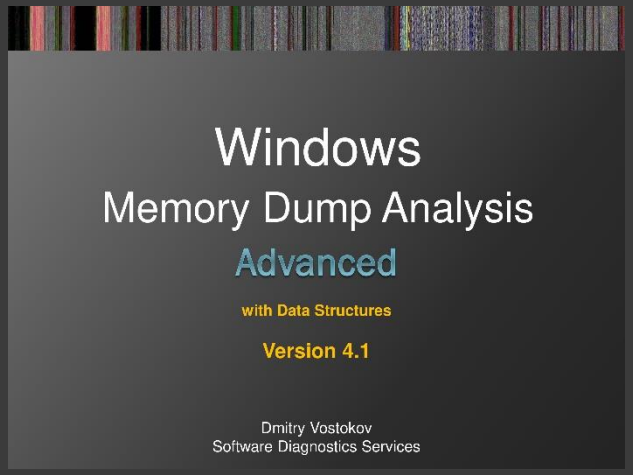
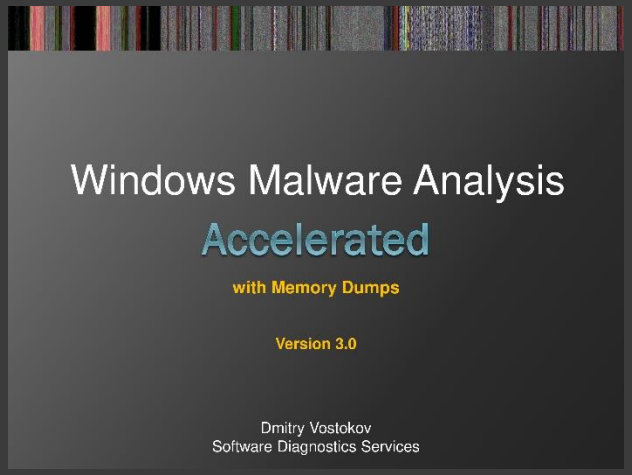
Windows Memory Forensics Malware Analysis Accelerated

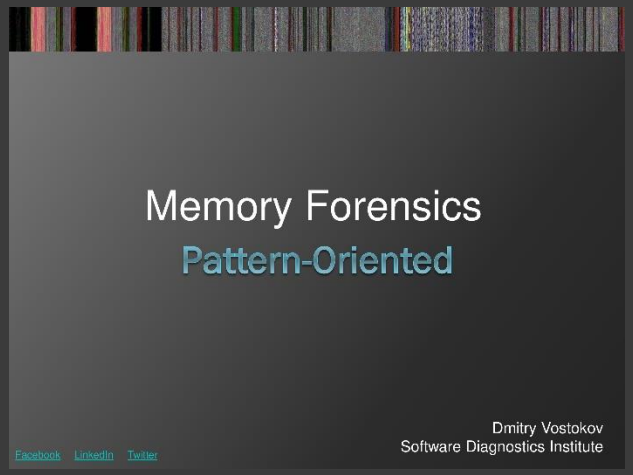
with Memory Dumps

Dmitry Vostokov
Software Diagnostics Services

Course Idea







Memory Acquisition Patterns

Structural Memory Patterns

Course Plan

- Pattern-Oriented Memory Forensics
- Malware Analysis with Memory Dumps
- Advanced Windows Memory Dump Analysis
- Structural Memory Patterns
- Memory Acquisition Patterns

Course Coverage

- Windows 10, 11, and a few older systems
- Both x64 and x86 code, WOW64
- Process and physical memory dumps
- Windows data structures
- Memory analysis patterns
- Structural memory patterns
- Malware analysis patterns
- Memory acquisition patterns

Most of the exercises are focused on x64 code.