

NAME – Ekta Shukla

EMAIL ID – [shuklaekta811@gmail.com](mailto:shuklaekta811@gmail.com)

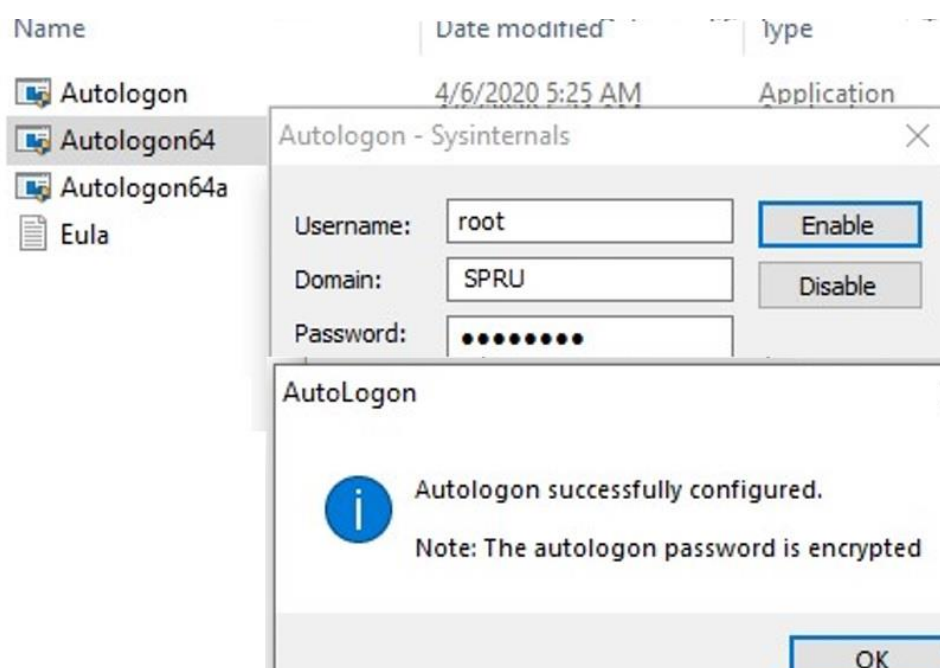
USER – 34746

## Windows tools for debugging with Screenshots and steps to create for Microsoft Intune Portal

These Sysinternals tools are valuable for troubleshooting and security analysis on Windows systems. Autologon automates user logins, while Process Explorer provides detailed process information. PsExec enables remote execution of commands and programs. PSTools helps manage logon sessions, and RegMon monitors registry activity. Sysmon provides system-level monitoring, and Whois (though not explicitly part of Sysinternals) is useful for network information.

