Day 11 Assignment

Step By Sep Process of Application Compatibility Toolkit (ACT):

Step 1: Install the ACT

1. **Download ACT**:
   - ACT is part of the **Windows Assessment and Deployment Kit (ADK)**.
   - Download from the official Microsoft website (Windows ADK).
2. **Install ACT Components**:
   - During ADK installation, choose to install:
     - Application Compatibility Manager
     - Compatibility Administrator
     - ACT Log Processing Service (optional)
     - SQL Server Express (or use an existing SQL Server)

Step 2: Set Up the ACT Database

1. **Launch Application Compatibility Manager**.
2. **Configure the Database**:

Step 3: Collect Inventory Data

1. **Deploy the ACT Data Collection Package**:
   - Create a **Data Collector Package (DCP)** from the Application Compatibility Manager.
   - Configure it to:
     - Collect inventory data
     - Monitor application usage (optional)
   - Deploy the DCP to client machines (via Group Policy, SCCM, etc.).
2. **Run DCP on Client Machines**:
   - Clients collect data (applications, system configurations, etc.).
   - The data is uploaded back to the ACT database.

Step 4: Analyze Inventory Data

1. **View Inventory in Application Compatibility Manager**:
   - After DCP results are uploaded, view them in the Manager.
2. **Check Compatibility Evaluations**:
   - ACT will match known apps against Microsoft's compatibility database.

Step 5: Mitigate Compatibility Issues

1. **Use Compatibility Administrator**:
   - Launch **Compatibility Administrator** tool from ACT.
   - Create **Shims** (compatibility fixes) for problem applications.

- Common fixes: Version Lie, Admin Privileges, File Redirects, etc.

2. **Test the Fixes Locally**:
   - Apply the shim to the application locally.
   - Validate that it runs as expected on the target OS.

Step 6: Deploy Compatibility Fixes

1. **Package and Deploy Shims**:
   - Export the compatibility fix database as an .sdb file.

Step 7: Monitor and Update

1. **Monitor Application Behavior**:
   - Continue collecting data using updated DCPs.
   - Address new issues as they arise.
2. **Update Shims and ACT Database as Needed**:
   - Add new fixes
   - Retire obsolete ones
   - Update inventory information

TroubleShooting Tools:

1. **Event Viewer**

Purpose: Event Viewer logs system, application, and security events. It helps identify crashes, errors, and system warnings.Use Details for Troubleshooting,Filter and Analyze **Error,Warning,Critical**

2.Process Monitor (ProcMon)

Purpose:
Process Monitor (from Sysinternals) captures real-time file system, registry, and process/thread activity. Great for troubleshooting installation issues, file access failures, registry issues, etc.

3. **Dependency Walker (depends.exe)**

Purpose:
Dependency Walker identifies all DLLs an executable depends on and flags missing or mismatched DLLs — useful for diagnosing app crashes or load errors.

Step 1: Download and Install.

Step 2: Open the Target Application.

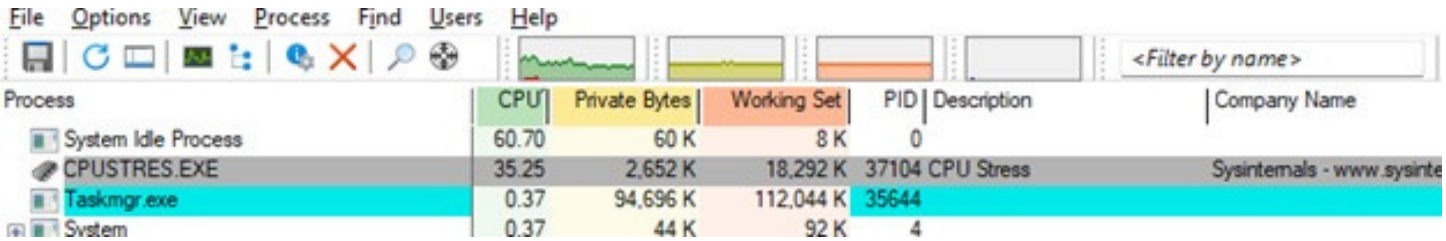
Step 3: Analyze Results.

Step 4: Fix Issues.

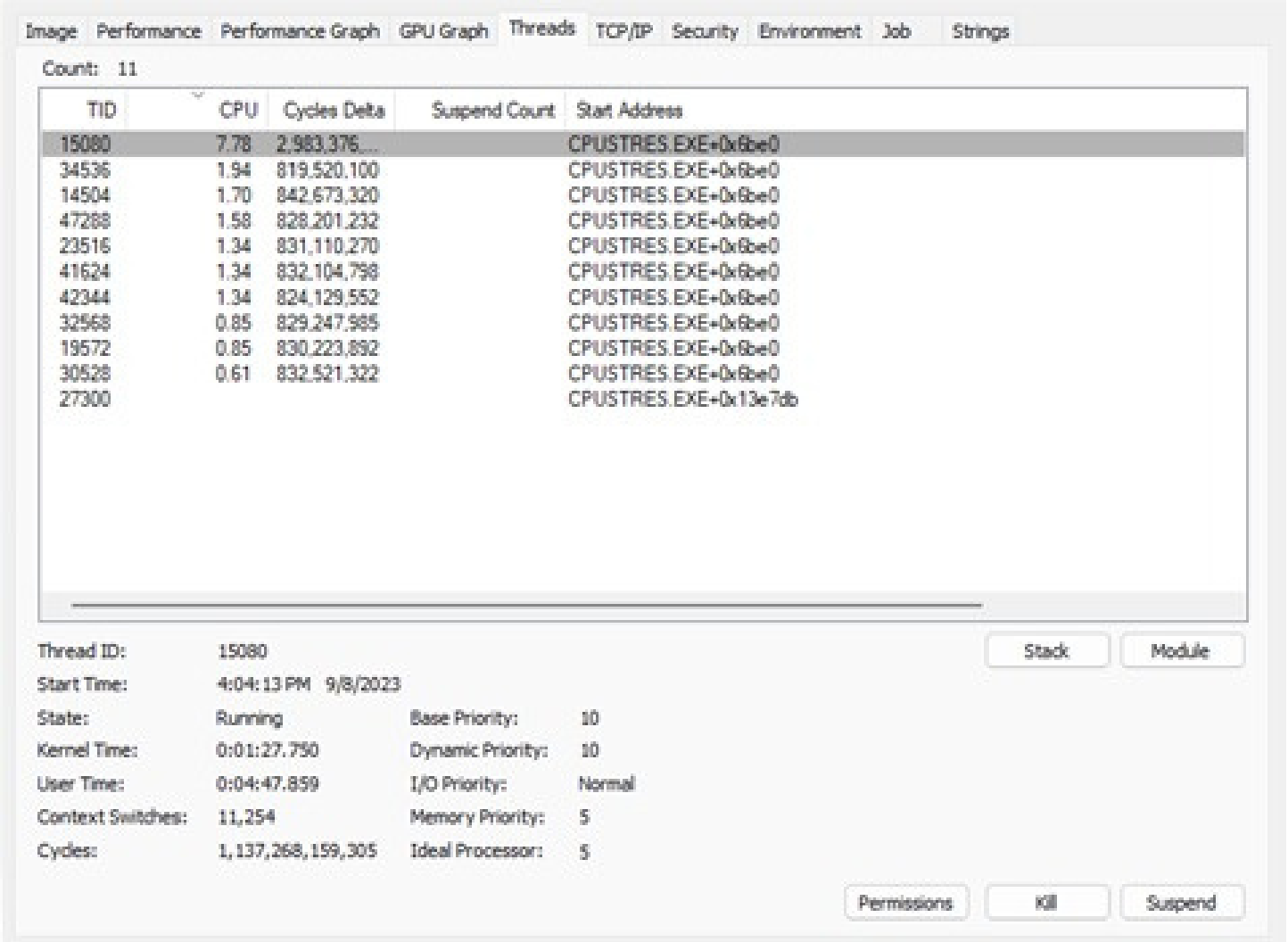
Tool	Use Case	Key Strength
Event Viewer	System/app crashes, errors	Historical log data
Process Monitor	Real-time monitoring	File, registry, process tracking
Dependency Walker	App load/launch failures	DLL/module analysis

