



Malware Narratives

Introduction

Revised Version

Dmitry Vostokov
Software Diagnostics Services

Prerequisites

Interest in software diagnostics and malware analysis

Why?

- ⦿ Communication language
- ⦿ Malware diagnostics as software diagnostics
- ⦿ Big DA+TA (Dump Artifacts + Trace Artifacts)

Software Diagnostics

A discipline studying signs of software structure and behavior in software execution artifacts (such as memory dumps, software and network traces and logs) using **systemic** and **pattern-oriented** analysis methodologies.

Diagnostics Pattern

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

Pattern Orientation

Pattern-driven

- ◉ Finding patterns in software artefacts
- ◉ Using checklists and pattern catalogs

Pattern-based

- ◉ Pattern catalog evolution
- ◉ Catalog packaging and delivery

Catalog Classification

- ◎ By abstraction

Meta-patterns

- ◎ **By artifact type**

Software Log* Memory Dump Network Trace*

- ◎ By story type

Problem Description Software Disruption UI Problem

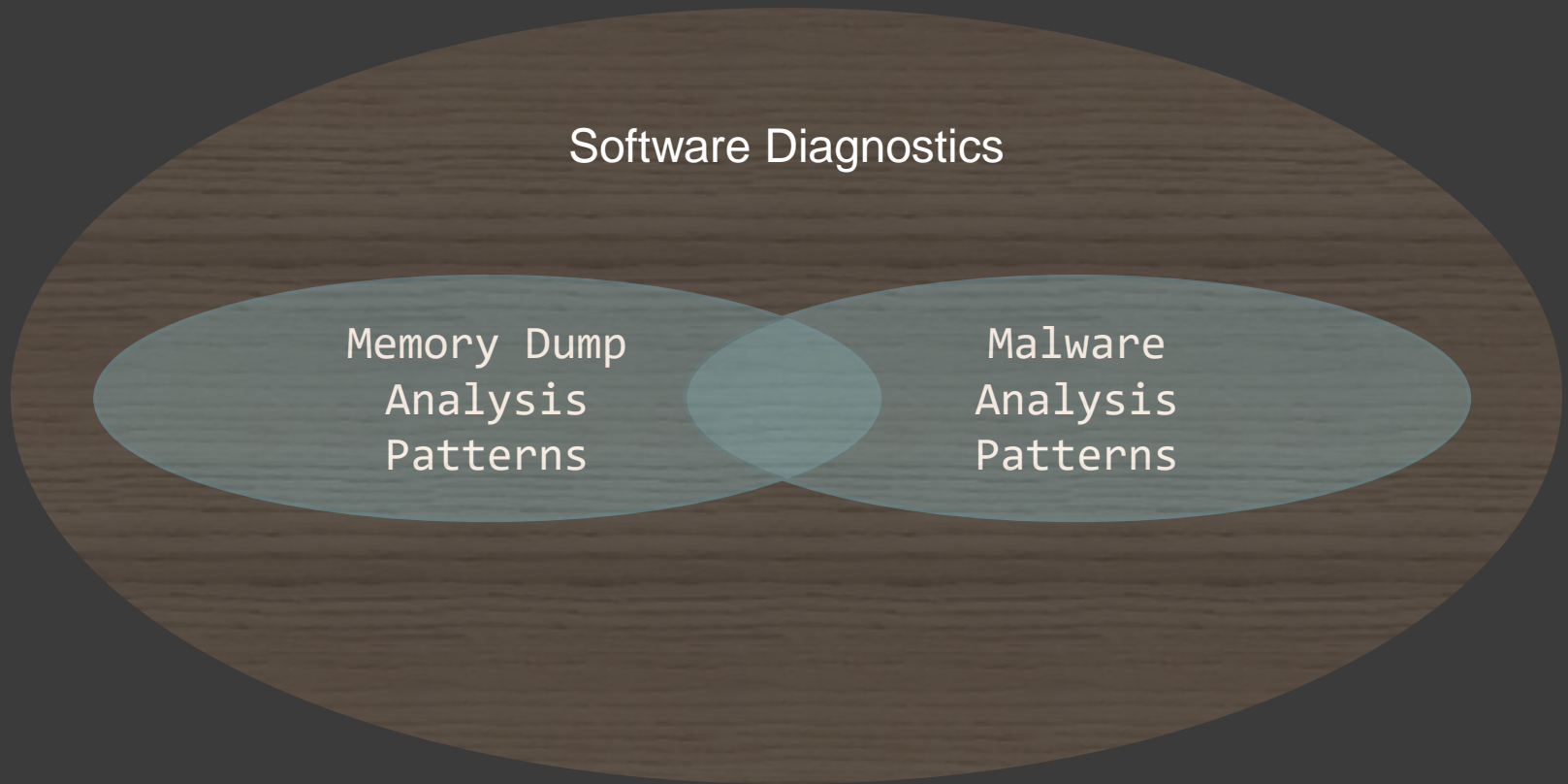
- ◎ **By intention**

Malware

Malware

Software that uses **planned alteration** of structure and behavior of software to serve malicious purposes.

