Software Trace Analysis

Accelerated

Revised Version

Part 1: Fundamentals and Basic Patterns

Dmitry Vostokov
Software Diagnostics Services
What’s it all About?

- General trace and log analysis patterns
- Some examples are from Windows
Prerequisites

Basic OS troubleshooting
Training Goals

- Review tracing and logging fundamentals
- Learn basic trace and log analysis patterns
Training Principles

- Lots of pictures
- Pattern relationships
Part 1A: Fundamentals
Basic Concepts

- Software Trace (Log)
- Process
- Thread
- **Adjoint Thread**
- Component (Module or Source)
- File
- Function
- Message (Operation)
- Stack trace
Software Trace (Log)

- A sequence of formatted messages
- Arranged by time
- A narrative story
Process

- PID
- Session
- Image Name
- Modules (DLLs)
- Examples:

svchost.exe
- PID 1
- PID 2

notepad.exe
- PID 3
- PID 4
Thread

- TID
- CPU
- Context
## Adjoint Thread

### Debugging TV Frame 0x14

<table>
<thead>
<tr>
<th>Time (s)</th>
<th>Process Name</th>
<th>PID</th>
<th>TID</th>
<th>Operation</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>18:43:0</td>
<td>dwm.exe</td>
<td>1560</td>
<td>1868</td>
<td>RegQueryValue</td>
<td>HKC</td>
</tr>
<tr>
<td>18:43:0</td>
<td>dwm.exe</td>
<td>1560</td>
<td>1868</td>
<td>RegQueryValue</td>
<td>HKC</td>
</tr>
<tr>
<td>18:43:0</td>
<td>dwm.exe</td>
<td>1560</td>
<td>1868</td>
<td>RegQueryValue</td>
<td>HKC</td>
</tr>
</tbody>
</table>

---

**Properties...**
- Ctrl+P: Properties
- Ctrl+K: Toggle Bookmark
- Ctrl+B: Jump To...
- Ctrl+J: Search Online...
- Ctrl+I: Include / Exclude / Highlight
- Ctrl+E: Edit Filter
- Ctrl+V: Copy
- Ctrl+F: Filter
- Ctrl+S: Save
- Ctrl+H: Help

---

**Process Name**
- Image Path
- Command Line
- Company
- Description
- Version
- Architecture
- Path
- Operation
- Result
- Event Class
- Detail
- Category
- PID
- TID
- Parent PID
- User
- Session
- Virtualized

---

© 2020 Software Diagnostics Services
Component / Module / Source

- Module Name
- Source Folder

- ApplicationA.exe
- ModuleB.dll
- ModuleC.dll

\source\library\*\c
// MainApp.c
foo () {
    trace("foo: entry");
    // do stuff
    trace("foo: exit");
}
Trace Message

// MainApp.c
foo () {
    trace("foo: entry");
    int result = bar();
    trace("bar result: 5");
    trace("foo: exit");
}

Invariant Variable Invariant Variable …
// MainApp.c
main() {
    trace("start");
    foo();
}

foo() {
    trace("foo: entry");
    bar();
}

bar() {
    trace("bar: entry");
    // do stuff
}
## Minimal Trace Graphs

<table>
<thead>
<tr>
<th>No</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Date</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ModuleA</td>
<td>4280</td>
<td>1736</td>
<td>5/28/2012</td>
<td>08:53:50.496</td>
<td>Trace message 1</td>
</tr>
<tr>
<td>2</td>
<td>ModuleB</td>
<td>6212</td>
<td>6216</td>
<td>5/28/2012</td>
<td>08:53:52.876</td>
<td>Trace message 2</td>
</tr>
</tbody>
</table>
Common Trace Formats

- ETW
- CSV
- Free
- Mixed
Pattern-Driven Analysis

**Diagnostic Pattern**: a common recurrent identifiable problem together with a set of recommendations and possible solutions to apply in a specific context.

**Diagnostic Problem**: a set of indicators (symptoms, signs) describing a problem.

**Diagnostic Analysis Pattern**: a common recurrent analysis technique and method of diagnostic pattern identification in a specific context.

