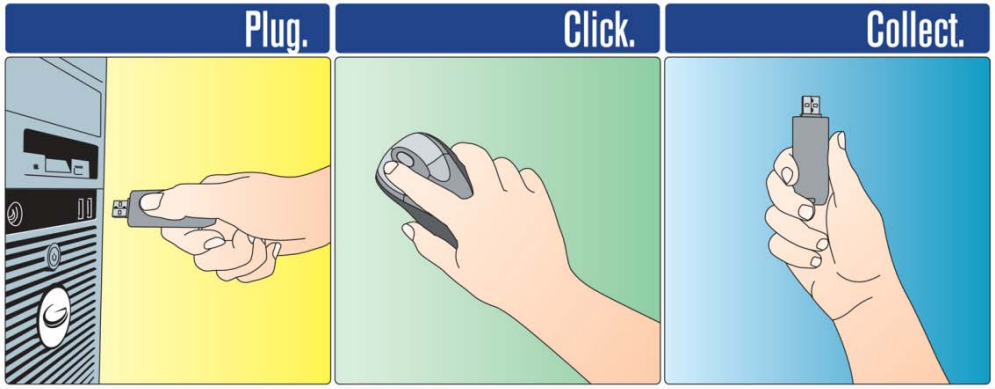
EnCase Portable Demo

© 2009 Guidance Software, Inc. All Rights Reserved.

Guidance® SOFTWARE
The World Leader in Digital Investigations™



EnCase Portable

Easy to Use Collection Solution

Brent Botta
Director of eDiscovery Solution

© 2009 Guidance Software, Inc. All Rights Reserved.

Agenda

- EnCase Portable Solution
  - What is it?
  - Business Issues to Utilize Portable
  - Package Contents
  - How does it work?
  - What can I do with it?
  - Let’s see it work – Need a volunteer

© 2009 Guidance Software, Inc. All Rights Reserved.

EnCase Portable – What is it?

- **Automated EnCase search and collection capabilities executed from a USB device**
- **Enables users to search and collect data when**
  - Target systems cannot be transported
  - Ultra portability is needed
  - Acquisition on multiple systems simultaneously with laptops is cost prohibitive
  - Experienced personnel cannot be used for the collection of data

© 2009 Guidance Software, Inc. All Rights Reserved.

Business Issues

- **Law Firms/Litigation Support**
  - Problem
    - Lag time between request for collection and the actual collection
    - Reliant on outside resources to collect data
    - Extremely expensive to use these outside resources
  - Impact of Problem
    - Time to case resolution
    - High consulting costs (airfare, meals, hotels, etc.)
  - Solution
    - Collect with in-house personnel with little training required
    - Immediate data collection and preservation
    - Reduce cost
    - Works immediately

© 2009 Guidance Software, Inc. All Rights Reserved.

Business Issues

- **Corporate IT**
  - Problem
    - One organization, many networks
    - Remote employees infrequently on the network
    - Limited resources
  - Impact of Problem
    - To collect expert may travel to remote location
    - Employees may be forced to send their machine to corporate
    - Downtime
  - Solution
    - Non-expert collect using trusted & proven technology
    - No training needed to collect (basic computer skills only)
    - Allowing employees to retain their machines and keeping expert resources focused on their core competency, analysis

© 2009 Guidance Software, Inc. All Rights Reserved.

Benefits and Why it is Needed

- Benefits
  - Data Collection solutions *anyone* can use
    - Basic computer user can be trained on the use of EnCase® Portable in a matter of minutes
  - All in One Solution
    - EnCase Portable is ready to use out of the box, just plug in and collect
  - Ultra-portability
    - Everything needed fits in small case, take it anywhere
  - Stealth Operation
    - Search and Collect without leaving a trace you were ever there
  - Forensically Sound
    - Data collected with EnCase Portable is stored in the forensically sound, court validated EnCase ® Logical Evidence File (LEF) format

© 2009 Guidance Software, Inc. All Rights Reserved.

Package Contents

© 2009 Guidance Software, Inc. All Rights Reserved.

Portable Kits

- Kit Contents
  - One 4GB USB drive with EnCase® Portable installed
  - One 16GB USB drive for additional storage
  - One four-port USB hub
  - EnCase® Portable security key
  - User quick reference guide
  - EnCase® Portable installation DVD
  - Windows Boot CD
  - Rugged carrying case

© 2009 Guidance Software, Inc. All Rights Reserved.

Technical Information

- System Requirements
  - EnCase Portable Configuration System
    - EnCase Forensic, Enterprise, or FIM (v6.14 or higher)
    - EnCase Security Key (Dongle)
    - USB 2.0 Port (2 recommended)
    - 2.4 GHz Pentium IV Processor or better
    - 2 GB of RAM or more
  - EnCase Portable – USB Device
    - USB 2.0 storage device
    - 16 GB recommended storage
- Boot mode Support
  - Windows 98
  - Windows 2000
  - Windows 2003
  - Windows XP
  - Windows Vista
  - Mac (Intel)
  - Linux
- Live Mode Support
  - Windows 98
  - Windows 2000
  - Windows 2003
  - Windows XP
  - Windows Vista

© 2009 Guidance Software, Inc. All Rights Reserved.

