

Course Aim

To provide delegates with a good working knowledge of how Covert Internet Investigations are carried out by UK law enforcements units and more importantly how this practice can be adapted to enhance their own investigations whilst adopting existing good practice.

Objectives

After attending the course the participant will be able to:

- ◆ Identify the function of the Internet and its applications.
- ◆ Describe the evidential requirements and admissibility of evidence during online activity.
- ◆ Describe the methodology for evidence capture and corroborations.
- ◆ Identify equipment and software required for effective online undercover investigations.
- ◆ Describe best practice in legend building and fieldcraft.
- ◆ Identify the legal issues pertinent to undercover online investigations.
- ◆ Describe the communications methodologies used.
- ◆ Prepare written statements for legal proceedings
- ◆ Identify the challenges and risks faced by online undercover investigators

Note: Delegates should expect to undertake a certain amount of preparatory work for this course which will depend on the exact requirements of each client. Much of the course is hands-on and delegates attending this course will undertake skills and knowledge checks. Certificates will be supplied to those who successfully complete the course.

Who should attend

This course is designed specifically to cater for those in law enforcement and other organisations who conduct covert internet operations, who wish to follow the procedures adopted by Law Enforcement Covert Internet Investigators.

Pre-Course Requirements

This is an advanced level course and is only intended to be undertaken by delegates who already have some Internet skills. Delegates attending this course should be able to demonstrate the knowledge and skills covered by TRL in their "Acquiring Online Information" course or demonstrate equivalent knowledge and skills.

Course Details

This course as designed consists of two x 3 day modules that can be taken as such or as a single course covering 6 days. Each course is adapted to meet the requirements of the client and therefore may vary in length. 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 Covert Internet Investigations course for the UK police service. He has delivered this training in the UK, Europe, Africa, the Middle East and Asia and has an excellent reputation as a trainer in this country and abroad.

James was also a member of the Skills for Justice Team that developed the UK National Occupational Standards for Covert Internet Investigator. He has produced this course in response to demands from colleagues who wish to comply or align with mainstream law enforcement practices.

All elements of training have been developed to conform to the National Occupational Standards for Countering E-Crime. (www.skillsforjustice.com). A broader outline of all areas covered in this training is described overleaf.

TRAINING OUTLINE - Covert Internet Operations

This course will cover the following subjects in sufficient detail for the student to be able to undertake the described activities with a full understanding of the methodologies, risks and dangers to them and others.

INITIAL STAGE - Theory and Good Practice

Covers the basic requirements for establishing a covert online capability including:

- Introduction to the Internet and its applications
- Covert Internet Operations
- ACPO CII Code of Conduct
- Hardware acquisition and use
- Operating Systems acquisition and use
- Software acquisition and use
- Evidence capture and Corroboration Methodology
- Cover Story Building and Fieldwork
- Risk assessment and authorities
- Matching equipment to the cover story
- Online payment methods
- Agent Provocateur & Legal Issues
- P.I.I. Issues and consideration for industry cases
- Open Source Capabilities – opportunities and risks

INTERMEDIATE STAGE - Communications

Examines specific issues of interest to undercover roles in respect of the following:

- Web Browsing
- E-mail
- Newsgroups
- ICQ and Instant Messenger
- IRC and Web chat
- Social Networking Sites
- Encryption
- Crossover Communications

FINAL STAGE – File Sharing

Includes application reviews, traceability, dangers and specific issues relating to:

- File Transfer Protocol
- Peer to Peer
- Internet Relay Chat
- Social Network Sites
- Bit Torrent Sites
- Online storage
- Cyber lockers
- Online auctions

Preparation of Statements and Evidence Session – Challenges to documents and statements

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