



Network Trace Analysis Pattern-Oriented

Version 1.0

Dmitry Vostokov
Software Diagnostics Services

Wireshark

Hark

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

Shorter Oxford English Dictionary

Hark back (*idiom*)

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

<http://www.thefreedictionary.com/hark>

Prerequisites

- ① Interest in software diagnostics, troubleshooting, debugging and network trace analysis
- ① 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

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

Linux logs
and patterns

Windows logs
and patterns

Mac OS X logs
and patterns

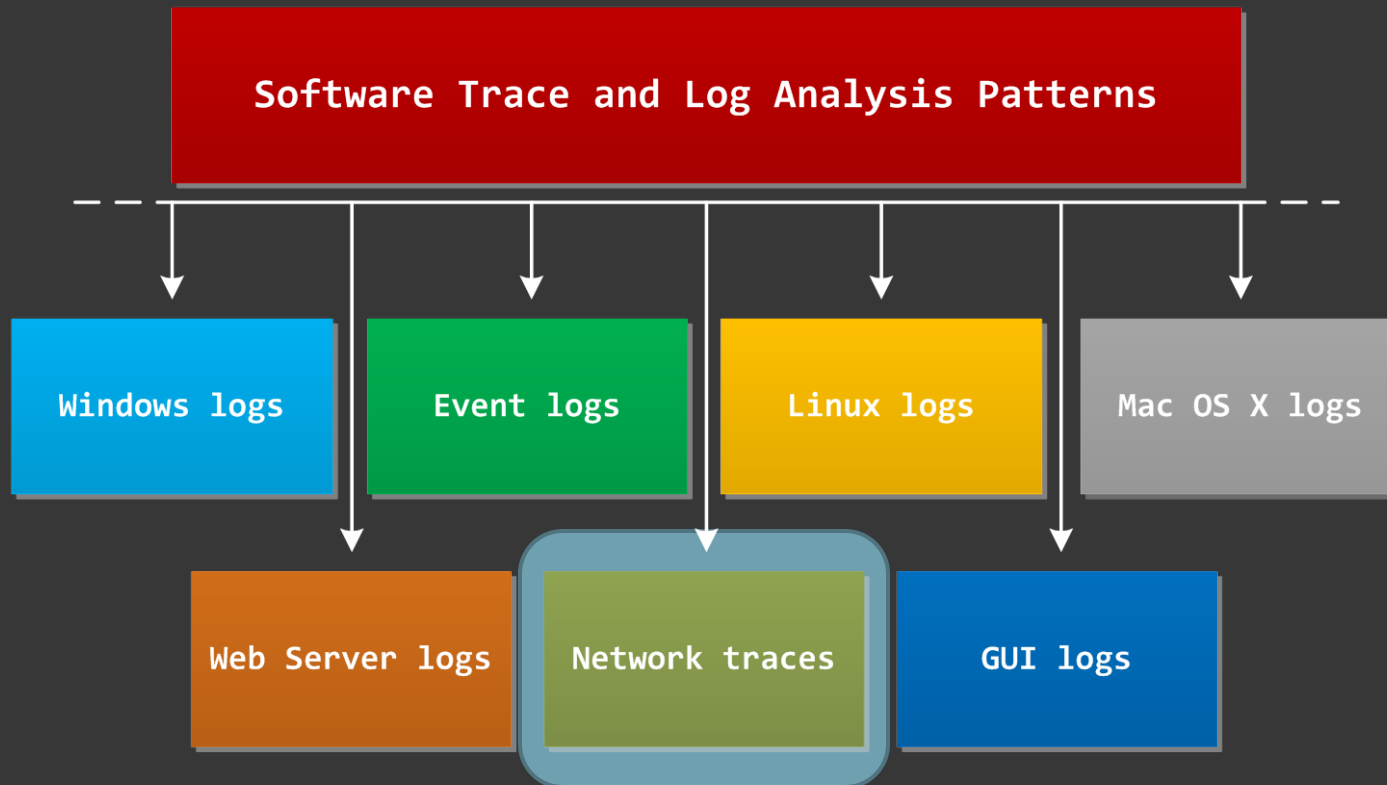
Event logs
and patterns

Web Server logs
and patterns

Network traces
and patterns

GUI logs
and patterns

Trace and Log Patterns

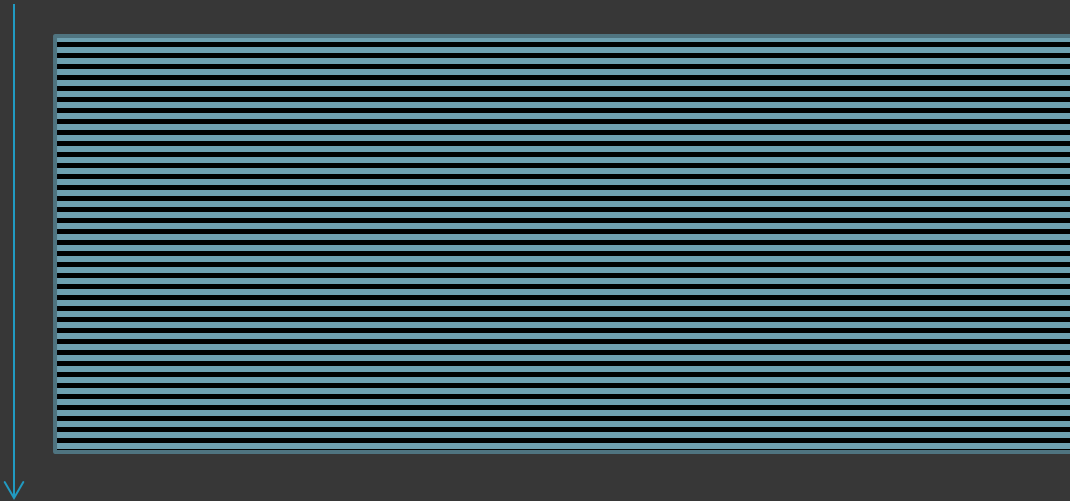


Software Narrative

A temporal sequence of events related to software execution.