Memory Analysis Patterns



Traces and Logs

Windows logs
and patterns

Linux logs
and patterns

macOS logs
and patterns

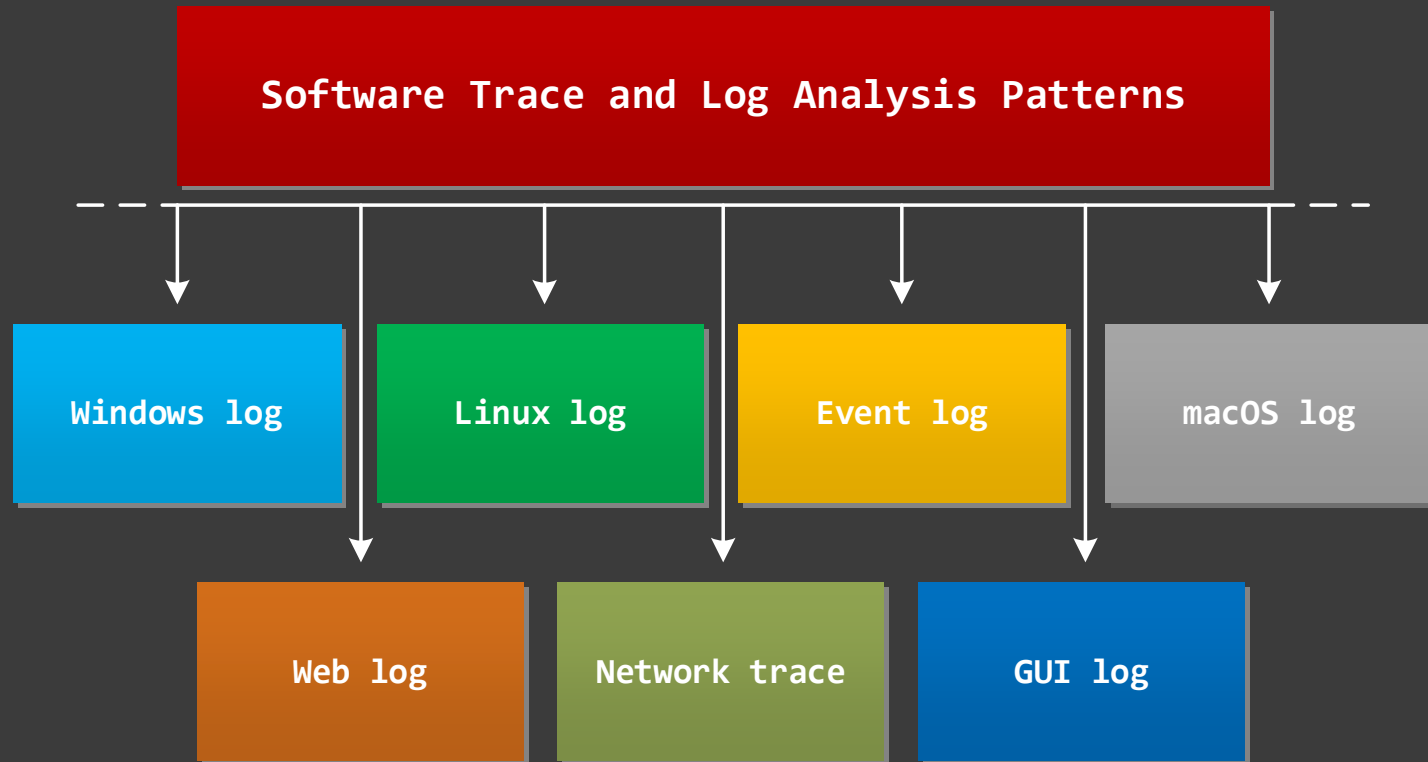
Event logs
and patterns

Web logs
and patterns

GUI logs
and patterns

Network traces
and patterns

Trace and Log Patterns



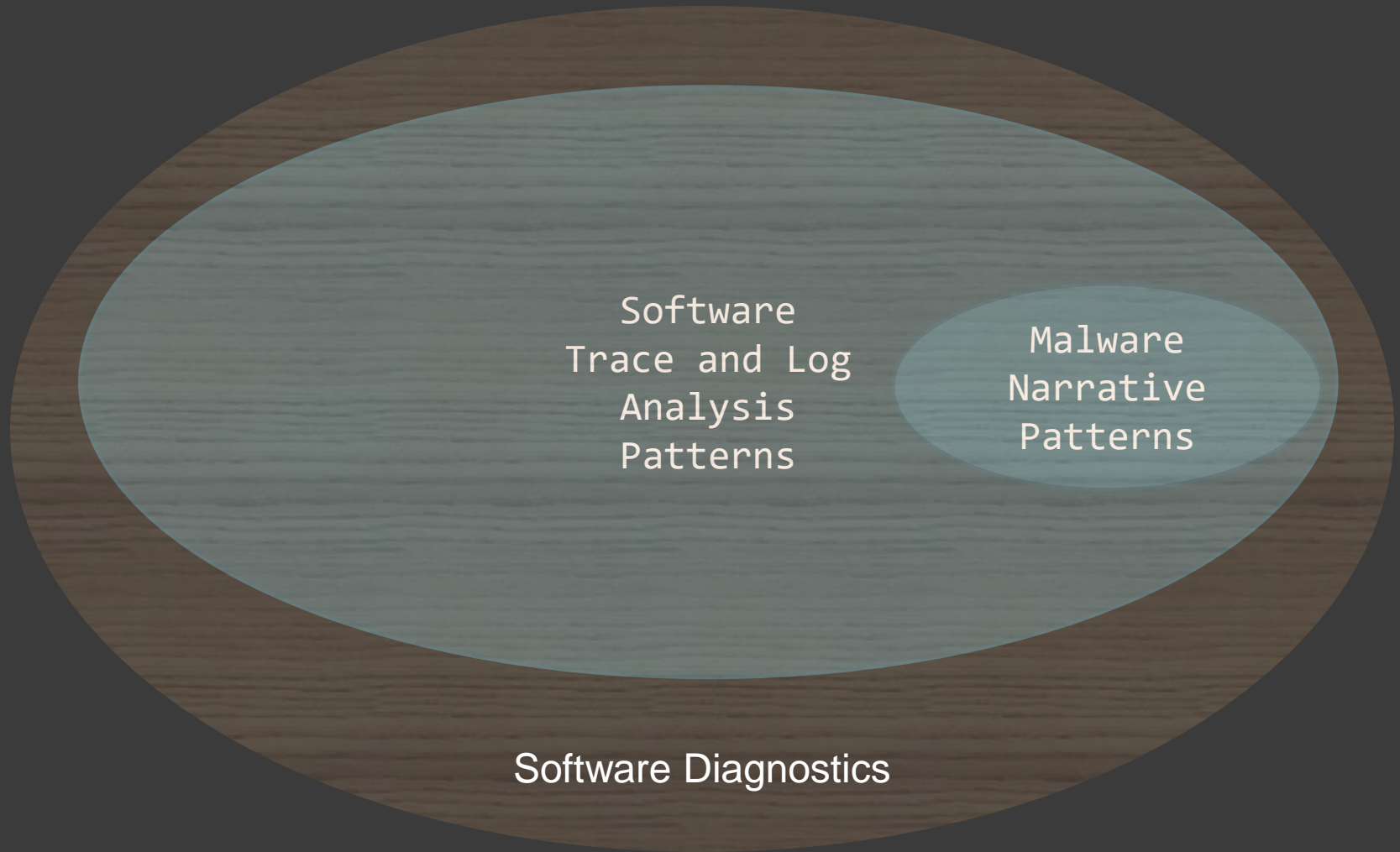
Software Narrative

A temporal sequence of events related to software execution.

Narrative Taxonomy

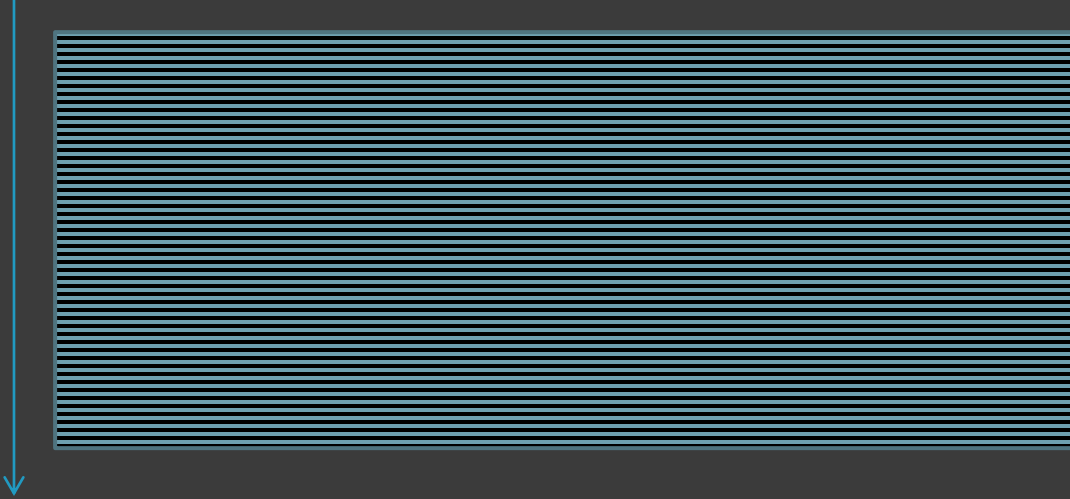
- ⦿ Incident stories
- ⦿ **Software traces and logs**
- ⦿ Malware analysis stories

Malware Narrative Patterns



Software Log

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



Minimal Trace Graphs

Time



No	Module	PID	TID	Date	Time	Message
1	ModuleA	4280	1736	5/28/2012	08:53:50.496	Trace message 1
2	ModuleB	6212	6216	5/28/2012	08:53:52.876	Trace message 2
[...]						