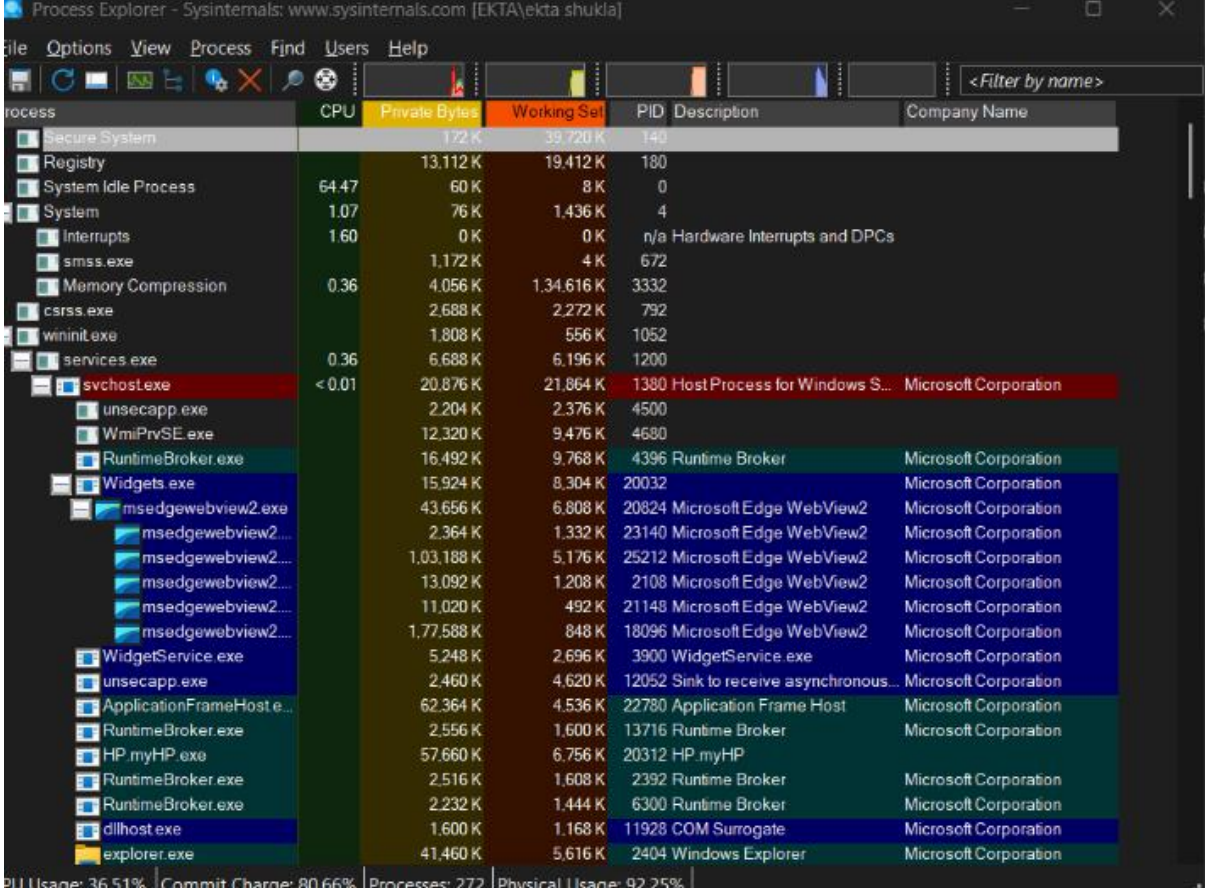
### 1. Autologon:

- **Purpose:** Automates the login process on a Windows system.
- **How it works:** It's a GUI tool that configures the Windows registry to automatically log on a specified user with provided credentials.
- **Usage:** Useful for headless systems or automated testing environments



## 2. Process Explorer:

- **Purpose:** A powerful tool for viewing and managing running processes.
- **How it works:** Provides detailed information about processes, including memory usage, handles, and open files.
- **Usage:** Essential for troubleshooting process-related issues, identifying resource bottlenecks, and investigating malware



The screenshot shows the Process Explorer window from Sysinternals. The interface includes a menu bar (File, Options, View, Process, Find, Users, Help) and a toolbar. The main window displays a list of processes in a table format. The columns are: Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. The processes are listed in a tree view on the left, with the 'svchost.exe' process highlighted in red. The status bar at the bottom shows 'CPU Usage: 36.51%', 'Commit Charge: 80.66%', 'Processes: 272', and 'Physical Usage: 92.25%'.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System		172 K	35,720 K	140		
Registry		13,112 K	19,412 K	180		
System Idle Process	64.47	60 K	8 K	0		
System	1.07	76 K	1,436 K	4		
Interrupts	1.60	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,172 K	4 K	672		
Memory Compression	0.36	4,056 K	1,34,616 K	3332		
csrss.exe		2,688 K	2,272 K	792		
wininit.exe		1,808 K	556 K	1052		
services.exe	0.36	6,688 K	6,196 K	1200		
svchost.exe	< 0.01	20,876 K	21,864 K	1380	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		2,204 K	2,376 K	4500		
WmiPrvSE.exe		12,320 K	9,476 K	4680		
RuntimeBroker.exe		16,492 K	9,768 K	4396	Runtime Broker	Microsoft Corporation
Widgets.exe		15,924 K	8,304 K	20032		Microsoft Corporation
msedgewebview2.exe		43,656 K	6,808 K	20824	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2,364 K	1,332 K	23140	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		1,03,188 K	5,176 K	25212	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		13,092 K	1,208 K	2108	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		11,020 K	492 K	21148	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		1,77,588 K	848 K	18096	Microsoft Edge WebView2	Microsoft Corporation
WidgetService.exe		5,248 K	2,696 K	3900	WidgetService.exe	Microsoft Corporation
unsecapp.exe		2,460 K	4,620 K	12052	Sink to receive asynchronous...	Microsoft Corporation
ApplicationFrameHost.exe		62,364 K	4,536 K	22780	Application Frame Host	Microsoft Corporation
RuntimeBroker.exe		2,556 K	1,600 K	13716	Runtime Broker	Microsoft Corporation
HP.myHP.exe		57,660 K	6,756 K	20312	HP.myHP	
RuntimeBroker.exe		2,516 K	1,608 K	2392	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,232 K	1,444 K	6300	Runtime Broker	Microsoft Corporation
dllhost.exe		1,600 K	1,168 K	11928	COM Surrogate	Microsoft Corporation
explorer.exe		41,460 K	5,616 K	2404	Windows Explorer	Microsoft Corporation

## 3. PsExec:

- **Purpose:** A powerful tool for remote execution of commands and programs.
- **How it works:** Allows administrators to run applications on a remote computer as if they were running locally.
- **Usage:** Useful for remote system management, patching, and troubleshooting malware.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

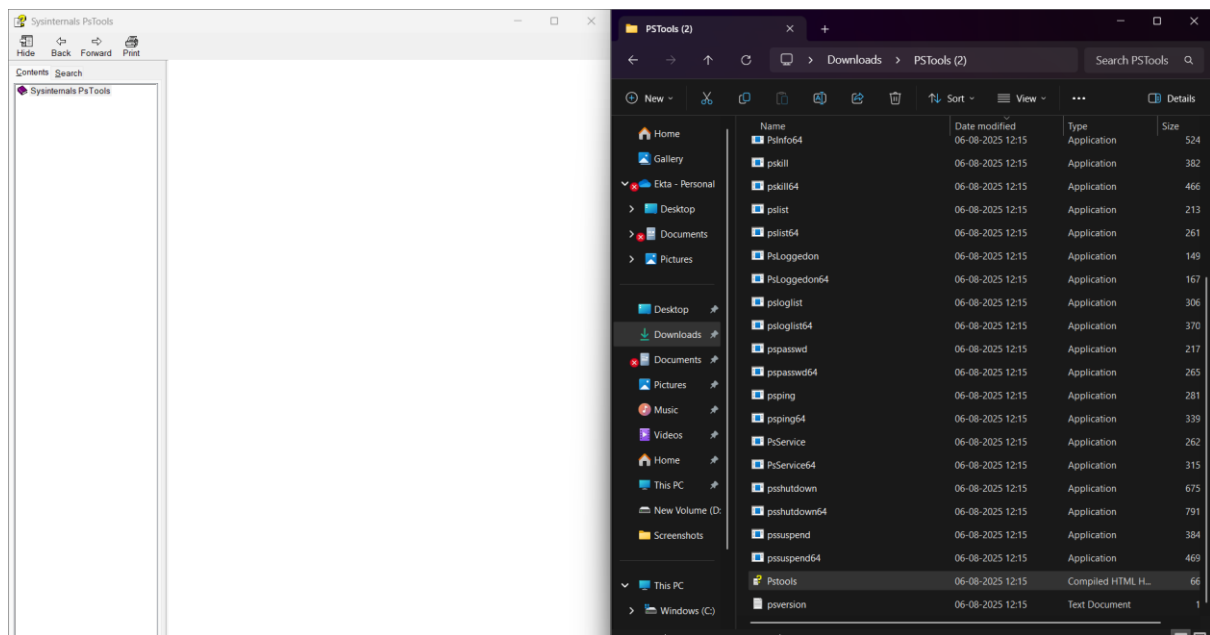
Time o...	Process Name	PID	Operation	Path	Result	Detail
12:42:17...	Explorer.EXE	23328	ReadFile	\Device\HarddiskVolume3\Windows\Sy...	SUCCESS	Offset 847872, Len...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\Windows.StateR...	SUCCESS	Offset 86016, Lengt...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 12680192, L...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\Windows.StateR...	SUCCESS	Offset 69632, Lengt...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\oleaut32.dll	SUCCESS	Offset 802816, Len...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 11515392, L...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset 1122304, Le...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 12819456, L...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\UIAutomationCor...	SUCCESS	Offset 4038848, Le...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\UIAutomationCor...	SUCCESS	Offset 4039176, Le...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\UIAutomationCor...	SUCCESS	Offset 4039192, Le...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\UIAutomationCor...	SUCCESS	Offset 4039456, Le...
12:42:17...	Explorer.EXE	23328	QueryStandardl...	C:\Windows\System32\UIAutomationCor...	SUCCESS	AllocationSize: 437...
12:42:17...	Explorer.EXE	23328	CreateFileMap...	C:\Windows\System32\UIAutomationCor...	FILE LOCKED WITH ONLY READERS	
12:42:17...	Explorer.EXE	23328	QueryStandardl...	C:\Windows\System32\UIAutomationCor...	SUCCESS	AllocationSize: 437...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 11970048, L...
12:42:17...	Explorer.EXE	23328	CreateFileMap...	C:\Windows\System32\UIAutomationCor...	SUCCESS	Sync Type: SyncTy...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset 1105920, Le...
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKCR\TypeLib\{EA39B853-5769-4937-8...	SUCCESS	
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 12758016, L...
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKCR\TypeLib\{EA39B853-5769-4937-8...	SUCCESS	
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset 1089536, Le...
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKCR\TypeLib\{EA39B853-5769-4937-8...	SUCCESS	
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKCR\TypeLib\{EA39B853-5769-4937-8...	SUCCESS	
12:42:17...	Explorer.EXE	23328	CloseFile	C:\Windows\System32\UIAutomationCor...	SUCCESS	
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset 1085440, Le...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 12778496, L...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset 1019904, Le...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 11499008, L...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\windows.storage...	SUCCESS	Offset 8388608, Le...
12:42:17...	lsass.exe	1228	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1703936, Le...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 12856320, L...
12:42:17...	lsass.exe	1228	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1687552, Le...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\windows.storage...	SUCCESS	Offset 7819264, Le...
12:42:17...	lsass.exe	1228	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1675264, Le...
12:42:17...	lsass.exe	1228	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1683456, Le...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 12839936, L...
12:42:17...	AdobeCollabSy...	27432	ReadFile	C:\Program Files\Adobe\Acrobat DC\Ac...	SUCCESS	Offset 41811456, L...
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 12056064, L...
12:42:17...	lsass.exe	1228	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1576960, Le...
12:42:17...	lsass.exe	1228	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1576960, Le...
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	
12:42:17...	Explorer.EXE	23328	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	
12:42:17...	AdobeCollabSy...	27432	ReadFile	C:\Program Files\Adobe\Acrobat DC\Ac...	SUCCESS	Offset 41233920, L...
12:42:17...	Explorer.EXE	23328	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset 1015808, Le...
12:42:17...	OneDrive.exe	22488	ReadFile	C:\Program Files\Microsoft OneDrive\25...	SUCCESS	Offset 11830784, L...

