COURSE REFERENCE CODE

RAP (Raid Actions - Protocols for Dealing with Computers)

COURSE OVERVIEW

Computers are now undeniably the largest source of documentary evidence in many criminal offences and conflict of interest situations, in the commercial world. Entities involved in the production of counterfeits, fraudulent and corrupt activity, to name just a few criminal activities, know this. The way in which an investigator handles a suspect computer could very well cause major issues for the investigation, for example it is possible to set up computers with anti-tamper protocols, so that attempting to access them without conforming in a specific way will cause them to obliterate their memory. The handling of computer hardware in an investigation can have both evidential and legal ramifications. Evidence must be seized and handled in accordance with standard operating procedures that follow the law in that jurisdiction. Ultimately, the process by which an investigator acquired the evidence is just as important as the evidence itself.

This module has not been designed to provide students with a detailed understanding of computer data forensic work, but to have a basic understanding of what to do and not do when a computer is first encountered during the course of an investigation to ensure potential electronic evidence is not lost or damaged.

COURSE OBJECTIVES

The following objectives will be covered during this module:

- Action when first encountering a computer;
- Handling a computer that is switched off;
- Handling a computer that is switched on;
- What should be seized for reconstruction of the computer system; and
- Protocols for dealing with hand held devices.

METHOD OF INSTRUCTION

The aim of this module is to demonstrate the most effective and legally responsible methods of handling computers and other electronic data storage devices when discovered during an investigation. While the primary method of instruction will be in the classroom, there will also be practical examples and a range of scenarios that will require input from the student to ensure understanding and application.

On conclusion of the module participants will receive a comprehensive set of student notes and certificate of completion.

COURSE DURATION	COURSE VALUE
1/2 day module	This module will be of value to both investigation managers and investigators who are likely to be involved in locating and seizing computers and other electronic data storage devices that could subsequently be subject to forensic examination during the investigation process, and eventual production as an exhibit in an enforcement complaint, judicial proceedings, internal disciplinary hearing, or similar.