**Name : Sajiya**

**Email id :** [**sajiyadl888@gmail.com**](mailto:sajiyadl888@gmail.com)

**PRACTICE ACTIVITY 2**

**Topics(i)-Using Windows Tools for Debugging: LogonSessions, Autologon, Process Explorer, Psexec, PSTools, RegMon, Whois, SysMon, Process Monitor**

**INTRODUCTION**

For effective Windows system debugging, tools like Autologon, Process Explorer, PsExec, and others from Sysinternals provide in-depth capabilities far beyond basic tools. Each one plays a specific role in diagnosing performance, security, and configuration problems. Understanding and applying them can greatly improve the speed and success of troubleshooting in both local and remote environments.

**1. Logon Sessions**

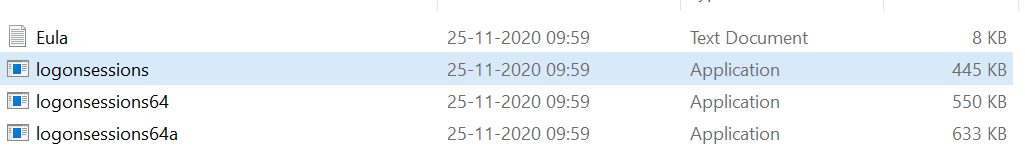
**Purpose:**  
Displays all users currently logged into the system along with session details.

**How it Works:**  
Shows login session data such as username, session ID, login time, and session type (local/remote).

**Use in Debugging:**

* Detects unauthorized or unexpected user logins
* Helps track active sessions during system issues
* Useful in security audits or suspicious activity detection

(screenshot)



**2. Autologon**

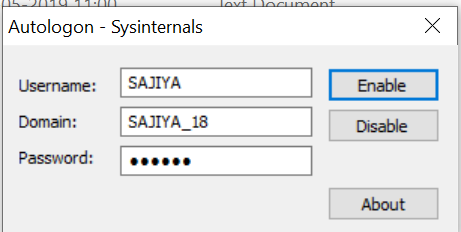
**Purpose:**  
Automatically logs in a user account during system startup.

**How it Works:**  
Stores login credentials securely in the Windows Registry and skips the login screen.

**Use in Debugging:**

* Speeds up repetitive testing or reboots
* Helps identify issues caused by startup applications
* Saves time in test environments and headless systems

(screenshot)



**3. Process Explorer**

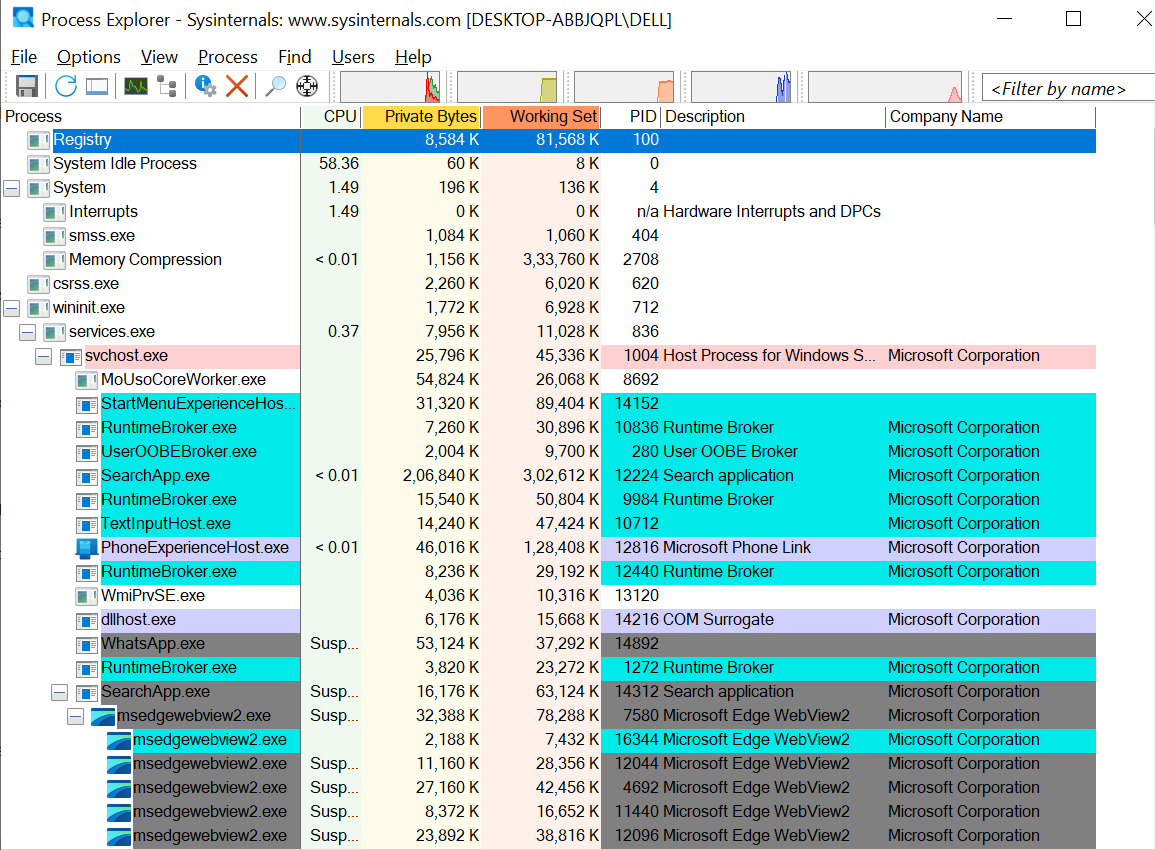
**Purpose:**  
An advanced Task Manager alternative that provides detailed information about running processes.

**How it Works:**  
Displays CPU and memory usage, file handles, DLLs, and process hierarchy.

**Use in Debugging:**

* Identifies high-resource processes or malware
* Analyzes application crashes or hangs
* Monitors background process behavior and open files

(Screenshot)



**4. PsExec**

**Purpose:**  
Allows remote execution of commands and applications on other systems.

**How it Works:**  
Runs programs on a remote machine via command line with administrative privileges.

**Use in Debugging:**

* Executes scripts or diagnostic tools remotely
* Troubleshoots systems without physical access
* Useful in managing multiple systems efficiently

**5. PSTools**

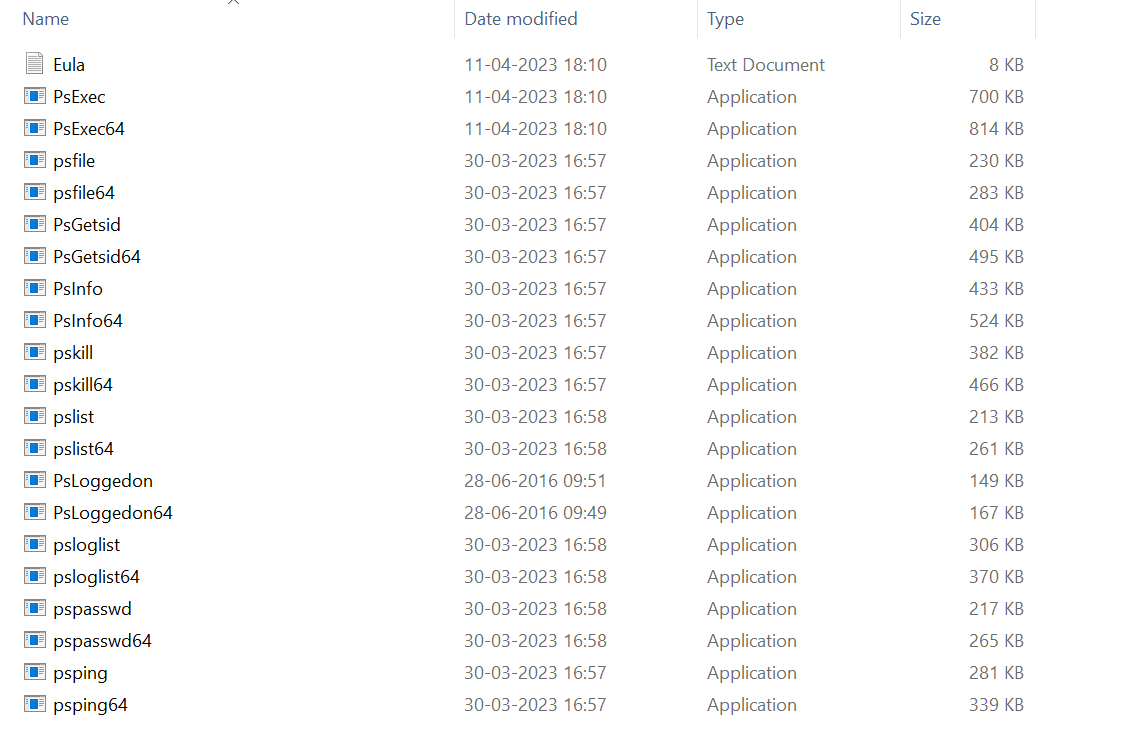
**Purpose:**  
A collection of command-line utilities for system management and monitoring.

