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

- 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

Catalog Classification

- By abstraction

Meta-patterns

- By artifact type

Software Log* Memory Dump **Network Trace***

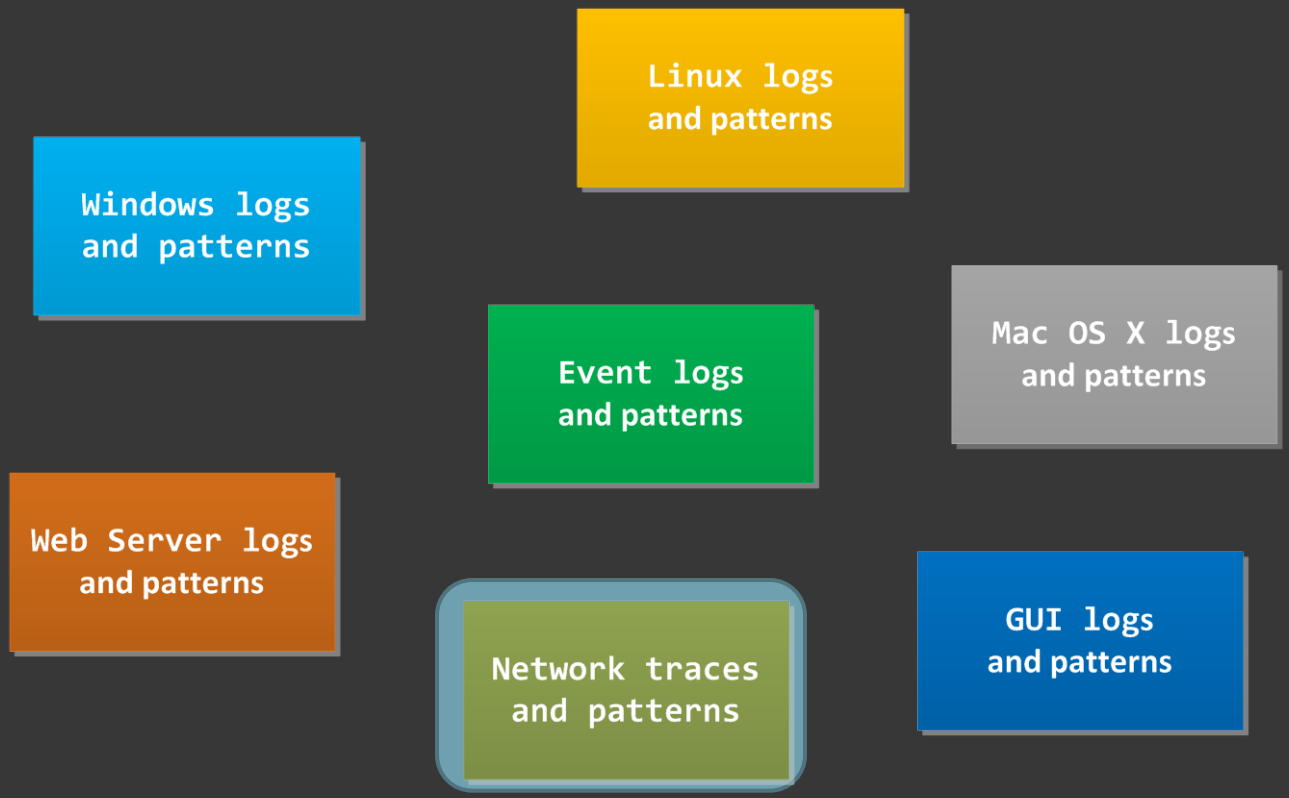
- By story type

Problem Description Software Disruption UI Problem

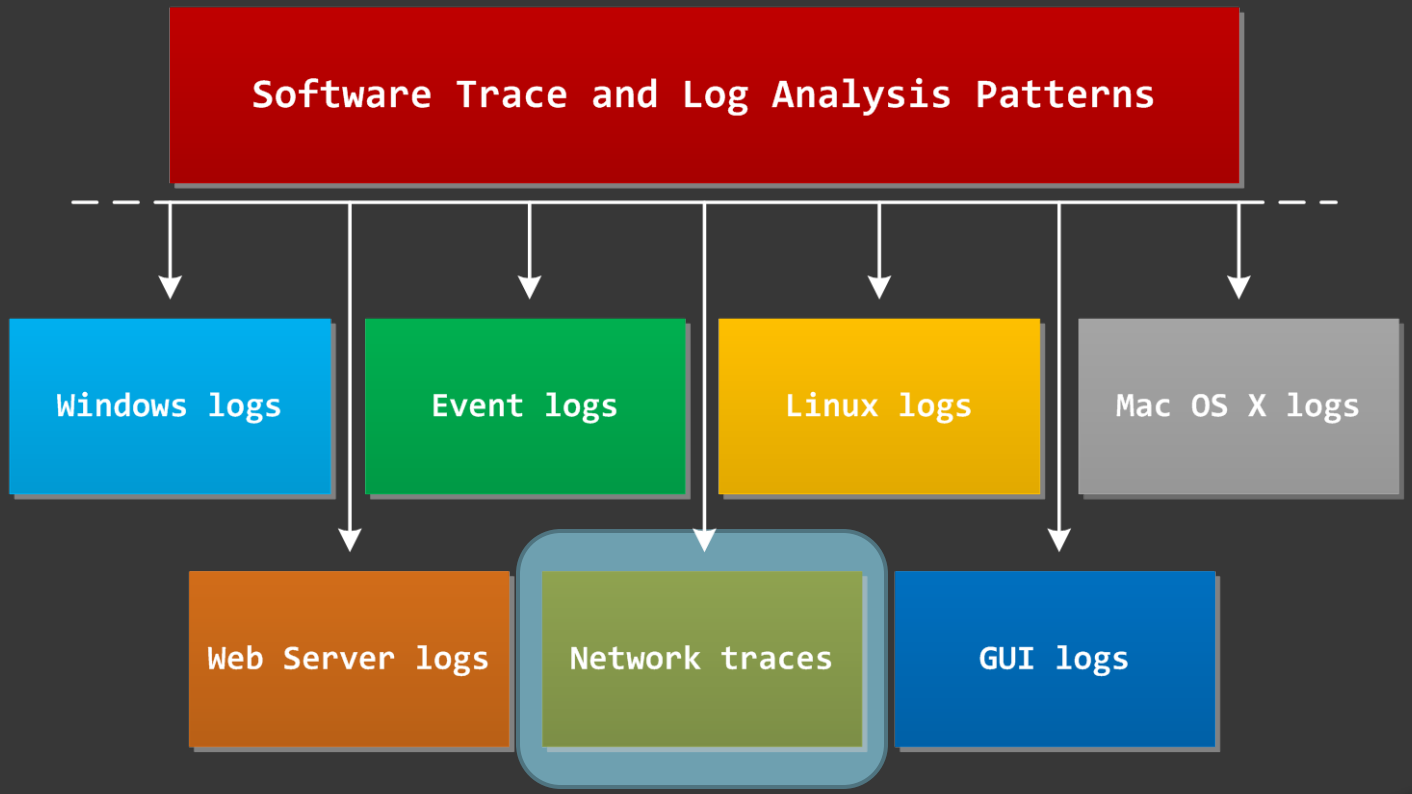
- By intention

Malware

Traces and Logs



Trace and Log Patterns

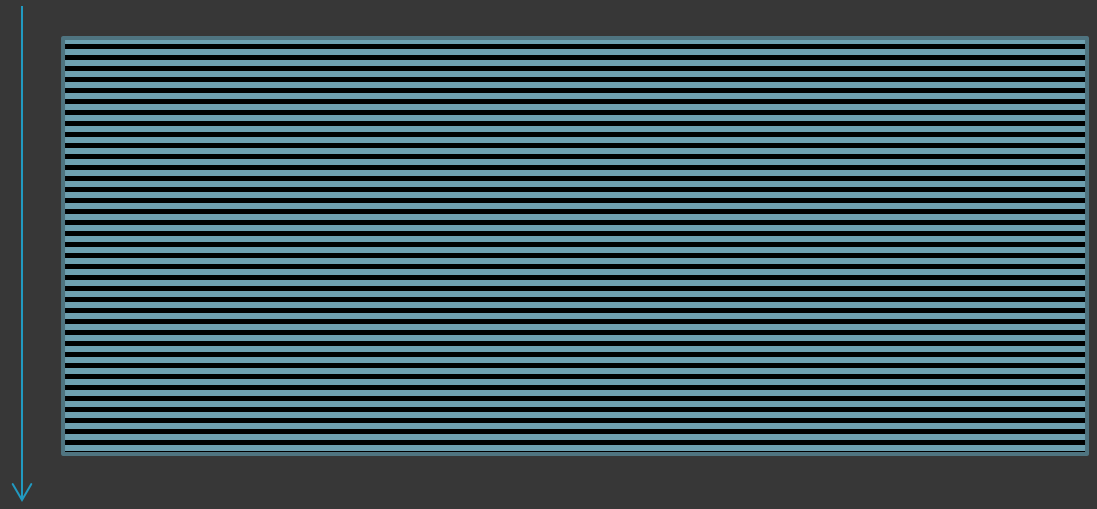


Software Narrative

> A temporal sequence of events related to software execution.

