Part II – Introduction to Windows Internals

Swapnil Pathak
Amit Malik

www.SecurityXploded.com

Disclaimer

The Content, Demonstration, Source Code and Programs presented here is "AS IS" without any warranty or conditions of any kind. Also the views/ideas/knowledge expressed here are solely of the trainer’s only and nothing to do with the company or the organization in which the trainer is currently working.

However in no circumstances neither the trainer nor SecurityXploded is responsible for any damage or loss caused due to use or misuse of the information presented here.

Acknowledgement

- Special thanks to **null** & **Garage4Hackers** community for their extended support and cooperation.
- Thanks to all the trainers who have devoted their precious time and countless hours to make it happen.

Reversing & Malware Analysis Training

This presentation is part of our **Reverse Engineering & Malware Analysis** Training program. Currently it is delivered only during our local meet for FREE of cost.

For complete details of this course, visit our Security Training page.

Who am I #1

Amit Malik (sometimes DouBle_Zer0,DZZ)

- Member SecurityXploded
- Security Researcher @ McAfee Labs
- RE, Exploit Analysis/Development, Malware Analysis
- Email: m.amit30@gmail.com

Who am I #2

Swapnil Pathak

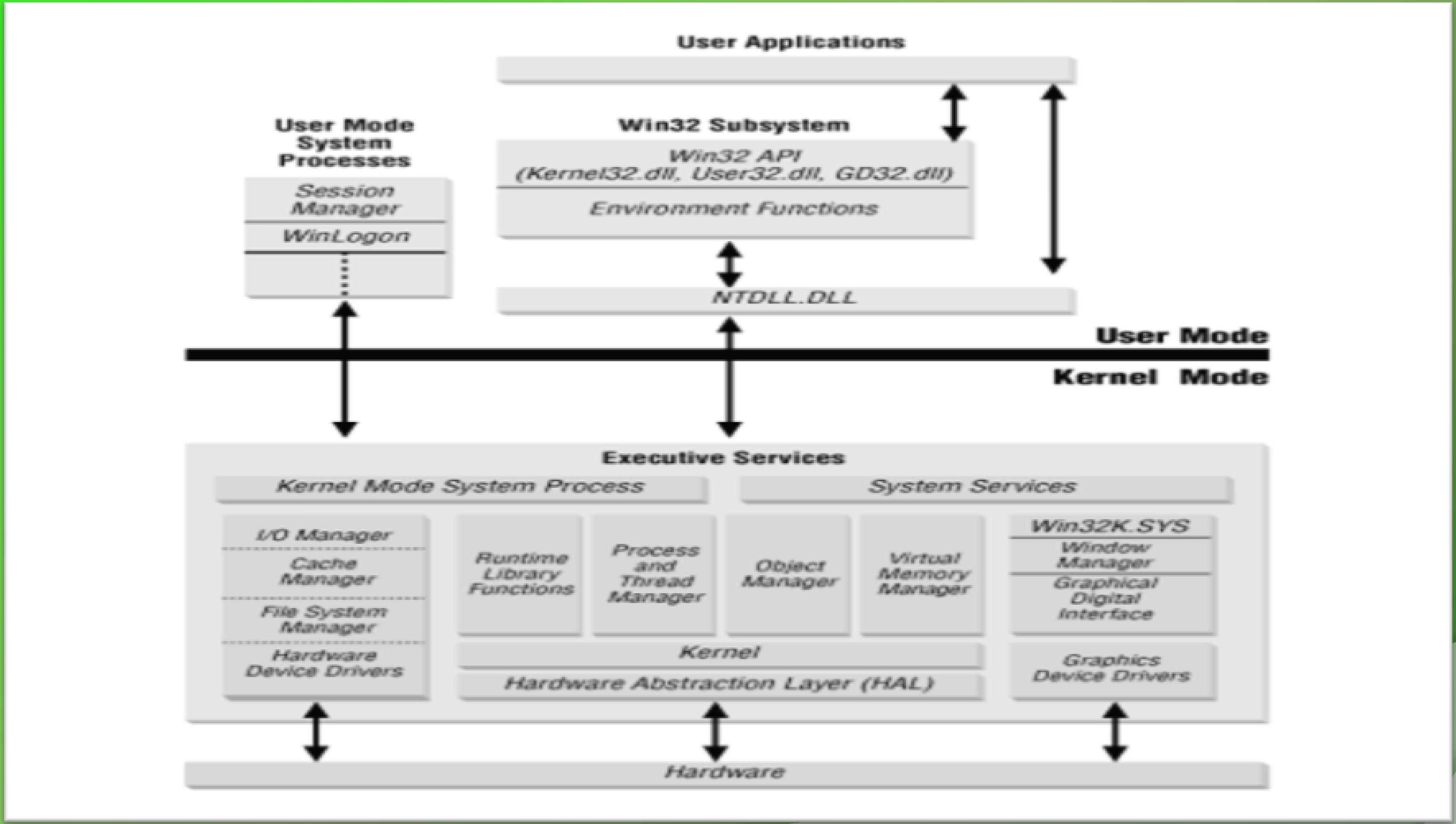
- Member SecurityXploded
- Security Researcher @ McAfee Labs
- RE, Malware Analysis, Network Security
- Email: swapnilpathak101@gmail.com

Course Q&A

- Keep yourself up to date with latest security news
  - http://www.securityphresh.com

- For Q&A, join our mailing list.
  - http://groups.google.com/group/securityxploded

Windows Architecture



Memory Management

- **Virtual Memory**
  - An invisible layer between a software and physical memory
  - Every process first get loaded into its virtual memory address space
  - Small units called "pages" are used to do mapping between physical memory and virtual memory.
- **Paging**
  - Memory management scheme that stores and retrieves data from secondary storage for use in main memory
  - Uses same size blocks called pages
  - Page table is used to translate virtual addresses in physical memory addresses

Memory Management Cont.

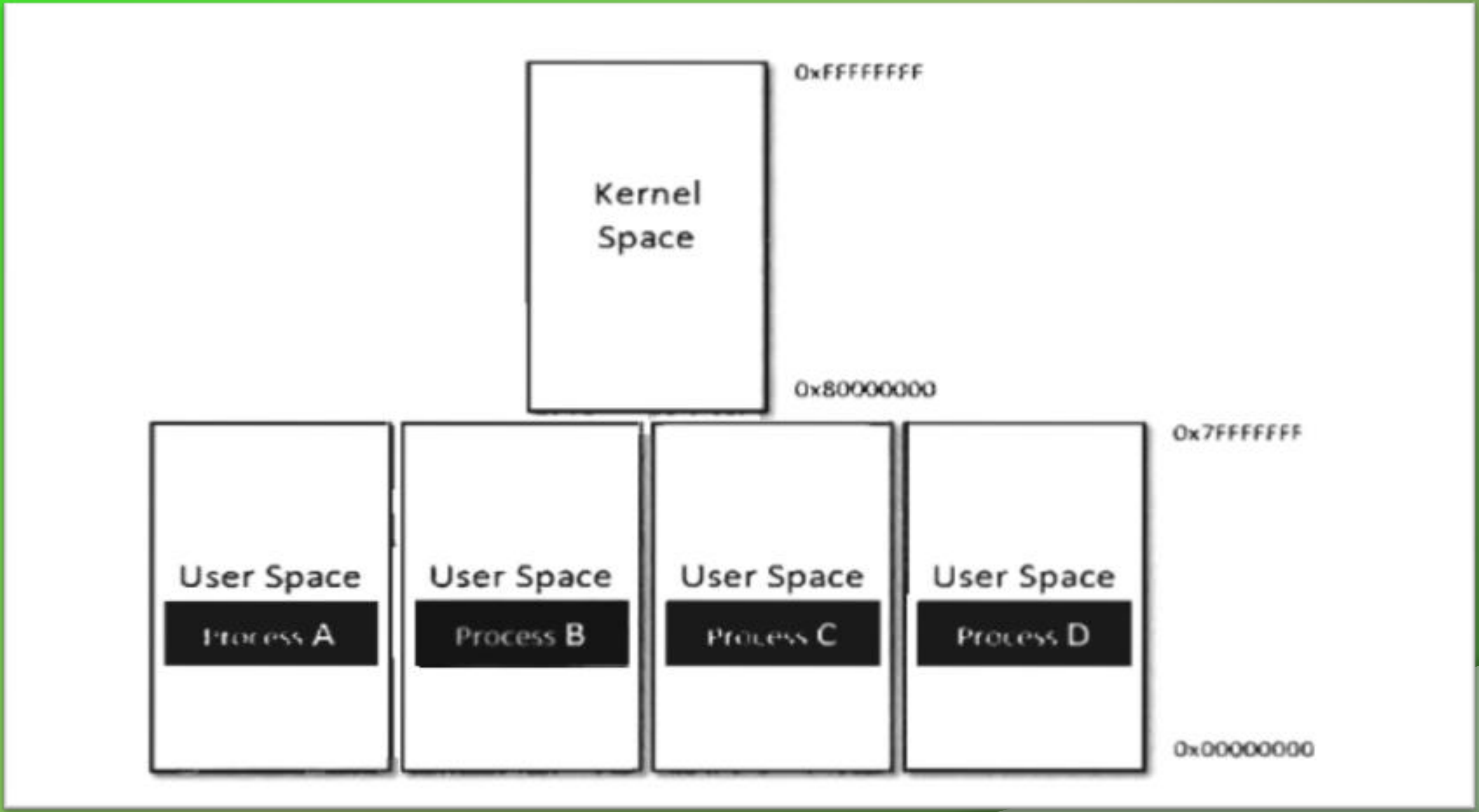
- **User Address Space**

- Allocated for user mode applications.
- All processes execute in their own virtual space.
- Use operating system dlls to interact with kernel

- **Kernel Address Space**

- Strictly reserved for kernel, device drivers and operating system executive.
- No user mode application can directly interact with the kernel.

