

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 preying 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 Term	Results	Filtered	Progress	Status
pedo	8	0	12 %	Searching
PTHC	35	0	21 %	Searching

Search Terms Entered

File Listings Returned From Ultrapeers

IP Addresses With This File

Digital Signature of the File (SHA1)

Keyword Search

Type your keywords here:

PTHC

Searching... Stop

Search Filter Options

With Terms: Without Terms:

Quick Filter

Filter Rules

File Type: Any Type

Min. file size: bytes Max. file size: bytes

Search Activity

New Search

Close Search

Information

Status: Searching

21%

Results: 35

Displayed: 35

Filtered: 0

File	Type	Size	Score	Rating	Speed	Sharing Host	Vendor	Infor...
daughter wakes up daddy pthc amateur chakuun cum fuavi		6,214.9 KB	100	6	1,936K/s (T3)	62.150.165.142:8086	Limewire	6EJR2ECRPLMIBXDYWFZP5
good Lesbians - Erotic - Young Goths Girls (The Hottest Tavi		72.1 Mb	100	6	1,130K/s (T1)	68.180.126.69:28991	Limewire	XLJ5AOZ5OZWSAKKDN2EJK
little girls mix (lolitas-preteens-reelkiddymov-r@yqold-hmpeq		79.4 MB	100	6	4,944K/s (T3)	71.178.215.131:47521	Limewire	WOJV433VD26BO3CD6BFSC
PTHC KeyGen.exe	exe	0 bytes	100	6	040,960K/s (T...	74.71.155.105:26720	Limewire	
girl in private school outfit - Oral Sex Anal & Facial C11Timg		33.2 MB	100	6	6,312K/s (T3)	98.247.4.214:42464	Limewire	67UVF64W4K1JUHRSKXN2A
Syo Girl Raped By Daddy - Preteen - Child Pornography - mpq		24.0 MB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	CTOSIVKLQZQLTHWP7HZ
STUPID YOUNG GIRLS IN THONGS #001 JailBait - pedo 107PO		432.8 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	CLLJMQL2443ABHUL2PBNNK
kinderqarten zip drapart2 hussyfan mpq new pthc solo plavi		10.3 MB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	NXWGMVYD2EYO6FGS2R4O
JailBait #003 - JANA ! Young Girls In Thongs Showing Off.JPG		74.4 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	ISHHUHDLIFTKBGOAL38LB
9yo Jenny nude with legs spread wide apart showing pussy.jpg		782.8 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	2VJDD35GIUYPJKNPED4OHE
JailBait #033 - JANA ! Young Girls In Thongs Showing Off.JPG		448.9 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	XZNLAAWD5WJY62KKWKF2
hot spermed little girls mix (porno-lolitas-preteens-reelkijpq		20.7 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	GCF53ZPC4DGEEV7BL7IDW
pthc - little boy fucks 4yo girl licks moms pussy - R@yqo mpq		45.2 MB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	57RSE27JFMUD84TDF2YOSB
JailBait #002 - JANA ! Young Girls In Thongs Showing Off.JPG		169.9 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	FVWBIOVLJUJCFMKHTQAM
bernadette mees & belia henning 13 years old jaar lopen.JPG		1,004.4 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	EK3BQ2D45FTRDG4LK683OI
child sexually abused MafiaSex.Ru_Children_Kids_Hard_0(mpq		28.1 MB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	YPMDCIZI37C4WJ6M7LIY7
la2-013-080 - 12yr old underage child daughter childsex.cjqp		388.1 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	6IA3LZLMQCZID62756AHQI
JailBait #003 - JANA ! Young Girls In Thongs Showing Off.JPG		67.9 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	BAXBOAIFSOOSW2TQZ7W
Kids Teens Women (Porno-Lolitas-Preteens-Reelkiddym.cjqp		13.4 KB	100	6	2,352K/s (T3)	98.247.4.214:42464	Limewire	DJZR3V3H44PYXZ6MV2WY
PTHC.wma	wma	4,670.7 KB	100	6	840,960K/s (T...	156.34.23.107:21922	Limewire	NA66OZ7OYMMHDQAZ8N
PTHC the newest hit.au	au	4,956.0 KB	100	6	2,048K/s (T3)	162.211.115.237:8944	Limewire	IGAFFJFLMXAET06MLNLC
PTHC live in europe.au	au	4,936.6 KB	100	1	2,048K/s (T3)	166.245.102.103:186...	Limewire	ELPSU8ZSUYOKECZ77GG3A
PTHC.au	au	5,737.5 KB	100	6	2,048K/s (T3)	2 hosts	2 hosts	XHPWSWJ5JOVNE2LGTGY7D
PTHC club mix by armin van buuren.au	au	5,315.9 KB	100	6	2,048K/s (T3)	2 hosts	2 hosts	UTDQBE4FRDDNDVXDOOLN
PTHC new remix.au	au	4,982.2 KB	100	6	2,048K/s (T3)	2 hosts	2 hosts	UHGMRBP2H74YIFZNZO38E

