Disassemble Memory File

Memory.DMP used in post-mortem debugging can be processed without "Debugging Tools for Windows", particularly to obtain a call tree for a given function.

UfSymbol.ps1 disassembles once a memory file and stores the output in local directory. A 2nd run uses the `.disassembly` file to parse the functions' body. The root body contains the symbol requested by the user. A dependency graph is built either upstream, representing all the callers of the function, or downstream representing the callees. Care must be taken when specifying `-Depth`: * generic functions have many callers

`$StopDisassembly` is a table of symbols where parsing stops. For example, `KeYieldProcessorEx` calls other functions that are minute.

Sample Output builds the call tree for `nt!KiSystemStartup`.

```
PS > (Measure-Command {
         $Image = 'D:\DataLake\2025-04-28\MEMORY.DMP'
         & '.\UfSymbol.ps1' -Symbol nt!KiSystemStartup -Image $Image -Depth 4 -Down | Out-Default
      }).TotalSeconds
File "D:\DataLake\2025-01-28\MEMORY.DMP" of 1194.36 Mb has been processed in 4570 seconds.
D:\Processing\53c6f2af-38db-4219-9f41-f794c7897f5a\53c6f2af-38db-4219-9f41-f794c7897f5a.disassembly
D:\Processing\53c6f2af-38db-4219-9f41-f794c7897f5a\53c6f2af-38db-4219-9f41-f794c7897f5a.meta
D:\Processing\53c6f2af-38db-4219-9f41-f794c7897f5a\53c6f2af-38db-4219-9f41-f794c7897f5a.retpoline
```

The 1st line gives a heads-up about the disassembly duration:

- a smaller file was processed in 1.26 hours on the same system.

The disassembly is done in parallel using all cores but 1. Once completed, the `.meta` file contains the properties:

- OS and Computer where the BSOD occurred
- Image path and Hash. The hash identifies image duplicates, resulting in a disassembly bypass.
- System where disassembly took place, number of CPUs alloted, CPU model, duration and Image size.
- The default modules used to disassemble the Image:
  - for a `.dmp` file *nt, pci, acpi and hal* functions are disassembled
  - *base name* for all others

The `.retpoline` file is an indirection table for bodies compiled with `/guard:cf`. Wherever `call nt!guard_dispatch_icall` is found, the function pointer is resolved in the memory file and displayed.

Back to `KiSystemStartup` call tree:

- 1302 callees are identified for `-Depth 4`
- Complete disassembly and identification took **5215** seconds on an "Intel(R) Core(TM) i3-7100U CPU @ 2.40GHz" with 3 cpus.
- `nt!atol`, `nt!KeQueryPerformanceCounter` can be part of `$StopDisassembly`.

```
uf nt!KdInitSystem
├──────────────────▷uf nt!KeQueryPerformanceCounter
│                                                 uf nt!HalpTimerGetInternalData
│                                                 uf nt!HalpTimerScaleCounter
│                  uf nt!ExAllocatePool2
│                  uf nt!_security_check_cookie
│                  uf nt!MmGetPagedPoolCommitPointer
├──────────────────▷uf nt!KdRegisterDebuggerDataBlock
 ...
uf nt!PpmUpdatePerformanceFeedback
uf nt!guard_dispatch_icall (nt!_security_cookie
                            nt!HalpOriginalPerformanceCounter
                            nt!HalPrivateDispatchTable+0x1b0=nt!HalpProcessorPrepareForIdle
                            nt!HalPrivateDispatchTable+0x1c0=nt!HalpProcessorResumeFromIdle
                            nt!HalpTimerReferencePage
                            nt!HalPrivateDispatchTable+0x418=nt!HalpLbrResumeRecording
                            nt!HalPrivateDispatchTable+0x2f8=nt!HalpTimerClockStop
                            nt!PopCsConsumption+0x140)
5215.506918
```

Notes

- PowerShell *Core* is required. *Desktop 5.1* is slow.
- `.retpoline` built is not parallelized.
- SVG rendering is not implemented.
- *UfSymbol* is meant for USB migration; the tool can run without internet.
- Removing CR character from the large disassembly can result in *OutOfMemory* exception.

```
PS > $prefix = "https://raw.githubusercontent.com/armaber/scripts/refs/heads/disasm/";
     "functions.ps1", "UfSymbol.ps1" | foreach {
         Invoke-WebRequest $prefix/DisassembleImage/$PSItem -OutFile $PSItem;
      }
```