

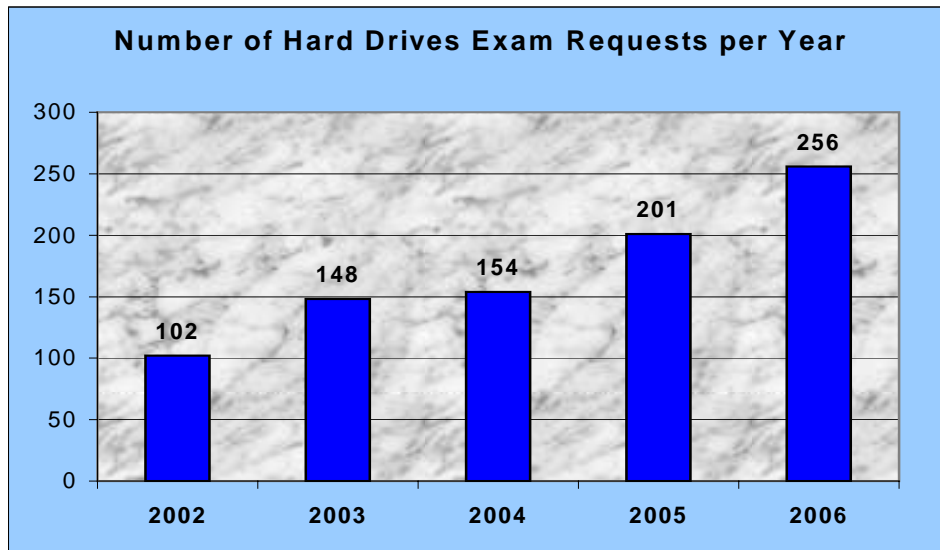
**MAINE STATE POLICE CRIME
LABORATORY
Computer Crimes Unit**



2006 ANNUAL REPORT

Since 1999, the Maine Computer Crimes Task Force (MCCTF) has been involved in virtually every computer crime investigation in the State of Maine. In 2005, the Maine State Police component of the MCCTF became a unit of the Maine State Police Crime Laboratory. Public Law 676, passed in 2006, formalized this relationship, increased personnel, and funding for the new unit.

In 2006, the Computer Crimes Unit received a total of 256 hard drives (up from 201 drives in 2005) for examination.



Since 2002 the requests for the Computer Crimes Unit to conduct forensic examinations on computers has gone up nearly 251%.

The Unit continues to be the portal for referrals to Maine from the National Center for Missing and Exploited Children. The Unit received 54 referrals from the National Center in 2006 (up from 33 in 2005), mostly solicitation of children for sexual acts and dissemination of child pornography.

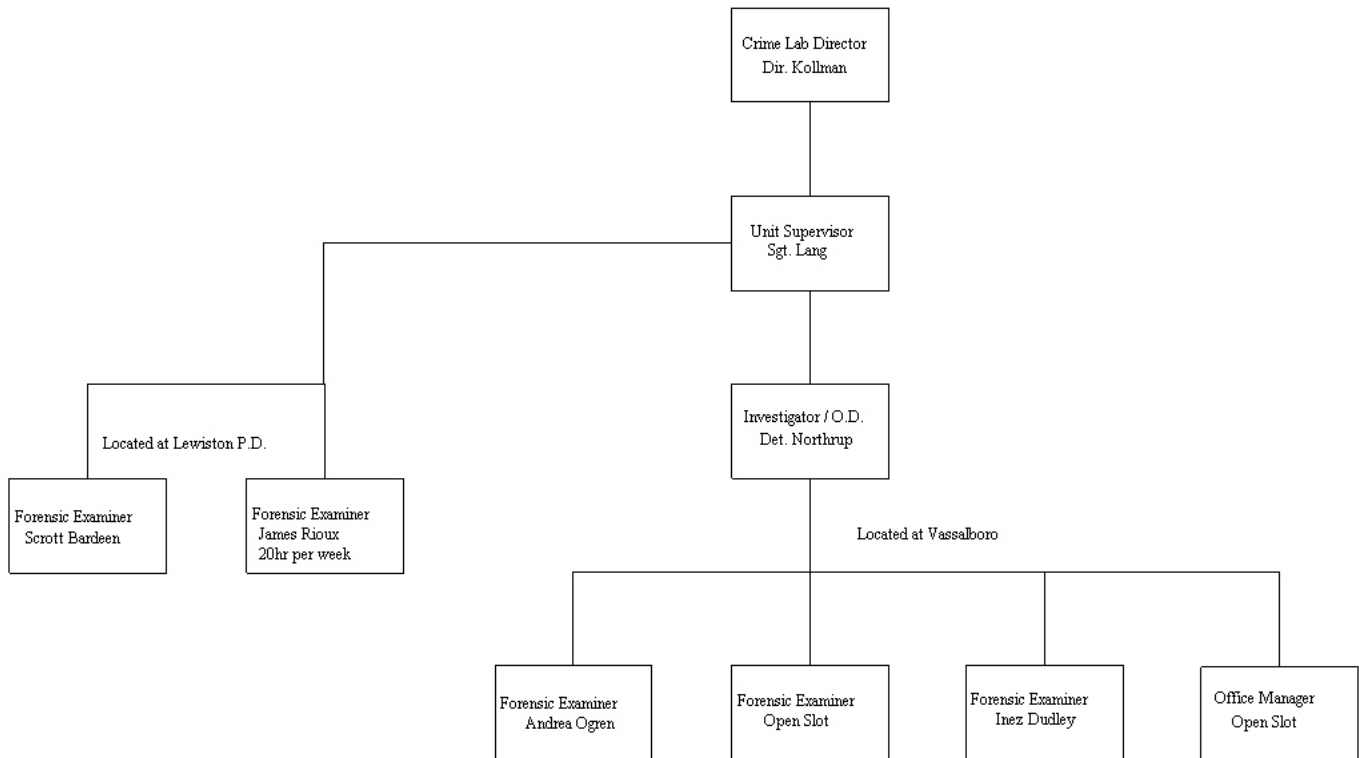
Types of Crimes the MCCTF investigated and assisted with in 2006

Animal Abuse – 2

Arson – 1
Bank Robbery – 1
Bomb Threat – 2
Burglary – 2
Child Abuse – 2
Child Pornography – Possession – 96
Child Pornography – Dissemination – 25
Child Pornography – Manufacturing – 1
Criminal Mischief – 1
Community Outreach (training/lecture/presentations) – 39
Drug Offense – 4
Enticement – 17
Fraud – 36
Gross Sexual Assault – 12
Hacking – 6
Harassment – 16
Homicide – 5
IF&W Violations – 1
Internal Affairs – 6
Missing Persons – 3
NCMEC Referrals – 54
Sexual Harassment – 1
Suicide – 3
Terrorism – 1
Terrorizing – 2
Theft – 12
Threatening – 2
Violation of a Protection Order – 4
Violation of Probation – 5

Number of complaints received by the computer crimes in 2006 actually decreased. In 2005 we received over 100 complaints with regard to fraud. In 2006 we only received 48 fraud complaints; most of them were directly from the public. Many officers have told us they no longer call us for most types of frauds because historically we have not had the manpower to address this type of complaint. Priority is given to crimes against persons such as child exploitation, Murder, stalking, etc.

Unit Staffing



Funding

In addition to the funding received under PL 676, \$125,000 for a year and one half is provided to the unit, as well as associates of the Maine Computer Crimes Task Force, from the Internet Crimes Against Children (ICAC) grant.

Peer-to-Peer Statistics

In August 2005, MCCTF members attended the annual meeting of ICAC investigators in Dallas, Texas. During an instructional seminar they were given access to a program that allowed them to further investigate the crime of distributing child pornography via the peer-to-peer network.

While we did not have the resources to pursue these cases it did give us the ability to examine the issue and determine how bad the problem is in Maine.

Below is a simplified description of an investigative technique used to examine the crime of dissemination of sexually explicit material on the peer-to-peer network and the results from 2006 in the State of Maine.

Please do not disseminate the investigative techniques described in this document further than necessary.

Definitions:

1) Peer to peer network on the Web:

- A peer-to-peer (or P2P) computer network is a network that relies on computing power at the edges (ends) of a connection rather than in the network itself. P2P networks are used for sharing content like audio, video, data or anything in digital format. P2P network can also mean grid computing.

In other words, the network is a group of individual users who have installed a program like Napster on their computer to allow them to connect to other individuals who have also installed the software to allow them to share files. There is no traditional “server” that is storing the content to be shared. The files reside on the individual’s computer and are placed in a directory the user designates to share with the world.

2) **Hash Value:** This is the digital fingerprint of a file and is considerably more accurate than DNA.

3) **I.P.# or Internet Protocol number:** This is a person's address on the Internet. The number is assigned to the person by the company who they pay to give them Internet access. Each Internet Service Provider has a large pool of I.P. numbers that they can assign to the subscribers. In most cases the number you are assigned is changed frequently – called dynamic I.P. assignment.

4) **ICAC:** Internet Crimes Against Children

5) **Shared directory:** When a person installs the peer to peer software on their computer they can elect to share files with other people. Anything they place in the directory they designate as the shared directory will be available for anyone who wishes to take a copy of the file. People can elect not to share any files, but still access other people files.

How the investigation is conducted.

The technique was created by Flint Waters of the Wyoming ICAC Unit.

Investigators from around the county install the peer-to-peer software on their computers. The software is free for download.

The peer-to-peer software connects the investigator's computer to other people's computers who have installed the peer-to-peer software. The investigators now have access to files that the other people have placed in "shared directories" for the express purpose of sharing them with the world.