**Diagnostics Pattern Language**: common names of diagnostic and diagnostic analysis patterns. The same language for any operating system: Windows, Mac OS X, Linux, ...

---


Pattern-Based Analysis

Usage → Software Trace → Discovery

Pattern Catalog + New Pattern
Pattern Hierarchy

- **Domain Independent**
  from IBM mainframes to mobile and embedded computers

- **Domain Specific**
  - Windows log
  - Linux log
  - Cloud log
  - Mac OS X log
  - Web Server log
  - Network trace
  - GUI message log
Pattern Classification

- Vocabulary
- Error
- Trace as a Whole
- Large Scale
- Activity
- Message
- Block
- Trace Set
Part 1B: Basic Patterns
Vocabulary Patterns

- Basic Facts
- Vocabulary Index
Basic Facts

- **Problem Description**

Application disappears after launch

- **Software Trace**

<table>
<thead>
<tr>
<th>PID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td>3f6</td>
<td>Create process AppA: PID 4a5</td>
</tr>
<tr>
<td>4a5</td>
<td>AppA loads DLLC</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td>3f6</td>
<td>Create process AppB: PID 5b8</td>
</tr>
<tr>
<td>5b8</td>
<td>AppB loads DLLD</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
Basic Facts Taxonomy

- Functional Facts
  Example: Expected a dialog to enter data

- Non-functional Facts
  Example: CPU consumption 100%

- Identification Facts
  Application name, PID, user name
Problem Description

A user Test123 authentication failed

Narrowing:

Related Patterns

Basic Facts
Activity Region
Error Patterns

- Error Message
- Exception Stack Trace
- False Positive Error
- Periodic Error ↓ *
- Error Distribution

* ‘ ↓ ’ sign means that a pattern involves time dependency
Error Message

- Explicit errors
- Implicit errors
- WinDbg command !error

0:000> !error c0000017
Error code: (NTSTATUS) 0xc0000017 (3221225495) - {Not Enough Quota} Not enough virtual memory or paging file quota is available to complete the specified operation.

0:000> !error 5
Error code: (Win32) 0x5 (5) - Access is denied.
## Exception Stack Trace

<table>
<thead>
<tr>
<th>No</th>
<th>PID</th>
<th>TID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>[...]</td>
<td>265800</td>
<td>8984</td>
<td>4216</td>
</tr>
<tr>
<td>265803</td>
<td>8984</td>
<td>4216</td>
<td>at ComponentA.Store.GetData(Byte[] pKey)</td>
</tr>
<tr>
<td>265804</td>
<td>8984</td>
<td>4216</td>
<td>at ComponentA.App.EnumBusinessObjects()</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Periodic Error**

<table>
<thead>
<tr>
<th>Time</th>
<th>#</th>
<th>PID</th>
<th>TID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>36495</td>
<td>1788</td>
<td>2250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>36883</td>
<td>1788</td>
<td>1986</td>
</tr>
</tbody>
</table>

Related Patterns

- Error Message
- Error Distribution
- False Positive Error
- Message Invariant

© 2020 Software Diagnostics Services
False Positive Error

- Expected errors
- Not relevant to our problem
- Implementation details

Related Patterns

- Error Message
- Master Trace
- Activity Region
Error Distribution

Related Patterns
- Partition
- Activity Region
Trace as a Whole

- Partition
- Circular Trace
- Message Density
- Message Current
- Trace Acceleration
- No Trace Metafile
- Empty Trace
- Missing Component
- Guest Component
- Truncated Trace
- Visibility Limit
- Sparse Trace
Partition

Related Patterns

- Significant Event
- Truncated Trace
- Adjoint Thread
Message Density

Similar relative density for 2 traces may show correlation:

\[ D_1 > D_2 \]

For correlated messages, different densities from 2 traces may show different partition or system conditions:

\[ D_{11} / D_{21} = D_{12} / D_{22} \]

\[ D_{11} >> D_{12} \]
Message Current ↓

Related Patterns

- Significant Event
- Activity Region
- Message Density

\[ J_1 > J_2 \]
Trace Acceleration

Message current $J_i < J_j$, $i < j < N$

Partial message currents:

- with respect to TID X: $J_k(TID=x)$
- with respect to PID Y: $J_k(PID=y)$
- with respect to PID X and TID Z: $J_k(PID=y \& TID=z)$
No Trace Metafile

<table>
<thead>
<tr>
<th>#</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21372</td>
<td>dllA</td>
<td>2968</td>
<td>5476</td>
<td>3:55:10.004</td>
<td>Calling foo()</td>
</tr>
<tr>
<td>21374</td>
<td>Unknown</td>
<td>2968</td>
<td>5476</td>
<td>3:55:10.004</td>
<td>Unknown GUID=A1E38F24-613D-4D71-B9F5-... (No Format Information found)</td>
</tr>
<tr>
<td>21375</td>
<td>Unknown</td>
<td>2968</td>
<td>5476</td>
<td>3:55:10.004</td>
<td>Unknown GUID=A1E38F24-613D-4D71-B9F5-... (No Format Information found)</td>
</tr>
<tr>
<td>21376</td>
<td>Unknown</td>
<td>2968</td>
<td>5476</td>
<td>3:55:10.004</td>
<td>Unknown GUID=A1E38F24-613D-4D71-B9F5-... (No Format Information found)</td>
</tr>
<tr>
<td>21377</td>
<td>Unknown</td>
<td>2968</td>
<td>5476</td>
<td>3:55:10.004</td>
<td>Unknown GUID=A1E38F24-613D-4D71-B9F5-... (No Format Information found)</td>
</tr>
<tr>
<td>21378</td>
<td>dllA</td>
<td>2968</td>
<td>5476</td>
<td>3:55:10.004</td>
<td>Calling bar()</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Possible patterns to detect:

- Circular Trace
- Message Density
- Message Current
- Discontinuity
- Time Delta
- Trace Acceleration

Related Patterns

Thread of Activity
Empty Trace

- Small file size
- Very few trace messages

Always open a trace before sending to someone else
Missing Component

Related Patterns
- Discontinuity
- Inter-Correlation
- No Activity
Guest Component

Related Patterns

Missing Component

<table>
<thead>
<tr>
<th>#</th>
<th>PID</th>
<th>TID</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Load: 3rdPartyActivity.dll</td>
</tr>
</tbody>
</table>
Truncated Trace

Related Patterns
- Partition
- Anchor Messages
- Missing Component
Visibility Limit

Related Patterns
- Truncated Trace
- Missing Component
- Sparse Trace
Sparse Trace

Related Patterns
- Missing Component
- Visibility Limit

Time

# PID TID Time                  Message

Missing

PLOT
Large Scale Patterns

- Characteristic Message Block
- Background Components
- Foreground Components
- Layered Periodization
- Focus of Tracing
- Event Sequence Order
- Trace Frames
Bird’s Eye Binary View
Characteristic Message Block
Background Components

Related Patterns

Foreground Components
Foreground Components

Component Foregrounding

Related Patterns

Background Components
Layered Periodization
Focus of Tracing

Activity regions: \( J_{m1}, J_{m2}, J_{m3} \)
Event Sequence Order

Related Patterns

- Significant Event
- Anchor Messages

Synchronization
Race Conditions
Deadlock
Frames (Source Code)
Trace Frames

Related Patterns

- Thread of Activity
- Adjoint Thread
- Truncated Trace
- Discontinuity
Activity Patterns

- Thread of Activity ↓
- Adjoint Thread of Activity ↓
- No Activity
- Activity Region
- Discontinuity ↓
- Time Delta ↓
- Glued Activity
- Break-in Activity ↓
- Resume Activity ↓
- Data Flow ↓
Thread of Activity

Related Patterns
- Discontinuity
- Sparse Trace
Adjoint Thread of Activity

Related Patterns

Thread of Activity
Message Invariant
No Activity

We expect this process

Possible causes:

- hang, wait chain, deadlock,
- terminated threads, CPU loop

Related Patterns

- Discontinuity
- Sparse Trace
- Missing Component
Activity Region

Message current: $J_{m2} > \max(J_{m1}, J_{m3})$
Discontinuity

Possible causes:

- blocked thread, IPC response
- delay, wait chains, long computation

Related Patterns

- Thread of Activity
- Missing Component
- Sparse Trace
## Time Delta

![Time Delta Diagram]

### Related Patterns
- Basic Facts
- Thread of Activity
- Discontinuity
- Significant Event

### Time

<table>
<thead>
<tr>
<th>#</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Time</th>
<th>File</th>
<th>Function</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>6060</td>
<td>dllA</td>
<td>1604</td>
<td>7108</td>
<td>10:06:21.746</td>
<td>fileA.c</td>
<td>DllMain</td>
<td>DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>24480</td>
<td>dllA</td>
<td>1604</td>
<td>7108</td>
<td>10:06:32.262</td>
<td>fileA.c</td>
<td>LaunchApp</td>
<td>Exec Path: C:\Program Files\CompanyA\appB.exe</td>
</tr>
</tbody>
</table>

30 seconds of discontinuity till the end of full trace
Glued Activity

ATID: Adjoint Thread ID

ImageA
ATID 2

ImageB
ATID 3

Trace
Session 1

Trace
Session 2

Related Patterns

Adjoint Thread
Break-in Activity

Related Patterns

- Thread of Activity
- Adjoint Thread
- Discontinuity
- Resume Activity

Discontinuity
Resume Activity

Related Patterns
- Break-in Activity
- Thread of Activity
- Adjoint Thread
Data Flow

Related Patterns
Adjoint Thread
Message Invariant

[...]
DriverA: Device 0xA IRP 0xB
[...]
DriverB: Device 0xC IRP 0xB
[...]
DriverC: Device 0xD IRP 0xB
DriverC: Processing IRP 0xB
[...]
Message Patterns

- Significant Event
- Defamiliarizing Effect
- Anchor Messages
- Diegetic Messages
- Message Change
- Message Invariant
- UI Message
- Original Message
- Implementation Discourse
- Opposition Messages
- Linked Messages
- Gossip
- Counter Value
- Message Context
- Marked Messages
- Incomplete History
- Message Interleave
- Fiber Bundle
Significant Event

Related Patterns
- Exception Stack Trace
- Error Message
- Basic Facts
- Vocabulary Index
Poetry of Software Traces

“Capturing delicate moments, one gives birth to a poetry of traces …”

Ange Leccia, Motionless Journeys, by Fabien Danesi
Defamiliarizing Effect

Related Patterns

Characteristic message Block
Activity Region
## Anchor Messages

<table>
<thead>
<tr>
<th>#</th>
<th>PID</th>
<th>TID</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>24226</td>
<td>2656</td>
<td>3480</td>
<td>10:41:05.774</td>
<td>AppA.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>108813</td>
<td>4288</td>
<td>4072</td>
<td>10:41:05.774</td>
<td>AppB.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>112246</td>
<td>4180</td>
<td>3836</td>
<td>10:41:05.940</td>
<td>DllHost.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>135473</td>
<td>2040</td>
<td>3296</td>
<td>10:41:12.615</td>
<td>AppC.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>703962</td>
<td>5020</td>
<td>1080</td>
<td>10:44:42.014</td>
<td>DllHost.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>705511</td>
<td>4680</td>
<td>3564</td>
<td>10:44:42.197</td>
<td>DllHost.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>705891</td>
<td>1528</td>
<td>2592</td>
<td>10:44:42.307</td>
<td>regedit.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>785231</td>
<td>2992</td>
<td>4912</td>
<td>10:45:26.516</td>
<td>AppE.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>786523</td>
<td>3984</td>
<td>1156</td>
<td>10:45:26.605</td>
<td>powershell.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>817979</td>
<td>4188</td>
<td>4336</td>
<td>10:45:48.707</td>
<td>wermgr.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>834875</td>
<td>3976</td>
<td>1512</td>
<td>10:45:52.342</td>
<td>LogonUI.exe: DLL_PROCESS_ATTACH</td>
</tr>
<tr>
<td>835229</td>
<td>4116</td>
<td>3540</td>
<td>10:45:52.420</td>
<td>AppG.exe: DLL_PROCESS_ATTACH</td>
</tr>
</tbody>
</table>
Diegetic Messages

Related Patterns

Anchor Messages
Message Change

Related Patterns

- Anchor Messages
- Message Invariant
- Adjoint Thread
Implementation Discourse

- Win32 API
- MFC
- Kernel Development
- COM
- C# / .NET
- C++
- Java
- Python
- …
# Message Invariant

## Related Patterns

<table>
<thead>
<tr>
<th>#</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2782</td>
<td>ModuleA</td>
<td>2124</td>
<td>5648</td>
<td>10:58:03.356</td>
<td><strong>CreateObject:</strong> pObject 0x00A83D30 <strong>data ([...]) version</strong> 0x4</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4793</td>
<td>ModuleA</td>
<td>2376</td>
<td>8480</td>
<td>09:22:01.947</td>
<td><strong>CreateObject:</strong> pObject 0x00BA4E20 <strong>data ([...]) version</strong> 0x5</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## UI Message

<table>
<thead>
<tr>
<th>#</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[..]</td>
</tr>
<tr>
<td>2782 ModuleA 2124 5648 10:58:03.356</td>
<td>CreateWindow: Title &quot;...&quot;, Class &quot;...&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[..]</td>
</tr>
<tr>
<td>3512 ModuleA 2124 5648 10:58:08.154</td>
<td>Menu command: Save Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[..]</td>
</tr>
<tr>
<td>3583 ModuleA 2124 5648 10:58:08.155</td>
<td>CreateWindow: Title &quot;Save As&quot;, Class &quot;Dialog&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[.. Data update and replication related messages ..]</td>
</tr>
<tr>
<td>4483 ModuleA 2124 5648 10:58:12.342</td>
<td>DestroyWindow: Title &quot;Save As&quot;, Class &quot;Dialog&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[..]</td>
</tr>
<tr>
<td>2782 ModuleA 2124 5648 10:58:03.356</td>
<td>CreateWindow: Title &quot;...&quot;, Class &quot;...&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3512 ModuleA 2124 5648 10:58:08.154</td>
<td>Menu command: Save Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3583 ModuleA 2124 5648 10:58:08.155</td>
<td>CreateWindow: Title &quot;Save As&quot;, Class &quot;Dialog&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4483 ModuleA 2124 5648 10:58:12.342</td>
<td>DestroyWindow: Title &quot;Save As&quot;, Class &quot;Dialog&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Module</td>
<td>PID</td>
<td>TID</td>
<td>Time</td>
<td>Message</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35835</td>
<td>ModuleA</td>
<td>12332</td>
<td>11640</td>
<td>18:27:28.720</td>
<td>LoadLibrary: \Program Files\MyProduct\System32\MyDLL.dll PID 12332</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37684</td>
<td>ModuleA</td>
<td>12332</td>
<td>9576</td>
<td>18:27:29.063</td>
<td>LoadLibrary: \Program Files\MyProduct\System32\MyDLL.dll PID 12332</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37687</td>
<td>ModuleA</td>
<td>12332</td>
<td>9576</td>
<td>18:27:29.064</td>
<td>LoadLibrary: \Program Files\MyProduct\System32\MyDLL.dll PID 12332</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Linked Messages

Related Patterns

Adjoint Thread

<table>
<thead>
<tr>
<th>#</th>
<th>PID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>128762 1260</td>
<td>CreateProcess: PPID 1260 PID 6356</td>
</tr>
<tr>
<td></td>
<td>128785 6356</td>
<td>ImageLoad: AppA.exe PID 6356</td>
</tr>
<tr>
<td></td>
<td>131137 6356</td>
<td>CreateProcess: PPID 6356 PID 6280</td>
</tr>
<tr>
<td></td>
<td>131239 6280</td>
<td>ImageLoad: AppB.exe PID 6280</td>
</tr>
<tr>
<td></td>
<td>132899 6356</td>
<td>CreateProcess: PPID 6356 PID 8144</td>
</tr>
<tr>
<td></td>
<td>132906 8144</td>
<td>ImageLoad: AppC.exe PID 8144</td>
</tr>
<tr>
<td>#</td>
<td>Module</td>
<td>PID</td>
</tr>
<tr>
<td>---</td>
<td>--------</td>
<td>------</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26875</td>
<td>ModuleA</td>
<td>2172</td>
</tr>
<tr>
<td>26876</td>
<td>ModuleB</td>
<td>2172</td>
</tr>
<tr>
<td>26877</td>
<td>ModuleC</td>
<td>2172</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26875</td>
<td>ModuleA</td>
<td>2172</td>
<td>5284</td>
<td>LoadImage: \Device\HarddiskVolume2\Windows\System32\notepad.exe PID 0x0000000000087C</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33132</td>
<td>ModuleA</td>
<td>4180</td>
<td>2130</td>
<td>LoadImage: \Device\HarddiskVolume2\Windows\System32\calc.exe PID 0x0000000001054</td>
</tr>
</tbody>
</table>
Counter Value

Module Variable


Performance-specific patterns:

Global Monotonicity
Constant Value

Related Patterns

Adjoint Thread
Significant Event
Activity Region
Focus of Tracing
Characteristic Message Block
Message Context

Related Patterns

- Significant Event
- Anchor Message
Marked Messages

Annotated messages:

- session database queries [+]  
- session initialization [-]  
- socket activity [+]
- process A launched [+]
- process B launched [-]
- process A exited [-]

[+] activity is present in a trace  
[-] activity is undetected or not present
Incomplete History

Code:

- Response-complete
- Exception-complete
- Call-complete

Related Patterns

- Opposition Messages
- Sparse Trace
- Truncated Trace
- Master Trace
Opposition Messages

- open - close
- create – destroy (discard)
- allocate - free (deallocation)
- call - return
- enter - exit (leave)
- load - unload
- save - load
- lock - unlock
- map - unmap

Related Patterns

<table>
<thead>
<tr>
<th>Incomplete History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sparse Trace</td>
</tr>
</tbody>
</table>
Block Patterns

- Macrofunction
- Periodic Message Block
- Intra-Correlation
<table>
<thead>
<tr>
<th>#</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42582</td>
<td>DBClient</td>
<td>5492</td>
<td>9476</td>
<td>11:04:33.398</td>
<td>Opening connection</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42585</td>
<td>DBClient</td>
<td>5492</td>
<td>9476</td>
<td>11:04:33.398</td>
<td>Sending SQL command</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42589</td>
<td>DBServer</td>
<td>6480</td>
<td>10288</td>
<td>11:04:33.399</td>
<td>Executing SQL command</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42592</td>
<td>DBClient</td>
<td>5492</td>
<td>9476</td>
<td>11:04:33.400</td>
<td>Closing connection</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Periodic Message Block

Related Patterns

- Periodic Error
- Adjoint Thread
- Invariant Message
- Discontinuity
Intra-Correlation

Handle: 00050586 Class: "Application A Class" Title: ""
Title changed at 15:52:4:3 to "Application A"
Title changed at 15:52:10:212 to "Application A - File1"
[...]
Process ID: 89c
Thread ID: d6c
[...]
Visible: true
Window placement command: SW_SHOWNORMAL
Placement changed at 15:54:57:506 to SW_SHOWMINIMIZED
Placement changed at 15:55:2:139 to SW_SHOWNORMAL
Foreground: false
Foreground changed at 15:52:4:3 to true
Foreground changed at 15:53:4:625 to false
Foreground changed at 15:53:44:498 to true
Foreground changed at 15:53:44:498 to false
Foreground changed at 15:53:44:552 to false
Foreground changed at 15:53:45:887 to true
Foreground changed at 15:53:47:244 to false
Foreground changed at 15:53:47:244 to true
Foreground changed at 15:53:47:353 to false
Foreground changed at 15:54:26:416 to true
Foreground changed at 15:54:27:55 to false
Foreground changed at 15:54:27:55 to true
Foreground changed at 15:54:27:180 to false
[...]

