Ex.No.9 Use Process Explorer to identify suspicious processes

AIM:

To use Process Explorer to monitor system activities and identify suspicious or malicious processes running on a Windows operating system.

DESCRIPTION:

Process Explorer, developed by **Microsoft Sysinternals**, is a powerful system monitoring and analysis tool that provides detailed information about all running processes on a Windows system. It serves as an advanced alternative to Task Manager, offering insights into process hierarchies, memory usage, handles, DLLs, and system resource consumption.

Digital forensic investigators and security analysts use Process Explorer to:

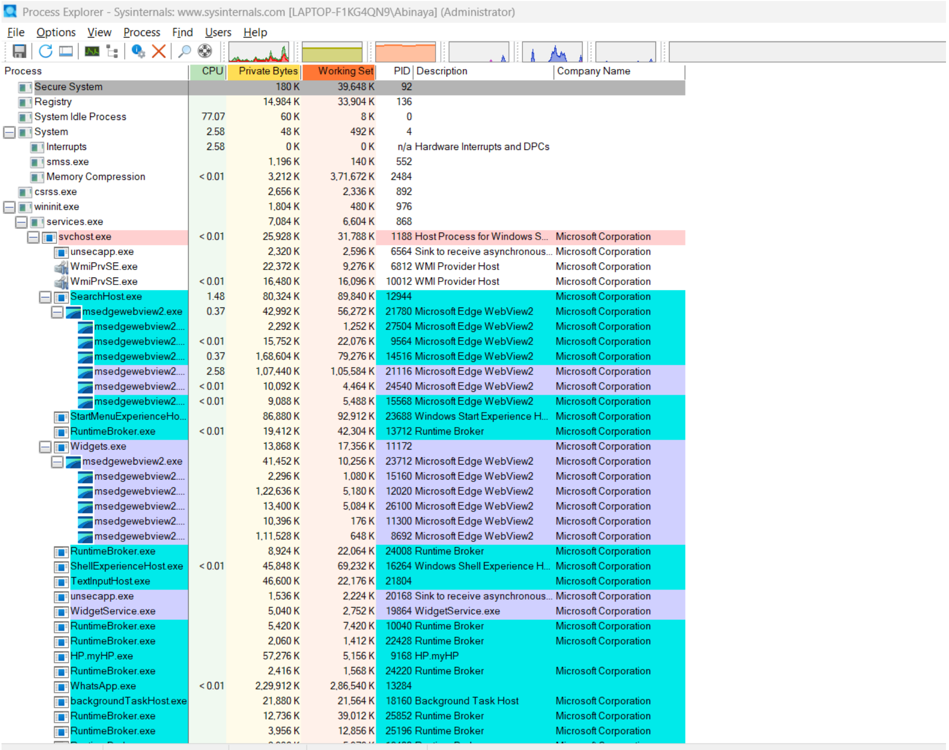
- Detect unauthorized or hidden processes
- Identify malware or trojan activities
- View real-time CPU and memory usage
- Examine process origins and digital signatures

Suspicious processes typically exhibit behaviors such as:

- Unrecognized executable names
- No verified digital signature
- Abnormal CPU or memory usage
- Running from unusual file paths

