Open Universiteit

PROF. DR. IR. H.M.A. (HARM) VAN BEEK

Digitale sporen: duidelijk onduidelijk

Van Beek HMA (2025). Digitale sporen: duidelijk onduidelijk.
Open Universiteit, Heerlen.
DOI: 10.71583/20250919hvb

Redactie: Eefje Marijt

De afbeelding op de omslag is gegenereerd met *Google Gemini / Imagen 3*.

Inhoud

Open Universiteit

Digitale sporen: duidelijk onduidelijk

Rede

Uitgesproken bij de openbare aanvaarding van het ambt van bijzonder hoogleraar Digital Forensics, ingesteld door het Nederlands Forensisch Instituut, aan de Open Universiteit op

vrijdag 19 september 2025

door prof. dr. ir. H.M.A. (Harm) van Beek

Meneer de rector magnificus, waarde leden van het curatorium, geachte decaan, geachte directie van het Nederlands Forensisch Instituut, beste collega's, oud-collega's, familie, vrienden en bekenden zowel hier in de zaal als online,

Welkom hier vandaag in Heerlen, waar ik mijn oratie mag uitspreken ter aanvaarding van het ambt van bijzonder hoogleraar Digital Forensics, ingesteld door het Nederlands Forensisch Instituut (NFI), bij de faculteit Bètawetenschappen van de Open Universiteit. Ik vind het fijn dat jullie naar Zuid-Limburg zijn gekomen, want voor de meesten van jullie is dit niet bepaald om de hoek.

Inleiding

Zoals velen van jullie weten, werk ik sinds 2009 bij het Nederlands Forensisch Instituut in Den Haag. Als informaticus onderzoek ik daar digitale sporen. Ik help de politie en officieren van justitie met het oplossen van strafzaken en ik leg als gerechtelijk deskundige aan rechters uit hoe ze digitale sporen kunnen gebruiken als belastend of ontlastend bewijs. Ook ben ik als wetenschapper betrokken bij meerdere onderzoeksprojecten. Deze leerstoel vormt dan ook een brug tussen de faculteiten Bètawetenschappen en Rechtswetenschappen van de Open Universiteit, en tussen het Nederlands Forensisch Instituut en deze twee faculteiten.

Ik zal eerst een achtergrond geven. Ik leg uit wat digitale sporen zijn, hoe je data in sporen kan omzetten en hoe deze normaal gesproken worden gebruikt voor digitale opsporing en bewijsvoering. Daarna zal ik kort toelichten waarom sporen in de digitale wereld anders werken dan in de fysieke wereld en wat dit betekent voor de betrouwbaarheid van de onderzoeken. Want het is belangrijk dat bewijs juist wordt geïnterpreteerd. Hierna ga ik in op het wetenschappelijk onderzoek dat ik binnen de leerstoel vorm wil geven, om digitale sporen beter te kunnen duiden, en rechtmatig te kunnen gebruiken.

1 Digitale sporen

We doen tegenwoordig veel digitaal. We communiceren digitaal, fotograferen digitaal en vinden digitaal een partner. Of we worden digitaal geholpen, bijvoorbeeld in het verkeer bij het vinden van de juiste weg, of in de winkel bij het contactloos betalen. Bewust of onbewust laten we hierbij continu digitale sporen achter. En niet maar een paar, nee, we strooien ermee alsof het niets kost. Om daar een goed beeld van te krijgen, wil ik met jullie graag een klein experiment uitvoeren. Als je een mobiele telefoon bij je hebt, Wil je dan je hand opsteken?

Zoals jullie kunnen zien is dat vrijwel iedereen, onafhankelijk van leeftijd, geslacht, baan of rol. Op al deze telefoons staan sporen die iets met deze oratie te maken hebben. Bedenk zelf maar eens op hoeveel van de volgende vragen je 'ja' moet antwoorden:

- Heb je een mail of bericht ontvangen over deze oratie?
- Staat deze oratie in jouw digitale agenda?
- Heb je op internet gezocht naar meer informatie over oraties?
- Of heb je het er met chatGPT over gehad?
- Heb je een bericht gestuurd of ontvangen over het plannen van je bezoek?
- Heb je een navigatiesysteem of -app gebruikt om in Heerlen te komen?
- Heb je onderweg contactloos betaald met je telefoon?
- Heb je zojuist of onderweg hiernaartoe een foto gemaakt en/of gedeeld?
- En draag je misschien een smartwatch of fitness-tracker?

Bij elke 'ja' strooi je met digitale sporen, namelijk de berichten en foto's zelf, de bestemmingen in de navigatie-app en transacties in de betaal-app, maar ook de gegevens die automatisch worden verzameld, zoals jouw locatie, het aantal door jou gezette stappen en hoe vol de batterij van je telefoon is. Zo laten we dus bewust en onbewust allemaal digitale sporen achter en hebben wij met elkaar vele duizenden sporen achtergelaten die te herleiden zijn naar deze oratie.

Deze sporen zijn grofweg op te delen in drie verschillende groepen. Ten eerste zijn er sporen die wij als mensen bewust maken, waarin we informatie vastleggen en/of met elkaar delen. Bijvoorbeeld een chatbericht, een e-mail of een digitale foto. Ten tweede zijn er sporen die zonder tussenkomst van een gebruiker door sensoren in apparaten worden vastgelegd, bijvoorbeeld op welke locatie je telefoon is, hoeveel stappen je hebt gezet, of wat je hartslag is. En ten derde zijn er sporen die het gebruik en de instellingen vastleggen, zoals sporen van het ontgrendelen van je telefoon of het verbinden met een wifi-netwerk. Er zijn ook combinaties mogelijk, bijvoorbeeld een digitale foto waarin ook een locatie is vastgelegd.

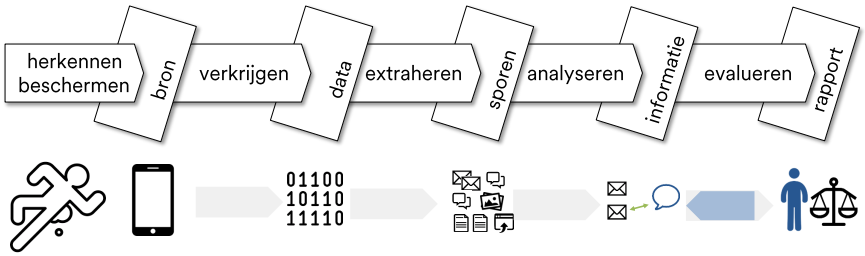
Al deze sporen kunnen iets zeggen over het gebruik van het apparaat en dus ook over de gebruiker van het apparaat. Als de gebruiker mogelijk betrokken is bij een strafbaar feit, bijvoorbeeld als verdachte of als slachtoffer, dan kunnen deze sporen dus ook aanwijzingen geven. Ze kunnen zo helpen met het oplossen van een zaak.

2 Digitale opsporing in de praktijk

Stel dat over twee weken de politie ineens bij je op de stoep staat. Je wordt ervan verdacht dat je enkele producten hebt gestolen. Dit vond plaats op 19 september 2025, rond kwart over vier, uit de supermarkt waar je meestal boodschappen doet.

Sporen in jouw telefoon kunnen dit mogelijk bevestigen of ontkrachten en de politie dus helpen met het oplossen van de zaak. Misschien heb je erover geappt of heb je de diefstal wel zelf vastgelegd. Ook sensorsporen zoals de locatie van je telefoon kunnen richting geven. Je zult het waarschijnlijk ontkennen, want op dat tijdstip was je bij deze oratie op de Open Universiteit in Heerlen. En, afhankelijk van hoe vaak je zojuist 'ja' hebt geantwoord, zijn daar sporen van in je telefoon, auto of smartwatch.

Als de politie gegevens uit jouw telefoon wil gebruiken, dan verloopt dat via een redelijk vast proces, waarbij rekening moet worden gehouden met technische, forensische en juridische eisen [6].



Figuur 2.1: Stappen in een forensisch onderzoek [6]

2.1 Digitale data veiligstellen

Als jouw telefoon in beslag wordt genomen, dan worden eerst met speciale apparatuur alle gegevens eruit gehaald, de zogenaamde *data*. Dit zijn alle nullen en énen die zijn vastgelegd op harde schijven en in geheugenchips. Voor een winkeldiefstal zal dat niet snel gebeuren, maar misschien zit er wel meer achter. Als er genoeg reden is voor zelfs een huiszoeking, dan vindt de politie naast jouw telefoon al snel tientallen apparaten waar mogelijk bewijs in zit.

