

PROCESS EXPLORER, ERRORS IN REPACKAGER, WHOIS TOOL AND SYSMON TOOL

GROUP C

Process Explorer

- Process Explorer is a powerful system monitoring and troubleshooting tool, developed by Mark Russinovich as part of the Sysinternals Suite.
- It acts as an advanced replacement for Windows Task Manager, providing in-depth details about running processes, resource usage, and system activity in real-time.

Key Features





- Real-time process monitoring – Track CPU, memory, GPU usage instantly.
- Tree view of processes – Shows parent–child process relationships.
- Detailed process properties – View threads, priorities, environment variables.
- DLL & handle viewing – Identify files, libraries, and resources in use
- Search capability – Find which process is using a specific file or handle.

Uses of process explorer in application packaging

- Identity background process
- Detect locked files during installation
- Check parent process of installers
- Verify digital signature
- Monitor resource usage during installation
- Check loaded DLL's and dependencies

Task Manager vs Process Explorer

Task Manager vs Process Explorer

Feature	Task Manager	Process Explorer
Purpose	Basic process & performance monitoring	Advanced, detailed process analysis
Details Shown	Limited info (CPU, Memory, Disk, Network)	Very detailed (open files, registry keys, DLLs, parent/child process tree)
Process Tree	Flat list (Windows 10/11 shows limited hierarchy)	Full parent-child hierarchy view
File Handles / Registry Keys	 Not shown	 Can search and view all handles/keys a process is using
Digital Signature Verification	 No	 Yes, checks if process is verified and from trusted publisher
Process Kill Options	Kill	Kill, Kill Tree, Suspend
Portable?	Built-in to Windows	Portable app, runs without install
Best For	Everyday monitoring, ending unresponsive apps	Deep troubleshooting, malware detection, application packaging analysis

Errors in Repackager – Application Packaging

- **Common Errors:**

- Missing files or locked files
- Missing registry keys (HKCU)
- Background process interference
- Wrong snapshot timing
- Missing dependencies (.NET, Java)

Errors in Repackager – Application Packaging

- **Fixes:**

- Always use a clean virtual machine
- Disable antivirus and Windows updates
- Take snapshot immediately after clean boot
- Install with correct user account
- Package dependencies separately.

Errors in Repackager – Application Packaging

- **Best Practices:**

- Maintain standard packaging checklist
- Test MSI in different environments
- Document any manual changes done post-capture
- Keep version control of your ISM/MSI files

- **Conclusion:**

- Errors are common but preventable
- Correct process = stable MSI output

What is WHOIS?

- A protocol used to query databases storing domain registration and IP allocation details.
- Acts like a public phone book for the internet.
- Provides ownership and technical information about domains and IP addresses.

Information from WHOIS

- Domain registrar, registrant name, and organization.
- Contact details (email, phone, address - sometimes hidden).
- Domain creation, expiration, and update dates.
- Nameservers used by the domain.
- For IP addresses: owner organization, location, IP range, and abuse contacts.

How to Use WHOIS Tools

- Command-line: `whois example.com` (Linux/macOS).
- Online tools: ICANN WHOIS, Whois.com, DomainTools.
- Integrated in security/network analysis software.
- Helps in domain research, security analysis, and troubleshooting.

Real-World Applications

- Website research and contacting owners.
- Cybersecurity investigations to track malicious domains.
- Domain acquisition and expiration tracking.
- Legal and compliance investigations.
- Verifying legitimacy of domains in network or app analysis.

Limitations of WHOIS

- Inconsistent Data Formats
- Unverified or Fake Information
- Delayed or Outdated Information
- Legal or Access Restrictions

Symon Tool Overview

- Symon is a no-code data analytics platform developed by Varicent.
- It is used to prepare, analyze, and visualize data quickly.
- Works with drag-and-drop tools instead of coding.

- **Key Features**

- Data Preparation – Clean, filter, and organize raw data.
- Data Analysis – Discover trends, patterns, and insights.
- Visualization – Create professional charts and dashboards.
- No Coding Required – Simple, user-friendly interface.

How It Works

- Upload Data from Excel, CSV, or databases.
- Process Data using tools like Clean, Combine, Group, Calculate, and Learn.
- Generate Visuals such as bar charts, line graphs, or tables.
- Export visuals for PPT, PDF, or dashboards..

Benefits

- Speed – Process large datasets quickly.
- Quality – Create professional-grade visuals.
- Intelligence – Get AI-powered insights.
- Simplicity – Designed for non-technical users.