Forensic Analytics

CSAS & Cell Site Analysis

Cellular Forensics Workshop

Version 1.0

09/05/2015

Course Code: FA012

Page left intentionally blank

Contents

Forensic Analytics

Background

Forensic Analytics Ltd was formed in 2013, but its principle staff have long experience in the telecoms and forensic industries.

Forensic Analytics' main business area is the development of data processing software tools that automate the most time-consuming aspects of cell site analysis. Our first product was CSAS (the Cell Site Analysis Suite), which provides a range of features designed to process, query, map and present mobile phone call records.

We also make use of our extensive technical backgrounds to provide consultancy, training and competence transfer services to law enforcement and forensic customers.

Forensic Analytics deals with many organisations that are new to cell site analysis. In addition to the training we can provide for users of our software, we are also able to offer training on the wider topics of cell site analysis and telecoms in general.

Cell Site Training

Organisations that wish to increase the level of cell site knowledge in their staff often require a series of courses that range from basic mobile telecoms overview courses through to complex technical discussions of cell site analysis and forensic radio survey techniques.

Such a programme of courses would be aimed at providing foundation knowledge on radio transmission, cellular network operations and the methods employed to generate and store billing and subscriber data. A typical cell site training programme might progress to include the development of competence in forensic radio survey techniques to enable the organisation to undertake their own surveys following current best practice guidelines.

A second strand of the training would be in providing the customer's cell site analysts with the knowledge and software tools they require to enable them to understand the content of CDR (Call Detail Records), which provide details of each call/text/data session made or received by an individual's mobile device. The Forensic Analytics CSAS (Cell Site Analysis Suite) software tool would be used as the basis of this programme and the course programme would include full training on CSAS as well as on wider cell site data processing techniques.

Forensic Analytics also has links with Wray Castle (www.wraycastle.com), a world leading provider of telecoms training, through whom we are able to offer access to a wide range of cellular technology and general telecoms training courses.

The expected outcome from such a training programme would be for personnel to have acquired the skills necessary to allow them to conduct their own cell site analysis investigations autonomously using industry standard tools, equipment and techniques in line with current best practice guidelines.

Participants in more advanced training programmes would eventually be expected to reach a level of competence that would allow them to be accepted as expert witnesses in cell site cases.

Cell Site Analysis

Cell site analysis attempts to provide evidence of where a mobile phone may have been when certain calls were made.

Mobile phone networks consist of a large number of radio ‘cells’ each of which covers a limited geographical area. Each cell is assigned a unique ‘Cell ID”, which is captured in the billing record (CDR) when calls are made.

Network operators are able, under tight regulatory guidelines, to provide details of the calls made by ‘target’ phones and can also provide details of the locations of the cells used by those phones.

Cell site analysis is designed to enable an investigator to determine whether calls made at or around the time of an incident or offence used cells that are located near the location of that offence.

Additional evidence can be provided by undertaking an RFPS (Radio Frequency Propagation Survey) at each significant location. RFPS equipment captures details of the cells that can be detected at a location and can indicate which cells are mostly like to be selected for use by a phone at those locations.

Cell site analysis, based on a combination of a phone’s billing records, cell location details and RFPS results, can provide compelling evidence to support an allegation made by investigators.

Course Outline

Course FA012 – Cellular Forensics Workshop

Duration: 0.5 days (4 hours)

Intended Audience: all levels of participant

Maximum Participants per Delivery: 50

Course description:

This course has been designed to provide a non-technical overview of cellular forensics, including cell site analysis and mobile device examination and introduces some of the activities undertaken to complete a forensic mobile investigation.

Along the way it introduces the many different types of information that can be combined to support an investigation, from cellular billing records, to handset examination reports, CCTV analysis, ANPR cameras and others.

The workshop is scenario-based, so all subjects will be presented as part of a coherent digital forensics investigation.

One of the objectives of the workshop is to highlight the time-savings that can be achieved by using an automated data processing tool, such as Forensic Analytics' CSAS (Cell Site Analysis Suite) tool, the use of which will be demonstrated alongside more traditional manual investigative methods.

We will provide free copies of our *Cell Site Analysis: A Guide for Investigators* booklet at each event.

Pre-requisites: none

Course Objectives: provide participants with basic details of how cellular networks work and with hands-on experience of the basic investigative activities undertaken to progress a digital forensics investigation.

