Introducing the—

# CONTINUING EDUCATION SERIES

An Ongoing Training Initiative That Provides Law Enforcement and First Responders with the Latest Information They Must Know About Digital Evidence.

To access the Series online, visit www.rcfl.gov.

# 5 KEY FACTS ABOUT DIGITAL EVIDENCE

1. Every type of crime involves digital evidence.

2. A criminal crime scene is also a digital evidence crime scene. Investigators must apply the same level of care, custody, and control to ensure their personal safety and to preserve the evidence.

3. Digital evidence can be fragile. If not handled properly—heat, cold, and magnets can destroy it.

4. Digital evidence can be easily altered. If a computer is off, leave it off. Just turning it on or taking a quick peek at the files can change the data. If the computer is on, perform a proper shutdown or ask a digital forensics Examiner for assistance. If the computer is on and destroying evidence, perform a "hard shut down" by pulling the plug from the wall. Remember, when in doubt, leave the device "off."

5. Never assume that digital evidence was destroyed. RCFL Examiners have extracted digital evidence from burned out computers and devices found at the bottom of a lake. Play it safe—always bring the device to a certified digital forensics Examiner for further study.

WWW.RCFL.GOV