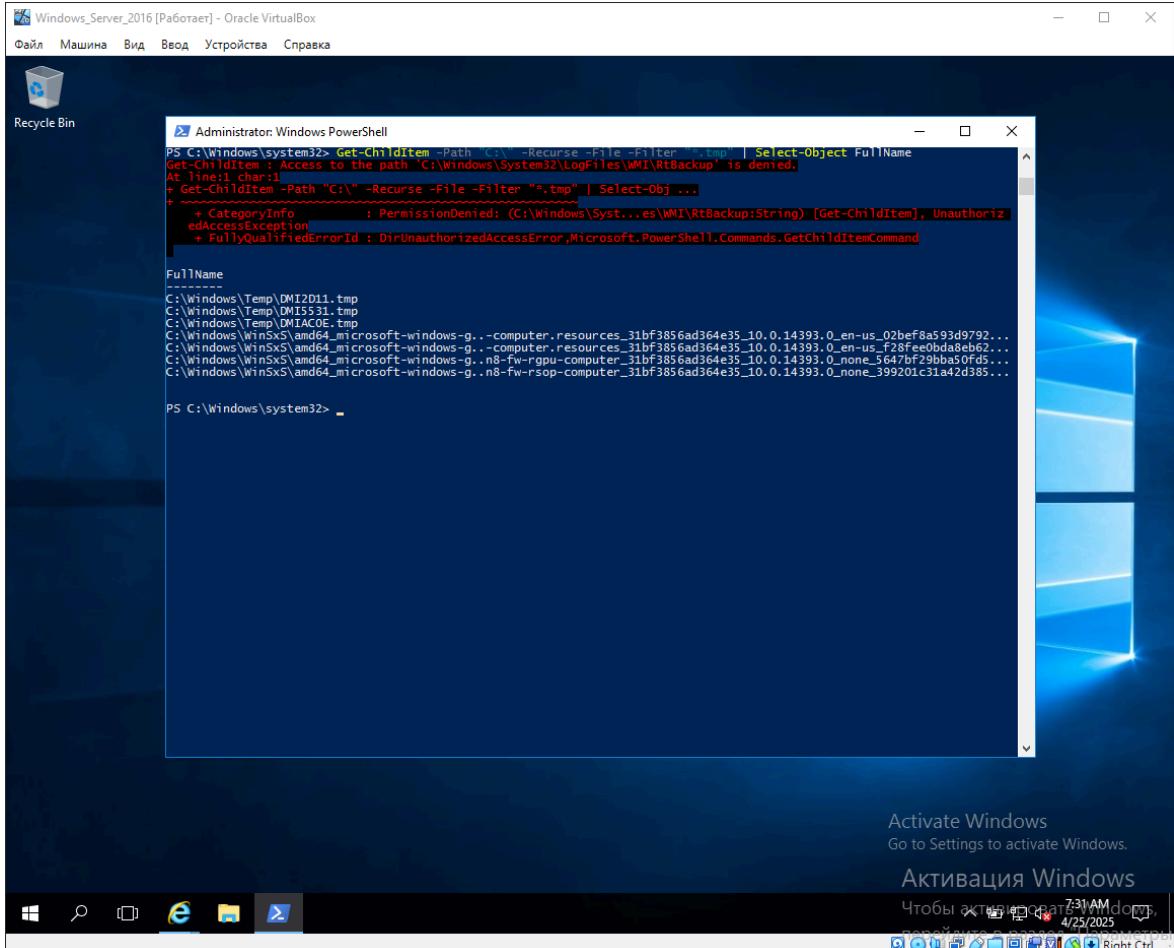
```
PS C:\Windows\system32> Get-ChildItem -Path "C:\Windows\Logs" -Recurse -File | Where-Object {Select-String -Path $_.FullName -Name 'error' -Count 1} | Select-Object FullName -Out-File -FilePath error_logs.txt
PS C:\Windows\system32> Get-Content -FilePath .\error_logs.txt
Get-Content : A parameter cannot be found that matches parameter name 'FilePath'.
At line:1 char:3
+ Get-Content -FilePath .\error_logs.txt
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Get-Content], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.GetContentCommand
PS C:\Windows\system32> Get-Content -Path .\error_logs.txt
FullName
-----
C:\Windows\Logs\CMS\CMS.log
C:\Windows\Logs\DISM\dism.log
C:\Windows\Logs\Install\install.log
C:\Windows\Logs\Setup\temp\Task\setupact.log
C:\Windows\Logs\WindowsUpdate\WindowsUpdate_20250405.04518.783.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate_20250425.063148.554.1.etl
```

The taskbar at the bottom shows several pinned icons, including File Explorer, Task View, and others. A notification bar at the bottom right indicates 'Activate Windows' and 'Активация Windows'.