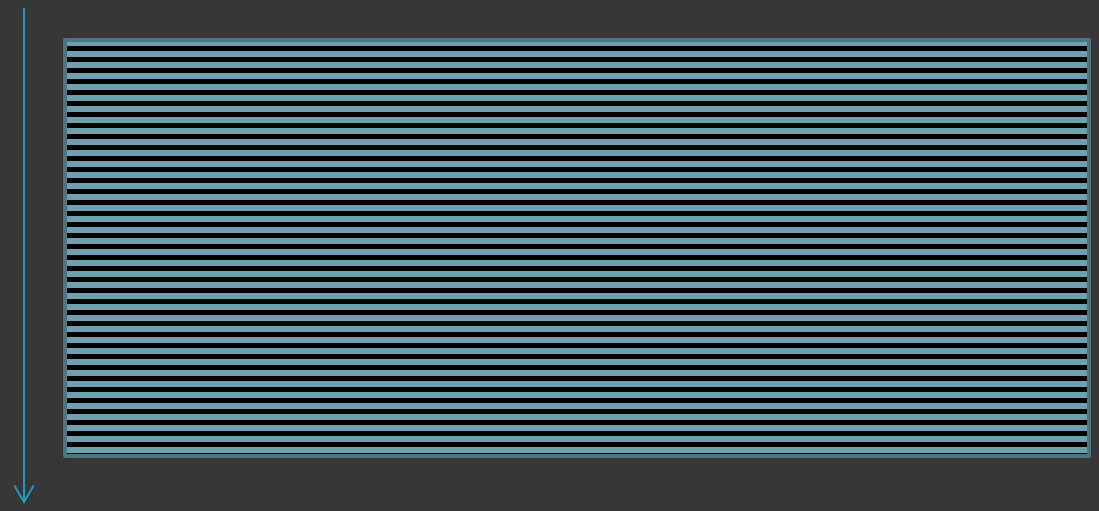
Software Trace

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

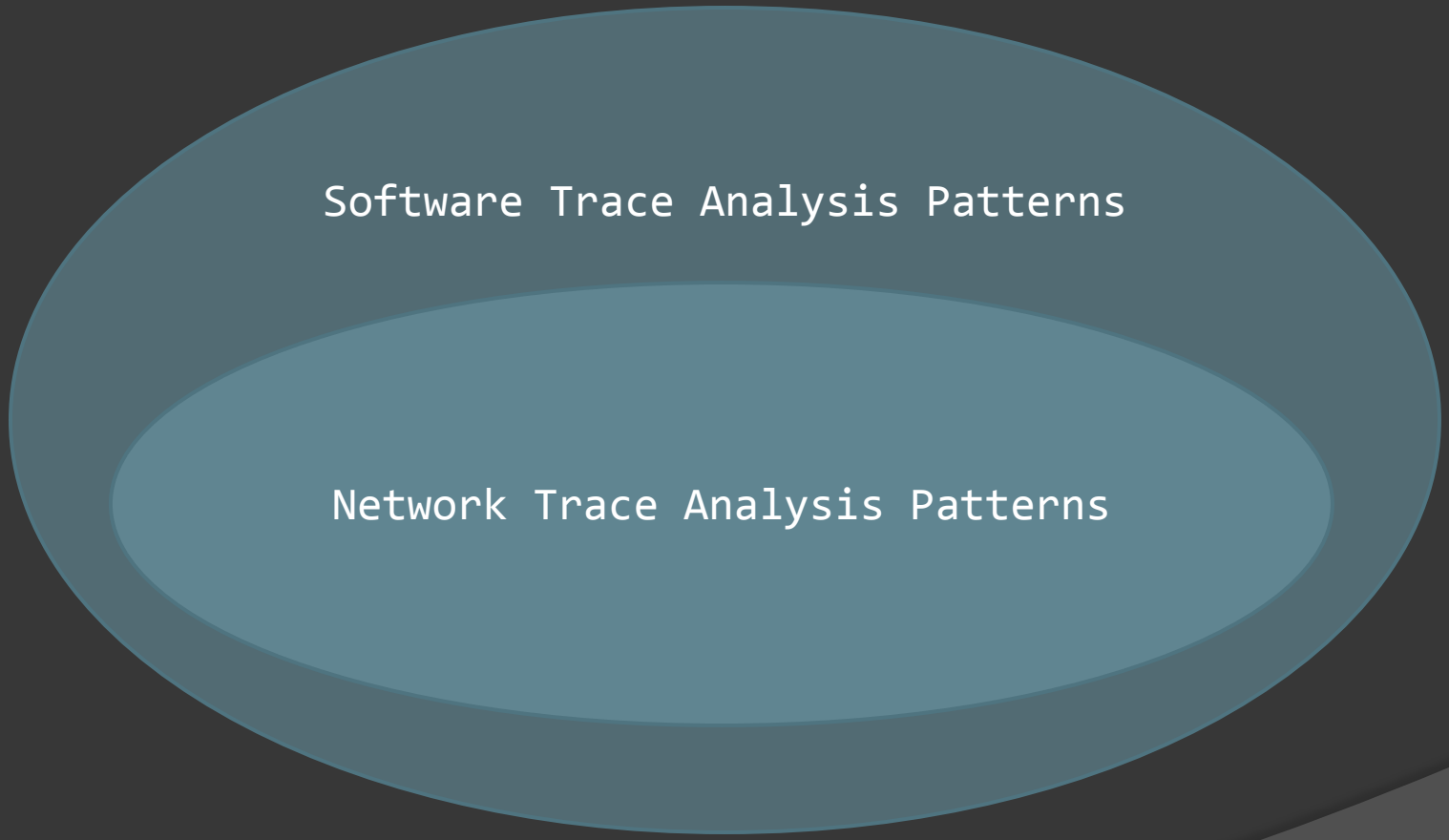


Network Trace

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



Network Trace Analysis



Capture Tool Placing

- Sniffer placing
- Process Monitor placing

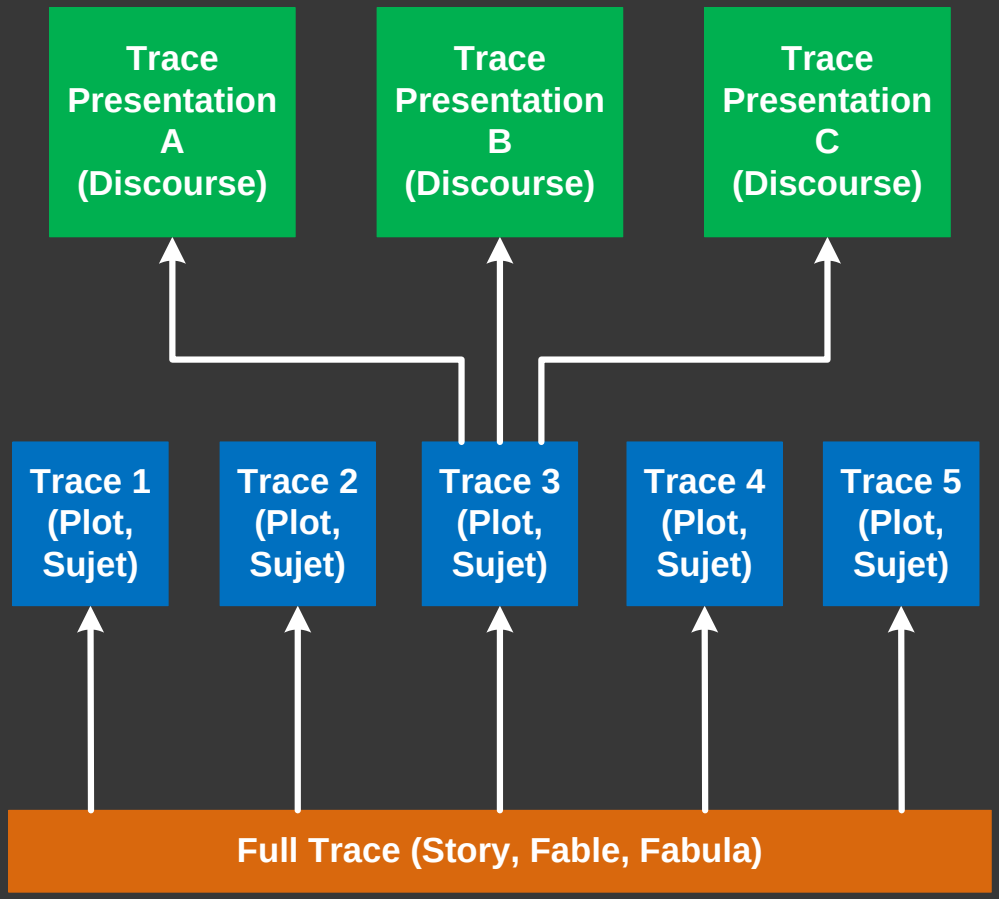
Trace Maps

