

Understanding Technology Enabled Crime

A Training Course for Investigators

Course Aim

This course is targeted at investigators within England and Wales Police Forces, as well as key contacts within ECD partners in both the wider public sector and industry. The course provides: an in depth understanding of how criminals exploit technology in the furtherance of crime; the range of technological tools and techniques open to them; the tools and techniques available to investigators to detect, intervene, disrupt, prevent and deter crime; and the collection and preservation of evidence from technology based systems to assist in criminal and civil court cases.

The individual learning aims and objectives can be summarised as:

- Enabling delegates to understand the jargon and slang applicable to technology enabled crime
- Providing orientation to the relevant technical concepts
- Giving an overview of tools and techniques in use
- Indicating the criminal groups, organised and otherwise, likely to exploit technology
- Overview of the law enforcement and other groups/agencies that exist to counter technology enabled crime
- In depth understanding of the methods that need to be applied during the investigation of technology enabled crime
- Impart knowledge of the types of intelligence and evidence that can be collected during investigations of technology enabled crime
- Provide knowledge of techniques used to assist surveillance, counter-surveillance, intervention disruption, prevention and deterrence
- Preview of developments in technology and likely scenarios of the crime it may enable
- Overview of legal and regulatory issues

Who Should Attend

This course is aimed at investigators and similar practitioners, especially those involved in the investigation of all types of economic crime. It is also useful for Senior Investigating Officers, ECD partners in the financial services, travel, entertainment and luxury/branded goods sectors, and others involved in the investigations process that are seeking to broaden their knowledge in this area. Delegates should already be generally familiar with the main principles of the law, conduct of investigations and computer based evidence handling.

Course Content

- Background to economic crime including current facts and figures
- Introduction of the primary technology resources used by criminals
- Hands-on exercise based on actual case histories
- Presentation by external expert on technology based investigation tools
- Including analysis of the technologies used by criminals within the investigation framework
- Detecting illicit technology use
- Collection and preservation of technology based evidence
- Intervention and disruption of criminal activities via the technology channels
- Deterrence and prevention of illicit technology use
- Hands-on access to open source technology tools

Training Documentation

Delegates will be given a comprehensive set of training documentation that includes the course notes and investigation resources.

Duration

3 Days

Course Syllabus

Day 1:

Introduction

The introductory session sets the scene and context for the remainder of the course and provides an early opportunity for the lecturers and delegates to get to know one another.

- Welcome to delegates
- Course aims and objectives
- Course programme
- Delegate introductions

Background of Economic Crime

The course focuses on the major crime areas that are enabled by technology: fraud and other economic crimes. This is done without forgetting that technology can be a factor in any crime, albeit with a lesser role. This and all subsequent sessions include the opportunity for delegate questions and answers.

- Definition of Economic Crime
- Classes of crime covered
- What crimes are not covered
- The perpetrators
- Latest statistics
- Contact points in the UK
- International context
- Cyber-crime relationships
- Legal and regulatory issues
- Questions and Answers Session

Introduction to Technology Enablers

This session provides orientation towards the major categories of technology that are exploited by criminals involved in economic or other criminal activities.

- Language orientation
- Definition of Technology Enablers
- Categories of technology exploits
- Good tools for bad purposes
- Bad tools for bad purposes
- Online dark markets
- Statistics of exploits
- How to stay ahead of the game
- How to turn the tables

- Questions and Answers Session

External Presentation Slot

An external expert provides illustrative demonstration of technology exploits on going in the real world (to be identified and confirmed for each course instance).

- Questions and Answers Session

Day 2:

Investigating Technology Exploits

This provides an introduction to the methods, tools and techniques that can be used to investigate technology enabled crime.

- Intelligence gathering
- Technology enabled surveillance
- Technology enabled counter-surveillance
- Using public domain resources
- Where to get expert advice
- What to look for at the physical and virtual crime scenes
- Alignment with the investigation method
- Case reviews
- Questions and Answers Session

Presentation Slot

This is a presentation given by the course lecturers of some open source tools, (available by definition for both legitimate and criminal use), that are installed on syndicate computers. Students will be provided with the opportunity for hands on access to these throughout the course.

- Demonstration of laptops loaded with open source technology tools
- All tools available for hands on use by course participants

Collection & Preservation of Technology Based Evidence

This session provides information on how to collect and preserve evidence during investigations of technology enabled crime, from the scene of crime through to presentation as evidence in court.

- Refresher on evidence handling
- Forensic support and ACPO guidelines

- Types and forms of technology evidence
- RIPA considerations
- Cross-jurisdictional issues
- Going to court
- Questions and Answers Session

Day 3:

Case Study

The case study is an opportunity to work through a scenario adapted from an actual case of a major technology enabled crime. Delegates will be given an overview of the crime and shown the sorts of tools and resources that could be used to carry out similar crimes.

Delegates will be given the opportunity to take on the role of “Investigator” and as a group will discuss what to look for as evidence and how to collect, preserve and examine it.

- Group discussion

Intervention and Disruption

This session provided an overview of intervention and disruption methods that can be employed in both specific investigation cases and as a means for crime reduction in general.

- Techniques for intervening in technology abuse
- Using technology against the perpetrators to disrupt criminal activities
- Real world case studies
- Questions and Answers Session

Prevention and Deterrence

The final presentation topic covers further crime reduction methods based on understanding motivations of the technology exploiters, means of increasing the probability of their discovery, putting into place awareness and reporting frameworks to aid rapid detection and introduction of the concept of “forensic readiness” that enables technology systems to be prepared beforehand to produce high quality evidence.

- NFA, NFIB and NFRC
- Deterrence and de-motivating factors
- Increasing likelihood of detection
- Best practices for preventing technology abuse
- Reporting frameworks

- Encouraging forensic readiness
- Questions and Answers Session

Conclusions

The course will complete with summary of the key learning points and reflection on how the content has contributed to meeting the original aims and objectives. This also includes a final opportunity for delegate feedback on the course and a final question and answer session.

- Review of course aims and objectives
- How technology enables crime
- How technology enabled crime can be investigated
- Issues relating to technology based evidence
- Methods for intervention and disruption of technology used to support criminal activities
- Preventing and deterring the use of technology for criminal purposes
- Feedback from delegates
- Final panel Questions and Answers session

Course Close

Delegates can take away the resources and other materials which they will have used on the course.

Coverage

The technological topic areas to be covered during the course include:

- Anonymous access
- Botnets
- Behavioural analysis
- Confidence tricks
- Computer misuse
- Computer fraud
- Cyber-activism
- Cyber-extortion
- Cyber-forgery
- Cyber-stalking and harassment
- Cyber-terrorism
- Cryptography abuse, steganography and covert channels
- Dark markets
- Denial of service
- Dumpster diving
- E-mail abuse, spam and phishing
- Electronic copyright theft
- Hacking
- Honeypots
- Information warfare
- Intrusion detection and prevention
- Logic bombs
- Man-in-the-middle attacks
- Online auction fraud
- Online banking fraud
- Online dating fraud
- Online fraud
- Online identity theft
- Online social networking
- Payment fraud
- Pornography and paedophilia
- Public key infrastructures and digital certificates
- Race hate
- Repudiation Reverse engineering
- Routing manipulation, eavesdropping, interception and domain name poisoning
- Social engineering
- Situational awareness
- Telecomms fraud and phreaking
- Tax fraud
- Virtual reality fraud
- Viruses, spyware, trojans and worms
- Web abuse, forgery and pharming