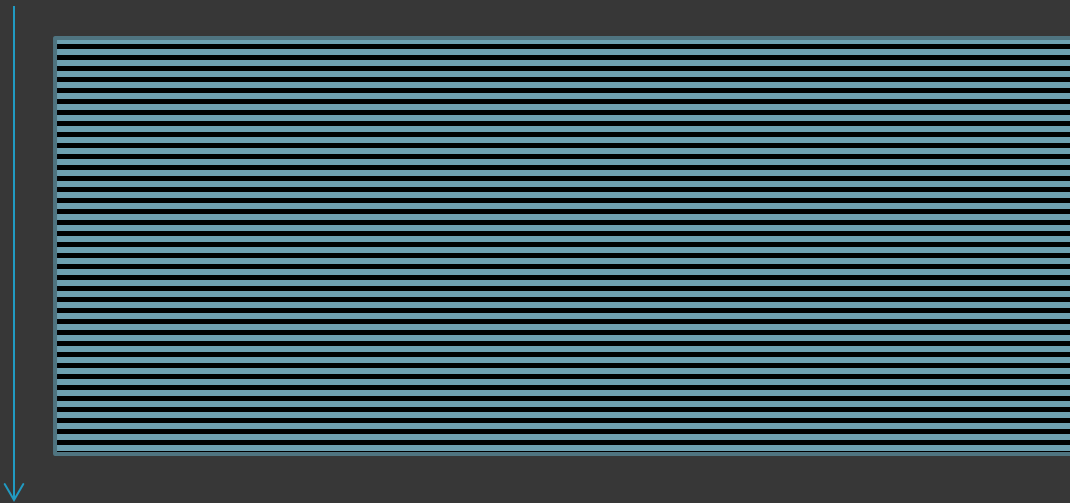
Software Trace

- 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

The diagram consists of two nested, horizontally-oriented ovals. The outer oval is a light teal color and contains the text 'Software Trace Analysis Patterns'. The inner oval is a darker teal color and contains the text 'Network Trace Analysis Patterns'. The inner oval is centered within the outer oval, indicating that network trace analysis is a subset or a specific application of software trace analysis patterns.

