



# How can Investigators stay ahead of the bad guys?

Luke Erickson

Forensic Examiner  
Bureau of Consumer Protection



# The “Average case” in 2007

- had more than one location
- produced over 20 forensic images
- produced over 20,000,000 files
- produced over 100 databases
  
- produced over 1.5 terabytes of data



# FTC stays ahead by

- Using advance hardware:
  - 22 Terabyte Server for “dirty” data/forensic images
  - Fast hardware forensic disk image devices
- Partnering with outside law enforcement:
  - Department of Commerce
  - Miami-Dade Police Department
  - Postal Inspection Service
  - FBI’s Regional Computer Forensics Laboratory
  - University Police Departments



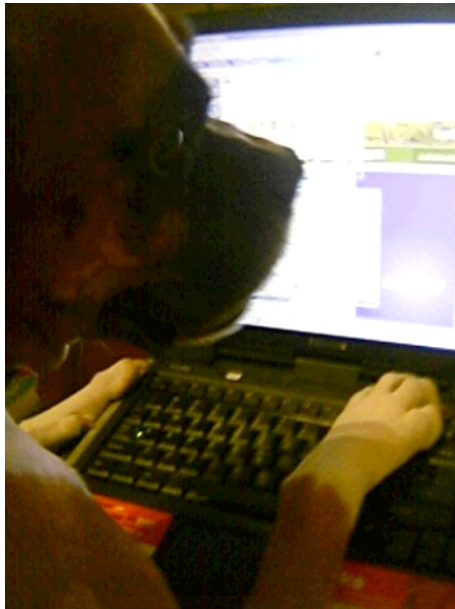
# Miami-Dade Mobile Lab



- Imaged 6.5 Terabytes in 48 hours



# How to catch the bad guys?



- Digital Evidence:
  - Video Screen Captures
  - Known Datasets



# Capturing evidence tips:

- Include audio with screen capture videos:
  - Who you are
  - Where you are physically located
  - Date and time of capture
  - What your going to capture
  - Specific details of what your clicking/typing
  - Specific details of what is happening



# Using known datasets

- Enter irregular factitious names and address:
  - » Luke Skywalker
  - » 1942 Londonpromo Street
  - » Blackberry, FL 32825
- Record date/time information was entered.
  - This help forensic examiners find current database fields.