Topics

- Thread
- Adjoint Thread
- Software Trace Analysis Patterns
- Examples (Procmon, CDFAnalyzer, Excel)
Thread

\[
\{ \text{msg} \mid \text{TID} = N \}
\]

SELECT * FROM Messages WHERE Messages.TID = N

\(<T|A> \quad <\text{Constant}|\text{Variable}>\)
Adjoint Thread

\{ \text{msg} \mid \text{Func} = \text{‘Text’} \}\]

SELECT * FROM Messages
WHERE Messages.Func = \text{‘CreateProcess’}

\langle T | A \rangle \iff \langle A | T \rangle

From mathematics: **Adjoints**
Log Analysis Patterns

- Discontinuity
- Time Delta
- Anchor Messages
- Fiber Bundle

Complex adjoint threads: nested filtering
Suggested Reading

Articles on adjoint threading:

• Extending Multithreading to Multibraiding

• What is an Adjoint Thread?

Tools supporting adjoint threading:

• Process Monitor

• Citrix CDFAnalyzer
<table>
<thead>
<tr>
<th>Date</th>
<th>Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2-5, 2012</td>
<td>Accelerated Windows Software Trace Analysis</td>
</tr>
<tr>
<td>November 16-26, 2012</td>
<td>Accelerated Windows Memory Dump Analysis</td>
</tr>
<tr>
<td>December 7-10, 2012</td>
<td>Accelerated Windows Malware Analysis</td>
</tr>
<tr>
<td>December 17, 2012</td>
<td>Philosophy of Software Diagnostics (FREE)</td>
</tr>
<tr>
<td>Early 2013</td>
<td>The New Old Debugging</td>
</tr>
</tbody>
</table>

**Debugging³**

Coming soon
Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV