



IHCFC
THE INTERNATIONAL
HI-TECH CRIME AND
FORENSICS CONFERENCE



Forensic Computing Training Workshop

Guide to Forensic Computing Training Courses

Contents

This guide contains the following sections:

1. A simple definition of Jobs or functions that are performed within the science of Forensic Computing.
2. A simple outline of Skill sets required by each of those defined jobs to carry out their work.
3. A comprehensive directory of known courses, divided into the following sections:

Non Profit Making Professional Organisations
Law Enforcement and other Affiliated Agencies
Academic Institutions
Commercial Organisations

Within each of those sections, there is a brief listing for each organisation that has been identified as carrying out training, such as; name of organisation, contact name and /or telephone number or email address, type of training give, and where known a web site address.

The guide does not include courses that are to be delivered to in-house staff only, as it is believed that this information will be known to the officers within their own organisation.

4. An Appendix containing more detailed information

The appendix of the guide contains documentation from organisations that have responded to an email request for further information. The Email address of one of the workshop facilitators, Mr. Norton, has been included to allow anyone to contact the guide and contribute material.

laurie.norton@fct.btinternet.com

It is intended to circulate the guide to all organisations listed to confirm the accuracy of the information and invite them to contribute more information.

IHCFC Workshop - Guide to Forensic Computing Training Courses

Please bear in mind the following points:

That the material is believed to be correct at 8th October 1999, but that information may date or become inaccurate very quickly. Material will added, as it becomes known. The workshop could only include that they were aware of, and many organisations may have been unintentionally left out. Any further material is welcomed.

Distribution:

It is intended to include the guide and accompanying report on the IHCFC web site. However it is felt that this guide should be made available as a public domain resource so that as many law enforcement officers as possible may have access to the information. Methodologies for distribution are invited. Any event, the workshop feels that the guide may be freely copied and distributed by any officer where not for commercial gain.

Definitions of Functions

The workshop determined that an explanation of terms was required in order to assist Law Enforcement Officers and needs assessors to use the guide:

Forensic Computing: The Preservation, Recovery and Examination of Seized Computer Evidence.

Law Enforcement Officer: Any officer who may seize or preserve electronic evidence.

(Civilian) Support Staff/Contractor and/or Vendor: Provision of directed technical services, for example, recovery of data, media analysis, encryption and steganography.

Forensic Examiner/Analyst: Responsible for the recovery, analysis, and subsequent presentation of electronic evidence to a court of law.

Investigator: Responsible for the Investigation and/or direction of specialists involved with computer evidence examination. Ultimately responsible for the presentation of the case to the Prosecutor.

Prosecutor: A member of the legal profession who is responsible for presenting the case against the suspect in a Court of Law

Skill Sets (relating to function)

What skills do we need each of these people to have in order to do their respective jobs?

Law Enforcement Officer: Be able to recognise electronic equipment; Computers, Laptops, Cell Phones, PDA's (Electronic Organisers), Fax machines & Digital Storage devices. Knowledge of procedures in order to preserve/safeguard potential electronic evidence/scenes.

(Civilian) Support Staff/Contract and/or Vendor: Possess technical skills that are requirement driven in support of a Forensic Computer investigation.

Forensic Examiner: Skills for using particular operating systems and procedures in order to image/copy, recover and analyze electronic evidence. To subsequently be able to present that evidence in a Court of law in such a way that it may be easily understood by the court.

Investigator: Have a good knowledge of the laws governing computer related crime. Case management skills, which include, amongst other things, an understanding of the nature of computer related investigations in terms of the law, confidentiality, relevance and the distinction between information, intelligence and evidence.

Prosecutor: Basic knowledge of forensic computer concepts together with an understanding of laws relating to computer crime. A familiarity with legal issues pertaining to seizure and search of computer systems and digital evidence.

COURSES

Training from Non Profit Making Professional Organisations

Training from Non Profit Making Professional Organisations

International Association of Computer Investigative Specialists (IACIS)

Course subjects: Certified Electronic Evidence Collection Specialist Courses, Certified Forensic Computer Examiner Courses, Advanced External Training Courses.

Contact: WILLIAM TAYLOR / admin@cops.org

Prerequisites: Employed by Law Enforcement agency.

Web Site: www.IACIS.com

High Tech Crime Investigators Association (HTCIA)

Course subjects:

Contact: Anthony R. Gentilucci / tony_gentilucci@hp.com

Prerequisites:

Web Site: www.HTCIA.crg

National Cybercrime Training Partnership

Washington, DC 202 514 0823

National White Collar Crime Centre (NW3C)

Computer Crime Centre, Fairmont, WV

Course subjects: Multiple courses on computer crime, ranging from basic to advanced.

Contact: BILL CRANE / admin@cybercrime.org Tel: 800 221 4424

Prerequisites:

Web Site:

DCITP (Department of Defence Computer Investigation Training Programme, USA)

Course subjects: Numerous courses covering a wide range of Forensic Computing issues.

Contact: GREG REDFERN

IHCFC Workshop - Guide to Forensic Computing Training Courses

Prerequisites:

Web Site:

Information Systems and Security Association (ISSA)

Course subjects: Variety of information and security courses. Selection of Forensic computing courses.

Contact: Howard Schmidt / howards@microsoft.com

Prerequisites:

Web Site: www.issa.org

Association of Certified Fraud Examiners (ACFE)

Course subjects: European Fraud Conference, Cyber Fraud, Cyberfraud in the 21st Century, Fundamentals of Computer Fraud, Video/workbook Computer Crime.

Contact: (1) 800 245 3321 memberacfe@aol.com

Prerequisites:

Web Site: www.acfe.com

Search Group: National Consortium of Justice/Statistics and Information

Course subjects: Internet investigation.
Advanced internet investigation.
Child exploitation - under development.
Network security course.

Contact: Twla R Cunningham / twyla.cunningham@search.org

Prerequisites:

Web Site: www.search.org

Training from Law Enforcement/Agencies

Training from Law Enforcement/Agencies

FBI Federal Bureau of Investigation (USA)

Course subjects: A variety of courses are on offer from various departments - CART offer in house training on all aspects of forensic computing (limited outside agency places) - QUANTICO offer a number of computer investigation courses - NIPC provide classes on computer intrusion.

Contact: CART - PAUL FRIELDS (1 2023249308)
QUANTICO - AL JOHNSON
NIPC - N/K.

Prerequisites: Nil.

Web Site: www.fbi.gov

FLETC (Federal Law Enforcement Training Centre)

Glynco, GA

Course subjects: 4 week Basic Seize Computer Evidence Recovery School (BSCER).
3 week Advanced Seize Computer Evidence Recovery School (ASCER).
Both open to outside agencies.

Contact: dfischer@fletc.treas.gov Tel: 800 74 FLETC

Prerequisites: BSCER - Nil, ASCER - Must have attended BSCER.

Web Site: www.treas.gov/fletc/

BRAMSHILL, POLICE TRAINING COLLEGE (UK)

Course subjects: 1 Week Computer Examination and Investigation Course.
2 week Advanced Examiners Course.
Both open to outside Law Enforcement only.

Contact: RAY BELL. +44 1252 842931

Prerequisites: Basic - Nil, Advanced - Must have attended basic course.

Web Site:

FFI (Financial Fraud Institute, USA)

Course subjects: 2 week Seize Computer Evidence Recovery Course - Open to other agencies.

Contact: cybercop@sprynet.com

Prerequisites: - Nil.

IHCFC Workshop - Guide to Forensic Computing Training Courses

Web Site: <http://all.net/esoi/>

RCMP (ROYAL CANADIAN MOUNTED POLICE, Canada)

Course Subjects: Basic Forensic Computing Course.
Network Course.
Apple MAC Course.
INTERNET Course.

Contact:

Prerequisites: Basic - Nil, Others - Must have attended Basic and also complete a passing in test (75%).

Web Site:

NATIONAL POLICE ACADAMY (Japan)

Course Subjects: Several courses in Forensic Computing and Networks - Not open to other agencies.

Contact:

Prerequisites:

Web Site:

ACADEMIC INSTITUTIONS (Worldwide)

ACADEMIC INSTITUTIONS, Worldwide

UNIVERSITY OF CENTRAL FLORIDA

Course Subjects: Forensic Computing Course - Open to all.

Contact: Dr JOHN LEESONE

Prerequisites:

Web Site: www.ucf.edu

CRANFIELD UNIVERSITY/ RMCS

Course Subjects: 2 week Forensic Computing Foundation Course.

1 week INTERNET Forensic Evidence Course.

1 week Networking Course.

Contact: STEVE BUDDPELL , sbuddell.ir.ac@gtnet.gov.uk

Prerequisites: Law Enforcement only.

Web Site:

QUEEN MARY & WESTFIELD COLLEGE (London)

Course Subjects: Specific Courses as requested by Law Enforcement.

Future academic course - details n/k.

Contact: Dr IAN WALDEN i.n.walden@qmw.ac.uk

Prerequisites:

Web Site: www.qmw.ac.uk

STRATHCLYDE UNIVERSITY (Glasgow, Scotland)

Course Subjects: Both under and postgraduate courses - details n/k.

Contact:

Prerequisites:

Web Site: www.cs.strath.ac.uk

GLAMORGAN UNIVERSITY (South Wales)

Course Subjects: MSC on Computer Forensics and Computer Law.

Contact: ANDREW BLYTH

Prerequisites: Recognised degree.

Web Site: www.glam.ac.uk

UTICA COLLEGE (USA)

**Course Subjects: White Collar Crime & Fraud Course.
Computer Crime Course.**

Contact: GARY GORDON / ggordon@utica.ucsu.edu

Prerequisites:

Web Site:

REDLANDS COLLEGE (USA)

Course Subjects: Computer Crime Course.

Contact: webmeister@uor.edu

Prerequisites:

Web Site: www.redlands.edu/

UNIVERSITY OF NEW HAVEN (USA)

**Course Subjects: Graduate Certificate in Forensic Computer Investigations.
Graduate Certificate in Information Protection and Security.
On-Line MS Degree in Information protection and Security.
11 Additional Courses (some on-line) dealing with the whole spectrum of Computer Crime.**

Contact: Dr THOMAS A. JOHNSON / taj@charger.newhaven.edu/california

Prerequisites: Vary depending on type of course - details on asking.

Web Site:

GEORGIA TECH UNIVERSITY (USA)

Course Subjects: Forensic Computing Course.
Course on Information security.

Contact:

Prerequisites:

Web Site: www.cc.gatech.edu

CARNIGIE - MELLON (USA)

Course Subjects: Training offered on network intrusion.

Contact: scs@cs.cmu.edu

Prerequisites:

Web Site: www.cs.cmu.edu/scs/scs.html

COMMERCIAL COURSES

COMMERCIAL COURSES

COMPUTER FORENSICS LTD. (UK)

Course subjects: Disk Image Backup System (DIBS) Modules 1,2,3,4.

Contact: PETER VERRICK / info@computer-forensics.com

Prerequisites: Nil.

Web Site: www.computer-forensics.com.

CompuForensics (USA)

Course subjects: Customised development and provision of graduate level computer forensics certification training for investigators (1-3 weeks with comprehensive exercises/exams) and 1-3 day seminars for managers at the customer's facility or home city (instructors travel to customer's location)

Contact: John J. Seither (cybercop@CompuForensics.com)

Prerequisites: Computer literate law enforcement and selected corporate security officers; well equipped computer classroom required for investigator's courses and recommended for manager's courses

Web Site: www.CompuForensics.com (see appendix 5)

Litton/TASC

Course subjects: Computer Forensics for Managers (4-12 hour) and Computer Forensics for Investigators (one week)

Contact: Gregory K. Lipscomb (gklipscomb@tasc.com)

Prerequisites: Law enforcement and selected corporate security

Web Site: www.tasc.com

ENCASE

Course subjects: Computer Forensics Training Course (3 days).

Contact: STEFANIE BAUER / info@guidancesoftware.com

Prerequisites: Nil.

