Bits en bites toegankelijk voor tactiek

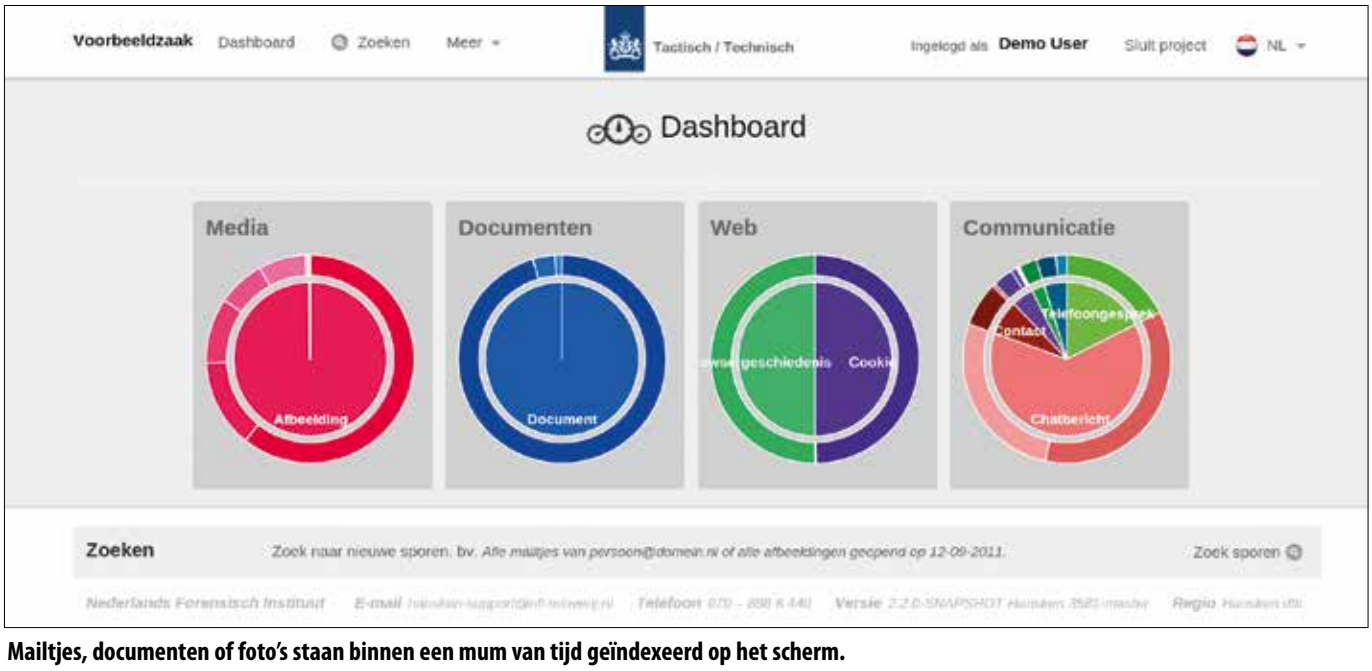
De tactische recherche kan sinds kort snel en efficiënt aan de slag met grote hoeveelheden in beslag genomen digitale data. Zoekmachine Hansken, de opvolger van Xiraf, indexeert al het materiaal.

Dankzij de inzet van zoekmachine Hansken, gelanceerd in oktober 2015, kan de tactische recherche snel en efficiënt zoeken in de inhoud van grote hoeveelheden in beslag genomen gegevensdragers. Mailtjes van een bepaalde afzender of foto's van een bepaalde datum staan binnen een mum van tijd geïndexeerd op het scherm. Een groot voordeel van Hansken is dat de tactisch rechercheur zelf makkelijk uitgebreid kan zoeken in de data. Over het algemeen deed de digitaal rechercheur dat, maar omdat die nauwelijks of geen zaakkennis had, bleef het meestal bij heel brede zoekvragen. Harm van Beek, forensisch onderzoeker digitale technologie bij het Nederlands Forensisch Instituut, dat Hansken ontwikkelde: "Tactiek had niet de juiste middelen om computers en dergelijke te onderzoeken, dus vroegen ze een digitaal rechercheur om bijvoorbeeld alle mailtjes of alle foto's te verzamelen. Maar dat is niet handig en kost ook heel veel tijd van beiden." In Hansken kan de tactisch rechercheur zoeken naar alles wat hij relevant acht. Op woorden, namen, of op eigenschappen van sporen, bijvoorbeeld alleen mails, chatberichten, of foto's al dan niet geschoten met een bepaalde camera. Maar ook in tijdsperiodes, en eventueel combinaties van dat alles. Dus: alle afbeeldingen uit januari 2015. Van Beek: "Zo kun je de zoekresultaten blijven filteren, totdat je van die miljoenen sporen alleen over hebt wat je één voor één kunt bekijken."

