Course Outline

Digital Evidence Investigator

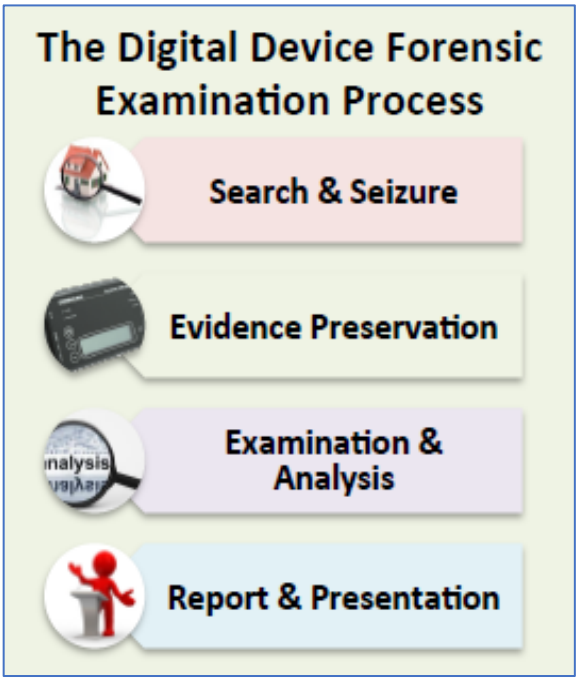
The ability to collect information and evidence from digital devices whilst maintaining the highest standards of forensic integrity and evidential continuity are crucial in today's criminal and civil investigations. Development of technology has seen more reliance on computers and other digital devices in daily life, which therefore provides significant opportunity in an investigative world.

These devices now provide critical and pivotal data in enquiries, providing evidence or intelligence whilst proving guilt or innocence. Dealing with them effectively and efficiently is key to all who are tasked in this process. Challenges to the way investigators have gathered or presented evidence from these devices are becoming more common and having the skills to do so competently is key.

This Foundation Course provides the basis for professionals to achieve comprehension of the techniques regarding recovery, capture, retention, analysis and presentation to meet the challenges of today's rapidly changing technological environment. The teaching closely follows current international standards and guidelines; providing delegates the ability to present those findings competently to an acceptable legal standard.

- **Course Duration** – this course can be delivered over 5 to 10 days duration, dependent on a client's need. The course can be tailored to the specific requirements of the organisation in terms of content or length. We try to make each course bespoke to meet with the training outcomes of each delivery

- **Target Audience** - this is a foundation course where delegates are expected to have minimal or no knowledge regarding digital evidence but be starting out in an investigative area where they will encounter digital devices. Ideal for those starting a career in High Tech Crime investigation; or their supervisors to provide technical knowledge. It also will be suitable for IT Professionals in security or investigative roles who may be concerned with identifying and securing data in a commercial environment



- **Pre-requisites** – there are no specific pre-requisites although some computer experience and a working knowledge of Windows would be an advantage to delegates attending

- **Trainers** – our trainers come from a digital evidence background gathered over many years. Each has extensive experience of device forensics and all have presented evidence as experts to the courts in the UK. As well as that experience as practitioners, they all have considerable experience in course design and training delivery in this area both in the UK and across the world and are security cleared

What's in our digital evidence course?

- **Identifying Digital Evidence** - Delegates will be provided with search & seizure scenarios and be expected to competently deal with devices in mock searches
- **Seizing & Securing Data** - Extensive discussion will assist delegates in identifying best practice at device seizure
- **Live Data Forensics** - An introduction to dealing with devices forensically at search scenes including 'doing the right thing' when encountering live devices
- **Evidential Principles & Continuity** - International digital forensic principles will be introduced, considered discussed throughout the course
- **Imaging & Hashing** - Understanding the basis of digital forensic examinations – the way data is captured & secured
- **Data Storage & Media Structure** - Dissecting how data is stored, read & understood – providing an understanding at a fundamental level to enable delegates to competently deal with digital evidence
- **Partitioning & Formatting** - How digital media is readied to receive data, along with the forensic implications of different structures & file systems
- **Common File Types** - Looking at the types of files that are found in criminal enquiries, and how they can be assessed for their provenance & evidential value
- **Metadata, Times & Dates** - Considering what information is held about data as well as providing an understanding of the issues of times & dates in forensic examination
- **Profiles & Users** - Understanding the role of users & administrators on a system – what user data means?
- **Registry & Artefacts** - Gathering & making use of non-standard system information & understanding its importance
- **Encryption** - Discussing the issues around encryption & dealing with encrypted material in investigations
- **Internet Data** - Information left behind by Internet usage & bringing it into the investigation
- **Data Carving & Reduction** - The principles of carving data from digital images & understanding how data sets can be reduced to aid investigation
- **Mac & Linux Forensics** - In introduction to dealing with the increasing issue of Mac devices as well as Linux operating systems
- **Reporting & Presenting Evidence** - Best practice in reporting the content of a digital evidence investigation & preparing the student to present their evidence to prosecutors & the Courts

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!