Web Site: www.guidancesoftware.com

MITRETEK

Course subjects: Forensic Computing Course.
Network Course.
Specific Operating Systems Courses.

Contact:

Prerequisites:

Web Site: www.mitretek.org

NTI (New Technologies Incorporated, USA)

Course subjects:

Contact: MICHAEL ANDERSON

Prerequisites:

Web Site:

VOGON INTERNATIONAL (UK)

Course subjects: Vogon Imager/ GenX Courses.

Contact: MARIA COOK / maria.cook@vogon.co.uk

Prerequisites: Nil.

Web Site: www.vogon-international.com

END OF GUIDE

Appendix

Table of contents

Appendix 1: Survey for the Identification of Computer Forensic Courses

Appendix 2: Copy of a letter sent to known training organisations in anticipation of the workshop.

Appendix 3: IACIS

Appendix 4: NWCCC

Appendix 5: CompuForensics /Wright State University

Appendix 1:

Survey for the Identification of Computer Forensic Courses

Supported by the National Centre for Forensic Science- (partnership between the University of Central Florida & National Institute of Justice).

Survey distributed by Dr Gary Gordon, Utica College, Utica, NY, USA, in association with Dr. John Leeson (leeson@cs.ucf.edu).

Introduced by Carrie Whitcombe.

This survey is currently underway. Your participation in the survey is requested, and survey forms can be obtained from : ggordon@utica.ucsu.edu.

The purpose of the survey is to identify the availability of current courses, training needs and develop future courses to meet those needs.

The IHCFC workshop supports the work of this survey.

Appendix 2:

Detailed below is a copy of a letter sent to known training organisations in anticipation of the workshop.

Dear Sir/Madam,

You may be aware of the International High Tech Crime and Forensic Computing Conference, beginning next week at Heathrow, London. (<http://www.ihcfc.com>). I am a facilitator of a workshop which will run on Tuesday and Wednesday next week which will be tasked with the aim of compiling a directory of Forensic Computing training courses. It is hoped to be as comprehensive as possible, but must rely upon the information available to the workshop delegates who will be attending from a number of nations, (currently 19 countries).

Please can you send me information on any courses you may run so that I can make this information available to the workshop. The exact format and content of the directory will be decided upon by the workshop delegates, but it is intended to be made available via the conference web site to law enforcement. It is anticipated though, that the type of information that may be included would include; length and cost of the course, subject matter covered, contact details, target candidates, restrictions applicable (i.e. Law enforcement only or open to commercial candidates), Any links to Web pages or any other information you may feel is relevant. We seek this information equally from commercial or co-operative/law enforcement centres of training, and I will ask the workshop to consider including information relating to training on specific commercial products that you may have available. The only proviso is that the course must relate to Forensic computing. A sister workshop will be considering training courses dealing with the area of Internet Investigation and I will be happy to pass any information on specific to that group.

This information you supply will be used only for the purposes of informing law enforcement and will not be made available for any commercial purpose. It is intended that some information on the web site will be restricted to law enforcement personnel only, through restricted site access and some will be within the public domain. If you wish to place a restriction on the circulation of your course information, please make that clear when you reply.

I would prefer to receive replies electronically, and I will still be able to include your responses up until Tuesday afternoon 5th October 1999, (UK time).

Thank you for your attention to this letter.

Etc.

Appendix 3:

IACIS

IACIS is an international volunteer non-profit corporation composed of law enforcement professionals dedicated to education in the field of forensic computer science. IACIS members represent Federal, State, Local and International Law Enforcement professionals. Regular IACIS members have been trained in the forensic science of seizing and processing computer systems.

The Beginning

IACIS began in 1989 when a group of federal, state, local, and international law enforcement officers graduated from the first class in seized computer and data recovery at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. These graduates and instructors immediately realized the demand for training in this field, and that no single agency would be able to provide the training, support, and continuing education required to keep law enforcement on the forefront in a rapidly changing world. These law enforcement professionals formed a non-profit corporation dedicated to the education and training of law enforcement in the area of computer forensics.