Network Trace Analysis Patterns

Capture Tool Placing

- Sniffer placing
- Process Monitor placing

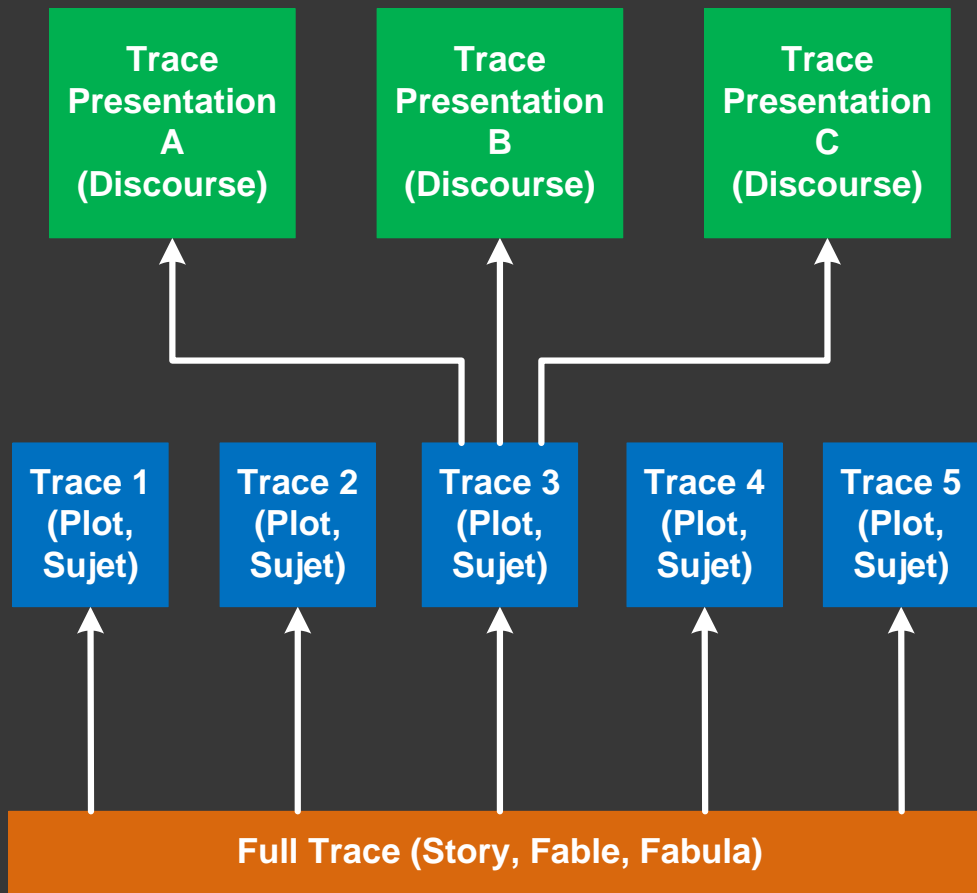
Trace Maps

- ⦿ Network map
- ⦿ Deployment architecture map

Name Resolution

- ⦿ MAC -> IP and IP -> DNS
- ⦿ PID -> process name

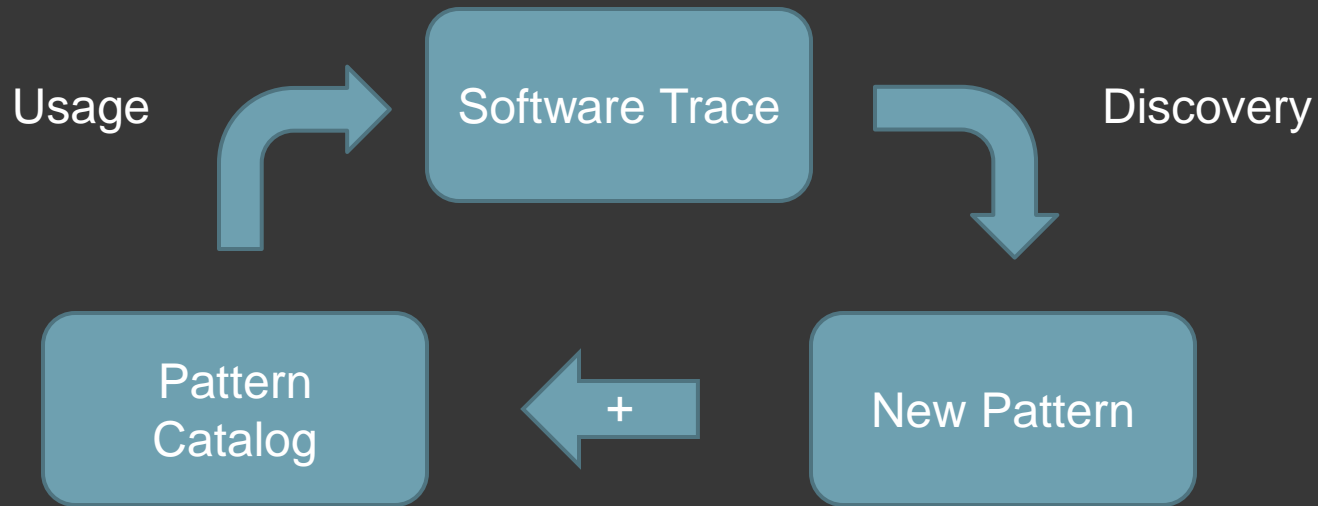
Trace Presentation



Pattern-Driven Analysis



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](#)

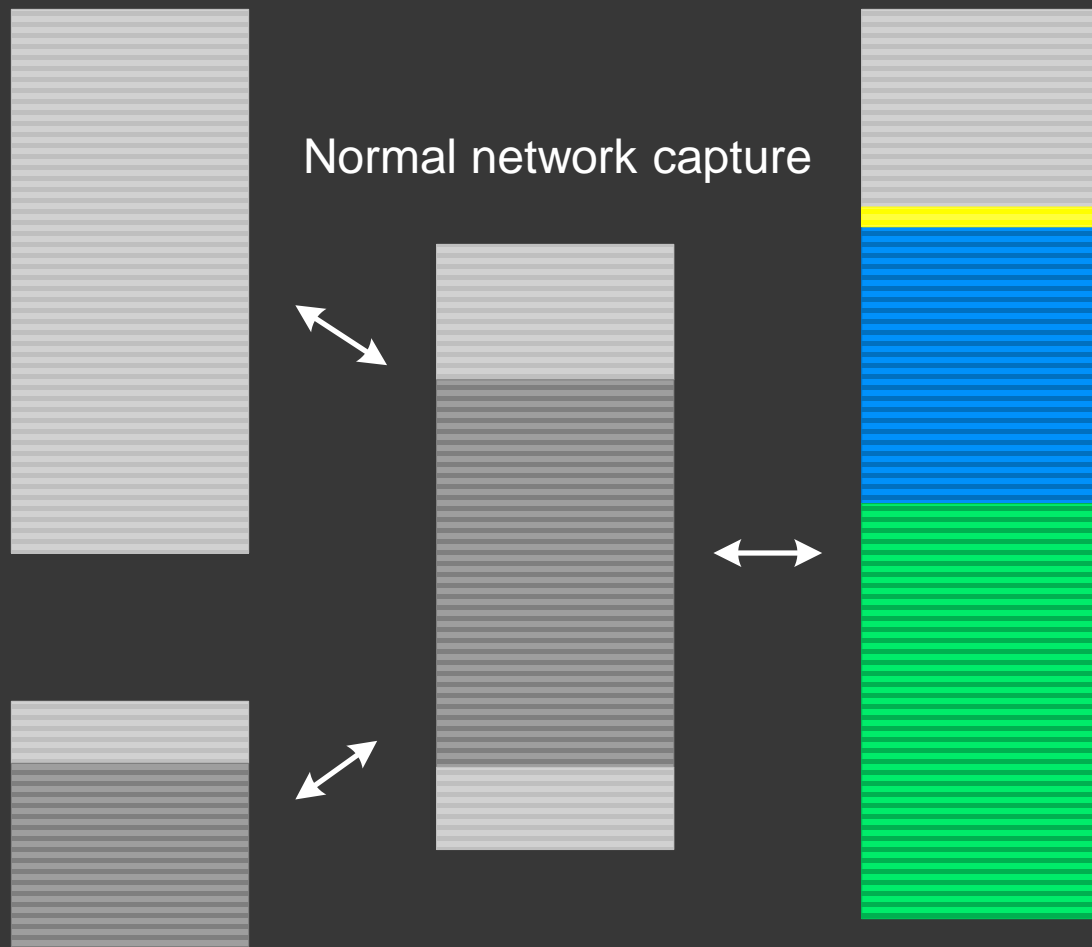
* Available as a full color paperback book, PDF book, on SkillsSoft Books 24x7. Recording is available for all book formats

