



 **NEUTRINO**™

**A Mobile Phone Acquisition and Analysis  
Solution to Streamline Digital Investigations...**



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

Because there is no single standardized approach to investigating mobile phones, most mobile phone 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 phones actually increases the complexity of mobile phone 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 phones at the same time, nor the correlation of mobile phone data with suspect computer media (hard drives, thumb drives, etc).

#### Neutrino is the solution:

- **Examine multiple phones and correlate with computer evidence at the same time.**
- **Share 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 75 of the most common phones, with new phones being added regularly.**
- **Access unallocated space on select phones.**
- **All cables are fully labeled and stored in individual storage units.**
- **Quickly find the correct connectors with an easy-reference catalog.**
- **Rely upon a Faraday bag that has been tested directly under cell towers to achieve the most dependable wireless blocking capabilities.**

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

**The Neutrino Faraday bag has been tested directly under 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 Faraday 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 Faraday bag that allows for the safe acquisition of mobile phone data, even within close proximity to cell towers.

## Neutrino™ Overview:

- Hardware support and parsing capabilities for more than 75 of the most common mobile phones from Nokia, Motorola, Samsung, Siemens, LG and Sony Ericsson.
- You will receive support for additional phones on an ongoing basis.
- Yearly subscription service provides monthly updates for acquiring newly supported phones 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 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 patent-pending Faraday bag technology 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 Neutrino™ Field Kit Includes:

- 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 phones.)
- Faraday bag
- Carrying/storage case

**Extracted mobile phone 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 phones within the Records Tab:**

- **Phone 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 phone**
  - 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)**



## 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 20,000 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 is also frequently honored with top security awards and recognition from *eWEEK*, *SC Magazine* and *Network Computing*, as well as the *Socha-Gelbmann* survey.



[www.guidancesoftware.com](http://www.guidancesoftware.com)

©2007 Guidance Software, Inc. All Rights Reserved. EnCase and Guidance Software are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners.