

Generating a Kernel Live Dump in Windows Server 2025

Planning / Implementation

A kernel live dump is a mechanism for capturing a snapshot of the system's memory without causing a crash or resetting the operating system.

A kernel live dump is non-disruptive so its primary benefit is to minimized downtime. Traditional crash dumps that are generated when the system crashes reset the operating system and disrupt user work, however, kernel live dumps allow the OS to continue to run while capturing memory information, which reduces downtime and user impact.

A Kernel live dump is effective for non-fatal issues. It is helpful in those scenarios where a crash has not occurred, but there are symptoms such as high CPU usage, memory leaks, or other abnormal behaviors.

Kernel Live dumps are similar to regular crash dump files, they can capture a consistent snapshot of kernel memory, including various memory pages including the following:

- KdDebuggerBlock
- Loaded Module List
- KiProcessorBlock
- PRCBs
- Current stack
- Current page directory table
- KI_USER_SHARED_DATA
- NTOS Kernel Image
- HAL Image

In this paper, we focus on kernel live dumps, which are code 0x161. These can be initiated manually by an administrator using Task Manager or a PowerShell command line.

Experiment: Using WinDbg to display the kernel live dump stop code information if created by Task Manager and PowerShell

0x161 is a stop code for kernel live dumps, it indicates the system administrator requested the collection of a kernel live dump. This code is used to identify live dumps only and never be used for a real bug check.

If the live dump is created by Task Manager, you can see the 1st parameter is `0x005461736b6d6772`, it means this file is created by Task Manager since this value is a hexadecimal encoding for the text string 'Taskmgr'.

```

0: kd> .bugcheck
Bugcheck code 00000161
Arguments 00546173`6b6d6772 00000000`00000000 00000000`00000000 00000000`00000000
0

0: kd> k
# Child-SP          RetAddr             Call Site
00 ffffffff05`f6f5a310 ffffffff801`781565d5 nt!IopLiveDumpCollectPages+0xd9
01 ffffffff05`f6f5a360 ffffffff801`78725307 nt!IopLiveDumpEndMirroringCallback+0x55
02 ffffffff05`f6f5a390 ffffffff801`78155bfa nt!MmDuplicateMemory+0x2e7
03 ffffffff05`f6f5a420 ffffffff801`78155cdc nt!IopLiveDumpCapture+0x86
04 ffffffff05`f6f5a480 ffffffff801`780a9fca nt!IopLiveDumpCaptureMemoryPages+0x50
05 ffffffff05`f6f5a5c0 ffffffff801`7813aa4e nt!IoCaptureLiveDump+0x432
06 ffffffff05`f6f5a7f0 ffffffff801`786f1caf nt!DbgkCaptureLiveKernelDump+0x336
07 ffffffff05`f6f5a890 ffffffff801`7828a255 nt!NtSystemDebugControl+0xc41bf
08 ffffffff05`f6f5a9b0 00007ffc`d2563054 nt!KiSystemServiceCopyEnd+0x25
09 0000007b`b6f7f838 00000000`00000000 0x00007ffc`d2563054
0: kd> .formats 00546173`6b6d6772
Evaluate expression:
Hex:      00546173`6b6d6772
Chars:    .Taskmgr

```

If the live dump is created by PowerShell, you can see the same stop code but the 1st parameter is null.

```

0: kd> .bugcheck
Bugcheck code 00000161
Arguments 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000
0

0: kd> k
# Child-SP          RetAddr             Call Site
00 fffffbd09`a52ced50 fffff802`d57565d5 nt!IopLiveDumpCollectPages+0xd9
01 fffffbd09`a52ceda0 fffff802`d5d25307 nt!IopLiveDumpEndMirroringCallback+0x55
02 fffffbd09`a52cedd0 fffff802`d5755bfa nt!MmDuplicateMemory+0x2e7
03 fffffbd09`a52cee60 fffff802`d5755cdc nt!IopLiveDumpCapture+0x86
04 fffffbd09`a52ceec0 fffff802`d56a9fca nt!IopLiveDumpCaptureMemoryPages+0x50
05 fffffbd09`a52cf000 fffff802`d573aa4e nt!IoCaptureLiveDump+0x432
06 fffffbd09`a52cf230 fffff802`d5cf1caf nt!DbgkCaptureLiveKernelDump+0x336
07 fffffbd09`a52cf2d0 fffff802`d588a255 nt!NtSystemDebugControl+0xc41bf
08 fffffbd09`a52cf3f0 00007ffc`c6dc3054 nt!KiSystemServiceCopyEnd+0x25
09 000000bb`ce27d458 00007ffc`9077eddf ntdll!NtSystemDebugControl+0x14
0a 000000bb`ce27d460 00000000`00000000 mispace!CLogCollectionServer::CaptureLiveDump+0x1b3

```

Using Task Manager to trigger a Kernel Live Dump

The Task Manager live dump feature is supported starting with Windows Server 2025.

