




# OpenText EnCase Forensic


Forensic data acquisition, triage, and analysis for law enforcement, agencies, and corporations



 **Leverage new artifact-first workflows** and automation with Artifacts Explorer

 **Court-validated chain of custody:** acquisition, investigation, reporting

 **Pull data from any device**

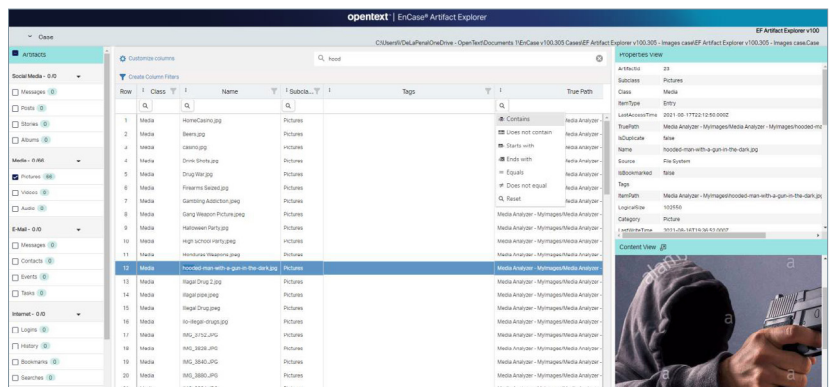
 **Speed investigations** with AI imagery categorization

**Digital investigations require triaging, assessing, and collating evidence collected from a vast array of sources while maintaining strict security and evidential integrity. Investigators must be able to work quickly and effectively to produce defensible, intuitive, and credible reports. With vital evidence spread across disparate devices, examiners risk complex, prolonged, or inefficient workloads impacting their ability to deliver positive outcomes.**

OpenText™ EnCase™ Forensic is a court-proven solution renowned for its deep dive evidence acquisition capabilities, powerful processing, and integrated investigative workflows. EnCase empowers investigators to complete any investigation, mobile or otherwise, on any device with full evidential integrity.

## Simplify evidence retrieval

Examiners are under pressure more than ever to streamline their workflows and deliver results in a collapsing timeframe. Artifacts Explorer, included within EnCase Forensic, utilizes artifact-first workflows and automation, so users can examine vast data acquisitions according to a customizable pre-determined set of values in order to extract what they need, when they need it.



**"With EnCase Forensic, we see a significant improvement in our efficiency, allowing us to investigate more complaints and bring more offenders to justice."**

Allen LaFontaine Forensic Examiner  
Southern Alberta Internet Child  
Exploitation Unit

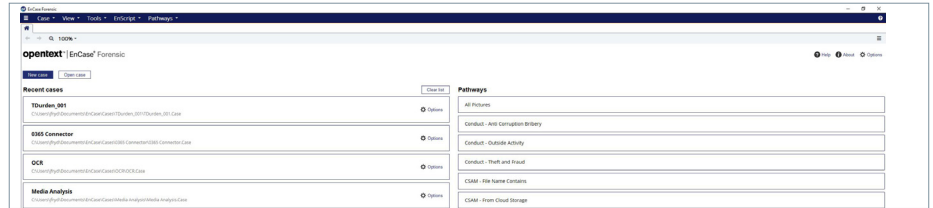
[Read the full case study](#)

[OpenText EnCase Forensic](#)

[OpenText Tableau Forensic](#)

## Court trusted acquisition and chain of custody

EnCase stores and presents evidence in a court approved format, resilient to scrutiny and process, giving all those involved complete faith in the security of the investigation.



## Pull data from any device

EnCase Forensic supports 35,000+ smartphone and tablet profiles, enabling a full spectrum of analysis in a world where smartphones and tablets form a significant proportion of digital investigation targets. The solution offers comprehensive operating system support for systems, files, artifacts, and encryption types.

Investigators can also leverage cloud connectivity to allow data and evidence collection from repositories such as Microsoft® 365, Microsoft® Sharepoint, Dropbox, Box, and a full suite of social media applications—Instagram, X (formerly Twitter), Facebook, and more..

## Speed investigations with AI imagery categorization

Includes EnCase Media Analyzer, an AI-driven tool enabling categorization of imagery within 25 data sets, such as firearms, vehicles, money, CSAM, etc. Media Analyzer can scan every image in recovered evidence, flagging items that meet data set criteria for human attention. Investigators can filter by confidence and reveal previously unnoticed evidence without relying solely on hash values.

EnCase Forensic is recognized as the industry standard for investigative data collection, with high levels of recognition and confidence in the courts. OpenText also offers a suite of training courses (virtual or onsite) to suit any organization or level of expertise, ensuring investigators can harness the full benefit of EnCase investments.

EnCase Forensic features	Description
<b>Enhanced indexing engine</b>	Empowers investigators to conduct investigations with powerful processing speeds, advanced index searching, comprehensive language support, and optimized performance.
<b>Easy reporting</b>	Provides customizable templates to help examiners create compelling, easy to read, professional reports that can be shared for every case.
<b>Extensibility</b>	Offers extensibility through EnScripts, which are automated code commands that streamline and automate tasks and extend the capabilities of EnCase Forensic for greater efficiency.
<b>Workflow automation</b>	Automated workflows allow examiners to activate/follow pre-determined processes in order to easily navigate evidence. They able to more quickly uncover which evidence is vital to their investigation.
<b>Updated encryption support</b>	Through encryption support for Microsoft® Windows® 10 Microsoft® Bitlocker® XTS-AES, Dell™ Data Protection 8.17, and Symantec™ PGP® v10.3 investigators can acquire encrypted evidence without worrying about data corruption or unnecessary delays.
<b>Apple File System (APFS) support</b>	Supports APFS, the file system used in helping investigators conduct targeted data collections from APFS and sends the output as an EnCase logical evidence file.
<b>Volume shadow copy capabilities</b>	Examines Volume Shadow Snapshot (VSS) backups, also known as volume shadow copies, generated by Microsoft Windows, allowing investigators to recover deleted or modified files, as well as full volumes and learn what may have taken place on a system before the investigation.
<b>Apple T2 Security Byass</b>	Acquires data from machines equipped with Apple T2 Security chips without additional hardware, drive partitions, or hassle. If the user is logged in, no credentials are required.