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, 2, 3, 4, 5, 6, 7]

Here's a more detailed look at each tool:

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, 2]

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. [3, 7, 8, 8, 9, 10, 11, 12, 13, 14, 15, 16]

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. [17, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]

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. [17, 17, 27, 28]

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. [3, 29, 29, 30, 31, 32, 33, 34]

6. Sysmon:

- **Purpose:** A Windows system service and driver that monitors and logs system activity. [7, 7]
- **How it works:** Provides detailed information about process creations, network connections, and file access changes. [6, 6, 7, 7]
- **Usage:** Essential for security monitoring, intrusion detection, and forensic analysis. [7, 7, 35, 36]

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. [37, 37, 38, 39, 40, 41, 42, 43]