



EnCase® Enterprise In Action

EnCase Enterprise Delivers Proven, Efficient and Cost Effective Remote Digital Investigations

EnCase® Enterprise provides proven remote investigation capabilities to give security professionals, investigators, computer incident response teams and litigation specialists the ability to immediately and thoroughly search, collect, preserve and analyze data from servers and workstations anywhere on a corporate network – without disrupting operations. The case studies that follow are groundbreaking real-world examples of how our customers are using EnCase Enterprise to conduct critical investigations that would otherwise be impossible or highly impracticable.

“As an office of one, **EnCase Enterprise is my capstone forensic tool.** It provides critical force multiplication factor that allows me to keep up with my heavy workload of forensic cases in addition to my normal duties as Information Security Officer.”

*Johnie Sullivan,
Information Security
Officer & Forensic
Investigator, UNLV*

CASE STUDY:

Intellectual Property Theft Investigation

EnCase® Enterprise used to support client's claim of IP theft



Guidance Software Professional Services consultants were hired by a product manufacturer to investigate the **theft of trade secrets**. The company alleged that a former employee removed files containing corporate secrets from their computer systems and then used these secrets to establish a new company, create a competitive product line and market to the same customer base. **Litigation had been ongoing for two years**, which allowed the opposition to continue their business operations and target the suppliers and vendors of our client, **resulting in significant lost revenue.**

The goal of this investigation was to prove that the files the opposition used as the basis for their product line were derived from our client's files. Using EnCase Enterprise as the only tool, **in just six hours our consultants identified the information necessary** to support the client's claims. It showed that the files used by the opposition in their manufacturing process had the identical metadata of the files originally created by our client, and that they had been modified to suit the opposition's plans. The similarities in document format, font selection, file creation dates and document **metadata proved to be the compelling evidence** our client needed to present their case.

CASE STUDY:

HR Investigation

Investigation team uses EnCase® Enterprise to verify reported allegations



A large financial institution routinely uses EnCase Enterprise to investigate **corporate computer usage policy violations**. EnCase Enterprise is part of a process to discreetly investigate and verify allegations of computer usage policy violations, performance issues and other policy violations. On a case-by-case basis, Human Resources notifies the company's investigation team of reported allegations. Investigators then use EnCase Enterprise to investigate and analyze employee actions, which might include **inappropriate material, email abuse, instant messaging and other non-business related activity.**

EnCase Enterprise **captures evidence, documents its findings and produces reports with supporting evidence** that is then submitted to relevant parties. This information is critical in proving or disproving allegations against employees. The solution not only **provides verifiable support of the allegations**, it enables the employee investigation process to be **discreet and thorough**, while minimizing the potential for any employee ill-will during investigations.

EnCase® Enterprise eliminated travel, overnight operations and radically reduced investigation time

A major utility company had an incident that required the acquisition of hard drives from many machines across its network. Doing it manually, using any other forensic tool, would have taken too much time. Guidance Software's EnCase Enterprise was implemented with a 3-concurrent-connection license, along with 10 extra concurrent connections to allow the company to complete this project. EnCase Enterprise was implemented and hard drives were being acquired within two hours.

- Travel was reduced by 100 percent
- Investigation time reduced by 75 percent per system
- The need for overnight operations was eliminated
- Covert investigations were done during normal business hours
- Sixty hard drives (20 GB average) were acquired in nine days

CASE STUDY:

Corporate Fraud Investigation

Recovery of previously deleted documents in an investigation leads to terminations and criminal charges



A large multinational corporation was **accused of questionable financial reporting** by the Securities and Exchange Commission, resulting in an investigation by a major independent consulting company. The goal of the investigation was to determine if the CFO had ordered his staff to alter or destroy transactions to help the company's financial position appear more favorable. **EnCase® Enterprise was used to perform an exhaustive search of all computer records** within the company's large finance division.

It was soon discovered that management had ordered staff to destroy key documents. However, some employees did not fully comply with the order, making the files easy to recover. The entire **process occurred covertly, without impacting 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.

CASE STUDY:

Internal Investigation

Enterprise-wide investigation reveals unauthorized, illegal activities conducted by company's team of system administrators



The chief technology officer 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 be misusing their access privileges** and the network servers for some unknown purpose.

An outside firm was engaged to perform a confidential after-hours investigation of the network and the system administrators. Using EnCase® Enterprise, network logs and the files on 60 network machines were examined. It was discovered that **unauthorized web servers** containing more than 20 gigabytes of pornographic material had been set up across the network. **EnCase Enterprise determined which users had access privileges** and who had logged onto the suspected machines.

An unexpected result of the **investigation revealed more rogue servers** placed above ceiling tiles, communicating with the network via multiple wireless access points. Every member of the system administration team was immediately terminated. Using EnCase Enterprise, **the entire investigation was performed in only two days** – 10 days fewer than expected – saving the company time and reducing fees paid to investigators. The **company also had sufficient evidence to protect itself** from wrongful termination suits.



www.guidancesoftware.com

Our Customers

Guidance Software's customers are corporations and government agencies in a wide variety of industries, such as financial and insurance services, technology, defense contracting, pharmaceutical, manufacturing and retail. Representative customers include Allstate, Chevron, FBI, Ford, General Electric, Honeywell, NATO, Northrop Grumman, Pfizer, SEC, UnitedHealth Group and Viacom.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to e-discovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 30,000 licensed users of the EnCase technology worldwide, the EnCase® Enterprise platform is used by more than half of the Fortune 100, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from *Law Technology News*, *KMWorld*, *Government Security News*, and *Law Enforcement Technology*.

©2011 Guidance Software, Inc. All Rights Reserved. EnCase and Guidance Software are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners.