Topics

- Process dumps: main algorithm
- Task Manager and userdump.exe examples
- Troubleshooting process dumps
Main Algorithm

1. PID is present?
   - Yes
     - Pre-Vista?
       - Yes
         - Task Manager
       - No
         - Pre-Vista?
           - Yes
             - userdmp
           - No
             - NTSD
     - No
       - Pre-Vista?
         - Yes
           - Task Manager
         - No
           - Local Dumps

© 2013 Software Diagnostics Institute
Userdump.exe

• x64

C:\kktools\userdump8.1\x64\userdump -p
C:\kktools\userdump8.1\x64\userdump <process name>|<PID>

• (x86 on x64)* or native x86

C:\kktools\userdump8.1\x86\userdump -p
C:\kktools\userdump8.1\x86\userdump <process name>|<PID>

* May not work on x64 Vista, Windows 7 and higher
x86 on x64

C:\Windows\SysWOW64\taskmgr.exe
Useful Links

- How to use userdump.exe
- TestWER
- WinDbg.org
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 20-25, 2013</td>
<td>Accelerated Windows Memory Dump Analysis</td>
</tr>
<tr>
<td>March, 25, 2013</td>
<td>Malware Narratives (FREE)</td>
</tr>
<tr>
<td>April, 26-29, 2013</td>
<td>Accelerated Windows Debugging³</td>
</tr>
<tr>
<td>May, 13, 2013</td>
<td>Philosophy of Software Diagnostics (FREE)</td>
</tr>
<tr>
<td>Summer, 2013</td>
<td>Accelerated Windows Network Trace Analysis</td>
</tr>
</tbody>
</table>

The New Old Debugging

Now Available for Booking
Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV