The Child Protection System

Child Protection System, or CPS, is a suite of programs centered on a web-based interface that provides access to investigative data gathered by automated tools and law enforcement searches. Traditionally IP based investigations have not allowed law enforcement to associate IP information with user data. By using CPS, investigators now have the option to correlate various data sources with IP addresses and screen names involved in criminal activity. All reports follow a standard convention in an easy to read format, which allows the investigator the ability to associate information.

The Child Protection System (CPS) allows trained investigators to identify offenders using peer-to-peer networks to distribute child pornography. Information is gathered by various automated tools and manual searches by law enforcement and accessed through CPS. This data can be used by investigators to gather, profile and track information tied to an Internet Protocol address (IP address) of the offender.

The Child Protection Systems provides a number of benefits to investigators. CPS future enhancements continue; here are a few of the current features:

- Investigators can quickly view activity of a specific IP address including other investigator interests in the IP address.
- Search by usernames (for example, superdad38@yahoo.com).
- File hashing – Files hash values in various formats.
- GUID (Globally Unique Identifier) histories reveal if other investigators have previously identified, shared interests and location information about that GUID. A GUID also may allow offender tracking across multiple IPs.
- Address searches reveal if other investigators have shared interest in an address (important for deconfliction). Latitude and longitude can be used to map addresses.
- Phone number searches reveal if other investigators have shared interest in an address (important for deconfliction).
- Service Providers provide legal contact information.

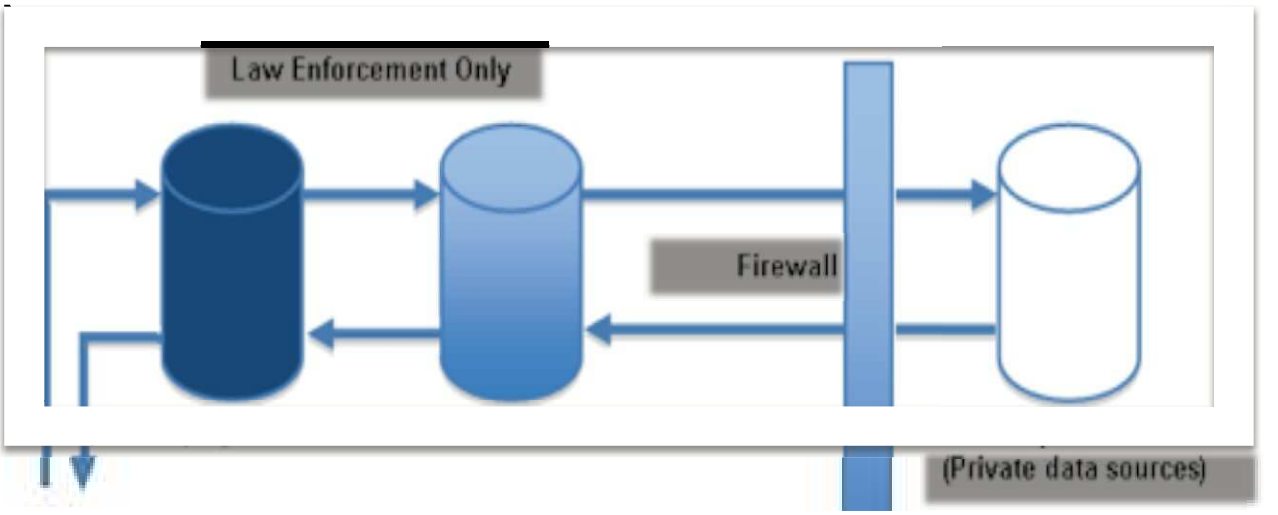
CPS is the web interface allowing the investigator to query the database, provide deconfliction, and investigative job creation. Licensed investigators, using their Gridcop username and password, may access the site at **https://cps.gridcop.com**.

CPS Data Sources

In CPS, the investigator has access to different data sources. Traditionally, all data generated by law enforcement personnel, or tools written by law enforcement, have been stored **on servers located at** the Wyoming Division of Criminal Investigation in Cheyenne, WY. In May of 2009, **when the Wyoming servers failed, a second set of servers, purchased by TLO in Florida, and donated to** the State Attorney for the Fifteenth Judicial Circuit, came online to provide replication, and are synchronized, allowing for redundancy, should one fail. Wyoming Toolkit users and automated tools such as Peer Spector contribute data to these servers.

With the assistance of TLO, an additional set of law enforcement only servers was added in Florida to store the increased volume of data generated by the software tools written by corporate

employees. These tools, including various crawlers and Peer Spectre2 (covered in other manuals), have the ability to capture more complete data on P2P targets, including GUIDs, firewall information, and push proxies (intermediary for requests).



The investigator also has the option of including private data sources in reports generated through CPS. TLO has allowed law enforcement access to data collected on Internet users from a variety of sources. This data includes marketing data that has been linked to IP addresses and email accounts from corporate sources. This data is considered unverified subscriber information and should never be considered a replacement for the subpoena or legal process, but is provided as intelligence information only. No logs are kept of any law enforcement query of corporate data, and TLO has no access to any law enforcement server.

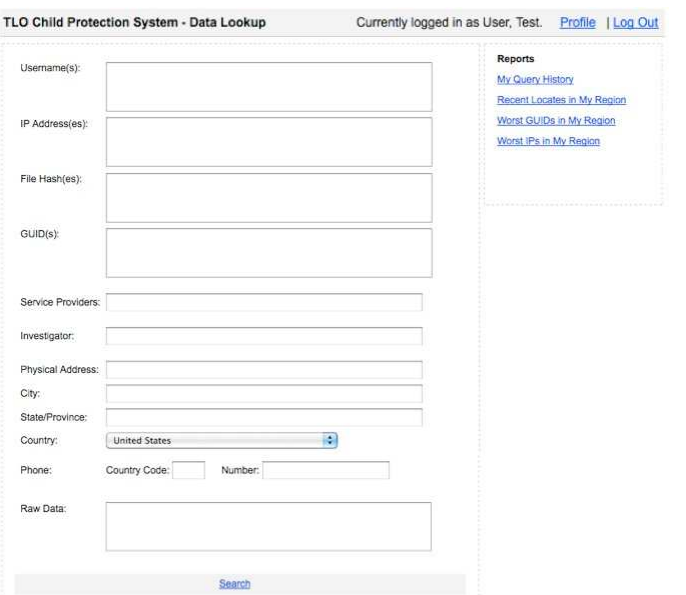
When a law enforcement officer initiates a query, it is first directed to one of the two Fairplay servers where deconfliction is handled; the request is then sent to the TLO law enforcement server where the results are compiled. If the investigator chooses, the query is then sent to the corporate database for any unconfirmed subscriber information. The transaction with the corporate server is one-way and nothing is logged on the corporate server.

CPS Main Page

The home screen of CPS is divided into two main sections:

Manual searches. These text boxes allow searches for individual types of data, such as usernames, IP addresses, file hashes, GUIDs and other information.

Preformatted reports. These links provide access to the most commonly used queries. The user may drill down further in each report, depending on the level of information needed.



Manual Searches

The following list describes the text box queries on the **Home** page. This is where you type information to query the databases. Click **Search** to generate a report on your query. All manual searches will generate a comment box. The comment should be brief but have some identifying information, such as an incident or case number, allowing the investigator to recall the reason for the search at a later date. This is for deconfliction purposes, should other investigators share interest in the item.

Username: Type a single username, or up to 20, separated by a comma. Wildcard or partial searches are allowed. Usernames stored in the deconfliction system may belong to undercover identities, victims, suspects, and witnesses to include victim identification, case building, and other possibilities.

IP Address: Type an individual IP address or up to 20 separated by a comma. Investigators can quickly view the history of a specific IP address including other investigator interests in the IP address.

File Hash(es): Type a hash number to search by or up to 20 separated by a comma. Hash files using the MD5, SHA1 algorithm in both base16 and base32, and SHA256 to determine what is known about a particular file based on its hash values. Multiple hashes are separated by a comma.

GUID(s): Type an individual GUID to search by (or multiples separated by a comma). The GUID query will show all instances where a particular GUID appears in the system. This can offer a chance to track an individual computer across different IPs. GUID histories reveal if other investigators have seen it before and give insight into the interests and location of the system associated with that GUID.

Investigator: Type the name of an investigator to search; names, states or partial text strings will be returned: broad or specific.

Physical Address: You must complete the Physical Address, City, State/Province, and Country fields (all four fields) for a complete address query. Type a physical address to search.

Phone: Country Code/Number: Type a phone number (or partial). The Phone field can be searched by Country Code (are code) or by the full phone number.

After entering an item and starting the search, a comment box will appear; this will allow the investigator to enter a brief reason for the search. If the item has not been seen before, it will be logged under the investigator's license. For deconfliction purposes, the investigator should enter a distinctive comment allowing him to recall the reason for the search at a latter date.

