

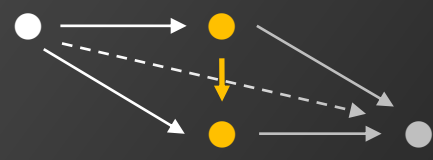
Part 3 Draft

# Windows API

for Software Diagnostics

## Accelerated

With Category Theory in View



Dmitry Vostokov  
Software Diagnostics Services

# Exports and Imports

- WinDbg (manual/scripts)
- 3<sup>rd</sup>-party WinDbg extensions ([SwishDbgEx](#))
- DUMPBIN

# API and System Calls

- ⦿ API that do not require kernel services

- `GetCurrentThreadId`

- ⦿ API that require kernel services

- `user32!CreateWindowExW` → `win32u!NtUserCreateWindowEx`
- `kernel32!ReadFile` → `ntdll!NtReadFile`

# Exercise W6

- ⦿ **Goal:** Explore exports and imports using dumpbin. Check whether the selected API functions use a system call
- ⦿ **ADDR Patterns:** Call Path
- ⦿ [\AWAPI-Dumps\Exercise-W6.pdf](#)

# Documented API

- ⦿ Online documentation
- ⦿ Present in headers
- ⦿ Example:

[Documentation](#)

kernel32!SuspendThread →  
    KERNELBASE!SuspendThread →  
        ntdll!NtSuspendThread

# Undocumented API

## ntdll!NtSuspendProcess

```
0:000> x /v ntdll!*
```

```
...
```

```
pub func 00007ffc`f6346ff0 0 ntdll!NtSuspendProcess (NtSuspendProcess)
```

```
...
```

# API Source Code

- [Wine](#) (GitLab) / [Wine-Mirror](#) (GitHub)

- Example:

`user32!CreateWindowExW`

<https://gitlab.winehq.org/wine/wine/-/blob/master/dlls/user32/win.c>

<https://github.com/wine-mirror/wine/blob/master/dlls/user32/win.c>

# API Name Patterns

- ⦿ Create/Open/Delete/Close
- ⦿ Process/Thread
- ⦿ Memory
- ⦿ Read/Write

WinDbg Commands

```
0:000> x /v module!fpattern
```



# API Namespaces

- ⦿ API sets / contracts

- Example: [CreateDialogParamW](#)

- ⦿ Functions required to accomplish a particular task

- Example: **screen capture**

```
gdi32!CreateCompatibleDC  
gdi32!StretchBlt  
gdi32!CreateDIBSection  
gdi32!SelectObject
```

```
user32!ReleaseDC  
user32!NtUserGetWindowDC  
user32!GetWindowRect
```

