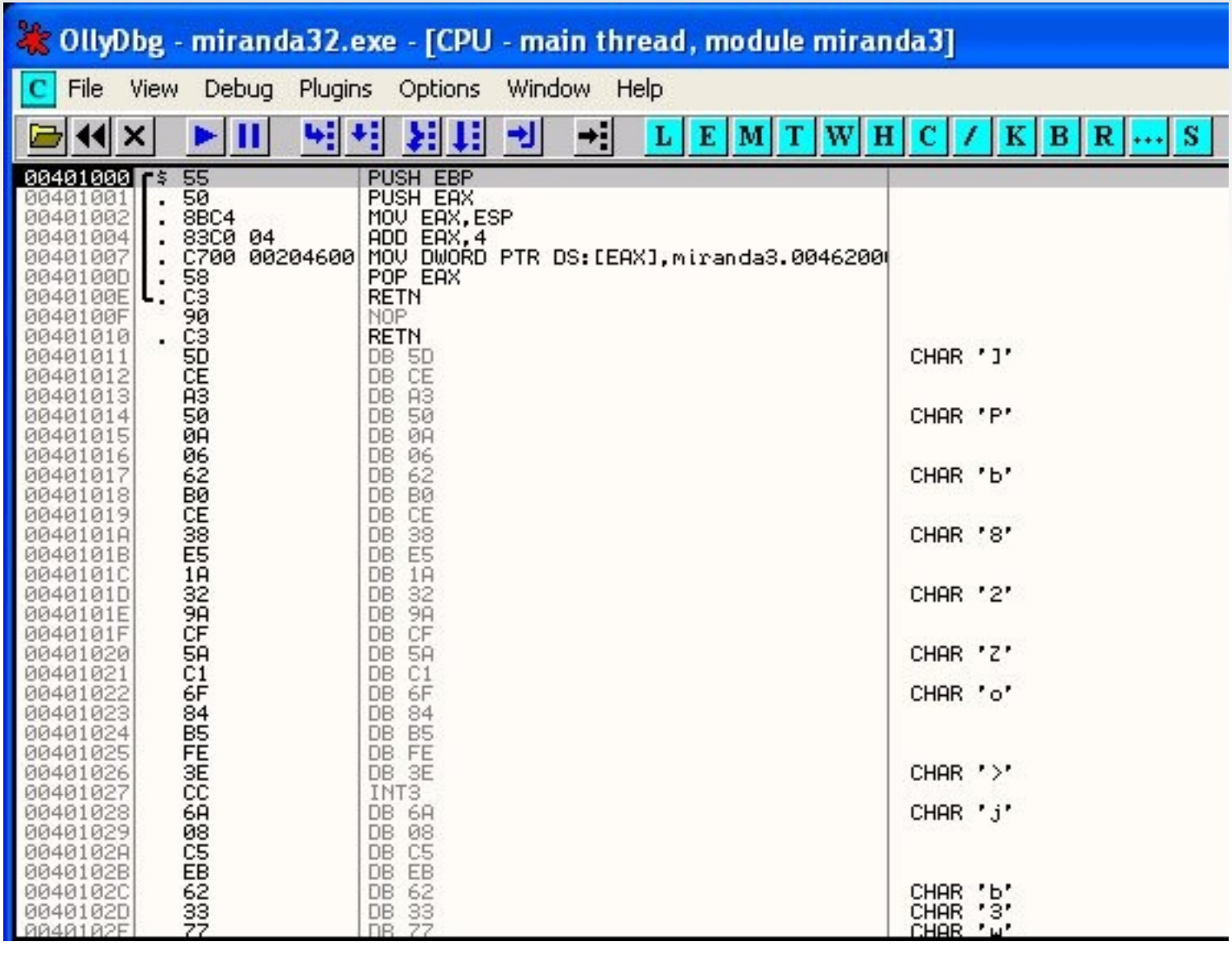
HL2 Hook

- The Program
- The Disassembly
- Other Tools
- Playing Around
- Conclusion

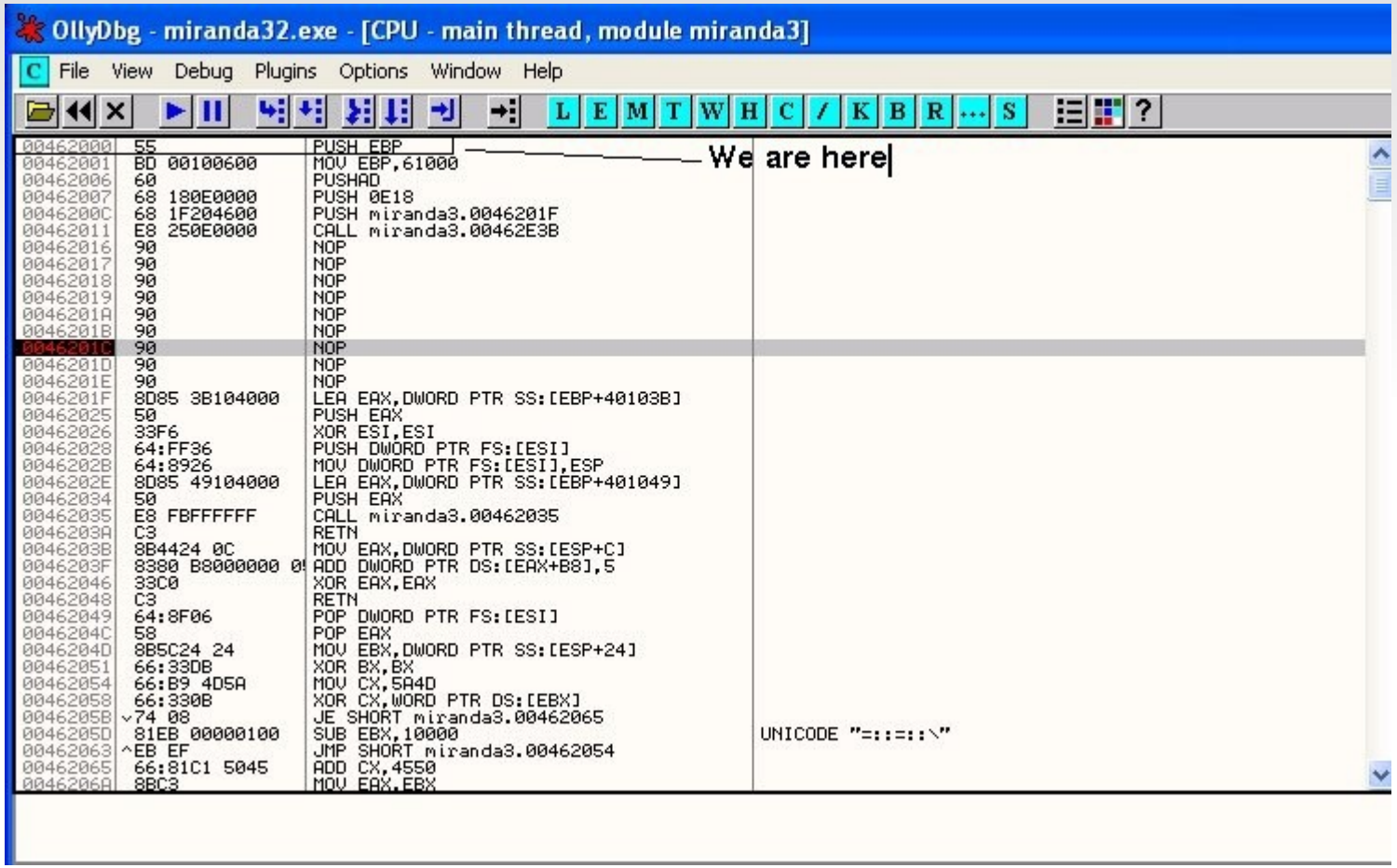
The Program Use Case

- Start the program
- Generates a widget showing it is ready
- Open CS:S
- HL2 Hook does its business and closes

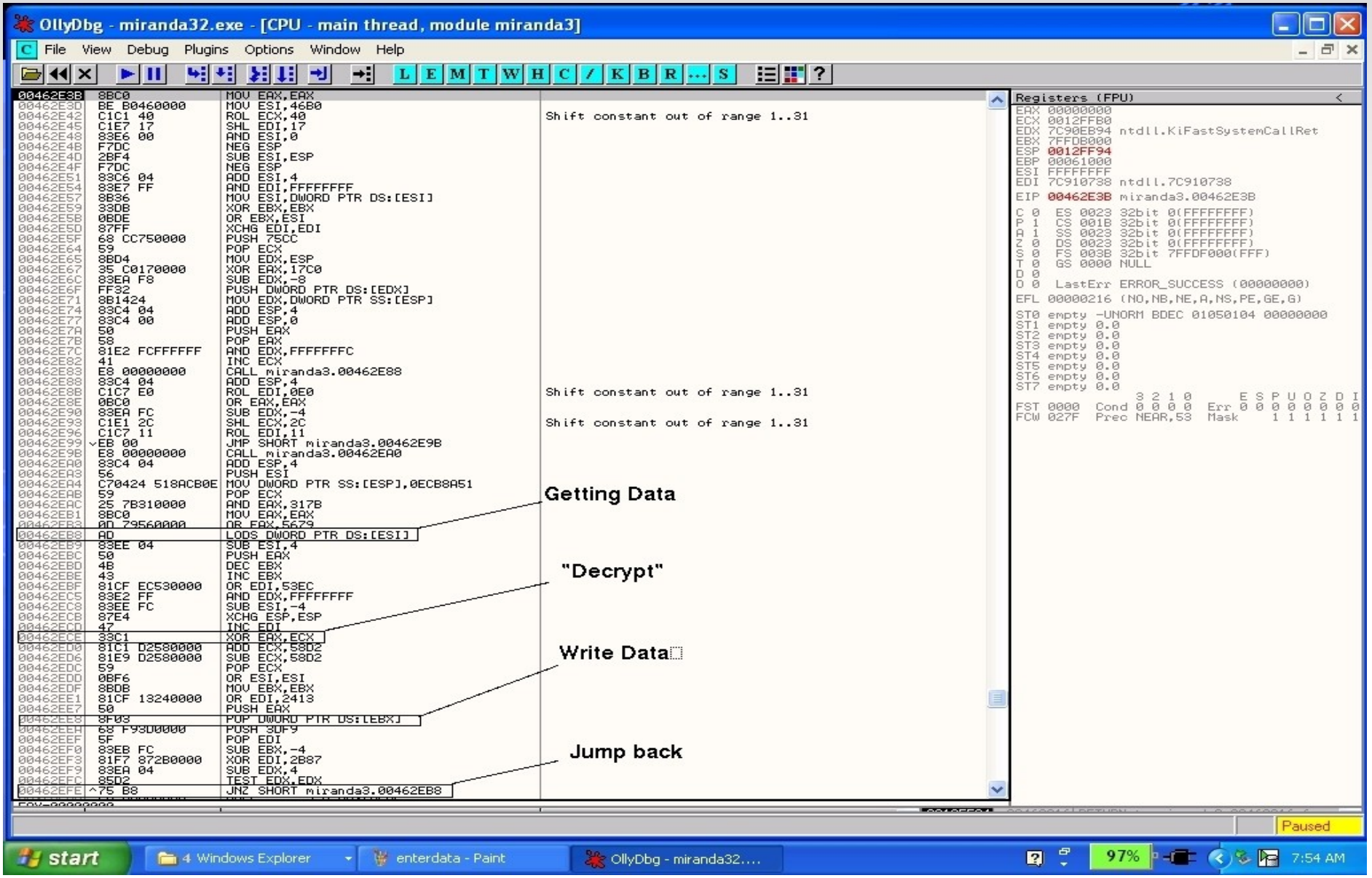
Disassembly, begin!



