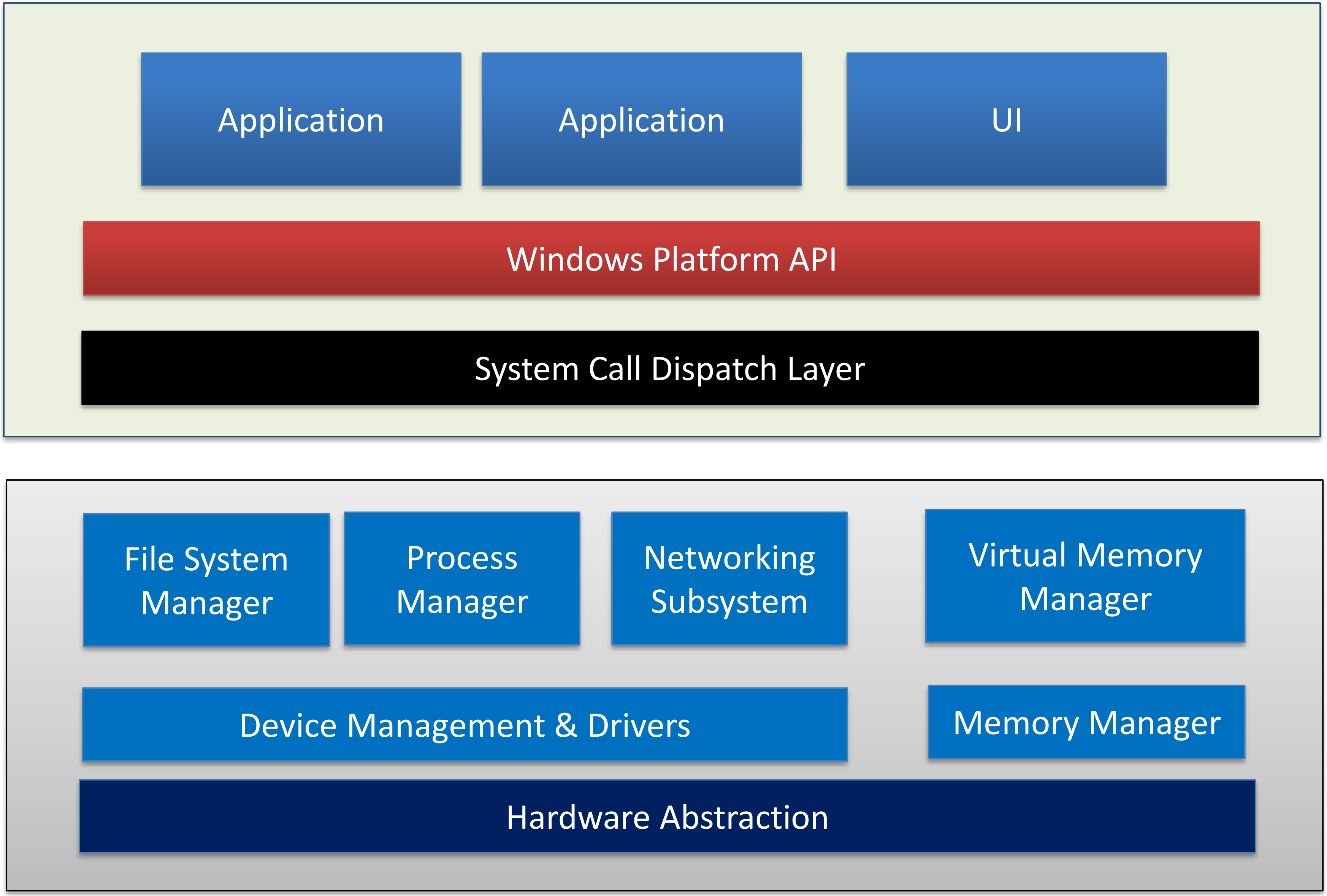
# The Windows Platform

Intro: Win32 Platform and API

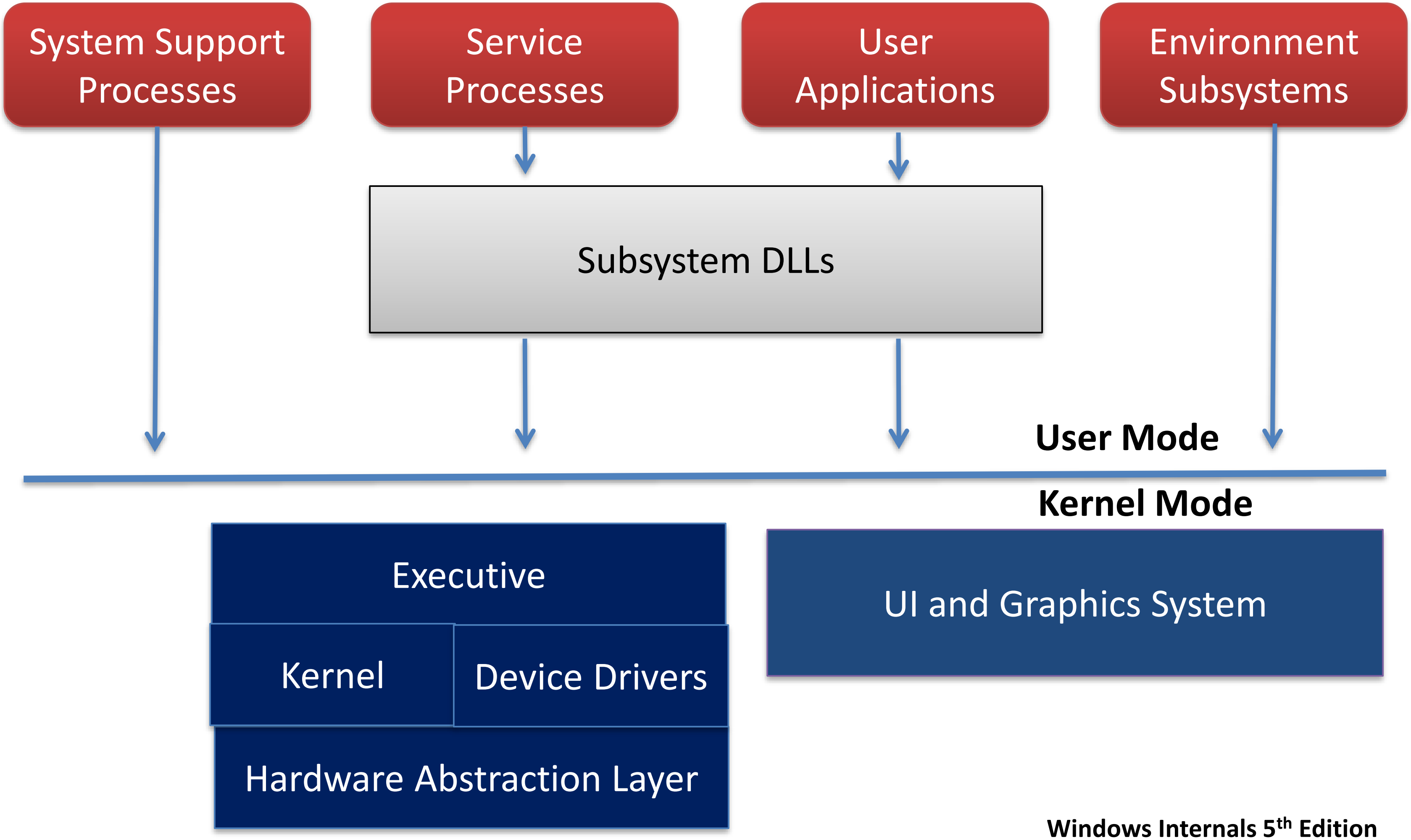
# Agenda

- Introduction to the Win32 Platform
  - Platform Architecture
  - Core Services
  - Programming Model
  - Process and System Initialization
- Introduction to Win32 API
  - System Service Call
  - Core API

# Generic OS Components



# Win32 Platform Architecture


System Support Processes

Service Processes

User Applications

Environment Subsystems

Subsystem DLLs

User Mode

Kernel Mode

Executive

Kernel

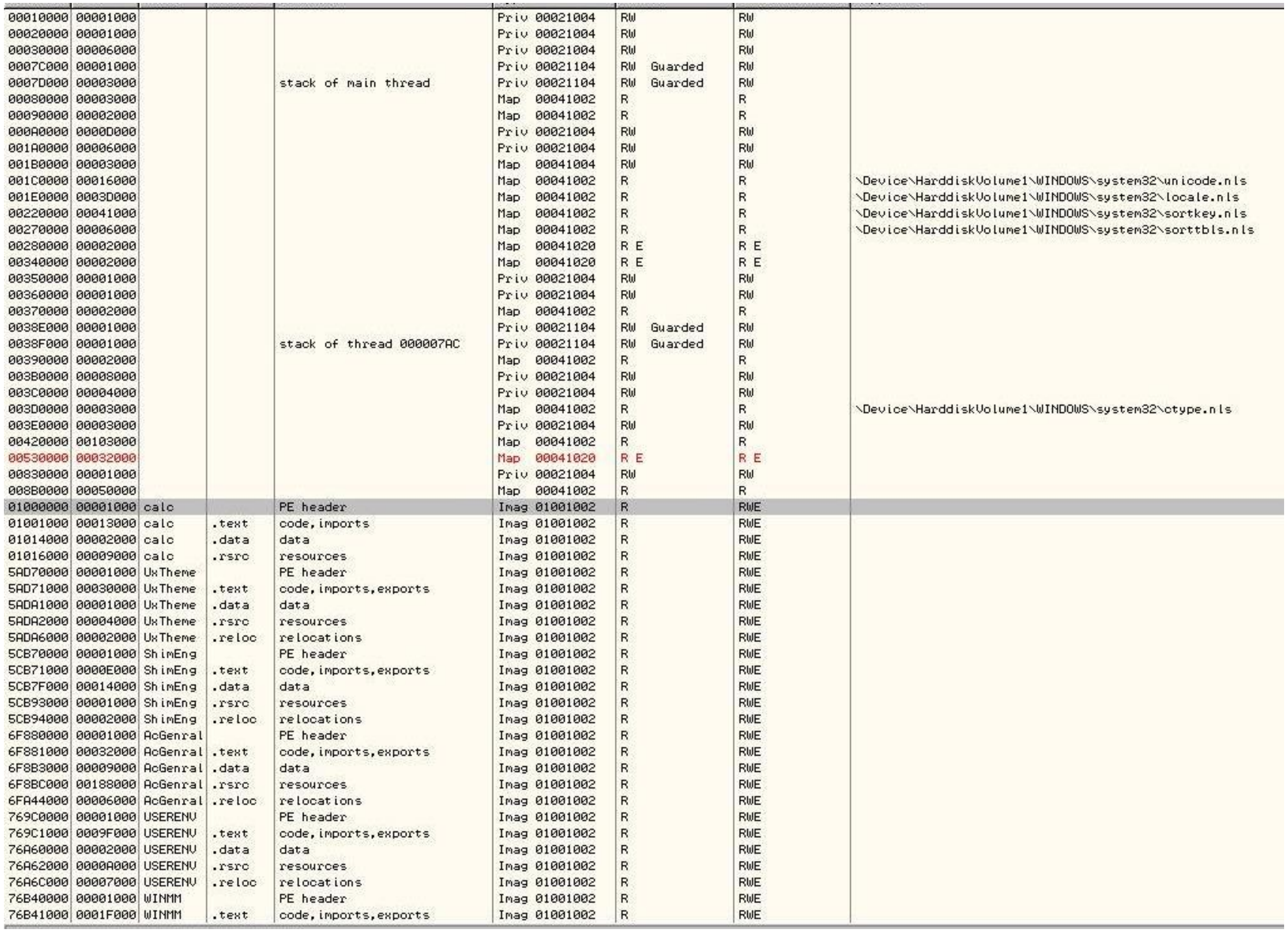
Device Drivers

Hardware Abstraction Layer

UI and Graphics System

**Windows Internals 5th Edition**

# Win32: Process Address Space



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 00010000 | 00001000 | | | | Priv 00021004 | RW | RW | |
| 00020000 | 00001000 | | | | Priv 00021004 | RW | RW | |
| 00030000 | 00006000 | | | | Priv 00021004 | RW | RW | |
| 0007C000 | 00001000 | | | | Priv 00021104 | RW  Guarded | RW | |
| 0007D000 | 00003000 | | | stack of main thread | Priv 00021104 | RW  Guarded | RW | |
| 00080000 | 00003000 | | | | Map  00041002 | R | R | |
| 00090000 | 00002000 | | | | Map  00041002 | R | R | |
| 000A0000 | 0000D000 | | | | Priv 00021004 | RW | RW | |
| 001A0000 | 00006000 | | | | Priv 00021004 | RW | RW | |
| 001B0000 | 00003000 | | | | Map  00041004 | RW | RW | |
| 001C0000 | 00016000 | | | | Map  00041002 | R | R | \Device\HarddiskVolume1\WINDOWS\system32\unicode.nls |
| 001E0000 | 0003D000 | | | | Map  00041002 | R | R | \Device\HarddiskVolume1\WINDOWS\system32\locale.nls |
| 00220000 | 00041000 | | | | Map  00041002 | R | R | \Device\HarddiskVolume1\WINDOWS\system32\sortkey.nls |
| 00270000 | 00006000 | | | | Map  00041002 | R | R | \Device\HarddiskVolume1\WINDOWS\system32\sorttbls.nls |
| 00280000 | 00002000 | | | | Map  00041020 | R E | R E | |
| 00340000 | 00002000 | | | | Map  00041020 | R E | R E | |
| 00350000 | 00001000 | | | | Priv 00021004 | RW | RW | |
| 00360000 | 00001000 | | | | Priv 00021004 | RW | RW | |
| 00370000 | 00002000 | | | | Map  00041002 | R | R | |
| 0038E000 | 00001000 | | | | Priv 00021104 | RW  Guarded | RW | |
| 0038F000 | 00001000 | | | stack of thread 000007AC | Priv 00021104 | RW  Guarded | RW | |
| 00390000 | 00002000 | | | | Map  00041002 | R | R | |
| 003B0000 | 00008000 | | | | Priv 00021004 | RW | RW | |
| 003C0000 | 00004000 | | | | Priv 00021004 | RW | RW | |
| 003D0000 | 00003000 | | | | Map  00041002 | R | R | \Device\HarddiskVolume1\WINDOWS\system32\ctype.nls |
| 003E0000 | 00003000 | | | | Priv 00021004 | RW | RW | |
| 00420000 | 00103000 | | | | Map  00041002 | R | R | |
| 00530000 | 00032000 | | | | Map  00041020 | R E | R E | |
| 00830000 | 00001000 | | | | Priv 00021004 | RW | RW | |
| 008B0000 | 00050000 | | | | Map  00041002 | R | R | |
| 01000000 | 00001000 | calc | | PE header | Imag 01001002 | R | RWE | |
| 01001000 | 00013000 | calc | .text | code,imports | Imag 01001002 | R | RWE | |
| 01014000 | 00002000 | calc | .data | data | Imag 01001002 | R | RWE | |
| 01016000 | 00009000 | calc | .rsrc | resources | Imag 01001002 | R | RWE | |
| 5AD70000 | 00001000 | UxTheme | | PE header | Imag 01001002 | R | RWE | |
| 5AD71000 | 00030000 | UxTheme | .text | code,imports,exports | Imag 01001002 | R | RWE | |
| 5ADA1000 | 00001000 | UxTheme | .data | data | Imag 01001002 | R | RWE | |
| 5ADA2000 | 00004000 | UxTheme | .rsrc | resources | Imag 01001002 | R | RWE | |
| 5ADA6000 | 00002000 | UxTheme | .reloc | relocations | Imag 01001002 | R | RWE | |
| 5CB70000 | 00001000 | ShimEng | | PE header | Imag 01001002 | R | RWE | |
| 5CB71000 | 0000E000 | ShimEng | .text | code,imports,exports | Imag 01001002 | R | RWE | |
| 5CB7F000 | 00014000 | ShimEng | .data | data | Imag 01001002 | R | RWE | |
| 5CB93000 | 00001000 | ShimEng | .rsrc | resources | Imag 01001002 | R | RWE | |
| 5CB94000 | 00002000 | ShimEng | .reloc | relocations | Imag 01001002 | R | RWE | |
| 6F880000 | 00001000 | AcGenral | | PE header | Imag 01001002 | R | RWE | |
| 6F881000 | 00032000 | AcGenral | .text | code,imports,exports | Imag 01001002 | R | RWE | |
| 6F8B3000 | 00009000 | AcGenral | .data | data | Imag 01001002 | R | RWE | |
| 6F8BC000 | 00188000 | AcGenral | .rsrc | resources | Imag 01001002 | R | RWE | |
| 6FA44000 | 00006000 | AcGenral | .reloc | relocations | Imag 01001002 | R | RWE | |
| 769C0000 | 00001000 | USERENV | | PE header | Imag 01001002 | R | RWE | |
| 769C1000 | 0009F000 | USERENV | .text | code,imports,exports | Imag 01001002 | R | RWE | |
| 76A60000 | 00002000 | USERENV | .data | data | Imag 01001002 | R | RWE | |
| 76A62000 | 0000A000 | USERENV | .rsrc | resources | Imag 01001002 | R | RWE | |
| 76A6C000 | 00007000 | USERENV | .reloc | relocations | Imag 01001002 | R | RWE | |
| 76B40000 | 00001000 | WINMM | | PE header | Imag 01001002 | R | RWE | |
| 76B41000 | 0001F000 | WINMM | .text | code,imports,exports | Imag 01001002 | R | RWE | |

