

oark
0.0.1

Generated by Doxygen 1.7.2

Thu Nov 25 2010 19:18:05

Contents

1	Data Structure Index	1
1.1	Data Structures	1
2	File Index	3
2.1	File List	3
3	Data Structure Documentation	5
3.1	_IDT_DESCRIPTOR Struct Reference	5
3.1.1	Field Documentation	6
3.1.1.1	DPL	6
3.1.1.2	gateType	6
3.1.1.3	offset00_15	6
3.1.1.4	offset16_31	6
3.1.1.5	P	6
3.1.1.6	selector	6
3.1.1.7	unused	6
3.1.1.8	zeroes	6
3.2	_IDTR Struct Reference	6
3.2.1	Field Documentation	6
3.2.1.1	baseAddressHi	6
3.2.1.2	baseAddressLow	6
3.2.1.3	nBytes	6
3.3	_KGDENTRY Struct Reference	7
3.3.1	Field Documentation	7
3.3.1.1	BaseLow	7
3.3.1.2	HighWord	7
3.3.1.3	LimitLow	7
3.4	_KIDTENTRY Struct Reference	7
3.4.1	Field Documentation	7
3.4.1.1	Access	7
3.4.1.2	ExtendedOffset	7
3.4.1.3	Offset	7
3.4.1.4	Selector	7
3.5	_KPCR Struct Reference	8
3.5.1	Field Documentation	8
3.5.1.1	GDT	8
3.5.1.2	IDR	8
3.5.1.3	IDT	8
3.5.1.4	Irql	8

3.5.1.5	IRR	8
3.5.1.6	IrrActive	8
3.5.1.7	KdVersionBlock	8
3.5.1.8	NtTib	8
3.5.1.9	Prpcb	8
3.5.1.10	SelfPcr	8
3.6	READ_KERN_MEM.s Struct Reference	9
3.6.1	Field Documentation	9
3.6.1.1	dst.address	9
3.6.1.2	size	9
3.6.1.3	src.address	9
3.6.1.4	type	9
4	File Documentation	11
4.1	common/common/common.h File Reference	11
4.1.1	Define Documentation	13
4.1.1.1	DEVICE_NAME	13
4.1.1.2	DRIVER_NAME	13
4.1.1.3	IDT_HARDCODE_SIZE	13
4.1.1.4	MAKEDWORD	13
4.1.1.5	NAMEOF_DEVICE	13
4.1.1.6	OARK_IOCTL_CHANGE_MODE	13
4.1.1.7	OARK_VERSION	13
4.1.1.8	SERVICE_NAME	13
4.1.1.9	SYMLINK_NAME	13
4.1.2	Typedef Documentation	13
4.1.2.1	IDT_DESCRIPTOR	13
4.1.2.2	IDTR	13
4.1.2.3	MEM_SYM_TYP_t	13
4.1.2.4	PIDT_DESCRIPTOR	13
4.1.2.5	READ_KERN_MEM_t	13
4.1.2.6	STATUS_t	13
4.1.3	Enumeration Type Documentation	13
4.1.3.1	MEM_SYM_TYP_e	13
4.1.3.2	STATUS_e	14
4.2	oark_driver/oark_driver/buildnumber.h File Reference	14
4.2.1	Define Documentation	14
4.2.1.1	_FILE_VERSION_BUILD	14
4.3	oark_driver/oark_driver/drvcommon.h File Reference	14
4.3.1	Define Documentation	14
4.3.1.1	_ANSISTRING	14
4.3.1.2	_WIDESTRING	15
4.3.1.3	ANSISTRING	15
4.3.1.4	CREATE_FVER	15
4.3.1.5	CREATE_PVER	15
4.3.1.6	CREATE_XVER	15
4.3.1.7	DebugPrint	15
4.3.1.8	PRESET_UNICODE_STRING	15
4.3.1.9	WIDESTRING	15
4.4	oark_driver/oark_driver/drvversion.h File Reference	15

4.4.1	Define Documentation	16
4.4.1.1	DRV_YEAR	16
4.4.1.2	FILE_BUILD	16
4.4.1.3	FILE_MAJVER	16
4.4.1.4	FILE_MINVER	16
4.4.1.5	PRD_BUILD	16
4.4.1.6	PRD_MAJVER	16
4.4.1.7	PRD_MINVER	16
4.4.1.8	TEXT_AUTHOR	16
4.4.1.9	TEXT_COMPANY	16
4.4.1.10	TEXT_COPYRIGHT	16
4.4.1.11	TEXT_FILEDESC	16
4.4.1.12	TEXT_INTERNALNAME	16
4.4.1.13	TEXT_MODULE	16
4.4.1.14	TEXT_PRODUCTNAME	16
4.4.1.15	TEXT_WEBSITE	16
4.5	oark_driver/oark_driver/makefile.inc File Reference	16
4.6	oark_driver/oark_driver/oark_driver.cpp File Reference	16
4.6.1	Function Documentation	17
4.6.1.1	DriverEntry	17
4.6.1.2	OARKDRIVER_DispatchCreateClose	17
4.6.1.3	OARKDRIVER_DispatchDeviceControl	17
4.6.1.4	OARKDRIVER_DriverUnload	17
4.6.1.5	WriteUserMode	17
4.6.2	Variable Documentation	17
4.6.2.1	pdoGlobalDrvObj	17
4.7	oark_driver/oark_driver/oark_driver.h File Reference	17
4.7.1	Define Documentation	18
4.7.1.1	FILE_DEVICE_OARKDRIVER	18
4.7.2	Function Documentation	18
4.7.2.1	PRESET_UNICODE_STRING	18
4.7.2.2	PRESET_UNICODE_STRING	18
4.8	oark_usermode/oark_usermode/debug.c File Reference	18
4.8.1	Function Documentation	19
4.8.1.1	EnableDebugPrivilege	19
4.8.2	Variable Documentation	19
4.8.2.1	debug	19
4.9	oark_usermode/oark_usermode/debug.h File Reference	19
4.9.1	Function Documentation	19
4.9.1.1	EnableDebugPrivilege	19
4.9.2	Variable Documentation	19
4.9.2.1	debug	19
4.10	oark_usermode/oark_usermode/driverusr.c File Reference	19
4.10.1	Function Documentation	20
4.10.1.1	IOCTLReadKernMem	20
4.10.1.2	LoadDriver	20
4.10.1.3	UnloadDriver	20
4.11	oark_usermode/oark_usermode/driverusr.h File Reference	20
4.11.1	Function Documentation	20
4.11.1.1	DumpRSRC	20

4.11.1.2	GetFullTempPath	20
4.11.1.3	IOCTLReadKernMem	20
4.11.1.4	LoadDriver	20
4.11.1.5	UnloadDriver	20
4.12	oark_usermode/oark_usermode/idt.c File Reference	20
4.12.1	Function Documentation	21
4.12.1.1	idt	21
4.13	oark_usermode/oark_usermode/idt.h File Reference	21
4.13.1	Typedef Documentation	22
4.13.1.1	KGDTENTRY	22
4.13.1.2	KIDTENTRY	22
4.13.1.3	KPCR	22
4.13.1.4	PKGDTENTRY	22
4.13.1.5	PKIDTENTRY	22
4.13.1.6	PKPCR	22
4.13.2	Function Documentation	22
4.13.2.1	idt	22
4.14	oark_usermode/oark_usermode/main.c File Reference	22
4.14.1	Function Documentation	22
4.14.1.1	main	22
4.15	oark_usermode/oark_usermode/others.c File Reference	22
4.15.1	Function Documentation	23
4.15.1.1	DumpRSRC	23
4.15.1.2	GetFullTempPath	23
4.15.1.3	LockInstance	23
4.16	oark_usermode/oark_usermode/others.h File Reference	23
4.16.1	Define Documentation	24
4.16.1.1	__OTHERS_H__	24
4.16.2	Function Documentation	24
4.16.2.1	DumpRSRC	24
4.16.2.2	GetFullTempPath	24
4.16.2.3	LockInstance	24
4.17	oark_usermode/oark_usermode/pebhooking.c File Reference	24
4.18	oark_usermode/oark_usermode/pebhooking.h File Reference	24
4.19	oark_usermode/oark_usermode/resource.h File Reference	24
4.19.1	Define Documentation	24
4.19.1.1	IDI_ICON1	24
4.19.1.2	IDR_OARK_DRIVER	24

Chapter 1

Data Structure Index

1.1 Data Structures

Here are the data structures with brief descriptions:

_IDT_DESCRIPTOR	5
_IDTR	6
_KGDENTRY	7
_KIDENTRY	7
_KPCR	8
READ_KERN_MEM_s	9

Chapter 2

File Index

2.1 File List

Here is a list of all files with brief descriptions:

common/common/ common.h	11
oark_driver/oark_driver/ buildnumber.h	14
oark_driver/oark_driver/ drvcommon.h	14
oark_driver/oark_driver/ drvversion.h	15
oark_driver/oark_driver/ makefile.inc	16
oark_driver/oark_driver/ oark_driver.cpp	16
oark_driver/oark_driver/ oark_driver.h	17
oark_usermode/oark_usermode/ debug.c	18
oark_usermode/oark_usermode/ debug.h	19
oark_usermode/oark_usermode/ driverusr.c	19
oark_usermode/oark_usermode/ driverusr.h	20
oark_usermode/oark_usermode/ idt.c	20
oark_usermode/oark_usermode/ idt.h	21
oark_usermode/oark_usermode/ main.c	22
oark_usermode/oark_usermode/ others.c	22
oark_usermode/oark_usermode/ others.h	23
oark_usermode/oark_usermode/ pebhooking.c	24
oark_usermode/oark_usermode/ pebhooking.h	24
oark_usermode/oark_usermode/ resource.h	24

Chapter 3

Data Structure Documentation

3.1 _IDT_DESCRIPTOR Struct Reference

```
#include <common.h>
```

Data Fields

- WORD [offset00_15](#)
- WORD [selector](#)
- BYTE [unused](#):5
- BYTE [zeroes](#):3
- BYTE [gateType](#):5
- BYTE [DPL](#):2
- BYTE [P](#):1
- WORD [offset16_31](#)

3.1.1 Field Documentation

3.1.1.1 BYTE DPL

3.1.1.2 BYTE gateType

3.1.1.3 WORD offset00_15

3.1.1.4 WORD offset16_31

3.1.1.5 BYTE P

3.1.1.6 WORD selector

3.1.1.7 BYTE unused

3.1.1.8 BYTE zeroes

The documentation for this struct was generated from the following file:

- common/common/[common.h](#)

3.2 _IDTR Struct Reference

```
#include <common.h>
```

Data Fields

- WORD [nBytes](#)
- WORD [baseAddressLow](#)
- WORD [baseAddressHi](#)

3.2.1 Field Documentation

3.2.1.1 WORD baseAddressHi

3.2.1.2 WORD baseAddressLow

3.2.1.3 WORD nBytes

The documentation for this struct was generated from the following file:

- common/common/[common.h](#)

3.3 _KGDTENTRY Struct Reference

```
#include <idt.h>
```

Data Fields

- WORD [LimitLow](#)
- WORD [BaseLow](#)
- ULONG [HighWord](#)

3.3.1 Field Documentation

3.3.1.1 WORD BaseLow

3.3.1.2 ULONG HighWord

3.3.1.3 WORD LimitLow

The documentation for this struct was generated from the following file:

- [oark_usermode/oark_usermode/idt.h](#)

3.4 _KIDTENTRY Struct Reference

```
#include <idt.h>
```

Data Fields

- WORD [Offset](#)
- WORD [Selector](#)
- WORD [Access](#)
- WORD [ExtendedOffset](#)

3.4.1 Field Documentation

3.4.1.1 WORD Access

3.4.1.2 WORD ExtendedOffset

3.4.1.3 WORD Offset

3.4.1.4 WORD Selector

The documentation for this struct was generated from the following file:

- [oark_usermode/oark_usermode/idt.h](#)

3.5 _KPCR Struct Reference

```
#include <idt.h>
```

Data Fields

- NT_TIB [NtTib](#)
- void * [SelfPcr](#)
- void * [Prcb](#)
- UCHAR [Irql](#)
- ULONG [IRR](#)
- ULONG [IrrActive](#)
- ULONG [IDR](#)
- PVOID [KdVersionBlock](#)
- PKIDENTRY [IDT](#)
- PKGDTENTRY [GDT](#)

3.5.1 Field Documentation

3.5.1.1 PKGDTENTRY GDT

3.5.1.2 ULONG IDR

3.5.1.3 PKIDENTRY IDT

3.5.1.4 UCHAR Irql

3.5.1.5 ULONG IRR

3.5.1.6 ULONG IrrActive

3.5.1.7 PVOID KdVersionBlock

3.5.1.8 NT_TIB NtTib

3.5.1.9 void* Prcb

3.5.1.10 void* SelfPcr

The documentation for this struct was generated from the following file:

- [oark_usermode/oark_usermode/idt.h](#)

3.6 READ_KERN_MEM_s Struct Reference

```
#include <common.h>
```

Data Fields

- void * [src_address](#)
- DWORD [size](#)
- [MEM_SYM_TYP_t](#) type
- void * [dst_address](#)

3.6.1 Field Documentation

3.6.1.1 void* [dst_address](#)

3.6.1.2 DWORD [size](#)

3.6.1.3 void* [src_address](#)

3.6.1.4 [MEM_SYM_TYP_t](#) type

The documentation for this struct was generated from the following file:

- common/common/[common.h](#)

Chapter 4

File Documentation

4.1 common/common/common.h File Reference

```
#include <WinDef.h>
```

Data Structures

- struct [READ_KERN_MEM_s](#)
- struct [_IDT_DESCRIPTOR](#)
- struct [_IDTR](#)

Defines

- #define [OARK_VERSION](#) "0.0.1"
- #define [DEVICE_NAME](#) "\\Device\\OARK_DRIVER"
- #define [SYMLINK_NAME](#) "\\DosDevices\\OARK_DRIVER"
- #define [NAMEOF_DEVICE](#) "\\\\.\\OARK_DRIVER"
- #define [DRIVER_NAME](#) "OARK_DRIVER.SYS"
- #define [SERVICE_NAME](#) "OARK_DRIVER"
- #define [OARK_IOCTL_CHANGE_MODE](#) CTL_CODE(FILE_DEVICE_UNKNOWN, 0x801, METHOD_OUT_DIRECT, FILE_READ_DATA | FILE_WRITE_DATA)
- #define [IDT_HARDCODE_SIZE](#) 0x7FF
- #define [MAKEDWORD](#)(a, b) (((unsigned int)((((WORD)(a)) | (((WORD)((WORD)(b))) << 16)))

Typedefs

- typedef enum [STATUS_e](#) [STATUS_t](#)
- typedef enum [MEM_SYM_TYP_e](#) [MEM_SYM_TYP_t](#)
- typedef struct [READ_KERN_MEM_s](#) [READ_KERN_MEM_t](#)

- typedef struct [_IDT_DESCRIPTOR](#) IDT_DESCRIPTOR
- typedef struct [_IDT_DESCRIPTOR](#) * PIDT_DESCRIPTOR
- typedef struct [_IDTR](#) IDTR

Enumerations

- enum [STATUS_e](#) { [ST_ERROR](#) = 0, [ST_OK](#) }
- enum [MEM_SYM_TYP_e](#) { [SYM_TYP_NULL](#) = 0, [SYM_TYP_KPCR](#), [SYM_TYP_IDT](#) }

4.1.1 Define Documentation

4.1.1.1 `#define DEVICE_NAME "\\Device\\OARK_DRIVER"`

4.1.1.2 `#define DRIVER_NAME "OARK_DRIVER.SYS"`

4.1.1.3 `#define IDT_HARDCODE_SIZE 0x7FF`

4.1.1.4 `#define MAKEDWORD(a, b) ((unsigned int)((((WORD)(a)) | ((WORD)((WORD)(b))) << 16))`

4.1.1.5 `#define NAMEOF_DEVICE "\\\\.\\OARK_DRIVER"`

4.1.1.6 `#define OARK_IOCTL_CHANGE_MODE CTL_CODE(FILE_DEVICE_UNKNOWN, 0x801, METHOD_OUT_DIRECT, FILE_READ_DATA | FILE_WRITE_DATA)`

4.1.1.7 `#define OARK_VERSION "0.0.1"`

4.1.1.8 `#define SERVICE_NAME "OARK_DRIVER"`

4.1.1.9 `#define SYMLINK_NAME "\\DosDevices\\OARK_DRIVER"`

4.1.2 Typedef Documentation

4.1.2.1 `typedef struct _IDT_DESCRIPTOR IDT_DESCRIPTOR`

4.1.2.2 `typedef struct _IDTR IDTR`

4.1.2.3 `typedef enum MEM_SYM_TYP_e MEM_SYM_TYP_t`

4.1.2.4 `typedef struct _IDT_DESCRIPTOR * PIDT_DESCRIPTOR`

4.1.2.5 `typedef struct READ_KERN_MEM_s READ_KERN_MEM_t`

4.1.2.6 `typedef enum STATUS_e STATUS_t`

4.1.3 Enumeration Type Documentation

4.1.3.1 `enum MEM_SYM_TYP_e`

Enumerator:

`SYM_TYP_NULL`

`SYM_TYP_KPCR`

`SYM_TYP_IDT`

4.1.3.2 enum STATUS_e

Enumerator:

ST_ERROR

ST_OK

4.2 oark_driver/oark_driver/buildnumber.h File Reference

Defines

- #define [_FILE_VERSION_BUILD](#) 47

4.2.1 Define Documentation

4.2.1.1 #define [_FILE_VERSION_BUILD](#) 47

4.3 oark_driver/oark_driver/drvcommon.h File Reference

Defines

- #define [_ANSISTRING](#)(text) #text
- #define [ANSISTRING](#)(text) [_ANSISTRING](#)(text)
- #define [_WIDESTRING](#)(text) L##text
- #define [WIDESTRING](#)(text) [_WIDESTRING](#)(text)
- #define [PRESET_UNICODE_STRING](#)(symbol, buffer)
- #define [CREATE_XVER](#)(maj, min, build) maj ## , ## min ## , 0, ## build
- #define [CREATE_FVER](#)(maj, min, build) maj ## . ## min ## .0. ## build
- #define [CREATE_PVER](#)(maj, min, build) maj ## . ## min
- #define [DebugPrint](#) /###/DbgPrint

4.3.1 Define Documentation

4.3.1.1 #define [_ANSISTRING](#)(text) #text

Copyright (c) 2010 - <company name="" here>="">

Useful macros

(File was in the PUBLIC DOMAIN - Created by: ddkwizard\assarbad\ .net)

4.3.1.2 `#define _WIDESTRING(text) L##text`

4.3.1.3 `#define ANSISTRING(text) _ANSISTRING(text)`

4.3.1.4 `#define CREATE_FVER(maj, min, build) maj ## . ## min ## .0. ## build`

4.3.1.5 `#define CREATE_PVER(maj, min, build) maj ## . ## min`

4.3.1.6 `#define CREATE_XVER(maj, min, build) maj ## , ## min ## , 0, ## build`

4.3.1.7 `#define DebugPrint /##/DbgPrint`

4.3.1.8 `#define PRESET_UNICODE_STRING(symbol, buffer)`

Value:

```

UNICODE_STRING symbol = \
    { \
        sizeof(WIDESTRING(buffer)) - sizeof(WCHAR), \
        sizeof(WIDESTRING(buffer)), \
        WIDESTRING(buffer) \
    };

```

4.3.1.9 `#define WIDESTRING(text) _WIDESTRING(text)`

4.4 oark_driver/oark_driver/drvversion.h File Reference

```
#include "buildnumber.h"
```

Defines

- `#define TEXT_AUTHOR` <author name(s)>
- `#define PRD_MAJVER` 1
- `#define PRD_MINVER` 0
- `#define PRD_BUILD` 0
- `#define FILE_MAJVER` 1
- `#define FILE_MINVER` 0
- `#define FILE_BUILD_FILE_VERSION_BUILD`
- `#define DRV_YEAR` 2010
- `#define TEXT_WEBSITE` <website>
- `#define TEXT_PRODUCTNAME` Supercool driver-based tool
- `#define TEXT_FILEDESC` The driver for the supercool driver-based tool
- `#define TEXT_COMPANY` <company name here>
- `#define TEXT_MODULE` oark_driver
- `#define TEXT_COPYRIGHT` Copyright \xA9 DRV_YEAR TEXT_COMPANY
- `#define TEXT_INTERNALNAME` oark_driver.sys

4.4.1 Define Documentation

4.4.1.1 `#define DRV_YEAR 2010`

4.4.1.2 `#define FILE_BUILD_FILE_VERSION_BUILD`

4.4.1.3 `#define FILE_MAJVER 1`

4.4.1.4 `#define FILE_MINVER 0`

4.4.1.5 `#define PRD_BUILD 0`

4.4.1.6 `#define PRD_MAJVER 1`

4.4.1.7 `#define PRD_MINVER 0`

4.4.1.8 `#define TEXT_AUTHOR <author name(s)>`

Copyright (c) 2010 - <company name="" here>="">

Defines for the version information in the resource file

(File was in the PUBLIC DOMAIN - Created by: ddkwizard\assarbad\.net)