- Network map
- Deployment architecture map

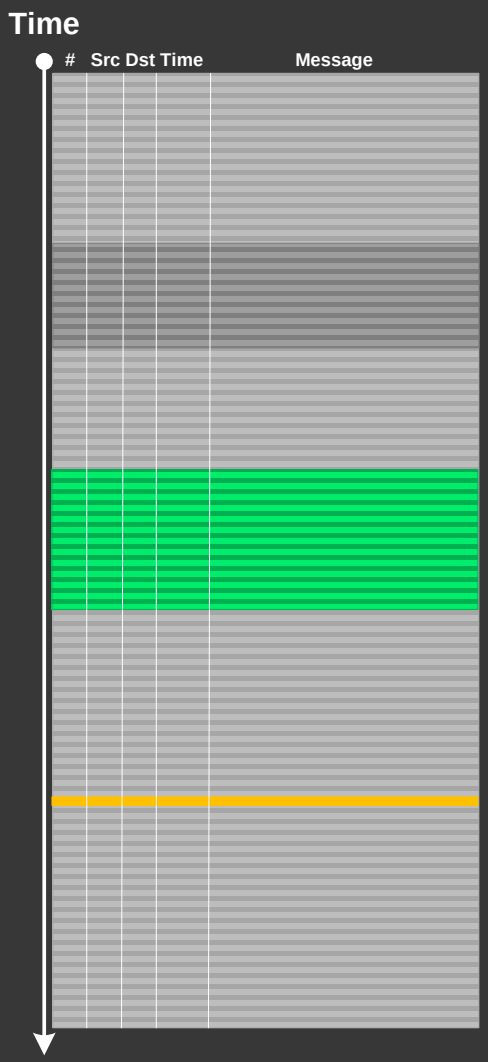
Name Resolution

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

Trace Presentation

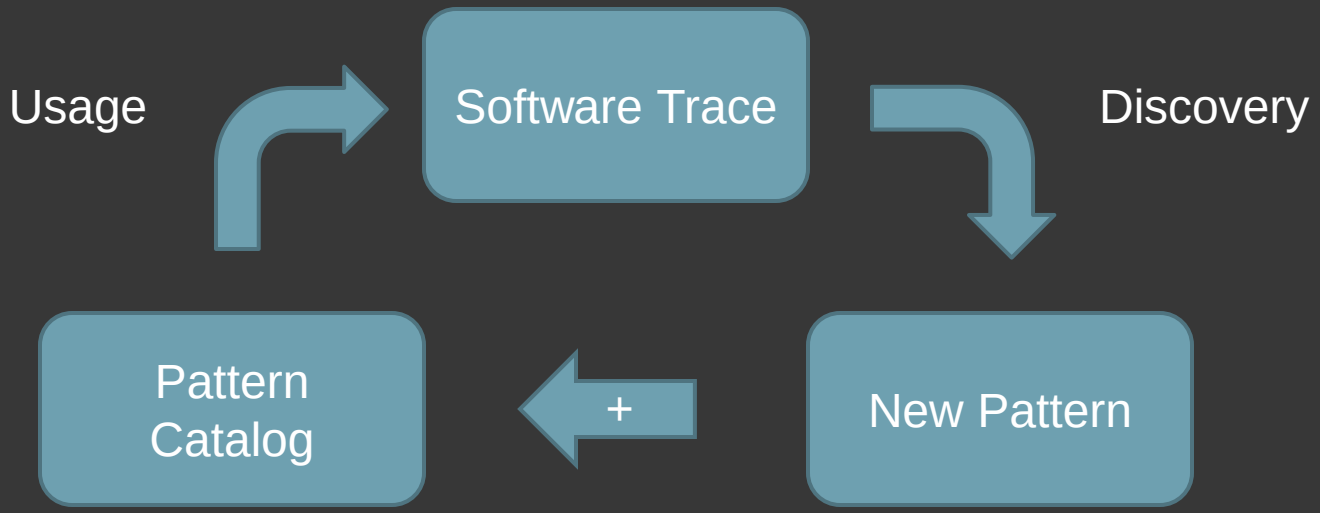


Minimal Trace Graphs



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*

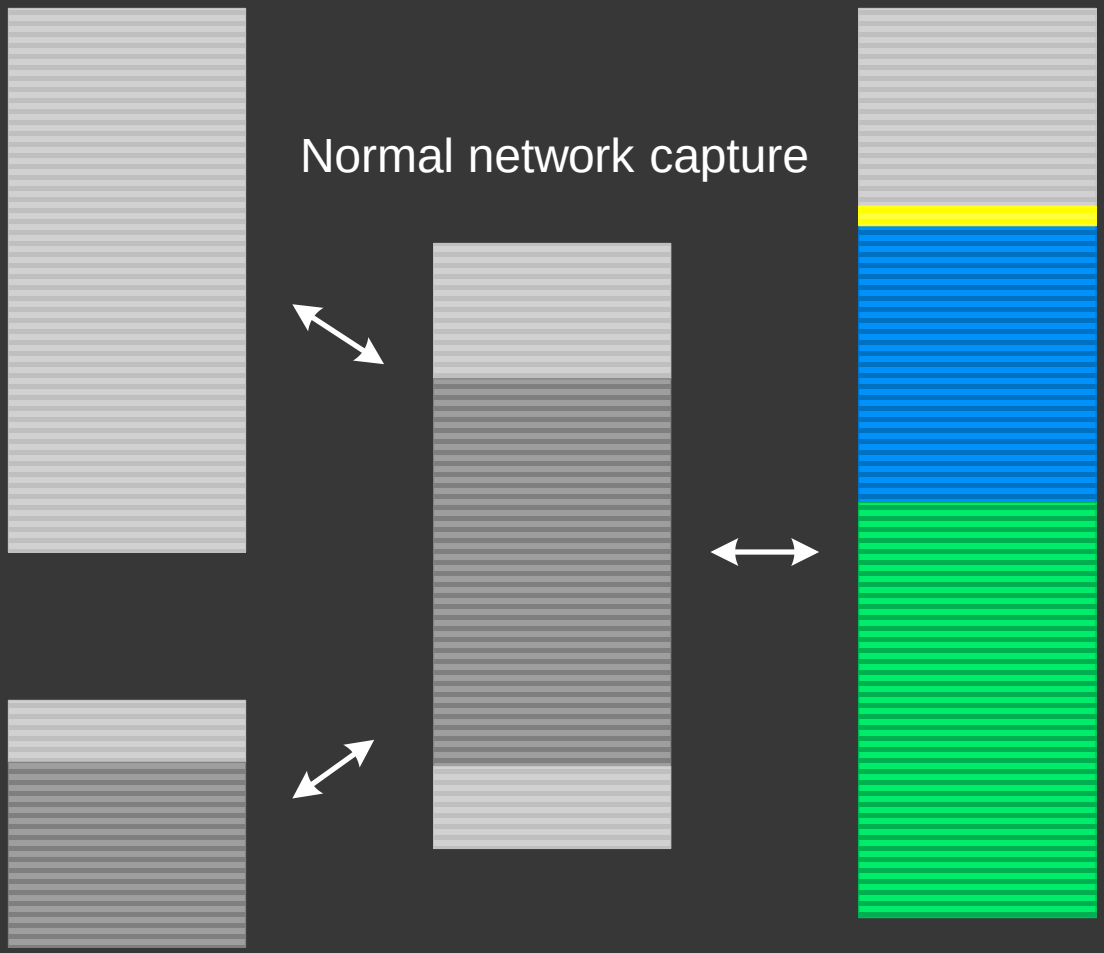
Accelerated Windows Software Trace Analysis

