SUPER SCIENCE

HANS HENSELER

DIGITAAL BEWIJS KAN VOOR NIET-INGEWIJDEN ALS HARD EN HELDER WORDEN GEZIEN, MAAR DE FORENSISCHE REALITEIT IS LASTIGER. JE MOET VOORZICHTIG ZIJN MET DATA IN OPSPORINGSZAKEN, WEET FORENSISCH EXPERT EN LECTOR HANS HENSELER. "HET GAAT STEEDS VAKER OM WAARSCHIJNLIJKHEDEN."

door Jasper Bakker beeld Marieke van Pagée

'IK VERBIND WETENSCHAP EN RECHERCHE'

Digital forensics verdrinkt bijna in data

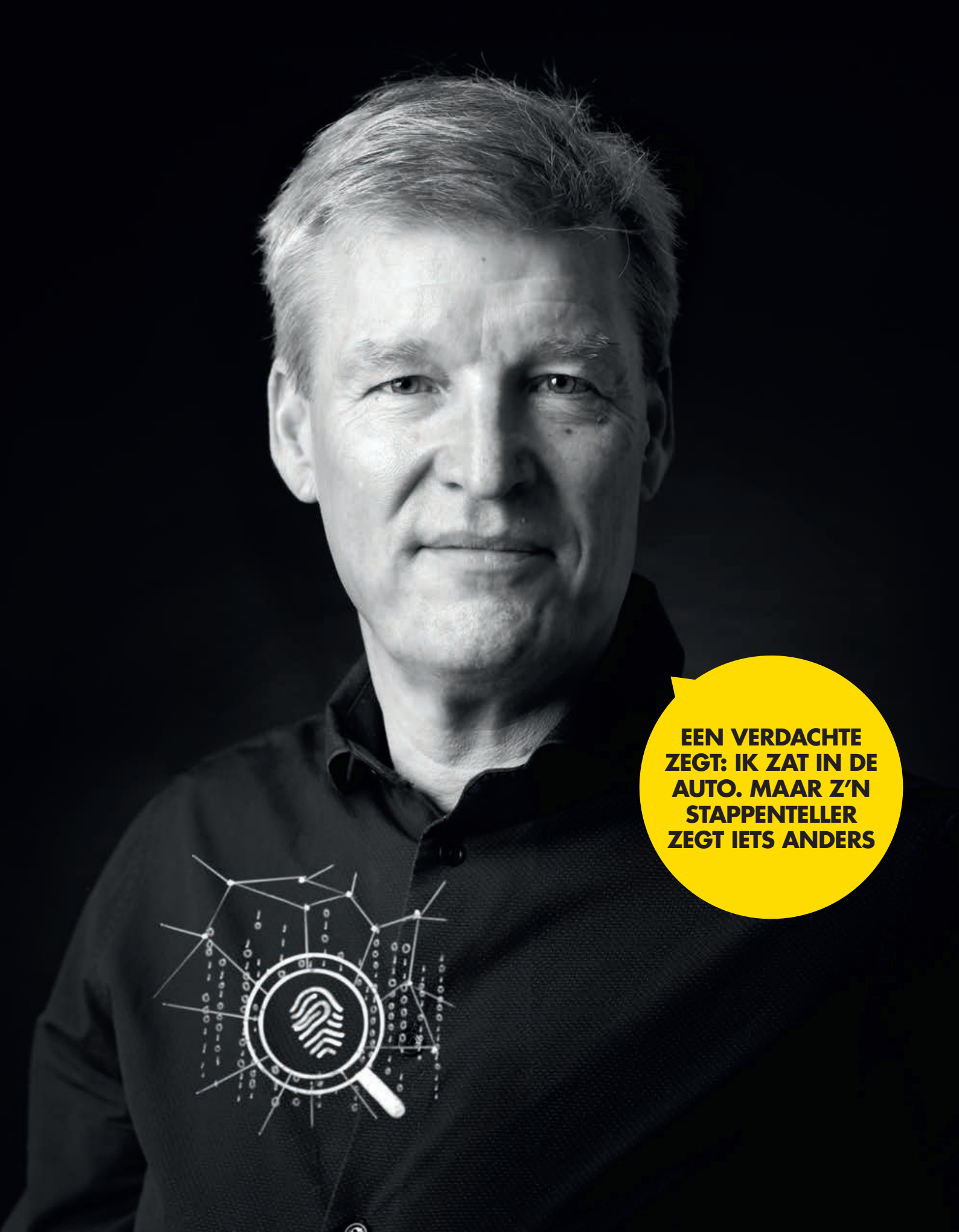
HOE DATA TE INTERPRETEREN EN WELKE SCENARIO'S DAARMEE MEER OF MINDER WAARSCHIJNLIJK ZIJN, dát is de praktijk van digital forensics. "Dat zie je in rechtszaken: een verdachte zegt: ik zat in de auto, maar de stappenteller zegt iets anders." Daarmee is niet keihard bewezen dat de verdachte liegt, maar er valt gerede twijfel te plaatsen. En daarmee is er mogelijk reden voor verder onderzoek naar meer digitale informatie en ander bewijsmateriaal.