Рисунок 21 - Запись списка

10. Поиск и удаление временных файлов:

10.1 Выполните поиск файлов с расширением .tmp на указанном вами диске с последующим их удалением



The screenshot shows a Windows Server 2016 desktop environment. In the center is an 'Administrator: Windows PowerShell' window. The command entered is:

```
PS C:\Windows\system32> Get-ChildItem -Path 'C:\' -Recurse -File -Filter *.tmp | Select-Object FullName
```

The output shows a list of file paths under the 'FullName' header:

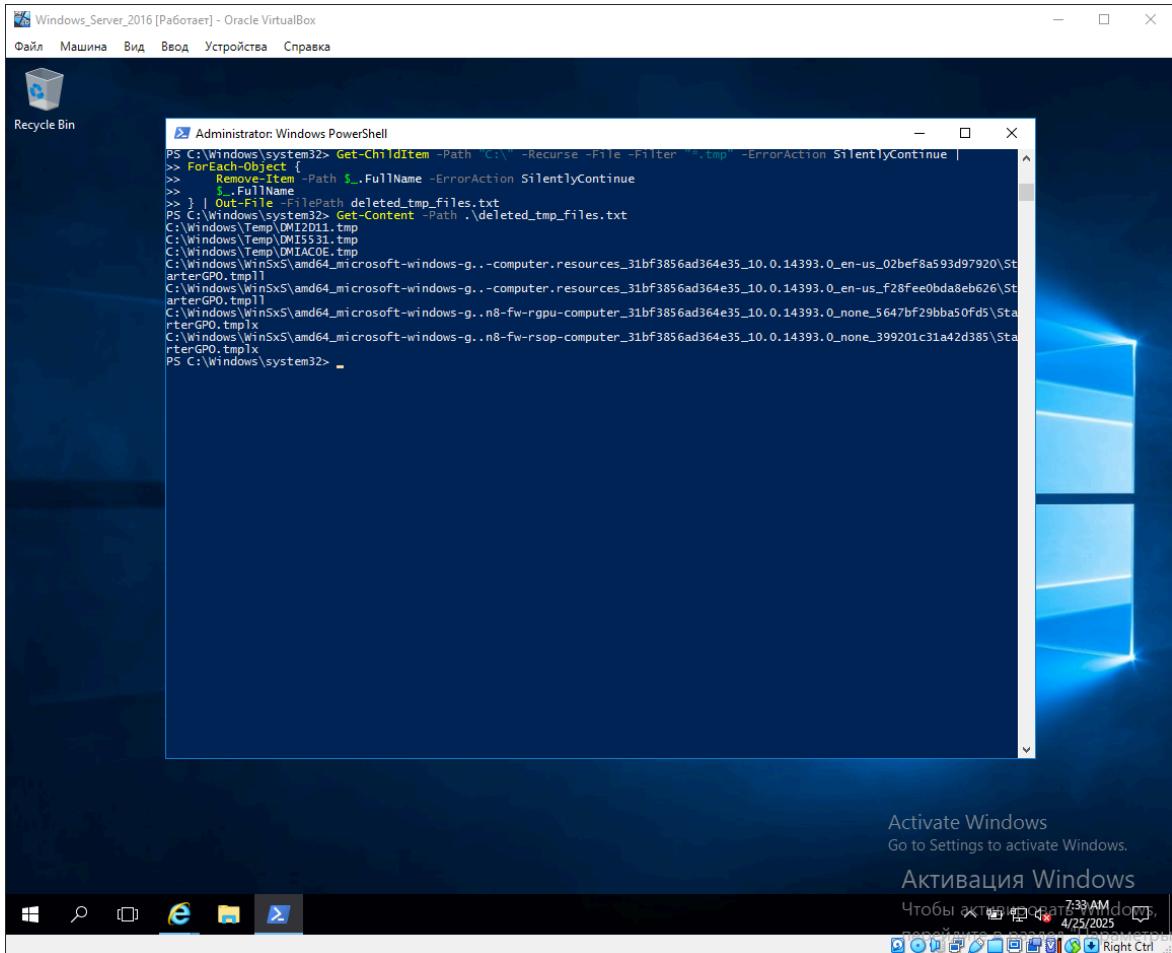
FullName
C:\Windows\Temp\DMI2D11.tmp
C:\Windows\Temp\DMIS531.tmp
C:\Windows\Temp\DMIACOE.tmp
C:\Windows\WinSxS\amd64_microsoft-windows-g...-computer.resources_31bf3856ad364e35_10.0.14393.0_en-us_02bef8a593d9792...
C:\Windows\WinSxS\amd64_microsoft-windows-g...-computer.resources_31bf3856ad364e35_10.0.14393.0_en-us_f28fee0bda8eb62...
C:\Windows\WinSxS\amd64_microsoft-windows-g...n8-fw-rgpu-computer_31bf3856ad364e35_10.0.14393.0_none_5647bf29bba50fd5...
C:\Windows\WinSxS\amd64_microsoft-windows-g...n8-fw-rsop-computer_31bf3856ad364e35_10.0.14393.0_none_399201c31a42d385...

At the bottom of the PowerShell window, the prompt is PS C:\Windows\system32>.

Below the desktop window, there is a taskbar with icons for Start, Search, Task View, Internet Explorer, File Explorer, and Task Manager. A system tray icon for Right Ctrl is also visible. On the right side of the screen, there is a 'Activate Windows' message and a 'Активация Windows' (Activation Windows) status bar.

Рисунок 22 - Список файлов .tmp

10.2 Запишите список удаленных файлов в файл deleted_tmp_files.txt.

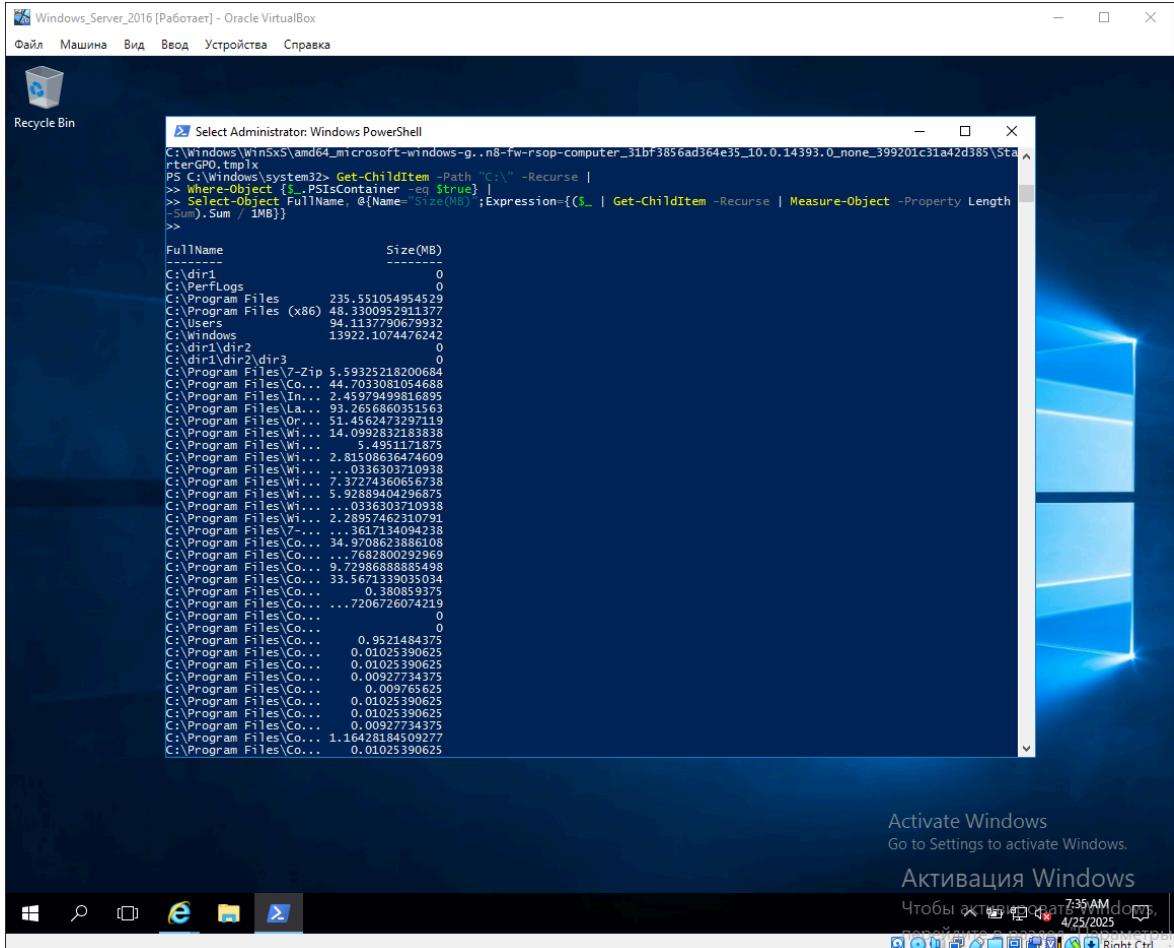


```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-ChildItem -Path "C:\\" -Recurse -File -Filter "*.tmp" -ErrorAction SilentlyContinue | >> ForEach-Object {>> Remove-Item -Path $_.FullName -ErrorAction SilentlyContinue >> $_.FullName } | Out-File -FilePath deleted_tmp_files.txt
PS C:\Windows\system32> Get-Content -Path .\deleted_tmp_files.txt
C:\Windows\Temp\DM1ZD11.tmp
C:\Windows\Temp\DM15531.tmp
C:\Windows\Temp\DMIACEO.tmp
C:\Windows\WinSxS\amd64_microsoft-windows-g...-computer.resources_31bf3856ad364e35_10.0.14393.0_en-us_02bef8a593d97920\StarterGPO.tmp11
C:\Windows\WinSxS\amd64_microsoft-windows-g...-computer.resources_31bf3856ad364e35_10.0.14393.0_en-us_f28fee0bda8eb626\StarterGPO.tmp11
C:\Windows\WinSxS\amd64_microsoft-windows-g...n8-fw-rgpu-computer_31bf3856ad364e35_10.0.14393.0_none_5647bf29bba50fd5\StarterGPO.tmp1x
C:\Windows\WinSxS\amd64_microsoft-windows-g...n8-fw-rsop-computer_31bf3856ad364e35_10.0.14393.0_none_399201c31a42d385\StarterGPO.tmp1x
PS C:\Windows\system32> -
```

