Course Outline

Cybercrime Investigator

Traditional investigative methods will always have a place in every investigation. However, with investigations now frequently including digital evidence and cybercrimes becoming increasingly prevalent, investigators need to have the knowledge, skills and abilities to properly deal with the digital information, intelligence and evidence they encounter; especially from and on the Internet.

This all needs to be to an acceptable, legal standard so that it can be used, presented and relied upon. It has to be gathered and considered consistently, efficiently and within the guidelines that are now international standards for all digital evidence. These investigators need to be able to speak to victims, witness and suspects with knowledge about the crimes they are dealing with and with credibility.

Our Cybercrime course offerings provide technically informative and professionally delivered 'mainstream' knowledge; then building upon that foundation to provide the cyber skills necessary to react to modern day crime and evidence sources and types. Courses are based at practitioner level and seek to address where the need for policing and industry skills require to overlap to provide the answer to the modern-day questions being posed to investigators. It is a must attend for all investigators dealing with digital evidence or any type; from the initial digital crime scene, through the enquiry, interview and evidence presentation process and on to the information that is available on the Internet as open source intelligence to assist and corroborate.

- **Course Duration** – this course can be delivered over 3, 4 or 5 days and can be tailored to the client's need or your specific requirements in terms of content or length

- **Target Audience** – designed for professional investigators in law enforcement and the private sector. Relevant to those who encounter digital evidence or Cybercrimes and who need to deal with digital materials at a search scene, gather online evidence, interview suspects and witnesses of Cybercrime or present to courts or tribunals. This course can be taught at foundation/entry level through to intermediate levels

- **Pre-requisites** – no specific computing experience is necessary; however, a working knowledge of Windows and Internet browsing would be beneficial. We will guide delegates from their existing levels of computing skills and build extensively on them

- **Trainers** – our qualified trainers are highly experienced practitioners with a strong background in intelligence, investigation and legal process. They have considerable experience in delivering their materials both nationally and internationally and are security cleared

What's in our Cybercrime Investigator courses?

• **Simplifying & Demystifying Computers**	What's in the box? How it works? How it connects? How it stores data, what it stores & where it stores it?
• **Basic Networking & the Internet**	How computers connect, how they speak & how they can be identified? How to find core Internet information?
• **Operating Systems**	Introduction to different OS including Linux & Apple at a base level. What they do & how they appear?
• **Wireless Networks & Technology**	Basics of identifying & investigating wireless connectivity & producing evidence from them
• **Cybercrime, Cyber Security & Hacking**	Trends & investigative possibilities – how to deal with victims, witnesses & suspects – collecting key evidence that can be used The legal aspects of online crime
• **First Responders & Search Scene Principles**	What to do? What not to do? How this has changed over the years? How to justify your actions at the scene?
• **Live Data Capture**	Equipping the investigator to deal properly with a live search scene & secure the maximum evidence correctly
• **Data Acquisition**	How it is captured? What we can take? Who should take it? What use can be made of it?
• **Encryption**	How it impacts us as investigators? Strategies for effectively dealing with it
• **E-Mail**	Discovering the possibilities & how to acquire it correctly for investigation
• **P2P Networks & Chat**	Introduction into the workings of Internet programs. How they are used by criminals & how to present evidence from them?
• **Darkweb & Cyber Currencies**	An introduction to the underground Web – how to get into it & what to look for?
• **Open Source Investigation**	An introduction to the basics of conducting open source investigation correctly. Will cover – Legality, Capture & Recording, Keeping safe & reducing footprints, Browsers, Searching, Social Media, Business Searches, Mapping & Photos
• **Assessment**	All delegates will undertake an assessment at the conclusion of the course to demonstrate a level of competence in the above skill areas

All modules on our courses contain theory but most importantly, practical, hands on experience that aids delegate learning.

Course Delivery

Courses can be delivered on-site or at a central location. Maximum student numbers are 12 per class.

For further details …..

Contact **Mark Cameron** Tel - **07825 742938** e-mail – **mark@mc-training.uk**

We don't want to just talk about it – we want delegates to actually do it; properly & professionally!