

SecurCube

What we do

SecurCube®

Investigative tools

- CDR (Call Detail records)
 - Standalone
 - client/server
- Cell forensics (BTS)
- SecurCube Downloader
- SecurCube Forensics Report

Security devices

- IMSI Catchers detector

Services

- Training
- Digital forensics examinations (EnCE – CCME - ...)

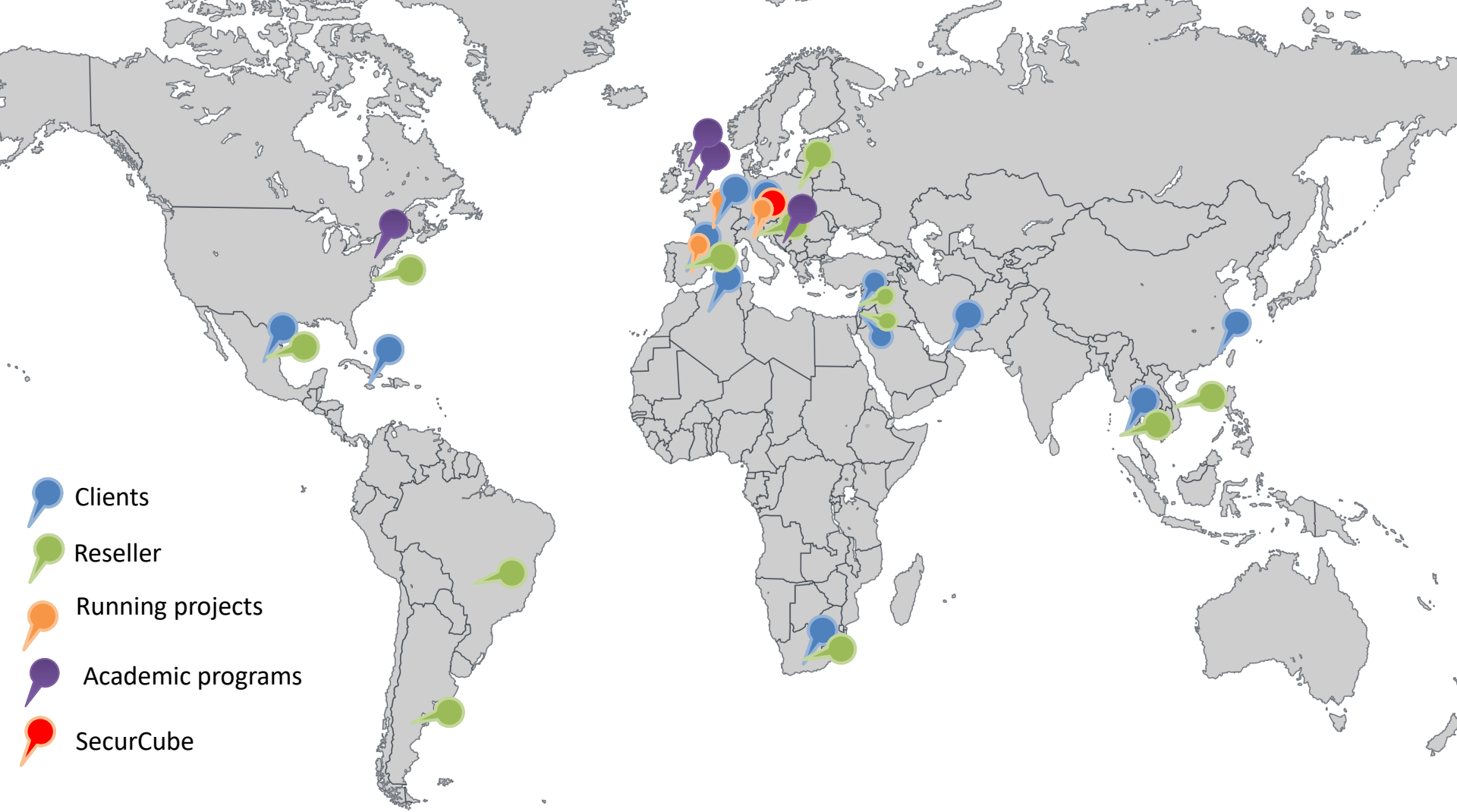
**Our
customers**

SecurCube®

**Police
enforcement**

**Private
Investigators**

**Academic
programs**



SecurCube Forensics Report

Automate the final reports creation,
following the international best
practices of the computer forensics



5 Add
Five
Hours
To
Your
Day

SECURCUBE FORENSICS REPORT

CUSTOMIZABLE AUTOMATED
REPORT CREATION
BEST PRACTICES COMPLIANT

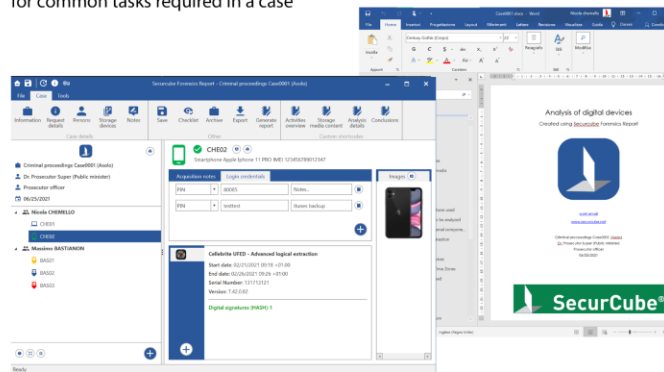


REDUCE THE TIME IT TAKES TO FILE FORENSICS REPORTS

Drag and drop
your acquisition logs
and let the software
create well written
word document,
compliant with international
best practices for
digital forensics.

Case management and automations
for common tasks required in a case

Easy to use error free
Highly customizable
Case Management
Automated tasks
Device status



Download your free 30 days trial: www.securcube.net

Forensics Report

Automate the acquisition's final report creation

Drag&Drop to create an editable word document

The screenshot displays the SecurCube Forensics Report application window. The title bar reads "Securcube Forensics Report - Criminal proceedings Case0001 (Asolo)". The interface is divided into several sections:

- Top Menu:** Includes "File", "Case", and "Tools". The "Tools" menu is expanded, showing options like "Information", "Request details", "Persons", "Storage devices", "Notes", "Save", "Checklist", "Archive", "Export", "Generate report", "Activities overview", "Storage media content", "Analysis details", and "Conclusions".
- Case Details Panel (Left):** Shows the case name "Criminal proceedings Case0001 (Asolo)", the prosecutor "Dr. Prosecutor Super (Public minister)", the officer "Prosecutor officer", and the date "06/25/2021". Below this, a list of users is shown: Nicola CHEMELLO (with sub-items CHE01 and CHE02) and Massimo BASTIANON (with sub-items BAS01, BAS02, and BAS03).
- Main Report Area (Center):** Displays details for device "CHE02", identified as a "Smartphone Apple Iphone 11 PRO IMEI 123456789012347". It features a table for "Acquisition notes" and "Login credentials":