Selected Patterns

Master Trace

Pattern Category

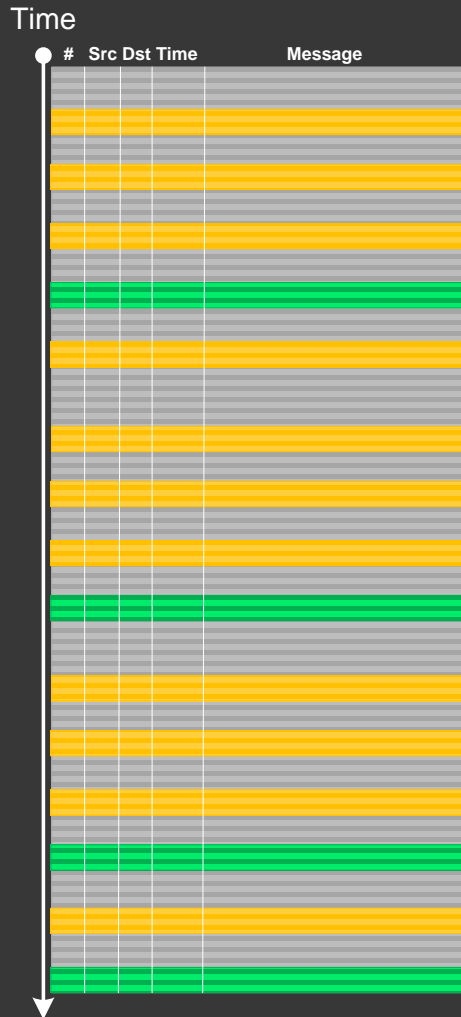
Trace Set



Message Density

Pattern Category

Trace as a Whole

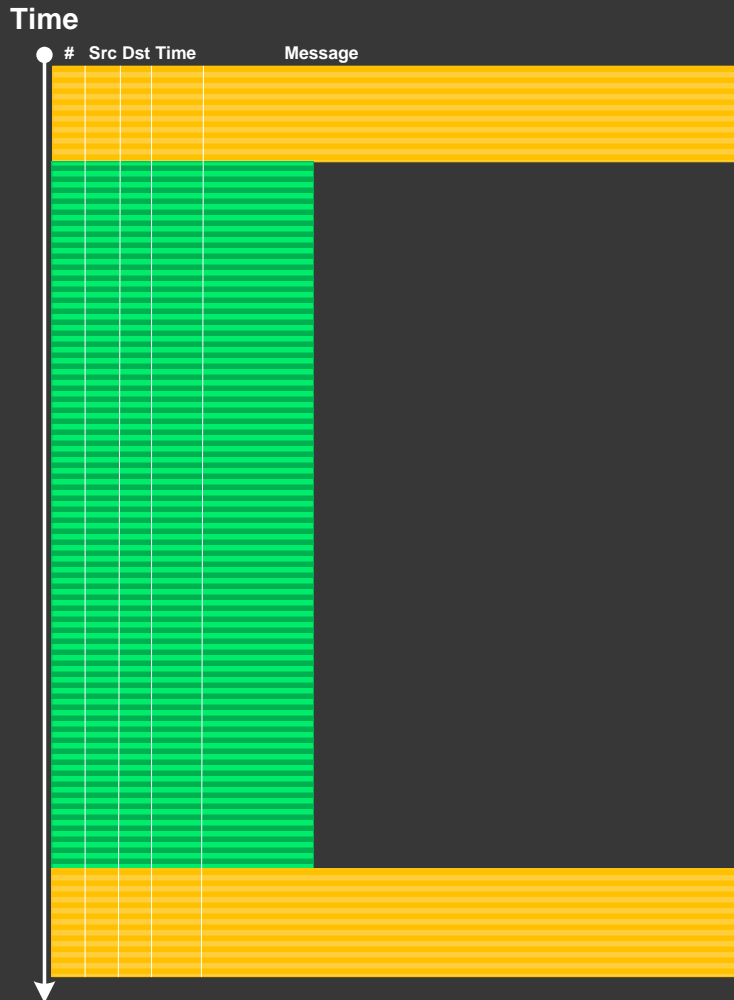


$$D_1 > D_2$$

Characteristic Block

Pattern Category

Large Scale



$$D_1 < D_2$$

$$L_1 > L_2$$

Example

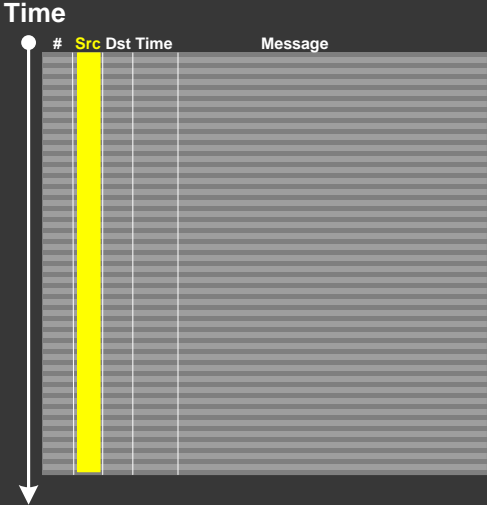
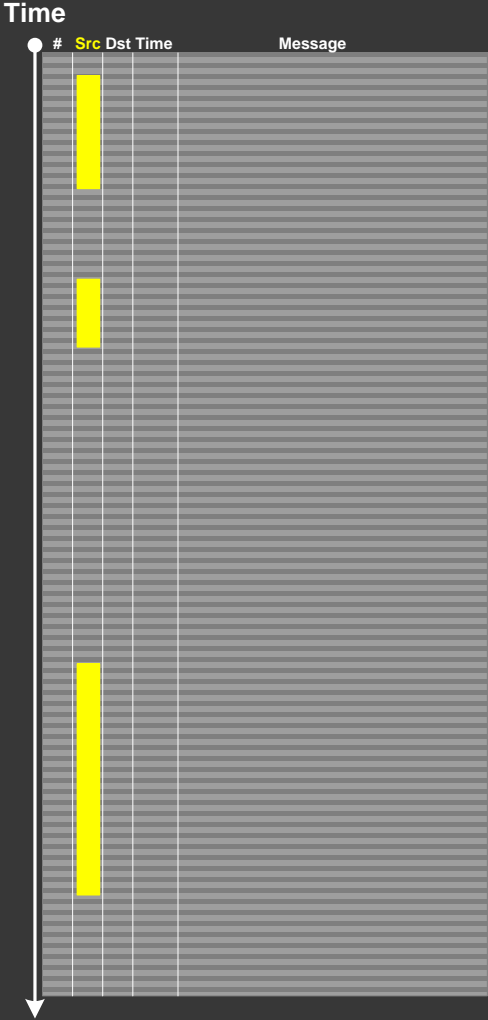
The screenshot shows a window titled "Conversations: networktrace.pcapng". It displays a list of network conversations under the "Ethernet: 6" category. The table below summarizes the data shown in the screenshot.

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
