Windows Kernel Courses Supplemental Material

Developed and Presented by :

CodeMachine

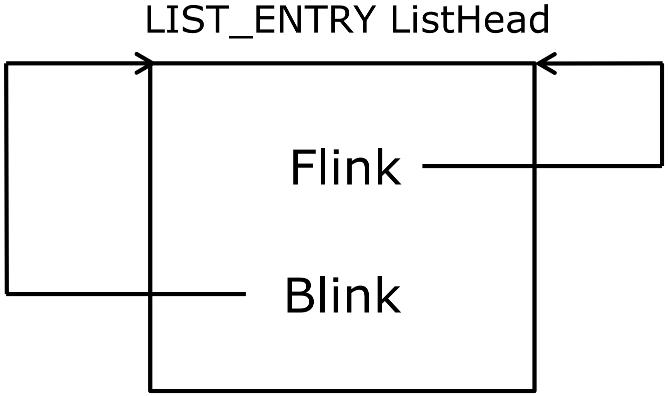
Security Research, Development and Training

www.codemachine.com
twitter.com/codemachineinc
facebook.com/codemachineinc

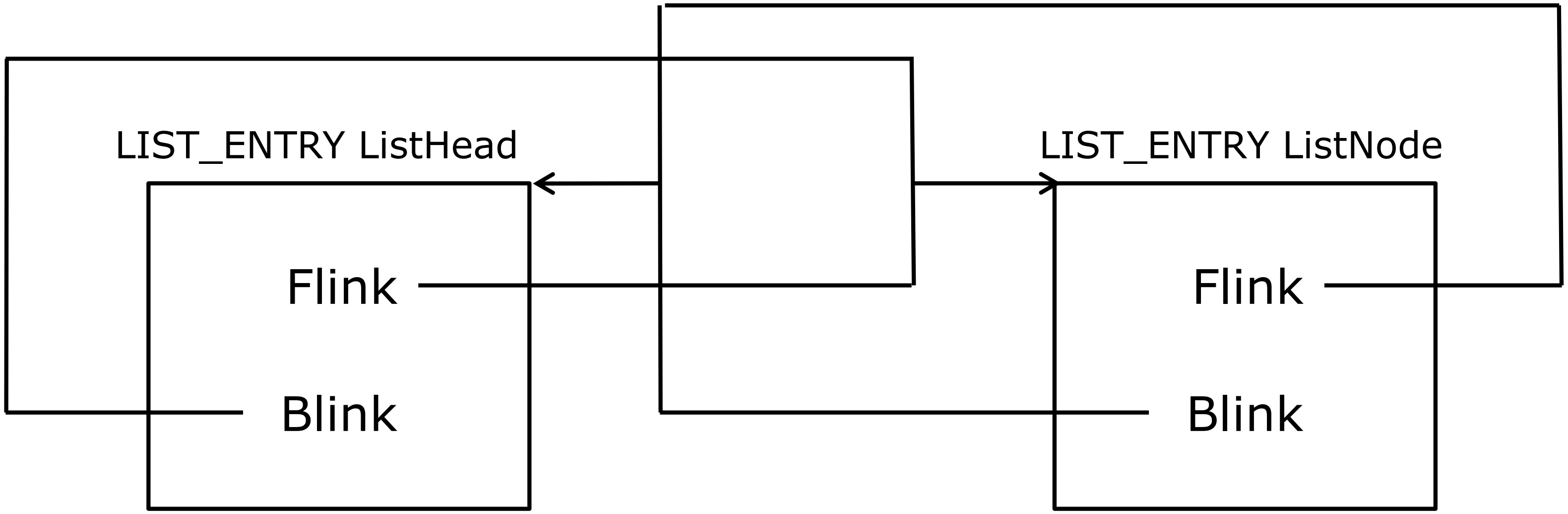
Kernel Function Naming Convention

Suffix	Meaning	Example
p	Private	Psp, Alpcp, Iop, Sep, Obp
i	Internal	Mi, Ki, Pi
f	Fast Call	Iof
v	Verifier	Iov