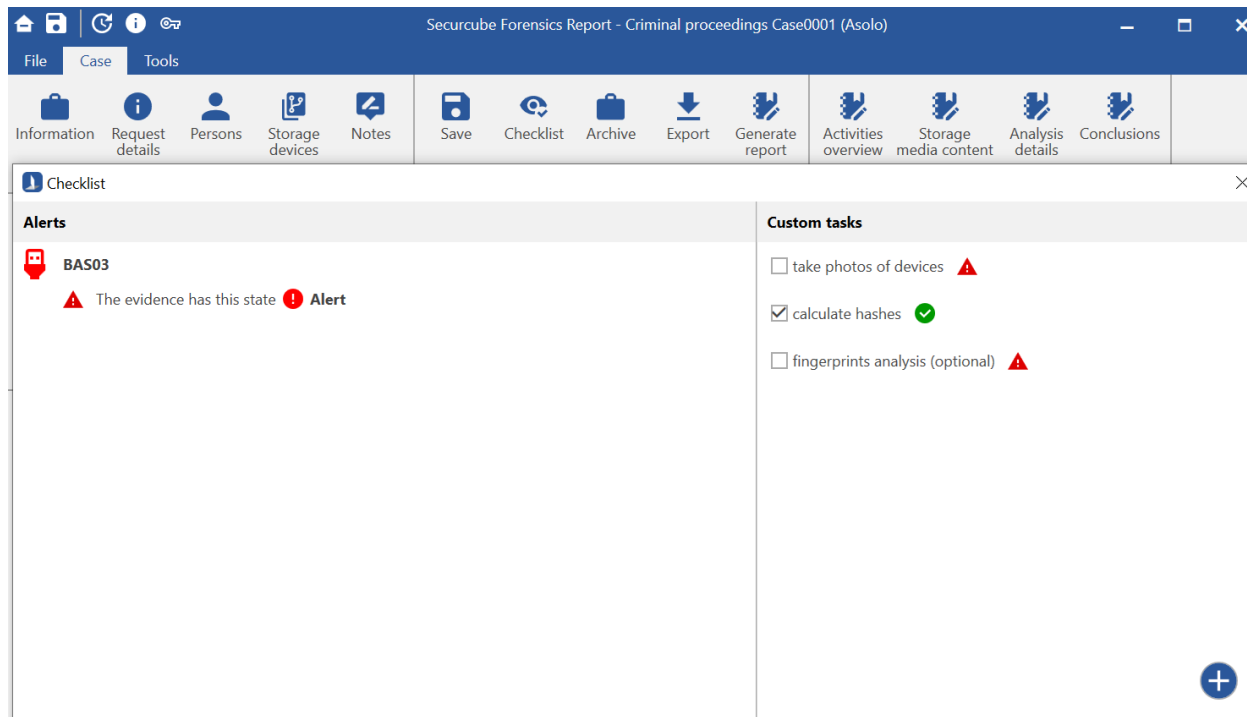
Category	Field	Value	Notes
Acquisition notes	PIN	80085	Notes...
	PIN	testtest	itunes backup
- Technical Details (Bottom Center):** A section titled "Cellebrite UFED - Advanced logical extraction" provides the following information:
 - Start date: 02/21/2021 09:18 +01:00
 - End date: 02/26/2021 09:26 +01:00
 - Serial Number: 131713121
 - Version: 7.42.0.82
 - Digital signatures (HASH): 1
- Images Panel (Right):** Shows a thumbnail image of the iPhone 11 Pro.

The status bar at the bottom indicates "Ready".

Checklist – ToDo list

Double check if you
Filled all the
Information required
In your case

Alerts if you missed
anything



The screenshot displays the SecurCube Forensics Report application window. The title bar reads "Securcube Forensics Report - Criminal proceedings Case0001 (Asolo)". The interface includes a menu bar with "File", "Case", and "Tools". Below the menu is a toolbar with icons for various functions: Information, Request details, Persons, Storage devices, Notes, Save, Checklist, Archive, Export, Generate report, Activities overview, Storage media content, Analysis details, and Conclusions. The main content area is titled "Checklist" and is divided into two sections: "Alerts" and "Custom tasks".

Alerts

- BAS03**
 - ⚠ The evidence has this state ⚠ **Alert**

Custom tasks

- take photos of devices ⚠
- calculate hashes ✓
- fingerprints analysis (optional) ⚠

A blue plus sign icon is visible in the bottom right corner of the application window.

The result: Word document

Result: Word document

Introduction

Description of the standard procedures used

This report presents the forensic procedures usually used when performing a digital autopsy. Any software and hardware used will be described when the procedure of the forensic report. In the case of an operation from the above procedure, there are described and explained in detail the reasons, objectives and analysis sections of the document.

Visual identification of the media to be analyzed

Before starting the forensic process, a complete inventory of all hardware equipment will be made, highlighting its technical characteristics in order to comply with the operational procedures to be performed.

Examples of hardware materials and equipment

- Computer desktop, laptop, server, etc., usually containing magnetic hard disk or several SSD memories.
- Mobile devices (mobile phone, personal digital assistant, GPS navigation, ...).
- Optical media (CD-ROM, DVD-RW, Blu-ray).
- Storage units (on magnetic tape, on magnetic disk, on optical disk, on external device).
- Removable device (USB interface, Flash, SD type memory cards, ...).
- Keyboard or a pointing device (using to make voice call, voice device (with headset) or any device that supports Call Center features).

Physical removal of the various internal components

If it is not possible to be analyzed a hard or optical computer, a server, or another device containing sensitive information, it is a good idea to be able to proceed with the disassembly of the anterior case and the consequent removal of hard components. Once the components that store the information to be analyzed have been identified, and having recorded their location (photographs for example, the serial number), the next step is to remove the device and subsequently make the acquisition of data. The parts of the analyzed materials are integrated within the forensic image or in the generated log file.

Figure 11

- Automatic backup (making of source and destination).
- WiFi and GPRS backup (the detection and handling of non-protected data (SMS on source and destination sites).

[[www.gigaset.com]]



COOLICE™ **EMRICE**
A low risk solution for finding, collecting and preserving digital forensic evidence. As technology evolves so do the challenges of digital forensic investigation. Investigators must deal with devices and operating systems, report on data and user behavior and generate reports in a fast, efficient, repeatable and transparent manner. The COOLICE™ EMRICE™ Forensic Evidence Manager™ is a comprehensive digital forensic investigation tool built with the investigator in mind. Reduce investigation time by fully tracking digital forensic data.

COOLICE™ EMRICE™ provides comprehensive digital forensic capture, acquisition, management, case analysis with detailed logs to help investigators understand, repeat or reproduce an investigation and generate a report.

Home: The Best Computer Forensic Solution (anytime) available running on 32 Windows.

Figure 14

Forensic image creation or data extraction

Forensic copies can be acquisition of two types:

- Physical copy (bitstream copy)
- Logical copy

A bitstream copy (bitstream) is an exact duplicate of the entire original media, including the data stored in memory locations that have not been used or are previously used and that devices are not normally accessible to the user (in particular, the file system). Understanding analysis, it is possible to proceed with the logical copy of many contents. The copy size can be smaller because contents are not larger duplicates with the master image of a device analyzed. This activity is carried out using appropriate hardware and software tools that can generate forensic procedure, differences depending on the type of device being analyzed. It is not possible to proceed with the bitstream acquisition of the information contained within the device to be analyzed. Having performed forensic acquisition of the contents of photographic documentation of the same can be used depending on the type of investigation or data without analysis.

When forensic copy procedure has been completed (for images of hard, optical and server), a good acquisition or a transcription (depending on the nature of the original media) is recommended and copied to the image of a compressed archive. The procedure is supported by software that the user can download to carry out the original data. Supply a copy of the media to avoid data loss in case of the acquisition technology used.

- Cloud Document copy (read with the technical report to be written in records)
- Cloud file copy (depends on read with the technical report, which can be used for further investigation by the judge or other involved parties)
- Internationally transferable copy, in which the user needs to answer the question asked and which is defined on the time of the non-report

In addition, that the copies are made are exact the same, and that the authenticity of the data is guaranteed by the digital signature in this report.

The choice of which one to use in the reports or which one to use for further investigation is made by the user, the selection between Cloud Document Copy and CloudCopy file is made by the user.

[[www.gigaset.com]]



The acquisition procedure shows the details of the forensic image created, and the final report (example in PDF, DOC, OpenOffice, compressed archive, ...).

Figure 13

Storage of the original devices

The activity described in the forensic process and the devices (hardware and software) used to perform the forensic copy / data extraction from the devices subjected to the forensic investigation.

Content analysis of the original devices

The analysis of the content acquired from the devices is forensic. This activity requires the forensic image analysis carried out on the forensic copy or a transcription.

In carrying a forensic image that consists of fragments checking the extracted contents is necessary, the analysis is performed on the original device documentation of the extracted operations.

Fixed report time considerations / time zones

When the generated reports, users (technical staff), the time zone is usually expressed in the UTC +3 format. The time zone (UTC) of the activity is usually expressed in a format of +1:00. When there is the same offset between the user for legal accounting, and the device (UTC +3) the acquisition corresponds to the time zone (UTC +3) format. If the user and the device are in the same time zone, the time zone of the acquisition, in reference to the UTC +3, the time zone is also called UTC+3. The acquisition time is the time generated by the acquisition device of the operation (margin, reference to the UTC +3). The time zone is also called UTC+3. The acquisition time is the time generated by the acquisition device of the operation (margin, reference to the UTC +3). The time zone is also called UTC+3. The acquisition time is the time generated by the acquisition device of the operation (margin, reference to the UTC +3). The time zone is also called UTC+3.

