

Name: - Sooraj B

User I'D: - 34753

E-mail I'D: - rajsooraj318@gmail.com

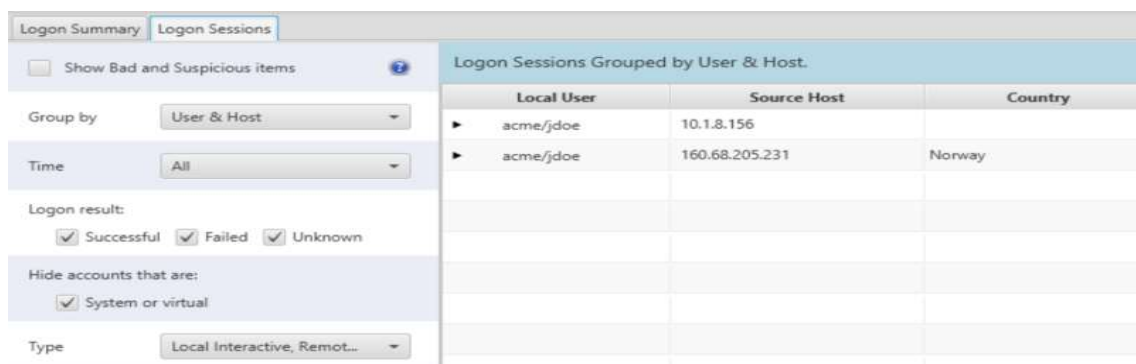
Assignment Topic: - Mention all windows tools for debugging with Screenshots and steps to create for Microsoft Intune Portal

Understanding Windows Debugging Tools (Sys internals Suite)

Today's session gave me a solid understanding of how powerful Sys internals tools are for troubleshooting Windows systems. Here's how I grasped each tool:

1.Logon Sessions:

- **Purpose:** Lists active user logon sessions on a Windows system.
- **Tool:** LogonSessions.exe (Sys internals Suite).
- **Use Case:**
 - Audit active sessions for security compliance.
 - Detect unauthorized logins (e.g., after-hours access).



The screenshot shows the 'Logon Sessions' window of the Sysinternals Suite. The left sidebar contains filters: 'Show Bad and Suspicious items' (unchecked), 'Group by' set to 'User & Host', 'Time' set to 'All', 'Logon result' with checkboxes for 'Successful', 'Failed', and 'Unknown' (all checked), 'Hide accounts that are:' with 'System or virtual' checked, and 'Type' set to 'Local Interactive, Remot...'. The main pane is titled 'Logon Sessions Grouped by User & Host.' and displays a table with three columns: 'Local User', 'Source Host', and 'Country'.

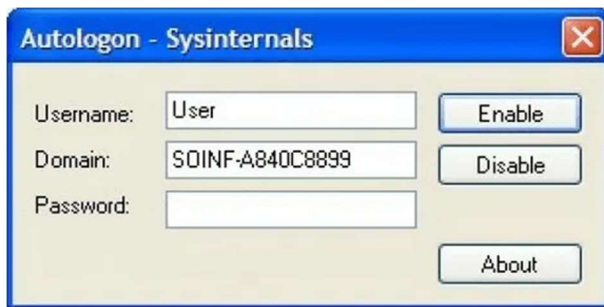
Local User	Source Host	Country
acme/jdoe	10.1.8.156	
acme/jdoe	160.68.205.231	Norway

This tool lists all active user logins on a system. It's useful for IT admins to track who's logged in, especially for security checks or auditing. Running LogonSessions.exe in the command line gives a quick snapshot of sessions, which helps in identifying unauthorized access.

2.Auto logon:

Purpose: Automates Windows login without manual password entry.

- **Tool:** GUI-based (Sysinternals).
- **How It Works:**
 - Stores encrypted credentials in HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
- **Use Case:**
 - Kiosks, automated testing environments.
- **Security Note:** Passwords are encrypted but should be used cautiously.