Preformatted Reports

The most commonly used queries have been added as links to the right of the CPS home page allowing you quick access to preformatted reports. Click a link to generate any of the following preformatted reports:

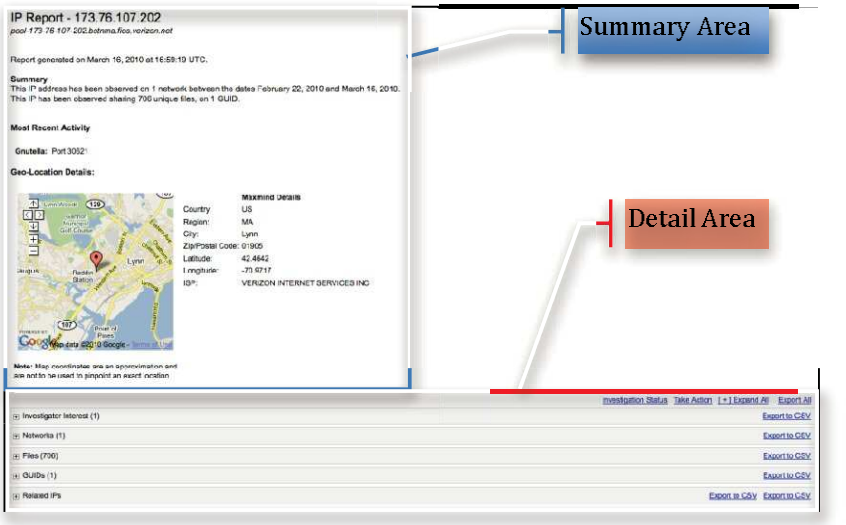
My Query History: The My Query History report shows all queries by an investigator sorted by type and date.

Recent Locates in My Region: The Recent Locates in My Region report shows the last 200 IPs that were seen in an investigators state. You can narrow the search to a specific county. The date range is defaulted to 30 days (but can be changed).

Worst GUIDs in My Region: The Worst GUIDs in My Region report displays GUIDs (Globally Unique Identifiers) sorted most to least. You can narrow the search to a specific county. The date range is defaulted to 30 days (but can be changed). Hyperlinks will export data to KML for display in Google Earth or to send Gnuwatch.

Worst IPs Region: The Get Worst IPs report GUIDs from most to least. You can narrow the search to a specific county. The date range is defaulted to 30 days (but can be changed). Hyperlinks will export data to KML for display in Google Earth or to send Gnuwatch.

Reports



CPS reports are designed to have a standard look, allowing the investigator to easily locate information and controls, regardless of what report is being viewed. Each report will follow the same layout, a summary area at the top and a detail area below. Depending on the information available, the report may include hyperlinked items indicating that the investigator can "drill down" and see further information about a particular piece of data. The information in the detail area may vary depending on the information available; the report will provide all information about the item that exists in the system. Between the two main areas of each report are links to actions the investigator may take with the information displayed. The action items available will vary depending on the type of report being viewed.

The action items available will vary depending on the type of report being viewed:

Export KML: Creates a Google Earth file for all points plotted on the displayed map. If the investigator has Google earth installed, it will open automatically and display.

Send Selected to Gnuwatch: Sends information about the current IP address to the Gnuwatch application. Gnuwatch will attempt to browse and log the target IP.

Monitor Selected Addresses: Sends information about the IP address to the Suspect Monitor application that will monitor the selected address.

Launch Media Library: Used with IP reports, this option will generate a listing of all files, by hash, that the IP was seen offering, start Media Library and load the hash values. This allows the investigator to quickly determine what files are already in the library and create magnets for those that are missing.

Launch Shareaza Job: Creates a task or job for the investigator's ShareazaLE program to browse and sole source download from the selected IP.

Shareaza Job (Browse Only): Similar to a Gnuwatch task, this task will send a job to ShareazaLE to browse and log the IP address.

Create Watch: notifies the investigator each time the IP is observed or run by another investigator.

Username Report

Username reports are usually a result of manual searches generated from the CPS Home page, and follow the usual CPS report format. The top portion of the report summarizes the report type, giving the username queried and the number of times it has been run. The detail area information will vary depending on what is available, but may include:

Unconfirmed Subscriber(s): shows any corporate information associated with the username. This may include name, address, date of birth, and phone number. As detailed in the Data Source section of the manual, it is considered unverified intelligence data and should not be acted on without confirming through legal process.

Investigative Activity: reveals any actions taken by other investigators in relation to this username. A column in this section is called Activity and shows the comment entered by each investigator. This section is useful for the investigator for deconfliction.

History Reports: Shows each time a history report was generated on this username, as well as the investigator running the name. Useful for deconfliction.

Action items are available for a username are:

Create Watch: this choice creates a job on the server under the investigator's license to notify the creating investigator of each time another system user takes an action with that username. Used for deconfliction purposes, the investigator is notified by a system message in the user Profile section.