

Computer Crimes: A Police Perspective

Lt. Dennis Lane
Commanding Officer
Computer Crimes Squad



Police Department
City of New York



Police Department

Patrol Services Bureau

Detective Bureau

Special Investigations Division

Computer Crimes Squad

Who We Are, What We Do

CCS investigates all types of crimes that involve the use of high technology and the Internet. Such as:

- Child Pornography
- Identity Theft
- Hacking
- Online Auction Fraud
- Use of stolen credit cards online

Who We Are, What We Do

Investigate crimes committed where the computer is:

- Used to facilitate the crime
- The object of the crime
- Or the repository of the evidence of the crime

Three Modules

- Online Crimes Module
- Investigative Module
- Forensic Laboratory Module

Online Crimes Module

- Proactively search the Internet for distribution of contraband
- Investigate distribution of Child Pornography
- Websites
- FTP Servers
- Monitor screen names of wanted felons

Investigative Module

- Conduct investigations
- Respond to search warrants
- Secure “electronic” crime scene
- Identify and secure evidence
- Properly shut down system / device
- Testify in court

Forensic Laboratory Module

- Image contents of storage device / media
- Hard Drives, External Drives
- Thumb Drives
- CD's, DVD's, Floppy, Zip, Jaz diskettes
- Memory cards, sticks or uncommon types
- Video/Still Digital Cameras, PDAs, Cell Phones
- Determine operability of equipment
- Determine true ownership of stolen property
- Retrieve hidden or “destroyed” data
- Prepare evidence for trial

How a Computer Crime is Investigated

- Call 311/911 or your local precinct
- Patrol unit will respond and collect information
- Precinct Detective Squad will conduct preliminary investigation
- CCS will assist the PDS or take over the investigation

What evidence do we need?

Child Pornography/Child Enticement

- Save original emails
- Instant Messenger logs
- Images
- Caller ID information
- Cell phone images
- Keep track of dates and times

What evidence do we need?

Identity Theft

- Original emails
- US mail materials
- Phony checks
- Bank information on you and the suspect
- Keep track of dates and times

Methods we use to investigate

- Track emails
- IP Address tracking
- Live monitoring of network
- Information from private IT professionals
- Forensic examination of digital artifacts

Obstacles to investigations

- Investigation leads outside of the United States
- ISP/Web site records have expired
- Suspect used tools to spoof IP Address

Cyber Bullying

Vives v. NYPD

- Carlos Vives was arrested by the NYPD in April 2002
- In August 2002, the NYCLU filed suit in federal District Court arguing that the statute under which Mr. Vives was arrested was unconstitutional under the First Amendment and that the arrest was unlawful.

Cyber Bullying

- On Nov. 24, 2003, the District Court ruled that the statute was unconstitutional on its face and that the arrest of Mr. Vives violated his First and Fourth Amendment rights. Further, the Court enjoined the NYPD from further enforcement of the statute.

Cyber Bullying

- Judge enjoins the NYPD from enforcing statute unless the communication is a *Death Threat*, threat of *Serious Physical Injury* or a threat of *Serious Property Damage*

Help us to Help You

- To protect children:
- Educate children to risk of ID Theft
- Explain why it is dangerous to give too much information on the Internet
- Images sent in emails persist forever
- Check your child's Internet usage through filtering and monitoring software
- Place computer in common area

Help us to Help You

- Encourage children to tell you what happens
- Listen and reassure – Don't judge and scold
- Notify police immediately

Questions?