Kernel & User Address Space

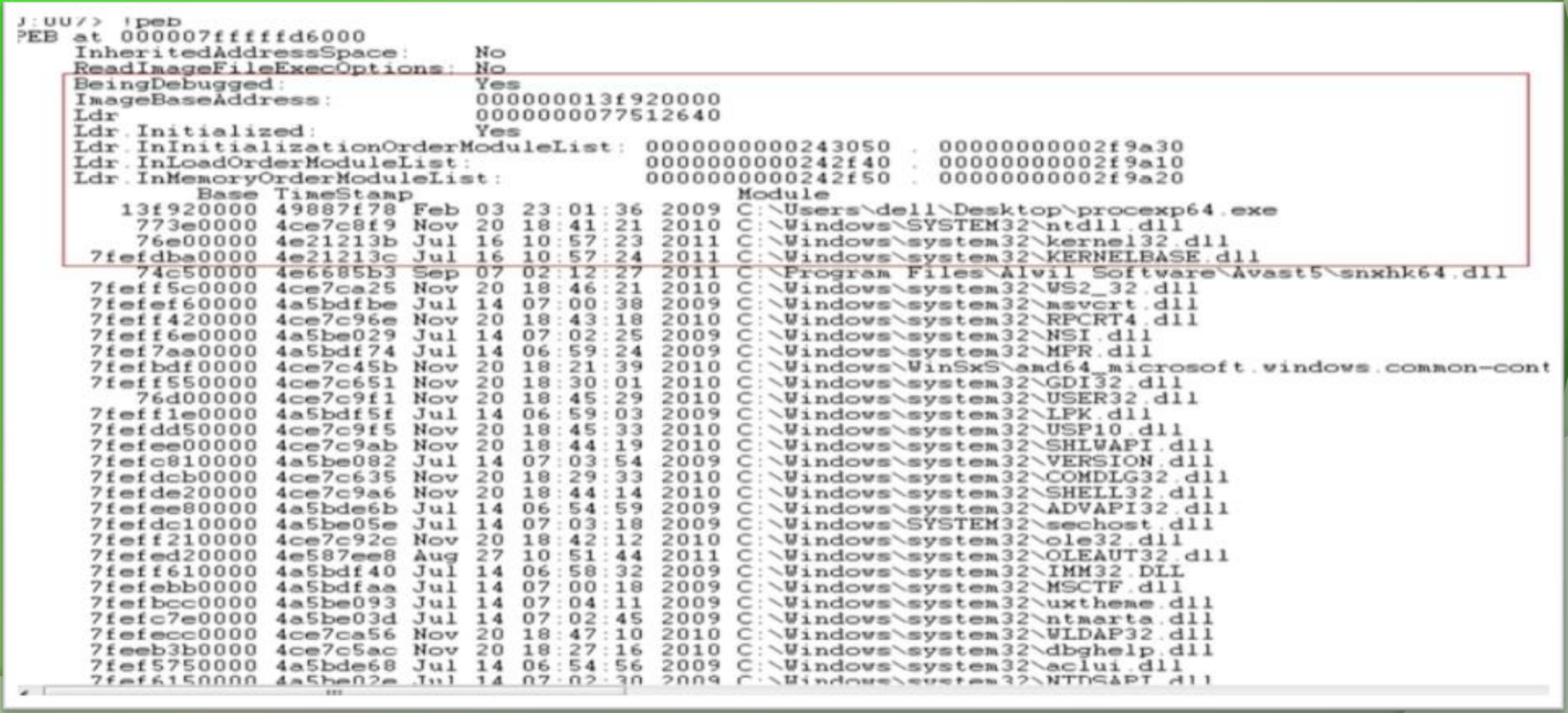


Process and Thread

- **Process**
  - Executing instance of an application.
  - Isolated address space
  - PEB data structure store information about process
  - PEB is an user space data structure
- **Threads**
  - Multiple threads share the same address space in the process.
  - Each process has **at least a single** executing thread.
  - TEB data structure store information about thread

