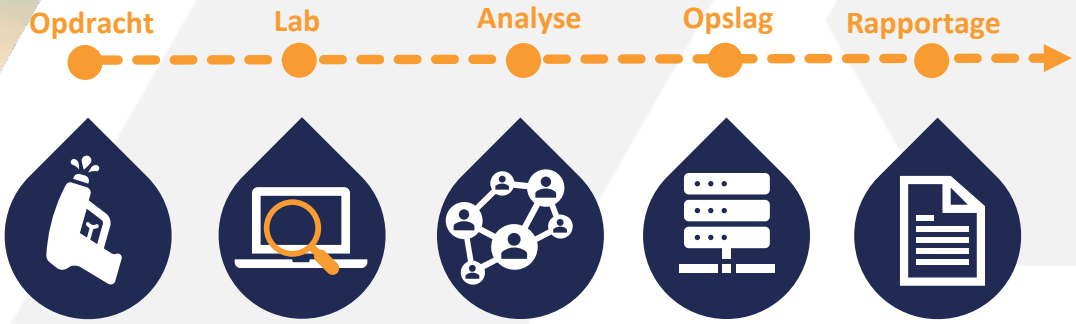
DataExpert

Your partner in the fight against (cyber)crime



Van gegevensdragers tot intelligence, hoe doen de experts bij Defensie dat?

In aanloop naar een grootschalig conflict, zoals een terreuraanslag, zijn een groot aantal criminele activiteiten al in gang gezet: Er worden mensen geworven door groeperingen met behulp van propaganda, er wordt in wapens en explosieven gehandeld, er wordt geld witgewassen en er vinden andere ondermijnende activiteiten plaats. Om te anticiperen op een mogelijk conflict, is het daarom van groot belang deze kleine activiteiten (preventief) te onderzoeken en aan elkaar te koppelen. Dit vraagt de samenwerking van verschillende specialistische teams binnen Defensie en Politie. Elk met zijn eigen werkwijze. In deze whitepaper nemen we een kijkje in de werkwijze van een gespecialiseerd onderdeel binnen Defensie dat zich bezighoudt met het verzamelen van data van gegevensdragers en het correleren en analyseren daarvan, met als doel deze informatie om te zetten naar actionable intelligence.

Klaar voor de start, af!

Het startschot voor de experts klinkt zodra ze een gerichte opdracht binnen krijgen. Dit kan bijvoorbeeld zijn: ga naar locatie x en verzamel daar de relevante gegevensdragers en achterhaal de hoofdrolspelers in een illegale wapendeal. Op het moment dat deze opdracht binnenkomt is het de taak van het zogenoemde FET (Field Exploitations Team) om in de auto of het vliegtuig te springen en zo snel mogelijk naar de desbetreffende locatie toe te gaan en alle gegevensdragers op te halen, te registreren en veilig te stellen.

Gegevensdragers kunnen onder meer drones, mobiele telefoons, computers of bijvoorbeeld auto's zijn. De gegevensdragers moeten op een dusdanige manier verzameld worden dat eventuele biologische sporen, zoals vingerafdrukken en DNA, op een later moment veiliggesteld kunnen worden in het lab. Daarnaast moet ervoor gezorgd worden dat het digitale bewijs dat aanwezig is op de gegevensdragers niet op afstand gewist kan worden. Om dit te voorkomen kan een gegevensdrager op vliegtuigmodus gezet worden of geplaatst worden in een zogenoemde Faraday bag. Een Faraday bag maakt het onmogelijk om verbinding te maken met het in de zak geplaatste toestel.

Afhankelijk van de onderzoeksvraag moet er besloten worden welk bewijsmateriaal als eerste veiliggesteld wordt. Het verzamelen van biologische sporen die aanwezig zijn op het toestel en het veiligstellen van digitale sporen gaat namelijk niet altijd even goed samen. Daarom is het van belang dat er bepaald wordt of de sporen op of in de telefoon of computer prioriteit hebben.

