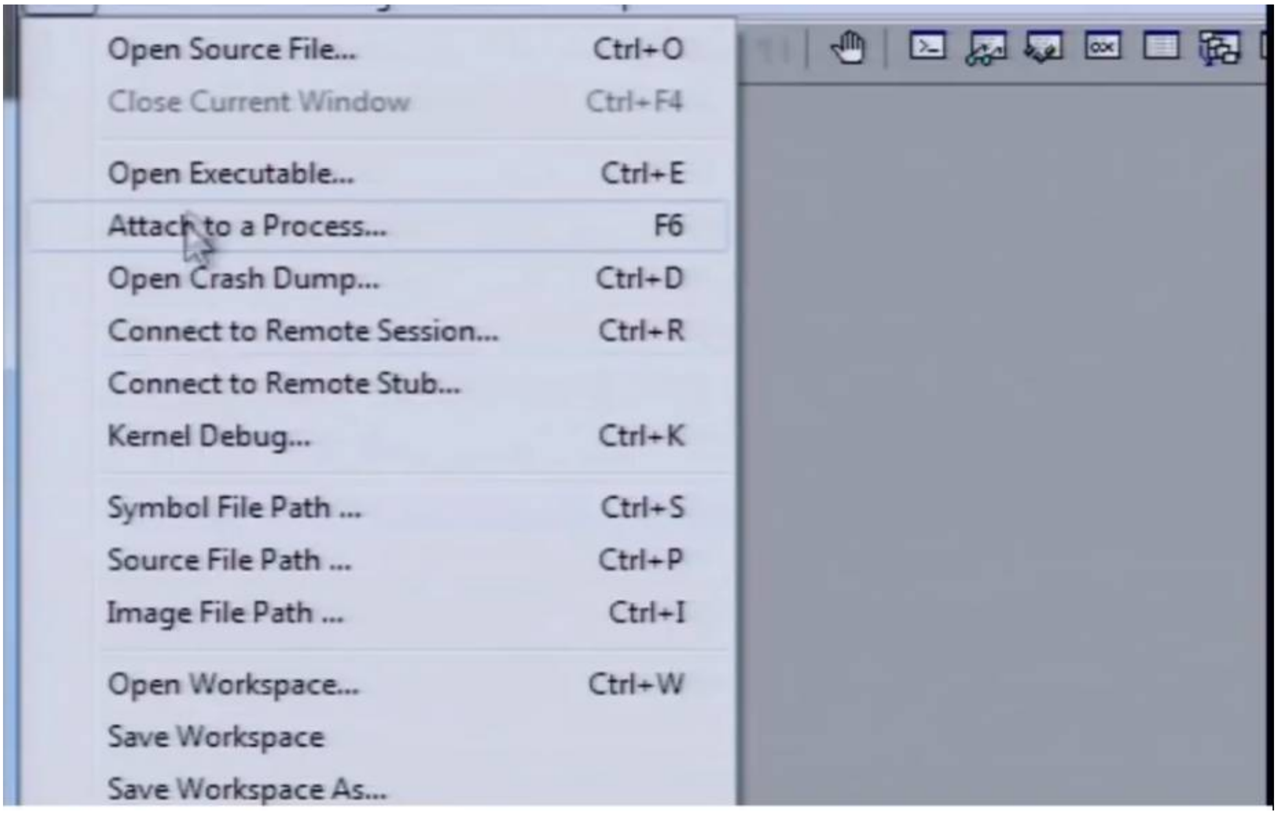
All commands can be insert in a script and can strated when the debugger starts.

Number which is shown left in the Windbg-GUI means the number of thread which has the exception (error)

Attach to a process with WinDBg in a physical machine to show what is going on in there.

Press the folder symbol in the left corner and press the attach to a process menu entree

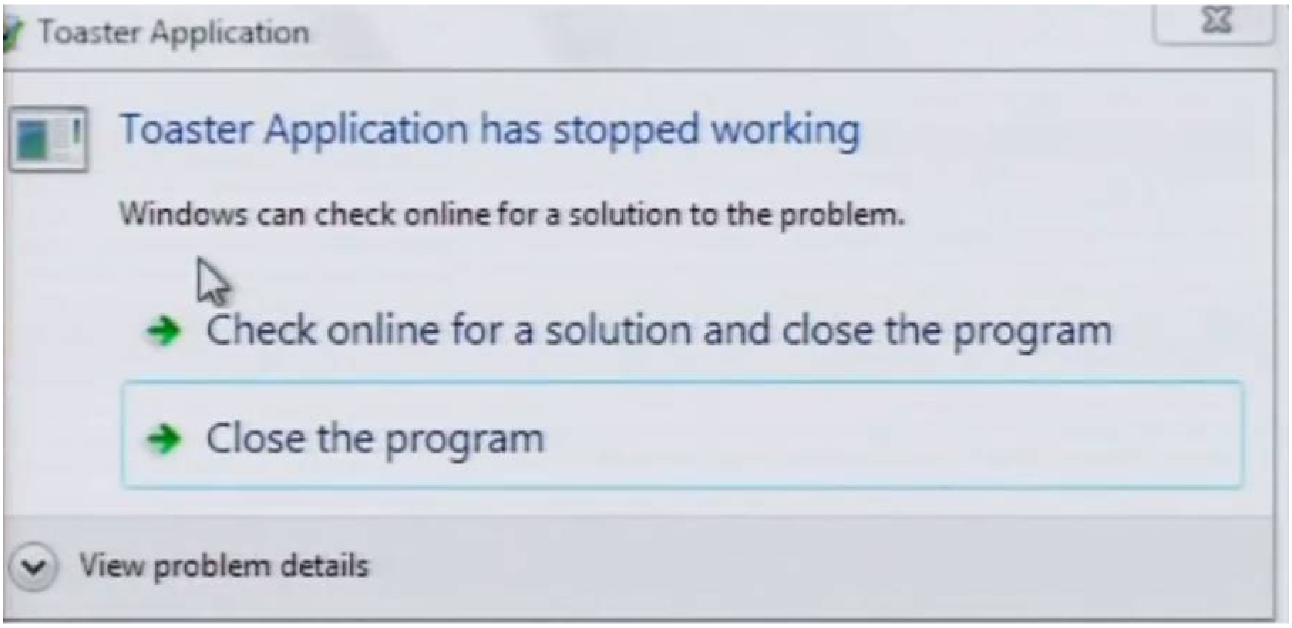
You can short this steps if you press windbg and the program name into the cmd or powershell.


Open Source File... Ctrl+O
Close Current Window Ctrl+F4
Open Executable... Ctrl+E
Attach to a Process... F6
Open Crash Dump... Ctrl+D
Connect to Remote Session... Ctrl+R
Connect to Remote Stub...
Kernel Debug... Ctrl+K
Symbol File Path ... Ctrl+S
Source File Path ... Ctrl+P
Image File Path ... Ctrl+I
Open Workspace... Ctrl+W
Save Workspace
Save Workspace As...

Select the program to which you want to be attached

Additional information:

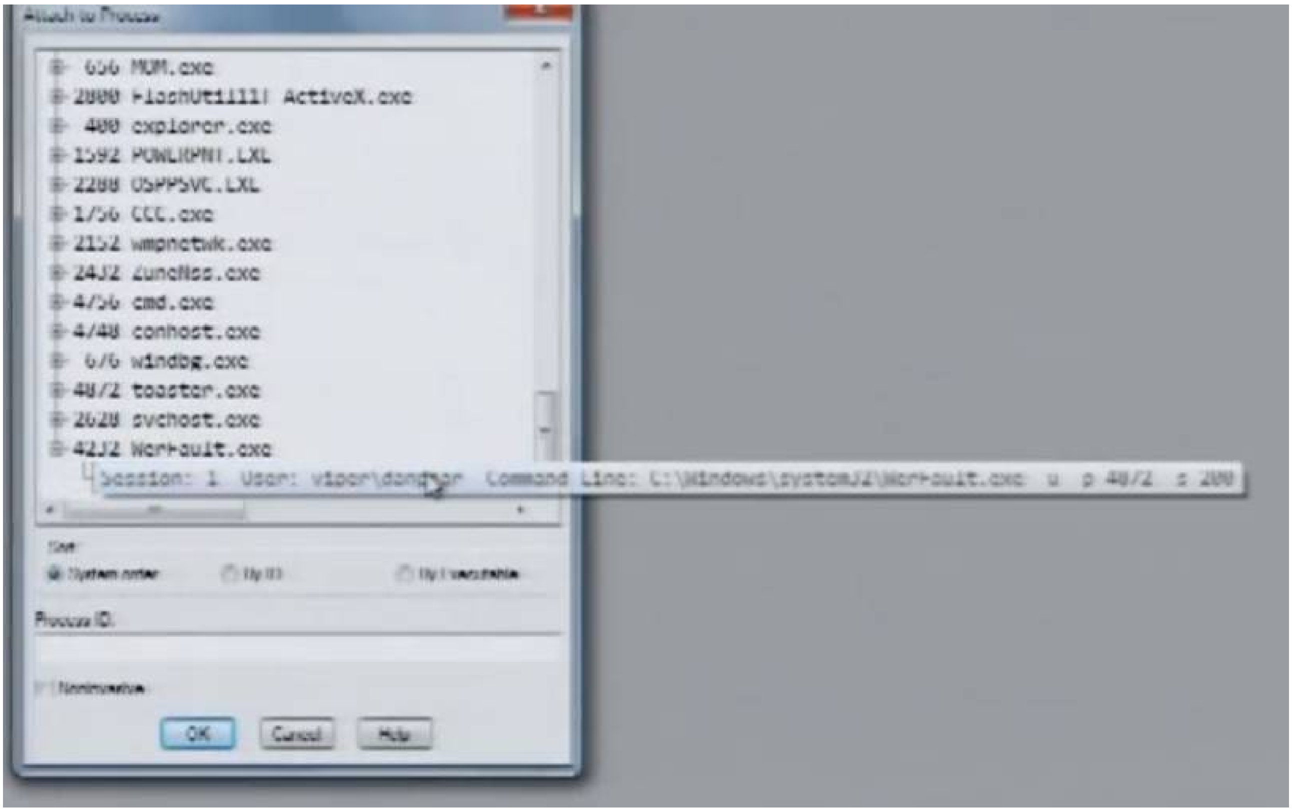
If a program crashed and the application shows the crash windows leave it open to show on the WerFault.exe process which captured the process ID of the crashed application



Toaster Application

Toaster Application has stopped working

Windows can check online for a solution to the problem.



Attach to Process

```
⊞  656 MDM.exe
⊞ 2800 FlashUtil11i ActiveX.exe
⊞  400 explorer.exe
⊞ 1592 POWERPNT.EXE
⊞ 2288 OSPPSVC.EXE
⊞ 1756 CCC.exe
⊞ 2152 wmpnetwk.exe
⊞ 2432 ZuneNss.exe
⊞ 4756 cmd.exe
⊞ 4748 conhost.exe
⊞  676 windbg.exe
⊞ 4872 toaster.exe
⊞ 2628 svchost.exe
⊞ 4232 WerFault.exe
  └ Session: 1  User: viper\[illegible]  Command Line: C:\Windows\system32\WerFault.exe -u -p 4872 -s 200
```

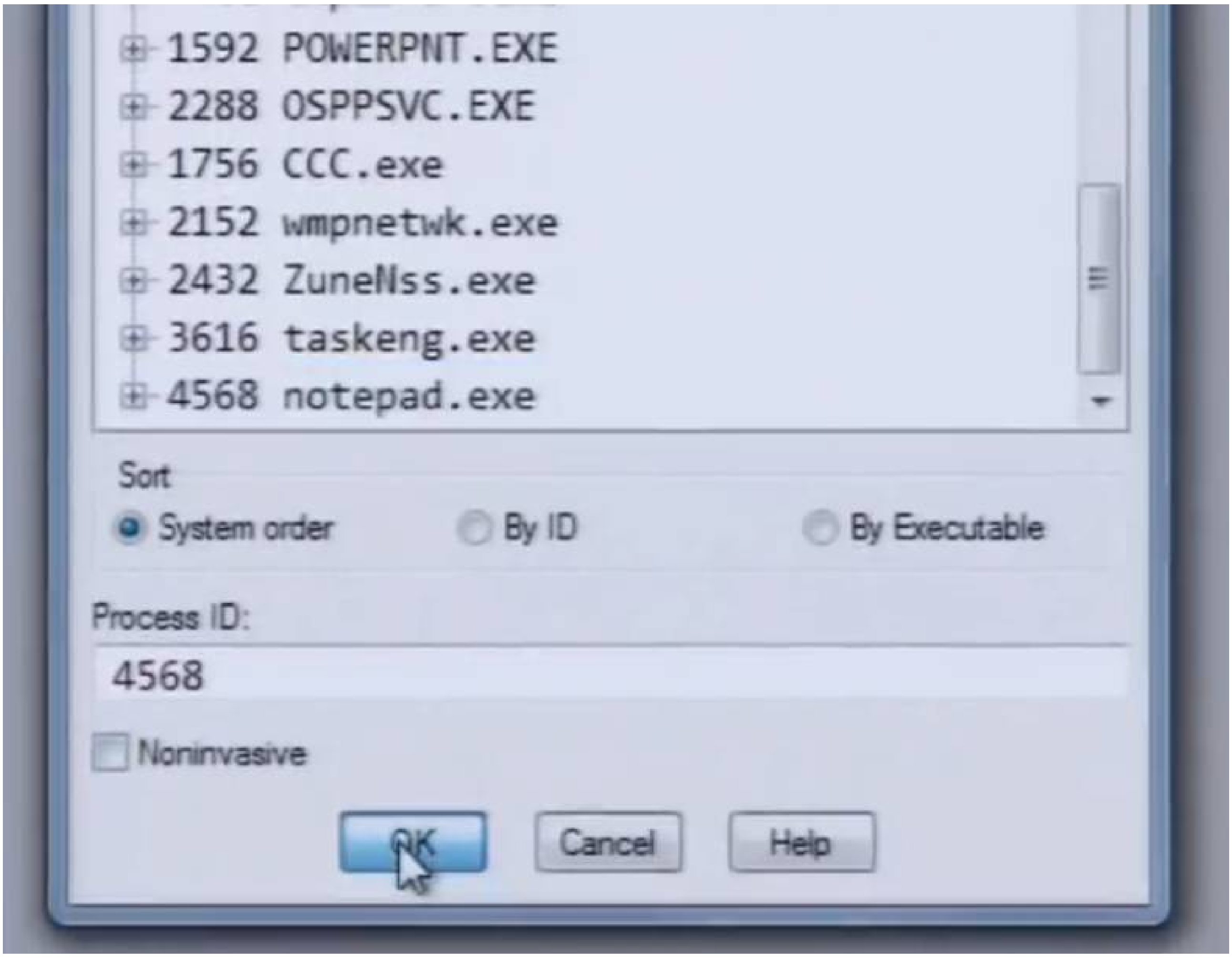
Sort

● System order ○ By ID ○ By Executable

Process ID:

□ Noninvasive

In the next Step attach to the crashed process and search for the captured process ID.



```
⊞ 1592 POWERPNT.EXE
⊞ 2288 OSPPSVC.EXE
⊞ 1756 CCC.exe
⊞ 2152 wmpnetwk.exe
⊞ 2432 ZuneNss.exe
⊞ 3616 taskeng.exe
⊞ 4568 notepad.exe
```

Sort

● System order ○ By ID ○ By Executable

Process ID: 4568

□ Noninvasive

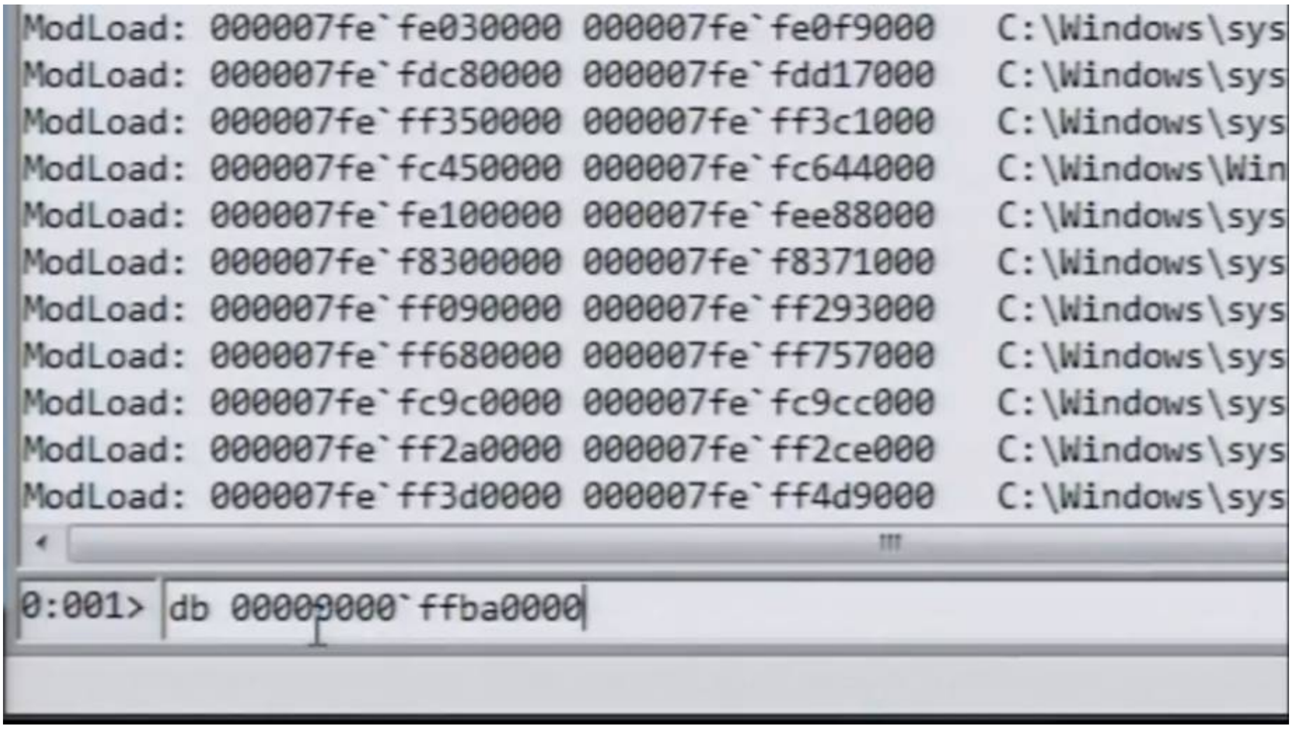
At this moment a direct access to the program is not possible until you enter the g-command in the debugging tool.

Important: If you close the debugging tool and the process you be attached is running, it will be closed instantly as the debugging tool is closed !

To prevent this issue press the qd-command into the debugging tool, so the program continue where the debugging tool is deattached and closed.

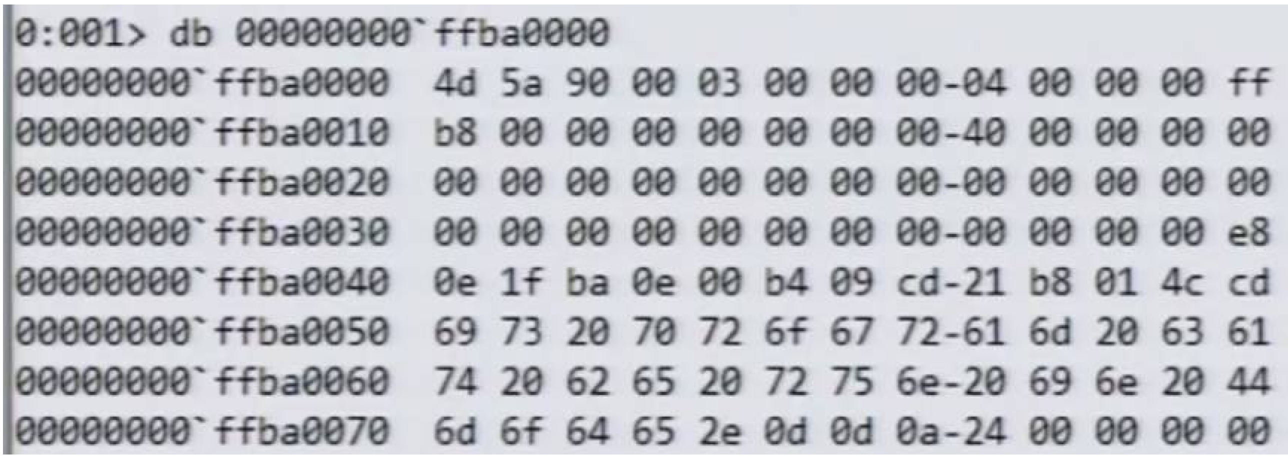
To see more debugging details of a process or crashdump file you can use the following commands for diffrent information:

At first view it present the loaded modules. You can also show the module list with the lm command.



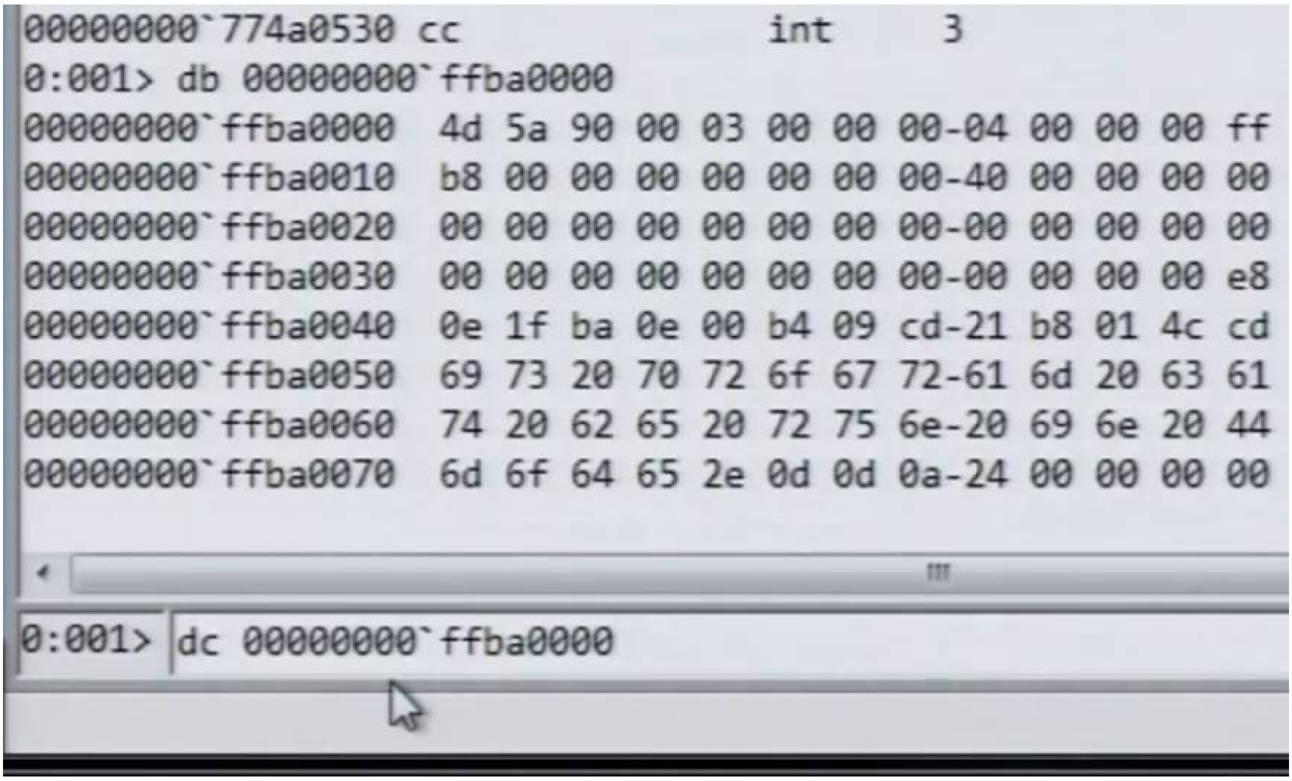
```
ModLoad: 000007fe`fe030000 000007fe`fe0f9000   C:\Windows\sys
ModLoad: 000007fe`fdc80000 000007fe`fdd17000   C:\Windows\sys
ModLoad: 000007fe`ff350000 000007fe`ff3c1000   C:\Windows\sys
ModLoad: 000007fe`fc450000 000007fe`fc644000   C:\Windows\Win
ModLoad: 000007fe`fe100000 000007fe`fee88000   C:\Windows\sys
ModLoad: 000007fe`f8300000 000007fe`f8371000   C:\Windows\sys
ModLoad: 000007fe`ff090000 000007fe`ff293000   C:\Windows\sys
ModLoad: 000007fe`ff680000 000007fe`ff757000   C:\Windows\sys
ModLoad: 000007fe`fc9c0000 000007fe`fc9cc000   C:\Windows\sys
ModLoad: 000007fe`ff2a0000 000007fe`ff2ce000   C:\Windows\sys
ModLoad: 000007fe`ff3d0000 000007fe`ff4d9000   C:\Windows\sys

0:001> db 00000000`ffba0000
```

Press the db command with the memory space address to see what is inside include Hex and ASCI values you want to see more details

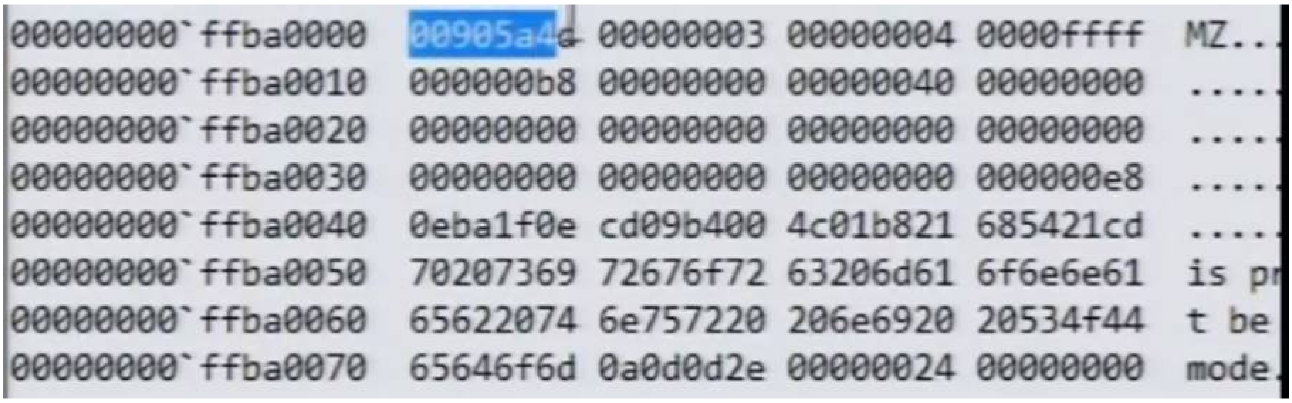


```
0:001> db 00000000`ffba0000
00000000`ffba0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff
00000000`ffba0010  b8 00 00 00 00 00 00 00-40 00 00 00 00
00000000`ffba0020  00 00 00 00 00 00 00 00-00 00 00 00 00
00000000`ffba0030  00 00 00 00 00 00 00 00-00 00 00 00 e8
00000000`ffba0040  0e 1f ba 0e 00 b4 09 cd-21 b8 01 4c cd
00000000`ffba0050  69 73 20 70 72 6f 67 72-61 6d 20 63 61
00000000`ffba0060  74 20 62 65 20 72 75 6e-20 69 6e 20 44
00000000`ffba0070  6d 6f 64 65 2e 0d 0d 0a-24 00 00 00 00
```

Press the dc command with the memory space address to see what is inside as Hex as Oktal and ASCI values

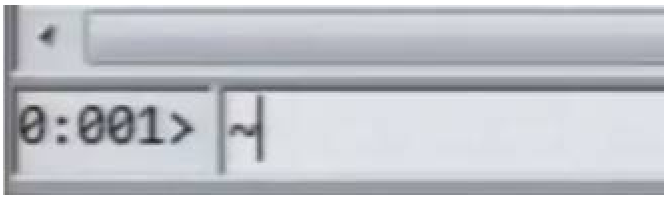


```
00000000`774a0530 cc              int     3
0:001> db 00000000`ffba0000
00000000`ffba0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff
00000000`ffba0010  b8 00 00 00 00 00 00 00-40 00 00 00 00
00000000`ffba0020  00 00 00 00 00 00 00 00-00 00 00 00 00
00000000`ffba0030  00 00 00 00 00 00 00 00-00 00 00 00 e8
00000000`ffba0040  0e 1f ba 0e 00 b4 09 cd-21 b8 01 4c cd
00000000`ffba0050  69 73 20 70 72 6f 67 72-61 6d 20 63 61
00000000`ffba0060  74 20 62 65 20 72 75 6e-20 69 6e 20 44
00000000`ffba0070  6d 6f 64 65 2e 0d 0d 0a-24 00 00 00 00

0:001> dc 00000000`ffba0000
```

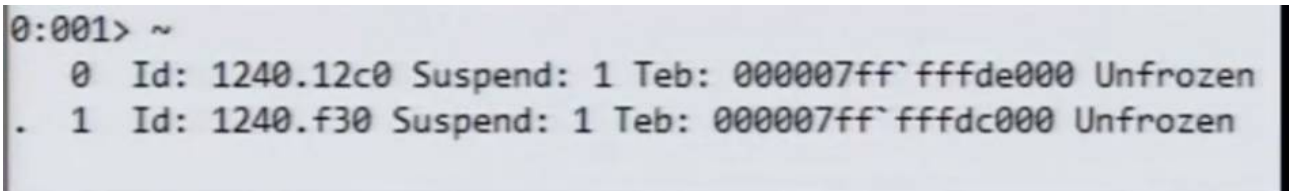


```
00000000`ffba0000  00905a4d 00000003 00000004 0000ffff  MZ..
00000000`ffba0010  000000b8 00000000 00000040 00000000  ....
00000000`ffba0020  00000000 00000000 00000000 00000000  ....
00000000`ffba0030  00000000 00000000 00000000 000000e8  ....
00000000`ffba0040  0eba1f0e cd09b400 4c01b821 685421cd  ....
00000000`ffba0050  70207369 72676f72 63206d61 6f6e6e61  is pr
00000000`ffba0060  65622074 6e757220 206e6920 20534f44  t be
00000000`ffba0070  65646f6d 0a0d0d2e 00000024 00000000  mode.
```

You can use the Tilde ~ command to see which Threads (with numbers) is inside this memory address space