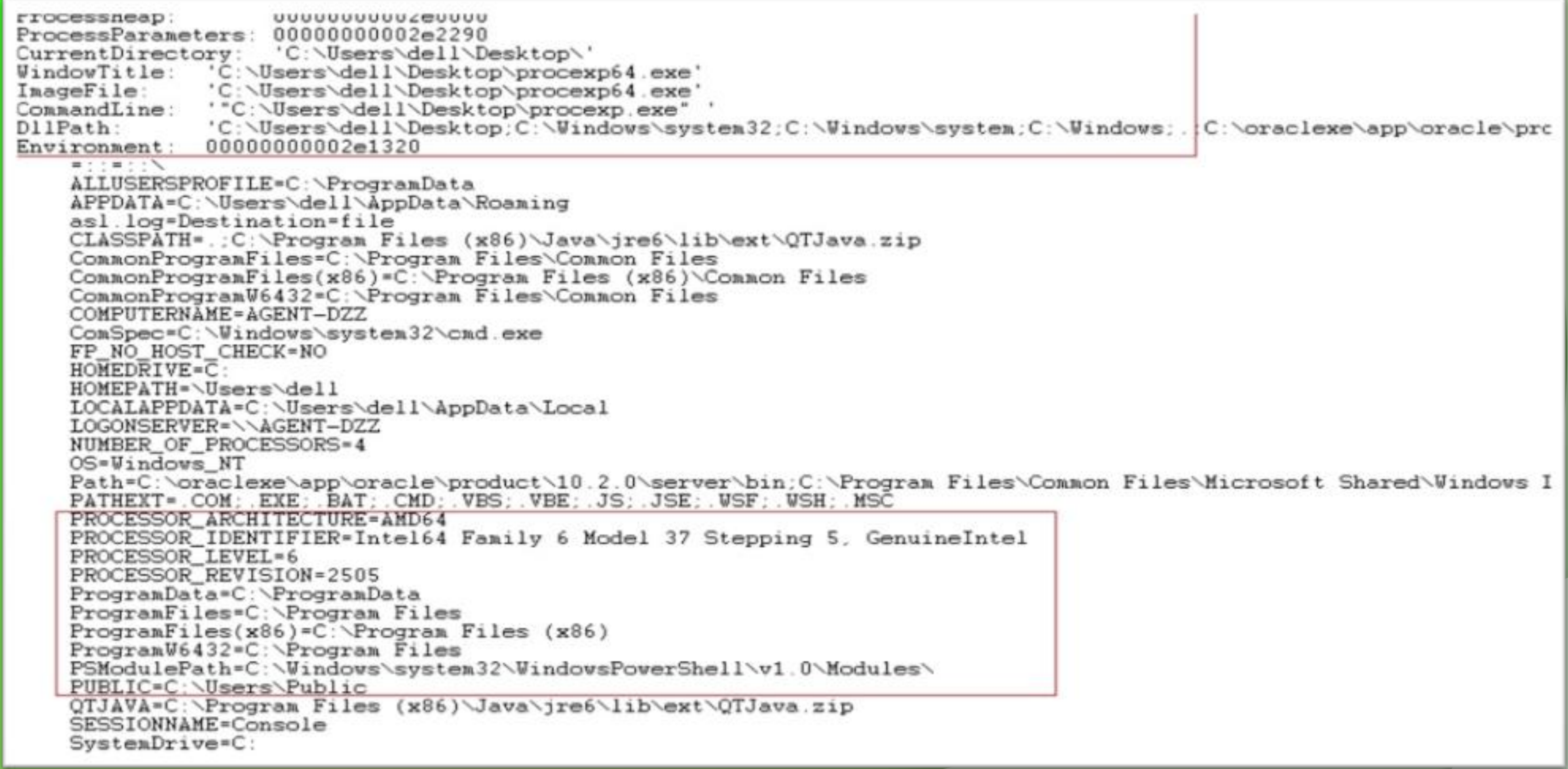
PEB (Process Environment Block)

