- **Best way to track CPU and ram utilization on device**
  Windows Task manager for basic, and ProcMon for more in-depth analyzing of RAM utilization.
- Focus on best way to track RAM and CPU utilization
  - Explain how microsoft/windows performance monitoring tool works (reports)
  - Look for additional tools
  - The best tools are the ones that are already built into windows
    - Process Explorer both verifies signatures and works hand in hand with virustotal so thats two things i couldve done
    - ProcMon doesnt seem to be the best to use for finding malware

- **Performance Monitoring tool built into windows**
  - Set up baseline reports and be able to tell how much utilization each process uses on average, to identify baseline
  - This will allow you to identify any weird things going on
    - DONE

- **Google cloud free tier for Windows 10/11**
  - Got VM working - windows 10 - didnt do much on it
    - Should install some sort of malware or something on it (how)

- **SideLoader Github Project (Cloned on VSCode)**
- **https://github.com/XForceIR/SideLoadHunter**
- **(could not run, its not digitally signed)??**
  - SideLoader is a PowerShell script designed to detect DLL sideloading by analyzing executables and DLLs within user profiles, System32, and SysWow64 directories. The script profiles these files, compares their attributes (file names, hash values, internal names), and checks for DLL sideloading. It also examines program executions for sideloaded executables that are no longer present on the disk. (malware leaves a trace).
  - It does this by using: Get-SideLoadDetect: Identifies executables in userland directories with DLLs that match System32/SysWow64 names but are unsigned by Microsoft.
  - Get-SusShimcache: Analyzes ShimCache entries to detect sideloaded executables that have run from non-standard locations but no longer exist on disk.
  - Get-SusExec & Get-SusDLLs: Profiles the system to find System32 and SysWow64 executables and DLLs that are not in their default locations.

- After analysis, results are exported into CSV files, organized by hostname and date.

How to proceed: (i think)

- Download malware on VM, see how it affects ProcExplorer/ProcMon, take note
  - Compare vs baseline results
- Write script that analyzes and looks for what happens when malware is ran

Screenshot of baseline process explorer