

OpenText EnCase Endpoint Investigator

The most powerful and efficient solution for corporations and government agencies to perform remote, discreet and secure internal investigations without disrupting an employee's productivity or day-to-day operations



Discreet, off-the-network collection capability



Image analysis quickly processes and filters using AI technology



Remote device access across geographies



Leverage credentials to collect from data repositories on-premises and in the cloud

Organizations are now tasked with more types of investigations than ever before; HR issues, compliance violations, regulatory inquiries, IP theft and more. To solve these issues, organizations may need to look deeper in to an employee's activity discreetly and even remotely without sacrificing employee productivity.

OpenText™ EnCase™ Endpoint Investigator equips internal investigators with a highly-effective tool for scanning, searching and collecting data related to any number of internal investigation needs, such as HR performance issues, harassment complaints, compliance violations, whistleblower claims, IT policy violations and potential financial reporting irregularities in a completely discreet and unobtrusive manner.

EnCase Endpoint Investigator eliminates the high costs and significant impact to employee productivity previously associated with internal investigations, replacing it with a highly dynamic, flexible and scalable process for completing investigations within an organization.

Discreet, off-the-network collection capability

Investigators can discreetly search and collect relevant information from endpoints with the help of the EnCase enhanced agent, which collects information based on the search criteria, whether the employee is in the office or working remotely with no network connection.

Broad OS support across various devices

Investigators can investigate on a comprehensive list of operating systems, including Microsoft® Windows®, Linux®, Apple® Mac® and UNIX®. Investigators can acquire from more than 26,000 mobile device profiles and analyze key data including email, text messages, browser artifacts and much more.



"I have about 100 different duties to perform on an annual basis. With EnCase Endpoint Investigator, I'm able to take care of 80 percent of my workload in 48 hours."

Deputy Director
IRM Office and ISSO
U.S. Federal Agency

Remote device access across geographies

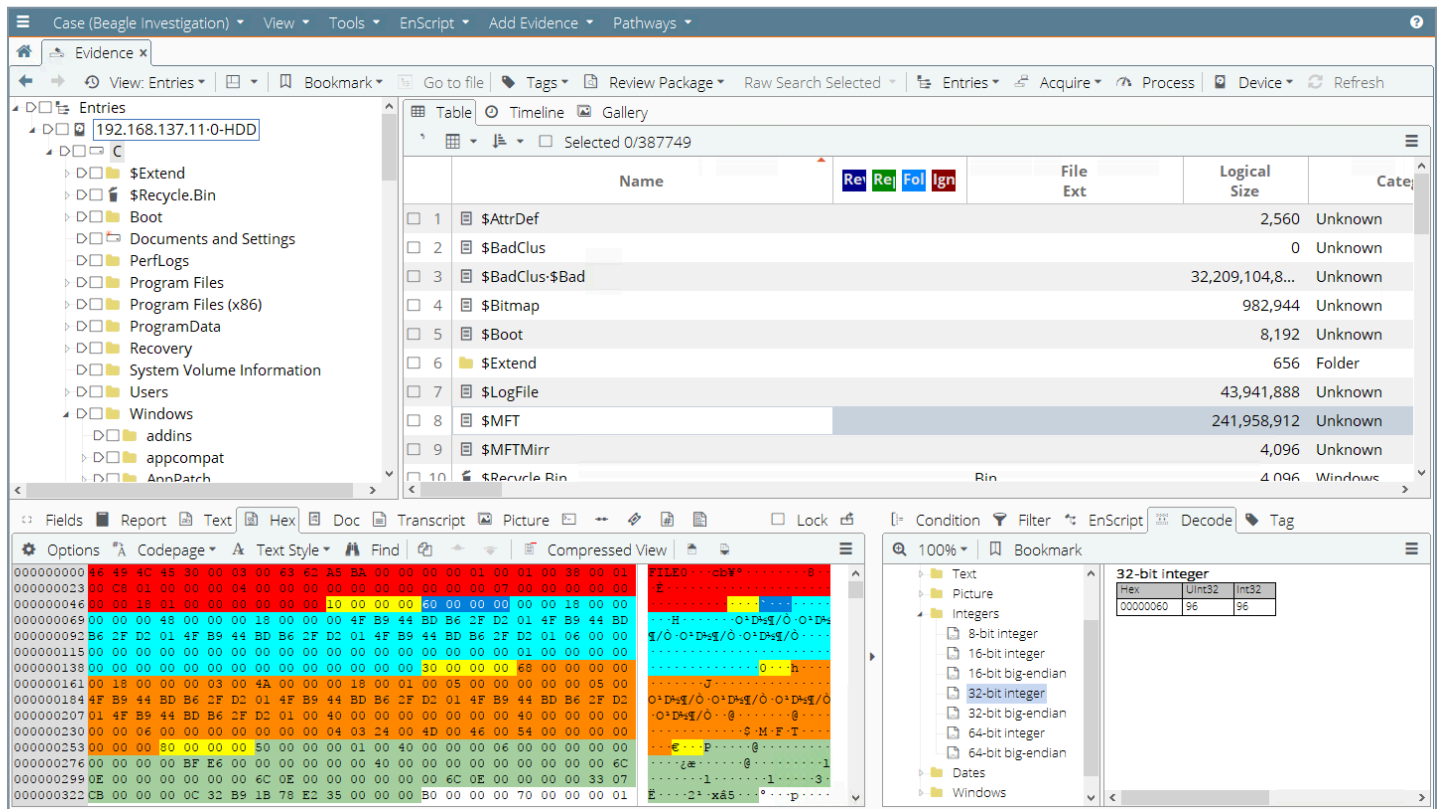
Investigators can remotely and discreetly collect and analyze data on any endpoint device no matter where it is geographically located.

Forensically sound collection

Evidence collected from remote machines is stored in the EnCase Evidence File format, which has been accepted and proven in courts worldwide as forensically sound.

OpenText offers a wide variety of professional training programs and certifications to help develop expertise in EnCase software and forensic security.

EnCase Endpoint Investigator provides investigators with seamless, remote access to laptops, desktops and servers ensuring that all investigation-relevant data is discreetly searched and collected in a forensically sound manner. With a five-star review from SC Magazine, and a proven track record of court acceptance, EnCase Endpoint Investigator outshines its competitors.




EnCase Endpoint Investigator enables investigators to perform remote, private and secure internal investigations in a forensically sound manner.

OpenText EnCase Endpoint Investigator features

Triage capability	Triage remote systems to determine if any relevant information exists on the machine before performing a collection
Whole disk data investigation	Examine the entire data content stored on the target machine hard drive including encrypted data
Multiple systems search capability	Perform search and collection across multiple machines at a time, improving productivity and decreasing the time to investigation closure
Accelerated investigations	Spend less time analyzing data and more time focusing on completing the investigation, thanks to automatic processing and indexing functions
Apple T2 Security Bypass	Acquire machines equipped with Apple T2 Security chips without additional hardware, drive partitions, or hassle. And if the user is logged in, no credentials are required
Threat hunting	In seconds, use Sweep Enterprise to scan ranges of endpoints to capture running processes, OS artifacts, network activity, user activity, targeted files, and more. Filter, bookmark, and report for escalation and response.

 [Learn more](#)

 [See the demo](#)

 [Keep up to date](#)

 [OpenText LinkedIn](#)

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- [OpenText CEO Mark Barrenechea's blog](#)
- opentext.com/security