Tech Share's Role

There are nearly 18,000 Federal, State, local, and tribal law enforcement agencies within the United States, all of which have different levels of technical expertise and varying investigative needs.

Tech Sharing was established to create and maintain a resource center for sharing technical solutions concerning widely used technical tools and applications. Identify and share best practices already in place within the law enforcement community.

- Assess existing law enforcement solutions and modify, if necessary, so they may be utilized throughout the law enforcement community.
- Focus on the acquisition, development and upkeep of the web portal.
- Develop and maintain electronic surveillance information, which includes solutions, technical expertise, and guidance.

Tool Overview

- Facebook Messenger Tool
- Cell Site Database
- IMEI TAC Code Search
- Gambit Web Service
- Catch and Handle
- CrossTalk
- TRAP
- iNimbus
- .Social
- RIPT
- U2L
- i1020

Location

The NDCAC, located in Fredericksburg, Virginia, opened in early 2013. The NDCAC facility is staffed with technical experts dedicated to supporting the law enforcement community. It also accommodates technical training sessions and meetings between law enforcement and industry.

Points of Contact:

Technical Resource Group
Main Number: 855-306-3222
E-mail: askndcac@ic.fbi.gov

NDCAC Main Number: 540-361-4600
E-mail: ndcac@ic.fbi.gov

Marybeth Paglino
Director, NDCAC

NATIONAL DOMESTIC COMMUNICATIONS ASSISTANCE CENTER
NDCAC

NATIONAL DOMESTIC COMMUNICATIONS ASSISTANCE CENTER
NDCAC

Technology Sharing

Cell Site Database

- Database of cell tower information for the correlation of communication detail records
- Provides current and historical cell tower information
- All information is downloadable for law enforcement use

Catch and Handle

- Consensual monitoring software utilizing the Android OS
- The LEA is responsible for the device with service
- Administrative agreement is required

TRAP

- The Report Analysis Program allows the user to analyze many different types of data such as CDRs, NELOS, GPS reports and more
- Cell Site Database Access is required

i1020

- A machine to machine real time lookup service for lawfully authorized cell site location and sector information
- This service requires an intercept collection box system to interface with the service

IMEI Database

- A lookup tool to research a particular device (ie. make and model, supported bands and wireless capabilities).
- The information is based on the Type Allocation Code (TAC) within the IMEI

CrossTalk

- Designed to assist with open source internet research by automating the submission of search terms to third-party websites and organizing the information in a data card
- Access as a Chrome extension

RIPT

- Imports communication IP Data lawfully obtained by LEAs
- RIPT does an RIR "WhoIs" lookup on all unique IPs found
- This tool is able to read various file types, parse out relevant information and then create a useful report with quick to read statistics and IP ownership

U2L

- Useful Utilities Lite is an Android application that combines a number of different spreadsheets and calculators needed to complete cellular analysis
- Copy the results to use in another application (email, etc)
- SMS results to other teammates

Facebook Messenger Tool

- Imports Facebook Messenger communication XML data lawfully obtained by LEAs from Facebook
- Ingests multiple files to create single report
- Creates comprehensive reporting in an Excel format

Gambit Unified Tool Suite

- A suite of tools that parse and plot geo-location data (cell tower or GPS information)
- Data is parsed for important geo-mapping details (latitude, longitude, direction and speed)
- Geo-location is mapped
- Common message types include the real time i1020 cell tower mapping and precision location GPS emails

.Social

- Parses content and media out of the Social Media return, organizes and makes it searchable by a series of categories.
- Performs analysis of the data in order to determine close friends, common IPs, common devices, timeline of activity, etc.
- Exports Social Media Return, filtered data and pertinent Data to csv.

iNimbus

- Reads in a raw iCloud backup zip data file, pursuant to lawful process.
- Uses the key included in the search warrant return to decrypt and reconstitute the content into their original format and directory paths based on instructions and decryption keys contained within the input zip file.
- Output all the original content into another zip file and create an excel report containing summary information regarding all the processed content.