Knoppen

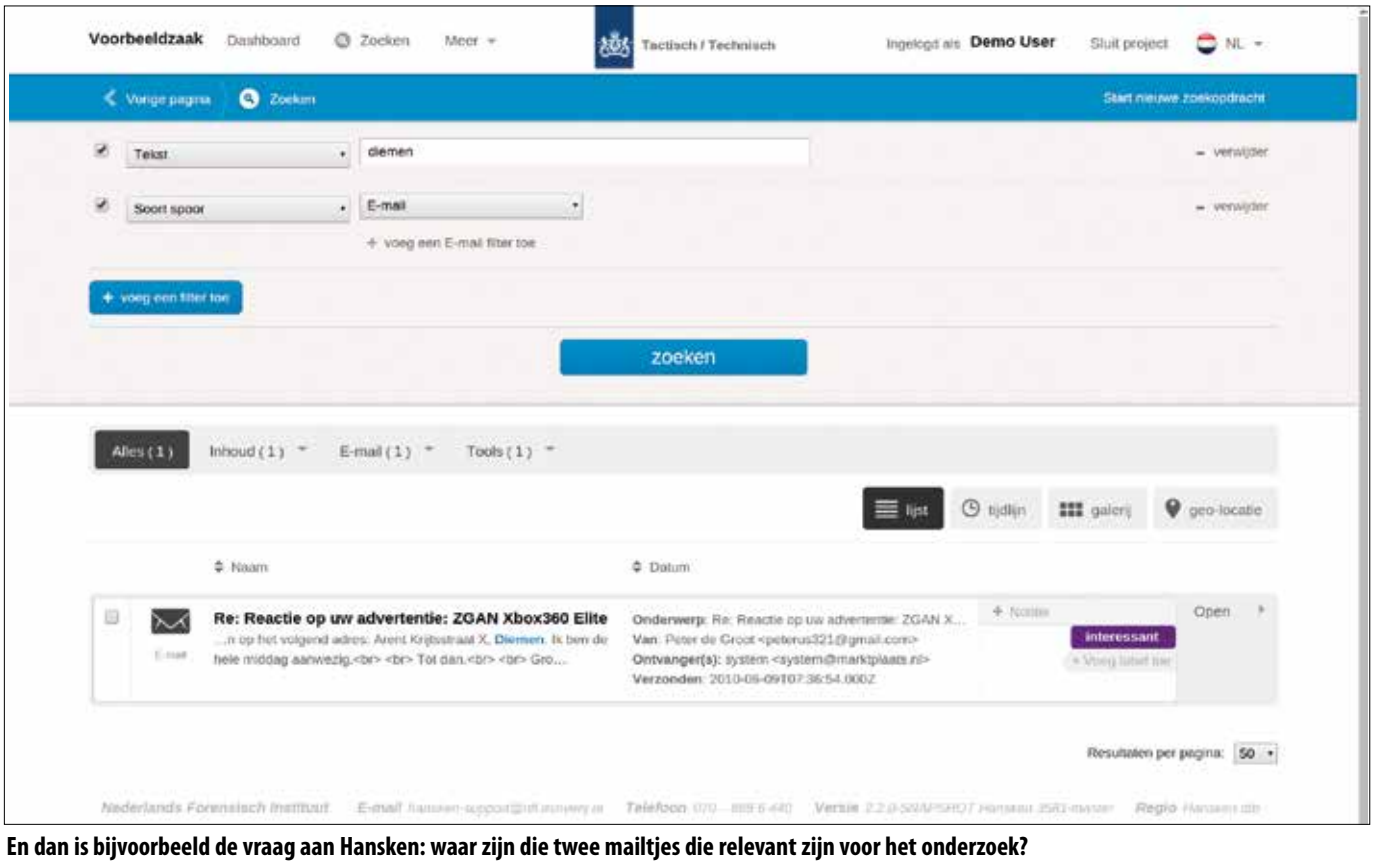
"Ik vind het een groot voordeel dat je als tactisch rechercheur zelf in de digitale data kunt zoeken", zegt Mayke Mollen, generalist tactische recherche bij Eenheid Oost-Brabant. "Je bent vaak beter dan de digitaal rechercheur op de hoogte van subjecten binnen een onderzoek, en van dingen die je moet bewijzen of juist weerleggen. Daardoor kun je zoekslagen beter formuleren én op de resultaten door rechercheren."

Het doel om de tactisch rechercheur zelfstandig achter de knoppen te zetten, is daarmee bereikt, maar hij of zij heeft nog wel ondersteuning nodig van een digitaal rechercheur om gevon-



Mailtjes, documenten of foto's staan binnen een mum van tijd geïndexeerd op het scherm.

Tekst: Joan Kurpershoek · **Foto's**: NFI



En dan is bijvoorbeeld de vraag aan Hansken: waar zijn die twee mailtjes die relevant zijn voor het onderzoek?