Dr. ir. Hans Henseler is al jaren bezig met deze (relatief nieuwe) tak van sport voor opsporing en bewijsvoering. Hij is lector Digital Forensics & E-Discovery bij de specialisatie Forensische ICT aan de Hogeschool Leiden, senior adviseur voor Digital Forensics bij het Nederlands Forensisch Instituut (NFI), en medeoprichter van Volto Labs dat technologie ontwikkelt voor zogeheten 'cyber humint' activiteiten. Dat laatste is het uit digitale middelen vergaren van inlichtingen uit 'menselijke bron' (human intelligence).

KWESTIE VAN WAARSCHIJNLIJKHEDEN

Digitaal forensisch onderzoek kan veel betekenen, voor cybercrime maar ook juist voor traditionele misdaad. Bijvoorbeeld om verdachten in beeld te krijgen, én om scenario's te testen. Welke verklaring voor een situatie is waarschijnlijk? Het zal dan nooit om 100% gaan, "maar wel om grote waarschijnlijkheden". Dit geldt ook voor DNA, aldus de expert. Hij spreekt van een trend waarbij er wordt geredeneerd met hypotheses en scenario's, zowel door de officier van Justitie als door de verdediging.
De crux is daarbij het interpreteren van data. "Sporen liegen niet." Als een smartwatch bijvoorbeeld aangeeft dat de hartslag van de drager om 4:01 uur is gestopt, dan zegt dat wat. De kunst is het uitdrukken van verschillende sporen in kansen, waarbij informatie zoals van een smartwatch wordt gecombineerd met ander materiaal om tot grotere waarschijnlijkheden te komen.

Aannemelijkheid van scenario's kan daadwerkelijk leiden tot veroordelingen. Een recent praktijkgeval is de Bûterweimoord, in Friesland. Een vrouw wordt ervan verdacht dat zij - met hulp - haar man heeft omgebracht. Zij verklaart dat ze de hele nacht naar haar man heeft gezocht. Onderzoekers vinden het vreemd dat ze niet heeft geprobeerd haar man te bellen. In haar verklaring stelt ze dat de accu van haar telefoon leeg was.
Uit het forensisch onderzoek kwamen echter geen aanwijzingen daarvoor, en het was waarschijnlijker dat ze haar telefoon had uitgezet, vertelt Henseler. Ook het ontbreken van data kan dus veelzeggend zijn. "Er is veel mee te doen, maar het is moeilijk."


EEN VERDACHTE ZEGT: IK ZAT IN DE AUTO. MAAR Z'N STAPPENTELLER ZEGT IETS ANDERS

DIGITALE SPELDEN IN DATA-HOOIBERG

Complicerende factor is de grote hoeveelheid digitaal materiaal. Om de beschikbare - en groeiende - bergen data door te spitten, heeft het Nederlands Forensisch Instituut (NFI) een zoekplatform ontwikkeld: Hansken. Vernoemd naar een circusolifant die in de 17e eeuw is geschilderd door Rembrandt.
"Hansken kon in het publiek (van een circusvoorstelling - red.) een crimineel aanwijzen", licht Henseler toe. Het gelijknamige zoekplatform van de 21e eeuw doet inmiddels al dienst bij veel opsporingsdiensten.

CRYPTOFOONS EN COMBINATIES

Een voorbeeld uit de praktijk wat digitale data allemaal kan betekenen voor opsporing en veroordeling van criminelen is het succes dat is geboekt met cryptofoons en versleutelde chat-apps. Sky ECC en Encrochat zijn twee gevallen uit de criminele wereld waarbij niet alleen de afgetapte conversaties van belang zijn geweest. Ook de combinatie met gewone, herleidbare smartphones; om zo communicatie te kunnen koppelen aan personen. "Kun je bewijzen dat twee smartphones in dezelfde broekzak zaten? Hoe waarschijnlijk is het?" Data kunnen het antwoord verschaffen.