A handy tool for automating Windows logins without manual password entry. It securely stores credentials in the registry under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. While great for test labs or kiosks, I learned it should be used cautiously in production due to security risks, even though passwords are encrypted.

3.Process Explorer:

- **Purpose:** Advanced process monitoring (replaces Task Manager).
- **Features:**
 - Tree-view of parent/child processes.

- DLL/file/registry access per process.
- **Use Case:**
- Identify malware (e.g., injected DLLs).
- Debug application crashes.

The screenshot shows the Process Explorer window from Sysinternals. The title bar reads 'Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-SH1HMG9C\diego]'. The menu bar includes File, Options, View, Process, Find, Users, and Help. The toolbar contains icons for refreshing, pausing, and other process management actions. The main pane displays a list of processes with the following columns: Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. The processes are listed in a hierarchical tree view on the left. The status bar at the bottom shows 'CPU Usage: 99.58%', 'Commit Charge: 54.55%', 'Processes: 191', and 'Physical Usage: 52.37%'.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		5,412 K	26,244 K	92		
System Idle Process	< 0.01	60 K	8 K	0		
System	1.58	56 K	1,248 K	4		
smss.exe	1.58	0 K	0 K	n/a	Hardware Interrupts and DPCs	
Memory Compression		1,088 K	1,128 K	460		
csrss.exe	< 0.01	1,024 K	320,324 K	2176		
wininit.exe		1,852 K	5,644 K	600		
services.exe	< 0.01	1,420 K	6,972 K	696		
svchost.exe	< 0.01	5,152 K	8,720 K	804		
SearchHost.exe	< 0.01	8,088 K	24,380 K	944	Host Process for Windows S...	Microsoft Corporation
RuntimeBroker.exe	Susp...	110,200 K	96,220 K	4660		Microsoft Corporation
RuntimeBroker.exe		5,456 K	22,480 K	4724	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	1.32	11,512 K	37,892 K	2564	Runtime Broker	Microsoft Corporation
TestInputHost.exe	< 0.01	74,288 K	97,960 K	6320		Microsoft Corporation
dlhost.exe		5,560 K	15,492 K	2132	COM Surrogate	Microsoft Corporation
StartMenuExperienceHost.exe		43,292 K	80,984 K	1936	Windows Start Experience H...	Microsoft Corporation
RuntimeBroker.exe		2,008 K	10,136 K	4508	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	34,920 K	59,364 K	8840	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		3,984 K	21,436 K	9056	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6,072 K	19,804 K	4532	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.exe	< 0.01	9,544 K	35,096 K	1012	Application Frame Host	Microsoft Corporation
dlhost.exe		1,556 K	7,544 K	7804	COM Surrogate	Microsoft Corporation
SystemSettings.exe		58,656 K	131,208 K	10116	Settings	Microsoft Corporation
UserOOBEBroker.exe		2,008 K	9,288 K	11048	User OOBEBroker	Microsoft Corporation
ScreenClippingHost.exe	8.57	23,140 K	59,048 K	10336		Microsoft Corporation
svchost.exe	2.64	6,712 K	13,820 K	556	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,452 K	8,076 K	904	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	1,520 K	5,844 K	1144	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,824 K	9,140 K	1156	Host Process for Windows S...	Microsoft Corporation

It shows detailed process hierarchies, loaded DLLs, and even file/registry activity for each process. I can see myself using this to diagnose slow systems or detect malware hiding in processes.

4.PS Exec :

- **Purpose:** Execute commands remotely.
- **Syntax:** PsExec \\RemotePC -u User -p Password command.
- **Use Case:**
- Deploy scripts across multiple machines without RDP.

```

C:\Windows\System32\winrm.cmd qc -q
PS D:\MyScripts>
PS D:\MyScripts> psexec \\webservice -s -h powershell -command Enable-PSRemoting -Force

PSEXEC v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

WinRM has been updated to receive requests.
WinRM service type changed successfully.
WinRM service started.

WinRM is already set up for remote management on this computer.
powershell exited on webservice with error code 0.
PS D:\MyScripts>

```

- These are game-changers for remote administration. With PS Exec, I can run commands on another PC remotely, like restarting a service or deploying a script. The PS Tools suite (PS Kill, PS Shutdown, etc.) makes managing multiple machines easier—no need for manual logins.

6. RegMon (Legacy)

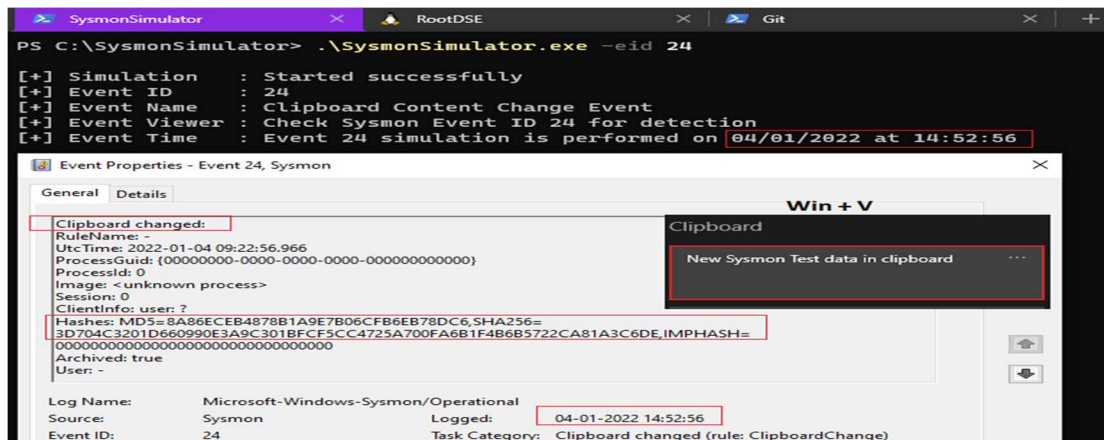
- **Replaced by:** Process Monitor (ProcMon).
- **Use Case:**
 - Track registry changes during software installations.

#	Time	Process	Request	Path
553	29.980...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
554	29.980...	ArVir.exe:2456	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
555	29.980...	ArVir.exe:2456	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
556	31.896...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
557	31.896...	ArVir.exe:2456	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
558	31.896...	ArVir.exe:2456	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
559	33.895...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
560	33.895...	ArVir.exe:2456	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
561	33.895...	ArVir.exe:2456	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
562	35.896...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
563	35.896...	ArVir.exe:2456	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
564	35.896...	ArVir.exe:2456	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
565	37.895...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
566	37.895...	ArVir.exe:2456	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
567	37.895...	ArVir.exe:2456	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
568	39.896...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
569	39.896...	ArVir.exe:2456	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
570	39.896...	ArVir.exe:2456	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
571	41.896...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
572	41.896...	ArVir.exe:2456	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
573	41.896...	ArVir.exe:2456	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
574	43.895...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
575	43.895...	ArVir.exe:2456	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
576	43.895...	ArVir.exe:2456	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
577	45.896...	ArVir.exe:2456	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

7. Sysmon

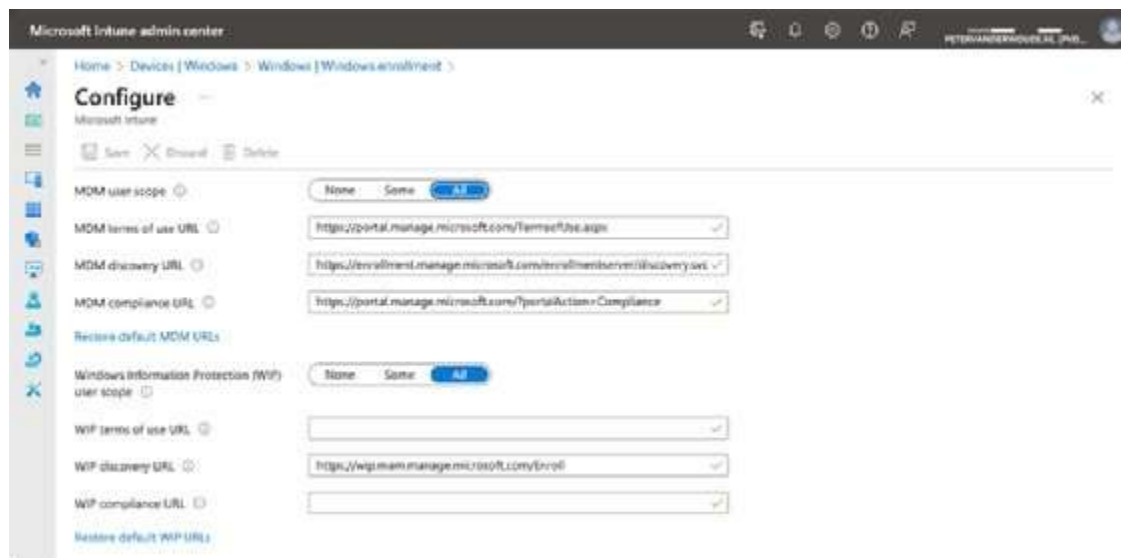
- **Purpose:** Log system events (e.g., process creation).

- **Configuration:** XML-based rules for event tracking.



- **Sysmon:** This tool logs system events (like new processes or network connections) to the Windows Event Log. It's a must for security teams to detect suspicious activity, like unexpected processes running in the background.

Intune Enrollment & Device Management



I also learned how to set up and use Microsoft Intune for managing devices:

- **Enrolling in the Free Trial:** Signing up is straightforward—just visit the Intune trial page, use a work/school email, and follow the prompts. Existing Azure AD users might need extra license assignments.
- **Syncing Devices:** After assigning apps or policies, devices need to sync to apply changes. This can be done through the Company Portal app (Settings > Sync) or directly from the Intune Admin Center under Devices > Select Device > Sync. For Windows, it can even be done via the taskbar's Company Portal icon.

Application Packaging & Registry Insights

We covered key concepts in MSI packaging and registry management:

- **Active Setup Versioning:** This ensures user-specific setups run during login. By tweaking the version number in `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{GUID}`, I can force setups to rerun for new users or after updates.
- **Intune win Conversion:** To deploy apps via Intune, they must be packaged as. Intune win files. The `IntuneWinAppUtil.exe` tool helps convert installers, but silent install commands (like `msi exec /i app.msi /qn`) are a must.
- **Tracking Installations:** The registry keys under `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` (for all users) and `HKCU\...` (per-user) store app details. Each app has a GUID, which can be used to silently uninstall it (`msiexec /x {GUID} /QN`).

Interactive vs. Non-Interactive Apps

I now understand the difference:

- **Interactive apps** (like Word or Chrome) need user input and have a GUI. They're what users directly interact with.
 - **Non-interactive apps** (like Windows Update or background services) run silently. They're crucial for automation but don't need user attention.
-

Troubleshooting with Logs & Proc Mon

- **Event Viewer:** The go-to for checking installation errors (Application logs) or system crashes (System logs).
 - **Process Monitor (Proc Mon):** Filters (e.g., Reg Set Value) help track registry/file changes during installs, making it easier to debug failed setups.
-

Final Thoughts

This session tied together tools and techniques for system debugging, Intune management, and software packaging. The hands-on tools like Sys internals and Intune will be incredibly useful in real-world scenarios—whether it's automating logins, remotely managing PCs, or deploying apps silently. Next, I'd like to practice converting an MSI to .intunewin and testing it in Intune's trial environment.