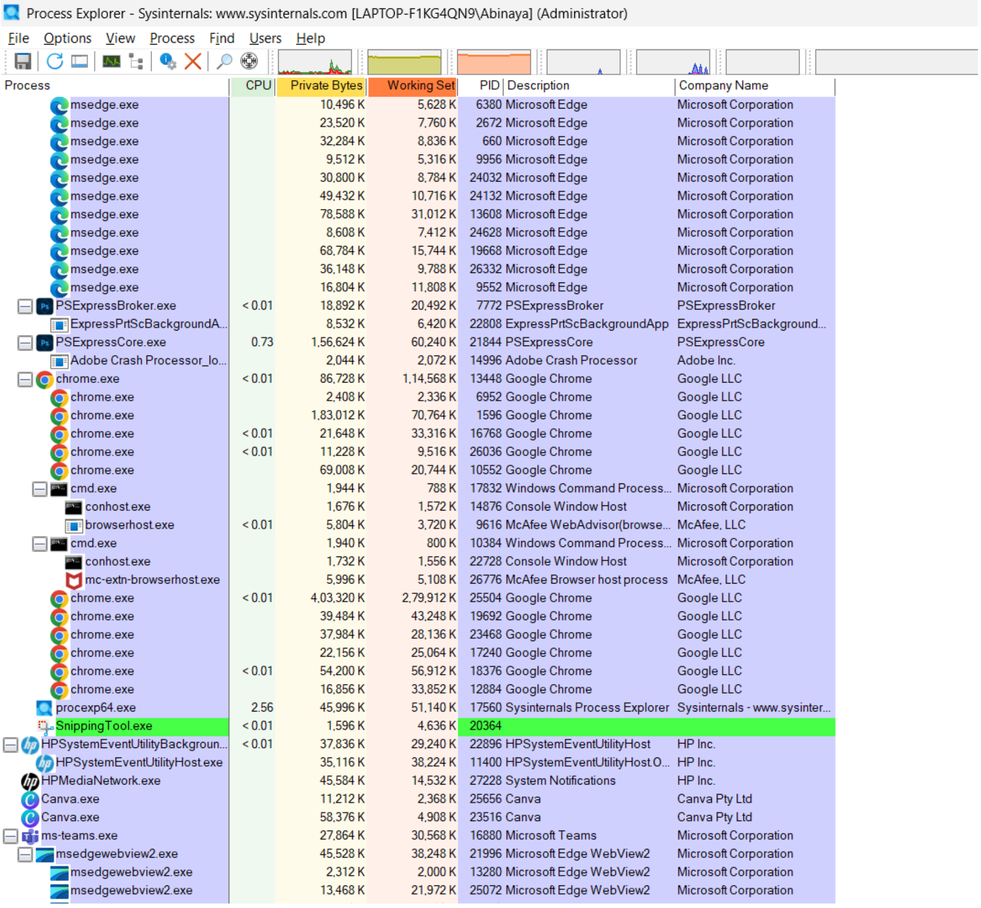
Process Explorer thus plays an important role in **live system analysis** during a forensic investigation.

PROCEDURE:



Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-F1KG4QN9\Abinaya] (Administrator)

