Windows Trace and Log Analysis Accelerated

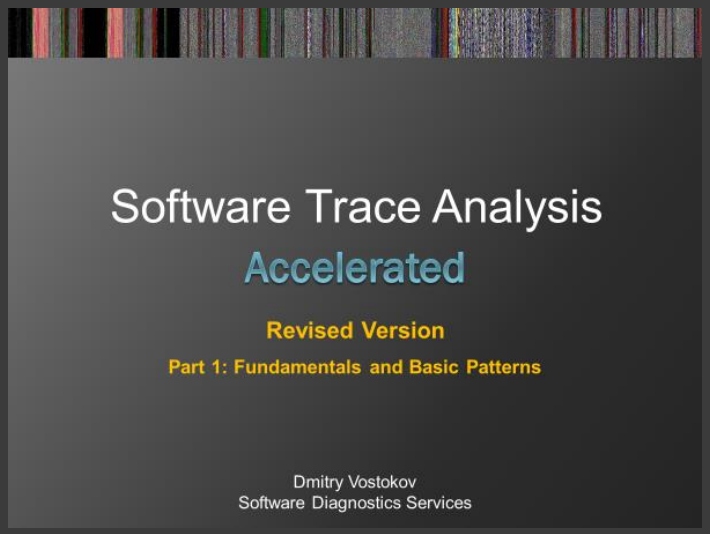
Version 2.0

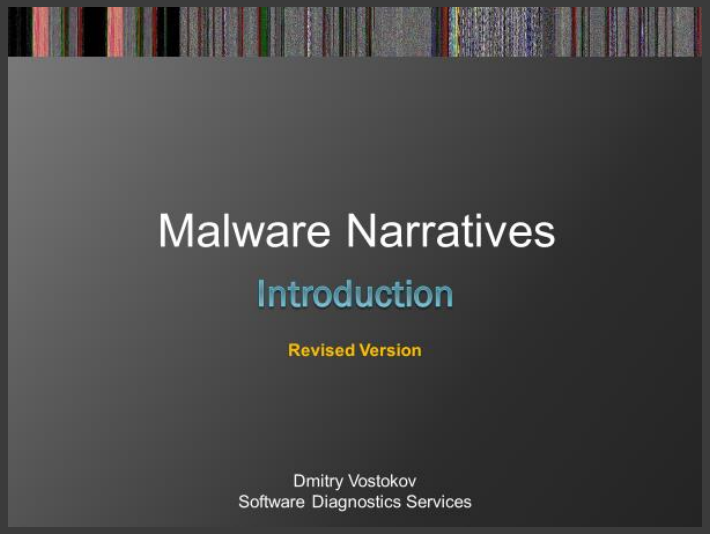
Dmitry Vostokov
Software Diagnostics Services

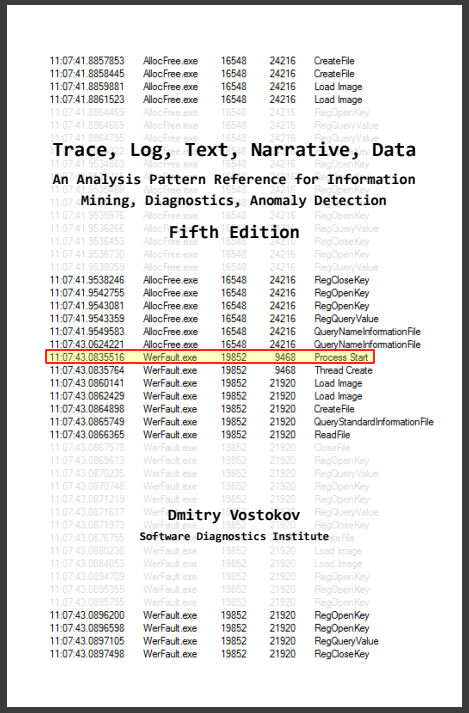
Training Goals

- Pattern-oriented trace and log analysis
  - Theory
  - Application
  - Tour
- Practice analysis patterns using tools

Training Parts







Trace and Log Formats

- Windows system logs (ETL, PML)
- Your and 3rd-party logs (ETL, CSV, JSON, Text)
- Performance data

Tools (Collection)

- Process Monitor
- OSQuery
- UIforETW (includes WPT)
- Windows Performance Toolkit (includes WPR)
- Message Analyzer (retired)
- PerfView
- CDFControl

Tools (Conversion)

- etl2pcapng
- etl-parser
- etw2json
- SilkETW

Tools (Viewing/Analysis)

Process Monitor	PML
OSQuery	SQL
Windows Performance Toolkit (includes WPA) PerfView Message Analyzer (retired) CDFControl	ETL
CSViewer Excel/LibreOffice Calc	CSV
Visual Studio Code	TXT

Exercise T0

1. Download Process Monitor
2. Trace system activity
3. Add more columns such as TID
4. Filter a thread based on TID
5. Reset filter
6. Filter an adjoint thread based on image name svchost.exe
7. Filter an adjoint thread based on PID

Exercise Q0

1. Download and install OSQuery
2. Run with CSV output

```
osqueryi.exe --csv --separator ","
```

3. Explore .help
4. Explore the list of existing .tables
5. Explore the processes table

```
select * from processes;
```

6. Explore the windows_crashes table

```
select * from windows_crashes;
```

7. .quit

Exercise T1

- **Goal:** Learn how to identify application crashes
- **Patterns:** Background Components; Adjoint Thread of Activity; Discontinuity; Guest Module

Exercise T2

- **Goal:** Learn how to identify CPU consumption, profile processes and threads
- **Patterns:** Activity Region; Characteristic Message Block; Periodic Message Block; Thread of Activity; No Activity; Counter Value; Sparse Trace

Exercise T3

- **Goal:** Learn how to calculate message current and density
- **Patterns:** Activity Region; Thread of Activity; Time Delta; Message Current; Message Density; Relative Density

Exercise T4

- **Goal:** Learn how to compare software traces and logs
- **Patterns:** Master Trace; Characteristic Message Block; Bifurcation Point

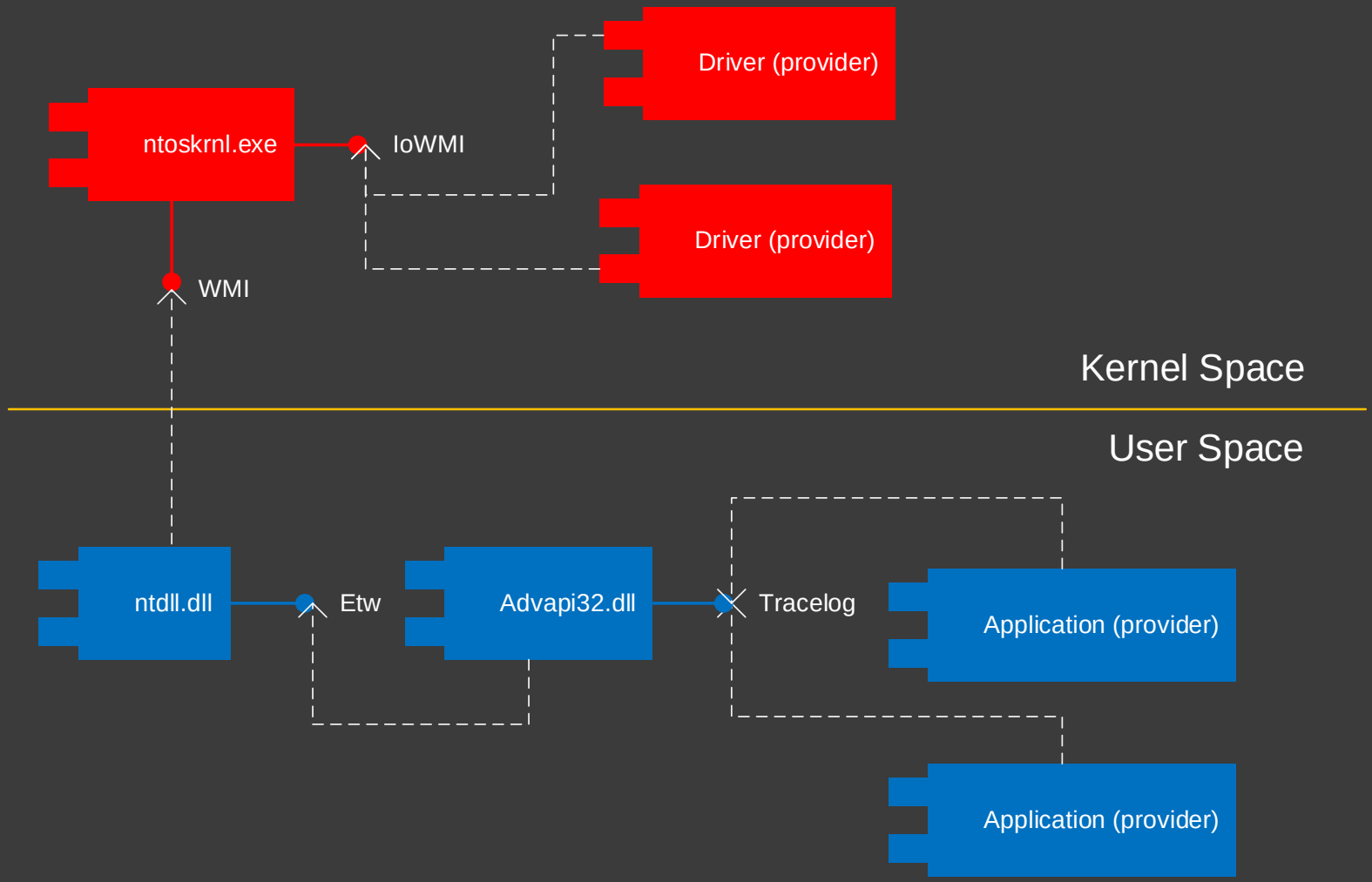
Exercise T5

- **Goal:** Learn the process startup sequence for a remote desktop session
- **Patterns:** Adjoint Thread of Activity; Anchor Messages; Message Interleave

Exercise T6

- **Goal:** Learn how to work with split traces
- **Patterns:** Split Trace; Adjoint Thread of Activity; Discontinuity; Time Delta; Break-in Activity; Resume Activity

ETW Architecture Simplified



Exercise L0

- **Goal:** Learn how to work with WPA, PerfView, and Message Analyzer
- **Patterns:** Discontinuity; Time Delta; Anchor Messages; Message Interleave

Q&A

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

Thank you for attendance!