Network Trace Analysis

Pattern-Oriented

Version 1.0

Dmitry Vostokov
Software Diagnostics Services
Hark

- Listen (to) “Hark! There’s the big bombardment.”
- Speak in one’s ear; whisper

Hark back (idiom)

- To return to a previous point, as in a narrative

http://www.thefreedictionary.com/hark
Prerequisites

- Interest in software diagnostics, troubleshooting, debugging and network trace analysis
- Experience in network trace analysis using Wireshark or Network Monitor
Why?

- A common diagnostics language
- Network diagnostics as software diagnostics
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.
Diagnostics Pattern

A common recurrent identifiable problem together with a set of recommendations and possible solutions to apply in a specific context.
Pattern Orientation

Pattern-driven

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

Pattern-based

- Pattern catalog evolution
- Catalog packaging and delivery

© 2013 Software Diagnostics Services
Catalog Classification

- By abstraction
  - Meta-patterns

- By artifact type
  - Software Log
  - Memory Dump
  - Network Trace

- By story type
  - Problem Description
  - Software Disruption
  - UI Problem

- By intention
  - Malware
Traces and Logs

Windows logs and patterns

Linux logs and patterns

Web Server logs and patterns

Event logs and patterns

Mac OS X logs and patterns

Network traces and patterns

GUI logs and patterns
Trace and Log Patterns

Software Trace and Log Analysis Patterns

- Windows logs
- Event logs
- Linux logs
- Mac OS X logs

- Web Server logs
- Network traces
- GUI logs
Software Narrative

A temporal sequence of events related to software execution.
Software Trace

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

- A sequence of formatted packets as trace messages
- Arranged by time
- A narrative story
Network Trace Analysis

Software Trace Analysis Patterns

Network Trace Analysis Patterns
Capture Tool Placing

- Sniffer placing
- Process Monitor placing
Trace Maps

- Network map
- Deployment architecture map
Name Resolution

- MAC -> IP and IP -> DNS
- PID -> process name
Minimal Trace Graphs
Pattern-Driven Analysis

Logs → Checklists ↔ Patterns → Action
Pattern-Based Analysis
Pattern Classification

- Vocabulary
- Error
- Trace as a Whole
- Large Scale
- Activity
- Message
- Block
- Trace Set
Reference and Course

- Catalog from Software Diagnostics Library
  Software Trace Analysis Patterns

- Free reference graphical slides
  Accelerated-Windows-Software-Trace-Analysis-Public.pdf

- Training course*
  Accelerated Windows Software Trace Analysis

* Available as a full color paperback book, PDF book, on SkillsSoft Books 24x7. Recording is available for all book formats
Selected Patterns
Master Trace

Normal network capture
Message Current

\[ J_1 > J_2 \]

Packets/s
Message Density

D_1 > D_2
Characteristic Block

Pattern Category
Large Scale

Time

# Src Dst Time Message

D₁ < D₂
L₁ > L₂
**Example**

The image shows a network trace analysis tool with a table displaying Ethernet conversations. The table includes columns for various parameters such as IP addresses, packet counts, byte counts, and duration. The tool allows for name resolution and display filter options.
Thread of Activity

Pattern Category

Activity
Adjoint Thread

Pattern Category
Activity

Filtered by:
- Source
- Destination
- Protocol
- Message
- Expression
We messages from other servers but only see our own traffic
Conversation between 2 endpoints
Significant Event

Time Reference feature in Wireshark
Marked Messages

Annotated messages:

- session initialization [+]
- session tear-off [-]
- port A activity [+]
- port B activity [-]
- protocol C used [-]
- address D used [-]

[+] activity is present in a trace
[-] activity is undetected or not present

Marked Packets feature in Wireshark
Connection initiation (Prologue) and termination (Epilogue)
Inter-Correlation

- Several packet sniffers at once
- Internal and external views

Process Monitor log + network trace
Circular Trace
Split Trace

Pattern Category

Trace Set
Paratext

Info column in Wireshark
Visibility Limit

Visibility window for sniffing

Pattern Category
- Trace as a Whole
Incomplete History

- Packet loss
- Missing ACK
Possible New Patterns

- Full Trace (promiscuous mode)
- Embedded Message (PDU chain, protocol data unit, packet)
- Ordered Message (TCP/IP sequence numbers)
- Illegal Message (sniffed with illegally obtained privileges)
- Dual Trace (in / out, duplex)
Further Reading

- Practical Packet Analysis, 2nd edition, by Chris Sanders
- Software Diagnostics Institute
- Memory Dump Analysis Anthology: Volumes 3, 4, 5, 6, …
  Volume 7 is in preparation (July, 2013)
- Introduction to Software Narratology
- Malware Narratives
What’s Next?

- Accelerated Network Trace Analysis
- Generative Software Narratology
- Pattern-Oriented Hardware Signal Analysis
Q&A

Please send your feedback using the contact form on DumpAnalysis.com
Thank you for attendance!