EnCase® Portable

Extend Your Forensic Reach with Powerful Triage & Data Collection

EnCase® Portable

Who Can Use EnCase Portable

- Police Officers
- Probation and Parole Officers
- Civilian Investigators
- Military Personnel
- Government Personnel
- IT Professionals
- Law firm Personnel
- Litigation Support Personnel
- Non-Technical Personnel

EnCase® Expert
Non-Expert

Triage and Collect with EnCase Portable

EnCase Portable is designed to address the challenge of completing forensic triage and data collection in the field, for both forensic professionals and non-technical personnel. The solution is composed of two components, *Triage* and *Collect*.

Triage allows forensic experts and non-experts alike to quickly review information stored on a computer in the field, in real time, without altering or damaging the information. By executing pre-configured triage searches, users can quickly browse pictures, view internet history, see who has been using a computer, and much more. Advanced users of *Triage* can also create new triage searches, in the field, in a matter of minutes, meaning no situation is out of reach of EnCase Portable *Triage*.

With *Collect*, anyone can become an extension of an organization's computer forensic, incident response, or e-discovery team. Running collection searches, pre-configured by the experts, anyone can use EnCase Portable to perform forensically sound collections in the field. *Collect* can be used to create a bit-by-bit copy of a computer's hard drive or perform a targeted collection based on the criteria required for the specific situation. In addition, with *Collect* users can collect an exact copy of a computer's memory, which can contain valuable information pertinent to an investigation.

With EnCase Portable, forensic professionals can get a handle on their case backlog by attacking the issue at the source, reducing the total amount of evidence brought in for analysis. For field personnel, EnCase Portable gives immediate access to critical information stored on a computer, without having to be an expert in computer forensics. For corporations, EnCase Portable enables easy, forensically sound collection of data from remote offices or locations without requiring expert personnel. The combination of *Triage* and *Collect* make EnCase Portable the most powerful, flexible, and field-ready solution for handling computer forensic tasks.

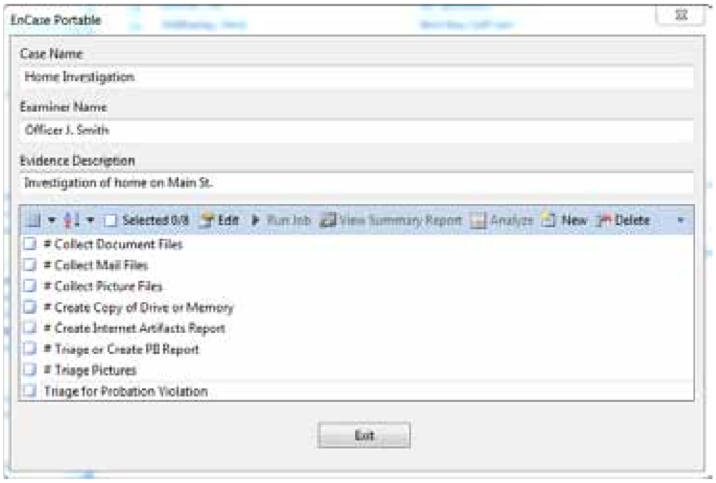
EnCase Portable Features at a Glance

CORE CAPABILITIES

Both Triage and Collect share these fundamental capabilities

- **Workflow:**
  1. Insert EnCase Portable USB (and storage drive if required) into computer
  2. Launch EnCase Portable from the USB device
  3. Select a job to execute
  4. EnCase Portable runs the selected job, collecting data or performing a triage search
  5. User, once satisfied with triage results or collection job has completed, closes EnCase Portable
  6. Collected data can be made available to the forensic professional for full analysis as required
- **Operating Modes:**
  - Execute EnCase Portable on an already running computer (Live Mode)
  - Boot a computer with EnCase Portable (Boot Mode)
  - In either mode, no EnCase files are installed on the suspect's computer

- **Default Jobs:**
    - Every EnCase Portable contains a combination of default Triage and Collect jobs, including:
        - Collect Document Files
        - Collect Mail Files
        - Collect Picture Files
        - Collect Copy of Drive or Memory
        - Create Internet Artifacts Report
        - Triage or Create PII Report
        - Triage Pictures



