

IOCE Training and KSAs

1.0 Introduction

The IOCE acknowledges the following:

- Growth of electronic evidence to become the primary source of evidence of illegal activities;
- The growth of the transnational nature of crimes involving computer evidence;
- Mission critical ability to capture process and handle electronic evidence in a forensically sound manner;
- Significant increase in crimes occurring over and through the internet, and the consequential increase in the need for on-line investigations;
- Growing importance of education, including that given to computer forensic examiners, managers, prosecutors, the judiciary, and private industry assisting law enforcement and imperative to forge partnerships among law enforcement agencies and between law enforcement agencies and the private sector to combat computer based and/or facilitated crimes.

2.0. Principles of Training

Individuals must have education skills and abilities commensurate with their responsibilities and on the job training specific to their position. Management shall ensure that trained and equipped personnel are available in order to facilitate the operation of the agency. Managers must recognize that 18 months to 2 years is required to achieve full competency and agency succession plans should take this into account. All personnel have an ongoing responsibility to remain current in their field. In addition, agencies should provide support and opportunities for continuing professional development.

Any agency must train their personnel in the areas of seizing, accessing, storing or transferring digital evidence in compliance with these principles:

- Training in general forensic and procedural principles.
- Training in seizing and handling of digital evidence so that actions taken should not change that evidence.
- Documenting all activity relating to the seizure, access, storage or transfer of digital evidence.
- Training in expert testimony.

- A basic understanding of English written technical manuals is recommended.
- Commitment to time for Research and Development

2.1. Minimum Recommendations for Training

Depending on experience and job assignments the following are suggested annual minimum requirements.

- Junior Level – The first year, starting with 80 hours of formal training followed by two months on-the-job training. Each following year there should be at least 80 hours of continuing formal training.
- Mid Level – 80 hours of continuing formal training.
- Senior Level – 40 hours of continuing formal training.

The training can be provided from a variety of sources, including but not limited to:

- Courses taught at the post-secondary educational level
- Courses taught by vendors
- In-service training conducted by the employer
- In-service training taught by external provider
- Attendance at workshops

Continuous professional development can be accomplished through:

- Participating in relevant scientific meetings or conferences.
- Maintaining membership in at least one field related professional organization.

2.2. Minimum training topics

These minimum training requirements allow agencies to structure their training program to meet their needs as it relates to the type of casework encountered, equipment available, and the level of competency of trainees.

2.2.1. A written training program focusing on the development of the theoretical and practical knowledge, skills and abilities necessary to perform examinations to include:

- A training curriculum including descriptions of the knowledge and skills an examiner is to be trained in (specific topic areas), milestones of achievement, and methods of testing or evaluating competency.
- Agencies should have written standards of competence for each role, a documented training program and processes for assessing that the trainee has achieved the level of competence required. These will include:

- practical tests
- written and oral examinations
- practical court exercises
- casework conducted under close supervision a portfolio of previous casework

- A period of supervised casework representative of the type he/she will be required to perform.

- Documentation verifying that the trainee has achieved the desired competence per specific topic area.

2.2.2. Topic areas in the training program will include, as a minimum, the following:

- Relevant background information on digital evidence, to include hardware, software, and operating systems

Hardware
 Operating Systems
 Relevant Applications
 File Identification
 Relevant Media (Digital/Analogue)
 File Systems

- Techniques, methodologies and equipment utilized in the examination of digital evidence and related materials.

Forensic Analysis Procedures
 Best Practices (Technical Procedures)
 Standard Operating Procedures

- Quality assurance.

Quality Assurance (consistency within the forensic community)
 Technical Writing (for concise, clear reports.)
 Presentation Skills (for the explanation of factual information)
 General Forensic Principles and Practices (knowledge base)

- Expert/Court testimony and legal requirements.

Public Speaking (to build confidence in speaking situations)
Testimony Skills (to establish a comfort level for testimony)
Admissibility (Daubert) Hearing Testimony (issue awareness)
General Criminal Justice (legal issues, purpose, authority and result of examinations)
Basic Crime Scene management (understanding scene and evidence complexity)

- Agency policy and procedures (such as evidence handling, documentation, safety and security) as they relate to the examination of digital evidence and related materials.

Safety (for the purpose of risk management and personal safety)
Security (to preserve chain of custody)
Ethics (to conform to a standard of integrity)
Evidence Handling (to preserve integrity of evidence)
Training Documentation (to demonstrate compliance)

2.2.3. An individual qualified to provide instruction must have demonstrated competence in the subject area and in the delivery of training.

2.3. Cost

Agencies that will initiate and/or have established digital evidence programs must be financially committed to supporting the cost associated with training. Computer related criminal techniques and capabilities change more rapidly than those in more traditional areas of criminal activities. Therefore a considerable effort is required in the area of continuous specialized training.

2.4. Cooperation

In order to stay current with best practices and methods, a sharing of resources and information is necessary. A means to accomplish these goals must be a priority for IOCE. For example, The Guide to Forensic Computing Training Courses must be updated continuously, description of recognized courses will be included, and eligibility/requirements for attendees. Ultimately IOCE will strive to create a list of recommended courses. To improve international cooperation a broad scope of training should address:

- Making training programs available to other countries
- Sharing contents of training programs
- Accept English as the recognized standard for Computer Forensic Training
- Embrace private industry's expertise in Information Technology

3.0. Core Training Standards

It is recognized that the diversity in personnel, experience and equipment available throughout the world makes the task of reaching a consensus of opinion regarding how examinations should be carried out an enormous one. The underlying section of the document will set down minimum core standards for the training of Technical Specialists, Technician/Analyst/Assistant in an attempt to reach that consensus opinion. Periodic revisions to this document will be necessary to meet the rapidly changing technology.

3.1. Personnel

With respect to the personnel as defined by the ISO 17025 document the definition of the personnel included are to be:

Technician/Analyst/Assistant - an individual carrying out general casework examinations/technical work under the supervision of a reporting officer or a technical specialist and who is able to provide information to assist with the interpretation of the tests.

Technical Specialist - a forensic scientist/officer who has achieved levels of technical competency for specific equipment and services. They are able to write reports/statements of factual information in their specific specialist areas and can provide factual testimony in court. This person can have the authority and responsibility for the technical quality of digital evidence casework when the Section Head/Operations manager is not competent in technical aspects of digital evidence.

3.2. Qualifications, Competance and Experience

Technician/Analyst/Assistant - qualifications in a natural or applied science; knowledge of the theories, technology and procedures applicable to the examination of digital technology (hardware and software), the practical skills to operate specialist equipment and to carry out examinations safely and reliably in compliance with laboratory protocols; and an understanding of the requirements of the criminal justice system.

Technical Specialist - a minimum of a Bachelor's Degree (or equivalent) in a natural or applied science, or peer acceptance as an expert in the field of digital evidence/technology through experience and publication; a high level of knowledge of the relevant technology and procedures applicable to the examination of digital technology (hardware and software); extensive experience

in the field over at least a two year period and proven competence in the evaluation of results and conclusions in cases involving digital evidence

Recommended Knowledge Base – Given the qualifications, competence and experience detailed above in the Minimum Training Topics section the practitioner should be able to demonstrate, explain and document, as a minimum, the following:

- Solid familiarization with computer hardware
- Care and handling of computer systems
- Operate and understand from a command line OS
- Understand, maintain and explain the evidentiary chain
- Understand the methodology and terminology of the tools used
- Document the procedures taken
- Insure the forensic capture of data and verify that the integrity of the data is maintained throughout the entire process.

4.0. Specialized Training

Recognizing that agencies are facing challenges in accessing and processing highly specialized technologies, agencies must dedicate resources to the task of acquiring knowledge and expertise in these specialized areas. The following are some examples of specific areas that require additional training:

AVI (Audio/Video/Imaging)

PDA

- Handheld
Phone
- Telephony
- Telecommunications

Cryptography

Data Hiding

- Steganography

Emerging Technologies

- Biometrics

Various Operating Systems (Forensics)

- Mac
- Windows
- Linux
- Unix
- Etc.