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.

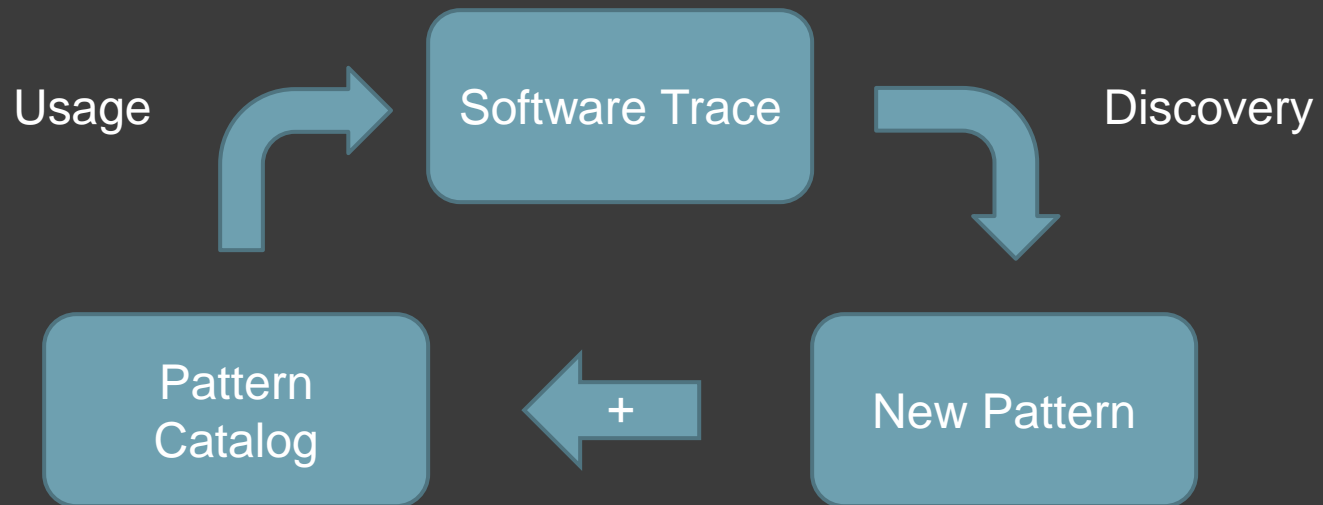
Diagnostics Pattern Language: common names of diagnostic and diagnostic analysis patterns. The same language for any operating system: Windows, macOS, Linux, ...



Checklist: <http://www.dumpanalysis.org/blog/index.php/2011/03/10/software-trace-analysis-checklist/>

Patterns: <http://www.dumpanalysis.org/blog/index.php/trace-analysis-patterns/>

Pattern-Based Analysis



Pattern Classification

- ⦿ Vocabulary
- ⦿ Error
- ⦿ Trace as a Whole
- ⦿ Large Scale
- ⦿ Activity
- ⦿ Message
- ⦿ Block
- ⦿ Trace Set

Reference and Course

- Catalog

[Software Trace and Log Analysis Patterns](#)

- Free reference graphical slides

[Accelerated-Software-Trace-Analysis-Part1-Public.pdf](#)

- Training course

[Accelerated Software Trace Analysis](#)

Vocabulary Patterns

- ◎ **Basic Facts***
- ◎ Vocabulary Index

* patterns marked with yellow color are most likely to be useful for malware detection and analysis

Error Patterns

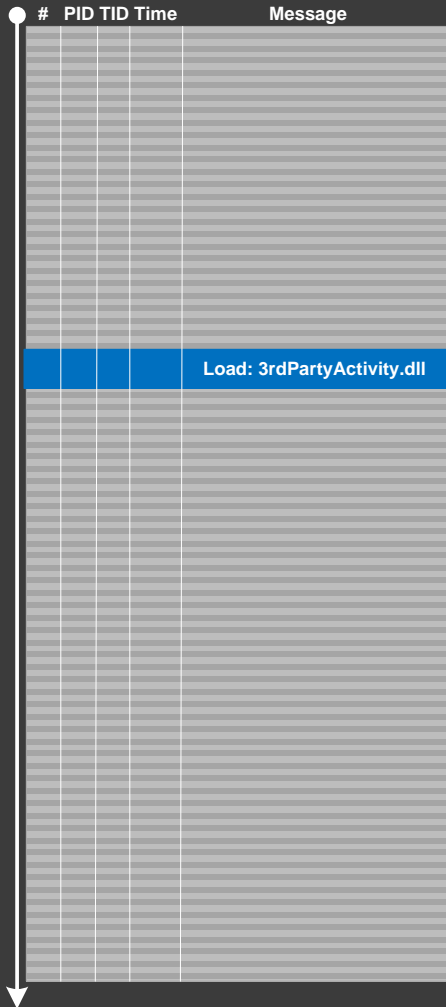
- ⦿ Error Message
- ⦿ Exception Stack Trace
- ⦿ False Positive Error
- ⦿ Periodic Error
- ⦿ Error Distribution

Trace as a Whole

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

Guest Component

Time

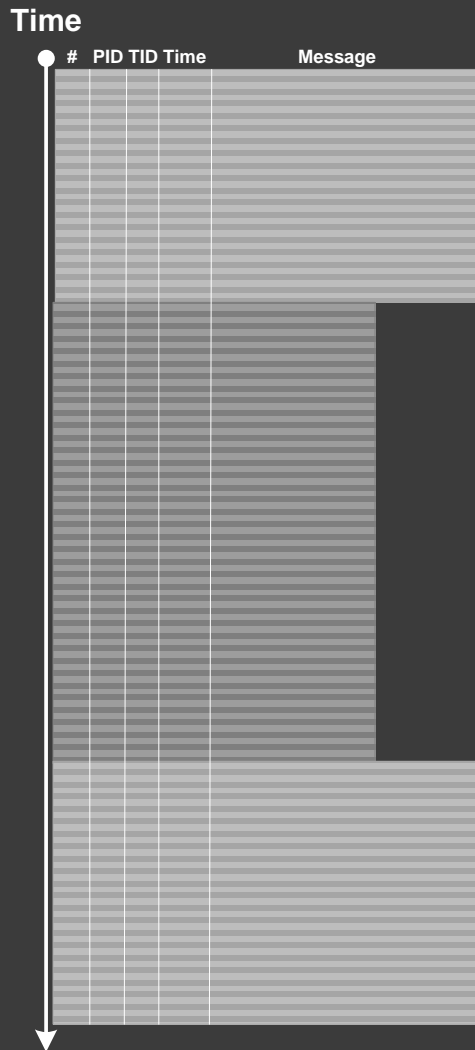


#	PID	TID	Time	Message
				Load: 3rdPartyActivity.dll

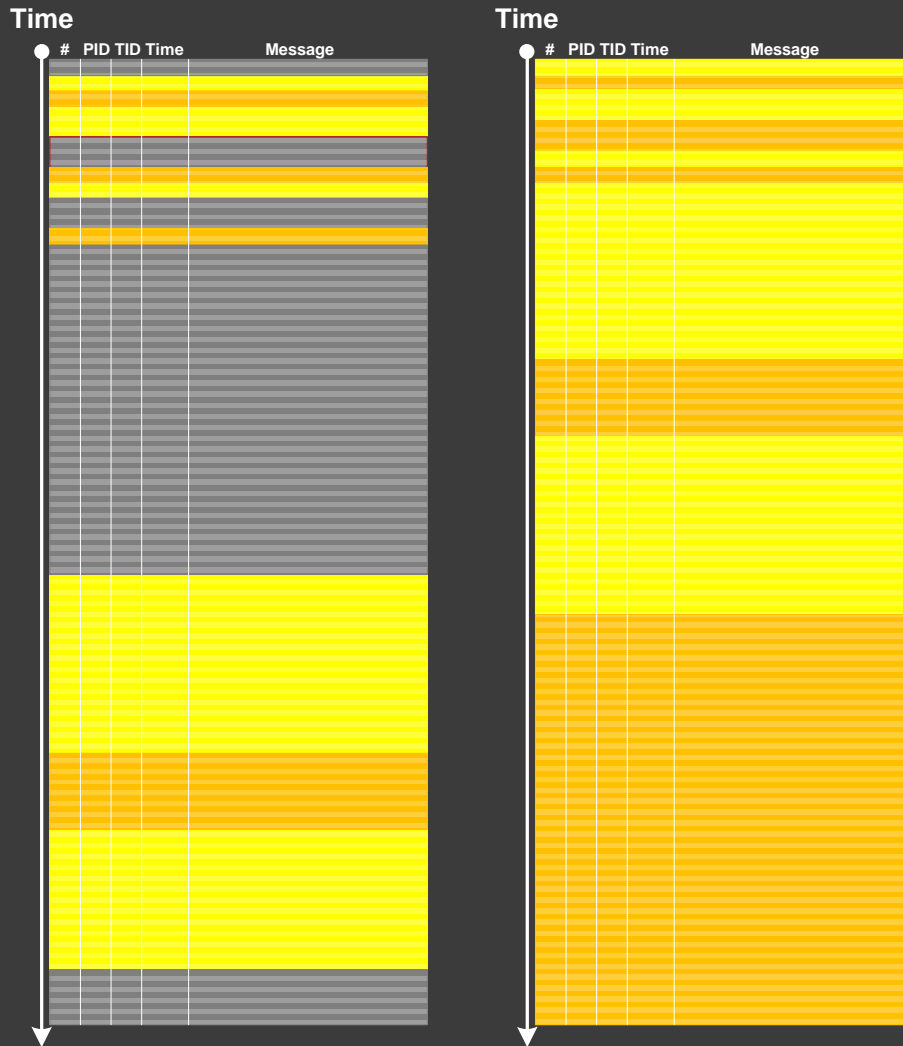
Large Scale Patterns

- ⦿ Characteristic Message Block
- ⦿ Background Components
- ⦿ Foreground Components
- ⦿ Layered Periodization
- ⦿ Focus of Tracing
- ⦿ Event Sequence Order
- ⦿ Trace Frames

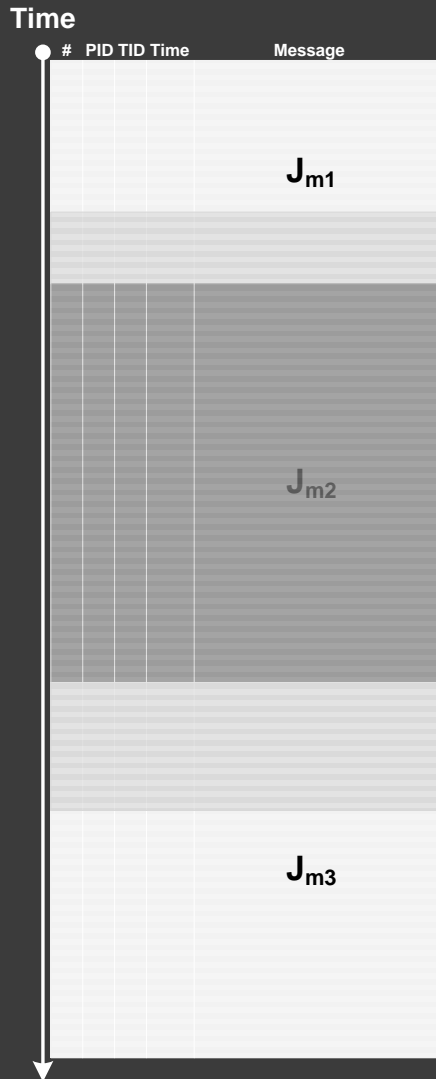
Characteristic Message Block



Foreground Components



Focus of Tracing

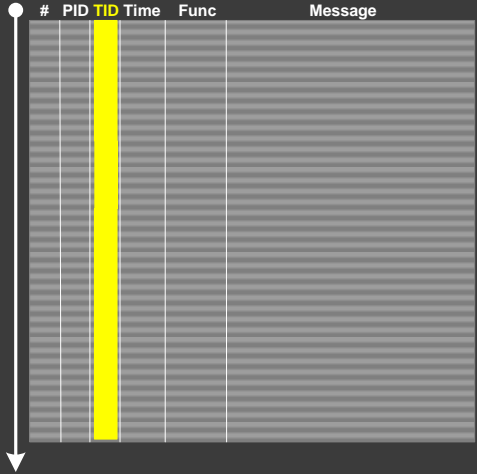
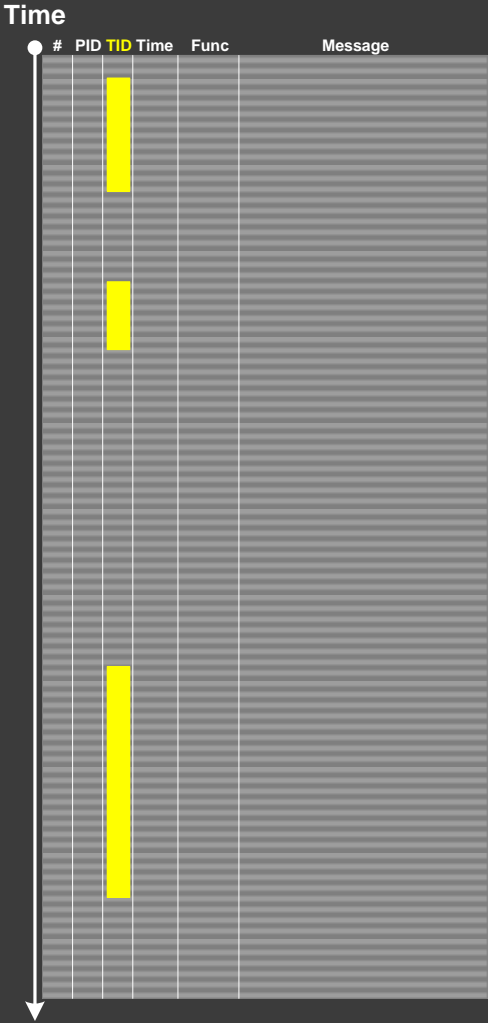