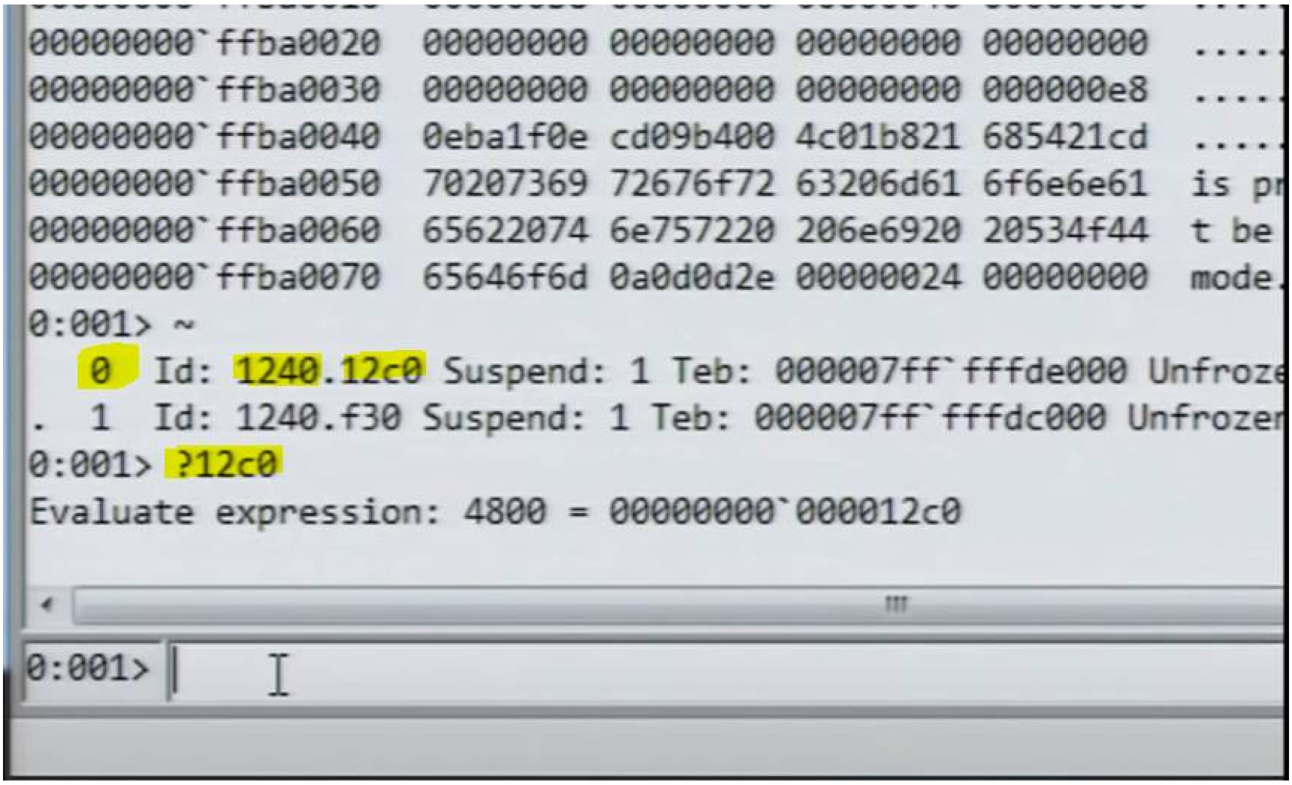


```
0:001> ~
```



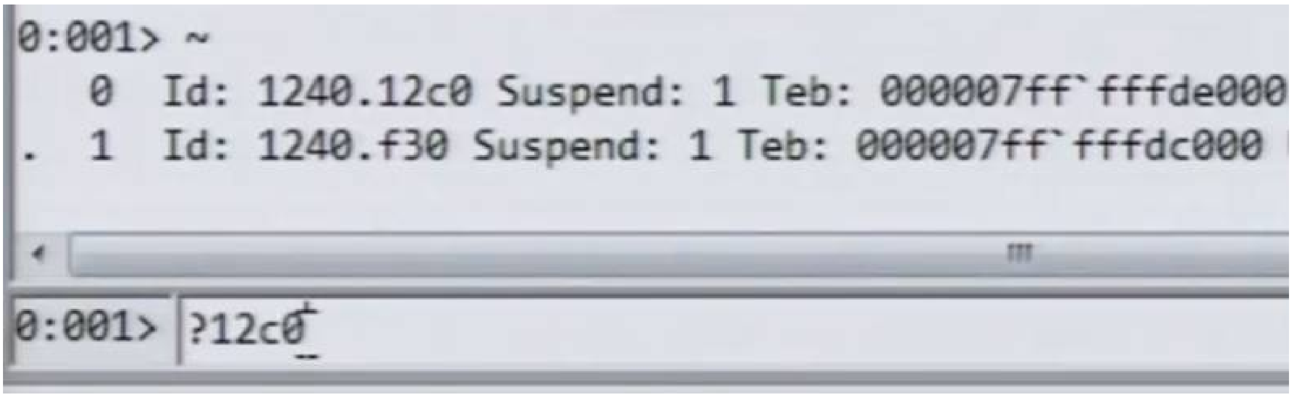
```
0:001> ~
   0  Id: 1240.12c0 Suspend: 1 Teb: 000007ff`fffde000 Unfrozen
.  1  Id: 1240.f30 Suspend: 1 Teb: 000007ff`fffdc000 Unfrozen
```

First value is the Threads Number, Second is the Process ID and third is rhe Thread ID

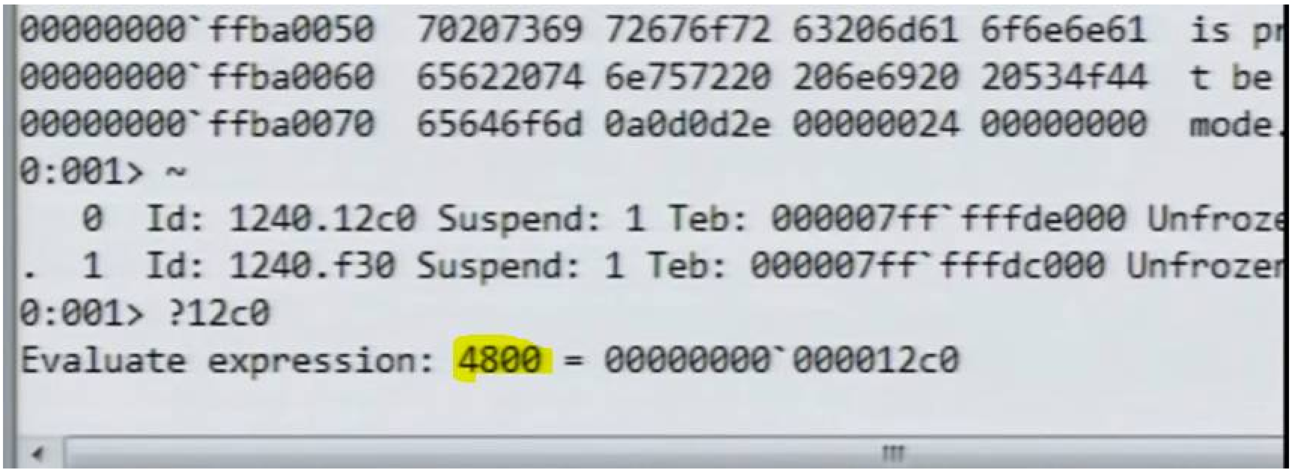


```
00000000`ffba0020  00000000 00000000 00000000 00000000  ....
00000000`ffba0030  00000000 00000000 00000000 000000e8  ....
00000000`ffba0040  0eba1f0e cd09b400 4c01b821 685421cd  ....
00000000`ffba0050  70207369 72676f72 63206d61 6f6e6e61  is pr
00000000`ffba0060  65622074 6e757220 206e6920 20534f44  t be
00000000`ffba0070  65646f6d 0a0d0d2e 00000024 00000000  mode.
0:001> ~
   0  Id: 1240.12c0 Suspend: 1 Teb: 000007ff`fffde000 Unfroze
.  1  Id: 1240.f30 Suspend: 1 Teb: 000007ff`fffdc000 Unfrozen
0:001> ?12c0
Evaluate expression: 4800 = 00000000`000012c0

0:001>
```

The Thread ID is a hex code. If you want to know the decimal number of the process in task manager you have to convert this value with the ?-command



```
0:001> ~
   0  Id: 1240.12c0 Suspend: 1 Teb: 000007ff`fffde000
.  1  Id: 1240.f30 Suspend: 1 Teb: 000007ff`fffdc000

0:001> ?12c0
```



```
00000000`ffba0050  70207369 72676f72 63206d61 6f6e6e61  is pr
00000000`ffba0060  65622074 6e757220 206e6920 20534f44  t be
00000000`ffba0070  65646f6d 0a0d0d2e 00000024 00000000  mode.
0:001> ~
   0  Id: 1240.12c0 Suspend: 1 Teb: 000007ff`fffde000 Unfroze
.  1  Id: 1240.f30 Suspend: 1 Teb: 000007ff`fffdc000 Unfrozen
0:001> ?12c0
Evaluate expression: 4800 = 00000000`000012c0
```

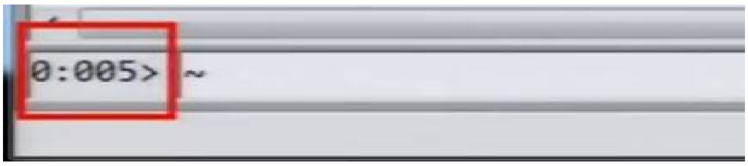
Debugging Steps of a Crashed Application or Process

Press the „attach to a process“ menu entree

show for the captured crashed process id looking on the WerFault.exe process

Attache the crashed application

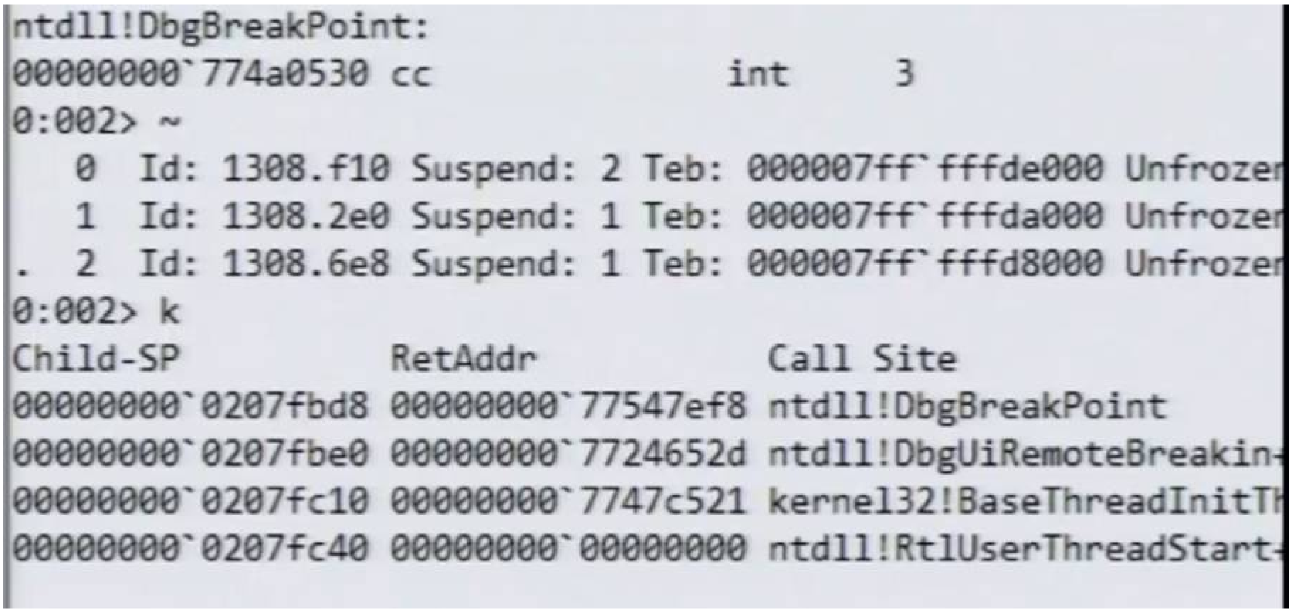
Show on the left side the number displayed on the command promp which shows the thread where the error or expection occurs.



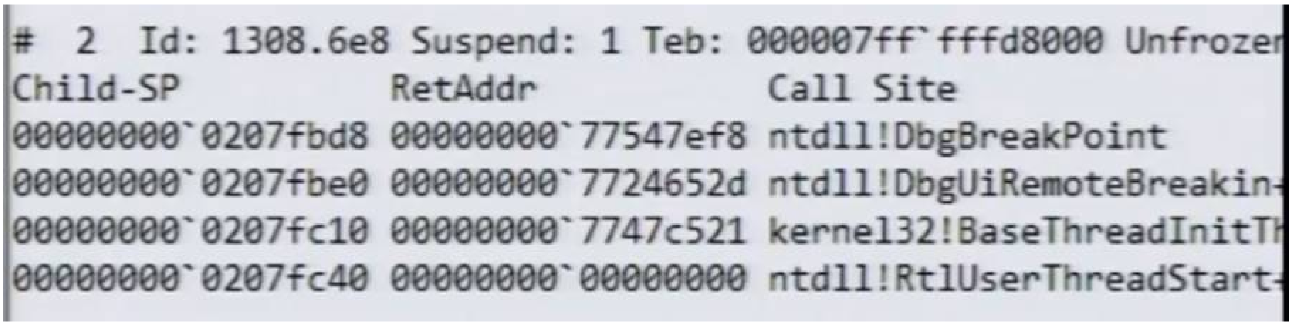
```
0:005> ~
```

Add the Tilde ~ command into the debugging tool to display open Threads

Add the k-command to display the stack and whats inside the stack of one thread or at the Tilde / Star ~* command with an option e.g k to display stack and whats inside the stack for each thread.

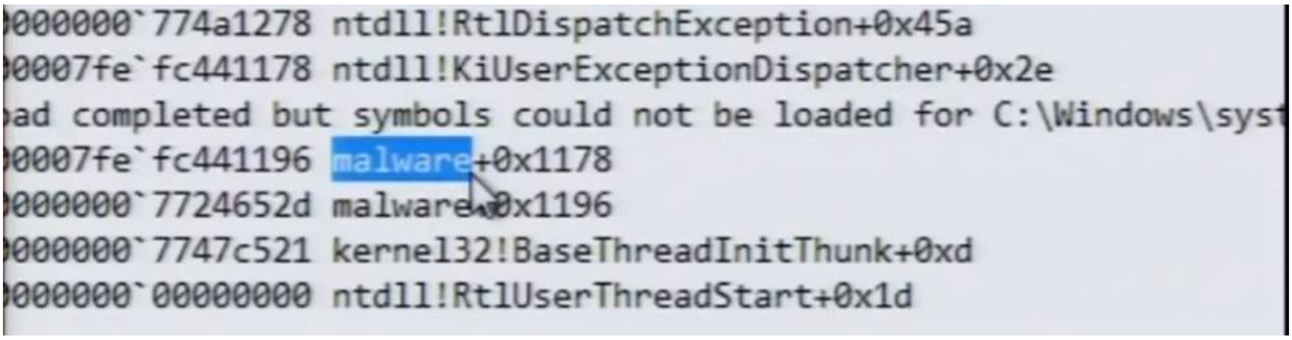


```
ntdll!DbgBreakPoint:
00000000`774a0530 cc              int     3
0:002> ~
   0  Id: 1308.f10 Suspend: 2 Teb: 000007ff`fffde000 Unfrozen
   1  Id: 1308.2e0 Suspend: 1 Teb: 000007ff`fffda000 Unfrozen
.  2  Id: 1308.6e8 Suspend: 1 Teb: 000007ff`fffd8000 Unfrozen
0:002> k
Child-SP          RetAddr           Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin+
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart+
```



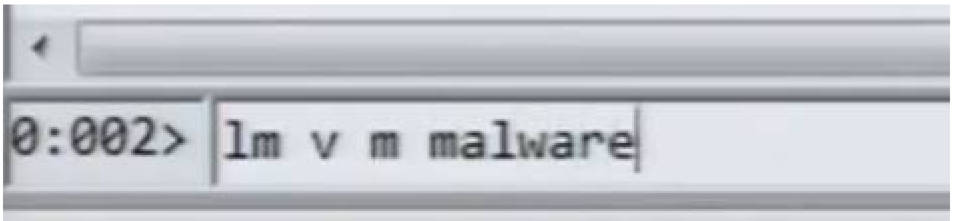
```
#  2  Id: 1308.6e8 Suspend: 1 Teb: 000007ff`fffd8000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin+
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart+
```

Now looking for e.g exceptions … to find the module which occures the crash

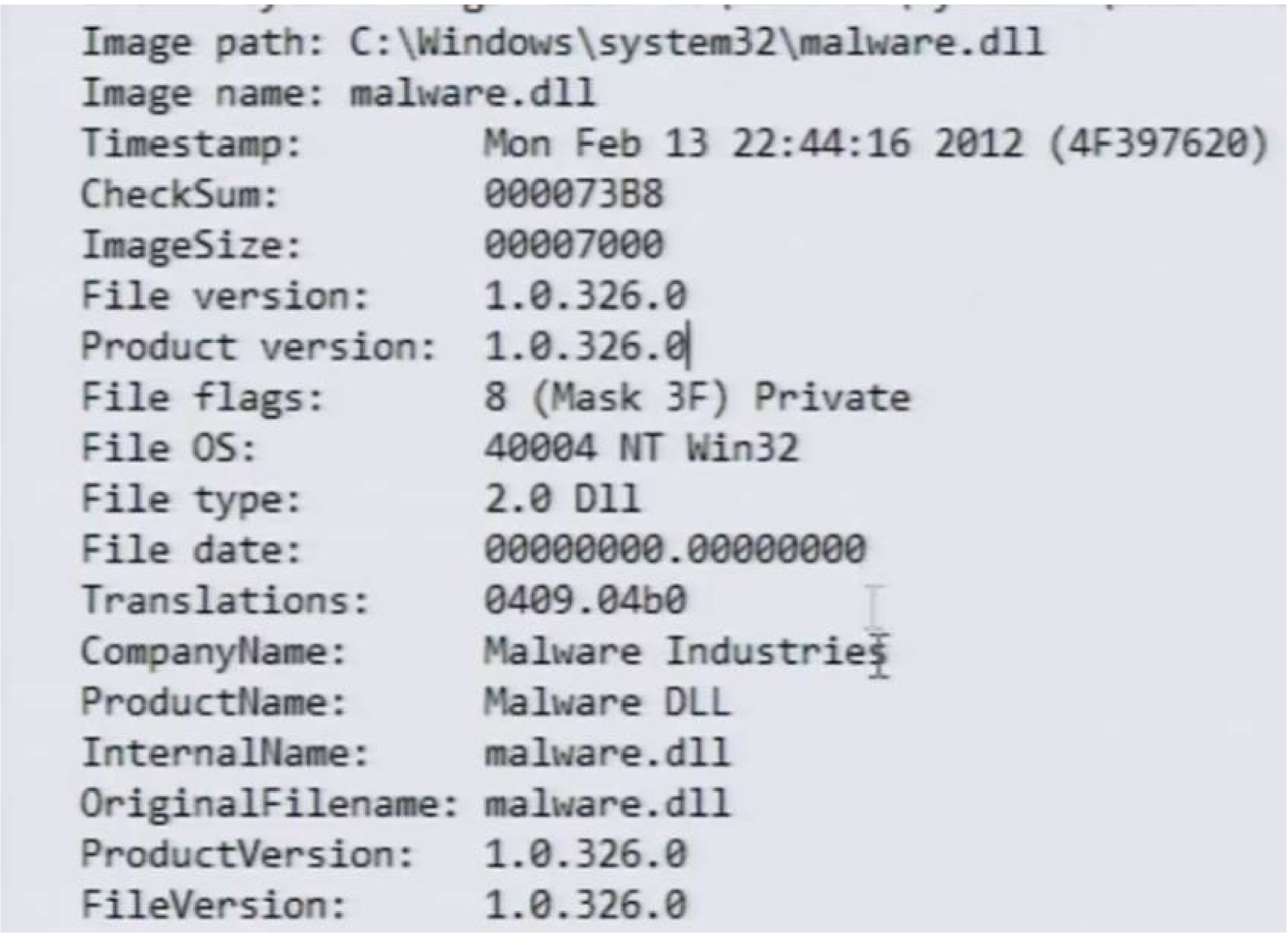


```
)000000`774a1278 ntdll!RtlDispatchException+0x45a
)0007fe`fc441178 ntdll!KiUserExceptionDispatcher+0x2e
)ad completed but symbols could not be loaded for C:\Windows\syst
)0007fe`fc441196 malware+0x1178
)000000`7724652d malware+0x1196
)000000`7747c521 kernel32!BaseThreadInitThunk+0xd
)000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

If you find something press the lm v m command combination include the module name you found. This means list modules(lm) in verbose mode (v / show as mutch information you find) and match (m) it



```
0:002> lm v m malware
```

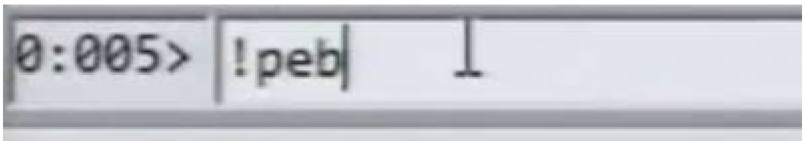


```
    Image path: C:\Windows\system32\malware.dll
    Image name: malware.dll
    Timestamp:        Mon Feb 13 22:44:16 2012 (4F397620)
    CheckSum:         000073B8
    ImageSize:        00007000
    File version:     1.0.326.0
    Product version:  1.0.326.0
    File flags:       8 (Mask 3F) Private
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Malware Industries
    ProductName:      Malware DLL
    InternalName:     malware.dll
    OriginalFilename: malware.dll
    ProductVersion:   1.0.326.0
    FileVersion:      1.0.326.0
```

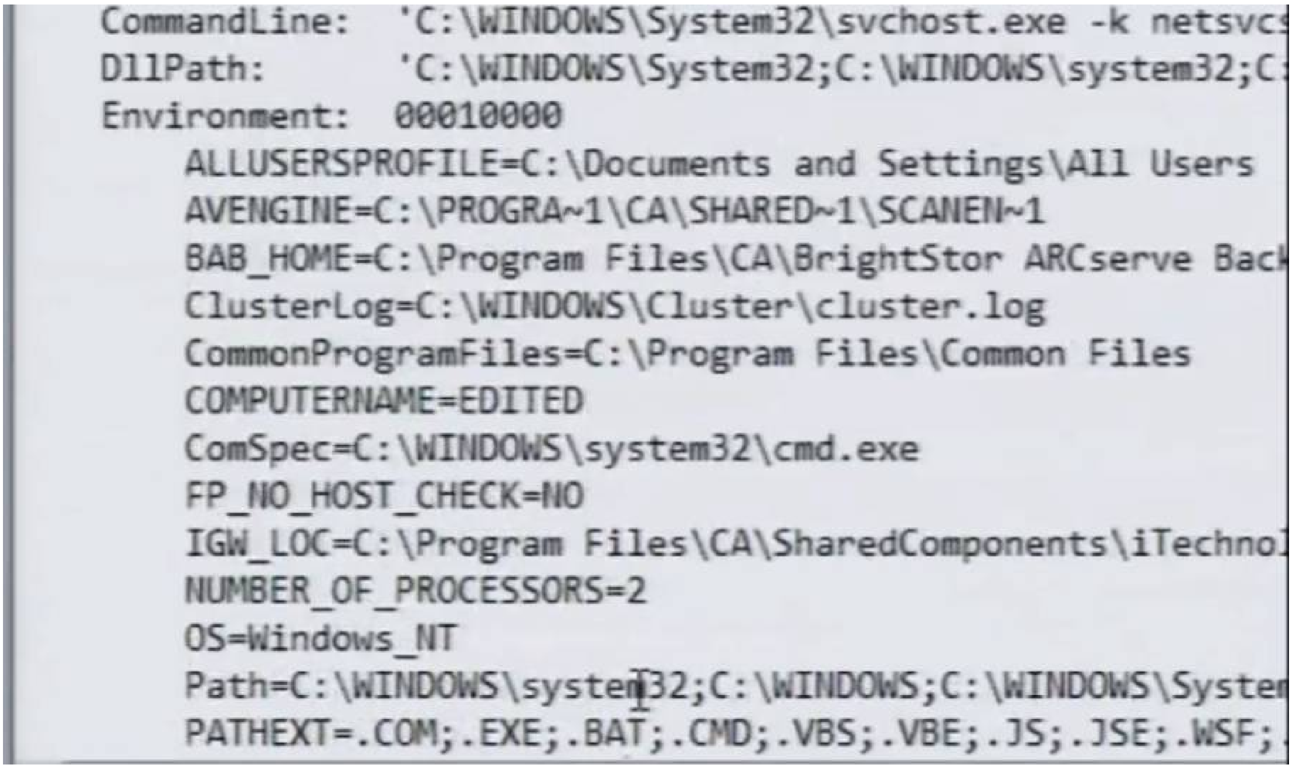
Debugging Steps to analyze a Dump file

Open the dump file with the „open dump file“ menu entree

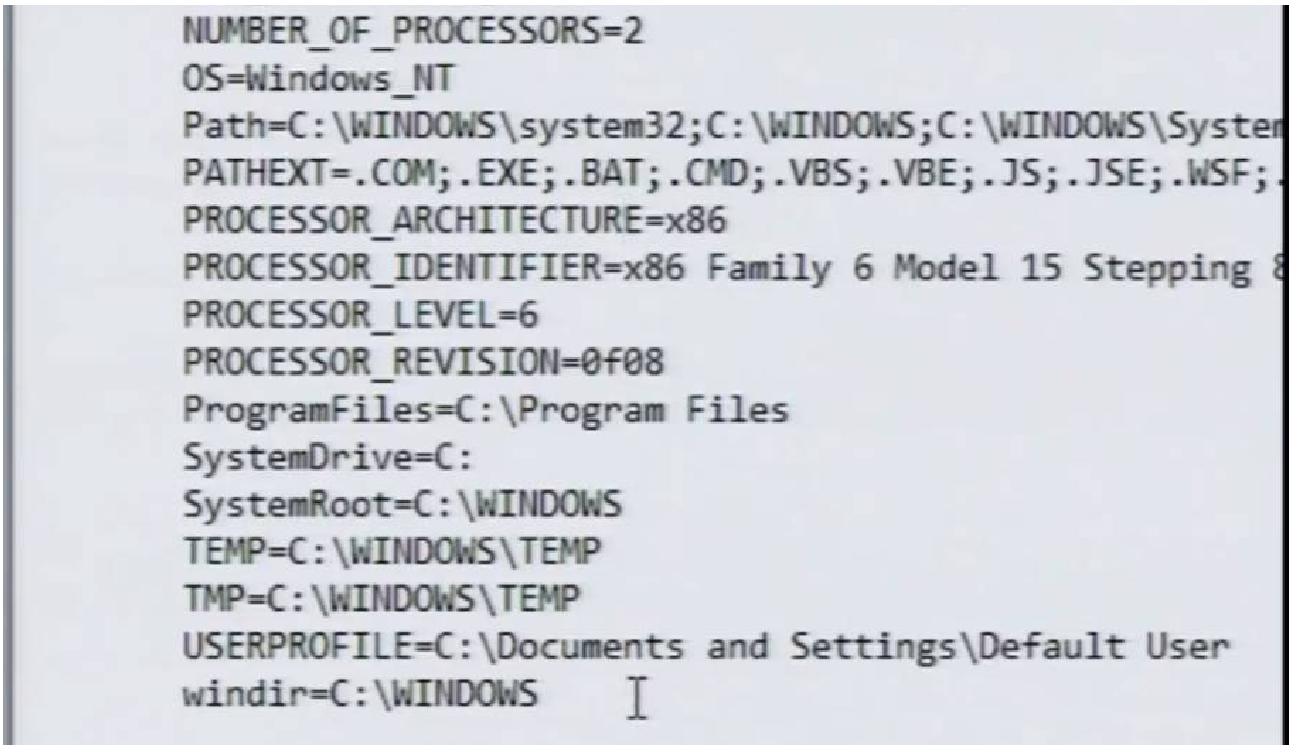
Add bang peb   !peb into the command promp which displays the process environment block which shows a lot of system information include corrupted process



```
0:005> !peb
```

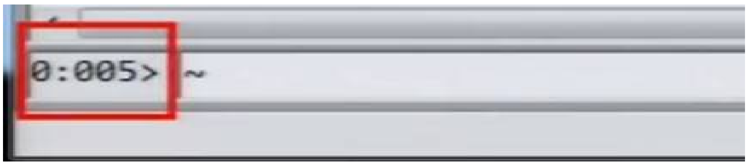


```
    CommandLine:  'C:\WINDOWS\System32\svchost.exe -k netsvcs
    DllPath:      'C:\WINDOWS\System32;C:\WINDOWS\system32;C:
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        AVENGINE=C:\PROGRA~1\CA\SHARED~1\SCANEN~1
        BAB_HOME=C:\Program Files\CA\BrightStor ARCserve Back
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=EDITED
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        IGW_LOC=C:\Program Files\CA\SharedComponents\iTechnol
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;
```



```
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\Syste
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 8
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0f08
ProgramFiles=C:\Program Files
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\Default User
windir=C:\WINDOWS
```

Show on the left side the number displayed on the command promp which shows the thread where the error or expection occurs.

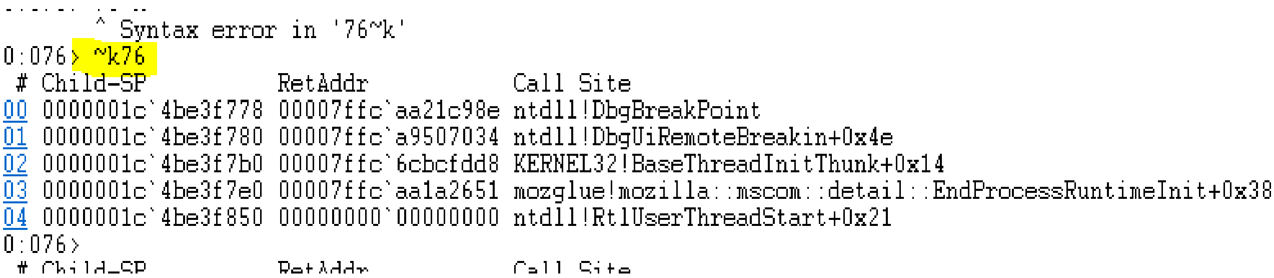


```
0:005> ~
```

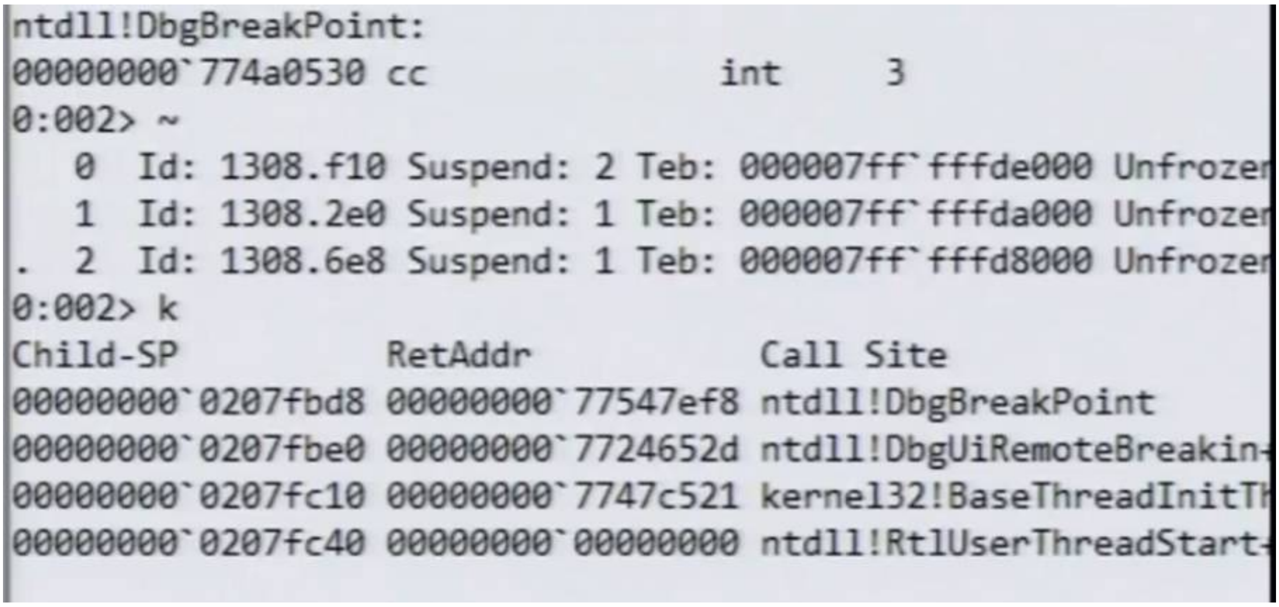
Add the Tilde ~ command into the debugging tool to display open Threads

Add the k-command to display the stack and whats inside the stack of one thread or at the Tilde / Star ~* command with an option e.g k to display stack and whats inside the stack for each thread.

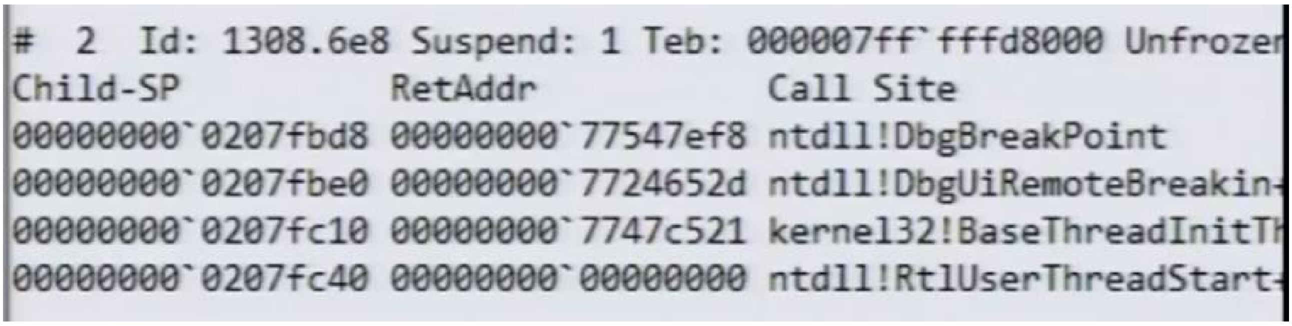
Or add the Thread number to only execute fo this thread.



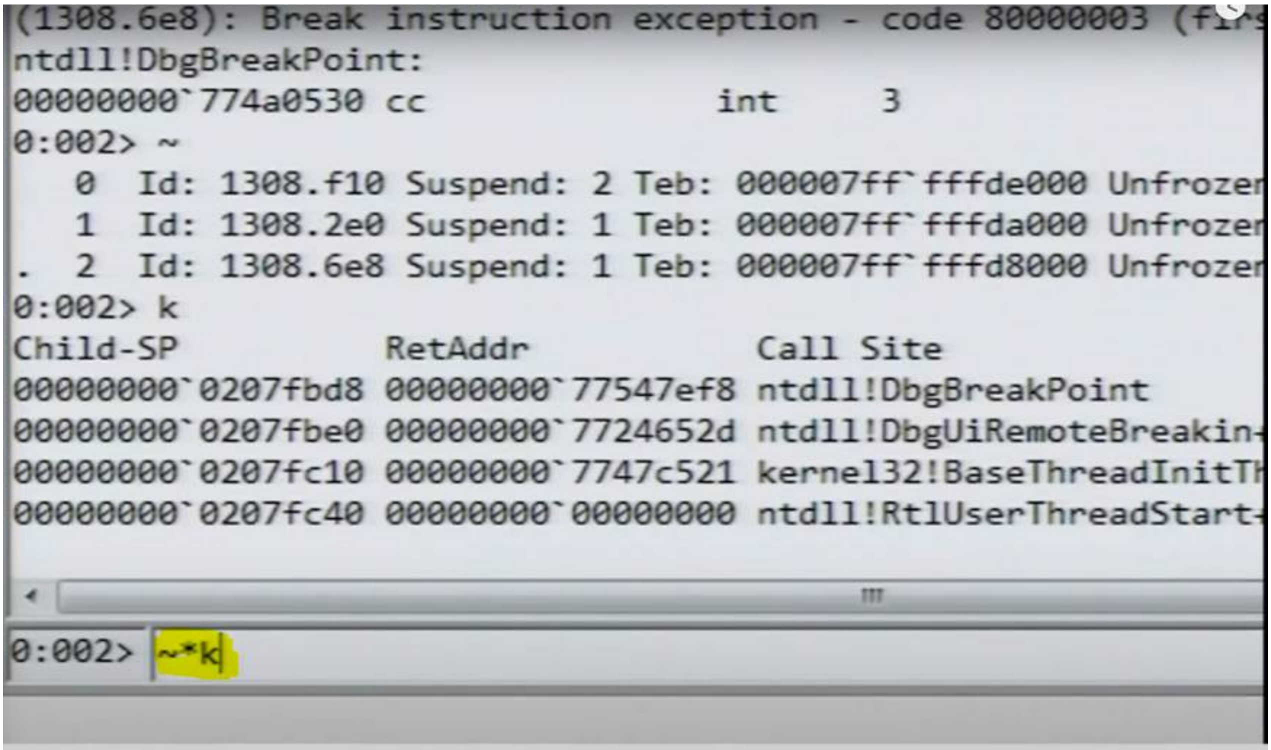
```
       ^ Syntax error in '76~k'
0:076> ~k76
 # Child-SP          RetAddr           Call Site
00 0000001c`4be3f778 00007ffc`aa21c98e ntdll!DbgBreakPoint
01 0000001c`4be3f780 00007ffc`a9507034 ntdll!DbgUiRemoteBreakin+0x4e
02 0000001c`4be3f7b0 00007ffc`6cbcfdd8 KERNEL32!BaseThreadInitThunk+0x14
03 0000001c`4be3f7e0 00007ffc`aa1a2651 mozglue!mozilla::mscom::detail::EndProcessRuntimeInit+0x38
04 0000001c`4be3f850 00000000`00000000 ntdll!RtlUserThreadStart+0x21
0:076>
 # Child-SP          RetAddr           Call Site
```



```
ntdll!DbgBreakPoint:
00000000`774a0530 cc              int     3
0:002> ~
   0  Id: 1308.f10 Suspend: 2 Teb: 000007ff`fffde000 Unfrozen
   1  Id: 1308.2e0 Suspend: 1 Teb: 000007ff`fffda000 Unfrozen
.  2  Id: 1308.6e8 Suspend: 1 Teb: 000007ff`fffd8000 Unfrozen
0:002> k
Child-SP          RetAddr           Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart
```

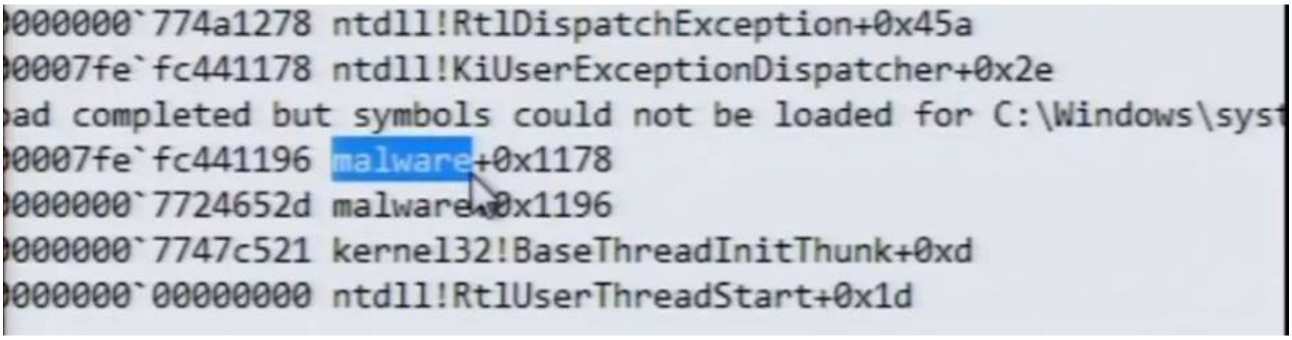


```
#  2  Id: 1308.6e8 Suspend: 1 Teb: 000007ff`fffd8000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart
```



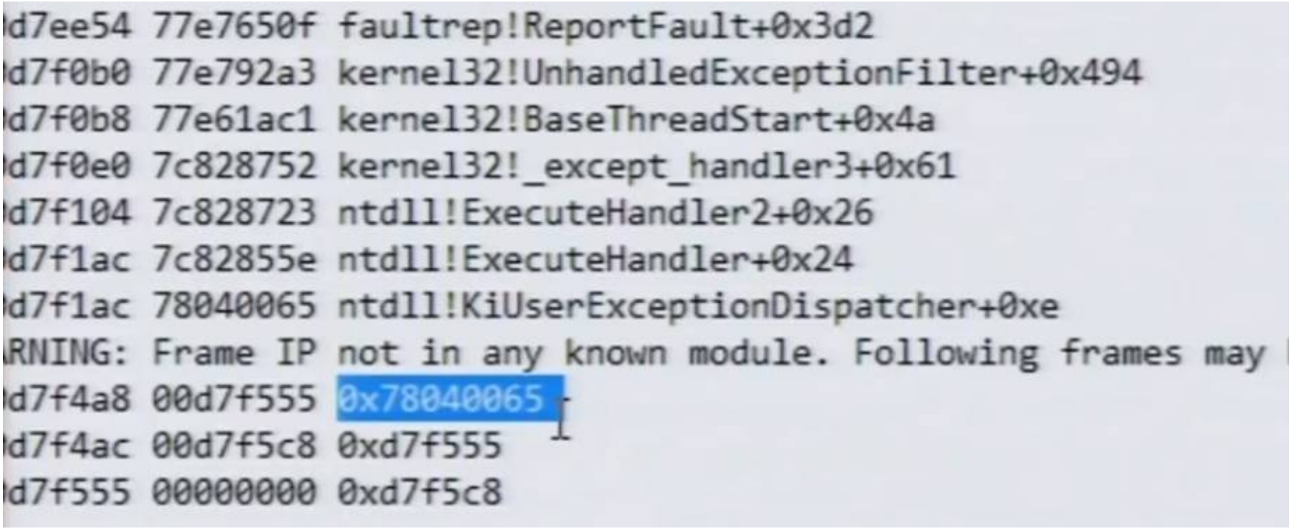
```
(1308.6e8): Break instruction exception - code 80000003 (fir
ntdll!DbgBreakPoint:
00000000`774a0530 cc              int     3
0:002> ~
   0  Id: 1308.f10 Suspend: 2 Teb: 000007ff`fffde000 Unfrozen
   1  Id: 1308.2e0 Suspend: 1 Teb: 000007ff`fffda000 Unfrozen
.  2  Id: 1308.6e8 Suspend: 1 Teb: 000007ff`fffd8000 Unfrozen
0:002> k
Child-SP          RetAddr           Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart

0:002> ~*k
```

Now looking for e.g excpetions … to find the module which occures the crash



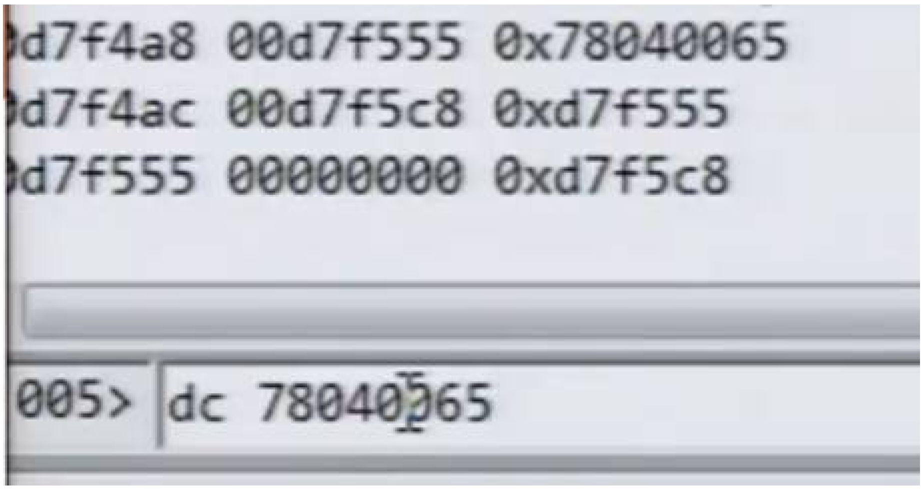
```
000000`774a1278 ntdll!RtlDispatchException+0x45a
0007fe`fc441178 ntdll!KiUserExceptionDispatcher+0x2e
ad completed but symbols could not be loaded for C:\Windows\syst
0007fe`fc441196 malware+0x1178
000000`7724652d malware+0x1196
000000`7747c521 kernel32!BaseThreadInitThunk+0xd
000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

IT is possible that you can´t finde the exception directly rather show continuing Hex-Code



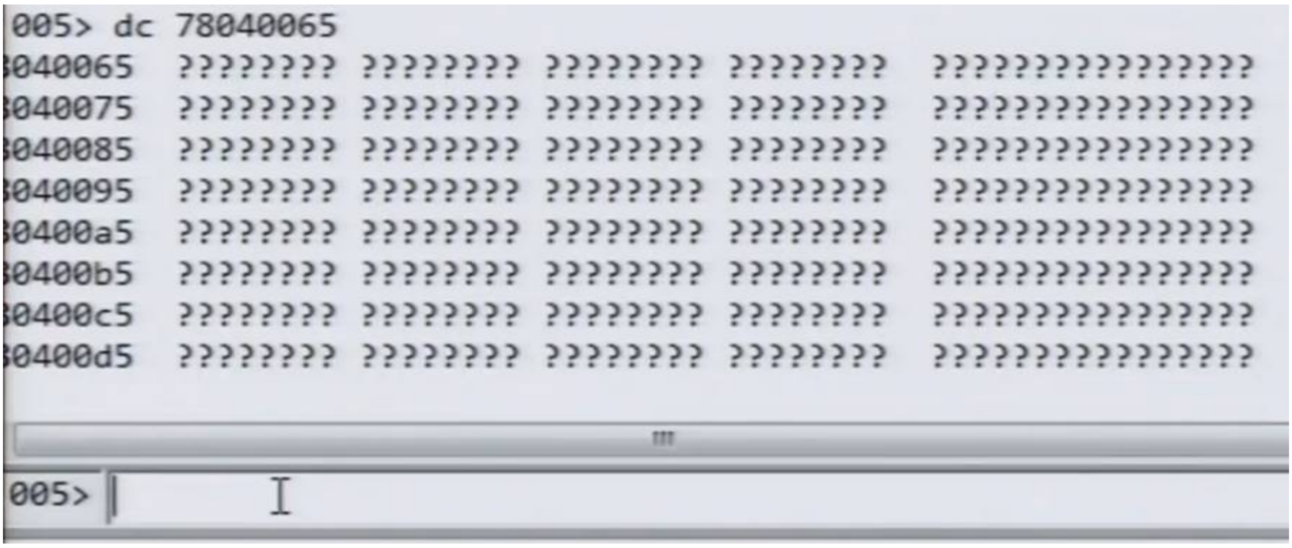
```
d7ee54 77e7650f faultrep!ReportFault+0x3d2
d7f0b0 77e792a3 kernel32!UnhandledExceptionFilter+0x494
d7f0b8 77e61ac1 kernel32!BaseThreadStart+0x4a
d7f0e0 7c828752 kernel32!_except_handler3+0x61
d7f104 7c828723 ntdll!ExecuteHandler2+0x26
d7f1ac 7c82855e ntdll!ExecuteHandler+0x24
d7f1ac 78040065 ntdll!KiUserExceptionDispatcher+0xe
RNING: Frame IP not in any known module. Following frames may
d7f4a8 00d7f555 0x78040065
d7f4ac 00d7f5c8 0xd7f555
d7f555 00000000 0xd7f5c8
```

In this case you have to convert the Hex code using dc **command with the memory space address to see what is inside as Hex as Oktal and ASCI values**



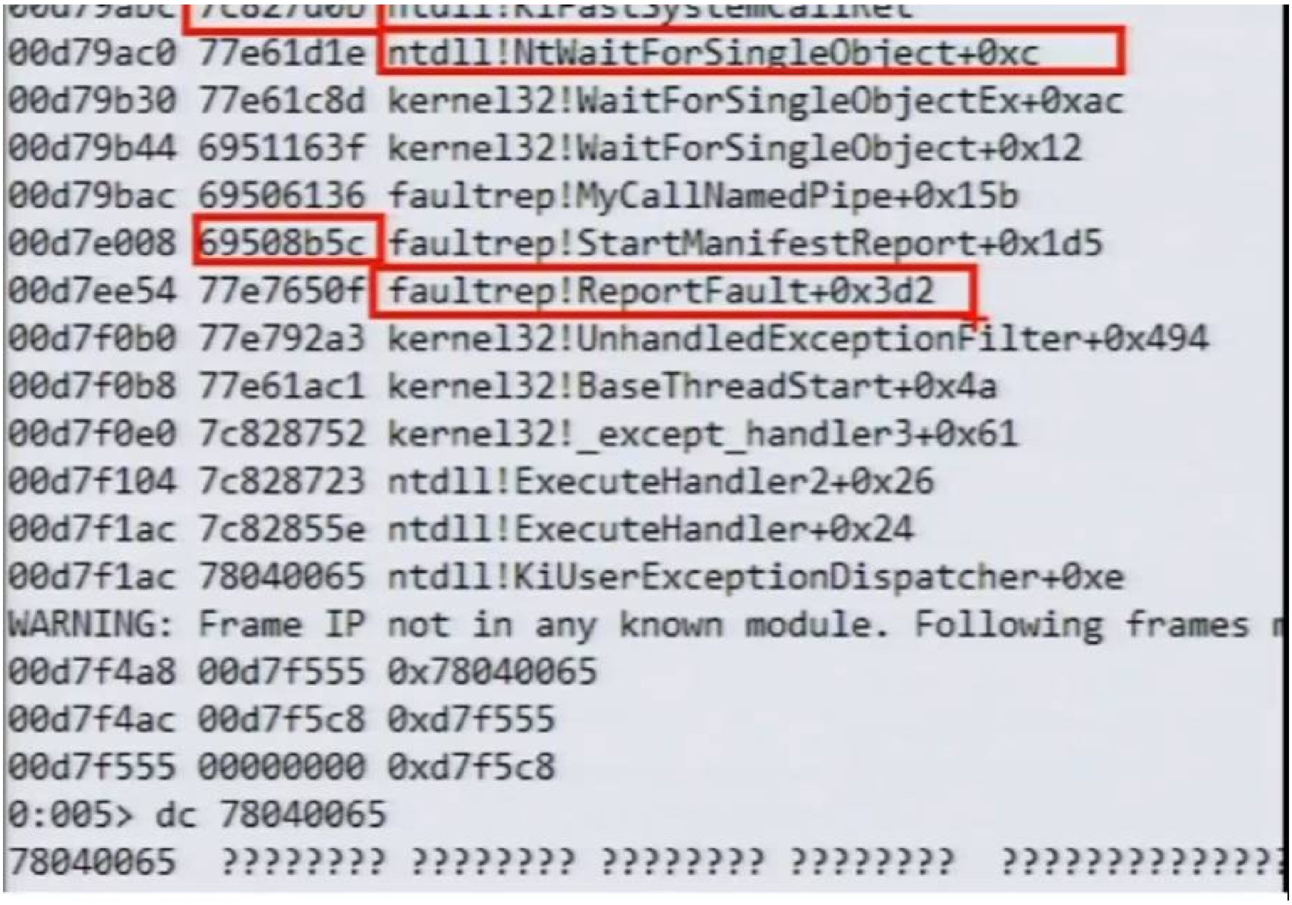
```
d7f4a8 00d7f555 0x78040065
d7f4ac 00d7f5c8 0xd7f555
d7f555 00000000 0xd7f5c8

005> dc 78040065
```

If the converted entree shows ??? the Hex code before has handle the last executions before the exception or error occurs and the system crashed. Repeat the last step with the dc command using the Hex code before this process handling.

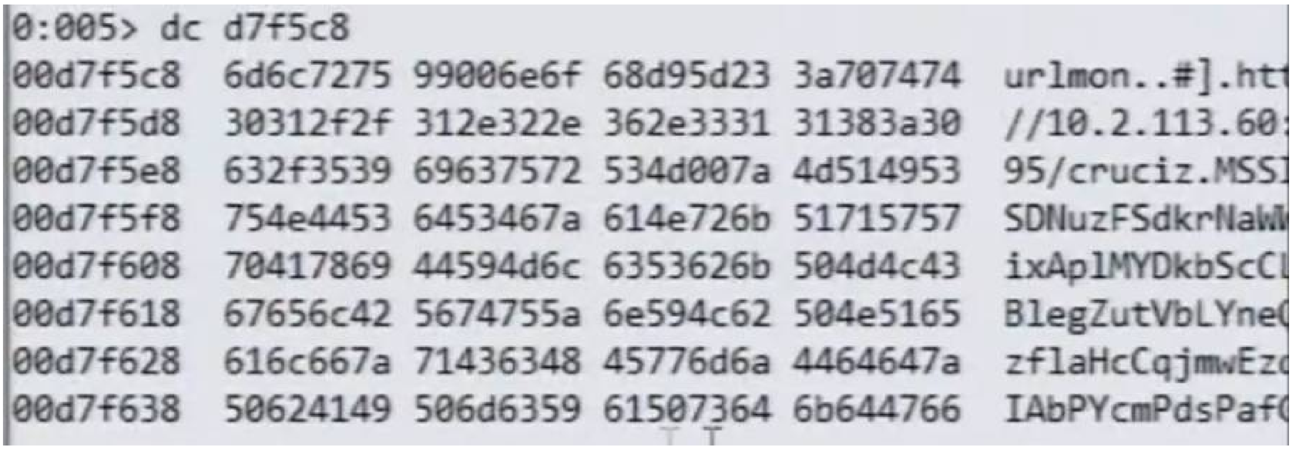


```
005> dc 78040065
8040065  ???????? ???????? ???????? ????????  ????????????????
8040075  ???????? ???????? ???????? ????????  ????????????????
8040085  ???????? ???????? ???????? ????????  ????????????????
8040095  ???????? ???????? ???????? ????????  ????????????????
80400a5  ???????? ???????? ???????? ????????  ????????????????
80400b5  ???????? ???????? ???????? ????????  ????????????????
80400c5  ???????? ???????? ???????? ????????  ????????????????
80400d5  ???????? ???????? ???????? ????????  ????????????????

005>
```

So the general process handling steps are different lines showing below. The Hex code in the upper line is handling the command showing in the next line and so on.



```
00d79abc 7c827d0b ntdll!KiFastSystemCallRet
00d79ac0 77e61d1e ntdll!NtWaitForSingleObject+0xc
00d79b30 77e61c8d kernel32!WaitForSingleObjectEx+0xac
00d79b44 6951163f kernel32!WaitForSingleObject+0x12
00d79bac 69506136 faultrep!MyCallNamedPipe+0x15b
00d7e008 69508b5c faultrep!StartManifestReport+0x1d5
00d7ee54 77e7650f faultrep!ReportFault+0x3d2
00d7f0b0 77e792a3 kernel32!UnhandledExceptionFilter+0x494
00d7f0b8 77e61ac1 kernel32!BaseThreadStart+0x4a
00d7f0e0 7c828752 kernel32!_except_handler3+0x61
00d7f104 7c828723 ntdll!ExecuteHandler2+0x26
00d7f1ac 7c82855e ntdll!ExecuteHandler+0x24
00d7f1ac 78040065 ntdll!KiUserExceptionDispatcher+0xe
WARNING: Frame IP not in any known module. Following frames m
00d7f4a8 00d7f555 0x78040065
00d7f4ac 00d7f5c8 0xd7f555
00d7f555 00000000 0xd7f5c8
0:005> dc 78040065
78040065  ???????? ???????? ???????? ????????  ??????????????
```

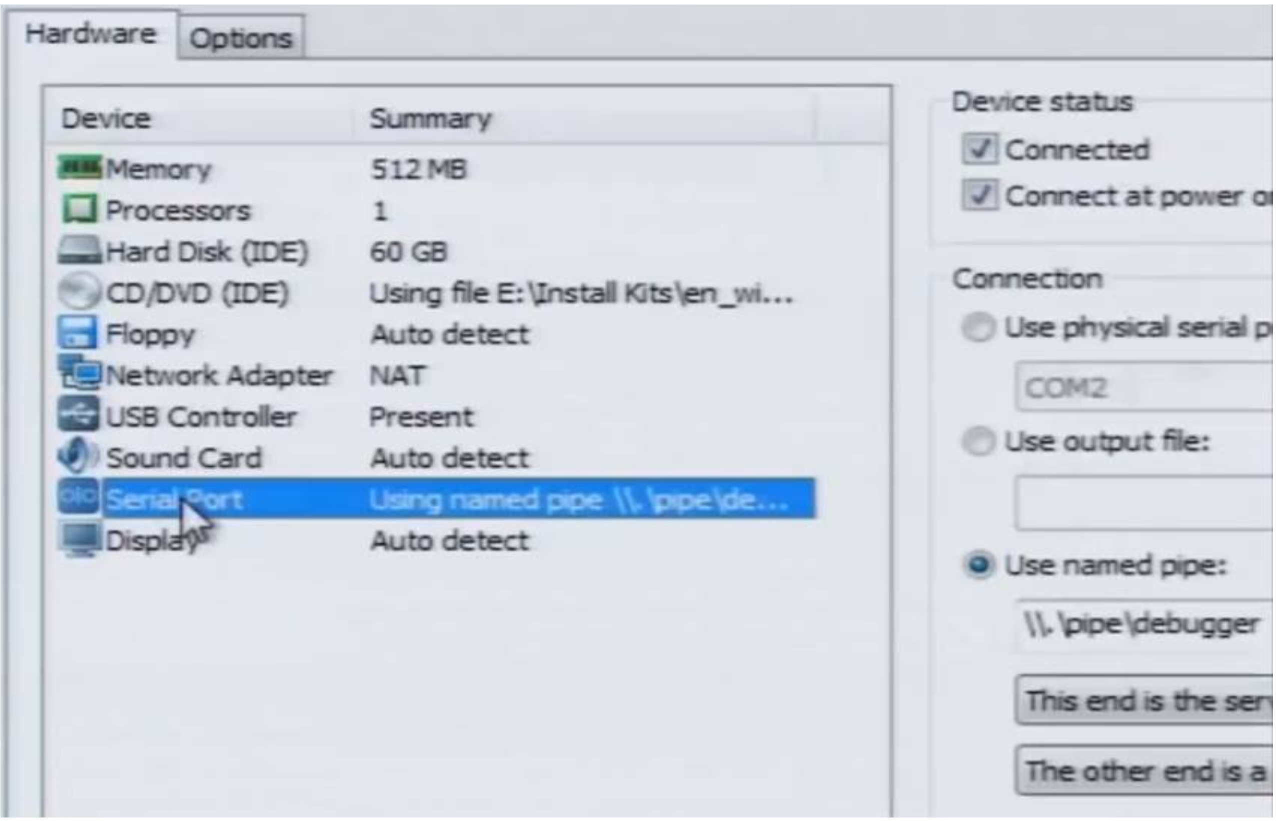


```
0:005> dc d7f5c8
00d7f5c8  6d6c7275 99006e6f 68d95d23 3a707474  urlmon..#].htt
00d7f5d8  30312f2f 312e322e 362e3331 31383a30  //10.2.113.60:
00d7f5e8  632f3539 69637572 534d007a 4d514953  95/cruciz.MSSI
00d7f5f8  754e4453 6453467a 614e726b 51715757  SDNuzFSdkrNaWW
00d7f608  70417869 44594d6c 6353626b 504d4c43  ixAplMYDkbScCL
00d7f618  67656c42 5674755a 6e594c62 504e5165  BlegZutVbLYneQ
00d7f628  616c667a 71436348 45776d6a 4464647a  zflaHcCqjmwEzd
00d7f638  50624149 506d6359 61507364 6b644766  IAbPYcmPdsPafG
```

The last picture shows the last code which was executed and crashed the system. Now futher investigating steps are needed also without the WinDbg.

Debugging Steps on Virtual / Remote Machine

To debug a virtual machine or other clients you can add a connection pipe on the virtual machine settings → Hardware → Serial Port to connect with a WinDbg from another machine.



Device	Summary
Memory	512 MB
Processors	1
Hard Disk (IDE)	60 GB
CD/DVD (IDE)	Using file E:\Install Kits\en_wi...
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Serial Port	Using named pipe \\.\pipe\de...
Display	Auto detect

Device status

☑ Connected

☑ Connect at power o

Connection

○ Use physical serial p

COM2

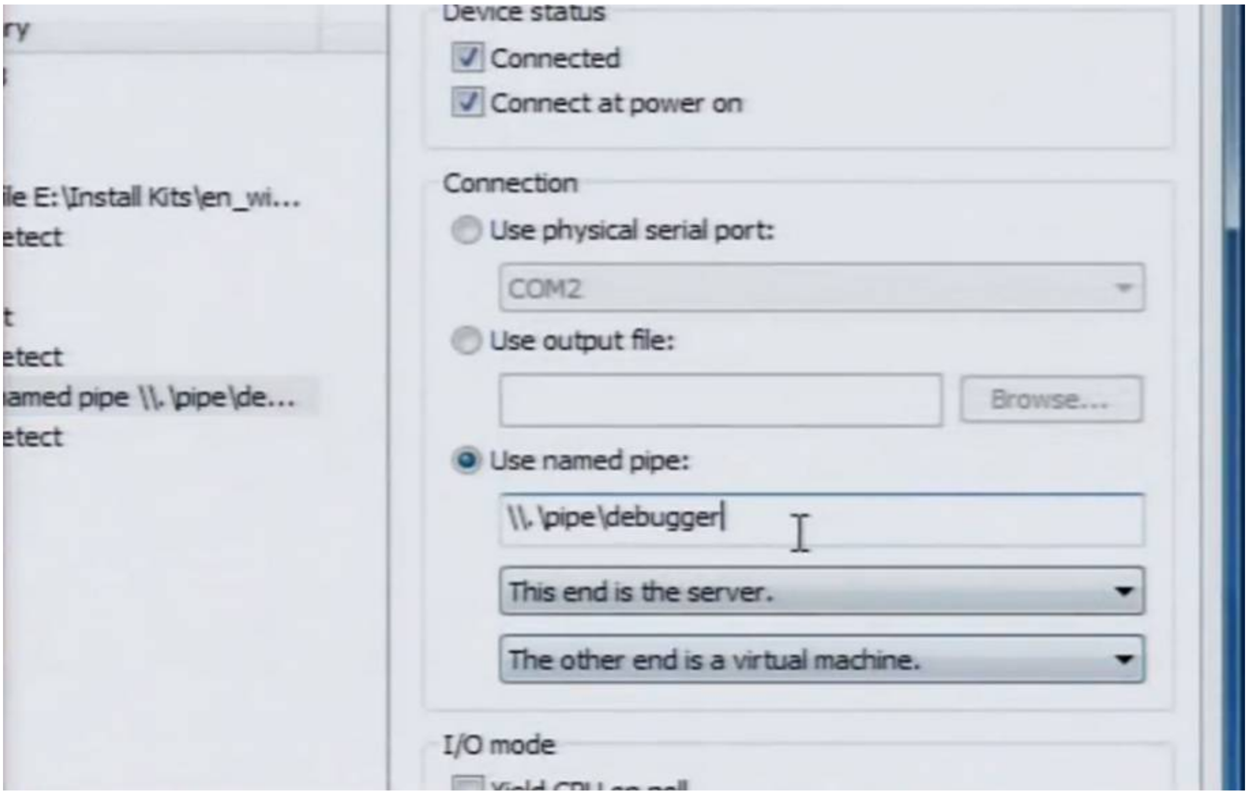
○ Use output file:

● Use named pipe:

\\.\pipe\debugger

This end is the ser

The other end is a



ry

le E:\Install Kits\en_wi...
etect
t
etect
amed pipe \\.\pipe\de...
etect

Device status

☑ Connected

☑ Connect at power on

Connection

○ Use physical serial port:

COM2

○ Use output file:

● Use named pipe:

\\.\pipe\debugger

This end is the server.

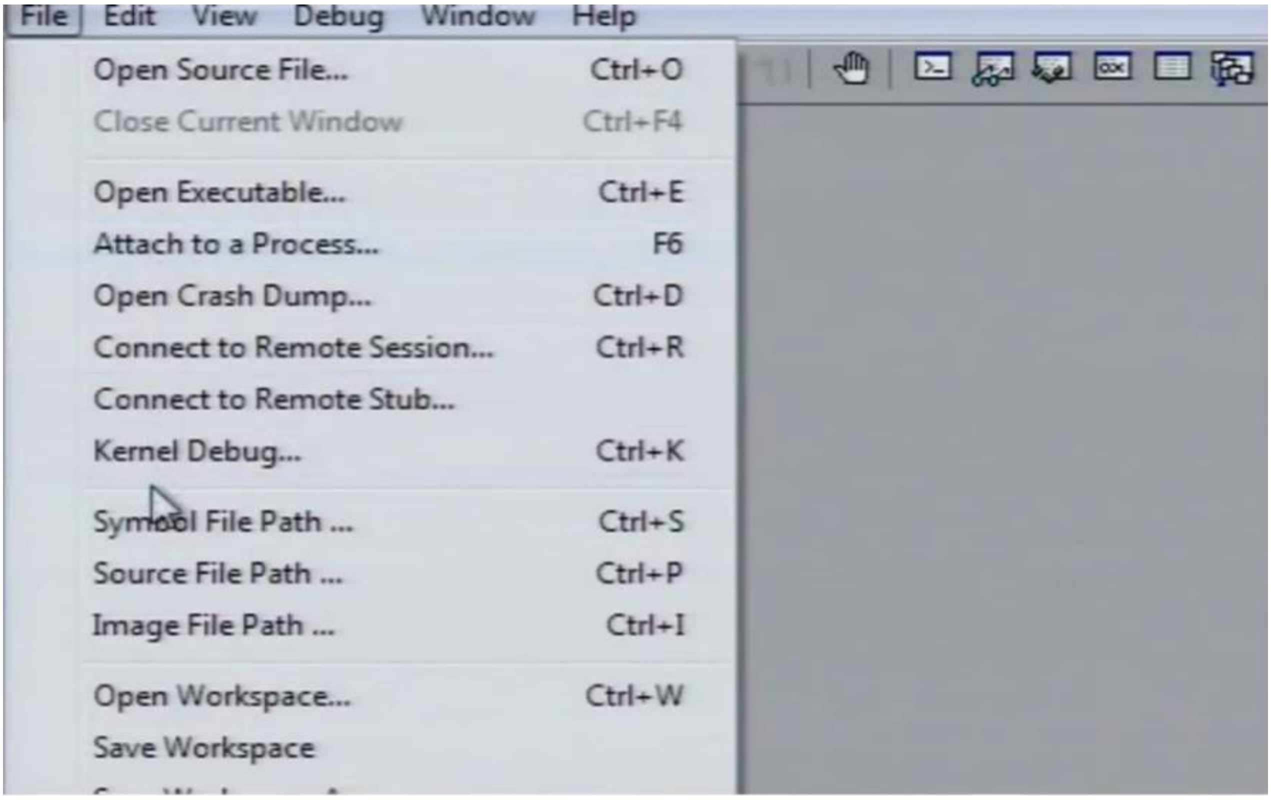
The other end is a virtual machine.