List Head States

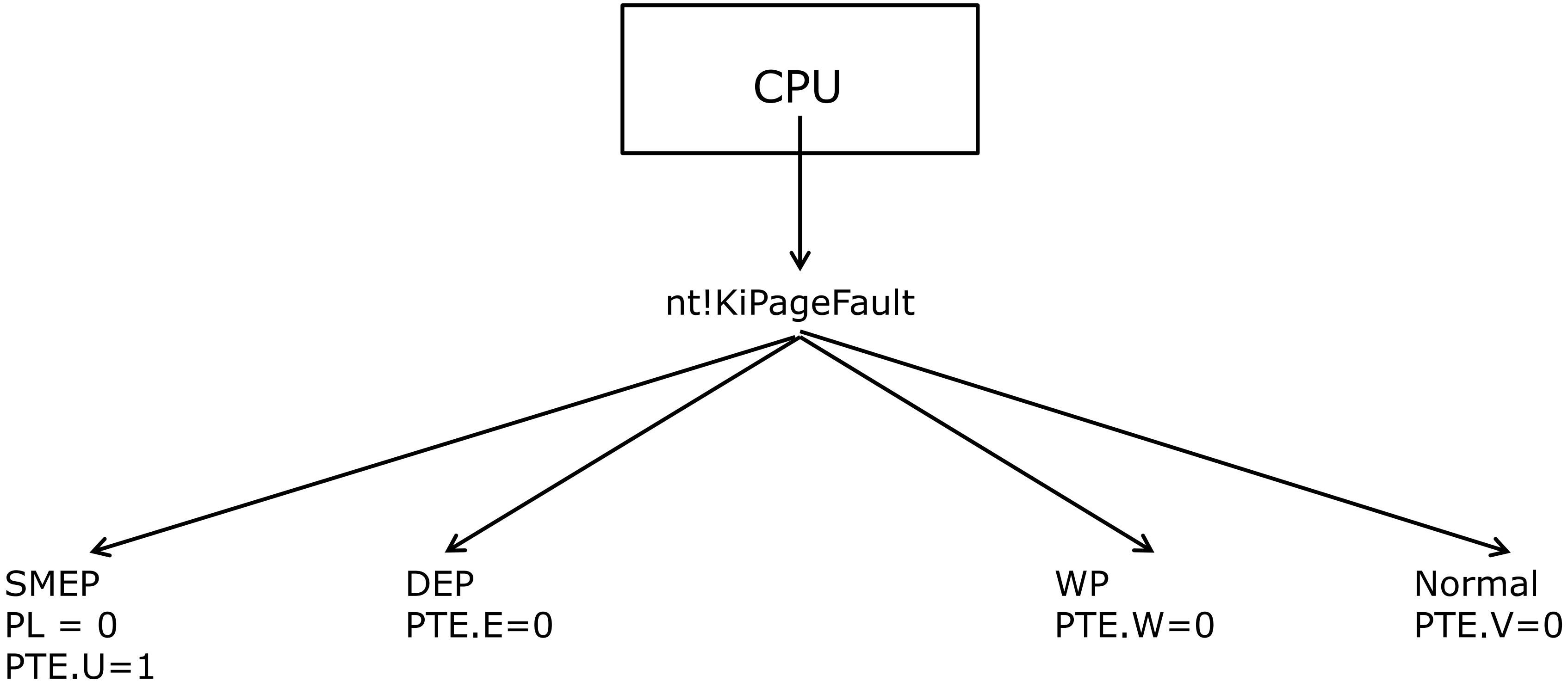


Empty List



List with single node

Page Faults and Violations



CPU

nt!KiPageFault

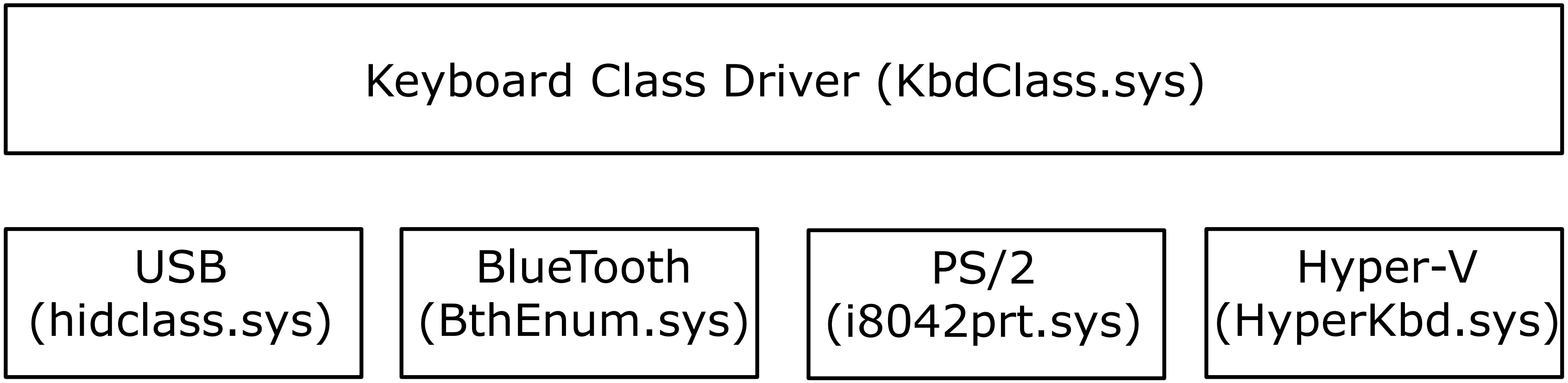
