SIREN

Investigating Mobile Device data with the Siren Platform: the unique advantage of automatic data fusion

By Giovanni Tummarello, Nicola Bertolin, Alfredo Milani Comparetti, Phil Glod

Investigating Mobile Device data with the Siren Platform: the unique advantage of automatic data fusion

The ability to lawfully analyze data coming from mobile phones, either physically or virtually captured, is key for Law Enforcement agencies worldwide.

After the data has been physically captured via specialized software and hardware - from providers like Cellebrite, Oxygen or MSAB - the quest for timely extraction of investigative value begins.

Popular eDiscovery tools like Nuix and vendor specific tools, typically succeed in giving you visibility on the content of the specific phone, or of a group of devices captured in a similar fashion.

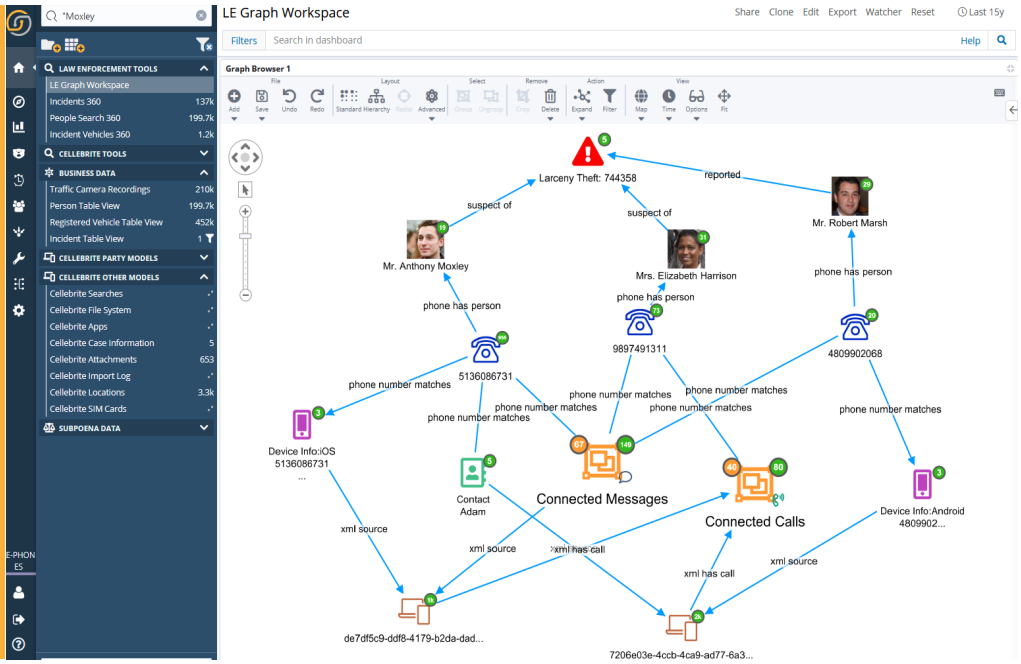
But there is a much bigger value to be unlocked: the **automatic connection of any extracted data identifier (e.g. phone number, email, contact person) with the whole of your agency background information**.

The Siren platform is unique for this, featuring the world's most scalable Investigative Search Engine technology to instantly connect mobile device data to CAD / RMS / Background records, Open Source Intelligence and data coming from any other discovery tool.

Enhance the value of mobile via automatic connectivity with your existing and third party data

Siren can take data files from these "physical extractors" or eDiscovery platforms (specifically UDFR reports and Concordance files) and load them in a way that not only allows search and discovery but also **immediately connects data points to any of the identifiers** (Phone numbers, e-mail addresses, media similarities) present in any of the connected data sources.

In the following screenshots, a mobile phone captured data is immediately connected to existing RMS records via shared identifiers.

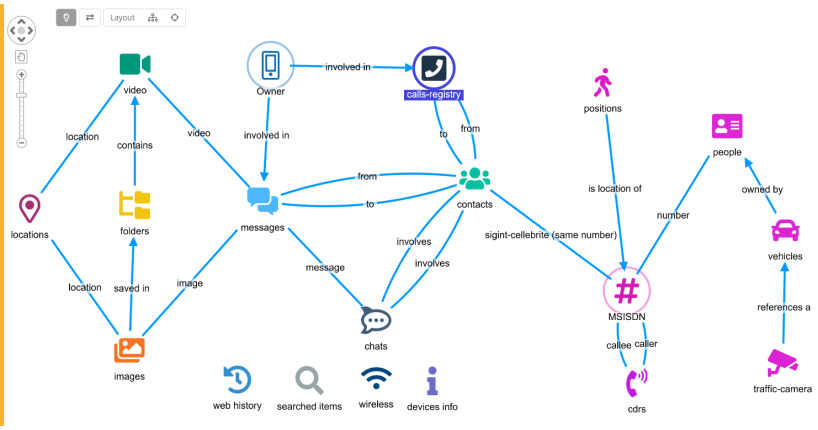


Mobile phone content automatically connects to existing RMS entries via shared identifiers

Siren capabilities are *entity-centric*

In Siren, the analysis is driven by *entity extraction*, which not only fits existing records into a data model but also extracts connections, locations, and topics associated from unstructured data.

Cleaned and consolidated entities form centers of aggregations that include phone numbers, social media handles, email addresses and usernames that are used in the linking process. The picture below demonstrates a typical data model used in Siren Law Enforcement deployments (this can be customized easily for any individual organization).



Thanks to this data model, in addition to standard "search" and "unified views", Siren can answer advanced questions such as:

» *What are the direct connections between a named entity and any record in Siren?*
» *Can the investigator associate a location stored on a phone to a named entity?*

But, most interesting of all:

» *What are the possible connections between apparently disconnected entities - via any of the information available to Siren?*

Let's see this in action in a real world scenario.

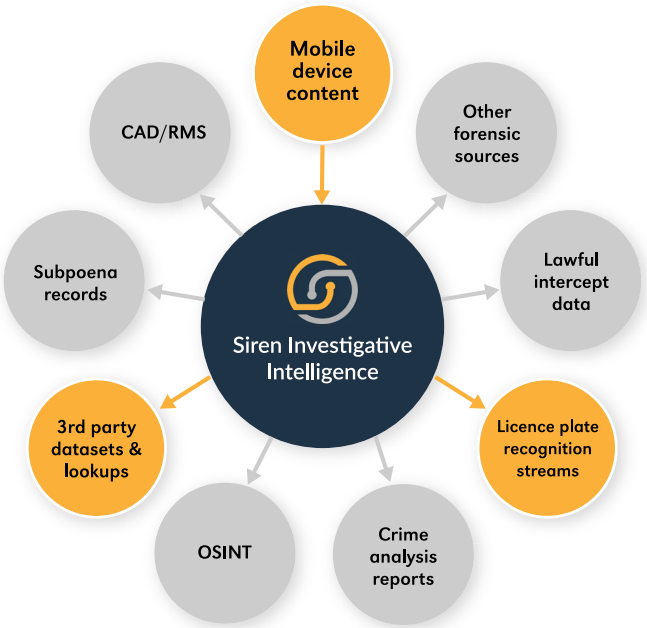
Connecting captured mobile data with car registrations and Licence Plate Recognition: a case study