The investigators search for a term often used by pedophiles to describe child pornography. One such term is “babyj”. The search results shows thousands of files being shared on the peer-to-peer network – some are child pornography some are not. The results show the I.P. of the person sharing the files as well as the files hash value or digital fingerprint.

The results of the search are sent to the Wyoming ICAC server where the hash values are compared to a database of images or movies that have been determined to be pre-pubescent child pornography. **The images and movies I have examined from this “known” database have all involved sexual intercourse with children who appear to be under 7 years in age.**

The results of the search are separated out by state as determined by automatically examining the IP number of the person sharing the image or movie. The only records that are saved in the state’s databases are the matches with known images and movies. The records for each state are stored on the server in Wyoming so that investigators from each state can have access to them.

The State records I have access to display a lot of data including:

The suspect’s IP number,

The hash value of the known file they were sharing

Date and time of the share

The name and department of the investigator who discovered the crime

Town where the offense was originating, based on public records of IP assignment

With the data that is found in our state record a subpoena can be issued to the Internet Service Providers who own the IP numbers that were being used to disseminate the child pornography. The subpoena would demand that the provider identify the account that was assigned the IP number on the date and time of the offense.

To pursue this further a search warrant could be obtained for the residence that was assigned the IP number to allow us to attempt to identify the person responsible for disseminating child pornography.

The Computer Crimes Unit drafted 21 search warrants in 2006. This is up from 5 drafted in 2005, **an increase of 75 percent**. All of the 2006 search warrants involved child exploitation. 18 of the search warrants were the result of peer-to-peer “hits”

The search warrant validated what other states have already discovered and that is that the data we are getting in our state records is accurate.

2006

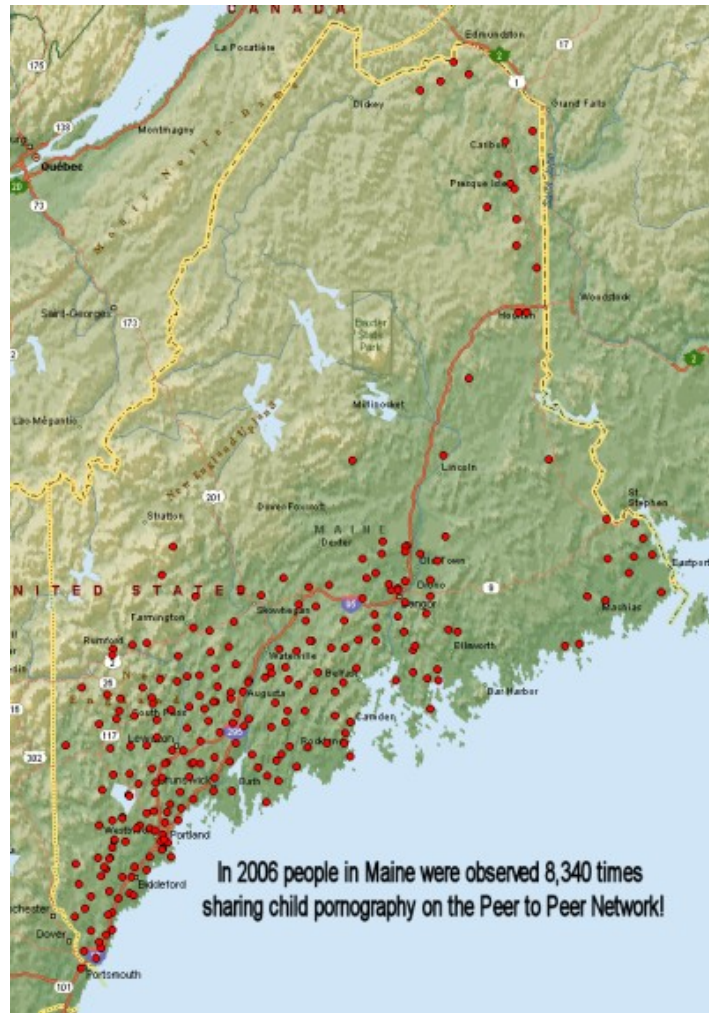
8,340 entries were made in Maine’s state record on the Wyoming database. This represents a 13.7 percent increase over 2005 (7,336).

Not all of these are unique as a person could be sharing child pornography with one IP number this week and a different number next week. There may also be some redundancy as two investigators may discover the same person, the same week, sharing child pornography.

In some cases the IP number traces may have only traced to a large town near the suspect. For example a trace of person distributing child pornography in Vassalboro may show up as Augusta because that is where the company who owns the IP number listed it. A subpoena of company records would be needed to confirm the exact location.

Below is the 2006 town list of Maine’s 13 highest offenders. It includes the name of the town and the number of times an investigator observed someone in that town distributing child pornography.

Brunswick	816
Portland	688
Saco	585
Kittery	499
Bangor	409
Augusta	303
Biddeford	270
Naples	230
South Portland	193
Orono	178
Lewiston	176
Rockland	174
Auburn	167



Locations of dissemination of child pornography via the Peer-to-Peer Network, 2006