



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

Software Trace Analysis Accelerated

Revised Version

Part 1: Fundamentals and Basic Patterns

Dmitry Vostokov
Software Diagnostics Services

Malware Narratives Introduction

Revised Version

Dmitry Vostokov
Software Diagnostics Services

Practical Demonstrations

```
11:07:41.8887853 AllocFree.exe 16548 24216 CreateFile
11:07:41.8889445 AllocFree.exe 16548 24216 CreateFile
11:07:41.8889881 AllocFree.exe 16548 24216 Load Image
11:07:41.8861523 AllocFree.exe 16548 24216 Load Image
11:07:41.8864653 AllocFree.exe 16548 24216 RegQueryValue
11:07:41.8869795 WerFault.exe 19852 21920 RegOpenKey
11:07:41.9532576 AllocFree.exe 16548 24216 RegOpenKey
11:07:41.9532698 AllocFree.exe 16548 24216 RegQueryValue
11:07:41.9536453 AllocFree.exe 16548 24216 RegCloseKey
11:07:41.9536720 AllocFree.exe 16548 24216 RegOpenKey
11:07:41.9539059 AllocFree.exe 16548 24216 RegQueryValue
11:07:41.9538246 AllocFree.exe 16548 24216 RegCloseKey
11:07:41.9542755 AllocFree.exe 16548 24216 RegOpenKey
11:07:41.9543081 AllocFree.exe 16548 24216 RegOpenKey
11:07:41.9543359 AllocFree.exe 16548 24216 RegQueryValue
11:07:41.9549583 AllocFree.exe 16548 24216 QueryNameInformationFile
11:07:43.0624221 AllocFree.exe 16548 24216 QueryNameInformationFile
11:07:43.0835516 WerFault.exe 19852 9468 Process Start
11:07:43.0835764 WerFault.exe 19852 9468 Thread Create
11:07:43.0860141 WerFault.exe 19852 21920 Load Image
11:07:43.0862429 WerFault.exe 19852 21920 Load Image
11:07:43.0864988 WerFault.exe 19852 21920 CreateFile
11:07:43.0865749 WerFault.exe 19852 21920 QueryStandardInformationFile
11:07:43.0866365 WerFault.exe 19852 21920 ReadFile
11:07:43.0866719 WerFault.exe 19852 21920 CreateFile
11:07:43.0869613 WerFault.exe 19852 21920 RegOpenKey
11:07:43.0870235 WerFault.exe 19852 21920 RegQueryValue
11:07:43.0870748 WerFault.exe 19852 21920 RegOpenKey
11:07:43.0871218 WerFault.exe 19852 21920 RegOpenKey
11:07:43.0871617 WerFault.exe 19852 21920 RegQueryValue
11:07:43.0871973 WerFault.exe 19852 21920 RegCloseKey
11:07:43.0876795 WerFault.exe 19852 21920 CreateFile
11:07:43.0880238 WerFault.exe 19852 21920 Load Image
11:07:43.0884853 WerFault.exe 19852 21920 Load Image
11:07:43.0894709 WerFault.exe 19852 21920 RegOpenKey
11:07:43.0895355 WerFault.exe 19852 21920 RegOpenKey
11:07:43.0895795 WerFault.exe 19852 21920 RegOpenKey
11:07:43.0896200 WerFault.exe 19852 21920 RegOpenKey
11:07:43.0896598 WerFault.exe 19852 21920 RegOpenKey
11:07:43.0897105 WerFault.exe 19852 21920 RegQueryValue
11:07:43.0897498 WerFault.exe 19852 21920 RegCloseKey
```

Trace, Log, Text, Narrative, Data

An Analysis Pattern Reference for Information

Mining, Diagnostics, Anomaly Detection

Fifth Edition

Dmitry Vostokov
Software Diagnostics Institute

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) ETL
- [CDFControl](#)

- [CSViewer](#) CSV
- Excel/[LibreOffice Calc](#)