Troubleshooting Example:

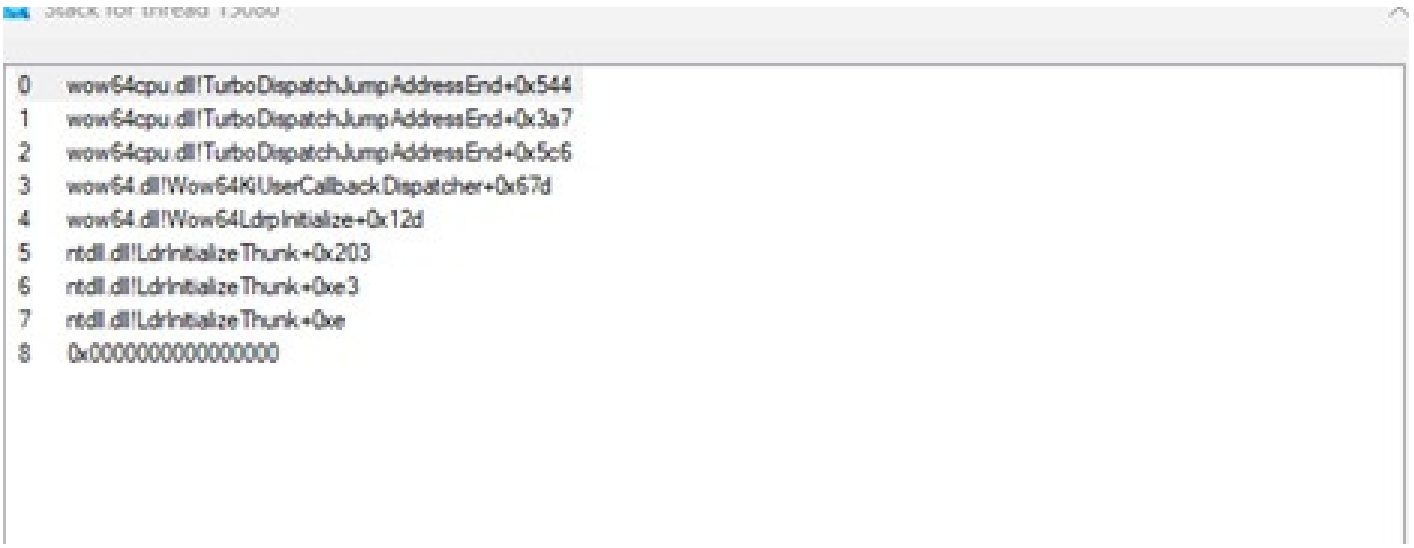
When you use CpuStres to simulate CPU activity by running several threads, you can see that the **CPUSTRES.EXE** process in Process Explorer consumes the highest CPU. For example:



Double-click **CPUSTRES.EXE** (or right-click **CPUSTRES.EXE** and select **Properties**) and go to the **Threads** tab.



You can see that many threads are consuming the CPU, among which TID 15080 consumes the most. There are many more details. When you select the most consuming thread, you get the call stack information:



The call stack information isn't updated automatically. To get the latest stack informat
select Refresh. However, this refresh has a minimum interval of one second. To see wh
happening in the thread each second, you can use Windows Performance Recorder (WPR) or
Windows Performance Analyzer (WPA).