4.4.1.9 `#define TEXT_COMPANY <company name here>`

4.4.1.10 `#define TEXT_COPYRIGHT Copyright \xA9 DRV_YEAR TEXT_COMPANY`

4.4.1.11 `#define TEXT_FILEDESC The driver for the supercool driver-based tool`

4.4.1.12 `#define TEXT_INTERNALNAME oark_driver.sys`

4.4.1.13 `#define TEXT_MODULE oark_driver`

4.4.1.14 `#define TEXT_PRODUCTNAME Supercool driver-based tool`

4.4.1.15 `#define TEXT_WEBSITE <website>`

4.5 oark_driver/oark_driver/makefile.inc File Reference

4.6 oark_driver/oark_driver/oark_driver.cpp File Reference

```
#include <ntddk.h>
#include <string.h>
#include "oark_driver.h"
#include "common.h"
```

Functions

- int [WriteUserMode](#) (void *address, DWORD size, void *data)
- NTSTATUS [OARKDRIVER_DispatchCreateClose](#) (IN PDEVICE_OBJECT DeviceObject, IN PIRP Irp)
- NTSTATUS [OARKDRIVER_DispatchDeviceControl](#) (IN PDEVICE_OBJECT DeviceObject, IN PIRP Irp)
- VOID [OARKDRIVER_DriverUnload](#) (IN PDRIVER_OBJECT DriverObject)
- NTSTATUS [DriverEntry](#) (IN OUT PDRIVER_OBJECT DriverObject, IN PUNICODE_STRING RegistryPath)

Variables

- PDRIVER_OBJECT [pdoGlobalDrvObj](#) = 0

4.6.1 Function Documentation

4.6.1.1 NTSTATUS [DriverEntry](#) (IN OUT PDRIVER_OBJECT *DriverObject*, IN PUNICODE_STRING *RegistryPath*)

4.6.1.2 NTSTATUS [OARKDRIVER_DispatchCreateClose](#) (IN PDEVICE_OBJECT *DeviceObject*, IN PIRP *Irp*)

4.6.1.3 NTSTATUS [OARKDRIVER_DispatchDeviceControl](#) (IN PDEVICE_OBJECT *DeviceObject*, IN PIRP *Irp*)

4.6.1.4 VOID [OARKDRIVER_DriverUnload](#) (IN PDRIVER_OBJECT *DriverObject*)

4.6.1.5 int [WriteUserMode](#) (void * *address*, DWORD *size*, void * *data*)

4.6.2 Variable Documentation

4.6.2.1 PDRIVER_OBJECT [pdoGlobalDrvObj](#) = 0

Copyright (c) 2010 - <company name="" here>="">

Original filename: [oark_driver.cpp](#) Project : oark_driver Date of creation : 2010-11-12

Author(s) : <author name(s)>

Purpose :

Revisions: 0000 [2010-11-12] Initial revision.

4.7 oark_driver/oark_driver/oark_driver.h File Reference

```
#include "drvcommon.h"
```

```
#include "drvversion.h"
```

```
#include "common.h"
```

Defines

- `#define FILE_DEVICE_OARKDRIVER 0x8000`

Functions

- `PRESET_UNICODE_STRING` (usDeviceName, DEVICE_NAME)
- `PRESET_UNICODE_STRING` (usSymlinkName, SYMLINK_NAME)

4.7.1 Define Documentation

4.7.1.1 `#define FILE_DEVICE_OARKDRIVER 0x8000`

4.7.2 Function Documentation

4.7.2.1 `PRESET_UNICODE_STRING (usDeviceName , DEVICE_NAME)`

Copyright (c) 2010 - <company name="" here>="">

Original filename: [oark_driver.h](#) Project : oark_driver Date of creation : <see [oark_driver.cpp](#)> Author(s) : <see [oark_driver.cpp](#)>

Purpose : <see [oark_driver.cpp](#)>

Revisions: <see [oark_driver.cpp](#)>

4.7.2.2 `PRESET_UNICODE_STRING (usSymlinkName , SYMLINK_NAME)`

4.8 oark_usermode/oark_usermode/debug.c File Reference

```
#include "debug.h"
```

Functions

- `STATUS_t EnableDebugPrivilege` (void)

Variables

- `debug` = TRUE

4.8.1 Function Documentation

4.8.1.1 `STATUS_t EnableDebugPrivilege (void)`

4.8.2 Variable Documentation

4.8.2.1 `debug = TRUE`

4.9 oark_usermode/oark_usermode/debug.h File Reference

```
#include <windows.h>
#include <stdio.h>
#include "common.h"
```

Functions

- [STATUS_t EnableDebugPrivilege](#) (void)

Variables

- `BOOL debug`

4.9.1 Function Documentation

4.9.1.1 `STATUS_t EnableDebugPrivilege (void)`

4.9.2 Variable Documentation

4.9.2.1 `BOOL debug`

4.10 oark_usermode/oark_usermode/driverusr.c File Reference

```
#include "driverusr.h"
```

Functions

- `void * IOCTLReadKernMem` (HANDLE device, [READ_KERN_MEM_t](#) *read_kern_mem)
- `BOOLEAN LoadDriver` (HANDLE *device)
- `int UnloadDriver` (HANDLE *device)

4.10.1 Function Documentation

4.10.1.1 void* IOCTLReadKernMem (HANDLE device, READ_KERN_MEM_t * read_kern_mem)

4.10.1.2 BOOLEAN LoadDriver (HANDLE * device)

4.10.1.3 int UnloadDriver (HANDLE * device)

4.11 oark_usermode/oark_usermode/driverusr.h File Reference

```
#include <stdio.h>
#include <windows.h>
#include "resource.h"
#include "debug.h"
#include "common.h"
#include "others.h"
```