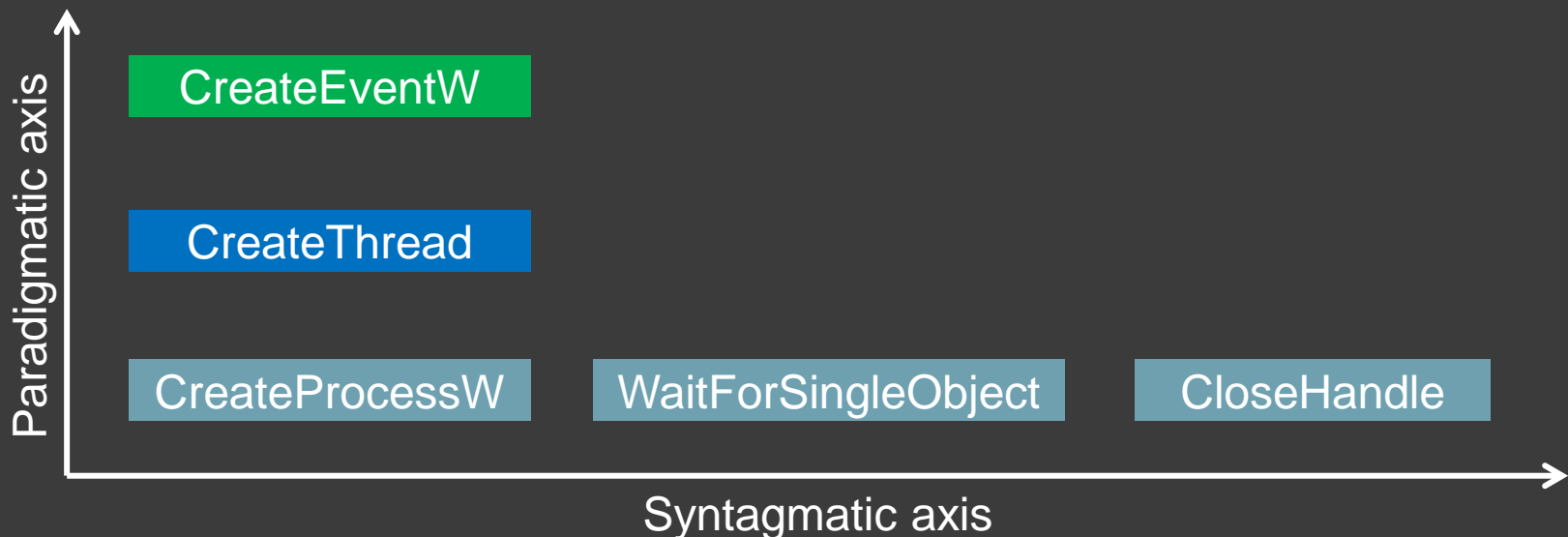
- **saving image**

```
GdiPlus!GdiplusStartup  
GdiPlus!GdipSaveImageToStream  
GdiPlus!GdipGetImageEncodersSize  
GdiPlus!GdipDisposeImage  
GdiPlus!GdipCreateBitmapFromHBITMAP  
GdiPlus!GdipGetImageEncoders
```

```
ole32!CreateStreamOnHGlobal
```

# API Syntagms/Paradigms

- ◎ Syntagms / syntagmatic analysis
- ◎ Paradigms / paradigmatic analysis



# Marked API

- Marked Message trace and log analysis pattern
- Points to presence or absence of activity
- Example:
  - CreateThread [-]
  - socket [+]
  - GetMessageW [-]
  - ReadConsoleW [+]

WinDbg Commands

```
0:000> x app!_imp_pattern
```

# ADDR Patterns

- ◎ From Accelerated Disassembly Deconstruction Reversing
- ◎ List of pattern names
- ◎ Pattern descriptions

# DebugWare Patterns

- Patterns for troubleshooting and debugging tools

- API Query

Periodic or asynchronous query of the same set of API and logging of their input and output data.