Why We Exist

IACIS is dedicated to the education and certification of law enforcement professionals in the field of computer forensic science. Virtually all law enforcement agencies have encountered criminals that use computers in the commission of a crime, or that commit computer crimes. Many agencies do not have officers trained personnel to deal with computer evidence in accordance with the laws of search and seizure, and the rules of evidence. IACIS exists to create and establish procedures, train personnel, and certify expert witnesses in the recovery of evidence from computer systems.

What We Offer

IACIS offers professional training in the seizure and processing computer systems. This training incorporates forensic methods for searching seized computers in accordance with the rules of evidence and laws of search and seizure. This includes evidence that has been hidden, concealed, encrypted, protected with passwords, software time-bombs, trojan horses, tsr's or other destruction devices that could destroy either the evidence, the physical computer, or both. IACIS provides an opportunity to network with other law enforcement officers trained in computer forensics, to share and learn from other experiences, and develop a pool of expert assistance to draw upon. IACIS members involved in research and development have designed specialized software, evidence searching tools and programs that are only available to IACIS trained law enforcement professional.

IHCFC Workshop - Guide to Forensic Computing Training Courses

IACIS trains members of law enforcement agencies around the world in the forensic seizure and processing of computers as evidence. These classes include seizing computers, seizure and processing computers, computer

Certified Electronic Evidence Collection Specialist Courses

Certified Forensic Computer Examiner Courses

Advanced External Training Courses

Appendix 4

NWCCC

Basic Data Recovery and Analysis (Formerly Cybercop 101)

Preparing Investigators for the Challenges Created by Computer Literate Criminals. Now Sponsored by The National Cybercrime Training Partnership.

In this computer-literate age, sophisticated criminals are using computers in their illegal activities. Advances in computer technology have provided criminals with a powerful tool. Reported incidents of high-technology theft and computer-related crime are increasing dramatically and successful investigations and prosecutions will be dependent on investigators' computer skills. This class will expose participants to the unique skills and methodologies necessary to assist in the investigation and prosecution of computer crime.

The course includes hands-on instruction and discussion about such topics as evidence identification and extraction, hardware and software needed to do a seizure, how to recover erased files, how to overcome encryption, high-tech legal issues, and more. If you are a criminal investigator, prosecutor, or support staff whose duties include the investigation and prosecution of high-technology crimes and the seizure of electronic evidence, this course could be of benefit to you.

Contact the NWCCC Computer Crimes Section at: 304-366-9094 (voice) or 304-366-9095 (fax) for additional information. The mailing address is 1000 Technology Drive, Suite 2130, Fairmont, WV, 26554.

CompuForensics /Wright State University

TRAINING OPPORTUNITY

Recently, CompuForensics began work with Wright State University to develop cost-effective college level computer forensics and Internet crime training for criminal and corporate investigators. The initial course offering, a 3-day seminar at Wright State University in Dayton, Ohio, provides critical skills needed to safely locate and secure computer evidence at the search site. This first seminar (Computer Forensics Initial Response Team, Wright State #AK2198) is scheduled for June 20-22, 2000 at Wright State University. This course is being held in an exceptionally well equipped computer classroom affording every student a late model server class computer. As the first seminar in its series, the material will be less than three months old during the June presentation. Conversely, the course benefits from lessons learned in providing basic and intermediate level computer forensics training to federal, state and local law enforcement agencies during the previous year.

Due to the potentially sensitive nature of the material covered and student interaction, course attendance is restricted to law enforcement and selected corporate investigative personnel. Although prior computer forensics training or experience is not required, attendees should possess a working knowledge of DOS command line and Windows graphical user interface operations. Upon successful course completion, students will be prepared to conduct a preliminary on-site analysis and seizure of DOS/Windows computer systems through the soon to be released Windows Millennium. For additional information or registration, download a course agenda from www.CompuForensics.com/TRAINING.HTM or contact:

Alan J. Yeck, Program Developer
Wright State University
Center for Professional Development
140 E. Monument Ave.
Dayton, OH 45402
Tel: (937) 775-1113
Fax: (937) 775-1111

John J. Seither, II	Tel/Fax: 931-484-4859
CompuForensics.com	Cellular: 931-260-2635