Рисунок 23 - Запись списка удалённых файлов

11. Анализ использования дискового пространства:

11.1 Получите информацию о размере всех файлов и папок в выбранном вами диске



The screenshot shows a Windows Server 2016 desktop environment within Oracle VirtualBox. A PowerShell window titled 'Select Administrator Windows PowerShell' is open, displaying a table of disk usage statistics. The table has two columns: 'FullName' and 'Size(MB)'. The data shows various folders and their sizes, such as C:\Windows (13922 MB), C:\Program Files (x86) (48,330 MB), and numerous smaller system and application folders. The PowerShell command used to generate this output is partially visible at the top of the window.

FullName	Size(MB)
C:\dir1	0
C:\Windows\Logs	0
C:\Program Files	235,551 MB
C:\Program Files (x86)	48,330 MB
C:\Users	94,113 MB
C:\Windows	13922,107 MB
C:\dir1\dir2	0
C:\dir1\dir2\dir3	0
C:\Program Files\7-Zip	5,392 MB
C:\Program Files\Co...	44,703 MB
C:\Program Files\In...	2,459 MB
C:\Program Files\La...	93,265 MB
C:\Program Files\Or...	51,456 MB
C:\Program Files\Wi...	14,099 MB
C:\Program Files\Wi...	5,495 MB
C:\Program Files\Wi...	2,815 MB
C:\Program Files\Wi...	7,136 MB
C:\Program Files\Wi...	7,136 MB
C:\Program Files\Wi...	5,928 MB
C:\Program Files\Wi...	0,0336 MB
C:\Program Files\Wi...	2,2895 MB
C:\Program Files\Wi...	361,713 MB
C:\Program Files\Co...	34,970 MB
C:\Program Files\Co...	3,768 MB
C:\Program Files\Co...	3,728 MB
C:\Program Files\Co...	33,562 MB
C:\Program Files\Co...	0,380 MB
C:\Program Files\Co...	...7206726074219
C:\Program Files\Co...	0
C:\Program Files\Co...	0
C:\Program Files\Co...	0,05214 MB
C:\Program Files\Co...	0,0102539 MB
C:\Program Files\Co...	0,0102539 MB
C:\Program Files\Co...	0,000927734 MB
C:\Program Files\Co...	0,0009765 MB
C:\Program Files\Co...	0,0102539 MB
C:\Program Files\Co...	0,0102539 MB
C:\Program Files\Co...	0,00927734 MB
C:\Program Files\Co...	1,164281845 MB
C:\Program Files\Co...	0,0102539 MB

Activate Windows
Go to Settings to activate Windows.

Активация Windows
Чтобы активировать Windows, нажмите на ссылку в правом верхнем углу.

7:35 AM
4/25/2025
Right Ctrl

Рисунок 24 - Информация о размере файлов и папок

11.2 Отфильтруйте вывод, оставив только информацию о файлах, размер которых больше 100МВ.