- Example: WindowHistory

# Patterns vs. Analysis Patterns

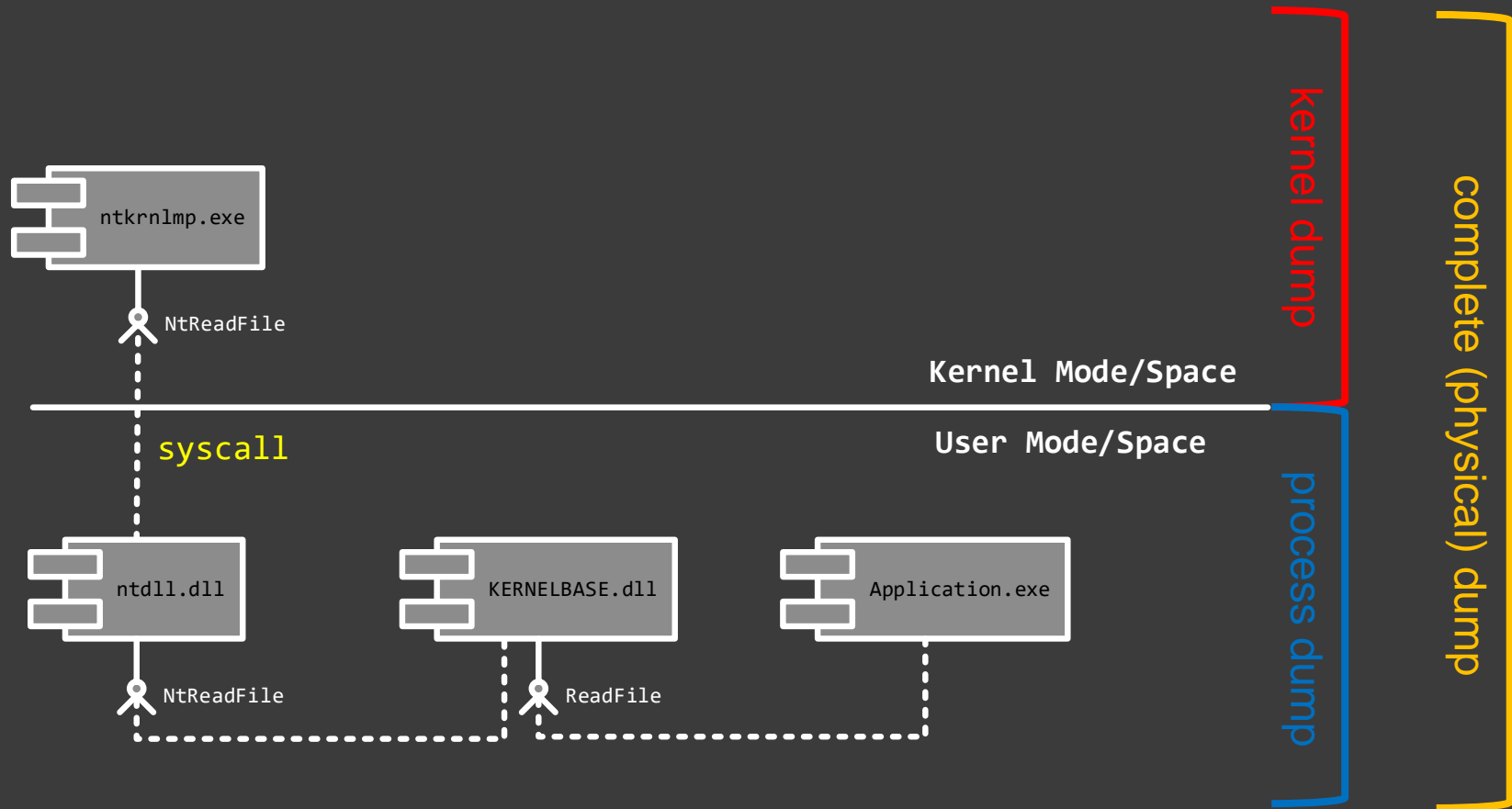
**Diagnostic Pattern:** a common recurrent identifiable problem together with a set of recommendations and possible solutions to apply in a specific context.

**Diagnostic Problem:** a set of indicators (symptoms, signs) describing a problem.

**Diagnostic Analysis Pattern:** a common recurrent analysis technique and method of **diagnostic pattern** identification in a specific context.

**Diagnostics Pattern Language:** common names of diagnostic and diagnostic analysis patterns. The same language for any operating system: Windows, Mac OS X, Linux, ...

