Foundation in Securing Computer Evidence

SAFELY ACQUIRE COMPUTER-BASED DATA

Securing computer-based evidence is no longer simply a case of "pulling the plug" and imaging hard disk drives back in the office. The use of cloud storage, encryption and non-removable storage are commonplace and mean that a more considered and multi-pronged approach to acquiring data is required. Without a clear understanding of the way in which devices store digital data both locally and and remotely, vital evidence can easily be missed, lost or altered during the acquisition process.

In addition to the technical complexities presented by current devices, the overwhelming volume of digital forensic submissions being made increases the need for triage-based approaches to assist in prioritising exhibits for analysis.

> "THE LOCATION, TRAINERS AND FACILITIES WERE EXCELLENT"

Course Aims

Foundation in Securing Computer Evidence is a 4½ day hands-on course designed to teach delegates how to acquire data from a wide range of devices, whilst either powered on at a search scene or powered down back in the office. Delegates will learn how to image traditional spinning disk hard drives, SSDs and USB storage devices using established forensic tools but will also learn:

- "Live forensics" techniques to acquire volatile data held in RAM, open encrypted containers and cloud storage
- "On-device imaging" techniques for dealing with storage devices which cannot or should not be removed from the host device (e.g. devices running Apple's APFS file system, RAID configurations etc.)
- Triage techniques for rapid identification of case-related material held on computer storage

Who should attend?

This entry-level course is targeted at practitioners who are new to computer acquisition or existing staff who have not had the benefit of formal training. The course is designed to meet the needs of both lab-based staff as well as those required to secure evidence at a search scene.

What you will learn

By the end of the course, delegates will be able to:

- Confidently secure evidence from a range of removable computer storage media in accordance with ACPO Principles of Computer Based Digital Evidence and ISO 17025
- Use a Linux boot disk to secure evidence from a computer whose storage media is difficult to remove or cryptographically bound to the host device
- Perform on-scene capture of live data from device RAM, open encrypted local storage or cloud storage
- Use forensic triage tools to identify relevant content in order to prioritise computer exhibits for evidential analysis
- Explain & justify their actions in court

contact

+44 (0)20 8133 8758
info@controlf.net
PO Box 167, Sandy, SG19 9AL
www.controlf.net

Dates & prices are on our website