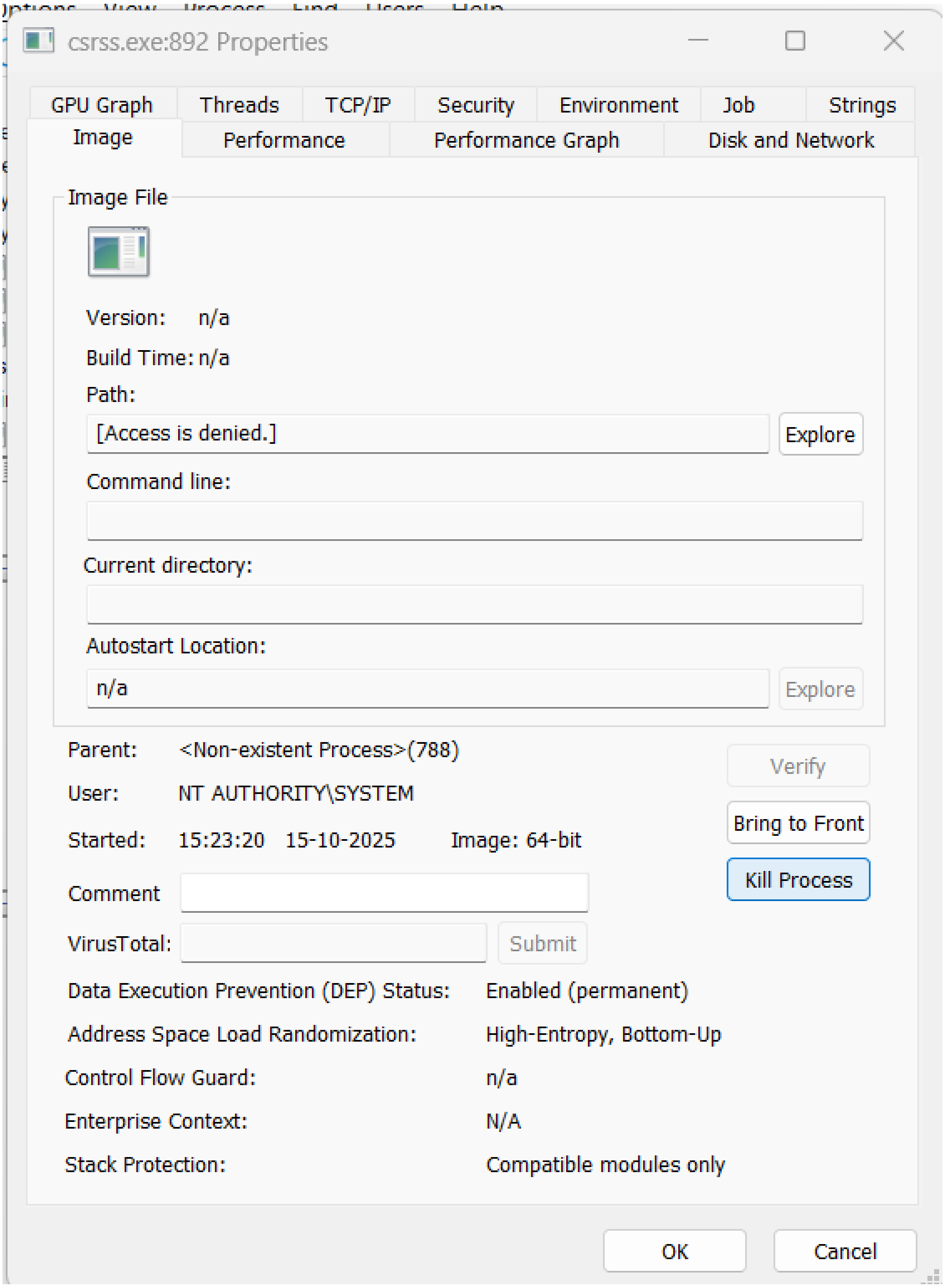
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System		180 K	39,648 K	92		
Registry		14,984 K	33,904 K	136		
System Idle Process	77.07	60 K	8 K	0		
System	2.58	48 K	492 K	4		
Interrupts	2.58	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,196 K	140 K	552		
Memory Compression	< 0.01	3,212 K	3,71,672 K	2484		
csrss.exe		2,656 K	2,336 K	892		
wininit.exe		1,804 K	480 K	976		
services.exe		7,084 K	6,604 K	868		
svchost.exe	< 0.01	25,928 K	31,788 K	1188	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		2,320 K	2,596 K	6564	Sink to receive asynchronous...	Microsoft Corporation
WmiPrvSE.exe		22,372 K	9,276 K	6812	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe	< 0.01	16,480 K	16,096 K	10012	WMI Provider Host	Microsoft Corporation
SearchHost.exe	1.48	80,324 K	89,840 K	12944		Microsoft Corporation
msedgewebview2.exe	0.37	42,992 K	56,272 K	21780	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		2,292 K	1,252 K	27504	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	< 0.01	15,752 K	22,076 K	9564	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	0.37	1,68,604 K	79,276 K	14516	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	2.58	1,07,440 K	1,05,584 K	21116	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	< 0.01	10,092 K	4,464 K	24540	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	< 0.01	9,088 K	5,488 K	15568	Microsoft Edge WebView2	Microsoft Corporation
StartMenuExperienceHo...		86,880 K	92,912 K	23688	Windows Start Experience H...	Microsoft Corporation
RuntimeBroker.exe	< 0.01	19,412 K	42,304 K	13712	Runtime Broker	Microsoft Corporation
Widgets.exe		13,868 K	17,356 K	11172		Microsoft Corporation
msedgewebview2.exe		41,452 K	10,256 K	23712	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		2,296 K	1,080 K	15160	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		1,22,636 K	5,180 K	12020	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		13,400 K	5,084 K	26100	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		10,396 K	176 K	11300	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		1,11,528 K	648 K	8692	Microsoft Edge WebView2	Microsoft Corporation
RuntimeBroker.exe		8,924 K	22,064 K	24008	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	< 0.01	45,848 K	69,232 K	16264	Windows Shell Experience H...	Microsoft Corporation
TextInputHost.exe		46,600 K	22,176 K	21804		Microsoft Corporation
unsecapp.exe		1,536 K	2,224 K	20168	Sink to receive asynchronous...	Microsoft Corporation
WidgetService.exe		5,040 K	2,752 K	19864	WidgetService.exe	Microsoft Corporation
RuntimeBroker.exe		5,420 K	7,420 K	10040	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,060 K	1,412 K	22428	Runtime Broker	Microsoft Corporation
HP.myHP.exe		57,276 K	5,156 K	9168	HP.myHP	
RuntimeBroker.exe		2,416 K	1,568 K	24220	Runtime Broker	Microsoft Corporation
WhatsApp.exe	< 0.01	2,29,912 K	2,86,540 K	13284		
backgroundTaskHost.exe		21,880 K	21,564 K	18160	Background Task Host	Microsoft Corporation
RuntimeBroker.exe		12,736 K	39,012 K	25852	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3,956 K	12,856 K	25196	Runtime Broker	Microsoft Corporation



Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-F1KG4QN9\Abinaya] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
msedge.exe		10,496 K	5,628 K	6380	Microsoft Edge	Microsoft Corporation
msedge.exe		23,520 K	7,760 K	2672	Microsoft Edge	Microsoft Corporation
msedge.exe		32,284 K	8,836 K	660	Microsoft Edge	Microsoft Corporation
msedge.exe		9,512 K	5,316 K	9956	Microsoft Edge	Microsoft Corporation
msedge.exe		30,800 K	8,784 K	24032	Microsoft Edge	Microsoft Corporation
msedge.exe		49,432 K	10,716 K	24132	Microsoft Edge	Microsoft Corporation
msedge.exe		78,588 K	31,012 K	13608	Microsoft Edge	Microsoft Corporation
msedge.exe		8,608 K	7,412 K	24628	Microsoft Edge	Microsoft Corporation
msedge.exe		68,784 K	15,744 K	19668	Microsoft Edge	Microsoft Corporation
msedge.exe		36,148 K	9,788 K	26332	Microsoft Edge	Microsoft Corporation
msedge.exe		16,804 K	11,808 K	9552	Microsoft Edge	Microsoft Corporation
PSExpressBroker.exe	< 0.01	18,892 K	20,492 K	7772	PSExpressBroker	PSExpressBroker
ExpressPrtScBackgroundA...		8,532 K	6,420 K	22808	ExpressPrtScBackgroundApp	ExpressPrtScBackground...
PSExpressCore.exe	0.73	1,56,624 K	60,240 K	21844	PSExpressCore	PSExpressCore
Adobe Crash Processor_lo...		2,044 K	2,072 K	14996	Adobe Crash Processor	Adobe Inc.
chrome.exe	< 0.01	86,728 K	1,14,568 K	13448	Google Chrome	Google LLC
chrome.exe		2,408 K	2,336 K	6952	Google Chrome	Google LLC
chrome.exe		1,83,012 K	70,764 K	1596	Google Chrome	Google LLC
chrome.exe	< 0.01	21,648 K	33,316 K	16768	Google Chrome	Google LLC
chrome.exe	< 0.01	11,228 K	9,516 K	26036	Google Chrome	Google LLC
chrome.exe		69,008 K	20,744 K	10552	Google Chrome	Google LLC
cmd.exe		1,944 K	788 K	17832	Windows Command Process...	Microsoft Corporation
conhost.exe		1,676 K	1,572 K	14876	Console Window Host	Microsoft Corporation
browserhost.exe	< 0.01	5,804 K	3,720 K	9616	McAfee WebAdvisor(browse...	McAfee, LLC
cmd.exe		1,940 K	800 K	10384	Windows Command Process...	Microsoft Corporation
conhost.exe		1,732 K	1,556 K	22728	Console Window Host	Microsoft Corporation
mc-extn-browserhost.exe		5,996 K	5,108 K	26776	McAfee Browser host process	McAfee, LLC
chrome.exe	< 0.01	4,03,320 K	2,79,912 K	25504	Google Chrome	Google LLC
chrome.exe		39,484 K	43,248 K	19692	Google Chrome	Google LLC
chrome.exe		37,984 K	28,136 K	23468	Google Chrome	Google LLC
chrome.exe		22,156 K	25,064 K	17240	Google Chrome	Google LLC
chrome.exe	< 0.01	54,200 K	56,912 K	18376	Google Chrome	Google LLC
chrome.exe		16,856 K	33,852 K	12884	Google Chrome	Google LLC
procexp64.exe	2.56	45,996 K	51,140 K	17560	Sysinternals Process Explorer	Sysinternals - www.sysinter...
SnippingTool.exe	< 0.01	1,596 K	4,636 K	20364		
HPSystemEventUtilityBackgroun...	< 0.01	37,836 K	29,240 K	22896	HPSystemEventUtilityHost	HP Inc.
HPSystemEventUtilityHost.exe		35,116 K	38,224 K	11400	HPSystemEventUtilityHost O...	HP Inc.
HPMediaNetwork.exe		45,584 K	14,532 K	27228	System Notifications	HP Inc.
Canva.exe		11,212 K	2,368 K	25656	Canva	Canva Pty Ltd
Canva.exe		58,376 K	4,908 K	23516	Canva	Canva Pty Ltd
ms-teams.exe		27,864 K	30,568 K	16880	Microsoft Teams	Microsoft Corporation
msedgewebview2.exe		45,528 K	38,248 K	21996	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2,312 K	2,000 K	13280	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		13,468 K	21,972 K	25072	Microsoft Edge WebView2	Microsoft Corporation

