Software Forensics

Pattern-Oriented

Version 1.0

Dmitry Vostokov
Software Diagnostics Services

Prerequisites

- Interest in computer forensics
- Experience in computer diagnostics

Why?

- A common computer forensics language
- Computer forensics as computer diagnostics

Forensics

> A discipline studying past structure and behavior

Computer Forensics

A discipline studying past structure and behavior of computers

Computers

- Hardware forensics
- Software forensics

Software Forensics preliminary

> A discipline studying past structure and behavior of software

Structure and Behavior

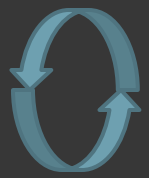
- Memory snapshots (dumps)
- Traces and logs
- Source code
- Digital data (media)

Software Diagnostics

A discipline studying abnormal software structure and behavior in software execution artifacts (such as memory dumps, software and network traces and logs) using pattern-driven, systemic and pattern-based analysis methodologies.

What is abnormal?

Normal



Abnormal

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

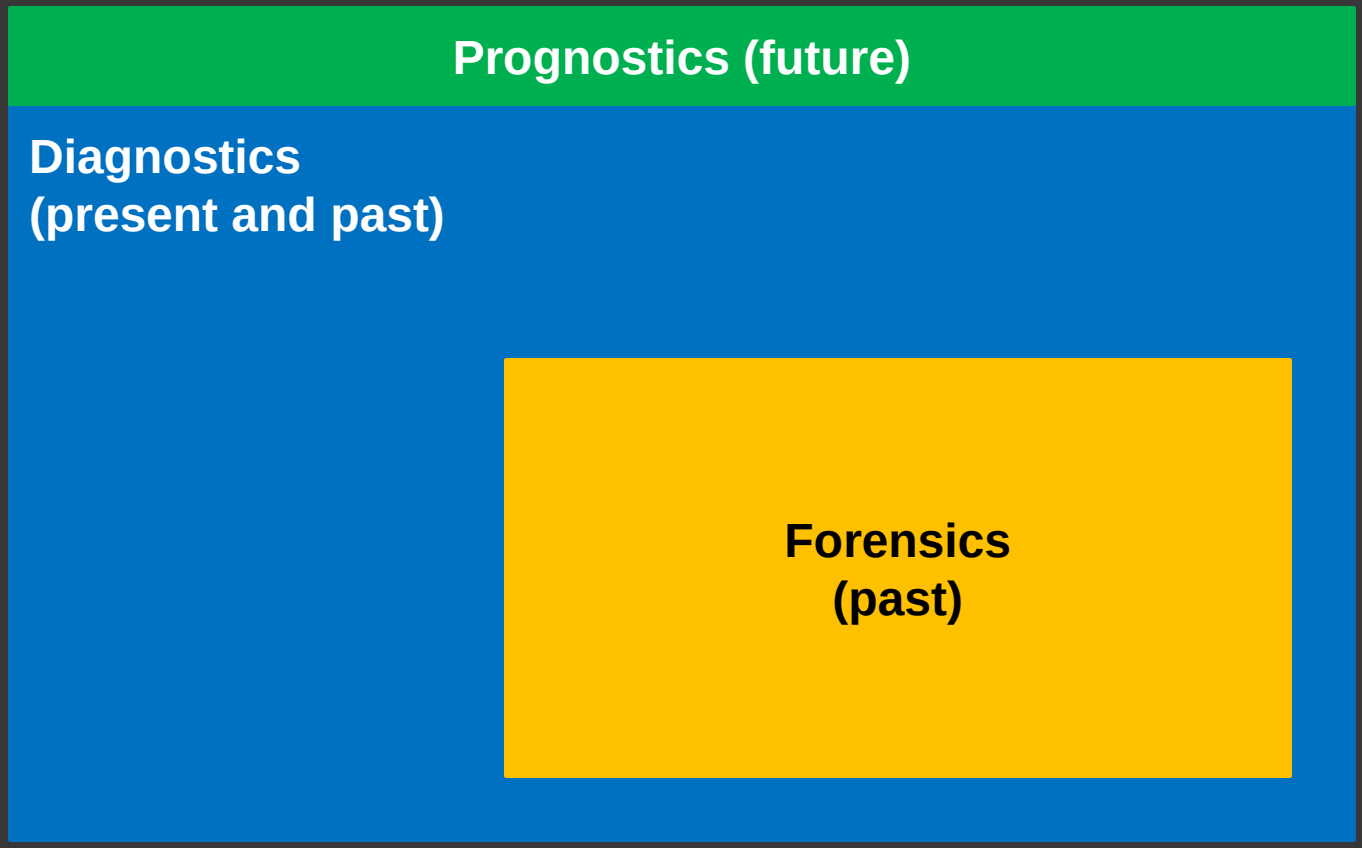
Forensic Pattern

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

Software Forensics

> A discipline studying past structure and behavior of software in execution artifacts using pattern-driven, systemic and pattern-based analysis methodologies.

Diagnostics and Forensics



Software Diagnostics revised

> 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.

Pattern Orientation

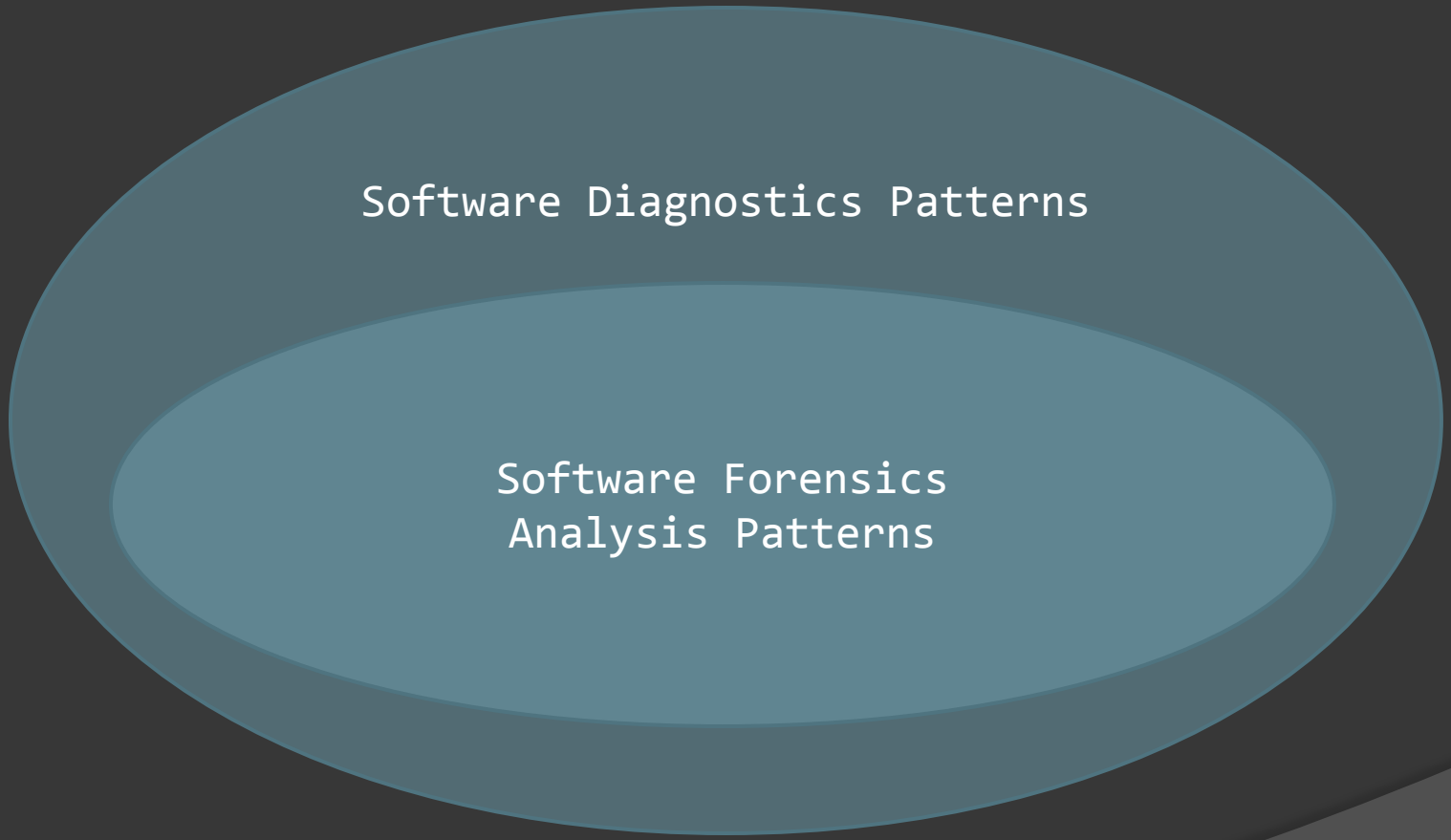
Pattern-driven

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

Pattern-based

- Pattern catalogue evolution
- Catalog packaging and delivery

Forensic Analysis Patterns



Catalog Classification

- By abstraction

Meta-patterns

- By artifact type

Software Log Memory Dump Network Trace
Source Code Data / Media

- By intention

Malware / Victimware

Catalog Partition

- By execution mode and space
- By elementary diagnostics patterns

Crash Hang Spike Leak

- By structure and behaviour

Structural memory patterns Software trace classification

- By objects

Thread Process Module

Pattern Implementation

- By OS vendor

Windows Mac OS X Linux

- By product lines
- By CPU architecture
- By digital media

Artefact Forensics

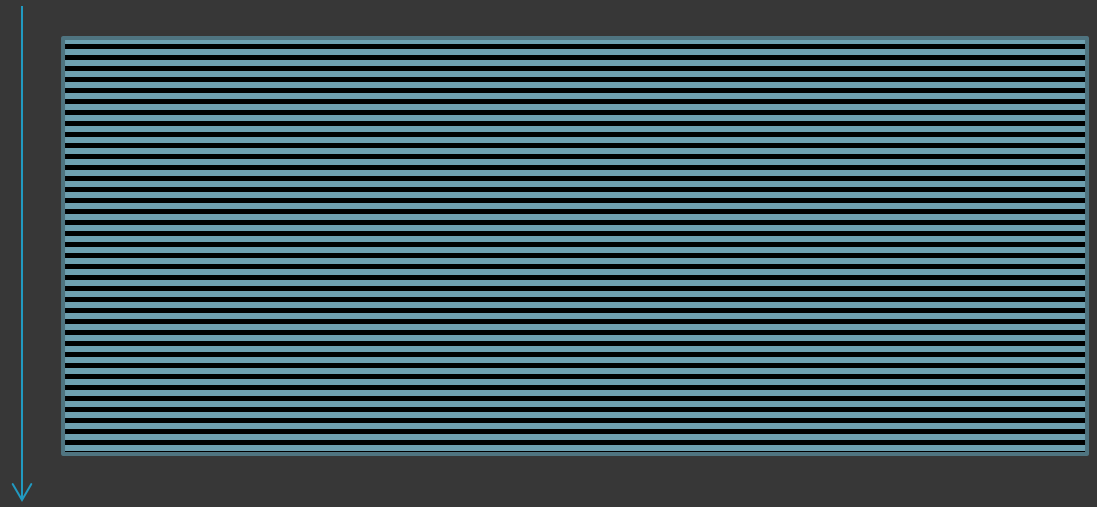
- Memory forensics
- Trace and log forensics

Software Narrative

> A temporal sequence of events related to software execution.

Software Trace

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



Generalized Narrative

> A sequence of memories related to software execution.

Hardware Narrative

> A temporal sequence of hardware signals.

Narratology of Things

A sequence of memories and events in Internet of Things (IoT)

Software NT for Forensics of Things

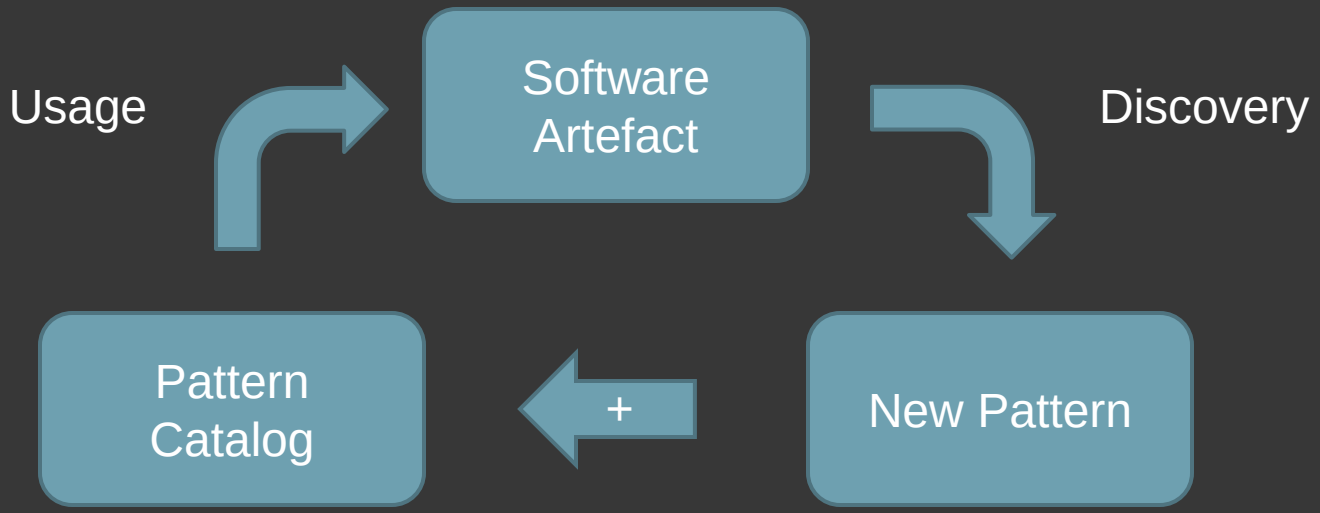
Robotic Narratology

A sequence of memories and events from robots

Robotic Forensics

Pattern-Driven Analysis

Pattern-Based Analysis



Further Reading (SD)

- Software Diagnostics Institute
- Memory Dump Analysis Anthology: Volumes 1 - 6

  Volume 7 is in preparation (January, 2014)
- Software Trace and Memory Dump Analysis
- Pattern-Driven Software Diagnostics
- Systemic Software Diagnostics
- Pattern-Based Software Diagnostics
- Philosophy of Software Diagnostics
- Mobile Software Diagnostics

Further Reading (MDA)

- Cloud Memory Dump Analysis
- Complete Crash and Hang Memory Dump Analysis

  Will be updated on 30th of December, 2013
- Victimware
- Debugging TV

PS. Applicable to memory forensics

Further Reading (STA)

- Software Narratology
- Malware Narratives
- Pattern-Oriented Network Trace Analysis
- Accelerated-Windows-Software-Trace-Analysis-Public.pdf

PS. Applicable to trace and log forensics

Reference and Courses

[Windows Memory Forensics Training Pack]

What's Next for 2013?

Fundamentals of Physical Memory Analysis

Will also be published as a book in earlier 2014

What's Next for 2014?

- Semiotics of Debugging
- Generative Software Narratology
- Pattern-Oriented Hardware Signal Analysis
- Pattern-Oriented Software Prognostics

Q&A

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

Thank you for attendance!

Facebook LinkedIn Twitter