To generate a kernel live dump using Task Manager, follow these steps:

1. Search "Task Manager" to start Windows Task Manager.

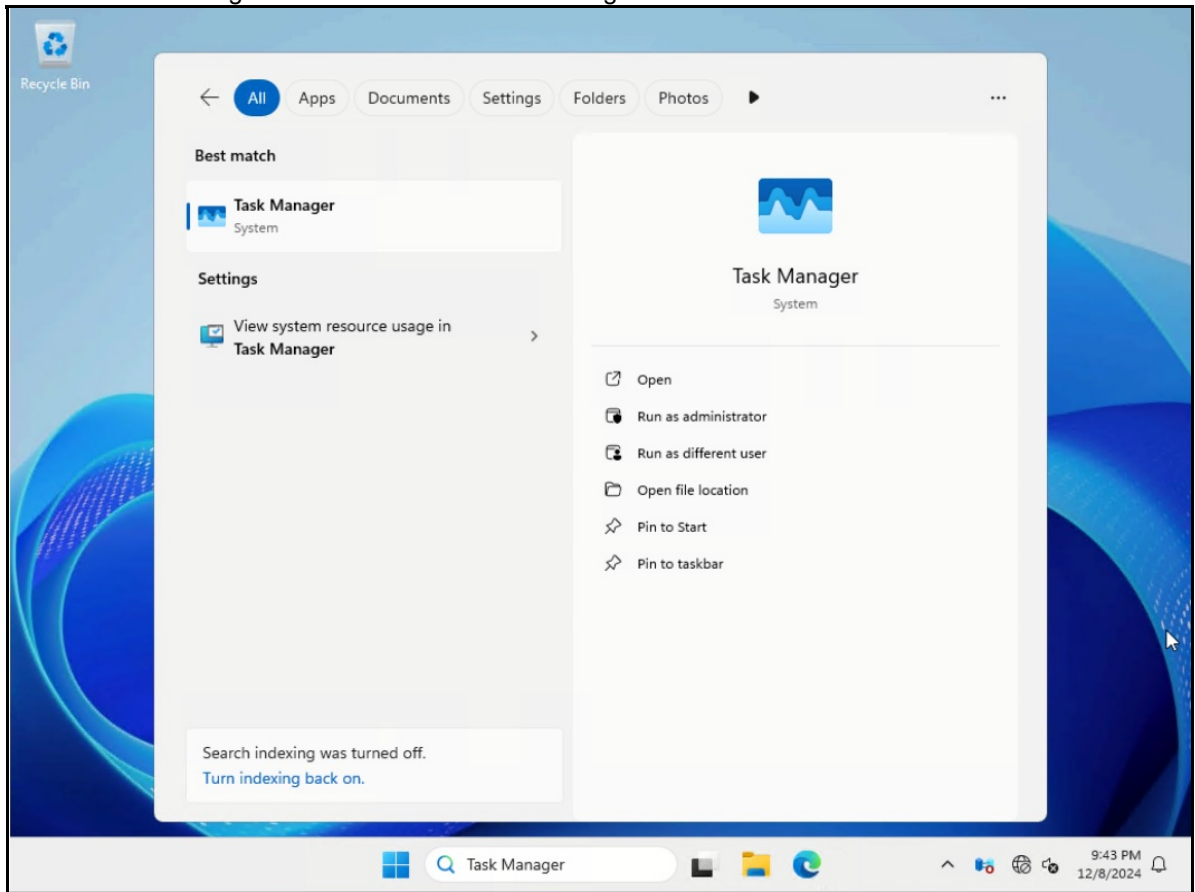


Figure 1. Start Windows Task Manager

2. Click the top left "Navigate" to **Details**.

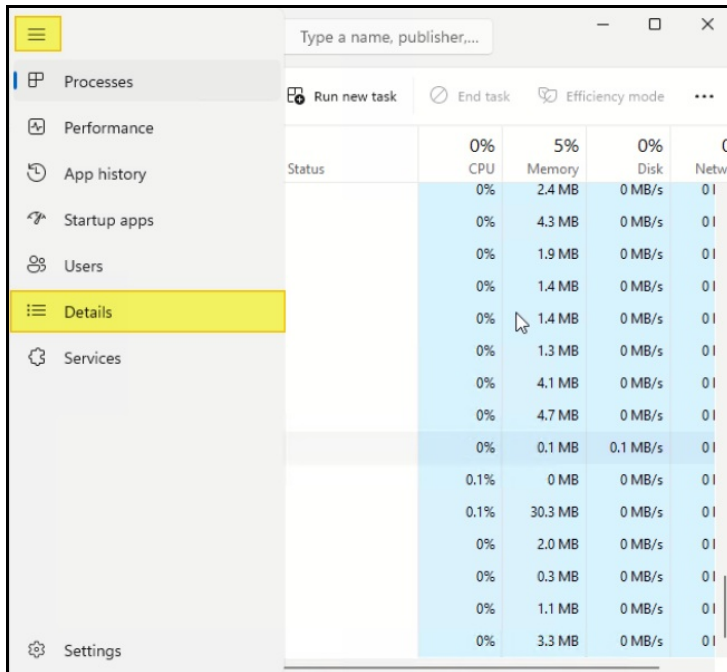


Figure 2. Navigate to Details

3. Find the **System**.

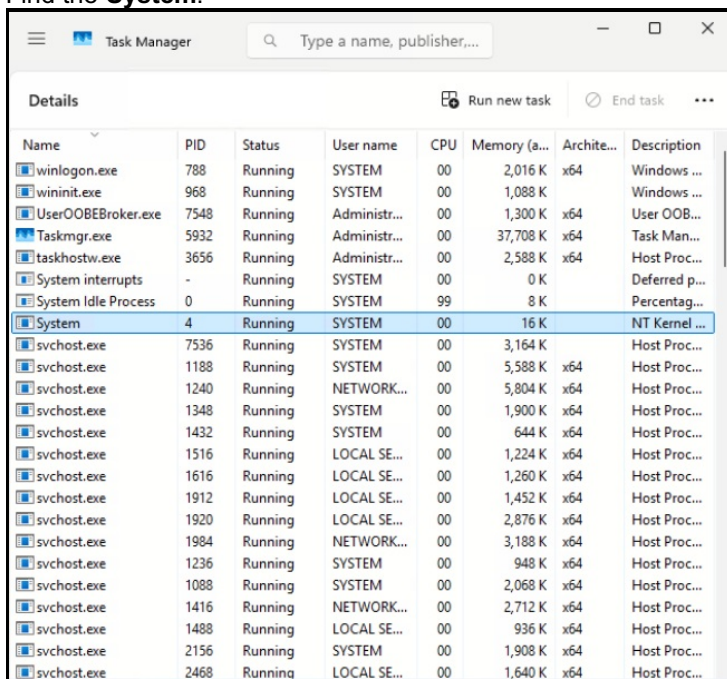


Figure 3. Locate the System process

4. Right click and select **Create live kernel memory dump file** . Then, select either a **Full live kernel memory dump** or a **Kernel stacks memory dump** from the pull-down menu.

The main differences between these two choices are as follows:

- o **Full live kernel memory dump** :
 - Contains active kernel memory.
 - Optional inclusion of hypervisor of hypervisor memory and user-mode memory.
 - Completed snapshot of the system's kernel memory.

- o **Kernel stacks memory dump:**
 - The file size is smaller than the full live kernel memory dump.
 - Limited to kernel processor stats and all kernel thread stacks.

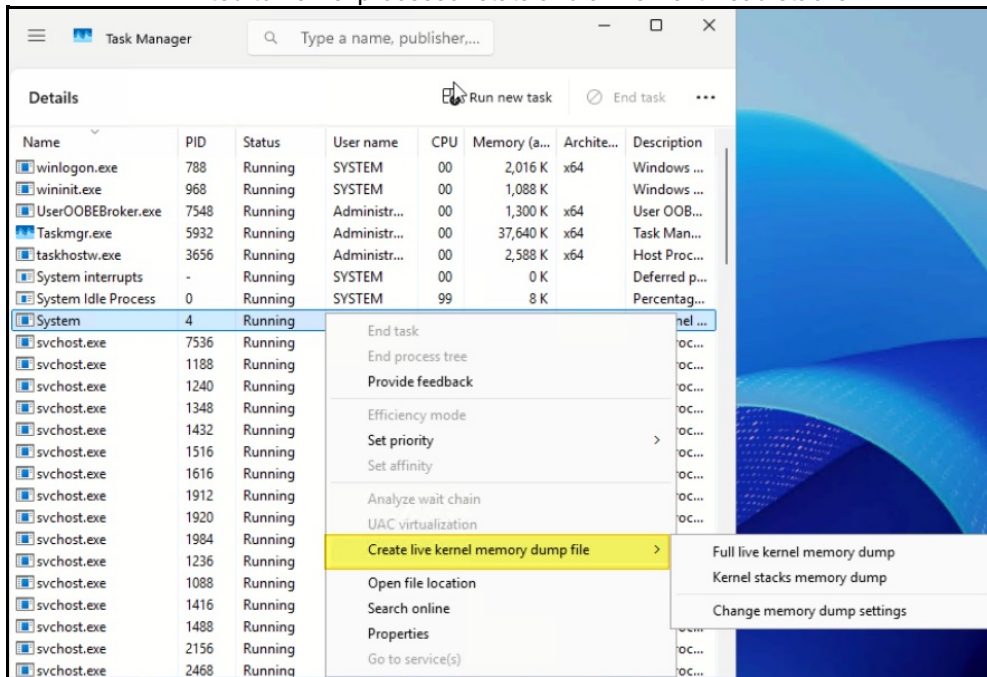


Figure 4. Create live kernel memory dump file by Task Manager

5. The kernel live dump will be created when the collecting is complete. The file is located at the default path:

C:\Users\
 <YourUserName>\AppData\Local\Microsoft\Windows\TaskManager\LiveKernelDumps

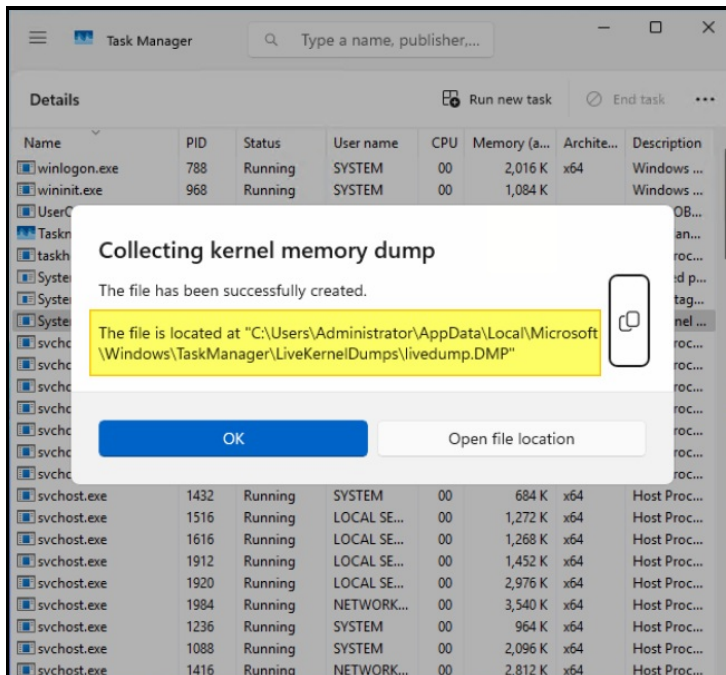


Figure 5. The kernel live dump is created at the default path

Using PowerShell to trigger a Kernel Live Dump

To generate a kernel live dump using PowerShell, follow these steps:

1. Search "Windows PowerShell Integrated Scripting Environment (ISE)" and select "Run as administrator".

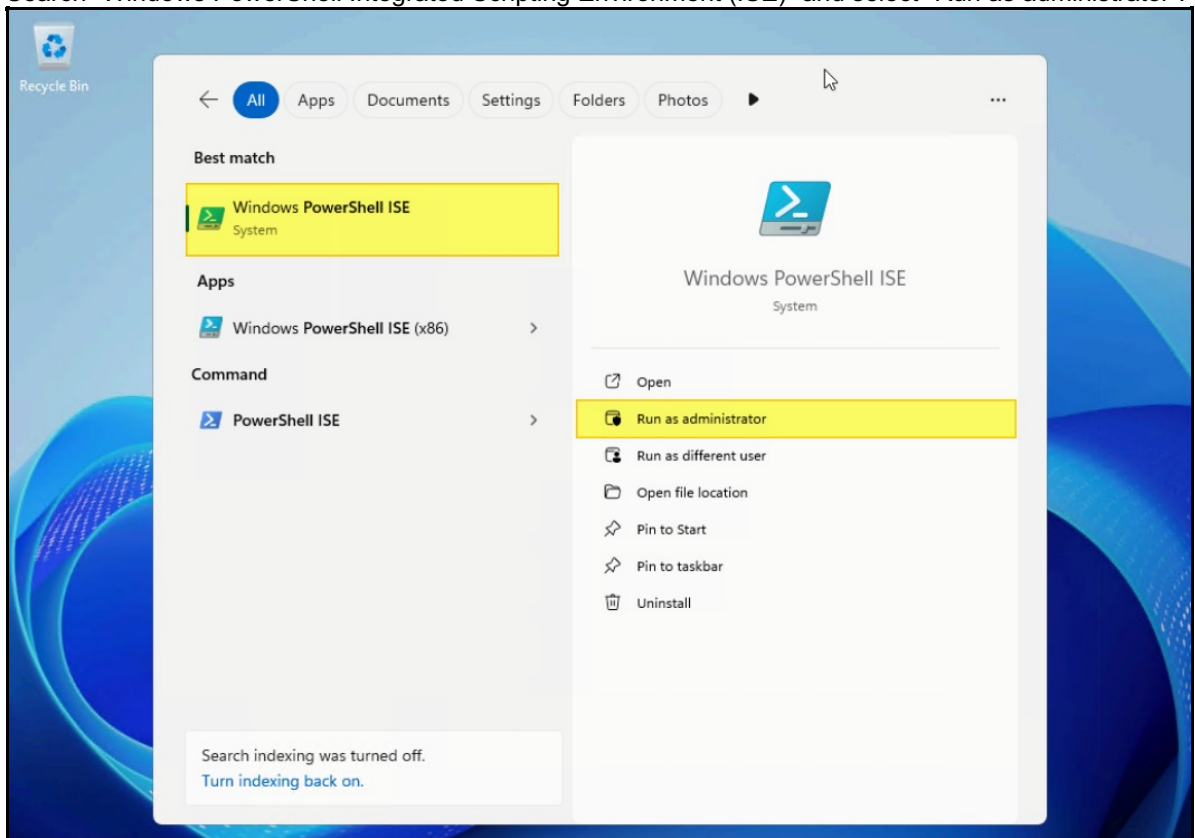


Figure 6. Run Windows PowerShell ISE as administrator

2. Copy and paste the following code to PowerShell ISE to create a PowerShell script. For example, save it as a file named **CreateLiveDump.ps1**.

```
Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process

$logPath="$env:userprofile\Desktop\logs" If (Test-Path -Path $logPath) {
    Remove-Item -Path $logPath -Force -Recurse
}

$storageName = Get-StorageSubSystem | Select-Object -ExpandProperty FriendlyName
Get-StorageDiagnosticInfo -StorageSubSystemFriendlyName $storageName -IncludeLiveDump -DestinationPath $logPath
```

The screenshot shows the Windows PowerShell ISE interface. The title bar reads "Administrator: Windows PowerShell ISE". The menu bar includes "File", "Edit", "View", "Tools", "Debug", "Add-ons", and "Help". The toolbar contains various icons for file operations and execution. The script editor shows a file named "CreateLiveDump.ps1" with the following code:

```
1 $logPath="$env:userprofile\Desktop\logs"
2
3 If (Test-Path -Path $logPath){
4     Remove-Item -Path $logPath -Force -Recurse
5 }
6
7
8
9 $storageName=Get-StorageSubSystem | Select -ExpandProperty FriendlyName
10 Get-StorageDiagnosticInfo -StorageSubSystemFriendlyName $storageName -IncludeLiveDump -DestinationPath $logPath
11
```

The console window at the bottom shows the prompt "PS C:\Users\Administrator>" with a cursor. The status bar at the bottom right indicates "Ln 6 Col 5" and "100%".

