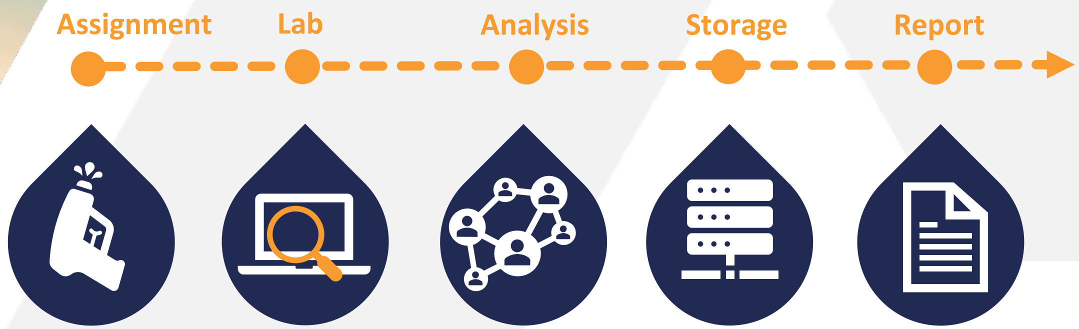
DataExpert

Your partner in the fight against (cyber)crime



From data carriers to intelligence, how do experts at the Dutch Ministry of Defence do it?

Before a large-scale conflict such as a terrorist attack takes place, a large number of criminal activities are already underway: People are recruited by groups using propaganda, weapons and explosives are traded, money is laundered and other subversive activities take place. Therefore, in order to anticipate a possible conflict, it is very important to investigate and link these small activities (preventively). This requires collaboration between various expert teams within the Ministry of Defence and Police. Each with its own way of working. In this whitepaper, we delve into the working methods of a specialised unit within the Dutch Ministry of Defence that deals with collecting data from data carriers and correlating and analysing it, for the purpose of converting this information into actionable intelligence.

Ready, set, go!

The starting signal for the experts sounds as soon as they receive a targeted assignment. This might include, for example, going to location x and collecting the relevant data carriers there and finding out the key players in an illegal arms deal. The moment this assignment comes in, it is the task of the so-called FET (Field Exploitations Team) to jump in the car or plane and go to the relevant location as quickly as possible and retrieve, register and secure all data carriers.

Data carriers can include drones, cell phones, computers or, for example, cars. The data carriers must be collected in such a way that any biological traces, such as fingerprints and DNA, can be secured in the lab at a later time. In addition, it must be ensured that the digital evidence present on the data carriers cannot be remotely erased. To prevent this, a data carrier can be put on airplane mode or placed in a so-called Faraday bag. A Faraday bag makes it impossible to connect to the device placed in the bag.

Depending on the investigation query, a decision must be made as to which evidence will be secured first. Indeed, collecting biological traces present on the device and securing digital traces do not always go well together. Therefore, it is important to determine whether the traces on or in the phone or computer are a priority.

On to the lab

Once the data carriers are collected, the FET takes the evidence to the lab. Here, other colleagues secure the biological traces and make copies of the data carriers. Which forensic software and hardware is used to collect the data usually depends on the type of data carriers found on site. Is it a mobile or a desktop, a Samsung or an Apple, and is it a brand new model or has it been around for years? It often involves mobile phones. Digital forensic software used in the lab to read these are XRY from MSAB and UFED Physical Analyzer from Cellebrite. All solutions are suitable for restoring and decrypting data stored on the device itself, in applications and the cloud. The tools also have functionalities to retrieve deleted data, to a certain extent.

After copying the data found, the lab specialists do an initial search to see if there is any relevant data surrounding, in this case, the illegal arms deal mentioned earlier. To do this, they use other digital forensics solutions that have filtering, searching and reporting functionalities. Without filtering by relevant keywords, photos, e-mails, documents, notable internet search queries or, for example, cryptocurrency transactions, it is searching for a needle in a haystack. In fact, often more than 95% of the data is irrelevant. Lab staff use UFED Reader and XAMN, among others, for this purpose. Both tools are capable of viewing, searching, filtering and highlighting the data present in one data carrier. The data the lab finds is often in Dutch or English, but sometimes they have to deal with other foreign languages such as Arabic. A translation tool is used for these languages. Cellebrite, among others, provides modules for this.