Ik weet niet hoe dat bij jullie is, maar bij mij ligt bijvoorbeeld in vrijwel elke la een USB-stick of oude telefoon, en je hebt vast ook wel een computer of een laptop.

Na inbeslagname worden de apparaten aan digitaal experts gegeven om de data eruit te halen. Dit is al een hele kunst op zich, zeker met alle beveiligingsmaatregelen die er juist voor zorgen dat de data in die apparaten niet zomaar toegankelijk zijn voor onbevoegden. Al die apparaten vragen dan ook om hun eigen technieken om de data eruit te halen. Als het lukt, levert dit per apparaat een hele berg data op.

2.2 Data inzichtelijk en doorzoekbaar maken

Als er eenmaal data zijn, dan is de volgende stap het inzichtelijk en doorzoekbaar maken van deze data, dus om er sporen van te maken die wij als mensen kunnen begrijpen. Er zijn verschillende manieren om dit te doen, afhankelijk van waar de data vandaan komen, hoeveel data er zijn en de onderzoeksvragen van de rechercheurs die aan de zaak werken. In het algemeen worden de data door digitaal experts geopend in forensische computerprogramma's, vaak gericht op een bepaalde bron zoals een telefoon of juist een USB-stick of harde schijf uit een computer.

NFI bouwt krachtige forensische zoekmachine voor digitaal onderzoek [17]
Het gemiddeld aantal digitale sporen dat onderzoekers in strafzaken aantreffen, verdubbelt elke vijftien maanden. Om deze groeiende hoeveelheden data snel en makkelijk doorzoekbaar te blijven maken, ontwikkelde het Nederlands Forensisch Instituut (NFI) de forensische zoekmachine Hansken.

Met behulp van Hansken kan de politie digitaal forensisch onderzoek snel en efficiënt blijven uitvoeren. Het maakt niet uit of rechercheurs een aantal laptops of een heel serverpark moeten doorspitten. Alle in beslag genomen gegevens worden in Hansken gekopieerd. Vervolgens identificeert de software zoveel mogelijk sporen. Door zijn opbouw is Hansken net als een zoekmachine in staat een enorme hoeveelheid data te herkennen en doorzoekbaar te maken.

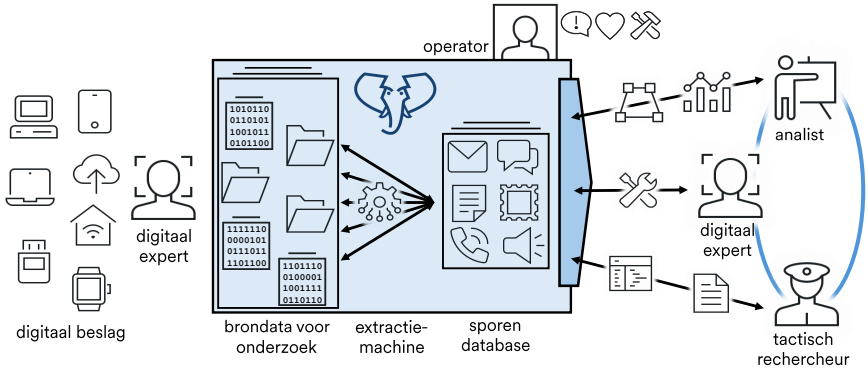
Deze Nederlandse implementatie van *Digital Forensics as a Service* [2, 3, 7] is de opvolger van Xiraf [1]. Inmiddels leveren ook partners uit de internationale community van inlichtingen- en opsporingsdiensten actief een bijdrage aan het platform. Ook het academisch netwerk rondom Hansken groeit. De deelnemende universiteiten en hogescholen werken hierin samen door Hansken in te zetten voor onderwijs en onderzoeksdoeleinden.

In 2024 won Hansken de eerste prijs in de categorie 'Digital Transformation' bij de European Public Sector Awards [21].

Zie hansken.org voor meer informatie over Hansken.

Digitaal experts kunnen data met deze computerprogramma's omzetten in leesbare sporen, zoals e-mails en afbeeldingen, en deze vervolgens doorzoeken. Digitale experts hebben vaak moeite om te bepalen welke gegevens relevant zijn, omdat ze niet inhoudelijk bij de zaak betrokken zijn. Rechercheurs, die onbekend zijn met de inhoud van de in beslag genomen apparaten, vragen daarom vaak om alle beschikbare e-mails, foto's of chatberichten, en soms zelfs gewoon om "alles". Dit werkt niet snel en efficiënt. Een oplossing is dat de rechercheurs zelf, met hulp van de digitaal experts, gebruik maken van de forensische computerprogramma's en zo op zoek gaan naar interessante sporen.

Als er veel verschillende bronnen zijn, dan willen de rechercheurs die aan een zaak werken graag zelf in alle data uit alle bronnen tegelijk zoeken. Ze zijn namelijk op zoek naar aanwijzingen of bewijs, maar het maakt ze niet uit of dat ene e-mailtje verstuurd is met Outlook vanaf een computer, met de Mail-app vanaf een iPhone, of met Gmail vanuit een browser. Om dit mogelijk te maken, heb ik met collega's van het NFI en meerdere inlichtingen- en opsporingsdiensten een platform ontwikkeld.



Figuur 2.2: Hansken: Digital Forensics as a Service [2, 3, 7]

Dit platform, met de naam Hansken [17], beschikt over technieken die er samen voor zorgen dat alle sporen in de data doorzoekbaar zijn. En dat dit zoeken aansluit bij hoe rechercheurs gewend zijn te werken. Dit zoeken op het Hanskenplatform lijkt op hoe je naar een product zoekt in een webwinkel. Je opent de Hanskenwebsite, logt in, opent de zaak waaraan je werkt en je krijgt alle sporen te zien. Dit zijn er zoals eerder uitgelegd heel veel. In een gemiddelde zaak vind je zomaar 10 miljoen sporen.

Die zijn natuurlijk niet allemaal relevant voor het onderzoek, net zoals niet alle kledingstukken in een webwinkel interessant voor je zijn. Daar kun je bijvoorbeeld filteren op de T-shirts, van een bepaald materiaal, in een bepaalde kleur, in een bepaalde maat, met een bepaalde opdruk. Op een gegeven moment ga je ze één voor één beoordelen. Op een vergelijkbare manier kunnen rechercheurs met Hansken filters toepassen om uiteindelijk individuele sporen te bekijken. Zo kunnen ze bijvoorbeeld filteren op de chatberichten, de e-mails of de afbeeldingen. En ook kunnen ze filters combineren, dus bijvoorbeeld alle chatberichten, verstuurd in 2025, waar het woord 'oratie' in voorkomt.

Tegenwoordig worden rechercheur hierbij ook geholpen door kunstmatige intelligentie (artifical intelligence, AI) [12]. Hansken kan bijvoorbeeld vaststellen wat er op een afbeelding staat. En gesproken berichten kan Hansken omzetten in leesbare tekst. Rechercheurs kunnen dan zoeken op foto's van een vuurwapen, een druglab of cash geld, of ze kunnen zoeken op audioberichten waarin een bepaalde naam wordt genoemd. Ook kan met moderne taalmodellen bijvoorbeeld een lang chatgesprek worden samengevat [9, 15]. Op deze manier is het vinden van mogelijk relevante sporen makkelijker.

Replica schedel Hansken van Het Rembrandthuis naar NFI [19]
Ze is een beroemde olifant, die in de zeventiende eeuw door de kunstenaar Rembrandt werd vastgelegd, én ze belichaamt de toekomst van de misdaadbestrijding in de 21e eeuw: Hansken. Een replica van de schedel van de olifant Hansken is door Museum Het Rembrandthuis in Amsterdam overgedragen aan het Nederlands Forensisch Instituut (NFI) in Den Haag. Het NFI vernoemde een digitale zoekmachine om snel grote hoeveelheden digitale data te doorzoeken naar de beroemde olifant. Opsporingsdiensten van over de hele wereld maken hier inmiddels gebruik van.

Het NFI is blij met de replica, vertelt Harm van Beek, senior digitaal onderzoeker bij het NFI. Hij is één van de 'founding fathers' van het digitaal-forensisch data-analyseplatform Hansken. "Ik had het imposante skelet al in Florence gezien. Dit is een replica van de schedel, maar het geeft toch een indruk van hoe imposant het dier was." Van Beek was een van de naamgevers van het platform. "De voorloper van Hansken was Xiraf. Dat was een acroniem, maar fonetisch doet het aan een giraf denken. Voor de grotere opvolger van Xiraf wilden we een soortgelijke naam," vertelt hij. "Een olifant is een goedaardig steppedier, net als de giraf. We wilden ook een link met Nederland en een collega kwam toen met de naam Hansken. Hansken was getraind in het doen van kunstjes en zij kon volgens de overlevering met haar slurf boeven aanwijzen in het publiek. Daarnaast wist ze door training met wapens om te gaan. Dat vonden we allemaal wel toepasselijk," lacht hij.

2.3 Relevante resultaten rapporteren

De relevante sporen worden gerapporteerd in een proces-verbaal. Als Hansken is gebruikt, dan wordt vaak ook een rapport van het spoor uit Hansken gehaald. Dit rapport bevat zowel de inhoud van het spoor, bijvoorbeeld een chatgesprek, als de locatie waar deze op een apparaat zijn gevonden. Dit is belangrijk voor het gebruik ervan als bewijs. Daarnaast worden de technieken beschreven die gebruikt zijn om tot deze resultaten te komen. Zo kun je controleren of het verwerken van data foutloos is verlopen. Ook dan kan er nog steeds discussie ontstaan over de gerapporteerde sporen. Daar kom ik later op terug.

Uiteindelijk vormt zich zo een dossier met alle informatie die onderbouwt wat er volgens de politie gebeurd is. Dit dossier gebruikt de officier van justitie van het Openbaar Ministerie om zijn beeld van de waarheid te onderbouwen en een gepaste straf voor te stellen bij een rechter. Jij, als verdachte, hebt misschien wel een ander beeld. Jouw advocaat kan met ontlastend bewijs komen, bijvoorbeeld een getuige die jouw beeld ondersteunt. Als jouw ontlastend bewijs in jouw telefoon zit, dan is dat wel lastig. Je telefoon kan namelijk nog bij de politie liggen. De politie kan jouw bewijs opzoeken en vastleggen in een proces-verbaal. In sommige gevallen, kan tegenwoordig ook jouw advocaat zelf toegang krijgen tot de data uit jouw telefoon [20] en de officier van justitie vragen om specifieke sporen in het dossier op te nemen. Dus dat chatberichtje dat je ‘net op tijd in Heerlen was voor de oratie’ kan er zo voor zorgen dat je niet in de problemen komt.

NFI maakt inzage cryptocommunicatie op werkplek advocaten mogelijk [20]
Het Nederlands Forensisch Instituut (NFI) heeft met de politie en het Openbaar Ministerie (OM) een methode ontwikkeld, waarmee advocaten via de digitale zoekmachine Hansken vanaf hun eigen kantoor cryptocommunicatie zoals met Encrochat kunnen inzien. “De nieuwe wijze van inzage in digitale bewijsmiddelen met een professionele zoekmachine vanaf de eigen werkplek van advocaten, is uniek in de wereld,” zegt de landelijk officier van justitie digitale opsporing Martijn Egberts. De eerste geluiden uit de advocatuur zijn positief.

Advocaten kunnen met de nieuwe methode – na toestemming om de data in te zien – vanaf hun eigen computer via een beveiligde verbinding toegang krijgen tot die data in Hansken. Advocaat Desiree de Jonge probeerde de nieuwe methode uit: “Met het realiseren van de inzagefunctie van Hansken op afstand wordt een grote en belangrijke stap gezet in het daadwerkelijk faciliteren van de inzagemogelijkheden die de verdediging in strafzaken moet hebben.”

3 De complexe digitale wereld

Bovenstaande werkwijze en onderzoek naar digitale sporen lijkt voordehand liggend. Wat kan er mis gaan? Het antwoord op die vraag is: heel veel!

Dit heeft van alles te maken met de verschillen tussen de digitale wereld en de fysieke wereld, en dus sporen in die werelden [16]. De digitale wereld is namelijk door mensen bedacht en ontworpen. Daarom gelden bijvoorbeeld de natuurwetten niet altijd. Daarnaast verandert deze wereld erg snel.

3.1 Een variëteit aan sporen

We hebben voor veel zaken die we vroeger in de fysieke wereld deden, nu een digitaal alternatief, die soms zelfs de oude manieren overbodig hebben gemaakt. Hierdoor ontstaan er continu nieuwe soorten digitale sporen.

Vroeger schreven we brieven, belden we met een vaste telefoon, of stuurden we een fax. Nu communiceren we via WhatsApp, e-mail en sociale media. Vroeger gebruikten we filmrolletjes, lieten die afdrukken en bewaarden de foto's in fotoalbums; nu maken we digitale foto's met onze smartphonecamera's en bewaren we ze "in de cloud". Vroeger lazen we boeken uit de bibliotheek of boekhandel; nu lezen we ook e-books op tablets of e-readers en luisteren we naar luisterboeken. Bankzaken regelen we nu via een app; vroeger moest je hiervoor naar het bankkantoor gaan of een acceptgiro invullen. We vergaderen nu vanuit huis via een videoverbinding. We winkelen in webshops en gaan steeds minder naar winkels in een winkelstraat. Vroeger hadden we cassettebandjes, cd's en vinylplaten; tegenwoordig luisteren we muziek via streamingdiensten, net als films en series. Vroeger huurden we videobanden bij de videotheek. En ga zo maar door. Al deze nieuwe manieren zorgen voor nieuwe sporen, die we niet zomaar allemaal begrijpen en kunnen duiden.

Naast dat alles nu digitaal is, verandert die digitale wereld ook continu. Ieder nieuw apparaat of nieuwe of geüpdatete app kan leiden tot andere of nieuwe sporen. Technieken die we vandaag kunnen gebruiken om data inzichtelijk te maken, werken morgen mogelijk niet meer.

NFI ontwerpt internationale kennisbank over digitaal forensisch onderzoek [23]
Het Nederlands Forensisch Instituut (NFI) heeft samen met de universiteiten van Oxford en Lausanne een raamwerk ontwikkeld voor een internationale kennisbank voor digitaal forensisch onderzoek. Harm van Beek van het NFI droeg bij aan het ontwerp van de kennisbank: “Nu is er nog geen centrale plaats om kennis te verzamelen over hoe je digitaal forensisch onderzoek doet. In de kennisbank worden de verschillende stappen in het forensische digitale proces op een eenduidige en gestructureerde manier vastgelegd. De kennisbank geeft digitaal forensisch onderzoekers straks meer grip op kennis en ontwikkelingen in de zich constant vernieuwende wereld van digitale forensische technieken.”

De kennisbank heet SOLVE-IT [14, 23], wat staat voor Systematic Objective-based Listing of Various Established (Digital) Investigation Techniques. Behalve de stappen in het proces, wordt ook vastgelegd welke technieken je kunt gebruiken, wat de kwetsbaarheden zijn, wat je kunt doen om deze te beperken en wordt er verwezen naar bronnen die meer informatie bieden.

Zie github.com/SOLVE-IT-DF/solve-it voor meer informatie.

3.2 Verschillende naamgeving van sporen

Een tweede uitdaging is dat we verschillende termen gebruiken voor hetzelfde. De ene app noemt een afbeelding bijvoorbeeld een ‘picture’, de andere een ‘image’ en weer een andere een ‘photo’. Als je als onderzoeker op zoek bent naar alle afbeeldingen, dan wil je sporen uit alle drie de apps vinden. Dit vraagt om een standaard: we maken een afspraak hoe we digitale objecten noemen.

In de digitale wereld gelden al veel standaarden, bijvoorbeeld standaarden die vastleggen hoe je pakketjes data over het internet kunt versturen. Ook voor e-mails hebben we al lang geleden, in 1982 om precies te zijn, een eerste standaard afgesproken [25]. Als je een mailtje stuurt, maakt het niet uit of de ontvanger Outlook, Gmail, of iCloud Mail gebruikt. Deze apps volgen allemaal de e-mailstandaard. Voor chat geldt dat (nog) niet. Je kunt nu bijvoorbeeld geen berichtje sturen van WhatsApp naar Signal.

Ondanks deze standaarden, is het nog steeds zo dat de ene app een e-mail een ‘mail’ noemt, en de andere app een ‘message’. En de ene app de

afzender de ‘from’ noemt en de andere app de ‘sender’. Er zijn meerdere initiatieven om tot eenduidige naamgeving te komen, in ieder geval voor digitaal-forensisch onderzoek. Hansken heeft hiervoor een uniform sporenmodel. Een groter internationaal initiatief is CASE, waarbij ik ben betrokken, dat mede gebaseerd is op de concepten van het sporenmodel van Hansken.

NFI een van de grondleggers van universele cybertaal die internationale strijd tegen criminaliteit makkelijker maakt [18]
Om criminaliteit effectief te bestrijden, is internationale samenwerking door opsporingsdiensten en digitaal-forensische onderzoekers essentieel. Denk bijvoorbeeld aan de uitwisseling van forensische instrumenten om cryptotelefoons uit te lezen. Om die samenwerking te vergemakkelijken, is het handig dat de instrumenten alle sporen in dezelfde ‘cybertaal’ vastleggen. Hiervoor is nu een internationale taal ontwikkeld: Cyberinvestigation Analysis Standard Expression (CASE) [4, 5, 18]. Het Nederlands Forensisch Instituut (NFI) is één van de grondleggers van deze wereldwijde taal.

Zie caseontology.org voor meer informatie over CASE.

3.3 Meerdere originelen van één object

In tegenstelling tot fysieke objecten, kunnen objecten in de digitale wereld op meerdere plaatsen tegelijk zijn. Een chatbericht dat je hebt gestuurd, zit bijvoorbeeld in jouw telefoon en tegelijkertijd in de telefoon van de ontvanger. Of de e-mail met de uitnodiging voor deze oratie die tegelijkertijd in al jullie computers en telefoons zit. Daarnaast worden data “in the cloud” op verschillende, vaak onbekende plaatsen tegelijkertijd opgeslagen. Weet jij waar jouw e-mail staat? Is dat in Nederland, of in het buitenland, of beide?

Als in een onderzoek meerdere verdachten zijn, dan zien we dus ook dat sporen meerdere keren in een zaak voorkomen. Dit maakt het voor de rechercheurs niet makkelijker, want na het filteren vinden ze soms vijf keer hetzelfde berichtje, of tien keer dezelfde afbeelding. En ze zijn op details vaak niet helemaal identiek. Bijvoorbeeld omdat een chatbericht van een iPhone naar een Android telefoon is gestuurd, of omdat een foto via WhatsApp bijgeknipt is. De sporen lijken dan op elkaar, maar zijn net anders vastgelegd in de data. Een open vraag is dan ook hoe we in het algemeen digitale sporen als uniek kunnen identificeren, en hoe we kunnen bepalen of sporen hetzelfde digitale object zijn.

3.4 Meerdere perspectieven op sporen

Als je filters toepast, ben je op zoek naar alle digitale sporen die aan je filter voldoen. Maar digitale sporen hebben vaak verschillende vormen, afhankelijk van hoe je ernaar kijkt. Een afbeelding kan bijvoorbeeld ook als e-mailbijlage voorkomen. Dus als je filtert op afbeeldingen, wil je deze vinden. Maar als je filtert op e-mailbijlagen, wil je ze ook tegenkomen. Dit fenomeen heeft ervoor gezorgd dat in het sporenmodel van Hansken, en ook in CASE, sporen vanuit meerdere perspectieven tegelijk beschreven kunnen worden.

3.5 Landsgrenzen bestaan niet

Een ander probleem in de digitale wereld is dat de landsgrenzen niet bestaan. Formeel bestaan deze wel, want een apparaat valt onder de wetten van het land waarin het zich bevindt. En voor de data die daarop staan, geldt dat dus ook. Voor data die “in de cloud” staan, bepalen complexe algoritmen waar deze data het beste opgeslagen kan worden. Daarbij houden de algoritmen, bewust of onbewust, niet altijd rekening met landsgrenzen. Voor de opsporingsdiensten is dit een groot probleem. Want binnen onze eigen grenzen gaan we zelf over onze wetgeving. Maar via de digitale weg kun je eenvoudig landsgrenzen passeren zonder toezicht. Zo kan een hacker uit het verre oosten via de digitale weg in Nederland digitale munten stelen [11]. Deze hacker voor de Nederlandse rechter brengen is vaak onbegonnen werk. Cybercriminaliteit, maar zeker ook de georganiseerde zware criminaliteit is een internationaal fenomeen, mede mogelijk gemaakt door alle digitale faciliteiten.

4 Betrouwbaarheid van onderzoeksresultaten

Het uniformeren en filteren werken goed bij sporen die wij als mensen gemaakt hebben, zoals de chatberichten en foto's. Dit geeft tactische informatie, die in het licht van de zaak een bepaald beeld ondersteunt of juist ontkracht. Zoals gezegd, kan er veel discussie zijn over digitale sporen. Deze discussie kan gaan over het proces van het verwerken van de data, over het eindresultaat van deze verwerking, of over de betekenis van deze resultaten in de context van de zaak.

4.1 Begrijpen wat de data betekenen

De data moeten zo worden gepresenteerd dat wij er onderzoek naar kunnen doen of dat analysesoftware de gegevens kunnen gebruiken voor (vervolg)analyses. Bestanden zoals afbeeldingen en documenten worden door computers en telefoons weergegeven op het scherm in een voor mensen begrijpelijk formaat. Op de gegevensdragers zelf worden deze echter digitaal gecodeerd en gestructureerd, oftewel "vertaald naar reeksen nullen en enen".

De codering van de data – het vastleggen van gegevens in een reeks nullen en enen – en de structuur van de data – hoe deze reeksen gecombineerd worden – bepalen wat de data betekenen. Deze "vertaling" vindt plaats door de programma's en apps die gebruikt zijn om de gegevens vast te leggen, zoals de camera-app, het Office-programma, het e-mailprogramma of de chat-app.

Omdat software continu doorontwikkelt – programma's en apps worden zeer regelmatig geüpdatet – verandert het gedrag van de software ook. Meestal heeft dit geen impact op hoe gegevens gecodeerd en gestructureerd worden, maar regelmatig worden bestaande en nieuwe gegevens hierdoor in nieuwe of andere coderingen en/of structuren vastgelegd.

Een deel van de gebruikte coderingen en structuren zijn bekend, maar een deel ook niet. Dit heeft vooral te maken met welk programma of app gebruikt is om de gegevens vast te leggen.

Programmeurs coderen software in programmacode. Deze programmacode heet de broncode. Om deze code uit te kunnen voeren op een computer, wordt deze omgezet (gecompileerd) in computerinstructies. Deze uitvoerbare code is voor mensen niet meer leesbaar. Als de broncode van het programma of de app beschikbaar is (open-source software), is de werking inzichtelijk en kan de codering en structuur achterhaald worden.

Het komt ook voor dat de gegevens gecodeerd en gestructureerd zijn volgens afgesproken standaarden. En sommige coderingen en structuren worden meer gebruikt dan andere. Ze worden dan een de-facto standaard, ofwel de eerste keuze voor ontwikkelaars van nieuwe of aangepaste software. Voorbeelden zijn ASCII voor tekst-codering, JPEG voor afbeeldingen, JSON voor gegevens en SQLite voor databases. Voor bekende coderingen en structuren bestaan vaak methoden om deze inzichtelijk te maken. En van deze methoden is vaak ook wel bekend hoe goed ze werken. Als de broncode van de software niet beschikbaar is en wanneer er geen documentatie is, dan zijn de coderingen en structuren niet bekend. Deze data inzichtelijk maken kan dan grofweg op vier manieren.

Allereerst kan gebruik worden gemaakt van de software die de data heeft vastgelegd. Dit maakt de data inzichtelijk, ondanks dat de codering en structuur van de data dan nog steeds onbekend zijn. Rechercheurs kunnen de data dan benaderen zoals een gewone gebruiker die met de software werkt. Dit kan bijvoorbeeld met complexe databases van boekhoudkundige programma's. De boekhouding kan dan met het boekhoudprogramma worden geopend en onderzocht.

Een tweede mogelijkheid is om met experimenten het gedrag van de software te onderzoeken. Door bekende ingevoerde gegevens te vergelijken met de tijdens de experimenten vastgelegde data, kan worden afgeleid hoe de gegevens in de data gecodeerd en gestructureerd zijn.

Als je bijvoorbeeld een chatberichtje stuurt naar een bekend telefoonnummer, kun je vaststellen waar het berichtje en het telefoonnummer in de data voorkomen.

Ten derde kunnen we de interne werking van de software onderzoeken. Door stapsgewijs de computerinstructies van de uitvoerbare code te volgen, kan worden uitgezocht hoe de software zich gedraagt. Dit heet reverse-engineering. Voor analyse van de code wordt tegenwoordig ook steeds vaker AI gebruikt.

De vierde optie is om allerlei bekende decodeermethoden toe te passen. Door verschillende bekende decodeermethoden uit te proberen op de data, kunnen de data mogelijk inzichtelijk gemaakt worden. Dit heet brute-forcing. Ook hier helpt AI een handje, bijvoorbeeld door slim patronen in de data te herkennen.

Vervolgens kunnen forensische onderzoeksprogramma's worden ontwikkeld om op basis van de opgedane kennis, de data inzichtelijk te maken. De resultaten van deze programma's kunnen uiteindelijk als bewijs dienen in de rechtbank. Omdat vaak niet alle mogelijkheden van de software kunnen worden onderzocht en er mogelijk aannames moeten worden gemaakt, kan zo'n programma onvolledige of onjuiste resultaten opleveren. Het is dus belangrijk dat de werking van deze programma's bekend is [8]. Als dat niet zo is, dan noemen we zo'n programma een 'black box'. Controleren met andere tools, waaronder de software die de data heeft gecodeerd en gestructureerd, is dan ook vrijwel altijd wenselijk. De resultaten van zo'n programma worden dan vergeleken met de resultaten van een ander programma. Dit heet *dual tool verification* [26, 29] en is een veel gebruikte manier om resultaten uit forensische onderzoeksprogramma's te controleren. De gedachte hierachter is dat als verschillende onderzoekers onafhankelijk van elkaar een eigen programma hebben ontwikkeld om data inzichtelijk te maken en deze verschillende programma's hetzelfde resultaat geven, dit resultaat gecontroleerd is.

4.2 Wat de sporen vertellen in een strafzaak

In strafzaken draait alles om waarheid en betrouwbaarheid. Dit gaat om het beantwoording van vragen zoals wie, wat, wanneer, hoe en waarom. Bewijs is geen doel op zich, maar een hulpmiddel om te komen tot een conclusie: heeft de verdachte het gedaan? En zo ja, hoe? In het recht gebruiken we hier een mooi woord voor: *redengevendheid*. Daarmee bedoelen we: in hoeverre ondersteunt een bepaald bewijsstuk de conclusie die we willen trekken?

Dat is niet altijd zo zwart-wit als het lijkt. Is het chatbericht door de verdachte zelf gestuurd of heeft iemand anders dit mogelijk gedaan? Is de e-mail verstuurd vanaf de telefoon of een andere computer? Wanneer is de website bezocht, was dit voor of na het delict? Waar is de foto gemaakt en met welk apparaat? Kortom: er is een spoor, maar hoe redengevend is het?

Bovenstaande vragen kunnen over vrijwel al het digitaal bewijs gesteld worden, je kunt er zelf vast nog veel meer bedenken. Om deze vragen te beantwoorden, onderzoeken forensisch deskundigen niet alleen de gevonden sporen, maar vaak ook de meer technische informatie die rondom de sporen in apparaten is vastgelegd. Denk hierbij aan instellingen en details van het historisch gebruik van de apparaten en apps. Dit is onderzoek op basis van wat de wetenschap ons leert. Het motto van het NFI is dan ook ‘gericht op waarheid, geleid door wetenschap, voor een veiliger samenleving.’

Figuur 4.1: Criminalistische zoom levels voor een afbeelding op een telefoon [16]

Afhankelijk van de vraag, wordt wetenschappelijke literatuur geraadpleegd, worden experimenten uitgevoerd om vergelijkbare sporen te kunnen reconstrueren, en worden de sporen met beschikbare of nieuw te ontwikkelen forensische programma's verder onderzocht.

Deze vragen kunnen om verschillende redenen gesteld worden. De beantwoording kan tijdens de opsporing richting geven, bijvoorbeeld voor het vinden van mogelijke verdachten, of het vaststellen van mogelijke scenario's. Dit noemen we sturingsinformatie.

Sporen kunnen ook dienen als bewijs in de rechtbank. In dat geval, doen we als gerechtelijk deskundigen een uitspraak over de sporen in het licht van verschillende hypothesen. Jouw chatberichtje over het 'net op tijd zijn bij deze oratie' heeft een bepaald gewicht in de weegschaal van Vrouwe Justitia, waarbij wordt afgewogen of je wel of niet iets gestolen hebt uit de supermarkt. Ook dat is nog best wel lastig, want uiteindelijk moet het berichtje ook aan jou persoonlijk gekoppeld kunnen worden. Was jij wel degene die dat berichtje met jouw telefoon stuurde? Of was dat iemand anders?

5 De leerstoel ‘Digital Forensics’

Het is jullie duidelijk geworden, dat er heel veel haken en ogen zitten aan het goed kunnen duiden van digitale sporen. Zowel bij het verkrijgen van data uit apparaten, als bij het vertalen van die data naar sporen die wij als mensen begrijpen, en bij het duiden van sporen in de context van een zaak. Met onderzoek binnen de leerstoel wil ik een aantal van deze onderwerpen aanpakken, maar zeker niet alle. De focus van het onderzoek ligt op het duiden van digitale sporen, binnen de juridische kaders en de context van een strafzaak. Deze leerstoel bevindt zich dus op het grensvlak van informatica, informatiekunde en recht. Het onderzoek heeft meerdere raakvlakken met onderzoek binnen de leerstoelen Software Engineering, Safe & Responsible AI en Cyber Security. De samenwerking tussen het NFI en de Open Universiteit is hierbij essentieel, met name met en tussen de vakgroepen Informatica, Informatiekunde en Publiekrecht (sectie Strafrecht).

5.1 Duiden met formele methoden

Ik heb een achtergrond in het modelleren van processen met formele methoden. Deze technieken worden nog minimaal toegepast voor (digitaal) forensisch onderzoek, hoewel ze veel elementen bevatten die juist belangrijk zijn voor opsporing en bewijsvoering in de rechtbank. Maar wat zijn formele methoden? Formele methoden zijn een soort supernauwkeurige manier van redeneren. Het zijn technieken uit de informatica en de wiskunde waarmee we systemen – denk aan software, netwerken, of (digitale) processen – tot in het kleinste detail kunnen beschrijven, controleren en/of analyseren. Je kunt het vergelijken met het verschil tussen een ruwe schets en een bouwtekening: de eerste geeft een globaal idee, de tweede vertelt hoe alles in elkaar zit.

Formele methoden maken gebruik van wiskundige logica en modellen om computersystemen of processen door te lichten. Ze worden bijvoorbeeld al jaren gebruikt in de luchtvaart en de spoorwegen. Denk aan een automatische piloot of een systeem dat treinen aanstuurt. In deze gevallen wil je écht zeker weten dat het goed gaat, want een klein foutje kan grote gevolgen hebben. Daarom worden deze systemen vaak formeel doorgerekend: Doet het in alle denkbare omstandigheden

wat je verwacht? Zijn er situaties waarin het systeem kan vastlopen of, erger nog, een ongeluk kan veroorzaken? Een bekend voorbeeld komt uit de ruimtevaart. NASA maakt bij de ontwikkeling van software voor ruimtevaartuigen gebruik van formele methoden om fouten te voorkomen. Bijvoorbeeld voor het systeem dat het Mars-rovertje Curiosity [28] bestuurt. Je kunt daar niet snel een update naartoe sturen als er iets misgaat, dus moet je van tevoren zeker weten dat alles klopt.