Op naar het lab

Eenmaal de gegevensdragers verzameld, brengt het FET het bewijsmateriaal naar het lab. Hier worden door andere collega's de biologische sporen

veiliggesteld en kopieën gemaakt van de gegevensdragers. Welke forensische soft- en hardware gebruikt wordt voor het verzamelen van de data, is veelal afhankelijk van het type gegevensdragers die aangetroffen zijn op locatie. Is het een mobiel of een desktop, een Samsung of een Apple, en is het een gloednieuw model of bestaat deze al jaren? Veelal betreffen het mobiele telefoons. Digitaal forensische software die in het lab wordt ingezet om deze uit te lezen zijn XRY van MSAB en UFED Physical Analyzer van Cellebrite. Alle oplossingen zijn geschikt voor het herstellen en decoderen van data opgeslagen op het apparaat zelf, in applicaties en de cloud. Ook beschikken de tools over functionaliteiten om, tot op zekere hoogte, gewiste gegevens terug te vinden.

Na het kopiëren van de aangetroffen gegevens maken de labspecialisten een eerste zoekslag om te kijken of er relevante data aanwezig is rondom, in dit geval, de eerder geschetste illegale wapendeal. Hiervoor gebruiken ze andere digitaal forensische oplossingen die beschikken over filter-, zoek- en rapportagefunctionaliteiten. Zonder te filteren op relevante zoekwoorden, foto's, e-mails, documenten, opvallende internetzoekslagen of bijvoorbeeld cryptocurrency transacties is het zoeken naar een speld in een hooiberg. Vaak is namelijk meer dan 95% van de data niet relevant. De medewerkers van het lab gebruiken hiervoor onder meer UFED Reader en XAMN. Beide tools zijn in staat om de data aanwezig in één gegevensdrager te bekijken, te doorzoeken, te filteren en te markeren. Vaak is de data die het lab aantreft in het Nederlands of Engels maar soms krijgen ze ook te maken met andere buitenlandse talen zoals Arabisch. Voor deze talen wordt een vertalingstool ingezet. Onder meer Cellebrite levert hier modules voor.

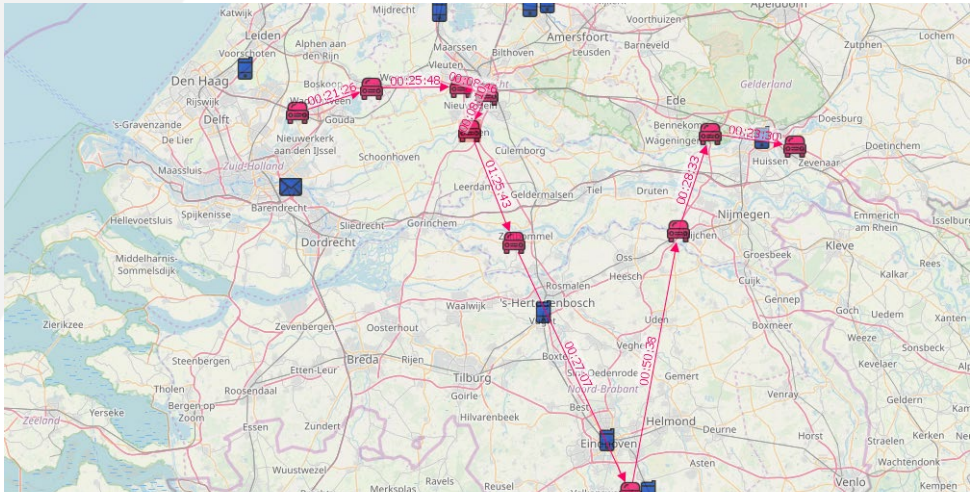
Eenmaal de relevante data per gegevensdrager in kaart gebracht en vertaald, wordt de informatie doorgezet naar de Technische Analyse Cel (TAC).