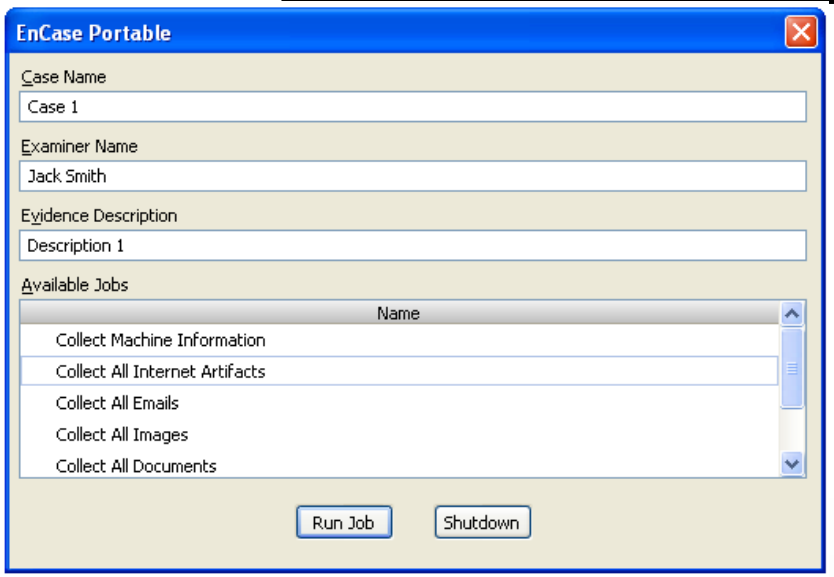
Different Ways to Use Portable

- Modes of Operation:
  - "Live" – There are instances that you might want to run Portable jobs on a live and running computer. If the drive is Whole Disk Encrypted is one example.
  - USB Boot Mode – In this mode you configure the BIOS to boot the USB device and it will automatically start the Portable GUI
  - CD Boot Mode – When configuring the USB boot is impossible on older computers, you can utilize a boot CDROM and it will then start the Portable GUI

© 2009 Guidance Software, Inc. All Rights Reserved.

How it Works

- EnCase Expert
  - Configures jobs using EnCase (Forensic, Enterprise, or FIM)
  - Creates Portable USB Device
- Portable Device User
  - Inserts EnCase Portable and a Storage device into USB ports on target machine
  - Live Mode
    - Launch EnCase Portable
  - Boot Mode
    - Starts target machine, EnCase Portable will automatically start
  - Drives write protected using EnCase Fastbloc Software Edition
  - Select desired job, clicks “Run Job”
  - Data is collected
  - Transport data back to expert for analysis



© 2009 Guidance Software, Inc. All Rights Reserved.

Why EnCase Portable?

- Turns basic computer users into data collectors in a matter of minutes
- Fully integrated with EnCase
- Runs on any USB device
- Utilizes the proven, vetted search and collection capabilities of EnCase
- Stores data in forensically sounds Logical Evidence File or E01 Formats

Solves the whole data collection problem in one solution!

© 2009 Guidance Software, Inc. All Rights Reserved.

I need a volunteer

- Anyone with the following qualifications:
  - Non-IT
  - Can plug in a USB device
  - Follow Simple Instructions

Any Takers??? ***(It will be worth your time)***

© 2009 Guidance Software, Inc. All Rights Reserved.

Sample Email Body

Dear Custodian,

To further the litigation hold notice for a current legal matter internally named “ILTA”, a collection device has been shipped to your location. The goal is to collect information from your assigned computer for this matter. The package will have a kit in it with a box labeled as “EnCase Portable”. Please follow the instructions below:

© 2009 Guidance Software, Inc. All Rights Reserved.

Sample Instructions

- Plug the Black, Blue, and Red USB devices into the Grey 4 port IOGEAR Micro Hub
- Plug the Grey USB Hub into your computer via the USB plug on the bottom
- Your computer will find a device named “EP_WIN” that has a file named “Run Portable.exe” in the main folder. Double click that file.
- A screen will appear that requires you to enter your Name and Media Description. Please use the model and serial number of your computer in the Media Description. The label will be on the bottom of the laptop.
- Then Click “Run Job”

© 2009 Guidance Software, Inc. All Rights Reserved.

Contact Info

Brent Botta

Director, eDiscovery Solutions

brent.botta@guidancesoftware.com (or)

botta@encase.com

© 2009 Guidance Software, Inc. All Rights Reserved.