




Memory Forensics

Pattern-Oriented

Revised Version

Dmitry Vostokov
Software Diagnostics Services

Forensics



A discipline studying past structure and behavior.

Memory Forensics

A discipline studying past structure and behavior in acquired computer memory.

We Have A Problem

- ⦿ Proliferation of computer architectures, operating systems, and tools
- ⦿ Different memory analysis narratives
- ⦿ Need to measure analysis quality

Solution

- ⦿ Empirical patterns
- ⦿ A pattern language
- ⦿ Pattern orientation

Forensic Pattern

A common recurrent identifiable set of indicators (signs) together with a set of recommendations to apply in a specific context.

Memory Forensics revised

A discipline studying past structure and behavior of software in acquired memory using pattern-oriented analysis methodology.

Software Forensics

Software execution artefacts

Memory forensics

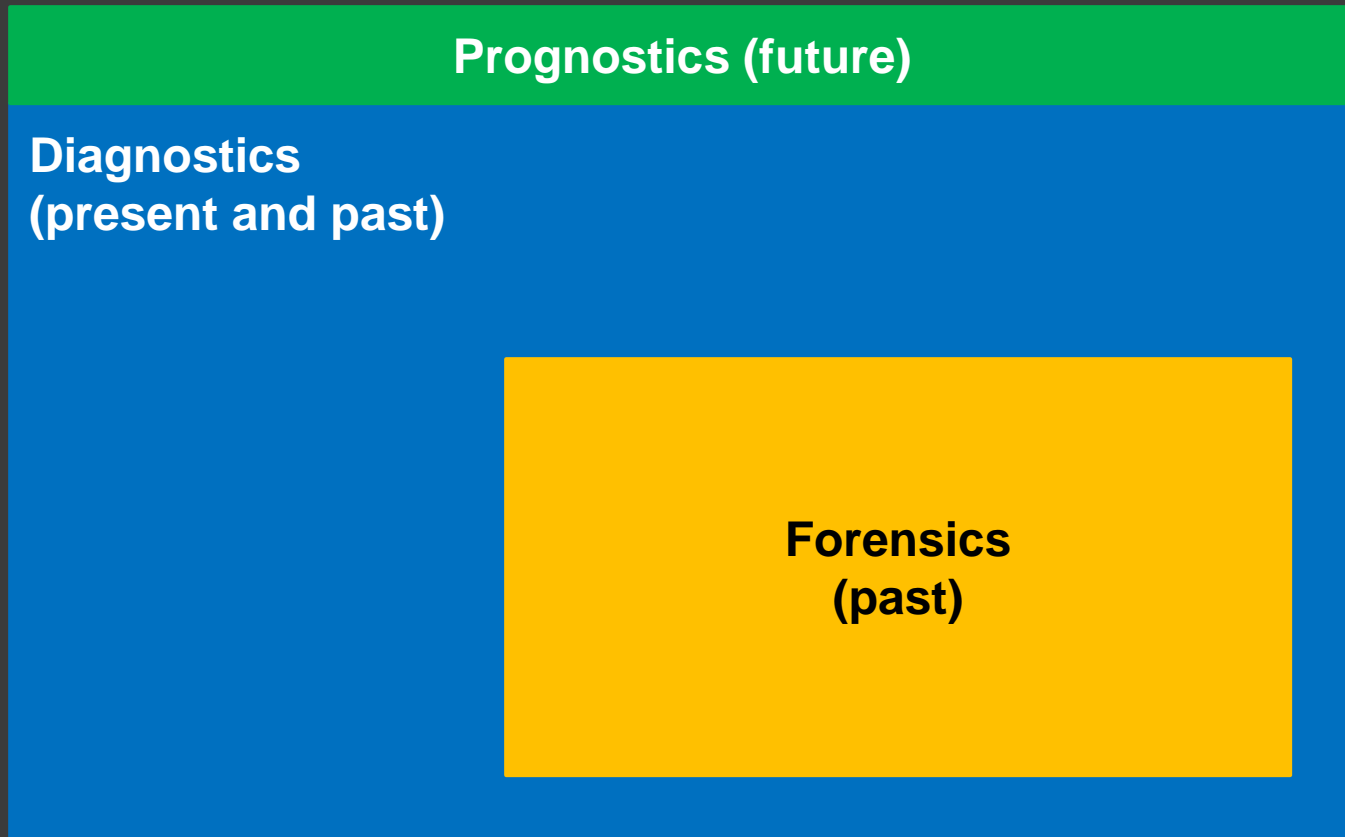
Software Forensics

A discipline studying past structure and behavior of software in execution artifacts using systemic and pattern-oriented analysis methodologies.

Structure and Behavior

- ◎ Memory snapshots (dumps)
- ◎ Traces and logs
- ◎ Source code
- ◎ Digital data (media)

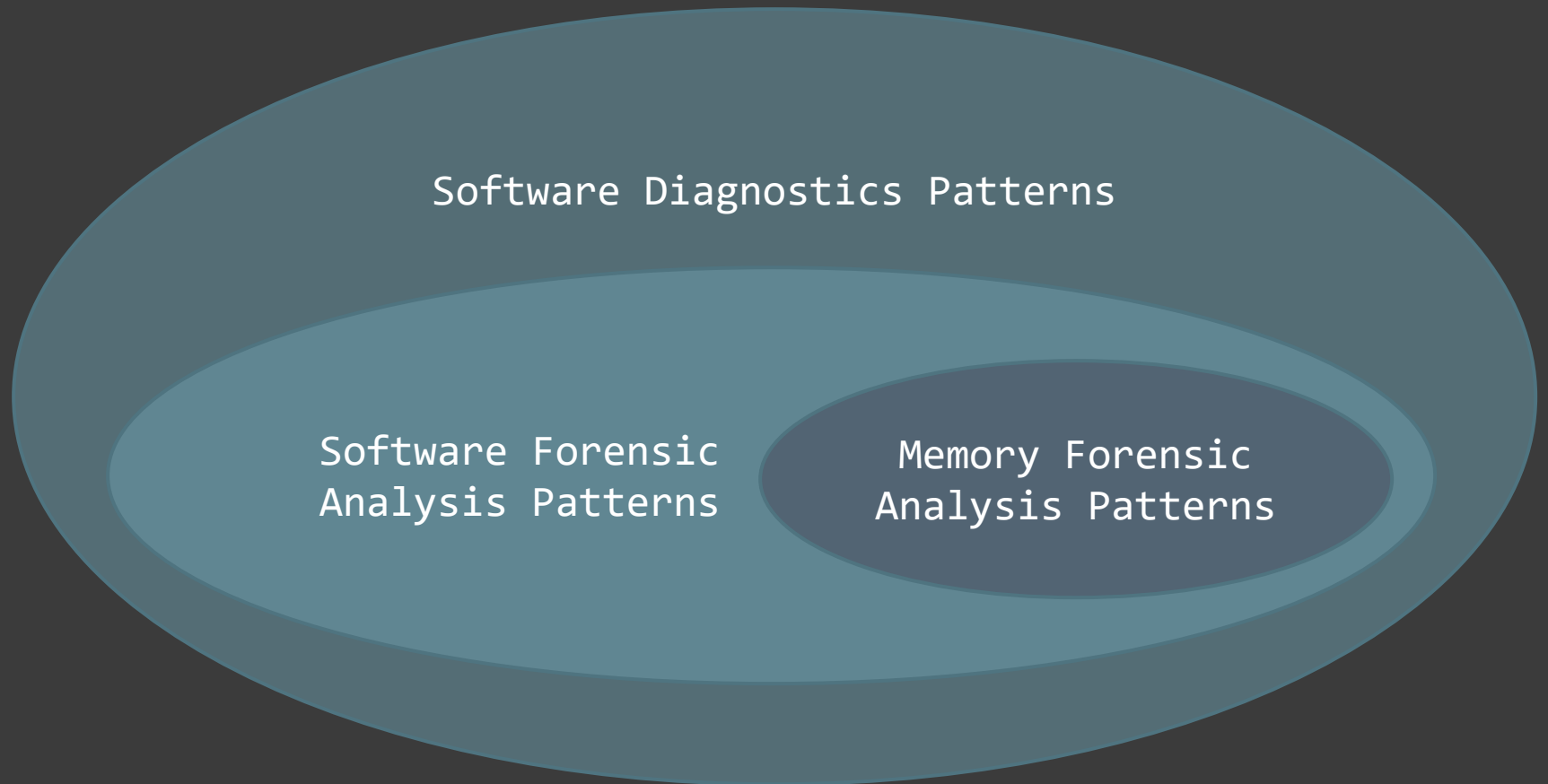
Diagnostics and Forensics



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.

Forensic Analysis Patterns



A Pattern Language

- The same detection and analysis language for different computer architectures, operating systems, and tools
- The same memory analysis narratives
- Measured analysis quality
- Predicting unknown

Pattern Orientation

1. Pattern-driven

- Finding patterns in memory
- Using checklists and pattern catalogs

2. Pattern-based

- Pattern catalogue evolution
- Catalog packaging and delivery

Main Pattern Catalogues

Memory Acquisition Patterns

Disassembly, Deconstruction, Reversing Patterns

Memory Analysis Patterns

...
Wait Chain
Execution Residue
Spiking Thread
Local Buffer Overflow
Shared Buffer Overwrite
Dynamic Memory
 Corruption
...

