sort lm n t by date/time
Posted by karl - 02 Aug 2011 - 01:54

When analyzing a minidump, how do I sort the output of lm n t by date-time?

==========

Re: sort lm n t by date/time
Posted by Robert Kuster - 02 Aug 2011 - 08:21

Welcome Carl.

You might try the !dll -l command. It lists all currently loaded dlls sorted by their load order, though enough memory information must be present in the dump for the command to work (.dump /mf c:mydump.dmp).

I hope this helps,
Robert

==========

Re: sort lm n t by date/time
Posted by karl - 02 Aug 2011 - 08:23

my objective is to sort the list by creation date-time to spot drivers which are woefully out-of-date.

==========

Re: sort lm n t by date/time
Posted by Robert Kuster - 02 Aug 2011 - 09:10

Oh, I see..my mistake. I guess the easiest way is to redirect the output of "lm n t" to an external PowerShell or Perl or VB script and sort it out there. For example: .shell -ci "lm n t" perl.exe parsemyoutput.pl. The sorted output from your script will then be displayed in WinDbg's Command window.

I hope this helps,
Robert

==========

Re: sort lm n t by date/time
Posted by karl - 02 Aug 2011 - 09:16

will not accomplish my objective. Remember that just sort by module, one merely adds sm.

==========

Re: sort lm n t by date/time

Posted by Robert Kuster - 11 Sep 2011 - 16:00

_____

Hi Karl,

this should have been your homework. But here it goes - copy the following VBScript and store it as c:mysort.vbs.

```
Dim StdIn, StdOut
Set StdIn = WScript.StdIn
Set StdOut = WScript.StdOut
ReDim lines(0), timeStamps(0)
c = 0

Do While Not StdIn.AtEndOfStream
  ReDim Preserve lines(UBound(lines) + 1)
  ReDim Preserve timeStamps(UBound(timeStamps) + 1)

  str = StdIn.ReadLine
  lines(c) = str
  timeStamps(c) = Replace(Right(str, Len(str) - InStrRev(str, "(")), ")", "")
  c = c + 1
Loop

For i = UBound(timeStamps) - 1 To 0 Step -1
  For j = 0 to i
    If timeStamps(j)>timeStamps(j+1) Then
      temp = lines(j+1)
      lines(j+1) = lines(j)
      lines(j) = temp

      temp = timeStamps(j+1)
      timeStamps(j+1) = timeStamps(j)
      timeStamps(j) = temp
    End if
  Next
Next

For Each x In lines
  StdOut.WriteLine x
Next
```

Then back in WinDbg type:

```
 0:002> .shell -ci "lm nt" cscript c:mysort.vbs
```

Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

```
01000000 0105a000   qslice   qslice.exe   Thu Dec 02 23:53:58 1999 (3846F886)
00b80000 00bda000   DpoSet   DpoSet.dll   Wed May 13 02:20:53 2009 (4A0A1265)
10000000 1007a000   DpoFeedb DpoFeedb.dll Wed May 13 02:28:51 2009 (4A0A1443)
74290000 7429b000   profapi  profapi.dll  Tue Jul 14 01:12:01 2009 (4A5BBF41)
74c50000 74c5c000   CRYPTBASE CRYPTBASE.dll Tue Jul 14 01:12:01 2009 (4A5BBF41)
72700000 72713000   dwmapi   dwmapi.dll   Tue Jul 14 03:06:15 2009 (4A5BDA07)
764e0000 765ac000   MSCTF    MSCTF.dll    Tue Jul 14 03:07:53 2009 (4A5BDA69)
760e0000 7618c000   msvcrt   msvcrt.dll   Tue Jul 14 03:07:59 2009 (4A5BDA6F)
76c30000 76c49000   sechost  sechost.dll  Tue Jul 14 03:10:28 2009 (4A5BDB04)
75360000 7536a000   LPK      LPK.dll      Tue Jul 14 03:11:23 2009 (4A5BDB3B)
72660000 726e0000   uxtheme  uxtheme.dll  Tue Jul 14 03:11:24 2009 (4A5BDB3C)
76400000 764a0000   ADVAPI32 ADVAPI32.dll Sat Nov 20 12:54:46 2010 (4CE7B706)
724c0000 7265e000   comctl32 comctl32.DLL Sat Nov 20 12:55:08 2010 (4CE7B71C)
762a0000 763fc000   ole32    ole32.dll    Sat Nov 20 13:05:03 2010 (4CE7B96F)
765b0000 76607000   SHLWAPI  SHLWAPI.dll  Sat Nov 20 13:06:58 2010 (4CE7B9E2)
74040000 74057000   USERENV  USERENV.dll  Sat Nov 20 13:08:08 2010 (4CE7BA28)
76770000 7680d000   USP10    USP10.dll    Sat Nov 20 13:08:09 2010 (4CE7BA29)
766e0000 76770000   GDI32    GDI32.dll    Sat Nov 20 13:08:51 2010 (4CE7BA53)
76ad0000 76b30000   IMM32    IMM32.DLL    Sat Nov 20 13:08:51 2010 (4CE7BA53)
77570000 776f0000   ntdll    ntdll.dll    Sat Nov 20 13:08:56 2010 (4CE7BA58)
74c60000 74cc0000   SspiCli  SspiCli.dll  Sat Nov 20 13:08:57 2010 (4CE7BA59)
768a0000 769a0000   USER32   USER32.dll   Sat Nov 20 13:08:57 2010 (4CE7BA59)
769a0000 76a90000   RPCRT4   RPCRT4.dll   Sat Nov 20 13:08:57 2010 (4CE7BA59)
76b70000 76bff000   OLEAUT32 OLEAUT32.dll Fri Feb 25 06:28:09 2011 (4D673DE9)
74eb0000 74fc0000   kernel32 kernel32.dll Sat Jul 16 06:27:04 2011 (4E211318)
76610000 76656000   KERNELBASE KERNELBASE.dll Sat Jul 16 06:27:05 2011 (4E211319)
start    end        module name
.shell: Process exited
```

Blink blink. The result is a list of modules sorted by their compilation dates.

I hope this helps,
Robert

==========

Re: sort lm n t by date/time

Posted by karl - 11 Sep 2011 - 16:15

_____

Robert,
I apologize for not getting back. I did some reading and wrote a PowerShell script to sort the list and perform a couple of other clean up operations.

Thanks,
karl

==========