REGIONAL COMPUTER FORENSICS LABORATORY

RCFL

CONTINUING EDUCATION SERIES

An ongoing training initiative that provides helpful news and information about the latest happenings in the digital forensics world.

THE RCFL PROGRAM

America's Premier and Most Accredited Digital Forensics Laboratory Network.

npo@rcfl.gov | 703-985-3677

CONTINUING EDUCATION SERIES

THE FIVE BASICS ABOUT LIVE CAPTURE

Live capture—also known as "running system forensics"—is the collection of digital evidence from a computer in a powered-on state, often without the use of a write blocker. Write blockers are hardware devices and software applications that allow the acquisition of information on a drive without changing or damaging its contents. Traditional digital forensics are performed on an exact copy of the data by using a write-blocker, and are typically conducted in a laboratory setting.

Below are the five basics about live capture which law enforcement officers (LEOs) should know:

1. **Wait Before Pulling the Plug**—Powering off a computer results in the permanent loss of volatile data which can include Random Access Memory (RAM), Internet history, websites visited, currently decrypted data, etc. To avoid losing volatile data, leave the device powered on. Perform a hard shut-down (pulling the plug) only in situations where the device is actively destroying data.

2. **Every Situation Varies**—Every live capture situation is unique and often complex—one size does not fit all. A trained expert can determine the best possible solution after assessing the device.

3. **Encryption Requires an Expert**— If encryption is suspected, immediately enlist an expert such as a Digital Forensics Examiner. In the interim, disable screen saver password protection and secure the area around the computer until the Digital Forensics Examiner arrives on-scene.

4. **Ask for Passwords & Look for Clues**—Always ask the suspect(s) for passwords. If the individual refuses to cooperate, look for hand-written notes in and around the computer, and observe and photograph your physical surroundings for clues and insights regarding potential passwords or pass phrases. This is especially critical if encryption is involved or suspected.

5. **Document the Scene**—When handling electronic devices such as computers—document and photograph any actions taken. Ideally, one person operates the computer system, while the other takes notes and photographs the screen. If an investigator is asked to testify in court, having detailed notes in his/her possession is invaluable. In time-sensitive situations when an Examiner is not yet present, documenting the scene can save precious minutes or hours.

Request an archive version of the RCFL Program's 2010 Webcast: "Capturing a Running Computer System: What Every Digital Forensics and Cyber Professional Should Know" by logging onto

WWW.RCFL.GOV