Network Forensics

Wireless Networks
Network Security (Hacking Cases)

4.1. Court Training/Legal Issues

We recognize that the ultimate objective is presentation of Technical Evidence to judges and/or juries. Taking a proactive approach to educating the analysts, investigators, prosecutors and the judiciary is an essential requirement in addressing the growing complexity of issues including but not limited to;

- Foundational Requirements
- Court Room Simulations
- Technical Presentation Skills for Analysts
- Training for Prosecutors and Judges
- Demonstrative Evidence
- Archive for Appellate Use

Partnerships (investigate legal issues)

In an effort to aid in investigations, protect forensic value and create a liaison with business in research and development interests, we encourage training and partnerships in the following areas:

- Academia
- Corporate
- Industry Development

4.2. Management Awareness

Information for management is required for support of personnel and justification in the budgetary process with exposure to the following areas:

- Orientation to the Issues
- Generalization v. Specialization
- Field Analysis v. Lab Analysis
- Personnel Issues
- Redundant Personnel (Risk Assessment/Analysis/Management)
- Networking (with other Agencies/Analysts)
- Cross Trained Personnel
- Commitment of time to Research and Development

5.0 Recommendations Regarding Training

In an effort to create opportunities for expanding training to a greater number of agencies we would like to promote “Train the Trainer” and “Global Sharing” through “Trainer

Exchange.” We recognize there are some obstacles that need to be addressed such as; Jurisdictional Issues, Language Barriers and Cost.

5.1. Recommendations for cooperation in training:

- Industry members producing hardware, software, new or improved information technology or telecommunications services to make best efforts to inform and educate law enforcement personnel prior to launching of their products and services. Any current or emerging impediments to lawful access to evidence through technology shall be communicated to law enforcement on an expedited basis and appropriate training provided, as needed.
- Government and the IT/telecom industry to create a permanent venue, and allocate appropriate funding, to plan formulate content and deliver training to:
 - Law enforcement regarding emerging technologies, and
 - Industry regarding law enforcement needs
- Law enforcement agencies to support opportunities to exchange knowledge and/or personnel to facilitate growth of computer forensic capability world-wide;
- Law enforcement agencies and private industry to consider, where appropriate, temporary exchange of personnel to improve training and development opportunities;
- Law enforcement agencies and industry to meet annually to establish a dialogue which
 - facilitates exchange of information and concerns;
 - informs on their respective current and emerging issues;
 - Enhances understanding and seeks to minimize the barriers to cooperation

5.2. Training for the G-8/24-7 Points of Contact

Recognizing the role that the 24/7 points of contact have in the collection and exchange of electronic evidence IOCE recommends that training for the network shall include:

- Minimum understanding of the nature, perishability and use of digital evidence;
- General understanding of legal systems globally and the implications the differences or similarities in treatment of offences across borders have on the exchange of digital evidence;
- A significant understanding of the importance of evidence handling; chain of possession; and maintaining of the integrity of digital evidence;
- Understanding of the critical importance of providing information and intelligence on the further links in the chain (other countries involved) of illegal activities;
- Knowledge of the definition of terms relating to computer evidence of all countries which are members of the network and for engaging the requesting/responding country in a discussion of these definitions;
- Knowledge of note-taking/documenting techniques and creation of records of conversations and steps in the request/response process
- Confidentiality awareness training; and importance and impact of rules of disclosure.

6.0 Recommendations to the Board

- Coordination with international bodies/organizations (Interpol, COE, OECD, ENFSI, Europol, ODCCP) to establish a permanent working group with the purpose of making training programs available to other countries and share contents of training programs
- Encourage and support the creation of an International Certification Body for Forensic Training
- Establish a continuous updated webpage to include publications of training programs and other available training courses. For example, The Guide to Forensic Computing Training Courses must be updated continuously, description of recognized courses will be included, and eligibility/requirements for attendees. Ultimately IOCE will strive to create a list of recommended courses.

Source Description:

Information provided in this document originated from SWGDE Best Practices (Scientific Working Group for Digital Evidence), Guidelines for Best Practice in the Forensic Examination of Digital Technology (Association of Chief Police Officers), Convention on Cyber Crime (Council of Europe), Creating a safer information society by improving the security of information infrastructure and computer related crimes (European Commission), Computer Crime Manual (Interpol), G8 Proposed Principles for the Procedures Relating to Digital Evidence (G8).

The format of this document has been based around the ISO 17025 document produced by Dr L.W.Russell, Chairman, FCG Quality Sub-Committee, Member of ENFSI-FIT Working Group, Secretary IOCE, and Operations Manager, FSS in March 2002 and the guide produced by the ENFSI Fibres Group.