

# Windows Kernel Source Internals

- Windows Kernel Hacker Device Driver Writer . -

1. 2004 7 4 . 1 .

:  
: [alphamcu@hanmail.net](mailto:alphamcu@hanmail.net)  
: <http://www.zap.pe.kr> ( )

# 1) Windows Kernel Source Internals ...

'Windows Kernel Source Internals' 2004 2 12 Windows 2000

1. 가
2. Windows Kernel(ntoskrnl.exe)  
 ( private/ntos/ .) ntoskrnl.exe  
export table ,
3. i386  
Hardware-Dependent 가  
i386  
e-Mail 가

## 2) Windows Kernel Source

Windows

가

### 1. Prefix

Prefix

ExAllocatePool

Prefix Ex

Executive

NtCreateFile

Io Prefix

I/O Manager

, Nt Zw

Prefix

(i386)

Prefix

### 2.

or 'global'

, Executive

'Prefix' + 'data'

가

'exdata.c'

'exglobal.c'

extern

가

### 3.

't' 가

Executive Lock

'tlock.c' 가

'u' 가

Usermode

Ring3

Undocumented

### 3) Windows Kernel Source

Windows 가 가

..

#### 1.

Windows 가 ,

4 5

( Tree )

가 77

#### 2. try exception

Windows NT try exception

( ),

#### 3. Windows Kernel ?

i386 Macro/Inline/Debugging

5700 가 Windows Kernel(ntoskrnl.exe)

Memory Manager가 1000 가 1/5 ,

I/O Manager, Runtime Library Kernel Debugger 가 10

가

4)

Private/ntos  
ntoskrnl.exe

가

### 1. PnP Resource Arbiter

:  
private/ntos/arb  
:  
I/O Manager가 . Arbiter가  
가 ,  
. Arbiter , ntoskrnl.exe export ,

### 2. Chache Manager

:  
private/ntos/cache  
:  
Filesystem Data-Caching  
,  
. Cache Manager Memory Manager

### 3. Configuration Manager

:  
private/ntos/config  
:  
Device Driver / /  
. App 'setupapi.h' Include  
(SetupDiXXXXX)

#### 4. KernelMode Debugger Support Routines

:  
private/ntos/dbgk

#### 5. Executive

:  
private/ntos/ex

가

/ /

#### 6. Filesystem Runtime Library

:  
private/ntos/fsrtl

Runtime Library 가

Passive

가

, Ndis 가

(

NdisAcquireSpinLock

ExAcquireSpinLock

.)

Ndis

'ntoskrnl.exe'

export

DDK

, IFS

가

#### 7. Default HAL Handler Routines

:  
private/ntos/fstub

(DMA)

## 8. I/O Management System

:

private/ntos/io

:

가

.

,

,

.

PnP

Arbiter

.

## 9. KernelMode Debugger APIs

:

private/ntos/kd

:

.

## 10. Kernel Routines

:

private/ntos/ke

:

/

## 11. LPC(Local Procedure Call)

:

private/ntos/lpc

:

Object Manager

Inter-Process

가

LPC

가

. Socket

,

Undocumented

Process

Usermode Application

Kernelmode Driver

, Usermode

App

Win32 Subsystem,

Win32 Subsystem

Kernel

## 12. Memory Management

:

private/ntos/mm

:

Pageable/Nonpageable , Code/Data Section . Virtual/Physical Address, 가 가 .

## 13. Object Manager

:

private/ntos/ob

:

가 .

Object Manager . , , .

## 14. Process Manager

:

private/ntos/ps

:

Job Process/Thread , 가 . , (Token), PEB/TEB .

## 15. Runtime Library

:

private/ntos/rtl

:

. Unicode/Ansi .



## 16. Security Manager

:  
private/ntos/se  
:  
(Descriptor)  
, Logon Access Token ,  
Process가 (Privilege)

## 17. VDM(Virtual DOS Machine) Manager

:  
private/ntos/vdm  
:  
DOS/Windows 9X DOS Win16  
. Win9X , 가 VM(Virtual Machine)  
Thread( Process) . ( 16  
) , 가 Request  
, VDM .

## 5)

```
#####  
#                               private/ntos/arb                               #  
#####
```

Abstract :

This module contains support routines for the Pnp resource arbiters.

Prefix :

Arb

Registry Keys :

HKLM\System\CurrentControlSet\Control\Arbiters

Files :

arbp.h

arbiter.c

debug.c

arbp.h :

nothing special.

debug.c : only for debug mode

ArbpDumpArbiterInstance

ArbpDumpArbiterRange

ArbpDumpArbitrationList

arbiter.c :

ArbpWstrToUnicodeString

ArbInitializeArbiterInstance

ArbReferenceArbiterInstance

ArbDereferenceArbiterInstance

ArbDeleteArbiterInstance

ArbTestAllocation

ArbpBuildAlternative

ArbpBuildAllocationStack

ArbSortArbitrationList

ArbCommitAllocation

ArbRollbackAllocation

ArbRetestAllocation

ArbBootAllocation

ArbArbiterHandler  
ArbBuildAssignmentOrdering  
ArbFindSuitableRange  
ArbAddAllocation  
ArbBacktrackAllocation  
ArbPreprocessEntry  
ArbAllocateEntry  
ArbGetNextAllocationRange  
ArbpGetRegistryValue  
ArbInitializeOrderingList  
ArbCopyOrderingList  
ArbAddOrdering  
ArbPruneOrdering  
ArbFreeOrderingList  
ArbOverrideConflict  
ArbpUpdatePriority  
ArbAddReserved  
ArbpQueryConflictCallback  
ArbQueryConflict  
ArbStartArbiter  
ArbpIndent

#####

# private/ntos/arcinst #

#####

Comment :

.

#####

# private/ntos/cache #

#####

Abstract :

The Memory Management based cache management routines for the common Cache subsystem.

Prefix :

Cc

Acronym :

vacb (Virtual Address Control Block)

bcb (Buffer Control Block)

Files :

cc.h

cachedat.c

cachesub.c

copysup.c

fssup.c

lazyrite.c

logsup.c

mdlup.c

pinsup.c

vacbsup.c

cc.h :

CcAcquireMasterLock

CcReleaseMasterLock

CcAcquireMasterLockAtDpcLevel

CcReleaseMasterLockFromDpcLevel

CcAcquireVacbLock

CcReleaseVacbLock

CcAcquireVacbLockAtDpcLevel

CcReleaseVacbLockFromDpcLevel

CcBugCheck

GetBcbListHead

CcLockVacbLevel

CcUnlockVacbLevel

CcAddToLog

CcIncrementOpenCount

CcDecrementOpenCount

GetActiveVacb

GetActiveVacbAtDpcLevel

SetActiveVacb

CcAllocateWorkQueueEntry

CcFreeWorkQueueEntry

CcAllocateVacbLevel

CcDeallocateVacbLevel

VacbLevelReference

IsVacbLevelReferenced

cachedat.c :

cache manager가

가

.

cachesub.c :

CcPinFileData

CcUnpinFileData

CcSetReadAheadGranularity

CcScheduleReadAhead

CcPerformReadAhead

CcFindBitmapRangeToDirty

CcFindBitmapRangeToClean

CcSetDirtyInMask

CcSetDirtyPinnedData

CcSetValidData

CcAcquireByteRangeForWrite

CcReleaseByteRangeFromWrite

CcWriteBehind

CcGetFlushedValidData

CcFlushCache

CcRemapBcb

CcRepinBcb

CcUnpinRepinnedBcb

CcFindBcb

CcAllocateInitializeBcb

CcDeallocateBcb

CcMapAndRead

CcFreeActiveVacb

CcMapAndCopy

CcLogError

CcDump

copysup.c :

CcCopyRead

CcFastCopyRead

CcCopyWrite

CcFastCopyWrite  
CcCopyReadExceptionFilter  
CcCanIWrite  
CcDeferWrite  
CcPostDeferredWrites

fssup.c :

IsSyscacheFile  
CcInitializeCacheManager  
CcInitializeCacheMap  
CcUninitializeCacheMap  
CcDeleteSharedCacheMap  
CcSetFileSizes  
CcPurgeAndClearCacheSection  
CcPurgeCacheSection  
CcUnmapAndPurge  
CcDeleteMbcB  
CcSetDirtyPageThreshold  
CcZeroEndOfLastPage  
CcZeroData  
CcGetFileObjectFromSectionPtrs  
CcGetFileObjectFromBcb

lazyrite.c :

CcScheduleLazyWriteScan  
CcScanDpc  
CcWaitForCurrentLazyWriterActivity  
CcLazyWriteScan  
CcExceptionFilter  
CcPostWorkQueue  
CcWorkerThread

logsup.c :

CcSetAdditionalCacheAttributes  
CcSetLogHandleForFile  
CcGetDirtyPages  
CcIsThereDirtyData  
CcGetLsnForFileObject

mdlup.c :

CcMdlRead  
CcMdlReadComplete  
CcMdlReadComplete2  
CcPrepareMdlWrite  
CcMdlWriteComplete  
CcMdlWriteComplete2

pinsup.c :

SetCallersAddress  
CcMapData  
CcPinMappedData  
CcPinRead  
CcPreparePinWrite  
CcUnpinData  
CcSetBcbOwnerPointer  
CcUnpinDataForThread  
CcAllocateOcbcb

```
#####  
#                               private/ntos/config                               #  
#####
```

Abstract :

Config Manager

Prefix :

Cm  
Hv

Files :

i386/geninst.c  
i386/geninst.h  
i386/init386.c  
i386/initdat.c  
i386/parseini.c  
i386/parseini.h  
i386/rules.c  
i386/rules.h  
cmapi2.c  
cmapi.c

cmboot.c  
cmchek2.c  
cmchek.c  
cmclose.c  
cmconfig.c  
cmcontrl.c  
cmdat2.c  
cmdat3.c  
cmdat.c  
cmdatini.c  
cmdelete.c  
cmgquota.c  
cmhvlist.c  
cmindex.c  
cminit.c  
cmname.c  
cmnotify.c  
cmp.h  
cmparse2.c  
cmparse.c  
cmplock.h  
cmquery.c  
cmsvres.c  
cmse.c  
cmsubs2.c  
cmsubs3.c  
cmsubs.c  
cmsysini.c  
cmtrecpy.c  
cmtredel.c  
cmtree.c  
cmworker.c  
cmwrapr2.c  
cmwrapr.c  
hive.h  
hivebin.c



hivecell.c  
hivechek.c  
hivefree.c  
hiveinit.c  
hiveload.c  
hivemap.c  
hivesum.c  
hivesync.c  
hwprofil.c  
ntapi.c

i386/geninst.c :

CmpGenInstall  
CmpProcessReg  
CmpProcessAddRegLine  
CmpProcessDelRegLine  
CmpProcessBitRegLine  
CmpGetAddRegInfData  
CmpOpenRegKey  
CmpAppendStringToMultiSz

i386/geninst.h :

nothing special

i386/init386.c :

CmpGetBiosDate  
CmpGetBiosVersion  
CmpInitializeMachineDependentConfiguration  
CmpPerformMachineIdentification

i386/initdat.c :

i386/parseini.c :

CmpAppendSection  
CmpAppendLine  
CmpAppendValue  
CmpGetToken  
CmpParseInfBuffer  
CmpProcessForSimpleStringSub  
CmpFreeValueList

CmpFreeLineList  
CmpFreeSectionList  
CmpSearchValueInLine  
CmpSearchSectionByName  
CmpSearchLineInSectionByIndex  
CmpOpenInfFile  
CmpCloseInfFile  
CmpSearchInfSection  
CmpGetKeyName  
CmpSearchInfLine  
CmpGetSectionLineIndex  
CmpGetSectionLineIndexValueCount  
CmpGetIntField  
CmpGetBinaryField

i386/parseini.h :

nothing special

i386/rules.c :

TABLE\_ENTRIES\_FROM\_RSDT\_POINTER  
CmpMatchInfList  
CmpMatchDescription  
CmpMatchDateRule  
CmpMatchMemoryRule  
CmpMatchSearchRule  
CmpMatchNextMatchRule  
CmpMatchPointerRule  
CmpMatchOemIdRule  
CmpMatchPModeRule  
CmpMatchRmPmSameRule  
CmpMatchInstallRule  
CmpMatchAcpiOemIdRule  
CmpMatchAcpiOemTableIdRule  
CmpMatchAcpiOemRevisionRule  
CmpMatchAcpiRevisionRule  
CmpMatchAcpiCreatorRevisionRule  
CmpMatchAcpiCreatorIdRule  
CmpGetInfData

CmpMapPhysicalAddress  
CmpCheckOperator  
CmpFindPattern  
CmpGetPnPBIOSTableAddress  
CmpFindACPI Table  
CmpFindRSDTTable  
CmpGetRegistryValue

i386/rules.h :

nothing special

cmapi2.c :

CmDeleteKey

cmapi.c :

CmDeleteValueKey

CmEnumerateKey

CmEnumerateValueKey

CmFlushKey

CmQueryKey

CmQueryValueKey

CmQueryMultipleValueKey

CmSetValueKey

CmpSetValueKeyExisting

CmpSetValueKeyNew

CmSetLastWriteTimeKey

CmLoadKey

CmpUnloadKeyWorker

CmUnloadKey

CmpDoFlushAll

CmReplaceKey

CmpMarkAllBinsReadOnly

cmboot.c :

CmpFindNLSData

CmpFindDrivers

CmpIsLoadType

CmpAddDriverToList

CmpSortDriverList

CmpDoSort



CmQueryRegistryQuotaInformation  
CmSetRegistryQuotaInformation  
CmpQuotaWarningWorker  
CmpClaimGlobalQuota  
CmpReleaseGlobalQuota  
CmpComputeGlobalQuotaAllowed  
CmpSetGlobalQuotaAllowed

cmhvlst.c :

CmpAddToHiveFileList  
CmpRemoveFromHiveFileList  
CmpGetHiveName

cmindex.c :

CmpFindSubKeyByName  
CmpFindSubKeyInRoot  
CmpFindSubKeyInLeaf  
CmpCompareInIndex  
CmpDoCompareKeyName  
CmpFindSubKeyByNumber  
CmpDoFindSubKeyByNumber  
CmpAddSubKey  
CmpAddToLeaf  
CmpSelectLeaf  
CmpSplitLeaf  
CmpMarkIndexDirty  
CmpRemoveSubKey

cminit.c :

CmpOpenHiveFiles  
CmpInitializeHive  
CmpDestroyHive  
CmpOpenFileWithExtremePrejudice

cmname.c :

CmpNameSize  
CmpCopyName  
CmpCompressedNameSize  
CmpCopyCompressedName  
CmpCompareCompressedName

cmnotify.c :

CmpCheckPostBlock  
CmpDummyApc  
CmpReportNotify  
CmpNotifyTriggerCheck  
CmpReportNotifyHelper  
CmpPostNotify  
CmpPostApc  
CmpPostApcRunDown  
CmNotifyRunDown  
CmpFlushNotify  
CmpNotifyChangeKey  
CmpFreeSlavePost  
CmpCancelSlavePost  
CmpAddToDelayedDeref  
CmpDelayedDerefKeys

cmp.h :

CmpRemoveEntryList  
CmpClearListEntry  
CmpWmiFireEvent  
StartWmiCmTrace  
EndWmiCmTrace  
CmpMakeSpecialPoolReadOnly  
CmpMakeSpecialPoolReadWrite  
CmpMakeValueCacheReadOnly  
CmpMakeValueCacheReadWrite  
LOCK\_KCB\_TREE  
UNLOCK\_KCB\_TREE  
CMLOG  
DCmCheckRegistry  
ASSERT\_PASSIVE\_LEVEL  
CM\_BUGCHECK  
VALIDATE\_CELL\_MAP  
CmpDumpSecurityDescriptor  
HASH\_KEY  
GET\_HASH\_INDEX

GET\_HASH\_ENTRY  
INIT\_KCB\_KEYBODY\_LIST  
ASSERT\_KEYBODY\_LIST\_EMPTY  
ENLIST\_KEYBODY\_IN\_KEYBODY\_LIST  
DELIST\_KEYBODY\_FROM\_KEYBODY\_LIST  
ASSERT\_KEY\_OBJECT  
ASSERT\_NODE  
ASSERT\_SECURITY  
PostBlockType  
IsMasterPostBlock  
SetMasterPostBlockFlag  
ClearMasterPostBlockFlag  
LOCK\_POST\_LIST  
UNLOCK\_POST\_LIST  
CmLockHive  
CmUnlockHive  
CmpHKeyNameLen  
CmpNcbNameLen  
CmpHKeyNodeSize  
CmpValueNameLen  
CmpHKeyValueSize  
CmpLockRegistry  
CmpLockRegistryExclusive  
CmpFindValueByName  
CmpCopyTree  
CmpCopyTreeEx  
CmpSyncTrees  
CmpMergeTrees  
CmpAllocateMasterPostBlock  
CmpAllocateSlavePostBlock  
SetUsed  
CmpSetIoStatus

cmparse2.c :

CmpDoCreate  
CmpDoCreateChild

cmparse.c :

CmpStepThroughExit  
CmpParseKey  
CmpGetNextName  
CmpDoOpen  
CmpCreateLinkNode  
CmpGetSymbolicLink  
CmpComputeHashValue  
CmpCacheLookup  
CmpAddInfoAfterParseFailure

cmlock.h :

ASSERT\_CM\_LOCK\_OWNED  
CMP\_LOCK\_REGISTRY  
CMP\_UNLOCK\_REGISTRY  
ASSERT\_REGISTRY\_LOCKED

cmquery.c :

CmpQueryKeyName

cmsavres.c :

CmRestoreKey  
CmpLoadHiveVolatile  
CmpRefreshWorkerRoutine  
CmpRefreshHive  
CmSaveKey  
CmSaveMergedKeys  
CmpSaveKeyByFileCopy  
CmpCreateTemporaryHive  
CmpDestroyTemporaryHive

cmse.c :

SECURITY\_CELL\_LENGTH  
CmpSecurityExceptionFilter  
CmpSecurityMethod  
CmpSetSecurityDescriptorInfo  
CmpAssignSecurityDescriptor  
CmpQuerySecurityDescriptorInfo  
CmpCheckCreateAccess  
CmpCheckNotifyAccess  
CmpGetObjectSecurity



CmpGetKeySecurity  
CmpHiveRootSecurityDescriptor  
CmpFreeSecurityDescriptor  
CmpFindMatchingDescriptorCell  
CmpInsertSecurityCellList  
CmpRemoveSecurityCellList

cmsubs2.c :

ALIGN\_OFFSET  
ALIGN\_OFFSET64  
CmpFreeValue  
CmpQueryKeyData  
CmpGetValueDataFromCache  
CmpQueryKeyValueData

cmsub3.c :

CmpLockRegistry  
CmpLockRegistryExclusive  
CmpUnlockRegistry  
CmpTestRegistryLock  
CmpTestRegistryLockExclusive

cmsubs.c :

CmpDumpKeyBodyList  
CmpFlushNotifiesOnKeyBodyList  
CmpSearchForOpenSubKeys  
CmpReferenceKeyControlBlock  
CmpGetNameControlBlock  
CmpDereferenceNameControlBlockWithLock  
CmpCleanupSubKeyInfo  
CmpCleanupKcbValueCache  
CmpCleanupKcbCacheWithLock  
CmpConstructName  
CmpRemoveFromDelayedClose  
CmpCreateKeyControlBlock  
CmpSearchKeyControlBlockTree  
CmpDereferenceKeyControlBlock  
CmpDereferenceKeyControlBlockWithLock  
CmpRemoveKeyControlBlock

CmpFreeKeyBody  
CmpInsertKeyHash  
CmpRemoveKeyHash  
CmpInitializeCache

cmsysini.c :

CmInitSystem1  
CmpInitializeHiveList  
CmpCreateObjectTypes  
CmpCreateRegistryRoot  
CmpCreateRootNode  
CmpLinkHiveToMaster  
CmpSetVersionData  
CmpInterlockedFunction  
CmpConfigureProcessors  
CmpInitializeSystemHive  
CmGetSystemDriverList  
CmpFreeDriverList  
CmpInitHiveFromFile  
CmpAddDockingInfo  
CmpAddAliasEntry  
CmpHwprofileDefaultSelect  
CmpCreateControlSet  
CmpCloneControlSet  
CmpSaveBootControlSet  
CmpDeleteCloneTree  
CmBootLastKnownGood  
CmpIsLastKnownGoodBoot  
CmShutdownSystem  
CmpLinkKeyToHive  
CmpValidateAlternate  
CmpCreatePerfKeys  
CmpCreatePredefined

cmtrecpy.c :

CmpCopySyncTree  
CmpCopySyncTree2  
CmpCopyKeyPartial

- CmpCopyValue
- CmpCopyCell
- CmpFreeKeyValues
- CmpMergeKeyValues
- CmpSyncKeyValues
- CmpInitializeKeyNameString
- CmpInitializeValueNameString
- CmpSyncSubKeysAfterDelete
- CmpMarkKeyValuesDirty
- CmpMarkKeyParentDirty

cmtredel.c :

- CmpDeleteTree
- CmpFreeKeyByCell
- CmpMarkKeyDirty

cmtree.c :

- CmpFindNameInList
- CmpGetValueListFromCache
- CmpGetValueKeyFromCache
- CmpFindValueByNameFromCache

cmworker.c :

- CmpWorker
- CmpLazyFlush
- CmpLazyFlushDpcRoutine
- CmpLazyFlushWorker
- CmpDiskFullWarningWorker
- CmpDiskFullWarning

cmwrapr2.c :

- CmpFileSetSize

cmwrapr.c :

- CmpAllocate
- CmpAllocateTag
- CmpFree
- CmpDoFileSetSize
- CmpCreateEvent
- CmpFileRead
- CmpFileWrite

```
    CmpFileFlush
hive.h :
    DhvCheckHive
    DhvCheckBin
    ROUND_UP
    ASSERT_LISTENTRY
    HvGetCell
    HvpGetHCell
hivebin.c :
    HvpAddBin
    HvpCoalesceDiscardedBins
hivecell.c :
    HvpComputeIndex
    HvpAdjustCellSize
    HvpGetCellPaged
    HvpGetCellFlat
    HvpGetCellMap
    HvGetCellSize
    HvAllocateCell
    HvpDoAllocateCell
    HvFreeCell
    HvpIsFreeNeighbor
    HvpEnlistFreeCell
    HvpDelistFreeCell
    HvReallocateCell
    HvpIsCellAllocated
    HvpDelistBinFreeCells
hivechek.c :
    HvCheckHive
    HvCheckBin
hivefree.c ;
    HvFreeHive
    HvFreeHivePartial
hiveinit.c :
    HvpDumpFreeDisplay
    HvpFreeAllocatedBins
```

HvInitializeHive

HvpFillFileName

hiveload.c :

HvLoadHive

HvpReadFileImageAndBuildMap

HvpGetHiveHeader

HvpGetLogHeader

HvpRecoverData

hivemap.c :

HvpBuildMapAndCopy

HvpInitMap

HvpEnlistBinInMap

HvpBuildMap

HvpEnlistFreeCells

HvpCleanMap

HvpFreeMap

HvpAllocateMap

hivesum.c :

HvpHeaderChecksum

hivesync.c :

DumpDirtyVector

HvMarkCellDirty

HvIsBinDirty

HvMarkDirty

HvMarkClean

HvpGrowLog1

HvpGrowLog2

HvSyncHive

HvpDoWriteHive

HvpWriteLog

HvpFindNextDirtyBlock

HvWriteHive

HvRefreshHive

HvpDiscardBins

HvpTruncateBins

HvpChangeBinAllocation

HvpMarkBinReadWrite

hwprofil.c :

CmpGetAcpiProfileInformation

CmpAddAcpiAliasEntry

CmSetAcpiHwProfile

CmpFilterAcpiDockingState

CmpMoveBiosAliasTable

CmpCloneHwProfile

CmDeleteKeyRecursive

CmpCreateHwProfileFriendlyName

ntapi.c :

ALLOCATE\_WITH\_QUOTA

CmpExceptionFilter

CmpCheckLockExceptionFilter

NtCreateKey

NtDeleteKey

NtDeleteValueKey

NtEnumerateKey

NtEnumerateValueKey

NtFlushKey

NtInitializeRegistry

NtNotifyChangeKey

NtNotifyChangeMultipleKeys

NtOpenKey

NtQueryKey

NtQueryValueKey

NtRestoreKey

NtSaveKey

NtSaveMergedKeys

NtSetValueKey

NtLoadKey

NtLoadKey2

NtUnloadKey

NtSetInformationKey

NtReplaceKey

NtQueryMultipleValueKey

CmpNameFromAttributes  
CmpFreePostBlock  
CmpAllocatePostBlock  
CmpExceptionFilter  
CmpEnumKeyObjectCallback  
NtQueryOpenSubKeys

```
#####  
#                               private/ntos/dbgk                               #  
#####
```

Abstract :

KernelMode Portion of the Debug Subsystem

Prefix :

Dbgk

Files :

dbgkp.h  
dbgkport.c  
dbgkproc.c  
udbgk.c

dbgkp.h :

nothing special

dbgkport.c :

DbgkpSendMessage  
DbgkForwardException

dbgkproc.c :

DbgkpSuspendProcess  
DbgkpResumeProcess  
DbgkpSectionHandleToFileHandle  
DbgkCreateThread  
DbgkExitThread  
DbgkExitProcess  
DbgkMapViewOfSection  
DbgkUnMapViewOfSection

udbgk.c :

```
#####  
#                               private/ntos/dll                               #  
#####
```

Comment :

CSR(Client Server Runtime).

```
#####  
#                               private/ntos/ex                               #  
#####
```

Abstract :

Excutive Functions

Prefix :

Ex

Acronym :

LUID(locally unique identifier)

Files :

i386/evpair.asm  
i386/fmutex.asm  
i386/intrlfs.asm  
i386/intrlock.asm  
i386/raisests.asm  
i386/resoura.asm  
i386/splocks.asm  
i386/tickcnt.asm  
callback.c  
callperf.c  
dbgctrl.c  
ddkresrc.c  
delay.c  
event.c  
eventpr.c  
exatom.c  
exdata.c  
exinfo.c  
exp.h  
handle.c



harderr.c  
intrloc2.c  
logger.c  
lookasid.c  
luid.c  
memprint.c  
mutant.c  
pool.c  
poolhack.c  
probe.c  
profile.c  
raise.c  
region.c  
regtest.c  
resource.c  
semphore.c  
spintrac.c  
sysenv.c  
sysinfo.c  
tex.c  
timer.c  
tlock.c  
tprofile.c  
uuid.c  
win32.c  
worker.c  
zone.c

i386/evpair.asm :

NtSetLowWaitHighThread  
NtSetHighWaitLowThread  
NtGetTickCount

i386/fmutex.asm :

ExAcquireFastMutexUnsafe  
ExReleaseFastMutexUnsafe  
ExTryToAcquireFastMutexUnsafe

i386/intrlfst.asm :

ExInterlockedAddLargeStatistic  
ExInterlockedAddUlong  
ExInterlockedInsertHeadList  
ExInterlockedInsertTailList  
ExInterlockedRemoveHeadList  
ExInterlockedPopEntryList  
ExInterlockedPushEntryList  
ExInterlockedPopEntrySList  
ExInterlockedPushEntrySList  
ExInterlockedFlushSList  
ExInterlockedPopEntrySList  
ExInterlockedPushEntrySList  
ExInterlockedFlushSList  
Exi386InterlockedIncrementLong  
Exi386InterlockedDecrementLong  
Exi386InterlockedExchangeUlong  
InterlockedIncrement  
InterlockedDecrement  
InterlockedCompareExchange  
ExInterlockedCompareExchange64  
InterlockedExchangeAdd

i386/intrlock.asm :

ExInterlockedAddLargeInteger  
ExInterlockedExchangeAddLargeInteger  
ExInterlockedAddUlong  
ExInterlockedInsertHeadList  
ExInterlockedInsertTailList  
ExInterlockedRemoveHeadList  
ExInterlockedPopEntryList  
ExInterlockedPushEntryList  
ExInterlockedIncrementLong  
ExInterlockedDecrementLong  
ExInterlockedExchangeUlong  
Exi386InterlockedIncrementLong  
ExInterlockedDecrementLong  
Exi386InterlockedExchangeUlong



NtClearEvent  
NtCreateEvent  
NtOpenEvent  
NtPulseEvent  
NtQueryEvent  
NtResetEvent  
NtSetEvent

eventpr.c :

ExpEventPairInitialization  
NtCreateEventPair  
NtOpenEventPair  
NtWaitLowEventPair  
NtWaitHighEventPair  
NtSetLowWaitHighEventPair  
NtSetHighWaitLowEventPair  
NtSetLowEventPair  
NtSetHighEventPair

exatom.c :

NtAddAtom  
NtFindAtom  
NtDeleteAtom  
NtQueryInformationAtom  
ExpGetGlobalAtomTable

exdata.c :

Executive

exinfo.c :

ExpCheckSystemInformation  
ExpCheckSystemInfoWork

exp.h :

nothing special

handle.c :

ExLockHandleTableShared  
ExLockHandleTableExclusive  
ExUnlockHandleTableShared  
ExUnlockHandleTableExclusive  
ExLockHandleTableEntry

ExUnlockHandleTableEntry  
ExInitializeHandleTablePackage  
ExCreateHandleTable  
ExRemoveHandleTable  
ExDestroyHandleTable  
ExEnumHandleTable  
ExDupHandleTable  
ExSnapshotHandleTables  
ExCreateHandle  
ExDestroyHandle  
ExChangeHandle  
ExMapHandleToPointer  
ExpAllocateHandleTable  
ExpFreeHandleTable  
ExpAllocateHandleTableEntry  
ExpFreeHandleTableEntry  
ExpLookupHandleTableEntry

harderr.c :

ExpSystemErrorHandler  
ExpRaiseHardError  
NtRaiseHardError  
ExRaiseHardError  
NtSetDefaultHardErrorPort  
\_purecall

intloc2.c :

ExInterlockedIncrementLong  
ExInterlockedDecrementLong

logger.c :

ExCreateDebugLog  
ExCreateDebugLogTag  
ExDebugLogEvent

lookasid.c :

ExAdjustLookasideDepth  
ExpComputeLookasideDepth  
ExpScanGeneralLookasideList  
ExpScanPoolLookasideList

ExInitializeNPagedLookasideList  
ExDeleteNPagedLookasideList  
ExInitializePagedLookasideList  
ExDeletePagedLookasideList  
ExAllocateFromPagedLookasideList  
ExFreeToPagedLookasideList  
ExpDummyAllocate

luid.c :

ExLuidInitialization  
NtAllocateLocallyUniqueId

memprint.c :

MemPrintInitialize  
MemPrint  
MemPrintFlush  
MemPrintWriteThread  
MemPrintWriteCompleteApc

mutant.c :

ExpDeleteMutant  
ExpMutantInitialization  
NtCreateMutant  
NtOpenMutant  
NtQueryMutant  
NtReleaseMutant

pool.c :

FREE\_CHECK\_ERESOURCE  
FREE\_CHECK\_KTIMER  
FREE\_CHECK\_WORKER  
LOCK\_POOL\_GRANULAR  
UNLOCK\_POOL\_GRANULAR  
DecodeLink  
EncodeLink  
PrivateInitializeListHead  
PrivateIsListEmpty  
PrivateRemoveHeadList  
PrivateRemoveTailList  
PrivateRemoveEntryList

PrivateInsertTailList  
PrivateInsertHeadList  
CHECK\_LIST  
CHECK\_POOL\_HEADER  
ASSERT\_ALLOCATE\_IRQL  
ASSERT\_FREE\_IRQL  
ASSERT\_POOL\_NOT\_FREE  
ASSERT\_POOL\_TYPE\_NOT\_ZERO  
CHECK\_POOL\_PAGE  
ExpAllocateStringRoutine  
ExOkayToLockRoutine  
ENCODE\_POOL\_INDEX  
DECODE\_POOL\_INDEX  
MARK\_POOL\_HEADER\_ALLOCATED  
MARK\_POOL\_HEADER\_FREED  
IS\_POOL\_HEADER\_MARKED\_ALLOCATED  
ExpLockNonPagedPool  
ExpUnlockNonPagedPool  
LOCK\_POOL  
LOCK\_IF\_PAGED\_POOL  
ExLockPool  
UNLOCK\_POOL  
UNLOCK\_IF\_PAGED\_POOL  
ExpUnlockPool  
ExpInitializePoolDescriptor  
InitializePool  
ExpCheckSingleFilter  
ExpAllocatePool  
ExpAllocatePoolWithTagPriority  
ExpAllocatePoolWithTag  
ExpInsertPoolTag  
ExpRemovePoolTag  
ExpInsertPoolTracker  
ExpRemovePoolTracker  
ExpAddTagForBigPages  
ExpFindAndRemoveTagBigPages

ExpAllocatePoolWithQuotaHandler  
ExAllocatePoolWithQuota  
ExAllocatePoolWithQuotaTag  
ExFreePool  
ExFreePoolWithTag  
ExQueryPoolBlockSize  
ExQueryPoolUsage  
ExReturnPoolQuota  
ExpSnapshotPoolPages  
ExSnapshotPool  
ExAllocatePoolSanityChecks  
ExFreePoolSanityChecks

poolhack.c :

LOCK\_POOL  
ExLockPool  
UNLOCK\_POOL  
ExUnlockPool  
InitializePool  
ExAllocatePool  
ExpAllocatePoolWithQuotaHandler  
ExAllocatePoolWithQuota  
AllocatePoolInternal  
ExFreePool  
DeallocatePoolInternal  
DumpPool  
CheckPool  
DumpAllocatedPool  
ExQueryPoolUsage

probe.c :

ProbeForWrite  
ProbeForRead

profile.c :

ExpProfileInitialization  
ExpProfileDelete  
NtCreateProfile  
NtStartProfile



NtStopProfile  
NtSetIntervalProfile  
NtQueryIntervalProfile  
NtQueryPerformanceCounter

raise.c :

ExRaiseAccessViolation  
ExRaiseDatatypeMisalignment

region.c :

ExInitializeRegion  
ExInterlockedExtendRegion

regtest.c :

가

resource.c :

IsExclusiveWaiting  
IsSharedWaiting  
IsOwnedExclusive  
IsBoostAllowed  
ExpIncrementCounter  
ExpResourceInitialization  
ExInitializeResourceLite  
ExReinitializeResourceLite  
ExDisableResourceBoostLite  
ExpAcquireResourceExclusiveLite  
ExAcquireResourceExclusiveLite  
ExTryToAcquireResourceExclusiveLite  
ExAcquireResourceSharedLite  
ExAcquireResourceSharedLite  
ExAcquireSharedStarveExclusive  
ExAcquireSharedStarveExclusive  
ExAcquireSharedWaitForExclusive  
ExReleaseResourceLite  
ExReleaseResourceForThreadLite  
ExSetResourceOwnerPointer  
ExConvertExclusiveToSharedLite  
ExDeleteResourceLite  
ExGetExclusiveWaiterCount

ExGetSharedWaiterCount  
ExIsResourceAcquiredExclusiveLite  
ExIsResourceAcquiredSharedLite  
ExQuerySystemLockInformation  
ExpBoostOwnerThread  
ExpWaitForResource  
ExpFindCurrentThread  
ExpAssertResource  
ExpCheckForResource

semphore.c :

ExpSemaphoreInitialization  
NtCreateSemaphore  
NtOpenSemaphore  
NtQuerySemaphore  
NtReleaseSemaphore

spintrac.c :

nothing special.

sysenv.c :

NtQuerySystemEnvironmentValue  
NtSetSystemEnvironmentValue

sysinfo.c :

ROUND\_UP  
NtQueryDefaultLocale  
NtSetDefaultLocale  
NtQueryInstallUILanguage  
NtQueryDefaultUILanguage  
ExpGetUILanguagePolicy  
ExpSetCurrentUserUILanguage  
ExpGetCurrentUserUILanguage  
NtSetDefaultUILanguage  
ExpValidateLocale  
NtQuerySystemInformation  
NtSetSystemInformation  
ExLockUserBuffer  
ExUnlockUserBuffer  
ExpGetProcessInformation

ExpCopyProcessInfo  
ExpCopyThreadInfo  
ExpGetInstemulInformation  
ExpGetStackTraceInformation  
ExpGetLockInformation  
ExpGetLookasideInformation  
ExpGetPoolInformation  
ExpGetHandleInformation  
ExpGetObjectInformation  
ExpGetPoolTagInfo  
ExpQueryModuleInformation  
ExIsProcessorFeaturePresent  
ExpQueryLegacyDriverInformation

tex.c :

Excutive Subcomponents

timer.c :

ExpTimerApcRoutine  
ExpTimerDpcRoutine  
ExpDeleteTimer  
ExpTimerInitialization  
ExTimerRundown  
NtCreateTimer  
NtOpenTimer  
NtCancelTimer  
NtQueryTimer  
NtSetTimer  
ExGetNextWakeTime

tlock.c :

ExInterlockedIn(De)crement

tprofile.c :

profile object . tex.c .

uuid.c :

ExpUuidLoadSequenceNumber  
ExpUuidSaveSequenceNumber  
ExpUuidSaveSequenceNumberIf  
ExpUuidInitialization

ExpAllocateUuids  
NtSetUuidSeed  
NtAllocateUuids  
ExpUuidGetValues  
ExUuidCreate

win32.c :

ExpWin32Initialization

worker.c :

ExpNewThreadNecessary  
ExpWorkerInitialization  
ExQueueWorkItem  
ExpWorkerThreadBalanceManager  
ExpWorkerThread  
ExpCheckDynamicThreadCount  
ExpDetectWorkerThreadDeadlock  
ExpWorkerThreadFilter  
ExpCreateWorkerThread  
ExpCheckForWorker

zone.c :

ExInitializeZone  
ExExtendZone  
ExInterlockedExtendZone

```
#####  
#                               private/ntos/fsrec                               #  
#####
```

Comment :

Mini-Filesystem Recognizer.

```
#####  
#                               private/ntos/fsrtl                               #  
#####
```

Abstract :

Filesystem RTL Components

Prefix :

FsRtl

Files :

dbcsname.c  
fastio.c  
faulttol.c  
filelock.c  
filter.c  
filtrctx.c  
fsrtl.h  
fsrtipc.c  
largemcb.c  
name.c  
notify.c  
oplock.c  
pnp.c  
stackovf.c  
tmcb.c  
tunnel.c  
unc.c

dbcsname.c :

FsRtlIsFatDbcsLegal  
FsRtlIsHpfsDbcsLegal  
FsRtlDissectDbcs  
FsRtlDoesDbcsContainWildCards  
GetDbcs  
FsRtlIsDbcsInExpression

fastio.c :

FsRtlCopyRead  
FsRtlCopyWrite  
FsRtlMdIReadDev  
FsRtlMdIRead  
FsRtlMdIReadComplete  
FsRtlMdIReadCompleteDev  
FsRtlPrepareMdIWriteDev  
FsRtlPrepareMdIWrite  
FsRtlMdIWriteComplete  
FsRtlMdIWriteCompleteDev

FsRtlAcquireFileForModWrite  
FsRtlReleaseFileForModWrite  
FsRtlAcquireFileForCcFlush  
FsRtlReleaseFileForCcFlush  
FsRtlAcquireFileExclusive  
FsRtlReleaseFile  
FsRtlGetFileSize  
FsRtlSetFileSize

faulttol.c :

FsRtlBalanceReads  
FsRtlSyncVolumes

filelock.c :

FsRtlAllocateSharedLock  
FsRtlAllocateExclusiveLock  
FsRtlAllocateWaitingLock  
FsRtlAllocateLockTreeNode  
FsRtlAllocateLockInfo  
FsRtlFreeSharedLock  
FsRtlFreeExclusiveLock  
FsRtlFreeWaitingLock  
FsRtlFreeLockTreeNode  
FsRtlFreeLockInfo  
FsRtlAcquireLockQueue  
FsRtlReacquireLockQueue  
FsRtlReleaseLockQueue  
FsRtlCompleteLockIrp  
FsRtlCompleteLockIrpReal  
FsRtlAllocateSharedLock  
FsRtlAllocateExclusiveLock  
FsRtlAllocateLockTreeNode  
FsRtlAllocateWaitingLock  
FsRtlAllocateLockInfo  
FsRtlFreeSharedLock  
FsRtlFreeExclusiveLock  
FsRtlFreeLockTreeNode  
FsRtlFreeWaitingLock

FsRtlFreeLockInfo  
FsRtlAcquireLockQueue  
FsRtlReacquireLockQueue  
FsRtlReleaseLockQueue  
FsRtlCompleteLockIrp  
FsRtlInitializeFileLocks  
FsRtlInitializeFileLock  
FsRtlPrivateInitializeFileLock  
FsRtlUninitializeFileLock  
FsRtlAllocateFileLock  
FsRtlFreeFileLock  
FsRtlProcessFileLock  
FsRtlCheckLockForReadAccess  
FsRtlCheckLockForWriteAccess  
FsRtlFindFirstOverlappingSharedNode  
FsRtlFindFirstOverlappingExclusiveNode  
FsRtlFindFirstOverlapInNode  
FsRtlGetNextFileLock  
FsRtlCheckNoSharedConflict  
FsRtlCheckNoExclusiveConflict  
FsRtlFastCheckLockForRead  
FsRtlFastCheckLockForWrite  
FsRtlSplitLocks  
FsRtlPrivateRemoveLock  
FsRtlFastUnlockSingle  
FsRtlFastUnlockSingleShared  
FsRtlFastUnlockSingleExclusive  
FsRtlFastUnlockAll  
FsRtlFastUnlockAllByKey  
FsRtlPrivateLock  
FsRtlPrivateInsertLock  
FsRtlPrivateInsertSharedLock  
FsRtlPrivateInsertExclusiveLock  
FsRtlPrivateCheckWaitingLocks  
FsRtlPrivateCheckForExclusiveLockAccess  
FsRtlPrivateCheckForSharedLockAccess

FsRtIPrivateResetLowestLockOffset

FsRtIPrivateFastUnlockAll

FsRtIPrivateCancelFileLockIrp

filter.c :

FsRtINormalizeNtstatus

FsRtIIsNtstatusExpected

FsRtIAllocatePool

FsRtIAllocatePoolWithQuota

FsRtIAllocatePoolWithTag

FsRtIAllocatePoolWithTagQuota

FsRtIIsTotalDeviceFailure

filtrctx.c :

MySearchList

FsRtIInsertFilterContext

FsRtILookupFilterContextInternal

FsRtIRemoveFilterContext

FsRtITeardownFilterContexts

fsrtl.h :

FsRtIAllocatePool

FsRtIAllocatePoolWithQuota

FsRtIAllocatePool

DebugTrace

DebugDump

FlagOn

BooleanFlagOn

SetFlag

ClearFlag

WordAlign

LongAlign

QuadAlign

SectorAlign

SectorsFromBytes

BytesFromSectors

CopyUchar1

CopyUchar2

CopyUchar4



try\_return

fsrtlpc.c :

FsRtlInitSystem

FsRtlAllocateResource

FsRtlGetCompatibilityModeValue

largemcb.c :

SizeOfMapping

PreviousEndingVbn

StartingVbn

EndingVbn

NextStartingVbn

PreviousEndingLbn

StartingLbn

EndingLbn

NextStartingLbn

SectorsWithinRun

FsRtlAllocateFirstMapping

FsRtlFreeFirstMapping

FsRtlAllocateFastMutex

FsRtlFreeFastMutex

FsRtlInitializeMcb

FsRtlUninitializeMcb

FsRtlTruncateMcb

FsRtlAddMcbEntry

FsRtlRemoveMcbEntry

FsRtlLookupMcbEntry

FsRtlLookupLastMcbEntry

FsRtlNumberOfRunsInMcb

FsRtlGetNextMcbEntry

FsRtlInitializeLargeMcb

FsRtlInitializeLargeMcb

FsRtlUninitializeLargeMcb

FsRtlTruncateLargeMcb

FsRtlResetLargeMcb

FsRtlAddLargeMcbEntry

FsRtlRemoveLargeMcbEntry

FsRtILookupLargeMcbEntry  
FsRtILookupLastLargeMcbEntry  
FsRtILookupLastLargeMcbEntryAndIndex  
FsRtINumberOfRunsInLargeMcb  
FsRtIGetNextLargeMcbEntry  
FsRtISplitLargeMcb  
FsRtIRemoveMcbEntryPrivate  
FsRtIFindLargeIndex  
FsRtIAddLargeEntry  
FsRtIRemoveLargeEntry

name.c :

FsRtIDissectName  
FsRtIDoesNameContainWildCards  
FsRtIAreNamesEqual  
FsRtIIsNameInExpression  
FsRtIIsNameInExpressionPrivate

notify.c :

Add2Ptr  
PtrOffset  
SetFlag  
ClearFlag  
AcquireNotifySync  
ReleaseNotifySync  
FsRtINotifyInitializeSync  
FsRtINotifyUninitializeSync  
FsRtINotifyChangeDirectory  
FsRtINotifyFullChangeDirectory  
FsRtINotifyReportChange  
FsRtINotifyFullReportChange  
FsRtINotifyCleanup  
FsRtIIsNotifyOnList  
FsRtINotifyCompleteIrp  
FsRtINotifySetCancelRoutine  
FsRtINotifyUpdateBuffer  
FsRtINotifyCompleteIrpList  
FsRtICancelNotify

FsRtlCheckNotifyForDelete

oplock.c :

FsRtlInitializeOplock  
FsRtlUninitializeOplock  
FsRtlOplockFsctrl  
FsRtlCheckOplock  
FsRtlOplockIsFastIoPossible  
FsRtlCurrentBatchOplock  
FsRtlAllocateOplock  
FsRtlRequestExclusiveOplock  
FsRtlRequestOplockII  
FsRtlAcknowledgeOplockBreak  
FsRtlOpBatchBreakClosePending  
FsRtlOplockBreakNotify  
FsRtlOplockCleanup  
FsRtlOplockBreakToII  
FsRtlOplockBreakToNone  
FsRtlRemoveAndCompleteIrp  
FsRtlWaitOnIrp  
FsRtlCompletionRoutinePriv  
FsRtlCancelWaitIrp  
FsRtlCancelOplockIIIRp  
FsRtlCancelExclusiveIrp  
FsRtlRemoveAndCompleteWaitIrp  
FsRtlNotifyCompletion

pnf.c :

FsRtlNotifyVolumeEvent

stackovf.c :

FsRtlInitializeWorkerThread  
FsRtlPostStackOverflow  
FsRtlPostPagingFileStackOverflow  
FsRtlPostStackOverflow  
FsRtlStackOverflowRead  
FsRtlWorkerThread

tmcb.c :

Tests the Pinball Map Control Block support routines

tunnel.c :

- DbIHex64
- FsRtlCompareNodeAndKey
- FsRtlFreeTunnelNode
- FsRtlEmptyFreePoolList
- FsRtlRemoveNodeFromTunnel
- FsRtlInitializeTunnels
- FsRtlInitializeTunnelCache
- FsRtlAddToTunnelCache
- FsRtlFindInTunnelCache
- FsRtlDeleteKeyFromTunnelCache
- FsRtlDeleteTunnelCache
- FsRtlPruneTunnelCache
- FsRtlGetTunnelParameterValue
- DumpTunnel
- DumpNode

unc.c :

- FsRtlpRegisterProviderWithMUP
- FsRtlpOpenDev
- FsRtlpSetSymbolicLink
- FsRtlRegisterUncProvider
- FsRtlDeregisterUncProvider
- FsRtlpIsDfsEnabled

#####

# private/ntos/fstub #

#####

Abstract :

- Default HAL Handler

Prefix :

- xHal
- Fstub

Files :

- drivesup.c
- drivesup.h
- haldisp.h

halfnc.c

translate.c

drivesup.c :

GET\_STARTING\_SECTOR

GET\_PARTITION\_LENGTH

xHalExamineMBR

xHalGetPartialGeometry

HalpCalculateChsValues

HalpQueryPartitionType

HalpQueryDriveLayout

HalpNextMountLetter

HalpNextDriveLetter

HalpEnableAutomaticDriveLetterAssignment

HalpSetMountLetter

HalpIsOldStyleFloppy

xHalIoAssignDriveLetters

xHalIoReadPartitionTable

xHalIoSetPartitionInformation

xHalIoWritePartitionTable

HalpIsValidPartitionEntry

xHalIoClearPartitionTable

HalpGetFullGeometry

DrivesupDebugPrint

drivesup.h :

nothing special

haldisp.h :

nothing special

halfnc.c :

xHalQuerySystemInformation

xHalSetSystemInformation

xHalQueryBusSlots

xHalRegisterBusHandler

xHalSetWakeEnable

xHalSetWakeAlarm

xHalLocateHiberRanges

xHalHandlerForBus

xHalReferenceHandler  
xHalInitPnpDriver  
xHalInitPowerManagement  
xHalGetDmaAdapter  
xHalPutDmaAdapter  
xHalAllocateCommonBuffer  
xHalFreeCommonBuffer  
xHalAllocateAdapterChannel  
xHalFlushAdapterBuffers  
xHalFreeAdapterChannel  
xHalFreeMapRegisters  
xHalMapTransfer  
xHalGetDmaAlignment  
xHalReadDmaCounter  
xHalGetScatterGatherList  
xHalPutScatterGatherList  
xHalAllocateAdapterCallback  
xHalTranslateBusAddress  
xHalAssignSlotResources  
xHalHaltSystem

translate.c :

FOR\_ALL\_IN\_LIST  
FOR\_ALL\_IN\_ARRAY  
FOR\_REST\_IN\_ARRAY  
xHalGetInterruptTranslator  
FstubTranslateResource  
FstubTranslateRequirement  
FstubTranslatorNull

#####

# private/ntos/inc #

#####

Comment :

Include Files.

#####

# private/ntos/io #

#####

Abstract :

Functions for I/O Management.

Prefix :

Io

PnP

Nt

Mapper

Triage

Acronym :

VPB (Volume Parameter Block)

Files :

pri\_bld/pnpsubs.c

arcsec.c

assign.c

complete.c

create.c

devctrl.c

devnode.c

dir.c

dockhwp.c

dumpctl.c

errorlog.c

filter.c

flunkirp.c

flunkirp.h

fsctrl.c

hashirp.c

hashirp.h

internal.c

ioassert.c

ioassert.h

iodata.c

ioguid.c

ioinit.c

iop.h  
iosubs.c  
ioverifier.c  
ioverifier.h  
loadunld.c  
lock.c  
mapper.c  
misc.c  
netboot.c  
objsup.c  
open.c  
parse.c  
pnparb.c  
pnpbusno.c  
pnpcvrt.c  
pnpdata.c  
pnpdd.c  
pnpdel.c  
pnpdma.c  
pnpeisa.c  
pnpenum.c  
pnpinit.c  
pnpioapi.c  
pnpiop.h  
pnpirp.c  
pnpirq.c  
pnpmap.c  
pnpmio.c  
pnppower.c  
pnpres.c  
pnprlist.c  
pnprlist.h  
pnpsubs.c  
qsea.c  
qsfs.c  
qsinfo.c



qsquota.c  
query.c  
read.c  
remlock.c  
remlock.h  
report.c  
sessnirp.c  
sessnirp.h  
trackirp.c  
trackirp.h  
triage.c  
write.c

pri\_bld/pnpsubs.c :

IopCreateMadeupNode  
IopRemoveStringFromValueKey  
IopAppendStringToValueKey  
IopConcatenateUnicodeStrings  
IopPrepareDriverLoading  
IopServiceInstanceToDeviceInstance  
IopOpenRegistryKeyPersist  
IopOpenServiceEnumKeys  
IopGetDeviceInstanceCsConfigFlags  
IopSetDeviceInstanceCsConfigFlags  
IopOpenCurrentHwProfileDeviceInstanceKey  
IopApplyFunctionToSubKeys  
IopRegMultiSzToUnicodeStrings  
IopApplyFunctionToServiceInstances  
IopMarkDuplicateDevice  
IopIsDuplicatedDevices  
IopFreeUnicodeStringList  
IopDriverLoadingFailed  
IopDisableDevice  
IopIsAnyDeviceInstanceEnabled  
IopIsDeviceInstanceEnabled  
IopDetermineResourceListSize  
IopReferenceDriverObjectByName

IopDeviceObjectFromDeviceInstance  
IopDeviceObjectToDeviceInstance  
IopCleanupDeviceRegistryValues  
IopGetDeviceResourcesFromRegistry  
IopReadDeviceConfiguration  
IopCmResourcesToIoResources  
IopFilterResourceRequirementsList  
IopMergeFilteredResourceRequirementsList  
IopMergeCmResourceLists  
IopIsLegacyDriver  
IopGetGroupOrderIndex  
IopDeleteLegacyKey  
IopDeviceCapabilitiesToRegistry  
IopRestartDeviceNode

arcsec.c :

IopProtectSystemPartition  
IopApplySystemPartitionProt

assign.c :

IoAssignResources  
IopSlotResourceOwner  
IO\_DESC\_MIN  
IO\_DESC\_MAX  
IopGenNextValidResourceList  
IopGenNextValidDescriptor  
IopFindCollisionInTList  
IopPickupCollisionInTList  
IopAllocateDirPool  
IopGetResourceReqRegistryValue  
IopAssignResourcesPhase1  
IopAssignResourcesPhase2  
IopAssignResourcesPhase3  
IopAssignResourcesPhase4  
IopLogConflict  
IopNewTransEntry  
IopAddCmDescriptorToInUseList  
IopBuildResourceDir

IopFreeResourceDir  
IopDumpIoResourceDir  
IopDumpIoResourceDescriptor  
IopCategorizeDescriptors  
IopDescriptorSortingWeight  
IopSortDescriptors

complete.c :

NtCreateIoCompletion  
NtOpenIoCompletion  
NtQueryIoCompletion  
NtSetIoCompletion  
NtRemoveIoCompletion  
IoSetIoCompletion  
IopFreeMiniPacket  
IopDeleteIoCompletion

create.c :

NtCreateFile  
NtCreateNamedPipeFile  
NtCreateMailslotFile

devctrl.c :

NtDeviceIoControlFile

devnode.c :

IopAllocateDeviceNode  
IopForAllDeviceNodes  
IopForAllChildDeviceNodes  
IopForAllDeviceNodesCallback  
IopDestroyDeviceNode  
IopInsertTreeDeviceNode  
IopRemoveTreeDeviceNode  
IopCheckForTargetDevice  
IopCheckDeviceNodeTree

dir.c :

BuildQueryDirectoryIrp  
NtQueryDirectoryFile  
NtNotifyChangeDirectoryFile

dockhwp.c :

IopHardwareProfileBeginTransition  
IopHardwareProfileMarkDock  
IopHardwareProfileQueryChange  
IopHardwareProfileCommitStartedDock  
IopHardwareProfileCommitRemovedDock  
IopHardwareProfileCancelRemovedDock  
IopHardwareProfileCancelTransition  
IopHardwareProfileSetMarkedDocksEjected  
IopHardwareProfileSendCommit  
IopHardwareProfileSendCancel  
IopUpdateHardwareProfile  
IopExecuteHwpDefaultSelect  
IopExecuteHardwareProfileChange  
IopProfileAcquisition  
IopFindPossibleProfiles  
IopAcpiQueryDockingProfileEvent

dumpctl.c :

X86PaeEnabled  
IopIsAddressRangeValid  
IoGetDumpStack  
IopGetDumpStack  
IopLoadDumpDriver  
IopGetDumpControlBlockCheck  
IoInitializeDumpStack  
IoGetDumpHiberRanges  
IoFreeDumpStack  
IoInitializeDumpSpaceAndType  
IoWriteCrashDump  
IopMapPhysicalMemory  
IopAddPageToPageMap  
IopRemovePageFromPageMap  
IoGetCrashDumpInformation  
IoGetCrashDumpStateInformation  
IoSetDumpRange  
IoFreeDumpRange  
IopCalculateRequiredDumpSpace

IopGetLoadedDriverInfo  
IopWriteDriverList  
IopWriteTriageDump  
IopWritePageToDisk  
IopWriteSummaryDump  
IopInitializeSummaryDump  
IopWriteSummaryHeader  
IopWriteToDisk  
IopMapVirtualToPhysicalMdl  
IopCreateSummaryDump  
IopDeleteNonExistentMemory  
IopCompleteDumpInitialization  
IopFreeDCB  
IoSetCrashDumpState  
IopReadDumpRegistry  
IopInitializeDCB  
IopConfigureCrashDump  
IopDebugPrint

errorlog.c :