SMEP
PL = 0
PTE.U=1

DEP
PTE.E=0

WP
PTE.W=0

Normal
PTE.V=0

Keyboard Class Driver



Keyboard Class Driver (KbdClass.sys)

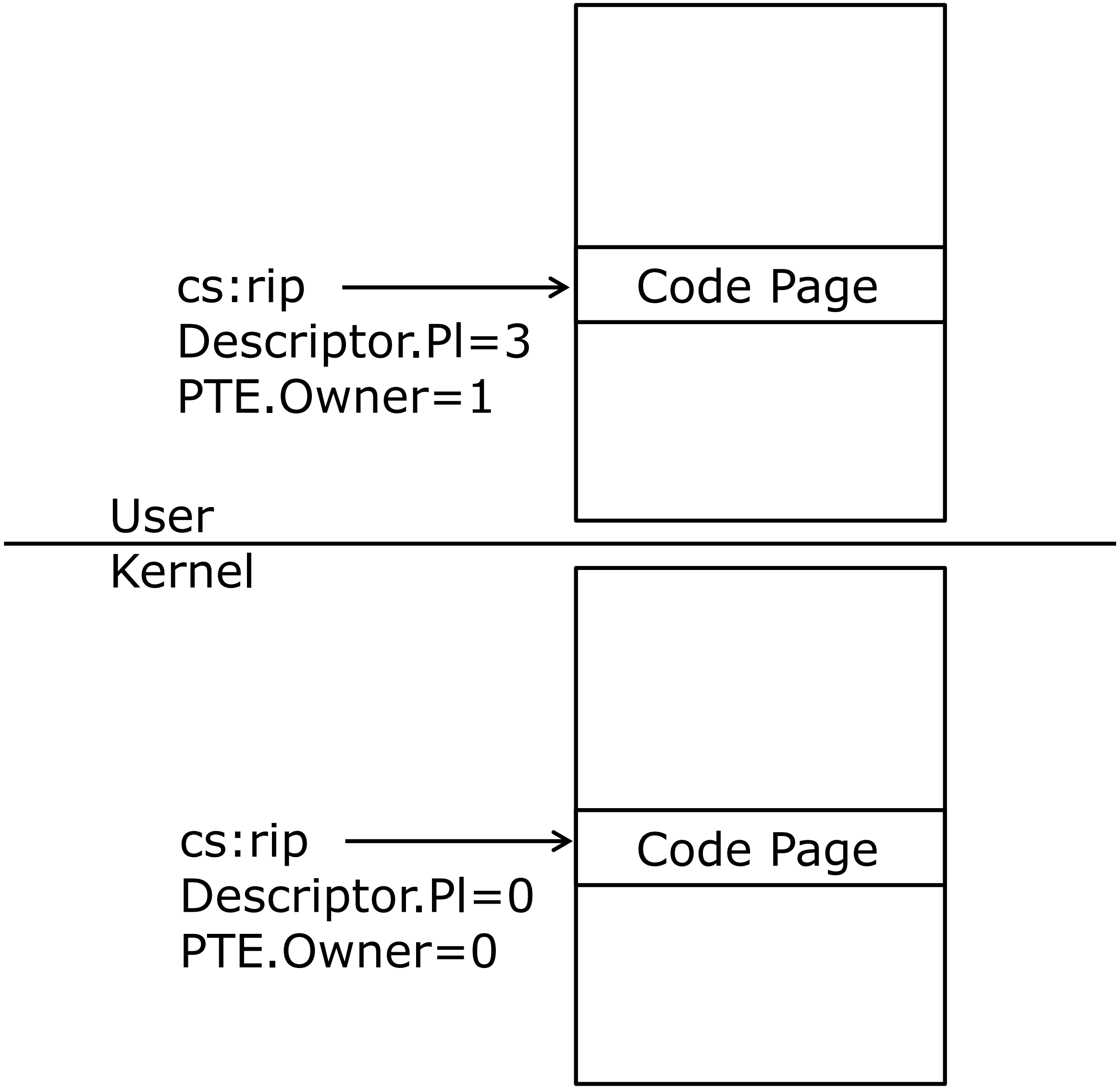
USB
(hidclass.sys)