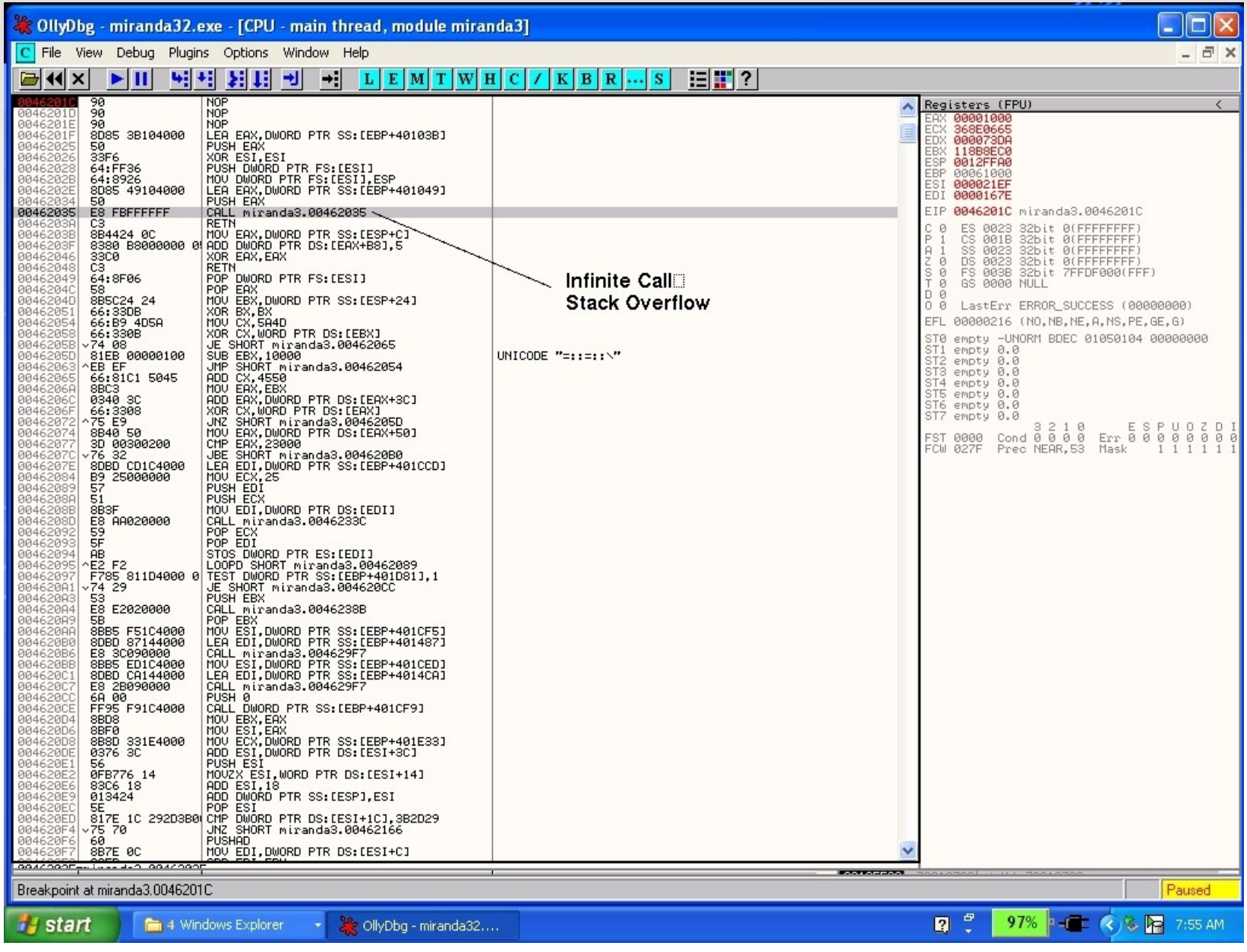
Jump, Leaving Code Section



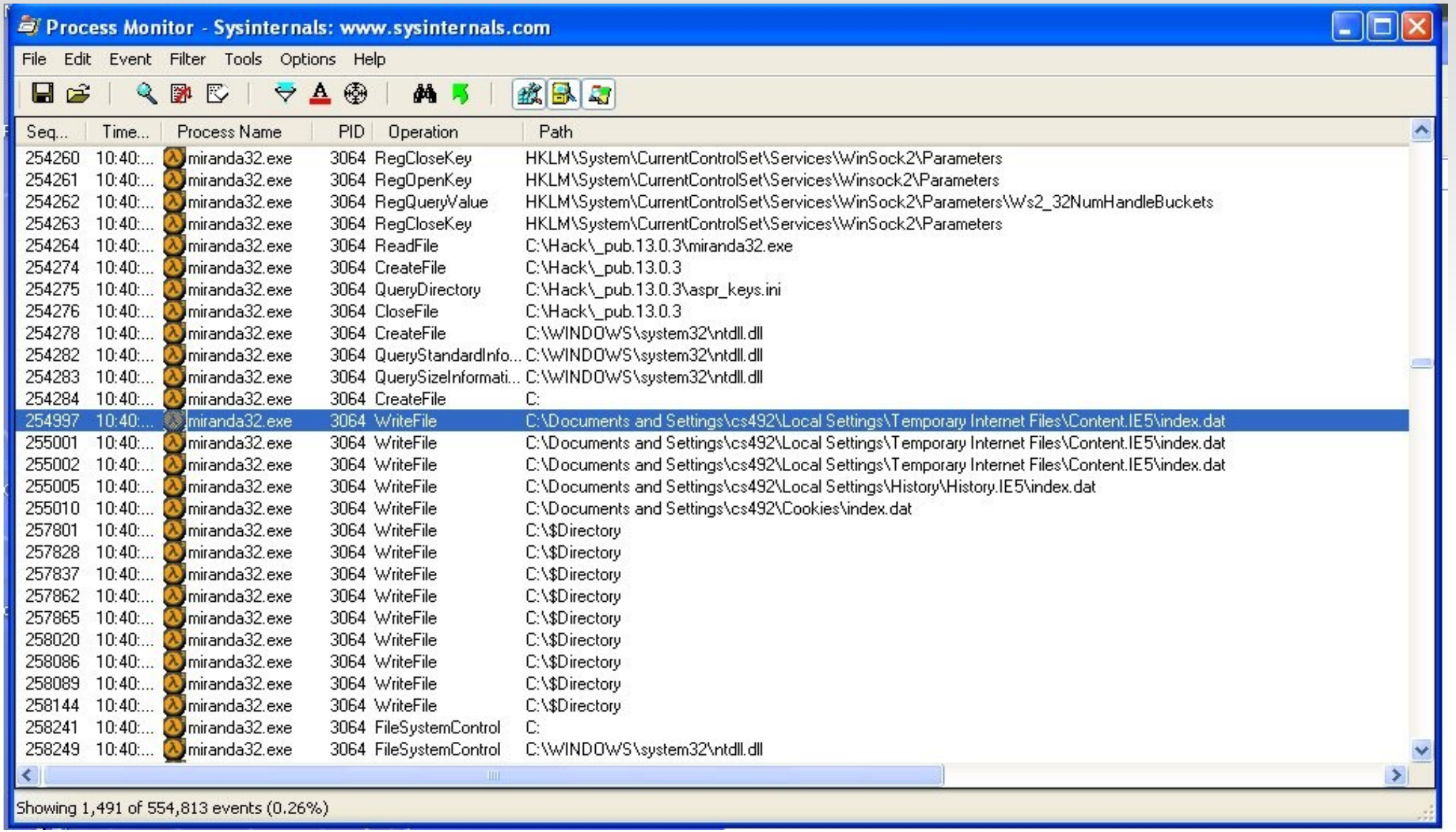
Time to Rewrite



The End, I Give Up

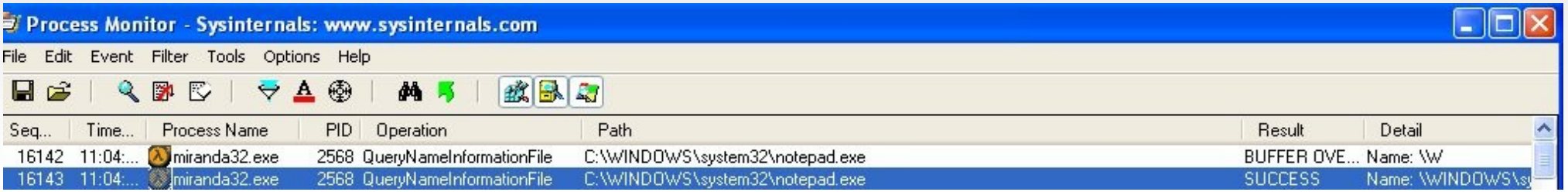


Process Monitor

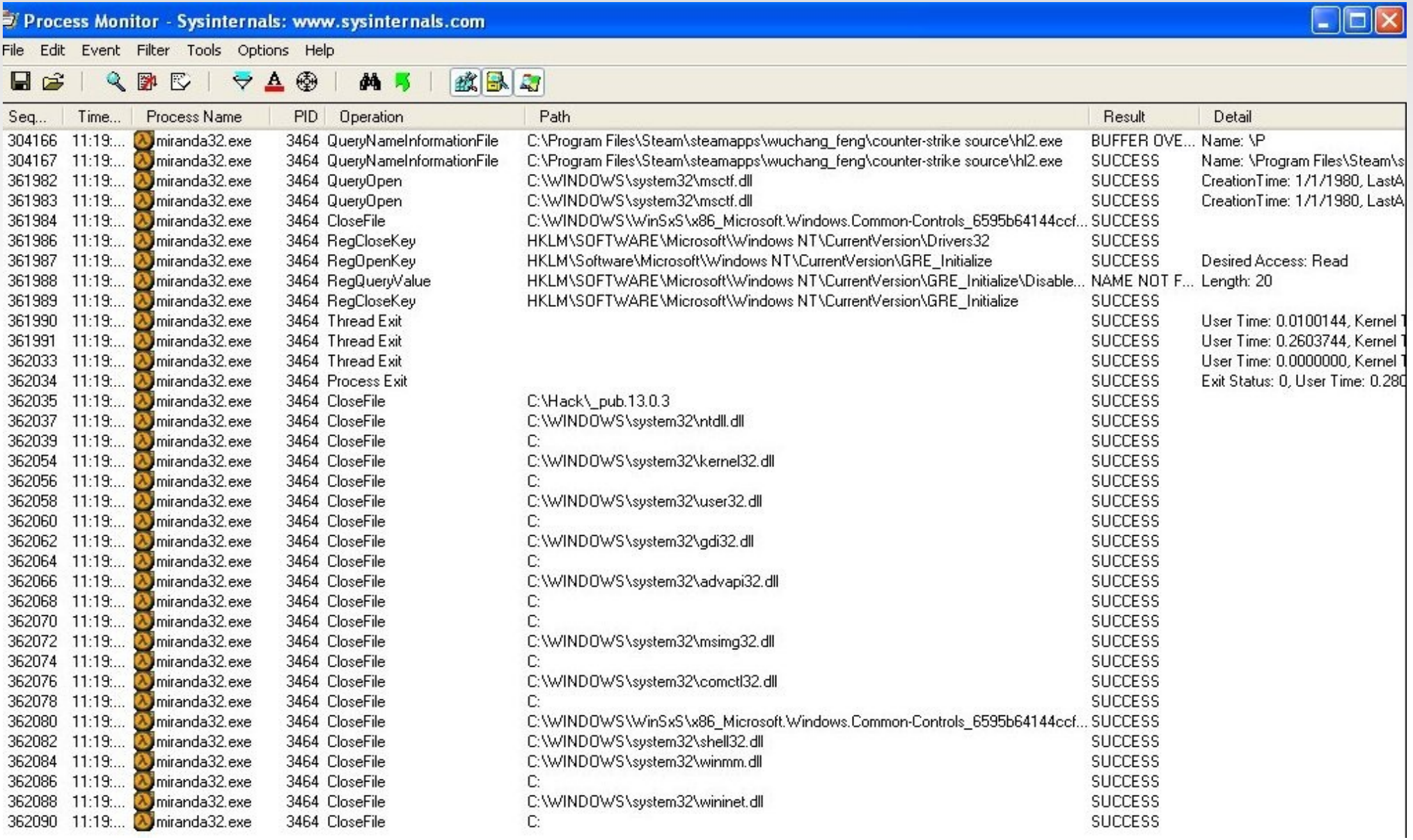


Detecting HL2

- Checks the name/path of all starting programs .exe

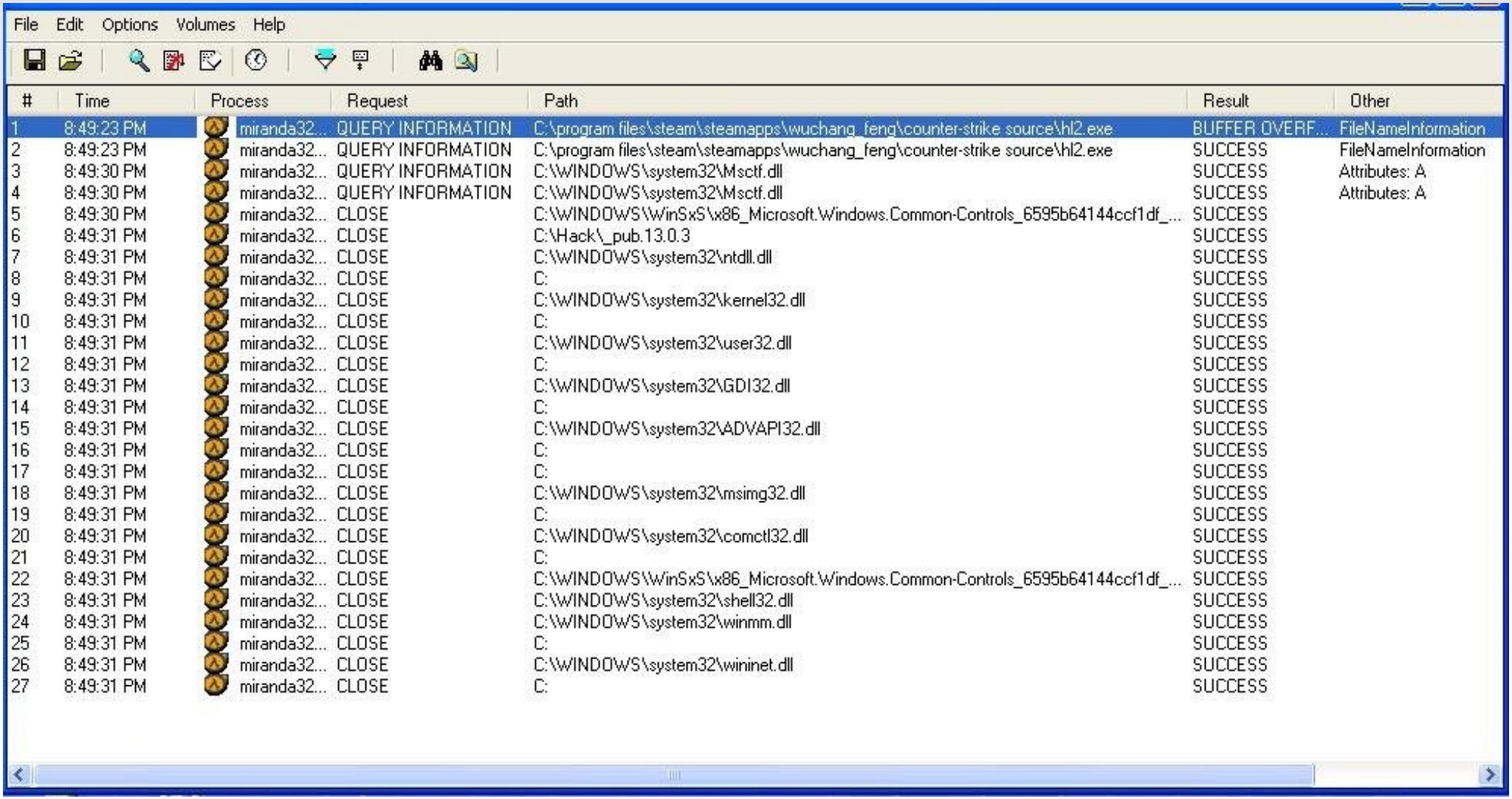


Found it



Seq...	Time...	Process Name	PID	Operation	Path	Result	Detail
304166	11:19:...	miranda32.exe	3464	QueryNameInformationFile	C:\Program Files\Steam\steamapps\wuchang_feng\counter-strike source\hl2.exe	BUFFER OVE...	Name: \P
304167	11:19:...	miranda32.exe	3464	QueryNameInformationFile	C:\Program Files\Steam\steamapps\wuchang_feng\counter-strike source\hl2.exe	SUCCESS	Name: \Program Files\Steam\s
361982	11:19:...	miranda32.exe	3464	QueryOpen	C:\WINDOWS\system32\msctf.dll	SUCCESS	CreationTime: 1/1/1980, LastA
361983	11:19:...	miranda32.exe	3464	QueryOpen	C:\WINDOWS\system32\msctf.dll	SUCCESS	CreationTime: 1/1/1980, LastA
361984	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf...	SUCCESS	