**How it Works:**  
Includes tools like PsKill, PsList, PsLoggedOn, and PsFile for process and user control.

**Use in Debugging:**

* Stops unresponsive or harmful processes
* Identifies currently logged-in users
* Tracks remote file usage and locked resources

(Screenshot)



**6. RegMon (Registry Monitor)**

**Purpose:**  
Monitors Windows Registry activity in real-time.

**How it Works:**  
Logs all registry changes including reads, writes, and deletions by processes.

**Use in Debugging:**

* Detects software configuration or installation issues
* Identifies registry modifications by malware
* Helps troubleshoot permission or access errors

**7. Sysmon (System Monitor)**

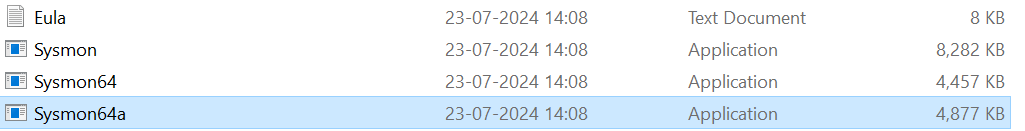
**Purpose:**  
Logs system-level events like process creation, network connections, and file access.

**How it Works:**  
Runs as a background service and logs data to the Windows Event Log for analysis.

**Use in Debugging:**

* Tracks detailed system behavior over time
* Identifies signs of intrusion or malware activity
* Aids in forensic investigation after system failure

(Screenshot)



**8. Whois**

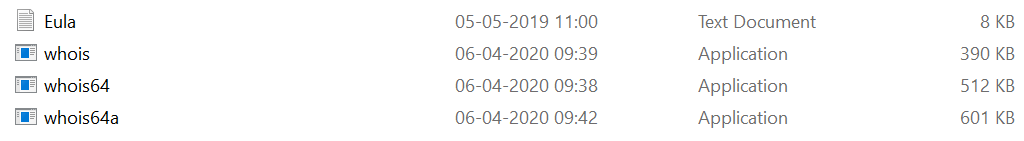
**Purpose:**  
Retrieves registration information about domain names or IP addresses.

**How it Works:**  
Queries public WHOIS databases to display domain ownership and contact details.

**Use in Debugging:**

* Investigates suspicious IPs or websites
* Helps resolve network access or DNS issues
* Useful in analyzing spam, phishing, or cyber threats

(Screenshot)



