



Forensics for Real Time Computing

Firms IT organizations cannot become real time in practice or reality – without instituting a systematic discipline to decomposing problems within their IT infrastructure. In our experience, we found that by leveraging a forensic sciences approach to cause and effect recreation or identification can rapidly improve IT service delivery and quality of experience.

Below overviews an IT based

Forensic (f-r-n-s-k, -z-k) adj. - Relating to the use of science or technology in the investigation and establishment of facts.

Methodology (m-th-d-l-j) n. - A body of practices, procedures, and rules used by those who work in a discipline or engage in an inquiry; a set of working methods.

Source American Heritage® Dictionary of the English Language, Fourth Edition

In the context of complex IT systems, Forensic Methodology is the process of systematically investigating a system to understand and document it in terms of its business functionality.

Complicated IT systems are generally poorly documented or understood because the amount of information needed to describe a system is larger than most can summarize without losing important details. (The classic problem: "Can't see the forest for the trees") Even the system's designer may be at a loss to describe the system in the context of its business function. Because of the complex and unwieldy nature of this information, organizations must create a discipline to rapidly identify relevant factual information about a system and document/communicate it.

There are three major contexts when Forensic Methodology makes sense to do:

- Documentation
- Diagnostics
- Prognostics

Documentation

Many systems are poorly documented, which can cause a number of problems for the operations team that is responsible for its upkeep or the development team looking to modify the system. The execution of the Forensic Methodology can quickly and accurately create a set of 'living' documentation which describes the system. As the system evolves, problems are resolved, or on-going concerns are tracked, there is a clear and concise way to keep the documentation up to date.

The generated documentation is hierarchically organized so that it can communicate to a broad audience, allowing the consumer to delve into the details up to their comfort level. This allows everyone from a business owner to the system architects and developers to work off the same information with a common understanding.

This context of the methodology needs to employ technology that can automatically discover, document and map application and system component dependencies. Moreover, the tooling must be able to fingerprint the infrastructure and triage any delta's of change that can quickly help isolate root cause and return service levels to norm.





Diagnostics

When a production problem occurs, the infrastructure operation and application support teams must be able to quickly diagnose the problem and take corrective action. The Forensic Methodology and the documentation it generates give these teams the ability to evaluate the system holistically. Its systemic approach makes such that the teams aren't myopic in their diagnostic evaluation.

The results of using the Forensic Methodology for diagnostic purposes is root cause resolution of performance or service delivery problems, especially useful when the faults are the combination of a number of technical or process problems.

The diagnostics context of forensic methodology needs to employ technology that tracks the user transactions as they actually are occurring in real time, so that rapid identification of the problem can be found. The data from the tooling both visual and in report form can enable accurate and rapid forensic "cause and effect" of where performance or service delivery is breaking down.

Prognostics

Prognostics, an extension of the diagnostic model in which predictive algorithms are used to diagnose failures before they occur, is the most undervalued aspect of the diagnostic process. Using the Forensic Methodology one can understand which aspects of a system are important to profile. By watching the growth rates of these targeted areas can eliminate many problems before they materialize in the production environment. Trending, the process of watching the usage of the limited resource pieces of a system over time, can predict when a resource constraint will be superseded. Proactive action resolves these issues before they have a production impact.

This context of forensic analysis needs to leverage "self-learning" technology that can analyze system events in real time and provide intuitive intelligence to proactively control problem and incident management.

Posted by Tony Bishop on April 21, 2008 (http://weblog.infoworld.com/real-time-enterprise/archives/2008/04/forensics_for_r.html?source=rss)