# Memory Dump Types



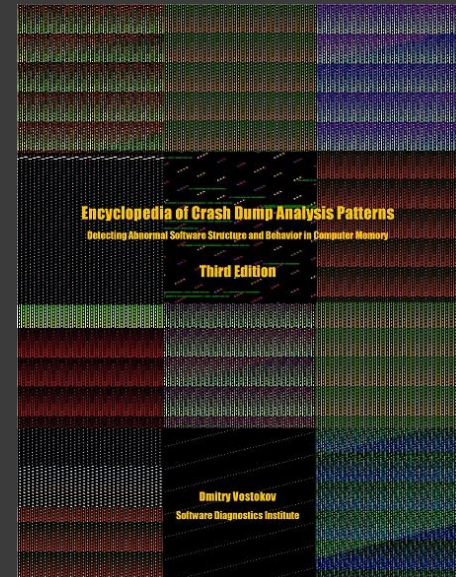
# Memory Analysis Patterns

## ⦿ User space

- Process memory dumps
- Complete memory dumps

## ⦿ Function analysis patterns

- [Stack Trace Collection](#)
- [Well-Tested Function](#)
- [False Function Parameters](#)
- [String Parameter](#)
- [Small Value](#) / [Design Value](#)
- [Virtualized Process](#)



- [Stack Trace](#)
- [Execution Residue](#)
- [Hidden Parameter](#)
- [Parameter Flow](#)
- [Data Correlation](#)



# Thread and Adjoint Thread

Process Monitor - Sysinternals: www.sysintern...

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	TID	Operation	Path
00:51:1...	Explorer.EXE	4092	44912	RegQueryKey	HKLM
00:51:1...	Explorer.EXE	4092	44912	RegOpenKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegSetInfoKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegQueryKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegCloseKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegQueryKey	HKLM
00:51:1...	Explorer.EXE	4092	44912	RegOpenKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegSetInfoKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegQueryKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegCloseKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryRemotePr...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryDirectory	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CloseFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QuerySizeInfor...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CloseFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryStandardl...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryStandardl...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryStandardl...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryStandardl...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryStandardl...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryStandardl...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	RegQueryKey	HKLM
00:51:1...	Explorer.EXE	4092	44912	RegOpenKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegSetInfoKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegQueryKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	RegCloseKey	HKLM\Sc
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryRemotePr...	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	QueryDirectory	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CloseFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.FXF	4092	44912	ReadFile	C:\Users\

Showing 12,154 of 1,253,816 events (0.96%)      Backed by virtual memor

Process Monitor - Sysinternals: www.sysintern...

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	TID	Operation	Path
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	22104	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	22104	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	69232	CreateFile	C:\NewW
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	svchost.exe	71072	16704	CreateFile	C:\Progra
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Kindle.exe	27088	9468	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	svchost.exe	71072	16704	CreateFile	C:\Progra
00:51:1...	svchost.exe	71072	16704	CreateFile	C:\Progra
00:51:1...	Explorer.EXE	4092	22104	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	22104	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	6288	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	6288	CreateFile	C:\Users\
00:51:1...	svchost.exe	71072	16704	CreateFile	C:\Progra
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	69232	CreateFile	C:\Progra
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.FXF	4092	68940	CreateFile	C:\Windo

Showing 18,322 of 1,253,816 events (1.4%)      Backed by virtual memor

# Fiber Bundle

Process Monitor - Sysinternals: www.sysintern...

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	TID	Operation	Path
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	22104	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	22104	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	69232	CreateFile	C:\NewW
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	svchost.exe	71072	16704	CreateFile	C:\Progra
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Kindle.exe	27088	9468	CreateFile	C:\Users\
00:51:1...	Kindle.exe	27088	9468	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	svchost.exe	71072	16704	CreateFile	C:\Progra
00:51:1...	svchost.exe	71072	16704	CreateFile	C:\Progra
00:51:1...	Explorer.EXE	4092	22104	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	22104	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	6288	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	6288	CreateFile	C:\Users\
00:51:1...	svchost.exe	71072	16704	CreateFile	C:\Progra
00:51:1...	Explorer.EXE	4092	44912	CreateFile	C:\Users\
00:51:1...	Explorer.EXE	4092	69232	CreateFile	C:\Progra
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.EXE	4092	63988	CreateFile	C:\Windo
00:51:1...	Explorer.FXF	4092	68940	CreateFile	C:\Windo

Showing 18,322 of 1,253,816 events (1.4%)      Backed by virtual memor...

Event Properties

Event Process Stack

Frame	Module	Location	Address	Path
K 0	FLTMGR.SYS	FileGetFileNameInformation + 0x111b	0xffff804688930b	C:\WINDOWS\system32\drivers
K 1	FLTMGR.SYS	FileGetFileNameInformation + 0x19a1	0xffff8046889a21	C:\WINDOWS\system32\drivers
K 2	FLTMGR.SYS	FileGetFileNameInformationUnsafe + 0x16af	0xffff80468896df	C:\WINDOWS\system32\drivers
K 3	ntoskrnl.exe	IoCallDriver + 0x55	0xffff80471ac8b75	C:\WINDOWS\system32\ntoskrnl.exe
K 4	ntoskrnl.exe	PsReferencePrimaryToken + 0x3599	0xffff80471ec55a9	C:\WINDOWS\system32\ntoskrnl.exe
K 5	ntoskrnl.exe	ObOpenObjectByNameEx + 0x1211	0xffff80471ec1181	C:\WINDOWS\system32\ntoskrnl.exe
K 6	ntoskrnl.exe	ObOpenObjectByNameEx + 0x1212	0xffff80471ec1182	C:\WINDOWS\system32\ntoskrnl.exe
K 7	ntoskrnl.exe	NtCreateFile + 0x4c9	0xffff80471ea49a9	C:\WINDOWS\system32\ntoskrnl.exe
K 8	ntoskrnl.exe	NtCreateFile + 0x79	0xffff80471ea4559	C:\WINDOWS\system32\ntoskrnl.exe
K 9	ntoskrnl.exe	setjmp + 0x8205	0xffff80471ca3a65	C:\WINDOWS\system32\ntoskrnl.exe
U 10	ntldr.dll	NtCreateFile + 0x14	0x7f90c1c814	C:\WINDOWS\system32\ntldr.dll
U 11	KERNELBASE.dll	CreateFileW + 0x481	0x7f909b678	C:\WINDOWS\system32\KERNELBASE.dll
U 12	KERNELBASE.dll	CreateFileW + 0x7c	0x7f909b63c	C:\WINDOWS\system32\KERNELBASE.dll
U 13	OLEAUT32.dll	LoadTypeInfo + 0x94	0x7f909ba1684	C:\WINDOWS\system32\OLEAUT32.dll
U 14	OLEAUT32.dll	LoadTypeInfo + 0xab	0x7f909ba10db	C:\WINDOWS\system32\OLEAUT32.dll

Event Properties

Event Process Stack

Frame	Module	Location	Address	Path
K 0	FLTMGR.SYS	FileGetFileNameInformation + 0x111b	0xffff804688930b	C:\WINDOWS\system32\drivers\FLTMGR.SYS
K 1	FLTMGR.SYS	FileGetFileNameInformation + 0x19a1	0xffff8046889a21	C:\WINDOWS\system32\drivers\FLTMGR.SYS
K 2	FLTMGR.SYS	FileGetFileNameInformationUnsafe + 0x16af	0xffff80468896df	C:\WINDOWS\system32\drivers\FLTMGR.SYS
K 3	ntoskrnl.exe	IoCallDriver + 0x55	0xffff80471ac8b75	C:\WINDOWS\system32\ntoskrnl.exe
K 4	ntoskrnl.exe	PsReferencePrimaryToken + 0x3599	0xffff80471ec55a9	C:\WINDOWS\system32\ntoskrnl.exe
K 5	ntoskrnl.exe	ObOpenObjectByNameEx + 0x1211	0xffff80471ec1181	C:\WINDOWS\system32\ntoskrnl.exe
K 6	ntoskrnl.exe	ObOpenObjectByNameEx + 0x1212	0xffff80471ec1182	C:\WINDOWS\system32\ntoskrnl.exe
K 7	ntoskrnl.exe	NtCreateFile + 0x4c9	0xffff80471ea49a9	C:\WINDOWS\system32\ntoskrnl.exe
K 8	ntoskrnl.exe	NtCreateFile + 0x79	0xffff80471ea4559	C:\WINDOWS\system32\ntoskrnl.exe
K 9	ntoskrnl.exe	setjmp + 0x8205	0xffff80471ca3a65	C:\WINDOWS\system32\ntoskrnl.exe
U 10	ntldr.dll	NtCreateFile + 0x14	0x7f90c1c814	C:\WINDOWS\system32\ntldr.dll
U 11	KERNELBASE.dll	CreateDirectoryW + 0x149	0x7f909b6732a	C:\WINDOWS\system32\KERNELBASE.dll
U 12	KernelBase.dll	CreateDirectoryW + 0x1f	0x7f909b6734f	C:\WINDOWS\system32\KernelBase.dll
U 13	wscnt.dll	DirGetClassObject + 0x1a024	0x7f90657254	C:\WINDOWS\system32\wscnt.dll
U 14	wscnt.dll	DirGetClassObject + 0x1a00a	0x7f9065720a	C:\WINDOWS\system32\wscnt.dll