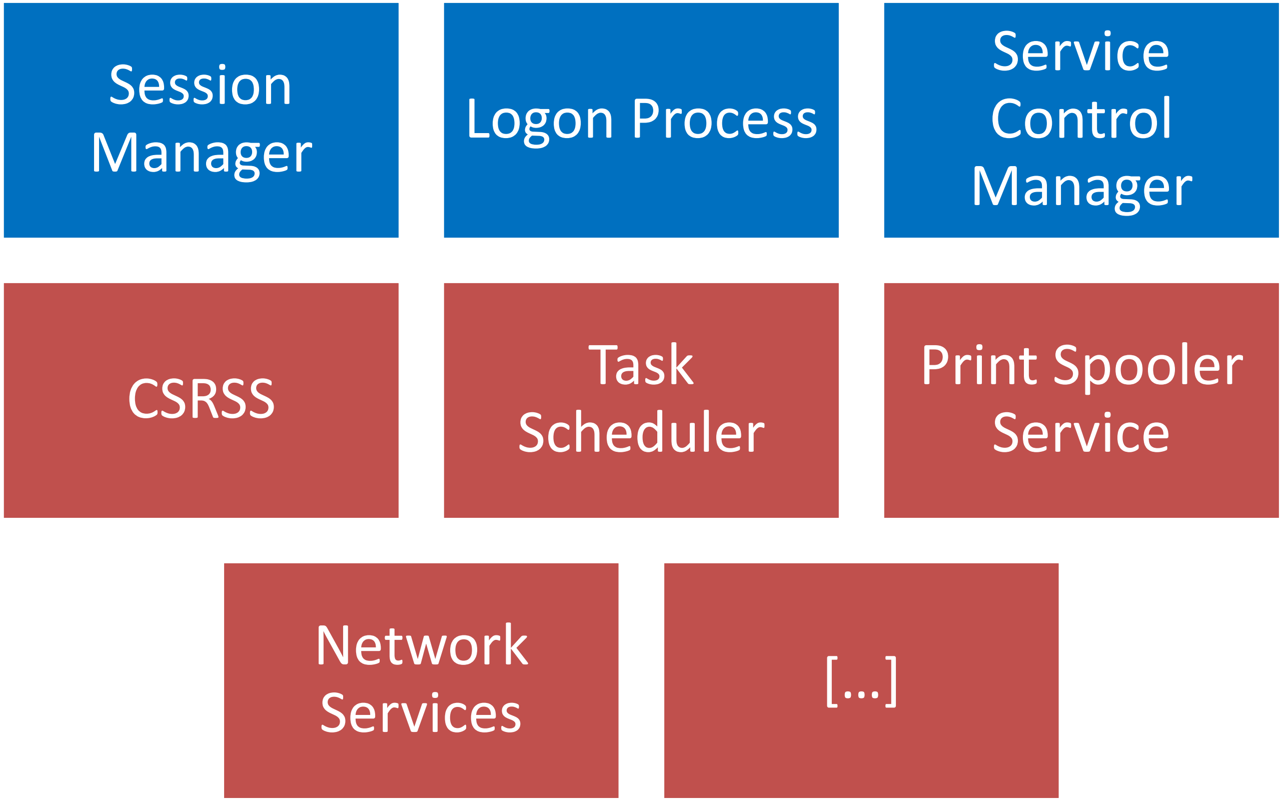
**calc.exe on Windows XP SP2**

# Win32: Core System Components

| Filename | Component |
|---|---|
| Ntoskrnl.exe | Executive and Kernel |
| Ntkrnlpa.exe | Executive and Kernel with PAE Support (32 bit systems only) |
| Hal.dll | Hardware Abstraction Layer |
| Win32k.sys | Kernel Mode part of Windows Sub-system |
| Ntdll.dll | System Utilities and System Service Dispatcher Stubs |
| Kernel32.dll, Advapi32.dll, User32.dll, Gdi32.dll | Core Windows Subsystem DLLs |