EnCase Portable

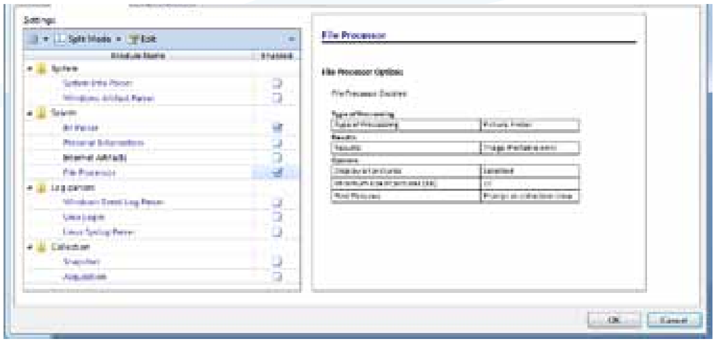
Case Name
Home Investigation

Examiner Name
Officer J. Smith

Evidence Description
Investigation of home on Main St.

□ Collect Document Files
□ Collect Mail Files
□ Collect Picture Files
□ Create Copy of Drive or Memory
□ Create Internet Artifacts Report
□ Triage or Create PII Report
□ Triage Pictures
□ Triage for Probation Violation

- **Job Creation:**
    - Create new jobs or edit existing jobs to meet specific case needs
    - New jobs can be created using EnCase® Forensic or EnCase® Enterprise
    - New jobs can also be created in-the-field, in real time without using EnCase Forensic or EnCase Enterprise
    - Transferrable from one device to another

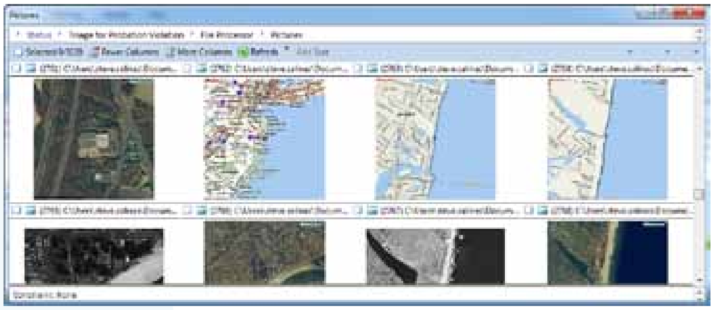


- **Collected Data:**
    - Collected data is managed with EnCase Forensic or EnCase Enterprise
    - Other solutions that support E01, L01, Ex01, or Lx01 can be used to review collected data
    - Easy import of collected data into current case.
- **Search & Collection Methodology:**
    - Valuable file attributes (metadata) and contents not altered during search and collection
    - Folder structures maintained for collected data
    - Collected data stored in EnCase® Evidence File Formats (E01, L01)
    - Encryption of collected data possible

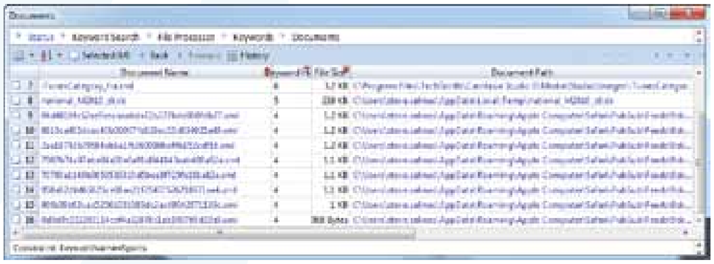
> *"EnCase Portable now gives any lawyer, paralegal, and litigation support specialist the ability to easily collect and preserve ESI anywhere, anytime."*
>
> -John J. Rosenthal,
> Partner and Chairman,
> e-Discovery and electronic information practice group,
> Winston & Strawn LLP

