



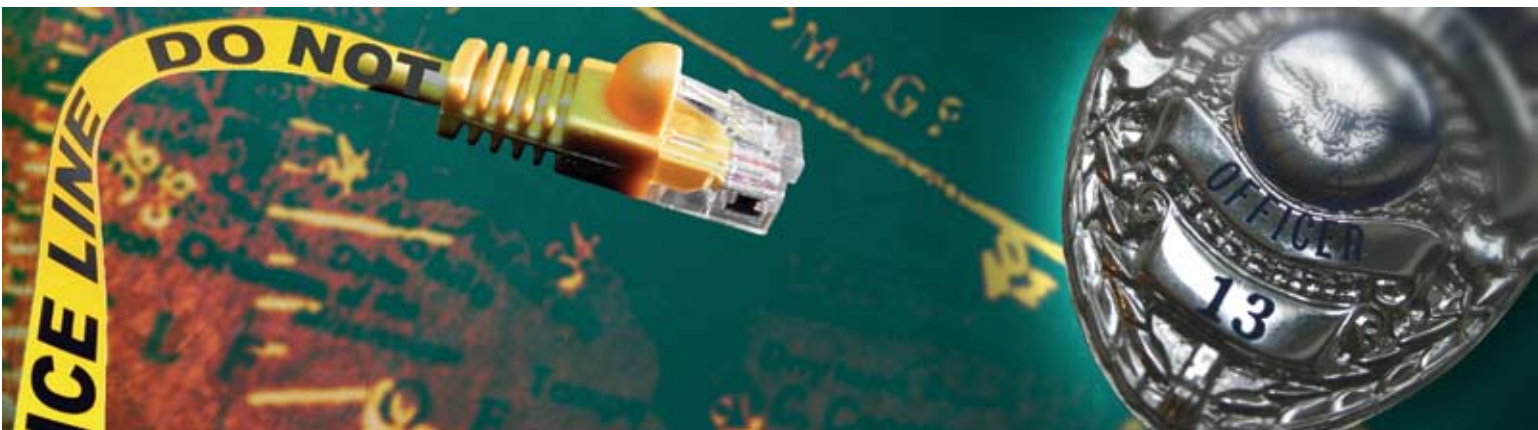
FIM

FIELD INTELLIGENCE MODEL

Credibility. Defensibility. Best Practices.

“With the size of today’s hard drives averaging anywhere from 60 to 80 gigabytes, I just don’t know how you would accurately analyze them in a timely manner with anything other than EnCase® (software)”

-Roy Hector-Computer Forensics Examiner
Austin Police Department, Austin Texas



Computer forensics investigations can be extremely disruptive. Seizing computers in cases of fraud, harassment, theft and criminal misconduct interrupt business operations which can lead to evidence loss – and expose your agency to legal and unnecessary liability. You need a solution that can search hard drives without bringing down servers or computers, tipping off suspects or compromising equipment.

When conducting investigations over a network, only one truly trusted tool can handle it all: EnCase Field Intelligence Model. It gives investigators a highly mobile solution to investigate, and analyze data from machines – all from a remote laptop or mobile workstation. By allowing investigators to complete an entire investigation from acquisition through analysis with one tool, you save the time and cost of learning and using multiple tools.

Start with a fast and effective acquisition

EnCase Field Intelligence Model speeds up and streamlines acquisitions by giving you control over how you acquire data – from the rate you use to capture data, to defining what happens when errors are found on hard drives.

As the size of drives continue to grow, it’s not realistic, effective or even necessary for admissibility in court, to acquire a complete bit stream image of a target drive. All you need to acquire is relevant data and to acquire it in a way that maintains its integrity.

With EnCase logical evidence files you can do just that. This unique capability, available in all EnCase products, lets you acquire only files relevant to your case and all information related to them, including metadata and the location of the data on the target machine.

EnCase creates a self-authenticated bit stream image of the data, which ensures the data doesn't change during acquisition. This means that you can capture and analyze one or many files and preserve them in a format that is defensible in court.

Find and retrieve hidden evidence – covertly

Experienced criminals often go to great lengths to cover their tracks. The challenge is to find hidden data without modifying the file system and jeopardizing the admissibility of the data.

With EnCase Field Intelligence Model, this is not only achievable, it is easy. EnCase Field Intelligence Model peers deeply and safely into the static and volatile memory of a computer to identify and capture all types of hidden information, ranging from files in unallocated space, to hidden processes such as rootkits. Then it delivers all of that data in a simplistic and court-admissible format.

Investigators can understand exactly what occurred or is occurring on a given machine, and catch sophisticated hackers and cybercriminals who routinely use leading-edge technologies to mask their activities.