**Windows Internals 5th Edition**

# Win32: Core Services



Session Manager

Logon Process

Service Control Manager

CSRSS

Task Scheduler

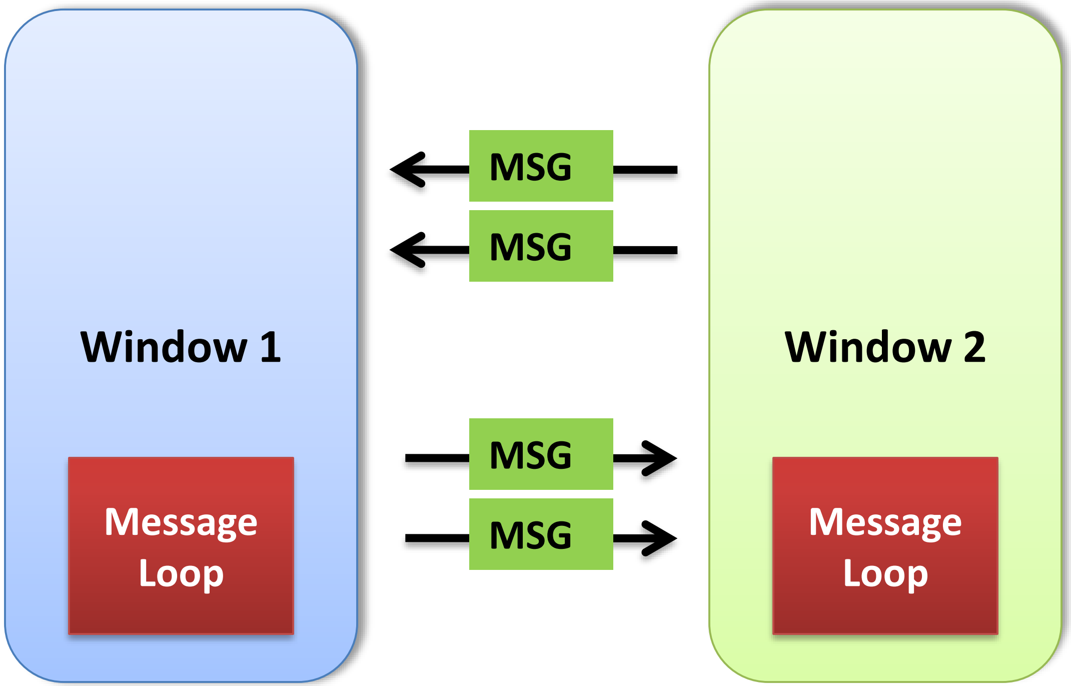
Print Spooler Service

Network Services

[…]

# The Win32 Programming Model

## The Message Loop Architecture

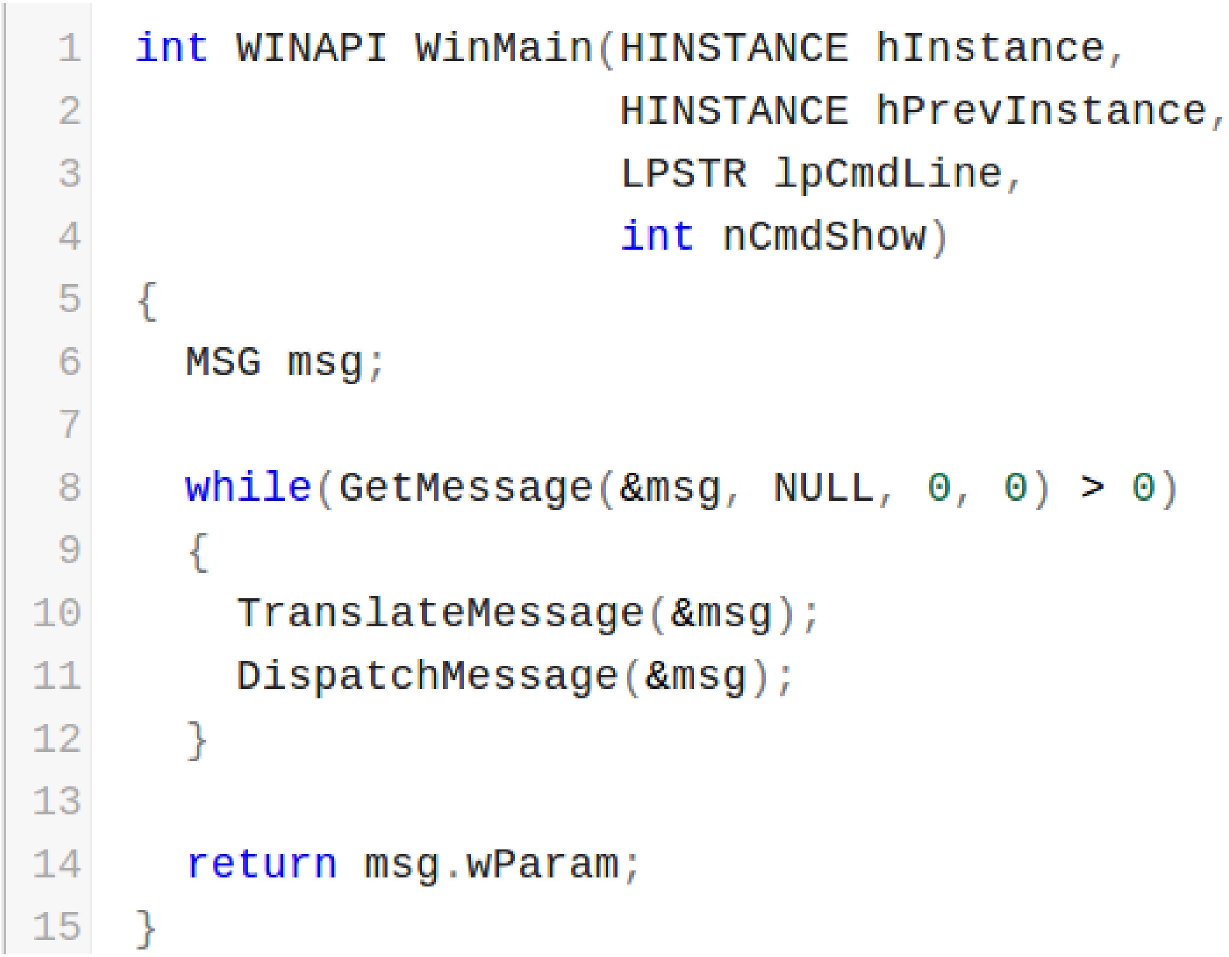


| MSG | |
|---|---|
| **HWND** | hw |
| **UINT** | message |
| **WPARAM** | wParam |
| **LPARAM** | lParam |
| **DWORD** | time |
| **POINT** | pt |