BlueTooth
(BthEnum.sys)

PS/2
(i8042prt.sys)

Hyper-V
(HyperKbd.sys)

User vs Kernel Mode



cs:rip

Descriptor.Pl=3

PTE.Owner=1

User

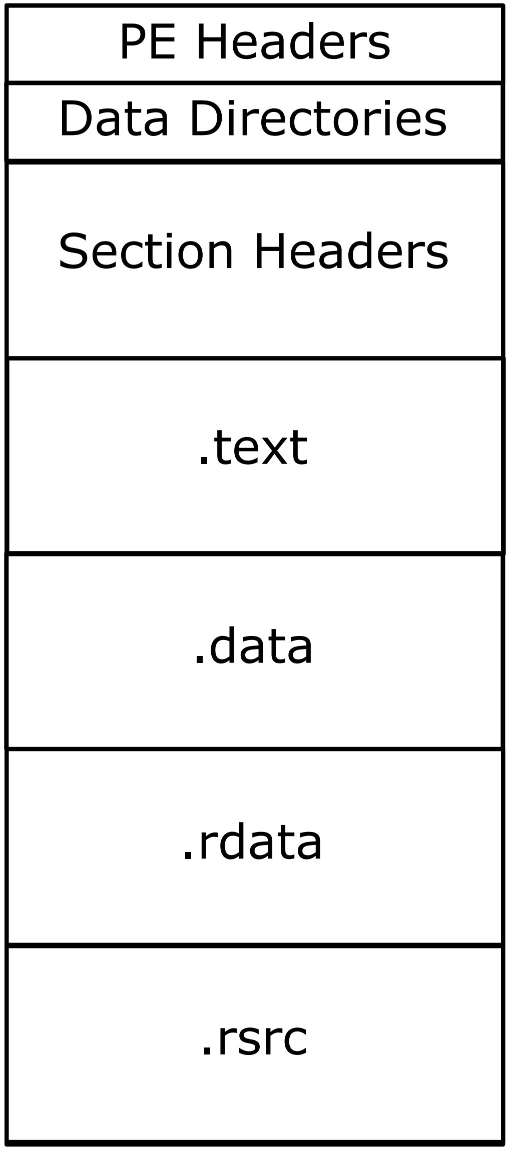
Kernel

cs:rip

Descriptor.Pl=0

