Law Enforcement Incident Response to Cybercrimes
&
Battling Current Technological Trends

Corey J. Bourgeois, Computer Forensic Examiner
&
David Ferris, Investigator

Louisiana Department of Justice

HTCU

A brief history...

Louisiana ICAC

- **Louisiana Department of Justice**

  1 director (ICAC commander)
  1 lab supervisor
  1 Supervisory Investigator
  5 investigators
  10 forensic examiners
  2 analysts
  1 Prosecutor
  174 affiliates

High Tech Investigations

Proactive & Reactive Investigations

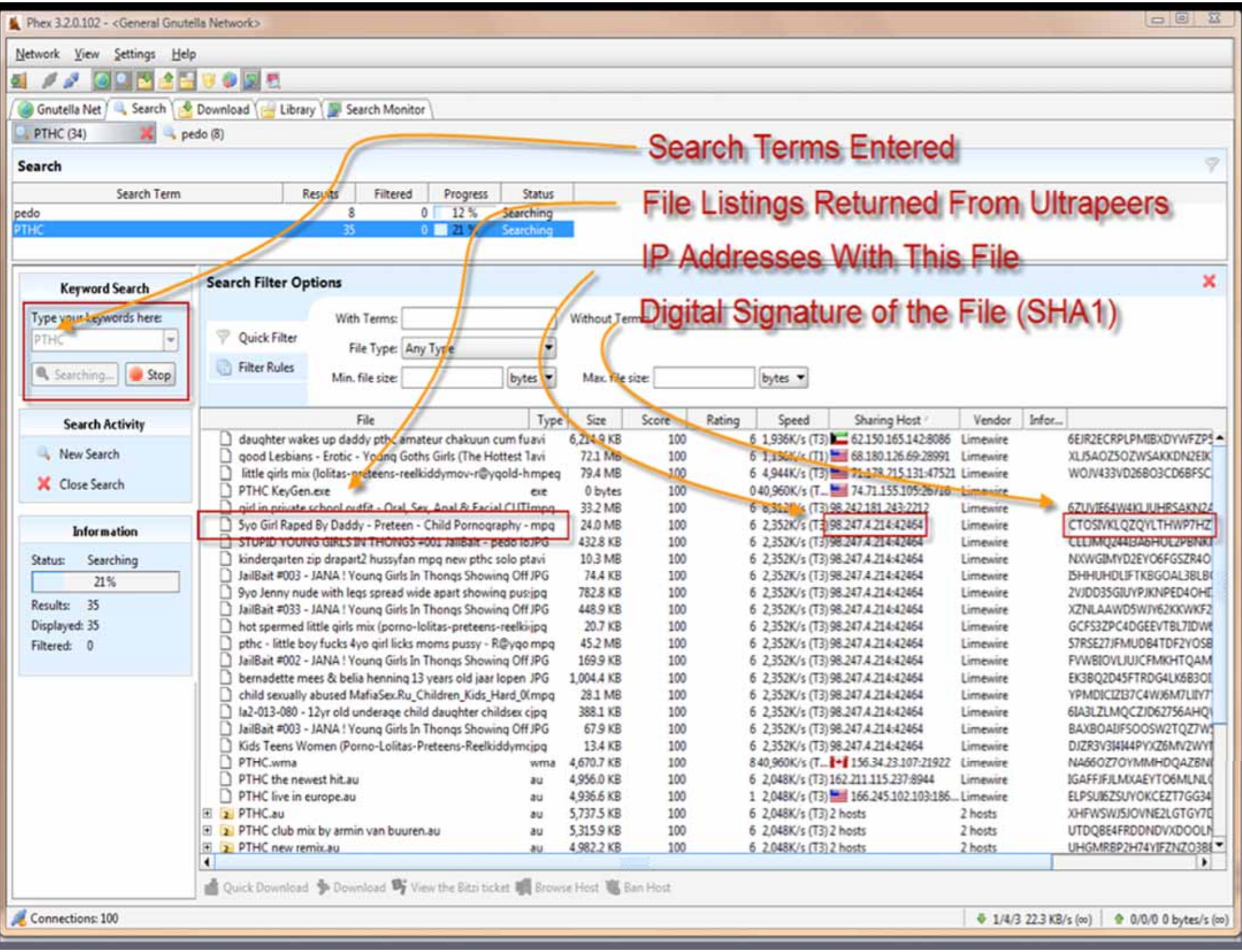
- Undercover Chatting
- Peer 2 Peer
- Juvenile Prostitution

Undercover Chatting

- Target - suspects online praying on children in chat rooms, social networking sights, and gaming sights
- Requires law enforcement officers to assume roles as either a child, the mother/father, or as individuals of like mind
- Covered under - indecent behavior with a juvenile, computer aided solicitation of a minor and pornography involving juveniles

Peer 2 Peer Investigations

- Peer to Peer File Sharing
  - Sharing occurs when two computers are directly connected and downloading files from their shared folder
- Primarily used to download, possess, and distribute images and movies of child pornography


Search Terms Entered
File Listings Returned From Ultrapeers
IP Addresses With This File
Digital Signature of the File (SHA1)

Pros

- Known image
- Tracking of image origination
- Documents the trafficking of images previously unknown in circulation
- Establishes historical record of SHA values

Cons

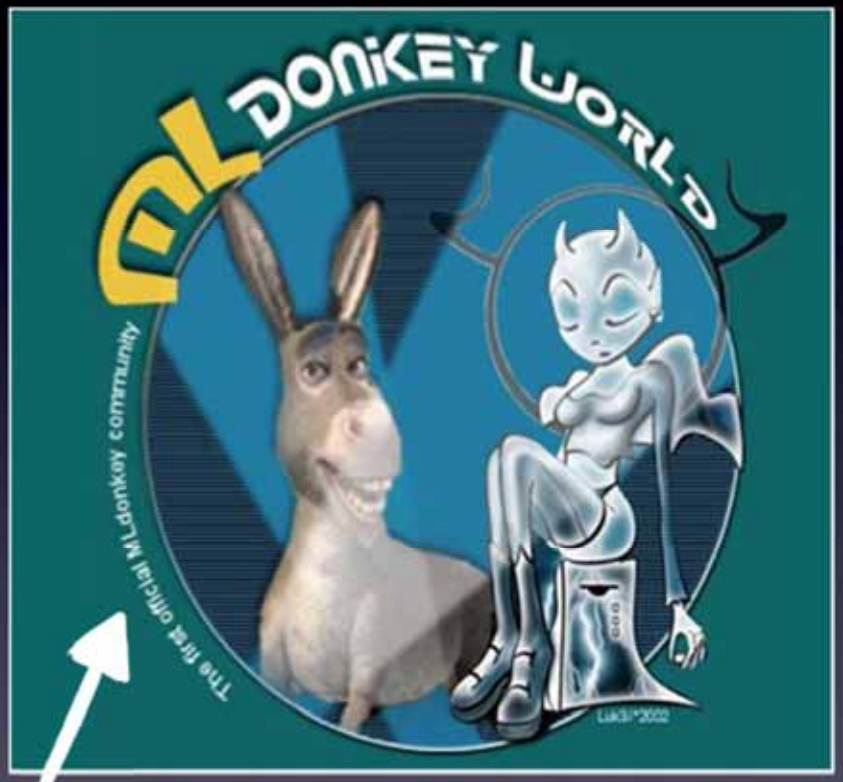
- IP based investigations - tied to subscriber, not necessarily the suspect
- ISP Errors/Hijacked IP Address
- Very large pool of targets