Maar wat als er toch iets is misgegaan? Dan willen we achteraf begrijpen hoe het is misgegaan. Ook daarvoor worden formele methoden ingezet. En dat is waar digitaal forensisch onderzoek om de hoek komt kijken. Bij digitaal forensisch onderzoek proberen we te achterhalen wat er is gebeurd: Wie heeft wat gedaan, wanneer en hoe? Zoals de winkeldiefstal waarvan jij verdacht wordt. De sporen die jij achterlaat zijn complex en niet altijd eenduidig. En hier komen formele methoden van pas. Zij helpen ons om die digitale sporen beter te begrijpen, structureren en analyseren. Ze dwingen ons om precies en transparant te redeneren: Wat weten we zeker op basis van de sporen? Wat zou er kunnen zijn gebeurd? En wat is uitgesloten? Formele methoden helpen hierbij door aannames expliciet en dus ook controleerbaar te maken.

5.1.1 Tijdslijnen reconstrueren

Een voorbeeld waarbij dit gebruik van formele methoden nuttig kan zijn, is het maken van tijdlijnen. Stel je voor: de politie vindt in jouw telefoon een aantal chatberichten, foto's en logregels. Er staan tijdstempels bij, maar sommige zijn onbetrouwbaar (bijvoorbeeld omdat de systeemklok verkeerd stond) [13]. Door gebruik te maken van formele modellen van tijd – bijvoorbeeld interval logica – kunnen we een consistente tijdlijn opstellen die rekening houdt met de onzekerheden. We kunnen dan zeggen: "Als deze foto is gemaakt ná dit chatbericht, dan moet deze handeling tussen ongeveer 16:00 en 16:05 hebben plaatsgevonden." Deze tijdsanalyses zijn essentieel om scenario's te vergelijken: klopt jouw alibi? Past jouw verhaal bij wat we digitaal kunnen reconstrueren?

5.1.2 Gedrag van systemen modelleren

Een ander voorbeeld is het gedrag van een app of een netwerk. Stel, de politie vermoedt dat jouw chat niet door jou is verstuurd maar automatisch door de app. Als onderzoeker wil je dan kunnen bepalen of

dit technisch mogelijk is. Door een formeel model te maken van hoe die app werkt – welke handelingen leiden tot welke sporen – kunnen we nagaan of dat scenario aannemelijk is. Is er bewijs voor automatisch gedrag, of zijn er menselijke handelingen nodig geweest? Deze redeneringen zijn sterk, omdat ze op logica gebaseerd zijn in plaats van op niet vastgelegde aannames.

5.1.3 Toetsen van scenario's

Formele methoden kunnen ook helpen om het beschikbare digitale bewijs te toetsen aan verschillende scenario's. Zo kunnen we bijvoorbeeld automatisch controleren welke sporen passen bij de scenario's, dus welke sporen redengevend zijn. Stel dat er discussie is of een USB-stick op een laptop van de verdachte is aangesloten. We kunnen dan formeel modelleren wat voor sporen een USB-aansluiting achterlaat, en wanneer. Zo kunnen we bepaalde scenario's uitsluiten, of juist aannemelijk maken.

Formele methoden zijn geen toverformule, maar eerder een slimme manier om zorgvuldig digitale puzzels te leggen. Zo helpen ze om vaagheden uit de discussie te halen. Ze maken het mogelijk om vragen te stellen als: Wat weten we zeker? Wat weten we niet? Welke feiten passen bij de scenario's? Dit soort vragen helpt niet alleen de onderzoekers, maar ook politie, officieren van justitie, rechters en advocaten om betere keuzes te maken en beslissingen te nemen. Ze maken de analyse herhaalbaar, transparant en controleerbaar. Dat is niet alleen goed voor de waarheidsvinding, maar ook voor de rechtszekerheid van verdachten.

5.2 Rechtmatig gebruik maken van digitale sporen

Jouw apparaten bevatten voor de opsporingsdiensten mogelijk waardevolle sporen. Ze kunnen cruciale aanwijzingen bevatten in een strafzaak. Maar dat betekent niet dat alles zomaar gebruikt mag worden voor een onderzoek. In het recht noemen we dat de 'toets op rechtmatigheid'. Daar horen een paar kernbegrippen bij. Allereerst, *proportionaliteit*: Het middel mag niet erger zijn dan de kwaal. Een complete kopie maken van alle data in jouw telefoon is waarschijnlijk niet proportioneel als je verdacht wordt van een enkele winkeldiefstal. Ten tweede, *privacy*: Jouw persoonlijke levenssfeer moet worden gerespecteerd, óók in een straf-

zaak [24]. Is het bijvoorbeeld nodig om iedereen in jouw adresboek te onderzoeken? Of al jouw privéfoto's van de afgelopen jaren te bekijken? En ten derde, het *verschoningsrecht* van advocaten, notarissen, artsen of geestelijken, met wie je informatie in vertrouwen deelt. 'In vertrouwen' betekent dat de politie deze communicatie dus ook niet mag inzien.

De realiteit is dat er vaak heel veel data zijn, die bijvoorbeeld met Hansken inzichtelijk en doorzoekbaar zijn gemaakt. Opsporingsdiensten moeten in die enorme hoeveelheden data zoeken naar dat éne stukje bewijs. En daar zit ook het risico: als je alles gaat doorzoeken "voor het geval dat", dan ben je al snel buitenproportioneel bezig. En bovendien: als je alle communicatie met een arts of advocaat ook inziet, loop je het risico dat het bewijs dat je wél vindt later niet mag worden gebruikt, omdat het onrechtmatig is verkregen. Dat is niet alleen inefficiënt, maar ook slecht voor het vertrouwen in de rechtstaat.

Formele methoden kunnen een rol spelen in het slim, precies en toetsbaar doorzoeken van grote hoeveelheden digitale data, zonder dat je meer ziet dan nodig is.

5.2.1 Verantwoord filteren

Soms bevat digitale data communicatie met personen die onder het verschoningsrecht vallen, bijvoorbeeld een advocaat. Die gegevens mogen niet worden ingezien, en al helemaal niet worden gebruikt in het onderzoek [10, 22]. Zowel formele methoden als AI kunnen helpen om automatisch zulke communicatie te herkennen, op basis van metadata (zoals het e-mailadres van de advocaat), communicatiepatronen, of zelfs stilistische kenmerken. Forensische programma's kunnen deze gegevens automatisch markeren of blokkeren, nog vóór dat een mens ze onder ogen krijgt. Op die manier kun je het verschoningsrecht niet alleen respecteren, maar ook technisch afdwingen. Dit vraagt nog wel om meer onderzoek, want dit moet op een transparante en verantwoorde manier gebeuren.

5.2.2 Proportioneel omgaan met data

Bij grootschalige digitale inbeslagnames – bijvoorbeeld bij de inbeslagname van servers of cloudopslag – is het belangrijk om niet méér te doen met de data dan nodig. Maar dit geldt ook voor kleinere dataverzamelin-

gen. De Hoge Raad concludeerde in 2017 in het smartphone-arrest [27] dat de politie een smartphone alleen beperkt mag bekijken. Voor een volledige doorzoeking van privégegevens is toestemming van een officier van justitie of rechter nodig. Na een uitspraak van het Europese Hof van Justitie in de zaak CG/Landeck [30], heeft de Hoge Raad in maart dit jaar gesteld dat er bij het onderzoek aan elektronische gegevensdragers 'geen grotere inbreuk mag worden gemaakt op de persoonlijke levenssfeer van de gebruiker dan noodzakelijk' [31]. Om dit te waarborgen, moet dit voor zover mogelijk geautomatiseerd worden gedaan.

Formele modellen kunnen worden gebruikt om zoekstrategieën vooraf te evalueren: welke data is relevant, en wat niet? Is het echt nodig om het hele archief door te nemen? Kun je een tussenstap inbouwen, bijvoorbeeld door eerst alleen metadata te bekijken? Door deze vragen vooraf formeel te modelleren, kun je het zoekproces efficiënt en doelgericht inrichten, waardoor het proportioneel blijft.

5.3 Een sterke strafrechtketen

Het mooie van deze formele aanpak is dat het ook het strafproces zelf helpt. Bewijs dat op een zorgvuldige, rechtmatige manier is verkregen, is veel sterker. De kans dat het standhoudt in de rechtszaal is groter. En het vertrouwen van burgers, verdachten én slachtoffers in een eerlijk proces neemt toe.