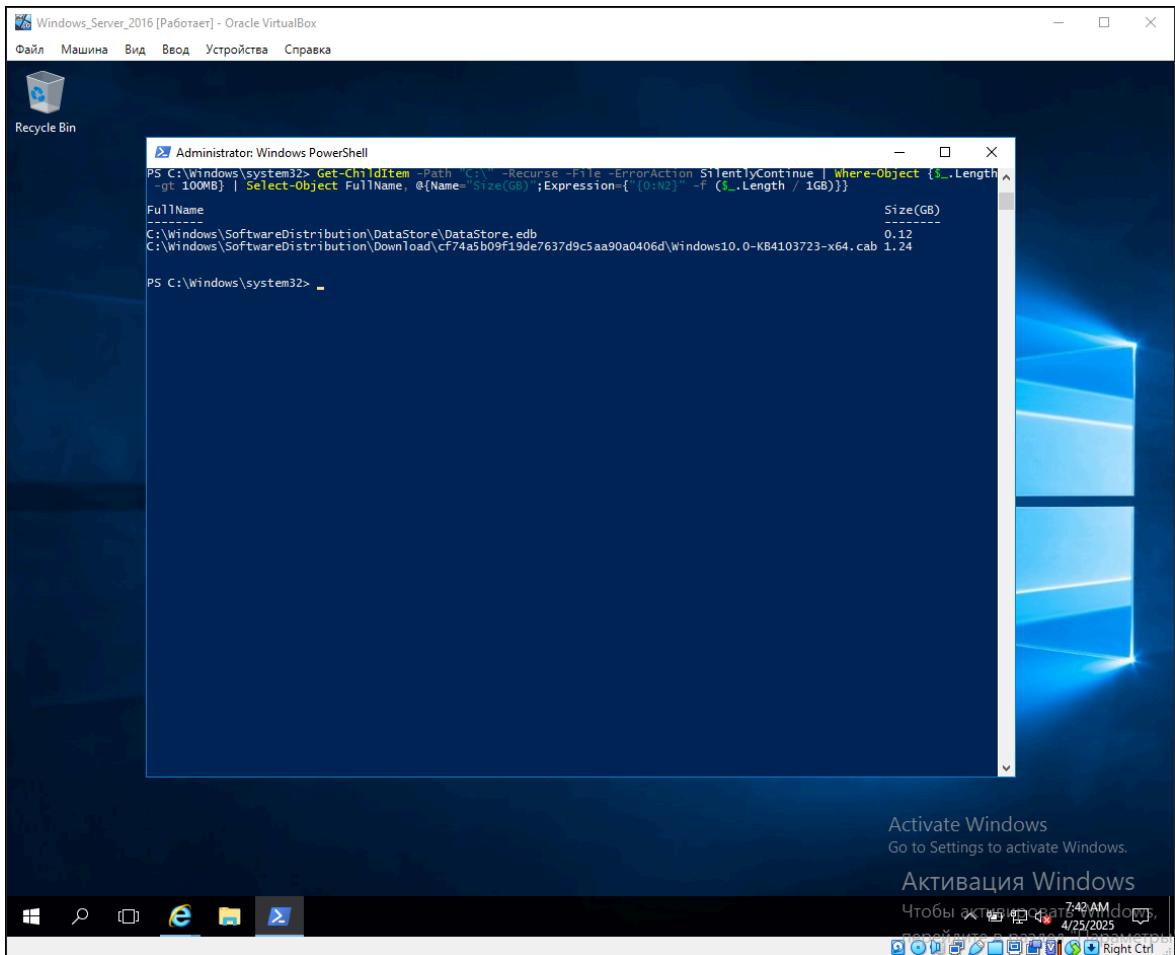


Рисунок 25 - Файлы размером больше 100 Мб

11.3 Отсортируйте вывод по размеру и запишите результат в файл large_var_files.txt.

The screenshot shows a Windows Server 2016 desktop environment. A PowerShell window titled "Administrator: Windows PowerShell" is open, displaying the following command and its output:

```
PS C:\Windows\system32> Get-ChildItem -Path 'C:\*' -Recurse -File -ErrorAction SilentlyContinue | >> Where-Object {$_..Length -gt 100MB} | >> Sort-Object FullName -Descending | >> Select-Object FullName, @{'Name='Size(GB)' ; Expression={ [0:N2] -f ($_.Length / 1GB)}} | >> Out-File $filepath Target=large_var_files.txt  
PS C:\Windows\system32> Get-Content -Path ..\large_var_files.txt
```

FullName	Size(GB)
C:\Windows\SoftwareDistribution\Download\cf74a5b09f19de7637d9c5aa90a0406d\windows10.0-K84103723-x64.cab	1.24
C:\Windows\SoftwareDistribution\DataStore.edb	0.12

The desktop background is the standard Windows 10 blue gradient. A "Recycle Bin" icon is visible on the desktop. The taskbar at the bottom shows several pinned icons, including File Explorer, Task View, and Start. A notification bar at the bottom right indicates "Activate Windows Go to Settings to activate Windows." and "Активация Windows". It also shows the date and time as "Чтобы активировать Windows 7:44 AM 4/25/2025" and includes a "Right Ctrl" key indicator.

Рисунок 26 - Запись в файл

12. Создание отчета о дисковом пространстве:

12.1 Получите информацию о всех дисках с помощью Get-PSDrive.