Pros

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

Cons

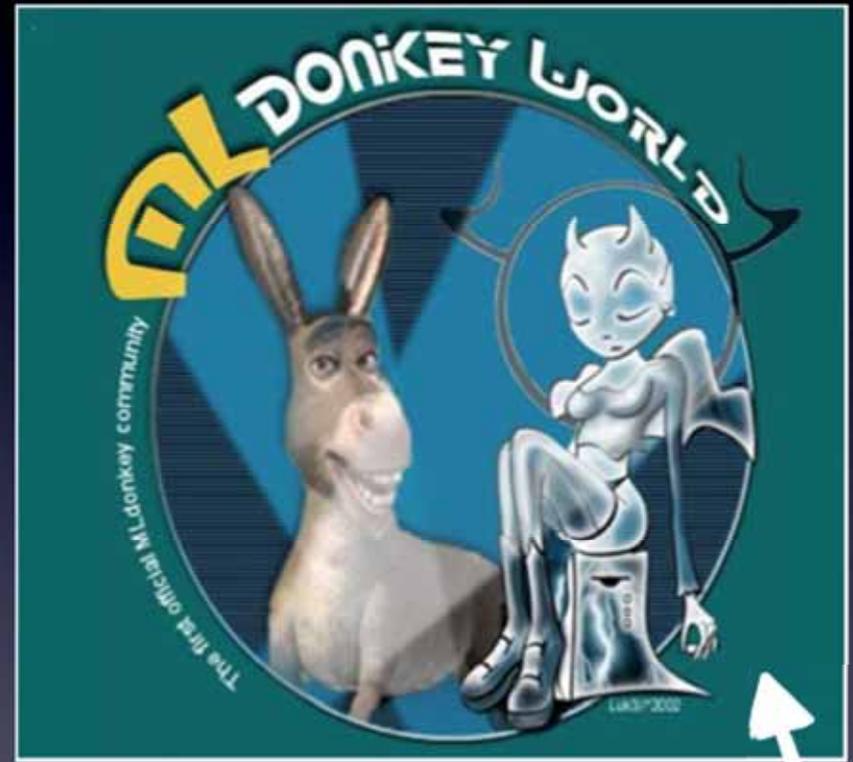
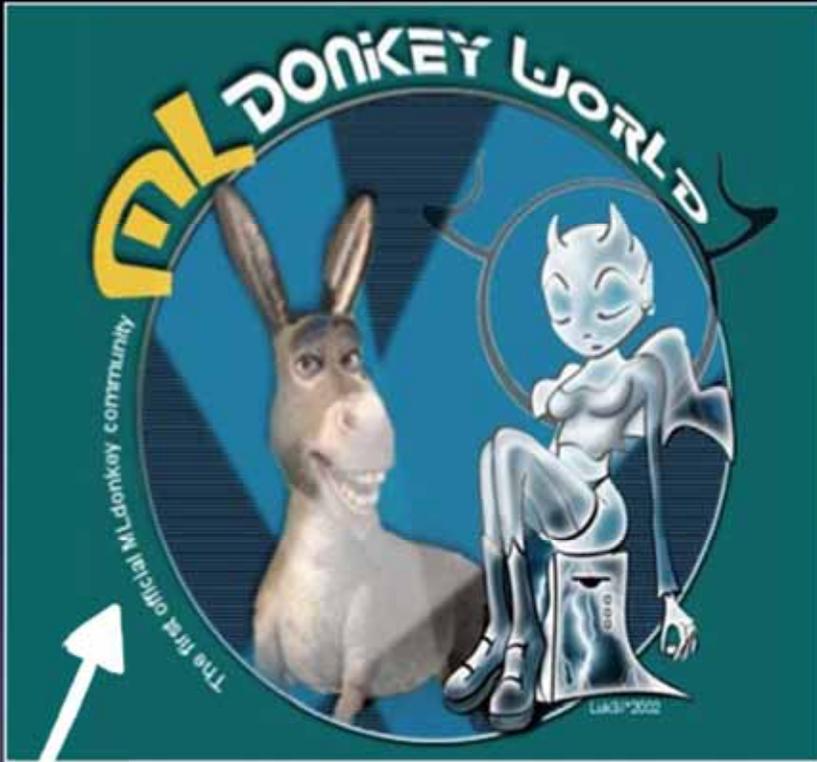
- IP based investigations - tied to subscriber, not necessarily the suspect
- ISP Errors/Hijacked IP Address
- Very large pool of targets

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^{160}) to find two different files that produce the same SHA-1 value.

Sha-1 EXAMPLE



JQI PDSTHWKMNDT2VLIE3H7EVLMPH6QNO

S33EBO3O5SKAHKKHVATJWSXYSZFOJ5NF

ML DONKEY WORLD

The first official ML donkey community



Luk30™ 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 ...of computer data
- documentation
- interpretation

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

bourgeois@ag.state.la.us

ferrisd@ag.state.la.us

225.326.6100