

Dependency Walker

Report

Static Malware Analysis Using DependencyWalker

Sakarie Sa'ad Osman (Sap iD:30025)

Riphah International University

Date: 19 May 2024

Table of Contents

Report.....	1
Executive Summary	3
Document Linked Libraries:	3
Libraries and Imports:	4
-Kernel32.DLL.....	5
Imported functions from Kernel32.dll:	5
-User32.DLL:	7
Imported Functions from User32.dll:	7
-Exports:.....	8

Executive Summary

Overview:

DependencyWalker is a free, standalone application for profiling and troubleshooting the dependencies of Windows applications. It helps identify the libraries and functions that an executable or DLL file relies on to run.

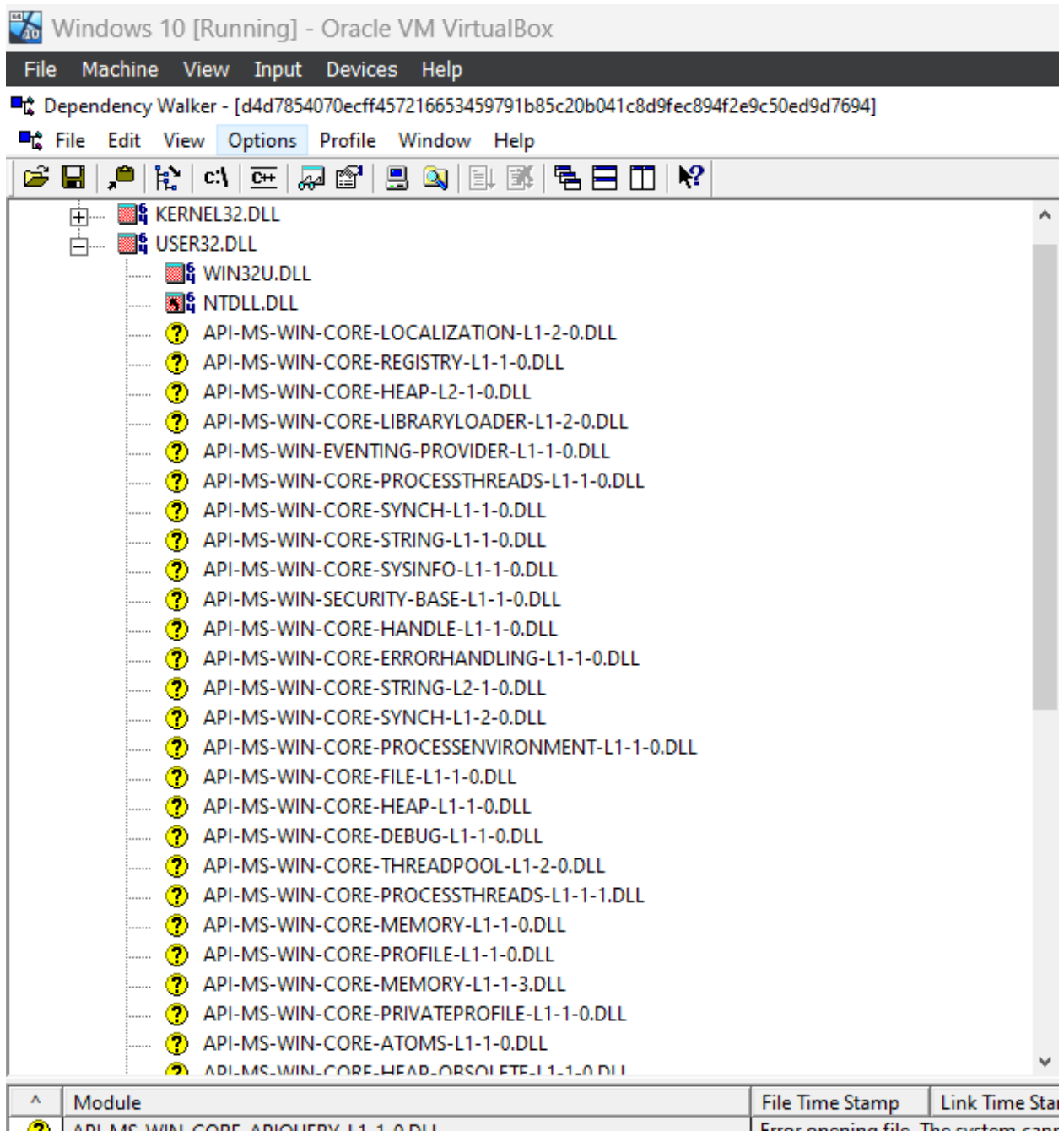
It builds a tree hierarchical tree diagram of all the dependent modules.

Document Linked Libraries:

Libraries:

Dependency Walker

- Kernel32.DLL
- User32.DLL







Libraries and Imports:

These are functions that the DLL calls from other libraries. This means the DLL relies on these functions to operate.

Dependency Walker

-Kernel32.DLL

Kernel32.dll is a core component of the Microsoft Windows operating system. It is a dynamic link library (DLL) that contains functions for managing memory, input/output operations, and various system services. This DLL plays a crucial role in the functionality and stability of the Windows environment.

PI^	Ordinal	Hint	Function	Entry Point
	N/A	0 (0x0000)	LoadLibraryA	Not Bound
	N/A	0 (0x0000)	ExitProcess	Not Bound
	N/A	0 (0x0000)	GetProcAddress	Not Bound
	N/A	0 (0x0000)	VirtualProtect	Not Bound

Imported functions from Kernel32.dll:

1. *LoadLibraryA.*

Description: Loads a specified module into the address space of the calling process. The module can be a .dll or .exe file. This function maps the module into the process's address space and returns a handle to the module.

Usage: Typically used to dynamically load a library at runtime, allowing an application to use functions within the DLL.

2. *ExitProcess.*

Description: Ends a process and all its threads. This function does not return and all pending I/O operations are terminated. It also calls the entry-point function of all attached DLLs with `DLL_PROCESS_DETACH`.

Usage: Used to terminate the calling process.

3. *GetProcAddress.*

Description: Retrieves the address of an exported function or variable from the specified dynamic-link library (DLL). This function is typically used to retrieve the addresses of functions in DLLs that were dynamically loaded using `LoadLibraryA`.

Usage: Used to dynamically call functions in a DLL

4. *VirtualProtect.*

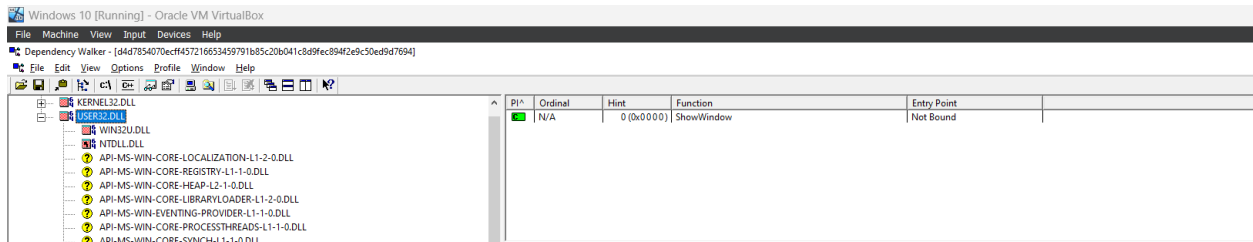
Description: Changes the protection on a region of committed pages in the virtual address space of the calling process. It is used to modify the access protection on memory pages, which can be important for handling executable memory regions.

Usage: Used to change the access protection of memory pages.

Dependency Walker

-User32.DLL:

User32.dll is a crucial component of the Windows operating system. It is a dynamic link library that contains functions related to the Windows user interface, such as window management, user input, and message handling.



Imported Functions from User32.dll:

1. *ShowWindow*:

function is part of the User32.dll in the Windows API and is used to set the specified window's show state. This function is essential for controlling how a window appears and behaves when it is initially created and displayed.

User32.dll Exports:

[illegible]

More functions

Windows 10 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Dependency Walker - [d4d7854070cf4532166534979185C208041C809EC8F4926C50d5f7694]

File Edit View Options Profile Window Help

☒ D4D7854070CF4532166534979185C208041C809EC8F4926C50d5f7694
☒ KERNEL32.DLL
☒ USER32.DLL
☒ WIN32UI.DLL
☒ NTDLL.DLL
☒ API-MS-WIN-CORE-LOCALIZATION-L1-2-0.DLL
☒ API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
☒ API-MS-WIN-CORE-HEAP-L2-1-0.DLL
☒ API-MS-WIN-CORE-LIBRARYLOADER-L1-2-0.DLL
☒ API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
☒ API-MS-WIN-CORE-PROCESS-THREADS-L1-1-0.DLL
☒ API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
☒ API-MS-WIN-CORE-STRING-L1-1-0.DLL
☒ API-MS-WIN-CORE-SYSTEM-L1-1-0.DLL
☒ API-MS-WIN-SECURITY-BASE-L1-1-0.DLL
☒ API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
☒ API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL
☒ API-MS-WIN-CORE-STRINGS-L1-1-0.DLL
☒ API-MS-WIN-CORE-SYNCH-L1-2-0.DLL
☒ API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-1-0.DLL
☒ API-MS-WIN-CORE-FILE-L1-1-0.DLL
☒ API-MS-WIN-CORE-HEAP-L1-1-0.DLL
☒ API-MS-WIN-CORE-DEBUG-L1-1-0.DLL
☒ API-MS-WIN-CORE-THREADPOOL-L1-2-0.DLL
☒ API-MS-WIN-CORE-PROFILER-L1-1-1.DLL
☒ API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
☒ API-MS-WIN-CORE-PROFILE-L1-1-0.DLL
☒ API-MS-WIN-CORE-MEMORY-L1-1-3.DLL
☒ API-MS-WIN-CORE-PRIVATEPROFILE-L1-1-0.DLL
☒ ADVAPI32.dll
☒ ADVAPI32.dll

PI ^a	Ordinal	Hint	Function	Entry Point
	N/A	0 (0x0000)	Show Window	Not Bound

E	Ordinal ^a	Hint	Function	Entry Point
	1681 (0x0691)	173 (0x004D)	DestroyAcceleratorTable	0x00027D80
	1682 (0x0692)	174 (0x004E)	DestroyCaret	0x0002C600
	1683 (0x0693)	175 (0x004F)	DestroyCursor	0x000233F0
	1684 (0x0694)	176 (0x0050)	DestroyCompositionRenderTarget	0x00034110
	1685 (0x0695)	177 (0x0051)	DestroyContext	0x000233F0
	1686 (0x0696)	178 (0x0052)	DestroyMenu	0x00034120
	1687 (0x0697)	179 (0x0053)	DestroyReasons	0x000318A0
	1688 (0x0698)	180 (0x0054)	DestroySyntheticPointerDevice	0x00034130
	1689 (0x0699)	181 (0x0055)	DestroyWindow	0x00034140
	1690 (0x069A)	182 (0x0056)	DialogBoxIndirectParam	0x00051200
	1691 (0x069B)	183 (0x0057)	DialogBoxIndirectParamW	0x00020700
	1692 (0x069C)	184 (0x0058)	DialogBoxIndirectParamW	0x00020700
	1693 (0x069D)	185 (0x0059)	DialogBoxParam	0x00051200
	1694 (0x069E)	186 (0x005A)	DialogBoxParamW	0x00020710
	1695 (0x069F)	187 (0x005B)	DisableProcessInWindowsGhosting	0x00020070
	1696 (0x06A0)	188 (0x005C)	DisplayMessage	0x00028B00
	1697 (0x06A1)	189 (0x005D)	DisplayMessageW	0x00028B00
	1698 (0x06A2)	190 (0x005E)	DisplayConfigDeviceInfo	0x00029CF0
	1699 (0x06A3)	191 (0x005F)	DisplayConfigDeviceInfo	0x00028B10
	1700 (0x06A4)	192 (0x0060)	DisplayConfigDeviceWarnings	0x000534F0
	1701 (0x06A5)	193 (0x0061)	DlgGetList	0x00076380
	1702 (0x06A6)	194 (0x0062)	DlgGetListComboBoxA	0x00054930
	1703 (0x06A7)	195 (0x0063)	DlgGetListComboBoxW	0x00054A20
	1704 (0x06A8)	196 (0x0064)	DlgGetListW	0x00076400
	1705 (0x06A9)	197 (0x0065)	DlgGetSelectComboBoxA	0x00054A80

Module	File Time Stamp	Link Time Stamp	File Size	Attr	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver	Link
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL																	
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL																	
API-MS-WIN-CORE-APIQUERY-L2-1-0.DLL																	

Error opening file. The system cannot find the file specified (2).
 Error opening file. The system cannot find the file specified (2).
 Error opening file. The system cannot find the file specified (2).

The list is long and will not fit these pages as I take these images as short examples.