Simple Course Overview

- Introduction – Forensic Analytics
- Cellular network types & how they work
- Sources of forensic information
- Scenario – bank raid in Letchworth
- Investigative stage 1 – Forensic radio coverage surveys
- Investigative stage 2 – handset download techniques
- Investigative stage 3 – request celullar billing records, perform cell site analysis
- Investigative stage 4 – identify WiFi hotspots used by target phone
- Additional CCTV evidence provided
- Investigative stage 5 – ANPR requests
- Recap the investigation and show how the dots were joined together
- Review the time taken to manually process the investigation
- Introduce CSAS – reprocess case data using automated methods
- Summary & Questions

Detailed Course Content:

1. Introduction – Forensic Analytics
2. Cellular network types & how they work
3. Sources of forensic information
    a. Device downloads
    b. Call Detail Records
    c. WiFi session logs
    d. Ancillary data – ANPR, tracker, satnav, CCTV,
    e. Witness sightings
4. Cell site analysis
    a. CDR analysis
    b. RFPS (forensic radio surveys)
    c. Cell site conclusions & evidence
5. Scenario – bank raid in Letchworth
6. Investigative stage 1 – RFPS survey objectives
    a. Workshop 1 – RF survey results
    b. Review survey results obtained from crime scene to see which cells provide coverage there
7. Investigative stage 2 – suspect is identified following a tip off. He is arrested and a handset is recovered
    a. Overview of device download systems – Cellebrite, Radio Tactics, XRY
    b. Workshop 2 – review handset download data – confirm target phone's number; try to determine the phone book names attributed to the other suspect's phone numbers based on analysing the content of the text message logs
8. Investigative stage 3 – as the suspect's phone number has been identified, request comms data from provider
    a. Overview of RIPA and the request process
    b. Workshop 3 – receive raw comms data, attempt to determine the Top 10 numbers called/calling for the phone and the cell site most often used
    c. Attempt to determine how often the target phone was in contact with phone's belonging to the other suspects (based on the text message analysis in step 7b)
    d. Create map of the cells used in the 30 minutes before the bank raid
    e. Look at the calls made immediately prior to the bank raid – do any if the cells used serve at the bank (refer RFPS results obtained in step 6b)?
    f. Problem – none of the cells serve and the call closest in time to the raid has no cell ID, in fact only has a MAC address – this means that it was a VoWiFi call
    g. Use device download report from step 7b to find the WiFi provider and username in use at the time that call was made
9. Investigative stage 4 – identify WiFi hotspots used by target phone
    a. Make a RIPA request to obtain WiFi session logs from the provider identified in step 8g
    b. Workshop 4 – correlate WiFi session (from WiFi session logs) with VoWiFi call record (from comms billing records) to determine the location of the hotspot used
    c. This shows that he call was made via the WiFi hotspot in a coffee shop near to bank
    d. Show the location of the coffee shop (based on the address information provided) on a map and compare to the location of the bank
10. Investigations at the coffee shop produce CCTV stills showing a car drawing up, then men running towards the bank, get the vehicle's VRM from the still images
11. Investigative stage 5 – ANPR requests
    a. Request ANPR data for the car's VRM
    b. Workshop 5 – correlate ANPR data (which shows postcode of cameras) with CDR call logs, which show postcode of cells – produce a new map showing locations of cameras vs cells
    c. Prove that user of target phone was in the car that was used in bank raid
12. Recap the investigation and show how the dots were joined together

13. Review the time taken to manually process the investigation
14. Introduce CSAS – do all of the above exercises again but using CSAS
    a. Import & Summarise RF survey results
    b. Import handset download data
    c. Produce address book summary
    d. View text message logs
    e. Import comms billing data
    f. Show cell locations on a map
    g. View WiFi session logs in handset download data
    h. Import ANPR data
    i. Correlate comms billing records with ANPR data
    j. Show correspondences on map
    k. Produce evidential call schedule
    l. Cellsite conclusions
    m. Time saving resulting from use of CSAS
    n. CSAS Product range & markets
15. Summary & Questions

Free copies of our Cell Site Analysis: A Guide for Investigators are also available by emailing cellsiteguide@forensicanalytics.co.uk

CSAS Software

The practical data processing aspects of our training programmes are based on the use of our CSAS (Cell Site Analysis Suite) software tool. This has been developed to simplify and automate the data processing and analysis work associated with cell site analysis.