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

Selected Patterns

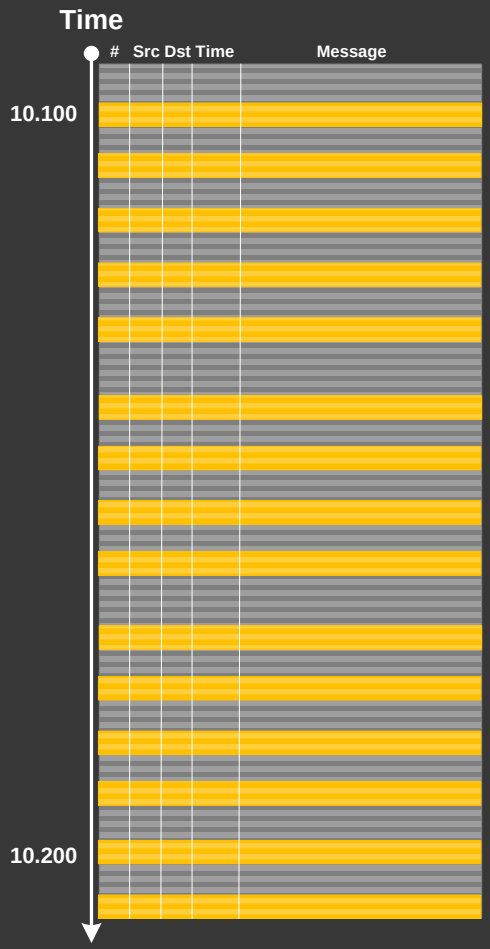
Master Trace

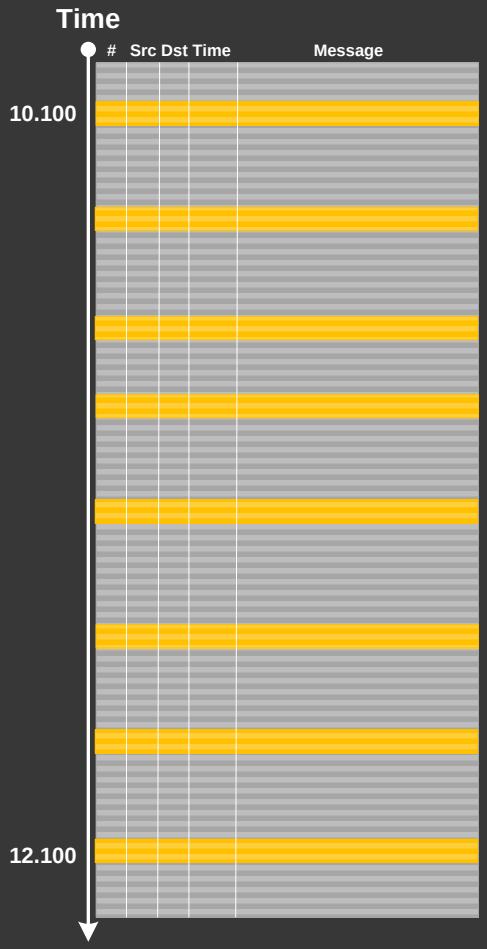
Pattern Category
Trace Set



Message Current

Pattern Category
Trace as a Whole