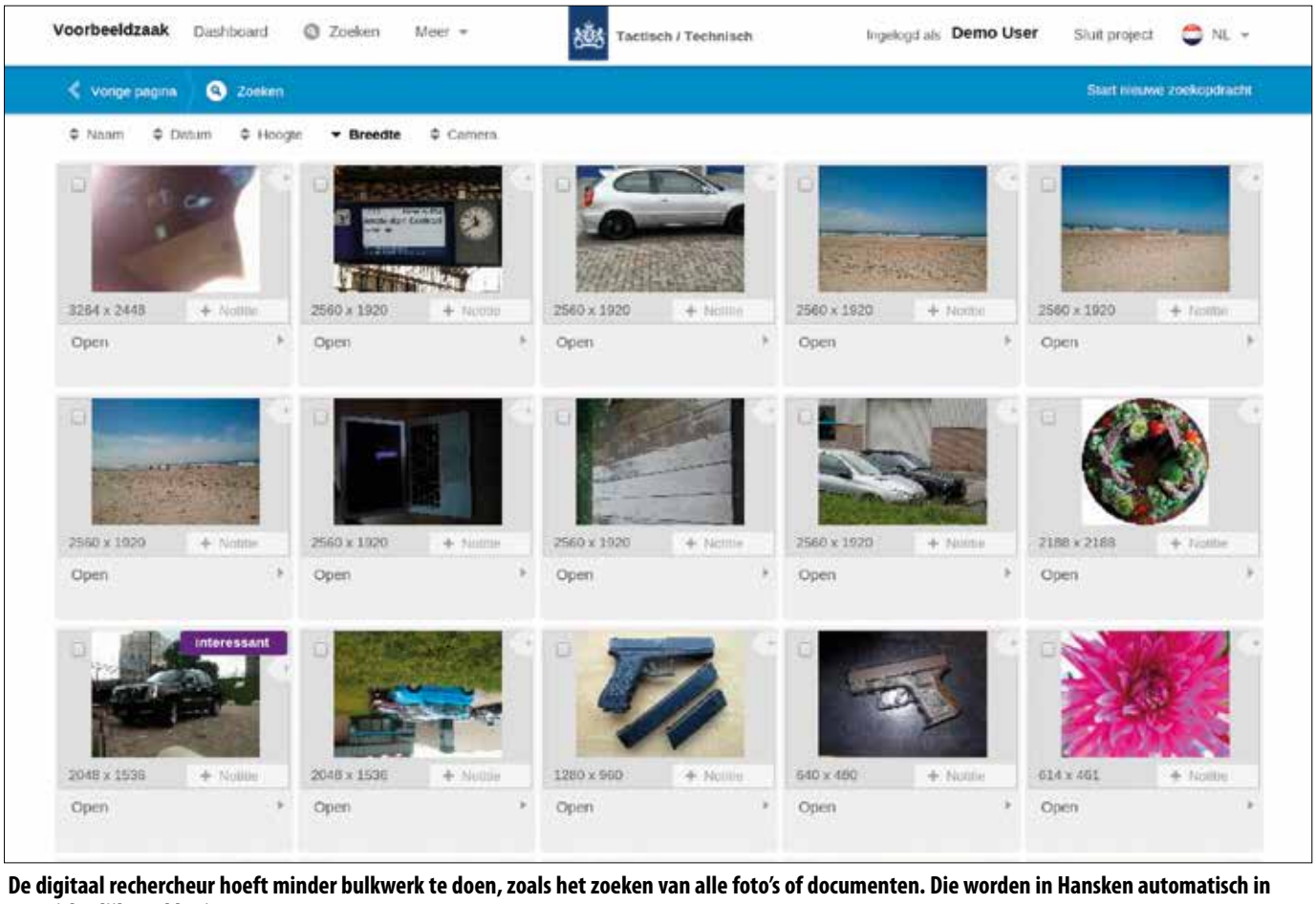
den sporen juist te interpreteren. "Met Hansken hebben we goed gekeken naar de forensische context", zegt Van Beek. "Je kunt wel veel data verwerken, maar als een plaatje of mailtje een bewijsstuk wordt, moet je kunnen aangeven waar dat gestaan heeft binnen die vier terabyte. Je kunt niet zeggen: 'Het stond ergens, geloof me maar.' En van bijvoorbeeld een mailtje dat in de conceptenmap staat, moet je zeker weten dat het niet is verzonden. De verdachte kan het daarnaartoe hebben versleept. De tactisch rechercheur is er niet voor opgeleid om dat soort dingen uit te zoeken, de digitaal rechercheur wel. Daarom adviseren wij om elk gevonden spoor voor een juiste interpretatie voor te leggen aan de expert, de digitaal rechercheur. 'Heb ik dit goed geïnterpreteerd, klopt het wat ik hier heb opgeschreven?'"

Zoekactie De eerder genoemde snelheid van indexeren, hangt een beetje af van de hoeveelheid data die in beslag is genomen en waaruit die bestaat - een paar grote of juist heel veel kleine bestanden - maar over het algemeen duurt zo'n zoekactie niet langer dan een paar seconden. Dat is heel snel, gezien de gigantische hoeveelheid informatie die tegenwoordig bij politieonderzoeken in beslag worden genomen. De grootste zaak tot nu toe was negentien terabyte, met zo'n zestig miljoen sporen afkomstig van ongeveer vijfhonderd apparaten. Harm van Beek, forensisch onderzoeker digitale technologie bij het Nederlands Forensisch Instituut, dat Hansken ontwikkelde: "En dan is bijvoorbeeld de vraag aan Hansken: waar zijn die twee mailtjes die relevant zijn voor het onderzoek?"

