

Digital Forensics in Child Pornography Cases

Lars Daniel, EnCE, ACE, AME, CTNS, CTA, CWA, CIPTS

Or

Larry Daniel, EnCE, ACE, DFCP, BCE, AME, CTNS, CTA, CWA

Course Objectives

The purpose of this class is to educate legal professionals on how digital evidence can play a critical role in child pornography cases. This class will cover common forensic artifacts found on computers, cell phones, and other electronic devices commonly seen in child pornography cases.

In this class attendees will learn about how law enforcement agencies perform online investigations for child pornography and child solicitation. The underlying technology and the evidence created by it will be covered, with particular interest paid to peer to peer file sharing. Case examples are used to illustrate the complexity of child exploitation cases, including issues related to user attribution, file distribution, and forensic artifacts related to the viewing and downloading of contraband. A section of the class is dedicated to how this evidence can be challenged using actual case examples.

1. Introduction (10 Minutes)

- a. This section will explain the major entities involved in child pornography cases and investigations. This will cover organization such as NCMEC (National Center for Missing and Exploited Children), ICAC (Internet Crimes Against Children), and others. Also covered will be the practical implications of the Adam Walsh Act on the examination of digital evidence in child pornography cases.

2. Peer to Peer Online Investigations and Forensic Artifacts (20 Minutes)

- a. This section covers the underlying technology behind the most prominent type of case, peer to peer file sharing. Attendees will learn how law enforcement performs online peer to peer examinations and how they are able to identify a suspect based upon peer-to-peer network activity.
 - i. Attendees will learn how law enforcement only software works that is used to monitor peer-to-peer networks.
 - ii. Attendees will learn how a law enforcement uniquely identifies a single location via their investigation, and how they are able to download from a single source from a peer-to-peer network.
 - iii. Attendees will learn how file hashing plays a critical role in the monitoring and identification of child pornography on peer-to-peer networks, and the implication this has for the authentication of videos and images in child

pornography cases.

- b. Attendees will learn about numerous types of forensic artifacts and importance they play in child photography cases. Forensic artifacts explained include Internet history, event logs, link files, shell bags, user assist data, peer-to-peer program forensic artifacts, application and search engine-based activity, and more.

3. Case Examples / Analysis and Examination (30 Minutes)

- a. Attendees will learn from actual case examples the importance of the various forensic artifacts covered in this class and how they are used to determine user attribution, intentionality, known versus unknown activity, and more.
 - i. Case example involving the transmission of contraband images via cell phones in a solicitation case, and the evidence used to determine if it was intentional receipt and possession or not.
 - ii. Case example involving the misidentification of forensic artifacts related to the Ares network by a law-enforcement examiner, and the ultimate dismissal of the case based in part upon our examination.
 - iii. Case example related to sentencing mitigation, in particular what a client was actually searching for versus what they received on the computer in the form of compound files and file naming conventions on peer-to-peer networks.
 - iv. Case example related to the improper interpretation of forensic artifacts in a case involving possession, distribution, and receipt of child pornography charges where I gave expert testimony, ultimately leading to a not guilty verdict for all indictments.

4. Question and Answer (5+ Minutes)

- a. As time allows, questions will be taken from the participants of the class.