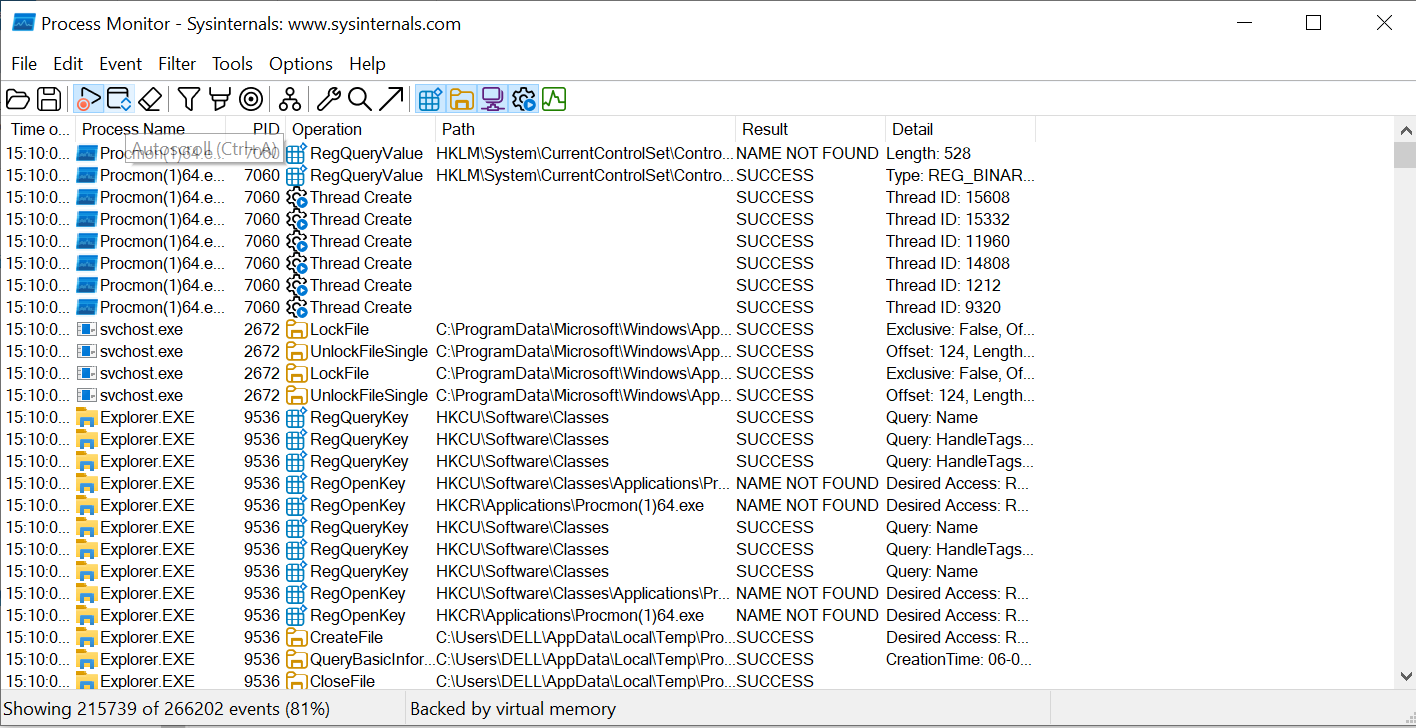
**9. Process Monitor**

**Purpose:**  
Monitors and logs file system, registry, and process/thread activity in real-time.

**How it Works:**  
Captures low-level activity on the system and shows detailed information about every event.

**Use in Debugging:**

* Troubleshoots software installation and launch failures
* Finds missing files or access denied errors
* Detects unusual behavior or unauthorized changes

(Screenshot)

**Topic(ii): Steps to create for Microsoft Intune portal**

**1. Review Supported Configurations**

Before using Intune, it’s important to check if the devices, operating systems, and web browsers are supported. Network requirements and proxy settings should also be reviewed.

**2. Sign Up or Sign In to Intune**

If the organization already uses Microsoft 365 or has a work/school account, Intune can be added to that subscription. Otherwise, a new account can be created for Intune access.

**3. Configure a Custom Domain (Optional)**

By default, Intune gives a domain ending with .onmicrosoft.com. A custom domain like company.com can be set up for a more professional look. This step is optional during trial.

**4. Add Users**

Users must be added so they can access Intune. This can be done manually or by syncing with Active Directory. Each user must have a Microsoft Entra ID account.

**5. Create Groups**

Groups help organize users or devices based on department, location, or job roles. This makes it easier to apply apps, policies, or settings to many users at once.

**6. Assign Licenses**

Every user needs an Intune license to enroll their devices. Licenses can be assigned after adding users, and unlicensed admins can also be allowed if needed.

**7. Manage Roles and Admin Access**

Using Role-Based Access Control (RBAC), admin roles can be assigned based on job responsibilities. Custom roles can also be created to give specific permissions.

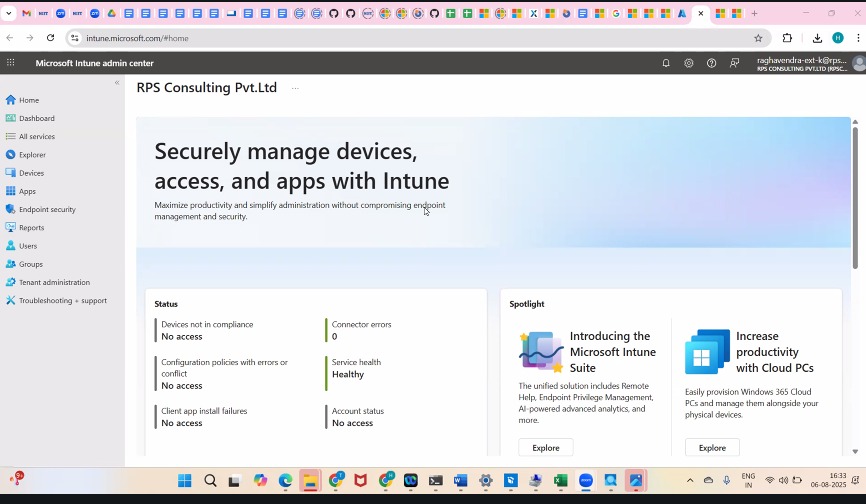
**8. Set the MDM Authority**

The Mobile Device Management (MDM) authority must be set before devices can be enrolled. Intune usually sets this automatically, but it can be changed if needed.

**9. Customize the Company Portal**

The Company Portal is where users install apps and manage their devices. It can be customized with the organization’s logo, contact info, and help details for a better user experience.

**Sample screenshot of created account for Microsoft Intune portal**

****