Event Properties

Event Process Stack

Frame	Module	Location	Address	Path
K 3	ntoskrnl.exe	IoCallDriver + 0x55	0xffff80471ac8b75	C:\WINDOWS\system32\ntoskrnl.exe
K 4	ntoskrnl.exe	PsReferencePrimaryToken + 0x3599	0xffff80471ec55a9	C:\WINDOWS\system32\ntoskrnl.exe
K 5	ntoskrnl.exe	ObOpenObjectByNameEx + 0x1211	0xffff80471ec1181	C:\WINDOWS\system32\ntoskrnl.exe
K 6	ntoskrnl.exe	ObOpenObjectByNameEx + 0x1212	0xffff80471ec1182	C:\WINDOWS\system32\ntoskrnl.exe
K 7	ntoskrnl.exe	NtCreateFile + 0x4c9	0xffff80471ea49a9	C:\WINDOWS\system32\ntoskrnl.exe
K 8	ntoskrnl.exe	NtOpenFile + 0x58	0xffff80471ea0268	C:\WINDOWS\system32\ntoskrnl.exe
K 9	ntoskrnl.exe	setjmp + 0x8205	0xffff80471ca3a65	C:\WINDOWS\system32\ntoskrnl.exe
U 10	ntldr.dll	NtOpenFile + 0x14	0x7f90c1c814	C:\WINDOWS\system32\ntldr.dll
U 11	KERNELBASE.dll	GetDiskFreeSpaceExW + 0xad	0x7f909b600d0	C:\WINDOWS\system32\KERNELBASE.dll
U 12	thumbcache.dll	thumbcache.dll + 0x1004e	0x7f909b1004e	C:\WINDOWS\system32\thumbcache.dll
U 13	thumbcache.dll	thumbcache.dll + 0x10057	0x7f909b10057	C:\WINDOWS\system32\thumbcache.dll
U 14	thumbcache.dll	DIGetClassObject + 0x1ba8	0x7f909b20966	C:\WINDOWS\system32\thumbcache.dll
U 15	thumbcache.dll	DIGetClassObject + 0x1b11	0x7f909b20841	C:\WINDOWS\system32\thumbcache.dll
U 16	thumbcache.dll	thumbcache.dll + 0x2423	0x7f909b20243	C:\WINDOWS\system32\thumbcache.dll
U 17	thumbcache.dll	thumbcache.dll + 0x8558	0x7f909b20858	C:\WINDOWS\system32\thumbcache.dll



# WOW64

- 64-bit process dumps
- 32-bit process dumps
- wow64 (kernel32)
- wow64win (user32, gdi32)
- wow64cpu

# Exercise W7

- ⦿ **Goal:** Explore Windows API calls in the WOW64 context
- ⦿ **Memory Analysis Patterns:** Stack Trace Collection; Virtualized Process
- ⦿ [\AWAPI-Dumps\Exercise-W7.pdf](#)