If a function requires to check when the data is in the report in order to attribute the correct time conversion.



[[www.gigaset.com]]

Figure 14

Operating reports - analysis procedure

This section describes the procedures and software to be used in order to view the created forensic images from the generated reports.

Please note: these procedures are not the only ones that exclusively allow the visualization and further analysis of the data.

Capabilities

Analyses performed on mobile devices are generally carried out using COOLICE™/EMRICE™.

When the forensic tool used is the containing the report in PDF format is necessary to open the program, search the data and Open, and subsequently search the file in the file system to be analyzed.

Once this has been done, navigating the menu on the left action of the application interface will be the visualization of the file contents. The type of information reported depends on the data extracted from the processed data (see corresponding screen).

Figure 18

Description of the forensic tool used

The activity described in the forensic process and the devices (hardware and software) used to perform the forensic copy / data extraction from the devices subjected to the forensic investigation.

Content analysis of the original devices

The analysis of the content acquired from the devices is forensic. This activity requires the forensic image analysis carried out on the forensic copy or a transcription.

In carrying a forensic image that consists of fragments checking the extracted contents is necessary, the analysis is performed on the original device documentation of the extracted operations.

Fixed report time considerations / time zones

When the generated reports, users (technical staff), the time zone is usually expressed in the UTC +3 format. The time zone (UTC) of the activity is usually expressed in a format of +1:00. When there is the same offset between the user for legal accounting, and the device (UTC +3) the acquisition corresponds to the time zone (UTC +3) format. If the user and the device are in the same time zone, the time zone of the acquisition, in reference to the UTC +3, the time zone is also called UTC+3. The acquisition time is the time generated by the acquisition device of the operation (margin, reference to the UTC +3). The time zone is also called UTC+3. The acquisition time is the time generated by the acquisition device of the operation (margin, reference to the UTC +3). The time zone is also called UTC+3.

If a function requires to check when the data is in the report in order to attribute the correct time conversion.

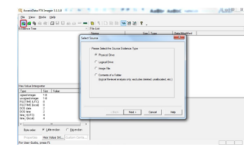


[[www.gigaset.com]]

Figure 14

[[www.gigaset.com]]

[[www.gigaset.com]]

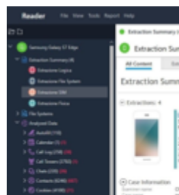


[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

Figure 14



[[www.gigaset.com]]

Figure 19

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

[[www.gigaset.com]]

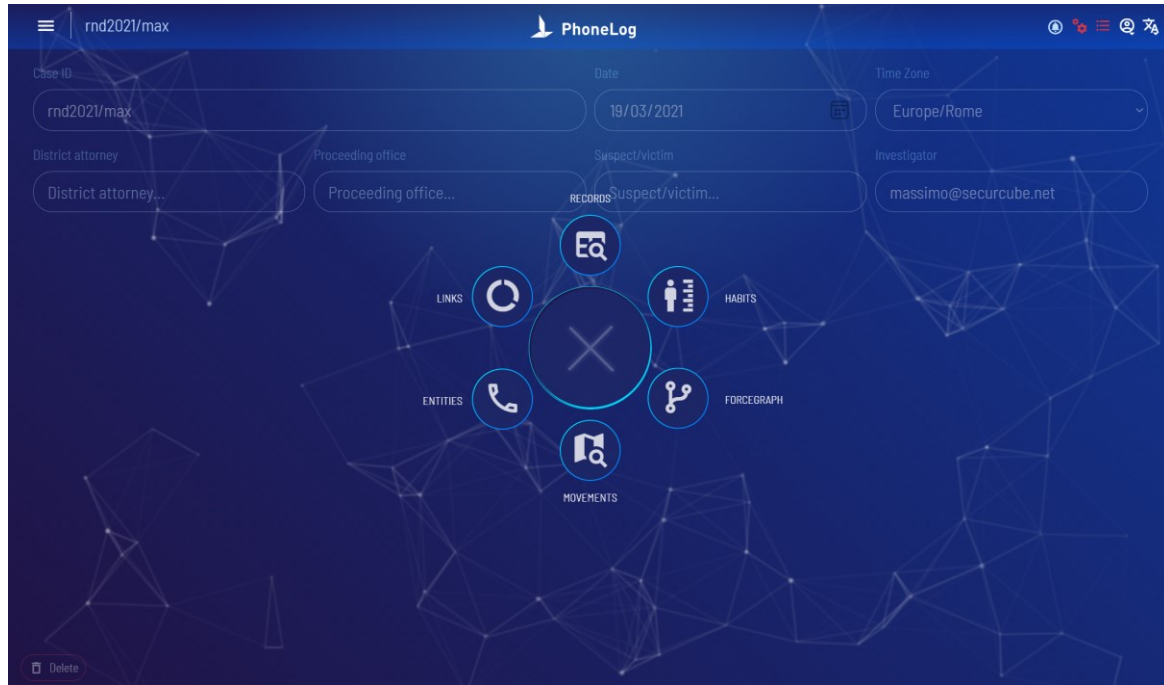
Figure 19



PHONELOG

CDR analyzer, data correlation & data validation

One interface – multiple sources



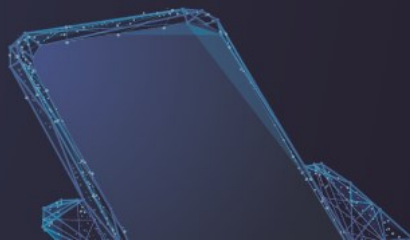
SECURCUBE PHONELOG

Software for phone records investigation and digital evidence correlation

Discover the modern forensics solution for communication records analytics, validated with smartphone generated evidence.

Designed by forensic experts and based on international law enforcement experience, court cases, and global best practices.

The all-in-one easy to use platform:
Import, analyze, and cross reference multilevel evidence including phone records, GPS logs, CCTV camera feeds, cell site real coverage, and much more.



Phonelog

Data validation

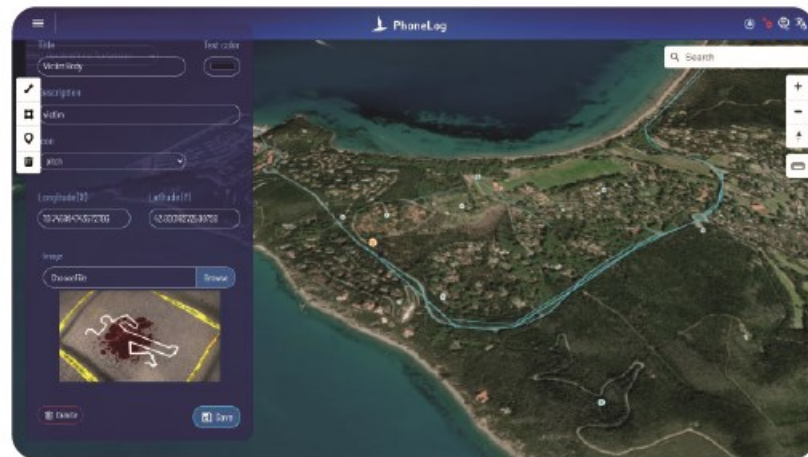
PhoneLog provides specific data analytics and mapping functions of your digital evidence.

Line up, confront, and map all your sources together by importing different types of mobile data to one system.