IopErrorLogThread  
IopErrorLogConnectPort  
IopErrorLogDpc  
IopErrorLogGetEntry  
IopErrorLogQueueRequest  
IopErrorLogRequeueEntry

filter.c :

IopAddDefaultResourceList  
IopCmResourcesToIoResources  
IopAdjustResourceListRange  
IopGetNextSupportedRange  
IopSortRanges

flunkirp.c :

IovpAssertIsNewRequest  
IovpAssertDoAdvanceStatus  
IovpAssertNewIrp  
IovpAssertFinalIrpStack

IoVpAssertNewRequest  
IoVpAssertIrpStackDownward  
IoVpAssertIrpStackUpward  
IoVpAssertIsValidIrpStatus  
IoVpThrowChaffAtStartedPdoStack  
IoVpThrowBogusSynchronousIrp  
IoVpStartObRefMonitoring  
IoVpStopObRefMonitoring  
IoVpIsSystemRestrictedIrp

flunkirp.h :

nothing special

fsctrl.c :

NtFsControlFile

hashirp.c :

IoVpTrackingDataInit  
IoVpTrackingDataCreateAndLock  
IoVpTrackingDataFree  
IoVpTrackingDataFindAndLock  
IoVpTrackingDataFindPointer  
IoVpTrackingDataAcquireLock  
IoVpTrackingDataReleaseLock  
IoVpTrackingDataReference  
IoVpTrackingDataDereference  
IoVpTrackingDataGetCurrentSessionData  
IoVpProtectedIrpAllocate  
IoVpProtectedIrpMakeUntouchable  
IoVpProtectedIrpMakeTouchable  
IoVpProtectedIrpFree  
IoVpWatermarkIrp

hashirp.h :

nothing special

internal.c :

IoVpAbortRequest  
IoVpAcquireFileObjectLock  
IoVpAllocateIrpCleanup  
IoVpAllocateIrpMustSucceed

IopApcHardError  
IopCancelAlertedRequest  
IopCheckGetQuotaBufferValidity  
IopCompleteUnloadOrDelete  
IopCompletePageWrite  
IopCompleteRequest  
IopConnectLinkTrackingPort  
IopDisassociateThreadIrp  
IopDeallocateApc  
IopDropIrp  
IopExceptionFilter  
IopExceptionCleanup  
IopFreeIrpAndMdl  
IopGetDriverNameFromKeyNode  
IopGetFileName  
IopGetMountFlag  
IopGetRegistryKeyInformation  
IopGetRegistryValue  
IopGetRegistryValues  
IopGetSetObjectId  
IopGetVolumeId  
IopHardErrorThread  
IopInvalidDeviceRequest  
IopIsSameMachine  
IopLoadDriver  
IopGetDeviceAttachmentBase  
IopGetDeviceAttachmentBaseRef  
IopDecrementDeviceObjectRef  
IopLoadFileSystemDriver  
IopLoadUnloadDriver  
IopMountVolume  
IopInvalidateVolumesForDevice  
IopNotifyPnpWhenChainDereferenced  
IopOpenLinkOrRenameTarget  
IopOpenRegistryKey  
IopQueryXxxInformation

IopRaiseHardError  
IopRaiseInformationalHardError  
IopReadyDeviceObjects  
IopResurrectDriver  
IopMarshalIds  
IopUnMarshalIds  
IopSendMessageToTrackService  
IopSetEaOrQuotaInformationFile  
IopSetRemoteLink  
IopStartApcHardError  
IopSynchronousApiServiceTail  
IopSynchronousServiceTail  
IopTimerDispatch  
IopTrackLink  
IopUserCompletion  
IopUserRundown  
IopXxxControlFile  
IopLookupBusStringFromID  
IopSafebootDriverLoad  
IopInitializeBootLogging  
IopBootLog  
IopCopyBootLogRegistryToFile  
IopBootLogToFile

ioassert.c :

IopDriverCorrectnessTakeLock  
IopDriverCorrectnessReleaseLock  
IopDriverCorrectnessCheckUnderLock  
IopDriverCorrectnessProcessParams  
IopDriverCorrectnessApplyControl  
IopDriverCorrectnessProcessMessageText  
IopDriverCorrectnessThrowBugCheck  
IopDriverCorrectnessPrintBuffer  
IopDriverCorrectnessPrintParamData  
IopDriverCorrectnessPrompt  
IopDriverCorrectnessAddressToFileHeader  
IopIsMemoryRangeReadable



```
    IopDriverCorrectnessPrintIrp
    IopDriverCorrectnessPrintIrpStack
ioassert.h :
    _DC_ASSERT_OUT
iodata.c :

ioguid.c :
    nothing special
ioinit.c :
    InitializeDriverObject
    IoInitSystem
    IopSetIoRoutines
    IopCheckDependencies
    IopCreateArcNames
    IopCreateObjectTypes
    IopCreateEntry
    IopCreateRootDirectories
    IopFreeGroupTree
    IopInitializeAttributesAndCreateObject
    IopInitializeBootDrivers
    IopInitializeBuiltinDriver
    IopInitializeSystemDrivers
    IopLookupGroupName
    IopMarkBootPartition
    IopReassignSystemRoot
    IopStoreSystemPartitionInformation
    IopGetDriverTagPriority
    IopInsertDriverList
    IopNotifySetupDevices
    IopLogErrorEvent
    IopWaitForBootDevicesStarted
    IopWaitForBootDevicesDeleted
    IopLoadBootFilterDriver
    IopCheckClassFiltersForBootDevice
    IopAddDeviceInstanceForClassFilters
iop.h :
```

IopAcquireFastLock  
IopAcquireCancelSpinLockAtDpcLevel  
IopReleaseCancelSpinLockFromDpcLevel  
IopAllocateIrp  
IsIoVerifierOn  
IopDequeueThreadIrp  
IopApcRoutinePresent  
IopInitializeIrp  
IopQueueThreadIrp  
IopReleaseFileObjectLock

iosubs.c :

IoAcquireCancelSpinLock  
IoAcquireVpbSpinLock  
IoAllocateAdapterChannel  
IoAllocateController  
IoAllocateDriverObjectExtension  
IoAllocateErrorLogEntry  
IoAllocateGenericErrorLogEntry  
IopAllocateErrorLogEntry  
IoAllocateIrp  
IopAllocateIrpPrivate  
IoAllocateMdl  
IoAsynchronousPageWrite  
IoAttachDevice  
IoAttachDeviceByPointer  
IoAttachDeviceToDeviceStack  
IoBuildAsynchronousFsdRequest  
IoBuildDeviceIoControlRequest  
IoBuildPartialMdl  
IoBuildSynchronousFsdRequest  
IopfCallDriver  
IoCallDriver  
IoCancelIrp  
IoCancelThreadIo  
IoCheckDesiredAccess  
IoCheckEaBufferValidity

IoCheckFunctionAccess  
IoCheckQuerySetFileInformation  
IoCheckQuerySetVolumeInformation  
IoCheckQuotaBufferValidity  
IoCheckShareAccess  
IoCompleteRequest  
IopfCompleteRequest  
IoConnectInterrupt  
IoCreateController  
IopInsertRemoveDevice  
IopCreateVpb  
IoCreateDevice  
IoCreateFile  
IoCreateNotificationEvent  
IoCreateStreamFileObject  
IoCreateStreamFileObjectLite  
IoCreateSymbolicLink  
IoCreateSynchronizationEvent  
IoCreateUnprotectedSymbolicLink  
IoDeleteController  
IopRemoveTimerFromTimerList  
IoDeleteDevice  
IopDeleteSessionSymLinks  
IoDeleteSymbolicLink  
IoDetachDevice  
IoDisconnectInterrupt  
IoEnqueueIrp  
IoFastQueryNetworkAttributes  
IoFreeController  
IoFreeIrp  
IopFreeIrp  
IoFreeMdl  
IoGetAttachedDevice  
IoGetAttachedDeviceReference  
IoGetBaseFileSystemDeviceObject  
IoGetConfigurationInformation

IoGetCurrentProcess  
IoGetDeviceObjectPointer  
IoGetDeviceToVerify  
IoGetDriverObjectExtension  
IoGetFileObjectGenericMapping  
IoGetInitialStack  
IoGetRelatedDeviceObject  
IoGetRequestorProcessId  
IoGetRequestorProcess  
IoGetTopLevelIrp  
IoInitializeIrp  
IoReuseIrp  
IoInitializeTimer  
IoIsOperationSynchronous  
IoIsSystemThread  
IoIsValidNameGraftingBuffer  
IoPdoNameTransmogri fy  
IoMakeAssociatedIrp  
IoPageFileCreated  
IoPageRead  
IoQueryFileInformation  
IoQueryVolumeInformation  
IoQueueThreadIrp  
IoRaiseHardError  
IoRaiseInformationalHardError  
ArePacketsEquivalent  
IoRegisterBootDriverReinitialization  
IoRegisterDriverReinitialization  
IoRegisterFileSystem  
IoRegisterFsRegistrationChange  
IoRegisterLastChanceShutdownNotification  
IoRegisterShutdownNotification  
IoReleaseCancelSpinLock  
IoReleaseVpbSpinLock  
IoRemoveShareAccess  
IoSetDeviceToVerify

IoSetHardErrorOrVerifyDevice  
IoSetInformation  
IoSetShareAccess  
IoSetThreadHardErrorMode  
IoSetTopLevelIrp  
IoShutdownSystem  
IoStartNextPacket  
IoStartNextPacketByKey  
IoStartPacket  
IoStartTimer  
IoStopTimer  
IoSynchronousPageWrite  
IoThreadToProcess  
IoUnregisterFileSystem  
IoUnregisterFsRegistrationChange  
IoUnregisterShutdownNotification  
IoUpdateShareAccess  
IoVerifyVolume  
IoWriteErrorLogEntry  
IoGetBootDiskInformation  
IoCallDriver  
IoCompleteRequest  
IoCreateDefaultDeviceSecurityDescriptor  
IoGetRequestorSessionId  
IoUpdateOtherOperationCount  
IoUpdateReadOperationCount  
IoUpdateWriteOperationCount  
IoUpdateOtherTransferCount  
IoUpdateReadTransferCount  
IoUpdateWriteTransferCount  
IoCancelFileOpen  
IoRetryIrpCompletions

ioverifier.c :

IsKernelHandle  
IoVerifierInit  
IoValidateDeviceObject

IovFreeIrp  
IovFreeIrpPrivate  
IovCallDriver  
IovCompleteRequest  
IovAllocateIrp  
IovBuildAsynchronousFsdRequest  
IovBuildDeviceIoControlRequest  
IovInitializeTimer  
IovpCompleteRequest  
IovSpecialIrpCompleteRequest  
ZeroAndDopeIrpStackLocation  
IovSpecialIrpCallDriver  
IovInitializeIrp  
IovAttachDeviceToDeviceStack  
IovDeleteDevice  
IovDetachDevice  
IovCancelIrp

ioverifier.h :

IOVP\_COMPLETE\_REQUEST  
IOV\_INITIALIZE\_IRP  
IOV\_DELETE\_DEVICE  
IOV\_DETACH\_DEVICE  
IOV\_ATTACH\_DEVICE\_TO\_DEVICE\_STACK  
IOV\_CANCEL\_IRP

loadunload.c :

NtLoadDriver  
IopCheckUnloadDriver  
NtUnloadDriver

lock.c :

NtLockFile  
NtUnlockFile

mapper.c :

MapperFindIdentMatch  
MapperTranslatePnPId  
MapperPeripheralCallback  
MapperCallback

MapperProcessFirmwareTree  
MapperMarkKey  
MapperSeedKey  
MapperFreeList  
MapperConstructRootEnumTree  
MapperAdjustResourceList  
ComPortDBAdd  
MapperPhantomizeDetectedComPorts  
MapperDebugPrint

misc.c :

NtCancelIoFile  
NtDeleteFile  
NtFlushBuffersFile  
NtQueryAttributesFile  
NtQueryFullAttributesFile  
IoAllocateWorkItem  
IoFreeWorkItem  
IoQueueWorkItem  
IoProcessWorkItem

netboot.c :

IopAddRemoteBootValuesToRegistry  
IopStartNetworkForRemoteBoot  
IopShutdownCsc  
IopAssignNetworkDriveLetter  
IopEnableRemoteBootSecurity  
IopStartTcpIpForRemoteBoot  
IopIsRemoteBootCard  
IopSetupRemoteBootCard  
IopInitCsc  
IopResetCsc  
IopBreakPath  
IopMarkRoot  
IopSetFlushCSC  
IopWalkDirectoryHelper  
IopWalkDirectoryTree  
IopGetShadowExW

IopAddHintFromInode  
IopSetShadowInfoW  
IopCreateShadowW  
IopCopyServerAcl  
IopGetShadowPathW  
IopWriteIpAddressToRegistry  
IopSetDefaultGateway  
IopCacheNetbiosNameForIpAddress  
IopTCPQueryInformationEx  
IopTCPSetInformationEx  
IopGetHarddiskInfo  
IoStartCscForTextmodeSetup

objsup.c :

IopCloseFile  
IopDeleteFile  
IopDeleteDriver  
IopDeleteDevice  
IopGetDevicePDO  
IopSetDeviceSecurityDescriptors  
IopGetSetSecurityObject

open.c :

NtOpenFile

parse.c :

RoundNameSize  
IopCheckDeviceAndDriver  
IopCheckVpbMounted  
IopDereferenceVpbAndFree  
IopParseDevice  
IopParseFile  
IopQueryName  
IopCheckBackupRestorePrivilege

pnparb.c :

nothing special

pnbusno.c :

IopBusNumberInitialize  
IopBusNumberUnpackRequirement



IopBusNumberScoreRequirement

IopBusNumberPackResource

IopBusNumberUnpackResource

pnpcvrt.c :

nothing special

pnpdata.c :

pnp

pnppdd.c :

IopAddDevicesToBootDriver

IopAddDevicesToBootDriverWorker

IopReleaseDeviceResources

IopPnPAddDevice

IopArbiterHandlerxx

IopTranslatorHandlerCm

IopTranslatorHandlerIo

IopPowerDispatch

IopPnPDispatch

IopPnPCompleteRequest

IopProcessAddDevices

IopProcessAddDevicesWorker

IopProcessAssignResources

IopProcessAssignResourcesWorker

IopGetDriverDeviceList

IopGetDriverDeviceListWorker

IopNewDevice

IopStartDriverDevices

IopAssignResourcesToDevices

IopWriteAllocatedResourcesToRegistry

IopIsFirmwareDisabled

pnpdel.c :

IopChainDereferenceComplete

IopDelayedRemoveWorker

IopDeleteLockedDeviceNode

IopDeleteLockedDeviceNodes

IopLockDeviceRemovalRelations

IopProcessRelation

IopQueuePendingEject  
IopInvalidateRelationsInList  
IopProcessCompletedEject  
IopQueuePendingSurpriseRemoval  
IopUnlockDeviceRemovalRelations  
IopRequestDeviceRemoval  
IopUnloadAttachedDriver

pnpdma.c :

IopDmaInitialize  
IopDmaUnpackRequirement  
IopDmaScoreRequirement  
IopDmaPackResource  
IopDmaUnpackResource  
IopDmaOverrideConflict

pnpeisa.c :

EisaBuildEisaDeviceNode  
EisaGetEisaDevicesResources  
EisaBuildSlotsResources

pnpenum.c :

IopRequestDeviceAction  
IopDeviceActionWorker  
IopBusCheck  
IopProcessStartDevices  
IopProcessStartDevicesWorker  
IopStartAndEnumerateDevice  
IopEnumerateDevice  
IopProcessNewChildren  
IopProcessNewDeviceNode  
IopCallDriverAddDevice  
IopCallDriverAddDeviceQueryRoutine  
IopQueryDeviceCapabilities  
IopProcessCriticalDevice  
IopProcessCriticalDeviceRoutine  
IopGetBusTypeGuidIndex  
IopFixupDeviceId  
IopFixupIds

IopGetRegistryDwordWithFallback  
IopGetRegistrySecurityWithFallback  
IopChangeDeviceObjectFromRegistryProperties  
IopProcessNewProfile  
IopProcessNewProfileWorker  
IopProcessNewProfileStateCallback

pnppinit.c :

IopInitializePlugPlayServices  
IopPnPDriverEntry  
IopGetRootDevices  
IopInitializeDeviceKey  
IopInitializeDeviceInstanceKey  
IopGetServiceType  
IopDetermineDefaultInterfaceType  
IopIsFirmwareMapperDevicePresent

pnpioapi.c :

IoGetDeviceProperty  
IoOpenDeviceRegistryKey  
IoCreateDriver  
IoDeleteDriver  
IoSynchronousInvalidateDeviceRelations  
IoInvalidateDeviceRelations  
IoRequestDeviceEject  
IopRequestDeviceEjectWorker  
IoReportDetectedDevice  
IopIsReportedAlready  
IoAllocateBuffer  
IoResizeBuffer  
IoFreeBuffer  
IoAppendBuffer  
IoOverwriteBuffer  
IoGetDeviceInterfaces  
IoGetDeviceInterfaces  
IoRealLoc  
IoSetDeviceInterfaceState  
IoOpenDeviceInterfaceRegistryKey

IopDeviceInterfaceKeysFromSymbolicLink  
IoRegisterDeviceInterface  
IopRegisterDeviceInterface  
IopUnregisterDeviceInterface  
IopRemoveDeviceInterfaces  
IopOpenOrCreateDeviceInterfaceSubKeys  
IoGetDeviceInterfaceAlias  
IopBuildSymbolicLinkStrings  
IopReplaceSeparatorWithPound  
IopDropReferenceString  
IopParseSymbolicLinkName  
IopAllocateUnicodeString  
IopFreeAllocatedUnicodeString  
IopSetRegistryStringValue  
IoUnregisterPlugPlayNotification  
IopProcessDeferredRegistrations  
IoReportTargetDeviceChange  
IoReportTargetDeviceChangeAsynchronous  
IopReportTargetDeviceChangeAsyncWorker  
IoInvalidateDeviceState  
IopQueueDeviceWorkItem  
IopInvalidateDeviceStateWorker  
IopResourceRequirementsChanged  
IoInitializePlugPlayNotification  
IopReferenceNotify  
IopDereferenceNotify  
IopRequestHwProfileChangeNotification  
IopNotifyHwProfileChange  
IopNotifyTargetDeviceChange  
IopNotifyDeviceClassChange  
IoRegisterPlugPlayNotification  
IopGetRelatedTargetDevice  
IoGetRelatedTargetDevice  
IopNotifySetupDeviceArrival  
IoIsWdmVersionAvailable  
IoGetDmaAdapter

IopOpenDeviceParametersSubkey  
IopSetupDeviceObjectFromDeviceClass  
IopSetSecurityObjectFromRegistry  
PpCreateLegacyDeviceIds  
IoNotifyPowerOperationVetoed  
IoPnPDeliverServicePowerNotification  
IopOrphanNotification  
IopPnPHydraCallback  
IopAppendLegacyVeto  
IopGetLegacyVetoListDevice  
IopGetLegacyVetoListDeviceNode  
IopGetLegacyVetoListDrivers  
IoGetLegacyVetoList  
IopDoDeferredSetInterfaceState  
IopProcessSetInterfaceState

pnp\iop.h :

IopDoesDevNodeHaveProblem  
IopIsDevNodeProblem  
IopClearDevNodeProblem  
IopSetDevNodeProblem  
IopIsProblemReadOnly  
IopRegistryDataToUnicodeString  
IopAcquireEnumerationLock  
IopReleaseEnumerationLock  
IopReleaseEnumerationLockForThread  
IopAcquireDeviceTreeLock  
IopReleaseDeviceTreeLock  
IopDeviceNodeFlagsToCapabilities  
IopConstStringSize  
IopConstStringLength  
IopKMTtoUMSymbolicLinkName  
IopUMtoKMSymbolicLinkName  
IopHashGuid  
IopAcquireNotifyLock  
IopReleaseNotifyLock  
IopCompareGuid

pnpirp.c :

PnpIrpStatusTracking  
HASH\_UNICODE\_STRING  
IopUncacheInterfaceInformation  
IopAsynchronousCall  
IopSynchronousCall  
IopStartDevice  
IopEjectDevice  
IopDeviceEjectComplete  
IopRemoveDevice  
IopLockMountedDeviceForRemove  
IopUnlockMountedDeviceForRemove  
IopFindMountableDevice  
IopDeviceStartComplete  
IopDeviceRelationsComplete  
IopQueryDeviceRelations  
IopQueryDeviceId  
IopQueryUniqueId  
IopMakeGloballyUniqueId  
IopQueryCompatibleIds  
IopQueryDeviceResources  
IopQueryResourceHandlerInterface  
IopQueryReconfiguration  
IopQueryLegacyBusInformation  
IopQueryPnpBusInformation  
IopQueryDeviceState  
IopIncDisableableDepends  
IopDecDisableableDepends  
IopQueryDeviceSerialNumber  
IopFilterResourceRequirementsCall  
IopQueryDockRemovalInterface

pnpirq.c :

IopIrqTranslateOrdering  
IopIrqInitialize  
IopIrqUnpackRequirement  
IopIrqScoreRequirement

IopIrqPackResource  
IopIrqUnpackResource

pnpmap.c :

PnPBIOSGetBIOSInfo  
PnPBIOSExpandProductId  
PnPBIOSIgnoreNode  
PnPGetDevnodeExcludeList  
PnPCheckFixedIoOverrideDecodes  
PnPBIOSCheckForExclusion  
PnPBIOSIoResourceListToCmResourceList  
PnPBIOSExtractCompatibleIDs  
PnPBIOSTranslateInfo  
PnPBIOSFindMatchingDevNode  
PnPBIOSEliminateDupes  
PnPBIOSGetDescription  
PnPBIOSCopyDeviceParamKey  
PnPBIOSWriteInfo  
PnPBIOSCopyIoDecode  
PnPBIOSCheckForHardwareDisabled  
PnPBIOSFreeDevNodeInfo  
PnPBIOSMapper  
PpFilterNtResource  
PnPBIOSDebugPrint

pnpmemio.c :

IopTranslateBusAddress  
IopGenericTranslateOrdering  
IopPortInitialize  
IopMemInitialize  
IopGenericUnpackRequirement  
IopGenericScoreRequirement  
IopGenericPackResource  
IopGenericUnpackResource  
IopPortRetestAllocation  
IopPortBacktrackAllocation  
IopPortFindSuitableRange  
IopPortGetNextAlias

IopPortAddAl location  
IopPortIsAliasedRangeAvai lable  
IopMemFindSui tableRange

pnppower.c :

IoBuildPoDeviceNot ifyList  
IopFreePoDeviceNot ifyListHead  
IopFreePoDeviceNot ifyList  
IopCaptureObjectName  
IopWarmEjectDevice

pnpres.c :

IopReleaseBootResources  
IopInitPool  
IopAllocPoolAl igned  
IopAllocPool  
IopAllocateResources  
IopGetResourceRequirementsForAssignTable  
IopResourceRequirementsListToReqList  
IopComparePriority  
IopCompareAl ternativeCount  
IopRearrangeReqList  
IopRearrangeAssignTable  
IopFreeReqAl ternative  
IopFreeReqList  
IopFreeResourceRequirementsForAssignTable  
IopBuildCmResourceList  
IopBuildCmResourceLists  
IopNeedToReleaseBootResources  
IopReleaseFilteredBootResources  
IopPlacement  
IopPlacementForReservation  
IopAddReqDescsToArbiters  
IopRemoveReqDescsFromArbiters  
IopIsBestConfiguration  
IopSaveCurrentConfiguration  
IopRestoreBestConfiguration  
IopAssign



IopAssignInner  
IopReserve  
IopFindResourceHandlerInfo  
IopSetupArbiterAndTranslators  
IopParentToRawTranslation  
IopChildToRootTranslation  
IopTranslateAndAdjustReqDesc  
IopCallArbiter  
IopDumpResourceRequirementsList  
IopDumpResourceDescriptor  
IopQueryRebalance  
IopQueryRebalanceWorker  
IopTestForReconfiguration  
IopPlacementForRebalance  
IopArbitrateDeviceResources  
IopFindResourcesForArbiter  
IopRebalance  
IopRestoreResourcesInternal  
IopReleaseResourcesInternal  
IopFindLegacyDeviceNode  
IopRemoveLegacyDeviceNode  
IopLegacyResourceAllocation  
IopFindBusDeviceNode  
IopFindBusDeviceNodeInternal  
IopDuplicateDetection  
IopSetLegacyDeviceInstance  
IopCombineLegacyResources  
IopCreateCmResourceList  
IopCombineCmResourceList  
IopReserveLegacyBootResources  
IopAllocateBootResources  
IopReserveBootResourcesInternal  
IopReserveBootResources  
IopReleaseResources  
IopReallocateResources  
IopCheckDataStructures

IopCheckDataStructuresWorker  
IopQueryConflictList  
IopEliminateBogusConflict  
IopQueryConflictFillString  
IopQueryConflictFillConflicts  
IopQueryConflictListInternal

pnprlist.c :

IopAddRelationToList  
IopAllocateRelationList  
IopCompressRelationList  
IopEnumerateRelations  
IopFreeRelationList  
IopGetRelationsCount  
IopGetRelationsTaggedCount  
IopIsRelationInList  
IopMergeRelationLists  
IopRemoveIndirectRelationsFromList  
IopRemoveRelationFromList  
IopSetAllRelationsTags  
IopSetRelationsTag

pnprlist.h :

nothing special

pnpsubs.c :

IopCreateMadeupNode  
IopRemoveStringFromValueKey  
IopAppendStringToValueKey  
IopConcatenateUnicodeStrings  
IopPrepareDriverLoading  
IopServiceInstanceToDeviceInstance  
IopOpenRegistryKeyEx  
IopCreateRegistryKeyEx  
IopOpenServiceEnumKeys  
IopGetDeviceInstanceCsConfigFlags  
IopGetServiceInstanceCsConfigFlags  
IopSetServiceInstanceCsConfigFlags  
IopOpenCurrentHwProfileDeviceInstanceKey

IopApplyFunctionToSubKeys  
IopRegMultiSzToUnicodeStrings  
IopApplyFunctionToServiceInstances  
IopMarkDuplicateDevice  
IopIsDuplicatedDevices  
IopFreeUnicodeStringList  
IopDriverLoadingFailed  
IopDisableDevice  
IopIsAnyDeviceInstanceEnabled  
IopIsDeviceInstanceEnabled  
IopDetermineResourceListSize  
IopReferenceDriverObjectByName  
IopDeviceObjectFromDeviceInstance  
IopDeviceObjectToDeviceInstance  
IopCleanupDeviceRegistryValues  
IopGetDeviceResourcesFromRegistry  
IopReadDeviceConfiguration  
IopCmResourcesToIoResources  
IopFilterResourceRequirementsList  
IopMergeFilteredResourceRequirementsList  
IopMergeCmResourceLists  
IopIsLegacyDriver  
IopGetGroupOrderIndex  
IopDeleteLegacyKey  
IopDeviceNodeCapabilitiesToRegistry  
IopDeviceCapabilitiesToRegistry  
IopRestartDeviceNode  
IopDeleteKeyRecursiveCallback  
IopDeleteKeyRecursive

qsea.c :

NtQueryEaFile  
NtSetEaFile

qsfs.c :

NtQueryVolumeInformationFile  
NtSetVolumeInformationFile

qsinfo.c :

IopGetModeInformation  
NtQueryInformationFile  
NtSetInformationFile

qsquota.c :  
NtQueryQuotaInformationFile  
NtSetQuotaInformationFile

query.c :  
IoQueryDeviceDescription  
pIoQueryBusDescription  
pIoQueryDeviceDescription

read.c :  
NtReadFile  
NtReadFileScatter

remlock.c :  
MinutesToTicks  
IoInitializeRemoveLockEx  
IoAcquireRemoveLockEx  
IoReleaseRemoveLockEx  
IoReleaseRemoveLockAndWaitEx

remlock.h :  
nothing special

report.c :  
IoInitializeResourceMap  
IoReportHalResourceUsage  
IoReportResourceForDetection  
IoReportResourceUsage  
IoReportResourceUsageInternal  
IoChangeInterfaceType  
IoWriteResourceList  
IoDumpCmResourceDescriptor  
IoDumpCmResourceList

sessnirp.c :  
IoVpSessionDataCreate  
IoVpSessionDataAdvance  
IoVpSessionDataDereference  
IoVpSessionDataReference

