GCN
GOVERNMENT COMPUTER NEWS

Special Report | ‘Live’ forensics is the future for law enforcement

07/31/06
By Patience Wait,

Until recently, users of computer forensics were concerned primarily with post-mortem analysis of digital media, looking for evidence of past actions.

But forensics is going “live.” The term might sound like an oxymoron, but in the post-Sept. 11 world, with intelligence and counterintelligence agencies trying to spot trouble before it happens, collecting forensic evidence in real time can boost efforts to protect citizens.

“Post-mortem digital investigations—pull the plug, image-the-drives forensics—are almost obsolete in today’s enterprise setting,” said Chet Hosmer, chief executive officer and chief scientist of WetStone Technologies Inc. of Cortland, N.Y.

“As terabyte drives, encrypted file systems, gigabyte removable memory sticks and memory-resident root kits arrive on the scene, our only chance to collect valuable forensic evidence is through methods of live, on-the-wire forensics,” he said.

Collecting possible evidence in real time, while desktop computers and servers are running, could provide the opportunity to build criminal cases while creating a window to prevent illegal acts as well, from distribution of child pornography to thwarting terrorist plots, Hosmer said. It also can make it much easier to identify geographically dispersed groups of people that are working in concert—truly connecting the dots.

Because of this, the shift toward live forensics is gaining momentum in government as well as the private sector. The Defense Cyber Crime Center is performing more and more live forensics analyses, according to Edmund Kong, director of engineering for the Defense Cyber Crime Institute, one of DC3’s divisions. DCCI has developed a tool of its own for live exams, he added.

DC3 provides some support for live network investigations, usually for other military agencies such as the Naval Criminal Investigative Service or Army Criminal Investigative Division, via its Defense Criminal Forensics Laboratory.

And DC3’s training division offers courses in conducting live network investigations, said Steven Shirley, the center’s executive director.

Whether preventing crimes this way is actually feasible, a live forensics approach can produce a host of useful information that help build a case, Hosmer said.

“Running processes, recently visited chat rooms and logs, recent e-mail messages, forbidden Web site visits and forms—those may be the only clues we ever get in cases of child abductions, corporate or government espionage, copying proprietary data onto flash drives or DVD-writable media, numerous policy violations and insider trading,” Hosmer said.