

Course Aim

This course is designed for those entering the field of IT forensics. It is an entry level course for new practitioners and will allow them to begin their career with knowledge and skills in dealing with electronic evidence that cannot be simply seized. It will also provide the fundamental knowledge to be able to investigate, evaluate and report on electronic evidence sources to support their responsibilities as part of a criminal or civil investigation and ensure the evidence is admissible in court or other proceedings.

Objectives

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. Delegates attending this course 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 IT forensic investigators and others who are beginning their careers and responsible for investigating, evaluating and reporting on 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 benefit fully.

Pre-Course Requirements

Delegates attending this course should be able to demonstrate the knowledge and skills required by the National Occupational Standards CO1 and CO2, as delivered by TC² in its "Recognising and Dealing with Electronic Evidence" course, or are able to demonstrate equivalent knowledge and skills.

Course Details

This course is a single course of 5 days and has been developed to enable investigators to meet the requirements of the Skills for Justice National Occupational Standards for Countering E-Crime that apply to corporate and law enforcement staff.

Trainers

The trainers for this course are recognised for their expertise in the field of IT forensics and chosen from the cadre of such trainers available to TRL.

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.

OBJECTIVES

After attending the course the participant will be able to:

At the scene

- Check that the necessary authorisations are in place
- Identify and select appropriate tools and consider options to meet the needs of capture
- Identify health and safety risks associated with capturing data from electronic devices
- Consider third party and volatile data and its preservation
- Preview the contents of the device in a forensically sound manner
- Capture and preserve evidence in accordance to 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
- Keep accurate records of procedures using appropriate documentation

At the lab

- Check that the necessary authorisations are in place
- Establish the scope of the investigation in consultation with the client
- Identify and select the correct equipment
- Conduct the investigation in accordance with legal and organisational requirements
- Conduct the investigation using evidentially sound forensic tools and techniques
- Conduct cross tool validation of results
- Perform necessary and proportionate research activities to obtain additional information
- Consult with relevant third parties to obtain information relevant to the investigation
- Create a working product for further investigation
- Review the scope of the investigation throughout the process, based on findings
- Document the investigation so all actions can be reproduced by a competent third party
- Provide a clear and accurate oral presentation of the findings
- Establish the content and purpose of the report, and identify the audience
- Conduct an impartial evaluation of the significance of the forensic examinations
- Produce an accurate, impartial and complete written report based on the findings
- Provide a clear and accurate oral presentation of the findings
- Keep accurate records of the process using appropriate documentation

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