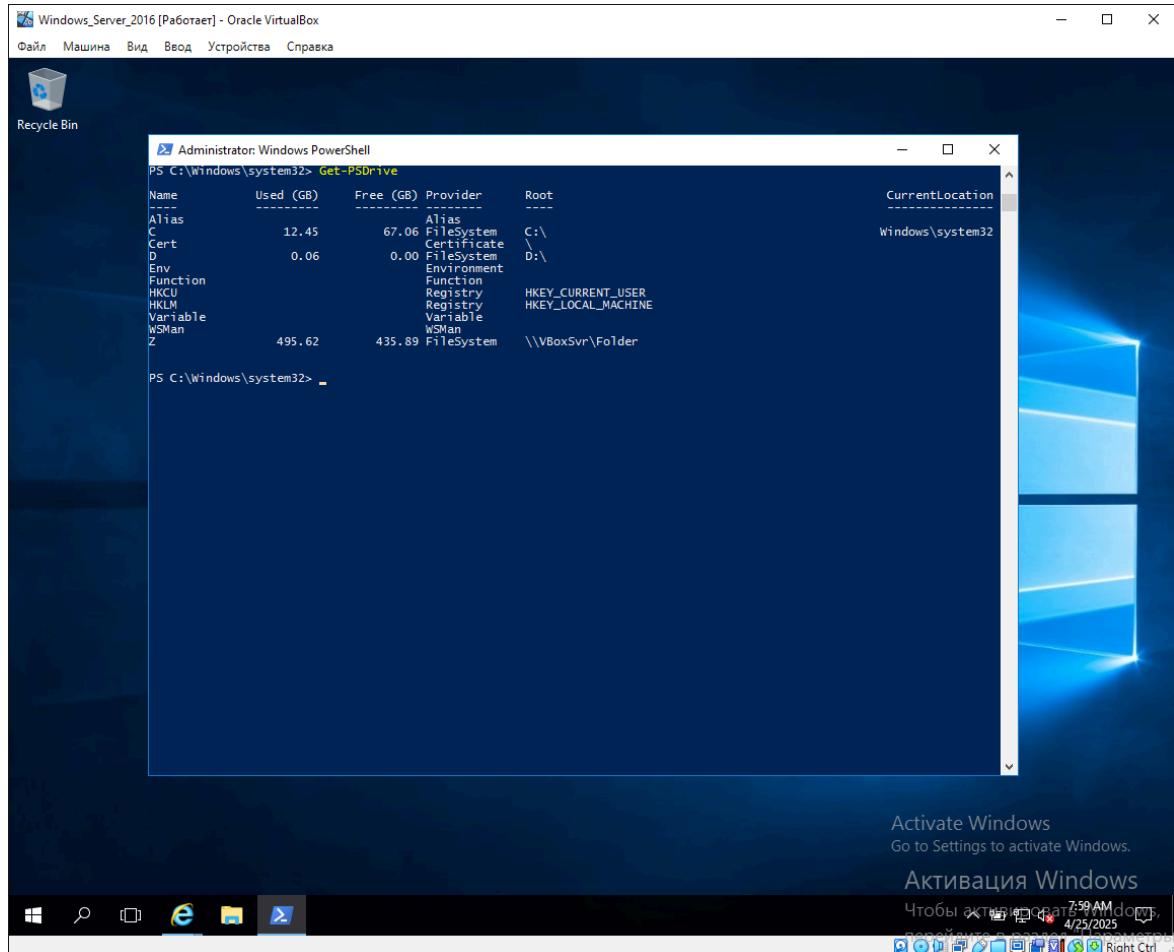
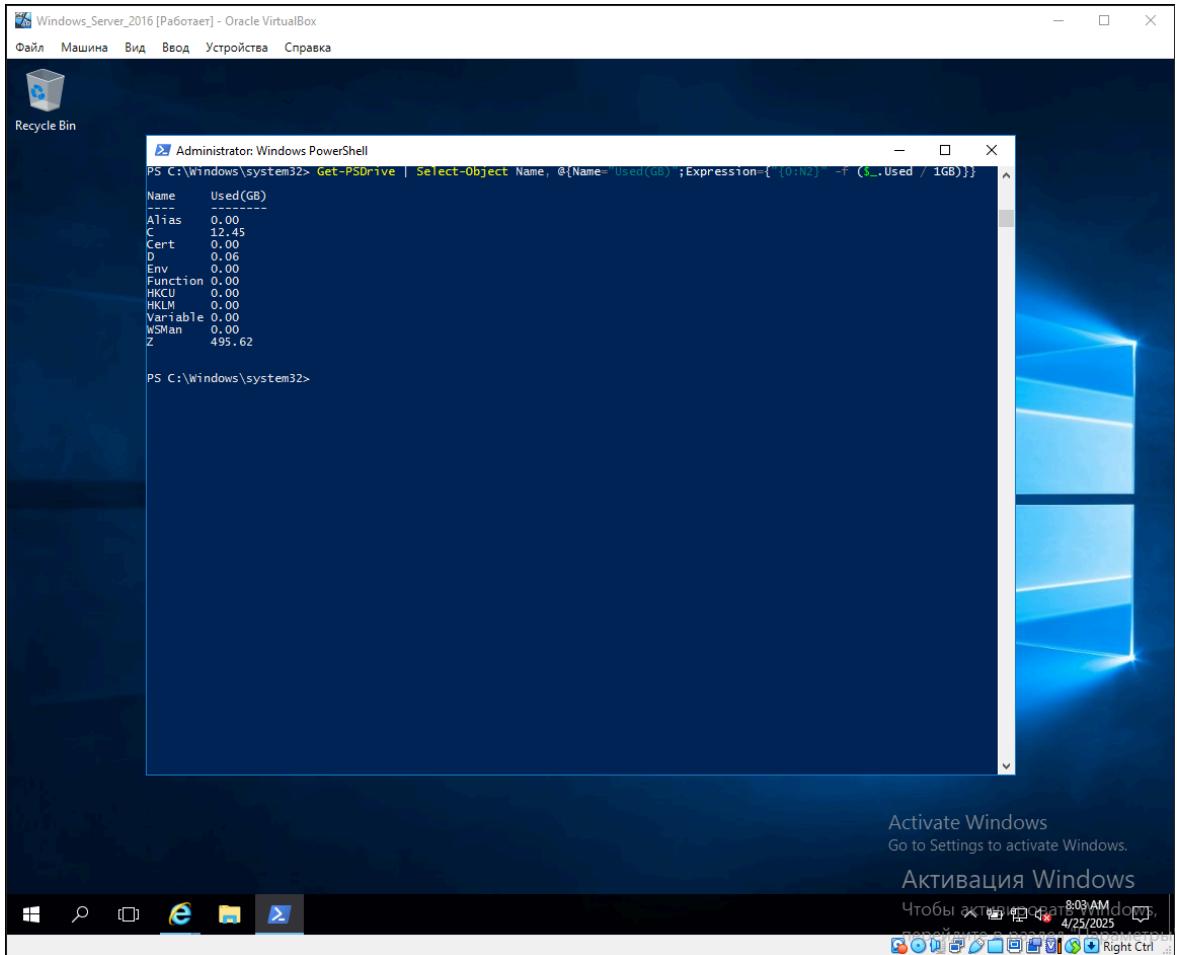