Handle: 000D0540 Class: "App B" Title: "Application B"
[...]
Process ID: 3ac
Thread ID: bd4
[...]
Foreground: false
Foreground changed at 15:50:36:972 to true
Foreground changed at 15:50:53:732 to false
Foreground changed at 15:50:53:732 to true
Foreground changed at 15:50:53:826 to false
Foreground changed at 15:51:51:352 to true
Foreground changed at 15:51:53:941 to false
Foreground changed at 15:53:8:135 to true
Foreground changed at 15:53:8:182 to false
Foreground changed at 15:53:10:178 to true
Foreground changed at 15:53:13:938 to false
Foreground changed at 15:53:30:443 to true
Foreground changed at 15:53:31:20 to false
Foreground changed at 15:53:31:20 to true
Foreground changed at 15:53:31:129 to false
[...]
Trace Set Patterns

- Master Trace
- Bifurcation Point
- Inter-Correlation
- Relative Density
- News Value
- Impossible Trace
- Split Trace
Master Trace

Related Patterns
- Activity Regions
- Background Components
- Foreground Components
- Event Sequence Order
- Guest Component
- Implementation Discourse
- Bifurcation Point
Bifurcation Point

Software Trace Diagrams

#  PID  TID  Message
-----------------------------------
[...]
25 2768 3056 Trace Statement A
26 3756 2600 Trace Statement B
27 3756 2600 Trace Statement C
[...]
149 3756 836 Query result: X
150 3756 836 Trace Statement 150.1
151 3756 836 Trace Statement 151.1
152 3756 836 Trace Statement 152.1
153 3756 836 Trace Statement 153.1
[...]
27 2768 3056 Trace Statement A
28 3756 2176 Trace Statement B
29 3756 2176 Trace Statement C
[...]
151 3756 5940 Query result: Y
152 3756 5940 Trace Statement 152.2
153 3756 5940 Trace Statement 153.2
154 3756 5940 Trace Statement 154.2
155 3756 5940 Trace Statement 155.2
[...]

© 2020 Software Diagnostics Services
Inter-Correlation

Tracing Tool

System

Tracing Tool

Trace File

Trace File

Related Patterns

Intra-Correlation
Basic Facts
Discontinuity
Sparse Trace

© 2020 Software Diagnostics Services
Relative Density

Related Patterns

Message Density
News Value

Related Patterns
- Inter-Correlation
- Basic Facts
- Master Trace
# Impossible Trace

<table>
<thead>
<tr>
<th>#</th>
<th>Module</th>
<th>PID</th>
<th>TID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>[…]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>ModuleA</td>
<td>202</td>
<td>404</td>
<td>foo: start</td>
</tr>
<tr>
<td>1002</td>
<td>ModuleA</td>
<td>202</td>
<td>404</td>
<td>foo: end</td>
</tr>
</tbody>
</table>

```
void foo()
{
    TRACE("foo: start");
    bar();
    TRACE("foo: end");
}

void bar()
{
    TRACE("bar: start");
    // some code ...
    TRACE("bar: end");
}
```
Split Trace

Related Patterns

Circular Trace
Resources

- TraceAnalysis.org / SoftwareDiagnostics.Institute / PatternDiagnostics.com
- Debugging.TV / YouTube.com/DebuggingTV / YouTube.com/PatternDiagnostics
- Software Trace and Memory Dump Analysis
- Software Diagnostics: Collected Seminars
- Theoretical Software Diagnostics
- Trace and Log Analysis: A Pattern Reference for Diagnostics and Anomaly Detection
Q&A

Please send your feedback using the contact form on PatternDiagnostics.com

© 2020 Software Diagnostics Services
Thank you for attendance!