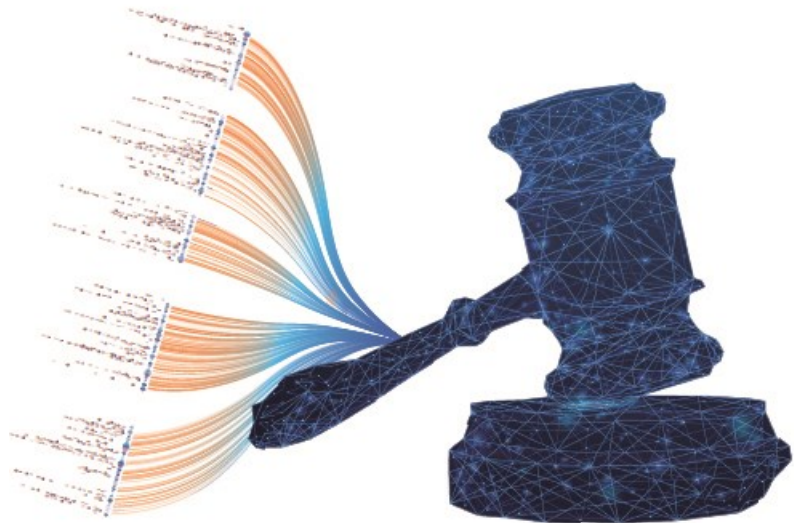
Pictures extracted from a device have metadata indicating when and where they were taken.

Call Detail Records log information on the cell towers to which the device connected to, which further validates and strengthens the specific mobile extraction.

Import CCTV camera feeds or vehicle GPS files: show them in parallel with CDR and mobile extractions creating a solid visualization of multiple-source evidence. A picture extracted from a device with a spoofed position in conflict with CDR data is automatically discovered and shown with precise cross referencing analytics. PhoneLog correlates multiple streams and delivers the 360° data validation every digital investigation requires.



Phonellog



Professional courtroom presentations

PhoneLog focuses on forensic international best practices: evidence integrity is warranted and protected by the built in Hash Code System: data is never modified or corrupted. Users can:

- **Integrate** the results with other solutions such as i2 Analyst's Notebook, for a smooth harmonization of multiple forensic applications
- **Export** every step of the analysis in easy to understand and customizable diagrams, charts, images, and voice-over video animations for the clearest display of the results.

Our experience in the courtrooms guarantees the best possible criminal case presentation.

Phonelog

Case scenarios

PhoneLog is designed to investigate criminal activity. In **kidnapping** cases, importing and mining mobile evidence is extremely useful. Start with:

- The complete cell tower traffic in the last seen area
- The victim's user CDR and last connected cell tower traffic

Cross reference a number of possible suspects to the missing person's last mobile activity and connected cell towers. Statistically analyzing the victim's mobile footprint and discovering deviations from the norm can lead to breakthrough insights.

When investigating **drug trafficking**, highlight potential meeting points or patterns among many persons of interest as single entities and as a group.

With just a few clicks define: users habits, most used locations, interactions, meeting points.

Continue to import evidence and open multiple pathways and to solve crime with PhoneLog.



Phonelog

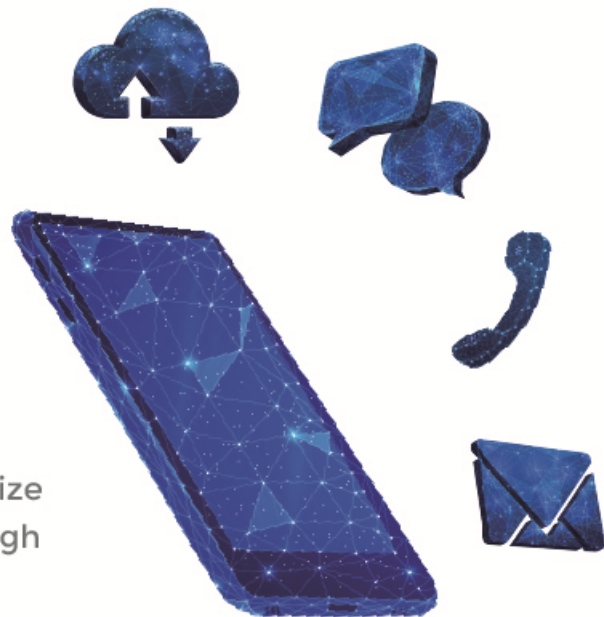
The digital environment

Everyone uses their smartphones to call, text, browse the web, and e-mail. The mobile networks that surround us run in parallel with the real world, turning people into traceable mobile identities.

Information is automatically stored in phone records and in a device's memory, an invaluable source of evidence for criminal court cases. The goal of digital forensics is to collect, define, and analyze this data to solve crimes, following digital footprints and reconstructing past events.

SecurCube PhoneLog is designed to empower investigators and maximize the potential of evidence generated by smartphones, validating it through third party and unalterable CDR data.

Achieve the most complete analysis results in the least amount of time.



Phonelog



Mobile forensics evidence

Smartphones produce key evidence that translates into opportunities for investigators to exploit.

Call Detail Records

The most impartial and reliable evidence source today.

Carriers automatically collect and store mobile data for billing purposes:

- Users, date, duration, and type of event: calls, SMS and data connections
- ID and location of every cell tower connecting to the SIM card
- All traffic generated by the network

Mobile Extractions

Technology that enables collecting a device's memory: pictures, e-mails, texts, internet navigation history, and more.

Cell Site Analysis

A careful survey of where cell towers spread their signal is the basis of a smartphone's past **geo-localization**.

Dig deeper with additional evidence: **CCTV camera feeds, GPS data, wiretaps, license plates, and much more.**

The user-friendly environment where all these types of data are analyzed, cross referenced, and maximized.

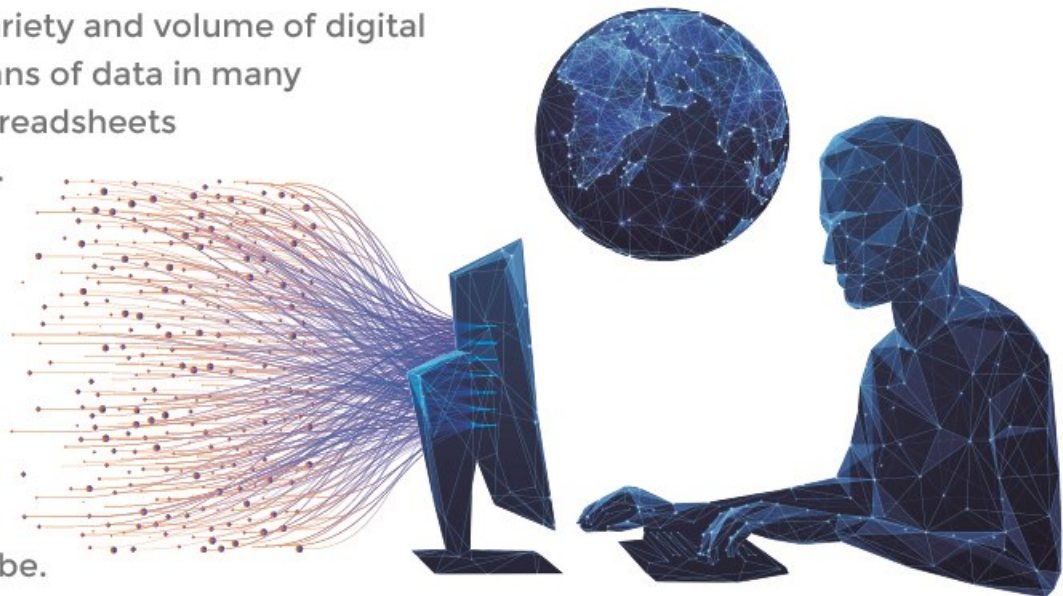
Phonelog

PhoneLog advanced importing

Analysts are usually overwhelmed by the variety and volume of digital evidence in a criminal case: rows and columns of data in many different formats. Stop wasting hours on spreadsheets and tools not designed for mobile forensics.

PhoneLog **Artificial Intelligence** imports and organizes data quickly and efficiently, uncovering hidden stored information. Save time, manpower, and resources by automatically and forensically creating evidence databases.

More cases solved in less time regardless of carrier, format, or structure with Securcube.