- [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

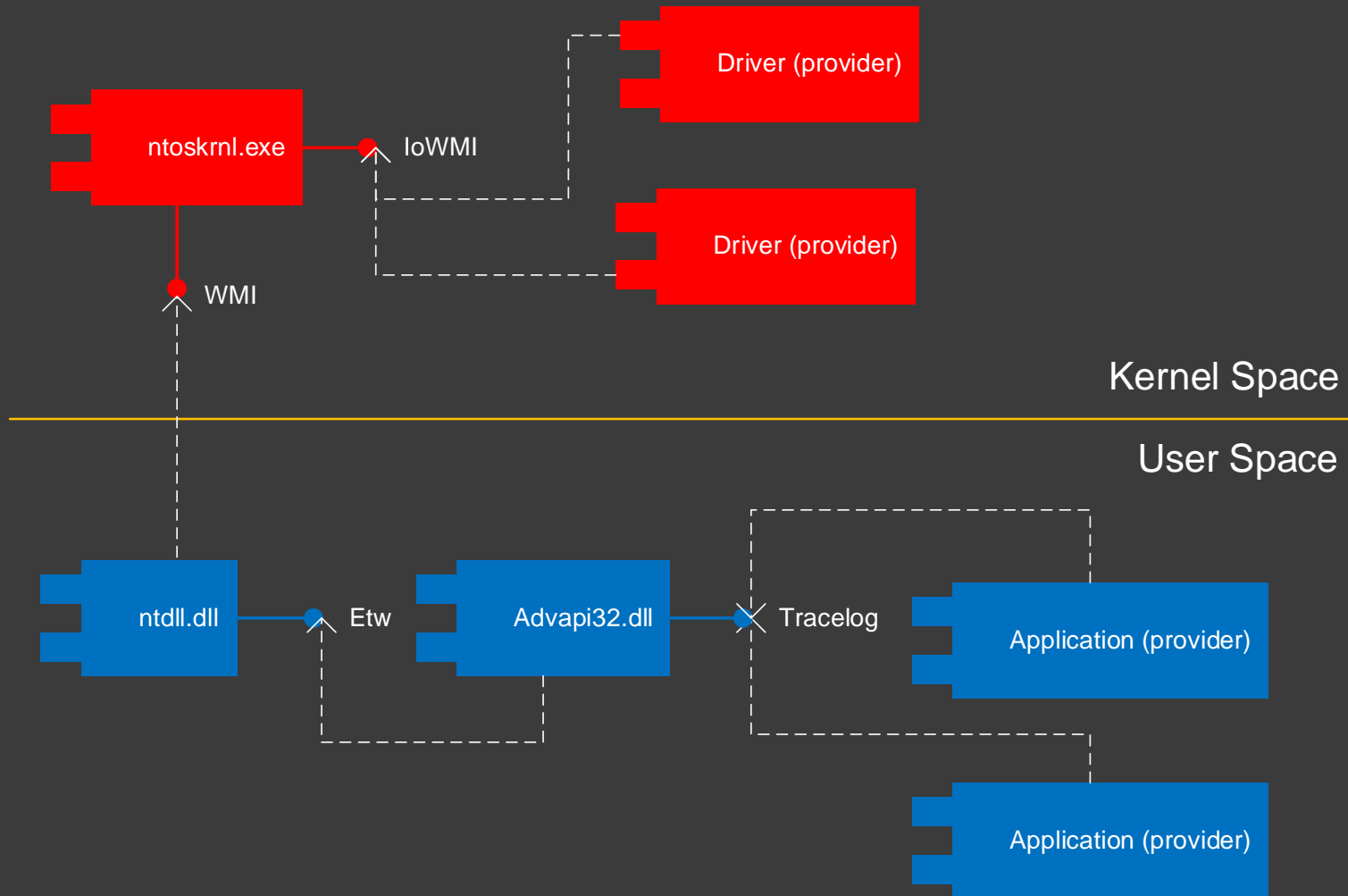
Exercise T5

- ⦿ **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!