HuaweiTe_fb	IntelCor_54:3	259	70 069	135	53 217	124	16 852	0.000000000	89.0852	4778.98	1513.34
IPv4mcast_7f	IntelCor_54:3	31	4 453	0	0	31	4 453	0.308180000	87.9477	N/A	405.06
IPv6mcast_0c	IntelCor_54:3	27	5 616	0	0	27	5 616	0.936276000	86.0141	N/A	522.33
HuaweiTe_fb	Broadcast	11	462	11	462	0	0	4.403077000	80.2791	46.04	N/A
IPv6mcast_0c	IntelCor_54:3	2	306	0	0	2	306	14.685769000	31.9996	N/A	76.50
IntelCor_54:3	Broadcast	1	42	1	42	0	0	78.882175000	0.0000	N/A	N/A

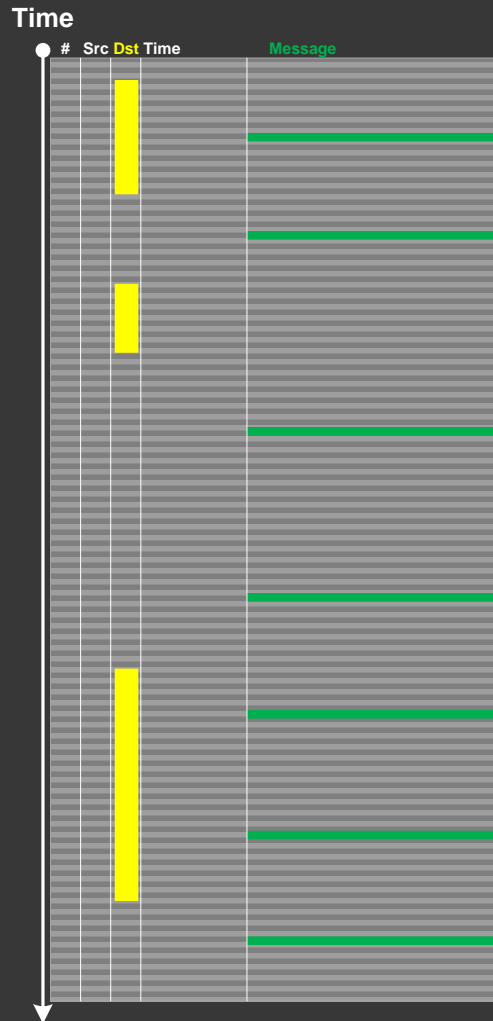
At the bottom of the window, there are checkboxes for "Name resolution" (checked) and "Limit to display filter" (unchecked). Buttons for "Help", "Copy", "Follow Stream", and "Close" are also present.

Thread of Activity

Pattern Category
Activity



Adjoint Thread



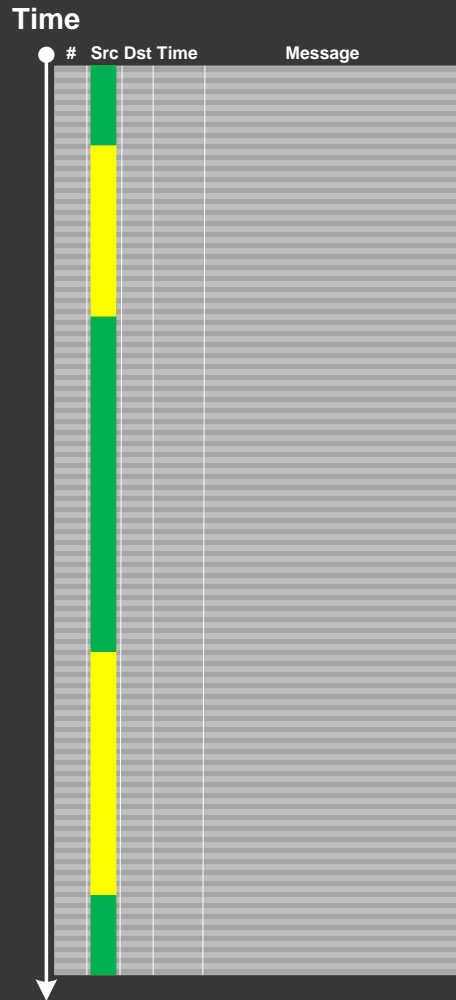
Pattern Category

Activity

Filtered by:

- Source
- Destination
- Protocol
- Message
- Expression

No Activity

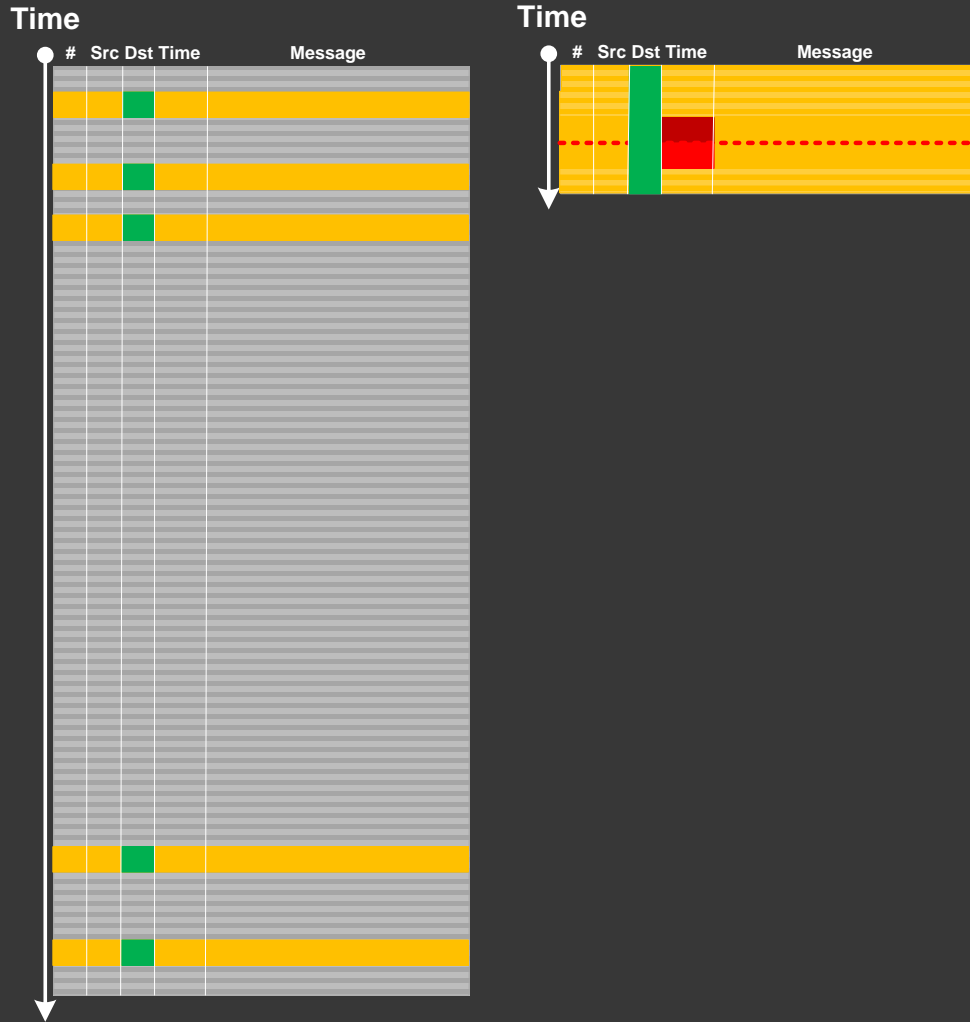


Pattern Category

Activity

We messages from other servers but only see our own traffic

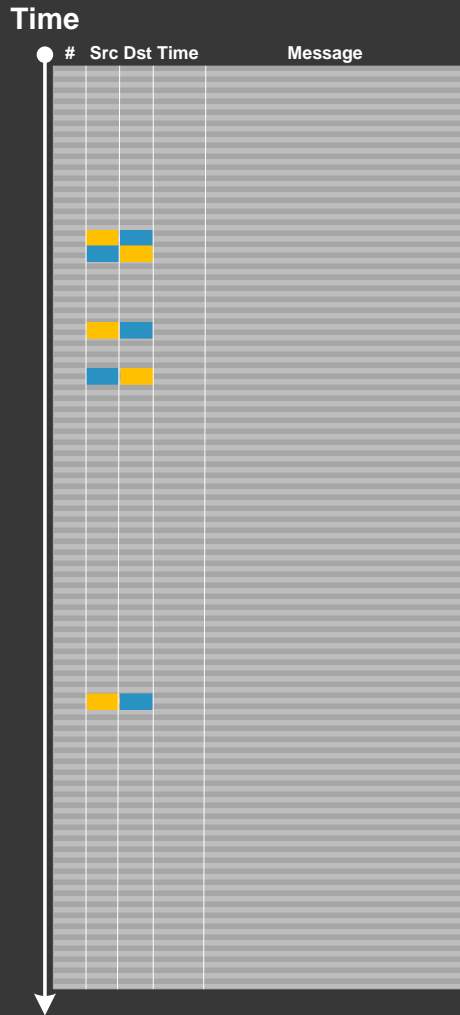
Discontinuity



Pattern Category

Activity

Dialog

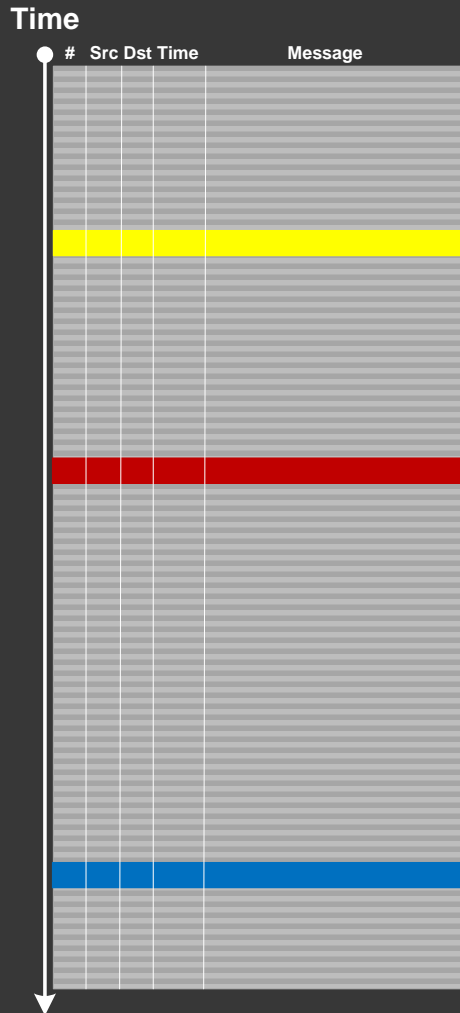


Conversation between 2 endpoints

Significant Event

Pattern Category

Message



Time Reference feature in Wireshark

Marked Messages

Pattern Category

Message

Annotated messages:

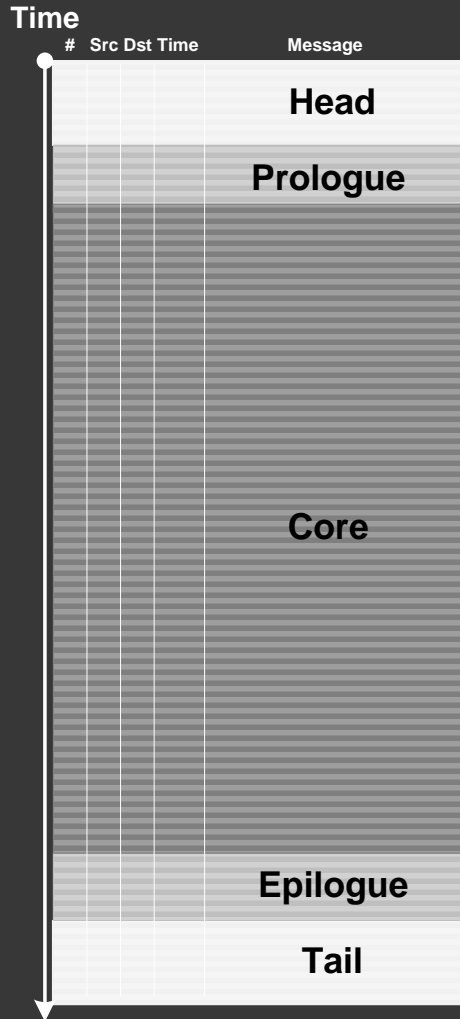
```
session initialization [+]
session tear-off [-]
port A activity [+]
port B activity [-]
protocol C used [-]
address D used [-]
```

Marked Packets
feature in Wireshark

[+] activity is present in a trace

[-] activity is undetected or not present

Partition



Pattern Category

Trace as a Whole

Connection initiation (Prologue) and
termination (Epilogue)