Phonelog

Investigation management

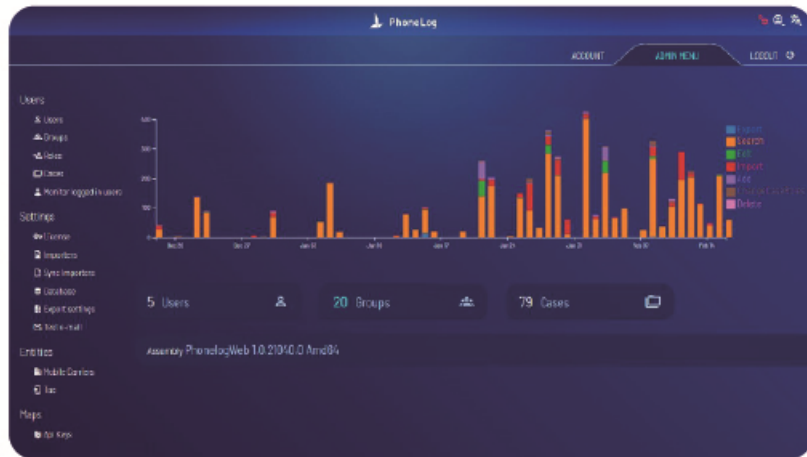
Phonelog is a flexible platform with custom solutions for every organization and each unique criminal case. The new browser-based solution does not require any software installations.

It can be used both online and offline.

Analysts can work on the same case and database, or on multiple ones on the shared platform, depending on the specific tasks and rights assigned to them.

An administrator account easily manages user roles, work groups, progress, and results in real time.

Our **support system** will train, certify, specialize, and assist PhoneLog users in their own language.



Phonelog

Statistical data mining: unlock digital footprints with your evidence

Once digital evidence is imported to PhoneLog, perform modern, in-depth **analytical investigation**. Functions developed in partnership with global law enforcement designed to optimize criminal research.



- Follow intuitions, and insights with precise queries specifically custom built for digital forensics like meeting points and movements
- Search records and entities
- Extract multiple user habits, connections, and patterns
- Understand digital footprints and the links to other users
- Analyze devices, cell tower environments, mobile extractions, social media accounts

PhoneLog develops a **solid and logical** method for the in-depth reconstruction of mobile profiles and alibis.

Phonelog

Mapping and movements

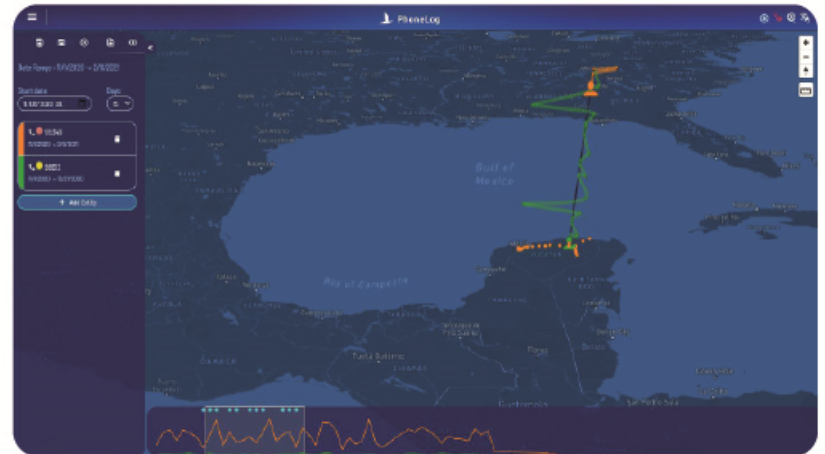
Every call, text, or internet connection is made by communicating with a cell tower. Phone records store specific location information relative to each cell in their networks.

Mobile forensics geo-locating technology relies on processing this information accurately.

Phonelog offers a state of the art **3D map** that can be populated with points of interest, pictures, and additional data traced by digital footprints created by smartphones connecting to cell towers.

Users can:

- **Animate** user paths, behaviors, and meeting points with others through Phonelog's state of the art mapping technology
- **Integrate** CDR theoretical coverage with statistical BTS Tracker real coverage data: the most complete mobile forensics map on the market



Phonelog

Main window

The screenshot displays the main window of the Phonelog application. The interface is dark-themed with a blue header. At the top left, there is a hamburger menu icon with a red notification badge containing the number '2'. The header text reads 'DEMO CASE - do not delete' and 'Caio'. The 'PhoneLog' logo is in the top right corner. Below the header, there are search filters for 'Case ID' (DEMO CASE - do not delete), 'Date' (15/03/2021), 'District attorney' (padova), 'Proceeding office' (CC Battaglia T.), and 'Suspect/victim' (Caio). A central navigation hub features a large 'X' icon surrounded by six circular buttons: 'RECORDS' (magnifying glass), 'LINKS' (circular arrows), 'ENTITIES' (phone handset), 'MOVEMENTS' (location pin), 'HABITS' (person with bar chart), and 'FORCEGRAPH' (network graph).

Phonelog

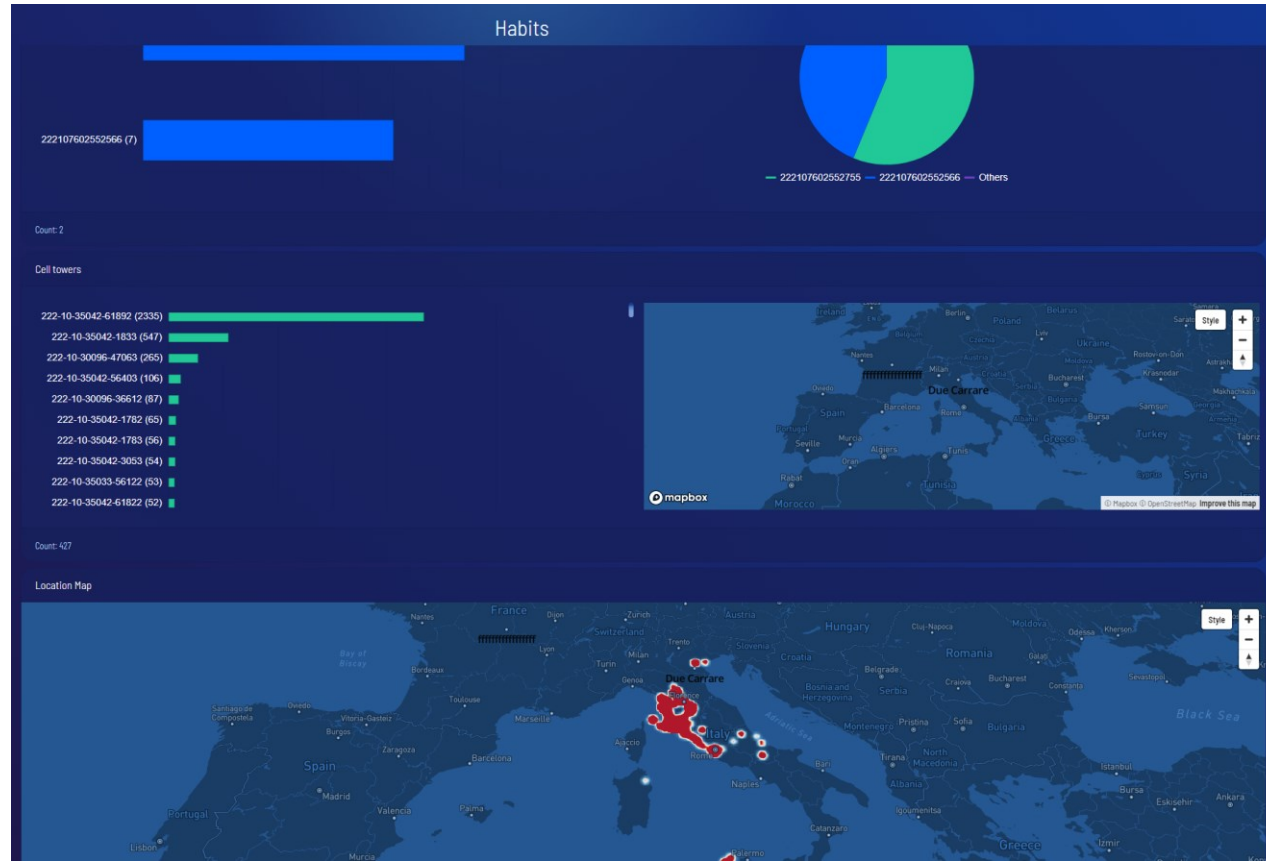
Habits:
Display statistics regarding one or two phone numbers, including the use of AI to highlight anomalies