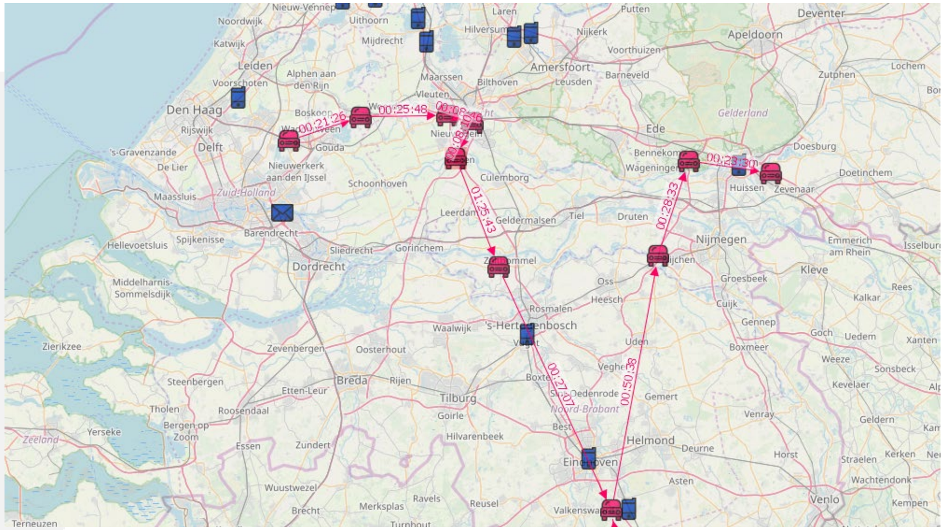
Once the relevant data per data carrier is mapped and translated, the information is passed to the Technical Analysis Cell (TAC).

Often more than 95% of the data is irrelevant

From data to intelligence

Whereas individual insights per data carrier can already be interesting, superimposing the data coming from the different data carriers provides new insights. The forensic solutions mentioned above do not allow for this. The analysts of the Technical Analysis Cell therefore first export the data present on the data carriers to a uniform format, such as XML. Once in a uniform format, the data can be imported into another analysis tool for further analysis. Because this investigation team mostly deals with telecom data, they deploy Ockham Solutions' Mercure software for this purpose.

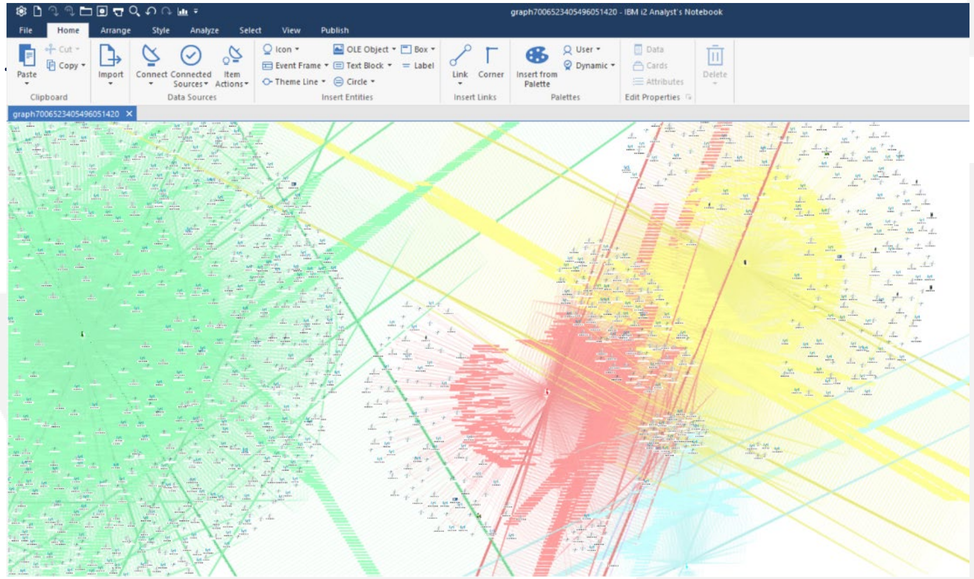
Mercure is a software tool that is well suited for analysing and correlating telecom data. It allows for loading in ‘histos’ (call data of user), mast data (which specifies the phone numbers that have been connected to a certain mast) and extraction data from cell phones. In addition, the software also offers a possibility to load GPS data from, for example, car beacons or ankle bracelets. These days, it is also possible to load in ANPR (Automatic Number Plate Recognition), which tracks cars through cameras on the road.