Formele methoden zijn dus geen rem op de opsporing, maar een kans: ze bieden manieren om het opsporingswerk preciezer, rechtvaardiger en transparanter te maken. En dat is precies waar het in de digitale rechtsstaat om draait. Dit onderzoeksprogramma is ambitieus en noodzakelijk gezien de centrale rol die digitale sporen spelen in de moderne misdaadbestrijding. Door de krachten van informatica, informatiekunde en rechtswetenschappen te bundelen en verbinding te leggen met de praktijk van het NFI, kan deze leerstoel de waarheidsvinding en de rechtspleging in Nederland en daarbuiten versterken.

Ik kijk ernaar uit om dit onderzoeksprogramma samen met collega's van de Open Universiteit, het NFI en andere partners tot uitvoering te brengen en daarmee een wetenschappelijke bijdrage te leveren aan een veiliger samenleving.

6 Dankwoord

Tot slot wil ik graag een aantal mensen bedanken.

Allereerst bedank ik het College van Bestuur van de Open Universiteit en in het bijzonder rector magnificus professor Theo Bastiaens, voor het in mij gestelde vertrouwen en mijn benoeming tot bijzonder hoogleraar Digital Forensics. Datzelfde geldt voor de directie van het NFI, algemeen directeur Marc Elsersohn en directeur Wetenschap & Technologie Annemieke de Vries.

Ik had deze leerstoel nooit kunnen bekleden, als professor Jos Baeten en professor Sjouke Mauw me in 2000 niet hadden overtuigd mijn afstudeerwerk voort te zetten in een promotieonderzoek. Bedankt voor het vertrouwen dat jullie toen in me hadden. En Jos, natuurlijk extra veel dank voor jouw bijdrage vanmiddag in het symposium.

Ik startte dat onderzoek in een periode waarin in met een aantal vrienden net een internetstartup was begonnen. Max Hufkens en Mark Hoogendoorn, maar ook alle andere oud-collega's van ISAAC, veel dank dat jullie me toen de ruimte hebben geven in deze uitdagende periode. En natuurlijk voor het begrip dat ik mijn carrière na tien jaar samenwerking een draai richting de (toegepaste) wetenschap wilde geven.

Ik bedank ook al mijn altijd behulpzame collega's en ex-collega's bij het NFI, vooral mijn collega's van Hansken, van de divisie Digitale & Biometrische Sporen, maar zeker ook van de verschillende ondersteunende diensten. En de mensen met wie ik samenwerk in de verschillende organisaties in de strafrechtketen. Dit zijn er te veel om hier allemaal individueel te noemen. Ik wil er toch een paar uitlichten. Ruud van Baar en Erwin van Eijk, omdat jullie met mij het diepe in hebben durven springen en de verantwoordelijkheid hebben genomen om samen Hansken te ontwikkelen. Hans Henseler, met jou heb ik de laatste jaren mijn wetenschappelijke ambities meer vorm kunnen geven. Veel dank daarvoor. Jeroen Venema, omdat je met jouw positieve energie het symposium vanmiddag tot een succes hebt gemaakt. En natuurlijk Martijn Egberts, voor jouw steun voor al het werk dat wij doen op het NFI en natuurlijk ook voor jouw bijdrage eerder vandaag.

Natuurlijk ook dank aan mijn nieuwe collega's van de Open Universiteit. Vincent van der Meer, bedankt voor jouw hulp in het voortraject van mijn benoeming en de verbinding met de decaan van de bétafaculteit, professor Petra de Weerd-Nederhof. Petra, jij hebt me vanaf onze eerste ontmoeting het vertrouwen gegeven en gesteund in het proces om bij de Open Universiteit deze bijzondere leerstoel te bekleden. Jouw *can do*-mentaliteit is aanstekelijk! Hugo Jonker, met jou heb ik veruit het meeste contact hier op de Open Universiteit. Ik geniet van onze discussies en waardeer je steun om de leerstoel invulling te geven. Professor Wilma Dreissen, bedankt voor jouw deelname in mijn curatorium en jouw presentatie vanmiddag. En natuurlijk veel dank aan de collega's die vanmiddag lightning talks hebben geven over de verschillende onderzoeken binnen de vakgroep Informatica.

Ook heel veel dank aan mijn familie en schoonfamilie. Mijn ouders hebben me geleerd dat hard werken loont. En zoals het tegeltje op jullie toilet in Westerhoven leert: *"Ge moet nie in problemen, mèr in oplossingen denken."* Jullie zorgen er samen met de rest van mijn familie voor dat ik met beide benen op de grond blijf. Daarnaast hebben jullie me altijd de ruimte gegeven om mijn eigen pad te volgen! Zonder die ruimte had ik hier niet gestaan.

Maar mijn allergrootste dank is natuurlijk voor mijn gezin, voor Cindy en mijn kinderen. Jullie steunen me altijd! Cin, op een of andere manier krijg jij het altijd voor elkaar om het gezin draaiende te houden en mij de ruimte te geven, zodat ik bijvoorbeeld regelmatig hier naar Heerlen af kan reizen. Wij leren onze kinderen dat ze vooral moeten genieten en lol moeten maken. Dus ik waardeer al jullie geintjes, zelfs over deze ceremoniële kledingstijl. Heel veel dank voor jullie steun en liefde.

Ik heb gezegd.

Referenties

Wetenschappelijke publicaties

[1] R. Bhoedjang, A. van Ballegooij, H. van Beek, J. van Schie, F. Dillema, R. van Baar, F. Ouwendijk en M. Streppel, “Engineering an online computer forensic service,” *Digital Investigation*, jrg. 9, nr. 2, p. 96–108, 2012. DOI: 10.1016/j.diin.2012.10.001.

[2] R. van Baar, H. van Beek en E. van Eijk, “Digital Forensics as a Service: A game changer,” *Digital Investigation*, jrg. 11, S54–S62, 2014, Proceedings of the First Annual DFRWS Europe. DOI: 10.1016/j.diin.2014.03.007.

[3] H. van Beek, E. van Eijk, R. van Baar, M. Ugen, J. Bodde en A. Siemelink, “Digital forensics as a service: Game on,” *Digital Investigation*, jrg. 15, p. 20–38, 2015, Special Issue: Big Data and Intelligent Data Analysis. DOI: 10.1016/j.diin.2015.07.004.

[4] E. Casey, S. Barnum, R. Griffith, J. Snyder, H. van Beek en A. Nelson, “Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language,” *Digital Investigation*, jrg. 22, p. 14–45, 2017. DOI: 10.1016/j.diin.2017.08.002.

[5] E. Casey, S. Barnum, R. Griffith, J. Snyder, H. van Beek en A. Nelson, “The Evolution of Expressing and Exchanging Cyber-Investigation Information in a Standardized Form,” in *Handling and Exchanging Electronic Evidence Across Europe*, M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci en F. Turchi, red. Cham: Springer International Publishing, 2018, p. 43–58. DOI: 10.1007/978-3-319-74872-6_4.

[6] H. van Beek, “A forensic visual aid: Traces versus knowledge,” *Science & Justice*, jrg. 58, nr. 6, p. 425–432, 2018. DOI: 10.1016/j.scijus.2018.08.006.

[7] H. van Beek, J. van den Bos, A. Boztas, E. van Eijk, R. Schramp en M. Ugen, “Digital forensics as a service: Stepping up the game,” *Forensic Science International: Digital Investigation*, jrg. 35, p. 301 021, 2020. DOI: 10.1016/j.fsidi.2020.301021.

[8] H. van Beek, “Forensische waarborgen in Hansken,” Nederlands Forensisch Instituut, Informatieblad, nov 2021.

[9] H. Henseler en H. van Beek, “ChatGPT as a Copilot for Investigating Digital Evidence,” in *Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace (LegalAIIA 2023)*, 2023, p. 58–69.

[10] H. van Beek, “Vernietigen van digitale sporen met verschoningsgerechtigde informatie,” Nederlands Forensisch Instituut, Informatieblad, apr 2023.

[11] R. Argentini en H. van Beek, “Bitcoin,” Nederlands Forensisch Instituut, Informatieblad, jan 2024.

[12] H. van Beek en H. Henseler, “Servicing Digital Investigations with Artificial Intelligence,” in *Artificial Intelligence (AI) in Forensic Sciences*, Z. Geradts en K. Franke, red., first edition, John Wiley & Sons Ltd, 2024, p. 103–122.