Phonelog

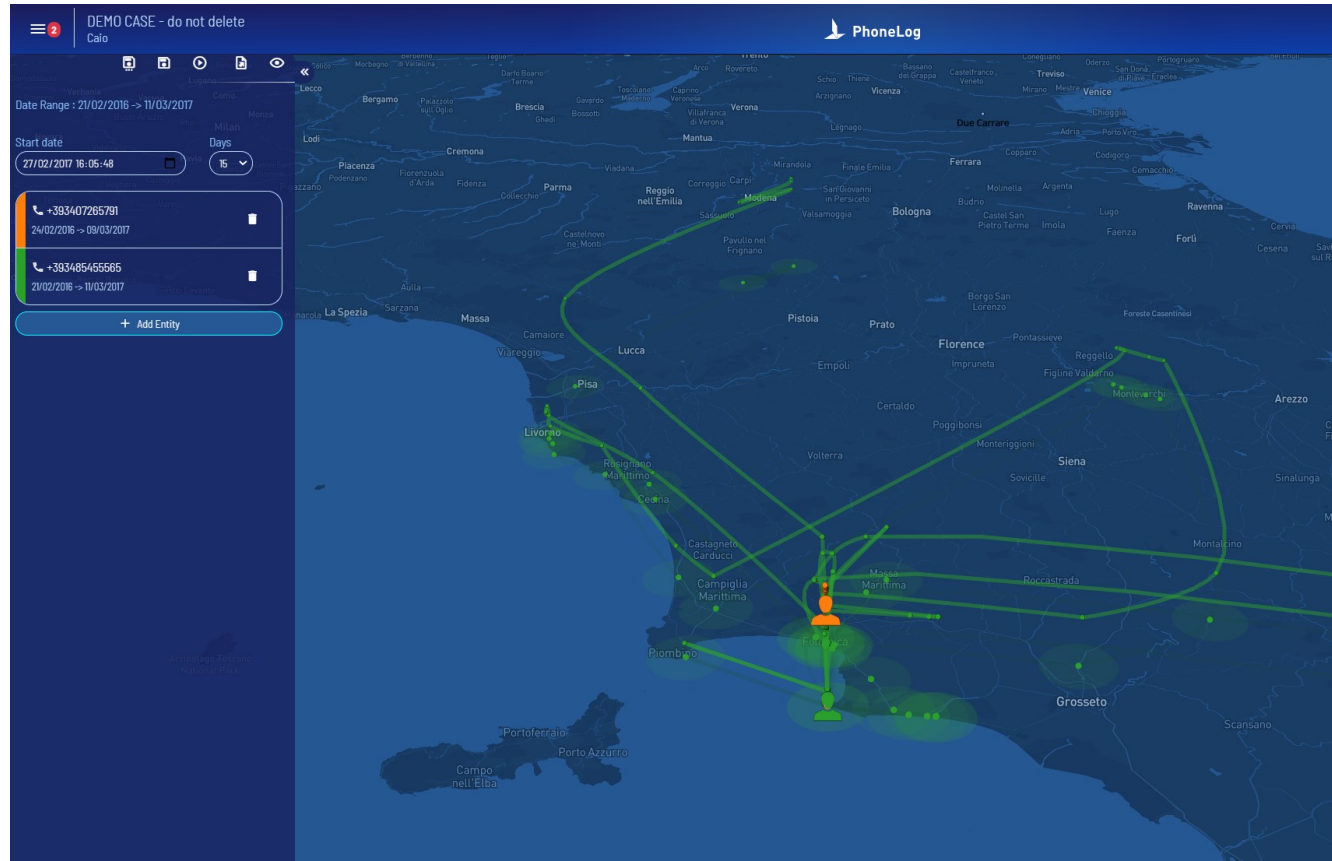
Habits:

Most contacted numbers, heatmap, map of movements, ...



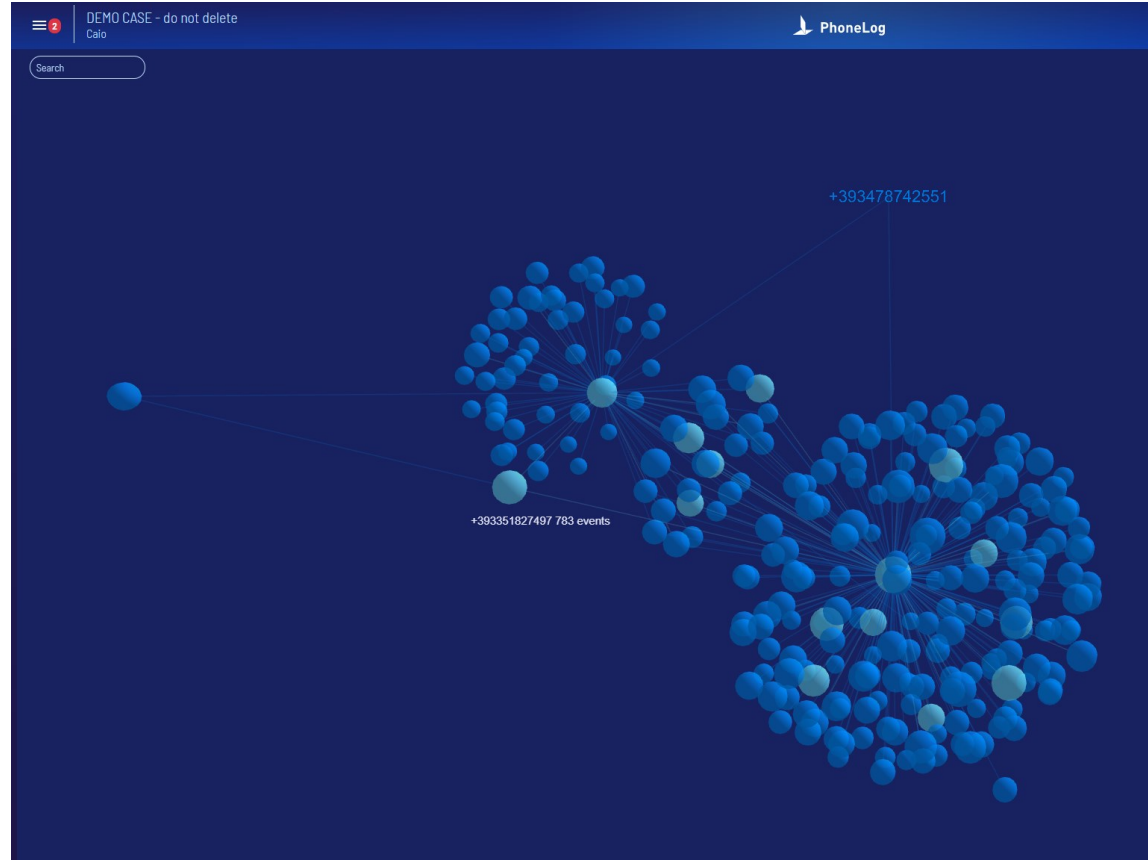
Phonelog

State of the art 3D map showing paths, timeline, meeting points, ...



Phonelog

ForceGraph:
3D link maps between
users inside the case



Phonellog

Links:
Visual highlights of
connections between
users



Phonelog

Data validation and correlation: mobile extractions, CDR, GPS paths all together

The screenshot displays the Phonelog interface. At the top, there is a navigation bar with a menu icon, a title "DEMO CASE - do not delete", and the "PhoneLog" logo. Below the navigation bar is a map showing the coastline of Tuscany, Italy, with a green shaded area indicating a specific location. The map includes labels for various towns and regions such as Piombino, Populonia, Fiorentina, Calmaria, La Spezia, Carrara, Follonica, Scarlino, and Punta Ala. The map is powered by Mapbox.

