

Course Aim

This course is designed to provide an investigator with the knowledge and skills to effectively recognise and deal with electronic evidence sources to support their responsibilities as part of a criminal or civil investigation and how to ensure the evidence is admissible in court or internal proceedings.

Objectives

The objectives for this training have been designed and developed to enable investigators to meet the requirements of the Skills for Justice UK National Occupational Standards for Countering E-Crime that apply to relevant corporate and law enforcement staff. These objectives are described overleaf.

Note: Delegates should expect to undertake a certain amount of preparatory work for this course and this will depend on the exact requirements of each client. This is a practical course and delegates will undertake skills and knowledge checks. Certificates will only be awarded to those who successfully complete the course.

Who should attend

This course is designed for all investigators that are responsible for recognising and dealing with electronic evidence for use in their work and who need to understand the methodologies, risks and dangers of such activity. Much of the course is hands-on and those who do not use a computer on a regular basis may not fully benefit.

Course Details

This training may be taken as a single course or as modules leading to the same outcomes. Each delivery will accommodate client requirements and may vary in duration to meet those criteria. The cost and training location will be determined in consultation with the client and will either be on a per student basis or an overall course fee.

Trainers

James Stark designed and developed the first and only e-learning high tech crime first responder programme for the UK police service. He has delivered training in the UK, Europe, Africa, the Middle East and Asia and has an excellent reputation as a trainer in this country and abroad.

Nigel Jones created and ran the national high tech crime training centre for the UK Police Service and has been involved in the delivery of high tech crime training for over 15 years. He currently delivers training on courses for Interpol

James and Nigel were also members of the team that developed the UK National Occupational Standards for Countering E-Crime and various groups that have developed good practice for the handling of electronic evidence in the UK, Europe and USA.

Skills for Justice

The following is an extract from the Skills for Justice web-site:

“The compelling case outlining the pressing need to tackle e-crime has been set out in a paper by EURIM, the all-party pan-industry European lobby. Only a small percentage of police officers in the UK have been trained to handle digital evidence at the basic level with fewer still involved with Computer Crime Units or having higher-level forensic skills. In addition, a great many private and public agencies are also involved in countering e-crime and individuals working in these organisations have similar skills needs. Crimes involving ICT systems and the Internet are now common and threaten the integrity of our national prosperity. These are the National Occupational Standards (NOS) for e-crime investigators and computer forensic experts, and have been developed by practitioners working within the field. If there is to be trust and sharing between people with these skills across the public and private sectors, there will be real benefit in having standards that are commonly acknowledged”.

All elements of training have been developed to conform to National Occupational Standards for Countering E-Crime. (www.skillsforjustice.co.uk)

A broader outline of all areas covered including training outcomes is available upon request.

OBJECTIVES

After attending the course the participant will be able to:

- Check that the necessary authorisations are in place
- Conduct preparatory research concerning the capabilities of the subject of the investigation
- Identify and select the appropriate tools and consider multiple options to meet the needs of capture or seizure
- Recognise devices capable of storing electronic evidence and determine whether they require capturing or seizing
- Identify any health and safety risks associated with the electronic devices
- Consider the volatility of data and its preservation
- Identify external connections to and from devices
- Isolate the scene and secure the electronic evidence sources to prevent contamination and external interference
- Determine whether to capture electronic data or to seize electronic devices
- Keep a record of the state of the device and potentially relevant information in the immediate vicinity
- Take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations
- Preview the contents of the device in a forensically sound manner
- Choose and apply the appropriate power off method for the device
- Photograph and label the components of the device making specific reference to ancillary leads and connections to the device
- Appropriately package, seal and label the device in accordance with current procedures
- Conduct a preliminary risk assessment of the requirements for the evidentially sound and safe capture of electronic evidence
- Ensure the preservation of third party and volatile data sources
- Capture and preserve electronic evidence in accordance with legal and organisational requirements
- Document the electronic evidence capture throughout the process so that all actions can be reproduced by a competent third party
- Create an evidential product of the data sources to a suitable medium

Technology Risk Limited

PO Box 255

Faversham

Kent

ME13 3AH

United Kingdom

Tel +44 (0) 20 3239 9669

Email enquiries@technologyrisklimited.co.uk

www.technologyrisklimited.co.uk