Guidance Software™

The World Leader in eDiscovery & Digital Investigations™

SANS Forensic 2009 Vendor Panel

Briefing on EnCase® Portable

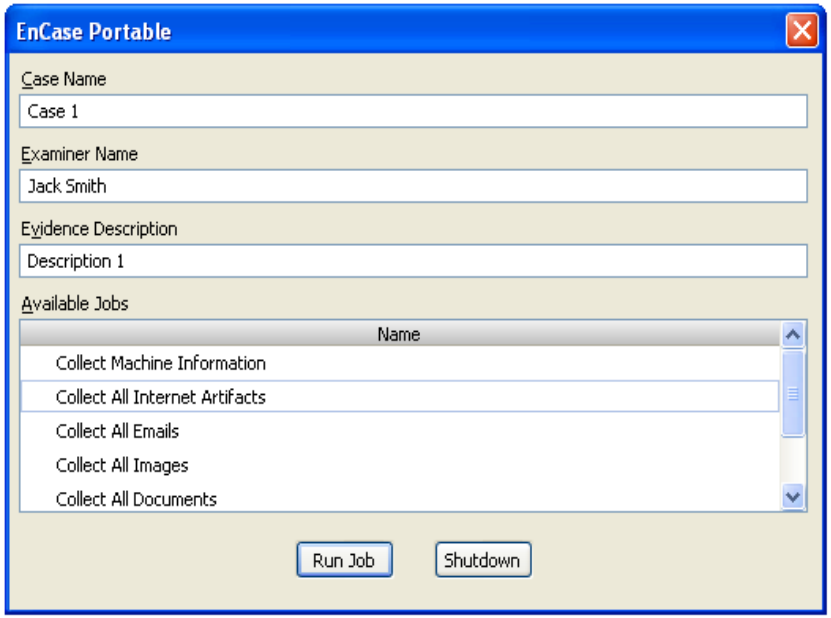
July 8th, 2009

EnCase® Portable

- "EnCase for Everyone": automated EnCase software search and collection/preservation capabilities executed from a bootable USB device
- Enables users to search and collect evidence when:
  - Target computers cannot be reached over the network
  - Ultra-portability is needed
  - Large numbers of target computers
  - Forensic personnel are unavailable for evidence collection
  - Time is of the essence
  - Covert action is necessary

EnCase® Portable – How it Works

- User Workflow:
  - Insert EnCase Portable and Storage (hard drive or USB) into USB hub and into USB port on target computer
  - Run EnCase Portable
    - Live Mode (computer running): Launch EnCase Portable
    - "Dead" box (computer off): Start target machine, EnCase Portable will start automatically
    - Target computer drives write-protected using EnCase write-blocking technology
  - Select desired job, click "Run Job"
    - Jobs can be out-of-the-box options or custom configured
  - Data is automatically collected into EnCase Evidence Files and stored on Storage drive

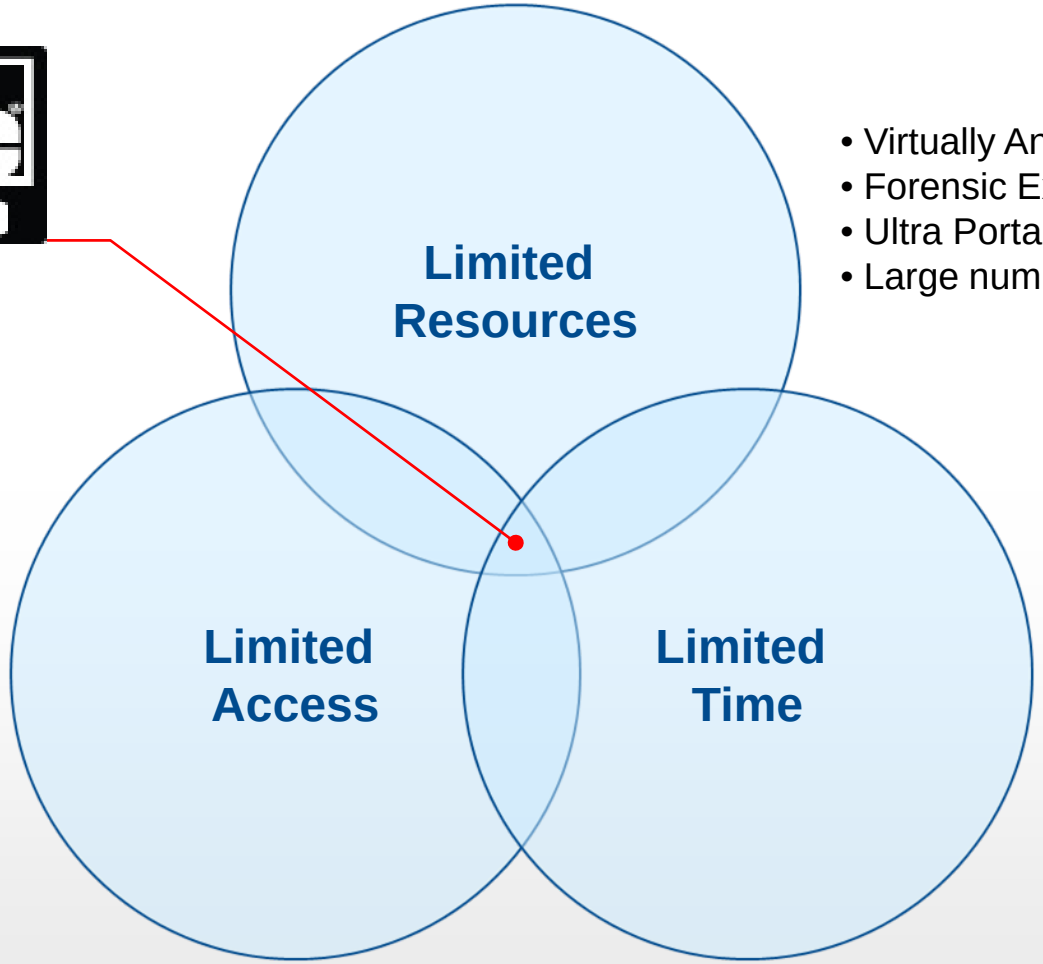


EnCase® Portable – Product Overview

Not Pictured

- EnCase Portable DVD
- BIOS Reference Guide

EnCase® Portable



- Virtually Anyone can use
- Forensic Experts not misused
- Ultra Portability is needed
- Large number of computers to triage

- No Network Reach
- Remote Sites
- VPN Users
- Covert Collection

- Focused extraction
- Rapid turn around
- Collect evidence
- Correlate collections