

ICAC Investigation Guideline

Cybertips	Referrals	Citizen Complaints	UC Work
-----------	-----------	--------------------	---------

Investigative Step	Thoughts and Resources
Case Assessment	Is it a crime? Is it in your jurisdiction? Is it an ICAC case? Is there enough information to proceed?
Initial Investigation on Screen names, email addresses, web sites, people, etc.	Phone calls to referents, witnesses, victims, NCMEC, etc. open source searches
Issue Search Warrants / Subpoenas to Hotmail, AOL, Yahoo!, My Space, Face Book, etc.	Profiles, subscriber info, additional screen names/emails, <u>connection logs</u> . Use compliance guides on class resource CD. Issue Preservation letters ASAP.
Check subscriber info. Check <u>connection logs</u> for recent/frequent IP addresses	Trace IP address to Internet Service Provider (ISP) Using ARIN, Check Domain, etc.
Identify ISP and obtain contact information	Obtain Provider and contact information. www.icaccop.com, www.search.org
Obtain Search Warrant or Subpoena for subject specific identity and location to be served on the Internet Provider	Request: Subscriber info., Emails, billing info. etc. by connection IP address. Issue Preservation letters ASAP. Date and time specific. Very important.
Verify Subscriber information	DOL photo, open source research, local records check, NCIC III, NCMEC, surveillance, etc
Obtain Search Warrant(s) and execute	Suspect Interviews -confessions Computer & digital evidence seizures
Computer Forensic Requests	State Police, ICAC Task Forces, FBI CART, FBI RCFL's, etc.
Review computer forensic results	Obtain chats, emails, identify additional suspects and victims, obtain images and movies, timelines, supporting evidence, etc.
Review images and movies for suspected illegal content	CVIP, series identification, victim identification, LESP, NCMEC reports valuable to case prosecution.
Prepare and submit case for prosecution	State vs. Federal