I/O mode

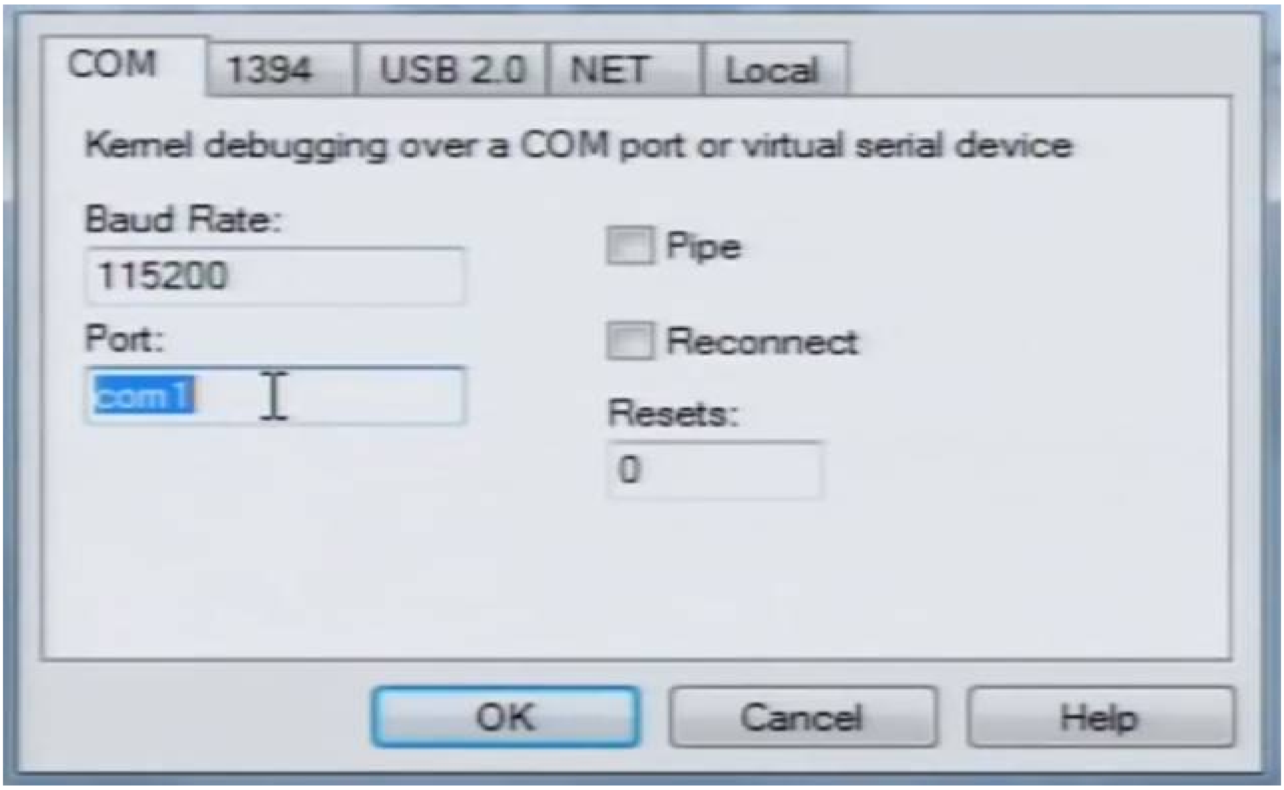
□ Yield CPU on poll

Add a debugging pipe eg. \\.\pipe\debugger in the virtual machine menu path.

After that open the WinDbg on the own machine and press the Kernel Debug menu option


File
Edit
View
Debug
Window
Help
Open Source File... Ctrl+O
Close Current Window Ctrl+F4
Open Executable... Ctrl+E
Attach to a Process... F6
Open Crash Dump... Ctrl+D
Connect to Remote Session... Ctrl+R
Connect to Remote Stub...
Kernel Debug... Ctrl+K
Symbol File Path ... Ctrl+S
Source File Path ... Ctrl+P
Image File Path ... Ctrl+I
Open Workspace... Ctrl+W
Save Workspace

On the open window the default port option is „com1“ enter the pipe from the VM and mark the pipe option



Kernel debugging over a COM port or virtual serial device

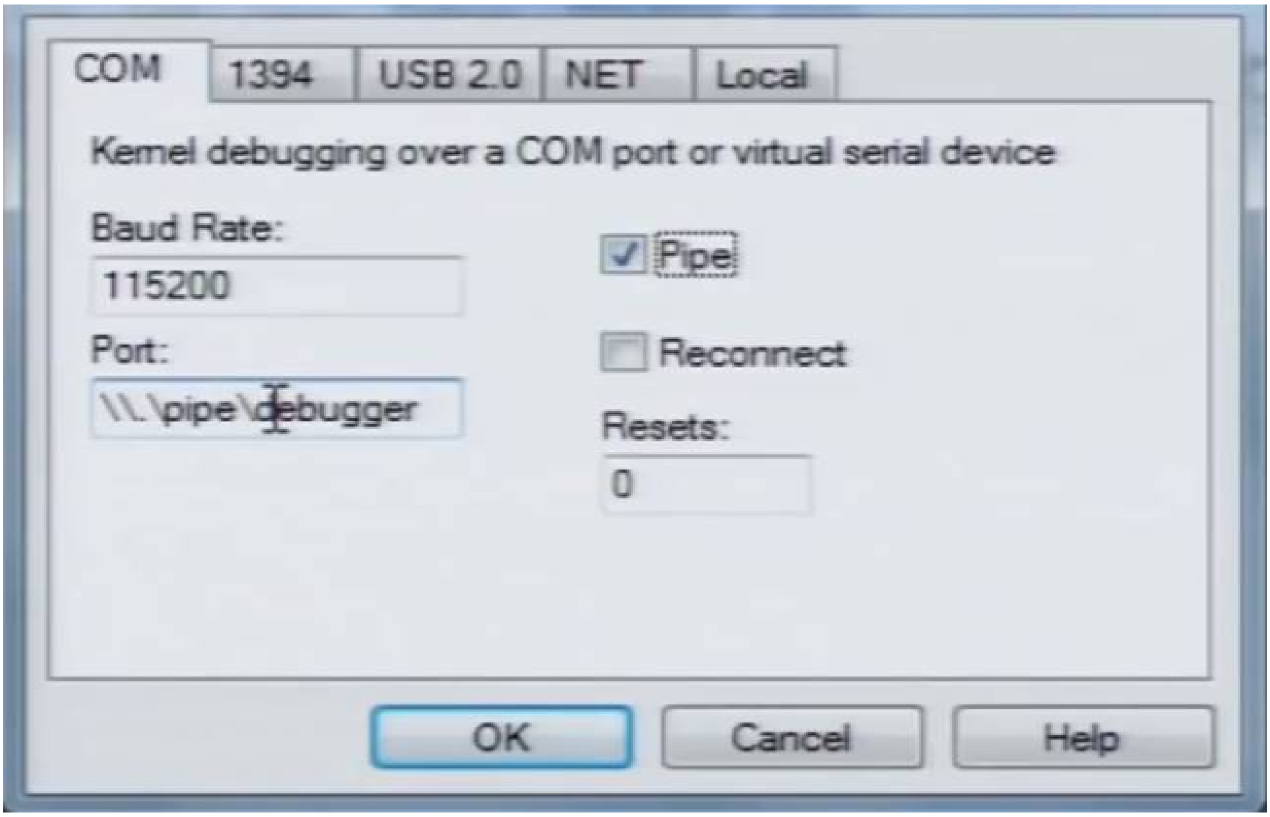
Baud Rate: 115200

Port: com1

□ Pipe

□ Reconnect

Resets: 0



Kernel debugging over a COM port or virtual serial device

Baud Rate: 115200

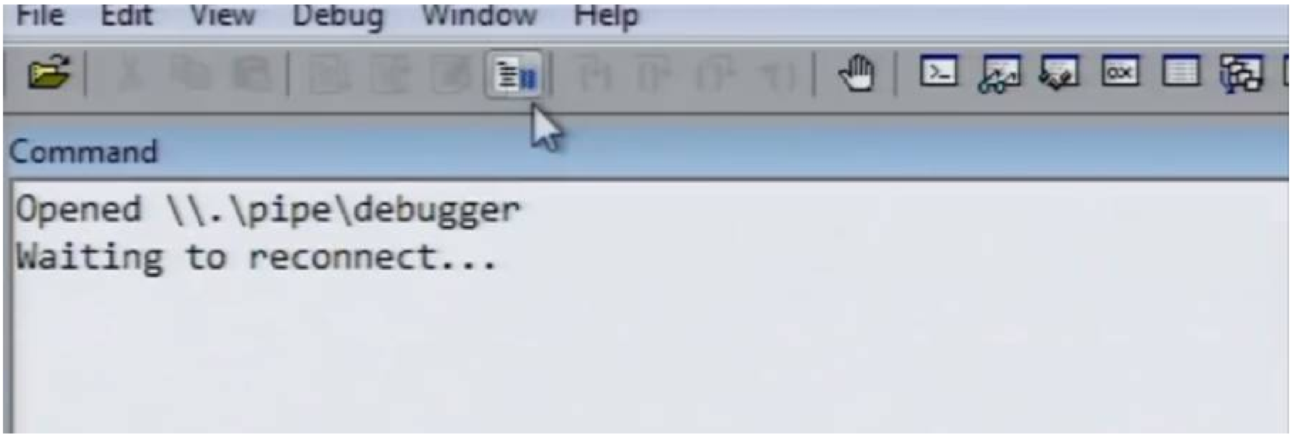
☑ Pipe

Port: \\.\pipe\debugger

□ Reconnect

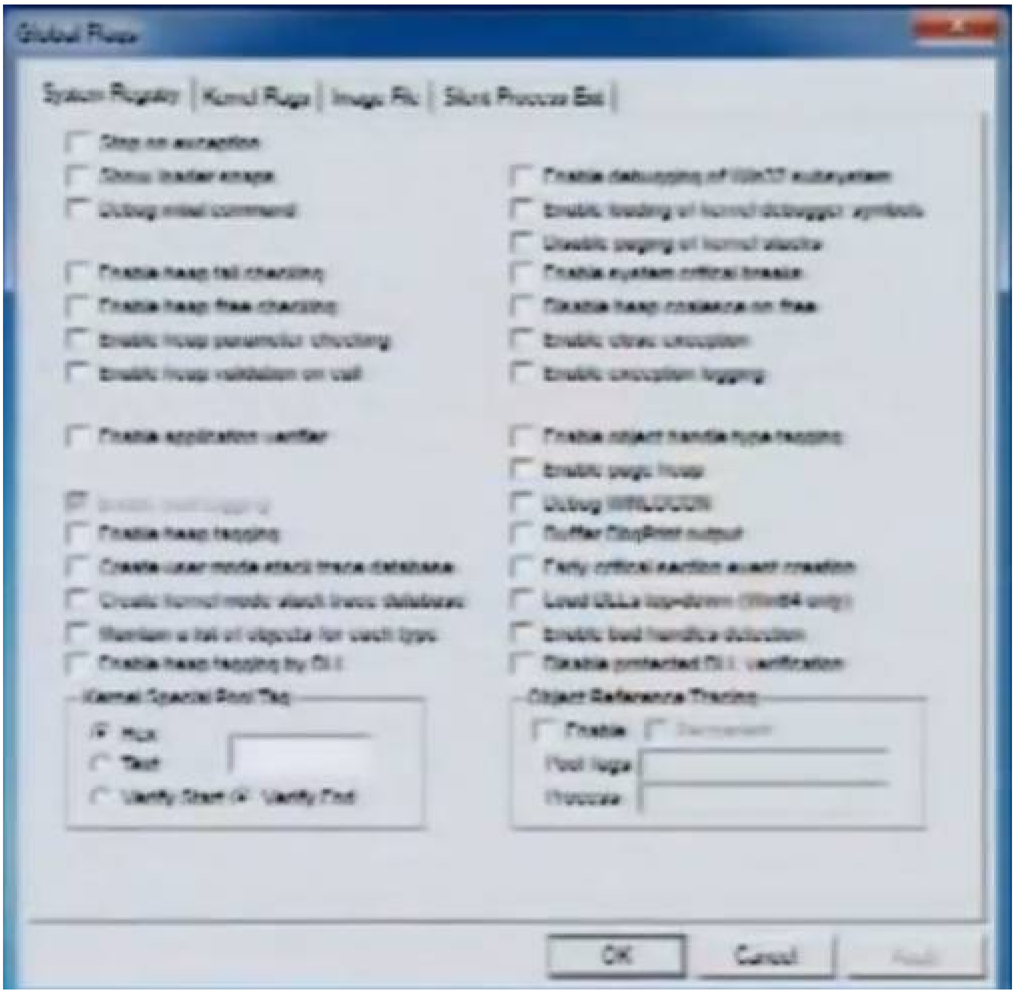
Resets: 0

After that press the icon showing in the picture to connect to the machine with the WinDbg. The connected machine is frozen until press the g-command



```
Opened \\.\pipe\debugger
Waiting to reconnect...
```

On the virtual machine install the sysinternal program global flags which provides more debugging options for the virtual machine.


Global Flags
System Registry | Kernel Flags | Image File | Silent Process Exit
OK
Cancel
Apply

□ Stop on exception
□ Show loader snaps
□ Debug initial command
□ Enable heap tail checking
□ Enable heap free checking
□ Enable heap parameter checking
□ Enable heap validation on call
□ Enable application verifier
☑ Enable pool tagging
□ Enable heap tagging
□ Create user mode stack trace database
□ Create kernel mode stack trace database
□ Maintain a list of objects for each type
□ Enable heap tagging by DLL

Kernel Special Pool Tag
● Hex
○ Text
○ Verify Start ● Verify End

□ Enable debugging of Win32 subsystem
□ Enable loading of kernel debugger symbols
□ Disable paging of kernel stacks
□ Enable system critical breaks
□ Disable heap coalesce on free
□ Enable close exception
□ Enable exception logging
□ Enable object handle type tagging
□ Enable page heap
□ Debug WINLOGON
□ Buffer DbgPrint output
□ Early critical section event creation
□ Load DLLs top-down (Win64 only)
□ Enable bad handles detection
□ Disable protected DLL verification

Object Reference Tracing
□ Enable □ Permanent
Pool tags
Process

On the option ImageFile it is possible to select the process which you want to debug. On the Debugger field you have also to enter the pipe you choiced

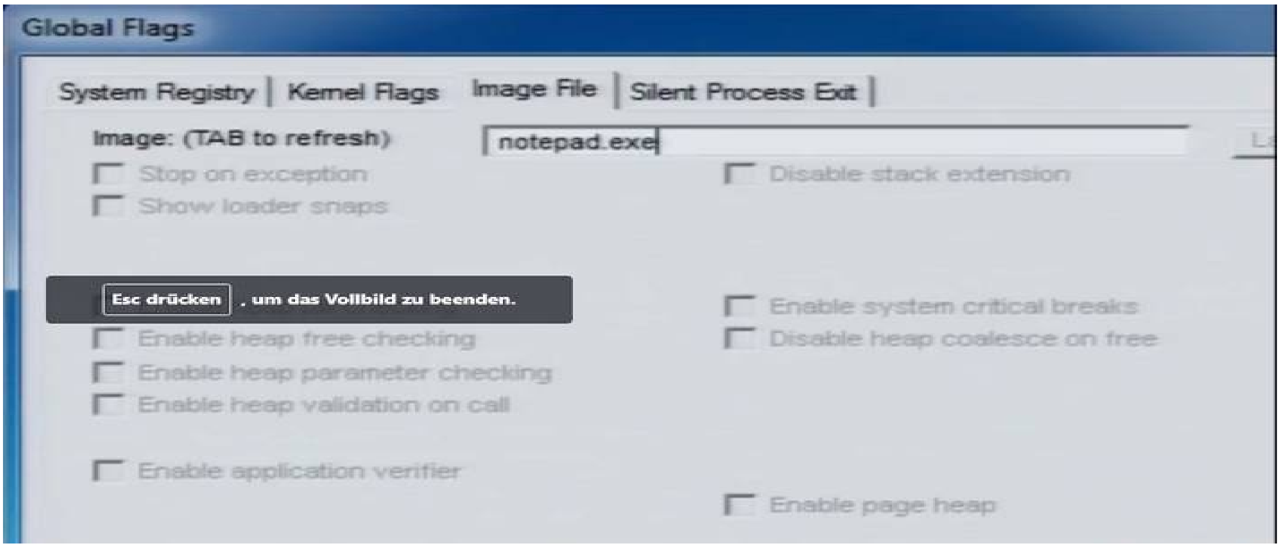
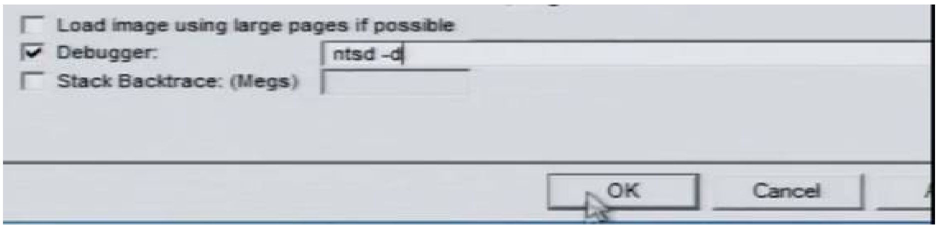

Global Flags
System Registry | Kernel Flags | Image File | Silent Process Exit
Esc drücken , um das Vollbild zu beenden.

Image: (TAB to refresh) notepad.exe

□ Stop on exception
□ Show loader snaps
□ Enable heap free checking
□ Enable heap parameter checking
□ Enable heap validation on call
□ Enable application verifier
□ Disable stack extension
□ Enable system critical breaks
□ Disable heap coalesce on free
□ Enable page heap



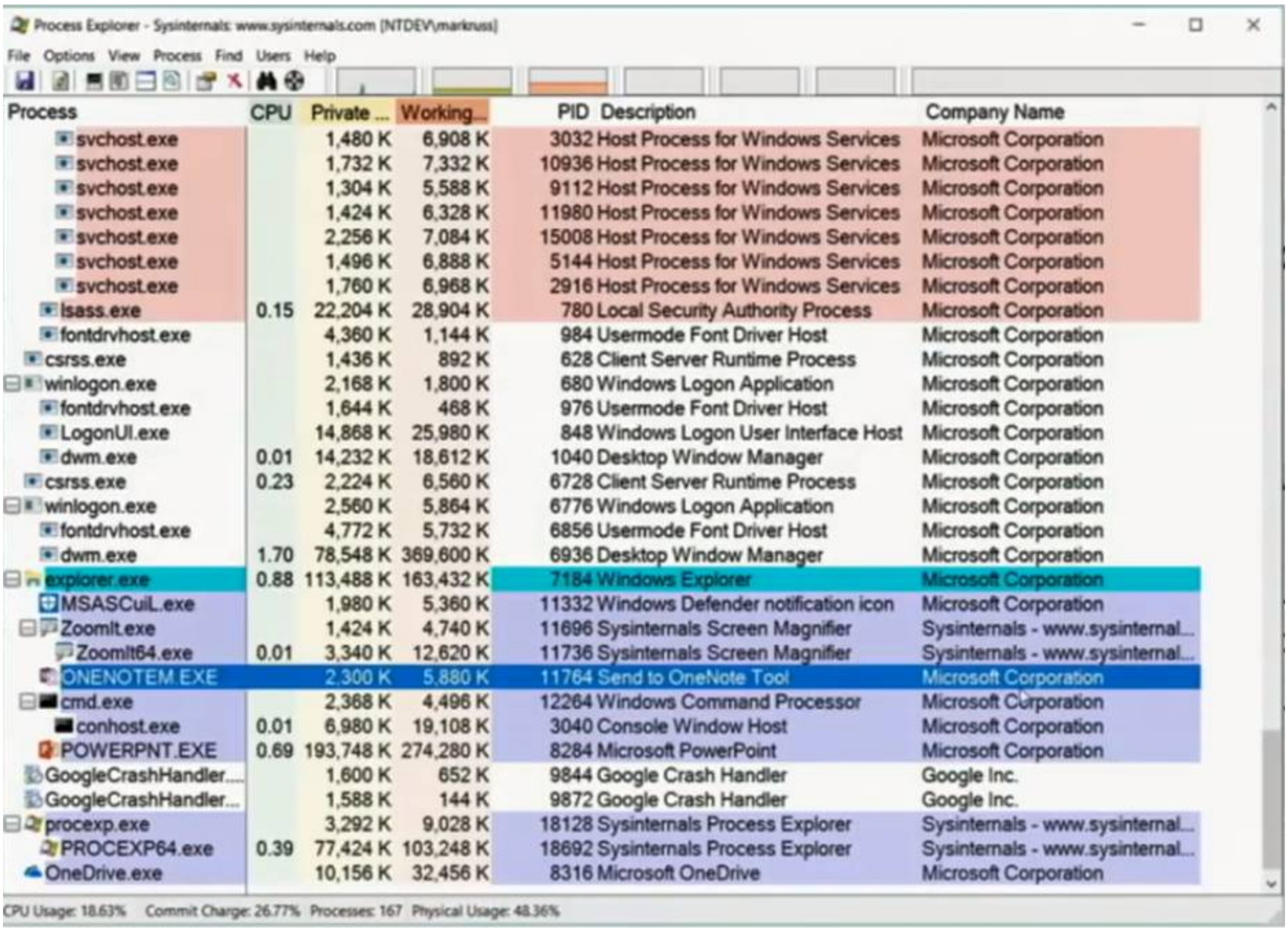
□ Load image using large pages if possible
☑ Debugger: ntsd -d
□ Stack Backtrace: (Megs)

WinDbg – Important Commands in short Overview

g - go	go start the program which is debugged
qd - quite detach	quite detach the debugged programm without close them (important for debugging server)
r – registry values	show register values
?	Change the value into decimal code
db – display bytes	display bytes of specific address include ASCII values
dc - display in bit counter	display in bit counter include ASCII values
~ - Tilde	show number and information of threads
k – kernel thread	show stack information of one kernel thread
~* - Tilde / Star e.g ~*k for kernel thread information	show stack information of all threads (compare e.g xarg by Linux) e.g ~*k or ~k76 (Threadnumber)
lm - list loaded modules	list loaded modules inside this space
v - verbose	verbose information / most information it can find
m - matching results	matching results into one big output
Machting to one command	example: lm v m malware
!peb – process environment block	displays the information of the process environment block (peb)

Troubelshooting with Process Explorer

Process Explorer is part of the sysinternal tools of windows.



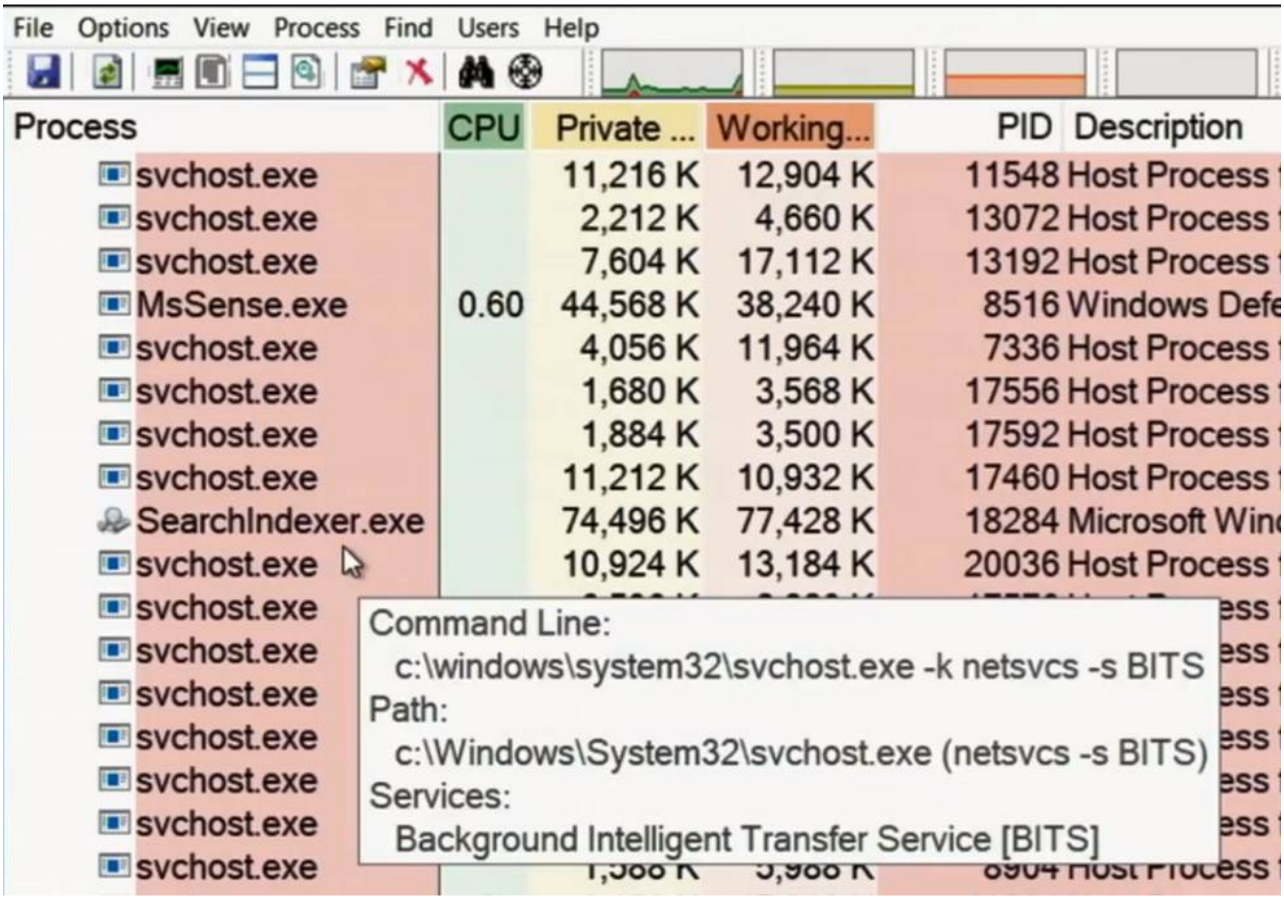
Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markruss]
File Options View Process Find Users Help

Process	CPU	Private ...	Working...	PID	Description	Company Name
svchost.exe		1,480 K	6,908 K	3032	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,732 K	7,332 K	10936	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,304 K	5,588 K	9112	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,424 K	6,328 K	11980	Host Process for Windows Services	Microsoft Corporation
svchost.exe		2,256 K	7,084 K	15008	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,496 K	6,888 K	5144	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,760 K	6,968 K	2916	Host Process for Windows Services	Microsoft Corporation
lsass.exe	0.15	22,204 K	28,904 K	780	Local Security Authority Process	Microsoft Corporation
fontdrvhost.exe		4,360 K	1,144 K	984	Usermode Font Driver Host	Microsoft Corporation
csrss.exe		1,436 K	892 K	628	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,168 K	1,800 K	680	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		1,644 K	468 K	976	Usermode Font Driver Host	Microsoft Corporation
LogonUI.exe		14,868 K	25,980 K	848	Windows Logon User Interface Host	Microsoft Corporation
dwm.exe	0.01	14,232 K	18,612 K	1040	Desktop Window Manager	Microsoft Corporation
csrss.exe	0.23	2,224 K	6,560 K	6728	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,560 K	5,864 K	6776	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		4,772 K	5,732 K	6856	Usermode Font Driver Host	Microsoft Corporation
dwm.exe	1.70	78,548 K	369,600 K	6936	Desktop Window Manager	Microsoft Corporation
explorer.exe	0.88	113,488 K	163,432 K	7184	Windows Explorer	Microsoft Corporation
MSASCuiL.exe		1,980 K	5,360 K	11332	Windows Defender notification icon	Microsoft Corporation
ZoomIt.exe		1,424 K	4,740 K	11696	Sysinternals Screen Magnifier	Sysinternals - www.sysinternal...
ZoomIt64.exe	0.01	3,340 K	12,620 K	11736	Sysinternals Screen Magnifier	Sysinternals - www.sysinternal...
ONENOTEM.EXE		2,300 K	5,880 K	11764	Send to OneNote Tool	Microsoft Corporation
cmd.exe		2,368 K	4,496 K	12264	Windows Command Processor	Microsoft Corporation
conhost.exe	0.01	6,980 K	19,108 K	3040	Console Window Host	Microsoft Corporation
POWERPNT.EXE	0.69	193,748 K	274,280 K	8284	Microsoft PowerPoint	Microsoft Corporation
GoogleCrashHandler....		1,600 K	652 K	9844	Google Crash Handler	Google Inc.
GoogleCrashHandler...		1,588 K	144 K	9872	Google Crash Handler	Google Inc.
procexp.exe		3,292 K	9,028 K	18128	Sysinternals Process Explorer	Sysinternals - www.sysinternal...
PROCEXP64.exe	0.39	77,424 K	103,248 K	18692	Sysinternals Process Explorer	Sysinternals - www.sysinternal...
OneDrive.exe		10,156 K	32,456 K	8316	Microsoft OneDrive	Microsoft Corporation

CPU Usage: 18.63% Commit Charge: 26.77% Processes: 167 Physical Usage: 48.36%

Process Explorer is called the super taskmanager because he displays very detailed information about currently running processes and futher information. The following Options are of important interest:

By scrolling over a specific process with the mouse it shows the command line command include the name of the program which is running inside them.



Process	CPU	Private ...	Working...	PID	Description
svchost.exe		11,216 K	12,904 K	11548	Host Process
svchost.exe		2,212 K	4,660 K	13072	Host Process
svchost.exe		7,604 K	17,112 K	13192	Host Process
MsSense.exe	0.60	44,568 K	38,240 K	8516	Windows Defe
svchost.exe		4,056 K	11,964 K	7336	Host Process
svchost.exe		1,680 K	3,568 K	17556	Host Process
svchost.exe		1,884 K	3,500 K	17592	Host Process
svchost.exe		11,212 K	10,932 K	17460	Host Process
SearchIndexer.exe		74,496 K	77,428 K	18284	Microsoft Win
svchost.exe		10,924 K	13,184 K	20036	Host Process
svchost.exe					ess
svchost.exe					ess
svchost.exe					ess
svchost.exe					ess
svchost.exe					ess
svchost.exe					ess
svchost.exe					

Command Line:
c:\windows\system32\svchost.exe -k netsvcs -s BITS
Path:
c:\Windows\System32\svchost.exe (netsvcs -s BITS)
Services:
Background Intelligent Transfer Service [BITS]

By double clicking to a process a window with detailed overview is open.