Malware Analysis Patterns

...
Raw Pointer
String Hint
Out-of-Module Pointer
Hooksware
Hidden Process
Deviant Module
Namespace
...

Structural Memory Patterns

...
Memory Region
Region Boundary
Anchor Region
Linked List
Value References
Regular Data
String Value
Small Value
Data Structure
...

Analysis Pattern Classification

...

Dynamic Memory Corruption Patterns

Stack Overflow Patterns

Stack Trace Patterns

Symbol Patterns

Exception Patterns

Meta-Memory Dump Patterns

Module Patterns

Optimization Patterns

Thread Patterns

Process Patterns

...

Structural Memory Patterns

<https://www.patterndiagnostics.com/Training/Structural-Memory-Patterns.pdf>

Memory Acquisition Patterns

<https://www.dumpanalysis.org/memory-acquisition-patterns>

<https://www.patterndiagnostics.com/Training/Memory-Acquisition-Patterns.pdf>

Structural space patterns

...

Process Memory Dump

Kernel memory Dump

Physical Memory Dump

Fiber Bundle Dump

...

Acquisition strategy patterns

...

External Dump

Self Dump

Conditional Dump

Dump Sequence

...

ADDR Patterns

<https://www.dumpanalysis.org/addr-patterns>

...

Potential Functionality

Function Skeleton

Function Call

Call Path

Local Variable

Static Variable

Pointer Dereference

Function Prologue

Function Epilogue

Variable Initialization

Memory Copy

Call Prologue

Call Parameter

Call Epilogue

Call Result

Control Path

Function Parameter

Structure Field

Last Call

...

Analysis Pattern Implementation

- By OS vendor (Windows, Mac OS X, Linux, ...)
- By tool (WinDbg, Volatility, IDA, GDB, LLDB, ...)
- By CPU architecture (x86, x64, ARM, ...)
- By digital media (memory, volume, file, blob, ...)

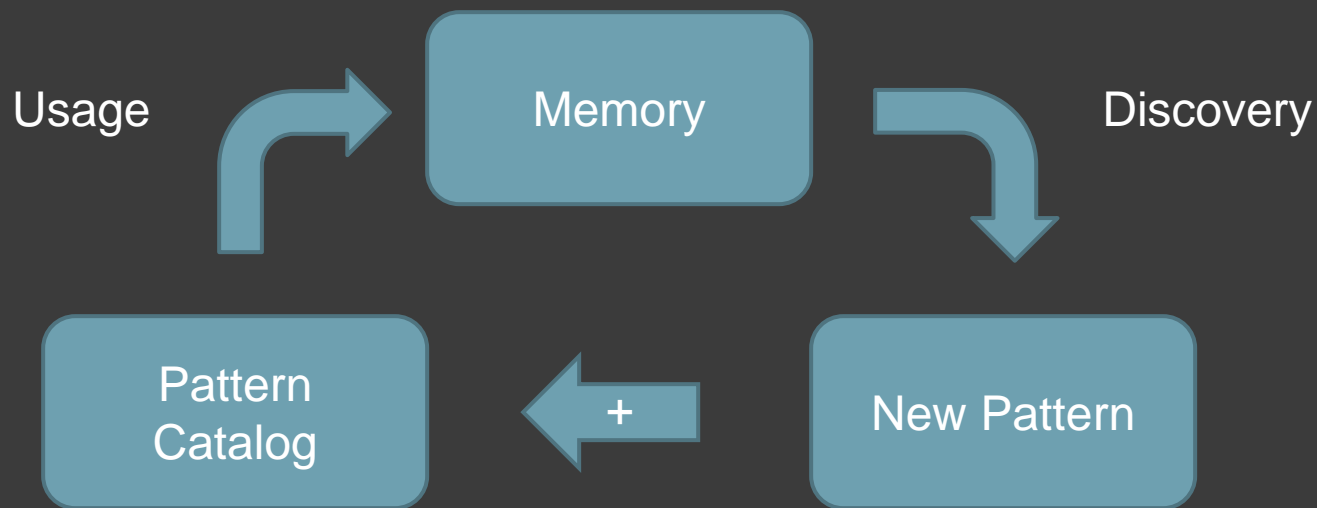
Pattern-Driven Analysis



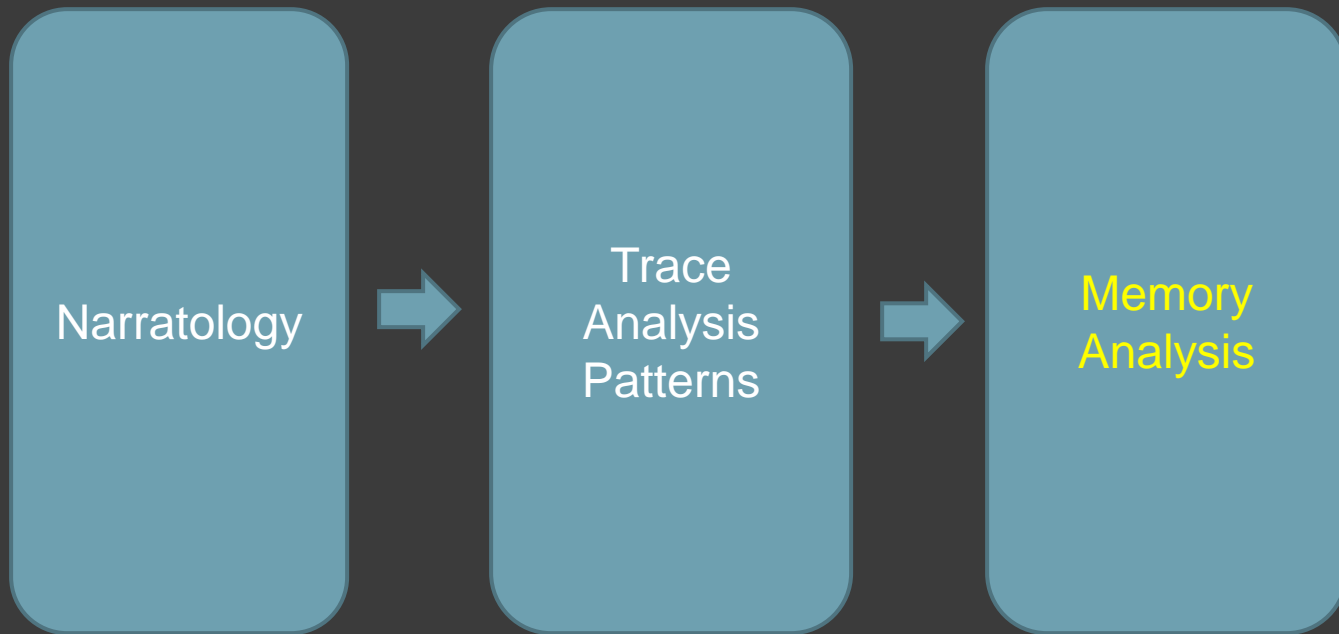
- ✓ Pattern
- Pattern
- Pattern
- ✓ Pattern
- ✓ Pattern

1. Tool-specific checklist: <https://www.dumpanalysis.org/windows-memory-analysis-checklist>
2. Pattern catalogue checklists: <https://dumpanalysis.org/>

Pattern-Based Analysis



Systems Approach



Native Memory Forensics

Using native OS debuggers such as **WinDbg** from Debugging Tools for Windows or GDB (Linux) or LLDB (Mac OS X).

Practical Examples

WinDbg session...

Analysis Patterns for Example A

- ⦿ Tampered Dump
- ⦿ Exception Stack Trace
- ⦿ Stored Exception
- ⦿ Lateral Damage
- ⦿ Execution Residue (Unmanaged Space, User)
- ⦿ Hidden Exception (User Space)
- ⦿ NULL Pointer (Data)

Analysis Patterns for Example B

- ⦿ Dynamic Memory Corruption (Process Heap)
- ⦿ Stack Trace Collection (Unmanaged Space)
- ⦿ RIP Stack Trace
- ⦿ Hooksware
- ⦿ Patched Code
- ⦿ Hidden Module
- ⦿ Deviant Module
- ⦿ String Hint
- ⦿ Fake Module
- ⦿ No Component Symbols
- ⦿ Namespace

Example C

Analysis pattern correspondence

- ① Process Dump
- ① Physical (Complete) Dump
- ① Kernel Dump

Further Reading (Patterns)

- ① The Timeless Way of Building (by Christopher Alexander)
- ① A Pattern Language: Towns, Buildings, Construction (by Christopher Alexander, et al.)
- ① Pattern Theory: Introduction and Perspectives on the Tracks of Christopher Alexander (by Helmut Leitner)

Further Reading (MDA)