An opaque data structure that store information about process in user space



```
0:000> !peb
PEB at 000007fffffd6000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            Yes
    ImageBaseAddress:         000000013f920000
    Ldr                       0000000077512640
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000243050 . 00000000002f9a30
    Ldr.InLoadOrderModuleList:           0000000000242f40 . 00000000002f9a10
    Ldr.InMemoryOrderModuleList:         0000000000242f50 . 00000000002f9a20
            Base TimeStamp                     Module
       13f920000 49887f78 Feb 03 23:01:36 2009 C:\Users\dell\Desktop\procexp64.exe
        773e0000 4ce7c8f9 Nov 20 18:41:21 2010 C:\Windows\SYSTEM32\ntdll.dll
        76e00000 4e21213b Jul 16 10:57:23 2011 C:\Windows\system32\kernel32.dll
     7fefdba0000 4e21213c Jul 16 10:57:24 2011 C:\Windows\system32\KERNELBASE.dll
        74c50000 4e6685b3 Sep 07 02:12:27 2011 C:\Program Files\Alwil Software\Avast5\snxhk64.dll
     7feff5c0000 4ce7ca25 Nov 20 18:46:21 2010 C:\Windows\system32\WS2_32.dll
     7fefef60000 4a5bdfbe Jul 14 07:00:38 2009 C:\Windows\system32\msvcrt.dll
     7feff420000 4ce7c96e Nov 20 18:43:18 2010 C:\Windows\system32\RPCRT4.dll
     7feff6e0000 4a5be029 Jul 14 07:02:25 2009 C:\Windows\system32\NSI.dll
     7fef7aa0000 4a5bdf74 Jul 14 06:59:24 2009 C:\Windows\system32\MPR.dll
     7fefbdf0000 4ce7c45b Nov 20 18:21:39 2010 C:\Windows\WinSxS\amd64_microsoft.windows.common-cont
     7feff550000 4ce7c651 Nov 20 18:30:01 2010 C:\Windows\system32\GDI32.dll
        76d00000 4ce7c9f1 Nov 20 18:45:29 2010 C:\Windows\system32\USER32.dll
     7feff1e0000 4a5bdf5f Jul 14 06:59:03 2009 C:\Windows\system32\LPK.dll
     7fefdd50000 4ce7c9f5 Nov 20 18:45:33 2010 C:\Windows\system32\USP10.dll
     7fefee00000 4ce7c9ab Nov 20 18:44:19 2010 C:\Windows\system32\SHLWAPI.dll
     7fefc810000 4a5be082 Jul 14 07:03:54 2009 C:\Windows\system32\VERSION.dll
     7fefdcb0000 4ce7c635 Nov 20 18:29:33 2010 C:\Windows\system32\COMDLG32.dll
     7fefde20000 4ce7c9a6 Nov 20 18:44:14 2010 C:\Windows\system32\SHELL32.dll
     7fefee80000 4a5bde6b Jul 14 06:54:59 2009 C:\Windows\system32\ADVAPI32.dll
     7fefdc10000 4a5be05e Jul 14 07:03:18 2009 C:\Windows\SYSTEM32\sechost.dll
     7feff210000 4ce7c92c Nov 20 18:42:12 2010 C:\Windows\system32\ole32.dll
     7fefed20000 4e587ee8 Aug 27 10:51:44 2011 C:\Windows\system32\OLEAUT32.dll
     7feff610000 4a5bdf40 Jul 14 06:58:32 2009 C:\Windows\system32\IMM32.DLL
     7fefebb0000 4a5bdfaa Jul 14 07:00:18 2009 C:\Windows\system32\MSCTF.dll
     7fefbcc0000 4a5be093 Jul 14 07:04:11 2009 C:\Windows\system32\uxtheme.dll
     7fefc7e0000 4a5be03d Jul 14 07:02:45 2009 C:\Windows\system32\ntmarta.dll
     7fefecc0000 4ce7ca56 Nov 20 18:47:10 2010 C:\Windows\system32\WLDAP32.dll
     7feeb3b0000 4ce7c5ac Nov 20 18:27:16 2010 C:\Windows\system32\dbghelp.dll
     7fef5750000 4a5bde68 Jul 14 06:54:56 2009 C:\Windows\system32\aclui.dll
     7fef6150000 4a5be02e Jul 14 07:02:30 2009 C:\Windows\system32\NTDSAPI.dll
```