IoVpSessionDataClose  
IoVpSessionDataDeterminePolicy  
IoVpSessionDataAttachSurrogate  
IoVpSessionDataFinalizeSurrogate

sessnirp.h :

nothing special

trackirp.c :

IoVpInitIrpTracking  
IoVpDoAssertIrps  
FAIL\_CALLER\_OF\_IOFCALLDRIVER  
FAIL\_CALLER\_OF\_IOFCALLDRIVER2  
IoVpCallDriver1  
IoVpCallDriver2  
IoVpCompleteRequest1  
IoVpCompleteRequest2  
IoVpCompleteRequest3  
IoVpCompleteRequest4  
IoVpCompleteRequest5  
IoVpCompleteRequestApc  
IoVpAdvanceStackDownwards  
IoVpExamineIrpStackForwarding  
IoVpInternalCompletionTrap  
IoVpInternalCompleteAtDPC  
IoVpInternalCompleteAfterWait  
IoVpInternalDeferredCompletion  
IoVpSwapSurrogateIrp  
IoVpCancelIrp  
IoVpFreeIrp  
IoVpAllocateIrp1  
IoVpAllocateIrp2  
IoVpInitializeIrp  
IoVpAttachDeviceToDeviceStack  
IoVpDetachDevice  
IoVpDeleteDevice  
IoVpReexamineAllStacks  
IoVpEnumDevObjCallback

IovPlsInterestingStack  
IovPlsInterestingDriver  
IovpExamineDevObjForwarding  
IovpGetDeviceAttachedTo  
IovpGetLowestDevice  
IovpAssertNonLegacyDevice  
IovPlsInFdoStack  
IovpSeedOnePage  
IovpSeedTwoPages  
IovpSeedThreePages  
IovpSeedStack

trackirp.h :

SPECIAL\_IRP\_MARK\_NON\_TRACKABLE  
SPECIAL\_IRP\_IO\_CALL\_1  
SPECIAL\_IRP\_IO\_CALL\_2  
SPECIAL\_IRP\_IO\_COMPLETE\_1  
SPECIAL\_IRP\_IO\_COMPLETE\_2  
SPECIAL\_IRP\_IO\_COMPLETE\_3  
SPECIAL\_IRP\_IO\_COMPLETE\_4  
SPECIAL\_IRP\_IO\_COMPLETE\_5  
SPECIAL\_IRP\_IO\_CANCEL\_IRP  
IOP\_DIAG\_THROW\_CHAFF\_AT\_STARTED\_PDO\_STACK  
SPECIAL\_IRP\_IO\_FREE\_IRP  
SPECIAL\_IRP\_IO\_ALLOCATE\_IRP\_1  
SPECIAL\_IRP\_IO\_ALLOCATE\_IRP\_2  
SPECIAL\_IRP\_IO\_INITIALIZE\_IRP  
SPECIAL\_IRP\_IO\_DELETE\_DEVICE  
SPECIAL\_IRP\_IO\_ATTACH\_DEVICE\_TO\_DEVICE\_STACK  
SPECIAL\_IRP\_IO\_DETACH\_DEVICE  
SPECIAL\_IRP\_WATERMARK\_IRP  
SPECIAL\_IRP\_IOP\_COMPLETE\_REQUEST  
TRACK\_IRP\_DBGPRINT  
TRACK\_IRP\_DBGPRINT

triage.c :

TriagepGetPageSize  
TriagepVerifyDump

TriageGetTriagePointer  
TriageGetVersion  
TriageGetDriverCount  
TriageGetContext  
TriageGetExceptionRecord  
TriageActUpon  
TriageGetBugcheckData  
TriageGetLoaderEntry  
TriageGetMmInformation

write.c :

NtWriteFile  
NtWriteFileGather

```
#####  
#                               private/ntos/ioe                               #  
#####
```

Comment :

IoErr APIs.

```
#####  
#                               private/ntos/kd                               #  
#####
```

Abstract :

Kernel Debugger APIs

Prefix :

Kd

Files :

i386/kdcmsup.c  
i386/kdcpuapi.c  
i386/kdpcpu.h  
i386/kdreboot.c  
i386/kdstr.asm  
i386/kdtrap.c  
kdapi.c  
kdbreak.c  
kdcmio.c

```
kddata.c
kddbgi.o.c
kdinit.c
kdlck.c
kdmov.c
kdp.h
i386/kdcmsup.c :
    KdpQueryPerformanceCounter
i386/kdcpuapi.c :
    KdpIsTryFinallyReturn
    KdpLevelChange
    regValue
    KdpIsSpecialCall
    KdpGetReturnAddress
    KdpSetLoadState
    KdpSetStateChange
    KdpGetStateChange
    KdpReadControlSpace
    KdpWriteControlSpace
    KdpReadIoSpace
    KdpWriteIoSpace
    KdpReadMachineSpecificRegister
    KdpWriteMachineSpecificRegister
    KdpGetCallNextOffset
i386/kdpcpu.h :
    nothing special
i386/kdreboot.c :
    KdpReboot
i386/kdstr.asm :
    KdpCopyDataToStack
i386/kdtrap.c :
    KdpTrap
    KdIsThisAKdTrap
    KdpStub
kdapi.c :
    Convert100nsToMilliseconds
```



KdpDprintf  
KdEnterDebugger  
KdExitDebugger  
KdUpdateTimeSlipEvent  
KdpTimeSlipDpcRoutine  
KdpTimeSlipWork  
InternalBreakpointCheck  
KdSetInternalBreakpoint  
KdGetTraceInformation  
KdGetInternalBreakpoint  
KdpSendWaitContinue  
KdpReadVirtualMemory  
KdpReadVirtualMemory64  
KdpWriteVirtualMemory  
KdpWriteVirtualMemory64  
KdpGetContext  
KdpSetContext  
KdpWriteBreakpoint  
KdpRestoreBreakpoint  
SymNumFor  
PotentialNewSymbol  
DumpTraceData  
TraceDataRecordCallInfo  
SkippingWhichBP  
KdQuerySpecialCalls  
KdSetSpecialCall  
KdClearSpecialCalls  
KdpCheckTracePoint  
KdpSwitchProcessor  
KdpReportExceptionStateChange  
KdpReportLoadSymbolsStateChange  
KdpReadPhysicalMemory  
KdpWritePhysicalMemory  
KdpProcessInternalBreakpoint  
KdpGetVersion  
KdpNotSupported

KdpCauseBugCheck  
KdpWriteBreakPointEx  
KdpRestoreBreakPointEx  
KdDisableDebugger  
KdEnableDebugger  
KdpSearchMemory

kdbreak.c :

KdSetOwnedBreakpoints  
KdpLowWriteContent  
KdpDeleteBreakpoint  
KdpDeleteBreakpointRange  
KdpSuspendBreakpoint  
KdpSuspendAllBreakpoints  
KdpSuspendBreakpointRange  
KdpRestoreBreakpointRange  
KdpLowRestoreBreakpoint  
KdpRestoreAllBreakpoints  
KdDeleteAllBreakpoints

kdcomio.c :

KdpComputeChecksum  
KdpReceivePacketLeader  
KdpReceiveString  
KdpSendString  
KdpSendControlPacket  
KdpReceivePacket  
KdpSendPacket

kddata.c :

kddbgi.o.c :

KdpPrintString  
KdpPromptString

kdinit.c :

KdInitSystem  
KdRegisterDebuggerDataBlock  
KdDeregisterDebuggerDataBlock  
KdLogDbgPrint



i386/apcuser.c  
i386/biosa.asm  
i386/biosc.c  
i386/callback.c  
i386/callout.asm  
i386/clockint.asm  
i386/cpu.asm  
i386/cpu.inc  
i386/ctxswap.asm  
i386/cyrix.c  
i386/emv86.asm  
i386/emxcptn.asm  
i386/exceptn.c  
i386/flush.c  
i386/flushtb.c  
i386/gdtsup.c  
i386/i386init.c  
i386/i386pcr.asm  
i386/instemul.asm  
i386/int.asm  
i386/intobj.c  
i386/intsup.asm  
i386/iopm.c  
i386/kernlini.c  
i386/ki386.h  
i386/kimacro.inc  
i386/largepa.c  
i386/ldtsup2.asm  
i386/ldtsup.c  
i386/mi.inc  
i386/misc.c  
i386/mpipia.asm  
i386/mtrr.c  
i386/mtrr.h  
i386/mtrrand.c  
i386/newsysbg.asm

i386/p2w.asm  
i386/pat.c  
i386/pat.h  
i386/procstat.asm  
i386/spindbg.asm  
i386/spininst.asm  
i386/spinlock.asm  
i386/threadbg.asm  
i386/thredini.c  
i386/timindex.asm  
i386/trap.asm  
i386/trapc.c  
i386/vdm.c  
i386/vdmint21.c  
i386/vdmp.h  
i386/zero.asm  
apcobj.c  
apcsup.c  
balmgr.c  
bugcheck.c  
channel.c  
config.c  
debug.c  
devquobj.c  
dpcobj.c  
dpcsup.c  
eventobj.c  
genxx.h  
genxx.inc  
kernldat.c  
ki.h  
kiinit.c  
misc.c  
mutntobj.c  
procobj.c  
profobj.c

queueobj.c  
raisexcp.c  
semphobj.c  
thredobj.c  
thredsup.c  
timerobj.c  
timersup.c  
wait.c  
waitsup.c  
xipi.c  
yield.c

i386/abios.h :

nothing special

i386/abiosa.asm :

STACK32\_TO\_STACK16  
STACK16\_TO\_STACK32  
COPY\_CALL\_FRAME  
KiAbiosGetGdt  
KiI386CallAbios  
KeI386Call16BitFunction  
KeI386Call16BitCStyleFunction

i386/abiosc.c :

KiInitializeAbiosGdtEntry  
KiI386SelectorBase  
KeI386GetLid  
KeI386ReleaseLid  
KeI386AbiosCall  
KeI386AllocateGdtSelectors  
KeI386ReleaseGdtSelectors  
KeI386FlatToGdtSelector  
Ki386InitializeGdtFreeList  
KiInitializeAbios

i386/allproc.c :

KeStartAllProcessors  
KiCloneSelector  
KiCloneDescriptor

i386/alr.inc :  
    assembler specific definition

i386/apcuser.c :  
    KiInitializeUserApc

i386/biosa.asm :  
    Ki386SetupAndExitToV86Code

i386/biosc.c :  
    Ke386CallBios

i386/callback.c :  
    KeUserModeCallback  
    NtW32Call

i386/callout.asm :  
    KiCallUserMode  
    KeSwitchKernelStack  
    KiGetUserModeStackAddress  
    NtCallbackReturn

i386/clockint.asm :  
    KeUpdateSystemTime  
    KeUpdateRunTime  
    KeProfileInterrupt  
    KeProfileInterruptWithSource

i386/cpu.asm :  
    KiSetProcessorType  
    CpuIdTrap6  
    Get386Stepping  
    Get486Stepping  
    Check486AStepping  
    Check486BStepping  
    Temporary486Int6  
    Check486CStepping  
    Check386B0  
    TemporaryInt6  
    Check386D1  
    TemporaryInt1  
    MultiplyTest  
    Multiply

KiIsNpxPresent  
CPUID  
RDTSC  
RDMSR  
WRMSR  
KeYieldProcessor

i386/cpu.inc :

assembler specific definition

i386/ctxswap.asm :

KiUnlockDispatcherDatabase  
KiSwapThread  
KiDispatchInterrupt  
SwapContext  
KeInterlockedSwapPte  
KeFlushCurrentTb  
KiFlushDcache  
KiFlushIcache  
Ki386EnableGlobalPage  
Ki386EnableFxsr  
Ki386EnableXMMExceptions  
Ki386EnableCurrentLargePage  
KiFlushSingleTb  
KiSwapProcess  
KiAdjustEsp0

i386/cyrix.c :

Ke386CyrixId  
ReadCyrixRegister  
WriteCyrixRegister  
Ke386ConfigureCyrixProcessor

i386/emv86.asm :

Ki386DispatchOpcodeV86  
OpcodeInvalidV86  
OpcodeGenericPrefixV86  
OpcodeINSBV86  
OpcodeINSWV86  
OpcodeOUTSBV86



OpcodeOUTSWV86  
OpcodePUSHFV86  
OpcodePOPFV86  
OpcodeINTnnV86  
OpcodeINTOV86  
OpcodeIRETV86  
OpcodeINBimmV86  
OpcodeINWimmV86  
OpcodeOUTBimmV86  
OpcodeOUTWimmV86  
OpcodeINBV86  
OpcodeINWV86  
OpcodeOUTBV86  
OpcodeOUTWV86  
OpcodeCLIV86  
OpcodeSTIV86  
VdmDispatchIntAck  
OpcodeHLTV86  
OpcodeNPXV86  
KiVdmSetUserCRO

i386/emxcptn.asm :

KiEm87StateToNpxFrames  
KiNpxFrameToEm87State

i386/exceptn.c :

KiEspFromTrapFrame  
KiEspToTrapFrame  
KiSegSsFromTrapFrame  
KiSegSsToTrapFrame  
KeContextFromKframes  
KeContextToKframes  
KiDispatchException  
KiCopyInformation  
KeRaiseUserException

i386/flush.c :

KeSweepDcache  
KeSweepIcache

KeSweepIcacheRange  
KeInvalidateAllCaches  
KeInvalidateAllCachesTarget

i386/flushb.c :

KeFlushEntireTb  
KiFlushTargetEntireTb  
KeFlushMultipleTb  
KiFlushTargetMultipleTb  
KeFlushSingleTb  
KiFlushTargetSingleTb  
KiFlushSingleTbSynchronous  
KiFlushTargetSingleTbSynchronous  
Ki386UseSynchronousTbFlush

i386/gdtsup.c :

Ke386GetGdtEntryThread  
KeI386SetGdtSelector

i386/i386init.c :

KiInitializeGDT  
KiInitializeGdtEntry  
KiInitializeMachineType

i386/i386pcr.asm :

KeGetPcr  
KeGetCurrentPrcb  
KeGetCurrentThread  
KeGetPreviousMode  
KeIsExecutingDpc  
GetMachineBootPointers

i386/instemul.asm :

Ki386DispatchOpcode  
OpcodeInvalid  
OpcodeGenericPrefix  
OpcodeOF  
OpcodeINSB  
OpcodeINSW  
OpcodeOUTSB  
OpcodeOUTSW

OpcodeINTnn  
OpcodeINTO  
OpcodeINBimm  
OpcodeINWimm  
OpcodeOUTBimm  
OpcodeOUTWimm  
OpcodeINB  
OpcodeINW  
OpcodeOUTB  
OpcodeOUTW  
OpcodeCLI  
OpcodeSTI  
CheckVdmFlags  
GetVirtualBits  
SetVirtualBits  
Ki386VdmReflectException  
Ki386VdmSegmentNotPresent  
VdmDispatchException  
PushInt  
CsToLinear  
CheckEip  
SsToLinear  
CheckEsp  
SwitchToHandlerStack  
GetHandlerAddress  
PushException  
Ki386VdmEnablePentiumExtensions

i386/int.asm :

KiPassiveRelease  
KiDisableInterrupts  
KiRestoreInterrupts

i386/intobj.c :

KeInitializeInterrupt  
KeConnectInterrupt  
KeDisconnectInterrupt  
KiGetVectorInfo

KiConnectVectorAndInterruptObject

i386/intsup.asm :

KeSynchronizeExecution  
KiChainedDispatch  
KiInterruptDispatch2ndLvl  
KiFloatingDispatch  
KiInterruptDispatch  
KiShutUpAssembler  
KiUnexpectedInterrupt

i386/iopm.c :

Ke386SetIoAccessMap  
KiSetIoMap  
Ke386QueryIoAccessMap  
Ke386IoSetAccessProcess  
KiLoadIopmOffset  
Ke386SetIOPL

i386/kernlini.c :

KiInitializeKernel  
KiInitializePcr  
KiInitializeDbgFaultTSS  
KiInitializeTSS  
KiInitializeTSS2  
KiSwapIDT  
KiGetCpuVendor  
KiGetFeatureBits  
KiGetCacheInformation  
KiInitMachineDependent  
KeOptimizeProcessorControlState  
KeSetup80387OrEmulate  
KiMoveRegTree  
KiI386PentiumLockErrataFixup

i386/ki386.h :

KiGetPpeIndex  
KiGetPdeIndex  
KiGetPteIndex

i386./kimacro.inc :

POLL\_DEBUGGER  
ASSERT\_FS  
SET\_DEBUG\_DATA  
ENTER\_DR\_ASSIST  
ENTER\_SYSCALL  
ENTER\_INTERRUPT  
ENTER\_INTERRUPT\_FORCE\_STATE  
ENTER\_TRAP  
EXIT\_ALL  
INTERRUPT\_EXIT  
SPURIOUS\_INTERRUPT\_EXIT  
ENTER\_TRAPV86  
EXIT\_TRAPV86

i386/largepag.c :

Ki386CreateIdentityMap  
Ki386AllocateContiguousMemory  
Ki386IdentityMapMakeValid  
Ki386MapAddress  
Ki386ConvertPte  
Ki386BuildIdentityBuffer  
Ki386ClearIdentityMap  
Ki386EnableTargetLargePage

i386/ldtsup2.asm :

KiLoadLdtr  
KiFlushDescriptors

i386/ldtsup.c :

Ke386SetLdtProcess  
Ki386LoadTargetLdtr  
Ke386SetDescriptorProcess  
Ki386FlushTargetDescriptors

i386/mi.inc :

nothing special

i386/misc.c :

Kix86FxSave  
Kix86FnSave  
Kix86LdMXCsr

Kix86StMXCsr  
KeSaveFloatingPointState  
KeRestoreFloatingPointState  
KeSaveStateForHibernate

i386/mpipia.asm :

KiIpiServiceRoutine  
KiIpiSend  
KiIpiSendPacket  
KiIpiSignalPacketDone  
KiIpiSignalPacketDoneAndStall

i386/mtrr.c :

KiInitializeMTRR  
KeRestoreMtrr  
KeSetPhysicalCacheTypeRange  
KiRemoveRange  
KiAddRange  
KiStartEffectiveRangeChange  
KiCompleteEffectiveRangeChange  
KiRangeWeight  
KiMaskToLength  
KiLengthToMask  
KiFindFirstSetRightBit  
KiFindFirstSetLeftBit  
KiDumpMTRR  
KiLoadMTRRTarget  
KiLoadMTRR  
KiSynchronizeMTRRLoad

i386/mtrr.h :

nothing special

i386/mtrrand.c :

KiAmdK6InitializeMTRR  
KiAmdK6MTRRAddRegionFromHW  
KiAmdK6MtrrSetMemoryType  
KiAmdK6HandleWcRegionRequest  
KiAmdK6AddRegion  
KiAmdK6FindFreeRegion

KiAmdK6MtrrCommitChanges  
KiAmdK6MtrrWRMSR  
i386/newsysbg.asm :  
KiSystemStartup  
KiRetireDpcList  
KiSetCROBits  
KiPollDebugger  
i386/p2w.asm :  
p2w  
i386/pat.c :  
KeRestorePAT  
KiInitializePAT  
KiLoadPATTarget  
KiLoadPAT  
KiSynchronizePATLoad  
i386/pat.h :  
nothing special  
i386/procstat.asm :  
KiSaveProcessorState  
KiSaveProcessorControlState  
KiRestoreProcessorState  
KiRestoreProcessorControlState  
i386/spindbg.asm :  
Ki i386SpinOnSpinLock  
i386/spininst.asm :  
KeInializeSpinLock  
SpinLockLazyInit  
KeFreeSpinLock  
KeInializeSpinLock2  
KeAcquireSpinLock  
KeReleaseSpinLock  
KiAcquireSpinLock  
KiReleaseSpinLock  
KeTryToAcquireSpinLock  
KiTryToAcquireSpinLock  
KiInst\_AcquireSpinLock

KiInst\_SpinOnSpinLock  
KiInst\_ReleaseSpinLock  
i386/spinlock.asm :  
KeInitializeSpinLock  
KeAcquireSpinLockAtDpcLevel  
KeAcquireSpinLockFromDpcLevel  
KeReleaseSpinLockFromDpcLevel  
KiAcquireSpinLock  
KiReleaseSpinLock  
KeTryToAcquireSpinLock  
KiTryToAcquireSpinLock  
KeTestSpinLock  
KiAcquireQueuedSpinLock  
KiReleaseQueuedSpinLock  
KiTryToAcquireQueuedSpinLock  
i386/threadbg.asm :  
KiThreadStartup  
i386/thredini.c :  
KiInitializeContextThread  
KeSetAutoAlignmentProcess  
KeSetAutoAlignmentThread  
KepSetAlignmentSpecialApc  
i386/timindex.asm :  
KiComputeTimerTableIndex  
i386/trap.asm :  
FAST\_V86\_TRAP\_D  
DISPATCH\_USER\_APC  
Ki16BitStackException  
KiSystemService  
KiGetTickCount  
KiCallbackReturn  
KiSetLowWaitHighThread  
KiExceptionExit  
Kei386EoiHelper  
KiUnexpectedInterruptTail



CommonDispatchException  
VERIFY\_BASE\_TRAP\_FRAME  
KiRestoreBaseFrame  
KiTrap00  
KiTrap01  
KiTrap02  
KiDebugService  
KiTrap03  
KiTrap04  
KiTrap05  
KiTrap06  
KiTrap07  
KiTrap08  
KiTrap09  
KiTrap0A  
KiTrap0B  
KiTrap0C  
KiTrap0D  
KeInvalidAccessAllowed  
KiTrap0E  
KiTrap0F  
KiTrap10  
KiTrap11  
KiTrap13  
KiCoprocesorError  
KiFlushNPXState  
KiSetHardwareTrigger  
KiSystemFatalException  
NtContinue  
NtRaiseException  
Ki386VdmReflectException\_A

i386/trap.c :

Ki386CheckDivideByZeroTrap  
KiNextIStreamByte  
Ki386CheckDelayedNpxTrap

i386/vdm.c :

Ki386GetSelectorParameters  
Ki386VdmDispatchIo  
Ki386VdmDispatchStringIo  
VdmDispatchIoToHandler  
VdmDispatchUnalignedIoToHandler  
VdmDispatchStringIoToHandler  
VdmCallStringIoHandler  
VdmConvertToLinearAddress  
KeI386VdmInitialize  
Ke386VdmInsertQueueApc  
Ke386VdmClearApcObject  
TestIoByteRoutine  
TestIoWordReadRoutine  
TestIoWordWriteRoutine  
TestIoDwordRoutine  
TestIoStringRoutine  
TestIoHandlerStuff

i386/vdmint21.c :

Ke386SetVdmInterruptHandler  
Ki386LoadTargetInt21Entry

i386/vdmp.h :

nothing special

i386/zero.asm :

KeZeroPage  
KiXMMIZeroPageNoSave  
KiXMMIZeroPage  
KiZeroPage

apcobj.c :

KeInitializeApc  
KeFlushQueueApc  
KeInsertQueueApc  
KeRemoveQueueApc

apcsup.c :

KiDeliverApc  
KiInsertQueueApc

balmgr.c :

KeBalanceSetManager  
KeSwapProcessOrStack  
KiInSwapKernelStacks  
KiInSwapProcesses  
KiOutSwapKernelStacks  
KiOutSwapProcesses  
KiScanReadyQueues

bugcheck.c :

KeBugCheck  
KeGetBugMessageText  
KeBugCheckUnicodeToAnsi  
KiBugCheckDebugBreak  
KiPcToFileHeader  
KiDumpParameterImages  
KeBugCheckEx  
KeEnterKernelDebugger  
KeDeregisterBugCheckCallback  
KeRegisterBugCheckCallback  
KiScanBugCheckCallbackList

channel.c :

NtCreateChannel  
NtListenChannel  
NtOpenChannel  
NtReplyWaitSendChannel  
NtSendWaitReplyChannel  
NtSetContextChannel  
KiAllocateReceiveBufferChannel  
KiChannelInitialization  
KiCloseChannel  
KiDeleteChannel  
KiRundownChannel  
KiListenChannel  
KiRendezvousWithThread

config.c :

KeFindConfigurationEntry  
KeFindConfigurationNextEntry

debug.c :

- KeFreezeExecution
- KiFreezeTargetExecution
- KeSwitchFrozenProcessor
- KeThawExecution
- KeReturnToFirmware
- KiPollFreezeExecution

devquobj.c :

- KeInitializeDeviceQueue
- KeInsertDeviceQueue
- KeInsertByKeyDeviceQueue
- KeRemoveDeviceQueue
- KeRemoveByKeyDeviceQueue
- KeRemoveEntryDeviceQueue

dpcobj.c :

- KeInitializeDpc
- KeInsertQueueDpc
- KeRemoveQueueDpc
- KeSetImportanceDpc
- KeSetTargetProcessorDpc

dpcsup.c :

- KiQuantumEnd
- KiCheckTimerTable
- KiTimerExpiration
- KiTimerListExpire

eventobj.c :

- KeInitializeEvent
- KeInitializeEventPair
- KeClearEvent
- KePulseEvent
- KeReadStateEvent
- KeResetEvent
- KeSetEvent
- KeSetEventBoostPriority

genxx.h :

- genDef

genAlt  
genCom  
genNam  
genNamUint  
genVal  
genValUint  
genSpc  
genStr  
genTxt  
DisableInc  
EnableInc  
setPath  
ROUND\_UP  
OFFSET

genxx.inc :

assembler specific definitions

kernldat.c :

ki.h :

ClearMember  
SetMember  
FindFirstSetLeftMember  
KiLockApcQueue  
KiUnlockApcQueue  
KiLockContextSwap  
KiUnlockContextSwap  
KiQueuedSpinLockContext  
KiBoostPriorityThread  
KiInsertWaitList  
IPI\_INSTRUMENT\_COUNT  
KiIpiSendSynchronousPacket  
KiRemoveTreeTimer  
KiRequestApcInterrupt  
KiRequestDispatchInterrupt  
KiWaitSatisfyAny  
KiWaitSatisfyMutant

KiWaitSatisfyOther

kiinit.c :

KeInitSystem

KiInitSystem

KiComputeReciprocal

misc.c :

KeEnterCriticalRegion

KeLeaveCriticalRegion

KeQueryInterruptTime

KeQuerySystemTime

KeQueryTickCount

KeQueryTimeIncrement

KeSetDmaIoCoherency

KeSetProfileIrql

KeSetSynchIrql

KeSetSystemTime

KiAdjustInterruptTime

KiCalibrateTimeAdjustment

KeSetTimeIncrement

KeAddSystemServiceTable

KeSetSwapContextNotifyRoutine

KeSetThreadSelectNotifyRoutine

KeSetTimeUpdateNotifyRoutine

KeQueryActiveProcessors

mutntobj.c :

KeInitializeMutant

KeInitializeMutex

KeReadStateMutant

KeReleaseMutant

KeReleaseMutex

procobj.c :

KeInitializeProcess

KeAttachProcess

KeForceAttachProcess

KeStackAttachProcess

KeDetachProcess

KeUnstackDetachProcess  
KeReadStateProcess  
KeSetProcess  
KeSetPriorityProcess  
KeSetDisableQuantumProcess  
KiAttachProcess  
KiMoveApcState

profobj.c :

KeInitializeProfile  
KeQueryIntervalProfile  
KeSetIntervalProfile  
KeStartProfile  
KeStopProfile  
KiStopProfileInterrupt  
KiStartProfileInterrupt

queueobj.c :

KeInitializeQueue  
KeReadStateQueue  
KeInsertQueue  
KeInsertHeadQueue  
KeRemoveQueue  
KeRundownQueue  
KiActivateWaiterQueue  
KiInsertQueue

raisexc.c :

KiContinuePreviousModeUser  
KiContinue  
KiRaiseException

semphobj.c :

KeInitializeSemaphore  
KeReadStateSemaphore  
KeReleaseSemaphore

thredobj.c :

KeInitializeThread  
KeAlertThread  
KeAlertResumeThread

KeBoostPriorityThread  
KeConfineThread  
KeDisableApcQueuingThread  
KeEnableApcQueuingThread  
KeForceResumeThread  
KeFreezeAllThreads  
KeQueryAutoAlignmentThread  
KeQueryBasePriorityThread  
KeQueryPriorityThread  
KeReadStateThread  
KeReadyThread  
KeResumeThread  
KeRevertToUserAffinityThread  
KeRundownThread  
KeSetAffinityThread  
KeSetSystemAffinityThread  
KeSetBasePriorityThread  
KeSetDisableBoostThread  
KeSetIdealProcessorThread  
KeSetKernelStackSwapEnable  
KeSetPriorityThread  
KeSuspendThread  
KeTerminateThread  
KeTestAlertThread  
KeThawAllThreads

thredsup.c :

KiSuspendNop  
KiFindReadyThread  
KiReadyThread  
KiSelectNextThread  
KiSetPriorityThread  
KiSuspendThread  
KiVerifyReadySummary

timerobj.c :

KeInitializeTimer  
KeInitializeTimerEx



KeClearTimer  
KeCancelTimer  
KeReadStateTimer  
KeSetTimer  
KeSetTimerEx  
KeQueryTimerDueTime  
KeCheckForTimer

timersup.c :

KiInsertTreeTimer  
KiReinsertTreeTimer  
KiInsertTimerTable

wait.c :

TestForAlertPending  
KiAdjustQuantumThread  
KeDelayExecutionThread  
KeWaitForMultipleObjects  
KeWaitForSingleObject  
KiSetServerWaitClientEvent  
KiComputeWaitInterval

waitsup.c :

KiUnwaitThread  
KeBoostCurrentThread  
KiWaitSatisfyAll  
KiWaitTest

xipi.c :

KiIpiGenericCall  
KiIpiGenericCallTarget  
KiIpiStallOnPacketTargets

yield.c :

NtYieldExecution

```
#####  
#                               private/ntos/lfs                               #  
#####
```

Comment :

Log File Service.

```
#####  
# private/ntos/lpc #  
#####
```

Abstract :

Local Procedure Call

Prefix :

Lpc

Files :

i386/lpcmove.asm  
lpcclose.c  
lpccompl.c  
lpcconn.c  
lpccreat.c  
lpcinit.c  
lpclistn.c  
lpcp.h  
lpcpriv.c  
lpcquery.c  
lpcqueue.c  
lpcrecv.c  
lpcreply.c  
lpcsend.c  
uclient.c  
ulpc.h  
userver.c

i386/lpcmove.asm :

LpcpMoveMessage

lpcclose.c :

LpcpClosePort  
LpcpDeletePort  
LpcExitThread

lpccompl.c :

NtAcceptConnectPort  
NtCompleteConnectPort  
LpcpPrepareToWakeClient

Ipcconn.c :

- NtConnectPort
- NtSecureConnectPort
- LpcpFreeConMsg

Ipccreat.c :

- NtCreatePort
- NtCreateWaitablePort
- LpcpCreatePort

Ipcinit.c :

- LpcInitSystem
- LpcpGetCreatorName
- LpcpPortExtraDataCreate
- LpcpPortExtraDataDestroy
- LpcpPortExtraDataPush
- LpcpSaveThread

Ipclistn.c :

- NtListenPort

Ipcp.h :

- LpcpGenerateMessageId
- LpcpGenerateCallbackId
- LpcpInitializeLpcpLock
- LpcpAcquireLpcpLock
- LpcpReleaseLpcpLock
- LpcpGetDynamicClientSecurity
- LpcpFreeDynamicClientSecurity
- LpcpReferencePortObject

Ipcpriv.c :

- NtImpersonateClientOfPort
- LpcpFreePortClientSecurity

Ipcquery.c :

- NtQueryInformationPort

Ipcqueue.c :

- LpcpInitializePortQueue
- LpcpDestroyPortQueue
- LpcpInitializePortZone
- LpcpExtendPortZone

LpcpAllocateFromPortZone  
LpcpFreeToPortZone  
LpcpSaveDataInfoMessage  
LpcpFreeDataInfoMessage  
LpcpFindDataInfoMessage  
Ipcrecv.c :  
NtReplyWaitReceivePort  
NtReplyWaitReceivePortEx  
Ipcreply.c :  
NtReplyPort  
NtReplyWaitReplyPort  
NtReadRequestData  
NtWriteRequestData  
LpcpCopyRequestData  
Ipcsend.c :  
NtRequestPort  
NtRequestWaitReplyPort  
LpcRequestPort  
LpcRequestWaitReplyPort  
uclient.c :  
Usermode LPC  
ulpc.h :  
Usermode Test (uclient.c, userver.c)  
userver.c :  
Usermode LPC

```
#####  
# private/ntos/mm #  
#####
```

Abstract :

Memory Manager

Prefix :

Mm

Acronym :

VA (Virtual Address)

PTE (Page Table Entry)

VAD (Virtual Address Descriptor)

Files :

i386/data386.c  
i386/debugsup.c  
i386/hypermap.c  
i386/init386.c  
i386/mi386.h  
i386/mipae.h  
i386/probewrt.c  
i386/setmodify.c  
accesschk.c  
addrsup.c  
allocpag.c  
allocvm.c  
checkpfn.c  
checkpte.c  
creasect.c  
deleteva.c  
dmpaddr.c  
dynmem.c  
extsect.c  
flushbuf.c  
flushsec.c  
forksup.c  
freevm.c  
iosup.c  
lockvm.c  
mapcache.c  
mapview.c  
mi.h  
miglobal.c  
mmfault.c  
mminit.c  
mmquota.c  
mmsup.c  
modwrite.c

pagfault.c  
pfndec.c  
pfnlist.c  
physical.c  
procsup.c  
protect.c  
querysec.c  
queryvm.c  
readwrt.c  
sectsup.c  
session.c  
sessload.c  
shutdown.c  
super.c  
sysload.c  
sysptes.c  
umapview.c  
vadtree.c  
verifier.c  
vlm.c  
wrtfault.c  
wslst.c  
wsmanage.c  
wstree.c  
zeropage.c

i386/data386.c :

Memory Manager가

i386

i386/debugsup.c :

MmDbgReadCheck

MmDbgWriteCheck

MmDbgReleaseAddress

MmDbgReadCheck64

MmDbgWriteCheck64

MmDbgTranslatePhysicalAddress64

i386/hypermap.c :

MiMapPageInHyperSpace

MiMapImageHeaderInHyperSpace  
MiUnmapImageHeaderInHyperSpace  
MiMapPageToZeroInHyperSpace

i386/init386.c :

MiInitMachineDependent  
MiRemoveLowPages  
MiAllocateLowMemory  
MiFreeLowMemory  
MiCheckPhysicalPagePattern

i386/mi386.h :

MI\_MAKE\_VALID\_PTE  
MI\_MAKE\_VALID\_PTE\_TRANSITION  
MI\_MAKE\_TRANSITION\_PTE  
MI\_MAKE\_TRANSITION\_PTE\_VALID  
MI\_SET\_PTE\_IN\_WORKING\_SET  
MI\_GET\_WORKING\_SET\_FROM\_PTE  
MI\_SET\_PTE\_WRITE\_COMBINE  
MI\_SET\_PTE\_DIRTY  
MI\_SET\_PTE\_CLEAN  
MI\_IS\_PTE\_DIRTY  
MI\_SET\_GLOBAL\_BIT\_IF\_SYSTEM  
MI\_SET\_GLOBAL\_STATE  
MI\_ENABLE\_CACHING  
MI\_DISABLE\_CACHING  
MI\_IS\_CACHING\_DISABLED  
MI\_SET\_PFN\_DELETED  
MI\_IS\_PFN\_DELETED  
MI\_CHECK\_PAGE\_ALIGNMENT  
MI\_INITIALIZE\_HYPERSPACE\_MAP  
MI\_GET\_PAGE\_COLOR\_FROM\_PTE  
MI\_GET\_PAGE\_COLOR\_FROM\_VA  
MI\_GET\_PAGE\_COLOR\_FROM\_SESSION  
MI\_PAGE\_COLOR\_PTE\_PROCESS  
MI\_PAGE\_COLOR\_VA\_PROCESS  
MI\_GET\_NEXT\_COLOR  
MI\_GET\_PREVIOUS\_COLOR

MI\_GET\_SECONDARY\_COLOR  
MI\_GET\_COLOR\_FROM\_SECONDARY  
MI\_GET\_MODIFIED\_PAGE\_BY\_COLOR  
MI\_GET\_MODIFIED\_PAGE\_ANY\_COLOR  
MI\_MAKE\_VALID\_PTE\_WRITE\_COPY  
MI\_DETERMINE\_OWNER  
MI\_SET\_ACCESSED\_IN\_PTE  
MI\_GET\_ACCESSED\_IN\_PTE  
MI\_SET\_OWNER\_IN\_PTE  
MI\_GET\_OWNER\_IN\_PTE  
MI\_SET\_PAGING\_FILE\_INFO  
MiPteToProto  
MiProtoAddressForPte  
MiProtoAddressForKernelPte  
MiGetSubsectionAddress  
MiGetSubsectionAddressForPte  
MiGetPpeAddress  
MiGetPdeAddress  
MiGetPteAddress  
MiGetPpeOffset  
MiGetPdeOffset  
MiGetPteOffset  
MiGetVirtualAddressMappedByPpe  
MiGetVirtualAddressMappedByPde  
MiGetVirtualAddressMappedByPte  
MiIsVirtualAddressOnPpeBoundary  
MiIsVirtualAddressOnPdeBoundary  
MiIsPteOnPpeBoundary  
MiIsPteOnPdeBoundary  
MiDoesPpeExistAndMakeValid  
GET\_PAGING\_FILE\_NUMBER  
GET\_PAGING\_FILE\_OFFSET  
IS\_PTE\_NOT\_DEMAND\_ZERO  
MI\_MAKING\_VALID\_PTE\_INVALID  
MI\_MAKING\_MULTIPLE\_PTES\_INVALID  
MI\_MAKE\_PROTECT\_WRITE\_COPY



MI\_SET\_PAGE\_DIRTY  
MI\_NO\_FAULT\_FOUND  
MI\_CAPTURE\_DIRTY\_BIT\_TO\_PFN  
MI\_IS\_PHYSICAL\_ADDRESS  
MI\_CONVERT\_PHYSICAL\_TO\_PFN  
MI\_GET\_PAGE\_FRAME\_FROM\_PTE  
MI\_GET\_PAGE\_FRAME\_FROM\_TRANSITION\_PTE  
MI\_GET\_PROTECTION\_FROM\_SOFT\_PTE  
MI\_GET\_PROTECTION\_FROM\_TRANSITION\_PTE  
MI\_WRITE\_VALID\_PTE  
MI\_WRITE\_INVALID\_PTE  
MI\_WRITE\_VALID\_PTE\_NEW\_PROTECTION  
MiFillMemoryPte  
MI\_IS\_PAGE\_TABLE\_ADDRESS  
MI\_IS\_KERNEL\_PAGE\_TABLE\_ADDRESS  
MI\_IS\_PAGE\_DIRECTORY\_ADDRESS  
MI\_IS\_HYPER\_SPACE\_ADDRESS  
MI\_IS\_PROCESS\_SPACE\_ADDRESS  
MI\_IS\_PTE\_PROTOTYPE  
MI\_IS\_SYSTEM\_CACHE\_ADDRESS  
MI\_BARRIER\_SYNCHRONIZE  
MI\_BARRIER\_STAMP\_ZEROED\_PAGE  
MI\_FLUSH\_SINGLE\_SESSION\_TB  
MI\_FLUSH\_ENTIRE\_SESSION\_TB

i386/mipae.h :

MI\_MAKE\_VALID\_PTE  
MI\_MAKE\_VALID\_PTE\_TRANSITION  
MI\_MAKE\_TRANSITION\_PTE  
MI\_MAKE\_TRANSITION\_PTE\_VALID  
MI\_SET\_PTE\_IN\_WORKING\_SET  
MI\_GET\_WORKING\_SET\_FROM\_PTE  
MI\_SET\_PTE\_WRITE\_COMBINE  
MI\_SET\_PTE\_DIRTY  
MI\_SET\_PTE\_CLEAN  
MI\_IS\_PTE\_DIRTY  
MI\_SET\_GLOBAL\_BIT\_IF\_SYSTEM

MI\_SET\_GLOBAL\_STATE  
MI\_ENABLE\_CACHING  
MI\_DISABLE\_CACHING  
MI\_IS\_CACHING\_DISABLED  
MI\_SET\_PFN\_DELETED  
MI\_IS\_PFN\_DELETED  
MI\_CHECK\_PAGE\_ALIGNMENT  
MI\_INITIALIZE\_HYPERSPACE\_MAP  
MI\_GET\_PAGE\_COLOR\_FROM\_PTE  
MI\_GET\_PAGE\_COLOR\_FROM\_VA  
MI\_GET\_PAGE\_COLOR\_FROM\_SESSION  
MI\_PAGE\_COLOR\_PTE\_PROCESS  
MI\_PAGE\_COLOR\_VA\_PROCESS  
MI\_GET\_NEXT\_COLOR  
MI\_GET\_PREVIOUS\_COLOR  
MI\_GET\_SECONDARY\_COLOR  
MI\_GET\_COLOR\_FROM\_SECONDARY  
MI\_GET\_MODIFIED\_PAGE\_BY\_COLOR  
MI\_GET\_MODIFIED\_PAGE\_ANY\_COLOR  
MI\_MAKE\_VALID\_PTE\_WRITE\_COPY  
MI\_DETERMINE\_OWNER  
MI\_SET\_ACCESSED\_IN\_PTE  
MI\_GET\_ACCESSED\_IN\_PTE  
MI\_SET\_OWNER\_IN\_PTE  
MI\_GET\_OWNER\_IN\_PTE  
MI\_SET\_PAGING\_FILE\_INFO  
MiPteToProto  
MiProtoAddressForPte  
MiProtoAddressForKernelPte  
MiGetSubsectionAddress  
MiGetSubsectionAddressForPte  
MiGetPpeAddress  
MiGetPteAddress  
MiGetPpeOffset  
MiGetPdPteOffset  
MiGetPdeOffset

MiGetPpePdeOffset  
MiGetPteOffset  
MiGetVirtualAddressMappedByPpe  
MiGetVirtualAddressMappedByPde  
MiGetVirtualAddressMappedByPte  
MiIsVirtualAddressOnPpeBoundary  
MiIsVirtualAddressOnPdeBoundary  
MiIsPteOnPpeBoundary  
MiIsPteOnPdeBoundary  
MiDoesPpeExistAndMakeValid  
GET\_PAGING\_FILE\_NUMBER  
GET\_PAGING\_FILE\_OFFSET  
IS\_PTE\_NOT\_DEMAND\_ZERO  
MI\_MAKING\_VALID\_PTE\_INVALID  
MI\_MAKING\_MULTIPLE\_PTES\_INVALID  
MI\_MAKE\_PROTECT\_WRITE\_COPY  
MI\_SET\_PAGE\_DIRTY  
MI\_NO\_FAULT\_FOUND  
MI\_CAPTURE\_DIRTY\_BIT\_TO\_PFN  
MI\_IS\_PHYSICAL\_ADDRESS  
MI\_CONVERT\_PHYSICAL\_TO\_PFN  
MI\_GET\_PAGE\_FRAME\_FROM\_PTE  
MI\_GET\_PAGE\_FRAME\_FROM\_TRANSITION\_PTE  
MI\_GET\_PROTECTION\_FROM\_SOFT\_PTE  
MI\_GET\_PROTECTION\_FROM\_TRANSITION\_PTE  
MI\_WRITE\_VALID\_PTE  
MI\_WRITE\_INVALID\_PTE  
MI\_WRITE\_VALID\_PTE\_NEW\_PROTECTION  
MiFillMemoryPte  
MI\_IS\_PAGE\_TABLE\_ADDRESS  
MI\_IS\_KERNEL\_PAGE\_TABLE\_ADDRESS  
MI\_IS\_PAGE\_DIRECTORY\_ADDRESS  
MI\_IS\_HYPER\_SPACE\_ADDRESS  
MI\_IS\_PROCESS\_SPACE\_ADDRESS  
MI\_IS\_PTE\_PROTOTYPE  
MI\_IS\_SYSTEM\_CACHE\_ADDRESS

MI\_BARRIER\_SYNCHRONIZE  
MI\_BARRIER\_STAMP\_ZEROED\_PAGE  
MI\_FLUSH\_SINGLE\_SESSION\_TB  
MI\_FLUSH\_ENTIRE\_SESSION\_TB

i386/probewrt.c :

MmProbeForWrite

i386/setmodify.c :

MiSetModifyBit  
MiDetermineUserGlobalPteMask  
MiSetDirtyBit

accesschk.c :

MiAccessCheck  
MiCheckForUserStackOverflow

addrsup.c :

MiReorderTree  
MiGetNextNode  
MiGetPreviousNode  
MiGetFirstNode  
MiInsertNode  
MiRemoveNode  
MiLocateAddressInTree  
MiCheckForConflictingNode  
MiFindEmptyAddressRangeInTree  
MiFindEmptyAddressRangeDownTree  
NodeTreeWalk

allocpag.c :

MiProtectFreeNonPagedPool  
MiUnprotectFreeNonPagedPool  
MiProtectedPoolInsertList  
MiProtectedPoolRemoveEntryList  
MmDeterminePoolType  
MiSessionPoolVector  
MiSessionPoolAllocated  
MiSessionPoolFreed  
MmResourcesAvailable  
MiFreeNonPagedPool

MiAllocatePoolPages  
MiFreePoolPages  
MiInitializeNonPagedPool  
MmSnapshotPool  
MmQuerySpecialPoolBlockSize  
MiInitializeSpecialPool  
MmSetSpecialPool  
MiSpecialPoolTimerDispatch  
MiInitializeSpecialPoolCriteria  
MmSqueezeBadTags  
MiEnableRandomSpecialPool  
MmAllocateSpecialPool  
MiAllocateSpecialPool  
MmFreeSpecialPool  
MiMakeSpecialPoolPagable  
MiCheckSessionPoolAllocations  
MiInitializeSessionPool  
MiFreeSessionPoolBitmaps  
MiInsertContiguousTag  
MiFindContiguousMemory  
MmIsHydraAddress  
MmIsSpecialPoolAddressFree  
MmProtectSpecialPool  
MiProtectSpecialPool

allocvm.c :

NtAllocateVirtualMemory  
MiResetVirtualMemory  
MiCreatePageTablesForPhysicalRange  
MiDeletePageTablesForPhysicalRange  
MiIsEntireRangeDecommitted

checkpfn.c :

MiCheckPfn  
MiDumpPfn  
MiFormatPfn

checkpte.c :

MiCheckPte

CheckValidPte  
CheckInvalidPte

creasect.c :

NtCreateSection  
MmCreateSection  
MiCreateImageFileMap  
INIT\_IMAGE\_INFORMATION  
MiCheckDosCalls  
MiVerifyImageHeader  
VALIDATE\_NTHEADER  
MiCreateDataFileMap  
MiCreatePagingFileMap  
NtOpenSection  
MiGetImageProtection  
MiGetPageForHeader  
MiUpdateImageHeaderPage  
MiRemoveImageHeaderPage  
MiFindImageSectionObject  
MiInsertImageSectionObject  
MiRemoveImageSectionObject  
MiGetWritablePagesInSection  
MiFlushDataSection

deleteva.c :

MiDeleteVirtualAddresses  
MiDeletePte  
MiReleasePageFileSpace  
MiUpdateModifiedWriterMdl  
MiFlushPteList

dmpaddr.c :

MiDumpValidAddresses  
MiFormatPte  
MiDumpWsl  
MiFlushUnusedSections  
MiFlushUnusedSectionInternal  
MmMemoryUsage  
MiBuildKernelMap

MiFlushCache  
MiDumpReferencedPages  
dynmem.c :  
MmAddPhysicalMemory  
MmRemovePhysicalMemory  
MmGetPhysicalMemoryRanges  
MiRemovePhysicalPages  
extsect.c :  
MiSubsectionConsistent  
NtExtendSection  
MmExtendSection  
MiGetProtoPteAddressExtended  
MiLocateSubsection  
flushbuf.c :  
NtFlushWriteBuffer  
MiFlushRangeFilter  
NtFlushInstructionCache  
flushsec.c :  
NtFlushVirtualMemory  
MiFlushAcquire  
MiFlushRelease  
MmFlushVirtualMemory  
MmFlushSection  
MiStartingOffset  
MiEndingOffset  
MiFlushSectionInternal  
MmPurgeSection  
MmFlushImageSection  
MiFlushDirtyBitsToPfn  
MiGetSystemCacheSubsection  
MiCheckProtoPtePageState  
forksup.c :  
MiCloneProcessAddressSpace  
MiDecrementCloneBlockReference  
MiWaitForForkToComplete  
CloneTreeWalk

MiUpPfnReferenceCount  
MiDownPfnReferenceCount  
MiUpControlAreaRefs  
MiDoneWithThisPageGetAnother  
MiUpCloneProcessRefCount  
MiUpCloneProtoRefCount  
MiHandleForkTransitionPte  
MiDownShareCountFlushEntireTb  
MiUpForkPageShareCount  
MiBuildForkPageTable  
MiRetrievePageDirectoryFrames

freevm.c :

NtFreeVirtualMemory  
MiIsEntireRangeCommitted  
MiDecommitPages  
MiProcessValidPteList  
MiDeleteFreeVm

iosup.c :

MmProbeAndLockPages  
MmProbeAndLockProcessPages  
MiAddMdITracker  
MiFreeMdITracker  
MmProbeAndLockSelectedPages  
MmUnlockPages  
MmBuildMdIForNonPagedPool  
MiInitializeIoTrackers  
MiInsertPteTracker  
MiRemovePteTracker  
MiInsertDeadPteTrackingBlock  
MiReleaseDeadPteTrackers  
MiGetHighestPteConsumer  
MmMapLockedPages  
MmMapLockedPagesSpecifyCache  
MiMapSinglePage  
MiUnmapSinglePage  
MiPhysicalViewInserter



MiPhysicalViewRemover  
MiPhysicalViewAdjuster  
MiMapLockedPagesInUserSpace  
MmUnmapLockedPages  
MiUnmapLockedPagesInUserSpace  
MmMapIoSpace  
MmUnmapIoSpace  
MmAllocateContiguousMemorySpecifyCache  
MmAllocateContiguousMemory  
MmAllocateIndependentPages  
MmSetPageProtection  
MiAllocateContiguousMemory  
MmAllocatePagesForMdl  
MmFreePagesFromMdl  
MmMapUserAddressesToPage  
MmFreeContiguousMemory  
MmFreeContiguousMemorySpecifyCache  
MmGetPhysicalAddress  
MmGetVirtualForPhysical  
MmAllocateNonCachedMemory  
MmFreeNonCachedMemory  
MmSizeOfMdl  
MmCreateMdl  
MmSetAddressRangeModified  
MiCheckForContiguousMemory  
MmLockPagableSectionByHandle  
MiLockCode  
MmGetSectionRange  
MmLockPagableDataSection  
MiLookupDataTableEntry  
MmUnlockPagableImageSection  
MmIsRecursiveIoFault  
MmMapMemoryDumpMdl  
MmReleaseDumpAddresses  
MmSetBankedSection  
MmMapVideoDisplay

MmUnmapVideoDisplay  
MmLockPagedPool  
MmUnlockPagedPool  
MmGatherMemoryForHibernate  
MmReturnMemoryForHibernate  
MmSetKernelDumpRange  
MmEnablePAT  
MmDispatchWin32Callout  
MmIsSystemAddressLocked  
MiVerifyLockedPageCharges

lockvm.c :

NtLockVirtualMemory  
NtUnlockVirtualMemory  
MiInsertConflictInList  
MiRemoveConflictFromList

mapcache.c :

MmMapViewInSystemCache  
MiAddMappedPtes  
MmUnmapViewInSystemCache  
MiRemoveMappedPtes  
MiInitializeSystemCache  
MmCheckCachedPageState  
MmCopyToCachedPage  
MiMapCacheExceptionHandler  
MmUnlockCachedPage

mapview.c :

MiDumpConflictingVad  
NtMapViewOfSection  
MmMapViewOfSection  
MiMapViewOfPhysicalSection  
MiMapViewOfImageSection  
MiMapViewOfDataSection  
MiCheckPurgeAndUpMapCount  
CacheImageSymbols  
NtAreMappedFilesTheSame  
MiSetPageModified

MmMapViewInSystemSpace  
MmMapViewInSessionSpace  
MiMapViewInSystemSpace  
MiFillSystemPageDirectory  
MmUnMapViewInSystemSpace  
MmUnMapViewInSessionSpace  
MiUnMapViewInSystemSpace  
MiInsertInSystemSpace  
MiRemoveFromSystemSpace  
MiInitializeSystemSpaceMap  
MiFreeSessionSpaceMap  
MmSecureVirtualMemory  
MmUnsecureVirtualMemory

mi.h :

MmIsRetryIoStatus  
MI\_CONVERT\_FROM\_PTE\_PROTECTION  
MI\_MASK\_TO\_PTE  
MI\_IS\_PTE\_PROTECTION\_COPY\_WRITE  
MI\_ROUND\_TO\_64K  
MI\_ROUND\_TO\_SIZE  
MI\_64K\_ALIGN  
MI\_ALIGN\_TO\_SIZE  
MI\_STARTING\_OFFSET  
MiFindEmptyAddressRangeDown  
MiGetPreviousVad  
MiGetNextVad  
MiGetFirstVad  
MiCheckForConflictingVad  
MiGetNextClone  
MiGetPreviousClone  
MiGetFirstClone  
MiInsertClone  
MiRemoveClone  
MiLocateCloneAddress  
MiCheckForConflictingClone  
MI\_VA\_TO\_PAGE

MI\_VA\_TO\_VPN  
MI\_VPN\_TO\_VA  
MI\_VPN\_TO\_VA\_ENDING  
MiGetByteOffset  
MI\_PFN\_ELEMENT  
MI\_MAKE\_PROTECT\_NOT\_WRITE\_COPY  
MiLockPfnDatabase  
MiUnlockPfnDatabase  
MiTryToLockPfnDatabase  
MiReleasePfnLock  
MiLockSystemSpace  
MiUnlockSystemSpace  
MiLockSystemSpaceAtDpcLevel  
MiUnlockSystemSpaceFromDpcLevel  
CONSISTENCY\_LOCK\_PFN  
CONSISTENCY\_UNLOCK\_PFN  
CONSISTENCY\_LOCK\_PFN2  
CONSISTENCY\_UNLOCK\_PFN2  
PFN\_LOCK\_OWNED\_BY\_ME  
LOCK\_PFN  
LOCK\_PFN\_WITH\_TRY  
UNLOCK\_PFN  
LOCK\_PFN2  
UNLOCK\_PFN2  
UNLOCK\_PFN\_AND\_THEN\_WAIT  
LOCK\_AWE  
UNLOCK\_AWE  
SYSLOAD\_LOCK\_OWNED\_BY\_ME  
MM\_PFN\_LOCK\_ASSERT  
MM\_SET\_EXPANSION\_OWNER  
MM\_CLEAR\_EXPANSION\_OWNER  
LOCK\_EXPANSION  
UNLOCK\_EXPANSION  
UNLOCK\_EXPANSION\_AND\_THEN\_WAIT  
LOCK\_EXPANSION\_IF\_ALPHA  
UNLOCK\_EXPANSION\_IF\_ALPHA

LOCK\_SYSTEM\_WS  
UNLOCK\_SYSTEM\_WS  
UNLOCK\_SYSTEM\_WS\_NO\_IRQ  
MM\_SYSTEM\_WS\_LOCK\_ASSERT  
LOCK\_HYPERSPACE  
UNLOCK\_HYPERSPACE  
MI\_WS\_OWNER  
MI\_NOT\_WS\_OWNER  
MI\_IS\_WS\_UNSAFE  
LOCK\_WS  
LOCK\_WS\_UNSAFE  
MI\_MUST\_BE\_UNSAFE  
MI\_MUST\_BE\_SAFE  
MI\_MUST\_BE\_UNSAFE  
MI\_MUST\_BE\_SAFE  
UNLOCK\_WS  
UNLOCK\_WS\_UNSAFE  
LOCK\_ADDRESS\_SPACE  
LOCK\_WS\_AND\_ADDRESS\_SPACE  
UNLOCK\_WS\_AND\_ADDRESS\_SPACE  
UNLOCK\_ADDRESS\_SPACE  
UNLOCK\_WS\_REGARDLESS  
LOCK\_WS\_REGARDLESS  
ZERO\_LARGE  
MI\_CHECK\_BIT  
MI\_SET\_BIT  
MI\_CLEAR\_BIT  
MI\_PFN\_IS\_AWE  
MI\_CAPTURE\_USED\_PAGETABLE\_ENTRIES  
MI\_RETRIEVE\_USED\_PAGETABLE\_ENTRIES\_FROM\_PTE  
MI\_ZERO\_USED\_PAGETABLE\_ENTRIES\_IN\_INPAGE\_SUPPORT  
MI\_ZERO\_USED\_PAGETABLE\_ENTRIES\_IN\_PFN  
MI\_INSERT\_USED\_PAGETABLE\_ENTRIES\_IN\_PFN  
MI\_ZERO\_USED\_PAGETABLE\_ENTRIES  
MI\_GET\_USED\_PTES\_HANDLE  
MI\_GET\_USED\_PTES\_FROM\_HANDLE

MI\_INCREMENT\_USED\_PTES\_BY\_HANDLE  
MI\_DECREMENT\_USED\_PTES\_BY\_HANDLE  
MI\_MARK\_PFN\_AS\_LOCK\_CHARGED  
MI\_UNMARK\_PFN\_AS\_LOCK\_CHARGED  
MI\_ADD\_LOCKED\_PAGE\_CHARGE  
MI\_ADD\_LOCKED\_PAGE\_CHARGE\_FOR\_MODIFIED\_PAGE  
MI\_ADD\_LOCKED\_PAGE\_CHARGE\_FOR\_TRANSITION\_PAGE  
MI\_REMOVE\_LOCKED\_PAGE\_CHARGE  
MI\_ZERO\_WSINDEX  
MI\_WSLE\_HASH  
MI\_GET\_PROTECTION\_FROM\_WSLE  
MI\_CALC\_NEXT\_ESTIMATION\_SLOT\_CONST  
MI\_NEXT\_VALID\_ESTIMATION\_SLOT  
MI\_NEXT\_VALID\_AGING\_SLOT  
MI\_CALCULATE\_USAGE\_ESTIMATE  
MI\_RESET\_WSLE\_AGE  
MI\_GET\_WSLE\_AGE  
MI\_INC\_WSLE\_AGE  
MI\_UPDATE\_USE\_ESTIMATE  
MI\_WS\_GROWING\_TOO\_FAST  
SECTION\_BASE\_ADDRESS  
Mi4KStartForSubsection  
Mi4KStartFromSubsection  
MiCreateBitMap  
MiRemoveBitMap  
MI\_INITIALIZE\_ZERO\_MDL  
LOCK\_SYSTEM\_VIEW\_SPACE  
UNLOCK\_SYSTEM\_VIEW\_SPACE  
MiDecrementShareCountOnly  
MiDecrementShareAndValidCount  
MiRemoveZeroPageIfAny  
MiUnmapPageInHyperSpace  
MiGetProtoPteAddress  
MM\_TRACK\_COMMIT  
MM\_BUMP\_COUNTER  
MI\_NONPAGABLE\_MEMORY\_AVAILABLE

MI\_UNUSED\_SEGMENTS\_COUNT\_UPDATE  
MI\_UNUSED\_SEGMENTS\_SURPLUS  
MI\_UNUSED\_SEGMENTS\_INSERT\_CHARGE  
MI\_UNUSED\_SEGMENTS\_REMOVE\_CHARGE  
MI\_IS\_SESSION\_IMAGE\_ADDRESS  
MI\_IS\_SESSION\_POOL\_ADDRESS  
MI\_IS\_SESSION\_ADDRESS  
MI\_IS\_SESSION\_PTE  
SESSION\_GLOBAL  
MM\_BUMP\_SESS\_COUNTER  
MM\_SNAP\_SESS\_MEMORY\_COUNTERS  
MI\_FLUSH\_SESSION\_TB  
MM\_SET\_SESSION\_LOCK\_OWNER  
MM\_CLEAR\_SESSION\_LOCK\_OWNER  
LOCK\_SESSION  
UNLOCK\_SESSION  
MM\_SET\_SESSION\_RESOURCE\_OWNER  
MM\_CLEAR\_SESSION\_RESOURCE\_OWNER  
MM\_SESSION\_SPACE\_WS\_LOCK\_ASSERT  
LOCK\_SESSION\_SPACE\_WS  
UNLOCK\_SESSION\_SPACE\_WS  
MiGetPdeSessionIndex  
MI\_GET\_DIRECTORY\_FRAME\_FROM\_PROCESS

miglobal.c :

Memory Manager

가

mmfault.c :

MmAccessFault

mminit.c :

MmInitSystem

MiMapBBTMemory

MmInitializeMemoryLimits

MiCheckPaeLicense

MiMergeMemoryLimit

MmFreeLoaderBlock

MiBuildPagedPool

MiFindInitializationCode

MiFreeInitializationCode  
MiEnablePagingTheExecutive  
MiEnablePagingOfDriverAtInit  
MmQuerySystemSize  
MmIsThisAnNtAsSystem  
MmSetPageFaultNotifyRoutine  
MmSetHardFaultNotifyRoutine

mmquota.c :

MiChargePageFileQuota  
MiReturnPageFileQuota  
MiChargeCommitment  
MiChargeCommitmentCantExpand  
MiReturnCommitment  
MiCalculatePageCommitment  
MiReturnPageTablePageCommitment  
MiCauseOverCommitPopup  
MmRaisePoolQuota  
MmReturnPoolQuota

mmsup.c :

MiIsPteDecommittedPage  
MiIsProtectionCompatible  
MiMakeProtectionMask  
MiDoesPpeExistAndMakeValid  
MiDoesPdeExistAndMakeValid  
MiMakePpeExistAndMakeValid  
MiMakePdeExistAndMakeValid  
MiMakeSystemAddressValid  
MiMakeSystemAddressValidPfnWs  
MiMakeSystemAddressValidPfnSystemWs  
MiMakeSystemAddressValidPfn  
MiLockPagedAddress  
MiUnlockPagedAddress  
MiZeroPhysicalPage  
MiRestoreTransitionPte  
MiGetSubsectionAndProtoFromPte  
MmIsNonPagedSystemAddressValid



MmHibernateInformation

MiCheckPageTableTrim

MiCheckPageTableInPage

modwrite.c :

MiCheckPageFilePath

MiReleaseModifiedWriter

NtCreatePagingFile

MiExtendPagingFileMaximum

MiCheckForCrashDump

MiCrashDumpWorker

MmGetCrashDumpInformation

MmGetCrashDumpStateInformation

MiAttemptPageFileExtension

MiExtendPagingFiles

MiContractPagingFiles

MiAttemptPageFileReduction

MiWriteComplete

MiCancelWriteOfMappedPfn

MiModifiedPageWriter

MiModifiedPageWriterTimerDispatch

MiModifiedPageWriterWorker

MiGatherMappedPages

MiGatherPagefilePages

MiClusterWritePages

MiMappedPageWriter

MmDisableModifiedWriteOfSection

MmGetPageFileInformation

MiCheckPageFileMapping

MiInsertPageFileInList

MiPageFileFull

MiFlushAllPages

MiIssuePageExtendRequest

MiIssuePageExtendRequestNoWait

pagfault.c :

MiDispatchFault

MiResolveDemandZeroFault

MiResolveTransitionFault  
MiResolvePageFileFault  
MiResolveProtoPteFault  
MiCompleteProtoPteFault  
MiResolveMappedFileFault  
MiWaitForInPageComplete  
MiFindActualFaultingPte  
MiCheckVirtualAddress  
MiCheckPdeForPagedPool  
MiCheckPdeForSessionSpace  
MiInitializePfn  
MiInitializeReadInProgressPfn  
MiInitializeTransitionPfn  
MiInitializeCopyOnWritePfn  
MmIsAddressValid  
MiInitializePfnForOtherProcess  
MiAddValidPageToWorkingSet  
MiGetInPageSupportBlock  
MiFreeInPageSupportBlock  
MiFlushInPageSupportBlock  
MiHandleBankedSection  
MiSessionCopyOnWrite  
MiCheckFileState

pfndec.c :

MiDecrementShareCount  
MiDecrementReferenceCount

pfnlist.c :

MI\_TALLY\_TRANSITION\_PAGE\_ADDITION  
MI\_TALLY\_TRANSITION\_PAGE\_REMOVAL  
MiInsertPageInList  
MiInsertStandbyListAtFront  
MiRemovePageFromList  
MiUnlinkPageFromList  
MiUnlinkFreeOrZeroedPage  
MiEnsureAvailablePageOrWait  
MiRemoveZeroPage

MiRemoveAnyPage  
MiRemovePageByColor  
MiInsertFrontModifiedNoWrite

physical.c :

NtMapUserPhysicalPages  
NtMapUserPhysicalPagesScatter  
NtAllocateUserPhysicalPages  
NtFreeUserPhysicalPages  
MiRemoveUserPhysicalPagesVad  
MiUpdateVadPhysicalPages  
MiCleanPhysicalProcessPages  
MiFlushUserPhysicalPteList

procsup.c :

MmCreateProcessAddressSpace  
MmInitializeProcessAddressSpace  
MmDeleteProcessAddressSpace  
MmCleanProcessAddressSpace  
MmCreateKernelStack  
MmDeleteKernelStack  
MmGrowKernelStack  
MmGrowKernelBackingStore  
MmOutPageKernelStack  
MmInPageKernelStack  
MmOutSwapProcess  
MmInSwapProcess  
MiCreatePebOrTeb  
MmCreateTeb  
MI\_INIT\_PEB\_FROM\_IMAGE  
MiInitializeWowPeb  
MmCreatePeb  
MmDeleteTeb  
MmAllowWorkingSetExpansion  
MiDeleteAddressesInWorkingSet  
MiDeleteValidAddress  
MiMakeOutswappedPageResident  
MmSetMemoryPriorityProcess

MiAllocateVad  
MiVerifyReferenceCounts  
MiPaeInitialize  
MiPaeAllocate  
MiPaeFree  
MiPaeReplenishList  
MiPaeFreeEntirePage

protect.c :

NtProtectVirtualMemory  
MiProtectVirtualMemory  
MiSetProtectionOnSection  
MiGetPageProtection  
MiChangeNoAccessForkPte  
MiFlushTbAndCapture  
MiSetProtectionOnTransitionPte  
MiCaptureSystemPte  
MiCheckSecuredVad  
MiMapInPfnDatabase  
MiUnMapPfnDatabase  
MiSetOriginalPteProtection  
MiSetModified

querysec.c :

NtQuerySection

queryvm.c :

NtQueryVirtualMemory  
MiQueryAddressState  
MiGetWorkingSetInfo

readwrt.c :

NtReadVirtualMemory  
NtWriteVirtualMemory  
MmCopyVirtualMemory  
MiGetExceptionInfo  
MiDoMappedCopy  
MiDoPoolCopy  
MiValidateUserTransfer

sectsup.c :

MiInsertBasedSection  
MiRemoveBasedSection  
MiFindEmptySectionBaseDown  
MiSegmentDelete  
MiSectionDelete  
MiDereferenceSegmentThread  
MiSectionInitialization  
MmForceSectionClosed  
MiCleanSection  
MmGetFileNameForSection  
MiCheckControlArea  
MiCheckForControlAreaDeletion  
MiCheckControlAreaStatus  
MiGetEventCounter  
MiFreeEventCounter  
MiFlushEventCounter  
MmCanFileBeTruncated  
MiCanFileBeTruncatedInternal  
MiRemoveUnusedSegments

session.c :

MmSessionLeader  
MmSessionSetUnloadAddress  
MiSessionAddProcess  
MiSessionRemoveProcess  
MiInitializeSessionIds  
MiSessionCreateInternal  
MmSessionCreate  
MmSessionDelete  
MiAttachSession  
MiDetachSession  
MiCheckSessionVirtualSpace  
MiSessionDeletePde  
MiDereferenceSession  
MiSessionCommitImagePages  
MiSessionCommitPageTables  
MiSessionOutSwapProcess

MiSessionInSwapProcess

sessload.c :

MiShareSessionImage

MiSessionInsertImage

MiSessionRemoveImage

MiSessionLookupImage

MiSessionUnloadAllImages

MiSessionWideInitializeAddresses

MiSessionWideInsertImageAddress

MiSessionWideReferenceImage

MiSessionWideGetImageSize

MiSessionWideReserveImageAddress

MiRemoveImageSessionWide

MiLookupPsLoadedModule

shutdown.c :

MmShutdownSystem

super.c :

NtCreateSuperSection

NtOpenSuperSection

NtMapViewOfSuperSection

NtQuerySuperSection

MiSuperSectionDelete

MiSuperSectionInitialization

sysload.c :

MmLoadSystemImage

MmLoadAndLockSystemImage

MiLoadSystemImage

MiLoadImageSection

MmFreeDriverInitialization

MiEnablePagingOfDriver

MiSetPagingOfDriver

MmPageEntireDriver

MmResetDriverPaging

MiClearImports

MiRememberUnloadedDriver

MmLocateUnloadedDriver

MmUnLoadSystemImage  
MiBuildImportsForBootDrivers  
MiCallDllUnloadAndUnloadDll  
MiLocateExportName  
MiDereferenceImports  
MiResolveImageReferences  
MiSnapThunk  
MiLookupImageSectionByName  
MmCheckSystemImage  
MmVerifyImageIsOkForMpUse  
MiDeleteSystemPagableVm  
MiSetImageProtect  
MiSetSystemCodeProtection  
MiWriteProtectSystemImage  
MiUpdateThunks  
MiReloadBootLoadedDrivers  
MiLocateKernelSections  
MmMakeKernelResourceSectionWritable  
MiInitializeLoadedModuleList  
MmCallDllInitialize  
MmGetSystemRoutineAddress  
MiFindExportedRoutineByName

sysptes.c :

MiValidateSystemPtes  
MiCheckPteAllocation  
MiCheckPteRelease  
MiRebuildPteTracker  
MiReserveSystemPtes  
MiFeedSysPtePool  
MiReserveSystemPtes2  
MiReleaseSystemPtes  
MiInitializeSystemPtes  
MiAddSystemPtes  
MiGetSystemPteListCount  
MiGetSystemPteAvailability  
MiDumpSystemPtes

MiCountFreeSystemPtes

unmapview.c :

NtUnmapViewOfSection

MmUnmapViewOfSection

MiRemoveMappedView

MiPurgeImageSection

vadtrees.c :

MiInsertVad

MiRemoveVad

MiLocateAddress

MiFindEmptyAddressRange

VadTreeWalk

verifier.c :

VerifierProbeAndLockPages

VerifierProbeAndLockProcessPages

VerifierProbeAndLockSelectedPages

ViAddBadMapper

VerifierMapIoSpace

VerifierMapLockedPages

VerifierMapLockedPagesSpecifyCache

VerifierUnlockPages

VerifierUnmapLockedPages

VerifierUnmapIoSpace

VerifierAllocatePool

VerifierAllocatePoolWithTag

VerifierAllocatePoolWithTagQuota

VerifierAllocatePoolWithTagQuotaTag

VerifierAllocatePoolWithTagPriority

ViInjectResourceFailure

ViReservePoolAllocation

ViInsertPoolAllocation

ViReleasePoolAllocation

ViCancelPoolAllocation

ViPostPoolAllocation

VeAllocatePoolWithTagPriority

VerifierFreeTrackedPool



VerifierFreePool  
VerifierFreePoolWithTag  
VerifierSetEvent  
VerifierExAcquireResourceExclusive  
VerifierExReleaseResource  
KfSanityCheckRaiseIrql  
KfSanityCheckLowerIrql  
ViTrimAllSystemPagableMemory  
VerifierKeAcquireSpinLock  
VerifierKeReleaseSpinLock  
VerifierKfAcquireSpinLock  
VerifierKfReleaseSpinLock  
VerifierKeAcquireQueuedSpinLock  
VerifierKeReleaseQueuedSpinLock  
VerifierKfRaiseIrql  
VerifierKfLowerIrql  
VerifierKeAcquireSpinLockAtDpcLevel  
VerifierKeReleaseSpinLockFromDpcLevel  
VerifierKeAcquireSpinLockRaiseToDpc  
VerifierExTryToAcquireFastMutex  
VerifierExAcquireFastMutex  
VerifierExAcquireFastMutexUnsafe  
VerifierExReleaseFastMutex  
VerifierExReleaseFastMutexUnsafe  
VerifierKeRaiseIrql  
VerifierKeLowerIrql  
VerifierSynchronizeExecution  
VerifierKeInitializeTimerEx  
VerifierKeInitializeTimer  
ViInitializeEntry  
MiInitializeDriverVerifierList  
ViInsertVerifierEntry  
ViLocateVerifierEntry  
MiApplyDriverVerifier  
MiVerifyingDriverUnloading  
MmIsDriverVerifying

MmAddVerifierThunks  
MiVerifierCheckThunks  
MmGetVerifierInformation  
MmSetVerifierInformation  
ViPrintString  
MiEnableVerifier  
MiEnableKernelVerifier

vlm.c :

NtAllocateVirtualMemory64  
NtFreeVirtualMemory64  
MiFindEmptyAddressRangeInTree64  
MiCommitPages64  
MiMakePdeExistAndMakeValid64  
MiDoesPdeExist64  
MiDecommitOrDeletePages64  
MiProcessValidPteList64  
MiReturnAvailablePages  
MiCheckPdeForDeletion  
MiDeleteVlmAddressSpace  
MiFlushPteList64  
MmIsAddressValid64  
NtMapViewOfVlmSection  
MiMapViewOfVlmDataSection  
NtUnmapViewOfVlmSection  
NtProtectVirtualMemory64  
MiIsEntireRangeCommitted64  
MiMakeValidPageNoAccess64  
MiMakeNoAccessPageValid64  
MiGetVlmInfo  
NtQueryVirtualMemory64  
MiQueryAddressState64  
NtAllocateVirtualMemory64  
NtFreeVirtualMemory64  
NtMapViewOfVlmSection  
NtUnmapViewOfVlmSection  
NtQueryVirtualMemory64

NtProtectVirtualMemory64

wrtfault.c :

MiCopyOnWrite

wslist.c :

MiLocateAndReserveWsle

MiDoReplacement

MmEnforceWorkingSetLimit

MiReplaceWorkingSetEntryUsingClaim

MiReplaceWorkingSetEntryUsingFaultInfo

MiRemovePageFromWorkingSet

MiReleaseWsle

MiUpdateWsle

MiFreeWsle

MiInitializeWorkingSetList

MiInitializeSessionWsSupport

MiSessionInitializeWorkingSetList

MmAssignProcessToJob

MmAdjustWorkingSetSize

MiAddWorkingSetPage

MiAddWsleHash

MiGrowWsleHash

MiTrimWorkingSet

MmPurgeWorkingSet

MiEliminateWorkingSetEntry

MiRemoveWorkingSetPages

MiEmptyWorkingSet

MiDumpWsleInCacheBlock

MiDumpPteInCacheBlock

MiCheckNullIndex

wsmanage.c :

MiAdjustWorkingSetManagerParameters

MiObtainFreePages

MmWorkingSetManager

MiCheckAndSetSystemTrimCriteria

MiCheckSystemTrimEndCriteria

MiCheckProcessTrimCriteria

MiCheckSystemCacheWsTrimCriteria  
MiDetermineWsTrimAmount  
MiAgePagesAndEstimateClaims  
MiAgeAndEstimateAvailableInWorkingSet  
MiAdjustClaimParameters  
MiRearrangeWorkingSetExpansionList  
MiEmptyAllWorkingSets  
MiEmptyAllWorkingSetsWorker  
MmTrimAllSystemPagableMemory

wstree.c :

MiInsertWsle  
MiCheckWsleHash  
MiLocateWsle  
MiLocateWsleAndParent  
MiRemoveWsle  
MiSwapWsleEntries  
MiLookupWsleHashIndex  
MiRemoveWsleFromFreeList  
MiSwapWsleEntries

zeropage.c :

MmZeroPageThread

```
#####  
#                               private/ntos/mountmgr                               #  
#####
```

Comment :

Mount Manager.

```
#####  
#                               private/ntos/nls                               #  
#####
```

Comment :

```
#####
```

# private/ntos/ob #

#####

Abstract :

Object Manager

Prefix :

Ob

Nt

Files :

obclose.c

obcreate.c

obdevmap.c

obdir.c

obhandle.c

obinit.c

obinsert.c

oblink.c

obp.h

obquery.c

obref.c

obsdata.c

obse.c

obtype.c

obwait.c

tob.c

uob.c

obclose.c :

NtClose

NtMakeTemporaryObject

ObMakeTemporaryObject

obcreate.c :

ObCreateObject

ObpCaptureObjectCreateInformation

ObpCaptureObjectName

ObpAllocateObjectNameBuffer

ObpFreeObjectNameBuffer

ObDeleteCapturedInsertInfo

ObpAllocateObject  
ObpFreeObject  
ObFreeObjectCreateInfoBuffer

obdevmap.c :

ObSetDeviceMap  
ObQueryDeviceMapInformation  
ObInheritDeviceMap  
ObDereferenceDeviceMap

obdir.c :

NtCreateDirectoryObject  
NtOpenDirectoryObject  
NtQueryDirectoryObject  
ObpLookupDirectoryEntry  
ObpInsertDirectoryEntry  
ObpDeleteDirectoryEntry  
ObpLookupObjectName

obhandle.c :

ObpIncrPointerCount  
ObpDecrPointerCount  
ObpDecrPointerCountWithResult  
ObpIncrHandleCount  
ObpDecrHandleCount  
NtDuplicateObject  
ObGetHandleInformation  
ObpCaptureHandleInformation  
ObpInsertHandleCount  
ObpIncrementHandleDataBase  
ObpIncrementHandleCount  
ObpIncrementUnnamedHandleCount  
ObpChargeQuotaForObject  
ObpDecrementHandleCount  
ObpCreateHandle  
ObpCreateUnnamedHandle  
ObpValidateDesiredAccess  
ObpComputeGrantedAccessIndex  
ObpTranslateGrantedAccessIndex

obinit.c :

- ObInitSystem
- ObDupHandleProcedure
- ObAuditInheritedHandleProcedure
- ObInitProcess
- ObInitProcess2
- ObDestroyHandleProcedure
- ObKillProcess
- ObpEnumFindHandleProcedure
- ObFindHandleForObject
- ObpCreateDosDevicesDirectory
- ObpGetDosDevicesProtection
- ObpFreeDosDevicesProtection

obinsert.c :

- ObInsertObject

oblink.c :

- NtCreateSymbolicLinkObject
- NtOpenSymbolicLinkObject
- NtQuerySymbolicLinkObject
- ObpParseSymbolicLink
- ObpDeleteSymbolicLink
- ObpDeleteSymbolicLinkName
- ObpCreateSymbolicLinkName
- ObpProcessDosDeviceSymbolicLink

obp.h :

- ExAllocatePool
- ExAllocatePoolWithQuota
- ObpBeginTypeSpecificCallOut
- ObpEndTypeSpecificCallOut
- ObpValidateIrql
- ObpIncrPointerCount
- ObpDecrPointerCount
- ObpDecrPointerCountWithResult
- ObpIncrHandleCount
- ObpDecrHandleCount
- ObpEnterObjectTypeMutex

ObpLeaveObjectTypeMutex  
ObpEnterRootDirectoryMutex  
ObpLeaveRootDirectoryMutex  
ObpGetObjectTable  
ObpCentralizedSecurity  
SD\_TO\_SD\_HEADER  
LINK\_TO\_SD\_HEADER  
NEXT\_SDHEADER  
PREV\_SDHEADER  
IsKernelHandle  
EncodeKernelHandle  
DecodeKernelHandle  
ObpIsOverflow  
ObpFreeObjectCreateInformation  
ObpReleaseObjectCreateInformation  
ObpAllocateObjectCreateInfoBuffer  
ObpFreeObjectCreateInfoBuffer

obquery.c :

NtQueryObject  
NtSetInformationObject  
ObQueryNameString  
ObQueryTypeName  
ObQueryTypeInfo  
ObQueryObjectAuditingByHandle  
ObGetObjectName  
ObpSetHandleAttributes

obref.c :

ObGetObjectPointerCount  
ObOpenObjectByName  
ObOpenObjectByPointer  
ObReferenceObjectByHandle  
ObReferenceObjectByName  
ObReferenceObjectByPointer  
ObfReferenceObject  
ObfDereferenceObject  
ObpProcessRemoveObjectQueue



ObpRemoveObjectRoutine

ObpDeleteNameCheck

ObDereferenceObject

obsdata.c :

IF\_OB\_GLOBAL

ObPrint

ObpInitSecurityDescriptorCache

ObpHashSecurityDescriptor

ObpHashBuffer

ObpLogSecurityDescriptor

ObpCreateCacheEntry

ObpReferenceSecurityDescriptor

ObDeassignSecurity

ObpDereferenceSecurityDescriptor

ObpDestroySecurityDescriptorHeader

ObpCompareSecurityDescriptors

ObpAcquireDescriptorCacheWriteLock

ObpAcquireDescriptorCacheReadLock

ObpReleaseDescriptorCacheLock

obse.c :

NtSetSecurityObject

ObSetSecurityObjectByPointer

NtQuerySecurityObject

ObCheckObjectAccess

ObpCheckObjectReference

ObpCheckTraverseAccess

ObCheckCreateObjectAccess

ObAssignObjectSecurityDescriptor

ObGetObjectSecurity

ObReleaseObjectSecurity

ObValidateSecurityQuota

ObAssignSecurity

ObQuerySecurityDescriptorInfo

ObSetSecurityDescriptorInfo

ObpValidateAccessMask

obtype.c :

ObCreateObjectType  
ObEnumerateObjectsByType  
ObpCreateTypeArray  
ObpDestroyTypeArray  
ObGetObjectInformation

obwait.c :

NtSignalAndWaitForSingleObject  
NtWaitForSingleObject  
NtWaitForMultipleObjects  
ObWaitForSingleObject

tob.c :

Object Manager

uob.c :

Object Manager

#####

# private/ntos/ps #

#####

Abstract :

Process Manager

Prefix :

Ps

Files :

i386/psctx386.c  
i386/psldt.c  
i386/psvdm.c  
create.c  
kulokup2.c  
kuloopup.c  
pscid.c  
psctx.c  
psdelete.c  
psimpers.c  
psinit.c  
psjob.c  
psopen.c

psp.h  
psquery.c  
psquota.c  
psspnd.c  
security.c

i386/psctx386.c :

PSPALIGN\_DOWN  
PSPALIGN\_UP  
PspGetContext  
PspSetContext  
PspGetSetContextSpecialApc

i386/psldt.c :

PspLdtInitialize  
PspQueryLdtInformation  
PspSetLdtSize  
PspSetLdtInformation  
PspCreateLdt  
PspIsDescriptorValid  
PspQueryDescriptorThread  
PspDeleteLdt  
NtSetLdtEntries

i386/psvdm.c :

ASERTEQUAL  
ASERTEQUALBREAK  
PspSetProcessIoHandlers  
PspDeleteVdmObjects  
Psp386RemoveIoHandler  
Psp386InstallIoHandler  
Psp386CreateVdmIoListHead  
Psp386InsertVdmIoHandlerBlock  
Ps386GetVdmIoHandler  
Psp386GetVdmIoHandler  
PspVdmInitialize

create.c :

NtCreateThread  
PsCreateSystemThread

PspMarkProcessIdValid  
PspCreateThread  
NtCreateProcess  
PsCreateSystemProcess  
PspCreateProcess  
PsSetCreateProcessNotifyRoutine  
PsSetCreateThreadNotifyRoutine  
PspUserThreadStartup  
PspUnhandledExceptionInSystemThread  
PspSystemThreadStartup  
PsLockProcess  
PsUnlockProcess  
PsGetCurrentProcessId  
PsGetCurrentThreadId  
PsGetVersion  
PsSetLoadImageNotifyRoutine  
PsCallImageNotifyRoutines

kulookup2.c :

PspLookupKernelUserEntryPoints

kulookup.c :

PspLookupKernelUserEntryPoints

pscid.c :

PsLookupProcessThreadByCid

PsLookupProcessByProcessId

PsLookupThreadByThreadId

psctx.c :

PspQueueApcSpecialApc

NtQueueApcThread

NtGetContextThread

NtSetContextThread

psdelete.c :

PsSetLegoNotifyRoutine

PspReaper

PspTerminateThreadByPointer

NtTerminateProcess

PspTerminateProcess

NtTerminateThread  
PsTerminateSystemThread  
PspNullSpecialApc  
PsExitSpecialApc  
PspExitNormalApc  
PspMarkCidInvalid  
PspExitThread  
PspExitProcess  
PspProcessDelete  
PspThreadDelete  
NtRegisterThreadTerminatePort  
PsGetProcessExitTime  
PspIsThreadTerminating

psimpers.c :

NtImpersonateThread

psinit.c : Process Manager가

PsInitSystem  
PspInitPhase0  
PspInitPhase1  
PsLocateSystemDll  
PspMapSystemDll  
PspInitializeSystemDll  
PspLookupSystemDllEntryPoint  
PsChangeQuantumTable

psjob.c :

NtCreateJobObject  
NtOpenJobObject  
NtAssignProcessToJobObject  
PspAddProcessToJob  
PspRemoveProcessFromJob  
PspExitProcessFromJob  
PspJobDelete  
PspJobClose  
NtQueryInformationJobObject  
NtSetInformationJobObject  
PspApplyJobLimitsToProcessSet

PspApplyJobLimitsToProcess  
NtTerminateJobObject  
PsEnforceExecutionTimeLimits  
PspTerminateAllProcessesInJob  
PspFoldProcessAccountingIntoJob  
PspCaptureTokenFilter  
PsChangeJobMemoryUsage  
PsReportProcessMemoryLimitViolation

psopen.c :

NtOpenProcess  
NtOpenThread

psp.h :

nothing special

psquery.c :

PspQueryWorkingSetWatch  
PspQueryQuotaLimits  
PspQueryPooledQuotaLimits  
PspSetPrimaryToken  
NtQueryInformationProcess  
PspSetQuotaLimits  
NtSetInformationProcess  
NtQueryInformationThread  
NtSetInformationThread  
PsWatchWorkingSet  
PsEstablishWin32Callouts  
PsSetProcessPriorityByClass  
PsConvertToGuiThread

psquota.c :

PsChargeSharedPoolQuota  
PsReturnSharedPoolQuota  
PsChargePoolQuota  
PsReturnPoolQuota  
PspInheritQuota  
PspDereferenceQuota

psspnd.c :

NtSuspendThread

NtResumeThread  
NtAlertThread  
NtAlertResumeThread  
NtTestAlert

security.c :

PsReferencePrimaryToken  
PsReferenceImpersonationToken  
PsReferenceEffectiveToken  
PsOpenTokenOfThread  
PsOpenTokenOfProcess  
PsOpenTokenOfJobObject  
PsImpersonateClient  
PsDisableImpersonation  
PsRestoreImpersonation  
PsRevertToSelf  
PspInitializeProcessSecurity  
PspDeleteProcessSecurity  
PspAssignPrimaryToken  
PspInitializeThreadSecurity  
PspDeleteThreadSecurity  
PsAssignImpersonationToken

```
#####  
#                               private/ntos/rtl                               #  
#####
```

Abstract :

Runtime Module

Prefix :

Rtl

Files :

i386/byteswap.asm  
i386/context.c  
i386/debug2.asm  
i386/debug3.c  
i386/divlarge.c  
i386/exdsptch.c

i386/exsup.asm  
i386/forceres.asm  
i386/halvprnt.c  
i386/ioaccess.asm  
i386/largeint.asm  
i386/movemem.asm  
i386/nlssup.asm  
i386/nlstrans.asm  
i386/ntcurteb.asm  
i386/ntrtl386.h  
i386/raise.asm  
i386/raisests.c  
i386/rtldump.c  
i386/slist.asm  
i386/stkwalk.asm  
i386/stringsp.asm  
i386/userdisp.asm  
i386/xcptmisc.asm  
acledit.c  
assert.c  
atom.c  
bitmap.c  
byteswap.c  
checksum.c  
cnvint.c  
debug.c  
dev2dos.c  
eballoc.c  
envrion.c  
error.c  
excpdbg.c  
gen8dot3.c  
generr.c  
gentable.c  
guid.c  
handle.c



heap.c  
heapdbg.c  
heapdll.c  
heappage.c  
heappage.h  
heappagi.h  
heappriv.h  
imagedir.c  
ldrreloc.c  
ldrsrc.c  
lookasid.c  
message.c  
mrcf.c  
nls.c  
nlsxlat.c  
ntrtlp.h  
pctohdr.c  
prefix.c  
prodtype.c  
random.c  
range.c  
range.h  
recip.c  
registry.c  
regutil.c  
remlock.c  
remlock.h  
rtlasing.c  
rtldata.c  
rtlexec.c  
rxact.c  
sertl.c  
splay.c  
stdtimep.h  
stktrace.c  
string.c

tacl.c  
tbitmap.c  
threads.c  
threads.h  
time.c  
tnlslat.c  
tprefix.c  
trandom.c  
triangle.c  
triangle.h  
trtl.c  
tsplay.c  
ttime.c  
ttri.c  
ucli.c  
uexec1.c  
uexec2.c  
uexec.c  
urtl.c  
utxcpt1.c  
utxcpt2.c  
utxcpt3.c  
utxcpt4.c  
version.c

i386/byteswap.asm :

RtlUshortByteSwap  
RtlUlongByteSwap  
RtlUlonglongByteSwap

i386/context.c :

RtlInitializeContext  
RtlRemoteCall

i386/debug2.asm :

DbgBreakPoint  
DbgUserBreakPoint  
DbgBreakPointWithStatus

i386/debug3.c :

```
    DebugPrint
    DebugPrompt
    DebugLoadImageSymbols
    DebugService
    DebugUnLoadImageSymbols
i386/divlarge.c :
    RtlLargeIntegerDivide
i386/exdsptch.c :
    RtlDispatchException
    RtlUnwind
i386/exsup.asm :
    nothing special
i386/forceres.asm :
    foo
i386/halvprnt.c :
    vprintf
    fields
    putx
    puti
    putu
    putc
    xatoi
i386/ioaccess.asm :
    READ_REGISTER_UCHAR
    READ_REGISTER_USHORT
    READ_REGISTER_ULONG
    READ_REGISTER_BUFFER_UCHAR
    READ_REGISTER_BUFFER_USHORT
    READ_REGISTER_BUFFER_ULONG
    WRITE_REGISTER_UCHAR
    WRITE_REGISTER_USHORT
    WRITE_REGISTER_ULONG
    WRITE_REGISTER_BUFFER_UCHAR
    WRITE_REGISTER_BUFFER_USHORT
    WRITE_REGISTER_BUFFER_ULONG
i386/largeint.asm :
```

RtlLargeIntegerAdd  
RtlEnlargedIntegerMultiply  
RtlEnlargedUnsignedMultiply  
RtlEnlargedUnsignedDivide  
RtlExtendedLargeIntegerDivide  
RtlExtendedMagicDivide  
RtlExtendedIntegerMultiply  
RtlLargeIntegerShiftLeft  
RtlLargeIntegerShiftRight  
RtlLargeIntegerArithmeticShift  
RtlLargeIntegerNegate  
RtlLargeIntegerSubtract  
RtlConvertLongToLargeInteger  
RtlConvertUlongToLargeInteger

i386/movemem.asm :

RtlCompareMemory  
RtlFillMemory  
RtlFillMemoryUlonglong  
RtlFillMemoryUlong  
RtlZeroMemory  
RtlMoveMemory

i386/nlssup.asm :

RtlAnsiCharToUnicodeChar  
RtlpAnsiPszToUnicodePsz

i386/nlstrans.asm :

RtlUnicodeToMultiByteN  
RtlUnicodeToOemN

i386/rtcurteb.asm :

NtCurrentTeb

i386/ntrtl386.h :

nothing special

i386/raise.asm :

RtlRaiseException

i386/raisests.c :

RtlRaiseStatus

i386/rtldump.c :

RtlpContextDump  
RtlpExceptionReportDump  
RtlpExceptionRegistrationDump  
i386/slist.asm :  
RtlpInterlockedPopEntrySList  
RtlpInterlockedPushEntrySList  
i386/stkwalk.asm :  
RtlGetCallersAddress  
RtlCaptureStackBackTrace  
i386/stringsp.asm :  
RtlInitAnsiString  
RtlInitUnicodeString  
i386/userdisp.asm :  
KiUserApcDispatcher  
KiUserCallbackDispatcher  
KiUserExceptionDispatcher  
KiRaiseUserExceptionDispatcher  
i386/xcptmisc.asm :  
RtlpExecuteHandlerForException  
RtlpExecuteHandlerForUnwind  
ExceptionHandler  
UnwindHandler  
RtlpUnlinkHandler  
RtlCaptureContext  
RtlpCaptureContext  
RtlpGetStackLimits  
RtlpGetRegistrationHead  
RtlpGetReturnAddress  
acledit.c :  
FirstAce  
NextAce  
LongAligned  
WordAligned  
RtlCreateAcl  
RtlValidAcl  
RtlQueryInformationAcl

RtlSetInformationAcl  
RtlAddAce  
RtlDeleteAce  
RtlGetAce  
RtlAddCompoundAce  
RtlpAddKnownAce  
RtlpAddKnownObjectAce  
RtlAddAccessAllowedAce  
RtlAddAccessAllowedAceEx  
RtlAddAccessDeniedAce  
RtlAddAccessDeniedAceEx  
RtlAddAuditAccessAce  
RtlAddAuditAccessAceEx  
RtlAddAccessAllowedObjectAce  
RtlAddAccessDeniedObjectAce  
RtlAddAuditAccessObjectAce  
RtlMakePosixAcl  
RtlInterpretPosixAcl  
RtlFirstFreeAce  
RtlpAddData  
RtlpDeleteData

assert.c :

RtlAssert

atom.c :

RtlpAllocateAtom  
RtlpFreeAtom  
RtlpInitializeLockAtomTable  
RtlpLockAtomTable  
RtlpUnlockAtomTable  
RtlpDestroyLockAtomTable  
RtlpInitializeHandleTableForAtomTable  
RtlpDestroyHandleTableForAtomTable  
RtlpAtomMapAtomToHandleEntry  
RtlpCreateHandleForAtom  
RtlpFreeHandleForAtom  
RtlInitializeAtomPackage

RtICreateAtomTable  
RtIDestroyAtomTable  
RtIEmptyAtomTable  
RtIIntegerAtom  
RtIHashStringToAtom  
RtIAddAtomToAtomTable  
RtILookupAtomInAtomTable  
RtIDeleteAtomFromAtomTable  
RtIPinAtomInAtomTable  
RtIQueryAtomInAtomTable  
RtIQueryAtomsInAtomTable

bitmap.c :

DumpBitMap  
GET\_BYTE\_DECLARATIONS  
GET\_BYTE\_INITIALIZATION  
GET\_BYTE  
RtIInitializeBitMap  
RtIClearAllBits  
RtISetAllBits  
RtIFindClearBits  
RtIFindSetBits  
RtIFindClearBitsAndSet  
RtIFindSetBitsAndClear  
RtIClearBits  
RtISetBits  
RtIFindClearRuns  
RtIFindLongestRunClear  
RtIFindFirstRunClear  
RtINumberOfClearBits  
RtINumberOfSetBits  
RtIAreBitsClear  
RtIAreBitsSet  
RtIFindNextForwardRunClear  
RtIFindLastBackwardRunClear  
RtIFindMostSignificantBit  
RtIFindLeastSignificantBit

byteswap.c :

- RtlUshortByteSwap
- RtlUlongByteSwap
- RtlUlonglongByteSwap

checksum.c :

- ChkSum
- LdrVerifyMappedImageMatchesChecksum

cnvint.c :

- RtlIntegerToChar
- RtlCharToInteger
- RtlUnicodeStringToInteger
- RtlIntegerToUnicode
- RtlIntegerToUnicodeString
- RtlLargeIntegerToChar
- RtlLargeIntegerToUnicode
- RtlInt64ToUnicodeString

debug.c :

- DbgPrint
- DbgPrintReturnControlC
- DbgPrompt
- DbgLoadImageSymbols
- DbgUnloadImageSymbols

dev2dos.c :

- QuerySymbolicLink
- QueryDeviceNameForPath
- OpenDeviceReparseIndex
- IsVolumeName
- GetNextReparseVolumePath
- FindPathForDevice
- RtlVolumeDeviceToDosName

eballoc.c :

- RtlAcquirePebLock
- RtlReleasePebLock

environ.c :

- RtlCreateEnvironment
- RtlDestroyEnvironment



```
RtlSetCurrentEnvironment
RtlQueryEnvironmentVariable_U
RtlSetEnvironmentVariable
error.c :
    RtlNtStatusToDosError
    RtlNtStatusToDosErrorNoTeb
excpdbg.c :
    RtlInitializeExceptionLog
    RtlpLogExceptionHandler
    RtlpLogLastExceptionDisposition
gen8dot3.c :
    IsDbcsCharacter
    RtlGenerate8dot3Name
    RtlIsValidOemCharacter
    GetNextWchar
    RtlComputeLfnChecksum
    RtlIsNameLegalDOS8Dot3
generr.c :
gentable.c :
    FindNodeOrParent
    RtlInitializeGenericTable
    RtlInsertElementGenericTable
    RtlInsertElementGenericTableFull
    RtlDeleteElementGenericTable
    RtlLookupElementGenericTable
    RtlLookupElementGenericTableFull
    RtlEnumerateGenericTable
    RtlIsGenericTableEmpty
    RtlGetElementGenericTable
    RtlNumberGenericTableElements
    RtlEnumerateGenericTableWithoutSplaying
guid.c :
    RtlStringFromGUID
    ScanHexFormat
    RtlGUIDFromString
```

handle.c :

- RtlInitializeHandleTable
- RtlDestroyHandleTable
- RtlAllocateHandle
- RtlFreeHandle
- RtlIsValidHandle
- RtlIsValidIndexHandle

heap.c :

- RtlFindFirstSetRightMember
- RtlCreateHeap
- RtlDestroyHeap
- RtlAllocateHeap
- RtlAllocateHeapSlowly
- RtlFreeHeap
- RtlFreeHeapSlowly
- RtlSizeHeap
- RtlZeroHeap
- RtlpCreateUnCommittedRange
- RtlpDestroyUnCommittedRange
- RtlpInsertUnCommittedPages
- RtlpFindAndCommitPages
- RtlpInitializeHeapSegment
- RtlpDestroyHeapSegment
- RtlpExtendHeap
- RtlpCoalesceFreeBlocks
- RtlpDeCommitFreeBlock
- RtlpInsertFreeBlock
- RtlpGetExtraStuffPointer
- RtlpGetSizeOfBigBlock
- RtlpCheckBusyBlockTail

heapdbg.c :

- RtlpUpdateHeapListIndex
- RtlpValidateHeapHeaders
- RtlDebugCreateHeap
- RtlpSerializeHeap
- RtlDebugDestroyHeap

RtIDebugAllocateHeap  
RtIDebugReAllocateHeap  
RtIDebugFreeHeap  
RtIDebugGetUserInfoHeap  
RtIDebugSetUserValueHeap  
RtIDebugSetUserFlagsHeap  
RtIDebugSizeHeap  
RtIDebugCompactHeap  
RtIDebugZeroHeap  
RtIDebugCreateTagHeap  
RtIDebugQueryTagHeap  
RtIDebugUsageHeap  
RtIDebugWalkHeap  
RtIpValidateHeapEntry  
RtIpValidateHeapSegment  
RtIpValidateHeap  
RtIpBreakPointHeap

heapdll.c :

RtIInitializeHeapManager  
RtIProtectHeap  
RtILockHeap  
RtIUnlockHeap  
RtIReAllocateHeap  
RtIGetUserInfoHeap  
RtISetUserValueHeap  
RtISetUserFlagsHeap  
RtICreateTagHeap  
RtIQueryTagHeap  
RtIExtendHeap  
RtICompactHeap  
RtIValidateHeap  
RtIValidateProcessHeaps  
RtIGetProcessHeaps  
RtIEnumProcessHeaps  
RtIUsageHeap  
RtIWalkHeap

RtlpCheckHeapSignature  
RtlpCoalesceHeap  
RtlpAddHeapToProcessList  
RtlpRemoveHeapFromProcessList  
RtlpGrowBlockInPlace  
RtlpAllocateTags  
RtlpGetTagName  
RtlpUpdateTagEntry  
RtlpResetTags  
RtlpDestroyTags  
RtlpAllocateHeapUsageEntry  
RtlpFreeHeapUsageEntry  
RtlpHeapIsLocked

heappage.c :

ROUNDUP2  
HEAP\_HANDLE\_FROM\_ROOT  
IF\_GENERATE\_EXCEPTION  
OUT\_OF\_VM\_BREAK  
ENQUEUE\_HEAD  
ENQUEUE\_TAIL  
DEQUEUE\_NODE  
BIAS\_POINTER  
UNBIAS\_POINTER  
IS\_BIASED\_POINTER  
PROTECT\_HEAP\_STRUCTURES  
UNPROTECT\_HEAP\_STRUCTURES  
BUMP\_GLOBAL\_COUNTER  
BUMP\_SIZE\_COUNTER  
RtlpDebugPageHeapBreak  
RtlpDebugPageHeapAssert  
RtlpDebugPageHeapEnterCriticalSection  
RtlpDebugPageHeapLeaveCriticalSection  
RtlpDebugPageHeapException  
RtlpDebugPageHeapPointerFromHandle  
RtlpDebugPageHeapProtectionText  
RtlpDebugPageHeapRobustProtectVM

RtlpDebugPageHeapProtectVM  
RtlpDebugPageHeapAllocateVM  
RtlpDebugPageHeapReleaseVM  
RtlpDebugPageHeapCommitVM  
RtlpDebugPageHeapDecommitVM  
RtlpDebugPageHeapTakeNodeFromUnusedList  
RtlpDebugPageHeapReturnNodeToUnusedList  
RtlpDebugPageHeapFindBusyMem  
RtlpDebugPageHeapRemoveFromAvailableList  
RtlpDebugPageHeapPlaceOnFreeList  
RtlpDebugPageHeapRemoveFromFreeList  
RtlpDebugPageHeapPlaceOnVirtualList  
RtlpDebugPageHeapPlaceOnBusyList  
RtlpDebugPageHeapRemoveFromBusyList  
RtlpDebugPageHeapSearchAvailableMemListForBestFit  
RtlpDebugPageHeapCoalesceNodeIntoAvailable  
RtlpDebugPageHeapCoalesceFreeIntoAvailable  
RtlpDebugPageHeapFindAvailableMem  
RtlpDebugPageHeapPlaceOnPoolList  
RtlpDebugPageHeapAddNewPool  
RtlpDebugPageHeapAllocateNode  
RtlpDebugPageHeapGrowVirtual  
RtlpDebugPageHeapProtectStructures  
RtlpDebugPageHeapUnprotectStructures  
RtlpDebugPageHeapVerifyList  
RtlpDebugPageHeapVerifyIntegrity  
RtlpDebugPageHeapCreate  
RtlpDebugPageHeapAllocate  
RtlpDebugPageHeapFree  
RtlpDebugPageHeapReAllocate  
RtlpDebugPageHeapDestroy  
RtlpDebugPageHeapSize  
RtlpDebugPageHeapGetProcessHeaps  
RtlpDebugPageHeapCompact  
RtlpDebugPageHeapValidate  
RtlpDebugPageHeapWalk

RtlpDebugPageHeapLock  
RtlpDebugPageHeapUnlock  
RtlpDebugPageHeapSetUserValue  
RtlpDebugPageHeapGetUserInfo  
RtlpDebugPageHeapSetUserFlags  
RtlpDebugPageHeapSerialize  
RtlpDebugPageHeapExtend  
RtlpDebugPageHeapZero  
RtlpDebugPageHeapReset  
RtlpDebugPageHeapUsage  
RtlpDebugPageHeapIsLocked  
RtlpDphShouldAllocateInPageHeap  
RtlpDphReportCorruptedBlock  
RtlpDphIsPageHeapBlock  
RtlpDphIsNormalHeapBlock  
RtlpDphIsNormalFreeHeapBlock  
RtlpDphWritePageHeapBlockInformation  
RtlpDphWriteNormalHeapBlockInformation  
RtlpDphNormalHeapAllocate  
RtlpDphNormalHeapFree  
RtlpDphNormalHeapReAllocate  
RtlpDphNormalHeapSize  
RtlpDphNormalHeapSetUserFlags  
RtlpDphNormalHeapSetUserValue  
RtlpDphNormalHeapGetUserInfo  
RtlpDphNormalHeapValidate  
RtlpDphInitializeDelayedFreeQueue  
RtlpDphAddToDelayedFreeQueue  
RtlpDphNeedToTrimDelayedFreeQueue  
RtlpDphTrimDelayedFreeQueue  
RtlpDphFreeDelayedBlocksFromHeap  
RtlpDphLogStackTrace  
RtlpDphTargetDIIISLogicInitialize  
RtlpDphTargetDIIISLoadCallback  
RtlpDphIsDIIITargeted  
RtlpDphSearchBlockInList

```
RtlpDphInternalValidatePageHeap
heappage.h :
    IS_DEBUG_PAGE_HEAP_HANDLE
    IF_DEBUG_PAGE_HEAP_THEN_RETURN
    IF_DEBUG_PAGE_HEAP_THEN_CALL
    IF_DEBUG_PAGE_HEAP_THEN_BREAK
    RtlpDebugPageHeapValidate
heappagi.h :
    nothing special
heappriv.h :
    RtlInitializeLockRoutine
    RtlAcquireLockRoutine
    RtlReleaseLockRoutine
    RtlDeleteLockRoutine
    RtlOkayToLockRoutine
    DEBUG_HEAP
    SET_LAST_STATUS
    HeapDebugPrint
    HeapDebugBreak
    SET_FREELIST_BIT
    CLEAR_FREELIST_BIT
    RtlpInsertFreeBlockDirect
    RtlpFastInsertFreeBlockDirect
    RtlpFastInsertDedicatedFreeBlockDirect
    RtlpFastInsertNonDedicatedFreeBlockDirect
    RtlpRemoveFreeBlock
    RtlpFastRemoveFreeBlock
    RtlpFastRemoveDedicatedFreeBlock
    RtlpFastRemoveNonDedicatedFreeBlock
    IS_HEAP_TAGGING_ENABLED
imagedir.c :
    RtlImageNtHeader
    RtlSectionTableFromVirtualAddress
    RtlAddressInSectionTable
    RtlpImageDirectoryEntryToData32
    RtlpImageDirectoryEntryToData64
```

RtlImageDirectoryEntryToData

RtlImageRvaToSection

RtlImageRvaToVa

ldrreloc.c :

SWAP\_SHORT

SWAP\_INT

SWAP\_LONG\_LONG

LdrRelocateImage

LdrProcessRelocationBlock

LdrDoubleRelocateImage

LdrpProcessVolatileRelocationBlock

ldrsrc.c :

LdrAccessResource

LdrpAccessResourceData

LdrFindEntryForAddress

LdrFindResource\_U

LdrFindResourceDirectory\_U

LdrpCompareResourceNames\_U

LdrpSearchResourceSection\_U

LdrEnumResources

LdrAlternateResourcesEnabled

LdrGetAlternateResourceModuleHandle

LdrpGetFileVersion

LdrpVerifyAlternateResourceModule

LdrpSetAlternateResourceModuleHandle

LdrLoadAlternateResourceModule

LdrUnloadAlternateResourceModule

LdrFlushAlternateResourceModules

lookasid.c :

RtlpInitializeHeapLookaside

RtlpDeleteHeapLookaside

RtlpAdjustHeapLookasideDepth

RtlpAllocateFromHeapLookaside

RtlpFreeToHeapLookaside

message.c :

RtlFindMessage



RtlFormatMessage

mrcf.c :

RtlDecompressBufferMrcf

MrcfSetBitBuffer

MrcfReadBit

MrcfReadNBits

MrcfFillBitBuffer

nls.c :

RtlAnsiStringToUnicodeString

RtlAnsiCharToUnicodeChar

RtlUnicodeStringToAnsiString

RtlUppcaseUnicodeStringToAnsiString

RtlOemStringToUnicodeString

RtlUnicodeStringToOemString

RtlUppcaseUnicodeStringToOemString

RtlOemStringToCountedUnicodeString

RtlUnicodeStringToCountedOemString

RtlUppcaseUnicodeStringToCountedOemString

RtlUppcaseUnicodeString

RtlDowncaseUnicodeString

RtlUppcaseUnicodeChar

RtlFreeUnicodeString

RtlFreeAnsiString

RtlFreeOemString

RtlxUnicodeStringToAnsiSize

RtlxUnicodeStringToOemSize

RtlxAnsiStringToUnicodeSize

RtlxOemStringToUnicodeSize

RtlCompareUnicodeString

RtlEqualUnicodeString

RtlPrefixUnicodeString

RtlCopyUnicodeString

RtlAppendUnicodeToString

RtlAppendUnicodeStringToString

RtlCreateUnicodeString

RtlEqualDomainName

RtlEqualComputerName  
RtlIsTextUnicode  
RtlDnsHostNameToComputerName

nlsxlat.c :

RtlConsoleMultiByteToUnicodeN  
RtlMultiByteToUnicodeN  
RtlOemToUnicodeN  
RtlMultiByteToUnicodeSize  
RtlUnicodeToMultiByteSize  
RtlUnicodeToMultiByteN  
RtlUppcaseUnicodeToMultiByteN  
RtlUnicodeToOemN  
RtlUppcaseUnicodeToOemN  
RtlpDidUnicodeToOemWork  
RtlCustomCPToUnicodeN  
RtlUnicodeToCustomCPN  
RtlUppcaseUnicodeToCustomCPN  
RtlInitCodePageTable  
RtlpInitUppcaseTable  
RtlInitNlsTables  
RtlResetRtlTranslations  
RtlGetDefaultCodePage

ntrtlp.h :

RtlpBitSetAnywhere  
RtlpBitsSetLow  
RtlpBitsSetHigh  
RtlpBitsSetTotal  
LOBYTE  
HIBYTE  
GET8  
GETH14  
GETL04  
TRAVERSE844W  
NLS\_UPCASE  
NLS\_DOWNCASE  
RtlpInitializeSListHead

```
RtIpQueryDepthSList
pctohdr.c :
    RtIpcToFileHeader
prefix.c :
    PfxInitialize
    PfxInsertPrefix
    PfxRemovePrefix
    PfxFindPrefix
    ComputeNameLength
    CompareNamesCaseSensitive
    RtlInitializeUnicodePrefix
    RtlInsertUnicodePrefix
    RtlRemoveUnicodePrefix
    RtlFindUnicodePrefix
    RtlNextUnicodePrefix
    ComputeUnicodeNameLength
    CompareUnicodeStrings
prodtype.c :
    RtIGetNtProductType
random.c :
    Multiplier
    Increment
    Modulus
    RtlUniform
    UniformMacro
    RtlRandom
range.c :
    RtlInitializeRangeListPackage
    RtlAllocateRangeListEntry
    RtlFreeRangeListEntry
    RtlRangeListAllocatePool
    RtlRangeListFreePool
    RtlAllocateRangeListEntry
    RtlFreeRangeListEntry
    RtlRangeListAllocatePool
    RtlRangeListFreePool
```

RtIInitializeRangeList  
RtIAddRange  
RtIpAddRange  
RtIpAddToMergedRange  
RtIpConvertToMergedRange  
RtIpCreateRangeListEntry  
RtIpAddIntersectingRanges  
RtIDeleteRange  
RtIDeleteOwnersRanges  
RtIpDeleteFromMergedRange  
RtIpCopyRangeListEntry  
RtICopyRangeList  
RtIpDeleteRangeListEntry  
RtIFreeRangeList  
RtIIsRangeAvailable  
RtIpIsRangeAvailable  
RtIFindRange  
RtIGetFirstRange  
RtIGetLastRange  
RtIGetNextRange  
RtIMergeRangeLists  
RtIInvertRangeList  
RtIpDumpRangeListEntry  
RtIpDumpRangeList

range.h :

MERGED  
SHARED  
CONFLICT  
FOR\_ALL\_IN\_LIST  
FOR\_ALL\_IN\_LIST\_SAFE  
FOR\_REST\_IN\_LIST  
FOR\_REST\_IN\_LIST\_SAFE  
FOR\_ALL\_IN\_LIST\_BACKWARDS  
FOR\_ALL\_IN\_LIST\_SAFE\_BACKWARDS  
FOR\_REST\_IN\_LIST\_BACKWARDS  
FOR\_REST\_IN\_LIST\_SAFE\_BACKWARDS