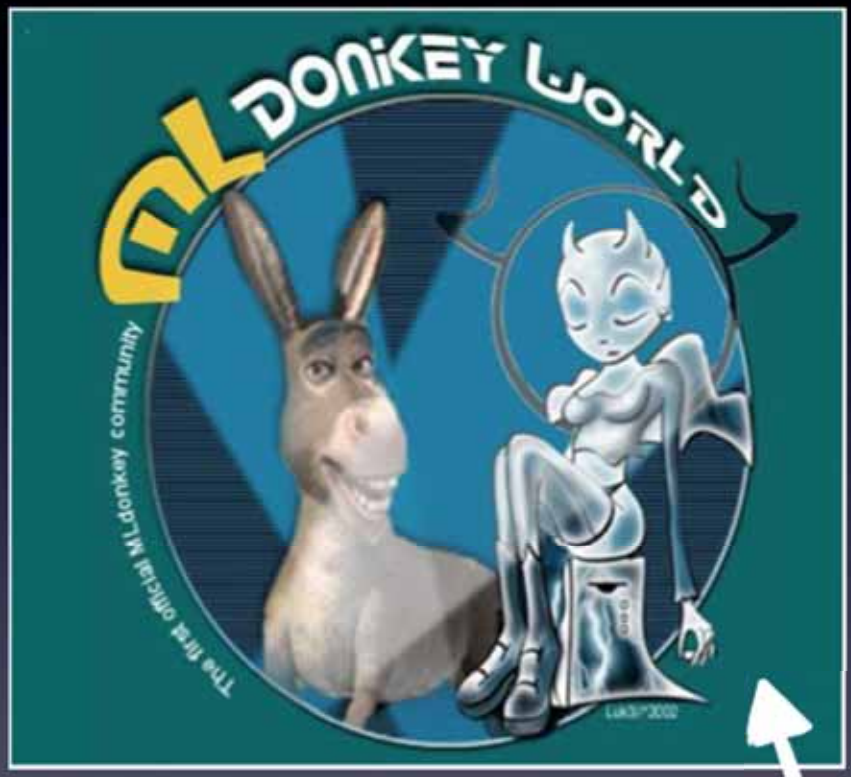
Identifying Contraband

Sha-1 Algorithm

- file encryption method which may be used to produce a unique digital signature of a file.
- it is computationally infeasible (2^160th) to find two different files that produce the same SHA-1 value.

Sha-1 EXAMPLE





JQTPDSTHWKMNDT2VLIE3H7EVLMPH6QNO

S33EBO3O5SKAHKKHVATJWSXYSZFQJ5NF

MLDONKEY WORLD

The first official MLdonkey community

Luk3@*2002

JUVENILE PROSTITUTION

- Investigations can target the “Johns” or attempt to recover the juveniles
- A large majority of your current prostitutes began when they were juveniles.
- Juvenile prostitution stings can occur:
  - Craigslist, Backpage, Cityvibe, chat rooms and social networking sites
- These stings involve juveniles selling themselves as well as parents of the juveniles selling their children

Reactive Online Investigations

- Internet Crime Complaint Center (IC3)
- National White Collar Crime (NWC3)
- National Center for Missing and Exploited Children (NCMEC) Cybertips
- Citizen’s Complaint

Computer Forensics

- preservation
- identification
- extraction
- documentation
- interpretation

...of computer data

Initial Response

- Arrive on scene
- Photograph computer location, screen, and any connections.
- Open case photograph the inside of the computer
- Conduct forensic preview
- Bag & Tag

Basic Methodology

- acquire evidence without altering or damaging the original
- authenticate that your recovered evidence is the same as the originally seized data
- analyze the data without modifying it

Acquire

Authenticate

Analyze

Always use sound forensic practices

Always work under the assumption that a case, no matter how small, could end up in a court of law.

Forensic Toolbox

- Forensic Computer (Standalone)
- Virtual Machine Application (VMWare Fusion or Parallels)
- Writeblockers (IDE, SATA, Firewire, USB)
- EnCase developed by Guidance Software
- FTK (Forensic Tool Kit) developed by Access Data
- Blacklight, MacQuisition, Softblock developed by Blackbag Technologies
- Internet Evidence Finder developed by JAD Software
- Cellebrite
- Oxygen
- Secure View
- Super Yahoo Chat Decoder

Don’t focus on a particular tool to get the job done. Think of computer forensics as a concept and the application and understanding of this concept is especially important for the credibility of the forensic examiner in a court of law

Our Lab

- 11 nerds (including myself)
- 11 mac pros
  - 2 x 2.93 GHz Quad - Core Intel Xeon Processors
  - 16 GB 1066 Mhz RAM
  - 4 x 1TB 7200 RPM Hitachi Hard drives
- 184 TB SAN (Storage Area Network)
  - 144 TB usable storage
- 2 x Xserve RAID

Assistance to Others

- **Training**
  - Cell phone examination
  - Computer forensic
  - On-scene forensic
  - Peer 2 Peer Undercover
  - Chat Undercover
  - Prostitution Training
  - On-Scene Seizure of Digital Evidence
- **Purchasing equipment for affiliate agencies**

Challenges

- storage media
- cell phones and cellular technology
- the cloud
- bit torrent
- encryption
- iOS
- computing power
- time
- keeping up with new technology
- security
- wellness

Questions?

Corey Bourgeois, Lab Supervisor
David Ferris, Lead Investigator

Louisiana Department of Justice

bourgeoisc@ag.state.la.us
ferrisd@ag.state.la.us
225.326.6100