361986	11:19:...	miranda32.exe	3464	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32	SUCCESS	
361987	11:19:...	miranda32.exe	3464	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: Read
361988	11:19:...	miranda32.exe	3464	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\Disable...	NAME NOT F...	Length: 20
361989	11:19:...	miranda32.exe	3464	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	
361990	11:19:...	miranda32.exe	3464	Thread Exit		SUCCESS	User Time: 0.0100144, Kernel T
361991	11:19:...	miranda32.exe	3464	Thread Exit		SUCCESS	User Time: 0.2603744, Kernel T
362033	11:19:...	miranda32.exe	3464	Thread Exit		SUCCESS	User Time: 0.0000000, Kernel T
362034	11:19:...	miranda32.exe	3464	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.280
362035	11:19:...	miranda32.exe	3464	CloseFile	C:\Hack_pub.13.0.3	SUCCESS	
362037	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
362039	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362054	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	
362056	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362058	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\user32.dll	SUCCESS	
362060	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362062	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\gdi32.dll	SUCCESS	
362064	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362066	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	
362068	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362070	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362072	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\msimg32.dll	SUCCESS	
362074	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362076	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\comctl32.dll	SUCCESS	
362078	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362080	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf...	SUCCESS	
362082	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	
362084	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\winmm.dll	SUCCESS	
362086	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	
362088	11:19:...	miranda32.exe	3464	CloseFile	C:\WINDOWS\system32\wininet.dll	SUCCESS	
362090	11:19:...	miranda32.exe	3464	CloseFile	C:	SUCCESS	