Activity regions: J_{m1} , J_{m2} , J_{m3}

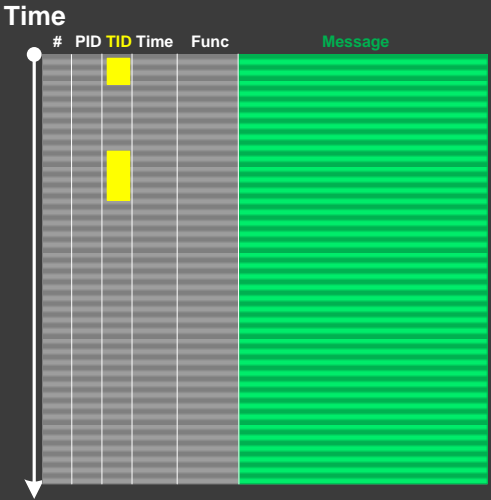
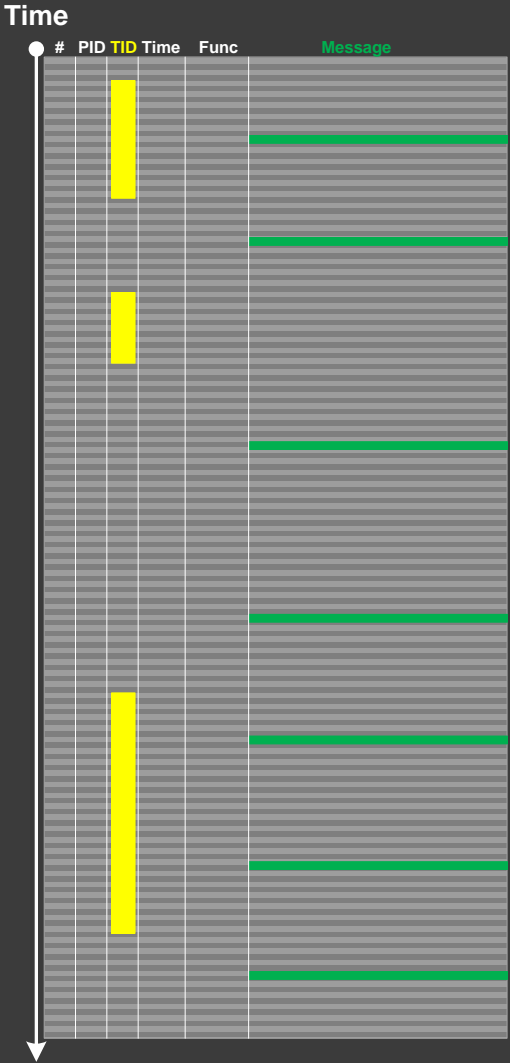
Activity Patterns

