FORENSIC IT

FORENSIC IT TRAINING SERIES / FREE SAMPLE

Diagnostic Tools Quick Reference

Before you run a tool

Record what failed, when it started, who is affected, and what changed. Save evidence in the case folder and handle dumps and traces as sensitive.

WHAT YOU SEE	WHERE TO LOOK FIRST
App hangs with low CPU	Check the process status in Task Manager. For .NET, a dotnet-stack report can show what its threads were doing.
App crashes and disappears	Check Reliability Monitor and the Application event log. Look for events such as 1000 or 1026 around the crash time.
One process uses high CPU	In Process Explorer, open the process Threads tab and sort by CPU to see which threads are doing the work.
Memory keeps growing	Track the process's Commit size over time. A trend gives you more context than a single reading.
A service won't connect	Use Test-NetConnection with the host and port to check whether the TCP connection succeeds.

Property of Forensic IT

Go deeper with the 5th edition

Diagnostic Tools for IT Professionals covers which evidence to collect and which tools to use to analyze it.

Adapted from the Diagnostic Tools Quick-Reference Card in Diagnostic Tools for IT Professionals, 5th Edition.