Filemon/Regmon

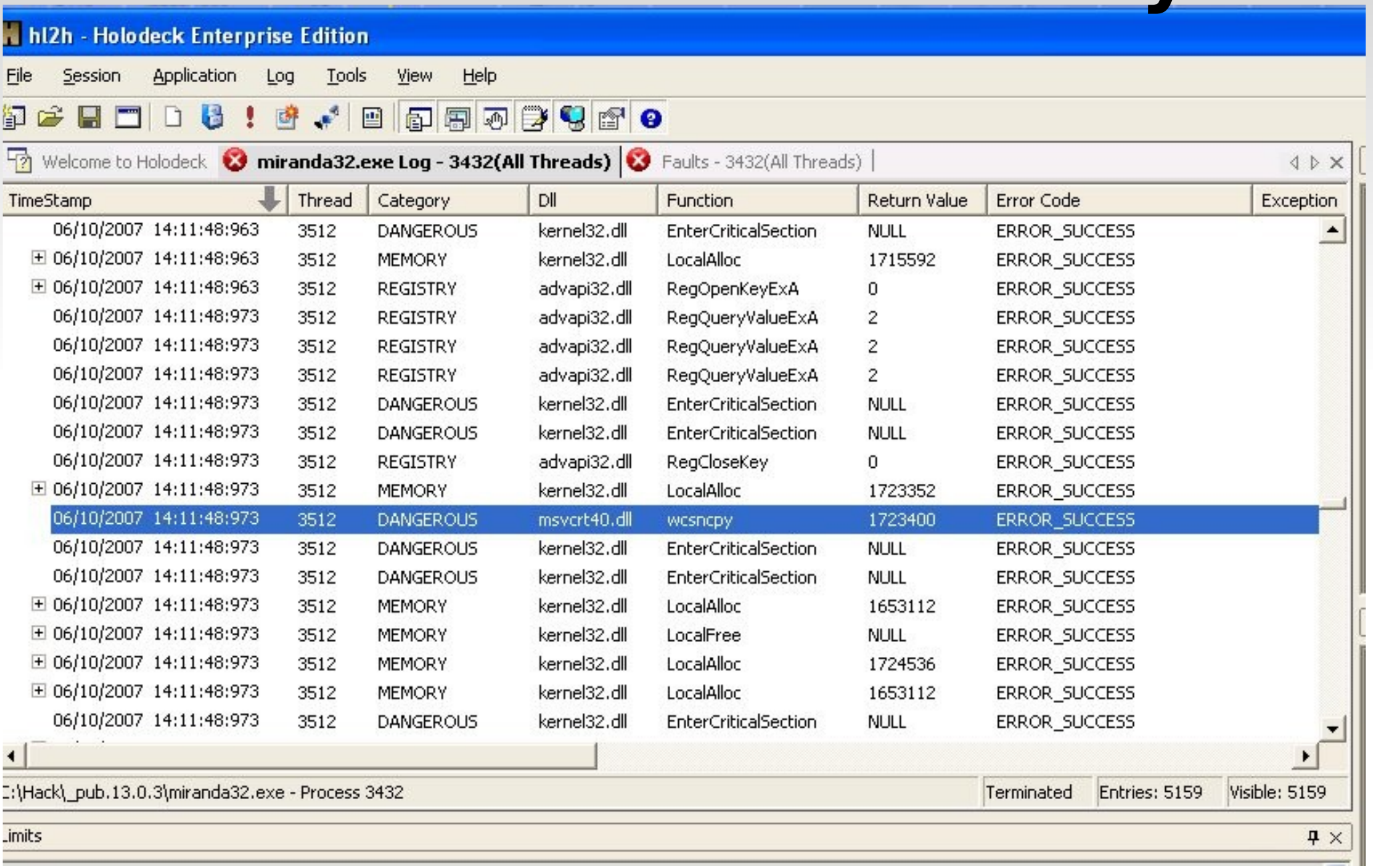


#	Time	Process	Request	Path	Result	Other
1	8:49:23 PM	miranda32...	QUERY INFORMATION	C:\program files\steam\steamapps\wuchang_feng\counter-strike source\hl2.exe	BUFFER OVERF...	FileNameInformation
2	8:49:23 PM	miranda32...	QUERY INFORMATION	C:\program files\steam\steamapps\wuchang_feng\counter-strike source\hl2.exe	SUCCESS	FileNameInformation
3	8:49:30 PM	miranda32...	QUERY INFORMATION	C:\WINDOWS\system32\Msctf.dll	SUCCESS	Attributes: A
4	8:49:30 PM	miranda32...	QUERY INFORMATION	C:\WINDOWS\system32\Msctf.dll	SUCCESS	Attributes: A
5	8:49:30 PM	miranda32...	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_...	SUCCESS	
6	8:49:31 PM	miranda32...	CLOSE	C:\Hack_pub.13.0.3	SUCCESS	
7	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
8	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
9	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\kernel32.dll	SUCCESS	
10	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
11	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\user32.dll	SUCCESS	
12	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
13	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\GDI32.dll	SUCCESS	
14	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
15	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\ADVAPI32.dll	SUCCESS	
16	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
17	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
18	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\msimg32.dll	SUCCESS	
19	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
20	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\comctl32.dll	SUCCESS	
21	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
22	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_...	SUCCESS	
23	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\shell32.dll	SUCCESS	
24	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\winmm.dll	SUCCESS	
25	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	
26	8:49:31 PM	miranda32...	CLOSE	C:\WINDOWS\system32\wininet.dll	SUCCESS	
27	8:49:31 PM	miranda32...	CLOSE	C:	SUCCESS	

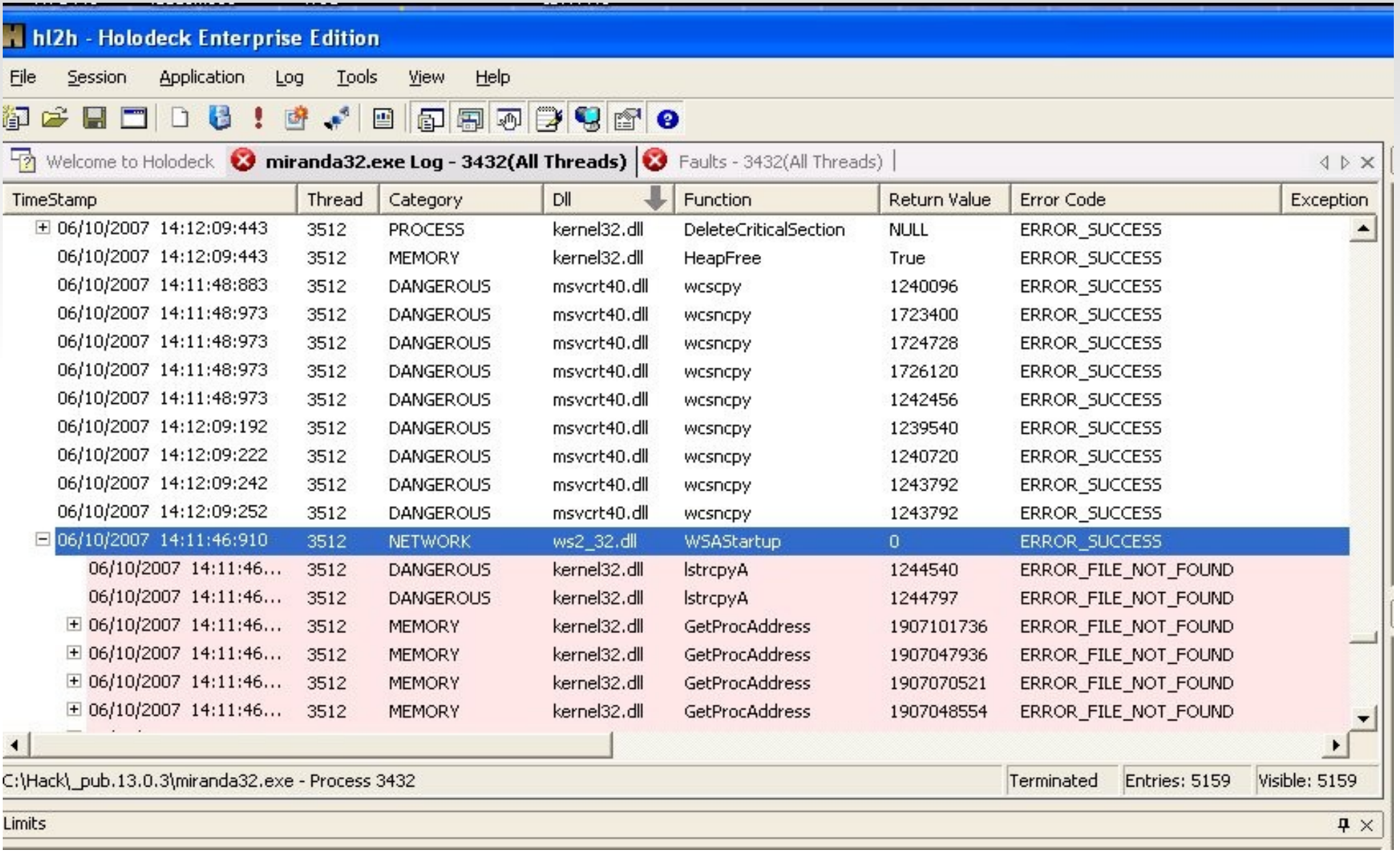
Holodeck


Network Down
Query Buffer Too Small
Protection Error
Debugger detected - please close it down and restart!
Windows NT users: Please note that having the WinIce/SoftIce service installed means that you are running a debugger!
OK
Access Denied

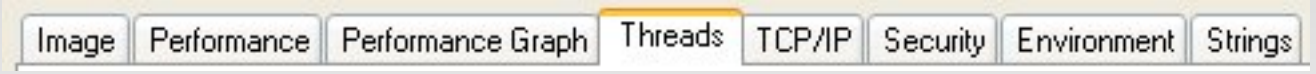
Standard MS C Library



Windows Socket API

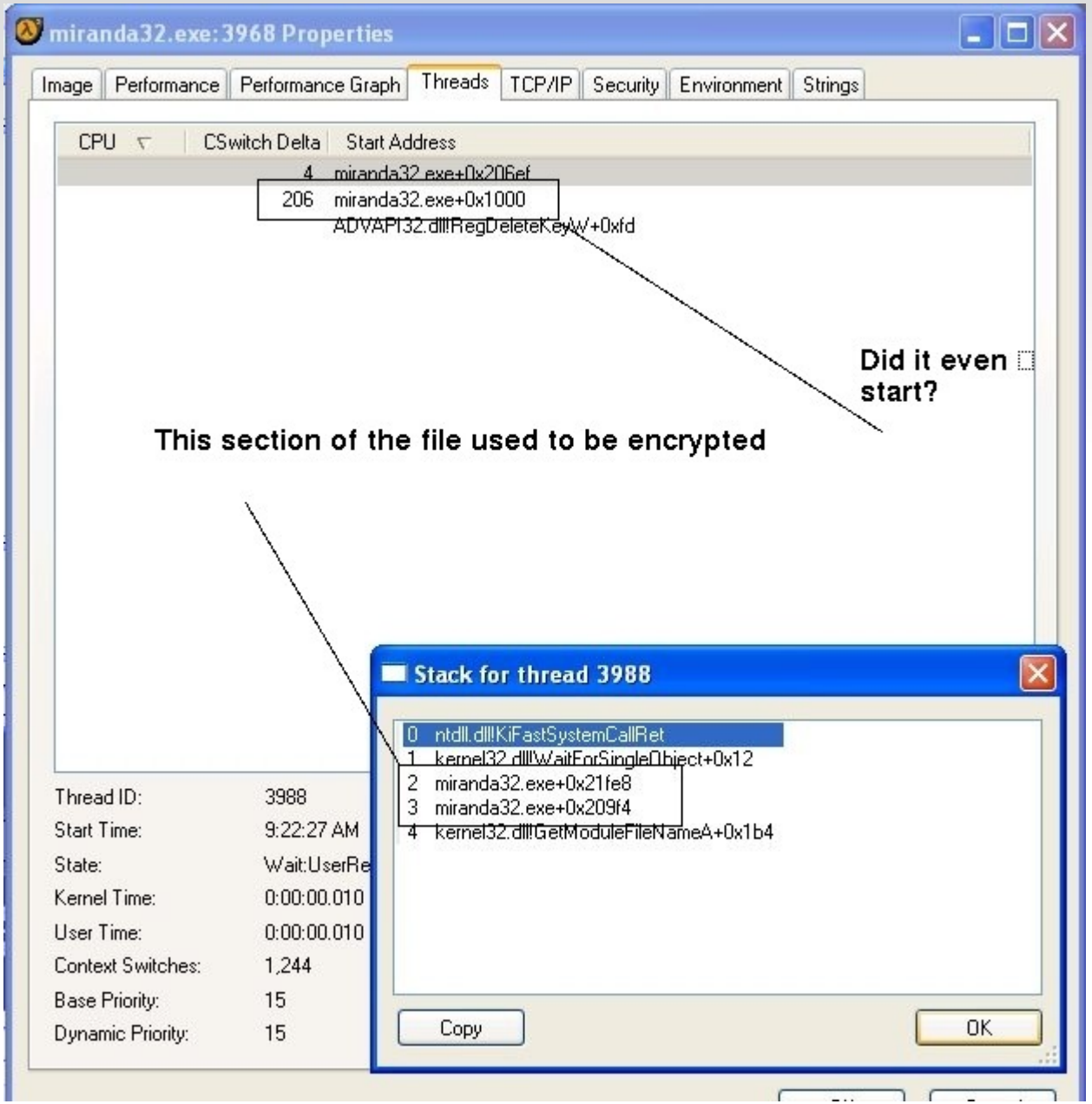


Process Explorer



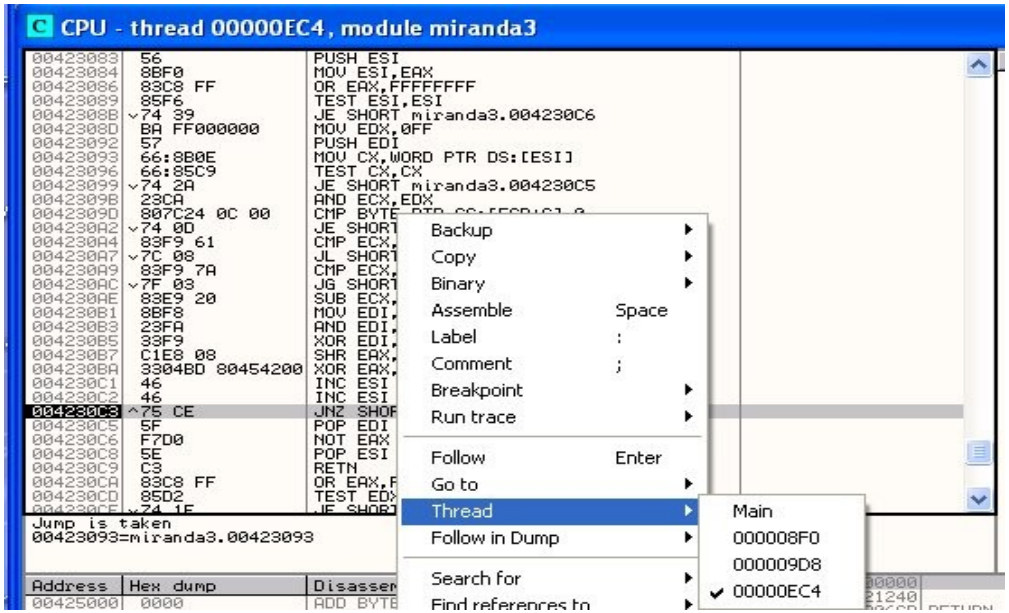
- Another Sysinternals program
- The threads
  - Doesn't appear to create a threat in the game or game launcher
- Nothing useful in strings

Stack During Load



Playing Around

- Post initial load
  - No obvious debugger detection but program will exit stepping through or resuming the process.
  - runs kernel32, user32, ntdll, and other OS modules.



Final

- Stealth
  - Likely not much
  - Named after common application
  - Encryption
- ”Code section” decrypts itself if no debugger present
  - Attatch debugger after program starts and view that section
  - Cannot get program to step through and generate/run it yet
  - Still ”holes” in decrypted code