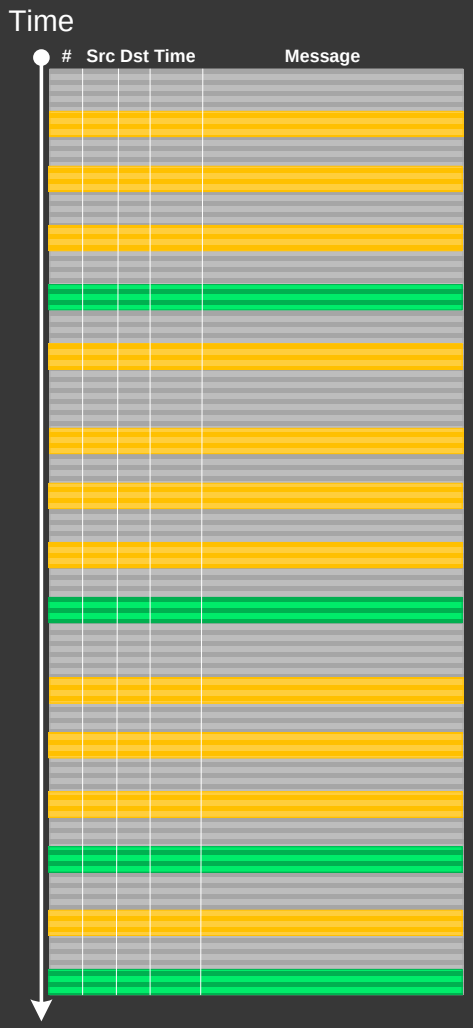


$J_1 > J_2$

Packets/s

Message Density

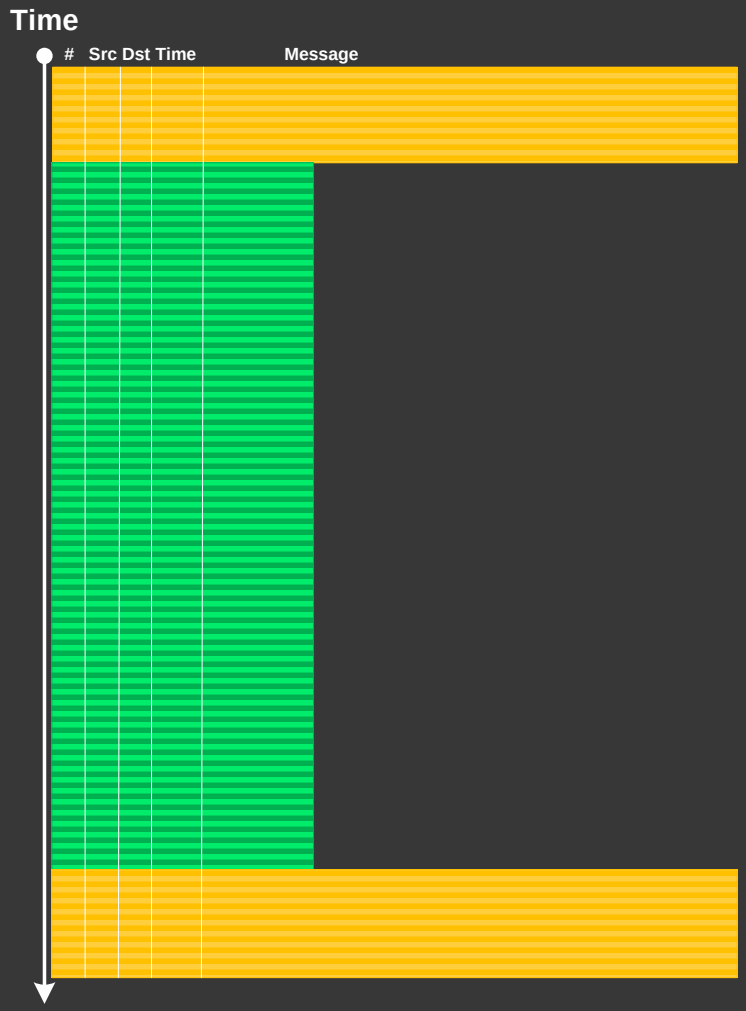
Pattern Category
Trace as a Whole



$D_1 > D_2$

Characteristic Block

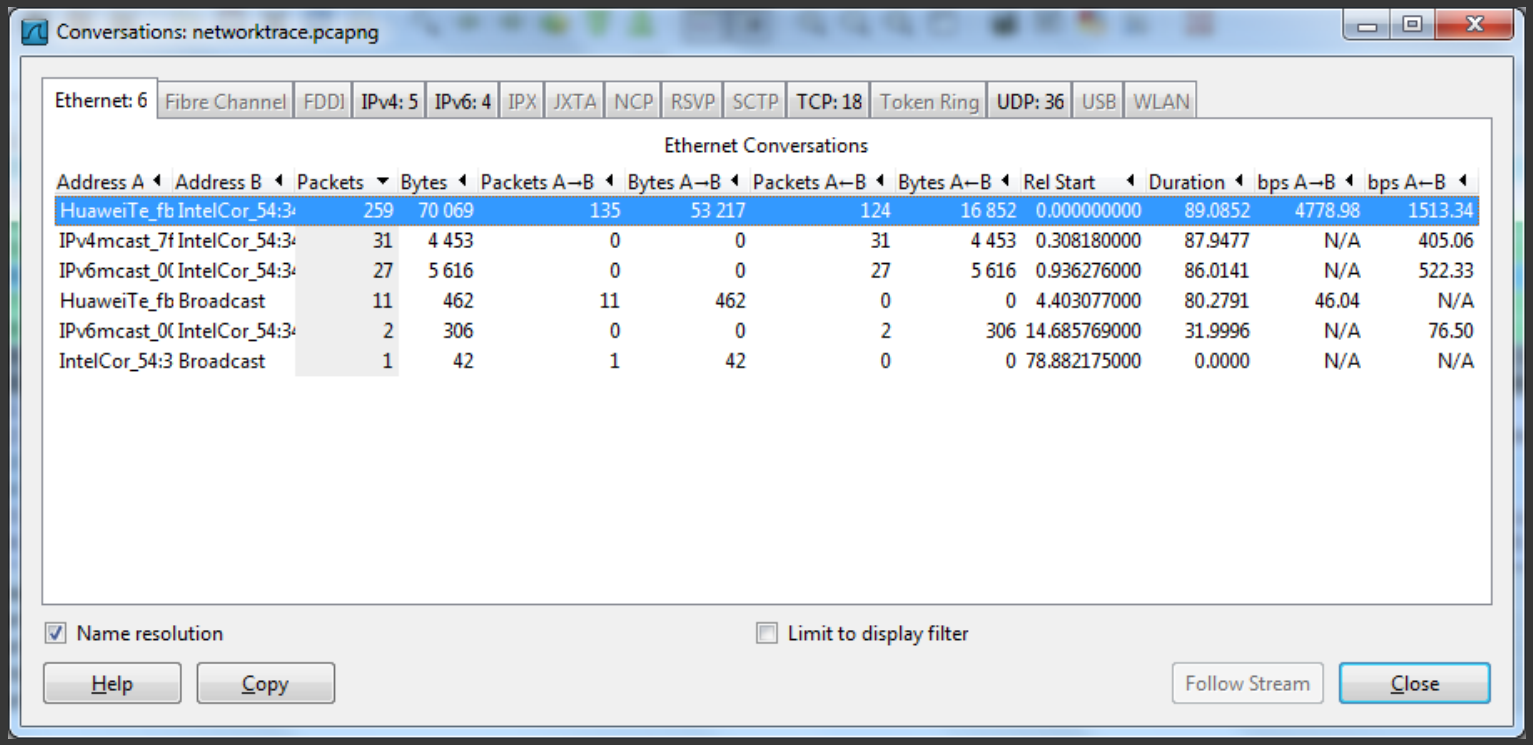
Pattern Category
Large Scale