CSAS – the Cell Site Analysis Suite – speeds up the call data processing tasks and also removes the human element, which is often the unwitting cause of inaccuracies or missed information. CSAS functions can be summarised as follows:

Cleanse CDR Data – all CSPs have different CDR formats, which often have to be combined into a single table for evidential purposes. The whole area of analysing pages of billing data and taking out repetition or collapsing multiple CDR entries into a single record is known as cleansing the data and is often the bane of an analyst's life.

It is an area where mistakes are easily made and it consumes a disproportionate amount of time. CSAS imports CDR billing files and cell site addressing files and combines and cleanses the data almost instantly (dependent upon data volumes) to create an evidential call table with colour-coded handsets and associated attribution details.

We currently recognize over 45 individual UK billing formats and have the ability incorporate international formats quickly and simply. As there are only three Cellular Service Providers (CSPs) operating in <customer> – this should be easy to achieve with the co-operation of the <customer>i Ministry.

As investigations evolve and target mobiles are added or removed from the investigation, CSAS enables this seamlessly and efficiently, instantly updating the database as old file or phones are removed or new files are added, whilst keeping an audit log for continuity purposes.

Analyse Data – Once data has been cleansed it is placed into a professional-grade database. Once in the database it can be viewed (using our filters or by using our powerful CDR Browser feature), filtered (by date/time, called/calling numbers, call type, etc.) or queried (using our best-in-class analytical engine). CSAS Analytics supports a range of standard queries – Top Callers, First Call/Last Call analysis, IMEI & IMSI timelines and many others - which allows analysts to gain quick, accurate access to information related to however many handsets feature within an investigation.

RF Survey Results – CSAS will import and process raw RF survey data captured by common RF survey devices, such as CSurv, NEMO, TEMS or CSU-4L. The data will be averaged and tabulated ready for analysts to review. CSAS also makes survey results available to CSAS Analytics, allowing it to be used as the basis for further queries and analysis, such as creating call tables showing calls made using cells that serve at key locations.

Mapping – the call data in the CSAS database can be used to automatically populate maps with call and cell details using Microsoft MapPoint or Google Maps and can also generate Map Labels for PowerPoint mapping presentations at the push of a button.

Continuity – CSAS treats each investigation as a separate case and as an investigation evolves, CSAS will log activity for continuity purposes providing an audit trail.

CSAS is a modular product, with each module supporting a specific range of functionality. The licence structure reflects the modular nature, with higher licence fees payable for higher levels of functionality.

The CSAS licence tiers are as follows:

CSAS Desktop Standard

- Fast, accurate automated CDR cleansing (75+ UK formats currently supported and international formats can be easily added)
- CDR Browser, allowing data to be viewed and filtered on screen
- Ability to 'colourise' target phone numbers and attribute to individuals
- Ability to view, manage, edit and import cell address details
- Ability to create call labels to add to Powerpoint map presentations
- Ability to create court-ready call table output files in Excel
- Audit file creation for simple case continuity management
- Case import/export function allows case details to be shared between CSAS users

CSAS Desktop Enhanced

- Ability to define significant times, events, locations and individuals
- Enhanced attribution management
- CSAS Desktop Enhanced provides access to a number of optional modules:
    - **Analytics module (integrated)**
        - Access to CSAS Analytics, 20+ powerful data query types
        - Analysis of single phone, pair of phones, groups of phones
    - **Mapping module (integrated)**
        - CSAS Mapping, create maps directly from the call data
        - Integrates with using Microsoft MapPoint, OS maps, ESRI, Northgate, web-based mapping applications (Google Maps or Bing Maps), up to 40 map data sources
        - Develop court-ready mapping presentations in CSAS and export to Powerpoint or Playback
    - **RF Survey module (optional)**
        - Import and process raw survey data from CSurv, NEMO, TEMS
        - Analytics and Mapping features related to RF survey data
    - **DMI (Digital Media Investigator) module (optional)**
        - Process non-cellular comms data – landline, interconnect, social media (WhatsApp, BBM, etc)
        - Import and process handset/SIM download data from radio Tactics, XRY, Cellebrite, etc
        - Create combined call schedules that include cellular and non-cellular data
    - **Playback module (optional)**
        - Create animated mapping, call data or RF survey data presentations to visualise data or to display in court

CSAS

Streamlining Cell Site through Automation

Training Services

Forensic Analytics Ltd
PO Box 324
Letchworth Garden City
SG6 9FL

0800 158 3830

training@forensicanalytics.co.uk
www.forensicanalytics.co.uk