TRIAGE SPECIFIC CAPABILITIES

- **Triage Options:**
  - Search for files that may contain *Personally Identifiable Information (PII)*
    - Credit Cards (Visa, MasterCard, American Express, Discover)
    - Phone Numbers (with or without area codes)
    - E-mail addresses
    - US Social Security Numbers
  - Review Images in a Gallery View
    - Search based on file extensions (.jpg, .bmp, .png, etc.)
    - Search based on file signature
    - Limit number of images and/or the minimum image file size



  - Identify files based on Hash Value matches
    - Create new hash sets
    - Use hash sets available in EnCase Forensic or EnCase Enterprise
    - Customize search by creating an Entry Condition to focus the search
  - Preview files based on Metadata
    - Focus searches based on any properties of a file (size, type, dates, etc.)
    - Specific search criteria is entered as an Entry Condition
    - Matching files can be reviewed instantly
  - Locate and review files that contain specific Keywords
    - Import a list of keywords or add keywords manually
    - Customize search by creating an Entry Condition to focus the search
    - Review the keyword search results for all files on the suspect computer



- **Reporting and Analysis:**
  - Perform a quick analysis on the collected data
  - Prepare a report on the triage and collection results in the field

- **Encryptions Support:**
  - Utilizing the EnCase® Decryption Suite, the following encryption products are supported
    - PGP Whole Disk Encryption
    - Microsoft Bitlocker
    - Guardian Edge Encryption Plus, Hard Disk, and Encryption Anywhere
    - Utimaco/Sophos Safeguard Easy
    - McAfee SafeBoot Offline (challenge/response not supported)
    - WinMagic SecureDoc
    - Checkpoint/PointSec Full Disk Encryption
  - Credentials required for each supported encryption product

> *"EnCase Portable lets anyone with minimal technical knowledge collect electronic evidence, with a chain of custody, from computers in the field. This will free up time for computer forensic experts and allow them to focus their attention on analysis and reporting, rather than initial collection."*
>
> *- "Collect Evidence With EnCase Portable," Product Review, Law Technology News*

COLLECTION SPECIFIC CAPABILITIES

- **Collection Options:**
  - Acquisition
    - Collect logical, physical, and/or removable drives
    - Acquire computers memory
    - Configure imaging job to prompt for desired drive at time of collection
  - Acquisition Configuration
    - Set segment file and block size
    - Select compression and error granularity settings
    - View calculated MD5 and/or SHA1 acquisition hashes
  - Snapshot Information
    - Calculate hash values for executables that are currently running
    - Identify processes that have been hidden from the operating system
    - Collect list of currently loaded dynamic link libraries (DLLs)
    - Gather information on currently logged on users
    - Detect if the MAC address of any Network Interface has been altered
  - Internet History
    - Collect history of visited websites
    - Collect user cache and bookmarks
    - Collect information on cookies and downloaded files
  - Instant Messages
    - Identify and parse information left on the computer related to instant messaging
    - Search for instant message artifacts can include the unallocated space of the hard drive
    - AOL, MSN, and Yahoo instant messaging clients supported
  - System Information
    - Collects system from artifacts related to
      - Network Information
      - Operating system information
      - Installed Software
      - Installed Hardware
      - User/Account information
      - Shared/mapped drives
      - User Activity (Linux Only)
      - Startup Routines (Linux Only)
    - Supports Ubuntu 8 Fedora 8 Linux distributions, in addition to Windows operating systems.
  - Linux System Logs
    - Collects and parses Linux system log files and their system messages
  - Windows Artifacts
    - Collects the following windows system files
      - MFT transaction logs
      - Link Files
      - Recycle Bin items
    - Search for windows artifacts can include the unallocated space of the hard drive
  - Unix Login
    - Parses the Unix systems WTMP and UTMP files, which hold all login activities
  - Windows Event Logs
    - Parses and collects information pertaining to Windows events recorded in the system logs, including application, system, and security logs
    - Entry condition may be used to target the search based on the entry properties
    - Included EVT and/or EVTX conditions to limit the search and collection further

ILTA'S DISTINGUISHED PEER AWARDS

ILTA's 2010 Distinguished Peer Award for the Innovative Vendor Category

Guidance® SOFTWARE

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 40,000 licensed users of the EnCase technology worldwide, the EnCase® Enterprise platform is used by more than sixty percent 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*.