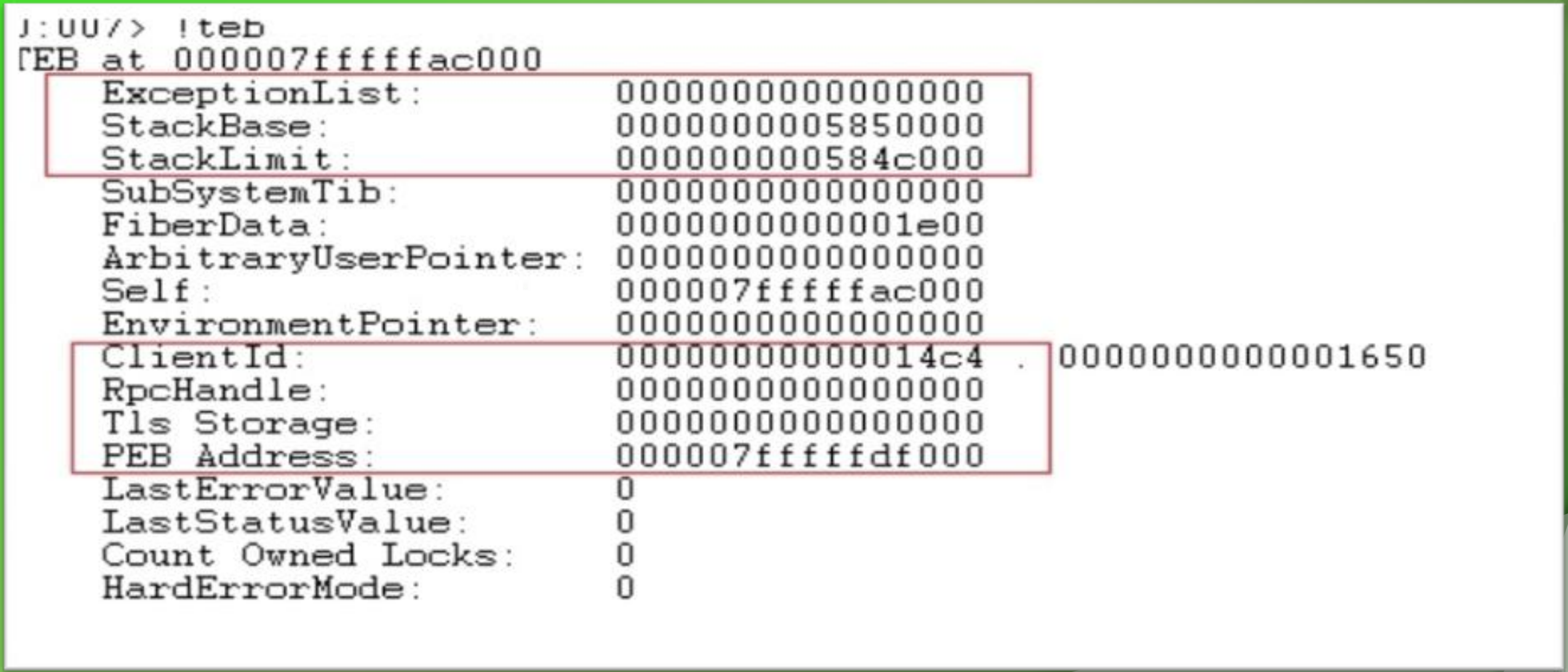
PEB Cont.



```
ProcessHeap:        00000000002e0000
ProcessParameters:  00000000002e2290
CurrentDirectory:   'C:\Users\dell\Desktop\'
WindowTitle:   'C:\Users\dell\Desktop\procexp64.exe'
ImageFile:     'C:\Users\dell\Desktop\procexp64.exe'
CommandLine:   '"C:\Users\dell\Desktop\procexp.exe" '
DllPath:       'C:\Users\dell\Desktop;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\oraclexe\app\oracle\prc
Environment:   00000000002e1320
    =::=::\
    ALLUSERSPROFILE=C:\ProgramData
    APPDATA=C:\Users\dell\AppData\Roaming
    asl.log=Destination=file
    CLASSPATH=.;C:\Program Files (x86)\Java\jre6\lib\ext\QTJava.zip
    CommonProgramFiles=C:\Program Files\Common Files
    CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
    CommonProgramW6432=C:\Program Files\Common Files
    COMPUTERNAME=AGENT-DZZ
    ComSpec=C:\Windows\system32\cmd.exe
    FP_NO_HOST_CHECK=NO
    HOMEDRIVE=C:
    HOMEPATH=\Users\dell
    LOCALAPPDATA=C:\Users\dell\AppData\Local
    LOGONSERVER=\\AGENT-DZZ
    NUMBER_OF_PROCESSORS=4
    OS=Windows_NT
    Path=C:\oraclexe\app\oracle\product\10.2.0\server\bin;C:\Program Files\Common Files\Microsoft Shared\Windows I
    PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
    PROCESSOR_ARCHITECTURE=AMD64
    PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 37 Stepping 5, GenuineIntel
    PROCESSOR_LEVEL=6
    PROCESSOR_REVISION=2505
    ProgramData=C:\ProgramData
    ProgramFiles=C:\Program Files
    ProgramFiles(x86)=C:\Program Files (x86)
    ProgramW6432=C:\Program Files
    PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
    PUBLIC=C:\Users\Public
    QTJAVA=C:\Program Files (x86)\Java\jre6\lib\ext\QTJava.zip
    SESSIONNAME=Console
    SystemDrive=C:
```

TEB (Thread Environment Block)

TEB is a data structure that store information about thread

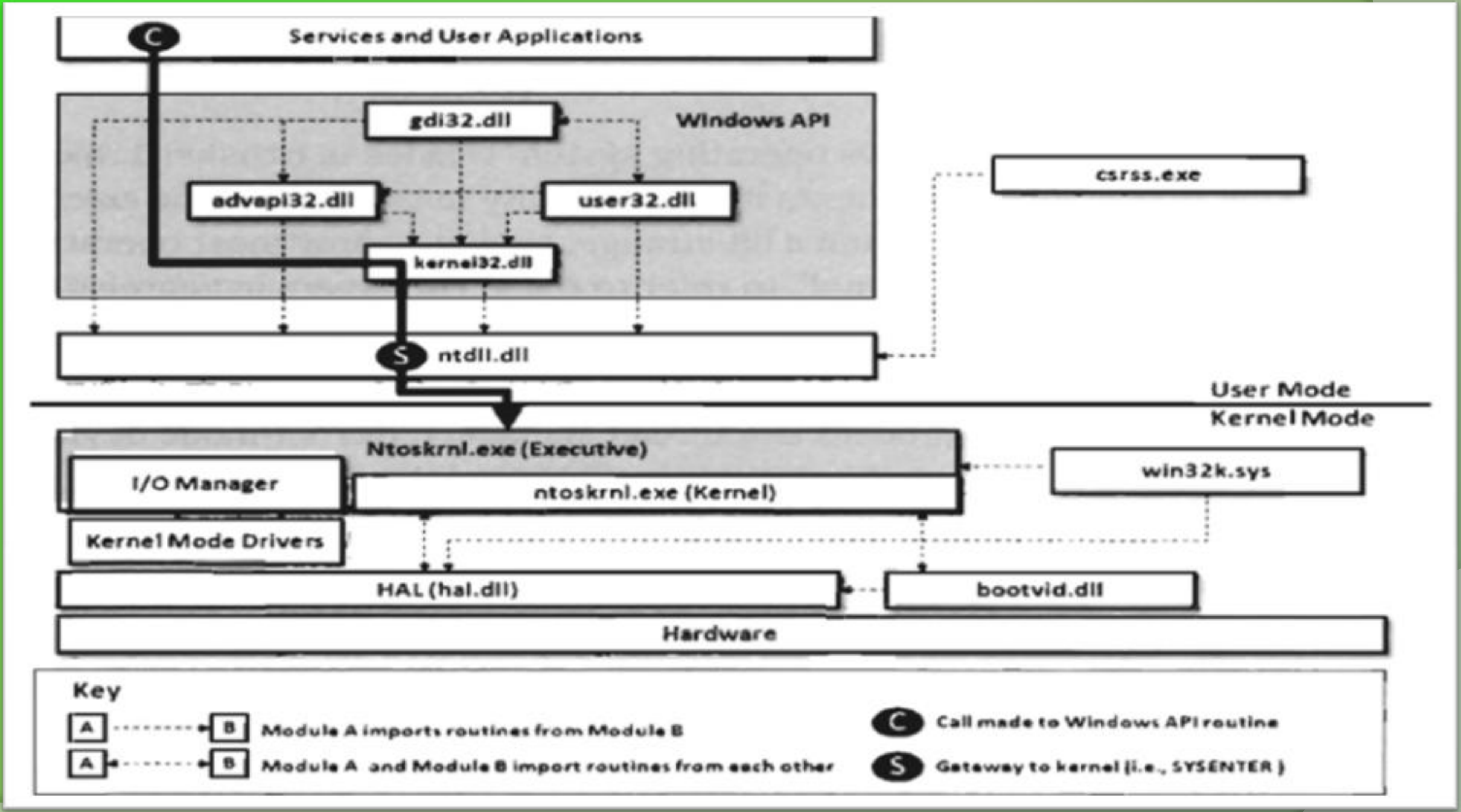


```
0:007> !teb
TEB at 000007fffffac000
    ExceptionList:        0000000000000000
    StackBase:            0000000005850000
    StackLimit:           000000000584c000
    SubSystemTib:         0000000000000000
    FiberData:            0000000000001e00
    ArbitraryUserPointer: 0000000000000000
    Self:                 000007fffffac000
    EnvironmentPointer:   0000000000000000
    ClientId:             00000000000014c4 . 0000000000001650
    RpcHandle:            0000000000000000
    Tls Storage:          0000000000000000
    PEB Address:          000007fffffdf000
    LastErrorValue:       0
    LastStatusValue:      0
    Count Owned Locks:    0
    HardErrorMode:        0
```