PTE.Owner=0

PE File Layout



PE Headers

Data Directories

Section Headers

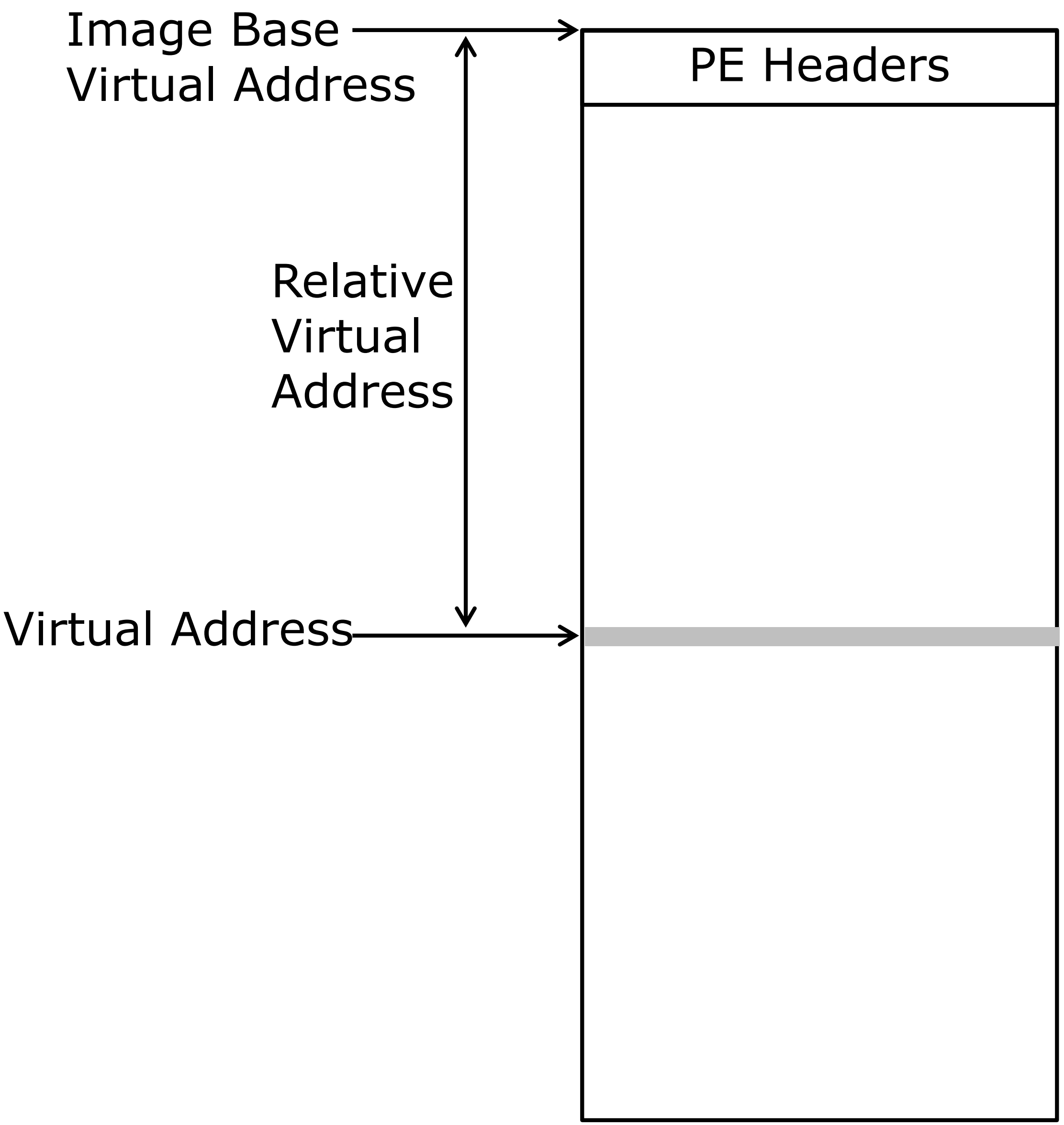
.text

.data

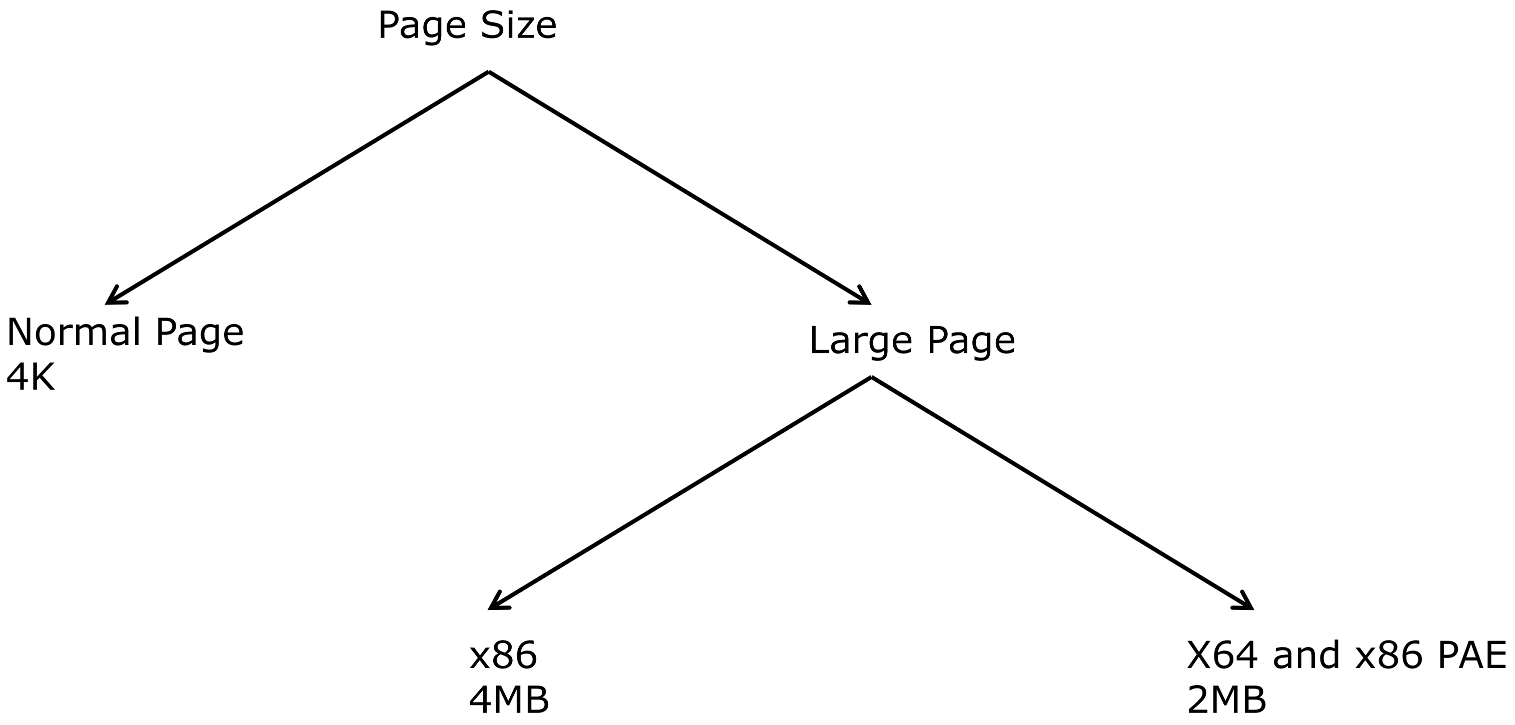
.rdata

.rsrc

Relative Virtual Address (RVA)