Below the map, the interface shows the date and time: "21/02/2016 08:23:29" and "00:09:57". A detailed record for a mobile phone number is displayed in a green-bordered box:

- Phone number: +393485455665
- Name: * Antonio Sarracino
- IMSI: 35338204764511
- MSISDN: 222107602652756
- Location: 222-10-35042-61892
- Address: Loc. Poggio del Barbero, CASTIGLIONE DELLA PESCAIA, GR

Below the record, there are several buttons and indicators:

- Record source: [Icon]
- Validated: [Green checkmark]
- Interactions between MSISDN: [Icon]

The "Files" section shows two files for download:

- CS - 5 - Suspect1_Antonio_Sarracino_User_3485455665.csv
- CS - 7 - Cell_Tower_Traffic_222-10-35042-61892.txt

The "Event Types" section shows a count of 2 events.

Phonelog

Comprehensive search
on records

DEMO CASE - do not delete
Cairo

PhoneLog

21 February 2016

Select entity	Date and time	User A	Event	User B
MSISON	21/02/2016 08:21:05	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892 Loc. Poggio del Barbieri, CASTIGLIONE DELLA PESCAIA, GR	00:00:23	+393357695524 &*
Event Type	21/02/2016 08:23:29	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892 Loc. Poggio del Barbieri, CASTIGLIONE DELLA PESCAIA, GR	00:09:57	+393351827497 &*
Date Range	21/02/2016 08:38:08	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892 Loc. Poggio del Barbieri, CASTIGLIONE DELLA PESCAIA, GR	00:00:36	+393351827497 &*
Time Range	21/02/2016 09:12:55	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892 Loc. Poggio del Barbieri, CASTIGLIONE DELLA PESCAIA, GR	00:01:14	+393478075255 &*
Location	21/02/2016 09:15:27	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892 Loc. Poggio del Barbieri, CASTIGLIONE DELLA PESCAIA, GR	00:01:16	+393478075255 &*
Distance of connected calls	21/02/2016 09:17:54	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892 Loc. Poggio del Barbieri, CASTIGLIONE DELLA PESCAIA, GR	00:04:15	+39057437725 &*
Search	21/02/2016 09:23:07	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892 Loc. Poggio del Barbieri, CASTIGLIONE DELLA PESCAIA, GR	00:01:15	+393403746525 &*
Raw search	21/02/2016 09:24:58	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892 Loc. Poggio del Barbieri, CASTIGLIONE DELLA PESCAIA, GR	00:00:49	+393478075255 &*
	21/02/2016 09:26:20	+393485455585 &* Antonio Sarracino SRRTN98C03F839K 35338204784511 222107802952566 222-10-35042-81892	00:02:35	+393336135156 &*

Figure out who is using stolen phones (carrier request)

Filter for the stolen IMEIs to check the «new» simcards that were used in these devices

Create list (TAG) of users/IMEI for blacklisted phone number, IMEI, IMSI, ... and use them as a filter

BTS TRACKER

Survey the cell towers coverage (HARDWARE)

BTS Tracker

Base Transceiver Stations, the cell towers that surround us all, spread their signal everywhere, but not in a straight, fixed line.

Cell coverage twists and shifts, it is reflected and reversed. Like all environments, the digital one is subject to change.

This is BTS Tracker

Hold the device able to survey and absorb how every cell tower connects to a smartphone.

BTS Tracker

Hardware module collects and charts where and how every cell tower spreads its signal. The software organizes and maps your cell site surveys in an easy to understand way. It also looks out for daily signal changes creating a statistical real coverage scenario based on signal strength, power, and location. The reality of BTS networks. **Bring your evidence to light.** Locate a smartphone more accurately: know where the coverage area really is. Make your case map **real.**

BTS Tracker

From a realistic outlook – **not a theoretical one** – locate your suspects and validate your criminal case.

The system that collects and analyzes the signal strength and coverage of cell towers where the scan is performed, **not intercepting communication**, but **defining the mobile environment**.

Go 360°: correlate real BTS cell site coverage analysis with your CDR phone record analytics. Locate a call in the area where its cell tower signal is really being spread – make your case map real.

Join your results with additional digital evidence and validate your criminal case.

This is BTS Tracker and PhoneLog – This is SecurCube – This is your success.

BTS Tracker



Strada per andare a Lugano

1/27/2021



EXPORT TO EXCEL

Code	Tecnology	Power	Cell Mode	Lat	Lon	Speed	C1	C2	Ta	Eci
222-88-24543-52832	UMTS	-46	Idle	45.782433...	11.909435					
222-10-20082-18051	GSM	-59	Serving	45.754978...	11.91191					
222-10-20082-18053	GSM	-61	Neighbor	45.782531...	11.909443...					
222-99-24543-52832	UMTS	-46	Idle	45.782433...	11.909435					
222-10-20082-3963	GSM	-74	Neighbor	45.782525	11.909441...					
222-10-20082-18053	GSM	-61	Neighbor	45.78246	11.909478...					
222-10-25032-31167	UMTS	-55	Idle	45.782433...	11.909435					

Cell tower list

BTS Tracker



2019-12-01 Beirut
12/2/2019

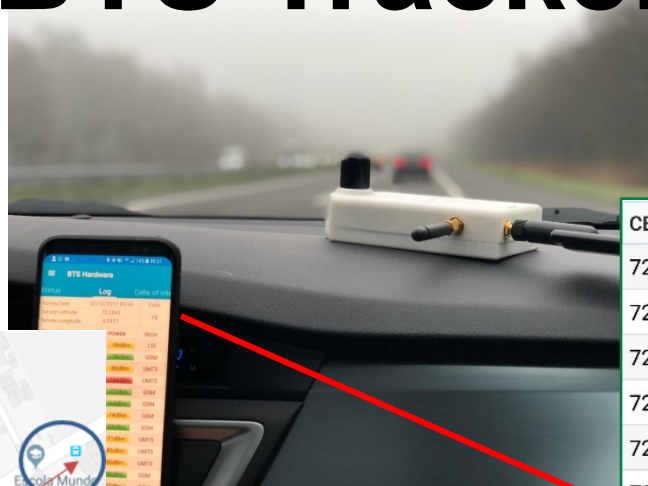


3D map of coverage
for cell towers



BTS Tracker

2



3

CELL CODE	POWER	TECH
724-02-465731-22	-101dBm	LTE
724-02-57171-12398	-82dBm	UMTS
724-02-57171-12402	-77dBm	UMTS
724-05-2771-11117	-73dBm	GSM
724-05-2771-11617	-74dBm	GSM
724-05-30271-62747	-63dBm	UMTS
724-05-30271-62750	-55dBm	UMTS
724-05-710334-4	-73dBm	LTE
724-11-1276-3	-90dBm	LTE

1



CELL SERVICE

Historical Cell tower informations

Cell Service

The only Historical Cell Site Location Information data management and mapping engine

Cell Service

- Information extracted from phone records is the starting point of every professional mobile forensics investigation.
- The who, the when, and the type of communication, the network of people in contact with each other.
- Phone records also list each cell tower too.
- Carriers supply Cell Lists of all the mobile antennas working in their infrastructure.
- And every cell tower is given a specific ID number.
- Just like us, each cell ID number has a profile, location, and history of any change of address.
- This gives you the power to map every event in your phone records.

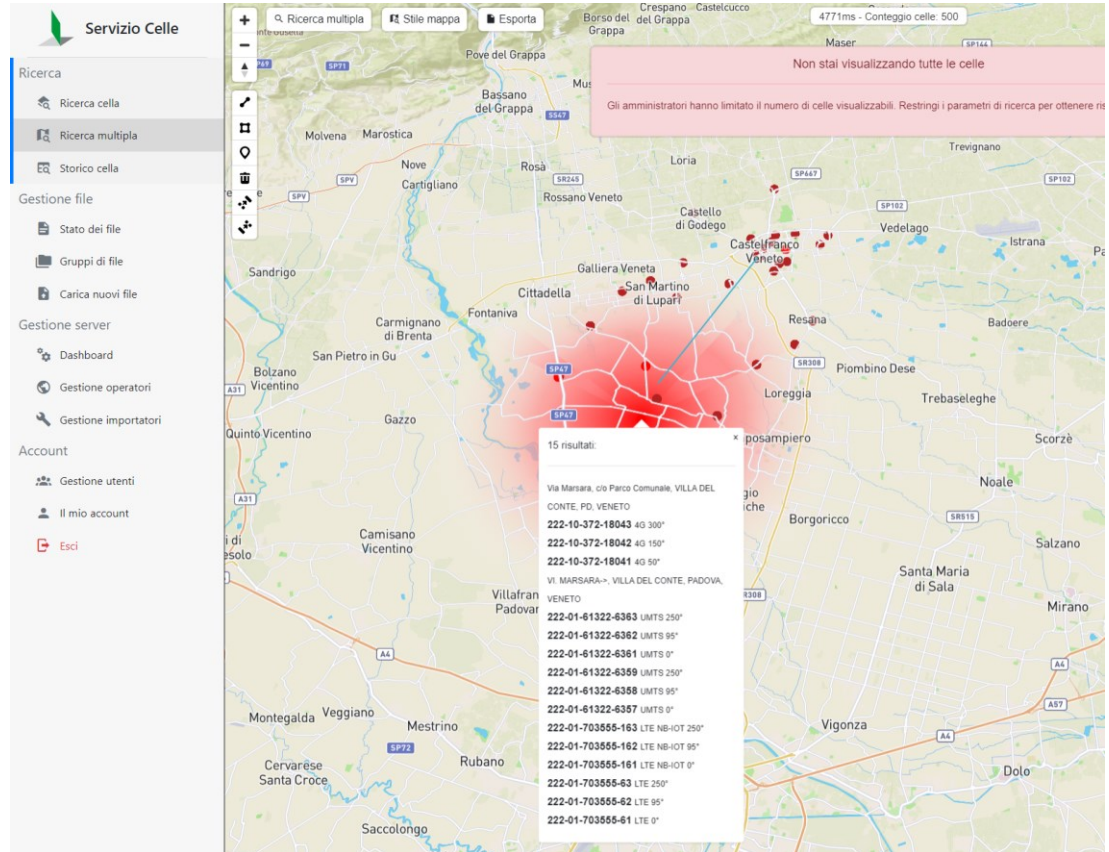
Cell Service

SecurCube Cell Service is the one-stop cell site information management system.

A fast, easy to use and complete interface that allows you to search for and map a case's mobile network infrastructure from carriers' data

Manage and visualize:

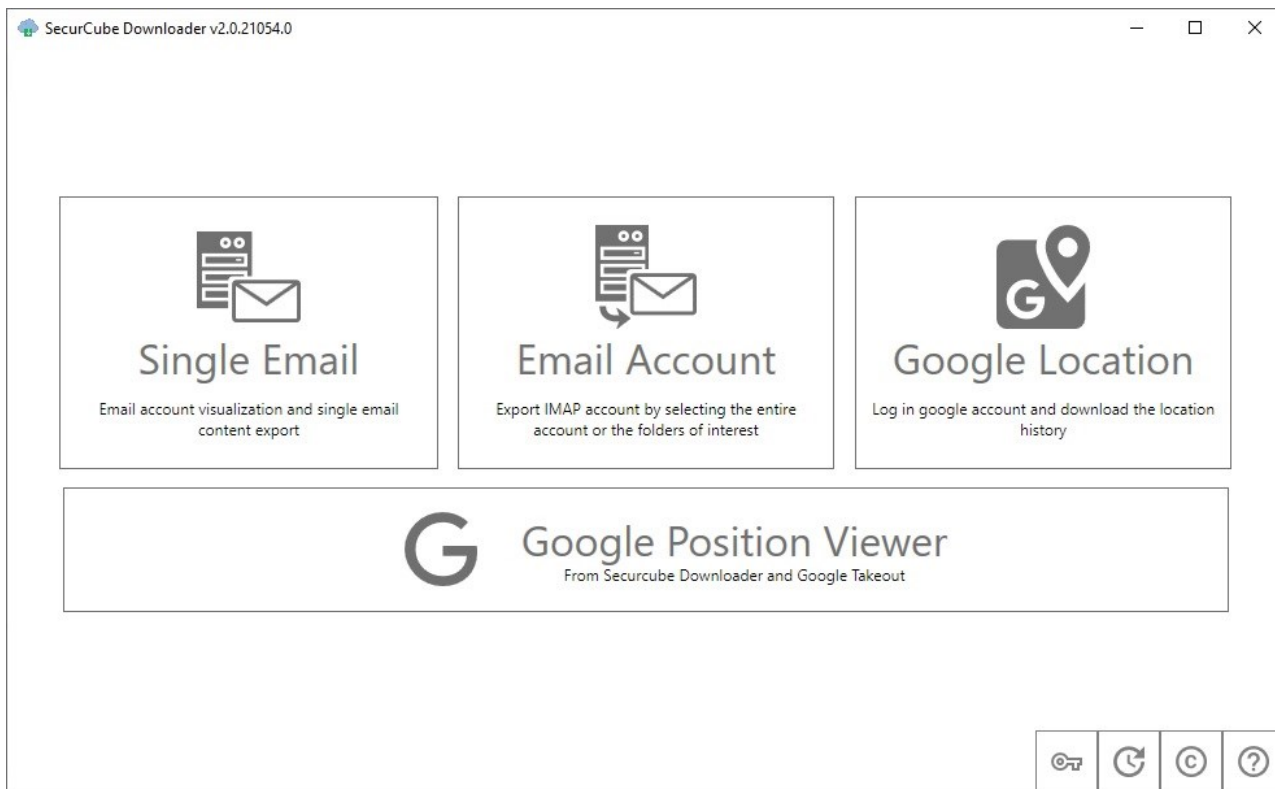
- Installation
- Change of location or ID realignments
- Theoretical cell signal coverage



SECURCUBE DOWNLOADER

Download emails & Google timeline
in a forensically sound way

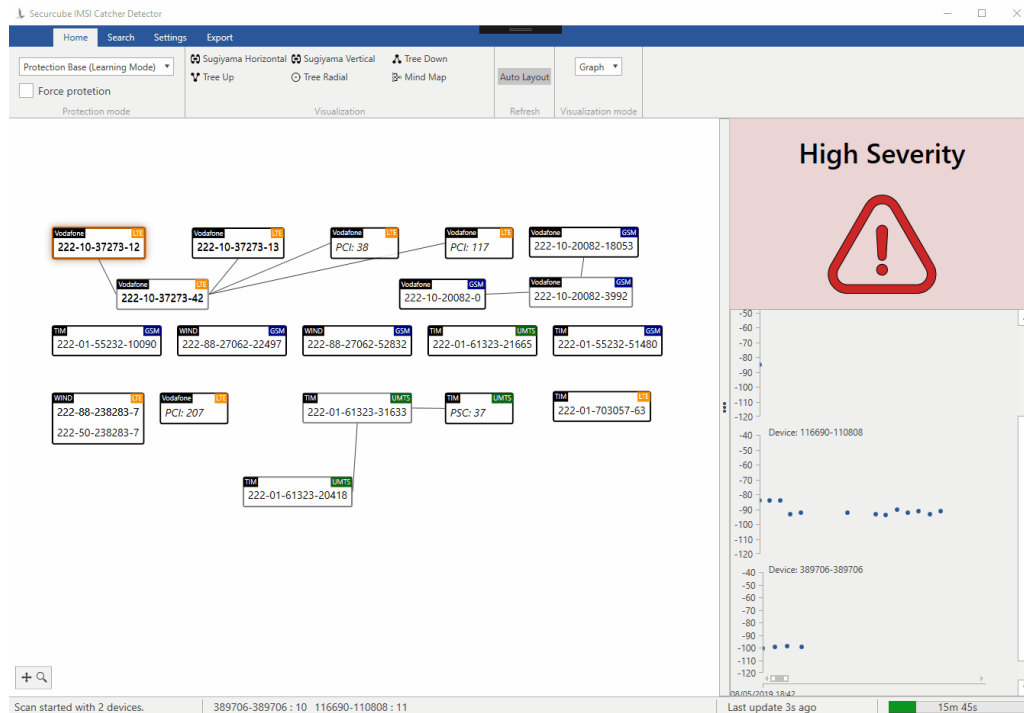
Securcube Downloader



IMSI Catcher Detector

Figure out if an IMSI Catcher is
running in your area

IMSI Catcher Detector



Academic program

Colleges and Universities in
EU/USA

Thank you!

www.securcube.net