| | | |
|---|---|---|
| **WM_QUIT** | **WM_DESTROY** | **WM_SETTEXT** |
| **WM_INPUT** | **WM_CREATE** | **WM_GETTEXT** |

http://wiki.winehq.org/List_Of_Windows_Messages

# The MSG Loop

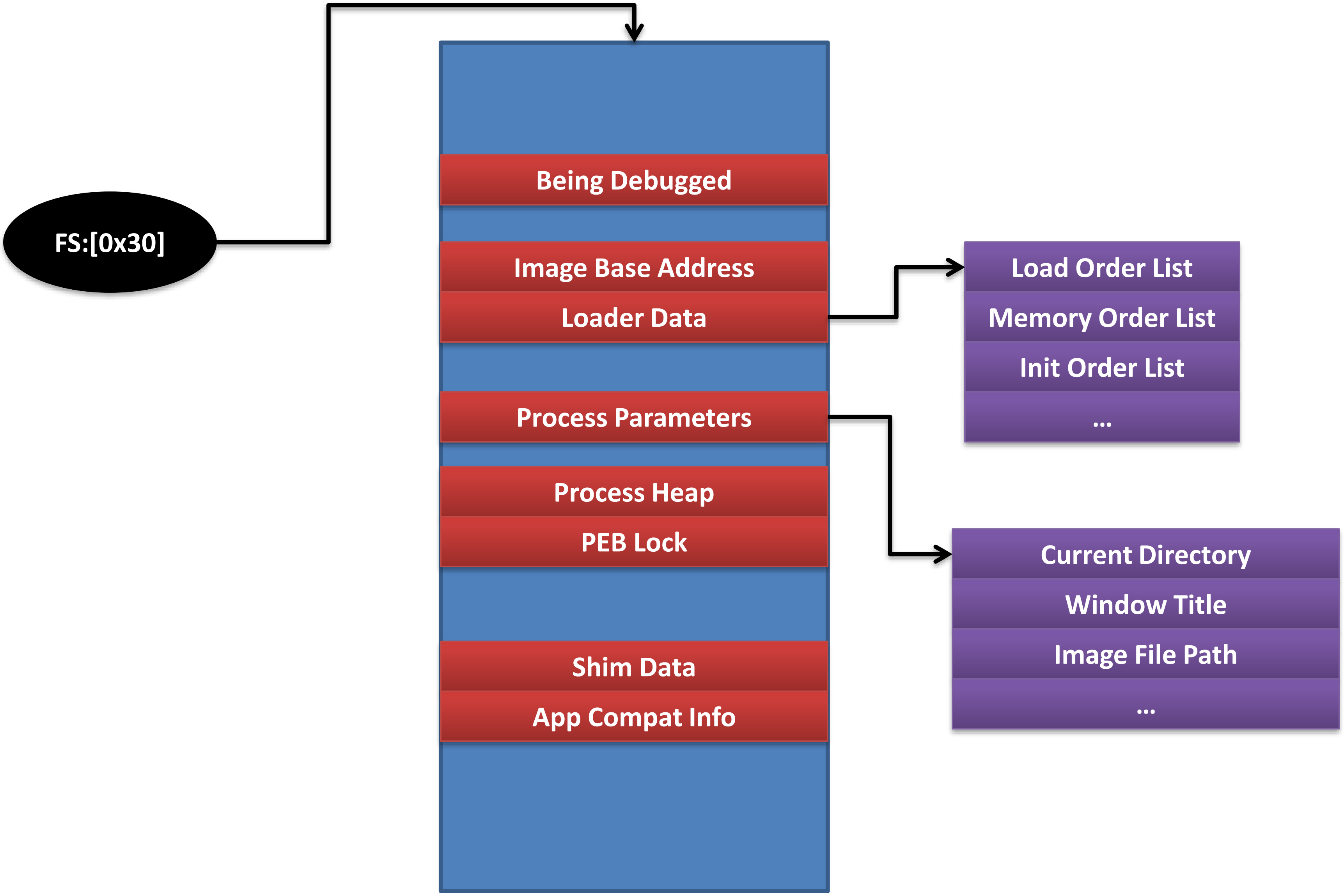


```
int WINAPI WinMain(HINSTANCE hInstance,
                   HINSTANCE hPrevInstance,
                   LPSTR lpCmdLine,
                   int nCmdShow)
{
  MSG msg;

  while(GetMessage(&msg, NULL, 0, 0) > 0)
  {
    TranslateMessage(&msg);
    DispatchMessage(&msg);
  }

  return msg.wParam;
}
```

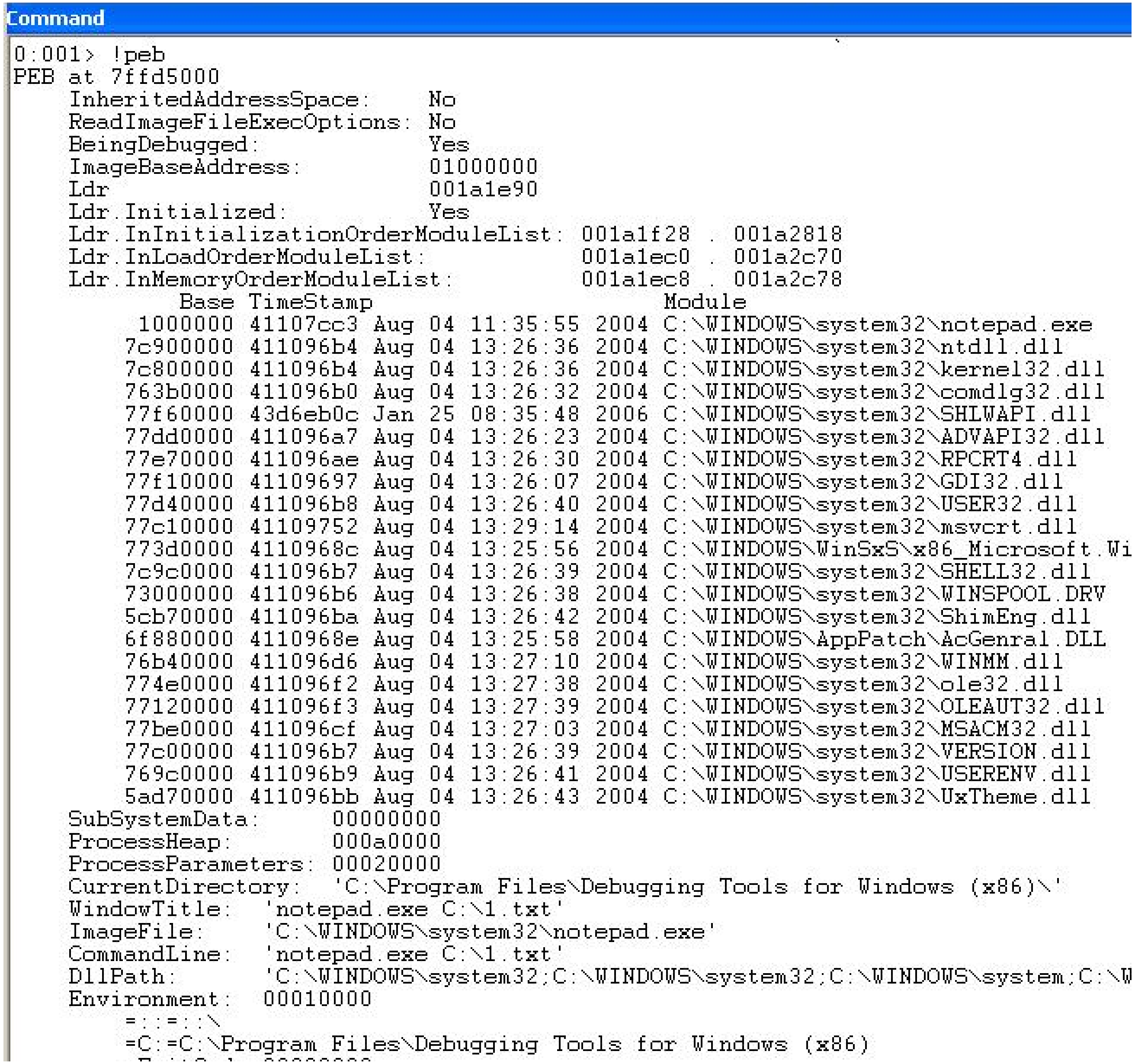
# The Process Environment Block



https://raw.github.com/abhisek/Pe-Loader-Sample/master/src/PEB.h

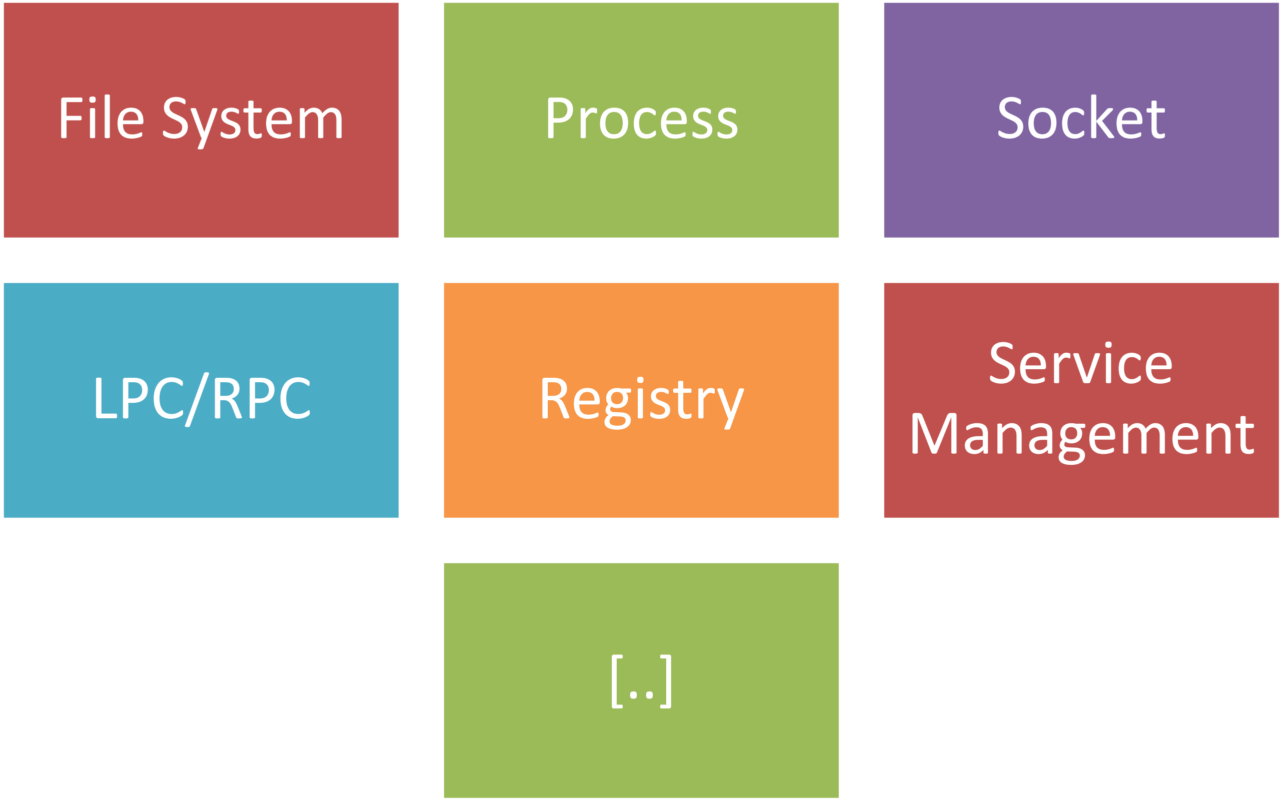
# PEB

## using WinDBG



```
0:001> !peb
PEB at 7ffd5000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            Yes
    ImageBaseAddress:         01000000
    Ldr                       001a1e90
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001a1f28 . 001a2818
    Ldr.InLoadOrderModuleList:           001a1ec0 . 001a2c70
    Ldr.InMemoryOrderModuleList:         001a1ec8 . 001a2c78
            Base TimeStamp                     Module
         1000000 41107cc3 Aug 04 11:35:55 2004 C:\WINDOWS\system32\notepad.exe
        7c900000 411096b4 Aug 04 13:26:36 2004 C:\WINDOWS\system32\ntdll.dll
        7c800000 411096b4 Aug 04 13:26:36 2004 C:\WINDOWS\system32\kernel32.dll
        763b0000 411096b0 Aug 04 13:26:32 2004 C:\WINDOWS\system32\comdlg32.dll
        77f60000 43d6eb0c Jan 25 08:35:48 2006 C:\WINDOWS\system32\SHLWAPI.dll
        77dd0000 411096a7 Aug 04 13:26:23 2004 C:\WINDOWS\system32\ADVAPI32.dll
        77e70000 411096ae Aug 04 13:26:30 2004 C:\WINDOWS\system32\RPCRT4.dll
        77f10000 41109697 Aug 04 13:26:07 2004 C:\WINDOWS\system32\GDI32.dll
        77d40000 411096b8 Aug 04 13:26:40 2004 C:\WINDOWS\system32\USER32.dll
        77c10000 41109752 Aug 04 13:29:14 2004 C:\WINDOWS\system32\msvcrt.dll
        773d0000 4110968c Aug 04 13:25:56 2004 C:\WINDOWS\WinSxS\x86_Microsoft.Wi
        7c9c0000 411096b7 Aug 04 13:26:39 2004 C:\WINDOWS\system32\SHELL32.dll
        73000000 411096b6 Aug 04 13:26:38 2004 C:\WINDOWS\system32\WINSPOOL.DRV
        5cb70000 411096ba Aug 04 13:26:42 2004 C:\WINDOWS\system32\ShimEng.dll
        6f880000 4110968e Aug 04 13:25:58 2004 C:\WINDOWS\AppPatch\AcGenral.DLL
        76b40000 411096d6 Aug 04 13:27:10 2004 C:\WINDOWS\system32\WINMM.dll
        774e0000 411096f2 Aug 04 13:27:38 2004 C:\WINDOWS\system32\ole32.dll
        77120000 411096f3 Aug 04 13:27:39 2004 C:\WINDOWS\system32\OLEAUT32.dll
        77be0000 411096cf Aug 04 13:27:03 2004 C:\WINDOWS\system32\MSACM32.dll
        77c00000 411096b7 Aug 04 13:26:39 2004 C:\WINDOWS\system32\VERSION.dll
        769c0000 411096b9 Aug 04 13:26:41 2004 C:\WINDOWS\system32\USERENV.dll
        5ad70000 411096bb Aug 04 13:26:43 2004 C:\WINDOWS\system32\UxTheme.dll
    SubSystemData:     00000000
    ProcessHeap:       000a0000
    ProcessParameters: 00020000
    CurrentDirectory:  'C:\Program Files\Debugging Tools for Windows (x86)\'
    WindowTitle:  'notepad.exe C:\1.txt'
    ImageFile:    'C:\WINDOWS\system32\notepad.exe'
    CommandLine:  'notepad.exe C:\1.txt'
    DllPath:      'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\W
    Environment:  00010000
        =::=::\
        =C:=C:\Program Files\Debugging Tools for Windows (x86)
```

# Win32 API



File System

Process

Socket

LPC/RPC

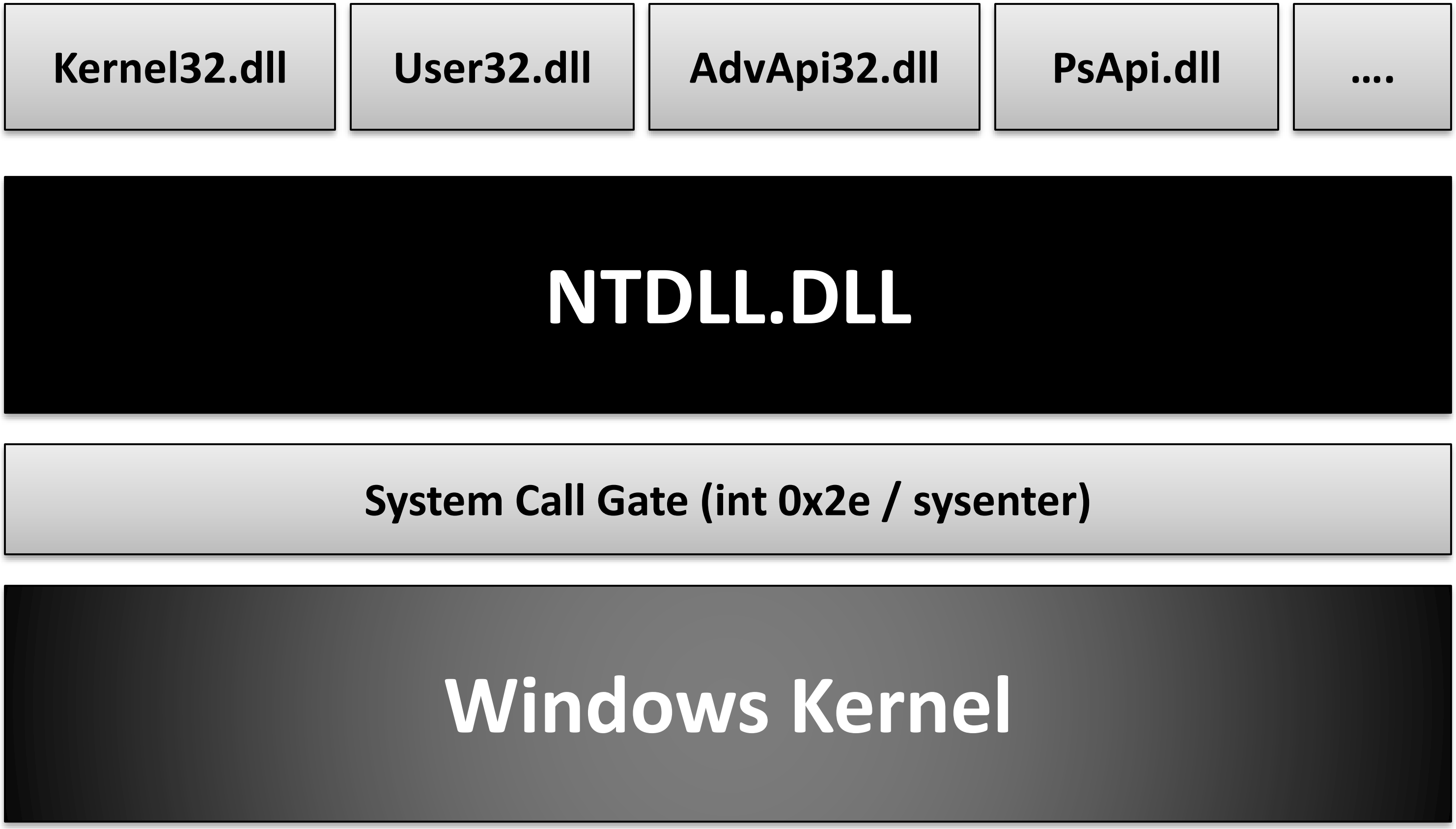
Registry

Service Management

[..]

**http://msdn.microsoft.com/**

# Win32 API Implementation



Kernel32.dll

User32.dll

AdvApi32.dll

PsApi.dll

....