Page Sizes



Page Size

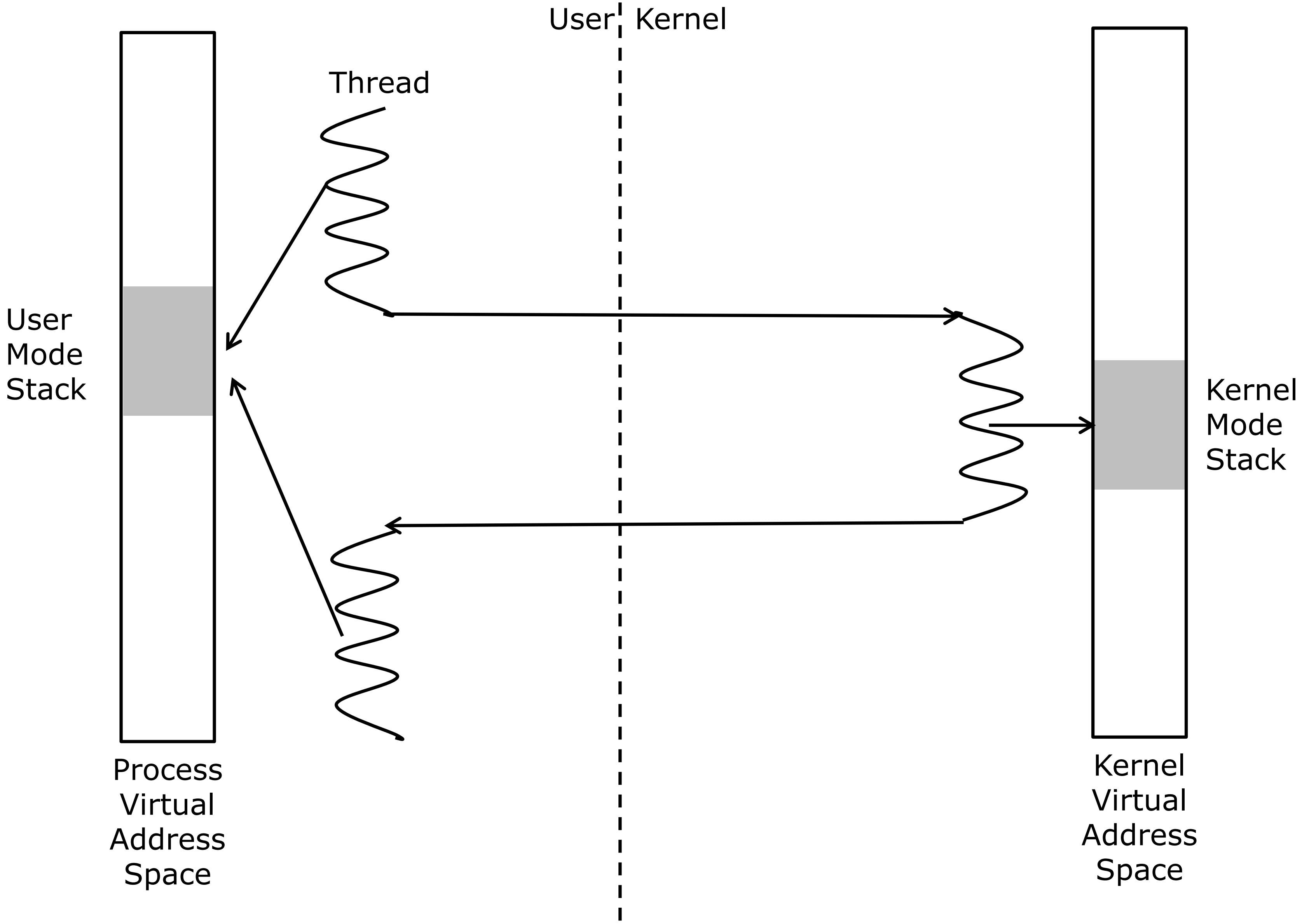
Normal Page
4K

Large Page

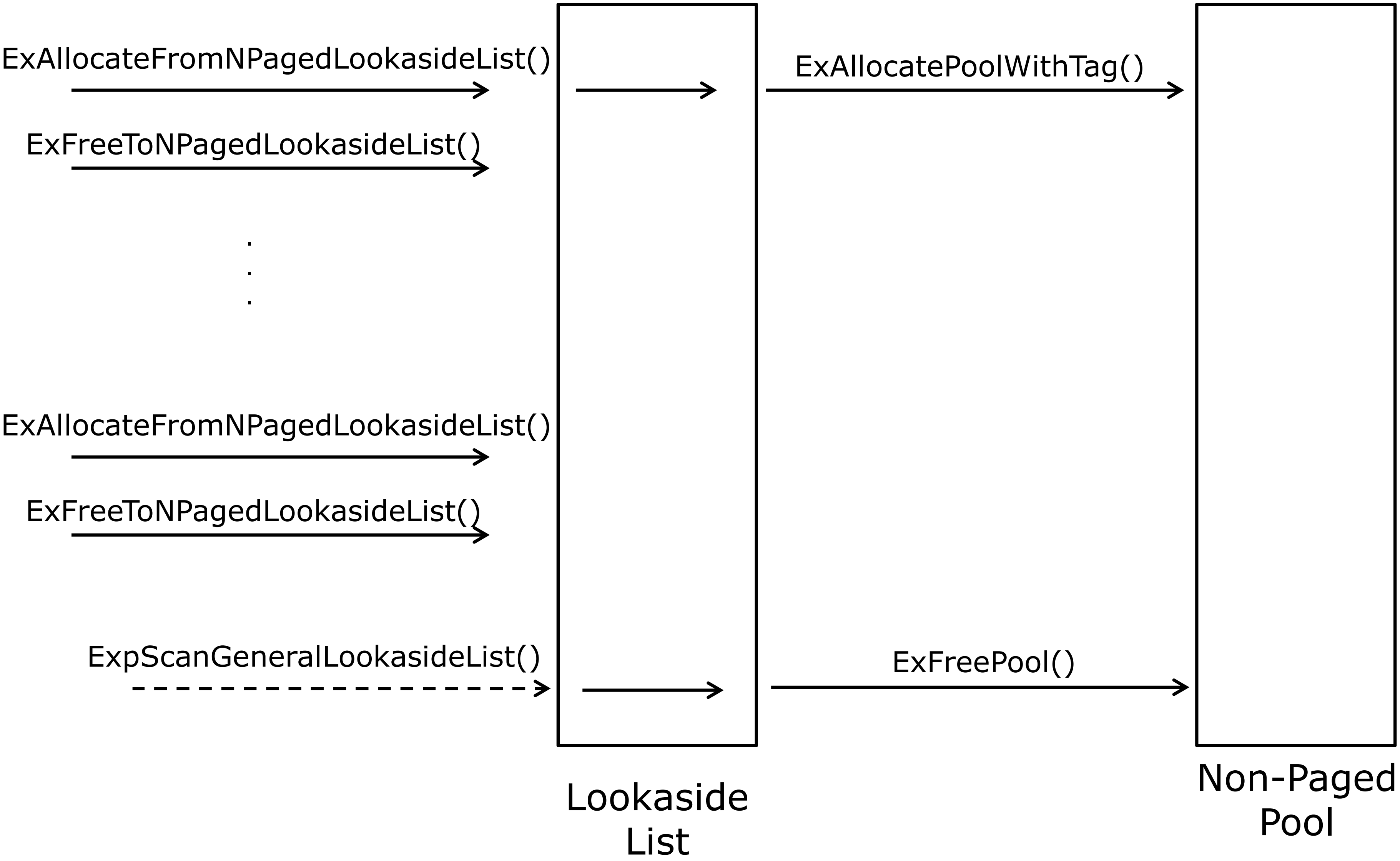
x86
4MB

X64 and x86 PAE
2MB

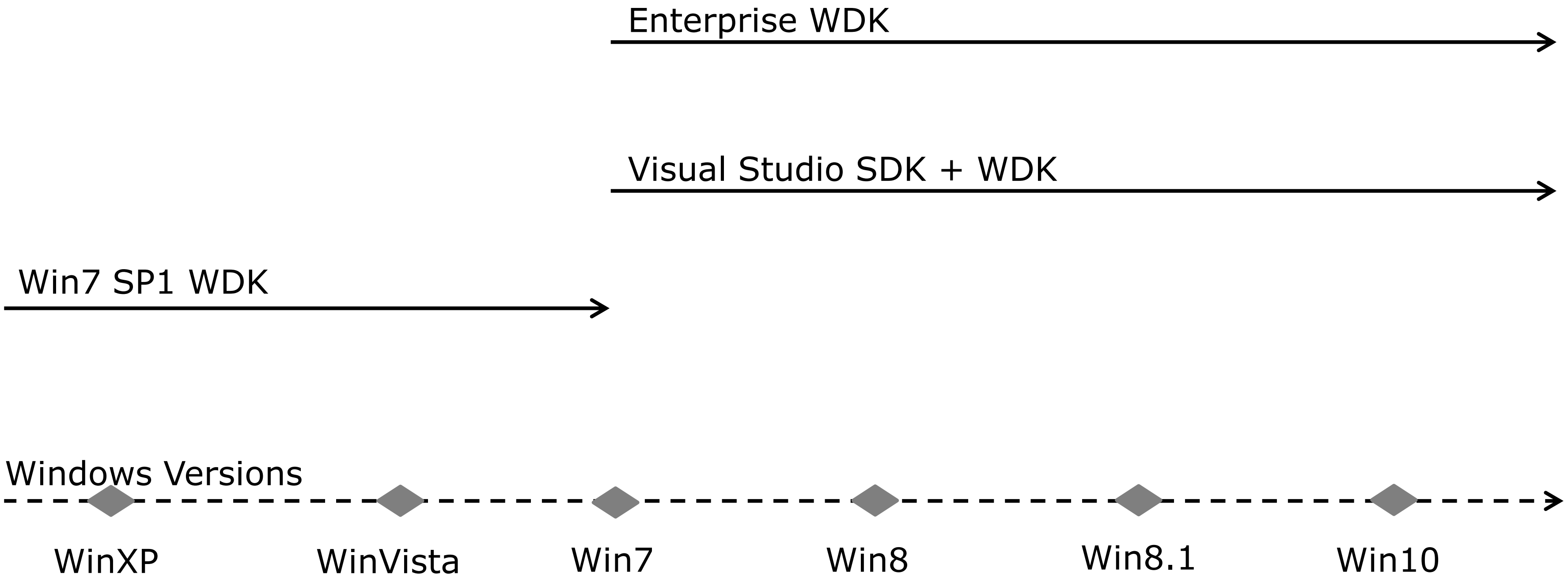
User and Kernel Mode Stack Usage



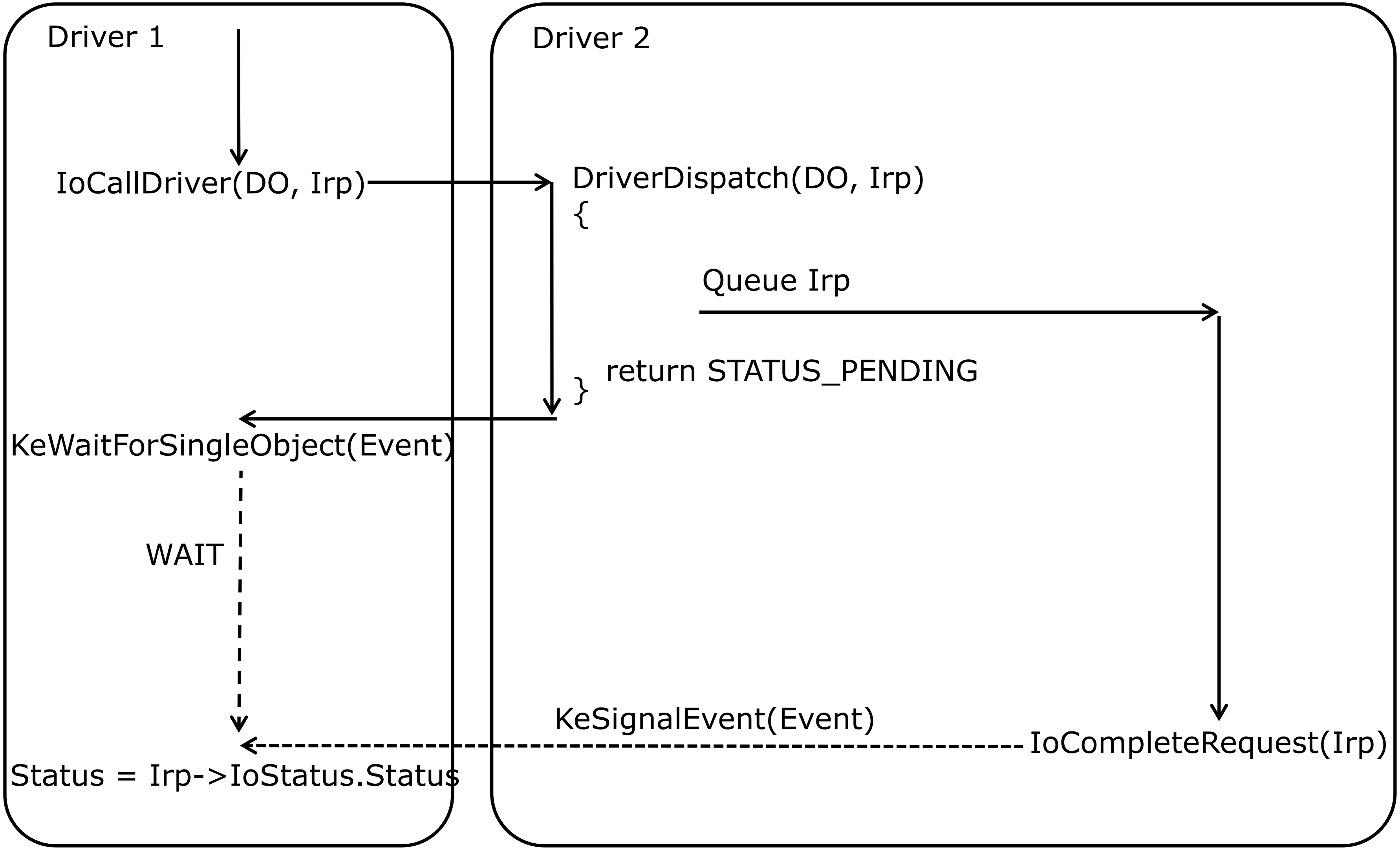
Lookaside Lists


ExAllocateFromNPagedLookasideList()
ExFreeToNPagedLookasideList()
. . .
ExAllocateFromNPagedLookasideList()
ExFreeToNPagedLookasideList()
ExpScanGeneralLookasideList()
ExAllocatePoolWithTag()
ExFreePool()
Lookaside List
Non-Paged Pool

Windows Driver Kit and OS support



Synchronous Driver Call



Driver 1

IoCallDriver(DO, Irp)

KeWaitForSingleObject(Event)

WAIT

Status = Irp->IoStatus.Status

Driver 2

DriverDispatch(DO, Irp)
{

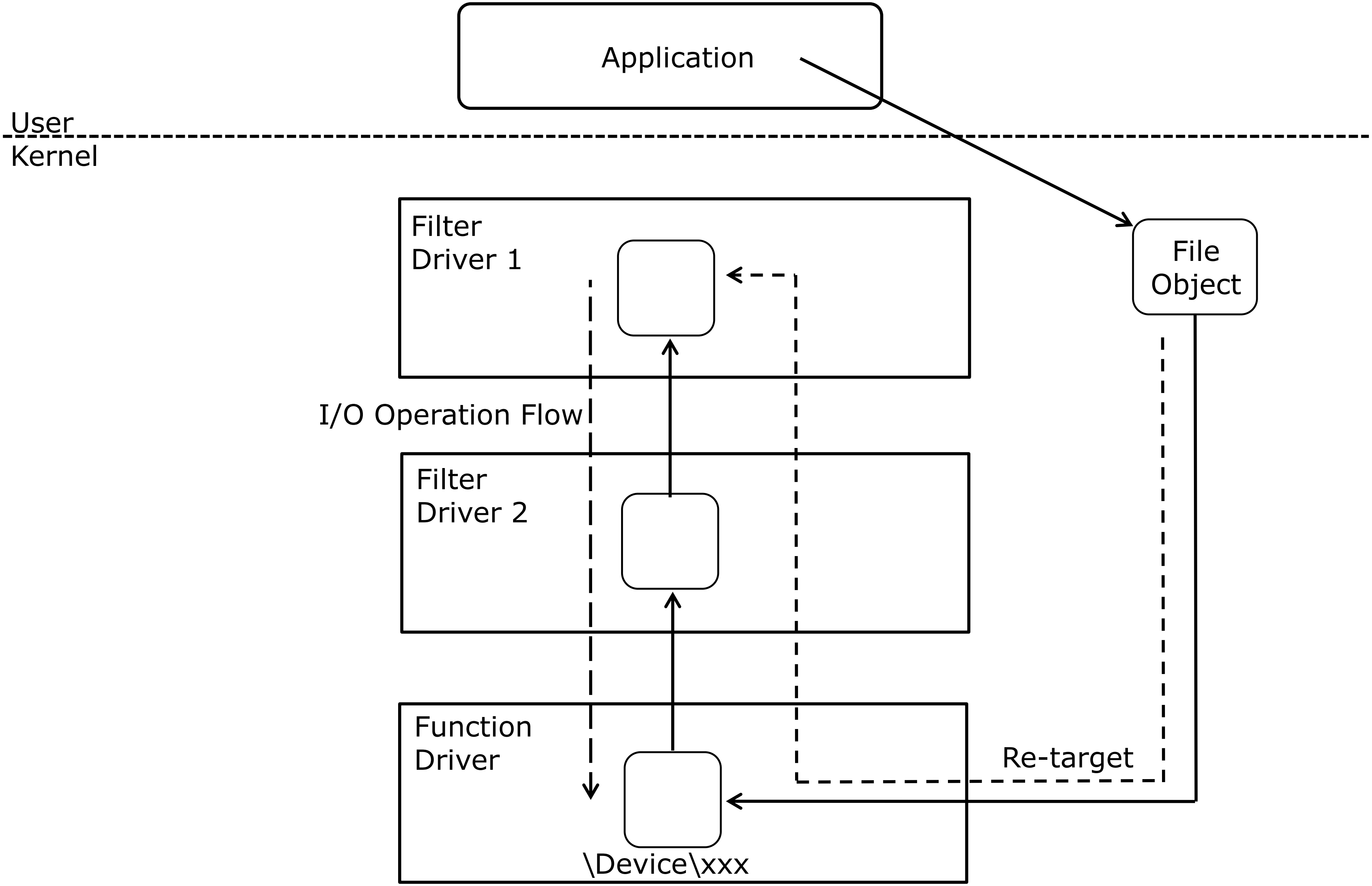
Queue Irp

return STATUS_PENDING
}

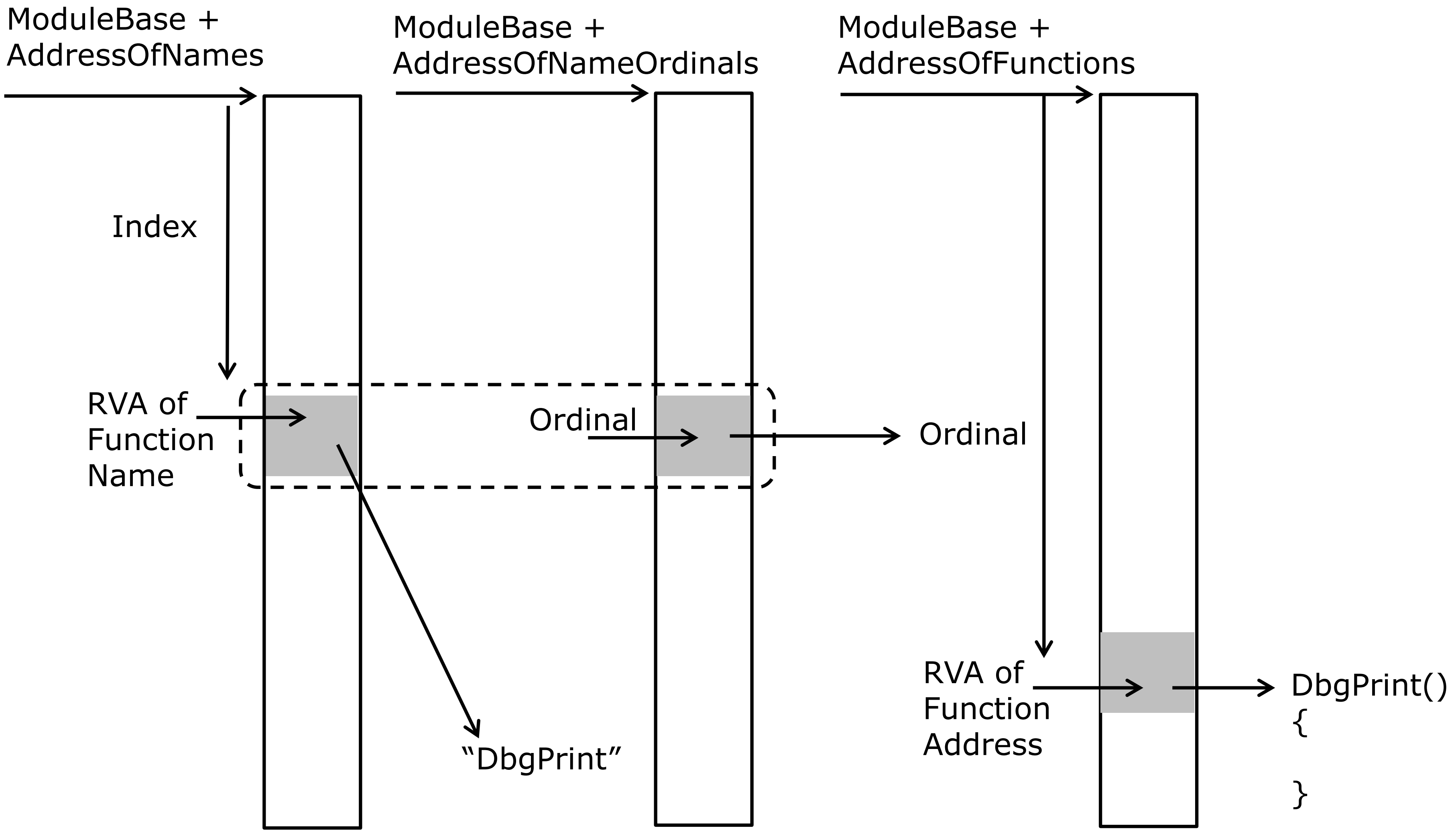
KeSignalEvent(Event)

IoCompleteRequest(Irp)

Filtering Process



Export Table


ModuleBase + AddressOfNames
ModuleBase + AddressOfNameOrdinals
ModuleBase + AddressOfFunctions
Index
RVA of Function Name
Ordinal
Ordinal
"DbgPrint"
RVA of Function Address
DbgPrint()
{
}