



ICAC Investigative Techniques

City, State

Date

Time	Agenda Item
Monday, Date	Day 1
8:00 am – 8:30 am	Welcome & Overview of Course – On-Site Training Coordinator
8:30 am – 12:00 pm	<p>Computer Crimes Against Children – Instructor 1</p> <p>This module will provide new members of Internet Crimes against Children (ICAC) Task Forces and their affiliate agencies with an understanding of the mission and history of the ICAC program. Participants will be presented with an overview of child sex offender typology and behavioral characteristics, including their relevance to computer-facilitated crimes against children. Specific issues of victimization, including compliant victims, will be presented. The related issues of child pornography and child erotica, both in computer and traditional cases, and their relationship to actual sexual abuse crimes will be examined. The importance of victim identification as a goal of every ICAC investigation will be discussed. Actual case examples will be utilized throughout this presentation to illustrate the learning objectives of this module.</p>
12:00 pm - 1:00 pm	Lunch (on own)
1:00 pm – 5:00 pm	<p>Legal Issues: Winning in Court – Instructor 2</p> <p>Participants will be provided with a comprehensive overview of privacy issues, search and seizure issues, and the legal exposure attendant with the investigation and prosecution of computer facilitated sexual exploitation of children. Participants will be instructed on the most recent court rulings in relevant cases and what the legal analysis means for the investigative protocol for law enforcement. Classic and evolving defenses will be examined and instruction on how to rebut these defenses in and out of court will be discussed. Special emphasis will be placed on warrantless acquisition of evidence, to include consensual searches, deception tactics and knock and talk investigations. Testifying in court will be examined. Jurisdiction and partnering will be addressed to empower local and state law enforcement to successfully investigate and prosecute computer exploitation cases.</p>
Tuesday, Date	Day 2
8:00 am – 12:00 pm	<p>Introduction to the Internet – Instructors 3 & 4</p> <p>This block of instruction will introduce participants to how the Internet works as it relates to online investigations. Key concepts covered are IP addresses, the Domain Name System, WHOIS services, ports, and investigative tools. By the end of this block participants will be able to perform IP address tracing, domain name resolution, and explain the role of ports in identifying the IP addresses of systems they are connected to. <i>(computer lab)</i></p>
12:00 pm – 1:00 pm	Lunch (on own)

Time	Agenda Item
1:00 pm – 2:00 pm	Introduction to the Internet (cont'd) – Instructors 3 & 4
2:00 pm – 3:00 pm	<p>Wireless Basics – Instructors 3 & 4 This module provides participants with information regarding the significance of today's wireless technology and crime and how it can impact investigations. Issues related to the "Some Other Dude Did It" defense are explained as they relate to 802.11 wireless networks. <i>(computer lab)</i></p>
3:00 pm – 5:00 pm	<p>Instruments of Child Exploitation - Peer-to-Peer – Instructors 3 & 4 This module provides participants with an introduction to peer to peer file sharing networks and clients with a focus on the Gnutella network. Together with the tools provided in prior blocks of instruction the student will learn how this network operates, the current methods used to investigate the dissemination of child pornography in this network and how to effectively respond to a P2P referral. This module will also outline the requirement for a search warrant and provide samples which can be used by the student. This module will also discuss related concepts including, hash values, geographic mapping of IP addresses and the "netstat" command.. <i>(computer lab)</i></p>

Wednesday, Date	Day 3
8:00 am – 8:30 am	Review of Tuesday – Instructors 3 & 4
8:30 am – 12:00 pm	<p>Instruments of Child Exploitation – Yahoo, MySpace & Craig's List – Instructors 3 & 4 This module is designed to guide the new ICAC investigator on how to conduct a reactive investigation into a suspect who is using a Yahoo identification. The investigator will learn how to search throughout Yahoo and find any and all information the suspect may have placed on Yahoo's server which would aid in identifying and locating them. The investigator will also learn how to preserve that information for their investigation. At the conclusion the investigator will be given a mock Cybertip using a Yahoo Group name and will have to try and find out as much information as they can about the suspect by using the techniques they learned during this module. <i>(computer lab)</i></p>
12:00 pm – 1:00 pm	Lunch (on own)

Time	Agenda Item
1:00 pm – 5:00 pm	<p>Corroborating the ICAC Investigation – Instructor 5</p> <p>This module of instruction will provide participants with investigative strategies to corroborate the ICAC investigation through one party consent phone calls, knock and talks and suspect interview/interrogation. Participants will be guided through the development of an interrogation strategy utilizing themes, alternative questions and deception. Many successful cases also involve the use of voluntary compliance and admissions made by the suspect as part of “knock & talk” investigations. Through lecture, class discussion, role playing and the illustration of actual cases, the instructor will equip participants with the tools and skills they need in this important area of child exploitation investigations</p>

Thursday, Date	Day 4
-----------------------	--------------

8:00 am – 11:00 am	<p>NCMEC Source of Leads Investigation of CyberTips – Instructor 6</p> <p>The focus of this block is to provide participants with an understanding of the mission, Internet knowledge, and free services provided by the Exploited Child Unit (ECU). Also covered in this presentation will be an overview of the National Center for Missing & Exploited Children (NCMEC). Participants will be provided information on the CyberTipline, including how it can generate, deconflict, and corroborate cases related to computer-facilitated crimes against children. In addition, an in-depth overview of CyberTipline reports will be included with a line-by-line explanation of the reports sent to ICAC Task Forces. The related issues of child pornography and child erotica, both in computer and traditional cases, will be discussed. Actual case examples will be utilized throughout this presentation to illustrate the learning objectives of this session. Participants will also learn about the ways NCMEC’s Child Victim Identification Program (CVIP) can provide a critical role in child pornography prosecutions. Case examples will demonstrate how previously unidentified child victims were rescued as a result of Image Analysis. Tools developed by CVIP that will help law enforcement prove distribution charges in their child pornography cases will be demonstrated. Specific instructions will be given on how participants can submit copies of child pornography images to CVIP for analysis.</p>
--------------------	---

11:00 am – 12:00 pm	<p>ICAC Data Network Toolkit – Instructors 7 & 8</p> <p>This class will focus on the first two tabs of the toolkit, Moniker and IP Address. Moniker tab instruction will teach students how to check the lookup history of a username, both individually, and as an imported file retrieved from a computer forensic examination. IP tab instruction will teach students how to both check the historical lookup of an IP address, as well as performing a “Geo Locate” on it. Students will be shown how to perform the checks individually, and as imported from a file. Students will obtain familiarity with SHA and GUID lookups as well. Detailed instruction of this functionality will be address during the courses of instruction requiring their use.</p>
---------------------	---

12:00 pm – 1:00 pm	Lunch (on own)
--------------------	-----------------------

Time	Agenda Item
1:00 pm – 4:00 pm	<p>Knoppix – Instructors 7, 8 & 9 Knoppix is a Linux based tool that allows Investigators or Probation/Parole officers to safely preview a subject’s computer at a scene. This tool can be used to search for both text and images on the subject’s computer without changing any original evidence. Investigators and Probation/Parole officers need this ability as it may influence an interview or help in establishing probable cause on whether to seize a particular computer. The student will learn how to install the program and become familiar with its use in the field. <i>(computer lab)</i></p>
4:00 pm – 5:00 pm	<p>Knoppix Practical Exercise – Instructors 7, 8 & 9 The practical exercise is designed to evaluate if the students will be able to use the knowledge and tools they were taught during this class in the real world. Students will demonstrate their ability to use KNOPPIX to preview the contents of the hard drive of a computer and preserve the evidence they may find. <i>(computer lab)</i></p>

Friday, Date	Day 5
---------------------	--------------

8:00 am – 9:00 am	<p>Building Your ICAC Case – Instructors 7 & 8 Responding to reactive cases reported through the CyberTip Line, complaints made by the public or during any type of proactive investigations require investigators to identify the location of the suspect and specific computer involved in the investigation. With the use of Yahoo and AOL reports participants will learn what steps must be taken in order to obtain the critical information needed in child exploitation investigations. Samples of court orders and subpoenas along with the Yahoo and AOL compliance guides will be given out to the participants.</p>
9:00 am – 10:30 am	<p>Crime Scene Response and Management – Instructors 7 & 8 This module provides participants with an overview of electronic evidence. Participants will be taught how to prepare for and respond to a computer crime scene. They will be able to identify, document, and properly seize computers and related evidence.</p>
10:30 am – 11:45 am	<p>Case Practical Exercise – Instructors 7 & 8 This module will provide participants with a practical table-top exercise that will challenge them to use the information that they learned during the training to “investigate” a computer facilitated crime of child sexual exploitation. Participants will have to apply both their sex crimes investigative skills and their technical understanding of computers and the Internet to “solve” this case. <i>(computer lab)</i></p>
11:45 am – 12:00 pm	<p>Evaluations and Certificates – On-Site Training Coordinator</p>