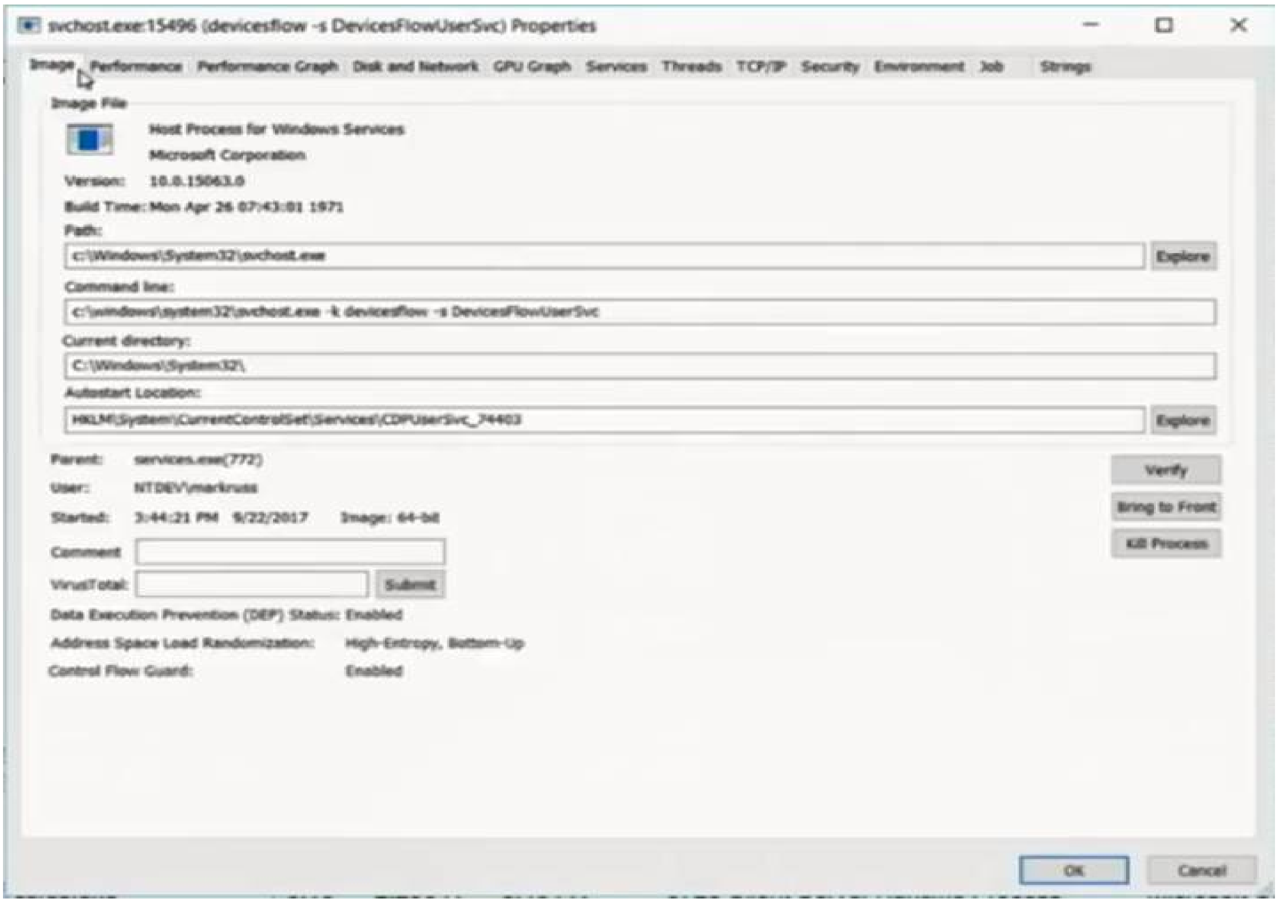

svchost.exe:15496 (devicesflow -s DevicesFlowUserSvc) Properties

Image File

Host Process for Windows Services
Microsoft Corporation

Version: 10.0.15063.0

Build Time: Mon Apr 26 07:43:01 1971

Path:
c:\Windows\System32\svchost.exe

Command line:
c:\windows\system32\svchost.exe -k devicesflow -s DevicesFlowUserSvc

Current directory:
C:\Windows\System32\

Autostart Location:
HKLM\System\CurrentControlSet\Services\CDPUserSvc_74403

Parent: services.exe(772)

User: NTDEV\markruss

Started: 3:44:21 PM 9/22/2017 Image: 64-bit

Comment:

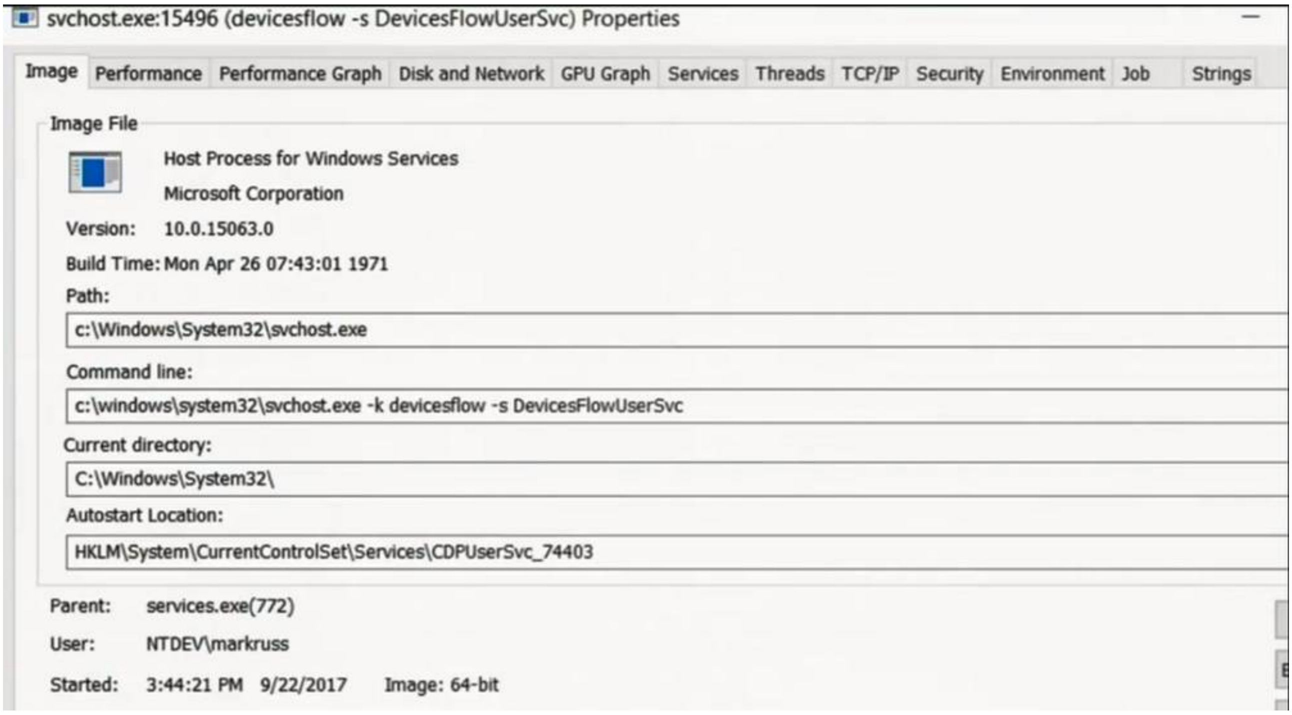
VirusTotal:

Data Execution Prevention (DEP) Status: Enabled

Address Space Load Randomization: High-Entropy, Bottom-Up

Control Flow Guard: Enabled

The important windows are:



Host Process for Windows Services

Microsoft Corporation

Version: 10.0.15063.0

Build Time: Mon Apr 26 07:43:01 1971

Path:

c:\Windows\System32\svchost.exe

Command line:

c:\windows\system32\svchost.exe -k devicesflow -s DevicesFlowUserSvc

Current directory:

C:\Windows\System32\

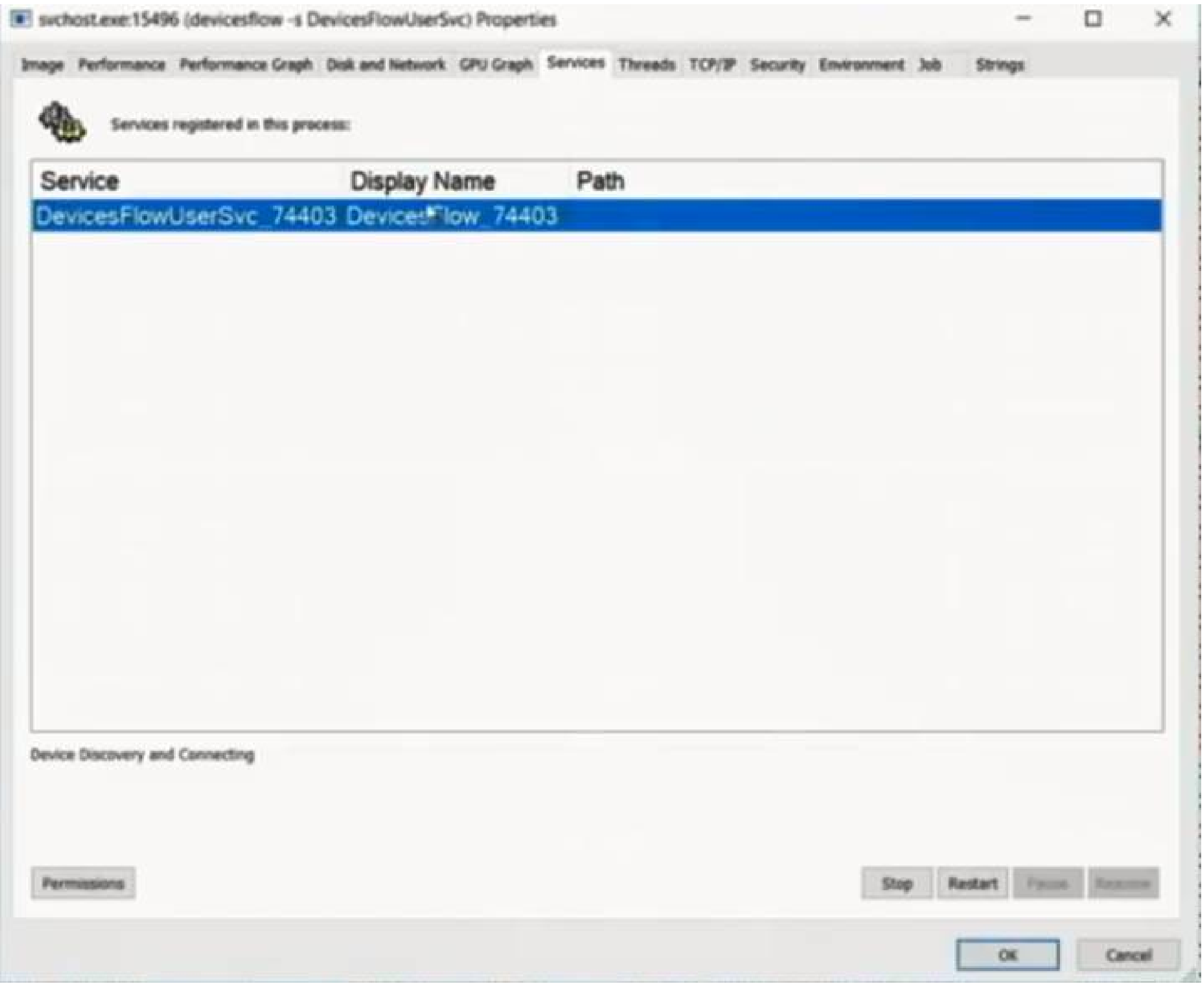
Autostart Location:

HKLM\System\CurrentControlSet\Services\CDPUserSvc_74403

Parent: services.exe(772)

User: NTDEV\markruss

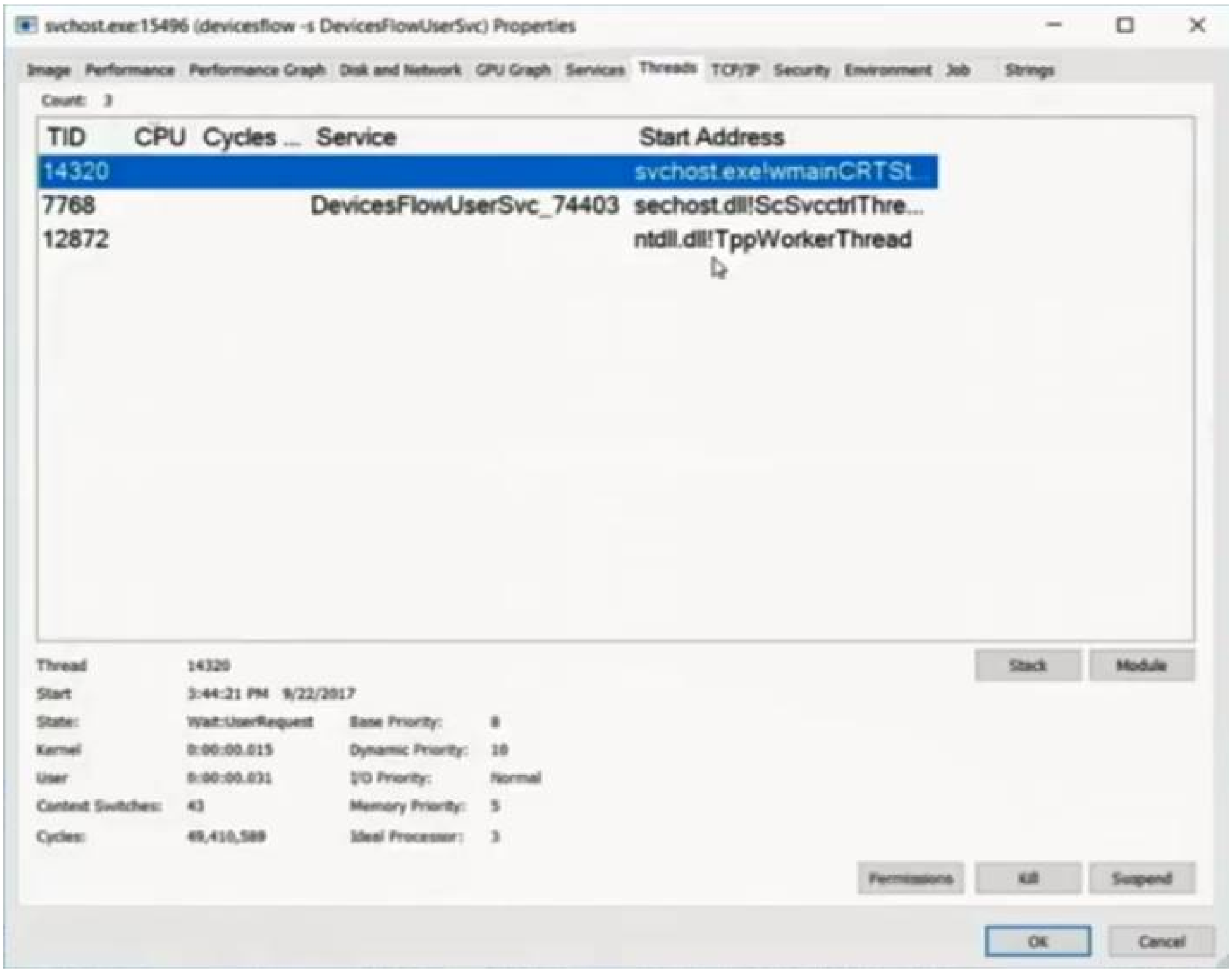
Started: 3:44:21 PM 9/22/2017 Image: 64-bit



Services registered in this process:

Service	Display Name	Path
DevicesFlowUserSvc_74403	DevicesFlow_74403	

Device Discovery and Connecting



svchost.exe:15496 (devicesflow -s DevicesFlowUserSvc) Properties

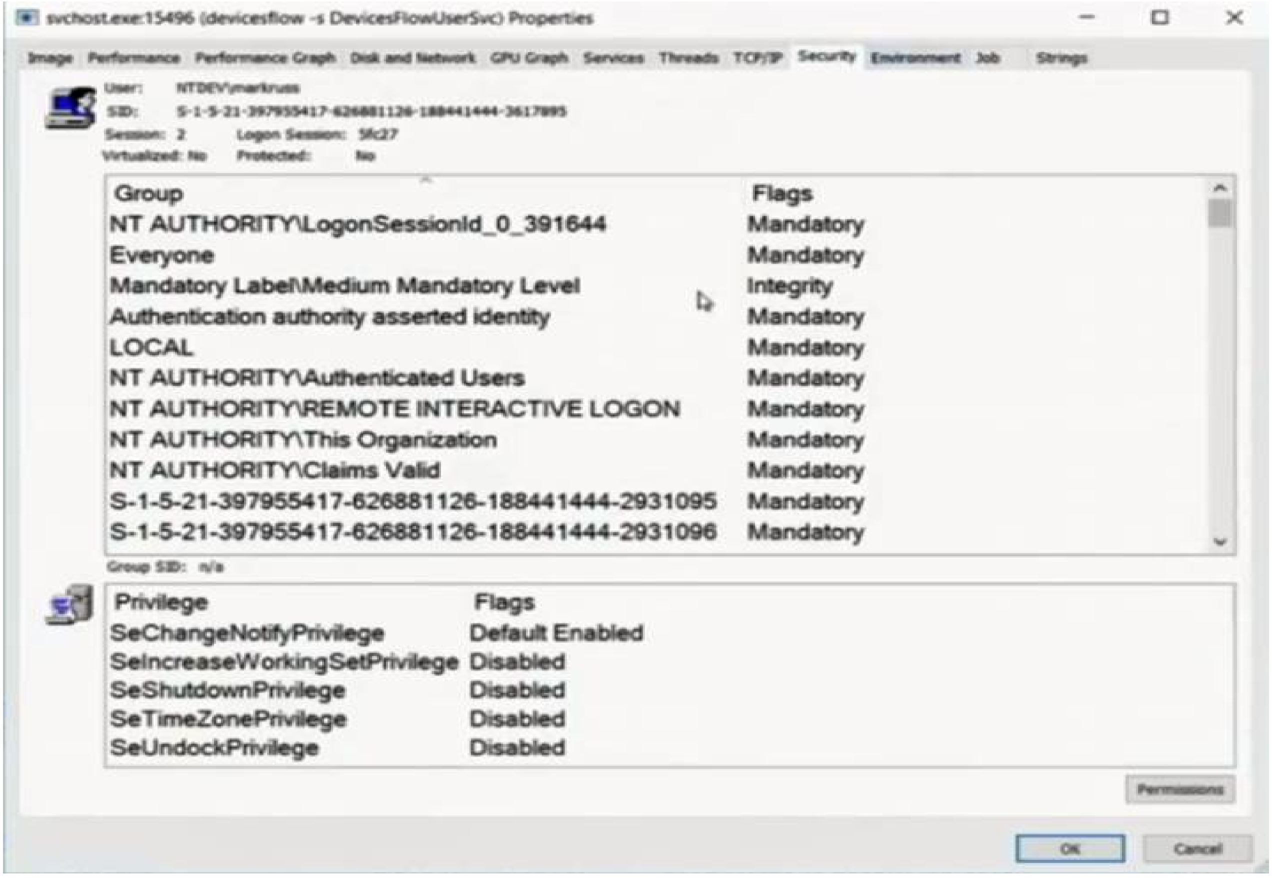
Count: 3

TID	CPU	Cycles ...	Service	Start Address
14320				svchost.exe!wmainCRTSt...
7768			DevicesFlowUserSvc_74403	sechost.dll!ScSvcctrlThre...
12872				ntdll.dll!TppWorkerThread

Thread 14320

Start 3:44:21 PM 9/22/2017

State:	Wait:UserRequest	Base Priority:	8
Kernel	0:00:00.015	Dynamic Priority:	10
User	0:00:00.031	I/O Priority:	Normal
Context Switches:	43	Memory Priority:	5
Cycles:	49,410,589	Ideal Processor:	3



svchost.exe:15496 (devicesflow -s DevicesFlowUserSvc) Properties

User: NTDEV\markruss

SID: S-1-5-21-397955417-626881126-188441444-3617895

Session: 2 Logon Session: 5fc27

Virtualized: No Protected: No

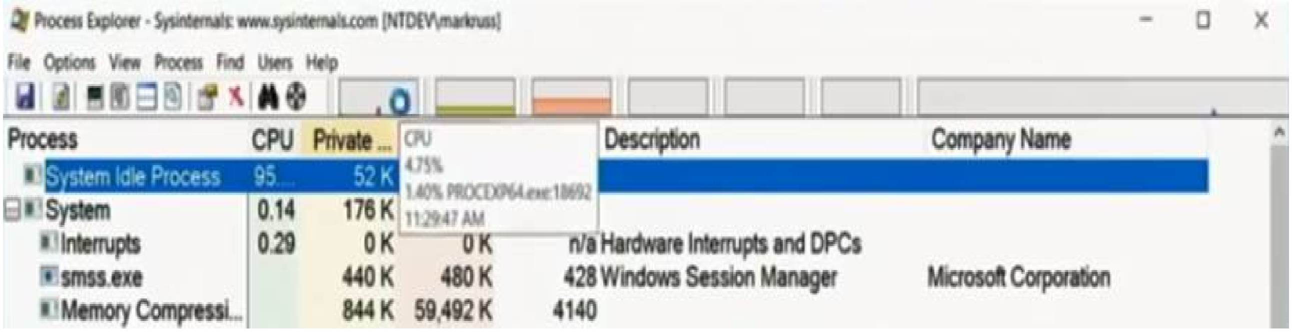
Group	Flags
NT AUTHORITY\LogonSessionId_0_391644	Mandatory
Everyone	Mandatory
Mandatory Label\Medium Mandatory Level	Integrity
Authentication authority asserted identity	Mandatory
LOCAL	Mandatory
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\REMOTE INTERACTIVE LOGON	Mandatory
NT AUTHORITY\This Organization	Mandatory
NT AUTHORITY\Claims Valid	Mandatory
S-1-5-21-397955417-626881126-188441444-2931095	Mandatory
S-1-5-21-397955417-626881126-188441444-2931096	Mandatory

Group SID: n/a

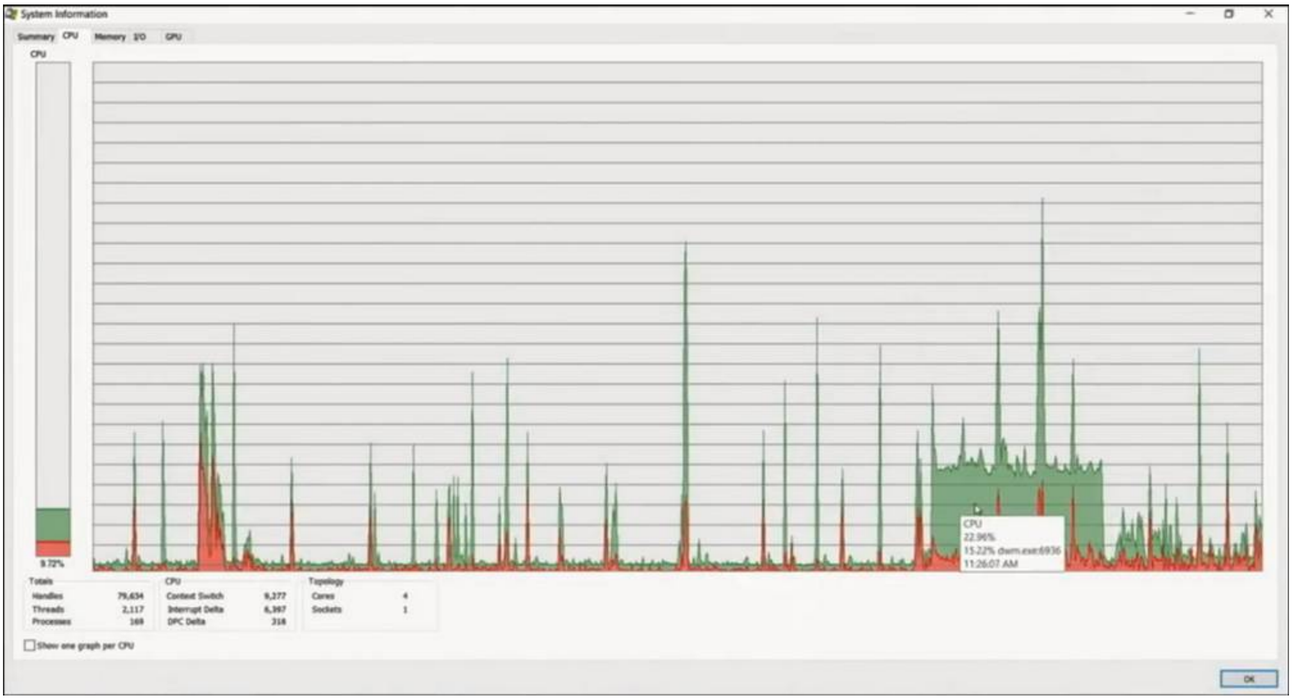
Privilege	Flags
SeChangeNotifyPrivilege	Default Enabled
SeIncreaseWorkingSetPrivilege	Disabled
SeShutdownPrivilege	Disabled
SeTimeZonePrivilege	Disabled
SeUndockPrivilege	Disabled

So the important windows of interest are Image, Services, Threads, Security, Environment Variables and Strings.

By double click to one of the graphical monitoring blocks on the top of the process explorer it open a window which shows the different processes with the name and marked in diffrent colors


Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markruss]
File Options View Process Find Users Help
CPU
4.75%
1.40% PROCEXP64.exe:18692
11:29:47 AM

Process	CPU	Private ...			Description	Company Name
System Idle Process	95...	52 K				
System	0.14	176 K				
Interrupts	0.29	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		440 K	480 K	428	Windows Session Manager	Microsoft Corporation
Memory Compressi...		844 K	59,492 K	4140		



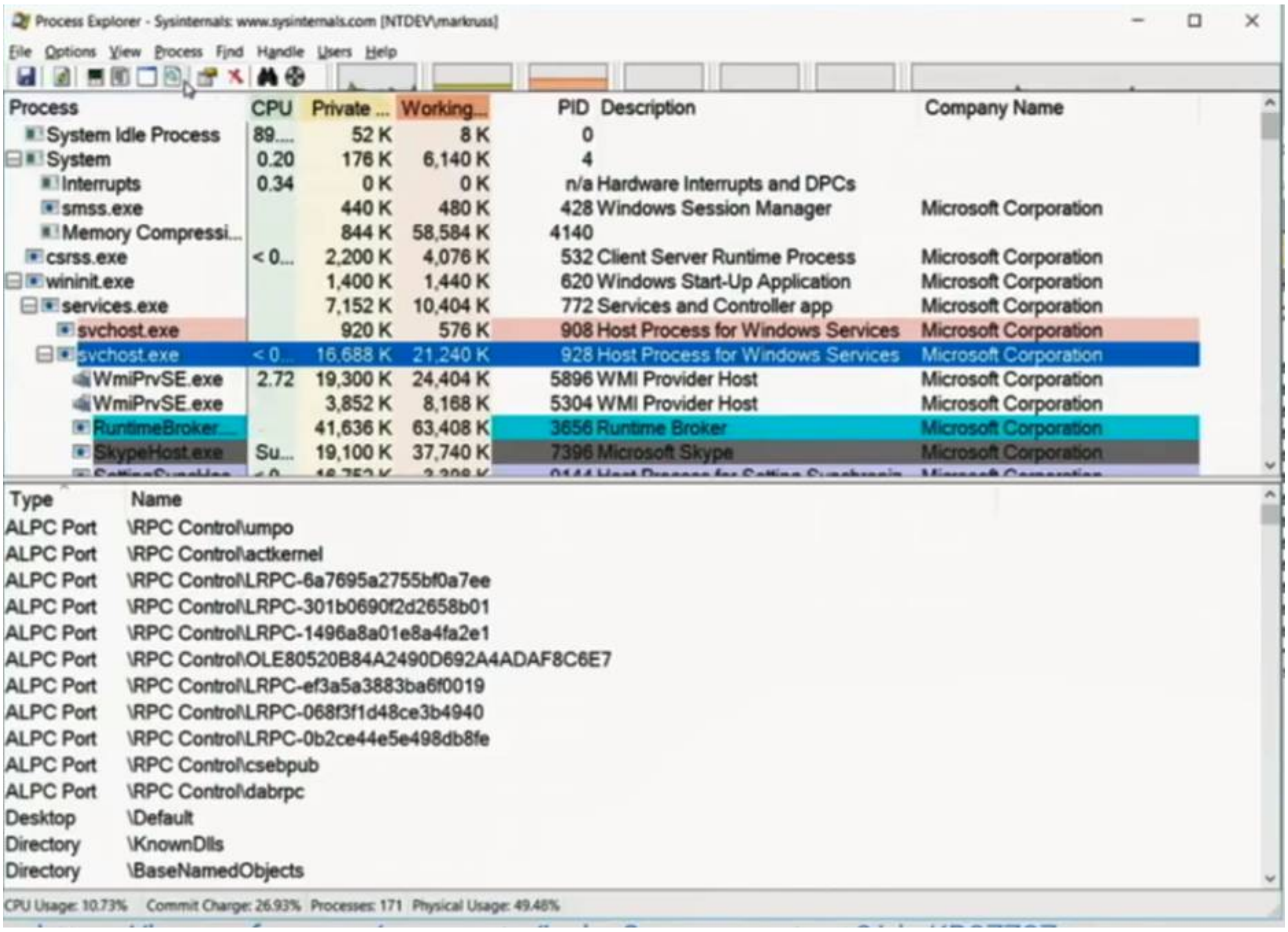
Totals
Handles 79,634
Threads 2,117
Processes 169

CPU
Context Switch 9,277
Interrupt Delta 6,397
DPC Delta 318

Topology
Cores 4
Sockets 1

□ Show one graph per CPU

By clicking in the process explorer of one of the symbols of the middle right top you can switch between the active kernel ressources and the dll file resources view.



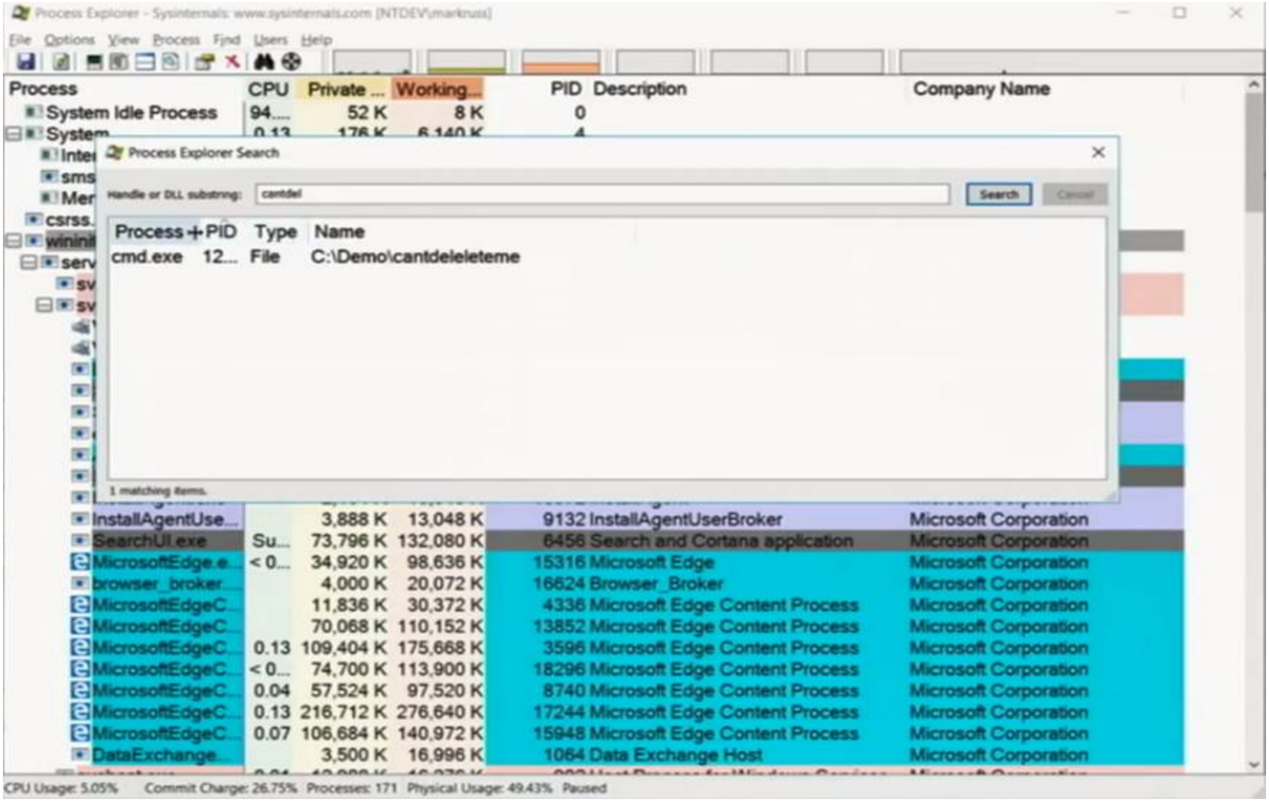
Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markruss]

Process	CPU	Private ...	Working...	PID	Description	Company Name
System Idle Process	89....	52 K	8 K	0		
System	0.20	176 K	6,140 K	4		
Interrupts	0.34	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		440 K	480 K	428	Windows Session Manager	Microsoft Corporation
Memory Compressi...		844 K	58,584 K	4140		
csrss.exe	< 0...	2,200 K	4,076 K	532	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,400 K	1,440 K	620	Windows Start-Up Application	Microsoft Corporation
services.exe		7,152 K	10,404 K	772	Services and Controller app	Microsoft Corporation
svchost.exe		920 K	576 K	908	Host Process for Windows Services	Microsoft Corporation
svchost.exe	< 0...	16,688 K	21,240 K	928	Host Process for Windows Services	Microsoft Corporation
WmiPrvSE.exe	2.72	19,300 K	24,404 K	5896	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		3,852 K	8,168 K	5304	WMI Provider Host	Microsoft Corporation
RuntimeBroker...		41,636 K	63,408 K	3656	Runtime Broker	Microsoft Corporation
SkypeHost.exe	Su...	19,100 K	37,740 K	7396	Microsoft Skype	Microsoft Corporation

Type	Name
ALPC Port	\RPC Control\umpo
ALPC Port	\RPC Control\actkernel
ALPC Port	\RPC Control\LRPC-6a7695a2755bf0a7ee
ALPC Port	\RPC Control\LRPC-301b0690f2d2658b01
ALPC Port	\RPC Control\LRPC-1496a8a01e8a4fa2e1
ALPC Port	\RPC Control\OLE80520B84A2490D692A4ADAF8C6E7
ALPC Port	\RPC Control\LRPC-ef3a5a3883ba6f0019
ALPC Port	\RPC Control\LRPC-068f3f1d48ce3b4940
ALPC Port	\RPC Control\LRPC-0b2ce44e5e498db8fe
ALPC Port	\RPC Control\csebpub
ALPC Port	\RPC Control\dabrpc
Desktop	\Default
Directory	\KnownDlls
Directory	\BaseNamedObjects

CPU Usage: 10.73% Commit Charge: 26.93% Processes: 171 Physical Usage: 49.48%

Clicking on the telescope button it opens a search bar which you can search for different matches for the current problem. So it scan the complete bunch in process explorer for that and shows the matched results. By double clicking the result it jumps into details.



Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markruss]

Process Explorer Search

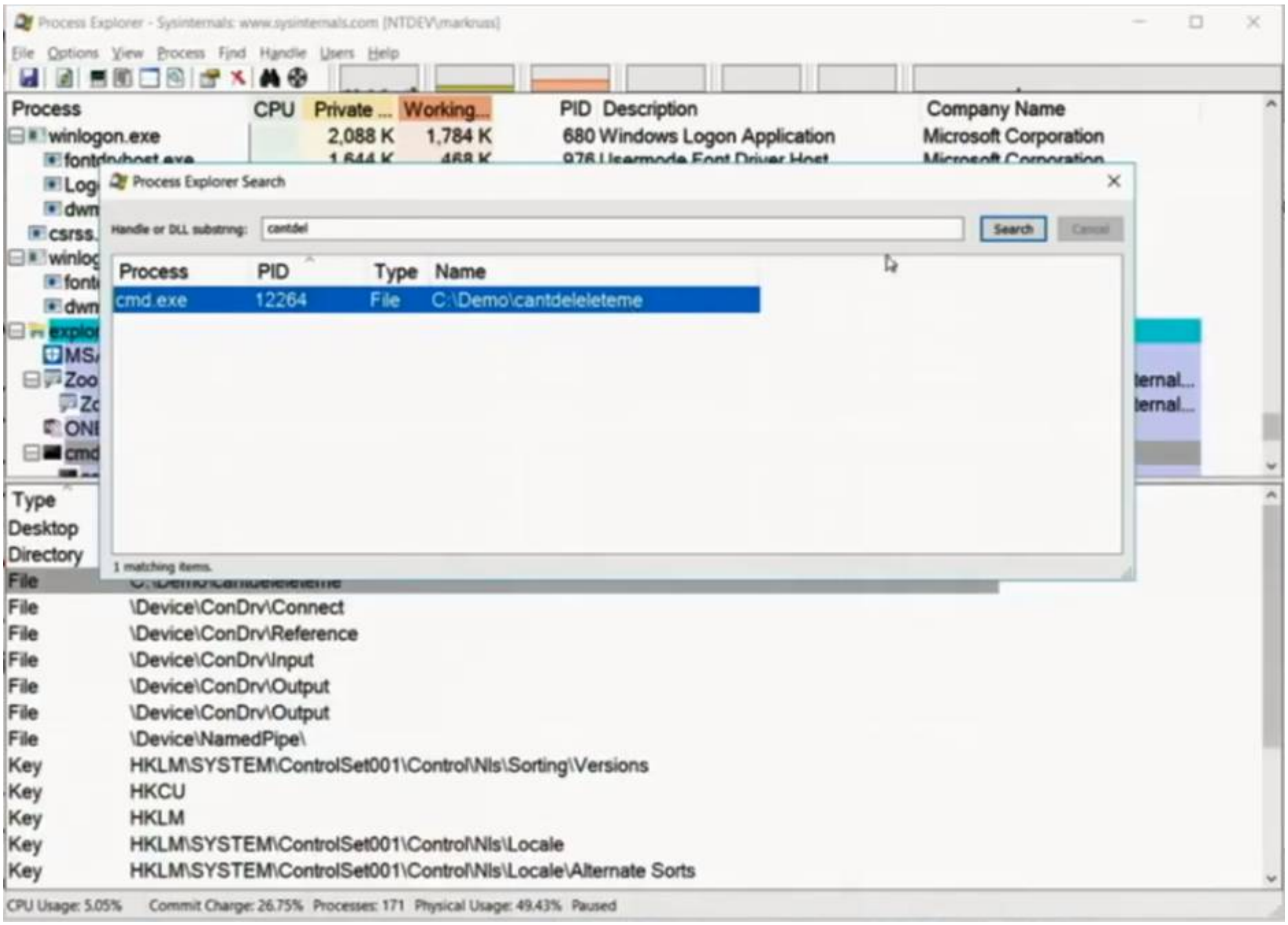
Handle or DLL substring: cantdel

Process	PID	Type	Name
cmd.exe	12...	File	C:\Demo\cantdeleleteme

1 matching items.

Process	CPU	Private ...	Working...	PID	Description	Company Name
System Idle Process	94....	52 K	8 K	0		
InstallAgentUse...		3,888 K	13,048 K	9132	InstallAgentUserBroker	Microsoft Corporation
SearchUI.exe	Su...	73,796 K	132,080 K	6456	Search and Cortana application	Microsoft Corporation
MicrosoftEdge.e...	< 0...	34,920 K	98,636 K	15316	Microsoft Edge	Microsoft Corporation
browser_broker...		4,000 K	20,072 K	16624	Browser_Broker	Microsoft Corporation
MicrosoftEdgeC...		11,836 K	30,372 K	4336	Microsoft Edge Content Process	Microsoft Corporation
MicrosoftEdgeC...		70,068 K	110,152 K	13852	Microsoft Edge Content Process	Microsoft Corporation
MicrosoftEdgeC...	0.13	109,404 K	175,668 K	3596	Microsoft Edge Content Process	Microsoft Corporation
MicrosoftEdgeC...	< 0...	74,700 K	113,900 K	18296	Microsoft Edge Content Process	Microsoft Corporation
MicrosoftEdgeC...	0.04	57,524 K	97,520 K	8740	Microsoft Edge Content Process	Microsoft Corporation
MicrosoftEdgeC...	0.13	216,712 K	276,640 K	17244	Microsoft Edge Content Process	Microsoft Corporation
MicrosoftEdgeC...	0.07	106,684 K	140,972 K	15948	Microsoft Edge Content Process	Microsoft Corporation
DataExchange...		3,500 K	16,996 K	1064	Data Exchange Host	Microsoft Corporation

CPU Usage: 5.05% Commit Charge: 26.75% Processes: 171 Physical Usage: 49.43% Paused


Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markruss]
File Options View Process Find Handle Users Help
Process Explorer Search
Handle or DLL substring:
Search
Cancel

Handle or DLL substring: cantdel

Process	PID	Type	Name
cmd.exe	12264	File	C:\Demo\cantdeleleteme

1 matching items.

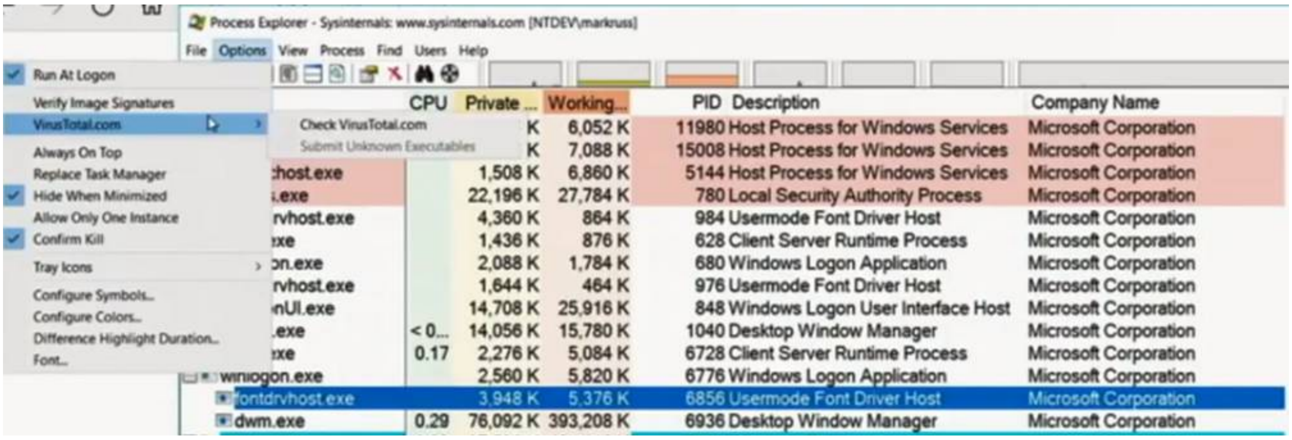
Process	CPU	Private ...	Working...	PID	Description	Company Name
winlogon.exe		2,088 K	1,784 K	680	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		1,644 K	468 K	976	Usermode Font Driver Host	Microsoft Corporation

Type	Name
Desktop	
Directory	
File	C:\Demo\cantdeleleteme
File	\Device\ConDrv\Connect
File	\Device\ConDrv\Reference
File	\Device\ConDrv\Input
File	\Device\ConDrv\Output
File	\Device\ConDrv\Output
File	\Device\NamedPipe\
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale\Alternate Sorts

CPU Usage: 5.05% Commit Charge: 26.75% Processes: 171 Physical Usage: 49.43% Paused

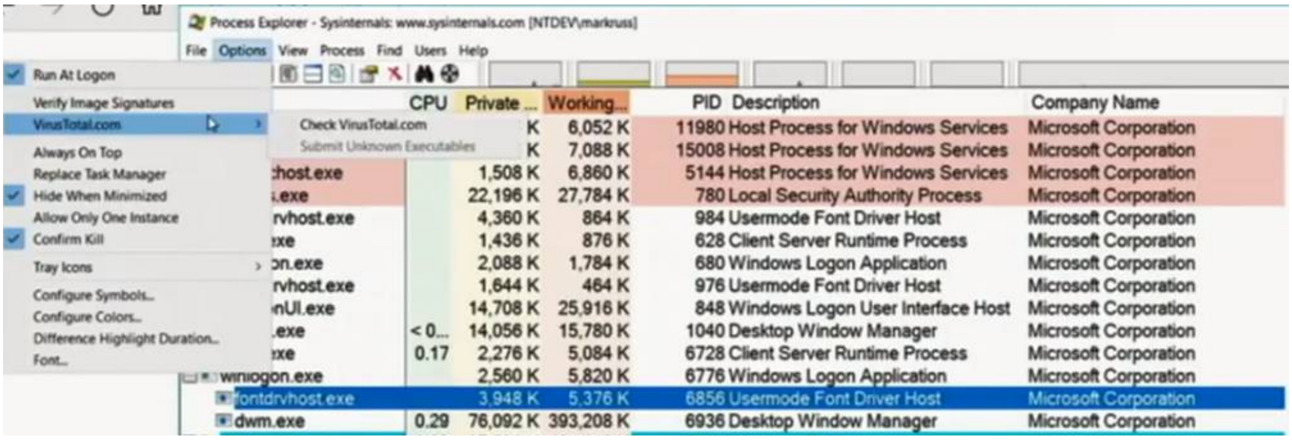
Use Process Explorer to find Malware

You can also search for malware use the integrated virus total check (internet connection required). Therefore use the Options register.

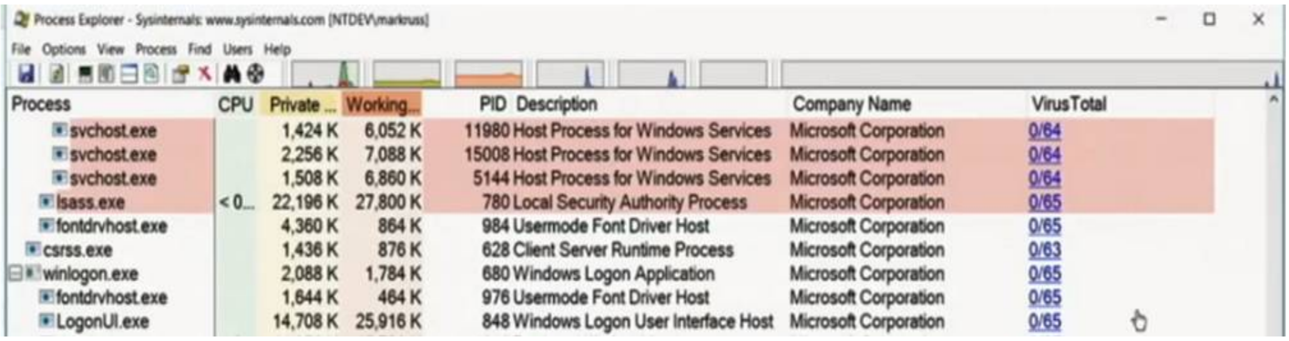


Process	CPU	Private ...	Working...	PID	Description	Company Name
		K	6,052 K	11980	Host Process for Windows Services	Microsoft Corporation
		K	7,088 K	15008	Host Process for Windows Services	Microsoft Corporation
...chost.exe		1,508 K	6,860 K	5144	Host Process for Windows Services	Microsoft Corporation
....exe		22,196 K	27,784 K	780	Local Security Authority Process	Microsoft Corporation
...rvhost.exe		4,360 K	864 K	984	Usermode Font Driver Host	Microsoft Corporation
...xe		1,436 K	876 K	628	Client Server Runtime Process	Microsoft Corporation
...on.exe		2,088 K	1,784 K	680	Windows Logon Application	Microsoft Corporation
...rvhost.exe		1,644 K	464 K	976	Usermode Font Driver Host	Microsoft Corporation
...nUI.exe		14,708 K	25,916 K	848	Windows Logon User Interface Host	Microsoft Corporation
....exe	< 0...	14,056 K	15,780 K	1040	Desktop Window Manager	Microsoft Corporation
...xe	0.17	2,276 K	5,084 K	6728	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,560 K	5,820 K	6776	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		3,948 K	5,376 K	6856	Usermode Font Driver Host	Microsoft Corporation
dwm.exe	0.29	76,092 K	393,208 K	6936	Desktop Window Manager	Microsoft Corporation

After that hashes of the process files will be uploaded to virus total and checked. So the results will be displayed in process explorer as a new field. A match which is up to 10 or more virus engines are highly sure malware.

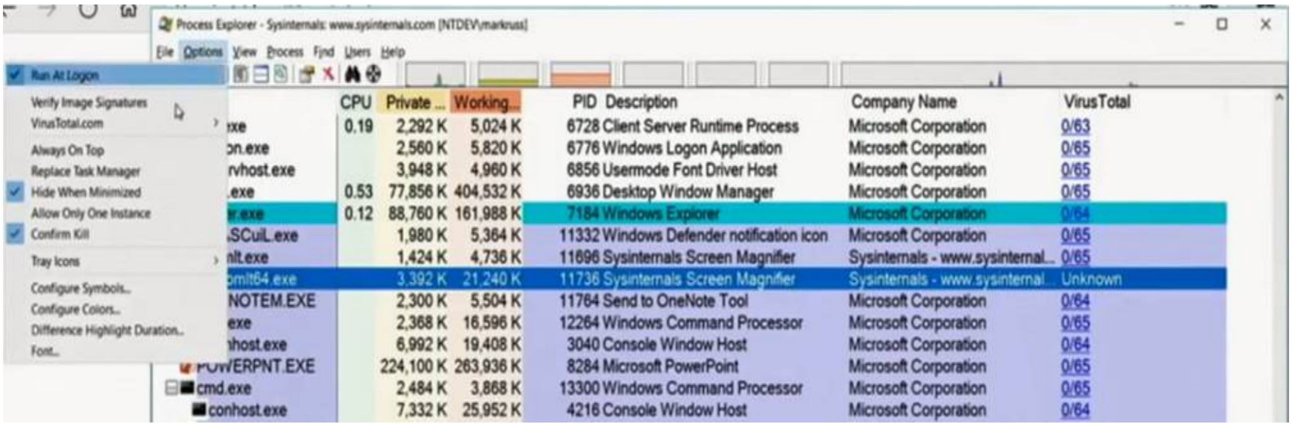


	CPU	Private ...	Working...	PID	Description	Company Name
		K	6,052 K	11980	Host Process for Windows Services	Microsoft Corporation
		K	7,088 K	15008	Host Process for Windows Services	Microsoft Corporation
chost.exe		1,508 K	6,860 K	5144	Host Process for Windows Services	Microsoft Corporation
.exe		22,196 K	27,784 K	780	Local Security Authority Process	Microsoft Corporation
rvhost.exe		4,360 K	864 K	984	Usermode Font Driver Host	Microsoft Corporation
xe		1,436 K	876 K	628	Client Server Runtime Process	Microsoft Corporation
on.exe		2,088 K	1,784 K	680	Windows Logon Application	Microsoft Corporation
rvhost.exe		1,644 K	464 K	976	Usermode Font Driver Host	Microsoft Corporation
nUI.exe		14,708 K	25,916 K	848	Windows Logon User Interface Host	Microsoft Corporation
.exe	< 0...	14,056 K	15,780 K	1040	Desktop Window Manager	Microsoft Corporation
xe	0.17	2,276 K	5,084 K	6728	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,560 K	5,820 K	6776	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		3,948 K	5,376 K	6856	Usermode Font Driver Host	Microsoft Corporation
dwm.exe	0.29	76,092 K	393,208 K	6936	Desktop Window Manager	Microsoft Corporation

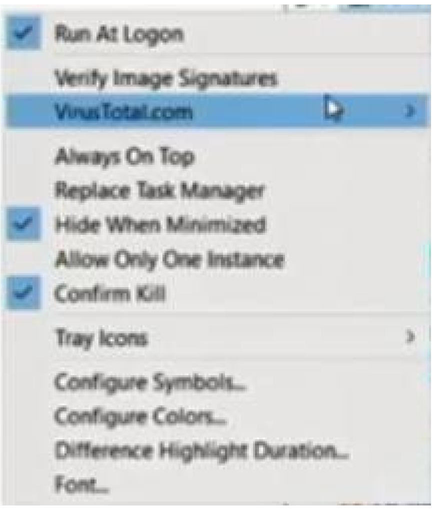

Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markruss]
File Options View Process Find Users Help

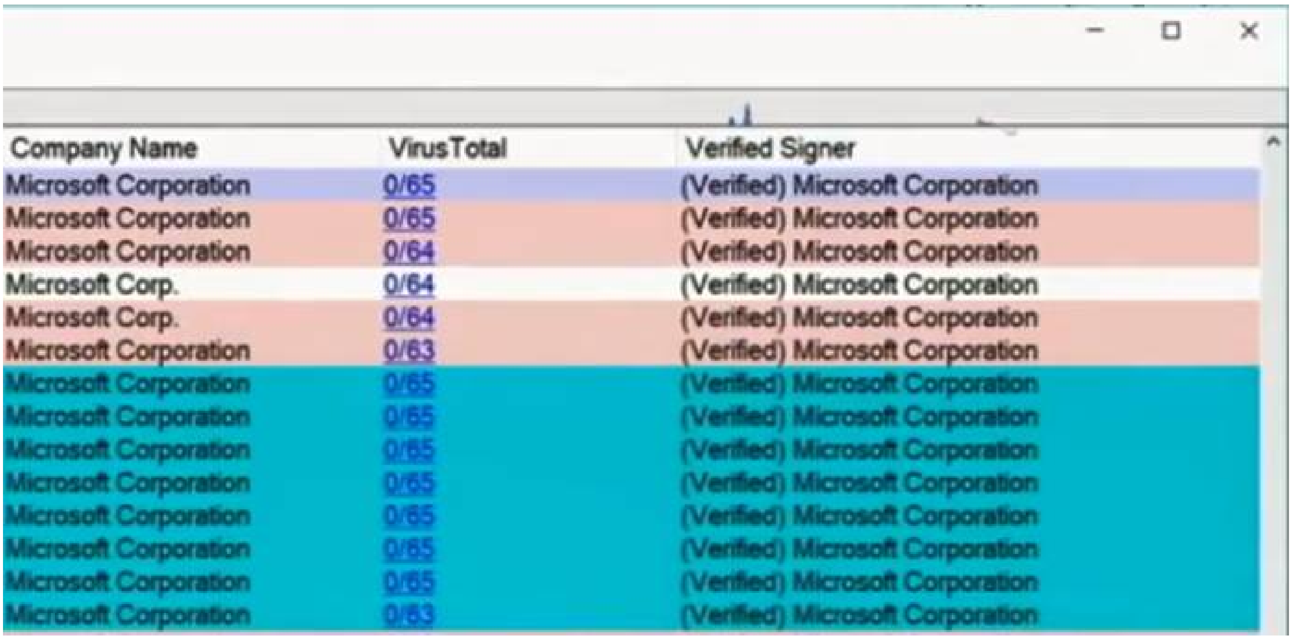
Process	CPU	Private ...	Working...	PID	Description	Company Name	VirusTotal
svchost.exe		1,424 K	6,052 K	11980	Host Process for Windows Services	Microsoft Corporation	0/64
svchost.exe		2,256 K	7,088 K	15008	Host Process for Windows Services	Microsoft Corporation	0/64
svchost.exe		1,508 K	6,860 K	5144	Host Process for Windows Services	Microsoft Corporation	0/64
lsass.exe	< 0...	22,196 K	27,800 K	780	Local Security Authority Process	Microsoft Corporation	0/65
fontdrvhost.exe		4,360 K	864 K	984	Usermode Font Driver Host	Microsoft Corporation	0/65
csrss.exe		1,436 K	876 K	628	Client Server Runtime Process	Microsoft Corporation	0/63
winlogon.exe		2,088 K	1,784 K	680	Windows Logon Application	Microsoft Corporation	0/65
fontdrvhost.exe		1,644 K	464 K	976	Usermode Font Driver Host	Microsoft Corporation	0/65
LogonUI.exe		14,708 K	25,916 K	848	Windows Logon User Interface Host	Microsoft Corporation	0/65

A second option is added in the Option register for virus total called Verify Image Signatures which verify all signatures on the system showing in process explorer



	CPU	Private ...	Working...	PID	Description	Company Name	VirusTotal
xe	0.19	2,292 K	5,024 K	6728	Client Server Runtime Process	Microsoft Corporation	0/63
on.exe		2,560 K	5,820 K	6776	Windows Logon Application	Microsoft Corporation	0/65
rvhost.exe		3,948 K	4,960 K	6856	Usermode Font Driver Host	Microsoft Corporation	0/65
.exe	0.53	77,856 K	404,532 K	6936	Desktop Window Manager	Microsoft Corporation	0/65
r.exe	0.12	88,760 K	161,988 K	7184	Windows Explorer	Microsoft Corporation	0/64
SCuiL.exe		1,980 K	5,364 K	11332	Windows Defender notification icon	Microsoft Corporation	0/65
nlt.exe		1,424 K	4,736 K	11696	Sysinternals Screen Magnifier	Sysinternals - www.sysinternal...	0/65
omlt64.exe		3,392 K	21,240 K	11736	Sysinternals Screen Magnifier	Sysinternals - www.sysinternal...	Unknown
NOTEM.EXE		2,300 K	5,504 K	11764	Send to OneNote Tool	Microsoft Corporation	0/64
exe		2,368 K	16,596 K	12264	Windows Command Processor	Microsoft Corporation	0/65
host.exe		6,992 K	19,408 K	3040	Console Window Host	Microsoft Corporation	0/64
POWERPNT.EXE		224,100 K	263,936 K	8284	Microsoft PowerPoint	Microsoft Corporation	0/65
cmd.exe		2,484 K	3,868 K	13300	Windows Command Processor	Microsoft Corporation	0/65
conhost.exe		7,332 K	25,952 K	4216	Console Window Host	Microsoft Corporation	0/64

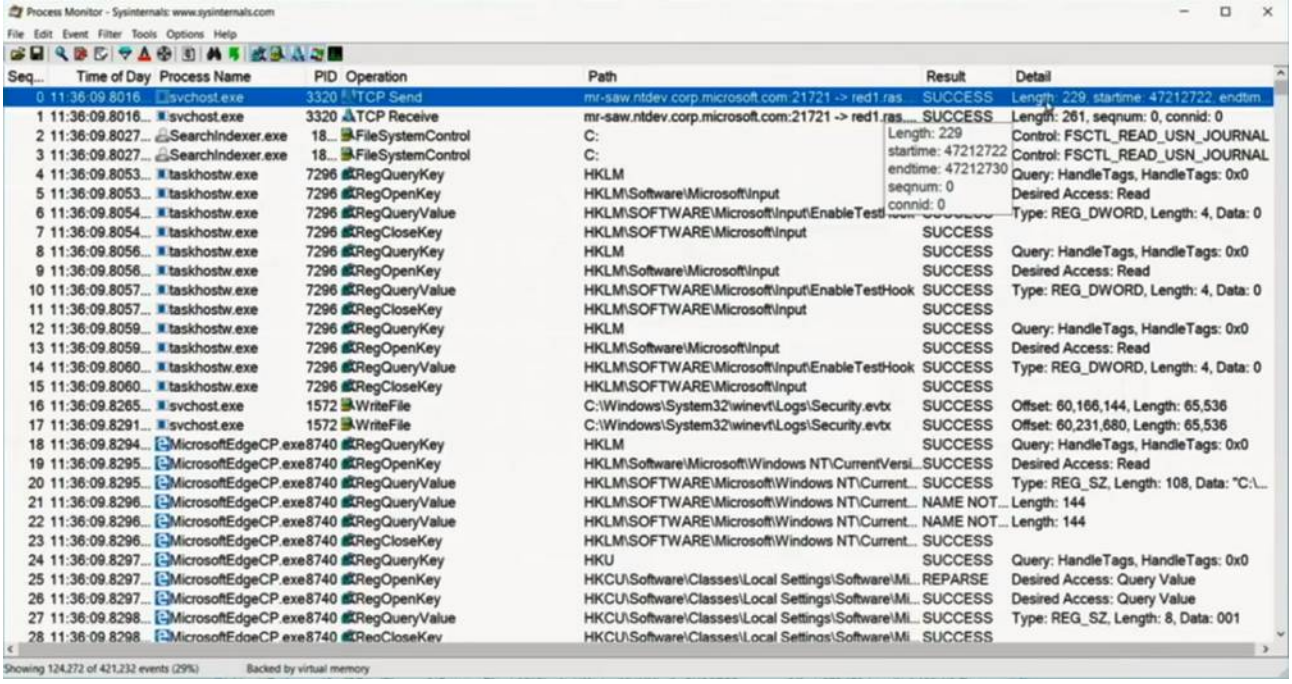




Company Name	VirusTotal	Verified Signer
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/64	(Verified) Microsoft Corporation
Microsoft Corp.	0/64	(Verified) Microsoft Corporation
Microsoft Corp.	0/64	(Verified) Microsoft Corporation
Microsoft Corporation	0/63	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/63	(Verified) Microsoft Corporation

Troubelshooting with Process Monitor (Procmon)

By starting process monitor it starts capturing every traffic on the system immediatly.

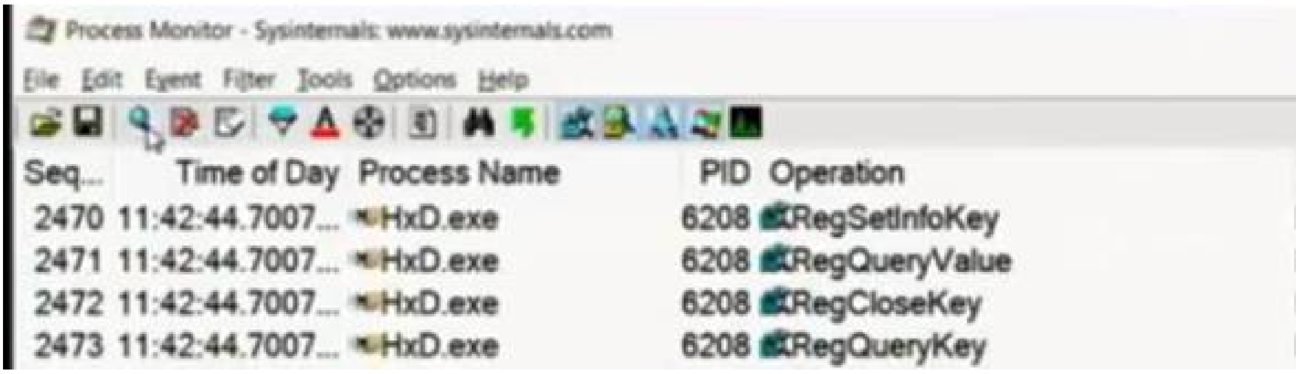

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Seq...	Time of Day	Process Name	PID	Operation	Path	Result	Detail
0	11:36:09.8016...	svchost.exe	3320	TCP Send	mr-saw.ntdev.corp.microsoft.com:21721 -> red1.ras...	SUCCESS	Length: 229, startime: 47212722, endtim...
1	11:36:09.8016...	svchost.exe	3320	TCP Receive	mr-saw.ntdev.corp.microsoft.com:21721 -> red1.ras...	SUCCESS	Length: 261, seqnum: 0, connid: 0
2	11:36:09.8027...	SearchIndexer.exe	18...	FileSystemControl	C:		Control: FSCTL_READ_USN_JOURNAL
3	11:36:09.8027...	SearchIndexer.exe	18...	FileSystemControl	C:		Control: FSCTL_READ_USN_JOURNAL
4	11:36:09.8053...	taskhostw.exe	7296	RegQueryKey	HKLM		Query: HandleTags, HandleTags: 0x0
5	11:36:09.8053...	taskhostw.exe	7296	RegOpenKey	HKLM\Software\Microsoft\Input		Desired Access: Read
6	11:36:09.8054...	taskhostw.exe	7296	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\EnableTest		Type: REG_DWORD, Length: 4, Data: 0
7	11:36:09.8054...	taskhostw.exe	7296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
8	11:36:09.8056...	taskhostw.exe	7296	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
9	11:36:09.8056...	taskhostw.exe	7296	RegOpenKey	HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
10	11:36:09.8057...	taskhostw.exe	7296	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11	11:36:09.8057...	taskhostw.exe	7296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
12	11:36:09.8059...	taskhostw.exe	7296	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
13	11:36:09.8059...	taskhostw.exe	7296	RegOpenKey	HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
14	11:36:09.8060...	taskhostw.exe	7296	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
15	11:36:09.8060...	taskhostw.exe	7296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
16	11:36:09.8265...	svchost.exe	1572	WriteFile	C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 60,166,144, Length: 65,536
17	11:36:09.8291...	svchost.exe	1572	WriteFile	C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 60,231,680, Length: 65,536
18	11:36:09.8294...	MicrosoftEdgeCP.exe	8740	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
19	11:36:09.8295...	MicrosoftEdgeCP.exe	8740	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersi...	SUCCESS	Desired Access: Read
20	11:36:09.8295...	MicrosoftEdgeCP.exe	8740	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	Type: REG_SZ, Length: 108, Data: "C:\...
21	11:36:09.8296...	MicrosoftEdgeCP.exe	8740	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
22	11:36:09.8296...	MicrosoftEdgeCP.exe	8740	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
23	11:36:09.8296...	MicrosoftEdgeCP.exe	8740	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	
24	11:36:09.8297...	MicrosoftEdgeCP.exe	8740	RegQueryKey	HKU	SUCCESS	Query: HandleTags, HandleTags: 0x0
25	11:36:09.8297...	MicrosoftEdgeCP.exe	8740	RegOpenKey	HKCU\Software\Classes\Local Settings\Software\Mi...	REPARSE	Desired Access: Query Value
26	11:36:09.8297...	MicrosoftEdgeCP.exe	8740	RegOpenKey	HKCU\Software\Classes\Local Settings\Software\Mi...	SUCCESS	Desired Access: Query Value
27	11:36:09.8298...	MicrosoftEdgeCP.exe	8740	RegQueryValue	HKCU\Software\Classes\Local Settings\Software\Mi...	SUCCESS	Type: REG_SZ, Length: 8, Data: 001
28	11:36:09.8298...	MicrosoftEdgeCP.exe	8740	RegCloseKey	HKCU\Software\Classes\Local Settings\Software\Mi...	SUCCESS	

Length: 229
startime: 47212722
endtime: 47212730
seqnum: 0
connid: 0

Showing 124,272 of 421,232 events (29%)   Backed by virtual memory

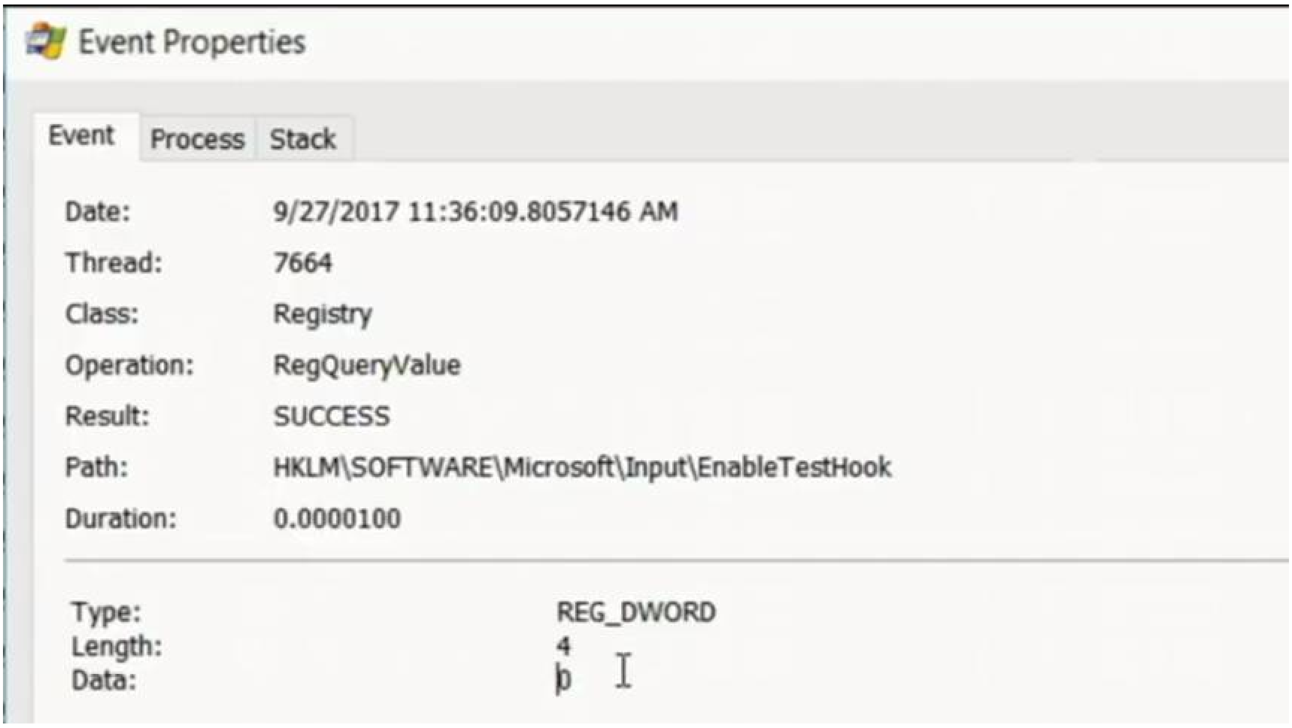
To stop process monitor to capture the traffic clicking on the search button on the top. It will stop and display a searchbutton with a black string. You can continue capturing by cklicking the search button again.



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
Seq...     Time of Day  Process Name      PID  Operation
 2470 11:42:44.7007...  HxD.exe           6208 RegSetInfoKey
 2471 11:42:44.7007...  HxD.exe           6208 RegQueryValue
 2472 11:42:44.7007...  HxD.exe           6208 RegCloseKey
 2473 11:42:44.7007...  HxD.exe           6208 RegQueryKey
```

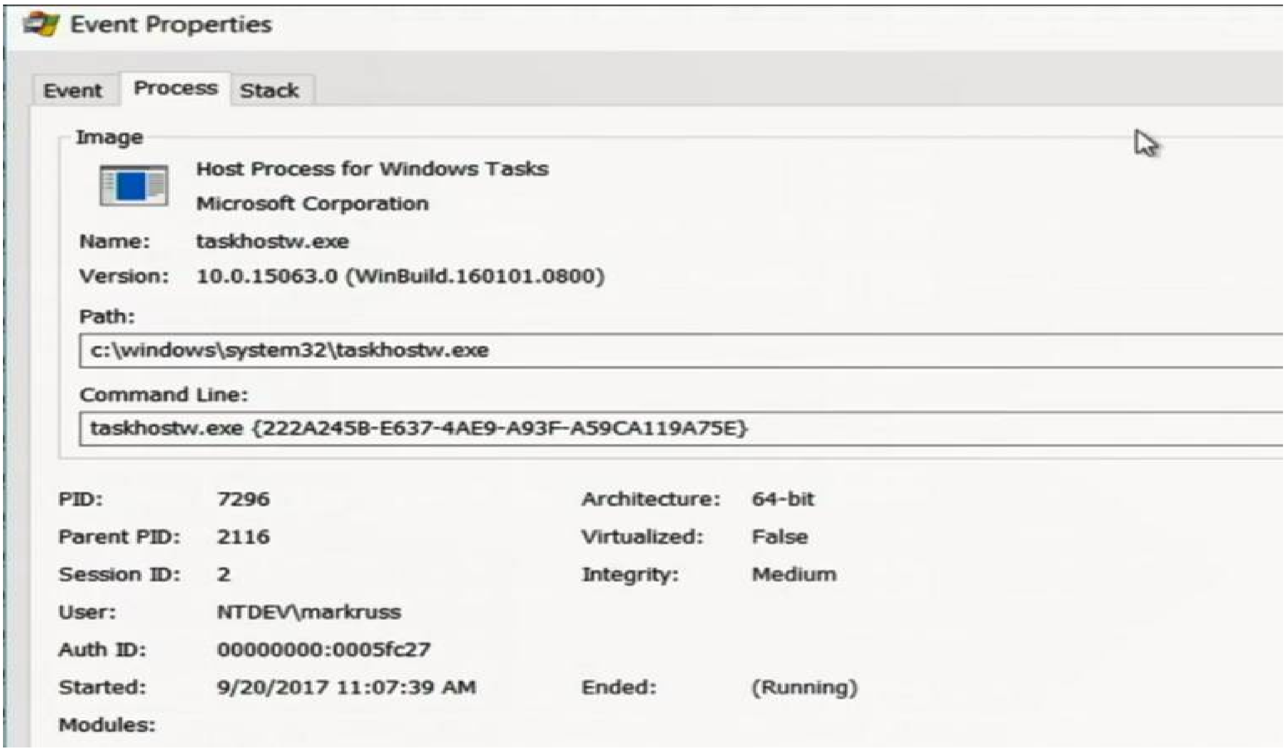
By double clicking of one of the running processes it opens a window which shows detailed information about the current process.



Date: 9/27/2017 11:36:09.8057146 AM
Thread: 7664
Class: Registry
Operation: RegQueryValue
Result: SUCCESS
Path: HKLM\SOFTWARE\Microsoft\Input\EnableTestHook
Duration: 0.0000100

Type: REG_DWORD
Length: 4
Data: 0

The Process register contains the same information as process explorer including dll Moduls.



Image

Host Process for Windows Tasks

Microsoft Corporation

Name: taskhostw.exe

Version: 10.0.15063.0 (WinBuild.160101.0800)

Path:

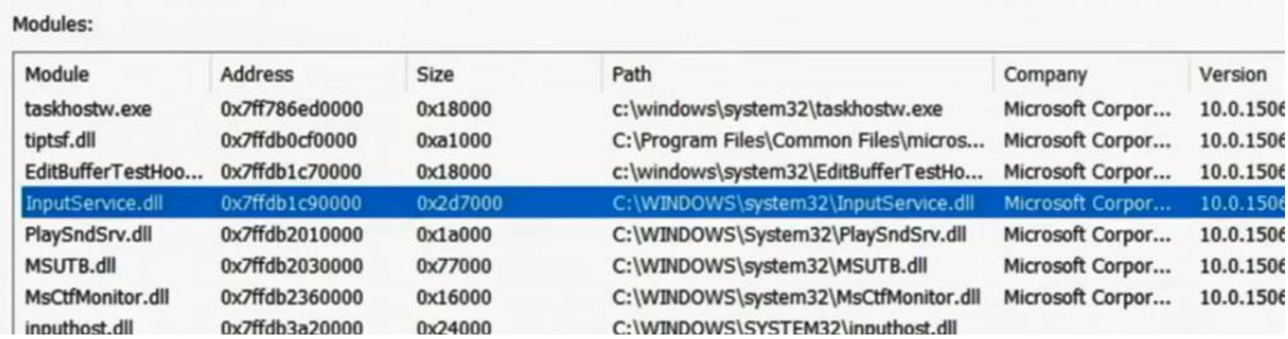
c:\windows\system32\taskhostw.exe

Command Line:

taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}

PID:	7296	Architecture:	64-bit
Parent PID:	2116	Virtualized:	False
Session ID:	2	Integrity:	Medium
User:	NTDEV\markruss		
Auth ID:	00000000:0005fc27		
Started:	9/20/2017 11:07:39 AM	Ended:	(Running)

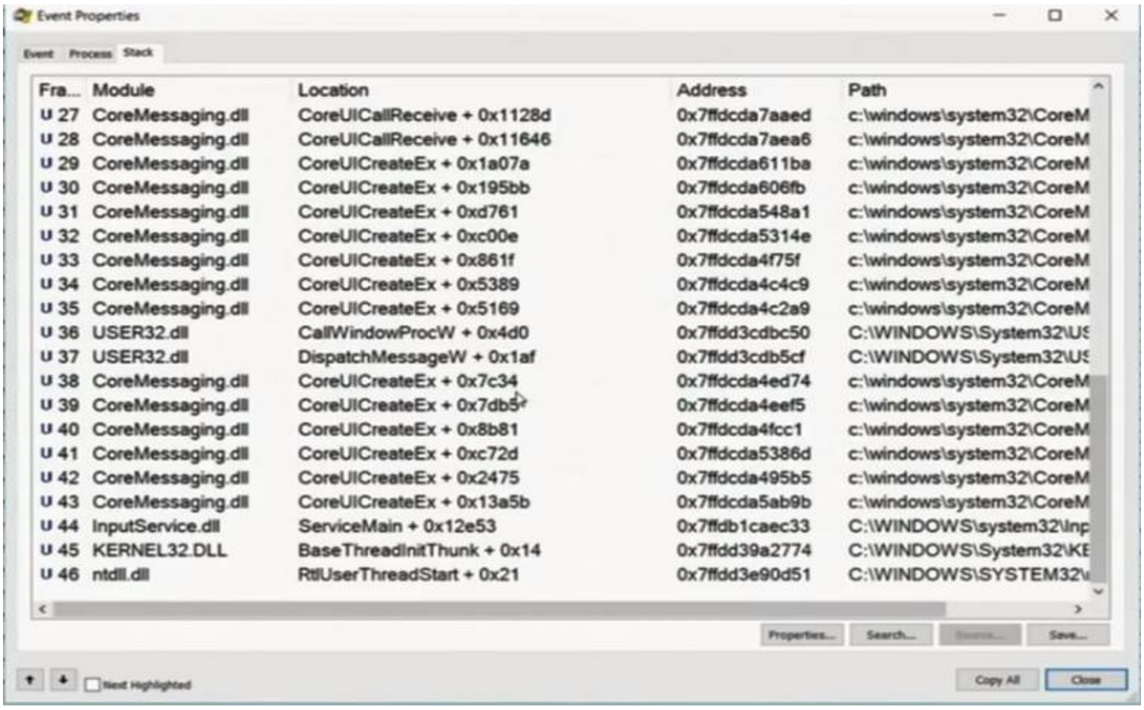
Modules:



Modules:

Module	Address	Size	Path	Company	Version
taskhostw.exe	0x7ff786ed0000	0x18000	c:\windows\system32\taskhostw.exe	Microsoft Corpor...	10.0.1506
tiptsf.dll	0x7ffdb0cf0000	0xa1000	C:\Program Files\Common Files\micros...	Microsoft Corpor...	10.0.1506
EditBufferTestHoo...	0x7ffdb1c70000	0x18000	c:\windows\system32\EditBufferTestHo...	Microsoft Corpor...	10.0.1506
InputService.dll	0x7ffdb1c90000	0x2d7000	C:\WINDOWS\system32\InputService.dll	Microsoft Corpor...	10.0.1506
PlaySndSrv.dll	0x7ffdb2010000	0x1a000	C:\WINDOWS\System32\PlaySndSrv.dll	Microsoft Corpor...	10.0.1506
MSUTB.dll	0x7ffdb2030000	0x77000	C:\WINDOWS\system32\MSUTB.dll	Microsoft Corpor...	10.0.1506
MsCtfMonitor.dll	0x7ffdb2360000	0x16000	C:\WINDOWS\system32\MsCtfMonitor.dll	Microsoft Corpor...	10.0.1506
inputhost.dll	0x7ffdb3a20000	0x24000	C:\WINDOWS\SYSTEM32\inputhost.dll		

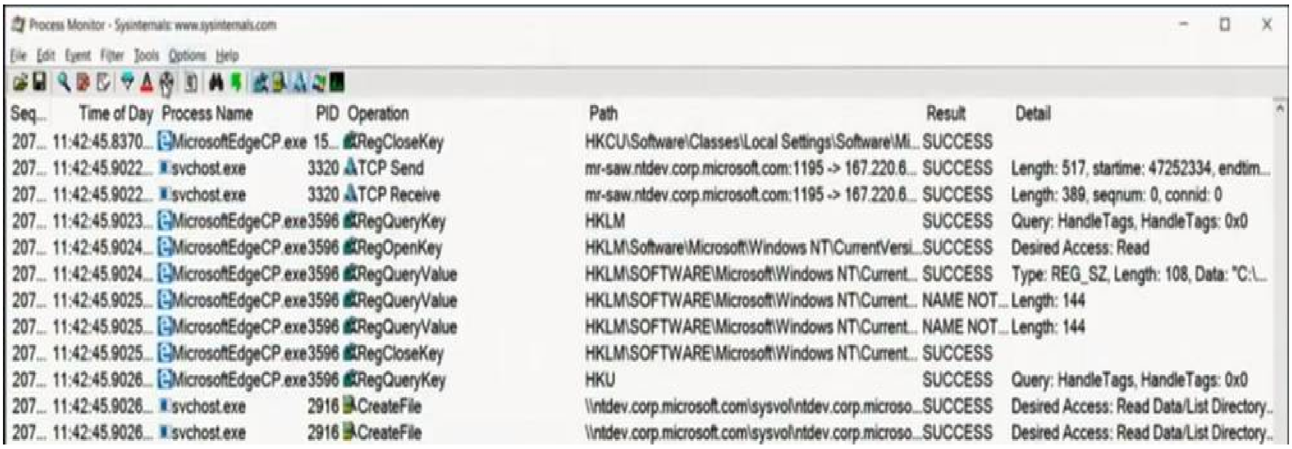
The Stack register shows the functions in the dll modules which was executed by the program



Fra...	Module	Location	Address	Path
U 27	CoreMessaging.dll	CoreUICallReceive + 0x1128d	0x7ffdcda7aaed	c:\windows\system32\CoreM
U 28	CoreMessaging.dll	CoreUICallReceive + 0x11646	0x7ffdcda7aea6	c:\windows\system32\CoreM
U 29	CoreMessaging.dll	CoreUICreateEx + 0x1a07a	0x7ffdcda611ba	c:\windows\system32\CoreM
U 30	CoreMessaging.dll	CoreUICreateEx + 0x195bb	0x7ffdcda606fb	c:\windows\system32\CoreM
U 31	CoreMessaging.dll	CoreUICreateEx + 0xd761	0x7ffdcda548a1	c:\windows\system32\CoreM
U 32	CoreMessaging.dll	CoreUICreateEx + 0xc00e	0x7ffdcda5314e	c:\windows\system32\CoreM
U 33	CoreMessaging.dll	CoreUICreateEx + 0x861f	0x7ffdcda4f75f	c:\windows\system32\CoreM
U 34	CoreMessaging.dll	CoreUICreateEx + 0x5389	0x7ffdcda4c4c9	c:\windows\system32\CoreM
U 35	CoreMessaging.dll	CoreUICreateEx + 0x5169	0x7ffdcda4c2a9	c:\windows\system32\CoreM
U 36	USER32.dll	CallWindowProcW + 0x4d0	0x7ffdd3cdbc50	C:\WINDOWS\System32\US
U 37	USER32.dll	DispatchMessageW + 0x1af	0x7ffdd3cdb5cf	C:\WINDOWS\System32\US
U 38	CoreMessaging.dll	CoreUICreateEx + 0x7c34	0x7ffdcda4ed74	c:\windows\system32\CoreM
U 39	CoreMessaging.dll	CoreUICreateEx + 0x7db5	0x7ffdcda4eef5	c:\windows\system32\CoreM
U 40	CoreMessaging.dll	CoreUICreateEx + 0x8b81	0x7ffdcda4fcc1	c:\windows\system32\CoreM
U 41	CoreMessaging.dll	CoreUICreateEx + 0xc72d	0x7ffdcda5386d	c:\windows\system32\CoreM
U 42	CoreMessaging.dll	CoreUICreateEx + 0x2475	0x7ffdcda495b5	c:\windows\system32\CoreM
U 43	CoreMessaging.dll	CoreUICreateEx + 0x13a5b	0x7ffdcda5ab9b	c:\windows\system32\CoreM
U 44	InputService.dll	ServiceMain + 0x12e53	0x7ffdb1caec33	C:\WINDOWS\system32\Inp
U 45	KERNEL32.DLL	BaseThreadInitThunk + 0x14	0x7ffdd39a2774	C:\WINDOWS\System32\KE
U 46	ntdll.dll	RtlUserThreadStart + 0x21	0x7ffdd3e90d51	C:\WINDOWS\SYSTEM32\

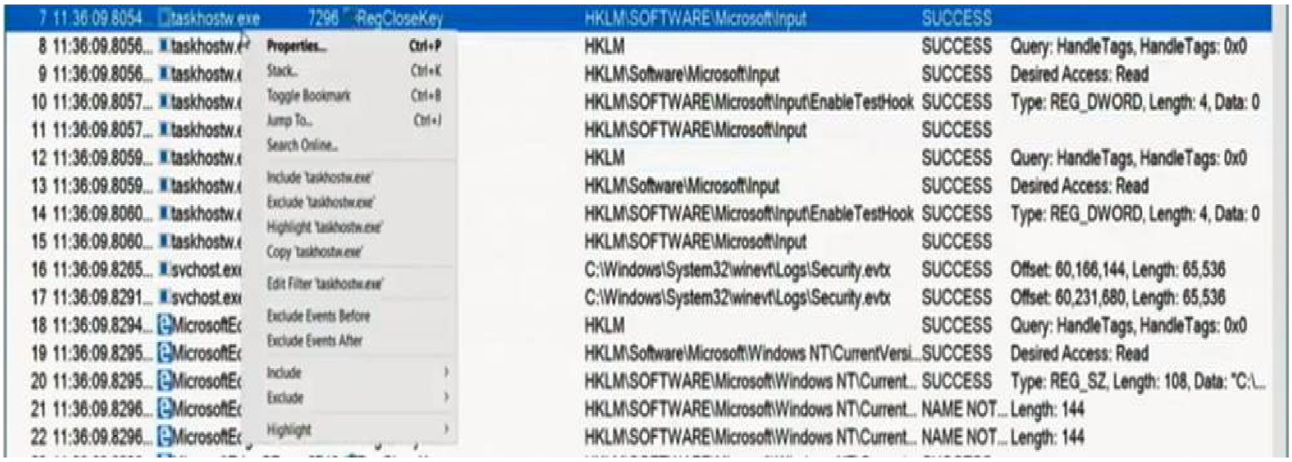
□ Next Highlighted

For filtering for a specific process the easiest way if the program is running in forground is to use the capture button and capture this process by sliding with the mouse to the program window.

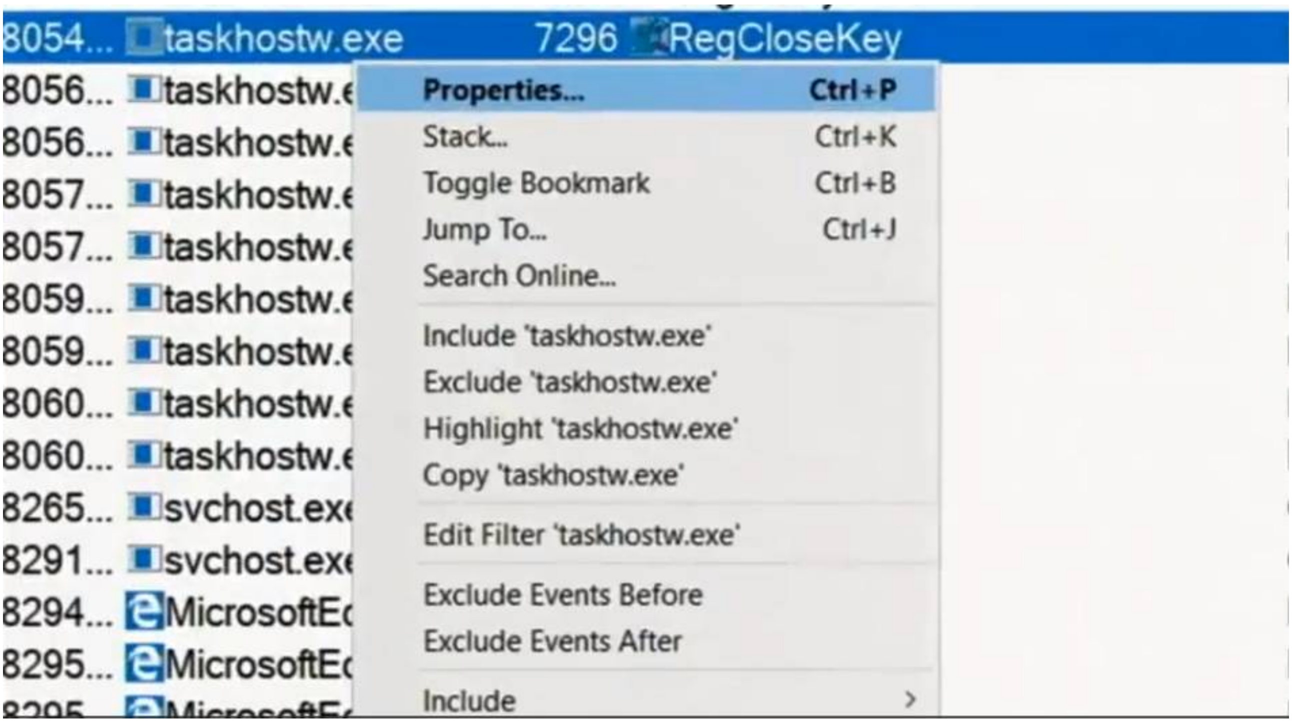


Seq...	Time of Day	Process Name	PID	Operation	Path	Result	Detail
207...	11:42:45.8370...	MicrosoftEdgeCP.exe	15...	RegCloseKey	HKCU\Software\Classes\Local Settings\Software\Mi...	SUCCESS	
207...	11:42:45.9022...	svchost.exe	3320	TCP Send	mr-saw.ntdev.corp.microsoft.com:1195 -> 167.220.6...	SUCCESS	Length: 517, startime: 47252334, endtim...
207...	11:42:45.9022...	svchost.exe	3320	TCP Receive	mr-saw.ntdev.corp.microsoft.com:1195 -> 167.220.6...	SUCCESS	Length: 389, seqnum: 0, connid: 0
207...	11:42:45.9023...	MicrosoftEdgeCP.exe	3596	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
207...	11:42:45.9024...	MicrosoftEdgeCP.exe	3596	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersi...	SUCCESS	Desired Access: Read
207...	11:42:45.9024...	MicrosoftEdgeCP.exe	3596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	Type: REG_SZ, Length: 108, Data: "C:\...
207...	11:42:45.9025...	MicrosoftEdgeCP.exe	3596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
207...	11:42:45.9025...	MicrosoftEdgeCP.exe	3596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
207...	11:42:45.9025...	MicrosoftEdgeCP.exe	3596	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	
207...	11:42:45.9026...	MicrosoftEdgeCP.exe	3596	RegQueryKey	HKU	SUCCESS	Query: HandleTags, HandleTags: 0x0
207...	11:42:45.9026...	svchost.exe	2916	CreateFile	\\ntdev.corp.microsoft.com\sysvol\ntdev.corp.microso...	SUCCESS	Desired Access: Read Data/List Directory...
207...	11:42:45.9026...	svchost.exe	2916	CreateFile	\\ntdev.corp.microsoft.com\sysvol\ntdev.corp.microso...	SUCCESS	Desired Access: Read Data/List Directory...

It is also possible to filter for relevant information by right clicking and selecting the options you need.

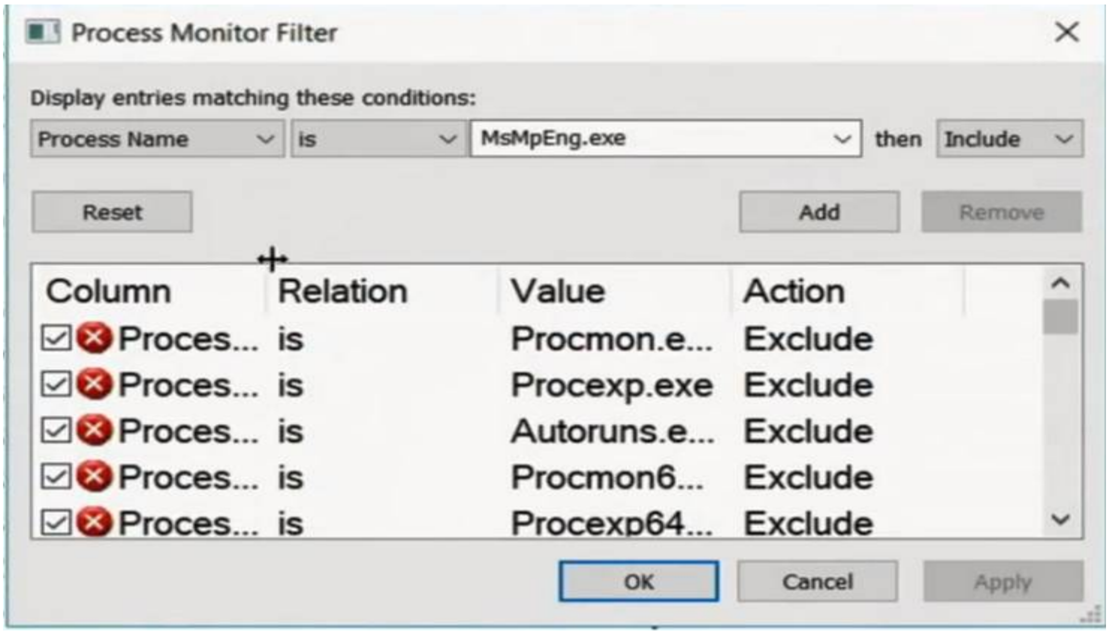


7	11:36:09.8054...	taskhostw.exe	7296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
8	11:36:09.8056...	taskhostw.e			HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
9	11:36:09.8056...	taskhostw.e			HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
10	11:36:09.8057...	taskhostw.e			HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11	11:36:09.8057...	taskhostw.e			HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
12	11:36:09.8059...	taskhostw.e			HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
13	11:36:09.8059...	taskhostw.e			HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
14	11:36:09.8060...	taskhostw.e			HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
15	11:36:09.8060...	taskhostw.e			HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
16	11:36:09.8265...	svchost.exe			C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 60,166,144, Length: 65,536
17	11:36:09.8291...	svchost.exe			C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 60,231,680, Length: 65,536
18	11:36:09.8294...	MicrosoftEc			HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
19	11:36:09.8295...	MicrosoftEc			HKLM\Software\Microsoft\Windows NT\CurrentVersi...	SUCCESS	Desired Access: Read
20	11:36:09.8295...	MicrosoftEc			HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	Type: REG_SZ, Length: 108, Data: "C:\...
21	11:36:09.8296...	MicrosoftEc			HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
22	11:36:09.8296...	MicrosoftEc			HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144