$D_1 < D_2$

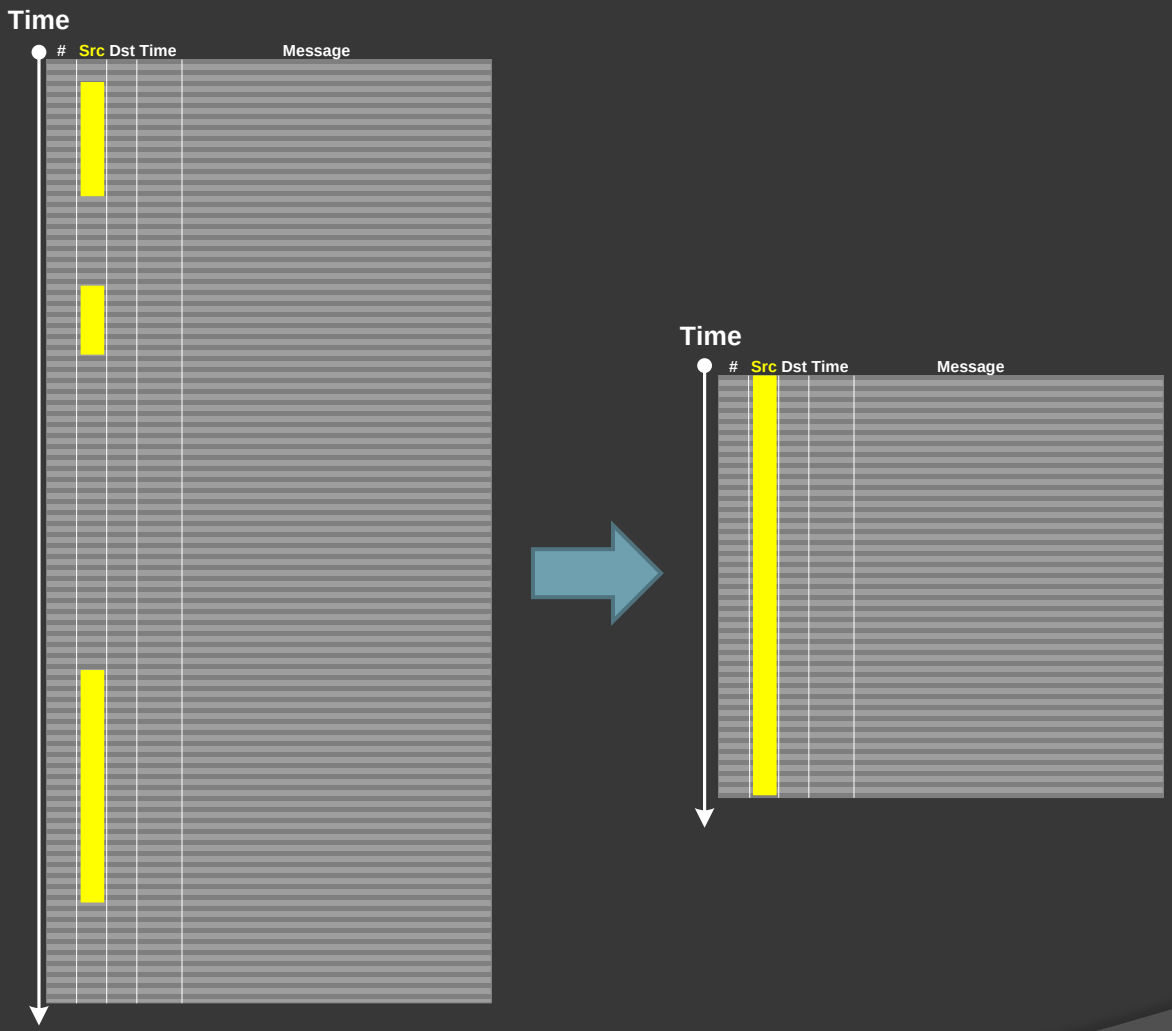
$L_1 > L_2$

Example



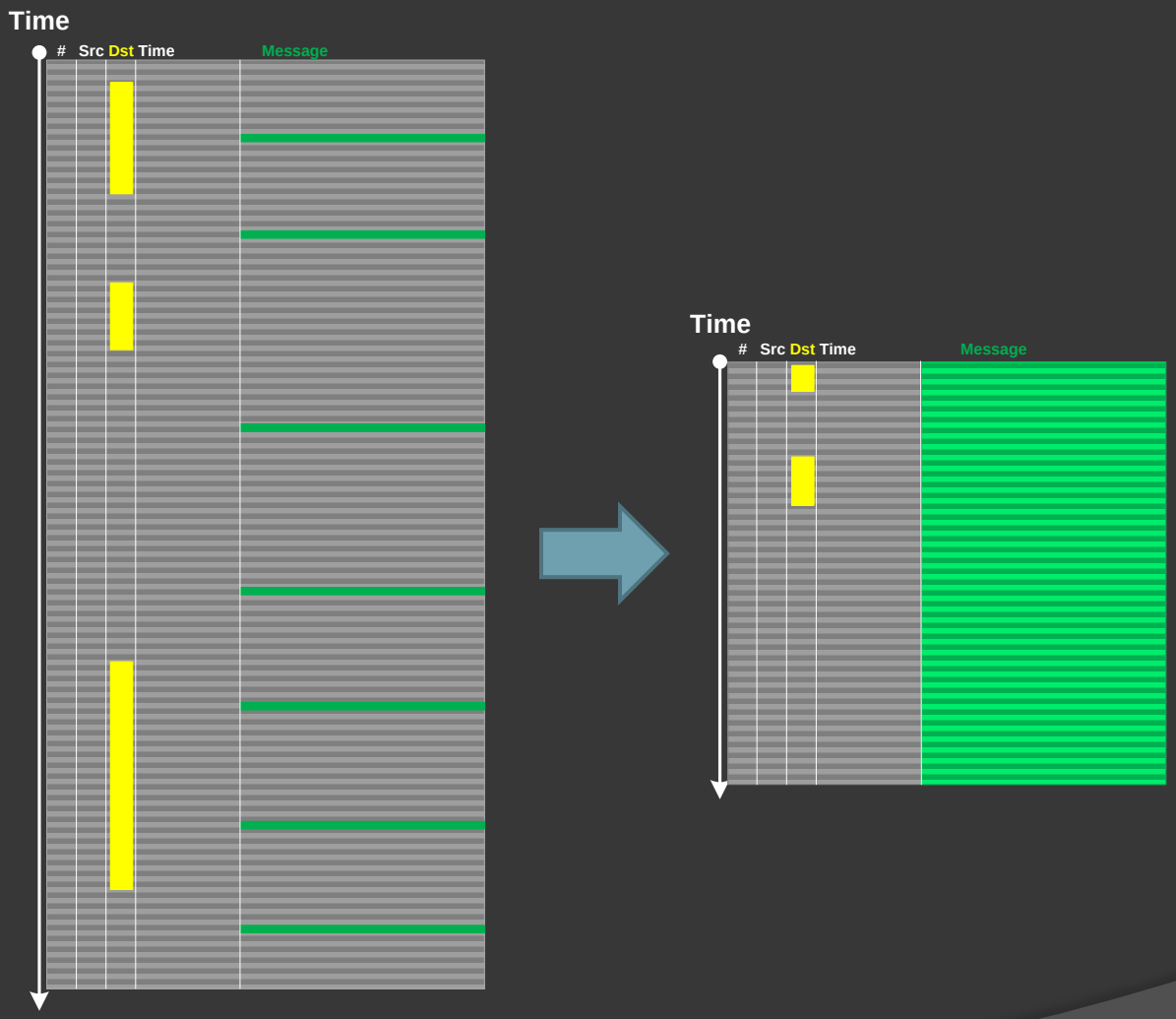
Thread of Activity

Pattern Category
Activity



Adjoint Thread

Pattern Category
Activity

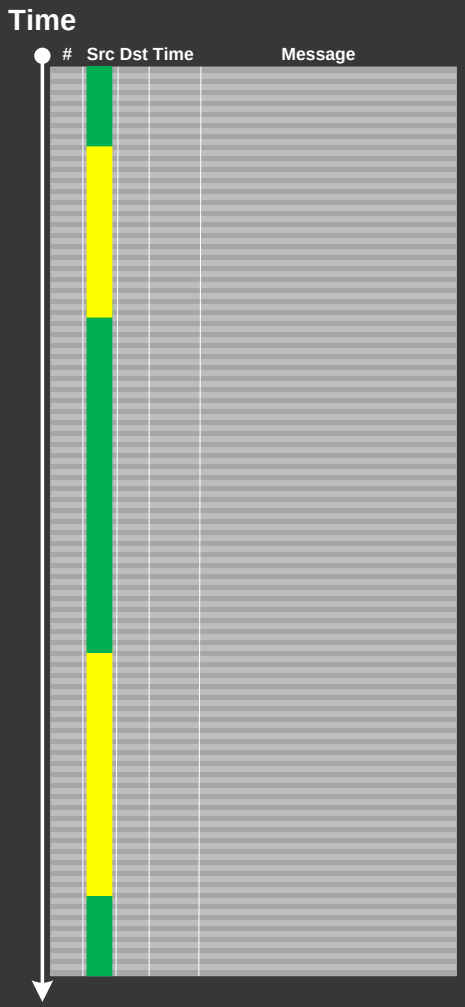


Filtered by:

- Source
- Destination
- Protocol
- Message
- Expression

No Activity

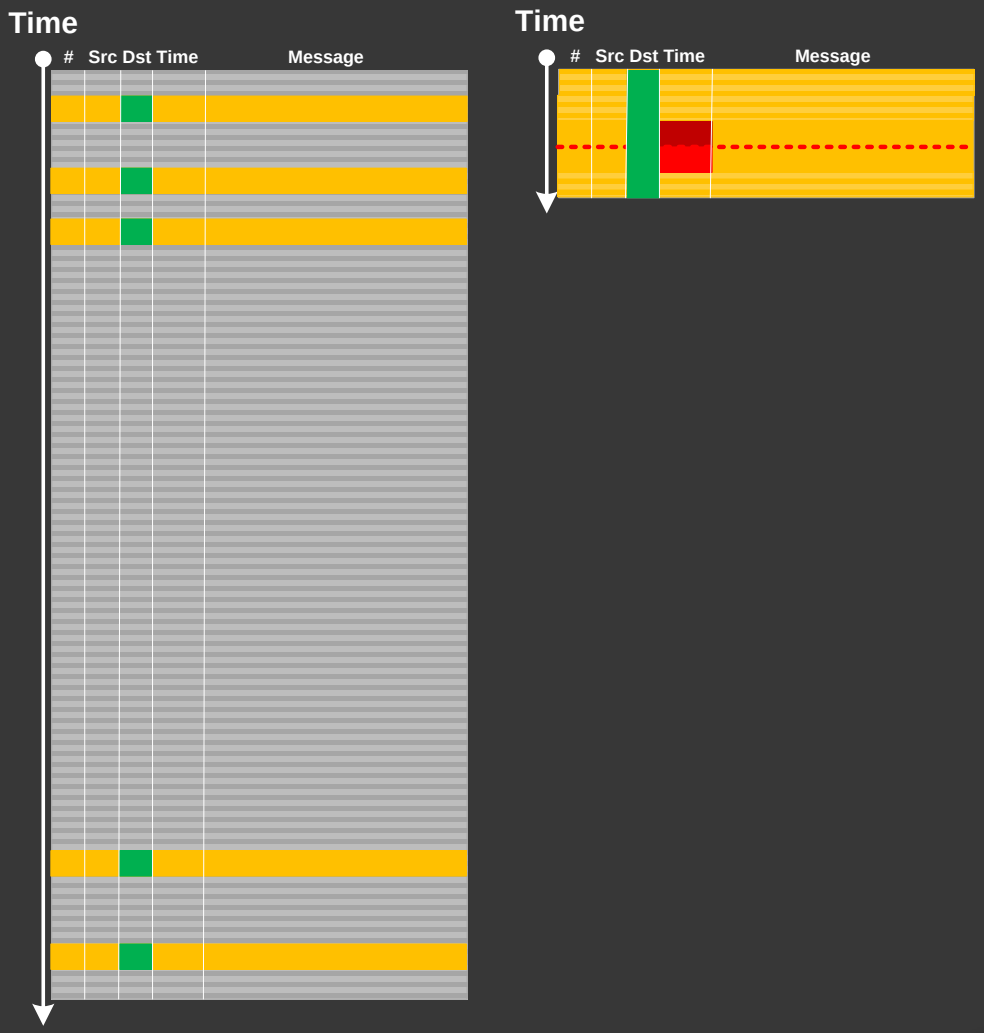
Pattern Category
Activity



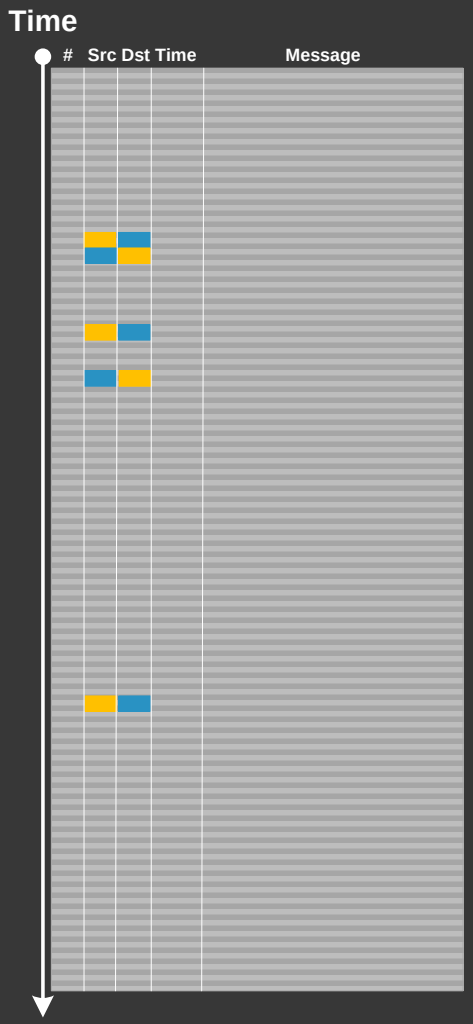
We messages from other servers but only see our own traffic