NTDLL.DLL

System Call Gate (int 0x2e / sysenter)

Windows Kernel

# Win32 API: Common Data Types

| Type | Primitive Type | Comments |
|---|---|---|
| HINSTANCE | Struct | Placeholder struct with 1 integer parameter |
| HANDLE | VOID* | Used to represent File Handle/Descriptor |
| HMODULE | HINSTANCE | Used to represent Executable Modules |
| PVOID | VOID* | VOID Pointer |
| DWORD | Unsigned Long | Double Word Storage |
| BYTE | Unsigned Char | Single Byte Storage |
| BOOL | Int | Integer with the convention to store TRUE or FALSE |
| HKEY | Struct | Registry Key Handle |
| LPSTR | CHAR* | String Pointer |
| LPTSTR | TCHAR* | Typed String Pointer (ASCII or Unicode) |

# Win32: Example File System API

```
HANDLE WINAPI CreateFile(
    __in        LPCTSTR lpFileName,
    __in        DWORD dwDesiredAccess,
    __in        DWORD dwShareMode,
    __in_opt  LPSECURITY_ATTRIBUTES lpSecurityAttributes,
    __in        DWORD dwCreationDisposition,
    __in        DWORD dwFlagsAndAttributes,
    __in_opt  HANDLE hTemplateFile
);
```

http://msdn.microsoft.com/en-us/library/windows/desktop/aa363858(v=vs.85).aspx

# Win32: Example Registry API

```
LONG WINAPI RegOpenKeyEx(
    __in          HKEY hKey,
    __in_opt      LPCTSTR lpSubKey,
    __reserved    DWORD ulOptions,
    __in          REGSAM samDesired,
    __out         PHKEY phkResult
);
```

http://msdn.microsoft.com/en-us/library/windows/desktop/ms724897(v=vs.85).aspx

# Win32 API: Encoding

- Multi-Byte (ASCII)
  - LoadLibrary**A**
  - CreateProcess**A**
  - RegOpenKeyEx**A**
- Wide-Character (Unicode)
  - LoadLibrary**W**
  - CreateProcess**W**
  - RegOpenKeyEx**W**

- Generic Wrapper
  - **#include <tchar.h>**
  - **TEXT("This is a Generic String")**

# Windows Debugger

- OllyDBG
- Immunity Debugger
- Visual Studio Debugger
- **WinDBG**
  - **Microsoft Supported Debugger**
  - **Best suited for exploring Win32 Internals**

# GFLAGS

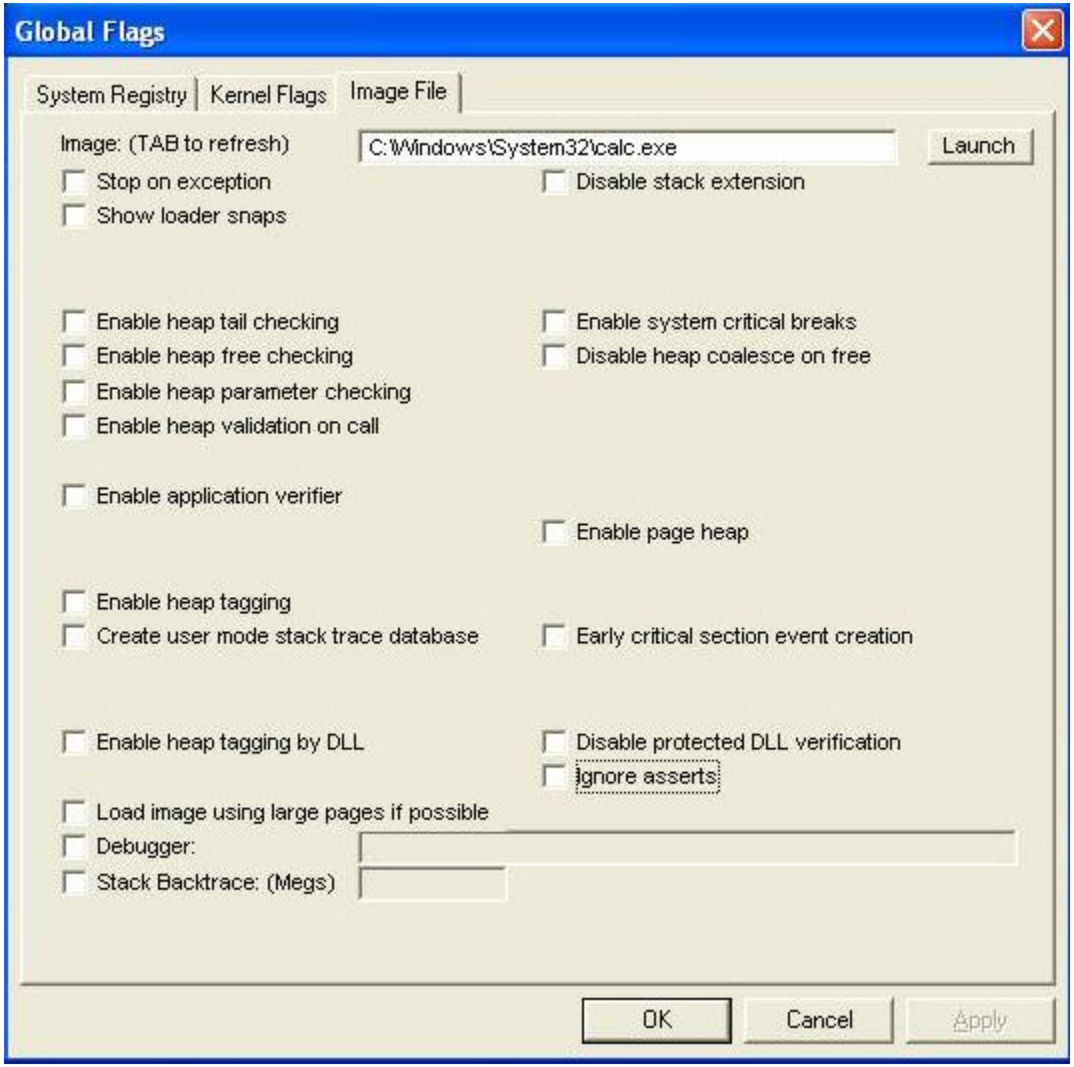


Image: (TAB to refresh) C:\Windows\System32\calc.exe

□ Stop on exception
□ Show loader snaps
□ Disable stack extension

□ Enable heap tail checking
□ Enable heap free checking
□ Enable heap parameter checking
□ Enable heap validation on call
□ Enable system critical breaks
□ Disable heap coalesce on free

□ Enable application verifier
□ Enable page heap

□ Enable heap tagging
□ Create user mode stack trace database
□ Early critical section event creation

□ Enable heap tagging by DLL
□ Disable protected DLL verification
□ Ignore asserts

□ Load image using large pages if possible
□ Debugger:
□ Stack Backtrace: (Megs)

- Global Debug Flags
- Per-Image Debug Flags
- System Flags for whole system

**GFLAGS.EXE**

Debugging Tools for Windows