TRAINING ANNOUNCEMENT

**Windows Forensic Environment On-Scene Triage**

Law enforcement investigators must be able to safely preview a suspect’s computer in the field to determine if it contains evidence of criminal activity. To do this, they can use the Windows Forensic Environment (WinFE), a tool that lets them create a forensic environment for on-scene computer triage. WinFE is a bootable forensic environment based on the Windows operating system. With it, investigators can forensically examine a suspect computer using Windows-based forensic software tools. Through discussion and hands-on training, this course shows investigators how to use software based on the Windows Preinstallation Environment (WinPE) to build forensically sound software versions of WinFE (based on the Windows 7 and 8.1 operating systems). After creating this software, students will practice booting a computer with a USB device to collect evidence.

**What you will learn**

This course takes students through the steps of building their very own WinFE that they can customize for their agency. (Due to Windows licensing restrictions, students will create a USB device and a DVD image using trial versions of Windows.) Students will receive instruction on the following topics:

- Windows Preinstallation Environment (WinPE)
- History of the open source WinFE project
- How to setup and configure WinBuilder
- Forensic Preview Software Tools:
  - osTriage 2
  - Field Search
  - FTK Imager Lite
- Capturing RAM
- Write protection software
  - How to use write protection
  - How to mount/un-mount a volume
- Identifying the presence of encryption software
- Conducting a preview
- Collecting potential evidence
- Preserving collected evidence

**Who should attend**

This 2½-day course is targeted to the experienced high-tech crime investigator. Attendees should have a background in online investigations and understand and have experience with the basic computer crime scene. This is not a computer forensic course, but an advanced high-tech crime scene investigation course.

**Enrollment in each course is limited to 20 persons.**
SEARCH training courses are limited to law enforcement personnel only.

**Find out more at**