OUTPUT:



Version: n/a

Build Time: n/a

Path:

[Access is denied.]

Command line:

Current directory:

Autostart Location:

n/a

Parent: <Non-existent Process>(788)

User: NT AUTHORITY\SYSTEM

Started: 15:23:20 15-10-2025 Image: 64-bit

Comment

VirusTotal:

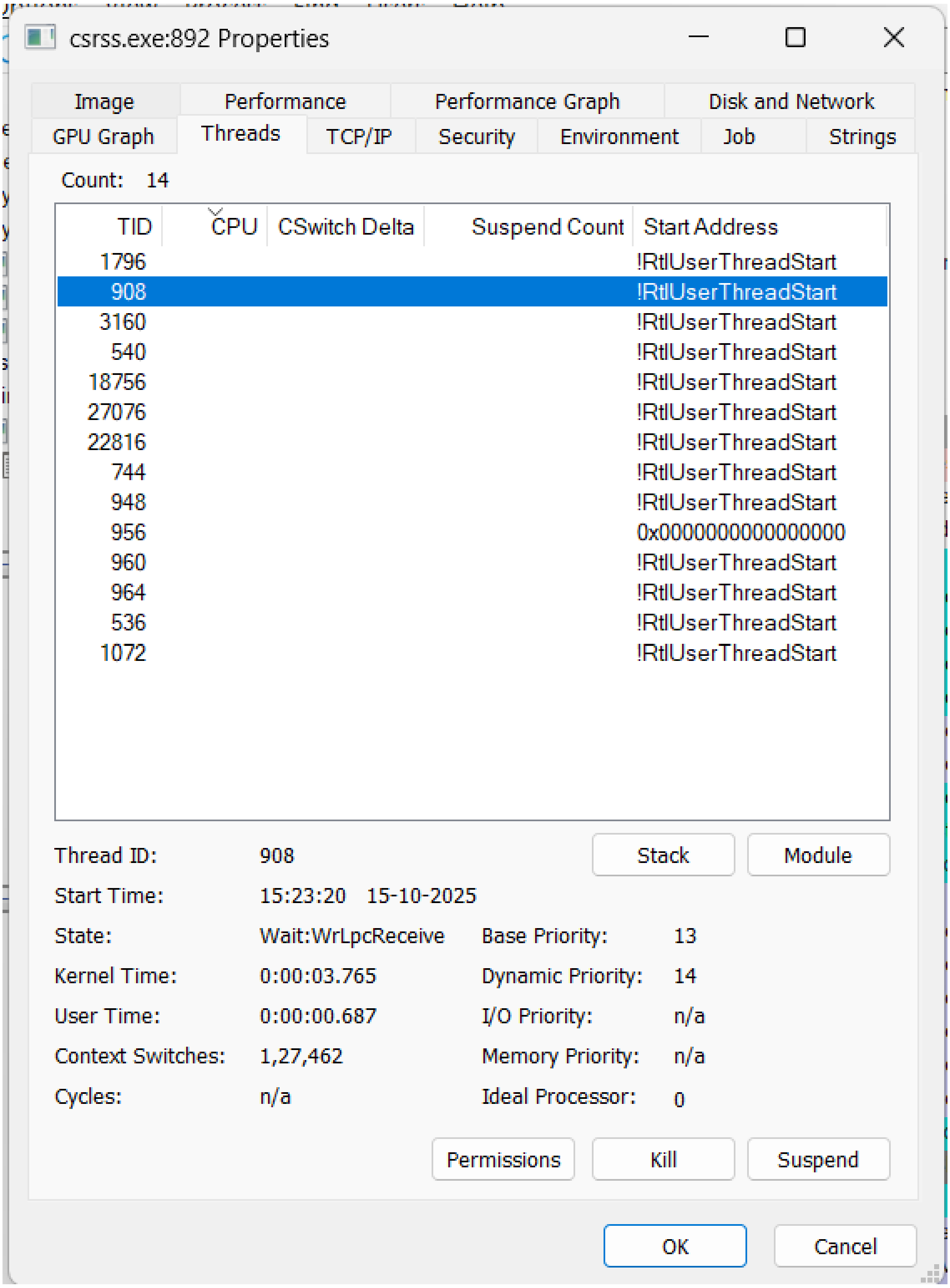
Data Execution Prevention (DEP) Status: Enabled (permanent)

Address Space Load Randomization: High-Entropy, Bottom-Up

Control Flow Guard: n/a

Enterprise Context: N/A

Stack Protection: Compatible modules only



Count: 14

TID	CPU	CSwitch Delta	Suspend Count	Start Address
1796				!RtlUserThreadStart
908				!RtlUserThreadStart
3160				!RtlUserThreadStart
540				!RtlUserThreadStart
18756				!RtlUserThreadStart
27076				!RtlUserThreadStart
22816				!RtlUserThreadStart
744				!RtlUserThreadStart
948				!RtlUserThreadStart
956				0x0000000000000000
960				!RtlUserThreadStart
964				!RtlUserThreadStart
536				!RtlUserThreadStart
1072				!RtlUserThreadStart

Thread ID: 908

Start Time: 15:23:20 15-10-2025

State: Wait:WrLpcReceive

Base Priority: 13

Kernel Time: 0:00:03.765

Dynamic Priority: 14

User Time: 0:00:00.687

I/O Priority: n/a

Context Switches: 1,27,462

Memory Priority: n/a

Cycles: n/a

Ideal Processor: 0

RESULT:

Thus, Process Explorer was successfully used to identify and analyze suspicious processes.