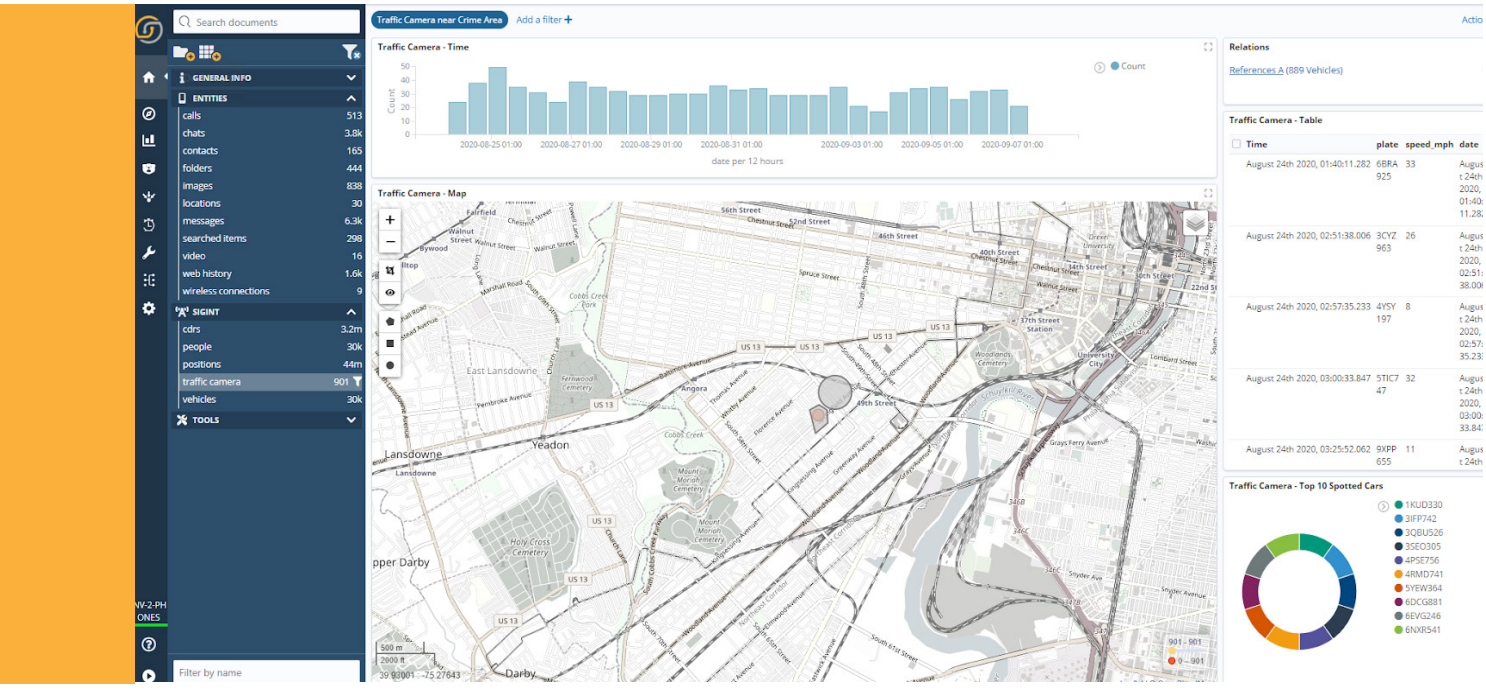
Data sources: *Mobile device data*, Licence Plate recognition streams or set of car registration records.

A mobile device was captured as part of an operation where suspects are believed to be involved with events that happened at a certain city location.

The investigator needs to know: *is there a connection between this device and cars seen near the incident?*