LAST\_IN\_LIST  
FIRST\_IN\_LIST  
RANGE\_DISJOINT  
RANGE\_INTERSECT  
RANGE\_LIMITS\_DISJOINT  
RANGE\_LIMITS\_INTERSECT  
RANGE\_LIST\_ENTRY\_FROM\_LIST\_ENTRY  
RANGE\_LIST\_FROM\_LIST\_HEAD  
FOR\_REST\_OF\_RANGES  
InsertEntryList

recip.c :

multiplication            integer division

registry.c :

RtlpNtOpenKey  
RtlpNtCreateKey  
RtlpNtQueryValueKey  
RtlpNtSetValueKey  
RtlpNtMakeTemporaryKey  
RtlpNtEnumerateSubKey

regutil.c :

RtlpGetRegistryHandle  
RtlpQueryRegistryDirect  
QuadAlignPtr  
RtlpCallQueryRegistryRoutine  
RtlpAllocDeallocQueryBuffer  
RtlQueryRegistryValues  
RtlWriteRegistryValue  
RtlCheckRegistryKey  
RtlCreateRegistryKey  
RtlDeleteRegistryValue  
RtlExpandEnvironmentStrings\_U  
RtlGetNtGlobalFlags  
RtlFormatCurrentUserKeyPath  
RtlOpenCurrentUser  
RtlpGetTimeZoneInfoHandle  
RtlQueryTimeZoneInformation

```
RtlSetTimeZoneInformation
RtlSetActiveTimeBias
remlock.c :
    MinutesToTicks
    RtlAllocateRemoveLock
    RtlAcquireRemoveLockEx
    RtlReleaseRemoveLock
    RtlReleaseRemoveLockAndWait
remlock.h :
    nothing special
rtlassig.c :
    RtlSelfRelativeToAbsoluteSD
    RtlMakeSelfRelativeSD
    RtlAbsoluteToSelfRelativeSD
    RtlpQuerySecurityDescriptor
    RtlSelfRelativeToAbsoluteSD2
rtldata.c :
    Runtime Library          가
rtlexec.c :
    ROUND_UP
    ISTERMINALSERVER
    RtlpCopyProcString
    RtlCreateProcessParameters
    RtlDestroyProcessParameters
    RtlpNormalizeProcessParam
    RtlpDeNormalizeProcessParam
    RtlNormalizeProcessParams
    RtlDeNormalizeProcessParams
    RtlpOpenImageFile
    RtlpCreateStack
    RtlpFreeStack
    RtlCreateUserProcess
    RtlCreateUserThread
    RtlFreeUserThreadStack
rxact.c :
    DwordAlign
```

RtlInitializeRXact  
RXactInitializeContext  
RtlStartRXact  
RtlAbortRXact  
RtlAddAttributeActionToRXact  
RtlAddActionToRXact  
RtlApplyRXact  
RtlApplyRXactNoFlush  
RXactpCommit  
RXactpOpenTargetKey

seridl.c :

RtlRunEncodeUnicodeString  
RtlRunDecodeUnicodeString  
RtlEraseUnicodeString  
RtlAdjustPrivilege  
RtlValidSid  
RtlEqualSid  
RtlEqualPrefixSid  
RtlLengthRequiredSid  
RtlAllocateAndInitializeSid  
RtlInitializeSid  
RtlFreeSid  
RtlIdentifierAuthoritySid  
RtlSubAuthoritySid  
RtlSubAuthorityCountSid  
RtlLengthSid  
RtlCopySid  
RtlCopySidAndAttributesArray  
RtlLengthSidAsUnicodeString  
RtlConvertSidToUnicodeString  
RtlEqualLuid  
RtlCopyLuid  
RtlCopyLuidAndAttributesArray  
RtlCreateSecurityDescriptor  
RtlCreateSecurityDescriptorRelative  
RtlValidSecurityDescriptor

RtlLengthSecurityDescriptor  
RtlLengthUsedSecurityDescriptor  
RtlSetAttributesSecurityDescriptor  
RtlGetControlSecurityDescriptor  
RtlSetControlSecurityDescriptor  
RtlSetDaclSecurityDescriptor  
RtlGetDaclSecurityDescriptor  
RtlSetSaclSecurityDescriptor  
RtlGetSaclSecurityDescriptor  
RtlSetOwnerSecurityDescriptor  
RtlGetOwnerSecurityDescriptor  
RtlSetGroupSecurityDescriptor  
RtlGetGroupSecurityDescriptor  
RtlAreAllAccessesGranted  
RtlAreAnyAccessesGranted  
RtlMapGenericMask  
RtlImpersonateSelf  
RtlIsValidOwnerSubjectContext  
RtlpApplyAclToObject  
RtlpCopyEffectiveAce  
RtlpCopyAces  
RtlpInheritAcl2  
RtlpInheritAcl  
RtlpGenerateInheritedAce  
RtlpGenerateInheritAcl  
RtlpComputeMergedAcl2  
RtlpComputeMergedAcl  
RtlDumpUserSid  
RtlpConvertToAutoInheritSecurityObject  
AceFlagsInAce  
RtlpCompareAces  
RtlpCompareKnownAces  
RtlpCompareKnownObjectAces  
RtlpConvertAclToAutoInherit  
RtlpIsDuplicateAce  
RtlpCreateServerAcl



RtlpGetDefaultsSubjectContext  
RtlpNewSecurityObject  
RtlpSetSecurityObject  
RtlpValidateSDOffsetAndSize  
RtlValidRelativeSecurityDescriptor  
RtlGetSecurityDescriptorRMControl  
RtlSetSecurityDescriptorRMControl

splay.c :

SwapPointers  
ParentsChildPointerAddress  
RtlSplay  
RtlDelete  
RtlDeleteNoSplay  
RtlSubtreeSuccessor  
RtlSubtreePredecessor  
RtlRealSuccessor  
RtlRealPredecessor  
SwapSplayLinks

stdtimep.h :

Convert100nsToMilliseconds  
ConvertMillisecondsTo100ns  
Convert100nsToSeconds  
ConvertSecondsTo100ns  
ConvertMillisecondsToDays  
ShiftStandardTimeRevision  
MaskStandardTimeTdf  
GetStandardTimeTdf  
GetStandardTimeRev  
IsPositive  
IsAbsoluteTime  
IsDeltaTime  
GreaterThanTime  
GreaterThanStdTime  
ElapsedDaysToYears  
NumberOfLeapYears  
ElapsedYearsToDays

IsLeapYear

MaxDaysInMonth

stktrace.c :

RtlGetCallersAddress

RtlInitStackTraceDataBaseEx

RtlInitializeStackTraceDataBase

RtlpAcquireStackTraceDataBase

RtlpReleaseStackTraceDataBase

RtlpExtendStackTraceDataBase

RtlLogStackBackTrace

RtlCaptureStackBackTrace

RtlWalkFrameChain

CollectFrameWalkStatistics

string.c :

RtlInitString

RtlInitAnsiString

RtlInitUnicodeString

RtlCopyString

RtlUpperChar

RtlCompareString

RtlEqualString

RtlPrefixString

RtlCreateUnicodeStringFromAsciiz

RtlUpperString

RtlAppendAsciizToString

RtlAppendStringToString

RtlCompareMemoryUlong

tacl.c :

ACL

tbitmap.c :

Bitmap Procedure

threads.c :

RtlRegisterWait

RtlDeregisterWait

RtlDeregisterWaitEx

RtlQueueWorkItem

RtlSetIoCompletionCallback  
RtlCreateTimerQueue  
RtlDeleteTimerQueue  
RtlDeleteTimerQueueEx  
RtlCreateTimer  
RtlUpdateTimer  
RtlDeleteTimer  
RtlSetThreadPoolStartFunc  
RtlThreadPoolCleanup  
RtlpQueueWorkerRequest  
RtlpExecuteWorkerRequest  
RtlpQueueIoWorkerRequest  
RtlpStartWorkerThread  
RtlpStartIoWorkerThread  
RtlpWorkerThreadTimerCallback  
RtlpInitializeWorkerThreadPool  
RtlpWorkerThreadInitializeTimers  
RtlpWorkerThread  
RtlpIoWorkerThread  
RtlpExecuteLongIoWorkItem  
RtlpExecuteIoWorkItem  
RtlpStartThread  
RtlpExitThread  
RtlpInitializeWaitThreadPool  
RtlpWaitThread  
RtlpAsyncCallbackCompletion  
RtlpProcessWaitCompletion  
RtlpAddWait  
RtlpDeregisterWait  
RtlpDeactivateWait  
RtlpDeleteWait  
RtlpDoNothing  
RtlpGet64BitTickCount  
RtlpResync64BitTickCount  
RtlpProcessTimeouts  
RtlpFireTimers

RtlpFindWaitThread  
RtlpAddTimer  
RtlpUpdateTimer  
RtlpCancelTimer  
RtlpCancelTimerEx  
RtlpDeactivateTimer  
RtlpDeleteTimer  
RtlpGetQueueRelativeTime  
RtlpGetTimeRemaining  
RtlpResetTimer  
RtlpInsertInDeltaList  
RtlpRemoveFromDeltaList  
RtlpReOrderDeltaList  
RtlpAddTimerQueue  
RtlpServiceTimer  
RtlpFireTimersAndReorder  
RtlpInsertTimersIntoDeltaList  
RtlpTimerThread  
RtlpInitializeTimerThreadPool  
RtlpDeleteTimerQueue  
RtlpDeleteTimerQueueComplete  
RtlpThreadCleanup  
RtlpWaitForEvent  
RtlpGetWaitEvent  
RtlpFreeWaitEvent  
RtlpInitializeEventCache  
PrintTimerQueue  
RtlDebugPrintTimes  
RtlSetTimer  
RtlpForceAllocateTPHeap  
RtlCancelTimer

threads.h :

ONE\_MILLISECOND\_TIMEOUT  
HUNDRED\_MILLISECOND\_TIMEOUT  
ONE\_SECOND\_TIMEOUT  
RtlpFreeTPHeap

RtlAllocateTPHeap  
ACQUIRE\_GLOBAL\_WAIT\_LOCK  
RELEASE\_GLOBAL\_WAIT\_LOCK  
ACQUIRE\_GLOBAL\_TIMER\_LOCK  
RELEASE\_GLOBAL\_TIMER\_LOCK  
IS\_COMPONENT\_INITIALIZED  
DBG\_SET\_FUNCTION  
RtlShiftWaitArray  
RtlGetResync64BitTickCount  
RtlSetFiring64BitTickCount  
SET\_SIGNATURE  
CHECK\_SIGNATURE  
SET\_DEL\_SIGNATURE  
CHECK\_DEL\_SIGNATURE  
CLEAR\_SIGNATURE  
SET\_DEL\_TIMERQ\_SIGNATURE

time.c :

Convert100nsToMilliseconds  
ConvertMillisecondsTo100ns  
Convert100nsToSeconds  
ConvertSecondsTo100ns  
ConvertMillisecondsToDays  
ConvertDaysToMilliseconds  
ElapsedDaysToYears  
NumberOfLeapYears  
ElapsedYearsToDays  
IsLeapYear  
MaxDaysInMonth  
TimeToDaysAndFraction  
DaysAndFractionToTime  
RtlTimeToTimeFields  
RtlCutoverTimeToSystemTime  
RtlTimeFieldsToTime  
RtlTimeToElapsedTimeFields  
RtlTimeToSecondsSince1980  
RtlSecondsSince1980ToTime

RtlTimeToSecondsSince1970

RtlSecondsSince1970ToTime

RtlSystemTimeToLocalTime

RtlLocalTimeToSystemTime

tnlsxlat.c :

Nlsxlat Procedure

tprefix.c :

Prefix Table

trandom.c :

Random Number Generator

triangle.c :

SwapPointers

SwapUlongs

SwapRefsButKeepFlags

SetRefViaPointer

TriSplay

TriDelete

TriSubtreeSuccessor

TriSubtreePredecessor

TriRealSuccessor

TriRealPredecessor

TriAddressOfBackRefViaParent

TriAddressOfBackRefViaChild

TriSwapSplayLinks

TriRotateRight

TriRotateLeft

triangle.h :

TriInitializeSplayLinks

TriParent

TriLeftChild

TriRightChild

TriIsRoot

TriIsLeftChild

TriIsRightChild

TriInsertAsLeftChild

TriInsertAsRightChild

IsParentRef  
MakeIntoParentRef  
IsSiblingRef  
MakeIntoSiblingRef  
IsLeftChildRef  
MakeIntoLeftChildRef  
IsRightChildRef  
MakeIntoRightChildRef  
MakeIntoPointer

trtl.c :  
Runtime Library

tsplay.c :  
SPlay Procedure

ttime.c :  
time

ttri.c :  
SPlay Procedure

ucli.c :  
Usermode Runtime Library

uexec1.c :  
Usermode Runtime Library . Sub 1

uexec2.c :  
Usermode Runtime Library . Sub 2

uexec.c :  
Usermode Runtime Library

urtl.c :  
Usermode Runtime Library

utxcpt1.c :  
user mode structured exception handling test 1

utxcpt2.c :  
user mode structured exception handling test 2

utxcpt3.c :  
user mode structured exception handling test 3

utxcpt4.c :  
user mode structured exception handling test 4

version.c :

OLD\_CONDITION  
OLD\_STYLE\_CONDITION\_MASK  
RTL\_GET\_CONDITION  
RtlGetVersion  
RtlpVerCompare  
RtlVerifyVersionInfo  
RtlpVerGetConditionMask  
VerSetConditionMask

```
#####  
#                               private/ntos/se                               #  
#####
```

Abstract :

Security Components

Prefix :

Se

Files :

accessck.c  
adt.h  
adtevent.c  
adtinit.c  
adtlog.c  
adtp.h  
adtutil.c  
adtvars.c  
capture.c  
ctaccess.c  
ctlpqos.c  
ctlpcqos.c  
ctseacc.c  
ctsertl.c  
cttoken.c  
dumpuser.c  
privileg.c  
rmaudit.c  
rmlogon.c



rmmain.c  
rmp.h  
rmvars.c  
seassign.c  
seastate.c  
seaudit.c  
seclient.c  
seglobal.c  
seinit.c  
semethod.c  
sep.c  
sep.h  
sepaudit.c  
subject.c  
token.c  
tokenadj.c  
tokendup.c  
tokenopn.c  
tokenp.h  
tokenqry.c  
tokenset.c  
tse.c  
tsecomm.c  
tseum.c  
tsevars.c  
ttokend.c  
ttseacc.c  
ttsertl.c  
uipers.c  
uipriv.c  
utaccess.c  
utlnpqos.c  
utlpcqos.c  
utseacc.c  
utseqos.c  
utsertl.c

uttoken.c

accessck.c :

SeCaptureObjectTypeList  
SeFreeCapturedObjectTypeList  
SepObjectInTypeList  
SepUpdateParentTypeList  
SepAddAccessTypeList  
SepSidInToken  
SepSidInTokenEx  
SepMaximumAccessCheck  
SepNormalAccessCheck  
SepAccessCheck  
NtAccessCheck  
NtAccessCheckByType  
NtAccessCheckByTypeResultList  
SeAccessCheckByType  
SeFreePrivileges  
SeAccessCheck  
SeProxyAccessCheck  
SePrivilegePolicyCheck  
SepTokenIsOwner  
SeFastTraverseCheck

adt.h :

SepAdtEventOnSuccess  
SepAdtEventOnFailure  
SepAdtAuditingEvent  
SepAdtAuditingEnabled  
SepAdtAuditingDisabled

adtevent.c :

nothing special

adtinit.c :

SepAdtValidateAuditBounds  
SepAdtInitializePhase1  
SepAdtInitializeBounds  
SepAdtInitializeCrashOnFail  
SepAdtInitializePrivilegeAuditing

```
        SepAdtInitializeAuditingOptions
adtlog.c :
    SepAdtLogAuditRecord
    SepAuditFailed
    SepAdtMarshalIAuditRecord
    SepAdtSetAuditLogInformation
    SepAdtCopyToLsaSharedMemory
    SepQueueWorkItem
    SepDequeueWorkItem
adtp.h :
    SepAdtAuditThisEvent
    SepAdtAuditThisEventEx
adtutil.c :
    SepDumpString
adtvars.c :
    Auditing
capture.c :
    SeCaptureSecurityDescriptor
    SeReleaseSecurityDescriptor
    SepCopyProxyData
    SepFreeProxyData
    SepProbeAndCaptureQosData
    SeFreeCapturedSecurityQos
    SeCaptureSecurityQos
    SeCaptureSid
    SeReleaseSid
    SeCaptureAcl
    SeReleaseAcl
    SeCaptureLuidAndAttributesArray
    SeReleaseLuidAndAttributesArray
    SeCaptureSidAndAttributesArray
    SeReleaseSidAndAttributesArray
    SeComputeQuotaInformationSize
    SeValidSecurityDescriptor
ctaccess.c :
    Common access validation test routines
```

ctInpqos.c :  
    Client-Side Test Routines

ctlpcqos.c :  
    Client-Side Test Routines

ctseacc.c :  
    Common security accessibility test routines

ctsertl.c :  
    Common security RTL test routines

cttoken.c :  
    Common token object test routines

dumpuser.c :  
    Usermode

privileg.c :  
    SepPrivilegeCheck  
    SePrivilegeCheck  
    NtPrivilegeCheck  
    SeSinglePrivilegeCheck  
    SeCheckPrivilegedObject

rmaudit.c :  
    SepRmSetAuditEventWrkr  
    SepRmSetAuditLogWrkr

rmlogon.c :  
    SepLogonSessionIndex  
    SepRmCreateLogonSessionWrkr  
    SepRmDeleteLogonSessionWrkr  
    SepReferenceLogonSession  
    SepDeReferenceLogonSession  
    SepCreateLogonSessionTrack  
    SepDeleteLogonSessionTrack  
    SepInformLsaOfDeletedLogon  
    SeRegisterLogonSessionTerminatedRoutine  
    SeUnregisterLogonSessionTerminatedRoutine  
    SeMarkLogonSessionForTerminationNotification  
    SepInformFileSystemsOfDeletedLogon  
    SepNotifyFileSystems

rmmain.c :

SeRmInitPhase1  
SepRmCommandServerThread  
SepRmCommandServerThreadInit  
SepRmComponentTestCommandWrkr  
SepRmSendCommandToLsaWrkr  
SepRmCallLsa  
SepRmInitPhase0

rpm.h :

SepRmAcquireDbReadLock  
SepRmAcquireDbWriteLock  
SepRmReleaseDbReadLock  
SepRmReleaseDbWriteLock

rmvars.c :

SepRmDbInitialization

seassign.c :

SeAssignSecurity  
SeAssignSecurityEx  
SeDeassignSecurity  
SepInheritAcl  
SeAssignWorldSecurityDescriptor  
SepDumpSecurityDescriptor  
SepPrintAcl  
SepPrintSid  
SepDumpTokenInfo  
SepSidTranslation

seastate.c :

SeCreateAccessState  
SeCreateAccessState  
SeDeleteAccessState  
SeDeleteAccessState  
SeSetAccessStateGenericMapping  
SeAppendPrivileges  
SepConcatenatePrivileges

seaudit.c :

SepSinglePrivilegeCheck  
SeCheckAuditPrivilege

SepProbeAndCaptureString\_U  
SepFreeCapturedString  
NtPrivilegeObjectAuditAlarm  
SePrivilegeObjectAuditAlarm  
NtPrivilegedServiceAuditAlarm  
SePrivilegedServiceAuditAlarm  
SepAccessCheckAndAuditAlarm  
NtAccessCheckAndAuditAlarm  
NtAccessCheckByTypeAndAuditAlarm  
NtAccessCheckByTypeResultListAndAuditAlarm  
NtAccessCheckByTypeResultListAndAuditAlarmByHandle  
NtOpenObjectAuditAlarm  
NtCloseObjectAuditAlarm  
NtDeleteObjectAuditAlarm  
SeOpenObjectAuditAlarm  
SeOpenObjectForDeleteAuditAlarm  
SeTraverseAuditAlarm  
SeCreateObjectAuditAlarm  
SeObjectReferenceAuditAlarm  
SeAuditHandleCreation  
SeCloseObjectAuditAlarm  
SeDeleteObjectAuditAlarm  
SepExamineSacl  
SepAuditTypeList  
SepSetAuditInfoForObjectTypes  
SepExamineSaclEx  
SepInitializePrivilegeFilter  
SepFilterPrivilegeAudits  
SeAuditingFileOrGlobalEvents  
SeAuditingFileEvents

seclient.c :

SepCreateClientSecurity  
SeCreateClientSecurity  
SeUpdateClientSecurity  
SeImpersonateClient  
SeImpersonateClientEx

SeCreateClientSecurityFromSubjectContext

seglobal.c :

SepVariableInitialization

SepInitSystemDacls

SepInitializePrivilegeSets

SepAssemblePrivileges

SepInitializeWorkList

seinit.c :

SeInitSystem

SepInitializationPhase0

SepInitializationPhase1

semethod.c :

SeSetSecurityAccessMask

SeQuerySecurityAccessMask

SeDefaultObjectMethod

SeSetSecurityDescriptorInfo

SeSetSecurityDescriptorInfoEx

SeQuerySecurityDescriptorInfo

SepDefaultDeleteMethod

sep.c :

SepCheckAcl

sep.h :

IF\_SE\_GLOBAL

SeDiagPrint

SepAreFlagsSet

SepSetFlags

SepClearFlags

SepPrivilegeSetSize

EffectiveToken

SepTokenUserSid

SepTokenAuthenticationId

SepBadImpersonationLevel

IsValidElementCount

SepLockLsaQueue

SepUnlockLsaQueue

SepWorkListHead

sepaudit.c :

- SepSetParmTypeSid
- SepSetParmTypeString
- SepSetParmTypeFileSpec
- SepSetParmTypeUlong
- SepSetParmTypeNoLogon
- SepSetParmTypeLogonId
- SepSetParmTypeAccessMask
- SepSetParmTypePrivileges
- SepSetParmTypeObjectTypes
- SepAdtPrivilegeObjectAuditAlarm
- SepAdtPrivilegedServiceAuditAlarm
- SepAdtOpenObjectAuditAlarm
- SepAdtOpenObjectForDeleteAuditAlarm
- SepAdtCloseObjectAuditAlarm
- SepAdtDeleteObjectAuditAlarm
- SepAdtHandleAuditAlarm
- SepAdtObjectReferenceAuditAlarm
- SepQueryNameString
- SepQueryTypeString
- SeAuditProcessCreation
- SeAuditHandleDuplication
- SeAuditProcessExit
- SepAdtGenerateDiscardAudit

subject.c :

- SeCaptureSubjectContext
- SeLockSubjectContext
- SeUnlockSubjectContext
- SeReleaseSubjectContext
- SepGetDefaultsSubjectContext
- SepIdAssignableAsGroup
- SepValidOwnerSubjectContext
- SeQueryAuthenticationIdSubjectContext

token.c :

- SeTokenType
- SeTokenIsAdmin



SeTokenIsRestricted  
SeTokenImpersonationLevel  
SeAssignPrimaryToken  
SeDeassignPrimaryToken  
SeExchangePrimaryToken  
SeGetTokenControlInformation  
SeMakeSystemToken  
SeMakeAnonymousLogonToken  
SeSubProcessToken  
SepTokenInitialization  
SepDumpToken  
NtCreateToken  
SepTokenDeleteMethod  
SepCreateToken  
SepIdAssignableAsOwner  
SeIsChildToken  
SeIsChildTokenByPointer  
NtImpersonateAnonymousToken

tokenadj.c :

NtAdjustPrivilegesToken  
NtAdjustGroupsToken  
SepAdjustPrivileges  
SepAdjustGroups

tokendup.c :

NtDuplicateToken  
SepDuplicateToken  
SepMakeTokenEffectiveOnly  
SepSidInSidAndAttributes  
SepRemoveDisabledGroupsAndPrivileges  
SeCopyClientToken  
NtFilterToken  
SeFilterToken  
SeFastFilterToken  
SepFilterToken

tokenopn.c :

SepCreateImpersonationTokenDacl

NtOpenProcessToken  
SepOpenTokenOfThread  
NtOpenThreadToken

tokenp.h :

IF\_TOKEN\_GLOBAL  
TokenDiagPrint  
SepAcquireTokenReadLock  
SepAcquireTokenWriteLock  
SepReleaseTokenReadLock  
SepReleaseTokenWriteLock  
SepArrayPrivilegeAttributes  
SepTokenPrivilegeAttributes  
SepArrayGroupAttributes  
SepTokenGroupAttributes

tokenqry.c :

NtQueryInformationToken  
SeQueryAuthenticationIdToken  
SeQueryInformationToken  
SeQuerySessionIdToken

tokenset.c :

NtSetInformationToken  
SepFreePrimaryGroup  
SepFreeDefaultDacL  
SepAppendPrimaryGroup  
SepAppendDefaultDacL  
SeSetSessionIdToken

tse.c :

SE . ( .)

tsecomm.c :

tseum.c :

Test program for the security system

tsevars.c :

This Module contains variables used in security test routines

ttokend.c :

This module tests token duplication



```
#####  
#                               private/ntos/udfs                               #  
#####
```

Comment :

```
#####  
#                               private/ntos/vdm                               #  
#####
```

Abstract :

VDM Manager

Prefix :

Nt

Vdm

Acronym :

VDM (Virtual DOS Machine)

Files :

i386/rdwr.c  
i386/strtexec.c  
i386/vdm.inc  
i386/vdmentry.c  
i386/vdmfault.c  
i386/vdminit.c  
i386/vdmints.c  
i386/vdmmisc.asm  
i386/vdmnpx.c  
i386/vdmop0f.asm  
i386/vdmoprnd.asm  
i386/vdmp.h  
i386/vdmprint.c  
i386/vdmprint.h  
i386/vdmtrace.c  
ntvdmp.h  
vdm.c

i386/rdwr.c :

GETFILEPOINTER

GETHANDLE  
GETBUFFER  
CONSOLE\_HANDLE  
NTFastDOSIO  
i386/strtexec.c :  
    VdmpStartExecution  
    VdmEndExecution  
i386/vdm.inc :  
    DISPATCH\_EXCEPTION  
    diBEGIN  
    dtI  
    diEND  
    dtBEGIN  
    dtS  
    dtEND  
    CsToLinearPM  
    CsToLinearV86  
i386/vdmentry.c :  
    AssertIrqlPassive  
    NtVdmControl  
i386/vdmfault.c :  
    VdmDispatchPageFault  
i386/vdminit.c :  
    VdmpInitialize  
i386/vdmints.c :  
    VdmpQueueInterrupt  
    VdmpQueueIntApcRoutine  
    VdmpQueueIntNormalRoutine  
    VdmDispatchInterrupts  
    RestartDelayedInterrupts  
    IcaScan  
    IcaAccept  
    GetIretHookAddress  
    PushRmInterrupt  
    PushPmInterrupt  
    VdmpDelayInterrupt

```
VdmpDelayIntDpcRoutine
VdmpDelayIntApcRoutine
VdmpDispatchableIntPending
VdmpIsThreadTerminating
VdmpNullRundownRoutine
VdmpExceptionHandler
i386/vdmmisc.asm :
    VdmSwapContexts
    VdmDispatchBop
    VdmpEnterIcaLock
    VdmpLeaveIcaLock
i386/vdmnp.c :
    VdmDispatchIRQ13
    VdmSkipNpxInstruction
i386/vdmop0f.asm :
    VdmOpcodeOf
    VdmOpcodeLmsw
    VdmOpcodeCIts
    VdmOpcodeGetCrx
    VdmOpcodeSetCrx
    VdmOpcodeGetDrx
    VdmOpcodeSetDrx
i386/vdmoprnd.asm :
    VdmDecodeOperand
i386/vdmp.h :
    nothing special
i386/vdmprint.c :
    VdmPrinterStatus
    VdmPrinterWriteData
    VdmFlushPrinterWriteData
    VdmpPrinterInitialize
    VdmpPrinterDirectIoOpen
    VdmpPrinterDirectIoClose
i386/vdmprint.h :
    get_status
    get_control
```

```
        host_lpt_status
        set_status
i386/vdmtrace.c :
        VdmTraceEvent
ntvdmp.h :
        nothing special
vdm.c :
        NtVdmControl
        VdmQueryDirectoryFile
```

```
#####
#                                     private/ntos/w32                             #
#####
```

```
Comment :
```

.