Figure 7. Create a PowerShell script

3. Launch PowerShell as administrator. Search "Windows PowerShell" and select "Run as Administrator".

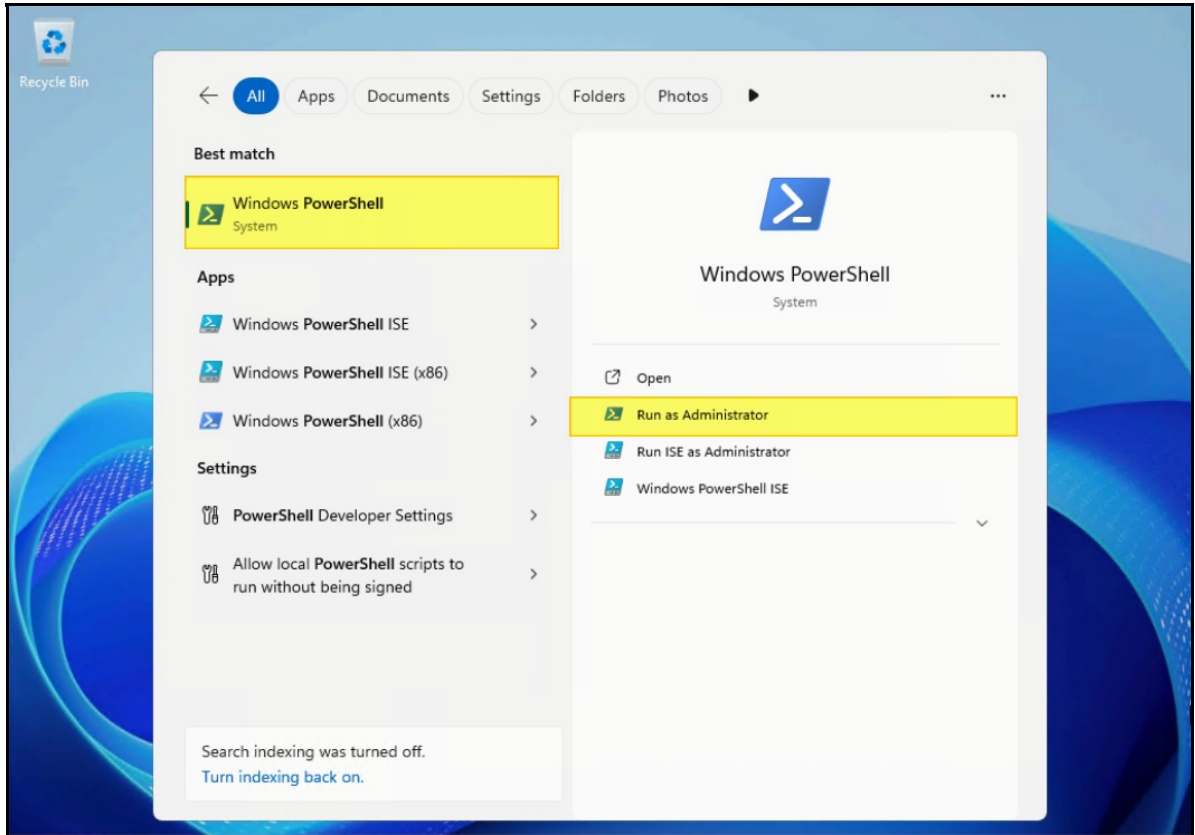


Figure 8. Run Windows PowerShell as administrator

4. Run the PowerShell script created in step 2.

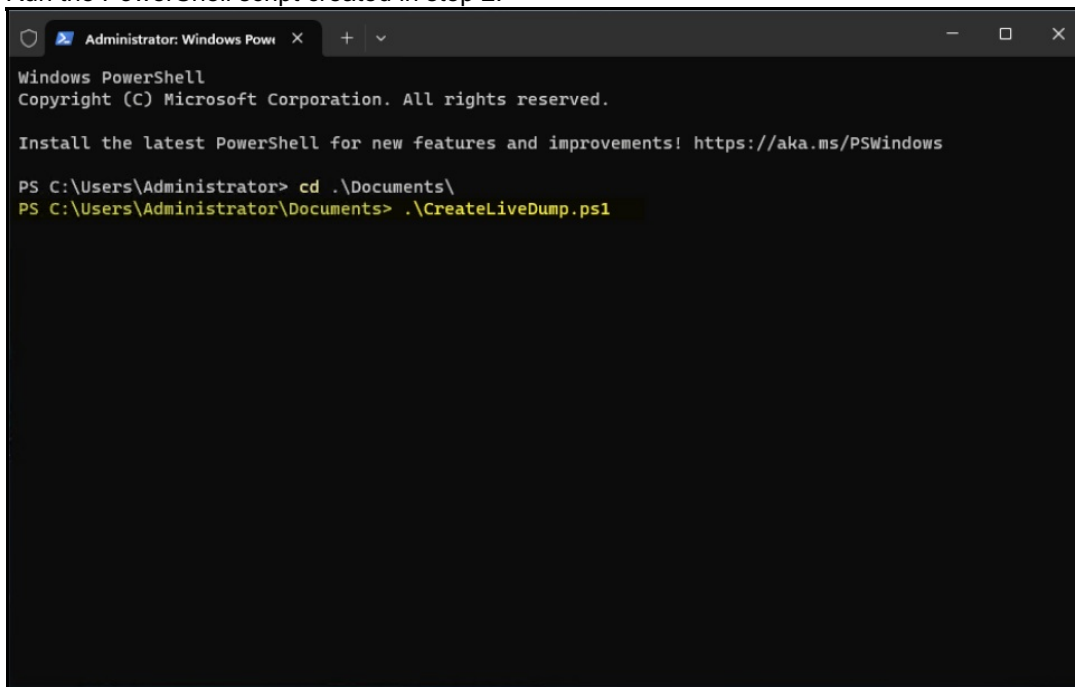
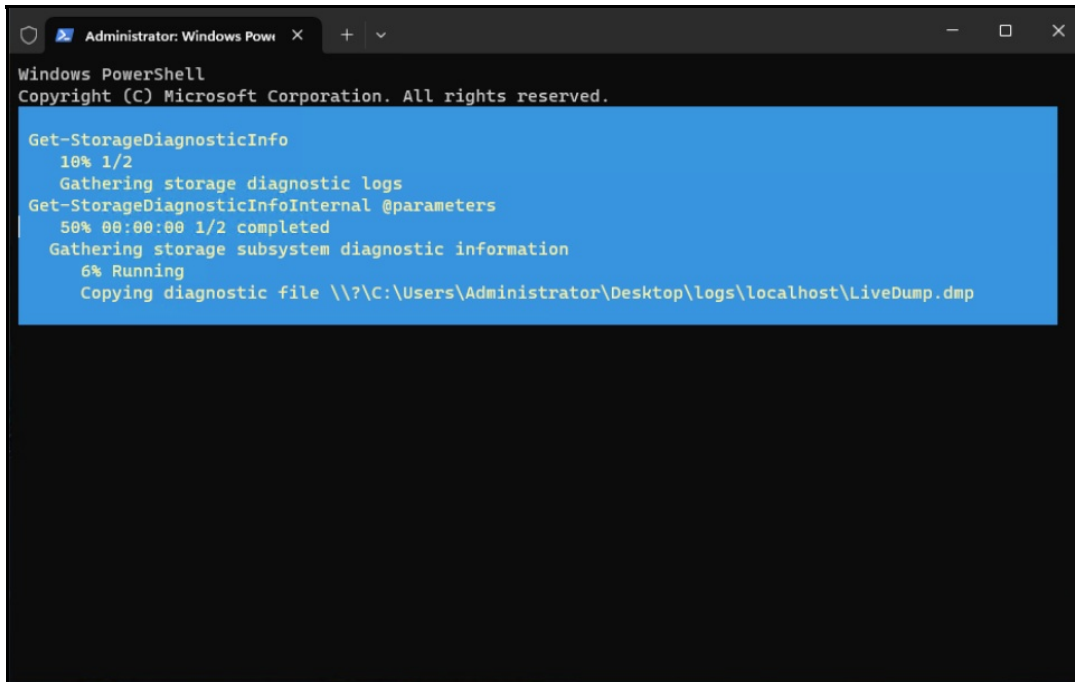


Figure 9. Run the PS script to create a kernel live dump

5. After running the script, the system starts to gather a kernel live dump in the specified storage subsystem.



```
Administrator: Windows Power...
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Get-StorageDiagnosticInfo
10% 1/2
Gathering storage diagnostic logs
Get-StorageDiagnosticInfoInternal @parameters
50% 00:00:00 1/2 completed
Gathering storage subsystem diagnostic information
6% Running
Copying diagnostic file \\?\C:\Users\Administrator\Desktop\logs\localhost\LiveDump.dmp
```

Figure 10. Gather the storage diagnostic information

Note: In this paper, we focus on how to manually trigger a kernel live dump on the system, so this using a PowerShell script to help to gather information about the boot device. This type of live dump, similar to a full live kernel memory dump, can also be created by Task Manager.