Snelle beschikbaarheid van de data kan zeer belangrijk zijn, bijvoorbeeld voor de scenariovorming, zegt Van Beek. "In de oude situatie was het digitale materiaal vaak pas zo laat beschikbaar, dat scenario's al bedacht waren en het hele tactisch plan al in uitvoering. Dan diende het vooral ter toetsing van de scenario's. Maar een mailtje of een chat tussen twee mensen kan juist aanleiding zijn voor een nieuw scenario. Ik zag dat tijdens een workshop die ik gaf over Xiraf (de voorganger van Hansken, red.). Tactisch rechercheurs konden daarmee de data doorzoeken van hun eigen onderzoek dat al een paar maanden liep. Ze vonden toen mailtjes van mensen die ze nog helemaal niet in het vizier hadden, maar die wel informatie deelden over wat er speelde in die zaak. Daaruit kwam een heel nieuw scenario bovendrijven. Dat is mooi, maar je wilt zoiets natuurlijk veel eerder in het proces."

Uploaden Hansken staat bij het rekencentrum van de politie, maar het uploaden gaat nu nog via het NFI. Een digitaal rechercheur levert daar kopieën aan van alle data. Bij elkaar kost dat een aantal dagen, maar de bedoeling is dat de digitaal rechercheur het straks zelf rechtstreeks uploadt. Het indexeren van de data, na het uploaden, gaat weer heel snel, aldus Van Beek. "Het belangrijkste van Hansken is, dat we in een ochtend een zaak beschikbaar kunnen stellen, waar dat eerst een paar dagen duurde. Maar in het huidige proces gaan daar dus wel een paar dagen aan vooraf. Op het moment dat de digitaal rechercheurs zelf die data in het systeem kunnen zetten, maak je daarin extra grote stappen."

>>



De digitaal rechercheur hoeft minder bulkwerk te doen, zoals het zoeken van alle foto's of documenten. Die worden in Hansken automatisch in overzichtelijke pakketjes neergezet.

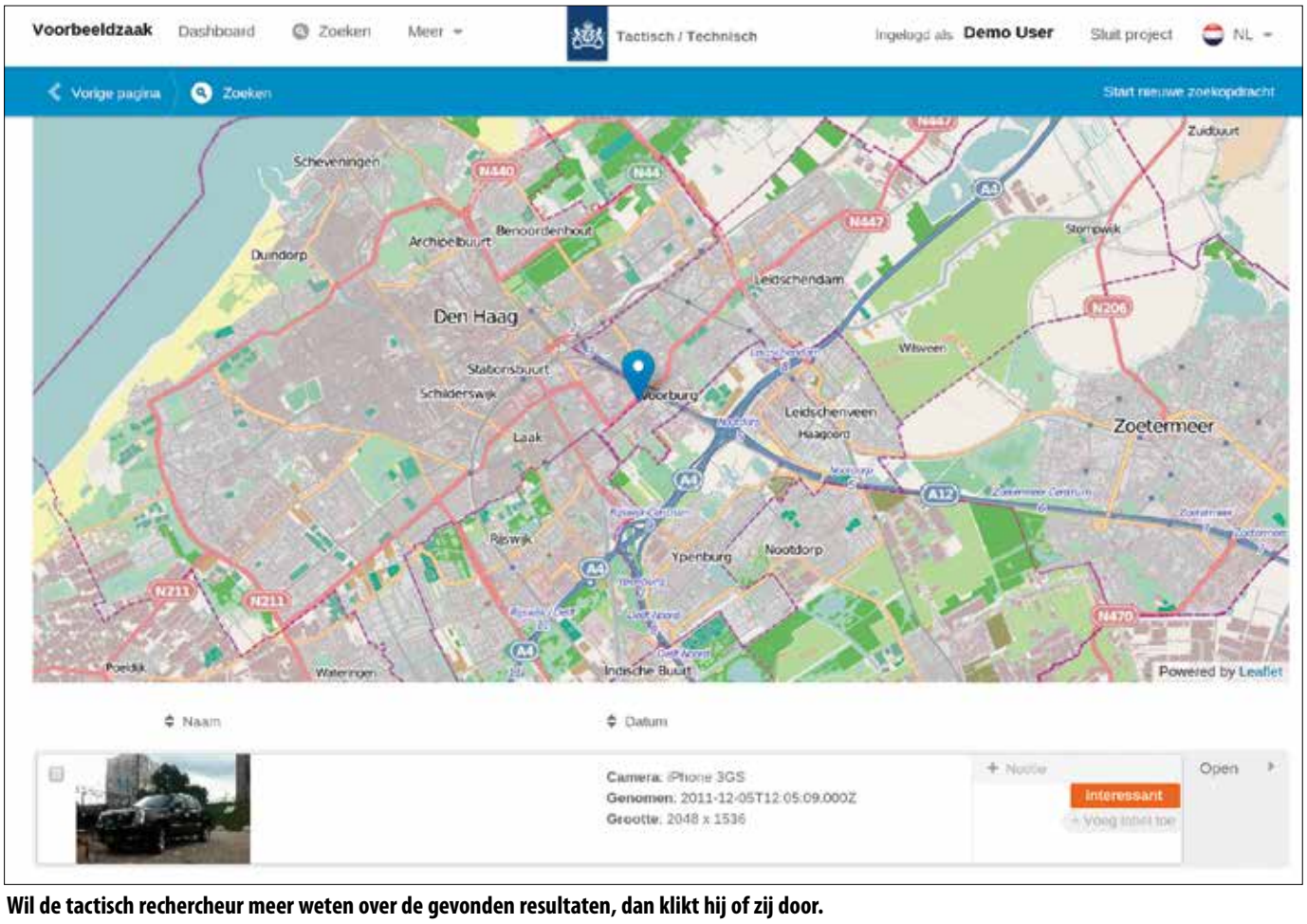
>> Dat heeft onder andere te maken met het netwerk waarop de zoekmachine is aangesloten, maar daar wordt naar gekeken. Dat netwerk bepaalt op dit ogenblik ook nog dat tactisch rechercheurs de zoekmachine niet rechtstreeks vanaf hun eigen bureau kunnen bedienen. Daarvoor moeten zij naar een PC binnen hun eenheid met een IRN-verbinding, het Internet Research Network. Rob Geerts is als informatiemanager bij de Dienst Informatiemanagement van de politie nauw betrokken bij de opzet en de doorontwikkeling van Hansken. "De verwachting is dat dat op den duur vanaf de eigen werkplek kan", zegt hij. "We proberen ervoor te zorgen dat dat zo snel mogelijk beschikbaar komt."

