# Windows Sysinternals Toolkit Walkthrough

**Date:** June 12th 2025
**Category:** Windows 11 Projects

---

## Tools Installed

Installed via Chocolatey:

```
choco install sysinternals -y --ignore-checksums
```

Install location:
`C:\ProgramData\chocolatey\lib\sysinternals\tools`

Command-line access enabled for:

```
procexp
autoruns
procmon
tcpview
```

Official Microsoft page:
https://learn.microsoft.com/sysinternals

---

# 1. Process Explorer

- **Launched** with `procexp`
- Enabled **VirusTotal integration**:
  - `Options > VirusTotal.com > Check VirusTotal.com`
- Investigated:

    - `PowerPanel Personal.exe` (flagged 1/72 — confirmed false positive)
- Verified digital signatures via:
    - Right-click process → Properties → `Verified:` field
- Used **Lower Pane View** for:
    - **DLLs** and **Handle usage**

---

# 2. Autoruns

- Launched with `autoruns`
- Configured:
    - `Options > Hide Microsoft Entries`
    - `Options > Scan Options > Submit Unknown Images`
- Focused on reviewing:
    - **Logon**, **Scheduled Tasks**, **Drivers**, **Services**
- Checked VirusTotal flags and verified digital signatures
- Disabled or marked suspicious unsigned entries

---

# 3. Process Monitor (Procmon)

- Launched with `procmon`
- Paused default capture: `Ctrl + E`
- Applied filters for:
    - Specific processes (e.g., `notepad.exe`)
    - Registry and file system operations
- Resumed capture for real-time inspection
- Saved capture via `File > Save > .PML`

---

# 4. TCPView – Active Network Monitoring

## Tool Summary:

- Launched with: `tcpview`

- Displays:
  - All active TCP/UDP connections
  - Local and remote addresses
  - Process ownership
  - Packet counts and traffic volume

# Observations:

| Process | Remote Host/Service | Notes |
|---|---|---|
| `firefox.exe` | `google.com` (via `142.250.x.x`) | Normal browser activity |
| `steam.exe` | `valve.net`, `akamai.net`, `u2-puls.tech` | Related to Steam/Valve CDN |
| `PowerPanel` | Internal `kubernetes.docker.internal` | Local/VM bridge — normal |
| `syncthing.exe` | `u2-puls.tech` / Docker bridges | Syncthing sync traffic — expected |

---

# WHOIS Lookup: `akamaitechnologies.com`

TCPView revealed connections to domains like `akamaistream.net`, a known CDN subdomain.

WHOIS record for `akamaitechnologies.com`:

| Field | Value |
|---|---|
| **Domain** | akamaitechnologies.com |
| **Registrar** | MarkMonitor Inc. |
| **Created** | August 18, 1998 |
| **Updated** | July 16, 2024 |
| **Expires** | August 17, 2025 |
| **DNS** | `AX0.AKAMAISTREAM.NET`, `NS2-32.AKAMAISTREAM.NET`, etc. |
| **Status** | Protected (delete/transfer/update disabled) |
| **Registrar Abuse** | abusecomplaints@markmonitor.com |
| **Official Whois** | https://www.icann.org/wicf/ |

Akamai Official Site: https://www.akamai.com

# Conclusion:

- Akamai is a globally trusted **CDN and security platform** used by Steam, Microsoft, Apple, and others.
- Connections to `akamaistream.net` and related domains in TCPView are **expected** and **not malicious**.
- WHOIS verified the legitimacy and ownership of the Akamai domains.

---

# 5. PowerShell Signature Verification

Command used:

```
Get-AuthenticodeSignature "C:\Path\To\File.exe"
```

Example:

```
Get-AuthenticodeSignature "C:\ProgramData\chocolatey\lib\sysinternals\tools\procexp.exe"
```

Reviewed:

- `Status` field = `Valid`
- `SignerCertificate.Subject` = Trusted vendor (e.g., Microsoft Corporation)

There are tons of other tools for system analysis as well.

---

Revision #1
Created 12 June 2025 22:01:49 by Nate Nash
Updated 28 December 2025 20:31:02 by Nate Nash