6. The folder “logs” is shown on the Desktop after finishing the progress. You can get the live dump under this folder.

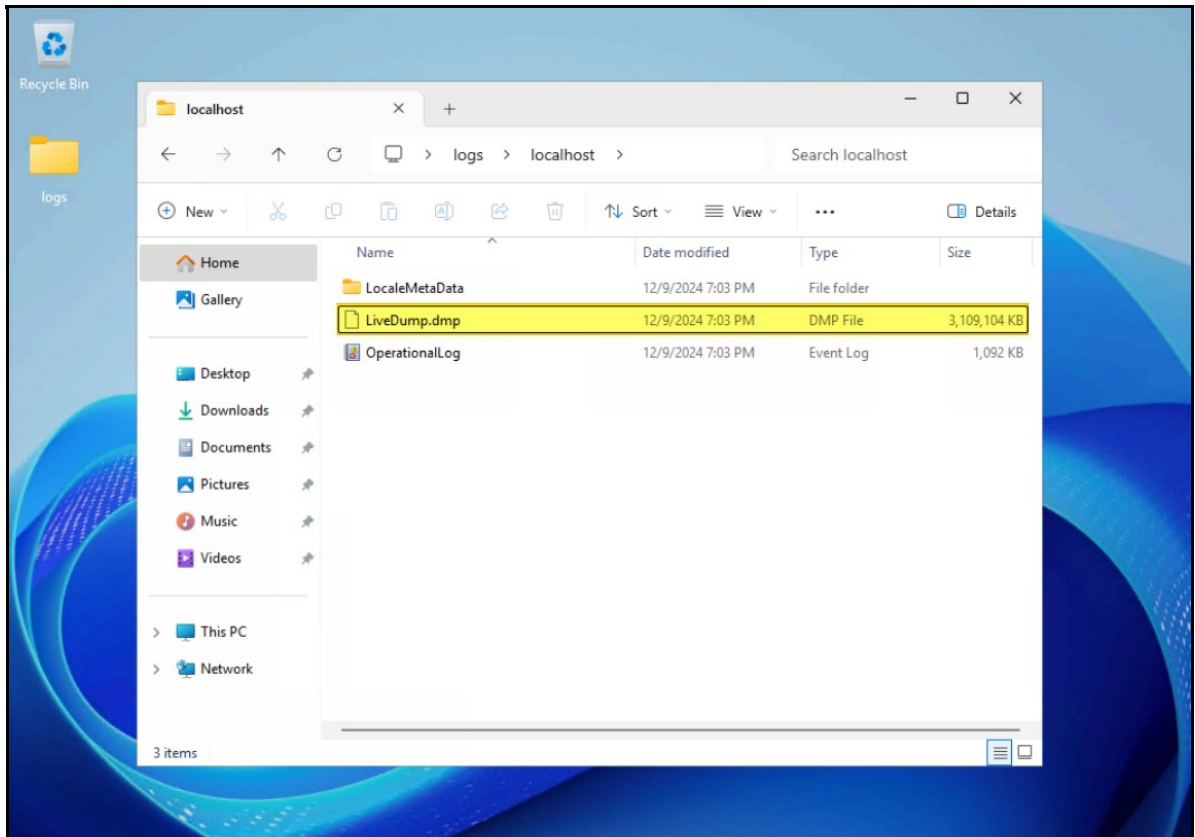


Figure 11. The kernel live dump is created on the folder logs

References

For more information, see these resources:

- Microsoft Learn, “Kernel Live Dump Code Reference,” <https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/kernel-live-dump-code-reference>
- Microsoft Learn, “Task Manager live memory dump,” <https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/task-manager-live-dump>
- Microsoft Learn, “Bug Check 0x161: LIVE_SYSTEM_DUMP,” <https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/bug-check-0x161--live-system-dump>
- Microsoft Learn, “Get-StorageDiagnosticInfo,” <https://learn.microsoft.com/en-us/powershell/module/storage/get-storagediagnosticinfo?view=windowsserver2025-ps>

Author

Wewe Chang is a Windows Engineer in the Lenovo Infrastructure Solutions Group, based in Taipei, Taiwan. She has more than 10 years of experience with Windows kernel and user mode debugging.

Special thanks to the following people for their contributions and suggestions:

- Boyong Li, Senior Engineer, OS Enablement
- Ronald Arndt Jr, Advisory Engineer, ThinkAgile Development
- Gary Cudak, OS Architect, ThinkAgile Development
- Jieting Li, Information Development
- David Watts, Lenovo Press

Related product families

Product families related to this document are the following:

- [Microsoft Windows](#)

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2025. All rights reserved.

This document, LP2142, was created or updated on February 3, 2025.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
<https://lenovopress.lenovo.com/LP2142>
- Send your comments in an e-mail to:
comments@lenovopress.com

This document is available online at <https://lenovopress.lenovo.com/LP2142>.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at <https://www.lenovo.com/us/en/legal/copytrade/>.

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo®

ThinkAgile®

The following terms are trademarks of other companies:

ISE™ is a trademark of Advanced Micro Devices, Inc.

Microsoft®, PowerShell, Windows PowerShell®, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.