[13] C. Vanini, C. Hargreaves, H. van Beek en F. Breitinger, “Was the clock correct? Exploring timestamp interpretation through time anchors for digital forensic event reconstruction,” *Forensic Science International: Digital Investigation*, jrg. 49, 2024, DFRWS USA 2024 - Selected Papers from the 24th Annual Digital Forensics Research Conference USA. DOI: 10.1016/j.fsidi.2024.301759.

[14] C. Hargreaves, H. van Beek en E. Casey, “SOLVE-IT: A proposed digital forensic knowledge base inspired by MITRE ATT&CK,” *Forensic Science International: Digital Investigation*, jrg. 52, mrt 2025, DFRWS EU 2025 - Selected Papers from the 12th Annual Digital Forensics Research Conference Europe. DOI: 10.1016/j.fsidi.2025.301864.

[15] G. Michelet, H. Henseler, H. van Beek, M. Scanlon en F. Breitinger, “Fine-Tuning Large Language Models for Digital Forensics Investigations: Case Study and General Recommendations,” in *Proceedings of the 14th International Conference on IT Security Incident Management & IT Forensics (IMF 2025)*, sep 2025. DOI: 10.1145/3748264.

[16] H. van Beek, C. van den Pol en J. van der Weerd, “Criminalistic zoom levels: Unravelling the hierarchy of forensic traces,” *Forensic Science International*, jrg. 372, jul 2025. DOI: 10.1016/j.forsciint.2025.112498.

Media

[17] Nederlands Forensisch Instituut. “NFI bouwt krachtige forensische zoekmachine voor digitaal onderzoek.” (okt 2015), adres: https://www.forensischinstituut.nl/actueel/nieuws/2015/10/13/nfi-bouwt-krachtige-forensische-zoekmachine-voor-digitaal-onderzoek.

[18] Nederlands Forensisch Instituut. “NFI een van de grondleggers van universele cybertaal die internationale strijd tegen criminaliteit makkelijker maakt.” (feb 2022), adres: https://www.forensischinstituut.nl/actueel/nieuws/2022/02/02/nfi-een-van-de-grondleggers-van-universele-cybertaal-die-internationale-strijd-tegen-criminaliteit-makkelijker-maakt.

[19] Nederlands Forensisch Instituut. “Replica schedel Hansken van Rembrandthuis naar NFI.” (feb 2022), adres: https://www.forensischinstituut.nl/actueel/nieuws/2022/02/021/replica-schedel-hansken-van-rembrandthuis-naar-nfi.

[20] Nederlands Forensisch Instituut. “NFI maakt inzage cryptocommunicatie op werkplek advocaten mogelijk.” (mrt 2023), adres: https://www.forensischinstituut.nl/actueel/nieuws/2023/03/20/nfi-maakt-inzage-cryptocommunicatie-op-werkplek-advocaten-mogelijk.

[21] Nederlands Forensisch Instituut. “Digitaal forensisch platform Hansken winnaar European Public Sector Award.” (mrt 2024), adres: https://www.forensischinstituut.nl/actueel/nieuws/2024/03/21/digitaal-forensisch-platform-hansken-winnaar-european-public-sector-award.

[22] Nederlands Forensisch Instituut. “Digitaal platform Hansken helpt bij filteren van toegang tot informatie op digitale gegevensdragers.” (mei 2025), adres: https://www.forensischinstituut.nl/actueel/achtergrondverhalen-nfi/digitaal-platform-hansken-helpt-bij-filteren-van-toegang-tot-informatie-op-digitale-gegevensdragers-eafs-2025-deel-3.

[23] Nederlands Forensisch Instituut. “NFI ontwerpt internationale kennisbank over digitaal forensisch onderzoek.” (mei 2025), adres: https://www.forensischinstituut.nl/actueel/nieuws/2025/05/02/nfi-ontwerpt-internationale-kennisbank-over-digitaal-forensisch-onderzoek.

[24] Open Magazine, Open Universiteit. “Privacy en digitale opsporing, een lastig parket.” (mei 2025), adres: https://www.ou.nl/-/openmagazine-2025-vranken-dreissen-van-beek.

Overige referenties

[25] D. Crocker, *Standard for the format of ARPA internet text messages*, RFC 822, aug 1982. DOI: 10.17487/RFC0822.

[26] Association of Chief Police Officers (ACPO), “Good Practice and Advice Guide for Managers of e-Crime Investigation,” ACPO Managers Guide, sep 2010.

[27] Hoge Raad der Nederlanden, *Smartphone-arrest*, ECLI:NL:HR:2017:584, apr 2017.

[28] R. Cardoso, M. Farrell, M. Luckcuck, A. Ferrando en M. Fisher, “Heterogeneous Verification of an Autonomous Curiosity Rover,” in *NASA Formal Methods*, R. Lee, S. Jha, A. Mavridou en D. Giannakopoulou, red., Cham: Springer International Publishing, 2020, p. 353–360.

[29] Scientific Working Group on Digital Evidence (SWGDE), “SWGDE Best Practices for Mobile Device Forensic Analysis,” Best Pactices, sep 2020.

[30] Hof van Justitie EU, *C-548/21, C.G. v Bezirkshauptmannschaft Landeck*, ECLI:EU:C:2024:830, okt 2024.

[31] Hoge Raad der Nederlanden, *Uitspraak over rechtmatigheid onderzoek gegevensdragers*, ECLI:NL:HR:2025:409, mrt 2025.

Symposium: Digitale sporen op de juridische weegschaal

19 september 2025, Open Universiteit, Heerlen
De moderne samenleving digitaliseert. Digitaal bewijs speelt daarom een steeds grotere rol in strafrechtelijke onderzoeken en rechtszaken. Denk aan gegevens van mobiele telefoons, e-mails, sociale media-berichten, GPS-data en online transacties. Deze gegevens zijn vaak omvangrijk en complex. Zorgvuldige duiding van zulke “digitale sporen” is van cruciaal belang om ze als bewijs in een strafzaak te kunnen gebruiken. Voorafgaand aan de oratie, zijn tijdens dit symposium het belang van digitaal bewijs en de juridische complexe kaders voor digitale opsporing belicht. Ook is uitgelegd hoe het toepassen van formele methoden kan helpen bij het beter duiden van de beschikbare digitale sporen.

Opening
drs. J. (Jeroen) Venema, dagvoorzitter
product manager Hansken, Nederlands Forensisch Instituut

Tussen fictie en werkelijkheid.
Wat begrijpt de strafrechtjurist van de toekomst van digitaal?
mr. M.M. (Martijn) Egberts
landelijk officier van justitie Digitale Opsporing, Openbaar Ministerie

Lightning talks
Vakgroep informatica, Open Universiteit

Over digitaal bewijsmateriaal in strafzaken: vertrouwen is goed, controle is beter
prof. mr. dr. W.H.B. (Wilma) Dreissen
hoogleraar straf- en strafprocesrecht, Open Universiteit

Lightning talks
Vakgroep informatica, Open Universiteit

Formele Methoden voor Digital Forensics
em. prof. dr. J.C.M. (Jos) Baeten
fellow van het Centrum Wiskunde & Informatica

We laten allemaal continu digitale sporen achter. Als we deze sporen willen gebruiken voor een strafrechtelijk onderzoek, dan is dat lastiger dan het lijkt. Wat betekenen ze precies, en hoe zeker weten we dat?

De leerstoel Digital Forensics aan de Open Universiteit beoogt samen met het Nederlands Forensisch Instituut antwoorden te vinden door het nauwkeuriger duiden van digitale sporen binnen juridische kaders, mede door formele methoden, om zo bij te dragen aan een sterkere strafrechtketen in het digitale tijdperk.

Harm van Beek richt zich sinds 2009 op het gebruik van digitale data als bewijs in strafzaken. Hij doet dit als senior wetenschappelijk onderzoeker en gerechtelijk deskundige bij het Nederlands Forensisch Instituut en sinds september 2024 ook als bijzonder hoogleraar Digital Forensics aan de Open Universiteit. Harm is gepromoveerd in formele methoden (technische informatica) aan de TU Eindhoven (2005). Voorheen was hij medeoprichter en CTO van ISAAC, nu onderdeel van iO, een bedrijf met focus op digitale strategie en ontwerp, ontwikkeling en integratie van digitale systemen.

Open Universiteit