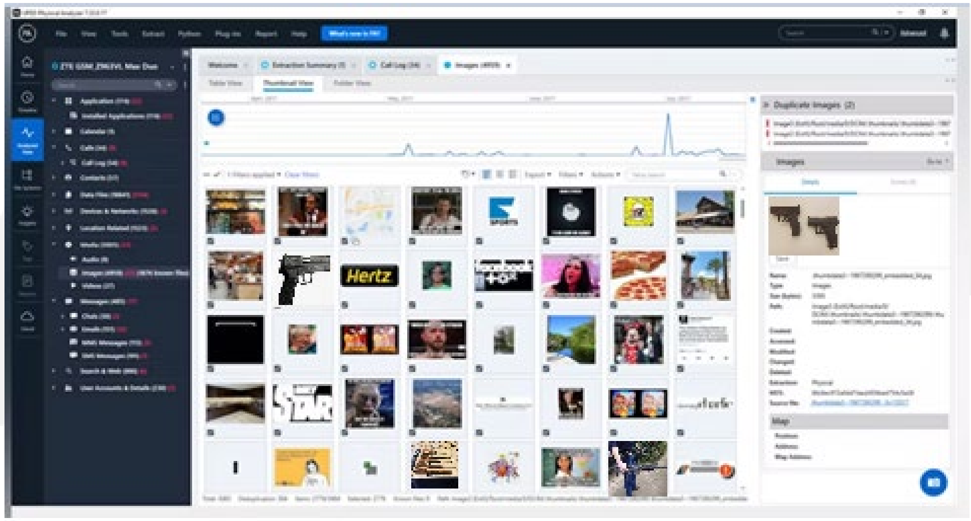
So with Mercure, the team can compare and correlate many different types of data. Large amounts of data can be loaded into Mercure. These can be queried using pre-programmed queries based on the current issue.

If necessary, the filtered and analysed data can be further analysed using i2 Analyst's Notebook (ANB).

Mercure connects seamlessly to this tool, making it easy to load data from Mercure into ANB. ANB offers different analysis functions than Mercure, and the TAC team primarily uses this tool for Social Network Analysis. This analysis function can be used to, for example, extract interesting persons or groups from the data that is overlooked in ordinary analyses. This can be used to identify two or more separate groups that interact with each other. For example, an arms deal may take place between a party that purchases the weapons and another party that intends to carry out the attack. This may indicate the previously mentioned large-scale conflict such as a terrorist attack



Incidentally, there continues to be interaction between the previously mentioned tools (UFED Reader, XAMN, etc.) and the analysis tools. For example, with Mercure, it is possible to aggregate the metadata of photos and videos with other data. However, this tool does not focus on content analysis of photos and videos. If the metadata of a photo/video turns out to be relevant in the analysis, then the photo/video can be displayed in UFED or analysed for content with another specialised tool.



Data storage and exchange

After uncovering relevant events and identities with Mercure and Analyst's Notebook, the team within this defence organisation stores the data in a database. The i2 iBase software is used for this purpose. Other teams within the Ministry of Defence use this as well. This makes the exchange of information and collaboration between different specialties easier, faster and more efficient.

However, there is mutual agreement amongst the teams on how to enter data. This prevents an entity or attribute from being noted/recorded in two different ways. For example, consider the different notation of phone numbers +31 or 0031.

DataExpert

Your partner in the fight against (cyber)crime

Reports & action

After data storage and possible exchange, a report is compiled. Photos are added to it and findings are described. The Technical Analysis Cell usually uses programs like Word or Excel for making reports, but it can also be the case that the results are presented to the client by means of a presentation.

Several actions can be taken as a result of the report. Which? This, of course, depends on the intelligence obtained. Covertly following, summoning for questioning or proceeding to arrest the suspect are all among the possibilities.

DataExpert at your service

Technology, as shown in this case, serves as a great tool to support the collection, searching and understanding of (big) data. Which technology is appropriate depends on the objective, the type of investigation, the organisation, and many other factors. The Digital Forensics and Analysis Experts at DataExpert are happy to help you determine which software and hardware solutions support and reinforce your work processes.

Contact us

Would you like to meet with our consultants and advisors or do you have other questions? Then please contact us:

- ✓ Vendelier 65, 3905 PD Veenendaal
- ✓ +31 (0)318 543173
- ✓ info@dataexpert.nl
- ✓ www.dataexpert.nl/en