Keuze Mayke Mollen heeft tot nu toe één groot onderzoek gedraaid met Hansken. "Wij hadden op verschillende locaties enkele tientallen gegevensdragers in beslag genomen, telefoons, computers, laptops, harde schijven en dergelijke. Daarvan hebben we een derde naar Hansken gekopieerd. Het andere materiaal was namelijk zo oud dat daar waarschijnlijk geen relevante gegevens op staan. Eventueel kun je die later alsnog bekijken. Het deel dat we wel hebben gekopieerd naar Hansken was al duizenden gegevens, teksten, e-mails, foto's enzovoorts."

Die keuze wat wel en niet in Hansken wordt geüpload, is in deze situatie meestal nog noodzakelijk, zegt Jos van den Oetelaar, als operationeel specialist A werkzaam bij Digitale Opsporing Oost-Brabant. "Wij maken voor Hansken een exacte kopie van de harde schijf van een computer, want je mag nooit met het origineel gaan werken. Bij een geheugen van drie of vier terabyte duurt dat al gauw een dag. Die kopie gaat op een harde schijf naar het NFI, waarna het wordt geüpload naar Hansken en dan geïndexeerd: alle mailtjes bij elkaar en dergelijke, zelfs verwijderde bestanden staan netjes aangegeven. Maar dat alles is tijdrovend. Vandaar dat er altijd een schifting wordt gemaakt in overleg met de coördinator van het onderzoeksteam."

Het werken met Hansken levert nú al tijdwinst op, ten opzichte van voorganger Xiraf. Dat ervaren ook tactisch rechercheurs Jolanda van Esch en Laurens Olde Engberink van de Dienst Regionale Recherche Oost-Brabant. Zij werken samen aan een zaak, met behulp van Hansken. "We zijn blij met de snelheid van Hansken, dat is een groot verschil", zegt Olde Engberink. "Maar ook met de mogelijkheden om te zoeken en zoekresultaten uit te filteren. Je kunt bijvoorbeeld een tijdlijn aangeven, zodat je echt per dag kunt zoeken." Van Esch: "Hansken is ook gebruiksvriendelijker. Je kunt makkelijker aangeven wat je zoekt, en je krijgt de resultaten heel overzichtelijk in beeld. Wil je daar meer van zien, dan klik je door."

Interpretatie De digitaal rechercheur komt ook aan het eind van het onderzoek weer in beeld, om de interpretatie van



Wil de tactisch rechercheur meer weten over de gevonden resultaten, dan klikt hij of zij door.

de zoekresultaten te verifiëren als er een proces-verbaal moet worden opgemaakt. Olde Engberink: "Als wij in Hansken dingen aantreffen waar een datum, tijd of iets anders specifieks wordt genoemd, moet een digitaal rechercheur beoordelen of dat inderdaad klopt." Volgens Mollen kun je bij een zoekopdracht ook onbekende begrippen tegenkomen. "Dan is het goed dat een digitaal rechercheur nog een keer kijkt of ik als generalist het goed heb geïnterpreteerd." Van den Oetelaar: "In principe gaat er bij ons nooit een proces-verbaal uit over wat zij hebben gevonden in Hansken, zonder dat wij daarnaar hebben gekeken. De tactische recherche kan bijvoorbeeld noteren dat zij een Word-document heeft aangetroffen in de bak van Pietje, in 'mijn documenten', aangemaakt op die datum. Maar wanneer het voor het laatst is bewerkt of geopend, dat moeten wij uitzoeken."

Het werk als digitaal rechercheur is door Hansken veranderd, bevestigt hij. "Wij hoeven minder bulkwerk te doen, zoals het zoeken van alle foto's of documenten en dergelijke. Die worden in Hansken automatisch in overzichtelijke pakketjes neergezet. Daardoor komen wij meer toe aan waar we voor zijn: digitaal specialisme."

Vertrouwelijkheid Met de ontwikkeling van Hansken is ook uitgebreid gekeken naar vertrouwelijkheid, privacy en veiligheid. Van Beek: "In Hansken wordt bepaald wie wel en wie niet bij de data mag komen. Een computer die in beslag mocht worden genomen in het kader van een onderzoek, mag niet zomaar door iedere collega worden bekeken. Dus autorisatie en authenticatie - wie is ingelogd en wie is wat aan het doen - waren belangrijke aspecten in dit project. Daarnaast kan een rechercheur bepaalde informatie, bijvoorbeeld een medisch dossier, markeren als vertrouwelijk. Dat verdwijnt dan uit beeld. En er is een protocol voor het omgaan met geheimhoudersstukken. Je kunt bijvoorbeeld dingen waarin de naam of het telefoonnummer van de advocaat voorkomt, automatisch laten markeren als stukken die je niet mag inzien. Maar dan is er nog wel een persoon die beoordeelt of dat terecht is. Als die advocaat Jansen heet, zijn er misschien te veel stukken gemarkeerd."

In die zin is Hansken forensisch beter toegerust dan zijn voorganger Xiraf, die nog wel draait maar waarvan onderzoeken, vooral de grote, worden overgeheveld naar zijn opvolger. Van Beek: "Met Xiraf hebben we toen überhaupt niet over dat soort zaken nagedacht, want dat was een researchproject om te kijken of we een bepaalde technologie konden gebruiken in de data-analyse. Het was oorspronkelijk helemaal niet de bedoeling dat in de praktijk te gaan toepassen, totdat eind 2010 de zaak Robert M. zich voordeed. Daar werd in één keer acht terabyte aan data in beslag genomen en er lag veel druk op die zaak om met resultaten te komen. Maar daar waren geen goede instrumenten