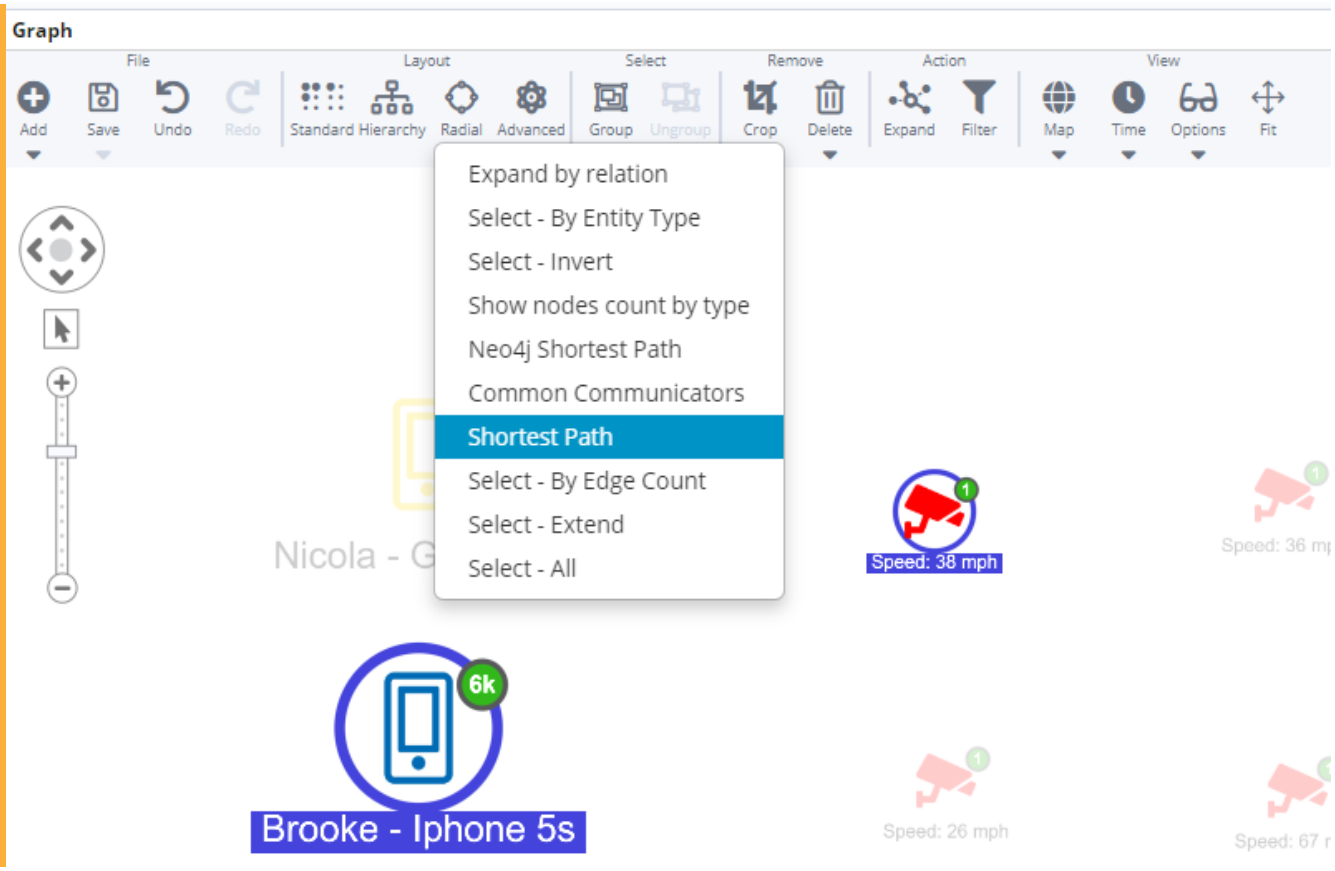
The local Police department has access to Licence Plate Recognition which is streaming. Within Siren one can simply open the dashboards related to LPR, select the area and time range to drill down to a set of car license plates which one wants to investigate for connections.



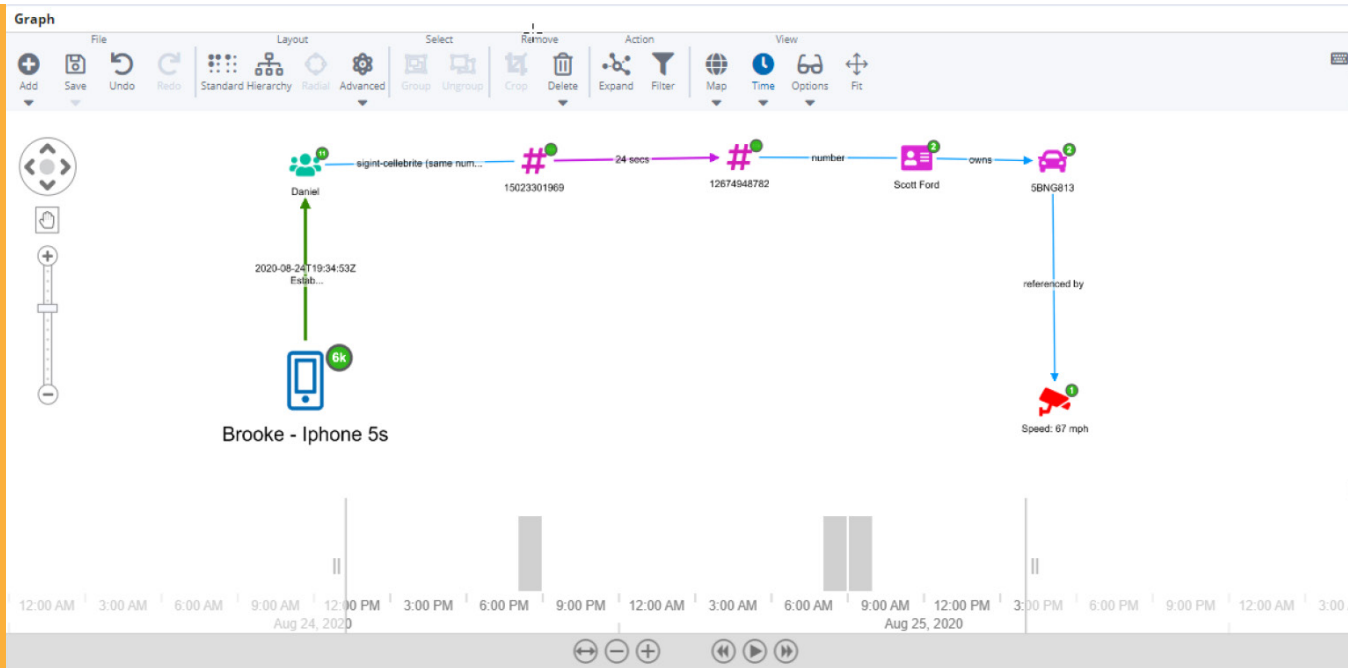


LPR records analytics and drill-downs

The next task is to find the connection - via any data path - to any of the identifiers extracted from the phone. This can also be done by dragging the camera readings in the graph and selecting the **Shortest Path** algorithm.



Doing so activates the Siren's big data "shortest path search" to find any path that might connect the 2 entities. This path is found in a few seconds and is ready to be analyzed on the graph also using Siren unique timebar mode.



Analyzing the shortest path between the mobile phone and relevant LPR records

The investigator can then see that, in our example, the owner of the confiscated device (Brooke) made a call to Daniel - a name coming from Brooke's contacts - the evening before the attack. A 24 seconds call highlighted in the timeline (screenshot below).

Analyzing the shortest path between the mobile phone and relevant LPR records

The callee's number then appears registered to an individual (Scott Ford), who, thanks to Vehicle Registration Data, is immediately connected to a licence plate spotted by the traffic camera around 9.45am, just 15 minutes before the attack.

Conclusion

To protect people, assets and networks, Siren investigative search engine technology delivers instant connections between mobile device extracted data and any bit of data which is made available to the Siren platform. Specifically, Siren now includes connectors to import mobile device data extracted by leading vendor platforms.

Investigators can now avail of the ability to merge, with very little effort, capabilities and datasets that were never easily connected - like the entire content of a mobile device and all the available background data within an organization.

Interested in learning more?

Qualifying organizations can reach out and request a demo and a trial by emailing **info@siren.io**.

e: info@siren.io
w: www.siren.io