```
8054... taskhostw.exe        7296 RegCloseKey
8056... taskhostw.e
8056... taskhostw.e
8057... taskhostw.e
8057... taskhostw.e
8059... taskhostw.e
8059... taskhostw.e
8060... taskhostw.e
8060... taskhostw.e
8265... svchost.exe
8291... svchost.exe
8294... MicrosoftEc
8295... MicrosoftEc
```

You can also use a own filter to use the Edit Filter option.



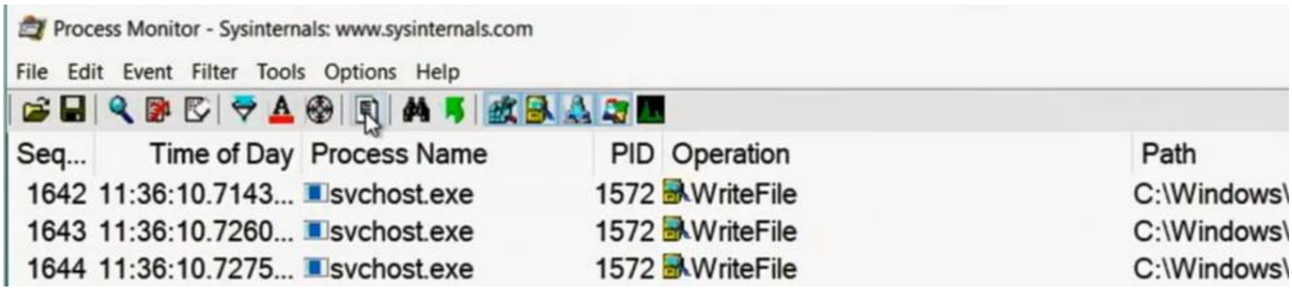
Process Monitor Filter

Display entries matching these conditions:

Process Name | is | MsMpEng.exe | then | Include

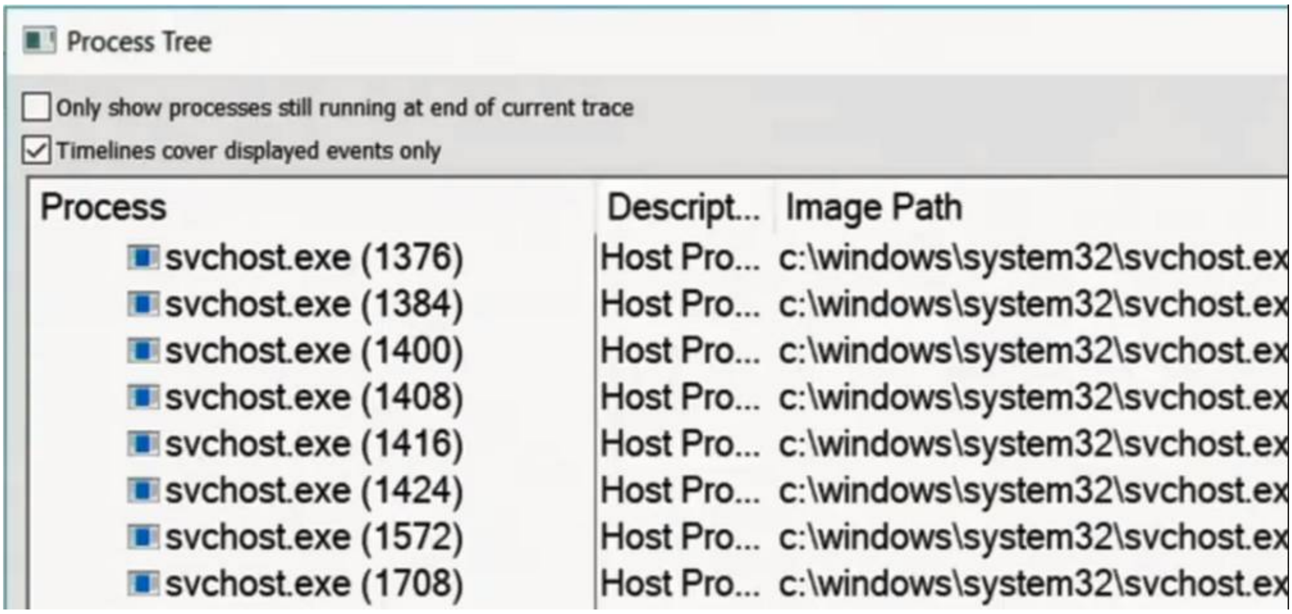
Column	Relation	Value	Action
☑ Proces...	is	Procmon.e...	Exclude
☑ Proces...	is	Procexp.exe	Exclude
☑ Proces...	is	Autoruns.e...	Exclude
☑ Proces...	is	Procmon6...	Exclude
☑ Proces...	is	Procexp64....	Exclude

If you searching for a specific process it is also possible to search it on the process tree and select them. To open the process tree click on the note symbol in the middle of the process monitor.



Process Monitor - Sysinternals: www.sysinternals.com

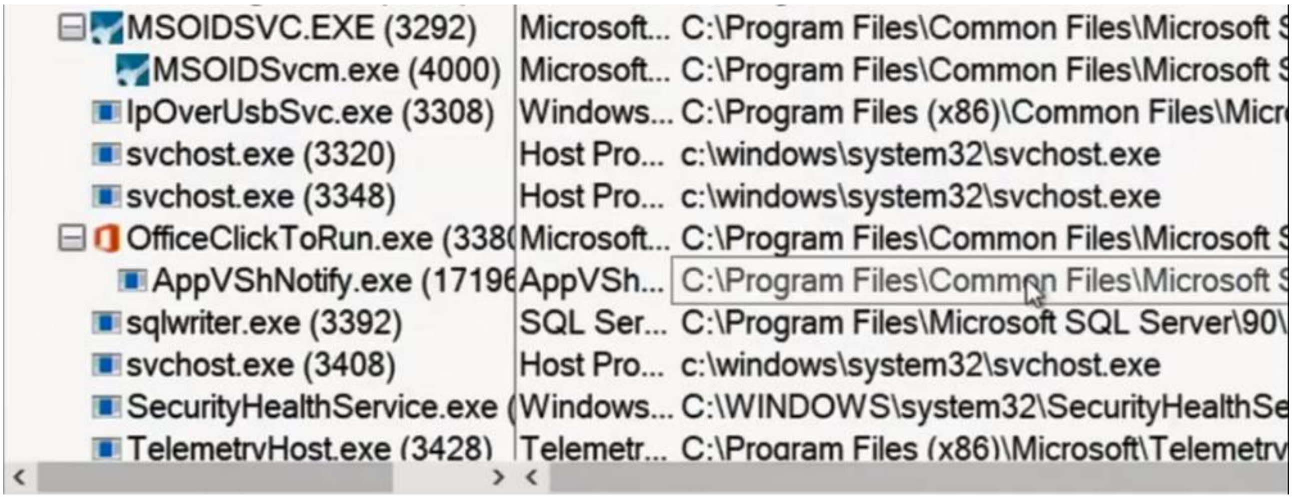
Seq...	Time of Day	Process Name	PID	Operation	Path
1642	11:36:10.7143...	svchost.exe	1572	WriteFile	C:\Windows\
1643	11:36:10.7260...	svchost.exe	1572	WriteFile	C:\Windows\
1644	11:36:10.7275...	svchost.exe	1572	WriteFile	C:\Windows\



□ Only show processes still running at end of current trace

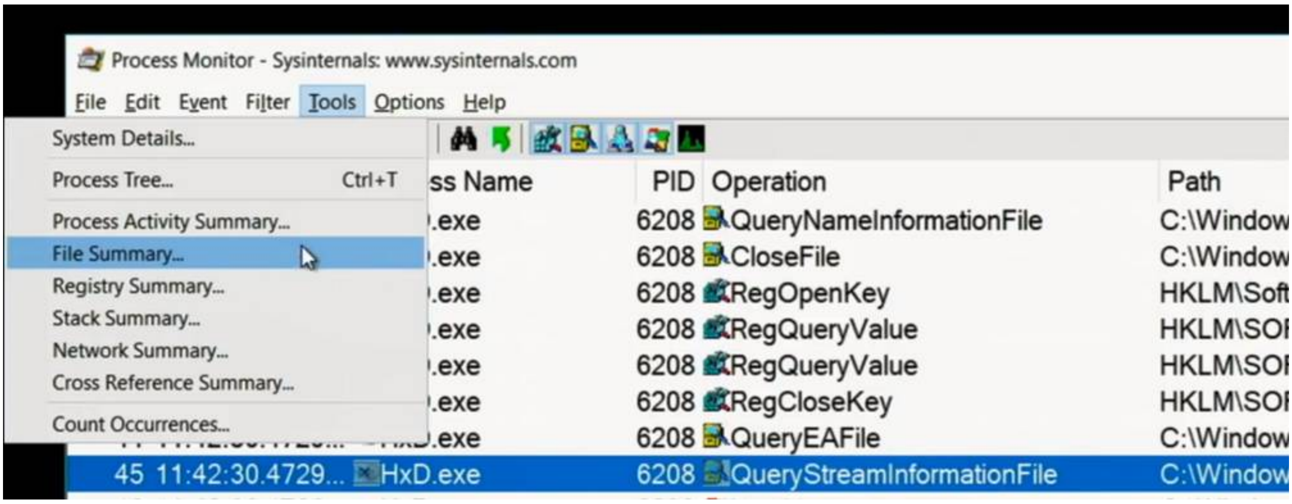
☑ Timelines cover displayed events only

Process	Descript...	Image Path
svchost.exe (1376)	Host Pro...	c:\windows\system32\svchost.ex
svchost.exe (1384)	Host Pro...	c:\windows\system32\svchost.ex
svchost.exe (1400)	Host Pro...	c:\windows\system32\svchost.ex
svchost.exe (1408)	Host Pro...	c:\windows\system32\svchost.ex
svchost.exe (1416)	Host Pro...	c:\windows\system32\svchost.ex
svchost.exe (1424)	Host Pro...	c:\windows\system32\svchost.ex
svchost.exe (1572)	Host Pro...	c:\windows\system32\svchost.ex
svchost.exe (1708)	Host Pro...	c:\windows\system32\svchost.ex

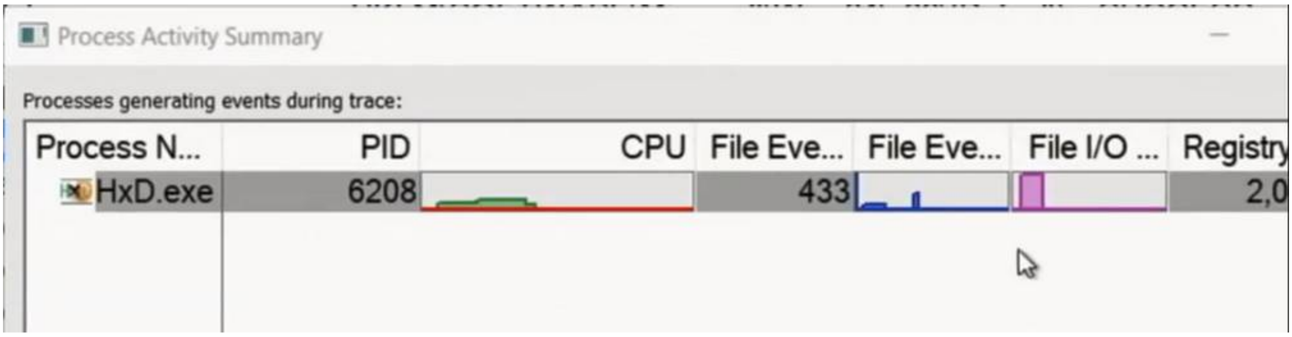


⊟ MSOIDSVC.EXE (3292)	Microsoft...	C:\Program Files\Common Files\Microsoft S
MSOIDSvcm.exe (4000)	Microsoft...	C:\Program Files\Common Files\Microsoft S
IpOverUsbSvc.exe (3308)	Windows...	C:\Program Files (x86)\Common Files\Micr
svchost.exe (3320)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (3348)	Host Pro...	c:\windows\system32\svchost.exe
⊟ OfficeClickToRun.exe (338	Microsoft...	C:\Program Files\Common Files\Microsoft S
AppVShNotify.exe (1719	AppVSh...	C:\Program Files\Common Files\Microsoft S
sqlwriter.exe (3392)	SQL Ser...	C:\Program Files\Microsoft SQL Server\90\
svchost.exe (3408)	Host Pro...	c:\windows\system32\svchost.exe
SecurityHealthService.exe (	Windows...	C:\WINDOWS\system32\SecurityHealthSe
TelemetryHost.exe (3428)	Telemetr...	C:\Program Files (x86)\Microsoft\Telemetry

By filtering a specific process a advanced option of process monitor is also useful. So by clicking on the Tool register on the top you can use the diffrent summary graphs of hardware and software activities e.g Process Activity Summary (CPU, File I/O etc) and after selecting you can jump to the specific line in the capturing trace.



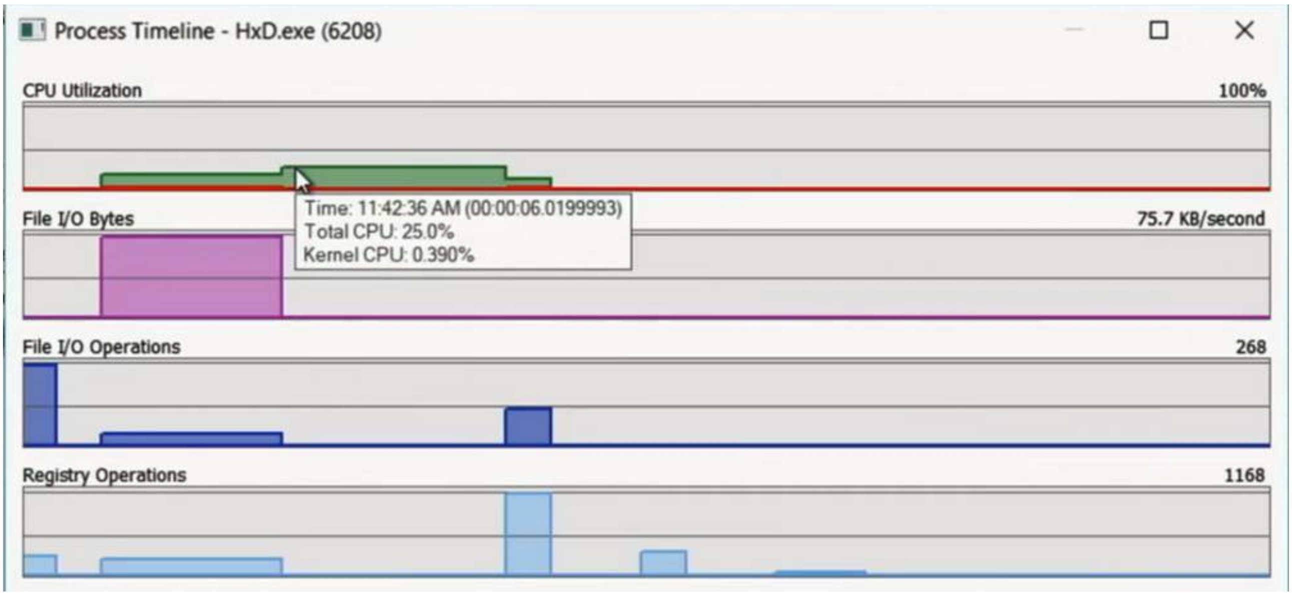
ss Name	PID	Operation	Path
.exe	6208	QueryNameInformationFile	C:\Window
.exe	6208	CloseFile	C:\Window
.exe	6208	RegOpenKey	HKLM\Soft
.exe	6208	RegQueryValue	HKLM\SOI
.exe	6208	RegQueryValue	HKLM\SOI
.exe	6208	RegCloseKey	HKLM\SOI
.exe	6208	QueryEAFile	C:\Window
45 11:42:30.4729... HxD.exe	6208	QueryStreamInformationFile	C:\Window



Process Activity Summary

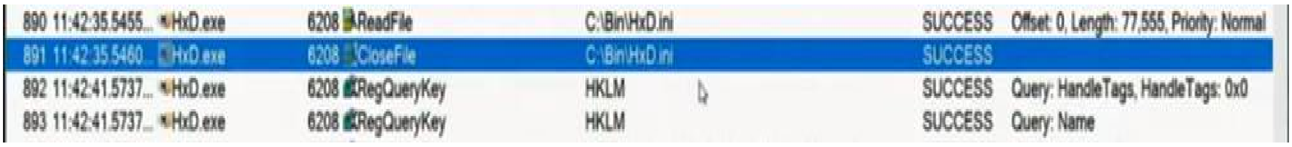
Processes generating events during trace:

Process N...	PID	CPU	File Eve...	File Eve...	File I/O ...	Registry
HxD.exe	6208		433			2,0



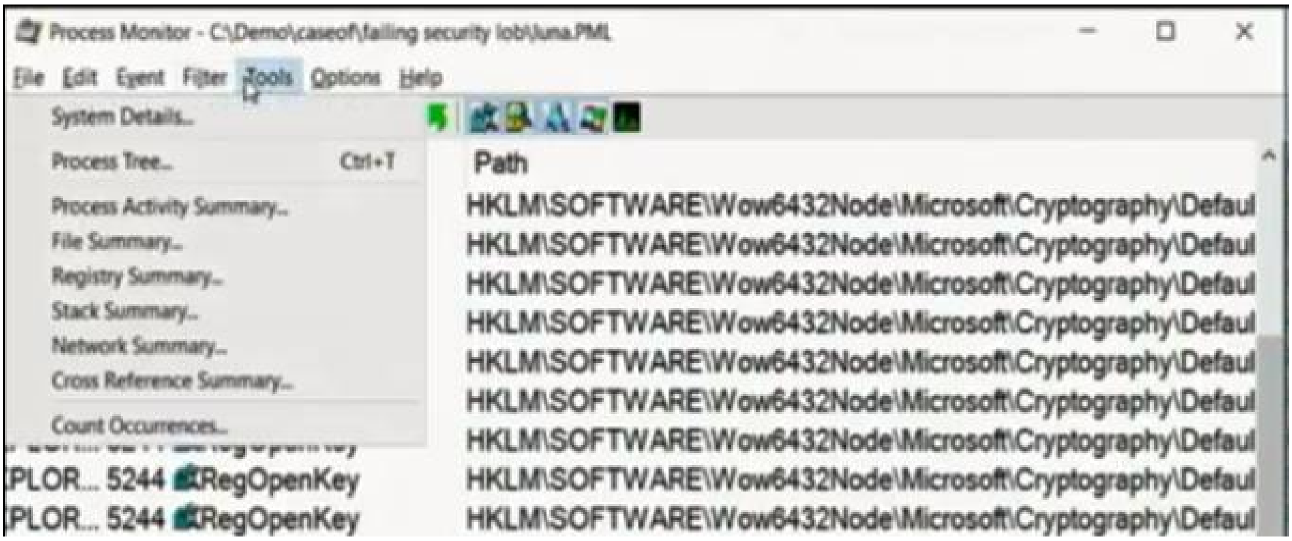
Process Timeline - HxD.exe (6208)

Time: 11:42:36 AM (00:00:06.0199993)
Total CPU: 25.0%
Kernel CPU: 0.390%

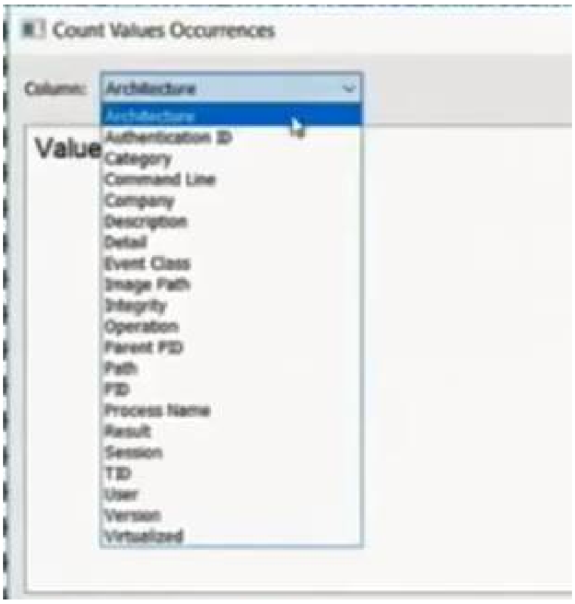


```
890 11:42:35.5455... HxD.exe   6208 ReadFile      C:\Bin\HxD.ini   SUCCESS   Offset: 0, Length: 77,555, Priority: Normal
891 11:42:35.5460... HxD.exe   6208 CloseFile     C:\Bin\HxD.ini   SUCCESS
892 11:42:41.5737... HxD.exe   6208 RegQueryKey   HKLM             SUCCESS   Query: HandleTags, HandleTags: 0x0
893 11:42:41.5737... HxD.exe   6208 RegQueryKey   HKLM             SUCCESS   Query: Name
```

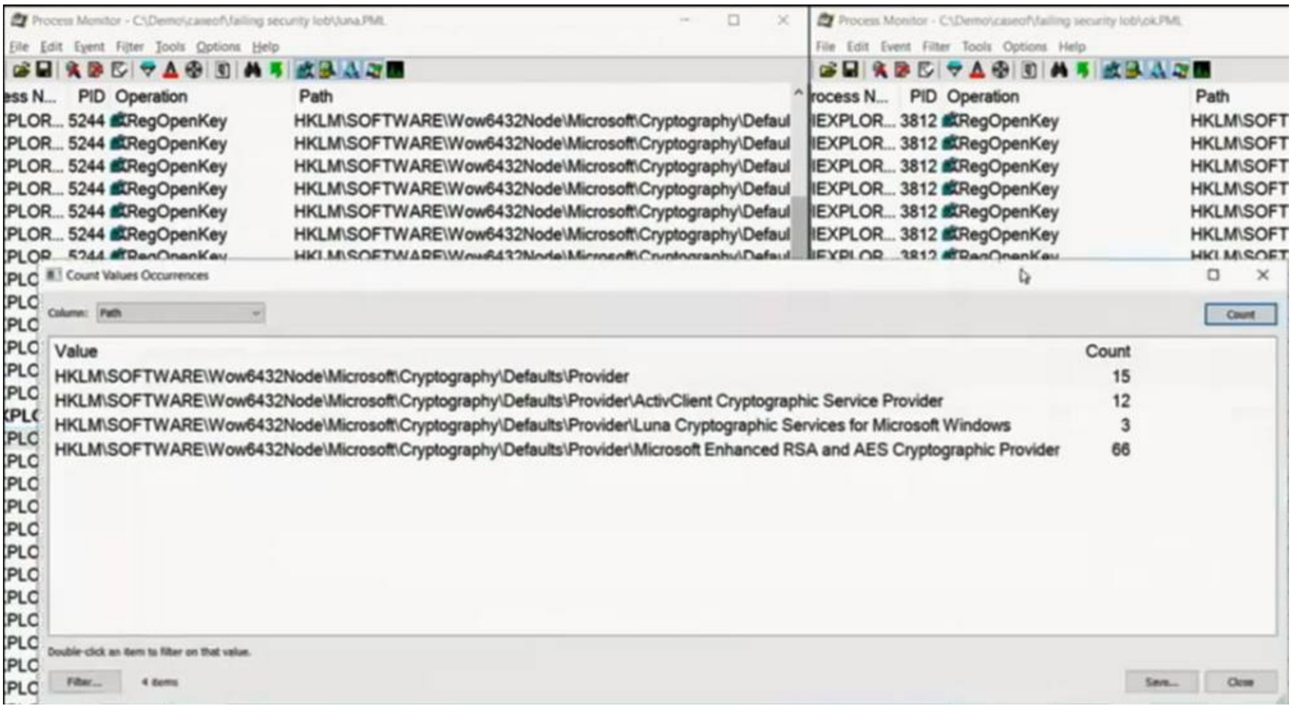
Antoher helpful option by filtering issues is to use the Count Occurences in the Tool register You can more specifice the Occurences by selecting the drop-down-menu



```
                              HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
                              HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
                              HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
                              HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
                              HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
                              HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
                              HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
PLOR... 5244 RegOpenKey       HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
PLOR... 5244 RegOpenKey       HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
```



Column: Architecture


Process Monitor - C:\Demo\caseof\failing security lob\luna.PML
File Edit Event Filter Tools Options Help
Process Monitor - C:\Demo\caseof\failing security lob\ok.PML
File Edit Event Filter Tools Options Help
Count Values Occurrences
Count
Double-click an item to filter on that value.
Filter...
4 items
Save...
Close

```
ess N...  PID  Operation    Path
PLOR...  5244  RegOpenKey   HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
PLOR...  5244  RegOpenKey   HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
PLOR...  5244  RegOpenKey   HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
PLOR...  5244  RegOpenKey   HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
PLOR...  5244  RegOpenKey   HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
PLOR...  5244  RegOpenKey   HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaul
```

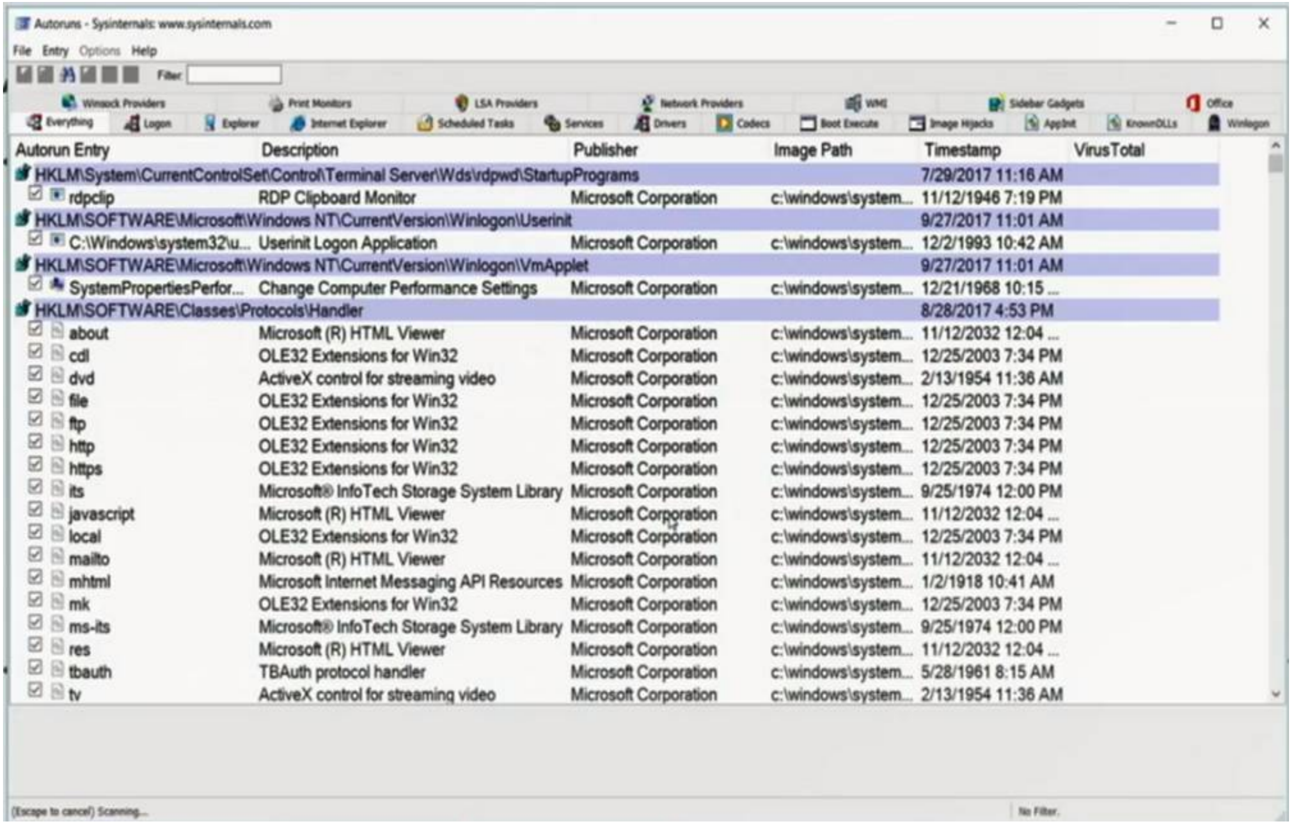
```
rocess N...  PID  Operation    Path
IEXPLOR...  3812  RegOpenKey   HKLM\SOFT
IEXPLOR...  3812  RegOpenKey   HKLM\SOFT
IEXPLOR...  3812  RegOpenKey   HKLM\SOFT
IEXPLOR...  3812  RegOpenKey   HKLM\SOFT
IEXPLOR...  3812  RegOpenKey   HKLM\SOFT
IEXPLOR...  3812  RegOpenKey   HKLM\SOFT
```

Column: Path

Value	Count
HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider	15
HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\ActivClient Cryptographic Service Provider	12
HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Luna Cryptographic Services for Microsoft Windows	3
HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic Provider	66

Using Autoruns for Troubelshooting

Autoruns also shows you detailed information about diffrent system components e.g dll files, drivers, services, scheduled tasks, codecs, office plugins etc.



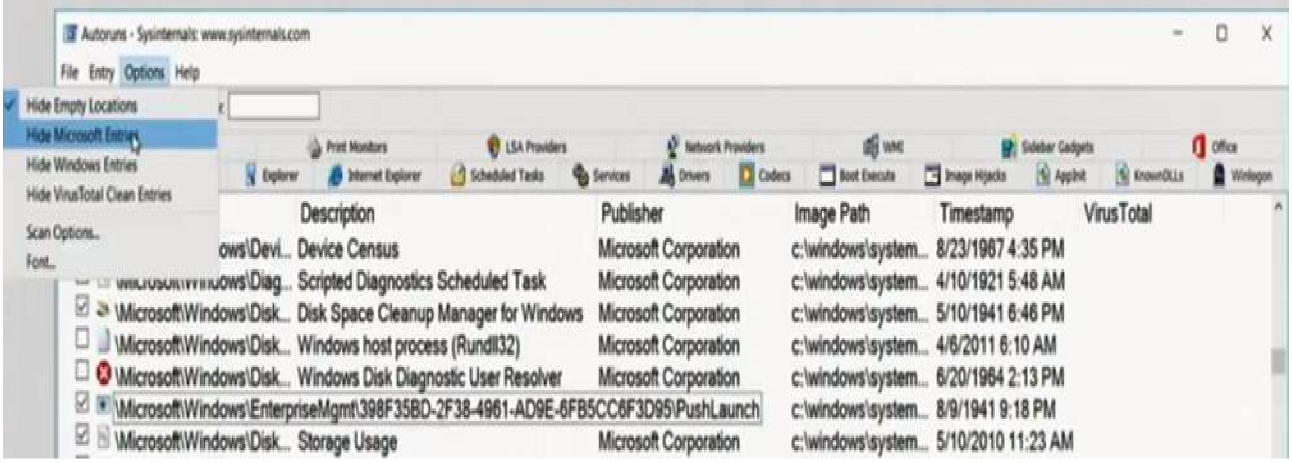
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms				7/29/2017 11:16 AM	
☑ rdpclip	RDP Clipboard Monitor	Microsoft Corporation	c:\windows\system...	11/12/1946 7:19 PM	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit				9/27/2017 11:01 AM	
☑ C:\Windows\system32\u...	Userinit Logon Application	Microsoft Corporation	c:\windows\system...	12/2/1993 10:42 AM	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet				9/27/2017 11:01 AM	
☑ SystemPropertiesPerfor...	Change Computer Performance Settings	Microsoft Corporation	c:\windows\system...	12/21/1968 10:15 ...	
HKLM\SOFTWARE\Classes\Protocols\Handler				8/28/2017 4:53 PM	
☑ about	Microsoft (R) HTML Viewer	Microsoft Corporation	c:\windows\system...	11/12/2032 12:04 ...	
☑ cdl	OLE32 Extensions for Win32	Microsoft Corporation	c:\windows\system...	12/25/2003 7:34 PM	
☑ dvd	ActiveX control for streaming video	Microsoft Corporation	c:\windows\system...	2/13/1954 11:36 AM	
☑ file	OLE32 Extensions for Win32	Microsoft Corporation	c:\windows\system...	12/25/2003 7:34 PM	
☑ ftp	OLE32 Extensions for Win32	Microsoft Corporation	c:\windows\system...	12/25/2003 7:34 PM	
☑ http	OLE32 Extensions for Win32	Microsoft Corporation	c:\windows\system...	12/25/2003 7:34 PM	
☑ https	OLE32 Extensions for Win32	Microsoft Corporation	c:\windows\system...	12/25/2003 7:34 PM	
☑ its	Microsoft® InfoTech Storage System Library	Microsoft Corporation	c:\windows\system...	9/25/1974 12:00 PM	
☑ javascript	Microsoft (R) HTML Viewer	Microsoft Corporation	c:\windows\system...	11/12/2032 12:04 ...	
☑ local	OLE32 Extensions for Win32	Microsoft Corporation	c:\windows\system...	12/25/2003 7:34 PM	
☑ mailto	Microsoft (R) HTML Viewer	Microsoft Corporation	c:\windows\system...	11/12/2032 12:04 ...	
☑ mhtml	Microsoft Internet Messaging API Resources	Microsoft Corporation	c:\windows\system...	1/2/1918 10:41 AM	
☑ mk	OLE32 Extensions for Win32	Microsoft Corporation	c:\windows\system...	12/25/2003 7:34 PM	
☑ ms-its	Microsoft® InfoTech Storage System Library	Microsoft Corporation	c:\windows\system...	9/25/1974 12:00 PM	
☑ res	Microsoft (R) HTML Viewer	Microsoft Corporation	c:\windows\system...	11/12/2032 12:04 ...	
☑ tbauth	TBAuth protocol handler	Microsoft Corporation	c:\windows\system...	5/28/1961 8:15 AM	
☑ tv	ActiveX control for streaming video	Microsoft Corporation	c:\windows\system...	2/13/1954 11:36 AM	

(Escape to cancel) Scanning...

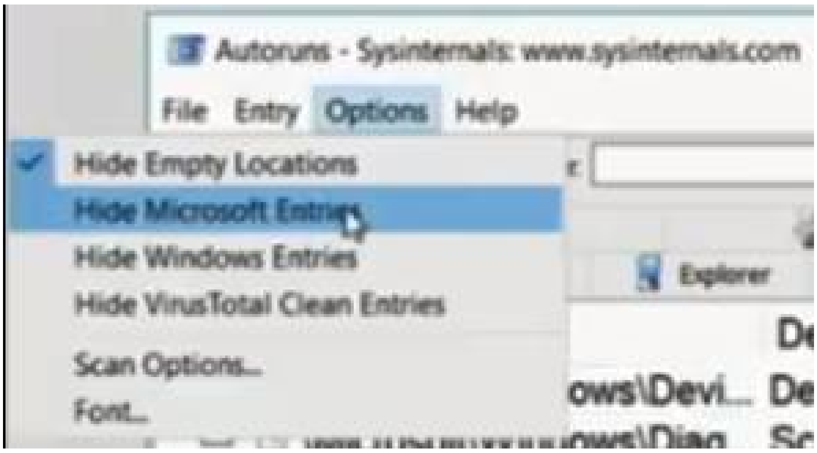
No Filter.

You can also use Autoruns to filter information or for malware scanning

To filter information use the Options register at the top and turn on and off default filters or use a own filter option

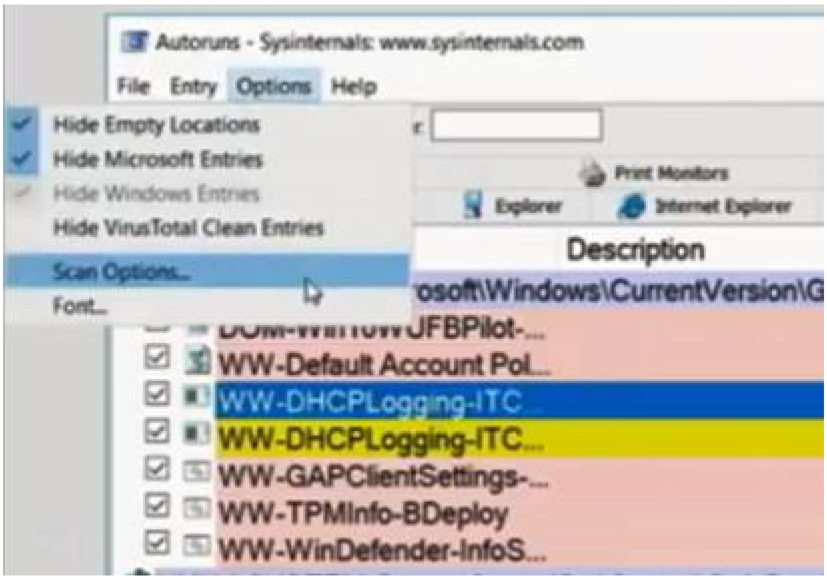


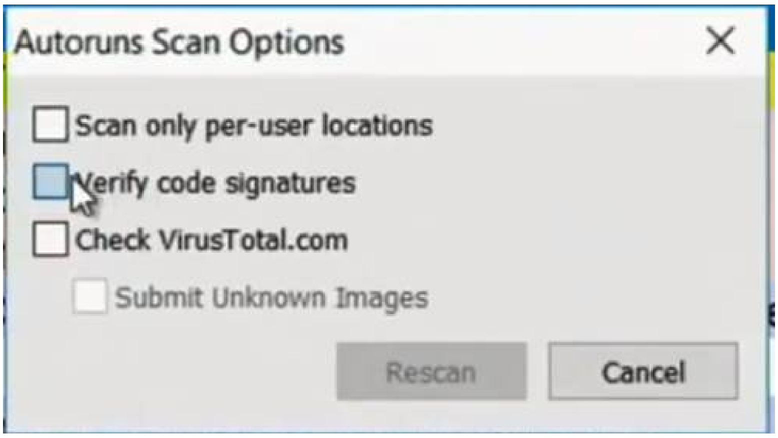
	Description	Publisher	Image Path	Timestamp	VirusTotal
...ows\Devi...	Device Census	Microsoft Corporation	c:\windows\system...	8/23/1987 4:35 PM	
\Microsoft\Windows\Diag...	Scripted Diagnostics Scheduled Task	Microsoft Corporation	c:\windows\system...	4/10/1921 5:48 AM	
☑ \Microsoft\Windows\Disk...	Disk Space Cleanup Manager for Windows	Microsoft Corporation	c:\windows\system...	5/10/1941 6:46 PM	
□ \Microsoft\Windows\Disk...	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system...	4/6/2011 6:10 AM	
□ \Microsoft\Windows\Disk...	Windows Disk Diagnostic User Resolver	Microsoft Corporation	c:\windows\system...	6/20/1984 2:13 PM	
☑ \Microsoft\Windows\EnterpriseMgmt\398F35BD-2F38-4961-AD9E-6FB5CC6F3D95\PushLaunch			c:\windows\system...	8/9/1941 9:18 PM	
☑ \Microsoft\Windows\Disk...	Storage Usage	Microsoft Corporation	c:\windows\system...	5/10/2010 11:23 AM	



To use the Autoruns for scanning malware use the Entry register at the top and use the Scan Options. Select the options you want.

Be careful with the Submit Unknown Images Option because this file information we be published in public and are not possible to delete so it could be a privacy incident !




Autoruns Scan Options

□ Scan only per-user locations

□ Verify code signatures

□ Check VirusTotal.com

□ Submit Unknown Images

Signatures can also be checked with the tool sigcheck

Quellen:

Steve Whiting - Case of the Unexplained

Tech-Days 2012 – Windows Debugging and Troubelshooting

Windows Debugging and Troubleshooting - Invidious (kavin.rocks)

Case of the Unexplained Windows Troubleshooting with Mark Russinovich - 2017 - Invidious (kavin.rocks)

https//dumpanalysis,.org

https://blogs.msdn.com/ntdebugging