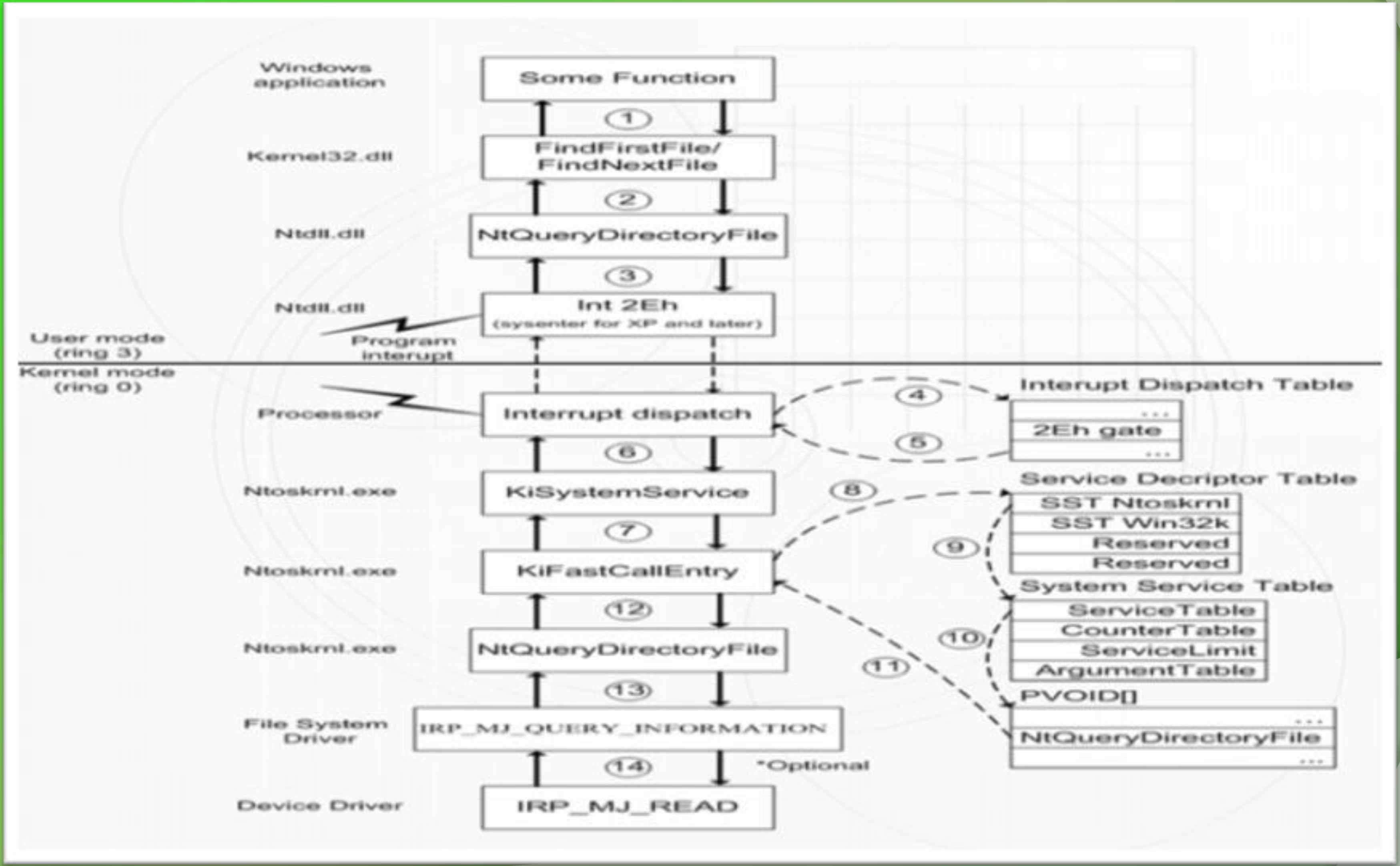
Application Programming Interface

- **API**
  - Includes functions, classes, data structures and variables
  - Interface between various software components to communicate with each other.
  - Windows APIs are used to interact with kernel or other modules.
- **MSDN**
  - Provides documentation for various API functions.
- **System Dlls**
  - ntdll.dll, kernel32.dll, user32.dll, advapi32.dll, hal.dll etc

System Service Dispatching



System Service Dispatching Cont.



Important API

- **File and Directories**

- CreateFile, GetSystemDirectory, ReadFile, WriteFile etc

- **Network**

- socket, send, recv, URLDownloadToFile etc

- **Registry**

- RegOpenKey, RegSetValue, RegQueryValue etc

Important API Cont.

- **Processes, Threads, Synchronization using mutex, semaphore.**

- CreateProcess, ReadProcessMemory, WriteProcessMemory,CreateRemoteThread, CreateMutex etc

- **Memory**

- VirtualAlloc, VirtualProtect ,HeapAlloc, LocalAlloc etc

Reference

- Complete Reference Guide for Reversing & Malware Analysis Training

Thank You !

http://SecurityXploded.com