- ◎ [Cloud Memory Dump Analysis](#)
- ◎ [Fundamentals of Physical Memory Analysis](#)
- ◎ [Victimware](#)
- ◎ [Pattern-Oriented Software Forensics](#)
- ◎ [Debugging TV](#)

Further Reading (SD)

- ◎ [Software Diagnostics Institute](#)
- ◎ [Pattern-Driven Software Diagnostics](#)
- ◎ [Systemic Software Diagnostics](#)
- ◎ [Pattern-Based Software Diagnostics](#)
- ◎ [Philosophy of Software Diagnostics](#)

Historical Reference

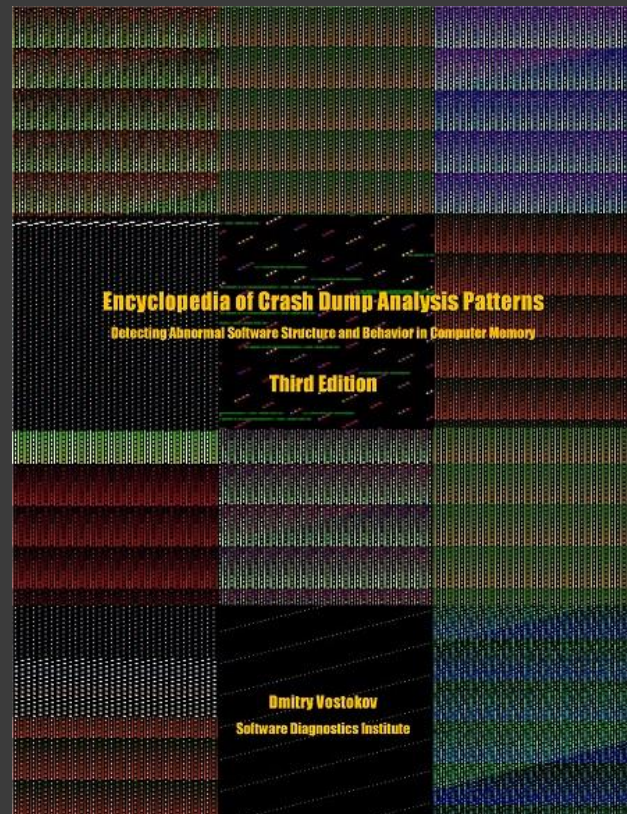
[Memory Dump Analysis Anthology \(Diagnomicon\)](#): 14 volumes



Volume 15 is planned for 2022/2023

Alphabetical Reference

[Encyclopedia of Crash Dump Analysis Patterns: Detecting Abnormal Software Structure and Behavior in Computer Memory, Third Edition](#)

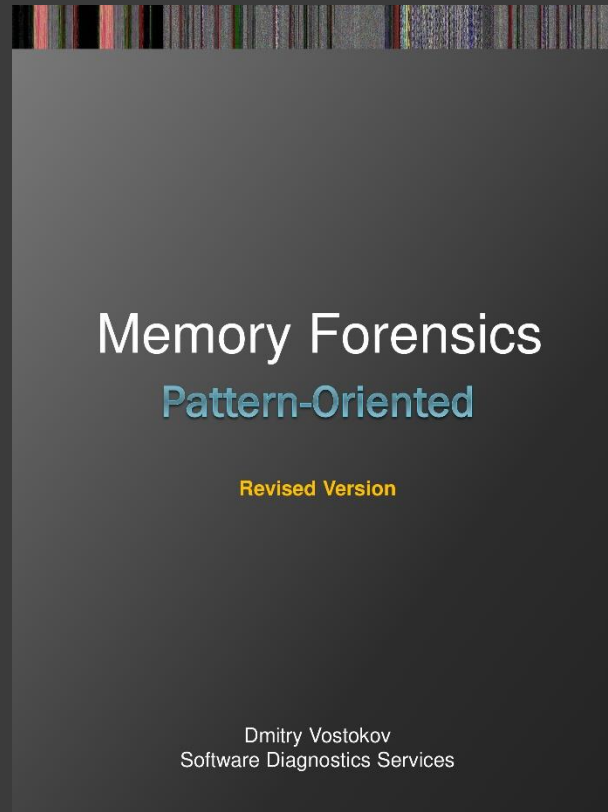


Referenced Training Courses

- [Accelerated Disassembly, Reconstruction and Reversing](#)
- [Accelerated Windows Malware Analysis with Memory Dumps](#)
- [Advanced Windows Memory Dump Analysis with Data Structures](#)

Transcript

Pattern-Oriented Memory Forensics: A Pattern Language Approach, Revised Edition
(ISBN-13: 978-1912636761)



Q&A

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

Thank you for attendance!