Discontinuity

Pattern Category
Activity



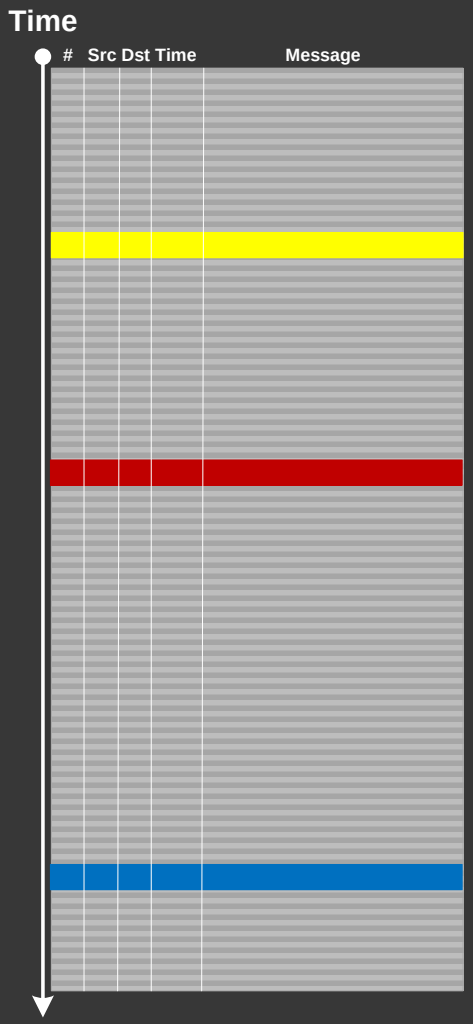
Dialog



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 [-]
```

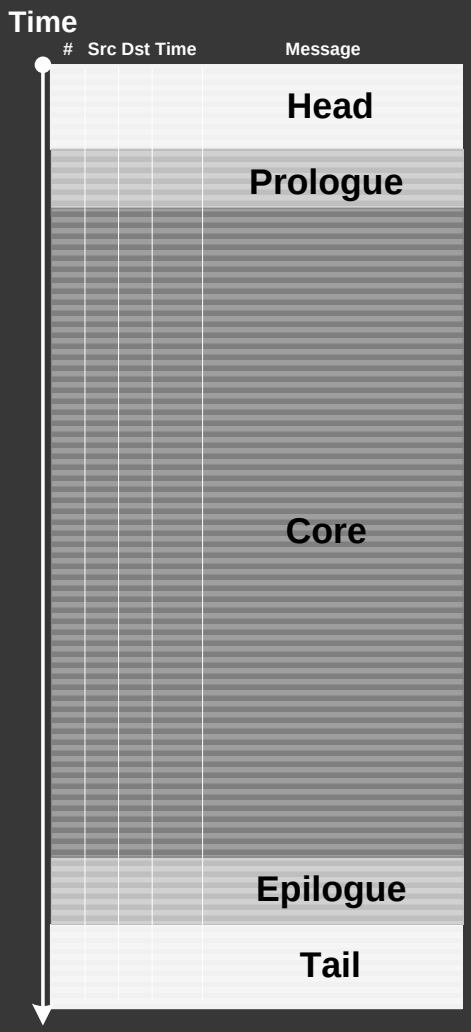
Marked Packets feature in Wireshark

`[+]` 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

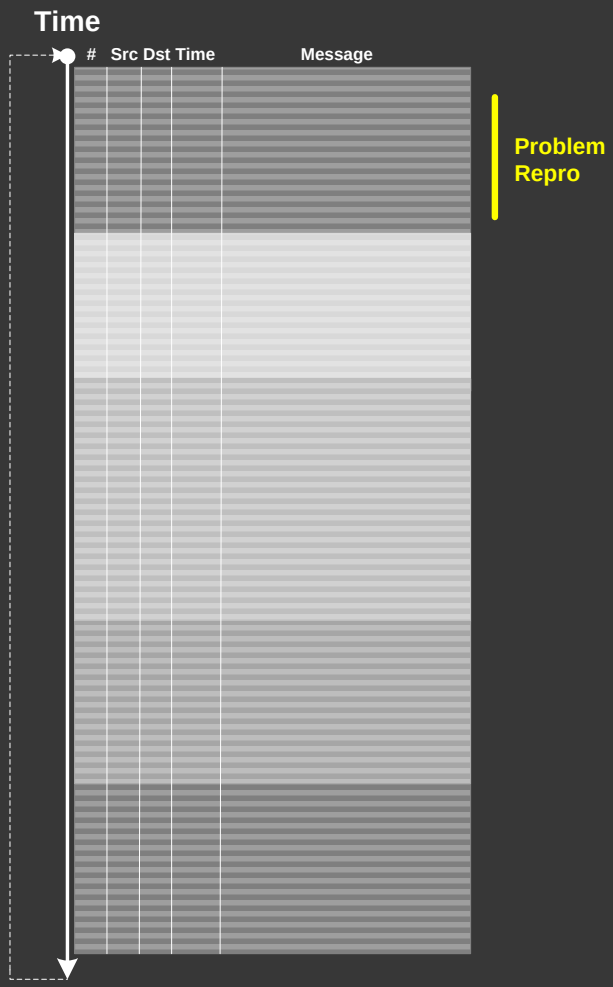
Pattern Category
Trace Set

- Several packet sniffers at once
- Internal and external views

Process Monitor log + network trace

Circular Trace

Pattern Category
Trace as a Whole



Split Trace

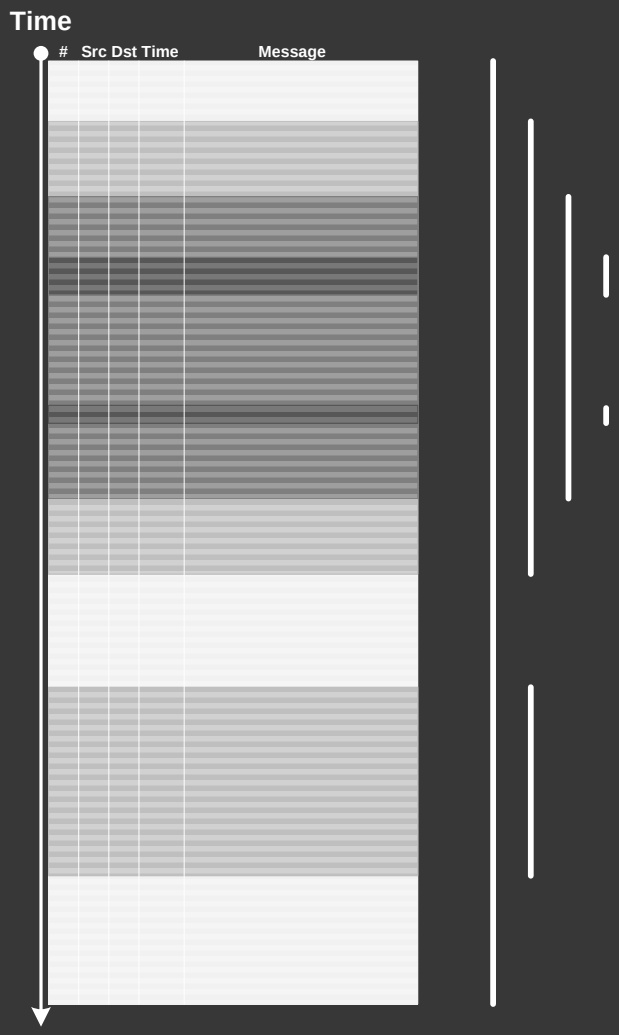
Pattern Category
Trace Set

Paratext

Info column in Wireshark

Frames

Pattern Category
Large Scale

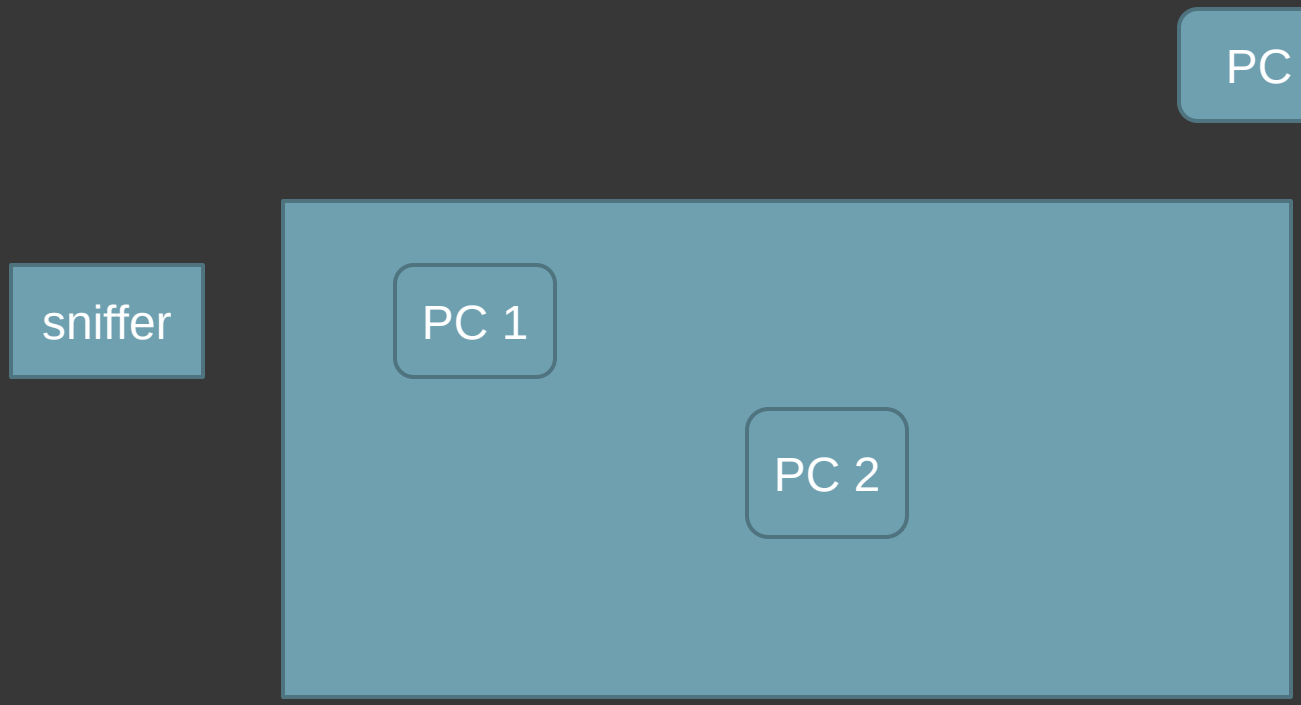


OSI, TCP/IP Layers

Visibility Limit

Pattern Category
Trace as a Whole

Visibility window for sniffing



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!

Facebook LinkedIn Twitter