



EnCase® Neutrino®

A Mobile Device Acquisition and Analysis Solution to Streamline Digital Investigations...



EnCase® Neutrino® is the solution:

- Examine multiple devices and correlate with computer evidence at the same time.
- Share EnCase® Neutrino® acquired Logical Evidence Files with other EnCase v6 examiners.
- Carry your entire tool set, organized and stored in a single field kit.
- Possess hardware support and parsing capabilities for more than 95* of the most common devices, with new devices being added regularly.
- Access unallocated space on select devices.
- All cables are fully labeled and stored in individual storage units.
- Quickly find the correct connectors with an easy-reference catalog.
- Rely upon our WaveShield™ signal-blocking bag that has been tested in [line-of-sight of multiple cell towers](#) to achieve the most dependable wireless blocking capabilities.

The need to acquire evidence from mobile devices has created new and complex challenges for investigators. The features of each device and the file contents vary by type of device and service provider. Unlike with computer media, different mobile device manufacturers rely upon different proprietary operating systems and data types.

Because there is no single standardized approach to investigating mobile devices, most mobile device forensic tools are only able to operate on a narrow range of handsets, focusing on specific platforms for a specific product line, a distinct operating system or particular hardware architecture. The broad variety of forensic tools makes it difficult for investigators to ensure that they have the proper tools for each device they encounter and to know they are getting all of the relevant data. The ever-changing advancement of mobile devices actually increases the complexity of mobile device examinations, as investigators struggle to keep their tool kits up to date. Last, but not least, no mobile forensic tool currently permits the analysis of multiple devices at the same time, nor the correlation of mobile device data with suspect computer media (hard drives, thumb drives, etc).

EnCase® Neutrino® is the only mobile device acquisition tool that integrates with EnCase® v6, allowing you to analyze both mobile devices and computer evidence at the same time. Because EnCase v6 software delivers analysis of data acquired by EnCase Neutrino, you can analyze and document both mobile device data and computer data simultaneously to correlate all evidence during an investigation.

The EnCase Neutrino WaveShield™ signal-blocking bag has been tested in close proximity to multiple cell towers to ensure reliability. It is not uncommon for an investigator to need the positions for the last cell towers, or longitude and latitude for their last contact, prior to the analysis. There are many wireless signal blocking technologies available, but many fail to dependably block wireless signals to the device being examined. Guidance Software has conducted extensive research and testing to create a reliable signal-blocking bag that allows for the safe acquisition of mobile device data, even within close proximity to cell towers.

EnCase® Neutrino® Overview:

- Hardware support and parsing capabilities for more than 95* of the most common mobile devices from Nokia, Motorola, Samsung, Siemens, LG and Sony Ericsson.
- You will receive support for additional devices on an ongoing basis.
- Yearly subscription service provides monthly updates for acquiring newly supported devices and includes the required cables.
- Cables are accompanied by a comprehensive catalog so investigators can easily and quickly find the correct connectors. The mobile phone wizard will also prompt for the specifically required cable.
- The EnCase Neutrino mobile phone wizard properly identifies...
 - currently supported devices.
 - steps to process each device.
 - the particular data that is parsed and accessible with EnCase v6.
 - whether logical and/or physical data is available for each particular device.
- Includes WaveShield™ signal-blocking bag delivering reliable wireless signal blocking protection even within close proximity to cell towers.
- All cables are fully labeled and stored in individual storage units.
- Portable with the entire tool set organized and stored in a single field kit bag.

The EnCase® Neutrino® Field Kit Includes:

- EnCase® Neutrino® forensic acquisition device
- 120/240v auto-switching power supply
- 12v automobile power supply
- Four types of foreign power adapters for use internationally
- USB cables of various lengths
- RJ-45 extension cables of various lengths
- SIM Card Reader (high-quality/multiple-use reader for processing a phone's SIM Card)
- Mobile-phone-specific cables (Guidance Software will periodically supply users with new cables that are necessary to access newly supported devices.)
- WaveShield™ signal-blocking bag
- Carrying/storage case

Extracted mobile device data is stored in an EnCase® Logical Evidence File (LEF) and can be examined via EnCase v6 only. EnCase software provides access to some or all of the following information from supported mobile devices within the Records Tab:

- **Device Settings**
 - serial number
 - manufacturer information
 - firmware/hardware information
 - IMSI#
 - IMEI#
 - cell tower location
 - ringer volume, etc
- **Contacts / Phone Book**
- **Call Logs**
 - received
 - dialed
 - missed calls
 - call duration
- **SMS and MMS messages**
- **Calendar**
- **Files stored on the device**
 - images
 - sounds
 - documents
 - ring tones
- **File System**
 - Java packages
 - games
 - programs
 - executables
- **Deleted content from unallocated space (available with SIM card and physical acquisitions only)**



*The number of phones supported is provided as of EnCase® Neutrino® Version 1.3 released in August 2007.

www.guidancesoftware.com

About Guidance Software® (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 and effective computer investigations of any kind, such as intellectual property theft, incident response, compliance auditing and responding to eDiscovery requests—all while maintaining the forensic integrity of the data. There are more than 27,000 licensed users of the technology, and thousands of investigators and corporate security personnel attend Guidance Software's forensic methodology training annually. Validated by numerous courts worldwide, EnCase software is also frequently honored with top security awards and recognition from eWEEK, SC Magazine and Network Computing, as well as the Socha-Gelbmann survey.