Fun with Traces Chapter 2

Stuart Kendrick, *Allen Institute for Brain Science*

Description

In this hands-on class, we review real-world case studies, broadly reviewing the environment before narrowing our focus to the packet traces taken during the actual analysis. We oscillate between coming together as a class and reviewing larger lessons and working individually practicing specific techniques. We use Wireshark as a lens through which we deepen our expertise in client/server protocols, expand our understanding of how IT systems interact with one another, and practice using particular Wireshark features.

During the class, we map what we uncover to larger Design Patterns in operating system behavior and misbehavior, trouble-shooting, and our own cognitive biases which lead us astray. We review diagramming techniques in support of trouble-shooting, practice refining Problem Statements, and move to the white board as needed to better understand computing concepts of various flavors. Depending on the class infrastructure (typically a shared network of hubs feeding everyone's laptop with a local NFS/SMB/Web server as a test bed plus a 'network nightmare' box), we practice capturing and analyzing sample transactions together: ARP, DHCP, HTTP downloading a home page, SMB Negotiation, others, as needed according to the flow of questions in the class. Have a trace from your environment which you would like help analyzing? Send me the trace, an environmental description, and a network map prior to class, and I'll consider it for inclusion.

Specific Wireshark techniques will include guidelines for selecting which columns and filters to deploy for which flavor of problem, the use of Profiles in organizing column and filter choices, and tools for analyzing IP, TCP, SMB, and NFS issues. In this class, I assume several years of light exposure to Wireshark (e.g. you found the homework easy).

Review the deck and perform your homework prior to attending class.

The course material includes real-world packet traces (lightly sanitized) and diagrams. BYOL (Bring Your Own Laptop) for a day of engaging your brain and delighting in the pleasure of puzzle solving.

Who should attend

Sys admins, network engineers, database administrators, and application specialists wanting to practice trouble-shooting using packet analysis.

Take back to work

Practice analyzing real-world traces and practice using the instructor’s Profile library.