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

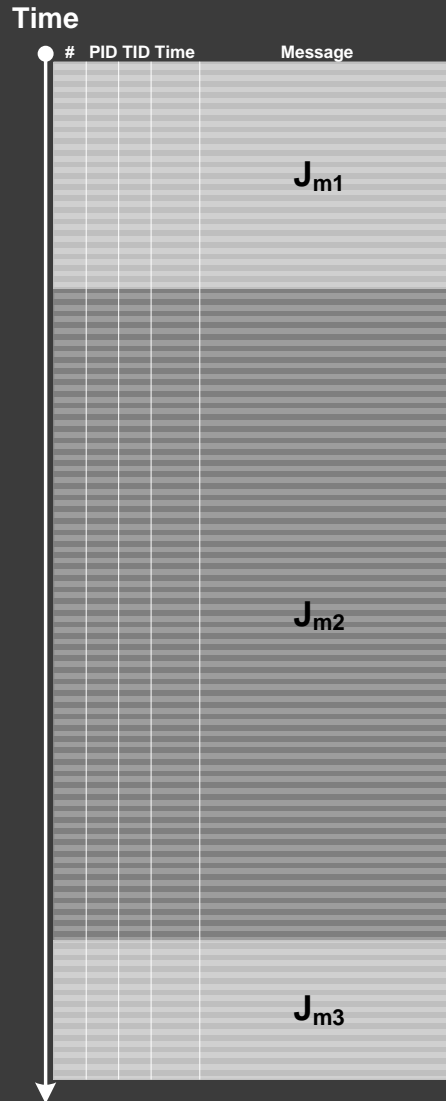
Thread of Activity



Adjoint Thread of Activity

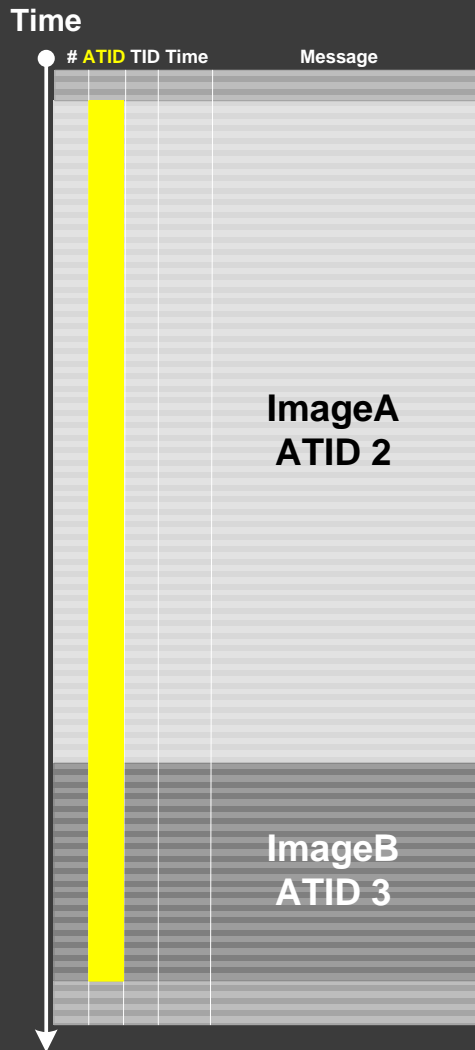


Activity Region

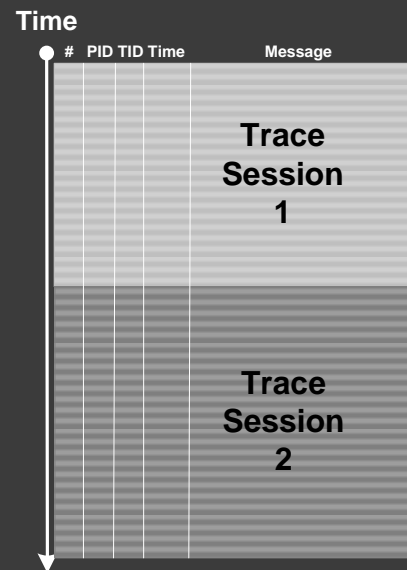


Message current : $J_{m2} > \max (J_{m1}, J_{m3})$

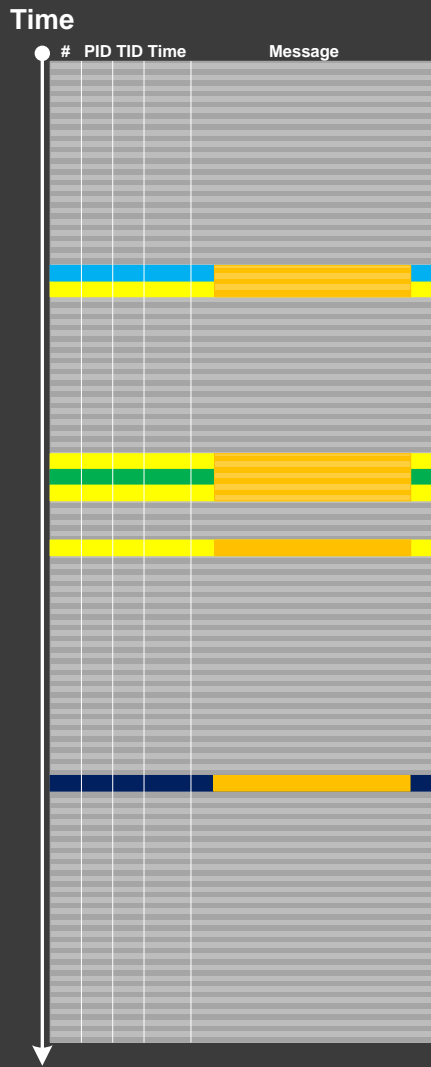
Glued Activity



ATID: Adjoint Thread ID



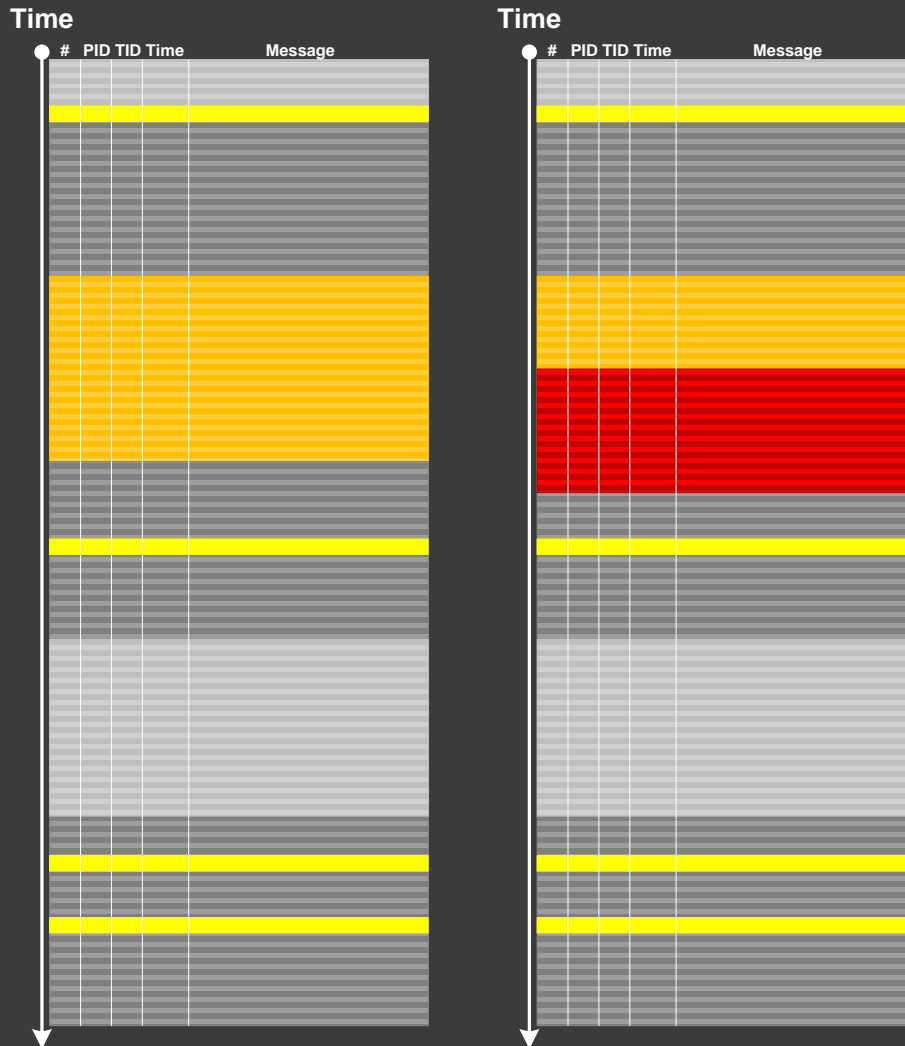
Data Flow



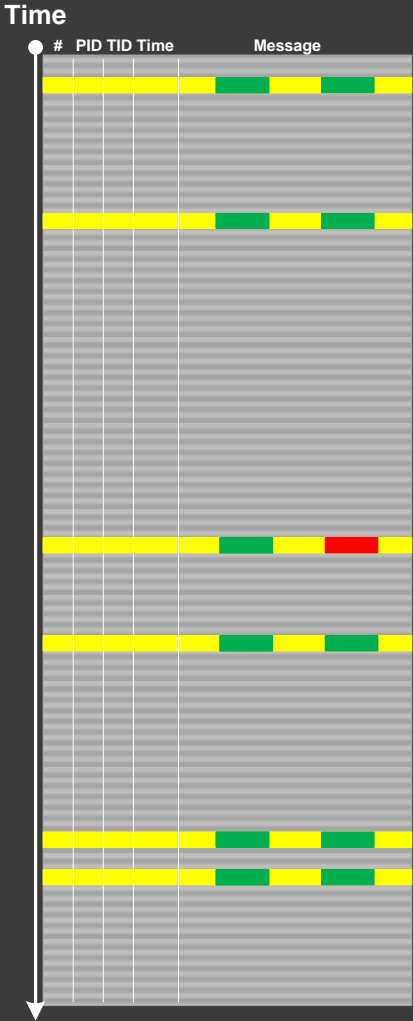
Message Patterns

- ◉ 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
- ◉ Abnormal Value
- ◉ Message Context
- ◉ Marked Messages
- ◉ Incomplete History
- ◉ Message Interleave
- ◉ Fiber Bundle

Defamiliarizing Effect



Abnormal Value



Marked Messages

Annotated messages:

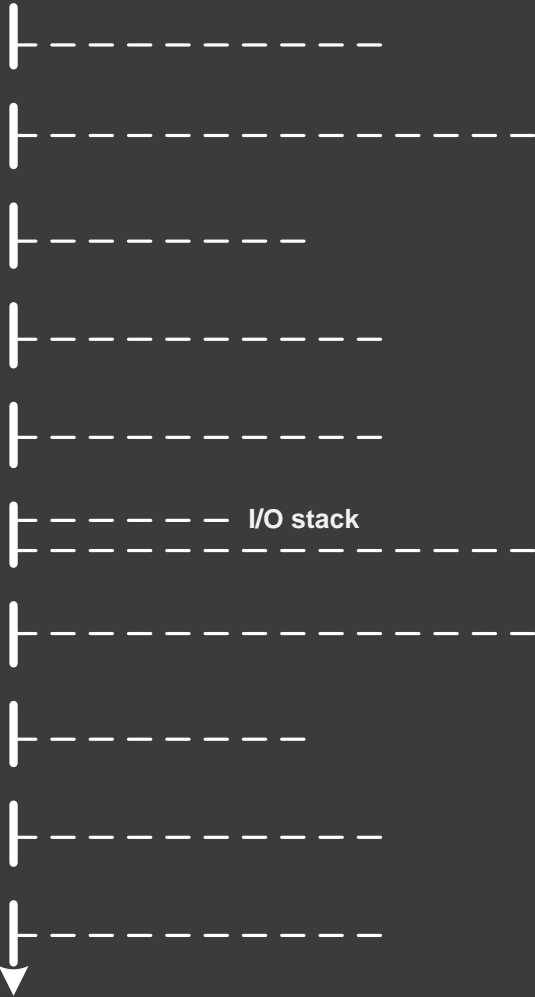
```
network activity [+]  
process A launched [+]  
process B launched [-]  
process A exited [-]
```

[+] activity is present in a trace

[-] activity is undetected or not present

Fiber Bundle

Trace
messages



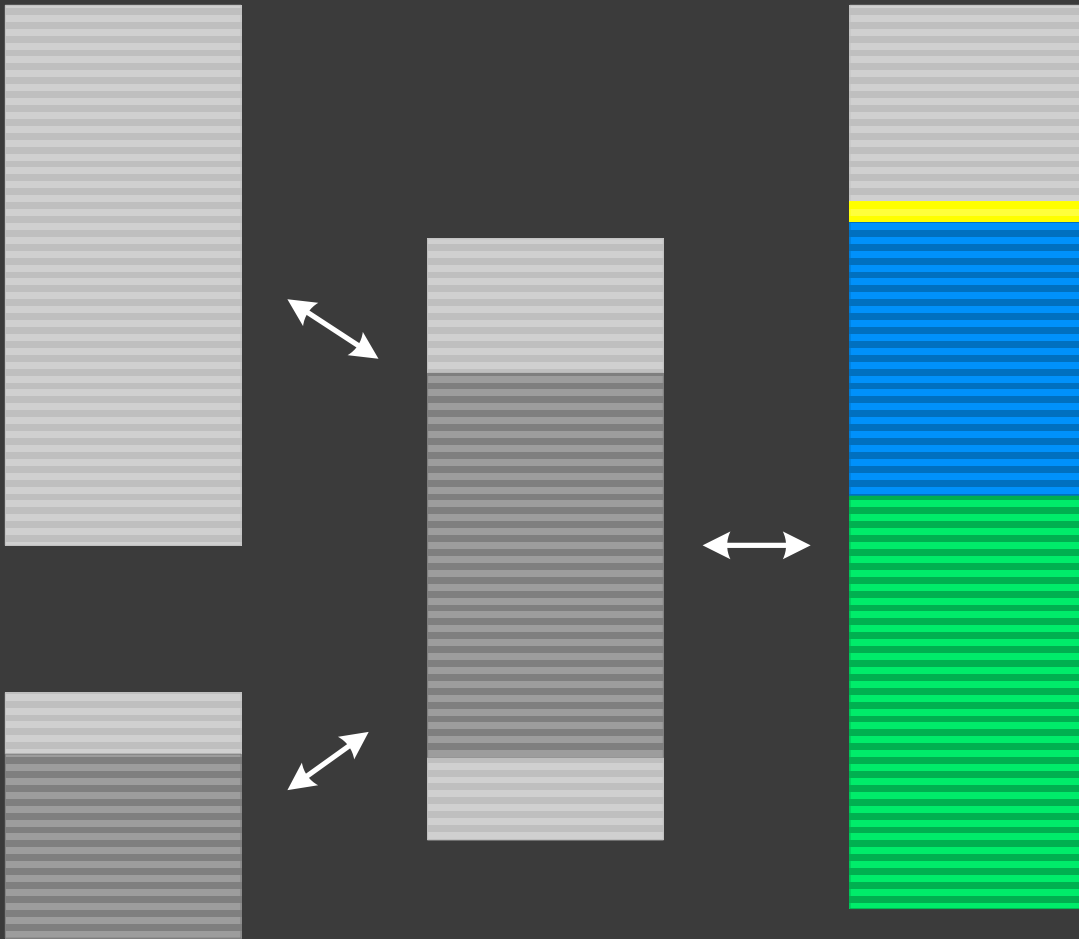
Block Patterns

- ⦿ Macrofunction
- ⦿ **Periodic Message Block**
- ⦿ Intra-Correlation

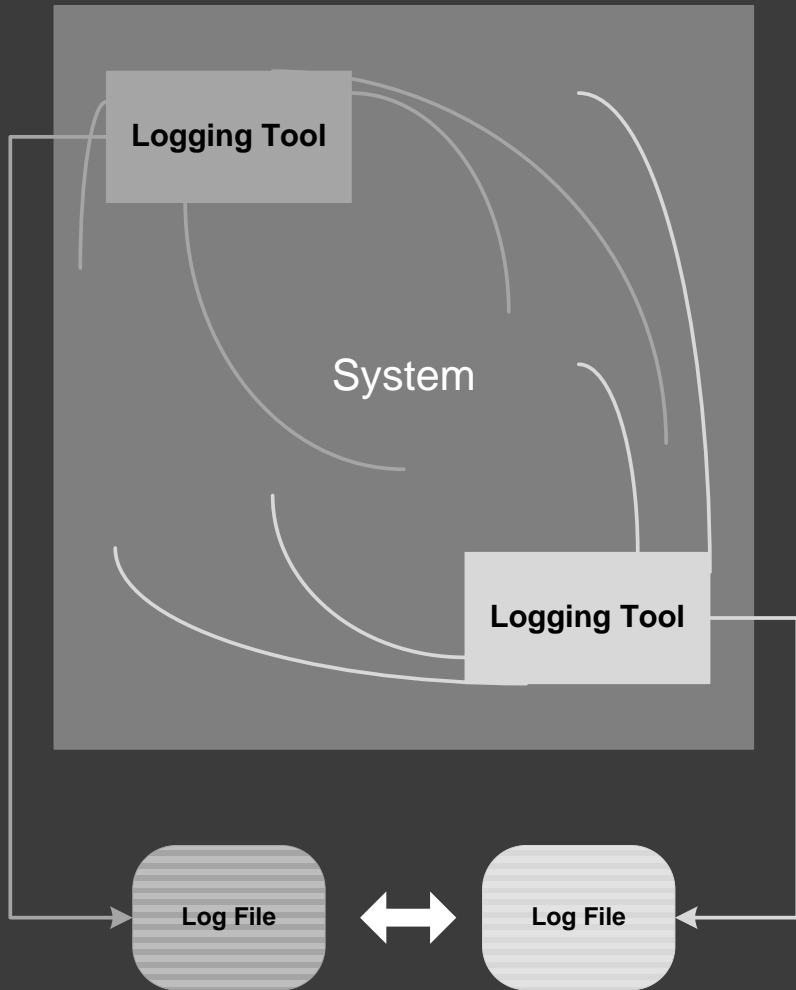
Trace Set Patterns

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

Master Trace



Inter-Correlation



Impossible Trace

```
#      Module  PID TID Message
-----
[...]  
1001 ModuleA 202 404 foo: start  
1002 ModuleA 202 404 foo: end  
[...]
```