Henseler benadrukt dat het hierbij niet alleen gaat om kunnen bewijzen, maar ook om kunnen ontkrachten. Scenario's falsificeren dus. "Stel: je vindt een lichaam, maar hebt geen verdachte.
Of: je hebt wel een verdachte, maar geen lichaam." Ook dan kunnen data veel betekenen om diverse scenario's te voorzien van verschillende waarschijnlijkheden.

In de praktijk blijkt het ontsleutelen van het criminele communicatienetwerk Encrochat ook als gevolg te hebben dat enorme hoeveelheden data doorzocht moeten worden. Er is veel, heel veel data beschikbaar, maar dat moet nog gekoppeld worden aan opsporingszaken en misdaden (waaronder ook onvermoede of onbekende misdaden).

> Voor rechercheurs moet de interface van digitale opsporingstools beter worden, intuïtief en simpel

Naast data-overvloed is er nog een ander probleem dat speelt voor digital forensics: versleuteling. "Het wordt steeds moeilijker om telefoons uit te lezen." Dat hoeft vooralsnog geen enorm probleem te zijn, want gelukkig zijn er nog veel andere databronnen waarbij encryptie zeldzaam is.

ZÉLF NADENKEN

Henseler relativeert nog: over vijf jaar zullen veel van de huidige middelen en methoden verouderd zijn. Door bijvoorbeeld 'iOS 19' tegen die tijd. "We leren studenten om zelf na te denken en om zelf tools te maken." Simpelweg vertrouwen op middelen die nú werken, is niet houdbaar en dus niet slim.

Belangrijk hierbij is om ook verder te kijken dan alleen bestaande of geijkte middelen. De huidige grote commerciële tools komen uit Zwitserland, Canada, de Verenigde Staten en Israël, vertelt Henseler. Maar van de FlitsMeister-app hebben veel onderzoekers en opsporingsmensen niet gehoord. "Die app houdt wel elke drie seconden je locatie bij."
Dan nog is het zaak om gezond verstand te gebruiken om niet te verdrinken in data. Door te denken in waarschijnlijkheden valt er beter te bepalen welke onderzoeksrichtingen wat kunnen opleveren. "Als je in een onderzoek honderd telefoons hebt, ga je niet honderd keer FlitsMeister-apps uitlezen. Dat moet dan alleen voor toestellen worden gedaan waarbij twijfel bestaat over de locatie van de toestelgebruiker, of het waarheidsgehalte van diens verklaring over locatie."

HANSKEN VOOR WETENSCHAPPERS

Naast zelf nadenken wordt er ook verder gebouwd aan digitale tools. Enerzijds dankzij vooruitgang op het gebied van bijvoorbeeld deep learning, Henseler is dertig jaar terug gepromoveerd op neurale netwerken. Anderzijds met vooruitgang op het gebied van simpelweg de gebruikersinterface. "Voor rechercheurs moet de interface echt beter worden, want zij gebruiken digitale forensische tools zeker niet dagelijks."
De werking moet dan intuïtief en simpel zijn - zonder dat dat de effectiviteit of accuraatheid raakt.

Het doorontwikkelen van digitale opsporingsmiddelen gebeurt niet alleen binnen het NFI of de politie, geeft Henseler nog aan. Zo wordt er van de forensische zoekmachine Hansken een academische versie gemaakt, waar hij bezig mee is bij de Hogeschool Leiden en de UvA (Universiteit van Amsterdam). "We proberen subsidie te krijgen om de academische versie als experimenteerplatform aan te bieden."
Dat is dan niet slechts voor gebruik 'buiten de politie', maar ook voor verbouwen en verbeteren van Hansken.

BRUG SLAAN

De toevoeging van externe plugins, bijvoorbeeld voor data-extractie, kan leiden tot een ware appstore voor ontwikkelaars. Dit kan dan interessant zijn voor wetenschappers, terwijl Hansken voor forensisch onderzoekers en voor de politie 'puur' kan blijven. "Ik probeer een brug te slaan tussen wetenschap en recherche."
Digital forensics heeft namelijk een grootse toekomst: anno nu heeft naar schatting zo'n 90% van alle opsporingszaken een digitaal component.