



EEE IN ACTION: REAL-WORLD SCENARIOS

How is EnCase Enterprise Edition Being Used?

KEY HIGHLIGHTS:

- Remote Investigation of Insider Fraud
- Government Inter-Continental Response
- Examination of a Live Mission-Critical Server
- Enterprise-Wide Investigation of Illegal Activities
- Financial Fraud Investigation

EnCase Enterprise Edition is revolutionizing the practice of computer forensics and incident response by providing the means for immediate and thorough forensic analysis of compromised servers and workstations anywhere on a wide area network.

EnCase Enterprise Edition is revolutionizing the practice of computer forensics and incident response by providing the means for immediate and thorough forensic analysis of compromised servers and workstations anywhere on a wide area network. Below are five groundbreaking real-world examples of customers using EnCase Enterprise Edition to conduct critical investigations that would otherwise be impossible or highly impracticable.

Remote Investigation of Insider Fraud

An examiner at a major financial institution in New York recently used EnCase Enterprise Edition to successfully preview two drives in Asia connected to the company wide area network. The drives were previewed in less than an hour after management determined that the investigation was necessary and that time was of the essence. The preview process revealed that one of the drives contained highly relevant information, and the drive was promptly acquired for further forensic analysis in New York.

The entire acquisition occurred without the knowledge of anyone in Asia and without disrupting operations. The investigation also revealed that the other drive did not contain relevant evidence. EnCase Enterprise Edition essentially enabled an investigation that otherwise would likely not have taken place. An investigation involving international travel, flyaway kits, and stand-alone computer forensics utilities would have delayed the process by several days, if not weeks, thus resulting in altered data or loss of evidence. An on-site response process may have compromised the

investigation in this case or, at a minimum, impacted business and morale due to the very non-clandestine physical presence of investigators.

Government Inter-Continental Response
A large government agency used EnCase Enterprise Edition and a high-speed network connection to image a drive on its WAN located approximately 10,000 miles (16,000 km) away. This process enabled a rapid incident response and the capturing of live data. Without EnCase Enterprise Edition the response would have been delayed by several days or may not have occurred.

Examination of a Live Mission-Critical Server

Law enforcement investigators arrived at a company site to collect computer evidence from a server. The company was not the perpetrator of the investigated crime, but apparently did possess important evidence that resided on a mission-critical server that could not be taken off-line. The examiners successfully used EnCase Enterprise Edition to preview the server and collect key evidence, without disrupting operations. Without EnCase Enterprise Edition investigators would have either walked away from the scene empty-handed or performed a highly invasive and incomplete investigation by making logical file copies of active data.

Enterprise-Wide Investigation of Illegal Activities

The CTO of a large beverage company suspected something was amiss when he noticed a significant amount of traffic traveling through the company network. He deduced that his trusted

staff of system administrators might have been misusing their access privileges and the network servers for some unknown purpose.

An outside firm was contracted to perform a confidential after-hours investigation of the network and the system administrators. Using EnCase Enterprise Edition, network logs and the files on 60 network machines were examined. The investigators determined that large amounts of pornography were traveling through the network. It was discovered that unauthorized web servers containing more than 20 gigabytes of pornographic material had been set up across the network. Using EnCase Enterprise Edition, they were able to determine which users had access privileges and had logged onto the suspected machines. An unexpected result of the investigation revealed additional rogue servers placed above ceiling tiles, communicating with the network via multiple wireless access points. In a weekend, enough evidence was gathered to determine that the entire network administration team had been part of a sophisticated porn operation. The whole team was immediately terminated.

Using EnCase Enterprise Edition, the entire investigation was performed in only 2 days; 10 days fewer than expected. The result was significant timesaving and reduced investigative fees. In addition, the company had sufficient evidence to protect itself from a wrongful termination suit. The porn operation was shut down and the corporate bandwidth returned to normal, and the company prevented a huge possible liability.

Financial Fraud Investigation

A large multinational corporation was accused of questionable financial reporting by the SEC, resulting in an investigation by a major independent consulting company. The goal of the investigation was to determine if the Chief Financial Officer had ordered his staff to alter or destroy transactions to help the company's financial position appear more favorable. EnCase Enterprise Edition was used to perform an exhaustive search of all computer records within the company's large finance division. It was soon discovered that management ordered staff to destroy key documents. However, certain staff members did not fully

comply with the order, making the files easily recoverable. In addition, on some systems, EnCase Enterprise Edition was able to recover incriminating documents that had been deleted. The entire process occurred without affecting business operations or productivity. Eventually, enough information was recovered to reconstruct the actual events and prove that numerous high-level managers had schemed to alter the records of the company. The suspected staff members were terminated and criminal charges were brought against them.



SC Magazine Annual Award Best Computer Forensics Solution

EnCase Enterprise Edition (EEE) received SC Magazine's Reader's Choice award for "Best Computer Forensics" solution. This is the second year in a row that EEE has been honored by SC Magazine. This year, EEE was recognized by actual product users, which include law enforcement through military intelligence, government agencies and large corporations including banking, manufacturing and telecommunications and airlines. Used in enterprise investigations around the world, EEE is accepted day in and day out by courts. The SC Magazine award validates that EnCase is the trusted forensics tool of choice.

About Guidance Software

Guidance Software is the leader in computer forensics and incident response solutions. Founded in 1997 and headquartered in Pasadena, Calif., Guidance Software has offices and training facilities in California, Virginia, New York and the United Kingdom. More than 13,000 corporate and government investigators depend on EnCase software, while more than 3,500 investigators attend Guidance Software's forensic methodology training annually. Accepted by numerous courts and honored with eWEEK's Excellence Award and SC Magazine's Annual Award, EnCase software is considered the standard forensic tool. For more information, visit Guidance Software's Web site at www.guidancesoftware.com.