Vaak is namelijk meer dan 95% van de data niet relevant

Van data naar intelligence

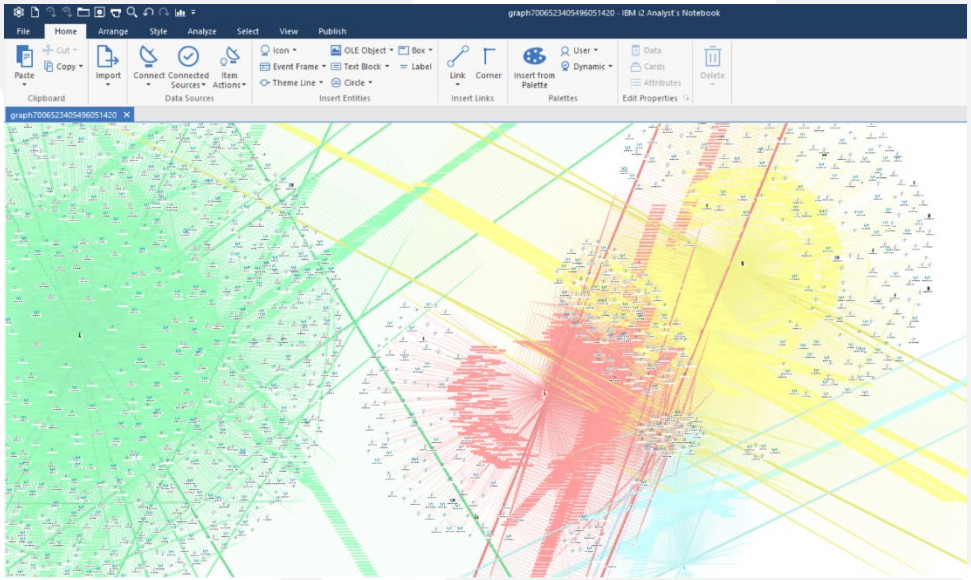
Waar losse inzichten per gegevensdrager al interessant kunnen zijn, levert het over elkaar heen leggen van de data afkomstig van de verschillende gegevensdragers nieuwe inzichten op. De hierboven genoemde forensische oplossingen bieden hier niet de mogelijkheid toe. De analisten van de Technische Analyse Cel exporteren daarom de data aanwezig op de gegevensdragers eerst naar een uniform formaat, zoals XML. Eenmaal in een uniform formaat kan de data in een andere analyse tool geïmporteerd worden voor verdere analyse. Omdat dit onderzoeksteam veelal te maken krijgt met telecomdata zetten ze hiervoor de software Mercure van Ockham Solutions in.

Mercure is een software tool dat zeer geschikt is voor het analyseren en correleren van telecomdata. Het is mogelijk hier histo's (belgegevens van gebruiker), mastgegevens (waarin de telefoonnummers genoteerd staan die aan een bepaalde mast verbonden zijn geweest) en extractiegegevens van mobiele telefoons in te laden. Daarnaast biedt de software ook een mogelijkheid om GPS gegevens uit bijvoorbeeld autobakens of enkelbanden te laden. Ook is het tegenwoordig mogelijk om ANPR (Automatic Number Plate Recognision) in te laden waarmee auto's gevolgd worden via camera's op de (snel)weg.

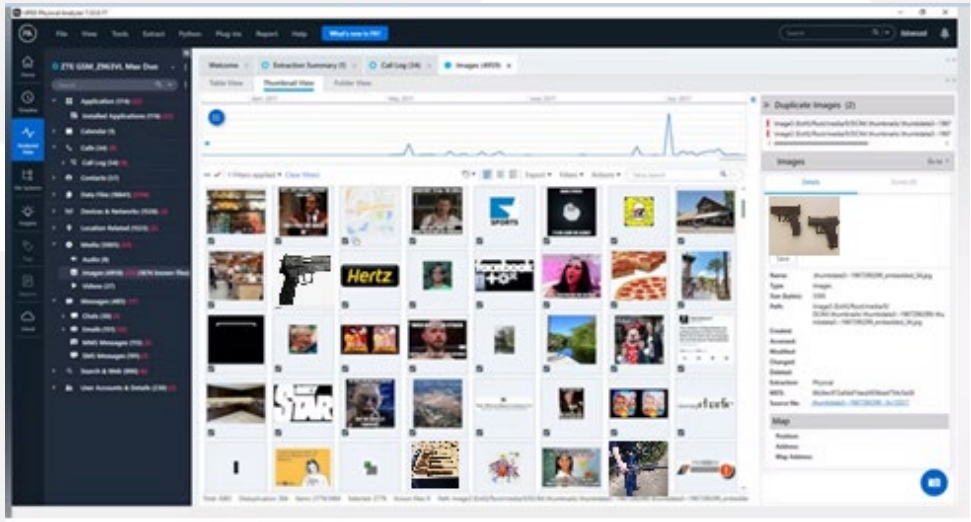


Met Mercure kan het team dus veel verschillende typen gegevens met elkaar vergelijken en correleren. Grote hoeveelheden data kunnen in Mercure geladen worden. Deze kunnen d.m.v. vooraf geprogrammeerde query's worden bevraagd op basis van het op dat moment actuele vraagstuk.