Functions

- void * [IOCTLReadKernMem](#) (HANDLE, [READ_KERN_MEM_t](#) *)
- BOOLEAN [LoadDriver](#) (HANDLE *)
- int [UnloadDriver](#) (HANDLE *)
- BOOLEAN [GetFullTempPath](#) (char **, char *)
- BOOLEAN [DumpRSRC](#) (char *, int, char *)

4.11.1 Function Documentation

4.11.1.1 BOOLEAN DumpRSRC (char *, int , char *)

4.11.1.2 BOOLEAN GetFullTempPath (char **, char *)

4.11.1.3 void* IOCTLReadKernMem (HANDLE , READ_KERN_MEM_t *)

4.11.1.4 BOOLEAN LoadDriver (HANDLE *)

4.11.1.5 int UnloadDriver (HANDLE *)

4.12 oark_usermode/oark_usermode/idt.c File Reference

```
#include "idt.h"
```

Functions

- int [idt](#) (HANDLE device)

4.12.1 Function Documentation

4.12.1.1 int idt (HANDLE device)

4.13 oark_usermode/oark_usermode/idt.h File Reference

```
#include <windows.h>
#include <stdio.h>
#include "common.h"
#include "driverusr.h"
```

Data Structures

- struct [_KIDTENTRY](#)
- struct [_KGDENTRY](#)
- struct [_KPCR](#)

Typedefs

- typedef struct [_KIDTENTRY](#) KIDTENTRY
- typedef struct [_KIDTENTRY](#) * PKIDTENTRY
- typedef struct [_KGDENTRY](#) KGDENTRY
- typedef struct [_KGDENTRY](#) * PKGDENTRY
- typedef struct [_KPCR](#) KPCR
- typedef struct [_KPCR](#) * PKPCR

Functions

- int [idt](#) (HANDLE)

4.13.1 Typedef Documentation

4.13.1.1 `typedef struct _KGDENTRY KGDENTRY`

4.13.1.2 `typedef struct _KIDENTRY KIDENTRY`

4.13.1.3 `typedef struct _KPCR KPCR`

4.13.1.4 `typedef struct _KGDENTRY * PKGDENTRY`

4.13.1.5 `typedef struct _KIDENTRY * PKIDENTRY`

4.13.1.6 `typedef struct _KPCR * PKPCR`

4.13.2 Function Documentation

4.13.2.1 `int idt (HANDLE)`

4.14 oark_usermode/oark_usermode/main.c File Reference

```
#include <stdio.h>
#include <windows.h>
#include "debug.h"
#include "common.h"
#include "driverusr.h"
#include "idt.h"
#include "others.h"
```

Functions

- `int main (void)`

4.14.1 Function Documentation

4.14.1.1 `int main (void)`

4.15 oark_usermode/oark_usermode/others.c File Reference

```
#include "others.h"
```

Functions

- [STATUS_t LockInstance](#) (DWORD *other_pid)
- BOOLEAN [GetFullTempPath](#) (char **out_full_temp_path, char *name)
- BOOLEAN [DumpRSRC](#) (char *full_temp_path, int resource_id, char *driver_name)

4.15.1 Function Documentation

4.15.1.1 **BOOLEAN DumpRSRC (char * *full_temp_path*, int *resource_id*, char * *driver_name*)**

4.15.1.2 **BOOLEAN GetFullTempPath (char ** *out_full_temp_path*, char * *name*)**

4.15.1.3 **STATUS_t LockInstance (DWORD * *other_pid*)**

4.16 oark_usermode/oark_usermode/others.h File Reference

```
#include <windows.h>
#include <tlhelp32.h>
#include "common.h"
#include "debug.h"
```

Defines

- #define [__OTHERS_H__](#)

Functions

- [STATUS_t LockInstance](#) (DWORD *)
- BOOLEAN [DumpRSRC](#) (char *, int, char *)
- BOOLEAN [GetFullTempPath](#) (char **, char *)

4.16.1 Define Documentation

4.16.1.1 `#define __OTHERS_H__`

4.16.2 Function Documentation

4.16.2.1 `BOOLEAN DumpRSRC (char *, int , char *)`

4.16.2.2 `BOOLEAN GetFullTempPath (char **, char *)`

4.16.2.3 `STATUS_t LockInstance (DWORD *)`

4.17 oark_usermode/oark_usermode/pebhooking.c File Reference

```
#include "pebhooking.h"
```

4.18 oark_usermode/oark_usermode/pebhooking.h File Reference

4.19 oark_usermode/oark_usermode/resource.h File Reference

Defines

- `#define IDR_OARK_DRIVER` 101
- `#define IDI_ICON1` 102

4.19.1 Define Documentation

4.19.1.1 `#define IDI_ICON1` 102

4.19.1.2 `#define IDR_OARK_DRIVER` 101

Index

- [_ANSISTRING](#)
 - [drvcommon.h, 14](#)
- [_FILE_VERSION_BUILD](#)
 - [buildnumber.h, 14](#)
- [_IDTR, 6](#)
 - [baseAddressHi, 6](#)
 - [baseAddressLow, 6](#)
 - [nBytes, 6](#)
- [_IDT_DESCRIPTOR, 5](#)
 - [DPL, 6](#)
 - [gateType, 6](#)
 - [offset00_15, 6](#)
 - [offset16_31, 6](#)
 - [P, 6](#)
 - [selector, 6](#)
 - [unused, 6](#)
 - [zeroes, 6](#)
- [_KGDENTRY, 7](#)
 - [BaseLow, 7](#)
 - [HighWord, 7](#)
 - [LimitLow, 7](#)
- [_KIDENTRY, 7](#)
 - [Access, 7](#)
 - [ExtendedOffset, 7](#)
 - [Offset, 7](#)
 - [Selector, 7](#)
- [_KPCR, 8](#)
 - [GDT, 8](#)
 - [IDR, 8](#)
 - [IDT, 8](#)
 - [Irql, 8](#)
 - [IRR, 8](#)
 - [IrrActive, 8](#)
 - [KdVersionBlock, 8](#)
 - [NtTib, 8](#)
 - [PrCb, 8](#)
 - [SelfPcr, 8](#)
- [_WIDESTRING](#)
 - [drvcommon.h, 14](#)
- [__OTHERS_H__](#)
 - [others.h, 24](#)

- [Access](#)
 - [_KIDENTRY, 7](#)
- [ANSISTRING](#)
 - [drvcommon.h, 15](#)
- [baseAddressHi](#)
 - [_IDTR, 6](#)
- [baseAddressLow](#)
 - [_IDTR, 6](#)
- [BaseLow](#)
 - [_KGDENTRY, 7](#)
- [buildnumber.h](#)
 - [_FILE_VERSION_BUILD, 14](#)
- [common.h](#)
 - [DEVICE_NAME, 13](#)
 - [DRIVER_NAME, 13](#)
 - [IDT_DESCRIPTOR, 13](#)
 - [IDT_HARDCODE_SIZE, 13](#)
 - [IDTR, 13](#)
 - [MAKEDWORD, 13](#)
 - [MEM_SYM_TYP_e, 13](#)
 - [MEM_SYM_TYP_t, 13](#)
 - [NAMEOF_DEVICE, 13](#)
 - [OARK_IOCTL_CHANGE_MODE, 13](#)
 - [OARK_VERSION, 13](#)
 - [PIDT_DESCRIPTOR, 13](#)
 - [READ_KERN_MEM_t, 13](#)
 - [SERVICE_NAME, 13](#)
 - [ST_ERROR, 14](#)
 - [ST_OK, 14](#)
 - [STATUS_e, 13](#)
 - [STATUS_t, 13](#)
 - [SYM_TYP_IDT, 13](#)
 - [SYM_TYP_KPCR, 13](#)
 - [SYM_TYP_NULL, 13](#)
 - [SYMLINK_NAME, 13](#)
- [common/common/common.h, 11](#)
- [CREATE_FVER](#)
 - [drvcommon.h, 15](#)
- [CREATE_PVER](#)

- drvcommon.h, 15
- CREATE_XVER
 - drvcommon.h, 15
- debug
 - debug.c, 19
 - debug.h, 19
- debug.c
 - debug, 19
 - EnableDebugPrivilege, 19
- debug.h
 - debug, 19
 - EnableDebugPrivilege, 19
- DebugPrint
 - drvcommon.h, 15
- DEVICE_NAME
 - common.h, 13
- DPL
 - _IDT_DESCRIPTOR, 6
- DRIVER_NAME
 - common.h, 13
- DriverEntry
 - oark_driver.cpp, 17
- driverusr.c
 - IOCTLReadKernMem, 20
 - LoadDriver, 20
 - UnloadDriver, 20
- driverusr.h
 - DumpRSRC, 20
 - GetFullTempPath, 20
 - IOCTLReadKernMem, 20
 - LoadDriver, 20
 - UnloadDriver, 20
- DRV_YEAR
 - drvversion.h, 16
- drvcommon.h
 - _ANSISTRING, 14
 - _WIDESTRING, 14
 - ANSISTRING, 15
 - CREATE_FVER, 15
 - CREATE_PVER, 15
 - CREATE_XVER, 15
 - DebugPrint, 15
 - PRESET_UNICODE_STRING, 15
 - WIDESTRING, 15
- drvversion.h
 - DRV_YEAR, 16
 - FILE_BUILD, 16
 - FILE_MAJVER, 16
 - FILE_MINVER, 16
- PRD_BUILD, 16
- PRD_MAJVER, 16
- PRD_MINVER, 16
- TEXT_AUTHOR, 16
- TEXT_COMPANY, 16
- TEXT_COPYRIGHT, 16
- TEXT_FILEDESC, 16
- TEXT_INTERNALNAME, 16
- TEXT_MODULE, 16
- TEXT_PRODUCTNAME, 16
- TEXT_WEBSITE, 16
- dst_address
 - READ_KERN_MEM_s, 9
- DumpRSRC
 - driverusr.h, 20
 - others.c, 23
 - others.h, 24
- EnableDebugPrivilege
 - debug.c, 19
 - debug.h, 19
- ExtendedOffset
 - _KIDTENTRY, 7
- FILE_BUILD
 - drvversion.h, 16
- FILE_DEVICE_OARKDRIVER
 - oark_driver.h, 18
- FILE_MAJVER
 - drvversion.h, 16
- FILE_MINVER
 - drvversion.h, 16
- gateType
 - _IDT_DESCRIPTOR, 6
- GDT
 - _KPCR, 8
- GetFullTempPath
 - driverusr.h, 20
 - others.c, 23
 - others.h, 24
- HighWord
 - _KGDTENTRY, 7
- IDI_ICON1
 - resource.h, 24
- IDR
 - _KPCR, 8
- IDR_OARK_DRIVER
 - resource.h, 24

IDT
 _KPCR, 8
 idt
 idt.c, 21
 idt.h, 22
 idt.c
 idt, 21
 idt.h
 idt, 22
 KGDTENTRY, 22
 KIDENTENTRY, 22
 KPCR, 22
 PKGDTENTRY, 22
 PKIDENTENTRY, 22
 PKPCR, 22
 IDT_DESCRIPTOR
 common.h, 13
 IDT_HARDCODE_SIZE
 common.h, 13
 IDTR
 common.h, 13
 IOCTLReadKernMem
 driverusr.c, 20
 driverusr.h, 20
 Irql
 _KPCR, 8
 IRR
 _KPCR, 8
 IrrActive
 _KPCR, 8

 KdVersionBlock
 _KPCR, 8
 KGDTENTRY
 idt.h, 22
 KIDENTENTRY
 idt.h, 22
 KPCR
 idt.h, 22

 LimitLow
 _KGDTENTRY, 7
 LoadDriver
 driverusr.c, 20
 driverusr.h, 20
 LockInstance
 others.c, 23
 others.h, 24

 main
 main.c, 22
 main.c
 main, 22
 MAKEDWORD
 common.h, 13
 MEM_SYM_TYP_e
 common.h, 13
 MEM_SYM_TYP_t
 common.h, 13

 NAMEOF_DEVICE
 common.h, 13
 nBytes
 _IDTR, 6
 NtTib
 _KPCR, 8

 oark_driver.cpp
 DriverEntry, 17
 OARKDRIVER_DispatchCreateClose,
 17
 OARKDRIVER_DispatchDeviceControl,
 17
 OARKDRIVER_DriverUnload, 17
 pdoGlobalDrvObj, 17
 WriteUserMode, 17
 oark_driver.h
 FILE_DEVICE_OARKDRIVER, 18
 PRESET_UNICODE_STRING, 18
 oark_driver/oark_driver/buildnumber.h, 14
 oark_driver/oark_driver/drvcommon.h, 14
 oark_driver/oark_driver/drvversion.h, 15
 oark_driver/oark_driver/makefile.inc, 16
 oark_driver/oark_driver/oark_driver.cpp, 16
 oark_driver/oark_driver/oark_driver.h, 17
 OARK_IOCTL_CHANGE_MODE
 common.h, 13
 oark_usermode/oark_usermode/debug.c, 18
 oark_usermode/oark_usermode/debug.h, 19
 oark_usermode/oark_usermode/driverusr.c,
 19
 oark_usermode/oark_usermode/driverusr.h,
 20
 oark_usermode/oark_usermode/idt.c, 20
 oark_usermode/oark_usermode/idt.h, 21
 oark_usermode/oark_usermode/main.c, 22
 oark_usermode/oark_usermode/others.c, 22
 oark_usermode/oark_usermode/others.h, 23
 oark_usermode/oark_usermode/pebhooking.c,
 24

oark_usermode/oark_usermode/pebhooking.h, oark_driver.h, 18
24

oark_usermode/oark_usermode/resource.h, READ_KERN_MEM_s, 9
24
dst_address, 9
size, 9
src_address, 9
type, 9

OARK_VERSION
common.h, 13

OARKDRIVER_DispatchCreateClose
oark_driver.cpp, 17

OARKDRIVER_DispatchDeviceControl
oark_driver.cpp, 17

OARKDRIVER_DriverUnload
oark_driver.cpp, 17

Offset
_KIDENTENTRY, 7

offset00_15
_IDT_DESCRIPTOR, 6

offset16_31
_IDT_DESCRIPTOR, 6

others.c
DumpRSRC, 23
GetFullTempPath, 23
LockInstance, 23

others.h
__OTHERS_H__, 24
DumpRSRC, 24
GetFullTempPath, 24
LockInstance, 24

P
_IDT_DESCRIPTOR, 6

pdoGlobalDrvObj
oark_driver.cpp, 17

PIDT_DESCRIPTOR
common.h, 13

PKGDTENTRY
idt.h, 22

PKIDENTENTRY
idt.h, 22

PKPCR
idt.h, 22

Prcb
_KPCR, 8

PRD_BUILD
drvversion.h, 16

PRD_MAJVER
drvversion.h, 16

PRD_MINVER
drvversion.h, 16

PRESET_UNICODE_STRING
drvcommon.h, 15

Selector
_KIDENTENTRY, 7

selector
_IDT_DESCRIPTOR, 6

SelfPcr
_KPCR, 8

SERVICE_NAME
common.h, 13

size
READ_KERN_MEM_s, 9

src_address
READ_KERN_MEM_s, 9

ST_ERROR
common.h, 14

ST_OK
common.h, 14

STATUS_e
common.h, 13

STATUS_t
common.h, 13

SYM_TYP_IDT
common.h, 13

SYM_TYP_KPCR
common.h, 13

SYM_TYP_NULL
common.h, 13

SYMLINK_NAME
common.h, 13

TEXT_AUTHOR
drvversion.h, 16

TEXT_COMPANY
drvversion.h, 16

TEXT_COPYRIGHT
drvversion.h, 16

TEXT_FILEDESC
drvversion.h, 16

TEXT_INTERNALNAME
 drvversion.h, [16](#)

TEXT_MODULE
 drvversion.h, [16](#)

TEXT_PRODUCTNAME
 drvversion.h, [16](#)

TEXT_WEBSITE
 drvversion.h, [16](#)

type
 READ_KERN_MEM_s, [9](#)

UnloadDriver
 driverusr.c, [20](#)
 driverusr.h, [20](#)

unused
 _IDT_DESCRIPTOR, [6](#)

WIDESTRING
 drvcommon.h, [15](#)

WriteUserMode
 oark_driver.cpp, [17](#)

zeroes
 _IDT_DESCRIPTOR, [6](#)