High Tech Crime Investigations for Supervisors

COURSE OUTLINE

Course Length 4 hours

I. Introduction
   A. Purpose
      1. To provide basic training to police supervisors to better understand, identify and lead the investigations of high technology crimes.
   B. Attendees Expectations
      1. Upon completion, personnel will have a working understanding of what constitutes a high tech crime, how technology is used in conventional crimes, and discuss evidentiary and legal issues with technology in criminal investigations.
      2. Personnel will have the ability to successfully define and identify a high tech crime and lead the investigation of it. They will also understand how technology is used in conventional crimes.

II. What is a high tech crime?
   A. Background and Introduction
      1. Background of technology and the Internet
         a. What is the Internet?
         b. Where did it come from?
         c. Technology crime evolution
         d. IP Numbers and other new terms
      2. What are high tech crimes?
         a. Hacking and intrusions
         b. Phishing and fraud
         c. Child porn trafficking

III. Search and Seizure Issues
   A. Search Warrants
      1. IP search warrant
      2. E-mail search warrants
      3. Computer search warrants
      4. Technical considerations
   B. Seizure of High Tech Equipment
      1. What to take
      2. What to look for
      3. Evidence collection and handling
      4. Legal Issues
      5. Computer forensics overview

IV. Internet Crimes Against Children (ICAC)

A. Overview of ICAC
    1. What it is
    2. What is Pasadena's connection?
    3. How are cases handled in ICAC?
    4. What resources are available to public and law enforcement

V. Conclusion and ties to Conventional Crimes
A. Technological connection to conventional crimes
    1. Computer use in other crimes
    2. Researching video and similar evidence
B. Conclusion
    1. Future considerations
    2. Questions and conclusion