Рисунок 27 - Получение информации о дисках

12.2 Отфильтруйте вывод, чтобы оставить информацию о диске и объеме использованного пространства.



The screenshot shows a Windows Server 2016 desktop environment within Oracle VirtualBox. A PowerShell window titled 'Administrator: Windows PowerShell' is open, displaying the following command and its output:

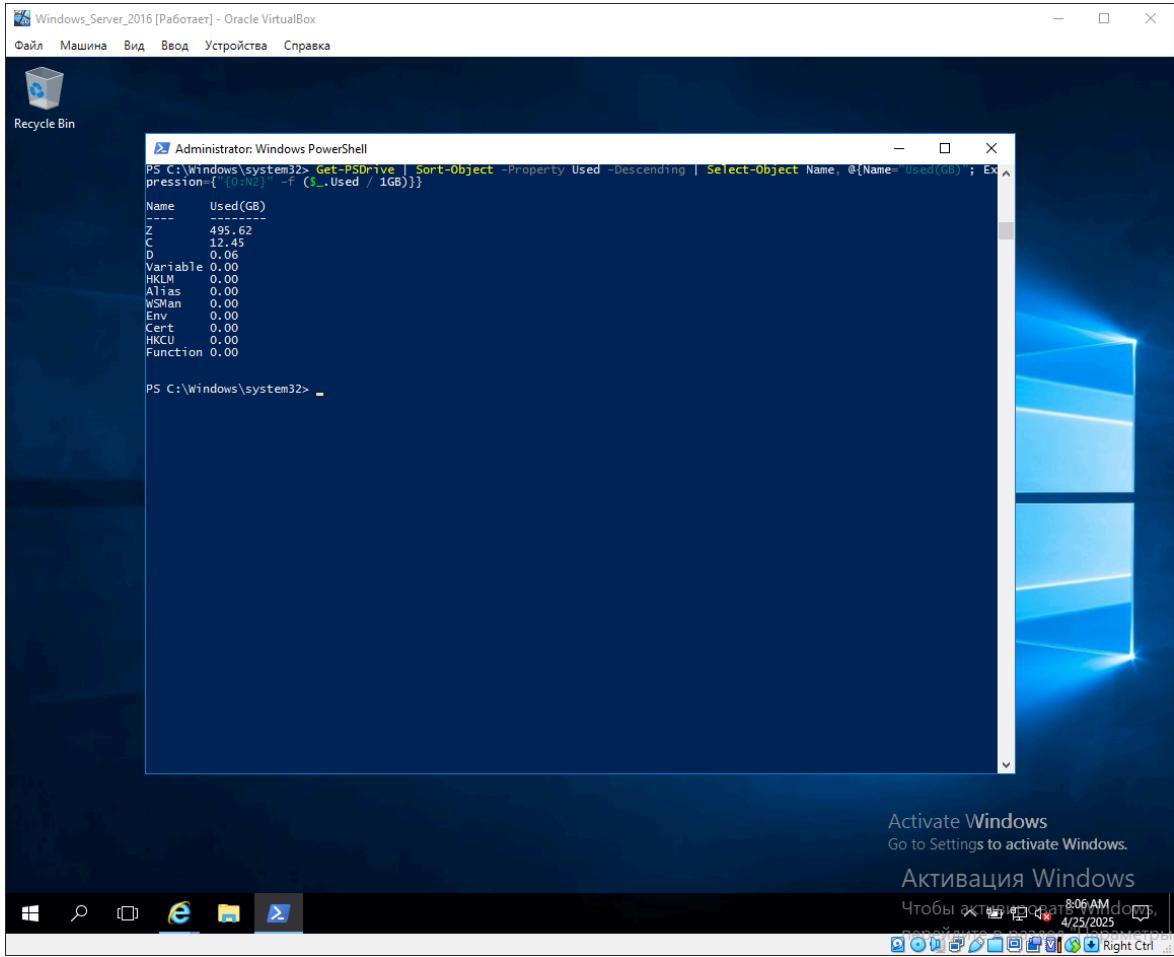
```
PS C:\Windows\system32> Get-PSDrive | Select-Object Name, @{Name='Used(GB'; Expression={ (0:Nz) -> ($_.Used / 1GB)})}
```

Name	Used(GB)
Alias	0.00
C	12.45
Cert	0.00
D	0.06
Env	0.00
Function	0.00
HKCU	0.00
HKLM	0.00
Variable	0.00
wSMAn	0.00
Z	495.62

The desktop background is the standard Windows 10 blue gradient. A 'Recycle Bin' icon is visible on the desktop. The taskbar at the bottom includes icons for File Explorer, Task View, Edge browser, and Start. A system tray notification from 'Activate Windows' is present, stating: 'Activate Windows Go to Settings to activate Windows.' Below it, another notification says: 'Активация Windows Чтобы активировать Windows 8:03 AM 4/25/2025' with a link to 'Проверить'.

Рисунок 28 - Отфильтрованный вывод

12.3 Сортируйте вывод по использованию диска.



The screenshot shows a Windows Server 2016 desktop environment within Oracle VirtualBox. A PowerShell window titled 'Administrator: Windows PowerShell' is open, displaying the following command and its output:

```
PS C:\Windows\system32> Get-PSDrive | Sort-Object -Property Used -Descending | Select-Object Name, @{Name= Used(GB); Expression={ $_.Used / 1GB}}
```

Name	Used(GB)
Z	495.62
C	12.45
D	0.06
Variable	0.00
HKL M	0.00
Alias	0.00
W SMan	0.00
Env	0.00
Cert	0.00
HKCU	0.00
Function	0.00

The desktop background is the standard Windows 10 blue gradient. A watermark for 'Activate Windows' is visible in the center of the screen, along with a 'Go to Settings to activate Windows.' link. The taskbar at the bottom shows several pinned icons, including File Explorer, Edge, and File History. The system tray shows the date and time as '8:06 AM 4/25/2025'.

Рисунок 29 - Отсортированный вывод

12.4 Передайте вывод в команду tee, чтобы записать его в файл disk_report.txt и одновременно отобразить на экране.

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-PSDrive | Sort-Object -Property Used -Descending | Select-Object Name, @{Name= Used(GB); Expression={ '{0:N2}' -f ($_.Used / 1GB) }} | Tee-Object -FilePath "disk_report.txt"; Exit
Name    Used(GB)
----   -----
Z      495.62
C      12.45
D      0.06
Variable 0.00
HKLM  0.00
Alias 0.00
wSMan 0.00
Env   0.00
Cert  0.00
HKCU  0.00
Function 0.00

PS C:\Windows\system32> Get-Content -Path .\disk_report.txt
Name    Used(GB)
----   -----
Z      495.62
C      12.45
D      0.06
Variable 0.00
HKLM  0.00
Alias 0.00
wSMan 0.00
Env   0.00
Cert  0.00
HKCU  0.00
Function 0.00

PS C:\Windows\system32>
```

Рисунок 30 - Передача вывода

Контрольные вопросы

1. Для используются текстовые файлы в ОС?

В ОС текстовые файлы используются для хранения конфигураций, логов, отчётов об ошибках.

2. Что такое стандартные файлы ОС?

Существует как минимум 3 стандартных файла:

стандартный файл ввода (stdio);

стандартный файл вывода (stdout);

стандартный файл ошибок (stderr).

Эти три стандартных файла доступны любому пользовательскому процессу с момента его возникновения. При работе пользовательского процесса можно организовать вывод в файл stdout (standard output), а

сообщения о состоянии – в специальный файл стандартный вывод ошибок stderr (standard error). Многие программы принимают ввод из специального файла с названием стандартный ввод stdin (standard input), который по умолчанию связан с клавиатурой.

3. Как осуществляется перенаправление работы стандартных файлов?

Перенаправление stdout: Команда > файл, добавление: >>.

Перенаправление stderr: Команда 2> файл, добавление: 2>>.

Объединение stdout и stderr: Команда *> файл или Команда 2>&1.

Перенаправление stdin: Get-Content файл | Команда.

4. Какие утилиты имеются в Windows для работы с текстом?

New-Item – позволяет создать текстовый файл.

Get-Content – позволяет получать данные из текстовых файлов.

Set-Content, Add-Content – заменяет или добавляют объекты в файл.

Out-File – записывает данные передаваемые по конвейеру в файл.

Tee-Object – сохраняет отображаемые объекты и передаёт их дальше по контейнеру.

Export-Csv, Import-Csv – предназначены для работы с csv-файлами.

Export-Clixml, Import-Clixml – предназначен для работы с xml-файлами.

5. Как произвести сохранение вывода любой команды в файл?

С помощью | (pipe) и команды Out-File, либо использовать перенаправление вывода с помощью >.

6. Как сделать замену символов в текстовом файле?

Замена символов производится при помощи команды Get-Content и ключа -replace