Showing 218090 of 427192 events (72%)

Backed by virtual memory

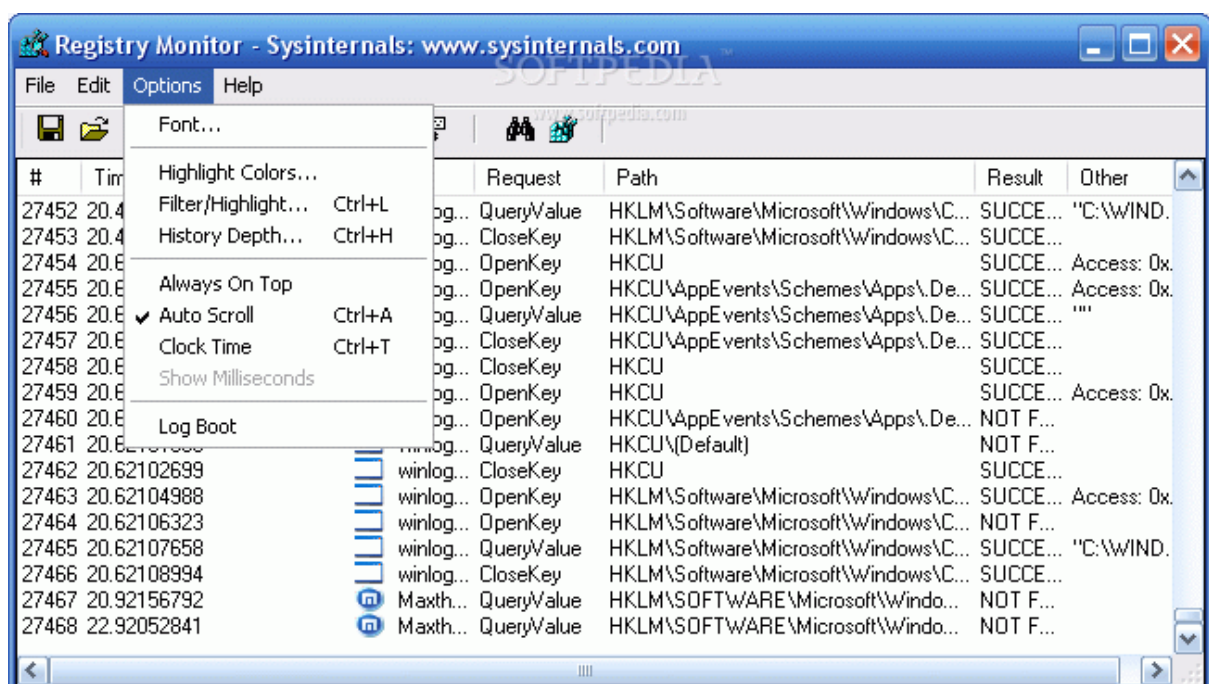
## 4. PSTools:

- **Purpose:** A collection of command-line tools for system administration and troubleshooting.
- **How it works:** Includes tools like PsLoggedOn, PsFile, and PsList, among others.
- **Usage:** Provides a wide range of administrative capabilities for local and remote systems.



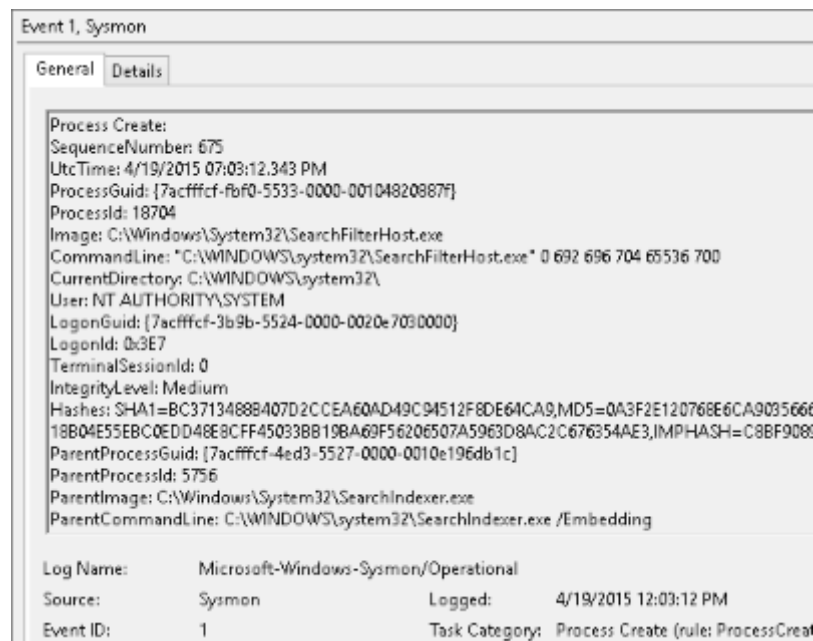
## 5. RegMon:

- **Purpose:** Monitors registry access and changes in real-time.
- **How it works:** Tracks all registry activity, including reads, writes, and deletes.
- **Usage:** Helps troubleshoot registry-related issues, identify rogue applications, and investigate security vulnerabilities.



## 6. Sysmon:

- **Purpose:** A Windows system service and driver that monitors and logs system activity.
- **How it works:** Provides detailed information about process creations, network connections, and file access changes.
- **Usage:** Essential for security monitoring, intrusion detection, and forensic analysis.



## 7. Whois:

- **Purpose:** A command-line tool (though not directly from Sysinternals) used to retrieve information about domain names and IP addresses.
- **How it works:** Queries a Whois database to retrieve registration details.
- **Usage:** Useful for network troubleshooting, identifying domain owners, and checking domain availability.



**Karen's Whols v2.7**

Welcome | Domain Name | IP Address

Paste or Enter Domain Name:  
KarenWare.com Lookup Info

WHOIS Server:  
Default WHOIS Server

Lookup Second-Level 'KARENWARE.COM' at whois.tucows.com

whois.internic.net | whois.tucows.com

```
Domain Name: KARENWARE.COM
Registry Domain ID: 24549448_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2018-04-07T03:58:08
Creation Date: 2000-04-10T02:48:26
Registrar Registration Expiration Date: 2019-04-10T02:48:26
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Reseller: Joe Winett dba SyiHosting.com
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
```

Copy Results | Tips ... | About ... | Exit

Response Received | 1 seconds | 12/5/2018 | 9:00 PM

## Steps to setup Microsoft Intune

