Troubleshooting

Complex IT systems require that tools exist to be able to troubleshoot them.

Businesses are dependant on these systems

Unknown factors can cause IT systems to break.

Tools are needed to identify and resolve these issues.

Gather and evaluate info

Guess - We need to start someplace, it’s an educated guess.

Talk to users, business analysts, other tech guys

After a guess, collect evidence

Logs

Wireshark

If evidence supports guess, create a plan and test it.

The troubleshooting process is iterative and imprecise.

If a guess isn’t supported, we revise our guess

Plans

Should attempt to be as least invasive as possible.

Derailing logic

Broken systems lead to anger, frustration, and illogical thinking.

Users may blame and attack you

Solve the issue, don’t worry about being blamed.

Managers may threaten you with penalties, “heads may roll”

Co-workers may bring their egos in and attempt to butt their nose in, trying to be heroes.

Don’t be your own worst enemy.

Be open-minded

You can make mistakes, own that possibility, be aware of your shortcomings as a human being

Protocol operation knowledge

Knowledge enables educated guesses.

You must understand the underlying protocols in order to troubleshoot effectively

Knowing protocols helps you use tools and be a hero, but it also may alienate others.

Quality Wireshark troubleshooting

Understand protocol operation

Understand diagnostic utility operation

Interpret wireshark output

Use information to support your guess

Protocol hierarchy

OSI model

Application layer

Transport layer

Network layer

Data link layer

Physical layer

Understanding how protocols build on each other can be helpful when troubleshooting.

ICMP

A weird exception in that it is a protocol that doesn’t make use of the transport layer.

Terms

Troubleshooting

A logical, systematic search for the source of a problem in order to solve it and make the system operational again.