Improve productivity by using only one tool

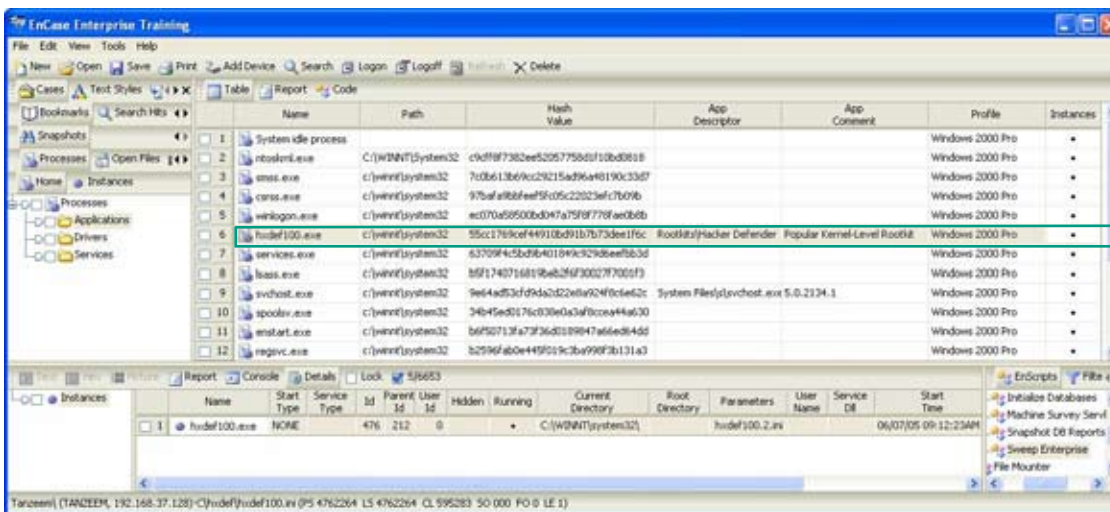
EnCase Field Intelligence Model can search and analyze great volumes of data quickly and easily to maximize your time and improve productivity. Unlike more limited-function tools on the market, it offers full investigative capabilities including the ability to analyze multiple operating systems, RAID configurations, thumb drives, file systems, firewire devices, encrypted volumes and foreign languages – eliminating the need for different tools at each step of your investigation.

It also automates many time-consuming tasks including e-mail analysis, exposing data within compound files, even carving data from unallocated space. And once you have acquired the data, you can easily share evidence files securely with other examiners who use EnCase software.

A name you can depend on

Guidance Software technology has been accepted and validated in courts worldwide, making it the solution by which all others are measured. "EnCase is unsurpassed," according to SC magazine. Take it from the experts who use EnCase because they can't risk inadmissibility of evidence: federal investigation agencies, regulatory agencies, regional forensics labs and international law enforcement agencies.

Using the same technology that has become the de facto standard for forensics investigations, EnCase Field Intelligence Model offers the most defensible solution on the market.



EnCase identifies the executable, path, parameters and the start time of rootkits, such as the Hacker Defender.

EnCase software captures volatile data so you can see hidden processes running on target machines and easily identify compromised machines.

Extend your investigative reach

Virtual File System — Provides immediate access to the internal contents of image files, including active, deleted files, system files, and lost and recovered files. Lets examiners use third-party software to aid their investigations, including password crackers, virus checkers, spyware detectors and steganography checkers.

Physical Disk Emulator — Eliminates the hours-long chore of restoring evidence from one hard drive to another. Also reveals a computer's hard drive, desktop and applications as seen and used by the suspect to provide compelling visual presentations for judges and jurors.

EnCase Decryption Suite — Saves time and increases productivity when tackling file decryption and password recovery for Microsoft EFS (Encrypted file system)



Count on Guidance Software expertise

Founded in 1997, Guidance Software is recognized worldwide as the industry leader in investigative technologies. Its EnCase® solutions provide the foundation for both law enforcement and corporate enterprise investigations that enable corporate, government and law enforcement agencies to conduct effective investigations of all types, respond promptly to eDiscovery requests, and take decisive action in response to external attacks, all while maintaining the forensic integrity of the data. More than 20,000 investigators depend on EnCase software, and more than 5,000 investigators attend Guidance Software's forensic methodology training annually. Validated by numerous courts worldwide, EnCase is also frequently honored with top security awards from eWEEK, SC Magazine, Network Computing and others.

215 North Marengo Avenue, Pasadena, CA 91101 | Ph: 626.229.9191 | Fax: 626.229.9199 | www.guidancesoftware.com