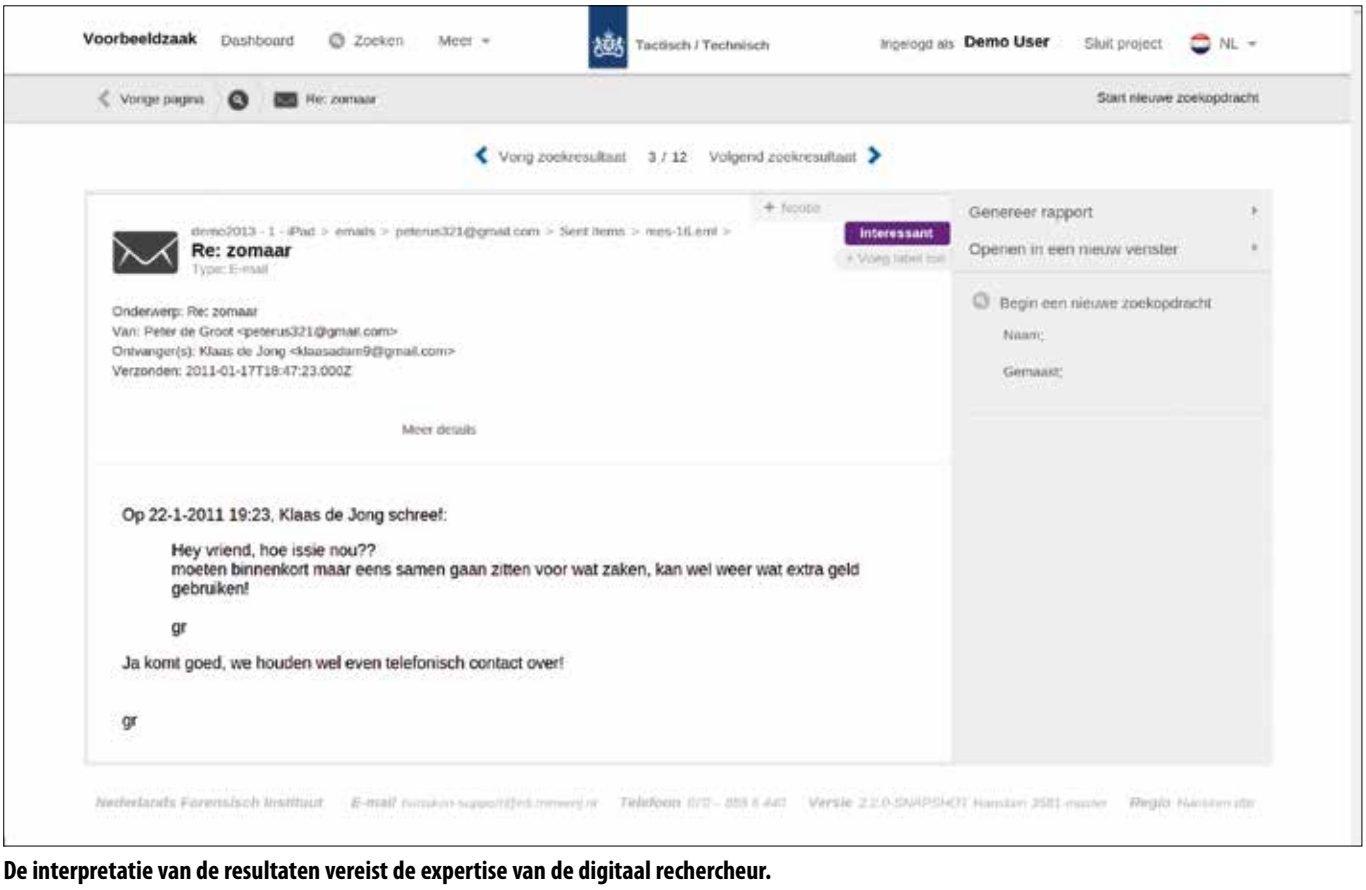
>>

>> voor. Omdat het project Xiraf best succesvol was, hebben we toen gezegd: je kunt het inzetten in deze zaak, probeer het gewoon. Xiraf hielp om snel door al die data te gaan en de goede mensen achter de knoppen te krijgen." Daarna zijn hiermee ook andere onderzoekszaken gedraaid, zelfs in het buitenland, onder andere in Canada, waarvandaan met behulp van Xiraf een groot internationaal kinderpornonetwerk werd opgerold.

Wedloop Xiraf bood vanaf 2010 dezelfde functionaliteit als Hansken, maar de laatste scoort duidelijk beter op snelheid en gebruiksvriendelijkheid en heeft veel meer capaciteit en uitbreidingsmogelijkheden. Toch is Hansken - genoemd naar een olifant die in de zeventiende eeuw door de Nederlanden toerde - nog niet helemaal af. En misschien zal hij ook wel nooit af zijn, zegt Harm van Beek. "Er zijn miljoenen apps, dus het is een soort wedloop om up-to-date te blijven met de meest gebruikte technieken. Een paar jaar geleden maakte ineens iedereen gebruik van WhatsApp, nu is dat Snapchat. Dan moeten we uitzoeken hoe dat precies werkt. Hoe slaat zo'n app bijvoorbeeld de chathistorie op een telefoon op? Wij leggen dat soort nieuwe ontwikkelingen vast in een digitale bibliotheek. Als we daarna in een zaak een telefoon tegenkomen, wordt vanuit die bibliotheek automatisch gekeken of die telefoon ook Snapchat-berichten bevat. Zo ja, dan voegen we die toe aan de sporendatabase. Toch zullen we altijd blijven achterlopen bij de realiteit, daar kun je niets aan doen. Wij zouden het fantastisch vinden als de bibliotheek ook wordt aangevuld met kennis van anderen. Bijvoorbeeld van digitaal rechercheurs, als die iets bijzonders tegenkomen in data. Als dat volgende week of volgend jaar in een andere zaak voorbijkomt, wordt het automatisch herkend. Dus wij zien Hansken ook wel als een kenniscentrum, waar we kennis verzamelen en automatisch kunnen toepassen op in beslag genomen data. Hoe meer kennis in Hansken, des te meer sporen we uit die data kunnen halen."

Rode auto Ook op andere vlakken blijft Hansken continu in ontwikkeling. Er wordt bijvoorbeeld nog software aan toegevoegd, PRNU, die foto's herkent aan het ruispatroon van één specifieke camera. Dan kun je zoeken op alle foto's van die camera. Verder zijn er met de UVA en de Vrije Universiteit in Amsterdam projecten rond het automatisch herkennen van teksten en afbeeldingen, bijvoorbeeld een rode auto, op foto's. "Dat is er nog niet over twee weken, maar het komt er wel aan", aldus Van Beek. Hansken kent al wel kenmerken van afbeeldingen van kinderporno en kan die foto's als zodanig markeren.

En hoewel Hansken al snel is, gaat er ook op dat vlak nog wel wat gebeuren. Wellicht wordt het in de toekomst mogelijk zelfs binnen één of twee dagen al te zoeken binnen de data. Dat zou dan van invloed kunnen zijn op de inverzekeringstelling van een verdachte. "Die eerste 72 uur kunnen cruciaal zijn", zegt Rob Geerts. "Hoe sneller we inzage hebben in de data van de telefoon van de verdachte, van zijn laptop, externe harde schijf of USB-stick, des te meer kans dat we binnen die tijd relevante informatie vinden."



De interpretatie van de resultaten vereist de expertise van de digitaal rechercheur.

Investeren Hansken is grotendeels ontwikkeld door het NFI, gebaseerd op input vanuit met name de politie en ervaringen met de voorloper Xiraf. Om deze producten te ontwikkelen heeft de politie de afgelopen jaren zowel met kennis als financieel veel geïnvesteerd. Daarbij is in eerste instantie vooral geïnvesteerd in het realiseren van een basis, Geerts noemt het 'Hansken Light'. Die is in oktober 2015 opgeleverd, ook al was het nog niet volledig af. Het is nu zaak deze light-versie door te ontwikkelen tot een volledig product. Daarnaast investeert de politie ook in het bouwen aan een partnership met het NFI voor de doorontwikkeling van Hansken.