De gefilterde en geanalyseerde gegevens kunnen indien nodig verder geanalyseerd worden m.b.v. i2 Analyst's Notebook (ANB). Mercure sluit naadloos aan op deze tool waardoor het eenvoudig is om data uit Mercure in ANB te laden. In ANB zijn andere analyse functies aanwezig dan in Mercure en het TAC team gebruikt deze tool voornamelijk voor Sociale Netwerk Analyse. Door middel van deze analysefunctie kunnen er bijvoorbeeld interessante personen of groeperingen uit de data gehaald worden die bij gewone analyses over het hoofd gezien worden. Hiermee kunnen twee of meer losstaande groeperingen geïdentificeerd worden die met elkaar in contact staan. Een wapendeal kan bijvoorbeeld plaatsvinden tussen een partij die de wapens inkoopt en een andere partij die de aanslag wil uitvoeren. Dit kan duiden op het eerder genoemd grootschalig conflict zoals een terroristische aanslag.



Er blijft overigens wel interactie tussen de eerder genoemde tools (UFED Reader, XAMN etc.) en de analyse tools plaatsvinden. Met Mercure is het bijvoorbeeld mogelijk om de metadata van foto's en video's met andere gegevens te aggregeren, echter focust deze tool niet op het inhoudelijk analyseren van foto's en video's. Blijkt de metadata van een foto/ video relevant te zijn in de analyse, dan kan in UFED de afbeelding/ video worden getoond of met een andere gespecialiseerde tool inhoudelijk geanalyseerd worden.



Data opslag en uitwisseling

Na relevante gebeurtenissen en identiteiten in beeld te hebben gebracht met Mercure en Analyst's Notebook, slaat het team binnen deze defensieorganisatie de data op in een database. Hiervoor wordt de software i2 iBase gebruikt. Ook andere teams binnen Defensie maken hier gebruik van. Hierdoor is het uitwisselen van informatie en samenwerking tussen verschillende specialismes eenvoudiger, efficiënter en sneller.

DataExpert

Your partner in the fight against (cyber)crime

Onderling is er bij de teams wel een afspraak over de manier van gegevensinvoer. Zo wordt voorkomen dat een entiteit of attribuut op twee verschillende manieren wordt genoteerd. Denk bijvoorbeeld aan de verschillende notering van telefoonnummers +31, 0031 of 06.

Rapportages & actie

Na de data opslag en eventuele uitwisseling wordt er een rapportage samengesteld. Hier worden foto's aan toegevoegd en bevindingen in omschreven. Voor het maken van rapportages maakt de Technische Analyse Cel veelal gebruik van bijvoorbeeld Word of Excel, maar het kan ook voorkomen dat het resultaat wordt gepresenteerd d.m.v. een presentatie aan de opdrachtgever.

Naar aanleiding van het rapport kunnen er verschillende acties worden ondernomen. Welke? Dat ligt natuurlijk aan de verkregen intelligence. Het heimelijk volgen, oproepen voor verhoor of overgaan tot arrestatie van de verdachte behoren allen tot de mogelijkheden.

DataExpert denkt met u mee

Technologie kan zoals in deze case naar voren komt zeer goed ondersteunen bij het verzamelen, doorzoeken en inzicht krijgen in (big) data. Welke technologie geschikt is, is afhankelijk van de doelstelling, het type onderzoek, de organisatie en nog vele andere factoren. De Digital Forensics en Analyse Experts bij DataExpert denken graag met u mee welke soft- en hardware oplossingen uw werkprocessen ondersteunen en versterken.

Neem contact met ons op

Wilt u graag met onze consultants en adviseurs om tafel of heeft u andere vragen? Neem dan contact met ons op:

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