Inter-Correlation

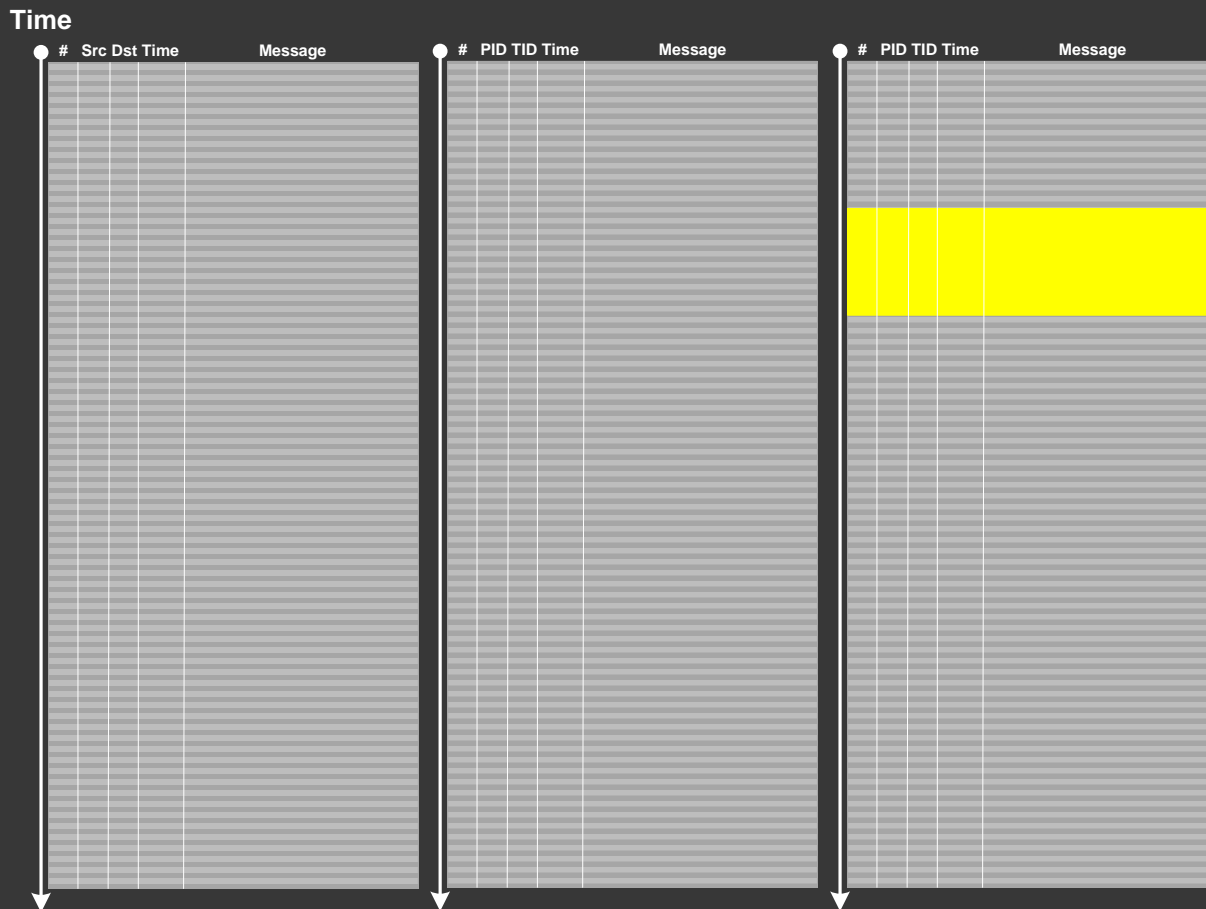
Pattern Category

Trace Set

- ⦿ Several packet sniffers at once
- ⦿ Internal and external views

Process Monitor log + network trace

Split Trace



Pattern Category

Trace Set

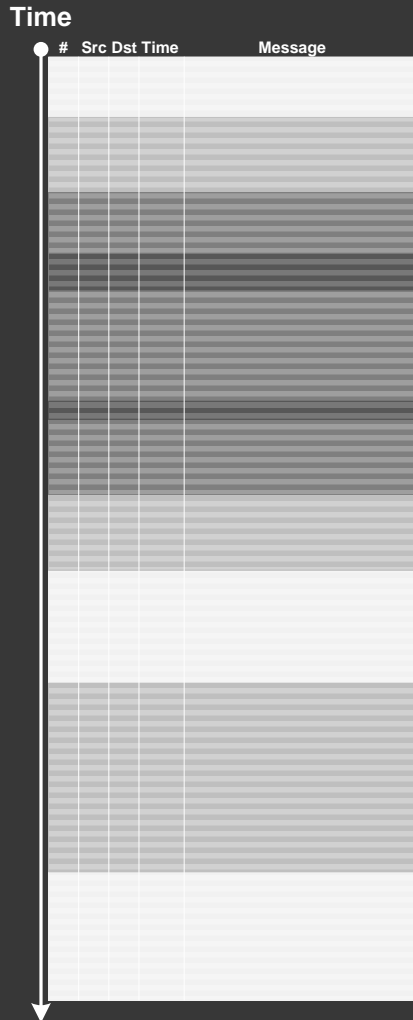
Paratext

Info column in Wireshark

Frames

Pattern Category

Large Scale



OSI, TCP/IP Layers

Visibility Limit

Visibility window for sniffing

Pattern Category

Trace as a Whole

PC 3

sniffer

PC 1

PC 2

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!