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

Grand Unification

- ⦿ Narrative and Trace

$$N: T \rightarrow M$$

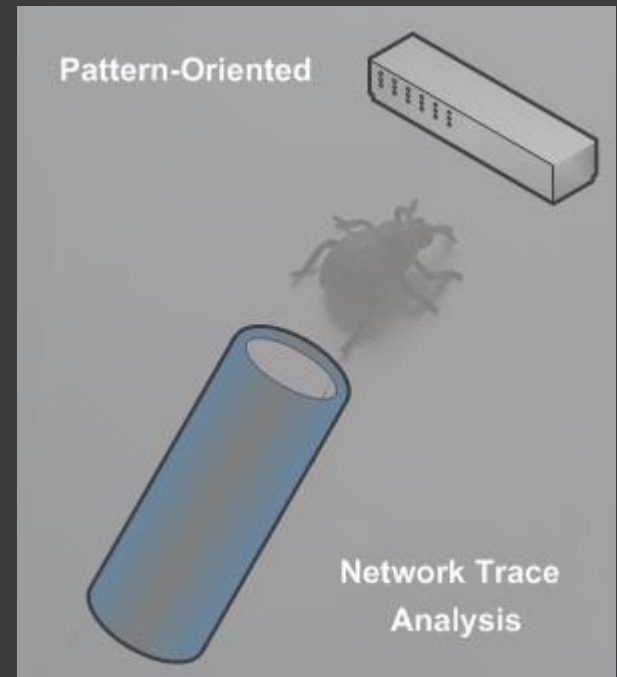
- ⦿ Generalized Narrative and Trace

$$GN: A \rightarrow M$$

$$GN_3 \circ GN_2 \circ GN_1: M \rightarrow M \rightarrow M$$

Further Reading

- ◉ [Software Diagnostics Institute](#)
- ◉ [Debugging.TV / YouTube.com/DebuggingTV / YouTube.com/PatternDiagnostics](#)
- ◉ [Software Trace and Memory Dump Analysis](#)
- ◉ [Pattern-Driven Software Diagnostics](#)
- ◉ [Systemic Software Diagnostics](#)
- ◉ [Pattern-Based Software Diagnostics](#)
- ◉ [Philosophy of Software Diagnostics](#)
- ◉ [Theoretical Software Diagnostics](#)
- ◉ [Software Narratology](#)
- ◉ [Malnarratives](#)
- ◉ [Pattern-Oriented Network Trace Analysis](#)
- ◉ [Accelerated Software Trace Analysis](#)



Historical Reference

[Memory Dump Analysis Anthology \(Diagnomicon\)](#): 14 volumes



Volume 15 is planned for 2023

Alphabetical Reference

[Trace, Log, Text, Narrative, Data: An Analysis Pattern Reference for Information Mining, Diagnostics, Anomaly Detection, Fifth Edition](#)

11.07.41.8857853	AlocFree.exe	16548	24216	CreateFile
11.07.41.8858445	AlocFree.exe	16548	24216	CreateFile
11.07.41.8859881	AlocFree.exe	16548	24216	Load Image
11.07.41.8861523	AlocFree.exe	16548	24216	Load Image
11.07.41.8864463	AlocFree.exe	16548	24216	RegOpenKey
11.07.41.8864463	AlocFree.exe	16548	24216	RegQueryValue
11.07.41.8864795	AlocFree.exe	16548	24216	RegOpenKey
11.07.41.8864795	AlocFree.exe	16548	24216	RegQueryValue
Trace, Log, Text, Narrative, Data				
An Analysis Pattern Reference for Information				
Mining, Diagnostics, Anomaly Detection				
11.07.41.9535576	AlocFree.exe	16548	24216	RegOpenKey
11.07.41.9536266	AlocFree.exe	16548	24216	RegQueryValue
11.07.41.9536452	AlocFree.exe	16548	24216	RegCloseKey
11.07.41.9536730	AlocFree.exe	16548	24216	RegOpenKey
11.07.41.9538099	AlocFree.exe	16548	24216	RegQueryValue
11.07.41.9538246	AlocFree.exe	16548	24216	RegCloseKey
11.07.41.9542755	AlocFree.exe	16548	24216	RegOpenKey
11.07.41.9543081	AlocFree.exe	16548	24216	RegOpenKey
11.07.41.9543359	AlocFree.exe	16548	24216	RegQueryValue
11.07.41.9549583	AlocFree.exe	16548	24216	QueryNameInformationFile
11.07.43.0824221	AlocFree.exe	16548	24216	QueryNameInformationFile
11.07.43.0835516	WerFault.exe	19852	9468	Process Start
11.07.43.0835764	WerFault.exe	19852	9468	Thread Create
11.07.43.0860141	WerFault.exe	19852	21920	Load Image
11.07.43.0862429	WerFault.exe	19852	21920	Load Image
11.07.43.0864898	WerFault.exe	19852	21920	CreateFile
11.07.43.0865749	WerFault.exe	19852	21920	QueryStandardInformationFile
11.07.43.0866365	WerFault.exe	19852	21920	ReadFile
11.07.43.0867376	WerFault.exe	19852	21920	CloseFile
11.07.43.0869913	WerFault.exe	19852	21920	RegOpenKey
11.07.43.0870235	WerFault.exe	19852	21920	RegQueryValue
11.07.43.0870748	WerFault.exe	19852	21920	RegOpenKey
11.07.43.0871219	WerFault.exe	19852	21920	RegOpenKey
11.07.43.0871617	WerFault.exe	19852	21920	RegQueryValue
11.07.43.0871973	WerFault.exe	19852	21920	RegCloseKey
11.07.43.0876755	WerFault.exe	19852	21920	RegCloseKey
11.07.43.0880236	WerFault.exe	19852	21920	Load Image
11.07.43.0884053	WerFault.exe	19852	21920	Load Image
11.07.43.0894709	WerFault.exe	19852	21920	RegOpenKey
11.07.43.0895355	WerFault.exe	19852	21920	RegOpenKey
11.07.43.0895795	WerFault.exe	19852	21920	RegOpenKey
11.07.43.0896200	WerFault.exe	19852	21920	RegOpenKey
11.07.43.0896598	WerFault.exe	19852	21920	RegOpenKey
11.07.43.0897105	WerFault.exe	19852	21920	RegQueryValue
11.07.43.0897496	WerFault.exe	19852	21920	RegCloseKey

[A Guide to Learning Software Trace and Log Analysis Patterns](#)

Q&A

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

Thank you for attendance!