Geerts: "Voor zowel de vernieuwing als de continuïteit van Hansken blijven investeringen nodig. De input, kennis en inzet van digitale expertise, intelligence en tactische recherche is onontbeerlijk om de gebruikersinterface, maar ook de kern van het systeem te verbeteren. We zijn bezig dit te organiseren, zodat we het NFI op de juiste manier met onze wensen en verbeteringen kunnen voeden. Maar de investeringen moeten natuurlijk passen in de ICT-portfolio, zodat we niet investeren in zaken die haaks staan op ontwikkelingen binnen de politie of de gekozen richtingen. Als we bijvoorbeeld kiezen meer te doen met social media en daar meer opsporingsgericht mee willen omgaan, dan zal dit in de ICT-portfolio prioriteit krijgen. De richting waarin we dan met Hansken ontwikkelen, zal daarop moeten aansluiten. De huidige financiële situatie en gedwongen bezuinigingen brengen met zich mee dat er keuzes gemaakt moeten worden en dat beïnvloedt de doorontwikkeling van Hansken of het tempo daarvan."

Intuïtief Sinds de lancering in oktober draaien er al zo'n zeventig zaken in Hansken, met rond de 3400 in beslag genomen apparaten en in totaal 190 terabyte aan data. Toch wordt de zoekmachine nog niet overal toegepast binnen de eenheden, maar volgens Geerts en Van Beek is dat een kwestie van tijd. Het NFI organiseert daarvoor trainingen. Niet zozeer om de rechercheurs te leren omgaan met de knoppen, want Hansken werkt 'intuïtief', aldus Geerts. "En bovendien wordt die interface nog doorontwikkeld, er wordt continu gewerkt aan de gebruiksvriendelijkheid." Van Beek: "Als je in digitaal materiaal gaat zoeken, kun je dingen tegenkomen waarvan je geen idee hebt wat het is. Met de trainingen willen we vooral bereiken dat tactisch rechercheurs een beetje begrijpen waar ze naar kijken: nullen en enen die zijn omgezet naar dingen die wij als mensen wél begrijpen, zoals teksten en plaatjes en dergelijke. Maar ook dat mensen niet bang zijn om Hansken te gaan gebruiken. En dat ze zich ervan bewust zijn, dat het onderzoek nog niet klaar is als zij iets hebben gevonden. Omdat de interpretatie daarvan de expertise van de digitaal rechercheur vereist."

De digitaal rechercheur wordt door de invoering van Hansken enigszins ontlast doordat hij zelf geen grootschalige zoekopdrachten meer hoeft uit te voeren. Maar met de interpretatie van zoekresultaten komt er weer werk bij, zeker gezien de toenemende hoeveelheid data. Rob Geerts: "De komende vier jaar moeten er zo'n vierhonderd digitaal rechercheurs bij komen. Die mogen we gaan werven, al is het natuurlijk nog wel een uitdaging om de juiste mensen te vinden. Dat betekent dat we méér zaken kunnen gaan ondersteunen, maar dus ook meer data gaan verwerken. Dat vraagt opnieuw om nóg slimmere toepassingen. Daarvoor willen we ook binnen de digitale opsporing Hansken inzetten, het betrekken in dat hele ontwikkelingsproces."

Pilot Raffinaderij

Naast de zoekmachine Hansken worden ook andere manieren onderzocht om grote hoeveelheden gestructureerde en ongestructureerde data doorzoekbaar te maken voor de rechercheurs. Momenteel draait daartoe de pilot Raffinaderij.

In de pilot 'Raffinaderij' onderzoeken rechercheurs en analisten uit de opsporing en informatieorganisatie de tools en mogelijkheden om snel grote hoeveelheden data te ontsluiten, betekenis te geven, te analyseren en te visualiseren. Het is namelijk van groot belang dat de data uit het digitaal beslag ook in samenhang met alle andere relevante (onderzoeks)data te analyseren zijn.

Momenteel richten de rechercheurs en analisten in de pilot zich op een beperkt aantal onderwerpen en thema's. Welke data zij gebruiken, hangt af van het onderzoek of thema. Deels gaat het om data uit digitaal beslag (Xiraf/Hansken), deels om de 'gewone' politiebronnen zoals BVH en Summ-IT. Ook ontsluiten zij gegevens die specifiek voor betreffende onderzoek(en) gebruikt mogen worden, zoals data die zijn verkregen met BOB-bevoegdheid. Komend jaar vindt met de operatie en de IV-organisatie een verkenning plaats of en zo ja op welke manier Raffinaderij wordt doorontwikkeld en uitgerold binnen de politie.

Wilt u reageren op dit artikel?
Mail naar redactie.blauw@politieacademie.nl

Voor meer informatie:
Kompol: zoektermen Computeronderzoek, Mobiele telefoononderzoek, Onderzoek aan digitale elektronica, Onderzoek overige gegevensdragers
Via navigeren > Forensische opsporing > Digitale opsporing