Dmitry Vostokov

Software Diagnostics Engineering and Diagnostics-Driven Development.

dmitry.vostokov@gmail.com

Summary

I founded the pattern-oriented software diagnostics discipline and Software Diagnostics Institute (DA +TA: DumpAnalysis.org + TraceAnalysis.org), authored more than 30 books on software diagnostics, forensics, root cause analysis and problem solving, memory dump analysis, debugging, software trace and log analysis, reverse engineering and malware analysis. I have more than 20 years of experience in software architecture, design, development, and maintenance in a variety of industries including leadership, technical and people management roles. In my spare time, I explore the mathematical and computer science foundations of Theoretical Software Diagnostics, Software Narratology, an applied science of software stories, and its further development as Narratology of Things and Diagnostics of Things (DoT). My practical focus is on software diagnostics engineering and diagnostics-driven development.

Summary of recent technical experience:

x86/x64/ARM assembly, C, C11, C++, C++17, STL, Boost, Python, C#, Java, JavaScript, JSON, jQuery Mobile, Node.js, REST, MongoDB, PowerShell, SQL, NoSQL, disassembling, reversing, malware analysis; debugging (WinDbg, GDB, LLDB); IDA Pro; Win32/Win64 API, MFC, COM, Windows internals, services and device drivers, process, kernel, and physical memory analysis; crash and hang memory dump analysis; Linux and Mac OS X core dump analysis; .NET postmortem debugging, iOS and Android log diagnostics; Raspberry Pi 3; network trace analysis, Wireshark; large-scale multithreaded and distributed systems; software fault modelling; Visual Studio, Xcode, Eclipse; code reviews, refactoring; architecture, design and implementation patterns including cloud architecture, UML; software diagnostics and root cause analysis; JIRA; iterative, incremental, and Agile processes; Git, Bitbucket, Subversion. All aspects of life cycle including security, testing, technical support, training, and writing technical documentation. Mathematica.

Timestamp: 13 May 2018

Experience

Software Engineer C++ at ThinScale Technology Ltd.
November 2017 - Present

ThinScale Technology creates solution driven lightweight and scalable products that meet the challenges in the Windows based Thin Client Software, Desktop Virtualization, VDI & Server Based Computing space.

Founder at Software Diagnostics Institute
March 2006 - Present

Owned a blog and public forum about crash dump and log analysis with millions of page views, a research portal and software diagnostics library of more than 500 analysis patterns.

Developed innovative analysis pattern methodology and pattern languages for software diagnostics, forensics, prognostics, root cause analysis, debugging, and software data analysis; patterns of software diagnostics architecture and software design patterns for diagnostic tools; software narratology, narratology of things, and theoretical software diagnostics. Major publication Memory Dump Analysis Anthology had 10 volumes and more than 4,000 pages.

Founder at Software Diagnostics Technology and Services
July 2010 - Present

Promoted pattern-oriented diagnostic analysis methodology from Software Diagnostics Institute and trained customers worldwide. Bought over 2,000 books for research purposes, all necessary hardware and software.

Developed and delivered seminars and training courses in software diagnostics and debugging, malware analysis, memory dump analysis, software and memory forensics, reversing, software trace and log analysis. Customers included operating system vendors, major antivirus, IT management, and virtualization companies. Provided abnormal software behavior analysis audit of Windows environments. Additional development projects included: Logtellect, DiaThings (IoT diagnostics), DoT (Diagnostics of Things), ArtDbg (Artificial Debugger), EasyDbg (GUI for debuggers), Dia|gram (a graphical language for diagnostics), ToolObjects, SupportSim (technical support activities simulation), Narrascope (a narrative debugger), Narrachain (an application of blockchain technology), Projective Debugger, Software Diagnostics Workbench, LogOS – Log OS – LoggingOS, PatternSight Training Platform, WinDbg debugger extensions, Android Java apps, Anolog.io (anomaly detection in logs, AI, ML), BriteTrace, WinNarrative.

Founder and Editor-in-Chief at OpenTask Publishing
February 2008 - Present

Iterative and Incremental Publishing. Technical book design and production. Managed a niche publisher with 85 titles in print, with content available on O'Reilly Safari Books Online and SkillSoft Books24x7. Owned book marketing, design, editing, and production, content conversion to Kindle and EPUB formats.

Senior Software Engineer II / Principal Dev Analysis Engineer at Citrix

October 2003 - October 2017 (14 years 1 month)

As an individual contributor performed diagnostics and root cause analysis of software execution artifacts from Fortune 100 and Fortune Global 500 customers. Interviewed and coached new hires. Provided training to global technical support and engineering teams on diagnostic tools and software internals, on improving data analysis quality. Presented various diagnostic methodologies and case studies using WinDbg at Citrix DevCon (2015). Generated ideas behind many company projects.

Technical Manager Dev Analysis EMEA / EMEA Development Analysis Team Manager

Managed diagnostic tool projects and project lines by prioritizing their features based on use cases and customer feedback. Developed roadmaps, evangelized the enhancements, and articulated vision of future unified tool frameworks to global teams. Exercised leadership in industry-wide product certification efforts in cooperation with a major operating systems vendor. Managed and coached the team of software engineers in a technical support environment, tracked their performance, oversaw promotions and salary increases based on merit. Wrote process guide for new technical support hires. Proposed and implemented various process improvements to increase internal and external customer satisfaction.

Escalation Dev Analysis Engineer / EMEA Dev Analysis Team Lead

Performed diagnostics and root cause analysis of memory dumps and software logs from Windows environments. Autonomously designed, implemented, and maintained software diagnostic tools. Proposed and implemented automated builds. Performed source code analysis of very large codebases. Used UML to communicate architectures and device driver internals. Wrote and reviewed knowledge base articles. Performed security reviews of diagnostic tools written by global support team members. Mentored EMEA and US team members. Provided code reading training to technical support and escalation engineers. Worked on critical situation cases. Developed and provided code fixes.

Founder at Debugging.TV

October 2011 - December 2013 (2 years 3 months)

Designed and presented more than 40 episodes featuring various facets of debugging, memory dump and software trace analysis on Windows, Mac OS X, and Android platforms including live WinDbg and GDB demonstrations.

Software Development Consultant at Guardeonic Solutions (Infineon)

April 2003 - September 2003 (6 months)

Designed and implemented a software prototype for a security product. Used: Windows NT/2000/XP/2003, WinDbg, C, C++, SQL, UML, XML, XSD, Visio, Poseidon, CVS, Visual C++, MFC, COM/

DCOM, STL, PKI, ASN.1, Cryptography (DES), Win32 API, Platform SDK, Windows NT/2000/XP DDK, GINA, Certificates, smartcard and fingerprint technology.

Senior Software Engineer at Programming Research
September 2001 - March 2003 (1 year 7 months)

- Owned feasibility studies, requirements analysis, architecture, design and implementation of several subsystems of deep flow static analysis tools for C and C++.
- Technology evaluation and research (semantics of .NET languages, C++, templates and STL).

OS Platforms: Windows 2000, Unix (Linux)
Languages: C, C99, C++, Embedded C++, UML, OCL, XML
Tools : Microsoft Visual Modeler, CVS, Wiki, VMware, GNU C++, Comeau C++, Intel C++, Visual C++, Visual C++.NET, QAC, QAC++, STL, Boost, eXtreme Programming
Technologies: Compiler front ends, scanners, parsers, data flow analysis, metrics, garbage collection, virtual machines, CLR, .NET

- Designed and implemented a high-performance multiplatform object-relational database for a compiler front end. Owned feasibility studies, requirements, architecture and design documentation.

OS Platforms: Windows 2000, Unix (Linux)
Languages: C++, UML, OCL, XML, SQL
Tools: Microsoft Visual Modeler, CVS, Wiki, VMware, GNU C++, Visual C++, QAC++, STL, eXtreme Programming
Technologies: Client-server, ORDBMS

- Designed and implemented Adobe Acrobat plug-in for ISO C++ Standard documentation.

OS Platforms: Windows 2000, Unix (Linux)
Languages: C
Tools: CVS, VMware, GNU C++, Visual C++, Adobe Acrobat SDK, eXtreme Programming

Senior Software Designer at Ericsson
January 2001 - August 2001 (8 months)

Owned analysis, design and implementation of core operation and maintenance interfaces for WCDMA/UMTS Media Gateway Cello platform, use case design realization and implementation in C++, portability across different platforms and languages. Created about 100 sequence and statechart UML diagrams. Debugged Rational Rose RealTime implementation models. Extended subsystems to support distributed clusters. Coached software engineers.

OS Platforms: Windows NT, Unix (Solaris), OSE Delta
Languages: C, C++, Java, SQL, UML, ROOM, SDL
Tools: Rational Rose RealTime, Rational Unified Process, ClearCase, Visual C++, ObjecTime, Microsoft Project
Technologies: Multi-tier, real time distributed systems, clusters, transactions, in-memory RDBMS, CORBA

Senior Software Engineer at Luxoft
July 2000 - January 2001 (7 months)

ISO 9001 and CMM Level 4 Certified Company.

- Project lead and architect of a multiplatform enterprise PDF manipulation, linearization and rasterization system for Boeing Commercial Airplanes Group. Designed and implemented its architectural prototype in C++. Owned feasibility, requirements and design documentation, system integration and deployment. Mentored a small team of software engineers.

OS Platforms: Windows NT, Unix (Linux, Solaris)
Languages: C, C++, XML, DTD, PDF, UML, OCL
Tools: Visio, Rational Rose, Rational SoDA, Rational Unified Process, VSS, VMware, Visual C++, STL, GNU C++, Microsoft Project
Technologies: SAX XML parsers, regular expression parsers, CORBA (ACE/TAO)

- Member of a team responsible for a web portal design and implementation for a large telecommunication company. Designed several subsystems. Owned design documentation.

Languages: Java 2 Enterprise Edition, UML, XML, XSL, HTML, WML
Tools: Rational Rose, Rational Unified Process, VSS, BEA Weblogic Application server
Technologies: Multi-tier, Servlets, WAP, DOM XML parsers, XSLT

Application Development Consultant at Accusoft Pegasus
April 1998 - December 2000 (2 years 9 months)

Remote work for a USA company located in Boston. Designed, implemented, and maintained the following projects:

- A wrapper to Scansoft TextBridge OCR API and ActiveX control. Wrote about 5,000 lines in C, 4,000 lines in C++ and 2,000 lines in Visual Basic.
- A Wireless BMP image converter to and from an internal image representation of a document imaging toolkit. Wrote about 1,000 lines in C.
- An ATL component for Image Annotation Toolkit. Wrote about 8,000 lines in C++.

- An image manipulation GUI library. Designed and implemented an ATL component. Designed and coded about 40 dialogs, wrote about 10,000 lines in C, 3,000 lines in C++ and 1,000 lines in Visual Basic.
- A JavaBean for Java Document Imaging Toolkit. Wrote about 13,000 lines in Java 1.1.
- Java Image Annotation classes. Wrote about 2,500 lines in Java 1.1.
- A multithreaded PDF rasterization extension for Document Imaging Toolkit.
- Member of an engineering team responsible for design and development of Java Document Imaging Toolkit (about 60,000 lines in Java). Implemented Java classes for image I/O via TCP/IP sockets. Wrote and tested about 3,000 lines in Java 1.1.
- Maintained and extended Win32 DLL and ActiveX MFC components for Image Annotation Toolkit as a part of Document Imaging Toolkit (more than 1,000,000 lines in C and C++). Owned API documentation, refactoring, extending functionality, testing and communication with technical support. Refactored about 50,000 lines in C and 20,000 lines in C++.
- Maintained Bar code recognition component.

Languages: C, C++, Visual Basic, VBScript, PDF, Java
Tools: VSS, Visual C++, Visual Basic, MFC, ATL, Win32 SDK, Borland JBuilder, Visual J++, Symantec Visual Cafe, Ghostscript, Delphi, MS Access, Microsoft Project
Technologies: COM, ActiveX, Client-server, TCP/IP, sockets, JavaBeans

Senior Software Engineer at IBS Group
October 1999 - June 2000 (9 months)

- Member of a team responsible for a web portal design and implementation for a large web hosting company. Owned technology evaluation, feasibility, requirements and vision documentation.

OS Platforms: Windows NT, Unix (Solaris)
Languages: Java 2 Enterprise Edition, UML, HTML, XML, XSLT
Tools: Rational Rose, Rational Unified Process, VSS, Sybase PowerDesigner/DataArchitect, BEA Weblogic Application and Personalization servers, Oracle 8.x
Technologies: Multi-tier, EJB, Servlets, JSP, DOM XML parsers

- Project lead and architect of Windows SGML Table validation and editing system for Boeing Commercial Airplanes Group. Designed and implemented GUI and system-level subsystems. Owned feasibility, requirements and design documentation. Wrote about 10,000 lines in Visual Basic and 1,000 lines in C. Maintained SGML to RTF and RTF to SGML converters written in C++. Owned system integration and deployment.

Languages: C, C++, Visual Basic, SGML, RTF, UML

Tools: Rational Rose, Rational Unified Process, VSS, Visio, Visual C++, STL, Visual Basic, Win32 SDK, Microsoft Project
Technologies: COM, OLE Automation

- Member of an engineering team responsible for C++ corporate software coding standard. Owned Visual Basic corporate software coding standard.

Senior System Software Engineer at Interactive Products
March 1994 - August 1999 (5 years 6 months)

Remote work for a USA company Interactive Products, Inc. founded by former Covox employees and located in Oregon. Designed and implemented the following projects:

- A secure wrapper for Windows screen savers and a secure electronic communication system for Windows NT and 9x that used instant verbal confirmation of a person's identity. Wrote about 15,000 lines in C++ and 1,000 lines in x86 assembler.
- Personal notebooks for Windows with ability to store compressed speech. Wrote about 6,000 lines in C++.
- A word processor DLL with word-wrapped pictures, object embedding and events. Wrote about 20,000 lines in C++.
- OpenTask - a visual prototyping system for Windows designed to carry out any task and visually create prototypes, interactive presentations, tutorials, instructions and educational programs using build-in compiler. Wrote about 10,000 lines in C++.
- A system for handicapped people which controls mouse by voice. Wrote about 1,000 lines in C.
- A speech recognition system which enabled voice control of any software application on Windows 95/NT. Designed and implemented a special version which enabled voice control of CAD/CAM systems. Localized the products for Spanish language. Designed and implemented a speech recognition server for Windows which facilitated client applications to use voice recognition. Wrote about 45,000 lines in C++ and 1,500 lines in x86 assembler.
- A speech recognition system which enabled voice control of any software application on Windows 3.x. Localized the product for Japanese language (NEC 9800 platform). Wrote about 20,000 lines in C++ and 1,000 lines in x86 assembler.
- Win16 API emulation library for text-based MS-DOS applications. Wrote about 8,000 lines in C and 3,000 lines in x86 assembler.

Languages: C, C++, x86 assembly language
Tools: Borland C++, TASM, Visual C++, Windows DDK and SDK, MASM, VSS, STL, MFC
Technologies: COM, Win32 CryptoAPI, OLE Automation, Client-server, DDE, CORBA

Application Development Consultant at PC Voice Club
June 1994 - December 1998 (4 years 7 months)

Designed and implemented the following projects:

- An image viewer application. Wrote about 2,000 lines in Visual Basic.
- A simple relational database and an applet for browsing that database. Wrote about 2,500 lines in Java 1.1 and 500 lines in Perl.
- A bilingual (Russian/English) text-to-speech system with embedded multimedia and presentation capabilities. Implemented GUI, presentation end editing components. Wrote about 14,000 lines in C++.
- A script language editor with syntax highlighting and word-processing capabilities. Wrote about 10,000 lines in Java 1.0.
- Several games in Java (client and server parts). Wrote about 8,000 lines in Java 1.0. Designed a protocol for communication between server and multiple clients.
- An application, which changes colour, shape or picture of caret according the current locale and language. Wrote about 1,000 lines in C.
- A system-level Windows DLL for synchronizing screen menu, windows and messages with synthesized speech. Wrote about 1,000 lines in C.

Languages: C, C++, Visual Basic, Java, Perl, JavaScript
Tools: Visual C++, Visual Basic, Visual J++, Visual InterDev, MFC, Win32 SDK, Borland C++
Technologies: Imaging for Windows, COM, OLE, Automation, ActiveX, CGI, RDBMS, Client-server, sockets

Independent Contractor (Software Engineer) at Agama
October 1994 - October 1995 (1 year 1 month)

Designed and implemented a word processor for Windows 3.x (as a part of a spelling and grammar correction system) and a DLL for spelling in every Windows application. Wrote about 18,000 lines in C.

Languages: C
Tools: Borland C++, Windows SDK

Software Engineer at Covox
February 1992 - March 1994 (2 years 2 months)

Remote work for a USA company Covox, Inc. located in Eugene, Oregon.

- Implemented a vocabulary editing and training DLL as a part of a speech recognition system for Windows 3.x. Wrote about 5,000 lines in C++.
- Designed and implemented an advanced macro recorder/playback program for Windows 3.x with C-style macro language.

Languages: C, C++
Tools: Borland C++, Windows SDK

Independent Contractor (Software Engineer) at Moscow State University
1987 - 1992 (6 years)

Paid work during my Chemistry studies. Includes contracts with Applied Mathematics and Chemistry Laboratory, Inorganic Chemistry Department, and Small Business Centre. Designed and implemented the following projects:

- An equation solving system with interpreter for Windows 3.x. Wrote about 4,000 lines in C++.
- A thin layers diffusion analysis system for MS DOS. Wrote about 3,000 lines in C++.
- An HPGL MS DOS emulator for IBM PagePrinter. Wrote about 1,000 lines in C.
- A cluster search and analysis system for a mass spectrometer. Wrote about 5,000 lines in C for MS DOS.
- Ported a program (800 Fortran lines) to an assembler equivalent as a part of a system that calculated properties of cosmos fuel for Russian Space Agency. Wrote about 2,500 PDP-11 assembler lines for RSX-11M.

Languages: C, C++, Fortran, x86 assembly language, PDP-11 assembler
Tools: Borland C++, third-party GUI C++ libraries, Microsoft FORTRAN, TASM, Turbo C

Education

Lomonosov Moscow State University (MSU)
Chemistry, 1987 - 1992
Izhevsk State Technical University (ISTU)
BSc/MSc, Computer Science, Software Engineering, 2003 - 2007

Dmitry Vostokov

Software Diagnostics Engineering and Diagnostics-Driven Development.

dmitry.vostokov@gmail.com

Contact Dmitry on LinkedIn

Appendix – Selected publications

- Theoretical Software Diagnostics, Second Edition (ISBN: 978-1908043900)
- Accelerated Windows Malware Analysis with Memory Dumps, Second Edition (ISBN: 978-1908043863)
- Advanced Windows Memory Dump Analysis with Data Structures, Third Edition (ISBN: 978-1908043849)
- Memory Dump Analysis Anthology, Volume 10 (ISBN: 978-1908043856)
- Encyclopedia of Crash Dump Analysis Patterns: Detecting Abnormal Software Structure and Behavior in Computer Memory, Second Edition (ISBN: 978-1908043832)
- Software Trace and Log Analysis: A Pattern Reference, Second Edition (ISBN: 978-1908043825)
- Memory Dump Analysis Anthology, Volume 9b (ISBN: 978-1908043368)
- Accelerated Windows Memory Dump Analysis, Fourth Edition (ISBN: 978-1908043467)
- Memory Dump Analysis Anthology, Volume 9a (ISBN: 978-1908043351)
- Accelerated Linux Core Dump Analysis (ISBN: 978-1908043979)
- Practical Foundations of Windows Debugging, Disassembling, Reversing (ISBN: 978-1908043948)
- Memory Dump Analysis Anthology, Volume 8b (ISBN: 978-1908043542)
- Memory Dump Analysis Anthology, Volume 8a (ISBN: 978-1908043535)
- Software Trace and Memory Dump Analysis: Patterns, Tools, Processes and Best Practices (978-1908043238)
- Pattern-Oriented Memory Forensics: A Pattern Language Approach (ISBN: 978-1908043764)
- Memory Dump Analysis Anthology, Volume 7 (ISBN: 978-1908043528)
- Accelerated Mac OS X Core Dump Analysis, Second Edition (ISBN: 978-1908043719)
- Fundamentals of Physical Memory Analysis (ISBN: 978-1906717155)
- Pattern-Oriented Software Forensics: A Foundation of Memory Forensics and Forensics of Things (ISBN: 978-1908043696)
- Accelerated Disassembly, Reconstruction and Reversing (ISBN: 978-1908043672)
- Mobile Software Diagnostics (ISBN: 978-1908043658)
- Pattern-Oriented Network Trace Analysis (ISBN: 978-1908043580)
- Malware Narratives: An Introduction (ISBN: 978-1908043481)
- Philosophy of Software Diagnostics (ISBN: 978-1908043571)
- Victimware: The Missing Part of the Equation (ISBN: 978-1908043634)
- Pattern-Based Software Diagnostics (ISBN: 978-1908043498)
- Accelerated .NET Memory Dump Analysis, Second Edition (ISBN: 978-1908043597)
- Systemic Software Diagnostics (ISBN: 978-1908043399)
- Accelerated Windows Debugging[3] (ISBN: 978-1908043566)
- Pattern-Driven Software Diagnostics (ISBN: 978-1908043382)
- Memory Dump Analysis Anthology, Volume 6 (ISBN: 978-1908043191)
- Accelerated Windows Software Trace Analysis (ISBN: 978-1908043429)
- Software Narratology: An Introduction to the Applied Science of Software Stories (ISBN: 978-1908043078)
- The Old New Crash: Cloud Memory Dump Analysis (ISBN: 978-1908043283)
- Introduction to Pattern-Driven Software Problem Solving (ISBN: 978-1908043177)
- Memory Dump Analysis Anthology, Volume 5 (ISBN: 978-1906717964)
- Memory Dump Analysis Anthology, Volume 4 (ISBN: 978-1906717865)
- Memory Dump Analysis Anthology, Volume 3 (ISBN: 978-1906717438)
- Memory Dump Analysis Anthology, Volume 2 (ISBN: 978-0955832871)
- Memory Dump Analysis Anthology, Volume 1 (ISBN: 978-0955832802)